Virtual Private Network

Getting Started

Issue 01

Date 2024-07-22

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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

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.

Registering 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 **Register** 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 **Individual 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 Administrator" 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 S2C 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 console.

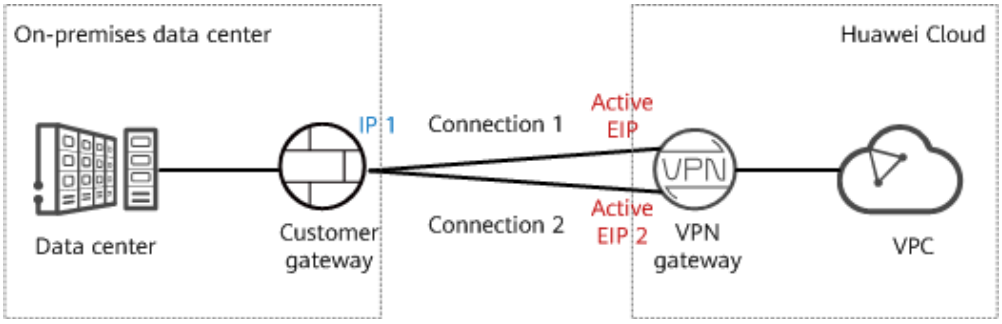
Scenario

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 uses the active-active mode. **Figure 2-1** shows the networking.

  In active-active mode, if connection 1 fails, traffic is automatically switched to connection 2, without affecting enterprise services. After connection 1 recovers, VPN still uses connection 2 for data transmission.

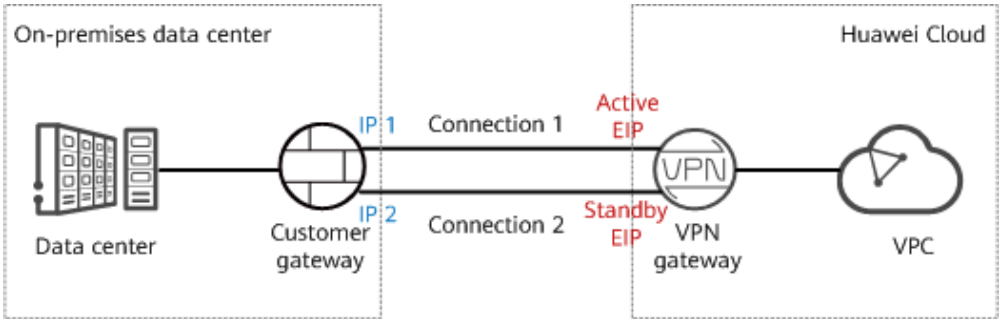
  Figure 2-1 Active-active mode



- 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 address	This address is used by a VPN gateway to establish an IPsec tunnel with a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • VPN connection 1: 169.254.70.1/30 • VPN connection 2: 169.254.71.1/30
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
	Tunnel interface address	• VPN connection 1: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30

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

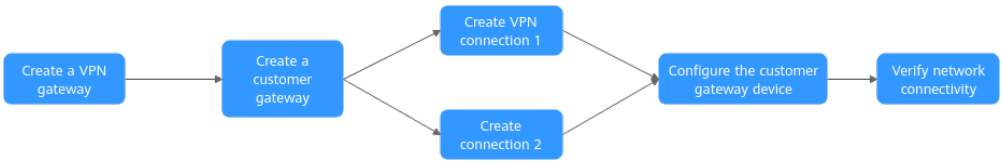


Table 2-2 Operation process description

No.	Step	Description
1	2.2 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.

