Virtual Private Network

Best Practices

Issue	01
Date	2021-08-30



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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.

Contents

1 Connecting an On-Premises Data Center to a VPC Through a VPN..... 1
2 Setting Up a Cross-Border Network Using VPN and CC.....3
3 Using VPN and Cloud Connect to Enable Communication Between On-Premises Data Centers and Multiple VPCs on HUAWEI CLOUD..... 9

 Copyright © Huawei Technologies Co., Ltd.

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

Scenarios

By default, ECSs in a VPC cannot communicate with your on-premises data center or private network. To enable network communication between them, you can set up a VPN. After that, configure security group rules for ECSs in the VPC to allow traffic from your on-premises data center, and check the connectivity between the VPC and your on-premises data center to ensure that the VPN is functional. VPNs can be classified into the following two types:

- Site-to-site VPN functions as a communication tunnel between a VPC and a single on-premises data center.
- By contrast, 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 PSK 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.
- The security group containing the ECSs in the VPC allows traffic from and to the on-premises data center.
- The status of a VPN changes to **Normal** only after ECSs and on-premises servers can access each other.

Prerequisites

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

Procedure

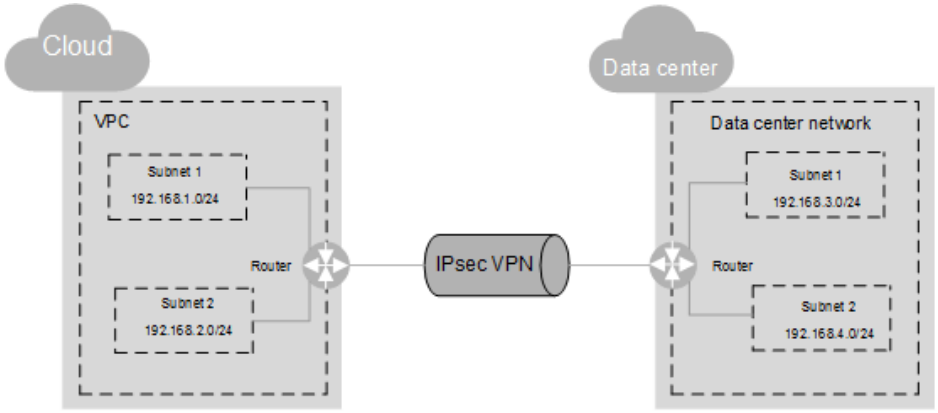
1. On the management console, select the appropriate IKE and IPsec policies to create a VPN.

 Copyright © Huawei Technologies Co., Ltd.

2. Check the IP address pools for the local and remote subnets.

   In **Figure 1-1**, 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 1-1 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 connection. If the data transmitted through the VPN connection cannot be forwarded to the network devices, check whether the remote LAN has policies configured to refuse the traffic.

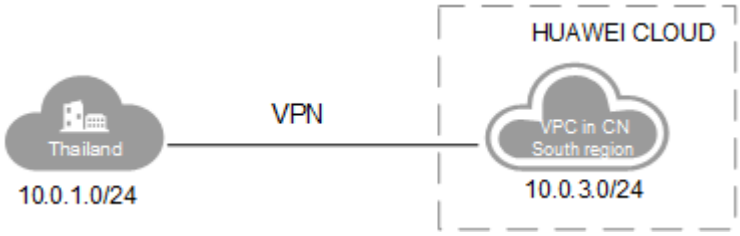
Copyright © Huawei Technologies Co., Ltd.

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

Scenarios

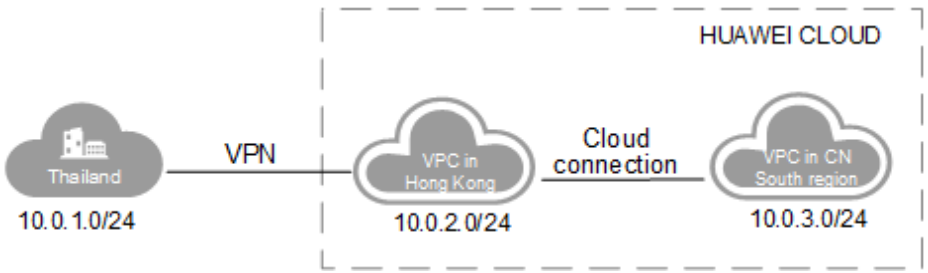
Your on-premises data center in Thailand (10.0.1.0/24) needs to communicate with your business system deployed in the VPC (10.0.3.0/24) in the HUAWEI CLOUD **CN South-Guangzhou** region. VPN may not be a good choice since it crosses borders and may be unstable.

