Virtual Private Network

Best Practices

Issue	01
Date	2025-02-05

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

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 S2C Enterprise Edition VPN

1.1 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active-Active Mode)

1.1.1 Overview

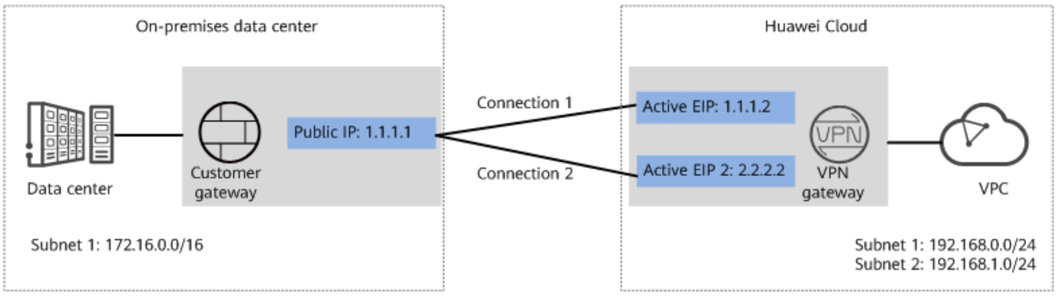
Scenario

VPN can be used to enable communication between an on-premises data center and ECSs in a VPC.

Networking

In this example, two VPN connections are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

Figure 1-1 Networking diagram



Solution Advantages

- A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.
- Active-active VPN gateways can be deployed in different AZs to ensure AZ-level high availability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

1.1.2 Planning Networks and Resources

Data Plan

Table 1-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	● 192.168.0.0/24 ● 192.168.1.0/24
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
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: ● Active EIP: 1.1.1.2 ● Active EIP 2: 2.2.2.2
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

Category	Item	Data
Customer gateway	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: 1.1.1.1
	Tunnel interface address	● VPN connection 1: 169.254.70.2/30 ● VPN connection 2: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	● Version: v2 ● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● DH algorithm: Group 15 ● Lifetime (s): 86400 ● Local ID: IP address ● Peer ID: IP address
	IPsec policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● PFS: DH Group15 ● Transfer protocol: ESP ● Lifetime (s): 3600

1.1.3 Procedure

Prerequisites

- Cloud side
  - 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**.
  - An enterprise router has been created if you want to use it to connect to a VPN gateway. For details, see the enterprise router documentation.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center. For details, see **Administrator Guide**.

Procedure

Huawei Cloud VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

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

   Table 1-2 only describes the key parameters for creating a VPN gateway.

Table 1-2 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**. If the VPN gateway is associated with an enterprise router, select **Enterprise Router**.	VPC
Enterprise Router	Specify the associated enterprise router only when **Associate With** is set to **Enterprise Router**.	er-001
VPC	VPC to which the interconnection subnet belongs. When **Associate With** is set to **Enterprise Router**, the associated enterprise router can be located in the VPC or not.	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	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24

Parameter	Description	Value
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active-active**.	Active-active
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure the customer gateway.

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

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

Table 1-3 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

Step 5 Configure VPN connections.

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

   Table 1-4 only describes the key parameters for creating a VPN connection.

Table 1-4 Parameter settings for VPN connection 1

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001

Parameter	Description	Value
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-fw
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

NOTE

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

Table 1-5 Parameter settings for VPN connection 2

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

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

Verification

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

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

1.2 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active/Standby Mode)

1.2.1 Overview

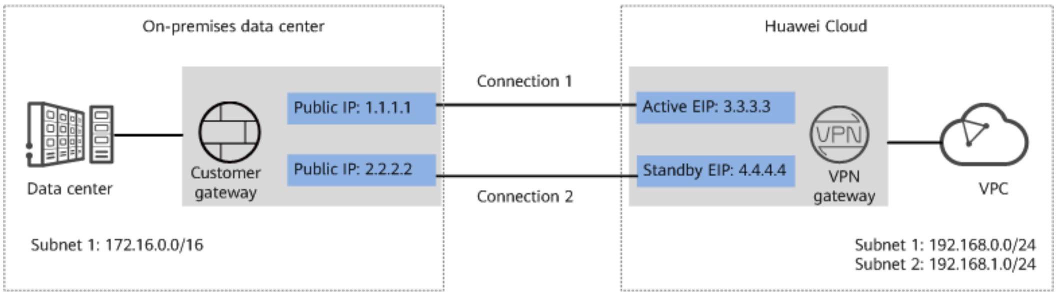
Scenario

VPN can be used to enable communication between an on-premises data center and ECSs in a VPC.

Networking

In this example, two VPN connections working in active/standby mode are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

Figure 1-2 Networking diagram



Solution Advantages

- A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.
- Active/Standby mode: A VPN gateway communicates with a customer gateway through the active connection. If the active connection fails, traffic is automatically switched to the standby VPN connection. After the fault is rectified, traffic is switched back to the original active VPN connection. Traffic leaving the cloud is preferentially transmitted through the active EIP, allowing you to determine the VPN connection through which traffic is transmitted.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

1.2.2 Planning Networks and Resources

Data Plan

Table 1-6 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	● 192.168.0.0/24 ● 192.168.1.0/24

Category	Item	Data
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/Standby
	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: 3.3.3.3 ● Standby EIP: 4.4.4.4
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	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: ● 1.1.1.1 ● 2.2.2.2
	Tunnel interface address	● VPN connection 1: 169.254.70.2/30 ● VPN connection 2: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	● Version: v2 ● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● DH algorithm: Group 15 ● Lifetime (s): 86400 ● Local ID: IP address ● Peer ID: IP address

Category	Item	Data
	IPsec policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● PFS: DH Group15 ● Transfer protocol: ESP ● Lifetime (s): 3600

1.2.3 Procedure

Prerequisites

- Cloud side
  - 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**.
  - An enterprise router has been created if you want to use it to connect to a VPN gateway. For details, see the enterprise router documentation.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center. For details, see **Administrator Guide**.

Procedure

Huawei Cloud VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

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

   Table 1-7 only describes the key parameters for creating a VPN gateway.

Table 1-7 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network

Parameter	Description	Value
Associate With	Select **VPC**. If the VPN gateway is associated with an enterprise router, select **Enterprise Router**.	VPC
Enterprise Router	Specify the associated enterprise router only when **Associate With** is set to **Enterprise Router**.	er-001
VPC	VPC to which the interconnection subnet belongs. When **Associate With** is set to **Enterprise Router**, the associated enterprise router can be located in the VPC or not.	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	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active/Standby**.	Active/Standby
Active EIP	Active EIP used by the VPN gateway to access the on-premises data center.	1.1.1.2
Standby EIP	Standby EIP used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure the customer gateway.

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

   Table 1-8 only describes the key parameters for creating a customer gateway.

Table 1-8 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

Step 5 Configure VPN connections.

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

   Table 1-9 only describes the key parameters for creating a VPN connection.

Table 1-9 Parameter settings for VPN connection 1

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-fw
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16

Parameter	Description	Value
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

NOTE

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

Table 1-10 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Standby EIP bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

Verification

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

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

1.3 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Access via Non-fixed IP Addresses)

1.3.1 Overview

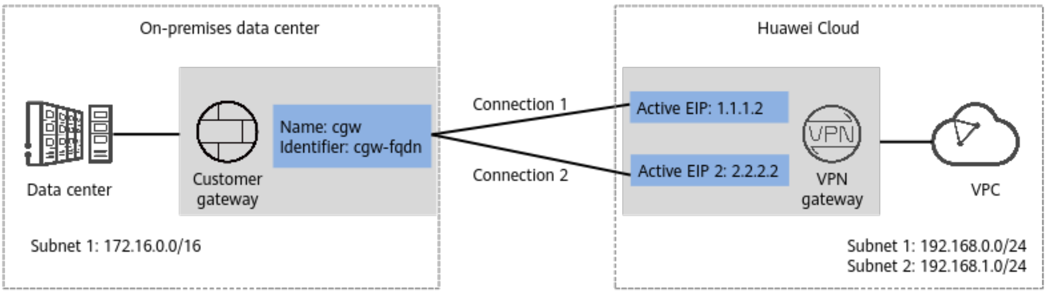
Scenario

When an on-premises data center needs to access ECSs in a VPC, non-fixed IP addresses on the customer network can be used for the access.

Networking

In this example, two VPN connections are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

Figure 1-3 Networking diagram



Solution Advantages

Non-fixed public IP addresses in the on-premises data center can be used for cloud access, making the networking flexible and reducing the bandwidth cost.

Notes and Constraints

- The on-premises data center supports VPN connections only in policy-based mode.
- The negotiation must be initiated by the on-premises data center.
- In non-fixed IP address access mode, only IKEv2 is supported. IKEv1 is not supported.

1.3.2 Planning Networks and Resources

Data Plan

Table 1-11 Data plan

Category	Item	Data
VPC	Subnets that need to access the on-premises data center	● 192.168.0.0/24 ● 192.168.1.0/24
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
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: ● Active EIP: 1.1.1.2 ● Active EIP 2: 2.2.2.2
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Identifier	cgw-fqdn (FQDN type)
Policy template	IKE policy	● Version: v2 ● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128-GCM-16 ● DH algorithm: Group 15 ● Lifetime (s): 86400 ● Local ID: IP address

Category	Item	Data
	IPsec policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128-GCM-16 ● PFS: DH Group15 ● Transfer protocol: ESP ● Lifetime (s): 3600

1.3.3 Procedure

Prerequisites

- Cloud side
  - 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**.
  - An enterprise router has been created if you want to use it to connect to a VPN gateway. For details, see the enterprise router documentation.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center. For details, see **Administrator Guide**.

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 Configure a VPN gateway.

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

   Table 1-12 only describes the key parameters for creating a VPN gateway.

Table 1-12 Description of VPN gateway parameters

Parameter	Description	Value
Billing Mode	Select **Yearly/Monthly**.	Yearly/Monthly
Name	Name of a VPN gateway.	vpngw-001

Parameter	Description	Value
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**. If the VPN gateway is associated with an enterprise router, select **Enterprise Router**.	VPC
Enterprise Router	Specify the associated enterprise router only when **Associate With** is set to **Enterprise Router**.	er-001
VPC	VPC to which the interconnection subnet belongs. When **Associate With** is set to **Enterprise Router**, the associated enterprise router can be located in the VPC or not.	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	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24
Specification	Select **Professional 1** and **Access via a non-fixed IP address**.	Professional 1: non-fixed IP address
HA Mode	Select **Active-active**.	Active-active
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure a customer gateway.

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

   Table 1-13 only describes the key parameters for creating a customer gateway.

   Table 1-13 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw
Identifier	Select **FQDN** and enter the customer gateway identifier.	FQDN cgw-fqdn

Step 5 Configure VPN connections.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections** and click **Buy VPN Connection**.
2. Set parameters for VPN connection 1 and click **Submit**.

   Table 1-14 only describes the key parameters for creating a VPN connection.

