Virtual Private Network

Administrator Guide

Issue 01

Date 2025-07-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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)

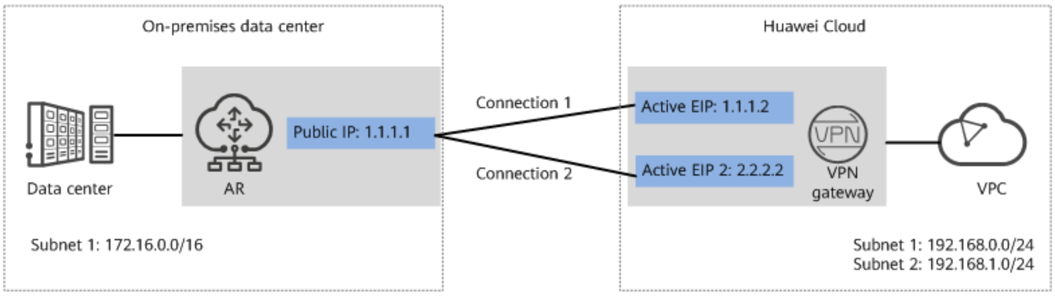
1.1.1 Static Routing Mode

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: 169.254.70.2/30 ● Customer tunnel interface address: 169.254.70.1/30	
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30	
	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

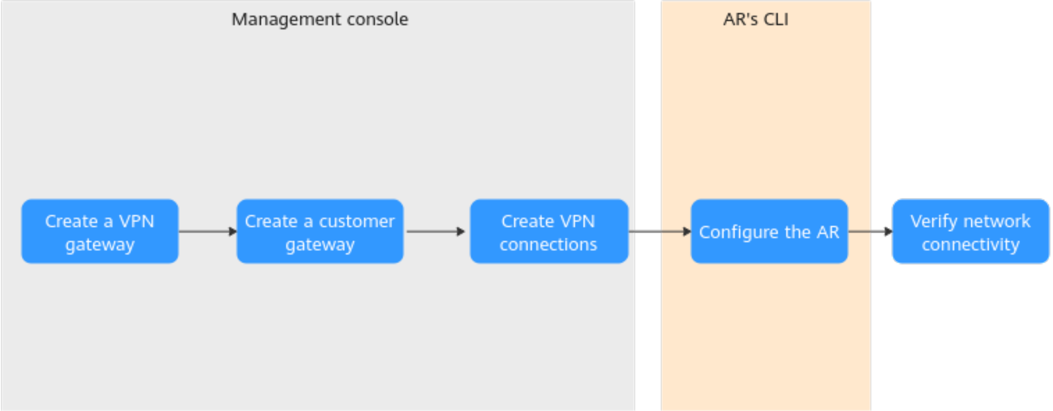


Table 1-2 Operation process description

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
HA Mode	Working mode of the VPN gateway.	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
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

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 and 214.0.0.0/8 cannot be used as customer subnets.	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, 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.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30

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: 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.	169.254.71.2/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----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.

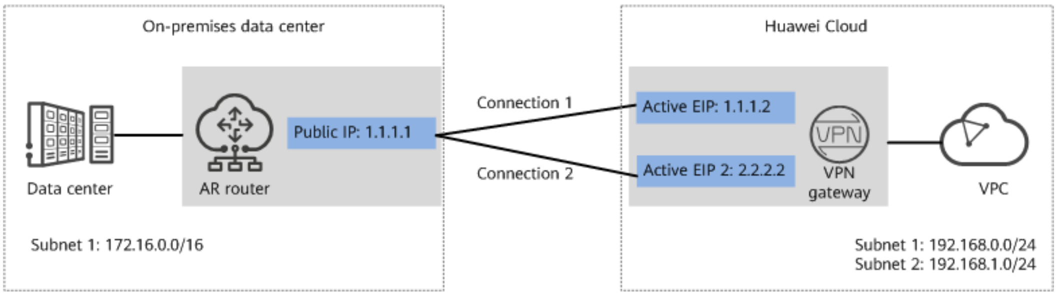
1.1.2 BGP Routing Mode

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: 169.254.70.2/30 ● Customer tunnel interface address: 169.254.70.1/30	
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30	
	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

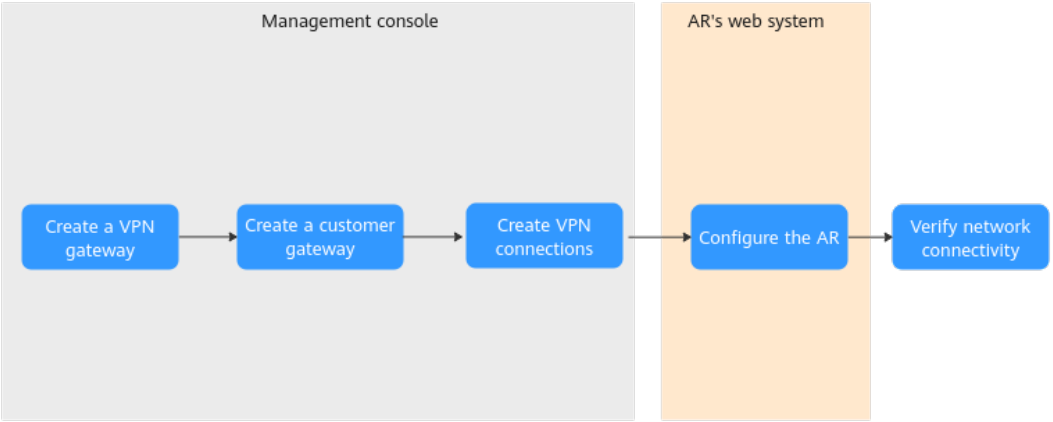


Table 1-7 Operation process description

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.	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
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
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 and 214.0.0.0/8 cannot be used as customer subnets.	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.*

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.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
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.	169.254.71.2/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----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

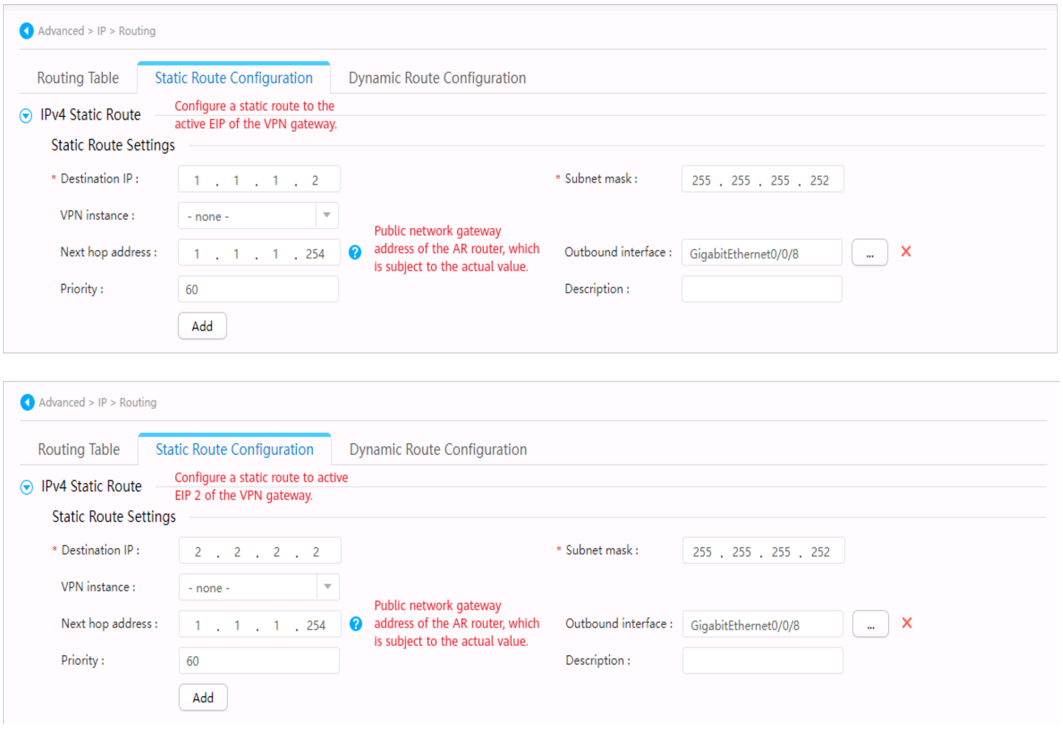
Step 1 Log in to the web system of the AR router.

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**, as shown in **Figure 1-5**.

Figure 1-5 Configuring static routes



Configure a static route to the active EIP of the VPN gateway.

Static Route Settings

* Destination IP : 1 . 1 . 1 . 2
* Subnet mask : 255 . 255 . 255 . 252
VPN instance : - none -
Next hop address : 1 . 1 . 1 . 254
Public network gateway address of the AR router, which is subject to the actual value.
Outbound interface : GigabitEthernet0/0/8
Priority : 60
Description :

Configure a static route to active EIP 2 of the VPN gateway.

Static Route Settings

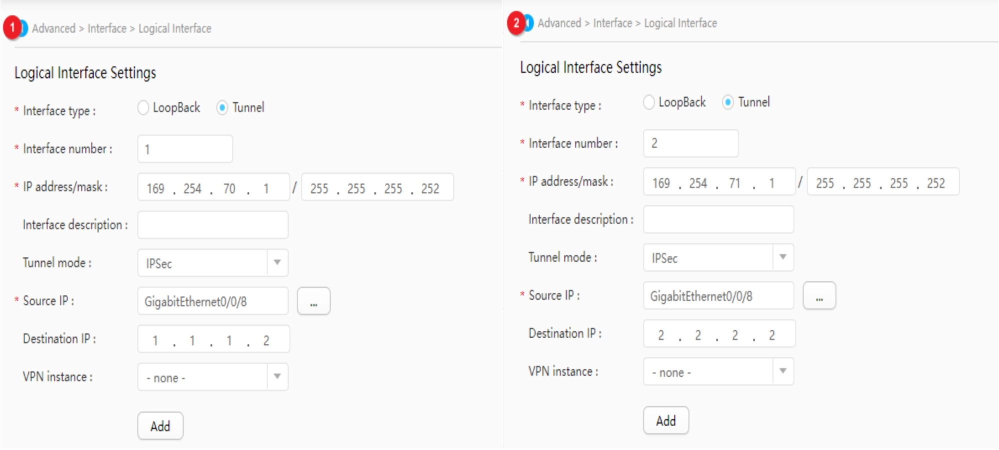
* Destination IP : 2 . 2 . 2 . 2
* Subnet mask : 255 . 255 . 255 . 252
VPN instance : - none -
Next hop address : 1 . 1 . 1 . 254
Public network gateway address of the AR router, which is subject to the actual value.
Outbound interface : GigabitEthernet0/0/8
Priority : 60
Description :

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



1 Advanced > Interface > Logical Interface

Logical Interface Settings

* Interface type : ○ LoopBack ● Tunnel

* Interface number : 1

* IP address/mask : 169 . 254 . 70 . 1 / 255 . 255 . 255 . 252

Interface description :

Tunnel mode : IPSec

* Source IP : GigabitEthernet0/0/8

Destination IP : 1 . 1 . 1 . 2

VPN instance : - none -

2 Advanced > Interface > Logical Interface

Logical Interface Settings

* Interface type : ○ LoopBack ● Tunnel

* Interface number : 2

* IP address/mask : 169 . 254 . 71 . 1 / 255 . 255 . 255 . 252

Interface description :

Tunnel mode : IPSec

* Source IP : GigabitEthernet0/0/8

Destination IP : 2 . 2 . 2 . 2

VPN instance : - none -

Step 4 Configure VPN connections.

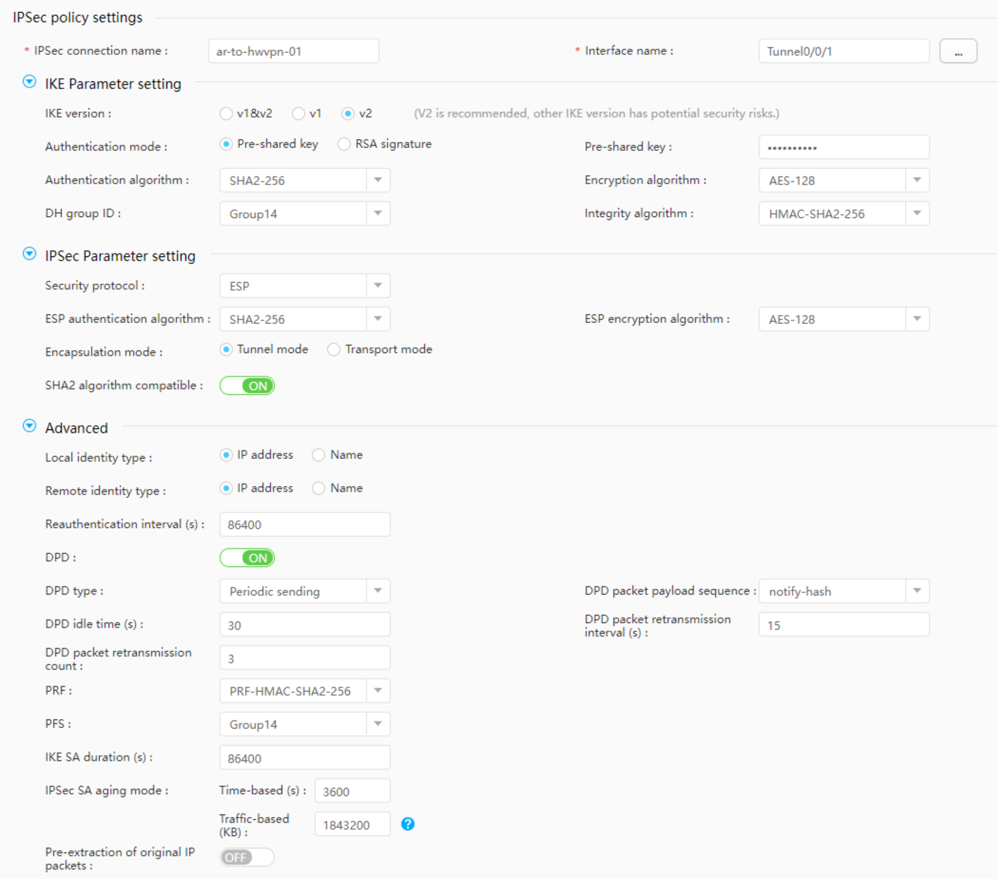
1. Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**.
2. Configure the IKE and IPsec policies for the two tunnels, as shown in **Figure 1-7** and **Figure 1-8**.

   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



IPSec policy settings

* IPSec connection name : ar-to-hwvpn-01

* Interface name : Tunnel0/0/1

IKE Parameter setting

IKE version : ○ v1&v2 ○ v1 ● v2 (V2 is recommended, other IKE version has potential security risks.)

Authentication mode : ● Pre-shared key ○ RSA signature

Pre-shared key : ••••••••••

Authentication algorithm : SHA2-256

Encryption algorithm : AES-128

DH group ID : Group14

Integrity algorithm : HMAC-SHA2-256

IPSec Parameter setting

Security protocol : ESP

ESP authentication algorithm : SHA2-256

ESP encryption algorithm : AES-128

Encapsulation mode : ● Tunnel mode ○ Transport mode

SHA2 algorithm compatible : ON

Advanced

Local identity type : ● IP address ○ Name

Remote identity type : ● IP address ○ Name

Reauthentication interval (s) : 86400

DPD : ON

DPD type : Periodic sending

DPD packet payload sequence : notify-hash

DPD idle time (s) : 30

DPD packet retransmission interval (s) : 15

DPD packet retransmission count : 3

PRF : PRF-HMAC-SHA2-256

PFS : Group14

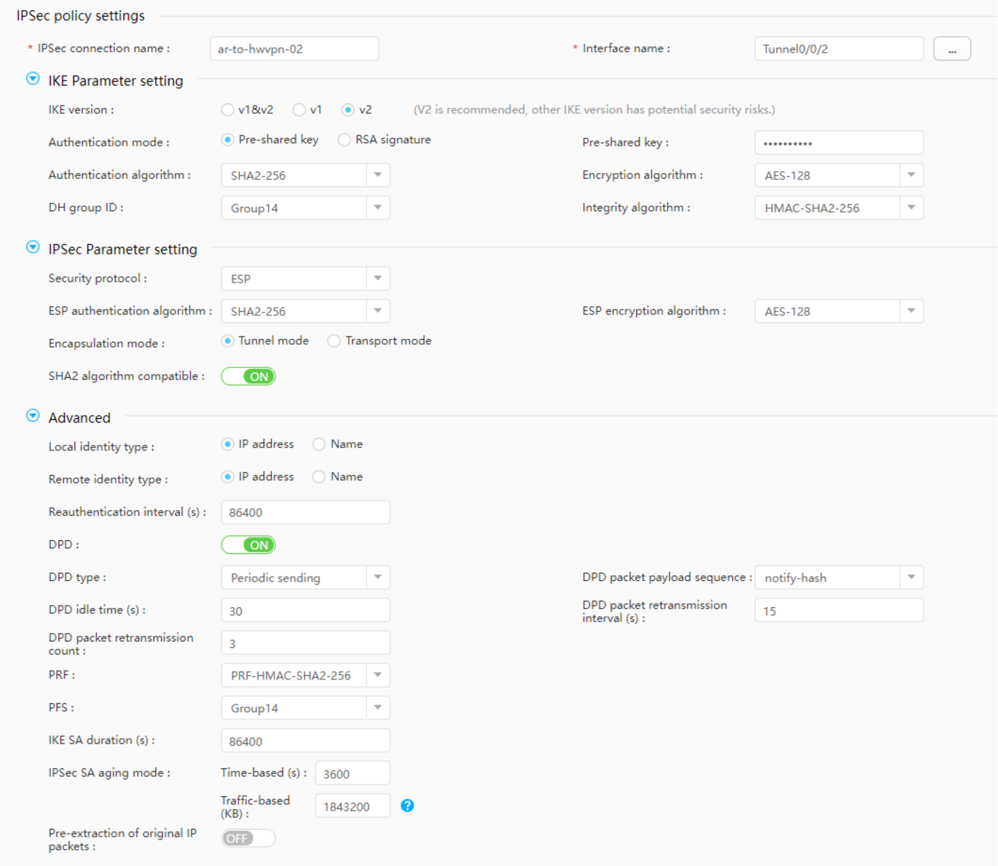
IKE SA duration (s) : 86400

IPSec SA aging mode : Time-based (s) : 3600

Traffic-based (KB) : 1843200

Pre-extraction of original IP packets : OFF

Figure 1-8 Configuring VPN connection 2



IPSec policy settings

* IPSec connection name : ar-to-hwvpn-02
* Interface name : Tunnel0/0/2 ...

