ALIBABA CLOUD

Alibaba Cloud

VPN Gateway

IPsec-VPN Quick Start

Document Version: 20210121

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Tutorial overview

This topic describes how to connect a VPC to an on-premises data center through IPsec-VPN.

Prerequisites

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

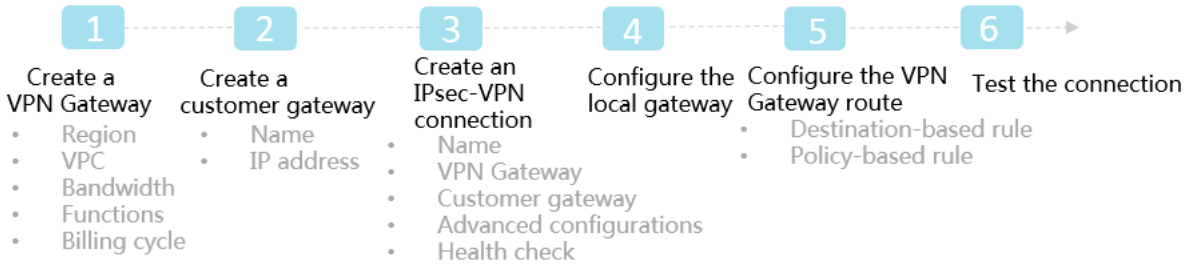
- The protocols IKEv1 and IKEv2 are supported by the gateway device of the on-premises data center.

  IPsec-VPN supports IKEv1 and IKEv2 protocols. Devices that support these two protocols can connect to Alibaba Cloud VPN Gateway, including devices of Huawei, H3C, Hillstone, SANGFOR, Cisco ASA, 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 on-premises data center to be connected do not conflict with each other.

Procedure

The following figure shows the procedure of connecting a VPC to an on-premises data center through IPsec-VPN.



1. Create a VPN Gateway

   Enable the IPsec-VPN function. Up to 10 IPsec-VPN connections can be established in a VPN Gateway.

2. Create a customer gateway

   By creating a customer gateway, you can register the local gateway to Alibaba Cloud and connect the customer gateway to the VPN Gateway. A customer gateway can be connected to multiple VPN Gateways.

3. Create an IPsec connection

   An IPsec connection is a VPN channel established between a VPN Gateway and a customer gateway. The encrypted communication between the VPN Gateway and the on-premises data center can be achieved only after the IPsec connection is established.

4. Configure the local gateway

   You need to load the VPN Gateway configurations to the local gateway device. For more information, see Local CPE configurations.

5. Configure the VPN Gateway route

   You need to configure a route in the VPN Gateway and publish it to the VPC route table. For more information, see VPN Gateway route overview.

6. Test the connection

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

For more information, see Connect on-premises data centers to VPC networks.

2.Connect on-premises data centers to VPC networks

This topic describes how to create IPsec-VPN connections on VPN gateways to connect an on-premises data center to a Virtual Private Cloud (VPC) network.

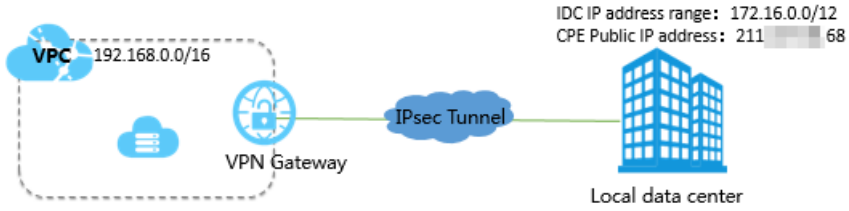
Prerequisites

Before you start, make sure that the following requirements are met:

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, click Create an Alibaba Cloud account.
- Check the gateway device in the on-premises data center. Alibaba Cloud VPN gateways support the standard IKEv1 and IKEv2 protocols. Any gateway device that supports these two protocols can connect to Alibaba Cloud VPN gateways, such as gateway devices manufactured by Huawei, H3C, Hillstone, Sangfor, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.
- Make sure that you have set a static public IP address for the gateway device in the on-premises data center.
- The CIDR block of the on-premises data center must not overlap with that of the VPC network.

Context

For example, a company creates a VPC network on Alibaba Cloud. The CIDR block of the VPC network is 192.168.0.0/16. The CIDR block of the on-premises data center is 172.16.0.0/12. The static public IP address for the gateway device in the on-premises data center is 211.xx.xx.68. To meet business requirements, the company needs to connect the on-premises data center to the VPC network.