No.	Step	Description
2	2.3 Step 2: Creating a Customer Gateway	Configure the VPN device in the on-premises data center as the customer gateway.
3	2.4 Step 3: Creating VPN Connection 1	Create a VPN connection between the active EIP of the VPN gateway and the customer gateway.
4	2.5 Step 4: Creating VPN Connection 2	Create a VPN connection between active EIP 2 of the VPN gateway and the customer gateway. It is recommended that the routing mode, PSK, IKE policy, and IPsec policy settings of the two VPN connections be the same.
5	2.6 Step 5: 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 connection, respectively. • The routing mode, PSK, IKE policy, and IPsec policy settings on the customer gateway device must be same as those of the Huawei Cloud VPN connection.
6	2.7 Step 6: 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 of the page, and choose **Networking** > **Virtual Private Network**.

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

Step 4 On the **S2C VPN Gateways** tab page, click **Buy S2C VPN Gateway**.

Step 5 Set parameters as prompted, click **Next**, 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.	AP-Singapore
Name	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	The options include **VPC** and **Enterprise Router**	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** and deselect **Access via a non-fixed IP address**.	Professional 1
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 **OK**.

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 Connection 1

Procedure

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

Step 2 On the **VPN Connections** page, click **Buy VPN Connection**.

Step 3 Set parameters for VPN connection 1 as prompted and click **Submit**.

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

Table 2-5 Parameter settings for VPN connection 1

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
Gateway IP Address	Select the active EIP of the VPN gateway.	11.xx.xx.11
Customer Gateway	Select the customer gateway created in **2.3 Step 2: Creating a Customer Gateway**.	cgw-001
VPN Type	Select **Static routing**.	Static routing
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.	172.16.0.0/16
Interface IP Address Assignment	The options include **Manually specify** and **Automatically assign**.	Manually specify
Local Tunnel Interface Address	Specify the tunnel interface address configured on 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

Parameter	Description	Example Value
Customer Tunnel Interface Address	Specify the tunnel interface address configured on the customer gateway device.	169.254.70.1/30
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

----End

Verification

Check the created VPN connection on the **VPN Connections** 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: Creating VPN Connection 2

Procedure

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

Step 2 On the **VPN Connections** page, click **Buy VPN Connection**.

For VPN connection 2, you are advised to use the same settings as VPN connection 1, except the connection name, gateway IP address, local tunnel interface IP address, and customer tunnel interface IP address.

Table 2-6 Parameter settings for VPN connection 2

Parameter	Description	Example Value
Name	Enter the name of VPN connection 2.	vpn-002
VPN Gateway	Select the VPN gateway created in **2.2 Step 1: Creating a VPN Gateway**.	vpngw-001
Gateway IP Address	Select active EIP 2 of the VPN gateway.	11.xx.xx.12
Customer Gateway	Select the customer gateway created in **2.3 Step 2: Creating a Customer Gateway**.	cgw-001
VPN Type	Select **Static routing**.	Static routing
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.	172.16.0.0/16
Interface IP Address Assignment	The options include **Manually specify** and **Automatically assign**.	Manually specify
Local Tunnel Interface Address	Specify the tunnel interface address configured on 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.	169.254.71.2/30

Parameter	Description	Example Value
Customer Tunnel Interface Address	Specify the tunnel interface address configured on the customer gateway device.	169.254.71.1/30
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

----End

Verification

Check the created VPN connection on the **VPN Connections** 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**.

2.6 Step 5: Configuring the Customer Gateway Device

Procedure

NOTE

In this example, the customer gateway device is an AR router of Huawei. For more examples of configuring customer gateway devices, see **Administrator Guide**.

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 gateway.
- **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 of the page, 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

2.7 Step 6: 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**.

In this example, use VNC provided on the management console to log in to an ECS.

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 Enterprise Edition 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

Employee A on a business trip needs to check important data that can be viewed only on the intranet. The website server storing the data is deployed on Huawei Cloud. Employee A wants to use a VPN client 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.
- The server certificate has been hosted by the Cloud Certificate Manager (CCM).

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
	Connections (created/ remaining)	0/10
	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 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 of the page, 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**.

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.	20
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

Parameter	Description	Example Value
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.

