Virtual Private Network

Getting Started

Issue 01

Date 2025-07-30

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

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

1 Preparations

Before using VPN, make the following preparations.

Signing up for a HUAWEI ID and Enabling Huawei Cloud Services

If you already have a HUAWEI ID and have enabled Huawei Cloud services, skip this step. If you do not have a HUAWEI ID, perform the following steps to create one:

1. Go to the **Huawei Cloud** official website, and click **Sign Up** in the upper right corner.
2. Complete the registration as prompted. For details, see **Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services**.

   If the registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in **Real-Name Authentication**.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For VPN pricing details, see **Pricing Details**.

Creating a User and Granting VPN Permissions

To use VPN, you must have the "VPN Fullaccess" permission.

- For details about system permissions supported by VPN, see **Permissions Management**.
- For details about how to create a user and grant permissions to the user, see **Creating a User and Granting VPN Permissions**.

2 Configuring Enterprise Edition VPN to Connect an On-premises Data Center to a VPC

2.1 Overview

Supported Regions

The supported regions are subject to those available on the management console.

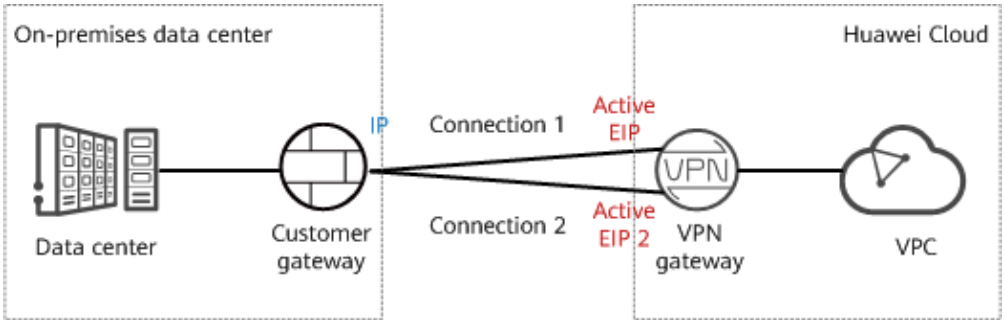
Scenario

To meet business development requirements, enterprise A needs to implement communication between its on-premises data center and its VPC. In this case, enterprise A can use the VPN service to create connections between the on-premises data center and the VPC.

- If the on-premises data center has only one customer gateway and this gateway can be configured with only one IP address, it is recommended that the VPN gateway use the active-active mode. **Figure 2-1** shows the networking.

  In active-active mode, if connection 1 is faulty, traffic is automatically switched to connection 2 for transmission, without affecting enterprise services.

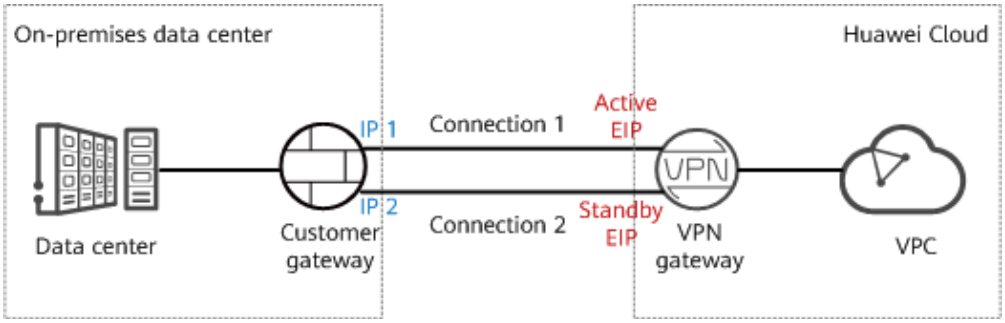
  Figure 2-1 Active-active mode



- If the on-premises data center has two customer gateways or has only one customer gateway that can be configured with two IP addresses, it is recommended that the VPN gateway use the active/standby mode. **Figure 2-2** shows the networking.

