

Huawei Certification Training

HCIP-Security

Lab Guide

Version: V4.0



HUAWEI TECHNOLOGIES CO., LTD

Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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

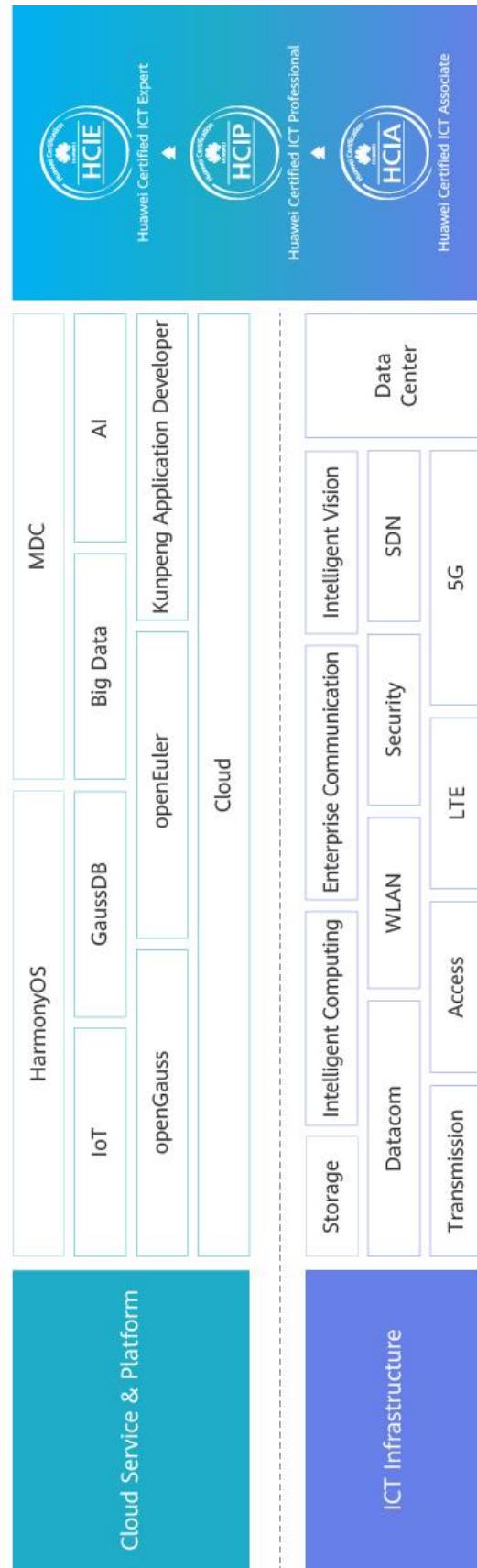
The Huawei certification system is a platform for shared growth, part of a thriving partner ecosystem. There are two types of certification: one for ICT architectures and applications, and one for cloud services and platforms.

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

Huawei certification courses cover the entire ICT domain, with a focus on how today's architecture generates cloud-pipe-device synergy. The courses present the latest developments of all essential ICT aspects to foster a thriving ICT talent ecosystem for the digital age.

Huawei Certified ICT Professional-Security (HCIP-Security) is designed for Huawei's frontline engineers and anyone who wants to understand Huawei's security products. HCIP-Security certification covers Huawei cyber security, content security, and WLAN security.

Huawei Certification



About This Document

Overview

This document is used for HCIP-Security certification training course. It is applicable to candidates who are preparing for HCIP-Security exams and readers who want to understand security basics, virtual systems, traffic management, user authentication, VPN technologies and troubleshooting, content security, attack defense, campus network design and construction, and security technology configuration and deployment.

Description

This lab guide contains 15 labs. Starting from hot backup of network security devices, this guide describes how to configure the firewall virtual system, traffic management, intelligent uplink selection, IPsec VPN, SSL VPN, anti-DDoS, content security, vulnerability and threat prevention, 802.1X wireless authentication, and Portal wireless authentication. The labs simulate faults in dual-device hot backup, IPsec VPN, SSL VPN, and Portal wireless authentication for troubleshooting.

This lab guide consists of the following labs:

- Lab 1: hot standby. The firewalls working in hot standby mode can automatically switch between the active and standby states based on the validity of the links where the outbound interfaces reside, ensuring service continuity.
- Lab 2: hot standby troubleshooting. In this lab, faults that may occur during deployment and maintenance of firewalls working in hot standby mode are simulated, and faults are effectively located. This lab helps you learn how to troubleshoot hot standby faults.
- Lab 3: traffic management. This lab focuses on IP address-based bandwidth management. This lab aims to help you understand how to configure IP address-based bandwidth management on the firewall.
- Lab 4: communication between virtual systems. This lab helps you understand application scenarios of virtual system communication and master the configuration methods.
- Lab 5: firewall intelligent uplink selection. By deploying the intelligent uplink selection on the firewall, you can select the optimal path for load balancing based on link quality.
- Lab 6: IPsec site-to-multisite application. By configuring the site-to-multisite IPsec VPN on the firewall, you can learn how to configure the site-to-multisite IPsec VPN and connect the networks.
- Lab 7: IPsec VPN troubleshooting. By solving problems that may occur during deployment and maintenance in the IPsec VPN site-to-multisite scenario, you can learn how to understand the IPsec VPN troubleshooting roadmap.

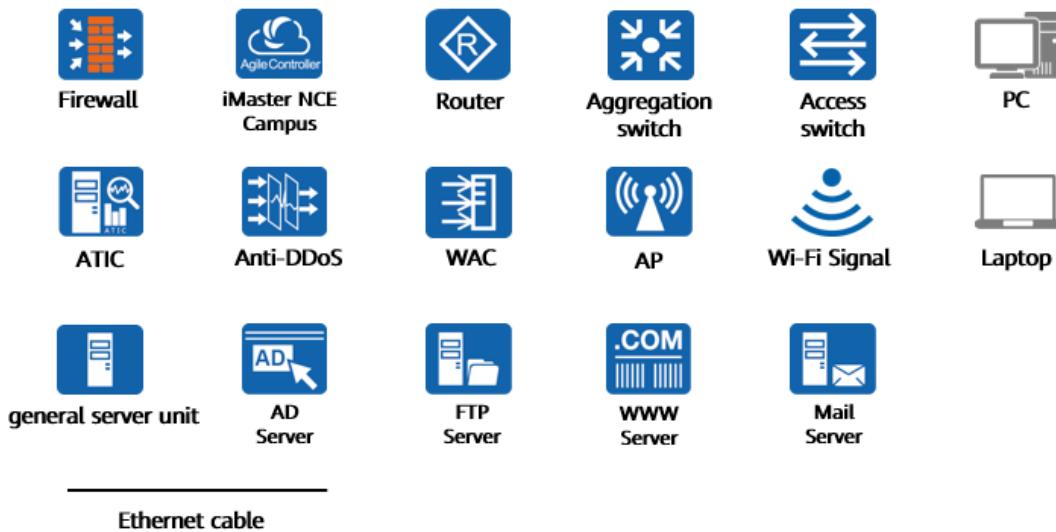
- Lab 8: SSL VPN troubleshooting. By solving problems that may occur during deployment and maintenance of SSL VPN network extension, you can learn how to understand the SSL VPN troubleshooting roadmap.
- Lab 9: anti-DDoS. Anti-DDoS devices are deployed at the enterprise egress to check the traffic from the Internet to the enterprise intranet and block threats in real time. This lab describes how to use and configure anti-DDoS devices.
- Lab 10: vulnerability and threat defense. In this lab, the intrusion prevention function is configured on the firewall device to defend against SQL injection attacks initiated by Internet users on the intranet web server. This lab helps you understand and master how to use the IPS function of the firewall.
- Lab 11: content security filtering. The URL filtering is deployed on the egress firewall to prevent employees from accessing game portals. The file blocking is deployed to block the download of executable files, reducing the risk of information leakage and virus infection on the intranet. The data filtering is deployed to filter files or applications containing confidential information, reducing the risk of leakage. All these operations help you understand how to configure firewall content security.
- Lab 12: 802.1X authentication. Enterprises usually deploy WLANs to provide wireless office environments for employees and 802.1X authentication is leveraged to authenticate access users. This lab describes how to implement 802.1X authentication.
- Lab 13: Portal authentication. Enterprises usually deploy WLANs to provide wireless office environments for employees and Portal authentication is leveraged to authenticate access users. This lab describes how to implement Portal authentication.
- Lab 14: Portal authentication troubleshooting. This lab simulates common faults that may occur during configuring and using Portal authentication and describes how to troubleshoot these faults.
- Lab 15: comprehensive exercise. It covers the design of a typical campus network, including the tasks of configuring link redundancy, device redundancy, VPN encrypted data transmission, service isolation, important service assurance, user authentication, user behavior audit, attack defense, and WLAN security policies. After completing these lab tasks, you shall understand the design logic of typical campus network topologies, master security protection methods of campus networks, and finally be able to build campus networks.

Background Knowledge Required

This is an HCIP course. The intended audience is expected to:

- Have basic computer skills.
- Be familiar with the principles of the TCP/IP protocol stack.
- Be familiar with the basic working principles of firewalls, Ethernet switches, routers, and WLAN.
- Have the knowledge and skills described in the HCIA-Security course.

Common Icons



Lab Environment Overview

Networking Introduction

This lab environment is intended for cyber security engineers who are preparing for the HCIP-Security exam. Each lab includes three firewalls, two enterprise egress routers, four switches for interconnection, one wireless access controller, one wireless access point (AP), two anti-DDoS devices, one ATIC, six servers of various types, and several PCs and laptops.

Device Introduction

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

The following table lists the devices, models, and versions.

Device Name	Device Model	Software Version
Firewall	USG6525E	V600R007C20SPC500
Enterprise egress router	AR6121E	V300R019C13SPC200
Switch for interconnection	S5735-S24T4X-X	V200R021C01SPC200
Wireless access controller	AC6508	V200R021C00SPC100
Wireless access point	AirEngine 5760-51	V200R021C00SPC100
Anti-DDoS	Anti-DDoS1905	V600R021C00SPC100
Anti-DDoS management center	SecoManager	V500R021C00SPC203

Authentication server	iMaster NCE-Campus	V300R021C00SPC110
-----------------------	--------------------	-------------------

Note: The port, output, and configuration information of devices in this document is provided based on the recommended topology. The actual information may vary according to the lab environment.

You can use a switch supporting Layer 3 functions as the switch for interconnection, with no specific requirement on the version.

Usage Instruction

Candidates must have basic understanding of datacom and HCIA-Security technologies. To reduce the pressure of datacom and basic configurations on candidates, the labs in the HCIP-Security lab guide focus on key devices and technologies, the configurations of interconnected devices in the lab topologies are displayed in the pre-configurations of the final configuration reference sections of each lab. The pre-configurations enables Layer 2 communication, routing, and others.

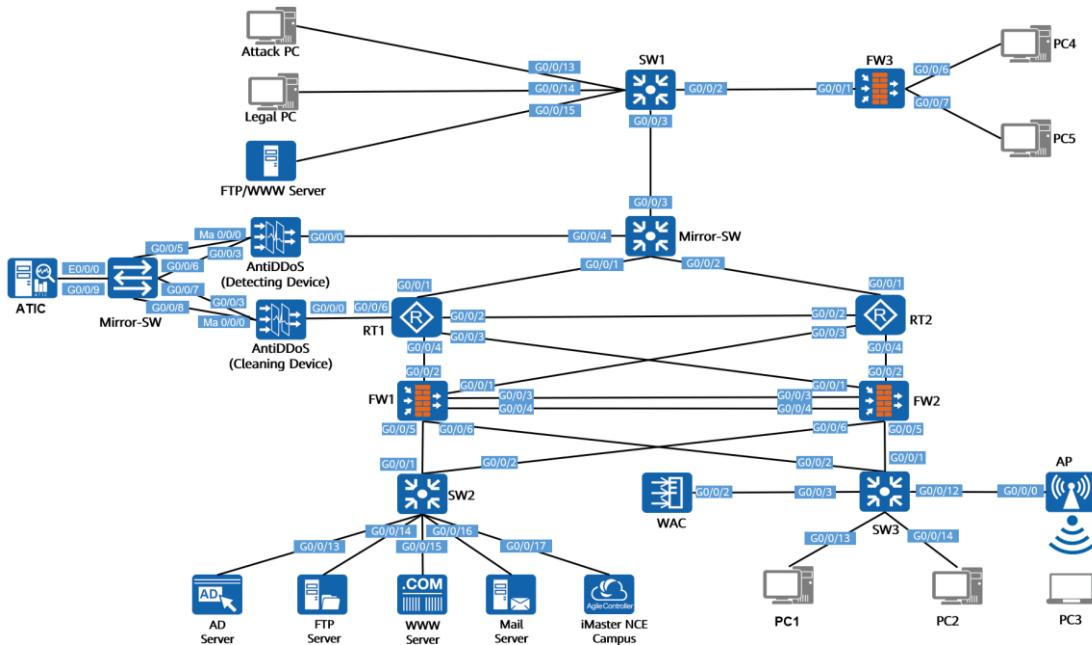
Lab Environment Preparation

Checking Devices

Before labs start, candidates of each group should check whether the devices in the following table are available:

Device Name	Quantity	Remarks
USG6525E	Three for each group	
AR6121E	Two for each group	
Huawei S5735	Four for each group	
AC6508	One for each group	
AirEngine 5760-51	One for each group	
Anti-DDoS1905	Two for each group	
SecoManager	One for each group	
NCE Campus	One for each group	
Virtual host	Seven	PC3 must be equipped with a wireless network adapter.
Virtual server	Five	
Twisted pair	Several	

Experiment Topology



The networking topology is described as follows:

This experiment topology simulates a medium-sized enterprise network. RT1 and RT2 function as enterprise border devices to connect to the Internet. FW1 and FW2 are deployed in hot standby mode to continuously provide services for enterprise networks.

Servers are deployed on the enterprise intranet in which terminals exist. Anti-DDoS devices monitor network intrusions. In addition, a WLAN is deployed inside the enterprise to provide services for wireless terminals.

FW3 is used in a simulated enterprise branch. The enterprise branch has two departments, and virtual firewalls need to be used to isolate services.

SW1, Legal PC, Attack PC, and FTP/WWW Server are devices on the Internet.

Labs in HCIP-Security v4.0 are completed in this topology.

Contents

About This Document	3
Overview	3
Description	3
Background Knowledge Required	4
Common Icons	5
Lab Environment Overview	5
Lab Environment Preparation	6
1 Firewall Hot Standby	16
1.1 Introduction	16
1.1.1 About This Lab	16
1.1.2 Objectives	16
1.1.3 Networking Topology	16
1.1.4 Lab Planning	17
1.2 Lab Configuration	19
1.2.1 Configuration Roadmap	19
1.2.2 Configuration Procedure on the CLI	19
1.2.3 Configuration Procedure on the Web UI	27
1.3 Verification	40
1.4 Configuration Reference	41
1.4.1 RT1's Configuration	41
1.4.2 RT2's Configuration	42
1.4.3 FW1's Configuration	43
1.4.4 FW2's Configuration	45
1.4.5 SW1's Pre-configuration	46
1.4.6 SW2's Pre-configuration	47
1.4.7 SW3's Pre-configuration	47
1.4.8 Mirror-SW's Pre-configuration	47
1.5 Quiz	48
2 Firewall Hot Standby Troubleshooting	49
2.1 Introduction	49
2.1.1 About This Lab	49
2.1.2 Objectives	49
2.1.3 Networking Topology	49
2.1.4 Lab Planning	50

2.2 Lab Configuration	52
2.2.1 Configuration Roadmap	52
2.2.2 Configuration Procedure	52
2.3 Configuration Reference	65
2.3.1 RT1's Configuration	65
2.3.2 RT2's Configuration	65
2.3.3 FW1's Configuration	66
2.3.4 FW2's Configuration	68
2.3.5 SW1's Configuration	69
2.3.6 SW2's Configuration	70
2.3.7 SW3's Configuration	70
2.3.8 Mirror-SW's Configuration	70
2.4 Quiz	71
3 Firewall Traffic Management	72
3.1 Introduction	72
3.1.1 About This Lab	72
3.1.2 Objectives	72
3.1.3 Networking Topology	72
3.1.4 Lab Planning	73
3.2 Lab Configuration	74
3.2.1 Configuration Roadmap	74
3.2.2 Configuration Procedure on the CLI	74
3.2.3 Configuration Procedure on the Web UI	76
3.3 Verification	83
3.4 Configuration Reference	87
3.4.1 FW2's Configuration	87
3.4.2 RT2's Pre-configuration	88
3.4.3 Mirror-SW's Pre-configuration	89
3.4.4 SW1's Pre-configuration	89
3.5 Quiz	89
4 Firewall Virtual System	91
4.1 Introduction	91
4.1.1 About This Lab	91
4.1.2 Objectives	91
4.1.3 Networking Topology	91
4.1.4 Lab Planning	92
4.2 Lab Configuration	93
4.2.1 Configuration Roadmap	93
4.2.2 Configuration Procedure on the CLI	93

4.2.3 Configuration Procedure on the Web UI.....	98
4.3 Verification.....	110
4.4 Configuration Reference.....	112
4.4.1 FW3's Configuration	112
4.4.2 SW1's Pre-configuration.....	116
4.5 Quiz	116
5 Firewall Intelligent Uplink Selection.....	117
5.1 Introduction	117
5.1.1 About This Lab.....	117
5.1.2 Objectives	117
5.1.3 Networking Topology.....	117
5.1.4 Lab Planning	118
5.2 Lab Configuration	119
5.2.1 Configuration Roadmap	119
5.2.2 Configuration Procedure on the CLI	120
5.2.3 Configuration Procedure on the Web UI.....	122
5.3 Verification.....	127
5.4 Configuration Reference.....	127
5.4.1 FW1's Configuration	127
5.4.2 RT1's Pre-configuration	128
5.4.3 RT2's Pre-configuration	129
5.4.4 SW1's Pre-configuration.....	129
5.4.5 Mirror-SW's Pre-configuration.....	130
5.4.6 SW3's Pre-configuration.....	130
5.5 Quiz	130
6 IPsec Site-to-Multisite Application.....	132
6.1 Introduction	132
6.1.1 About This Lab.....	132
6.1.2 Objectives	132
6.1.3 Networking Topology.....	132
6.1.4 Lab Planning	133
6.2 Lab Configuration	135
6.2.1 Configuration Roadmap	135
6.2.2 Configuration Procedure on the CLI	135
6.2.3 Configuration Procedure on the Web UI.....	142
6.3 Verification.....	152
6.4 Configuration Reference.....	156
6.4.1 FW1's Configuration	156
6.4.2 FW2's Configuration	158

6.4.3 FW3's Configuration	159
6.4.4 RT1's Pre-configuration	161
6.4.5 RT2's Pre-configuration	161
6.4.6 SW1's Pre-configuration.....	162
6.4.7 Mirror-SW's Pre-configuration.....	162
6.4.8 SW2's Pre-configuration.....	162
6.4.9 SW3's Pre-configuration.....	163
6.5 Quiz	163
7 IPsec VPN Troubleshooting	164
7.1 Introduction	164
7.1.1 About This Lab.....	164
7.1.2 Objectives	164
7.1.3 Networking Topology.....	164
7.1.4 Lab Planning	165
7.2 Lab Configuration	167
7.2.1 Configuration Roadmap	167
7.2.2 Configuration Procedure	167
7.3 Verification.....	186
7.4 Configuration Reference	186
7.4.1 FW1's Configuration	186
7.4.2 FW2's Configuration	188
7.4.3 FW3's Configuration	190
7.4.4 RT1's Configuration.....	191
7.4.5 RT2's Configuration.....	192
7.4.6 SW1's Configuration	192
7.4.7 Mirror-SW's Configuration	193
7.4.8 SW2's Configuration	193
7.4.9 SW3's Configuration	193
7.5 Quiz	194
8 SSL VPN Troubleshooting	195
8.1 Introduction	195
8.1.1 About This Lab	195
8.1.2 Objectives	195
8.1.3 Networking Topology.....	195
8.1.4 Lab Planning	196
8.2 Lab Configuration	197
8.2.1 Configuration Roadmap	197
8.2.2 Configuration Procedure	197
8.3 Configuration Reference	206

8.3.1 SW1's Configuration	206
8.3.2 Mirror-SW's Configuration	207
8.3.3 RT2's Configuration.....	207
8.3.4 FW2's Configuration	207
8.3.5 SW3's Configuration	209
8.4 Quiz	209
9 Anti-DDoS	211
9.1 Introduction.....	211
9.1.1 About This Lab.....	211
9.1.2 Objectives	211
9.1.3 Networking Topology.....	212
9.1.4 Lab Planning	213
9.2 Lab Configuration	215
9.2.1 Configuration Roadmap	215
9.2.2 Configuration Procedure	215
9.3 Verification.....	226
9.4 Configuration Reference.....	227
9.4.1 SW1's Pre-configuration.....	227
9.4.2 SW2's Pre-configuration.....	228
9.4.3 Mirror-SW's Pre-configuration.....	228
9.4.4 RT1's Configuration.....	228
9.4.5 FW1's Configuration	229
9.4.6 Anti-DDoS Detecting Device's Configuration	230
9.4.7 Anti-DDoS Cleaning Device's Configuration	234
9.5 Quiz	237
10 Vulnerability Defense	239
10.1 Introduction	239
10.1.1 About This Lab	239
10.1.2 Objectives	239
10.1.3 Networking Topology	239
10.1.4 Lab Planning	240
10.2 Lab Configuration	240
10.2.1 Configuration Roadmap.....	240
10.2.2 Configuration Procedure on the Web UI	241
10.2.3 Verification.....	249
10.3 Configuration Reference.....	250
10.3.1 RT1's Pre-configuration.....	250
10.3.2 FW1's Configuration	251
10.4 Quiz.....	252

11 Content Security Filtering.....	253
11.1 Introduction	253
11.1.1 About This Lab	253
11.1.2 Objectives.....	253
11.1.3 Networking Topology	253
11.1.4 Lab Planning	254
11.2 Lab Configuration.....	255
11.2.1 Configuration Roadmap.....	255
11.2.2 Configuration Procedure on the CLI.....	255
11.2.3 Configuration Procedure on the Web UI.....	258
11.3 Verification	263
11.4 Configuration Reference.....	268
11.4.1 FW1's Configuration.....	268
11.4.2 SW1's Pre-configuration	270
11.4.3 Mirror-SW's Pre-configuration	270
11.4.4 RT1's Pre-configuration.....	271
11.4.5 SW3's Pre-configuration	271
11.5 Quiz.....	271
12 802.1X Authentication.....	272
12.1 Introduction	272
12.1.1 About This Lab	272
12.1.2 Objectives.....	272
12.1.3 Networking Topology	272
12.1.4 Lab Planning	273
12.2 Lab Configuration.....	274
12.2.1 Configuration Roadmap.....	274
12.2.2 Configuration Procedure.....	274
12.3 Verification	284
12.4 Configuration Reference.....	286
12.4.1 SW2's Configuration.....	286
12.4.2 SW3's Configuration.....	286
12.4.3 FW2's Configuration.....	287
12.4.4 WAC's Configuration	287
12.5 Quiz.....	289
13 Portal Authentication	290
13.1 Introduction	290
13.1.1 About This Lab	290
13.1.2 Objectives.....	290

13.1.3 Networking Topology	290
13.1.4 Lab Planning	291
13.2 Lab Configuration	292
13.2.1 Configuration Roadmap.....	292
13.2.2 Configuration Procedure.....	292
13.3 Verification	298
13.4 Configuration Reference.....	300
13.4.1 SW2's Configuration.....	300
13.4.2 SW3's Configuration.....	300
13.4.3 FW2's Configuration.....	301
13.4.4 WAC's Configuration	301
13.5 Quiz.....	303
14 Portal Authentication Troubleshooting	304
14.1 Introduction	304
14.1.1 About This Lab	304
14.1.2 Objectives.....	304
14.1.3 Networking Topology	304
14.1.4 Lab Planning	305
14.2 Lab Configuration.....	306
14.2.1 Configuration Roadmap.....	306
14.2.2 Configuration Procedure.....	306
14.3 Verification	317
14.4 Configuration Reference.....	319
14.4.1 SW2's Configuration.....	319
14.4.2 SW3's Configuration.....	319
14.4.3 FW2's Configuration.....	320
14.4.4 WAC's Configuration	320
14.5 Quiz.....	322
15 Enterprise Network Security Deployment.....	324
15.1 Introduction	324
15.1.1 About This Lab	324
15.1.2 Objectives.....	324
15.1.3 Networking Topology	325
15.1.4 Lab Planning	326
15.2 Lab Configuration.....	331
15.2.1 Configuration Roadmap.....	331
15.2.2 Configuration Procedure.....	332
15.3 Verification	353
15.4 Configuration Reference.....	357

15.4.1 SW1's Configuration.....	357
15.4.2 SW2's Configuration.....	358
15.4.3 SW3's Configuration.....	359
15.4.4 Mirror-SW's Configuration.....	360
15.4.5 RT1's Configuration	360
15.4.6 RT2's Configuration	361
15.4.7 FW1's Configuration.....	362
15.4.8 FW2's Configuration.....	366
15.4.9 FW3's Configuration.....	370
15.4.10 WAC's Configuration.....	374
15.5 Quiz.....	376

1

Firewall Hot Standby

1.1 Introduction

1.1.1 About This Lab

Hosts on an enterprise intranet need to access the Internet. To prevent link interruption caused by network device faults or external uncontrollable factors, redundancy needs to be added to enterprise network devices to enhance network reliability.

In this lab, two firewalls are deployed in hot standby mode as gateways, and two routers are deployed as egress devices of the enterprise network. This ensures smooth communication between the intranet and Internet when a single device is faulty.

1.1.2 Objectives

- Firewalls connect to routers in the upstream direction and switches in the downstream direction and work in load balancing mode.
- Eth-Trunk and Bidirectional Forwarding Detection (BFD) are deployed to improve hot standby reliability.

1.1.3 Networking Topology

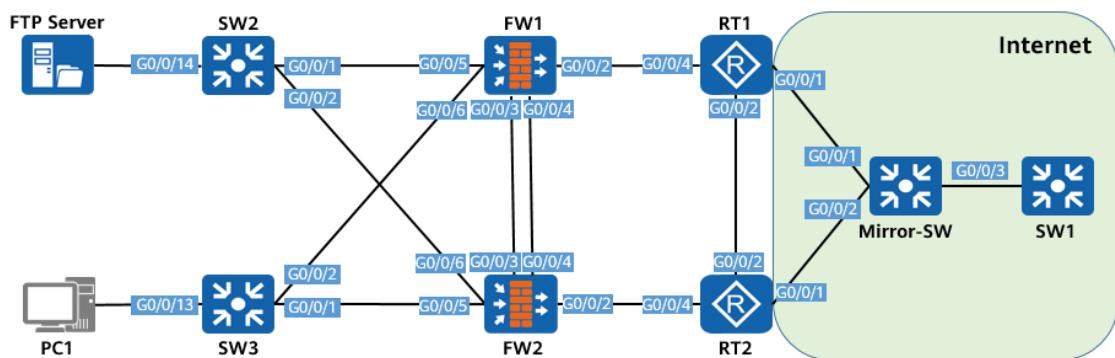


Figure 1-1 Hot standby

The preceding figure shows device connections. For details about IP address planning, see Table 1-1.

FW1 and FW2 work in hot standby mode. The gateways of PC1 and the FTP server are the VRRP1 and VRRP2 virtual gateways on the firewall, respectively. OSPF runs between IP addresses of the interfaces connecting to firewalls on RT1 and RT2, VRRP1 virtual gateway, and VRRP2 virtual gateway. RT1 and RT2 simulate the egresses of the enterprise network.

SW1 and Mirror-SW simulate the Internet. The lab purpose is that PC1 and the FTP server on the intranet can communicate with the Internet.

The configuration of SW1 and Mirror-SW simulating the Internet, as well as SW2 and SW3 functioning as access switches to connect to endpoints is not described in the following procedure. For details, see 1.4 Configuration Reference.

Disable the unused interfaces of FW1, FW2, RT1, and RT2 in the lab.

1.1.4 Lab Planning

Table 1-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
RT1	G0/0/1.2	Layer 3 sub-interface	4.4.4.2/30 Termination VLAN 2	Network outbound interface, connecting to Mirror-SW
	G0/0/2	Layer 3 interface	10.1.1.1/30	Interface for connecting to RT2
	G0/0/4	Layer 3 interface	10.3.1.1/30	Interface for connecting to FW1
	LoopBack0	Layer 3 interface	33.33.33.1/32	OSPF Router-ID
RT2	G0/0/1.40	Layer 3 sub-interface	3.3.3.2/30 Termination VLAN 40	Network outbound interface, connecting to Mirror-SW
	G0/0/2	Layer 3 interface	10.1.1.2/30	Interface for connecting to RT1
	G0/0/4	Layer 3 interface	10.6.1.1/30	Interface for connecting to FW2
	LoopBack0	Layer 3 interface	44.44.44.1/32	OSPF Router-ID
FW1	G0/0/2	Layer 3 interface	10.3.1.2/30 Security zone: Untrust	Interface for connecting to RT1 in the upstream direction
	G0/0/3	Eth-trunk 0 Aggregation interface	10.10.10.1/24 Security zone: DMZ	Hot standby heartbeat interfaces
	G0/0/4			

	G0/0/5	Layer 3 interface	172.16.30.2/24 Security zone: Trust	Interfaces for connecting to switches. VRRP virtual gateways need to be configured for the interfaces.
	G0/0/6	Layer 3 interface	172.16.20.2/24 Security zone: Trust	
	LoopBack0	Layer 3 interface	11.11.11.1/32	
FW2	G0/0/2	Layer 3 interface	10.6.1.2/30 Security zone: Untrust	Interface for connecting to RT2 in the upstream direction
	G0/0/3	Eth-trunk 0 Aggregation interface	10.10.10.2/24 Security zone: DMZ	Hot standby heartbeat interfaces
	G0/0/4			
	G0/0/5	Layer 3 interface	172.16.20.3/24 Security zone: Trust	Interfaces for connecting to switches. VRRP virtual gateways need to be configured for the interfaces.
	G0/0/6	Layer 3 interface	172.16.30.3/24 Security zone: Trust	
	LoopBack0	Layer 3 interface	22.22.22.1/32	
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interface for connecting to Mirror-SW
	VLANIF2	Layer 3 interface	4.4.4.1/30	Interface for directly connecting to the egress interface of RT1
	VLANIF40	Layer 3 interface	3.3.3.1/30	Interface for directly connecting to the egress interface of RT2
SW2	G0/0/1	Access	PVID: 30	Interfaces that allow only traffic of the service VLANs to pass through
	G0/0/2			
	G0/0/14			

SW3	G0/0/1	Access	PVID: 40	Interfaces that allow only traffic of the service VLANs to pass through
	G0/0/2			
	G0/0/13			
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interfaces that allow only traffic of the service VLANs to pass through
	G0/0/2			
	G0/0/3			
PC1	Ethernet0	Network adapter	172.16.20.10/24 Gateway: 172.16.20.1/24	Endpoint
FTP Server	Ethernet0	Network adapter	172.16.30.10/24 Gateway: 172.16.30.1/24	Endpoint

1.2 Lab Configuration

1.2.1 Configuration Roadmap

- Configure IP addresses for FW1, FW2, RT1, and RT2, as well as the security zones to which firewall interfaces belong.
- Configure OSPF on FW1, FW2, RT1, and RT2. RT1 and RT2 simulate the egresses of the enterprise network, and SW1 simulates the Internet. Configure a default route and NAT on RT1 and RT2, and import the default static route to OSPF so that PC1 and PC2 on the intranet can access the Internet.
- Complete the hot standby configuration of FW1 and FW2. Use Eth-Trunk interfaces as the heartbeat interfaces. Configure the two firewalls to connect to the downstream switches through VRRP.
- Configure firewall security policies as planned.
- Associate hot standby with BFD to detect whether a router is reachable in real time.

1.2.2 Configuration Procedure on the CLI

Step 1 Set basic network parameters.

Set basic network parameters according to the table in 1.1.4 Lab Planning.

SW1, SW2, SW3, and Mirror-SW are pre-configured. For details, see 1.4 Configuration Reference.

When configuring IP addresses for firewall interfaces, assign the interfaces to security zones according to Table 1-1. G0/0/1 on FW1 is used as an example. The configuration of other interfaces is similar to that of G0/0/1.

```
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface GigabitEthernet 0/0/1
```

```
[FW1-zone-untrust] quit
```

Step 2 Configure OSPF.

Configure OSPF on corresponding interfaces on FW1, FW2, RT1, and RT2 as planned, with the OSPF process ID being 1.

Configure OSPF on FW1 and enable OSPF on the interconnection interfaces, PC1 gateway interface, and PC2 gateway interface.

```
[FW1] ospf 1 router-id 11.11.11.1
[FW1-ospf-1] area 0
[FW1-ospf-1-area-0.0.0.0] quit
[FW1-ospf-1] quit
[FW1] interface GigabitEthernet0/0/2
[FW1-GigabitEthernet0/0/2] ospf enable 1 area 0
[FW1-GigabitEthernet0/0/2] quit
[FW1] interface GigabitEthernet0/0/5
[FW1-GigabitEthernet0/0/5] ospf enable 1 area 0
[FW1-GigabitEthernet0/0/5] quit
[FW1] interface GigabitEthernet0/0/6
[FW1-GigabitEthernet0/0/6] ospf enable 1 area 0
[FW1-GigabitEthernet0/0/6] quit
```

Configure OSPF on FW2 and enable OSPF on the interconnection interfaces, PC1 gateway interface, and PC2 gateway interface.

```
[FW2] ospf 1 router-id 22.22.22.2
[FW2-ospf-1] area 0
[FW2-ospf-1-area-0.0.0.0] quit
[FW2-ospf-1] quit
[FW2] interface GigabitEthernet0/0/2
[FW2-GigabitEthernet0/0/2] ospf enable 1 area 0
[FW2-GigabitEthernet0/0/2] quit
[FW2] interface GigabitEthernet0/0/5
[FW2-GigabitEthernet0/0/5] ospf enable 1 area 0
[FW2-GigabitEthernet0/0/5] quit
[FW2] interface GigabitEthernet0/0/6
[FW2-GigabitEthernet0/0/6] ospf enable 1 area 0
[FW2-GigabitEthernet0/0/6] quit
```

Configure OSPF on RT1, and enable OSPF on the interconnection interfaces.

```
[RT1] ospf 1 router-id 33.33.33.1
[RT1-ospf-1] area 0
[RT1-ospf-1-area-0.0.0.0] quit
[RT1-ospf-1] quit
[RT1] interface GigabitEthernet0/0/2
[RT1-GigabitEthernet0/0/2] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/2] quit
[RT1] interface GigabitEthernet0/0/4
[RT1-GigabitEthernet0/0/4] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/4] quit
```

Configure OSPF on RT2, and enable OSPF on the interconnection interfaces.

```
[RT2] ospf 1 router-id 44.44.44.1
[RT2-ospf-1] area 0
[RT2-ospf-1-area-0.0.0.0] quit
[RT2-ospf-1] quit
[RT2] interface GigabitEthernet0/0/2
[RT2-GigabitEthernet0/0/2] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/2] quit
[RT2] interface GigabitEthernet0/0/4
[RT2-GigabitEthernet0/0/4] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/4] quit
```

Whether OSPF packets are controlled by security policies depends on whether the **firewall packet-filter basic-protocol enable** command is configured. By default, **firewall packet-filter basic-protocol enable** is enabled on the USG6000E V6R7 firewalls. That is, OSPF packets are controlled by security policies. This section describes how to make OSPF packets not controlled by firewall security policies using the **undo firewall packet-filter basic-protocol enable** command.

Disable the function of controlling OSPF packets through security policies on FW1 and FW2.

```
[FW1] undo firewall packet-filter basic-protocol enable
```

```
[FW2] undo firewall packet-filter basic-protocol enable
```

Check the OSPF neighbor relationships on FW1 and RT2.

```
[FW1] display ospf peer brief
OSPF Process 1 with Router ID 11.11.11.1
Peer Statistic Information
-----
Area Id      Interface          Neighbor id    State
0.0.0.0      GigabitEthernet0/0/2  33.33.33.1   Full
0.0.0.0      GigabitEthernet0/0/5  22.22.22.1   Full
0.0.0.0      GigabitEthernet0/0/6  22.22.22.1   Full
-----
Total Peer(s): 3
```

```
[FW2] display ospf peer brief  
OSPF Process 1 with Router ID 22.22.22.1  
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GigabitEthernet0/0/2	44.44.44.1	Full
0.0.0.0	GigabitEthernet0/0/5	11.11.11.1	Full
0.0.0.0	GigabitEthernet0/0/6	11.11.11.1	Full

```
Total Peer(s): 3  
[FW2]
```

OSPF neighbor relationships have been established properly.

On RT1, add a default route to the Internet (SW1 in the networking topology).

```
[RT1] ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
```

On RT2, add a default route to the Internet (SW1 in the networking topology).

```
[RT2] ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
```

Configure a return route on SW1.

```
[SW1] ip route-static 0.0.0.0 0.0.0.0 4.4.4.2
```

Configure a source NAT policy on RT1 for source address translation when intranet users access the Internet.

```
[RT1] acl number 3500  
[RT1-acl-adv-3500] rule 5 permit ip  
[RT1-acl-adv-3500] quit  
[RT1] interface GigabitEthernet 0/0/1.2  
[RT1-GigabitEthernet0/0/1.2] nat outbound 3500  
[RT1-GigabitEthernet0/0/1.2] quit
```

Configure a source NAT policy on RT2 for source address translation when intranet users access the Internet.

```
[RT2] acl number 3500  
[RT2-acl-adv-3500] rule 5 permit ip  
[RT2-acl-adv-3500] quit  
[RT2] interface GigabitEthernet0/0/1.40  
[RT2-GigabitEthernet0/0/1.40] nat outbound 3500  
[RT2-GigabitEthernet0/0/1.40] quit
```

Import an external default route (that is, the default route destined for SW1) to OSPF on RT1.

```
[RT1] ospf 1  
[RT1-ospf-1] import-route static  
[RT1-ospf-1] default-route-advertise always
```

```
[RT1-ospf-1] quit
```

Import an external default route (that is, the default route destined for SW1) to OSPF on RT2.

```
[RT2] ospf 1
[RT2-ospf-1] import-route static
[RT2-ospf-1] default-route-advertise always
[RT2-ospf-1] quit
```

Check OSPF routes on FW1 and FW2.

```
[FW1] display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
-----
Public routing table : OSPF
    Destinations : 4      Routes : 6
OSPF routing table status : <Active>
    Destinations : 4      Routes : 6
Destination/Mask Proto Pre Cost   Flags NextHop       Interface
  0.0.0.0/0   O_ASE 150  1        D  10.3.1.1      GigabitEthernet0/0/2
  10.1.1.0/30 OSPF   10   2        D  10.3.1.1      GigabitEthernet0/0/2
  10.6.1.0/30 OSPF   10   2        D  172.16.30.3   GigabitEthernet0/0/5
                           OSPF   10   2        D  172.16.20.3   GigabitEthernet0/0/6
  172.16.20.1/32 OSPF   10   2        D  172.16.30.3   GigabitEthernet0/0/5
                           OSPF   10   2        D  172.16.20.3   GigabitEthernet0/0/6
OSPF routing table status : <Inactive>
    Destinations : 0      Routes : 0
```

```
[FW2] display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
-----
Public routing table : OSPF
    Destinations : 4      Routes : 6
OSPF routing table status : <Active>
    Destinations : 4      Routes : 6
Destination/Mask Proto Pre Cost   Flags NextHop       Interface
  0.0.0.0/0   O_ASE 150  1        D  10.6.1.1      GigabitEthernet0/0/2
  10.1.1.0/30 OSPF   10   2        D  10.6.1.1      GigabitEthernet0/0/2
  10.3.1.0/30 OSPF   10   2        D  172.16.30.2   GigabitEthernet0/0/6
                           OSPF   10   2        D  172.16.20.2   GigabitEthernet0/0/5
  172.16.30.1/32 OSPF   10   2        D  172.16.30.2   GigabitEthernet0/0/6
                           OSPF   10   2        D  172.16.20.2   GigabitEthernet0/0/5
OSPF routing table status : <Inactive>
    Destinations : 0      Routes : 0
```

FW1 and FW2 have learned routes in the entire OSPF area. FW1 has an external default route destined for RT1, and FW2 has an external default route destined for RT2.

Step 3 Configure hot standby.

Configure a VGMP group on firewalls to monitor the uplink interfaces, add the downlink interfaces to a VRRP group, and use an Eth-Trunk interface as the heartbeat interface.

Configure GigabitEthernet0/0/3 and GigabitEthernet0/0/4 as Eth-Trunk 0 on FW1.

```
[FW1] interface Eth-Trunk 0
[FW1-Eth-Trunk0] quit
[FW1] interface GigabitEthernet 0/0/3
[FW1-GigabitEthernet0/0/3] eth-trunk 0
[FW1-GigabitEthernet0/0/3] quit
[FW1] interface GigabitEthernet 0/0/4
[FW1-GigabitEthernet0/0/4] eth-trunk 0
[FW1-GigabitEthernet0/0/4] quit
```

Configure GigabitEthernet0/0/3 and GigabitEthernet0/0/4 as Eth-Trunk 0 on FW2.

```
[FW2] interface Eth-Trunk 0
[FW2-Eth-Trunk0] quit
[FW2] interface GigabitEthernet 0/0/3
[FW2-GigabitEthernet0/0/3] eth-trunk 0
[FW2-GigabitEthernet0/0/3] quit
[FW2] interface GigabitEthernet 0/0/4
[FW2-GigabitEthernet0/0/4] eth-trunk 0
[FW2-GigabitEthernet0/0/4] quit
```

Configure a VGMP group on the firewalls to monitor their uplink interfaces.

```
[FW1] hrp track interface GigabitEthernet 0/0/2
```

```
[FW2] hrp track interface GigabitEthernet 0/0/2
```

Configure VRRP group 1 on the downlink service interface GE0/0/6 of FW1 and set the status of the VRRP group to standby. Configure VRRP group 1 on the downlink service interface GE0/0/5 of FW2 and set the status of the VRRP group to active.

```
[FW1] interface GigabitEthernet 0/0/6
[FW1-GigabitEthernet0/0/6] vrrp vrid 1 virtual-ip 172.16.20.1 standby
[FW1-GigabitEthernet0/0/6] quit
```

```
[FW2] interface GigabitEthernet 0/0/5
[FW2-GigabitEthernet0/0/5] vrrp vrid 1 virtual-ip 172.16.20.1 active
[FW2-GigabitEthernet0/0/5] quit
```

Configure VRRP group 2 on the downlink service interface GE0/0/5 of FW1 and set the status of the VRRP group to active. Configure VRRP group 2 on the downlink service interface GE0/0/6 of FW2 and set the status of the VRRP group to standby.

```
[FW1] interface GigabitEthernet 0/0/5
```

```
[FW1-GigabitEthernet0/0/5] vrrp vrid 2 virtual-ip 172.16.30.1 active  
[FW1-GigabitEthernet0/0/5] quit
```

```
[FW2] interface GigabitEthernet 0/0/6  
[FW2-GigabitEthernet0/0/6] vrrp vrid 2 virtual-ip 172.16.30.1 standby  
[FW2-GigabitEthernet0/0/6] quit
```

Configure the function of adjusting the OSPF cost based on VGMP status on the firewalls.

```
[FW1] hrp adjust ospf-cost enable
```

```
[FW2] hrp adjust ospf-cost enable
```

In load sharing networking, configure quick session backup on the firewalls in case of inconsistent paths for forward and return packets.

```
[FW1] hrp mirror session enable
```

```
[FW2] hrp mirror session enable
```

Specify the heartbeat interface and enable hot standby on the firewalls.

```
[FW1] hrp interface Eth-Trunk0 remote 10.10.10.2  
[FW1] hrp enable
```

```
[FW2] hrp interface Eth-Trunk0 remote 10.10.10.1  
[FW2] hrp enable
```

Check the HRP hot standby status on the two firewalls.

```
HRP_M[FW1] display hrp state  
Role: active, peer: active  
Running priority: 45000, peer: 45000  
Backup channel usage: 0.00%  
Stable time: 0 days, 0 hours, 7 minutes  
Last state change information: 202X-XX-XX 17:08:46 HRP core state changed, old_state = abnormal(standby), new_state = normal, local_priority = 45000, peer_priority = 45000.
```

```
HRP_S[FW2] display hrp state  
Role: active, peer: active  
Running priority: 45000, peer: 45000
```

```
Backup channel usage: 0.00%
Stable time: 0 days, 0 hours, 7 minutes
Last state change information: 202X-XX-XX 17:08:55 HRP link changes to up.
```

Step 4 Configure security policies.

Because FW1 and FW2 work in hot standby mode, the security policy configuration on FW1 is automatically synchronized to FW2. Therefore, you only need to configure a security policy on FW1.

```
# Configure a security policy to allow intranet users to access the Internet.
```

```
HRP_M[FW1] security-policy
HRP_M[FW1-policy-security] rule name policy_sec1
HRP_M[FW1-policy-security-rule-policy_sec1] source-zone trust
HRP_M[FW1-policy-security-rule-policy_sec1] destination-zone untrust
HRP_M[FW1-policy-security-rule-policy_sec1] action permit
HRP_M[FW1-policy-security-rule-policy_sec1] quit
```

Step 5 Configure interworking between hot standby and BFD.

Firewalls monitor the outbound interfaces through interworking between BFD and hot standby. When the outbound interface of the link where FW1 resides goes Down, FW2 switches to the active device and takes over service traffic.

```
# Enable BFD globally on FW1 and configure BFD session 1 with peer IP address 4.4.4.2, local source IP address 10.3.1.2, local discriminator 20, and remote discriminator 10.
```

```
HRP_M[FW1] bfd
HRP_M[FW1-bfd] quit
HRP_M[FW1] bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2
HRP_M[FW1-bfd-session-1] discriminator local 20
HRP_M[FW1-bfd-session-1] discriminator remote 10
HRP_M[FW1-bfd-session-1] commit
HRP_M[FW1-bfd-session-1] quit
```

```
# Enable BFD globally on RT1 and configure BFD session 1 with peer IP address 10.3.1.2, local source IP address 4.4.4.2, local discriminator 10, and remote discriminator 20.
```

```
[RT1] bfd
[RT1] bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2
[RT1-bfd-session-1] discriminator local 10
[RT1-bfd-session-1] discriminator remote 20
[RT1-bfd-session-1] commit
[RT1-bfd-session-1] quit
```

```
# Enable BFD globally on FW2 and configure BFD session 2 with peer IP address 3.3.3.2, local source IP address 10.6.1.2, local discriminator 40, and remote discriminator 30.
```

```
HRP_S[FW2] bfd
HRP_S[FW2-bfd] quit
HRP_S[FW2] bfd 2 bind peer-ip 3.3.3.2 source-ip 10.6.1.2
HRP_S[FW2-bfd-session-2] discriminator local 40
HRP_S[FW2-bfd-session-2] discriminator remote 30
```

```
HRP_S[FW2-bfd-session-2] commit  
HRP_S[FW2-bfd-session-2] quit
```

Enable BFD globally on RT2 and configure BFD session 2 with peer IP address 10.6.1.2, local source IP address 3.3.3.2, local discriminator 30, and remote discriminator 40.

```
[RT2] bfd  
[RT2] bfd 2 bind peer-ip 10.6.1.2 source-ip 3.3.3.2  
[RT2-bfd-session-2] discriminator local 30  
[RT2-bfd-session-2] discriminator remote 40  
[RT2-bfd-session-2] commit  
[RT2-bfd-session-2] quit
```

Configure interworking between BFD and hot standby on FW1.

```
HRP_M[FW1] hrp track bfd-session 20
```

Configure interworking between BFD and hot standby on FW2.

```
HRP_S[FW2] hrp track bfd-session 40
```

1.2.3 Configuration Procedure on the Web UI

Step 1 Set basic network parameters.

Set basic network parameters according to the table in 1.1.4 Lab Planning.

SW1, SW2, SW3, and Mirror-SW are pre-configured. For details, see 1.4 Configuration Reference.

When configuring IP addresses for firewall interfaces, assign the interfaces to security zones according to Table 1-1. G0/0/2 on FW1 is used as an example. The configuration of other firewall interfaces is similar to that of G0/0/2. For basic configurations of router and switch interfaces, see Table 1-1.

Modify GigabitEthernet Interface

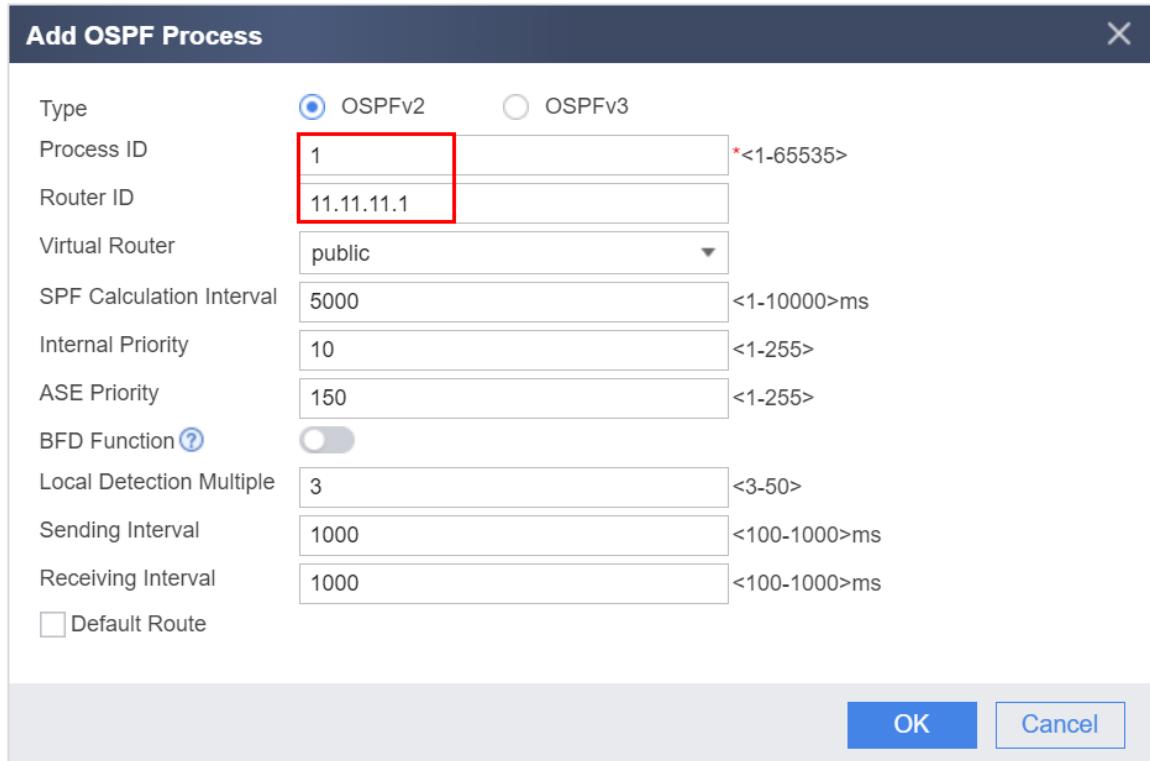
Interface Name	GigabitEthernet0/0/2 *
Alias	
Virtual System	public *
Zone	untrust
Mode	<input checked="" type="radio"/> Routing <input type="radio"/> Switching <input type="radio"/> Bypass <input type="radio"/> Interface Pair
IPv4 IPv6	
Connection Type	<input checked="" type="radio"/> Static IP <input type="radio"/> DHCP <input type="radio"/> PPPoE
IP Address	10.3.1.2/255.255.255.252
Enter each IP address on a separate line. For example: "10.10.1.2/255.255.255.0" "10.10.1.2/24".	

Step 2 Configure OSPF.

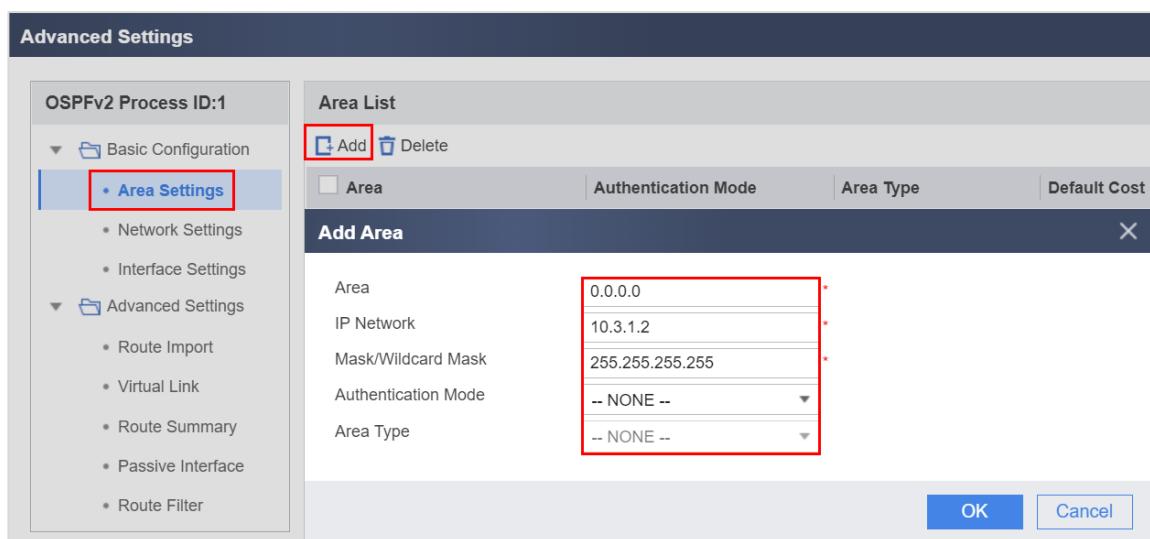
Configure OSPF on FW1, FW2, RT1, and RT2 as planned, set the router ID to the IP address of Loopback0 on each device, set the OSPF process ID to 1, and advertise the network segments where Loopback0 interfaces reside in the OSPF area.

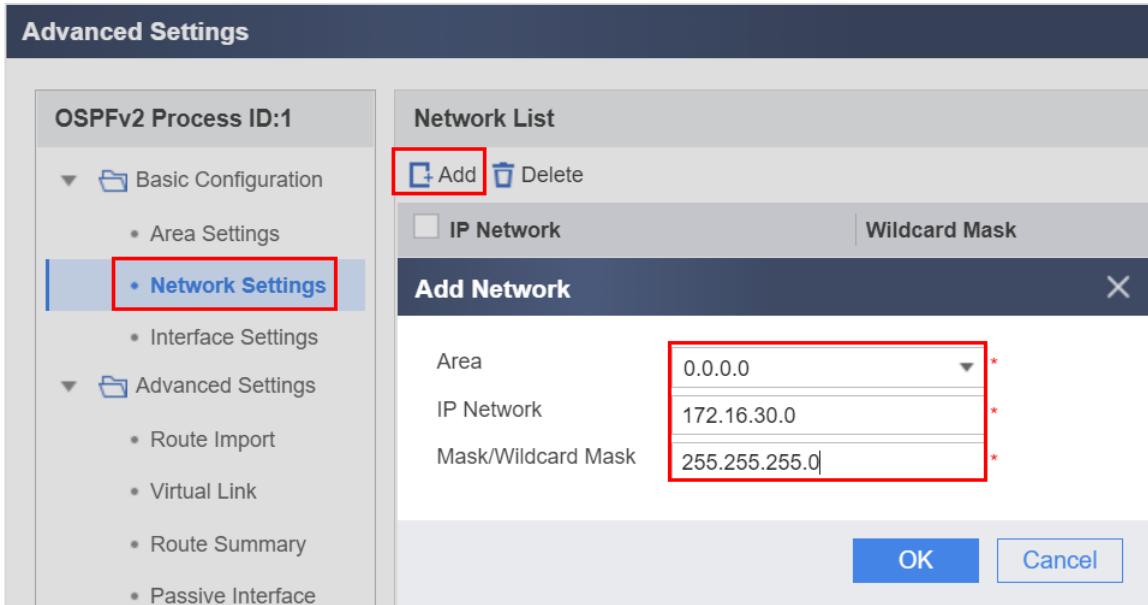
Configure OSPF on FW1 and advertise the network segments where the interconnection interfaces and the interfaces functioning as the gateways of PC1 and FTP server reside in the OSPF area.

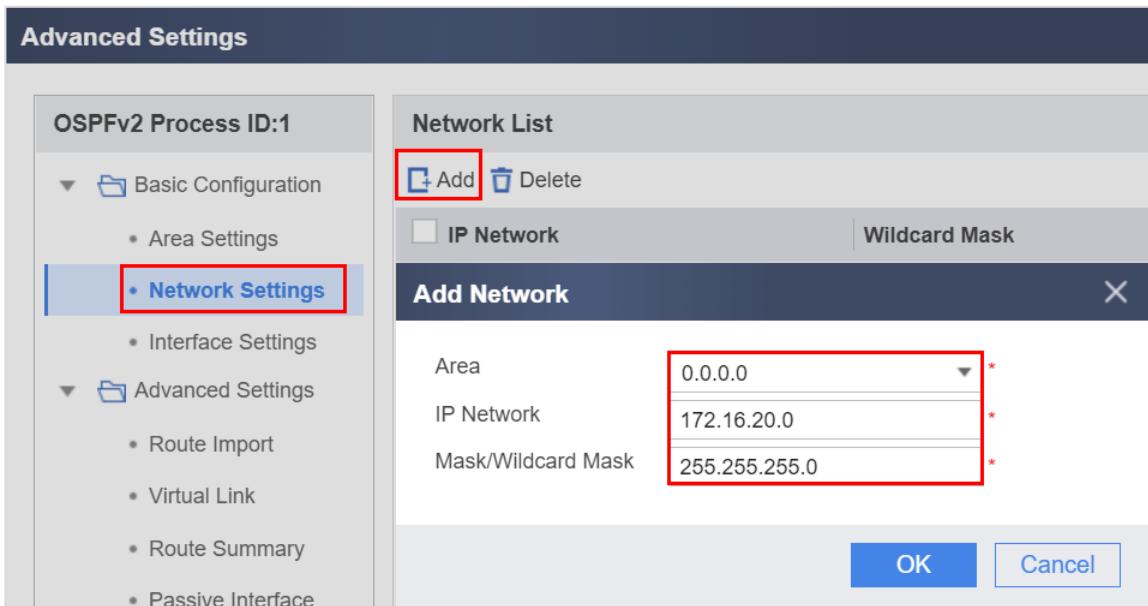
Choose **Network > Route > OSPF** and create an OSPF process in **OSPF Process List**.



Choose **Network > Route > OSPF**, click the newly created OSPF process in **OSPF Process List**, and click **Advanced Settings** to continue OSPF configurations.







Configure OSPF on FW2 and advertise the network segments where the interconnection interfaces and the interfaces functioning as the gateways of PC1 and FTP server reside in the OSPF area.

Choose **Network > Route > OSPF** and create an OSPF process in **OSPF Process List**.

Add OSPF Process

Type	<input checked="" type="radio"/> OSPFv2 <input type="radio"/> OSPFv3
Process ID	1 *<1-65535>
Router ID	22.22.22.1
Virtual Router	public
SPF Calculation Interval	5000 <1-10000>ms
Internal Priority	10 <1-255>
ASE Priority	150 <1-255>
BFD Function	<input type="checkbox"/>
Local Detection Multiple	3 <3-50>
Sending Interval	1000 <100-1000>ms
Receiving Interval	1000 <100-1000>ms
<input type="checkbox"/> Default Route	

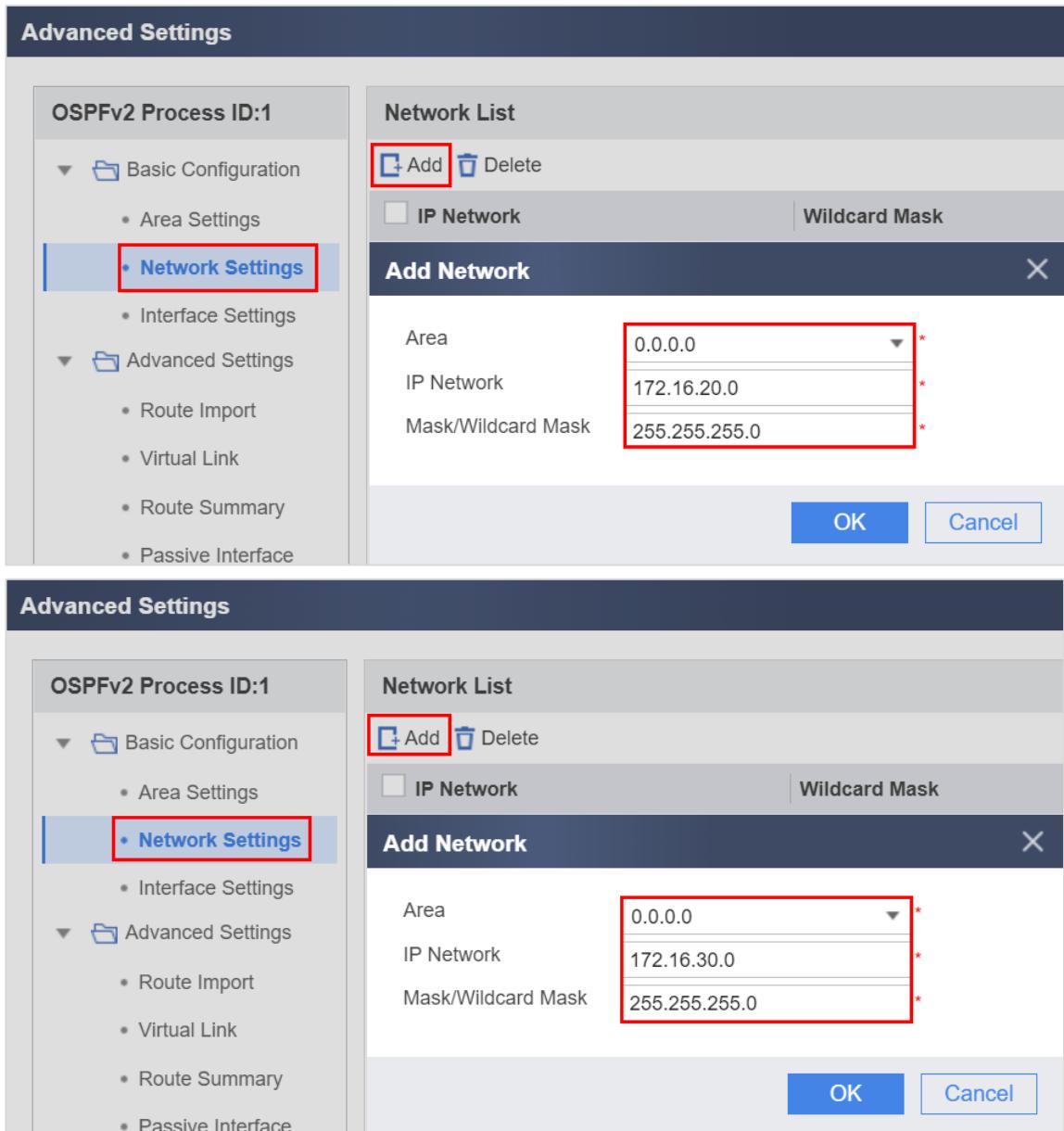
OK **Cancel**

Choose Network > Route > OSPF, click the newly created OSPF process in **OSPF Process List**, and click **Advanced Settings** to continue OSPF configurations.

Advanced Settings

OSPFv2 Process ID:1	Area List												
<ul style="list-style-type: none"> Basic Configuration Area Settings Network Settings Interface Settings 	<ul style="list-style-type: none"> Add Delete <table border="1"> <thead> <tr> <th>Area</th> <th>Authentication Mode</th> <th>Area Type</th> <th>Default Cost</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0</td> <td>10.6.1.2</td> <td>255.255.255.255</td> <td>-- NONE --</td> </tr> <tr> <td>-- NONE --</td> <td>-- NONE --</td> <td>-- NONE --</td> <td>-- NONE --</td> </tr> </tbody> </table>	Area	Authentication Mode	Area Type	Default Cost	0.0.0.0	10.6.1.2	255.255.255.255	-- NONE --				
Area	Authentication Mode	Area Type	Default Cost										
0.0.0.0	10.6.1.2	255.255.255.255	-- NONE --										
-- NONE --	-- NONE --	-- NONE --	-- NONE --										
<ul style="list-style-type: none"> Advanced Settings Route Import Virtual Link Route Summary Passive Interface Route Filter 	<p>Add Area</p> <table border="1"> <tr> <td>Area</td> <td>0.0.0.0</td> </tr> <tr> <td>IP Network</td> <td>10.6.1.2</td> </tr> <tr> <td>Mask/Wildcard Mask</td> <td>255.255.255.255</td> </tr> <tr> <td>Authentication Mode</td> <td>-- NONE --</td> </tr> <tr> <td>Area Type</td> <td>-- NONE --</td> </tr> </table>	Area	0.0.0.0	IP Network	10.6.1.2	Mask/Wildcard Mask	255.255.255.255	Authentication Mode	-- NONE --	Area Type	-- NONE --		
Area	0.0.0.0												
IP Network	10.6.1.2												
Mask/Wildcard Mask	255.255.255.255												
Authentication Mode	-- NONE --												
Area Type	-- NONE --												

OK **Cancel**



The screenshot shows two instances of the 'Advanced Settings' interface for OSPFv2. In both cases, the 'Network Settings' option is selected under the 'OSPFv2 Process ID:1' section. A red box highlights the 'IP Network' field in the 'Add Network' dialog, which contains the values: Area 0.0.0.0, IP Network 172.16.20.0, and Mask/Wildcard Mask 255.255.255.0.

Whether OSPF packets are controlled by security policies depends on whether the **firewall packet-filter basic-protocol enable** command is configured. By default, **firewall packet-filter basic-protocol enable** is enabled on the USG6000E V6R7 firewalls. That is, OSPF packets are controlled by security policies. This section describes how to make OSPF packets not controlled by firewall security policies using the **undo firewall packet-filter basic-protocol enable** command.

Click **CLI Console** in the lower right corner on the web UI of FW1 and FW2, and run the following commands:

```
<FW1> system-view
Enter system view, return user view with Ctrl+Z.
[FW1] undo firewall packet-filter basic-protocol enable
[FW1]
```

```
<FW2> system-view
Enter system view, return user view with Ctrl+Z.
[FW2] undo firewall packet-filter basic-protocol enable
[FW2]
```

Configure OSPF on RT1, and enable OSPF on the interconnection interfaces.

```
[RT1] ospf 1 router-id 33.33.33.1
[RT1-ospf-1] area 0
[RT1-ospf-1-area-0.0.0.0] quit
[RT1-ospf-1] quit
[RT1]interface GigabitEthernet0/0/2
[RT1-GigabitEthernet0/0/2] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/2] quit
[RT1]interface GigabitEthernet0/0/4
[RT1-GigabitEthernet0/0/4] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/4] quit
```

Configure OSPF on RT2, and enable OSPF on the interconnection interfaces.

```
[RT2] ospf 1 router-id 44.44.44.1
[RT2-ospf-1] area 0
[RT2-ospf-1-area-0.0.0.0] quit
[RT2-ospf-1] quit
[RT2]interface GigabitEthernet0/0/2
[RT2-GigabitEthernet0/0/2] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/2] quit
[RT2]interface GigabitEthernet0/0/4
[RT2-GigabitEthernet0/0/4] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/4] quit
```

Check the OSPF neighbor relationships on FW2.

OSPF Peer List					
Interface	Peer Router ID	Peer Address	Peer State	Designated Router (DR)	Backup Designated Router (BDR)
▲ OSPFv2 Process ID:1 (Router ID:22.22.22.1)					
GE0/0/2	44.44.44.1	10.6.1.1	Full	10.6.1.2	10.6.1.1
GE0/0/5	11.11.11.1	172.16.20.2	Full	172.16.20.2	172.16.20.3
GE0/0/6	11.11.11.1	172.16.30.2	Full	172.16.30.2	172.16.30.3

Check the OSPF neighbor relationship on RT2.

```
[RT2]display ospf peer brief
      OSPF Process 1 with Router ID 44.44.44.1
      Peer Statistic Information
-----
      Area Id          Interface          Neighbor id        State
      0.0.0.0          GigabitEthernet0/0/2    33.33.33.1       Full
      0.0.0.0          GigabitEthernet0/0/4    22.22.22.1       Full
-----
      Total Peer(s):   2
```

OSPF neighbor relationships have been established properly.

On RT1, add a default route to the Internet (SW1 in the networking topology).

```
[RT1]ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
```

On RT2, add a default route to the Internet (SW1 in the networking topology).

```
[RT1]ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
```

Configure a source NAT policy on RT1 for source address translation when intranet users access the Internet.

```
[RT1] acl number 3500  
[RT1-acl-adv-3500] rule 5 permit ip  
[RT1-acl-adv-3500] quit  
[RT1] interface GigabitEthernet 0/0/1.2  
[RT1-GigabitEthernet0/0/1.2] nat outbound 3500  
[RT1-GigabitEthernet0/0/1.2] quit
```

Configure a source NAT policy on RT2 for source address translation when intranet users access the Internet.

```
[RT2] acl number 3500  
[RT2-acl-adv-3500] rule 5 permit ip  
[RT2-acl-adv-3500] quit  
[RT2] interface GigabitEthernet0/0/1.40  
[RT2-GigabitEthernet0/0/1.40] nat outbound 3500  
[RT2-GigabitEthernet0/0/1.40] quit
```

Import an external default route (that is, the default route to SW1) to OSPF on RT1.

```
[RT1]ospf 1  
[RT1-ospf-1]import-route static  
[RT1-ospf-1]default-route-advertise always  
[RT1-ospf-1]quit
```

Import an external default route (that is, the default route to SW1) to OSPF on RT2.

```
[RT2]ospf 1  
[RT2-ospf-1]import-route static  
[RT2-ospf-1]default-route-advertise always  
[RT2-ospf-1]quit
```

Choose **Network > Route > Routing Table** on the web UI of FW1 to check OSPF routes.

Routing Table					
Protocol	Destination/Mask	Priority	Cost	Next Hop	Interface
OSPF	0.0.0.0/0	150	1	10.3.1.1	GE0/0/2
OSPF	10.1.1.0/30	10	2	10.3.1.1	GE0/0/2
Direct	10.3.1.0/30	0	0	10.3.1.2	GE0/0/2
Direct	10.3.1.2/32	0	0	127.0.0.1	GE0/0/2
Direct	10.3.1.3/32	0	0	127.0.0.1	GE0/0/2

Choose Network > Route > Routing Table on the web UI of FW2 to check OSPF routes.

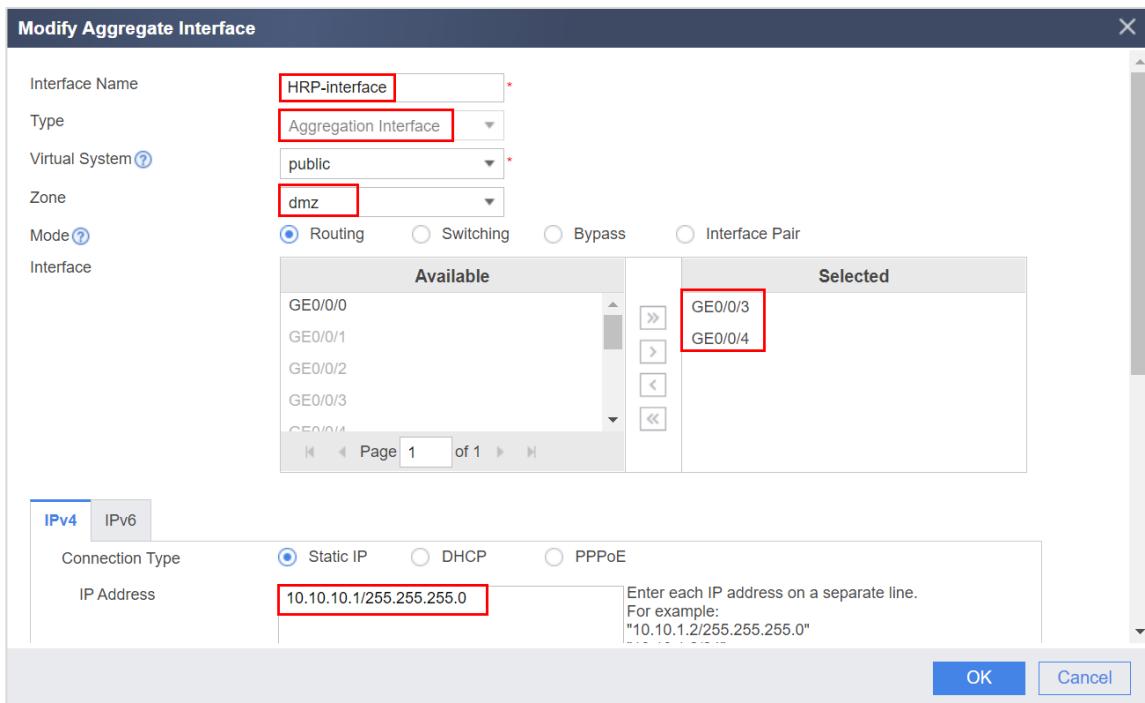
Routing Table					
Protocol	Destination/Mask	Priority	Cost	Next Hop	Interface
OSPF	0.0.0.0/0	150	1	10.6.1.1	GE0/0/2
OSPF	10.1.1.0/30	10	2	10.6.1.1	GE0/0/2
OSPF	10.3.1.0/30	10	2	172.16.30.2	GE0/0/6
OSPF	10.3.1.0/30	10	2	172.16.20.2	GE0/0/5
Direct	10.6.1.0/30	0	0	10.6.1.2	GE0/0/2

FW1 and FW2 have learned routes in the entire OSPF area. FW1 has an external default route destined for RT1, and FW2 has an external default route destined for RT2.

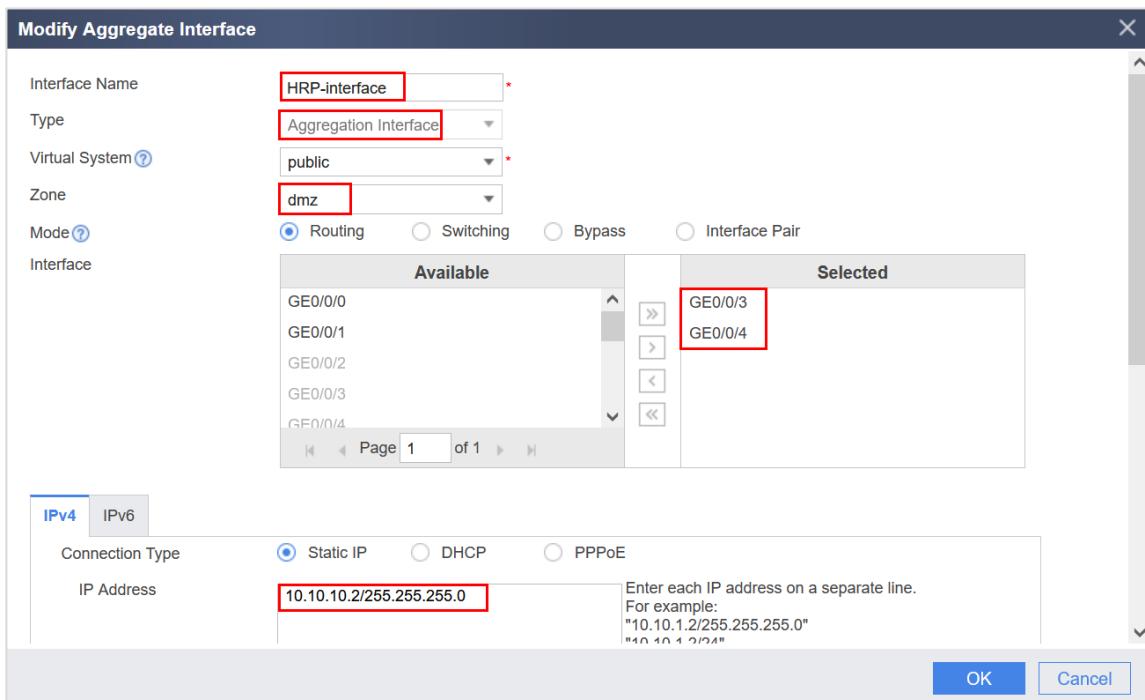
Step 3 Configure the hot standby and BFD functions.

Configure a VGMP group on firewalls to monitor the uplink interfaces, add the downlink interfaces to a VRRP group, and use an Eth-Trunk interface as the heartbeat interface.

Configure GigabitEthernet0/0/3 and GigabitEthernet0/0/4 as Eth-Trunk 0 on FW1.



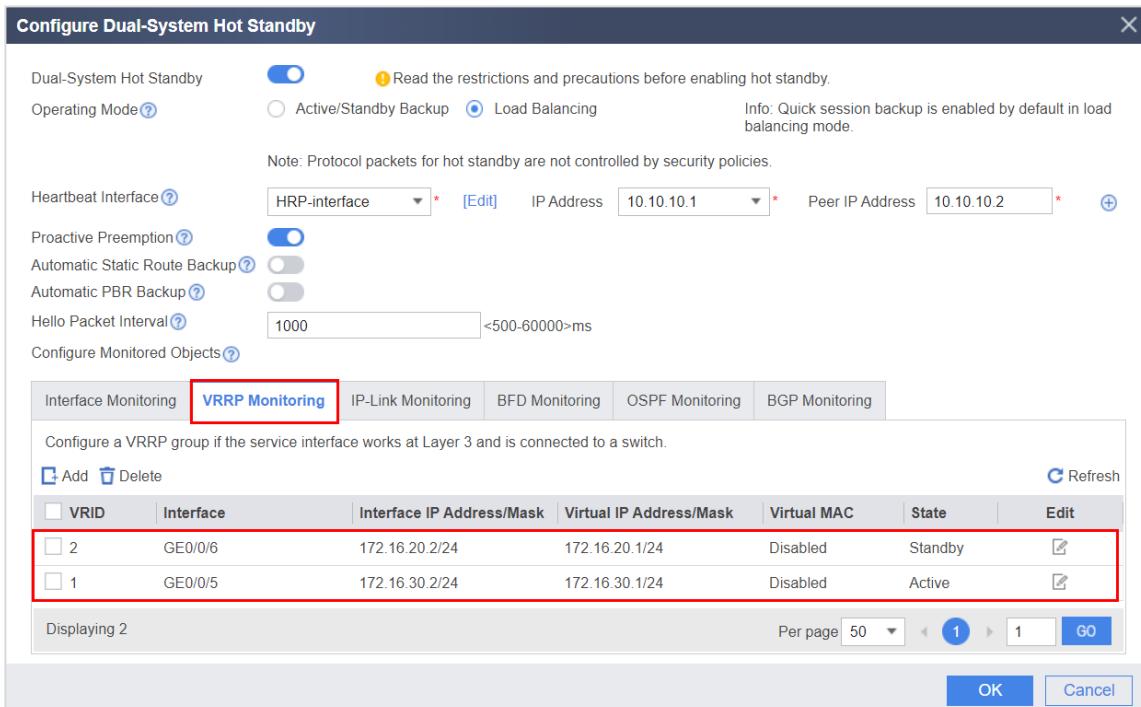
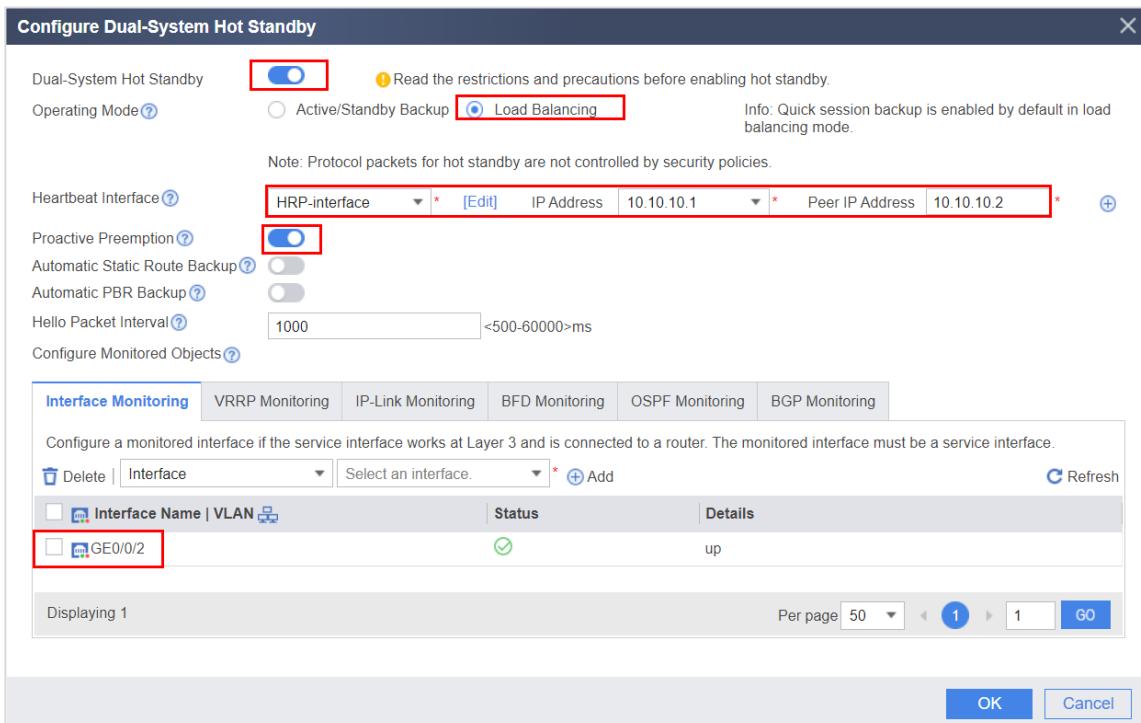
Configure GigabitEthernet0/0/3 and GigabitEthernet0/0/4 as Eth-Trunk 0 on FW2.

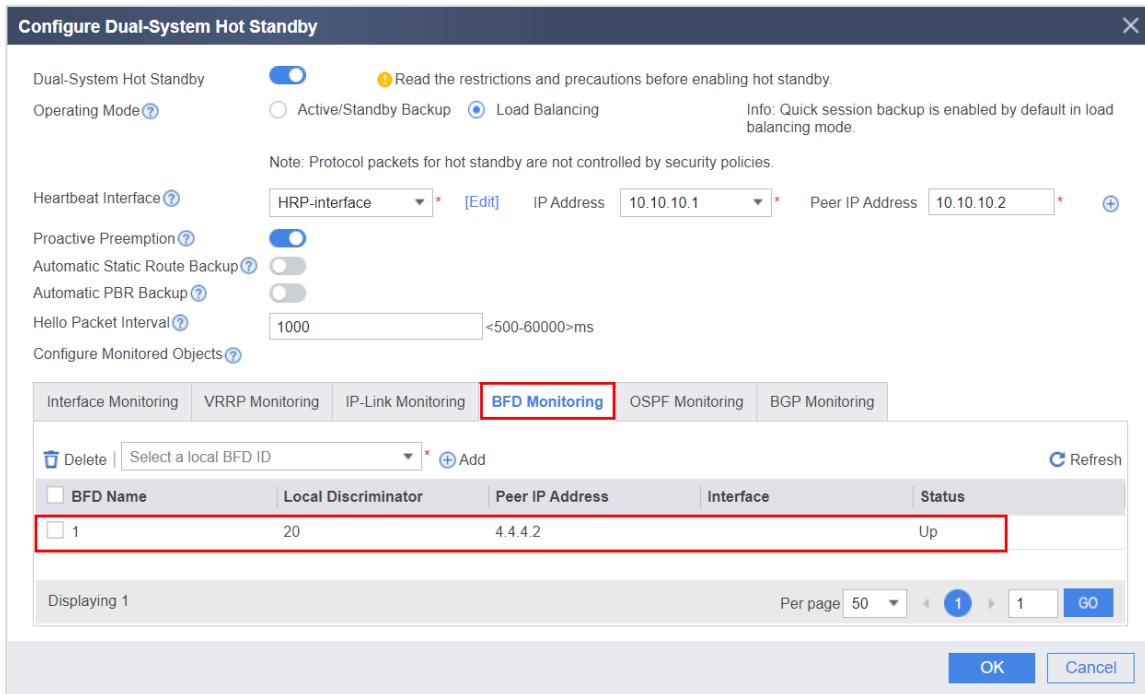


Enable BFD globally on RT1 and configure BFD session 1 with peer IP address 10.3.1.2, local source IP address 4.4.4.2, local discriminator 10, and remote discriminator 20.

```
[RT1] bfd
[RT1] bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2
[RT1-bfd-session-1] discriminator local 10
[RT1-bfd-session-1] discriminator remote 20
[RT1-bfd-session-1] commit
[RT1-bfd-session-1] quit
```

On FW1, choose **System > High Availability > Dual-System Hot Standby**, click **Edit**, and set the parameters as follows:

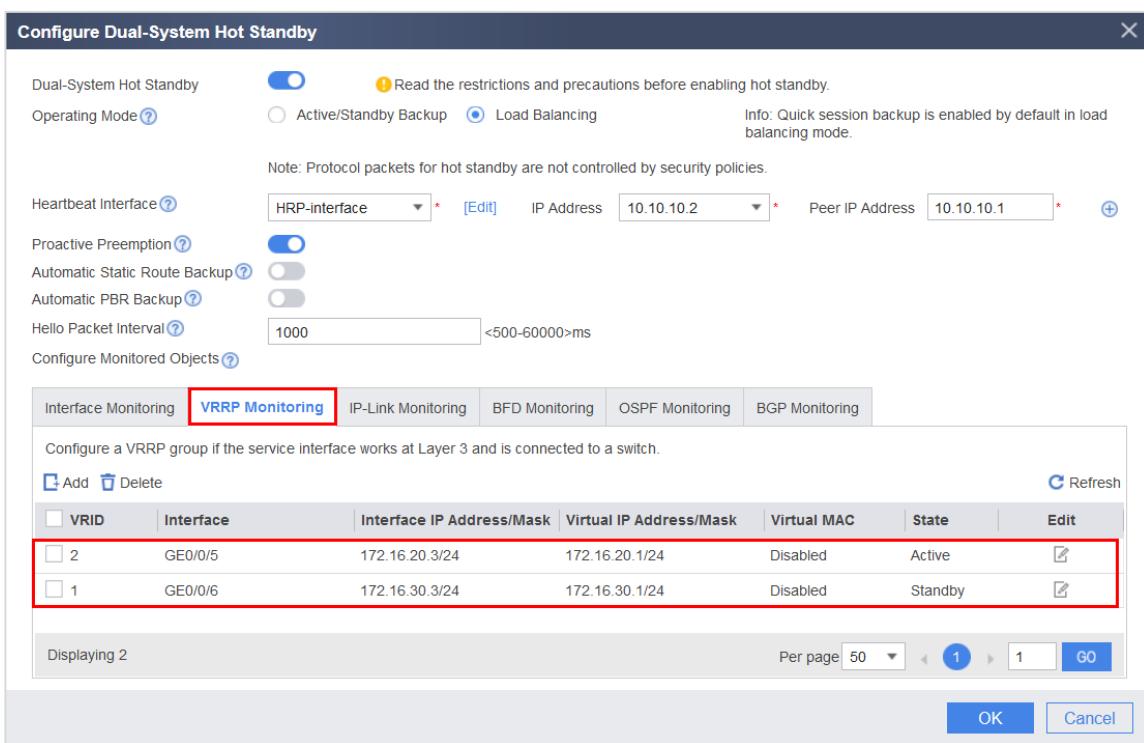
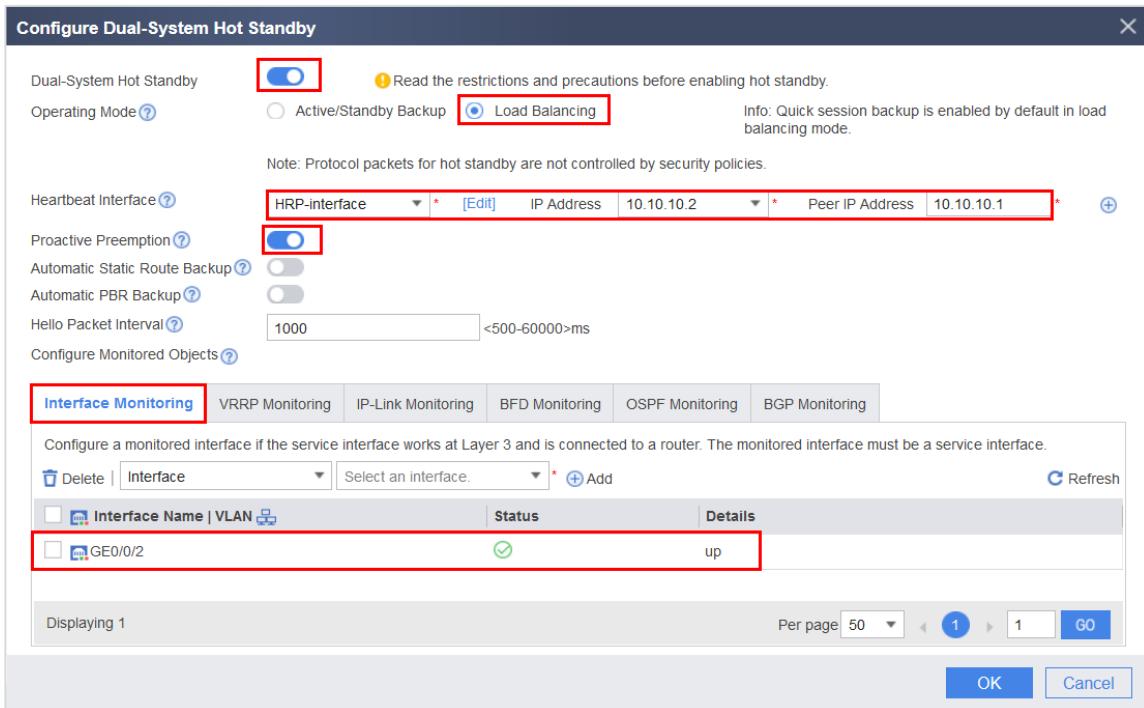


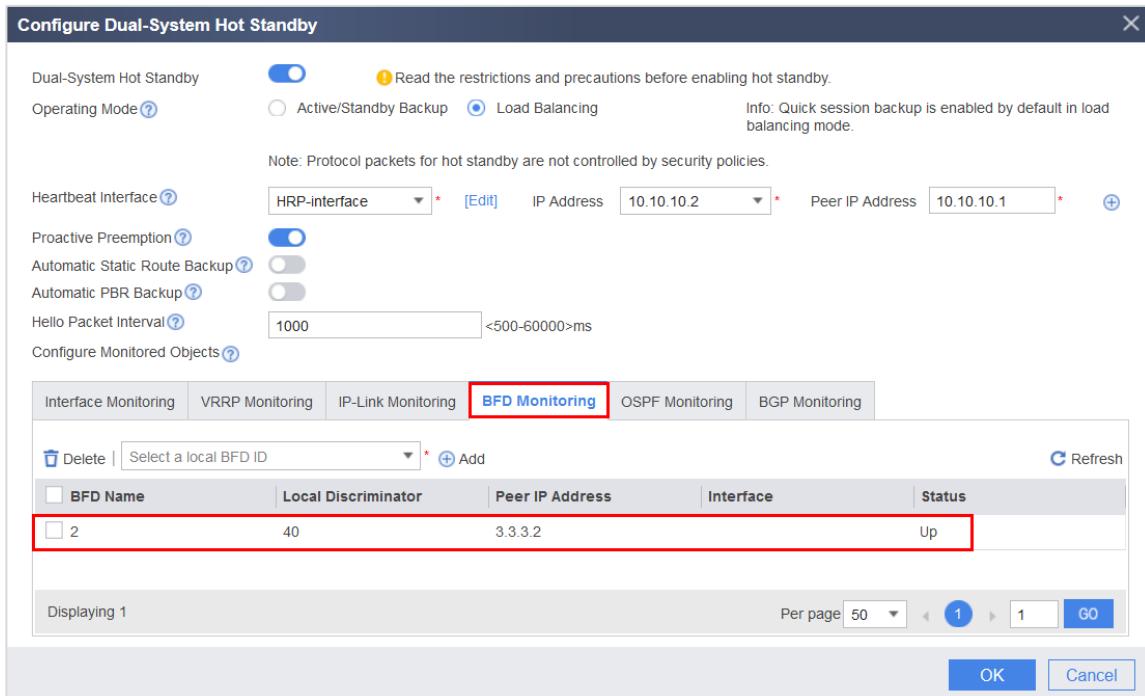


Enable BFD globally on RT2 and configure BFD session 2 with peer IP address 10.6.1.2, local source IP address 3.3.3.2, local discriminator 30, and remote discriminator 40.