The preceding figure displays that the on-premises data center is connected to the VPC network through IPsec-VPN. Cloud resources can be shared with on-premises data centers.

Step 1: Create a VPN gateway

Take the following steps to create a VPN gateway:

1. Log on to the VPN gateway console.
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. On the **VPN Gateways** page, click **Create VPN Gateway**.
4. On the buy page, set the following parameters, click **Buy Now**, and complete the payment.
   - **Name**: Enter a name for the VPN gateway.
   - **Region**: Select the region where you want to deploy the VPN gateway.

> **Note** Make sure that the VPC network and the VPN gateway associated with the VPC network are deployed in the same region.

- **VPC**: Select the VPC network to be associated with the VPN gateway.
- **Bandwidth**: Specify the maximum bandwidth of the VPN gateway. The bandwidth is provided for data transfer over the Internet.
- **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway.
- **SSL-VPN**: Specify whether to enable SSL-VPN. SSL-VPN allows you to connect a client to a VPC network from any places.
- **SSL Connections**: Specify the maximum number of concurrent SSL connections that the VPN gateway supports.

  > **Note** This parameter is available only after SSL-VPN is enabled.

- **Billing Cycle**: Specify the subscription duration.

5. Go to the VPN Gateways page to view the newly created VPN gateway. The newly created VPN gateway is in the Preparing state. Its status changes to Normal after about two minutes. The Normal state indicates that the VPN gateway is initialized and ready for use.

   > **Note** It takes about one to five minutes to create a VPN gateway.

Step 2: Create a customer gateway

Take the following steps to create a customer gateway.

1. In the left-side navigation pane, choose **VPN > Customer Gateways**.
2. Select the region where you want to deploy the customer gateway
3. On the **Customer Gateways** page, click **Create Customer Gateway**.
4. On the **Create Customer Gateway** page, set the following parameters, and then click **Submit**.
   - **Name**: Enter a name for the customer gateway.
   - **IP Address**: Enter the public IP address of the gateway device in the on-premises data center that is to be connected to the VPC network. In this example, enter **211.xx.xx.68**.
   - **Description**: Enter a description for the customer gateway.

Step 3: Create an IPsec-VPN connection

Take the following steps to create an IPsec-VPN connection:

1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. Select the region where you want to create an IPsec-VPN connection.
3. On the **IPsec Connections** page, click **Create IPsec Connection**.
4. On the **Create IPsec Connection** page, set the following parameters for the IPsec-VPN connection, and click **Submit**.
   - **Name**: Enter a name for the IPsec-VPN connection.
   - **VPN Gateway**: Select a VPN gateway.

- **Customer Gateway**: Select the customer gateway to be connected through the IPsec-VPN connection.
- **Source CIDR Block**: Enter the CIDR block of the VPC network with which the selected VPN gateway is associated. In this example, enter **192.168.0.0/16**.
- **Destination CIDR Block**: Enter the CIDR block of the on-premises data center. In this example, enter **172.16.0.0/12**.
- **Immediate Effect**: Specify whether to start connection negotiations immediately.
  - **Yes**: negotiate immediately after the configuration is complete.
  - **No**: negotiate when traffic is detected in the IPsec-VPN connection.
- **Pre-shared Key**: Enter the pre-shared key. The pre-shared key must be the same as that of the gateway device deployed in the on-premises data center.

  Use the default settings for other parameters.

Step 4: Load the configurations of the IPsec-VPN connection to the customer gateway device

Take the following steps to load the configurations of the IPsec-VPN connection to the customer gateway device:

1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. Select the region where the IPsec-VPN connection is established.
3. On the **IPsec Connections** page, find the target IPsec-VPN connection, and then choose **More > Download Configuration** in the **Actions** column.
4. Load the configurations of the IPsec-VPN connection to the customer gateway device by following the instructions described in Configure customer gateways. . RemotSubnet and LocalSubnet in the downloaded configurations are opposite to RemotSubnet and LocalSubnet that you specify when you create an IPsec-VPN connection. For a VPN gateway, RemotSubnet refers to the CIDR block of the on-premises data center and LocalSubnet refers to the CIDR block of the VPC network. For a customer gateway, LocalSubnet refers to the CIDR block of the on-premises data center and RemoteSubnet refers to the CIDR block of the VPC network.

