Virtual Private Network

Administrator Guide

Issue 01

Date 2026-07-09

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

1 S2C Enterprise Edition VPN

1.1 Interconnection with an AR Router of Huawei (Active-Active Connections)

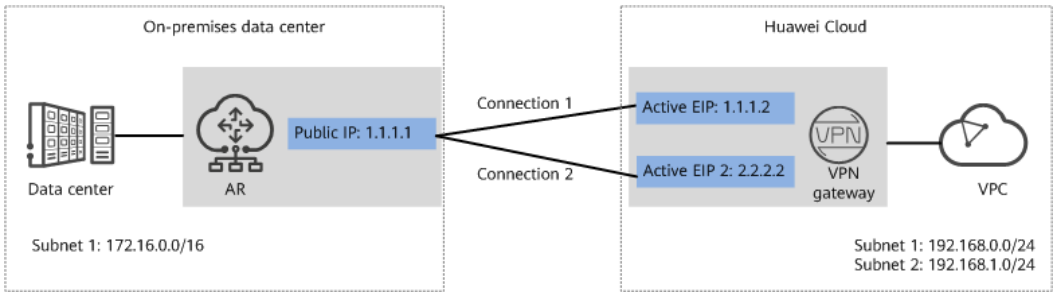
1.1.1 Static Routing Mode

1.1.1.1 Operation Guide

Scenario

Figure 1-1 shows the typical networking where a VPN gateway connects to an access router (AR) of Huawei 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 needs to be 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 Value for the AR Router	Example Value for the Huawei Cloud Side
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 addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 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

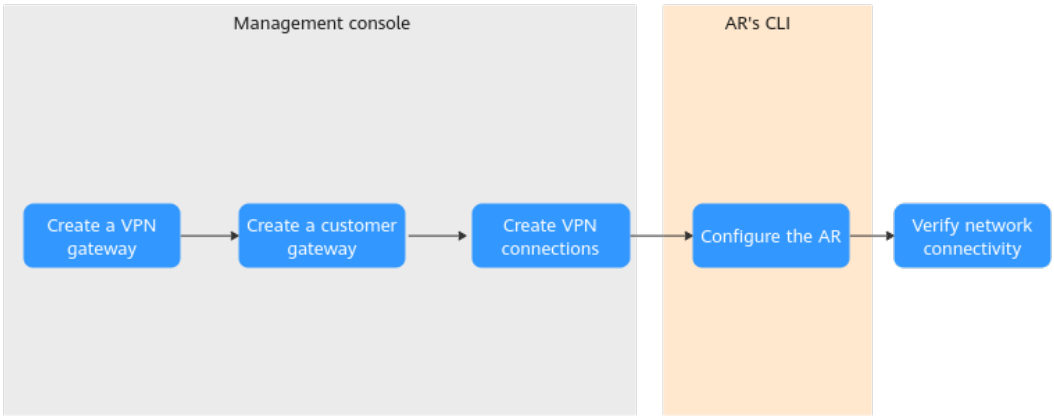


Table 1-2 Operation process description

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 connections.**	• Create two VPN connections between the VPN gateway (active EIP and active EIP 2) and the customer gateway. • The PSK, IKE policy, and IPsec policy settings of connections must be the same as those of the AR router.
4	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 configured on the VPN console.

No.	Configuration Interface	Step	Description
5	-	Verify network connectivity.	Run the **ping** command to verify network connectivity.

1.1.1.2 Configuration on the Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted.

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

Table 1-3 Parameters for creating a VPN gateway

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512

Parameter	Description	Value
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

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

Table 1-4 Parameters for creating a customer gateway

Parameter	Description	Value
Name	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
BGP ASN	ASN of your on-premises data center or private network. The value must be different from the BGP ASN of the VPN gateway.	65000

Step 5 Configure VPN connections.

In this scenario, create a VPN connection 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 **Create VPN Connection**.

1. Create VPN connections.

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

Table 1-5 Parameters for creating VPN connections

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, health check, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets. The VPN gateway can automatically perform NQA detection on the peer interface address that has been configured on the customer gateway.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.1.1.3 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 169.254.70.2 255.255.255.252
[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 169.254.71.2 255.255.255.252
[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 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.2
[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 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.2
[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

1.1.1.4 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.

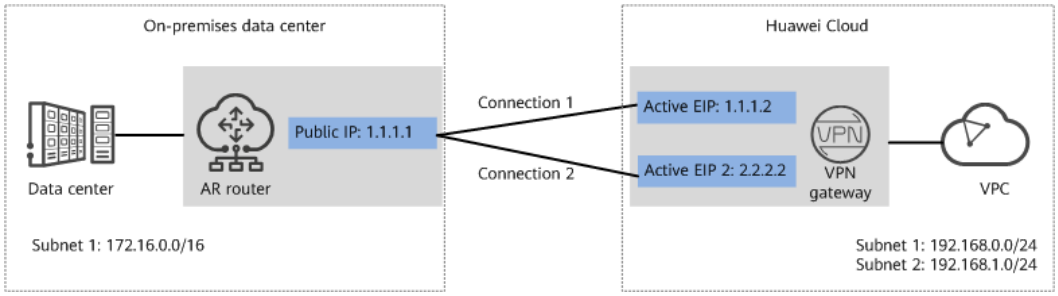
1.1.2 BGP Routing Mode

1.1.2.1 Operation Guide

Scenario

Figure 1-3 shows the typical networking where a VPN gateway connects to the Huawei AR router in an on-premises data center in BGP routing mode.

Figure 1-3 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 needs to be 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 1-6 Data plan

Category	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
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
	BGP ASN	64515	64512
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 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	

Category	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH group 14 • Transfer protocol: ESP • Lifetime (s): 3600	

Operation Process

Figure 1-4 shows the process of using the VPN service to enable communication between the data center and VPC.

Figure 1-4 Operation process

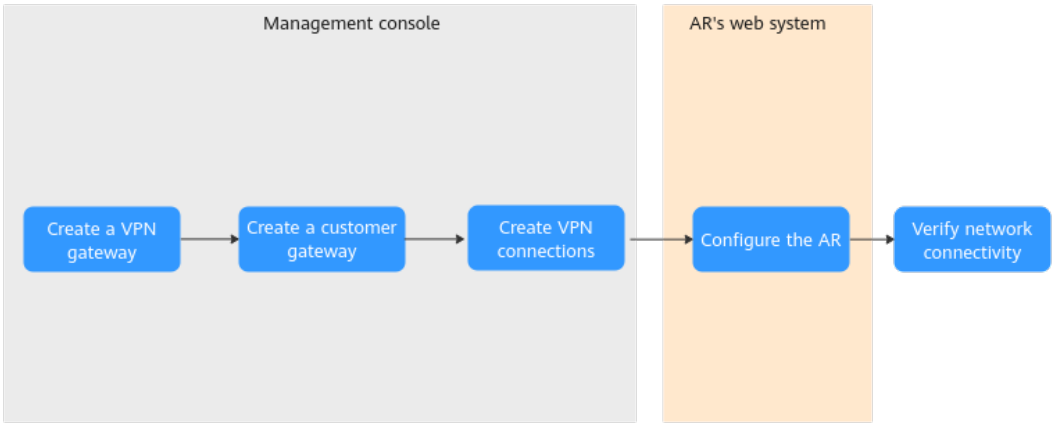


Table 1-7 Operation process description

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.

No.	Configuration Interface	Step	Description
3		**Create VPN connections.**	• Create two VPN connections between the VPN gateway (active EIP and active EIP 2) and the customer gateway. • It is recommended that the connection mode, PSK, IKE policy, and IPsec policy settings of connection 2 be the same as those of connection 1.
4	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 configured on the VPN console.
5	-	**Verify network connectivity.**	Run the **ping** command to verify network connectivity.

1.1.2.2 Configuration on the Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-8 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-8 Key parameters for creating a VPN gateway

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-9 describes the parameters for creating a customer gateway.

Table 1-9 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar

Parameter	Description	Value
Identifier	Select **IP Address**, and enter the public IP address of the AR router.	IP Address 1.1.1.1
BGP ASN	BGP AS number of the AR router.	65000

Step 5 Configure VPN connections.

In this scenario, create a VPN connection 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 **Create VPN Connection**.

1. Create VPN connections.

   Table 1-10 only describes the key parameters for creating VPN connections.

   Table 1-10 Parameters for creating VPN connections

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **BGP routing**.	BGP routing

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the AR router.	*Set parameters 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.1.2.3 Configuration on the AR Router

Prerequisites

- The uplink public network interface GE0/0/8 of the AR router has been configured. Assume that the public IP address of the interface is 1.1.1.1.
- The downlink private network interface GE0/0/1 of the AR router has been configured. Assume that the private IP address of the interface is 172.16.0.1.

Procedure

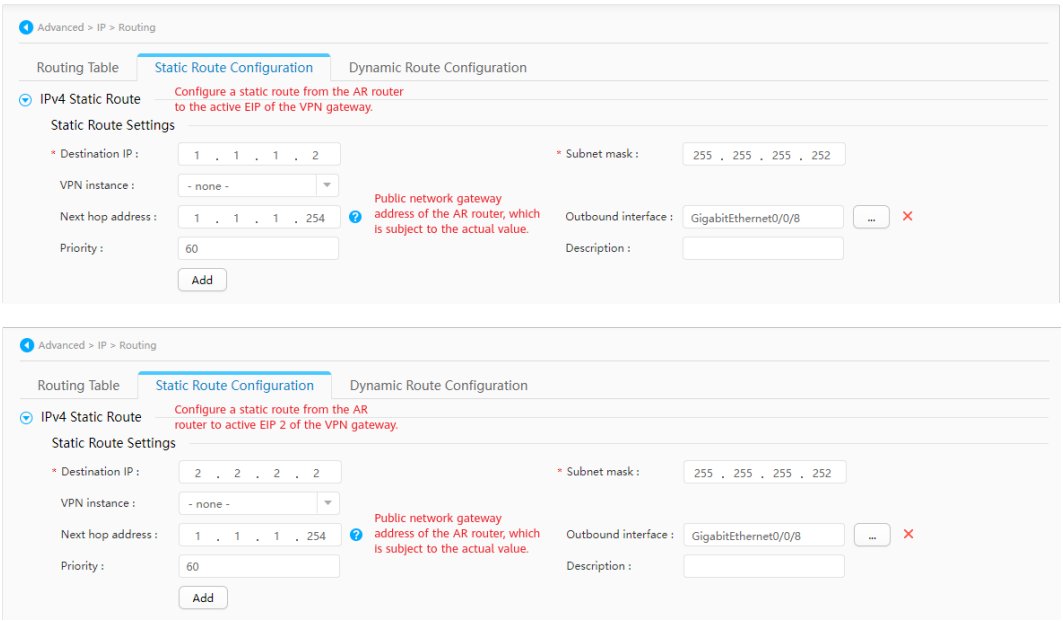
Step 1 Log in to the web system of the AR router.

An AR651 running V300R019C13SPC200 is used as an example. The web system may vary according to the device model and software version.

Step 2 Complete basic settings.

Choose **Advanced** > **IP** > **Routing** > **Static Route Configuration**. In the **IPv4 Static Route** area, configure static routes to the active EIP and active EIP 2 of the VPN gateway, and click **Add**. **Figure 1-5** shows the key parameter settings.

Figure 1-5 Configuring static routes

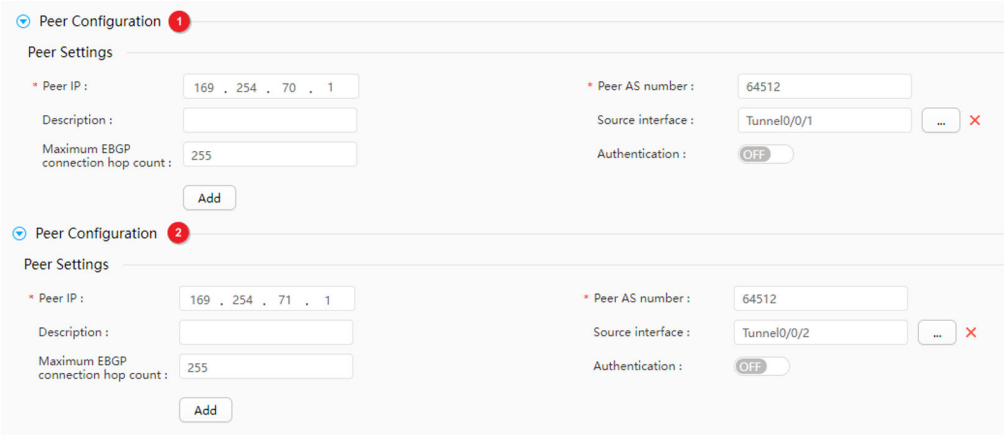


Step 3 Configure tunnel interfaces.

1. Choose **Advanced** > **Interface** > **Logical Interface**.
2. Configure two tunnel interfaces and click **Add**.

   Figure 1-6 shows the key parameter settings.

   Figure 1-6 Configuring tunnel interfaces



Step 4 Configure VPN connections.

1. Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**.
2. Configure the IKE and IPsec policies for the two tunnels, as shown in **Figure 1-7** and **Figure 1-8**.

   NOTE

   - When IKEv1 is used for IPsec negotiation, if the traffic hard lifetime is set to 0 on either device, both the local and remote devices disable the traffic timeout function.
   - When IKEv2 is used for IPsec negotiation, if the traffic hard lifetime is set to 0 on a device, this device disables the traffic timeout function.

Figure 1-7 Configuring VPN connection 1

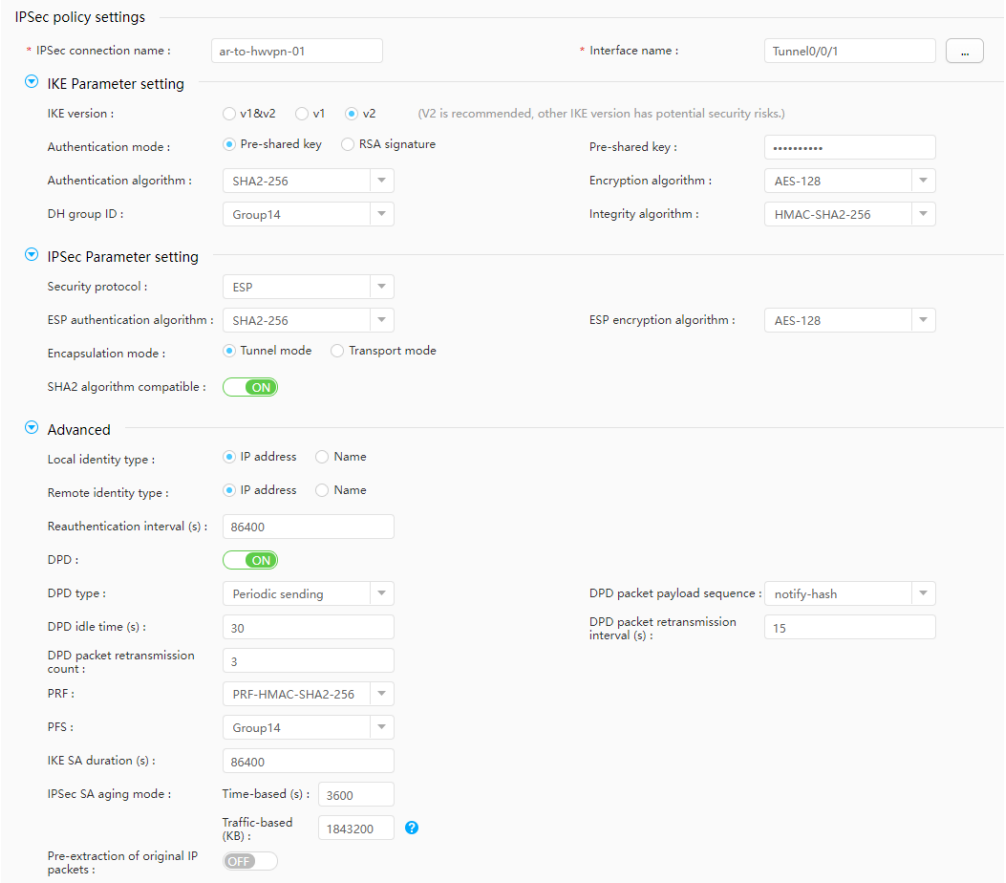
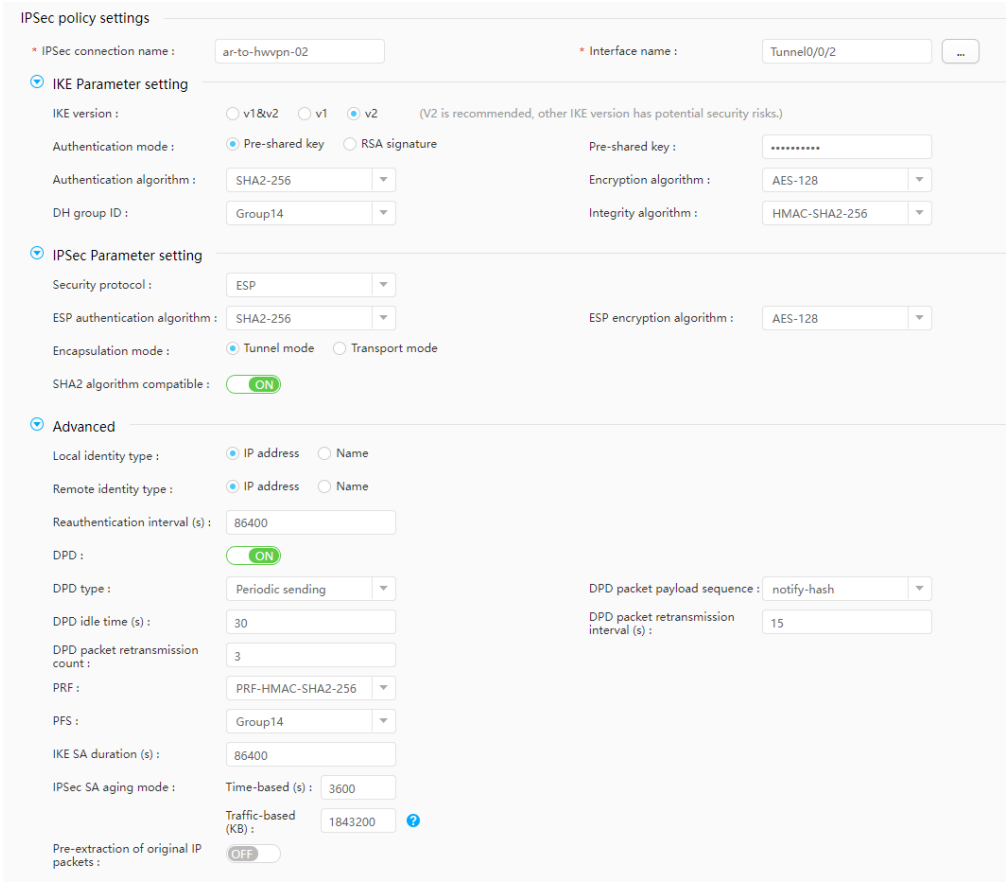


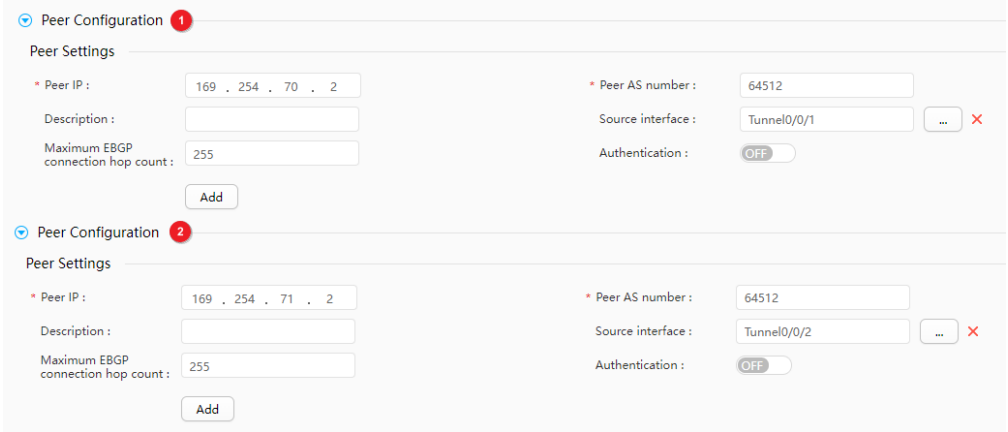
Figure 1-8 Configuring VPN connection 2



Step 5 Configure BGP.

1. Choose **Advanced** > **IP** > **Routing** > **Dynamic Route Configuration** > **BGP**.
2. Toggle on **Enable BGP**, set **AS Number** to the BGP ASN of the AR router, set **Router ID** to the gateway address of the downlink private network interface on the AR router, and click **Apply**.
3. Configure BGP peers, as shown in **Figure 1-9**.

Figure 1-9 Configuring BGP peers



4. In the **Route Import Configuration** area, set **Protocol type** to **Direct**.

----End

1.1.2.4 Verification

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

    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 Huawei Cloud VPC subnets can ping each other.

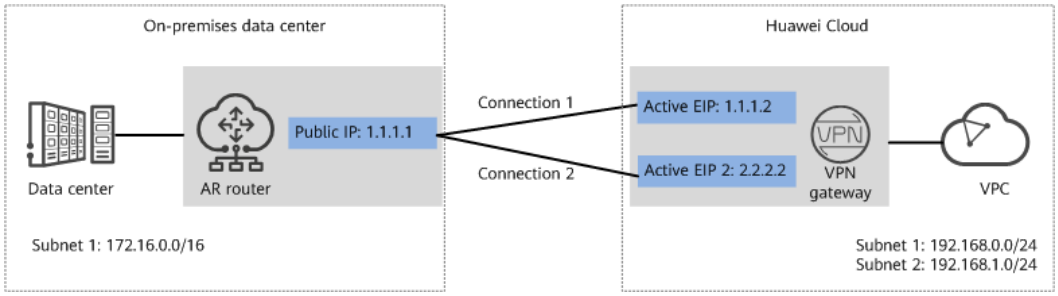
1.1.3 Policy-based Mode

1.1.3.1 Operation Guide

Scenario

Figure 1-10 shows the typical networking where a VPN gateway connects to the Huawei AR router in an on-premises data center in policy-based mode.

Figure 1-10 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 needs to be 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 1-11 Data plan

Category	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
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	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 1-11 shows the process of using the VPN service to enable communication between the data center and VPC.

Figure 1-11 Operation process

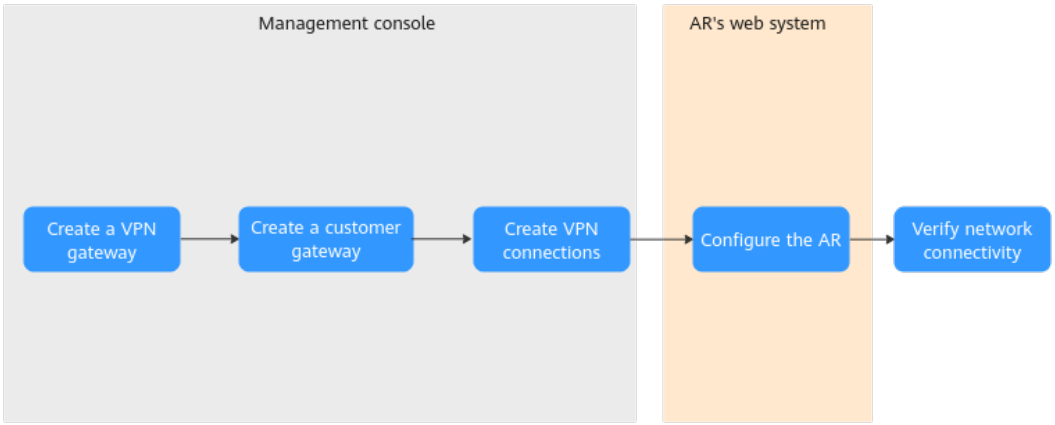


Table 1-12 Operation process description

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 connections.**	• Create two VPN connections between the VPN gateway (active EIP and active EIP 2) and the customer gateway. • It is recommended that the connection mode, PSK, IKE policy, and IPsec policy settings of connection 2 be the same as those of connection 1.
4	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 configured on the VPN console.
5	-	**Verify network connectivity.**	Run the **ping** command to verify network connectivity.

1.1.3.2 Configuration on the Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-13 only describes the key parameters for configuring a VPN gateway. For other parameters, use their default settings.

Table 1-13 Key parameters for creating a VPN gateway

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active-active

Parameter	Description	Value
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-14 describes the parameters for creating a customer gateway.

Table 1-14 Parameters for creating a customer gateway

Parameter	Description	Value
Name	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
BGP ASN	BGP AS number of the AR router.	65000

Step 5 Configure VPN connections.

In this scenario, create a VPN connection 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 **Create VPN Connection**.
2. Set parameters as prompted.

   The following table only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-15 Parameters for creating VPN connections

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2

Parameter	Description	Value
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Policy-based**.	Policy-based
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the health check, PSK, confirm PSK, and policies for the VPN gateway IP address of connection 1.	*Set parameters based on the site requirements.*
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy	A policy rule defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. – Source CIDR Block The source CIDR block must contain some local subnets. 0.0.0.0/0 indicates any address. – Destination CIDR Block The destination CIDR block must contain all customer subnets.	– Source CIDR block 1: 192.168.0.0/24 – Destination CIDR block 1: 172.16.0.0/16 – Source CIDR block 2: 192.168.1.0/24 – Destination CIDR block 2: 172.16.0.0/16

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** It is recommended that the configuration of connection 2 be the same as that of connection 1.	Enabled

----End

1.1.3.3 Configuration on the AR Router

Prerequisites

- The WAN interface GE0/0/8 on the AR router has been configured. Assume that the public IP address of the WAN interface is 1.1.1.1.
- The LAN interface GE0/0/1 on the AR router has been configured. Assume that the public IP address of the LAN interface is 172.16.0.1.

Procedure

Step 1 Log in to the web system of the AR router.

An AR651 running V300R019C13SPC200 is used as an example. The web system may vary according to the device model and software version.

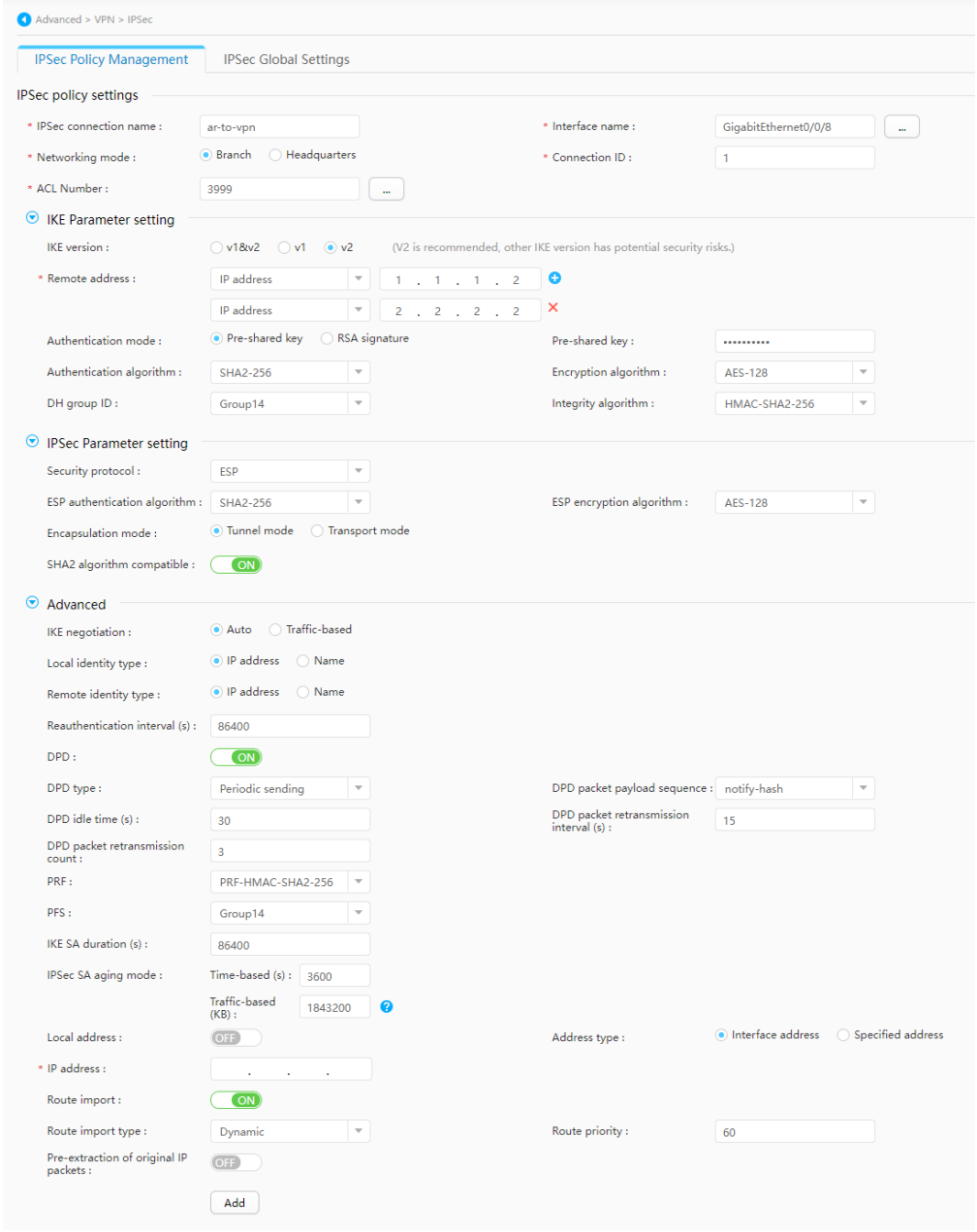
Step 2 Configure VPN connections.

1. Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**.
2. Configure the IKE and IPsec policies, as shown in **Figure 1-12**.

   NOTE

   - When IKEv1 is used for IPsec negotiation, if the traffic hard lifetime is set to 0 on either device, both the local and remote devices disable the traffic timeout function.
   - When IKEv2 is used for IPsec negotiation, if the traffic hard lifetime is set to 0 on a device, this device disables the traffic timeout function.
   - If the AR router uses a non-fixed IP address to connect to the VPN gateway, click **Advanced**, set **Local identity type** to **Name**, and enter the customer gateway identifier configured on the cloud in the **Local name** text box.

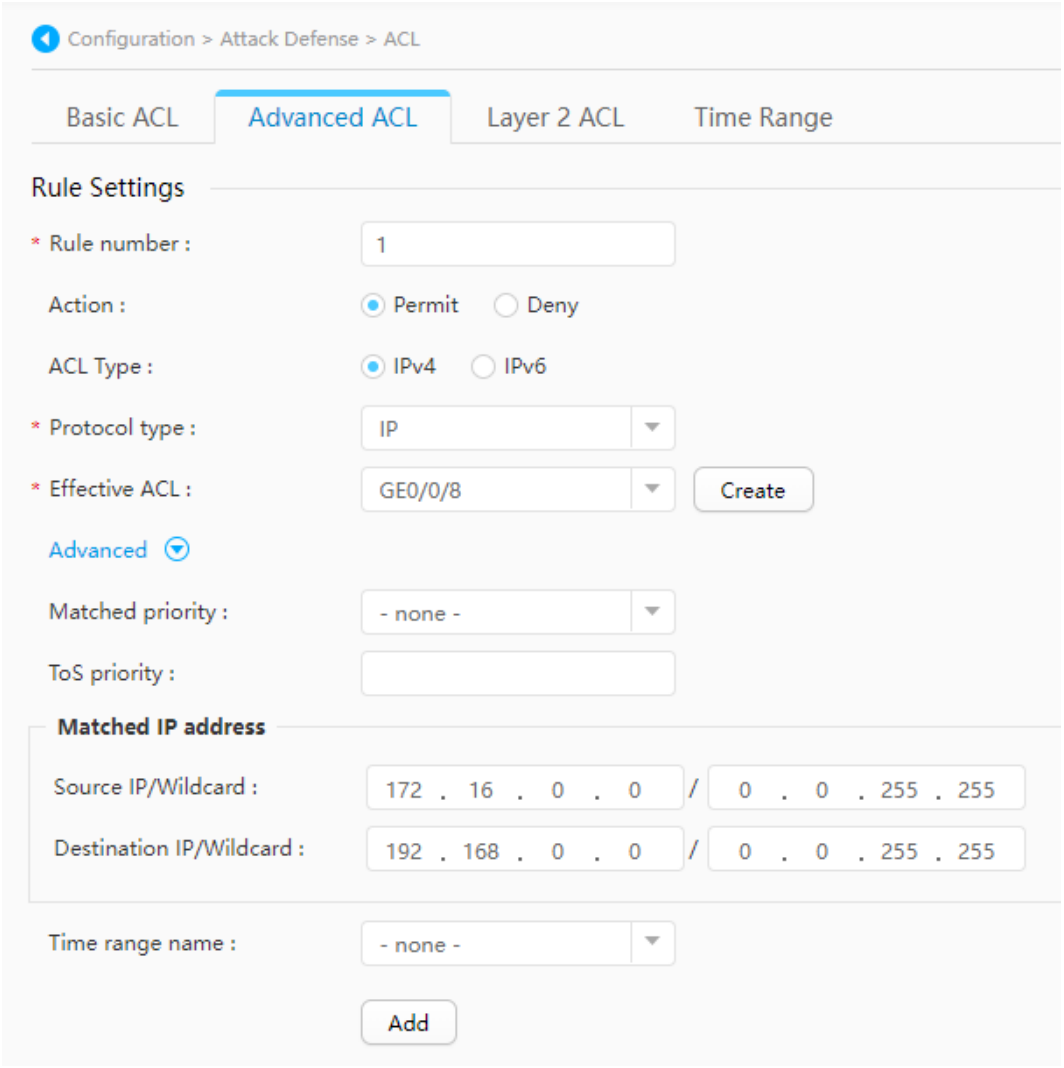
Figure 1-12 Configuring VPN connections



Step 3 Configure a VPN security policy.