```
[RT2] bfd
[RT2] bfd 2 bind peer-ip 10.6.1.2 source-ip 3.3.3.2
[RT2-bfd-session-2] discriminator local 30
[RT2-bfd-session-2] discriminator remote 40
[RT2-bfd-session-2] commit
[RT2-bfd-session-2] quit
```

On FW2, choose **System > High Availability > Dual-System Hot Standby**, click **Edit**, and set the parameters as follows:

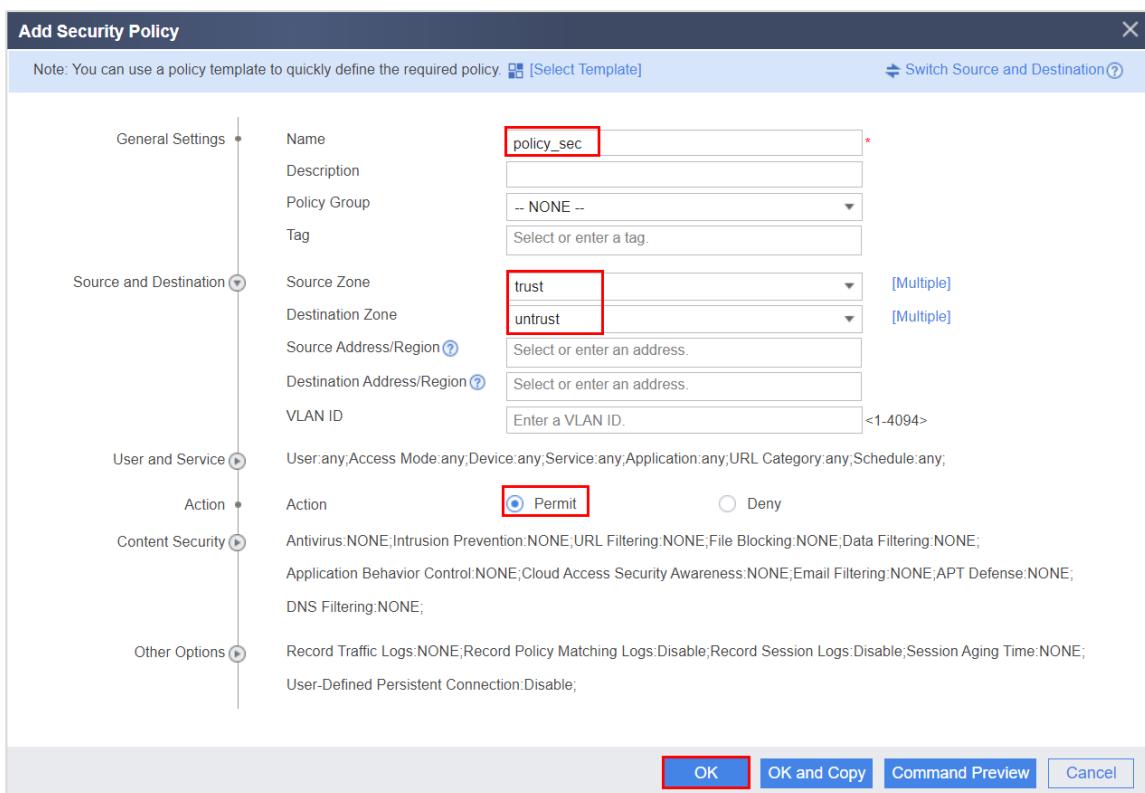




Step 4 Configure a security policy on the firewall.

Because FW1 and FW2 work in hot standby mode, the security policy configuration on FW1 is automatically synchronized to FW2. Therefore, you only need to configure a security policy on FW1.

Configure a security policy to allow intranet users to access the Internet.



1.3 Verification

After the preceding configurations are complete, check the final implementation effect.

1. The FTP server can ping the Internet address 3.3.3.1 (IP address of VLANIF 40 on SW1).
2. PC1 can ping the Internet address 4.4.4.1 (IP address of VLANIF 2 on SW1).
3. Manually disable the uplink interface G0/0/2 on FW1. The FTP server and PC1 can still ping an Internet address.
4. Manually enable the uplink interface G0/0/2 on FW1 and disable the uplink interface G0/0/2 on FW2. The FTP server and PC1 can still ping an Internet address.

Ping 3.3.3.1 on SW1 from the FTP server. The connectivity is normal.

```
C:\Users\Administrator>
C:\Users\Administrator>ping 3.3.3.1

Pinging 3.3.3.1 with 32 bytes of data:
Reply from 3.3.3.1: bytes=32 time=2ms TTL=252
Reply from 3.3.3.1: bytes=32 time=1ms TTL=252
Reply from 3.3.3.1: bytes=32 time=1ms TTL=252
Reply from 3.3.3.1: bytes=32 time=1ms TTL=252

Ping statistics for 3.3.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Tracert 3.3.3.1 on SW1 from the FTP server.

The traffic path is FTP server -> SW2 -> FW1 -> RT1 -> SW1.

```
C:\Users\Administrator>tracert 3.3.3.1

Tracing route to 3.3.3.1 over a maximum of 30 hops
  1      *          *          *      Request timed out.
  2      4 ms      <1 ms      <1 ms  10.3.1.1
  3      1 ms      <1 ms      <1 ms  3.3.3.1

Trace complete.
```

Ping 4.4.4.1 on SW1 from PC1. The connectivity is normal.

```
C:\Users\Security>ping 4.4.4.1

Pinging 4.4.4.1 with 32 bytes of data:
Reply from 4.4.4.1: bytes=32 time=1ms TTL=252

Ping statistics for 4.4.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Tracert 4.4.4.1 on SW1 from PC1. The traffic path is PC1 -> SW3 -> FW2 -> RT2 -> SW1.

```
C:\Users\Security>tracert 4.4.4.1

Tracing route to 4.4.4.1 over a maximum of 30 hops
  1      *          *          *      Request timed out.
  2      1 ms      1 ms      <1 ms  10.6.1.1
  3      1 ms      <1 ms      <1 ms  4.4.4.1

Trace complete.
```

Manually disable G0/0/2 on FW1. Ping 3.3.3.1 on SW1 from the FTP server. The connectivity is normal. Ping and tracert 3.3.3.1 on SW1 from the FTP server. The traffic path is as follows:

FTP Server -> SW3 -> FW2 -> RT2 -> SW1.

```
C:\Users\Administrator>ping 3.3.3.1
Pinging 3.3.3.1 with 32 bytes of data:
Reply from 3.3.3.1: bytes=32 time=34ms TTL=252
Reply from 3.3.3.1: bytes=32 time=1ms TTL=252
Reply from 3.3.3.1: bytes=32 time=1ms TTL=252
Reply from 3.3.3.1: bytes=32 time=1ms TTL=252

Ping statistics for 3.3.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 34ms, Average = 9ms

C:\Users\Administrator>tracert 3.3.3.1
Tracing route to 3.3.3.1 over a maximum of 30 hops
  1      *          *          *      Request timed out.
  2      1 ms     <1 ms      1 ms  10.6.1.1
  3      1 ms     <1 ms      <1 ms  3.3.3.1
```

Manually enable G0/0/2 on FW1 and disable G0/0/2 on FW2. Ping 4.4.4.1 on SW1 from PC1. The connectivity is normal. Tracert 4.4.4.1 on SW1 from PC1. The traffic path is PC1 -> SW2 -> FW1 -> RT1 -> SW1.

```
C:\Users\Security>ping 4.4.4.1
Pinging 4.4.4.1 with 32 bytes of data:
Reply from 4.4.4.1: bytes=32 time<1ms TTL=252

Ping statistics for 4.4.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Security>.
C:\Users\Security>tracert 4.4.4.1
Tracing route to 4.4.4.1 over a maximum of 30 hops
  1      <1 ms      <1 ms      <1 ms  172.16.20.2
  2      1 ms       1 ms       1 ms  10.3.1.1
  3      <1 ms      <1 ms      <1 ms  4.4.4.1

Trace complete.
```

1.4 Configuration Reference

1.4.1 RT1's Configuration

```
#  
sysname RT1  
#  
acl number 3500  
rule 5 permit ip
```

```
#  
bfd  
#  
interface GigabitEthernet0/0/1  
undo portswitch  
#  
interface GigabitEthernet0/0/1.2  
dot1q termination vid 2  
ip address 4.4.4.2 255.255.255.252  
nat outbound 3500  
#  
interface GigabitEthernet0/0/2  
undo portswitch  
ip address 10.1.1.1 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/4  
undo portswitch  
ip address 10.3.1.1 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface LoopBack0  
ip address 33.33.33.1 255.255.255.255  
#  
bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2  
discriminator local 10  
discriminator remote 20  
commit  
#  
ospf 1 router-id 33.33.33.1  
default-route-advertise always  
import-route static  
area 0.0.0.0  
#  
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1  
#  
return
```

1.4.2 RT2's Configuration

```
#  
sysname RT2  
#  
acl number 3500  
rule 5 permit ip  
#  
bfd  
#  
interface GigabitEthernet0/0/1  
undo portswitch  
#  
interface GigabitEthernet0/0/1.40  
dot1q termination vid 40  
ip address 3.3.3.2 255.255.255.252
```

```
nat outbound 3500
#
interface GigabitEthernet0/0/2
undo portswitch
ip address 10.1.1.2 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.6.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
ip address 44.44.44.1 255.255.255.255
#
bfd 2 bind peer-ip 10.6.1.2 source-ip 3.3.3.2
discriminator local 30
discriminator remote 40
commit
#
ospf 1 router-id 44.44.44.1
default-route-advertise always
import-route static
area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

1.4.3 FW1's Configuration

```
#
sysname FW1
#
undo firewall packet-filter basic-protocol enable
#
hrp enable
hrp interface Eth-Trunk0 remote 10.10.10.2
hrp mirror session enable
hrp standby config enable
hrp load balance device
hrp track interface GigabitEthernet0/0/2
hrp track bfd-session 20
#
bfd
#
interface Eth-Trunk0
ip address 10.10.10.1 255.255.255.0
alias HRP-heart-interface
#
interface GigabitEthernet0/0/2
undo shutdown
ip address 10.3.1.2 255.255.255.252
ospf enable 1 area 0.0.0.0
```

```
#  
interface GigabitEthernet0/0/3  
undo shutdown  
eth-trunk 0  
#  
interface GigabitEthernet0/0/4  
undo shutdown  
eth-trunk 0  
#  
interface GigabitEthernet0/0/5  
undo shutdown  
ip address 172.16.30.2 255.255.255.0  
vrrp vrid 2 virtual-ip 172.16.30.1 active  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/6  
undo shutdown  
ip address 172.16.20.2 255.255.255.0  
vrrp vrid 1 virtual-ip 172.16.20.1 standby  
ospf enable 1 area 0.0.0.0  
#  
interface LoopBack0  
ip address 11.11.11.1 255.255.255.255  
#  
firewall zone local  
set priority 100  
#  
firewall zone trust  
set priority 85  
add interface GigabitEthernet0/0/5  
add interface GigabitEthernet0/0/6  
#  
firewall zone untrust  
set priority 5  
add interface GigabitEthernet0/0/1  
add interface GigabitEthernet0/0/2  
#  
firewall zone dmz  
set priority 50  
add interface Eth-Trunk0  
#  
bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2  
discriminator local 20  
discriminator remote 10  
commit  
#  
ospf 1 router-id 11.11.11.1  
area 0.0.0.0  
#  
security-policy  
rule name policy_sec1  
source-zone trust  
destination-zone untrust  
action permit  
#
```

[return](#)

1.4.4 FW2's Configuration

```
#  
sysname FW2  
#  
undo firewall packet-filter basic-protocol enable  
#  
    hrp enable  
    hrp interface Eth-Trunk0 remote 10.10.10.1  
    hrp mirror session enable  
    hrp standby config enable  
    hrp load balance device  
    hrp track interface GigabitEthernet0/0/2  
    hrp track bfd-session 40  
#  
bfd  
#  
interface Eth-Trunk0  
ip address 10.10.10.2 255.255.255.0  
alias HRP-heart-interface  
#  
interface GigabitEthernet0/0/2  
undo shutdown  
ip address 10.6.1.2 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/3  
undo shutdown  
eth-trunk 0  
#  
interface GigabitEthernet0/0/4  
undo shutdown  
eth-trunk 0  
#  
interface GigabitEthernet0/0/5  
undo shutdown  
ip address 172.16.20.3 255.255.255.0  
vrrp vrid 2 virtual-ip 172.16.20.1 active  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/6  
undo shutdown  
ip address 172.16.30.3 255.255.255.0  
vrrp vrid 2 virtual-ip 172.16.30.1 standby  
ospf enable 1 area 0.0.0.0  
#  
interface LoopBack0  
ip address 22.22.22.1 255.255.255.255  
#  
firewall zone local  
set priority 100  
#
```

```
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/5
    add interface GigabitEthernet0/0/6
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
    add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
    add interface Eth-Trunk0
#
bfd 2 bind peer-ip 3.3.3.2 source-ip 10.6.1.2
    discriminator local 40
    discriminator remote 30
    commit
#
ospf 1 router-id 22.22.22.1
    area 0.0.0.0
#
security-policy
    rule name policy_sec1
        source-zone trust
        destination-zone untrust
        action permit
#
return
```

1.4.5 SW1's Pre-configuration

```
#
sysname SW1
#
vlan batch 2 40
#
interface vlanif2
    ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
    ip address 3.3.3.1 255.255.255.252
#
interface GigabitEthernet0/0/3
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.2
#
return
```

1.4.6 SW2's Pre-configuration

```
#  
sysname SW2  
#  
vlan batch 30  
#  
interface GigabitEthernet0/0/1  
    port link-type access  
    port default vlan 30  
#  
interface GigabitEthernet0/0/2  
    port link-type access  
    port default vlan 30  
#  
interface GigabitEthernet0/0/14  
    port link-type access  
    port default vlan 30  
#  
return
```

1.4.7 SW3's Pre-configuration

```
#  
sysname SW3  
#  
vlan batch 40  
#  
interface GigabitEthernet0/0/1  
    port link-type access  
    port default vlan 40  
#  
interface GigabitEthernet0/0/2  
    port link-type access  
    port default vlan 40  
#  
interface GigabitEthernet0/0/13  
    port link-type access  
    port default vlan 40  
#  
return
```

1.4.8 Mirror-SW's Pre-configuration

```
#  
sysname Mirror-SW  
#  
vlan batch 2 40  
#  
interface GigabitEthernet0/0/1  
    port link-type trunk  
    port trunk allow-pass vlan 2 40
```

```
#  
interface GigabitEthernet0/0/2  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
return
```

1.5 Quiz

What are the prerequisites before configuring hot standby?

Answer: The two firewalls that form a hot standby group must have the same model, and the same number and types of boards installed in the same layout.

2

Firewall Hot Standby Troubleshooting

2.1 Introduction

2.1.1 About This Lab

Two firewalls are deployed at the egress of an enterprise network. To improve network reliability, the two firewalls need to work in hot standby mode. During deployment, faults may occur when hot standby is configured.

In this lab, a pre-configured script is used to set hot standby failure points for trainees to practice troubleshooting.

2.1.2 Objectives

- Understand the networking principles of hot standby in load sharing mode.
- Master the key configurations of hot standby.
- Learn how to troubleshoot networking faults of hot standby in load sharing mode.

2.1.3 Networking Topology

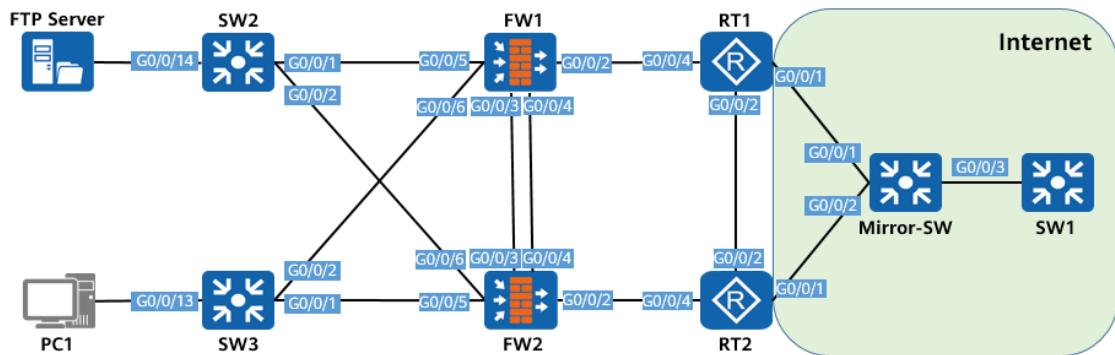


Figure 2-1 Hot standby troubleshooting

The preceding figure shows device connections. For details about IP address planning, see Table 2-1.

FW1 and FW2 work in hot standby mode. The gateways of the FTP server and PC1 are the VRRP1 and VRRP2 virtual gateways on the firewall, respectively. OSPF runs between IP addresses of the interfaces connecting to firewalls on RT1 and RT2, VRRP1 virtual gateway, and VRRP2 virtual gateway. RT1 and RT2 simulate the egresses of the enterprise network, and SW1 simulates the Internet. The lab purpose is that PC1 and the FTP server on the intranet can access the Internet.

2.1.4 Lab Planning

Table 2-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
RT1	G0/0/1.2	Layer 3 sub-interface	4.4.4.2/30 Termination VLAN 2	Network outbound interface, connected to Mirror-SW
	G0/0/2	Layer 3 interface	10.1.1.1/30	Interface for connecting to RT2
	G0/0/4	Layer 3 interface	10.3.1.1/30	Interface for connecting to FW1
	LoopBack0	Layer 3 interface	33.33.33.1/32	OSPF Router-ID
RT2	G0/0/1.40	Layer 3 sub-interface	3.3.3.2/30 Termination VLAN 40	Network outbound interface, connected to Mirror-SW
	G0/0/2	Layer 3 interface	10.1.1.2/30	Interface for connecting to RT1
	G0/0/4	Layer 3 interface	10.6.1.1/30	Interface for connecting to FW1
	LoopBack0	Layer 3 interface	44.44.44.1/32	OSPF Router-ID
FW1	G0/0/2	Layer 3 interface	10.3.1.2/30 Security zone: Untrust	Interface for connecting to RT1 in the upstream direction
	G0/0/3	Eth-trunk 0 Aggregation interface	10.10.10.1/24 Security zone: DMZ	Hot standby heartbeat interfaces
	G0/0/4			
	G0/0/5	Layer 3 interface	172.16.30.2/24 Security zone: Trust	Interface for connecting to switches in the downstream direction, and VRRP virtual
	G0/0/6	Layer 3 interface	172.16.20.2/24 Security zone: Trust	

				gateways need to be configured
	LoopBack0	Layer 3 interface	11.11.11.1/32	OSPF Router-ID
FW2	G0/0/2	Layer 3 interface	10.6.1.2/30 Security zone: Untrust	Interface for connecting to RT2 in the upstream direction
	G0/0/3	Eth-trunk 0 Aggregation interface	10.10.10.2/24 Security zone: DMZ	Hot standby heartbeat interfaces
	G0/0/4			
	G0/0/5	Layer 3 interface	172.16.20.3/24 Security zone: Trust	Interface for connecting to switches in the downstream direction, and VRRP virtual gateways need to be configured
	G0/0/6	Layer 3 interface	172.16.30.3/24 Security zone: Trust	OSPF Router-ID
	LoopBack0	Layer 3 interface	22.22.22.1/32	
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interconnection interface
	VLANIF2	Layer 3 interface	4.4.4.1/30	Interface for directly connecting to the egress address of RT1
	VLANIF40	Layer 3 interface	3.3.3.1/30	Interface for directly connecting to the egress address of RT2
SW2	G0/0/1	Access	PVID: 30	Interfaces that allow only traffic of the service VLANs to pass through
	G0/0/2			
	G0/0/14			
SW3	G0/0/1	Access	PVID: 40	Interfaces that allow only traffic of the service VLANs to pass
	G0/0/2			
	G0/0/13			

				through
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interfaces that allow only traffic of the service VLANs to pass through
	G0/0/2			
	G0/0/3			
PC1	Ethernet0	Network adapter	172.16.20.10/24 Gateway: 172.16.20.1/24	The gateway is the VRRP virtual gateway configured on the firewall.
FTP Server	Ethernet0	Network adapter	172.16.30.10/24 Gateway: 172.16.30.1/24	The gateway is the VRRP virtual gateway configured on the firewall.

2.2 Lab Configuration

2.2.1 Configuration Roadmap

1. Import the pre-configuration to the corresponding devices.
2. Check whether services are normal according to the lab planning and rectify faults one by one.

2.2.2 Configuration Procedure

Step 1 Pre-configure devices.

Construct the network according to the lab topology, disable the interfaces that are not used in the lab, and import the pre-configured scripts to the corresponding devices.

RT1's configuration

```

#
sysname RT1
#
acl number 3500
rule 5 permit ip
#
bfd
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.2
dot1q termination vid 2

```

```
ip address 4.4.4.2 255.255.255.252
nat outbound 3500
#
interface GigabitEthernet0/0/2
undo portswitch
ip address 10.1.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.3.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
ip address 33.33.33.1 255.255.255.255
#
bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2
discriminator local 10
discriminator remote 20
commit
#
ospf 1 router-id 33.33.33.1
default-route-advertise always
import-route static
area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

RT2's configuration

```
#
sysname RT2
#
acl number 3500
rule 5 permit ip
#
bfd
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.40
dot1q termination vid 40
ip address 3.3.3.2 255.255.255.252
nat outbound 3500
#
interface GigabitEthernet0/0/2
undo portswitch
ip address 10.1.1.2 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
undo portswitch
```

```
ip address 10.6.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
    ip address 44.44.44.1 255.255.255.255
#
bfd 2 bind peer-ip 10.6.1.2 source-ip 3.3.3.2
discriminator local 30
discriminator remote 40
commit
#
ospf 1 router-id 44.44.44.1
default-route-advertise always
import-route static
area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

FW1's configuration

```
#
sysname FW1
#
undo firewall packet-filter basic-protocol enable
#
interface Eth-Trunk0
    ip address 10.10.10.1 255.255.255.0
    alias HRP-heart-interface
#
hrp enable
    hrp interface Eth-Trunk0 remote 1.1.1.1
    hrp mirror session enable
    hrp standby config enable
    hrp load balance device
    hrp track interface GigabitEthernet0/0/2
    hrp track bfd-session 20
#
bfd
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 10.3.1.2 255.255.255.252
    ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/3
    undo shutdown
    eth-trunk 0
#
interface GigabitEthernet0/0/4
    undo shutdown
    eth-trunk 0
#
interface GigabitEthernet0/0/5
```

```
undo shutdown
ip address 172.16.30.2 255.255.255.0
vrrp vrid 2 virtual-ip 172.16.30.1 active
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/6
undo shutdown
ip address 172.16.20.2 255.255.255.0
vrrp vrid 1 virtual-ip 172.16.20.1 active
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
ip address 11.11.11.1 255.255.255.255
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
add interface GigabitEthernet0/0/6
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/1
add interface GigabitEthernet0/0/2
#
firewall zone dmz
set priority 50
add interface Eth-Trunk0
#
bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2
discriminator local 20
discriminator remote 10
commit
#
ospf 1 router-id 11.11.11.1
area 0.0.0.0
#
security-policy
rule name policy_sec1
source-zone trust
destination-zone untrust
action permit
#
return
```

FW2's configuration

```
#
sysname FW2
#
undo firewall packet-filter basic-protocol enable
#
interface Eth-Trunk0
```

```
ip address 10.10.10.2 255.255.255.0
alias HRP-heart-interface
#
hrp enable
    hrp interface Eth-Trunk0 remote 10.10.10.1
    hrp mirror session enable
    hrp standby config enable
    hrp load balance device
    hrp track interface GigabitEthernet0/0/2
    hrp track bfd-session 40
#
bfd
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 10.6.1.2 255.255.255.252
    ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/3
    undo shutdown
    eth-trunk 0
#
interface GigabitEthernet0/0/4
    undo shutdown
    eth-trunk 0
#
interface GigabitEthernet0/0/5
    undo shutdown
    ip address 172.16.20.3 255.255.255.0
    vrrp vrid 2 virtual-ip 172.16.20.1 active
    ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/6
    undo shutdown
    ip address 172.16.30.3 255.255.255.0
    vrrp vrid 2 virtual-ip 172.16.30.1 standby
    ospf enable 1 area 0.0.0.0
#
interface LoopBack0
    ip address 22.22.22.1 255.255.255.255
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/5
    add interface GigabitEthernet0/0/6
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
    add interface GigabitEthernet0/0/2
#
firewall zone dmz
```

```
set priority 50
#
bfd 2 bind peer-ip 3.3.3.2 source-ip 10.6.1.2
discriminator local 40
discriminator remote 30
commit
#
ospf 1 router-id 22.22.22.2
area 0.0.0.0
#
security-policy
rule name policy_sec1
source-zone trust
destination-zone untrust
action permit
#
return
```

SW1's configuration

```
#
sysname SW1
#
vlan batch 2 40
#
interface vlanif2
ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
ip address 3.3.3.1 255.255.255.252
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 2 40
#
return
```

SW2's configuration

```
#
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 30
#
interface GigabitEthernet0/0/2
port link-type access
port default vlan 30
#
interface GigabitEthernet0/0/14
port link-type access
port default vlan 30
```

```
#  
return
```

SW3's configuration

```
#  
sysname SW3  
#  
vlan batch 40  
#  
interface GigabitEthernet0/0/1  
    port link-type access  
    port default vlan 40  
#  
interface GigabitEthernet0/0/2  
    port link-type access  
    port default vlan 40  
#  
interface GigabitEthernet0/0/13  
    port link-type access  
    port default vlan 40  
#  
return
```

Mirror-SW's configuration

```
#  
sysname Mirror-SW  
#  
vlan batch 2 40  
#  
interface GigabitEthernet0/0/1  
    port link-type trunk  
    port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/2  
    port link-type trunk  
    port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/3  
    port link-type trunk  
    port trunk allow-pass vlan 2 40  
#  
return
```

Step 2 Check the hot standby status.

In this lab, the firewalls work in hot standby load sharing mode. The firewalls are connected to switches in the downstream direction and routers in the upstream direction. The heartbeat interface is the Eth-Trunk interface aggregated by GigabitEthernet0/0/3 and GigabitEthernet0/0/4. The correct configuration roadmap is as follows:

1. Monitor the status of uplink and downlink interfaces on firewalls.
2. Configure VRRP groups that connect to the downstream switches.

3. Configure dynamic routes pointing to the upstream routers.
4. Ensure that the heartbeat interfaces are reachable.
5. Specify the heartbeat interface and enable the hot standby function.

Locate the fault one by one according to the preceding configuration roadmap.

After the pre-configuration is imported, check the hot standby status of FW1 and FW2.

```
HRP_M[FW1] display hrp state
Role: active, peer: unknown
Running priority: 44998, peer: unknown
Backup channel usage: 0.00%
Stable time: 0 days, 0 hours, 2 minutes
Last state change information: HRP link changes to down due to heartbeat lost.
```

```
HRP_M[FW2] display hrp state
Role: active, peer: unknown
Running priority: 45000, peer: unknown
Backup channel usage: 0.00%
Stable time: 0 days, 0 hours, 2 minutes
Last state change information: HRP link changes to down due to heartbeat lost.
```

Both FW1 and FW2 consider themselves as the active device in hot standby and are unaware of the status of the peer device. Therefore, you need to locate the fault according to the preceding configuration roadmap.

Check the configuration of FW1 and FW2 to monitor the uplink and downlink interfaces.

```
HRP_M[FW1] hrp track interface GigabitEthernet0/0/2
```

```
HRP_M[FW2] hrp track interface GigabitEthernet0/0/2
```

Check the status of the interfaces monitored by FW1 and FW2. The command output shows that the status is Up, which is normal.

```
HRP_M[FW1] display interface GigabitEthernet 0/0/2
GigabitEthernet0/0/2 current state : UP
Line protocol current state : UP
HRP_M[FW2] display interface GigabitEthernet 0/0/2
GigabitEthernet0/0/2 current state : UP
Line protocol current state : UP
```

Check the status of VRRP groups on FW1. Normally, GigabitEthernet 0/0/5 on FW1 is the active interface of VRRP group 2, and GigabitEthernet 0/0/6 is the standby interface of VRRP group 1.

```
HRP_M[FW1] display vrrp brief
Total:2    Master:2    Backup:0    Non-active:0
VRID   State      Interface          Type      Virtual IP
```

1	Master	GE0/0/6	Vgmp	172.16.20.1
2	Master	GE0/0/5	Vgmp	172.16.30.1

Check the status of VRRP groups on FW2. Normally, GigabitEthernet 0/0/5 on FW2 is the active interface of VRRP group 1, and GigabitEthernet 0/0/6 is the standby interface of VRRP group 2.

HRP_M[FW2] display vrrp brief				
Total:2	Master:2	Backup:0	Non-active:0	
VRID	State	Interface	Type	Virtual IP
2	Master	GE0/0/6	Vgmp	172.16.30.1
2	Master	GE0/0/5	Vgmp	172.16.20.1

The status of the VRRP groups on FW1 and FW2 is Master, and the VRID of the VRRP groups on GigabitEthernet 0/0/5 and GigabitEthernet 0/0/6 of FW2 is 2, which does not meet the expectation.

VRRP group 1 consists of GigabitEthernet 0/0/5 on FW2 and GigabitEthernet 0/0/6 on FW1. In normal cases, GigabitEthernet 0/0/5 on FW2 is the active interface, and GigabitEthernet 0/0/6 on FW1 is the standby interface.

VRRP group 2 consists of GigabitEthernet 0/0/5 on FW1 and GigabitEthernet 0/0/6 on FW2. In normal cases, GigabitEthernet 0/0/5 on FW1 is the active interface, and GigabitEthernet 0/0/6 on FW2 is the standby interface.

Check the interface configuration of VRRP group 2.

```
HRP_M[FW1] interface GigabitEthernet 0/0/5
HRP_M[FW1-GigabitEthernet0/0/5] display this
#
interface GigabitEthernet0/0/5
undo shutdown
ip address 172.16.30.2 255.255.255.0
vrrp vrid 2 virtual-ip 172.16.30.1 active
ospf enable 1 area 0.0.0.0
#
```

```
HRP_M[FW2] interface GigabitEthernet 0/0/6
HRP_M[FW2-GigabitEthernet0/0/6] display this
#
interface GigabitEthernet0/0/6
undo shutdown
ip address 172.16.30.3 255.255.255.0
vrrp vrid 2 virtual-ip 172.16.30.1 standby
ospf enable 1 area 0.0.0.0
#
```

VRRP group 2 is correctly configured.

Check the interface configuration of VRRP group 1.

```
HRP_M[FW2] interface GigabitEthernet 0/0/5
HRP_M[FW2-GigabitEthernet0/0/5] display this
#
interface GigabitEthernet0/0/5
undo shutdown
ip address 172.16.20.3 255.255.255.0
vrrp vrid 2 virtual-ip 172.16.20.1 active
ospf enable 1 area 0.0.0.0
#
Return
```

```
HRP_M[FW1] interface GigabitEthernet 0/0/6
HRP_M[FW1-GigabitEthernet0/0/6] display this
#
interface GigabitEthernet0/0/6
undo shutdown
ip address 172.16.20.2 255.255.255.0
vrrp vrid 1 virtual-ip 172.16.20.1 active
ospf enable 1 area 0.0.0.0
#
return
```

The command output shows that the VRID of the VRRP group on GigabitEthernet 0/0/5 of FW2 is 2 and needs to be changed to 1. In addition, GigabitEthernet 0/0/6 of FW1 should be the standby interface.

Modify the VRRP configuration of GigabitEthernet 0/0/5 on FW2.

```
HRP_M[FW2] interface GigabitEthernet 0/0/5
HRP_M[FW2-GigabitEthernet0/0/5] undo vrrp vrid 2
HRP_M[FW2-GigabitEthernet0/0/5] vrrp vrid 1 virtual-ip 172.16.20.1 active
HRP_M[FW2-GigabitEthernet0/0/5] quit
```

Modify the VRRP configuration of GigabitEthernet 0/0/6 on FW1.

```
HRP_M[FW1] interface GigabitEthernet 0/0/6
HRP_M[FW1-GigabitEthernet0/0/6] undo vrrp vrid 1
HRP_M[FW1-GigabitEthernet0/0/6] vrrp vrid 1 virtual-ip 172.16.20.1 standby
HRP_M[FW1-GigabitEthernet0/0/6] quit
```

After the preceding check, ensure that the VRRP group configuration is correct.

Check the status of the VRRP groups on FW1 and FW2.

HRP_M[FW1] display vrrp brief					
Total:2		Master:2		Backup:0	Non-active:0
VRID	State	Interface	Type	Virtual IP	
1	Master	GE0/0/6	Vgmp	172.16.20.1	
2	Master	GE0/0/5	Vgmp	172.16.30.1	

```
HRP_M[FW2] display vrrp brief
Total:2 Master:2 Backup:0 Non-active:0
VRID State Interface Type Virtual IP
-----
1 Master GE0/0/5 Vgmp 172.16.20.1
2 Master GE0/0/6 Vgmp 172.16.30.1
```

The command output shows that the VRRP status is normal. Proceed to the next step.

Check the configuration of the heartbeat interface on FW1.

```
#
interface Eth-Trunk0
ip address 10.10.10.1 255.255.255.0
alias HRP-heart-interface
#
```

```
hrp interface Eth-Trunk0 remote 1.1.1.1
```

Check the configuration of the heartbeat interface on FW2.

```
#
interface Eth-Trunk0
ip address 10.10.10.2 255.255.255.0
alias HRP-heart-interface
#
```

```
hrp interface Eth-Trunk0 remote 10.10.10.1
```

Compare the heartbeat interface configuration of FW1 and FW2. It is found that the peer IP address configured on FW1 is incorrect.

Modify the IP address of the peer heartbeat interface on FW1.

```
HRP_M[FW1] hrp interface Eth-Trunk0 remote 10.10.10.2
```

Ping the HRP heartbeat interface on FW2 from the HRP heartbeat interface on FW1.

```
HRP_M<FW1> ping 10.10.10.2
PING 10.10.10.2: 56  data bytes, press CTRL_C to break
Request time out
--- 10.10.10.2 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

The heartbeat interfaces of the firewalls in a hot standby group need to communicate with each other, which is the prerequisite of the hot standby networking. You are advised to add the heartbeat interfaces to the DMZ. By default, the DMZs can communicate with each other.

Check the security zone configuration on FW1.

```
#  
firewall zone trust  
    set priority 85  
    add interface GigabitEthernet0/0/5  
    add interface GigabitEthernet0/0/6  
#  
firewall zone untrust  
    set priority 5  
    add interface GigabitEthernet0/0/1  
    add interface GigabitEthernet0/0/2  
#  
firewall zone dmz  
    set priority 50  
    add interface Eth-Trunk0  
#
```

Check the security zone configuration on FW2.

```
#  
firewall zone local  
    set priority 100  
#  
firewall zone trust  
    set priority 85  
    add interface GigabitEthernet0/0/5  
    add interface GigabitEthernet0/0/6  
#  
firewall zone untrust  
    set priority 5  
    add interface GigabitEthernet0/0/1  
    add interface GigabitEthernet0/0/2  
#  
firewall zone dmz  
    set priority 50  
#
```

The command output shows that the HRP heartbeat interface on FW2 is not added to any security zone.

Add the heartbeat interface Eth-Trunk 0 on FW2 to the DMZ.

```
HRP_M[FW2] firewall zone dmz  
HRP_M[FW2-zone-dmz] add interface Eth-Trunk 0  
HRP_M[FW2-zone-dmz] quit
```

Check the hot standby configuration on FW1.

```
HRP_M<FW1> display hrp state
Role: active, peer: active
  Running priority: 45000, peer: 45000
  Backup channel usage: 0.00%
  Stable time: 0 days, 0 hours, 0 minutes
  Last state change information: XXXX-06-28 23:48:01 HRP core state changed, old_state = abnormal(standby), new_state = normal, local_priority = 45000, peer_priority = 45000.
```

Check the hot standby configuration on FW2.

```
HRP_S<FW2> display hrp state
Role: active, peer: active
  Running priority: 45000, peer: 45000
  Backup channel usage: 0.00%
  Stable time: 0 days, 0 hours, 0 minutes
  Last state change information: XXXX-06-28 23:48:41 HRP core state changed, old_state = abnormal(active), new_state = normal, local_priority = 45000, peer_priority = 45000.
```

FW1 and FW2 form a hot standby networking in load sharing mode.

Check the status of VRRP groups on FW1.

```
HRP_M<FW1> display vrrp brief
Total:2 Master:1 Backup:1 Non-active:0
VRID State Interface Type Virtual IP
-----
1   Backup  GE0/0/6   Vgmp   172.16.20.1
2   Master   GE0/0/5   Vgmp   172.16.30.1
```

Check the status of the VRRP groups on FW2.

```
HRP_S<FW2> display vrrp brief
Total:2 Master:1 Backup:1 Non-active:0
VRID State Interface Type Virtual IP
-----
1   Master   GE0/0/5   Vgmp   172.16.20.1
2   Backup   GE0/0/6   Vgmp   172.16.30.1
```

The command output shows that the VRRP group meets the following requirements:

VRRP group 1 consists of GigabitEthernet 0/0/5 on FW2 and GigabitEthernet 0/0/6 on FW1.
In normal cases, GigabitEthernet 0/0/5 on FW2 is the active interface, and GigabitEthernet 0/0/6 on FW1 is the standby interface.

VRRP group 2 consists of GigabitEthernet 0/0/5 on FW1 and GigabitEthernet 0/0/6 on FW2.
In normal cases, GigabitEthernet 0/0/5 on FW1 is the active interface, and GigabitEthernet 0/0/6 on FW2 is the standby interface.

In conclusion, the hot standby troubleshooting lab is complete.

2.3 Configuration Reference

2.3.1 RT1's Configuration

```
#  
sysname RT1  
#  
acl number 3500  
rule 5 permit ip  
#  
bfd  
#  
interface GigabitEthernet0/0/1  
undo portswitch  
#  
interface GigabitEthernet0/0/1.2  
dot1q termination vid 2  
ip address 4.4.4.2 255.255.255.252  
nat outbound 3500  
#  
interface GigabitEthernet0/0/2  
undo portswitch  
ip address 10.1.1.1 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/4  
undo portswitch  
ip address 10.3.1.1 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface LoopBack0  
ip address 33.33.33.1 255.255.255.255  
#  
bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2  
discriminator local 10  
discriminator remote 20  
commit  
#  
ospf 1 router-id 33.33.33.1  
default-route-advertise always  
import-route static  
area 0.0.0.0  
#  
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1  
#  
return
```

2.3.2 RT2's Configuration

```
#  
sysname RT2  
#  
acl number 3500
```

```
rule 5 permit ip
#
bfd
#
interface GigabitEthernet0/0/1
    undo portswitch
#
interface GigabitEthernet0/0/1.40
    dot1q termination vid 40
    ip address 3.3.3.2 255.255.255.252
    nat outbound 3500
#
interface GigabitEthernet0/0/2
    undo portswitch
    ip address 10.1.1.2 255.255.255.252
    ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
    undo portswitch
    ip address 10.6.1.1 255.255.255.252
    ospf enable 1 area 0.0.0.0
#
interface LoopBack0
    ip address 44.44.44.1 255.255.255.255
#
bfd 2 bind peer-ip 10.6.1.2 source-ip 3.3.3.2
    discriminator local 30
    discriminator remote 40
    commit
#
ospf 1 router-id 44.44.44.1
    default-route-advertise always
    import-route static
    area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

2.3.3 FW1's Configuration

```
#
sysname FW1
#
undo firewall packet-filter basic-protocol enable
#
hrp enable
hrp interface Eth-Trunk0 remote 10.10.10.2
hrp mirror session enable
hrp standby config enable
hrp load balance device
hrp track interface GigabitEthernet0/0/2
hrp track bfd-session 20
#
```

```
bfd
#
interface Eth-Trunk0
    ip address 10.10.10.1 255.255.255.0
    alias HRP-heart-interface
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 10.3.1.2 255.255.255.252
    ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/3
    undo shutdown
    eth-trunk 0
#
interface GigabitEthernet0/0/4
    undo shutdown
    eth-trunk 0
#
interface GigabitEthernet0/0/5
    undo shutdown
    ip address 172.16.30.2 255.255.255.0
    vrrp vrid 2 virtual-ip 172.16.30.1 active
    ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/6
    undo shutdown
    ip address 172.16.20.2 255.255.255.0
    vrrp vrid 1 virtual-ip 172.16.20.1 standby
    ospf enable 1 area 0.0.0.0
#
interface LoopBack0
    ip address 11.11.11.1 255.255.255.255
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/5
    add interface GigabitEthernet0/0/6
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
    add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
    add interface Eth-Trunk0
#
bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2
    discriminator local 20
    discriminator remote 10
    commit
```

```
#  
ospf 1 router-id 11.11.11.1  
area 0.0.0.0  
#  
security-policy  
rule name policy_sec1  
source-zone trust  
destination-zone untrust  
action permit  
#  
return
```

2.3.4 FW2's Configuration

```
#  
sysname FW2  
#  
undo firewall packet-filter basic-protocol enable  
#  
hrp enable  
hrp interface Eth-Trunk0 remote 10.10.10.1  
hrp mirror session enable  
hrp standby config enable  
hrp load balance device  
hrp track interface GigabitEthernet0/0/2  
hrp track bfd-session 40  
#  
bfd  
#  
interface Eth-Trunk0  
ip address 10.10.10.2 255.255.255.0  
alias HRP-heart-interface  
#  
interface GigabitEthernet0/0/2  
undo shutdown  
ip address 10.6.1.2 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/3  
undo shutdown  
eth-trunk 0  
#  
interface GigabitEthernet0/0/4  
undo shutdown  
eth-trunk 0  
#  
interface GigabitEthernet0/0/5  
undo shutdown  
ip address 172.16.20.3 255.255.255.0  
vrrp vrid 2 virtual-ip 172.16.20.1 active  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/6  
undo shutdown
```

```
ip address 172.16.30.3 255.255.255.0
vrrp vrid 2 virtual-ip 172.16.30.1 standby
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
    ip address 22.22.22.1 255.255.255.255
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/5
    add interface GigabitEthernet0/0/6
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
    add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
    add interface Eth-Trunk0
#
bfd 2 bind peer-ip 3.3.3.2 source-ip 10.6.1.2
    discriminator local 40
    discriminator remote 30
    commit
#
ospf 1 router-id 22.22.22.1
    area 0.0.0.0
#
security-policy
    rule name policy_sec1
        source-zone trust
        destination-zone untrust
        action permit
#
return
```

2.3.5 SW1's Configuration

```
#
sysname SW1
#
vlan batch 2 40
#
interface vlanif2
    ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
    ip address 3.3.3.1 255.255.255.252
#
interface GigabitEthernet0/0/3
```

```
port link-type trunk
port trunk allow-pass vlan 2 40
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.2
#
return
```

2.3.6 SW2's Configuration

```
#
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
    port link-type access
    port default vlan 30
#
interface GigabitEthernet0/0/2
    port link-type access
    port default vlan 30
#
interface GigabitEthernet0/0/14
    port link-type access
    port default vlan 30
#
return
```

2.3.7 SW3's Configuration

```
#
sysname SW3
#
vlan batch 40
#
interface GigabitEthernet0/0/1
    port link-type access
    port default vlan 40
#
interface GigabitEthernet0/0/2
    port link-type access
    port default vlan 40
#
interface GigabitEthernet0/0/13
    port link-type access
    port default vlan 40
#
return
```

2.3.8 Mirror-SW's Configuration

```
#
```

```
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/1
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
return
```

2.4 Quiz

During troubleshooting, why are all VRRP groups on FW1 and FW2 in the Master state when the hot standby relationship is not established between FW1 and FW2?

Answer: If hot standby is configured on both devices but hot standby negotiation fails, both devices consider themselves as the active device and set their VRRP groups to the Master state.

3 Firewall Traffic Management

3.1 Introduction

3.1.1 About This Lab

An enterprise deploys a firewall at the network border as the egress gateway so that intranet users can access the Internet. In the office environment, to improve the work efficiency of employees, the enterprise intend to allocate a fixed traffic quota and bandwidth rate to each employee and control the online duration of employees.

In this lab, the upload/download bandwidth from each intranet PC to the Internet is limited to 400 kbit/s and 600 kbit/s, a fixed traffic quota is allocated to each employee, and the online duration of each employee is controlled.

3.1.2 Objectives

- Learn how to configure a traffic policy to limit the upload/download bandwidth of intranet PCs.
- Implement local Portal authentication for enterprise employees.
- Allocate a fixed traffic quota to each employee.

3.1.3 Networking Topology

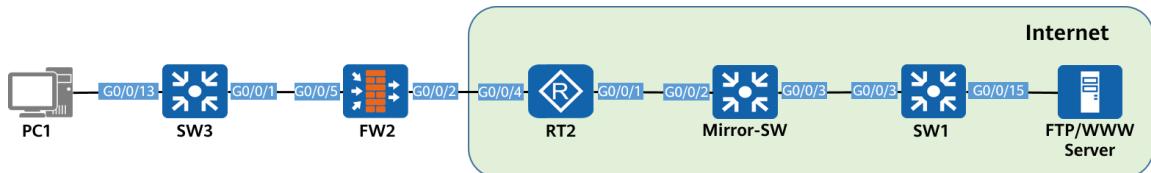


Figure 3-1 Traffic management

The preceding figure shows device connections. For details about IP address planning, see Table 3-1.

SW3 and Mirror-SW are responsible for Layer 2 communication. Routes need to be established between RT2 and SW1. The configurations of SW3, Mirror-SW, RT2, and SW1 are not described in the lab procedure. For details, see the pre-configurations in 3.4 Configuration Reference. The lab procedure focuses on the key configurations on FW2.

3.1.4 Lab Planning

Table 3-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
FW2	G0/0/2	Layer 3 interface	100.6.1.2/30 Security zone: Untrust	Uplink interface of the network which is connected to RT2.
	G0/0/5	Layer 3 interface	172.16.20.3/24 Security zone: Trust	Interface for connecting to SW3
RT2	G0/0/1.40	Layer 3 interface	3.3.3.2/30 Termination VLAN 40	Interface for connecting to Mirror-SW
	G0/0/4	Layer 3 interface	100.6.1.1/30	Interface for connecting to FW2
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 40	Interface for connecting to RT2
	G0/0/15	Access	PVID: 300	Interface for connecting to the FTP/WWW Server
	VLANIF 40	Layer 3 interface	3.3.3.1/30	On the same network segment as an RT2 interface
	VLANIF 300	Layer 3 interface	100.20.1.1/24	Interface for connecting to the FTP/WWW Server
Mirror-SW	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 40	Interconnection interface
	G0/0/3			
SW3	G0/0/1	Access	PVID: 40	Interface for connecting to an endpoint
	G0/0/13			Interface for connecting to FW2
PC1	Ethernet0	NIC	172.16.20.111/24 Gateway: 172.16.20.3/24	Intranet test endpoint
FTP/WWW	Ethernet0	NIC	100.20.1.2/24	Internet server

Server			Gateway: 100.20.1.1/24	
--------	--	--	---------------------------	--

3.2 Lab Configuration

3.2.1 Configuration Roadmap

1. Configure IP addresses for devices.
2. Configure security policies, static routes, and NAT policies to allow intranet users to access the Internet.
3. Configure traffic policy to limit the upload and download rates of intranet users.
4. Configure user identity authentication. Users must pass Portal authentication before accessing the Internet.
5. Configure user-based quota management to limit the total online traffic and online duration of the user, after a user passes identity authentication.

3.2.2 Configuration Procedure on the CLI

Step 1 Set basic network parameters.

Set basic network parameters according to Table 3-1 Lab Planning.

RT2, Mirror-SW, and SW1 have been preconfigured. For details, see 3.4 Configuration Reference.

Configure an IP address for each FW interface and add interfaces to security zones.

Configure an IP address for GigabitEthernet0/0/2, and add the interface to the Untrust zone.

```
<FW2> system-view
[FW2] interface GigabitEthernet0/0/2
[FW2-GigabitEthernet0/0/2] ip address 100.6.1.2 255.255.255.252
[FW2-GigabitEthernet0/0/2] quit
[FW2] firewall zone untrust
[FW2-zone-untrust] add interface GigabitEthernet0/0/2
[FW2-zone-untrust] quit
```

Configure an IP address for GigabitEthernet0/0/5, and add the interface to the Trust zone.

```
[FW2] interface GigabitEthernet0/0/5
[FW2-GigabitEthernet0/0/5] ip address 172.16.20.3 255.255.255.0
[FW2-GigabitEthernet0/0/5] quit
[FW2] firewall zone trust
[FW2-zone-trust] add interface GigabitEthernet0/0/5
[FW2-zone-trust] quit
```

Step 2 Configure security policies.

```
# Configure a security policy to allow packet exchange between a specified intranet segment and the Internet.
```

```
[FW2] security-policy  
[FW2-policy-security] rule name trust-untrust  
[FW2-policy-security-rule-trust-untrust] source-zone trust  
[FW2-policy-security-rule-trust-untrust] destination-zone untrust  
[FW2-policy-security-rule-trust-untrust] source-address 172.16.20.0 24  
[FW2-policy-security-rule-trust-untrust] action permit  
[FW2-policy-security-rule-trust-untrust] quit  
[FW2-policy-security] quit
```

Step 3 Configure a route.

```
# Configure a default route so that intranet traffic can be properly forwarded to a router on the Internet.
```

```
[FW2] ip route-static 0.0.0.0 0.0.0.0 100.6.1.1
```

Step 4 Configure a NAT policy.

```
# Configure a source NAT policy on an outbound interface so that intranet users can use the public IP address of an interface on FW2 to access the Internet.
```

```
[FW2] nat-policy  
[FW2-policy-nat] rule name easyip  
[FW2-policy-nat-rule-easyip] source-zone trust  
[FW2-policy-nat-rule-easyip] destination-zone untrust  
[FW2-policy-nat-rule-easyip] source-address 172.16.20.0 mask 255.255.255.0  
[FW2-policy-nat-rule-easyip] action source-nat easy-ip  
[FW2-policy-nat-rule-easyip] quit  
[FW2-policy-nat] quit
```

Step 5 Configure a traffic profile.

```
# Configure a traffic profile for users to access the Internet.
```

```
[FW2] traffic-policy  
[FW2-policy-traffic] profile ftp  
[FW2-policy-traffic-profile-ftp] bandwidth maximum-bandwidth whole downstream 20000  
[FW2-policy-traffic-profile-ftp] bandwidth maximum-bandwidth per-ip downstream 2000  
[FW2-policy-traffic-profile-ftp] quit
```

Step 6 Configure a traffic policy.

```
# Configure a traffic policy for users to access the Internet.
```

```
[FW2-policy-traffic] rule name ftp  
[FW2-policy-traffic-rule-ftp] source-zone trust  
[FW2-policy-traffic-rule-ftp] destination-zone untrust  
[FW2-policy-traffic-rule-ftp] source-address 172.16.20.0 mask 255.255.255.0  
[FW2-policy-traffic-rule-ftp] action qos profile ftp  
[FW2-policy-traffic-rule-ftp] quit
```

```
[FW2-policy-traffic] quit
```

Step 7 Configure Portal authentication.

To complete identity authentication on internal users who intend to access the Internet, security policies must be implemented to permit packets from the Trust zone to the Local zone.

Configure the Portal authentication.

```
[FW2] auth-policy
[FW2-policy-auth] default action auth
[FW2-policy-auth] rule name portal
[FW2-policy-auth-rule-portal] source-zone trust
[FW2-policy-auth-rule-portal] destination-zone untrust
[FW2-policy-auth-rule-portal] action auth
[FW2-policy-auth-rule-portal] quit
[FW2-policy-auth] quit
```

Set the user name to **staff** and password to **Huawei@123** on the firewall.

```
[FW2] user-manage user staff
[FW2-localuser-staff] password Huawei@123
[FW2-localuser-staff] quit
```

Configure a security policy to allow access from the Trust zone to the Local zone so that intranet users can be authenticated.

```
[FW2] security-policy
[FW2-policy-security] rule name trust-local
[FW2-policy-security-rule-trust-local] source-zone trust
[FW2-policy-security-rule-trust-local] destination-zone local
[FW2-policy-security-rule-trust-local] action permit
[FW2-policy-security-rule-trust-local] quit
[FW2-policy-security] quit
```

Configure a quota control policy for user staff on the firewall to limit the traffic volume to 2048 MB and the online duration to 4 hours during working hours each day. If the traffic volume or online duration is exceeded, user staff cannot access the Internet.

```
[FW2] quota-policy
[FW2-policy-quota] profile staff-limit
[FW2-policy-quota-profile-staff-limit] stream-daily 2048 reminder-threshold 80
[FW2-policy-quota-profile-staff-limit] time-daily 240 reminder-threshold 80
[FW2-policy-quota-profile-staff-limit] rule name staff-limit
[FW2-policy-quota-rule-staff-limit] user username staff
[FW2-policy-quota-rule-staff-limit] action quota profile staff-limit
[FW2-policy-quota-rule-staff-limit] quit
```

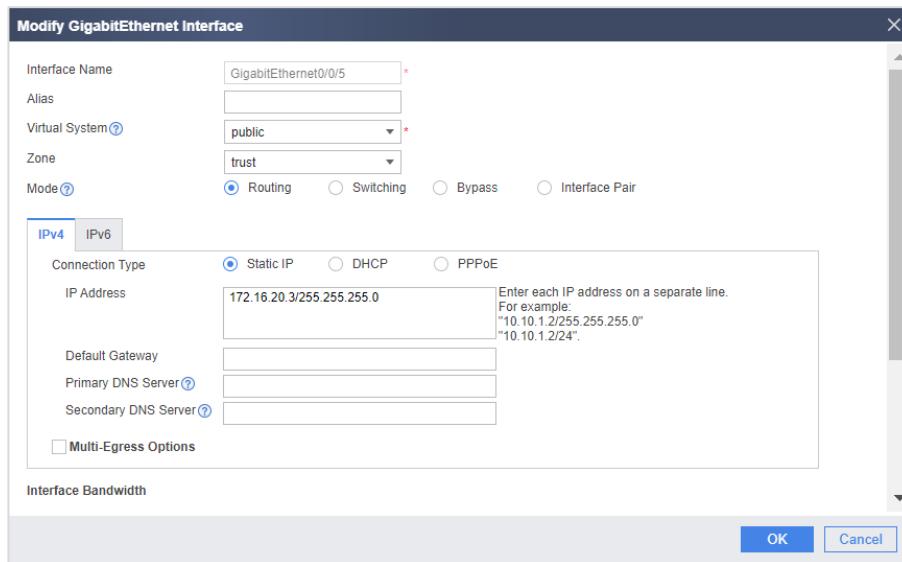
3.2.3 Configuration Procedure on the Web UI

Step 1 Set basic network parameters.

Set basic network parameters according to Table 3-1 Lab Planning.

RT2, Mirror-SW, and SW1 have been preconfigured. For details, see 3.4 Configuration Reference.

Configure an IP address for each FW interface and add interfaces to security zones. Choose **Network > Interface** and click  next to the interface to be configured. Select or set parameters and click **OK** Configure GigabitEthernet0/0/5, as shown in the following figure.



Configuring GigabitEthernet0/0/2 on FW2 is similar to that of GigabitEthernet0/0/5, and is not described here.

Step 2 Configuring a Security Policy

Configure security policies. # Choose **Policy > Security Policy** to create a security policy. Set parameters to allow packet exchange between a specified intranet segment and the Internet.

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [\[Select Template\]](#) [Switch Source and Destination](#)

General Settings	Name	trust-untrust *
	Description	
	Policy Group	-- NONE --
	Tag	Select or enter a tag.
Source and Destination	Source Zone	trust [Multiple]
	Destination Zone	untrust [Multiple]
	Source Address/Region	172.16.20.0/24
	Destination Address/Region	any
	VLAN ID	Enter a VLAN ID. <1-4094>
User and Service	User	Select or enter a user name. [Multiple]
	Access Mode	Select an access mode.
	Device	Select or enter a device.
	Service	Select or enter a service.
	Application	Select or enter an application. [Multiple]
	URL Category	Select or enter a url category. [Multiple]
	Schedule	Select a time range.
Action	Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security	Antivirus	-- NONE -- [Configure]

OK OK and Copy Command Preview Cancel

Step 3 Configure a default route.

Configure a default route. # Choose Network > Route > Static Route to create a static route, so that intranet traffic can be forwarded to the router on the Internet.

Add Static Route

Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Source Virtual Router	public
Destination Address/Mask	0.0.0.0/0.0.0.0 *
Destination Virtual Router	public
Interface	-- NONE --
Next Hop	10.6.1.1
Priority	60 <1-255>
Reliability Detection	<input checked="" type="radio"/> No Detection <input type="radio"/> BFD Binding <input type="radio"/> IP Link Binding
Description	

OK Cancel

Step 4 Configure a NAT policy.

Configure a source NAT policy on an outbound interface. # Choose Policy > NAT Policy > NAT Policy to create a NAT policy so that intranet users can directly use the public IP address of an interface on FW2 to access the Internet.

Add NAT Policy

[Show Overview]

Name	easyip *
Description	<input type="text"/>
Tag	Select or enter a tag.
NAT Type	<input checked="" type="radio"/> NAT <input type="radio"/> NAT64 <input type="radio"/> NAT66
NAT Mode	Source address translation
Schedule	Select a time range.
Original Data Packet	
Source Zone	trust [Multiple]
Destination Type	<input checked="" type="radio"/> Destination Zone <input type="radio"/> Outbound Interface
Source Address	untrust [Multiple]
Destination Address	<input type="text"/> 172.16.20.0/24
Service	Select or enter a service.
Translated Data Packet	
Source Address Translated To	<input type="radio"/> Address in the IP address pool <input checked="" type="radio"/> Outbound interface
Note: To ensure that the device can properly forward NAT service traffic, configure a security policy. [Add Security Policy]	

OK **Cancel**

Step 5 Configure bandwidth management.

Configure bandwidth management for Internet access users.

Choose **Policy > Bandwidth Management > Traffic Profile** to configure a traffic profile for users to access the Internet.

Add Traffic Profile

Name: ftp *

Global Traffic Limiting

Reference Mode	<input checked="" type="radio"/> Exclusive <input type="radio"/> Shared
Upstream Bandwidth	Maximum: <input type="text"/> kbps <60-200000000> Guaranteed: <input type="text"/> kbps <60-200000000>
Downstream Bandwidth	Maximum: <input type="text"/> Mbps <1-200000> Guaranteed: <input type="text"/> kbps <60-200000000>
Max. Connections	<input type="text"/> <1-8000000>
Max. Connection Rate	<input type="text"/> <1-500000>per second

Per-IP/User Traffic Limit

Traffic Limiting Object	<input checked="" type="radio"/> Per-IP <input type="radio"/> Per-User
Even Distribution	<input type="checkbox"/>
Upstream Bandwidth	Maximum: <input type="text"/> kbps <60-200000000> Guaranteed: <input type="text"/> kbps <60-200000000>
Downstream Bandwidth	Maximum: <input type="text"/> Mbps <1-200000> Guaranteed: <input type="text"/> khns <60-200000000>

OK **Cancel**

Choose **Policy > Bandwidth Management > Traffic Policy** to configure a corresponding traffic policy for Internet access users.

Add Traffic Policy

Name	ftp *
Description	
Tag	Select or enter a tag.
Parent Policy	
Source Type	<input type="radio"/> Inbound Interface <input checked="" type="radio"/> Source Zone
Destination Type	<input type="radio"/> Outbound Interface <input checked="" type="radio"/> Destination Zone
Source Address/Region	trust [Multiple]
Destination Address/Region	untrust [Multiple]
User	any [Multiple]
Service	any [Multiple]
Application	any [Multiple]
Specifying an application will automatically enable the SA function. This function reduces system performance.	
URL Category	any [Multiple]
Schedule	any [Multiple]
DSCP Value	any [Multiple]
Action	<input checked="" type="radio"/> Limit <input type="radio"/> None
Traffic Profile	ftp * [Configure]
Note: To ensure that the service traffic controlled by the traffic policy can be forwarded successfully, you need to configure security policies. [Add Security Policy]	
OK Cancel	

Step 6 Configure Portal authentication.

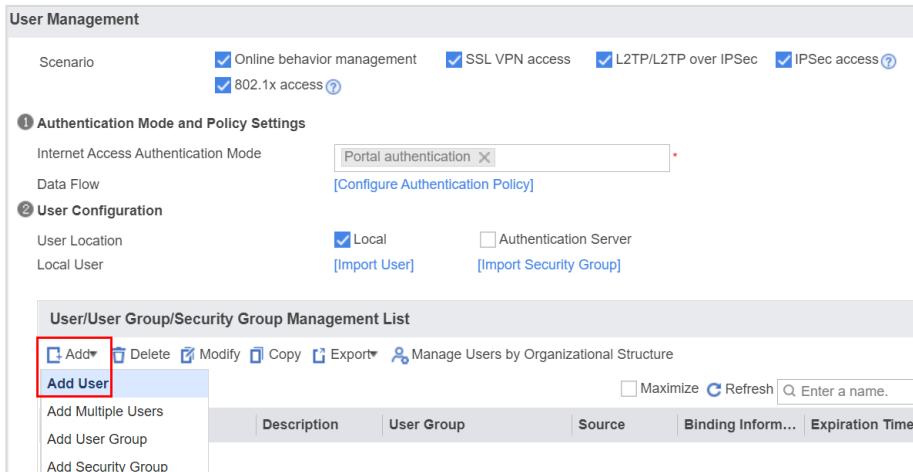
Configure local user authentication. Intranet users must pass identity authentication before accessing the Internet. The user name and password are set on the firewall and the security policy must be configured to permit packets from the Trust zone to the Local zone for user authentication.

Choose Object > User > default and set the **Internet Access Authentication Mode** to **Portal authentication**.

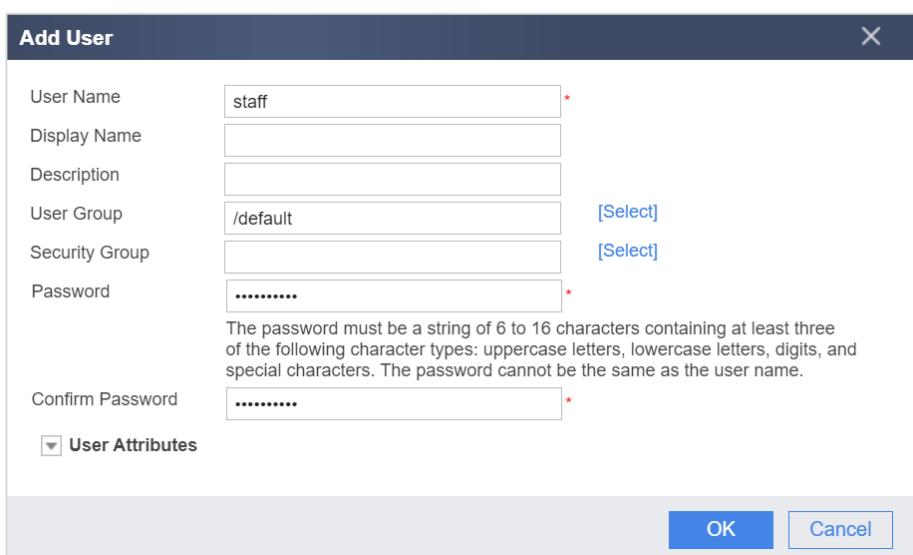
User Management

Scenario	<input checked="" type="checkbox"/> Online behavior management <input checked="" type="checkbox"/> SSL VPN access <input checked="" type="checkbox"/> L2TP/L2TP over IPSec <input checked="" type="checkbox"/> IPSec access <input type="checkbox"/> Administrator access
Authentication Mode and Policy Settings	
Internet Access Authentication Mode	Portal authentication [Configure Authentication Policy]
Data Flow	

Choose Object > User > default. Create a user named **staff** and set the password to **Huawei@123**.



The screenshot shows the 'User Management' interface. Under 'Scenario', several checkboxes are selected: 'Online behavior management', 'SSL VPN access', 'L2TP/L2TP over IPSec', and 'IPSec access'. Below this, under '① Authentication Mode and Policy Settings', 'Internet Access Authentication Mode' is set to 'Portal authentication'. Under '② User Configuration', 'User Location' is set to 'Local'. The 'Add User' button in the 'User/User Group/Security Group Management List' is highlighted with a red box.



The 'Add User' dialog box contains fields for 'User Name' (staff), 'Display Name', 'Description', 'User Group' (/default), 'Security Group', 'Password', and 'Confirm Password'. A note below the password fields specifies password requirements: "The password must be a string of 6 to 16 characters containing at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The password cannot be the same as the user name." There is also a checked checkbox for 'User Attributes'.

Choose Object > User > Authentication Policy. Create an authentication policy named **Portal**, which requires users to pass identity authentication before accessing the Untrust zone from the Trust zone.

Add Authentication Policy

Name	Portal *
Description	
Tag	Select or enter a tag.
Source Zone	trust [Multiple]
Destination Zone	untrust [Multiple]
Source Address/Region	Select or enter an address.
Destination Address/Region	Select or enter an address.
Service	Select or enter a service.
Action	<input checked="" type="radio"/> Portal authentication <input type="radio"/> Authentication exemption <input type="radio"/> No authentication
Portal Authentication Template	<input type="checkbox"/>

OK **Cancel**

Choose **Policy > Quota Control Policy > Quota Control Policy** and create a quota control policy named **staff-limit**. In this policy, user staff can use a maximum of 2048 MB traffic and 4 hours of online duration during working hours each day. After the quota is exceeded, user staff cannot access the Internet.

HUAWEI USG6525E

Dashboard **Monitor** **Policy** **Object** **Network** **System**

Add Quota Control Policy

Name	staff-limit *
Description	
Tag	Select or enter a tag.
User	staff [Multiple]
Schedule	worktime
Quota Settings	<input checked="" type="radio"/> Configured <input type="radio"/> Not Configured
Daily	<input checked="" type="checkbox"/> Traffic Quota: 2048 MB <input type="checkbox"/> Notification Threshold: 80 %
Monthly	<input type="checkbox"/> Traffic Quota: 1-300000 MB <input type="checkbox"/> Notification Threshold: 1-99 %

OK **Cancel**

Add Quota Control Policy

Schedule	worktime
Quota Settings	<input checked="" type="radio"/> Configured <input type="radio"/> Not Configured
Daily	
Traffic Quota	2048 * <1-10240>MB
Notification Threshold ?	80 <1-99>%
Duration of Internet Use	240 * <1-1439>minutes
Notification Threshold ?	80 <1-99>%
Reset Time	00:00
Monthly	
Traffic Quota	<1-300000>MB
Notification Threshold ?	<1-99>%
Reset Date	1
Action	
Excess Max. Bandwidth	0 * <0-102400>Kbps

OK **Cancel**

Choose **Policy > Security Policy** to create a security policy. Select or enter the parameters. Configure security policies to permit the access from the Trust zone to the Local zone and allows intranet users to be authenticated.

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [\[Select Template\]](#) [Switch Source and Destination](#)

General Settings	Name: trust-local
	Description:
	Policy Group: -- NONE --
	Tag: Select or enter a tag.
Source and Destination	Source Zone: trust Destination Zone: local [Multiple]
	Source Address/Region ? : Select or enter an address.
	Destination Address/Region ? : Select or enter an address.
	VLAN ID: Enter a VLAN ID. <1-4094>
User and Service	User:any;Access Mode:any;Device:any;Service:any;Application:any;URL Category:any;Schedule:any;
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security	Antivirus:NONE;Intrusion Prevention:NONE;URL Filtering:NONE;File Blocking:NONE;Data Filtering:NONE; Application Behavior Control:NONE;Cloud Access Security Awareness:NONE;Email Filtering:NONE;APT Defense:NONE; DNS Filtering:NONE;
Other Options	Record Traffic Loss:NONE:Record Policy Matching Loss:Disable:Record Session Loss:Disable:Session Aging Time:NONE:

OK **OK and Copy** **Command Preview** **Cancel**

3.3 Verification

After the preceding configurations are complete, check the final implementation effect.

1. When Portal authentication is not performed on PC1, PC1 cannot access the Internet and cannot ping the FTP/WWW Server.
2. Enter any IP address, for example, **http://1.1.1.1**, in the address box of the browser on PC1 to trigger user authentication on the firewall. Enter the user name and password to log in. After the login is successful, PC1 can ping the FTP/WWW Server.
3. Check whether the traffic policy takes effect. Use PC1 to download files from the FTP/WWW Server through FTP.
4. Check whether the quota control policy takes effect. Use PC1 to download a large number of files from the FTP/WWW Server through FTP. When the quota is exceeded, PC1 cannot download files any more.

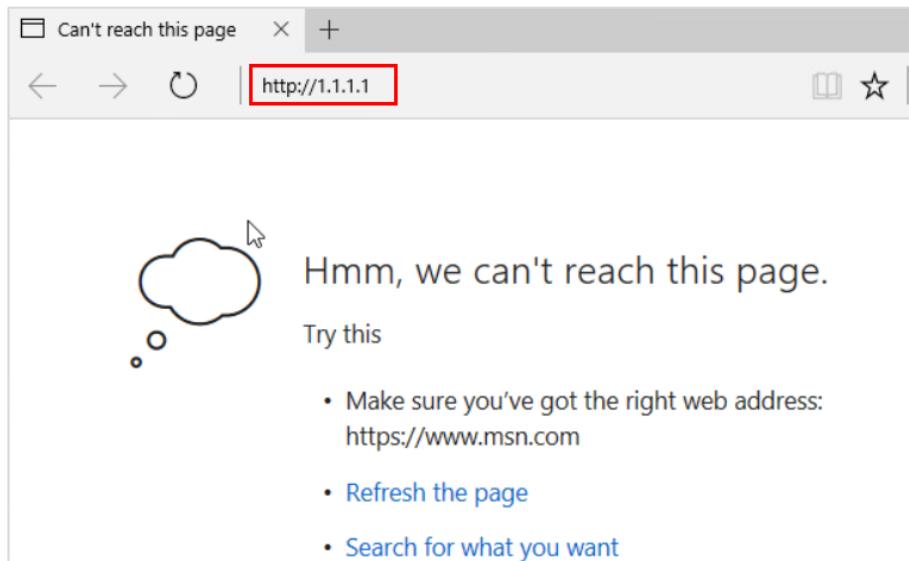
PC1 cannot ping the FTP/WWW Server when user authentication is not performed.

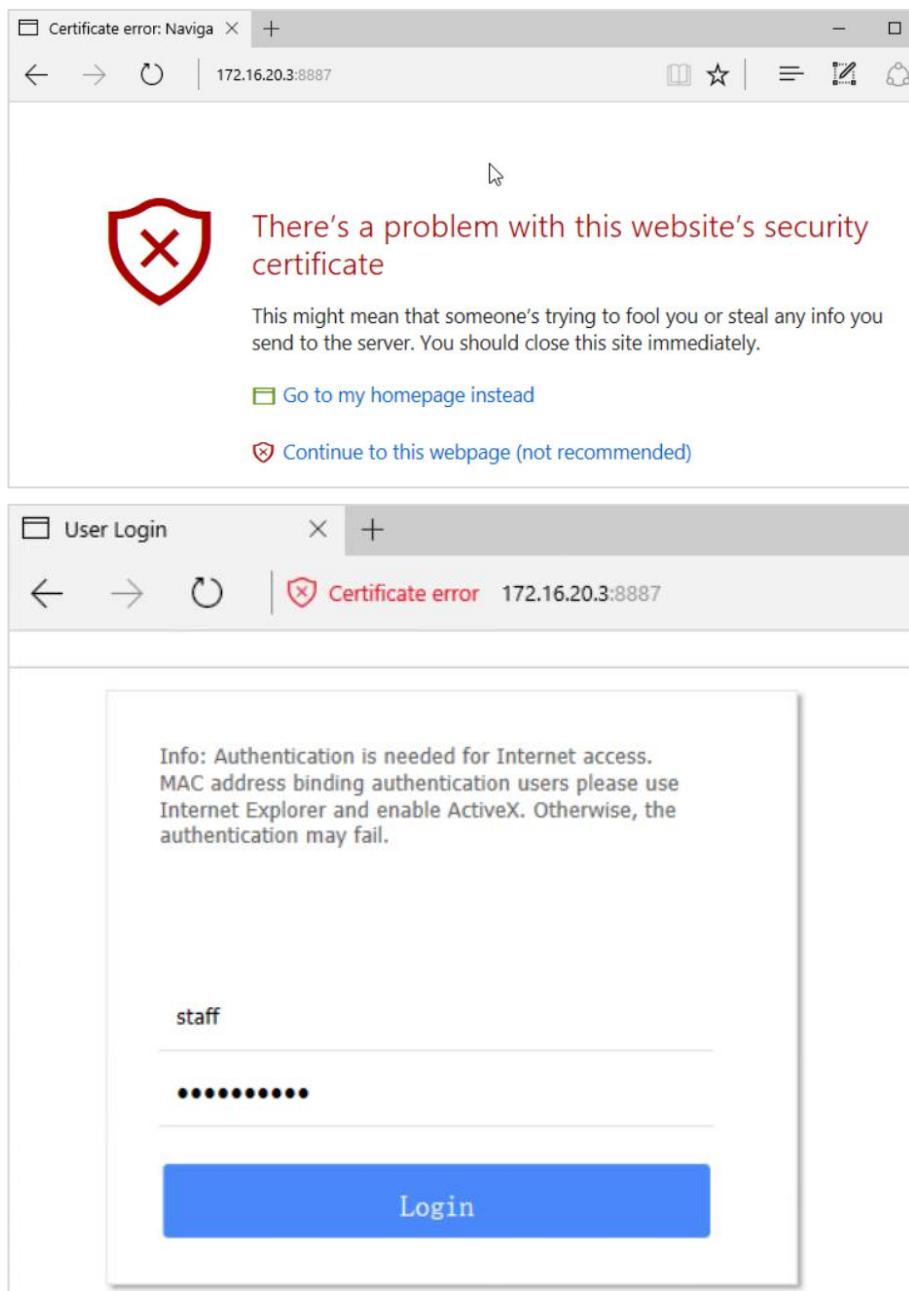
```
C:\Users\Security>ping 100.20.1.2

Pinging 100.20.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

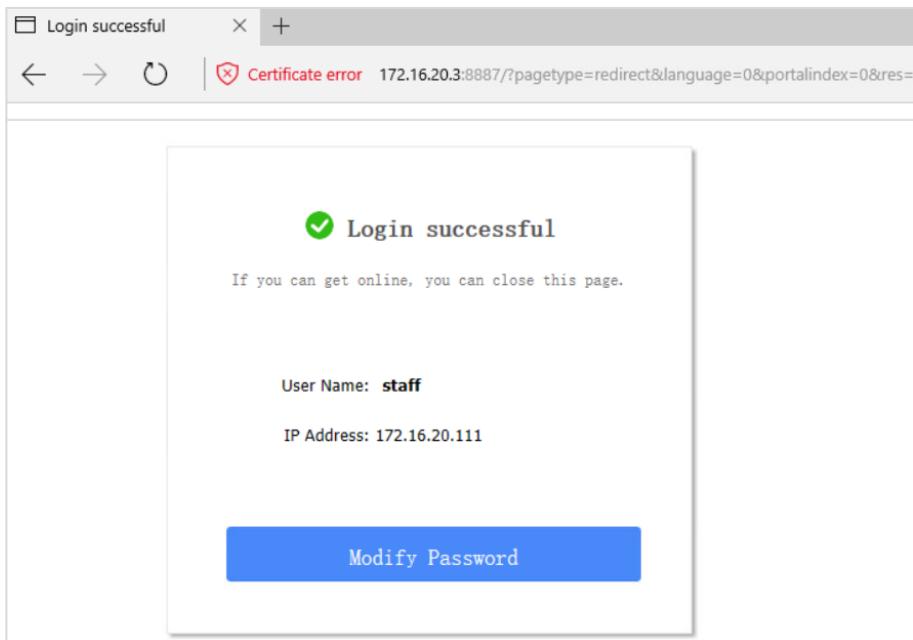
Ping statistics for 100.20.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Security>
```

Enter **http://1.1.1.1** in the address box of the browser on PC1. On the page that is displayed, enter the configured user name and password to log in.





The screenshot shows two stacked browser windows. The top window is titled "Certificate error: Naviga" and has the URL "172.16.20.3:8887". It displays a red shield icon with a large red X. The message reads: "There's a problem with this website's security certificate. This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately." Below the message are two buttons: "Go to my homepage instead" (disabled) and "Continue to this webpage (not recommended)". The bottom window is titled "User Login" and also has the URL "172.16.20.3:8887". It shows a login form with a placeholder "staff" and a masked password field. A blue "Login" button is at the bottom.



After PC1 is authenticated successfully, PC1 can ping the FTP/WWW Server successfully.

```
C:\Users\Security>ping 100.20.1.2

Pinging 100.20.1.2 with 32 bytes of data:
Reply from 100.20.1.2: bytes=32 time=1ms TTL=253

Ping statistics for 100.20.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

After the traffic policy is configured, the rate at which intranet user PC1 downloads files from the FTP/WWW Server on the Internet is limited.

```
C:\Users\Security>ftp 100.20.1.2
Connected to 100.20.1.2.
220 3Com 3CDaemon FTP Server Version 2.0
530 Not logged in
User (100.20.1.2:(none)): 111
331 User name ok, need password
Password:
230 User logged in
ftp> get 2_NotePad++.6.6.9.Installer.exe
200 PORT command successful.
150 File status OK ; about to open data connection
226 Closing data connection; File transfer successful.
ftp: 7945210 bytes received in 32.00Seconds 248.28Kbytes/sec.
```

After the traffic policy is canceled, the rate at which the user downloads the same file from the Internet is not limited.

```
C:\Users\Security>ftp 100.20.1.2
Connected to 100.20.1.2.
220 3Com 3CDaemon FTP Server Version 2.0
530 Not logged in
User (100.20.1.2:(none)): 111
331 User name ok, need password
Password:
230 User logged in
ftp> get 2_NotePad++.6.6.9.Installer.exe
200 PORT command successful.
150 File status OK ; about to open data connection
226 Closing data connection; File transfer successful.
ftp: 7945210 bytes received in 4.00Seconds 1986.30Kbytes/sec.
```

3.4 Configuration Reference

3.4.1 FW2's Configuration

```
#  
sysname FW2  
#  
interface GigabitEthernet0/0/2  
  undo shutdown  
  ip address 100.6.1.2 255.255.255.252  
#  
interface GigabitEthernet0/0/5  
  undo shutdown  
  ip address 172.16.20.3 255.255.255.0  
#  
firewall zone local  
  set priority 100  
#  
firewall zone trust  
  set priority 85  
  add interface GigabitEthernet0/0/5  
#  
firewall zone untrust  
  set priority 5  
  add interface GigabitEthernet0/0/2  
#  
firewall zone dmz  
  set priority 50  
#  
ip route-static 0.0.0.0 0.0.0.0 100.6.1.1  
#  
traffic-policy  
  profile ftp  
    bandwidth maximum-bandwidth whole downstream 20000  
    bandwidth maximum-bandwidth per-ip downstream 2000  
    quit  
#  
rule name ftp  
  source-zone trust  
  destination-zone untrust
```

```
source-address 172.16.20.0 mask 255.255.255.0
    action qos profile ftp
#
security-policy
    default action permit
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 172.16.20.0 mask 255.255.255.0
        action permit
#
nat-policy
    rule name easyip
        source-zone trust
        destination-zone untrust
        source-address 172.16.20.0 mask 255.255.255.0
        action source-nat easy-ip
#
auth-policy
    default action auth
    rule name portal
        source-zone trust
        destination-zone untrust
        action auth
#
user-manage user staff
password Huawei@123
#
security-policy
    rule name trust-local
        source-zone trust
        destination-zone local
        action permit
#
quota-policy
profile staff-limit
stream-daily 2048 reminder-threshold 80
time-daily 240 reminder-threshold 80
rule name staff-limit
    user username staff
action quota profile staff-limit
#
```

3.4.2 RT2's Pre-configuration

```
#
sysname RT2
#
interface GigabitEthernet0/0/1
undo portswitch
interface GigabitEthernet0/0/1.40
dot1q termination vid 40
    ip address 3.3.3.2 255.255.255.252
#
```

```
interface GigabitEthernet0/0/4
undo portswitch
ip address 100.6.1.1 255.255.255.252
#
ip route-static 100.20.1.0 255.255.255.0 3.3.3.1
#
```

3.4.3 Mirror-SW's Pre-configuration

```
#
sysname Mirror-SW
#
vlan batch 40
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 40
#
```

3.4.4 SW1's Pre-configuration

```
#
vlan batch 40 300
#
interface vlanif40
ip address 3.3.3.1 255.255.255.252
#
interface vlanif300
ip address 100.20.1.1 255.255.255.0
#
interface GigabitEthernet 0/0/3
port link-type trunk
port trunk allow-pass vlan 40
#
interface GigabitEthernet 0/0/15
port link-type access
port default vlan 300
#
ip route-static 10.6.1.0 255.255.255.252 3.3.3.2
#
```

3.5 Quiz

What are the differences between bandwidth management policies and quota control policies?

Answers:

1. Bandwidth management enables a firewall to manage and control traffic based on the inbound interfaces/source security zones, outbound interfaces/destination security zones, source addresses/regions, destination addresses/regions, users, services, applications, URL categories, schedules, and DSCP priorities. Bandwidth management enables the firewall to limit bandwidth, guarantee bandwidth, and limit the maximum number of connections to improve bandwidth efficiency and prevent bandwidth exhaustion.
2. Quota control policies control users' online traffic and online duration to avoid bandwidth overuse and impact on work efficiency due to long online duration.

4 Firewall Virtual System

4.1 Introduction

4.1.1 About This Lab

A large-scale enterprise, comprising R&D and marketing departments, uses the firewall as the egress gateway of its network. The enterprise wants to use the virtual system function of the firewall to manage the networks of R&D and marketing departments separately, thereby implementing refined management of access permissions between the two departments and between the departments and the Internet. This can ensure network security while meeting service requirements.

In this lab, deploy a firewall as the gateway, and use a switch to simulate the Internet to demonstrate virtual system configuration.

4.1.2 Objectives

- Learn how to create virtual systems and allocate virtual system resources.
- Implement communication between virtual systems and the public system.
- Implement communication between virtual systems.
- Enable the R&D and marketing departments in the enterprise to use the same public IP address of the public system to access the Internet.

4.1.3 Networking Topology

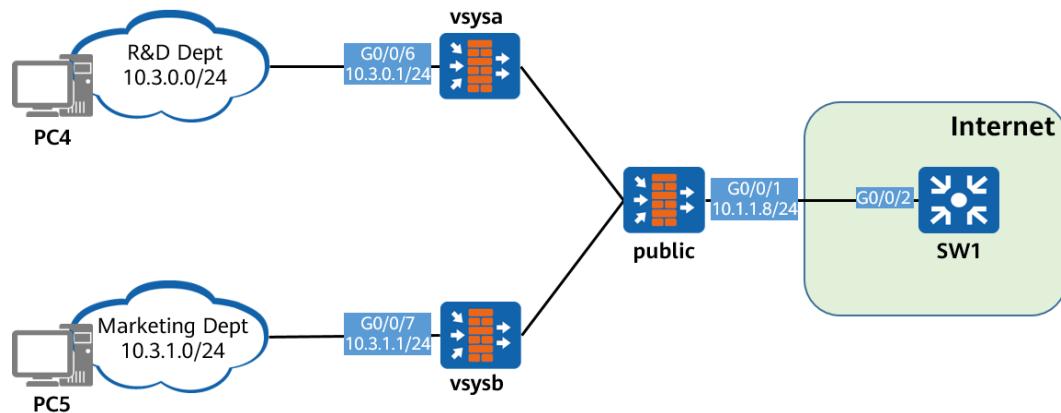


Figure 4-1 Topology for configuring communication between firewall virtual systems

The preceding figure shows device connections. For details about IP address planning, see Table 4-1.

Virtual systems named **vsysa** and **vsysb** are created on the firewall. GigabitEthernet0/0/6 belongs to vsysa, GigabitEthernet0/0/7 belongs to vsysb, and GigabitEthernet0/0/1 belongs to the public system.

SW1 simulates the Internet. This part of configurations is not described in the configuration procedure. For details, see 4.4 Configuration Reference.

4.1.4 Lab Planning

Table 4-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
FW3	G0/0/1	Layer 3 interface	100.1.1.8/24 Security zone: Untrust	Enterprise outbound interface, connecting to the Internet
	G0/0/6	Layer 3 interface	10.3.0.1/24 Security zone: Trust	Internal communication interface of vsysa
	G0/0/7	Layer 3 interface	10.3.1.1/24 Security zone: Trust	Internal communication interface of vsysb
	Virtual-if0	Layer 3 interface	172.16.0.1/24 Security zone: Trust	Virtual interface of the public firewall, connecting to vsysa and vsysb
	Virtual-if1	Layer 3 interface	172.16.1.1/24 Security zone: Untrust	Virtual interface of vsysa, connecting to the public system
	Virtual-if2	Layer 3 interface	172.16.2.1/24 Security zone: Untrust	Virtual interface of vsysb, connecting to the public system
SW1	G0/0/2	Access	PVID: 1	Interface for connecting to the firewall
	VLANIF1	Layer 3 interface	100.1.1.1/24	Interface for simulating the Internet
PC4	Ethernet0	NIC	10.3.0.100/24 Gateway: 10.3.0.1/24	Terminal
PC5	Ethernet0	NIC	10.3.1.100/24 Gateway: 10.3.1.1/24	Terminal

4.2 Lab Configuration

4.2.1 Configuration Roadmap

1. Enable the virtual system function.
2. Configure a resource class based on service requirements, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.
3. Configure interfaces for the public system, vsysa, and vsysb, and add the interfaces to security zones.
4. Configure routes in the public system, vsysa, and vsysb to divert traffic from hosts in the R&D and marketing departments to the Internet.
5. Configure security policies in the public system, vsysa, and vsysb based on service requirements and permit traffic from hosts on 10.3.0.100 to 10.3.0.110 in the R&D department and all hosts in the marketing department to the Internet.
6. Configure a source NAT policy in the public system to translate the source IP addresses of the packets from the intranet to the Internet into the IP address of the public interface in the public system.
7. In the public system, configure routes for communication between employees in the R&D and marketing departments.

4.2.2 Configuration Procedure on the CLI

Step 1 Set basic network parameters.

Set basic network parameters according to the table in 4.1.4 Lab Planning.

SW1 has been preconfigured. For details, see 4.4 Configuration Reference.

Step 2 Enable the virtual system function.

Enable the virtual system function.

```
<FW> system-view  
[FW] vsys enable
```

Step 3 Configure a resource class.

Configure a resource class, create virtual systems vsysa and vsysb in the public system, and allocate resources to the virtual systems.

Configure a resource class.

```
[FW] resource-class r1  
[FW-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000  
[FW-resource-class-r1] resource-item-limit policy reserved-number 300  
[FW-resource-class-r1] resource-item-limit bandwidth 20 entire  
[FW-resource-class-r1] quit
```

Create virtual system vsysa and allocate resources to it.

```
[FW] vsys name vsysa  
[FW-vsyst-vsysa] assign resource-class r1  
[FW-vsyst-vsysa] assign interface GigabitEthernet 0/0/6  
[FW-vsyst-vsysa] quit
```

Create virtual system vsysb and allocate resources to it.

```
[FW] vsys name vsysb  
[FW-vsyst-vsysb] assign resource-class r1  
[FW-vsyst-vsysb] assign interface GigabitEthernet 0/0/7  
[FW-vsyst-vsysb] quit
```

Step 4 Configure interfaces for the public system.

Configure interfaces for the public system and add them to security zones.

```
[FW] interface GigabitEthernet 0/0/1  
[FW-GigabitEthernet0/0/1] ip address 100.1.1.8 24  
[FW-GigabitEthernet0/0/1] quit  
[FW] interface Virtual-if 0  
[FW-Virtual-if0] ip address 172.16.0.1 24  
[FW-Virtual-if0] quit  
[FW] firewall zone trust  
[FW-zone-trust] add interface Virtual-if 0  
[FW-zone-trust] quit  
[FW] firewall zone untrust  
[FW-zone-untrust] add interface GigabitEthernet 0/0/1  
[FW-zone-untrust] quit
```

Step 5 Configure a route from the public system to the Internet.

Configure a route from the public system to the Internet to divert traffic from hosts in the R&D and marketing departments to the Internet. 100.1.1.1 is the next-hop address of the route from the public system to the Internet.

```
[FW] ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
```

Step 6 Configure a security policy for the public system.

Configure a security policy in the public system to permit traffic from hosts in the R&D and marketing departments to the Internet.

```
[FW] security-policy  
[FW-policy-security] rule name trust_to_untrust  
[FW-policy-security-rule-trust_to_untrust] source-zone trust  
[FW-policy-security-rule-trust_to_untrust] destination-zone untrust  
[FW-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24  
[FW-policy-security-rule-trust_to_untrust] source-address 10.3.1.0 24  
[FW-policy-security-rule-trust_to_untrust] action permit  
[FW-policy-security-rule-trust_to_untrust] quit  
[FW-policy-security] quit
```

Step 7 Configure a NAT policy for the public system.

Configure a source NAT policy for the public system to translate the source IP addresses of the packets from the R&D and marketing departments to the Internet into the IP address of the public interface GE0/0/1 in the public system.

```
[FW] nat-policy  
[FW-policy-nat] rule name nat1  
[FW-policy-nat-rule-nat1] source-zone trust  
[FW-policy-nat-rule-nat1] egress-interface GigabitEthernet 0/0/1  
[FW-policy-nat-rule-nat1] source-address 10.3.0.0 24  
[FW-policy-nat-rule-nat1] source-address 10.3.1.0 24  
[FW-policy-nat-rule-nat1] action source-nat easy-ip  
[FW-policy-nat-rule-nat1] quit  
[FW-policy-nat] quit
```

Step 8 Set parameters for virtual system vsysa.

Configure interfaces for vsysa, add them to security zones, and configure routes and security policies for vsysa.

Switch from the user view of the public system to the system view of vsysa.

```
[FW] switch vsys vsysa  
<FW-vsysa> system-view
```

Configure interfaces for vsysa and add them to security zones.

```
[FW-vsysa] interface GigabitEthernet0/0/6  
[FW-vsysa-GigabitEthernet0/0/6] ip address 10.3.0.1 255.255.255.0  
[FW-vsysa-GigabitEthernet0/0/6] quit  
[FW-vsysa] interface Virtual-if 1  
[FW-vsysa-Virtual-if1] ip address 172.16.1.1 255.255.255.0  
[FW-vsysa] firewall zone trust  
[FW-vsysa-zone-trust] add interface GigabitEthernet0/0/6  
[FW-vsysa-zone-trust] quit  
[FW-vsysa] firewall zone untrust  
[FW-vsysa-zone-untrust] add interface Virtual-if1  
[FW-vsysa-zone-untrust] quit
```

Configure a route from vsysa to the public system to divert the traffic from hosts in the R&D department accessing the Internet to the public system.

```
[FW-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a security policy in vsysa to allow hosts on the IP address range of 10.3.0.100 to 10.3.0.110 in the R&D department to access the Internet.

```
[FW-vsysa] security-policy  
[FW-vsysa-policy-security] rule name to_internet_allow  
[FW-vsysa-policy-security-rule-to_internet_allow] source-zone trust  
[FW-vsysa-policy-security-rule-to_internet_allow] destination-zone untrust  
[FW-vsysa-policy-security-rule-to_internet_allow] source-address range 10.3.0.100 10.3.0.110  
[FW-vsysa-policy-security-rule-to_internet_allow] action permit  
[FW-vsysa-policy-security-rule-to_internet_allow] quit
```

Configure a security policy in vsysa to allow all hosts in the R&D department to access hosts in the marketing department.

```
[FW-vsysa] security-policy  
[FW-vsysa-policy-security] rule name to_market_allow  
[FW-vsysa-policy-security-rule-to_market_allow] source-zone trust  
[FW-vsysa-policy-security-rule-to_market_allow] destination-zone untrust  
[FW-vsysa-policy-security-rule-to_market_allow] destination-address 10.3.1.0 24  
[FW-vsysa-policy-security-rule-to_market_allow] action permit  
[FW-vsysa-policy-security-rule-to_market_allow] quit
```

Configure a security policy in vsysa to forbid hosts beyond the IP address range of 10.3.0.100 to 10.3.0.110 in the R&D department to access the Internet.

```
[FW-vsysa-policy-security] rule name to_internet_block  
[FW-vsysa-policy-security-rule-to_internet_block] source-zone trust  
[FW-vsysa-policy-security-rule-to_internet_block] destination-zone untrust  
[FW-vsysa-policy-security-rule-to_internet_block] action deny  
[FW-vsysa-policy-security-rule-to_internet_block] quit
```

Step 9 Set parameters for virtual system vsysb.

Configure interfaces for vsysb, add them to security zones, and configure routes and security policies for vsysb.

Switch from the user view of vsysa to the system view of vsysb.

```
[FW-vsysa] quit  
<FW-vsysa> quit  
[FW] switch vsys vsysb  
<FW-vsysb> system-view
```

Configure interfaces for vsysb and add them to security zones.

```
[FW-vsysb] interface GigabitEthernet0/0/7  
[FW-vsysb-GigabitEthernet0/0/7] ip address 10.3.1.1 255.255.255.0  
[FW-vsysb-GigabitEthernet0/0/7] quit  
[FW-vsysb] interface Virtual-if 2  
[FW-vsysb-Virtual-if2] ip address 172.16.2.1 255.255.255.0  
[FW-vsysb-Virtual-if2] quit  
[FW-vsysb] firewall zone trust  
[FW-vsysb-zone-trust] add interface GigabitEthernet0/0/7  
[FW-vsysb-zone-trust] quit  
[FW-vsysb] firewall zone untrust  
[FW-vsysb-zone-untrust] add interface Virtual-if2  
[FW-vsysb-zone-untrust] quit
```

Configure a route from vsysb to the public system to divert the traffic from hosts in the marketing department accessing the Internet to the public system.

```
[FW-vsysb] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a security policy in vsysb to allow all hosts in the marketing department to access the Internet.

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

Step 10 Configure routes for communication between virtual systems.

Configure routes in the public system and security policies in vsysa and vsysb for employees in the R&D and marketing departments to communicate with each other.

Switch from the user view of vsysb to the user view of the public system.