Figure 2-1 Cross-border VPN connection



In this scenario, use Cloud Connect (CC) and VPN to ensure more stable communication. Use VPN to connect your on-premises data center to a HUAWEI CLOUD VPC nearest to your data center, for example, the VPC (10.0.2.0/24) in the **AP-Hong Kong** region. Then create a cloud connection to connect the VPC (10.0.2.0/24) in the **AP-Hong Kong** region to the VPC (10.0.3.0/24) in the **CN South-Guangzhou** region. **Figure 2-2** shows the data center and regions connected by a VPN and a cloud connection, respectively.

Figure 2-2 Data center and regions connected by a VPN and a cloud connection



 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Configure a VPN in the **AP-Hong Kong** region.
   a. Click in the upper left corner and select the **CN-Hong Kong** region.
   b. Click **Service List** in the upper left corner. Under **Networking**, select **Virtual Private Network**.
   c. On the **Virtual Private Network** console, click **Buy VPN Gateway**.
   d. Configure the parameters based on **Table 2-1** and click **Next**.

Table 2-1 VPN parameters

Parameter	Description	Example Value
Billing Mode	VPNs are billed on a pay-per-use basis.	Pay-per-use
Region	A region is a geographical area where you can run your VPN service. Each region comprises one or more AZs and is completely isolated from other regions. AZs within the same region can communicate with one another through a private network, while those in different regions cannot. Set it to **CN-Hong Kong**.	CN-Hong Kong
Name	VPN name.	vpn-001
VPC	The name of the VPC that the VPN accesses to. Select a VPC created in the **AP-Hong-Kong** region.	vpc-001
Local Subnet	The VPC subnets that will access your on-premises network through a VPN Select **Specify CIDR Block** and enter the subnets in the **AP-Hong Kong** and **CN South-Guangzhou** regions to ensure that traffic from the **CN South-Guangzhou** region can pass the VPN tunnel. Enter **10.0.2.0/24** and **10.0.3.0/24**.	10.0.2.0/24, 10.0.3.0/24

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Remote Gateway	The VPN gateway address in the on-premises data center Set this parameter to the VPN gateway address in the data center in Thailand.	N/A
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN Enter **10.0.1.0/24**.	10.0.1.0/24
PSK	The pre-shared key, which is a private key shared by two ends of a VPN connection. The PSK configurations for 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	Enter the pre-shared key again.	Test@123
Advanced Settings	● **Default**: Use default IKE and IPsec policies. ● **Custom**: including **IKE Policy** and **IPsec Policy**, which specifies the encryption and authentication algorithms of a VPN tunnel.	Custom

2. Configure the VPN gateway in your on-premises data center. (User VPN gateway in the Thailand data center)

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

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Configure the ACL referenced by the IPsec policy as follows:

- Source: 10.0.1.0/24
- Destination: 10.0.2.0/24 and 10.0.3.0/24

3. Buy a cloud connection in the Cloud Connect service. For details, see **Step 2: Create a Cloud Connection**.
4. Load network instances.

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

   NOTE

   - **Table 2-2** lists the parameters required to load the VPC in the Hong Kong region to the cloud connection.
   - When loading the VPC in the South China region, you only need to specify subnet **10.0.3.0/24**.

Table 2-2 Parameters for loading the VPC

Parameter	Description	Example Value
Account	Whether the VPC is from your account or the other user's account.	Current account
Region	The region where the VPC you want to load the cloud connection is located.	CN-Hong Kong
Instance Type	The type of the instance you want to load to the cloud connection.	VPC
VPC	Name of the VPC that you want to load to the cloud connection. Select the VPC created in **1.d**.	vpc-001

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
VPC CIDR Block	CIDR block of the VPC that you want to load to the cloud connection. Because you have set **Instance Type** to **VPC**, configure the following two parameters: • **Subnet**: The subnets in the VPC. Set it to the subnet whose CIDR block is **10.0.2.0/24**. • **Custom 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 **Custom CIDR Block**: 10.0.1.0/24
Virtual Gateway	Name of the virtual gateway that you want to load to the cloud connection. This parameter is mandatory when **Instance Type** is set to **Virtual gateway**.	vgw-w2
Virtual Gateway CIDR Block	The VPC and its CIDR block of the virtual gateway that needs to be loaded to the cloud connection. If **Instance Type** is set to **Virtual gateway**, configure the following two parameters: • VPC CIDR Block • Remote Subnet	**VPC CIDRs**: 192.168.0.3/24

5. Configure the inter-region bandwidth.

   For details, see **Step 6: Configure Inter-Region Bandwidths**.