Choose **Configuration** > **Attack Defense** > **ACL** > **Advanced ACL**, configure an advanced ACL, and click **Add**. **Figure 1-13** shows the key parameter settings.

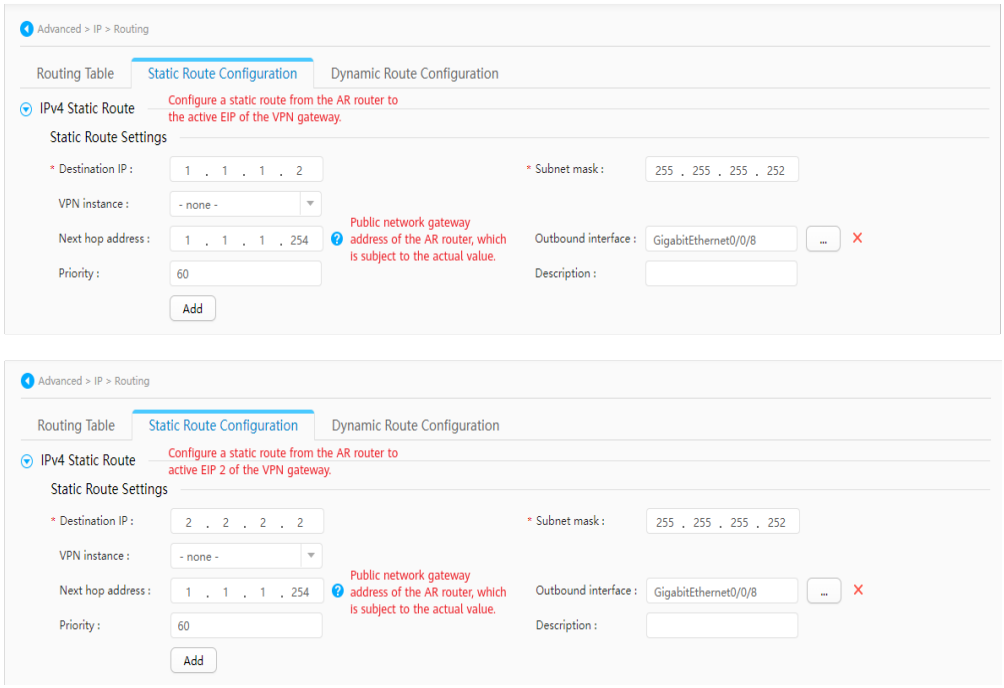
Figure 1-13 Configuring an advance ACL



Step 4 Configure service routes.

Choose **Advanced** > **IP** > **Routing** > **Static Route Configuration**. In the **IPv4 Static Route** area, configure static routes to the active EIP and active EIP 2 of the VPN gateway and a static route to the VPC, and click **Add**. **Figure 1-14** shows the key parameter settings.

Figure 1-14 Configuring service routes



----End

1.1.3.4 Verification

NOTE

In policy-based mode, an AR router uses one interface to establish two VPN connections. Due to the specification limit of the AR router, only one VPN connection can be established at a time.

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

    Choose **Virtual Private Network** > **Enterprise – VPN Connections**. Only one VPN connection is in **Normal** state.
  - AR router

    Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**. Only one VPN connection is in **READY|STAYLIVE** state.
- Verify that servers in the on-premises data center and ECSs in the VPC subnet can ping each other.

1.2 Interconnection with a Huawei AR Router (Dual Internet Lines in Active-Active Mode)

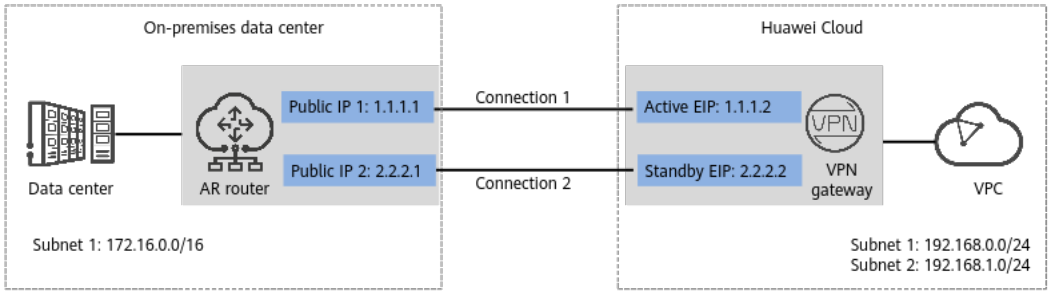
1.2.1 Static Routing Mode

1.2.1.1 Operation Guide

Scenario

Figure 1-15 shows the typical networking where a Huawei Cloud VPN gateway connects to a Huawei access router (AR) in an on-premises data center in static routing mode.

Figure 1-15 Typical networking diagram



In this scenario, the AR router has two IP addresses, and the Huawei Cloud VPN gateway uses the active/standby mode. A total of two VPN connections need to be created between the active and standby EIPs of the VPN gateway and the two IP addresses of the AR router.

Limitations and Constraints

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

Data Plan

Table 1-16 Data plan

Category	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/16	• 192.168.0.0/24 • 192.168.1.0/24
VPN gateway	Gateway IP address	• Public IP address 1: 1.1.1.1 • Public IP address 2: 2.2.2.1	• Active EIP: 1.1.1.2 • Standby EIP: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24

Category	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 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 1-16 shows the process of using the VPN service to enable communication between the data center and VPC.

Figure 1-16 Operation process

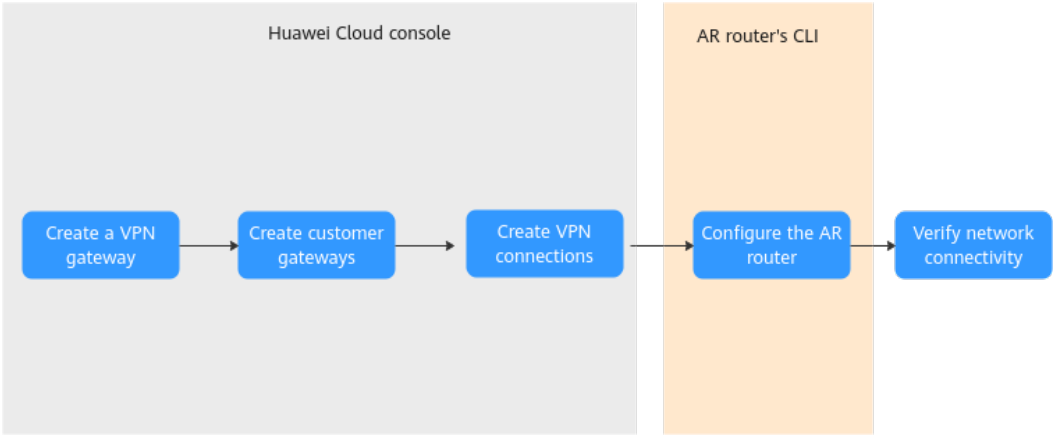


Table 1-17 Operation process description

No.	Configuration Interface	Step	Description
1	Huawei Cloud 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 customer gateways.**	Create two customer gateways with their IP addresses set to the public IP addresses of the AR router.
3		**Create VPN connections.**	• Create a total of two VPN connections between the active and standby EIPs of the VPN gateway and the customer gateways. • It is recommended that the routing mode, PSK, IKE policy, and IPsec policy settings of the two connections be the same.
5	Command-line interface (CLI) of the AR router	**Configure the AR router.**	• The local and remote interface addresses configured on the AR router must be the same as the customer and local interface addresses configured on the VPN console, respectively. • The routing 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.

1.2.1.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-18 describes the parameters for creating a VPN gateway.

Table 1-18 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active/Standby
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2

Parameter	Description	Value
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure customer gateways.

1. Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.
2. Set parameters to create the first customer gateway.

   Table 1-19 describes the parameter settings of the first customer gateway.

   Table 1-19 Parameter settings of the first customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar01
Identifier	One public IP address of the AR router.	1.1.1.1

3. Set parameters to create the second customer gateway.

   Table 1-20 describes the parameter settings of the second customer gateway.

   Table 1-20 Parameter settings of the second customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar02
Identifier	The other public IP address of the AR router.	2.2.2.1

Step 5 Configure VPN connections.

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

   Table 1-21 describes the key parameters for creating VPN connections.

   Table 1-21 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001

Parameter	Description	Value
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	2.2.2.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, health check, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify

Parameter	Description	Value
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, VPN traffic will fail to be forwarded.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	Test@123

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.2.1.3 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 IP addresses for WAN interfaces.

```
[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
[AR651]interface GigabitEthernet 0/0/9
[AR651-GigabitEthernet0/0/9]ip address 2.2.2.1 255.255.255.0
[AR651-GigabitEthernet0/0/9]quit
```

Step 4 Configure default routes.

```
[AR651]ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
[AR651]ip route-static 0.0.0.0 0.0.0.0 2.2.2.254 preference 100
```

In the commands, 1.1.1.254 and 2.2.2.254 are the gateway addresses for the AR router's public IP addresses. Replace them with the actual gateway addresses.

Step 5 Configure routes to the active and standby EIPs 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 2.2.2.254
```

- 1.1.1.2 and 2.2.2.2 are the active and standby EIPs of the VPN gateway, respectively.
- 1.1.1.254 and 2.2.2.254 are the gateway addresses for the AR router's public IP addresses.

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 2.2.2.1
[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 or standby EIP of the VPN gateway.

Step 10 Configure IPsec profiles.

```
[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]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.2 255.255.255.252
[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]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.2 255.255.255.252
[AR651-Tunnel0/0/2]source 2.2.2.1
[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 the standby EIP 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 or standby EIP 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 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.2
[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 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.2
[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 the standby EIP 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/standby 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

1.2.1.4 Verification

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

    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 Huawei Cloud VPC subnets can ping each other.

1.3 Interconnection with Alibaba Cloud

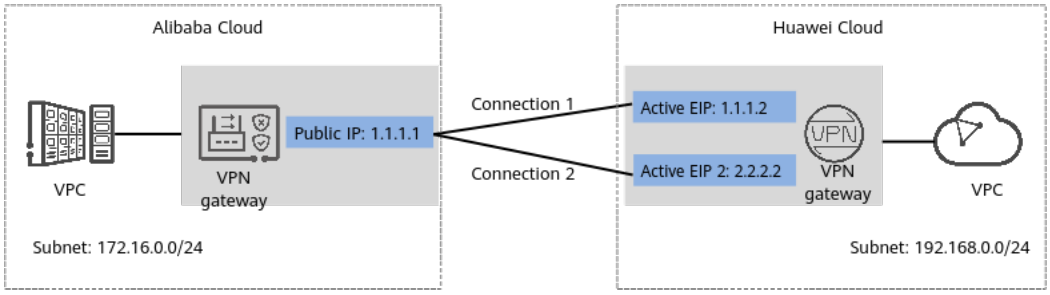
1.3.1 Static Routing Mode

1.3.1.1 Operation Guide

Scenario

Figure 1-17 shows the typical networking where a VPN gateway on Huawei Cloud connects to a VPN gateway on Alibaba Cloud in static routing mode.

Figure 1-17 Typical networking diagram



In this scenario, the Alibaba Cloud VPN gateway has only one IP address, and the Huawei Cloud VPN gateway uses the active-active mode. A VPN connection needs to be created between each of the two active EIPs of the Huawei Cloud VPN gateway and the IP address of the Alibaba Cloud VPN gateway.

Data Plan

Table 1-22 Data Plan

Category	Item	Example Value for the Alibaba Cloud Side	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/24	192.168.0.0/24
VPN gateway	Gateway IP address	1.1.1.1	• Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30	
	IKE policy	• IKE version: IKEv2 • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 14 • Local ID: IP address • Peer ID: IP address	
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group 14	

1.3.1.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   The following table only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-23 Parameters for creating a VPN gateway

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24
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 communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-24 only describes the key parameters for configuring a customer gateway. For other parameters, use their default settings.

Table 1-24 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ali
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway device to permit UDP port 4500.	IP Address 1.1.1.1

Step 5 Configure VPN connections.

In this scenario, the customer gateway has only one IP address. It is recommended that the VPN gateway on Huawei Cloud use the active-active mode. In this case, a VPN connection needs to be created between each of the two active EIPs of the VPN gateway and the IP address of the customer gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Set parameters as prompted.

   Table 1-25 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-25 Description of key VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001

Parameter	Description	Value
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/24
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, health check, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify

Parameter	Description	Value
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
Link Detection	Alibaba Cloud does not support the NQA function.	**NQA** disabled
Health Check	After health check is configured, the VPN gateway sends probe packets to the customer gateway to collect statistics about the round-trip time and packet loss rate of the physical link, which reflect the VPN connection quality. By default, health check is enabled. Enabling health check does not impact tunnel connectivity.	Enabled
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall. For details, see **Table 1-22**.	– 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.3.1.3 Configuration on the Alibaba Cloud Console

Prerequisites

A VPC and its subnets have been created on Alibaba Cloud.

Procedure

Step 1 Log in to the Alibaba Cloud console.

Step 2 Choose **Products and Services** > **Network & CDN** > **Hybrid cloud-network** > **VPN Gateway**.

Step 3 Configure a VPN gateway.

1. Click **Create VPN Gateway**.
2. Set parameters as prompted.

   Table 1-26 describes the parameters for configuring a VPN gateway. For other parameters, use their default settings.

   Table 1-26 Parameters for creating a VPN gateway

Parameter	Description	Value
Instance Name	Name of a VPN gateway.	vpngw-ali
VPC	Select VPC information.	vpc-ali
Bandwidth	VPN forwarding bandwidth specification.	5Mbps
IPsec-VPN	-	Enabled
SSL-VPN	-	Disabled
Billing Cycle	Specifies the required duration of the VPN gateway.	1 Month

Step 4 Configure a customer gateway.

1. Choose **VPN** > **Customer gateway**, and click **Create Customer Gateway**.

2. Set parameters as prompted.

   Table 1-27 only describes the key parameters for configuring a customer gateway. For other parameters, use their default settings.

   Table 1-27 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of the Huawei VPN gateway.	cgw-hw01
IP address	Active EIP of the Huawei Cloud VPN gateway.	1.1.1.2

3. Repeat the preceding steps to configure the customer gateway corresponding to active EIP 2 of the Huawei Cloud VPN gateway.

Step 5 Configure VPN connections.

1. Choose **VPN** > **IPsec Connections** and click **Create IPsec Connection**.
2. Set parameters as prompted.

   Table 1-28 describes the key parameters for configuring a VPN connection. For other parameters, use their default settings.

   Table 1-28 Description of key VPN connection parameters

Module	Parameter	Description	Value
-	Name	VPN connection name.	vpn-ali
	Bind Resource to VIP Subnet	Selecting a VPN gateway	VPN gateway
	VPN gateway	Select Alibaba Cloud VPN gateway.	vpngw-ali
	User gateway address	Select the Huawei Cloud VPN gateway.	cgw-hw01
	Routing Mode	Select Destination Route Mode	Destination routing mode
	Immediately effective	-	Yes

Module	Parameter	Description	Value
	Pre-shared key	The value must be the same as the pre-shared key set in **Table 1-25**.	*Set this parameter based on the site requirements.*
	Advanced Settings	-	Enabled
IKE policy	Version	The settings must be the same as those of the IKE policy configured in **Table 1-25**.	– Version: IKEv2 – Negotiation mode: main – Encryption Algorithm: AES-128 – Authentication algorithm: SHA2-256 – DH group: Group 14 – SA lifetime: 86400 – LocalId: 1.1.1.1 – RemoteId: 1.1.1.2
	Negotiation Mode		
	Encryption Algorithm		
	Authentication Algorithm		
	DH group		
	SA lifetime		
	LocalId		
	Remote Id		
IPsec policy	Encryption Algorithm	The settings must be the same as those of the IPsec policy configured in **Table 1-25**. **NOTE** The NAT traversal function must be enabled.	– Encryption Algorithm: AES-128 – Authentication algorithm: SHA2-256 – DH group: Group 14 – SA lifetime: 3600 – DPD: enabled – NAT traversal: enabled
	Authentication Algorithm		
	DH group		
	SA lifetime		
	DPD		

Module	Parameter	Description	Value
	Establishing an IPsec tunnel in a NAT traversal scenario		
Health Check	Configuring a Health Check	-	– Health check: enabled – Destination IP address: 192.168.0.10 – Source IP address: 172.16.0.10 – Retry interval: 3 – Retry counts: 3
	Target IP address.	Private IP address of the server in the Huawei Cloud VPC subnet. The value is only an example.	
	Specifies a source IP address.	Alibaba Cloud Private IP address of the server in the VPC subnet. The value is only an example.	
	Re-execution interval	-	
	Retry times.	-	

3. Repeat the preceding steps to configure a VPN connection for the customer gateway (cgw-hw02) corresponding to active EIP 2 of the Huawei Cloud VPN gateway.

Step 6 Configure routes.

You need to add a route to the Huawei Cloud VPC subnet on Alibaba Cloud.

1. Choose **VPN** > **VPN Gateway**.
2. Click the name of the target VPN gateway. On the **Destination Routing Table** tab page, click **Add Route Entry**.
3. Set parameters as prompted.
   – Configure a route to the active EIP, as described in **Table 1-29**.

Table 1-29 Parameters for configuring a route to the active EIP

Parameter	Description	Value
Destination network segment	Local subnet of the Huawei Cloud VPN gateway. If there are multiple local subnets, create multiple routes.	192.168.0.0/24
Next-hop type.	Select IPsec Connection.	IPsec connection
Next Hop	Select Alibaba Cloud VPN gateway.	vpn-ali/xxxxxxxxx
Publish to VPC	-	Yes
Weight Value	-	100

- Configure a route to active EIP 2, as described in **Table 1-30**.

Table 1-30 Parameters for configuring a route to active EIP 2

Parameter	Description	Value
Destination network segment	Local subnet of the Huawei Cloud VPN gateway. If there are multiple local subnets, create multiple routes.	192.168.0.0/24
Next-hop type.	Select IPsec Connection.	IPsec connection
Next Hop	Select Alibaba Cloud VPN gateway.	vpn-ali/xxxxxxxxx
Publish to VPC	-	Yes
Weight Value	-	0

----End

1.3.1.4 Verification

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

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

  - Alibaba Cloud

    Choose VPN > IPsec Connection. The status of the two VPN connections is displayed as Phase 2 negotiation succeeded. Because the Alibaba Cloud VPN connection uses the active/standby mode, the health check status is displayed as Active connection normal and Standby connection abnormal.

- The servers in the VPC subnet and those in the Huawei Cloud VPC subnet can ping each other.

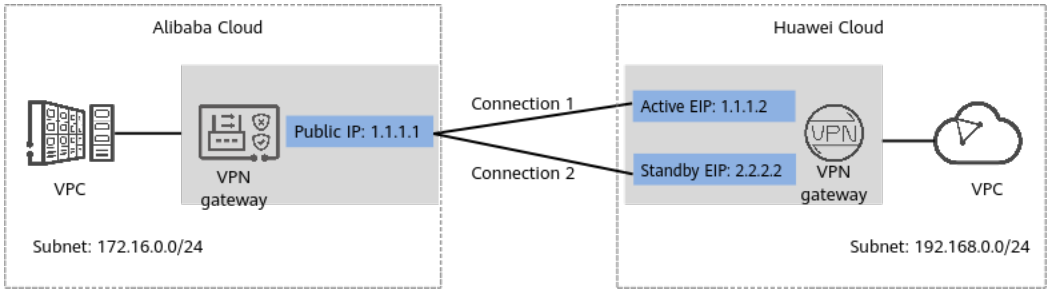
1.3.2 BGP Routing Mode

1.3.2.1 Operation Guide

Scenario

Figure 1-18 shows the typical networking where a VPN gateway on Huawei Cloud connects to a VPN gateway on Alibaba Cloud in BGP routing mode.

Figure 1-18 Typical networking diagram



In this scenario, the Alibaba Cloud VPN gateway has only one IP address. A VPN connection needs to be created between each of the two active EIPs of the Huawei Cloud VPN gateway and the IP address of the Alibaba Cloud VPN gateway.

Data Plan

Table 1-31 Data Plan

Category	Item	Example Value for the Alibaba Cloud Side	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/24	192.168.0.0/24
VPN gateway	Gateway IP address	1.1.1.1	• Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
	BGP ASN	65515	64512

Category	Item	Example Value for the Alibaba Cloud Side	Example Value for the Huawei Cloud Side
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30	
	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 14 • IKE version: IKEv2 • Local ID: IP address • Peer ID: IP address	
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group 14	

1.3.2.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

Table 1-32 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-32 Key parameters for creating a VPN gateway

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24
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 communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-33 only describes the key parameters for creating a customer gateway. For other parameters, use their default settings.

Table 1-33 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ali

Parameter	Description	Value
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway device to permit UDP port 4500.	IP Address 1.1.1.1
BGP ASN	ASN of your on-premises data center or private network. The value must be different from the BGP ASN of the VPN gateway.	65515

Step 5 Configure VPN connections.

In this scenario, the Alibaba Cloud VPN gateway has only one IP address. A VPN connection needs to be created between each of the two active EIPs of the Huawei Cloud VPN gateway and the IP address of the Alibaba Cloud VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Set parameters as prompted.

   Table 1-34 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-34 Description of key VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1

Parameter	Description	Value
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **BGP routing**.	BGP routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/24
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30

Parameter	Description	Value
Health Check	After health check is configured, the VPN gateway sends probe packets to the customer gateway to collect statistics about the round-trip time and packet loss rate of the physical link, which reflect the VPN connection quality. By default, health check is enabled. Enabling health check does not impact tunnel connectivity.	Enabled
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the firewall.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– IKE Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-128 ▪ DH Algorithm: Group 14 ▪ Version: v2 ▪ 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.3.2.3 Configuration on the Alibaba Cloud Console

Prerequisites

A VPC and its subnets have been created on Alibaba Cloud.

Procedure

Step 1 Log in to the Alibaba Cloud console.

Step 2 Choose **Products and Services** > **Network & CDN** > **Hybrid cloud-network** > **VPN Gateway**.

Step 3 Configure a VPN gateway.

1. Choose **VPN** > **VPN Gateways** and click **Buy VPN Gateway**.
2. Set parameters as prompted.

   Table 1-35 describes the VPN gateway parameters. For other parameters, use their default settings.

Table 1-35 Key parameters for creating a VPN gateway

Parameter	Description	Value
Instance Name	Name of a VPN gateway.	vpngw-ali
Region.	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to you.	CN North-Beijing2
VPC	Select VPC information.	vpc-ali
Bandwidth	VPN forwarding bandwidth specification.	5Mbps

Parameter	Description	Value
IPsec-VPN	-	Enabled
SSL-VPN	-	Disabled
Billing Cycle	Specifies the required duration of the VPN gateway.	One month

Step 4 Configure a user gateway.

1. Choose **VPN** > **Customer gateway**, and click **Create Customer Gateway**.
2. Set parameters as prompted.

   Table 1-36 describes the customer gateway parameters. For other parameters, use their default settings.

   Table 1-36 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of the Huawei VPN gateway.	cgw-hw01
IP address	IP address used by the Huawei Cloud VPN gateway to communicate with the active EIP of the Alibaba Cloud VPN gateway.	1.1.1.2
Indicates the AS number.	BGP AS number. The value must be the same as the BGP ASN set in **Table 1-35**.	64512

3. Configure the user gateway corresponding to the standby EIP of the Huawei Cloud VPN gateway by referring to step 2.

Step 5 Configure VPN connections.

1. Choose **VPN** > **IPsec Connections** and click **Create IPsec Connection**.
2. Set parameters as prompted.

   Parameters of the VPN connection are described in **Table 1-37**. For other parameters, use their default settings.

   Table 1-37 Description of key VPN connection parameters

Module	Parameter	Description	Value
-	Parameter	Name of a VPN connection.	vpn-ali

Module	Parameter	Description	Value
	Bind Resource to VIP Subnet	Selecting a VPN gateway	VPN gateway
	VPN Gateway	Select Alibaba Cloud VPN gateway.	vpngw-ali
	User gateway address	Select the Huawei Cloud VPN gateway.	cgw-hw01
	Routing Mode	Select Destination Route Mode	Destination routing mode
	Immediately effective	-	Yes
	Specifies a pre-shared key.	The value must be the same as the pre-shared key of the Huawei Cloud VPN connection.	*Set this parameter based on the site requirements.*
	Advanced Settings	-	Enabled
IKE configuration	Version	The IKE configuration must be the same as the **IKE Policy** of the Huawei Cloud VPN connection.	– Version: IKEv2 – Negotiation mode: main – Encryption Algorithm: AES-128 – Authentication Algorithm: SHA2-256 – DH group: Group 14 – SA lifetime: 86400 – LocalId: 1.1.1.1 – RemoteId: 1.1.1.2
	Negotiation Mode		
	Encryption Algorithm		
	Authentication Algorithm		
	DH group		

Module	Parameter	Description	Value
	SA lifetime		
	LocalId		
	RemoteId		
Configure IPsec.	Encryption Algorithm	The IPsec configuration must be the same as the **IPsec Policy** of the Huawei Cloud VPN connection. **NOTE** The NAT traversal function must be enabled.	– Encryption Algorithm: AES-128 – Authentication Algorithm: SHA2-256 – DH group: Group 14 – SA lifetime: 3600 – DPD: enabled – NAT traversal: enabled
	Authentication Algorithm		
	DH group		
	SA lifetime		
	DPD		
	Establishing an IPsec tunnel in a NAT traversal scenario		
BGP Configuration	BGP Configuration	-	Enabled
	Tunnel CIDR block	The value must be the same as the tunnel interface CIDR block configured in **Table 1-34**.	169.254.70.0/30
	Local BGP address	The value must be the same as the peer interface address configured in **Table 1-34**.	169.254.70.1

Module	Parameter	Description	Value
	Local Autonomous System Number	The value must be the same as the BGP ASN set in **Table 1-33**.	65515
Health Check	Health Check	-	– Health check: enabled – Destination IP address: 192.168.0.10 – Source IP address: 172.16.0.10 – Retry interval: 3 – Retry counts: 3
	Target IP address.	Private IP address of the server in the Huawei Cloud VPC subnet. The value is only an example.	
	Specifies a source IP address.	Alibaba Cloud Private IP address of the server in the VPC subnet. The value is only an example.	
	Re-execution interval	-	
	Retry Attempts	-	

3. Repeat the preceding steps to configure a VPN connection for the user gateway (cgw-hw02) corresponding to the standby EIP of the Huawei Cloud VPN gateway.

Step 6 Configure routes.

BGP routes cannot be automatically advertised to the VPC. You need to configure a static route to the VPN gateway.

1. Select Route Table.
2. Click the name of a route table. On the **Route List** > **Custom Routes** tab page, click Add Route.
3. Set parameters as prompted.

Table 1-38 Route table parameters

Parameter	Description	Value
Destination network segment	Local subnet of the Huawei Cloud VPN gateway. If there are multiple local subnets, create multiple routes.	192.168.0.0/24
Next-hop type.	Select a VPN gateway.	VPN Gateway
Next Hop	Select Alibaba Cloud VPN gateway.	vpn-ali/xxxxxxxxx
Publish to VPC	-	Yes

----End

1.3.2.4 Verification

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

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

    Choose VPN > IPsec Connection. The status of the two VPN connections is displayed as Phase 2 negotiation succeeded. Because the Alibaba Cloud VPN connection uses the active/standby mode, the health check status is displayed as Active connection normal and Standby connection abnormal.
- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

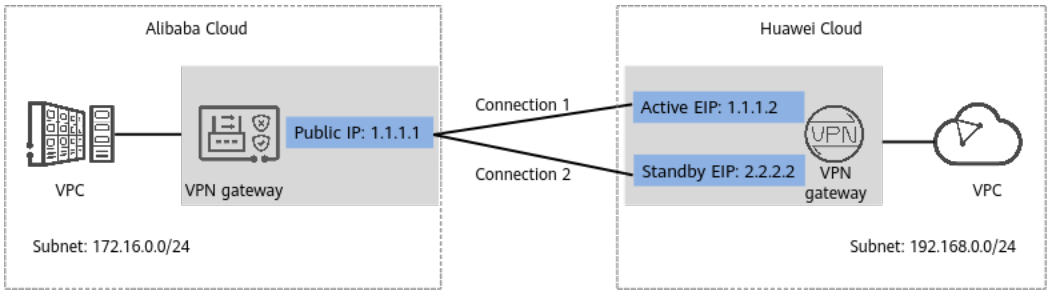
1.3.3 Policy-based Mode

1.3.3.1 Operation Guide

Scenario

Figure 1-19 shows the typical networking where a Huawei Cloud VPN gateway connects to Alibaba Cloud in policy-based mode.

Figure 1-19 Typical networking diagram



In this scenario, the Alibaba Cloud VPN gateway has only one IP address. A VPN connection needs to be created between each of the two active EIPs of the Huawei Cloud VPN gateway and the IP address of the Alibaba Cloud VPN gateway.

Data Plan

Table 1-39 Data Plan

Category	Item	Example Value for the Alibaba Cloud Side	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/24	192.168.0.0/24
VPN gateway	Gateway IP address	1.1.1.1	• Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
VPN connection	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 14 • IKE version: IKEv2 • Local ID: IP address • Peer ID: IP address	
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group 14	

1.3.3.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-40 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

   Table 1-40 Parameters for creating a VPN gateway

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24
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 communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-41 only describes the key parameters for creating a customer gateway. For other parameters, use their default settings.

Table 1-41 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ali
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway device to permit UDP port 4500.	IP Address 1.1.1.1

Step 5 Configure VPN connections.

In this scenario, the Alibaba Cloud VPN gateway has only one IP address. A VPN connection needs to be created between each of the two active EIPs of the Huawei Cloud VPN gateway and the IP address of the Alibaba Cloud VPN gateway.

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

1. Set parameters as prompted.

   Table 1-42 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-42 Description of key VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1

Parameter	Description	Value
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Policy-based**.	Policy-based
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/24
Connection 1's Configuration	Configure the health check, PSK, confirm PSK, and policies for the VPN gateway IP address of connection 1.	*Set parameters based on the site requirements.*
Health Check	After health check is configured, the VPN gateway sends probe packets to the customer gateway to collect statistics about the round-trip time and packet loss rate of the physical link, which reflect the VPN connection quality. By default, health check is enabled. Enabling health check does not impact tunnel connectivity.	Enabled
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy	A policy rule defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. – Source CIDR Block The source CIDR block must contain some local subnets. 0.0.0.0/0 indicates any address. – Destination CIDR Block The destination CIDR block must contain all customer subnets.	– Source CIDR Block: 192.168.0.0/24 – Destination CIDR Block: 172.16.0.0/24

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– IKE Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-128 ▪ DH Algorithm: Group 14 ▪ Version: v2 ▪ 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** It is recommended that the configuration of connection 2 be the same as that of connection 1.	Enabled

----End

1.3.3.3 Configuration on the Alibaba Cloud Console

Prerequisites

A VPC and its subnets have been created on Alibaba Cloud.

Procedure

Step 1 Log in to the Alibaba Cloud console.

Step 2 Choose **Products and Services** > **Network & CDN** > **Hybrid cloud-network** > **VPN Gateway**.

Step 3 Configure a VPN gateway.

1. Choose **VPN** > **VPN Gateways** and click **Buy VPN Gateway**.
2. Set parameters as prompted.

   Table 1-43 describes the VPN gateway parameters. For other parameters, use their default settings.

Table 1-43 Parameters for creating a VPN gateway

Parameter	Description	Value
Instance Name	Name of a VPN gateway.	vpngw-ali
VPC	Select VPC information.	vpc-ali
Bandwidth	VPN forwarding bandwidth specification.	5Mbps
IPsec-VPN	-	Enabled
SSL-VPN	-	Disabled
Billing Cycle	Specifies the required duration of the VPN gateway.	One month

Step 4 Configure a customer gateway.

1. Choose **VPN** > **Customer gateway**, and click **Create Customer Gateway**.
2. Set parameters as prompted.

   Table 1-44 describes the customer gateway parameters. For other parameters, use their default settings.

Table 1-44 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of the Huawei VPN gateway.	cgw-hw01

Parameter	Description	Value
IP address	Active EIP of the Huawei Cloud VPN gateway.	1.1.1.2

3. Configure the user gateway corresponding to the standby EIP of the Huawei Cloud VPN gateway by referring to step 2.

Step 5 Configure VPN connections.

1. Choose **VPN** > **IPsec Connections** and click **Create IPsec Connection**.
2. Set parameters as prompted.

   Parameters of the VPN connection are described in **Table 1-45**. For other parameters, use their default settings.