IKE Parameter setting

IKE version : ○ v1&v2 ○ v1 ● v2 (V2 is recommended, other IKE version has potential security risks.)
Authentication mode : ● Pre-shared key ○ RSA signature
Pre-shared key : ••••••••••
Authentication algorithm : SHA2-256
Encryption algorithm : AES-128
DH group ID : Group14
Integrity algorithm : HMAC-SHA2-256

IPSec Parameter setting

Security protocol : ESP
ESP authentication algorithm : SHA2-256
ESP encryption algorithm : AES-128
Encapsulation mode : ● Tunnel mode ○ Transport mode
SHA2 algorithm compatible : ON

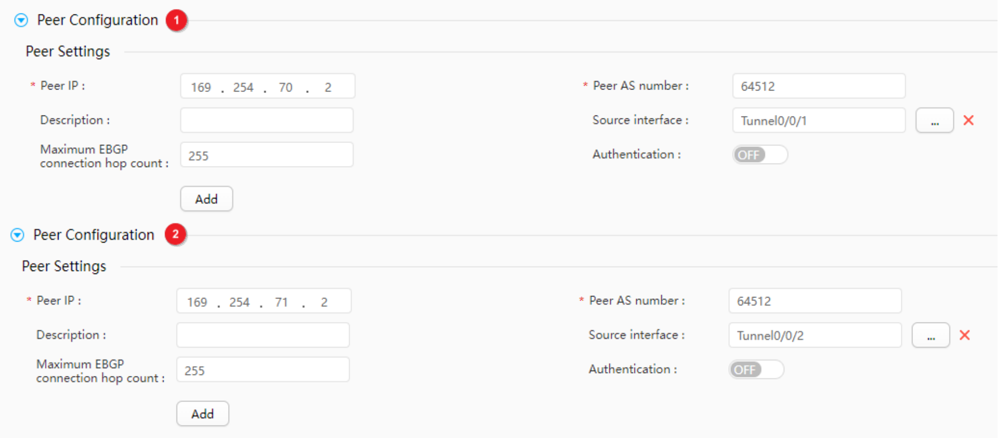
Advanced

Local identity type : ● IP address ○ Name
Remote identity type : ● IP address ○ Name
Reauthentication interval (s) : 86400
DPD : ON
DPD type : Periodic sending
DPD packet payload sequence : notify-hash
DPD idle time (s) : 30
DPD packet retransmission interval (s) : 15
DPD packet retransmission count : 3
PRF : PRF-HMAC-SHA2-256
PFS : Group14
IKE SA duration (s) : 86400
IPSec SA aging mode : Time-based (s) : 3600
Traffic-based (KB) : 1843200
Pre-extraction of original IP packets : OFF

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



Peer Configuration 1

Peer Settings

* Peer IP : 169 . 254 . 70 . 2
* Peer AS number : 64512
Description :
Source interface : Tunnel0/0/1 ... ✕
Maximum EBGP connection hop count : 255
Authentication : OFF
Add

Peer Configuration 2

Peer Settings

* Peer IP : 169 . 254 . 71 . 2
* Peer AS number : 64512
Description :
Source interface : Tunnel0/0/2 ... ✕
Maximum EBGP connection hop count : 255
Authentication : OFF
Add

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.

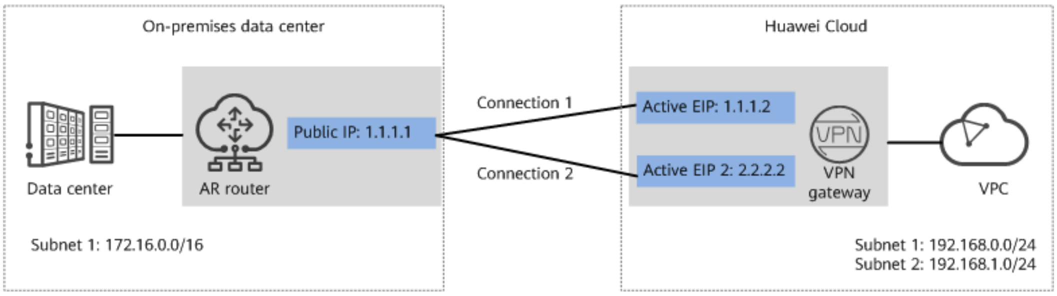
1.1.3 Policy-based Mode

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

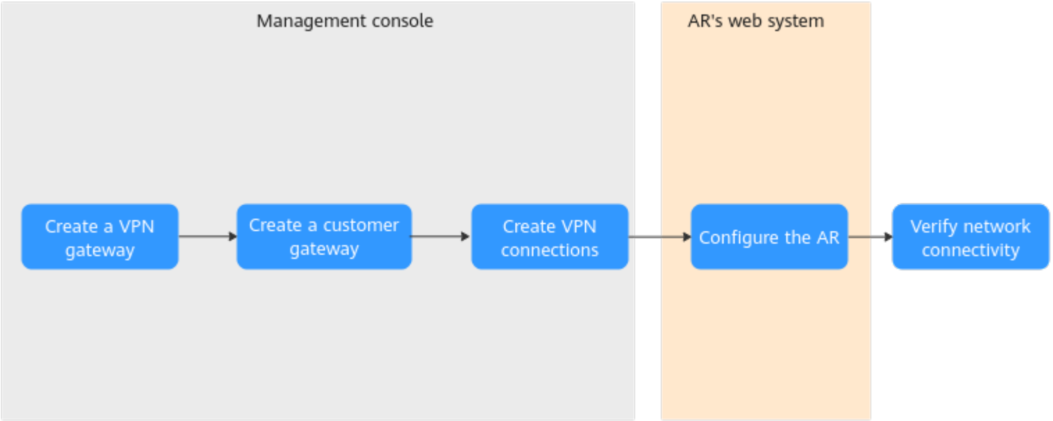


Table 1-12 Operation process description

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.	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.

   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
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

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 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Connection 1's Configuration	Configure the 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.*
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.

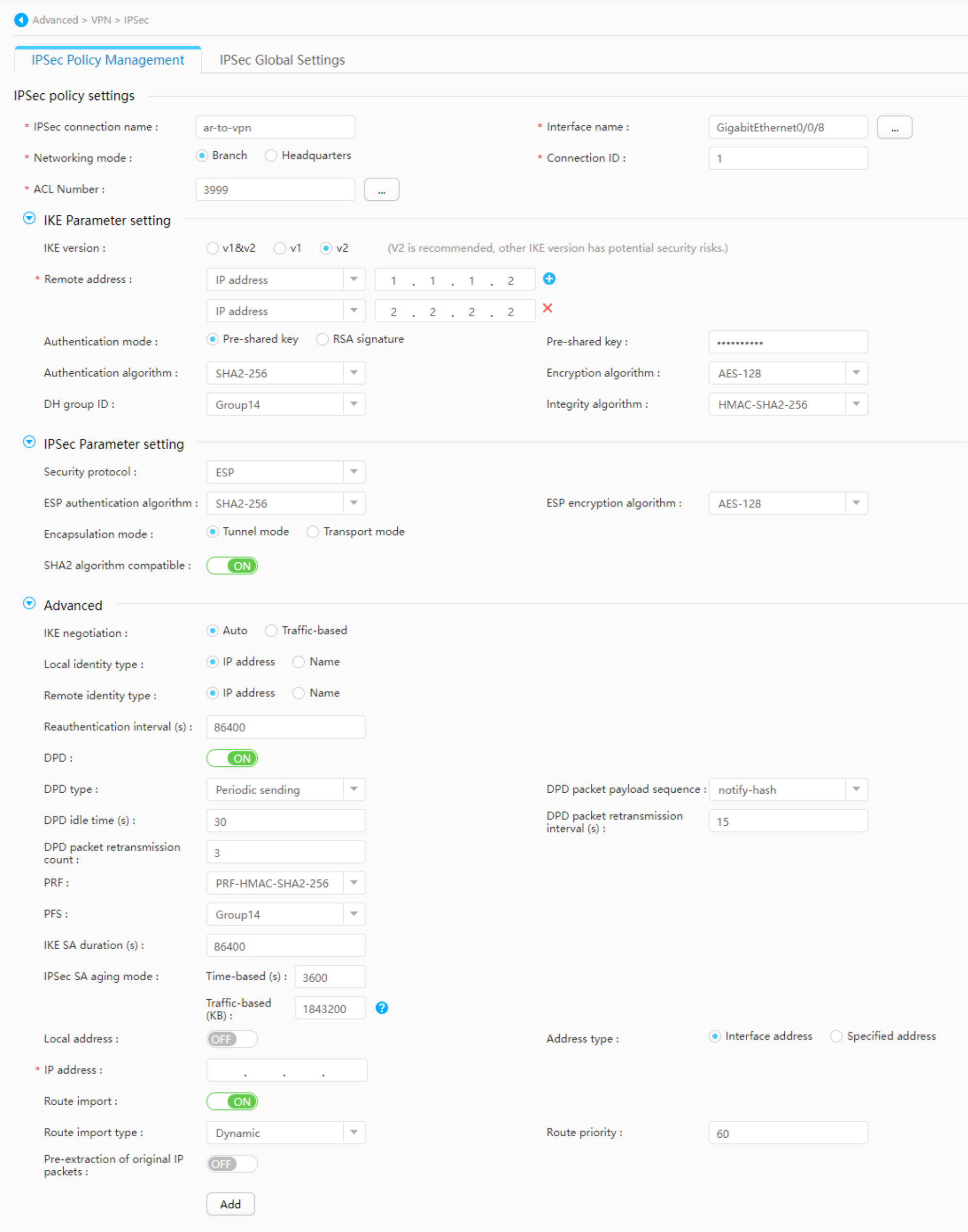
1. Choose **Advanced** > **VPN** > **IPSec** > **IPSec Policy Management**.
2. Configure the IKE and IPsec policies, as shown in **Figure 1-12**.

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.

Figure 1-12 Configuring VPN connections



Advanced > VPN > IPSec

IPSec Policy Management | IPSec Global Settings

IPSec policy settings

- * IPSec connection name : ar-to-vpn
- * Interface name : GigabitEthernet0/0/8 ...
- * Networking mode : ● Branch ○ Headquarters
- * Connection ID : 1
- * ACL Number : 3999 ...

IKE Parameter setting

- IKE version : ○ v1&v2 ○ v1 ● v2 (V2 is recommended, other IKE version has potential security risks.)
- * Remote address : IP address 1 . 1 . 1 . 2
- IP address 2 . 2 . 2 . 2
- Authentication mode : ● Pre-shared key ○ RSA signature
- Pre-shared key : ••••••••••
- Authentication algorithm : SHA2-256
- Encryption algorithm : AES-128
- DH group ID : Group14
- Integrity algorithm : HMAC-SHA2-256

IPSec Parameter setting

- Security protocol : ESP
- ESP authentication algorithm : SHA2-256
- ESP encryption algorithm : AES-128
- Encapsulation mode : ● Tunnel mode ○ Transport mode
- SHA2 algorithm compatible : ON

Advanced

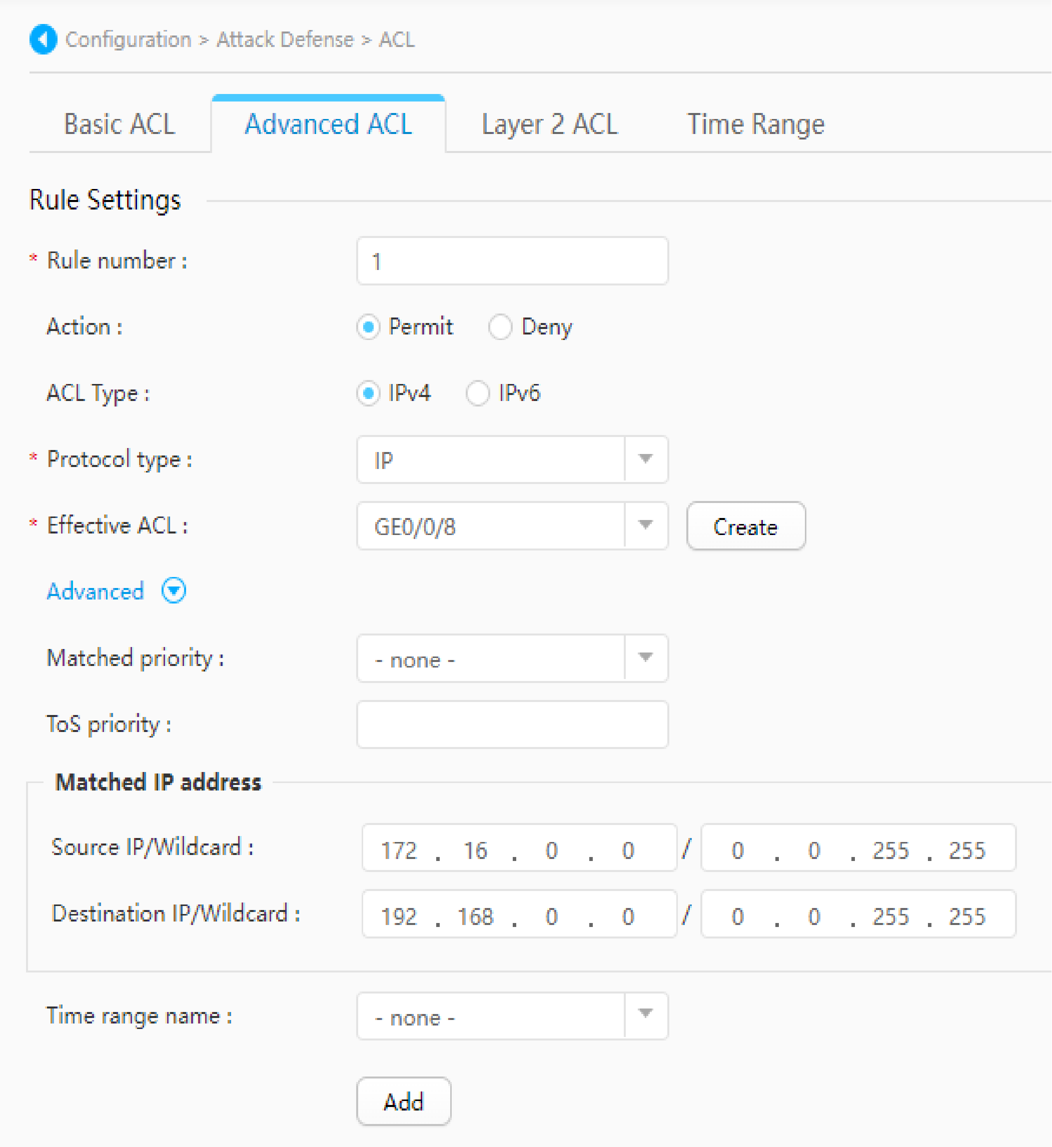
- IKE negotiation : ● Auto ○ Traffic-based
- Local identity type : ● IP address ○ Name
- Remote identity type : ● IP address ○ Name
- Reauthentication interval (s) : 86400
- DPD : ON
- DPD type : Periodic sending
- DPD packet payload sequence : notify-hash
- DPD idle time (s) : 30
- DPD packet retransmission interval (s) : 15
- DPD packet retransmission count : 3
- PRF : PRF-HMAC-SHA2-256
- PFS : Group14
- IKE SA duration (s) : 86400
- IPSec SA aging mode : Time-based (s) : 3600
- Traffic-based (KB) : 1843200
- Local address : OFF
- Address type : ● Interface address ○ Specified address
- * IP address : . . .
- Route import : ON
- Route import type : Dynamic
- Route priority : 60
- Pre-extraction of original IP packets : OFF

Add

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



Rule Settings

* Rule number : 1

Action : ● Permit ○ Deny

ACL Type : ● IPv4 ○ IPv6

* Protocol type : IP

* Effective ACL : GE0/0/8

Matched priority : - none -

ToS priority :

Matched IP address

Source IP/Wildcard : 172 . 16 . 0 . 0 / 0 . 0 . 255 . 255

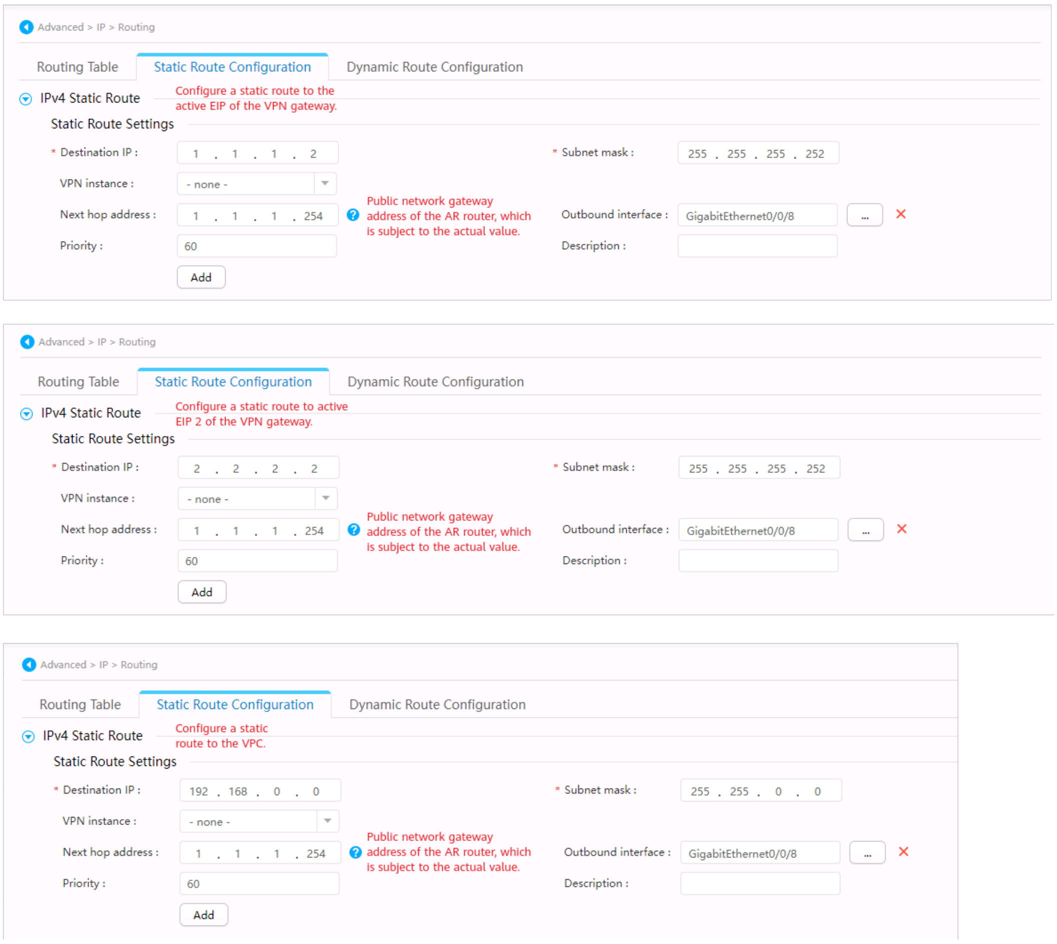
Destination IP/Wildcard : 192 . 168 . 0 . 0 / 0 . 0 . 255 . 255

Time range name : - none -

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



Configure a static route to the active EIP of the VPN gateway.

