Alibaba Cloud
vpn gateway

IPsec-VPN Quick Start

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

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Tutorial introduction

This topic describes how to create a site-to-site VPN connection through IPsec-VPN.

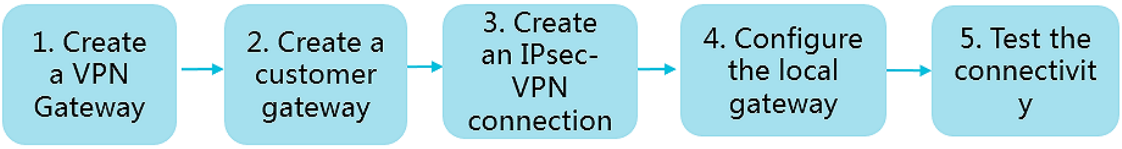
Prerequisites

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 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.

Procedure

The following figure shows the procedure of establishing a site-to-site VPN connection through IPsec-VPN.


1. Create a VPN Gateway
2. Create a customer gateway
3. Create an IPsec-VPN connection
4. Configure the local gateway
5. Test the connectivit y

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.

   Create a customer gateway, and then upload the configuration of the local gateway to Alibaba Cloud. A customer gateway can be connected to multiple VPN Gateways.
3. Create an IPsec-VPN connection.

   Create an IPsec-VPN connection to implement an encrypted communicat ion tunnel between your on-premises data center and the VPN Gateway. We recommend that you synchronize the route entries of the data flow that needs to be encrypted to the VPN route table.

4. Configure the local gateway.

   Configure the local gateway according to the IPsec-VPN connection configurations. For more information, see *Configure local CPEs*.

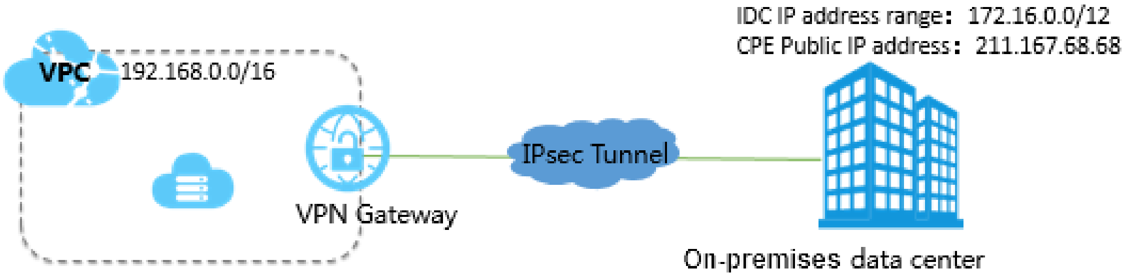
5. Test the connectivity.

   Log on to an ECS instance that does not have a public IP address in the target Alibaba Cloud VPC. Then, ping the private IP address of a host in your on-premises data center to test if the VPC and the on-premises data center can communicate with each other.

For more information, see *Create a site-to-site connection through IPsec-VPN*.

2 Create a site-to-site connection through IPsec-VPN

This topic describes how to create a site-to-site VPN connection through IPsec-VPN to connect an Alibaba Cloud VPC with an on-premises data center.


IDC IP address range: 172.16.0.0/12
CPE Public IP address: 211.167.68.68
VPC
192.168.0.0/16
VPN Gateway
IPsec Tunnel
On-premises data center

Prerequisites

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

- 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

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).

