

# Alibaba Cloud vpn gateway

## Best Practices

Issue: 20190417

## 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Notice:</b> 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.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<b><code>{}</code> or <code>{a b}</code></b>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 Use IPsec-VPN in the classic network.....	1
2 High availability architecture using IPsec-VPN connections.....	3
2.1 Dual IPsec-VPN tunnel configuration.....	3
2.2 Dual customer gateway configuration.....	13
3 Establish a global network through VPN Gateway and CEN...23	
4 Implement an active/standby configuration by using VPN Gateway and Express Connect.....	27




# 1 Use IPsec-VPN in the classic network

In the VPC network, you can create a site-to-site connection directly by using the IPsec-VPN function of VPN Gateway. However, to use VPN Gateway in the classic network, you must first configure the ClassicLink.

## Prerequisites

Before you begin, plan your network:

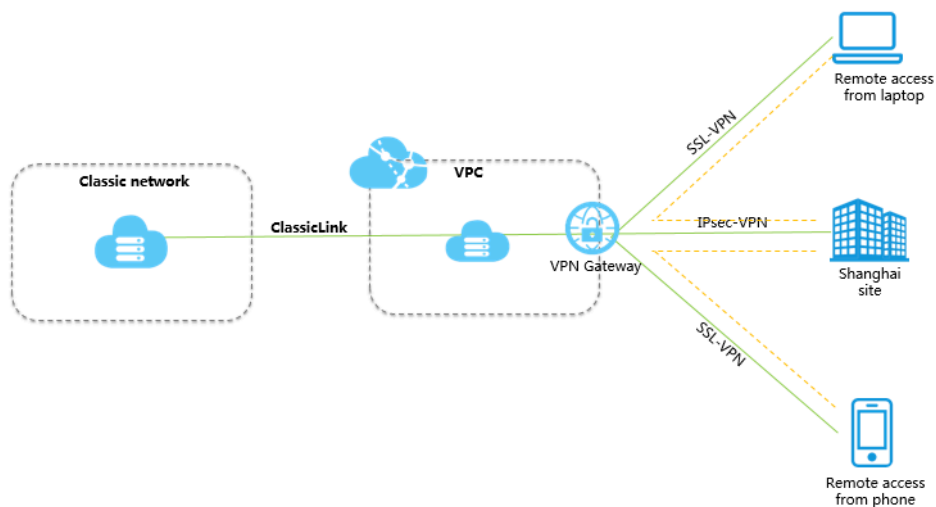
- The IP address range of the local client or office must belong to the IP address range of the VPC, but cannot conflict with the IP address ranges of VSwitches in the VPC.
- Plan the VPC for which a VPN gateway is created. If the ECS instances in the classic network do not need to communicate with ECS instances in the existing VPC, we recommend creating a new VPC.
- You have created a VPC. The VPC must use the following IP address range or its subnet, and meet the corresponding requirements:

VPC CIDR Block	Limitations
172.16.0.0/12	There is no route entry destined for 10.0.0.0/8 in this VPC.
192.168.0.0/16	<ul style="list-style-type: none"><li>- There is no route entry destined for 10.0.0.0/8 in this VPC.</li><li>- A route, of which the destination CIDR block is 192.168.0.0/16 and the next hop is the private NIC, is added to the ECS instance of the classic network. You can use the provided script to add the route. Click <a href="#">Here</a> to download the route script.</li></ul> <div> <b>Note:</b> Before running the script, read the readme file in the script carefully.</div>

## Context

If you want to use VPN Gateway in the classic network, purchase a VPN Gateway for the VPC, and configure the IPsec-VPN function. After the configuration, the local data center or office site can access the VPC. Then, connect the VPC and the ECS instances

in the classic network using the ClassicLink function. Once the private connection is established, the local office site can access the ECS instances in the classic network.



## Procedure

1. Create an IPsec-VPN connection.

For more information, see [Create a site-to-site connection through IPsec-VPN](#).

2. Create an SSL-VPN connection.

For more information, see [Linux client remote access](#).

3. Create a ClassicLink connection.

For more information, see [Build a ClassicLink connection](#).

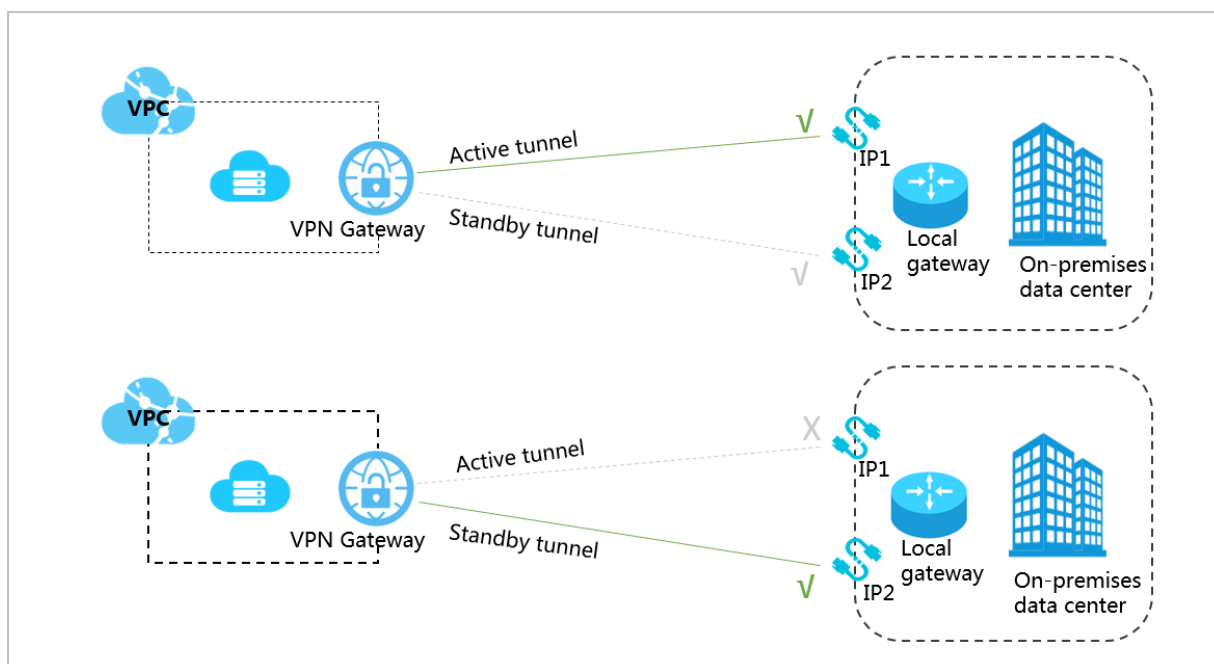
## 2 High availability architecture using IPsec-VPN connections

### 2.1 Dual IPsec-VPN tunnel configuration

This topic describes how to establish two IPsec-VPN tunnels with a VPN Gateway to implement active and standby tunnels. This configuration is suitable for when your local gateway has two public IP addresses.