Step 5: Configure routes for the VPN gateway

Take the following steps to configure routes for the VPN gateway:

1. In the left-side navigation pane, choose **VPN > VPN Gateways**.
2. Select the region where the VPN gateway is deployed.
3. On the **VPN Gateways** page, find the target VPN gateway, and then click the instance ID in the **Instance ID/Name** column.
4. In the **Destination-based routing** tab, click **Add Route Entry**.
5. In the **Add Route Entry** dialog box, set the following parameters and click **OK**.
   - **Destination CIDR Block**: Enter the CIDR block of the on-premises data center. In this example, enter **172.16.0.0/12**.
   - **Next Hop Type**: Select IPsec Connection.
   - **Next Hop**: Select an IPsec instance.
   - **Publish to VPC**: Specify whether to automatically publish new route entries to the VPC route

table. In this example, select **Yes**.

- **Weight**: Select a weight. In this example, select **100**.

Step 6: Verify the settings

Log on to an Elastic Compute Service (ECS) instance that is not assigned a public IP address in the VPC network. Run the **ping** command to **ping** the private IP address of a server that resides in the on-premises data center, and test the connectivity.

3.Establish a connection between a VPC network and an on-premises data center with BGP dynamic routing

This topic describes how to use the IPsec-VPN feature to establish a connection between a Virtual Private Cloud (VPC) network and an on-premises data center, and how to use Border Gateway Protocol (BGP) dynamic routing to connect the VPC network and on-premises data center. This reduces network maintenance costs and network configuration errors.

Prerequisites

Before you start, make sure the following requirements are met:

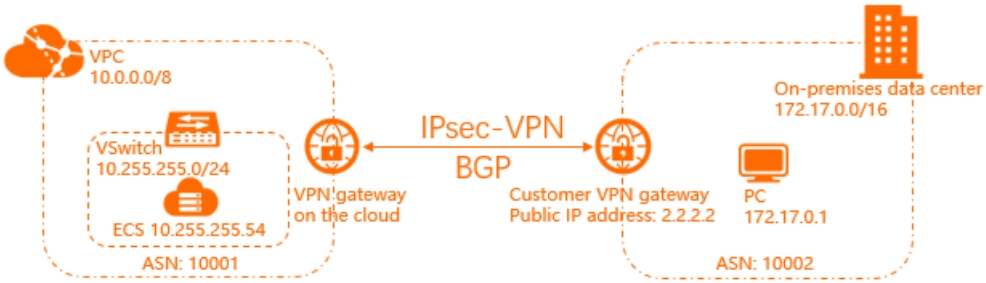
- You have created an Alibaba Cloud account. To create an Alibaba Cloud account, log on to the Alibaba Cloud site. For more information, see Create an Alibaba Cloud account.
- You have created a VPC network that you want to connect to your on-premises data center. The CIDR block of the VPC is different from that of the on-premises data center. For more information, see Create a VPC.

Context

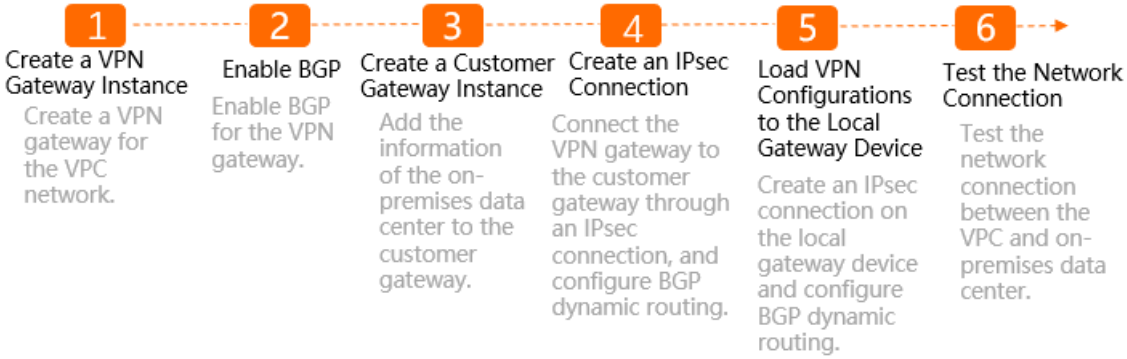
This topic takes the following scenario as an example. A company has created a VPC network in Germany (Frankfurt). The CIDR block of the VPC is 10.0.0.0/8 and the Autonomous System Number (ASN) is 10001. The company has an on-premises data center in Frankfurt. The public IP address of the data center is 2.2.2.2, the CIDR block is 172.17.0.0/16, and the ASN is 10002. The company needs to establish a connection between the VPC network and the on-premises data center for business development.

