Alibaba Cloud
vpn gateway

IPsec-VPN Quick Start

Issue: 20181009

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade

secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Tutorial overview

This section includes a tutorial that illustrates how to use IPsec-VPN to connect a VPC to a local data center. This section also includes a tutorial that illustrates how to use IPsec-VPN to connect two VPCs.

Prerequisites

Before creating a site-to-site VPN connection, make sure the following conditions are met:

- The gateway device of the local data center support IKEv1 and ikev2 protocols.

  IPsec-VPN supports IKEv1 and IKEv2 protocols. Any device that supports these two protocols can connect to Alibaba Cloud VPN Gateway. Supported devices include: Huawei, H3C, Cisco, ASN, Juniper, SonicWall, Nokia, IBM, and Ixia.
- A static IP address is configured for the local gateway.
- The IP address ranges of the VPC and local data center to be connected do not conflict with each other.

Create a site-to-site connection

To use IPsec-VPN to connect different sites, you must:

1. Create a VPN gateway with IPsec-VPN enabled.

   Up to 10 IPsec connections can be established within a VPN gateway.
2. Create a customer gateway.

   By creating a customer gateway, you can upload the configuration of the local gateway to the Alibaba Cloud. A customer gateway can be connected to multiple VPN gateways.
3. Create an IPsec connection.

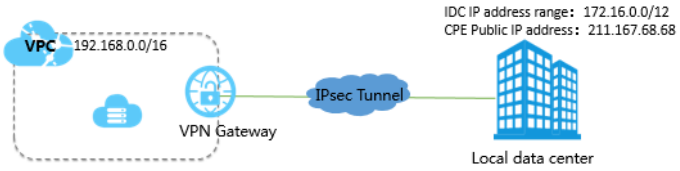
   Create an IPsec connection to connect the VPN gateway and customer gateway to establish an encrypted communication tunnel.
4. Configure the local gateway.

   Configure the local gateway according to the IPsec connection configurations.
5. Configure the route and security groups.

   Finally, you must configure corresponding routing in the VPC to complete the data transmission .

2 Configure a site-to-site connection

This document illustrates how to create a site-to-site connection to connect a VPC with a local data center.



Prerequisites

You must meet the following requirements before creating an IPsec connection:

- Check the gateway device in the local data center. Alibaba Cloud VPN gateways support standard IKEv1 and IKEv2 protocols. Any device that supports these two protocols can connect to Alibaba Cloud VPN Gateway. Supported devices include: Huawei, H3C, Cisco, ASN, Juniper, SonicWall, Nokia, IBM, and Ixia.
- A static public IP address is configured for the local gateway.
- The IP address ranges of the VPC and local data center to be connected do not conflict with each other.

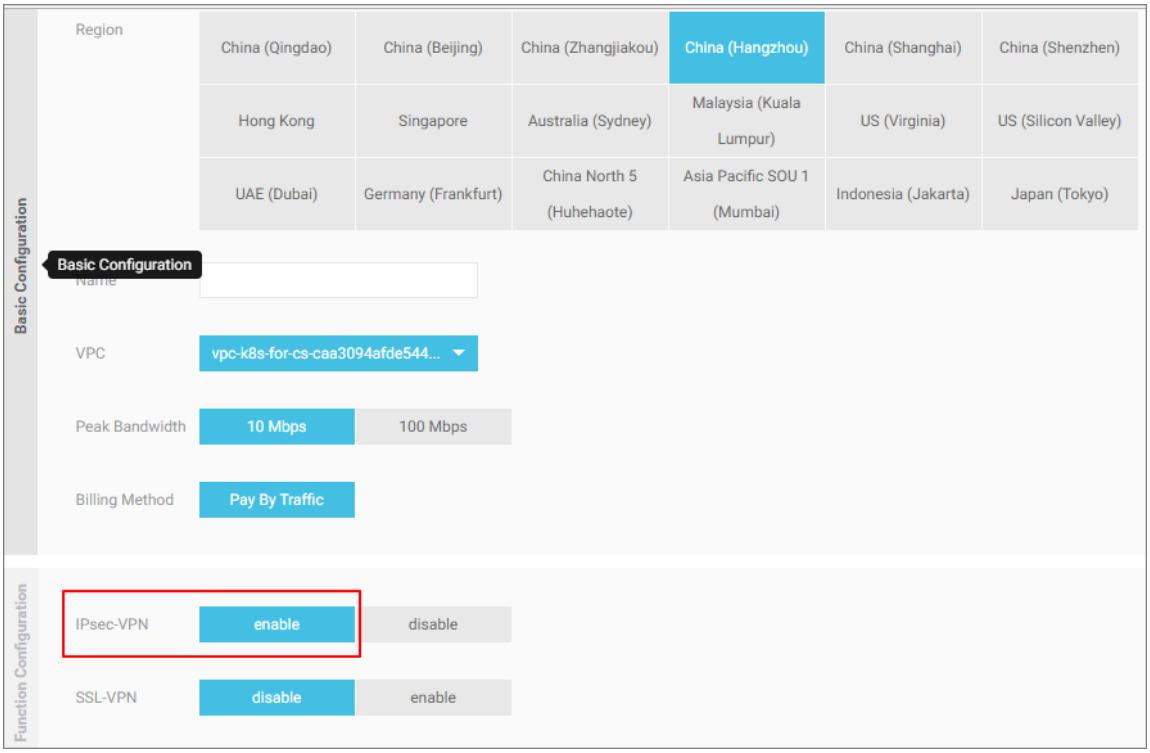
Step 1: Create a VPN gateway

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **VPN Gateways**.
3. On the VPN Gateways page, click **Create VPN Gateway**.
4. On the purchase page, configure the VPN gateway and complete the payment. In this tutorial, the VPN Gateway uses the following configurations:
   - **Region**: Select the region of the VPN gateway. In this tutorial, **China (Hangzhou)** is selected.