#### Overview

You can connect a VPN Gateway with two public IP addresses (in this example, they are labeled as IP1 and IP2) to establish two IPsec-VPN connections, and enable health checks. Afterwards, you can set the weights of the corresponding two routes to set one route as the active route and the other route as the standby route. In this way, when the IP1-based Internet link is normal, all traffic between the on-premises data center and the VPC is forwarded only through this connection because it is the active tunnel. When the IP1-based Internet link is abnormal, all traffic between the on-premises data center and the VPC is directed to the standby tunnel.



## Prerequisites

- The protocols IKEv1 and IKEv2 are supported by the gateway device located at the on-premises data center, and a static IP address is configured for the gateway device.
- The IP address ranges used by the VPC and the on-premises data center do not conflict with each other.

## Step 1: Create a VPN Gateway

To create a VPN Gateway, follow these steps:

1. Log on to the [VPC console](#).
2. In the left-side navigation pane, choose VPN > VPN Gateways.
3. Click Create VPN Gateway.
4. On the purchase page, configure the VPN Gateway and complete the payment. In this example, use the following configurations:

- **Region:** Select the region of the VPN Gateway. In this example, select China (Hangzhou).



### Note:

In an actual scenario, make sure that the VPC and the VPN Gateway are in the same region.

- **Name:** Enter a name for the VPN Gateway to be created.
- **VPC:** Select the VPC to be connected.
- **Peak Bandwidth:** Select a peak bandwidth. The bandwidth is the Internet bandwidth of the VPN Gateway.
- **IPsec-VPN:** Choose whether to enable the IPsec-VPN feature. In this example, select Enable.
- **SSL-VPN:** Choose whether to enable the SSL-VPN feature.
- **SSL connections:** Select the maximum number of clients you want to connect to simultaneously.



### Note:

**You can only configure this option after you enable the SSL-VPN feature.**

- **Billing Cycle:** The billing cycle is set to By Hour by default.

VPN Gateway

Region

China (Qingdao)	China (Beijing)	China (Zhangjiakou)	<b>China (Hangzhou)</b>	China (Shanghai)	China (Shenzhen)
Hong Kong	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
UAE (Dubai)	Germany (Frankfurt)	China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
UK(London)					

Basic

Name

TEST123

VPC

emr\_test\_vpc

Peak Bandwidth

10 Mbps

100 Mbps

200 Mbps

Billing Method

Pay By Traffic

Function Config

IPsec-VPN

Enable

Disable

SSL-VPN

Disable

**Enable**

For VPN Gateway instances purchased before Jan 20, 2018, a ticket needs to be submitted to enable SSL-VPN function.

SSL connections

5

10

20

50

100

500

1000

Please choose your SSL Connections based on the maximum number of VPN clients connected at the same time

Purchase Plan

Billing Cycle

By Hour

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

The initial status of a VPN Gateway is Preparing, which indicates the initialization of the VPN Gateway and may take up to two minutes to be completed. When the status of the VPN Gateway changes to Normal, it indicates that the VPN Gateway is ready to use.



**Note:**

---

**It usually takes 1 to 5 minutes to create a VPN Gateway.**

### **Step 2: Create two customer gateways**

Create two customer gateways and register the two public IP addresses of the local gateway to the customer gateways. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > Customer Gateways.
2. Select the China (Hangzhou) region.
3. Click Create Customer Gateway.
4. Configure the customer gateway according to the following information:
  - **Name:** Enter a name for the customer gateway to be created.
  - **IP Address:** Enter one of the two public IP addresses of the gateway device at the on-premises data center.
  - **Description:** Enter a description of the customer gateway.

5. On the Create Customer Gateway page, click + Add to add another customer gateway.

Create Customer Gateway

• Name ?

local 5/128 ✓

• IP Address ?

Description

+ Add Delete

OK Cancel

Contact Us

### Step 3: Create two IPsec-VPN connections

Create two IPsec-VPN connections to connect the VPN Gateway with the two customer gateways. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select the China (Hangzhou) region.
3. Click Create IPsec Connection.

4. Configure the IPsec-VPN connection according to the following information and then click OK:

- **Name:** Enter a name for the IPsec-VPN connection to be created.
- **VPN Gateway:** Select the created VPN Gateway.
- **Customer Gateway:** Select one of the two created customer gateways.
- **Local Network:** Enter the IP address range of the VPC to be connected with the on-premises data center. In this example, enter 192.168.0.0/16. To add multiple local networks, click + Add Local Network.



**Note:**

Only IKE v2 supports multiple local networks.

- **Remote Network:** Enter the CIDR block of the on-premises data center to be connected with the VPC. In this example, enter 172.16.0.0/12. To add multiple remote networks, click + Add Remote Network.



**Note:**



**Only IKE v2 supports multiple remote networks.**

- **Effective Immediately:** Choose whether to delete the negotiated IPsec-VPN tunnel and re-initiate the negotiation.
  - **Yes:** Re-initiates the negotiation immediately after the IPsec-VPN connection is created.
  - **No:** Re-initiates the negotiation when traffic is detected in the tunnel.
- **Synchronize to VPN Route Table:** Choose whether to synchronize IPsec-VPN traffic routes to the VPN route table. We recommend that you select Yes.
  - **Yes:** The IPsec-VPN traffic routes are synchronized to the VPN route table after the IPsec-VPN connection is created.
  - **No:** The IPsec-VPN traffic routes are not synchronized to the VPN route table after the IPsec-VPN connection is created. You need to add gateway routes on the VPN Gateway page. For more information, see [VPN Gateway route overview](#).
- **Pre-Shared Key:** Enter the pre-shared key. This value must be the same as that configured in the local gateway.
- **Health Check:** Enable the health check feature and enter the destination IP address, source IP address, retry interval, and retry times.

Use the default configurations for other parameters.