   Table 1-14 Parameter settings for VPN connection 1

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

Parameter	Description	Value
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Template	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

NOTE

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

Table 1-15 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

Verification

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

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

1.4 Connecting Multiple On-premises Branch Networks Through a VPN Hub

1.4.1 Overview

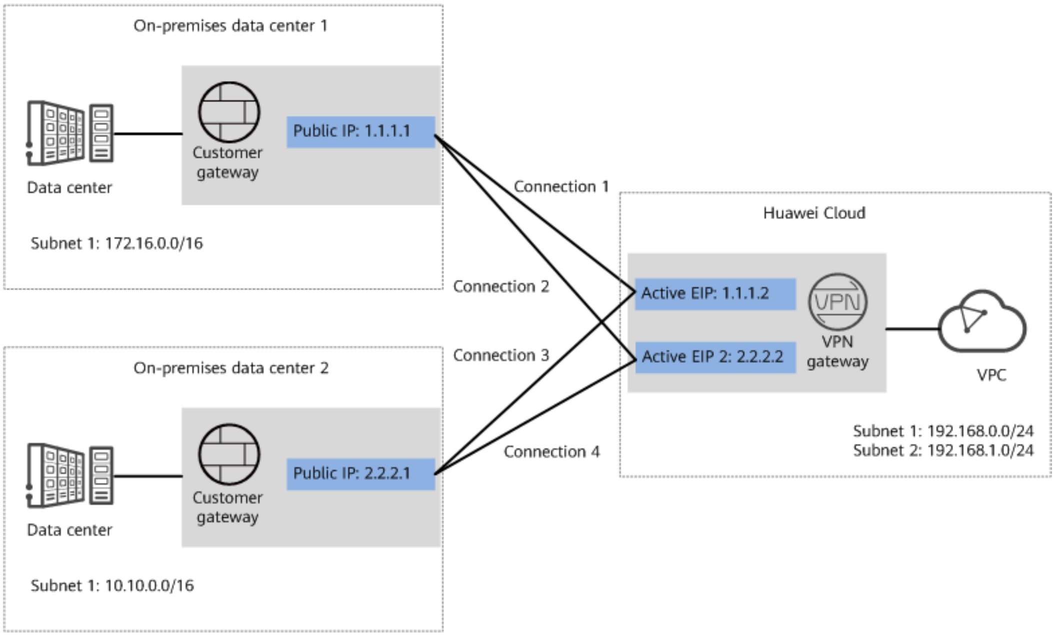
Scenario

To meet service requirements, enterprise A needs to implement communication between its two on-premises data centers.

Networking

Figure 1-4 shows the networking where the VPN service is used to connect the two on-premises data centers.

Figure 1-4 Networking diagram



Solution Advantages

- A VPN gateway on the cloud can function as a VPN hub to enable communication between on-premises branch sites. This eliminates the need to configure VPN connections between every two sites.
- A VPN gateway provides two IP addresses to establish dual independent VPN connections with each customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection, ensuring reliability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

1.4.2 Planning Networks and Resources

Data Plan

Table 1-16 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data centers	● 192.168.0.0/24 ● 192.168.1.0/24
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
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: ● Active EIP: 1.1.1.2 ● Active EIP 2: 2.2.2.2
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 connections set up with on-premises data center 1 – VPN connection 1: 169.254.70.1/30 – VPN connection 2: 169.254.71.1/30 ● VPN connections set up with on-premises data center 2 – VPN connection 3: 169.254.72.1/30 – VPN connection 4: 169.254.73.1/30
On-premises data center 1	Subnet that needs to access the VPC	172.16.0.0/16

Category	Item	Data
Customer gateway in on-premises data center 1	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: 1.1.1.1
	Tunnel interface address	● VPN connection 1: 169.254.70.2/30 ● VPN connection 2: 169.254.71.2/30
On-premises data center 2	Subnet that needs to access the VPC	10.10.0.0/16
Customer gateway in on-premises data center 2	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: 2.2.2.1
	Tunnel interface address	● VPN connection 3: 169.254.72.2/30 ● VPN connection 4: 169.254.73.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● DH algorithm: Group 15 ● Version: v2 ● Lifetime (s): 86400 ● Local ID: IP address ● Peer ID: IP address
	IPsec policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● PFS: DH Group15 ● Transfer protocol: ESP ● Lifetime (s): 3600

1.4.3 Procedure

Prerequisites

- Cloud side
  - 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**.

- Data center side
  - IPsec has been configured on the VPN devices in the two on-premises data centers. For details, see **Administrator Guide**.
  - The remote subnets of the VPN device in on-premises data center 1 must contain the local subnet of the Huawei Cloud VPC and the subnet to be interconnected in on-premises data center 2. The remote subnets of the VPN device in on-premises data center 2 must contain the local subnet of the Huawei Cloud VPC and the subnet to be interconnected in on-premises data center 1.

Procedure

Huawei Cloud VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Configure a VPN gateway.

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

   Table 1-17 only describes the key parameters for creating a VPN gateway.

Table 1-17 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**. If the VPN gateway is associated with an enterprise router, select **Enterprise Router**.	VPC
VPC	Huawei Cloud VPC that the on-premises data centers need to access.	vpc-001(192.168.0.0/16)
Local Subnet	VPC subnets that the on-premises data centers need to access.	192.168.0.0/24,192.168.1.0/24
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
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active-active**.	Active-active

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

Step 2 Configure customer gateways.

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

   Table 1-18 only describes the key parameters for creating a customer gateway.

   Table 1-18 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw1
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway in on-premises data center 1 to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

3. Repeat the preceding operations to configure the customer gateway (2.2.2.1) in on-premises data center 2.

Step 3 Configure VPN connections between the cloud side and on-premises data center 1.

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

   Table 1-19 only describes the key parameters for creating a VPN connection.

   Table 1-19 Description of VPN connection parameters

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001

Parameter	Description	Value
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
VPN Type	Select **Static routing**.	Static routing
Customer Gateway	Name of a customer gateway.	cgw-fw1
Customer Subnet	Subnet in on-premises data center 1 that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

NOTE

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

Table 1-20 Parameter settings for VPN connection 2

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

Step 4 Configure VPN connections between the cloud side and on-premises data center 2.

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

   Table 1-21 only describes the key parameters for creating a VPN connection.

Table 1-21 Description of VPN connection parameters

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-003
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-fw2
VPN Type	Select **Static routing**.	Static routing

Parameter	Description	Value
Customer Subnet	Subnet in on-premises data center 2 that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	10.10.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.72.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.72.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device in on-premises data center 2.	Test@123
Policy Settings	The policy settings must be the same as those configured on the customer gateway device in on-premises data center 2.	Default

3. Create VPN connection 2.

NOTE

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

Table 1-22 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-004
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.73.1
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway in on-premises data center 2.	169.254.73.2

Step 5 Configure customer gateway devices in on-premises data centers 1 and 2.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

Verification

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

  Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the four VPN connections are all **Normal**.
- Verify that servers in on-premises data center 1 and servers in on-premises data center 2 can ping each other.

1.5 Allowing Direct Connect and VPN to Work in Active and Standby Mode to Link Data Center to Cloud

1.5.1 Overview

Application Scenarios

Direct Connect establishes a dedicated, secure, and stable network connection between your on-premises data center and VPC. It can work together with an enterprise router to build a large-scale hybrid cloud network.

VPN establishes a secure, encrypted communication tunnel between your data center and your VPC. Compared with Direct Connect, VPN is cost-effective and can be quickly deployed.

To achieve high reliability of hybrid cloud networking and control costs, you can attach both Direct Connect and VPN connections to an enterprise router to enable the connections to work in an active and standby way. If the active connection is faulty, services are automatically switched to the standby one, reducing the risk of service interruptions.

NOTE

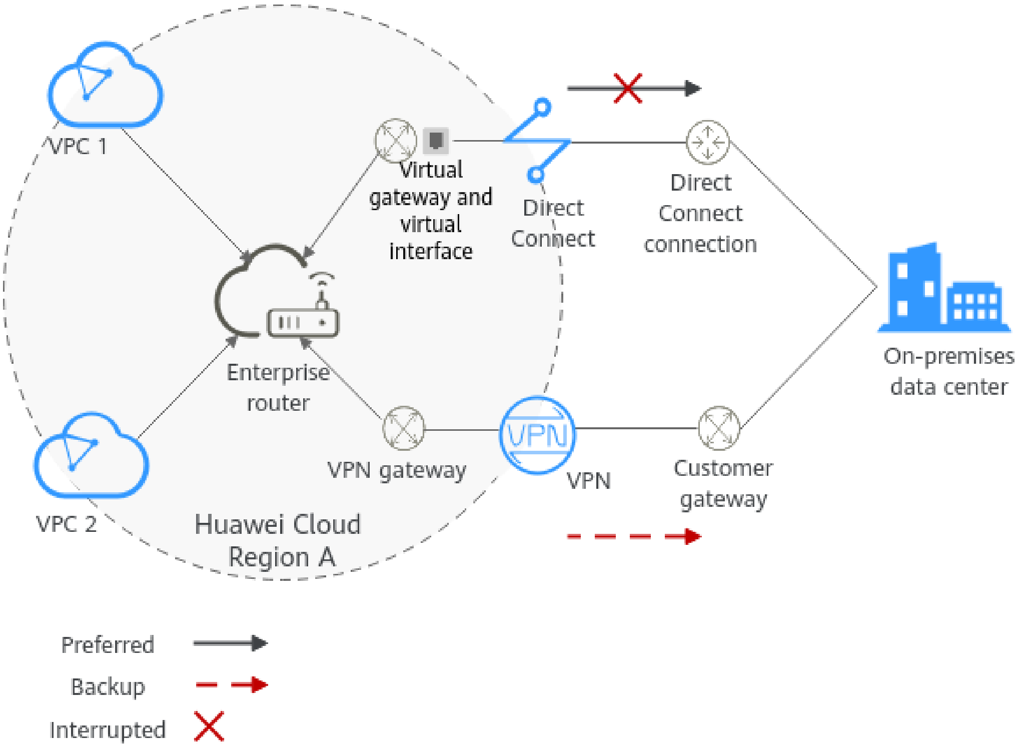
For more information about enterprise routers, see **Enterprise Router Overview**.

Architecture

To improve the reliability of a hybrid cloud networking, an enterprise uses both Direct Connect and VPN connections to connect VPCs to the on-premises data center. The Direct Connect connection works as the active connection and the VPN connection works as the standby one. If the active connection is faulty, services are automatically switched to the standby one, reducing the impact of network interruptions on services.

- VPC 1, VPC 2, and the Direct Connect connection are attached to the enterprise router. VPC1 and VPC 2 can communicate with each other. They communicate with the on-premises data center through the Direct Connect connection.
- The VPN connection is also attached to the enterprise router. If the Direct Connect connection is faulty, VPC 1 and VPC 2 can communicate with the data center through the VPN connection.

Figure 1-5 Network diagram of Direct Connect and VPN connections working in active/standby mode



Advantages

An enterprise router allows automatic switchover between active and standby Direct Connect and VPN connections. You do not need to manually switch between them. This prevents service loss and reduces maintenance costs.

Notes and Constraints

The subnet CIDR blocks of VPCs and the data center cannot overlap.

