ALIBABA CLOUD

Alibaba Cloud

VPN Gateway

IPsec-VPN Quick Start

Document Version: 20211228

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.Overview of IPsec-VPN

IPsec-VPN allows you connect a data center to a VPC. This topic describes how to use IPsec-VPN.

Prerequisites

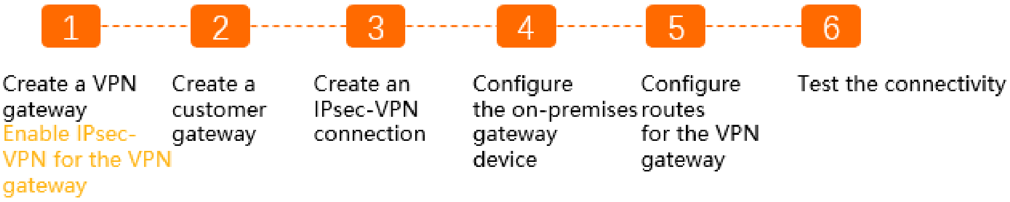
Before you use IPsec-VPN to connect a data center to a VPC, make sure that the following requirements are met:

- The gateway device in the data center supports the IKEv1 and IKEv2 protocols.

  IPsec-VPN supports the IKEv1 and IKEv2 protocols. All gateway devices that support these two protocols can connect to VPN gateways on Alibaba Cloud.

- A static public IP address is assigned to the gateway device in the data center
- The CIDR block of the data center does not overlap with the CIDR block of the VPC.
- You have read and understand the security group rules that apply to the Elastic Compute Service (ECS) instances in the VPC, and the security rules allow gateway devices in the data center to access cloud resources. For more information, see Query security group rules.

Procedure


1
Create a VPN gateway
Enable IPsec-VPN for the VPN gateway
2
Create a customer gateway
3
Create an IPsec-VPN connection
4
Configure the on-premises gateway device
5
Configure routes for the VPN gateway
6
Test the connectivity

1. Create a VPN gateway

   You must enable the IPsec-VPN feature for the VPN gateway. You can create multiple IPsec-VPN connections for each VPN gateway.

2. Create a customer gateway

   A customer gateway registers the information about the gateway device in the data center to Alibaba Cloud.

3. Create an IPsec-VPN connection

   An IPsec-VPN connection is a VPN channel between the VPN gateway and the gateway device in the data center. The data center can exchange encrypted data with Alibaba Cloud only after an IPsec-VPN connection is created.

4. Configure the gateway device

   You must load the configuration of the VPN gateway on Alibaba Cloud to the gateway device in the data center. For more information, see Configure a gateway device in a data center.

5. Configure routes for the VPN gateway

   You must configure routes for the VPN gateway and advertise these routes to the VPC route table. This way, the VPC and the data center can communicate with each other. For more information, see VPN Gateway route overview.

6. Test the connectivity

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

Basic scenarios

- Connect a data center to a VPC
- Connect a data center to a VPC and enable BGP dynamic routing

2.Connect a data center to a VPC

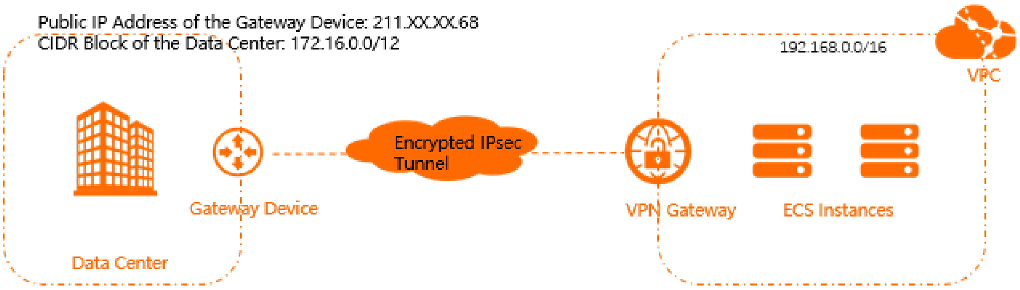
This topic describes how to use IPsec-VPN to connect a data center to a virtual private cloud (VPC). After you establish an IPsec-VPN connection, the data center and the VPC can communicate with each other.

Prerequisites

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, create one.
- The gateway device in the data center support the IKEv1 and IKEv2 protocols. All gateway devices that support these protocols can connect to the VPN gateway.
- A static public IP address is assigned to the gateway device in the data center.
- The CIDR block of the data center does not overlap with the CIDR block of the VPC.
- You have read and understand the security group rules that apply to the ECS instances in VPCs, and the security group rules allow gateway devices in the data center to access cloud resources. For more information, see Query security group rules and Add security group rules.

Context

The following scenario is used as an example in this topic. An enterprise has created a VPC on Alibaba Cloud. The CIDR block of the VPC is 192.168.0.0/16. The CIDR block of the data center is 172.16.0.0/12. The static public IP address for the gateway device in the data center is 211.XX.XX.68. To meet business requirements, the enterprise needs to connect the data center to the VPC. You can establish an IPsec-VPN connection between the data center and the VPC, as shown in the following figure. This way, the data center and VPC can share resources with each other.


Public IP Address of the Gateway Device: 211.XX.XX.68
CIDR Block of the Data Center: 172.16.0.0/12
192.168.0.0/16
VPC
Encrypted IPsec Tunnel
Gateway Device
Data Center
VPN Gateway
ECS Instances

Step 1: Create a VPN gateway

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, click **Buy Now**, and then 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 and the VPN gateway are deployed in the same region.

   - **VPC**:Select the VPC to be associated with the VPN gateway.
   - **Specify vSwitch**: Specify whether to create the VPN gateway in a vSwitch of the VPC. In this

example, **No** is selected.

If you select **Yes**, you must also specify a **vSwitch**.