Create IPsec Connection?×

●

Name?

0/128

●

VPN Gateway

Please select

▼

●

Customer Gateway

Please select

▼

●

Local Network?

0.0.0.0/0

+

Add Local Network

●

Remote Network?

0.0.0.0/0

+

Add Remote Network

Effective Immediately?

☐ Yes

☒ No

OK

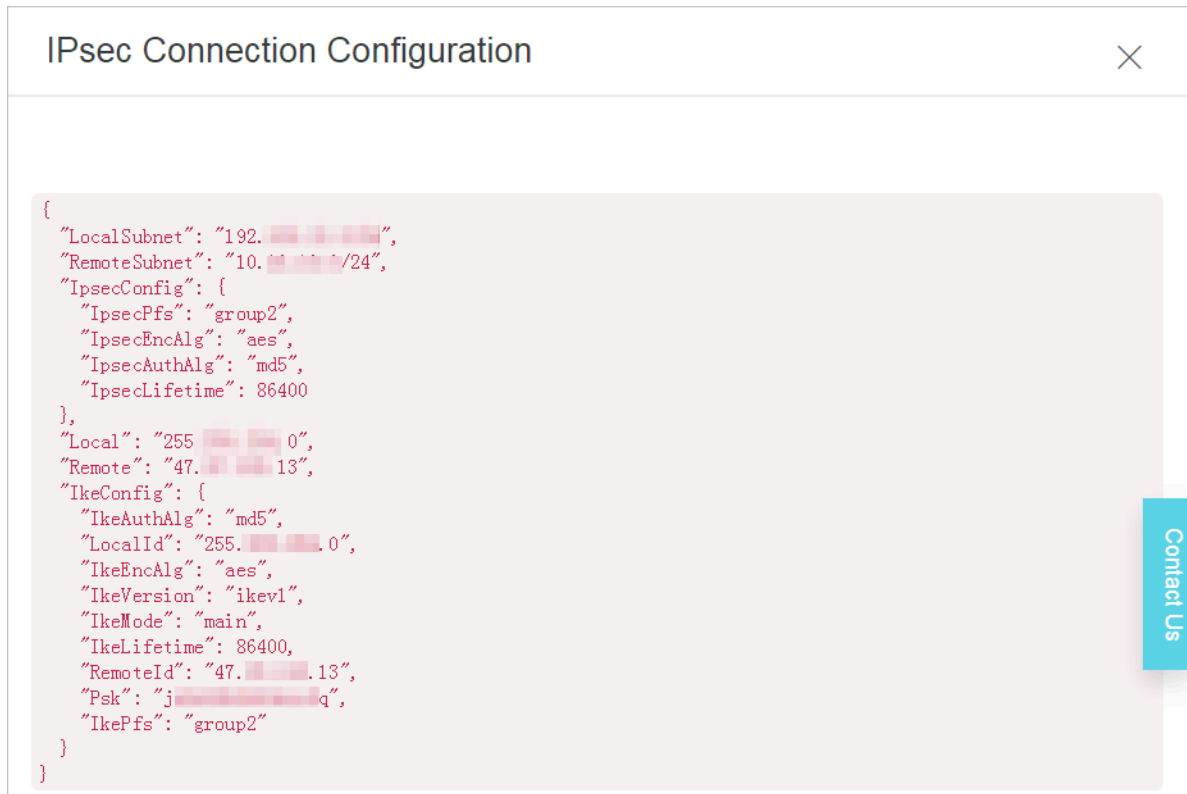
Cancel

Contact Us

5. In the displayed dialog box, click OK.



local gateway, LocalSubnet is the CIDR block of the on-premises data center and RemoteSubnet is the CIDR block of the VPC.



#### Step 5: Set route weights

To set route weights, follow these steps:

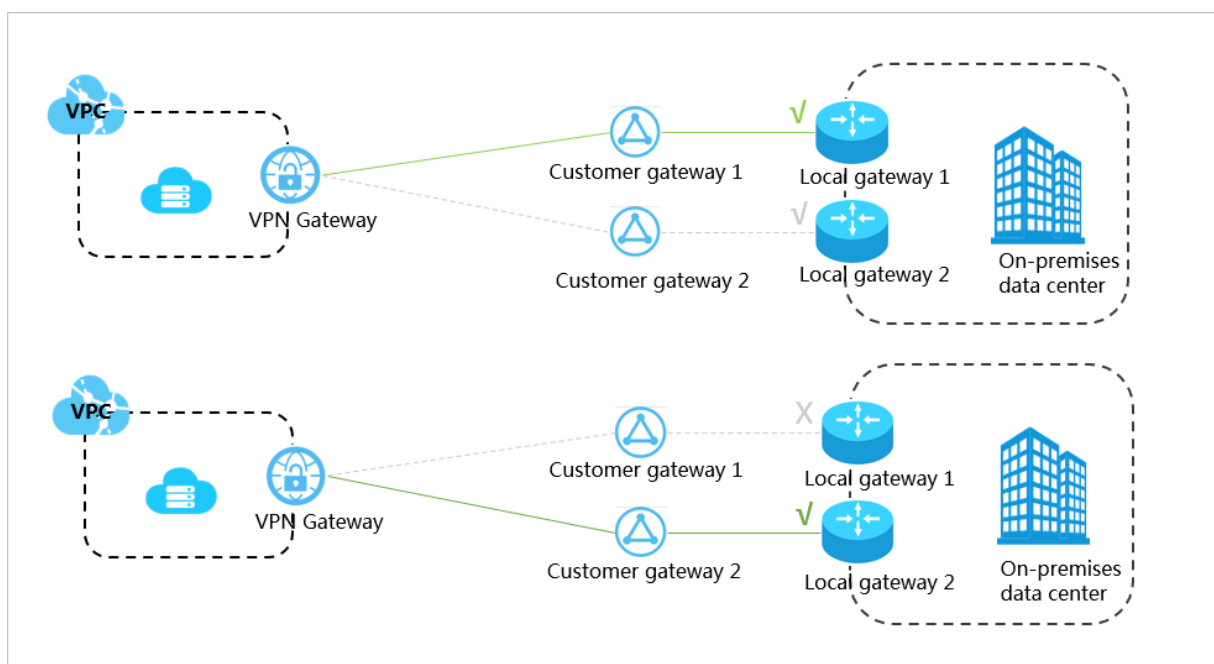
1. In the left-side navigation pane, choose VPN > VPN Gateways.
2. Select the region of the target VPN Gateway.
3. Find the target VPN Gateway, and click the instance ID.
4. On the Policy-based Routing tab page, find the target policy-based route and click Edit in the Actions column.
5. In the displayed dialog box, set the weight to 100.
6. Repeat the preceding steps to set the weight of the other route to 0.