You can use the IPsec-VPN feature to establish a connection between the VPC network and on-premises data center, and configure BGP dynamic routing. After configuration, network interconnection can be achieved by using the dynamic routing protocol to automatically learn routes. This reduces network maintenance costs and network configuration errors.

> **Note** An Autonomous System (AS) is a small unit that independently decides which routing protocol to adopt in the system. This unit is an independent and manageable network unit. It may consist of a simple network or a network group that is controlled by one or more network administrators. Each AS has a specific identifier called ASN.



Procedure



Step 1: Create a VPN gateway instance

VPN Gateway enables network connections and achieves encrypted communications on the Internet. Create a VPN gateway instance for the VPC network that you want to connect to the on-premises data center.

To create a VPN gateway instance, follow these steps:

1. Log on to the VPN gateway console.
2. On the **VPN Gateways** page, click **Create VPN Gateway**.
3. On the buy page, set the following parameters, and create a VPN gateway instance.
   - **Name**: Enter a name for the VPN gateway instance. In this example, enter **VPN**.
   - **Region**: Select the region where the VPN gateway instance is deployed.

     The VPN gateway instance and the VPC network must be deployed in the same region. In this example, select **Germany (Frankfurt)**.
   - **VPC**: Select the VPC network that you want to connect. In this example, select the VPC network that is created in Germany (Frankfurt).
   - **Assign VSwitch**: Choose whether to assign a VSwitch to the VPN gateway instance. In this example, select **No**.
   - **VSwitch**: Select the VSwitch to which the VPN gateway instance is attached.

     > **Note** The option is only displayed when you select **Yes** in the **Assign VSwitch** section.
   - **Peak Bandwidth**: Select the peak bandwidth.

     The peak bandwidth refers the maximum Internet bandwidth of the VPN gateway instance. In this example, select **5 Mbps**.
   - **IPsec-VPN**: Specify whether to enable the IPsec-VPN feature.

     You can use IPsec-VPN to connect an on-premises data center to a VPC network or connect multiple VPC networks. In this example, select **Enable**.
   - **SSL-VPN**: Specify whether to enable the SSL-VPN feature.

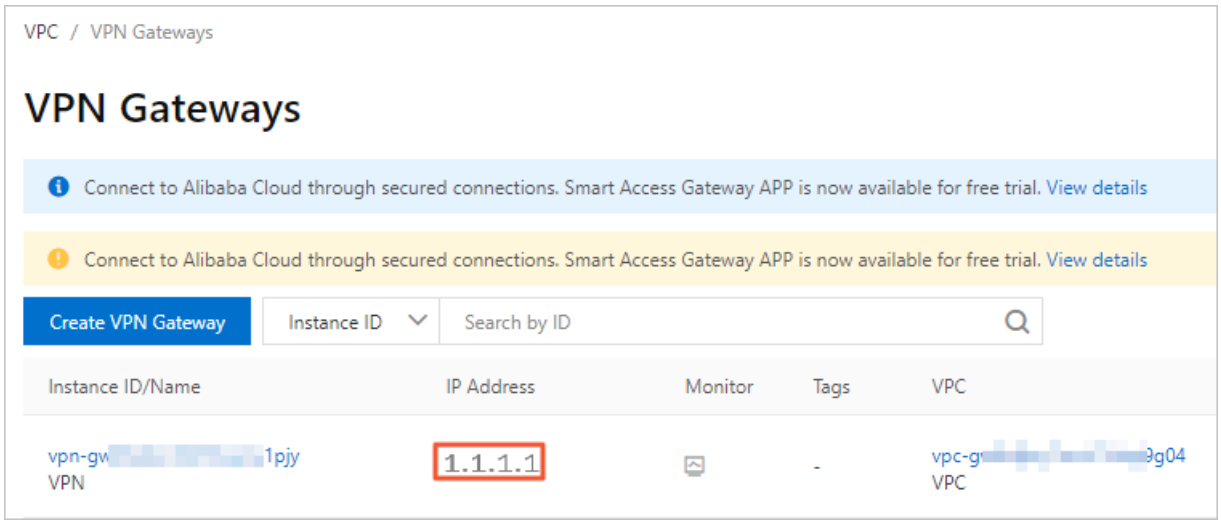
     The SSL-VPN feature allows you to connect to a VPC network from a local host that is located in any region. In this example, select **Disabled**.
   - **SSL Connections**: Specify the maximum number of concurrent SSL connections.