     Note:
     Make sure that the VPC and the VPN gateway are in the same region.
   - **VPC**: Select the VPC to be connected.
   - **Bandwidth specification**: Select a bandwidth specification. The bandwidth specification is the Internet bandwidth of the VPN gateway.
   - **IPsec-VPN**: Select whether to enable the IPsec-VPN feature.

- **SSL-VPN**: Select whether to enable the SSL-VPN feature. The SSL-VPN feature allows you to connect to a VPC from a single computer anywhere.
- **Concurrent SSL Connections**: Select the maximum number of clients you want to connect to simultaneously.

> **Note:**
> You can only configure this option after you enables the SSL-VPN feature.



5. Go back to the VPN Gateways page, select **China (Hangzhou)** region to view the created VPN Gateway.

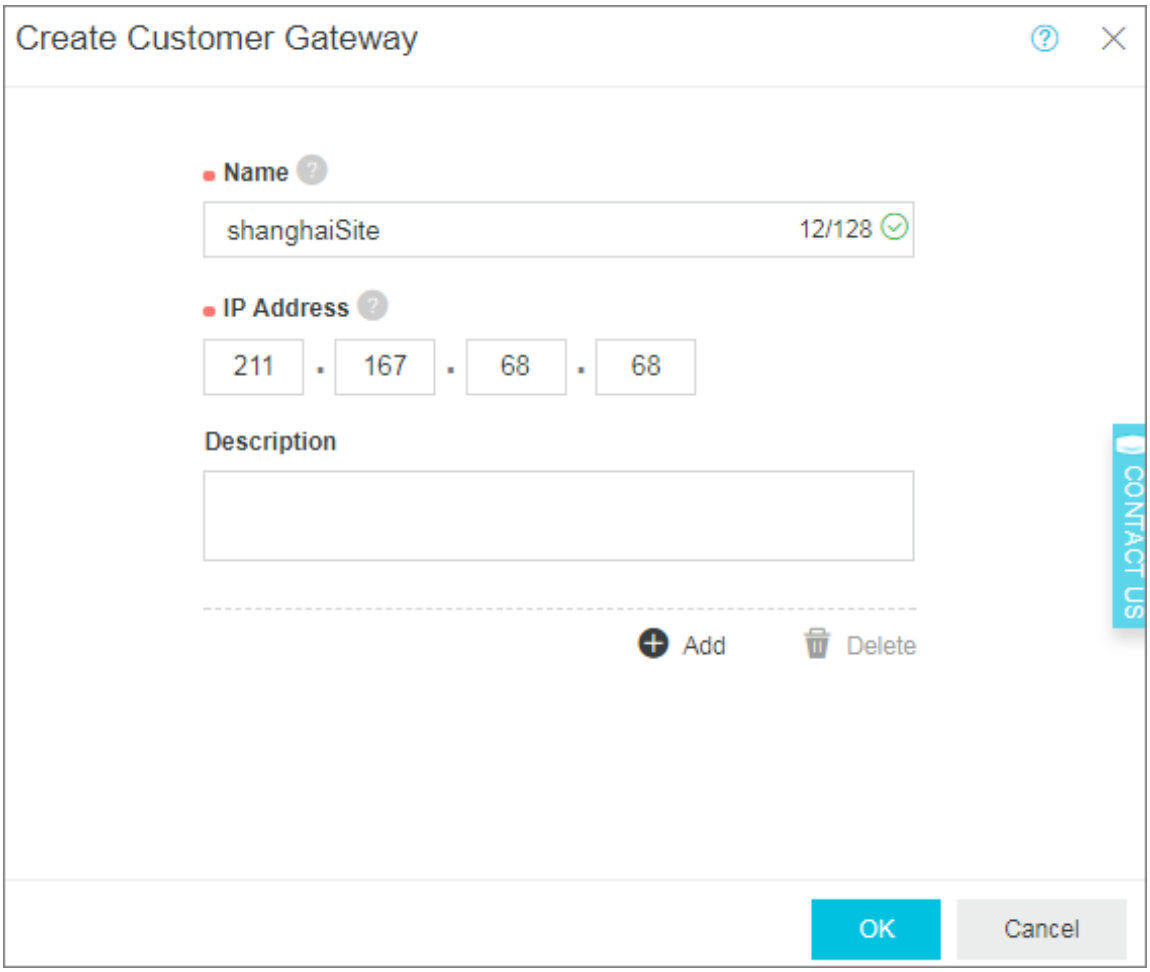
   The initial status of a VPN Gateway is Preparing. It changes to Normal in about 2 minutes. When it changes to Normal, it indicates that the VPN Gateway is ready to use.