6. View route information.

   The VPC in the **AP-Hong Kong** region has two routes with destinations **10.0.1.0/24** and **10.0.2.0/24**, respectively.

Copyright © Huawei Technologies Co., Ltd.

The VPC in the south China region contains one route with destination **10.0.3.0/24**.

For details, see **Viewing Route Information**.

7. Test network connectivity.

   Create an ECS in the CN South-Guangzhou region, with its private IP address set to **10.0.3.17**.

   Assume that the IP address of an on-premises server is 10.0.1.17.

   Ping **10.0.3.17** from **10.0.1.17** to trigger tunnel negotiation.

   The network communication is normal if the IP address can be pinged. You can view the IPsec VPN tunnel information on the VPN gateway in the customer data center. The method for checking the IPsec VPN tunnel information varies depending on the VPN device models.

Copyright © Huawei Technologies Co., Ltd.

3 Using VPN and Cloud Connect to Enable Communication Between On-Premises Data Centers and Multiple VPCs on HUAWEI CLOUD

Scenarios

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

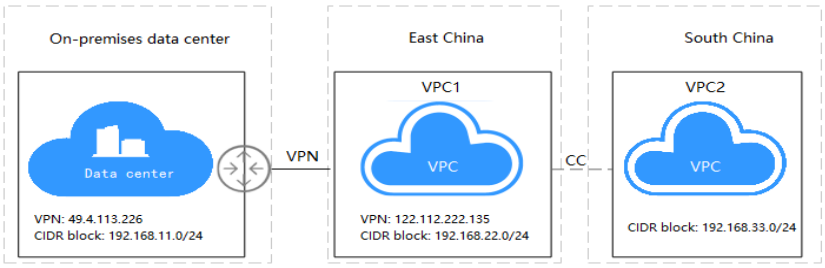
Multiple VPCs in the same region can also be connected through Cloud Connect connections.

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. Connection topology

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-1 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 IP address: 122.112.222.135
- VPC2 subnet: 192.168.33.0/24

3. Configuration overview

Table 3-1 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 gateway IP address and VPC1 are mutually mirrored. The VPN resources are the same as 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 view the routing information to verify the network instance configuration.

 Copyright © Huawei Technologies Co., Ltd.

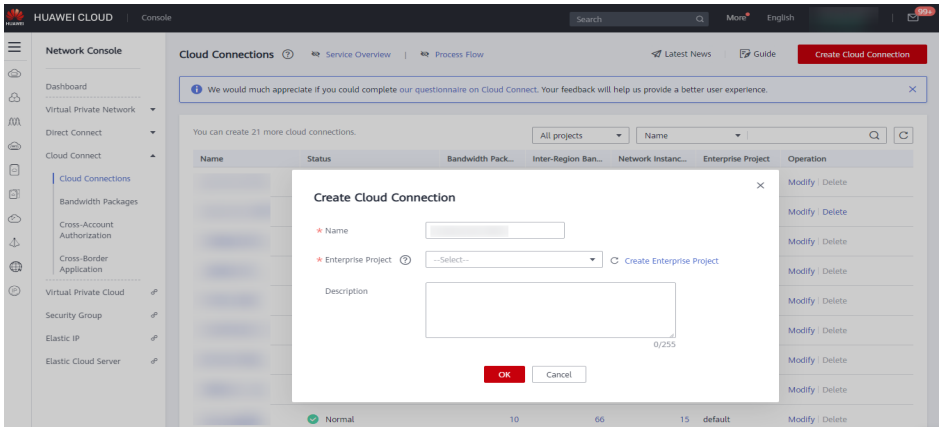
4. Configuration plan
   - Use a cloud connection to connect VPC1 in East China to VPC2 in South China.
   - Keep the local subnet of the VPN connection in your on-premises data center unchanged, and change the remote subnet to 192.168.22.0/24 and 192.168.33.0/24.
   - Change the local subnet of the 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 management 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 3-2 Create Cloud Connection