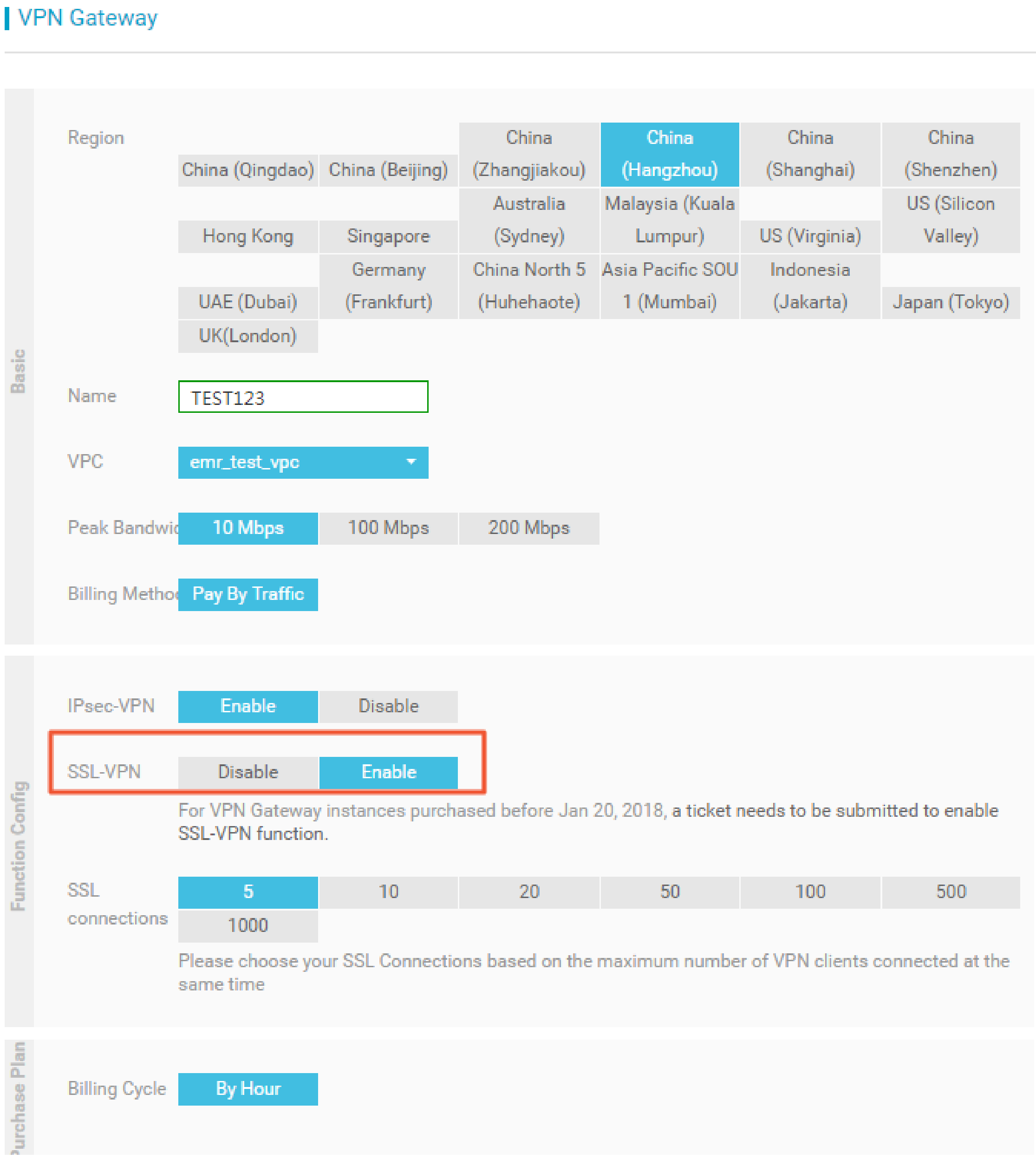
      Note:

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: Select whether to enable the IPsec-VPN feature.
- SSL-VPN: Select 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.



VPN Gateway

Basic

Region

China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	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)					