  In active/standby mode, connection 1 is the active link and connection 2 is the standby link. By default, traffic is transmitted only through the active link. If the active link fails, traffic is automatically switched to the standby link, without affecting enterprise services. After the active link recovers, traffic is switched back to the active link.

Figure 2-2 Active/Standby mode



Limitations and Constraints

- The customer gateway device must support standard IKE and IPsec protocols.
- The interconnection subnets of the on-premises data center neither overlap with those of the VPC nor contain 100.64.0.0/10 or 214.0.0.0/8.

  If the VPC uses Direct Cloud or Cloud Connect connections to communicate with other VPCs, the on-premises data center subnets cannot overlap with those of these VPCs.

Data Plan

Table 2-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	192.168.0.0/16
VPN gateway	Interconnection subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	HA mode	Active-active

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: 11.xx.xx.11 • Active EIP 2: 11.xx.xx.12
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	The IP addresses are used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Gateway IP address	The gateway IP address is assigned by a carrier. In this example, the gateway IP address is: 22.xx.xx.22

Operation Process

Figure 2-3 shows the process of using the VPN service to enable communication between an on-premises data center and a VPC.

Figure 2-3 Operation process

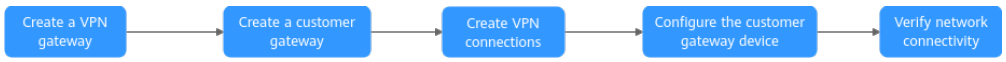


Table 2-2 Operation process description

No.	Step	Description
1	**Step 1: Creating 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	**Step 2: Creating a Customer Gateway**	Configure the VPN device in the on-premises data center as the customer gateway.
3	**Step 3: Creating VPN Connections**	• Create two VPN connections between the VPN gateway (active EIP and active EIP 2) and the customer gateway. • The connection mode, PSK, IKE policy, and IPsec policy settings of connection 2 must be the same as those of connection 1.
4	**Step 4: Configuring the Customer Gateway Device**	• The local and remote tunnel interface addresses configured on the customer gateway device must be the same as the customer and local tunnel interface addresses of the Huawei Cloud VPN connections, respectively. • The connection mode, PSK, IKE policy, and IPsec policy settings on the customer gateway device must be same as those of the Huawei Cloud VPN connections.
5	**Step 5: Verifying Network Connectivity**	Log in to an ECS and run the **ping** command to verify the network connectivity.

2.2 Step 1: Creating a VPN Gateway

Prerequisites

- A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.
- Security group rules have been configured for ECSs in the VPC, and allow the customer gateway in the on-premises data center to access VPC resources. For details about how to configure security group rules, see **Security Group Rules**.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner, and choose **Networking** > **Virtual Private Network**.

Step 3 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.

Step 4 Click **Buy S2C VPN Gateway**.

Step 5 Set parameters as prompted, click **Buy Now**, and complete the payment.

Step 6 The following describes only key parameters. For details about more parameters, see **Creating a VPN Gateway**.

Table 2-3 Key VPN gateway parameters

Parameter	Description	Example Value
Billing Mode	The options include **Yearly/Monthly** and **Pay-per-use**.	Yearly/Monthly
Region	Select the region nearest to you.	EU-Dublin
AZ	Two types of AZs are supported: **General**.	General
Name	Enter the name a VPN gateway.	vpngw-001
Network Type	• **Public network**: A VPN gateway communicates with a customer gateway in an on-premises data center through the Internet. • **Private network**: A VPN gateway communicates with a customer gateway in an on-premises data center through a private network.	Public network
Associate With	• **VPC**: Through a VPC, the VPN gateway sends messages to the customer gateway or servers in the local subnet.	VPC
VPC	Select the VPC that needs to access the on-premises data center.	vpc-001(192.168.0.0/16)
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Specify the VPC subnet that needs to access the on-premises data center. You can manually enter a CIDR block or select a subnet from the drop-down list box.	192.168.0.0/24
Specification	Select **Professional 1**.	Professional 1

Parameter	Description	Example Value
HA Mode	Select **Active-active**.	Active-active
Active EIP	You can buy a new EIP or use an existing EIP.	11.xx.xx.11
Active EIP 2		11.xx.xx.12

----End

Verification

Check the created VPN gateway on the **VPN Gateways** page. The initial state of the VPN gateway is **Creating**. When the VPN gateway state changes to **Normal**, the VPN gateway is successfully created.