Configuring a Server

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

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

Area	Parameter	Description	Example Value
Authentication Information	Server Certificate	Click **Upload** in the drop-down list box.	cert-server
	Client Authentication Mode	• Select **Certificate authentication**. Click **Upload Client CA Certificate**, open the CA certificate file in .pem format as a text file, and copy the certificate content to the **Content** text box in the **Upload Client CA Certificate** dialog box. • Select **Password authentication (local)**. After clicking **OK**, you can manage users and configure access policies.	Password authentication (local)
Advanced Settings	Protocol	Use the default value.	TCP
	Port	Use the default value.	443
	Encryption Algorithm	Use the default value.	AES-128-GCM
	Authentication Algorithm	Use the default value.	SHA256

Managing Users

1. On the **P2C VPN Gateways** page, locate the target VPN gateway and click **Configure Server** in the **Operation** column.
2. Set parameters as prompted and click **OK**.
3. 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

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 3-6 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**, and **administrator** (case-insensitive).	Test_01
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 the following special characters: `~!@#$%^&*()-_=+|[{}];:'",<.>/? 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.*

Parameter	Description	Example Value
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

Creating an Access Policy

1. On the **P2C VPN Gateways** page, locate the target VPN gateway and click **View Server** in the **Operation** column.
2. Click the **Access Policies** tab, and click **Create Policy**.
3. Set parameters as prompted and click **OK**.

   The following table describes only key parameters.

   Table 3-7 Key parameters for creating a policy

Parameter	Description	Example Value
Name	Only letters, digits, underscores (_), and hyphens (-) are allowed.	Policy_01
Destination CIDR Block	If you enter multiple CIDR blocks, separate them with commas (,), for example, **192.168.1.0/24,192.168.2.0/24**.	192.168.1.0/24
User Group	Select a user group.	Testgroup_01

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.

Downloading the Client Configuration

1. 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.
2. 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.

Installing the Client Software and Importing 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

1. 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**.

2. 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.

3. 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.

4. 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 pge.	*Set this parameter based on the site requirements.*

