Huawei ICT Competition Regional Stage

Lab Exam

Issue: 1.0

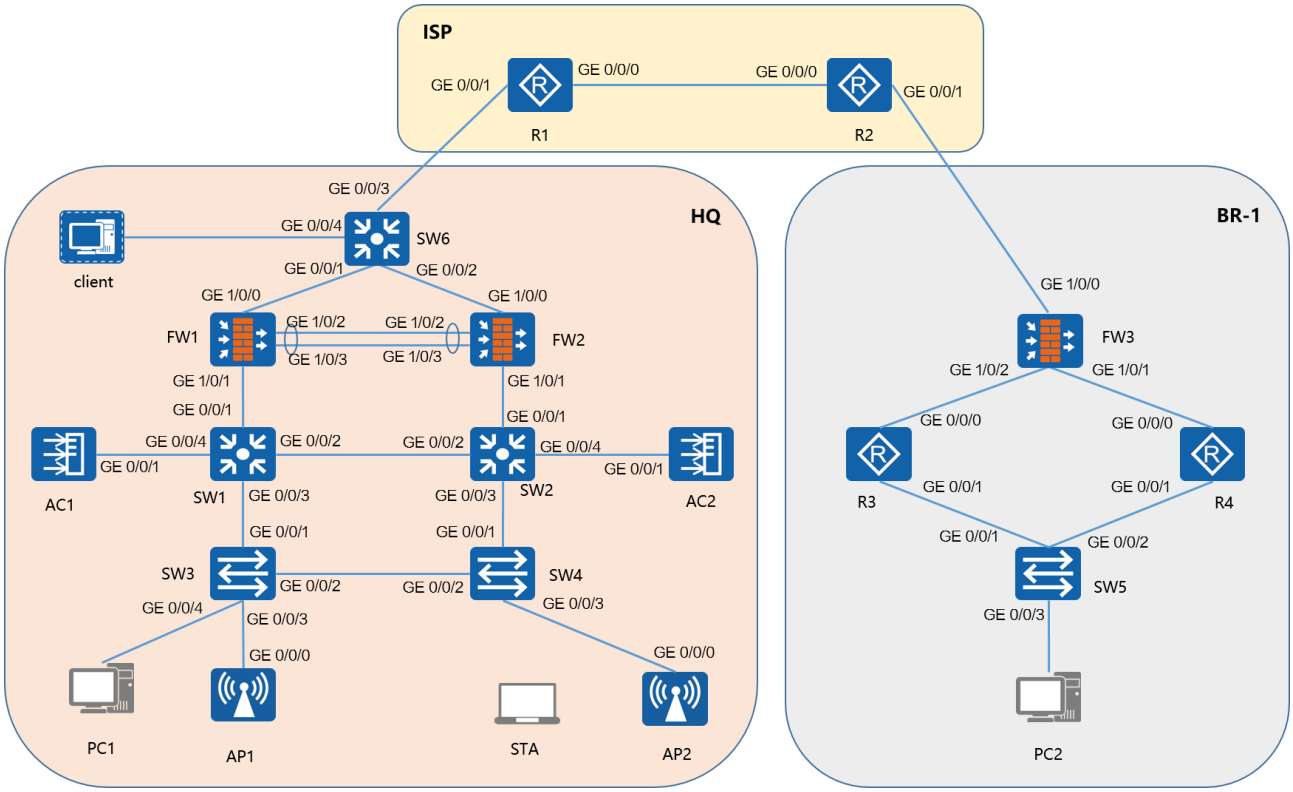
Contents

1 Background

A large enterprise has an HQ and a branch (BR-1). The HQ network provides wired and wireless access for employees. To improve network security, firewalls are deployed at the egresses of the HQ and branch networks. To improve reliability, hot standby is enabled at the HQ. To secure communication between the HQ and branch, IPSec VPN needs to be configured.