```
[FW-vsysb] quit  
<FW-vsysb> quit
```

Configure routes.

```
[FW] ip route-static vpn-instance vsysb 10.3.0.0 255.255.255.0 vpn-instance vsysa  
[FW] ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsysb
```

Enter vsysa and configure a security policy to permit traffic from hosts in vsysb to access hosts in vsysa.

```
[FW] switch vsys vsysa  
<FW-vsysa> system-view  
Enter system view, return user view with Ctrl+Z.  
[FW-vsysa] security-policy  
[FW-vsysa-policy-security] rule name vsysb_to_vsysa  
[FW-vsysa-policy-security-rule-vsysb_to_vsysa] source-zone untrust  
[FW-vsysa-policy-security-rule-vsysb_to_vsysa] destination-zone trust  
[FW-vsysa-policy-security-rule-vsysb_to_vsysa] source-address 10.3.1.0 24  
[FW-vsysa-policy-security-rule-vsysb_to_vsysa] destination-address 10.3.0.0 24  
[FW-vsysa-policy-security-rule-vsysb_to_vsysa] action permit  
[FW-vsysa-policy-security-rule-vsysb_to_vsysa] quit  
[FW-vsysa-policy-security] quit
```

Enter vsysb and configure a security policy to permit traffic from hosts in vsysa to access hosts in vsysb.

```
[FW] switch vsys vsysb  
<FW-vsysb> system-view  
Enter system view, return user view with Ctrl+Z.  
[FW-vsysb] security-policy  
[FW-vsysb-policy-security] rule name vsysa_to_vsysb  
[FW-vsysb-policy-security-rule-vsysa_to_vsysb] source-zone untrust  
[FW-vsysb-policy-security-rule-vsysa_to_vsysb] destination-zone trust  
[FW-vsysb-policy-security-rule-vsysa_to_vsysb] source-address 10.3.0.0 24  
[FW-vsysb-policy-security-rule-vsysa_to_vsysb] destination-address 10.3.1.0 24
```

```
[FW-vsystb-policy-security-rule-vsysta_to_vsystb] action permit  
[FW-vsystb-policy-security-rule-vsysta_to_vsystb] quit  
[FW-vsystb-policy-security] quit
```

4.2.3 Configuration Procedure on the Web UI

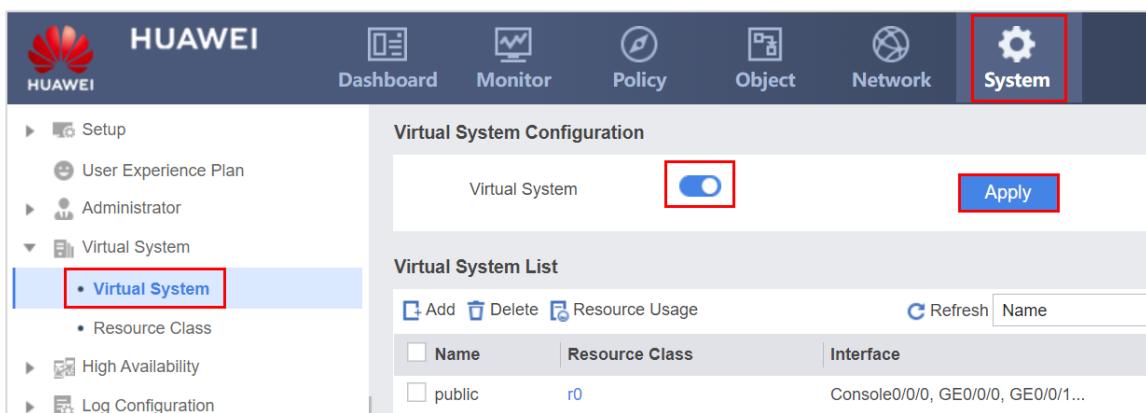
Step 1 Set basic network parameters.

Set basic network parameters according to the table in 4.1.4 Lab Planning.

SW1 has been preconfigured. For details, see 4.4 Configuration Reference.

Step 2 Enable the virtual system function.

Choose **System > Virtual System > Virtual System**, enable the virtual system function, and click **Apply**.



Step 3 Configure a resource class.

Configure a resource class, create virtual systems vsysa and vsystb in the public system, and allocate resources to the virtual systems.

Choose **System > Virtual System > Resource Class** and click **Add**.

Add Resource Class

Name	R1	*																																																			
Description																																																					
<table border="1"> <thead> <tr> <th>Name</th> <th>Reserved</th> <th>Maximum</th> </tr> </thead> <tbody> <tr> <td>Sessions (IPv4)</td> <td>10000</td> <td><1-3000000></td> </tr> <tr> <td>Sessions (IPv6)</td> <td></td> <td><1-3000000></td> </tr> <tr> <td>Online Users</td> <td></td> <td><1-8000></td> </tr> <tr> <td>Users</td> <td></td> <td><1-8000></td> </tr> <tr> <td>User Groups</td> <td></td> <td><1-6000></td> </tr> <tr> <td>Security Groups</td> <td></td> <td><1-5000></td> </tr> <tr> <td>Policies</td> <td>300</td> <td><1-15000></td> </tr> <tr> <td>Traffic Policies</td> <td></td> <td><1-512></td> </tr> <tr> <td>IPSec Tunnels</td> <td></td> <td><1-5280></td> </tr> <tr> <td>L2TP Tunnels</td> <td></td> <td><1-4000></td> </tr> <tr> <td>SSL VPN Concurrent Users</td> <td></td> <td><1-500></td> </tr> <tr> <td>Downstream Bandwidth</td> <td></td> <td><1-10000>Mbps</td> </tr> <tr> <td>Upstream Bandwidth</td> <td></td> <td><1-10000>Mbps</td> </tr> <tr> <td>Total Bandwidth</td> <td>20</td> <td><1-10000>Mbps</td> </tr> <tr> <td>New Session Rates (IPv4)</td> <td></td> <td><1-80000></td> </tr> <tr> <td>New Session Rates (IPv6)</td> <td></td> <td><1-80000></td> </tr> </tbody> </table>			Name	Reserved	Maximum	Sessions (IPv4)	10000	<1-3000000>	Sessions (IPv6)		<1-3000000>	Online Users		<1-8000>	Users		<1-8000>	User Groups		<1-6000>	Security Groups		<1-5000>	Policies	300	<1-15000>	Traffic Policies		<1-512>	IPSec Tunnels		<1-5280>	L2TP Tunnels		<1-4000>	SSL VPN Concurrent Users		<1-500>	Downstream Bandwidth		<1-10000>Mbps	Upstream Bandwidth		<1-10000>Mbps	Total Bandwidth	20	<1-10000>Mbps	New Session Rates (IPv4)		<1-80000>	New Session Rates (IPv6)		<1-80000>
Name	Reserved	Maximum																																																			
Sessions (IPv4)	10000	<1-3000000>																																																			
Sessions (IPv6)		<1-3000000>																																																			
Online Users		<1-8000>																																																			
Users		<1-8000>																																																			
User Groups		<1-6000>																																																			
Security Groups		<1-5000>																																																			
Policies	300	<1-15000>																																																			
Traffic Policies		<1-512>																																																			
IPSec Tunnels		<1-5280>																																																			
L2TP Tunnels		<1-4000>																																																			
SSL VPN Concurrent Users		<1-500>																																																			
Downstream Bandwidth		<1-10000>Mbps																																																			
Upstream Bandwidth		<1-10000>Mbps																																																			
Total Bandwidth	20	<1-10000>Mbps																																																			
New Session Rates (IPv4)		<1-80000>																																																			
New Session Rates (IPv6)		<1-80000>																																																			
Displaying 16																																																					
OK		Cancel																																																			

Choose **System > Virtual System > Virtual System**. On the **Virtual System List** page, click **Add** to create virtual system vsysa and allocate resources to it.

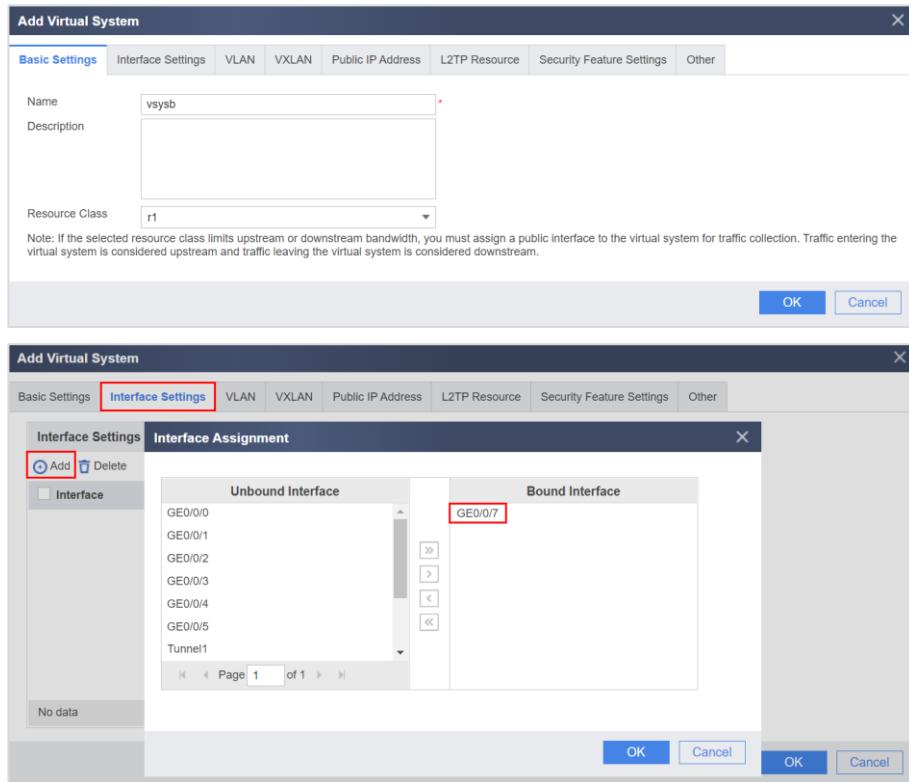
Add Virtual System

Basic Settings	Interface Settings	VLAN	VXLAN	Public IP Address	L2TP Resource	Security Feature Settings	Other
Name	vsysa						
Description							
Resource Class	r1						
<small>Note: If the selected resource class limits upstream or downstream bandwidth, you must assign a public interface to the virtual system for traffic collection. Traffic entering the virtual system is considered upstream and traffic leaving the virtual system is considered downstream.</small>							
OK		Cancel					

Add Virtual System

Basic Settings	Interface Settings	VLAN	VXLAN	Public IP Address	L2TP Resource	Security Feature Settings	Other																												
<table border="1"> <tr> <td>Interface Settings</td> <td>Interface Assignment</td> </tr> <tr> <td> <input checked="" type="radio"/> Add <input type="checkbox"/> Delete <input type="checkbox"/> Interface </td> <td> <table border="1"> <thead> <tr> <th>Unbound Interface</th> <th>Bound Interface</th> </tr> </thead> <tbody> <tr> <td>GE0/0/0</td> <td>GE0/0/0</td> </tr> <tr> <td>GE0/0/1</td> <td></td> </tr> <tr> <td>GE0/0/2</td> <td></td> </tr> <tr> <td>GE0/0/3</td> <td></td> </tr> <tr> <td>GE0/0/4</td> <td></td> </tr> <tr> <td>GE0/0/5</td> <td></td> </tr> <tr> <td>GE0/0/7</td> <td></td> </tr> </tbody> </table> </td> </tr> <tr> <td colspan="8"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </td> </tr> </table>								Interface Settings	Interface Assignment	<input checked="" type="radio"/> Add <input type="checkbox"/> Delete <input type="checkbox"/> Interface	<table border="1"> <thead> <tr> <th>Unbound Interface</th> <th>Bound Interface</th> </tr> </thead> <tbody> <tr> <td>GE0/0/0</td> <td>GE0/0/0</td> </tr> <tr> <td>GE0/0/1</td> <td></td> </tr> <tr> <td>GE0/0/2</td> <td></td> </tr> <tr> <td>GE0/0/3</td> <td></td> </tr> <tr> <td>GE0/0/4</td> <td></td> </tr> <tr> <td>GE0/0/5</td> <td></td> </tr> <tr> <td>GE0/0/7</td> <td></td> </tr> </tbody> </table>	Unbound Interface	Bound Interface	GE0/0/0	GE0/0/0	GE0/0/1		GE0/0/2		GE0/0/3		GE0/0/4		GE0/0/5		GE0/0/7		<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>							
Interface Settings	Interface Assignment																																		
<input checked="" type="radio"/> Add <input type="checkbox"/> Delete <input type="checkbox"/> Interface	<table border="1"> <thead> <tr> <th>Unbound Interface</th> <th>Bound Interface</th> </tr> </thead> <tbody> <tr> <td>GE0/0/0</td> <td>GE0/0/0</td> </tr> <tr> <td>GE0/0/1</td> <td></td> </tr> <tr> <td>GE0/0/2</td> <td></td> </tr> <tr> <td>GE0/0/3</td> <td></td> </tr> <tr> <td>GE0/0/4</td> <td></td> </tr> <tr> <td>GE0/0/5</td> <td></td> </tr> <tr> <td>GE0/0/7</td> <td></td> </tr> </tbody> </table>	Unbound Interface	Bound Interface	GE0/0/0	GE0/0/0	GE0/0/1		GE0/0/2		GE0/0/3		GE0/0/4		GE0/0/5		GE0/0/7																			
Unbound Interface	Bound Interface																																		
GE0/0/0	GE0/0/0																																		
GE0/0/1																																			
GE0/0/2																																			
GE0/0/3																																			
GE0/0/4																																			
GE0/0/5																																			
GE0/0/7																																			
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>																																			

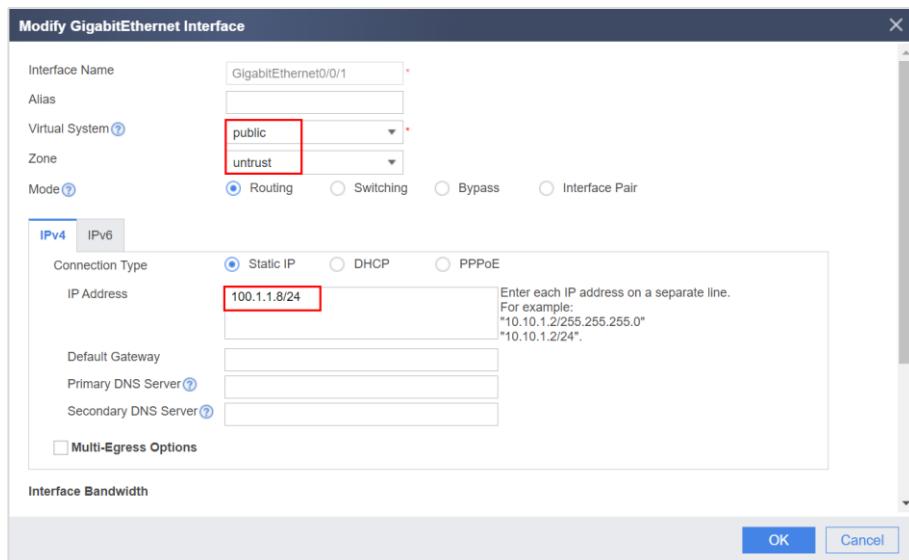
Choose **System > Virtual System > Virtual System**. On the **Virtual System List** page, click **Add** to create virtual system vsysb and allocate resources to it.



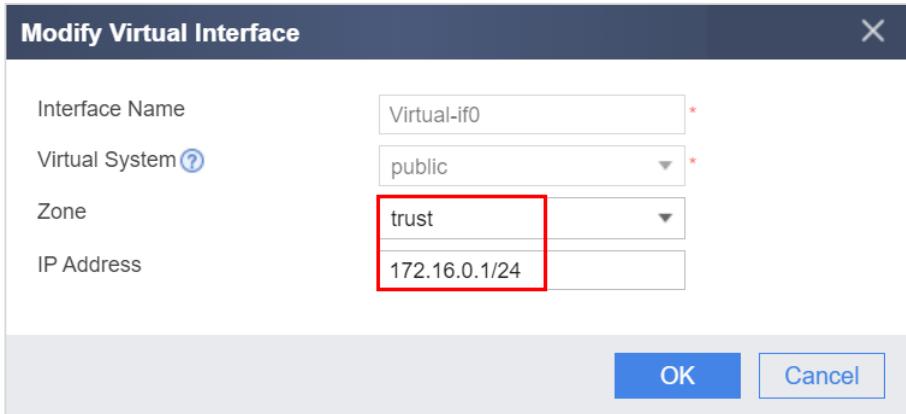
Step 4 Configure interfaces for the public system.

Configure interfaces for the public system and add them to security zones.

Choose **Network > Interface** and click  next to an interface to be configured. Set parameters and then click **OK** to configure GigabitEthernet0/0/1, as shown in the following figure.



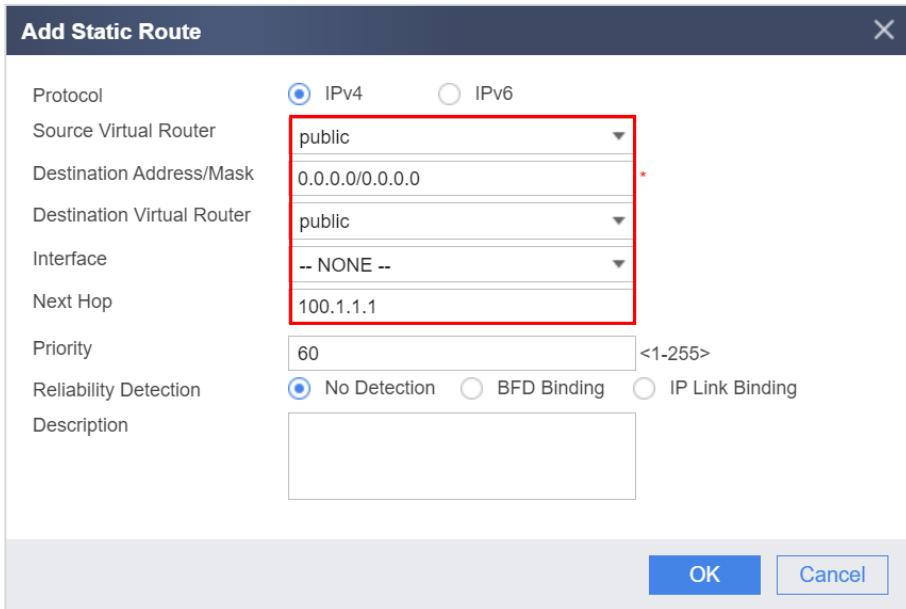
Configure Virtual-if0, as shown in the following figure.



Step 5 Configure a route from the public system to the Internet.

Configure a route to divert traffic from hosts in the R&D and marketing departments to the Internet.

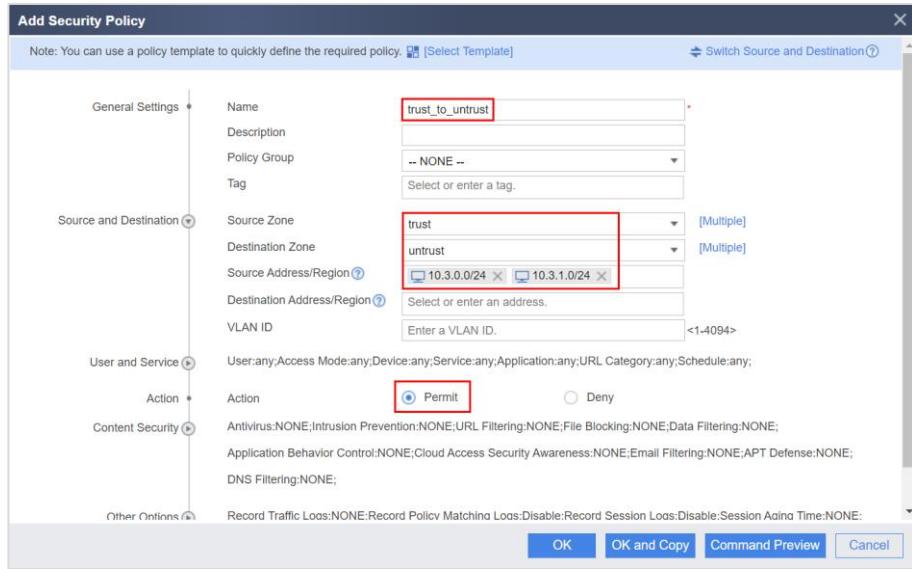
Choose **Network > Route > Static Route** and click **Add**. Configure a route from the public system to the Internet to divert traffic from hosts in the R&D and marketing departments to the Internet. 100.1.1.1 is the next-hop address of the route from the public system to the Internet.



Step 6 Configure a security policy for the public system.

Configure a security policy to permit traffic from hosts in the R&D and marketing departments to the Internet.

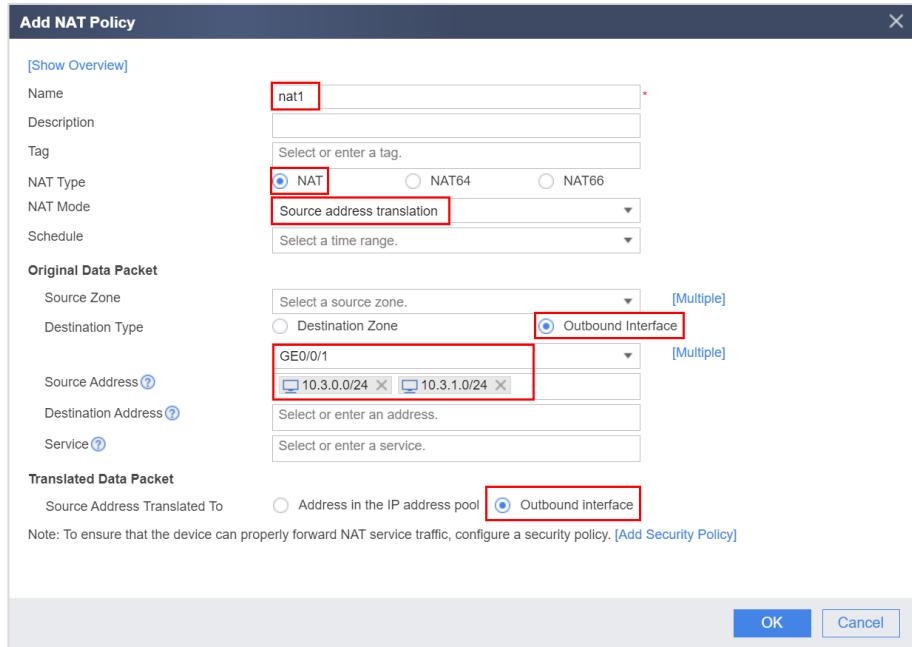
Choose **Policy > Security Policy > Security Policy**, click **Add Security Policy**, and configure a security policy in the public system to permit traffic from hosts in the R&D and marketing departments to the Internet.



Step 7 Configure a NAT policy for the public system.

Configure a NAT policy to translate the source IP addresses of the packets from the R&D and marketing departments to the Internet into the IP address of the public interface GE0/0/1 in the public system.

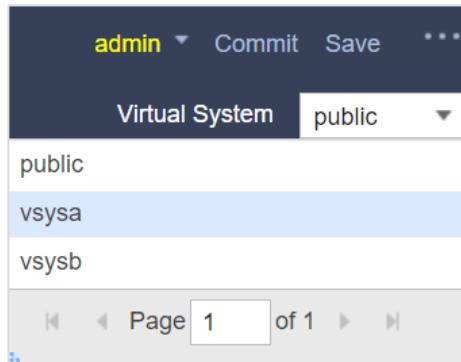
Choose **Policy > NAT Policy > NAT Policy**, click **Add**, and configure a source NAT policy in the public system to translate the source IP addresses of the packets from the intranet to the Internet into the IP address of the public interface GE0/0/1 in the public system.



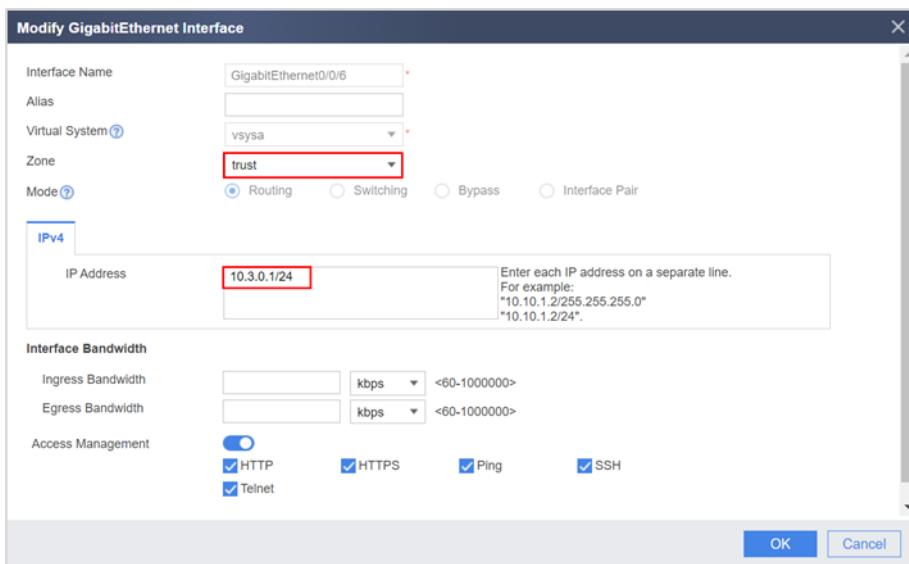
Step 8 Set parameters for virtual system vsysa.

Configure interfaces for vsysa, add them to security zones, and configure routes and security policies for vsysa.

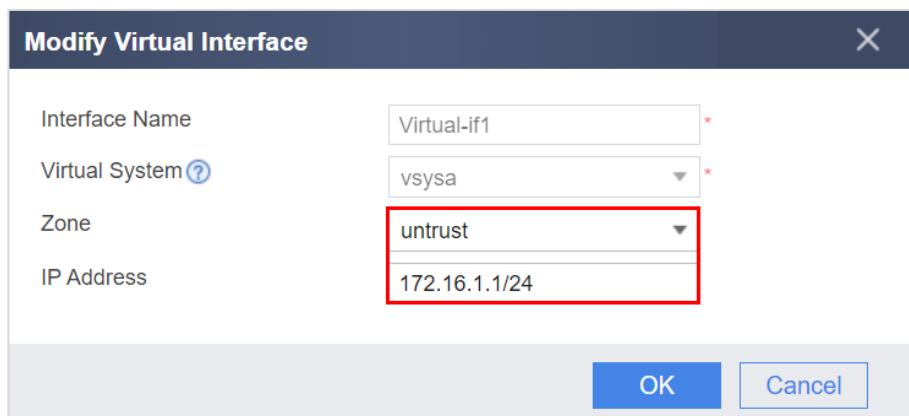
Select **vsysa** from the **Virtual System** drop-down list in the upper right corner to access vsysa.



Choose **Network > Interface** and click  next to an interface to be configured. Set parameters and then click **OK** to configure GigabitEthernet0/0/6, as shown in the following figure.



Configure Virtual-if1, as shown in the following figure.



Choose **Network > Route > Static Route**, click **Add**, and configure a route from vsysa to the public system to divert the traffic from hosts in the R&D department accessing the Internet to the public system.

Add Static Route

Source Virtual Router	vsysa
Destination Address/Mask	0.0.0.0/0.0.0.0 *
Destination Virtual Router	public
Interface	-- NONE --
Priority	<1-255>
Reliability Detection	<input checked="" type="radio"/> No Detection <input type="radio"/> IP Link Binding
Description	

OK **Cancel**

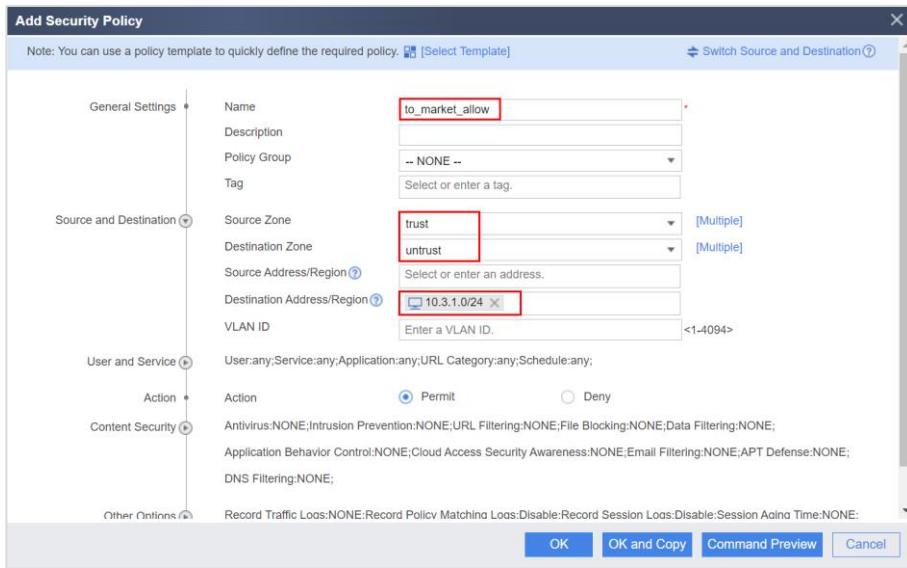
Choose Policy > Security Policy > Security Policy, click Add Security Policy, and configure a security policy for vsysa to allow hosts in the IP address range of 10.3.0.100 to 10.3.0.110 in the R&D department to access the Internet.

Add Security Policy

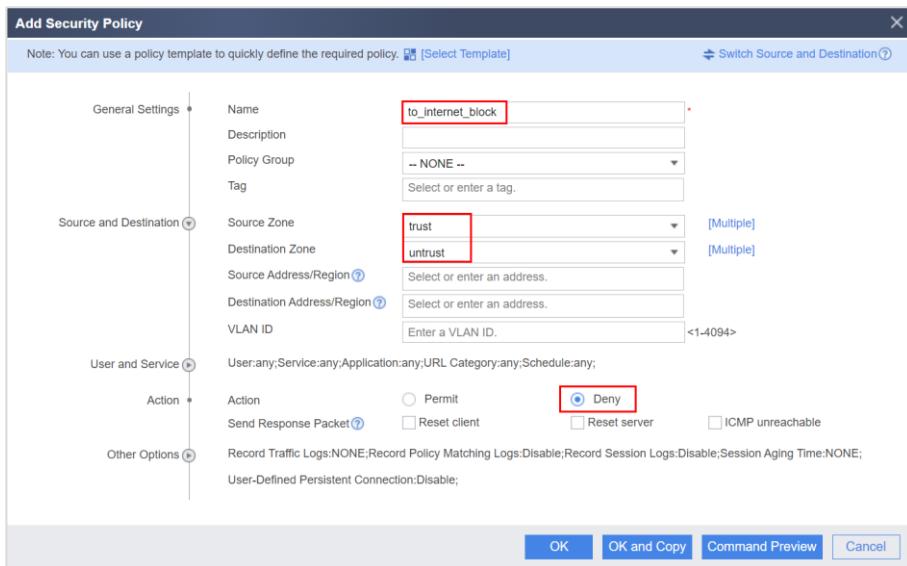
General Settings		Name: <input type="text" value="to_internet_allow"/>
Source and Destination		Source Zone: trust Destination Zone: untrust Source Address/Region: <input type="text" value="10.3.0.100-10.3.0.110"/>
Action		Action: <input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security		
Other Options		

OK **OK and Copy** **Command Preview** **Cancel**

Choose Policy > Security Policy > Security Policy, click Add Security Policy, and configure a security policy for vsysa to allow all hosts in the R&D department to access hosts in the marketing department.



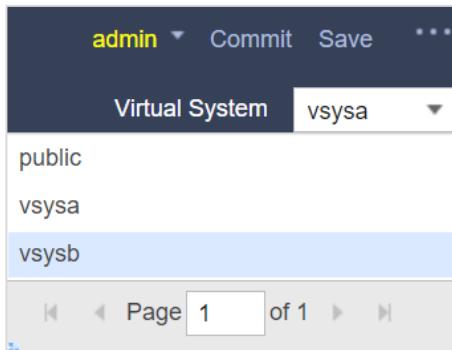
Choose **Policy > Security Policy > Security Policy**, click **Add Security Policy**, and configure a security policy for vsysa to forbid hosts beyond the IP address range of 10.3.0.100 to 10.3.0.110 in the R&D department to access the Internet.



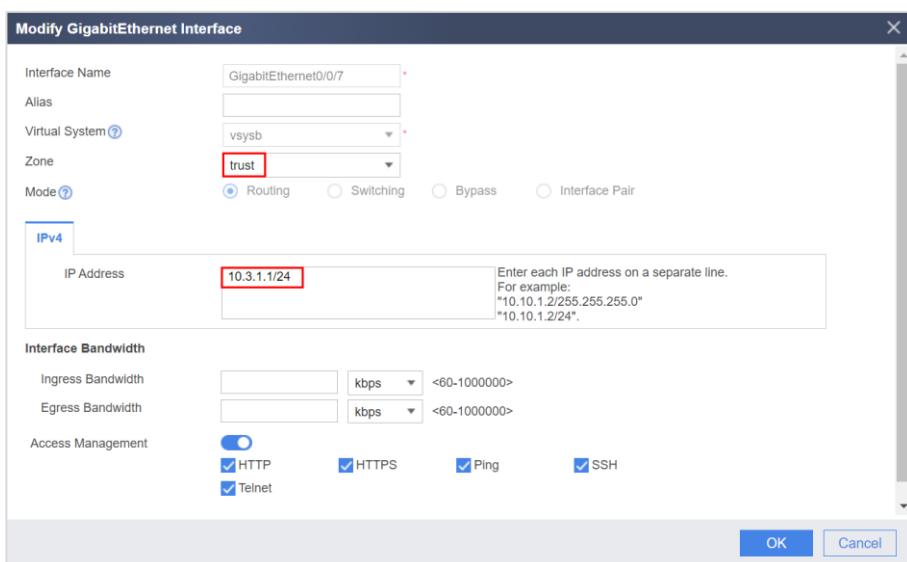
Step 9 Set parameters for virtual system vsysb.

Configure interfaces for vsysb, add them to security zones, and configure routes and security policies for vsysb.

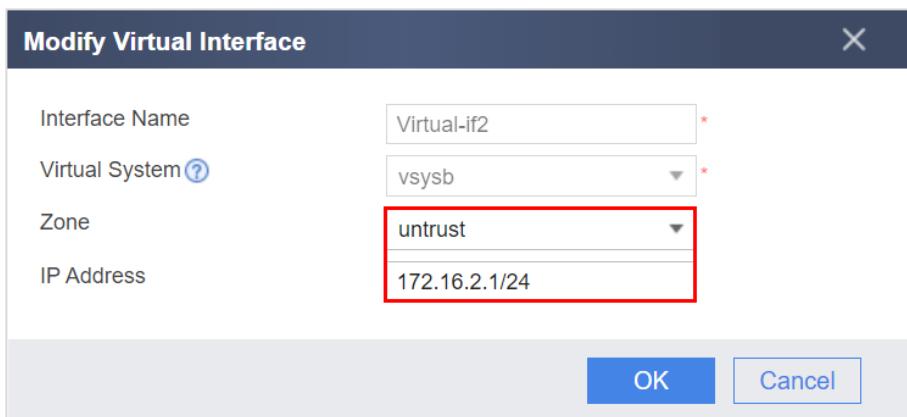
Select **vsysb** from the **Virtual System** drop-down list in the upper right corner to access vsysb.



Choose **Network > Interface** and click  next to an interface to be configured. Set parameters and then click **OK** to configure GigabitEthernet0/0/7, as shown in the following figure.



Configure Virtual-if2, as shown in the following figure.



Choose **Network > Route > Static Route**, click **Add**, and configure a route from vsysb to the public system to divert the traffic from hosts in the R&D department accessing the Internet to the public system.

Add Static Route

Source Virtual Router	vsysb
Destination Address/Mask	0.0.0.0/0.0.0.0 *
Destination Virtual Router	public
Interface	-- NONE --
Priority	<1-255>
Reliability Detection	<input checked="" type="radio"/> No Detection <input type="radio"/> IP Link Binding
Description	

OK **Cancel**

Choose **Policy > Security Policy > Security Policy**, click **Add Security Policy**, and configure a security policy in vsysb to allow all hosts in the marketing department to access the Internet.

Add Security Policy

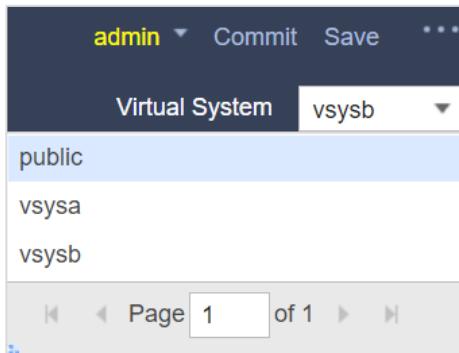
General Settings		Name: to_internet_allow
Source and Destination		Source Zone: trust [Multiple] Destination Zone: untrust [Multiple]
User and Service		User:any;Service:any;Application:any;URL Category:any;Schedule:any;
Action		Action: <input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security		Antivirus:NONE;Intrusion Prevention:NONE;URL Filtering:NONE;File Blocking:NONE;Data Filtering:NONE; Application Behavior Control:NONE;Cloud Access Security Awareness:NONE;Email Filtering:NONE;APT Defense:NONE; DNS Filtering:NONE;
Other Options		Record Traffic Logs:NONE;Record Policy Matching Logs:Disable;Record Session Logs:Disable;Session Aging Time:NONE;

OK **OK and Copy** **Command Preview** **Cancel**

Step 10 Configure routes for communication between virtual systems.

Configure routes in the public system and security policies in vsysa and vsysb for employees in the R&D and marketing departments to communicate with each other.

Select **public** from the **Virtual System** drop-down list in the upper right corner to access the public system.



Choose **Network > Route > Static Route** and click **Add** to configure routes.

Add Static Route

Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Source Virtual Router	vsysb
Destination Address/Mask	10.3.0.0/24 *
Destination Virtual Router	vsysa
Interface	-- NONE --
Next Hop	
Priority	60 <1-255>
Reliability Detection	<input checked="" type="radio"/> No Detection <input type="radio"/> IP Link Binding
Description	

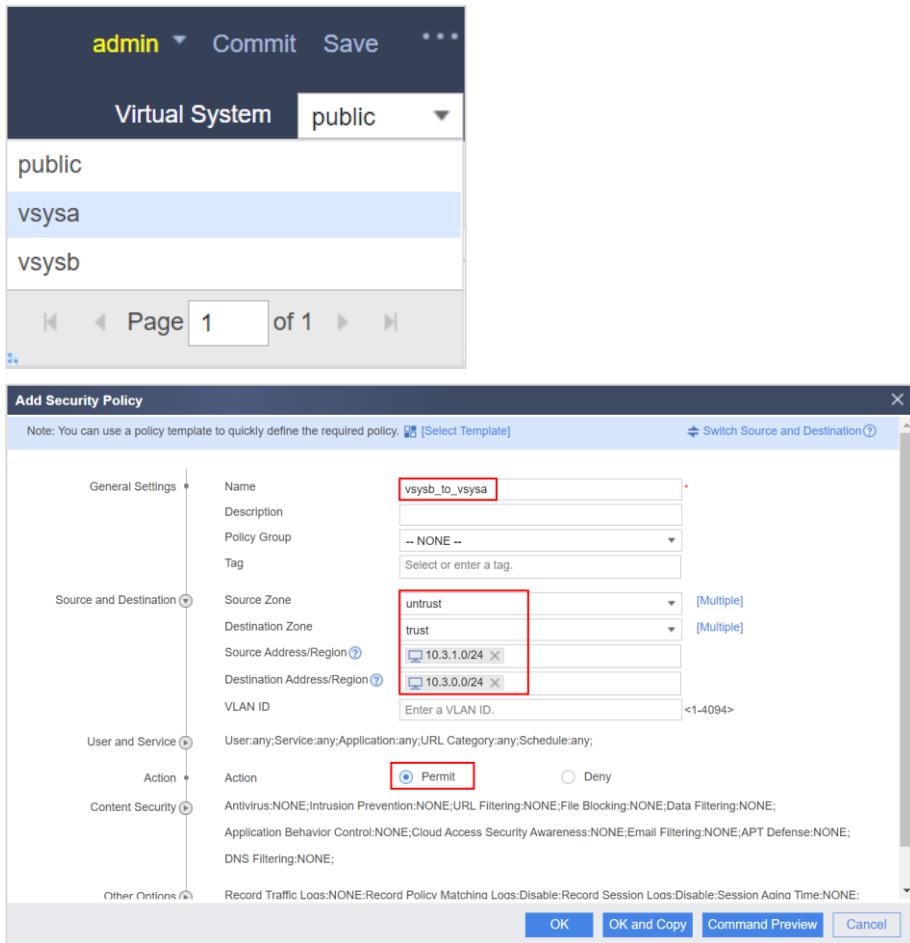
OK **Cancel**

Add Static Route

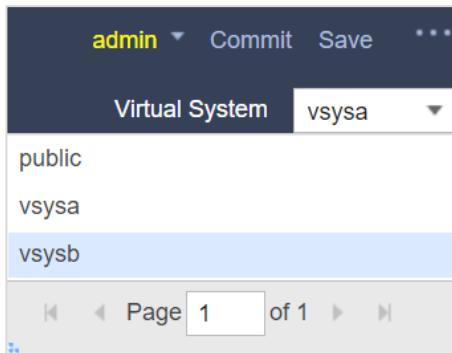
Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Source Virtual Router	vsysa
Destination Address/Mask	10.3.1.0/24 *
Destination Virtual Router	vsysb
Interface	-- NONE --
Next Hop	
Priority	60 <1-255>
Reliability Detection	<input checked="" type="radio"/> No Detection <input type="radio"/> IP Link Binding
Description	

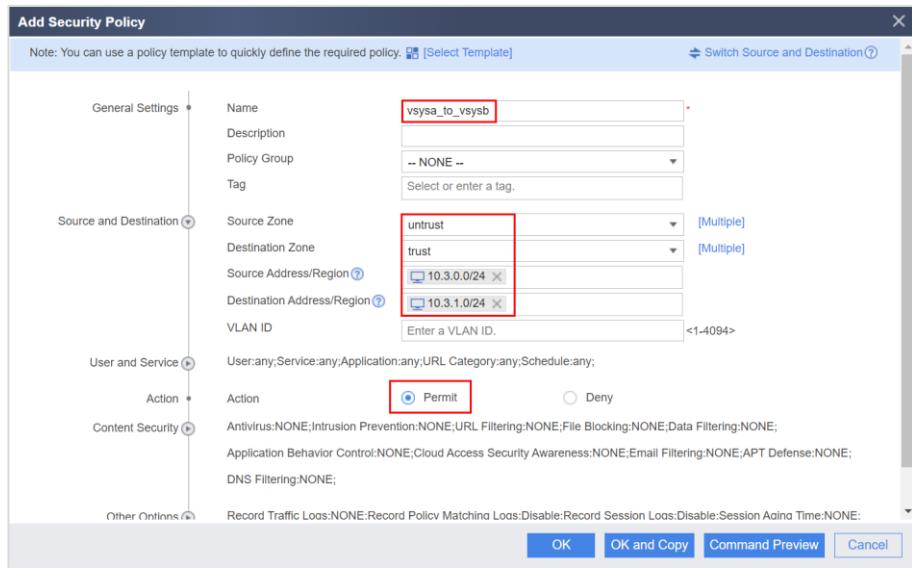
OK **Cancel**

Enter vsysa and configure a security policy to permit traffic from hosts in vsysb to access hosts in vsysa.



Enter vsysb and configure a security policy to permit traffic from hosts in vsysa to access hosts in vsysb.





4.3 Verification

After the preceding configurations are complete, check the final implementation effect.

1. Only hosts on the IP address range of 10.3.0.100 to 10.3.0.110 in the R&D department can access the Internet.
2. Hosts on network segment 10.3.1.0/24 in the marketing department can access the Internet.
3. Hosts in the R&D and marketing departments can communicate with each other.

Change the IP address of a host in the R&D department to 10.3.0.100/24 and the gateway address to 10.3.0.1/24 and verify that the host can ping 100.1.1.1 (IP address of VLANIF 1 on SW1) on the Internet.

```
C:\Users\Security>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::b541:310f:3fab:df88%5
IPv4 Address . . . . . : 10.3.0.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.3.0.1

C:\Users\Security>ping 100.1.1.1

Pinging 100.1.1.1 with 32 bytes of data:
Reply from 100.1.1.1: bytes=32 time=1ms TTL=252

Ping statistics for 100.1.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Change the IP address of a host in the R&D department to 10.3.0.120/24 and the gateway address to 10.3.0.1/24 and verify that the host cannot ping 100.1.1.1 (IP address of VLANIF 1 on SW1) on the Internet.

```
C:\Users\Security>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::b541:310f:3fab:df88%5  
IPv4 Address. . . . . : 10.3.0.120  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.3.0.1  
  
C:\Users\Security>ping 100.1.1.1  
  
Pinging 100.1.1.1 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 100.1.1.1:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Change the IP address of a host in the marketing department to 10.3.1.100/24 and the gateway address to 10.3.1.1/24 and verify that the host can ping 100.1.1.1 (IP address of VLANIF 1 on SW1) on the Internet.

```
C:\Users\Security>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::94e4:bff1:39fe:9ca5%15  
IPv4 Address. . . . . : 10.3.1.100  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.3.1.1  
  
C:\Users\Security>ping 100.1.1.1  
  
Pinging 100.1.1.1 with 32 bytes of data:  
Reply from 100.1.1.1: bytes=32 time=1ms TTL=252  
  
Ping statistics for 100.1.1.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Verify that a host in the R&D department can ping a host in the marketing department.

```
C:\Users\Security>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::b541:310f:3fab:df88%5  
IPv4 Address. . . . . : 10.3.0.120  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.3.0.1  
  
C:\Users\Security>ping 10.3.1.100  
  
Pinging 10.3.1.100 with 32 bytes of data:  
Reply from 10.3.1.100: bytes=32 time<1ms TTL=126  
  
Ping statistics for 10.3.1.100:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Verify that a host in the marketing department can ping a host in the R&D department.

```
C:\Users\Security>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::94e4:bff1:39fe:9ca5%15  
IPv4 Address. . . . . : 10.3.1.100  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.3.1.1  
  
C:\Users\Security>ping 10.3.0.120  
  
Pinging 10.3.0.120 with 32 bytes of data:  
Reply from 10.3.0.120: bytes=32 time<1ms TTL=126  
  
Ping statistics for 10.3.0.120:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4.4 Configuration Reference

4.4.1 FW3's Configuration

```
#  
vsys enable  
resource-class r1  
    resource-item-limit session reserved-number 10000 maximum 50000  
    resource-item-limit bandwidth 20 entire  
    resource-item-limit policy reserved-number 300
```

```
#  
vsys name vsysa 1  
    assign interface GigabitEthernet0/0/6  
    assign resource-class r1  
#  
vsys name vsysb 2  
    assign interface GigabitEthernet0/0/7  
    assign resource-class r1  
#  
ip vpn-instance default  
    ipv4-family  
#  
ip vpn-instance vsysa  
    ipv4-family  
    ipv6-family  
#  
ip vpn-instance vsysb  
    ipv4-family  
    ipv6-family  
#  
#  
interface GigabitEthernet0/0/1  
undo shutdown  
ip address 100.1.1.8 255.255.255.0  
service-manage http permit  
service-manage https permit  
service-manage ping permit  
service-manage ssh permit  
service-manage snmp permit  
service-manage telnet permit  
service-manage netconf permit  
#  
interface GigabitEthernet0/0/6  
undo shutdown  
ip binding vpn-instance vsysa  
ip address 10.3.0.1 255.255.255.0  
service-manage http permit  
service-manage https permit  
service-manage ping permit  
service-manage ssh permit  
service-manage telnet permit  
#  
interface GigabitEthernet0/0/7  
undo shutdown  
ip binding vpn-instance vsysb  
ip address 10.3.1.1 255.255.255.0  
service-manage http permit  
service-manage https permit  
service-manage ping permit  
service-manage ssh permit  
service-manage telnet permit  
#  
interface Virtual-if0  
ip address 172.16.0.1 255.255.255.0  
#
```

```
interface Virtual-if1
    ip address 172.16.1.1 255.255.255.0
#
interface Virtual-if2
    ip address 172.16.2.1 255.255.255.0
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface Virtual-if0
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
#
firewall zone dmz
    set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsysb
ip route-static vpn-instance vsysb 10.3.0.0 255.255.255.0 vpn-instance vsysa
#
security-policy
    rule name trust_to_untrust
        source-zone trust
        destination-zone untrust
        source-address 10.3.0.0 mask 255.255.255.0
        source-address 10.3.1.0 mask 255.255.255.0
        action permit
#
nat-policy
    rule name nat1
        source-zone trust
        egress-interface GigabitEthernet0/0/1
        source-address 10.3.0.0 mask 255.255.255.0
        source-address 10.3.1.0 mask 255.255.255.0
        action source-nat easy-ip
#
switch vsys vsysa
#
interface GigabitEthernet0/0/6
    undo shutdown
    ip binding vpn-instance vsysa
    ip address 10.3.0.1 255.255.255.0
    service-manage http permit
    service-manage https permit
    service-manage ping permit
    service-manage ssh permit
    service-manage telnet permit
#
interface Virtual-if1
    ip address 172.16.1.1 255.255.255.0
#
```

```
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/6
#
firewall zone untrust
    set priority 5
    add interface Virtual-if1
#
firewall zone dmz
    set priority 50
#
security-policy
    rule name to_internet_allow
        source-zone trust
        destination-zone untrust
        source-address address-set 10.3.0.100-10.3.0.110
        action permit
    rule name to_market_allow
        source-zone trust
        destination-zone untrust
        destination-address 10.3.1.0 mask 255.255.255.0
        action permit
    rule name to_internet_block
        source-zone trust
        destination-zone untrust
        action deny
    rule name vsysb_to_vsysa
        source-zone untrust
        destination-zone trust
        source-address 10.3.1.0 mask 255.255.255.0
        destination-address 10.3.0.0 mask 255.255.255.0
        action permit
#
ip route-static 0.0.0.0 0.0.0.0 public
#
switch vsys vsysb
#
interface GigabitEthernet0/0/7
    undo shutdown
    ip binding vpn-instance vsysb
    ip address 10.3.1.1 255.255.255.0
    service-manage http permit
    service-manage https permit
    service-manage ping permit
    service-manage ssh permit
    service-manage telnet permit
#
interface Virtual-if2
    ip address 172.16.2.1 255.255.255.0
#
firewall zone local
    set priority 100
```

```
#  
firewall zone trust  
    set priority 85  
    add interface GigabitEthernet0/0/7  
#  
firewall zone untrust  
    set priority 5  
    add interface Virtual-if2  
#  
firewall zone dmz  
    set priority 50  
#  
security-policy  
    rule name to_internet_allow  
        source-zone trust  
        destination-zone untrust  
        action permit  
    rule name vsysa_to_vsysb  
        source-zone untrust  
        destination-zone trust  
        source-address 10.3.0.0 mask 255.255.255.0  
        destination-address 10.3.1.0 mask 255.255.255.0  
        action permit  
#  
ip route-static 0.0.0.0 0.0.0.0 public  
#
```

4.4.2 SW1's Pre-configuration

```
#  
sysname SW1  
#  
interface vlanif1  
    ip address 100.1.1.1 255.255.255.255  
#  
interface GigabitEthernet0/0/1  
    port link-type access  
#
```

4.5 Quiz

What are the functions of Virtual-if interfaces configured in the public system and virtual systems on a firewall?

Answer: A Virtual-if is a logical interface that is automatically generated during the creation of a virtual system for communication with other virtual systems. The link status and protocol status of a Virtual-if interface are always up. For communication between virtual systems, each involved Virtual-if interface must be configured with an IP address and added to a security zone in order to operate correctly.

5

Firewall Intelligent Uplink Selection

5.1 Introduction

5.1.1 About This Lab

Assume that an enterprise has a 100 M link connected to ISP1 and a 50M link connected to ISP2. The enterprise requires that traffic be forwarded to ISP1 and ISP2 links based on the bandwidth ratio to ensure full utilization of bandwidth resources. When one ISP link is overloaded, subsequent traffic will be forwarded on the other ISP link to ensure access availability.

In this lab, a global route selection policy based on link bandwidth load balancing is deployed on the firewall to meet enterprise requirements.

5.1.2 Objectives

- Understand the intelligent uplink selection mode of a firewall.
- Understand how to configure intelligent uplink selection on the firewall.

5.1.3 Networking Topology

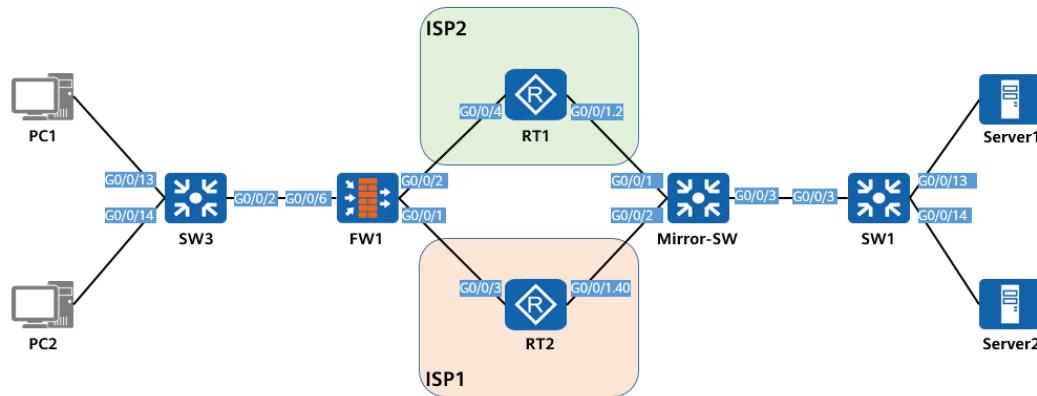


Figure 5-1 Networking topology for configuring firewall intelligent uplink selection

The preceding figure shows device connections. For details about IP address planning, see Table 5-1 in 5.1.4 Lab Planning.

FW1, as the egress gateway of the enterprise, connects to the ISP through dual links. RT1 and RT2 are used to simulate the Internet. The configurations of SW3, RT1, RT2, Mirror-

SW, and SW1 are not described in the configuration procedure. For details, see section 5.4 Configuration Reference.

5.1.4 Lab Planning

Table 5-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
FW1	G0/0/1	Layer 3 interface	100.5.1.2/30 Security zone: Untrust	Interface for connecting to the outbound interface of ISP1 and RT2
	G0/0/2	Layer 3 interface	100.3.1.2/30 Security zone: Untrust	Interface for connecting to the outbound interface of ISP2 and RT1
	G0/0/6	Layer 3 interface	172.16.20.2/24 172.16.40.2/24 sub Security zone: Trust	Interface for connecting to SW3
RT1	G0/0/1.2	Layer 3 sub-interface	4.4.4.2/30 Termination VLAN 2	On the same network segment as a VLANIF 2 of SW1
	G0/0/4	Layer 3 interface	100.3.1.1/30	Interface for connecting to FW1
RT2	G0/0/1.40	Layer 3 sub-interface	3.3.3.2/30 Termination VLAN 40	On the same network segment as a VLANIF 40 of SW1
	G0/0/3	Layer 3 interface	100.5.1.1/30	Interface for connecting to FW1
SW1	VLANIF 2	Layer 3 interface	4.4.4.1/30	On the same network segment as an RT1 interface
	VLANIF 40	Layer 3 interface	3.3.3.1/30	On the same network segment as an RT2 interface
	G0/0/3	Trunk	Allow-pass VLAN: 2, 40	Interface for connecting to Mirror-SW
	G0/0/13	Access	PVID: 1000	Interface for

				connecting to Server1
	G0/0/14	Access	PVID: 2000	Interface for connecting to the Server2
	VLANIF 1000	Layer 3 interface	100.20.1.1/24	Gateway address of Server1
	VLANIF 2000	Layer 3 interface	100.40.1.1/24	Gateway address of Server2
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interconnection interface
	G0/0/2			
	G0/0/3			
SW3	G0/0/2	Access	PVID: 50	Interface for connecting to FW1
	G0/0/13			Interface for connecting to PC1
	G0/0/14			Interface for connecting to PC2
PC1	Ethernet0	NIC	172.16.20.10/24 Gateway: 172.16.20.2/24	Endpoint PC
PC2	Ethernet0	NIC	172.16.40.10/24 Gateway: 172.16.40.2/24	Endpoint PC
Server1	Ethernet0	NIC	100.20.1.2/24 Gateway: 100.20.1.1/24	Endpoint
Server2	Ethernet0	NIC	100.40.1.2/24 Gateway: 100.40.1.1/24	Endpoint

5.2 Lab Configuration

5.2.1 Configuration Roadmap

1. Configure the health check function and configure a health check for ISP1 and ISP2 respectively.

2. Configure IP addresses, security zones, gateway addresses, bandwidth, and overload protection thresholds for interfaces. Apply health check on the interfaces.
3. Configure a global route selection policy. Set the intelligent uplink selection mode to load balancing by link bandwidth and configure the outbound interfaces on the firewall connected to ISP1 and ISP2 as intelligent uplink selection member interfaces.
4. Configure a security policy and NAT policy to allow enterprise intranet users to access extranet resources.

5.2.2 Configuration Procedure on the CLI

Step 1 Set basic network parameters.

Set basic network parameters according to the table in 5.1.4 Lab Planning.

RT1, RT2, SW1, Mirror-SW, and SW3 have been preconfigured. For details, see section 5.4 Configuration Reference.

Step 2 Configure service health check.

Configure health check on FW1 and create a health check task for ISP1 and ISP2 links respectively. Assume that the destination network segment is 100.20.1.0/24 for ISP1 and is 100.40.1.0/24 for ISP2.

```
<FW1> system-view
[FW1] healthcheck enable
[FW1] healthcheck name isp1-healthcheck
[FW1-healthcheck-isp1-healthcheck] destination 100.20.1.2 interface GigabitEthernet0/0/1 protocol
icmp
[FW1-healthcheck-isp1-healthcheck] quit
[FW1] healthcheck name isp2-healthcheck
[FW1-healthcheck-isp2-healthcheck] destination 100.40.1.2 interface GigabitEthernet0/0/2 protocol
icmp
[FW1-healthcheck-isp2-healthcheck] quit
```

100.20.1.2 and 100.40.1.2 are existing device addresses on ISP1 and ISP2 networks, that is, Server1 and Server2 in the networking diagram.

Step 3 Configure interfaces.

Configure IP addresses, gateway addresses, as well as link bandwidth, and overload protection thresholds of the links where the interfaces reside. Apply the corresponding health check on the interfaces.

```
[FW1] interface GigabitEthernet0/0/1
[FW1-GigabitEthernet0/0/1] ip address 100.5.1.2 255.255.255.252
[FW1-GigabitEthernet0/0/1] gateway 100.5.1.1
[FW1-GigabitEthernet0/0/1] healthcheck isp1-healthcheck
[FW1-GigabitEthernet0/0/1] bandwidth ingress 50000 threshold 90
[FW1-GigabitEthernet0/0/1] bandwidth egress 50000 threshold 90
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface GigabitEthernet0/0/2
[FW1-GigabitEthernet0/0/2] ip address 100.3.1.2 255.255.255.252
[FW1-GigabitEthernet0/0/2] gateway 100.3.1.1
```

```
[FW1-GigabitEthernet0/0/2] healthcheck isp2-healthcheck
[FW1-GigabitEthernet0/0/2] bandwidth ingress 100000 threshold 95
[FW1-GigabitEthernet0/0/2] bandwidth ingress 100000 threshold 95
[FW1-GigabitEthernet0/0/2] quit
[FW1] interface GigabitEthernet 0/0/6
[FW1-GigabitEthernet0/0/6] ip address 172.16.20.2 255.255.255.0
[FW1-GigabitEthernet0/0/6] ip address 172.16.40.2 255.255.255.0 sub
[FW1-GigabitEthernet0/0/6] quit
```

Step 4 Configure a global route selection policy.

Configure a global route selection policy to load balance traffic by link bandwidth.

```
[FW1] multi-interface
[FW1-multi-inter] mode proportion-of-bandwidth
[FW1-multi-inter] add interface GigabitEthernet0/0/1
[FW1-multi-inter] add interface GigabitEthernet0/0/2
[FW1-multi-inter] quit
```

Step 5 Add interfaces to corresponding security zones.

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface GigabitEthernet0/0/6
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface GigabitEthernet0/0/1
[FW1-zone-untrust] add interface GigabitEthernet0/0/2
[FW1-zone-untrust] quit
```

Step 6 Configure a security policy.

Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access resources on the Internet.

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

Step 7 Configure a NAT policy.

Configure a source NAT policy on an outbound interface so that intranet users can directly use the public IP address of FW1 to access the Internet.

```
[FW1] nat-policy
[FW1-policy-nat] rule name trust-untrust
[FW1-policy-nat-rule-trust-untrust] source-zone trust
[FW1-policy-nat-rule-trust-untrust] destination-zone untrust
[FW1-policy-nat-rule-trust-untrust] action source-nat easy-ip
[FW1-policy-nat-rule-trust-untrust] quit
```

5.2.3 Configuration Procedure on the Web UI

Step 1 Set basic network parameters.

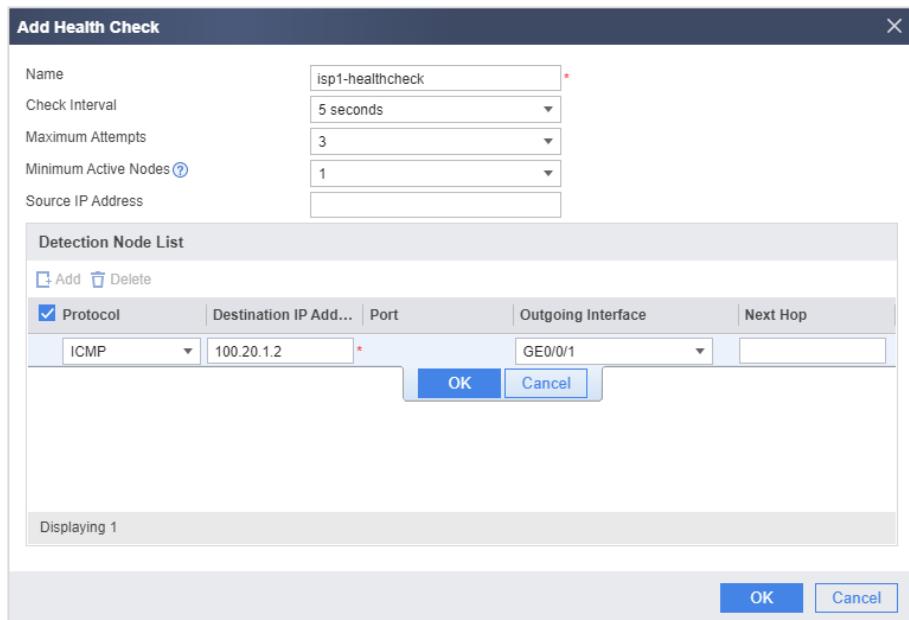
Set basic network parameters according to the table in 5.1.4 Lab Planning.

RT1, RT2, SW1, Mirror-SW, and SW3 have been preconfigured. For details, see section 5.4 Configuration Reference.

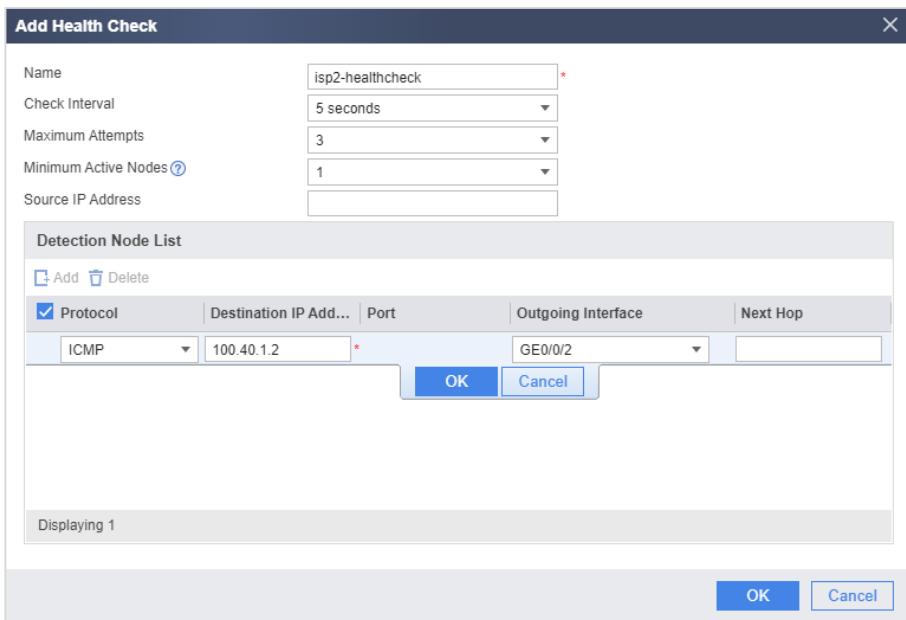
Step 2 Configure the health check.

Enable the health check function of the firewall and create a health check for ISP1 and ISP2 respectively. Assume that the destination network segment is 100.20.1.0/24 for ISP1 and is 100.40.1.0/24 for ISP2.

Choose **Object > Health Check**. Click **Add** in the **Health Check List** area to create a health check for ISP1.



Click **Add** to create a health check for ISP2.



100.20.1.2 and 100.40.1.2 are existing device addresses on ISP1 and ISP2 networks respectively.

Step 3 Set the parameters of the interface in the Untrust zone of the FW.

Set the IP addresses and gateway addresses of G0/0/1 and G0/0/2, and add them to the Untrust zone. Configure the bandwidth and overload protection thresholds of the links where the interfaces reside. Apply the corresponding health check on the interfaces.

Choose **Network > Interface** and click  next to the interface to be configured. Select or set parameters and click **OK**. Configure GigabitEthernet0/0/1 and GigabitEthernet0/0/2, as shown in the following figures.

Modify GigabitEthernet Interface

Interface Name	GigabitEthernet0/0/1	
Alias		
Virtual System	public	
Zone	untrust	
Mode	<input checked="" type="radio"/> Routing <input type="radio"/> Switching <input type="radio"/> Bypass <input type="radio"/> Interface Pair	
<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6		
Connection Type	<input checked="" type="radio"/> Static IP <input type="radio"/> DHCP <input type="radio"/> PPPoE	
IP Address	100.5.1.2/255.255.255.252	Enter each IP address on a separate line. For example: "10.10.1.2/255.255.255.0" "10.10.1.2/24".
Default Gateway	100.5.1.1	
Primary DNS Server		
Secondary DNS Server		
<input checked="" type="checkbox"/> Multi-Egress Options Carrier: Select a carrier. Default Route: <input checked="" type="checkbox"/> Sticky Load Balancing: <input type="checkbox"/> Health Check: isp1-healthcheck		
Interface Bandwidth Ingress Bandwidth: 50 Mbps <1-1000> Overload Protection Threshold: 90 % Egress Bandwidth: 50 Mbps <1-1000> Overload Protection Threshold: 90 %		
Access Management <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> Telnet <input checked="" type="checkbox"/> NETCONF <input checked="" type="checkbox"/> SNMP		
<input type="checkbox"/> Advanced		

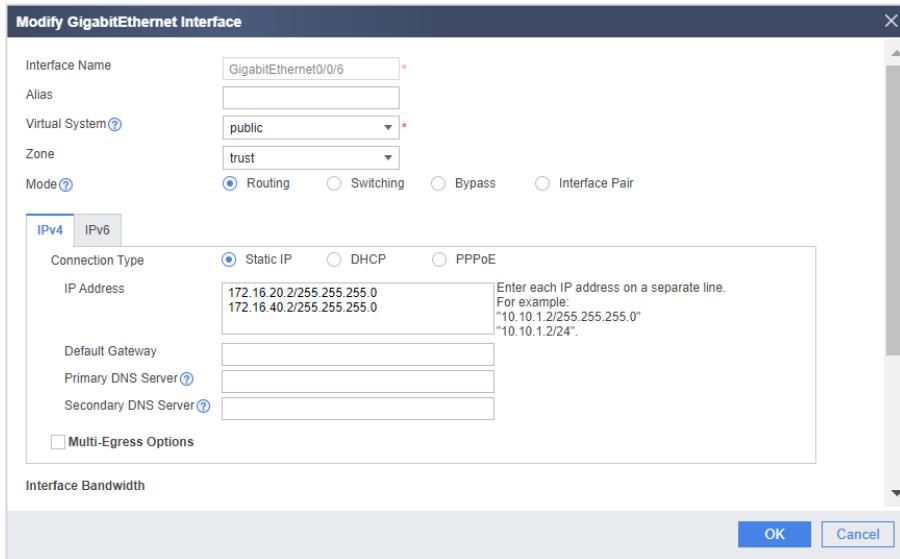
Modify GigabitEthernet Interface

Interface Name	GigabitEthernet0/0/2	
Alias		
Virtual System	public	
Zone	untrust	
Mode	<input checked="" type="radio"/> Routing <input type="radio"/> Switching <input type="radio"/> Bypass <input type="radio"/> Interface Pair	
<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6		
Connection Type	<input checked="" type="radio"/> Static IP <input type="radio"/> DHCP <input type="radio"/> PPPoE	
IP Address	100.3.1.2/255.255.255.252	Enter each IP address on a separate line. For example: "10.10.1.2/255.255.255.0" "10.10.1.2/24".
Default Gateway	100.3.1.1	
Primary DNS Server		
Secondary DNS Server		
<input checked="" type="checkbox"/> Multi-Egress Options Carrier: Select a carrier. Default Route: <input checked="" type="checkbox"/> Sticky Load Balancing: <input type="checkbox"/> Health Check: isp2-healthcheck		
Interface Bandwidth Ingress Bandwidth: 100 Mbps <1-1000> Overload Protection Threshold: 95 % Egress Bandwidth: 100 Mbps <1-1000> Overload Protection Threshold: 95 %		
Access Management <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> Telnet <input checked="" type="checkbox"/> NETCONF <input checked="" type="checkbox"/> SNMP		
<input type="checkbox"/> Advanced		

Step 4 Set the parameters of the interface in the Trust zone of the FW.

Configure the IP address for GigabitEthernet0/0/6, and add the interface to the Trust zone.

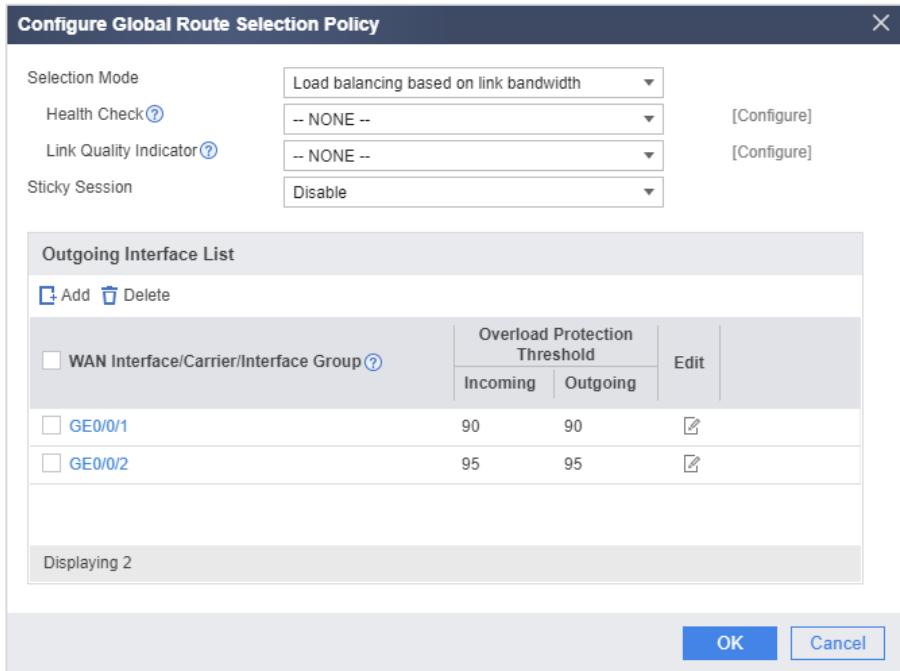
Choose **Network > Interface** and click next to the interface to be configured. Select or set parameters and click **OK** to configure GigabitEthernet0/0/6, as shown in the following figure.



Step 5 Configure a global route selection policy.

Configure a global route selection policy of the firewall, set load balancing by link bandwidth, and add GigabitEthernet0/0/1 and GigabitEthernet0/0/2 to the outbound interface list.

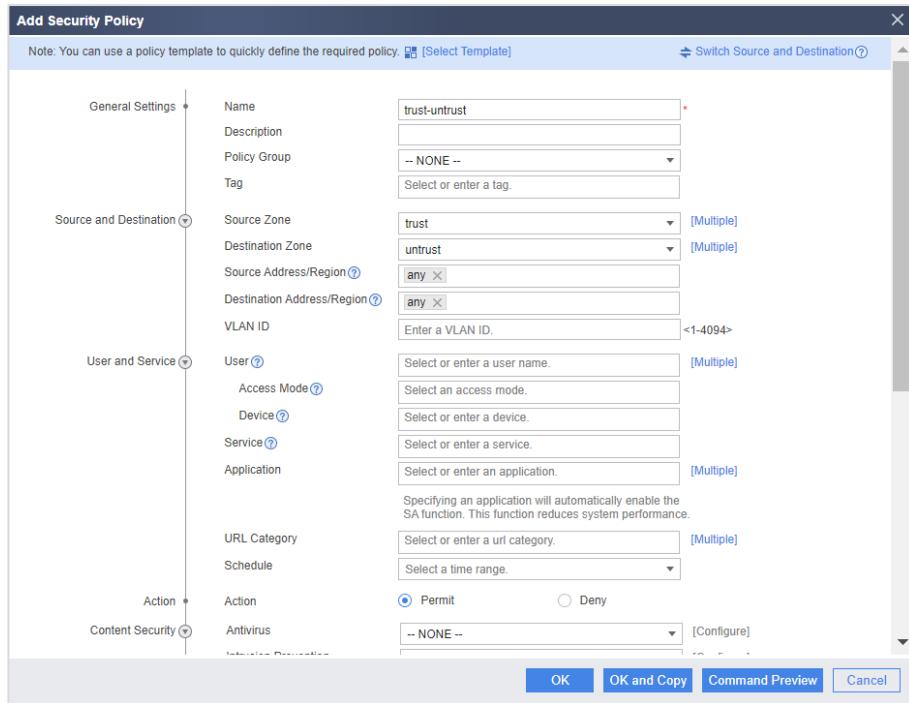
Choose **Network > Route > Intelligent Uplink Selection**. In the **Global Routing Policy** area, click **Edit**.



Step 6 Configure a security policy.

Configure a Trust-to-Untrust interzone security policy to allow enterprise intranet users to access resources on the Internet.

Choose Policy > Security Policy > Security Policy and click Add Security Policy.



Add Security Policy

Note: You can use a policy template to quickly define the required policy. [Select Template] [Switch Source and Destination](#)

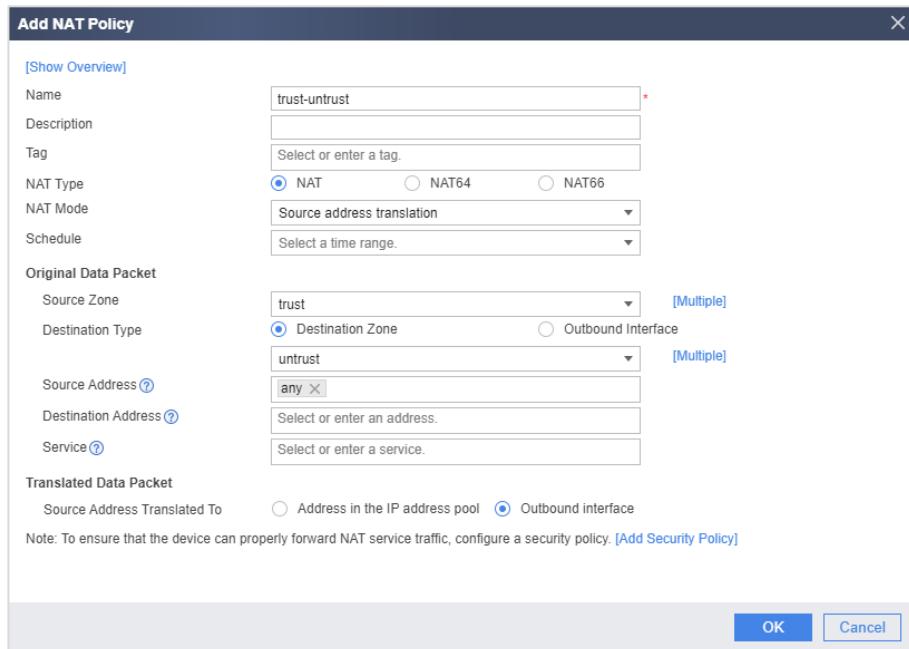
General Settings	Name	trust-untrust *
	Description	(empty)
	Policy Group	-- NONE --
	Tag	Select or enter a tag.
Source and Destination	Source Zone	trust [Multiple]
	Destination Zone	untrust [Multiple]
	Source Address/Region	any X
	Destination Address/Region	any X
	VLAN ID	Enter a VLAN ID. <1-4094>
User and Service	User	Select or enter a user name. [Multiple]
	Access Mode	Select an access mode.
	Device	Select or enter a device.
	Service	Select or enter a service.
	Application	Select or enter an application. [Multiple]
	Specifying an application will automatically enable the SA function. This function reduces system performance.	
	URL Category	Select or enter a url category. [Multiple]
	Schedule	Select a time range.
Action	Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security	Action	-- NONE -- [Configure]

Buttons: OK, OK and Copy, Command Preview, Cancel

Step 7 Configure a NAT policy.

Configure a source NAT policy on an outbound interface so that intranet users can directly use the public IP address of an interface on FW1 to access the Internet.

Choose Policy > NAT Policy > NAT Policy and click Add.



Add NAT Policy

[Show Overview]

Name	trust-untrust *
Description	(empty)
Tag	Select or enter a tag.
NAT Type	<input checked="" type="radio"/> NAT <input type="radio"/> NAT64 <input type="radio"/> NAT66
NAT Mode	Source address translation
Schedule	Select a time range.
Original Data Packet	Source Zone: trust Destination Type: Destination Zone Destination Zone: untrust [Multiple] Source Address: any X Destination Address: Select or enter an address. Service: Select or enter a service.
Translated Data Packet	Source Address Translated To: <input type="radio"/> Address in the IP address pool <input checked="" type="radio"/> Outbound interface

Note: To ensure that the device can properly forward NAT service traffic, configure a security policy. [Add Security Policy]

Buttons: OK, Cancel

5.3 Verification

After the configuration is complete, check whether health link detection can be started normally. If the status is **up**, the destination address is reachable. If the status is **down**, the destination address is unreachable.

Health Check List										
Name	Status	Source IP Addr	Destination...	Proto...	Port	Outg...	Next Hop	Delay(ms)	Jitter(ms)	Packet Loss Ratio(%)
isp2-h...	up	—	100.40.1.2	ICMP	—	GE0/0/2	—	1	0	0
isp1-h...	up	—	100.20.1.2	ICMP	—	GE0/0/1	—	0	0	0

After the global route selection policy is configured, check whether the link is available. If the current status is displayed as a green up arrow, the link is available. If the current status is displayed as a red down arrow, the link is unavailable.

Global Routing Policy			
Item	Current Status	Last 5 Minutes	
		Upstream Traffic Percentage	Downstream Traffic Percentage
Global Route Selection Mode	Load balancing based on link bandwidth	--	--
Transparent DNS Proxy	Disable[Configure]	--	--
GE0/0/1	▲	0% 50 Mbps	0% 50 Mbps
GE0/0/2	▲	0% 100 Mbps	0% 100 Mbps

5.4 Configuration Reference

5.4.1 FW1's Configuration

```

#
sysname FW1
#
healthcheck enable
healthcheck name isp2-healthcheck
    destination 100.40.1.1 interface GigabitEthernet0/0/2 protocol icmp
healthcheck name isp1-healthcheck
    destination 100.20.1.1 interface GigabitEthernet0/0/1 protocol icmp
#
interface GigabitEthernet0/0/1
    undo shutdown
    ip address 100.5.1.2 255.255.255.252
    healthcheck isp1-healthcheck
    gateway 100.5.1.1
    bandwidth ingress 50000 threshold 90
    bandwidth egress 50000 threshold 90
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 100.3.1.2 255.255.255.252
    healthcheck isp2-healthcheck
    gateway 100.3.1.1
    bandwidth ingress 100000 threshold 95
    bandwidth egress 100000 threshold 95
#
interface GigabitEthernet0/0/6

```

```
undo shutdown
ip address 172.16.20.2 255.255.255.0
ip address 172.16.40.2 255.255.255.0 sub
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/6
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
    add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
#
multi-interface
    mode proportion-of-bandwidth
    add interface GigabitEthernet0/0/1
    add interface GigabitEthernet0/0/2
#
security-policy
    rule name trust-untrust
        source-zone local
        source-zone trust
        destination-zone untrust
        action permit
#
nat-policy
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        action source-nat easy-ip
#
```

5.4.2 RT1's Pre-configuration

```
#
sysname RT1
#
interface GigabitEthernet0/0/1
    undo portswitch
#
interface GigabitEthernet0/0/1.2
    dot1q termination vid 2
    ip address 4.4.4.2 255.255.255.252
#
interface GigabitEthernet0/0/4
    undo portswitch
    ip address 100.3.1.1 255.255.255.252
#
```

```
ip route-static 100.20.1.0 255.255.255.0 4.4.4.1  
ip route-static 100.40.1.0 255.255.255.0 4.4.4.1  
#
```

5.4.3 RT2's Pre-configuration

```
#  
sysname RT2  
#  
interface GigabitEthernet0/0/1  
undo portswitch  
#  
interface GigabitEthernet0/0/1.40  
dot1q termination vid 40  
ip address 3.3.3.2 255.255.255.252  
#  
interface GigabitEthernet0/0/3  
undo portswitch  
ip address 100.5.1.1 255.255.255.252  
#  
ip route-static 100.20.1.0 255.255.255.0 3.3.3.1  
ip route-static 100.40.1.0 255.255.255.0 3.3.3.1  
#
```

5.4.4 SW1's Pre-configuration

```
#  
sysname SW1  
#  
vlan batch 2 40 1000 2000  
#  
interface vlanif2  
ip address 4.4.4.1 255.255.255.252  
#  
interface vlanif40  
ip address 3.3.3.1 255.255.255.252  
#  
interface vlanif1000  
ip address 100.20.1.1 255.255.255.0  
#  
interface vlanif2000  
ip address 100.40.1.1 255.255.255.0  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
ip route-static 100.3.1.0 255.255.255.252 4.4.4.2  
ip route-static 100.5.1.0 255.255.255.252 3.3.3.2  
#  
interface GigabitEthernet0/0/13  
port link-type access  
port default vlan 1000
```

```
#  
interface GigabitEthernet0/0/14  
port link-type access  
port default vlan 2000  
#
```

5.4.5 Mirror-SW's Pre-configuration

```
#  
sysname Mirror-SW  
#  
vlan batch 2 40  
#  
interface GigabitEthernet0/0/1  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/2  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#
```

5.4.6 SW3's Pre-configuration

```
#  
sysname SW3  
#  
vlan batch 50  
#  
interface GigabitEthernet0/0/2  
port link-type access  
port default vlan 50  
#  
interface GigabitEthernet0/0/13  
port link-type access  
port default vlan 50  
#  
interface GigabitEthernet0/0/14  
port link-type access  
port default vlan 50  
#
```

5.5 Quiz

How to implement traffic load balancing by link weight among egress links?

Reference answer: When configuring a global route selection policy, set the intelligent uplink selection mode to load balancing by link weight instead of load balancing by link



bandwidth. Configure the outbound interfaces that directly connected to ISP1 and ISP2 on the firewall as intelligent uplink selection member interfaces, and set weights for the interfaces.

6 IPsec Site-to-Multisite Application

6.1 Introduction

6.1.1 About This Lab

An enterprise network consists of the headquarters and two branches. The egress gateways are firewalls, but they are located in different geographical areas. The headquarters and branches need to communicate with each other across the Internet. To ensure data security, IPsec VPNs need to be established between the headquarters and branch 1 and branch 2 to encrypt exchanged data.

In this lab, IPsec VPNs are established between the firewalls of the headquarters and two branches to implement secure communication.

6.1.2 Objectives

- Complete basic interface configurations and route configurations.
- Complete the IPsec VPN site-to-multisite configuration.
- Configure firewall security policies of the IPsec VPN.

6.1.3 Networking Topology

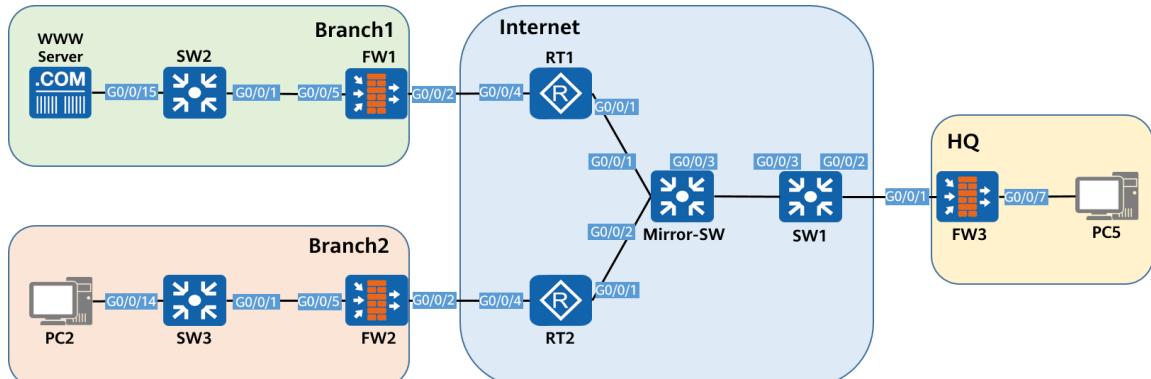


Figure 6-1 Topology for IPsec VPN site-to-multisite application

The preceding figure shows device connections. For details about IP address planning, see Table 6-1 in 6.1.4 Lab Planning.

In the scenario where IPsec VPN is established between the headquarters and multiple branches, FW1 is the egress gateway of branch 1, FW2 is the egress gateway of branch 2, and FW3 is the egress gateway of the headquarters. RT1 and RT2 are used to simulate the

Internet. SW2 and SW3 are access switches. SW1 functions as a Layer 3 switch on the Internet. The WWW server, PC2, and PC5 connect to the network as users.

Branch network planning: Uplink and downlink ports of the SW2 and SW3 are access ports, and PCs are assigned to corresponding VLANs. Configure the gateway of the WWW server on FW1 and the gateway of PC2 on FW2.

Internet zone network planning: RT1, RT2, and SW1 are at Layer 3. Static routes are used to ensure that the outbound addresses of FW1, FW2, and FW3 are reachable.

Headquarters network planning: Configure an IP address for PC5 whose gateway is on FW3. The configurations of RT1, RT2, Mirror-SW, SW1, SW2, and SW3 are not described in the configuration procedure. For details, see section 6.4 Configuration Reference.

6.1.4 Lab Planning

Table 6-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
FW1	GE0/0/2	Layer 3 interface	10.3.1.2/30 Security zone: Untrust	Interface for connecting to the outbound interface of Internet and RT1
	GE0/0/5	Layer 3 interface	172.16.30.2/24 Security zone: Trust	Interface for connecting to SW2
FW2	GE0/0/2	Layer 3 interface	10.6.1.2/30 Security zone: Untrust	Interface for connecting to the outbound interface of Internet and RT1
	GE0/0/5	Layer 3 interface	172.16.40.2/24 Security zone: Trust	Interface for connecting to SW3
FW3	GE0/0/1	Layer 3 interface	100.1.1.8/24 Security zone: Untrust	Interface for connecting to the outbound interface of Internet and SW1
	GE0/0/7	Layer 3 interface	100.100.1.1/24 Security zone: Trust	Interface for connecting to PC5
RT1	G0/0/1.2	Layer 3 sub-interface	4.4.4.2/30 Termination VLAN 2	On the same network segment as a VLANIF 2 of SW1
	G0/0/4	Layer 3 interface	10.3.1.1/30	Interface for connecting to FW1

RT2	G0/0/1.40	Layer 3 sub-interface	3.3.3.2/30 Termination VLAN40	On the same network segment as a VLANIF 40 of SW1
	G0/0/4	Layer 3 interface	10.6.1.1/30	Interface for connecting to FW2
SW1	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 1	Interface for connecting to FW3
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interface for connecting to Mirror-SW
	VLNAIF1	Layer 3 interface	100.1.1.1/24	On the same network segment as an FW3 interface
	VLNAIF2	Layer 3 interface	4.4.4.1/30	On the same network segment as an RT1 interface
	VLNAIF40	Layer 3 interface	3.3.3.1/30	On the same network segment as an RT2 interface
SW2	G0/0/1	Access	PVID: 30	Interface for connecting to FW1
	G0/0/15	Access	PVID: 30	Interface for connecting to WWW server
SW3	G0/0/1	Access	PVID: 40	Interface for connecting to FW2
	G0/0/14	Access	PVID: 40	Interface for connecting to PC2
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interconnection interface
	G0/0/2			
	G0/0/3			
WWW Server	Ethernet0	Layer 3 interface	172.16.30.10/24 Gateway: 72.16.30.2/24	Endpoint
PC2	Ethernet0	Layer 3 interface	172.16.40.10/24 Gateway: 172.16.40.2/24	Endpoint
PC5	Ethernet0	Layer 3 interface	100.100.1.10/24 Gateway:	Endpoint

			100.100.1.1/24	
--	--	--	----------------	--

6.2 Lab Configuration

6.2.1 Configuration Roadmap

1. Configure basic IP addresses for devices. For details about the IP addresses and security zones of interfaces on FW1, FW2, and FW3, see the preceding table. For details about the IP addresses and gateways of the WWW server, PC2, and PC5, see the preceding table. For details about how to configure SW1, SW2, SW3, Mirror-SW, RT1, and RT2, see 6.4 Configuration Reference.
2. Configure an Untrust-to-Local interzone security policy so that the IP addresses of the outbound interfaces on FW1, FW2, and FW3 can be pinged with each other, meeting the prerequisites for establishing an IPsec VPN.
3. Set IPsec parameters between the headquarters and branch to establish an IPsec VPN.
4. Configure a service security policy between the branch and headquarters to allow the WWW server, PC2, and PC5 to communicate with each other.

6.2.2 Configuration Procedure on the CLI

Step 1 Set basic network parameters.

Set basic network parameters according to the table in 6.1.4 Lab Planning.

RT1, RT2, SW1, SW2, SW3, and Mirror-SW are pre-configured. For details, see section 6.4 Configuration Reference.

```
# Configure IP addresses and security zones for GigabitEthernet0/0/2 and  
GigabitEthernet0/0/5 on FW1.
```

```
<FW1> system-view  
[FW1] interface GigabitEthernet 0/0/2  
[FW1-GigabitEthernet0/0/2] ip address 10.3.1.2 255.255.255.252  
[FW1-GigabitEthernet0/0/2] quit
```

```
[FW1] interface GigabitEthernet 0/0/5  
[FW1-GigabitEthernet0/0/5] ip address 172.16.30.2 255.255.255.0  
[FW1-GigabitEthernet0/0/5] quit
```

```
[FW1] firewall zone untrust  
[FW1-zone-untrust] add interface GigabitEthernet 0/0/2  
[FW1-zone-untrust] quit  
[FW1] firewall zone trust  
[FW1-zone-trust] add interface GigabitEthernet 0/0/5
```

```
[FW1-zone-trust] quit
```

```
# Configure IP addresses and security zones for GigabitEthernet0/0/2 and  
GigabitEthernet0/0/5 on FW2.
```

```
<FW2> system-view  
[FW2] interface GigabitEthernet 0/0/2  
[FW2-GigabitEthernet0/0/2] ip address 10.6.1.2 255.255.255.252  
[FW2-GigabitEthernet0/0/2] quit
```

```
[FW2] interface GigabitEthernet 0/0/5  
[FW2-GigabitEthernet0/0/5] ip address 172.16.40.2 255.255.255.0  
[FW2-GigabitEthernet0/0/5] quit
```

```
[FW2] firewall zone untrust  
[FW2-zone-untrust] add interface GigabitEthernet 0/0/2  
[FW2-zone-untrust] quit  
[FW2] firewall zone trust  
[FW2-zone-trust] add interface GigabitEthernet 0/0/5  
[FW2-zone-trust] quit
```

```
# Configure IP addresses and security zones for GigabitEthernet0/0/1 and  
GigabitEthernet0/0/7 on FW3.
```

```
<FW3> system-view  
[FW3] interface GigabitEthernet 0/0/1  
[FW3-GigabitEthernet0/0/1] ip address 100.1.1.8 255.255.255.0  
[FW3-GigabitEthernet0/0/1] quit
```

```
[FW3] interface GigabitEthernet 0/0/7  
[FW3-GigabitEthernet0/0/7] ip address 100.100.1.1 255.255.255.0  
[FW3-GigabitEthernet0/0/7] quit
```

```
[FW3] firewall zone untrust  
[FW3-zone-untrust] add interface GigabitEthernet 0/0/1  
[FW3-zone-untrust] quit  
[FW3] firewall zone trust  
[FW3-zone-trust] add interface GigabitEthernet 0/0/7  
[FW3-zone-trust] quit
```

Step 2 Configure routes on the firewall.

Configure default routes to the Internet on the FW1, FW2, and FW3.

Configure a default route to the Internet on the FW1.