## 2.2 Dual customer gateway configuration

You can deploy two local gateways and connect the two local gateways to a VPN Gateway to create two IPsec-VPN connections. In this way, you can implement an IPsec-VPN connection redundancy.

### Solution

As shown in the following figure, you can connect each of the two customer gateways to the VPN Gateway to create two IPsec-VPN tunnels. Then, you can enable health checks for the two IPsec-VPN tunnels and make sure that the two IPsec-VPN tunnels are negotiated successfully. After that, if a health check detects that one customer gateway is abnormal, the traffic switches to the other customer gateway automatically.



### Prerequisites

Make sure that the following requirements are met before you begin:

- The protocols IKEv1 and IKEv2 are supported by the gateway devices located at your on-premises data center, and static IP addresses are configured for the gateway devices.
- The IP address ranges used by the VPC and the on-premises data center do not conflict with each other.

## Step 1: Create a VPN Gateway

To create a VPN Gateway, follow these steps:

1. Log on to the [VPC console](#).
2. In the left-side navigation pane, choose VPN > VPN Gateways.
3. Click Create VPN Gateway.
4. On the purchase page, configure the VPN Gateway and complete the payment. In this example, use the following configurations:

- **Region:** Select the region of the VPN Gateway. In this example, select China (Hangzhou).



**Note:**

In an actual scenario, make sure that the VPC and the VPN Gateway are in the same region.

- **Name:** Enter a name for the VPN Gateway to be created.
- **VPC:** Select the VPC to be connected.
- **Peak Bandwidth:** Select a peak bandwidth. The bandwidth is the Internet bandwidth of the VPN Gateway.
- **IPsec-VPN:** Choose whether to enable the IPsec-VPN feature. In this example, select Enable.
- **SSL-VPN:** Choose whether to enable the SSL-VPN feature.
- **SSL connections:** Select the maximum number of clients you want to connect to simultaneously.



**Note:**

**You can configure this option only after you enable the SSL-VPN feature.**

- **Billing Cycle:** The billing cycle is set to By Hour by default.

**VPN Gateway**

Basic	Region	China (Qingdao)	China (Beijing)	China (Zhangjiakou)	<b>China (Hangzhou)</b>	China (Shanghai)	China (Shenzhen)
				Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
				China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
	Name	TEST123					
	VPC	emr_test_vpc					
	Peak Bandwidth	10 Mbps		100 Mbps		200 Mbps	
	Billing Method	Pay By Traffic					
Function Config	IPsec-VPN	Enable					
	SSL-VPN	Disable					
		Enable					
	For VPN Gateway instances purchased before Jan 20, 2018, a ticket needs to be submitted to enable SSL-VPN function.						
	SSL connections	5	10	20	50	100	500
		1000					
	Please choose your SSL Connections based on the maximum number of VPN clients connected at the same time						
Purchase Plan	Billing Cycle	By Hour					

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

The initial status of a VPN Gateway is Preparing, which indicates the initialization of the VPN Gateway and may take up to two minutes to be completed. When the status of the VPN Gateway changes to Normal, it indicates that the VPN Gateway is ready to use.



**Note:**

**It usually takes one to five minutes to create a VPN Gateway.**

## **Step 2: Create two customer gateways**

Create two customer gateways and register the public IP addresses of the local gateway devices to the customer gateways. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > Customer Gateways.
2. Select the China (Hangzhou) region.
3. Click Create Customer Gateway.
4. Configure the customer gateway according to the following information:
  - **Name:** Enter a name for the customer gateway to be created.
  - **IP Address:** Enter the public IP address of the gateway device at the on-premises data center.
  - **Description:** Enter a description of the customer gateway.
5. On the Create Customer Gateway page, click + Add to add another customer gateway.



**6. Click OK.**

Create Customer Gateway

• Name ?

local 5/128 ✓

• IP Address ?

Description

+ Add Delete

OK Cancel

Contact Us

**Step 3: Create two IPsec-VPN connections**

Create two IPsec-VPN connections to connect the VPN Gateway with the two customer gateways. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select the China (Hangzhou) region.
3. Click Create IPsec Connection.

4. Configure the IPsec-VPN connection according to the following information and then click OK:

- **Name:** Enter a name for the IPsec-VPN connection.
- **VPN Gateway:** Select the created VPN Gateway.
- **Customer Gateway:** Select one of the two created customer gateways.
- **Local Network:** Enter the IP address range of the VPC to be connected with the on-premises data center. In this example, enter 192.168.0.0/16. To add multiple local networks, click + Add Local Network.



**Note:**

Only IKE v2 supports multiple local networks.

- **Remote Network:** Enter the CIDR block of the on-premises data center to be connected with the VPC. In this example, enter 172.16.0.0/12. To add multiple remote networks, click + Add Remote Network.



**Note:**

**Only IKE v2 supports multiple local networks.**

- **Effective Immediately:** Choose whether to delete the negotiated IPsec-VPN tunnel and re-initiate the negotiation.
  - **Yes:** Re-initiates the negotiation immediately after the IPsec-VPN connection is created.
  - **No:** Re-initiates the negotiation when traffic is detected in the tunnel.
- **Synchronize to VPN Route Table:** Choose whether to synchronize IPsec-VPN traffic routes to the VPN route table. We recommend that you select Yes.
  - **Yes:** The IPsec-VPN traffic routes are synchronized to the VPN route table after the IPsec-VPN connection is created.
  - **No:** The IPsec-VPN traffic routes are not synchronized to the VPN route table after the IPsec-VPN connection is created. You need to add gateway routes on the VPN Gateway page. For more information, see [VPN Gateway route overview](#).
- **Pre-Shared Key:** Enter the pre-shared key. This value must be the same as that configured in the local gateway.
- **Health Check:** Enable the health check feature and enter the destination IP address, source IP address, retry interval, and retry times.

Use the default configurations for other parameters.

Create IPsec Connection

Name ?

0/128

VPN Gateway

Please select

Customer Gateway

Please select

Local Network ?

0.0.0.0/0

+ Add Local Network

Remote Network ?