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

3.5 Step 4: Verifying Connectivity

Procedure

1. Open the CLI of the client device.

2. Run the **ping 192.168.1.10** command to test connectivity.

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

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
```


4 Classic VPN Purchase Process

4.1 Overview

The process of configuring Classic VPNs varies in different regions, as described in **Table 4-1**.

Table 4-1 Overview

Supported Regions	The supported regions are subject to those available on the console.	
VPN Creation	Perform the following steps in sequence: 1. **4.3 Buying a VPN Gateway** 2. **4.4 Buying a VPN Connection** 3. **4.5 Configuring the Remote Device**	Perform the following steps in sequence: 1. **Creating a VPN (LA-Mexico City1/LA-Sao Paulo1)** 2. **4.5 Configuring the Remote Device**

4.2 Buying a VPN (LA-Mexico City1/LA-Sao Paulo1)

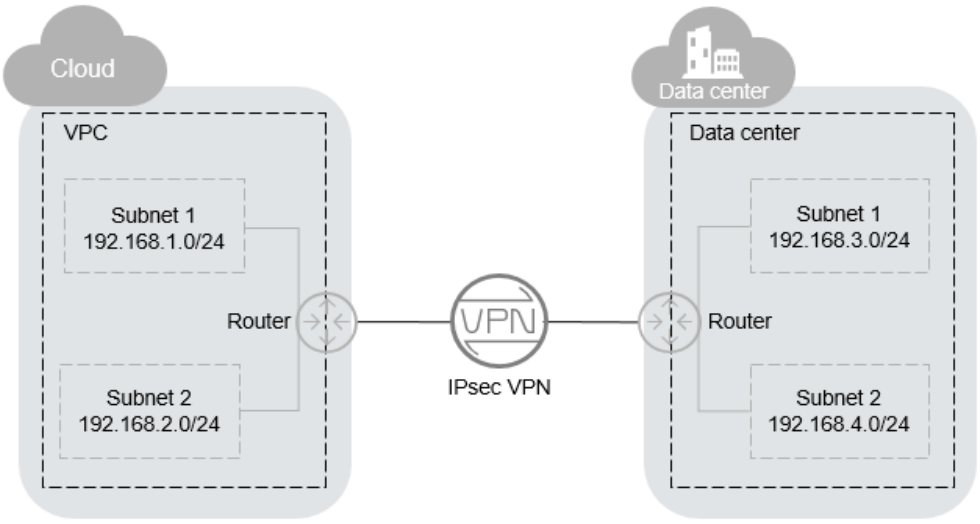
Overview

By default, ECSs in a VPC cannot communicate with devices in your on-premises data center or private network. To enable communication between them, you can use a VPN by creating it in your VPC and updating security group rules.

IPsec VPN Topology

In **Figure 4-1**, the VPC has subnets 192.168.1.0/24 and 192.168.2.0/24. Your on-premises data center has subnets 192.168.3.0/24 and 192.168.4.0/24. You can use VPN to enable subnets in the VPC to communicate with those in your data center.

Figure 4-1 IPsec VPN



Site-to-site VPN is supported to enable communication between VPC subnets and on-premises data center subnets. Before establishing an IPsec VPN, ensure that the on-premises data center where the VPN is to be established meets the following conditions:

- On-premises devices that support the standard IPsec protocol are available.
- The on-premises devices have fixed public IP addresses, which can be statically configured or translated by NAT.
- The on-premises subnets do not conflict with VPC subnets, and devices in the on-premises subnets can communicate with the on-premises devices.

If the preceding conditions are met, ensure that the IKE policies and IPsec policies at both ends are consistent and the subnets at both ends are matched pairs when configuring IPsec VPN.

After the configuration is complete, VPN negotiation needs to be triggered by private network data flows.

Scenarios

You need a VPN that sets up a secure, isolated communications tunnel between your on-premises data center and cloud services.

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

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
5. On the **Virtual Private Network** page, click **Buy VPN**.

   If Enterprise Edition VPN is available for the selected region, click **Buy VPN** on the **Classic** page.
6. Configure required parameters and click **Next**.

   Table 4-2, **Table 4-3**, and **Table 4-4** describe the parameters.

Table 4-2 Basic parameters

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	AP-Singapore
Billing Mode	VPNs are billed on a pay-per-use basis.	Pay-per-use
Name	The VPN name	VPN-001
VPC	The VPC name	VPC-001
Local Subnet	VPC subnets that will access your on-premises network through a VPN.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC.	N/A

Parameter	Description	Example Value
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnets cannot overlap with CIDR blocks involved in existing VPC peering connections created for the VPC.	192.168.3.0/24, 192.168.4.0/24
PSK	Private key shared by two ends of a VPN connection for negotiation. PSKs configured at both ends of the VPN connection must be the same. The PSK can contain 6 to 128 characters.	Test@123
Confirm PSK	Enter the PSK again.	Test@123
Advanced Settings	• **Default**: Use default IKE and IPsec policies. • **Custom**: Use custom IKE and IPsec policies. For details, see **Table 4-3** and **Table 4-4**.	Custom

Table 4-3 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default value is **SHA2-256**.	SHA2-256

Parameter	Description	Example Value
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported: • Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 The default value is **Group 14**.	Group 14
Version	Version of the IKE protocol. The value can be one of the following: • v1 (not recommended due to security risks) • v2 The default value is **v2**.	v2
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **86400**.	86400

Parameter	Description	Example Value
Negotiation Mode	This parameter is available only when **Version** is set to **v1**. You can set **Negotiation Mode** to **Main** or **Aggressive**. The default mode is **Main**.	Main

Table 4-4 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default value is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128

Parameter	Description	Example Value
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: • DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 The default value is **DH group 14**.	DH group 14
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • AH • AH-ESP • ESP The default protocol is **ESP**.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **3600**.	3600