Table 1-45 Description of key VPN connection parameters

Module	Parameter	Description	Value
-	Name	VPN connection name.	vpn-ali
	VPN Gateway	Select Alibaba Cloud VPN gateway.	vpngw-ali
	User gateway address	Select the Huawei Cloud VPN gateway.	cgw-hw01
	Local CIDR Block	Alibaba Cloud: VPC subnet.	172.16.0.0/24
	Peer Network	Subnet of the Huawei Cloud VPC. **NOTE** If there are multiple local or peer CIDR blocks, you need to create a VPN connection from each local CIDR block to each peer CIDR block. The total number of VPN connections to be created is the number of local CIDR blocks multiplied by the number of peer CIDR blocks. For example, if there are two local CIDR blocks and three peer CIDR blocks, you need to create 2 x 3 VPN connections on Alibaba Cloud.	192.168.0.0/24
	Immediately effective	-	Yes

Module	Parameter	Description	Value
	Specifies a pre-shared key.	The value must be the same as the pre-shared key specified by **Table 1-42**.	*Set this parameter based on the site requirements.*
	Advanced Settings	-	Enabled
IKE configuration	Version	The value must be the same as the IKE policy configured in **Table 1-42**.	– Version: IKEv2 – Negotiation mode: main – Encryption Algorithm: AES-128 – Authentication Algorithm: SHA2-256 – DH group: Group 14 – SA lifetime: 86400 – LocalId: 1.1.1.1 – RemoteId: 1.1.1.2
	Negotiation Mode		
	Encryption Algorithm		
	Authentication Algorithm		
	DH group		
	SA lifetime		
	LocalId		
	Remote Id		
Configure IPsec.	Encryption Algorithm	The value must be the same as the IPsec policy configured in **Table 1-42**.	– Encryption Algorithm: AES-128 – Authentication Algorithm: SHA2-256 – DH group: Group 14 – SA lifetime: 3600
	Authentication Algorithm		
	DH group		
	SA lifetime		

Module	Parameter	Description	Value
Configuring a Health Check	Configuring a Health Check	-	– Health check: enabled – Destination IP address: 192.168.0.10 – Source IP address: 172.16.0.10 – Retry interval: 3 – Retry counts: 3
	Target IP address.	Private IP address of the server in the Huawei Cloud VPC subnet. The value is only an example.	
	Specifies a source IP address.	Alibaba Cloud Private IP address of the server in the VPC subnet. The value is only an example.	
	Re-execution interval	-	
	Retry Attempts	-	

3. Repeat the preceding steps to configure a VPN connection for the user gateway (cgw-hw02) corresponding to the standby EIP of the Huawei Cloud VPN gateway.

Step 6 Configure routes.

You need to add a route to the Huawei Cloud VPC subnet on Alibaba Cloud.

1. Choose **VPN** > **VPN Gateway**.
2. Click the name of the target VPN gateway. On the **Destination Routing Table** tab page, click **Add Route Entry**.
3. Set parameters as prompted.
   – Configure the route to the active EIP, as described in **Table 1-46**.

Table 1-46 Parameters of the route table to the active EIP

Parameter	Description	Value
Destination network segment	Local subnet of the Huawei Cloud VPN gateway. If there are multiple local subnets, create multiple routes.	192.168.0.0/24

Parameter	Description	Value
Next-hop type.	Select IPsec Connection.	IPsec connection
Next Hop	Select Alibaba Cloud VPN gateway.	vpn-ali/xxxxxxxxx
Publish to VPC	-	Yes
Weight Value	-	100

- Configure the route to the standby EIP, as described in **Table 1-47**.

  Table 1-47 Parameters for configuring the route table of the standby EIP

Parameter	Description	Value
Destination network segment	Local subnet of the Huawei Cloud VPN gateway. If there are multiple local subnets, create multiple routes.	192.168.0.0/24
Next-hop type.	Select IPsec Connection.	IPsec connection
Next Hop	Select Alibaba Cloud VPN gateway.	vpn-ali/xxxxxxxxx
Publish to VPC	-	Yes
Weight Value	-	0

----End

1.3.3.4 Verification

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

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

    Choose VPN > IPsec Connection. The status of the two VPN connections is displayed as Phase 2 negotiation succeeded. Because the Alibaba Cloud VPN connection uses the active/standby mode, the health check status is displayed as Active connection normal and Standby connection abnormal.

- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

1.4 Interconnection with Tencent Cloud

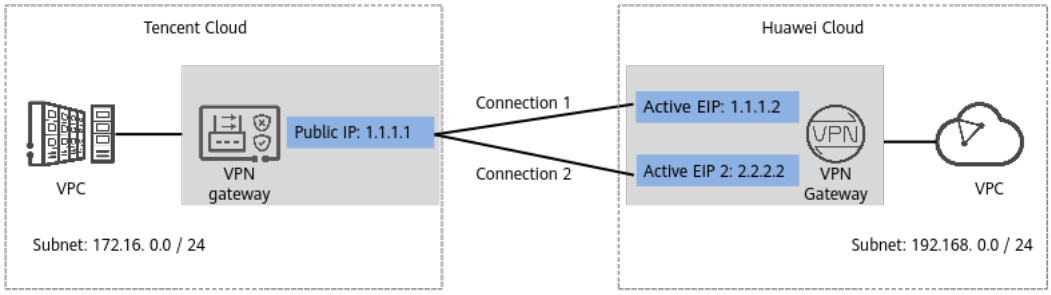
1.4.1 Static Routing

1.4.1.1 Operation

Scenario

Typical networking shows the typical networking for connecting a Huawei Cloud VPN gateway to a Tencent Cloud VPN gateway using static routes.

Figure 1-20 Typical networking diagram



In this scenario, the Tencent Cloud VPN gateway supports only the single-IP address solution. The active-active mode is recommended for the Huawei Cloud VPN gateway. Create a VPN connection between the active EIP, active EIP2, and the IP address of the Tencent Cloud VPN gateway.

Data Plan

Table 1-48 Data plan

Category	Item	Tencent Cloud Example Value	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/24	192.168.0.0/24
VPN gateway	Gateway IP address	1.1.1.1	• Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24

Category	Item	Tencent Cloud Example Value	Example Value for the Huawei Cloud Side
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30	
	IKE policy	• Version: v2 • Authentication algorithm: SHA2-256 • Encryption Algorithm: AES-128 • DH algorithm: Group 14 • Local ID: IP address • Peer ID: IP address	
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption Algorithm: AES-128 • PFS: DH group 14 • DPD timeout period: 45s The default DPD timeout period at the Huawei Cloud side is 45 seconds, which cannot be configured.	

1.4.1.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-49 describes the parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-49 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

1. Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.

2. Set parameters as prompted.

   Table 1-50 describes the parameters for creating a customer gateway. For other parameters, use their default settings.

   Table 1-50 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-tx
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway to permit UDP port 4500.	IP Address 1.1.1.1

Step 5 Configure VPN connections.

In this scenario, the customer gateway has only one IP address. It is recommended that the VPN gateway on Huawei Cloud use the active-active mode. In this case, a VPN connection needs to be created between each of the two active EIPs of the VPN gateway and the IP address of the customer gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Set parameters as prompted.

   Table 1-51 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

   Table 1-51 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2

Parameter	Description	Value
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/24
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, health check, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– IKE Policy ▪ Version: v2 ▪ 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.4.1.3 Procedure on the Tencent Cloud Console

Prerequisites

A VPC and its subnets have been created on Tencent Cloud.

Procedure

Step 1 Log in to the Tencent Cloud console.

Step 2 Choose **Cloud Products** > **Hybrid Cloud Network** > **VPN Connections**.

Step 3 Configure a VPN gateway.

1. Choose **VPN Connections** > **VPN Gateways** and click **Create**.
2. Set the parameters as prompted and click Create.

   Table 1-52 describes the VPN gateway parameters. For other parameters, use their default settings.

Table 1-52 Description of VPN gateway parameters

Parameter	Description	Value
Gateway Name	Name of a VPN gateway.	vpngw-tx
Protocol Type	Select IPsec.	IPsec
Network type	Select Private network.	Private network
CIDR Block	Select the VPC that needs to communicate with the Huawei Cloud VPC.	vpc-tx(172.16.0.0/16)

Step 4 Configure a customer gateway. indicates the Huawei Cloud VPN gateway information.

1. Choose **VPN Connections** > **Customer Gateways** and click **Create**.
2. Set parameters as prompted and click **OK**.

   Table 1-53 describes the customer gateway parameters. For other parameters, use their default settings.

Table 1-53 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	hwvpn-01
Gateway IP Address	Active EIP of the Huawei Cloud VPN gateway.	1.1.1.2

3. Repeat the preceding steps to create the gateway information (hwvpn-02) corresponding to the primary EIP (2.2.2.2) of the Huawei Cloud VPN gateway.

Step 5 Configure VPN connections.

1. Choose **VPN Connections** > **VPN Tunnels** and click **Create**.
2. Set the parameters as prompted and click **Create**.

   Table 1-54 only describes the key parameters for creating a VPN connection. For other parameters, use their default settings.

Table 1-54 Description of VPN connection parameters

Module	Parameter	Description	Value
Basic configuration	VPN Tunnel Name	VPN connection name.	vpn-tx
	VPN Type	Select Private network.	Private network
	Private network	Select the VPC that needs to communicate with the Huawei Cloud VPC.	vpc-tx(172.16.0.0/16)
	VPN Gateway	Select the VPN gateway created in **Step 3**.	vpngw-tx
	Customer Gateway	Select Select Existing and select the customer gateway created in **Step 4**.	hwvpn-01
	PSK	The pre-shared key must be the same as that configured for the Huawei Cloud VPN connection.	*Set this parameter based on the site requirements.*
	Negotiation Mode	Select Active.	Active
Communication Modes	-	Select Destination route.	Destination route.

Module	Parameter	Description	Value
Advanced Settings	DPD	The default DPD timeout period at the Huawei Cloud side is 45 seconds, which cannot be configured.	45
	Health Check	The local and remote addresses are the same as the tunnel addresses used for connecting to Huawei Cloud. **NOTE** Health check must be configured. Otherwise, traffic cannot be switched after the Tencent Cloud connection is faulty.	Health
IKE This parameter is optional.	Version	The IKE configuration must be the same as the IKE policy configured in **Table 1-51**.	– Version: IKEv2 – Encryption Algorithm: AES-128 – Authentication Algorithm: SHA2-256 – Local ID: IP address – Remote ID: IP Address (1.1.1.2) – DH group: DH14 – IKE SA Lifetime: 86400
	Encryption Algorithm		
	Authentication Algorithm		
	Local ID		
	Remote ID		
	DH group		
	IKE SA Lifetime		

Module	Parameter	Description	Value
IPsec Configuration (Optional)	Encryption Algorithm	The IPsec configuration must be the same as the IPsec policy configured in **Table 1-51**.	– Encryption Algorithm: AES-128 – Authentication Algorithm: SHA2-256 – Packet Encapsulation Mode: Tunnel – Security protocol: ESP – PFS: DH-GROUP14 – IPsec sa Lifetime: 3600 s – IPsec sa Lifetime: 1843200 KB
	Authentication Algorithm		
	PFS		
	IPsec sa Lifetime		

3. Repeat the preceding steps to create a VPN connection between the Tencent Cloud VPN gateway and the primary EIP (hwvpn-002) of the Huawei Cloud VPN gateway.

Step 6 Add route information to the VPC route table.

1. Choose **Cloud Product** > **Cloud Network** > **Private Network** > **Route Table** > **Route Table** and click **Create**.
2. Set the parameters as prompted and click **Create**.

   Table 1-55 describes the route table parameters. For other parameters, use their default settings.

Table 1-55 Description of route table parameters

Parameter	Description	Value
Name	Route table name.	route-hw
CIDR Block	Select the VPC that needs to communicate with the Huawei Cloud VPC.	vpc-tx(172.16.0.0/16)
End	Subnet of the Huawei Cloud VPC. If there are multiple Huawei Cloud VPC subnets, you need to add multiple route policies.	192.168.0.0/24
Next Hop Type	Select VPN gateway.	VPN Gateway

Parameter	Description	Value
Next Hop	VPN gateway for which VPN connections are created.	vpngw-tx

Step 7 Add route information to the VPN gateway route table.

1. Choose **Cloud Product** > **Hybrid Cloud Network** > **VPN Connection** > **VPN Gateway** > **Details** > **Route Table** and click **Add Route Policy**.
2. Set parameters as prompted and click **Create**.

   Table 1-56 describes the route table parameters. For other parameters, use their default settings.

   Table 1-56 Description of route table parameters

Parameter	Description	Value
End	Subnet of the Huawei Cloud VPC. If there are multiple Huawei Cloud VPC subnets, you need to add multiple route policies.	192.168.0.0/24
Next Hop	Select the first VPN connection.	vpn-tx
Route type	Select **Static**.	Static route
Weighted	Priority of a VPN connection. Smaller values correspond to higher priorities.	0

3. Repeat the preceding steps to configure the route information corresponding to the second VPN connection.

   NOTE

   It is recommended that the weights of the routes corresponding to the two VPN connections be the same.

----End

1.4.1.4 Verification

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

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

    Choose VPN Connections > VPN Tunnels. The two VPN connections are in the Connected state, and the health status is Healthy.

- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

1.5 Interconnection with a Huawei USG Firewall

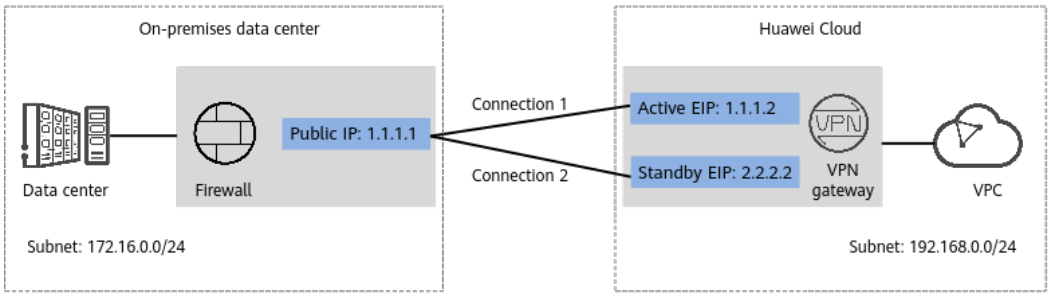
1.5.1 Static Routing Mode

1.5.1.1 Operation Guide

Scenario

Figure 1-21 shows the typical networking where a Huawei Cloud VPN gateway connects to a Huawei firewall in an on-premises data center in static routing mode.

Figure 1-21 Typical networking diagram



In this scenario, the firewall has only one public IP address. A VPN connection needs to be created between the public IP address of the firewall and each of the active and standby EIPs of the Huawei Cloud VPN gateway.

Data Plan

Table 1-57 Data plan

Category	Item	Example Value for the Huawei USG Firewall	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/24	192.168.0.0/24
VPN gateway	Gateway IP address	1.1.1.1	• Active EIP: 1.1.1.2 • Standby EIP: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24

Category	Item	Example Value for the Huawei USG Firewall	Example Value for the Huawei Cloud Side
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30	
	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: group 15 • IKE version: IKEv2 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address	
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH group 15 • Dead peer detection (DPD) timeout period: 45s The default DPD timeout period at the Huawei Cloud side is 45 seconds, which cannot be configured. • Lifetime (s): 3600	

1.5.1.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-58 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-58 Parameters for creating a VPN gateway

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active/Standby
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-59 only describes the key parameters for creating a customer gateway. For other parameters, use their default settings.

Table 1-59 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway to permit UDP port 4500.	IP Address 1.1.1.1

Step 5 Configure VPN connections.

In this scenario, the firewall has only one public IP address. A VPN connection needs to be created between the public IP address of the firewall and each of the active and standby EIPs of the Huawei Cloud VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Set parameters as prompted.

   Table 1-60 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-60 Parameters for creating VPN connections

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001

Parameter	Description	Value
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/24
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, health check, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify

Parameter	Description	Value
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets. The VPN gateway can automatically perform NQA detection on the peer interface address that has been configured on the customer gateway.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– IKE Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-128 ▪ DH Algorithm: Group 15 ▪ Version: v2 ▪ Lifetime (s): 86400 ▪ Local ID: IP Address ▪ Customer ID: IP Address – IPsec Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-128 ▪ PFS: DH group 15 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 3600
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.5.1.3 Configuration on the Firewall

Procedure

1. Log in to the command line interface (CLI) of the firewall.

   The commands may vary according to the firewall models and versions. For details, see the product documentation of the corresponding version.

2. Configure basic information.

   a. Configure IP addresses for interfaces of the firewall.

   ```
   interface GigabitEthernet1/0/1                # Configure a public IP address for an interface of the firewall.
   ip address 1.1.1.1 255.255.255.0
   interface GigabitEthernet1/0/2                # Configure a private IP address for an interface of the firewall.
   ip address 172.16.0.233 255.255.255.0
   ```

   b. Add interfaces to security zones.

   ```
   firewall zone untrust
   add interface GigabitEthernet1/0/1
   firewall zone trust
   add interface GigabitEthernet1/0/2
   ```

   c. Configures the TCP MSS.

   ```
   firewall tcp-mss 1300
   ```

3. Configure negotiation policies.

   ```
   ike proposal 100                # Configure an IKE policy for the VPN connection to be established between the public IP address of the firewall and the active EIP of the VPN gateway.
   authentication-algorithm SHA2-256     # Set the same authentication algorithm as that configured in the IKE policy in Table 1-60.
   encryption-algorithm AES-128          # Set the same encryption algorithm as that configured in the IKE policy in Table 1-60.
   authentication-method pre-share
   integrity-algorithm HMAC-SHA2-256
   prf HMAC-SHA2-256
   dh group15                      # Set the same DH algorithm as that configured in the IKE policy in Table 1-60.
   sa duration 86400                 # Set the same lifetime as that configured in the IKE policy in Table 1-60.

   ike peer hwcloud_peer33
   undo version 1                  # Set the same IKE version as that configured in the IKE policy in Table 1-60.
   pre-shared-key XXXXXXX              # Set the same PSK as that configured in Table 1-60.
   ike-proposal 100
   remote-address 1.1.1.2              # Specify the active EIP of the VPN gateway.

   IPsec proposal IPsec-pro100          # Configure an IPsec policy for the VPN connection to be established between the public IP address of the firewall and the active EIP of the VPN gateway.
   transform esp
   encapsulation-mode tunnel
   esp authentication-algorithm SHA2-256 # Set the same authentication algorithm as that configured
   ```



```
in the IPsec policy in Table 1-60.
esp encryption-algorithm aes-128    # Set the same encryption algorithm as that configured in the IPsec policy in Table 1-60.

ike proposal 200                # Configure policies for the VPN connection to be established between the public IP address of the firewall and the standby EIP of the VPN gateway.
authentication-algorithm SHA2-256
encryption-algorithm AES-128
authentication-method pre-share
integrity-algorithm HMAC-SHA2-256
prf HMAC-SHA2-256
dh group15
sa duration 86400

ike peer hwcloud_peer44
undo version 1
pre-shared-key XXXXXXX
ike-proposal 200
remote-address 2.2.2.2                # Specify the standby EIP of the VPN gateway.

IPsec proposal IPsec-pro200
transform esp
encapsulation-mode tunnel
esp authentication-algorithm SHA2-256
esp encryption-algorithm aes-128
```

4. Configure IPsec tunnels.

```
IPsec profile HW-IPsec100  # Configure a routing policy for the public IP address of the firewall.
ike-peer hwcloud_peer33
proposal IPsec-pro100
pfs dh-group15                # Set the same PFS as that configured in the IPsec policy in Table 1-60.
sa duration time-based 3600       # Set the same lifetime as that configured in the IPsec policy in Table 1-60.

interface Tunnel100
ip address 169.254.70.2 255.255.255.252       # Specify the IP address of tunnel interface 1 on the firewall.
tunnel-protocol IPsec
source 1.1.1.1                        # Specify the public IP address of the firewall.
destination 1.1.1.2                     # Specify the active EIP of the VPN gateway.
service-manage ping permit
IPsec profile HW-IPsec100
firewall zone untrust
add interface Tunnel100

IPsec profile HW-IPsec200
ike-peer hwcloud_peer44
proposal IPsec-pro200
pfs dh-group15                # Set the same PFS as that configured in the IPsec policy in Table 1-60.
sa duration time-based 3600       # Set the same lifetime as that configured in the IPsec policy in Table 1-60.

interface Tunnel200
ip address 169.254.71.2 255.255.255.252     # Specify the IP address of tunnel interface 2 on the firewall.
tunnel-protocol IPsec
source 1.1.1.1                      # Specify the public IP address of the firewall.
destination 2.2.2.2                     # Specify the standby EIP of the VPN gateway.
service-manage ping permit
IPsec profile HW-IPsec200
firewall zone untrust
add interface Tunnel200
```

5. Configure routes.

   a. Configure static routes to the public IP addresses of the Huawei Cloud side.

   ```
   ip route-static 1.1.1.2 255.255.255.255 1.1.1.1    # Active EIP of the VPN gateway + 255.255.255.255 + Gateway address of the firewall's public IP address
   ```



```
ip route-static 2.2.2.2 255.255.255.255 1.1.1.1    # Standby EIP of the VPN gateway + 255.255.255.255 + Gateway address of the firewall's public IP address
```

b. Configure static routes to the private IP addresses of the Huawei Cloud side.

```
ip route-static 192.168.0.0 255.255.255.0 Tunnel100 1.1.1.2

ip route-static 192.168.0.0 255.255.255.0 Tunnel200 2.2.2.2
```

NOTE

- The command format is **ip route-static** *VPC subnet 1* + *Subnet mask* + *Tunnel interface number* + *Active or standby EIP of the VPN gateway*.
- If there are multiple VPC subnets, you need to configure two routes to each VPC subnet.

6. Configure a security policy.

```
ip address-set localsubnet172 type object      # Define an address object.
address 0 172.16.0.0 mask 24                   # Configure the subnet of the on-premises data center.
ip address-set HWCsubnet192 type object
address 0 192.168.0.0 mask 24                  # Configure the subnet of the Huawei Cloud VPC.

security-policy
rule name IPsec_permit1
source-zone untrust
source-zone internet
source-zone local
destination-zone untrust
destination-zone internet
destination-zone local
service ah esp
service protocol udp destination-port 500 4500
action permit
rule name IPsec_permit2
source-zone untrust
source-zone internet
source-zone trust
destination-zone untrust
destination-zone internet
destination-zone trust
source-address address-set localsubnet172
source-address address-set HWCsubnet192
destination-address address-set localsubnet172
destination-address address-set HWCsubnet192
action permit

nat-policy
rule name IPsec_subnet_bypass
source-zone trust
destination-zone untrust
destination-zone internet
source-address address-set localsubnet172
destination-address address-set HWCsubnet192
action no-nat
```

1.5.1.4 Verification

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

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

    Choose **Network** > **IPSec** > **IPSec**. The negotiation states of the two VPN connections are both **Succeeded**.

- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

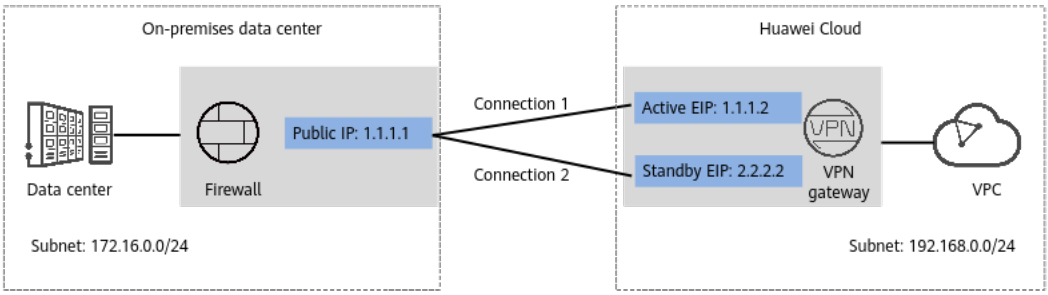
1.5.2 BGP Routing Mode

1.5.2.1 Operation Guide

Scenario

Figure 1-22 shows the typical networking where a Huawei Cloud VPN gateway connects to a Huawei firewall in an on-premises data center in BGP routing mode.

Figure 1-22 Typical networking diagram



In this scenario, the firewall has only one public IP address. A VPN connection needs to be created between the public IP address of the firewall and each of the active and standby EIPs of the Huawei Cloud VPN gateway.

Data Plan

Table 1-61 Data plan

Category	Item	Example Value for the Firewall	Example Value for the Huawei Cloud Side
VPC	Subnet	172.16.0.0/24	192.168.0.0/24
VPN gateway	Gateway IP address	1.1.1.1	Active EIP: 1.1.1.2 Standby EIP: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
	BGP ASN	64515	64512

Category	Item	Example Value for the Firewall	Example Value for the Huawei Cloud Side
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30	
	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: group 15 • IKE version: IKEv2 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address	
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH group 15 • DPD timeout period: 45s The default DPD timeout period at the Huawei Cloud side is 45 seconds, which cannot be configured. • Lifetime (s): 3600	

1.5.2.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-62 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-62 Parameters for creating a VPN gateway

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active/Standby
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-63 only describes the key parameters for creating a customer gateway. For other parameters, use their default settings.

Table 1-63 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway to permit UDP port 4500.	IP Address 1.1.1.1
BGP ASN	ASN of your on-premises data center or private network. The value must be different from the BGP ASN of the VPN gateway.	64515

Step 5 Configure VPN connections.

In this scenario, the firewall has only one public IP address. A VPN connection needs to be created between the public IP address of the firewall and each of the active and standby EIPs of the Huawei Cloud VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Set parameters as prompted.

   Table 1-64 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-64 Parameters for creating VPN connections

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **BGP routing**.	BGP routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/24
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the firewall.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– IKE Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-128 ▪ DH Algorithm: Group 15 ▪ Version: v2 ▪ Lifetime (s): 86400 ▪ Local ID: IP Address ▪ Customer ID: IP Address – IPsec Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-128 ▪ PFS: DH group 15 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 3600
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.5.2.3 Configuration on the Firewall

1. Log in to the CLI of the firewall.

   The commands may vary according to the firewall models and versions. For details, see the product documentation of the corresponding version.

2. Configure basic information.

   a. Configure IP addresses for interfaces of the firewall.

   ```
   interface GigabitEthernet1/0/1                # Configure a public IP address for an interface of the firewall.
   ip address 1.1.1.1 255.255.255.0
   interface GigabitEthernet1/0/2                # Configure a private IP address for an interface of the firewall.
   ip address 172.16.0.233 255.255.0.0
   ```

   b. Add interfaces to security zones.

   ```
   firewall zone untrust
   add interface GigabitEthernet1/0/1
   firewall zone trust
   add interface GigabitEthernet1/0/2
   ```

   c. Configures the TCP MSS.

   ```
   firewall tcp-mss 1300
   ```

3. Configure negotiation policies.

   ```
   ike proposal 100                # Configure an IKE policy for the VPN connection to be established between the public IP address of the firewall and the active EIP of the VPN gateway.
   authentication-algorithm SHA2-256     # Set the same authentication algorithm as that configured in the IKE policy in Table 1-60.
   encryption-algorithm AES-128          # Set the same encryption algorithm as that configured in the IKE policy in Table 1-60.
   authentication-method pre-share
   integrity-algorithm HMAC-SHA2-256
   prf HMAC-SHA2-256
   dh group15                      # Set the same DH algorithm as that configured in the IKE policy in Table 1-60.
   sa duration 86400                 # Set the same lifetime as that configured in the IKE policy in Table 1-60.

   ike peer hwcloud_peer33
   undo version 1                    # Set the same IKE version as that configured in the IKE policy in Table 1-60.
   pre-shared-key Test@123             # Set the same PSK as that configured in Table 1-60.
   ike-proposal 100
   remote-address 1.1.1.2              # Specify the active EIP of the VPN gateway.

   IPsec proposal IPsec-pro100         # Configure an IPsec policy for the VPN connection to be established between the public IP address of the firewall and the active EIP of the VPN gateway.
   transform esp
   encapsulation-mode tunnel
   esp authentication-algorithm SHA2-256    # Set the same authentication algorithm as that configured in the IPsec policy in Table 1-60.
   esp encryption-algorithm aes-128    # Set the same encryption algorithm as that configured in the IPsec policy in Table 1-60.
   ```



```
ike proposal 200                # Configure policies for the VPN connection to be established between the public IP address of the firewall and the standby EIP of the VPN gateway.
authentication-algorithm SHA2-256
encryption-algorithm AES-128
authentication-method pre-share
integrity-algorithm HMAC-SHA2-256
prf HMAC-SHA2-256
dh group15
sa duration 86400

ike peer hwcloud_peer44
undo version 1
pre-shared-key Test@123
ike-proposal 200
remote-address 2.2.2.2                          # Specify the standby EIP of the VPN gateway.

IPsec proposal IPsec-pro200
transform esp
encapsulation-mode tunnel
esp authentication-algorithm SHA2-256
esp encryption-algorithm aes-128
```

4. Configure IPsec tunnels.

```
IPsec profile HW-IPsec100     # Configure a routing policy for the public IP address of the firewall.
ike-peer hwcloud_peer33
proposal IPsec-pro100
pfs dh-group15                  # Set the same PFS as that configured in the IPsec policy in Table 1-60.
sa duration time-based 3600        # Set the same lifetime as that configured in the IPsec policy in Table 1-60.

interface Tunnel100
ip address 169.254.70.2 255.255.255.252       # Specify the IP address of tunnel interface 1 on the firewall.
tunnel-protocol IPsec
source 1.1.1.1                          # Specify the public IP address of the firewall.
destination 1.1.1.2                       # Specify the active EIP of the VPN gateway.
service-manage ping permit
IPsec profile HW-IPsec100
firewall zone untrust
add interface Tunnel100

IPsec profile HW-IPsec200
ike-peer hwcloud_peer44
proposal IPsec-pro200
pfs dh-group15                  # Set the same PFS as that configured in the IPsec policy in Table 1-60.
sa duration time-based 3600        # Set the same lifetime as that configured in the IPsec policy in Table 1-60.

interface Tunnel200
ip address 169.254.71.2 255.255.255.252       # Specify the IP address of tunnel interface 2 on the firewall.
tunnel-protocol IPsec
source 1.1.1.1                          # Specify the public IP address of the firewall.
destination 2.2.2.2                       # Specify the standby EIP of the VPN gateway.
service-manage ping permit
IPsec profile HW-IPsec200
firewall zone untrust
add interface Tunnel200
```

5. Configure routes.
   a. Configure static routes to the public IP addresses of the Huawei Cloud side.

```
ip route-static 1.1.1.2 255.255.255.255 1.1.1.1    # Active EIP of the VPN gateway + 255.255.255.255 + Gateway address of the firewall's public IP address
ip route-static 2.2.2.2 255.255.255.255 1.1.1.1    # Standby EIP of the VPN gateway + 255.255.255.255 + Gateway address of the firewall's public IP address
```

   b. Configure BGP peers and BGP routes.

```
bgp 64515
 router-id 1.1.1.1
```



```
private-4-byte-as enable
peer 169.254.70.1 as-number 64512
peer 169.254.70.1 connect-interface Tunnel100
peer 169.254.71.1 as-number 64512
peer 169.254.71.1 connect-interface Tunnel200
#
ipv4-family unicast
 network 172.16.0.0 255.255.255.0
 peer 169.254.70.1 enable
 peer 169.254.71.1 enable
```

6. Configure a security policy.

```
ip address-set localsubnet172 type object          # Define an address object.
address 0 172.16.0.0 mask 16                       # Configure the subnet of the on-premises data center.
ip address-set HWCsubnet192 type object
address 0 192.168.0.0 mask 24                      # Configure the subnet of the Huawei Cloud VPC.
address 0 192.168.1.0 mask 24

security-policy
rule name IPsec_permit1
source-zone untrust
source-zone internet
source-zone local
destination-zone untrust
destination-zone internet
destination-zone local
service ah esp
service protocol udp destination-port 500 4500
action permit
rule name IPsec_permit2
source-zone untrust
source-zone internet
source-zone trust
destination-zone untrust
destination-zone internet
destination-zone trust
source-address address-set localsubnet172
source-address address-set HWCsubnet192
destination-address address-set localsubnet172
destination-address address-set HWCsubnet192
action permit

nat-policy
rule name IPsec_subnet_bypass
source-zone trust
destination-zone untrust
destination-zone internet
source-address address-set localsubnet172
destination-address address-set HWCsubnet192
action no-nat
```

1.5.2.4 Verification

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

  Huawei Cloud

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

- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

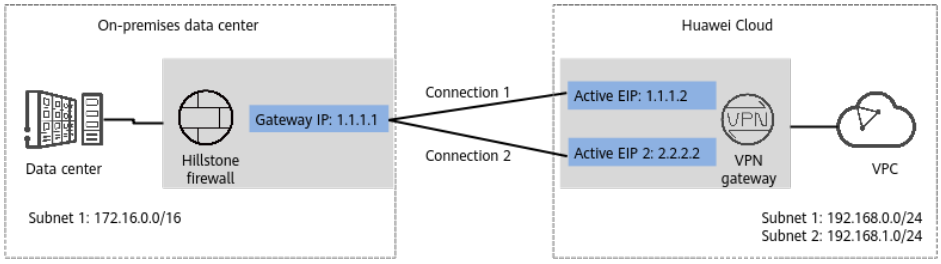
1.6 Interconnection with a Hillstone Firewall

1.6.1 Static Routing Mode

1.6.1.1 Scenario

Figure 1-23 shows the typical networking where a Huawei Cloud VPN gateway connects to a Hillstone firewall in an on-premises data center in static routing mode.

Figure 1-23 Typical networking diagram



In this scenario, the Hillstone firewall has only one IP address, and the Huawei Cloud VPN gateway uses the active-active mode. A VPN connection needs to be created between each of the two active EIPs of the VPN gateway and the IP address of the Hillstone firewall.

Limitations and Constraints

- Hillstone firewalls support only IKEv1 policies.
- Huawei Cloud VPN and Hillstone firewalls support different authentication and encryption algorithms. When creating connections, ensure that the policy configurations at both ends are the same.

1.6.1.2 Data Plan

Table 1-65 Data plan

Category	Item	Example Value for the Hillstone Firewall	Example Value for the Huawei Cloud Side
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 on the Hillstone firewall)	Active EIP: 1.1.1.2 Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24

Category	Item	Example Value for the Hillstone Firewall	Example Value for the Huawei Cloud Side
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30	
	IKE Policy	• Version: v1 • Negotiation mode: main • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • DH algorithm: group 15 • Lifetime (s): 86400 • Local ID: FQDN • Peer ID: FQDN	
	IPsec Policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • PFS: DH group 15 • Lifetime (s): 28800	

1.6.1.3 Configuration on the Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-66 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-66 VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

1. Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.

2. Set parameters as prompted.

   Table 1-67 describes the parameters for creating a customer gateway.

Table 1-67 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-hillstone
Identifier	Select **IP Address**, and enter the IP address used by the Hillstone firewall to communicate with the Huawei Cloud VPN gateway.	IP Address 1.1.1.1

Step 5 Configure VPN connections.