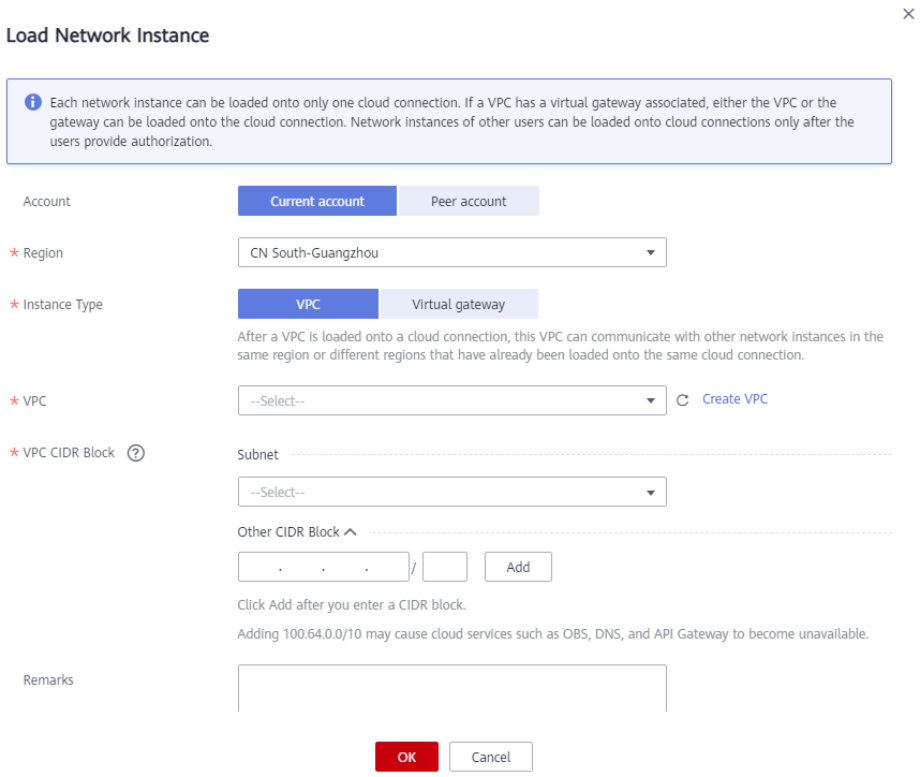
You can create a cloud connection in any region where the VPC is located. If you have two VPCs in the same region, you can use a VPC peering connection (with a lower latency) or a cloud connection to connect the two VPCs. If you have more than two VPCs, use cloud connections to connect them.

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

   Configure required parameters and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

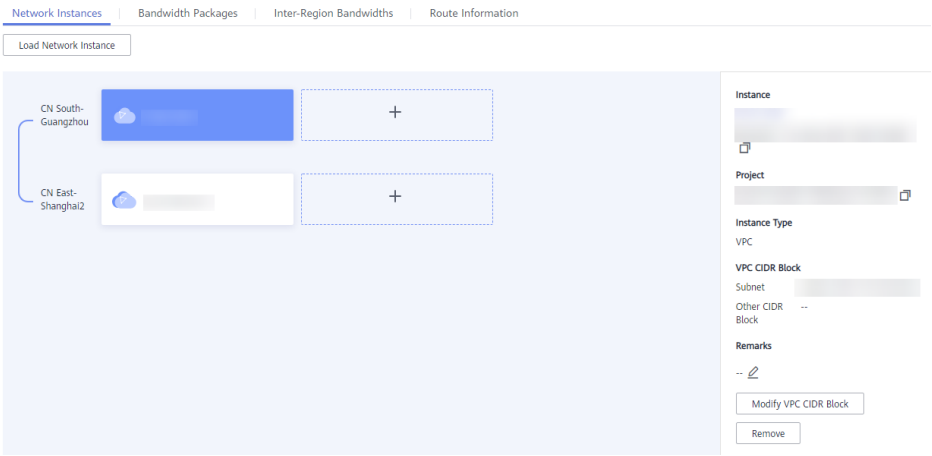
Figure 3-3 Loading network instance 1



5. Select **CN South-Guangzhou** for **Region**. Select VPC2. You can select some or all some 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 3-4 Loading network instance 2