- **Peak Bandwidth**: Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
- **Traffic**: By default, the VPN gateway uses the pay-by-data-transfer billing method. For more information, see Pay-as-you-go.
- **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway. In this example, **Enable** is selected.
- **SSL-VPN**: Specify whether to enable SSL-VPN. In this example, **Disable** is selected.
- **Duration**: By default, the VPN gateway is billed on an hourly basis. For more billing information, see Pay-as-you-go.

4. Return to the VPN Gateways page to view the VPN gateway.

   The newly created VPN gateway is in the **Preparing** state. The VPN gateway changes to the **Normal** state after about 1 to 5 minutes. After the status changes to **Normal**, the VPN gateway is ready for use.

Step 2: Create a customer gateway

1. In the left-side navigation pane, choose **Interconnections > VPN > Customer Gateways**.
2. In the top navigation bar, select the region where you want to create the customer gateway.

   > Note Make sure that the customer gateway and the VPN gateway to be connected belong to the same region.

3. On the **User Gateway** page, click **Create Customer Gateway**.
4. On the **Create Customer Gateway** page, set the following parameters and click **OK**.
   - **Name**: Enter a name for the customer gateway.
   - **IP Address**: Enter the public IP address of the gateway device in the data center that you want to connect to the VPC. In this example,211.XX.XX.68 is entered.
   - **Description**: Enter a description for the customer gateway.

   For more information about the related parameters, see Create a customer gateway.

Step 3: Create an IPsec-VPN connection

1. In the left-side navigation pane, choose **Interconnections > VPN > IPsec Connections**.
2. In the top navigation bar, select the region where you want to create the IPsec-VPN connection.

   > Note Make sure that the IPsec-VPN connection and the VPN gateway to be connected belong to the same region.

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 **OK**.
   - **Name**: Enter a name for the IPsec-VPN connection.
   - **VPN Gateway**: Select the VPN gateway that you created.
   - **Customer Gateway**: Select the customer gateway that you created.

- **Routing Mode**: Select a routing mode. In this example, **Destination Routing Mode** is selected.
- **Effective Immediately**: Select whether to immediately start connection negotiations. In this example, **No** is selected.
  - **Yes**: immediately starts negotiations after you complete the configuration.
  - **No**: starts negotiations when traffic is detected.
- **Pre-shared Key**: Enter a pre-shared key (PSK). The pre-shared key must be the same as the pre-shared key of the gateway device in the data center.

  If you do not enter a value, the system generates a 16-bit random string by default.

Use the default settings for other parameters. For more information, see Create an IPsec-VPN connection.

Step 4: Load the configuration of the IPsec-VPN connection to the gateway device in the data center

1. In the left-side navigation pane, choose **Interconnections** > **VPN** > **IPsec Connections**.
2. On the **IPsec Connections** page, find the IPsec-VPN connection that you want to manage, and choose ⋮ > **Download Configuration** in the **Actions** column.
3. Load the configuration of the IPsec-VPN connection to the gateway device in the data center. For more information, see Configure on-premises gateway devices. .

Step 5: Configure routes for the VPN gateway

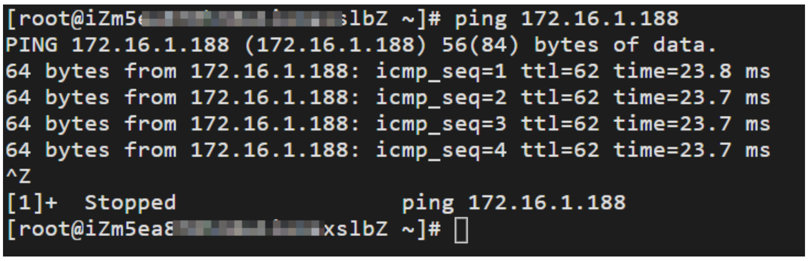
1. In the left-side navigation pane, choose **Interconnections** > **VPN** > **VPN Gateways**.
2. On the **VPN Gateway** page, find the VPN gateway that you want to manage and click its ID.
3. On the **Destination-based Routing** tab, click **Add Route Entry**.
4. In the **Add Route Entry** panel, set the following parameters and click **OK**.
   - **Destination CIDR Block**: Enter the CIDR block of the data center. In this example, **172.16.0.0/12** is entered.
   - **Next Hop Type**: Select **IPsec Connection**.
   - **Next Hop**: Select the IPsec-VPN connection that you created.
   - **Publish to VPC**: Specify whether to automatically advertise new routes to the VPC route table. In this example, **Yes** is selected.
   - **Weight**: Select a weight for the route. In this example, **100** is selected.
     - **100**: specifies a high priority for the route.
     - **0**: specifies a low priority for the route.

   > **Note** If two destination-based routes are configured with the same destination CIDR block, you cannot set the weights of the routes to 100.

Step 6: Test the connectivity

1. Log on to an ECS instance that is not assigned a public address in the VPC. For more information about how to log on to an ECS instance, see Methods used to connect to ECS instances.

2. Run the **ping** command to access a server in the data center and test the connectivity.



```
[root@iZm5[redacted]slbZ ~]# ping 172.16.1.188
PING 172.16.1.188 (172.16.1.188) 56(84) bytes of data.
64 bytes from 172.16.1.188: icmp_seq=1 ttl=62 time=23.8 ms
64 bytes from 172.16.1.188: icmp_seq=2 ttl=62 time=23.7 ms
64 bytes from 172.16.1.188: icmp_seq=3 ttl=62 time=23.7 ms
64 bytes from 172.16.1.188: icmp_seq=4 ttl=62 time=23.7 ms
^Z
[1]+  Stopped                 ping 172.16.1.188
[root@iZm5ea8[redacted]xslbZ ~]#
```