```
[FW1] ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
```

Configure a default route to the Internet on the FW2.

```
[FW2] ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
```

Configure a default route to the Internet on the FW3.

```
[FW3] ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
```

Step 3 Configure security policies.

Configure interzone security policies on FW1, FW2, and FW3 to allow the traffic to be transmitted between the Local zone and the Untrust zone. In this way, the outbound interfaces of FW1, FW2, and FW3 can be pinged with each other.

Configure a security policy for the Untrust-to-Local interzone on FW1.

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

By default, the firewall interface does not allow the ping test. To facilitate the test, you can enable the ping function on the interface.

```
[FW1] interface GigabitEthernet 0/0/2  
[FW1-GigabitEthernet0/0/2] service-manage ping permit  
[FW1-GigabitEthernet0/0/2] quit
```

The configuration of the Untrust-to-Local interzone security policy on FW2 and FW3 is the same as that on FW1, and is not mentioned here.

Step 4 Configure IPsec VPN.

In this example, there are multiple branches. IPsec VPN is established on FW3 at the headquarters in template mode, and it is established on FW1 and FW2 at branches in ISAKMP mode.

Create ACL 3500 on FW1 to match the interesting traffic from FW1 at the branch to FW3 at the headquarters.

```
[FW1] acl number 3500  
[FW1-acl-adv-3500] rule permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255  
[FW1-acl-adv-3500] quit
```

Create an IPsec proposal 1 on FW1. You do not need to set default parameters.

```
[FW1] ipsec proposal 1
[FW1-ipsec-proposal-1] encapsulation-mode tunnel
[FW1-ipsec-proposal-1] esp authentication-algorithm sha2-256
[FW1-ipsec-proposal-1] esp encryption-algorithm aes-256
[FW1-ipsec-proposal-1] quit
```

Configure an IKE proposal on FW1.

```
[FW1] ike proposal 1
[FW1-ike-proposal-1] encryption-algorithm aes-256
[FW1-ike-proposal-1] dh group14
[FW1-ike-proposal-1] authentication-algorithm sha2-256
[FW1-ike-proposal-1] authentication-method pre-share
[FW1-ike-proposal-1] quit
```

Configure an IKE peer on FW1.

```
[FW1] ike peer 1
[FW1-ike-peer-1] pre-shared-key Huawei@123
[FW1-ike-peer-1] remote-address 100.1.1.8
[FW1-ike-peer-1] ike-proposal 1
[FW1-ike-peer-1] quit
```

Configure an IPsec policy.

```
[FW1] ipsec policy 1 10 isakmp
[FW1-ipsec-policy-isakmp-1-10] ike-peer 1
[FW1-ipsec-policy-isakmp-1-10] proposal 1
[FW1-ipsec-policy-isakmp-1-10] security acl 3500
[FW1-ipsec-policy-isakmp-1-10] quit
```

Invoke an IPsec policy to the outbound interface of FW1.

```
[FW1] interface GigabitEthernet 0/0/2
[FW1-GigabitEthernet0/0/2] ipsec policy 1
[FW1-GigabitEthernet0/0/2] quit
```

Create ACL 3500 on FW2 to match the interesting traffic from FW2 at the branch to FW3 at the headquarters.

```
[FW2] acl number 3500
[FW2-acl-adv-3500] rule permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
[FW2-acl-adv-3500] quit
```

Create an IPsec proposal 1 on FW2. You do not need to set default parameters.

```
[FW2] ipsec proposal 1
[FW2-ipsec-proposal-1] encapsulation-mode tunnel
[FW2-ipsec-proposal-1] esp authentication-algorithm sha2-256
[FW2-ipsec-proposal-1] esp encryption-algorithm aes-256
```

```
[FW2-ipsec-proposal-1] quit
```

Configure an IKE proposal on FW2.

```
[FW2] ike proposal 1
[FW2-ike-proposal-1] encryption-algorithm aes-256
[FW2-ike-proposal-1] dh group14
[FW2-ike-proposal-1] authentication-algorithm sha2-256
[FW2-ike-proposal-1] authentication-method pre-share
[FW2-ike-proposal-1] quit
```

Configure an IKE peer on FW2.

```
[FW2] ike peer 1
[FW2-ike-peer-1] pre-shared-key Huawei@123
[FW2-ike-peer-1] remote-address 100.1.1.8
[FW2-ike-peer-1] ike-proposal 1
[FW2-ike-peer-1] quit
```

Configure an IPsec policy.

```
[FW2] ipsec policy 1 10 isakmp
[FW2-ipsec-policy-isakmp-1-10] ike-peer 1
[FW2-ipsec-policy-isakmp-1-10] proposal 1
[FW2-ipsec-policy-isakmp-1-10] security acl 3500
[FW2-ipsec-policy-isakmp-1-10] quit
```

Invoke an IPsec policy to the outbound interface of FW2.

```
[FW2] interface GigabitEthernet 0/0/2
[FW2-GigabitEthernet0/0/2] ipsec policy 1
[FW2-GigabitEthernet0/0/2] quit
```

Create ACL 3500 on FW3 to match the interesting traffic from FW3 at the headquarters to FW1 and FW2 at the branch.

```
[FW3] acl number 3500
[FW3-acl-adv-3500] rule permit ip source 100.100.1.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
[FW3-acl-adv-3500] rule permit ip source 100.100.1.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
[FW3-acl-adv-3500] quit
```

Create an IPsec proposal 1 on FW3. You do not need to set default parameters.

```
[FW3] ipsec proposal 1
[FW3-ipsec-proposal-1] encapsulation-mode tunnel
[FW3-ipsec-proposal-1] esp authentication-algorithm sha2-256
[FW3-ipsec-proposal-1] esp encryption-algorithm aes-256
[FW3-ipsec-proposal-1] quit
```

Configure an IKE proposal on FW3.

```
[FW3] ike proposal 1
```

```
[FW3-ike-proposal-1] encryption-algorithm aes-256
[FW3-ike-proposal-1] dh group14
[FW3-ike-proposal-1] authentication-algorithm sha2-256
[FW3-ike-proposal-1] authentication-method pre-share
[FW3-ike-proposal-1] quit
```

Configure an IKE peer on FW3.

```
[FW3] ike peer 1
[FW3-ike-peer-1] pre-shared-key Huawei@123
[FW3-ike-peer-1] ike-proposal 1
[FW3-ike-peer-1] quit
```

Configure an IPsec template and invoke the interesting traffic, IPsec proposal, and IKE peer in the template.

```
[FW3] ipsec policy-template map1 10
[FW3-ipsec-policy-templet-map1-10] security acl 3500
[FW3-ipsec-policy-templet-map1-10] ike-peer 1
[FW3-ipsec-policy-templet-map1-10] proposal 1
[FW3-ipsec-policy-templet-map1-10] quit
```

Associate the IPsec policy with IPsec template map1.

```
[FW3] ipsec policy 1 10 isakmp template map1
```

Invoke an IPsec policy to the outbound interface of FW3.

```
[FW3] interface GigabitEthernet 0/0/1
[FW3-GigabitEthernet0/0/1] ipsec policy 1
[FW3-GigabitEthernet0/0/1] quit
```

Step 5 Configure service security policies.

Configure interzone security policies on FW1, FW2, and FW3 to allow PCs in the Trust zone and those in the Untrust zone to access each other. In this way, the WWW server, PC2, and PC5 can be pinged with each other.

Configure a Trust-to-Untrust interzone security policy on FW1.

```
[FW1] security-policy
[FW1-policy-security] rule name trust-untrust
[FW1-policy-security-rule-trust-untrust] source-zone trust
[FW1-policy-security-rule-trust-untrust] destination-zone untrust
[FW1-policy-security-rule-trust-untrust] source-address 172.16.30.0 mask 255.255.255.0
[FW1-policy-security-rule-trust-untrust] destination-address 100.100.1.0 mask 255.255.255.0
[FW1-policy-security-rule-trust-untrust] action permit
[FW1-policy-security-rule-trust-untrust] quit
[FW1-policy-security] quit
```

Configure an Untrust-to-Trust interzone security policy on FW1.

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

```
[FW1-policy-security] rule name untrust-trust
[FW1-policy-security-rule-untrust-trust] source-zone untrust
[FW1-policy-security-rule-untrust-trust] destination-zone trust
[FW1-policy-security-rule-untrust-trust] source-address 100.100.1.0 mask 255.255.255.0
[FW1-policy-security-rule-untrust-trust] destination-address 172.16.30.0 mask 255.255.255.0
[FW1-policy-security-rule-untrust-trust] action permit
[FW1-policy-security-rule-untrust-trust] quit
[FW1-policy-security] quit
```

Configure a Trust-to-Untrust interzone security policy on FW2.

```
[FW2] security-policy
[FW2-policy-security] rule name trust-untrust
[FW2-policy-security-rule-trust-untrust] source-zone trust
[FW2-policy-security-rule-trust-untrust] destination-zone untrust
[FW2-policy-security-rule-trust-untrust] source-address 172.16.40.0 mask 255.255.255.0
[FW2-policy-security-rule-trust-untrust] destination-address 100.100.1.0 mask 255.255.255.0
[FW2-policy-security-rule-trust-untrust] action permit
[FW2-policy-security-rule-trust-untrust] quit
[FW2-policy-security] quit
```

Configure an Untrust-to-Trust interzone security policy on FW2.

```
[FW2] security-policy
[FW2-policy-security] rule name untrust-trust
[FW2-policy-security-rule-untrust-trust] source-zone untrust
[FW2-policy-security-rule-untrust-trust] destination-zone trust
[FW2-policy-security-rule-untrust-trust] source-address 100.100.1.0 mask 255.255.255.0
[FW2-policy-security-rule-untrust-trust] destination-address 172.16.40.0 mask 255.255.255.0
[FW2-policy-security-rule-untrust-trust] action permit
[FW2-policy-security-rule-untrust-trust] quit
[FW2-policy-security] quit
```

Configure a Trust-to-Untrust interzone security policy on FW3.

```
[FW3] security-policy
[FW3-policy-security] rule name trust-untrust
[FW3-policy-security-rule-trust-untrust] source-zone trust
[FW3-policy-security-rule-trust-untrust] destination-zone untrust
[FW3-policy-security-rule-trust-untrust] source-address 100.100.1.0 mask 255.255.255.0
[FW3-policy-security-rule-trust-untrust] destination-address 172.16.40.0 mask 255.255.255.0
[FW3-policy-security-rule-trust-untrust] destination-address 172.16.30.0 mask 255.255.255.0
[FW3-policy-security-rule-trust-untrust] action permit
[FW3-policy-security-rule-trust-untrust] quit
[FW3-policy-security] quit
```

Configure an Untrust-to-Trust interzone security policy on FW3.

```
[FW3] security-policy
[FW3-policy-security] rule name untrust-trust
[FW3-policy-security-rule-untrust-trust] source-zone untrust
[FW3-policy-security-rule-untrust-trust] destination-zone trust
[FW3-policy-security-rule-untrust-trust] source-address 172.16.30.0 mask 255.255.255.0
[FW3-policy-security-rule-untrust-trust] source-address 172.16.40.0 mask 255.255.255.0
```

```
[FW3-policy-security-rule-untrust-trust] destination-address 100.100.1.0 mask 255.255.255.0
[FW3-policy-security-rule-untrust-trust] action permit
[FW3-policy-security-rule-untrust-trust] quit
[FW3-policy-security] quit
```

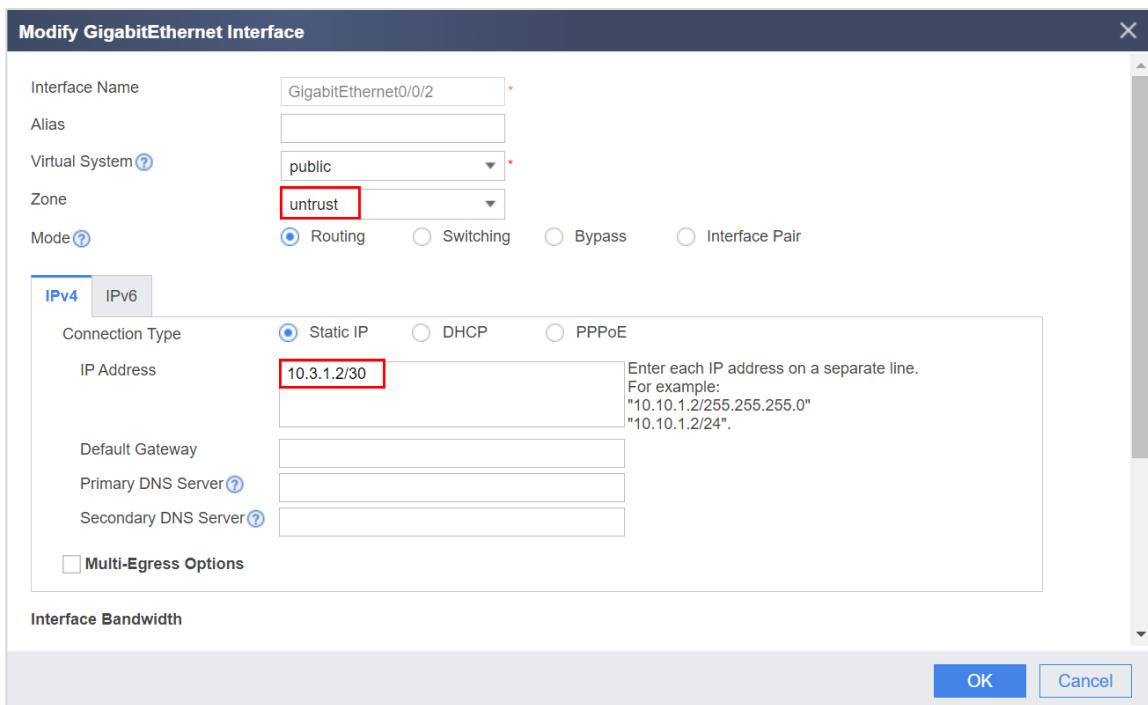
6.2.3 Configuration Procedure on the Web UI

Step 1 Set basic network parameters.

Set basic network parameters according to the table in 6.1.4 Lab Planning.

RT1, RT2, SW1, SW2, SW3, and Mirror-SW are pre-configured. For details, see section 6.4 Configuration Reference.

Configure IP addresses for interfaces on FW1, FW2, and FW3, and assign the interfaces to corresponding security zones. On the web UI of FW1, choose **Network > Interface**, and configure IP addresses and security zones for GigabitEthernet0/0/2 and GigabitEthernet0/0/5.



Modify GigabitEthernet Interface

Interface Name	GigabitEthernet0/0/5
Alias	
Virtual System	public
Zone	trust
Mode	<input checked="" type="radio"/> Routing <input type="radio"/> Switching <input type="radio"/> Bypass <input type="radio"/> Interface Pair
<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	
Connection Type	<input checked="" type="radio"/> Static IP <input type="radio"/> DHCP <input type="radio"/> PPPoE
IP Address	172.16.30.2/24
Enter each IP address on a separate line. For example: "10.10.1.2/255.255.255.0" "10.10.1.2/24".	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
<input type="checkbox"/> Multi-Egress Options	
Interface Bandwidth	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Configure GigabitEthernet0/0/2, GigabitEthernet0/0/5 on FW2 and GigabitEthernet0/0/1 and GigabitEthernet0/0/7 on FW3. For details, see the table in 6.1.4 Lab Planning.

Step 2 Configure routes on the firewall.

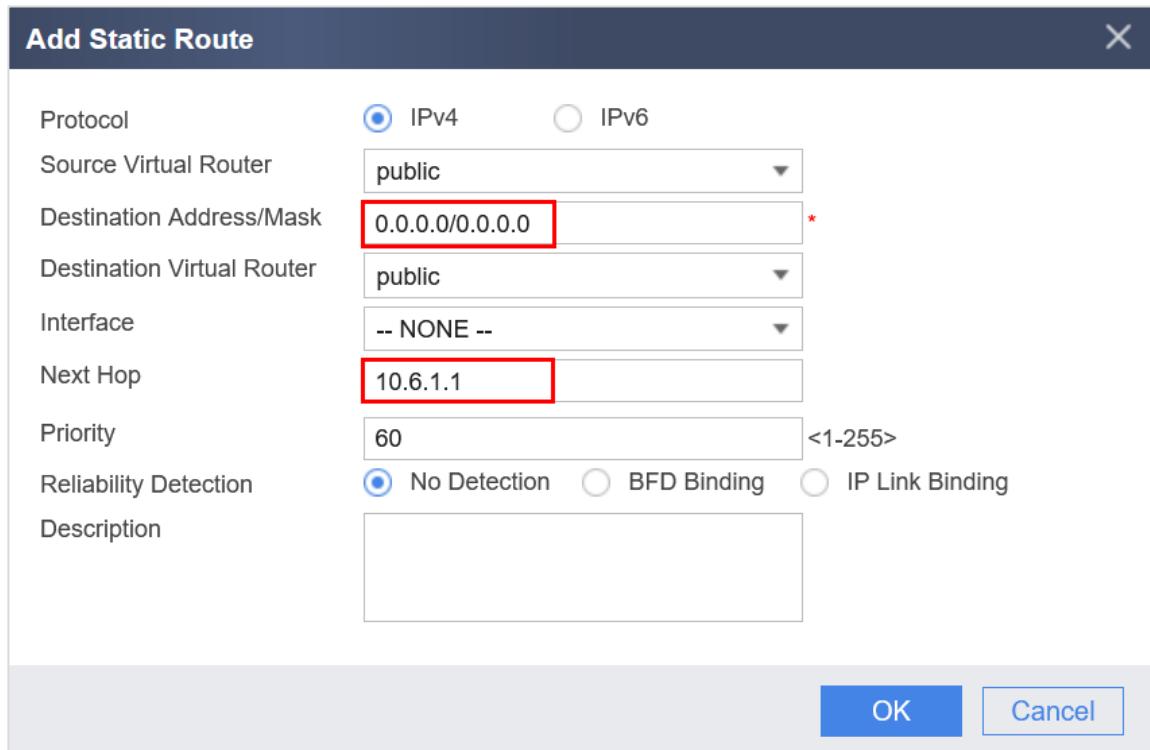
Configure default routes to the Internet on the FW1, FW2, and FW3.

On FW1, choose **Network > Route > Static Route** to create a default route to the Internet.

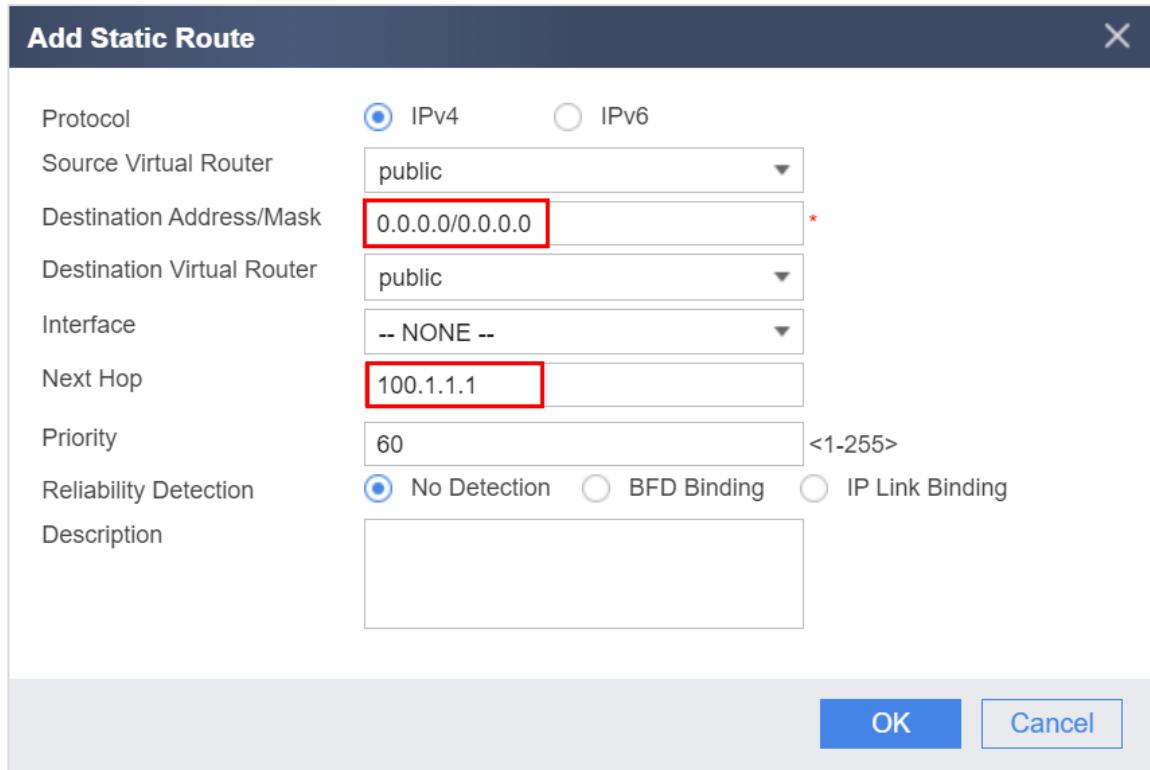
Add Static Route

Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Source Virtual Router	public
Destination Address/Mask	0.0.0.0/0.0.0.0
Destination Virtual Router	public
Interface	-- NONE --
Next Hop	10.3.1.1
Priority	60 <1-255>
Reliability Detection	<input checked="" type="radio"/> No Detection <input type="radio"/> BFD Binding <input type="radio"/> IP Link Binding
Description	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

On FW2, choose **Network > Route > Static Route** to create a default route to the Internet.



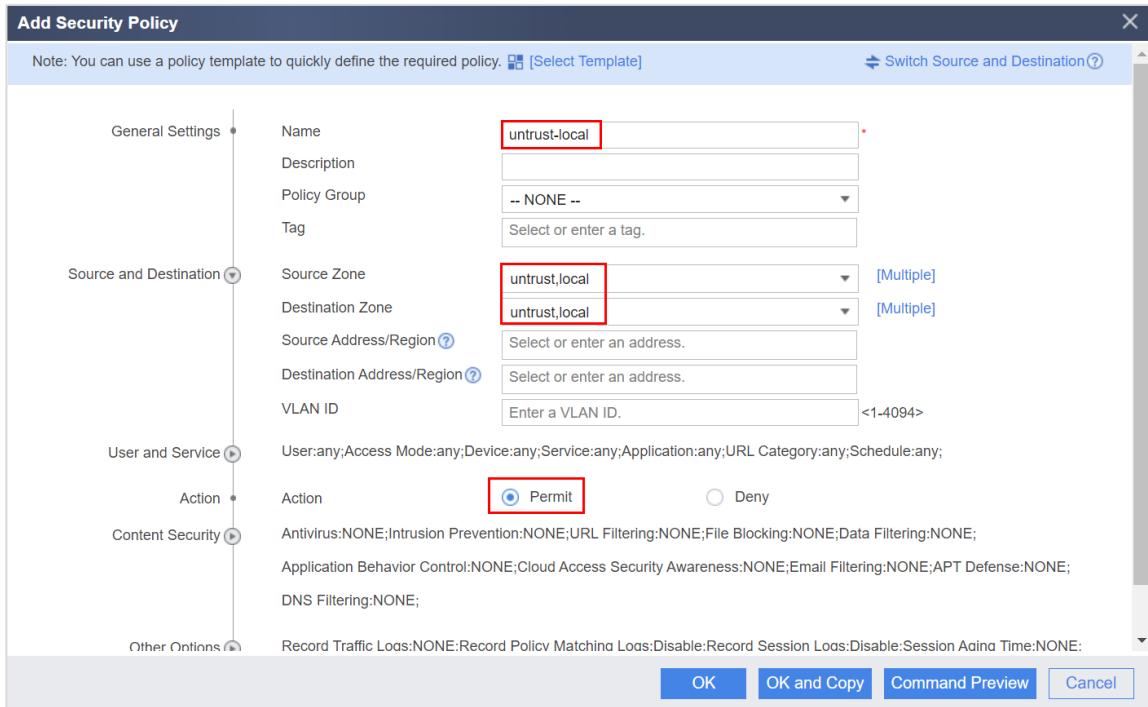
On FW3, choose **Network > Route > Static Route** to create a default route to the Internet.



Step 3 Configure security policies.

Configure interzone security policies on FW1, FW2, and FW3 to allow the traffic to be transmitted between the Local zone and the Untrust zone. In this way, the outbound interfaces of FW1, FW2, and FW3 can be pinged with each other.

On FW1, choose **Policy > Security Policy > Security Policy** and create a security policy named **untrust-local**.



The configuration of the Untrust-to-Local interzone security policy on FW2 and FW3 is the same as that on FW1, and is not mentioned here.

Step 4 Configure IPsec VPN.

In this case, there are multiple branches. IPsec VPN is established in site-to-multisite mode on FW3 at the headquarters, and in site-to-site mode on FW1 and FW2 at branches.

Choose **Network > IPSec > IPSec** on the FW1 to create an IPsec policy. Virtual systems, basic configurations, data flows to be encrypted, and security proposals have been configured.

Add IPSec Policy

Scenario Site-to-site Site-to-multipoint

 This mode is used when the peer device is a single gateway.
 The local device is a branch gateway in a star topology, or the gateway at either end of a tunnel.
 The peer device has a fixed IP address or domain name.

Option IPSec Intelligent Link Selection

Virtual System Configuration

Virtual System: public

Basic Configuration

Policy Name: 1-10

Local Interface: GE0/0/2 [Configure]

Local Address:

Peer Address: 100.1.1.8 ✓ A reachable route exists.

Note: To ensure that negotiation messages interoperate, enable the two-way security policy. [\[Add Security Policy\]](#)

Authentication Type: Pre-shared key

Pre-shared key RSA signature RSA digital envelope SM2 digital envelope

Pre-shared key:

Local ID: IP Address

Peer ID: Any

Data Flow to Encrypt

Address Type: IPv4

Source Address or Group	Destination Address or Group	Protocol	Source Port	Destin... Port	Action	Edit
172.16.30.0/24	100.100.1.1/24	any	any	any	Encrypt	

Displaying 1

Reverse Route Injection:

IKE/IPSec Proposal

Advanced

IKE Parameters

IKE Version: v1 v2 IKEv2 is used to initiate negotiations. Either IKEv1 or IKEv2 is used to accept negotiations.

Negotiation Mode: Automatic

Encryption: SM4 AES-256 AES-192 AES-128

Authentication: SM3 SHA2-512 SHA2-384 SHA2-256

Integrity Hash: SHA2-512 SHA2-384 SHA2-256 AES-128

PRF: SHA2-512 SHA2-384 SHA2-256 AES-128

DH Group: 24 21 20 19
 18 16 15 14

SA Timeout: 86400 <60-604800>seconds

IPSec Parameters

Encapsulation Mode: Automatic

Security Protocol: ESP

ESP Encryption: SM4 GCM256 GCM192 GCM128
 GMAC256 GMAC192 GMAC128 AES-256
 AES-192 AES-128

ESP Authentication: SM3 SHA2-512 SHA2-384 SHA2-256

PFS: NONE 24 21 20
 19 18 16 15

SA Timeout: By Time 3600 <30-604800>Seconds
 By Traffic 5242880 <0 , 256-200000000>KB

Dead Peer Detection (DPD)

Detection Mode: Periodic

Detection Interval: 30 <10-3600>seconds

Retry Interval: 15 <2-60>seconds

Retrans Times: 3 <3-10>Times

Buttons

Apply Return

On FW2, choose **Network > IPSec > IPSec** to create an IPsec policy. Virtual systems, basic configurations, data flows to be encrypted, and security proposals have been configured.

On FW3, choose **Network > IPSec > IPSec** to create an IPsec policy. Virtual systems, basic configurations, data flows to be encrypted, and security proposals have been configured.

Add IPSec Policy

Scenario Site-to-site Site-to-multipoint

This mode is used when the local device is a core gateway and the peer devices are multiple gateways.
 This mode is also used with L2TP over IPSec, IKEv1, and IKEv2 dial-up access.
 The peer device can be a branch gateway, PC, iOS device, Android device, or wireless base station.

Peer Type Branch Gateway L2TP over IPSec Client IKEv1 Client IKEv2 Client

Virtual System Configuration
Virtual System: public

Basic Configuration
Policy Name: map1-10
Local Interface: GE0/0/1 [Configure]
Local Address:
Peer Address:
 Note: To ensure that negotiation messages interoperate, enable the two-way security policy. [\[Add Security Policy\]](#)

Authentication Type Pre-shared key RSA signature RSA digital envelope SM2 digital envelope
Key Type Identical Different
Pre-shared key:
Local ID:
Peer ID: Any

Data Flow to Encrypt
Address Type: IPv4

Source Address or Group	Destination Address or Group	Protocol	Source Port	Destin... Port	Action	Edit
100.100.1.0/24	172.16.30.0/24	any	any	any	Encrypt	
100.100.1.0/24	172.16.40.0/24	any	any	any	Encrypt	

 Displaying 2
Reverse Route Injection:

IKE/IPSec Proposal
 Accept proposal from peer device:

Advanced

IKE Parameters
IKE Version: v1 v2
Negotiation Mode: Automatic Main Aggressive
Encryption: AES-256 AES-192 AES-128
Authentication: SHA2-256 SHA2-384 SHA2-512
Integrity Hash: SHA2-512 SHA2-384 SHA2-256
PRF: SHA2-256 SHA2-384 SHA2-512
DH Group: 24 21 20 19
DH Group: 18 16 15 14
SA Timeout: 86400 <60-604800>seconds

IPSec Parameters
Encapsulation Mode: Automatic Transport Tunnel
Security Protocol: ESP AH AH-ESP
ESP Encryption: AES-256 AES-192 AES-128
ESP Authentication: SHA2-256 SHA2-384 SHA2-512
PFS: NONE 24 21 20
 19 18 16 15
SA Timeout
 By Time: 3600 <30-604800>Seconds
 By Traffic: 524880 <0 , 256-200000000>KB

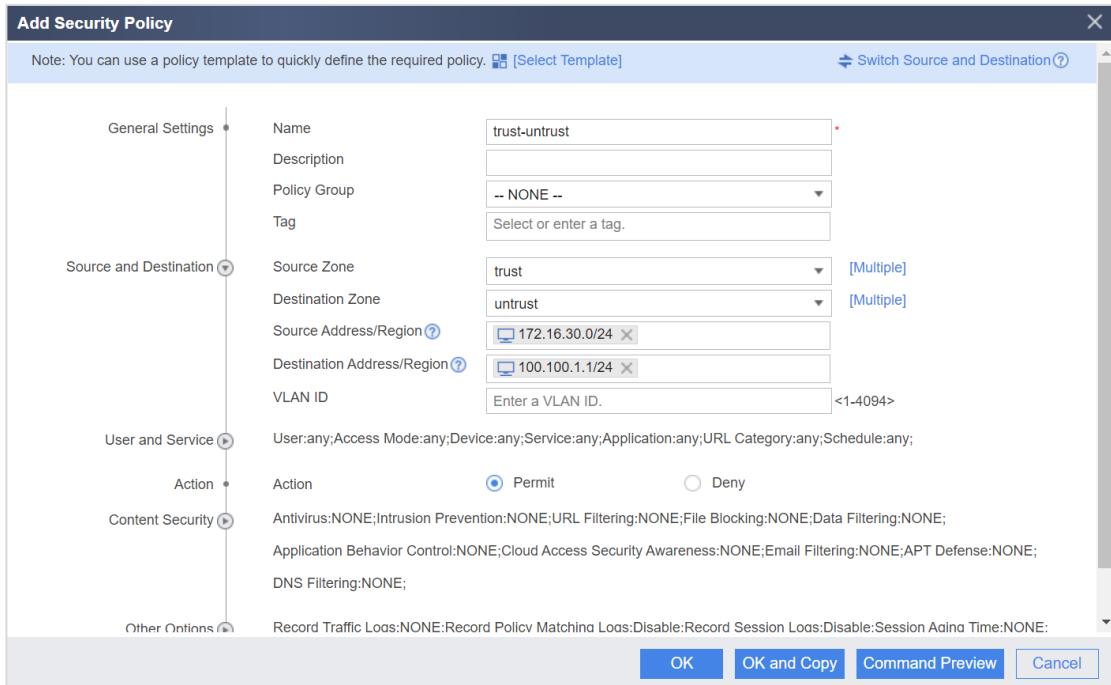
Dead Peer Detection (DPD):
Detection Mode: Periodic On-demand
Detection Interval: 30 <10-3600>seconds
Retry Interval: 15 <2-60>seconds
Retrans Times: 3 <3-10>Times

Apply **Return**

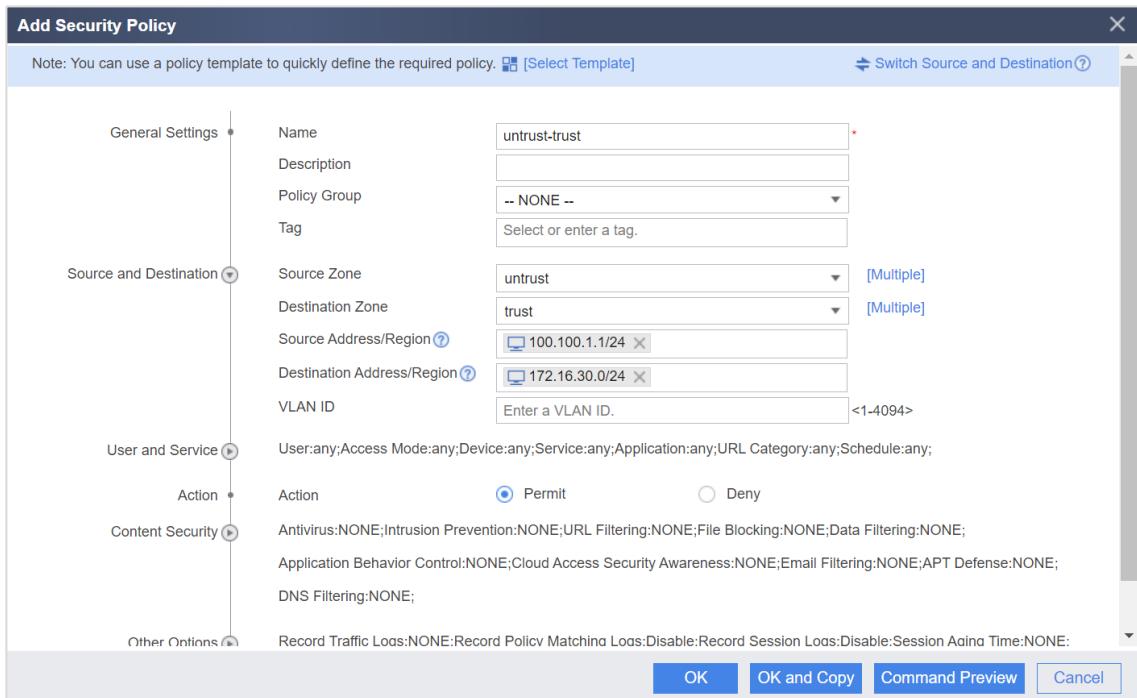
Step 5 Configure service security policies.

Configure interzone security policies on FW1, FW2, and FW3 to allow PCs in the Trust zone and those in the Untrust zone to access each other. In this way, the WWW server, PC2, and PC5 can be pinged with each other.

On FW1, choose **Policy > Security Policy > Security Policy** and create a security policy named **trust-untrust**.



On FW1, choose **Policy > Security Policy > Security Policy** and create a security policy named **untrust-trust**.



On FW2, choose **Policy > Security Policy > Security Policy** and create a security policy named **trust-untrust**.

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [Select Template] Switch Source and Destination

General Settings	Name	trust-untrust *
	Description	
	Policy Group	-- NONE --
	Tag	Select or enter a tag.
Source and Destination	Source Zone	trust [Multiple]
	Destination Zone	untrust [Multiple]
	Source Address/Region	<input type="text"/> 172.16.40.0/24
	Destination Address/Region	<input type="text"/> 100.100.1.0/24
	VLAN ID	Enter a VLAN ID. <1-4094>
User and Service	User:any;Access Mode:any;Device:any;Service:any;Application:any;URL Category:any;Schedule:any;	
Action	Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security	Antivirus:NONE;Intrusion Prevention:NONE;URL Filtering:NONE;File Blocking:NONE;Data Filtering:NONE;Application Behavior Control:NONE;Cloud Access Security Awareness:NONE;Email Filtering:NONE;APT Defense:NONE;DNS Filtering:NONE;	

OK OK and Copy Command Preview Cancel

On FW2, choose **Policy > Security Policy > Security Policy** and create a security policy named **untrust-trust**.

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [Select Template] Switch Source and Destination

General Settings	Name	untrust-trust *
	Description	
	Policy Group	-- NONE --
	Tag	Select or enter a tag.
Source and Destination	Source Zone	untrust [Multiple]
	Destination Zone	trust [Multiple]
	Source Address/Region	<input type="text"/> 100.100.1.0/24
	Destination Address/Region	<input type="text"/> 172.16.40.0/24
	VLAN ID	Enter a VLAN ID. <1-4094>
User and Service	User:any;Access Mode:any;Device:any;Service:any;Application:any;URL Category:any;Schedule:any;	
Action	Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security	Antivirus:NONE;Intrusion Prevention:NONE;URL Filtering:NONE;File Blocking:NONE;Data Filtering:NONE;Application Behavior Control:NONE;Cloud Access Security Awareness:NONE;Email Filtering:NONE;APT Defense:NONE;DNS Filtering:NONE;	

OK OK and Copy Command Preview Cancel

On FW3, choose **Policy > Security Policy > Security Policy** and create a security policy named **trust-untrust**.

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [Select Template] Switch Source and Destination?

General Settings	Name	trust-untrust *
	Description	
	Policy Group	-- NONE --
	Tag	Select or enter a tag.
Source and Destination	Source Zone	trust [Multiple]
	Destination Zone	untrust [Multiple]
	Source Address/Region?	100.100.1.0/24
	Destination Address/Region?	172.16.30.0/24 172.16.40.0/24
	VLAN ID	Enter a VLAN ID. <1-4094>
User and Service	User:any;Access Mode:any;Device:any;Service:any;Application:any;URL Category:any;Schedule:any;	
Action	Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security	Antivirus:NONE;Intrusion Prevention:NONE;URL Filtering:NONE;File Blocking:NONE;Data Filtering:NONE;Application Behavior Control:NONE;Cloud Access Security Awareness:NONE;Email Filtering:NONE;APT Defense:NONE;DNS Filtering:NONE;	
Other Options	Record Traffic Logs:NONE:Record Policy Matching Logs:Disable:Record Session Logs:Disable:Session Aging Time:NONE:	

OK OK and Copy Command Preview Cancel

On FW3, choose Policy > Security Policy > Security Policy and create a security policy named **untrust-trust**.

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [Select Template] Switch Source and Destination?

General Settings	Name	untrust-trust *
	Description	
	Policy Group	-- NONE --
	Tag	Select or enter a tag.
Source and Destination	Source Zone	untrust [Multiple]
	Destination Zone	trust [Multiple]
	Source Address/Region?	172.16.30.0/24 172.16.40.0/24
	Destination Address/Region?	100.100.1.0/24
	VLAN ID	Enter a VLAN ID. <1-4094>
User and Service	User:any;Access Mode:any;Device:any;Service:any;Application:any;URL Category:any;Schedule:any;	
Action	Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Content Security	Antivirus:NONE;Intrusion Prevention:NONE;URL Filtering:NONE;File Blocking:NONE;Data Filtering:NONE;Application Behavior Control:NONE;Cloud Access Security Awareness:NONE;Email Filtering:NONE;APT Defense:NONE;DNS Filtering:NONE;	
Other Options	Record Traffic Logs:NONE:Record Policy Matching Logs:Disable:Record Session Logs:Disable:Session Aging Time:NONE:	

OK OK and Copy Command Preview Cancel

6.3 Verification

The final result is that the IPsec VPNs between FW1 and FW3 and between FW2 and FW3 are established, and the IKE SA and IPsec SA can be queried. At the same time, the WWW server and PC5, and PC2 and PC5 can be pinged with each other.

Ping the IP address of PC5 from the WWW server. The ping operation succeeds.

```
C:\Users\Security>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 100.100.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Security>
```

Ping the IP address of PC5 from the PC2. The ping operation succeeds.

```
C:\Users\Security>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Reply from 100.100.1.10: bytes=32 time=2ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 100.100.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Security>
```

Query the IKE SA and IPsec SA on FW1.

```
<FW1> display ike sa
IKE SA information :
  Conn-ID   Peer           VPN   Flag(s)   Phase  RemoteType  RemoteID
  -----  -----
  45       100.1.1.8/500      RD|ST|A    v2:2     IP       100.1.1.8
  44       100.1.1.8/500      RD|ST|A    v2:1     IP       100.1.1.8
  Number of IKE SA : 2
  -----
```

```
<FW1> display ipsec sa
ipsec sa information:
```

```
=====
Interface: GigabitEthernet0/0/2
=====

IPSec policy name: "1"
Sequence number : 10
Acl group      : 3500/IPv4
Acl rule       : 10
Mode           : ISAKMP

Connection ID   : 45
Encapsulation mode: Tunnel
Holding time    : 0d 0h 27m 45s
Tunnel local    : 10.3.1.2/500
Tunnel remote   : 100.1.1.8/500
Flow source     : 172.16.30.0/255.255.255.0 0/0-65535
Flow destination: 100.100.1.0/255.255.255.0 0/0-65535

[Outbound ESP SAs]
SPI: 187369605 (0xb2b0885)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 17825792/1397
SA remaining hard duration (kilobytes/sec): 20971520/1936
Max sent sequence-number: 13
UDP encapsulation used for NAT traversal: N
SA encrypted packets (number/bytes): 12/720

[Inbound ESP SAs]
SPI: 187186009 (0xb283b59)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 18035507/1433
SA remaining hard duration (kilobytes/sec): 20971520/1936
Max received sequence-number: 12288
UDP encapsulation used for NAT traversal: N
SA decrypted packets (number/bytes): 12/720
Anti-replay : Enable
Anti-replay window size: 1024
```

Query the IKE SA and IPsec SA on FW2.

```
<FW2> display ike sa
IKE SA information :
Conn-ID  Peer      VPN  Flag(s)  Phase  RemoteType  RemotID
-----
8        100.1.1.8/500  RD|ST|A  v2:2      IP      100.1.1.8
7        100.1.1.8/500  RD|ST|A  v2:1      IP      100.1.1.8
Number of IKE SA : 2
```

```
<FW2> display ipsec sa
ipsec sa information:
=====
Interface: GigabitEthernet0/0/2
```

```
=====
-----
IPSec policy name: "1"
Sequence number : 1
Acl group      : 3500/IPv4
Acl rule       : 5
Mode           : ISAKMP
-----
Connection ID   : 8
Encapsulation mode: Tunnel
Holding time    : 0d 0h 39m 43s
Tunnel local    : 10.6.1.2/500
Tunnel remote   : 100.1.1.8/500
Flow source     : 172.16.40.0/255.255.255.0 0/0-65535
Flow destination : 100.100.1.0/255.255.255.0 0/0-65535
```

```
[Outbound ESP SAs]
SPI: 196970639 (0xbbd88f)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 17406360/606
SA remaining hard duration (kilobytes/sec): 20971519/1217
Max sent sequence-number: 21
UDP encapsulation used for NAT traversal: N
SA encrypted packets (number/bytes): 20/1632
```

```
[Inbound ESP SAs]
SPI: 195779478 (0xbab5b96)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 17825791/678
SA remaining hard duration (kilobytes/sec): 20971519/1217
Max received sequence-number: 12288
UDP encapsulation used for NAT traversal: N
SA decrypted packets (number/bytes): 15/1212
Anti-replay : Enable
Anti-replay window size: 1024
```

Query the IKE SA and IPsec SA on FW3.

```
<FW3> display ike sa
IKE SA information :
Conn-ID  Peer      VPN  Flag(s)  Phase  RemoteType  Remoteld
-----
49       10.6.1.2/500  RD|A    v2:2    IP      10.6.1.2
48       10.6.1.2/500  RD|A    v2:1    IP      10.6.1.2
53       10.3.1.2/500  RD|A    v2:2    IP      10.3.1.2
52       10.3.1.2/500  RD|A    v2:1    IP      10.3.1.2
Number of IKE SA : 4
```

```
<FW3> display ipsec sa
XXXX-06-15 17:31:07.250
ipsec sa information:
=====
```

Interface: GigabitEthernet0/0/1

```
=====
-----  
IPSec policy name: "1"  
Sequence number : 1  
Acl group      : 3500/IPv4  
Acl rule       : 15  
Mode           : Template  
  
-----  
Connection ID   : 53  
Tunnel index    : 2684354576  
Encapsulation mode: Tunnel  
Holding time    : 0d 0h 35m 4s  
Tunnel local    : 100.1.1.8/500  
Tunnel remote   : 10.3.1.2/500  
Flow source     : 100.100.1.0/255.255.255.0 0/0-65535  
Flow destination: 172.16.30.0/255.255.255.0 0/0-65535
```

[Outbound ESP SAs]

```
SPI: 187186009 (0xb283b59)  
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128  
SA remaining soft duration (kilobytes/sec): 4351590/885  
SA remaining hard duration (kilobytes/sec): 5242880/1496  
Max sent sequence-number: 24576  
UDP encapsulation used for NAT traversal: N  
SA encrypted packets (number/bytes): 12/720
```

[Inbound ESP SAs]

```
SPI: 187369605 (0xb2b0885)  
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128  
SA remaining soft duration (kilobytes/sec): 4666163/1101  
SA remaining hard duration (kilobytes/sec): 5242880/1496  
Max received sequence-number: 1  
UDP encapsulation used for NAT traversal: N  
SA decrypted packets (number/bytes): 12/720  
Anti-replay : Enable  
Anti-replay window size: 1024
```

```
=====
-----  
IPSec policy name: "1"  
Sequence number : 1  
Acl group      : 3500/IPv4  
Acl rule       : 20  
Mode           : Template
```

```
-----  
Connection ID   : 49  
Tunnel index    : 2684354574  
Encapsulation mode: Tunnel  
Holding time    : 0d 0h 45m 56s  
Tunnel local    : 100.1.1.8/500  
Tunnel remote   : 10.6.1.2/500  
Flow source     : 100.100.1.0/255.255.255.0 0/0-65535  
Flow destination: 172.16.40.0/255.255.255.0 0/0-65535
```

[Outbound ESP SAs]

```
SPI: 195779478 (0xbab5b96)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 4613733/413
SA remaining hard duration (kilobytes/sec): 5242879/844
Max sent sequence-number: 24576
UDP encapsulation used for NAT traversal: N
SA encrypted packets (number/bytes): 15/1212

[Inbound ESP SAs]
SPI: 196970639 (0xbbd888f)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 4666162/449
SA remaining hard duration (kilobytes/sec): 5242879/844
Max received sequence-number: 1
UDP encapsulation used for NAT traversal: N
SA decrypted packets (number/bytes): 20/1632
Anti-replay : Enable
Anti-replay window size: 1024
```

6.4 Configuration Reference

6.4.1 FW1's Configuration

```
#  
sysname FW1  
#  
acl number 3500  
rule 5 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255  
#  
ipsec proposal 1  
esp authentication-algorithm sha2-256  
esp encryption-algorithm aes-256  
#  
ike proposal 1  
encryption-algorithm aes-256  
dh group14  
authentication-algorithm sha2-256  
authentication-method pre-share  
integrity-algorithm hmac-sha2-256  
prf hmac-sha2-256  
#  
ike peer 1  
pre-shared-key Huawei@123  
ike-proposal 1  
remote-address 100.1.1.8  
rsa encryption-padding oaep  
rsa signature-padding pss  
local-id-preference certificate enable  
#  
ipsec policy 1 10 isakmp  
security acl 3500  
ike-peer 1
```

```
proposal 1
tunnel local applied-interface
sa trigger-mode auto
#
interface GigabitEthernet0/0/2
undo shutdown
ip address 10.3.1.2 255.255.255.252
service-manage ping permit
ipsec policy 1
#
interface GigabitEthernet0/0/5
undo shutdown
ip address 172.16.30.2 255.255.255.0
service-manage http permit
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
add interface MEth0/0/0
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/2
#
firewall zone dmz
set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
#
security-policy
rule name untrust-local
source-zone untrust
source-zone local
destination-zone untrust
destination-zone local
action permit
rule name trust-untrust
source-zone trust
destination-zone untrust
source-address 172.16.30.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
action permit
rule name untrust-trust
source-zone untrust
destination-zone trust
source-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.30.0 mask 255.255.255.0
action permit
#
return
```

6.4.2 FW2's Configuration

```
#  
sysname FW2  
#  
acl number 3500  
rule 5 permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255  
#  
ipsec proposal 1  
esp authentication-algorithm sha2-256  
esp encryption-algorithm aes-256  
#  
ike proposal 1  
encryption-algorithm aes-256  
dh group14  
authentication-algorithm sha2-256  
authentication-method pre-share  
integrity-algorithm hmac-sha2-256  
prf hmac-sha2-256  
#  
ike peer 1  
pre-shared-key Huawei@123  
ike-proposal 1  
remote-address 100.100.1.1  
remote-address 100.1.1.8  
rsa encryption-padding oaep  
rsa signature-padding pss  
local-id-preference certificate enable  
ikev2 authentication sign-hash sha2-256  
#  
ipsec policy 1 10 isakmp  
security acl 3500  
ike-peer 1  
proposal 1  
#  
interface GigabitEthernet0/0/2  
undo shutdown  
ip address 10.6.1.2 255.255.255.252  
service-manage ping permit  
ipsec policy 1  
#  
interface GigabitEthernet0/0/5  
undo shutdown  
ip address 172.16.40.2 255.255.255.0  
service-manage ping permit  
#  
firewall zone local  
set priority 100  
#  
firewall zone trust  
set priority 85  
add interface GigabitEthernet0/0/5  
add interface MEth0/0/0  
#  
firewall zone untrust
```

```
set priority 5
add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
#
security-policy
    rule name untrust-local
        source-zone untrust
        source-zone local
        destination-zone untrust
        destination-zone local
        action permit
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 172.16.40.0 mask 255.255.255.0
        destination-address 100.100.1.0 mask 255.255.255.0
        action permit
    rule name untrust-trust
        source-zone untrust
        destination-zone trust
        source-address 100.100.1.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
        action permit
#
return
```

6.4.3 FW3's Configuration

```
<FW3>
sysname FW3
#
acl number 3500
    rule 5 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
    rule 10 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
#
ipsec proposal 1
    esp authentication-algorithm sha2-256
    esp encryption-algorithm aes-256
#
ike proposal 1
    encryption-algorithm aes-256
    dh group14
    authentication-algorithm sha2-256
    authentication-method pre-share
    integrity-algorithm hmac-sha2-256
    prf hmac-sha2-256
#
ike peer 1
    pre-shared-key Huawei@123
    ike-proposal 1
```

```
rsa encryption-padding oaep
rsa signature-padding pss
local-id-preference certificate enable
ikev2 authentication sign-hash sha2-256
#
ipsec policy-template map1 10
    security acl 3500
    ike-peer 1
    proposal 1
#
ipsec policy 1 10 isakmp template map1
#
interface GigabitEthernet0/0/1
    undo shutdown
    mtu 1000
    ip address 100.1.1.8 255.255.255.0
    service-manage ping permit
    ipsec policy 1
#
interface GigabitEthernet0/0/7
    undo shutdown
    ip address 100.100.1.1 255.255.255.0
    service-manage ping permit
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/0
    add interface GigabitEthernet0/0/7
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
#
firewall zone dmz
    set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
#
security-policy
    rule name untrust-local
        source-zone untrust
        source-zone local
        destination-zone untrust
        destination-zone local
        action permit
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 100.100.1.0 mask 255.255.255.0
        destination-address 172.16.30.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
        action permit
```

```
rule name untrust-trust
    source-zone untrust
    destination-zone trust
    source-address 172.16.30.0 mask 255.255.255.0
    source-address 172.16.40.0 mask 255.255.255.0
    destination-address 100.100.1.0 mask 255.255.255.0
    action permit
#
return
```

6.4.4 RT1's Pre-configuration

```
#
sysname RT1
#
interface GigabitEthernet0/0/1
    undo portswitch
#
interface GigabitEthernet0/0/1.2
    dot1q termination vid 2
    ip address 4.4.4.2 255.255.255.252
#
interface GigabitEthernet0/0/4
    undo portswitch
    ip address 10.3.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

6.4.5 RT2's Pre-configuration

```
#
sysname RT2
#
interface GigabitEthernet0/0/1
    undo portswitch
#
interface GigabitEthernet0/0/1.40
    dot1q termination vid 40
    ip address 3.3.3.2 255.255.255.252
#
interface GigabitEthernet0/0/4
    undo portswitch
    ip address 10.6.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

6.4.6 SW1's Pre-configuration

```
#  
sysname SW1  
#  
vlan batch 2 40  
#  
interface vlanif1  
ip address 100.1.1.1 255.255.255.0  
#  
interface vlanif2  
ip address 4.4.4.1 255.255.255.252  
#  
interface vlanif40  
ip address 3.3.3.1 255.255.255.252  
#  
interface GigabitEthernet0/0/2  
port link-type trunk  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
ip route-static 10.3.1.0 255.255.255.252 4.4.4.2  
ip route-static 10.6.1.0 255.255.255.252 3.3.3.2  
#  
return
```

6.4.7 Mirror-SW's Pre-configuration

```
#  
sysname Mirror-SW  
#  
vlan batch 2 40  
#  
interface GigabitEthernet0/0/1  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/2  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
Return
```

6.4.8 SW2's Pre-configuration

```
#
```

```
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
    port link-type access
    port default vlan 30
#
interface GigabitEthernet0/0/15
    port link-type access
    port default vlan 30
#
return
```

6.4.9 SW3's Pre-configuration

```
#
sysname SW3
#
vlan batch 40
#
interface GigabitEthernet0/0/1
    port link-type access
    port default vlan 40
#
interface GigabitEthernet0/0/14
    port link-type access
    port default vlan 40
#
return
```

6.5 Quiz

Can branches communicate with each other after this lab is complete?

Reference answer: In this lab, branches cannot communicate with each other through IPsec VPN.

7 IPsec VPN Troubleshooting

7.1 Introduction

7.1.1 About This Lab

A medium-or large-sized enterprise has two branches. The headquarters and branches are located in different cities, which need to communicate with each other. Data access between the headquarters and branches needs to cross the Internet. IPsec VPNs are established between the headquarters and branches 1 and 2 to encrypt exchanged data. In addition, services of branches 1 and 2 need to communicate with each other.

In this lab, a pre-configured script is used to simulate the problems that may occur during the deployment. You need to meet the requirements for secure communication between the branch and headquarters.

7.1.2 Objectives

- Learn how to configure IPsec VPN.
- Master the key points for configuring IPsec VPN in NAT scenarios.
- Master the troubleshooting methods of IPsec VPN.
- Implement the communication of enterprise branches through IPsec VPN.

7.1.3 Networking Topology

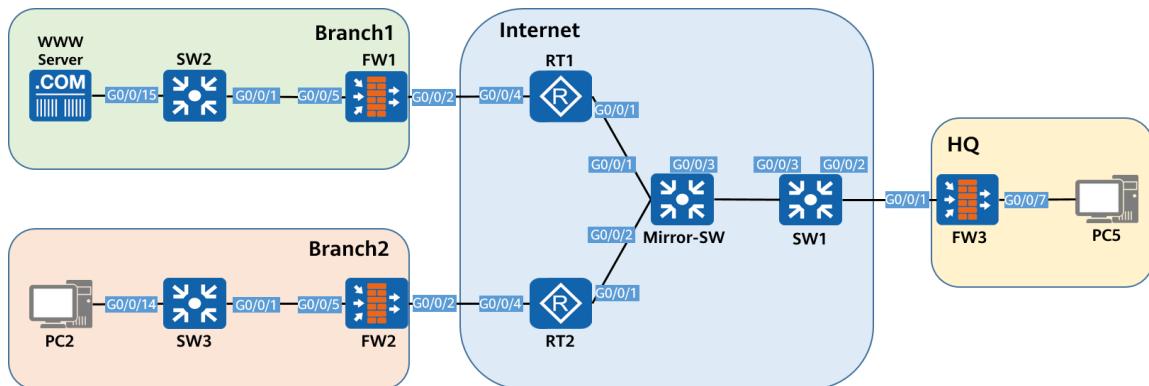


Figure 7-1 Topology for IPsec VPN troubleshooting

The preceding figure shows device connections. For details about IP address planning, see Figure 7-1 in 7.1.4 Lab Planning.

According to the scenario where IPsec VPN is established between the headquarters and multiple branches, SW2 and SW3 are access switches, SW1 functions as a Layer 3 switch on the Internet, and WWW server, PC2, and PC5 function as user access networks.

1. Branch network planning: On SW2 and SW3, the uplink and downlink interfaces are access interfaces. The gateway of the WWW server is on FW1, and the gateway of PC2 is on FW2.
2. Internet zone network planning: RT1, RT2, and SW1 are at Layer 3. Static routes are used to ensure that the outbound addresses of FW1, FW2, and FW3 are reachable.
3. Headquarters network planning: The gateway of PC5 is deployed on FW3.
4. FW1 at branch 1 needs to establish an IPsec VPN with FW3 at the headquarters. The WWW server at branch 1 needs to access the Internet.
5. FW2 at branch 2 needs to establish an IPsec VPN with FW3 at the headquarters. PCs at branch 2 are not allowed to access the Internet. PC2 at branch 2 needs to communicate with PC5 at the headquarters.
6. Branch 1 and branch 2 need to communicate with each other. For security purposes, the headquarters requires that data transmitted between branches be forwarded by the headquarters.

7.1.4 Lab Planning

Table 7-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
FW1	GE0/0/2	Layer 3 interface	10.3.1.2/30 Security zone: Untrust	Interface for connecting to the outbound interface of Internet and RT1
	GE0/0/5	Layer 3 interface	172.16.30.2/24 Security zone: Trust	Interface for connecting to SW2
FW2	GE0/0/2	Layer 3 interface	10.6.1.2/30 Security zone: Untrust	Interface for connecting to the outbound interface of Internet and RT1
	GE0/0/5	Layer 3 interface	172.16.40.2/24 Security zone: Trust	Interface for connecting to SW3
FW3	GE0/0/1	Layer 3 interface	100.1.1.8/24 Security zone: Untrust	Interface for connecting to the outbound interface of Internet and SW1
	GE0/0/7	Layer 3 interface	100.100.1.1/24 Security zone: Trust	Interface for connecting to PC5

RT1	G0/0/1.2	Layer 3 sub-interface	4.4.4.2/30 Termination VLAN 2	On the same network segment as a VLANIF 2 of SW1
	G0/0/4	Layer 3 interface	10.3.1.1/30	Interface for connecting to FW1
RT2	G0/0/1.40	Layer 3 sub-interface	3.3.3.2/30 Termination VLAN40	On the same network segment as a VLANIF 40 of SW1
	G0/0/4	Layer 3 interface	10.6.1.1/30	Interface for connecting to FW2
SW1	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 1	Interface for connecting to FW3
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interface for connecting to Mirror-SW
SW2	G0/0/1	Access	PVID: 30	Interface for connecting to FW1
	G0/0/15	Access	PVID: 30	Interface for connecting to WWW server
SW3	G0/0/1	Access	PVID: 40	Interface for connecting to FW2
	G0/0/14	Access	PVID: 40	Interface for connecting to PC2
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interconnection interface
	G0/0/2			
	G0/0/3			
WWW Server	Ethernet0	Layer 3 interface	172.16.30.10/24 Gateway: 172.16.30.2/24	Endpoint
PC2	Ethernet0	Layer 3 interface	172.16.40.10/24 Gateway: 172.16.40.2/24	Endpoint
PC5	Ethernet0	Layer 3 interface	100.100.1.10/24 Gateway: 100.100.1.1/24	Endpoint

7.2 Lab Configuration

7.2.1 Configuration Roadmap

1. Import the pre-configurations to the corresponding devices.
2. Check whether services are normal according to the 7.1.4 Lab Planning and rectify faults one by one.

7.2.2 Configuration Procedure

Step 1 Pre-configure devices.

Construct the network according to the lab topology, disable the interfaces that are not used in the lab, and import the pre-configuration scripts to the corresponding devices for device pre-configuration.

Pre-configure FW1.

```
<FW1>
sysname FW1
#
acl number 3500
    rule 5 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
#
ipsec proposal 1
    esp authentication-algorithm sha2-256
    esp encryption-algorithm aes-256
#
ike proposal 1
    encryption-algorithm aes-256
    dh group14
    authentication-algorithm sha2-256
    authentication-method pre-share
    integrity-algorithm hmac-sha2-256
    prf hmac-sha2-256
#
ike peer 1
    pre-shared-key Admin@123
    ike-proposal 1
    remote-address 100.1.1.8
    rsa encryption-padding oaep
    rsa signature-padding pss
    local-id-preference certificate enable
#
ipsec policy 1 10 isakmp
    security acl 3500
    ike-peer 1
    proposal 1
    tunnel local applied-interface
    sa trigger-mode auto
#
interface GigabitEthernet0/0/2
    undo shutdown
```

```
ip address 10.3.1.2 255.255.255.252
service-manage ping permit
ipsec policy 1
#
interface GigabitEthernet0/0/5
undo shutdown
ip address 172.16.30.2 255.255.255.0
service-manage http permit
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
add interface MEth0/0/0
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/2
#
firewall zone dmz
set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
#
security-policy
rule name untrust-local
source-zone untrust
source-zone local
destination-zone untrust
destination-zone local
action permit
rule name trust-untrust
source-zone trust
destination-zone untrust
source-address 172.16.30.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
action permit
rule name untrust-trust
source-zone untrust
destination-zone trust
source-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.30.0 mask 255.255.255.0
action permit
#
nat-policy
rule name nat
source-zone local
source-zone trust
destination-zone untrust
action source-nat easy-ip
#
return
```

Pre-configure FW2.

```
<FW2>
sysname FW2
#
acl number 3500
    rule 5 permit ip source 172.16.40.2 0.0.0.0 destination 100.100.1.0 0.0.0.255
#
ipsec proposal 1
    transform ah
        ah authentication-algorithm sha2-256
#
ike proposal 1
    encryption-algorithm aes-256
    dh group14
        authentication-algorithm sha2-256
        authentication-method pre-share
        integrity-algorithm hmac-sha2-256
        prf hmac-sha2-256
#
ike peer 1
    pre-shared-key Huawei@123
    ike-proposal 1
    remote-address 100.100.1.1
    remote-address 100.1.1.8
    rsa encryption-padding oaep
    rsa signature-padding pss
    local-id-preference certificate enable
    ikev2 authentication sign-hash sha2-256
#
ipsec policy 1 1 isakmp
    security acl 3500
    ike-peer 1
    proposal 1
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 10.6.1.2 255.255.255.252
    service-manage ping permit
    ipsec policy 1
#
interface GigabitEthernet0/0/5
    undo shutdown
    ip address 172.16.40.2 255.255.255.0
    service-manage ping permit
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/5
    add interface MEth0/0/0
#
firewall zone untrust
```

```
set priority 5
add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.6.6.1
#
security-policy
    rule name untrust-local
        source-zone untrust
        source-zone local
        destination-zone untrust
        destination-zone local
        action permit
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 172.16.40.0 mask 255.255.255.0
        destination-address 100.100.1.0 mask 255.255.255.0
        action permit
    rule name untrust-trust
        source-zone untrust
        destination-zone trust
        source-address 100.100.1.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
        action permit
#
return
```

Pre-configure FW3.

```
<FW3>
sysname FW3
#
acl number 3500
    rule 5 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
    rule 10 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
#
ipsec proposal 1
    esp authentication-algorithm sha2-256
    esp encryption-algorithm aes-256
#
ike proposal 1
    encryption-algorithm aes-256
    dh group14
    authentication-algorithm sha2-256
    authentication-method pre-share
    integrity-algorithm hmac-sha2-256
    prf hmac-sha2-256
#
ike peer 1
    pre-shared-key Huawei@123
    ike-proposal 1
    rsa encryption-padding oaep
```

```
rsa signature-padding pss
local-id-preference certificate enable
ikev2 authentication sign-hash sha2-256
#
ipsec policy-template map1 10
    security acl 3500
    ike-peer 1
    proposal 1
#
ipsec policy 1 1 isakmp template map1
#
interface GigabitEthernet0/0/1
    undo shutdown
    mtu 1000
    ip address 100.1.1.8 255.255.255.0
    service-manage ping permit
    ipsec policy 1
#
interface GigabitEthernet0/0/7
    undo shutdown
    ip address 100.100.1.1 255.255.255.0
    service-manage ping permit
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/0
    add interface GigabitEthernet0/0/7
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
#
firewall zone dmz
    set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
#
security-policy
    rule name untrust-local
        source-zone untrust
        source-zone local
        destination-zone untrust
        destination-zone local
        action permit
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 100.100.1.0 mask 255.255.255.0
        destination-address 172.16.30.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
        action permit
    rule name untrust-trust
```

```
source-zone untrust
destination-zone trust
source-address 172.16.30.0 mask 255.255.255.0
source-address 172.16.40.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
action permit
#
return
```

Pre-configure RT1.

```
<RT1>
sysname RT1
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.2
dot1q termination vid 2
ip address 4.4.4.2 255.255.255.252
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.3.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

Pre-configure RT2.

```
<RT2>
sysname RT2
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.40
dot1q termination vid 40
ip address 3.3.3.2 255.255.255.252
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.6.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

Pre-configure SW1.

```
<SW1>
sysname SW1
#
```

```
vlan batch 2 40
#
interface vlanif1
    ip address 100.1.1.1 255.255.255.0
#
interface vlanif2
    ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
    ip address 3.3.3.1 255.255.255.252
#
interface GigabitEthernet0/0/2
    port link-type trunk
#
interface GigabitEthernet0/0/3
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
ip route-static 10.3.1.0 255.255.255.252 4.4.4.2
ip route-static 10.6.1.0 255.255.255.252 3.3.3.2
#
return
```

SW2 and SW3 are used only for transmitting the traffic. Ensure that the uplink and downlink interfaces belong to the same VLAN. You can retain the default settings or refer to the configurations of SW2 and SW3 in configuration reference.

Pre-configure Mirror-SW.

```
< Mirror-SW >
sysname Mirror-SW
#
vlan 2 40
#
interface GigabitEthernet0/0/1
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
return
```

Configure the IP addresses of the NIC on the WWW server, PC2, and PC5 according to the 7.1.4 Lab Planning.

Step 2 Check the services between branch 1 and the headquarters.

The prerequisite for establishing an IPsec VPN between two firewalls is that the outbound interfaces can ping each other, and the Untrust-to-Local interzone security policy does not

block IPsec packets and port numbers. At the same time, one end triggers the establishment of SAs. Both the IKE SA and IPsec SA exist. Service can be transmitted only when the encrypted interesting traffic contains service addresses.

Verify that FW1 can ping G0/0/1 of FW3.

```
<FW1> ping 100.1.1.8
PING 100.1.1.8: 56 data bytes, press CTRL_C to break
    Reply from 100.1.1.8: bytes=56 Sequence=1 ttl=253 time=22 ms
    Reply from 100.1.1.8: bytes=56 Sequence=2 ttl=253 time=4 ms
    Reply from 100.1.1.8: bytes=56 Sequence=3 ttl=253 time=56 ms
    Reply from 100.1.1.8: bytes=56 Sequence=4 ttl=253 time=5 ms
    Reply from 100.1.1.8: bytes=56 Sequence=5 ttl=253 time=54 ms
--- 100.1.1.8 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/28/56 ms
```

Use the service address gateway on FW1 to ping the service address gateway of the headquarters.

```
<FW1> ping -a 172.16.30.2 100.100.1.1
PING 100.100.1.1: 56 data bytes, press CTRL_C to break
    Request time out
    Request time out
--- 100.100.1.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

The test result shows that service traffic fails to be transmitted.

Check whether the IKE SA and IPsec SA are established on FW1.

```
<FW1> display ike sa
```

```
<FW1> display ipsec sa
```

If no IKE SA or IPsec SA is found, the IPsec VPN fails to be established. In this case, you need to establish the IKE SA first. Check the configuration of IKE phase 1.

Display the cause of an IKE negotiation failure.

```
[FW1] display ike error-info verbose
    current info Num :17
    Ike error information:
        current ike Error-info number :17
```

```
Peer      : 100.1.1.8
Port      : 500
version   : v2
Reason    : authentication fail
Detail    : recv peer auth fail notification(pre-share-key)
Error-time : 20XX-XX-XX
```

The IKE negotiation fails because the pre-shared key authentication fails.

Check the pre-configuration of IKE phase 1 on FW1.

```
#
ike proposal 1
  encryption-algorithm aes-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ike peer 1
  pre-shared-key Admin@123
  ike-proposal 1
  remote-address 100.1.1.8
  rsa encryption-padding oaep
  rsa signature-padding pss
  local-id-preference certificate enable
#
```

Check the pre-configuration of IKE phase 1 on FW2.

```
ike proposal 1
  encryption-algorithm aes-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ike peer 1
  pre-shared-key Huawei@123
  ike-proposal 1
  remote-address 100.100.1.1
  remote-address 100.1.1.8
  rsa encryption-padding oaep
  rsa signature-padding pss
  local-id-preference certificate enable
  ikev2 authentication sign-hash sha2-256
#
```

The pre-shared keys configured on the IKE peers of FW1 and FW2 are inconsistent.

Change the IKE peer key of FW1.

```
[FW1] ike peer 1
```

```
[FW1-ike-peer-1] pre-shared-key Huawei@123  
[FW1-ike-peer-1] quit
```

Use the service address gateway on FW1 to ping the service address gateway of the headquarters again.

```
<FW1> ping -a 172.16.30.2 100.100.1.1  
PING 100.100.1.1: 56 data bytes, press CTRL_C to break  
Request time out  
--- 100.100.1.1 ping statistics ---  
5 packet(s) transmitted  
0 packet(s) received  
100.00% packet loss
```

The test result shows that service traffic fails to be transmitted.

Check the IKE SA and IPsec SA on FW1.

```
<FW1> display ike sa  
IKE SA information :  
Conn-ID    Peer          VPN   Flag(s)    Phase  RemoteType  RemoteID  
-----  
55         100.1.1.8/500  RD|ST|A    v2:2    IP        100.1.1.8  
54         100.1.1.8/500  RD|ST|A    v2:1    IP        100.1.1.8  
Number of IKE SA : 2
```

```
<FW1> display ipsec sa  
ipsec sa information:  
=====  
Interface: GigabitEthernet0/0/2  
=====  
-----  
IPSec policy name: "1"  
Sequence number : 10  
Acl group      : 3500/IPv4  
Acl rule       : 10  
Mode           : ISAKMP  
-----  
Connection ID   : 45  
Encapsulation mode: Tunnel  
Holding time    : 0d 0h 0m 45s  
Tunnel local    : 10.3.1.2/500  
Tunnel remote   : 100.1.1.8/500  
Flow source     : 172.16.30.0/255.255.255.0 0/0-65535  
Flow destination : 100.100.1.0/255.255.255.0 0/0-65535
```

[Outbound ESP SAs]

```
SPI: 187369605 (0xb2b0885)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 17825792/1397
SA remaining hard duration (kilobytes/sec): 20971520/1936
Max sent sequence-number: 13
UDP encapsulation used for NAT traversal: N
SA encrypted packets (number/bytes): 5/720

[Inbound ESP SAs]
SPI: 187186009 (0xb283b59)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 18035507/1433
SA remaining hard duration (kilobytes/sec): 20971520/1936
Max received sequence-number: 12288
UDP encapsulation used for NAT traversal: N
SA decrypted packets (number/bytes): 5/720
Anti-replay : Enable
Anti-replay window size: 1024
```

If IKE SA and IPsec SA exist but service traffic fails to be transmitted, check whether ACL 3500 matches service traffic.

```
<FW1> display acl all
Advanced ACL 3500, 1 rule ( Reference counter 1 )
Acl's step is 5
rule 10 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255 (0 times matched)
```

It is found that the number of ACL 3500 does not increase. Therefore, it can be determined that the traffic is not processed by the IPsec module. When processing packets, the firewall performs NAT first and uses the IPsec module to match the packets. Source NAT is required for branch 1 to access the Internet.

Check the NAT configuration of the firewall.

```
nat-policy
rule name nat
source-zone local
source-zone trust
destination-zone untrust
action source-nat easy-ip
```

The preceding NAT configuration indicates that the source NAT is performed when traffic is forwarded from the Local and Trust zones of FW1 to the Untrust zone. The outbound interface of the FW1's route is G0/0/2. Therefore, the source address of the traffic received by the IPsec module is 10.3.1.2, which cannot match ACL 3500.

Delete the NAT policy before modifying NAT configurations.

```
[FW1] nat-policy
[FW1-policy-nat] undo rule name nat
```

Reconfigure NAT.

```
[FW1] nat-policy
[FW1-policy-nat] rule name IPSec-deny
[FW1-policy-nat-rule-IPSec-deny] destination-address 100.100.1.0 mask 255.255.255.0
[FW1-policy-nat-rule-IPSec-deny] source-zone local
[FW1-policy-nat-rule-IPSec-deny] source-zone trust
[FW1-policy-nat-rule-IPSec-deny] destination-zone untrust
[FW1-policy-nat-rule-IPSec-deny] action no-nat
[FW1-policy-nat-rule-IPSec-deny] quit
[FW1-policy-nat] rule name nat
[FW1-policy-nat-rule-nat] source-zone local
[FW1-policy-nat-rule-nat] source-zone trust
[FW1-policy-nat-rule-nat] destination-zone untrust
[FW1-policy-nat-rule-nat] action source-nat easy-ip
[FW1-policy-nat-rule-nat] quit
[FW1-policy-nat] quit
```

The NAT policy of USG6000E V600R007 matches traffic from top to bottom. First, the traffic matches the **IPSec-deny** rule to disable NAT for the traffic destined for 100.100.1.0/24 at the headquarters, and then the traffic matches the IPsec interesting traffic. Furthermore, the firewall initiates an IKE negotiation, and uses the **nat** rule to ensure that users on FW1 can access the Internet.

Use the service address gateway on FW1 to ping the service address gateway of the headquarters again.

```
[FW1] ping -a 172.16.30.2 100.100.1.1
PING 100.100.1.1: 56  data bytes, press CTRL_C to break
Reply from 100.100.1.1: bytes=56 Sequence=1 ttl=255 time=4 ms
Reply from 100.100.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
Reply from 100.100.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
Reply from 100.100.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
Reply from 100.100.1.1: bytes=56 Sequence=5 ttl=255 time=2 ms
--- 100.100.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/4 ms
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

Use the WWW server at branch 1 to ping PC5 at the headquarters. The ping operation succeeds.

```
C:\Users\Security>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 100.100.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Security>
```

After the fault between branch 1 and the headquarters is rectified, PCs are reachable to each other.

Step 3 Check the services between branch 2 and the headquarters.

Perform the check by referring to the troubleshooting roadmap for branch 1 and headquarters in Step 2.

```
# Verify that FW2 fails to ping G0/0/1 of FW3.
```

```
<FW2> ping 100.1.1.8
PING 100.1.1.8: 56 data bytes, press CTRL_C to break
Request time out
--- 100.1.1.8 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

```
# The security policy on FW2 permits traffic from the Local zone to the Untrust zone.
```

```
security-policy
rule name untrust-local
source-zone untrust
source-zone local
destination-zone untrust
destination-zone local
action permit
```

```
# Check the routing table. The default route from FW2 to the Internet is not found.
```

```
<FW2> display ip routing-table
XXXX-06-15 21:45:11.330
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
```

Destinations : 19			Routes : 19			
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.6.1.0/30	Direct	0	0	D	10.6.1.2	GigabitEthernet0/0/2
10.6.1.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/2
10.6.1.3/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/2
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
172.16.40.0/24	Direct	0	0	D	172.16.40.2	GigabitEthernet0/0/5
172.16.40.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/5
172.16.40.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/5
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

Check the configuration of the default route.

```
<FW2> display current-configuration | include route-s
ip route-static 0.0.0.0 0.0.0.0 10.6.6.1
```

It is found that the next hop of the default route is incorrectly configured. Change the next hop to 10.6.1.1.

Perform the ping test again. FW2 can ping G0/0/1 of FW3.

```
<FW2> ping 100.1.1.8
PING 100.1.1.8: 56  data bytes, press CTRL_C to break
Reply from 100.1.1.8: bytes=56 Sequence=1 ttl=253 time=2 ms
    Reply from 100.1.1.8: bytes=56 Sequence=2 ttl=253 time=3 ms
    Reply from 100.1.1.8: bytes=56 Sequence=3 ttl=253 time=33 ms
    Reply from 100.1.1.8: bytes=56 Sequence=4 ttl=253 time=2 ms
    Reply from 100.1.1.8: bytes=56 Sequence=5 ttl=253 time=2 ms
--- 100.1.1.8 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 2/8/33 ms
```

On FW2, use the service address gateway to ping the service address gateway of the headquarters to trigger IKE negotiation.

```
<FW2> ping -a 172.16.40.2 100.100.1.1
PING 100.100.1.1: 56  data bytes, press CTRL_C to break
Request time out
--- 100.100.1.1 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

Check whether the IKE SA and IPsec SA are established on FW2.

```
<FW2> display ike sa
```

IKE SA information :

Conn-ID	Peer	VPN	Flag(s)	Phase	RemoteType	RemoteID
14	100.1.1.8/500		RD ST A	v2:1	IP	100.1.1.8
Number of IKE SA : 1						

```
<FW2> dis ipsec sa
```

The check result shows that the IKE SA negotiation is normal but the IPsec SA does not exist, which indicates that the IKE negotiation in phase 1 succeeds but the IKE negotiation in phase 2 fails. This problem is usually caused by inconsistent interconnection parameters.

Check the IPsec proposal configuration on FW2.

```
[FW2] ipsec proposal 1
[FW2-ipsec-proposal-1] display this
#
ipsec proposal 1
transform ah
ah authentication-algorithm sha2-256
#
```

It is found that the transmission mode of the IPsec proposal on FW2 is AH, but the transmission mode on FW3 is ESP. The configurations are inconsistent.

Modify IPsec proposal 1 on FW2 as follows:

```
[FW2] ipsec proposal 1
[FW2-ipsec-proposal-1] transform esp
[FW2-ipsec-proposal-1] esp authentication-algorithm sha2-256
[FW2-ipsec-proposal-1] esp encryption-algorithm aes-256
[FW2-ipsec-proposal-1] quit
```

On FW2, use the service address gateway to ping the service address gateway of the headquarters again to trigger IKE negotiation.

```
<FW2> ping -a 172.16.40.2 100.100.1.1
PING 100.100.1.1: 56 data bytes, press CTRL_C to break
Request time out
Reply from 100.100.1.1: bytes=56 Sequence=2 ttl=255 time=3 ms
Reply from 100.100.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 100.100.1.1: bytes=56 Sequence=4 ttl=255 time=2 ms
Reply from 100.100.1.1: bytes=56 Sequence=5 ttl=255 time=2 ms
--- 100.100.1.1 ping statistics ---
5 packet(s) transmitted
4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

The service IP address can be pinged, indicating that the IKE SA and IPsec SA are successfully negotiated.

Ping PC5 from PC2. The ping operation fails and service traffic fails to be transmitted.

```
C:\Users\Security>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.100.1.10:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Security>
```

The service gateway addresses on the two firewalls are reachable to each other, but service traffic fails to be transmitted. In this case, you need to check whether the gateway settings of the PC are correct. In this lab, PC's gateway is correct by default.

Check the matching count of ACL 3500.

```
<FW2> display acl all
Advanced ACL 3500, 1 rule ( Reference counter 1 )
Acl's step is 5
  rule 5 permit ip source 172.16.40.2 0.0.0.0 destination 100.100.1.0 0.0.0.255 (5 times matched)
```

The count of the ACL before and after PC2 pings PC5 is both 5, which does not increase. Check the configuration again. It is found that the source address of ACL 3500 does not contain the entire service network segment of FW2.

Modify the configuration of ACL 3500 on FW2.

```
[FW2] acl number 3500
[FW2-acl-adv-3500] rule permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
[FW2-acl-adv-3500] quit
```

Use PC2 at branch 2 to ping PC5 at the headquarters. Services are normal.

```
C:\Users\Security>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 100.100.1.10:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Security>
```

After the fault between branch 2 and the headquarters is rectified, PCs are reachable to each other.

Step 4 Check the services of branch 1 and 2.

The traffic between branches needs to be forwarded by the headquarters. The traffic is forwarded along the following path: WWW server \leftrightarrow FW1 \leftrightarrow FW3 \leftrightarrow FW2 \leftrightarrow PC2. Through data exchange, no IPsec VPN needs to be established between branches. The WWW server at branch 1 accesses PC2 at branch 2. When a packet reaches FW1 of branch 1, FW1 performs IPsec VPN encapsulation on the packet and forwards it to FW3. FW3 forwards the packet to FW2 through the IPsec VPN. The logic for PC2 to access the WWW server is the same.

Use the WWW server at branch 1 to ping PC2 at branch 2.

```
C:\Users\Security>ping 172.16.40.10

Pinging 172.16.40.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.40.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Check whether the ACL of branch 1 is matched. If so, encrypt and send the traffic to the headquarters over the IPsec VPN tunnel..

```
<FW1> display acl all
Advanced ACL 3500, 2 rules ( Reference counter 1 )
Acl's step is 5
rule 10 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255 (13 times matched)
```

Check the ACL on FW1 and find that the interesting traffic from WWW server network segment to PC2 network segment is not configured and needs to be added.

On the ACL 3500 of FW1, add the interesting traffic from WWW server network segment to PC2 network segment.

```
[FW1] acl number 3500
[FW1-acl-adv-3500] rule permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
[FW1-acl-adv-3500] quit
```

Similarly, the interesting traffic of FW2 and FW3 also need to be added.

On the ACL 3500 of FW2, add the interesting traffic from PC2 network segment to WWW server network segment.

```
[FW2] acl number 3500
[FW2-acl-adv-3500] rule permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
[FW2-acl-adv-3500] quit
```

On the ACL 3500 of FW3, add the interesting traffic from WWW server network segment to PC2 network segment and from PC2 network segment to PC1 network segment.

```
[FW3] acl number 3500
[FW3-acl-adv-3500] rule permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
[FW3-acl-adv-3500] rule permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
[FW3-acl-adv-3500] quit
```

PC2 at branch 2 cannot be pinged using the WWW server at branch 1.

```
C:\Users\Security>ping 172.16.40.10

Pinging 172.16.40.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.40.10:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Check whether the ACL of branch 1 is matched.

```
<FW1> display acl all
Advanced ACL 3500, 2 rules ( Reference counter 1 )
Acl's step is 5
rule 10 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255 (13 times matched)
rule 15 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255 (0 times matched)
```

If the traffic is not matched by the interesting traffic in IPsec VPN, source NAT may be performed on the traffic.

Check the NAT configuration on FW1.

```
#
nat-policy
rule name IPSec-deny
source-zone local
source-zone trust
destination-zone untrust
destination-address 100.100.1.0 mask 255.255.255.0
action no-nat
rule name nat
source-zone local
source-zone trust
destination-zone untrust
action source-nat easy-ip
#
```

It is found that the FW1 performs source NAT on the traffic sent from the WWW server to PC2.

Modify the NAT configuration on FW1.

```
[FW1] nat-policy
```

```
[FW1-policy-nat] rule name IPSec-deny
[FW1-policy-nat-rule-IPSec-deny] destination-address 172.16.40.0 mask 255.255.255.0
[FW1-policy-nat-rule-IPSec-deny] quit
[FW1-policy-nat] quit
```

Check the security policy configuration on FW1.

```
#  
security-policy  
rule name untrust-local  
source-zone untrust  
source-zone local  
destination-zone untrust  
destination-zone local  
action permit  
rule name trust-untrust  
source-zone trust  
destination-zone untrust  
source-address 172.16.30.0 mask 255.255.255.0  
destination-address 100.100.1.0 mask 255.255.255.0  
action permit  
rule name untrust-trust  
source-zone untrust  
destination-zone trust  
source-address 100.100.1.0 mask 255.255.255.0  
destination-address 172.16.30.0 mask 255.255.255.0  
action permit  
#
```

It is found that Untrust-to-Trust interzone security policy does not permit traffic from network segment 172.16.40.0/24.

Modify the security policy of FW1.

```
[FW1] security-policy
[FW1-policy-security] rule name trust-untrust
[FW1-policy-security-rule-trust-untrust] destination-address 172.16.40.0 mask 255.255.255.0
[FW1-policy-security-rule-trust-untrust] rule name untrust-trust
[FW1-policy-security-rule-untrust-trust] source-address 172.16.40.0 mask 255.255.255.0
[FW1-policy-security-rule-untrust-trust] quit
[FW1-policy-security] quit
```

Modify the security policy of FW2 in the same way.

```
[FW2] security-policy
[FW2-policy-security] rule name trust-untrust
[FW2-policy-security-rule-trust-untrust] destination-address 172.16.30.0 mask 255.255.255.0
[FW2-policy-security-rule-trust-untrust] rule name untrust-trust
[FW2-policy-security-rule-untrust-trust] source-address 172.16.30.0 mask 255.255.255.0
[FW2-policy-security-rule-untrust-trust] quit
[FW2-policy-security] quit
```

Use the WWW server at branch 1 to ping PC2 at branch 2.

```
C:\Users\Security>ping 172.16.40.10

Pinging 172.16.40.10 with 32 bytes of data:
Reply from 172.16.40.10: bytes=32 time=1ms TTL=125

Ping statistics for 172.16.40.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Branches can communicate with each other after the troubleshooting is complete.

7.3 Verification

After the troubleshooting is complete, the corresponding result verification is displayed at the end of the step. The final symptom is as follows:

1. An IPsec VPN is established between FW1 and FW3. The WWW server on FW1 can access the Internet, PC5 at the headquarters, and PC2 at branch 2.
2. An IPsec VPN is established between FW2 and FW3. The PC2 on FW2 can access PC5 at the headquarters and the WWW server at branch 1.
3. PC5 on FW3 can access the WWW server and PC2 at the branches.

7.4 Configuration Reference

7.4.1 FW1's Configuration

```
#  
sysname FW1  
#  
acl number 3500  
rule 10 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255  
rule 15 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255  
#  
ipsec proposal 1  
esp authentication-algorithm sha2-256  
esp encryption-algorithm aes-256  
#  
ike proposal 1  
encryption-algorithm aes-256  
dh group14  
authentication-algorithm sha2-256  
authentication-method pre-share  
integrity-algorithm hmac-sha2-256  
prf hmac-sha2-256  
#
```

```
ike peer 1
    pre-shared-key Huawei@123
    ike-proposal 1
        remote-address 100.1.1.8
        rsa encryption-padding oaep
        rsa signature-padding pss
        local-id-preference certificate enable
#
ipsec policy 1 10 isakmp
    security acl 3500
    ike-peer 1
    proposal 1
    tunnel local applied-interface
    sa trigger-mode auto
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 10.3.1.2 255.255.255.252
    service-manage ping permit
    ipsec policy 1
#
interface GigabitEthernet0/0/5
    undo shutdown
    ip address 172.16.30.2 255.255.255.0
    service-manage http permit
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/5
    add interface MEth0/0/0
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
#
security-policy
    rule name untrust-local
        source-zone untrust
        source-zone local
        destination-zone untrust
        destination-zone local
        action permit
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 172.16.30.0 mask 255.255.255.0
        destination-address 100.100.1.0 mask 255.255.255.0
```

```
destination-address 172.16.40.0 mask 255.255.255.0
action permit
rule name untrust-trust
source-zone untrust
destination-zone trust
source-address 100.100.1.0 mask 255.255.255.0
source-address 172.16.40.0 mask 255.255.255.0
destination-address 172.16.30.0 mask 255.255.255.0
action permit
#
nat-policy
rule name IPSec-deny
source-zone local
source-zone trust
destination-zone untrust
destination-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.40.0 mask 255.255.255.0
action no-nat
rule name nat
source-zone local
source-zone trust
destination-zone untrust
action source-nat easy-ip
#
return
```

7.4.2 FW2's Configuration

```
#
sysname FW2
#
acl number 3500
    rule 5 permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
    rule 5 permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
#
ipsec proposal 1
    esp authentication-algorithm sha2-256
    esp encryption-algorithm aes-256
#
ike proposal 1
    encryption-algorithm aes-256
    dh group14
    authentication-algorithm sha2-256
    authentication-method pre-share
    integrity-algorithm hmac-sha2-256
    prf hmac-sha2-256
#
ike peer 1
    pre-shared-key Huawei@123
    ike-proposal 1
    remote-address 100.100.1.1
    remote-address 100.1.1.8
    rsa encryption-padding oaep
    rsa signature-padding pss
```

```
local-id-preference certificate enable
ikev2 authentication sign-hash sha2-256
#
ipsec policy 1 1 isakmp
  security acl 3500
  ike-peer 1
  proposal 1
#
interface GigabitEthernet0/0/2
  undo shutdown
  ip address 10.6.1.2 255.255.255.252
  service-manage ping permit
  ipsec policy 1
#
interface GigabitEthernet0/0/5
  undo shutdown
  ip address 172.16.40.2 255.255.255.0
  service-manage ping permit
#
firewall zone local
  set priority 100
#
firewall zone trust
  set priority 85
  add interface GigabitEthernet0/0/5
  add interface MEth0/0/0
#
firewall zone untrust
  set priority 5
  add interface GigabitEthernet0/0/2
#
firewall zone dmz
  set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
#
security-policy
  rule name untrust-local
    source-zone untrust
    source-zone local
    destination-zone untrust
    destination-zone local
    action permit
  rule name trust-untrust
    source-zone trust
    destination-zone untrust
    source-address 172.16.40.0 mask 255.255.255.0
    destination-address 100.100.1.0 mask 255.255.255.0
    destination-address 172.16.30.0 mask 255.255.255.0
    action permit
  rule name untrust-trust
    source-zone untrust
    destination-zone trust
    source-address 100.100.1.0 mask 255.255.255.0
    source-address 172.16.30.0 mask 255.255.255.0
```

```
destination-address 172.16.40.0 mask 255.255.255.0
action permit
#
return
```

7.4.3 FW3's Configuration

```
#  
sysname FW3  
#  
acl number 3500  
rule 5 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.30.0 0.0.0.255  
rule 10 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.40.0 0.0.0.255  
rule 15 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255  
rule 20 permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255  
#  
ipsec proposal 1  
esp authentication-algorithm sha2-256  
esp encryption-algorithm aes-256  
#  
ike proposal 1  
encryption-algorithm aes-256  
dh group14  
authentication-algorithm sha2-256  
authentication-method pre-share  
integrity-algorithm hmac-sha2-256  
prf hmac-sha2-256  
#  
ike peer 1  
pre-shared-key Huawei@123  
ike-proposal 1  
rsa encryption-padding oaep  
rsa signature-padding pss  
local-id-preference certificate enable  
ikev2 authentication sign-hash sha2-256  
#  
ipsec policy-template map1 10  
security acl 3500  
ike-peer 1  
proposal 1  
#  
ipsec policy 1 1 isakmp template map1  
#  
interface GigabitEthernet0/0/1  
undo shutdown  
mtu 1000  
ip address 100.1.1.8 255.255.255.0  
service-manage ping permit  
ipsec policy 1  
#  
interface GigabitEthernet0/0/7  
undo shutdown  
ip address 100.100.1.1 255.255.255.0  
service-manage ping permit
```

```
#  
firewall zone local  
    set priority 100  
#  
firewall zone trust  
    set priority 85  
    add interface GigabitEthernet0/0/0  
    add interface GigabitEthernet0/0/7  
#  
firewall zone untrust  
    set priority 5  
    add interface GigabitEthernet0/0/1  
#  
firewall zone dmz  
    set priority 50  
#  
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1  
#  
security-policy  
    rule name untrust-local  
        source-zone untrust  
        source-zone local  
        destination-zone untrust  
        destination-zone local  
        action permit  
    rule name trust-untrust  
        source-zone trust  
        destination-zone untrust  
        source-address 100.100.1.0 mask 255.255.255.0  
        destination-address 172.16.30.0 mask 255.255.255.0  
        destination-address 172.16.40.0 mask 255.255.255.0  
        action permit  
    rule name untrust-trust  
        source-zone untrust  
        destination-zone trust  
        source-address 172.16.30.0 mask 255.255.255.0  
        source-address 172.16.40.0 mask 255.255.255.0  
        destination-address 100.100.1.0 mask 255.255.255.0  
        action permit  
#  
return
```

7.4.4 RT1's Configuration

```
#  
sysname RT1  
#  
interface GigabitEthernet0/0/1  
    undo portswitch  
#  
interface GigabitEthernet0/0/1.2  
    dot1q termination vid 2  
    ip address 4.4.4.2 255.255.255.252  
#
```

```
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.3.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

7.4.5 RT2's Configuration

```
#
sysname RT2
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.40
dot1q termination vid 40
ip address 3.3.3.2 255.255.255.252
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.6.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

7.4.6 SW1's Configuration

```
#
sysname SW1
#
vlan batch 2 40
#
interface vlanif1
ip address 100.1.1.1 255.255.255.0
#
interface vlanif2
ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
ip address 3.3.3.1 255.255.255.252
#
interface GigabitEthernet0/0/2
port link-type trunk
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 2 40
#
ip route-static 10.3.1.0 255.255.255.252 4.4.4.2
ip route-static 10.6.1.0 255.255.255.252 3.3.3.2
```

```
#  
return
```

7.4.7 Mirror-SW's Configuration

```
#  
sysname Mirror-SW  
#  
vlan 2 40  
#  
interface GigabitEthernet0/0/1  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/2  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
Return
```

7.4.8 SW2's Configuration

```
#  
sysname SW2  
#  
vlan batch 30  
#  
interface GigabitEthernet0/0/1  
port link-type access  
port default vlan 30  
#  
interface GigabitEthernet0/0/15  
port link-type access  
port default vlan 30  
#  
return
```

7.4.9 SW3's Configuration

```
#  
sysname SW3  
#  
vlan batch 40  
#  
interface GigabitEthernet0/0/1  
port link-type access  
port default vlan 40  
#
```

```
interface GigabitEthernet0/0/14
port link-type access
port default vlan 40
#
return
```

7.5 Quiz

To meet the requirements of mutual access between branches through IPsec VPN, how to configure security policies on the firewall at the headquarters?

Reference answer: The firewall at the headquarters needs to permit traffic transmitted between the Untrust zone to the Untrust zone. (By default, the traffic between the same zones of the same firewall is automatically permitted.)

8 SSL VPN Troubleshooting

8.1 Introduction

8.1.1 About This Lab

The firewall is deployed at the egress of the enterprise headquarters. Internet users access services of the enterprise headquarters in SSL VPN network extension mode.

In this lab, a pre-configured script is used to simulate the problems that may occur during the deployment. You need to meet the requirements for secure communication between Internet users and the headquarters.

8.1.2 Objectives

- Learn how to configure SSL VPN.
- Master the SSL VPN troubleshooting roadmap.
- Enable Internet users to communicate with the headquarters.

8.1.3 Networking Topology

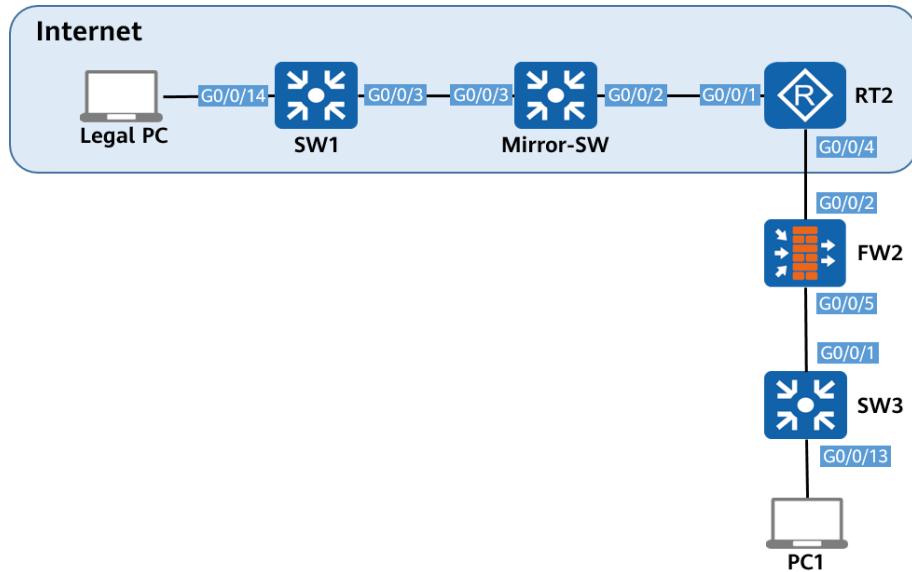


Figure 8-1 Topology for SSL VPN troubleshooting

The preceding figure shows device connections. For details about IP address planning, see Table 8-1 in 8.1.4 Lab Planning.

FW2 functions as the security device at the egress of the enterprise network. The legal PC establishes a tunnel connection with FW2 through SSL VPN network extension and accesses PC1 through SSL VPN.

Key configurations of device interfaces are described in 8.3 Configuration Reference.

8.1.4 Lab Planning

Table 8-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 40	Interface for connecting to Mirror-SW
	G0/0/14	Access	PVID: 1000	Interface for connecting to the legal PC
	VLANIF 1000	Layer 3 interface	100.20.1.1/24	Gateway of legal PC
Mirror-SW	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 40	Interconnection interface
	G0/0/3			
SW3	G0/0/1	Access	PVID: 1	Interface for connecting to FW2
	G0/0/13	Access	PVID: 1	Interface for connecting to PC1
FW2	GE0/0/2	Layer 3 interface	10.6.1.2/30	Interface for connecting to the outbound interface of Internet and RT2
	GE0/0/5	Layer 3 interface	172.16.10.1/24	Gateway of PC1
RT2	GE0/0/1.40	Layer 3 sub-interface	3.3.3.2/30 Termination VLAN 40	Interface for connecting to Mirror-SW
	GE0/0/4	Layer 3 interface	10.6.1.1/30	Interface for connecting to FW2
Legal	Ethernet0	NIC	100.20.1.2/24	Endpoint

PC			Gateway: 100.20.1.1	
PC1	Ethernet0	NIC	172.16.10.2/24 Gateway: 172.16.10.1	Endpoint

8.2 Lab Configuration

8.2.1 Configuration Roadmap

1. Import the pre-configurations to the corresponding devices.
2. Check whether services are normal according to the 8.1.4 Lab Planning and rectify faults one by one.

8.2.2 Configuration Procedure

Step 1 Pre-configure devices.

Construct the network according to the lab topology, disable the interfaces that are not used in the lab, and import the pre-configuration scripts to the corresponding devices for device pre-configuration.

Pre-configure SW1.

