Virtual Private Network

Administrator Guide

Issue 01

Date 2024-02-29

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Interconnection with a Huawei AR Router (Active-Active Connections)

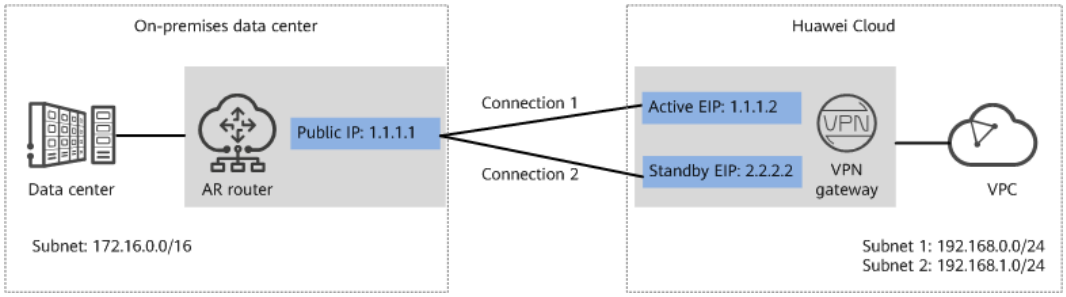
1.1 Static Routing Mode

1.1.1 Operation Guide

Scenario

Figure 1-1 shows the typical networking where a VPN gateway connects to a Huawei access router (AR) in an on-premises data center in static routing mode.

Figure 1-1 Typical networking diagram



In this scenario, the AR router has only one IP address, and the VPN gateway uses the active-active mode. A VPN connection is created between each of the two active EIPs of the VPN gateway and the IP address of the AR router.

Limitations and Constraints

VPN and AR routers support different authentication and encryption algorithms. When creating connections, ensure that the policy settings at both ends are the same.

Data Plan

Table 1-1 Data plan

Category	Item	Example of AR Router Planning	Example of Cloud-Side Planning
VPC	Subnet	172.16.0.0/16	• 192.168.0.0/24 • 192.168.1.0/24
VPN gateway	Gateway IP address	1.1.1.1 (IP address of the uplink public network interface GE0/0/8 on the AR router)	• Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
VPN connection	Tunnel interface address	• VPN connection 1: 169.254.70.1/30 • VPN connection 2: 169.254.71.1/30	• VPN connection 1: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30
	IKE policy	• IKE version: IKEv2 • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 14 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address	
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH group 14 • Transfer protocol: ESP • Lifetime (s): 3600	

Operation Process

Figure 1-2 shows the process of using the VPN service to enable communication between the data center and VPC.

Figure 1-2 Operation process

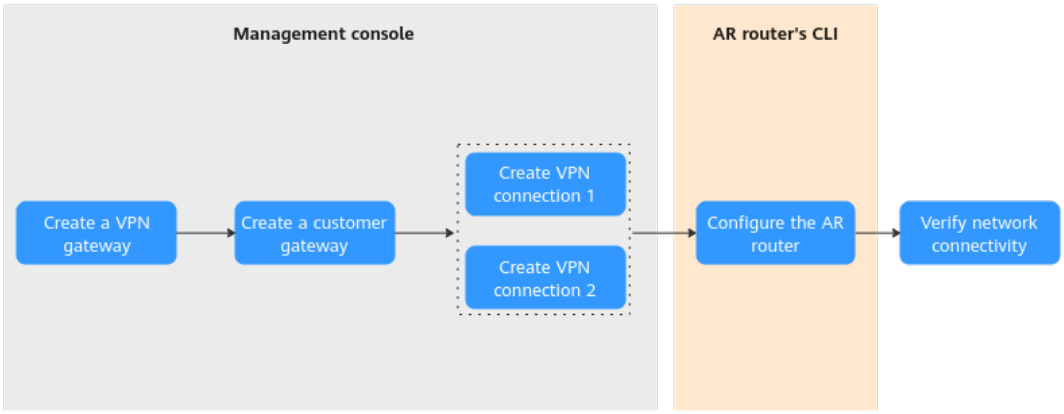


Table 1-2 Operation process description

No.	Configuration Interface	Step	Description
1	Management console	**Create a VPN gateway.**	Bind two EIPs to the VPN gateway. If you have purchased EIPs, you can directly bind them to the VPN gateway.
2		**Create a customer gateway.**	Configure the AR router as the customer gateway.
3		**Create VPN connection 1.**	Create a VPN connection between the active EIP of the VPN gateway and the customer gateway.
4		**Create VPN connection 2.**	Create a VPN connection between active EIP 2 of the VPN gateway and the customer gateway. It is recommended that the connection mode, PSK, IKE policy, and IPsec policy settings of the two VPN connections be the same.
5	Command-line interface (CLI) of the AR router	**Configure the AR router.**	• The local and remote tunnel interface addresses configured on the AR router must be the same as the customer and local tunnel interface addresses configured on the VPN console, respectively. • The connection mode, PSK, IKE policy, and IPsec policy settings on the AR router must be same as those of VPN connections.
6	-	**Verify network connectivity.**	Run the **ping** command to verify network connectivity.

1.1.2 Configuration on the Cloud Console

Prerequisites

- A VPC and its subnets have been created on the management console.

Procedure

Step 1 Log in to the management console, and choose **Networking** > **Virtual Private Network**.

Step 2 Create a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy VPN Gateway**.
2. Set parameters as prompted.

   Table 1-3 only describes the key parameters for creating a VPN gateway.

Table 1-3 VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	VPC that the on-premises data center needs to access.	vpc-001(192.168.0.0/16)
Interconnection Subnet	Subnet used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	VPC subnets that the on-premises data center needs to access.	192.168.0.0/24,192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway.	Active-active
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 3 Create a customer gateway, that is, an AR router.

1. Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.
2. Set parameters as prompted.

   Table 1-4 only describes the key parameters for creating a customer gateway.

Table 1-4 Customer gateway parameters

Parameter	Description	Value
Name	Enter the name of a customer gateway.	cgw-ar
Identifier	Select **IP Address**, and enter the public IP address of the AR router.	IP Address 1.1.1.1

Step 4 Create VPN connections.

In this scenario, a VPN connection is created between the AR router and each of the active EIP and active EIP 2 of the VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.
2. Create VPN connection 1.

   Table 1-5 only describes the key parameters for creating a VPN connection.

Table 1-5 Parameter settings for VPN connection 1

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-ar
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Customer-side subnet that needs to access the VPC on the cloud through VPN connections. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify – Automatically assign	Manually specify

Parameter	Description	Value
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the AR router.	169.254.70.1/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address. After this function is enabled, the VPN gateway automatically performs Network Quality Analysis (NQA) on the tunnel interface IP address of the customer gateway.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the AR router.	*Set this parameter based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the AR router.	– IKE Policy ▪ Version: v2 ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-128 ▪ DH Algorithm: Group 14 ▪ Lifetime (s): 86400 ▪ Local ID: IP Address ▪ Customer ID: IP Address – IPsec Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-128 ▪ PFS: DH group 14 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 3600

3. Create VPN connection 2.

   NOTE

   For VPN connection 2, you are advised to use the same parameter settings as VPN connection 1, except the parameters listed in the following table.

Table 1-6 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.2/30
Customer Tunnel Interface Address	Tunnel IP address of the AR router.	169.254.71.1/30

----End

1.1.3 Configuration on the AR Router

Procedure

Step 1 Log in to the AR router.

Step 2 Enter the system view.

```
<AR651>system-view
```

Step 3 Configure an IP address for the WAN interface.

```
[AR651]interface GigabitEthernet 0/0/8
[AR651-GigabitEthernet0/0/8]ip address 1.1.1.1 255.255.255.0
[AR651-GigabitEthernet0/0/8]quit
```

Step 4 Configure a default route.

```
[AR651]ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

In this command, 1.1.1.254 is the gateway address for the AR router's public IP address. Replace it with the actual gateway address.

Step 5 Configure routes to the active EIP and active EIP 2 of the VPN gateway.

```
[AR651]ip route-static 1.1.1.2 255.255.255.255 1.1.1.254
[AR651]ip route-static 2.2.2.2 255.255.255.255 1.1.1.254
```

- 1.1.1.2 and 2.2.2.2 are the active EIP and active EIP 2 of the VPN gateway, respectively.
- 1.1.1.254 is the gateway address for the AR router's public IP address.

Step 6 Enable the SHA-2 algorithm to be compatible with the standard RFC algorithms.

```
[AR651]IPsec authentication sha2 compatible enable
```

Step 7 Configure an IPsec proposal.

```
[AR651]IPsec proposal hwproposal1
[AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
[AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
[AR651-IPsec-proposal-hwproposal1]quit
```

Step 8 Configure an IKE proposal.

```
[AR651]ike proposal 2
[AR651-ike-proposal-2]encryption-algorithm aes-128
[AR651-ike-proposal-2]dh Group14
[AR651-ike-proposal-2]authentication-algorithm sha2-256
[AR651-ike-proposal-2]authentication-method pre-share
[AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
[AR651-ike-proposal-2]prf hmac-sha2-256
[AR651-ike-proposal-2]quit
```

Step 9 Configure IKE peers.

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]undo version 1
[AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer1]ike-proposal 2
[AR651-ike-peer-hwpeer1]local-address 1.1.1.1
[AR651-ike-peer-hwpeer1]remote-address 1.1.1.2
[AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer1]rsa signature-padding pss
[AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer1]quit
#
[AR651]ike peer hwpeer2
[AR651-ike-peer-hwpeer2]undo version 1
[AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer2]ike-proposal 2
[AR651-ike-peer-hwpeer2]local-address 1.1.1.1
[AR651-ike-peer-hwpeer2]remote-address 2.2.2.2
[AR651-ike-peer-hwpeer2]rsa encryption-padding oaep
```



```
[AR651-ike-peer-hwpeer2]rsa signature-padding pss
[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer2]quit
```

The commands are described as follows:

- **ike peer hwpeer1** and **ike peer hwpeer2**: correspond to two VPN connections.
- **pre-shared-key cipher**: specifies a pre-shared key.
- **local-address**: specifies the public IP address of the AR router.
- **remote-address**: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 10 Configure an IPsec profile.

```
[AR651]IPsec profile hwpro1
[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1
[AR651-IPsec-profile-hwpro1]proposal hwproposal1
[AR651-IPsec-profile-hwpro1]pfs dh-Group14
[AR651-IPsec-profile-hwpro1]quit
#
[AR651]IPsec profile hwpro2
[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2
[AR651-IPsec-profile-hwpro2]proposal hwproposal1
[AR651-IPsec-profile-hwpro2]pfs dh-Group14
[AR651-IPsec-profile-hwpro2]quit
```

Step 11 Configure virtual tunnel interfaces.