Static Route Settings

* Destination IP : 1 . 1 . 1 . 2
* Subnet mask : 255 . 255 . 255 . 252
VPN instance : - none -
Next hop address : 1 . 1 . 1 . 254
Public network gateway address of the AR router, which is subject to the actual value.
Outbound interface : GigabitEthernet0/0/8
Priority : 60
Description :

Configure a static route to active EIP 2 of the VPN gateway.

Static Route Settings

* Destination IP : 2 . 2 . 2 . 2
* Subnet mask : 255 . 255 . 255 . 252
VPN instance : - none -
Next hop address : 1 . 1 . 1 . 254
Public network gateway address of the AR router, which is subject to the actual value.
Outbound interface : GigabitEthernet0/0/8
Priority : 60
Description :

Configure a static route to the VPC.

Static Route Settings

* Destination IP : 192 . 168 . 0 . 0
* Subnet mask : 255 . 255 . 0 . 0
VPN instance : - none -
Next hop address : 1 . 1 . 1 . 254
Public network gateway address of the AR router, which is subject to the actual value.
Outbound interface : GigabitEthernet0/0/8
Priority : 60
Description :

----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)

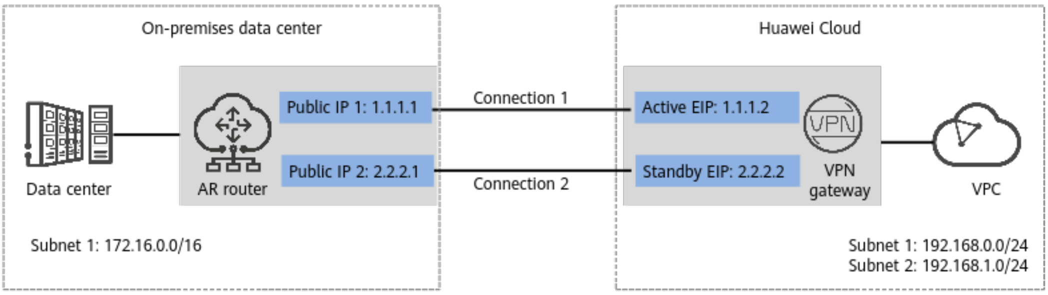
1.2.1 Static Routing Mode

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

Category	Item	Example Value for the AR Router	Example Value for the Huawei Cloud Side
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
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	● Local tunnel interface address: 169.254.70.2/30 ● Customer tunnel interface address: 169.254.70.1/30	
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30	
	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

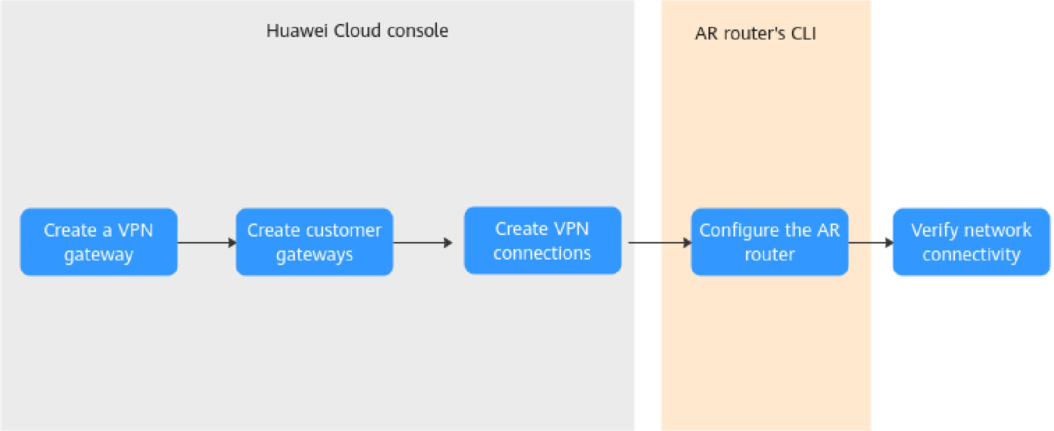


Table 1-17 Operation process description

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	Select **Active/Standby**.	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 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
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	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.	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, 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.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
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.	169.254.71.2/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----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 169.254.70.1 255.255.255.252
[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 169.254.71.1 255.255.255.252
[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 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit
```

The commands are described as follows:

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

  In this example, the test instance **IPsec_nqa1** is created for the VPN connection to which the active EIP of the VPN gateway belongs; the test instance **IPsec_nqa2** is created for the VPN connection to which 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 a Huawei USG Firewall

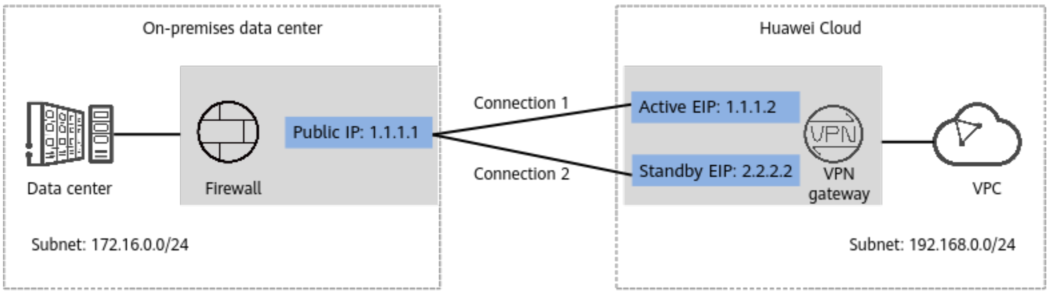
1.3.1 Static Routing Mode

1.3.1.1 Operation Guide

Scenario

Figure 1-17 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 1-17 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 1-22 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
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	● Local tunnel interface address: 169.254.70.2/30 ● Customer tunnel interface address: 169.254.70.1/30	
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30	
	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	

Category	Item	Example Value for the Huawei USG Firewall	Example Value for the Huawei Cloud Side
	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	

1.3.1.2 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**.

   Table 1-23 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

Parameter	Description	Value
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
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 1-24 only describes the key parameters for creating 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-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 1-25 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-25 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 **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 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/24

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, 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.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
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.	169.254.71.2/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----End

1.3.1.3 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 1-25.
   encryption-algorithm AES-128         # Set the same encryption algorithm as that configured in the IKE policy in Table 1-25.
   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 1-25.
   sa duration 86400                     # Set the same lifetime as that configured in the IKE policy in Table 1-25.

   ike peer hwcloud_peer33
   undo version 1                       # Set the same IKE version as that configured in the IKE policy in Table 1-25.
   pre-shared-key XXXXXXX               # Set the same PSK as that configured in Table 1-25.
   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 1-25.
esp encryption-algorithm aes-128    # Set the same encryption algorithm as that configured in the
IPsec policy in Table 1-25.

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 1-25.
sa duration time-based 3600       # Set the same lifetime as that configured in the IPsec policy in
Table 1-25.

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

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
```

1.3.1.4 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**.
  - 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.

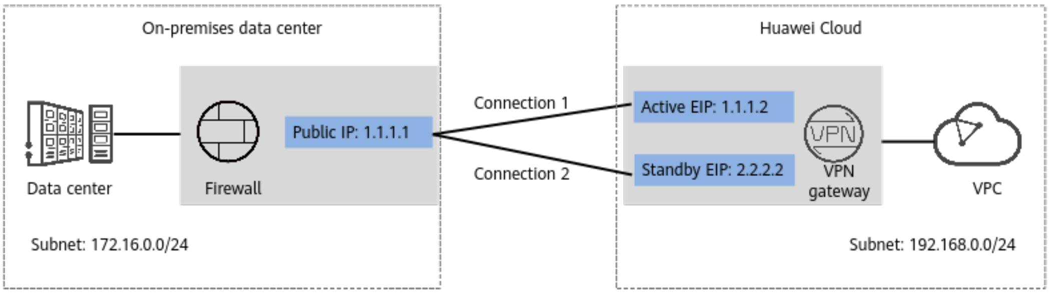
1.3.2 BGP Routing Mode

1.3.2.1 Operation Guide

Scenario

Figure 1-18 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 1-18 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 1-26 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
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	- Local tunnel interface address: 169.254.70.2/30 - Customer tunnel interface address: 169.254.70.1/30	

Category	Item	Example Value for the Firewall	Example Value for the Huawei Cloud Side
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30	
	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	

1.3.2.2 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 1-27 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-27 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
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 1-28 only describes the key parameters for creating a customer gateway. For other parameters, use their default settings.

Table 1-28 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
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 1-29 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-29 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

Parameter	Description	Value
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 and 214.0.0.0/8 cannot be used as customer subnets.	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.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
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.	169.254.71.2/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----End

1.3.2.3 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 1-25.
   encryption-algorithm AES-128         # Set the same encryption algorithm as that configured in the
   IKE policy in Table 1-25.
   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 1-25.
   sa duration 86400                    # Set the same lifetime as that configured in the IKE policy in Table
   1-25.

   ike peer hwcloud_peer33
   undo version 1                      # Set the same IKE version as that configured in the IKE policy in
   Table 1-25.
   pre-shared-key Test@123              # Set the same PSK as that configured in Table 1-25.
   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 1-25.
   esp encryption-algorithm aes-128     # Set the same encryption algorithm as that configured in the
   IPsec policy in Table 1-25.
   ```

```
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 1-25.
sa duration time-based 3600       # Set the same lifetime as that configured in the IPsec policy in
Table 1-25.