```
#  
sysname SW1  
#  
vlan batch 2 40 1000  
#  
interface vlanif40  
ip address 3.3.3.1 255.255.255.252  
#  
interface vlanif1000  
ip address 100.20.1.1 255.255.255.0  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2 40  
#  
interface GigabitEthernet0/0/14  
port link-type access  
port default vlan 1000  
#  
ip route-static 10.6.1.0 255.255.255.252 3.3.3.2  
#  
return
```

Pre-configure RT2.

```
#
```

```
sysname RT2
#
interface GigabitEthernet0/0/1.40
    dot1q termination vid 40
    ip address 3.3.3.2 255.255.255.252
#
interface GigabitEthernet0/0/4
    undo portswitch
    ip address 10.6.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
Return
```

Pre-configure FW2.

```
#
sysname FW2
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 10.6.1.2 255.255.255.252
    service-manage ping permit
#
interface GigabitEthernet0/0/5
    undo shutdown
    ip address 172.16.10.1 255.255.255.0
    service-manage ping permit
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/5
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/2
#
ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
#
v-gateway public ssl version tlsv12
v-gateway public ssl public-key algorithm rsa
v-gateway public ssl ciphersuit custom aes256-sha aes128-sha
v-gateway ssl-renegotiation-attack defend enable
v-gateway ssl weak-encryption enable
v-gateway gateway interface GigabitEthernet0/0/2 private
v-gateway gateway alias gateway
#
#****BEGIN***gateway**1****#
v-gateway gateway
basic
ssl version tlsv12
ssl timeout 5
```

```
ssl lifecycle 1440
ssl public-key algorithm rsa
ssl ciphersuit custom aes256-sha aes128-sha
service
    network-extension enable
    network-extension keep-alive enable
    network-extension keep-alive interval 120
    network-extension netpool 10.10.1.1 10.10.1.10 255.255.255.0
    netpool 10.10.1.1 default
    network-extension mode manual
security
    policy-default-action permit vt-src-ip
    certification cert-anonymous cert-field user-filter subject cn group-filter subject cn
    certification cert-anonymous filter-policy permit-all
    certification cert-challenge cert-field user-filter subject cn
    certification user-cert-filter key-usage any
    undo public-user enable
hostchecker
cachecleaner
vpndb
    group /default
role
    role default
    role default condition all
    role default network-extension enable
#
security-policy
    rule name untrust-local
        source-zone untrust
        destination-zone local
        destination-address 10.6.1.2 mask 255.255.255.255
        action permit
    rule name untrust-trust
        source-zone untrust
        destination-zone trust
        source-address 10.10.1.0 mask 255.255.255.0
        source-address 100.100.1.0 mask 255.255.255.0
        destination-address 172.16.1.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
        action permit
#
The following configurations are saved in the database and are not displayed in the configuration file.
user-manage user user01 domain default
password Huawei@123
parent-group /default
#
return
```

Pre-configure SW3.

```
#
sysname SW3
#
interface GigabitEthernet0/0/1
    port link-type access
```

```
#  
interface GigabitEthernet0/0/13  
port link-type access  
#  
Return
```

Pre-configure Mirror-SW.

```
#  
sysname Mirror-SW  
#  
vlan 40  
interface GigabitEthernet0/0/2  
port link-type trunk  
port trunk allow-pass vlan 2 to 4094  
##  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2 to 4094  
#  
return
```

Step 2 Check the connectivity

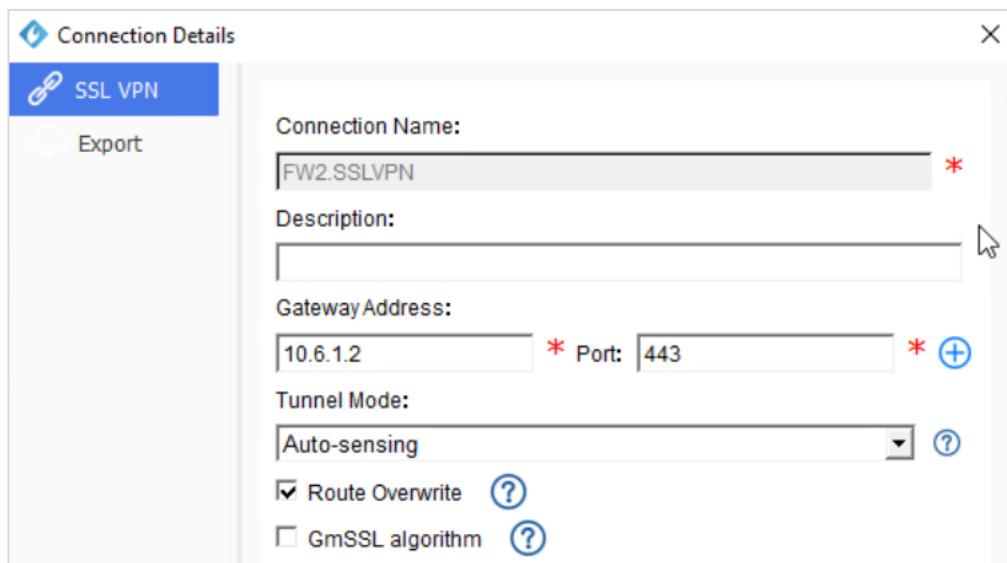
Before configuring SSL VPN, you should ensure that legal PC can communicate with the outbound interface GigabitEthernet0/0/1 of FW2 and FW2 can communicate with PC1.

On the legal PC, ping the outbound interface GigabitEthernet0/0/1 of FW2. The ping operation succeeds.

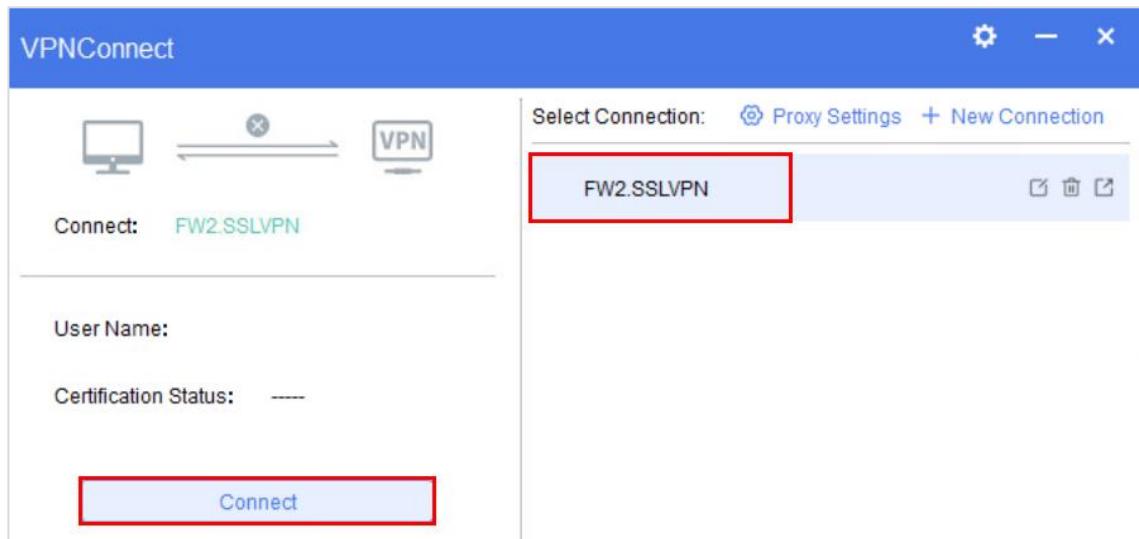
```
C:\Users\Security>ping 10.6.1.2  
  
Pinging 10.6.1.2 with 32 bytes of data:  
Reply from 10.6.1.2: bytes=32 time=1ms TTL=253  
Reply from 10.6.1.2: bytes=32 time<1ms TTL=253  
Reply from 10.6.1.2: bytes=32 time<1ms TTL=253  
Reply from 10.6.1.2: bytes=32 time<1ms TTL=253  
  
Ping statistics for 10.6.1.2:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Step 3 Test VPN dial-up on the client

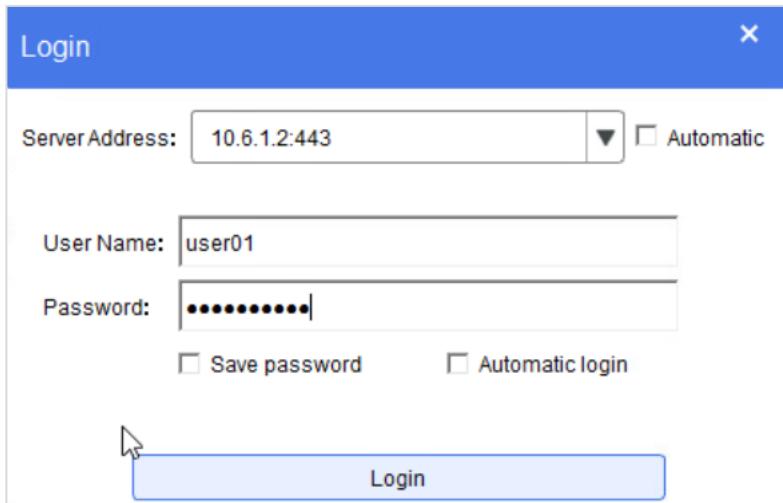
Use the UniVPN client software on the legal PC to create an SSL VPN connection.



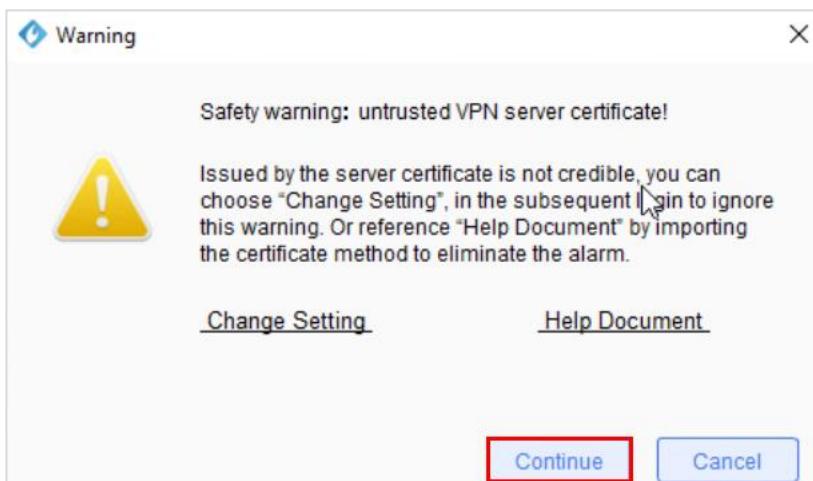
On the home page of the UniVPN client software, select the new VPN connection and click Connect.



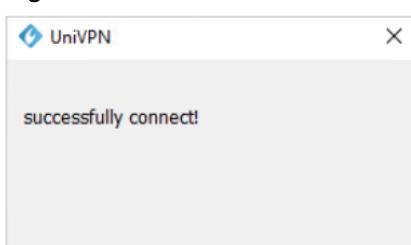
On the login page that is displayed, enter the user name user01 and password Huawei@123, and click Login.



Click Continue.



A message is displayed in the lower right corner of the computer, indicating that the login is successful.



Step 4 Test the service connectivity.

The SSL VPN in network extension mode is used. After the VPN dial-up of the legal PC is successful, check whether the CMD of the legal PC contains the route to the headquarters. Check the FW2 at the headquarters and permit the traffic from the area where the legal PC resides to the area where the internal service resides.

Check whether the IP address assigned by FW2 is obtained from the CMD of the legal PC.

```
C:\Users\Security>ipconfig

Windows IP Configuration

Unknown adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Link-local IPv6 Address . . . . . : fe80::51e2:b0c9:b33d:a77b%6
        IPv4 Address. . . . . : 10.10.1.4
        Subnet Mask . . . . . : 255.255.255.0
        Default Gateway . . . . . :
```

Check the CMD routing table of legal PC.

```
C:\Users\Security>route print
=====
Interface List
 6...00 ff de 2e c0 da ....TAP-Windows Adapter V9
 5...00 0c 29 b3 21 a1 ....Intel(R) 82574L Gigabit Network Connection
 3...00 0c 29 b3 21 b5 ....Intel(R) 82574L Gigabit Network Connection #3
 1.....Software Loopback Interface 1
 7...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 31...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 2...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0      0.0.0.0   100.20.1.1  100.20.1.3    281
          10.6.1.2  255.255.255.255  100.20.1.1  100.20.1.3    257
          10.10.1.0  255.255.255.0       On-link     10.10.1.4      1
          10.10.1.4  255.255.255.255  10.10.1.4     10.10.1.4    257
          10.10.1.255 255.255.255.255  10.10.1.4     10.10.1.4    257
          100.20.1.0  255.255.255.0       On-link    100.20.1.3    281
          100.20.1.3  255.255.255.255  100.20.1.3    100.20.1.3    281
          100.20.1.255 255.255.255.255  100.20.1.3    100.20.1.3    281
          127.0.0.0    255.0.0.0       On-link     127.0.0.1    331
          127.0.0.1    255.255.255.255  127.0.0.1     127.0.0.1    331
 127.255.255.255  255.255.255.255  127.0.0.1     127.0.0.1    331
          192.168.10.0  255.255.255.0       On-link   192.168.10.6    281
          192.168.10.6  255.255.255.255  192.168.10.6   192.168.10.6    281
 192.168.10.255  255.255.255.255  192.168.10.6   192.168.10.6    281
          224.0.0.0    240.0.0.0       On-link     127.0.0.1    331
          224.0.0.0    240.0.0.0       On-link   192.168.10.6    281
          224.0.0.0    240.0.0.0       On-link   100.20.1.3    281
          224.0.0.0    240.0.0.0       On-link     10.10.1.4    257
 255.255.255.255  255.255.255.255  127.0.0.1     127.0.0.1    331
 255.255.255.255  255.255.255.255  192.168.10.6   192.168.10.6    281
 255.255.255.255  255.255.255.255  100.20.1.3    100.20.1.3    281
 255.255.255.255  255.255.255.255  10.10.1.4     10.10.1.4    257
```

The check result shows that the legal PC has no route to the network segment of FW2 service address. This problem needs to be solved.

Check the configuration of the SSL VPN network extension routing mode on FW2.

```
v-gateway gateway
basic
ssl version tlsv12
ssl timeout 5
ssl lifecycle 1440
ssl public-key algorithm rsa
ssl ciphersuit custom aes256-sha aes128-sha
service
```

```
network-extension enable  
network-extension keep-alive enable  
network-extension keep-alive interval 120  
network-extension netpool 10.10.1.1 10.10.1.10 255.255.255.0  
netpool 10.10.1.1 default  
network-extension mode manual
```

It is found that the routing mode of network extension is set to manual routing mode, but the specific route to the service address of the headquarters is not added in manual routing mode.

Complete the network extension configuration on FW2 and add specific routes to the headquarters network in manual routing mode.

```
[FW2] v-gateway gateway  
[FW2-gateway-basic] service  
[FW2-gateway-service] network-extension mode manual  
[FW2-gateway-service] network-extension manual-route 172.16.10.0 255.255.255.0  
[FW2-gateway-service] quit
```

After the SSL VPN configuration is modified on FW2, the VPN of legal PC is forcibly terminated. After re-dialing in to the VPN, check the IP address obtained by legal PC.

```
C:\Users\Security>ipconfig  
Windows IP Configuration  
  
Unknown adapter Local Area Connection:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::51e2:b0c9:b33d:a77b%6  
IPv4 Address . . . . . : 10.10.1.5  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

Check the routing table of the CMD in the legal PC.

```
C:\Users\Security>route print
=====
Interface List
 6...00 ff de 2e c0 da ....TAP-Windows Adapter V9
 5...00 0c 29 b3 21 a1 ....Intel(R) 82574L Gigabit Network Connection
 3...00 0c 29 b3 21 b5 ....Intel(R) 82574L Gigabit Network Connection #3
 1.....Software Loopback Interface 1
 7...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 31...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 2...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====
IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0          0.0.0.0   100.20.1.1    100.20.1.3    281
          10.6.1.2  255.255.255.255  100.20.1.1    100.20.1.3    257
          10.10.1.0  255.255.255.0    On-link       10.10.1.4      1
          10.10.1.4  255.255.255.255  On-link       10.10.1.4    257
          10.10.1.255  255.255.255.255  On-link       10.10.1.4    257
          100.20.1.0  255.255.255.0    On-link       100.20.1.3    281
          100.20.1.3  255.255.255.255  On-link       100.20.1.3    281
          100.20.1.255  255.255.255.255  On-link       100.20.1.3    281
          127.0.0.0          255.0.0.0    On-link       127.0.0.1    331
          127.0.0.1          255.255.255  On-link       127.0.0.1    331
 127.255.255.255  255.255.255.255  On-link       127.0.0.1    331
          172.16.10.0  255.255.255.0    On-link       10.10.1.4      1
          172.16.10.255  255.255.255.255  On-link       10.10.1.4    257
          192.168.10.0          255.255.255  On-link      192.168.10.6    281
          192.168.10.6          255.255.255  On-link      192.168.10.6    281
 192.168.10.255  255.255.255.255  On-link      192.168.10.6    281
          224.0.0.0          240.0.0.0    On-link       127.0.0.1    331
          224.0.0.0          240.0.0.0    On-link      192.168.10.6    281
          224.0.0.0          240.0.0.0    On-link       100.20.1.3    281
          224.0.0.0          240.0.0.0    On-link       10.10.1.4    257
          255.255.255.255  255.255.255.255  On-link       127.0.0.1    331
          255.255.255.255  255.255.255.255  On-link      192.168.10.6    281
          255.255.255.255  255.255.255.255  On-link       100.20.1.3    281
          255.255.255.255  255.255.255.255  On-link       10.10.1.4    257
=====
```

Ping the service address 172.16.10.2 of the headquarters on the legal PC.

```
C:\Users\Security>ping 172.16.10.2
Pinging 172.16.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.10.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

It is found that the service address is unreachable. The routing table of the legal PC has sent the data packet to FW2. Therefore, you need to check the FW2 configuration.

Enable the debugging function on FW2 to view detailed information about data packets processed on FW2.

```
[FW2] acl number 3005
[FW2-acl-adv-3005] rule per ip destination 172.16.10.0 0.0.0.255
[FW2-acl-adv-3005] quit
<FW2> debugging security-policy packet acl 3005
<FW2> terminal debugging
<FW2> terminal monitor
```

Ping the service address 172.16.10.2 of the headquarters on the legal PC to trigger the service.

The command output on FW2 is as follows:

```
<FW2>
INFO_01:Sec Policy match rule id:0x0, action:0, log:0, condition SrcZone:2, DstZone:1, SrcGroup:0,
DstGroup:0, SrcIp:a0a0102, DstIp:ac100a02, Pro:1, SrcPort:8, DstPort:0, User:8000, App:131071, Url:1-
60000-0, Vsys:0,AccessType:0, DeviceType:0, VlanId:0, SrcLocId:2098, DstLocId:2098, SrcMacId:0,
DstMacId:0,SrcDomainId:2048-2048, DstDomainId:2048-2048, accRtn:0, TrafficLog:0
```

The ping packet matches the security policy whose ID is **0x0**. In USG6500E V600R007C20SPC500, rule id **0x0** indicates the default security policy. That is, the packet does not match any specific security policy. Because the default action of the security policy is **deny**, the packet is denied.

Modify the security policy on FW2.

```
[FW2] security-policy
[FW2-policy-security] rule name untrust-trust
[FW2-policy-security-rule-untrust-trust] source-zone untrust
[FW2-policy-security-rule-untrust-trust] destination-zone trust
[FW2-policy-security-rule-untrust-trust] destination-address 172.16.10.0 mask 255.255.255.0
[FW2-policy-security-rule-untrust-trust] action permit
[FW2-policy-security-rule-untrust-trust] quit
```

Ping 172.16.10.2 from the legal PC. The connectivity is normal.

```
C:\Users\Security>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:
Reply from 172.16.10.2: bytes=32 time=1ms TTL=127
Reply from 172.16.10.2: bytes=32 time=1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

8.3 Configuration Reference

8.3.1 SW1's Configuration

```
#
#sysname SW1
#
vlan batch 40 1000
#
interface vlanif40
    ip address 3.3.3.1 255.255.255.252
#
interface vlanif1000
    ip address 100.20.1.1 255.255.255.0
#
interface GigabitEthernet0/0/3
    port link-type trunk
```

```
port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/14
    port link-type access
    port default vlan 1000
#
ip route-static 10.6.1.0 255.255.255.252 4.4.4.2
#
Return
```

8.3.2 Mirror-SW's Configuration

```
#
sysname Mirror-SW
#
vlan 40
#
interface GigabitEthernet0/0/2
    port link-type trunk
    port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/3
    port link-type trunk
    port trunk allow-pass vlan 40
#
Return
```

8.3.3 RT2's Configuration

```
#
sysname RT2
#
interface GigabitEthernet0/0/1
    undo portswitch
#
interface GigabitEthernet0/0/1.40
    dot1q termination vid 40
    ip address 3.3.3.2 255.255.255.252
#
interface GigabitEthernet0/0/4
    undo portswitch
    ip address 10.6.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
Return
```

8.3.4 FW2's Configuration

```
#
sysname FW2
#
```

```
interface GigabitEthernet0/0/2
undo shutdown
ip address 10.6.1.2 255.255.255.252
service-manage ping permit
#
interface GigabitEthernet0/0/5
undo shutdown
ip address 172.16.10.1 255.255.255.0
service-manage ping permit
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/2
#
ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
#
v-gateway public ssl version tlsv12
v-gateway public ssl public-key algorithm rsa
v-gateway public ssl ciphersuit custom aes256-sha aes128-sha
v-gateway ssl-renegotiation-attack defend enable
v-gateway ssl weak-encryption enable
v-gateway gateway interface GigabitEthernet0/0/2 private
v-gateway gateway alias gateway
#
#****BEGIN***gateway**1***#
v-gateway gateway
basic
ssl version tlsv12
ssl timeout 5
ssl lifecycle 1440
ssl public-key algorithm rsa
ssl ciphersuit custom aes256-sha aes128-sha
service
network-extension enable
network-extension keep-alive enable
network-extension keep-alive interval 120
network-extension netpool 10.10.1.1 10.10.1.10 255.255.255.0
netpool 10.10.1.1 default
network-extension mode manual
network-extension manual-route 172.16.10.0 255.255.255.0
security
policy-default-action permit vt-src-ip
certification cert-anonymous cert-field user-filter subject cn group-filter subject cn
certification cert-anonymous filter-policy permit-all
certification cert-challenge cert-field user-filter subject cn
certification user-cert-filter key-usage any
undo public-user enable
hostchecker
```

```
cachecleaner
vpndb
  group /default
role
  role default
  role default condition all
  role default network-extension enable
*****END****
#
security-policy
  rule name untrust-local
    source-zone untrust
    destination-zone local
    destination-address 10.6.1.2 mask 255.255.255.255
    action permit
  rule name untrust-trust
    source-zone untrust
    destination-zone trust
    source-address 10.10.1.0 mask 255.255.255.0
    source-address 100.100.1.0 mask 255.255.255.0
    destination-address 172.16.1.0 mask 255.255.255.0
    destination-address 172.16.10.0 mask 255.255.255.0
    destination-address 172.16.40.0 mask 255.255.255.0
    action permit
#
The following configurations are saved in the database and are not displayed in the configuration file.
  user-manage user user01 domain default
    password Huawei@123
    parent-group /default
#
return
```

8.3.5 SW3's Configuration

```
#
sysname SW3
#
interface GigabitEthernet0/0/1
  port link-type access
#
interface GigabitEthernet0/0/13
  port link-type access
#
Return
```

8.4 Quiz

In addition to the manual routing mode, what are the other routing modes of the SSL VPN on the firewall? What are their logics?

Reference answer: There are three routing modes for SSL VPN: split routing mode, full routing mode, and manual routing mode.

In split routing mode, The data sent from the client to the intranet is identified by the system routing table and forwarded by the vNIC, and the vNIC uses the virtual IP address as the source IP address of the data. The data destined for the local subnet is forwarded by a NIC, and the NIC uses the actual IP address as the source IP address of the data. Therefore, network extension forwards only the data to the intranet. At the same time, the vNIC also forwards the data not destined for the local subnet.

In full routing mode, No matter what resources the device accesses, the data is intercepted by the virtual NIC, and the vNIC forwards the data to the virtual gateway.

In manual routing mode, configure a static route to the intranet on the device. The client identifies the data destined for the intranet and forwards the data through the vNIC.

9 Anti-DDoS

9.1 Introduction

9.1.1 About This Lab

Large-scale DDoS attacks may occur on the Internet. An enterprise deploys anti-DDoS devices at the network egress to check traffic from the Internet to the intranet, blocking threats in real time.

In this lab, static traffic diversion is deployed in off-path mode to block packets from known attack sources on the Internet to access the enterprise intranet.

9.1.2 Objectives

- Learn how to use the Abnormal Traffic Inspection & Control System (ATIC) management center to manage anti-DDoS devices.
- Understand how to use the SecoManager management center.
- Learn how to divert traffic based on the Modular QoS Command-Line Interface (MQC).
- Understand the usage logic of source NAT and destination NAT in the anti-DDoS scenario.
- Manage anti-DDoS devices through the SecoManager to block traffic.

9.1.3 Networking Topology

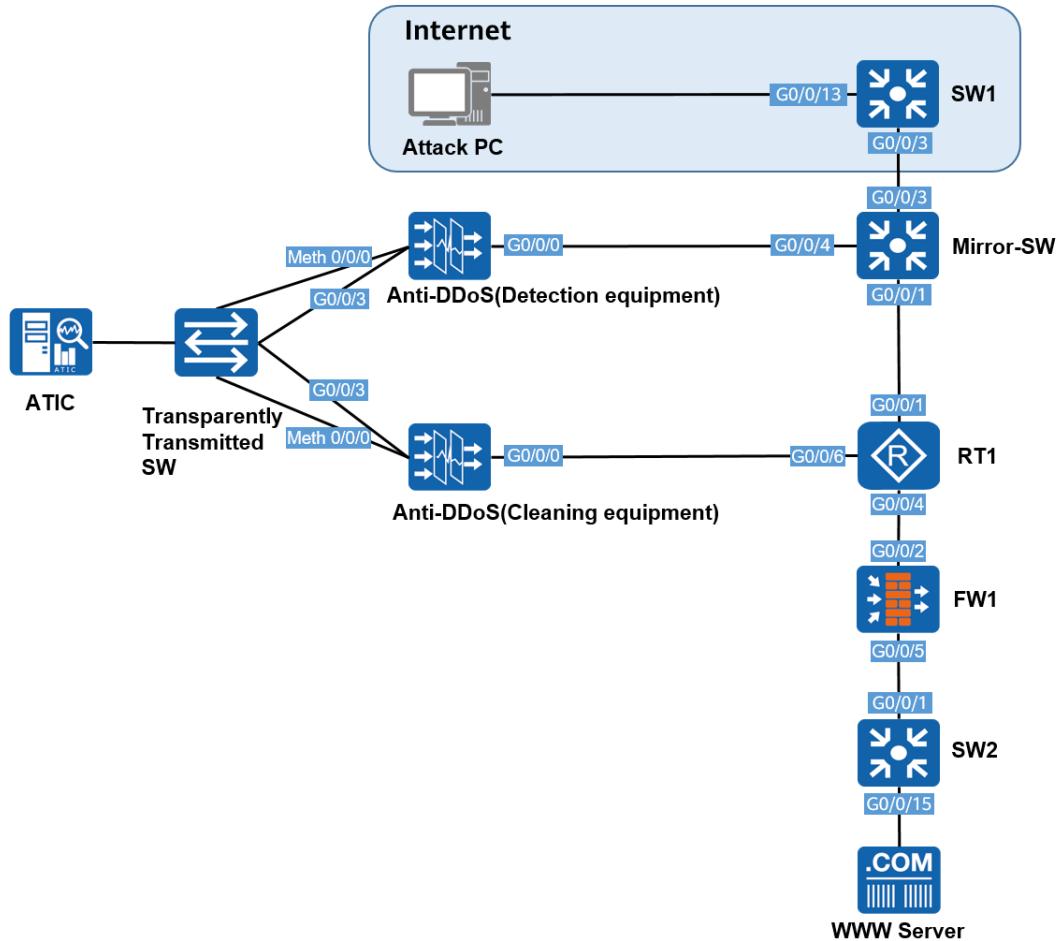


Figure 9-1 Anti-DDoS

The preceding figure shows device connections. For details about IP address planning, see Figure 9-1.

Attack PC simulates the Internet attack source. RT1 is the egress router of the enterprise headquarters, and a mirroring switch (Mirror-SW) connects to RT1. A web server (WWW Server) providing services for the Internet is in the downstream direction of the intranet firewall.

Note: The transparent transmission switch (Transparently Transmitted SW) connected to the anti-DDoS devices is actually the same device as Mirror-SW. Compared to the actual topology, the current topology is easier to understand. In addition, the interfaces connecting the anti-DDoS device to Mirror-SW are configured by default and the configurations are not described here.

For configurations of SW1, SW2, and Mirror-SW, see 9.4 Configuration Reference.

1. Internet area: The gateway of Attack PC is on SW1.
2. Egress area of the enterprise headquarters: The mirroring switch is at the border of the area. It mirrors the traffic (from the Internet to the intranet) to the anti-DDoS detecting device for threat detection. MQC is used on the egress router to divert

traffic (from the Internet to the intranet) to the anti-DDoS cleaning device for cleaning.

3. Anti-DDoS area: The ATIC manages and delivers corresponding policies to the anti-DDoS detecting and cleaning devices.
4. Intranet area of the enterprise headquarters: The web server on the intranet needs to provide services for the Internet and the gateway of the web server is deployed on the firewall.

9.1.4 Lab Planning

Table 9-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2	Interface for connecting to Mirror-SW
	G0/0/13	Access	PVID: 11	Interface for connecting to Attack PC
SW2	G0/0/1	Access	PVID: 1	Interface for connecting to FW1
	G0/0/15	Access	PVID: 1	Interface for connecting to WWW Server
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2	Interconnection interface
	G0/0/3			
	G0/0/4	Trunk	PVID: 1 Allow-pass VLAN: 1	Interface for connecting to the anti-DDoS detecting device, and the default configuration is used
RT1	G0/0/1.2	Layer 3 sub-interface	4.4.4.2/30 Termination VLAN 2	Interface for connecting to SW1
	G0/0/4	Layer 3 interface	10.3.1.1/30	Interface for connecting to FW1
	G0/0/6	Trunk	PVID: 1 Allow-pass VLAN: 15, 20	Interface for connecting to the anti-DDoS cleaning

				device
	VLANIF15	Layer 3 interface	1.1.1.1/24	Traffic diversion interface, connecting to G0/0/0.15 on the anti-DDoS cleaning device
	VLANIF20	Layer 3 interface	2.2.2.1/24	Traffic injection interface, connecting to G0/0/0.20 on the anti-DDoS cleaning device
FW1	G0/0/2	Layer 3 interface	10.3.1.2/30	Interface for connecting to RT1
	G0/0/5	Layer 3 interface	172.16.30.2/24	Interface for connecting to SW2
Anti-DDoS detecting device	MEth0/0/0	Layer 3 interface	vpn instance: _management_vpn_ 192.168.2.10/24	Management interface
	G0/0/0	Layer 3 interface	/	Traffic diversion interface, connecting to Mirror-SW
	G0/0/3	Layer 3 interface	192.168.2.13/24	Interface for sending logs
Anti-DDoS cleaning device	MEth0/0/0	Layer 3 interface	vpn instance: _management_vpn_ 192.168.2.12/24	Management interface
	G0/0/0.15	Layer 3 interface	1.1.1.2/24	Traffic diversion interface
	G0/0/0.20	Layer 3 interface	2.2.2.2/24	Traffic injection interface
	G0/0/3	Layer 3 interface	192.168.2.14/24	Interface for sending logs
Attack PC	Ethernet0	Network adapter	20.20.20.2/24 Gateway: 20.20.20.1/24	Endpoint
WWW Server	Ethernet0	Network adapter	172.16.30.10/24 Gateway: 172.16.30.2/24	Endpoint

9.2 Lab Configuration

9.2.1 Configuration Roadmap

1. Configure IP addresses for devices.
2. Activate the functions of the anti-DDoS detecting and cleaning devices.
3. Use the SecoManager to manage anti-DDoS detecting and cleaning devices.
4. Configure protection policies and filters on the SecoManager.
5. Mirror the traffic on Mirror-SW to the anti-DDoS detecting device.
6. On RT1, use MQC to divert traffic (from the Internet to the intranet) to the anti-DDoS cleaning device.
7. Configure a route for traffic injection on the anti-DDoS cleaning device.
8. Configure network intercommunication on the enterprise intranet, including configuring firewall security policies and gateways.
9. Use Attack PC on the Internet to access the web server on the intranet and check the lab result.

9.2.2 Configuration Procedure

Step 1 Set basic network parameters.

Set basic network parameters according to the table in 9.1.4 Lab Planning.

SW1, SW2, and Mirror-SW are pre-configured. For details, see 9.4 Configuration Reference.

Step 2 Activate the anti-DDoS function.

You need to run commands to specify and activate the related functions on the anti-DDoS detecting and cleaning devices.

Specify the CPU detection function on the anti-DDoS detecting device.

```
[check] firewall ddos detect-spu slot 0 cpu 0
```

After specifying the CPU detection function, you need to save the configuration and restart the device to make the configuration of the detection interface take effect.

Save the configuration and restart the anti-DDoS detecting device.

```
[check] quit
<check> save
Warning: The current configuration will be written to the device. Continue? [Y/N]:Y
Info: Please input the file name(*.cfg, *.zip, *.dat):
Now saving the current configuration to the slot 0 ..
Info: Save the configuration successfully.
<check> reboot
slot 0:
Next startup system software: flash:/AntiDDoS1900_V600R021C00SPC100.cc
Next startup saved-configuration file: flash:/vrpcfg.zip
Next startup paf file: default
Next startup patch package: flash:/AntiDDoS1900_V600R021SPH001.PAT
```

```
Warning: The system will reboot. Continue? [Y/N]:Y
```

Enable the detection and the traffic statistics collection function on the interface of the anti-DDoS detecting device.

```
[check] interface GE0/0/0  
[check -GE0/0/0] anti-ddos flow-statistic enable  
[check -GE0/0/0] anti-ddos detect enable  
[check -GE0/0/0] quit
```

Enable the cleaning and the traffic statistics collection function on the interfaces of the anti-DDoS cleaning device and configure IP addresses for the interfaces.

```
[clean] interface GE0/0/0  
[clean-GE0/0/0] anti-ddos flow-statistic enable  
[clean-GE0/0/0] anti-ddos clean enable  
[clean-GE0/0/0] quit
```

```
[clean] interface GE0/0/0.15  
[clean-GE0/0/0.15] ip address 1.1.1.2 24  
[clean-GE0/0/0.15] dot1q termination vid 15  
[clean-GE0/0/0.15] anti-ddos flow-statistic enable  
[clean-GE0/0/0.15] anti-ddos clean enable  
[clean-GE0/0/0.15] quit
```

```
[clean] interface GE0/0/0.20  
[clean-GE0/0/0.20] ip address 2.2.2.2 24  
[clean-GE0/0/0.20] dot1q termination vid 20  
[clean-GE0/0/0.20] anti-ddos flow-statistic enable  
[clean-GE0/0/0.20] anti-ddos clean enable  
[clean-GE0/0/0.20] quit
```

Step 3 Use the SecoManager to manage anti-DDoS devices.

Generally, the SecoManager uses Simple Network Management Protocol (SNMP) to manage anti-DDoS devices through the Meth management interface. To enable the SecoManager to manage anti-DDoS devices, you need to enable the Network Configuration Protocol (NETCONF) and SSH functions on anti-DDoS devices.

This step uses the anti-DDoS detecting device as an example. The configuration of the anti-DDoS cleaning device is the same as that of the detecting device and is not mentioned here.

Configure the SNMP version. This step is optional. By default, SNMPv3 is used.

```
[DDoS1-check] snmp-agent  
[DDoS1-check] snmp-agent sys-info version v3
```

Configure the range of objects included in the MIB view.

```
[DDoS1-check] snmp-agent mib-view included mib2view iso
```

Configure an SNMPv3 user and user group, and configure the authentication key and encryption key.

```
[DDoS1-check] snmp-agent usm-user v3 admin
Warning: The privacy and authentication passwords are the same, which is insecure. It is recommended that the privacy and authentication passwords be different.
[DDoS1-check] snmp-agent usm-user v3 admin group group1
Warning: The privacy and authentication passwords are the same, which is insecure. It is recommended that the privacy and authentication passwords be different.
[DDoS1-check] snmp-agent usm-user v3 admin authentication-mode sha2-256
Please configure the authentication password (8-255)
Enter Password: Huawei@123
Confirm Password: Huawei@123
[DDoS1-check] snmp-agent usm-user v3 admin privacy-mode aes256
Please configure the privacy password (8-255)
Enter Password: Huawei@123
Confirm Password: Huawei@123
```

Grant the read, write, and alarm reporting permissions to the user group on the device.

```
[DDoS1-check] snmp-agent group v3 group1 privacy read-view mib2view write-view mib2view notify-view mib2view
```

Enable the SNMP Trap function on the device and set the source port.

```
[DDoS1-check] snmp-agent trap source GigabitEthernet0/0/3
[DDoS1-check] snmp-agent protocol source-interface MEth0/0/0
[DDoS1-check] snmp-agent trap enable
```

Configure the NETCONF administrator and the corresponding service type, level, and authentication type, and enable SSH.

```
[DDoS1-check] aaa
[DDoS1-check-aaa] local-user netconf-admin password irreversible-cipher Hello@123
[DDoS1-check-aaa] local-user netconf-admin privilege level 3
[DDoS1-check-aaa] local-user netconf-admin service-type ssh
[DDoS1-check-aaa] quit
[DDoS1-check] ssh user netconf-admin
[DDoS1-check] ssh user netconf-admin authentication-type all
[DDoS1-check] ssh user netconf-admin service-type all
```

Enable NETCONF and use the default port 830.

```
[DDoS1-check] snetconf server enable
[DDoS1-check] netconf
[DDoS1-check-netconf] protocol inbound ssh ipv4 port 830
[DDoS1-check-netconf] nacm
[DDoS1-check-netconf-nacm] nacm enable
[DDoS1-check-netconf-nacm] group-name nacm-group
[DDoS1-check-netconf-nacm-nacm-group-nacm-group] user-name netconf
[DDoS1-check-netconf-nacm-nacm-group-nacm-group] quit
```

```
[DDoS1-check-netconf-nacm] execute-default permit  
[DDoS1-check-netconf-nacm] quit  
[DDoS1-check-netconf] quit
```

Configure the STelnet protocol on the device and configure the local key pair.

```
[DDoS1-check] rsa local-key-pair create  
The key name will be:Host  
The range of public key size is (512 ~ 2048).  
NOTE: Key pair generation will take a short while.  
Please input the modulus [default = 2048]:2048
```

Set the VTY user authentication mode to AAA and configure the VTY user interface to support SSH.

```
[DDoS1-check] user-interface vty 0 14  
[DDoS1-check-ui-vty0-4] authentication-mode aaa  
[DDoS1-check-ui-vty0-4] user privilege level 3  
[DDoS1-check-ui-vty0-4] protocol inbound ssh  
[DDoS1-check-ui-vty0-4] quit
```

Configure a local user and the user service mode.

```
[DDoS1-check] aaa  
[DDoS1-check-aaa] local-user admin123 password  
Please configure the login password (8-128)  
It is recommended that the password consist of four types of characters, including lowercase letters, uppercase letters, numerals and special characters.  
Please enter password:Huawei@123  
Please confirm password: Huawei@123  
[DDoS1-check-aaa] local-user admin123 service-type ssh  
[DDoS1-check-aaa] local-user admin123 privilege level 3  
[DDoS1-check-aaa] quit
```

Create an SSH user and configure the authentication mode and service type.

```
[DDoS1-check] ssh user admin123  
[DDoS1-check] ssh user admin123 authentication-type password  
[DDoS1-check] ssh user admin123 service-type stelnet  
[DDoS1-check] stelnet server enable  
[DDoS1-check] ssh server-source -i MEth 0/0/0
```

For details about the configuration on the anti-DDoS cleaning device, see the preceding operations.

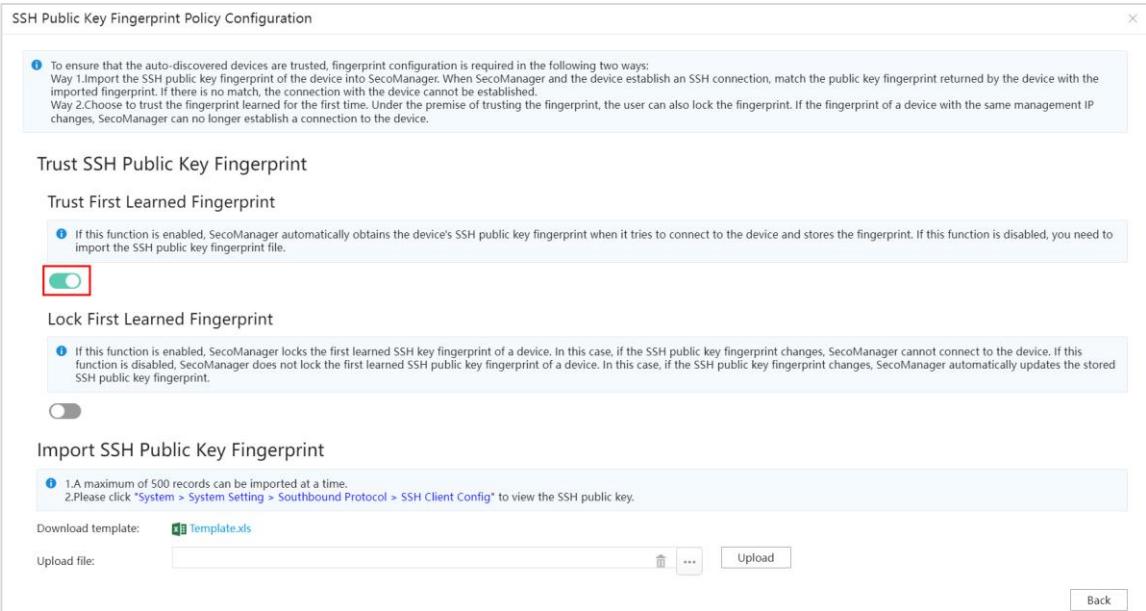
On the anti-DDoS detecting device, set the source address for sending logs to the address of the local GigabitEthernet0/0/3 interface and the address of the log receiving server to the address of the SecoManager server.

```
[DDoS1-check] firewall ddos log-local-ip 192.168.2.13  
[DDoS1-check] firewall ddos log-server-ip 192.168.2.200
```

On the anti-DDoS cleaning device, set the source address for sending logs to the address of the local GigabitEthernet0/0/3 interface and the address of the log receiving server to the address of the SecoManager server.

```
[DDoS2-clean] firewall ddos log-local-ip 192.168.2.14  
[DDoS2-clean] firewall ddos log-server-ip 192.168.2.200
```

On the SecoManager web UI, choose **Device Management > Device > Device** from the main menu. In the **More** drop-down list, click **SSH Public Key Fingerprint Policy** and set the parameters as follows:



On the SecoManager web UI, choose **Device Management > Device > Device** from the main menu. In the **Add Device** drop-down list, click **Auto Discover**, set the parameters as follows, and click **Start Scanning**.

Device Management / Device / Device

1.The scanning rule defines the IP address segment and the protocol used (SNMP or NETCONF). The SecoManager discovers devices based on the scanning rule.
2.Import the public key fingerprint of the device first. If the fingerprint is not imported, choose [SSH Public Key Fingerprint](#), enable Trust First Learned Fingerprint, and disable Lock First.

*** Device Discovery Protocol Type:**

1. Set Rule

Location

Location: [+ Select](#)

Management IP address

* Management IP address

[Select Template](#) [Save Template](#)

SNMPv3

SHA and MD5 are not secure enough due to their limitations. Using AES_256 to improve security is recommended.

* User name :	admin	* Authentication key :
* Authentication protocol :	SHA2-256	* Encryption algorithm :	AES-256
* Port :	161	* Timeout period (ms) :	4000
* Retries (times) :	3		

NETCONF

* User name :	netconf-admin	* Password :
* Port :	830		

STELNET

The STELNET protocol is a unique parameter of the AntiDDoS.

* User name :	admin123	* Password :
---------------	----------	--------------	-------

Public key:

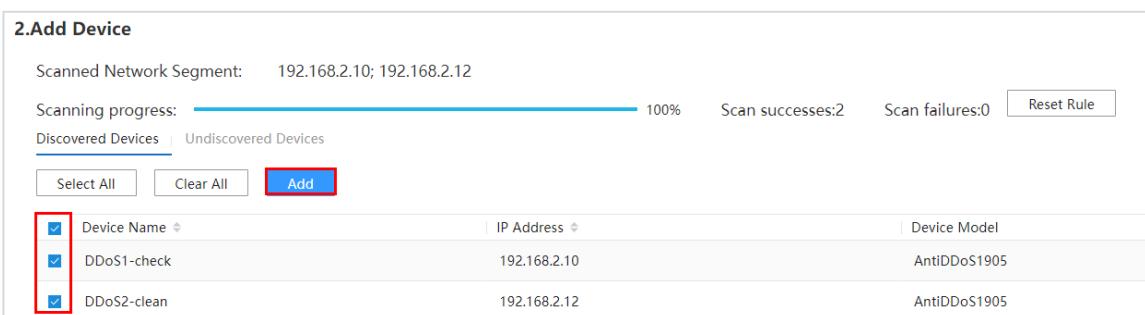
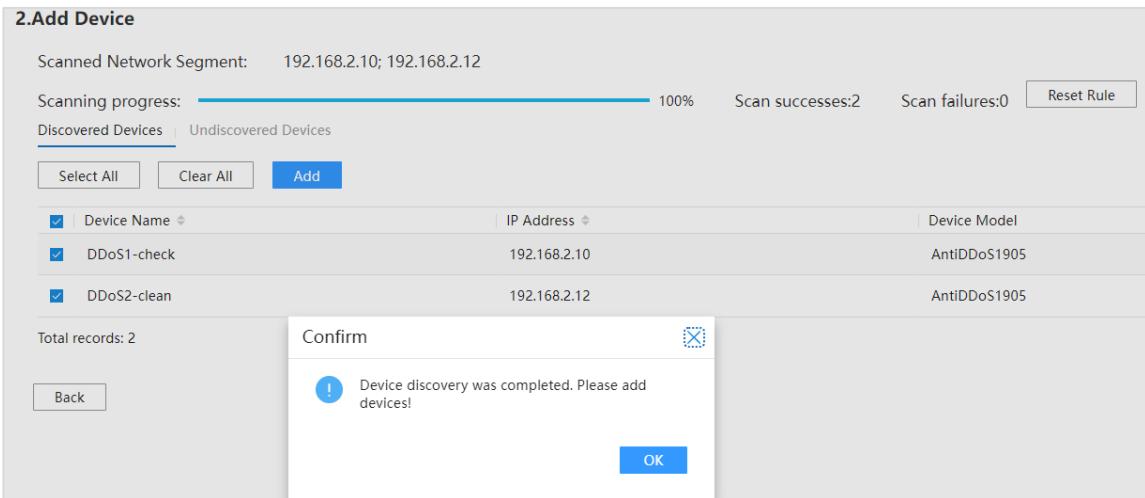
1. If the public key is entered, the device is authenticated using the public key when the STElnet or SFTP protocol is used to access the device. 2. To ensure data transmission security, you are advised to enter the public key.

Log

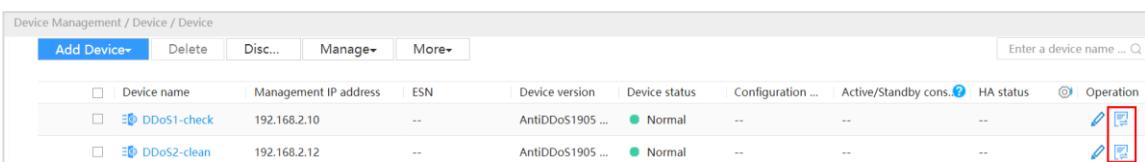
* Log password:

[Start Scanning](#)

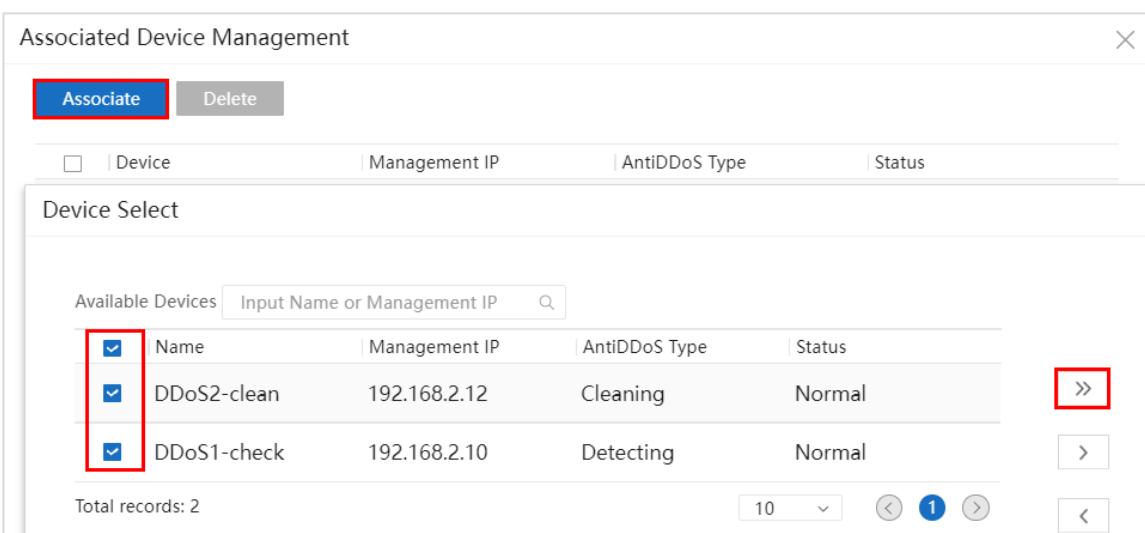
After the scanning is successful, add two devices as prompted.



Choose **Device Management > Device > Device** and click **Information collection** on the right to collect anti-DDoS information to the SecoManager.



Choose **Device Management > Device > AntiDDoS Collector**, click **Associate device** in the upper left corner, select two devices as shown in the following figure, and click **OK**.



Step 4 Configure attack defense on the SecoManager.

Choose AntiDDoS Attack Defense > Attack Defense > Zone, create a Zone named **test**, and set the parameters as follows.

Choose AntiDDoS Attack Defense > Attack Defense > Zone. Click the drop-down list in front of **test** to display the detailed protection policies of the two devices.

Click **Edit**, modify the ICMP policies of **DDoS1-check** and **DDoS1-clean**, and deploy the policies.

Countermeasures

All Enabled Countermeasures

- Zone Rate Limiting
- IP Flood Rate Limiting
- IP Flood Defense
- TCP Malformed Defense
- SYN Flood Defense
- SYN-ACK Flood Defense
- ACK Flood Defense
- FIN/RST Flood Defense
- TCP Connection Flood Defense
- TCP Rate Limiting
- UDP Malformed Defense
- UDP Flood Defense
- UDP Rate Limiting
- HTTP Flood Defense
- HTTP Connection Defense
- TLS-based Encryption
- Attack Defense**
- TLS-based Session Attack Defense
- DNS Malformed Defense
- DNS Query Flood Defense
- DNS Reply Flood Defense
- DNS Rate Limiting
- ICMP Rate Limiting
- IP rate limiting (pps) (1-2,000,000)
- SIP Flood Defense
- SIP Rate Limiting

Save **Back** **Deploy**

Choose AntiDDoS Attack Defense > Attack Defense > Zone, select test, and click Deploy.

Create	Delete	Deploy	Undeploy	Apply Baseline	
<input checked="" type="checkbox"/> Zone	Baseline ...	Operatio...	Defense Status	Diversio...	Deployment Status
test	Not Learne	Normal	--	Not Diverted	

Step 5 Configure traffic mirroring on Mirror-SW.

On Mirror-SW, mirror incoming and outgoing traffic on G0/0/3 to the anti-DDoS detecting device through G0/0/4.

```
[Mirror-SW] observe-port 1 interface GigabitEthernet0/0/4
[Mirror-SW] interface GigabitEthernet0/0/3
[Mirror-SW -G0/0/3] port-mirroring to observe-port 1 outbound
[Mirror-SW -G0/0/3] port-mirroring to observe-port 1 inbound
[Mirror-SW -G0/0/3] quit
```

Step 6 Divert traffic through RT1.

On RT1, divert the traffic (from the Internet to the intranet) to the anti-DDoS cleaning device. That is, redirect the inbound traffic that pass through GigabitEthernet0/0/1.2 on RT1 to the IP address of GigabitEthernet0/0/0.15 on the anti-DDoS cleaning device.

```
[RT1] acl number 3500
[RT1-acl-adv-3500] rule permit ip
[RT1-acl-adv-3500] quit
[RT1] traffic classifier 1 operator or
[RT1-classifier-1] if-match acl 3500
[RT1-classifier-1] traffic behavior 1
[RT1-behavior-1] redirect ip-nexthop 1.1.1.2
[RT1-behavior-1] traffic policy 1
[RT1-trafficpolicy-1] classifier 1 behavior 1
[RT1-trafficpolicy-1] quit
[RT1] int GigabitEthernet0/0/1.2
[RT1-GigabitEthernet0/0/1.2] traffic-policy 1 inbound
[RT1-GigabitEthernet0/0/1.2] quit
```

Step 7 Inject traffic through the anti-DDoS cleaning device.

On the anti-DDoS cleaning device, configure a default route to inject cleaned data packets back to the traffic injection interface (2.2.2.1) on RT1. The anti-DDoS cleaning device has the configuration about security zones and security policy. Therefore, you need to add interfaces to security zones and configure the security policy for allowing traffic to pass through.

Configure a route for traffic injection.

```
[DDoS2-clean] ip route-static 0.0.0.0 0.0.0.0 2.2.2.1
```

Configure a security policy.

```
[DDoS2-clean] firewall zone untrust
[DDoS2-clean-zone-untrust] add interface GE 0/0/0
[DDoS2-clean-zone-untrust] add interface GE 0/0/0.15
[DDoS2-clean-zone-untrust] add interface GE 0/0/0.20
[DDoS2-clean-zone-untrust] quit
[DDoS2-clean] security-policy
[DDoS2-clean-policy-security] rule name pass
[DDoS2-clean-policy-security-rule-pass] action permit
[DDoS2-clean-policy-security-rule-pass] quit
[DDoS2-clean-policy-security] quit
```

Step 8 Divert traffic through RT1.

The anti-DDoS cleaning device sends cleaned traffic to VLANIF 20 on RT1 through a static route, and RT1 needs to forward the traffic to WWW Server on the intranet. To achieve this need, configure destination NAT on VLANIF 20 of RT1. When WWW Server returns packets to Attack PC, there must be a default route destined for the Internet and source NAT must be configured on the router.

Configure destination NAT on VLANIF 20 of RT1.

```
[RT1] interface vlanif 20
[RT1-VLANIF20] nat server global 10.10.10.10 inside 172.16.30.10
[RT1-VLANIF20] quit
```

Configure service routes destined for FW1 on the intranet on RT1.

```
[RT1] ip route-static 172.16.20.0 255.255.255.0 10.3.1.2
[RT1] ip route-static 172.16.30.0 255.255.255.0 10.3.1.2
```

Configure a default route destined for the Internet and source NAT on RT1.

```
[RT1] acl number 3500
[RT1-acl-adv-3500] rule permit ip
[RT1-acl-adv-3500] quit
[RT1] int GigabitEthernet 0/0/1
[RT1-GigabitEthernet0/0/1] undo portswitch
[RT1-GigabitEthernet0/0/1] quit
[RT1] interface GigabitEthernet0/0/1.2
[RT1-GigabitEthernet0/0/1.2] nat outbound 3500
[RT1-GigabitEthernet0/0/1.2] dot1q termination vid 2
[RT1-GigabitEthernet0/0/1.2] ip address 4.4.4.2 255.255.255.252
[RT1-GigabitEthernet0/0/1.2] nat outbound 3500
[RT1-GigabitEthernet0/0/1.2] quit
```

Configure a default route on RT1.

```
[RT1] ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
```

Step 9 Configure network intercommunication on the enterprise intranet.

On FW1, add interfaces to corresponding security zones and configure the security policy for allowing traffic to pass through.

```
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface GigabitEthernet 0/0/2
[FW1-zone-untrust] quit
[FW1] firewall zone trust
[FW1-zone-trust] add interface GigabitEthernet 0/0/5
[FW1-zone-trust] quit
[FW1] security-policy
[FW1-policy-security] rule name pass
[FW1-policy-security-rule-pass] action permit
[FW1-policy-security-rule-pass] quit
```

Configure a default route to RT1 on FW1.

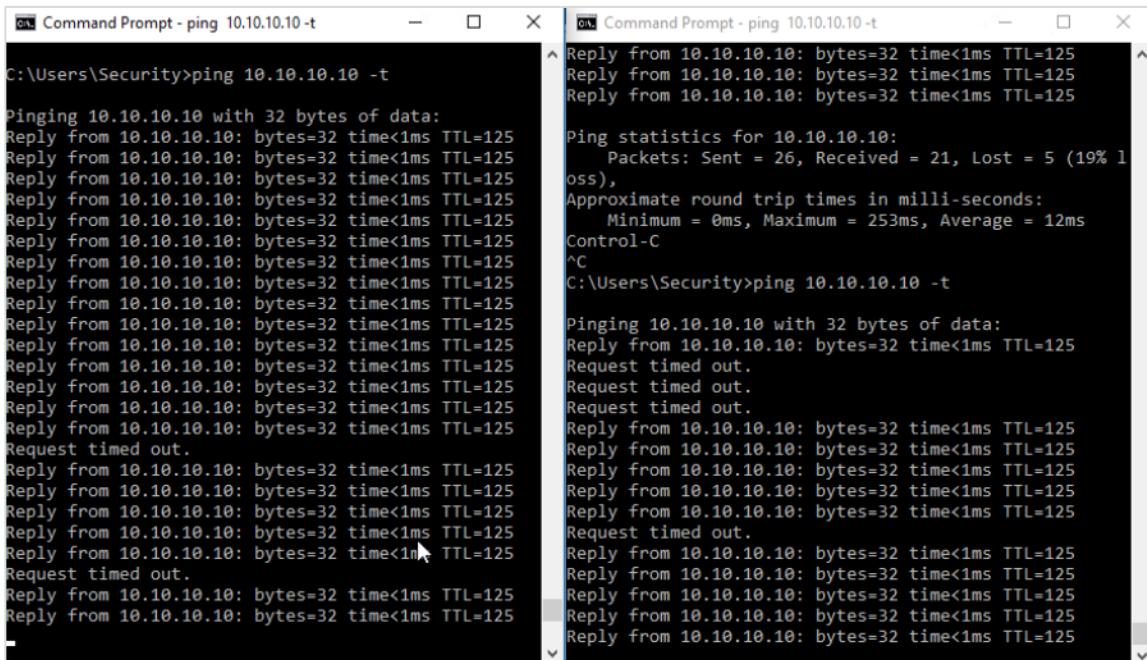
```
[FW1] ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
```

9.3 Verification

In this lab, the alarm threshold for the Zone to receive ICMP packets is set to 1 time/s in the anti-DDoS devices. If the packet sending rate exceeds the threshold, the system considers that an attack occurs. Open multiple CMD windows on Attack PC and continuously ping WWW Server on the enterprise intranet. The anti-DDoS devices block the ping requests and the SecoManager generates an event alarm.

This lab simulates a scenario where an Internet user attacks the enterprise intranet server. The enterprise intranet server uses the public IP address 10.10.10.10 to provide services for Internet users. In the lab, NAT Server is configured on VLANIF 20 of RT1 according to the traffic direction to meet service and test requirements.

After completing the configuration according to the configuration procedure, open multiple CMD windows on Attack PC and ping 10.10.10.10 at the same time.



The ping results are intermittent, indicating that the anti-DDoS function takes effect.

On the SecoManager, choose **AntiDDoS Attack Defense > Attack Defense > Zone**. An anomaly is displayed. Click **Attacked** to view details.



Create	Delete	Deploy	Undeploy	Apply Baseline
<input type="checkbox"/>	Zone	Baseline ...	Operatio...	Defense Status
<input checked="" type="checkbox"/>	test	Not Learne	Attacked	Automatically Defended
				Not Diverte Succeeded

Abnormal Events		Dynamic Blacklist		MachineLearning Blacklist							
Defense											
	Direction	Destination IP	Device	AntiDDoS Type	Start Time	Attack Type	Threshold	Incoming Traffic P.	Attack Traffic	State	
<input type="checkbox"/>	Inbound	10.10.10.10	DDoS1-check	Detecting	01:03:48 2022~...	ICMP Flood	1pps	2pps	-	Abnormal	
<input type="checkbox"/>	Inbound	10.10.10.10	DDoS2-clean	Cleaning	01:03:48 2022~...	ICMP Flood	1pps	2pps	3KB	Attacked	

```
# Cancel traffic diversion configured on RT1 and perform the ping test again. No packet loss occurs.
```

```
[RT1] int GigabitEthernet0/0/1.2  
[RT1-GigabitEthernet0/0/1.2] undo traffic-policy inbound  
[RT1-GigabitEthernet0/0/1.2] quit
```

9.4 Configuration Reference

9.4.1 SW1's Pre-configuration

```
#  
sysname SW1  
#  
vlan batch 2 11  
#  
interface vlanif2  
    ip address 4.4.4.1 255.255.255.252  
#  
interface vlanif11  
    ip address 20.20.20.1 255.255.255.0  
#  
interface GigabitEthernet0/0/3  
    port link-type trunk  
    port trunk allow-pass vlan 2
```

```
#  
interface GigabitEthernet0/0/13  
port link-type access  
port default vlan 11  
#  
ip route-static 10.10.10.0 255.255.255.0 4.4.4.2  
#  
return
```

9.4.2 SW2's Pre-configuration

```
#  
sysname SW2  
#  
interface GigabitEthernet0/0/1  
port link-type access  
#  
interface GigabitEthernet0/0/15  
port link-type access  
#
```

9.4.3 Mirror-SW's Pre-configuration

```
#  
sysname Mirror-SW  
#  
vlan 2  
#  
observe-port 1 interface GigabitEthernet0/0/4  
#  
interface GigabitEthernet0/0/1  
port link-type trunk  
port trunk allow-pass vlan 2  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 2  
port-mirroring to observe-port 1 inbound  
port-mirroring to observe-port 1 outbound  
#  
interface GigabitEthernet0/0/4  
port link-type trunk  
#  
return
```

9.4.4 RT1's Configuration

```
#  
sysname RT1  
#  
vlan batch 15 20  
#
```

```
acl number 3500
    rule 5 permit ip
#
traffic classifier 1 operator or
    if-match acl 3500
#
traffic behavior 1
    redirect ip-nexthop 1.1.1.2
#
traffic policy 1
    classifier 1 behavior 1 precedence 5
#
interface vlanif15
    ip address 1.1.1.1 255.255.255.0
#
interface vlanif20
    ip address 2.2.2.1 255.255.255.0
    nat server global 10.10.10.10 inside 172.16.30.10
#
interface GigabitEthernet0/0/1
    undo portswitch
#
interface GigabitEthernet0/0/1.2
    dot1q termination vid 2
    ip address 4.4.4.2 255.255.255.252
nat outbound 3500
    traffic-policy 1 inbound
#
interface GigabitEthernet0/0/4
    undo portswitch
    ip address 10.3.1.1 255.255.255.252
#
interface GigabitEthernet0/0/6
    port link-type trunk
    port trunk allow-pass vlan 15 20
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
ip route-static 172.16.20.0 255.255.255.0 10.3.1.2
ip route-static 172.16.30.0 255.255.255.0 10.3.1.2
#
return
```

9.4.5 FW1's Configuration

```
#
sysname FW1
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 10.3.1.2 255.255.255.252
    service-manage ping permit
#
interface GigabitEthernet0/0/5
    undo shutdown
```

```
ip address 172.16.30.2 255.255.255.0
service-manage http permit
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/5
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
#
security-policy
    rule name pass
        action permit
#
return
```

9.4.6 Anti-DDoS Detecting Device's Configuration

```
#
sysname DDoS1-check
#
firewall defend action discard
#
    firewall ddos detect-spu slot 0 cpu 0
#
firewall ddos log-local-ip 192.168.2.13
firewall ddos log-server-ip 192.168.2.200
anti-ddos packet-capture
key %+###!!!!!!!"!!!#!!!!*!!!!ag]j2t^t\"q9kx,mh(RY^RW<TmnU]7^F'cG!!!!2jp5!!!!!!q!!!!*9x7@aj{FD$=bg
3G+jZ&qjU`&V2F%XSUsf39zt`40g"bJcEB,,U#>f0E}J2.lao;/Yj9%sq7zT!pyj0y@Va7+&qJ*<+.L"b5".>%+%
anti-ddos packet-capture key enable
#
telnet server disable
telnet ipv6 server disable
undo telnet server-source all-interface
undo telnet ipv6 server-source all-interface
#
ip vpn-instance _management_vpn_
    ipv4-family
#
aaa
    authentication-scheme default
        authentication-mode local
    authorization-scheme default
        authorization-mode local
```

```
accounting-scheme default
  accounting-mode none
  local-user policy security-enhance
  local-aaa-user password policy administrator
  domain default
    authentication-scheme default
    accounting-scheme default
  local-user admin123 password irreversible-cipher
$1d$e2Qq>~HR#9ffEg90$B2s7SwidM51WMQLv=Mf9E)A[9!s3hINKS.Ul;o[0$
  local-user admin123 privilege level 3
  local-user admin123 service-type ssh
  local-user netconf-admin password irreversible-cipher
$1d$"FzPBP.$>~"oJ&$Q$K]jjC8S8ZEJzo01*)NpQO7SOAY1,tM82^".&~^!;$
  local-user netconf-admin privilege level 3
  local-user netconf-admin service-type ssh
#
interface MEth0/0/0
  ip binding vpn-instance _management_vpn_
  ip address 192.168.2.10 255.255.255.0
#
interface GE0/0/0
  anti-ddos flow-statistic enable
  anti-ddos detect enable
#
interface GE0/0/3
  ip address 192.168.2.13 255.255.255.0
#
snmp-agent sys-info version v3
snmp-agent group v3 group1 privacy read-view mib2view write-view mib2view notify-view mib2view
snmp-agent group v3 testgroup privacy read-view mib2view write-view mib2view notify-view
mib2view
#
snmp-agent mib-view included mib2view iso
snmp-agent usm-user v3 admin
snmp-agent usm-user v3 admin group group1
snmp-agent usm-user v3 admin authentication-mode sha2-256
cipher %+%#!!#!!!!!!!#!#!*!!!ag]j2t^t\"cw8cA*D"!!M*/l;@&kH;f_zv)!!!!2jp5!!!!;!!!!u|:,#ny>WT0jC.:ee
$Z22u:XI]ji#>#+:S!!!!%+%
snmp-agent usm-user v3 admin privacy-mode aes256
cipher %+%#!!#!!!!!!!#!#!*!!!ag]j2t^t\"Okf&,JCeD7y/&K/YXJJS[tDZL!!!!2jp5!!!!;!!!!2o)~@a\R4I2U2`V
;_YpB-g(W5,b;_Nr7a.Q!!!!%+%
#
snmp-agent trap source GE0/0/3
#
snmp-agent protocol source-interface MEth0/0/0
undo snmp-agent protocol source-status all-interface
undo snmp-agent protocol source-status ipv6 all-interface
#
undo snmp-agent proxy protocol source-status all-interface
undo snmp-agent proxy protocol source-status ipv6 all-interface
#
snmp-agent trap enable
#
stelnet server enable
snetconf server enable
```

```
ssh server authentication-retries 5
undo ssh server authentication-type keyboard-interactive enable
ssh user admin123
ssh user admin123 authentication-type password
ssh user admin123 service-type stelnet
ssh user netconf-admin
ssh user netconf-admin authentication-type all
ssh user netconf-admin service-type all
ssh server-source -i MEth0/0/0
undo ssh server-source all-interface
undo ssh ipv6 server-source all-interface
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey dsa ecc rsa
#
ssh server dh-exchange min-len 1024
#
ssh client publickey rsa_sha2_256 rsa_sha2_512
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh client hmac sha2_512 sha2_256
ssh client key-exchange dh_group_exchange_sha256
#
user-interface con 0
authentication-mode password
set authentication password cipher
$1d$WdD^YC9)0KO!G2'$kObj"7%n/9bN'w>MlR8'=s:_1bH:Q<}CMNG8'3Q/$
#
user-interface vty 0 14
authentication-mode aaa
user privilege level 3
protocol inbound ssh
#
netconf
protocol inbound ssh ipv4 port 830
#
nacm
nacm enable
execute-default permit
group-name nacm-group
user-name netconf
#
warranty
#
anti-ddos filter name attack type ip
source-ip ip 20.20.20.0 24
filter-id 5
#
ddos-zone name zone_16
zone-id 16
ip address 172.16.30.0 24
```

```
ip address 10.10.10.0 24
ip address 4.4.4.2 32
anti-ddos destination-ip session-limit protocol udp max-speed 10000
bandwidth-limit destination-ip type udp max-speed 50000
bandwidth-limit destination-ip type icmp max-speed 1
bandwidth-limit destination-ip type tcp-fragment max-speed 1000
bandwidth-limit destination-ip type udp-fragment max-speed 1000
bandwidth-limit destination-ip type other max-speed 100000
anti-ddos rst-flood session-check
anti-ddos syn-flood source-detect mode advanced
anti-ddos tcp-abnormal-flood alert-rate 500
anti-ddos syn-flood source-limit max-number 20 duration 3
anti-ddos dns format-check alert-rate 500
anti-ddos dns-request-flood source-detect
anti-ddos ack-flood session-check
anti-ddos udp-flood fingerprint-learn enable
anti-ddos udp-malformed-flood alert-rate 500
anti-ddos udp-flood defend alert-speed 500
anti-ddos https-flood defend alert-rate 20000
anti-ddos https-flood ssl-defend illegal-session-num 3 interval 5
anti-ddos https-flood ssl-defend incomplete-negotiation enable
anti-ddos tls-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos tls-flood fixed-resource illegal-ratio 90 min-number 20 interval 5
anti-ddos tls-flood concurrent-connection alert-number 10000
anti-ddos http-flood defend alert-request 5000
anti-ddos http-flood detect-uri source-statistic illegal-ratio 90 min-number 20 interval 5
anti-ddos http-flood detect-uri index 1 uri / full-matching
anti-ddos http-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos http-flood illegal-session-check
anti-ddos http-flood illegal-session-check null-method-check enable
anti-ddos http-flood illegal-session-check range-header-check enable
anti-ddos http-flood illegal-session-check multi-method-check enable
anti-ddos http-flood concurrent-connection alert-number 10000
anti-ddos tcp-connection-flood alert-number 20000
anti-ddos tcp-connection-flood alert-rate 5000
anti-ddos tcp-connection-flood illegal-session-check packet-min-number 1 interval 5
anti-ddos tcp-connection-flood illegal-session-check illegal-session-num 3 interval 5
anti-ddos dns-request-limit source-ip other max-rate 200
anti-ddos first-packet-check tcp interval upper-limit 1
anti-ddos first-packet-check udp interval upper-limit 2
anti-ddos first-packet-check syn interval lower-limit 2 upper-limit 4
anti-ddos first-packet-check syn-ack interval lower-limit 2 upper-limit 4
anti-ddos filter attack alert-rate 10000
anti-ddos source-port statistic enable
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GE0/0/0
#
firewall zone untrust
set priority 5
add interface GE0/0/3
```



```
#  
firewall zone dmz  
    set priority 50  
#  
security-policy  
    default action permit  
    rule name pass  
        action permit  
#  
return
```

9.4.7 Anti-DDoS Cleaning Device's Configuration

```
#  
sysname DDoS2-clean  
#  
firewall ddos log-local-ip 192.168.2.14  
firewall ddos log-server-ip 192.168.2.200  
anti-ddos packet-capture  
key %+%%#!!!!!!\"!!!!*!!YHRY<$&*7K`G!N'3@Pl*c1]s,f':1K*v/v"!!!!2jp5!!!!q!!!!^fM-!qSv8(-6}3-  
V01XS&EQB%Shxe@st>U~t>,uT966mF3;|CU~ys:.)y+2RK@Gl68Vr>)c9t$Qjvf(VF+f=RbVY:2\*}V+WK/Z%  
+%#  
anti-ddos packet-capture key enable  
#  
ip vpn-instance _management_vpn_  
    ipv4-family  
#  
aaa  
    authentication-scheme default  
        authentication-mode local  
    authorization-scheme default  
        authorization-mode local  
accounting-scheme default  
    accounting-mode none  
local-user policy security-enhance  
local-aaa-user password policy administrator  
domain default  
    authentication-scheme default  
    accounting-scheme default  
local-user admin123 password irreversible-cipher  
$1d$7pr`Yv7*E9ZR7.$4O2~X"[u8=C:<'SNR*)n1=[:u8=%>lgu^MZ;;LU$  
local-user admin123 privilege level 3  
local-user admin123 service-type ssh  
local-user netconf-admin password irreversible-cipher  
$1d$cu8]:DRh_/[E[+Tu$k+T]~l`0!(M"uuNX]c>G;Bgr3/~mLK#XPOG8+d*6$  
local-user netconf-admin privilege level 3  
local-user netconf-admin service-type ssh  
#  
interface MEth0/0/0  
    ip binding vpn-instance _management_vpn_  
    ip address 192.168.2.12 255.255.255.0  
#  
interface GE0/0/0  
    anti-ddos flow-statistic enable
```

```
anti-ddos clean enable
#
interface GE0/0/0.15
    ip address 1.1.1.2 255.255.255.0
    dot1q termination vid 15
    anti-ddos flow-statistic enable
    anti-ddos clean enable
#
interface GE0/0/0.20
    ip address 2.2.2.2 255.255.255.0
    dot1q termination vid 20
    anti-ddos flow-statistic enable
    anti-ddos clean enable
#
interface GE0/0/3
    ip address 192.168.2.14 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 2.2.2.1
#
snmp-agent
#
snmp-agent sys-info version v3
snmp-agent group v3 group1 privacy read-view mib2view write-view mib2view notify-view mib2view
#
snmp-agent mib-view included mib2view iso
snmp-agent usm-user v3 admin
snmp-agent usm-user v3 admin group group1
snmp-agent usm-user v3 admin authentication-mode sha2-256
cipher %+%#!!!!!!"!!!!"!!!!*!!!!YHRY<$&*7K4iqh+"a`z;<ddS4B>d&,N4+-!!!!2jp5!!!!;!!!!["]4)&5P]=b0s
Q~77]d4,O6H,vU,HLLdCiE!!!!%+%
snmp-agent usm-user v3 admin privacy-mode aes256
cipher %+%#!!!!!!"!!!!"!!!!*!!!!YHRY<$&*7K#2.!N6hqgDO>k6X7hq6Cr7pKS!!!!2jp5!!!!;!!!!x}Mm,s=RLV
pGa`"zBVt!!ciOA,fO0J-H_8I!!!!%+%
#
snmp-agent trap source GE0/0/3
#
snmp-agent protocol source-interface MEth0/0/0
undo snmp-agent protocol source-status all-interface
undo snmp-agent protocol source-status ipv6 all-interface
#
undo snmp-agent proxy protocol source-status all-interface
undo snmp-agent proxy protocol source-status ipv6 all-interface
#
stelnet server enable
snetconf server enable
undo ssh server authentication-type keyboard-interactive enable
ssh user admin123
ssh user admin123 authentication-type password
ssh user admin123 service-type stelnet
ssh user netconf-admin
ssh user netconf-admin authentication-type all
ssh user netconf-admin service-type all
ssh server-source -i MEth0/0/0
undo ssh server-source all-interface
undo ssh ipv6 server-source all-interface
```

```
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey dsa ecc rsa
#
ssh server dh-exchange min-len 1024
#
ssh client publickey rsa_sha2_256 rsa_sha2_512
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh client hmac sha2_512 sha2_256
ssh client key-exchange dh_group_exchange_sha256
#
user-interface vty 0 14
    authentication-mode aaa
    user privilege level 3
    protocol inbound ssh
#
netconf
    protocol inbound ssh ipv4 port 830
#
nacm
    nacm enable
    execute-default permit
    group-name nacm-group
    user-name netconf
#
anti-ddos filter name attack type ip
    source-ip ip 20.20.20.0 24
    filter-id 5
#
ddos-zone name zone_16
    zone-id 16
    ip address 172.16.30.0 24
    ip address 10.10.10.0 24
    ip address 4.4.4.2 32
    anti-ddos destination-ip session-limit protocol udp max-speed 10000
    bandwidth-limit destination-ip type udp max-speed 50000
    bandwidth-limit destination-ip type icmp max-speed 1
    bandwidth-limit destination-ip type tcp-fragment max-speed 1000
    bandwidth-limit destination-ip type udp-fragment max-speed 1000
    bandwidth-limit destination-ip type other max-speed 100000
    anti-ddos rst-flood session-check
    anti-ddos syn-flood source-detect mode advanced
    anti-ddos tcp-abnormal-flood alert-rate 500
    anti-ddos syn-flood source-limit max-number 20 duration 3
    anti-ddos dns format-check alert-rate 500
    anti-ddos dns-request-flood source-detect
    anti-ddos ack-flood session-check
    anti-ddos udp-flood fingerprint-learn enable
    anti-ddos udp-malformed-flood alert-rate 500
    anti-ddos udp-flood defend alert-speed 500
```