0.0.0.0/0

+ Add Remote Network

Effective Immediately ?

☐ Yes

☒ No

OK

Cancel

Contact Us

5. In the displayed dialog box, click OK.

6. Find the target route entry, click Publish in the Actions column, and then in the displayed dialog box, click OK.

**Create IPsec Connection**

• **Name** ?

0/128

• **VPN Gateway**

Please select

• **Customer Gateway**

Please select

• **Local Network** ?

0.0.0.0/0

+ Add Local Network

• **Remote Network** ?

0.0.0.0/0

+ Add Remote Network

**Effective Immediately** ?

☐ Yes ☒ No

OK Cancel

Contact Us

7. Repeat the preceding steps to create another IPsec-VPN connection that connects to the other customer gateway.

#### Step 4: Configure the local gateways

To configure the local gateways, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.

2. Select the China (Hangzhou) region.
3. Find the target IPsec-VPN connection and click Download Configuration.

IPsec Connections					
Create IPsec Connection		Refresh	Custom	Instance ID <input type="text"/> Enter a ID <input type="button" value="Q"/>	
Instance ID/Name	VPN Gateway	Customer Gateway	Connection Status	Created At	Actions
vpn- IPsec	vpn- vpn2	cg- customer2	-	01/25/2018, 16:42:44	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Download Configuration</a>

4. Configure the local gateways by loading the downloaded IPsec-VPN connection configurations to the local gateway device. For more information, see [Configure local gateways](#).

The RemoteSubnet and LocalSubnet in the downloaded configurations are converse in operation of the local network and the remote network you configured when you create the IPsec-VPN connection. Specifically, from the perspective of VPN Gateway, the remote network is the on-premises data center and the local network is the VPC. However, from the perspective of the local gateway, LocalSubnet is the CIDR block of the on-premises data center and RemoteSubnet is the CIDR block of the VPC.

IPsec Connection Configuration

```

{
  "LocalSubnet": "192.168.0.0/24",
  "RemoteSubnet": "10.0.0.0/24",
  "IpsecConfig": {
    "IpsecPfs": "group2",
    "IpsecEncAlg": "aes",
    "IpsecAuthAlg": "md5",
    "IpsecLifetime": 86400
  },
  "Local": "255.255.255.0",
  "Remote": "47.93.13",
  "IkeConfig": {
    "IkeAuthAlg": "md5",
    "LocalId": "255.255.255.0",
    "IkeEncAlg": "aes",
    "IkeVersion": "ikev1",
    "IkeMode": "main",
    "IkeLifetime": 86400,
    "RemoteId": "47.93.13",
    "Psk": "j1q",
    "IkePfs": "group2"
  }
}

```

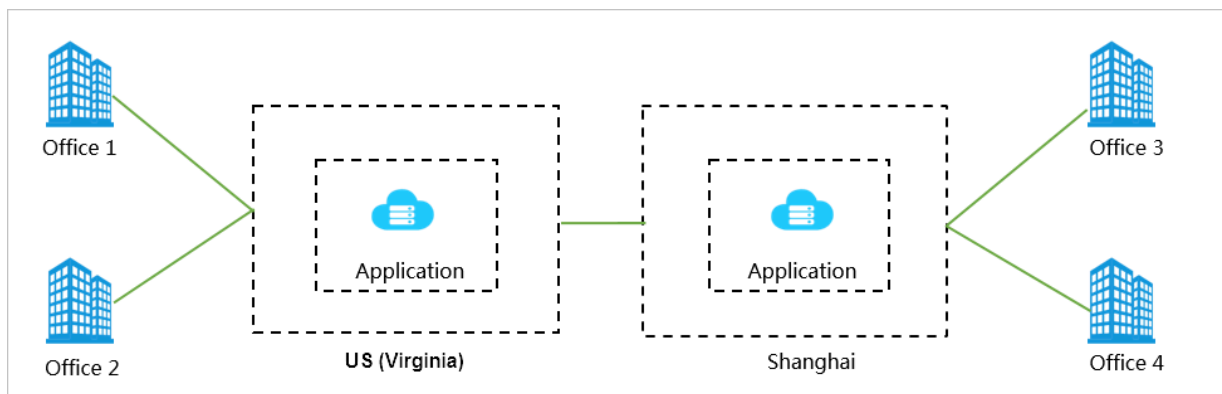
Contact Us

## 3 Establish a global network through VPN Gateway and CEN

This topic describes how to establish a global network by using VPN Gateway and Cloud Enterprise Network (CEN). International enterprises can establish a global network by using VPN Gateway and CEN. CEN can reduce cross-border network latency and VPN Gateway can help lower the cost of last-mile connections and client connections.

### Scenario

An international company wants to deploy different applications in multiple countries, but the applications need to be accessible by multiple offices in each country. In this example, the company has one VPC in the US (Virginia) region, and one in the China (Shanghai) region, and each VPC has a separate application deployed. The company also has two offices in Virginia and two in Shanghai.



### Solution

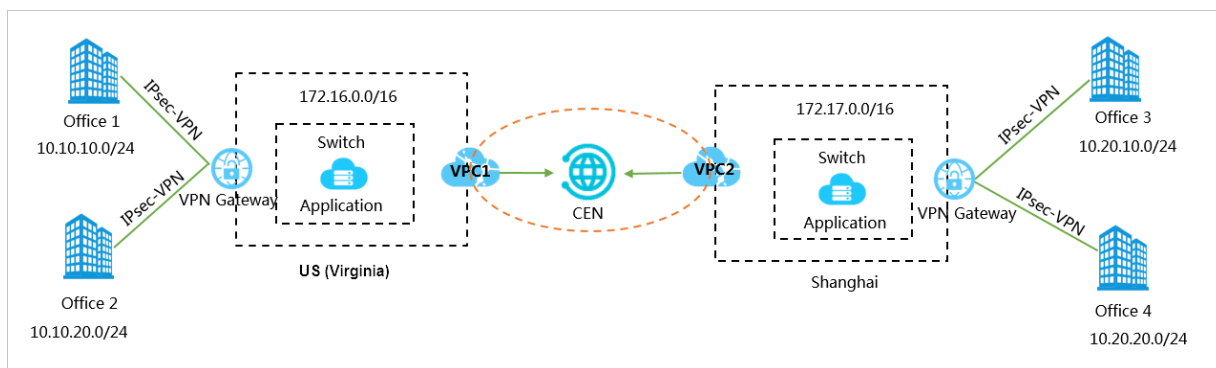
The following table details traditional connectivity solutions for offices across the globe to communicate with each other, and the problems inherent in these traditional solutions.