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

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
```

1.3.2.4 Verification

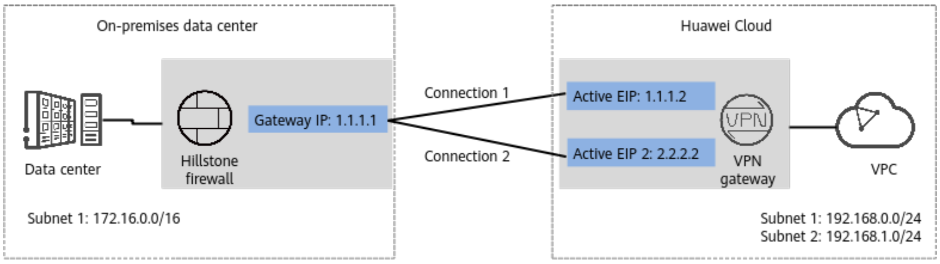
1.4 Interconnection with a Hillstone Firewall

1.4.1 Static Routing Mode

1.4.1.1 Scenario

Figure 1-19 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 1-19 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.

1.4.1.2 Data Plan

Table 1-30 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
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	● Local tunnel interface address: 169.254.70.2/30 ● Customer tunnel interface address: 169.254.70.1/30	

Category	Item	Example Value for the Hillstone Firewall	Example Value for the Huawei Cloud Side
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30	
	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	

1.4.1.3 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 1-31 only describes the key parameters for creating a VPN gateway. For other parameters, use their default settings.

Table 1-31 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.	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 1-32 describes the parameters for creating a customer gateway.

Table 1-32 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 1-33 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
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 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/24

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, 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.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
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: 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.	169.254.71.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----End

1.4.1.4 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.

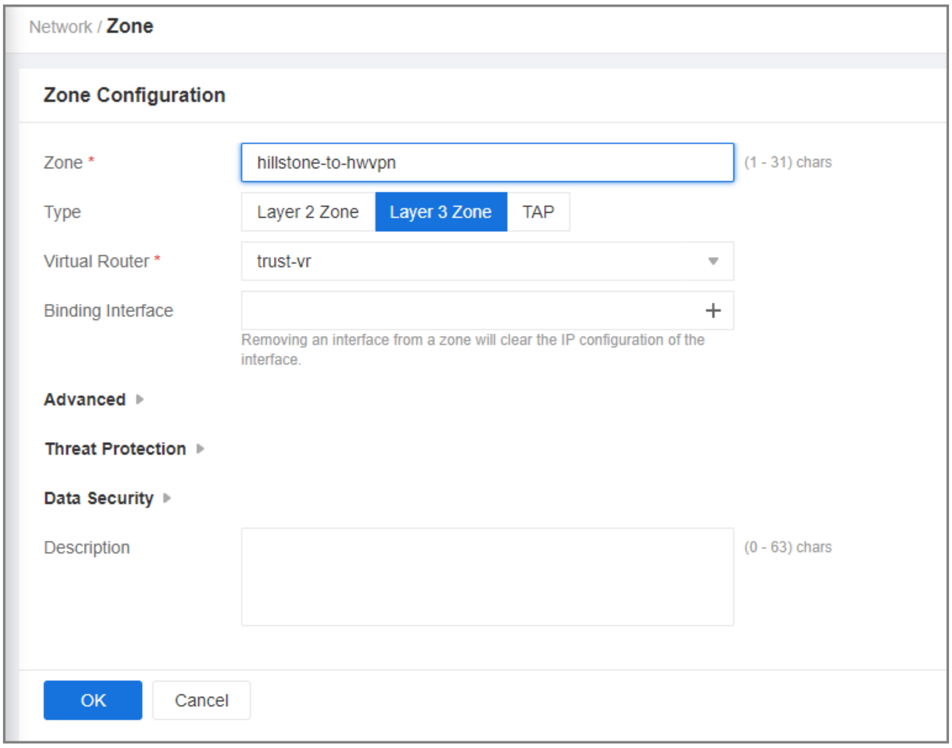
   A firewall running the 5.5R9 version is used as an example. The configuration pages may vary according to the firewall models and software versions.

2. Complete basic settings.

   a. Configure a security zone.

      Choose **Network** > **Zone**. Click **New** and set parameters, as shown in **Figure 1-20**.

Figure 1-20 Configuring a security zone



Network / Zone

Zone Configuration

Zone *: hillstone-to-hwvpn (1 - 31) chars

Type: Layer 2 Zone | **Layer 3 Zone** | TAP

Virtual Router *: trust-vr

Binding Interface:

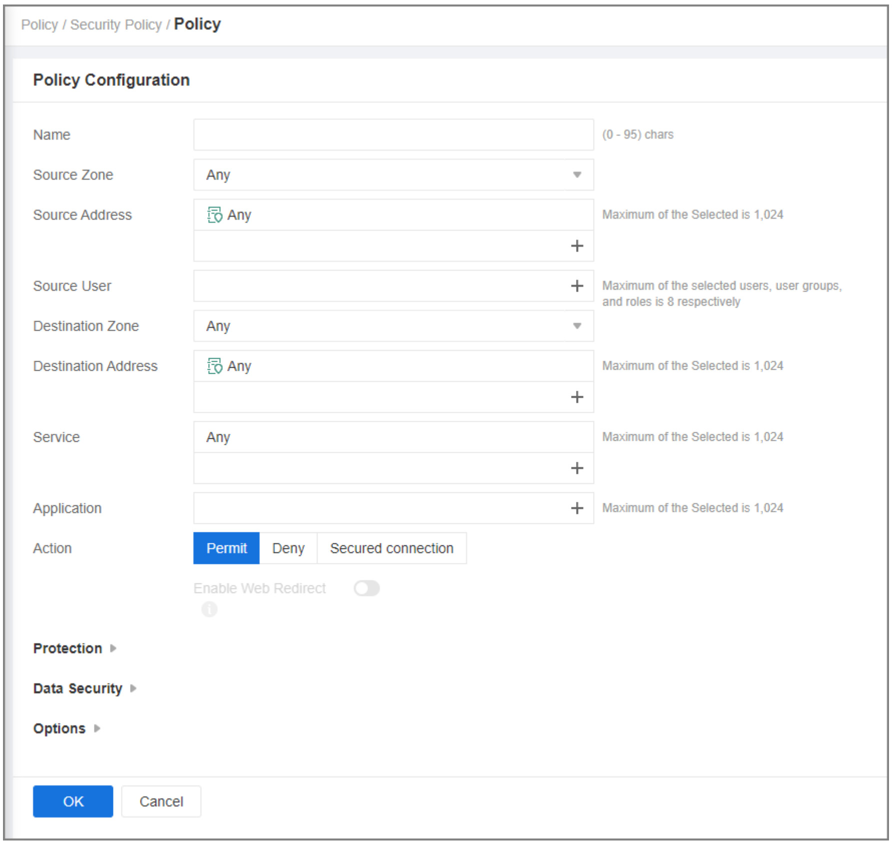
Removing an interface from a zone will clear the IP configuration of the interface.

Description: (0 - 63) chars

b. Configure a security policy.

Choose **Policy** > **Security Policy** > **Policy**. Click **New**, choose **Policy**, and set parameters, as shown in **Figure 1-21**.

Figure 1-21 Configuring a policy



Policy / Security Policy / **Policy**

Policy Configuration

Name: (0 - 95) chars

Source Zone: Any

Source Address: Any — Maximum of the Selected is 1,024

Source User: Maximum of the selected users, user groups, and roles is 8 respectively

Destination Zone: Any

Destination Address: Any — Maximum of the Selected is 1,024

Service: Any — Maximum of the Selected is 1,024

Application: Maximum of the Selected is 1,024

Action: Permit | Deny | Secured connection

Enable Web Redirect

Protection

Data Security

Options

OK | Cancel

c. Configure a basic route.

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

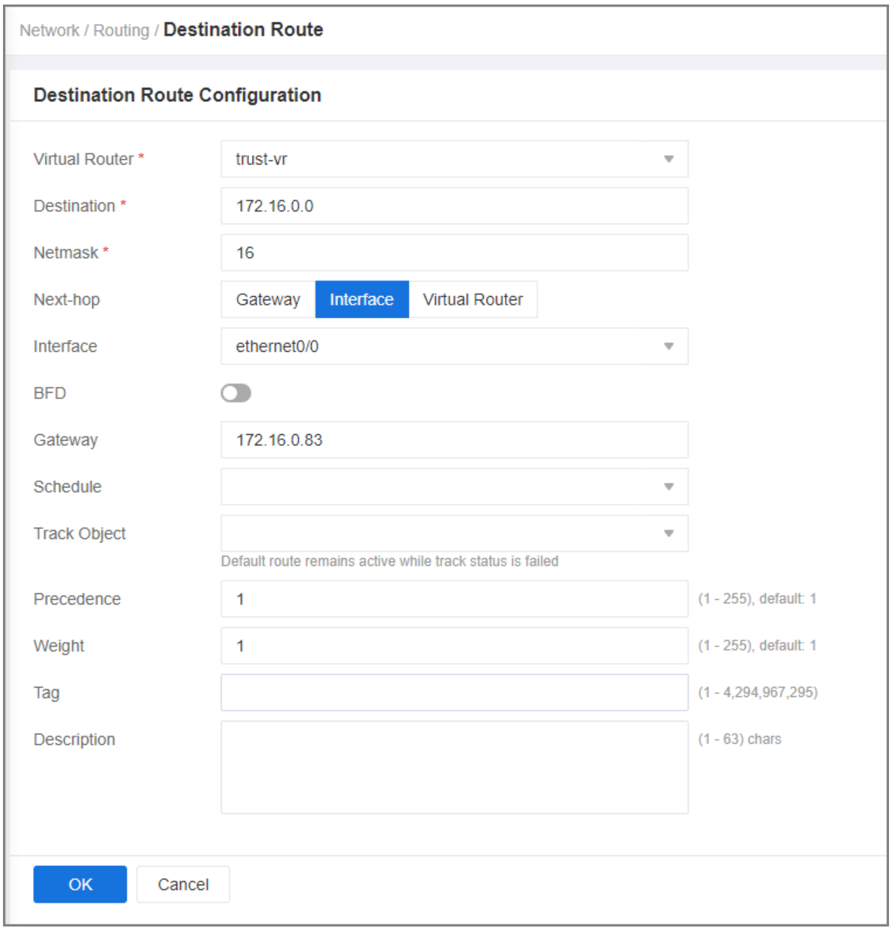
ii. In **Destination Route**, add a static route to the VPC of the Hillstone firewall.

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 1-22 shows the key parameter settings.

Figure 1-22 Configuring a destination route



Network / Routing / **Destination Route**

Destination Route Configuration

Virtual Router *	trust-vr	
Destination *	172.16.0.0	
Netmask *	16	
Next-hop	Gateway / **Interface** / Virtual Router	
Interface	ethernet0/0	
BFD	○	
Gateway	172.16.0.83	
Schedule		
Track Object	 Default route remains active while track status is failed	
Precedence	1	(1 - 255), default: 1
Weight	1	(1 - 255), default: 1
Tag		(1 - 4,294,967,295)
Description		(1 - 63) chars

v. Click **OK**.

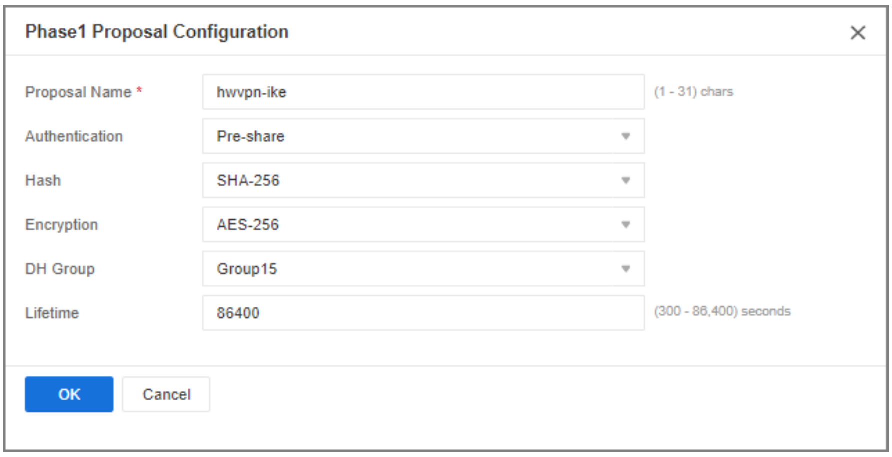
3. Configure VPN connections.

   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 1-23** shows the key parameter settings.

Figure 1-23 Configuring a phase-1 proposal



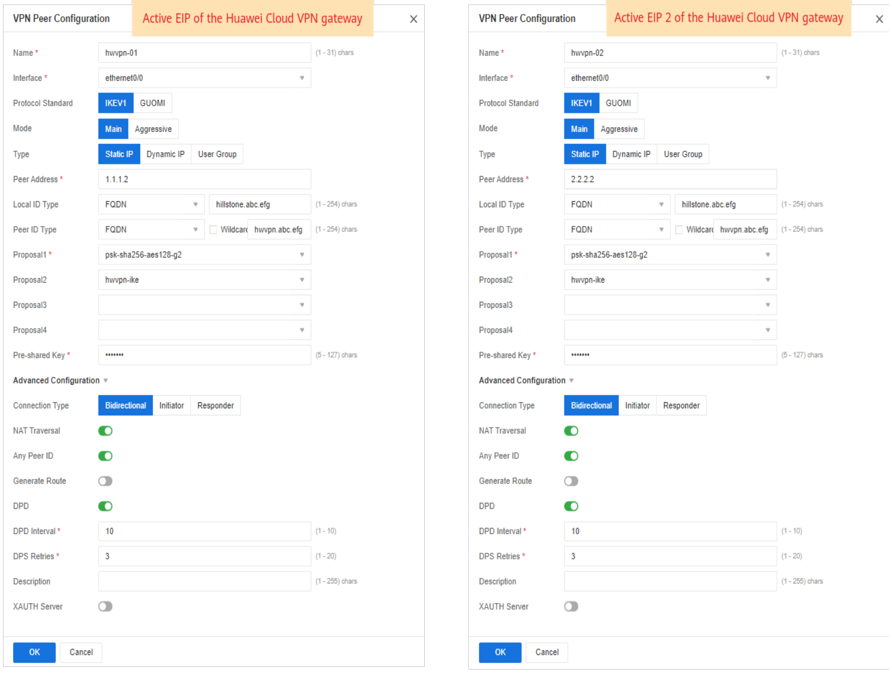
Phase1 Proposal Configuration

Proposal Name *	hwvpn-ike	(1 - 31) chars
Authentication	Pre-share	
Hash	SHA-256	
Encryption	AES-256	
DH Group	Group15	
Lifetime	86400	(300 - 86,400) seconds

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 1-24 Configuring VPN peers



VPN Peer Configuration — Active EIP of the Huawei Cloud VPN gateway

Name *	hwvpn-01	(1 - 31) chars
Interface *	ethernet0/0	
Protocol Standard	IKEV1	
Mode	Main	
Type	Static IP	
Peer Address *	1.1.1.2	
Local ID Type	FQDN hillstone.abc.efg	(1 - 254) chars
Peer ID Type	FQDN □ Wildcard hwvpn.abc.efg	(1 - 254) chars
Proposal1 *	psk-sha256-aes128-g2	
Proposal2	hwvpn-ike	
Proposal3		
Proposal4		
Pre-shared Key *	•••••••	(5 - 127) chars
Advanced Configuration		
Connection Type	Bidirectional	
NAT Traversal	●	
Any Peer ID	●	
Generate Route	○	
DPD	●	
DPD Interval *	10	(1 - 10)
DPS Retries *	3	(1 - 20)
Description		(1 - 255) chars
XAUTH Server	○	

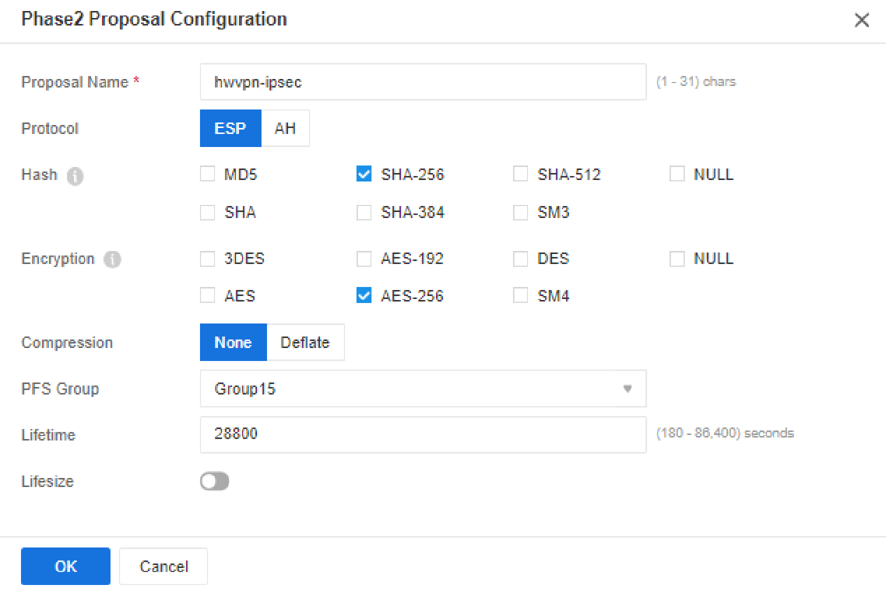
VPN Peer Configuration — Active EIP 2 of the Huawei Cloud VPN gateway

Name *	hwvpn-02	(1 - 31) chars
Interface *	ethernet0/0	
Protocol Standard	IKEV1	
Mode	Main	
Type	Static IP	
Peer Address *	2.2.2.2	
Local ID Type	FQDN hillstone.abc.efg	(1 - 254) chars
Peer ID Type	FQDN □ Wildcard hwvpn.abc.efg	(1 - 254) chars
Proposal1 *	psk-sha256-aes128-g2	
Proposal2	hwvpn-ike	
Proposal3		
Proposal4		
Pre-shared Key *	•••••••	(5 - 127) chars
Advanced Configuration		
Connection Type	Bidirectional	
NAT Traversal	●	
Any Peer ID	●	
Generate Route	○	
DPD	●	
DPD Interval *	10	(1 - 10)
DPS Retries *	3	(1 - 20)
Description		(1 - 255) chars
XAUTH Server	○	

IKEV1 GUOMI
Main Aggressive
Static IP Dynamic IP User Group
Bidirectional Initiator Responder
OK
Cancel

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 1-25 shows the key parameter settings.

Figure 1-25 Configuring a phase-2 proposal



Phase2 Proposal Configuration

Proposal Name *: hwvpn-ipsec (1 - 31) chars

Protocol: ESP | AH

Hash: ☐ MD5 ☑ SHA-256 ☐ SHA-512 ☐ NULL ☐ SHA ☐ SHA-384 ☐ SM3

Encryption: ☐ 3DES ☐ AES-192 ☐ DES ☐ NULL ☐ AES ☑ AES-256 ☐ SM4

Compression: None | Deflate

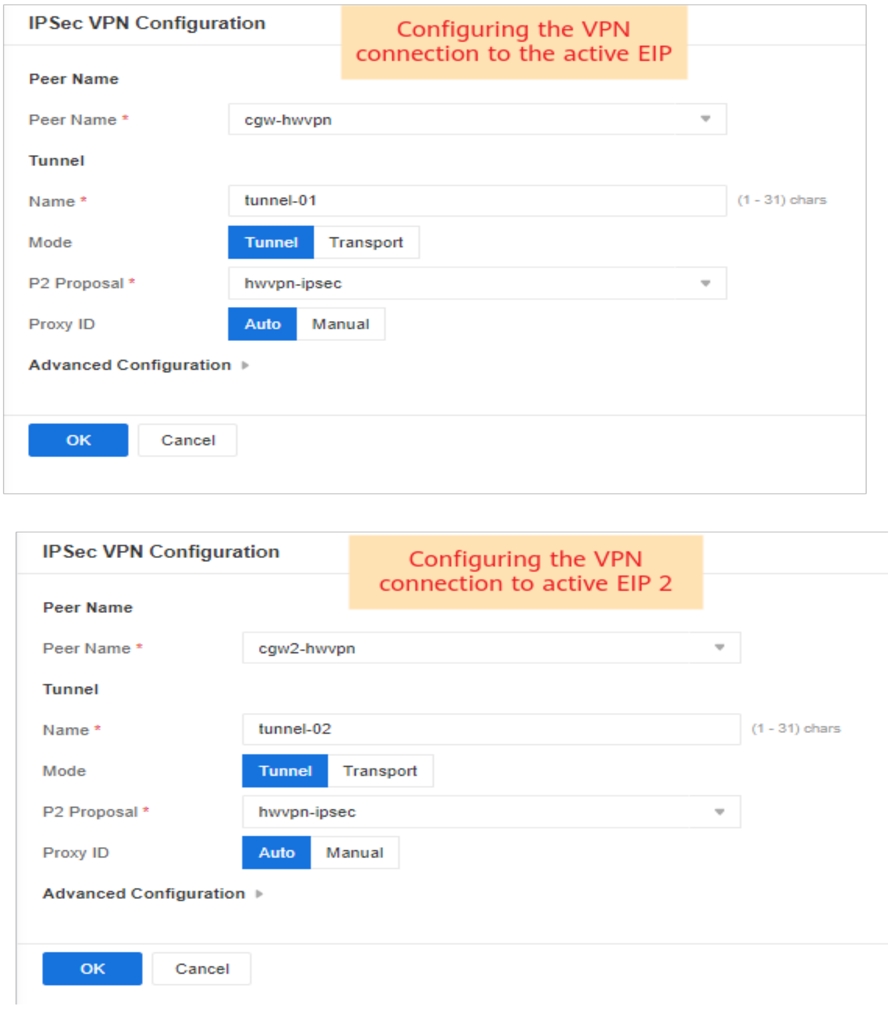
PFS Group: Group15

Lifetime: 28800 (180 - 86,400) seconds

Lifesize

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 1-26 Configuring IPsec VPN



IPSec VPN Configuration

Configuring the VPN connection to the active EIP

Peer Name

Peer Name *: cgw-hwvpn

Tunnel

Name *: tunnel-01 (1 - 31) chars

Mode: Tunnel | Transport

P2 Proposal *: hwvpn-ipsec

Proxy ID: Auto | Manual

Advanced Configuration

OK | Cancel

IPSec VPN Configuration

Configuring the VPN connection to active EIP 2

Peer Name

Peer Name *: cgw2-hwvpn

Tunnel

Name *: tunnel-02 (1 - 31) chars

Mode: Tunnel | Transport

P2 Proposal *: hwvpn-ipsec

Proxy ID: Auto | Manual

Advanced Configuration

OK | Cancel

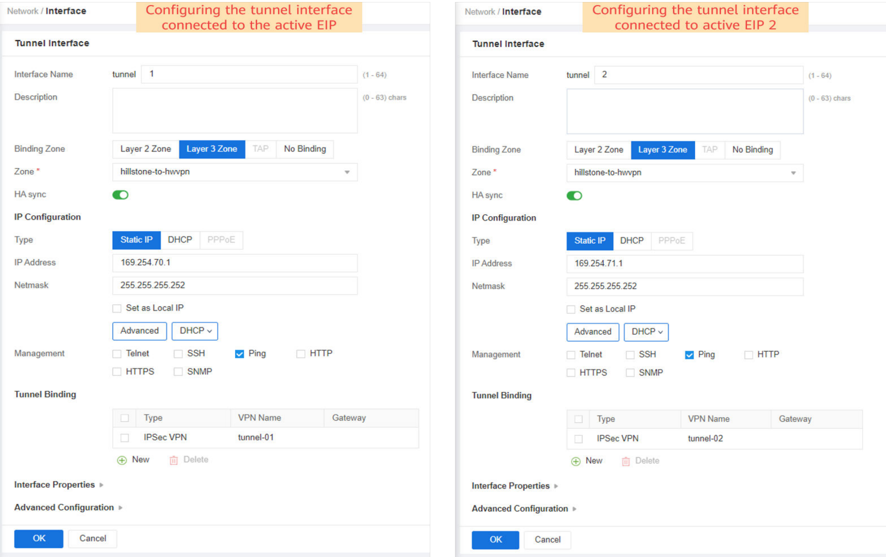
4. Configure tunnel interfaces.

   a. Choose **Network** > **Interface**, click **New**, and choose **Tunnel Interface**.

   b. Configure two tunnel interfaces. **Figure 1-27** 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 1-27 Configuring tunnel interfaces



Configuring the tunnel interface connected to the active EIP

Network / **Interface**

Tunnel Interface

Interface Name: tunnel 1 (1 - 64)
Description: (0 - 63) chars
Binding Zone: Layer 2 Zone | **Layer 3 Zone** | TAP | No Binding
Zone *: hillstone-to-hwvpn
HA sync: ●

IP Configuration
Type: **Static IP** | DHCP | PPPoE
IP Address: 169.254.70.1
Netmask: 255.255.255.252
□ Set as Local IP
Advanced | DHCP ⌄
Management: □ Telnet □ SSH ☑ Ping □ HTTP □ HTTPS □ SNMP

Tunnel Binding

□	Type	VPN Name	Gateway
□	IPSec VPN	tunnel-01	

⊕ New Delete

Interface Properties ▸
Advanced Configuration ▸
OK | Cancel

Configuring the tunnel interface connected to active EIP 2

Network / **Interface**

Tunnel Interface

Interface Name: tunnel 2 (1 - 64)
Description: (0 - 63) chars
Binding Zone: Layer 2 Zone | **Layer 3 Zone** | TAP | No Binding
Zone *: hillstone-to-hwvpn
HA sync: ●

IP Configuration
Type: **Static IP** | DHCP | PPPoE
IP Address: 169.254.71.1
Netmask: 255.255.255.252
□ Set as Local IP
Advanced | DHCP ⌄
Management: □ Telnet □ SSH ☑ Ping □ HTTP □ HTTPS □ SNMP

Tunnel Binding

□	Type	VPN Name	Gateway
□	IPSec VPN	tunnel-02	

⊕ New Delete

Interface Properties ▸
Advanced Configuration ▸
OK | Cancel

5. Configure service routes.

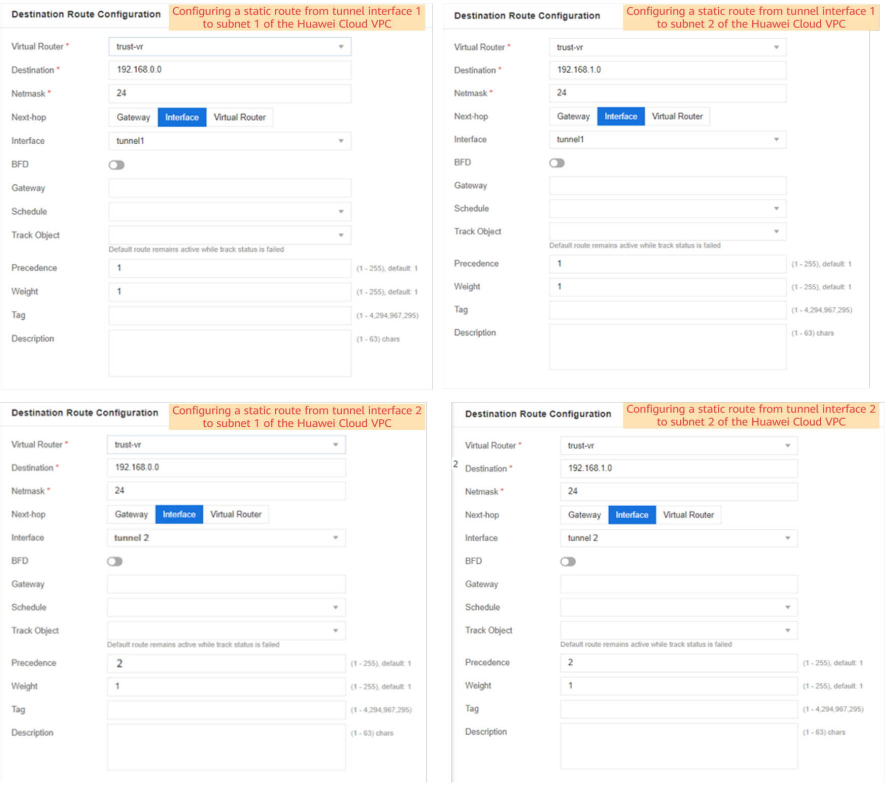
   a. Choose **Network** > **Routing** > **Destination Route**, and click **New**.

   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 1-28**.

      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 1-28 Configuring service routes



Destination Route Configuration — Configuring a static route from tunnel interface 1 to subnet 1 of the Huawei Cloud VPC

Virtual Router *	trust-vr	
Destination *	192.168.0.0	
Netmask *	24	
Next-hop	Gateway / **Interface** / Virtual Router	
Interface	tunnel1	
BFD	○	
Gateway		
Schedule		
Track Object	 Default route remains active while track status is failed	
Precedence	1	(1 - 255), default: 1
Weight	1	(1 - 255), default: 1
Tag		(1 - 4,294,967,295)
Description		(1 - 63) chars

Destination Route Configuration — Configuring a static route from tunnel interface 1 to subnet 2 of the Huawei Cloud VPC

Virtual Router *	trust-vr	
Destination *	192.168.1.0	
Netmask *	24	
Next-hop	Gateway / **Interface** / Virtual Router	
Interface	tunnel1	
BFD	○	
Gateway		
Schedule		
Track Object	 Default route remains active while track status is failed	
Precedence	1	(1 - 255), default: 1
Weight	1	(1 - 255), default: 1
Tag		(1 - 4,294,967,295)
Description		(1 - 63) chars

Destination Route Configuration — Configuring a static route from tunnel interface 2 to subnet 1 of the Huawei Cloud VPC

Virtual Router *	trust-vr	
Destination *	192.168.0.0	
Netmask *	24	
Next-hop	Gateway / **Interface** / Virtual Router	
Interface	tunnel 2	
BFD	○	
Gateway		
Schedule		
Track Object	 Default route remains active while track status is failed	
Precedence	2	(1 - 255), default: 1
Weight	1	(1 - 255), default: 1
Tag		(1 - 4,294,967,295)