3.Connect a data center to a VPC and enable BGP dynamic routing

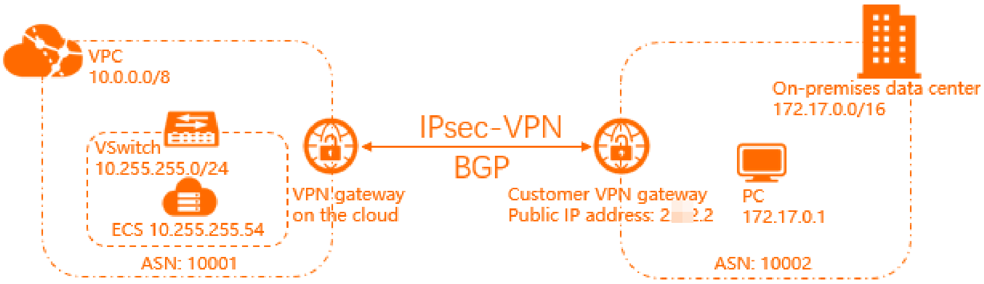
This topic describes how to establish an IPsec-VPN connection between a virtual private cloud (VPC) and a data center, and how to configure Border Gateway Protocol (BGP) dynamic routing for a VPN gateway to automatically learn routes. This way, the VPC and the data center can share resources with each other. This reduces network maintenance costs and network configuration errors.

Scenario

The following scenario is used as an example. An enterprise has created a VPC in the Germany (Frankfurt) region. The private CIDR block of the VPC is 10.0.0.0/8 and the autonomous system number (ASN) is 10001. The company has a data center in Frankfurt. The public IP address of the data center is 2.XX.XX.2, the CIDR block is 172.17.0.0/16, and the ASN is 10002. The enterprise wants to establish a connection between the VPC and the data center for business development.

You can use IPsec-VPN to establish a connection between the VPC and the data center, and configure BGP dynamic routing. After the configuration is completed, the VPC and the data center can automatically learn routes and can communicate with each other. 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 globally unique identifier called ASN.



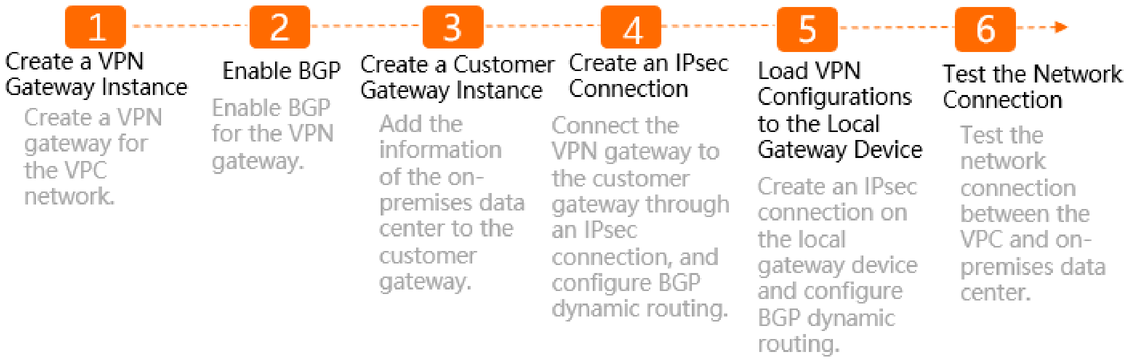
Regions that support BGP dynamic routing

Area	Region
Asia Pacific	China (Hangzhou), China (Shanghai), China (Qingdao), China (Beijing), China (Zhangjiakou), China (Hohhot), China (Shenzhen), China (Hong Kong), Singapore (Singapore), Japan (Tokyo), Malaysia (Kuala Lumpur), Indonesia (Jakarta), and Australia (Sydney)
Europe & Americas	US (Virginia), US (Silicon Valley), Germany (Frankfurt), and UK (London)
Middle East & India	India (Mumbai) and UAE (Dubai)

Prerequisites

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, create one.
- A VPC is created in the Germany (Frankfurt) region and cloud services are deployed in the VPC. For more information, see Create an IPv4 VPC.
- The gateway device in the data center supports the Internet Key Exchange Version 1 (IKEv1) and IKEv2 protocols. All gateway devices that support these protocols can connect to the VPN gateway.
- A static public IP address is assigned to the gateway device in the data center.
- The CIDR block of the data center does not overlap with the CIDR block of the VPC.
- You have read and understand the security group rules that apply to the ECS instances in VPCs, and the security group rules allow gateway devices in the data center to access cloud resources. For more information, see Query security group rules and Add security group rules.

Procedure


1
Create a VPN Gateway Instance
Create a VPN gateway for the VPC network.
2
Enable BGP
Enable BGP for the VPN gateway.
3
Create a Customer Gateway Instance
Add the information of the on-premises data center to the customer gateway.
4
Create an IPsec Connection
Connect the VPN gateway to the customer gateway through an IPsec connection, and configure BGP dynamic routing.
5
Load VPN Configurations to the Local Gateway Device
Create an IPsec connection on the local gateway device and configure BGP dynamic routing.
6
Test the Network Connection
Test the network connection between the VPC and on-premises data center.

Step 1: Create a VPN gateway

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, click **Buy Now**, and then complete the payment.
   - **Name**: Enter a name for the VPN gateway. In this example, VPN is used.
   - **Region**:Select the region where you want to deploy the VPN gateway.

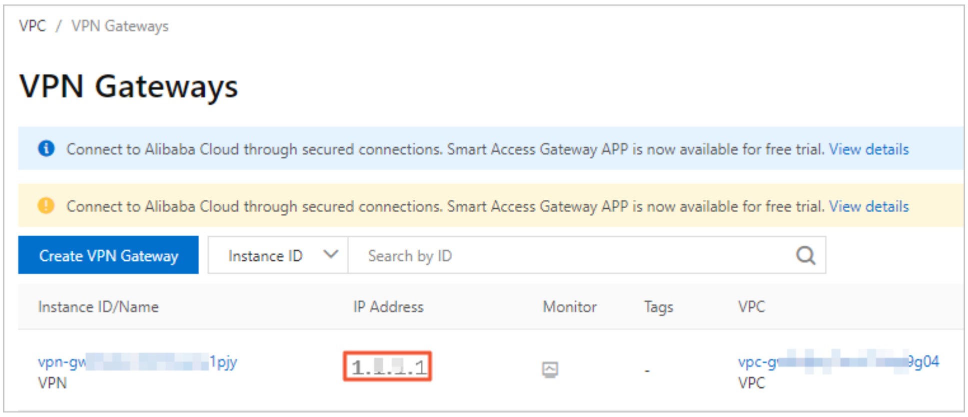
     Make sure that the VPN gateway and the VPC are deployed in the same region. In this example, **Germany (Frankfurt)** is selected.
   - **VPC**:Select the VPC to be associated with the VPN gateway. In this example, the VPC that is created in Germany (Frankfurt) is selected.
   - **Specify vSwitch**: Select whether to specify a vSwitch for the VPN gateway. In this example, **No** is selected.