2.3 Step 2: Creating a Customer Gateway

Procedure

Step 1 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.

Step 2 On the **Customer Gateways** page, click **Create Customer Gateway**.

Step 3 Set parameters as prompted and click **Create Now**.

The following describes only key parameters. For details about more parameters, see **Creating a Customer Gateway**.

Table 2-4 Customer gateway parameters

Parameter	Description	Example Value
Name	Name a customer gateway.	cgw-001
Identifier	Enter the IP address of the customer gateway.	IP Address, 22.xx.xx.22

----End

Verification

Check the created customer gateway on the **Customer Gateways** page.

2.4 Step 3: Creating VPN Connections

Procedure

Step 1 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.

Step 2 On the **VPN Connection** page, click **Create VPN Connection**.

Step 3 Set VPN connection parameters as prompted and click **Buy Now**.

The following describes only key parameters. For details, see **Creating a VPN Connection**.

Table 2-5 Description of VPN connection parameters

Parameter	Description	Example Value
Name	Enter the name of VPN connection 1.	vpn-001
VPN Gateway	Select the VPN gateway created in **2.2 Step 1: Creating a VPN Gateway**.	vpngw-001
VPN Gateway IP of Connection 1	Select the active EIP of the VPN gateway.	11.xx.xx.11
Customer Gateway of Connection 1	Select the customer gateway of connection 1.	cgw-001
VPN Gateway IP of Connection 2	Select active EIP 2 of the VPN gateway.	11.xx.xx.12
Customer Gateway of Connection 2	Select the customer gateway of connection 2.	cgw-001
VPN Type	Select **Static routing**.	Static routing

Parameter	Description	Example Value
Customer Subnet	Enter the subnet of the on-premises data center that needs to access the VPC. **NOTE** • The customer subnet can overlap with the local subnet but cannot be the same as the local subnet. • A customer subnet cannot be included in the existing subnets of the VPC associated with the VPN gateway. It also cannot be the destination address in the route table of the VPC associated with the VPN gateway. • Customer subnets cannot be the reserved CIDR blocks of VPCs, for example, 100.64.0.0/10 or 214.0.0.0/8. • If the interconnection subnet is associated with an ACL rule, ensure that the ACL rule permits the TCP port for traffic between all local and customer subnets. • Address groups cannot be used to configure the source and destination subnets in a policy on customer gateway devices.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of gateway 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	The options include **Manually specify** and **Automatically assign**.	Manually specify
Local Tunnel Interface Address	Specify the tunnel interface address of the VPN gateway. **NOTE** The local and remote interface addresses configured on the customer gateway device must be the same as the values of **Customer Tunnel Interface IP Address** and **Local Tunnel Interface IP Address**, respectively.	169.254.70.2/30
Customer Tunnel Interface Address	Specify the tunnel interface address of the customer gateway device.	169.254.70.1/30

Parameter	Description	Example Value
Link Detection	This function is used for route reliability detection in multi-link scenarios. **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	Specify the negotiation key of the VPN connection. The PSKs configured on the VPN console and the customer gateway device must be the same.	Test@123
Policy Settings	Configure the IKE and IPsec policies, which define the encryption algorithms used by the VPN tunnel. The policy settings on the VPN console and the customer gateway device must be the same.	Default
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**.	Disabled
Local Tunnel Interface Address	Specify the tunnel interface address of the VPN gateway.	169.254.71.2/30
Customer Tunnel Interface Address	Specify the tunnel interface address of the customer gateway device.	169.254.71.1/30

----End

Verification

Check the created VPN connection on the **VPN Connection** page. The initial state of the VPN connection is **Creating**. As the customer gateway device has not been configured, no VPN connection can be established. After about 2 minutes, the VPN connection state changes to **Not connected**.