> **Note:**
> It usually takes 1-5 minutes to create a VPN Gateway.

Step 2: Create a customer gateway

1. In the left-side navigation pane, click **VPN** > **Customer Gateways**.
2. Click the China (Hangzhou) region.
3. On the **Customer Gateways** page, click **Create Customer Gateway**.

4. Configure the customer gateway according to the following information:
   - **Name**: Enter a customer gateway name.
   - **IP Address**: Enter the public IP configured for the local gateway. In this tutorial, 211.167.68.68 is used.
   - **Description**: Enter the description of the customer gateway.



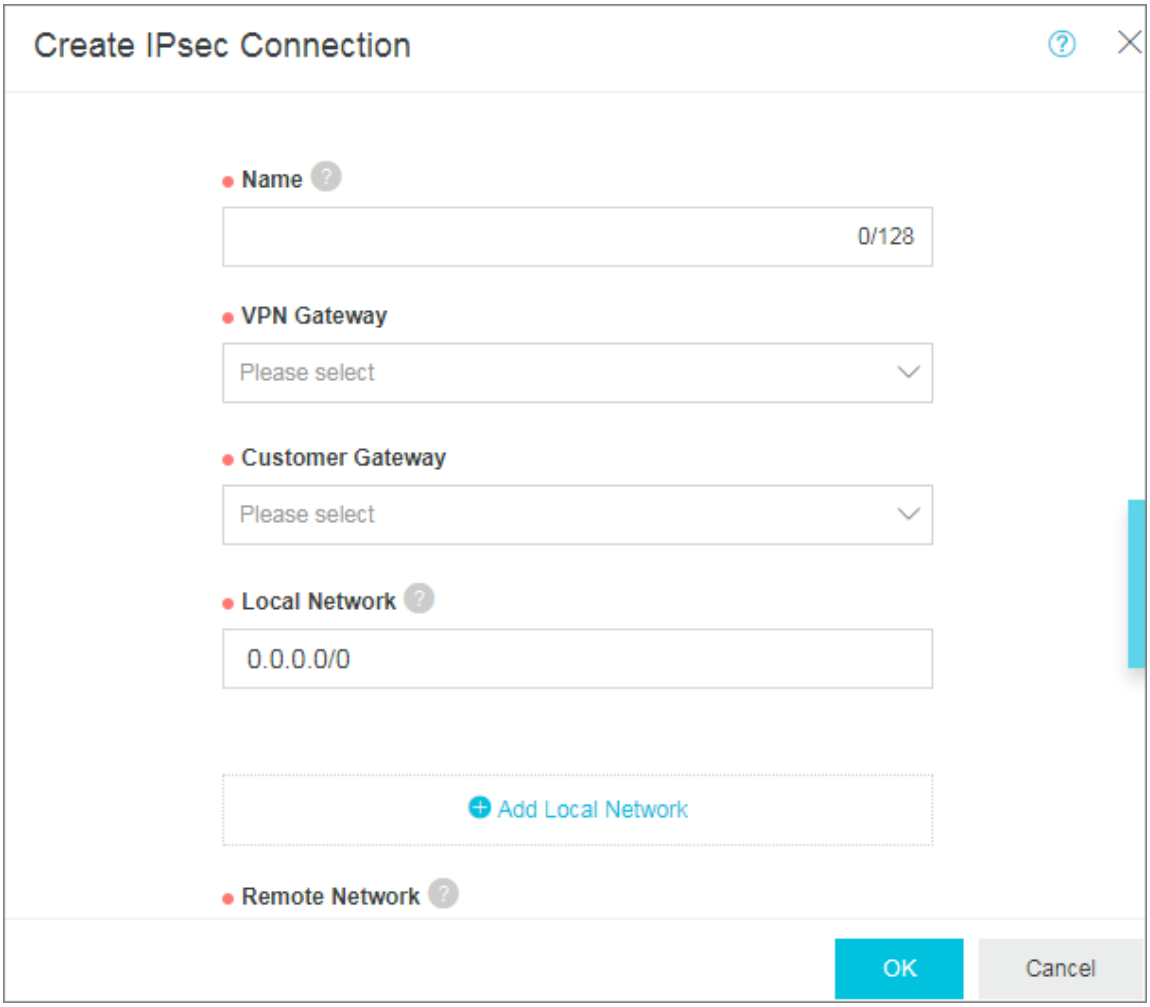
5. On the **Create Customer Gateway** page, click **Add +** to add multiple customer gateways.

Step 3: Create an IPsec connection

1. In the left-side navigation pane, click **VPN** > **IPsec Connections**.
2. Select the China (Hangzhou) region.
3. On the **IPsec Connection** page, click **Create IPsec Connection**.
4. Configure the IPsec connection according to the following information:
   - **Name**: Enter a name for the IPsec connection.
   - **VPN Gateway**: Select the created VPN Gateway.
   - **Customer Gateway**: Select the created customer gateway.