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 1.1.1.1
[AR651-Tunnel0/0/1]destination 1.1.1.2
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
#
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
```



```
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 1.1.1.1
[AR651-Tunnel0/0/2]destination 2.2.2.2
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

The commands are described as follows:

- **interface Tunnel0/0/1** and **interface Tunnel0/0/2**: indicate the tunnel interfaces corresponding to the two VPN connections.

  In this example, Tunnel0/0/1 establishes a VPN connection with the active EIP of the VPN gateway, and Tunnel0/0/2 establishes a VPN connection with active EIP 2 of the VPN gateway.
- **ip address**: configures an IP address for a tunnel interface on the AR router.
- **source**: specifies the public IP address of the AR router.
- **destination**: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 12 Configure NQA.

```
[AR651]nqa test-instance IPsec_nqa1 IPsec_nqa1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]test-type icmp
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
#
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit
```

The commands are described as follows:

- **nqa test-instance IPsec_nqa1 IPsec_nqa1** and **nqa test-instance IPsec_nqa2 IPsec_nqa2**: configure two NQA test instances named **IPsec_nqa1** and **IPsec_nqa2**.

In this example, the test instance **IPsec_nqa1** is created for the VPN connection to which the active EIP of the VPN gateway belongs; the test instance **IPsec_nqa2** is created for the VPN connection to which active EIP 2 of the VPN gateway belongs.

- **destination-address**: specifies the tunnel interface address of the VPN gateway.
- **source-address**: specifies the tunnel interface address of the AR router.

Step 13 Configure association between the static route and NQA.

[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1

[AR651]ip route-static 192.168.1.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1

[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 preference 100 track nqa IPsec_nqa2 IPsec_nqa2

[AR651]ip route-static 192.168.1.0 255.255.255.0 Tunnel0/0/2 preference 100 track nqa IPsec_nqa2 IPsec_nqa2

The parameters are described as follows:

- **192.168.0.0** and **192.168.1.0**: indicate VPC subnets.
  - Association between the static route and NQA needs to be configured for each subnet.
  - **Tunnel***x* and **IPsec_nqa***x* in the same command correspond to the same VPN connection.
- **preference 100** indicates the route preference. If this parameter is not specified, the default value 60 is used.

  In this example, the two VPN connections work in active-active mode, and traffic is preferentially transmitted through the VPN connection to which the active EIP of the VPN gateway belongs.

  To load balance traffic between the two VPN connections, delete **preference 100** from the preceding configuration.

----End

1.1.4 Verification

- About 5 minutes later, check states of the VPN connections.
  - Cloud console

    Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the two VPN connections are both **Normal**.
  - AR router

    Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**. The states of the two VPN connections are both **READY|STAYLIVE**.
- Verify that servers in the on-premises data center and ECSs in the VPC subnet can ping each other.

2 Classic VPN

2.1 Overview

Welcome to the *Virtual Private Network Administrator Guide*. This guide helps you configure the VPN device to implement the interconnection between your network and the VPC subnet.

A VPN connection connects your data center or network to your VPC. A customer gateway can be a physical or software device.

- **Huawei USG6600 Series**
- **Configuring VPN When Fortinet FortiGate Firewall Is Used**
- **Configuring VPN When Sangfor Firewall Is Used**
- **Using TheGreenBow IPsec VPN Client to Configure On- and Off-Cloud Communication**
- **Using Openswan to Configure On- and Off-Cloud Communication**
- **Using strongSwan to Configure On- and Off-Cloud Communication**

2.2 Huawei USG6600 Series

This section uses a Huawei USG6600 series firewall running V100R001C30SPC300 as an example to describe how to configure VPN.

Assume that the subnets of the data center are 192.168.3.0/24 and 192.168.4.0/24, the subnets of the VPC are 192.168.1.0/24 and 192.168.2.0/24, and the public IP address of the IPsec tunnel egress in the VPC is 1.1.1.1, which can be obtained from the local gateway parameters of the IPsec VPN in the VPC.

Procedure

1. Log in to the CLI of the firewall.
2. Check firewall version information.

```
display version
17:20:502017/03/09
Huawei Versatile Security Platform Software
Software Version: USG6600 V100R001C30SPC300(VRP (R) Software, Version 5.30)
```


3. Create an access control list (ACL) and bind it to the target VPN instance.

```
acl number 3065 vpn-instance vpn64
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
q
```

4. Create an IKE proposal.

```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```

5. Create an IKE peer and bind it to the created IKE proposal. The peer IP address is 1.1.1.1.

```
ike peer vpnikepeer_64
pre-shared-key ******** (******** specifies the pre-shared key.)
ike-proposal 64
undo version 2
remote-address vpn-instance vpn64 1.1.1.1
sa binding vpn-instance vpn64
q
```

6. Create an IPsec proposal.

```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```

7. Create an IPsec policy, and bind the IKE policy and IPsec proposal to it.

```
IPsec policy vpnIPsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal IPsecpro64
local-address xx.xx.xx.xx
q
```

8. Apply the IPsec policy to the corresponding sub-interface.

```
interface GigabitEthernet0/0/2.64
IPsec policy vpnIPsec64
q
```

9. Test the connectivity.

   After you perform the preceding operations, you can test the connectivity between your ECSs in the cloud and the hosts in your data center. For details, see the following figure.


```
root@i-psiybqhh:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:7c:ba:bf:cc
          inet addr:192.168.3.2  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:7cff:feba:bfcc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2304 (2.3 KB)  TX bytes:3404 (3.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1296 (1.2 KB)  TX bytes:1296 (1.2 KB)

root@i-psiybqhh:/home/ubuntu# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=62 time=4.55 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=62 time=1.27 ms
64 bytes from 192.168.1.2: icmp_req=3 ttl=62 time=1.25 ms
64 bytes from 192.168.1.2: icmp_req=4 ttl=62 time=0.871 ms
64 bytes from 192.168.1.2: icmp_req=5 ttl=62 time=0.886 ms
64 bytes from 192.168.1.2: icmp_req=6 ttl=62 time=0.676 ms
64 bytes from 192.168.1.2: icmp_req=7 ttl=62 time=1.06 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.676/1.510/4.554/1.258 ms
```

2.3 Configuring VPN When Fortinet FortiGate Firewall Is Used

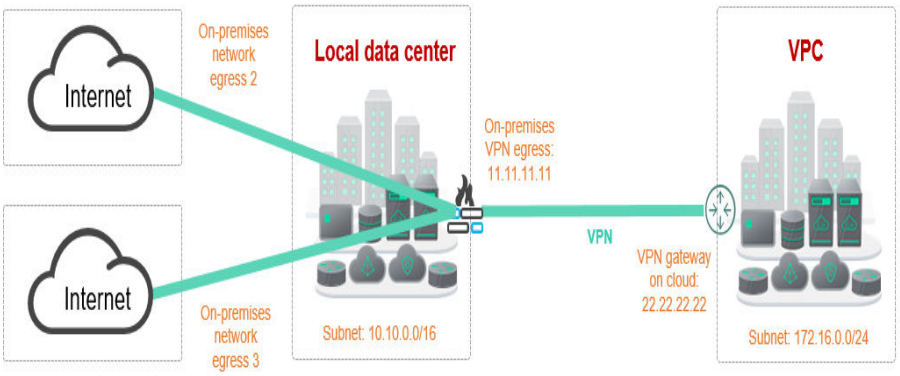
Scenarios

This section describes how to purchase and configure a VPN gateway and VPN connections on HUAWEI CLOUD to connect your on-premises network to a VPC subnet if your local data center uses FortiGate firewalls as Internet egresses.

Topology Connection

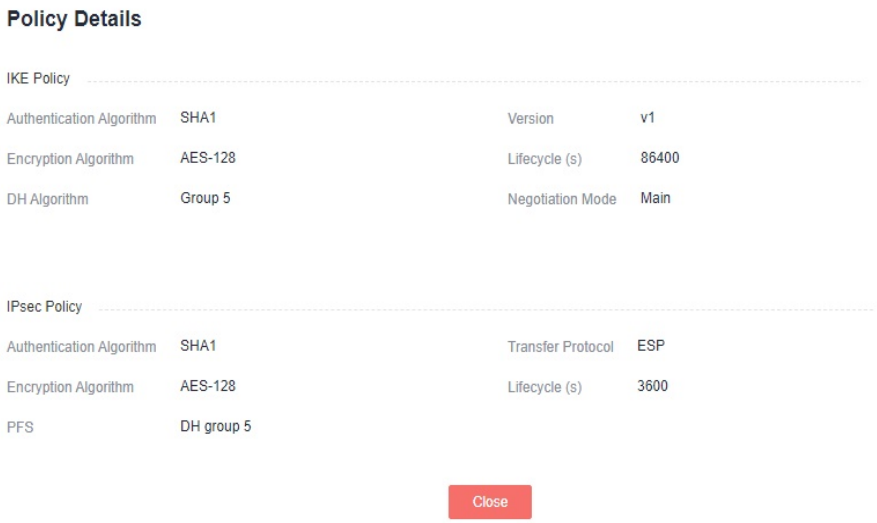
As shown in **Figure 2-1**, the local data center has multiple Internet egresses. The egress 11.11.11.11 is specified to establish a VPN connection with a HUAWEI CLOUD VPC. The subnet of the local data center is 10.10.0.0/16, and the VPC subnet on HUAWEI CLOUD is 172.16.0.0/24. The IP address of the VPN gateway you purchased on HUAWEI CLOUD is 22.22.22.22. Create a VPN connection to connect your on-premises network to the VPC subnet.

Figure 2-1 Multi-egress on-premises network connecting to a VPC through a VPN



Configure the VPN connection policies on HUAWEI CLOUD based on **Figure 2-2**.

Figure 2-2 Policy details on HUAWEI CLOUD



Configuration Procedure

This example describes how to configure a VPN if the FortiGate firewall is used on your local data center.

Step 1 Configure IPsec VPN.

1. Create a tunnel.
2. Configure the basic information for the tunnel.
3. Configure IKE phase 1 parameters.
4. Configure IPsec phase 2 parameters.
5. Configure the IPsec tunnel.

Step 2 Configure routes.

1. Add a static route.

Add a route to the cloud VPC subnet 172.16.0.0/24, with the outbound interface being the VPN tunnel interface.

2. Configure policy-based routes for multiple egresses.

   Set the source address to the subnet of the local data center and the destination address to the subnet of the VPC. Adjust the configuration sequence of the policy-based routes to ensure that the policy-based routes will be preferentially used.

Step 3 Configure policies and NAT.

1. Configure the policy to access the cloud from the local data center.
2. Configure the policy to access the local data center from the cloud.