NOTE

An IKE policy specifies the encryption and authentication algorithms to be used in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to be used in the data transmission phase of an IPsec tunnel. The IKE and IPsec policies must be the same at both ends of a VPN connection. If they are different, the VPN connection cannot be set up.

The following algorithms are not recommended because they are not secure enough:

- Authentication algorithms: SHA1 and MD5
- Encryption algorithm: 3DES
- DH algorithms: Group 1, Group 2, and Group 5

7. Submit your application.

   After the IPsec VPN is created, a public IP address is assigned to the VPN. The IP address is the local gateway address of the created VPN. When configuring the remote tunnel in your data center, you must set the remote gateway address to this IP address.

8. You need to configure an IPsec VPN tunnel on the router or firewall in your on-premises data center.

4.3 Buying a VPN Gateway

Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, buy a VPN gateway first. If you choose to buy a pay-per-use VPN gateway, a VPN connection will be created together with the 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

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.

5. On the **VPN Gateways** page, click **Buy VPN Gateway**.
6. Configure parameters based on **Table 4-5** and click **Buy Now**.

Table 4-5 Description of VPN gateway parameters

Parameter	Description	Example Value
Billing Mode	Billing mode of a VPN gateway, which can be pay-per-use **Pay-per-use**: When you buy a pay-per-use VPN gateway, you must buy a VPN connection together with the VPN gateway. **Yearly/Monthly**: When you buy a yearly/monthly VPN gateway, the price includes the gateway bandwidth fee and the fee of the VPN connections that can be created for the gateway.	Pay-per-use
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	AP-Singapore
Name	Name of a VPN gateway.	vpngw-001
VPC	Name of the VPC to which the VPN gateway connects.	vpc-001
Type	VPN type. **IPsec** is selected by default.	IPsec
Billed By	A pay-per-use VPN gateway can be billed by bandwidth or by traffic. • **Bandwidth**: You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth. • **Traffic**: You need to specify a bandwidth limit and pay for the traffic you generate.	Traffic

Parameter	Description	Example Value
Bandwidth (Mbit/s)	The bandwidth of the VPN gateway. The bandwidth is shared by all VPN connections created for the VPN gateway. The total bandwidth size used by all VPN connections created for a VPN gateway cannot exceed the VPN gateway bandwidth size. During the use of VPN, if the network traffic exceeds the VPN gateway bandwidth, network congestion may occur and VPN connections may be interrupted. As such, ensure that you configure enough bandwidth. You can configure alarm rules on Cloud Eye to monitor the bandwidth.	10

NOTE

When you buy a pay-per-use VPN gateway, you also need to configure a VPN connection that will be created together with the gateway (excepting the **CN South-Shenzhen** region). For details, see **Table 4-6**.

Table 4-6 Description of VPN connection parameters

Parameter	Description	Example Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created.	vpcgw-001
Local Subnet	VPC subnets that will access your on-premises network through a VPN. You can set the local subnet using either of the following methods: • **Select subnet**: Select the subnets that need to access your on-premises data center or private network. • **Specify CIDR block**: Enter the CIDR blocks that need to access your on-premises data center or private network. **NOTE** CIDR blocks of local subnets cannot overlap.	192.168.1.0/24, 192.168.2.0/24

Parameter	Description	Example Value
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC.	N/A
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnet cannot overlap with CIDR blocks involved in existing VPC peering, Direct Connect, or Cloud Connect connections created for the local VPC. **NOTE** CIDR blocks of remote subnets cannot overlap.	192.168.3.0/24, 192.168.4.0/24
PSK	PSKs configured at both ends of a VPN connection must be the same. The PSK: • Contains 6 to 128 characters. • Can contain only: – Digits – Letters – Special characters: ~ ` ! @ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Enter the PSK again.	Test@123
Advanced Settings	• **Default**: Use default IKE and IPsec policies. • **Custom**: Use custom IKE and IPsec policies. For details about the policies, see **Table 4-7** and **Table 4-8**.	Custom

Table 4-7 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported: • Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 The default value is **Group 14**. DH algorithms configured at both ends of a VPN connection must be the same. Otherwise, the negotiation will fail.	Group 14

Parameter	Description	Example Value
Version	Version of the IKE protocol. The value can be one of the following: • v1 (not recommended due to security risks) • v2 The default value is **v2**.	v2
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **86400**.	86400