     If you select **Yes**, you must also specify a **vSwitch**.
   - **Peak Bandwidth**: Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.

     The bandwidth is used for data transfer over the Internet. In this example,**5 M** is selected.
   - **Traffic**: By default, the VPN gateway uses the pay-by-data-transfer metering method. For more information, see Pay-as-you-go.
   - **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway. In this example, **Enable** is elected.
   - **SSL-VPN**: Specify whether to enable SSL-VPN. In this example, **Disable** is selected.

- **Duration**: By default, the VPN gateway is billed on an hourly basis. For more information about billing, see Pay-as-you-go.

The newly created VPN gateway is in the **Preparing** state and changes to the **Normal** state after about 1 to 5 minutes. After the VPN gateway changes to the **Normal** state, the VPN gateway is ready for use. After the VPN gateway is created, a public IP address is automatically assigned to the gateway for establishing VPN connections.



VPC / VPN Gateways

VPN Gateways

Connect to Alibaba Cloud through secured connections. Smart Access Gateway APP is now available for free trial. View details

Connect to Alibaba Cloud through secured connections. Smart Access Gateway APP is now available for free trial. View details

Instance ID/Name	IP Address	Monitor	Tags	VPC
vpn-gw[redacted]1pjy VPN	1.[redacted].1		-	vpc-g[redacted]9g04 VPC

Note If you want to use an existing VPN gateway, make sure that it is updated to the latest version. If the existing VPN gateway does not use the latest version, you cannot use BGP dynamic routing by default.

You can check whether your VPN gateway uses the latest version based on the status of the **Upgrade** button. If your VPN gateway does not use the latest version, you can click **upgrade** to update your VPN gateway. For more information, see Update a VPN gateway.

Step 2: Enable BGP dynamic routing

BGP is used to exchange routing information in different ASs. To use BGP dynamic routing, you must enable it for the VPN gateway.

Note You cannot disable BGP dynamic routing after you enable it.

1. In the left-side navigation pane, choose **Interconnections > VPN > VPN Gateways**.
2. In the top navigation bar, select the region of the VPN gateway.
3. On the **VPN Gateways** page, find the VPN gateway that you created and select ⋮ > **Enable Automatic BGP Propagation** in the **Actions** column.
4. In the **Enable Automatic BGP Propagation** dialog box, click **OK**.

   After you enable automatic BGP advertising, the VPN gateway automatically advertises BGP routes to the VPC.

Step 3: Create a customer gateway

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

1. In the left-side navigation pane, choose **Interconnections > VPN > Customer Gateways**.
2. In the top navigation bar, select the region where you want to create the customer gateway.

> ? **Note** Make sure that the customer gateway and the VPN gateway to be connected are deployed in the same region.

3. On the **User Gateway** page, click **Create Customer Gateway**.
4. On the **Create Customer Gateway** page, set the following parameters and click **OK**.
   - **Name**: Enter a name for the customer gateway. In this example, CGW is entered.
   - **IP Address**: Enter the public IP address of the gateway device in the data center. In this example, 2.XX.XX.2 is used.
   - **ASN**: Enter the ASN of the data center. In this example, 10002 is entered.
   - **Description**: Enter a description for the customer gateway.

   For more information about the parameters, see Create a customer gateway.

Step 4: Create an IPsec-VPN connection

1. In the left-side navigation pane, choose **Interconnections > VPN > IPsec Connections**.
2. In the top navigation bar, select the region where you want to create the IPsec-VPN connection.

   > ? **Note** Make sure that the IPsec-VPN connection and the VPN gateway to be connected are deployed in the same region.

3. On the **IPsec Connections** page, click **Create IPsec Connection**.
4. On the **Create IPsec Connection** page that appears, set the following parameters to create an IPsec-VPN connection between the VPC and the data center, and click **OK**.
   - **Name**: Enter a name for the IPsec-VPN connection. In this example, VPC TO IDC is entered.
   - **VPN Gateway**: Select the VPN gateway to be connected.

     In this example, the VPN gateway that is created in Step 1 is selected.
   - **Customer Gateway**: Select the customer gateway to be connected.

     In this example, the customer gateway that is created in Step 3 is selected.
   - **Routing Mode**: Select a routing mode. In this example, **Destination Routing Mode** is selected.
   - **Effective Immediately**: Select whether to immediately start negotiations.
     - **Yes**: starts negotiations immediately after you complete the configuration.
     - **No**: starts negotiations when data transfer is detected.

     Yes is selected in this example.
   - **Pre-shared Key**: Enter a pre-shared key (PSK).

     Make sure that the VPC and the data center use the same PSK. In this example, 123456 is used.
   - **Version**: Select an IKE version. In this example, **ikev2** is selected.
   - **Encryption Algorithm**: Select an encryption algorithm. In this example, **aes** is selected.
   - **Authentication Algorithm**: Select an authentication algorithm. In this example, **sha1** is selected.
   - **DH Group**: Select a Diffie-Hellman (DH) group. In this example, **group2** is selected.
   - **Tunnel CIDR Block**: Enter the CIDR block of the IPsec tunnel. The CIDR block belongs to

169.254.0.0/16. The subnet mask of the CIDR block is 30 bits in length. In this example, 169.254.10.0/30 is entered.