----End

Configuration Verification

1. Check whether the on-premises VPN status is normal.
2. Check whether the cloud-based VPN status is normal.

Configuration Using the CLI

1. Configure the physical interface.

```
config system interface
  edit "port1"
      set vdom "root"
      set ip 11.11.11.11 255.255.255.0
      set type physical
next
   edit "IPsec"                          //Tunnel interface configuration
      set vdom "root"
      set type tunnel
      set interface "port1"             //Physical interface bound to the tunnel
           next
       end
```

2. Configure interface zones.

```
config system zone
   edit "trust"
      set intrazone allow
      set interface "A1"
   next
   edit "untrust"
      set intrazone allow
      set interface "port1 "
   next
end
```

3. Configure subnets.

```
config firewall address
       edit "hw-172.16.0.0/24"
      set uuid f612b4bc-5487-51e9-e755-08456712a7a0
      set subnet 172.16.0.0 255.255.255.0          //Subnet on the cloud
       next
   edit "local-10.10.0.0/16"
      set uuid 9f268868-5489-45e9-d409-5abc9a946c0c
      set subnet 10.10.0.0 255.255.0.0              //Subnet of the local data center
   next
```

4. Configure IPsec.

```
config vpn IPsec phase1-interface                          //Phase 1 configuration
   edit "IPsec"
      set interface "port1"
      set nattraversal disable
```



```
        set proposal aes128-sha1
        set comments "IPsec"
        set dhgrp 5
        set remote-gw 22.22.22.22
        set psksecret ENC dmFyLzF4tRrIjV3T
+lSzhQeU2nGEoYKC31NaYRWFJl8krlwNmZX5SfwUi5W5RLJqFu82VYKYsXp5+HZJ13VYY8O2Sn/
vruzdLxqu84zbHEIQkTlf5n/
63KEru1rRoNiHDTWfh3A3ep3fKJmxf43pQ7OD64t151ol06FMjUBLHgJ1ep9d32Q0F3f3oUxfDQs21Bi9RA
==
    next
end
config vpn IPsec phase2-interface                                    //Phase 2 configuration
    edit "IP-TEST"
        set phase1name "IPsec "
        set proposal aes128-sha1
        set dhgrp 5
        set keylifeseconds 3600
        set src-subnet 10.10.0.0 255.255.0.0
        set dst-subnet 172.16.0.0 255.255.255.0
    next
end
```

5. Configure access policies.

```
config firewall policy
 edit 15                                          //Policy 15 is used to access the on-premises data center
from the cloud. NAT is disabled.
        set uuid 4f452870-ddb2-51e5-35c9-38a987ebdb6c
        set srcintf "IPsec"
        set dstintf "trust"
        set srcaddr "hw-172.16.0.0/24"
        set dstaddr "local-10.10.0.0/16"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 29                                      //Policy 29 is used to access the cloud from the on-premises
data center. NAT is disabled.
        set uuid c2d0ec77-5254-51e9-80dc-2813ccf51463
        set srcintf "trust"
        set dstintf "IPsec"
        set srcaddr "local-10.10.0.0/16"
        set dstaddr "hw-172.16.0.0/24"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
```

6. Configure routes.

```
config router static
    edit 24                          //Route 24 is a static route that is used to access on the cloud.
        set dst 172.16.0.0 255.255.255.0
        set gateway 11.11.11.1
        set distance 10
        set device "port1"
config router policy
edit 2                      //Policy-based route 2 is used to access the cloud from the on-premises data
center.
        set input-device "A1"
        set src "10.10.00/255.255.0.0"
        set dst "172.16.0.0/255.255.255.0"
        set gateway 11.11.11.1
        set output-device "port1"
```


2.4 Configuring VPN When Sangfor Firewall Is Used

Scenarios

Your local data center uses Sangfor firewalls as Internet egresses. An IPsec VPN device is connected to the DMZ zone and needs to access the HUAWEI CLOUD network through a VPN connection.

Topology Connection

Topology connection mode:

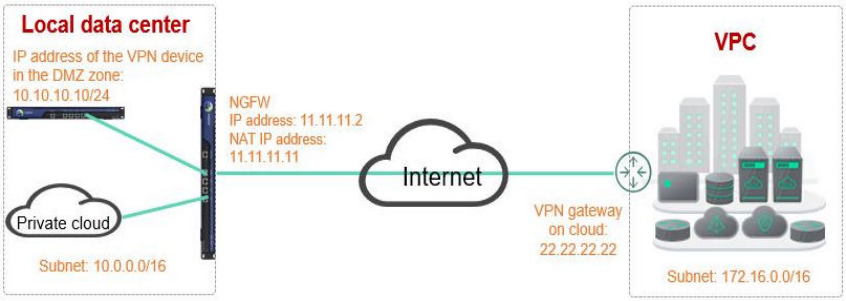
- Use the firewall to establish a VPN connection with the cloud.
- Use the VPN device in the DMZ zone and the NAT traversal technique to establish a VPN connection with the cloud.

The configuration details are as follows.

- Private IP address of the VPN device in the local data center: 10.10.10.10/24
- On-premises subnet: 10.0.0.0/16
- IP address of the next-generation firewall: 11.11.11.2/24; Public network gateway: 11.11.11.1; NAT IP address of the VPN device: 11.11.11.11
- IP address of the VPN gateway on the cloud: 22.22.22.22; Subnet on the cloud: 172.16.0.0/16

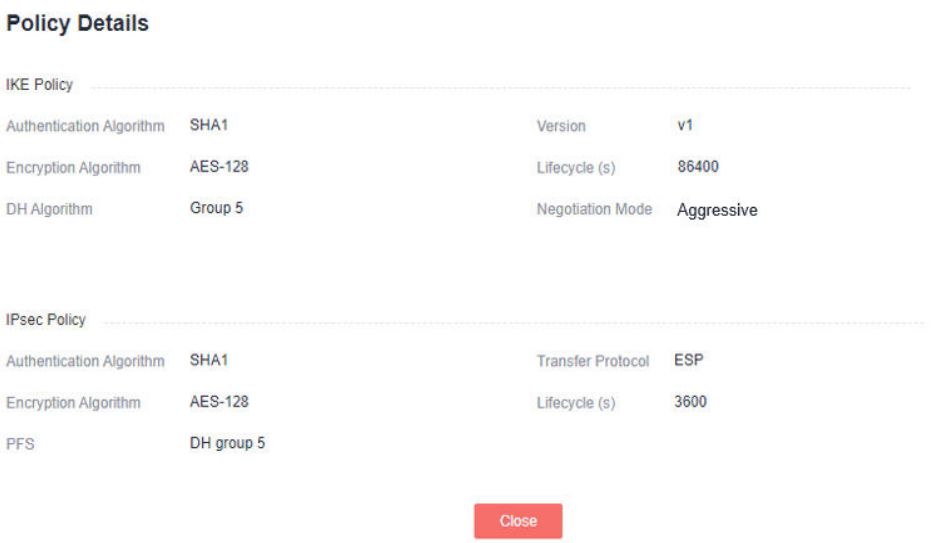
Create a VPN connection to connect an on-premises network to the VPC subnet.

Figure 2-3 Using a VPN to Connect a VPC with a local data center that uses Sangfor firewall and the NAT traversal technique



Configure the VPN connection on HUAWEI CLOUD based on **Figure 2-4**. If the VPN device in the DMZ zone uses NAT traversal, the aggressive negotiation mode should be used. If the firewall is used, the main negotiation mode should be used.

Figure 2-4 Policy details on HUAWEI CLOUD



Configuration Procedure

This example describes how to configure a VPN if the Sangfor firewall is used in your local data center.

Step 1 Configure IPsec VPN.

1. **Configure IKE phase 1 parameters.**
2. **Configure IPsec phase 2 parameters.**
3. **Configure security parameters.**

Step 2 Configure routes.

Step 3 Configure policies and NAT.

----End

Configuration Verification

Check whether the on-premises subnet can communicate with the subnet on the cloud.

2.5 Using TheGreenBow IPsec VPN Client to Configure On- and Off-Cloud Communication

Scenarios

This section describes how to use TheGreenBow IPsec VPN Client to establish a VPN connection between a VPC and a cloud desktop or between two VPCs.

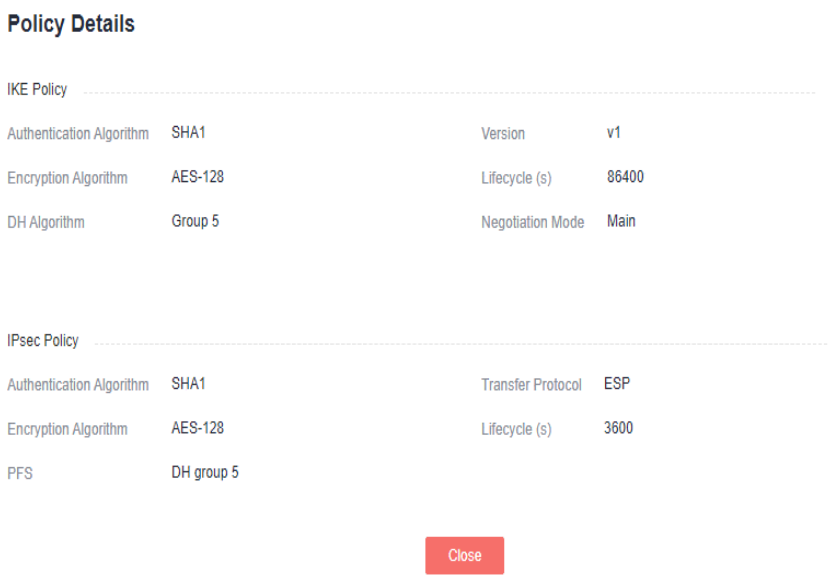
This following describes the configuration details if TheGreenBow IPsec VPN Client is used.

- **Scenario 1: Install the client on the cloud desktop that connects to the VPN gateway of the VPC.**
  a. The cloud desktop must run the Windows OS.
  b. The cloud desktop can ping the VPN gateway IP address of the VPC. (If the ping fails, the VPN connection cannot be established.)
- **Scenario 2: Install the client on the ECS in VPC1 that connects to the VPN gateway of VPC2.**
  a. Windows ECS in VPC1 has EIP.
  b. The ECS in VPC1 can ping the VPN gateway IP address of VPC2. (If the ping fails, the VPN connection cannot be established.)