Name: TEST123

VPC: emr_test_vpc

Peak Bandwic: 10 Mbps | 100 Mbps | 200 Mbps

Billing Methoc: 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

urchase Plan

Billing Cycle: By Hour

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

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

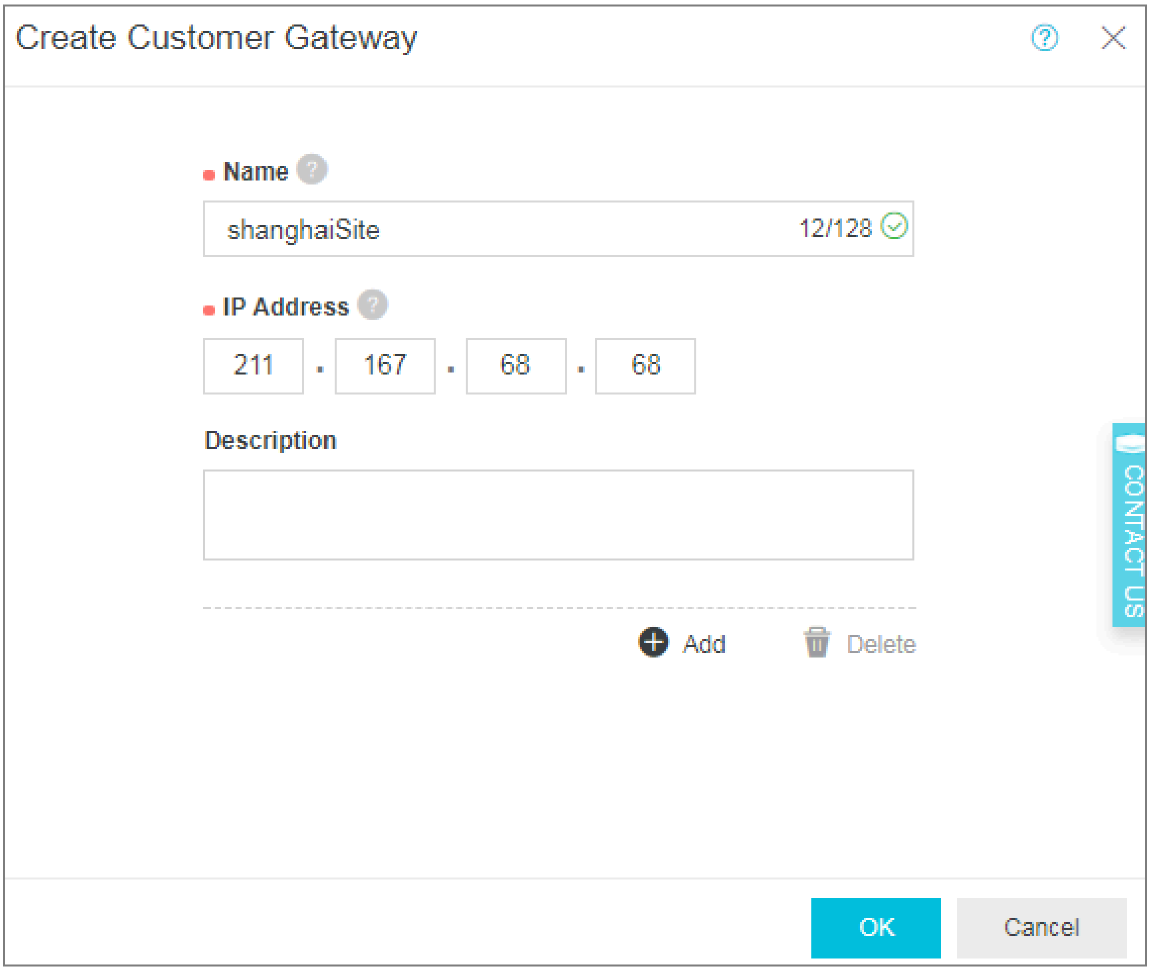
The initial status of a VPN Gateway is Preparing, which indicates the initialization of the VPN Gateway and may take up to two minutes to be completed. When the status of the VPN Gateway changes to Normal, it indicates that the VPN Gateway is ready to use.

Note:

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

Step 2: Create a customer gateway

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, and then click OK.
   - Name: Enter a name for the customer gateway to be created.
   - IP Address: Enter the public IP address configured for the gateway device of the on-premises data center.
   - Description: Enter a description of the customer gateway.



Create Customer Gateway

Name: shanghaiSite 12/128

IP Address: 211 . 167 . 68 . 68

Description:

You can also click + to add multiple customer gateways.