Description		(1 - 63) chars

Destination Route Configuration — Configuring a static route from tunnel interface 2 to subnet 2 of the Huawei Cloud VPC

Virtual Router *	trust-vr	
Destination *	192.168.1.0	
Netmask *	24	
Next-hop	Gateway / **Interface** / Virtual Router	
Interface	tunnel 2	
BFD	○	
Gateway		
Schedule		
Track Object	 Default route remains active while track status is failed	
Precedence	2	(1 - 255), default: 1
Weight	1	(1 - 255), default: 1
Tag		(1 - 4,294,967,295)
Description		(1 - 63) chars

1.4.1.5 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

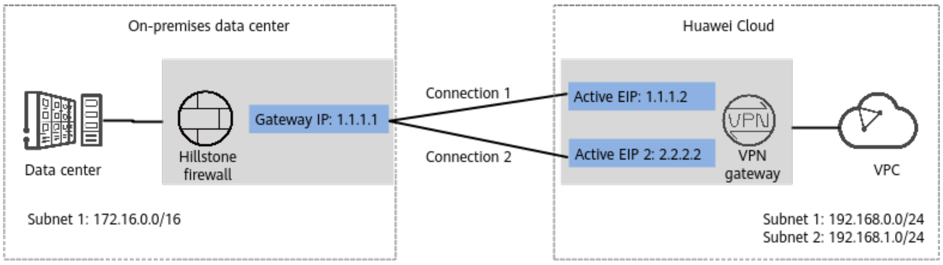
    Choose **Network** > **VPN** > **IPSec VPN**. The states of the two VPN connections are normal.
- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnet can ping each other.

1.4.2 BGP Routing Mode

1.4.2.1 Scenario

Figure 1-29 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 1-29 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.

1.4.2.2 Data Plan

Table 1-34 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: 169.254.70.2/30 ● Customer tunnel interface address: 169.254.70.1/30	

Category	Item	Example Value	Example Value for the Huawei Cloud Side
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30	
	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	

1.4.2.3 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 1-35 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.	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 1-36 Description of 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
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 1-37 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
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 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/24

Parameter	Description	Value
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.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
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.	169.254.71.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----End

1.4.2.4 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.

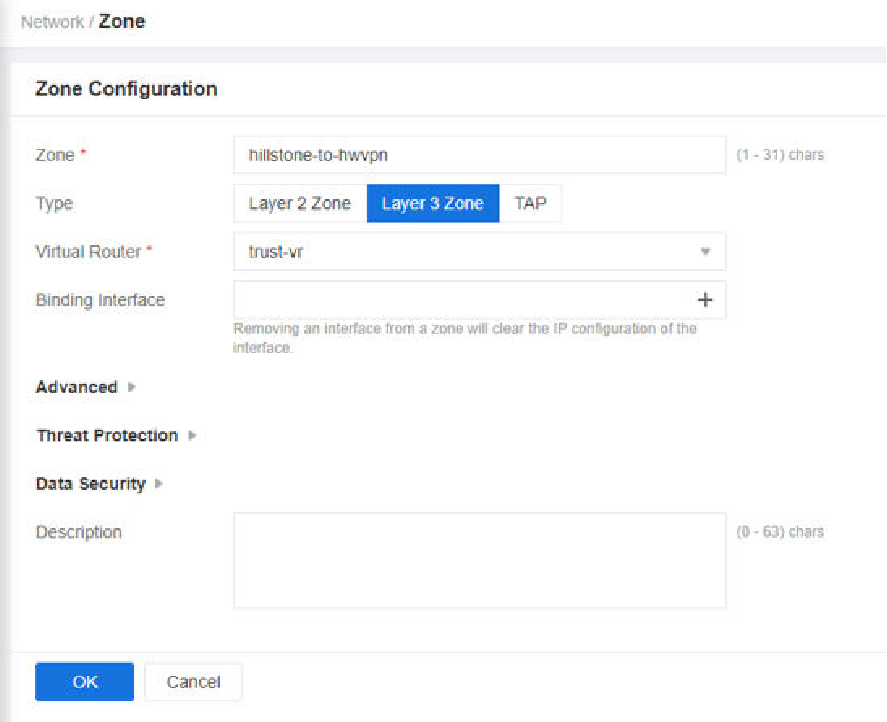
   A firewall running the 5.5R9 version is used as an example. The configuration pages may vary according to the firewall models and software versions.

2. Complete basic settings.

   a. Configure a security zone.

      Choose **Network** > **Zone**. Click **New** and set parameters, as shown in **Figure 1-30**.

Figure 1-30 Configuring a security zone



Network / **Zone**

Zone Configuration

Zone * hillstone-to-hwvpn (1 - 31) chars

Type: Layer 2 Zone | **Layer 3 Zone** | TAP

Virtual Router * trust-vr

Binding Interface +

Removing an interface from a zone will clear the IP configuration of the interface.

Advanced

Threat Protection

Data Security

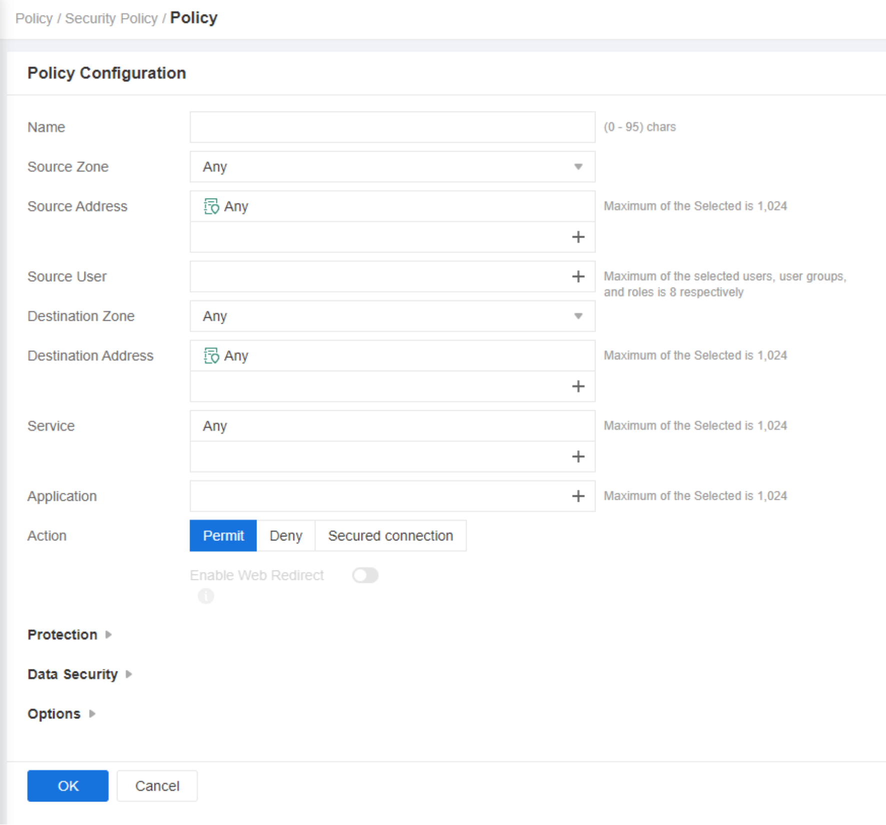
Description (0 - 63) chars

OK Cancel

b. Configure a security policy.

Choose **Policy** > **Security Policy** > **Policy**. Click **New**, choose **Policy**, and set parameters, as shown in **Figure 1-31**.

Figure 1-31 Configuring a policy



Policy / Security Policy / **Policy**

Policy Configuration

Name		(0 - 95) chars
Source Zone	Any	
Source Address	Any	Maximum of the Selected is 1,024
Source User		Maximum of the selected users, user groups, and roles is 8 respectively
Destination Zone	Any	
Destination Address	Any	Maximum of the Selected is 1,024
Service	Any	Maximum of the Selected is 1,024
Application		Maximum of the Selected is 1,024
Action	[✓ Permit] Deny Secured connection	

Enable Web Redirect

Protection

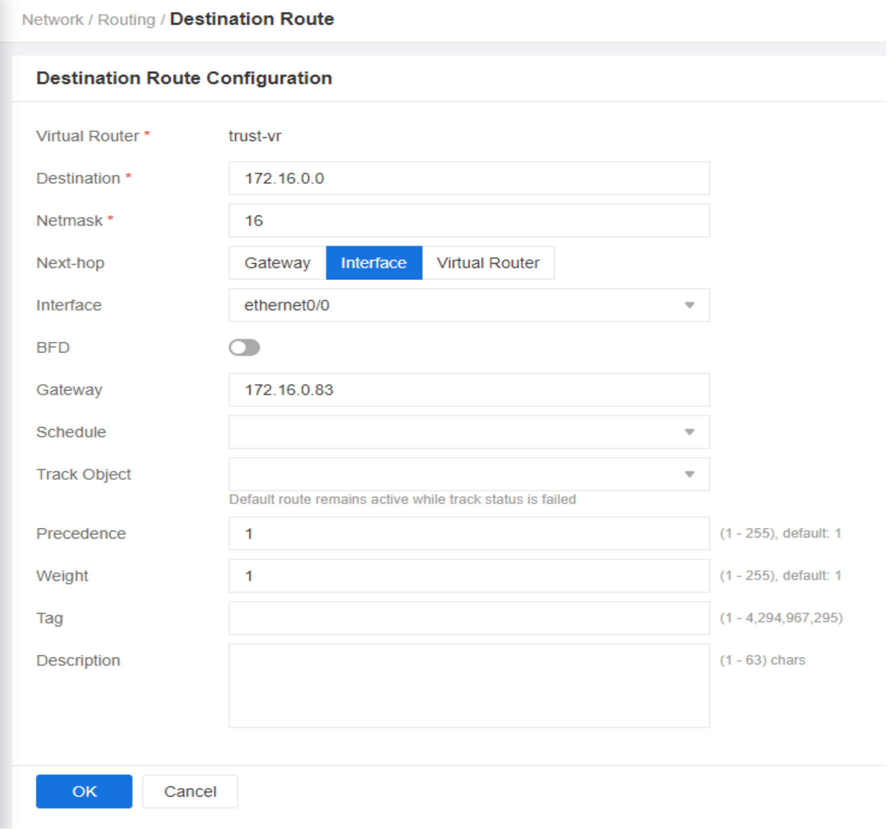
Data Security

Options

c. Configure a basic route.

Choose **Network** > **Routing** > **Destination Route**. Click **New** and set parameters, as shown in **Figure 1-32**.

Figure 1-32 Configuring a destination route



Network / Routing / Destination Route

Destination Route Configuration

Virtual Router *	trust-vr
Destination *	172.16.0.0
Netmask *	16
Next-hop	Gateway / **Interface** / Virtual Router
Interface	ethernet0/0
BFD	○
Gateway	172.16.0.83
Schedule	
Track Object	 Default route remains active while track status is failed
Precedence	1 (1 - 255), default: 1
Weight	1 (1 - 255), default: 1
Tag	(1 - 4,294,967,295)
Description	(1 - 63) chars

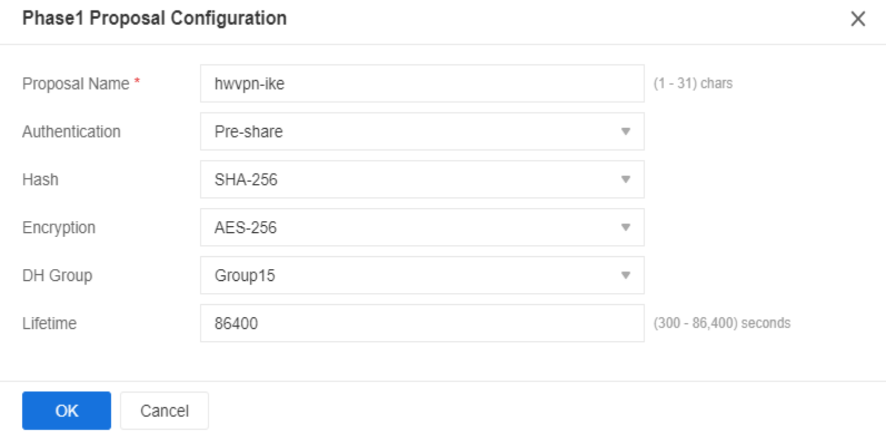
3. Configure VPN connections.

   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 1-33** shows the key parameter settings.

Figure 1-33 Configuring a phase-1 proposal



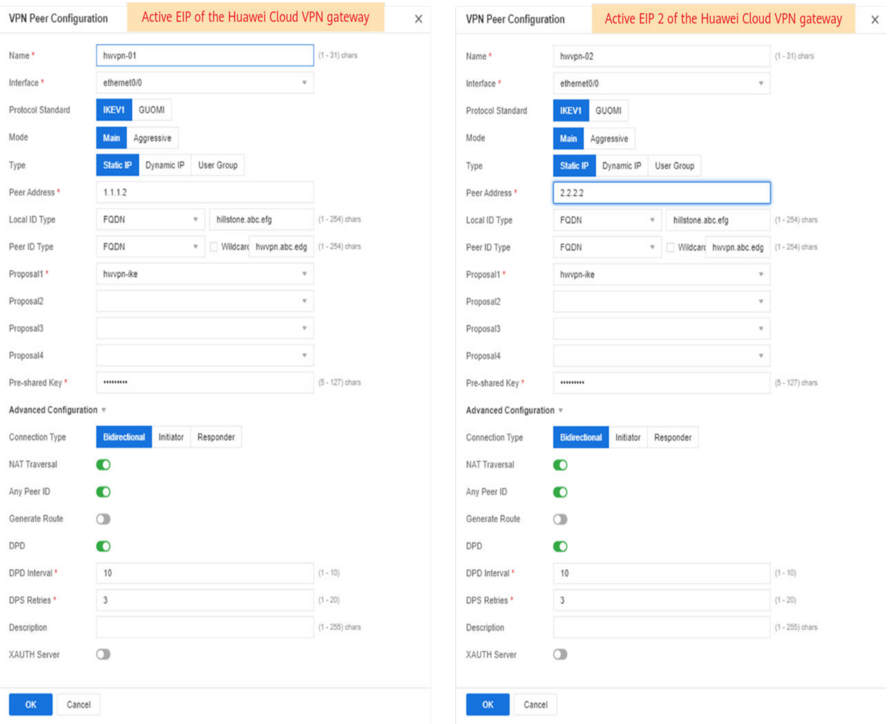
Phase1 Proposal Configuration

Proposal Name *	hwvpn-ike (1 - 31) chars
Authentication	Pre-share
Hash	SHA-256
Encryption	AES-256
DH Group	Group15
Lifetime	86400 (300 - 86,400) seconds

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 1-34 Configuring VPN peers



VPN Peer Configuration

Active EIP of the Huawei Cloud VPN gateway

- Name *: hwvpn-01 (1 - 31) chars
- Interface *: ethernet0/0
- Protocol Standard: [✓ IKEV1] GUOMI
- Mode: [✓ Main] Aggressive
- Type: [✓ Static IP] Dynamic IP User Group
- Peer Address *: 1.1.1.2
- Local ID Type: FQDN hillstone.abc.efg (1 - 254) chars
- Peer ID Type: FQDN ☐ Wildcard hwvpn.abc.edg (1 - 254) chars
- Proposal1 *: hwvpn-ike
- Proposal2:
- Proposal3:
- Proposal4:
- Pre-shared Key *: •••••••••• (5 - 127) chars

Advanced Configuration

- Connection Type: [✓ Bidirectional] Initiator Responder
- NAT Traversal: ●
- Any Peer ID: ●
- Generate Route: ○
- DPD: ●
- DPD Interval *: 10 (1 - 10)
- DPS Retries *: 3 (1 - 20)
- Description: (1 - 255) chars
- XAUTH Server: ○

OK Cancel

VPN Peer Configuration

Active EIP 2 of the Huawei Cloud VPN gateway

- Name *: hwvpn-02 (1 - 31) chars
- Interface *: ethernet0/0
- Protocol Standard: [✓ IKEV1] GUOMI
- Mode: [✓ Main] Aggressive
- Type: [✓ Static IP] Dynamic IP User Group
- Peer Address *: 2.2.2.2
- Local ID Type: FQDN hillstone.abc.efg (1 - 254) chars
- Peer ID Type: FQDN ☐ Wildcard hwvpn.abc.edg (1 - 254) chars
- Proposal1 *: hwvpn-ike
- Proposal2:
- Proposal3:
- Proposal4:
- Pre-shared Key *: •••••••••• (5 - 127) chars

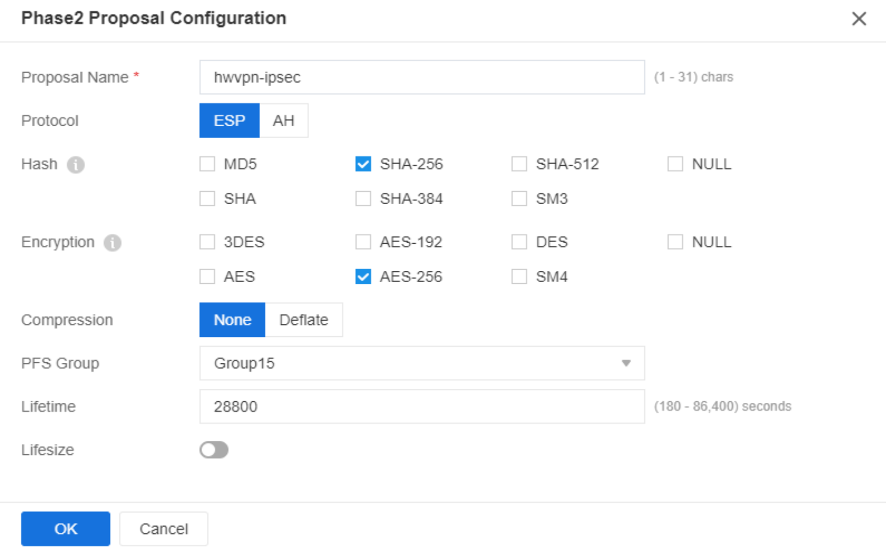
Advanced Configuration

- Connection Type: [✓ Bidirectional] Initiator Responder
- NAT Traversal: ●
- Any Peer ID: ●
- Generate Route: ○
- DPD: ●
- DPD Interval *: 10 (1 - 10)
- DPS Retries *: 3 (1 - 20)
- Description: (1 - 255) chars
- XAUTH Server: ○

OK Cancel

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 1-35 shows the key parameter settings.

Figure 1-35 Configuring a phase-2 proposal



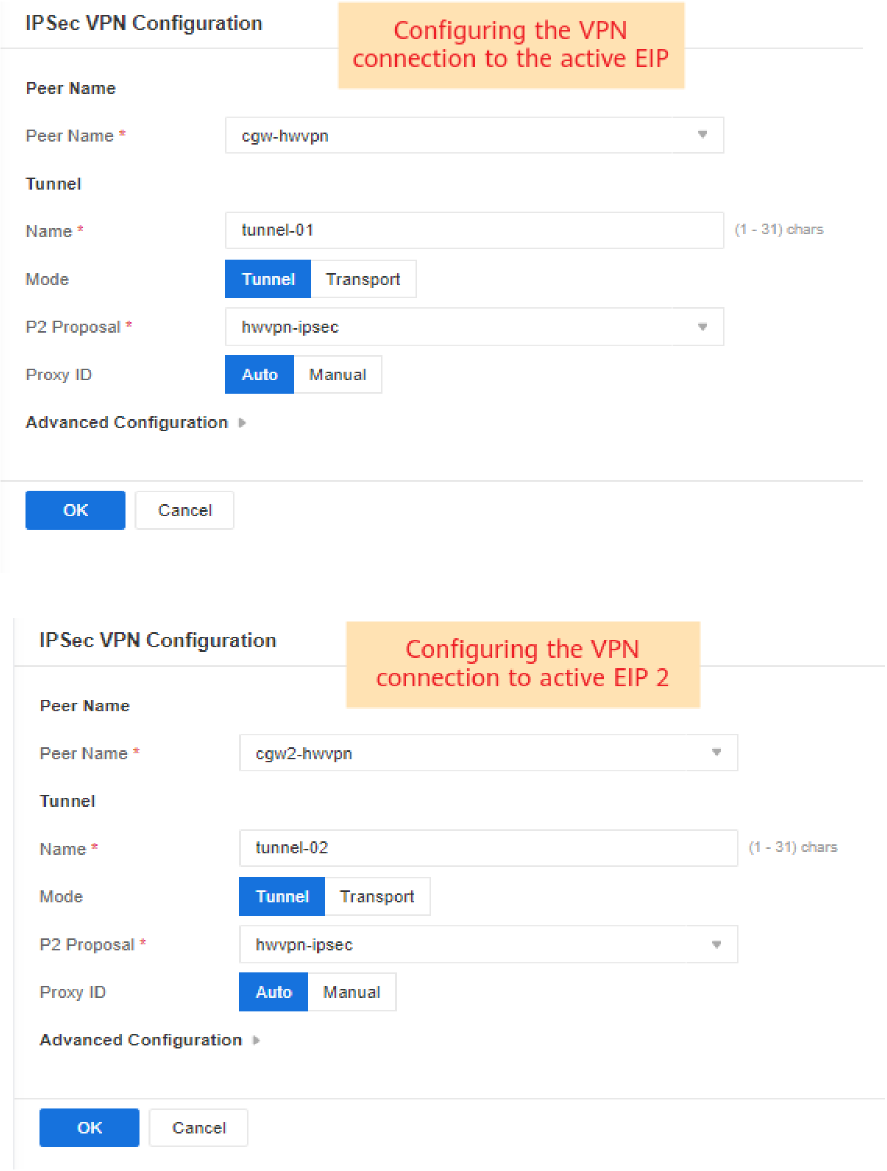
Phase2 Proposal Configuration

- Proposal Name *: hwvpn-ipsec (1 - 31) chars
- Protocol: [✓ ESP] AH
- Hash: ☐ MD5 ☑ SHA-256 ☐ SHA-512 ☐ NULL ☐ SHA ☐ SHA-384 ☐ SM3
- Encryption: ☐ 3DES ☐ AES-192 ☐ DES ☐ NULL ☐ AES ☑ AES-256 ☐ SM4
- Compression: [✓ None] Deflate
- PFS Group: Group15
- Lifetime: 28800 (180 - 86,400) seconds
- Lifesize: ○

OK Cancel

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 1-36 Configuring IPsec VPN



IPSec VPN Configuration

Configuring the VPN connection to the active EIP

Peer Name

Peer Name *: cgw-hwvpn

Tunnel

Name *: tunnel-01 (1 - 31) chars

Mode: Tunnel | Transport

P2 Proposal *: hwvpn-ipsec

Proxy ID: Auto | Manual

Advanced Configuration

OK | Cancel

IPSec VPN Configuration

Configuring the VPN connection to active EIP 2

Peer Name

Peer Name *: cgw2-hwvpn

Tunnel

Name *: tunnel-02 (1 - 31) chars

Mode: Tunnel | Transport

P2 Proposal *: hwvpn-ipsec

Proxy ID: Auto | Manual

Advanced Configuration

OK | Cancel

4. Configure tunnel interfaces.

a. Choose **Network** > **Interface**, click **New**, and choose **Tunnel Interface**.

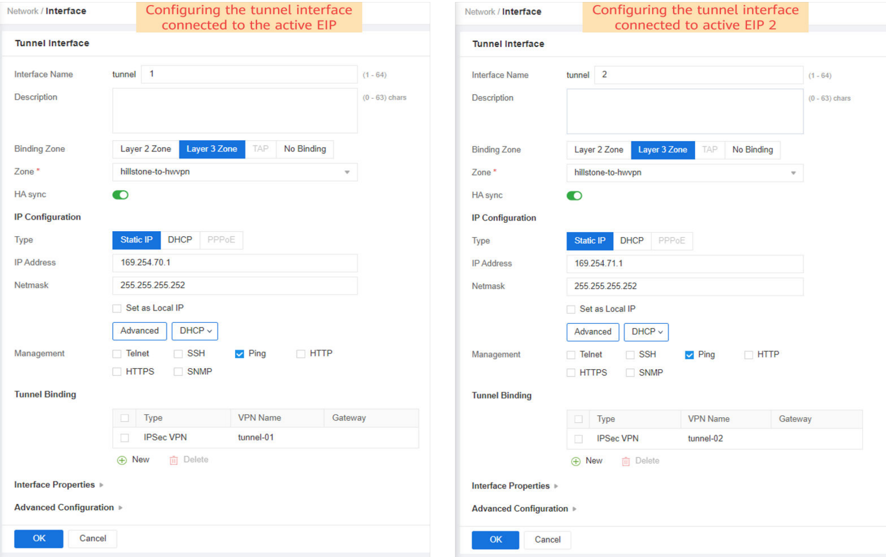
b. Configure two tunnel interfaces. **Figure 1-37** shows the key parameter settings.

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 1-37 Configuring tunnel interfaces



Network / **Interface**

Configuring the tunnel interface connected to the active EIP

Tunnel Interface

Interface Name: tunnel 1 (1 - 64)

Description: (0 - 63) chars

Binding Zone: Layer 2 Zone | **Layer 3 Zone** | TAP | No Binding

Zone *: hillstone-to-hwvpn

HA sync: ●

IP Configuration

Type: **Static IP** | DHCP | PPPoE

IP Address: 169.254.70.1

Netmask: 255.255.255.252

□ Set as Local IP

Advanced | DHCP

Management: □ Telnet □ SSH ☑ Ping □ HTTP □ HTTPS □ SNMP

Tunnel Binding

□	Type	VPN Name	Gateway
□	IPSec VPN	tunnel-01	

New Delete

Interface Properties

Advanced Configuration

OK Cancel

Network / **Interface**

Configuring the tunnel interface connected to active EIP 2

Tunnel Interface

Interface Name: tunnel 2 (1 - 64)

Description: (0 - 63) chars

Binding Zone: Layer 2 Zone | **Layer 3 Zone** | TAP | No Binding

Zone *: hillstone-to-hwvpn

HA sync: ●

IP Configuration

Type: **Static IP** | DHCP | PPPoE

IP Address: 169.254.71.1

Netmask: 255.255.255.252

□ Set as Local IP

Advanced | DHCP

Management: □ Telnet □ SSH ☑ Ping □ HTTP □ HTTPS □ SNMP

Tunnel Binding

□	Type	VPN Name	Gateway
□	IPSec VPN	tunnel-02	

New Delete

Interface Properties

Advanced Configuration

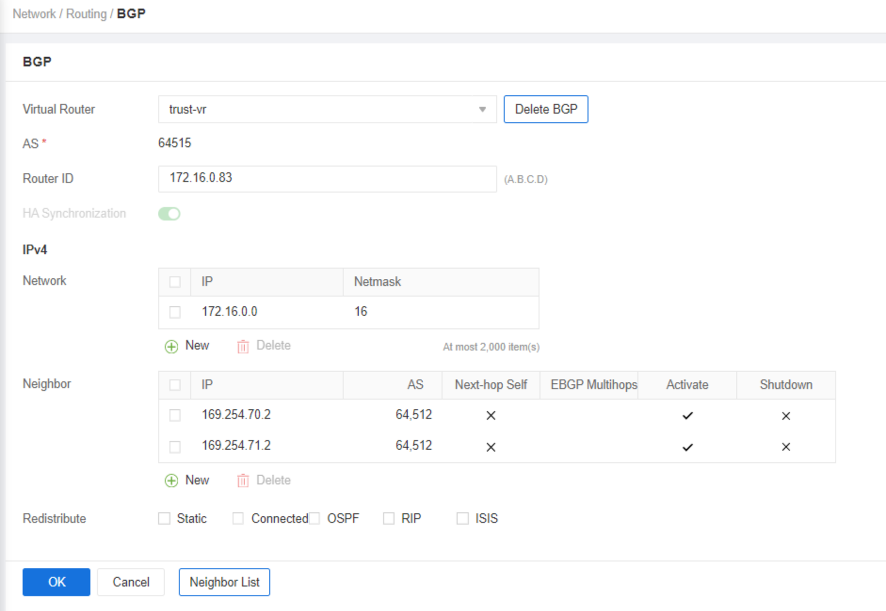
OK Cancel

5. Configure BGP.

   Choose **Network** > **Routing** > **BGP**, and complete the BGP configuration, as shown in **Figure 1-38**.

   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 1-38 Configuring BGP



Network / Routing / **BGP**

BGP

Virtual Router: trust-vr | Delete BGP

AS *: 64515

Router ID: 172.16.0.83 (A.B.C.D)

HA Synchronization: ●

IPv4

Network:

□	IP	Netmask
□	172.16.0.0	16

New Delete At most 2,000 item(s)

Neighbor:

□	IP	AS	Next-hop Self	EBGP Multihops	Activate	Shutdown
□	169.254.70.2	64,512	×		✓	×
□	169.254.71.2	64,512	×		✓	×

New Delete

Redistribute: □ Static □ Connected □ OSPF □ RIP □ ISIS

OK Cancel Neighbor List

1.4.2.5 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.

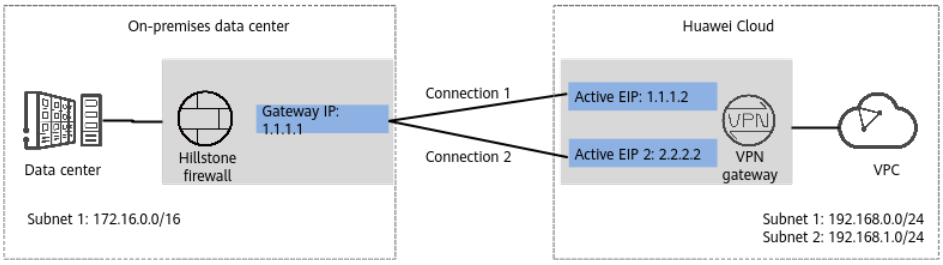
- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnet can ping each other.

1.4.3 Policy-based Mode

1.4.3.1 Scenario

Figure 1-39 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 1-39 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.

1.4.3.2 Data Plan

Table 1-38 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

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