Prerequisites

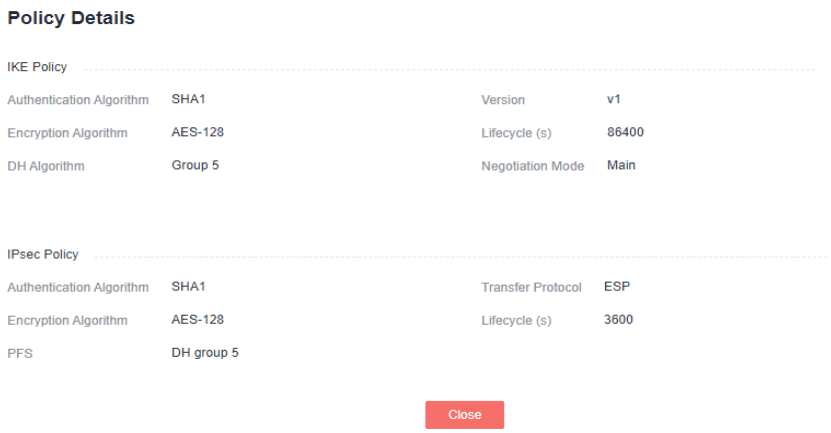
- **Scenario 1: Cloud desktop + VPC**
  - The VPC, subnet, and ECS have been configured on the cloud.
  - The VPN gateway and VPN connection on the cloud have been configured.

    Figure 2-5 Policy details

  - TheGreenBow IPsec VPN Client has been installed on the cloud desktop.
  - The cloud desktop can ping the IP address of the VPN gateway.
- **Scenario 2: VPC + VPC**
  - The VPCs, subnets, and ECSs in two regions have been configured. The ECS in VPC2 runs the Windows OS.
  - The VPN gateway and VPN connection in VPC1 have been configured.

Figure 2-6 Policy details



- TheGreenBow IPsec VPN Client has been installed on the Windows ECS in VPC2.
- The ECS in VPC2 can ping the VPN gateway IP address of VPC1.

NOTE

Use the default VPN configurations on HUAWEI CLOUD.

Configuration Procedure

Scenario 1: Client configuration in the "cloud desktop + VPC" scenario

1. Configure global parameters.
2. Configure IKE phase 1 parameters.
3. Configure IPsec phase 2 parameters.

Scenario 2: Client configuration in the "VPC + VPC" scenario

1. Configure global parameters.
2. Configure IKE phase 1 parameters.
3. Configure IPsec phase 2 parameters.

Configuration Verification

- **Scenario 1: Cloud desktop + VPC**

  Check whether the cloud desktop and the ECS in the VPC can communicate with each other.

  a. Check whether the VPN connection is successfully established.
  b. Check the VPN connection status of the VPC.
  c. Check the network configurations of the cloud desktop.
  d. Ping the ECS in the VPC from the cloud desktop.
  e. Ping the cloud desktop from the ECS in the VPC.

  The cloud desktop and the ECS in the VPC can communicate with each other successfully.

- **Scenario 2: VPC + VPC**

Check whether the ECS in VPC1 and the ECS installed with the client in VPC2 can communicate with each other.

a. Check whether the VPN connection is successfully established.
b. Check the VPN connection status of the VPC.
c. Check the VPC network configurations.
d. Ping the ECS in VPC2 from the ECS in VPC1.
e. Ping the ECS in VPC1 from the ECS in VPC2.

The ECS in VPC1 and the ECS installed with the client in VPC2 can communicate with each other successfully.

2.6 Using Openswan to Configure On- and Off-Cloud Communication

Scenarios

The VPC on the cloud has VPN gateways and VPN connections. Servers in customer data center are installed with the IPsec software to interconnect with the cloud. One-to-one NAT mapping has been configured between the customer server IP addresses and public IP addresses on the network egress.

Topology Connection

Figure 2-7 shows the topology connection and policy negotiation configurations.

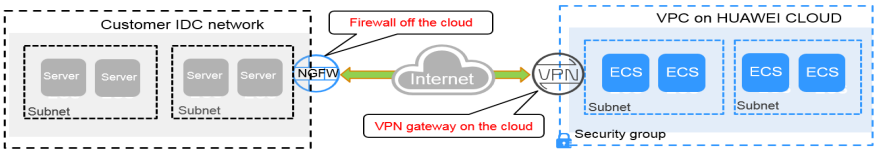
The VPN gateway IP address of the VPC is 11.11.11.11 and the local subnet is 192.168.200.0/24.

The NAT mapping IP address of the customer server is 22.22.22.22 and the local subnet is 192.168.222.0/24.

The ECS IP address and the customer server IP address are 192.168.200.200 and 192.168.222.222, respectively.

The negotiation parameters of the VPN connection use the default configurations defined on Huawei Cloud.

Figure 2-7 Topology connection and policy negotiation configuration information



Your network		Interconnection mode description: 1. The Linux servers of customers are installed with IPsec software for interconnection. 2. One-to-one NAT mapping has been configured between the customer server IP addresses and public IP addresses on the network egress.	HUAWEI CLOUD network	
IKE policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, DH algorithm **Group 5**, version **v1**, negotiation mode **Main**, and lifecycle (s) **86400**		IKE policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, DH algorithm **Group 5**, version **v1**, negotiation mode **Main**, and lifecycle (s) **86400**
IPsec policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, PFS **DH group 5**, and lifecycle (s) **3600**		IPsec policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, PFS **DH group 5**, and lifecycle (s) **3600**
Authentication mode	Pre-shared key		Authentication mode	Pre-shared key
Customer gateway	22.22.22.22		HUAWEI CLOUD gateway	11.11.11.11
Customer subnet	192.168.200.0/24		HUAWEI CLOUD subnet	192.168.200.0/24

Configuration Procedure

In this example, the Openswan IPsec client is installed on CentOS 6.8.

Step 1 Install the Openswan client.

yum install -y openswan

Step 2 Enable IPv4 forwarding.

vim /etc/sysctl.conf

1. Add the following content to this file:
```
net.ipv4.ip_forward = 1
```
2. Run the **/sbin/sysctl -p** command for the forwarding configuration to take effect.

Step 3 Configure iptables.

Run the **iptables -L** command to check whether the firewall is disabled or the data flow forwarding is allowed.
```
iptables -L
  Chain INPUT (policy ACCEPT)
  target     prot opt source               destination
  Chain FORWARD (policy ACCEPT)
  target     prot opt source               destination
  Chain OUTPUT (policy ACCEPT)
  target     prot opt source               destination
```

Step 4 Configure the pre-shared key.

vim /etc/ipsec.d/open_IPsec.secrets

Add the following content to this file:
```
22.22.22.22 11.11.11.11 : psk "IPsec-key"
```

Format: IP address for connection+Space+Customer gateway IP address+Space +English colon (:)+Space+PSK (case insensitive)+Pre-shared key. There are spaces on both sides of the colon. The key is enclosed in double quotation marks.

Step 5 Configure the IPsec connection.

vim /etc/ipsec.d/open_IPsec.conf

Add the following content to this file:
```
conn openswan_IPsec               # Set the connection name to openswan_IPsec.
  type=tunnel                   # Enable the tunnel mode.
  auto=start                    # The value can be add, route, or start.

  left=192.168.222.222             # Set the local IP address. The value must be the actual host IP address in the NAT scenario.
  leftid=22.22.22.22               # Set the local ID.
  leftsourceip=22.22.22.22         # In the NAT scenario, enter the post-NAT public IP address.
  leftsubnet=192.168.222.0/24      # Set the local subnet.
  leftnexthop=22.22.22.1           # In the NAT scenario, enter the post-NAT gateway IP address.
  right=11.11.11.11                # Set the VPN gateway IP address.
  rightid=11.11.11.11              # Set the ID of the VPN gateway.
  rightsourceip=11.11.11.11        # Set the VPN gateway IP address.
  rightsubnet=192.168.200.0/24     # Set the subnet of the VPN gateway.
  rightnexthop=%defaultroute       # Set the default route.

  authby=secret                 # Set the authentication mode to PSK.
  keyexchange=ike               # Set the IKE key exchange mode.
  ike=aes128-sha1;modp1536         # Define the IKE algorithm and group based on the configuration of the VPN gateway.
```



```
 ikev2=never                    # Disable the IKEv2 version.
 ikelifetime=86400s               # Set the lifetime of IKE SAs.

 phase2=esp                     # Set the data transmission format in phase 2.
 phase2alg=aes128-sha1;modp1536    # Set the algorithm and group in the IPsec policy based on the
configuration of the VPN gateway.
 pfs=yes                      # Enable PFS.
 compress=no                    # Disable compression.
 salifetime=3600s               # Set the lifetime of SAs in phase 2.
```

NOTE

- In NAT traversal scenarios, you can set **forceencaps** to yes as required.
- For details about the bits of DH groups used by Huawei Cloud VPN, see **What Are the Bits of the DH Groups Used by Huawei Cloud VPN?**.

After the configuration is complete, run the **ipsec verify** command to verify the configuration items. If **OK** is displayed for all items in the command output, the configuration is successful.

```
ipsec verify
Verifying installed system and configuration files
Version check and IPsec on-path                         [OK]
Libreswan 3.25 (netkey) on 3.10.0-957.5.1.el7.x86_64
Checking for IPsec support in kernel                          [OK]
 NETKEY: Testing XFRM related proc values
       ICMP default/send_redirects              [OK]
       ICMP default/accept_redirects            [OK]
       XFRM larval drop                       [OK]
Pluto IPsec.conf syntax                         [OK]
Two or more interfaces found, checking IP forwarding[OK]
Checking rp_filter                            [OK]
Checking that pluto is running                  [OK]
 Pluto listening for IKE on udp 500             [OK]
 Pluto listening for IKE/NAT-T on udp 4500      [OK]
 Pluto IPsec.secret syntax                    [OK]
Checking 'ip' command                           [OK]
Checking 'iptables' command                     [OK]
Checking 'prelink' command does not interfere with FIPS[OK]
Checking for obsolete IPsec.conf options        [OK]
```

If the following information is displayed, the configuration fails:

```
Checking rp_filter                            [ENABLED]
 /proc/sys/net/ipv4/conf/default/rp_filter        [ENABLED]
 /proc/sys/net/ipv4/conf/lo/rp_filter             [ENABLED]
 /proc/sys/net/ipv4/conf/eth0/rp_filter           [ENABLED]
 /proc/sys/net/ipv4/conf/eth1/rp_filter           [ENABLED]
 /proc/sys/net/ipv4/conf/ip_vti01/rp_filter           [ENABLED]
```

To rectify the fault, run the following commands:

```
echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/default/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/lo/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/ip_vti01/rp_filter
```

Step 6 Start the service.

service ipsec stop # Stop the service.

service ipsec start # Start the service.

service ipsec restart # Restart the service.

ipsec auto --down openswan_IPsec # Disable the connection.

ipsec auto --up openswan_IPsec # Enable the connection.

NOTE

Restart the service and enable the connection after each modification.