```
anti-ddos https-flood defend alert-rate 20000
anti-ddos https-flood ssl-defend illegal-session-num 3 interval 5
anti-ddos https-flood ssl-defend incomplete-negotiation enable
anti-ddos tls-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos tls-flood fixed-resource illegal-ratio 90 min-number 20 interval 5
anti-ddos tls-flood concurrent-connection alert-number 10000
anti-ddos http-flood defend alert-request 5000
anti-ddos http-flood detect-uri source-statistic illegal-ratio 90 min-number 20 interval 5
anti-ddos http-flood detect-uri index 1 uri / full-matching
anti-ddos http-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos http-flood illegal-session-check
anti-ddos http-flood illegal-session-check null-method-check enable
anti-ddos http-flood illegal-session-check range-header-check enable
anti-ddos http-flood illegal-session-check multi-method-check enable
anti-ddos http-flood concurrent-connection alert-number 10000
anti-ddos tcp-connection-flood alert-number 20000
anti-ddos tcp-connection-flood alert-rate 5000
anti-ddos tcp-connection-flood illegal-session-check packet-min-number 1 interval 5
anti-ddos tcp-connection-flood illegal-session-check illegal-session-num 3 interval 5
anti-ddos dns-request-limit source-ip other max-rate 200
anti-ddos first-packet-check tcp interval upper-limit 1
anti-ddos first-packet-check udp interval upper-limit 2
anti-ddos first-packet-check syn interval lower-limit 2 upper-limit 4
anti-ddos first-packet-check syn-ack interval lower-limit 2 upper-limit 4
anti-ddos filter attack alert-rate 10000
anti-ddos source-port statistic enable
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
#
firewall zone untrust
    set priority 5
    add interface GE0/0/0
    add interface GE0/0/0.15
    add interface GE0/0/0.20
    add interface GE0/0/3
#
firewall zone dmz
    set priority 50
#
security-policy
    default action permit
    rule name pass
        action permit
#
return
```

9.5 Quiz

1. Describe the direction of traffic from Attack PC to WWW Server.

Answer: Attack PC -> SW1 -> Mirro-SW -> RT1 -> Anti-DDoS (cleaning device) -> RT1 -> FW1 -> SW1 -> WWW Server.

2. When the anti-DDoS device configuration is cleared and the devices are reconfigured, the SecoManager cannot manage the anti-DDoS devices. What are the possible causes?

Answer: SNMP, NETCONF, and STelnet usernames and passwords on the SecoManager and the anti-DDoS devices should be the same for device management. Check whether the usernames and passwords are the same. After the STelnet user names and passwords are created on anti-DDoS devices, the passwords must be changed upon the first login. The passwords configured on the SecoManager must be the same as the new passwords set on the anti-DDoS devices.

10 Vulnerability Defense

10.1 Introduction

10.1.1 About This Lab

On an enterprise network, the enterprise server provides web services for external users. Authorized Internet users can access web server resources on the intranet. However, unauthorized Internet users may exploit SQL injection vulnerabilities to access data in the database on the intranet without authorization and steal users' personal information, causing information leakage. Therefore, the intrusion prevention function should be configured on the firewall to defend against SQL injection attacks (initiated by Internet users) targeting the web server on the enterprise intranet.

10.1.2 Objectives

- Understand the principles and exploitation methods of SQL injection vulnerabilities in Hypertext Preprocessor (PHP) through Damn Vulnerable Web Application (DVWA) instances.
- Understand how to configure the intrusion prevention function on the firewall for threat prevention.

10.1.3 Networking Topology

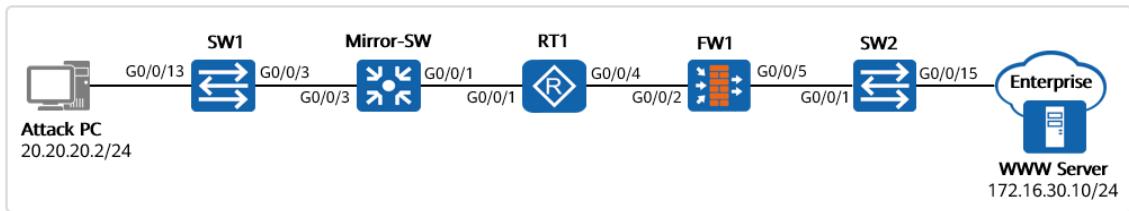


Figure 10-1 Vulnerability and threat prevention

The preceding figure shows device connections. For details about IP address planning, see Table 10-1.

FW1 functions as the enterprise egress gateway. Attack PC simulates an attacker to initiate an SQL injection attack to the web server on the intranet. A signature filter is configured on the FW1 device for attack prevention.

The configurations of RT1 is not described in the configuration procedure. For details, see 10.3 Configuration Reference.

10.1.4 Lab Planning

Table 10-1 Interface planning

Device	Interface	Interface Type	IP Address	Description
FW1	G0/0/2	Layer 3 interface	10.1.3.2/30 Security zone: Untrust	Interface for connecting to RT1
	G0/0/5	Layer 3 interface	172.16.30.1/24 Security zone: Trust	Interface for connecting to the SW2 device
Attack PC	Ethernet0	Network adapter	20.20.20.2/24 Gateway: 20.20.20.1/24	Terminal
WWW Server	Ethernet0	Network adapter	172.16.30.10/24	Terminal
RT1	G0/0/1	Layer 3 interface	20.20.20.1/24	Interface for connecting to Mirror-SW and the interface IP address is the gateway IP address of Attack PC.
	G0/0/4	Layer 3 interface	10.1.3.1/30	Interface for connecting to FW1

10.2 Lab Configuration

10.2.1 Configuration Roadmap

1. Configure interface IP addresses, security zones, and basic network parameters to ensure that Attack PC can communicate with WWW Server.
2. Use SQL statements to test whether there are any injection points and determine the injection type.
3. Use SQL statements to query the database and version information.
4. Update the IPS signature database, create an IPS profile, and configure a signature filter.
5. Configure a security policy and invoke an IPS profile.

Note: For details about network configurations, see the pre-configurations in this lab. This chapter describes only the SQL injection vulnerability test and the process of intrusion prevention.

10.2.2 Configuration Procedure on the Web UI

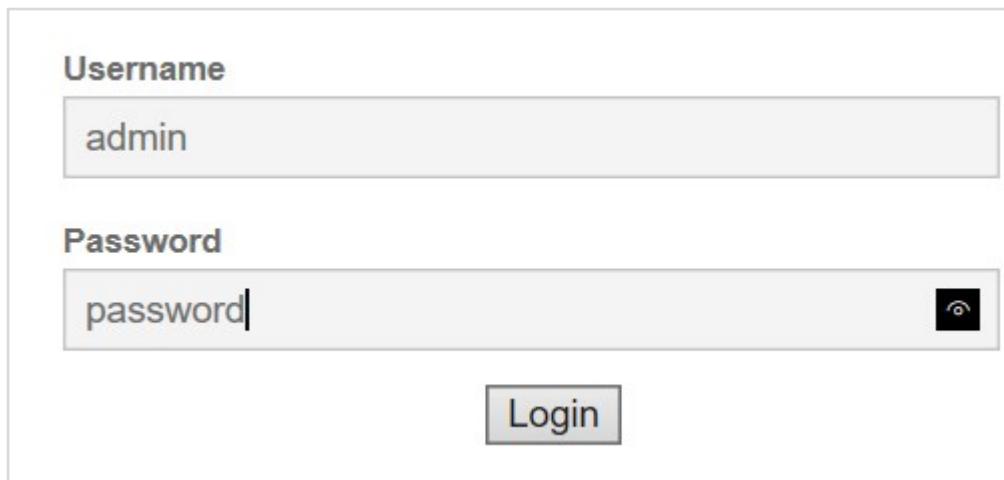
Step 1 Set basic network parameters.

Set basic network parameters according to the table in 10.1.4 Lab Planning.

RT1 has been pre-configured. For details, see 10.3 Configuration Reference.

Step 2 Log in to the DVWA system.

On Attack PC, enter `http://172.16.30.10:8080` in the address bar of the browser to open the DVWA system. Enter the user name **admin** and password **password** for login as shown in the following figure.



The image shows a screenshot of a web browser displaying the DVWA login page. It features two input fields: one for 'Username' containing 'admin' and another for 'Password' containing 'password'. To the right of the password field is a small icon of a key with a lock. Below these fields is a 'Login' button.

Step 3 Adjust the security level.

After login, change the DVWA security level to **low** as shown in the following figure.

DVWA Security 

Security Level

Security level is currently: low.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and has no security measures at all. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge for users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low
Low
 Medium
 High
 Impossible

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

Step 4 Choose SQL Injection for ID query.

Enter a correct user ID (for example, 1) and click Submit. The First name and Surname of the ID are displayed.

Vulnerability: SQL Injection

User ID:

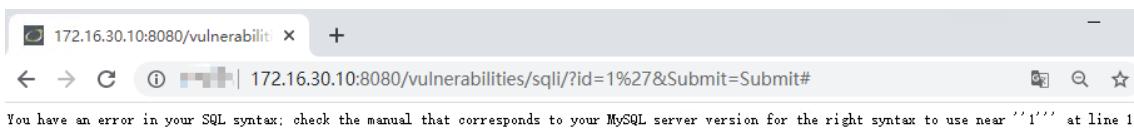
ID: 1
 First name: admin
 Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

Step 5 Detect SQL injection vulnerabilities.

Enter the user ID 1. The user name and password can be returned normally. Add ' after 1.



The screenshot shows a browser window with the URL `172.16.30.10:8080/vulnerabilities/sql/`. The page displays an error message: "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' at line 1".

An error is reported, indicating that an injection point exists.

Step 6 Determine the SQL injection type.

Determine whether the injection is a character injection or numeric injection according to the following steps:

Enter **1 and 1=1** at the injection point.

Vulnerability: SQL Injection

User ID: Submit

ID: 1 and 1=1
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

The data is successfully returned. Then, enter **1 and 1=2** at the injection point.

Vulnerability: SQL Injection

User ID: Submit

ID: 1 and 1=2
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

The data is still successfully returned. Therefore, the injection is not a numeric injection because the return value is not affected by numbers.

Enter **0' or 1#** at the injection point to determine whether the injection is a character injection.

Vulnerability: SQL Injection

User ID: Submit

ID: 0' or 1#
First name: admin
Surname: admin

ID: 0' or 1#
First name: Gordon
Surname: Brown

ID: 0' or 1#
First name: Hack
Surname: Me

ID: 0' or 1#
First name: Pablo
Surname: Picasso

ID: 0' or 1#
First name: Bob
Surname: Smith

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

All the contents in the database can be queried. Therefore, the injection is a character injection.

Step 7 Query the length of the information list.

Use the **order by [num]** statement to query the length of the information list. Enter 1'
order by 1#.

Vulnerability: SQL Injection

User ID: Submit

ID: 1' order by 1#
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

The data is properly displayed on the result page. Enter 1' **order by 2#**.

Vulnerability: SQL Injection

User ID: Submit

ID: 1' order by 2#
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

The data is properly displayed on the result page. Enter 1' order by 3#.



When 3 is entered, an error message is displayed. The preceding figure shows the error information. Therefore, it is determined that the length of the query result is two columns.

Step 8 Query the current database user and database name.

Craft the ' union select user(),database()# statement to query the current database user and database name.

Vulnerability: SQL Injection

User ID: Submit

ID: ' union select user(),database()#
First name: root@localhost
Surname: dvwa

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

The result indicates that the current database user is **root@localhost** and the database name is **dvwa**.

Step 9 Query the current database version.

Craft the 1' and 1=2 union select version(),database()# statement to query the current database version.

Vulnerability: SQL Injection

User ID: Submit

ID: 1' and 1=2 union select version(),database()#
First name: 5.7.26
Surname: dvwa

More Information

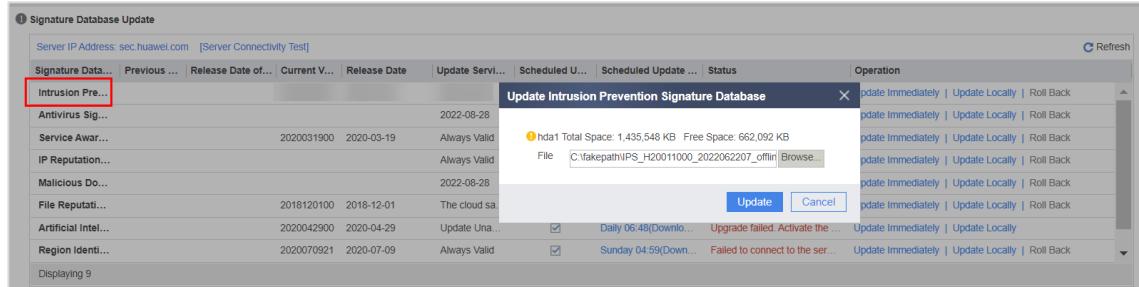
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

As shown in the preceding figure, the database version is 5.7.26.

Attackers may exploit SQL injection vulnerabilities to access data in the database without authorization and steal users' personal information, causing information leakage. As a security vulnerability that occurs most frequently and is highly threatening, SQL injection vulnerabilities are extensive, covert, harmful, and easy to operate. Therefore, we need to defend against injection attacks to protect enterprise and user information.

Step 10 Update the IPS signature database.

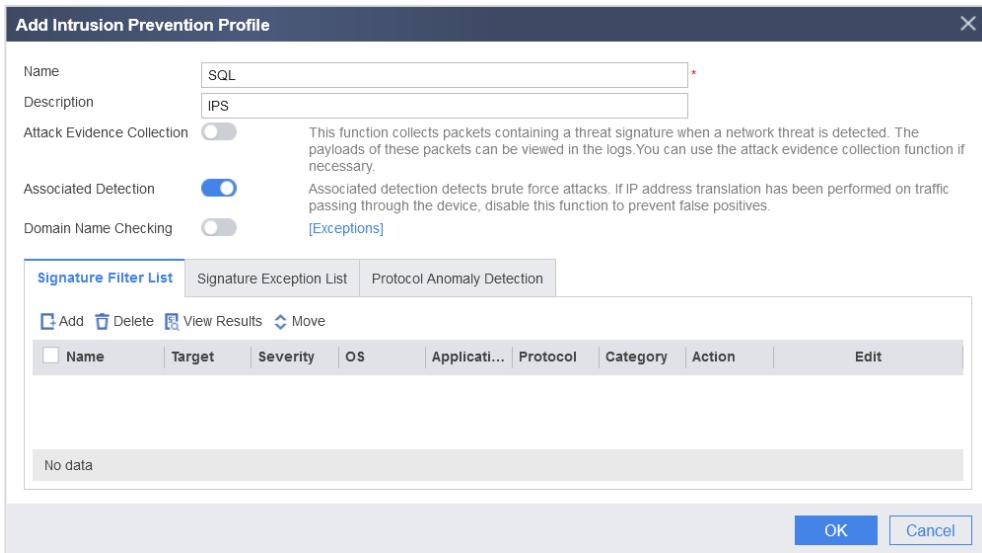
Choose **System > Update Center > Signature Database Update**, select the row where the IPS signature database resides, click **Update Locally**, import the IPS signature database, and click **Update** as shown in the following figure.



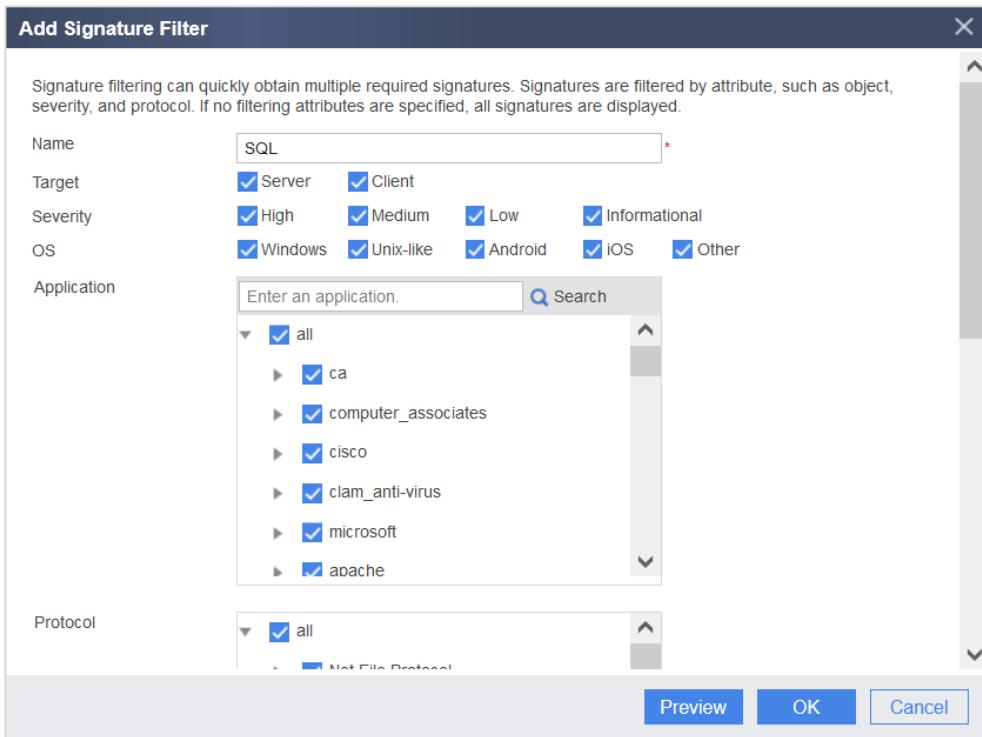
Note: The IPS signature database can be updated only after the license is loaded.

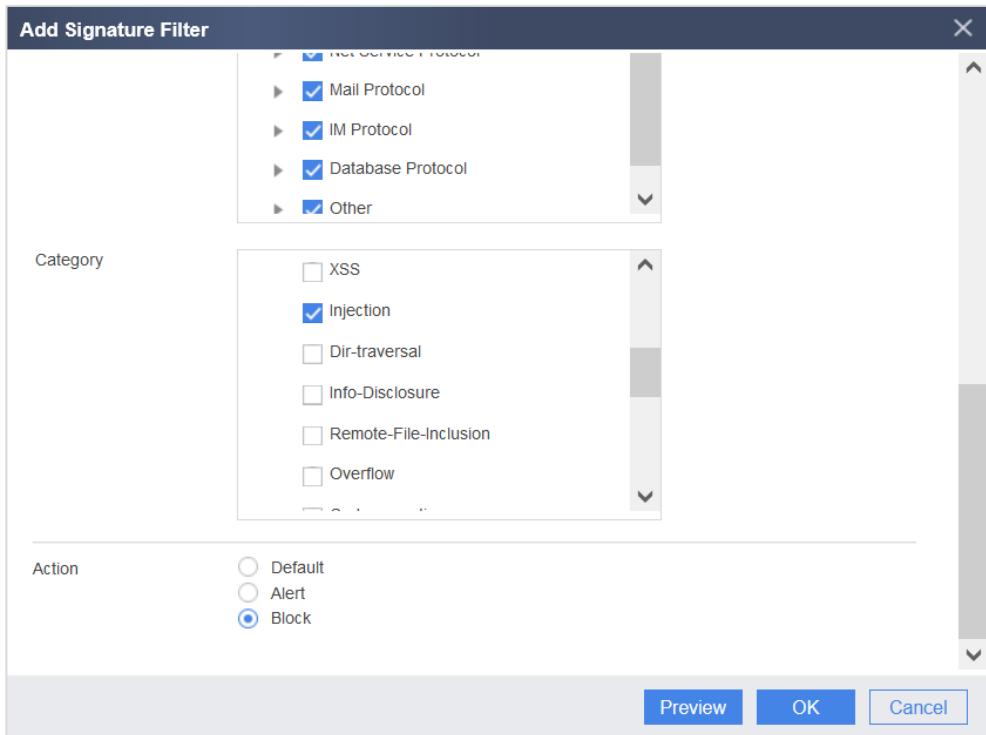
Step 11 Create an IPS profile and configure a signature filter.

Choose **Object > Security Profiles > Intrusion Prevention**. On the **Intrusion Prevention Profile List** page, click **Add** and enter the name and description as shown in the following figure.

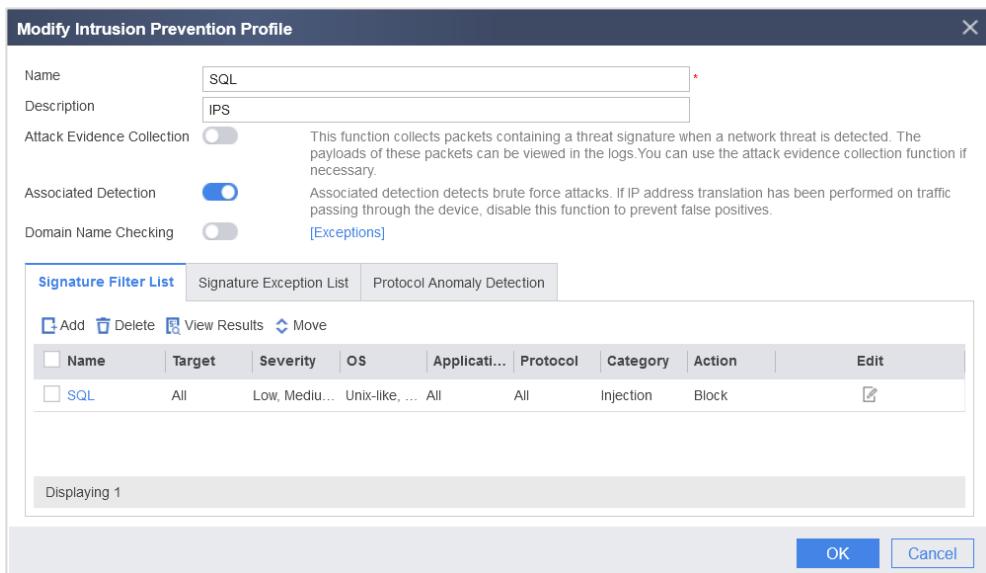


Click the **Signature Filter List** tab, click **Add**, and set parameters as shown in the following figures.

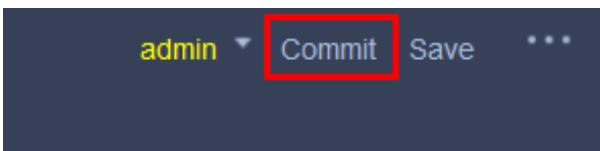




Click **OK** to complete the configuration of the web signature filter. The result is shown in the following figure.

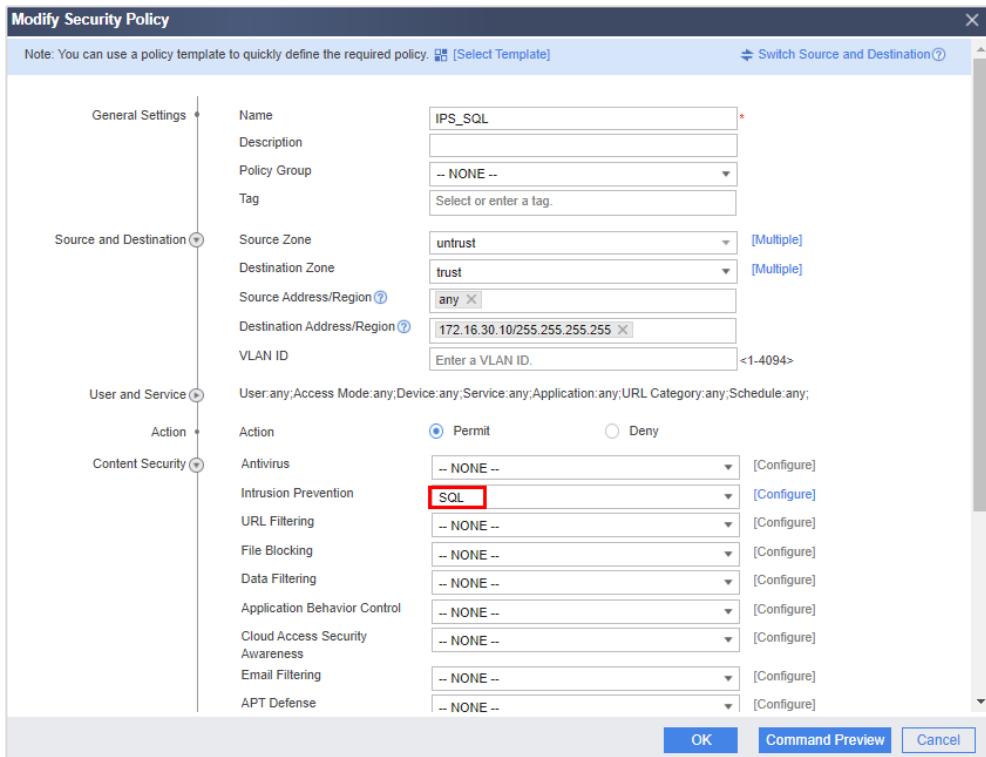


Click **Commit** in the upper right corner to make the configurations take effect.



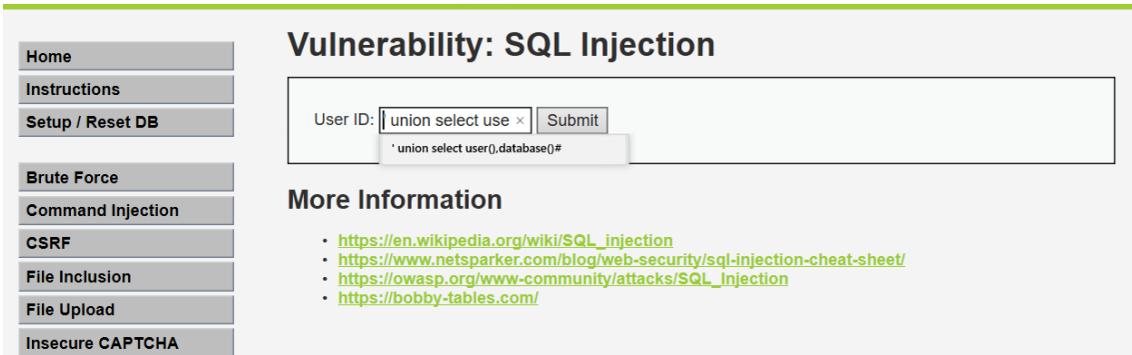
Step 12 Invoke an IPS profile.

Choose Policy > Security Policy > Security Policy. On the Security Policy List tab page, click Add Security Policy. Set or select parameters to protect the intranet server against attacks from external users as shown in the following figure.



10.2.3 Verification

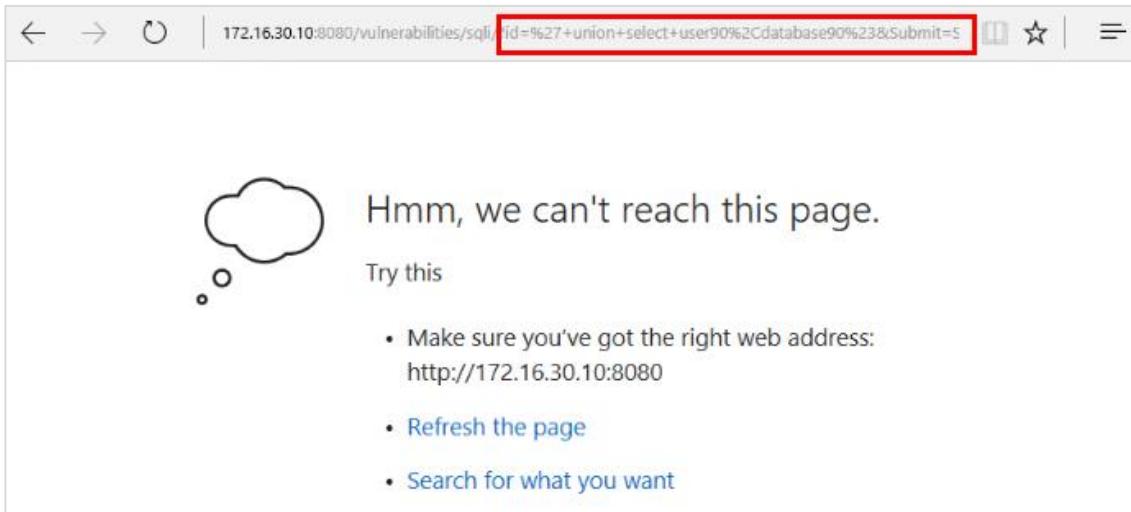
On Attack PC, access the DVWA page and use the ' union select user(),database()#' statement to query the current database user and database name.



The screenshot shows the DVWA SQL Injection page. On the left, there's a sidebar with links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, and Insecure CAPTCHA. The main area has a title 'Vulnerability: SQL Injection'. Below it, a form has a 'User ID' input field containing the SQL injection payload: 'union select user(),database()#'. A 'Submit' button is next to the input field. Below the input field, the same payload is also displayed in a smaller text area. To the right of the input field, there's a 'More Information' section with a bulleted list of links:

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

The page is blocked by the IPS device as shown in the following figure.



Query threat logs on the IPS device as shown in the following figure.

Threat ID	Threat Name	Occurrences	CVE Number	Source Zone	Destination Zone	Attacker	Attack Target	Source Address...	Destination Address...	Application
20091427	SQL Injection Attempt - Cross-Table Query(union select) 3	1	NA	untrust	trust	20.20.20.2	172.16.30.10	20.20.20.2.56254	172.16.30.10:8080	HTTP
20091427	SQL Injection Attempt - Cross-Table Query(union select) 1	1	NA	untrust	trust	20.20.20.2	172.16.30.10	20.20.20.2.56254	172.16.30.10:8080	HTTP
20091427	SQL Injection Attempt - Cross-Table Query(union select) 3	1	NA	untrust	trust	20.20.20.2	172.16.30.10	20.20.20.2.56243	172.16.30.10:8080	HTTP

Click a threat name to view detailed information as shown in the following figure.

SQL Injection Attempt - Cross-Table Query(union select) 1

Threat ID:	2000132	CVSS:	NA
CVE:	NA	Severity:	High
Release Date:		Updated Date:	
Version:	2	CNNVD:	NA
Vendor ID:	NA		

Vulnerability Description
This alert indicates that an attacker tried to exploit a SQL injection vulnerability. The flaw is due to insufficient sanitizing of user input. A remote authenticated attacker may exploit this vulnerability by sending a crafted HTTP request to the target server. A successful exploitation of this vulnerability may lead to execution of arbitrary SQL queries within the database in the security context of the application's database connection.

Suggested Treatment
1.Add firewall rules to filter out malicious SQL commands sent to an database server. 2.Restrict access to database servers to trusted users only.

Reference Link
https://www.owasp.org/index.php/SQL_Injection

10.3 Configuration Reference

10.3.1 RT1's Pre-configuration

```
#  
sysname R1  
#  
interface GigabitEthernet0/0/1  
undo portswitch  
ip address 20.20.20.1 255.255.255.0
```

```
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.1.3.1 255.255.255.0
#
ip route-static 172.16.30.0 255.255.255.0 10.1.3.2
#
```

10.3.2 FW1's Configuration

```
#
sysname FW1
#
interface GigabitEthernet0/0/2
undo shutdown
ip address 10.1.3.2 255.255.255.0
#
interface GigabitEthernet0/0/5
undo shutdown
ip address 172.16.30.1 255.255.255.0
#
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/2
#
#
ip route-static 0.0.0.0 0.0.0.0 10.1.3.1
#
#
profile type ips name SQL
description IPS
signature-set name SQL
action block
os unix-like windows android ios other
target both
severity low medium high information
protocol all
category Injection
#
security-policy
default action permit
rule name IPS_SQL
policy logging
session logging
traffic logging enable
source-zone untrust
destination-zone trust
destination-address 172.16.30.10 mask 255.255.255.255
profile ips SQL
rule name www
```

```
source-zone untrust  
destination-zone trust  
action permit  
rule name outside  
source-zone trust  
destination-zone untrust  
action permit  
#
```

10.4 Quiz

Is a license required for intrusion prevention?

Answer: Before updating a signature database, ensure that the license for the update service has been purchased and activated.

11 Content Security Filtering

11.1 Introduction

11.1.1 About This Lab

On an enterprise network, employees need to access the Internet. To control the Internet access permissions of employees, the enterprise wants to use the URL filtering, file blocking, and data filtering functions of the firewall to meet the following requirements:

URL filtering prevents employees from accessing game portal websites such as www.example.com, improving work efficiency and preventing a great amount of bandwidth consumption.

File blocking blocks the download of executable files from the Internet, reducing the risk of information leakage and virus infection on the intranet.

Data filtering filters files or applications that contain confidential information, reducing the risk of leakage.

11.1.2 Objectives

- Learn how to configure URL filtering, file blocking, and data filtering on the CLI and web UI.

11.1.3 Networking Topology

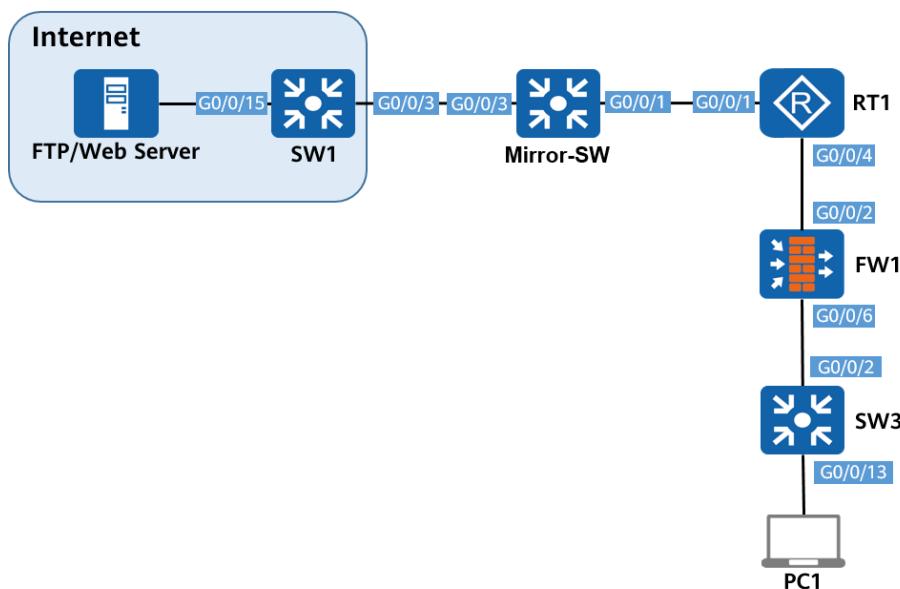


Figure 11-1 Topology for configuring firewall content security

The preceding figure shows device connections. For details about IP address planning, see Table 11-1 in 11.1.4 Lab Planning.

SW1 simulates the Internet, and the firewall functions as the enterprise security gateway to filter content for intranet users to ensure enterprise information security.

The configurations of SW1, SW3, Mirror-SW, and RT1 are not described in the configuration procedure. For details, see 11.4 Configuration Reference.

11.1.4 Lab Planning

Table 11-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
FW1	G0/0/2	Layer 3 interface	100.3.1.2/30 Security zone: Untrust	Interface for connecting to R1
	G0/0/6	Layer 3 interface	172.16.20.2/24 Security zone: Trust	Interface for connecting to SW3 and functioning as the gateway of PC1
RT1	G0/0/1.2	Layer 3 interface	4.4.4.2/30	Interface for connecting to Mirror-SW
	G0/0/4	Layer 3 interface	100.3.1.1/30	Interface for connecting to FW1
SW1	G0/0/15	Access	PVID: 1003	Interconnection interface – interface for connecting to FTP/web server
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 1003	Interface for connecting to Mirror-SW
	VLANIF 2	Layer 3 interface	4.4.4.1/30	On the same network segment as an RT1 interface
	VLANIF 1003	Layer 3 interface	172.17.100.1/24	Gateway of the server
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2	Interconnection interface
	G0/0/3			

SW3	G0/0/2	Access	PVID: 40	Interface for connecting to FW1
	G0/0/13	Access	PVID: 40	Interface for connecting to PC1
FTP/Web Server	Ethernet 0	NIC	172.17.100.10/24 Gateway: 172.17.100.1/24	Endpoint
PC1	Ethernet 0	NIC	172.16.20.111/24 Gateway: 172.16.20.2/24	Endpoint

11.2 Lab Configuration

11.2.1 Configuration Roadmap

1. Configure IP addresses for interfaces, add the interfaces to security zones, and complete basic parameter settings.
2. Configure a user-defined URL category and set the URLs to be filtered out.
3. Configure a URL filtering security profile, and set the default action and user-defined URL category action.
4. Configure a security policy and invoke a URL filtering security profile.
5. Configure a file blocking security profile and set the file type, policy direction, and policy action.
6. Configure a data filtering keyword group and set matching types, keywords, and the keyword weight.
7. Configure a data filtering security profile, associate the data filtering keyword group with the profile, and set the direction and action.
8. Configure a security policy and invoke the file blocking security profile and data filtering security profile.

11.2.2 Configuration Procedure on the CLI

Step 1 Set basic network parameters.

Set basic network parameters according to the table in 11.1.4 Lab Planning.

SW1, SW3, Mirror-SW, and RT1 have been preconfigured. For details, see section 11.4 Configuration Reference.

Configure the IP address for GigabitEthernet0/0/2 of FW1, and add the interface to the Untrust zone.

```
<FW1> system-view
```

```
[FW1] interface GigabitEthernet0/0/2
[FW1-GigabitEthernet0/0/2] ip address 100.3.1.2 255.255.255.252
[FW1-GigabitEthernet0/0/2] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface GigabitEthernet0/0/2
[FW1-zone-untrust] quit
```

Configure the IP address for GigabitEthernet0/0/6, and add the interface to the Trust zone.

```
[FW1] interface GigabitEthernet0/0/6
[FW1-GigabitEthernet0/0/5] ip address 172.16.20.2 255.255.255.0
[FW1-GigabitEthernet0/0/5] quit
[FW1] firewall zone trust
[FW1-zone-trust] add interface GigabitEthernet0/0/6
[FW1-zone-trust] quit
```

Step 2 Configure user-defined URL categories.

```
[FW1] url-filter category user-defined name "illegal website"
[FW1-cate-user-defined-illegal website] add url 172.17.100.10/illegal/game.html
[FW1-cate-user-defined-illegal website] quit
```

Step 3 Configure a URL filtering security profile.

```
[FW1] profile type url-filter name url_profile
[FW1-profile-url-filter-url_profile] category user-defined name "illegal website" action block
[FW1-profile-url-filter-url_profile] quit
```

Step 4 Invoke a URL filtering security profile.

Configure a security policy and invoke the URL filtering security profile.

```
[FW1] security-policy
[FW1-policy-security] rule name sec_url_policy
[FW1-policy-security-rule-sec_url_policy] source-zone trust
[FW1-policy-security-rule-sec_url_policy] destination-zone untrust
[FW1-policy-security-rule-sec_url_policy] source-address 172.16.20.111 24
[FW1-policy-security-rule-sec_url_policy] profile url-filter url_profile
[FW1-policy-security-rule-sec_url_policy] action permit
[FW1-policy-security-rule-sec_url_policy] quit
[FW1-policy-security] quit
```

Step 5 Configure a NAT policy.

Configure a NAT policy to translate the source IP address of the client into the IP address of an outbound interface on FW1 to access the Internet.

```
[FW1] nat-policy
[FW1-policy-nat] rule name trust-untrust
[FW1-policy-nat-rule-trust-untrust] source-zone trust
[FW1-policy-nat-rule-trust-untrust] destination-zone untrust
[FW1-policy-nat-rule-trust-untrust] action source-nat easy-ip
```

```
[FW1-policy-nat-rule-trust-untrust] quit  
[FW1-policy-nat] quit
```

Step 6 Configure a file blocking security profile.

```
[FW1] profile type file-block name profile  
[FW1-profile-file-block-profile] rule name download  
[FW1-profile-file-block-profile-rule-download] file-type pre-defined name EXE MSI RPM OCX A ELF  
DLL PE SYS  
[FW1-profile-file-block-profile-rule-download] application all  
[FW1-profile-file-block-profile-rule-download] direction download  
[FW1-profile-file-block-profile-rule-download] action block  
[FW1-profile-file-block-profile-rule-download] quit  
[FW1-profile-file-block-profile] quit
```

Step 7 Configure a data filtering keyword group.

```
[FW1] keyword-group name secret  
[FW1-keyword-group-secret] user-defined-keyword name secret  
[FW1-keyword-group-secret-keyword-secret] expression match-mode text secret  
[FW1-keyword-group-secret-keyword-secret] weight 1  
[FW1-keyword-group-secret-keyword-secret] quit  
[FW1-keyword-group-secret] quit
```

Step 8 Configure a data filtering security profile.

```
[FW1] profile type data-filter name secret  
[FW1-profile-data-filter-secret] rule name secret  
[FW1-profile-data-filter-secret-rule-secret] keyword-group name secret  
[FW1-profile-data-filter-secret-rule-secret] file-type all  
[FW1-profile-data-filter-secret-rule-secret] application all  
[FW1-profile-data-filter-secret-rule-secret] action block  
[FW1-profile-data-filter-secret-rule-secret] quit  
[FW1-profile-data-filter-secret] quit
```

Step 9 Invoke file blocking/data filtering.

```
# Configure a security policy and invoke the file blocking security profile and data filtering security profile.
```

```
[FW1] security-policy  
[FW1-policy-security] rule name sec_filter  
[FW1-policy-security-rule-sec_filter] source-zone trust  
[FW1-policy-security-rule-sec_filter] destination-zone untrust  
[FW1-policy-security-rule-sec_filter] profile data-filter secret  
[FW1-policy-security-rule-sec_filter] profile file-block profile  
[FW1-policy-security-rule-sec_filter] action permit  
[FW1-policy-security-rule-sec_filter] quit  
[FW1-policy-security] quit
```

Step 10 Configuring a default route.

Configure a default route so that intranet traffic can be normally forwarded to a router on the Internet.

```
[FW1] ip route-static 0.0.0.0 0.0.0.0 100.3.1.1
```

11.2.3 Configuration Procedure on the Web UI

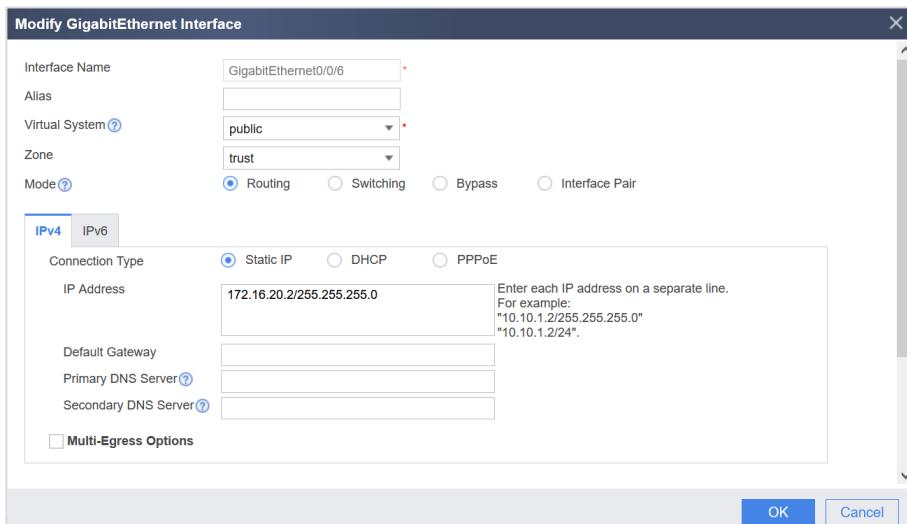
Step 1 Set basic network parameters.

Set basic network parameters according to the table in section 11.1.4 Lab Planning.

SW1, SW3, Mirror-SW, and RT1 have been preconfigured. For details, see section 11.4 Configuration Reference.

Configure interfaces on FW1. Configure IP addresses for the interfaces and add the interfaces to security zones.

Choose **Network > Interface** and click  next to the interface to be configured. Select or set parameters and click **OK** to configure GigabitEthernet0/0/6, as shown in the following figure.



GigabitEthernet0/0/2 on FW1 is configured in the same way.

Step 2 Configure user-defined URL categories.

Choose **Object > URL Category** and click **Add**. Set parameters and enter a URL to be filtered.

Add URL Category

Name	illegal website
Description	Websites that employees are prohibited from accessing
URL ?	172.17.100.10/illegal/game.html
Host ?	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

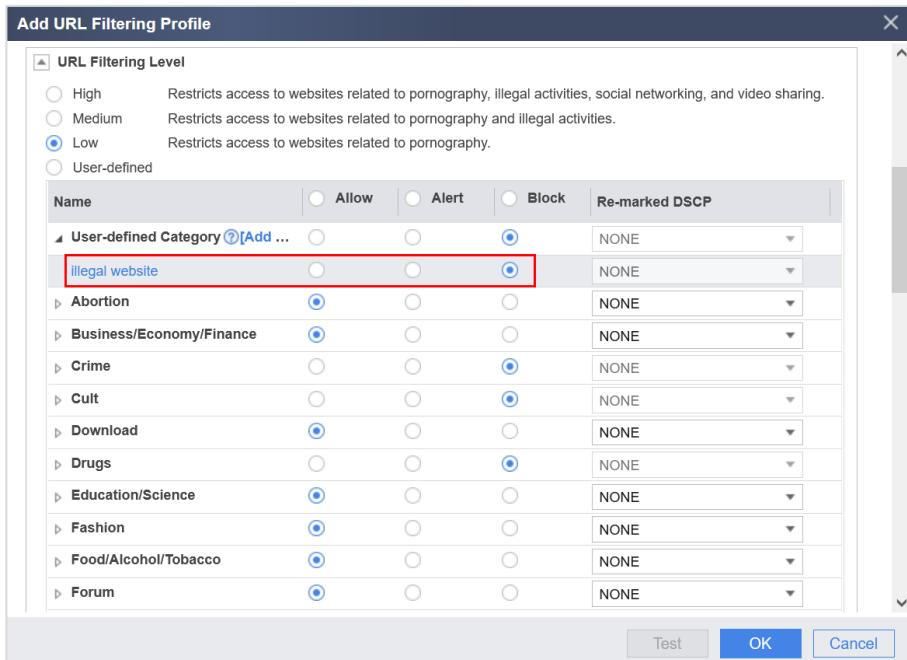
Step 3 Configure URL filtering.

Configure a URL filtering security profile, and set the default action and user-defined URL category action.

Choose **Object > Security Profiles > URL Filtering** and click **Add**. Select or enter the parameters and set **Default Action** to **Block**.

Add URL Filtering Profile

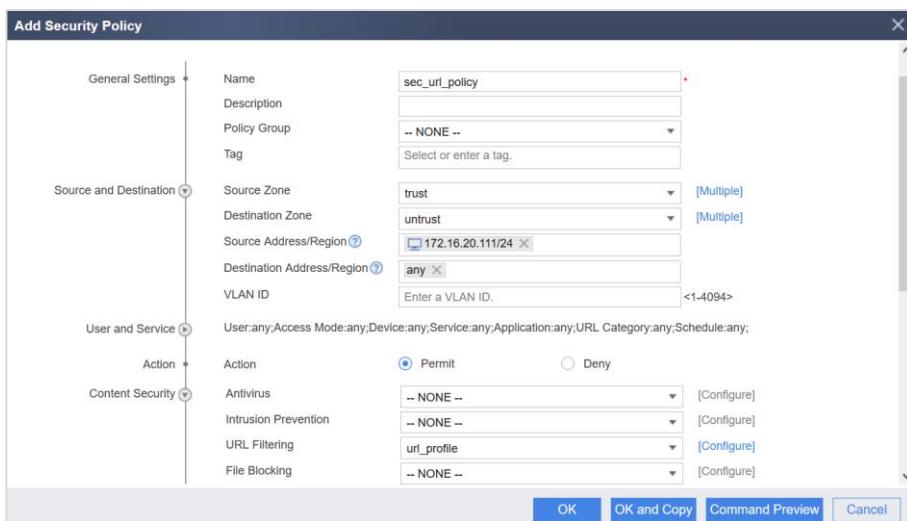
Name	url_profile										
Description											
Filter Encrypted Traffic	<input checked="" type="checkbox"/> This function facilitates URL filtering on encrypted HTTPS traffic.										
Default Action	Allow										
Malicious URL Detection	<input checked="" type="checkbox"/> This function blocks access to malicious URLs. Enabling remote URL query further enhances its effectiveness.										
Type	<table border="1"> <thead> <tr> <th></th> <th>Whitelist</th> <th>Blacklist</th> </tr> </thead> <tbody> <tr> <td>URL ?</td> <td>Whitelist entries take precedence over blacklist entries.</td> <td>Whitelist entries take precedence over blacklist entries.</td> </tr> <tr> <td>Host ?</td> <td>Whitelist entries take precedence over blacklist entries.</td> <td>Whitelist entries take precedence over blacklist entries.</td> </tr> </tbody> </table>			Whitelist	Blacklist	URL ?	Whitelist entries take precedence over blacklist entries.	Whitelist entries take precedence over blacklist entries.	Host ?	Whitelist entries take precedence over blacklist entries.	Whitelist entries take precedence over blacklist entries.
	Whitelist	Blacklist									
URL ?	Whitelist entries take precedence over blacklist entries.	Whitelist entries take precedence over blacklist entries.									
Host ?	Whitelist entries take precedence over blacklist entries.	Whitelist entries take precedence over blacklist entries.									
<input type="checkbox"/> URL Filtering Level <input type="checkbox"/> Advanced Settings											
<input type="button" value="Test"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>											



Step 4 Invoke URL filtering.

Configure a security policy to allow packet exchange between a specified internal network segment and the Internet, and configure content security URL filtering.

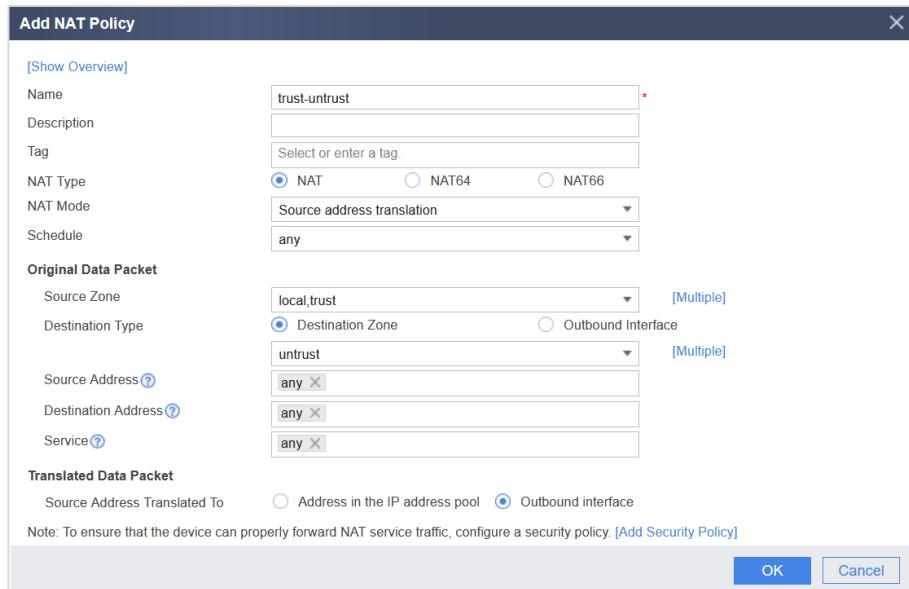
Choose **Policy > Security Policy > Security Policy** and click **Add Security Policy**. Set parameters, configure a security policy to allow packet exchange between a specified intranet segment and the Internet, and configure URL filtering.



Step 5 Configure a NAT policy.

Configure a NAT policy to translate the source IP address of the client into the IP address of an outbound interface on FW1 to access the Internet.

Choose **Policy > NAT Policy > NAT Policy** and click **Add**. Set parameters for the NAT policy.



Add NAT Policy

Name: trust-untrust *

Description:

Tag: Select or enter a tag

NAT Type: NAT NAT64 NAT66

NAT Mode: Source address translation

Schedule: any

Original Data Packet

Source Zone: local_trust [Multiple]

Destination Type: Destination Zone Outbound Interface

Source Address: untrust [Multiple]

Destination Address: any

Service: any

Translated Data Packet

Source Address Translated To: Address in the IP address pool Outbound interface

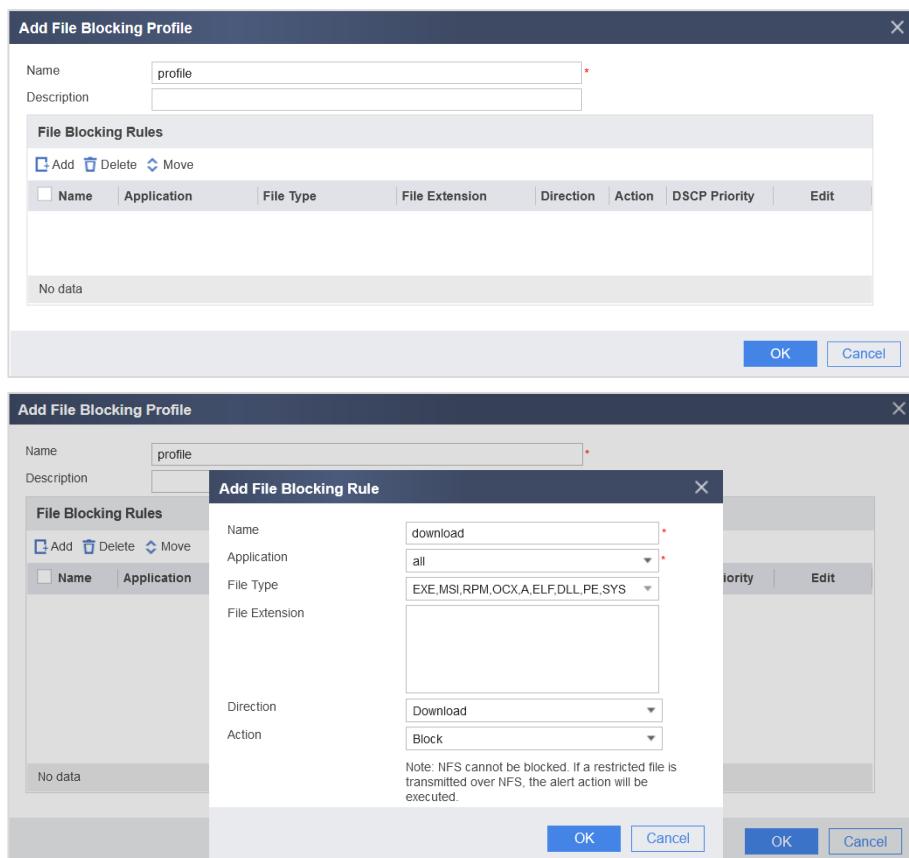
Note: To ensure that the device can properly forward NAT service traffic, configure a security policy. [\[Add Security Policy\]](#)

OK Cancel

Step 6 Configure file blocking/data filtering.

Configure a security profile to block the download of executable files from the Internet.

Choose Object > Security Profiles > File Blocking and click Add. Set the download direction. Set File Type to Executable File, Direction to Download, and Action to Block.



Add File Blocking Profile

Name: profile *

Description:

File Blocking Rules

Add Delete Move

Name	Application	File Type	File Extension	Direction	Action	DSCP Priority	Edit
No data							

OK Cancel

Add File Blocking Rule

Name: download *

Application: all

File Type: EXE,MSI,RPM,Ocx,A,ELF,DLL,PE,SYS

Direction: Download

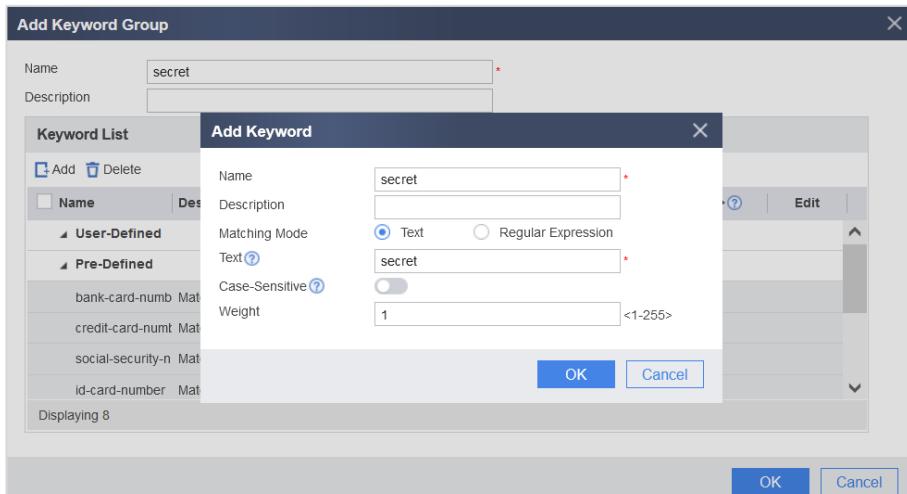
Action: Block

Note: NFS cannot be blocked. If a restricted file is transmitted over NFS, the alert action will be executed.

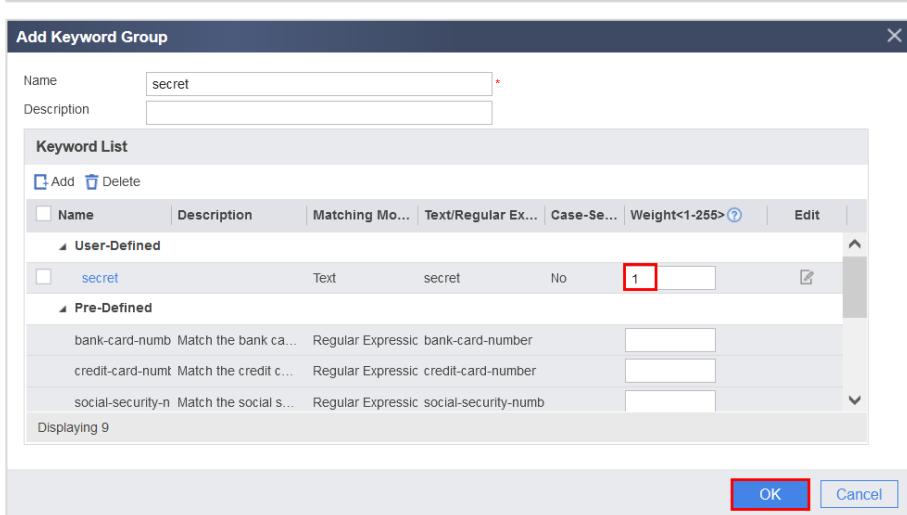
Priority Edit

OK Cancel

Choose Object > Keyword Group and click Add. Choose Keyword List > Add. Set Matching Mode to Text, Text to secret, and Weight to 1.

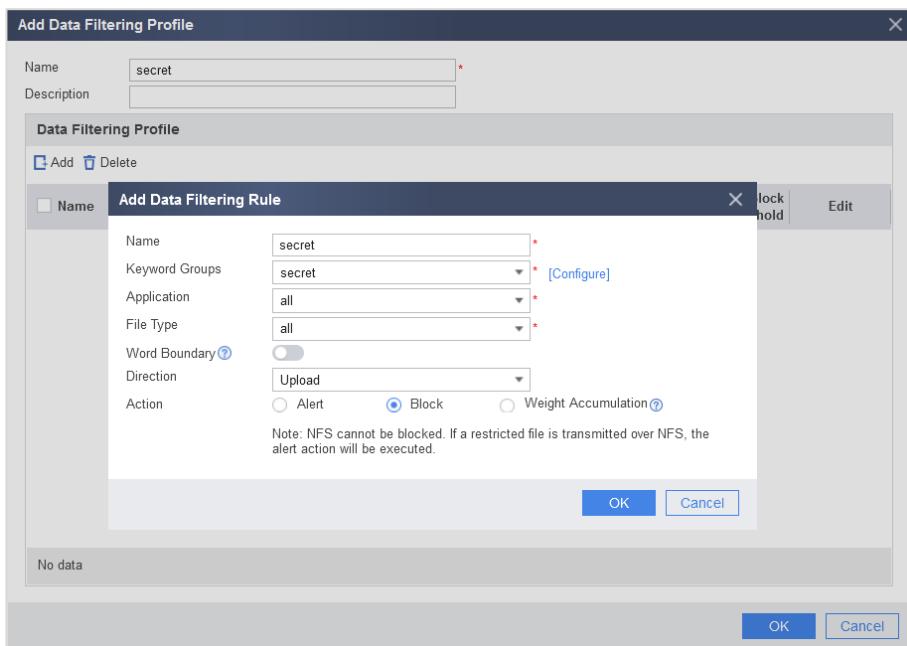


The screenshot shows the 'Add Keyword Group' dialog. In the main window, a keyword group named 'secret' is being created. A sub-dialog titled 'Add Keyword' is open, showing a keyword entry for 'secret' with 'Matching Mode' set to 'Text'. The 'OK' button is highlighted.



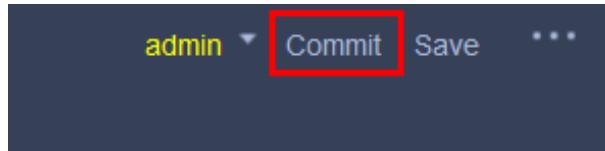
The screenshot shows the 'Add Keyword Group' dialog again. The keyword 'secret' has been successfully added to the keyword list. The 'Weight' field for the keyword 'secret' is highlighted with a red box.

Choose Object > Security Profiles > Data Filtering and click Add. Click Data Filtering Rule > Add, set Keyword Groups, set Direction to Upload, and set Action to Block.



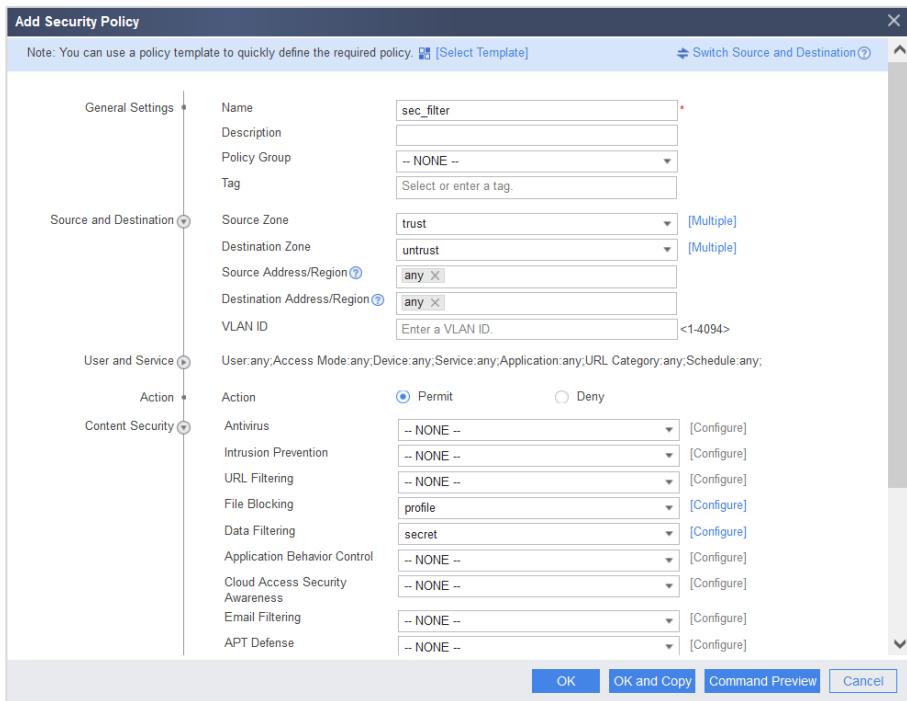
The screenshot shows the 'Add Data Filtering Profile' dialog. A sub-dialog titled 'Add Data Filtering Rule' is open, showing a rule named 'secret'. The 'Direction' is set to 'Upload' and 'Action' is set to 'Block'. The 'OK' button is highlighted.

After the configuration is complete, click **Commit** in the upper right corner to make the configuration take effect.



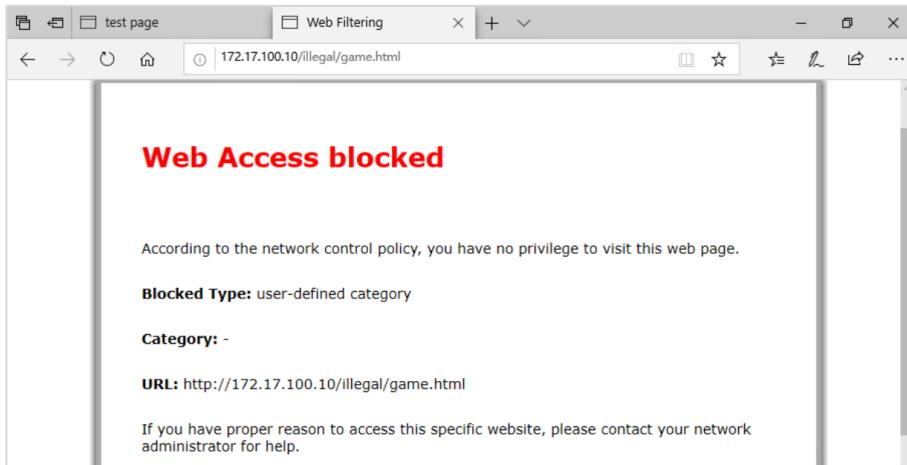
Step 7 Invoke file blocking/data filtering.

Choose **Policy > Security Policy** and click **Add Security Policy**. Select or enter the parameters and set **File Blocking** and **Data Filtering**.

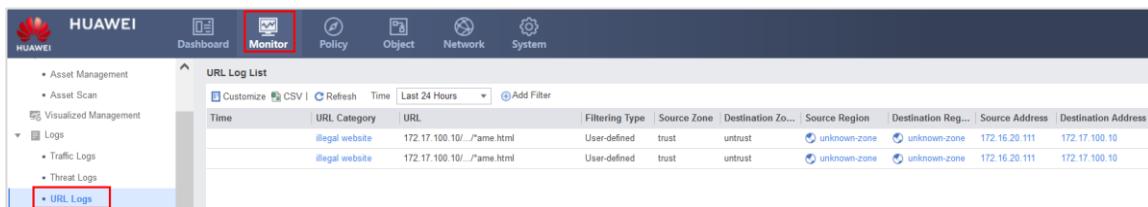


11.3 Verification

Access a game page on PC1. It is found that the page is blocked by the firewall.

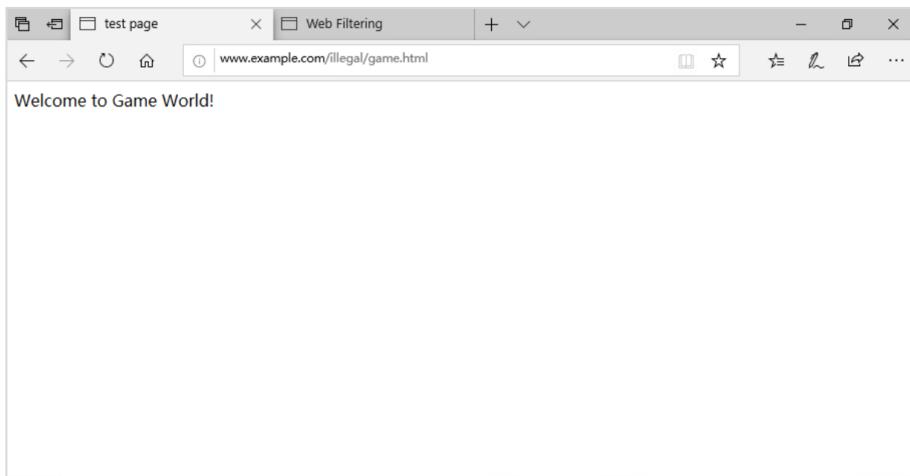


View URL logs.

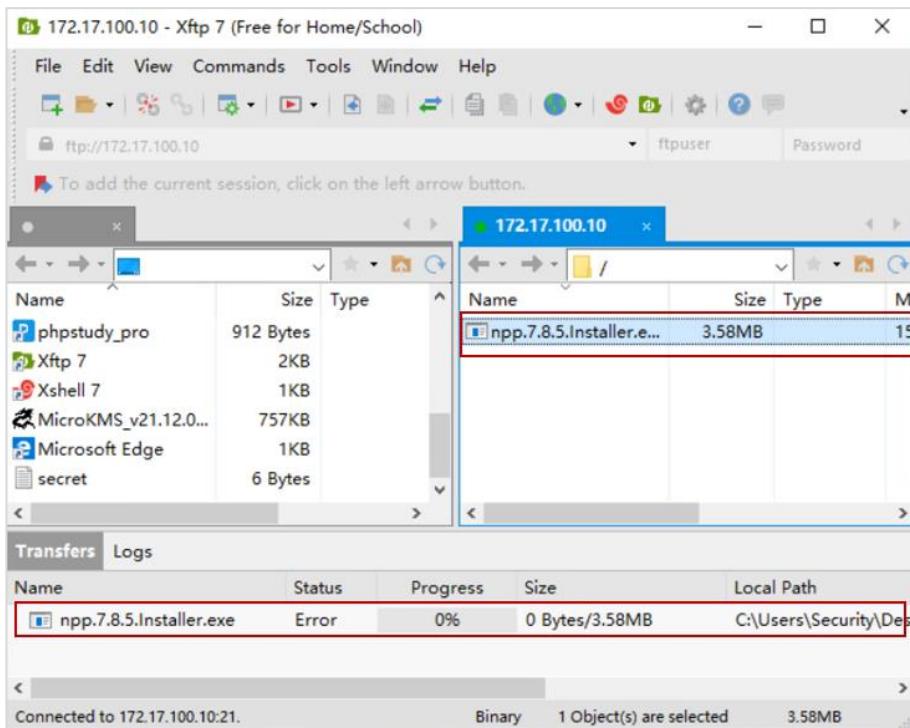


Time	URL Category	URL	Filtering Type	Source Zone	Destination Zon...	Source Region	Destination Reg...	Source Address	Destination Address
	illegal website	172.17.100.10/...ame.html	User-defined	trust	untrust	unknown-zone	unknown-zone	172.16.20.111	172.17.100.10
	illegal website	172.17.100.10/...ame.html	User-defined	trust	untrust	unknown-zone	unknown-zone	172.16.20.111	172.17.100.10

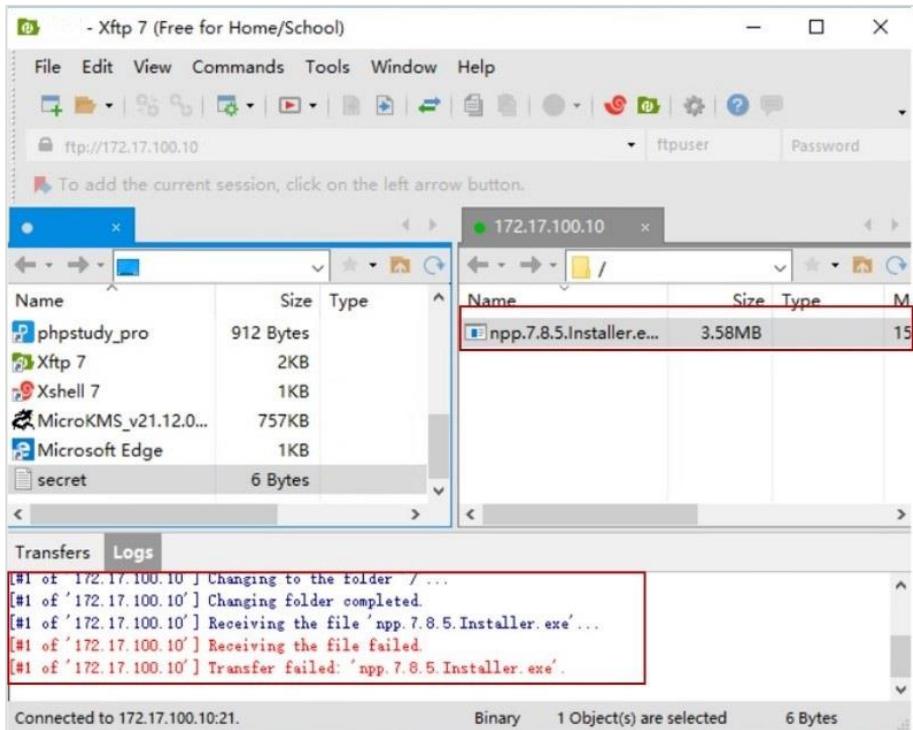
Cancel the URL filtering policy and the user can access the game page.



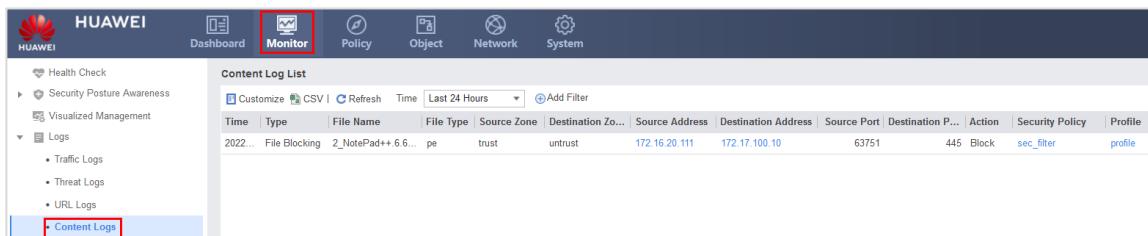
Disable security policy **sec_url_policy**. Use the XSFP software on the client of PC1 to connect to the Internet FTP server and then download executable files from the Internet through FTP. The download is blocked and the **Status** is displayed as **Error** on the transmission page.



Name	Status	Progress	Size	Local Path
npp.7.8.5.Installer.exe	Error	0%	0 Bytes/3.58MB	C:\Users\Security\Des...



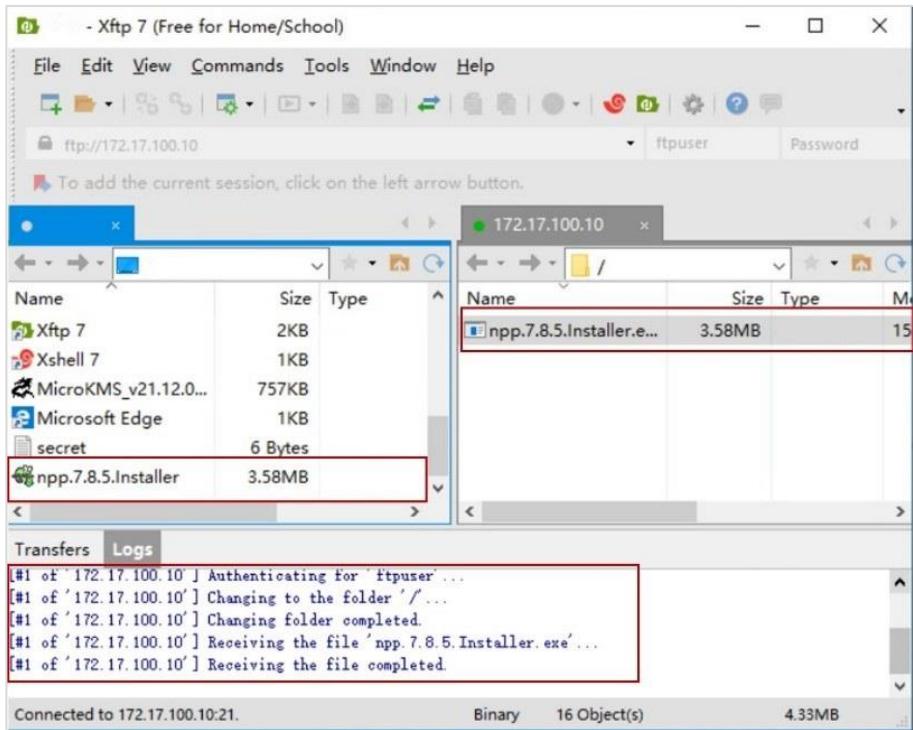
View firewall logs.



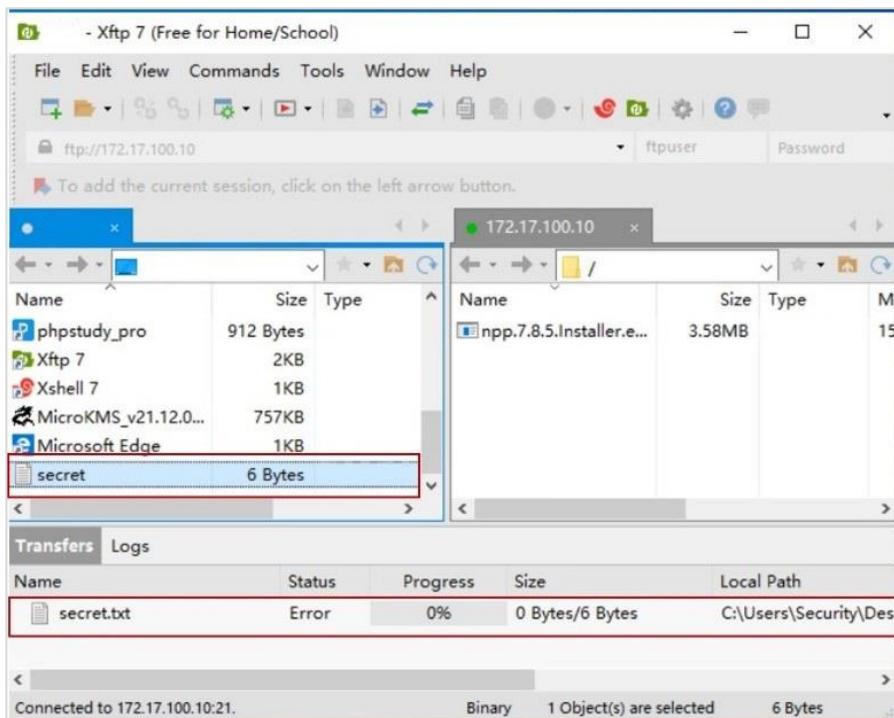
The screenshot shows the Huawei Security Posture Awareness interface under the Monitor tab. The left sidebar has sections for Health Check, Security Posture Awareness, Visualized Management, Logs (Traffic Logs, Threat Logs, URL Logs), and Content Logs (which is highlighted with a red box). The main content area displays a Content Log List table with the following data:

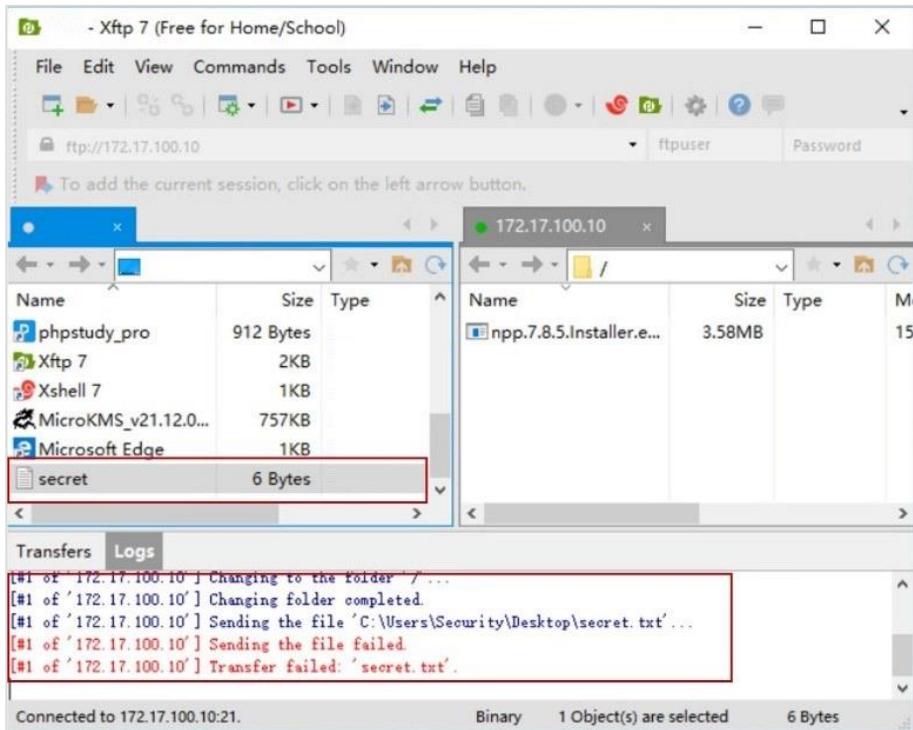
Time	Type	File Name	File Type	Source Zone	Destination Zone	Source Address	Destination Address	Source Port	Destination Port	Action	Security Policy	Profile
2022...	File Blocking	2_NotePad++ 6.6...	pe	trust	untrust	172.16.20.111	172.17.100.10	63751	445	Block	sec_filter	profile

Cancel the file blocking policy and the user can download executable files from the Internet.



Use the XSFP software on PC1 to connect to the FTP server on the Internet and upload confidential files containing keyword **secret** to the Internet through FTP. It is found that the upload operation is blocked and the **Status** is displayed as **Error** on the transmission page.

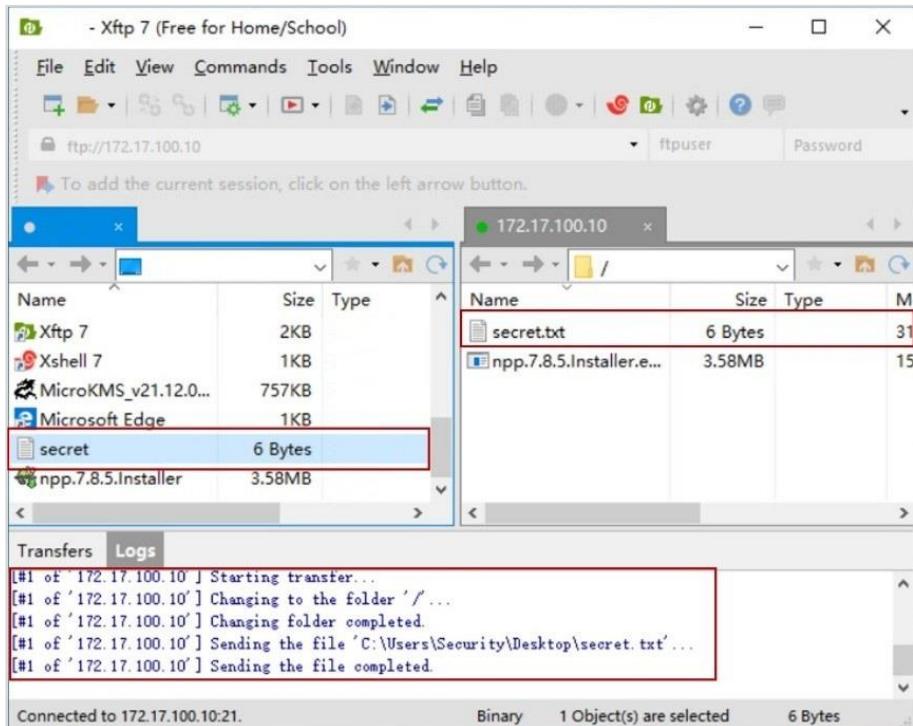




View firewall logs.

Time	Type	File Name	File Type	Source Zone	Destination Zone	Source Address	Destination Address	Source Port	Destination Port	Action	Security Policy	Profile
2022...	Data Filtering	secret.txt	text/html	trust	untrust	172.16.20.111	172.17.100.10	63753	21	Block	sec_filter	secret
2022...	File Blocking	2_NotePad++.6.6...	pe	trust	untrust	172.16.20.111	172.17.100.10	63751	445	Block	sec_filter	profile

Cancel the data filtering policy and the user can upload confidential files to the Internet.



11.4 Configuration Reference

11.4.1 FW1's Configuration

```
#  
sysname FW1  
#  
interface GigabitEthernet0/0/2  
undo shutdown  
ip address 100.3.1.2 255.255.255.252  
service-manage http permit  
service-manage https permit  
service-manage ping permit  
service-manage ssh permit  
service-manage snmp permit  
service-manage telnet permit  
service-manage netconf permit  
#  
interface GigabitEthernet0/0/6  
undo shutdown  
ip address 172.16.20.2 255.255.255.0  
service-manage http permit  
service-manage https permit  
service-manage ping permit  
service-manage ssh permit  
service-manage snmp permit  
service-manage telnet permit  
service-manage netconf permit
```

```
#  
firewall zone local  
    set priority 100  
#  
firewall zone trust  
    set priority 85  
    add interface GigabitEthernet0/0/6  
#  
firewall zone untrust  
    set priority 5  
    add interface GigabitEthernet0/0/1  
    add interface GigabitEthernet0/0/2  
#  
firewall zone dmz  
    set priority 50  
#  
ip route-static 0.0.0.0 0.0.0.0 100.3.1.1  
#  
url-filter category user-defined name "illegal website"  
    add url 172.17.100.10/illegal/game.html  
#  
profile type url-filter name url_profile  
    category user-defined name "illegal website" action block  
    default action block  
#  
profile type file-block name profile  
    rule name download  
        file-type pre-defined name EXE MSI RPM OCX A ELF DLL PE SYS  
        application all  
        direction download  
        action block  
#  
keyword-group name secret  
    user-defined-keyword name secret  
    expression match-mode text secret  
    undo case-sensitive enable  
#  
profile type data-filter name secret  
    rule name secret  
        keyword-group name secret  
        file-type all  
        application all  
        action block  
#  
security-policy  
    default action permit  
    rule name sec_url_policy  
        source-zone trust  
        destination-zone untrust  
        source-address address-set 172.16.20.111/24  
        profile url-filter url_profile  
        action permit  
    rule name sec_filter  
        source-zone trust  
        destination-zone untrust
```

```
profile data-filter secret
profile file-block profile
action permit
#
nat-policy
rule name trust-untrust
source-zone local
source-zone trust
destination-zone untrust
action source-nat easy-ip
#
```

11.4.2 SW1's Pre-configuration

```
#
sysname SW1
#
vlan batch 2 1003
#
interface vlanif2
ip address 4.4.4.1 255.255.255.252
#
interface vlanif1003
ip address 172.17.100.1 255.255.255.0
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/15
port link-type access
port default vlan 1003
#
ip route-static 0.0.0.0 0.0.0.0 100.10.1.1
ip route-static 100.3.1.0 255.255.255.252 4.4.4.2
#
```

11.4.3 Mirror-SW's Pre-configuration

```
#
sysname Mirror-SW
#
vlan batch 2
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 2
#
```

11.4.4 RT1's Pre-configuration

```
#  
sysname RT1  
#  
interface GigabitEthernet0/0/1  
    undo portswitch  
#  
interface GigabitEthernet0/0/1.2  
    dot1q termination vid 2  
    ip address 4.4.4.2 255.255.255.252  
#  
interface GigabitEthernet0/0/4  
    undo portswitch  
    ip address 100.3.1.1 255.255.255.252  
#  
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1  
#
```

11.4.5 SW3's Pre-configuration

```
#  
sysname SW3  
#  
vlan batch 40  
#  
interface GigabitEthernet0/0/2  
    port link-type access  
    port default vlan 40  
#  
interface GigabitEthernet0/0/13  
    port link-type access  
    port default vlan 40  
#
```

11.5 Quiz

What are the common parameters in a URL filtering profile?

Reference answer: default action, blacklist and whitelist, and URL filtering level.

12 802.1X Authentication

12.1 Introduction

12.1.1 About This Lab

Enterprises usually deploy WLANs to provide wireless office environments for employees. For security purposes, 802.1X authentication is leveraged to authenticate employees. Because there are a large number of employees, the RADIUS server is used to manage employee accounts and permissions in a unified manner.

This lab describes how to implement 802.1X authentication.

12.1.2 Objectives

- Learn to onboard an AP.
- Learn to configure a WLAN profile.
- Understand how to configure WLAN 802.1X authentication.

12.1.3 Networking Topology

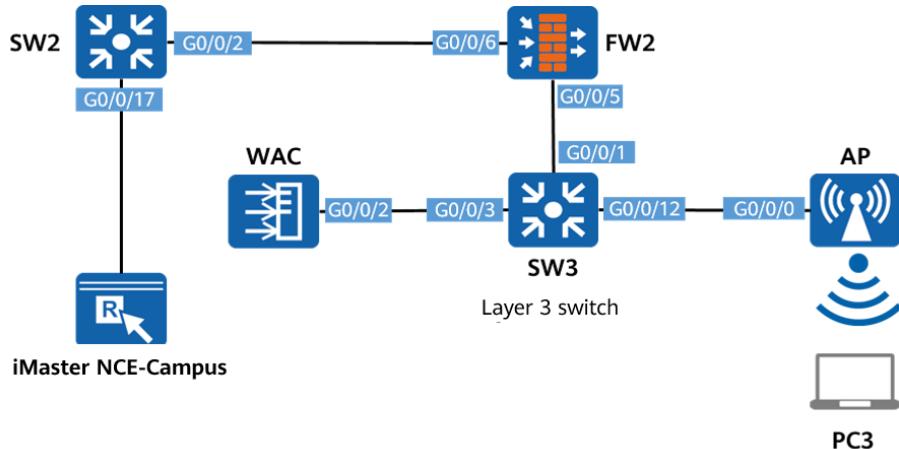


Figure 12-1 802.1X wireless authentication

The preceding figure shows device connections. For details about IP address planning, see Table 12-1.

Layer 2 networking is used between the WAC and AP, and between the WAC and RADIUS server. For key configurations of interfaces, see 12.4 Configuration Reference.

1. An external power module is used to supply power to the AP. iMaster NCE-Campus functions as the RADIUS server.

2. Layer 2 networking is used between the AP and WAC. The DHCP address pools of the AP and terminal are obtained from the WAC.
3. Layer 2 networking is used between the WAC and RADIUS server. AAA authentication for the wireless terminal is performed by the RADIUS server.
4. FW2 only transparently transmits packets.
5. SSID for network access: 802.1X authentication is required for connecting to the Wi-Fi named **HCIP-Security**. In addition, to enhance PC access management, the RADIUS server delivers ACLs to restrict terminal access to resources.

12.1.4 Lab Planning

Table 12-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
SW2	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to FW2
	G0/0/17	Access	PVID: 10	Interface for connecting to iMaster NCE-Campus
SW3	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to FW2
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	Interface for connecting to the WAC
	G0/0/12	Trunk	PVID: 4000 Allow-pass VLAN: 4000	Interface for connecting to the AP
FW2	GE0/0/5	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to SW3
	GE0/0/6	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to SW2
WAC	GE0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	Interface for connecting to SW3
AP	GE0/0/0	/	Retain default settings.	Interface for connecting to

				SW3
iMaster NCE-Campus	Ethernet0	Network adapter	192.168.2.201/24	Server interface IP address

12.2 Lab Configuration

12.2.1 Configuration Roadmap

1. Configure interconnection interfaces between the WAC and the AP.
2. Configure the DHCP server function on the WAC to assign a management address to the AP and a service address to the wireless terminal.
3. Configure AP onboarding.
4. Configure the RADIUS function on iMaster NCE-Campus for WLAN user authentication.
5. Configure profiles (including the SSID profile) and WLAN 802.1X authentication.

12.2.2 Configuration Procedure

Step 1 Complete basic device configurations.

Complete basic configurations for the interconnection interfaces between the WAC and SW3, as well as those between SW3 and the AP according to the table in 12.1.4 Lab Planning. Complete basic configurations for the interconnection interfaces between SW3 and FW2, as well as those between FW2 and SW2. Configure firewall security policies to allow traffic to pass through.

```
# Configure GigabitEthernet0/0/2 on the WAC.
```

```
[AC] interface GigabitEthernet0/0/2
[AC-GigabitEthernet0/0/2] port link-type trunk
[AC-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[AC-GigabitEthernet0/0/2] port trunk allow-pass vlan 10 4000 4001
[AC-GigabitEthernet0/0/2] quit
```

```
# Configure G0/0/3, G0/0/12, and G0/0/1 on SW3.
```

```
[SW3] interface GigabitEthernet0/0/3
[SW3-G0/0/3] port link-type trunk
[SW3-G0/0/3] port trunk allow-pass vlan 10 4000 4001
[SW3-G0/0/3] quit
```

```
[SW3] interface GigabitEthernet0/0/12
[SW3-G0/0/12] port link-type trunk
[SW3-G0/0/12] port trunk pvid vlan 4000
```

```
[SW3-G0/0/12] port trunk allow-pass vlan 4000  
[SW3-G0/0/12] quit
```

```
[SW3] interface GigabitEthernet0/0/1  
[SW3-G0/0/1] port link-type trunk  
[SW3-G0/0/1] port trunk allow-pass vlan 10  
[SW3-G0/0/1] quit
```

Configure GE0/0/5 and GE0/0/6 on FW2 and add the interfaces to the security zone.

```
[FW2] interface GigabitEthernet0/0/5  
[FW2-GigabitEthernet0/0/5] portswitch  
[FW2-GigabitEthernet0/0/5] port link-type trunk  
[FW2-GigabitEthernet0/0/5] undo port trunk allow-pass vlan 1  
[FW2-GigabitEthernet0/0/5] port trunk allow-pass vlan 10  
[FW2-GigabitEthernet0/0/5] quit
```

```
[FW2] interface GigabitEthernet0/0/6  
[FW2-GigabitEthernet0/0/6] portswitch  
[FW2-GigabitEthernet0/0/6] port link-type trunk  
[FW2-GigabitEthernet0/0/6] undo port trunk allow-pass vlan 1  
[FW2-GigabitEthernet0/0/6] port trunk allow-pass vlan 10  
[FW2-GigabitEthernet0/0/6] quit
```

```
[FW2] firewall zone trust  
[FW2-zone-trust] add interface GigabitEthernet0/0/5  
[FW2-zone-trust] add interface GigabitEthernet0/0/6  
[FW2-zone-trust] quit
```

```
[FW2] security-policy  
[FW2-policy-security] rule name pass  
[FW2-policy-security-rule-pass] action permit  
[FW2-policy-security-rule-pass] quit  
[FW2-policy-security] quit
```

Configure G0/0/2 and G0/0/17 on SW2.

```
[SW2] interface GigabitEthernet 0/0/2  
[SW2-G0/0/2] port link-type trunk  
[SW2-G0/0/2] undo port trunk allow-pass vlan 1  
[SW2-G0/0/2] port trunk allow-pass vlan 10  
[SW2-G0/0/2] quit
```

```
[SW2] interface GigabitEthernet 0/0/17
[SW2-G0/0/24] port link-type access
[SW2-G0/0/24] port default vlan 10
[SW2-G0/0/24] quit
```

Step 2 Configure the DHCP server function on the WAC.

The WAC needs to provide a management address for the AP and a service address for wireless users. Configure VLAN 4000 for the DHCP server on the management network segment and VLAN 4001 for the DHCP server on the user network segment according to 12.1.4 Lab Planning.

```
# Enable the DHCP function on the WAC.
```

```
[AC] dhcp enable
```

```
# Configure the gateway IP address on the management network segment of the AP and select the global DHCP address pool.
```

```
[AC] interface vlanif4000
[AC-VLANIF4000] ip address 10.10.1.1 255.255.255.0
[AC-VLANIF4000] dhcp select global
[AC-VLANIF4000] quit
```

```
# Configure the DHCP server on the management network segment of the AP.
```

```
[AC] ip pool vlan4000
[AC-ip-pool-vlan4000] gateway-list 10.10.1.1
[AC-ip-pool-vlan4000] network 10.10.1.0 mask 255.255.255.0
[AC-ip-pool-vlan4000] option 43 sub-option 3 ascii 10.10.1.1
[AC-ip-pool-vlan4000] quit
```

```
# Configure the gateway IP address on the network segment of wireless services and select the global DHCP address pool.
```

```
[AC] interface vlanif4001
[AC-VLANIF4001] ip address 10.20.1.1 255.255.255.0
[AC-VLANIF4001] dhcp select global
[AC-VLANIF4001] quit
```

```
# Configure the DHCP server on the network segment of wireless users.
```

```
[AC] ip pool vlan4001
[AC-ip-pool-vlan4001] gateway-list 10.20.1.1
[AC-ip-pool-vlan4001] network 10.20.1.0 mask 255.255.255.0
[AC-ip-pool-vlan4001] quit
```

```
# Configure the authentication IP address for wireless users to communicate with iMaster NCE-Campus.
```

```
[AC] interface vlanif10
[AC-VLANIF10] ip address 192.168.2.10 255.255.255.0
```

```
[AC-VLANIF10] quit
```

Step 3 Configure AP onboarding.

Enable the function of establishing CAPWAP DTLS sessions through the preset certificate.

```
[AC] capwap dtls cert-mandatory-match enable
```

Note: When adding an AP running V200R021C00 or later, to avoid AP onboarding failures, you can enable this function to allow the AP to establish a DTLS session through the preset certificate for AP onboarding. After AP onboarding, the AP obtains a new DTLS certificate to initiate a DTLS session in secure mode and onboard again. To ensure network security, disable this function immediately after the AP onboards again to prevent unauthorized APs from accessing the network.

Create an AP group to which APs with the same configurations are added.

```
[AC] wlan  
[AC-wlan-view] ap-group name ap-group1  
[AC-wlan-ap-group-ap-group1] quit
```

Create a regulatory domain profile, configure the country code of the WAC in the profile, and bind the profile to the AP group.

```
[AC-wlan-view] regulatory-domain-profile name domain1  
[AC-wlan-regulate-domain-domain1] country-code cn  
[AC-wlan-regulate-domain-domain1] quit  
[AC-wlan-view] ap-group name ap-group1  
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1  
Continue?[Y/N]:y  
[AC-wlan-ap-group-ap-group1] quit  
[AC-wlan-view] quit
```

Configure the source interface of the WAC.

```
[AC] capwap source interface vlanif4000
```

Import the AP offline on the WAC.

```
[AC] wlan  
[AC-wlan-view] ap auth-mode mac-auth  
[AC-wlan-view] ap-id 1 ap-mac 14ab-0228-5f80  
[AC-wlan-ap-1] ap-name a5760  
Warning: The AP name cannot be the MAC address of another AP. Otherwise, the AP name may be lost after the device restarts.  
Warning: The AP name of more than 31 characters does not take effect for APs in versions earlier than V200R009C00.  
Warning: This operation may cause AP reset. Continue? [Y/N]:Y  
[AC-wlan-ap-1] ap-group ap-group1  
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio. Whether to continue? [Y/N]:Y  
[AC-wlan-ap-1] quit
```

Run the **display ap all** command to check the AP state. If the **State** field displays **nor**, the AP onboards properly.

```
[AC] display ap all
Total AP information:
nor : normal [1]
ExtraInfo : Extra information
-----
ID   MAC        Name  Group    IP          Type      State  STA  Uptime ExtraInfo
-----
1   14ab-0228-5f80 a5760 ap-group1 10.10.1.226 AirEngine5760-51 nor   0   -   -
-----
Total: 1
```

Step 4 Configure RADIUS server parameters for interconnection.

Create a RADIUS server template on the WAC.

```
[AC] radius-server template t1
[AC-radius-wlan-t1] radius-server authentication 192.168.2.201 1812
[AC-radius-wlan-t1] radius-server accounting 192.168.2.201 1813
[AC-radius-wlan-t1] radius-server shared-key cipher Huawei@123
[AC-radius-wlan-t1] quit
```

On the WAC, set the source IP address for communicating with the RADIUS server to 192.168.2.10.

```
[AC] radius-server source ip-address 192.168.2.10
```

Create a RADIUS authentication scheme.

```
[AC] aaa
[AC-aaa] authentication-scheme HCIP-Security
[AC-aaa-authen-HCIP-Security] authentication-mode radius
[AC-aaa-authen-HCIP-Security] quit
```

Step 5 Configure 802.1X authentication and SSID.

Create an 802.1X access profile **HCIP-Security** and set the authentication mode to EAP relay.

```
[AC] dot1x-access-profile name HCIP-Security
[AC-dot1x-access-profile-HCIP-Security] dot1x authentication-method eap
[AC-dot1x-access-profile-HCIP-Security] quit
```

Create an authentication profile **HCIP-Security**, and bind the 802.1X access profile, authentication scheme, and RADIUS server template to the authentication profile.

```
[AC] authentication-profile name HCIP-Security
[AC-authentication-profile-HCIP-Security] dot1x-access-profile HCIP-Security
[AC-authentication-profile-HCIP-Security] authentication-scheme HCIP-Security
[AC-authentication-profile-HCIP-Security] radius-server t1
```

```
[AC-authentication-profile-HCIP-Security] quit
```

Create a security profile named **HCIP-Security** and configure a security policy.

```
[AC] wlan  
[AC-wlan-view] security-profile name HCIP-Security  
[AC-wlan-sec-prof-HCIP-Security] security wpa-wpa2 dot1x aes  
[AC-wlan-sec-prof-HCIP-Security] quit
```

Create an SSID profile named **HCIP-Security** and set the SSID name to **HCIP-Security**.

```
[AC-wlan-view] ssid-profile name HCIP-Security  
[AC-wlan-ssid-prof-HCIP-Security] ssid HCIP-Security  
[AC-wlan-ssid-prof-HCIP-Security] quit
```

Create a VAP profile named **HCIP-Security**, set the data forwarding mode to tunnel forwarding, set the service VLAN, and bind the security profile, authentication profile, and SSID profile to the VAP profile.

```
[AC-wlan-view] vap-profile name HCIP-Security  
[AC-wlan-vap-prof-HCIP-Security] forward-mode tunnel  
[AC-wlan-vap-prof-HCIP-Security] service-vlan vlan-id 4001  
[AC-wlan-vap-prof-HCIP-Security] security-profile HCIP-Security  
[AC-wlan-vap-prof-HCIP-Security] authentication-profile HCIP-Security  
[AC-wlan-vap-prof-HCIP-Security] ssid-profile HCIP-Security  
[AC-wlan-vap-prof-HCIP-Security] quit
```

Bind the VAP profile named **HCIP-Security** to the AP group and apply configurations in this VAP profile to radio 0 and radio 1 of the APs in the AP group.

```
[AC-wlan-view] ap-group name ap-group1  
[AC-wlan-ap-group-ap-group1] vap-profile HCIP-Security wlan 1 radio 0  
[AC-wlan-ap-group-ap-group1] vap-profile HCIP-Security wlan 1 radio 1  
[AC-wlan-ap-group-ap-group1] quit  
[AC-wlan-view] quit
```

Configure the user group named **group1** for the post-authentication domain to allow only user group members to access network resources on network segment 10.23.200.0/24.