1.5.2 Planning Networks and Resources

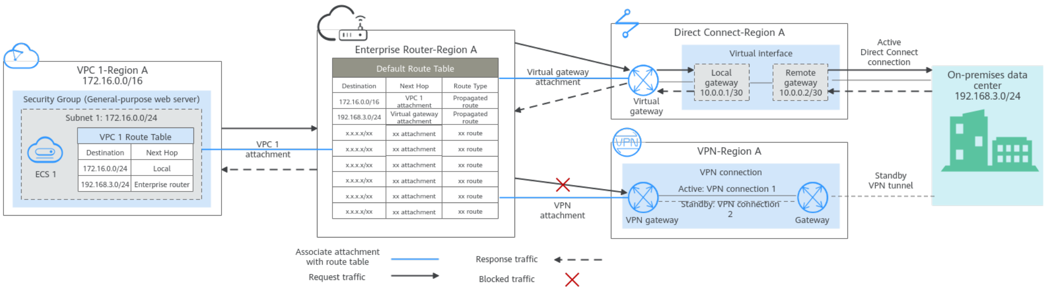
To attach both Direct Connect and VPN connections to an enterprise router to allow them to work in active/standby mode, you need to:

- **Network Planning**: plan CIDR blocks of VPCs and their subnets, Direct Connect connection, VPN connection, enterprise router, and routes.
- **Resource Planning**: plan the quantity, names, and parameters of cloud resources, including VPCs, Direct Connect connection, VPN connection, and enterprise router.

Network Planning

Figure 1-6 shows the network diagram of Direct Connect and VPN connections that work in the active/standby mode. **Table 1-24** describes the network planning.

Figure 1-6 Network diagram of Direct Connect and VPN connections working in active/standby mode



VPC 1 Route Table

Destination	Next Hop
172.16.0.0/24	Local
192.168.3.0/24	Enterprise router

Default Route Table

Destination	Next Hop	Route Type
172.16.0.0/16	VPC 1 attachment	Propagated route
192.168.3.0/24	Virtual gateway attachment	Propagated route
x.x.x.x/xx	xx attachment	xx route
x.x.x.x/xx	xx attachment	xx route
x.x.x.x/xx	xx attachment	xx route
x.x.x.x/xx	xx attachment	xx route
x.x.x.x/xx	xx attachment	xx route
x.x.x.x/xx	xx attachment	xx route

Direct Connect and VPN connections work in the active/standby mode. If the Direct Connect connection is normal, it is preferentially selected for traffic forwarding.

- Only preferred routes are displayed in the enterprise router route table. The routes of a virtual gateway attachment have a higher priority than those of a VPN gateway attachment. Therefore, routes of the VPN gateway attachment will not be displayed in the route table.
- By default, the Direct Connect connection is used for communications between the VPCs and the data center. **Table 1-23** shows the details about the traffic flows in this example.

Table 1-23 Network traffic flows

Path	Description
Request from VPC 1 to the on-premises data center	1. The route table of VPC 1 has routes with next hop set to the enterprise router to forward traffic from VPC 1 to the enterprise router. 2. The route table of the enterprise router has a route with next hop set to virtual gateway attachment to forward traffic from the enterprise router to the virtual gateway. 3. The virtual gateway is connected to the virtual interface. Traffic from the virtual gateway is forwarded to the physical connection through the remote gateway of the virtual interface. 4. Traffic is sent to the on-premises data center over the connection.
Response from the on-premises data center to VPC 1	1. Traffic is forwarded to the virtual interface through the connection. 2. The virtual interface is connected to the virtual gateway. Traffic from the virtual interface is forwarded to the virtual gateway through the local gateway of the virtual interface. 3. Traffic is forwarded from the virtual gateway to the enterprise router. 4. The route table of the enterprise router has a route with next hop set to VPC 1 attachment to forward traffic from the enterprise router to VPC 1.

Table 1-24 Description of network planning for Direct Connect and VPN connections that work in active/standby mode

Resource	Description
VPC	VPC 1 (Service VPC) that your services are deployed: ● The CIDR blocks of the VPC and the data center cannot overlap. ● The VPC has a default route table. ● Routes in the default route table: – Local: a system route for communications between subnets in a VPC. – Enterprise router: traffic from a VPC subnet can be forwarded to the enterprise router. The destination is set to the subnet CIDR block of the data center. **Table 1-25** shows the route.

Resource	Description
	A VPC that has a subnet used by the VPN gateway. When you create the VPN gateway, you need to enter the subnet CIDR block. The subnet used by the VPN gateway cannot overlap with existing subnets in the VPC.
Direct Connect	● One physical connection that you lease from a carrier to link your on-premises data center to the cloud. ● One virtual gateway that is attached to the enterprise router. ● One virtual interface that connects the virtual gateway with the connection.
VPN	● One VPN gateway that is attached to the enterprise router. ● One customer gateway that is the gateway of the on-premises data center. ● Two VPN connections that connect the VPN gateway and the customer gateway and work in active/standby mode.
Enterprise router	After **Default Route Table Association** and **Default Route Table Propagation** are enabled and an attachment is created, the system will automatically: ● VPC: – Associate the VPC attachment with the default route table of the enterprise router. – Propagate the VPC attachment to the default route table of the enterprise router. The route table automatically learns the VPC CIDR block as the destination of a route. For details, see **Table 1-26**. ● Direct Connect – Associate the virtual gateway attachment with the default route table of the enterprise router. – Propagate the virtual gateway attachment to the default route table of the enterprise router. The route table automatically learns the route information of the virtual gateway attachment. For details, see **Table 1-26**. ● VPN – Associate the VPN gateway attachment with the default route table of the enterprise router. – Propagate the VPN gateway attachment to the default route table of the enterprise router. The route table automatically learns the route information of the VPN gateway attachment. For details, see **Table 1-26**.

Resource	Description
ECS	One ECS in the service VPC. The ECS is used to verify communications between the cloud and the on-premises data center. If you have multiple ECSs associated with different security groups, you need to add rules to the security groups to allow network access.

Table 1-25 VPC route table

Destination	Next Hop	Route Type
192.168.3.0/24	Enterprise router	Static route (custom)

NOTE

- If you enable **Auto Add Routes** when creating a VPC attachment, you do not need to manually add static routes to the VPC route table. Instead, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.
- If an existing route in the VPC route tables has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the routes will fail to be added. In this case, you are advised not to enable **Auto Add Routes**. After the attachment is created, manually add routes.
- You need to add a route to the VPC route table with destination set to the CIDR block of the on-premises data center and next hop set to enterprise router.

Table 1-26 Enterprise router route table

Destination	Next Hop	Route Type
VPC 1 CIDR block: 172.16.0.0/16	VPC 1 attachment: er-attach-01	Propagated route
Data center CIDR block: 192.168.3.0/24	Virtual gateway attachment: vgw-demo	Propagated route
Data center CIDR block: 192.168.3.0/24	VPN gateway attachment: vpngw-demo	Propagated route

NOTICE

- Only preferred routes are displayed in the enterprise router route table. If both the Direct Connect and VPN connections are working normally, the routes of the virtual gateway attachment take priority and can be viewed in the enterprise router route table. Routes (including routes that are not preferred) of the VPN gateway attachment cannot be viewed.
- If the Direct Connect connection is faulty and services are switched to the VPN connection, you can view the propagated routes of the VPN gateway attachment in the enterprise router route table on the management console.

Resource Planning

An enterprise router, a Direct Connect connection, VPN resources, two VPCs, and an ECS are in the same region but they can be in different AZs.

NOTE

The following resource details are only examples. You can modify them as required.

Table 1-27 Details of required resources

Resource	Quantity	Description
VPC	2	Service VPC that your services are deployed and needs to be attached to the enterprise router ● VPC name: Set it based on site requirements. In this example, **vpc-for-er** is used. ● VPC IPv4 CIDR block: The CIDR block must be different from that of the data center. Set it based on site requirements. In this example, **172.16.0.0/16** is used. ● Subnet name: Set it based on site requirements. In this example, **subnet-for-er** is used. ● Subnet IPv4 CIDR block: The CIDR block must be different from that of the data center. Set it based on site requirements. In this example, **172.16.0.0/24** is used.

Resource	Quantity	Description
		A VPC that has a subnet used by the VPN gateway. ● VPC name: Set it based on site requirements. In this example, **vpc-for-vpn** is used. ● VPC IPv4 CIDR block: Set it based on site requirements. In this example, **10.0.0.0/16** is used. ● Subnet name: A default subnet is created together with a VPC. Set it based on site requirements. In this example, **subnet-01** is used. ● Subnet IPv4 CIDR block: The default subnet is not used in this example. Set it based on site requirements. In this example, **10.0.0.0/24** is used. **NOTICE** When creating a VPN gateway, you need to set **VPC** to this VPC and **Interconnection Subnet** to a subnet of this VPC. Ensure that the configured interconnection subnet has four or more assignable IP addresses.
Enterprise router	1	● **Name**: Set it based on site requirements. In this example, **er-test-01** is used. ● **ASN**: The ASN must be different from that of the data center. In this example, retain the default value **64512**. ● **Default Route Table Association**: Select **Enable**. ● **Default Route Table Propagation**: Select **Enable**. ● **Auto Accept Shared Attachments**: Set it based on site requirements. In this example, **Enable** is selected. ● Three attachments on the enterprise router: – VPC attachment: er-attach-VPC – Virtual gateway attachment: er-attach-VGW – VPN gateway attachment: er-attach-VPN
Direct Connect	1	Connection: Create one based on site requirements.
		Virtual gateway ● **Name**: Set it based on site requirements. In this example, **vgw-demo** is used. ● **Attachment**: Select **Enterprise Router**. ● **Enterprise Router**: Select your enterprise router. In this example, the router is **er-test-01**. ● **BGP ASN**: The ASN can be the same as or different from that of the enterprise router. In this example, retain the default value **64512**.

Resource	Quantity	Description
		Virtual interface ● **Name**: Set it based on site requirements. In this example, **vif-demo** is used. ● **Virtual Gateway**: Select your virtual gateway. In this example, the virtual gateway is **vgw-demo**. ● **Local Gateway**: Set it based on site requirements. In this example, **10.0.0.1/30** is used. ● **Remote Gateway**: Set it based on site requirements. In this example, **10.0.0.2/30** is used. ● **Remote Subnet**: Set it based on site requirements. In this example, **192.168.3.0/24** is used. ● **Routing Mode**: Select **BGP**. ● **BGP ASN**: ASN of the data center, which must be different from the ASN of the virtual gateway on the cloud. In this example, **65525** is used.
VPN	1	VPN gateway ● **Name**: Set it based on site requirements. In this example, **vpngw-demo** is used. ● **Associate With**: Select **Enterprise Router**. ● **Enterprise Router**: Select your enterprise router. In this example, the router is **er-test-01**. ● **BGP ASN**: The ASN must be the same as that of the virtual gateway because the Direct Connect and VPN connections back up each other. In this example, **64512** is used. ● **VPC**: Select your VPC. In this example, select **vpc-for-vpn**. ● **Interconnection Subnet**: Specify the subnet used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. Set this parameter based on the site requirements. In this example, the value is **10.0.5.0/24**.
		Customer gateway ● **Name**: Set it based on site requirements. In this example, **cgw-demo** is used. ● **Routing Mode**: Select **Dynamic (BGP)**. ● **BGP ASN**: ASN of the data center. The ASN must be the same as that of the virtual gateway because the Direct Connect and VPN connections back up each other. In this example, 65525 is used.