----End

Configuration Verification

Run the **ipsec --status** command to query the IPsec status. Information (extract) similar to the following is displayed.

```
Connection list:
000
000 "openswan_IPsec":
192.168.222.0/24===192.168.222.222<192.168.222.222>[22.22.22.22]---22.22.22.1...11.11.11.11<11.11.11.11>
===192.168.200.0/24; erouted; eroute owner: #30
000 "openswan_IPsec":     oriented; my_ip=22.22.22.22; their_ip=11.11.11.11; my_updown=IPsec _updown;
000 "openswan_IPsec":   xauth us:none, xauth them:none,  my_username=[any]; their_username=[any]
000 "openswan_IPsec":   our auth:secret, their auth:secret
000 "openswan_IPsec":   modecfg info: us:none, them:none, modecfg policy:push, dns:unset, domains:unset,
banner:unset, cat:unset;
000 "openswan_IPsec":   labeled_IPsec:no;
000 "openswan_IPsec":   policy_label:unset;
000 "openswan_IPsec":   ike_life: 86400s; IPsec_life: 3600s; replay_window: 32; rekey_margin: 540s;
rekey_fuzz: 100%; keyingtries: 0;
000 "openswan_IPsec":   retransmit-interval: 500ms; retransmit-timeout: 60s;
000 "openswan_IPsec":   initial-contact:no; cisco-unity:no; fake-strongswan:no; send-vendorid:no; send-no-
esp-tfc:no;
000 "openswan_IPsec":   policy: PSK+ENCRYPT+TUNNEL+PFS+UP+IKEV1_ALLOW+SAREF_TRACK
+IKE_FRAG_ALLOW+ESN_NO;
000 "openswan_IPsec":   conn_prio: 24,24; interface: eth0; metric: 0; mtu: unset; sa_prio:auto; sa_tfc:none;
000 "openswan_IPsec":   nflog-group: unset; mark: unset; vti-iface:unset; vti-routing:no; vti-shared:no; nic-
offload:auto;
000 "openswan_IPsec":   our idtype: ID_IPV4_ADDR; our id=1.1.1.1; their idtype: ID_IPV4_ADDR; their
id=2.2.2.2
000 "openswan_IPsec":   dpd: action:hold; delay:0; timeout:0; nat-t: encaps:auto; nat_keepalive:yes;
ikev1_natt:both
000 "openswan_IPsec":   newest ISAKMP SA: #3; newest IPsec SA: #30;
000 "openswan_IPsec":   IKE algorithms: AES_CBC_128-HMAC_SHA1-MODP1536
000 "openswan_IPsec":   IKE algorithm newest: AES_CBC_128-HMAC_SHA1-MODP1536
000 "openswan_IPsec":   ESP algorithms: AES_CBC_128-HMAC_SHA1_96-MODP1536
000 "openswan_IPsec":   ESP algorithm newest: AES_CBC_128-HMAC_SHA1_96; pfsgroup=MODP1536
000
000 Total IPsec connections: loaded 1, active 1
000
000 State Information: DDoS cookies not required, Accepting new IKE connections
000 IKE SAs: total(1), half-open(0), open(0), authenticated(1), anonymous(0)
000 IPsec SAs: total(1), authenticated(1), anonymous(0)
000
000 #3: "openswan_IPsec":4500 STATE_MAIN_R3 (sent MR3, ISAKMP SA established); EVENT_SA_REPLACE
in 15087s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0); idle; import:admin initiate
000 #30: "openswan_IPsec":4500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in
1744s; newest IPsec; eroute owner; isakmp#3; idle; import:admin initiate
000 #30: "openswan_IPsec" esp.b810a24@11.11.11.11 esp.aab7b496@192.168.222.222 tun.0@11.11.11.11
tun.0@192.168.222.222 ref=0 refhim=0 Traffic: ESPin=106KB ESPout=106KB! ESPmax
=4194303B
```

2.7 Using strongSwan to Configure On- and Off-Cloud Communication

Scenarios

The VPC on the cloud has VPN gateways and VPN connections. Servers in customer data center are installed with the IPsec software to interconnect with

the cloud. One-to-one NAT mapping has been configured between the customer server IP addresses and public IP addresses on the network egress.

Topology Connection

Figure 2-8 shows the topology connection and policy negotiation configurations.

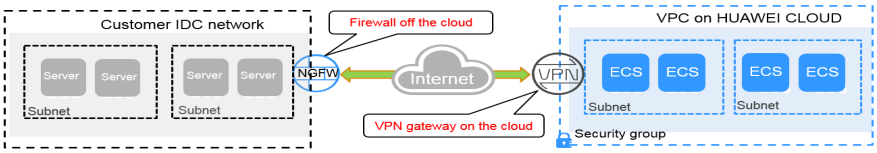
The VPN gateway IP address of the VPC is 11.11.11.11 and the local subnet is 192.168.200.0/24.

The NAT mapping IP address of the customer server is 22.22.22.22 and the local subnet is 192.168.222.0/24.

The ECS IP address and the customer server IP address are 192.168.200.200 and 192.168.222.222, respectively.

The negotiation parameters of the VPN connection use the default configurations defined on Huawei Cloud.

Figure 2-8 Topology connection and policy negotiation configuration information



Your network		Interconnection mode description: 1. The Linux servers of customers are installed with IPsec software for interconnection. 2. One-to-one NAT mapping has been configured between the customer server IP addresses and public IP addresses on the network egress.	HUAWEI CLOUD network	
IKE policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, DH algorithm **Group 5**, version **v1**, negotiation mode **Main**, and lifecycle (s) **86400**		IKE policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, DH algorithm **Group 5**, version **v1**, negotiation mode **Main**, and lifecycle (s) **86400**
IPsec policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, PFS **DH group 5**, and lifecycle (s) **3600**		IPsec policy	Authentication algorithm **SHA1**, encryption algorithm **AES-128**, PFS **DH group 5**, and lifecycle (s) **3600**
Authentication mode	Pre-shared key		Authentication mode	Pre-shared key
Customer gateway	22.22.22.22		HUAWEI CLOUD gateway	11.11.11.11
Customer subnet	192.168.200.0/24		HUAWEI CLOUD subnet	192.168.200.0/24

Configuration Procedure

The configurations may vary according to the the strongSwan version. The following uses strongSwan 5.7.2 as an example to describe the VPN configurations of strongSwan in the Linux system.

Step 1 Install the IPsec VPN client.

yum install strongswan

During the installation, select **Y**. The installation is complete when the message "Complete!" is displayed. The configuration files of strongSwan are stored in the **/etc/strongswan** directory. During the configuration, you only need to edit the **IPsec.conf** and **IPsec.secrets** files.

Step 2 Enable IPv4 forwarding.

vim /etc/sysctl.conf

1. Add the following content to this file:


```
net.ipv4.ip_forward = 1
```

2. Run the **/sbin/sysctl -p** command for the forwarding configuration to take effect.

Step 3 Configure iptables.

Run the **iptables -L** command to check whether the firewall is disabled or the data flow forwarding is allowed.

```
iptables -L
  Chain INPUT (policy ACCEPT)
  target     prot opt source               destination
  Chain FORWARD (policy ACCEPT)
  target     prot opt source               destination
  Chain OUTPUT (policy ACCEPT)
  target     prot opt source               destination
```

Step 4 Configure the pre-shared key.

```
vim /etc/strongswan/IPsec.secrets          # Edit the IPsec.secrets file.
22.22.22.22 11.11.11.11 : PSK "IPsec-key"
```

Format: IP address for connection+Space+Customer gateway IP address+Space +English colon (:)+Space+PSK (uppercase)+Pre-shared key. There are spaces on both sides of the colon. The key is enclosed in double quotation marks.

Step 5 Configure the IPsec connection.

vim /etc/strongswan/IPsec.conf

Add the following content to this file:

```
config setup
conn strong_IPsec                    # Set the connection name to strong_IPsec.
 auto=route                         # The value can be add, route, or start.
  type=tunnel                        # Enable the tunnel mode.
 compress=no                         # Disable compression.
 leftauth=psk                       # Set the local authentication mode to PSK.
 rightauth=psk                       # Set the remote authentication mode to PSK.
 ikelifetime=86400s                   # Set the lifetime of IKE SAs.
 lifetime=3600s                     # Set the lifetime of IPsec SAs.
 keyexchange=ikev1                     # Set the IKE version to version 1.
 ike=aes128-sha1-modp1536!                  # Set the algorithm and group in the IKE policy based on the
configuration of the VPN gateway.
 esp=aes128-sha1-modp1536!                   # Set the algorithm and group in the IPsec policy based on the
configuration of the VPN gateway.
 leftid=22.22.22.22                  # Set the local ID.
 left=192.168.222.222                  # Set the local IP address. The value must be the actual host IP
address in the NAT scenario.
 leftsubnet=192.168.222.0/24              # Set the local subnet.
 rightid=11.11.11.11                 # Set the ID of the VPN gateway.
 right=11.11.11.11                   # Set the VPN gateway IP address.
 rightsubnet=192.168.200.0/24              # Set the subnet of the VPN gateway.
```

NOTE

For details about the bits of DH groups used by Huawei Cloud VPN, see **What Are the Bits of the DH Groups Used by Huawei Cloud VPN?**.

Step 6 Start the service.

service strongswan stop # Stop the service.

service strongswan start # Start the service.

service strongswan restart # Restart the service.

strongswan stop # Disable the connection.

strongswan start # Enable the connection.

NOTE

Restart the service and enable the connection after each modification.