Traditional solution	Problem
Communication through the Internet	Data stored locally is exposed over the Internet and the network quality of the Internet connection is not guaranteed.

Traditional solution	Problem
Communication through IPsec-VPN	Cross-border communication is affected by the network quality of the Internet connection.
Communication through dedicated lines	The installation of dedicated lines and subsequent maintenance incur high costs.

To resolve the preceding problems of traditional connection solutions, Alibaba Cloud allows you to use VPN Gateway and CEN to connect applications and offices located around the world.

In the Alibaba Cloud solution, an application is deployed to each VPC located in US (Virginia) and China (Shanghai) respectively (in this example, the VPCs for Virginia and Shanghai are VPC1 and VPC2 respectively). Then, VPC1 and VPC2 are connected by using CEN. After that, Office 1 and Office 2 in Virginia are connected to the VPN Gateway of VPC1, and Office 3 and Office 4 in Shanghai are connected to the VPN Gateway of VPC2 through IPsec-VPN connections. In this way, the applications and offices connected to the VPCs in the US (Virginia) region and the China (Shanghai) region can communicate with each other.



### Prerequisites

- The Alibaba Cloud environment is prepared. Specifically, VPCs and VSwitches are created and applications are deployed.
- Local gateways are configured in the offices and a static public IP address is configured for each local gateway.
- The CIDR blocks to be connected do not conflict with each other.



**Step 1: Create IPsec-VPN connections for the offices in Virginia**

1. Create a VPN Gateway for the VPC in the US (Virginia) region. For more information, see [Create a VPN Gateway](#).
2. Create two customer gateways and register the public IP addresses of the two local gateways in the two Virginia offices to the customer gateways.

The IP addresses of customer gateways are the public IP addresses of local gateways in the offices. For more information, see [Create a customer gateway](#).

3. Create two IPsec-VPN connections to connect the VPN Gateway with the two customer gateways. For more information, see [Create an IPsec-VPN connection](#).

- Local Network: Enter 0.0.0.0/0.

**Note:**

We recommend that you set the CIDR block at the Alibaba Cloud side to 0.0.0.0/0 to simplify your network topology. In that way, you only need to establish an IPsec-VPN connection to connect each office with Alibaba Cloud and do not need to modify the configurations of the connection if you add new offices to the network.

- Remote Network: Enter the CIDR blocks of Office 1 and Office 2, that is, 10.10.10.0/24 and 10.10.20.0/24.

4. Configure local gateways in the Virginia offices.

Configure local gateways based on the configurations of the created IPsec-VPN connections. For more information, see [Configure local gateways](#).

**Step 2: Create IPsec-VPN connections for the offices in Shanghai**

Create IPsec-VPN connections for the offices in Shanghai. To do so, refer to the instructions detailed in Step 1.

**Step 3: Connect VPCs**

Connect the VPCs by using CEN. For more information, see [Tutorial overview](#).

**Step 4: Add routes in CEN**

Publish the routes in the VPCs that are directed to the VPN Gateways to CEN so that other networks in CEN can learn the routes.

For more information, see [Publish a route entry to CEN](#).

**Step 5: Configure security groups**

**Configure security groups for the ECS instances where you applications are deployed.**

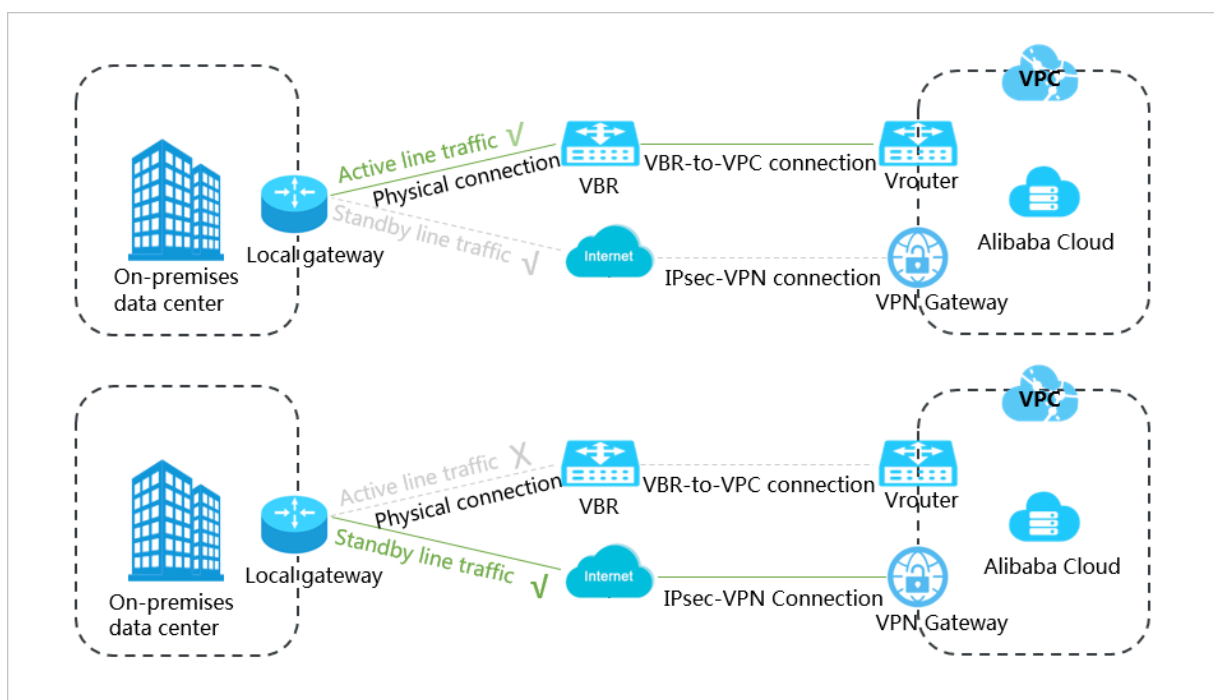
**After you have completed the preceding steps, you can connect your applications with offices in different regions, and the offices and applications can communicate with each other over the intranet.**

## 4 Implement an active/standby configuration by using VPN Gateway and Express Connect

This topic describes how to implement an active/standby configuration by using a VPN Gateway and a physical connection of Express Connect to improve the availability of your applications.