Step 3: Create an IPsec-VPN connection

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 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:

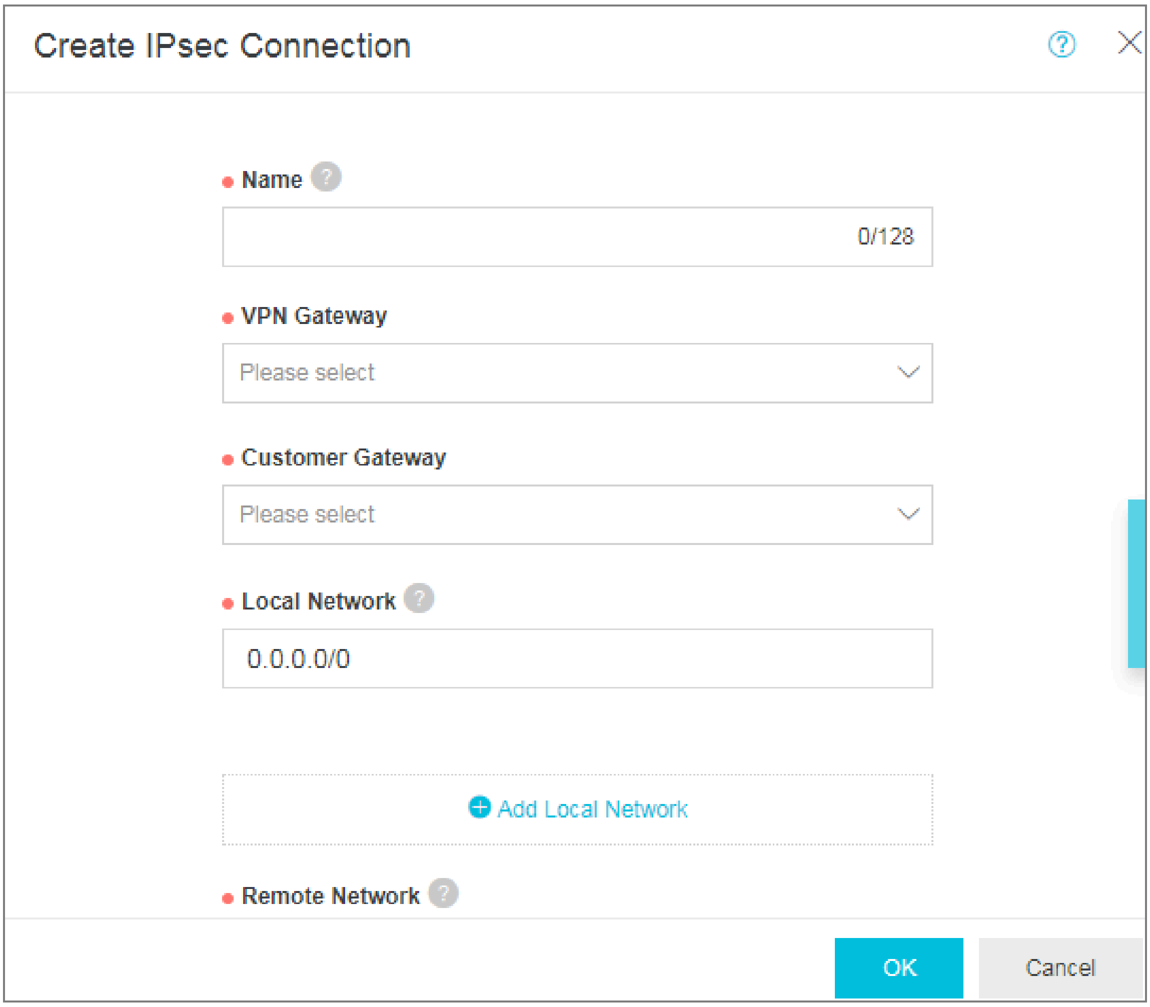
     Only IKE v2 supports multiple local networks.
   - Remote Network: Enter the CIDR block of the on-premises data center to be connected with the VPC. In this example, enter 172.16.0.0/12. To add multiple local networks, click + Add Remote Network.

     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.
- Pre-Shared Key: Enter a pre-shared key. This value must be the same as that configured in the local gateway.

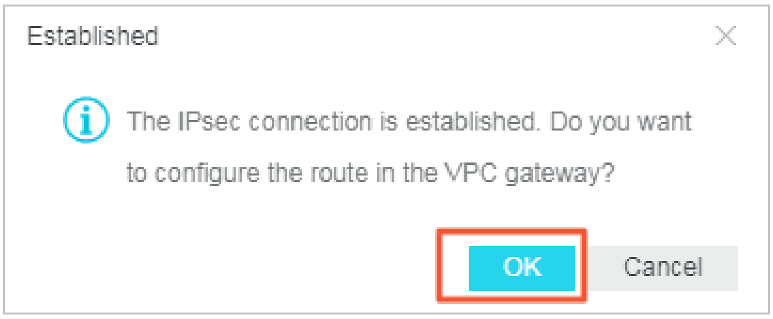
Use the default configurations for other parameters.