> **Note** You can configure SSL connections only when SSL-VPN authentication is enabled.

- **Billing Cycle**: Select a billing cycle for the VPN gateway instance.

4. Click **Buy Now** to complete the payment.

It takes about 1 to 5 minutes to create a VPN gateway instance. The status of a newly created VPN gateway instance is Preparing and then changes to Normal after about two minutes. After the status changes to Normal, the VPN gateway instance is ready to use. After the VPN gateway instance is created, a public IP address is automatically assigned to the instance for establishing VPN connections.



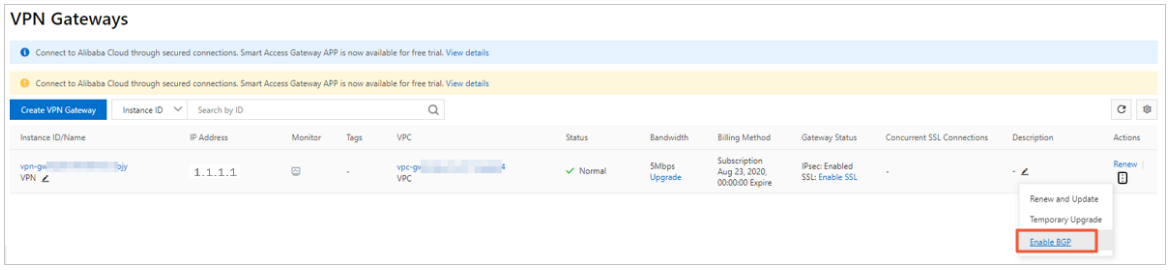
Step 2: Enable BGP

BGP is used to exchange routing information in different ASs. To use the BGP feature, you need to enable BGP for the VPN gateway instance.

> **Note** The BGP feature cannot be disabled after it is enabled.

To enable BGP, follow these steps:

1. In the left-side navigation pane, select **VPN > VPN Gateways**.
2. On the **VPN Gateways** page, find the VPN gateway instance created in step 1, and click **Enable BGP** in the **Actions** column.



3. In the **Enable BGP** page that appears, select whether to propagate BGP routes to the VPC network.
   - **Yes**: The VPN gateway instance automatically propagates BGP routes to the VPC network.
   - **No**: The VPN gateway instance does not propagate BGP routes to the VPC network. You need

to manually advertise BGP routes to the VPC network.

In this example, select **Yes**.

4. Click **OK**.

After you enable the BGP feature for the VPN gateway instance, the status of the VPN gateway changes to **Enable BGP**.

Step 3: Create a customer gateway instance

You can create a customer gateway instance to register and update information about the on-premises data center to Alibaba Cloud, and then connect the customer gateway instance to the VPN gateway instance.

To create a customer gateway instance, follow these steps:

1. In the left-side navigation pane, select **VPN > Customer Gateways**.
2. On the **Customer Gateways** page, click **Create Customer Gateway**.
3. On the **Create Customer Gateway** page that appears, set the following parameters:
   - **Name**: Enter a name for the customer gateway instance. In this example, enter **CGW**.
   - **IP Address**: Enter the public IP address of the gateway device in the on-premises data center. In this example, enter **2.2.2.2**.
   - **ASN**: Enter the ASN of the on-premises data center network. In this example, enter **10002**.
   - **Description**: Enter a description for the customer gateway instance.
4. Click **OK**.

Step 4: Create an IPsec connection

IPsec-VPN is based on routes. It facilitates the configuration and maintenance of VPN policies, and provides flexible traffic routing methods.

To create an IPsec connection, follow these steps:

1. In the left-side navigation pane, select **VPN > IPsec Connections**.
2. On the **IPsec Connections** page, click **Create IPsec Connection**.
3. On the **Create IPsec Connection** page that appears, set the following parameters:
   - **Name**: Enter a name for the IPsec-VPN connection. In this example, enter **VPC TO IDC**.
   - **VPN Gateway**: Select a VPN gateway instance.