2.5 Step 4: Configuring the Customer Gateway Device

Procedure

> NOTE
>
> In this example, the customer gateway device is an AR router of Huawei.

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. In this example, the WAN interface of the AR router is GigabitEthernet 0/0/8.

```
[AR651]interface GigabitEthernet 0/0/8
[AR651-GigabitEthernet0/0/8]ip address 22.xx.xx.22 255.255.255.0
[AR651-GigabitEthernet0/0/8]quit
```

Step 4 Configure a default route.

```
[AR651]ip route-static 0.0.0.0 0.0.0.0 22.xx.xx.1
```

In this command, *22.xx.xx.1* is the gateway address of the AR router's public IP address. Replace it with the actual gateway address.

Step 5 Enable the SHA-2 algorithm to be compatible with the standard RFC algorithms.

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

Step 6 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 7 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 8 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 22.xx.xx.22
[AR651-ike-peer-hwpeer1]remote-address 11.xx.xx.11
[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 22.xx.xx.22
[AR651-ike-peer-hwpeer2]remote-address 11.xx.xx.12
```



```
[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:

- **pre-shared-key cipher**: configures a PSK, which must be the same as that configured on the VPN console.
- **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 9 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 10 Configure virtual tunnel interfaces.

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 22.xx.xx.22
[AR651-Tunnel0/0/1]destination 11.xx.xx.11
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 22.xx.xx.22
[AR651-Tunnel0/0/2]destination 11.xx.xx.12
[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 11 Configure NQA.

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



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

The commands are described as follows:

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

  In this example, the test instance **IPsec_nqa1** is created for the VPN connection to which the active EIP of the VPN gateway belongs; the test instance **IPsec_nqa2** is created for the VPN connection to which active EIP 2 of the VPN gateway belongs.
- **destination-address**: specifies the tunnel interface address of the VPN connection.
- **source-address**: specifies the tunnel interface address of the AR router.

Step 12 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 192.168.0.0 255.255.255.0 Tunnel0/0/2 track nqa IPsec_nqa2 IPsec_nqa2
```

The parameters are described as follows:

- **192.168.0.0** indicates the local subnet of the VPC.
- **Tunnel***x* and **IPsec_nqa***x* in the same command correspond to the same VPN connection.

----End

Verification

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner, and choose **Networking** > **Virtual Private Network**.

Step 3 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.

Verify that the states of the two VPN connections are both **Normal**.

----End

2.6 Step 5: Verifying Network Connectivity

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 **Service List** and choose **Compute** > **Elastic Cloud Server**.

Step 4 Log in to an ECS.

Multiple methods are available for logging in to an ECS. For details, see **Logging In to an ECS**.

Login using VNC on the management console is used as an example. For details, see **Login Using VNC**.

Step 5 Run the following command on the ECS:

ping 172.16.0.100

172.16.0.100 is the IP address of a server in the on-premises data center. Replace it with an actual server IP address.

If information similar to the following is displayed, the VPC on the cloud and the on-premises data center can communicate with each other.