----End

Configuration Verification

Run the **strongswan statusall** command to query the connection start time.

```
Status of IKE charon daemon (strongSwan 5.7.2, Linux 3.10.0-957.5.1.el7.x86_64, x86_64):
  uptime: 5 minutes, since Apr 24 19:25:29 2019
  malloc: sbrk 1720320, mmap 0, used 593088, free 1127232
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 1
  loaded plugins: charon pkcs11 tpm aesni aes des rc2 sha2 sha1 md4 md5 mgf1 random nonce x509
revocation constra
ints acert pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt fips-prf gmp curve25519
chapoly x
cbc cmac hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default farp stroke vici updown eap-
identity ea
p-sim eap-aka eap-aka-3gpp eap-aka-3gpp2 eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-
tls eap-ttls eap
-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp led duplicheck unity counters
Listening IP addresses:192.168.222.222
Connections:
strong_IPsec:  192.168.222.222...11.11.11.11  IKEv1
strong_IPsec:   local:  [22.22.22.22] uses pre-shared key authentication
strong_IPsec:   remote: [11.11.11.11] uses pre-shared key authentication
strong_IPsec:   child:  192.168.222.0/24 === 192.168.200.0/24 TUNNEL
Routed Connections:
strong_IPsec{1}:  ROUTED, TUNNEL, reqid 1
strong_IPsec{1}:   192.168.222.0/24 === 192.168.200.0/24
Security Associations (0 up, 1 connecting):
strong_IPsec[1]: CONNECTING, 192.168.222.222[%any]...11.11.11.11[%any]
strong_IPsec[1]: IKEv1 SPIs: c3090f6512ec6b7d_i* 0000000000000000_r
strong_IPsec[1]: Tasks queued: QUICK_MODE QUICK_MODE
strong_IPsec[1]: Tasks active: ISAKMP_VENDOR ISAKMP_CERT_PRE MAIN_MODE ISAKMP_CERT_POST
ISAKMP_NATD
Ping the server with IPsec client installed in VPC 2 from the VPC 1.
ping 192.168.222.222
PING 192.168.222.222 (192.168.222.222) 56(84) bytes of data.
64 bytes from 192.168.222.222: icmp_seq=1 ttl=62 time=3.07 ms
64 bytes from 192.168.222.222: icmp_seq=2 ttl=62 time=3.06 ms
64 bytes from 192.168.222.222: icmp_seq=3 ttl=62 time=3.98 ms
64 bytes from 192.168.222.222: icmp_seq=4 ttl=62 time=3.04 ms
64 bytes from 192.168.222.222: icmp_seq=5 ttl=62 time=3.11 ms
64 bytes from 192.168.222.222: icmp_seq=6 ttl=62 time=3.71 ms
```

2.8 Appendixes

2.8.1 Configuration Guide for Connecting an H3C-SecPath Firewall (V7) to Huawei Cloud

Huawei Cloud Configuration Information

VPN gateway IP address: 11.11.11.11

Local Subnet: **192.168.10.0/24,192.168.20.0/24**

Remote Gateway: **22.22.22.22**

Remote Subnet: **172.16.10.0/24,172.16.20.0/24,172.16.30.0/24**

Negotiation policy details:

Phase 1 policy (**IKE Policy**)

Authentication Algorithm: **SHA2-256**

Encryption Algorithm: **AES-128**

Version: **v2**

DH Algorithm: **Group14**

Lifetime (s): **86400**

Phase 2 policy (**IPsec Policy**)

Transfer Protocol: **ESP**

Authentication Algorithm: **SHA2-256**

Encryption Algorithm: **AES-128**

PFS: **DH group14**

Lifetime (s): **86400**

Customer-Side Device Networking and Basic Settings Assumptions

1. Assume that the basic networking configuration on the customer side is as follows:
   - Intranet interface: GigabitEthernet1/0/0 belongs to the Trust zone. The interface IP address is 10.0.0.1/30.
   - The subnets for encryption transmission are 172.16.10.0/24, 172.16.20.0/24, and 172.16.30.0/24, and they belong to the Trust zone.
   - Extranet interface: GigabitEthernet1/0/1 belongs to the Untrust zone. The interface IP address is 22.22.22.22/24.
   - Default route: Set destination to 0.0.0.0/0, outbound interface to GE1/0/1, and the next hop to 22.22.22.1.
   - Security policy: For the access from the Trust zone to the Untrust zone, set the source address, destination address, and protocol to any, and set the action to permit.
   - NAT policy: The source address is an intranet CIDR block, the destination address is ANY, and the action is Easy IP. That is, the intranet CIDR block is translated into the IP address of the interface.
2. The basic settings commands are as follows:

```
interface GigabitEthernet1/0/0
ip address 10.0.0.1 255.255.255.252
#
interface GigabitEthernet1/0/1
ip address 22.22.22.22 255.255.255.0
#
ip route-static 0.0.0.0 0 GigabitEthernet1/0/1 22.22.22.1
ip route-static 172.16.10.0 255.255.255.0 0 GigabitEthernet1/0/0 10.0.0.2
ip route-static 172.16.20.0 255.255.255.0 0 GigabitEthernet1/0/0 10.0.0.2
ip route-static 172.16.30.0 255.255.255.0 0 GigabitEthernet1/0/0 10.0.0.2
#
security-zone name Trust
```



```
import interface GigabitEthernet1/0/0
#
security-zone name Untrust
import interface GigabitEthernet1/0/1
#
security-policy ip
rule 0 name Policy-Internet
  action pass
  logging enable
  counting enable
  source-zone Trust
  destination-zone Untrust
#
object-group ip address Customer-subnet172.16.10.0/24
0 network subnet 172.16.10.0 255.255.255.0
#
object-group ip address Customer-subnet172.16.20.0/24
0 network subnet 172.16.20.0 255.255.255.0
#
object-group ip address Customer-subnet172.16.30.0/24
0 network subnet 172.16.30.0 255.255.255.0
#
nat policy
rule name Snat_Internet
  source-ip Customer-subnet172.16.10.0/24
  source-ip Customer-subnet172.16.20.0/24
  source-ip Customer-subnet172.16.30.0/24
  outbound-interface GigabitEthernet1/0/1
  action easy-ip port-preserved
```

IPsec Configuration Guidelines

1. The procedure for configuring the VPN on the web page is as follows:

   Log in to the web management page of the device and choose **VPN** > **IPsec** in the navigation pane.

   a. Configure an IKE proposal. Select the IKE proposal, and set the authentication mode, authentication algorithm, encryption algorithm, DH, and lifetime to be the same as those configured on Huawei Cloud.

   b. Configure an IPsec policy.

      In the basic settings area, set the role to peer/branch node, IP address type to IPv4, interface to extranet interface, local IP address to the corresponding public IP address, and peer IP address to the IP address of the Huawei Cloud gateway.

      In the IKE policy, configure the same negotiation mode and pre-shared key (PSK) as Huawei. Use the created IKE proposal. Set the local ID and peer ID to IPv4 addresses and enter the corresponding public IP address.

      The source address of the protected data flow is the local private CIDR block, and the destination address is the private CIDR block on Huawei Cloud.

      In advanced settings of IPsec parameters, the encapsulation mode, security protocol, authentication algorithm, encryption algorithm, PFS, and TTL must be the same as those configured on Huawei Cloud. You are advised to enable DPD.

   c. Configure security policies. Add security policies to allow communications between the customer private CIDR block and Huawei Cloud private CIDR block. Set the service to ANY and action to pass. Pin the two security policies on top.

d. Configure a NAT Policy. Add a NAT rule in which the source address is the customer intranet CIDR block and the destination address is the Huawei Cloud private CIDR block and the action is no-nat. Pin the rule on top.

CAUTION

- Add the mutual access rule between the local public IP address and the Huawei Cloud gateway IP address to the security policy. The protocol is UDP 500, UDP 4500, ESP, and AH. This ensures that the negotiation flow and encrypted flow data can be normally transmitted.
- Ensure that the negotiation traffic from the local public IP address to Huawei Cloud is not forwarded through NAT.
- Ensure that the route of the destination subnet is destined for the next hop of the public network outbound interface.
- Set the CIDR block of the data flow to be encrypted to the actual IP address and mask. Do not invoke the address object.
- If the customer network has multiple outbound interfaces, when the customer accesses the Huawei Cloud VPN gateway or private CIDR block, ensure that traffic is transmitted via the public network outbound interface. Use the static route configuration to select the appropriate outbound interface.

2. Command configuration description:

   # Add address sets.

```
object-group ip address HWCloud_subnet192.168.10.0/24
0 network subnet 192.168.10.0 255.255.255.0
#
object-group ip address HWCloud_subnet192.168.20.0/24
0 network subnet 192.168.20.0 255.255.255.0
```

   # Configure a phase-1 proposal. The algorithm details are the same as those of Huawei Cloud.

```
ikev2 proposal 100
  encryption aes-cbc-128
  integrity sha256
  dh group14
  prf sha256
```

   # Configure the same PSKs at both ends.

```
ikev2 keychain IPsec-KEY
  peer keypeername
    address 11.11.11.11 255.255.255.255
    pre-shared-key local plaintext ******
    pre-shared-key remote plaintext ******
```

   # Configure the IKEv2 profile, set the authentication method to PSK, and configure **local address** and **remote identity address**.

```
ikev2 profile IKE-PROFILE
  authentication-method local pre-share
  authentication-method remote pre-share
  keychain IPsec-KEY
  identity local address 22.22.22.22
  match local address 22.22.22.22
  match remote identity address 11.11.11.11 255.255.255.255
  sa duration 86400
```

   # Configure the IKE policy, which is similar to the IKE peer configuration. Invoke the IKE proposal and associate it with the interface IP address.

```
ikev2 policy IKE-PEER
  proposal 100
  match local address 22.22.22.22
```

Configure interesting traffic.

```
acl advanced 3999
  rule 0 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
  rule 1 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
  rule 2 permit ip source 172.16.30.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
  rule 4 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
  rule 5 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
  rule 6 permit ip source 172.16.30.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
```

Configure a phase-2 proposal.

```
IPsec transform-set IPsec-PH2
  encapsulation-mode tunnel
  esp authentication-algorithm sha256
  esp encryption-algorithm aes-cbc-128
  pfs dh-group14
```

Configure an IPsec policy by configuring the interesting traffic and phase-2 proposal.

```
IPsec policy IPsec-HW 1 isakmp
  transform-set IPsec-PH2
  security acl 3999
  local-address 22.22.22.22
  remote-address 11.11.11.11
  ikev2-profile IKE-PROFILE
  sa duration time-based 3600
```

Bind the IPsec policy to the negotiation interface.

```
interface GigabitEthernet1/0/1
  ip address 22.22.22.22 255.255.255.0
  tcp mss 1300
  IPsec apply policy IPsec-HW
```

Configure security policies to permit data communications between private networks at both ends and traffic between public IP addresses.

```
security-policy ip
rule 1 name IPsec-OUT
 action pass
 logging enable
 counting enable
 source-zone Trust
 destination-zone Untrust
 source-ip Customer-subnet172.16.10.0/24
 source-ip Customer-subnet172.16.20.0/24
 source-ip Customer-subnet172.16.30.0/24
 destination-ip HWCloud_subnet192.168.10.0/24
 destination-ip HWCloud_subnet192.168.20.0/24
rule 2 name IPsec-IN
 action pass
 logging enable
 counting enable
 source-zone Untrust
 destination-zone Trust
 source-ip HWCloud_subnet192.168.10.0/24
 source-ip HWCloud_subnet192.168.20.0/24
 destination-ip Customer-subnet172.16.10.0/24
 destination-ip Customer-subnet172.16.20.0/24
 destination-ip Customer-subnet172.16.30.0/24
rule 3 name IPsec-NEG-pass
 action pass
 logging enable
 counting enable
 source-ip 11.11.11.11 255.255.255.255
 source-ip 22.22.22.22 255.255.255.255
 destination-ip 11.11.11.11 255.255.255.255
 destination-ip 22.22.22.22 255.255.255.255
```



```
rule 0 name Policy-Internet
...
```

Configure a NAT policy in which **action** is set to **no-nat** to ensure that the local subnets can access the Huawei Cloud subnets.

```
nat policy
rule name IPsec_NONAT
  source-ip Customer-subnet172.16.10.0/24
  source-ip Customer-subnet172.16.20.0/24
  source-ip Customer-subnet172.16.30.0/24
  destination-ip HWCloud_subnet192.168.10.0/24
  destination-ip HWCloud_subnet192.168.20.0/24
  outbound-interface GigabitEthernet1/0/1
  action no-nat
rule name Snat_Internet
...
```

Configure route. The route for accessing the Huawei Cloud subnet is routed out of the public network interface.

```
ip route-static 0.0.0.0 0 GigabitEthernet1/0/1 B.B.B.1
...
```

3. Description of differentiated configurations when IKEv1 is used for negotiation:

   #If IKEv1 is used, the algorithms are as follows.