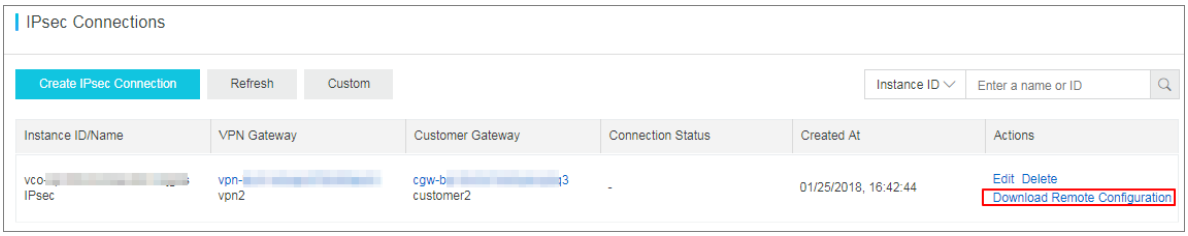
- **Local Network**: Enter the IP address range of the VPC. In this tutorial, 192.168.0.0/16 is used.
- **Remote Network**: Enter the CIDR block of the local data center. In this tutorial, 172.16.0.0/12 is used.
- **Pre-Shared Key**: Enter a pre-shared key. This value must be the same as the one configured in the local gateway.

Use the default configuration for other options.



Step 4: Configure the local gateway

1. In the left-side navigation pane, click **VPN** > **IPsec Connections**.
2. Select the China (Hangzhou) region.
3. Find the target IPsec connection and click **Download Config**.



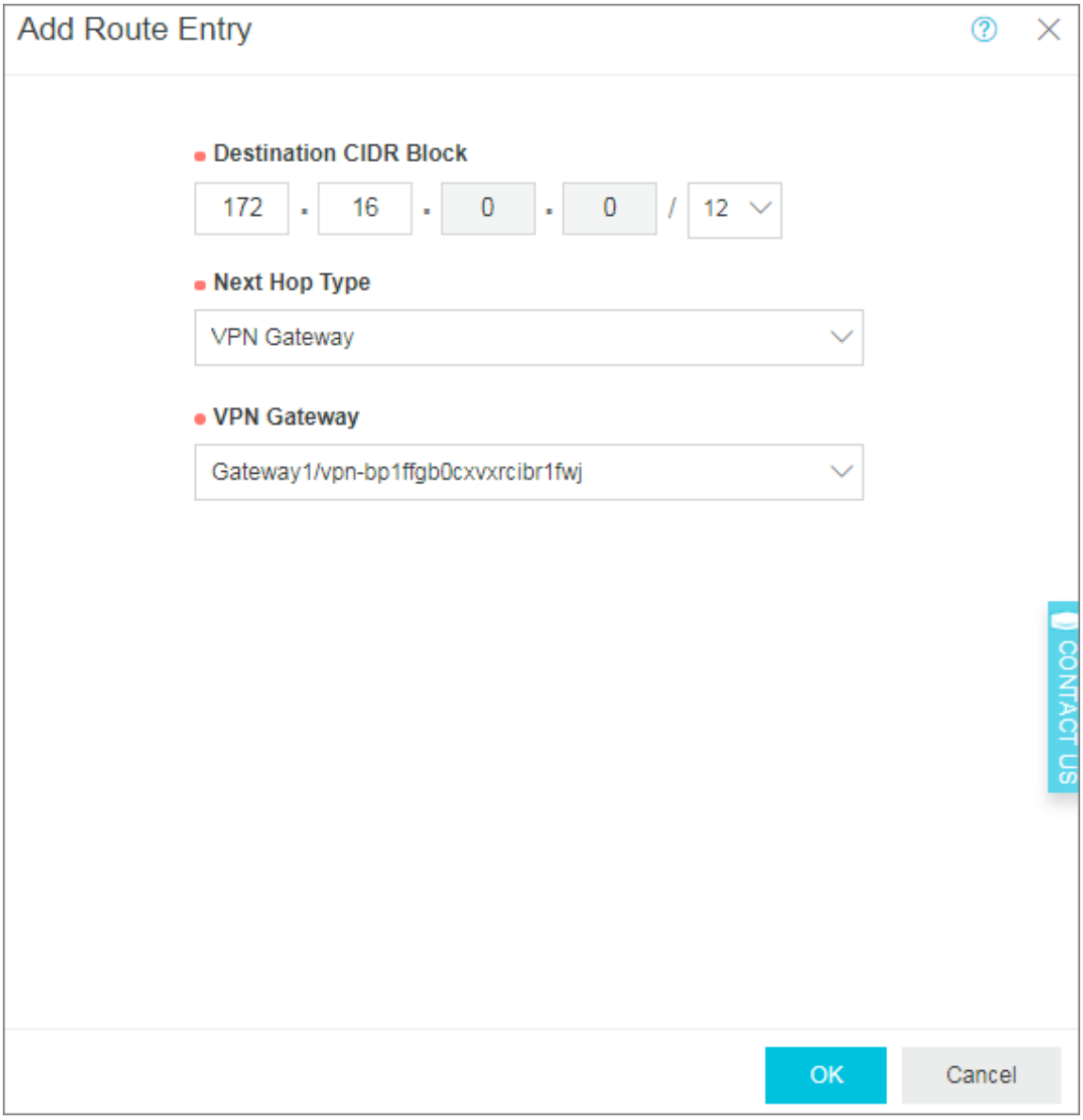
4. Configure the local gateway accordingly. For more information, see *Local gateway configuration*.