2 Network Topology

Figure 2-1 Network topology



This lab involves the following devices:

- Three USG6000V firewalls (FW1 to FW3)
- Four AR2220 routers (R1 to R4)
- Three S5700 switches (SW1 to SW2,SW6)
- Two S3700 switches (SW3 to SW5)
- Two AC6005s (AC1 and AC2)
- Two AP4050DNs (AP1 and AP2)
- Two PCs (PC1 and PC2)
- One STA (STA1)

Table 2-1 Device login information

Device	User Name	Default Password	New Password
Firewall	admin	Admin@123	Huawei@123

Table 2-2 VLAN plan

Device Name	Interface	Link Type	VLAN Plan
SW1	GE0/0/1	Trunk	Allow-pass: 104
	GE0/0/2	Trunk	Allow-pass: 101, 102, 103, 105
	GE0/0/3	Trunk	Allow-pass: 101, 102, 103
SW2	GE0/0/1	Trunk	Allow-pass: 106
	GE0/0/2	Trunk	Allow-pass: 101, 102, 103, 105
	GE0/0/3	Trunk	Allow-pass: 101, 102, 103
SW3	GE0/0/1	Trunk	Allow-pass: 101, 102, 103
	GE0/0/2	Trunk	Allow-pass: 101, 102, 103
	GE0/0/3	Trunk	
	GE0/0/4	Access	VLAN: 102
SW4	GE0/0/1	Trunk	Allow-pass: 101, 102, 103
	GE0/0/2	Trunk	Allow-pass: 101, 102, 103
	GE0/0/3	Trunk	

Table 2-3 IP address plan

Device Name	Interface	IP Address
R1	Loopback0	1.1.1.1/24
	GE0/0/1	100.1.1.1/24
	GE0/0/0	12.1.1.1/30
R2	Loopback0	2.2.2.2/24
	GE0/0/1	200.1.1.1/24
	GE0/0/0	12.1.1.2/30

Device Name	Interface	IP Address
FW1	Eth-Trunk 0	192.168.100.1/30
	GE1/0/0	100.1.1.2/24
	GE1/0/1.104	192.168.104.1/30
FW2	Eth-Trunk 0	192.168.100.2/30
	GE1/0/0	100.1.1.3/24
	GE1/0/1.106	192.168.106.1/30
SW1	VLANIF 101	192.168.101.1/24
	VLANIF 102	192.168.102.1/24
	VLANIF 103	10.11.103.254/24
	VLANIF 104	192.168.104.2/30
	VLANIF 105	192.168.105.1/30
SW2	VLANIF 105	192.168.105.2/30
	VLANIF 106	192.168.106.2/30
FW3	GE1/0/0	200.1.1.2/30
	GE1/0/2	10.10.1.1/30
	GE1/0/1	10.10.2.1/30
R3	GE0/0/0	10.10.1.2/30
	GE0/0/1	10.10.3.1/30
R4	GE0/0/0	10.10.2.2/30
	GE0/0/1	10.10.4.1/30
SW5	GE0/0/1	Vlanif 3:10.10.3.2/30
	GE0/0/2	Vlanif 4:10.10.4.2/30
	GE0/0/3	Vlanif 5:10.10.5.1/24
SW6	GE0/0/4	Vlanif 1:192.168.56.100/24
PC2	Static IP address	10.10.5.2/24

3 Configuration Tasks

3.1 HQ Network Configuration

3.1.1 Task 1: Configuring MSTP

1. Create VLANs 101, 102, and 103 on SW1, SW2, SW3, and SW4. Enable the STP protocol, and configure SW1 as the root bridge and SW2 as the secondary root bridge.
2. Create an MST region named **huawei**, and allow packets from VLANs 101 to 103 to be forwarded in the MST region.
3. Enable root protection on the designated port of the root bridge.

3.1.2 Task 2: Configuring IP Addresses

Configure IP addresses for interfaces on the network topology shown in Figure 2-1. Table 2-3 provides the planned IP addresses.

3.1.3 Task 3: Configuring DHCP

SW1 functions as the gateway of the HQ intranet and has the DHCP function enabled to allocate IP addresses to devices on the HQ's wired and wireless networks. On SW1, create DHCP service based on the interface address pool to assign IP addresses to AP1, AP2, the STA, and PC1.

1. The IP address pool for the STA and PC is 192.168.102.0/24, their gateway address is 192.168.102.1, and their DNS server IP address is 114.114.114.114.
2. The IP address pool for APs is 192.168.101.0/24, and the APs' gateway address is 192.168.101.1.

3.1.4 Task 4: Configuring OSPF

1. Enable OSPF on FW1, FW2, SW1, and SW2, and set the OSPF process ID to 1.
2. Enable OSPF on GE1/0/1.104 of FW1, GE1/0/1.106 of FW2, VLANIF104 and VLANIF105 of SW1, as well as VLANIF105 and VLANIF106 of SW2. Add these interfaces to area 0.0.0.0.
3. Configure a routing policy on SW1 to match routes to the network segment where PC1 and the STA reside, and apply the routing policy when OSPF imports user routes.