- **Local BGP IP Address**: Enter the BGP IP address of the VPC. This IP address falls within the CIDR block of the IPsec tunnel. In this example, 169.254.10.1 is entered.

> **Note** Make sure that the BGP IP addresses of the VPC and the data center do not conflict with each other.

- **Local ASN**: Enter the ASN of the VPC. In this example, 10001 is entered.

Use the default settings for other parameters. For more information, see Create an IPsec-VPN connection.

Step 5: Load the configuration of the VPN gateway to the gateway device in the data center

To establish a connection between the VPC and the data center, you must load the configuration of the VPN gateway to the gateway device in the data center after you create the IPsec-VPN connection in the cloud.

The following example shows how to load the configuration of the VPN gateway to the gateway device in the data center. A Cisco firewall device that runs the Cisco IOS XE system is used in the example.

1. Log on to the command-line interface (CLI) 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. In this example, aes-cbc-128 is used.
integrity sha1                  //Set the authentication algorithm. In this example, sha1 is used.
group 2                         //Set the DH group. In this example, group 2 is used.
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.XX.XX.1                //Set the public IP address of the VPN gateway on the VPC side. In this example, 1.XX.XX.1 is used.
pre-shared-key 123456          //Set the PSK. In this example, 123456 is used.
exit
!
```

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

```
crypto ikev2 profile alicloud
match identity remote address 1.XX.XX.1 255.255.255.255    //Match the public IP address of the VPN gateway on the VPC side. The matched IP address is 1.XX.XX.1 in this example.
identity local address 2.XX.XX.2    //Set the public IP address of the data center. In this example, 2.XX.XX.2 is used.
authentication remote pre-share   //Set the authentication mode for the VPC to PSK.
authentication local pre-share    //Set the authentication mode for the data center to PSK.
keyring local alicloud            //Invoke the IKEv2 keyring.
exit
!
```

5. Run the following commands to set 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 profiles:

```
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:

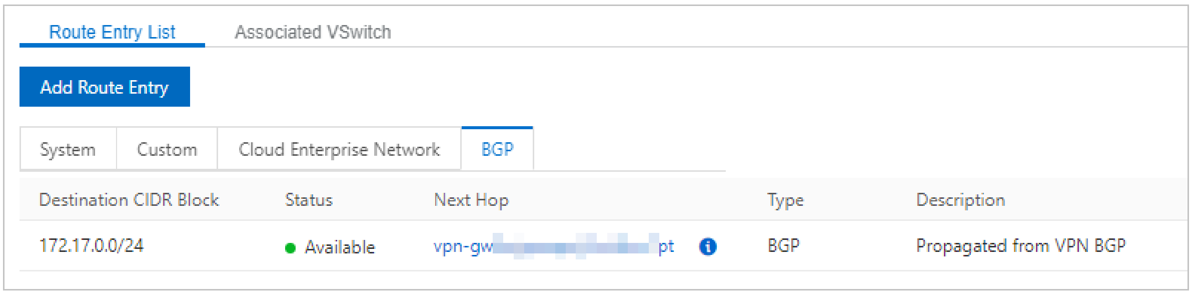
```
interface Tunnel100
ip address 169.254.10.2 255.255.255.252    //Set the tunnel address for the data center. In this example, 169.254.10.2 is used.
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 1.XX.XX.1                 //The public IP address of the VPN gateway on the Alibaba Cloud side. In this example, 1.XX.XX.1 is used.
tunnel protection ipsec profile alicloud
no shutdown
exit
!
interface GigabitEthernet1
ip address 2.XX.XX.2 255.255.255.0
negotiation auto
!
```

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

```
router bgp 10002                         //Enable BGP routing and set an ASN for the da
ta center. In this example, 10002 is used.
bgp router-id 169.254.10.2               //Set the BGP router ID. In this example, 169.
254.10.2 is used.
bgp log-neighbor-changes
neighbor 169.254.10.1 remote-as 10001    //Set an ASN for the BGP neighbor.
neighbor 169.254.10.1 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 data center.
In this example, the CIDR block is 172.17.0.0/16.
neighbor 169.254.10.1 activate           //Activate the BGP neighbor.
exit-address-family
!
```

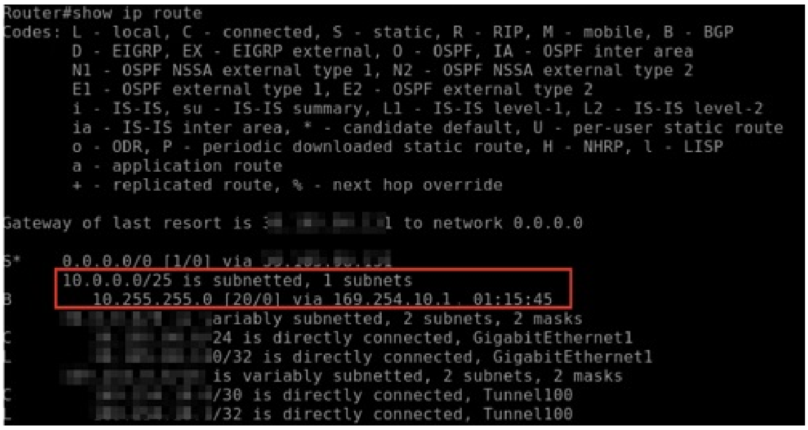
After you establish the IPsec-VPN connection, the VPN gateway of the VPC and the gateway device in the data center advertise the following routes:

- The gateway device in the data center automatically learns routes from the CIDR block of the data center through BGP, and then advertises the routes to the VPN gateway of the VPC. The VPN gateway of the VPC automatically advertises the learned routes to the VPC route table.



Destination CIDR Block	Status	Next Hop	Type	Description
172.17.0.0/24	● Available	vpn-gw[redacted]pt	BGP	Propagated from VPN BGP

- The VPN gateway of the VPC automatically learns routes from the route table of the VPC through BGP, and then advertises the routes to the gateway device in the data center.