1.4.3.3 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 1-39 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.	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 1-40 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 1-41 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 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Connection 1's Configuration	Configure the 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

1.4.3.4 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.

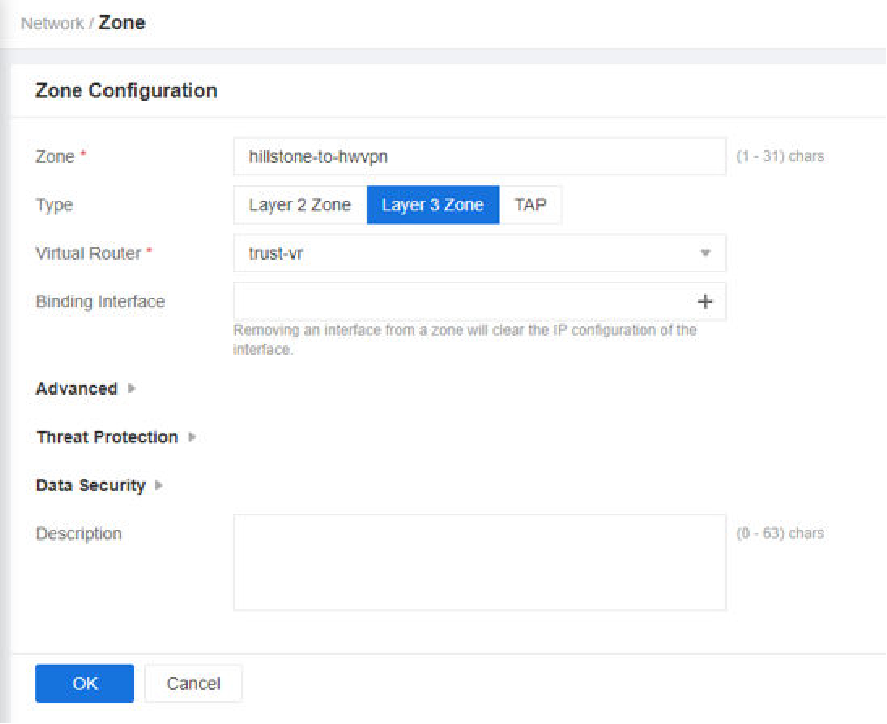
   A firewall running the 5.5R9 version is used as an example. The configuration pages may vary according to the firewall models and software versions.

2. Complete basic settings.

   a. Configure a security zone.

      Choose **Network** > **Zone**. Click **New** and set parameters, as shown in **Figure 1-40**.

      Figure 1-40 Configuring a security zone



Network / Zone

Zone Configuration

Zone * hillstone-to-hwvpn (1 - 31) chars

Type: Layer 2 Zone / Layer 3 Zone (selected) / TAP

Virtual Router * trust-vr

Binding Interface +

Removing an interface from a zone will clear the IP configuration of the interface.

Advanced ▸

Threat Protection ▸

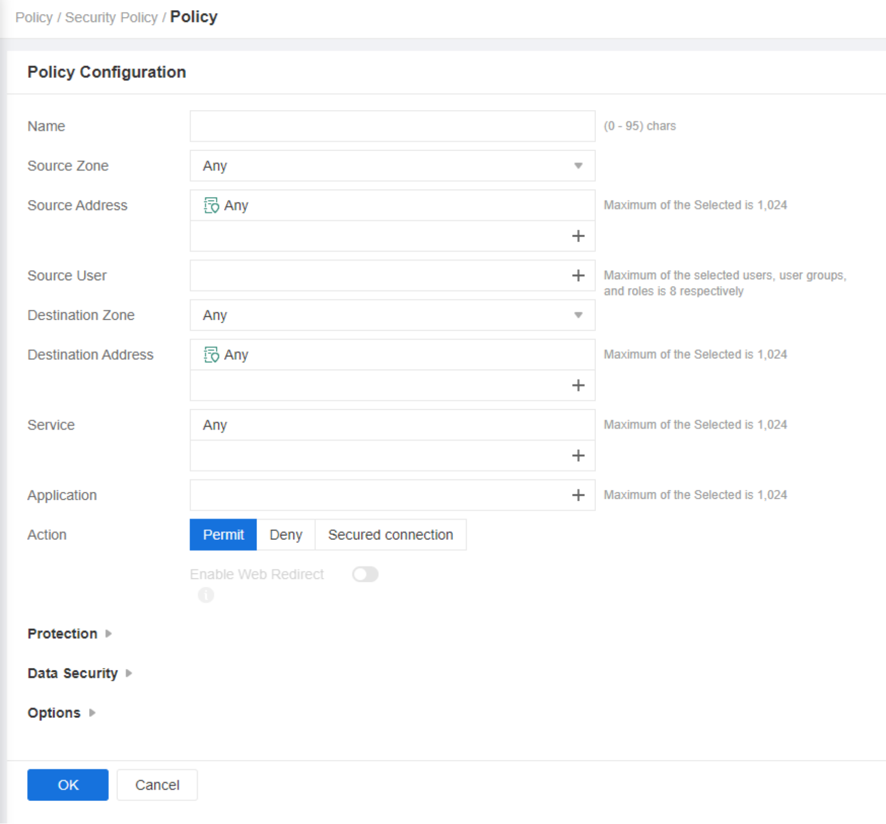
Data Security ▸

Description (0 - 63) chars

   b. Configure a security policy.

      Choose **Policy** > **Security Policy** > **Policy**. Click **New**, choose **Policy**, and set parameters, as shown in **Figure 1-41**.

Figure 1-41 Configuring a policy



Policy / Security Policy / **Policy**

Policy Configuration

Name (0 - 95) chars

Source Zone: Any

Source Address: Any — Maximum of the Selected is 1,024

Source User — Maximum of the selected users, user groups, and roles is 8 respectively

Destination Zone: Any

Destination Address: Any — Maximum of the Selected is 1,024

Service: Any — Maximum of the Selected is 1,024

Application — Maximum of the Selected is 1,024

Action: [✓ Permit] Deny Secured connection

Enable Web Redirect

Protection

Data Security

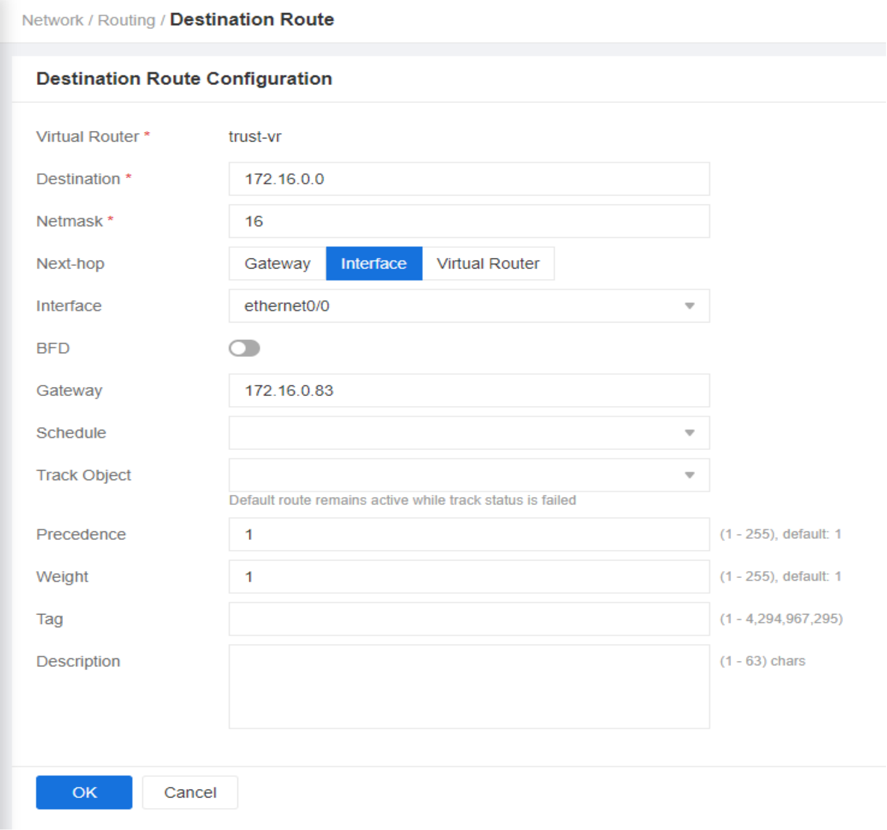
Options

OK Cancel

c. Configure a basic route.

Choose **Network** > **Routing** > **Destination Route**. Click **New** and set parameters, as shown in **Figure 1-42**.

Figure 1-42 Configuring a destination route



Network / Routing / **Destination Route**

Destination Route Configuration

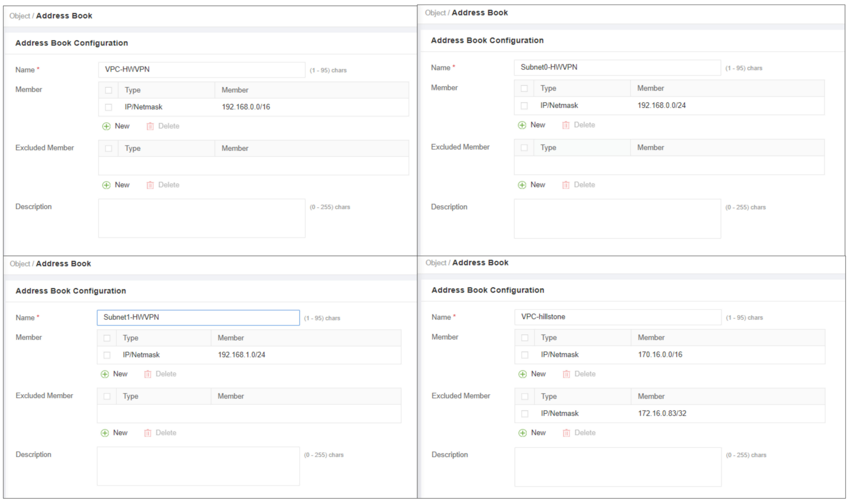
Virtual Router *	trust-vr	
Destination *	172.16.0.0	
Netmask *	16	
Next-hop	Gateway / **Interface** / Virtual Router	
Interface	ethernet0/0	
BFD	○	
Gateway	172.16.0.83	
Schedule		
Track Object	Default route remains active while track status is failed	
Precedence	1	(1 - 255), default: 1
Weight	1	(1 - 255), default: 1
Tag		(1 - 4,294,967,295)
Description		(1 - 63) chars

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 1-43 Configuring CIDR block information



Object / **Address Book**

Address Book Configuration

Name *	VPC-HWVPN	(1 - 95) chars
Member	Type: IP/Netmask Member: 192.168.0.0/16	
Excluded Member		
Description		(0 - 255) chars

Object / **Address Book**

Address Book Configuration

Name *	Subnet0-HWVPN	(1 - 95) chars
Member	Type: IP/Netmask Member: 192.168.0.0/24	
Excluded Member		
Description		(0 - 255) chars

Object / **Address Book**

Address Book Configuration

Name *	Subnet1-HWVPN	(1 - 95) chars
Member	Type: IP/Netmask Member: 192.168.1.0/24	
Excluded Member		
Description		(0 - 255) chars

Object / **Address Book**

Address Book Configuration

Name *	VPC-hillstone	(1 - 95) chars
Member	Type: IP/Netmask Member: 170.16.0.0/16	
Excluded Member	Type: IP/Netmask Member: 172.16.0.83/32	
Description		(0 - 255) chars

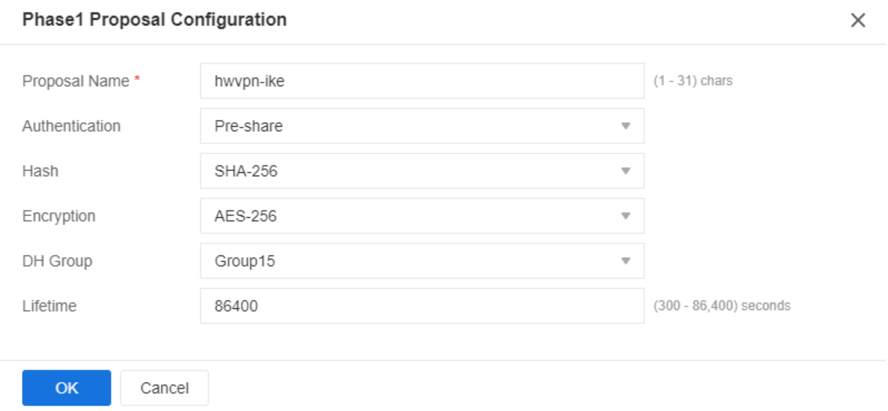
3. Configure VPN connections.

   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 1-44** shows the key parameter settings.

Figure 1-44 Configuring a phase-1 proposal



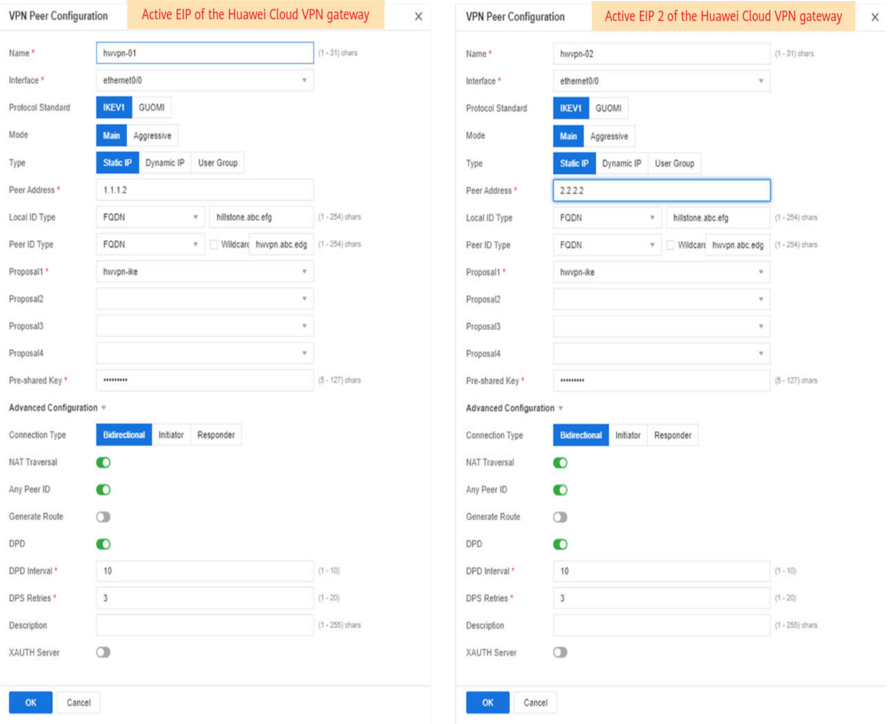
Phase1 Proposal Configuration

Proposal Name *	hwvpn-ike	(1 - 31) chars
Authentication	Pre-share	
Hash	SHA-256	
Encryption	AES-256	
DH Group	Group15	
Lifetime	86400	(300 - 86,400) seconds

   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 1-45 Configuring VPN peers



Active EIP of the Huawei Cloud VPN gateway
Active EIP 2 of the Huawei Cloud VPN gateway

VPN Peer Configuration

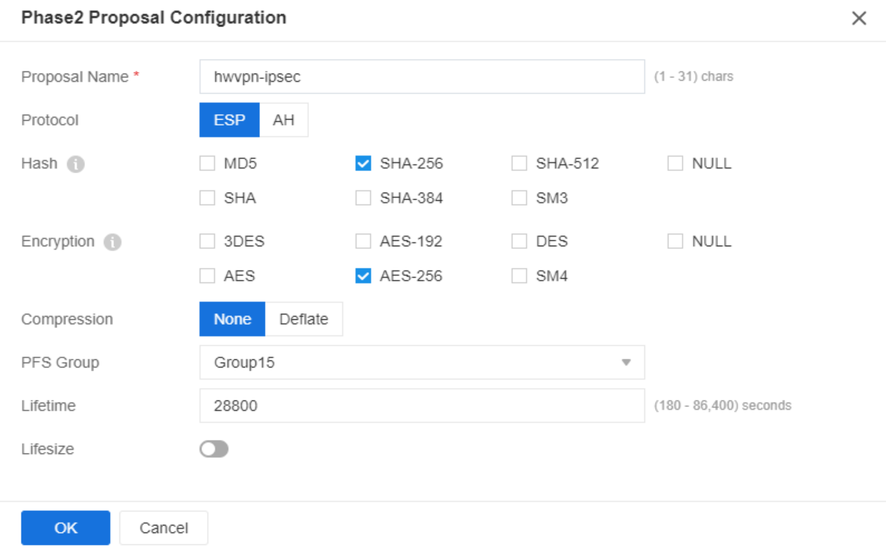
Name *	hwvpn-01 (1 - 31) chars
Interface *	ethernet0/0
Protocol Standard	IKEV1
Mode	Main
Type	Static IP
Peer Address *	1.1.1.2
Local ID Type	FQDN, hillstone.abc.efg (1 - 254) chars
Peer ID Type	FQDN, □ Wildcard, hwvpn.abc.edg (1 - 254) chars
Proposal1 *	hwvpn-ike
Proposal2	
Proposal3	
Proposal4	
Pre-shared Key *	•••••••••• (5 - 127) chars
Advanced Configuration	
Connection Type	Bidirectional
NAT Traversal	On
Any Peer ID	On
Generate Route	Off
DPD	On
DPD Interval *	10 (1 - 10)
DPS Retries *	3 (1 - 20)
Description	(1 - 255) chars
XAUTH Server	Off

VPN Peer Configuration

Name *	hwvpn-02 (1 - 31) chars
Interface *	ethernet0/0
Protocol Standard	IKEV1
Mode	Main
Type	Static IP
Peer Address *	2.2.2.2
Local ID Type	FQDN, hillstone.abc.efg (1 - 254) chars
Peer ID Type	FQDN, □ Wildcard, hwvpn.abc.edg (1 - 254) chars
Proposal1 *	hwvpn-ike
Proposal2	
Proposal3	
Proposal4	
Pre-shared Key *	•••••••••• (5 - 127) chars
Advanced Configuration	
Connection Type	Bidirectional
NAT Traversal	On
Any Peer ID	On
Generate Route	Off
DPD	On
DPD Interval *	10 (1 - 10)
DPS Retries *	3 (1 - 20)
Description	(1 - 255) chars
XAUTH Server	Off

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 1-46** shows the key parameter settings.

Figure 1-46 Configuring a phase-2 proposal

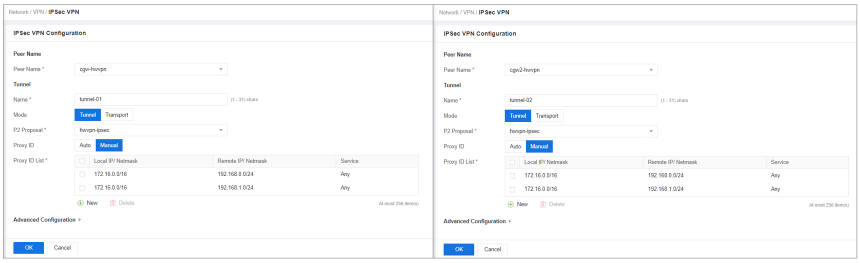


Phase2 Proposal Configuration

Proposal Name *	hwvpn-ipsec (1 - 31) chars
Protocol	ESP
Hash	□ MD5 ☑ SHA-256 □ SHA-512 □ NULL □ SHA □ SHA-384 □ SM3
Encryption	□ 3DES □ AES-192 □ DES □ NULL □ AES ☑ AES-256 □ SM4
Compression	None
PFS Group	Group15
Lifetime	28800 (180 - 86,400) seconds
Lifesize	Off

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 1-47** shows the key parameter settings.

Figure 1-47 Configuring IPsec VPN



Network / VPN / **IPSec VPN**

IPSec VPN Configuration

Peer Name

Peer Name *: cgw-hwvpn

Tunnel

Name *: tunnel-01 (1 - 31) chars

Mode: [✓ Tunnel] Transport

P2 Proposal *: hwvpn-ipsec

Proxy ID: Auto [✓ Manual]

Proxy ID List *:

□	Local IP/ Netmask	Remote IP/ Netmask	Service
□	172.16.0.0/16	192.168.0.0/24	Any
□	172.16.0.0/16	192.168.1.0/24	Any

New Delete At most 256 item(s)

Advanced Configuration

OK Cancel

Network / VPN / **IPSec VPN**

IPSec VPN Configuration

Peer Name

Peer Name *: cgw2-hwvpn

Tunnel

Name *: tunnel-02 (1 - 31) chars

Mode: [✓ Tunnel] Transport

P2 Proposal *: hwvpn-ipsec

Proxy ID: Auto [✓ Manual]

Proxy ID List *:

□	Local IP/ Netmask	Remote IP/ Netmask	Service
□	172.16.0.0/16	192.168.0.0/24	Any
□	172.16.0.0/16	192.168.1.0/24	Any

New Delete At most 256 item(s)

Advanced Configuration

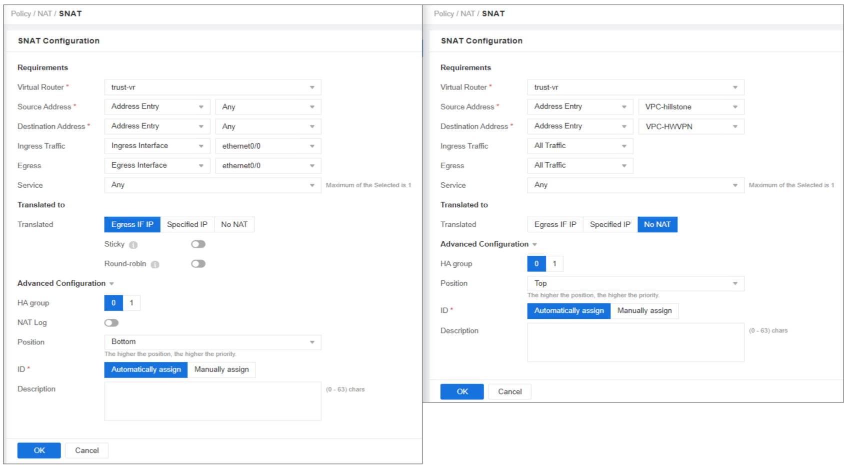
OK Cancel

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 1-48**.

Figure 1-48 Configuring source NAT



Policy / NAT / **SNAT**

SNAT Configuration

Requirements

Virtual Router *: trust-vr

Source Address *: Address Entry | Any

Destination Address *: Address Entry | Any

Ingress Traffic: Ingress Interface | ethernet0/0

Egress: Egress Interface | ethernet0/0

Service: Any Maximum of the Selected is 1

Translated to

Translated: [✓ Egress IF IP] Specified IP No NAT

Sticky: off

Round-robin: off

Advanced Configuration

HA group: [✓ 0] 1

NAT Log: off

Position: Bottom
The higher the position, the higher the priority.

ID *: [✓ Automatically assign] Manually assign

Description: (0 - 63) chars

OK Cancel

Policy / NAT / **SNAT**

SNAT Configuration

Requirements

Virtual Router *: trust-vr

Source Address *: Address Entry | VPC-hillstone

Destination Address *: Address Entry | VPC-HWVPN

Ingress Traffic: All Traffic

Egress: All Traffic

Service: Any Maximum of the Selected is 1

Translated to

Translated: Egress IF IP Specified IP [✓ No NAT]

Advanced Configuration

HA group: [✓ 0] 1

Position: Top
The higher the position, the higher the priority.

ID *: [✓ Automatically assign] Manually assign

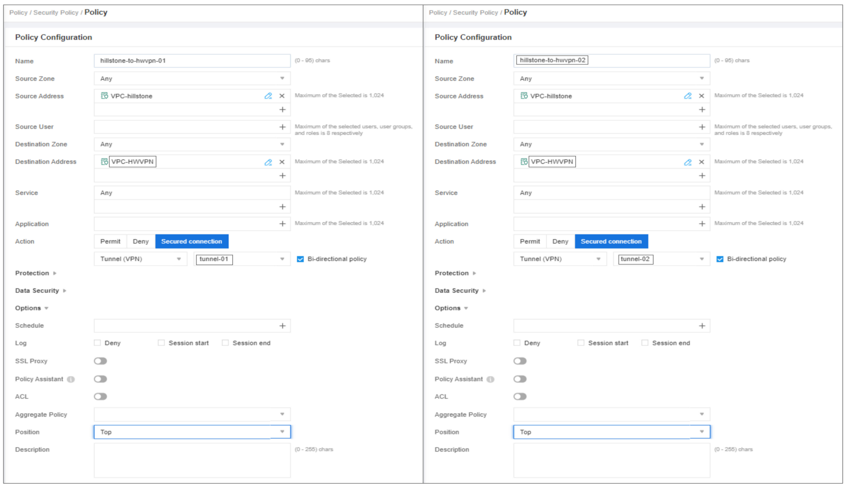
Description: (0 - 63) chars

OK Cancel

   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 1-49**.

Figure 1-49 Configuring VPN security policies



Policy / Security Policy / **Policy**

Policy Configuration

Name: hillstone-to-hwvpn-01 (0 - 95) chars
Source Zone: Any
Source Address: VPC-hillstone — Maximum of the Selected is 1,024
Source User: — Maximum of the selected users, user groups, and roles is 8 respectively
Destination Zone: Any
Destination Address: VPC-HWVPN — Maximum of the Selected is 1,024
Service: Any — Maximum of the Selected is 1,024
Application: — Maximum of the Selected is 1,024
Action: Permit | Deny | **Secured connection**
Tunnel (VPN) | tunnel-01 | ☑ Bi-directional policy
Protection
Data Security
Options
Schedule:
Log: □ Deny □ Session start □ Session end
SSL Proxy: ○
Policy Assistant: ○
ACL: ○
Aggregate Policy:
Position: Top
Description: (0 - 255) chars

Policy / Security Policy / **Policy**

Policy Configuration

Name: hillstone-to-hwvpn-02 (0 - 95) chars
Source Zone: Any
Source Address: VPC-hillstone — Maximum of the Selected is 1,024
Source User: — Maximum of the selected users, user groups, and roles is 8 respectively
Destination Zone: Any
Destination Address: VPC-HWVPN — Maximum of the Selected is 1,024
Service: Any — Maximum of the Selected is 1,024
Application: — Maximum of the Selected is 1,024
Action: Permit | Deny | **Secured connection**
Tunnel (VPN) | tunnel-02 | ☑ Bi-directional policy
Protection
Data Security
Options
Schedule:
Log: □ Deny □ Session start □ Session end
SSL Proxy: ○
Policy Assistant: ○
ACL: ○
Aggregate Policy:
Position: Top
Description: (0 - 255) chars

1.4.3.5 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.

1.5 Interconnection with a Sangfor Vrtual Firewall

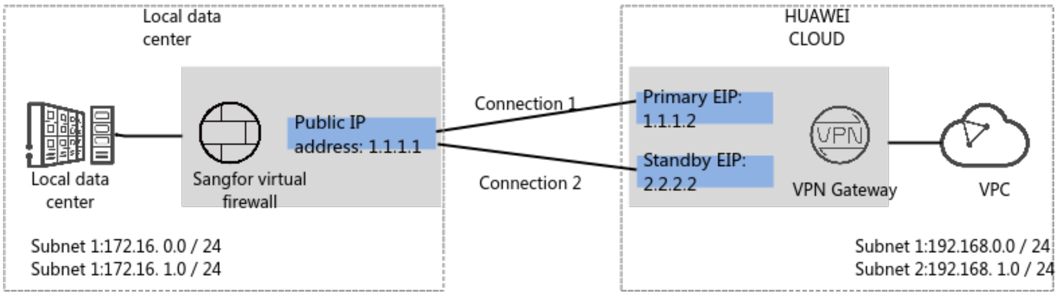
1.5.1 Policy-based Mode

1.5.1.1 Operation Guide

Scenario

Figure 1-50 shows the typical networking for connecting a Huawei Cloud VPN gateway to a Sangfor virtual firewall in policy-based mode.

Figure 1-50 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 1-42 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	
	IPsec policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-256 ● PFS: DH group 15 ● Transfer protocol: ESP ● Lifetime (s): 3600 ● Packet encapsulation mode: TUNNEL	

1.5.1.2 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 1-43 describes the parameters for creating a VPN gateway.

Table 1-43 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