In this scenario, the customer gateway has only one IP address. It is recommended that the VPN gateway on Huawei Cloud use the active-active mode. In this case, a VPN connection needs to be created between each of the two active EIPs of the VPN gateway and the IP address of the customer gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Set parameters as prompted.

   The following table only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-68 Parameters for creating a VPN connection

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Static routing**.	Static routing

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/24
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, health check, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30

Parameter	Description	Value
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets. The VPN gateway can automatically perform NQA detection on the peer interface address that has been configured on the customer gateway.	NQA enabled
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– IKE Policy ▪ Version: v1 ▪ Negotiation Mode: Main ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-256 ▪ DH Algorithm: Group 15 ▪ Lifetime (s): 86400 ▪ Local ID: FQDN(hwvpn.abc.efg) ▪ Customer ID: FQDN(hillstone.abc.efg) – IPsec Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-256 ▪ PFS: DH group 15 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 28800

Parameter	Description	Value
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.6.1.4 Configuration on the Hillstone Firewall

Prerequisites

The basic network configuration of the Hillstone firewall has been completed.

Procedure

1. Log in to the configuration page.

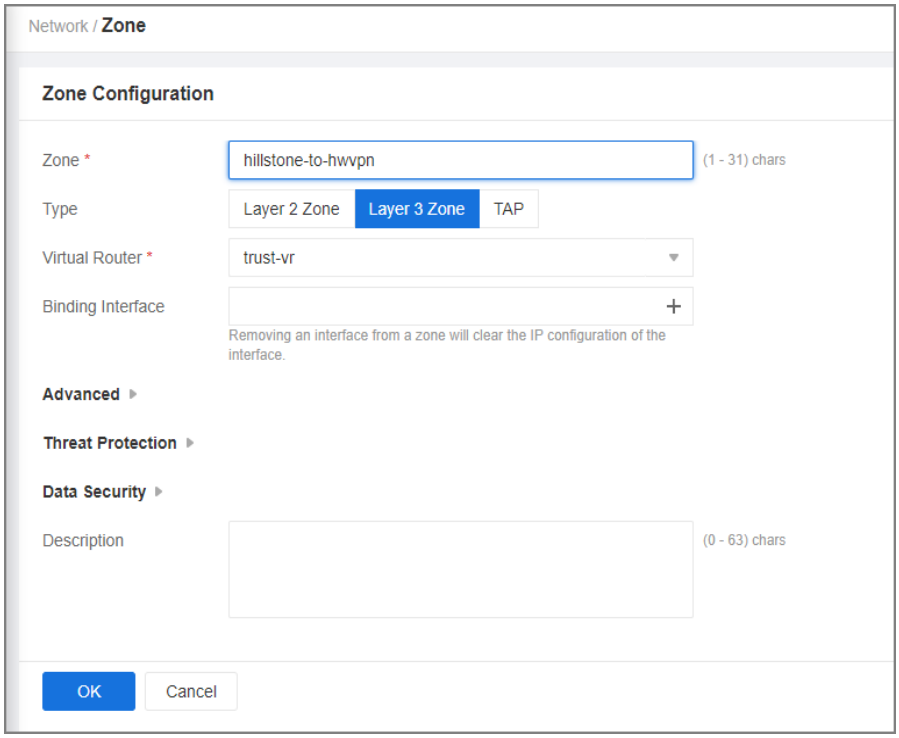
   A firewall running the 5.5R9 version is used as an example. The configuration pages may vary according to the firewall models and software versions.

2. Complete basic settings.

   a. Configure a security zone.

   Choose **Network** > **Zone**. Click **New** and set parameters, as shown in **Figure 1-24**.

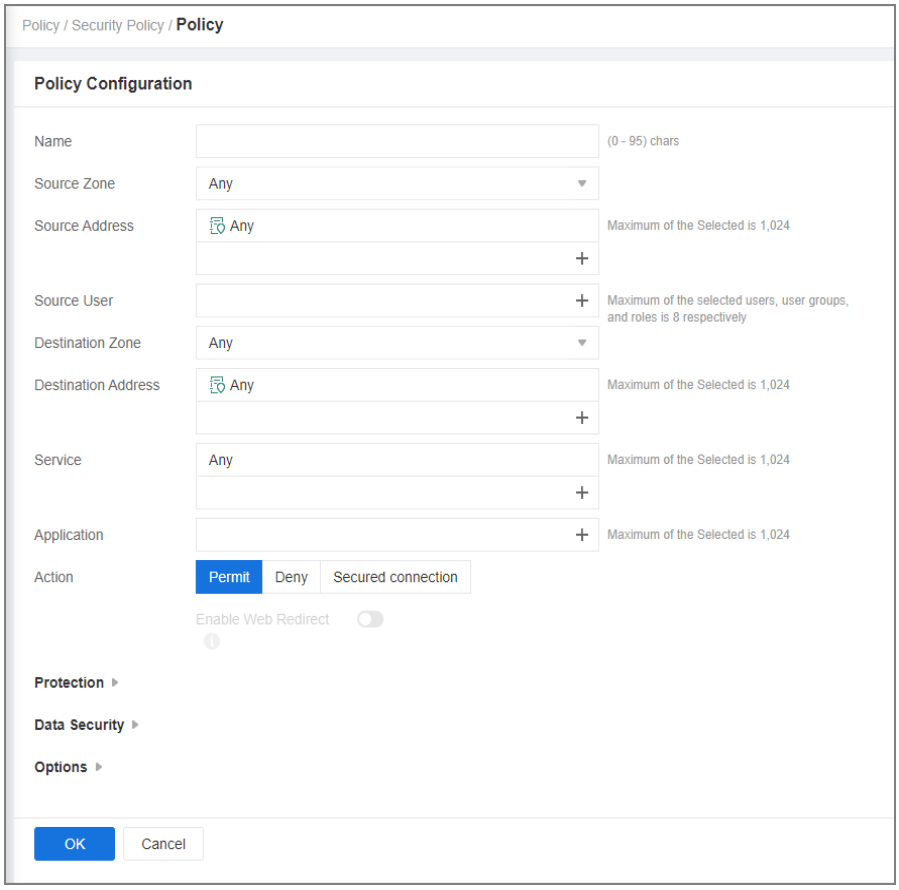
Figure 1-24 Configuring a security zone



b. Configure a security policy.

Choose **Policy** > **Security Policy** > **Policy**. Click **New**, choose **Policy**, and set parameters, as shown in **Figure 1-25**.

Figure 1-25 Configuring a policy



c. Configure a basic route.

i. Choose **Network** > **Routing** > **Destination Route**, and click **New**.

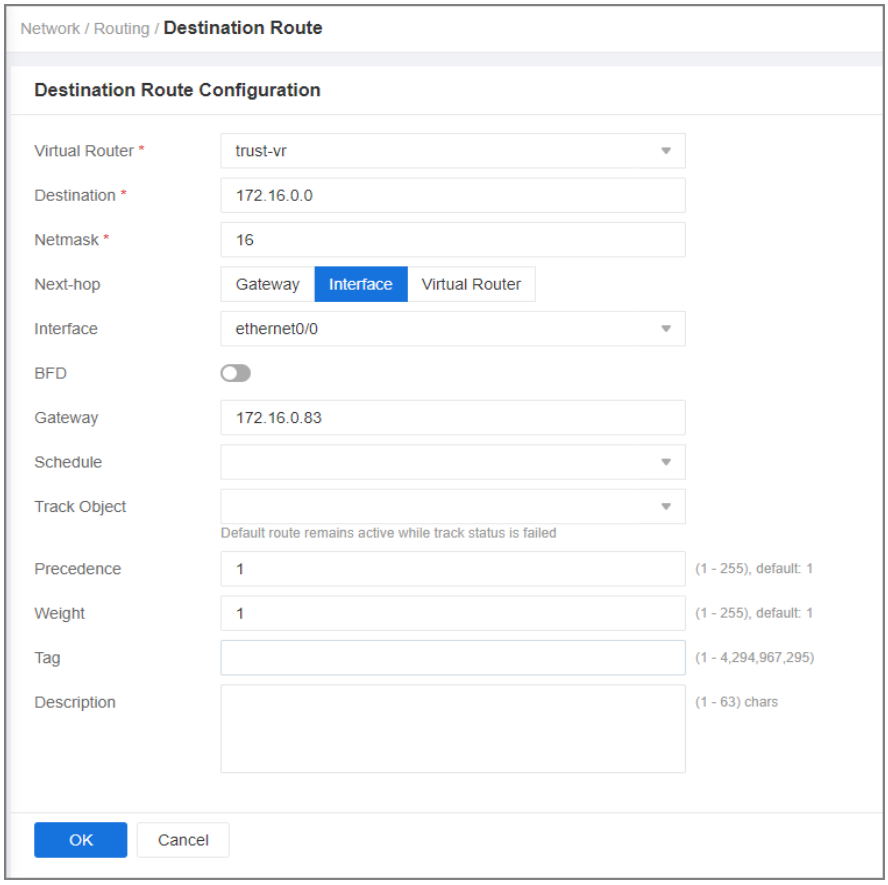
ii. In **Destination Route**, add a static route to the VPC of the Hillstone firewall.

iii. Set **Next-hop** to an interface of the Hillstone firewall.

iv. Set **Gateway** to the subnet gateway address for the private IP address of the Hillstone firewall's interface.

Figure 1-26 shows the key parameter settings.

Figure 1-26 Configuring a destination route



v. Click **OK**.

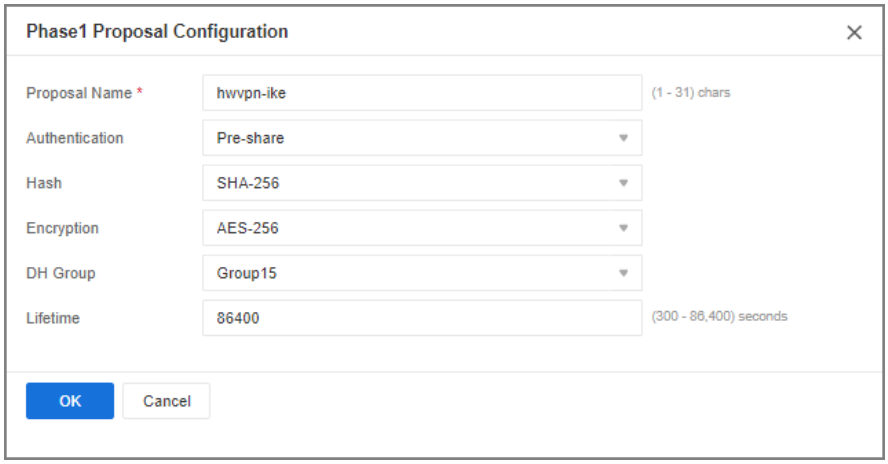
3. Configure VPN connections.

   a. Choose **Network** > **VPN** > **IPSec VPN**. On the **IPsec VPN** tab page, click **New**.

   b. Click the plus sign (+) in the **Peer Name** drop-down list box to add peer information.

   c. Click the plus sign (+) in the **Proposal1** drop-down list box to create a phase-1 proposal. Set parameters and click **OK**. **Figure 1-27** shows the key parameter settings.

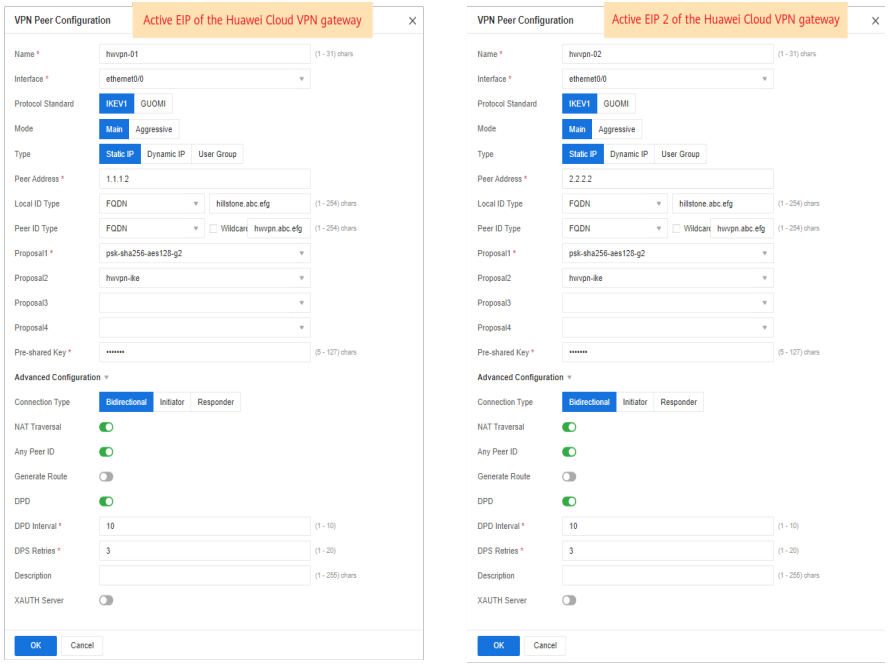
Figure 1-27 Configuring a phase-1 proposal



d. Configure VPN peers. As the Huawei Cloud VPN gateway has two EIPs bound, you need to configure two peers.

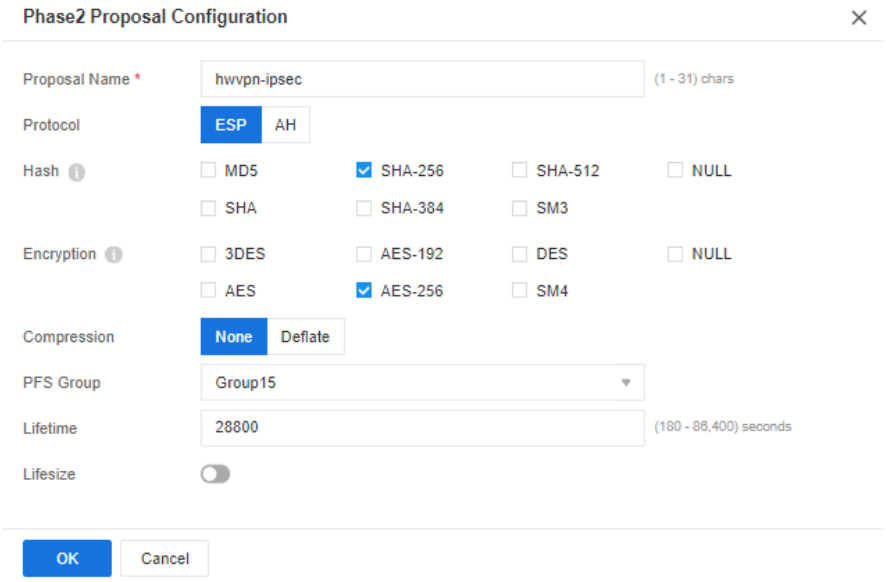
Select the phase-1 proposal created in **c** from the **Proposal1** drop-down list box. Click **Advanced Configuration**, toggle on **NAT Traversal** and **DPD**, and click **OK**.

Figure 1-28 Configuring VPN peers



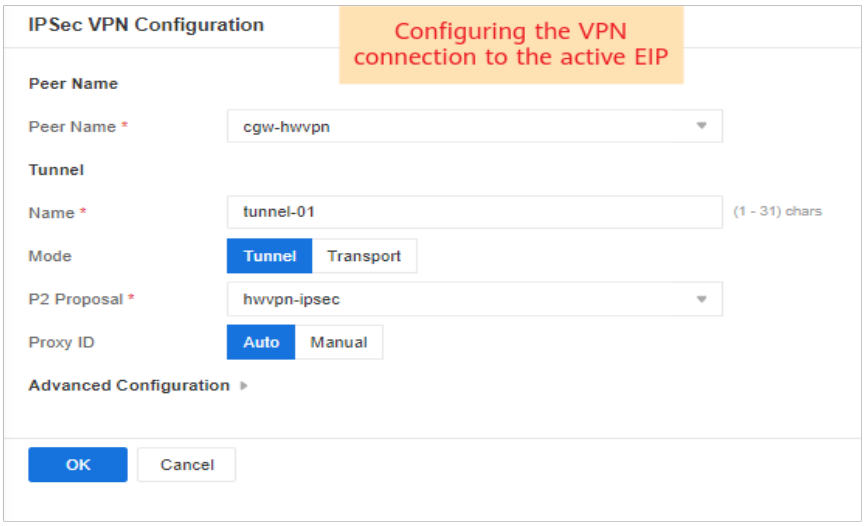
e. Click the plus sign (+) in the **P2 Proposal** drop-down list box to create a phase-2 proposal. Set parameters and click **OK**. **Figure 1-29** shows the key parameter settings.

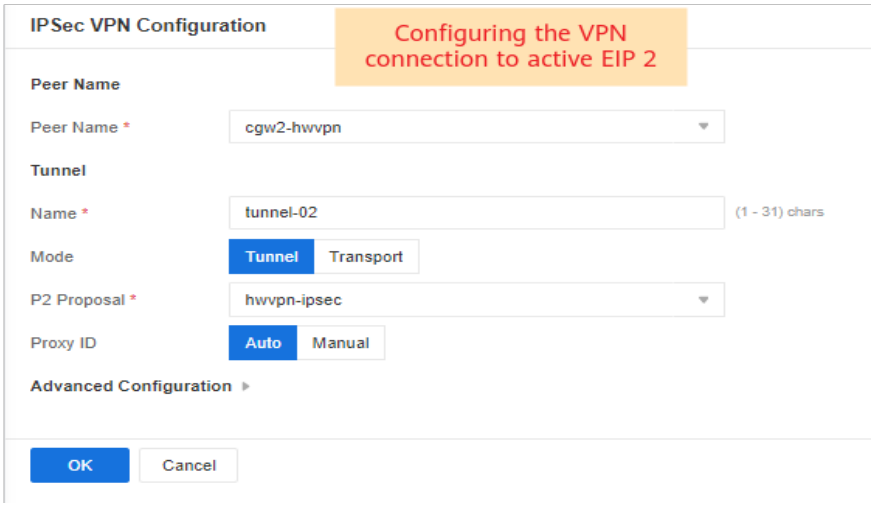
Figure 1-29 Configuring a phase-2 proposal



f. Configure VPN connection information. Select each of the VPN peers created in **d** from the **Peer Name** drop-down list box, select the phase-2 proposal created in **e** from the **P2 Proposal** drop-down list box, and click **OK**.

Figure 1-30 Configuring IPsec VPN

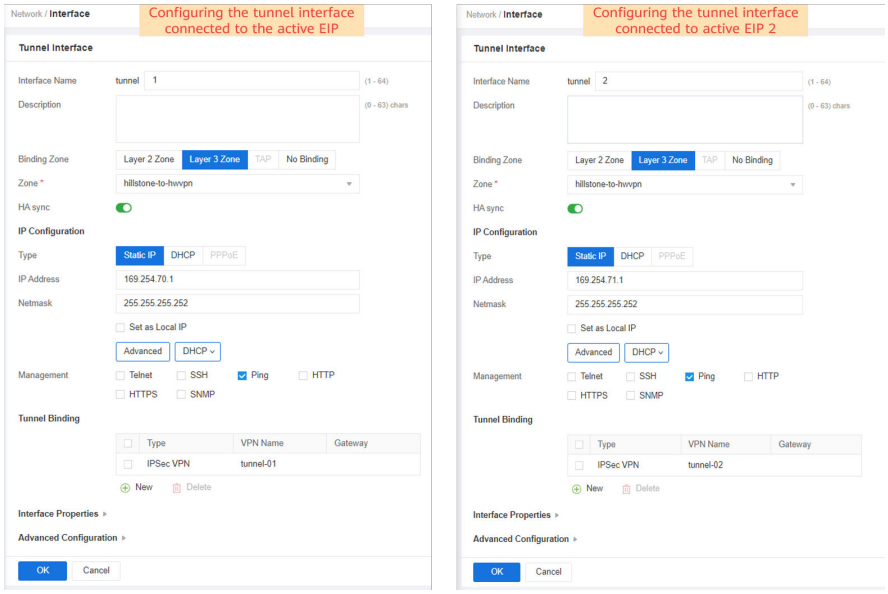




4. Configure tunnel interfaces.
   a. Choose **Network** > **Interface**, click **New**, and choose **Tunnel Interface**.
   b. Configure two tunnel interfaces. **Figure 1-31** shows the key parameter settings.

      Select the security zone created in **a** from the **Zone** drop-down list box, and select each of the two tunnel names configured in **f** for **VPN Name**.

Figure 1-31 Configuring tunnel interfaces

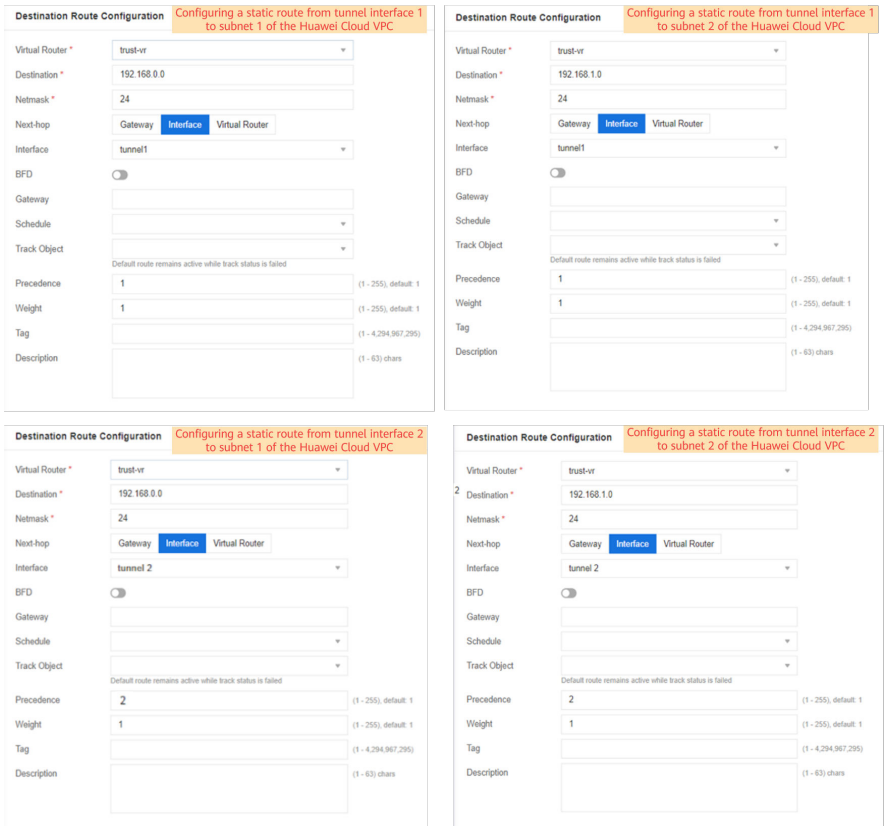


5. Configure service routes.
   a. Choose **Network** > **Routing** > **Destination Route**, and click **New**.
   b. Configure static routes from the Hillstone firewall to the Huawei Cloud VPC.

      In this example, the Hillstone firewall communicates with the Huawei Cloud VPC through two tunnels, and the Huawei Cloud VPC has two subnets. As such, you need to configure four static routes, as shown in **Figure 1-32**.

      Static routes 3 and 4 have the same destination addresses as static routes 1 and 2, respectively, but have lower priorities. In this way, static routes 3 and 4 are inactive after being configured.

Figure 1-32 Configuring service routes



1.6.1.5 Verification

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

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

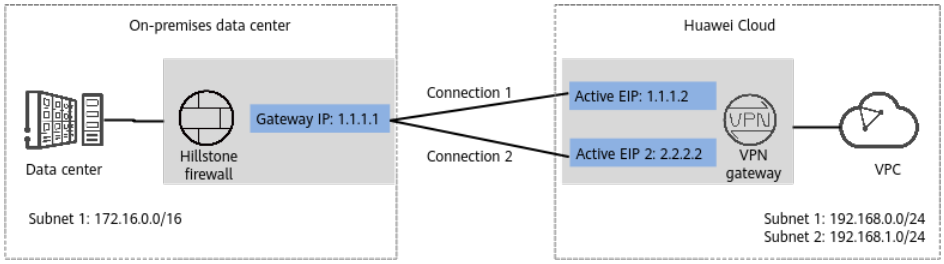
    Choose **Network** > **VPN** > **IPSec VPN**. The states of the two VPN connections are normal.
- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnet can ping each other.

1.6.2 BGP Routing Mode

1.6.2.1 Scenario

Figure 1-33 shows the typical networking where a Huawei Cloud VPN gateway connects to a Hillstone firewall in an on-premises data center in BGP routing mode.

Figure 1-33 Typical networking diagram



In this scenario, the Hillstone firewall has only one IP address, and the Huawei Cloud VPN gateway uses the active-active mode. A VPN connection needs to be created between each of the two active EIPs of the VPN gateway and the IP address of the Hillstone firewall.

Limitations and Constraints

- Hillstone firewalls support only IKEv1 policies.
- Huawei Cloud VPN and Hillstone firewalls support different authentication and encryption algorithms. When creating connections, ensure that the policy settings at both ends are the same.

1.6.2.2 Data Plan

Table 1-69 Data plan

Category	Item	Example Value	Example Value for the Huawei Cloud Side
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 on the Hillstone firewall)	Active EIP: 1.1.1.2 Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
	BGP ASN	64515	64512
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30	

Category	Item	Example Value	Example Value for the Huawei Cloud Side
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30	
	IKE policy	• Version: v1 • Negotiation mode: main • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • DH algorithm: group 15 • Lifetime (s): 86400 • Local ID: FQDN • Peer ID: FQDN	
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • PFS: DH group 15 • Lifetime (s): 28800	

1.6.2.3 Configuration on the Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   The following table only describes the key parameters for creating a VPN gateway.

Table 1-70 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   The following table only describes the key parameters for creating a customer gateway. For other parameters, use their default settings.

Table 1-71 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-hillstone

Parameter	Description	Value
Identifier	Select **IP Address**, and enter the IP address used by the Hillstone firewall to communicate with the Huawei Cloud VPN gateway.	IP Address 1.1.1.1
BGP ASN	BGP AS number.	64515

Step 5 Configure VPN connections.

In this scenario, a VPN connection is created between the Hillstone firewall and the primary EIP of the Huawei Cloud VPN gateway, and another VPN connection is created between the Hillstone firewall and the secondary EIP of the Huawei Cloud VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Set parameters as prompted.

   The following table only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-72 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **BGP routing**.	BGP routing

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/24
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the firewall.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– IKE Policy ▪ Version: v1 ▪ Negotiation Mode: Main ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-256 ▪ DH Algorithm: Group 15 ▪ Lifetime (s): 86400 ▪ Local ID: FQDN(hwvpn.abc.efg) ▪ Customer ID: FQDN(hillstone.abc.efg) – IPsec Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-256 ▪ PFS: DH group 15 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 28800

Parameter	Description	Value
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.6.2.4 Configuration on the Hillstone Firewall

Prerequisites

The basic network configuration of the Hillstone firewall has been completed.

Procedure

1. Log in to the configuration page.

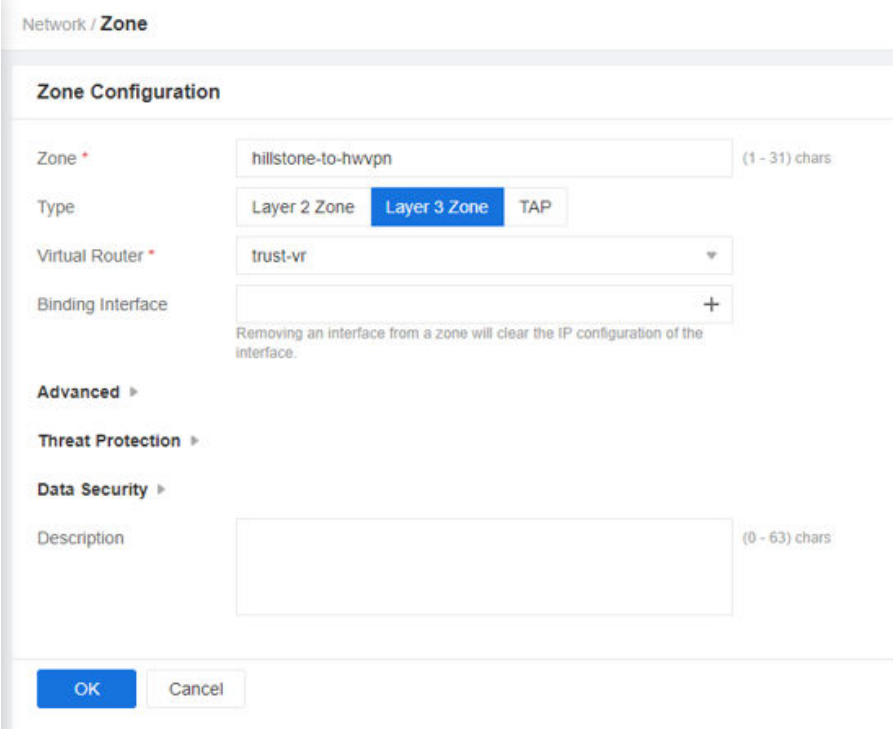
   A firewall running the 5.5R9 version is used as an example. The configuration pages may vary according to the firewall models and software versions.

2. Complete basic settings.

   a. Configure a security zone.

   Choose **Network** > **Zone**. Click **New** and set parameters, as shown in **Figure 1-34**.

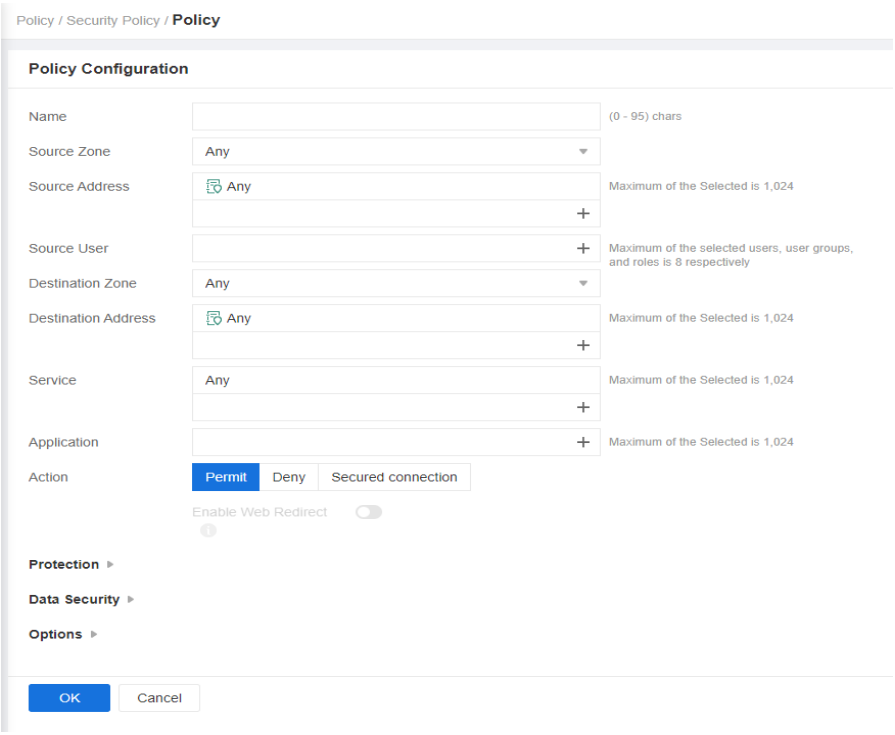
Figure 1-34 Configuring a security zone



b. Configure a security policy.

Choose **Policy** > **Security Policy** > **Policy**. Click **New**, choose **Policy**, and set parameters, as shown in **Figure 1-35**.

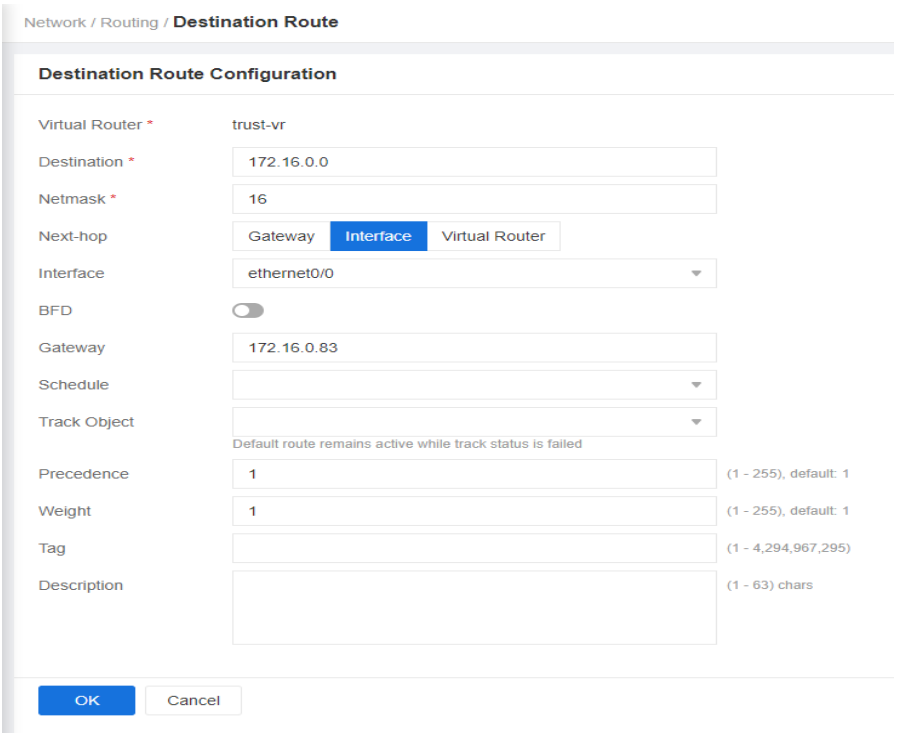
Figure 1-35 Configuring a policy



c. Configure a basic route.