     In this example, select the VPN gateway instance that is created in step 1. For more information, see Step 1: Create a VPN gateway instance.
   - **Customer Gateway**: Select a customer gateway instance.

     In this example, select the customer gateway instance that is created in step 3. For more information, see Step 3: Create a customer gateway instance.
   - **Local Network**: Enter the CIDR block of the VPC network. In this example, enter **10.0.0.0/8**.
   - **Remote Network**: Enter the CIDR block of the on-premises data center. In this example, enter **172.17.0.0/16**.
   - **Effective Immediately**: Specify whether to negotiate immediately.
     - Yes: Negotiate immediately after the configuration is completed.

- No: Negotiate only when traffic is detected.

In this example, select **Yes**.

- **Pre-shared key**: Enter a pre-shared key (PSK).

  The pre-shared key must be the same as that configured for the local gateway. In this example, enter **123456**.
- **Version**: Select an Internet Key Exchange (IKE) version. In this example, select **ikev2**.
- **Encryption Algorithm**: Select an encryption algorithm. In this example, select **aes**.
- **Authentication Algorithm**: Select an authentication algorithm. In this example, select **sha1**.
- **DH Group**: Select a DH group. In this example, select **group2**.
- **Tunnel CIDR Block**: Enter the CIDR block of the IPsec tunnel. The subnet mask of the CIDR block is 30 bits in 169.254.0.0/16. In this example, enter **169.254.10.0/30**.
- **Local BGP IP Address**: Enter the local BGP IP address. This IP address is within the IPsec tunnel CIDR block. In this example, enter **169.254.10.1**.

  > **Note** Make sure that the BGP IP addresses of the VPC network and the on-premises data center do not conflict with each other.
- **ASN**: Enter the ASN of the VPC network. In this example, enter **10001**.

Use the default settings for the other parameters.

4. Click **OK**.

Step 5: Load VPN configurations to the local gateway device

To establish a connection between the VPC network and the on-premises data center, you need to load VPN configurations to the local gateway device after creating the IPsec connection in the cloud.

The following example shows how to load VPN configurations to the local gateway device in the Cisco IOSXE system.

1. Log on to the command line interface of the Cisco firewall device.
2. Run the following commands to set the IKEv2 proposal and policy.

```
crypto ikev2 proposal alicloud
encryption aes-cbc-128 //Set the encryption algorithm. Set to aes-cbc-128 in this example.
integrity sha1 //Set the authentication algorithm. Set to sha1 in example.
group2 //Set the DH group. Set to group2 in this example.
exit
!
crypto ikev2 policy Pureport_Pol_ikev2
proposal Pureport_prop
exit
!
```

3. Run the following commands to set the IKEv2 keyring.

```
crypto ikev2 keyring alicloud
peer alicloud
address 1.1.1.1 //Set the public IP address for the VPN gateway instance of the VPC network. Set to 1.1.1.1 in this example.
pre-shared-key 123456 //Set the pre-shared key. Set to 123456 in this example.
exit
!
```

4. Run the following commands to set the IKEv2 profile.

```
crypto ikev2 profile alicloud
match identity remote address 1.1.1.1 255.255.255.255 //Match the public IP address for the VPN gateway instance of the VPC network. The matched address is 1.1.1.1 in this example.
identity local address 2.2.2.2 //Set the public IP address for the VPN gateway instance of the on-premises data center. Set to 2.2.2.2 in this example.
authentication remote pre-share //Set the authentication mode for remote networks to PSK.
authentication local pre-share //Set the authentication mode for local networks to PSK.
keyring local alicloud //Invoke the IKEv2 keyring.
exit
!
```

5. Run the following commands to set the transform.

```
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
mode tunnel
exit
!
```

6. Run the following commands to set the IPsec profile and to invoke the transform, PFS, and IKEv2 profile.

```
crypto ipsec profile alicloud
set transform-set TSET
set pfs group2
set ikev2-profile alicloud
exit
!
```

