Virtual Private Network

Best Practices

Issue	01
Date	2025-11-13

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

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

1 S2C Enterprise Edition VPN

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

1.1.1 Overview

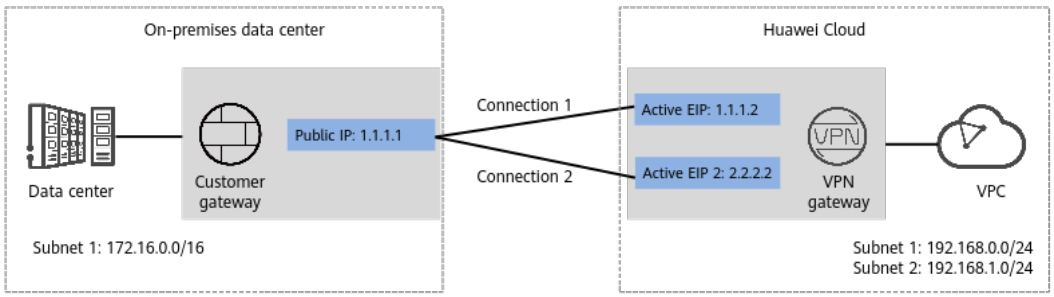
Scenario

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

Networking

In this example, a group of 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 addresses under **Connection 1's Configuration**	IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30

Category	Item	Data
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is as follows: 1.1.1.1
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 S2C 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

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-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
Identifier	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 **Create VPN Connection**.
2. Set VPN connection parameters and click **Buy Now**.

   Table 1-4 describes the key parameters for creating VPN connections.

Table 1-4 Description of VPN connection parameters

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

Parameter	Description	Value
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.71.1/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

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

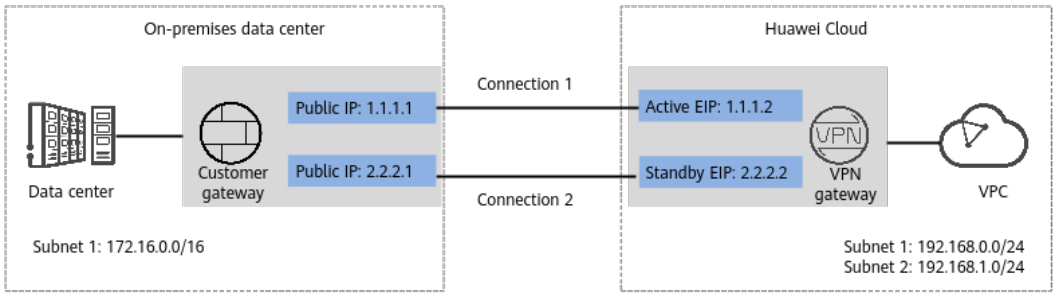
Scenario

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 1-5 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/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 addresses under **Connection 1's Configuration**	IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30

Category	Item	Data
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP addresses are as follows: • 1.1.1.1 • 2.2.2.1
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

1.2.3 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 S2C VPN Gateway**.
2. Set parameters as prompted.

   Table 1-6 only describes the key parameters for creating a VPN gateway.

Table 1-6 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

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 the customer gateway.

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

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

Table 1-7 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Identifier	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 **Create VPN Connection**.
2. Set VPN connection parameters and click **Buy Now**.

   Table 1-8 only describes the key parameters for creating VPN connections.

Table 1-8 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	2.2.2.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

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

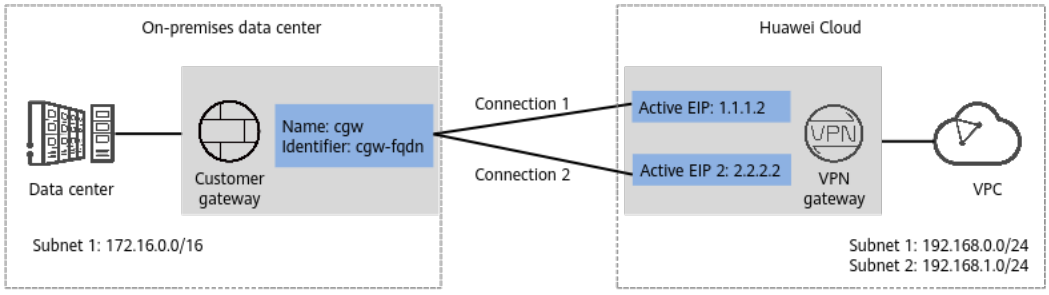
Scenario

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, a group of 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 1-9 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
	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, and choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

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

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

Table 1-10 Description of VPN gateway parameters

Parameter	Description	Value
Billing Mode	Select **Yearly/Monthly**.	Yearly/Monthly
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

Parameter	Description	Value
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 1-11 only describes the key parameters for creating a customer gateway.

Table 1-11 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw

Parameter	Description	Value
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 **Create VPN Connection**.
2. Set VPN connection parameters and click **Buy Now**.

   Table 1-12 describes the key parameters for creating VPN connections.

   Table 1-12 Description of VPN connection parameters

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

Parameter	Description	Value
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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the PSK, confirm PSK, and policy template for the VPN gateway IP address of connection 1.	*Set parameters based on the site requirements.*
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Template	The policy settings must be the same as those on the customer gateway device.	Default
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** It is recommended that the configuration of connection 2 be the same as that of connection 1.	Enabled

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

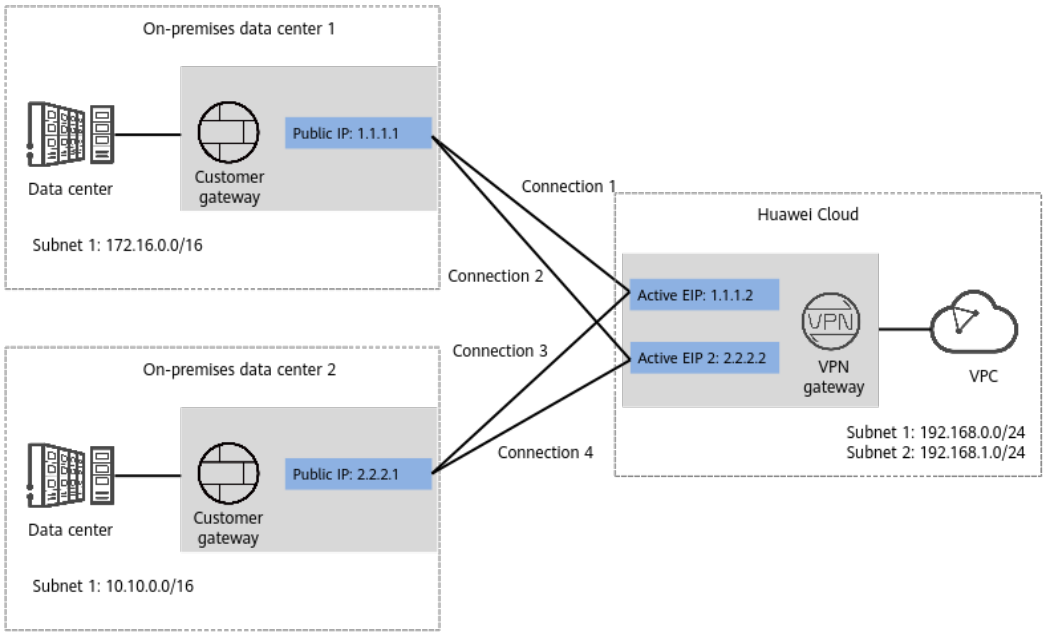
Scenario

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 1-13 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
On-premises data center 1	Subnet that needs to access the VPC	172.16.0.0/16
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 as follows: 1.1.1.1

Category	Item	Data
VPN connections of on-premises data center 1	Tunnel interface addresses under **Connection 1's Configuration**	IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30
On-premises data center 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 as follows: 2.2.2.1
VPN connections of on-premises data center 2	Tunnel interface addresses under **Connection 1's Configuration**	IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.72.1/30 • Customer tunnel interface address: 169.254.72.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.73.1/30 • Customer tunnel interface address: 169.254.73.2/30
IKE and IPsec policies	PSK	Test@123

Category	Item	Data
	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**.
  - 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 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 S2C VPN Gateway**.

2. Set parameters as prompted.

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

   Table 1-14 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
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 1-15 only describes the key parameters for creating a customer gateway.

   Table 1-15 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw1

Parameter	Description	Value
Identifier	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 **Create VPN Connection**.
2. Set VPN connection parameters and click **Buy Now**.

   Table 1-16 only describes the key parameters for creating VPN connections.

Table 1-16 Description of VPN connection parameters

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

Parameter	Description	Value
Customer Subnet	Subnet in 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
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.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123

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

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 **Create VPN Connection**.
2. Set VPN connection parameters and click **Buy Now**.

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

Table 1-17 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-002
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	2.2.2.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2

Parameter	Description	Value
Customer Gateway of Connection 2	Customer gateway of connection 2.	2.2.2.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	10.10.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.72.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.72.2/30

Parameter	Description	Value
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.73.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.73.2/30

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

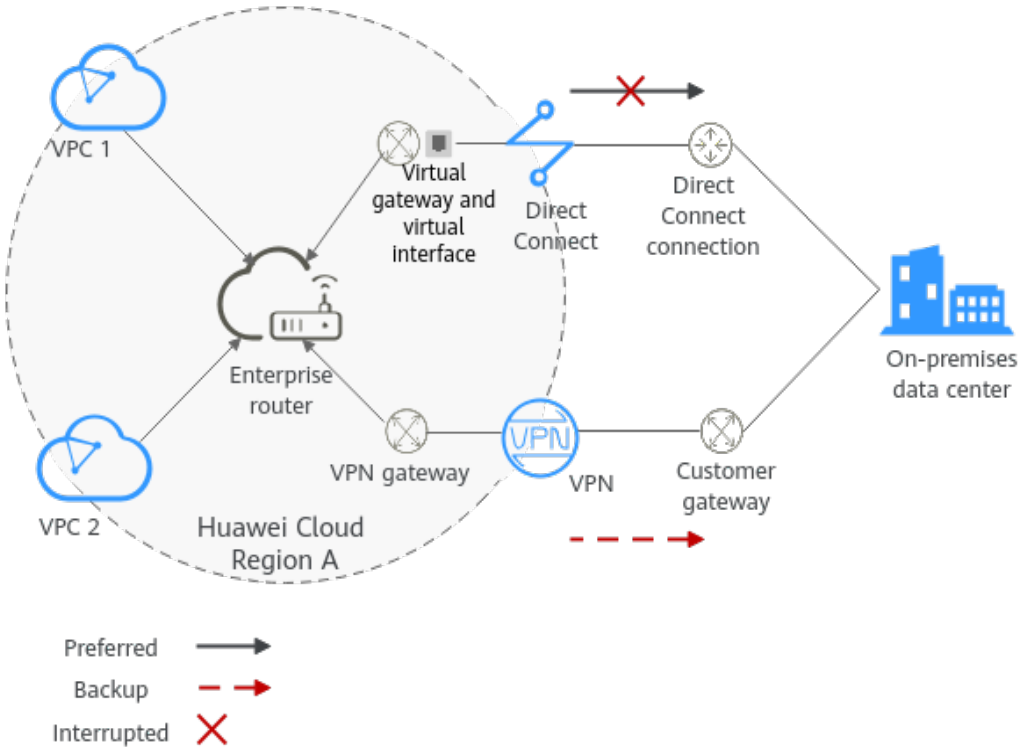
For more information about enterprise routers, see **Enterprise Router Overview**.

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

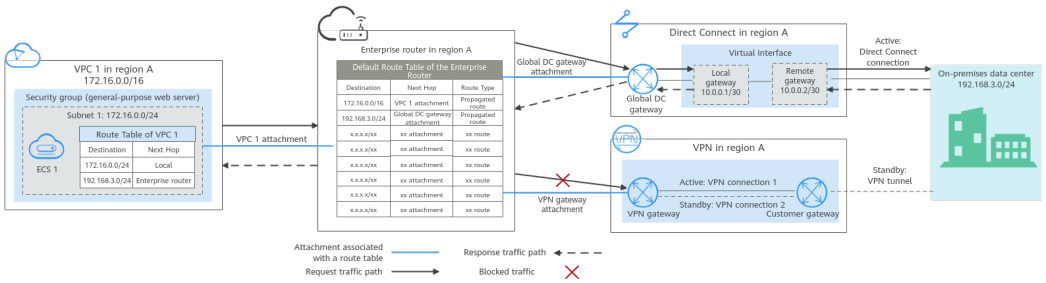
To attach both Direct Connect and VPN connections to an enterprise router to allow them to work in active/standby mode, you need to:

- **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 1-19** describes the network planning.

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



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's route table. The routes of a global DC gateway attachment have a higher priority than those of a VPN gateway attachment. As such, 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 1-18** shows the details about the traffic flows in this example.

Table 1-18 Network traffic flows

Path	Description
Request from VPC 1 to the on-premises data center	1. Traffic is forwarded to the enterprise router according to a route with the next hop being the enterprise router in the route table of VPC 1. 2. The enterprise router forwards traffic to the global DC gateway according to a route with the next hop being the global DC gateway attachment in its route table. 3. The global DC gateway forwards traffic to the Direct Connect connection through the remote gateway of the connected virtual interface. 4. Traffic is then forwarded to the on-premises data center over the Direct Connect connection.
Response from the on-premises data center to VPC 1	1. Traffic is forwarded to the virtual interface through the Direct Connect connection. 2. The virtual interface forwards traffic to the connected global DC gateway through its local gateway. 3. The global DC gateway forwards traffic to the enterprise router. 4. The enterprise router forwards traffic to VPC 1 according to a route with the next hop being VPC 1 attachment in its route table.

Table 1-19 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 1-20** shows the route.
	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 global DC gateway that is attached to an enterprise router. • One virtual interface that connects to the global DC gateway and the Direct Connect connection.
VPN	• One VPN gateway that is attached to the enterprise router. • One customer gateway, which is the gateway in the on-premises data center. • A group of VPN connections that connect the VPN gateway and the customer gateway. The two VPN connections work in active/standby mode.

Resource	Description
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, so that the enterprise router can learn a route to the VPC CIDR block. For details, see **Table 1-21**. • Direct Connect – Associate the global DC gateway attachment with the default route table of the enterprise router. – Propagate the global DC gateway attachment to the default route table of the enterprise router, so that the enterprise router can learn the routes of Direct Connect. For details, see **Table 1-21**. • 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 1-21**.
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 1-20 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 1-21 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	Global DC gateway attachment: **dgw-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's route table. When both the DC and VPN connections are normal, there are propagated routes of the global DC gateway attachment and VPN gateway attachment destined for the on-premises data center. In this case, only the route of the global DC gateway attachment can be displayed in the route table of the enterprise router as it has a higher priority than the route of the VPN gateway attachment. All routes of the VPN gateway attachment (including those not preferred) will not be displayed in the route table of the enterprise router.
- 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 1-22 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.
		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** – Global DC gateway attachment: **er-attach-DGW** – VPN gateway attachment: **er-attach-VPN**

Resource	Quantity	Description
Direct Connect	1	Connection: Create one based on site requirements.
		Global DC gateway • **Name**: Set it based on site requirements. In this example, **dgw-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**.
		Virtual interface • **Name**: Set it based on site requirements. In this example, **vif-demo** is used. • **Global DC Gateway**: In this example, select **dgw-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 used by the on-premises data center, which must be different from the ASN of the global DC 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 global DC gateway because 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**.