```
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=27ms TTL=245
```

----End

3 Configuring P2C VPN to Connect Mobile Terminals to a VPC

3.1 Overview

Supported Regions

The supported regions are subject to those available on the console.

Scenario

Enterprise employee A on a business trip needs to access a service website, for which the website server is deployed on Huawei Cloud. Employee A wants to use a VPN client on a PC to access this website server.

Limitations and Constraints

- The client CIDR block cannot overlap with the destination CIDR block in the VPC to be accessed, and cannot contain special CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8.
- The client device can access the Internet.

Prerequisites

- You have obtained the server certificate and private key, created a user, and configured a password for the user. For details about how to issue a certificate by yourself, see **Using Easy-RSA to Issue Certificates (Server and Client Sharing a CA Certificate)**.
- The server certificate has been hosted by the Cloud Certificate Manager (CCM). For details about how to host a server certificate, see **Using the CCM to Manage a Server Certificate**.

Data Plan

Table 3-1 Data plan

Category	Item	Data
VPC	Subnet to be interconnected	192.168.0.0/16
VPN gateway	Interconnection subnet	Subnet used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has three or more assignable IP addresses. 192.168.2.0/24
	Maximum number of connections	10
	EIP	An EIP is automatically generated when you buy it. In this example, the EIP 11.*xx.xx*.11 is generated.
Server	Local CIDR block	192.168.1.0/24
	Server certificate	cert-server (name of the server certificate hosted by the CCM)
	SSL parameters	• Protocol: TCP • Port: 443 • Encryption algorithm: AES-128-GCM • Authentication algorithm: SHA256 • Compression: disabled
Client	Client CIDR block	172.16.0.0/16
	Client authentication mode	Default mode: password authentication (local) • User group – Name: Testgroup_01 • User – Name: Test_01 – Password: *Set it based on the site requirements.* – User group: Testgroup_01 • Access policy – Name: Policy_01 – Destination CIDR block: 192.168.1.0/24 – User group: Testgroup_01

Operation Process

Figure 3-1 shows the process of configuring the VPN service to allow a client to remotely access a VPC.

Figure 3-1 Operation process

Table 3-2 Operation process description

No.	Step	Description
1	3.2 Step 1: Creating a VPN Gateway	A VPN gateway needs to have an EIP bound. If you have purchased an EIP, you can directly bind it to the VPN gateway.
2	3.3 Step 2: Configuring a Server	• Specify the CIDR block used by the client (client CIDR block) to access a specified destination CIDR block (local CIDR block). • Select the server certificate and client authentication mode used for identity authentication during VPN connection establishment. The client authentication mode can be set to **Certificate authentication** or **Password authentication (local)**. • Configure SSL parameters (such as the protocol, port, authentication algorithm, and encryption algorithm) for the VPN connection.
3	3.4 Step 3: Configuring a Client	Download the client configuration from the management console, modify the configuration file as required, and import it to the VPN client.
4	3.5 Step 4: Verifying Connectivity	Open the command-line interface (CLI) on the client device, and run the **ping** command to verify the connectivity.

3.2 Step 1: Creating a VPN Gateway

Prerequisites

- A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.

- Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see **Security Group Rules**.

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, and then click **Buy P2C VPN Gateway**.

Step 6 Set parameters as prompted and click **Buy Now**.

The following describes only key parameters. For details about more parameters, see **Creating a VPN Gateway**.

Table 3-3 VPN gateway parameters

Parameter	Description	Example Value
Billing Mode	Only **Yearly/Monthly** is supported.	Yearly/Monthly
Region	Select the region nearest to you.	CN-Hong Kong
Name	Enter the name of a VPN gateway.	p2c-vpngw-001
VPC	Select the VPC that the client needs to access.	vpc-001(192.168.0.0/16)
Interconnection Subnet	Subnet used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has three or more assignable IP addresses.	192.168.2.0/24
Specification	Select a VPN gateway specification.	Professional 1
AZ	• If two or more AZs are available, select two AZs. • If only one AZ is available, select this AZ.	AZ1, AZ2
Connections	A VPN connection between a server and a client is counted as one connection. **NOTE** If you set the number of VPN connections to 10, all the 10 connections are free of charge.	10