Resource	Quantity	Description
		Two VPN connections that work in active/standby mode: ● **Name**: Set it based on site requirements. In this example, the active VPN connection is **vpn-demo-01**, and the standby VPN connection is **vpn-demo-02**. ● **VPN Gateway**: Select your VPN gateway. In this example, the VPN gateway is **vpngw-demo**. ● **EIP**: Set it based on site requirements. Select the active EIP for the active VPN connection and the standby EIP for the standby VPN connection. ● **VPN Type**: Select **Route-based**. ● **Customer Gateway**: Select your customer gateway. In this example, the customer gateway is **cgw-demo**. ● **Interface IP Address Assignment**: In this example, **Automatically assign** is selected. ● **Routing Mode**: Select **Dynamic (BGP)**.
ECS	1	● **ECS Name**: Set it based on site requirements. In this example, **ecs-demo** is used. ● **Image**: Select an image based on site requirements. In this example, a public image (CentOS 8.2 64bit) is used. ● **Network** – VPC: Select your VPC. In this example, select **vpc-for-er**. – Subnet: Select a subnet. In this example, select **subnet-for-er**. ● **Security Group**: Select a security group based on site requirements. In this example, the security group uses a general-purpose web server template and its name is **sg-demo**. ● Private IP address: 172.16.1.137

NOTICE

- The virtual gateway and the VPN gateway must use the same ASN to prevent network loops because the Direct Connect and VPN connections back up each other. In this example, **64512** is used.
- The ASN of the enterprise router can be the same as or different from that of the virtual gateway and the VPN gateway. In this example, **64512** is used.
- The ASN of the data center must be different from that of the cloud. Set this ASN of the data center based on site requirements. In this example, **65525** is used.

1.5.3 Construction Process

Table 1-28 describes the overall process of constructing the hybrid cloud network using Direct Connect and VPN connections that work in the active/standby mode and an enterprise router.

Table 1-28 Process description of constructing the hybrid cloud network

Procedure	Description
Step 1: Create Cloud Resources	1. Create one enterprise router for connecting VPCs in the same region. 2. Create a service VPC with a subnet. 3. Create an ECS in the service VPC subnet.
Step 2: Create a Virtual Gateway Attachment to the Enterprise Router	1. Create a Direct Connect connection to connect the on-premises data center to the Huawei Cloud over a line leased from a carrier. 2. Create a virtual gateway and attach it to the enterprise router. 3. Create a virtual interface to associate the virtual gateway with the Direct Connect connection. 4. Configure routes on the router of the on-premises data center.
Step 3: Create a VPC Attachment to the Enterprise Router	1. Attach the service VPC to the enterprise router. 2. Add a route with the enterprise router as the next hop and the CIDR block of the data center as the destination to the VPC route table.
Step 4: Verify the Network Connectivity Over the Direct Connect Connection	Log in to the ECS and run the **ping** command to verify the network connectivity through the Direct Connect connection.
Step 5: Create a VPN Attachment to the Enterprise Router	1. Create a VPN gateway and attach it to the enterprise router. 2. Create a customer gateway, that is the gateway of the data center. 3. Create two VPN connections that connect the VPN gateway and the customer gateway and work in active/standby mode. 4. Configure routes on the router of the on-premises data center.

Procedure	Description
Step 6: Verify the Network Connectivity Over the VPN Connection	Log in to the ECS and run the **ping** command to verify the network connectivity through the VPN connections. A VPN connection is a standby one. If you need to verify the network connectivity through a VPN connection, you need to simulate a fault on the active connection, that is the Direct Connect connection.

1.5.4 Construction Procedure

Step 1: Create Cloud Resources

The following describes how to create an enterprise router, service VPC, and ECS. For details about these cloud resources, see **Table 1-27**.

Step 1 Create an enterprise router.

For details, see **Creating an Enterprise Router**.

Step 2 Create a service VPC.

For details, see **Creating a VPC and Subnet**.

Step 3 Create an ECS.

In this example, the ECS is used to verify the communication between the VPC and the data center. The ECS quantity and configuration are for reference only.

For details, see **Purchasing a Custom ECS**.

----End

Step 2: Create a Virtual Gateway Attachment to the Enterprise Router

For details about Direct Connect resources, see **Table 1-27**.

Step 1 Create a connection.

For details, see **Creating a Connection**.

Step 2 Create a virtual gateway and attach it to the enterprise router.

1. On the Direct Connect console, create a virtual gateway.

   For details, see **Step 2: Create a Virtual Gateway**.

2. On the enterprise router console, check whether the virtual gateway attachment has been added to the enterprise router.

   For details, see **Viewing an Attachment**.

   If the status of the virtual gateway attachment is **Normal**, the attachment has been added.

   Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. Therefore, after you add the virtual gateway attachment to the enterprise router, the system will automatically:

- Associate the virtual gateway attachment with the default route table of the enterprise router.
- Propagate the virtual gateway attachment to the default route table of the enterprise router. The routes to the on-premises data center are propagated to the route table.

  You can view routes to the data center in the route table of the enterprise router only after performing the following steps.

Step 3 Create a virtual interface.

Create a virtual interface to connect the virtual gateway with the on-premises data center. For details, see **Step 3: Create a Virtual Interface**.

Step 4 Configure routes on the on-premises network device.

The Direct Connect and VPN connections back up each other. Therefore, pay attention to the following when configuring routes:

- The routing mode of the Direct Connect and VPN connections must be the same. In this example, BGP routing is used.
- The route preference of the Direct Connect connection must be higher than that of the VPN connection.
- The amount of time that the disconnection of Direct Connect and VPN connections is detected should be the same as that of the cloud network.

----End

Step 3: Create a VPC Attachment to the Enterprise Router

Step 1 Attach the service VPC to the enterprise router.

When creating the VPC attachment, do not enable **Auto Add Routes**.

NOTICE

If this function is enabled, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC. In this example, you need to add a route to the VPC route table with destination set to the CIDR block of the on-premises data center and next hop set to enterprise router.

For details, see **Creating VPC Attachments for the Enterprise Router**.

Step 2 Check the route with destination set to the VPC CIDR block in the enterprise router route table.

In this example, **Default Route Table Association** and **Default Route Table Propagation** are enabled for the enterprise router, and the system automatically adds routes pointing to VPC CIDR blocks when you attach the VPCs to the enterprise router.

For details about the routes of the enterprise router, see **Table 1-24** and **Table 1-26**.

To view routes of the enterprise router, see **Viewing Routes**.

Step 3 In the route table of the service VPC, add a route with next hop set to enterprise router.

For details about VPC routes, see **Table 1-25**.

For details about how to configure route information, see **Adding Routes to VPC Route Tables**.

----End

Step 4: Verify the Network Connectivity Over the Direct Connect Connection

Step 1 Log in to ecs-demo.

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 2 Check whether the service VPC can communicate with the data center through the enterprise router.

ping *Any IP address of the data center*

Example command:

ping 192.168.3.10

If information similar to the following is displayed, vpc-for-er can communicate with the data center through the enterprise router:

```
[root@ecs-A02 ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.102) 56(84) bytes of data.
64 bytes from 192.168.3.102: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.102: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.102: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.102: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.102 ping statistics ---
```

----End

Step 5: Create a VPN Attachment to the Enterprise Router

For details about the VPC used by VPN, see **Table 1-27**.

Step 1 Create a VPC for the VPN gateway.

For details, see **Creating a VPC and Subnet**.

NOTICE

When creating a VPN gateway, you need to set **VPC** to this VPC and **Interconnection Subnet** to a subnet of this VPC. Ensure that the configured interconnection subnet has four or more assignable IP addresses.

Step 2 Create a VPN gateway and attach it to the enterprise router.

1. On the VPN management console, create a VPN gateway.

   For details, see **Creating a VPN Gateway**.

2. On the enterprise router console, check whether the VPN gateway attachment has been added to the enterprise router.

   For details, see **Viewing an Attachment**.

   If the status of the VPN gateway attachment is **Normal**, the attachment has been added.

   Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. Therefore, after you add the VPN gateway attachment to the enterprise router, the system will automatically:

   - Associate the VPN gateway attachment with the default route table of the enterprise router.
   - Propagate the VPN gateway attachment to the default route table of the enterprise router. The routes to the on-premises data center are propagated to the route table.

     You can view routes to the data center in the route table of the enterprise router only after performing the following steps.

Step 3 Create a customer gateway.

For details, see **Creating a Customer Gateway**.

Step 4 Create two VPN connections that will work in active/standby mode.

1. Create the active VPN connection. For details, see **Creating VPN Connection 1**.
2. Create the standby VPN connection. For details, see **Creating VPN Connection 2**.

Step 5 Configure routes on the on-premises network device.

The Direct Connect and VPN connections back up each other. Therefore, pay attention to the following when configuring routes:

- The routing mode of the Direct Connect and VPN connections must be the same. In this example, BGP routing is used.
- The route preference of the Direct Connect connection must be higher than that of the VPN connection.
- The amount of time that the disconnection of Direct Connect and VPN connections is detected should be the same as that of the cloud network.

----End

Step 6: Verify the Network Connectivity Over the VPN Connection

A VPN connection is a backup one. If you need to verify network connectivity of a VPN connection, you need to simulate a fault of the primary connection, that is, the Direct Connect connection.

Step 1 Simulate a fault on the Direct Connect connection to ensure that the service VPC cannot communicate with the data center over the connection.

NOTICE

Simulate a fault only when no service is running on the Direct Connect connection to prevent service interruptions.

Step 2 Log in to ecs-demo.

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 3 Check whether the service VPC can communicate with the data center through the enterprise router.

ping *Any IP address of the data center*

Example command:

ping 192.168.3.10

If information similar to the following is displayed, vpc-for-er can communicate with the data center through the enterprise router:

```
[root@ecs-A02 ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.102) 56(84) bytes of data.
64 bytes from 192.168.3.102: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.102: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.102: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.102: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.102 ping statistics ---
```

----End

1.6 Using VPN to Connect to the Cloud Through Two Internet Lines

1.6.1 Overview

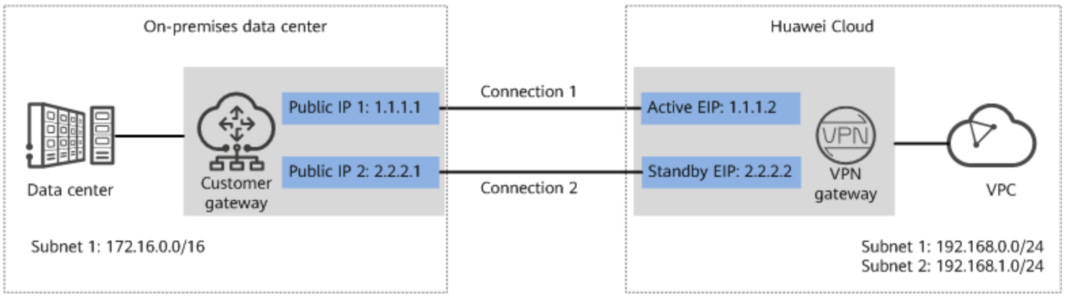
Scenario

To meet service requirements, enterprise A needs to implement communication between its on-premises data center and a VPC on the cloud. For reliability purposes, enterprise A requires that its on-premises data center use two public IP addresses to connect to the VPN gateway on the cloud.

Networking

Figure 1-7 shows the networking where the VPN service is used to connect the on-premises data center to the VPC.

Figure 1-7 Networking diagram



Solution Advantages

- A VPN gateway provides two EIPs to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection, ensuring reliability.
- Active-active VPN gateways can be deployed in different AZs to ensure AZ-level high availability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

1.6.2 Planning Networks and Resources

Data Plan

Table 1-29 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	• 192.168.0.0/24 • 192.168.1.0/24
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

Category	Item	Data
	HA Mode	Active/Standby
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: ● Active EIP: 1.1.1.2 ● Standby EIP: 2.2.2.2
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	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: ● Public IP address 1: 1.1.1.1 ● Public IP address 2: 2.2.2.1
	Tunnel interface address	● VPN connection 1: 169.254.70.2/30 ● VPN connection 2: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● DH algorithm: Group 15 ● Version: v2 ● Lifetime (s): 86400 ● Local ID: IP address ● Peer ID: IP address
	IPsec policy	● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● PFS: DH Group15 ● Transfer protocol: ESP ● Lifetime (s): 3600

1.6.3 Procedure

Prerequisites

- Cloud side
  - 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**.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center. For details, see **Administrator Guide**.