Resource	Quantity	Description
		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 Direct Connect virtual interface as the Direct Connect and VPN connections back up each other. In this example, **65525** is used.
		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, 64-bit) 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

- As Direct Connect and VPN connections back up each other, the global DC gateway and the VPN gateway must use the same ASN to prevent network loops. In this example, **64512** is used.
- The ASN of the enterprise router can be the same as or different from those of the global DC 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 1-23 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 1-23 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: Attach the Global DC Gateway 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 global DC gateway and attach it to the enterprise router. 3. Create a virtual interface to connect the global DC gateway to 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.

Procedure	Description
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, which is the gateway in the data center. 3. Create a group of VPN connections that connect the VPN gateway and the customer gateway. The two VPN connections work in active/standby mode. 4. Configure routes on the router in the on-premises data center.
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 1-22**.

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: Attach the Global DC Gateway to the Enterprise Router

For details about Direct Connect resources, see **Table 1-22**.

Step 1 Create a connection.

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

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

1. On the Direct Connect console, create a global DC gateway.

   For details, see **Creating a Global DC Gateway**.

2. On the enterprise router console, view the global DC gateway attachment created for the enterprise router.

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

   If the status of the global DC gateway attachment is **Normal**, the attachment has been successfully created.

   Default Route Table Association and **Default Route Table Propagation** are enabled when the enterprise router is created. After the global DC gateway is attached to the enterprise router, the system will automatically:

   - Associate the global DC gateway attachment with the default route table of the enterprise router.
   - Propagate the global DC gateway attachment to the default route table of the enterprise router, so that 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 global DC gateway to 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 1-19** and **Table 1-21**.

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 1-20**.

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 1-22**.

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 active and standby VPN connections. For details, see **Creating VPN Connections**.

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

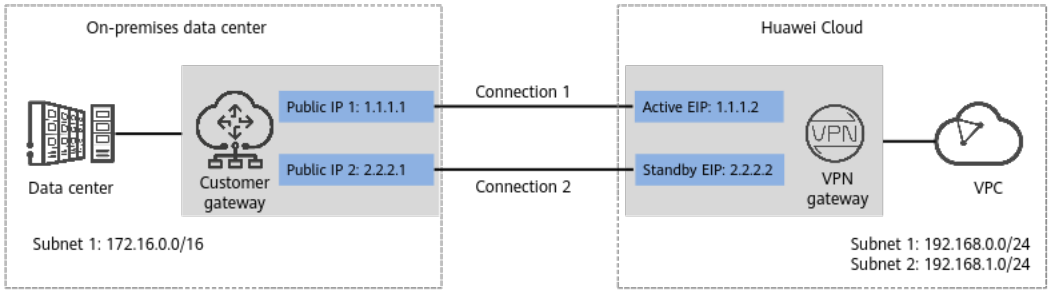
To meet service requirements, enterprise A needs to implement communication between its on-premises data center and a VPC on the cloud. For reliability

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 1-24 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/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 addresses under **Connection 1's Configuration**	IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16

Category	Item	Data
Customer gateway	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP addresses are as follows: • Public IP address 1: 1.1.1.1 • Public IP address 2: 2.2.2.1
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**.
  - 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 S2C VPN Gateway**.
2. Set parameters as prompted.

   Table 1-25 only describes the key parameters for creating a VPN gateway.

Table 1-25 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
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 1-26 only describes the key parameters for creating a customer gateway.

   Table 1-26 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar01
Identifier	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 1-27 only describes the key parameters for creating a customer gateway.

   Table 1-27 Parameters for the second customer gateway

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-ar02
Identifier	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 **Create VPN Connection**.
2. Set VPN connection parameters and click **Buy Now**.

   Table 1-28 only describes the key parameters for creating VPN connections.

Table 1-28 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	2.2.2.1
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*

Parameter	Description	Value
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK 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
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

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

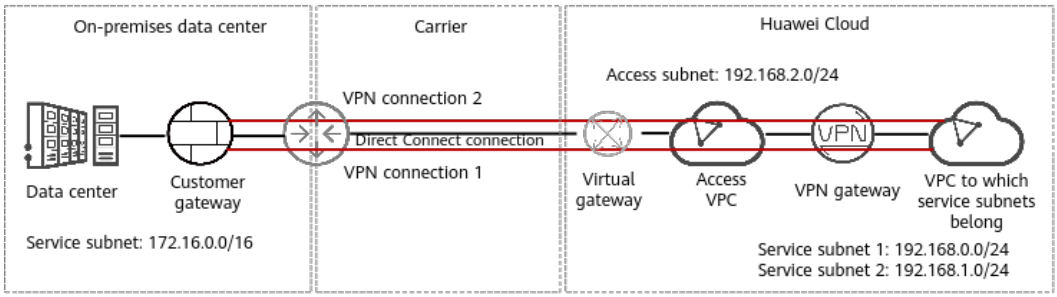
Scenario

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



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 1-29 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
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

Category	Item	Data
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
	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

Category	Item	Data
VPN connection	Tunnel interface addresses under **Connection 1's Configuration**	IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	• Local tunnel interface address: 169.254.71.1/30 • Customer tunnel interface address: 169.254.71.2/30
Customer gateway	Gateway IP address	This IP address is planned and configured by the administrator of the on-premises data center. 172.16.0.111
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

1.7.3 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 1-30 Parameters for creating a connection

Parameter	Description	Value
Connection Name	Name of a connection.	phlk_01

Step 4 Create a virtual gateway.

Table 1-31 only describes the key parameters for creating a virtual gateway. For details about all parameters, see **Create a Virtual Gateway**.

Table 1-31 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
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 1-32 only describes the key parameters for creating a virtual interface. For details about all parameters, see **Creating a Virtual Interface**.

Table 1-32 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

Parameter	Description	Value
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 S2C VPN Gateway**.
2. Set parameters as prompted.

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

Table 1-33 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
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

Parameter	Description	Value
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
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 1-34 only describes the key parameters for creating a customer gateway.

Table 1-34 Description of customer gateway parameters

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

Parameter	Description	Value
Identifier	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 **Create VPN Connection**.
2. Set VPN connection parameters and click **Buy Now**.

   Table 1-35 only describes the key parameters for creating VPN connections.

Table 1-35 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Private IP address bound to the VPN gateway.	192.168.2.100
Customer Gateway of Connection 1	Customer gateway of connection 1.	172.16.0.111
VPN Gateway IP of Connection 2	Another private IP address bound to the VPN gateway.	192.168.2.101
Customer Gateway of Connection 2	Customer gateway of connection 2.	172.16.0.111
VPN Type	Select **Static routing**.	Static routing

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.70.2/30
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

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

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

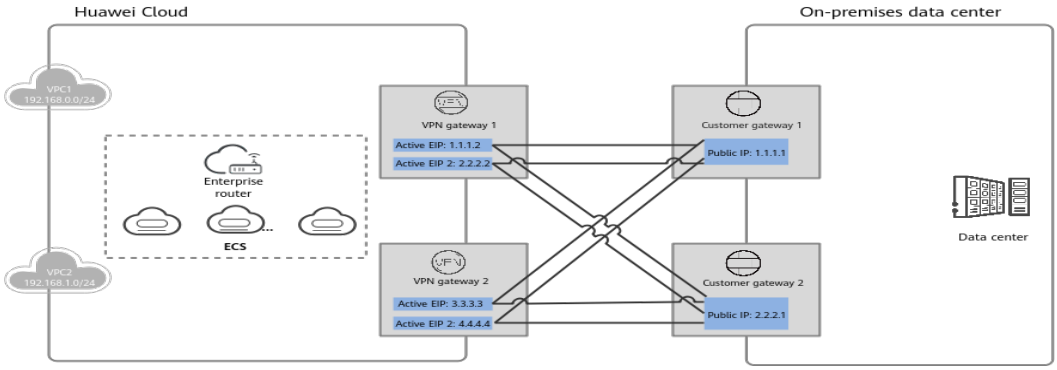
Scenario

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 1-36 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 addresses under **Connection 1's Configuration**	IP addresses used to establish an IPsec tunnel between VPN gateway 1 and customer gateway 1. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● Local tunnel interface address: 169.254.70.1/30 ● Customer tunnel interface address: 169.254.70.2/30 IP addresses used to establish an IPsec tunnel between VPN gateway 1 and customer gateway 2. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● Local tunnel interface address: 169.254.71.1/30 ● Customer tunnel interface address: 169.254.71.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	IP addresses used to establish an IPsec tunnel between VPN gateway 1 and customer gateway 1. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● Local tunnel interface address: 169.254.72.1/30 ● Customer tunnel interface address: 169.254.72.2/30 IP addresses used to establish an IPsec tunnel between VPN gateway 1 and customer gateway 2. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● Local tunnel interface address: 169.254.73.1/30 ● Customer tunnel interface address: 169.254.73.2/30
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

Category	Item	Data
	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
	Tunnel interface addresses under **Connection 1's Configuration**	IP addresses used to establish an IPsec tunnel between VPN gateway 2 and customer gateway 1. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.74.1/30 • Customer tunnel interface address: 169.254.74.2/30 IP addresses used to establish an IPsec tunnel between VPN gateway 2 and customer gateway 2. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.75.1/30 • Customer tunnel interface address: 169.254.75.2/30
	Tunnel interface addresses under **Connection 2's Configuration**	IP addresses used to establish an IPsec tunnel between VPN gateway 2 and customer gateway 1. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.76.1/30 • Customer tunnel interface address: 169.254.76.2/30 IP addresses used to establish an IPsec tunnel between VPN gateway 2 and customer gateway 2. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.77.1/30 • Customer tunnel interface address: 169.254.77.2/30
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

Category	Item	Data
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
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
	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 four 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 1-37 describes the parameter settings for VPN gateway 1.

Table 1-37 Parameter settings for VPN gateway 1

Parameter	Description	Value
Name	VPN gateway name.	vpngw-001
Network Type	Select **Public network**.	Public network
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 1-38 Parameter settings for VPN gateway 2

Parameter	Description	Value
Name	VPN gateway name.	vpngw-002

Parameter	Description	Value
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 1-39 describes the parameter settings for customer gateway 1.

   Table 1-39 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

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 1-40 Parameter settings for customer gateway 2

Parameter	Description	Value
Name	Customer gateway name.	cgw-fw2

Parameter	Description	Value
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. Create the first group of VPN connections and click **Buy Now**.

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

Table 1-41 Parameter settings for the first group of VPN connections

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

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the 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, 100.64.0.0/12, and 214.0.0.0/8 cannot be used as customer subnets. The reserved CIDR blocks vary according to regions and are subject to those displayed on the console. If you need to use 100.64.0.0/10 or 100.64.0.0/12, **submit a service ticket**.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
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.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123

Parameter	Description	Value
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.72.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.72.2/30

3. Create the second group of VPN connections.

   NOTE

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

Table 1-42 Parameter settings for the second group of VPN connections

Parameter	Description	Value
Name	VPN connection name.	vpn-002
VPN Gateway IP of Connection 1	Active EIP of VPN gateway 1.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	2.2.2.1
VPN Gateway IP of Connection 2	Active EIP 2 of VPN gateway 1.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	2.2.2.1

Parameter	Description	Value
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	*Set parameters based on the site requirements.*
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.71.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway.	169.254.71.2/30
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. **NOTE** If you disable **Same as that of connection 1**, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.73.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.73.2/30

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

Scenario

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

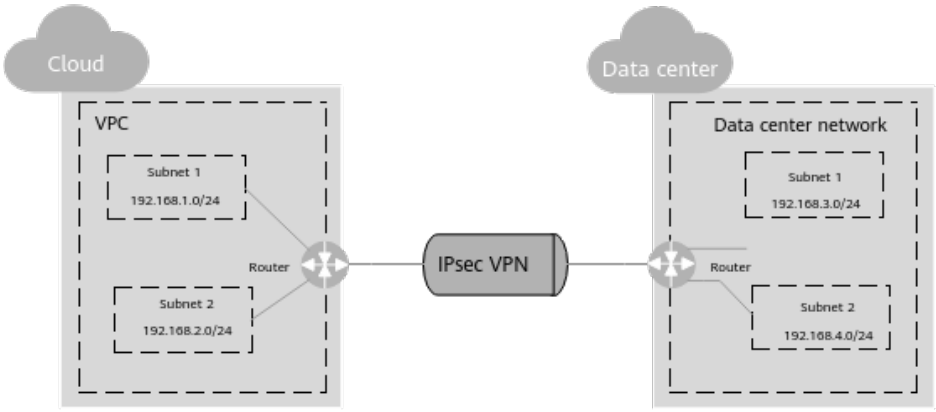
You have created the VPC and subnets that the on-premises data center wants to access.

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.

2.2 Setting Up a Cross-Border Network Using VPN and CC

2.2.1 Overview

Scenario

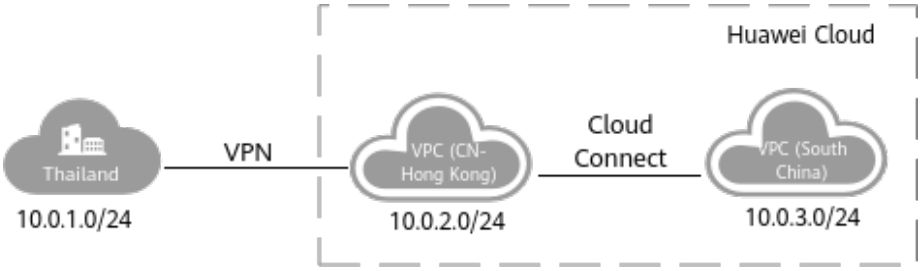
A large multinational company deploys its data center in Thailand and its cloud services in a South China region of Huawei Cloud. The company has cross-border service access requirements. If the data center in Thailand is directly connected to a VPC in the South China region through VPN, the network may be unstable.

This solution uses the Cloud Connect and VPN services to implement stable cross-border network connections.

Networking

Use the VPN service to connect the data center to the nearest Huawei Cloud VPC, for example, a VPC in the CN-Hong Kong region. Then, use Cloud Connect to connect VPCs in different regions, for example, the VPC in the CN-Hong Kong region and a VPC in the South China region, as shown in **Figure 2-2**.