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

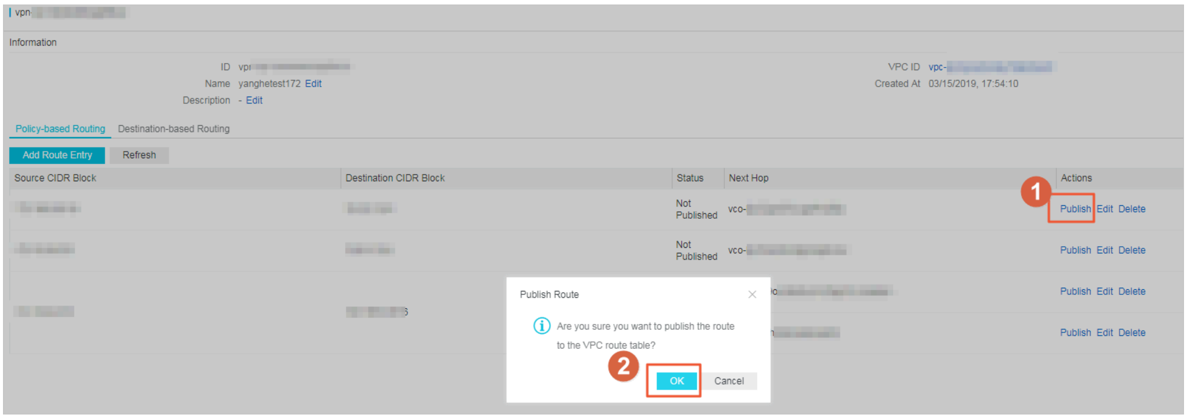
5. In the displayed dialog box, click OK.



Established

The IPsec connection is established. Do you want to configure the route in the VPC gateway?

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



vpn-[redacted]

Information

ID vp[redacted]
Name yanghetest172 Edit
Description - Edit

VPC ID vpc-[redacted]
Created At 03/15/2019, 17:54:10

Policy-based Routing Destination-based Routing

Add Route Entry Refresh

Source CIDR Block	Destination CIDR Block	Status	Next Hop	Actions
[redacted]	[redacted]	Not Published	vco-[redacted]	Publish Edit Delete
[redacted]	[redacted]	Not Published	vco-[redacted]	Publish Edit Delete
[redacted]	[redacted]		[redacted]	Publish Edit Delete
			[redacted]	Publish Edit Delete

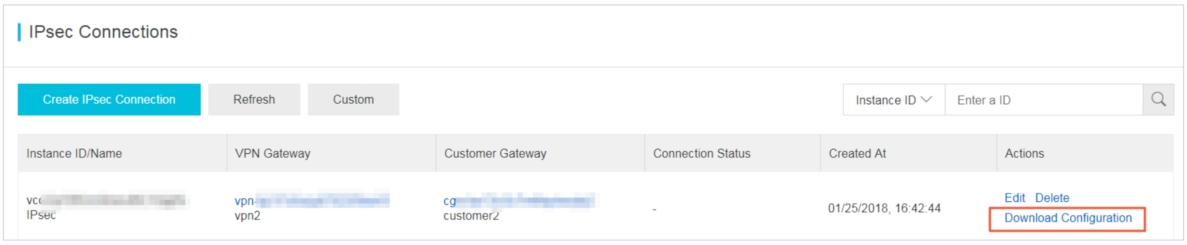
Publish Route

Are you sure you want to publish the route to the VPC route table?

OK Cancel

Step 4: Configure the local gateway

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.