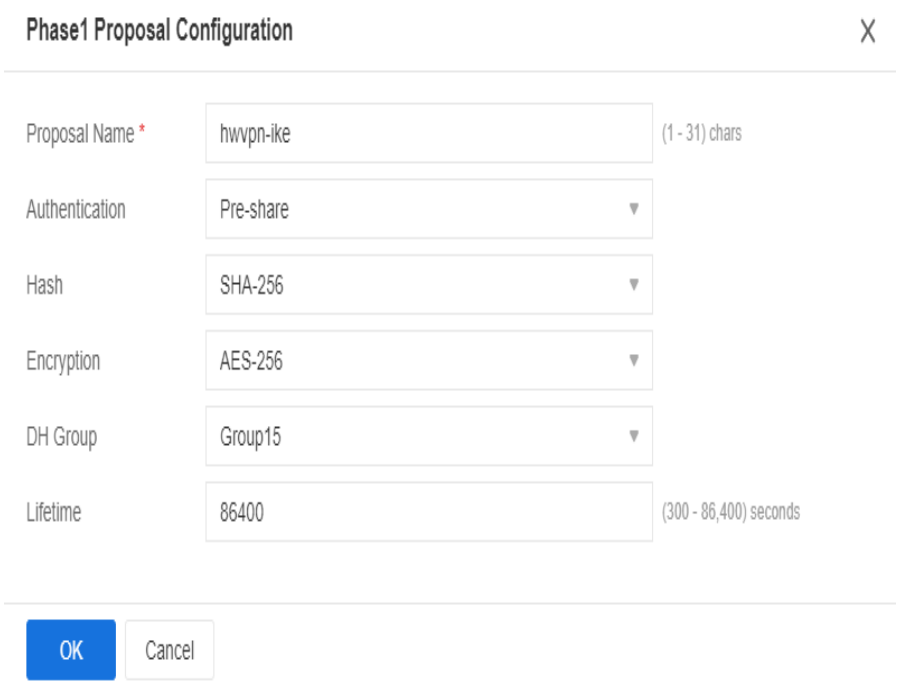
Choose **Network** > **Routing** > **Destination Route**. Click **New** and set parameters, as shown in **Figure 1-36**.

Figure 1-36 Configuring a destination route



3. Configure VPN connections.
   a. Choose **Network** > **VPN** > **IPSec VPN**. On the **IPsec VPN** tab page, click **New**.
   b. Click the plus sign (+) in the **Peer Name** drop-down list box to add peer information.
   c. Click the plus sign (+) in the **Proposal1** drop-down list box to create a phase-1 proposal. Set parameters and click **OK**. **Figure 1-37** shows the key parameter settings.

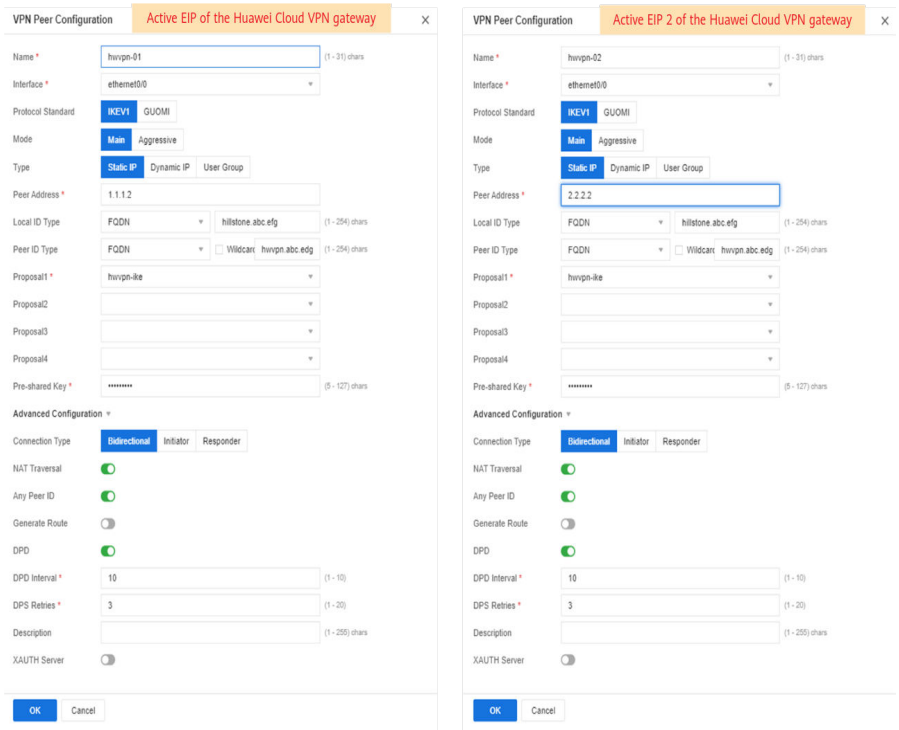
Figure 1-37 Configuring a phase-1 proposal



d. Configure VPN peers. As the Huawei Cloud VPN gateway has two EIPs bound, you need to configure two peers.

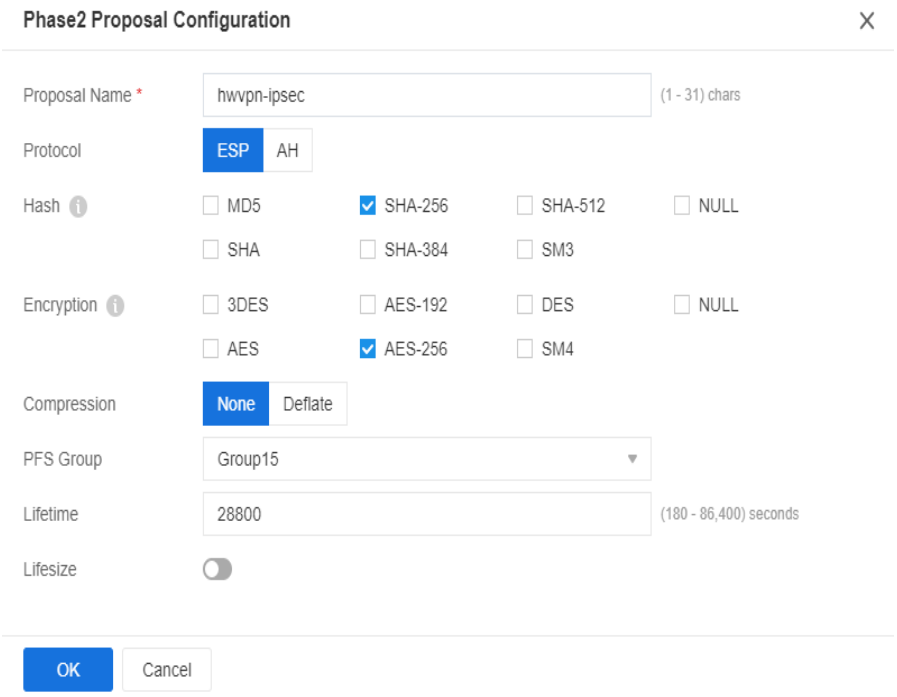
Select the phase-1 proposal created in **c** from the **Proposal1** drop-down list box. Click **Advanced Configuration**, toggle on **NAT Traversal** and **DPD**, and click **OK**.

Figure 1-38 Configuring VPN peers



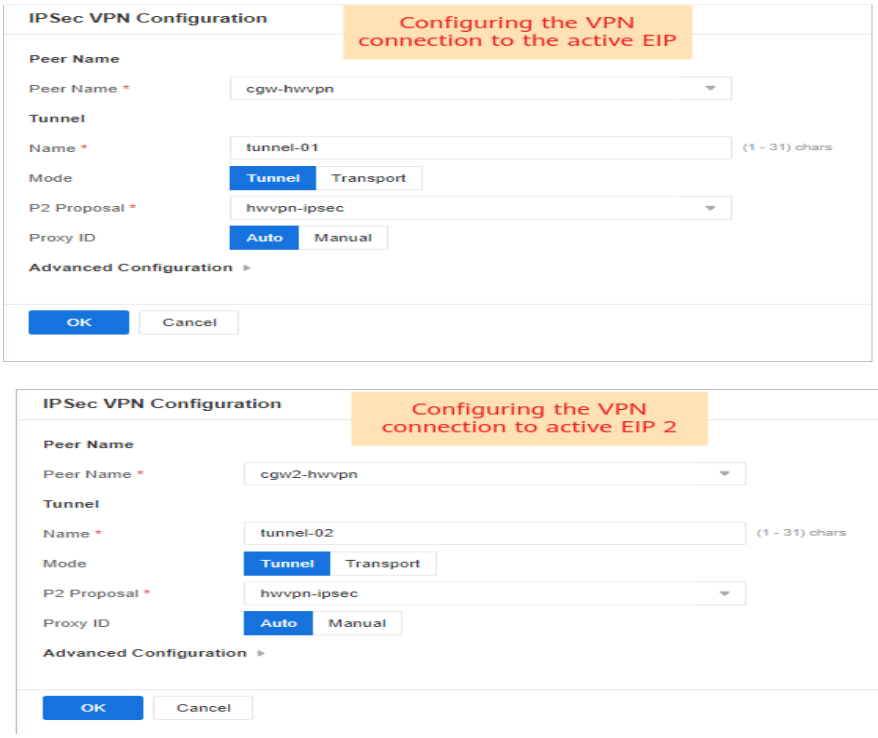
e. Click the plus sign (+) in the **P2 Proposal** drop-down list box to create a phase-2 proposal. Set parameters and click **OK**. **Figure 1-39** shows the key parameter settings.

Figure 1-39 Configuring a phase-2 proposal



f. Configure VPN connection information. Select each of the VPN peers created in **d** from the **Peer Name** drop-down list box, select the phase-2 proposal created in **e** from the **P2 Proposal** drop-down list box, and click **OK**.

Figure 1-40 Configuring IPsec VPN



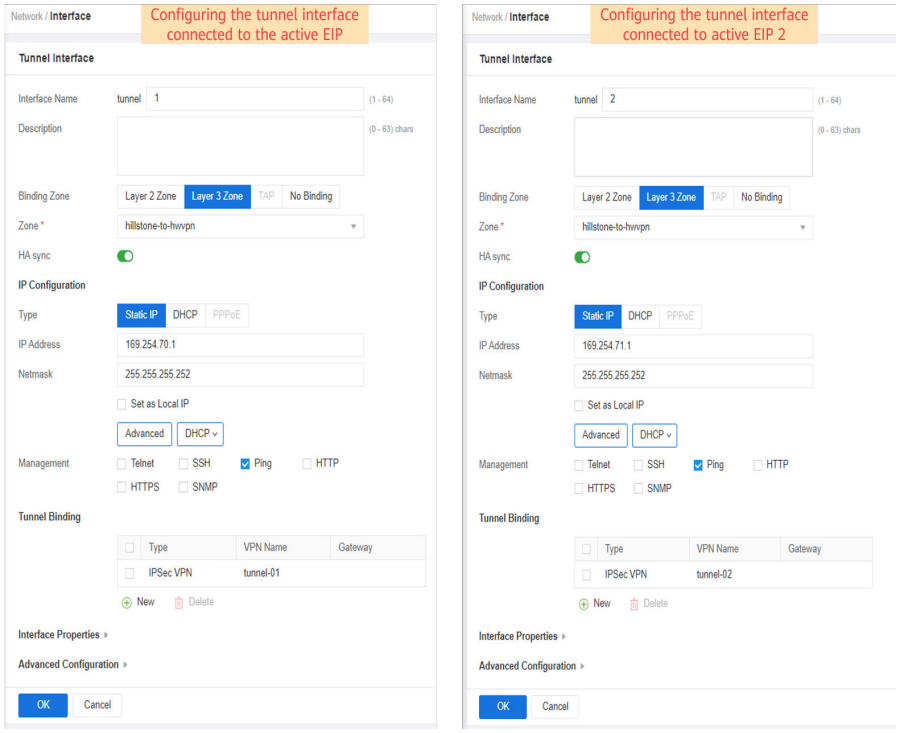
4. Configure tunnel interfaces.
   a. Choose **Network** > **Interface**, click **New**, and choose **Tunnel Interface**.
   b. Configure two tunnel interfaces. **Figure 1-41** shows the key parameter settings.

      Select the security zone created in **a** from the **Zone** drop-down list box, and select each of the two tunnel names configured in **f** for **VPN Name**.

      NOTE

      In the **Tunnel Binding** area, the gateway address must be set to the IP address of the peer tunnel interface. Otherwise, traffic cannot be forwarded.

Figure 1-41 Configuring tunnel interfaces

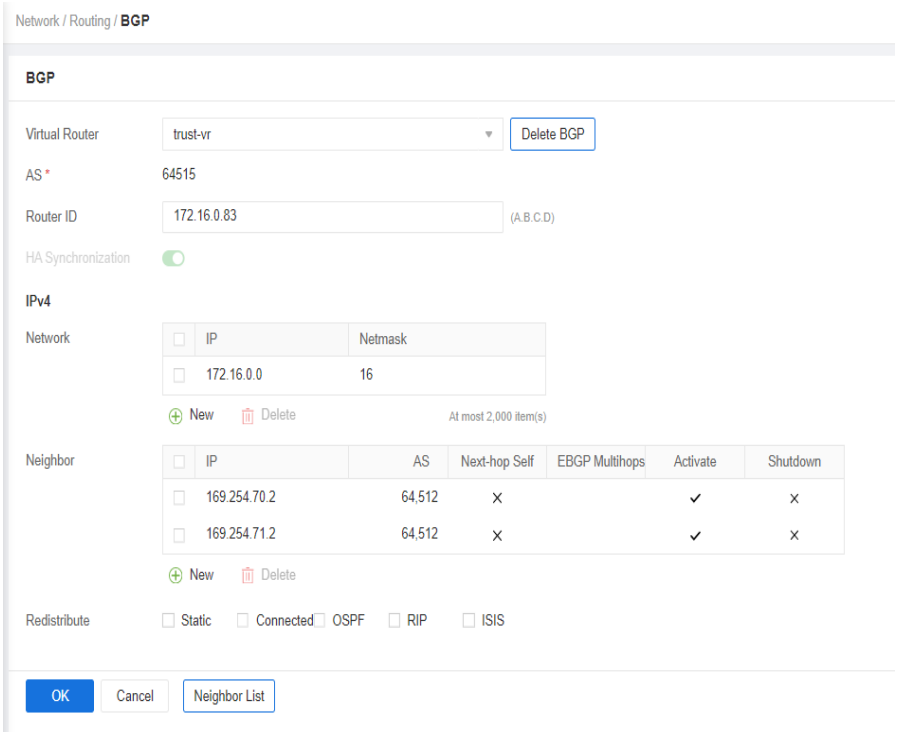


5. Configure BGP.

   Choose **Network** > **Routing** > **BGP**, and complete the BGP configuration, as shown in **Figure 1-42**.

   Set **Router ID** to the gateway address of the downlink private network interface on the Hillstone firewall, **Network** to the CIDR block of the on-premises data center, and **Neighbor** to each of the two peer tunnel interfaces.

Figure 1-42 Configuring BGP



1.6.2.5 Verification

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

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

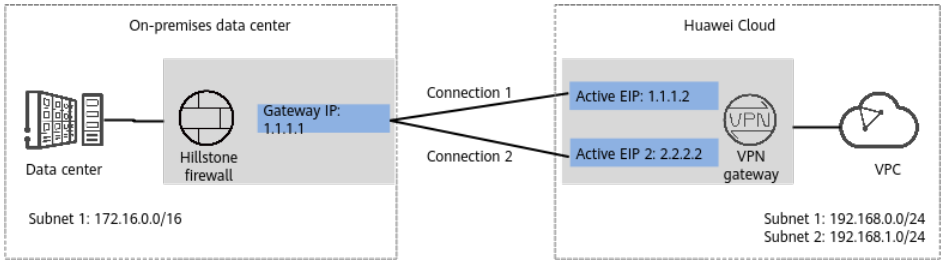
    Choose **Network** > **VPN** > **IPSec VPN**. The states of the two VPN connections are normal.
- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnet can ping each other.

1.6.3 Policy-based Mode

1.6.3.1 Scenario

Figure 1-43 shows the typical networking where a Huawei Cloud VPN gateway connects to a Hillstone firewall in an on-premises data center in policy-based mode.

Figure 1-43 Typical networking diagram



In this scenario, the Hillstone firewall has only one IP address, and the Huawei Cloud VPN gateway uses the active-active mode. A VPN connection needs to be created between each of the two active EIPs of the VPN gateway and the IP address of the Hillstone firewall.

Limitations and Constraints

- Hillstone firewalls support only IKEv1 policies.
- Huawei Cloud VPN and Hillstone firewalls support different authentication and encryption algorithms. When creating connections, ensure that the policy settings at both ends are the same.

1.6.3.2 Data Plan

Table 1-73 Data plan

Category	Item	Example of Hillstone Firewall Planning	Example of Huawei Cloud 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 on the Hillstone firewall)	• Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2
	Interconnection subnet	-	192.168.2.0/24
VPN connection	IKE policy	• Version: v1 • Negotiation mode: main • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • DH algorithm: Group 15 • Lifetime (s): 86400 • Local ID: FQDN • Peer ID: FQDN	

Category	Item	Example of Hillstone Firewall Planning	Example of Huawei Cloud Planning
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • PFS: DH group 15 • Lifetime (s): 28800	

1.6.3.3 Configuration on the Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   The following table only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-74 VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24

Parameter	Description	Value
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active-active
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   The following table only describes the key parameters for creating a customer gateway. For other parameters, use their default settings.

   Table 1-75 Customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-hillstone
Identifier	Select **IP Address**, and enter the IP address used by the Hillstone firewall to communicate with the Huawei Cloud VPN gateway.	IP Address 1.1.1.1

Step 5 Configure VPN connections.

In this scenario, a VPN connection is established between the Hillstone firewall and the primary EIPs of the Huawei Cloud VPN gateway and primary EIP2.

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

   The following table only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-76 VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Policy-based**.	Policy-based
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the health check, PSK, confirm PSK, and policies for the VPN gateway IP address of connection 1.	*Set parameters based on the site requirements.*
PSK, Confirm PSK	The value must be the same as the PSK configured on the Hillstone firewall.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Policy	A policy rule defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. – Source CIDR Block The source CIDR block must contain some local subnets. 0.0.0.0/0 indicates any address. – Destination CIDR Block The destination CIDR block must contain all customer subnets.	– Source CIDR block 1: 192.168.0.0/24 – Destination CIDR block 1: 172.16.0.0/16 – Source CIDR block 2: 192.168.1.0/24 – Destination CIDR block 2: 172.16.0.0/16

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the Hillstone firewall.	– IKE Policy ▪ Version: v1 ▪ Negotiation Mode: Main ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-256 ▪ DH Algorithm: Group 15 ▪ Lifetime (s): 86400 ▪ Local ID: FQDN(hwvpn.abc.efg) ▪ Customer ID: FQDN(hillstone.abc.efg) – IPsec Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-256 ▪ PFS: DH group 15 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 28800
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** It is recommended that the configuration of connection 2 be the same as that of connection 1.	Enabled

----End

1.6.3.4 Configuration on the Hillstone Firewall

Prerequisites

The basic network configuration of the Hillstone firewall has been completed.

Procedure

1. Log in to the configuration page.

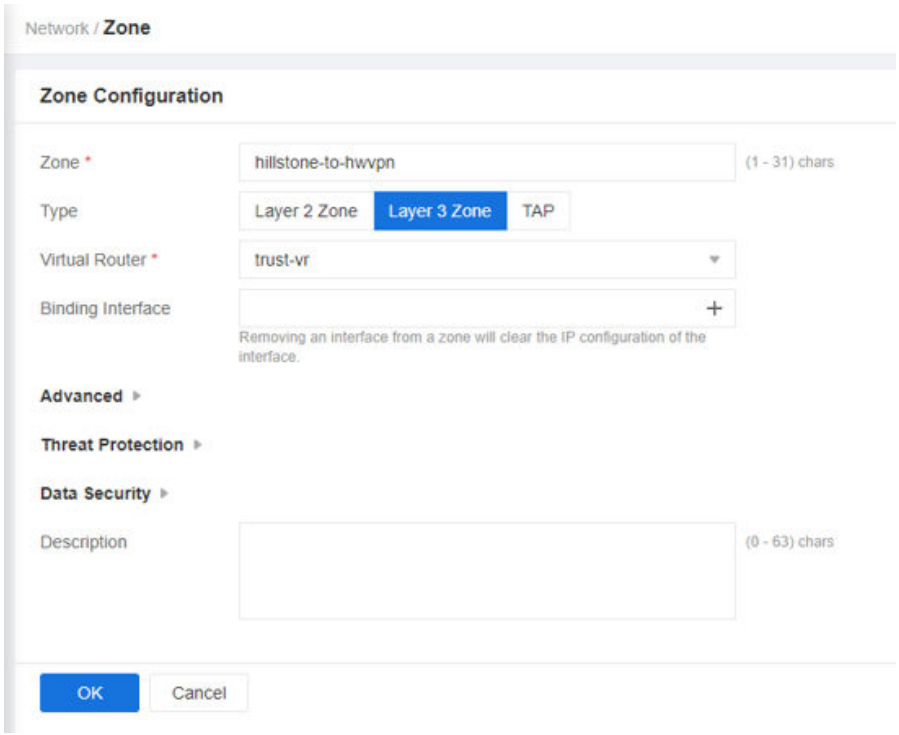
   A firewall running the 5.5R9 version is used as an example. The configuration pages may vary according to the firewall models and software versions.

2. Complete basic settings.

   a. Configure a security zone.

   Choose **Network** > **Zone**. Click **New** and set parameters, as shown in **Figure 1-44**.

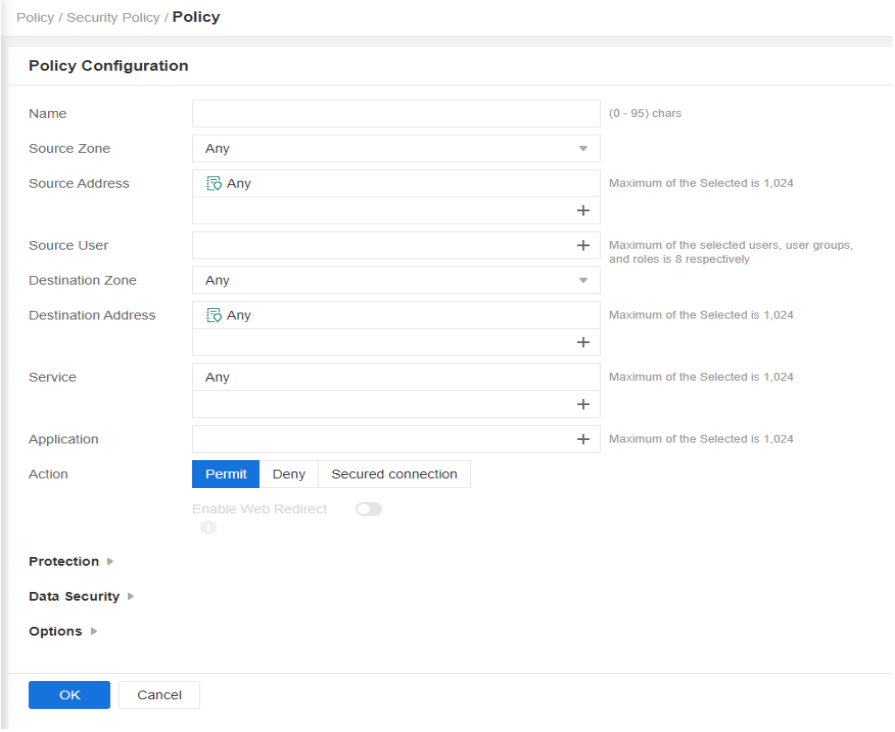
   Figure 1-44 Configuring a security zone



   b. Configure a security policy.

   Choose **Policy** > **Security Policy** > **Policy**. Click **New**, choose **Policy**, and set parameters, as shown in **Figure 1-45**.

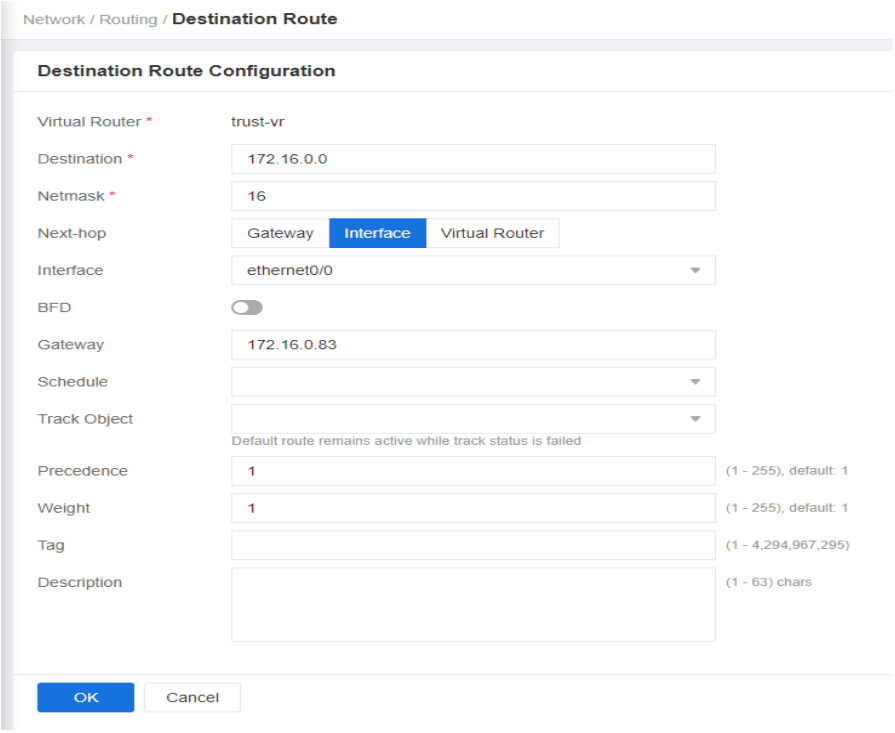
Figure 1-45 Configuring a policy



c. Configure a basic route.

Choose **Network** > **Routing** > **Destination Route**. Click **New** and set parameters, as shown in **Figure 1-46**.

Figure 1-46 Configuring a destination route

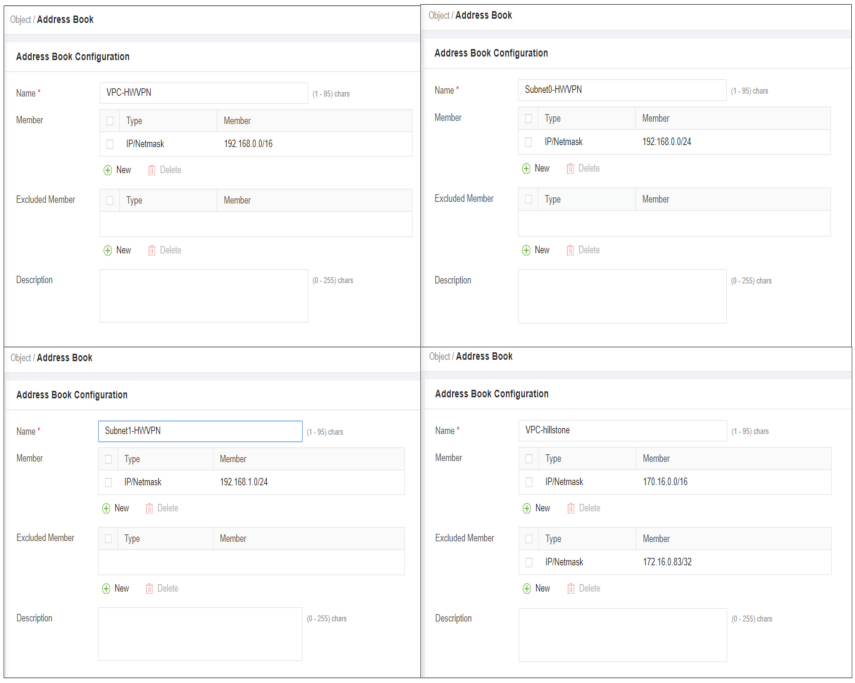


d. Configure CIDR block information.

Choose **Object** > **Address Book**. Click **New**, and configure CIDR block information of Huawei Cloud and the on-premises data center in sequence.

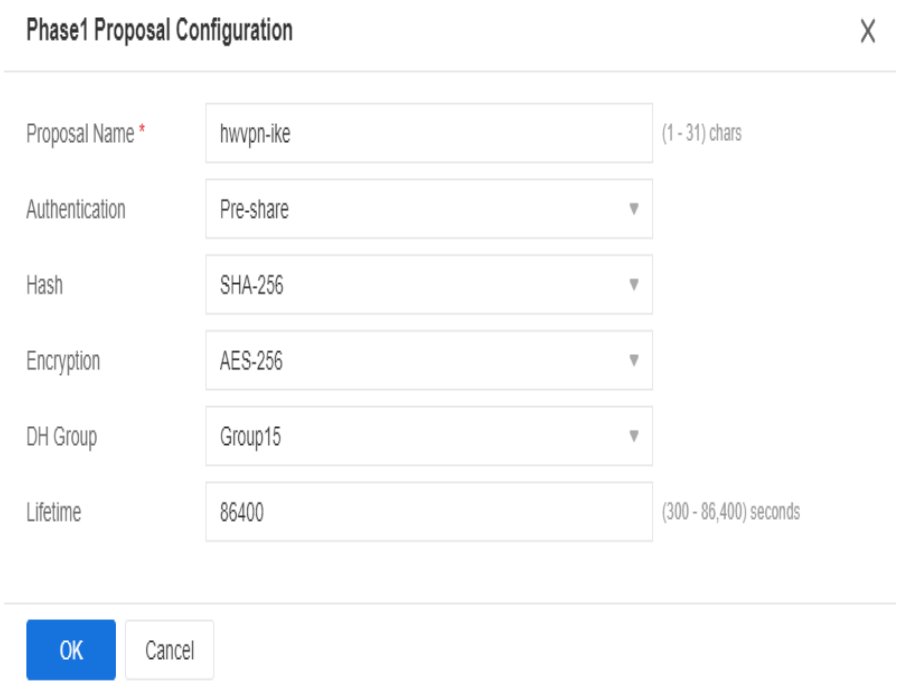
When configuring CIDR block information of the on-premises data center, exclude the gateway address of the downlink private network interface on the Hillstone firewall.

Figure 1-47 Configuring CIDR block information



3. Configure VPN connections.
   a. Choose **Network** > **VPN** > **IPSec VPN**. On the **IPsec VPN** tab page, click **New**.
   b. Click the plus sign (+) in the **Peer Name** drop-down list box to add peer information.
   c. Click the plus sign (+) in the **Proposal1** drop-down list box to create a phase-1 proposal. Set parameters and click **OK**. **Figure 1-48** shows the key parameter settings.

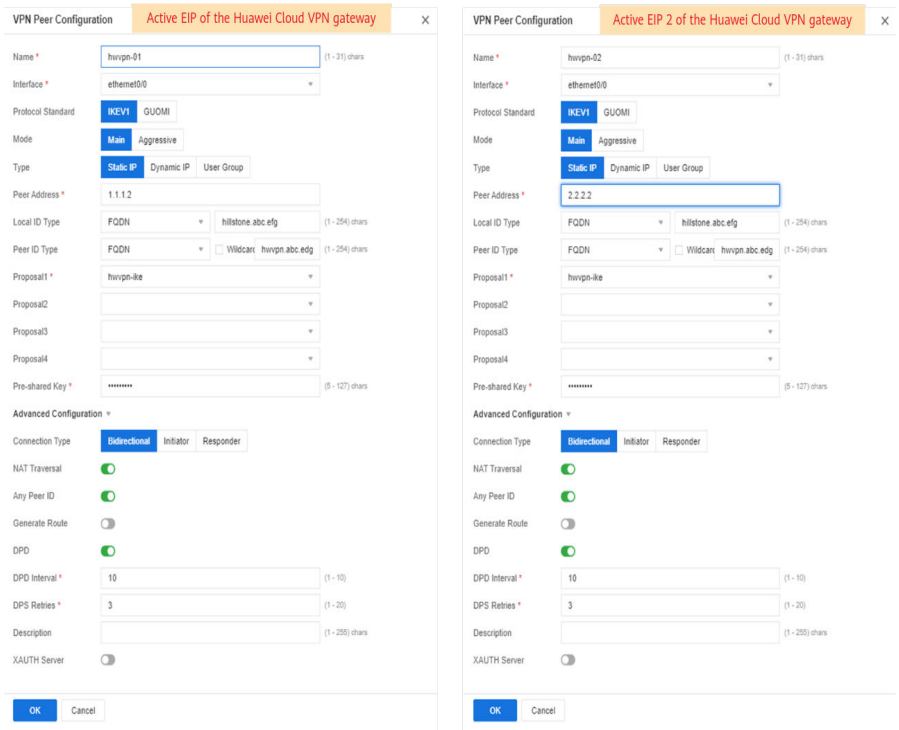
Figure 1-48 Configuring a phase-1 proposal



d. Configure VPN peers. As the Huawei Cloud VPN gateway has two EIPs bound, you need to configure two peers.