Table 4-8 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128

Parameter	Description	Example Value
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: • DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 The default algorithm is **DH group 14**.	DH group 14
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • ESP • AH • AH-ESP The default protocol is **ESP**.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **3600**.	3600

CAUTION

The following algorithms are not recommended because they are not secure enough:

Authentication algorithms: SHA1 and MD5

Encryption algorithm: 3DES

DH algorithms: Group 1, Group 2, and Group 5

7. Confirm the VPN gateway information and click **Buy Now**.

   After a VPN gateway is created, the system automatically assigns a public IP address, that is, the IP address displayed in the **Gateway IP Address** column in the VPN gateway list. The gateway IP address is also the remote gateway IP address configured on the on-premises VPN network.

4.4 Buying a VPN Connection

Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a VPN connection after a VPN gateway is obtained.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
5. On the **VPN Connections** page, click **Buy VPN Connection**.
6. Configure the parameters as prompted and click **Pay Now**. **Table 4-9** lists the VPN connection parameters.

Table 4-9 Description of VPN connection parameters

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	CN North-Beijing4
Name	Name of a VPN connection.	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created.	vpcgw-001

Parameter	Description	Example Value
Local Subnet	VPC subnets that will access your on-premises network through a VPN. You can set the local subnet using either of the following methods: • **Select subnet**: Select the subnets that need to access your on-premises data center or private network. • **Specify CIDR block**: Enter the CIDR blocks that need to access your on-premises data center or private network. **NOTE** CIDR blocks of local subnets cannot overlap.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC.	N/A
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnet cannot overlap with CIDR blocks involved in existing VPC peering, Direct Connect, or Cloud Connect connections created for the local VPC. **NOTE** CIDR blocks of remote subnets cannot overlap.	192.168.3.0/24, 192.168.4.0/24
PSK	Private key shared by two ends of a VPN connection for negotiation. PSKs configured at both ends of the VPN connection must be the same. The PSK: • Contains 6 to 128 characters. • Can contain only: – Digits – Letters – Special characters: ~ ` ! @ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Enter the PSK again.	Test@123

Parameter	Description	Example Value
Advanced Settings	• **Default**: Use default IKE and IPsec policies. • **Existing**: Use existing IKE and IPsec policies. • **Custom**: including **IKE Policy** and **IPsec Policy**, which specifies the encryption and authentication algorithms of a VPN tunnel. For details about the policies, see **Table 4-10** and **Table 4-11**.	Custom

Table 4-10 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128

Parameter	Description	Example Value
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported: • Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 The default algorithm is **Group 14**.	Group 14
Version	Version of the IKE protocol. The value can be one of the following: • v1 (not recommended due to security risks) • v2 The default value is **v2**.	v2
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **86400**.	86400

Table 4-11 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128

Parameter	Description	Example Value
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: • DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 The default algorithm is **DH group 14**.	DH group 14
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • AH • ESP • AH-ESP The default protocol is **ESP**.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **3600**.	3600

NOTE

An IKE policy specifies the encryption and authentication algorithms to be used in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to be used in the data transmission phase of an IPsec tunnel. The IKE and IPsec policies must be the same at both ends of a VPN connection. If they are different, the VPN connection cannot be set up.

The following algorithms are not recommended because they are not secure enough:

- Authentication algorithms: SHA1 and MD5
- Encryption algorithm: 3DES
- DH algorithms: Group 1, Group 2, and Group 5

7. Click **Submit**.
8. You need to configure an IPsec VPN tunnel on the router or firewall in your on-premises data center.

4.5 Configuring the Remote Device

For details about how to configure the remote device, see **Virtual Private Network Administrator Guide**. This guide helps you configure the local VPN device to implement the interconnection between your local network and a VPC subnet.

For details about the configuration examples, see the following:

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