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 1-44 only describes the key parameters for creating a customer gateway.

Table 1-44 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 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 1-45 describes the key parameters for creating VPN connections.

Table 1-45 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

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 **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 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Connection 1's Configuration	Configure the 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

1.5.1.3 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.
   1. Choose **Network** > **Interface** > **Physical Interface**.
   2. Locate the row that contains eth0 and click **Edit** in the **Operation** column to configure the interface attributes.
   3. Set **Zone** to **L3_trust_A** and select **WAN** for **Basic Attributes**.
3. Enable the IPsec VPN capability of the firewall.
   1. Choose **Network** > **IPSecVPN** > **DLAN Running Status**.
   2. In the VPN Running Status area, select **Enable VPN service**.
4. Configure an IPsec VPN line.
   1. Choose **Network** > **IPSecVPN** > **Basic Configuration**.
   2. In the IPsec VPN Line area, click **Add Line**.
   3. Set parameters as prompted.

      Table 1-46 describes the parameters. For other parameters, use their default settings.

Table 1-46 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 1-47**. For other parameters, use their default settings.

Table 1-47 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 1-48**. For other parameters, use their default settings.

Table 1-48 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 1-49 describes the parameters. For other parameters, use their default settings.

Table 1-49 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 1-45**.	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 1-45**. – 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 1-45**. – 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 1-45**. - 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 1-45**. – 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 1-45**. 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

1.5.1.4 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**.
- 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 TheGreenBow VPN Client

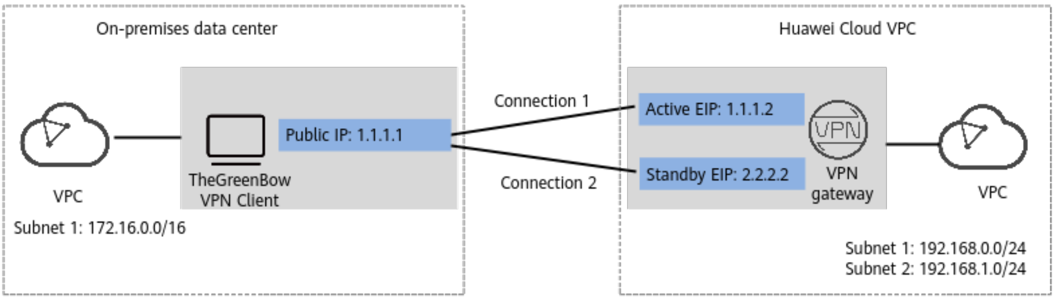
1.6.1 Static Routing Mode

1.6.1.1 Operation Guide

Scenario

Figure 1-51 shows the typical networking where a Huawei Cloud VPN gateway connects to TheGreenBow VPN Client in static routing mode.

Figure 1-51 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 1-50 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: 169.254.70.2/30 ● Customer tunnel interface address: 169.254.70.1/30
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30
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

1.6.1.2 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 1-51 describes the parameters for creating a VPN gateway.

Table 1-51 Description of VPN gateway parameters

Paramete r	Description	Value
Name	Name of a VPN gateway.	vpngw-001

Paramete r	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
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 1-52 describes the parameters for creating a customer gateway.

Table 1-52 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 1-53 describes the parameters for creating VPN connections.

Table 1-53 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 and 214.0.0.0/8 cannot be used as customer subnets.	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, 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.	169.254.70.2/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30
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.	169.254.71.2/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----End

1.6.1.3 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 1-54 describes the key parameters. For other parameters, use their default settings.

Table 1-54 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 1-53**.	Test@123
	Encryption	The settings must be the same as those of the IKE policy configured in **Table 1-53**.	• 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 1-52**.	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 1-53**.	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 1-55 describes the key parameters. For other parameters, use their default settings.

Table 1-55 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 1-53.	• 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

1.6.1.4 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.

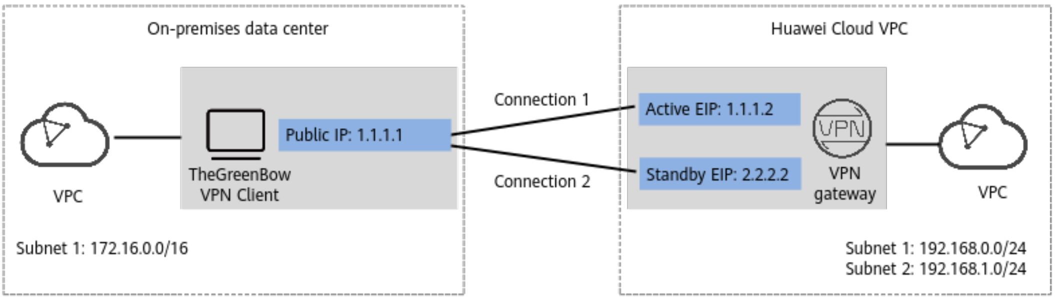
1.6.2 Policy-based Mode

1.6.2.1 Operation Guide

Scenario

Figure 1-52 shows the typical networking where a Huawei Cloud VPN gateway connects to TheGreenBow VPN Client in policy-based mode.

Figure 1-52 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 1-56 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

1.6.2.2 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 1-57 describes the parameters for creating a VPN gateway.

Table 1-57 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
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 1-58 describes the parameters for creating a customer gateway.

Table 1-58 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 1-59 only describes the parameters for creating VPN connections.

Table 1-59 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
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 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Connection 1's Configuration	Configure the 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

1.6.2.3 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 1-60 describes the key parameters. For other parameters, use their default settings.

Table 1-60 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 1-59**.	Test@123

Tab Page	Parameter	Description	Value
	Encryption	The settings must be the same as those of the IKE policy configured in **Table 1-59**.	- 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 1-58**.	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 1-59**.	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 1-61 describes the key parameters. For other parameters, use their default settings.

Table 1-61 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 1-59**.	• 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

1.6.2.4 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.

1.7 16 Interconnection with strongSwan

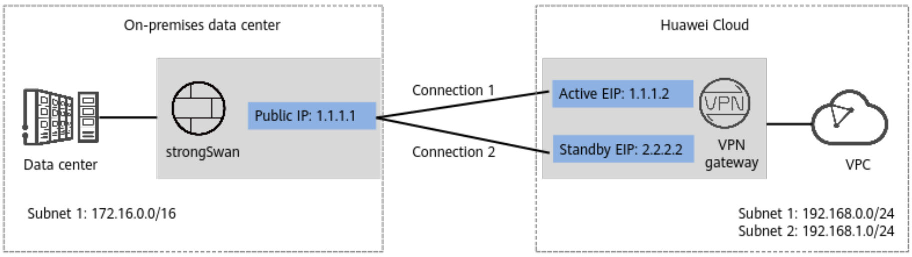
1.7.1 Static Routing Mode

1.7.1.1 Operation Guide

Scenario

Figure 1-53 shows the typical networking where a Huawei Cloud VPN gateway connects to strongSwan in static routing mode.

Figure 1-53 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 1-62 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: 169.254.70.2/30 ● Customer tunnel interface address: 169.254.70.1/30
	Tunnel interface addresses under **Connection 2's Configuration**	● Local tunnel interface address: 169.254.71.2/30 ● Customer tunnel interface address: 169.254.71.1/30
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

1.7.1.2 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 1-63 describes the parameters for creating a VPN gateway.

Table 1-63 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
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 1-64 describes the parameters for creating a customer gateway.

Table 1-64 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 1-65 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

Parameter	Description	Value
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 and 214.0.0.0/8 cannot be used as customer subnets.	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, 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.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.70.1/30

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. **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.	169.254.71.2/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.1/30

----End

1.7.1.3 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

1.7.1.4 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.

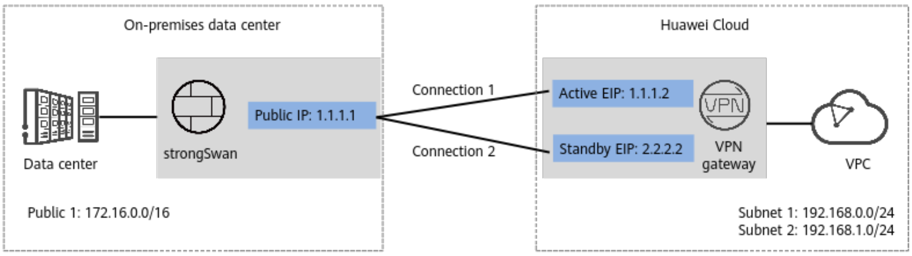
1.7.2 Policy-based Mode

1.7.2.1 Operation Guide

Scenario

Figure 1-54 shows the typical networking where a Huawei Cloud VPN gateway connects to strongSwan in policy-based mode.

Figure 1-54 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 1-66 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

1.7.2.2 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 1-67 describes the parameters for creating a VPN gateway.

Table 1-67 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

Paramete r	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 1-68 describes the parameters for creating a customer gateway.

Table 1-68 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 1-69 only describes the key parameters for creating VPN connections. For other parameters, use their default settings.

Table 1-69 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
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 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Connection 1's Configuration	Configure the 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

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 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

1.7.2.3 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

1.7.2.4 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 P2C VPN

2.1 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, click **Upload** in the **Server Certificate** 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.

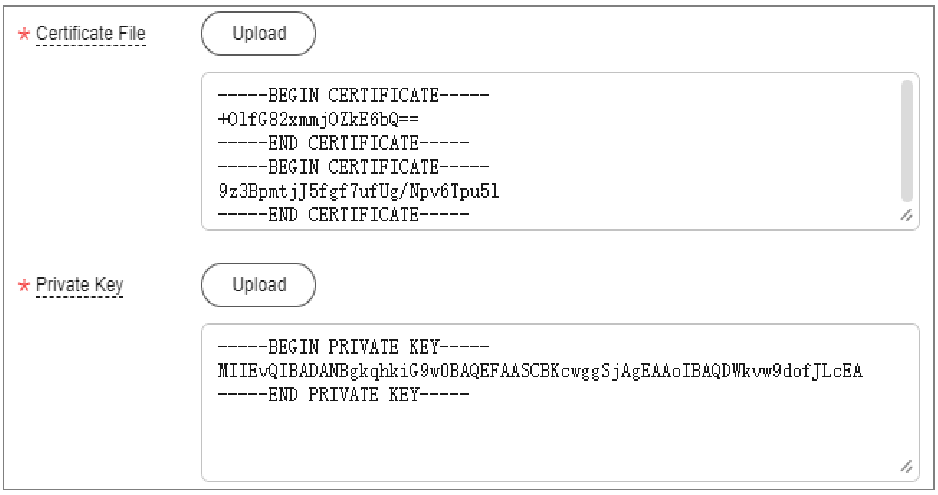
Table 2-1 describes the parameters for uploading a certificate.

Table 2-1 Parameters for uploading an international standard certificate

Parameter	Description
Certificate standard	Select **International**.
Certificate Name	User-defined name of a certificate.
Enterprise Project	Select the enterprise project to which the SSL certificate is to be added.

Parameter	Description
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 2-1**.
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 2-1**.

Figure 2-1 Format of the certificate content to be uploaded