```
[AC] acl 3001  
[AC-acl-adv-3001] rule 1 permit ip destination 10.10.10.0 0.0.0.255  
[AC-acl-adv-3001] rule 2 deny ip destination any  
[AC-acl-adv-3001] quit  
[AC] user-group group1  
[AC-user-group-group1] acl-id 3001  
[AC-user-group-group1] quit
```

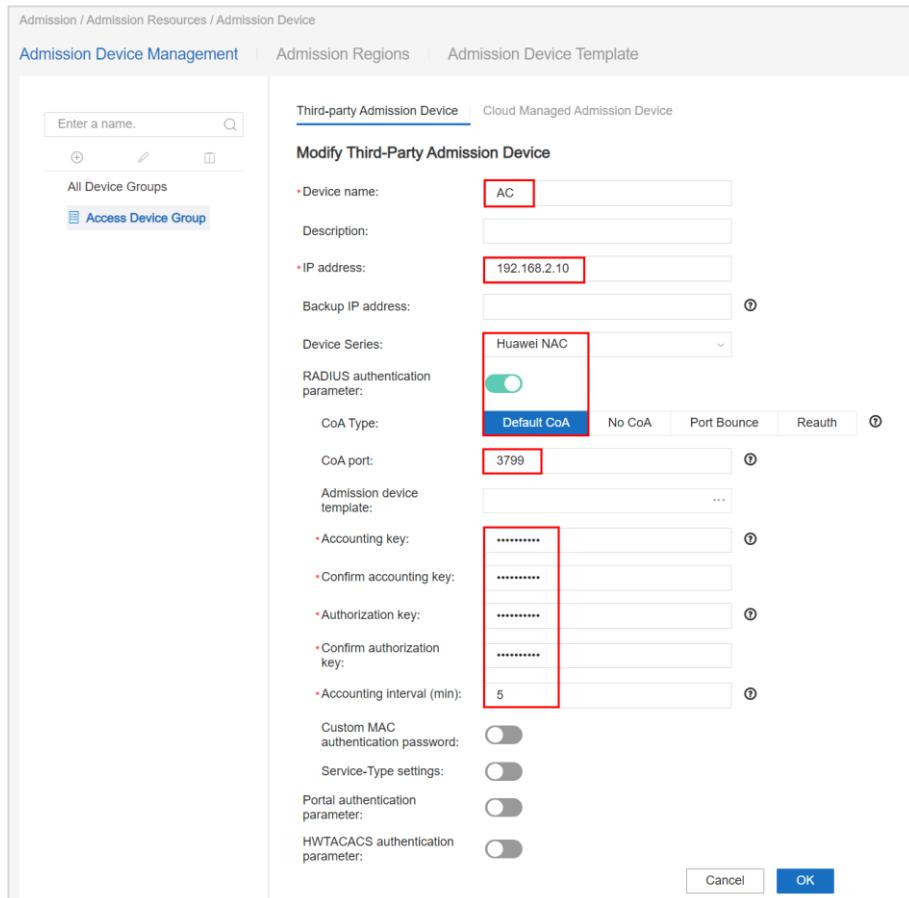
Configure the user group named **group1** for the post-authentication domain to allow only user group members to access network resources on network segment 10.10.10.0/24.

Step 6 Configure the RADIUS server.

In this lab, iMaster NCE-Campus is used as the RADIUS server. Only the tenant administrator account can be used to log in to iMaster NCE-Campus for configuration. The user name and password for login are **operator-admin** and **Huawei@123**, respectively.

Before configuring RADIUS authentication, add the WAC to iMaster NCE-Campus. Configure accounting and authorization passwords, which must be the same as those configured in the RADIUS server template of the wireless controller. Add a user name and password.

Choose **Admission > Admission Resources > Admission Advice**. Create a WAC, set the accounting and authorization keys to **Huawei@123**, and set other parameters as follows:



The screenshot shows the 'Modify Third-Party Admission Device' configuration page. Key fields highlighted with red boxes include:

- Device name: AC
- IP address: 192.168.2.10
- Device Series: Huawei NAC
- CoA Type: Default CoA
- CoA port: 3799
- Accounting key: (redacted)
- Confirm accounting key: (redacted)
- Authorization key: (redacted)
- Confirm authorization key: (redacted)
- Accounting interval (min): 5

Choose **Admission > Admission Resources > User Management**. Create a user named **admin**, set the password to **Huawei@123**, and set other parameters as follows:

Admission / Admission Resources / User Management

User Management | Role Management | Blacklist Management

User | MAC Account | PPSK | User Operation Log

Basic Information

* User name: admin

* Password:

* Confirm password:

Role:

Max. number of terminals: ⓘ All authentication modes except HWTACACS authentication are supported.

Expiration time:

Change password upon next login:

This parameter is valid only for built-in portal authentication and self-service portal login.

* Available login mode: Portal 802.1X & Portal 2.0 HWTACACS

To configure Portal 2.0 authentication, select both Portal and 802.1X & Portal 2.0. To configure HACA authentication, select Portal.

Use only mobile certificates for authentication: Specifies 802.1X authentication based on the EAP-TLS protocol. Do not select this option in the Boarding scenario.

Other Information

Name:

Email:

Phone number:

Description:

Terminals Bound to an Admission Device ⌂

RADIUS attribute ⓘ ⌂

Choose Admission > Admission Policy > Authentication and Authorization.

iMaster NCE-Campus

Design Provision **Admission** Monitoring Maintenance System

Welcome to iMaster NCE-Campus

You can enable the dashboard function on this page during insight into the network-wide data status and trend.

Network Scenario

Branch Network Guide you through service planning and configuration f...

VXLAN Fabric Network Guide you through service planning and configuration f...

Admission Resources

- User Management
- Guest Management
- Terminal Management
- Page Management
- Admission Device
- External Data Source
- Certificate Authentication

Device Administrator

- HWTACACS Authentication ...

VAS

- Online Behavior Management
- RADIUS Accounting Device

Admission Policy

- Authentication and Authoriza...
- Online User Control
- Admission Settings

Free Mobility

- Security Group
- Resource Group
- Policy Control
- IP-Security Group Entry Sub...
- IP-Security Group Entry

Configure an authentication rule.

Admission / Admission Policy / Authentication and Authorization

[Authentication Rules](#) | [Authorization Result](#) | [Authorization Rules](#) | [Policy Element](#)

Modify Authentication Rule

Basic Information

*Name:	802.1x		
Description:			
Authentication mode:	User access authentication	MAC address authentication	Device administrator authentication
Enable Portal-HACA:	<input type="checkbox"/>		
Access mode:	Wireless	Wired	Cellular network

User Information

Match user groups:	<input type="checkbox"/>						
Match accounts:	<input checked="" type="checkbox"/>						
Account:	Select Remove						
<table border="1"> <thead> <tr> <th><input type="checkbox"/> Account</th> <th>Account Type</th> <th>User Group</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> admin</td> <td>User</td> <td>ROOT</td> </tr> </tbody> </table>		<input type="checkbox"/> Account	Account Type	User Group	<input type="checkbox"/> admin	User	ROOT
<input type="checkbox"/> Account	Account Type	User Group					
<input type="checkbox"/> admin	User	ROOT					

Retain default settings for other parameters.

Configure an authorization result to authorize ACL3001 to the wireless user named **admin**, specifying that the user can access only the resources permitted by ACL3001. (ACL3001 must be created on the WAC in advance.)

Admission / Admission Policy / Authentication and Authorization

[Authentication Rules](#) | **Authorization Result** | [Authorization Rules](#) | [Policy Element](#)

Create

*Name:	802.1x
Description:	

Strategy

Device management service:	<input type="checkbox"/>	
VIP users:	<input type="checkbox"/>	
For APs and LSWs only.		
ACL:	3001	X...

Configure an authorization rule. Set the name to **802.1x**, authentication mode to **User access authentication**, and access mode to **Wireless**. Enable account information matching and select the corresponding account. Retain default settings for other parameters. Set the authorization result to **802.1x**.

Modify Authorization Rule

Basic Information

*Name: **802.1x**

Description:

Authentication mode: **User access authentication** MAC address authentication Device administrator authentication

Portal-HACA:

Access mode: **Wireless** Wired Cellular network

User Information

Match user groups:

Match external groups:

Match accounts:

Account: **Select** **Remove**

<input type="checkbox"/> Account	Account Type
<input type="checkbox"/> admin	User

Authorization Result

*Authorization result: **802.1x** **...**

Configure an authorization rule. Set the name to **802.1x-AC-test**, authentication mode to **User access authentication**, and access mode to **Wired**. Enable account information matching and select the corresponding account. Retain default settings for other parameters. Set the authorization result to **Permit Access**. The authorization rule named **802.1x-AC-test** is created to check whether the WAC and RADIUS server are running properly.

Authentication Rules | Authorization Result | **Authorization Rules** | Policy Element

Create Authorization Rule

Basic Information

*Name:	802.1x-AC-test
Description:	
Authentication mode:	User access authentication
Portal-HACA:	<input checked="" type="checkbox"/>
Access mode:	Wireless <input checked="" type="radio"/> Wired Cellular network

User Information

Match user groups:	<input type="checkbox"/>
Match external groups:	<input type="checkbox"/>
Match accounts:	<input checked="" type="checkbox"/>
Account:	<input type="button" value="Select"/> <input type="button" value="Remove"/>
<input type="checkbox"/> Account <input type="button" value="Account Type"/> admin Users	

Authorization Result

*Authorization result:	Permit Access
------------------------	---------------

12.3 Verification

Verify the following:

1. Check whether AP onboarding is successful.
2. Check the connectivity between the WAC and RADIUS server.
3. Check whether the wireless terminal can connect to the Wi-Fi named **HCIP-Security** and whether detailed information about the access user and the delivered dynamic ACL3001 are displayed on the WAC.

AP onboarding is successful on the WAC.

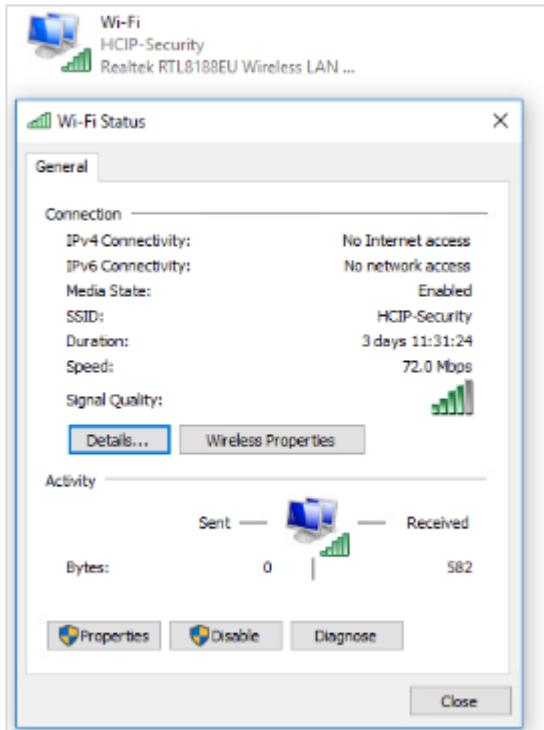
```
[AC] display ap all
Total AP information:
nor : normal [1]
ExtraInfo : Extra information
-----
ID MAC Name Group IP Type State STA Uptime ExtraInfo
-----
1 14ab-0228-5f80 a5760 ap-group1 10.10.1.226 AirEngine5760-51 nor 0 - -
-----
```

Total: 1

On the WAC, the account **admin** and password **Huawei@123** can be used to ensure successful RADIUS authentication.

```
[AC] test-aaa admin Huawei@123 radius-template t1 accounting  
Info: Account test succeeded.
```

The wireless terminal can connect to the Wi-Fi network named **HCIP-Security**.



On the WAC, you can view detailed information about the access user and the delivered dynamic ACL3001.

```
[AC] display access-user username admin
```

User ID	Username	IP address	MAC	Status
4186	admin	10.20.1.100	e0e1-a954-ae5e	Success

Total: 1, printed: 1

```
[AC] display access-user user-id 4186
```

Basic:

User ID	:	4186
User name	:	admin
User MAC	:	e0e1-a954-ae5e
User IP address	:	10.20.1.100
User vpn-instance	:	-
User IPv6 address	:	-

User access Interface	:	Wlan-Dbss17496
User vlan event	:	Success
QinQVlan/UserVlan	:	0/4001
User vlan source	:	user request
User accounting session ID	:	AC0000000000400111****010005a
User accounting mult session ID	:	30FD65F8FDE0E0E1A954AE5E62B58****DBBF8BF
User access type	:	802.1x
AP name	:	a5760
Radio ID	:	0
AP MAC	:	14ab-0228-5f80
SSID	:	HCIP-Security
Online time	:	324(s)
Dynamic ACL ID(Effective)	:	3001
User Group Priority	:	0

AAA:

User authentication type	:	802.1x authentication
Current authentication method	:	RADIUS
Current authorization method	:	-
Current accounting method	:	None

12.4 Configuration Reference

12.4.1 SW2's Configuration

```
#  
sysname SW2  
#  
vlan batch 10  
#  
interface GigabitEthernet0/0/2  
    port link-type trunk  
    undo port trunk allow-pass vlan 1  
    port trunk allow-pass vlan 10  
#  
interface GigabitEthernet0/0/17  
    port link-type access  
    port default vlan 10  
#
```

12.4.2 SW3's Configuration

```
#  
sysname SW3  
#  
vlan batch 10 4000 4001  
#  
interface GigabitEthernet0/0/1  
    port link-type trunk  
    port trunk allow-pass vlan 10  
#
```

```
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 10 4000 4001
#
interface GigabitEthernet0/0/12
port link-type trunk
port trunk pvid vlan 4000
port trunk allow-pass vlan 4000
#
```

12.4.3 FW2's Configuration

```
#
sysname FW2
#
vlan batch 10
#
interface GigabitEthernet0/0/5
portswitch
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/6
portswitch
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
add interface GigabitEthernet0/0/6
#
security-policy
rule name pass
action permit
#
```

12.4.4 WAC's Configuration

```
#
sysname AC
#
vlan batch 10 4000 4001
#
authentication-profile name HCIP-Security
dot1x-access-profile HCIP-Security
authentication-scheme HCIP-Security
radius-server t1
#
```

```
radius-server source ip-address 192.168.2.10
#
dhcp enable
#
radius-server template t1
    radius-server shared-key cipher %^%#E:Vc*u,;6B{ei,W|^yJ@1qi404pQXA[Pcl:xU\L-%^%#
    radius-server authentication 192.168.2.201 1812 source ip-address 192.168.2.10 weight 80
    radius-server accounting 192.168.2.201 1813 source ip-address 192.168.2.10 weight 80
#
ip pool vlan4001
    gateway-list 10.20.1.1
    network 10.20.1.0 mask 255.255.255.0
#
ip pool vlan4000
    gateway-list 10.10.1.1
    network 10.10.1.0 mask 255.255.255.0
    option 43 sub-option 3 ascii 10.10.1.1
#
interface vlanif10
    ip address 192.168.2.10 255.255.255.0
#
interface vlanif4000
    ip address 10.10.1.1 255.255.255.0
    dhcp select global
#
interface vlanif4001
    ip address 10.20.1.1 255.255.255.0
    dhcp select global
#
interface GigabitEthernet0/0/2
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 10 4000 4001
#
capwap source interface vlanif4000
#
aaa
    authentication-scheme HCIP-Security
        authentication-mode radius
#
wlan
    security-profile name HCIP-Security
    security wpa-wpa2 dot1x aes
    ssid-profile name HCIP-Security
    ssid HCIP-Security
    vap-profile name HCIP-Security
    forward-mode tunnel
    service-vlan vlan-id 4001
    ssid-profile HCIP-Security
    security-profile HCIP-Security
    authentication-profile HCIP-Security
    ap-group name ap-group1
    radio 0
        vap-profile HCIP-Security wlan 1
    radio 1
```

```
vap-profile HCIP-Security wlan 1
radio 2
    vap-profile HCIP-Security wlan 1
ap-id 1 type-id 130 ap-mac 14ab-0228-5f80 ap-sn 2102353GES6RN5008931
    ap-name a5760
    ap-group ap-group1
#
dot1x-access-profile name HCIP-Security
#
```

12.5 Quiz

What is the function of dynamic ACL delivery?

Answer: The RADIUS server delivers dynamic ACLs to limit the resources that wireless clients can access.

13 Portal Authentication

13.1 Introduction

13.1.1 About This Lab

Enterprises usually deploy WLANs to provide wireless office environments for employees. For security purposes, the enterprises want to authenticate their employees through an AD server deployed on the intranet.

This lab describes how to implement Portal authentication through the AD server.

13.1.2 Objectives

- Learn to onboard an AP.
- Learn to configure a WLAN profile.
- Understand how to configure WLAN Portal authentication.

13.1.3 Networking Topology

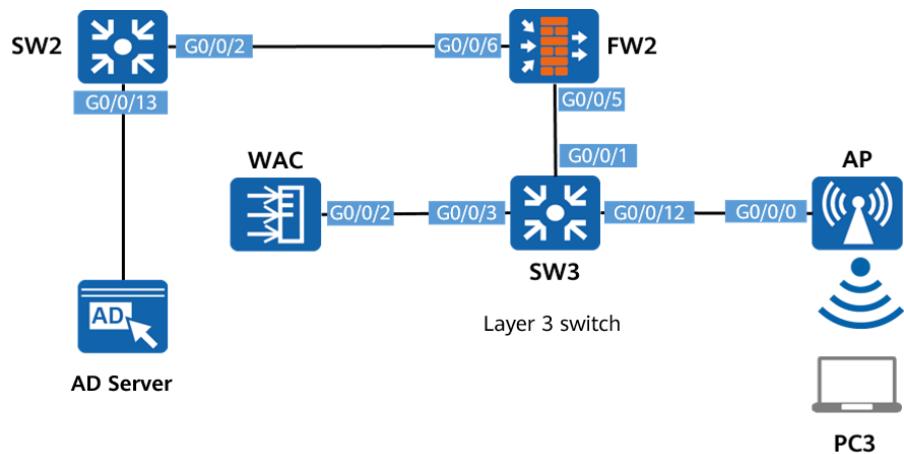


Figure 13-1 Portal wireless authentication

The preceding figure shows device connections. For details about IP address planning, see Table 13-1.

Layer 2 networking is used between the WAC and AP, and between the WAC and AD server. For key configurations of interfaces, see 13.4 Configuration Reference.

1. An external power module is used to supply power to the AP.

2. Layer 2 networking is used between the AP and WAC. The DHCP address pools of the AP and terminal are obtained from the WAC.
3. Layer 2 networking is used between the WAC and AD server. Authentication for the wireless terminal is performed by the AD server.
4. FW2 only transparently transmits packets.
5. SSID for network access: Portal authentication is required for connecting to the Wi-Fi named **HCIP-Security** and the local Portal page of the WAC is used.

13.1.4 Lab Planning

Table 13-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
SW2	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to FW2
	G0/0/13	Access	PVID: 10	Interface for connecting to AD Server
SW3	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to FW2
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	Interface for connecting to the WAC
	G0/0/12	Trunk	PVID: 4000 Allow-pass VLAN: 4000	Interface for connecting to the AP
FW2	GE0/0/5	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to SW3
	GE0/0/6	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to SW2
WAC	GE0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	Interface for connecting to SW3
AP	GE0/0/0	/	Retain default settings.	Interface for connecting to SW3
AD Server	Ethernet0	Network adapter	172.16.30.100/24	Server IP

13.2 Lab Configuration

13.2.1 Configuration Roadmap

1. Configure interconnection interfaces between the WAC and the AP.
2. Configure the DHCP server function on the WAC to assign a management address to the AP and a service address to the wireless terminal.
3. Configure the AP for onboarding.
4. Configure parameters on the WAC for interconnection with the AD server.
5. Configure profiles (including the SSID profile) and WLAN Portal authentication on the WAC.
6. Configure a user name and password on the AD server for WLAN user authentication.

13.2.2 Configuration Procedure

Step 1 Complete basic device configurations.

Complete basic configurations for the interconnection interfaces between the WAC and SW3, as well as those between SW3 and the AP. Complete basic configurations for the interconnection interfaces between SW3 and FW2, as well as those between FW2 and SW2. Configure firewall security policies to allow traffic to pass through.

Configure GigabitEthernet0/0/2 on the WAC.

```
[AC] interface GigabitEthernet0/0/2
[AC-GigabitEthernet0/0/2] port link-type trunk
[AC-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[AC-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 4000 4001
[AC-GigabitEthernet0/0/2] quit
```

Configure G0/0/3, G0/0/12, and G0/0/1 on SW3.

```
[SW3] interface GigabitEthernet0/0/3
[SW3-G0/0/3] port link-type trunk
[SW3-G0/0/3] port trunk allow-pass vlan 10 4000 4001
[SW3-G0/0/3] quit
```

```
[SW3] interface GigabitEthernet0/0/12
[SW3-G0/0/12] port link-type trunk
[SW3-G0/0/12] port trunk pvid vlan 4000
[SW3-G0/0/12] port trunk allow-pass vlan 4000
[SW3-G0/0/12] quit
```

```
[SW3] interface GigabitEthernet0/0/1
[SW3-G0/0/1] port link-type trunk
```

```
[SW3-G0/0/1] port trunk allow-pass vlan 10  
[SW3-G0/0/1] quit
```

Configure GE0/0/5 and GE0/0/6 on FW2 and add the interfaces to the security zone.

```
[FW2] interface GigabitEthernet0/0/5  
[FW2-GigabitEthernet0/0/5] portswitch  
[FW2-GigabitEthernet0/0/5] port link-type trunk  
[FW2-GigabitEthernet0/0/5] undo port trunk allow-pass vlan 1  
[FW2-GigabitEthernet0/0/5] port trunk allow-pass vlan 10  
[FW2-GigabitEthernet0/0/5] quit
```

```
[FW2] interface GigabitEthernet0/0/6  
[FW2-GigabitEthernet0/0/6] portswitch  
[FW2-GigabitEthernet0/0/6] port link-type trunk  
[FW2-GigabitEthernet0/0/6] undo port trunk allow-pass vlan 1  
[FW2-GigabitEthernet0/0/6] port trunk allow-pass vlan 10  
[FW2-GigabitEthernet0/0/6] quit
```

```
[FW2] firewall zone trust  
[FW2-zone-trust] add interface GigabitEthernet0/0/5  
[FW2-zone-trust] add interface GigabitEthernet0/0/6  
[FW2-zone-trust] quit
```

```
[FW2] security-policy  
[FW2-policy-security] rule name pass  
[FW2-policy-security-rule-pass] action permit  
[FW2-policy-security-rule-pass] quit  
[FW2-policy-security] quit
```

Configure G0/0/2 and G0/0/13 on SW2.

```
[SW2] interface GigabitEthernet 0/0/2  
[SW2-G0/0/2] port link-type trunk  
[SW2-G0/0/2] undo port trunk allow-pass vlan 1  
[SW2-G0/0/2] port trunk allow-pass vlan 10  
[SW2-G0/0/2] quit
```

```
[SW2] interface GigabitEthernet 0/0/13  
[SW2-G0/0/24] port link-type access  
[SW2-G0/0/24] port default vlan 10  
[SW2-G0/0/24] quit
```

Step 2 Configure the DHCP server function on the WAC.

The WAC needs to provide a management address for the AP and a service address for wireless users. Configure VLAN 4000 for the DHCP server on the management network segment and VLAN 4001 for the DHCP server on the user network segment according to 13.1.4 Lab Planning.

Enable the DHCP function on the WAC.

```
[AC] dhcp enable
```

Create VLANs on the WAC.

```
[AC] vlan batch 10 4000 4001
```

Configure the gateway IP address on the management network segment of the AP and select the global DHCP address pool.

```
[AC] interface vlanif4000  
[AC-VLANIF4000] ip address 10.10.1.1 255.255.255.0  
[AC-VLANIF4000] dhcp select global  
[AC-VLANIF4000] quit
```

Configure the DHCP server on the management network segment of the AP.

```
[AC] ip pool vlan4000  
[AC-ip-pool-vlan4000] gateway-list 10.10.1.1  
[AC-ip-pool-vlan4000] network 10.10.1.0 mask 255.255.255.0  
[AC-ip-pool-vlan4000] option 43 sub-option 3 ascii 10.10.1.1  
[AC-ip-pool-vlan4000] quit
```

Configure the gateway IP address on the network segment of wireless services and select the global DHCP address pool.

```
[AC] interface vlanif4001  
[AC-VLANIF4001] ip address 10.20.1.1 255.255.255.0  
[AC-VLANIF4001] dhcp select global  
[AC-VLANIF4001] quit
```

Configure the DHCP server on the network segment of wireless users.

```
[AC] ip pool vlan4001  
[AC-ip-pool-vlan4001] gateway-list 10.20.1.1  
[AC-ip-pool-vlan4001] network 10.20.1.0 mask 255.255.255.0  
[AC-ip-pool-vlan4001] quit
```

Configure the authentication IP address for wireless users to communicate with the AD server.

```
[AC] interface vlanif10  
[AC-VLANIF10] ip address 172.16.30.10 255.255.255.0  
[AC-VLANIF10] quit
```

Step 3 Configure AP onboarding.

Create an AP group to which APs with the same configurations are added.

```
[AC] wlan  
[AC-wlan-view] ap-group name ap-group1  
[AC-wlan-ap-group-ap-group1] quit
```

Create a regulatory domain profile, configure the country code of the WAC in the profile, and bind the profile to the AP group.

```
[AC-wlan-view] regulatory-domain-profile name domain1  
[AC-wlan-regulate-domain-domain1] country-code cn  
[AC-wlan-regulate-domain-domain1] quit  
[AC-wlan-view] ap-group name ap-group1  
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1  
Continue?[Y/N]:y  
[AC-wlan-ap-group-ap-group1] quit  
[AC-wlan-view] quit
```

Configure the source interface of the WAC.

```
[AC] capwap source interface vlanif4000
```

Import the AP offline on the WAC.

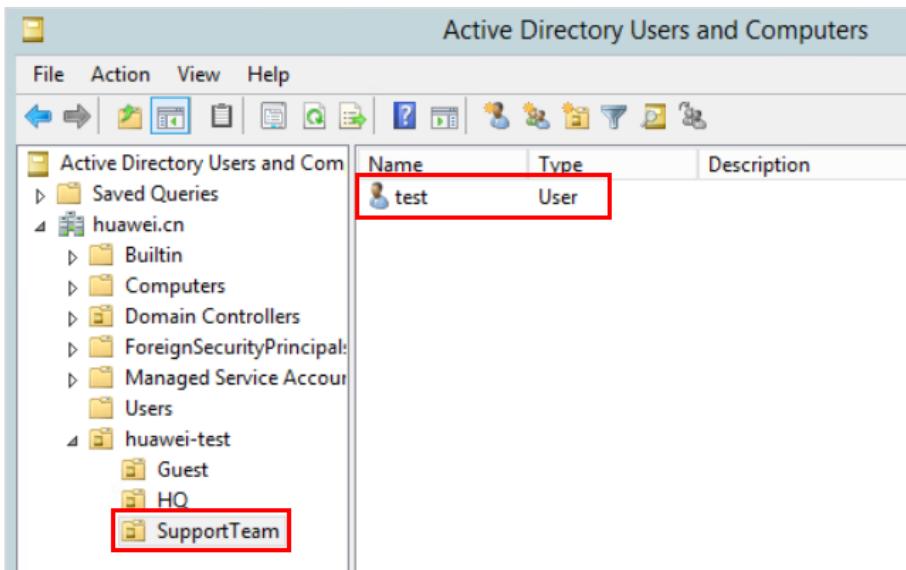
```
[AC] wlan  
[AC-wlan-view] ap auth-mode mac-auth  
[AC-wlan-view] ap-id 1 ap-mac 14ab-0228-5f80  
[AC-wlan-ap-1] ap-name a5760  
[AC-wlan-ap-1] ap-group ap-group1  
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power  
and antenna gain configurations of the radio, Whether to continue? [Y/N]:y  
[AC-wlan-ap-1] quit
```

Run the **display ap all** command to check the AP state. If the **State** field displays **nor**, the AP onboards properly.

```
[AC] display ap all  
Total AP information:  
nor : normal [1]  
ExtraInfo : Extra information  
-----  
ID MAC Name Group IP Type State STA Uptime ExtraInfo  
-----  
1 14ab-0228-5f80 a5760 ap-group1 10.10.1.226 AirEngine5760-51 nor 0 - -  
-----  
Total: 1
```

Step 4 Configure AD server parameters.

Create a user named **test** in **SupportTeam** on the AD server and set the password to **Huawei@123**.

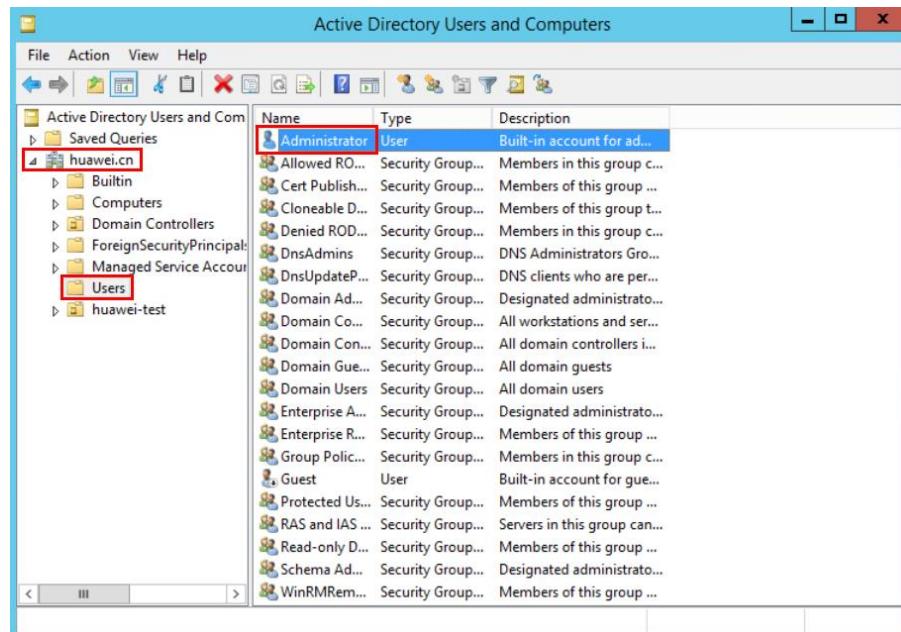


Query the parameters of the AD server.

As shown in the following figure, the Base DN (domain name) is **huawei.cn**.

The administrator account and password of the AD server are **Administrator** and **Huawei@123** respectively.

On the Windows Server page, the host name displays **WIN-Q2QSOCUE8QT.huawei.cn**.



Step 5 Configure AD server parameters for interconnection.

Create an AD server template on the WAC and set the parameters according to those in step 4.

```
[AC] ad-server template t1
[AC-ad-t1] ad-server authentication 172.16.30.100 88 no-ssl
Warning: The no-ssl configuration is not safe, it is recommended to config ldap-over-ssl type.
Continue?[Y/N]Y
```

```
[AC-ad-t1] ad-server authentication base-dn dc=huawei,dc=cn  
[AC-ad-t1] ad-server authentication manager cn=Administrator,cn=users Huawei@123  
[AC-ad-t1] ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn  
[AC-ad-t1] quit
```

Step 6 Configure Portal authentication and SSID.

Create a Portal access profile named **Portal-AD** and enable the built-in Portal server.

```
[AC] portal-access-profile name Portal-AD  
[AC-portal-access-profile-Portal-AD] portal local-server enable  
[AC-portal-access-profile-Portal-AD] quit
```

Set the IP address of the built-in Portal server to 10.20.1.1.

```
[AC] portal local-server ip 10.20.1.1
```

Set the port number of the built-in Portal server to 8080.

```
[AC] portal local-server http port 8080
```

Create authentication and authorization schemes named **AD**.

```
[AC] aaa  
[AC-aaa] authentication-scheme Portal-AD  
[AC-aaa-authen-Portal-AD] authentication-mode ad  
[AC-aaa-authen-Portal-AD] quit  
[AC-aaa] authorization-scheme AD  
[AC-aaa-author-AD] authorization-mode ad  
[AC-aaa-author-AD] quit
```

Create an authentication profile named **Portal-AD** and bind the Portal access profile, authentication scheme, authorization scheme, and AD server to the authentication profile.

```
[AC] authentication-profile name Portal-AD  
[AC-authentication-profile-Portal-AD] portal-access-profile Portal-AD  
[AC-authentication-profile-Portal-AD] authentication-scheme Portal-AD  
[AC-authentication-profile-Portal-AD] authorization-scheme AD  
[AC-authentication-profile-Portal-AD] ad-server t1  
[AC-authentication-profile-Portal-AD] quit
```

Create a security profile named **Portal-AD** and configure a security policy.

```
[AC] wlan  
[AC-wlan-view] security-profile name Portal-AD  
[AC-wlan-sec-prof-Portal-AD] security open  
[AC-wlan-sec-prof-Portal-AD] quit
```

Create an SSID profile named **Portal-AD** and set the SSID name to **Portal-AD**.

```
[AC-wlan-view] ssid-profile name Portal-AD  
[AC-wlan-ssid-prof-Portal-AD] ssid Portal-AD
```

```
[AC-wlan-ssid-prof-Portal-AD] quit
```

Create a VAP profile named **Portal-AD**, set the data forwarding mode to tunnel forwarding, set the service VLAN, and bind the security profile, authentication profile, and SSID profile to the VAP profile.

```
[AC-wlan-view] vap-profile name Portal-AD
[AC-wlan-vap-prof-Portal-AD] forward-mode tunnel
[AC-wlan-vap-prof-Portal-AD] service-vlan vlan-id 4001
[AC-wlan-vap-prof-Portal-AD] ssid-profile Portal-AD
[AC-wlan-vap-prof-Portal-AD] security-profile Portal-AD
[AC-wlan-vap-prof-Portal-AD] authentication-profile Portal-AD
[AC-wlan-vap-prof-Portal-AD] quit
```

Bind the VAP profile named **Portal-AD** to the AP group and apply configurations in this VAP profile to radio 0 and radio 1 of the APs in the AP group.

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile Portal-AD wlan 3 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile Portal-AD wlan 3 radio 1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

Set the local server authentication mode to PAP on the WAC.

```
[AC] portal local-server authentication-method pap
```

13.3 Verification

After the configuration is complete, verify the following:

1. Check whether AP onboarding is successful.
2. Check the connectivity between the WAC and the AD server and whether the user name and password can be used for login.
3. After the wireless terminal connects to the Wi-Fi network named **Portal-AD**, check whether the authentication page is displayed and whether the user name **test** and password **Huawei@123** can be used to ensure successful authentication.

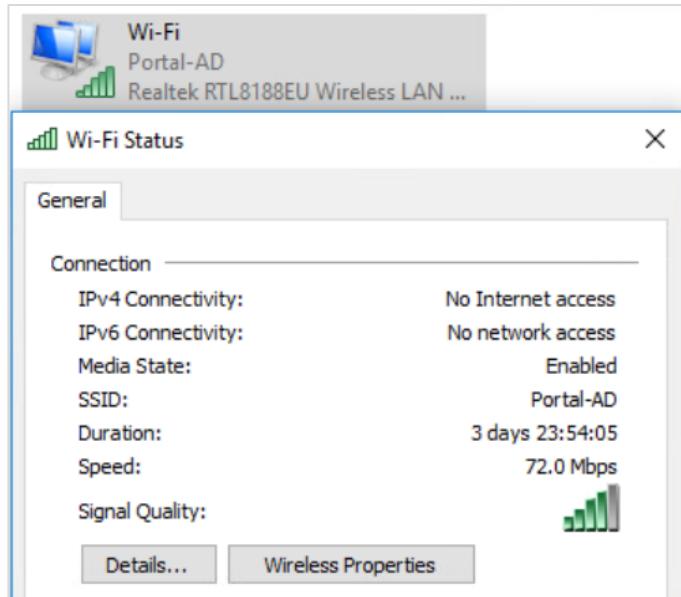
AP onboarding is successful on the WAC.

```
[AC] display ap all
Total AP information:
nor : normal      [1]
ExtraInfo : Extra information
-----
ID  MAC          Name  Group     IP           Type       State   STA   Uptime ExtraInfo
-----
1   14ab-0228-5f80 a5760 ap-group1 10.10.1.226 AirEngine5760-51 nor    0   -   -
-----
Total: 1
```

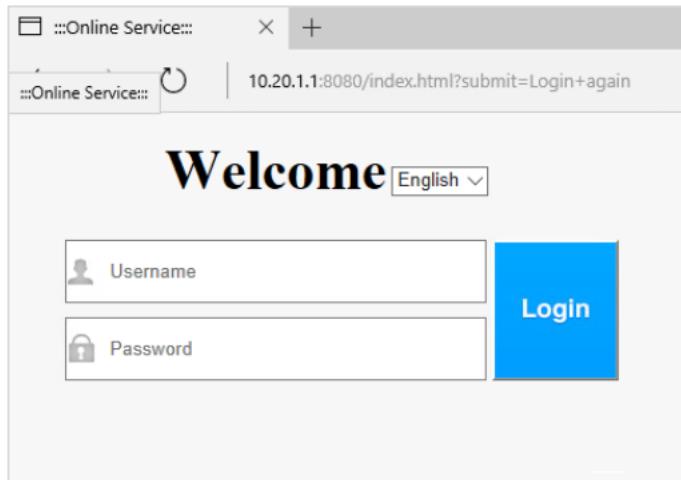
On the WAC, the account **test** and password **Huawei@123** can be used to ensure successful AD server authentication. This operation can be used to check whether the connectivity between the WAC and AD server is normal and whether the parameters are successfully configured.

```
[AC] test-aaa test Huawei@123 ad-template t1
Info: Server detection succeeded.
```

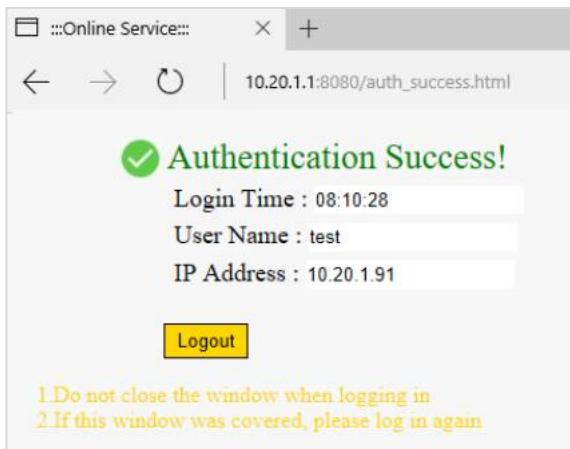
The wireless terminal can connect to the Wi-Fi network named **Portal-AD**.



Enter **1.1.1.1** in the address bar of the browser on the wireless terminal. The authentication page is displayed.



Enter the user name **test** and password **Huawei@123**, and click **Login**.



13.4 Configuration Reference

13.4.1 SW2's Configuration

```
#  
sysname SW2  
#  
vlan batch 10  
#  
interface GigabitEthernet0/0/2  
port link-type trunk  
undo port trunk allow-pass vlan 1  
port trunk allow-pass vlan 10  
#  
interface GigabitEthernet0/0/13  
port link-type access  
port default vlan 10  
#
```

13.4.2 SW3's Configuration

```
#  
sysname SW3  
#  
vlan batch 10 4000 4001  
#  
interface GigabitEthernet0/0/1  
port link-type trunk  
port trunk allow-pass vlan 10  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 10 4000 4001  
#  
interface GigabitEthernet0/0/12  
port link-type trunk
```

```
port trunk pvid vlan 4000
port trunk allow-pass vlan 4000
#
```

13.4.3 FW2's Configuration

```
#
sysname FW2
#
vlan batch 10
#
interface GigabitEthernet0/0/5
portswitch
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/6
portswitch
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
add interface GigabitEthernet0/0/6
#
security-policy
rule name pass
action permit
#
```

13.4.4 WAC's Configuration

```
#
sysname AC
#
http secure-server ssl-policy default_policy
http secure-server server-source -i all
http server enable
#
portal local-server ip 10.20.1.1
portal local-server authentication-method pap
portal local-server http port 8080
#
portal https-redirect tls1.1 enable
#
portal pass dns enable
#
vlan batch 10 4000 4001
```

```
#  
authentication-profile name Portal-AD  
    mac-access-profile Portal-AD  
    portal-access-profile Portal-AD  
    authentication-scheme Portal-AD  
    authorization-scheme AD  
    ad-server t1  
#  
dns resolve  
dns proxy enable  
#  
dhcp enable  
#  
ad-server template t1  
    ad-server authentication 172.16.30.100 88 no-ssl  
    ad-server authentication base-dn dc=huawei,dc=cn  
    ad-server authentication manager  
    cn=Administrator,cn=users %^%#fBzRQc;\\y6xPIIX`G#*~Kku#.Wch~-flrN4WjNM#%^%#  
    ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn  
    ad-server authentication ldap-port 389  
    ad-server user-filter sAMAccountName  
    ad-server group-filter ou  
    ad-server cipher-suite aes256-hmac-sha1  
#  
portal-access-profile name Portal-AD  
    portal local-server enable  
#  
ip pool vlan4001  
    gateway-list 10.20.1.1  
    network 10.20.1.0 mask 255.255.255.0  
#  
ip pool vlan4000  
    gateway-list 10.10.1.1  
    network 10.10.1.0 mask 255.255.255.0  
    option 43 sub-option 3 ascii 10.10.1.1  
#  
aaa  
    authentication-scheme Portal-AD  
        authentication-mode ad  
    authorization-scheme AD  
        authorization-mode ad  
#  
interface vlanif10  
    ip address 172.16.30.10 255.255.255.0  
#  
interface vlanif4000  
    ip address 10.10.1.1 255.255.255.0  
    dhcp select global  
#  
interface vlanif4001  
    ip address 10.20.1.1 255.255.255.0  
    dhcp select global  
#  
interface GigabitEthernet0/0/2  
    port link-type trunk
```

```
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10 4000 4001
#
capwap source interface wlanif4000
#
wlan
security-profile name Portal-AD
    security open
ssid-profile name Portal-AD
    ssid Portal-AD
vap-profile name Portal-AD
    forward-mode tunnel
    service-vlan vlan-id 4001
    ssid-profile Portal-AD
    security-profile Portal-AD
    authentication-profile Portal-AD
    ap-group name ap-group1
        radio 0
            vap-profile Portal-AD wlan 3
        radio 1
            vap-profile Portal-AD wlan 3
        radio 2
            vap-profile Portal-AD wlan 3
ap-id 1 type-id 130 ap-mac 14ab-0228-5f80 ap-sn 2102353GES6RN5008931
    ap-name a5760
    ap-group ap-group1
#
return
```

13.5 Quiz

How do I open the Portal authentication page of a third-party server?

Answer: Configure **web-auth-server** and bind it to **portal-access-profile**.

14 Portal Authentication Troubleshooting

14.1 Introduction

14.1.1 About This Lab

Enterprises usually deploy WLANs to provide wireless office environments for employees. For security purposes, the enterprises want to authenticate their employees through an AD server deployed on the intranet.

This lab sets the common faults that may occur during configuring and using Portal authentication and describes how to troubleshoot these faults through the AD server.

14.1.2 Objectives

- Understand the process of Portal authentication.
- Learn to identify Portal authentication faults.
- Understand how to troubleshoot common Portal authentication faults.

14.1.3 Networking Topology

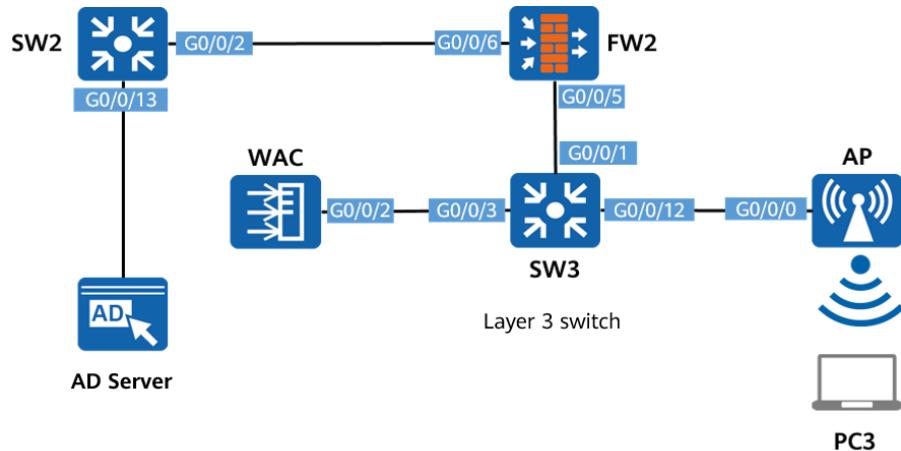


Figure 14-1 Portal wireless authentication

The preceding figure shows device connections. For details about IP address planning, see Table 14-1.

Layer 2 networking is used between the WAC and AP, and between the WAC and AD server. For key configurations of interfaces, see 14.4 Configuration Reference.

1. An external power module is used to supply power to the AP based on the existing scenario.
2. Layer 2 networking is used between the AP and WAC. The DHCP address pools of the AP and terminal are obtained from the WAC.
3. Layer 2 networking is used between the WAC and AD server. Authentication for the wireless terminal is performed by the AD server.
4. FW2 only transparently transmits packets.
5. SSID for network access: Portal authentication is required for connecting to the Wi-Fi named **HCIP-Security** and the local Portal page of the WAC is used.

14.1.4 Lab Planning

Table 14-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
SW2	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to FW2
	G0/0/13	Access	PVID: 10	Interface for connecting to AD Server
SW3	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to FW2
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	Interface for connecting to the WAC
	G0/0/12	Trunk	PVID: 4000 Allow-pass VLAN: 4000	Interface for connecting to the AP
FW2	GE0/0/5	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to SW3
	GE0/0/6	Trunk	PVID: 1 Allow-pass VLAN: 10	Interface for connecting to SW2
WAC	GE0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	Interface for connecting to SW3
AP	GE0/0/0	/	Retain default settings.	Interface for

				connecting to SW3
AD Server	Ethernet0	Network adapter	172.16.30.100/24	Server IP

14.2 Lab Configuration

14.2.1 Configuration Roadmap

1. Import the pre-configurations to the corresponding devices.
2. Check whether services are normal according to the lab planning and rectify faults one by one.

14.2.2 Configuration Procedure

Step 1 Pre-configure devices.

Construct the network according to the lab topology, disable the interfaces that are not used in the lab, and import the pre-configuration scripts to the corresponding devices for device pre-configuration.

Pre-configure SW2.

```
#  
sysname SW2  
#  
vlan batch 10  
#  
interface GigabitEthernet0/0/2  
    port link-type trunk  
    undo port trunk allow-pass vlan 1  
    port trunk allow-pass vlan 10  
#  
interface GigabitEthernet0/0/13  
    port link-type access  
    port default vlan 10  
#
```

Pre-configure SW3.

```
#  
sysname SW3  
#  
vlan batch 10 4000 4001  
#  
interface GigabitEthernet0/0/1  
    port link-type trunk  
    port trunk allow-pass vlan 10  
#  
interface GigabitEthernet0/0/3
```

```
port link-type trunk
port trunk allow-pass vlan 10 4000 4001
#
interface GigabitEthernet0/0/12
port link-type trunk
port trunk pvid vlan 4000
port trunk allow-pass vlan 4000
#
```

Pre-configure FW2.

```
#
sysname FW2
#
vlan batch 10
#
interface GigabitEthernet0/0/5
portswitch
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/6
portswitch
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
add interface GigabitEthernet0/0/6
#
security-policy
rule name pass
action permit
#
```

Pre-configure the WAC.

```
#
sysname AC
#
http secure-server ssl-policy default_policy
http secure-server server-source -i all
Y
http server enable
#
portal local-server ip 10.20.1.1
portal local-server http port 8080
#
portal https-redirect tls1.1 enable
Y
```

```
#  
vlan batch 10 4000 4001  
#  
dns resolve  
dns proxy enable  
Y  
#  
dhcp enable  
#  
interface vlanif10  
    ip address 172.16.30.10 255.255.255.0  
#  
interface vlanif4000  
    ip address 10.10.1.1 255.255.255.0  
    dhcp select global  
#  
interface vlanif4001  
    ip address 10.20.1.1 255.255.255.0  
    dhcp select global  
#  
ad-server template t1  
    ad-server authentication 172.16.30.100 88 no-ssl  
Y  
    ad-server authentication base-dn dc=huawei,dc=cn  
    ad-server authentication manager cn=Administrator,cn=users Huawei@123  
    ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn  
    ad-server authentication ldap-port 389  
    ad-server user-filter sAMAccountName  
    ad-server group-filter ou  
    ad-server cipher-suite aes256-hmac-sha1  
#  
portal-access-profile name Portal-AD  
    portal http-proxy-redirect enable  
#  
ip pool vlan4001  
    gateway-list 10.20.1.1  
    network 10.20.1.0 mask 255.255.255.0  
#  
ip pool vlan4000  
    gateway-list 10.10.1.1  
    network 10.10.1.0 mask 255.255.255.0  
    option 43 sub-option 3 ascii 10.10.1.1  
#  
aaa  
    authentication-scheme Portal-AD  
        authentication-mode ad  
    authorization-scheme AD  
        authorization-mode ad  
#  
authentication-profile name Portal-AD  
authentication-scheme Portal-AD  
authorization-scheme AD  
ad-server t1  
#  
interface GigabitEthernet0/0/2
```

```
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10 4000 4001
#
wlan
    security-profile name Portal-AD
        security open
Y
Y
ssid-profile name Portal-AD
    ssid Portal-AD
vap-profile name Portal-AD
    forward-mode tunnel
    service-vlan vlan-id 4001
    ssid-profile Portal-AD
    security-profile Portal-AD
Y
ap-group name ap-group1
radio 0
    vap-profile Portal-AD wlan 3
radio 1
    vap-profile Portal-AD wlan 3
radio 2
    vap-profile Portal-AD wlan 3
ap-id 1 type-id 130 ap-mac 14ab-0228-5f80 ap-sn 2102353GES6RN5008931
    ap-name a5760
Y
ap-group ap-group1
Y
#
```

Configure the source interface of the CAPWAP tunnel on the WAC and configure the corresponding password. For details, see the following configurations in bold.

[AC] capwap source interface vlanif 4000
Set the DTLS inter-controller PSK(contains 8-32 plain-text characters, or 48 or 68 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):**Huawei@123**
Confirm PSK:**Huawei@123**
Configuring the new PSK, waiting.....done.

Info: Deliver DTLS PSK to devices using CAPWAP connections. It may take a few minutes.

CAPWAP DTLS PSK deliver result
Deliver Number : 0
Success Number : 0
Failed Number : 0

-----done.
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters, underscores, and digits, and must start with a letter):**admin**
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters):**Huawei@123**
Confirm password:**Huawei@123**

Set the global temporary-management psk (contains 8-63 plain-text characters, or 48-108 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): **Huawei@123**

Confirm PSK: **Huawei@123**

Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be interrupted.

Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.

Step 2 Check the network connection of the wireless terminal.

The Wi-Fi network named **Portal-AD** is not recorded by the wireless network adapter of the wireless terminal.

Check AP onboarding on the WAC.

```
[AC] display ap all
```

Total AP information:

idle : idle [1]

ExtraInfo : Extra information

ID	MAC	Name	Group	IP Type	State	STA	Uptime	ExtraInfo
1	14ab-0228-5f80	a5760	ap-group1 -	AirEngine5760-51	idle	0	-	-

Total: 1

The AP onboarding fails, but the relevant configurations are correct. When the WAC connects to an AP running V200R021C00 or later, AP onboarding may fail due to a lack of DTLS certificate. In this case, perform the following operations:

Enable the function of establishing CAPWAP DTLS sessions through the preset certificate.

```
[AC] capwap dtls cert-mandatory-match enable
```

Warning: This operation allows for device access using the preset certificate when DTLS is enabled and brings security risks. After the device goes online for the first time, disable this function to prevent security risks. Continue?[Y/N]:Y

Note: When adding an AP running V200R021C00 or later, you can enable this function to allow the AP to establish a DTLS session through the preset certificate to prevent AP onboarding failures. After AP onboarding, the AP obtains a new DTLS certificate to initiate a DTLS session securely and onboard again. To ensure network security, disable this function immediately after the AP onboards again to prevent unauthorized APs from accessing the network.

Check AP onboarding again.

```
[AC] display ap all
```

Total AP information:

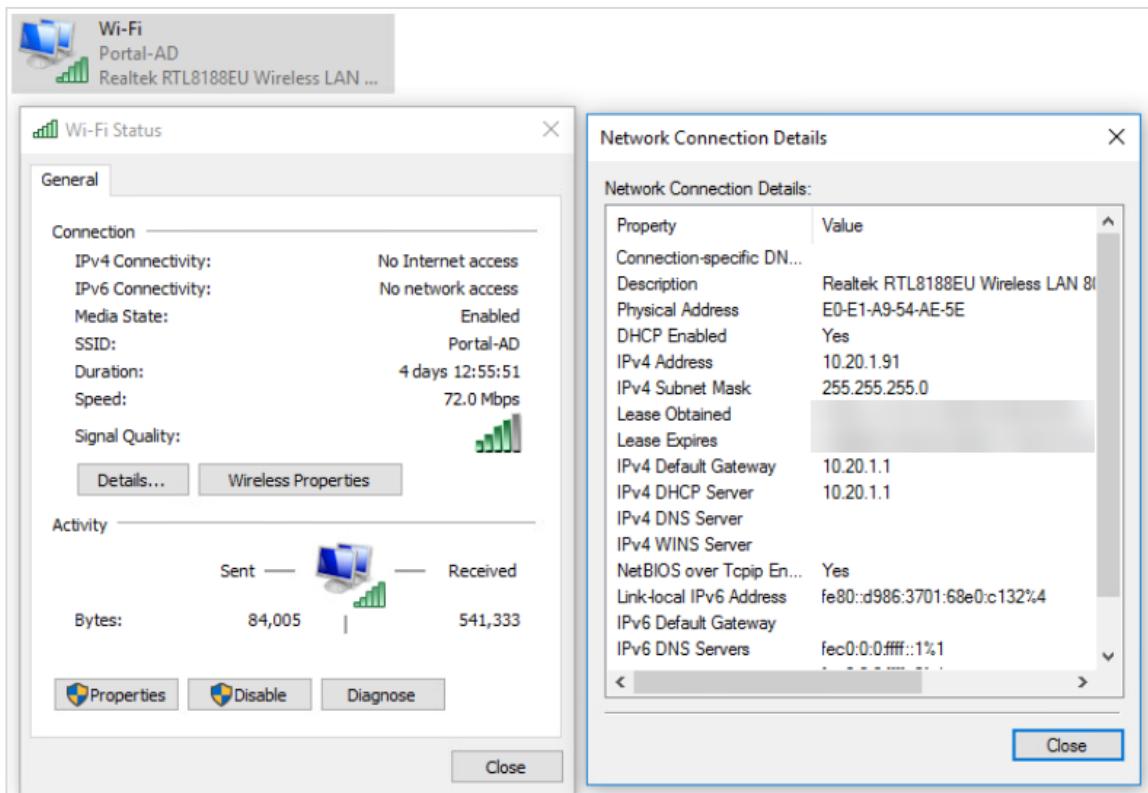
nor : normal [1]

ExtraInfo : Extra information

ID	MAC	Name	Group	IP	Type	State	STA	Uptime	ExtraInfo
----	-----	------	-------	----	------	-------	-----	--------	-----------

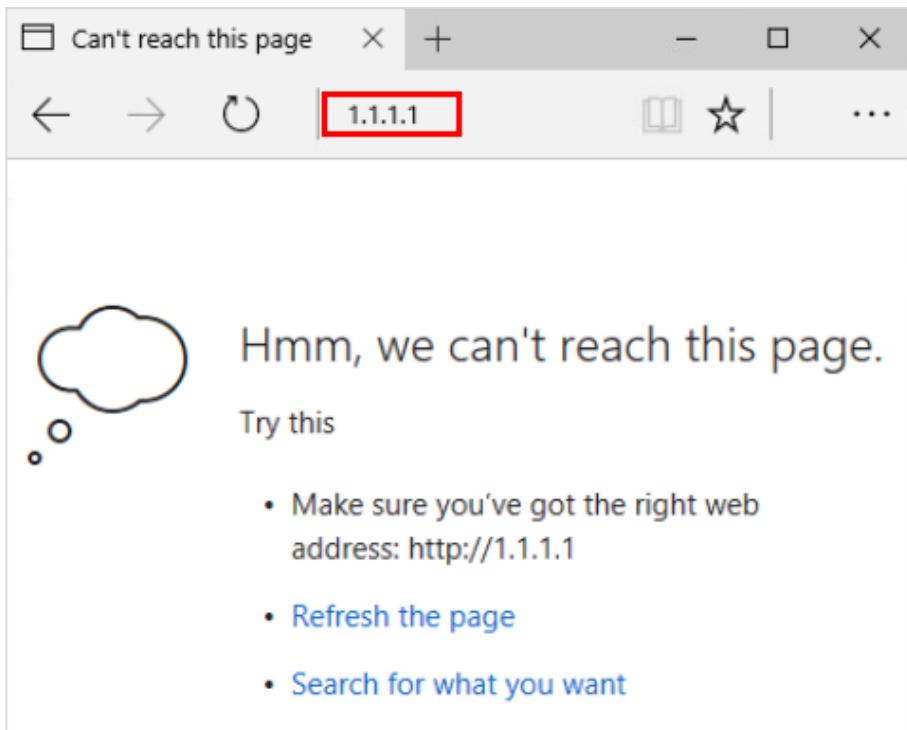
1	14ab-0228-5f80	a5760	ap-group1	10.10.1.131	AirEngine5760-51	nor	0	24S	-
Total: 1									

The wireless terminal can connect to the Wi-Fi network named Portal-AD.



Step 3 Check Portal page display.

After the wireless terminal successfully connects to the Wi-Fi network, enter a random IP address in the address bar of the browser on the terminal and press **Enter**. No Portal page is displayed.



The preceding result indicates that the local Portal page of the WAC does not respond. The possible causes are as follows: The wireless terminal cannot communicate with the WAC. The Portal authentication configurations are incorrect. Configurations of the local Portal page on the WAC are incorrect. You need to check the possible causes one by one.

Check whether the wireless terminal can ping the IP address of the Portal server on the WAC.

```
C:\Users\Security>ping 10.20.1.1

Pinging 10.20.1.1 with 32 bytes of data:
Reply from 10.20.1.1: bytes=32 time=27ms TTL=255
Reply from 10.20.1.1: bytes=32 time=36ms TTL=255
Reply from 10.20.1.1: bytes=32 time=7ms TTL=255
Reply from 10.20.1.1: bytes=32 time=11ms TTL=255

Ping statistics for 10.20.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 36ms, Average = 20ms
```

Check the Portal authentication configurations.

```
#  
authentication-profile name Portal-AD  
  
    authentication-scheme Portal-AD  
    authorization-scheme AD  
    ad-server t1  
#
```

The authentication and authorization schemes are bound to the authentication profile, but the Portal access profile is not bound.

Check the configurations in the Portal access profile.

```
#  
portal-access-profile name Portal-AD  
    portal http-proxy-redirect enable  
#
```

The local Portal server page of the WAC is used in this lab. Therefore, the configurations are incorrect.

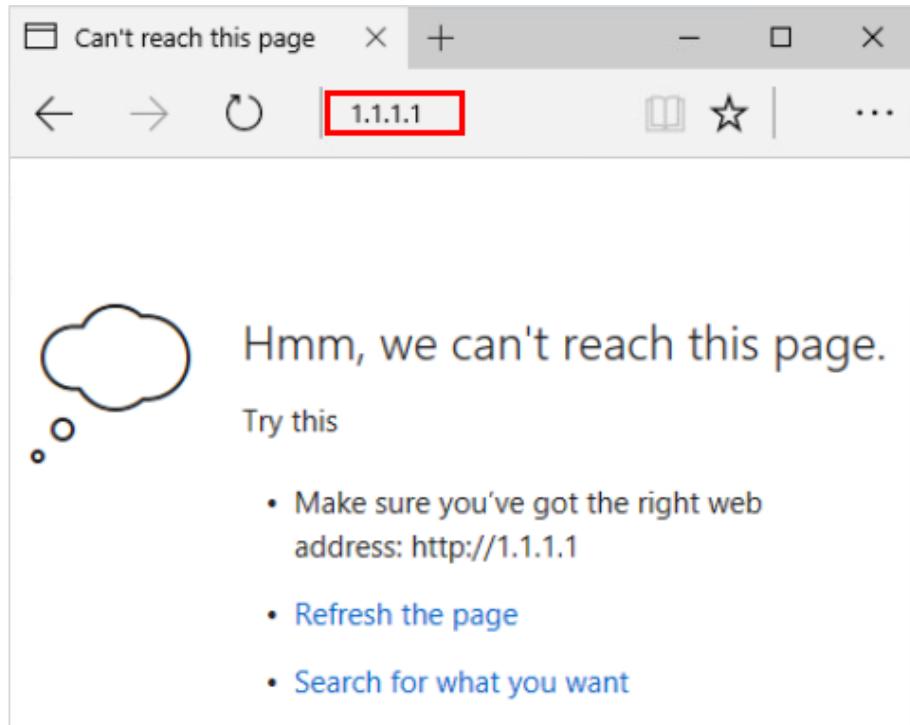
Modify the configurations in the Portal access profile and enable the built-in Portal server.

```
[AC] portal-access-profile name Portal-AD  
[AC-portal-access-profile-Portal-AD] undo portal http-proxy-redirect enable  
[AC-portal-access-profile-Portal-AD] portal local-server enable  
[AC-portal-access-profile-Portal-AD] quit
```

Bind the Portal access profile to the authentication profile.

```
[AC] authentication-profile name Portal-AD  
[AC-authentication-profile-Portal-AD] portal-access-profile Portal-AD  
[AC-authentication-profile-Portal-AD] quit
```

Use the wireless terminal to perform the test again. The Portal page cannot be opened on the browser.



According to the configuration roadmap, the Portal access profile needs to be bound to the authentication profile, which then needs to be bound to the VAP profile view.

Check the configurations in the VAP profile view.

```
[AC] wlan
```

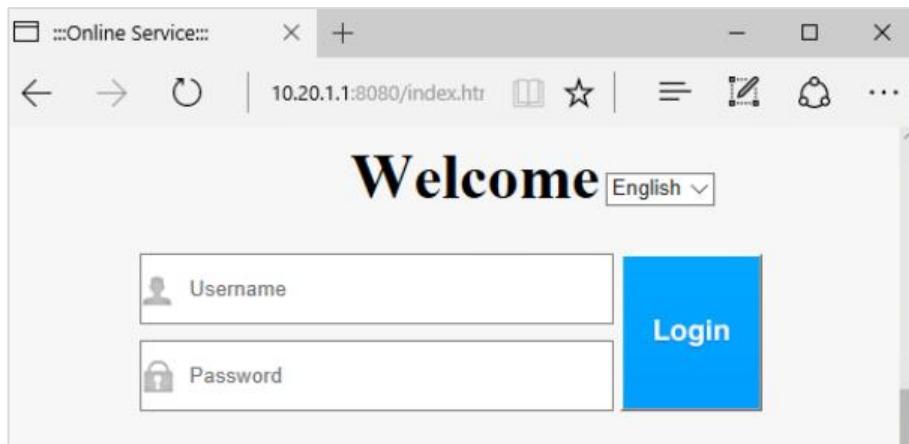
```
[AC-wlan-view] vap-profile name Portal-AD
[AC-wlan-vap-prof-Portal-AD] display this
#
forward-mode tunnel
service-vlan vlan-id 4001
ssid-profile Portal-AD
security-profile Portal-AD
#
```

The preceding configurations indicate that the authentication profile is not bound to the VAP profile view.

Complete the configurations in the VAP profile view.

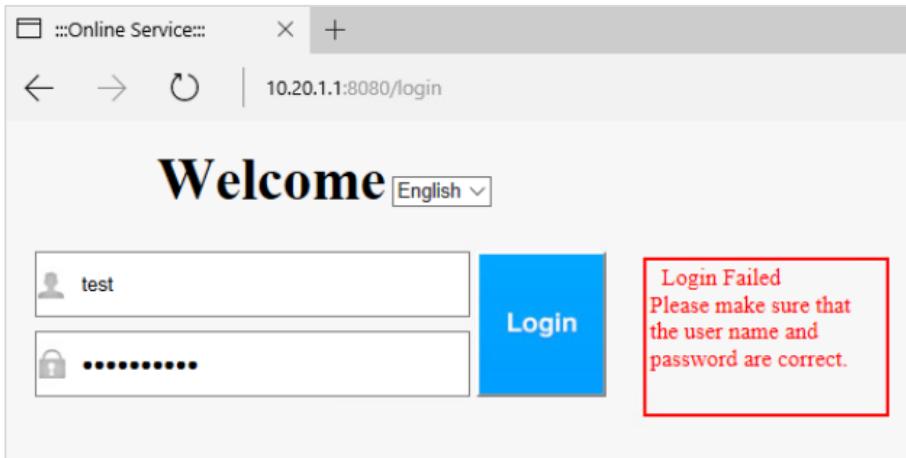
```
[AC] wlan
[AC-wlan-view] vap-profile name Portal-AD
[AC-wlan-vap-prof-Portal-AD] authentication-profile Portal-AD
Warning: This action may cause service interruption. Continue?[Y/N]Y
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-Portal-AD] quit
```

Use the wireless terminal to perform the test again. The built-in Portal page of the WAC can be opened in the browser.



Step 4 Check AD authentication.

On the Portal page, enter the user name **test** and password **Huawei@123** on the AD server for test.



The user authentication fails. When the user enters the user name and password for authentication, the user name and password are forwarded by the WAC and then verified by the AD server.

Check the configurations of **authentication-scheme Portal-AD** on the WAC.

```
[AC] aaa
[AC-aaa] authentication-scheme Portal-AD
[AC-aaa-authen-Portal-AD] display this
#
  authentication-scheme Portal-AD
    authentication-mode ad
#
#
```

The authentication mode is AD authentication, which is correct.

Check the configurations of **authorization-scheme Portal-AD** on the WAC.

```
[AC] aaa
[AC-aaa] authorization-scheme Portal-AD
[AC-aaa-author-Portal-AD] display this
#
  authorization-scheme Portal-AD
    authorization-mode ad
#
#
```

The authorization mode is AD authorization, which is correct.

Check the AD server configurations on the WAC.

```
[AC] ad-server template t1
[AC-ad-t1] display this
#
ad-server template t1
  ad-server authentication 172.16.30.100 88 no-ssl
  ad-server authentication base-dn dc=huawei,dc=cn
  ad-server authentication manager
  cn=Administrator,cn=users %^%#fBzRQc;y6xPILX`G#*~Kku#.Wch~-flrN4WjNM#%^%#
  ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn
  ad-server authentication ldap-port 389
  ad-server user-filter sAMAccountName
```

```
ad-server group-filter ou  
ad-server cipher-suite aes256-hmac-sha1  
#
```

The parameters are correctly configured.

On the WAC, test whether the user name and password are recorded on the AD server.

```
[AC] test-aaa test Huawei@123 ad-template t1  
Info: Server detection succeeded.
```

The preceding result indicates that the interconnection parameters between the WAC and AD server as well as the user name, and password are correct. Therefore, the fault occurs on the wireless terminal and WAC.

Run debugging commands on the WAC and enter the user name and password again on the wireless terminal for login.

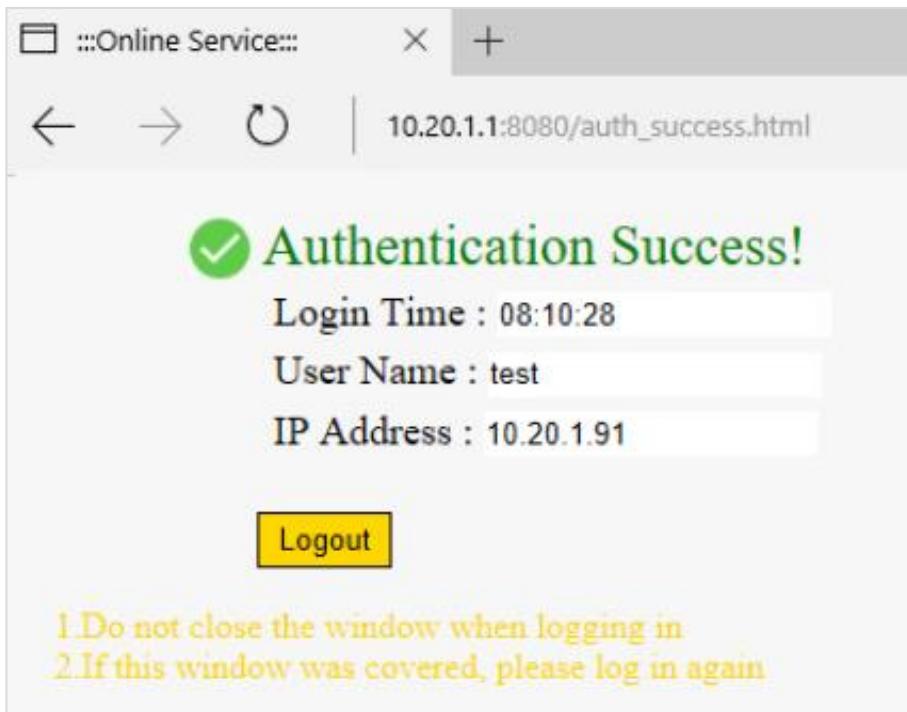
```
<AC> debugging portal event  
<AC> debugging portal message  
<AC> terminal debugging  
<AC> terminal monitor  
<AC> Aug 15 XXXX 01:29:06.804.1+00:00  
AC %%01WEBS/4/USER_ACCESSRESULT(l)[0]:[WEBS_USER_ONLINEFAIL]USERNAME:test;IPADDRESS:  
10.20.1.202;MAC:-;ERRCODE:303;
```

ERRCODE:303: Portal server authentication fails. According to documentations, Portal authentication supports AD/LDAP authentication, but the authentication mode must be set to PAP. Because the built-in Portal server uses CHAP authentication by default, you need to run the **portal local-server authentication-method { chap | pap }** command to manually set the authentication mode to PAP.

Change the built-in Portal authentication mode of the WAC to PAP.

```
[AC] portal local-server authentication-method pap
```

On the Portal page, enter the user name **test** and password **Huawei@123** on the AD server. The test is successful.



14.3 Verification

After the configuration is complete, verify the following:

1. Check whether AP onboarding is successful.
2. Check the connectivity between the WAC and the AD server and whether the user name and password can be used for login.
3. After the wireless terminal connects to the Wi-Fi network named **Portal-AD**, check whether the authentication page is displayed and whether the user name **test** and password **Huawei@123** can be used to ensure successful authentication.

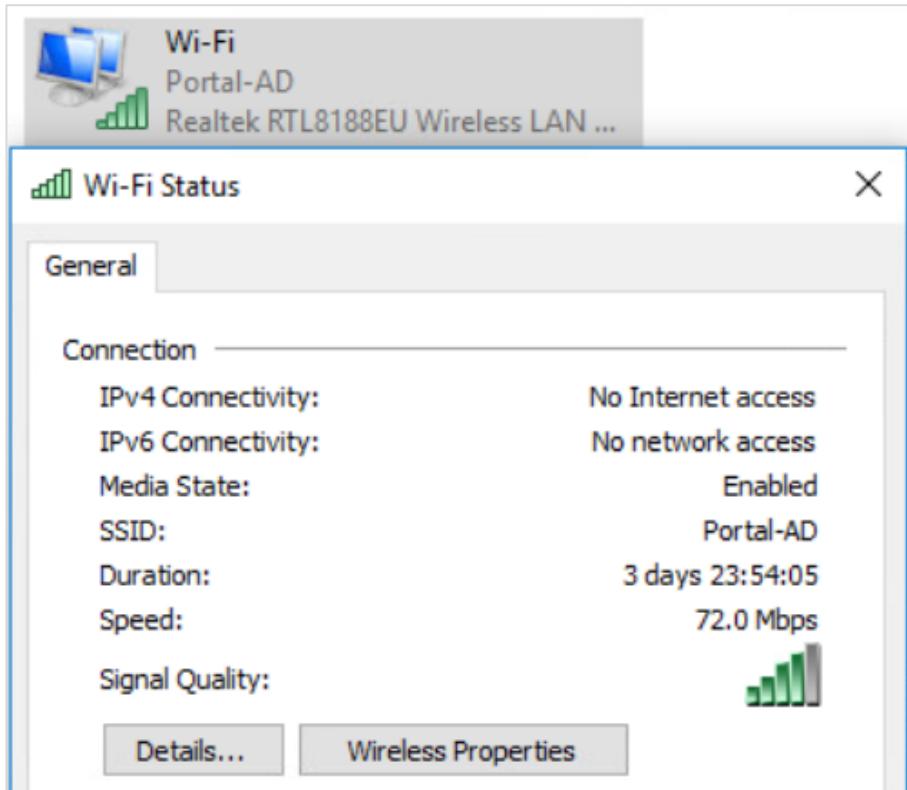
AP onboarding is successful on the WAC.

```
[AC] display ap all
Total AP information:
nor  : normal      [1]
ExtraInfo : Extra information
-----
ID  MAC          Name  Group    IP           Type       State  STA   Uptime ExtraInfo
-----
1  14ab-0228-5f80 a5760 ap-group1 10.10.1.226 AirEngine5760-51 nor  0  -   -
-----
Total: 1
```

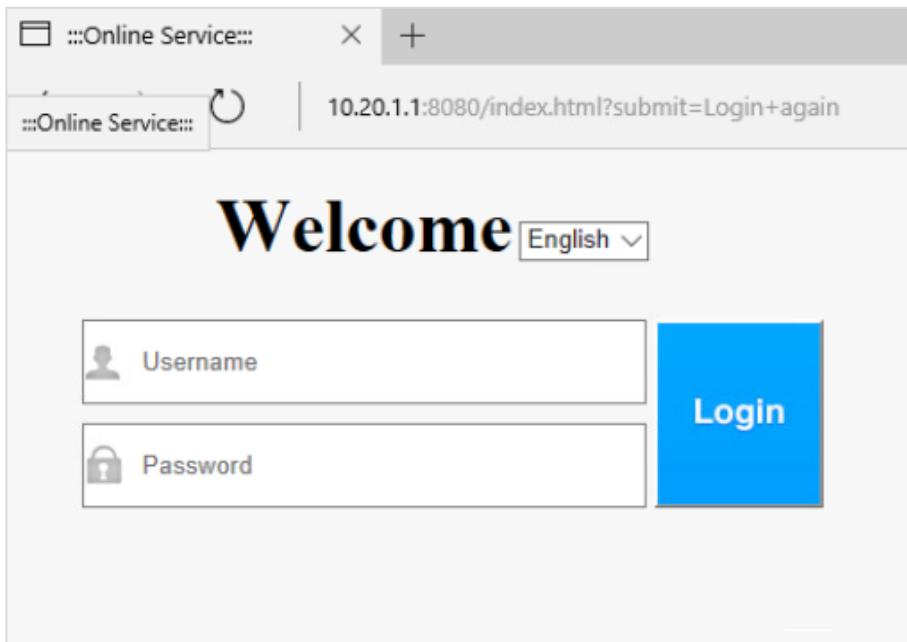
On the WAC, the account **test** and password **Huawei@123** can be used to ensure successful AD server authentication. This operation can be used to check whether the connectivity between the WAC and AD server is normal and whether the parameters are successfully configured.

```
[AC] test-aaa test Huawei@123 ad
[AC] test-aaa test Huawei@123 ad-template t1
Info: Server detection succeeded.
```

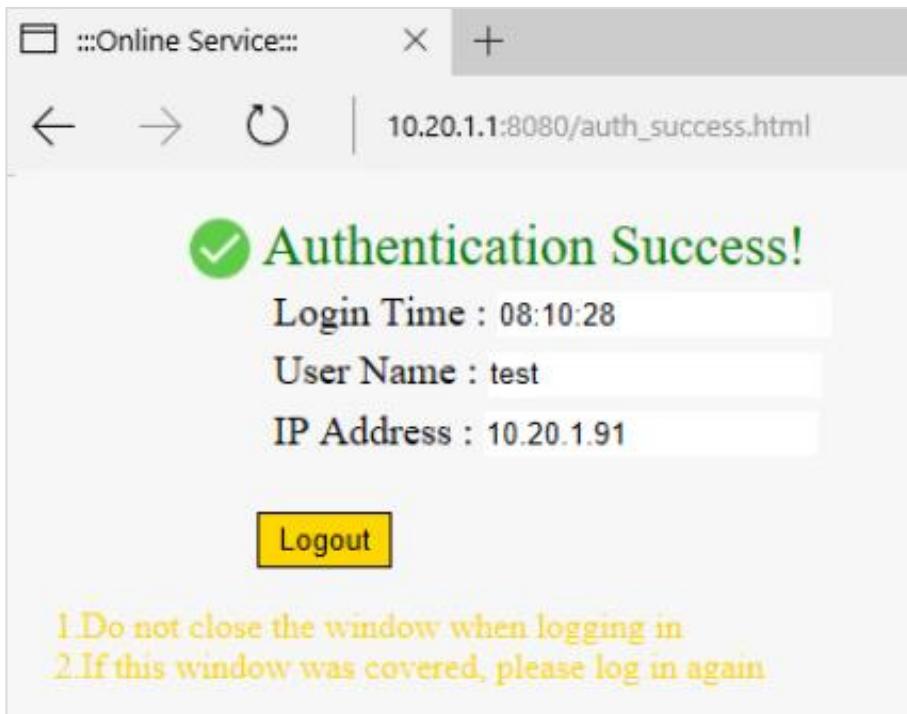
The wireless terminal can connect to the Wi-Fi network named Portal-AD.



Enter 1.1.1.1 in the address bar of the browser on the wireless terminal, the authentication page is displayed.



Enter the user name **test** and password **Huawei@123**, and click **Login**.



14.4 Configuration Reference

14.4.1 SW2's Configuration

```
#  
sysname SW2  
#  
vlan batch 10  
#  
interface GigabitEthernet0/0/2  
port link-type trunk  
undo port trunk allow-pass vlan 1  
port trunk allow-pass vlan 10  
#  
interface GigabitEthernet0/0/13  
port link-type access  
port default vlan 10  
#
```

14.4.2 SW3's Configuration

```
#  
sysname SW3  
#  
vlan batch 10 4000 4001  
#  
interface GigabitEthernet0/0/1  
port link-type trunk
```

```
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 10 4000 4001
#
interface GigabitEthernet0/0/12
port link-type trunk
port trunk pvid vlan 4000
port trunk allow-pass vlan 4000
#
```

14.4.3 FW2's Configuration

```
#
sysname FW2
#
vlan batch 10
#
interface GigabitEthernet0/0/5
portswitch
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/6
portswitch
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
add interface GigabitEthernet0/0/6
#
security-policy
rule name pass
action permit
#
```

14.4.4 WAC's Configuration

```
#
sysname AC
#
http secure-server ssl-policy default_policy
http secure-server server-source -i all
http server enable
#
portal local-server ip 10.20.1.1
```

```
portal local-server authentication-method pap
portal local-server http port 8080
#
portal https-redirect tls1.1 enable
#
portal pass dns enable
#
vlan batch 10 4000 4001
#
dns resolve
dns proxy enable
#
dhcp enable
#
ad-server template t1
ad-server authentication 172.16.30.100 88 no-ssl
ad-server authentication base-dn dc=huawei,dc=cn
ad-server authentication manager
cn=Administrator,cn=users %^%#fBzRQc;\y6xPILX`G#*~Kku#.Wch~-flrN4WjNM#%^%#
ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn
ad-server authentication ldap-port 389
ad-server user-filter sAMAccountName
ad-server group-filter ou
ad-server cipher-suite aes256-hmac-sha1
#
portal-access-profile name Portal-AD
    portal local-server enable
#
ip pool vlan4001
    gateway-list 10.20.1.1
    network 10.20.1.0 mask 255.255.255.0
#
ip pool vlan4000
    gateway-list 10.10.1.1
    network 10.10.1.0 mask 255.255.255.0
    option 43 sub-option 3 ascii 10.10.1.1
#
aaa
    authentication-scheme Portal-AD
        authentication-mode ad
    authorization-scheme AD
        authorization-mode ad
#
authentication-profile name Portal-AD
    portal-access-profile Portal-AD
        authentication-scheme Portal-AD
    authorization-scheme AD
    ad-server t1
#
interface vlanif10
    ip address 172.16.30.10 255.255.255.0
#
interface vlanif4000
    ip address 10.10.1.1 255.255.255.0
    dhcp select global
```

```
#  
interface vlanif4001  
    ip address 10.20.1.1 255.255.255.0  
    dhcp select global  
#  
interface GigabitEthernet0/0/2  
    port link-type trunk  
    undo port trunk allow-pass vlan 1  
    port trunk allow-pass vlan 10 4000 4001  
#  
capwap source interface vlanif4000  
#  
wlan  
    security-profile name Portal-AD  
    security open  
    ssid-profile name Portal-AD  
    ssid Portal-AD  
    vap-profile name Portal-AD  
        forward-mode tunnel  
        service-vlan vlan-id 4001  
        ssid-profile Portal-AD  
        security-profile Portal-AD  
        authentication-profile Portal-AD  
        ap-group name ap-group1  
            radio 0  
                vap-profile Portal-AD wlan 3  
            radio 1  
                vap-profile Portal-AD wlan 3  
            radio 2  
                vap-profile Portal-AD wlan 3  
ap-id 1 type-id 130 ap-mac 14ab-0228-5f80 ap-sn 2102353GES6RN5008931  
ap-name a5760  
ap-group ap-group1  
#
```

14.5 Quiz

In the preceding WAC + Fit AP networking scenario, which of the following are possible causes for AP onboarding failures?

Answer: There are many possible causes for AP onboarding failures and the major ones are as follows:

Physical device failures: AP failures, WAC failures, intermediate network device failures, cable failures, etc.

Power supply failures: Insufficient power supply of switches, incorrect power supply modes, etc.

Network configuration failures: incorrect DHCP configurations, failures to obtain IP addresses by APs, unreachable network between the AP and WAC, incorrect AP authentication configurations, incorrect source address of the CAPWAP tunnel, incorrect blacklist and whitelist configurations on the WAC, etc.

Software version failures: Unmatched AP and WAC software versions, software version

upgrade failures, etc.

License: occupation of all license resources on the WAC, etc.

15 Enterprise Network Security Deployment

15.1 Introduction

15.1.1 About This Lab

As campus network services increase, service attributes become more important. To ensure stable service running, enterprises have higher requirements on the overall planning of enterprise network topologies and network security.

This lab covers the design of a typical campus network, including the tasks of configuring link redundancy, device redundancy, VPN encrypted data transmission, service isolation, important service assurance, user authentication, user behavior audit, attack defense, and WLAN security policies. After completing these lab tasks, trainees shall understand the design logic of typical campus network topologies, master security protection methods of campus networks, and finally be able to build campus networks.

15.1.2 Objectives

- Learn how to design a campus network.
- Have a good command of key campus network technologies.
- Implement secure network interworking.

15.1.3 Networking Topology

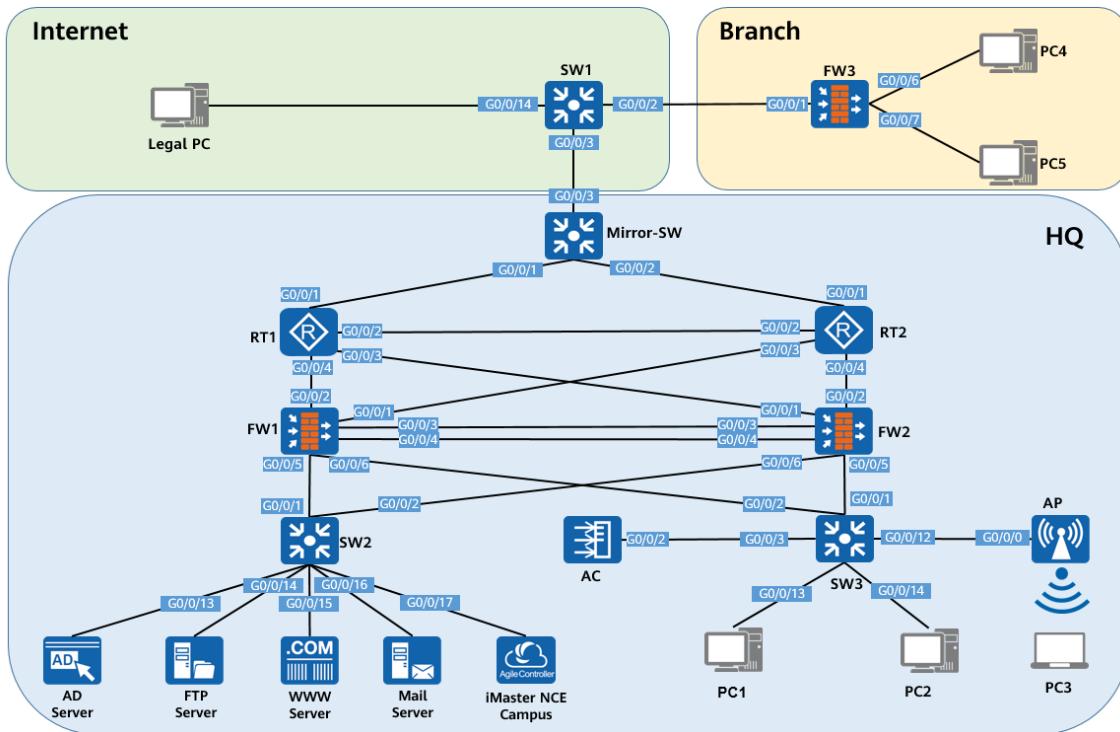


Figure 15-1 Comprehensive lab topology

The preceding figure shows device connections. For details about IP address planning, see Table 15-1.

The lab topology includes the HQ zone, branch zone, and Internet zone, simulating various service requirements on a campus network.

In the HQ zone, the gateway of the servers and wired PCs is deployed on the firewalls, which are FW1 and FW2 working in hot standby mode. The IP address of this gateway is the VRRP virtual IP address. The gateway of PC3 is deployed on the WAC. OSPF runs between FW1, FW2, RT1, and RT2. A PC is used to simulate a legal terminal, and servers are used to simulate an Internet website, an FTP server, and so on.

A firewall (FW3) is deployed at the egress of the branch zone. PC4 and PC5 are used to simulate services. The gateway of the PCs is deployed on the firewall.

The networking requirements are as follows:

1. Deploy devices and links in redundancy mode for key network nodes in the HQ zone. Configure the two firewalls to work in hot standby mode. Enable VRRP between the firewalls and switches. Configure OSPF between the firewalls and egress routers. All these ensure high network reliability. In addition, most traffic is transmitted over high-quality links, which prevents resource waste.
2. Establish an IPsec VPN tunnel between the HQ zone and branch zone to guarantee the confidentiality of service data exchanged between the two zones.
3. Deploy an SSL VPN in network expansion mode on the firewalls in the HQ zone to allow employees on business trips to access intranet resources.

4. Configure virtual systems on the egress firewall in the branch zone to strictly isolate the R&D area (where PC4 is located) from the guest area (where PC5 is located).
5. Deploy an anti-DDoS device at the egress of the HQ zone to prevent servers in the HQ zone from being attacked.
6. Authenticate the identity of employees in the HQ zone when they attempt to access the intranet. In addition, user behaviors need to be controlled. For example, employees are forbidden to disclose important information or release violation information and are restricted to access specific websites.
7. Prevent employees from disclosing confidential information through emails, and prevent spam from occupying too many resources or affecting employees' normal email sending and receiving.

15.1.4 Lab Planning

Table 15-1 Interface planning

Device	Interface	Interface Type	Interface Information	Description
SW1	G0/0/2	Access	PVID: 1	Interface for connecting to FW3
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interface for connecting to Mirror-SW
	G0/0/14	Access	PVID: 200	Interface for connecting to the legal PC
	G0/0/15	Access	PVID: 300	Interface for connecting to the FTP server or WWW server
	VLANIF1	Layer 3 interface	100.1.1.1/24	Interface for connecting to FW3
	VLANIF2	Layer 3 interface	4.4.4.1/30	On the same network segment as an RT1 interface
	VLANIF40	Layer 3 interface	3.3.3.1/30	On the same network segment as an RT2 interface

	VLANIF200	Layer 3 interface	20.20.1.1/30	Legal PC gateway
SW2	G0/0/1	Access	PVID: 30	Interface for connecting to FW1
	G0/0/2			Interface for connecting to FW2
	G0/0/13			Interface for connecting to the AD server
	G0/0/14			Interface for connecting to the FTP server
	G0/0/15			Interface for connecting to the WWW server
	G0/0/16			Interface for connecting to the mail server
	G0/0/17			Interface for connecting to iMaster NCE-Campus
SW3	G0/0/1	Access	PVID: 40	Interface for connecting to FW2
	G0/0/2	Access	PVID: 40	Interface for connecting to FW1
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 10, 40, 2000, 4000	Interface for connecting to WAC
	G0/0/12	Trunk	PVID: 4000 Allow-pass VLAN: 4000	Interface for connecting to the AP
	G0/0/13	Access	PVID: 40	Interface for connecting to PC1

	G0/0/14	Access	PVID: 40	Interface for connecting to PC2
	VLANIF40	Layer 3 interface	172.16.20.20/24	Address for interconnecting with FW2
	VLANIF2000	Layer 3 interface	22.22.22.2/24	On the same network segment as VLANIF 2000 on the WAC
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	Interface for connecting to RT1
	G0/0/2			Interface for connecting to RT2
	G0/0/3			Interface for connecting to SW1
RT1	GE0/0/1.2	Layer 3 sub-interface	4.4.4.2/30 Termination VLAN 2	Interface for connecting to SW1
	GE0/0/2	Layer 3 interface	10.1.1.1/30	Interface for connecting to RT2
	GE0/0/3	Layer 3 interface	10.2.1.1/30	Interface for connecting to FW2
	GE0/0/4	Layer 3 interface	10.3.1.1/30	Interface for connecting to FW1
RT2	GE0/0/1.40	Layer 3 sub-interface	3.3.3.2/30	Interface for connecting to SW1
	GE0/0/2	Layer 3 interface	10.1.1.2/30	Interface for connecting to RT1
	GE0/0/3	Layer 3 interface	10.5.1.1/30	Interface for connecting to FW1
	GE0/0/4	Layer 3 interface	10.6.1.1/30	Interface for connecting to FW2

FW1	GE0/0/1	Layer 3 interface	10.5.1.2/30	Interface for connecting to R2
	GE0/0/2	Layer 3 interface	10.3.1.2/30	Interface for connecting to R1
	GE0/0/3	Layer 3 aggregation interface Eth-Trunk0	10.10.10.1/24	Interface for connecting to FW2
	GE0/0/4			
	GE0/0/5	Layer 3 interface	172.16.30.2/24 Virtual IP address of VRRP group 2 (master): 172.16.30.1/24	Interface for connecting to SW2
	GE0/0/6	Layer 3 interface	172.16.20.2/24 Virtual IP address of VRRP group 1 (backup): 172.16.30.1/24	Interface for connecting to SW3
FW2	GE0/0/1	Layer 3 interface	10.2.1.2/30	Interface for connecting to Mirror-SW
	GE0/0/2	Layer 3 interface	10.6.1.2/30	Interface for connecting to R1
	GE0/0/3	Layer 3 aggregation interface Eth-Trunk0	10.10.10.2/24	Interface for connecting to FW1
	GE0/0/4			Interface for connecting to FW1
	GE0/0/5	Layer 3 interface	172.16.20.3/24 Virtual IP address of VRRP group 1 (backup): 172.16.20.1/24	Interface for connecting to SW3
	GE0/0/6	Layer 3 interface	172.16.30.3/24 Virtual IP address of VRRP group 2 (backup):	Interface for connecting to SW2

			172.16.30.1/24	
FW3	GE0/0/1	Layer 3 interface	100.1.1.8/24	On the same network segment as VLANIF 1 on SW1
	GE0/0/6	Layer 3 interface	172.16.40.1/24	PC4 gateway
	GE0/0/7	Layer 3 interface	172.16.50.1/24	PC5 gateway
WAC	GE0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10, 40, 2000, 4000	Interface for connecting to SW3
	VLANIF2000	Layer 3 interface	22.22.22.1/30	On the same network segment as VLANIF 2000 on SW3
	VLANIF4000	Layer 3 interface	10.20.1.1/24	AP management gateway
	VLANIF4001	Layer 3 interface	10.10.1.1/24	Service gateway
PC1	Ethernet0	NIC	172.16.20.100/24 Gateway: 172.16.20.1/24	Terminal
PC2	Ethernet0	NIC	172.16.20.101/24 Gateway: 172.16.20.1/24	Terminal
PC3	Ethernet0	NIC	Automatically obtaining an IP address	Wireless terminal
PC4	Ethernet0	NIC	172.16.40.10/24 Gateway: 172.16.40.1/24	Terminal
PC5	Ethernet0	NIC	172.16.50.10/24 Gateway: 172.16.50.1/24	Terminal
Legal PC	Ethernet0	NIC	20.20.1.10/24 Gateway: 20.20.1.1/24	Terminal

AD server	Ethernet0	NIC	172.16.30.100/24 Gateway: 172.16.30.1/24	Terminal
FTP server	Ethernet0	NIC	172.16.30.101/24 Gateway: 172.16.30.1/24	Terminal
WWW server	Ethernet0	NIC	172.16.30.102/24 Gateway: 172.16.30.1/24	Terminal
Mail server	Ethernet0	NIC	172.16.30.103/24 Gateway: 172.16.30.1/24	Terminal
iMaster NCE-Campus	GE0/0/0	NIC	192.168.10.103/24	Terminal

15.2 Lab Configuration

15.2.1 Configuration Roadmap

1. Complete the basic configuration of device IP addresses.
2. Configure VRRP on FW1 and FW2 with FW1 being the VRRP master device and FW2 being the VRRP backup device.
3. Configure OSPF between FW1/FW2 and RT1/RT2.
4. Configure hot standby in active/standby mode on FW1 and FW2 with FW1 being the active device.
5. Configure NAT on RT1 and RT2 to enable the intranet users to access the Internet and the Internet users to access intranet servers through the public IP address of RT1.
6. Configure virtual systems on FW3 to isolate PC4 services from PC5 services and allow PC5 to access the Internet and PC4 to communicate only with hosts in the HQ zone.
7. Establish an IPsec VPN tunnel between FW1, FW2, and FW3 to secure communication between PC4 and the servers in the HQ zone.
8. Configure SSL VPN in network extension mode on FW1 to allow the legal PC on the Internet to access intranet servers.
9. Configure URL filtering on FW1 and FW2 to prevent enterprise employees from accessing the game portal website www.example.com.
10. Configure the WLAN function for the HQ zone: Enable the AP to go online and broadcast the **Portal-AD** signal; configure tunnel forwarding and AD+Portal authentication for wireless terminals.

15.2.2 Configuration Procedure

Step 1 Complete basic device configurations.

Set basic network parameters according to the table in 15.1.4 Lab Planning.

Step 2 Configure VRRP on firewalls.

Configure VRRP group 1 on the downstream service interface GE0/0/6 of FW1 and set the status of the VRRP group to active. Configure VRRP group 1 on the downstream service interface GE0/0/5 of FW2 and set the status of the VRRP group to standby.