You can connect your on-premises data center to an Alibaba Cloud VPC through both a physical connection and an IPsec-VPN connection.

- When the physical connection works normally, the traffic between the on-premises data center and the VPC is forwarded through the physical connection.
- When the physical connection is abnormal, the traffic between the on-premises data center and the VPC is directed to the IPsec-VPN tunnel.



### Prerequisites

A physical connection is created to allow intercommunication between your on-premises data center and the VPC.

For more information, see [Connect an on-premises IDC to a VPC through a physical connection](#).

---

**Step 1: Create a VPN Gateway**

To create a VPN Gateway, follow these steps:

1. Log on to the [VPC console](#).
2. In the left-side navigation pane, choose VPN > VPN Gateways.
3. Click Create VPN Gateway.
4. On the purchase page, configure the VPN Gateway and complete the payment. In this example, use the following configurations:

- **Region:** Select the region of the VPN Gateway to be created. In this example, select China (Hangzhou).



**Note:**

In an actual scenario, make sure that the VPC and the VPN Gateway are in the same region.

- **Name:** Enter a name for the VPN Gateway to be created.
- **VPC:** Select the VPC to be connected.
- **Peak Bandwidth:** Select a peak bandwidth. The bandwidth is the Internet bandwidth of the VPN Gateway.
- **IPsec-VPN:** Choose whether to enable the IPsec-VPN feature. In this example, select Enable.
- **SSL-VPN:** Choose whether to enable the SSL-VPN feature.
- **SSL connections:** Select the maximum number of clients you want to connect to simultaneously.



**Note:**

**You can only configure this option after you enable the SSL-VPN feature.**

- **Billing Cycle:** The billing cycle is set to By Hour by default.

VPN Gateway

Region

China (Qingdao)	China (Beijing)	China (Zhangjiakou)	<b>China (Hangzhou)</b>	China (Shanghai)	China (Shenzhen)
Hong Kong	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
UAE (Dubai)	Germany (Frankfurt)	China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
UK(London)					

Basic

Name

TEST123

VPC

emr\_test\_vpc

Peak Bandwidth

10 Mbps

100 Mbps

200 Mbps

Billing Method

Pay By Traffic

Function Config

IPsec-VPN

Enable

Disable

SSL-VPN

Disable

**Enable**

For VPN Gateway instances purchased before Jan 20, 2018, a ticket needs to be submitted to enable SSL-VPN function.

SSL connections

5	10	20	50	100	500
1000					

Please choose your SSL Connections based on the maximum number of VPN clients connected at the same time

Purchase Plan

Billing Cycle

By Hour

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

The initial status of a VPN Gateway is Preparing, which indicates the initialization of the VPN Gateway and may take up to two minutes to be completed. When the status of the VPN Gateway changes to Normal, it indicates that the VPN Gateway is ready to use.



**Note:**

It usually takes 1 to 5 minutes to create a VPN Gateway.

### Step 2: Create a customer gateway

Create a customer gateway and register the public IP address of the local gateway to the customer gateway. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > Customer Gateways.
2. Select the China (Hangzhou) region.
3. Click Create Customer Gateway.
4. Configure the customer gateway according to the following information:
  - Name: Enter a name for the customer gateway to be created.
  - IP Address: Enter the public IP address of the gateway device located at the on-premises data center.
  - Description: Enter a description of the customer gateway.

### Step 3: Create an IPsec-VPN connection

Create an IPsec-VPN connection to connect the VPN Gateway with the customer gateway. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select the China (Hangzhou) region.
3. Click Create IPsec Connection.
4. Configure the IPsec-VPN connection according to the following information and then click OK.
  - Name: Enter a name for the IPsec-VPN connection to be created.
  - VPN Gateway: Select the created VPN Gateway.
  - Customer Gateway: Select the created customer gateway.
  - Local Network: Enter the IP address range of the VPC to be connected with the on-premises data center. In this example, enter 192.168.0.0/16. To add multiple local networks, click + Add Local Network.



Note:

---

**Only IKE v2 supports multiple local networks.**

- **Remote Network:** Enter the CIDR block of the on-premises data center to be connected with the VPC. In this example, enter 172.16.0.0/12. To add multiple remote networks, click + Add Remote Network.

**Note:**

---

**Only IKE v2 supports multiple remote networks.**

- **Effective Immediately:** Choose whether to delete the negotiated IPsec-VPN tunnel and re-initiate the negotiation.
  - **Yes:** Re-initiates the negotiation immediately after the IPsec-VPN connection is created.
  - **No:** Re-initiates the negotiation when traffic is detected in the tunnel.
- **Synchronize to VPN Route Table:** Choose whether to synchronize IPsec-VPN traffic routes to the VPN route table. We recommend that you select Yes.
  - **Yes:** The IPsec-VPN traffic routes are synchronized to the VPN route table after the IPsec-VPN connection is created.
  - **No:** The IPsec-VPN traffic routes are not synchronized to the VPN route table after the IPsec-VPN connection is created. You need to add gateway routes on the VPN Gateway page. For more information, see [VPN Gateway route overview](#).
- **Pre-Shared Key:** Enter the pre-shared key. This value must be the same as that configured in the local gateway.
- **Health Check:** Enable the health check feature and enter the destination IP address, source IP address, retry interval, and retry times.

Use the default configurations for other parameters.



### Create IPsec Connection

?

×

● Name ?

0/128

● VPN Gateway

Please select

▼

● Customer Gateway

Please select

▼

● Local Network ?

0.0.0.0/0

+ Add Local Network

● Remote Network ?

0.0.0.0/0

+ Add Remote Network

Effective Immediately ?