Figure 2-2 Networking diagram



Solution Advantages

- Reliable connection and stable network
- Multiple payment modes including pay-per-use

2.2.2 Resources and Fees

Table 2-1 lists the resources and corresponding fees involved in this solution. For details, see **Pricing Details** at the Huawei Cloud official website.

Table 2-1 Resources and fees

Service	Configuration Example	Estimated Fee/Month
VPN	Pay-per-use: The VPN gateway bandwidth price is $2.8 USD/hour, and the VPN connection price is $0.05 USD/hour. For more information, see **Pricing Details**. • Region: CN-Hong Kong • Billing mode: pay-per-use • Billed by bandwidth • Bandwidth: 100 Mbit/s	$2052.46 USD

Service	Configuration Example	Estimated Fee/Month
Cloud Connect	Monthly billing: $11996.85 USD/month. For more information, see **Pricing Details**. • Billing mode: yearly/monthly • Billed by bandwidth • Interconnection type: inter-region interconnection • Interconnected regions: a region in Chinese mainland and a region in Asia Pacific • Bandwidth: 100 Mbit/s	$11996.85 USD
Total	—	$14049.31 USD

2.2.3 Procedure (Manual)

2.2.3.1 Configuring VPN

Step 1 Configure the VPN service in the CN-Hong Kong region of Huawei Cloud.

1. Click in the upper left corner and select the CN-Hong Kong region.
2. Choose **Networking** > **Virtual Private Network**.
3. In the navigation pane on the left, choose **Virtual Private Network** > **Classic**.
4. On the **VPN Gateways** page, click **Buy VPN Gateway**.
5. Configure parameters based on **Table 2-2** and click **Buy Now**.

Table 2-2 Descriptions of VPN gateway parameters

Parameter	Description	Example Value
Billing Mode	VPN gateways in this region can be billed on a pay-per-use basis.	Pay-per-use
Region	The networks in different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users. In this example, select **CN-Hong Kong**.	CN-Hong Kong
Name	Name of a VPN gateway.	vpcgw-001

Parameter	Description	Example Value
VPC	Name of the VPC to which the VPN gateway connects. Select a VPC in the CN-Hong Kong region.	vpc-001
Type	VPN type. The default value is **IPsec**.	IPsec
Billed By	Pay-per-use billing includes two modes: billed by bandwidth and billed by traffic. – **Bandwidth**: You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth. – **Traffic**: You need to specify a bandwidth limit and pay for the traffic you generate.	Traffic
Bandwidth (Mbit/s)	Bandwidth of the VPN gateway, in Mbit/s. The bandwidth is shared by all VPN connections created for the VPN gateway. The total bandwidth of all VPN connections created for a VPN gateway cannot exceed the VPN gateway bandwidth. During the use of VPN, if the network traffic exceeds the VPN gateway bandwidth, network congestion may occur and VPN connections may be interrupted. As such, ensure that you configure enough bandwidth. You can configure alarm rules on Cloud Eye to monitor the bandwidth.	100

Table 2-3 Description of VPN connection parameters

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

Parameter	Description	Example Value
Local Subnet	VPC subnets that need to access the on-premises network through VPN. Select **Specify CIDR Block**, and enter subnets in the CN-Hong Kong and South China regions to ensure that traffic from the South China region can also enter the VPN tunnel. In this example, enter **10.0.2.0/24** and **10.0.3.0/24**.	10.0.2.0/24, 10.0.3.0/24
Remote Gateway	Address of the VPN gateway in the on-premises data center. Set this parameter to the address of the VPN gateway in the on-premises data center in Thailand.	-
Remote Subnet	Subnets of the on-premises network that need to access a VPC through VPN In this example, enter **10.0.1.0/24**.	10.0.1.0/24
PSK	Pre-shared key, which is a private key shared by the two ends of a VPN connection. The PSK configurations at both ends of a VPN connection must be the same. This key is used for VPN connection negotiation. The PSK: – Must contain 6 to 128 characters. – Can contain only: ▪ Digits ▪ Letters ▪ Special characters ~`!@#$ %^()-_+=[]{}|\,./:;	Test@123
Confirm PSK	Reenter the pre-shared key.	Test@123
Advanced Settings	– **Default**: Use default IKE and IPsec policies. – **Custom**: Use custom IKE and IPsec policies. For details about the policies, see **Table 2-4** and **Table 2-5**.	Custom

Table 2-4 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The options include **SHA1**, **SHA2-256**, **SHA2-384**, **SHA2-512**, and **MD5** The default value is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The options include **AES-128**, **AES-192**, **AES-256**, and **3DES (Insecure. Not Recommended.)**. The default value is **AES-128**.	AES-128
DH Algorithm	Diffie-Hellman key exchange algorithm. The options include **Group 1**, **Group 2**, **Group 5**, **Group 14** , **Group 15**, **Group 16**, **Group 19**, **Group 20**, and **Group 21** The default value is **Group 14**. DH algorithms configured at both ends of a VPN connection must be the same. Otherwise, the negotiation will fail.	Group 14
Version	IKE key exchange protocol version. The options include **v1** (not recommended due to security risks) and **v2**. The default value is **v2**.	v2
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **86400**.	86400
Negotiation Mode	This parameter is available only when **Version** is set to **v1**. You can set **Negotiation Mode** to **Main** or **Aggressive**. The default mode is **Main**.	Main

Table 2-5 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The options include **SHA1**, **SHA2-256**, **SHA2-384**, **SHA2-512**, and **MD5** The default value is **SHA2-256**.	SHA2-256

Parameter	Description	Example Value
Encryption Algorithm	Encryption algorithm. The options include **AES-128**, **AES-192**, **AES-256**, and **3DES (Insecure. Not Recommended.)**. The default value is **AES-128**.	AES-128
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. The PFS algorithm can be **DH group 1**, **DH group 2**, **DH group 5**, **DH group 14**, **DH group 15**, **DH group 16**, **DH group 19**, **DH group 20**, or **DH group 21**. The default value is **DH group 14**.	DH group 14
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The options include **AH**, **ESP**, and **AH-ESP**. The default value is **ESP**.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **3600**.	3600

CAUTION

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

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

Step 2 Configure the VPN gateway in the on-premises data center in Thailand.

Configure VPN on the VPN gateway device in the on-premises data center.

NOTE

Configure an ACL referenced by the IPsec policy as follows:

- Source CIDR block: 10.0.1.0/24
- Destination CIDR blocks: 10.0.2.0/24 and 10.0.3.0/24

----End

2.2.3.2 Configuring Cloud Connect

Step 1 Buy a cloud connection in the Cloud Connect service.

1. Log in to the management console.
2. Choose **Networking** > **Cloud Connect**.
3. On the **Cloud Connections** page, click **Create Cloud Connection**.
4. Configure cloud connection parameters based on **Table 2-6**.

Table 2-6 Description of cloud connection parameters

Parameter	Description
Name	Name of a cloud connection. The value is a string of 1 to 64 characters, which can contain letters, digits, underscores (_), hyphens (-), and periods (.).
Tag	A tag identifies a Cloud Connect resource. It consists of a key and a value. You can add a maximum of 10 tags for a cloud connection.
Description	Description of the cloud connection. The value is a string of 0 to 255 characters.

Table 2-7 Tag key and value requirements of the Cloud Connect service

Parameter	Requirement
Key	– Cannot be left blank. – Must be unique for each resource. – Can contain a maximum of 36 characters. – Can contain only letters, digits, hyphens (-), and underscores (_).
Value	– Can be left blank. – Can contain a maximum of 43 characters. – Can contain only letters, digits, periods (.), hyphens (-), and underscores (_).

5. Click **OK**. The cloud connection is created.

Step 2 Load network instances.

Add the VPCs in the CN-Hong Kong and South China regions to the cloud connection.

NOTE

- Table 2-8 lists the parameters required to load the VPC in the CN-Hong Kong region to the cloud connection.
- When loading the VPC in the South China region, you only need to specify the subnet 10.0.3.0/24. The subnet 10.0.1.0/24 in Thailand does not need to be repeatedly specified.

Table 2-8 Parameters for loading a VPC

Parameter	Description	Example Value
Account	Whether the VPC is from your account or the other user's account.	Current account
Region	Region where the VPC to be loaded is located.	CN-Hong Kong
Instance Type	Type of the instance to be loaded to the cloud connection.	VPC
VPC	Name of the VPC to be loaded to the cloud connection. Select the VPC created in Step 1.5.	vpc-001
VPC CIDR Block	CIDR block of the VPC to be loaded to the cloud connection. When **Instance Type** is set to **VPC**, configure the following two parameters: • **Subnet**: Select the subnet of the VPC, which is 10.0.2.0/24 in this example. • **Other CIDR Block**: Enter CIDR block 10.0.1.0/24 so that data can be transmitted to the on-premises data center over the cloud connection.	Subnet: 10.0.2.0/24 Other CIDR Block: 10.0.1.0/24

Step 3 Configure the inter-region bandwidth.

1. Log in to the management console.
2. Choose **Networking** > **Cloud Connect**.

3. In the cloud connection list, click the name of the target cloud connection.
4. Click the **Inter-Region Bandwidths** tab.
5. Click **Assign Inter-Region Bandwidth** and configure the parameters based on **Table 2-9**.

Table 2-9 Description of inter-region bandwidth parameters

Parameter	Description
Regions	Regions of the network instances that need to communicate with each other. Select two regions.
Bandwidth Package	Bandwidth package to be bound to the cloud connection.
Bandwidth	Bandwidth required for communication between the two regions. The sum of all inter-region bandwidths you assign cannot exceed the total bandwidth of the bandwidth package.

6. Click **OK**.

   Now the network instances in the two regions can communicate with each other.

   NOTE

   The default security group rules deny incoming traffic. Ensure that security group rules in both directions are correctly configured for resources in the regions to ensure normal communication.

Step 4 View route information.

The VPC in the CN-Hong Kong region needs to have a route to 10.0.1.0/24 and a route to 10.0.2.0/24.

The VPC in the South China region needs to have a route to 10.0.3.0/24.

1. Log in to the management console.
2. Choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, click the name of the target cloud connection. On the displayed page, click the **Route Information** tab.
4. Select the target region from the drop-down list.
5. View routes in the list.

----End

2.2.3.3 Verification

Step 1 Create a VM in the South China region and deploy services on it.

Step 2 Ping a host in the on-premises data center in Thailand from the VM in the South China region.

The network communication is normal if the ping is successful. You can view the IPsec VPN tunnel information on the VPN gateway in the on-premises data center. The method of checking the IPsec VPN tunnel information varies according to the VPN device models.

----End

2.3 Using VPN and Cloud Connect to Enable Communication Between On-Premises Data Centers and Multiple VPCs on Huawei Cloud

Scenario

To use VPN to connect to Huawei Cloud, create a VPC in each Huawei Cloud region. Configure Cloud Connect connections to enable communication between your on-premises data center and VPC subnets in multiple regions.

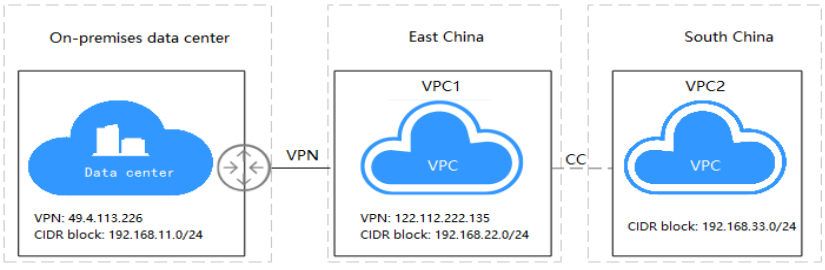
NOTE

Multiple VPCs in the same region can also be connected through Cloud Connect connections.

Prerequisites

1. Prepared resources
   - You have purchased VPN connections to connect your on-premises data center to the VPCs on Huawei Cloud.
   - You have created VPCs in multiple regions, and the subnets of each VPC do not conflict with each other. The ECS service in VPCs is running properly.
2. Topology

   Figure 2-3 Using VPN together with Cloud Connect



NOTE

- Subnet of your on-premises data center: 192.168.11.0/24; VPN gateway IP address: 49.4.113.226
- VPC1 subnet: 192.168.22.0/24; VPN gateway address: 122.112.222.135
- VPC2 subnet: 192.168.33.0/24

3. Configuration overview

Table 2-10 Configuration description

On-premises Data Center	VPC1 (East China)	VPC2 (South China)
VPN connection subnet configuration Local gateway: 49.4.113.226 Local subnet: 192.168.11.0/24 Remote subnet: 192.168.22.0/24 192.168.33.0/24 Remote gateway: 122.112.222.135 The local and remote gateway IP addresses in the on-premises data center and VPC1 are reversed. The VPN configurations in the on-premises data center are consistent with those of VPC1.	VPN connection subnet configuration Local gateway: 122.112.222.135 Local subnet: 192.168.22.0/24 192.168.33.0/24 Remote gateway: 49.4.113.226 Remote subnet: 192.168.11.0/24 Cloud Connect network instance configuration Network instance: 192.168.22.0/24 192.168.11.0/24	Cloud Connect network instance configuration Network instance: 192.168.33.0/24

NOTE

Cloud Connect network instances can be configured at any region. You can check the route information to verify the network instance configuration.

4. Configuration roadmap
   - Use a cloud connection to connect VPC1 in East China to VPC2 in South China.
   - Keep the local subnet of the VPN connection in your on-premises data center unchanged, and change the remote subnet to 192.168.22.0/24 and 192.168.33.0/24.
   - Change the local subnet of the VPN connection in VPC1 to 192.168.22.0/24 and 192.168.33.0/24, and keep the remote subnet unchanged.

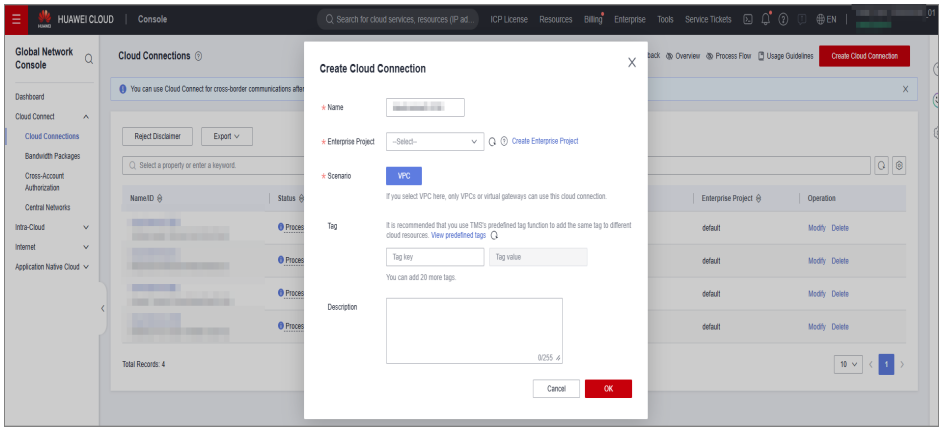
- The cloud connection of VPC1 updates the VPC CIDR blocks and adds 192.168.11.0/24 to the VPC subnet.
- The network information of VPC2 remains unchanged.
- Configure the inter-region bandwidth.
- Verify the route information of the cloud connection.