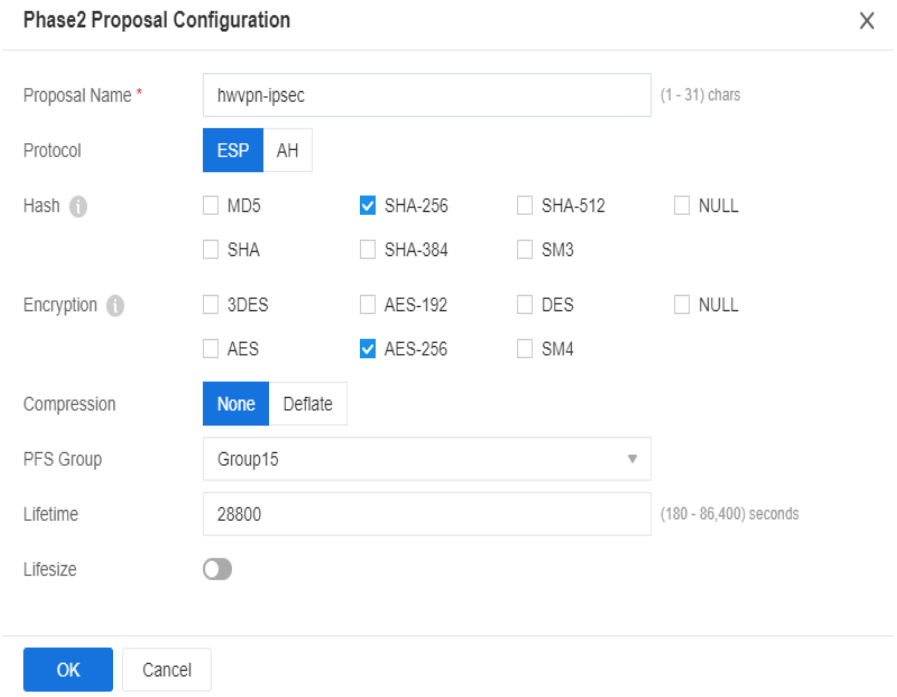
Select the phase-1 proposal created in **c** from the **Proposal1** drop-down list box. Click **Advanced Configuration**, toggle on **NAT Traversal** and **DPD**, and click **OK**.

Figure 1-49 Configuring VPN peers



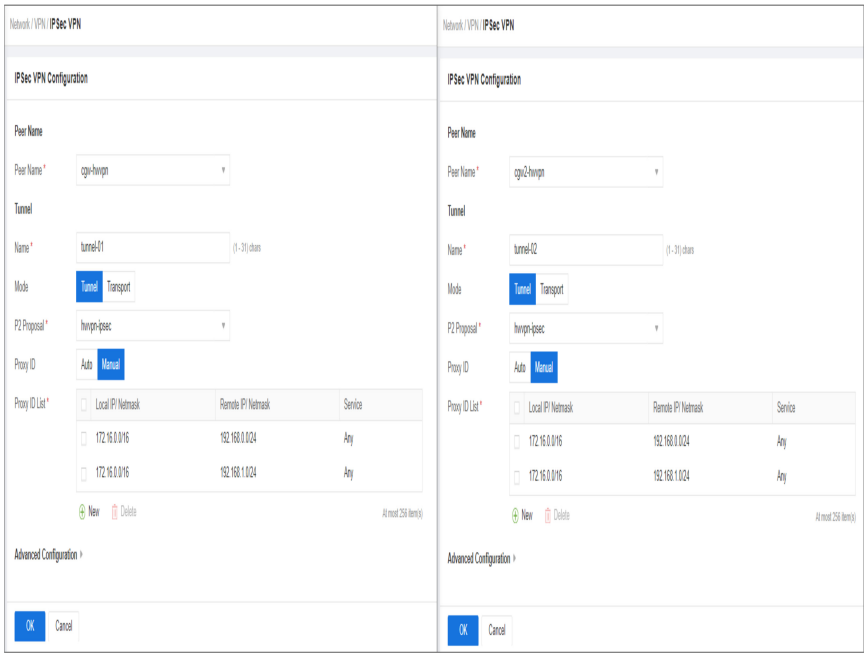
e. Click the plus sign (+) in the **P2 Proposal** drop-down list box to create a phase-2 proposal. Set parameters and click **OK**. **Figure 1-50** shows the key parameter settings.

Figure 1-50 Configuring a phase-2 proposal



f. Configure VPN connection information. Select each of the VPN peers created in **d** from the **Peer Name** drop-down list box, select the phase-2 proposal created in **e** from the **P2 Proposal** drop-down list box, select **Manual** for **Proxy ID**, configure **Proxy ID List**, and click **OK**. **Figure 1-51** shows the key parameter settings.

Figure 1-51 Configuring IPsec VPN

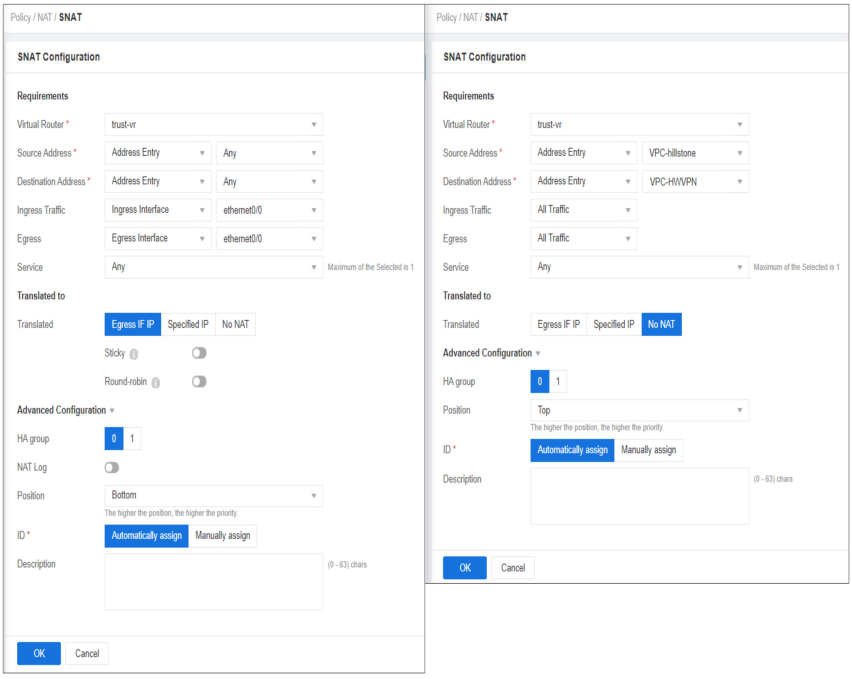


4. Configure VPN policies.

   a. Configure source network address translation (NAT) policies.

      Choose **Policy** > **NAT** > **SNAT**. Click **New**, configure two source NAT policies, and set their priorities, as shown in **Figure 1-52**.

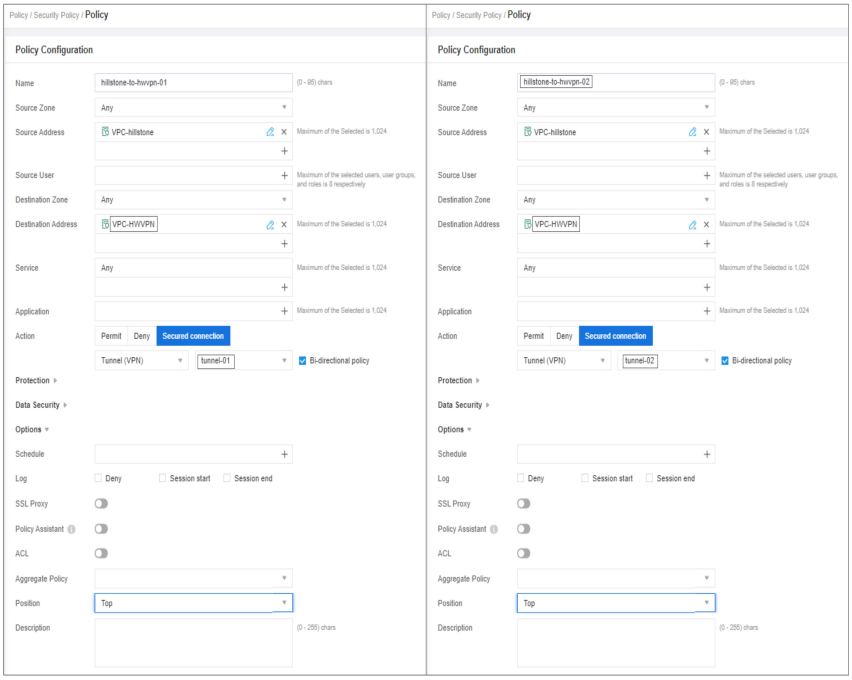
Figure 1-52 Configuring source NAT



b. Configure VPN security policies.

Choose **Policy** > **Security Policy** > **Policy**. Click **New** and choose **Policy**. Configure two VPN security policies and set their priorities to be higher than that of the default security policy configured in **b**, as shown in **Figure 1-53**.

Figure 1-53 Configuring VPN security policies



1.6.3.5 Verification

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

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

    Choose **Network** > **VPN** > **IPSec VPN**. The states of the two VPN connections are normal.
- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnet can ping each other.

1.7 Interconnection with a Sangfor Vrtual Firewall

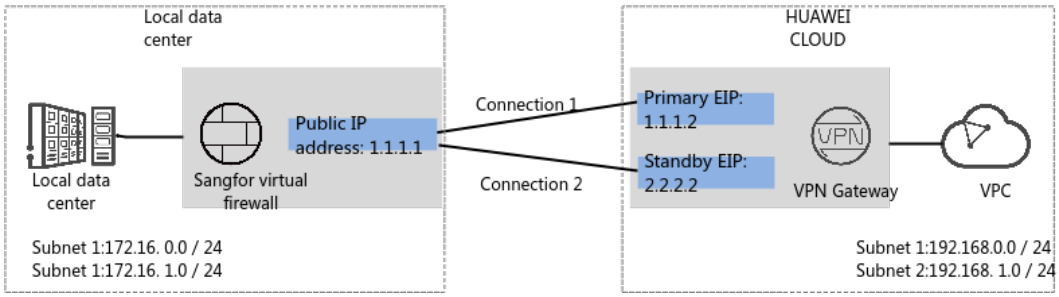
1.7.1 Policy-based Mode

1.7.1.1 Operation Guide

Scenario

Figure 1-54 shows the typical networking for connecting a Huawei Cloud VPN gateway to a Sangfor virtual firewall in policy-based mode.

Figure 1-54 Typical networking diagram



In this scenario, the Sangfor virtual firewall supports the single-IP address solution. A VPN connection is created between the public IP address of the Sangfor virtual firewall and the primary and standby EIPs of the Huawei Cloud VPN gateway.

Data Plan

Table 1-77 Data plan

Category	Item	Sangfor Firewall Example Value	Example Value for the Huawei Cloud Side
VPC	Subnets that can communicate with each other	172.16.0.0/24 172.16.1.0/24	• 192.168.0.0/24 • 192.168.1.0/24
VPN gateway	Gateway IP address	1.1.1.1	• Active EIP: 1.1.1.2 • Standby EIP: 2.2.2.2
VPN connection	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • DH algorithm: group 15 • IKE version: IKEv2 • Lifetime (s): 28800 • Peer ID: IP address • Local ID: IP address	

Category	Item	Sangfor Firewall Example Value	Example Value for the Huawei Cloud Side
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • PFS: DH group 15 • Transfer protocol: ESP • Lifetime (s): 3600 • Packet encapsulation mode: TUNNEL	

1.7.1.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-78 describes the parameters for creating a VPN gateway.

Table 1-78 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud VPC that the on-premises data center needs to access.	vpc-001(192.168.0.0/16)
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24

Parameter	Description	Value
Interconnection Subnet	Subnet used for communication between the VPN gateway and the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active/Standby
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-79 only describes the key parameters for creating a customer gateway.

Table 1-79 Parameters for creating a customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw

Parameter	Description	Value
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway to permit UDP port 4500.	IP Address 1.1.1.1

Step 5 Configure VPN connections.

In this scenario, the single-IP address solution of the firewall is used. A VPN connection is created between the primary EIP of the Huawei Cloud VPN gateway and the IP address of the firewall.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Set parameters as prompted.

   Table 1-80 describes the key parameters for creating VPN connections.

Table 1-80 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2

Parameter	Description	Value
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Policy-based**.	Policy-based
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the health check, PSK, confirm PSK, and policies for the VPN gateway IP address of connection 1.	*Set parameters based on the site requirements.*
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	Test@123
Policy	A policy rule defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. – Source CIDR Block The source CIDR block must contain some local subnets. 0.0.0.0/0 indicates any address. – Destination CIDR Block The destination CIDR block must contain all customer subnets.	– Source CIDR block 1: 192.168.0.0/24 – Destination CIDR block 1: 172.16.0.0/24, 172.16.1.0/24 – Source CIDR block 2: 192.168.1.0/24 – Destination CIDR block 2: 172.16.0.0/24, 172.16.1.0/24

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the firewall.	– IKE Policy ▪ Version: v2 ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-256 ▪ DH Algorithm: Group 15 ▪ Lifetime (s): 28800 ▪ Local ID: IP Address ▪ Customer ID: IP Address – IPsec Policy ▪ Authentication Algorithm: SHA2-256 ▪ Encryption Algorithm: AES-256 ▪ PFS: DH group 15 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 3600 ▪ Packet encapsulation mode: TUNNEL

----End

1.7.1.3 Configuration on the Firewall

Prerequisites

The basic network configuration of the Sangfor virtual firewall has been completed.

Procedure

1. Log in to the firewall management page.

   The following uses 8.35R1 as an example. The management page may vary depending on the firewall version. For details, see the product documentation of the corresponding version.
2. Configure the uplink port on the firewall.
   a. Choose **Network** > **Interface** > **Physical Interface**.
   b. Locate the row that contains eth0 and click **Edit** in the **Operation** column to configure the interface attributes.
   c. Set **Zone** to **L3_trust_A** and select **WAN** for **Basic Attributes**.
3. Enable the IPsec VPN capability of the firewall.
   a. Choose **Network** > **IPSecVPN** > **DLAN Running Status**.
   b. In the VPN Running Status area, select **Enable VPN service**.
4. Configure an IPsec VPN line.
   a. Choose **Network** > **IPSecVPN** > **Basic Configuration**.
   b. In the IPsec VPN Line area, click **Add Line**.
   c. Set parameters as prompted.

      Table 1-81 describes the parameters. For other parameters, use their default settings.

Table 1-81 Parameter description

Parameter	Description	Value
Line interface	WAN If no option is available, check whether **Step 2** is successfully executed. If the network deployment mode is changed, delete the original line and add a line by referring to **Step 2**.	eth0

Parameter	Description	Value
Link type.	• Fixed IP address • Internet dial-up line • Private line • 4G	Fixed IP address
Carrier	• CMCC • **China Unicom** • **China Telecom**	**China Unicom**
EIP	If the device is deployed in one-armed mode and no public IP address is configured for the WAN interface, you need to configure a public IP address for the line.	1.1.1.1
Enable Status	Select **Enable**.	Enable

d. Click **Expand Settings** in the Advanced area, set **VPN Interface** to **Custom**, and set the VPN interface IP address to the public IP address of the firewall.

5. Configure an access control policy.
   a. Choose **Policy** > **Access Control** > **Application Control Policy**.
   b. On the Policy Configuration tab page, click **Create**.
   c. Configure an application control policy, as shown in **Table 1-82**. For other parameters, use their default settings.

Table 1-82 Parameter description

Parameter	Description	Value
Basic Info	Name	any
	Status	Enable
Source	Source area	any
	Source address	Network Object-All
Purpose	Destination zone	any
	Destination address	All
	Service	any

Parameter	Description	Value
	Application	All
Effective Condition Settings	**Mandatory/ Optional**	Allow
	Effective time	**Full day**

6. Configure a source NAT policy.
   a. Choose **Policy** > **Address Translation**.
   b. In the IPv4 Address Translation area, click **Create**.
   c. Configure source NAT information, as shown in **Table 1-83**. For other parameters, use their default settings.

Table 1-83 Parameter description

Parameter	Description	Value
-	Translation Type	Source NAT
Setting basic information	Name	snat001
	Enabling State	Enable
	Effective time	**Full day**
Original Data Packet	Source area	L3_trust_A, which must be the same as the value of **Parameter** configured in **Step 2**.
	Source address	All
	Destination Zone/Interface	Zone, L3_trust_A,
	Destination address	All
	Service	any
Translated Data Packet	Source Address After NAT	Specified IP address, 172.16.0.0/24.
	Destination Address Translation To	No translation
	Destination Port Translated To	No translation

7. Configure VPN connection information.
   a. Choose **Network** > **IPSecVPN** > **Third-Party Interconnection Management** and click **Add Third-Party Device**.

b. Set parameters as prompted.

Table 1-84 describes the parameters. For other parameters, use their default settings.

Table 1-84 Parameter description

Area	Parameter	Description	Value
Performing Basic Configurations	Device Name	Select the VPN peer name.	hwvpn-01
	Enable/Disable	Select **Enable**.	Enable
	Peer device address type	Select **Fixed IP**.	Fixed IP
	Peer IP address	This parameter is mandatory only when **Peer Device Address Type** is set to **Fixed IP**.	1.1.1.2
	Peer Domain Name Address	This parameter is mandatory only when **Peer Device Address Type** is set to **Dynamic Domain Name**.	-
	Authentication Mode - Pre-shared Key	The value must be the same as the pre-shared key configured in **Table 1-80**.	Test@123
	Local Connection Line	Select the IPsec VPN line configured in **Configuring an IPsec VPN Line**.	eth0 (Fixed IP address of China Unicom Internet)

Area	Parameter	Description	Value
	Encrypted data flow	Encrypted data flows must be configured for subnet 1V1. For example, if there are two subnets in the user data center and two subnets in the Huawei Cloud VPC, four encrypted data flows need to be configured. **When configuring the data flow for the first time, click Add to add the encrypted data flow information.**	Encrypted data flow 1 • Local IP address: 172.16.0.0/24 • Local intranet service: ALL Services • Peer address: 192.168.0.0/24 • Peer intranet service: ALL Services • Phase 2 security proposal: Configure the IPsec policy information, which must be the same as the IPsec policy information configured in **Table 1-80**. – Protocol: ESP – Encryption algorithm: SHA2-256 – Authentication algorithm: AES-256 – Perfect forward secrecy (PFS): group 15 • Priority: 128

Area	Parameter	Description	Value
			Encrypted data flow 2: • Local IP address: 172.16.0.0/24 • Local intranet service: ALL Services • Peer address: 192.168.1.0/24 • Peer intranet service: • Phase 2 security proposal: The IPSec policy information must be the same as that configured in **Table 1-80**. – Protocol: ESP – Encryption algorithm: SHA2-256 – Authentication algorithm: AES-256 – Perfect forward secrecy (PFS): group 15 • Priority: 128 Encrypted data flow 3 • Local IP address:

Area	Parameter	Description	Value
			172.16.1.0/24 • Local intranet service: ALL Services • Peer address: 192.168.0.0/24 • Peer intranet service: ALL Services • Phase 2 security proposal: The IPSec policy information must be the same as that configured in **Table 1-80**. – Protocol: ESP – Encryption algorithm: SHA2-256 – Authentication algorithm: AES-256 – Perfect forward secrecy (PFS): group 15 • Priority: 128 Encrypted data flow 4 • Local IP address: 172.16.1.0/24 • Local intranet

Area	Parameter	Description	Value
			service: ALL Services • Peer address: 192.168.1.0/24 • Peer intranet service: ALL Services • Phase 2 security proposal: The IPSec policy information must be the same as that configured in **Table 1-80**. – Protocol: ESP – Encryption algorithm: SHA2-256 – Authentication algorithm: AES-256 – Perfect forward secrecy (PFS): group 15 • Priority: 128
IKE	IKE version	Select **IKEv2**.	IKEv2
	Active Connection	Select **Enable**.	Enable
	Local identity type	Select **IP Address(IPV4_ADDR)**.	IP Address(IPV4_ADDR)

Area	Parameter	Description	Value
	Local identity ID	When **Peer device address type** is set to **Fixed IP** or **Dynamic domain name** and **Local identity type** is set to **IP Address(IPV4_ADDR)** or **Certificate DN(DN)**, this parameter can be left empty. If NAT is deployed between the two devices, this parameter must be set.	1.1.1.1
	Peer identity type	Select **IP Address(IPV4_ADDR)**.	IP Address(IPV4_ADDR)
	Peer identity ID	If **Peer device address type** is set to **Fixed IP** or **Dynamic domain name**, you do not need to set **Peer identity type** to **IP address (IPV4_ADDR)** or **Certificate DN (DN)**. If NAT is configured between the two devices, the identity ID must be set.	1.1.1.2
	IKE SA timeout	Lifetime of a security association (SA). An SA will be renegotiated when its lifetime expires. • Unit: second • Value range: 600 to 864000	3600
	D-H group	Set this parameter to **group 15**.	group 15

Area	Parameter	Description	Value
	DPD	Specifies whether to automatically send dead peer detection (DPD) packets to check whether the peer end is alive and delete incorrect tunnels in a timely manner. DPD packets must be enabled or disabled on both ends.	Enable
	Detection time	• Unit: second • Value range: 5 to 60	30
	Number of timeouts	Value range: 1 to 6	5
	Phase 1 security proposal	Specifies the IKE policy information, which must be the same as that configured in **Table 1-80**. The security proposal is sent to the peer end and compared with the peer security proposal. The proposal supported by both ends is used. **If this is the first configuration, click Add to add IKE policy information.**	• Encryption algorithm: AES256 • Authentication Algorithm: SHA2-256 • PRF: SHA2-256
IPsec	Number of retry times.	Specifies the number of times that negotiation packets are retransmitted when negotiation packets are lost or not received during a single negotiation. • Value range: 1–20	10

Area	Parameter	Description	Value
	IPSec SA timeout	Lifetime of a security association (SA). An SA will be renegotiated when its lifetime expires. • Unit: second • Value range: 600 to 864000	28800
	Expiration time	Select **Disable**.	Disable

1.7.1.4 Verification

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

    Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the two VPN connections are both **Normal**.
- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

1.8 Interconnection with TheGreenBow VPN Client

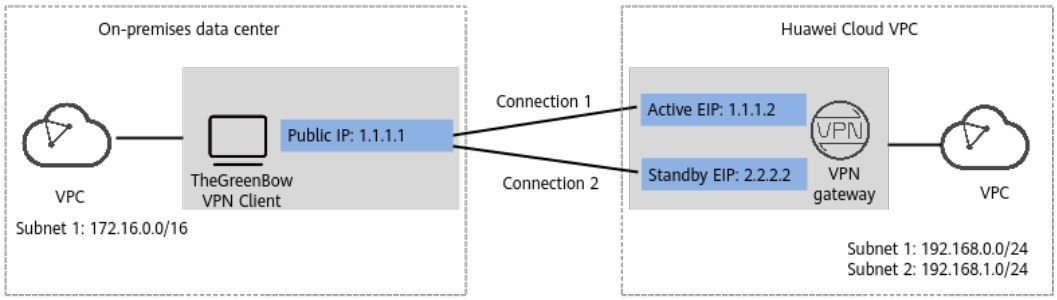
1.8.1 Static Routing Mode

1.8.1.1 Operation Guide

Scenario

Figure 1-55 shows the typical networking where a Huawei Cloud VPN gateway connects to TheGreenBow VPN Client in static routing mode.

Figure 1-55 Typical networking diagram



In this scenario, TheGreenBow VPN Client has only one IP address. A VPN connection needs to be created between the IP address of TheGreenBow VPN Client and each of the active and standby EIPs of the Huawei Cloud VPN gateway.

Data Plan

Table 1-85 Data plan

Category	Item	Data
Huawei Cloud VPC	Subnet to be interconnected	• 192.168.0.0/24 • 192.168.1.0/24
Huawei Cloud VPN gateway	Interconnection subnet	Subnet used for communication between the VPN gateway and the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	Elastic IP address (EIP)	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Standby EIP: 2.2.2.2
VPC at the TheGreenBow VPN Client side	Subnet to be interconnected	172.16.0.0/16
Gateway at the TheGreenBow VPN Client side	Public IP address (EIP bound to the Windows host)	1.1.1.1
	Private IP address (NIC address of the Windows host)	172.16.1.1
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30
IKE and IPsec policies	Pre-shared key (PSK)	Test@123

Category	Item	Data
	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • DH algorithm: group 15 • IKE version: IKEv2 **NOTE** TheGreenBow VPN Client 5.55 supports only IKEv1. TheGreenBow VPN Client 6.6 supports both IKEv1 and IKEv2. IKEv1 cannot be used for interconnection with Huawei Cloud Enterprise Edition VPN. • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • PFS: DH group 15 • Transfer protocol: ESP • Lifetime (s): 3600

1.8.1.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-86 describes the parameters for creating a VPN gateway.

Table 1-86 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001

Parameter	Description	Value
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active/Standby
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-87 describes the parameters for creating a customer gateway.

Table 1-87 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-TheGreenBow
Identifier	Select **IP Address**, and enter the IP address used by TheGreenBow VPN Client to communicate with the Huawei Cloud VPN gateway.	1.1.1.1

Step 5 Configure VPN connections.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Configure VPN connections as prompted.

   Table 1-88 describes the parameters for creating VPN connections.

Table 1-88 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16

Parameter	Description	Value
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, health check, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, VPN traffic will fail to be forwarded.	**NQA** deselected
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	Test@123

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on TheGreenBow VPN Client.	– IKE Policy ▪ Encryption Algorithm: AES-256 ▪ Authentication Algorithm: SHA2-256 ▪ DH Algorithm: Group 15 ▪ Version: v2 ▪ Lifetime (s): 86400 ▪ Local ID: IP Address ▪ Customer ID: IP Address – IPsec Policy ▪ Encryption Algorithm: AES-256 ▪ Authentication Algorithm: SHA2-256 ▪ PFS: DH group 15 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 3600
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.8.1.3 Configuration on TheGreenBow VPN Client

Prerequisites

- TheGreenBow VPN Client has been installed on a Windows host.
- A VPC and its subnets have been created.

Procedure

Step 1 Start TheGreenBow VPN Client on the Windows host.

TheGreenBow VPN Client 6.6 is used as an example. The configuration pages may vary according to the client version. For details, see the product documentation of the corresponding version.

Step 2 Choose **VPN Configuration** > **IKE V1**, right-click the configuration examples **tgbtestIPV4** and **tgbtestIPV6**, and choose **Delete** from the shortcut menu.

Step 3 Create a VPN gateway.

Choose **VPN Configuration** > **IKE V2**, right-click **IKE V2**, and choose **New IKE AUTH** from the shortcut menu.

Step 4 Configure VPN gateway information.

Choose **VPN Configuration** > **IKE V2** > **Ikev2Gateway**, and enter the required information.

Table 1-89 describes the key parameters. For other parameters, use their default settings.

Table 1-89 Parameter description

Tab Page	Parameter	Description	Value
Authentication	Interface	Select the public IP address of TheGreenBow VPN Client.	1.1.1.1

Tab Page	Parameter	Description	Value
	Remote Gateway	Select the active EIP of the Huawei Cloud VPN gateway, which is used to communicate with TheGreenBow VPN Client.	1.1.1.2
	Preshared Key	Select **Preshared Key**. The value must be the same as the PSK configured in **Table 1-88**.	Test@123
	Encryption	The settings must be the same as those of the IKE policy configured in **Table 1-88**.	• Encryption: AES CBC 256 • Authentication: SHA2-256 • Key Group: DH15 (MODP 3072)
	Authentication		
	Key Group		
Protocol	Local ID	Select **IPV4 Address**, and enter the public IP address of TheGreenBow VPN Client. The value must be the same as the customer ID configured in **Table 1-87**.	1.1.1.1
	Remote ID	Select **IPV4 address**, and enter the active EIP of the Huawei Cloud VPN gateway. The value must be the same as the local ID configured in **Table 1-88**.	1.1.1.2
Gateway	Redundant Gateway	Leave this parameter blank when TheGreenBow VPN Client has a single IP address.	Leave this parameter blank.

Step 5 Create a VPN connection.

Choose **VPN Configuration** > **IKE V2** > **Ikev2Gateway**, right-click **Ikev2Gateway**, and choose **New Child SA** from the shortcut menu.

Step 6 Configure VPN connection information.

Choose **VPN Configuration** > **IKE V2** > **Ikev2Gateway** > **Ikev2Tunnel**, deselect **Request configuration from the gateway**, and enter related information as prompted.

Table 1-90 describes the key parameters. For other parameters, use their default settings.

Table 1-90 Parameter description

Tab Page	Parameter	Description	Value
Child SA	VPN Client address	Enter the private IP address of TheGreenBow VPN Client.	172.16.1.1
	Address type	Select **Subnet address**.	Subnet address
	Remote LAN address	CIDR block of the Huawei Cloud VPC.	192.168.0.0
	Subnet mask		255.255.0.0
	Encryption	The settings must be the same as those of the IPsec policy configured in Table 1-88.	• Encryption: AES CBC 256 • Integrity: SHA2-256 • Diffie-Hellman: DH15 (MODP 3072) • Child SA Lifetime: 3600 sec
	Integrity		
	Diffie-Hellman		
	Child SA Lifetime		
Automation	Automatic Open mode	-	• Select **Automatically open this tunnel when VPN Client starts after logon**. • Select **Automatically open this tunnel on traffic detection**.

Step 7 Choose **Configuration** from the menu bar in the upper left corner, and then click **Save**.

----End

1.8.1.4 Verification

- Check VPN connections.

  - Huawei Cloud

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

    Choose **VPN Configuration** > **IKE V2** > **Ikev2Gateway** > **Ikev2Tunnel**, right-click **Ikev2Tunnel**, and choose **Open tunnel** from the shortcut menu. The tunnel states are normal (icons are displayed in green).
- Ping the IP address of a server in the local subnet of the Huawei Cloud VPC from the Windows host where the TheGreenBow VPN Client is located.

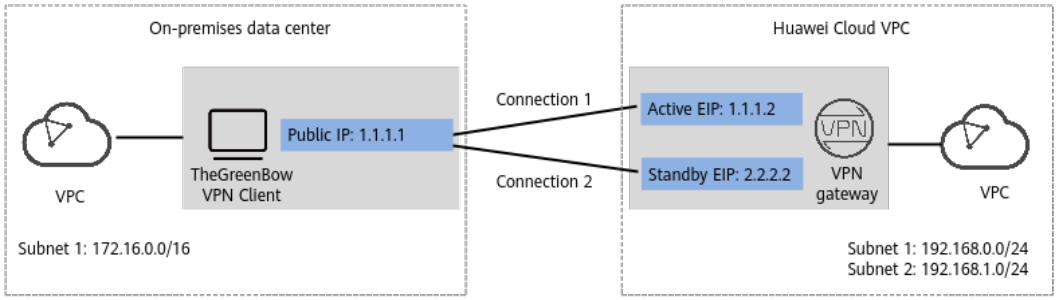
1.8.2 Policy-based Mode

1.8.2.1 Operation Guide

Scenario

Figure 1-56 shows the typical networking where a Huawei Cloud VPN gateway connects to TheGreenBow VPN Client in policy-based mode.

Figure 1-56 Typical networking diagram



In this scenario, it is recommended that TheGreenBow VPN Client use only one IP address. A VPN connection needs to be created between the IP address of TheGreenBow VPN Client and each of the active and standby EIPs of the Huawei Cloud VPN gateway.

Data Plan

Table 1-91 Data plan

Category	Item	Data
Huawei Cloud VPC	Subnet to be interconnected	• 192.168.0.0/24 • 192.168.1.0/24

Category	Item	Data
Huawei Cloud VPN gateway	Interconnection subnet	Subnet used for communication between the VPN gateway and the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Standby EIP: 2.2.2.2
VPC at the TheGreenBow VPN Client side	Subnet to be interconnected	172.16.0.0/16
Gateway at the TheGreenBow VPN Client side	Public IP address (EIP bound to the Windows host)	1.1.1.1
	Private IP address (NIC address of the Windows host)	172.16.1.1
IKE and IPsec policies	PSK	Test@123
	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • DH algorithm: group 15 • IKE version: IKEv2 **NOTE** TheGreenBow VPN Client 5.55 supports only IKEv1. TheGreenBow VPN Client 6.6 supports both IKEv1 and IKEv2. IKEv1 cannot be used for interconnection with Huawei Cloud Enterprise Edition VPN. • Lifetime (s): 7200 • Local ID: IP address • Peer ID: IP address
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-256 • PFS: DH group 15 • Transfer protocol: ESP • Lifetime (s): 3600

1.8.2.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-92 describes the parameters for creating a VPN gateway.

Table 1-92 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud 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 the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active/Standby

Parameter	Description	Value
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-93 describes the parameters for creating a customer gateway.

Table 1-93 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-TheGreenBow
Identifier	Select **IP Address**, and enter the IP address used by TheGreenBow VPN Client to communicate with the Huawei Cloud VPN gateway.	1.1.1.1

Step 5 Configure VPN connections.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Configure VPN connections as prompted.

   Table 1-94 only describes the parameters for creating VPN connections.

Table 1-94 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2

Parameter	Description	Value
VPN Type	Select **Policy-based**.	Policy-based
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the health check, PSK, confirm PSK, and policies for the VPN gateway IP address of connection 1.	*Set parameters based on the site requirements.*
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	Test@123
Policy	A policy rule defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. – Source CIDR Block The source CIDR block must contain some local subnets. 0.0.0.0/0 indicates any address. – Destination CIDR Block The destination CIDR block must contain all customer subnets.	– Source CIDR Block: 192.168.0.0/16 – Destination CIDR Block: 172.16.1.1/32

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on TheGreenBow VPN Client.	– IKE Policy ▪ Encryption Algorithm: AES-256 ▪ Authentication Algorithm: SHA2-256 ▪ DH Algorithm: Group 15 ▪ Version: v2 ▪ Lifetime (s): 7200 ▪ Local ID: IP Address ▪ Customer ID: IP Address – IPsec Policy ▪ Encryption Algorithm: AES-256 ▪ Authentication Algorithm: SHA2-256 ▪ PFS: DH group 15 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 3600
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** It is recommended that the configuration of connection 2 be the same as that of connection 1.	Enabled

----End

1.8.2.3 Configuration on TheGreenBow VPN Client

Prerequisites

- TheGreenBow VPN Client has been installed on a Windows host.
- A VPC and its subnets have been created.

Procedure

Step 1 Start TheGreenBow VPN Client on the Windows host.

TheGreenBow VPN Client 6.6 is used as an example. The configuration pages may vary according to the client version. For details, see the product documentation of the corresponding version.

Step 2 Choose **VPN Configuration** > **IKE V1**, right-click the configuration examples **tgbtestIPV4** and **tgbtestIPV6**, and choose **Delete** from the shortcut menu.