Procedure

Huawei Cloud VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

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

   Table 1-30 only describes the key parameters for creating a VPN gateway.

Table 1-30 VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**. If the VPN gateway is associated with an enterprise router, select **Enterprise Router**.	VPC
VPC	Huawei Cloud VPC that the on-premises data center needs to access.	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

Parameter	Description	Value
Local Subnet	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active/Standby**.	Active/Standby
Active EIP	Active EIP used by the VPN gateway to access the on-premises data center.	1.1.1.2
Standby EIP	Standby EIP used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure customer gateways.

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

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

   Table 1-31 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar01
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

3. Set parameters for the second customer gateway.

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

Table 1-32 Parameters for the second customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar02
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	2.2.2.1

Step 5 Configure VPN connections.

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

   Table 1-33 only describes the key parameters for creating a VPN connection.

Table 1-33 Parameter settings for VPN connection 1

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-ar01
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16

Parameter	Description	Value
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

NOTE

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

Table 1-34 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Standby EIP bound to the VPN gateway.	2.2.2.2
Customer Gateway	Name of a customer gateway.	cgw-ar02
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1

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

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

Verification

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

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

1.7 Using VPN to Encrypt Data over Direct Connect Lines

1.7.1 Overview

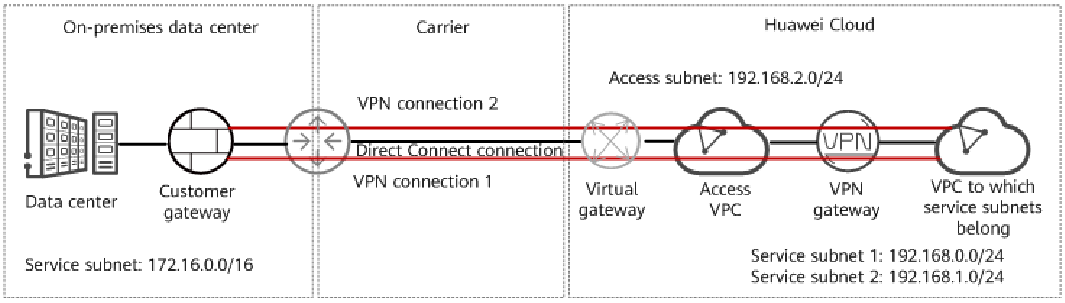
Scenario

The on-premises data center of a financial institution connects to the cloud through Direct Connect. To ensure data transmission security, the financial institution wants to use VPN to encrypt the data entering and leaving the cloud.

Networking

Figure 1-8 shows the VPN networking.

Figure 1-8 Networking


On-premises data center
Carrier
Huawei Cloud
Access subnet: 192.168.2.0/24
VPN connection 2
Direct Connect connection
VPN connection 1
Data center
Customer gateway
Virtual gateway
Access VPC
VPN
VPN gateway
VPC to which service subnets belong
Service subnet: 172.16.0.0/16
Service subnet 1: 192.168.0.0/24
Service subnet 2: 192.168.1.0/24

Solution Advantages

- Dual connections: A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.
- More secure: Direct Connect provides independent lines to ensure data transmission quality. VPN provides data encryption to ensure data transmission security.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

1.7.2 Planning Networks and Resources

Data Plan

Table 1-35 Data plan

Category	Item	Data
On-premises data center	Service subnet to be interconnected	Subnet to which the IP address of the customer gateway in VPN belongs. 172.16.0.0/16
	Access subnet	Subnet to which the IP address of the Direct Connect remote gateway belongs. The access subnet can be the same as the service subnet. In this example, the access subnet and service subnet are the same. 172.16.0.0/16
VPC to which service subnets belong	VPC name	tenant_vpc
Direct Connect virtual gateway	VPC	Same as the access VPC of the VPN gateway. tenant_vpc
	Local subnet	Same as the access subnet of the VPN gateway. 192.168.2.0/24

Category	Item	Data
Direct Connect virtual interface	IP address of the local gateway	This address is used by the Direct Connect virtual gateway to communicate with the Direct Connect remote gateway. At both ends, the configured local and remote gateway addresses must be reversed. 1.1.1.1/30
	IP address of the remote gateway	2.2.2.2/30
	Remote subnet	Access subnet to which the Direct Connect remote gateway belongs. 172.16.0.0/16
VPN gateway	VPC	VPC to which service subnets belong tenant_vpc
	Interconnection subnet	This subnet is used for communication between the VPN gateway and the VPC to which service subnets belong. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	Local subnet	Subnet used by the VPC to communicate with the on-premises data center. ● 192.168.0.0/24 ● 192.168.1.0/24
	HA mode	Active-active
	Access VPC	It can be the same as or different from the VPC to which service subnets belong. In this example, the access VPC and the VPC to which service subnets belong are the same. tenant_vpc

Category	Item	Data
	Access subnet	● If the access VPC and the VPC to which service subnets belong are the same and the access subnet and the interconnection subnet are also the same, ensure that the interconnection subnet has four or more assignable IP addresses. This scenario is used as an example. 192.168.2.0/24 ● If the access VPC and the VPC to which service subnets belong are the same and the access subnet and the interconnection subnet are different, ensure that the access subnet has two or more assignable IP addresses. ● If the access VPC and the VPC to which service subnets belong are different, ensure that the access subnet has two or more assignable IP addresses.
	Gateway IP Address	Manually specify the gateway IP addresses. ● Private IP address 1: 192.168.2.100 ● Private IP address 2: 192.168.2.101
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
Customer gateway in VPN	Gateway IP address	This IP address is planned and configured by the administrator of the on-premises data center. 172.16.0.111
	Tunnel interface address	● VPN connection 1: 169.254.70.2/30 ● VPN connection 2: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	● Version: v2 ● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● DH algorithm: Group 15 ● Lifetime (s): 86400 ● Local ID: IP address ● Peer ID: IP address

Category	Item	Data
	IPsec policy	- Authentication algorithm: SHA2-256 - Encryption algorithm: AES-128 - PFS: DH Group15 - Transfer protocol: ESP - Lifetime (s): 3600

1.7.3 Configuring Direct Connect

Procedure

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click **Service List** and choose **Networking** > **Direct Connect**.

Step 3 Create a connection.

You can choose self-service installation or full-service installation based on your service scenarios.

For details, see **Creating a Connection**.

Table 1-36 Parameters for creating a connection

Parameter	Description	Value
Connection Name	Name of a connection.	phlk_01

Step 4 Create a virtual gateway.

Table 1-37 only describes the key parameters for creating a virtual gateway. For details about all parameters, see **Create a Virtual Gateway**.

Table 1-37 Parameters for creating a virtual gateway

Parameter	Description	Value
Name	Name of a virtual gateway.	dcgw_01
VPC	VPC to which the virtual gateway is attached. In this scenario, select the access VPC.	tenant_vpc

Parameter	Description	Value
Local Subnet	VPC subnet to be accessed using Direct Connect. In this scenario, select the access subnet corresponding to the access VPC.	192.168.2.0/24

Step 5 Create a virtual interface.

Table 1-38 only describes the key parameters for creating a virtual interface. For details about all parameters, see **Creating a Virtual Interface**.

Table 1-38 Parameters for creating a virtual interface

Parameter	Description	Value
Name	Name of a virtual interface.	dcif_01
Connection	Connection used to connect the on-premises data center to the cloud.	phlk_01
Virtual Gateway	Virtual gateway to which the virtual interface connects.	dcgw_01
Local Gateway	IP address of the network interface on the Huawei Cloud side.	1.1.1.1/30
Remote Gateway	IP address of the remote gateway in the on-premises data center. The IP addresses of the remote gateway and local gateway must be in the same network segment. Generally, a subnet with the mask length of 30 is used.	2.2.2.2/30
Remote Subnet	Access subnet and mask on the on-premises data center side.	172.16.0.0/16
Routing Mode	Two options are available: **Static** and **BGP**.	Static

----End

1.7.4 Configuring VPN

Prerequisites

- Cloud side
  - 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**.
- An enterprise router has been created if you want to use it to connect to a VPN gateway. For details, see the enterprise router documentation.

- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center. For details, see **Administrator Guide**.

Procedure

Huawei Cloud VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Log in to the Huawei Cloud management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

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

   Table 1-39 only describes the key parameters for creating a VPN gateway.

Table 1-39 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Private network**.	Private network
Associate With	Select **VPC**. If the VPN gateway is associated with an enterprise router, select **Enterprise Router**.	VPC
Enterprise Router	Specify the associated enterprise router only when **Associate With** is set to **Enterprise Router**.	er-001
VPC	Select the VPC where the subnet to be accessed by the on-premises data center is located.	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

Paramete r	Description	Value
Local Subnet	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24
HA Mode	Select **Active-active**.	Active-active
Advanced Settings	Advanced settings are available only when **Associate With** is set to **VPC** and **Network Type** is set to **Private network**.	-
Access VPC	– Same as the associated VPC Use the VPC associated with the VPN gateway as the access VPC. – Another VPC Select another VPC as the access VPC.	Same as the associated VPC
Access Subnet	– When **Access VPC** is set to **Same as the associated VPC**: ■ Same as the interconnection subnet The private IP addresses of the VPN gateway are assigned from the interconnection subnet. The access subnet and interconnection subnet each require two IP addresses. As such, ensure that the access subnet has four or more available IP addresses. ■ Another subnet Ensure that the access subnet has two or more available IP addresses. – When **Access VPC** is set to a specific VPC: Ensure that the selected access subnet has two or more available IP addresses.	Same as the interconnection subnet

Parameter	Description	Value
Gateway IP Address	Select **Manually-specified IP address** and specify gateway IP addresses.	– Private IP address 1: 192.168.2.100 – Private IP address 2: 192.168.2.101

Step 4 Configure a customer gateway.

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

   Table 1-40 only describes the key parameters for creating a customer gateway.

Table 1-40 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	172.16.0.111

Step 5 Configure VPN connections.

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

   Table 1-41 only describes the key parameters for creating a VPN connection.

Table 1-41 Parameter settings for VPN connection 1

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001

Parameter	Description	Value
Gateway IP Address	Private IP address bound to the VPN gateway.	192.168.2.100
Customer Gateway	Name of a customer gateway.	cgw-fw
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

NOTE

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

Table 1-42 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Another private IP address bound to the VPN gateway.	192.168.2.101
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

1.7.5 Verification

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

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

1.8 Configuring VPN Load Balancing to Provide High Bandwidth for Cloud and On-Premises Interconnection

1.8.1 Overview

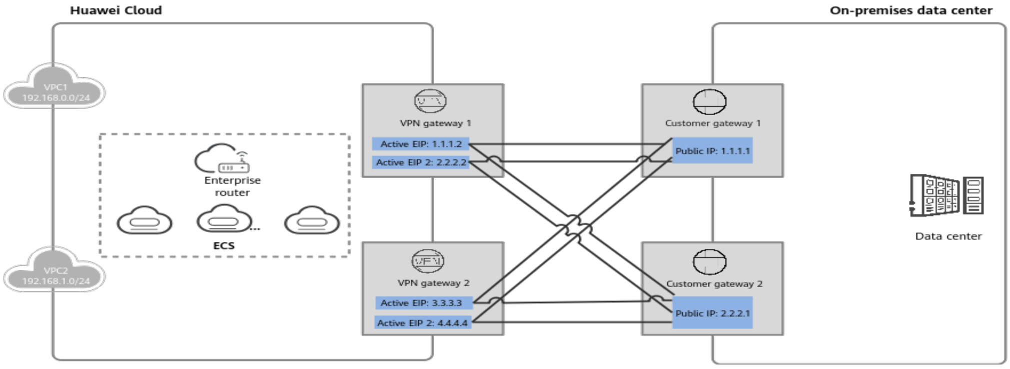
Scenario

Multiple VPN gateways attached to the same enterprise router need to establish multiple BGP connections with customer gateways to implement load balancing and provide high bandwidth.