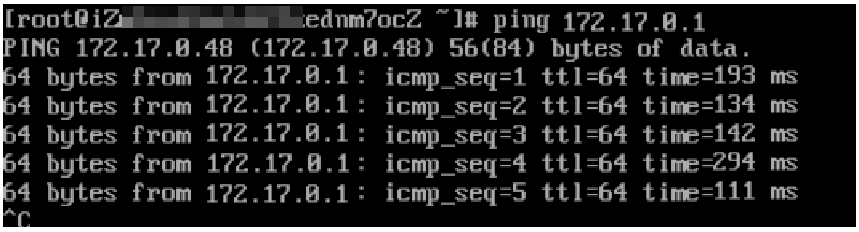


```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is [redacted] to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via [redacted]
      10.0.0.0/25 is subnetted, 1 subnets
B        10.255.255.0 [20/0] via 169.254.10.1, 01:15:45
      [redacted]ariably subnetted, 2 subnets, 2 masks
C        [redacted]24 is directly connected, GigabitEthernet1
L        [redacted]0/32 is directly connected, GigabitEthernet1
      [redacted] is variably subnetted, 2 subnets, 2 masks
C        [redacted]/30 is directly connected, Tunnel100
L        [redacted]/32 is directly connected, Tunnel100
```

Step 6: Test the connectivity

1. Log on to an Elastic Compute Service (ECS) instance that is not assigned a public address in the VPC. For more information about how to log on to an ECS instance, see Methods used to connect to ECS instances.
2. Run the `ping` command to access a client in the local data center and test the connectivity.

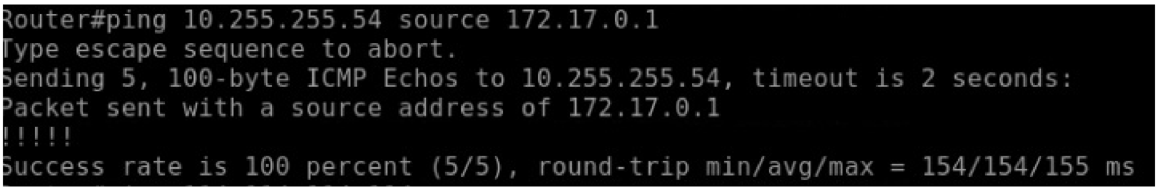
   The result shows that the ECS instance in the VPC can access the client in the data center.



```
[root@iZ[redacted]ednm7ocZ ~]# ping 172.17.0.1
PING 172.17.0.48 (172.17.0.48) 56(84) bytes of data.
64 bytes from 172.17.0.1: icmp_seq=1 ttl=64 time=193 ms
64 bytes from 172.17.0.1: icmp_seq=2 ttl=64 time=134 ms
64 bytes from 172.17.0.1: icmp_seq=3 ttl=64 time=142 ms
64 bytes from 172.17.0.1: icmp_seq=4 ttl=64 time=294 ms
64 bytes from 172.17.0.1: icmp_seq=5 ttl=64 time=111 ms
^C
```

3. Log on to the client in the data center.
4. Run the `ping` command to access an ECS instance in the VPC and test the connectivity.

   The result shows that the client in the data center can access the ECS instance in the VPC.



```
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
```

4.Connect an iOS device to a VPN gateway by using the built-in VPN software

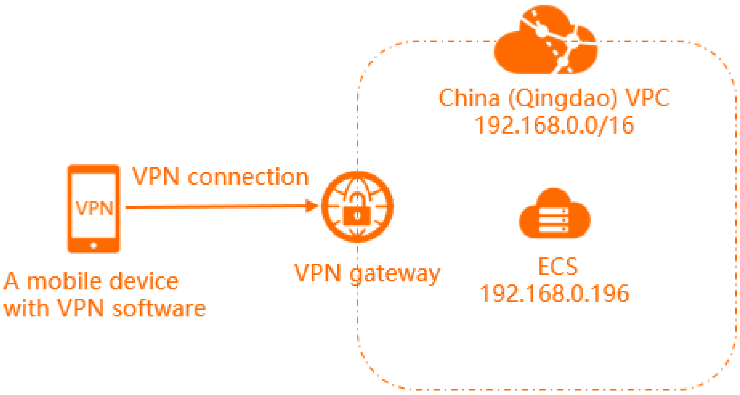
This topic describes how to connect an iOS device to a VPN gateway by using the built-in VPN software of the iOS device. This allows mobile clients to access resources in a virtual private cloud (VPC) that is associated with the VPN gateway.

Prerequisites

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, create one.
- Your mobile client runs the iOS operating system.
- A VPC is created in a region that supports IPsec-VPN servers. For more information, see Create an IPv4 VPC.

> Note
>
> - IPsec-VPN servers are supported only in the following regions: China (Hangzhou), China (Shanghai), China (Qingdao), China (Beijing), China (Zhangjiakou), China (Ulanqab), China (Shenzhen), China (Hong Kong), Singapore (Singapore), Japan (Tokyo), Malaysia (Kuala Lumpur), Indonesia (Jakarta), Australia (Sydney), US (Virginia), US (Silicon Valley), Germany (Frankfurt), UK (London), India (Mumbai), and UAE (Dubai).
> - Only iOS devices can connect to a VPN gateway by using the built-in VPN software.

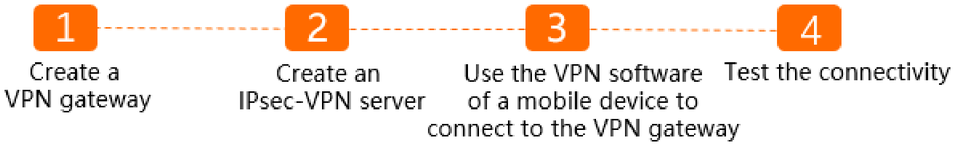
Scenario



A company has created Elastic Compute Service (ECS) instances in the China (Qingdao) region and deployed enterprise applications on the ECS instances. Due to business growth, employees on business trips need to remotely access the enterprise applications deployed on Alibaba Cloud from iOS devices.