☐ Yes ☒ No

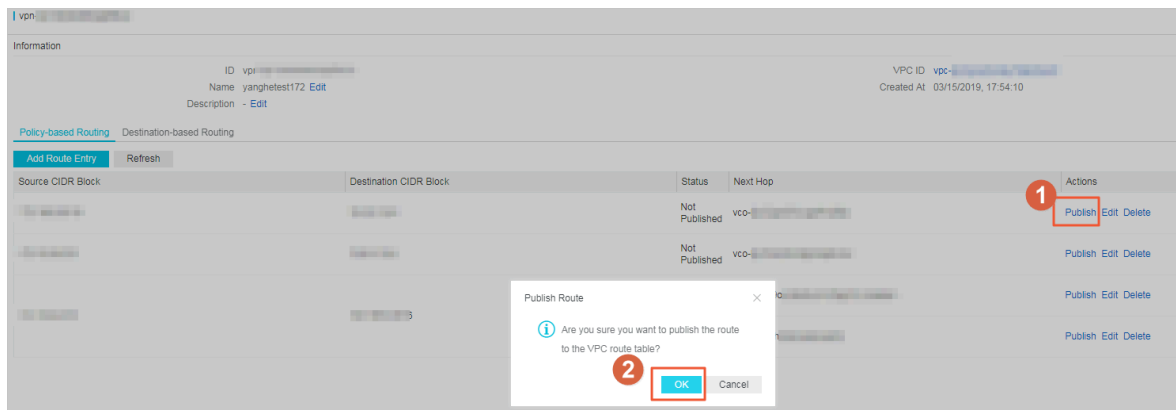
OK

Cancel

Contact Us

5. In the displayed dialog box, click OK.

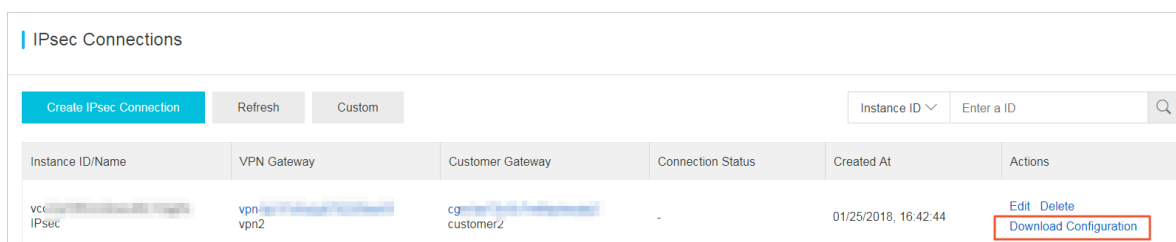
- Find the target route entry, click Publish in the Actions column, and then in the displayed dialog box, click OK.



#### Step 4: Configure the local gateway

To configure the local gateway, follow these steps:

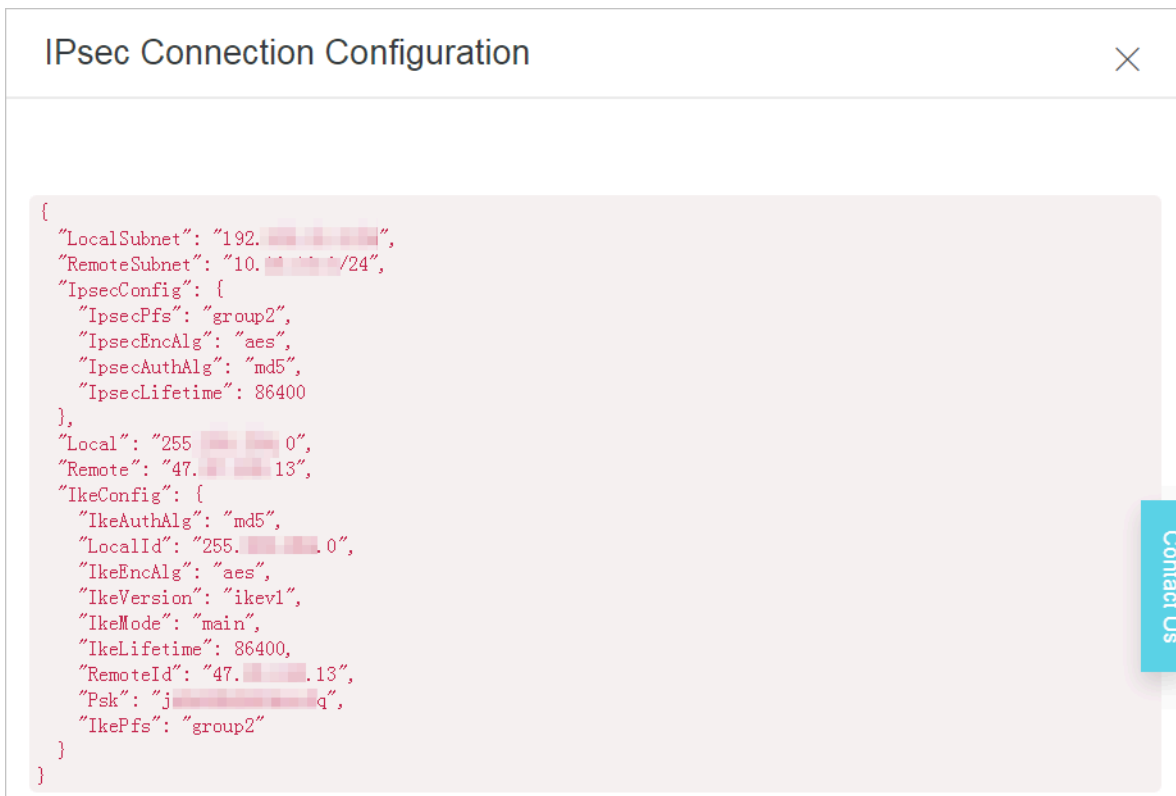
- In the left-side navigation pane, choose VPN > IPsec Connections.
- Select the China (Hangzhou) region.
- Find the target IPsec-VPN connection and click Download Configuration.



- Configure the local gateway based on the downloaded configurations of the IPsec-VPN connection. For more information, see [Configure local gateways](#).

The items RemoteSubnet and LocalSubnet in the downloaded configurations operate converse to the setup of the local network and the remote network you configured when you create the IPsec-VPN connection. Specifically, from the perspective of VPN Gateway, the remote network is the on-premises data center and the local network is the VPC. However, from the perspective of the local

gateway, LocalSubnet is the CIDR block of the on-premises data center and RemoteSubnet is the CIDR block of the VPC.



#### Step 5: Configure health checks for the VBR of the physical connection

Configure health checks for the Virtual Border Router (VBR) of the physical connection to make sure that the status of the physical connection can be checked by the VPC and traffic can be directed to the IPsec-VPN connection when the physical connection fails.

For more information, see [Configure health checks](#).

#### Step 6: Configure the physical connection device

Configure an active route and a standby route to direct to the VPC on the physical connection device, and enable the health check function for the physical connection. In this way, when the physical connection fails, traffic is forwarded to the IPsec-VPN connection.