Networking

Figure 1-9 shows the VPN networking.

Figure 1-9 Networking diagram



Solution Advantages

Multiple VPN gateways can connect to multiple customer gateways in full-mesh networking, achieving load balancing and providing high bandwidth.

Limitations and Constraints

- A maximum of 10 VPN gateways can be attached to an enterprise router.
- The maximum forwarding performance of a VPN gateway is 2 Gbit/s when its specification is Professional 2. Given this, the maximum forwarding performance of 10 VPN gateways is 20 Gbit/s.

1.8.2 Planning Networks and Resources

Data Plan

Table 1-43 Data plan

Category	Item	Data
VPC	Subnet to be interconnected	● VPC1: 192.168.0.0/24 ● VPC2: 192.168.1.0/24
	Enterprise router	Enterprise router attached to VPC1 and VPC2.
	ECS	Three ECSs are in different VPCs. If the ECSs are in different security groups, add rules to the security groups to allow access to each other.
VPN gateway 1	Access subnet	Subnet used for communication between the VPN gateway and VPCs. Ensure that the selected access 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, VPN gateway 1 uses two EIPs. In this example, the EIPs are as follows: ● Active EIP: 1.1.1.2 ● Active EIP 2: 2.2.2.2
	Tunnel interface address	IP addresses used by VPN gateway 1 to establish IPsec tunnels with customer gateway 1. At the two ends of an 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 IP addresses used by VPN gateway 1 to establish IPsec tunnels with customer gateway 2. At the two ends of an IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● VPN connection 3: 169.254.72.1/30 ● VPN connection 4: 169.254.73.1/30
VPN gateway 2	Access subnet	Subnet used for communication between the VPN gateway and VPCs. Ensure that the selected access subnet has four or more assignable IP addresses. 192.168.3.0/24
	HA mode	Active-active
	EIP	EIPs are automatically generated when you buy them. By default, VPN gateway 2 uses two EIPs. In this example, the EIPs are as follows: ● Active EIP: 3.3.3.3 ● Active EIP 2: 4.4.4.4

Category	Item	Data
	Tunnel interface address	IP addresses used by VPN gateway 2 to establish IPsec tunnels with customer gateway 1. At the two ends of an IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● VPN connection 5: 169.254.74.1/30 ● VPN connection 6: 169.254.75.1/30 IP addresses used by VPN gateway 2 to establish IPsec tunnels with customer gateway 2. At the two ends of an IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● VPN connection 7: 169.254.76.1/30 ● VPN connection 8: 169.254.77.1/30
On-premises data center	Subnet to be interconnected	172.16.0.0/16
Customer gateway 1	Public IP address	Public IP address assigned by a carrier. In this example, the public IP address is as follows: 1.1.1.1
	Tunnel interface address	● VPN connection 1: 169.254.70.2/30 ● VPN connection 2: 169.254.71.2/30 ● VPN connection 5: 169.254.74.2/30 ● VPN connection 6: 169.254.75.2/30
Customer gateway 2	Public IP address	Public IP address assigned by a carrier. In this example, the public IP address is as follows: 2.2.2.1
	Tunnel interface address	● VPN connection 3: 169.254.72.2/30 ● VPN connection 4: 169.254.73.2/30 ● VPN connection 7: 169.254.76.2/30 ● VPN connection 8: 169.254.77.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	● IKE version: IKEv2 ● Authentication algorithm: SHA2-256 ● Encryption algorithm: AES-128 ● DH algorithm: group 15 ● Lifetime (s): 86400 ● Local ID: IP address ● Peer ID: IP address

Category	Item	Data
	IPsec policy	- Authentication algorithm: SHA2-256 - Encryption algorithm: AES-128 - PFS: DH group15 - Transfer protocol: ESP - Lifetime (s): 3600

1.8.3 Procedure

Prerequisites

- Cloud side
  - VPCs have been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.
  - Security group rules have been configured for the VPCs, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see **Security Group Rules**.
  - An enterprise router has been created. For details, see the enterprise router documentation.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center. For details, see **Administrator Guide**.

Procedure

In this scenario, the BGP routing mode is used, and you need to create eight VPN connections between the cloud and the on-premises data center.

Step 1 Log in to the management console.

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

Step 3 Configure VPN gateways.

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

   Table 1-44 describes the parameter settings for VPN gateway 1.

Table 1-44 Parameter settings for VPN gateway 1

Parameter	Description	Value
Name	VPN gateway name.	vpngw-001
Network Type	Select **Public network**.	Public network

Parameter	Description	Value
Associate With	Select **Enterprise Router**.	Enterprise Router
Enterprise Router	Enterprise router to which the VPN gateway is attached.	er-001
Access VPC	This parameter is mandatory only when **Associate With** is set to **Enterprise Router**.	vpc-001(192.168.0.0/24)
Access Subnet	Subnet used for communication between VPN gateway 1 and VPCs. Ensure that the selected access subnet has four or more assignable IP addresses.	192.168.2.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active-active**.	Active-active
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	2.2.2.2

3. Configure VPN gateway 2 (192.168.3.0/24) by referring to the preceding steps.

NOTE

VPN gateway 2 has different settings of **Name**, **Access Subnet**, **Active EIP**, and **Active EIP 2** from VPN gateway 1. Other parameter settings are the same.

Table 1-45 Parameter settings for VPN gateway 2

Parameter	Description	Value
Name	VPN gateway name.	vpngw-002
Access Subnet	Subnet used for communication between VPN gateway 2 and VPCs. Ensure that the selected access subnet has four or more assignable IP addresses.	192.168.3.0/24
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	3.3.3.3
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	4.4.4.4

Step 4 Configure customer gateways.

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

   Table 1-46 describes the parameter settings for customer gateway 1.

   Table 1-46 Parameter settings for customer gateway 1

Parameter	Description	Value
Name	Customer gateway name.	cgw-fw1
Identifier	IP address used by customer gateway 1 to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1
BGP ASN	BGP AS number.	65000
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**.	-

3. Configure customer gateway 2 (2.2.2.1) by referring to the preceding steps.

   NOTE

   Customer gateway 2 has different settings of **Name** and **Identifier** (IP address) from customer gateway 1. Other parameters are the same.

   Table 1-47 Parameter settings for customer gateway 2

Parameter	Description	Value
Name	Customer gateway name.	cgw-fw2
Identifier	IP address used by customer gateway 2 to communicate with the Huawei Cloud VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	2.2.2.1

Step 5 Configure VPN connections between VPN gateway 1 on the cloud and the data center.

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

   Table 1-48 describes the parameters for creating a VPN connection.

Table 1-48 Parameter settings for VPN connection 1

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway 1 for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to VPN gateway 1.	1.1.1.2
Customer Gateway	Name of customer gateway 1.	cgw-fw1
VPN Type	Select **BGP routing**.	BGP routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPCs on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.70.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled

Parameter	Description	Value
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Configure VPN connections 2, 3, and 4.

NOTE

The name, gateway IP address, customer gateway, local tunnel interface IP address, and customer tunnel interface IP address for these VPN connections are different from those of VPN connection 1. Other parameter settings are the same.

Table 1-49 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	VPN connection name.	vpn-002
Customer Gateway	Name of customer gateway 1.	cgw-fw1
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway.	169.254.71.2

Table 1-50 Parameter settings for VPN connection 3

Parameter	Description	Value
Name	VPN connection name.	vpn-003
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
VPN Gateway	VPN gateway 1 for which the VPN connection is created.	vpngw-001
Customer Gateway	Name of customer gateway 2.	cgw-fw2

Parameter	Description	Value
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.72.1
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway in the on-premises data center.	169.254.72.2

Table 1-51 Parameter settings for VPN connection 4

Parameter	Description	Value
Name	VPN connection name.	vpn-004
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
VPN Gateway	VPN gateway 1 for which the VPN connection is created.	vpngw-001
Customer Gateway	Name of customer gateway 2.	cgw-fw2
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.73.1
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway in the on-premises data center.	169.254.73.2

Step 6 Configure VPN connections between VPN gateway 2 on the cloud and the data center.

The configuration procedure is the same as that for VPN gateway 1.

Step 7 Configure the customer gateway device in the on-premises data center.

The configuration procedures may vary according to the type of the customer gateway device. For details, see **Administrator Guide**.

----End

1.8.4 Verification

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

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

- Verify that servers in the on-premises data center and ECSs in the Huawei Cloud VPC subnets can ping each other.
- Check inbound traffic statistics of the customer gateway. The statistics show that traffic is load balanced between gateways.

2 S2C Classic VPN

2.1 Connecting an On-Premises Data Center to a VPC Through a VPN

Scenarios

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 configure VPN. After that, you need to configure security group rules and check subnet connectivity to ensure that the VPN is available. VPNs can be classified into the following two types:

- A site-to-site VPN functions as a communication tunnel between a VPC and a single on-premises data center.
- By contrast, a hub-and-spoke VPN is between a VPC and multiple on-premises data centers.

Pay attention to the following when you configure a VPN:

- The local and remote subnets cannot conflict.
- The IKE policies, IPsec policies, and PSKs configured on the cloud and in the on-premises data center must be the same.
- The parameters configured for the local and remote subnets and gateways must be symmetric.
- Security group rules permit access to and from the ECSs in the VPC.
- The status of a VPN changes to **Normal** only after ECSs and on-premises servers access each other.

Prerequisites

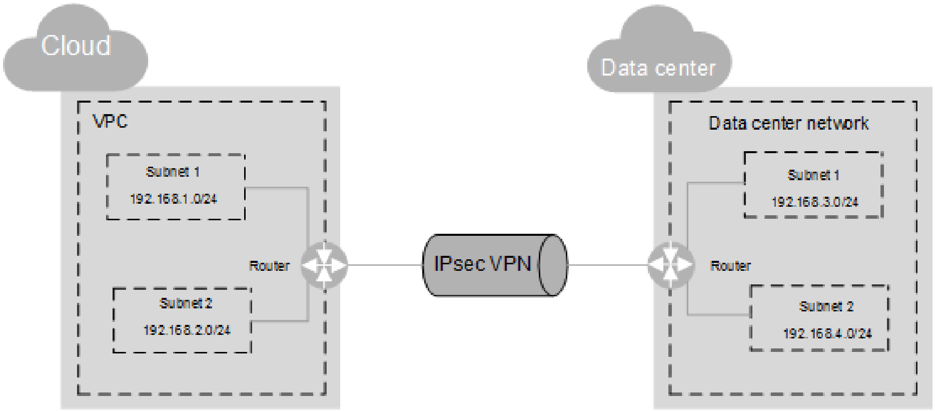
You have created the VPC and subnets that the on-premises data center wants to access.