Procedure

Step 1 Create a cloud connection.

1. Log in to the console. Click **Service List** in the upper left corner. Under **Networking**, select **Cloud Connect**. In the navigation pane on the left, choose **Cloud Connections**. On the displayed page, click **Create Cloud Connection** in the upper right corner.
2. Configure required parameters and click **OK**.

Figure 2-4 Create Cloud Connection

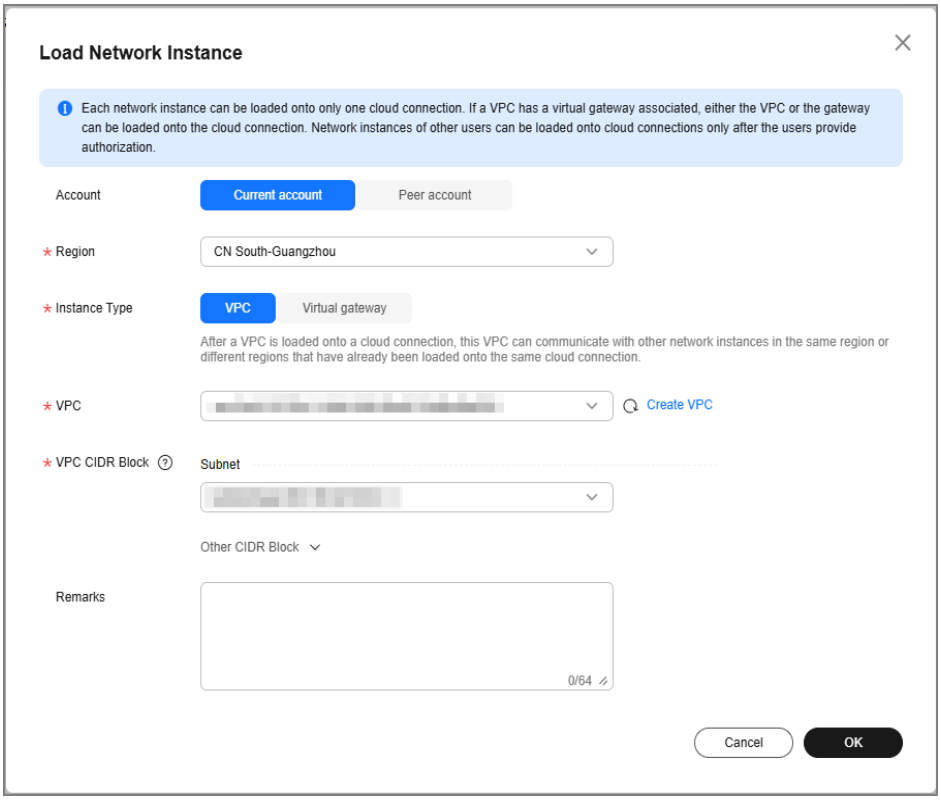


You can create a cloud connection in any region where the VPC is located. If you have two VPCs in the same region, you can use a VPC peering connection (with a lower latency) or a cloud connection to connect the two VPCs. If you have more than two VPCs, use cloud connections to connect them.

3. Click the cloud connection name.
4. Select the **Network Instances** tab and click **Load Network Instance**.

   Configure required parameters and click **OK**.

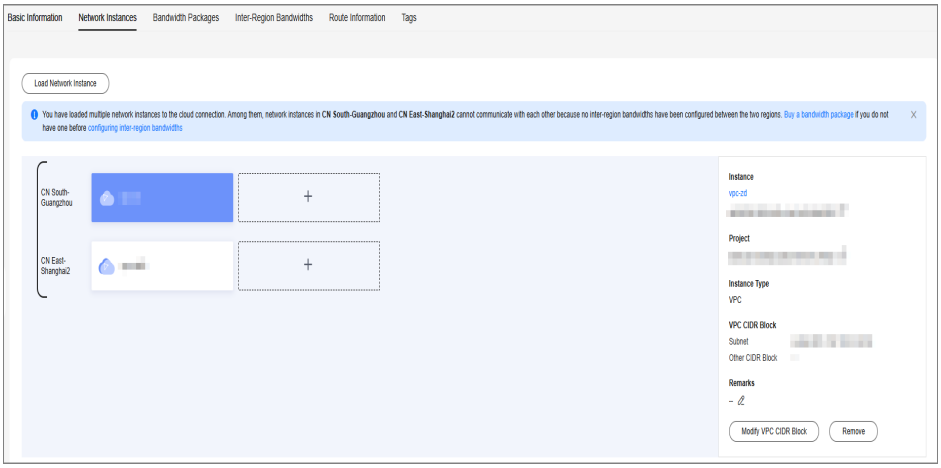
Figure 2-5 Loading network instance 1



5. Select **CN South-Guangzhou** for **Region**. Select VPC2. You can select some or all subnets for **Subnet**. You can also add VPC subnets by customizing CIDR blocks.

   Add VPC1 in the **CN East-Shanghai1** region and add its network configuration.

Figure 2-6 Loading network instance 2

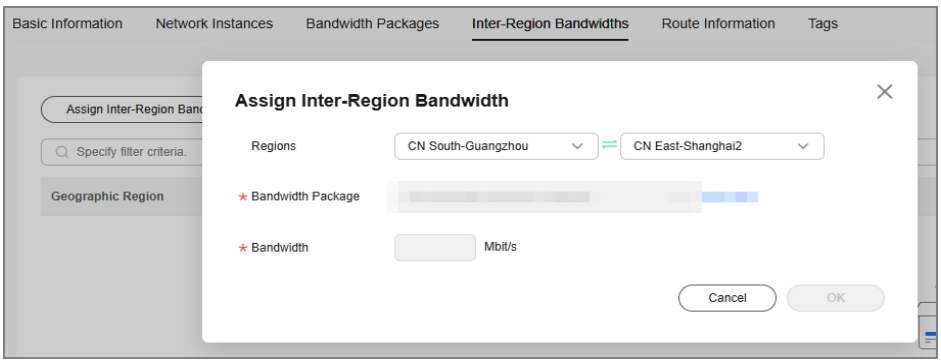


NOTE

- A cloud connection can be created using the same account or different accounts. If you want to create a cross-account connection, obtain authorization first.
- The system does not verify custom subnets.

6. Click the **Inter-Region Bandwidths** tab, and click **Configure Inter-Region Bandwidth**. If there are multiple regions, allocate the total bandwidth of the cloud connection among multiple regions based on the bandwidth usage in each region. In this example, the bandwidth is used for interconnection between two regions.

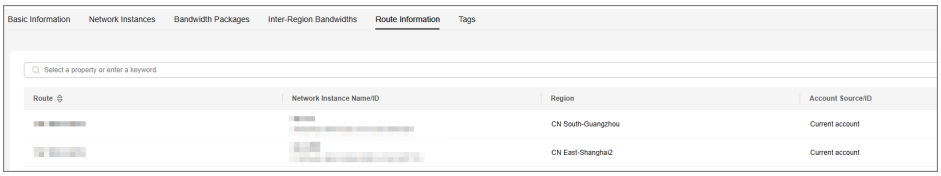
Figure 2-7 Configuring the inter-region bandwidth



7. To verify the route information, select the **Route Information** tab.

   Route information for interconnection between regions is displayed. The subnets in the route are the subnets that are interconnected through the cloud connection. At this time, the subnets of VPC1 and VPC2 can access each other.

Figure 2-8 Verifying the route information

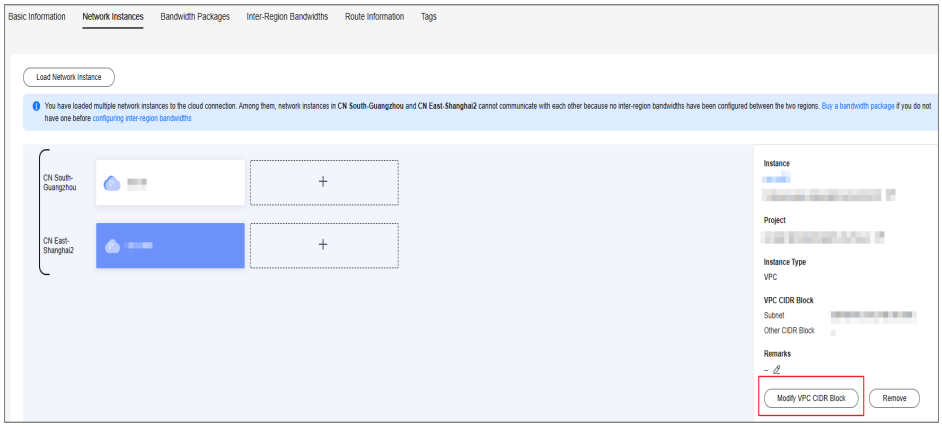


Step 2 Modify VPC CIDR blocks.

When you configure a network instance for the cloud connection between VPC1 and VPC2, the subnet connected to VPN is also considered to be connected to VPC1. Therefore, you need to modify the network instance of VPC1.

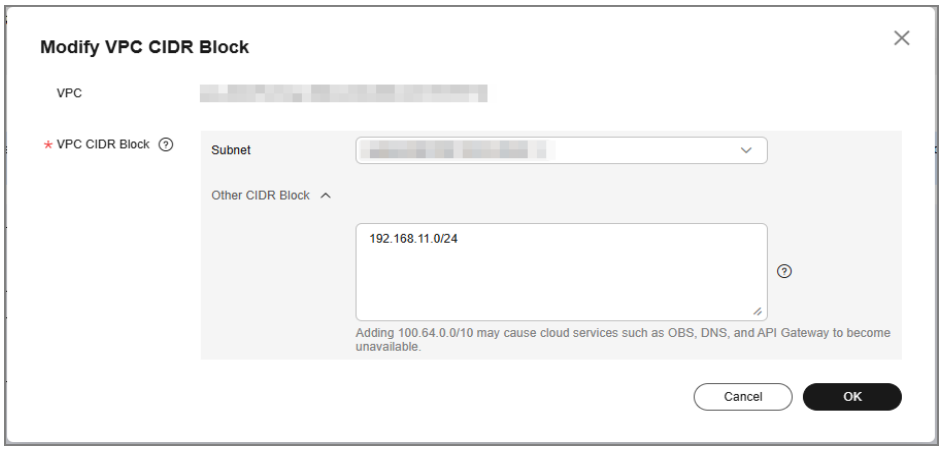
1. Click the cloud connection name to go to the cloud connection details page.
2. On the **Network Instances** tab page, select a network instance in the **CN East-Shanghai2** region.
3. Click **Modify VPC CIDR Block** on the right of the page.

Figure 2-9 Modifying the VPC CIDR block



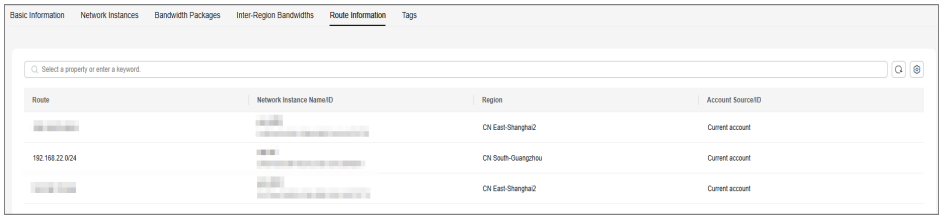
4. For **Other CIDR Block** in the **Advanced Settings** area, enter the CIDR block to which VPC1 connects through the VPN connection and click **OK**.

Figure 2-10 Modifying the VPC CIDR block



5. Verify the configuration update on the **Route Information** tab page.

Figure 2-11 Verifying the configuration update



Step 3 Update VPN configurations.

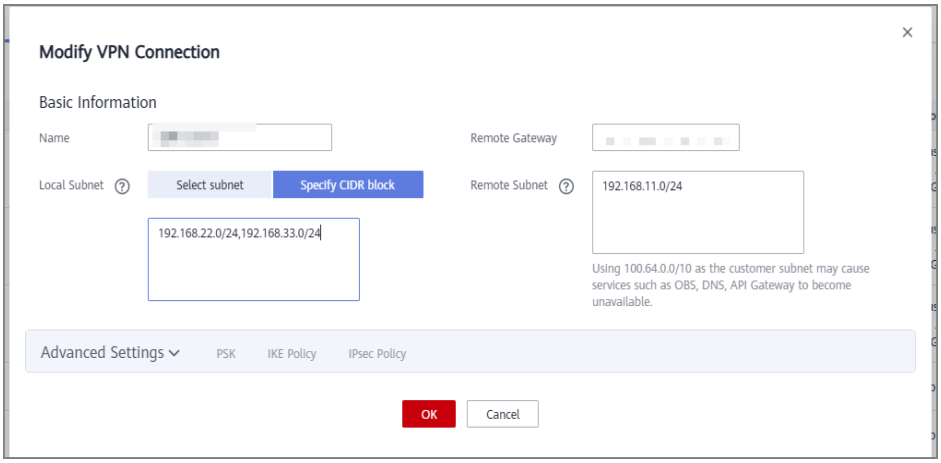
After VPC1 and VPC2 are connected through the cloud connection, the VPN subnet between user data center network and VPC1 changes. From the perspective of the VPN connection, the local subnet of VPC1 should contain the subnet of VPC1 and the subnet of VPC2 that is connected through the cloud connection, and the remote subnet of the client VPN also needs to be adjusted accordingly.

- On-premises data center: Keep the local subnet unchanged, and add the subnet of VPC2 as a remote subnet, which is 192.168.33.0/24 in this example.

- VPC1: Add a subnet of VPC2 to the local subnet. In this example, the subnet is 192.168.33.0/24, and the remote subnet remains unchanged.

1. Choose **Virtual Private Network** > **Classic**, locate the VPN connection created for VPC1, and choose **More** > **Modify** in the **Operation** column.
2. On the **Modify VPN Connection** page, select **Specify CIDR block** for **Local Subnet** and enter the subnets of VPC1 and VPC2. Use a comma (,) to separate the two subnets. Keep the remote subnet and other information unchanged.

   Figure 2-12 Modifying the VPN connection

3. Modify the remote subnet in the VPN configuration.

   Add the VPC1 and VPC2 subnets on Huawei Cloud to the remote subnet configuration of the VPN connection. Retain other configurations.

----End

Verification

In this environment, the user data center, VPC1, and VPC2 each has three ECSs deployed. The IP addresses of the three ECSs are 192.168.11.11, 192.168.22.170, and 192.168.33.33, respectively. ECS1 (192.168.11.11) can communicate with ECS2 (192.168.22.170) through VPN. ECS3 (192.168.33.33) cannot communicate with other two ECSs. After a cloud connection is established, ECS3 can communicate with ECS2 but cannot communicate with ECS1.