   The RemoteSubnet and LocalSubnet in the download configuration are the opposite of the local network and the remote network when creating an IPsec connection. From the perspective of VPN Gateway, the remote network is the local IDC and the local network is the VPC. From the perspective of local IDC, the remote network is the VPC and the local network is the local IDC.

Step 5: Configure the route

1. In the left-side navigation pane, click **Route Tables**.

2. Select the region to which the connected VPC belongs. In this tutorial, the China (Hangzhou) region is selected.
3. Find the target VPC and click **Manage**.
4. On the **Route Tables** page, click **Add route entry**.
5. Configure the route entry according to the following information, and then click **OK**.
   - **Destination CIDR Block**: Enter the IP address range of the local IDC. In this tutorial, 172.16.0.0/12 is used.
   - **Next Hop Type**: Select VPN Gateway.
   - **VPN Gateway**: Select the created VPN gateway.

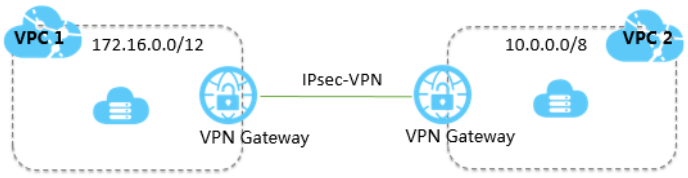


Step 6: Verify the connection

Log on to an ECS instance (without a public IP) in the connected VPC network. Ping the private IP address of a server in the local data center to check whether the connection is established.

3 Configure a VPC-to-VPC connection

This tutorial illustrates how to create an IPsec connection over the IPsec-VPN tunnel to connect two VPCs.



The following two VPCs under the same account are used as an example in this tutorial. The procedure of connecting two VPCs of different accounts is the same as connecting two VPCs under the same account. The only difference is that you must obtain the public IP address of the peer VPN Gateway and use this IP address to create a customer Gateway.

VPC name	VPC name	VPC ID	VPC ID
VPC1	172.16.0.0/12	vpc-xxxxz0	ECS 1
VPC2	10.0.0.0/8	vpc-xxxxut	ECS2

Note:
VPN gateways enable communication by creating an encrypted tunnel over the Internet, and thus the communication performance depends on the quality of Internet connection. If the requirement on the communication quality is high, you can use Express Connect. For more information, see *Cross-account VPC communication* and *Cross-region VPC communication*.

Prerequisites

The IP address ranges of these two VPCs are not in conflict.

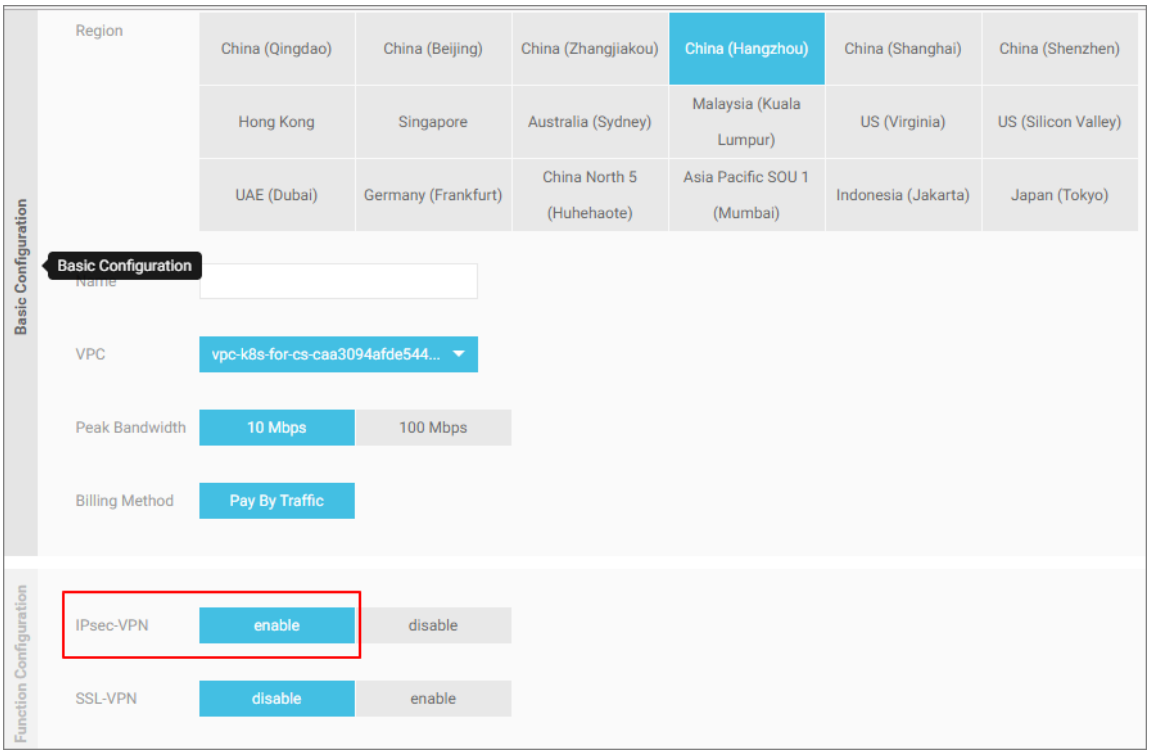
Step 1: Create two VPN Gateways

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **VPN Gateways** .
3. On the VPN Gateways page, click **Create VPN Gateway**.
4. On the purchase page, configure the VPN gateway and complete the payment. In this tutorial, the VPN gateway uses the following configurations:
   - **Region**: Select the region of the VPN gateway. In this operation, select **China (Hangzhou)**.