```
-----BEGIN CERTIFICATE-----
+OlfG82xmmjOZkE6bQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
9z3BpmtjJ5fgf7ufUg/Npv6Tpu5l
-----END CERTIFICATE-----
```

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDWkvw9dofJLcEA
-----END PRIVATE KEY-----
```

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

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

Scenario

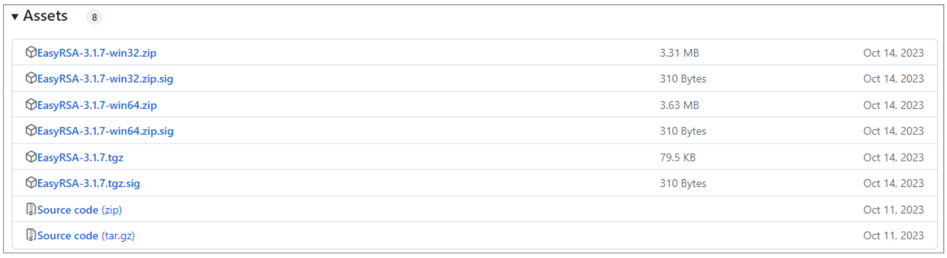
Easy-RSA is an open-source certificate management tool used to generate and manage digital certificates.

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.

   ▾ Assets 8

EasyRSA-3.1.7-win32.zip	3.31 MB	Oct 14, 2023
EasyRSA-3.1.7-win32.zip.sig	310 Bytes	Oct 14, 2023
EasyRSA-3.1.7-win64.zip	3.63 MB	Oct 14, 2023
EasyRSA-3.1.7-win64.zip.sig	310 Bytes	Oct 14, 2023
EasyRSA-3.1.7.tgz	79.5 KB	Oct 14, 2023
EasyRSA-3.1.7.tgz.sig	310 Bytes	Oct 14, 2023
Source code (zip)		Oct 11, 2023
Source code (tar.gz)		Oct 11, 2023

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 **.\EasyRSA-Start.bat** command to start Easy-RSA.

   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 **./easyrsa init-pki** command to initialize the PKI environment.

   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 **./easyrsa build-ca nopass** command to generate a CA certificate.

   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 **./easyrsa build-server-full** *p2cserver.com* **nopass** command to generate a server certificate and private key.

    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 **./easyrsa build-client-full** *p2cclient.com* **nopass** command to generate a client certificate and private key.

    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.

2.3 Using Easy-RSA to Issue Certificates (Server and Client Using Different CA Certificates)

Scenario

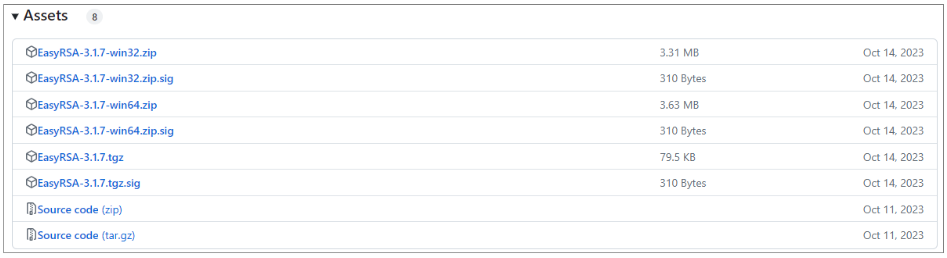
Easy-RSA is an open-source certificate management tool used to generate and manage digital certificates.

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.



▾ Assets 8

EasyRSA-3.1.7-win32.zip	3.31 MB	Oct 14, 2023
EasyRSA-3.1.7-win32.zip.sig	310 Bytes	Oct 14, 2023
EasyRSA-3.1.7-win64.zip	3.63 MB	Oct 14, 2023
EasyRSA-3.1.7-win64.zip.sig	310 Bytes	Oct 14, 2023
EasyRSA-3.1.7.tgz	79.5 KB	Oct 14, 2023
EasyRSA-3.1.7.tgz.sig	310 Bytes	Oct 14, 2023
Source code (zip)		Oct 11, 2023
Source code (tar.gz)		Oct 11, 2023

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 **.\EasyRSA-Start.bat** command to start Easy-RSA.

   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 **./easyrsa init-pki** command to initialize the PKI environment.

   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 **.\EasyRSA-Start.bat** command to start Easy-RSA.

   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 **./easyrsa build-ca nopass** command to generate a server CA certificate.

   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 **./easyrsa build-server-full** *p2cserver.com* **nopass** command to generate a server certificate and private key.

    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 **.\EasyRSA-Start.bat** command to start Easy-RSA.

    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 **./easyrsa build-ca nopass** command to generate a client CA certificate.

      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 **./easyrsa build-client-full** *p2cclient.com* **nopass** command to generate a client certificate and private key.

    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.

2.4 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. .
    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. .