After updating the VPC CIDRs and VPN configurations, ECS1, ECS2, and ECS3 can communicate with each other.

- On-premises data center

  ECS1 can access ECS2 in the VPC1 subnet through the VPN connection.


```
[root@ecs--11 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.11  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::f816:3eff:fefc:eef5  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:fc:ee:f5  txqueuelen 1000  (Ethernet)
        RX packets 5325  bytes 503031 (491.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12328  bytes 1165686 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs--11 ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=61 time=30.8 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=61 time=30.0 ms
64 bytes from 192.168.22.170: icmp_seq=3 ttl=61 time=29.3 ms
```

ECS1 can access ECS3 in the VPC2 subnet.

```
[root@ecs--11 ~]# ping 192.168.33.33
PING 192.168.33.33 (192.168.33.33) 56(84) bytes of data.
64 bytes from 192.168.33.33: icmp_seq=1 ttl=59 time=64.2 ms
64 bytes from 192.168.33.33: icmp_seq=2 ttl=59 time=63.5 ms
64 bytes from 192.168.33.33: icmp_seq=3 ttl=59 time=63.2 ms
64 bytes from 192.168.33.33: icmp_seq=4 ttl=59 time=63.2 ms
```

- VPC1 on Huawei Cloud

  ECS2 in the VPC1 subnet can access ECS1 in the subnet of your on-premises data center.

```
[root@ecs-vpc2-22 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.22.170  netmask 255.255.255.0  broadcast 192.168.22.255
        inet6 fe80::f816:3eff:fe4d:4bbd  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:4d:4b:bd  txqueuelen 1000  (Ethernet)
        RX packets 1693564  bytes 600255226 (572.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1903616  bytes 3023942348 (2.8 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc2-22 ~]# ping 192.168.11.11
PING 192.168.11.11 (192.168.11.11) 56(84) bytes of data.
64 bytes from 192.168.11.11: icmp_seq=1 ttl=62 time=31.4 ms
64 bytes from 192.168.11.11: icmp_seq=2 ttl=62 time=29.4 ms
```

  ECS2 in the VPC1 subnet can access ECS3 in the VPC2 subnet.

```
[root@ecs-vpc2-22 ~]# ping 192.168.33.33
PING 192.168.33.33 (192.168.33.33) 56(84) bytes of data.
64 bytes from 192.168.33.33: icmp_seq=1 ttl=61 time=42.2 ms
64 bytes from 192.168.33.33: icmp_seq=2 ttl=61 time=36.7 ms
64 bytes from 192.168.33.33: icmp_seq=3 ttl=61 time=37.4 ms
```

- VPC2 on Huawei Cloud

  ECS3 in the VPC2 subnet can access ECS2 in the VPC1 subnet.


```
[root@ecs-vpc2-33 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.33.33  netmask 255.255.255.0  broadcast 192.168.33.255
        inet6 fe80::f816:3eff:fe23:c69e  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:23:c6:9e  txqueuelen 1000  (Ethernet)
        RX packets 10127  bytes 1005602 (982.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13258  bytes 1258814 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc2-33 ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=61 time=37.7 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=61 time=36.7 ms
64 bytes from 192.168.22.170: icmp_seq=3 ttl=61 time=36.5 ms
```

ECS3 in the VPC2 subnet can access ECS1 in the subnet of your on-premises data center.

```
[root@ecs-vpc2-33 ~]# ping 192.168.11.11
PING 192.168.11.11 (192.168.11.11) 56(84) bytes of data.
64 bytes from 192.168.11.11: icmp_seq=1 ttl=60 time=64.9 ms
64 bytes from 192.168.11.11: icmp_seq=2 ttl=60 time=63.7 ms
64 bytes from 192.168.11.11: icmp_seq=3 ttl=60 time=64.0 ms
```

2.4 Using VPN and VPC Peering to Enable Communication Between an On-Premises Data Center and Multiple VPCs in the Same Region

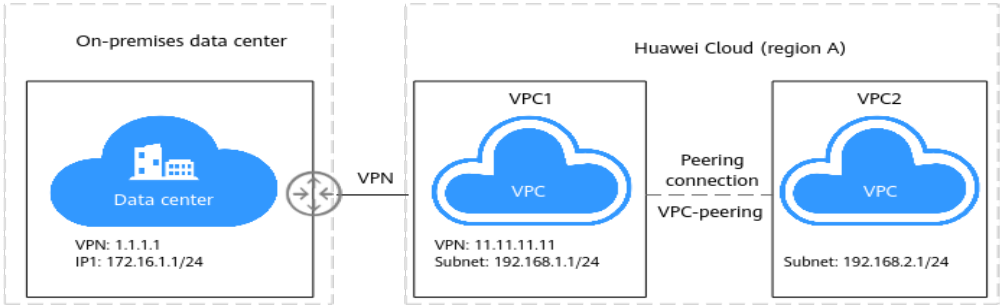
Scenario

Two VPCs are created in the same region on Huawei Cloud. The on-premises data center is connected to one of the VPCs through VPN. This section describes how to create a VPC peering connection between the two VPCs to enable communication between the on-premises data center and the two VPCs.

Prerequisites

1. Prepared resources
   - You have purchased VPN connections to connect your on-premises data center to a Huawei Cloud VPC.
   - You have created two VPCs, and the subnets of each VPC do not conflict with each other. ECSs in each VPC are running properly.
2. Topology

Figure 2-13 Using VPN with VPC peering



NOTE

- Subnet of your on-premises data center: 172.16.1.0/24; VPN gateway IP address: 1.1.1.1
- VPC1 subnet: 192.168.1.0/24, VPN gateway IP address: 11.11.11.11
- VPC2 subnet: 192.168.2.0/24

3. Configuration overview

Table 2-11 Configuration description

Item	On-premises Data Center	VPC1	VPC2
VPN connection subnet configuration	Local gateway: 1.1.1.1 Local subnet: 172.16.1.0/24 Remote subnets: 192.168.1.0/24 192.168.2.0/24 Remote gateway: 11.11.11.11 **NOTE** • The local and remote gateway IP addresses in the on-premises data center and VPC1 are reversed. • The VPN configurations in the on-premises data center are consistent with those of VPC1.	Local gateway: 11.11.11.11 Local subnets: 192.168.1.0/24 192.168.2.0/24 Remote gateway: 1.1.1.1 Remote subnet: 172.16.1.0/24	-
Routes for the VPC peering connection	-	Destination address: 192.168.2.0/24	Destination addresses: 172.16.1.0/24 and 192.168.1.0/24

Item	On-premises Data Center	VPC1	VPC2
Remarks	• In this example, VPC1 is specified as the local end and VPC2 as the remote end when a VPC peering connection is created. • Cloud Connect network instances can be configured at any region. You can check the route information to verify the network instance configuration.		

4. Configuration roadmap
   - Create a VPC peering connection between VPC1 and VPC2.
   - Keep the local subnet of the VPN connection in your on-premises data center unchanged, and change the remote subnets to 192.168.1.0/24 and 192.168.2.0/24.
   - Change the local subnets of the VPN connection in VPC1 to 192.168.1.0/24 and 192.168.2.0/24, and keep the remote subnet unchanged.
   - For the peering connection of VPC1, configure a local route to the subnet of VPC2, which is 192.168.2.0/24.
   - For the peering connection of VPC2, configure a remote route to the subnet of VPC1 (192.168.1.0/24) and another remote route to the subnet of the customer network (172.16.1.0/24).

Procedure

Step 1 Create a VPC peering connection.

1. Log in to the management console, select the region where the VPCs are located, and choose **Virtual Private Cloud** in the service list. Choose **VPC Peering Connections** from the navigation tree, and click **Create VPC Peering Connection**. On the displayed page, configure the local and peer VPCs, and click **OK**.

   When creating a VPC peering connection, check whether the CIDR blocks of the specified local and remote VPCs match. After the VPC peering connection is created, the VPC information cannot be modified, and you can only modify the VPC peering connection name and configure VPC routes.
2. Query information about the created VPC peering connection, including the local and remote VPC CIDR blocks. You need to add routes to enable communication between the local and remote VPC CIDR blocks.

   In this example, VPC1 connected to the on-premises data center through VPN is the local VPC, and VPC2 is the remote VPC.

Step 2 Add routes for the VPC peering connection.

1. For a common VPC peering connection, you only need to add routes to the subnets of the two VPCs. In this example, you also need to add a route to the on-premises data center because the local VPC is connected to the on-premises data center network through VPN. On the **VPC Peering Connections** page, click the name of the VPC peering connection to be edited. The page for adding routes is displayed.

2. Click **Add Route** in the **Associated Routes** area.

   On the page that is displayed, enter the destination network information. You can add multiple routes one by one.

   NOTE

   Although VPC1 connects to the on-premises data center through VPN, VPC2 connects to the on-premises data center through a VPC peering connection. As such, when configuring remote routes, you need to configure a route to the on-premises data center in addition to a route to the local subnet.

   The next-hop address of a route is automatically generated and does not need to be manually configured.

Step 3 Modify the VPN configuration.

1. After VPC 1 and VPC 2 are connected through the VPC peering connection, the VPN subnets between the on-premises data center network and VPC 1 change. From the perspective of the VPN connection, the local subnets of VPC 1 contain the subnet of VPC 1 and the subnet of VPC 2 that is connected through the VPC peering connection, and the remote subnet of the client VPN also needs to be adjusted accordingly.

   NOTE

   On-premises data center: Keep the local subnet unchanged, and add the subnet of VPC2 as a remote subnet, which is 192.168.2.0/24 in this example.

   VPC1: Add a subnet of VPC2 to the local subnet. In this example, the subnet is 192.168.2.0/24, and the remote subnet remains unchanged.

2. Choose **Virtual Private Network** > **Classic**, locate the VPN connection created for VPC1, and choose **More** > **Modify** in the **Operation** column.
3. On the **Modify VPN Connection** page, select **Specify CIDR block** for **Local Subnet**, and enter the subnets of VPC1 and VPC2. Use a comma (,) to separate the two subnets. Keep the remote subnet and other information unchanged.

   For the VPN configuration in the on-premises data center, you need to add the subnets of VPC1 and VPC2 to the remote subnet configuration.

----End

Verification

In this environment, the IP address of the ECSs in the on-premises data center, VPC1, and VPC2 are 172.16.1.1, 192.168.1.1, and 192.168.2.1, respectively. ECS1 (172.16.1.1) can communicate with ECS2 (192.168.1.1) through VPN. ECS3 (192.168.2.1) cannot communicate with the other two ECSs. After the VPC peering connection is established, ECS3 can communicate with ECS2 but cannot communicate with ECS1.

After the configuration adjustment in **3** is complete, ECS1, ECS2, and ECS3 can communicate with each other. The verification result is as follows:

- On-premises data center

  ECS1 can access ECS2 in the VPC1 subnet through the VPN connection.


```
[root@ecs-1 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.1    netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::f816:3eff:fe8c:1ec9  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:8c:1e:c9  txqueuelen 1000  (Ethernet)
        RX packets 1190  bytes 155372 (151.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1223  bytes 113478 (110.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-1 ~]# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=61 time=38.4 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=61 time=31.4 ms
```

ECS1 can access ECS3 in the VPC2 subnet.

```
[root@ecs-1 ~]# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=61 time=31.7 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=61 time=31.6 ms
```

- Huawei Cloud VPC1

  ECS2 in the VPC1 subnet can access ECS1 in the subnet of the on-premises data center.

```
[root@ecs-vpc1-11x ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1    netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fe43:2462  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:43:24:62  txqueuelen 1000  (Ethernet)
        RX packets 190954  bytes 61952364 (59.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 215881  bytes 253528145 (241.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc1-11x ~]# ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=61 time=33.8 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=61 time=31.6 ms
```

ECS2 in the VPC1 subnet can access ECS3 in the VPC2 subnet.

```
[root@ecs-vpc1-11x ~]# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=7.18 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=3.05 ms
```

- Huawei Cloud VPC2

  ECS3 in the VPC2 subnet can access ECS2 in the VPC1 subnet.

```
[root@ecs-vpc2-22 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.1    netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::f816:3eff:fe4d:4bbd  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:4d:4b:bd  txqueuelen 1000  (Ethernet)
        RX packets 138865  bytes 56965509 (54.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 160536  bytes 250433082 (238.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc2-22 ~]# ping 192.168.11.84
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=9.78 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=4.29 ms
```

ECS3 in the VPC2 subnet can access ECS1 in the subnet of the on-premises data center.

```
[root@ecs-vpc2-22 ~]# ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=61 time=34.0 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=61 time=31.7 ms
```


2.5 Using VPN and Cloud Connect to Enable Communication Between Multiple On-premises Data Centers Through the VPN Hub Function

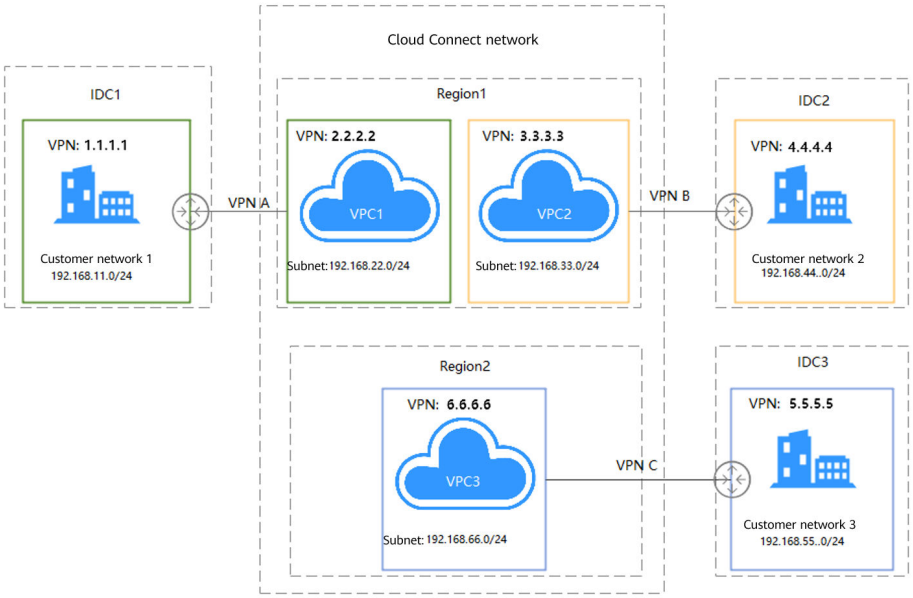
Scenario

A customer has multiple data centers in different regions and has purchased VPCs in multiple regions on Huawei Cloud. Each data center is connected to a VPC network on the cloud through VPN. This section describes how to use cloud connections in the same region and across different regions to connect multiple data center networks to enable communication between these data centers.