> **Note:**
> Make sure that the region of the VPC to be connected and the region of the VPN Gateway are the same.

- **VPC**: Select the VPC to be connected.
- **Bandwidth specification**: Select a bandwidth specification. The bandwidth specification is the Internet bandwidth of the VPN gateway.
- **IPsec-VPN**: Select whether to enable the IPsec-VPN feature.
- **SSL-VPN**: Select whether to enable the SSL-VPN feature. The SSL-VPN feature allows you to connect to a VPC from a single computer anywhere.
- **Concurrent SSL Connections**: Select the maximum number of clients you want to connect to simultaneously.

> **Note:**
> You can only configure this option after you enables the SSL-VPN feature.

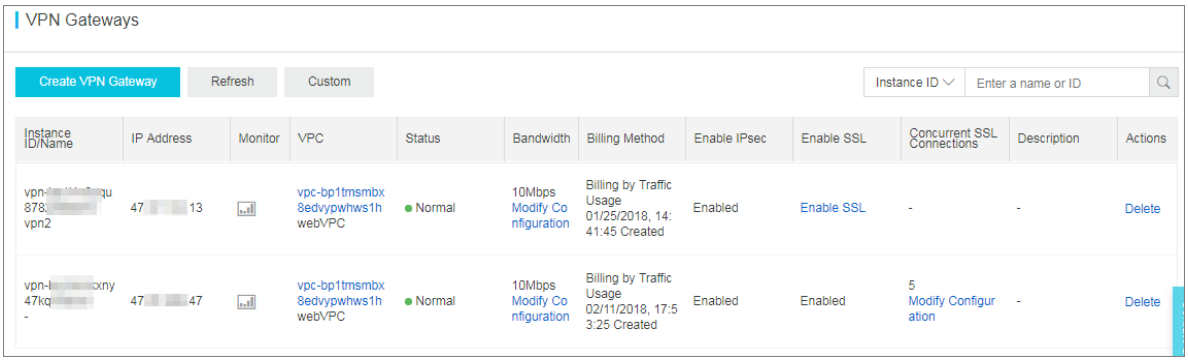


5. Repeat the preceding steps to create a VPN gateway for the other VPC.

   The initial status of a VPN Gateway is Preparing. It changes to Normal in about 2 minutes. When it changes to Normal, it indicates that the VPN Gateway is ready to use. VPN After the gateway is created, the system automatically assigns two Internet IPs.

Note:

It usually takes 1-5 minutes to create a VPN gateway.



In this tutorial, the public IP address assigned is 121. XXX. XX.143 and 118. XXX. XX.149, as shown in the following table.

VPC	VPN Gateway	IP address
Name: VPC1 ID: vpc-xxxxz0 IP address range: 172.16.0.0 /12	vpn-xxxxxqwj	118.xxx.xx.149
Name: vpc2 ID: vpc-xxxxut IP address range: 10.0.0.0/8	vpn-xxxxxl5z	121. x

Step 2: Create two customer Gateways

1. In the left-side navigation pane, click **VPN** > **Customer Gateways** .
2. Select the China (Hangzhou) region.
3. On the **Customer Gateways** page, click **Create Customer Gateway**.
4. Configure the customer gateway according to the following information:
   - **Name**: Enter the name of the customer gateway.
   - **IP Address**: Enter the public IP address of the VPN gateway of the peer VPC.
   - **Description**: Enter the description of the customer gateway.
5. Repeat these steps to create another customer gateway using the public IP address of the other VPN Gateway.

   After creating two customer Gateways in this tutorial, the relationship between VPC, VPN Gateways and customer Gateways are as follows:

VPC	VPN Gateway	IP address	Customer Gateway
Name: VPC1 ID: vpc-xxxxz0 IP address range: 172.16.0.0/12	vpn-xxxxxqwj	121.xxx.xx.143	user_VPC1
Name: VPC2 ID: vpc-xxxxut IP address range: 10.0.0.0/8	vpn-xxxxxl5z	118.xxx.xx.149	user_VPC