```
[FW1] interface GigabitEthernet 0/0/6
[FW1-GigabitEthernet0/0/6] vrrp vrid 1 virtual-ip 172.16.20.1 active
[FW1-GigabitEthernet0/0/6] quit
```

```
[FW2] interface GigabitEthernet 0/0/5
[FW2-GigabitEthernet0/0/5] vrrp vrid 1 virtual-ip 172.16.20.1 standby
[FW2-GigabitEthernet0/0/5] quit
```

Configure VRRP group 2 on the downstream service interface GE0/0/5 of FW1 and set the status of the VRRP group to active. Configure VRRP group 2 on the downstream service interface GE0/0/6 of FW2 and set the status of the VRRP group to standby.

```
[FW1] interface GigabitEthernet 0/0/5
[FW1-GigabitEthernet0/0/5] vrrp vrid 2 virtual-ip 172.16.30.1 active
[FW1-GigabitEthernet0/0/5] quit
```

```
[FW2] interface GigabitEthernet 0/0/6
[FW2-GigabitEthernet0/0/6] vrrp vrid 2 virtual-ip 172.16.30.1 standby
[FW2-GigabitEthernet0/0/6] quit
```

Step 3 Configure OSPF.

Configure OSPF on FW1 and enable OSPF on the interconnection interface, gateway interface for connecting to PC1, and gateway interface for connecting to the servers.

```
[FW1] ospf 1
[FW1-ospf-1] area 0
[FW1-ospf-1-area-0.0.0.0] quit
[FW1-ospf-1] quit
[FW1] interface GigabitEthernet0/0/1
[FW1-GigabitEthernet0/0/1] ospf enable 1 area 0
[FW1] interface GigabitEthernet0/0/2
[FW1-GigabitEthernet0/0/2] ospf enable 1 area 0
[FW1-GigabitEthernet0/0/2] quit
[FW1] interface GigabitEthernet0/0/5
[FW1-GigabitEthernet0/0/5] ospf enable 1 area 0
```

```
[FW1-GigabitEthernet0/0/5] quit  
[FW1] interface GigabitEthernet0/0/6  
[FW1-GigabitEthernet0/0/6] ospf enable 1 area 0  
[FW1-GigabitEthernet0/0/6] quit
```

Change the OSPF cost value of GigabitEthernet0/0/1 on FW1 to 10 to prepare for the IPsec VPN lab.

```
[FW1] interface GigabitEthernet0/0/1  
[FW1-GigabitEthernet0/0/1] ospf cost 10
```

Configure OSPF on FW1 and advertise the network segment routes of servers to OSPF.

```
[FW1] ospf 1  
[FW1-ospf-1] area 0  
[FW1-ospf-1-area-0.0.0.0] network 172.16.30.0 0.0.0.255  
[FW2-ospf-1-area-0.0.0.0] network 172.16.20.0 0.0.0.255  
[FW1-ospf-1-area-0.0.0.0] quit
```

To prevent the security policy of the firewall from affecting OSPF packets, disable the function of controlling protocol packets based on the security policy on FW1.

```
[FW1] undo firewall packet-filter basic-protocol enable
```

Configure OSPF on FW2 and enable OSPF on the interconnection interface, gateway interface for connecting to PC1, and gateway interface for connecting to the servers.

```
[FW2] ospf 1  
[FW2-ospf-1] area 0  
[FW2-ospf-1-area-0.0.0.0] quit  
[FW2-ospf-1] quit  
[FW2] interface GigabitEthernet0/0/1  
[FW2-GigabitEthernet0/0/1] ospf enable 1 area 0  
[FW2] interface GigabitEthernet0/0/2  
[FW2-GigabitEthernet0/0/2] ospf enable 1 area 0  
[FW2-GigabitEthernet0/0/2] quit  
[FW2] interface GigabitEthernet0/0/5  
[FW2-GigabitEthernet0/0/5] ospf enable 1 area 0  
[FW2-GigabitEthernet0/0/5] quit  
[FW2] interface GigabitEthernet0/0/6  
[FW2-GigabitEthernet0/0/6] ospf enable 1 area 0  
[FW2-GigabitEthernet0/0/6] quit
```

Configure OSPF on FW2 and advertise the network segment routes of PC1 to OSPF.

```
[FW2] ospf 1  
[FW2-ospf-1] area 0  
[FW1-ospf-1-area-0.0.0.0] network 172.16.30.0 0.0.0.255  
[FW2-ospf-1-area-0.0.0.0] network 172.16.20.0 0.0.0.255  
[FW1-ospf-1-area-0.0.0.0] quit
```

To prevent the security policy of the firewall from affecting OSPF packets, disable the function of controlling protocol packets based on the security policy on FW2.

```
[FW2] undo firewall packet-filter basic-protocol enable
```

Configure OSPF on RT1, and enable OSPF on the interconnection interface.

```
[RT1] ospf 1
[RT1-ospf-1] area 0
[RT1-ospf-1-area-0.0.0.0] quit
[RT1-ospf-1] quit
[RT1] interface GigabitEthernet0/0/2
[RT1-GigabitEthernet0/0/2] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/2] quit
[RT1] interface GigabitEthernet0/0/3
[RT1-GigabitEthernet0/0/3] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/3] quit
[RT1] interface GigabitEthernet0/0/4
[RT1-GigabitEthernet0/0/4] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/4] quit
```

Configure OSPF on RT2, and enable OSPF on the interconnection interface.

```
[RT2] ospf 1
[RT2-ospf-1] area 0
[RT2-ospf-1-area-0.0.0.0] quit
[RT2-ospf-1] quit
[RT2] interface GigabitEthernet0/0/2
[RT2-GigabitEthernet0/0/2] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/2] quit
[RT2] interface GigabitEthernet0/0/3
[RT2-GigabitEthernet0/0/3] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/3] quit
[RT2] interface GigabitEthernet0/0/4
[RT2-GigabitEthernet0/0/4] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/4] quit
```

On RT1, add a default route to the Internet.

```
[RT1] ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
```

On RT2, add a default route to the Internet.

```
[RT1] ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
```

Import external default routes to OSPF on RT1.

```
[RT1] ospf 1
[RT1-ospf-1] import-route static
[RT1-ospf-1] default-route-advertise always
[RT1-ospf-1] quit
```

Import external default routes to OSPF on RT2.

```
[RT2] ospf 1  
[RT2-ospf-1] import-route static  
[RT2-ospf-1] default-route-advertise always  
[RT2-ospf-1] quit
```

Step 4 Configure firewall hot standby.

Configure a VGMP group on firewalls to monitor the uplink interfaces, add the downlink interfaces to a VRRP group, and use an Eth-Trunk interface as the heartbeat interface.

Add GigabitEthernet0/0/3 and GigabitEthernet0/0/4 to Eth-Trunk 0 on FW1.

```
[FW1] interface Eth-Trunk 0  
[FW1-Eth-Trunk0] quit  
[FW1] interface GigabitEthernet 0/0/3  
[FW1-GigabitEthernet0/0/3] eth-trunk 0  
[FW1-GigabitEthernet0/0/3] quit  
[FW1] interface GigabitEthernet 0/0/4  
[FW1-GigabitEthernet0/0/4] eth-trunk 0  
[FW1-GigabitEthernet0/0/4] quit
```

Add GigabitEthernet0/0/3 and GigabitEthernet0/0/4 to Eth-Trunk 0 on FW2.

```
[FW2] interface Eth-Trunk 0  
[FW2-Eth-Trunk0] quit  
[FW2] interface GigabitEthernet 0/0/3  
[FW2-GigabitEthernet0/0/3] eth-trunk 0  
[FW2-GigabitEthernet0/0/3] quit  
[FW2] interface GigabitEthernet 0/0/4  
[FW2-GigabitEthernet0/0/4] eth-trunk 0  
[FW2-GigabitEthernet0/0/4] quit
```

Configure a VGMP group on the firewalls to monitor their uplink interfaces.

```
[FW1] hrp track interface GigabitEthernet 0/0/2
```

```
[FW2] hrp track interface GigabitEthernet 0/0/2
```

Configure the function of adjusting the OSPF cost based on VGMP status on the firewalls.

```
[FW1] hrp adjust ospf-cost enable
```

```
[FW2] hrp adjust ospf-cost enable
```

In load sharing networking, configure quick session backup on the firewalls in case of inconsistent paths for forward and return packets.

```
[FW1] hrp mirror session enable
```

```
[FW2] hrp mirror session enable
```

Specify the heartbeat interface and enable hot standby on the firewalls.

```
[FW1] hrp interface Eth-Trunk0 remote 10.10.10.2  
[FW1] hrp enable
```

```
[FW2] hrp interface Eth-Trunk0 remote 10.10.10.1  
[FW2] hrp enable
```

Step 5 Configure NAT.

The scenarios where NAT is required are as follows:

1. Source NAT is required for the server network segment, PC1 network segment, PC2 network segment, and PC3's WLAN network segment in the HQ zone to access the Internet.
2. Destination NAT is required for the Internet users to access the WWW server in the HQ zone.
3. Destination NAT is required for forwarding IPsec VPN traffic to the firewall (NAT traversal) when IPsec VPN is configured for encrypted communication between the HQ zone and branch zone and the firewall is deployed on the intranet of the enterprise.

Configure source NAT on RT1 and RT2.

```
[RT1] acl number 3500  
[RT1-acl-adv-3500] rule 5 permit ip source 172.16.20.0 0.0.0.255  
[RT1-acl-adv-3500] rule 10 permit ip source 172.16.30.0 0.0.0.255  
[RT1-acl-adv-3500] quit  
[RT1] interface GigabitEthernet0/0/1.2  
[RT1-GigabitEthernet0/0/1.2] nat outbound 3500  
[RT1-GigabitEthernet0/0/1.2] quit
```

```
[RT2-acl-adv-3500] acl number 3500  
[RT2-acl-adv-3500] rule 5 permit ip source 172.16.20.0 0.0.0.255  
[RT2-acl-adv-3500] rule 10 permit ip source 172.16.30.0 0.0.0.255  
[RT2-acl-adv-3500] quit  
[RT2] interface g0/0/1.40  
[RT2-GigabitEthernet0/0/1.40] nat outbound 3500  
[RT2-GigabitEthernet0/0/1.40] quit
```

Configure destination NAT on RT1.

```
[RT1] interface GigabitEthernet0/0/1.2
[RT1-GigabitEthernet0/0/1.2] nat server protocol tcp global interface GigabitEthernet 0/0/1.2 8080
inside 172.16.30.102 www
[RT1-GigabitEthernet0/0/1.2] quit
```

Configure destination NAT on RT2.

```
[RT2] interface GigabitEthernet 0/0/1.40
[RT2-GigabitEthernet0/0/1.40] nat server protocol tcp global interface GigabitEthernet 0/0/1.40 8080
inside 172.16.30.102 www
[RT2-GigabitEthernet0/0/1.40] quit
```

Configure a security policy on the firewalls in hot standby mode to allow interworking between specified services.

```
HRP_M[FW1] security-policy
HRP_M[FW1-policy-security] rule name trust-untrust
HRP_M[FW1-policy-security-rule-trust-untrust] source-zone trust
HRP_M[FW1-policy-security-rule-trust-untrust] destination-zone untrust
HRP_M[FW1-policy-security-rule-trust-untrust] source-address 172.16.20.0 mask 255.255.255.0
HRP_M[FW1-policy-security-rule-trust-untrust] destination-address 4.4.4.0 mask 255.255.255.0
HRP_M[FW1-policy-security-rule-trust-untrust] action permit
HRP_M[FW1-policy-security-rule-trust-untrust] rule name untrust-trust
HRP_M[FW1-policy-security-rule-untrust-trust] source-zone untrust
HRP_M[FW1-policy-security-rule-untrust-trust] destination-zone trust
HRP_M[FW1-policy-security-rule-untrust-trust] source-address 20.20.1.0 mask 255.255.255.0
HRP_M[FW1-policy-security-rule-untrust-trust] destination-address 172.16.30.0 mask 255.255.255.0
HRP_M[FW1-policy-security-rule-untrust-trust] action permit
HRP_M[FW1-policy-security-rule-untrust-trust] quit
HRP_M[FW1-policy-security] quit
```

Step 6 Configure virtual systems.

On FW3, enable the virtual system function, configure a resource class, create virtual systems vsysa and vsysb, and allocate resources to them. Configure vsysa and vsysb. PC4 belongs to vsysa, and PC5 belongs to vsysb. Use the virtual systems to isolate PC4 services from PC5 services and allow PC5 to access the Internet and PC4 to communicate only with the servers in the HQ zone.

Enable the virtual system function.

```
<FW3> system-view
[FW3] vsys enable
```

Configure a resource class.

```
[FW3] resource-class r1
[FW3-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[FW3-resource-class-r1] resource-item-limit policy reserved-number 300
[FW3-resource-class-r1] resource-item-limit bandwidth 20 entire
[FW3-resource-class-r1] quit
```

Create virtual system vsysa and allocate resources to it.

```
[FW3] vsys name vsysa  
[FW3-vsys-vsya] assign resource-class r1  
[FW3-vsys-vsya] assign interface GigabitEthernet 0/0/6  
[FW3-vsys-vsya] quit
```

Create virtual system vsysb and allocate resources to it.

```
[FW3] vsys name vsysb  
[FW3-vsys-vsystb] assign resource-class r1  
[FW3-vsys-vsystb] assign interface GigabitEthernet 0/0/7  
[FW3-vsys-vsystb] quit
```

Configure interfaces for the public system and add them to security zones.

```
[FW3] interface GigabitEthernet 0/0/1  
[FW3-GigabitEthernet0/0/1] ip address 100.1.1.8 24  
[FW3-GigabitEthernet0/0/1] quit  
[FW3] interface Virtual-if 0  
[FW3-Virtual-if0] ip address 172.16.0.1 24  
[FW3-Virtual-if0] quit  
[FW3] firewall zone trust  
[FW3-zone-trust] add interface Virtual-if 0  
[FW3-zone-trust] quit  
[FW3] firewall zone untrust  
[FW3-zone-untrust] add interface GigabitEthernet 0/0/1  
[FW3-zone-untrust] quit
```

Configure a route from the public system to the Internet to divert traffic from PC5 attached to vsysb to the Internet. 100.1.1.1 is the next-hop address of the route from the public system to the Internet.

```
[FW3] ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
```

Configure a security policy in the public system to permit traffic from PC5 attached to vsysb to the Internet.

```
[FW3] security-policy  
[FW3-policy-security] rule name PC5-trust-to-untrust  
[FW3-policy-security-rule-PC5-trust-to-untrust] source-zone trust  
[FW3-policy-security-rule-PC5-trust-to-untrust] destination-zone untrust  
[FW3-policy-security-rule-PC5-trust-to-untrust] source-address 172.16.50.0 mask 255.255.255.0  
[FW3-policy-security-rule-PC5-trust-to-untrust] action permit  
[FW3-policy-security-rule-PC5-trust-to-untrust] quit
```

Configure a source NAT policy for the public system to translate the source IP addresses of the packets from PC5 to the Internet into the IP address of the public interface GE0/0/1 in the public system.

```
[FW3] nat-policy  
[FW3-policy-nat] rule name nat1  
[FW3-policy-nat-rule-nat1] source-zone trust  
[FW3-policy-nat-rule-nat1] egress-interface GigabitEthernet 0/0/1
```

```
[FW3-policy-nat-rule-nat1] source-address 172.16.50.0 24
[FW3-policy-nat-rule-nat1] action source-nat easy-ip
[FW3-policy-nat-rule-nat1] quit
[FW3-policy-nat] quit
```

Configure interfaces for vsysa, add them to security zones, and configure routes and security policies for vsysa.

```
# Switch from the user view of the public system to the system view of vsysa.
```

```
[FW3] switch vsys vsysa
<FW-vsysa> system-view
```

```
# Configure interfaces for vsysa and add them to security zones.
```

```
[FW3-vsysa] interface GigabitEthernet0/0/6
[FW3-vsysa-GigabitEthernet0/0/6] ip address 172.16.40.1 255.255.255.0
[FW3-vsysa-GigabitEthernet0/0/6] quit
[FW3-vsysa] interface Virtual-if 1
[FW3-vsysa-Virtual-if1] ip address 172.16.1.1 255.255.255.0
[FW3-vsysa] firewall zone trust
[FW3-vsysa-zone-trust] add interface GigabitEthernet0/0/6
[FW3-vsysa-zone-trust] quit
[FW3-vsysa] firewall zone untrust
[FW3-vsysa-zone-untrust] add interface Virtual-if1
[FW3-vsysa-zone-untrust] quit
```

```
# Configure a route from vsysa to the public system to divert the traffic from PC4 to the public system.
```

```
[FW3-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

```
# Configure a security policy in vsysa to allow hosts on the network segment of PC4 in the R&D department to communicate with the servers in the HQ zone.
```

```
[FW3-vsysa] security-policy
[FW3-vsysa-policy-security] rule name to_HQ_allow
[FW3-vsysa-policy-security-rule-to_HQ_allow] source-zone trust
[FW3-vsysa-policy-security-rule-to_HQ_allow] destination-zone untrust
[FW3-vsysa-policy-security-rule-to_HQ_allow] source-address 172.16.40.0 mask 255.255.255.0
[FW3-vsysa-policy-security-rule-to_HQ_allow] destination-address 172.16.30.0 mask 255.255.255.0
[FW3-vsysa-policy-security-rule-to_HQ_allow] action permit
[FW3-vsysa-policy-security-rule-to_HQ_allow] quit
[FW3-vsysa-policy-security] rule name allow-HQ-in
[FW3-vsysa-policy-security-rule-allow-HQ-in] source-zone untrust
[FW3-vsysa-policy-security-rule-allow-HQ-in] destination-zone trust
[FW3-vsysa-policy-security-rule-allow-HQ-in] source-address 172.16.30.0 mask 255.255.255.0
[FW3-vsysa-policy-security-rule-allow-HQ-in] destination-address 172.16.40.0 mask 255.255.255.0
[FW3-vsysa-policy-security-rule-allow-HQ-in] action permit
[FW3-vsysa-policy-security-rule-allow-HQ-in] quit
```

Configure interfaces for vsysb, add them to security zones, and configure routes and security policies for vsysb.

Switch from the user view of vsysa to the system view of vsysb.

```
[FW3-vsysa] quit  
<FW-vsysa> quit  
[FW3] switch vsys vsysb  
<FW-vsysb> system-view
```

Configure interfaces for vsysb and add them to security zones.

```
[FW3-vsysb] interface GigabitEthernet0/0/7  
[FW3-vsysb-GigabitEthernet0/0/7] ip address 172.16.50.1 255.255.255.0  
[FW3-vsysb-GigabitEthernet0/0/7] quit  
[FW3-vsysb] interface Virtual-if 2  
[FW3-vsysb-Virtual-if2] ip address 172.16.2.1 255.255.255.0  
[FW3-vsysb-Virtual-if2] quit  
[FW3-vsysb] firewall zone trust  
[FW3-vsysb-zone-trust] add interface GigabitEthernet0/0/7  
[FW3-vsysb-zone-trust] quit  
[FW3-vsysb] firewall zone untrust  
[FW3-vsysb-zone-untrust] add interface Virtual-if2  
[FW3-vsysb-zone-untrust] quit
```

Configure a route from vsysb to the public system to divert the traffic from hosts in the marketing department accessing the Internet to the public system.

```
[FW3-vsysb] ip route-static 0.0.0.0 0.0.0.0 public
```

Configure a security policy in vsysb to allow all hosts in the marketing department to access the Internet.

```
[FW3-vsysb] security-policy  
[FW3-vsysb-policy-security] rule name to_internet_allow  
[FW3-vsysb-policy-security-rule-to_internet_allow] source-zone trust  
[FW3-vsysb-policy-security-rule-to_internet_allow] destination-zone untrust  
[FW3-vsysb-policy-security-rule-to_internet_allow] action permit  
[FW3-vsysb-policy-security-rule-to_internet_allow] quit
```

Step 7 Configure IPsec VPN.

Establish an IPsec VPN tunnel between FW1 and FW3 to secure communication between PC4 and the servers in the HQ zone.

Configure an IPsec proposal on FW3. You do not need to set default parameters.

```
[FW3] ipsec proposal 1  
[FW3-ipsec-proposal-1] esp authentication-algorithm sha2-256  
[FW3-ipsec-proposal-1] esp encryption-algorithm aes-256  
[FW3-ipsec-proposal-1] quit
```

Configure an IKE proposal on FW3.

```
[FW3] ike proposal 2  
[FW3-ike-proposal-2] encryption-algorithm aes-256
```

```
[FW3-ike-proposal-2] dh group14
[FW3-ike-proposal-2] authentication-algorithm sha2-256
[FW3-ike-proposal-2] authentication-method pre-share
[FW3-ike-proposal-2] integrity-algorithm hmac-sha2-256
[FW3-ike-proposal-2] prf hmac-sha2-256
[FW3-ike-proposal-2] quit
```

Configure the IKE peer on FW3.

```
[FW3] ike peer 1
[FW3-ike-peer-1] pre-shared-key Huawei@123
[FW3-ike-peer-1] ike-proposal 2
[FW3-ike-peer-1] local-id-type ip ip-configurable
[FW3-ike-peer-1] remote-id-type none
[FW3-ike-peer-1] rsa encryption-padding oaep
[FW3-ike-peer-1] rsa signature-padding pss
[FW3-ike-peer-1] local-id-preference certificate enable
[FW3-ike-peer-1] ikev2 authentication sign-hash sha2-256
[FW3-ike-peer-1] quit
```

Create ACL 3004 to match interesting traffic on FW3.

```
[FW3] acl number 3004
[FW3-acl-adv-3004] rule permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
[FW3-acl-adv-3004] quit
```

Configure an IPsec policy template on FW3.

```
[FW3] ipsec policy-template Branch1 1
[FW3-ipsec-policy-templet-Branch1-1] security acl 3004
[FW3-ipsec-policy-templet-Branch1-1] ike-peer 1
[FW3-ipsec-policy-templet-Branch1-1] proposal 1
[FW3-ipsec-policy-templet-Branch1-1] quit
[FW3] ipsec policy 1 10 isakmp template Branch1
```

Apply the IPsec policy to GigabitEthernet0/0/1 on FW3.

```
[FW3] interface GigabitEthernet0/0/1
[FW3-GigabitEthernet0/0/1] ipsec policy 1
[FW3-GigabitEthernet0/0/1] quit
```

On FW3, configure a route to the service network segment of the virtual system.

```
[FW3] ip route-static 172.16.40.0 255.255.255.0 vpn-instance vsysa
```

Create a security policy in vsysa on FW3 to permit traffic between the PC4 network segment and the server network segment in the HQ zone.

```
[FW3] switch vsys vsysa
<FW3-vsysa> system-view
Enter system view, return user view with Ctrl+Z.
[FW3-vsysa] security-policy
```

```
[FW3-vsya-policy-security] rule name to_HQ_allow
[FW3-vsya-policy-security-rule-to_HQ_allow] source-zone local
[FW3-vsya-policy-security-rule-to_HQ_allow] source-zone trust
[FW3-vsya-policy-security-rule-to_HQ_allow] destination-zone untrust
[FW3-vsya-policy-security-rule-to_HQ_allow] source-address 172.16.40.0 mask 255.255.255.0
[FW3-vsya-policy-security-rule-to_HQ_allow] destination-address 172.16.30.0 mask 255.255.255.0
[FW3-vsya-policy-security-rule-to_HQ_allow] action permit
[FW3-vsya-policy-security-rule-to_HQ_allow] rule name allow-HQ-in
[FW3-vsya-policy-security-rule-allow-HQ-in] source-zone untrust
[FW3-vsya-policy-security-rule-allow-HQ-in] destination-zone trust
[FW3-vsya-policy-security-rule-allow-HQ-in] destination-zone local
[FW3-vsya-policy-security-rule-allow-HQ-in] source-address 172.16.30.0 mask 255.255.255.0
[FW3-vsya-policy-security-rule-allow-HQ-in] destination-address 172.16.40.0 mask 255.255.255.0
[FW3-vsya-policy-security-rule-allow-HQ-in] action permit
[FW3-vsya-policy-security-rule-allow-HQ-in] quit
```

Configure security policies on FW3 to allow IPsec VPN tunnel establishment and service interworking.

```
[FW3] security-policy
[FW3-policy-security] rule name untrust-local
[FW3-policy-security-rule-untrust-local] source-zone untrust
[FW3-policy-security-rule-untrust-local] destination-zone local
[FW3-policy-security-rule-untrust-local] destination-address 100.1.1.8 mask 255.255.255.255
[FW3-policy-security-rule-untrust-local] action permit
[FW3-policy-security-rule-untrust-local] quit
[FW3-policy-security] rule name local-untrust
[FW3-policy-security-rule-local-untrust] source-zone local
[FW3-policy-security-rule-local-untrust] destination-zone untrust
[FW3-policy-security-rule-local-untrust] source-address 100.1.1.0 mask 255.255.255.0
[FW3-policy-security-rule-local-untrust] destination-address 4.4.4.0 mask 255.255.255.0
[FW3-policy-security-rule-local-untrust] action permit
[FW3-policy-security-rule-local-untrust] quit
[FW3-policy-security] rule name trust-untrust
[FW3-policy-security-rule-trust-untrust] source-zone trust
[FW3-policy-security-rule-trust-untrust] destination-zone untrust
[FW3-policy-security-rule-trust-untrust] source-address 172.16.40.0 mask 255.255.255.0
[FW3-policy-security-rule-trust-untrust] destination-address 172.16.30.0 mask 255.255.255.0
[FW3-policy-security-rule-trust-untrust] action permit
[FW3-policy-security-rule-trust-untrust] quit
[FW3-policy-security] rule name untrust-trust
[FW3-policy-security-rule-untrust-trust] source-zone untrust
[FW3-policy-security-rule-untrust-trust] destination-zone trust
[FW3-policy-security-rule-untrust-trust] source-address 172.16.30.0 mask 255.255.255.0
[FW3-policy-security-rule-untrust-trust] destination-address 172.16.40.0 mask 255.255.255.0
[FW3-policy-security-rule-untrust-trust] action permit
[FW3-policy-security-rule-untrust-trust] quit
```

Configure NAT Server on RT1 so that FW3 can proactively send an IPsec VPN tunnel establishment request to FW1.

```
[RT1] interface g0/0/1.2
[RT1-GigabitEthernet0/0/1.2] nat server protocol tcp global interface GigabitEthernet 0/0/1.2 4500
inside 10.3.1.2 4500
```

```
[RT1-GigabitEthernet0/0/1.2] nat server protocol tcp global interface GigabitEthernet 0/0/1.2 500  
inside 10.3.1.2 500  
[RT1-GigabitEthernet0/0/1.2] quit
```

Configure an IPsec proposal on FW1. You do not need to set default parameters.

```
HRP_M[FW1] ipsec proposal 1  
HRP_M[FW1-ipsec-proposal-1] esp authentication-algorithm sha2-256  
HRP_M[FW1-ipsec-proposal-1] esp encryption-algorithm aes-256  
HRP_M[FW1-ipsec-proposal-1] quit
```

Configure an IKE proposal on FW1.

```
HRP_M[FW1] ike proposal 2  
HRP_M[FW1-ike-proposal-2] encryption-algorithm aes-256  
HRP_M[FW1-ike-proposal-2] dh group14  
HRP_M[FW1-ike-proposal-2] authentication-algorithm sha2-256  
HRP_M[FW1-ike-proposal-2] authentication-method pre-share  
HRP_M[FW1-ike-proposal-2] integrity-algorithm hmac-sha2-256  
HRP_M[FW1-ike-proposal-2] prf hmac-sha2-256  
HRP_M[FW1-ike-proposal-2] quit
```

Configure an IKE peer on FW1 and bind it to vsysa.

```
HRP_M[FW1] ike peer 1  
HRP_M[FW1-ike-peer-1] pre-shared-key Huawei@123  
HRP_M[FW1-ike-peer-1] ike-proposal 2  
HRP_M[FW1-ike-peer-1] remote-id-type none  
HRP_M[FW1-ike-peer-1] remote-address 100.1.1.8  
HRP_M[FW1-ike-peer-1] rsa encryption-padding oaep  
HRP_M[FW1-ike-peer-1] rsa signature-padding pss  
HRP_M[FW1-ike-peer-1] local-id-preference certificate enable  
HRP_M[FW1-ike-peer-1] ikev2 authentication sign-hash sha2-256  
HRP_M[FW1-ike-peer-1] quit
```

Create ACL 3003 on FW1.

```
HRP_M[FW1] acl number 3003  
HRP_M[FW1-acl-adv-3003] rule 15 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0  
0.0.0.255  
HRP_M[FW1-acl-adv-3003] quit
```

Configure an IPsec policy on FW1.

```
HRP_M[FW1] ipsec policy 1 1 isakmp  
HRP_M[FW1-ipsec-policy-isakmp-1-1] security acl 3003  
HRP_M[FW1-ipsec-policy-isakmp-1-1] ike-peer 1  
HRP_M[FW1-ipsec-policy-isakmp-1-1] proposal 1  
HRP_M[FW1-ipsec-policy-isakmp-1-1] quit
```

Apply the IPsec policy to GigabitEthernet 0/0/2 on FW1.

```
HRP_M[FW1] interface GigabitEthernet 0/0/2
```

```
HRP_M[FW1-GigabitEthernet0/0/2] ipsec policy 1  
HRP_M[FW1-GigabitEthernet0/0/2] quit
```

Configure security policies on FW1 to allow IPsec VPN tunnel establishment and service interworking.

```
HRP_M[FW1] security-policy  
HRP_M[FW1-policy-security] rule name untrust-local  
HRP_M[FW1-policy-security-rule-untrust-local] source-zone untrust  
HRP_M[FW1-policy-security-rule-untrust-local] destination-zone local  
HRP_M[FW1-policy-security-rule-untrust-local] destination-address 10.3.1.2 mask 255.255.255.255  
HRP_M[FW1-policy-security-rule-untrust-local] destination-address 172.16.30.0 mask 255.255.255.0  
HRP_M[FW1-policy-security-rule-untrust-local] action permit  
HRP_M[FW1-policy-security-rule-untrust-local] quit  
HRP_M[FW1-policy-security] rule name local-untrust  
HRP_M[FW1-policy-security-rule-local-untrust] source-zone local  
HRP_M[FW1-policy-security-rule-local-untrust] destination-zone untrust  
HRP_M[FW1-policy-security-rule-local-untrust] source-address 172.16.30.0 mask 255.255.255.0  
HRP_M[FW1-policy-security-rule-local-untrust] destination-address 100.1.1.8 mask 255.255.255.255  
HRP_M[FW1-policy-security-rule-local-untrust] action permit  
HRP_M[FW1-policy-security-rule-local-untrust] quit  
HRP_M[FW1-policy-security] rule name untrust-trust  
HRP_M[FW1-policy-security-rule-untrust-trust] source-zone untrust  
HRP_M[FW1-policy-security-rule-untrust-trust] destination-zone trust  
HRP_M[FW1-policy-security-rule-untrust-trust] source-address 172.16.40.0 mask 255.255.255.0  
HRP_M[FW1-policy-security-rule-untrust-trust] destination-address 172.16.30.0 mask 255.255.255.0  
HRP_M[FW1-policy-security-rule-untrust-trust] action permit  
HRP_M[FW1-policy-security-rule-untrust-trust] quit  
HRP_M[FW1-policy-security] rule name trust-untrust  
HRP_M[FW1-policy-security-rule-trust-untrust] source-zone trust  
HRP_M[FW1-policy-security-rule-trust-untrust] destination-zone untrust  
HRP_M[FW1-policy-security-rule-trust-untrust] source-address 172.16.30.0 mask 255.255.255.0  
HRP_M[FW1-policy-security-rule-trust-untrust] destination-address 172.16.40.0 mask 255.255.255.0  
HRP_M[FW1-policy-security-rule-trust-untrust] action permit  
HRP_M[FW1-policy-security-rule-trust-untrust] quit
```

Step 8 Configure SSL VPN.

Configure SSL VPN in network extension mode on FW1 to allow the legal PC on the Internet to access intranet servers.

Configure local authentication for users.

```
HRP_M[FW1] aaa  
HRP_M[FW1-aaa] authentication-scheme default  
HRP_M[FW1-aaa-authen-default] authorization-scheme default  
HRP_M[FW1-aaa-author-default] accounting-scheme default  
HRP_M[FW1-aaa-accounting-default] domain default  
HRP_M[FW1-aaa-domain-default] service-type internetaccess ssl-vpn l2tp ike dot1x  
HRP_M[FW1-aaa-domain-default] internet-access mode password  
HRP_M[FW1-aaa-domain-default] reference user current-domain  
HRP_M[FW1-aaa-domain-default] quit
```

Create a virtual gateway and configure it to use local authentication in the default domain.

```
HRP_M[FW1] v-gateway gateway interface GigabitEthernet0/0/2 private  
HRP_M[FW1] v-gateway gateway authentication-domain default
```

Set virtual gateway parameters to allocate addresses to terminals, set the routing mode to manual routing, and deliver the network segment routes of the servers in the HQ zone.

```
HRP_M[FW1] v-gateway gateway  
HRP_M[FW1-gateway] basic  
HRP_M[FW1-gateway-basic] ssl version tlsv12  
HRP_M[FW1-gateway-basic] ssl timeout 5  
HRP_M[FW1-gateway-basic] ssl lifecycle 1440  
HRP_M[FW1-gateway-basic] ssl public-key algorithm rsa  
HRP_M[FW1-gateway-basic] ssl ciphersuit custom aes256-sha aes128-sha  
HRP_M[FW1-gateway-basic] service  
HRP_M[FW1-gateway-service] network-extension enable  
HRP_M[FW1-gateway-service] network-extension keep-alive enable  
HRP_M[FW1-gateway-service] network-extension keep-alive interval 120  
HRP_M[FW1-gateway-service] network-extension netpool 11.11.11.10 11.11.11.20 255.255.255.0  
HRP_M[FW1-gateway-service] netpool 11.11.11.10 default  
HRP_M[FW1-gateway-service] network-extension mode manual  
HRP_M[FW1-gateway-service] network-extension manual-route 172.16.30.0 255.255.255.0  
HRP_M[FW1-gateway-service] security  
HRP_M[FW1-gateway-security] policy-default-action permit vt-src-ip  
HRP_M[FW1-gateway-security] certification cert-anonymous cert-field user-filter subject cn group-filter subject cn  
HRP_M[FW1-gateway-security] certification cert-anonymous filter-policy permit-all  
HRP_M[FW1-gateway-security] certification cert-challenge cert-field user-filter subject cn  
HRP_M[FW1-gateway-security] certification user-cert-filter key-usage any  
HRP_M[FW1-gateway-security] undo public-user enable  
HRP_M[FW1-gateway-security] hostchecker  
HRP_M[FW1-gateway-hostchecker] cache-cleaner  
HRP_M[FW1-gateway] vpndb  
HRP_M[FW1-gateway-vpndb] group /default  
HRP_M[FW1-gateway-vpndb-group-/default] role  
HRP_M[FW1-gateway-role] role default  
HRP_M[FW1-gateway-role] role default condition all  
HRP_M[FW1-gateway-role] role default network-extension enable  
HRP_M[FW1-gateway-role] quit
```

Create a user name and a password.

```
HRP_M[FW1] user-manage user user01 domain default  
HRP_M[FW1-localuser-user01] password Huawei@123  
HRP_M[FW1-localuser-user01] parent-group /default  
HRP_M[FW1-localuser-user01] quit
```

Configure a security policy to allow SSL VPN users to access the servers in the HQ zone.

```
HRP_M[FW1] security-policy  
HRP_M[FW1-policy-security] rule name untrust-trust
```

```
HRP_M[FW1-policy-security-rule-untrust-trust] source-zone untrust
HRP_M[FW1-policy-security-rule-untrust-trust] destination-zone trust
HRP_M[FW1-policy-security-rule-untrust-trust] source-address 11.11.11.0 mask 255.255.255.0
HRP_M[FW1-policy-security-rule-untrust-trust] destination-address 172.16.30.0 mask 255.255.255.0
HRP_M[FW1-policy-security-rule-untrust-trust] action permit
HRP_M[FW1-policy-security-rule-untrust-trust] quit
```

Step 9 Configure content security.

Configure URL filtering on FW1 and FW2 to prevent enterprise employees from accessing the game portal website www.example.com. FW1 and FW2 work in hot standby mode. The configuration on FW1 will be synchronized to FW2. Therefore, the configuration only needs to be performed on FW1.

```
# Create URL filtering profile url_profile_01 and add www.example.com to the blacklist.
```

```
HRP_M[FW1] profile type url-filter name url_profile_01
HRP_M[FW1-profile-url-filter-url_profile_01] add blacklist url www.example.com
HRP_M[FW1-profile-url-filter-url_profile_01] quit
```

```
# Configure a security policy and reference the url_profile_01 profile to control URL access.
```

```
HRP_M[FW1] security-policy
HRP_M[FW1-policy-security] rule name trust-untrust-internet
HRP_M[FW1-policy-security-rule-trust-untrust-internet] source-zone trust
HRP_M[FW1-policy-security-rule-trust-untrust-internet] destination-zone untrust
HRP_M[FW1-policy-security-rule-trust-untrust-internet] source-address 172.16.30.0 mask
255.255.255.0
HRP_M[FW1-policy-security-rule-trust-untrust-internet] source-address 172.16.20.0 mask
255.255.255.0
HRP_M[FW1-policy-security-rule-trust-untrust-internet] action permit
HRP_M[FW1-policy-security-rule-trust-untrust-internet] profile url-filter url_profile_01
HRP_M[FW1-policy-security-rule-trust-untrust-internet] quit
```

Step 10 Configure the WLAN function.

Configure the WLAN function for the HQ zone: Enable the AP to go online and broadcast the **Portal-AD** signal. Configure tunnel forwarding and AD+Portal authentication for wireless terminals. This configuration enables PC3 to connect to the Wi-Fi network named **Portal-AD** and access the Internet after authentication.

```
# Configure GigabitEthernet0/0/2 on the WAC.
```

```
[AC] interface GigabitEthernet0/0/2
[AC-GigabitEthernet0/0/2] port link-type trunk
[AC-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[AC-GigabitEthernet0/0/2] port trunk allow-pass vlan 10 40 2000 4000
[AC-GigabitEthernet0/0/2] quit
```

```
# Configure G0/0/3, G0/0/12, and G0/0/1 on SW3.
```

```
[SW3] interface GigabitEthernet0/0/3
[SW3-G0/0/3] port link-type trunk
[SW3-G0/0/3] port trunk allow-pass vlan 10 40 200 4000
```

```
[SW3-G0/0/3] quit
```

```
[SW3] interface GigabitEthernet0/0/12
[SW3-G0/0/12] port link-type trunk
[SW3-G0/0/12] port trunk pvid vlan 4000
[SW3-G0/0/12] port trunk allow-pass vlan 2 to 4094
[SW3-G0/0/12] quit
```

```
[SW3] interface GigabitEthernet0/0/1
[SW3-G0/0/1] port link-type access
[SW3-G0/0/1] port default vlan 40
[SW3-G0/0/1] quit
[SW3] interface GigabitEthernet0/0/2
[SW3-G0/0/2] port link-type access
[SW3-G0/0/2] port default vlan 40
[SW3-G0/0/2] quit
```

Configure G0/0/1, G0/0/2, and G0/0/13 on SW2.

```
[SW2] interface GigabitEthernet 0/0/1
[SW2-G0/0/1] port link-type access
[SW2-G0/0/1] port default vlan 30
[SW2-G0/0/1] quit
[SW2] interface GigabitEthernet 0/0/2
[SW2-G0/0/2] port link-type access
[SW2-G0/0/2] port default vlan 30
[SW2-G0/0/2] quit
[SW2] interface GigabitEthernet 0/0/13
[SW2-G0/0/13] port link-type access
[SW2-G0/0/13] port default vlan 30
[SW2-G0/0/13] quit
```

The WAC needs to provide a management address for the AP and a service address for wireless users. Configure VLAN 4000 as the DHCP server on the management network segment and VLAN 4001 as the DHCP server on the user network segment according to 15.1.4 Lab Planning.

Enable the DHCP function on the WAC.

```
[AC] dhcp enable
```

Create VLANs on the WAC to assign management addresses and STA addresses to the AP.

```
[AC] vlan batch 4000 4001
```

Configure the gateway IP address on the management network segment of the AP and select the global DHCP address pool.

```
[AC] interface vlanif4000
[AC-VLANIF4000] ip address 10.10.1.1 255.255.255.0
[AC-VLANIF4000] dhcp select global
[AC-VLANIF4000] quit
```

Configure the DHCP server on the management network segment of the AP.

```
[AC] ip pool vlan4000
[AC-ip-pool-vlan4000] gateway-list 10.10.1.1
[AC-ip-pool-vlan4000] network 10.10.1.0 mask 255.255.255.0
[AC-ip-pool-vlan4000] option 43 sub-option 3 ascii 10.10.1.1
[AC-ip-pool-vlan4000] quit
```

Configure the gateway IP address on the network segment of wireless services and select the global DHCP address pool.

```
[AC] interface vlanif4001
[AC-VLANIF4001] ip address 10.20.1.1 255.255.255.0
[AC-VLANIF4001] dhcp select global
[AC-VLANIF4001] quit
```

Configure the DHCP server on the network segment of wireless users.

```
[AC] ip pool vlan4001
[AC-ip-pool-vlan4001] gateway-list 10.20.1.1
[AC-ip-pool-vlan4001] network 10.20.1.0 mask 255.255.255.0
[AC-ip-pool-vlan4001] quit
```

Create an AP group to which APs with the same configurations are added.

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
```

Create a regulatory domain profile, configure the country code of the WAC in the profile, and bind the profile to the AP group.

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```

Configure the source interface of the WAC.

```
[AC] capwap source interface vlanif 4000
```

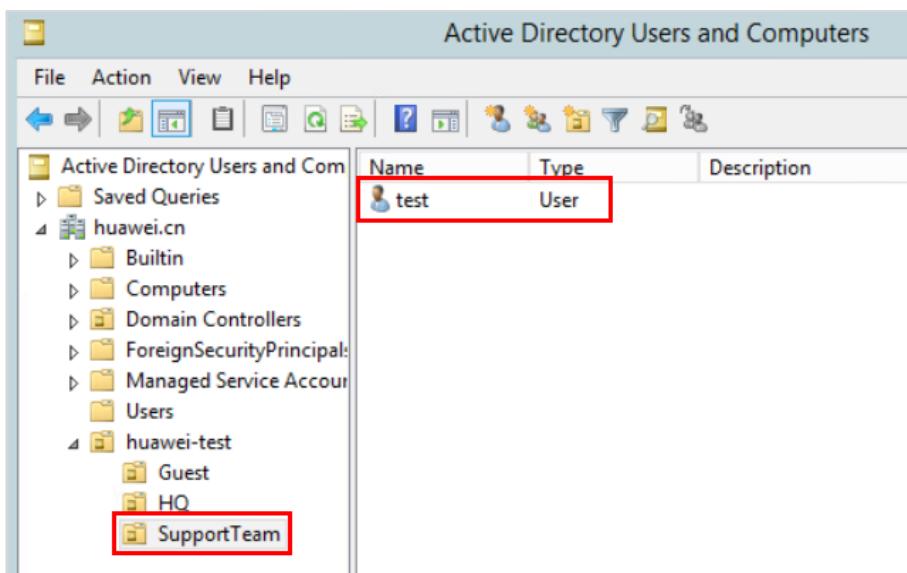
Import the AP offline on the WAC.

```
[AC] wlan
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 1 ap-mac 14ab-0228-5f80
[AC-wlan-ap-1] ap-name a5760
[AC-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power
and antenna gain configurations of the radio, Whether to continue? [Y/N]:y
[AC-wlan-ap-1] quit
```

Run the **display ap all** command to check the AP state. If the **State** field displays **nor**, the AP goes online properly.

```
[AC] display ap all
Total AP information:
nor : normal      [1]
ExtraInfo : Extra information
-----
ID  MAC          Name   Group     IP           Type       State  STA  Uptime ExtraInfo
-----  
1  14ab-0228-5f80  a5760  ap-group1  10.10.1.226 AirEngine5760-51 nor    0   -   -
```

Create a user named **test** in **SupportTeam** on the AD authentication server and set the password to **Huawei@123**.

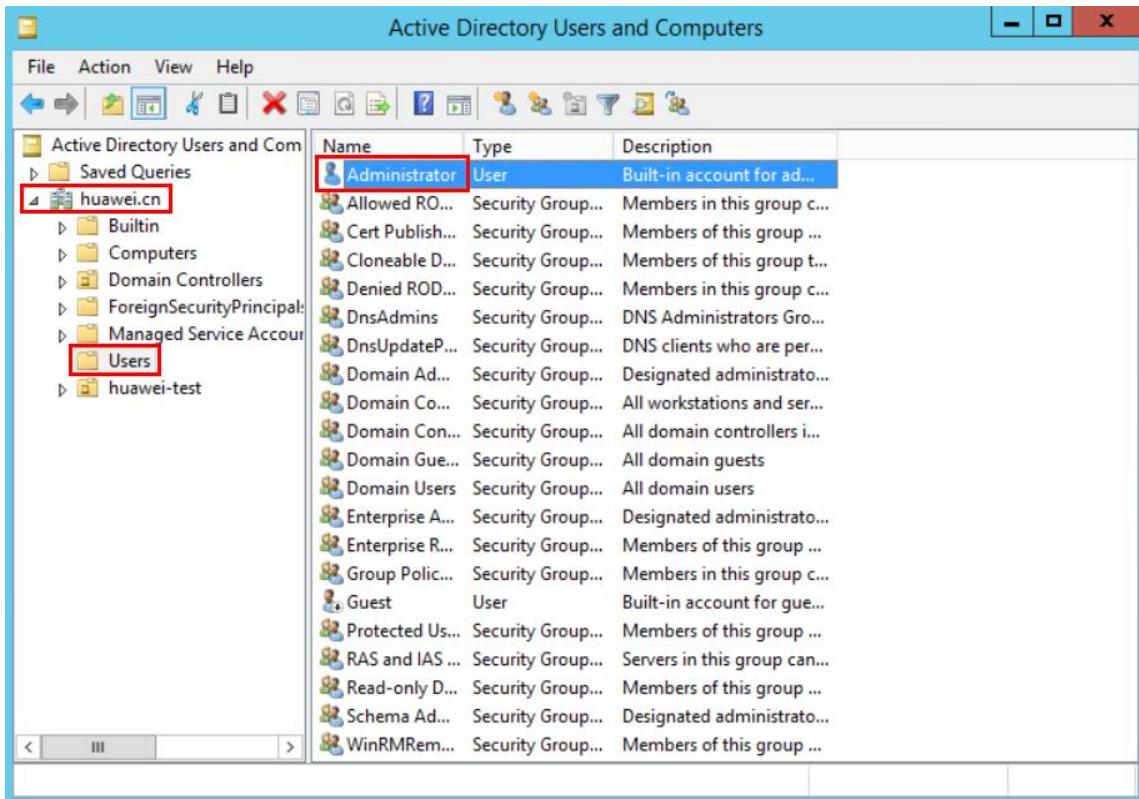


Query the parameters of the AD authentication server.

As shown in the following figure, the domain name is **huawei.cn**.

The administrator user name and password of the AD server are **Administrator** and **Huawei@123**, respectively.

On the Windows server page, the host name displays **WIN-B3JG2458G73.huawei.cn**.



Create an AD server template on the WAC and set the parameters according to those obtained in the previous step.

```
[AC] ad-server template t1
[AC-ad-t1] ad-server authentication 172.16.30.100 88 no-ssl
Warning: The no-ssl configuration is not safe, it is recommended to config ldap-over-ssl type.
Continue?[Y/N]Y
[AC-ad-t1] ad-server authentication base-dn dc=huawei,dc=cn
[AC-ad-t1] ad-server authentication manager cn=Administrator,cn=users Huawei@123
[AC-ad-t1] ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn
[AC-ad-t1] quit
```

Create a Portal access profile named **Portal-AD** and enable the built-in Portal server.

```
[AC] portal-access-profile name Portal-AD
[AC-portal-access-profile-Portal-AD] portal local-server enable
[AC-portal-access-profile-Portal-AD] quit
```

Set the IP address of the built-in Portal server to 10.20.1.1.

```
[AC] portal local-server ip 10.20.1.1
```

Set the port number of the built-in Portal server to 8080.

```
[AC] portal local-server http port 8080
```

Create authentication and authorization schemes named **AD**.

```
[AC] aaa  
[AC-aaa] authentication-scheme Portal-AD  
[AC-aaa-authen-Portal-AD] authentication-mode ad  
[AC-aaa-authen-Portal-AD] quit  
[AC-aaa] authorization-scheme AD  
[AC-aaa-author-AD] authorization-mode ad  
[AC-aaa-author-AD] quit
```

Create an authentication profile named **Portal-AD** and bind the Portal access profile, authentication scheme, authorization scheme, and AD server to the authentication profile.

```
[AC] authentication-profile name Portal-AD  
[AC-authentication-profile-Portal-AD] portal-access-profile Portal-AD  
[AC-authentication-profile-Portal-AD] authentication-scheme Portal-AD  
[AC-authentication-profile-Portal-AD] authorization-scheme AD  
[AC-authentication-profile-Portal-AD] ad-server t1  
[AC-authentication-profile-Portal-AD] quit
```

Create a security profile named **Portal-AD** and configure a security policy.

```
[AC] wlan  
[AC-wlan-view] security-profile name Portal-AD  
[AC-wlan-sec-prof-Portal-AD] security open  
[AC-wlan-sec-prof-Portal-AD] quit
```

Create an SSID profile named **Portal-AD** and set the SSID name to **Portal-AD**.

```
[AC-wlan-view] ssid-profile name Portal-AD  
[AC-wlan-ssid-prof-Portal-AD] ssid Portal-AD  
[AC-wlan-ssid-prof-Portal-AD] quit
```

Create a VAP profile named **Portal-AD**, set the data forwarding mode to tunnel forwarding, set the service VLAN, and bind the security profile, authentication profile, and SSID profile to the VAP profile.

```
[AC-wlan-view] vap-profile name Portal-AD  
[AC-wlan-vap-prof-Portal-AD] forward-mode tunnel  
[AC-wlan-vap-prof-Portal-AD] service-vlan vlan-id 4001  
[AC-wlan-vap-prof-Portal-AD] ssid-profile Portal-AD  
[AC-wlan-vap-prof-Portal-AD] security-profile Portal-AD  
[AC-wlan-vap-prof-Portal-AD] authentication-profile Portal-AD  
[AC-wlan-vap-prof-Portal-AD] quit
```

Bind the VAP profile to the AP group and apply configurations in this VAP profile to radio 0 and radio 1 of the APs in the AP group.

```
[AC-wlan-view] ap-group name ap-group1  
[AC-wlan-ap-group-ap-group1] vap-profile Portal-AD wlan 3 radio 0  
[AC-wlan-ap-group-ap-group1] vap-profile Portal-AD wlan 3 radio 1  
[AC-wlan-ap-group-ap-group1] quit  
[AC-wlan-view] quit
```

Set the local server authentication mode to PAP on the WAC.

```
[AC] portal local-server authentication-method pap
```

Configure routes to implement Layer 3 communication between the WAC and the AD server and between the WAC and the Internet because the gateway of PC3 is deployed on the WAC.

Configure VLANIF 2000 on the WAC and SW3.

```
[AC] vlan 2000
[AC-vlan2000] quit
[AC]interface vlan 2000
[AC-VLANIF2000] ip address 22.22.22.1 255.255.255.252
[AC-VLANIF2000] quit
```

```
[SW3] vlan 2000
[SW3-vlan2000] quit
[SW3] interface vlan 2000
[SW3-VLANIF2000] ip address 22.22.22.2 255.255.255.0
[SW3-VLANIF2000] quit
```

Configure a default route to SW3 on the WAC so that all traffic is diverted to SW3 for routing table searching.

```
[AC] ip route-static 0.0.0.0 0.0.0.0 22.22.22.2
```

Configure an IP address for VLANIF 40 on SW3.

```
[SW3] vlan 40
[SW3-vlan40] quit
[SW3] interface vlan 40
[SW3-VLANIF40] ip address 172.16.20.20 255.255.255.0
[SW3-VLANIF40] quit
```

On SW3, configure a default route to the VRRP virtual gateway 172.16.20.1 of the firewall.

```
[SW3] ip route-static 0.0.0.0 0.0.0.0 172.16.20.1
```

Specify the return route for WAC traffic on FW1.

```
HRP_M[FW1] ip route-static 10.20.1.0 255.255.255.0 172.16.20.20
HRP_M[FW1] ip route-static 22.22.22.0 255.255.255.252 172.16.20.20
```

Import static routes to OSPF on FW1 so that RT1 and RT2 have network segment routes of PC3. When PC3 accesses the Internet, RT1 and RT2 can search for return routes for returned packets.

```
HRP_M[FW1] ospf 1
```

```
HRP_M[FW1-ospf-1] import-route static  
HRP_M[FW1-ospf-1] quit
```

On SW3, specify the return route of PC3.

```
[SW3] ip route-static 10.20.1.0 255.255.255.0 22.22.22.1
```

15.3 Verification

After the configuration is complete, verify the following:

1. FW1 and FW2 form a hot standby group and work in active/standby mode, and FW1 is the active device.
2. PC1 can ping 4.4.4.1 on the Internet.
3. The legal PC on the Internet can access the website of the WWW server through the IP address of RT1.
4. In the virtual system of FW3, PC5 can ping 100.1.1.1 on the Internet.
5. IPsec SAs exist on FW3 and FW1, and PC4 can ping the servers in the HQ zone.
6. The legal PC on the Internet can access the servers in the HQ zone through SSL VPN.
7. PC3 can access the Internet after connecting to the wireless network named **Portal-AD** and completing AD authentication on the Portal page.

Display the hot standby status of the firewalls.

```
HRP_M<FW1> display hrp state  
Role: active, peer: standby  
Running priority: 45000, peer: 45000  
Backup channel usage: 0.00%  
Stable time: 0 days, 2 hours, 34 minutes  
Last state change information: XX HRP core state changed, old_state = abnormal(active), new_state = normal, local_priority = 45000, peer_priority = 45000.
```

```
HRP_M<FW1> display vrrp brief  
Total:2 Master:2 Backup:0 Non-active:0  
VRID State Interface Type Virtual IP  
-----  
1 Master GE0/0/6 Vgmp 172.16.20.1  
2 Master GE0/0/5 Vgmp 172.16.30.1
```

```
HRP_S<FW2> display hrp state  
Role: standby, peer: active  
Running priority: 45000, peer: 45000  
Backup channel usage: 0.00%  
Stable time: 0 days, 2 hours, 35 minutes
```

Last state change information: XX HRP core state changed, old_state = abnormal(standby), new_state = normal, local_priority = 45000, peer_priority = 45000.

HRP_S<FW2> display vrrp brief					
Total:2	Master:0	Backup:2	Non-active:0		
VRID	State	Interface	Type	Virtual IP	
1	Backup	GE0/0/5	Vgmp	172.16.20.1	
2	Backup	GE0/0/6	Vgmp	172.16.30.1	

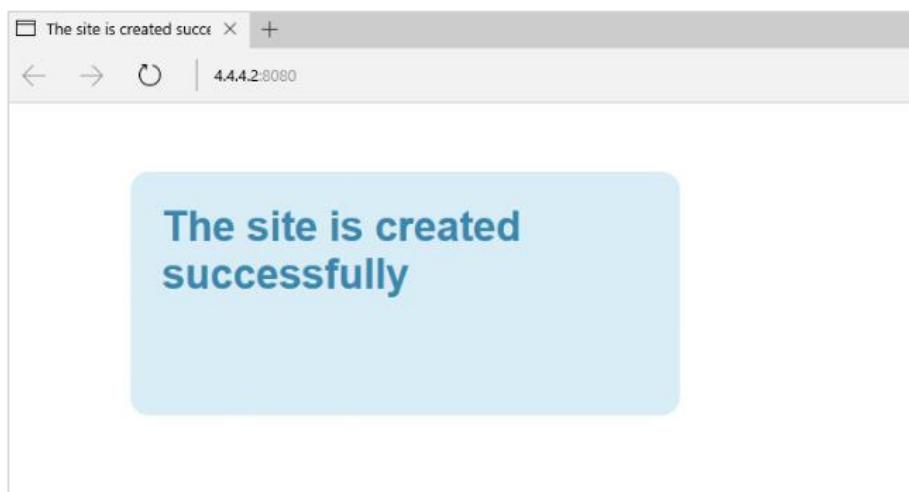
Verify that PC1 can ping 4.4.4.1 on the Internet.

```
C:\Users\Security>ping 4.4.4.1

Pinging 4.4.4.1 with 32 bytes of data:
Reply from 4.4.4.1: bytes=32 time=6ms TTL=250
Reply from 4.4.4.1: bytes=32 time=8ms TTL=250
Reply from 4.4.4.1: bytes=32 time=13ms TTL=250
Reply from 4.4.4.1: bytes=32 time=10ms TTL=250

Ping statistics for 4.4.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 13ms, Average = 9ms
```

Verify that the legal PC on the Internet can access the website of the WWW server through the IP address of RT1.



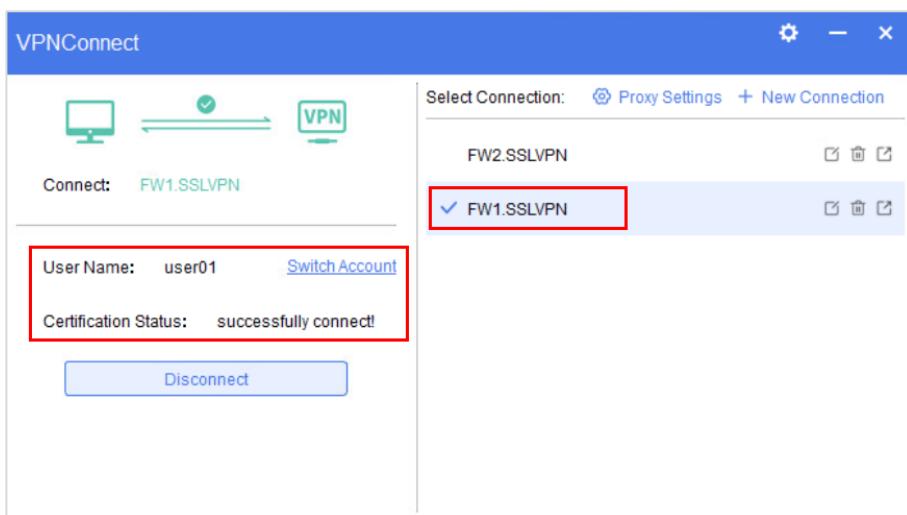
Verify that PC4 can ping the servers in the HQ zone.

```
C:\Windows\system32>ping 172.16.30.100

Pinging 172.16.30.100 with 32 bytes of data:
Reply from 172.16.30.100: bytes=32 time=14ms TTL=125
Reply from 172.16.30.100: bytes=32 time=30ms TTL=125
Reply from 172.16.30.100: bytes=32 time=30ms TTL=125
Reply from 172.16.30.100: bytes=32 time=5ms TTL=125

Ping statistics for 172.16.30.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 30ms, Average = 19ms
```

Verify that the legal PC on the Internet can access the servers in the HQ zone through SSL VPN.

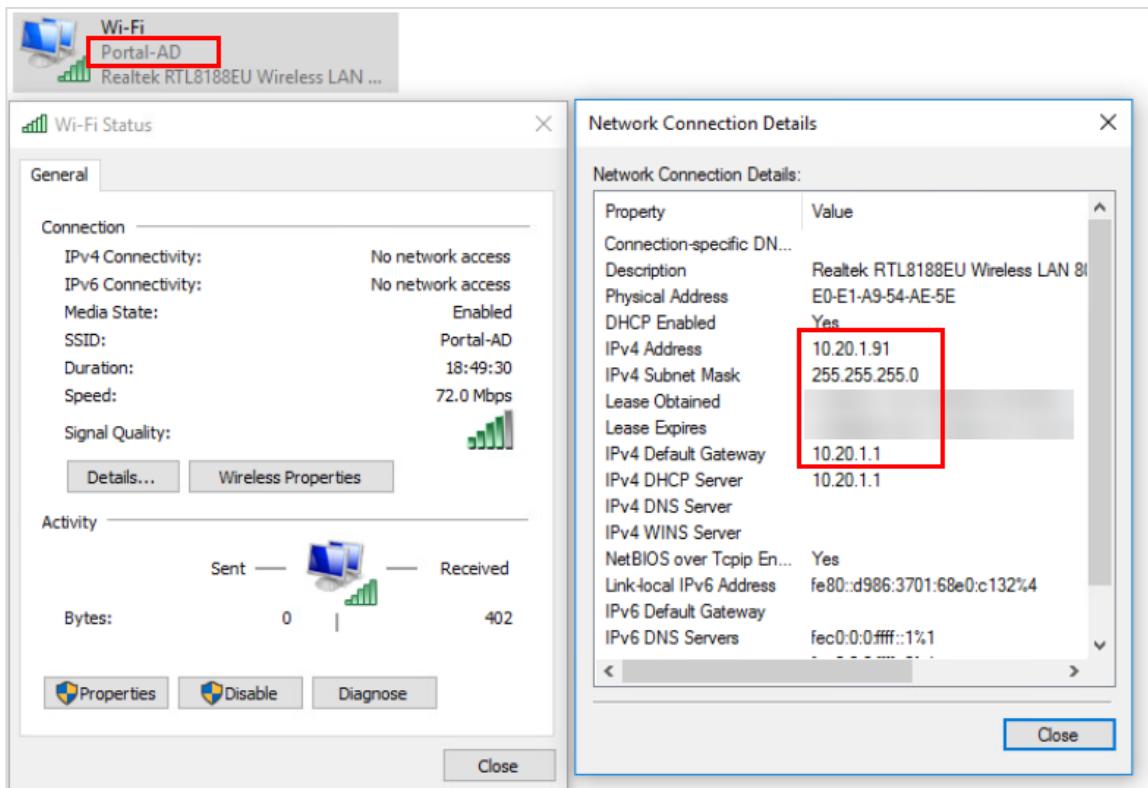


```
C:\Windows\system32>ping 172.16.30.100

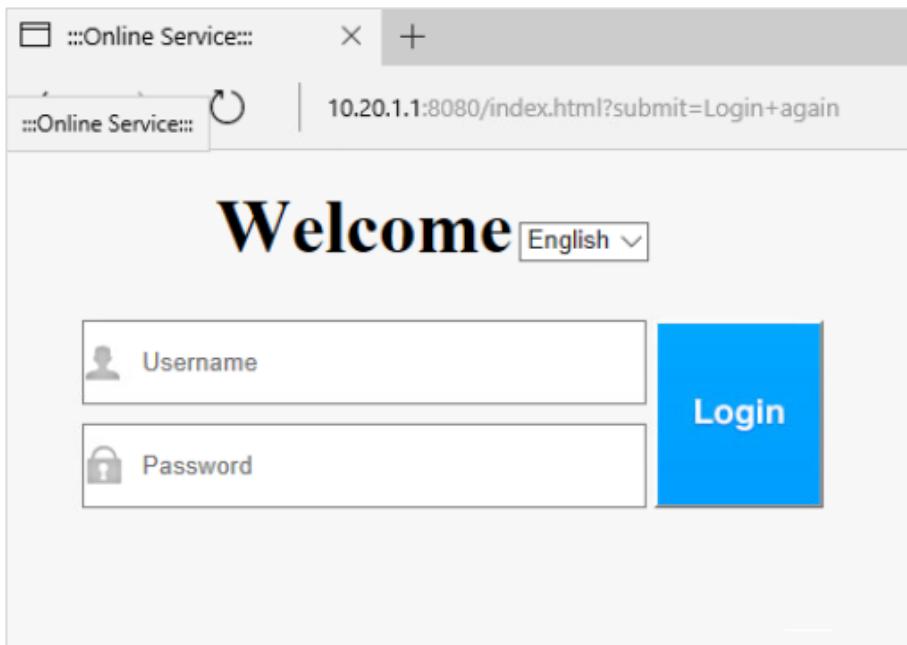
Pinging 172.16.30.100 with 32 bytes of data:
Reply from 172.16.30.100: bytes=32 time=18ms TTL=125
Reply from 172.16.30.100: bytes=32 time=10ms TTL=125
Reply from 172.16.30.100: bytes=32 time=25ms TTL=125
Reply from 172.16.30.100: bytes=32 time=43ms TTL=125

Ping statistics for 172.16.30.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 43ms, Average = 24ms
```

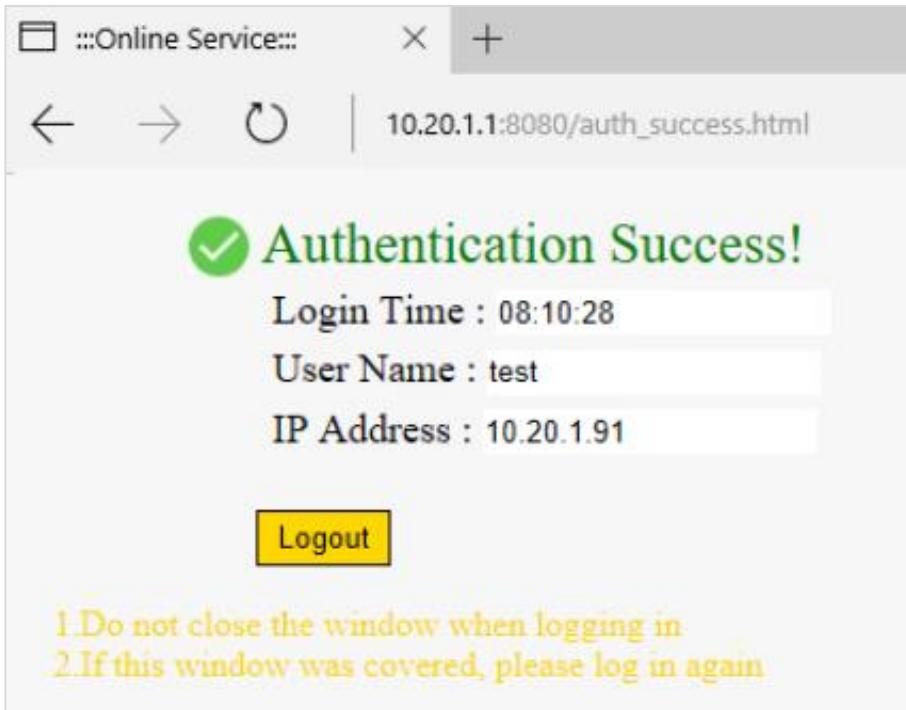
Verify that PC3 can access the Internet after connecting to the wireless network named Portal-AD and completing AD authentication on the Portal page.



Verify that the authentication page is displayed after 1.1.1.1 is entered in the address bar of the browser on the wireless terminal.



Enter the user name test and password Huawei@123, and click Login.



Verify that PC3 can ping 4.4.4.1 on the Internet in the CLI.

```
C:\Users\Security>ping 4.4.4.1

Pinging 4.4.4.1 with 32 bytes of data:
Reply from 4.4.4.1: bytes=32 time=6ms TTL=250
Reply from 4.4.4.1: bytes=32 time=12ms TTL=250
Reply from 4.4.4.1: bytes=32 time=17ms TTL=250
Reply from 4.4.4.1: bytes=32 time=37ms TTL=250

Ping statistics for 4.4.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 37ms, Average = 18ms
```

15.4 Configuration Reference

15.4.1 SW1's Configuration

```
#  
sysname SW1  
#  
vlan batch 2 40 100 200 300  
#  
bfd  
#  
interface vlanif1  
    ip address 100.1.1.1 255.255.255.0  
#  
interface vlanif2
```

```
ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
ip address 3.3.3.1 255.255.255.252
#
interface vlanif200
ip address 20.20.1.1 255.255.255.252
#
interface GigabitEthernet0/0/2
port link-type access
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/13
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/14
port link-type access
port default vlan 200
#
interface GigabitEthernet0/0/15
port link-type access
port default vlan 300
#
return
```

15.4.2 SW2's Configuration

```
#
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 30
#
interface GigabitEthernet0/0/2
port link-type access
port default vlan 30
#
interface GigabitEthernet0/0/3

#
interface GigabitEthernet0/0/13
port link-type access
port default vlan 30
#
interface GigabitEthernet0/0/14
port link-type access
port default vlan 30
```

```
#  
interface GigabitEthernet0/0/15  
port link-type access  
port default vlan 30  
#  
interface GigabitEthernet0/0/16  
port link-type access  
port default vlan 30  
#  
interface GigabitEthernet0/0/17  
port link-type access  
port default vlan 30  
#  
return
```

15.4.3 SW3's Configuration

```
#  
sysname SW3  
#  
vlan batch 10 40 2000 4000  
#  
#  
interface vlanif40  
ip address 172.16.20.20 255.255.255.0  
#  
interface vlanif2000  
ip address 22.22.22.2 255.255.255.0  
#  
interface GigabitEthernet0/0/1  
port link-type access  
port default vlan 40  
#  
interface GigabitEthernet0/0/2  
port link-type access  
port default vlan 40  
#  
interface GigabitEthernet0/0/3  
port link-type trunk  
port trunk allow-pass vlan 10 40 2000 4000  
#  
interface GigabitEthernet0/0/12  
description link-to-AP manager-vlan4000  
port link-type trunk  
port trunk pvid vlan 4000  
port trunk allow-pass vlan 4000  
#  
interface GigabitEthernet0/0/13  
description link-to-PC1  
port link-type access  
port default vlan 40  
#  
interface GigabitEthernet0/0/14  
description link-to-PC2
```

```
port link-type access
port default vlan 40
#
ip route-static 0.0.0.0 0.0.0.0 172.16.20.1
ip route-static 10.20.1.0 255.255.255.0 22.22.22.1
#
return
```

15.4.4 Mirror-SW's Configuration

```
#
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/1
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
    port link-type trunk
    port trunk allow-pass vlan 2 40
#
return
```

15.4.5 RT1's Configuration

```
#
sysname RT1
#
bfd
#
acl number 3500
rule 5 permit ip source 172.16.20.0 0.0.0.255
rule 10 permit ip source 172.16.30.0 0.0.0.255
#
interface GigabitEthernet0/0/1.2
dot1q termination vid 2
ip address 4.4.4.2 255.255.255.252
nat server protocol tcp global interface GigabitEthernet 0/0/1.2 8443 inside 10.3.1.2 443
nat server protocol tcp global interface GigabitEthernet 0/0/1.2 4500 inside 10.3.1.2 4500
nat server protocol tcp global interface GigabitEthernet 0/0/1.2 500 inside 10.3.1.2 500
nat server protocol tcp global interface GigabitEthernet 0/0/1.2 8080 inside 172.16.30.102 www
nat outbound 3500
#
interface GigabitEthernet0/0/2
undo portswitch
ip address 10.1.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
```

```
#  
interface GigabitEthernet0/0/3  
undo portswitch  
ip address 10.2.1.1 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/4  
undo portswitch  
ip address 10.3.1.1 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2  
discriminator local 10  
discriminator remote 20  
commit  
#  
ospf 1  
default-route-advertise alway  
import-route static  
area 0.0.0.0  
#  
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1  
#  
return
```

15.4.6 RT2's Configuration

```
#  
sysname RT2  
#  
bfd  
#  
acl number 3500  
rule 5 permit ip source 172.16.20.0 0.0.0.255  
rule 10 permit ip source 172.16.30.0 0.0.0.255  
#  
interface GigabitEthernet0/0/1.40  
dot1q termination vid 40  
ip address 3.3.3.2 255.255.255.252  
nat server protocol tcp global interface GigabitEthernet 0/0/1.40 8080 inside 172.16.30.102 www  
nat outbound 3500  
#  
interface GigabitEthernet0/0/2  
undo portswitch  
ip address 10.1.1.2 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/3  
undo portswitch  
ip address 10.5.1.1 255.255.255.252  
ospf enable 1 area 0.0.0.0  
#  
interface GigabitEthernet0/0/4  
undo portswitch
```

```
ip address 10.6.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
bfd 2 bind peer-ip 10.6.1.2 source-ip 3.3.3.2
discriminator local 30
discriminator remote 40
commit
#
ospf 1
default-route-advertise always
import-route static
area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

15.4.7 FW1's Configuration

```
#
sysname FW1
#
hrp enable
hrp interface Eth-Trunk0 remote 10.10.10.2
hrp mirror session enable
hrp standby config enable
hrp load balance device
hrp track interface GigabitEthernet0/0/2
hrp track bfd-session 20
#
bfd
#
acl number 3003
rule 15 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
#
ipsec proposal 1
esp authentication-algorithm sha2-256
esp encryption-algorithm aes-256
#
ike proposal 2
encryption-algorithm aes-256
dh group14
authentication-algorithm sha2-256
authentication-method pre-share
integrity-algorithm hmac-sha2-256
prf hmac-sha2-256
#
ike peer 1
pre-shared-key %%^#-o`2Fz^3L%=eGt3H\|a%6't{HKksE:w4KZVxvN3N%^%#
ike-proposal 2
remote-id-type none
remote-address 100.1.1.8
rsa encryption-padding oaep
rsa signature-padding pss
```

```
local-id-preference certificate enable
ikev2 authentication sign-hash sha2-256
#
ipsec policy 1 1 isakmp
    security acl 3003
    ike-peer 1
    proposal 1
    tunnel local applied-interface
    alias 1-10
    sa trigger-mode auto
    sa duration traffic-based 20971520
    sa duration time-based 3600
#
portal-access-profile name default
#
interface Eth-Trunk0
    ip address 10.10.10.1 255.255.255.0
#
#
interface GigabitEthernet0/0/1
    undo shutdown
    ip address 10.5.1.2 255.255.255.252
    ospf enable 1 area 0.0.0.0
    ospf cost 10
#
interface GigabitEthernet0/0/2
    undo shutdown
    ip address 10.3.1.2 255.255.255.252
    ospf enable 1 area 0.0.0.0
    ipsec policy 1
#
interface GigabitEthernet0/0/3
    undo shutdown
    eth-trunk 0
#
interface GigabitEthernet0/0/4
    undo shutdown
    eth-trunk 0
#
interface GigabitEthernet0/0/5
    undo shutdown
    ip address 172.16.30.2 255.255.255.0
    vrrp vrid 2 virtual-ip 172.16.30.1 active
    ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/6
    undo shutdown
    ip address 172.16.20.2 255.255.255.0
    vrrp vrid 1 virtual-ip 172.16.20.1 active
    ospf enable 1 area 0.0.0.0
#
firewall zone local
    set priority 100
#
firewall zone trust
```

```
set priority 85
add interface GigabitEthernet0/0/5
add interface GigabitEthernet0/0/6
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
    add interface GigabitEthernet0/0/2
#
firewall zone dmz
    set priority 50
    add interface Eth-Trunk0
#
bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2
discriminator local 20
discriminator remote 10
commit
#
ospf 1
import-route static
area 0.0.0
    network 172.16.30.0 0.0.0.255
network 172.16.20.0 0.0.0.255
#
ip route-static 10.20.1.0 255.255.255.0 172.16.20.20
ip route-static 22.22.22.0 255.255.255.252 172.16.20.20
#
v-gateway public ssl version tlsv12
v-gateway public ssl public-key algorithm rsa
v-gateway public ssl ciphersuit custom aes256-sha aes128-sha
v-gateway public certificate-server server_local.cer enable
v-gateway ssl-renegotiation-attack defend enable
v-gateway ssl weak-encryption enable
v-gateway gateway interface GigabitEthernet0/0/2 private
v-gateway gateway authentication-domain default
v-gateway gateway alias gateway
#
profile type url-filter name url_profile_01
    add blacklist url www.example.com
#
*****BEGIN***gateway**1****#
v-gateway gateway
basic
    ssl version tlsv12
    ssl timeout 5
    ssl lifecycle 1440
    ssl public-key algorithm rsa
    ssl ciphersuit custom aes256-sha aes128-sha
service
    network-extension enable
    network-extension keep-alive enable
    network-extension keep-alive interval 120
    network-extension netpool 11.11.11.10 11.11.11.20 255.255.255.0
    netpool 11.11.11.10 default
    network-extension mode manual
```

```
network-extension manual-route 172.16.30.0 255.255.255.0
security
    policy-default-action permit vt-src-ip
    certification cert-anonymous cert-field user-filter subject cn group-filter subject cn
    certification cert-anonymous filter-policy permit-all
    certification cert-challenge cert-field user-filter subject cn
    certification user-cert-filter key-usage any
    undo public-user enable
hostchecker
cache-cleaner
vpndb
    group /default
role
    role default
    role default condition all
    role default network-extension enable
*****END****#
#
security-policy
    rule name untrust-local
        source-zone untrust
        destination-zone local
        destination-address 10.3.1.2 mask 255.255.255.255
        destination-address 172.16.30.0 mask 255.255.255.0
        action permit
    rule name local-untrust
        source-zone local
        destination-zone untrust
        source-address 172.16.30.0 mask 255.255.255.0
        destination-address 100.1.1.8 mask 255.255.255.255
        action permit
    rule name untrust-trust
        source-zone untrust
        destination-zone trust
        source-address 172.16.40.0 mask 255.255.255.0
        source-address 20.20.1.0 mask 255.255.255.0
        destination-address 172.16.30.0 mask 255.255.255.0
        action permit
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 172.16.30.0 mask 255.255.255.0
        source-address 172.16.20.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
        destination-address 4.4.4.0 mask 255.255.255.0
        action permit
    rule name trust-untrust-internet
        source-zone trust
        destination-zone untrust
        source-address 172.16.30.0 mask 255.255.255.0
        source-address 172.16.20.0 mask 255.255.255.0
        profile url-filter url_profile_01
        action permit
#
return
```

15.4.8 FW2's Configuration

```
#  
sysname FW2  
#  
vlan batch 10  
#  
    hrp enable  
    hrp interface Eth-Trunk0 remote 10.10.10.1  
    hrp mirror session enable  
    hrp standby config enable  
    hrp load balance device  
    hrp track interface GigabitEthernet0/0/2  
    hrp track bfd-session 40  
#  
bfd  
#  
ip address-set 192.168.10.0/24 type object  
    address 0 192.168.10.0 mask 24  
#  
ip address-set 192.168.20.0/24 type object  
    address 0 192.168.20.0 mask 24  
#  
ip address-set 1.1.1.1/24 type object  
    address 0 1.1.1.0 mask 24  
#  
ip address-set 10.2.0.0/24 type object  
    address 0 range 10.2.0.1 10.2.0.254  
#  
ip address-set 172.16.20.0/24 type object  
    address 0 172.16.20.0 mask 24  
#  
ip address-set 172.16.40.0/255.255.255.0 type object  
    address 0 172.16.40.0 mask 255.255.255.0  
#  
acl number 3003  
    rule 15 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255  
acl number 3005  
    rule 5 permit ip destination 172.16.10.0 0.0.0.255  
acl number 3500  
    rule 5 permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255  
    rule 15 permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255  
    rule 20 permit ip  
#  
ipsec proposal 1  
    esp authentication-algorithm sha2-256  
    esp encryption-algorithm aes-256  
ipsec proposal test  
    transform ah  
        ah authentication-algorithm sha2-256  
#  
ike proposal 2  
    encryption-algorithm aes-256  
    dh group14  
    authentication-algorithm sha2-256
```

```
authentication-method pre-share
integrity-algorithm hmac-sha2-256
prf hmac-sha2-256
#
ike peer 1
pre-shared-key %^%#-o`2Fz^3L%=eGt3HI\%6't{HKksE:w4KZVxvN3N%^%#
ike-proposal 2
remote-id-type none
remote-address 100.1.1.8
rsa encryption-padding oaep
rsa signature-padding pss
local-id-preference certificate enable
ikev2 authentication sign-hash sha2-256
#
ipsec policy 1 1 isakmp
security acl 3003
ike-peer 1
proposal 1
tunnel local applied-interface
alias 1-10
sa trigger-mode auto
sa duration traffic-based 20971520
sa duration time-based 3600
#
portal-access-profile name default
#
interface vlanif10
ip address 192.168.10.111 255.255.255.0
#
interface Eth-Trunk0
ip address 10.10.10.2 255.255.255.0
#
interface GigabitEthernet0/0/1
undo shutdown
ip address 10.2.1.2 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/2
undo shutdown
ip address 10.6.1.2 255.255.255.252
ospf enable 1 area 0.0.0.0
ipsec policy 1
#
interface GigabitEthernet0/0/3
undo shutdown
eth-trunk 0
#
interface GigabitEthernet0/0/4
undo shutdown
eth-trunk 0
#
interface GigabitEthernet0/0/5
undo shutdown
ip address 172.16.20.3 255.255.255.0
vrrp vrid 1 virtual-ip 172.16.20.1 standby
```

```
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/6
  undo shutdown
  ip address 172.16.30.3 255.255.255.0
  vrrp vrid 2 virtual-ip 172.16.30.1 standby
  ospf enable 1 area 0.0.0.0
#
firewall zone local
  set priority 100
#
firewall zone trust
  set priority 85
  add interface GigabitEthernet0/0/5
  add interface GigabitEthernet0/0/6
  add interface vlanif10
#
firewall zone untrust
  set priority 5
  add interface GigabitEthernet0/0/1
  add interface GigabitEthernet0/0/2
#
firewall zone dmz
  set priority 50
  add interface Eth-Trunk0
#
bfd 2 bind peer-ip 3.3.3.2 source-ip 10.6.1.2
  discriminator local 40
  discriminator remote 30
  commit
#
ospf 1
import-route static
  area 0.0.0.0
    network 172.16.20.0 0.0.0.255
  network 172.16.30.0 0.0.0.255
#
#
  v-gateway public ssl version tlsv12
  v-gateway public ssl public-key algorithm rsa
  v-gateway public ssl ciphersuit custom aes256-sha aes128-sha
  v-gateway ssl-renegotiation-attack defend enable
  v-gateway ssl weak-encryption enable
  v-gateway gateway interface GigabitEthernet0/0/2 private
  v-gateway gateway authentication-domain default
  v-gateway gateway alias gateway
#
profile type url-filter name url_profile_01
  add blacklist url www.example.com
#
*****BEGIN***gateway**1****#
v-gateway gateway
  basic
    ssl version tlsv12
    ssl timeout 5
```

```
ssl lifecycle 1440
ssl public-key algorithm rsa
ssl ciphersuit custom aes256-sha aes128-sha
service
    network-extension enable
    network-extension keep-alive enable
    network-extension keep-alive interval 120
    network-extension netpool 10.10.1.1 10.10.1.10 255.255.255.0
    network-extension netpool 11.11.11.10 11.11.11.20 255.255.255.0
    netpool 11.11.11.10 default
    network-extension mode manual
    network-extension manual-route 172.16.10.0 255.255.255.0
    network-extension manual-route 172.16.30.0 255.255.255.0
security
    policy-default-action permit vt-src-ip
    certification cert-anonymous cert-field user-filter subject cn group-filter subject cn
    certification cert-anonymous filter-policy permit-all
    certification cert-challenge cert-field user-filter subject cn
    certification user-cert-filter key-usage any
    undo public-user enable
hostchecker
cachecleaner
vpndb
    group /default
role
    role default
        role default condition all
        role default network-extension enable
*****END****#
#
security-policy
    rule name untrust-local
        source-zone untrust
        destination-zone local
        destination-address 10.3.1.2 mask 255.255.255.255
        destination-address 172.16.30.0 mask 255.255.255.0
        action permit
    rule name local-untrust
        source-zone local
        destination-zone untrust
        source-address 172.16.30.0 mask 255.255.255.0
        destination-address 100.1.1.8 mask 255.255.255.255
        action permit
    rule name untrust-trust
        source-zone untrust
        destination-zone trust
        source-address 11.11.1.0 mask 255.255.255.0
        source-address 172.16.40.0 mask 255.255.255.0
        destination-address 172.16.30.0 mask 255.255.255.0
        action permit
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 172.16.30.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
```

```
action permit
rule name trust-untrust-internet
source-zone trust
destination-zone untrust
source-address 172.16.30.0 mask 255.255.255.0
source-address 172.16.20.0 mask 255.255.255.0
profile url-filter url_profile_01
action permit
#
return
```

15.4.9 FW3's Configuration

```
#  
sysname FW3  
#  
vsys enable  
resource-class r1  
    resource-item-limit session reserved-number 10000 maximum 50000  
    resource-item-limit bandwidth 20 entire  
    resource-item-limit policy reserved-number 300  
#  
vsys name vsysa 1  
    assign interface GigabitEthernet0/0/6  
    assign resource-class r1  
#  
vsys name vsysb 2  
    assign interface GigabitEthernet0/0/7  
    assign resource-class r1  
#  
ip vpn-instance default  
    ipv4-family  
#  
ip vpn-instance vsysa  
    ipv4-family  
    ipv6-family  
#  
ip vpn-instance vsysb  
    ipv4-family  
    ipv6-family  
#  
acl number 3004  
    rule 5 permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255  
#  
ipsec proposal 1  
    esp authentication-algorithm sha2-256  
    esp encryption-algorithm aes-256  
#  
ike proposal 2  
    encryption-algorithm aes-256  
    dh group14  
    authentication-algorithm sha2-256  
    authentication-method pre-share  
    integrity-algorithm hmac-sha2-256
```

```
prf hmac-sha2-256
#
ike peer 1
pre-shared-key %^%#^rHq#+>;>&y~t50lvEM>\SOyJ"bn_NTHD(~4+E4:%^%#
    ike-proposal 2
    local-id-type ip ip-configurable
    remote-id-type none
    rsa encryption-padding oaep
    rsa signature-padding pss
    local-id-preference certificate enable
    ikev2 authentication sign-hash sha2-256
#
ipsec policy-template Branch1 1
    security acl 3004
    ike-peer 1
    proposal 1
#
ipsec policy 1 10 isakmp template Branch1
#
interface GigabitEthernet0/0/1
    undo shutdown
    mtu 1000
    ip address 100.1.1.8 255.255.255.0
    ipsec policy 1
#
interface GigabitEthernet0/0/6
    undo shutdown
    ip binding vpn-instance vsysa
    ip address 172.16.40.1 255.255.255.0
#
interface GigabitEthernet0/0/7
    undo shutdown
    ip binding vpn-instance vsysb
    ip address 172.16.50.1 255.255.255.0
#
interface Virtual-if0
    ip address 172.16.0.1 255.255.255.0
#
interface Virtual-if1
    ip address 172.16.1.1 255.255.255.0
#
interface Virtual-if2
    ip address 172.16.2.1 255.255.255.0
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface Virtual-if0
#
firewall zone untrust
    set priority 5
    add interface GigabitEthernet0/0/1
#
```

```
firewall zone dmz
    set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
ip route-static vpn-instance vsysa 172.16.50.0 255.255.255.0 vpn-instance vsysb
ip route-static vpn-instance vsysb 172.16.40.0 255.255.255.0 vpn-instance vsysa
ip route-static 172.16.40.0 255.255.255.0 vpn-instance vsysa
#
security-policy
    rule name trust-untrust
        source-zone trust
        destination-zone untrust
        source-address 172.16.40.0 mask 255.255.255.0
        destination-address 172.16.30.0 mask 255.255.255.0
        action permit
    rule name untrust-trust
        source-zone untrust
        destination-zone trust
        source-address 172.16.30.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
        action permit
    rule name untrust-local
        source-zone untrust
        destination-zone local
        destination-address 100.1.1.8 mask 255.255.255.255
        action permit
    rule name local-untrust
        source-zone local
        destination-zone untrust
        source-address 100.1.1.0 mask 255.255.255.0
        destination-address 4.4.4.0 mask 255.255.255.0
        action permit
    rule name PC5-trust-to-untrust
        source-zone trust
        destination-zone untrust
        source-address 172.16.50.0 mask 255.255.255.0
        action permit
#
nat-policy
    rule name nat1
        source-zone trust
        egress-interface GigabitEthernet0/0/1
        source-address 172.16.50.0 mask 255.255.255.0
        action source-nat easy-ip
#
switch vsys vsysa
#
interface GigabitEthernet0/0/6
    undo shutdown
    ip binding vpn-instance vsysa
    ip address 172.16.40.1 255.255.255.0
#
interface Virtual-if1
    ip address 172.16.1.1 255.255.255.0
#
```

```
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/6
#
firewall zone untrust
    set priority 5
    add interface Virtual-if1
#
firewall zone dmz
    set priority 50
#
security-policy
    rule name to_HQ_allow
        source-zone local
        source-zone trust
        destination-zone untrust
        source-address 172.16.40.0 mask 255.255.255.0
        destination-address 172.16.30.0 mask 255.255.255.0
        action permit
    rule name allow-HQ-in
        source-zone untrust
        destination-zone trust
        destination-zone local
        source-address 172.16.30.0 mask 255.255.255.0
        destination-address 172.16.40.0 mask 255.255.255.0
        action permit
#
ip route-static 0.0.0.0 0.0.0.0 public
#
return
#
switch vsys vsysb
#
interface GigabitEthernet0/0/7
    undo shutdown
    ip binding vpn-instance vsysb
    ip address 172.16.50.1 255.255.255.0
#
interface Virtual-if2
    ip address 172.16.2.1 255.255.255.0
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
    add interface GigabitEthernet0/0/7
#
firewall zone untrust
    set priority 5
    add interface Virtual-if2
#
```

```
firewall zone dmz
    set priority 50
#
security-policy
    rule name to_internet_allow
        source-zone trust
        destination-zone untrust
        action permit
#
ip route-static 0.0.0.0 0.0.0.0 public
#
return
```

15.4.10 WAC's Configuration

```
#
sysname AC
#
portal local-server ip 10.20.1.1
portal local-server authentication-method pap
portal local-server http port 8080
#
portal https-redirect tls1.1 enable
#
portal pass dns enable
#
vlan batch 10 40 2000 4000 4001
#
authentication-profile name Portal-AD
    mac-access-profile Portal-AD
    portal-access-profile Portal-AD
    authentication-scheme Portal-AD
    authorization-scheme AD
    ad-server t1
#
dns resolve
dns proxy enable
#
web-auth-server server-source all-interface
#
dhcp enable
#
ad-server template t1
    ad-server authentication 172.16.30.100 88 no-ssl
    ad-server authentication base-dn dc=huawei,dc=cn
    ad-server authentication manager
    cn=Administrator,cn=users %^%#fBzRQc;\y6xPllX`G#*~Kku#.Wch~-flrN4WjNM#%^%#
    ad-server authentication host-name WIN-B3JG2458G73.huawei.cn
    ad-server authentication ldap-port 389
    ad-server user-filter sAMAccountName
    ad-server group-filter ou
    ad-server cipher-suite aes256-hmac-sha1
#
pki realm default
```

```
certificate-check none
#
portal-access-profile name Portal-AD
    portal local-server enable
#
ip pool vlan4001
    gateway-list 10.20.1.1
    network 10.20.1.0 mask 255.255.255.0
#
ip pool vlan4000
    gateway-list 10.10.1.1
    network 10.10.1.0 mask 255.255.255.0
    option 43 sub-option 3 ascii 10.10.1.1
#
aaa
    authentication-scheme Portal-AD
        authentication-mode ad
    authentication-scheme ad
        authentication-mode ad
    authorization-scheme Portal-AD
        authorization-mode ad
    domain default
        authentication-scheme default
        accounting-scheme default
        radius-server default
    domain default_admin
        authentication-scheme default
        accounting-scheme default
#
interface vlanif2000
    ip address 22.22.22.1 255.255.255.252
#
interface vlanif4000
    ip address 10.10.1.1 255.255.255.0
    dhcp select global
#
interface vlanif4001
    ip address 10.20.1.1 255.255.255.0
    dhcp select global
#
interface GigabitEthernet0/0/2
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 10 40 2000 4000
#
ip route-static 0.0.0.0 0.0.0.0 22.22.22.2
#
capwap source interface vlanif4000
capwap dtls control-link encrypt off
capwap dtls inter-controller control-link encrypt off
capwap dtls psk %^%#Q&*WA~9+*&]\Rs(\xoc$Uk*s~.gp(5nxAZ=}zew7%^%#
capwap dtls inter-controller psk %^%#Q&*WA~9+*&]\Rs(\xoc$Uk*s~.gp(5nxAZ=}zew7%^%#
#
wlan
temporary-management psk %^%##D&d:|*,@,SB2*:grN"#7r9)qj}X<6hum3~%v8Z%^%#
```

```
ap username A6070 password cipher %^%#^336,v*cZF<tH<H|F.wK35'k%cj.-~paZwWlP&R)%^%#
security-profile name Portal-AD
    security open
ssid-profile name Portal-AD
    ssid Portal-AD
vap-profile name Portal-AD
    forward-mode tunnel
service-vlan vlan-id 4001
ssid-profile Portal-AD
    security-profile Portal-AD
    authentication-profile Portal-AD
ap-group name ap-group1
    radio 0
        vap-profile Portal-AD wlan 3
    radio 1
        vap-profile Portal-AD wlan 3
    radio 2
        vap-profile Portal-AD wlan 3
ap-id 1 type-id 130 ap-mac 14ab-0228-5f80 ap-sn 2102353GES6RN5008931
    ap-name a5760
    ap-group ap-group1
provision-ap
#
return
```

15.5 Quiz

Why cannot Easy IP be deployed in the hot standby networking?

Answer: You cannot specify the VRID in Easy IP configuration. In normal cases, the active firewall uses the IP address of its outbound interface as the public IP address to set up sessions. After an active/standby switchover, the standby firewall also uses the IP address of its outbound interface as the public IP address. In this case, the sessions synchronized from the active firewall do not match the IP address of the outbound interface on the standby firewall. As a result, services are interrupted.