Prerequisites

1. **Prepared resources**
   - The customer has purchased VPCs in multiple regions on Huawei Cloud, with multiple VPCs in a certain region.
   - The VPC in each region is connected to an on-premises data center through VPN.
   - The subnets of the VPCs on Huawei Cloud do not conflict with those of the on-premises data centers, and the ECS service is running properly.
2. **Topology**

   Figure 2-14 VPN hub topology



3. **Configuration roadmap**

   a. Connect VPC1, VPC2, and VPC3 through Cloud Connect, and configure Cloud Connect routes. You need to purchase a bandwidth package during the actual network configuration.

b. Create VPN connections between IDC1 and VPC1, between IDC2 and VPC2, and between IDC3 and VPC3.

c. Update the local and remote subnets of each VPN connection.

4. **Configuration description**

Table 2-12 Configuration description

Node	Identifier	Local VPN Gateway	Local VPN Subnet	Remote VPN Gateway	Remote VPN Subnet	Cloud Connect Instance
IDC1	VPN A	49.4.113.226	192.168.11.0/24	122.112.222.135	192.168.22.0/24 192.168.33.0/24 192.168.44.0/24 192.168.55.0/24 192.168.66.0/24	-
VPC1		122.112.222.135	192.168.22.0/24 192.168.33.0/24 192.168.44.0/24 192.168.55.0/24 192.168.66.0/24	49.4.113.226	192.168.11.0/24	192.168.22.0/24 192.168.11.0/24
IDC2	VPN B	139.159.222.28	192.168.44.0/24	122.112.222.112	192.168.11.0/24 192.168.22.0/24 192.168.33.0/24 192.168.55.0/24 192.168.66.0/24	-

Node	Identifier	Local VPN Gateway	Local VPN Subnet	Remote VPN Gateway	Remote VPN Subnet	Cloud Connect Instance
VPC 2		122.112.222.112	192.168.11.0/24 192.168.22.0/24 192.168.33.0/24 192.168.55.0/24 192.168.66.0/24	139.159.222.28	192.168.44.0/24	192.168.33.0/24 192.168.44.0/24
IDC 3	VPN C	139.9.226.244	192.168.55.0/24	122.112.222.112	192.168.11.0/24 192.168.22.0/24 192.168.33.0/24 192.168.44.0/24 192.168.66.0/24	-
VPC 3		117.78.30.55	192.168.11.0/24 192.168.22.0/24 192.168.33.0/24 192.168.44.0/24 192.168.66.0/24	139.9.226.244	192.168.55.0/24	192.168.55.0/24 192.168.66.0/24

NOTE

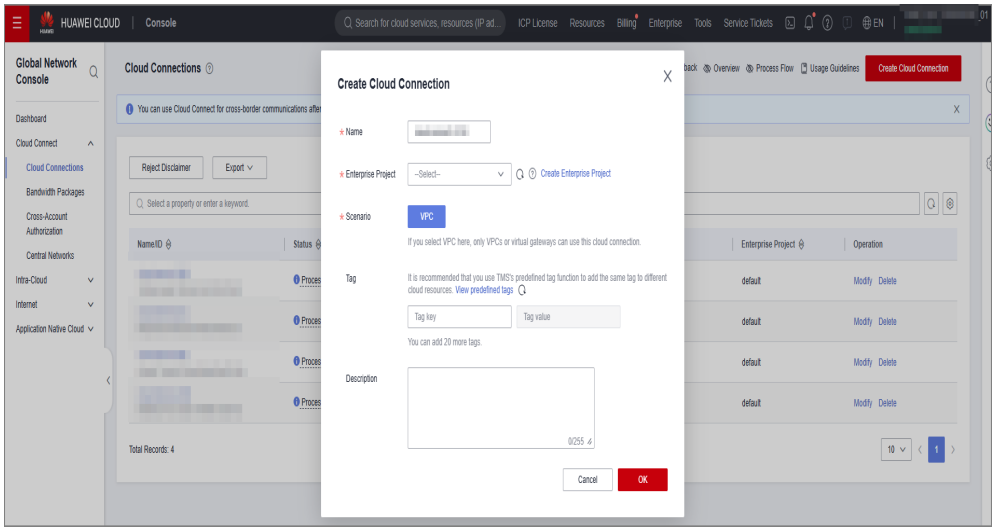
- Cloud Connect network instances can be configured at any region. You can check the route information to verify the network instance configuration.
- The local and remote gateway IP addresses in the on-premises data center and a VPC are reversed. The VPN connection configurations in the on-premises data center are consistent with those on Huawei Cloud.

Procedure

Step 1 Create cloud connections.

1. Log in to the console, select the region where VPC1 is located, and choose **Networking** > **Cloud Connect** from the service list. Click **Create Cloud Connection**, enter related information based on **Figure 2-15**, and click **OK**.

   Figure 2-15 Creating a cloud connection

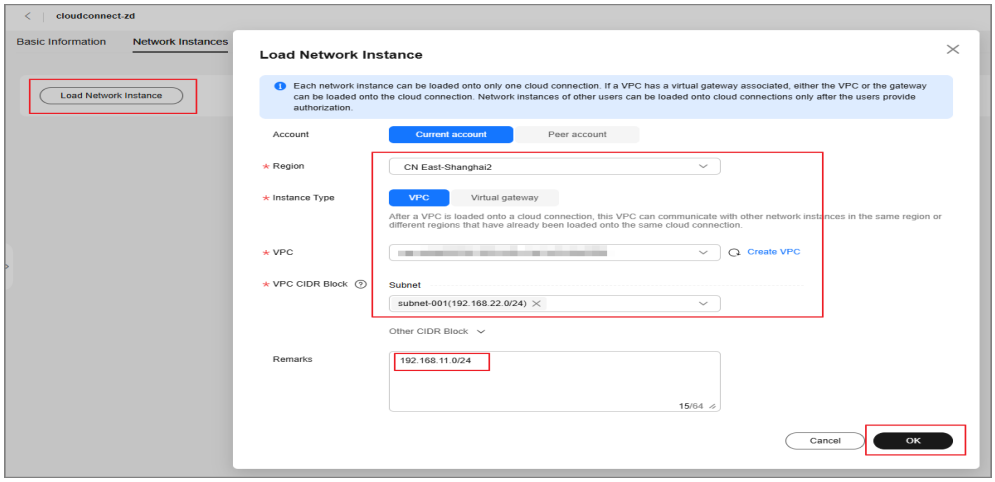


2. Click the name of the created cloud connection, and load a network instance.

   Figure 2-16 Created cloud connection

   On the **Network Instances** tab page, click **Load Network Instance**. Select the VPC for which the cloud connection has been created, select the VPC subnet, and manually add the subnet of the on-premises data center connected through VPN. Then, click **OK**.

Figure 2-17 Loading a network instance

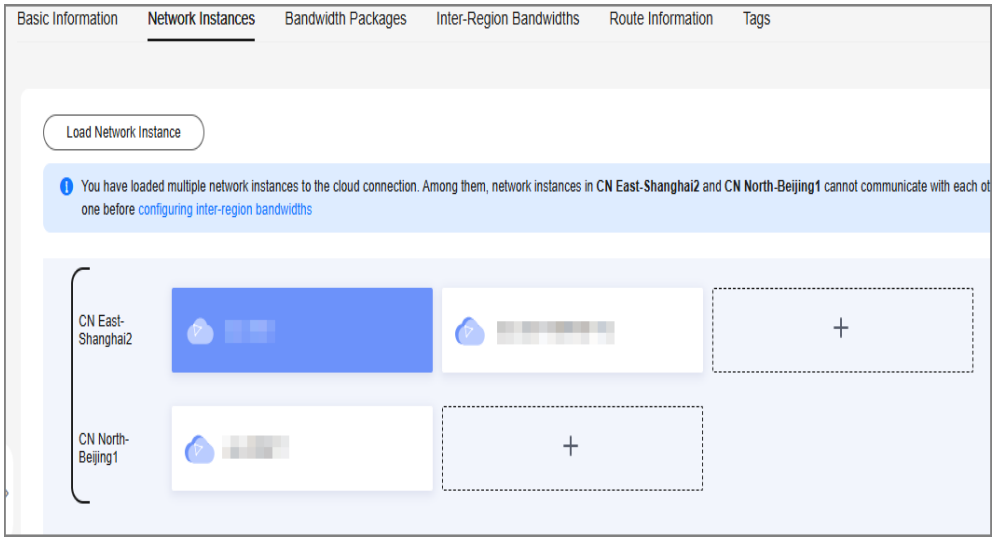


The configuration of VPC2 is the same as that of VPC1. If you do not add the subnet of the on-premises data center connected through a VPN connection during the configuration, you can click **Modify VPC CIDR Block** to add it.

Figure 2-18 Modifying the VPC CIDR block

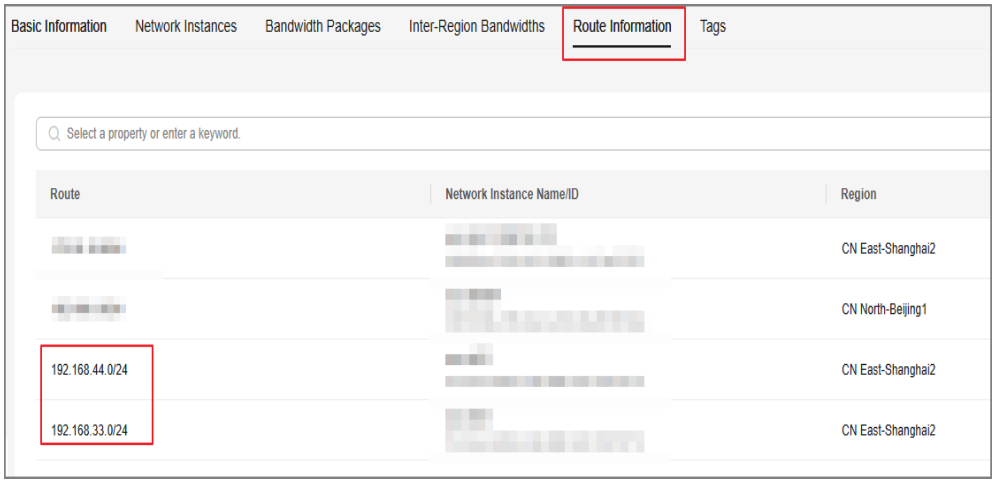
The following figure shows the network instance connection diagram after cloud connections are configured.

Figure 2-19 Network instance connection



Verify the route configuration.

Figure 2-20 Verifying the route configuration



Step 2 Update the VPN network configuration.

Modification method:

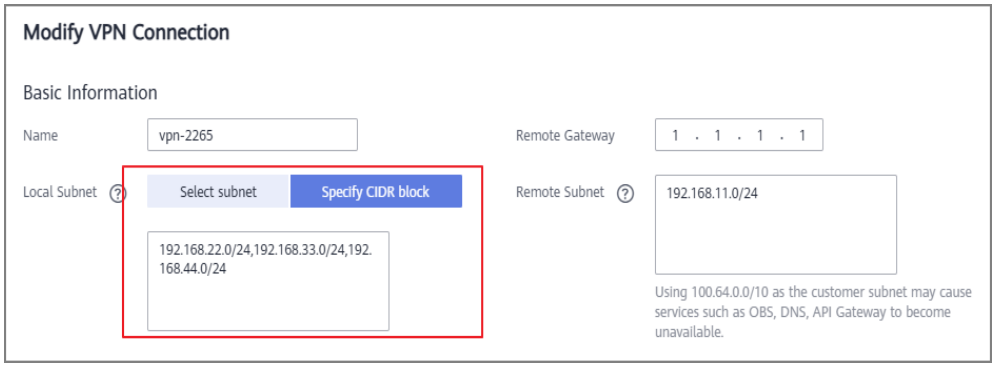
On-premises data center: Keep the local subnet unchanged, and add the subnet of VPC2 as a remote subnet.

VPC: Add the subnet of VPC2 as a local subnet, and keep the remote subnet unchanged.

1. Select the VPN configuration on Huawei Cloud, and modify the local subnet configuration of the created VPN connection.
2. Select **Specify CIDR block** for **Local Subnet**, and add the network instance loaded to the cloud connection of VPC1, as well as the local VPC subnet. Keep the remote network information unchanged.

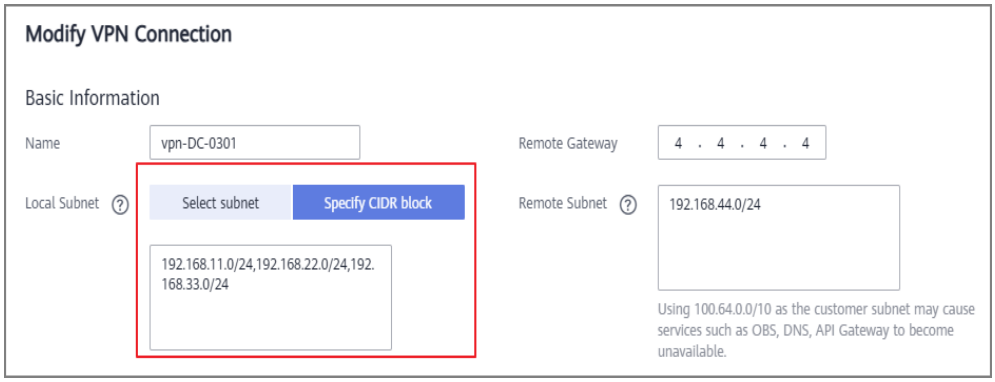
   The following figure shows the VPN connection configuration of VPC1.

Figure 2-21 Modifying the VPN connection



The following figure shows the VPN connection configuration of VPC2.

Figure 2-22 Modifying the VPN connection



----End

Verification

In this environment, the IP addresses of the ECSs in the on-premises data center, VPC1, and VPC2 are 192.168.1.151, 192.168.11.84, and 192.168.22.170, respectively. ECS1 (192.168.1.151) can communicate with ECS2 (192.168.11.84) through VPN. ECS3 (192.168.22.170) cannot communicate with the other two ECSs. After the VPC peering connection is established, ECS3 can communicate with ECS2 but cannot communicate with ECS1.