7. Run the following commands to set the IPsec tunnel.

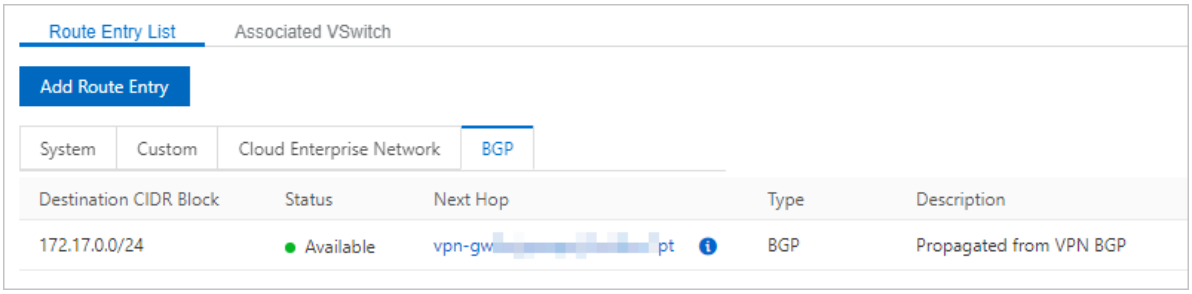
```
interface Tunnel100
ip address 169.254.10.2 255.255.255.252 //Set the tunnel address for the local network (on-premises data center). Set to 169.254.10.2 in this example.
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 1.1.1.1 //Set the public IP address for the remote network (VPN gateway instance). Set to 1.1.1.1 in this example.
tunnel protection ipsec profile alicloud
no shutdown
exit
!
interface GigabitEthernet1
ip address 2.2.2.2 255.255.255.0
negotiation auto
Exclamation points (!)
```

8. Run the following commands to set the BGP routing protocol.

```
router bgp 10002 //Enable the BGP routing protocol and set an ASN for the local network (on-premises data center). Set to 10002 in this example.
bgp router-id 169.254.10.2 //Set the BGP router ID. Set to 169.254.10.2 in this example.
bgp log-neighbor-changes
neighbor 169.254.10.1 remote-as 10001 //Set an ASN for the BGP neighbor.
neighbor 169.254.10.2 ebgp-multihop 10 //Set the EBGP hop-count to 10.
!
address-family ipv4
network 172.17.0.0 mask 255.255.0.0 //Advertise the CIDR block of the local network (on-premises data center). The CIDR block is 172.17.0.0/16 in this example.
neighbor 169.254.10.1 activate //Activate the BGP neighbor.
exit-address-family
!
```

After the establishment of the IPsec connection, the following routes are advertised by VPN gateway instances of the VPC network and the on-premises data center.

- The local VPN gateway instance automatically learns routes from the CIDR block of the on-premises data center through BGP, and then advertises the routes to the VPN gateway instance of the VPC network. The VPN gateway instance of the VPC network automatically propagates the learned routes to the VPC route table.



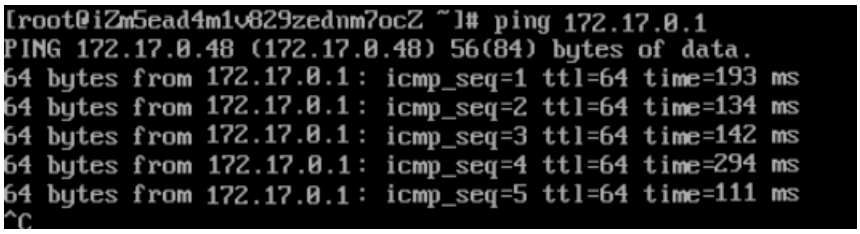
- The VPN gateway instance of the VPC network automatically learns routes from the CIDR block of the VPC network through BGP, and then advertises the routes to the VPN gateway instance of the on-premises data center.

Step 6: Test the network connection

After the IPsec connection is established, you can test the network connectivity between the VPC network and the on-premises data center.

> **Note** Make sure that the firewall rules for the terminal in the on-premises data center allow remote connections.

1. Log on to an ECS instance in the connected VPC network.
2. Run the `ping` command to `ping` the IP address of the terminal in the on-premises data center to check whether the network connection is established.The ECS instance in the VPC network can access the terminal in the on-premises data center.



3. Log on to the terminal in the on-premises data center.
4. Run the `ping` command to `ping` the IP address of the ECS instance in the VPC network to check whether the network connection is established.The terminal in the on-premises data center can access the ECS instance in the VPC network.

```
Router#ping 10.255.255.54 source 172.17.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.54, timeout is 2 seconds:
Packet sent with a source address of 172.17.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 154/154/155 ms
```