Step 3 Create a VPN gateway.

Choose **VPN Configuration** > **IKE V2**, right-click **IKE V2**, and choose **New IKE AUTH** from the shortcut menu.

Step 4 Configure IKE phase 1.

Choose **VPN Configuration** > **IKE V2** > **Ikev2Gateway**, and enter the required information.

Table 1-95 describes the key parameters. For other parameters, use their default settings.

Table 1-95 Parameter description

Tab Page	Parameter	Description	Value
Authentication	Interface	Select the public IP address of TheGreenBow VPN Client.	1.1.1.1
	Remote Gateway	Select the active EIP of the Huawei Cloud VPN gateway, which is used to communicate with TheGreenBow VPN Client.	1.1.1.2
	Preshared Key	Select **Preshared Key**. The value must be the same as the PSK configured in **Table 1-94**.	Test@123

Tab Page	Parameter	Description	Value
	Encryption	The settings must be the same as those of the IKE policy configured in **Table 1-94**.	• Encryption: AES CBC 256 • Authentication: SHA2-256 • Key Group: DH15 (MODP 3072)
	Authentication		
	Key Group		
Protocol	Local ID	Select **IPV4 Address**, and enter the public IP address of TheGreenBow VPN Client. The value must be the same as the customer ID configured in **Table 1-93**.	1.1.1.1
	Remote ID	Select **IPV4 address**, and enter the active EIP of the Huawei Cloud VPN gateway. The value must be the same as the local ID configured in **Table 1-94**.	1.1.1.2
Gateway	Redundant Gateway	Leave this parameter blank when TheGreenBow VPN Client has a single IP address.	Leave this parameter blank.

Step 5 Create a VPN connection.

Choose **VPN Configuration** > **IKE V2** > **Ikev2Gateway**, right-click **Ikev2Gateway**, and choose **New Child SA** from the shortcut menu.

Step 6 Configure IPsec phase 2.

Choose **VPN Configuration** > **IKE V2** > **Ikev2Gateway** > **Ikev2Tunnel**, deselect **Request configuration from the gateway**, and enter related information as prompted.

Table 1-96 describes the key parameters. For other parameters, use their default settings.

Table 1-96 Parameter description

Tab Page	Parameter	Description	Value
Child SA	VPN Client address	Enter the private IP address of TheGreenBow VPN Client.	172.16.1.1
	Address type	Select **Subnet address**.	Subnet address
	Remote LAN address	CIDR block of the Huawei Cloud VPC.	192.168.0.0
	Subnet mask		255.255.0.0
	Encryption	The settings must be the same as those of the IPsec policy configured in **Table 1-94**.	• Encryption: AES CBC 256 • Integrity: SHA2-256 • Diffie-Hellman: DH15 (MODP 3072) • Child SA Lifetime: 3600 sec
	Integrity		
	Diffie-Hellman		
	Child SA Lifetime		
Automation	Automatic Open mode	-	• Select **Automatically open this tunnel when VPN Client starts after logon**. • Select **Automatically open this tunnel on traffic detection**.

Step 7 Choose **Configuration** from the menu bar in the upper left corner, and then click **Save**.

----End

1.8.2.4 Verification

- Check VPN connections.
  - Huawei Cloud

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

    Choose **VPN Configuration** > **IKE V2** > **Ikev2Gateway** > **Ikev2Tunnel**, right-click **Ikev2Tunnel**, and choose **Open tunnel** from the shortcut menu. The tunnel states are normal (icons are displayed in green).
- Ping the IP address of a server in the local subnet of the Huawei Cloud VPC from the Windows host where the TheGreenBow VPN Client is located.

1.9 Interconnection with strongSwan

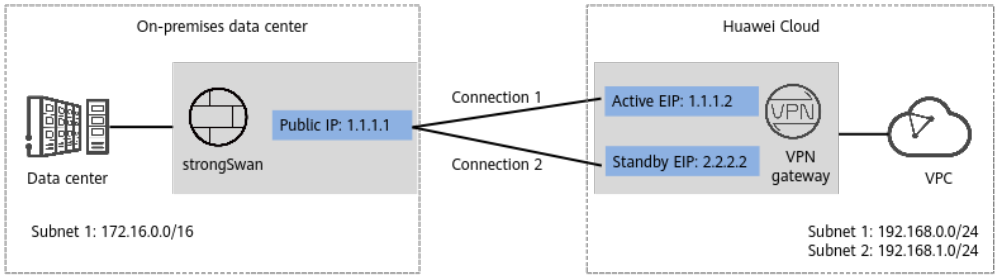
1.9.1 Static Routing Mode

1.9.1.1 Operation Guide

Scenario

Figure 1-57 shows the typical networking where a Huawei Cloud VPN gateway connects to strongSwan in static routing mode.

Figure 1-57 Typical networking diagram



In this scenario, strongSwan has only one IP address, and the Huawei Cloud VPN gateway uses the active/standby mode. A VPN connection needs to be created between each of the active and standby EIPs of the Huawei Cloud VPN gateway and the IP address of strongSwan.

Data Plan

Table 1-97 Data plan

Category	Item	Data
Huawei Cloud VPC	Subnet to be interconnected	• 192.168.0.0/24 • 192.168.1.0/24
Huawei Cloud VPN gateway	Interconnection subnet	Subnet used for communication between the VPN gateway and the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24

Category	Item	Data
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Standby EIP: 2.2.2.2
VPC at the strongSwan side	Subnet to be interconnected	172.16.0.0/16
VPN gateway at the strongSwan side	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is as follows: 1.1.1.1
	Private IP address	In this example, the private IP address is as follows: 172.16.0.195
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	• Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	• Authentication algorithm: SHA1 • Encryption algorithm: AES-128 • DH algorithm: group 2 • IKE version: IKEv2 • Lifetime (s): 86400
	IPsec policy	• Authentication algorithm: SHA1 • Encryption algorithm: AES-128 • PFS: DH group 2 • Lifetime (s): 86400

1.9.1.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-98 describes the parameters for creating a VPN gateway.

Table 1-98 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud VPC that the on-premises data center needs to access.	vpc-001(192.168.0.0/16)
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
Interconnection Subnet	Subnet used for communication between the VPN gateway and the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active/Standby
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-99 describes the parameters for creating a customer gateway.

Table 1-99 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-strongswan
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway to permit UDP port 4500.	1.1.1.1

Step 5 Configure VPN connections.

In this scenario, strongSwan has only one public IP address. A VPN connection needs to be created between the public IP address of strongSwan and each of the active and standby EIPs of the Huawei Cloud VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Configure VPN connections as prompted.

   The following table only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-100 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2

Parameter	Description	Value
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, health check, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, **Manually specify** is selected. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address. Otherwise, VPN traffic will fail to be forwarded.	**NQA** selected
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	Test@123

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those of strongSwan.	– IKE Policy ▪ Encryption Algorithm: AES-128 ▪ Authentication Algorithm: SHA1 ▪ DH Algorithm: Group 2 ▪ Version: v2 ▪ Lifetime (s): 86400 ▪ Local ID: IP Address ▪ Customer ID: IP Address – IPsec Policy ▪ Encryption Algorithm: AES-128 ▪ Authentication Algorithm: SHA1 ▪ PFS: DH group 2 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 86400
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

----End

1.9.1.3 Configuration in the On-Premises Data Center

Notes and Constraints

This section uses a strongSwan device that runs the CentOS 8.2 64-bit operating system as an example. For other operating systems, see the official documentation of strongSwan.

Procedure

Step 1 Download the strongSwan installation package from the official website.

The installation and configuration methods may vary according to the strongSwan version. This example uses strongSwan 5.9.10 as an example.

Step 2 Install the strongSwan software.

1. Log in to the CentOS 8.2 operating system as the **root** user and open the CLI window.
2. Upload the strongSwan installation package to a directory on the CentOS operating system, for example, **/opt/**.
3. Run the following command to go to the directory where the installation package is stored:

   cd /opt/
4. Run the following command to install strongSwan:

   rpm -ivh strongswan-5.9.10-1.el8.x86_64.rpm --force --nodeps

   NOTE

   strongswan-5.9.10-1.el8.x86_64.rpm is the installation package name. Replace it with the actual one.

   If the following information in bold is displayed, the installation is successful.

   ```
   Verifying...                          ################################# [100%]
   Preparing...                          ################################# [100%]
   Updating / installing...
      1:strongswan-5.9.10-1.el8          ################################# [100%]
   ```
5. Run the following command to check the strongSwan version:

   strongswan version

   The following information in bold is displayed:

   ```
   Linux strongSwan U5.9.10/K4.18.0-348.7.1.el8_5.x86_64
   University of Applied Sciences Rapperswil, Switzerland
   ```

Step 3 Configure firewall policies.

- Run the following command to permit the ESP protocol (IP protocol number: 50):

  iptables -I INPUT -p 50 -j ACCEPT
- Run the following command to permit UDP port 500:

  iptables -I INPUT -p udp --dport 500 -j ACCEPT
- Run the following command to permit UDP port 4500:

  iptables -I INPUT -p udp --dport 4500 -j ACCEPT

Step 4 Enable the traffic forwarding function.

Run the following command to enable traffic forwarding:

echo 1 > /proc/sys/net/ipv4/ip_forward

The preceding command is a temporary command. After the strongSwan device is restarted, you need to run this command again. If you want to permanently enable traffic forwarding for the strongSwan device, perform the following operations:

1. Run the following command to open the **/etc/sysctl.conf** file:

   vi /etc/sysctl.conf
2. Add the following configuration to the file:
   ```
   net.ipv4.ip_forward = 1
   ```
3. Press **Esc**, enter **:wq**, and press **Enter**.

   The system saves the configuration and exits the editor.
4. Run the following command for the configuration to take effect:

   sudo sysctl -p

Step 5 Configure dual tunnels.

1. Run the following command to back up the strongSwan configuration file:

   mv /etc/strongswan/swanctl/swanctl.conf /etc/strongswan/swanctl/swanctl.conf.bak
2. Run the following command to open the strongSwan configuration file:

   vi /etc/strongswan/swanctl/swanctl.conf
3. Add the following configurations according to the data plan:
   ```
   connections {
     vco1 {              # Add the VPN configuration of IPsec VPN tunnel 1.
       version = 2       # Specify the IKE version, which must be the same as that configured for Huawei Cloud connection 1. The value 2 indicates IKEv2.
       local_addrs  = 172.16.0.195       # Specify the local IP address.
       remote_addrs = 1.1.1.2        # Set the remote IP address of tunnel 1 to the gateway IP address of Huawei Cloud connection 1.
       dpd_delay = 10
       rekey_time = 86400            # Specify the SA lifetime of tunnel 1, which must be the same as that specified in the IKE configuration of Huawei Cloud connection 1.
       over_time = 1800
       proposals = aes128-sha1-modp1024   # Specify the encryption algorithm, authentication algorithm, and DH algorithm of tunnel 1, which must be the same as those specified in the IKE configuration of Huawei Cloud connection 1. modp1024 corresponds to DH group 2.
       encap = yes

       local {
         auth = psk          # Set the local authentication mode to PSK.
         id = 1.1.1.1        # Specify the public IP address of the local egress.
       }
       remote {
   ```



```
      auth = psk              # Set the authentication mode of Huawei Cloud to PSK.
      id = 1.1.1.2            # Specify the active EIP of Huawei Cloud connection 1.
    }
    children {
      vco_child1 {
        local_ts  = 172.16.0.0/16     # Set the private CIDR block of the local protected data flows to
172.16.0.0/16.
        remote_ts = 192.168.0.0/24     # Set the VPC CIDR block of the protected data flows at the
Huawei Cloud site to 192.168.0.0/24.
        mode = tunnel
        rekey_time = 85500
        life_time = 86400          # Specify the SA lifetime of tunnel 1, which must be the same as
that specified in the IPsec configuration of Huawei Cloud connection 1.
        dpd_action = restart
        start_action = start
        close_action = start
        esp_proposals = aes128-sha1-modp1024   # Specify the encryption algorithm,
authentication algorithm, and DH algorithm of tunnel 1, which must be the same as those specified
in the IPsec configuration of Huawei Cloud connection 1. modp1024 corresponds to DH group 2.
      }
    }
  }
  vco2 {                # Add the VPN configuration of IPsec VPN tunnel 2.
    version = 2          # Specify the IKE version, which must be the same as that configured for
Huawei Cloud connection 2. The value 2 indicates IKEv2.
    local_addrs  = 172.16.0.195        # Specify the local IP address.
    remote_addrs = 2.2.2.2      # Set the remote IP address of tunnel 2 to the gateway IP address of
Huawei Cloud connection 2.
    dpd_delay = 10
    rekey_time = 84600          # Specify the SA lifetime of tunnel 2, which must be the same as that
specified in the IKE configuration of Huawei Cloud connection 2.
    over_time = 1800
    proposals = aes128-sha1-modp1024       # Specify the encryption algorithm, authentication
algorithm, and DH algorithm of tunnel 2, which must be the same as those specified in the IKE
configuration of Huawei Cloud connection 2. modp1024 corresponds to DH group 2.
    encap = yes

    local {
      auth = psk          # Set the local authentication mode to PSK.
      id = 1.1.1.1        # Specify the public IP address of the local egress.
    }
    remote {
      auth = psk          # Set the authentication mode of Huawei Cloud to PSK.
      id = 2.2.2.2        # Specify the standby EIP of Huawei Cloud connection 2.
    }
    children {
      vco_child2 {
        local_ts  = 172.16.0.0/16     # Set the private CIDR block of the local protected data flows to
172.16.0.0/16.
        remote_ts = 192.168.0.0/24      # Set the VPC CIDR block of the protected data flows at the
Huawei Cloud site to 192.168.0.0/24.
        mode = tunnel
        rekey_time = 85500
        life_time = 86400        # Specify the SA lifetime of tunnel 2, which must be the same as that
specified in the IPsec configuration of Huawei Cloud connection 2.
        dpd_action = restart
        start_action = start
        close_action = start
        esp_proposals = aes-sha1-modp1024     # Specify the encryption algorithm, authentication
algorithm, and DH algorithm of tunnel 2, which must be the same as those specified in the IPsec
configuration of Huawei Cloud connection 2. modp1024 corresponds to DH group 2.
      }
    }
  }
}

secrets {
  ike-vco1 {
    secret = Test@123   # Specify the PSK of tunnel 1, which must be the same as that configured
```



```
for Huawei Cloud connection 1.
  }
  ike-vco2 {
    secret = Test@123   # Specify the PSK of tunnel 2, which must be the same as that configured
for Huawei Cloud connection 2.
  }
}
```

4. Press **Esc**, enter **:wq**, and press **Enter**.

   The system saves the configuration and exits the editor.

5. Run the following command to restart the strongSwan process:

   systemctl restart strongswan

6. Run the following command to check the tunnel status:

   watch swanctl --list-sas

   Information similar to the following is displayed:

```
ecs-b6b4-strongswan: Tue Mar 11 16:51:19 2025
plugin 'sqlite': failed to load - sqlite_plugin_create not found and no plugin file available
vco2: #2, ESTABLISHED, IKEv2, c2786dfe3bc7d7e0_i* 75e148eba08c17e1_r
...
...
vco1: #1, ESTABLISHED, IKEv2, 3d3396aa3797c86f_i* d89bb869311c580c_r
...
...
```

----End

1.9.1.4 Verification

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

  Huawei Cloud

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

- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

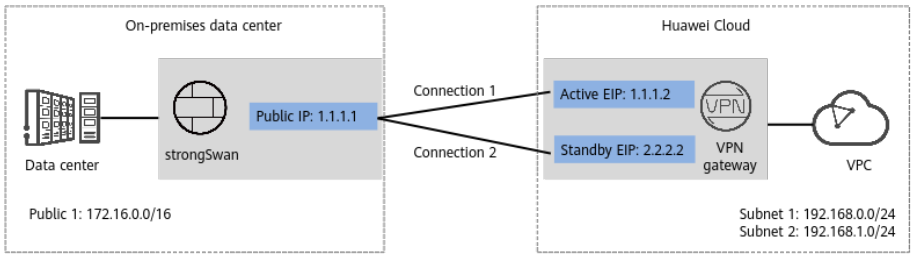
1.9.2 Policy-based Mode

1.9.2.1 Operation Guide

Scenario

Figure 1-58 shows the typical networking where a Huawei Cloud VPN gateway connects to strongSwan in policy-based mode.

Figure 1-58 Typical networking diagram



In this scenario, strongSwan has only one IP address, and the Huawei Cloud VPN gateway uses the active/standby mode. A VPN connection needs to be created between each of the active and standby EIPs of the Huawei Cloud VPN gateway and the IP address of strongSwan.

Data Plan

Table 1-101 Data plan

Category	Item	Data
Huawei Cloud VPC	Subnet to be interconnected	• 192.168.0.0/24 • 192.168.1.0/24
Huawei Cloud VPN gateway	Interconnection subnet	Subnet used for communication between the VPN gateway and the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Standby EIP: 2.2.2.2
VPC at the strongSwan side	Subnet to be interconnected	172.16.0.0/16
VPN gateway at the strongSwan side	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is as follows: 1.1.1.1
	Private IP address	In this example, the private IP address is as follows: 172.16.0.233
IKE and IPsec policies	PSK	Test@123
	IKE policy	• Authentication algorithm: SHA1 • Encryption algorithm: AES-128 • DH algorithm: group 2 • IKE version: IKEv2 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address

Category	Item	Data
	IPsec policy	• Authentication algorithm: SHA1 • Encryption algorithm: AES-128 • PFS: DH group 2 • Transfer protocol: ESP • Lifetime (s): 86400

1.9.2.2 Configuration on the Huawei Cloud Console

Prerequisites

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

Procedure

Step 1 Log in to Huawei Cloud management console.

Step 2 Choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy S2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 1-102 describes the parameters for creating a VPN gateway.

Table 1-102 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Associate With	Select **VPC**.	VPC
VPC	Huawei Cloud VPC that the on-premises data center needs to access.	vpc-001(192.168.0.0/16)
Local Subnet	Huawei Cloud VPC subnet that needs to communicate with the VPC of the on-premises data center.	192.168.0.0/24 192.168.1.0/24
Interconnection Subnet	Subnet used for communication between the VPN gateway and the VPC of the on-premises data center. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
BGP ASN	BGP AS number.	64512

Parameter	Description	Value
HA Mode	Working mode of the VPN gateway. **NOTE** The HA modes of the VPN gateway and customer gateway must be the same. If the customer gateway performs path consistency checks and does not support asymmetric routing, you are advised to create a VPN gateway in active/standby mode.	Active/Standby
Active EIP	EIP 1 used by the VPN gateway to communicate with the on-premises data center.	1.1.1.2
Standby EIP	EIP 2 used by the VPN gateway to communicate with the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-103 describes the parameters for creating a customer gateway.

Table 1-103 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-strongswan
Identifier	– **IP Address**: Specify the IP address of the customer gateway. – **FQDN**: Set the fully qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). If the customer gateway does not have a fixed IP address, select **FQDN**. **NOTE** Ensure that an ACL rule has been configured on the customer gateway to permit UDP port 4500.	1.1.1.1

Step 5 Configure VPN connections.

In this scenario, strongSwan has only one public IP address. A VPN connection needs to be created between the public IP address of strongSwan and each of the active and standby EIPs of the Huawei Cloud VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Create VPN Connection**.
2. Configure VPN connections as prompted.

   Table 1-104 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-104 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select **Policy-based**.	Policy-based

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the health check, PSK, confirm PSK, and policies for the VPN gateway IP address of connection 1.	*Set parameters based on the site requirements.*
PSK, Confirm PSK	The value must be the same as the PSK of the connection configured on the customer gateway.	Test@123
Policy	A policy rule defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. – Source CIDR Block The source CIDR block must contain some local subnets. 0.0.0.0/0 indicates any address. – Destination CIDR Block The destination CIDR block must contain all customer subnets.	– Source CIDR block 1: 192.168.0.0/24 – Destination CIDR block 1: 172.16.0.0/16 – Source CIDR block 2: 192.168.1.0/24 – Destination CIDR block 2: 172.16.0.0/16

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those of strongSwan.	– IKE Policy ▪ Encryption Algorithm: AES-128 ▪ Authentication Algorithm: SHA1 ▪ DH Algorithm: Group 2 ▪ Version: v2 ▪ Lifetime (s): 86400 ▪ Local ID: IP Address ▪ Customer ID: IP Address – IPsec Policy ▪ Encryption Algorithm: AES-128 ▪ Authentication Algorithm: SHA1 ▪ PFS: DH group 2 ▪ Transfer Protocol: ESP ▪ Lifetime (s): 86400
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** It is recommended that the configuration of connection 2 be the same as that of connection 1.	Enabled

----End

1.9.2.3 Configuration in the On-Premises Data Center

Notes and Constraints

This section uses a strongSwan device that runs the CentOS 8.2 64-bit operating system as an example. For other operating systems, see the official documentation of strongSwan.

Procedure

Step 1 Download the strongSwan installation package from the official website.

The installation and configuration methods may vary according to the strongSwan version. This example uses strongSwan 5.9.10 as an example.

Step 2 Install the strongSwan software.

1. Log in to the CentOS 8.2 operating system as the **root** user and open the CLI window.
2. Upload the strongSwan installation package to a directory on the CentOS operating system, for example, **/opt/**.
3. Run the following command to go to the directory where the installation package is stored:

   cd /opt/
4. Run the following command to install strongSwan:

   rpm -ivh strongswan-5.9.10-1.el8.x86_64.rpm --force --nodeps

   NOTE

   strongswan-5.9.10-1.el8.x86_64.rpm is the installation package name. Replace it with the actual one.

   If the following information in bold is displayed, the installation is successful.

   ```
   Verifying...                          ################################# [100%]
   Preparing...                          ################################# [100%]
   Updating / installing...
     1:strongswan-5.9.10-1.el8           ################################# [100%]
   ```
5. Run the following command to check the strongSwan version:

   strongswan version

   The following information in bold is displayed:

   ```
   Linux strongSwan U5.9.10/K4.18.0-348.7.1.el8_5.x86_64
   University of Applied Sciences Rapperswil, Switzerland
   ```

Step 3 Configure firewall policies.

- Run the following command to permit the ESP protocol (IP protocol number: 50):

  iptables -I INPUT -p 50 -j ACCEPT
- Run the following command to permit UDP port 500:

  iptables -I INPUT -p udp --dport 500 -j ACCEPT
- Run the following command to permit UDP port 4500:

  iptables -I INPUT -p udp --dport 4500 -j ACCEPT

Step 4 Enable the traffic forwarding function.

Run the following command to enable traffic forwarding:

echo 1 > /proc/sys/net/ipv4/ip_forward

The preceding command is a temporary command. After the strongSwan device is restarted, you need to run this command again. If you want to permanently enable traffic forwarding for the strongSwan device, perform the following operations:

1. Run the following command to open the **/etc/sysctl.conf** file:

   vi /etc/sysctl.conf

2. Add the following configuration to the file:

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

3. Press **Esc**, enter **:wq**, and press **Enter**.

   The system saves the configuration and exits the editor.

4. Run the following command for the configuration to take effect:

   sudo sysctl -p

Step 5 Configure dual tunnels.

1. Run the following command to back up the strongSwan configuration file:

   mv /etc/strongswan/swanctl/swanctl.conf /etc/strongswan/swanctl/swanctl.conf.bak

2. Run the following command to open the strongSwan configuration file:

   vi /etc/strongswan/swanctl/swanctl.conf

3. Add the following configurations according to the data plan:

   ```
   connections {
     vco1 {              # Add the VPN configuration of IPsec VPN tunnel 1.
       version = 2       # Specify the IKE version, which must be the same as that configured for Huawei Cloud connection 1. The value 2 indicates IKEv2.
       local_addrs  = 172.16.0.195       # Specify the local IP address.
       remote_addrs = 1.1.1.2        # Set the remote IP address of tunnel 1 to the gateway IP address of Huawei Cloud connection 1.
       dpd_delay = 10
       rekey_time = 86400            # Specify the SA lifetime of tunnel 1, which must be the same as that specified in the IKE configuration of Huawei Cloud connection 1.
       over_time = 1800
       proposals = aes128-sha1-modp1024   # Specify the encryption algorithm, authentication algorithm, and DH algorithm of tunnel 1, which must be the same as those specified in the IKE configuration of Huawei Cloud connection 1. modp1024 corresponds to DH group 2.
       encap = yes

       local {
         auth = psk            # Set the local authentication mode to PSK.
         id = 1.1.1.1          # Specify the public IP address of the local egress.
       }
       remote {
         auth = psk            # Set the authentication mode of Huawei Cloud to PSK.
         id = 1.1.1.2          # Specify the active EIP of Huawei Cloud connection 1.
       }
       children {
         vco_child1 {
           local_ts  = 172.16.0.0/16     # Set the private CIDR block of the local protected data flows to 172.16.0.0/16.
           remote_ts = 192.168.0.0/24     # Set the VPC CIDR block of the protected data flows at the Huawei Cloud site to 192.168.0.0/24.
           mode = tunnel
           rekey_time = 85500
           life_time = 86400        # Specify the SA lifetime of tunnel 1, which must be the same as that specified in the IPsec configuration of Huawei Cloud connection 1.
           dpd_action = restart
   ```



```
        start_action = start
        close_action = start
        esp_proposals = aes128-sha1-modp1024   # Specify the encryption algorithm, authentication algorithm, and DH algorithm of tunnel 1, which must be the same as those specified in the IPsec configuration of Huawei Cloud connection 1. modp1024 corresponds to DH group 2.
      }
    }
  }
  vco2 {              # Add the VPN configuration of IPsec VPN tunnel 2.
    version = 2       # Specify the IKE version, which must be the same as that configured for Huawei Cloud connection 2. The value 2 indicates IKEv2.
    local_addrs  = 172.16.0.195       # Specify the local IP address.
    remote_addrs = 2.2.2.2      # Set the remote IP address of tunnel 2 to the gateway IP address of Huawei Cloud connection 2.
    dpd_delay = 10
    rekey_time = 84600          # Specify the SA lifetime of tunnel 2, which must be the same as that specified in the IKE configuration of Huawei Cloud connection 2.
    over_time = 1800
    proposals = aes128-sha1-modp1024      # Specify the encryption algorithm, authentication algorithm, and DH algorithm of tunnel 2, which must be the same as those specified in the IKE configuration of Huawei Cloud connection 2. modp1024 corresponds to DH group 2.
    encap = yes

    local {
      auth = psk        # Set the local authentication mode to PSK.
      id = 1.1.1.1      # Specify the public IP address of the local egress.
    }
    remote {
      auth = psk        # Set the authentication mode of Huawei Cloud to PSK.
      id = 2.2.2.2      # Specify the standby EIP of Huawei Cloud connection 2.
    }
    children {
      vco_child2 {
        local_ts  = 172.16.0.0/16     # Set the private CIDR block of the local protected data flows to 172.16.0.0/16.
        remote_ts = 192.168.0.0/24      # Set the VPC CIDR block of the protected data flows at the Huawei Cloud site to 192.168.0.0/24.
        mode = tunnel
        rekey_time = 85500
        life_time = 86400       # Specify the SA lifetime of tunnel 2, which must be the same as that specified in the IPsec configuration of Huawei Cloud connection 2.
        dpd_action = restart
        start_action = start
        close_action = start
        esp_proposals = aes-sha1-modp1024     # Specify the encryption algorithm, authentication algorithm, and DH algorithm of tunnel 2, which must be the same as those specified in the IPsec configuration of Huawei Cloud connection 2. modp1024 corresponds to DH group 2.
      }
    }
  }
}

secrets {
  ike-vco1 {
    secret = Test@123   # Specify the PSK of tunnel 1, which must be the same as that configured for Huawei Cloud connection 1.
  }
  ike-vco2 {
    secret = Test@123   # Specify the PSK of tunnel 2, which must be the same as that configured for Huawei Cloud connection 2.
  }
}
```

4. Press **Esc**, enter **:wq**, and press **Enter**.

   The system saves the configuration and exits the editor.

5. Run the following command to restart the strongSwan process:

   systemctl restart strongswan

6. Run the following command to check the tunnel status:

   watch swanctl --list-sas

   Information similar to the following is displayed:

   ```
   ecs-b6b4-strongswan: Tue Mar 11 16:51:19 2025
   plugin 'sqlite': failed to load - sqlite_plugin_create not found and no plugin file available
   vco2: #2, ESTABLISHED, IKEv2, c2786dfe3bc7d7e0_i* 75e148eba08c17e1_r
   ...
   ...
   vco1: #1, ESTABLISHED, IKEv2, 3d3396aa3797c86f_i* d89bb869311c580c_r
   ...
   ...
   ```

----End

1.9.2.4 Verification

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

  Huawei Cloud

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

- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.

2 S2C Classic VPN

2.1 Overview

This guide helps you configure your local VPN device to implement interconnection between your network and a Huawei Cloud 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

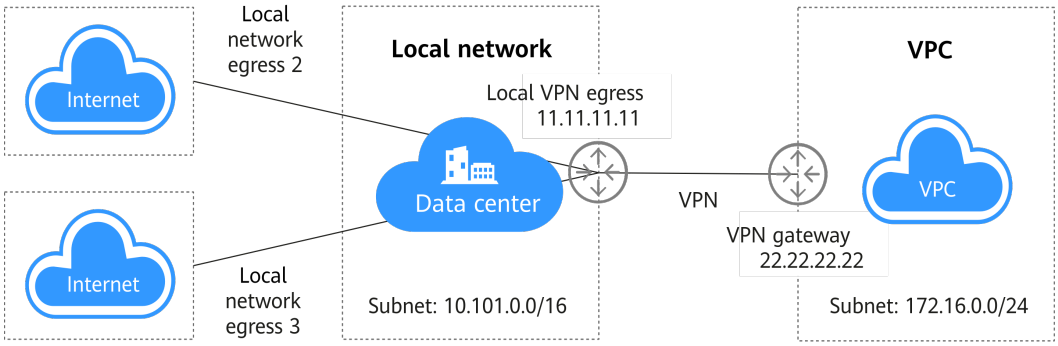
Scenarios

This section describes how to purchase a VPN gateway and create 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

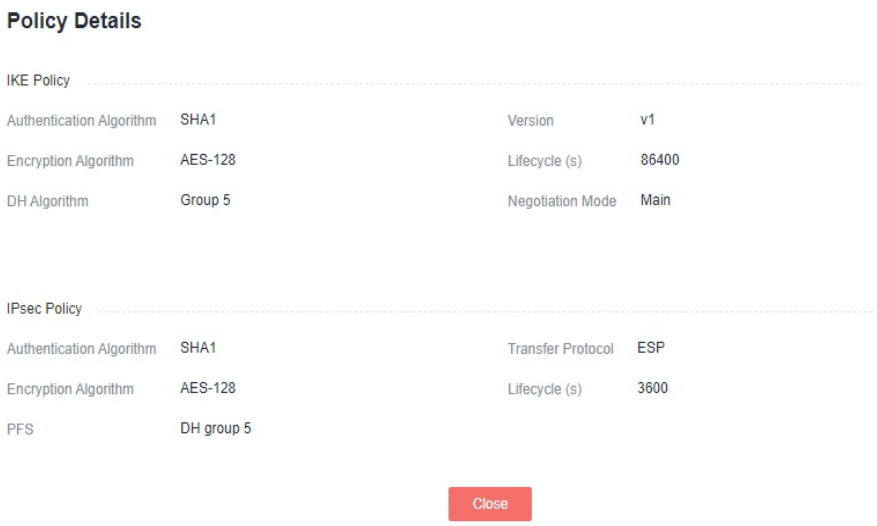
As shown in **Figure 2-1**, the local data center has multiple Internet egresses. The egress 11.11.11.11 is specified to establish a VPN connection with a Huawei Cloud VPC. The subnet of the local data center is 10.10.0.0/16, and the VPC subnet on Huawei Cloud is 172.16.0.0/24. The IP address of the 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 VPN connection policies on Huawei Cloud based on **Figure 2-2**.

Figure 2-2 Policy details



Configuration Procedure

This example describes how to configure a VPN when a FortiGate firewall is used in 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 a policy for access to the cloud from the local data center.
2. Configure a policy for access to 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:

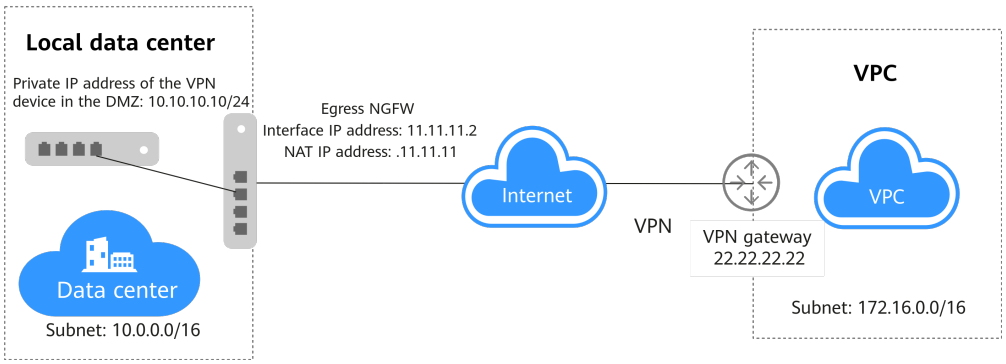
- Use the firewall to establish a VPN connection with the cloud.
- Use the VPN device in the DMZ zone and the NAT traversal technique to establish a VPN connection with the cloud.