Procedure

1. On the management console, select the appropriate IKE and IPsec policies to create a VPN.
2. Check the IP address pools for the local and remote subnets.

   In **Figure 2-1**, 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 set up a VPN to connect these subnets.

   Figure 2-1 IPsec VPN

   The IP address pools for the local subnets cannot overlap with those for the remote subnets. Like in this example, the IP address pool for the remote subnets cannot contain the two subnets of the VPC.
3. Configure security group rules for the ECSs to allow packets from and to the on-premises data center over the VPN.
4. Ping the ECSs from the on-premises data center to verify that the security group allows packets from and to the on-premises data center over the VPN.
5. Check the on-premises network configuration.

   A route must be configured for the on-premises network to enable traffic to be forwarded to network devices on the network over the VPN. If the data transmitted through the VPN cannot be forwarded to the network devices, check whether the remote LAN has rules configured to refuse the traffic.

3 P2C VPN

3.1 Configuring Enterprise Edition P2C VPN to Connect Mobile Terminals to a VPC (Certificate Authentication)

3.1.1 Overview

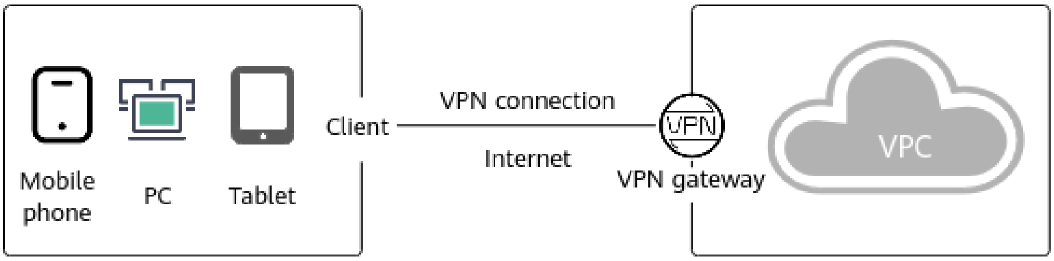
Scenario

P2C VPN supports certificate authentication. A server uses a client CA certificate to verify the identity of a client.

Networking

Clients can use the certificates issued by a CA to connect to a VPN gateway for access to a VPC.

Figure 3-1 Networking diagram



Solution Advantages

Users can connect to a VPN gateway through client certificate authentication, securing data transmission.

Limitations and Constraints

A maximum of 10 client CA certificates can be added.

3.1.2 Planning Networks and Resources

Data Plan

Table 3-1 Data plan

Category	Item	Data
VPC	Subnet to be interconnected	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 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	192.168.0.0/24
	Server certificate	cert-server (name of the server certificate hosted by the CCM)
Client	SSL parameters	● Protocol: TCP ● Port: 443 ● Encryption algorithm: AES-128-GCM ● Authentication algorithm: SHA256 ● Compression: disabled
	Client CIDR block	172.16.0.0/16
	Client authentication mode	Select **Certificate authentication** and click **Upload Client CA Certificate**. ● Name: ca-cert-client ● Content: -----BEGIN CERTIFICATE----- od2VC7zXq7vmsVS5ZuyzeZA9CG +kzHsznZnmMjK+L9ddtRrLolRKIlE7VgWSVvn NCnGre6nQErWV688fsKJFIJ7xEBpt +S10zNuuk42OA36RsSauJWtLtebvhTav5df -----END CERTIFICATE-----

3.1.3 Procedure

Prerequisites

- Cloud side
  - 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**.
- Data center side
  - The VPN client software has been configured on a user terminal. For details, see **Administrator Guide**.

Limitations and Constraints

A maximum of 10 client CA certificates can be added.

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 Configure a VPN gateway.

1. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
2. Click the **P2C VPN Gateways** tab, and then click **Buy P2C VPN Gateway**.
3. Set parameters as prompted and click **Buy Now**.

   Table 3-2 describes the VPN gateway parameters.

Table 3-2 Description of VPN gateway parameters

Parameter	Description	Example Value
Region	For low network latency and fast resource access, select the region nearest to your target users. Resources cannot be shared across regions.	*Set this parameter based on the actual condition.*
Name	Enter the name of a VPN gateway.	p2c-vpngw-001
VPC	Select a VPC.	vpc-001(192.168.0.0/16)

Parameter	Description	Example Value
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has three or more assignable IP addresses.	192.168.66.0/24
Specification	Only **Professional 1** is supported. – Maximum bandwidth: 300 Mbit/s – Maximum number of VPN connections: 500	Professional 1
AZ	An availability zone (AZ) is a geographic location with independent power supply and network facilities in a region. AZs in the same VPC are interconnected through private networks and are physically isolated. – If two or more AZs are available, select two AZs. The VPN gateway deployed in two AZs has higher availability. You are advised to select the AZs where resources in the VPC are located. – If only one AZ is available, select this AZ.	AZ1, AZ2
Connections	Ten VPN connections are included free of charge with the purchase of a VPN gateway. You can select or customize the number of required VPN connections.	10
EIP	Set the EIP used by the VPN gateway to communicate with clients. – **Create now**: Buy a new EIP. The billing mode of a new EIP is pay-per-use. – **Use existing**: Use an existing EIP. Only EIPs with dedicated bandwidth are supported. **NOTE** If an existing EIP is used, its billing mode can be pay-per-use or yearly/monthly.	Create now
EIP Type	This parameter is available only when a new EIP is created. **Dynamic BGP**: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails. For more information about EIP types, see **What Is Elastic IP?**.	Dynamic BGP

Parameter	Description	Example Value
Bandwidth (Mbit/s)	This parameter is available only when a new EIP is created. Specify the bandwidth of the EIP. – All VPN connections created using the EIP share the bandwidth of the EIP. The total bandwidth consumed by all the VPN connections cannot exceed the bandwidth of the EIP. If network traffic exceeds the bandwidth of the EIP, 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. – You can customize the bandwidth within the allowed range. – Some regions support only 300 Mbit/s bandwidth by default. If higher bandwidth is required, select 300 Mbit/s bandwidth and then **submit a service ticket** for capacity expansion.	20 Mbit/s
Bandwidth Name	This parameter is available only when a new EIP is created. Specify the name of the EIP bandwidth.	p2c-vpngw-bandwidth1

Step 5 Configure a server.

1. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
2. Click the **P2C VPN Gateways** tab. Then, click **Configure Server** in the **Operation** column of the target VPN gateway, or click the name of the target VPN gateway and click the **Server** tab.
3. Set parameters as prompted and click **OK**.

   Table 3-3 describes the server parameters.

Table 3-3 Server parameters

Area	Parameter	Description	Example Value
Basic Information	Local CIDR Block	Destination CIDR block that clients need to access through the P2C VPN gateway. The CIDR block can be within or connected to a Huawei Cloud VPC. A maximum of 20 local CIDR blocks can be specified. The local CIDR block cannot be set to 0.0.0.0. The local CIDR block cannot overlap or conflict with the following special CIDR blocks: 0.0.0.0/8, 224.0.0.0/4, 240.0.0.0/4, and 127.0.0.0/8. – Select subnet Select subnets of the local VPC. – Enter CIDR block Enter subnets of the local VPC or subnets of the VPC that establishes a peering connection with the local VPC. **NOTE** After the local CIDR block is modified, clients need to be reconnected.	192.168.0.0/24
	Client CIDR Block	CIDR block for assigning IP addresses to virtual NICs of clients. It cannot overlap with the local CIDR block or the CIDR blocks in the route table of the VPC where the VPN gateway is located. The client CIDR block must be in the format of dotted decimal notation/ mask. The mask ranges from 16 to 26. When assigning an IP address to a client, the system assigns a smaller CIDR block with the mask of 30 to ensure proper network communication. As such, ensure that the number of available IP addresses in the specified client CIDR block is at least four times the number of VPN connections. The recommended client CIDR blocks vary according to the number of VPN connections. For details, see **Table 3-4**. **NOTE** After the client CIDR block is modified, clients need to be reconnected.	172.16.0.0/16

Area	Parameter	Description	Example Value
	Tunnel Type	Secure Sockets Layer (SSL) is a transport layer protocol used to establish a secure channel between a client and a server. The value is fixed at **OpenVPN (SSL)**.	OpenVPN (SSL)
Authentication Information	Server Certificate	SSL certificate of the server. Clients use this certificate to verify the server's identity. – To use an uploaded certificate, select it from the drop-down list box. – To upload a new certificate, choose **Upload** from the drop-down list box to go to the Cloud Certificate Manager (CCM) service page. Upload a server certificate as prompted. For details, see **Uploading an External Certificate**. – It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. **NOTE** If you delete the referenced server certificate in CCM after configuring the server, the availability of the server certificate is not affected.	*Set this parameter based on the actual condition.*

Area	Parameter	Description	Example Value
	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. A maximum of 10 client CA certificates can be added. It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. Certificates using the RSA-2048 encryption algorithm have risks. Exercise caution when using such certificates. – After a CA certificate is verified, you can view its basic information, including the name, serial number, signature algorithm, issuer, subject, and expiration time. **NOTE** After the CA certificate is deleted, clients cannot connect to the server.	Certificate authentication
Advanced Settings	Protocol	Protocol used by P2C VPN connections. – TCP (default)	TCP
	Port	Port used by P2C VPN connections. – 443 (default) – 1194	443
	Encryption Algorithm	Encryption algorithm used by P2C VPN connections. – AES-128-GCM (default) – AES-256-GCM	AES-128-GCM
	Authentication Algorithm	Authentication algorithm used by P2C VPN connections. – When the encryption algorithm is AES-128-GCM, the authentication algorithm is SHA256. – When the encryption algorithm is AES-256-GCM, the authentication algorithm is SHA384.	SHA256

Area	Parameter	Description	Example Value
	Compression	Whether to compress the transmitted data. By default, this function is disabled and cannot be modified.	Disabled

Table 3-4 Recommended client CIDR blocks

Number of VPN Connections	Recommended Client CIDR Block
10	CIDR blocks with the mask less than or equal to 26 Example: 10.0.0.0/26 and 10.0.0.0/25
20	CIDR blocks with the mask less than or equal to 25 Example: 10.0.0.0/25 and 10.0.0.0/24
50	CIDR blocks with the mask less than or equal to 24 Example: 10.0.0.0/24 and 10.0.0.0/23
100	CIDR blocks with the mask less than or equal to 23 Example: 10.0.0.0/23 and 10.0.0.0/22
200	CIDR blocks with the mask less than or equal to 22 Example: 10.0.0.0/22 and 10.0.0.0/21
500	CIDR blocks with the mask less than or equal to 21 Example: 10.0.0.0/21 and 10.0.0.0/20

4. Upload a server certificate.

   a. On the **Server** tab page, click **Upload** in the **Server Certificate** drop-down list box. The **Cloud Certificate Manager** page is displayed.