Parameter	Description	Example Value
EIP	Select the EIP to be bound to the VPN gateway. You can buy a new EIP or use an existing EIP.	Create now
EIP Type	Select the type of the EIP to be bound to the VPN gateway.	Dynamic BGP
Bandwidth (Mbit/s)	Set the EIP bandwidth.	20
Bandwidth Name	Specify the name of the EIP bandwidth.	p2c-vpngw-bandwidth1
Advanced Settings > Tags	• A tag identifies a VPN resource. It consists of a key and a value. A maximum of 20 tags can be added. • You can select predefined tags or customize tags. • To view predefined tags, click **View predefined tags**.	• Tag key: vpn_key1 • Tag value: vpn-01

----End

Verification

Check the VPN gateway on the **P2C VPN Gateways** page. The initial state of the VPN gateway is **Creating**. When the VPN gateway state changes to **Normal**, the VPN gateway is successfully created.

3.3 Step 2: Configuring a Server

Prerequisites

The server certificate has been hosted by the CCM. For details about how to host a server certificate, see **Using the CCM to Manage a Server Certificate**.

Procedure

1. Configure a server.
   a. On the **P2C VPN Gateways** page, locate the target VPN gateway and click **Configure Server** in the **Operation** column.
   b. Set parameters as prompted and click **OK**.

      The following table only lists the key server parameters. For more information, see **Configuring a Server**.

Table 3-4 Server parameters

Area	Parameter	Description	Example Value
Basic Information	Local CIDR Block	Specify the destination CIDR block that clients need to access. You can select a subnet or enter a CIDR block.	192.168.1.0/24
	Client CIDR Block	Specify the CIDR block for assigning addresses to virtual NICs of clients.	172.16.0.0/16
Authentication Information	Server Certificate	Click **Upload** in the drop-down list box. Upload the certificate. For details, see **Using the CCM to Manage a Server Certificate**.	cert-server
	Client Authentication Mode	• Select **Password authentication (local)**. • Select **Certificate authentication**. Click **Upload CA Certificate**, use a text editor (such as Notepad++) to open the CA certificate file in PEM format, and copy the certificate content to the **Content** text box in the **Upload CA Certificate** dialog box. After clicking **OK**, you can manage users and configure access policies.	Password authentication (local)
Advanced Settings	Protocol	Currently, only **TCP** is supported.	TCP
	Port	The options include **443** and **1149**.	443
	Encryption Algorithm	The options include **AES-128-GCM** and **AES-256-GCM**.	AES-128-GCM
	Authentication Algorithm	The options include **SHA256** and **SHA384**.	SHA256

Area	Parameter	Description	Example Value
	Domain Name Access	Determine whether to enable domain name access. • Enabling domain name access – Valid DNS server addresses: – Not 0.0.0.0 – Non-loopback address. The loopback address range is 127.0.0.0 to 127.255.255.255. – Non-multicast address. The multicast address range is 224.0.0.0 to 239.255.255.255. – Address not starting or ending with 0 – Enter two different DNS server addresses. – Not 255.255.255.255 • Disabling domain name access By default, domain name access is disabled.	Disabled

2. Create a user group.
   a. On the **P2C VPN Gateways** page, locate the target VPN gateway and click **View Server** in the **Operation** column.
   b. Click the **User Management** and **User Groups** tabs in sequence, and click **Create User Group**.
   c. Set parameters as prompted and click **OK**.
      The following table describes only key parameters.

      Table 3-5 Key parameter for creating a user group

Parameter	Description	Example Value
Name	Enter a user group name.	Testgroup_01

3. Create an access policy.
   a. On the **P2C VPN Gateways** page, locate the target VPN gateway and click **View Server** in the **Operation** column.
   b. Click the **Access Policies** tab, and click **Create Policy**.
   c. Set parameters as prompted and click **OK**.
      The following table describes only key parameters.

Table 3-6 Key parameters for creating a policy

Parameter	Description	Example Value
Name	Only letters, digits, underscores (_), and hyphens (-) are allowed.	Policy_01
Destination CIDR Block	Enter one or more CIDR blocks. You need to separate multiple CIDR blocks with commas (,). Examples are as follows: • Single destination CIDR block: 192.168.1.0/24 • Multiple destination CIDR blocks: 192.168.1.0/24,192.168.2.0/24	192.168.1.0/24
User Group	Select a user group.	Testgroup_01

4. Create a user.
   a. On the **P2C VPN Gateways** page, locate the target VPN gateway and click **View Server** in the **Operation** column.
   b. Click the **User Management** tab. On the **Users** tab page, click **Create User**.