3.1.5 Task 5: Configuring Security Zones on Firewalls

1. Create a security zone named **ISP**, set the priority to **15**, and add GE1/0/0 to the zone to connect to the ISP network.
2. Create a security zone named **Heart**, set the priority to **75**, and add the hot standby heartbeat interface (Eth-trunk0) to the zone.
3. Add GE 1/0/1 and its sub-interface to the Trust zone.

3.1.6 Task 6: Configuring Firewalls to Work in Hot Standby Mode

The firewall functions as the enterprise egress gateway. To improve reliability of the HQ network, two firewalls are deployed in hot standby mode. In normal cases, FW1 functions as the active device to forward traffic. If FW1 is faulty, the enterprise network traffic is switched to FW2 to ensure normal communication between the internal and external networks.

1. Configure a VRRP group on FW1 and FW2. For details, see the VRRP data plan in Table 3-1.
2. Specify the heartbeat interface (Eth-trunk0) on FW1 and FW2, and enable hot standby on the firewalls.
3. Ensure that the OSPF route to FW1 is preferentially selected.
4. Configure a link group, so that the active/standby switchover of the firewalls can be triggered upon the failure of the uplink or downlink interface (GE1/0/0 or GE1/0/1) of FW1.

Table 3-1 VRRP data plan

VRRP Group	FW1	FW2
VRID 1	IP address: 100.1.1.2 Virtual IP address: 100.1.1.100 (active)	IP address: 100.1.1.3 Virtual IP address: 100.1.1.100 (standby)

3.1.7 Task 7: Configuring NAT on the Firewall

To ensure that users on the 192.168.102.0/24 network segment can access the Internet, configure a source NAT policy on the firewall. Employees of the enterprise need to frequently access the Internet, so port translation needs to be enabled. In addition to the IP addresses of the public network interfaces, the enterprise has applied for seven IP addresses (100.1.1.4 to 100.1.1.10) from the ISP as the public IP addresses into which private addresses can be translated.

3.1.8 Task 8: Configuring the WLAN

1. Configure the IP addresses for VLANIF 103 on AC1 and AC2 (the management interface of the two ACs) according to the AC data plan in Table 3-2, so that the ACs can communicate with each other.
2. Configure basic WLAN services to ensure that the STA can successfully obtain an IP address and access the Internet (that is, the STA can ping 1.1.1.1).
3. Configure VRRP to implement hot standby for ACs. If AC1 fails, AC2 takes over services from AC1 to ensure service continuity. The VRRP group ID is 1, interface IP addresses are 10.11.103.2 and 10.11.103.3, and the virtual IP address is 10.11.103.1.
4. Configure related devices to implement Layer 2 roaming for the STA in the WLAN coverage area.

Table 3-2 AC data plan

Configuration Item	Data
Management VLAN for APs	VLAN101
Service VLAN for the STA	VLAN102
DHCP server	SW1 functions as a DHCP server to assign IP addresses to APs and the STA. STA's gateway address: 192.168.102.1/24 APs' gateway address: 192.168.101.1/24
IP address pool for APs	192.168.101.4 – 192.168.101.254/24
IP address pool for the STA	192.168.102.4 – 192.168.102.254/24
AC's source interface	10.11.103.1 (VRRP virtual IP address)
Management IP address of AC1	VLANIF 103: 10.11.103.2/24
Management IP address of AC2	VLANIF 103: 10.11.103.3/24
IP address and port number of the hot standby channel for AC1	IP address: VLANIF 103, 10.11.103.2/24 Port number: 10241
IP address and port number of the hot standby channel for AC2	IP address: VLANIF 103, 10.11.103.3/24 Port number: 10241
AP group	Name: huawei Referenced profiles: VAP profile **huawei** and regulatory domain profile **huawei**
Regulatory domain profile	Name: huawei Country code: CN
SSID profile	Name: huawei SSID name: huaweiICT
Security profile	Name: huawei Security policy: WPA-WPA2+PSK+AES Password: huawei123
VAP profile	Name: huawei Forwarding mode: direct forwarding Service VLAN: VLAN 102 Referenced profiles: SSID profile **huawei** and security profile **huawei**

3.1.9 Task 9: Configuring QoS

1. On GE0/0/1 of SW1, limit the rate of outgoing traffic with TCP destination port numbers 6881 to 6999 from 8:00 to 18:00 on Monday through Friday, by setting the CIR to 2 Mbit/s.
2. Configure GE0/0/2 and GE0/0/3 of SW1 to re-mark the DSCP priority of incoming packets from PC1 and the STA as AF43 (38).