You can create a VPN gateway and then create an IPsec-VPN server on the gateway. This way, the employees can use the built-in VPN software of their iOS devices to connect to the VPN gateway. After a mobile client is connected to the VPN gateway, employees can remotely access the enterprise applications deployed on Alibaba Cloud.

Procedure


1
Create a VPN gateway
2
Create an IPsec-VPN server
3
Use the VPN software of a mobile device to connect to the VPN gateway
4
Test the connectivity

Step 1: Create a VPN gateway

1. Log on to the VPN Gateway console.
2. In the top navigation bar, select the region of the VPC to be associated with the VPN gateway. **China (Qingdao)** is selected in this example.
3. On the **VPN Gateways** page, click **Create VPN Gateway**.
4. On the buy page, set the following parameters, click **Buy Now**, and then complete the payment:
   - **Name**: Enter a name for the VPN gateway.

     The name must be 2 to 128 characters in length, and can contain digits, hyphens (-), and underscores (_). It must start with a letter.
   - **Region**: Select the region where you want to deploy the VPN gateway.

     China (Qingdao) is selected in this example.
   - **VPC**: Select the VPC to be associated with the VPN gateway.
   - **Specify VSwitch**: Select whether to specify a vSwitch for the VPN gateway.
     - If you select **No**, you do not need to specify a vSwitch for the VPN gateway. The system connects the VPN gateway to a random vSwitch in the VPC.
     - If you select **Yes**, you must specify a vSwitch for the VPN gateway. The system connects the VPN gateway to the specified vSwitch.
   - **Peak Bandwidth**: Specify the maximum bandwidth for the VPN gateway. The bandwidth is used for data transfer over the Internet.

     In this example, **10 M** is selected.
   - **Traffic**: By default, the VPN gateway uses the pay-by-data-transfer metering method. For more information, see Pay-as-you-go.
   - **IPsec-VPN**: Enable or disable the IPsec-VPN feature. After you enable this feature, you can establish connections between data centers and VPCs.

     Disable is selected in this example.
   - **SSL-VPN**: Enable or disable the SSL-VPN feature. The SSL-VPN feature allows you to connect to a VPC from a device anywhere.

     The SSL-VPN feature must be enabled before you can use the built-in VPN software of a mobile device to establish a connection with the VPN gateway. **Enabled** is selected in this example.
   - **SSL connections**: Select the maximum number of clients that can be connected to the VPN gateway at the same time.

     5 is selected in this example.

> **Note** The number of SSL connections specified in this parameter includes both SSL-VPN and IPsec-VPN connections. For example, if you set the maximum number of SSL connections to 5 and three SSL clients are connected through SSL-VPN connections, it indicates that you can connect only two mobile clients to the IPsec-VPN server.

- **Duration**: By default, the VPN gateway is billed on an hourly basis.

5. Return to the VPN Gateways page to view the VPN gateway.

   The newly created VPN gateway is in the **Preparing** state. The VPN gateway enters the **Normal** state after about 2 minutes. The Normal state indicates that the VPN gateway is initialized and ready for use. The system assigns a public IP address to the VPN gateway. The IP address is used to establish connections between mobile clients and the VPN gateway.

   > **Note** If you want to use an existing VPN gateway instead of a new VPN gateway, make sure that the VPN gateway is updated to the latest version. If the existing VPN gateway does not use the latest version, you cannot use the IPsec-VPN server.
   >
   > You can check whether your VPN gateway uses the latest version based on the status of the **Upgrade** button. If your VPN gateway does not use the latest version, you can click **upgrade** to update your VPN gateway. For more information, see Update a VPN gateway.

Step 2: Create an IPsec-VPN server

1. Log on to the VPN Gateway console.
2. In the left-side navigation pane, choose **Interconnections > VPN > IPsec-VPN Server**.
3. In the top navigation bar, select the region of the IPsec-VPN server.
4. On the **IPsec-VPN Server** page, click **Create IPsec-VPN Server**.
5. On the **Create IPsec-VPN Server** page, set the required parameters.

   - **Name**: Enter a name for the IPsec-VPN server.

     The name must be 2 to 128 characters in length, and can contain digits, hyphens (-), and underscores (_). It must start with a letter.

   - **VPN Gateway**: Select the VPN gateway to which you want to connect by using the built-in VPN software of your mobile device.

     The VPN gateway created in Step 1 is selected in this example.

   - **Local Network**: Enter the CIDR block of the VPC to be accessed by the mobile device.

     192.168.0.0/16 is used in this example.

   - **Client Subnet**: Enter the private CIDR block of the mobile client in the IPsec-VPN connection.

     The client subnet is not the private CIDR block of the mobile client but the private CIDR block assigned to the virtual network adapter of the mobile client. When the mobile client accesses the VPC, the VPN gateway assigns an IP address from the specified client subnet to the client.

     > **Note** The CIDR block of the client must not overlap with that of the vSwitch in the VPC.

     10.0.0.0/16 is used in this example.

- **Pre-Shared Key**: The pre-shared key is used for identity verification between the IPsec-VPN server and the mobile client. An IPsec-VPN connection can be established only when both ends have the same key. You can specify a key or use the default key that is randomly generated by the system.