   ```
   ike proposal 100
      authentication-algorithm sha256
      encryption-algorithm aes-cbc-128
      authentication-method pre-share
      dh group14
      sa duration 86400
   ```

   #If IKEv1 is used, run the following commands to configure the PSK for IKE negotiation:

   ```
   ike keychain IPsec-KEY
      pre-shared-key address 11.11.11.11 255.255.255.255 key simple *******
   ```

   # If IKEv1 is used, **exchange-mode** is added, the phase-1 proposal is directly invoked, and you do not need to configure the IKE policy separately.

   ```
   ike profile IKE-PROFILE
      keychain IPsec-KEY
      local-identity address 22.22.22.22
      exchange-mode main     //aggressive
      dpd interval 3 periodic
      match remote identity address 11.11.11.11 255.255.255.255
      match local address 22.22.22.22
      proposal 100
   ```

Function Verification

After a VPN connection is configured, the cloud does not automatically trigger tunnel establishment. Instead, data flows are required to trigger negotiation.

Triggering method: Use data flows between private networks to trigger a VPN connection. For example, use a host on 192.168.10.0/24 to ping a host on 172.16.10.0/24, or the other way around.

CAUTION

Tunnel negotiation is not triggered when a private IP address pings the IP address of the peer public gateway. For example, when a host 172.16.10.0/24 pings 11.11.11.11, tunnel establishment is not triggered.

2.8.2 Configuration Guide for Interconnecting an HW-USG Firewall (V5) with Huawei Cloud

Huawei Cloud Configuration Information

VPN gateway IP address: 11.11.11.11

Local Subnet: **192.168.10.0/24,192.168.20.0/24**

Remote Gateway: **22.22.22.22**

Remote Subnet: **172.16.10.0/24,172.16.20.0/24,172.16.30.0/24**

Negotiation policy details:

Phase 1 policy (**IKE Policy**)

Authentication Algorithm: **SHA2-256**

Encryption Algorithm: **AES-128**

Version: **v2**

DH Algorithm: **Group14**

Lifetime (s): **86400**

Phase 2 policy (**IPsec Policy**)

Transfer Protocol: **ESP**

Authentication Algorithm: **SHA2-256**

Encryption Algorithm: **AES-128**

PFS: **DH group14**

Lifetime (s): **86400**

Customer-Side Device Networking and Basic Settings Assumptions

1. Assume that the basic networking configuration on the customer side is as follows:

Intranet interface: GigabitEthernet1/0/0 belongs to the Trust zone. The interface IP address is 10.0.0.1/30.

The subnets for encryption transmission are 172.16.10.0/24, 172.16.20.0/24, and 172.16.30.0/24, and they belong to the Trust zone.

Extranet interface: GigabitEthernet1/0/1 belongs to the Untrust zone. The interface IP address is 22.22.22.22/24.

Default route: Set destination to 0.0.0.0/0, outbound interface to GE1/0/1, and the next hop to 22.22.22.1.

Security policy: For the access from the Trust zone to the Untrust zone, set the source address, destination address, and protocol to any, and set the action to permit.

NAT policy: The source address is an intranet CIDR block, the destination address is ANY, and the action is Easy IP. That is, the intranet CIDR block is translated into the IP address of the interface.

2. The basic settings commands are as follows:

```
interface GigabitEthernet1/0/0
ip address 10.0.0.1 255.255.255.252
#
interface GigabitEthernet1/0/1
ip address 22.22.22.22 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 22.22.22.1
ip route-static 172.16.10.0 255.255.255.0 10.0.0.2
ip route-static 172.16.20.0 255.255.255.0 10.0.0.2
ip route-static 172.16.30.0 255.255.255.0 10.0.0.2
#
firewall zone trust
set priority 85
import interface GigabitEthernet1/0/0
#
firewall zone untrust
set priority 5
import interface GigabitEthernet1/0/1
#
ip address-set Customer-subnet172.16.10.0/24 type object
address 0 172.16.10.0 mask 24
#
ip address-set Customer-subnet172.16.20.0/24 type object
address 0 172.16.20.0 mask 24
#
ip address-set Customer-subnet172.16.30.0/24 type object
address 0 172.16.30.0 mask 24
#
security-policy
rule name Policy-Internet
  policy logging
  session logging
  source-zone trust
  destination-zone untrust
  action permit
#
nat-policy
rule name Snat_Internet
  source-zone trust
  egress-interface GigabitEthernet1/0/1
  action nat easy-ip
```

IPsec Configuration Guidelines

1. The procedure for configuring the VPN on the web page is as follows:

   Log in to the web management page, choose **Network** > **IPsec**, and create an IPsec policy.

   a. Basic settings: Configure a naming policy. Set the outbound interface to the local interface, local address to the public IP address of the outbound interface, peer address to the IP address of the Huawei Cloud VPN gateway, authentication mode to pre-shared key, key information to be the same as that configured on Huawei Cloud, and local and peer IDs to IP addresses.

   b. To-be-encrypted data flow: Create ACL rules. The source address is the customer subnets, and the destination address is the Huawei Cloud subnets. Enter multiple subnets separately. The number of entries is the product of the number of subnets at both ends. Set the protocol to any and the action to permit.

c. Security proposal: The IKE and IPsec parameter settings, including the IKE version must be the same as those on Huawei Cloud. You are advised to enable periodic DPD.

d. Security policy: Add two security policies to allow communications between the customer private CIDR block and Huawei Cloud private CIDR block. Set the service to ANY and action to permit. Pin the two security policies on top.

e. NAT Policy. Add a NAT rule in which the source address is the customer intranet CIDR block and the destination address is the Huawei Cloud private CIDR block and the action is no-nat. Pin the rule on top.

⚠ CAUTION

- Add the mutual access rule between the local public IP address and the Huawei Cloud gateway IP address to the security policy. The protocol is UDP 500, UDP 4500, ESP, and AH. This ensures that the negotiation flow and encrypted flow data can be normally transmitted.
- Ensure that the negotiation traffic from the local public IP address to Huawei Cloud is not forwarded through NAT.
- Ensure that the route of the destination subnet is destined for the next hop of the public network outbound interface.
- Set the CIDR block of the data flow to be encrypted to the actual IP address and mask. Do not invoke the address object.
- If the customer network has multiple outbound interfaces, when the customer accesses the Huawei Cloud VPN gateway or private CIDR block, ensure that traffic is transmitted via the public network outbound interface. Use the static route configuration to select the appropriate outbound interface.

2. Command configuration description:

   # Add address sets.

```
ip address-set HWCloud_subnet192.168.10.0/24 type object
address 0 192.168.10.0 mask 24
#
ip address-set HWCloud_subnet192.168.20.0/24 type object
address 0 192.168.20.0 mask 24
```

   # Configure the IKE proposal. The configuration methods of IKEv1 and IKEv2 are the same. IKEv1 uses authentication and encryption, and IKEv2 uses encryption, integrity, and PRF.

```
ike proposal 100
authentication-algorithm sha2-256
encryption-algorithm aes-128
authentication-method pre-share
integrity-algorithm hmac-sha2-256
prf hmac-sha2-256
dh group14
sa duration 86400
```

   #Set IKE peer version to IKEv2, and configure the IKE proposal. (If you set IKE peer version to IKEv1, **exchange-mode** needs to be configured.)

```
ike peer IKE-PEER
undo version 1
pre-shared-key ******
```



```
ike-proposal 100
remote-address 11.11.11.11
dpd type periodic
```

Configure interesting traffic.

```
acl number 3999
rule 0 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
rule 1 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
rule 2 permit ip source 172.16.30.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
rule 4 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
rule 5 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
rule 6 permit ip source 172.16.30.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
```

Configure a phase-2 proposal.

```
IPsec proposal IPsec-PH2
transform esp
encapsulation-mode tunnel
esp authentication-algorithm sha2-256
esp encryption-algorithm aes-128
```

#Configure the IPsec policy by specifying the IKE peer, IPsec proposal, and ACL. Set the same PFS as that on Huawei Cloud.

```
IPsec policy IPsec-HW 1 isakmp
proposal IPsec-PH2
security acl 3999
ike-peer IKE-PEER
tunnel local 22.22.22.22
pfs dh-group14
sa duration time-based 3600
```

Set **tcp-mss** and it will take effect globally.

```
firewall tcp-mss 1300
# Bind the IPsec policy to an interface.
interface GigabitEthernet1/0/1
ip address B.B.B.Y 255.255.255.0
IPsec apply policy IPsec-HW
#
security-policy
rule name IPsec-OUT
policy logging
session logging
source-zone trust
destination-zone untrust
source-address address-set Customer-subnet172.16.10.0/24
source-address address-set Customer-subnet172.16.20.0/24
source-address address-set Customer-subnet172.16.30.0/24
destination-address address-set HWCloud_subnet192.168.10.0/24
destination-address address-set HWCloud_subnet192.168.20.0/24
action permit
rule name IPsec-IN
policy logging
session logging
source-zone untrust
destination-zone trust
source-address address-set HWCloud_subnet192.168.10.0/24
source-address address-set HWCloud_subnet192.168.20.0/24
destination-address address-set Customer-subnet172.16.10.0/24
destination-address address-set Customer-subnet172.16.20.0/24
destination-address address-set Customer-subnet172.16.30.0/24
action permit
rule name IPsec-NEG-pass
logging enable
counting enable
source-ip 11.11.11.11 255.255.255.255
source-ip 22.22.22.22 255.255.255.255
destination-ip 11.11.11.11 255.255.255.255
destination-ip 22.22.22.22 255.255.255.255
action permit
rule name Policy-Internet
```



```
...
#
nat policy
rule name IPsec_NONAT
description IPsec_NONAT
source-zone trust
destination-zone untrust
source-address address-set Customer-subnet172.16.10.0/24
source-address address-set Customer-subnet172.16.20.0/24
source-address address-set Customer-subnet172.16.30.0/24
destination-address address-set HWCloud_subnet192.168.10.0/24
destination-address address-set HWCloud_subnet192.168.20.0/24
action no-nat
rule name Snat_Internet
...
```

Configure route. The route for accessing the Huawei Cloud subnet is routed out of the public network interface.

```
ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet1/0/1 22.22.22.1
```

Function Verification

After a VPN connection is configured, the cloud does not automatically trigger tunnel establishment. Instead, data flows are required to trigger negotiation.