3.1.10 Task 10: Configuring Network Automation

The enterprise has a S5700 (SW6) with the management IP address being 192.168.56.100/24. You need to compile a script on the Client for automatically obtaining the current configuration file of the device. In the network topology shown in Figure 2-1, the Client refers to the host where Python is installed, that is, the host where the simulator is located.

1. Set the management address of the SW6 switch to its VLANIF interface IP address, that is VLANIF 1,192.168.56.100/24.
2. Enable STelnet on the SW6 switch and configure VTY user interfaces.
3. Create a local user named **python** on the SW6 switch, add the user to the administrator group, and set the service type of the user to **SSH**.
4. Create an SSH user on the SW6 switch, set the authentication mode to simple password authentication, and set the service type to **SSH**.
5. Run the Jupyter Notebook (anaconda3) software on the Client, compile a Python script for automatically logging in to the SW6 switch and displaying the configuration information of the switch.
6. Save this Python file as **python_ssh.ipynb**.

3.2 Branch Network Configuration

3.2.1 Task 1: Configuring IP Addresses

Configure IP addresses according to the IP address plan in Table 2-3.

3.2.2 Task 2: Configuring OSPF

1. Enable OSPF on FW3, R3, R4, and SW5, and set the OSPF process ID to 1.
2. Enable OSPF on GE1/0/2 and GE1/0/1 of the firewall, GE0/0/0 and GE0/0/1 of R3, GE0/0/0 and GE0/0/1 of R4, as well as GE0/0/1, GE0/0/2 and GE0/0/3 of SW5. Then add these interfaces to area 0.
3. Configure PC2 not to receive OSPF packets.
4. Traffic from PC2 to the Internet (ping 2.2.2.2) must be preferentially forwarded by R3, and traffic from the Internet to PC2 be forwarded by R4.

3.2.3 Task 3: Configuring Firewalls

1. On FW3, add GE1/0/0 to the Untrust zone and GE1/0/2 and GE1/0/1 to the Trust zone.
2. Configure a security policy to allow the branch user (PC2) to access the ISP network (1.1.1.1).

NOTE

The security policies of FW1, FW2, and FW3 cannot allow all traffic to pass through, and each security policy must be configured based on the actual requirements.

3.3 ISP Network Configuration

3.3.1 Task 1: Configuring IP Addresses

Configure router IP addresses according to the IP address plan in Table 2-3.

3.3.2 Task 2: Configuring IS-IS

1. Configure IS-IS according to the IS-IS data plan in Table 3-3, and change R1 and R2 to Level-2 routers.
2. To improve security, configure IS-IS interface authentication. Set the authentication mode of the IS-IS interface to simple authentication and the password to **Huawei@123**.

Table 3-3 IS-IS data plan

Device	Network-entity
R1	10.0000.0000.0001.00
R2	10.0000.0000.0002.00

3.4 Configuration for Communication Between the HQ and Branch

3.4.1 Task 1: Configuring an IPSec VPN

Configure a highly reliable IPSec VPN and create an IPSec tunnel using the VRRP virtual IP address.

1. Configure advanced ACL 3000 on FW1 to define the protected data flow from the HQ to the branch (source IP address: 192.168.102.0/24; destination IP address: 10.10.0.0/16).
2. Configure advanced ACL 3000 on FW3 to define the protected data flow from the HQ to the branch (source IP address: 10.10.0.0/16; destination IP address: 192.168.102.0/24).
3. Create an IPSec VPN between the HQ and branch to enable mutual access between intranet users. Establish an IPSec tunnel in IKE pre-shared key (PSK) mode. Table 3-4 provides the IPSec configuration parameters.

Table 3-4 IPSec configuration parameters

Configuration Item	FW1 and FW2	FW3
IPSec policy parameters	Method of creating an IPSec policy: ISAKMP mode	Method of creating an IPSec policy: ISAKMP mode

Configuration Item	FW1 and FW2	FW3
	Local ID type: IP address Remote ID type: IP address	Local ID type: IP address Remote ID type: IP address
IPSec proposal	Encapsulation mode: tunnel mode Security protocol: ESP	Encapsulation mode: tunnel mode Security protocol: ESP
IKE proposal	Authentication method: PSK authentication PSK: Huawei@123 Encryption algorithm: AES-256 Authentication algorithm: SHA2-256	Authentication method: PSK authentication PSK: Huawei@123 Encryption algorithm: AES-256 Authentication algorithm: SHA2-256