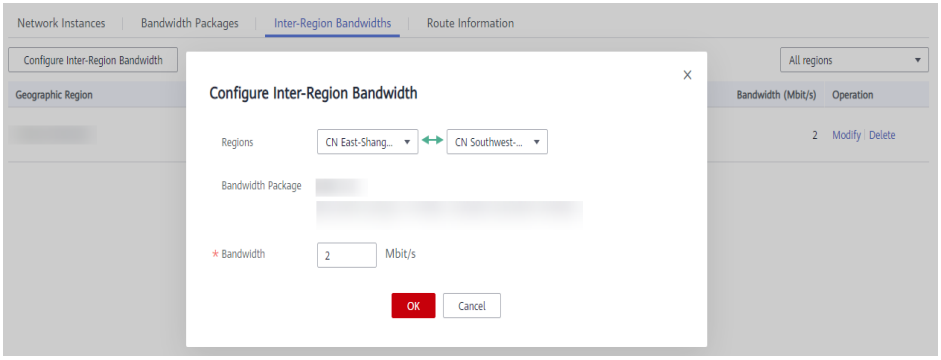
 Copyright © Huawei Technologies Co., Ltd.

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. Select 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.

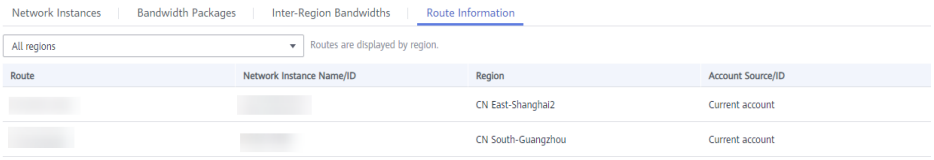
Figure 3-5 Configure Inter-Region Bandwidth



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 3-6 Verifying the route information



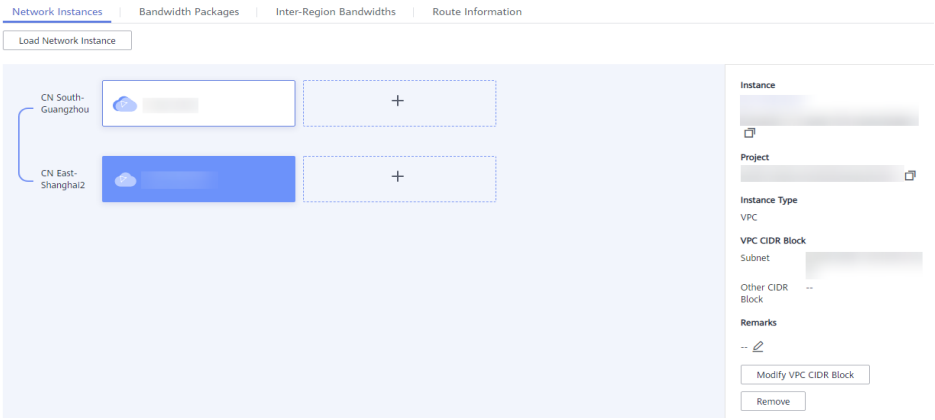
Step 2 Modify VPC CIDR blocks.

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.

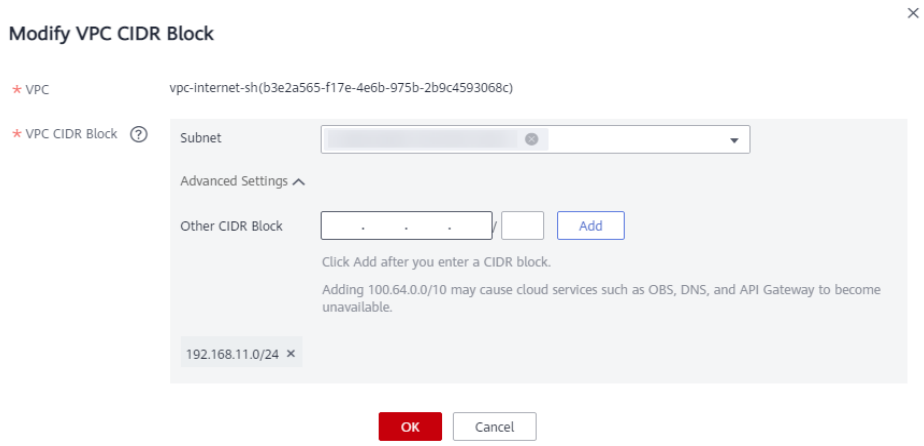
 Copyright © Huawei Technologies Co., Ltd.