After the configuration adjustment in **Step 2** is complete, ECS1, ECS2, and ECS3 can communicate with each other. The verification result is as follows:

- IDC1

  ECS1 can access ECS2 in the VPC1 subnet through a VPN connection.


```
[root@ecs-1 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.151  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fe8c:1ec9  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:8c:1e:c9  txqueuelen 1000  (Ethernet)
        RX packets 1190  bytes 155372 (151.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1223  bytes 113478 (110.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-1 ~]# ping 192.168.11.84
PING 192.168.11.84 (192.168.11.84) 56(84) bytes of data.
64 bytes from 192.168.11.84: icmp_seq=1 ttl=61 time=38.4 ms
64 bytes from 192.168.11.84: icmp_seq=2 ttl=61 time=31.4 ms
```

ECS1 can access ECS3 in the VPC2 subnet.

```
[root@ecs-1 ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=61 time=31.7 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=61 time=31.6 ms
```

- IDC2

  ECS1 can access ECS2 in the VPC1 subnet through a VPN connection.

```
[root@ecs-1 ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.151  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fe8c:1ec9  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:8c:1e:c9  txqueuelen 1000  (Ethernet)
        RX packets 1190  bytes 155372 (151.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1223  bytes 113478 (110.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-1 ~]# ping 192.168.11.84
PING 192.168.11.84 (192.168.11.84) 56(84) bytes of data.
64 bytes from 192.168.11.84: icmp_seq=1 ttl=61 time=38.4 ms
64 bytes from 192.168.11.84: icmp_seq=2 ttl=61 time=31.4 ms
```

  ECS1 can access ECS3 in the VPC2 subnet.

```
[root@ecs-1 ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=61 time=31.7 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=61 time=31.6 ms
```

- Huawei Cloud VPC1

  ECS2 in the VPC1 subnet can access ECS1 in the subnet of the on-premises data center.

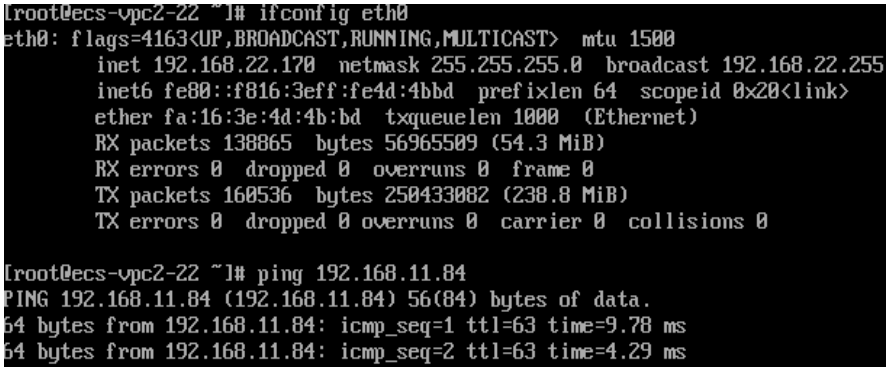
```
[root@ecs-vpc1-11x ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.84  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::f816:3eff:fe43:2462  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:43:24:62  txqueuelen 1000  (Ethernet)
        RX packets 190954  bytes 61952364 (59.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 215881  bytes 253528145 (241.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ecs-vpc1-11x ~]# ping 192.168.1.151
PING 192.168.1.151 (192.168.1.151) 56(84) bytes of data.
64 bytes from 192.168.1.151: icmp_seq=1 ttl=61 time=33.8 ms
64 bytes from 192.168.1.151: icmp_seq=2 ttl=61 time=31.6 ms
```

  ECS2 in the VPC1 subnet can access ECS3 in the VPC2 subnet.

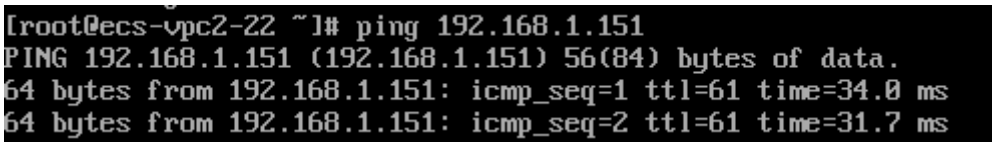
```
[root@ecs-vpc1-11x ~]# ping 192.168.22.170
PING 192.168.22.170 (192.168.22.170) 56(84) bytes of data.
64 bytes from 192.168.22.170: icmp_seq=1 ttl=63 time=7.18 ms
64 bytes from 192.168.22.170: icmp_seq=2 ttl=63 time=3.05 ms
```


- Huawei Cloud VPC2

  ECS3 in the VPC2 subnet can access ECS2 in the VPC1 subnet.



  ECS3 in the VPC2 subnet can access ECS1 in the subnet of the on-premises data center.



3 P2C VPN

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

3.1.1 Overview

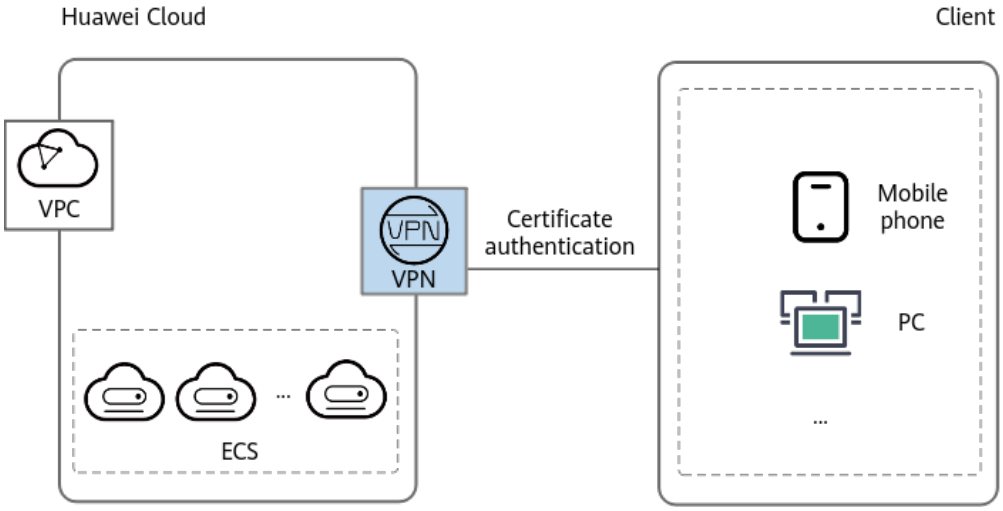
Scenario

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	**Existing 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

Category	Item	Data
	Client authentication mode	Select **Certificate authentication** and click **Upload 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, 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, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.

Step 6 Configure a VPN gateway.

1. On the **P2C VPN Gateways** page, click **Buy P2C VPN Gateway**.
2. 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)
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	Two options are available: **Professional 1** and **Professional 2**. For details about the differences between specifications, see **Specifications Introduction**.	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

Parameter	Description	Example Value
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
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 7 Configure a server.

1. On the **P2C VPN Gateways** page, click **Configure Server** in the **Operation** column of the target VPN gateway. Alternatively, click the name of the target VPN gateway and then click the **Server** tab.
2. 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

Area	Parameter	Description	Example Value
	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
	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)

Area	Parameter	Description	Example Value
Authentication Information	Server Certificate	SSL certificate of the server. Clients use this certificate to verify the server's identity. **Existing certificate**: View and select an uploaded certificate. – 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 to SCM**. – 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.	Existing certificate
	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

Area	Parameter	Description	Example Value
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
	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

Number of VPN Connections	Recommended Client CIDR Block
500	CIDR blocks with the mask less than or equal to 21 Example: 10.0.0.0/21 and 10.0.0.0/20

3. 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.
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

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**.

4. 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

Parameter	Description	Example Value
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 8 Download the client configuration.

1. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.
2. Decompress the package to obtain the **client_config.conf**, **client_config.ovpn**, and **README.md** files.
   - The **client_config.conf** file applies to the Linux operating system.
   - The **client_config.ovpn** file applies to the Windows, macOS, and Android operating systems.

Step 9 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 10 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)

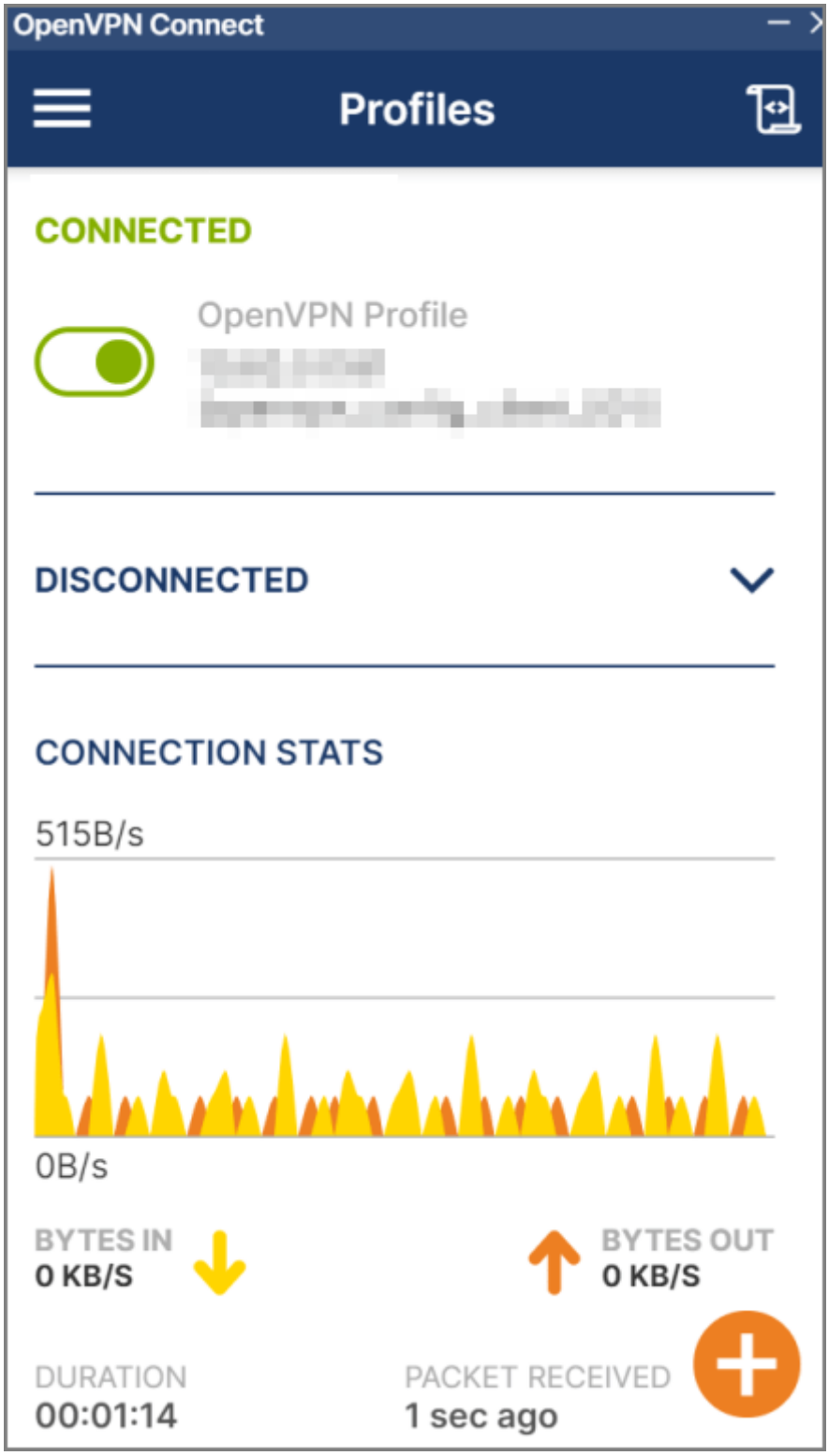
For more client configuration cases, see **Configuring a Client**.

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

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 following command to verify the connectivity:

   ping 192.168.1.10

   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
```

3.2 Configuring P2C VPN to Connect Mobile Terminals to a VPC (IAM Authentication)

3.2.1 Overview

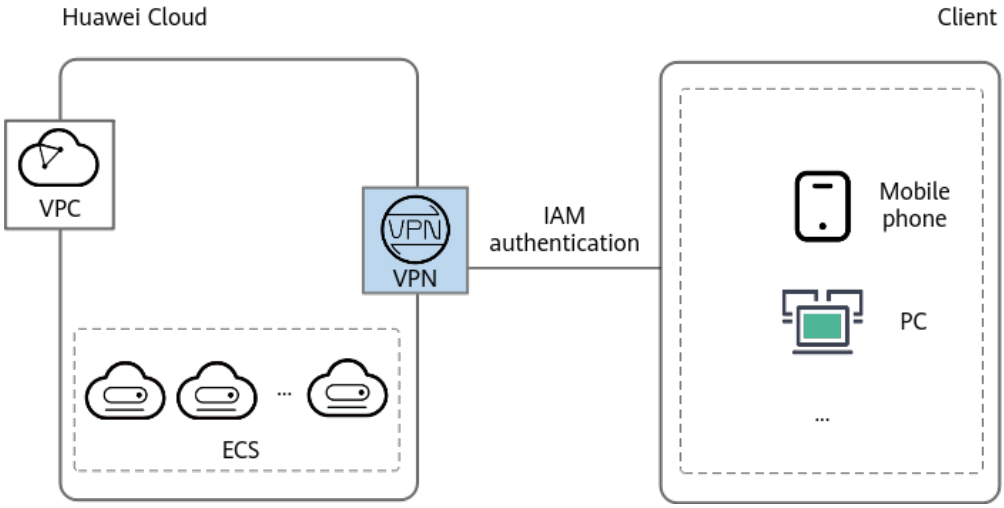
Scenario

P2C VPN supports third-party user authentication. A server uses IAM authentication to verify the identity of a client.

Networking

Multiple clients can use IAM authentication to connect to a VPN gateway for access to a VPC.

Figure 3-5 Networking



Solution Advantages

You can use client IAM authentication to manage accounts in a unified manner.

Limitations and Constraints

When the client authentication mode is IAM authentication, gateway resources in the sub-projects of regions cannot be used. For details about sub-projects, see **Project Management**.

3.2.2 Planning Networks and Resources

Data Plan

Table 3-7 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	Service self-signed certificate
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	IAM authentication

3.2.3 Procedure

Prerequisites

- Cloud side
  - A VPC has been created. For details, 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**.

Precautions

Changing the client authentication mode will interrupt existing VPN connections. Exercise caution when performing this operation.

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 **Management & Governance** > **Identity and Access Management**.

Step 4 Create a user group, grant permission to the user group, and create an IAM user.

1. Create a user group.
   a. Choose **User Groups** from the navigation pane.
   b. On the **User Groups** page, click **Create User Group**.
   c. Configure user group information, such as the user group name.
   d. Click **OK**. The user group is created.

      You can view the created user group in the user group list.
2. Grant permission to the user group.
   a. Click **Authorize** in the **Operation** column of the created user group.
   b. In the search box in the upper right corner, search for **VPN SSOAccessPolicy** and select it.
   c. Click **Next** and select the authorization scope as required.
   d. Click **OK**. The permission is grated to the user group.
3. Create an IAM user.
   a. Choose **Users** from the navigation pane.
   b. On the **Users** page, click **Create User**.
   c. Configure user information as prompted.

      For details about how to configure user information, see **Creating an IAM User**.

d. Click **Next**.

e. (Optional) Select the user group to which the user is to be added.

After being added to a user group, a user inherits the permission granted to the user group.

Step 5 Click  in the upper left corner, and choose **Networking** > **Virtual Private Network**.

Step 6 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.

Step 7 Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.

Step 8 Configure a VPN gateway.

1. On the **P2C VPN Gateways** page, click **Buy P2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.

   Table 3-2 describes the VPN gateway parameters.

Table 3-8 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)
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	Two options are available: **Professional 1** and **Professional 2**. For details about the differences between specifications, see **Specifications Introduction**.	Professional 1

Parameter	Description	Example Value
AZ	An 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 9 Configure a server.

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

   Table 3-9 describes the server parameters.

Table 3-9 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	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	Select **Service self-signed certificate**.	Service self-signed certificate
	Client Authentication Mode	Select **IAM authentication**.	IAM 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
	Compression	Whether to compress the transmitted data. By default, this function is disabled and cannot be modified.	Disabled

Table 3-10 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

3. Click **OK**.

Step 10 Download the client configuration.

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

Step 11 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)

  Only clients running 3.4.0 and later versions support IAM authentication.

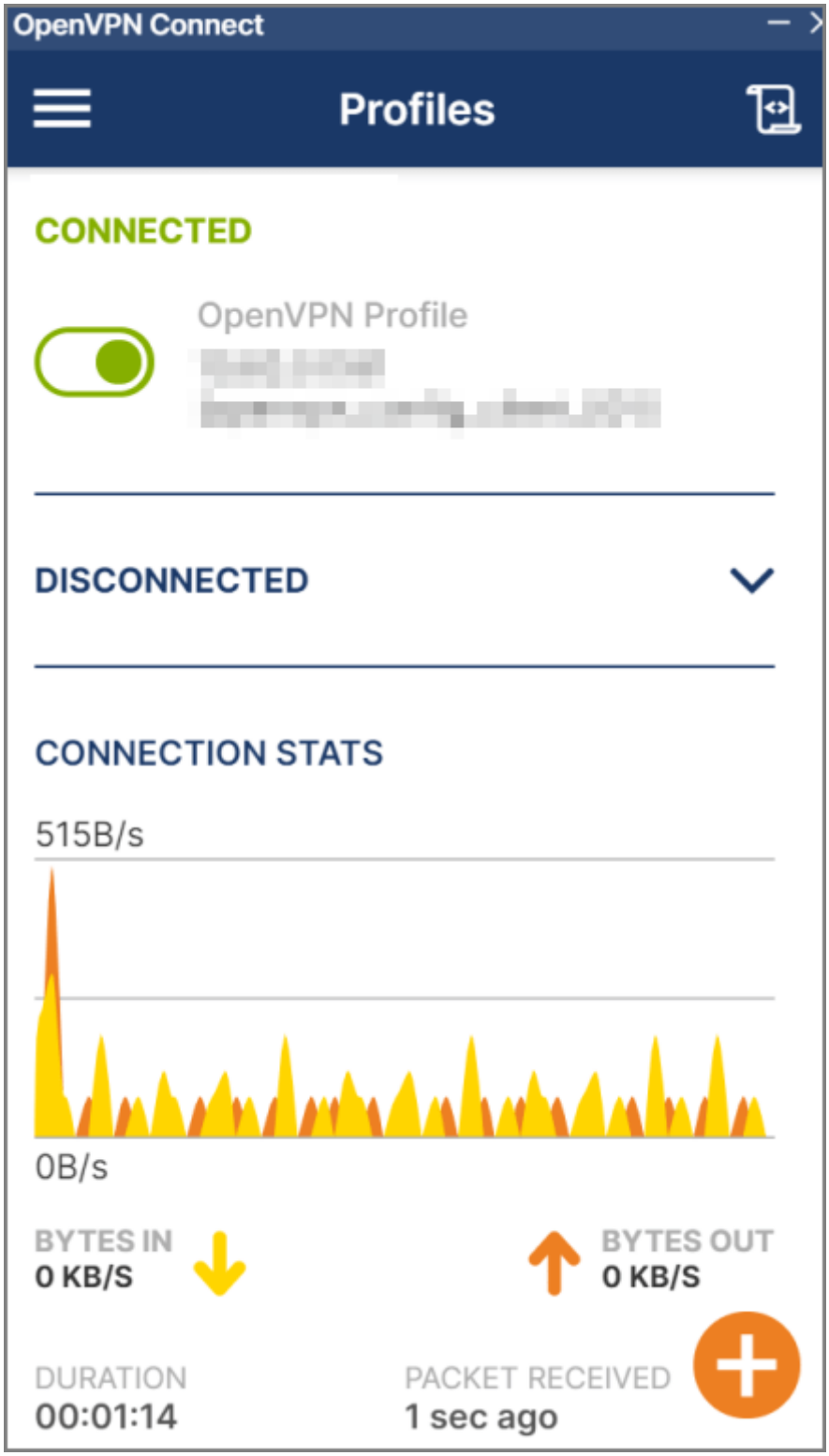
For more client configuration cases, see **Configuring a Client**.

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 3-6 Uploading a configuration file

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

Figure 3-7 Connection established



4. Use the IAM username and password to log in to the web client.
   - If the login page displays a message indicating that the authentication is successful, the VPN connection has been established successfully.

- If the login page displays a message indicating that the authentication fails, you can modify the configuration based on the error information. For details about the error information, see *Troubleshooting*.

----End

Verification

1. Press **win+R** and enter **cmd** to open the CLI of the client device.
2. Run the following command to verify the connectivity:

   ping 192.168.1.10

   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
```

3.3 Configuring P2C VPN to Connect Mobile Terminals to a VPC (Federated Authentication)

3.3.1 Overview

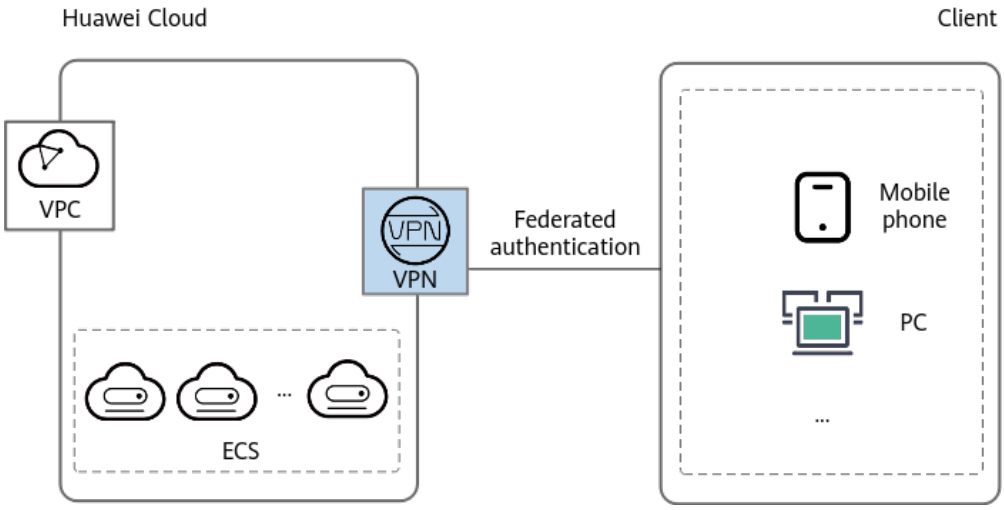
Scenario

P2C VPN supports third-party user authentication. A server uses federated authentication to verify the identity of a client.

Networking

Multiple clients can use federated authentication to connect to a VPN gateway for access to a VPC.

Figure 3-8 Networking



Solution Advantages

You can use client federated authentication to manage accounts in a unified manner, securing user data transmission.

Limitations and Constraints

When the client authentication mode is federated authentication, gateway resources in the sub-projects of regions cannot be used. For details about sub-projects, see **Project Management**.

3.3.2 Planning Networks and Resources

Data Plan

Table 3-11 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	Service self-signed certificate
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

Category	Item	Data
	Client authentication mode	Federated authentication
	Identity provider	p2c-vpngw-saml1

3.3.3 Procedure

Prerequisites

- Cloud side
  - A VPC has been created. For details, 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**.
  - An identity provider has been configured. Currently, only identity providers for virtual user SSO via SAML are supported. For details about how to configure an identity provider for virtual user SSO, see **Virtual User SSO via SAML**.

    One or more identity conversion rules must have been configured for the identity provider. When configuring identity conversion rules, select the user group with the VPN SSOAccessPolicy permission. For details about how to create a user group, see **Creating a User Group and Granting Permission**.

    NOTE

    When you configure or modify an identity conversion rule by editing a JSON file, the username cannot contain only spaces.

Precautions

Changing the client authentication mode or identity provider will interrupt existing VPN connections. Exercise caution when performing this operation.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Click in the upper left corner of the page, and choose **Management & Governance** > **Identity and Access Management**.

Step 5 Create a user group and grant permission to it.

1. Create a user group.
   a. Choose **User Groups** from the navigation pane.
   b. On the **User Groups** page, click **Create User Group**.
   c. Configure user group information, such as the user group name.
   d. Click **OK**. The user group is created.
      You can view the created user group in the user group list.
2. Grant permission to the user group.
   a. Click **Authorize** in the **Operation** column of the created user group.
   b. In the search box in the upper right corner, search for **VPN SSOAccessPolicy** and select it.
   c. Click **Next** and select the authorization scope as required.
   d. Click **OK**. The permission is grated to the user group.

Step 6 Click in the upper left corner, and choose **Networking** > **Virtual Private Network**.

Step 7 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.

Step 8 Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.

Step 9 Configure a VPN gateway.

1. On the **P2C VPN Gateways** page, click **Buy P2C VPN Gateway**.
2. Set parameters as prompted and click **Buy Now**.
   Table 3-2 describes the VPN gateway parameters.

Table 3-12 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	Two options are available: **Professional 1** and **Professional 2**. For details about the differences between specifications, see **Specifications Introduction**.	Professional 1
AZ	An 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 10 Configure a server.

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

   Table 3-9 describes the server parameters.

Table 3-13 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	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	Select **Service self-signed certificate**.	Service self-signed certificate
	Client Authentication Mode	Select **Federated authentication**.	Federated authentication
	Identity Provider	Select an existing identity provider. If no identity provider is available, you can click **Create Identity Provider** in the drop-down list to create one on the IAM console. For details about how to create an identity provider, see **Creating an IdP Entity**.	*Set this parameter based on the actual condition.*
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
	Compression	Whether to compress the transmitted data. By default, this function is disabled and cannot be modified.	Disabled

Table 3-14 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

3. Click **OK**.

Step 11 Download the client configuration.

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

Step 12 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)

  Only clients running 3.4.0 and later versions support federated authentication.

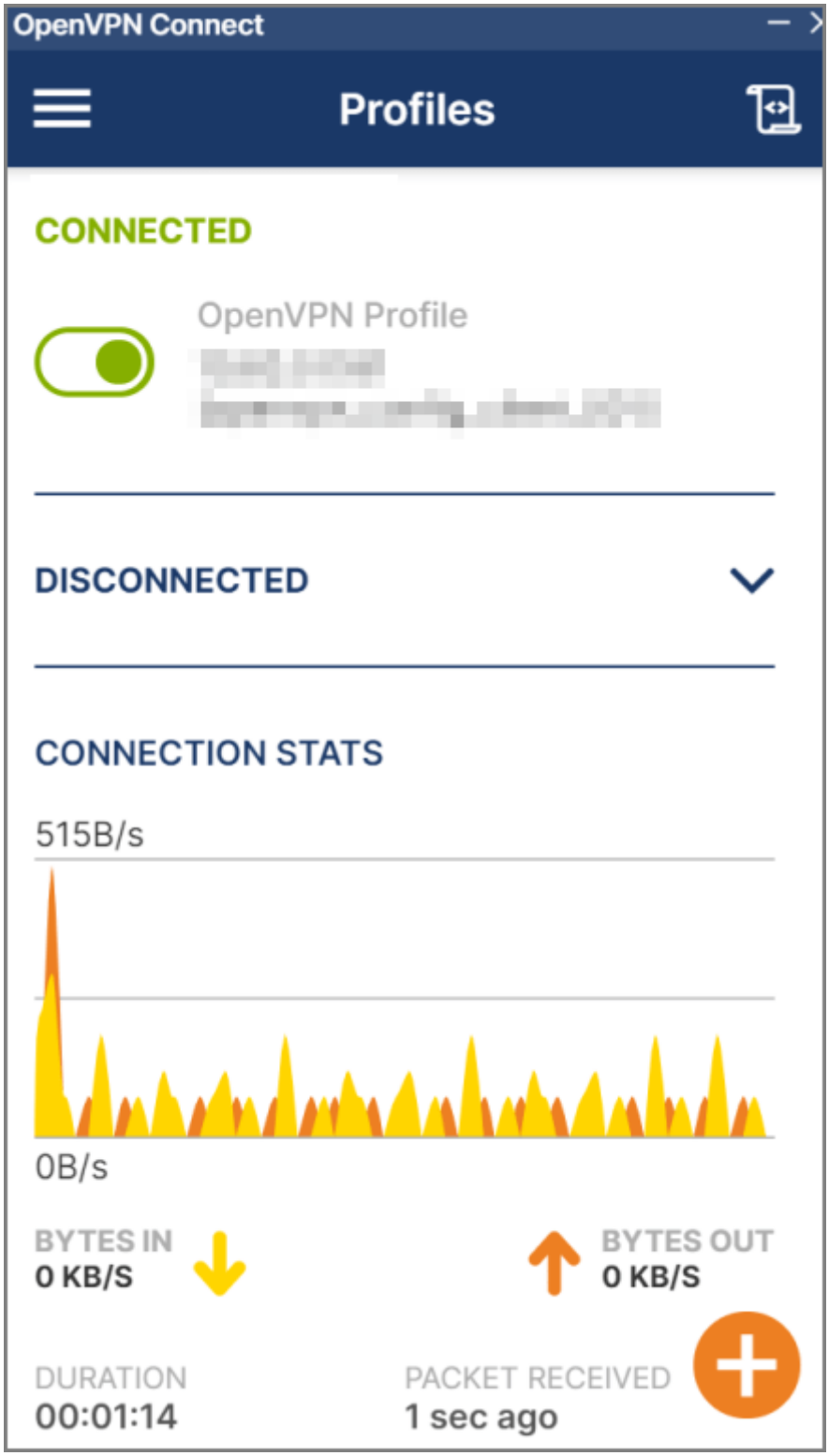
For more client configuration cases, see **Configuring a Client**.

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 3-9 Uploading a configuration file

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

Figure 3-10 Connection established



Step 13 Log in to the web client using the federated username and password.

- If the login page displays a message indicating that the authentication is successful, the VPN connection has been established successfully.

- If the login page displays a message indicating that the authentication fails, you can modify the configuration based on the error information. For details about the error information, see *Troubleshooting*.

----End

Verification

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

   ping 192.168.1.10

   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
```