Triggering method: Use data flows between private networks to trigger a VPN connection. For example, use a host on 192.168.10.0/24 to ping a host on 172.16.10.0/24, or the other way around.

CAUTION

Tunnel negotiation is not triggered when a private IP address pings the IP address of the peer public gateway. For example, when a host 172.16.10.0/24 pings 11.11.11.11, tunnel establishment is not triggered.

2.8.3 Configuration Guide for Connecting a Hillstone-G Firewall (V5.5) to Huawei Cloud

Huawei Cloud Configuration Information

VPN gateway IP address: 11.11.11.11

Local Subnet: **192.168.10.0/24,192.168.20.0/24**

Remote Gateway: **22.22.22.22**

Remote Subnet: **172.16.10.0/24,172.16.20.0/24,172.16.30.0/24**

Negotiation policy details:

Phase 1 policy (**IKE Policy**)

Authentication Algorithm: **SHA2-256**

Encryption Algorithm: **AES-128**

Version: **v1**

DH Algorithm: **Group14**

Lifetime (s): **86400**

Exchange-mode: main

Phase 2 policy (**IPsec Policy**)

Transfer Protocol: **ESP**

Authentication Algorithm: **SHA2-256**

Encryption Algorithm: **AES-128**

PFS: **DH group14**

Lifetime (s): **86400**

Customer-Side Device Networking and Basic Settings Assumptions

Intranet interface: ethnet0/0 belongs to the Trust zone. The interface IP address is b.b.b.1/24.

Extranet interface: ethnet0/1 belongs to the Untrust zone. The interface IP address is B.B.B.Y/24.

Default route: Set destination to 0.0.0.0/0, outbound interface to ethnet0/1, and the next hop to the gateway IP address, such as B.B.B.1.

Security policy: For the access from the Trust zone to the Untrust zone, set the source address, destination address, and protocol to any, and set the action to permit.

NAT policy: The source address is intranet CIDR block. The destination address is ANY. Translate the intranet CIDR block to the IP address of the outbound interface.

VPN Configuration Procedure

Log in to the web management page of the device. In the navigation pane, choose **VPN** > **IPsec VPN**.

1. Configure the P1 proposal: Enter the proposal name, set the authentication mode to Pre-share, and configure parameters such as the authentication algorithm, encryption algorithm, and DH group. For details about the parameters, see **Huawei Cloud Configuration Information**.
2. Configure the phase-2 proposal. Specify parameters such as the proposal name, protocol, authentication algorithm, encryption algorithm, and PFS. For details about the parameters, see **Huawei Cloud Configuration Information**. Disable compression and TTL.
3. Configure the VPN peer list.
   a. Basic settings: Enter the name, select ethnet0/1, select the protocol standard (only V1 is supported), and configure the authentication mode. Set type to static IP, peer IP address to 11.11.11.11, the IP address of the Huawei Cloud VPN gateway, and local ID to IPv4 22.22.22.22, invoke the configured phase-1 proposal and enter the same PSK as that on Huawei Cloud.
   b. Advanced settings: Set connection type to bidirectional, enable NAT traversal, and enable DPD. Retain the default values of DPD interval and retry time, and disable the XAUTH server.

4. Configure the IKE VPN list.
   a. Basic settings:

      Peer: Use the existing configuration of the peer list.

      Tunnel: Enter the name, set mode to tunnel, invoke the P2 proposal, and set Proxy ID to manual. That is, configure interesting traffic in the format of IP address+mask. The number of configured entries is the product of the number of local subnets and the number of remote subnets.
   b. Advanced settings: Retain the default settings. You can enable VPN tunnel detection. The source address is the local private IP address and the destination address is the private IP address of Huawei Cloud. (Select an available address.)
5. Configure interfaces.
   a. In the navigation pane, choose security zone, and create a VPN security zone. Name it VPN, and set the type to layer-3 security zone.
   b. In the navigation pane, choose interface, and create a tunnel interface. Specify the interface name, number, and security zone. (Add the interface to the newly-created VPN security zone). Set IP address to static IP and do not specify IP information. Set tunnel type to IPsec VPN and bind the tunnel to the created IKE VPN list.
6. Security policy: Create the following security policies and pin them on top.
   a. Set source zone to trust, destination zone to VPN, service to any, and action to permit.
   b. Set source zone to VPN, destination zone to trust, service to any, and action to permit.
7. Set the destination of the route to the Huawei Cloud private network (192.168.10.0/24, 192.168.20.0/24), set the next hop to interface, and set the interface to the tunnel interface used by the VPN.

CAUTION

- Add the mutual access rule between the local public IP address and the Huawei Cloud gateway IP address to the security policy. The protocol is UDP 500, UDP 4500, ESP, and AH. This ensures that the negotiation flow and encrypted flow data can be normally transmitted.
- Set the CIDR block of the data flow to be encrypted (proxy ID) to the actual IP address and mask. Do not invoke the address sets.
- If the customer network has multiple outbound interfaces, when the customer accesses the Huawei Cloud VPN gateway or private CIDR block, ensure that traffic is transmitted via the public network outbound interface. Use the static route configuration to select the appropriate outbound interface.

Function Verification

After the VPN connection is configured, if active connection is selected for the Sangfor device, the Sangfor device initiates a negotiation. Huawei Cloud does not proactively trigger tunnel establishment.

Triggered by Huawei Cloud: Use data flows between private networks to trigger a VPN connection. For example, use a host on 192.168.10.0/24 to ping a host on 172.16.10.0/24, or the other way around.

CAUTION

Tunnel negotiation is not triggered when a private IP address pings the IP address of the peer public gateway. For example, when a host 172.16.10.0/24 pings 11.11.11.11, tunnel establishment is not triggered.

2.8.4 Configuration Guide for Interconnecting Sangfor-SSL-M7.6 with Huawei Cloud

Huawei Cloud Configuration Information

VPN gateway IP address: 11.11.11.11

Local Subnet: **192.168.10.0/24,192.168.20.0/24**

Remote Gateway: **22.22.22.22**

Remote Subnet: **172.16.10.0/24,172.16.20.0/24,172.16.30.0/24**

Negotiation policy details:

Phase 1 policy (**IKE Policy**)

Authentication Algorithm: **SHA2-256**

Encryption Algorithm: **AES-128**

Version: **v1**

DH Algorithm: **Group14**

Lifetime (s): **86400**

Exchange-mode: main

Phase 2 policy (**IPsec Policy**)

Transfer Protocol: **ESP**

Authentication Algorithm: **SHA2-256**

Encryption Algorithm: **AES-128**

PFS: **DH group14**

Lifetime (s): **86400**

Customer-Side Device Networking and Basic Settings Assumptions

Deployment mode: gateway mode

Intranet interface: The IP address of the LAN interface is 192.168.10.1/24.

External interface: The IP address of line 1 (WAN1 interface) is 22.22.22.22/24.

Default route: The next hop is the gateway IP address of line 1, for example, 22.22.22.1.

Firewall rule: When the LAN accesses the WAN, set the source address, destination address, and service to any, and the action to permit.

CIDR block configuration for Internet access through proxy: Set the source interface to LAN, source address to the intranet CIDR block, the destination to interface WAN1, and the destination address to All IP. Translate All IP to the IP address of the destination interface.

VPN Configuration Procedure

Log in to the web management console of the device and choose **IPsec VPN** > **Third-Party Interconnection** on the console.

1. Security proposal: Configure a phase-2 proposal. Click Add. On the displayed tab page, specify the same name, protocol, authentication algorithm, and encryption algorithm as those on Huawei Cloud. For details, see **Huawei Cloud Configuration Information**.
2. Phase 1:
   a. Basic settings: Click Add on the right. On the tab page that is displayed, enter a name, set line to public network line 1, device address type to peer fixed IP address, fixed IP address to 11.11.11.11, authentication mode to PSK, and enter the PSK. Enable device and enable active connection.
   b. Advanced settings: Click advanced in the lower left corner of the basic page. On the tab page that is displayed, set parameters such as lifetime, supported mode, D-H group, authentication algorithm, and encryption algorithm to be the same as those on Huawei Cloud. Enable DPD and use the default values for interval and times.
   c. Special settings: When NAT traversal exists on Sangfor, only the aggressive mode can be used for interconnection. In addition, the Sangfor device does not support IKEv2. When selecting the aggressive mode, set the Sangfor ID to the IPv4 public IP address, that is, the public IP address after NAT.
3. Phase 2:
   a. Inbound policy: Click add. On the page that is displayed, enter the policy name, set source IP address type to subnet+mask, enter a Huawei Cloud private CIDR block (192.168.10.0/24, 192.168.20.0/24) at a time. Set service to all services and effective duration to all day. Enable this policy.
   b. Outbound policy: Click add. On the displayed tab page, enter the name, set source IP type to subnet+mask, and enter a local private CIDR block (172.16.10.0/24, 172.16.20.0/24, 172.16.30.0/24) at a time. The peer device invokes the configured phase-1 proposal. The lifecycle is the same as that of Huawei Cloud. Set service to all services and effective duration to all day. Enable this policy. For the security options, invoke the configured security proposal. Enable this policy and select Perfect Forward Secrecy (PFS).
   c. Special settings: After PFS is selected, the D-H group in phase 2 is the same as that in phase 1. If there are multiple subnets in the on-premises

data center, configure the peer device, security options, and PFS for each outbound policy.

4. Firewall rule settings: Add policies to allow mutual access between VPN and LAN. The services are all-tcp, all-udp, and ping, respectively.

CAUTION

- Add the mutual access rule between the local public IP address and the Huawei Cloud gateway IP address to the security policy. The protocol is UDP 500, UDP 4500, ESP, and AH. This ensures that the negotiation flow and encrypted flow data can be normally transmitted.
- Set the CIDR block of the data flow to be encrypted to the actual IP address and mask. Do not invoke the address object.
- If the customer network has multiple outbound interfaces, when the customer accesses the Huawei Cloud VPN gateway or private CIDR block, ensure that traffic is transmitted via the public network outbound interface. Use the static route configuration to select the appropriate outbound interface.

Function Verification

After the VPN connection is configured, if active connection is selected for the Sangfor device, the Sangfor device initiates a negotiation. Huawei Cloud does not proactively trigger tunnel establishment.

Triggered by Huawei Cloud: Use data flows between private networks to trigger a VPN connection. For example, use a host on 192.168.10.0/24 to ping a host on 172.16.10.0/24, or the other way around.

CAUTION

Tunnel negotiation is not triggered when a private IP address pings the IP address of the peer public gateway. For example, when a host 172.16.10.0/24 pings 11.11.11.11, tunnel establishment is not triggered.