Figure 3-7 Modify VPC CIDR Block



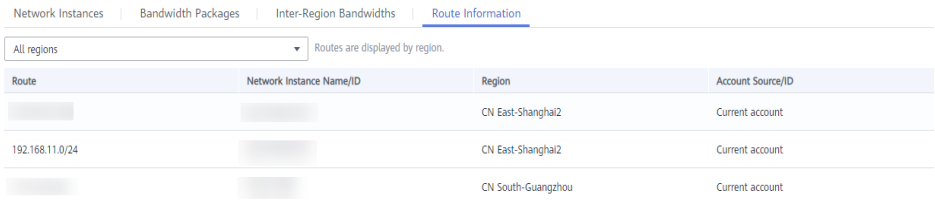
4. For **Other CIDR Block** in the **Advanced Settings** area, enter the CIDR block to which VPC1 connects through the VPN connection and click **OK**.

Figure 3-8 Modify VPC CIDR Block



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

Figure 3-9 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.

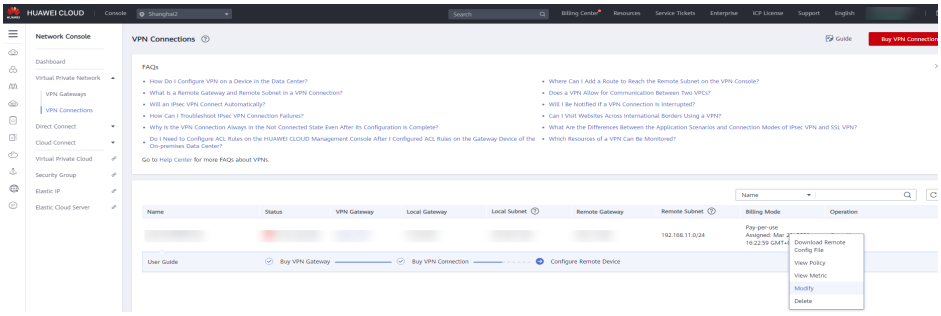
- On-premises data center: Retain the local subnet and add a subnet of VPC2 to the remote subnet. In this example, the subnet is 192.168.33.0/24.

 Copyright © Huawei Technologies Co., Ltd.

- 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.

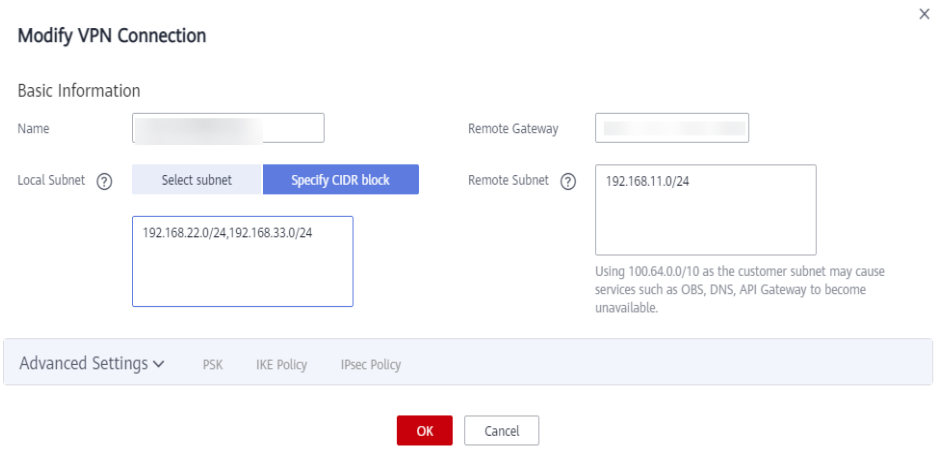
1. Choose **Virtual Private Network** > **VPN Connections**, locate the VPN connection created for VPC1, and choose **More** > **Modify** in the **Operation** column.

Figure 3-10 Modifying a VPN connection



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 network subnets. Retain the remote subnet and other information unchanged.

Figure 3-11 Modify 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

Configuration 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.

 Copyright © Huawei Technologies Co., Ltd.

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.

 Copyright © Huawei Technologies Co., Ltd.

```
[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
```

 Copyright © Huawei Technologies Co., Ltd.