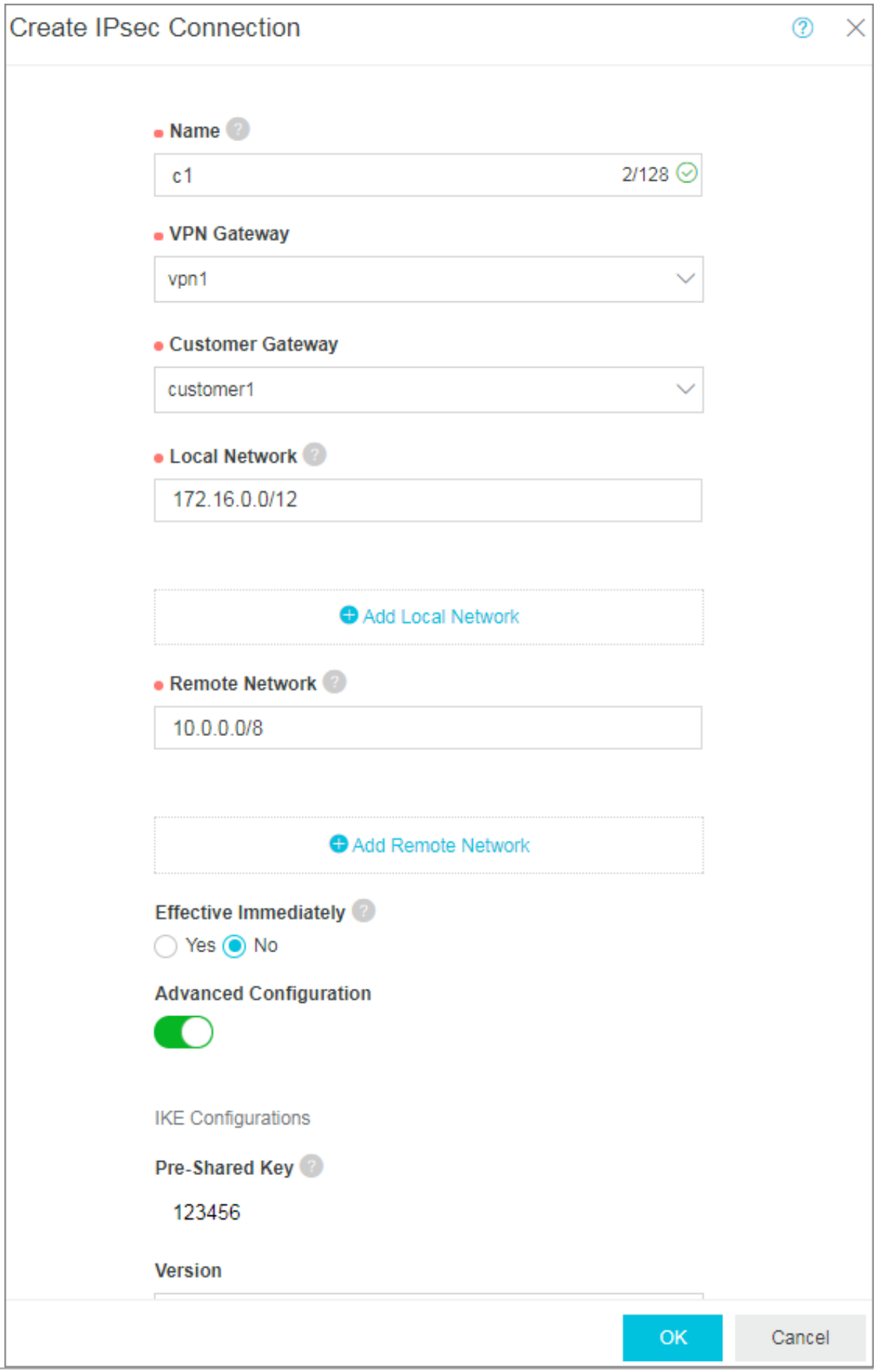
Step 3: Create two IPsec connections

After creating the VPN gateways and the customer gateways, you must create two IPsec connections to build the VPN channels:

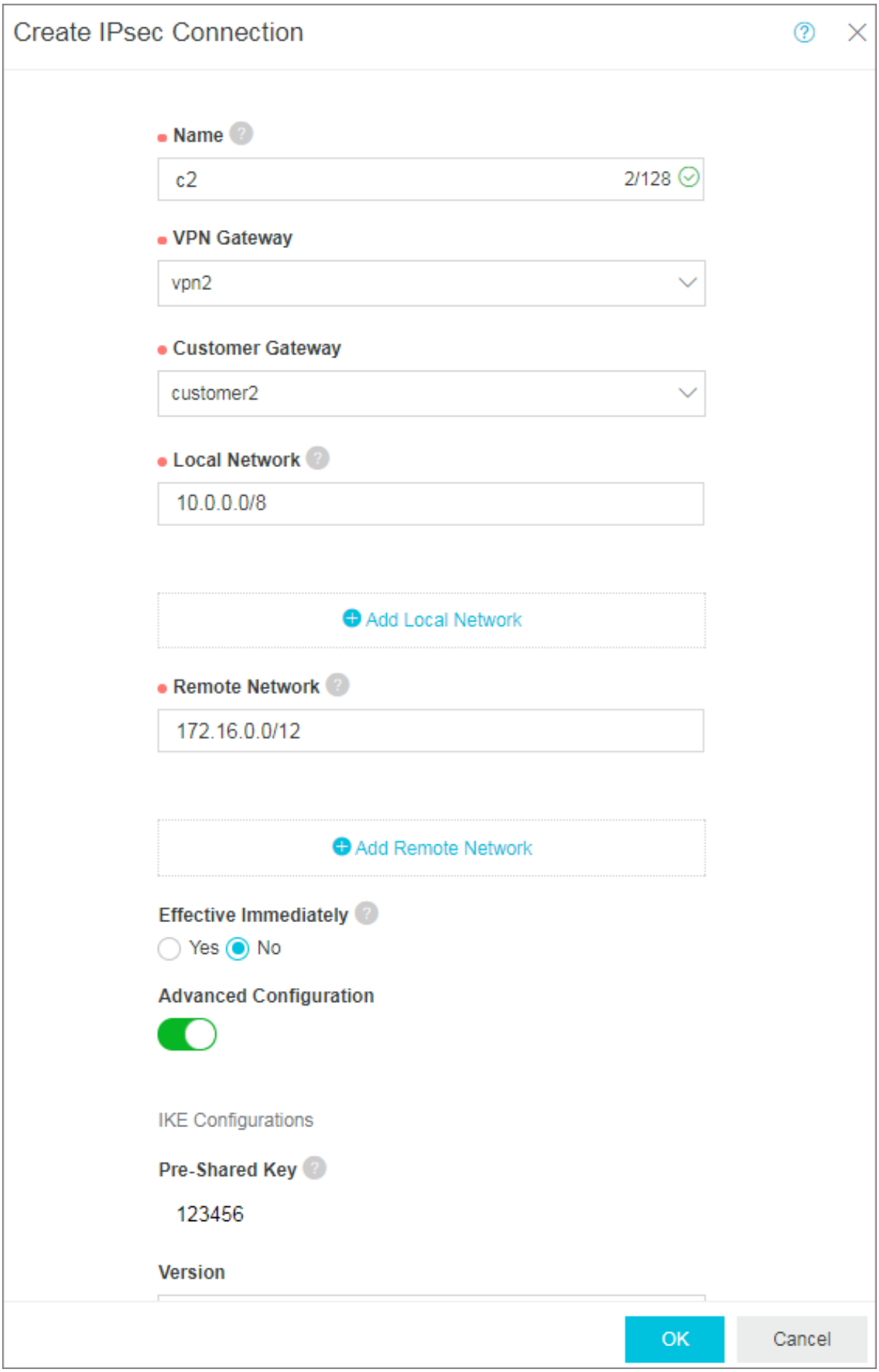
1. In the left-side navigation pane, click **VPN** > **IPsec Connections**.
2. Select the China (Hangzhou) region.
3. On the **IPsec Connections** page, click **Create IPSec Connection**.
4. Configure the IPsec connection according to the following information:
   - **Name**: Enter a name for the IPsec connection.
   - **VPN Gateway**: Select the created VPN Gateway. In this tutorial, the VPN gateway vpn-xxxxxqwj of VPC1 is selected.
   - **Customer Gateway**: Select the customer gateway created by using the public IP address of the peer VPN gateway. In this tutorial, the customer gateway user_VPC2 of VPC2 is selected.

     .
   - **Local Network**: Enter the IP address range of the VPC to which the selected VPN gateway belongs. In this tutorial, the IP address range 172.16.0.0/12 of VPC1 is entered.
   - **Remote Network**: Enter the IP address range of the peer VPC. In this tutorial, the IP address range 10.0.0.0/8 of VPC2 is entered.
   - **Pre-Shared Key**: Enter a pre-shared key. In this tutorial, 123456 is entered. This value must be the same as configured in the other IPsec connection.
5. Repeat these steps to create another IPsec connection.

   In this tutorial, the IPsec connection configurations of VPC1 is as follows:


Create IPsec Connection
Name
c1
2/128
VPN Gateway
vpn1
Customer Gateway
customer1
Local Network
172.16.0.0/12
Add Local Network
Remote Network
10.0.0.0/8
Add Remote Network
Effective Immediately
Yes
No
Advanced Configuration
IKE Configurations
Pre-Shared Key
123456
Version
OK
Cancel

In this tutorial, the IPsec connection configurations of VPC2 is as follows:


Create IPsec Connection
Name
c2
2/128
VPN Gateway
vpn2
Customer Gateway
customer2
Local Network
10.0.0.0/8
Add Local Network
Remote Network
172.16.0.0/12
Add Remote Network
Effective Immediately
Yes
No
Advanced Configuration
IKE Configurations
Pre-Shared Key
123456
Version
OK
Cancel

Step 4: Configure routes

1. In the left-side navigation pane, click **Route Tables**.
2. Select the region to which the connected VPC belongs. In this tutorial, the China (Hangzhou) region is selected.
3. Find VPC1 and click **Manage**.
4. On the **Route Tables** page, click **Add Route Entry**.
5. Configure the route entry according to the following information and then click **OK**.
   - **Destination CIDR Block**: Enter the IP address range of the peer VPC. In this tutorial, the IP address range 10.0.0.0/8 of VPC2 is entered.
   - **Next Hop Type**: Select VPN Gateway.
   - **VPN Gateway**: Select the VPN gateway deployed in the local VPC. In this tutorial, the VPN gateway created for VPC1 is selected.
6. Repeat these steps to add a route entry for VPC2. In the route entry, the destination CIDR block is 172.16.0.0/12, and the next hop is the VPN gateway of VPC2.

   In this tutorial, the route configurations are as follows:

VPC	Destination CIDR block	Next hop type	Next hop
VPC1	10.0.0.0/8	VPN Gateway	The VPN Gateway created in this tutorial for VPC1 is vpn-xxxxxqwj.
VPC2	172.16.0.0/12	VPN Gateway	The VPN Gateway created in this tutorial for VPC2 is vpn-xxxxxl5z.

Step 5: Verify the connection

Log on to the ECS1, and then Ping the private IP address of the ECS2 to check whether the connection is established.