   c. Set parameters as prompted and click **OK**.

      The following table describes only key parameters.

Table 3-7 Key parameters for creating a user

Parameter	Description	Example Value
Name	The value can contain a maximum of 64 characters, including letters, digits, periods (.), underscores (_), and hyphens (-). **NOTE** Do not use the following usernames that are reserved in the system: • **L3SW_** (prefix) • **link** • **Cascade** • **SecureNAT** • **localbridge** • **administrator** (case-insensitive)	Test_01

Parameter	Description	Example Value
Password	• The value contains 8 to 32 characters. • The value must contain at least two types of the following characters: uppercase letters, lowercase letters, digits, and special characters including `~!@#$%^&*()-_=+|[{}];:'",<.>/? and spaces. • The password cannot be the username or the reverse of the username.	*Set this parameter based on the site requirements.*
Confirm Password	Reenter the password.	*Set this parameter based on the site requirements.*
User Group	Select the user group to which the user belongs. **NOTE** A user that is not added to any user group cannot access resources on the cloud.	Testgroup_01
Specify Client IP Address	Toggle off this option.	Disabled

3.4 Step 3: Configuring a Client

Prerequisites

- You have created a user and configured a password for the user.
- The client device can access the Internet.

Procedure

1. Download the client configuration.
   a. On the **P2C VPN Gateways** page, locate the target VPN gateway, and click **Download Client Configuration** in the **Operation** column to download the configuration package.
   b. Decompress the package to obtain the **client_config.conf**, **client_config.ovpn**, and **README.md** files.
      - The **client_config.conf** file applies to the Linux operating system.
      - The **client_config.ovpn** file applies to the Windows, macOS, and Android operating systems.

2. Install the client software and import the configuration file.

   NOTE

   This example describes how to configure a client on the Windows operating system. The configuration process varies according to the type and version of the VPN client software.

   - Operating system: Windows 10
   - Client software: OpenVPN-2.6.6-I001

   For more client configuration cases, see **Configuring a Client**.

   a. Download the OpenVPN GUI installation package and install it as prompted.

      The installation package varies according to the Windows operating system as follows:

      - For a 32-bit Windows operating system, download the **Windows 32-bit MSI installer**.
      - For a 64-bit Windows operating system, download the **Windows 64-bit MSI installer**.
      - For a 64-bit Windows ARM-based operating system, download the **Windows ARM64 MIS installer**.

   b. Click **OpenVPN GUI** in the Start menu to start the client.

      The message "OpenVPN GUI is already running. Right click on the tray icon to start." is displayed in the lower right corner.

   c. Right-click the  icon on the Windows taskbar, choose **Import** > **Import file**, and import the **client_config.ovpn** file.

      When the file is imported, the message "File imported successfully." is displayed in the lower right corner.

   d. Double-click the  icon on the Windows taskbar. On the **OpenVPN GUI** page that is displayed, set parameters as prompted and click **OK**.

      Table 3-8 OpenVPN Connect parameters

Parameter	Description	Example Value
Username	Enter the name of the user created on the **User Management** tab page.	Test_01
Password	Enter the password of the user created on the **User Management** tab page.	*Set this parameter based on the site requirements.*

   e. Right-click the  icon on the Windows taskbar, and choose **Connect**.

      When the icon on the taskbar changes to  , the connection is established successfully.

3.5 Step 4: Verifying Connectivity

Procedure

1. Open the CLI of the client device.
2. Run the following command to verify connectivity:

   ping 192.168.1.10

   192.168.1.10 is the IP address of an ECS. Replace it with the actual IP address.

   To obtain the IP address of an ECS, perform the following operations:

   a. On the **P2C VPN Gateways** page, click the name of the VPC to which the target VPN gateway belongs.

   b. On the **Summary** tab page, click the number of created ECSs in the **VPC Resources** area.

   c. On the **Elastic Cloud Server** page, locate the target ECS, and view its private IP address in the **IP Address** column.
3. If information similar to the following is displayed, the client can communicate with the ECS:

```
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=27ms TTL=245
```