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

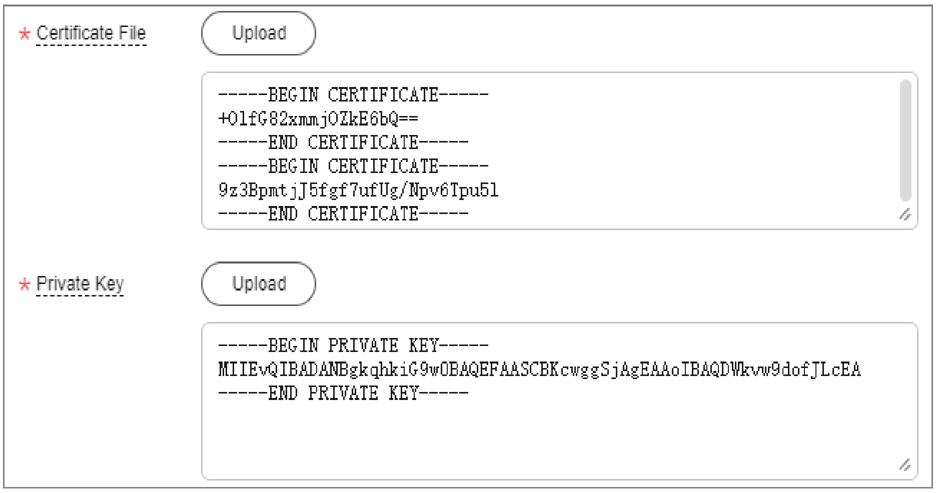
      Table 3-5 describes the parameters for uploading a certificate.

Table 3-5 Parameters for uploading an international standard certificate

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

Parameter	Description
Enterprise Project	Select the enterprise project to which the SSL certificate is to be added.
Certificate File	Use a text editor (for example, Notepad++) to open the certificate file in PEM format to be uploaded, and copy the certificate content to this text box. You need to upload a combined certificate file that contains both the server certificate content and CA certificate content. The CA certificate content must be pasted below the server certificate content. For the format of the certificate file content to be uploaded, see **Figure 3-2**.
Private Key	Use a text editor (for example, Notepad++) to open the certificate file in KEY format to be uploaded, and copy the private key content to this text box. You only need to upload the private key of the server certificate. For the format of the private key content to be uploaded, see **Figure 3-2**.

Figure 3-2 Format of the certificate content to be uploaded



```
-----BEGIN CERTIFICATE-----
+O1fG82xmmjOZkE6bQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
9z3BpmtjJ5fgf7ufUg/Npv6Tpu5l
-----END CERTIFICATE-----
```

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

NOTE

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

c. Click **Submit**. The certificate is uploaded.

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

5. Upload a client CA certificate.

a. On the **Server** tab page, choose **Certificate authentication** from the **Client Authentication Mode** drop-down list box, and click **Upload Client CA Certificate**.

b. Set parameters as prompted.

Table 3-6 Parameters for uploading a CA certificate

Parameter	Description	Example Value
Name	This parameter can be modified.	ca-cert-xxxx
Content	Use a text editor (for example, Notepad++) to open the signature certificate file in PEM format, and copy the certificate content to this text box. **NOTE** ■ It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. ■ Certificates using the RSA-2048 encryption algorithm have risks. Exercise caution when using such certificates.	-----BEGIN CERTIFICATE----- *Certificate content* -----END CERTIFICATE-----

c. Click **OK**.

NOTE

A maximum of 10 client CA certificates can be added.

Step 6 Download the client configuration.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner of the page, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab. In the VPN gateway list, locate the target VPN gateway, and click **Download Client Configuration** in the **Operation** column.

   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.

Step 7 Add certificate information.

1. Use a text editor (for example, Notepad++) to open the **client_config.ovpn** file.
2. Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
Client certificate content
</cert>
<key>
Private key of the client certificate
</key>
```

3. Save the file and exit.

Step 8 Configure a client.

NOTE

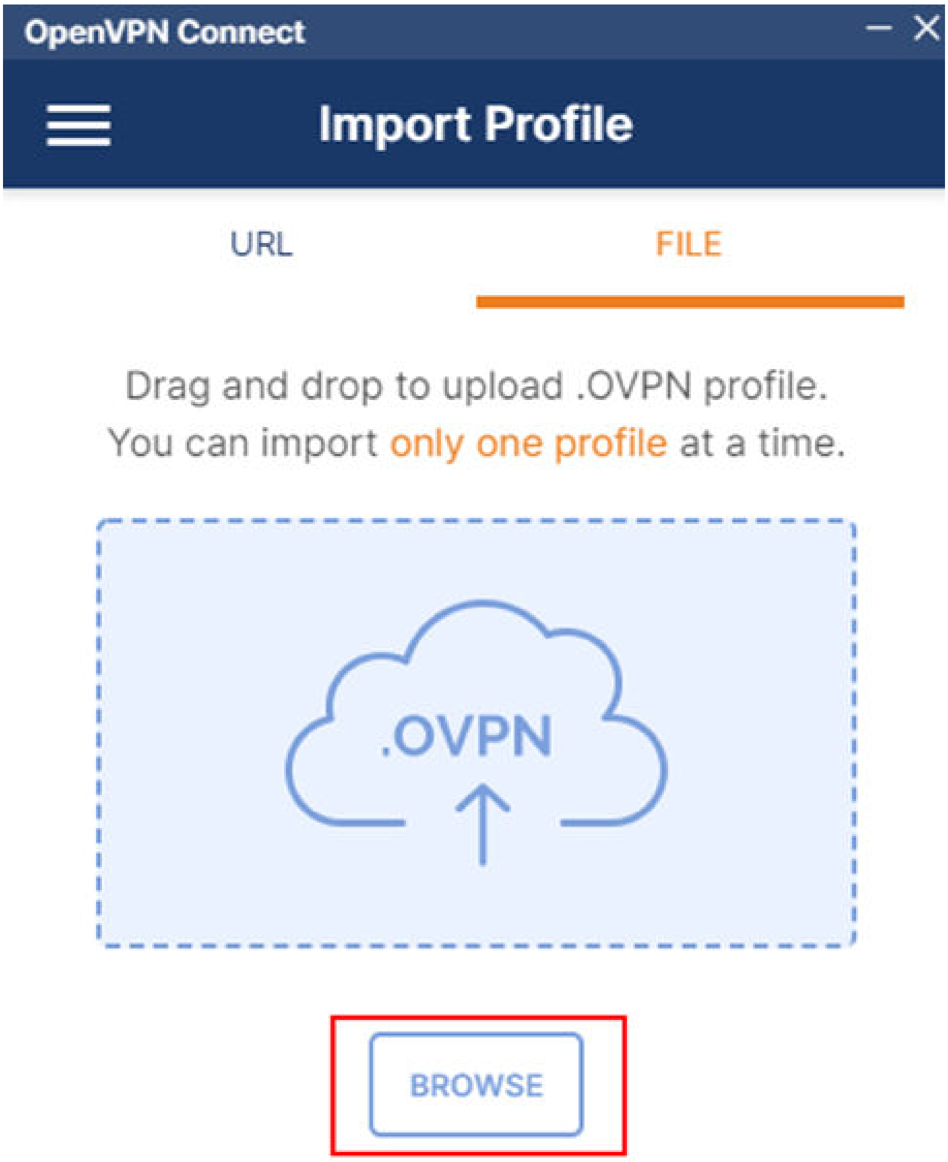
This example describes how to configure a client on the Windows operating system. The configuration process varies according to the type and version of the VPN client software.

- Operating system: Windows 10
- Client software: OpenVPN Connect 3.4.2 (3160)

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

1. **Download OpenVPN Connect** from the OpenVPN official website, and install it as prompted.
2. Start the OpenVPN Connect client, click **BROWSE** on the **FILE** tab page, and upload the client configuration file.

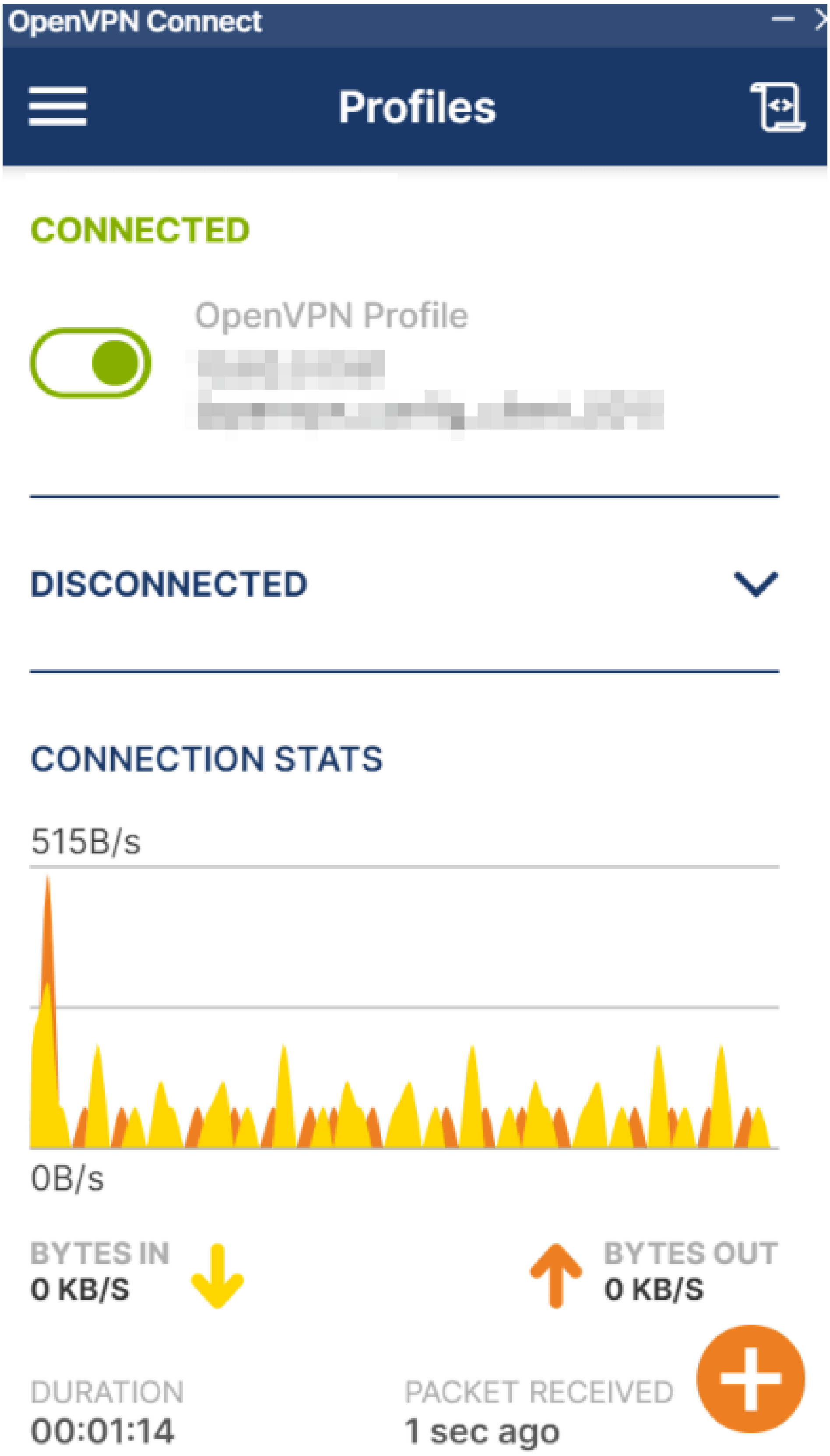
Figure 3-3 Uploading a configuration file



Drag and drop to upload .OVPN profile.
You can import only one profile at a time.

3. Click **CONNECT** to establish a VPN connection. If information similar to the following is displayed, the connection is successfully established.

Figure 3-4 Connection established



----End

Verification

1. Open the CLI on 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
```