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

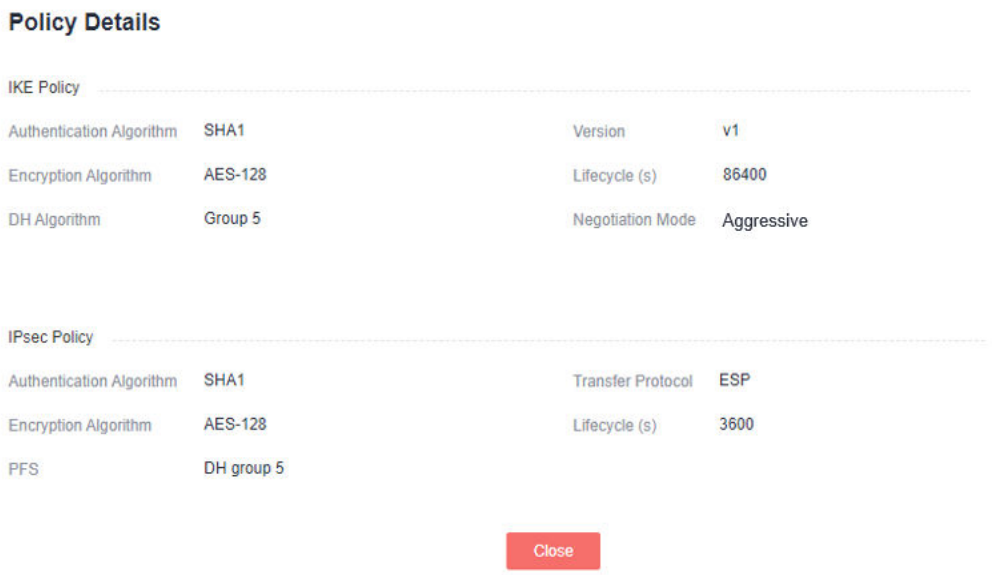
Create a VPN connection to connect an on-premises network to the VPC subnet.

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 a 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 when a 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.

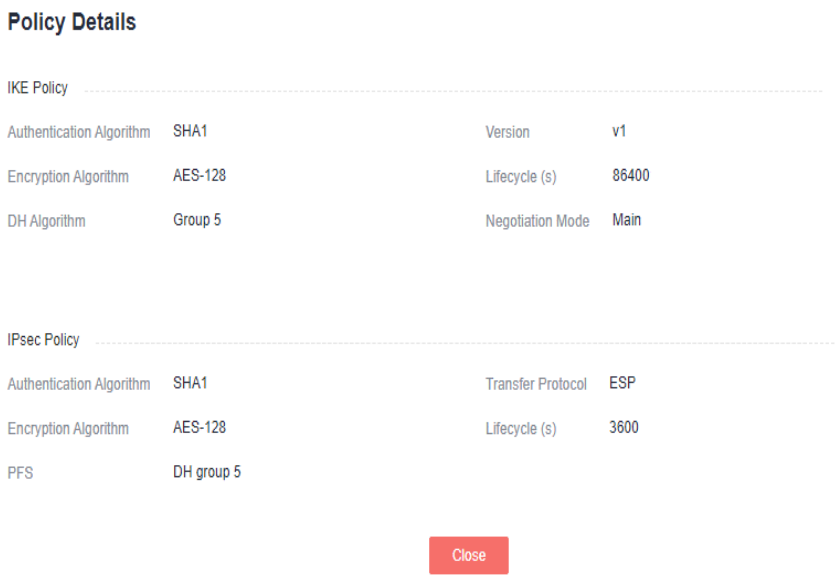
This following describes the configuration details if TheGreenBow IPsec VPN Client is used.

- **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

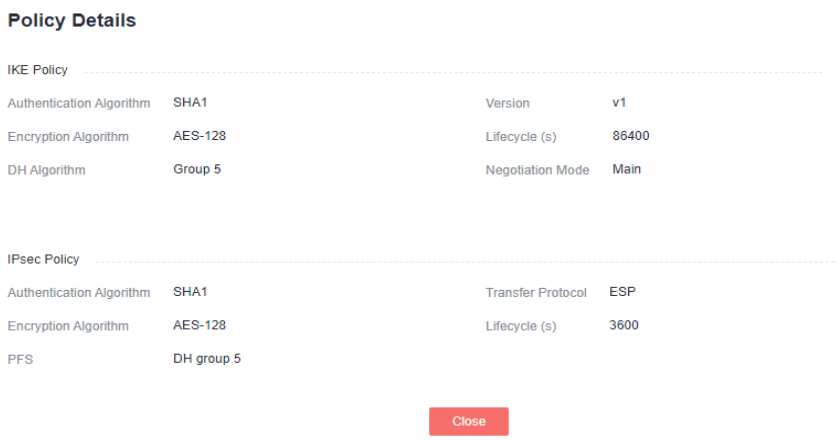
- **Scenario 1: Cloud desktop + VPC**
  - The VPC, subnet, and ECS have been configured on the cloud.
  - The VPN gateway and VPN connection on the cloud have been configured.

    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.

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.

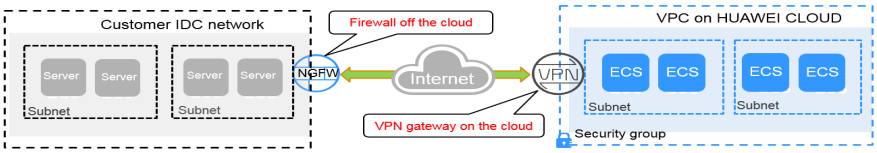
The VPN gateway IP address of the VPC is 11.11.11.11 and the local subnet is 192.168.200.0/24.

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 Run the following command to install the Openswan client:

yum install -y openswan

Step 2 Run the following command to enable IPv4 forwarding:

vim /etc/sysctl.conf

1. Add the following content to this file:
   ```
   net.ipv4.ip_forward = 1
   ```
2. Run the following command to make the forwarding configuration take effect:

   /sbin/sysctl -p

Step 3 Run the following command to check whether the firewall is disabled or whether the data flow forwarding is allowed:

iptables -L

```
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 Run the following command to 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 Run the following command to configure an 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 **How Many Bits Do the DH Groups Used by VPN Have?**.

Run the following command to verify the configuration:

ipsec verify

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 Run the following commands to 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 following command to query the IPsec status:

ipsec --status

The following shows a part of the result:

```
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.

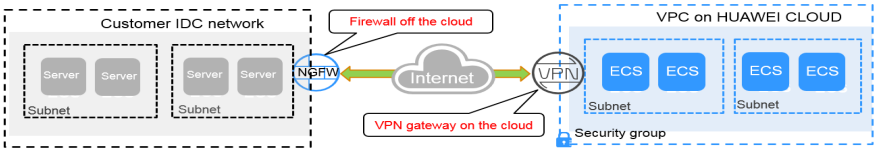
The VPN gateway IP address of the VPC is 11.11.11.11 and the local subnet is 192.168.200.0/24.

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 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 Run the following command to install the IPsec VPN client:

yum install strongswan

During the installation, select **Y**. If **Complete!** is displayed, the installation is complete. The strongSwan configuration files are all stored in the **/etc/strongswan** directory. You only need to edit the **ipsec.conf** and **ipsec.secrets** files.

Step 2 Run the following command to enable IPv4 forwarding:

vim /etc/sysctl.conf

1. Add the following content to this file:
   ```
   net.ipv4.ip_forward = 1
   ```
2. Run the following command to make the forwarding configuration take effect:

   /sbin/sysctl -p

Step 3 Run the following command to check whether the firewall is disabled or whether the data flow forwarding is allowed:

iptables -L

```
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 Run the following command to configure the pre-shared key:

vim /etc/strongswan/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 (uppercase)+Pre-shared key. There are spaces on both sides of the colon. The key is enclosed in double quotation marks.

Step 5 Run the following command to configure an 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 DH group in the IKE policy based on the configuration of the VPN gateway.
 esp=aes128-sha1-modp1536!                        # Set the algorithm and DH 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 **How Many Bits Do the DH Groups Used by VPN Have?**.

Step 6 Run the following commands to 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 following command to query the run time of the connection.

strongswan statusall

```
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
```

Run the following command to ping the IP address of the host where the IPsec client is installed:

VPC1 ping

```
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
```


3 P2C VPN

3.1 Using the CCM to Manage a Server Certificate

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select the desired region and project.

Step 3 Click in the upper left corner, and choose **Networking** > **Virtual Private Network**.

Step 4 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **Configure Server** in the **Operation** column.

Step 6 On the **Server** tab page, set **Server Certificate** to **Existing certificate**, and click **Upload** in the drop-down list box. The **Cloud Certificate & Manager** page is displayed.

Step 7 On the **SSL Certificate Manager** page, click the **Hosted Certificates** tab, click **Upload Certificate**, and enter related information as prompted.

Table 3-1 describes the parameters for uploading a certificate.

Table 3-1 Parameters for uploading an international standard certificate

Parameter	Description
Certificate standard	Select **International**.
Certificate Name	User-defined name of a certificate.

Parameter	Description
Enterprise Project	Select the enterprise project to which the SSL certificate is to be added.
Certificate File	Use a text editor (such as Notepad++) to open the certificate file in CER or CRT format to be uploaded, and copy the certificate content to this text box. You need to upload a combined certificate file that contains both the server certificate content and CA certificate content. The CA certificate content must be pasted below the server certificate content. **NOTE** If you do not have a certificate, you can generate a self-issued certificate and upload it. For details, see **Using Easy-RSA to Issue Certificates (Server and Client Sharing a CA Certificate)**. For the format of the certificate file content to be uploaded, see **Figure 3-1**.
Private Key	Use a text editor (such as Notepad++) to open the certificate file in KEY format to be uploaded, and copy the private key content to this text box. You only need to upload the private key of the server certificate. For the format of the private key content to be uploaded, see **Figure 3-1**.

Figure 3-1 Format of the certificate content to be uploaded

NOTE

The common name (CN) of a server certificate must be in the domain name format.

Step 8 Click **Submit**. The certificate is uploaded.

Step 9 In the certificate list, verify that the certificate status is **Hosted**.

----End

3.2 Using Easy-RSA to Issue Certificates (Server and Client Sharing a CA Certificate)

Scenario

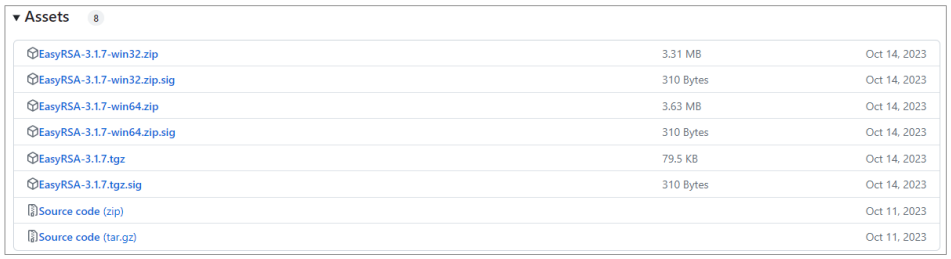
Easy-RSA is an open-source certificate management tool used to generate and manage digital certificates.

This example describes how to use Easy-RSA to issue certificates on the Windows operating system in the scenario where the server and client share a CA certificate. In this example, Easy-RSA 3.1.7 is used. For other software versions, visit the official website for the corresponding operation guide.

Procedure

1. Download an Easy-RSA installation package to the **D:** directory based on your Windows operating system.
   - 32-bit Windows operating system: Download **EasyRSA-3.1.7-win32.zip**.
   - 64-bit Windows operating system: Download **EasyRSA-3.1.7-win64.zip**.

   In this example, **EasyRSA-3.1.7-win64** is downloaded.

2. Decompress **EasyRSA-3.1.7-win64.zip** to a specified directory, for example, **D:\EasyRSA-3.1.7**.
3. Go to the **D:\EasyRSA-3.1.7** directory.
4. Enter **cmd** in the address bar and press **Enter** to open the CLI.
5. Run the following command to start Easy-RSA:

   .\EasyRSA-Start.bat

   Information similar to the following is displayed:

   ```
   Welcome to the EasyRSA 3 Shell for Windows.
   Easy-RSA 3 is available under a GNU GPLv2 license.

   Invoke './easyrsa' to call the program. Without commands, help is displayed.

   EasyRSA Shell
   #
   ```

6. Run the following command to initialize the PKI environment:

   ./easyrsa init-pki

   Information similar to the following is displayed:


```
Notice
------
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* D:/EasyRSA-3.1.7/pki

Using Easy-RSA configuration:
* undefined


EasyRSA Shell
#
```

After the command is executed, the **pki** folder is automatically generated in the **D:\EasyRSA-3.1.7** directory.

7. Set parameters.
   a. Copy the **vars.example** file in **D:\EasyRSA-3.1.7** to the **D:\EasyRSA-3.1.7\pki** directory.
   b. Rename **vars.example** in the **D:\EasyRSA-3.1.7\pki** directory to **vars**.

      NOTE

      By default, the **vars** file uses the same parameter settings as the **vars.example** file. You can also set parameters in the **vars** file as required.

8. Run the following command to generate a CA certificate:

   ./easyrsa build-ca nopass

   Information similar to the following is displayed:

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.....+..+.............+......+........+...+...+....++++++++++++++++++++++++++++++++++++++++
+*.+.+.....+..........+............+...++++++++++++++++++++++++++++++++++++++++
+*.............+.....+......+...+....+..+..........+.....+....+..............+..+.........+.............+......+..+...+....+..+.+.........+.....+.........+....+.....
.....+...+...+.....+.........................+...+.+.....+....+...+.........+...+...+...+.....+......+.........................++++++
.++++++++++++++++++++++++++++++++++++++++*.........+..........+++++++++++++++++++++++++++++++++
+++++++*.+......++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:p2cvpn.com    # Set a name for the CA certificate.

Notice
------
CA creation complete. Your new CA certificate is at:
* D:/EasyRSA-3.1.7/pki/ca.crt


EasyRSA Shell
#
```

9. View the CA certificate and private key.
   – By default, the generated CA certificate is stored in the **D:\EasyRSA-3.1.7\pki** directory.

     In this example, the certificate **ca.crt** is generated.

– By default, the generated CA private key is stored in the **D:\EasyRSA-3.1.7\pki\private** directory.

  In this example, the private key **ca.key** is generated.

10. Run the following command to generate a server certificate and its private key:

    ./easyrsa build-server-full *p2cserver.com* **nopass**

    NOTE

    In this command, ***p2cserver.com*** is the common name (CN) of the server certificate. Replace it with the actual CN. The CN must be in the domain name format; otherwise, the certificate cannot be managed by the Cloud Certificate & Manager (CCM).

    Information similar to the following is displayed:

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.+.....+.....+.....+.....+.+.....+.....+....+.....+.....+.+..+.....+.....+....+.....+..+.....+.+.....
....+.....+.....++++++++++++++++++++++++++++++++++++++++*...+.....+.....+.....+...+++++++++++++++
++++++++++++++++++++++
+*..+...+.....+.....+.....+....+.....+.....+....+.....+....+.....+...+.....+...+..+.....+..+.....+.....+...+.....+.....
.....+.....+..+.....+..+.....+.....+.....+....+.....+....+.....+.....+.+..+.....+.....+.....+.....+.....+.....
...+...+....+..+.....+.....+.....+.+...+..+...+.+.....+.....+...+....+.....+.....+....+...+..+.....+..+...+.....+..+....
..+.....+.....+...+..+.....+.....+......++++++
.....+.+.....+...+.....+.....+...+.+.....+.+.....+.....++++++++++++++++++++++++++++++++++++++++
+*...+.....+...+.+.....+.....+.....++++++++++++++++++++++++++++++++++++++++
+*.....+.....+.+...+.....+.+.....+.+...+...+.....+.....+.....+.....+...+....+...+..+.+.....+.....
...+.+..+.+.....+....+.....+.....+.....+....+.....+...+.....+.....+.+.....+...+.....+.....+....+.....+.
.....+..+.....+.....+.+.....+...+.....+.....+.....+.....+.....+.....+.....+.....+...+.+...+
..+...+.+.....+.+.....+.....+.....+..+....+..+....+.....+.....+.....+...+...+..+.....+...+.....+..+.
.....+.....+.....+.....+.....+...+.....+.....+.....+...+.....+.+.....+.+...+.....+.+...+...+.....+..+.....+..
.....+.....+...+...+.....+.....+...+....+.....+.....+...+.....+.....+.....+.+.....+....+.....+.+..+.....+.....
..+...+.....+.+...+.....+.+.....+...++++++
-----

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7/pki/reqs/p2cserver.com.req
* key: D:/EasyRSA-3.1.7/pki/private/p2cserver.com.key

You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for '825' days:

subject=
    commonName                = p2cserver.com

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes    # Enter yes to continue.

Using configuration from D:/EasyRSA-3.1.7/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'p2cserver.com'
Certificate is to be certified until Sep 22 09:56:54 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
```

```
Certificate created at:
* D:/EasyRSA-3.1.7/pki/issued/p2cserver.com.crt

Notice
------
Inline file created:
* D:/EasyRSA-3.1.7/pki/inline/p2cserver.com.inline


EasyRSA Shell
#
```

11. View the server certificate and private key.
    - By default, the generated server certificate is stored in the **D:\EasyRSA-3.1.7\pki\issued** directory.

      In this example, the server certificate **p2cserver.com.crt** is generated.
    - By default, the generated server private key is stored in the **D:\EasyRSA-3.1.7\pki\private** directory.

      In this example, the server private key **p2cserver.com.key** is generated.
12. Run the following command to generate a client certificate and its private key:

    ./easyrsa build-client-full *p2cclient.com* **nopass**

    NOTE

    In this command, the client certificate name (for example, ***p2cclient.com***) must be different from the server certificate name (for example, ***p2cserver.com***).

    Information similar to the following is displayed:

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.......++++++++++++++++++++++++++++++++++++++++*...+...+...+.....+...+....+......+......+........+.+.....+............++++
++++++++++++++++++++++++++++++++
+*.+.....+.+.....+.........+.......+..+...+.......+...+..+......+.+......+........+....+...+...+..+.......+......+.....+...........+...........+....+......+.....+
.........+......+.+..+...+..........+........+......+....+.....+...........+.......+.....+.............+..+.+...........+..........+...+..+.........+......+.+........
+.........+.+.................+..+..........+...+.....+.+...........+....+.....+.........+....+.....+.....+...+..+....+..+.......+...+.
............+.....+.............+.+.........+.......+.....+....+.........+..+.............+...........+..+.............+...+...+..++++++
..+.....+.......+.....+.........+....++++++++++++++++++++++++++++++++++++++++++++++++*.....+......+..+++++++++++++++++
++++++++++++++++++++++
+*.......+.+.....+....+.........+...+.....+.........+...+.................+...+....+.....+.+...+......+......+...+.........+..+...+...+....+.........+..+...+.......
.............+......+.....+.+...+...+.........+.....+.....................+...+...+......+.+..+......+.+.......+.....+...+..........+..+.............+.......+.........+.....
+......+.+..+.............+.................+..+...+....+......+.....+...+....+..+......+.........+.........++++++
-----


Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7/pki/reqs/p2cclient.com.req
* key: D:/EasyRSA-3.1.7/pki/private/p2cclient.com.key

You are about to sign the following certificate:
Request subject, to be signed as a client certificate
for '825' days:

subject=
    commonName                = p2cclient.com

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes    # Enter yes to continue.
```



```
Using configuration from D:/EasyRSA-3.1.7/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'p2cclient.com'
Certificate is to be certified until Sep 22 09:58:26 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* D:/EasyRSA-3.1.7/pki/issued/p2cclient.com.crt

Notice
------
Inline file created:
* D:/EasyRSA-3.1.7/pki/inline/p2cclient.com.inline


EasyRSA Shell
#
```

13. View the client certificate and private key.
    - By default, the generated client certificate is stored in the **D:\EasyRSA-3.1.7\pki\issued** directory.

      In this example, the client certificate **p2cclient.com.crt** is generated.
    - By default, the generated client private key is stored in the **D:\EasyRSA-3.1.7\pki\private** directory.

      In this example, the client private key **p2cclient.com.key** is generated.

3.3 Using Easy-RSA to Issue Certificates (Server and Client Using Different CA Certificates)

Scenario

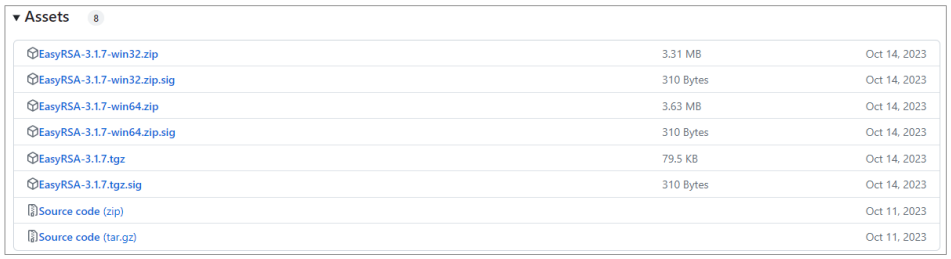
Easy-RSA is an open-source certificate management tool used to generate and manage digital certificates.

This example describes how to use Easy-RSA to issue certificates on the Windows operating system in the scenario where the server and client use different CA certificates. In this example, Easy-RSA 3.1.7 is used. For other software versions, visit the official website for the corresponding operation guide.

Procedure

1. Download an Easy-RSA installation package to the **D:** directory based on your Windows operating system.
   - 32-bit Windows operating system: Download **EasyRSA-3.1.7-win32.zip**.
   - 64-bit Windows operating system: Download **EasyRSA-3.1.7-win64.zip**.

   In this example, **EasyRSA-3.1.7-win64** is downloaded.



2. Decompress **EasyRSA-3.1.7-win64.zip** to a specified directory, for example, **D:\EasyRSA-3.1.7**.
3. Go to the **D:\EasyRSA-3.1.7** directory.
4. Enter **cmd** in the address bar and press **Enter** to open the CLI.
5. Run the following command to start Easy-RSA:

   .\EasyRSA-Start.bat

   Information similar to the following is displayed:

   ```
   Welcome to the EasyRSA 3 Shell for Windows.
   Easy-RSA 3 is available under a GNU GPLv2 license.

   Invoke './easyrsa' to call the program. Without commands, help is displayed.

   EasyRSA Shell
   #
   ```

6. Run the following command to initialize the PKI environment:

   ./easyrsa init-pki

   Information similar to the following is displayed:

   ```
   Notice
   ------
   'init-pki' complete; you may now create a CA or requests.

   Your newly created PKI dir is:
   * D:/EasyRSA-3.1.7/pki

   Using Easy-RSA configuration:
   * undefined


   EasyRSA Shell
   #
   ```

   After the command is executed, the **pki** folder is automatically generated in the **D:\EasyRSA-3.1.7** directory.

7. Set parameters.

   a. Copy the **vars.example** file in **D:\EasyRSA-3.1.7** to the **D:\EasyRSA-3.1.7\pki** directory.

   b. Rename **vars.example** in the **D:\EasyRSA-3.1.7\pki** directory to **vars**.

   > NOTE
   >
   > By default, the **vars** file uses the same parameter settings as the **vars.example** file. You can also set parameters in the **vars** file as required.

8. Generate a server CA certificate and private key.

   a. Copy the decompressed **EasyRSA-3.1.7** folder to the **D:** directory, and rename the folder, for example, **EasyRSA-3.1.7 - server**.

   b. Go to the **D:\EasyRSA-3.1.7 - server** directory.

c. In the address bar of the **D:\EasyRSA-3.1.7 - server** folder, enter **cmd** and press **Enter** to open the CLI.

d. Run the following command to start Easy-RSA:

.\EasyRSA-Start.bat

Information similar to the following is displayed:

```
Welcome to the EasyRSA 3 Shell for Windows.
Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easyrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell
#
```

e. Run the following command to generate a server CA certificate:

./easyrsa build-ca nopass

NOTE

When this command is run, set **[Easy-RSA CA]** to the name of the server CA certificate as prompted, for example, **p2cvpn_server.com**.

Information similar to the following is displayed:

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7 - server/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
..+.....+...+.........+..+.......+..+.........+...+...+..+......+.......+...++++++++++++++++++++++++++++++++++++++++
++*.++++++++++++++++++++++++++++++++++++++++*.........+..........+...+......++++++
.......+.......+...+......+...+.....+...+...++++++++++++++++++++++++++++++++++++++++
+*......+.....+....+..+....+......+...+......+...+......+.....+.++++++++++++++++++++++++++++++++++++++++
+*.......+......+.......+..............+.+...+.....+....+........+.........+....+..+.............+.+.....+....+.+..+.+.+.........+.....+.
..+...................+.......+..+.......+.....+..........+......+..+.+.....+.+.....+....+.....+.......+...+.........+..+......+...+.......+...+.........+...
...+......+...........+....+......+...+..+...+......+...+.+.....+.......+..+.......+...+...+..+..............+.........+.........+.+.........+.........+....+
.........+.....+.........+.................+.....+.+........+.......+.....+.+........+....+..+...+..........+..+......+...+.........+.................+......+....
.+....+......+......+.............+..+......+...+.......+..................+.+......+......+..+.+...........+.........+.........+.+......++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:p2cvpn_server.com    # Set a name for the server CA certificate.

Notice
------
CA creation complete. Your new CA certificate is at:
* D:/EasyRSA-3.1.7 - server/pki/ca.crt


EasyRSA Shell
#
```

9. View the server CA certificate and private key.
   - By default, the generated server CA certificate is stored in the **D:\EasyRSA-3.1.7 - server\pki** directory.

     In this example, the server certificate **ca.crt** is generated.
   - By default, the generated server CA private key is stored in the **D:\EasyRSA-3.1.7 - server\pki\private** directory.

     In this example, the server private key **ca.key** is generated.

10. Run the following command to generate a server certificate and its private key:

    ./easyrsa build-server-full *p2cserver.com* **nopass**

    NOTE

    In this command, ***p2cserver.com*** is the common name (CN) of the server certificate. Replace it with the actual CN. The CN must be in the domain name format; otherwise, the certificate cannot be managed by the Cloud Certificate & Manager (CCM).

    Information similar to the following is displayed:

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7 - server/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.+.+......+...+.....+......+...+.......+.....+.+...+..+...+....+.....+......++++++++++++++++++++++++++++++++++++++++
+*....+..+....++++++++++++++++++++++++++++++++++++++
+*.................+.......+..+.+..+..+......+.............+...+...+.........+........+.........+...+......+.+...+...+.....+....+.....+.+.............+.....+...+.
...+...........+....+..+......+.............+.........+........+...+.+......+.....+.....+.....+.....+.....+.+.....+....+.....+...+.....+...+..+.............+.+........+.........
+.+..+.........+......+...+....+.....+....+.....+....+.....+.....+.....+.....+...+........+.+.....+.+.....................+.......+.....+.+..+.....+...+++
+++
.....+.....+...+.+.........+..+.+..+...++++++++++++++++++++++++++++++++++++++++++++*.......+...+........+....+...+..+...+++
++++++++++++++++++++++++++++++++++
+*..+.........+...+.......+......+..................+...+...+.............+...+....+........+.........+..........+......+...+............+.+..+.............+.+........+....
+...........+....+...........+......+.............+......+.....++++++
-----

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7 - server/pki/reqs/p2cserver.com.req
* key: D:/EasyRSA-3.1.7 - server/pki/private/p2cserver.com.key

You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for '825' days:

subject=
    commonName                = p2cserver.com

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes    # Enter yes to continue.

Using configuration from D:/EasyRSA-3.1.7 - server/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'p2cserver.com'
Certificate is to be certified until Oct  6 03:28:14 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* D:/EasyRSA-3.1.7 - server/pki/issued/p2cserver.com.crt

Notice
------
Inline file created:
* D:/EasyRSA-3.1.7 - server/pki/inline/p2cserver.com.inline


EasyRSA Shell
#
```


11. View the server certificate and private key.
    - By default, the generated server certificate is stored in the **D:\EasyRSA-3.1.7 - server\pki\issued** directory.

      In this example, the server certificate **p2cserver.com.crt** is generated.
    - By default, the generated server private key is stored in the **D:\EasyRSA-3.1.7 - server\pki\private** directory.

      In this example, the server private key **p2cserver.com.key** is generated.
12. Generate a client CA certificate and private key.
    a. Copy the decompressed **EasyRSA-3.1.7** folder to the **D:** directory, and rename the folder, for example, **EasyRSA-3.1.7 - client**.
    b. Go to the **EasyRSA-3.1.7 - client** directory.
    c. In the address bar of the **EasyRSA-3.1.7 - client** folder, enter **cmd** and press **Enter** to open the CLI.
    d. Run the following command to start Easy-RSA:

       .\EasyRSA-Start.bat

       Information similar to the following is displayed:

       ```
       Welcome to the EasyRSA 3 Shell for Windows.
       Easy-RSA 3 is available under a GNU GPLv2 license.

       Invoke './easyrsa' to call the program. Without commands, help is displayed.

       EasyRSA Shell
       #
       ```
    e. Run the following command to generate a client CA certificate:

       ./easyrsa build-ca nopass

       Information similar to the following is displayed:

       ```
       Using Easy-RSA 'vars' configuration:
       * D:/EasyRSA-3.1.7 - client/pki/vars

       Using SSL:
       * openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
       .++++++++++++++++++++++++++++++++++++++++
       +*.....+.+..+...+....+.....................+..+...+....+.........+.....+......+.+.....+....++++++++++++++++++++++++++++++++
       ++++++++*....+...+...+...+.............+.........++++++
       .+.........+.........+.+......+............+....+.....+.........+....+..+...+.+.........+......+......+...+.....+......+......+..........++++++++++
       ++++++++++++++++++++++++++++*.+.........+......+.++++++++++++++++++++++++++++++++++++++++
       ++*...........+.................+..............+.........+.+...+.....................+..+....+.....+..........+...+...+..+.++++++
       -----
       You are about to be asked to enter information that will be incorporated
       into your certificate request.
       What you are about to enter is what is called a Distinguished Name or a DN.
       There are quite a few fields but you can leave some blank
       For some fields there will be a default value,
       If you enter '.', the field will be left blank.
       -----
       Common Name (eg: your user, host, or server name) [Easy-RSA CA]:p2cvpn_client.com    # Set
       a name for the client CA certificate.

       Notice
       ------
       CA creation complete. Your new CA certificate is at:
       * D:/EasyRSA-3.1.7 - client/pki/ca.crt


       EasyRSA Shell
       #
       ```


13. View the client CA certificate and private key.
    - By default, the generated client CA certificate is stored in the **D:\EasyRSA-3.1.7 - client\pki** directory.

      In this example, the client certificate **ca.crt** is generated.
    - By default, the generated client CA private key is stored in the **D:\EasyRSA-3.1.7 - client\pki\private** directory.

      In this example, the client private key **ca.key** is generated.
14. Run the following command to generate a client certificate and its private key:

    ./easyrsa build-client-full *p2cclient.com* **nopass**

    NOTE

    In this command, the client certificate name (for example, ***p2cclient.com***) must be different from the server certificate name (for example, ***p2cserver.com***).

    Information similar to the following is displayed:

```
Using Easy-RSA 'vars' configuration:
* D:/EasyRSA-3.1.7 - client/pki/vars

Using SSL:
* openssl OpenSSL 3.1.2 1 Aug 2023 (Library: OpenSSL 3.1.2 1 Aug 2023)
.++++++++++++++++++++++++++++++++++++++++*.....+.....+...+.+.....+.+.....+.....+.+.....+.....++++++++++
++++++++++++++++++++++++++++
+*.....+...+...+..+.....+...+..+.+.....+.....+.+..+.+.....+.....+.....+.....+.....+..+....+...+.....+..+....+.....+..
.....+.....+...+...+.....+....+.....++++++
.+..+.....+.....++++++++++++++++++++++++++++++++++++++++*...+..++++++++++++++++++++++++++
++++++++++++*.....+.....+.....+.....+.....+....+.....+...+.....+....+...+.....+....+.....+.+.....+.....++
++++
-----

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: D:/EasyRSA-3.1.7 - client/pki/reqs/p2cclient.com.req
* key: D:/EasyRSA-3.1.7 - client/pki/private/p2cclient.com.key

You are about to sign the following certificate:
Request subject, to be signed as a client certificate
for '825' days:

subject=
    commonName                = p2cclient.com

Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes

Using configuration from D:/EasyRSA-3.1.7 - client/pki/openssl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'p2cclient.com'
Certificate is to be certified until Oct  7 11:19:52 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* D:/EasyRSA-3.1.7 - client/pki/issued/p2cclient.com.crt

Notice
```



```
------
Inline file created:
* D:/EasyRSA-3.1.7 - client/pki/inline/p2cclient.com.inline


EasyRSA Shell
#
```

15. View the client certificate and private key.
    - By default, the generated client certificate is stored in the **D:\EasyRSA-3.1.7 - client\pki\issued** directory.

      In this example, the client certificate **p2cclient.com.crt** is generated.
    - By default, the generated client private key is stored in the **D:\EasyRSA-3.1.7 - client\pki\private** directory.

      In this example, the client private key **p2cclient.com.key** is generated.

3.4 Using the CCM to Purchase Certificates

Context

In addition to purchasing certificates from CAs and issuing certificates by yourselves, you can use the CCM to purchase certificates, including the server and client certificates.

Constraints

If you purchase a server certificate using the CCM, you need to add the server root certificate content to the client configuration file.

Procedure

- Purchasing a server certificate
  a. Log in to the CCM console.
  b. **Purchase an SSL certificate**.
  c. **Apply for an SSL certificate**.

     Certificates purchased from the CCM are automatically hosted.
  d. **Download a root certificate**.
  e. Install the root certificate.

     Open the root certificate using a text editor (for example, Notepad++), and copy the certificate content to the end of the existing CA certificate in the client configuration file. For details, see **How Do I Fix an Incomplete SSL Certificate Chain?**.

     The format is as follows:

     ```
     ...
     <ca>
     -----BEGIN CERTIFICATE-----
     Default level-2 CA certificate content of the server
     -----END CERTIFICATE-----
     -----BEGIN CERTIFICATE-----
     Server root certificate content
     -----END CERTIFICATE-----
     </ca>
     ...
     ```


- Purchasing a client certificate
  a. Log in to the CCM console.
  b. **Purchase an SSL certificate**.
  c. **Apply for an SSL certificate**.
  d. **Download the SSL certificate**.