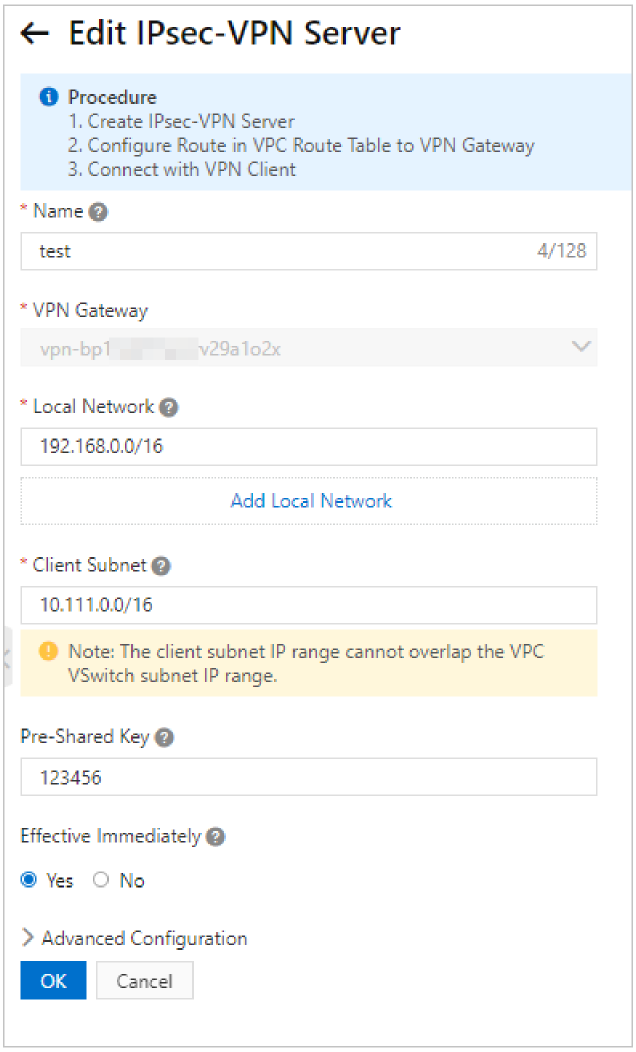
  123456 is used in this example.

- **Effective Immediately**: Select whether to immediately start connection negotiations.

  - **Yes**: starts negotiations immediately after you complete the configuration.
  - **No**: starts negotiations when data transfer is detected.

  In this example, **Yes** is selected.

- **Advanced Configuration**: The default settings are used in this example.



← Edit IPsec-VPN Server

Procedure
1. Create IPsec-VPN Server
2. Configure Route in VPC Route Table to VPN Gateway
3. Connect with VPN Client

* Name

test 4/128

* VPN Gateway

vpn-bp1[redacted]v29a1o2x

* Local Network

192.168.0.0/16

Add Local Network

* Client Subnet

10.111.0.0/16

Note: The client subnet IP range cannot overlap the VPC VSwitch subnet IP range.

Pre-Shared Key

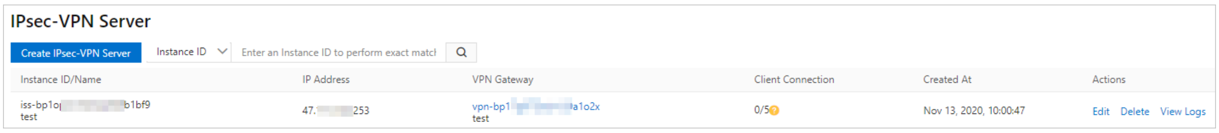
123456

Effective Immediately

● Yes ○ No

6. Click **OK**.

After the IPsec-VPN server is created, you can go to the **IPsec-VPN Server** page to view the created IPsec-VPN server.



IPsec-VPN Server

Instance ID/Name	IP Address	VPN Gateway	Client Connection	Created At	Actions
iss-bp1o[redacted]b1bf9 test	47.[redacted]253	vpn-bp1[redacted]a1o2x test	0/5	Nov 13, 2020, 10:00:47	Edit Delete View Logs

Step 3: Connect to the VPN gateway by using the built-in VPN software of a mobile device

The following operations describe how to connect an iOS device to a NAT gateway by using the built-in VPN software. In this example, the device runs in iOS 14.

1. Go to **Settings**.
2. Choose **General > VPN > Add VPN Configuration**.
3. On the **Add Configurations** page, set the following parameters:
   - **Type**: Select a VPN type.

     IKEv2 is selected in this example.
   - **Description**: Enter a description for the VPN.
   - **Server**: Enter the public IP address of the VPN gateway to which you want to connect the mobile client.

     In this example, the public IP address of the VPN gateway in Step 1 is entered.
   - **Remote ID**: Enter the public IP address of the VPN gateway to which you want to connect the mobile client.

     In this example, the public IP address of the VPN gateway in Step 1 is entered.
   - **Local ID**: This parameter is not set in this example.
   - **User Authentication**: Select a user authentication type.

     None is selected in this example.
   - **Use Certificate**: The parameter is disabled in this example.
   - **Secret**: The secret is used for identity verification between the IPsec-VPN server and the mobile client. An IPsec-VPN connection can be established only when both ends use the same secret.

     123456 is used in this example.
4. Click **Complete**.
5. On the **VPN** page, select the VPN configuration and turn on **Status**.

The IPsec-VPN connection is established after the status changes to **Connected**.

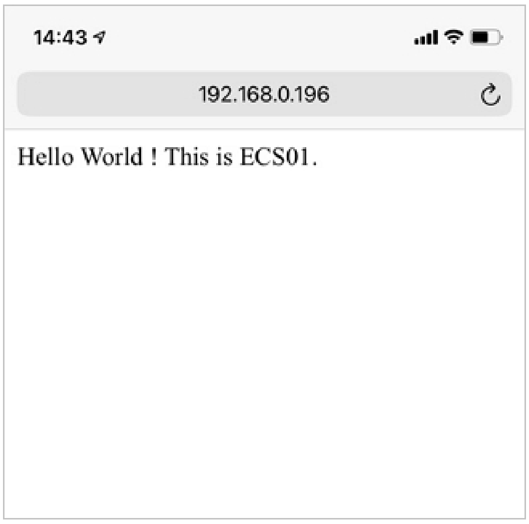
Step 4: Test network connectivity

Complete the following steps to test the connectivity between the mobile device and the VPC.

1. Open a browser on the mobile device.
2. Enter the private IP address of an ECS instance into the address bar of the browser.

   192.168.0.196 is used in this example.

The result shows that the mobile client can access resources deployed in the VPC.



Hello World ! This is ECS01.