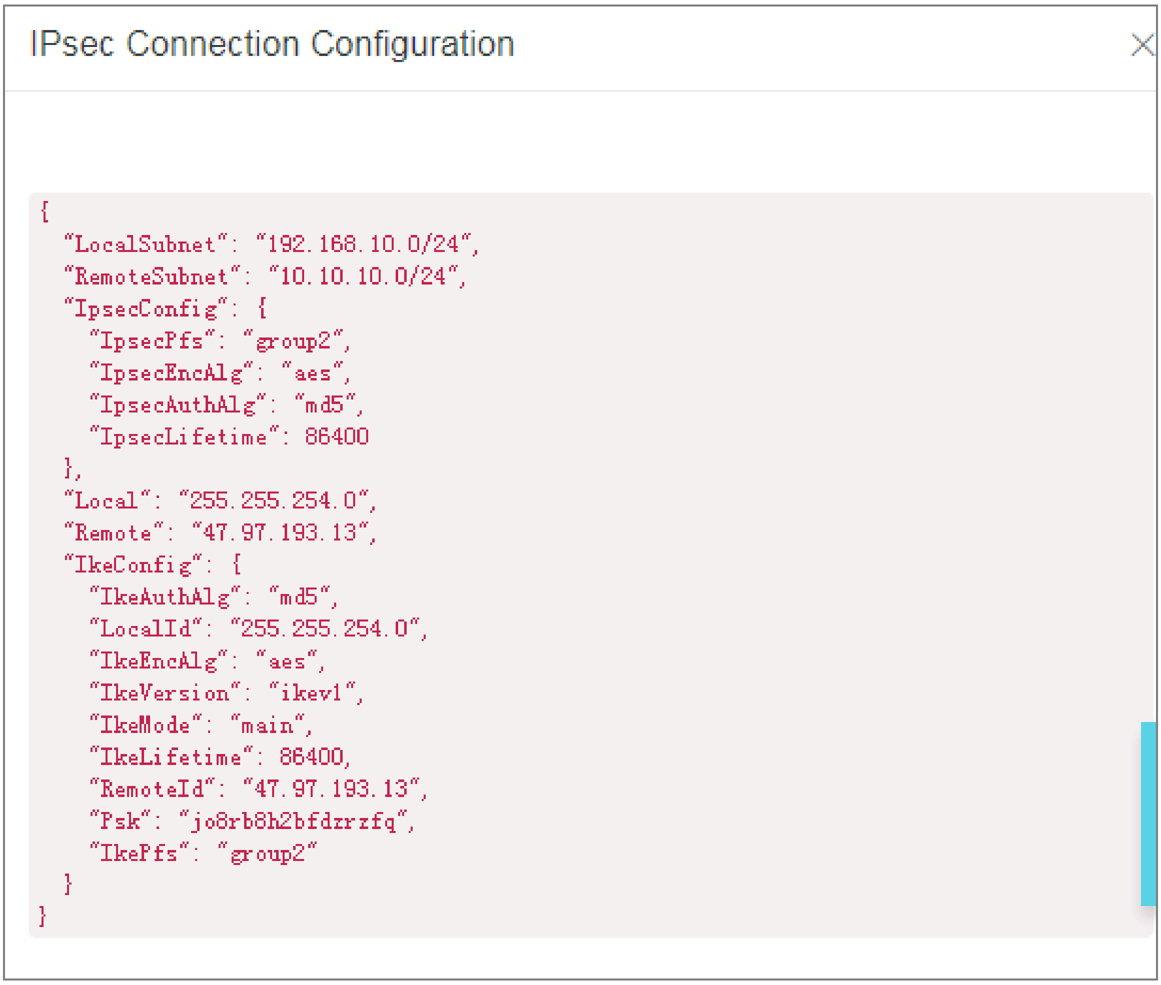
IPsec Connections

Create IPsec Connection Refresh Custom Instance ID Enter a ID

Instance ID/Name	VPN Gateway	Customer Gateway	Connection Status	Created At	Actions
vc[redacted] IPsec	vpn-[redacted] vpn2	cg[redacted] customer2	-	01/25/2018, 16:42:44	Edit Delete Download Configuration

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

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



IPsec Connection Configuration

```
{
  “LocalSubnet”: “192.168.10.0/24”,
  “RemoteSubnet”: “10.10.10.0/24”,
  “IpsecConfig”: {
    “IpsecPfs”: “group2”,
    “IpsecEncAlg”: “aes”,
    “IpsecAuthAlg”: “md5”,
    “IpsecLifetime”: 86400
  },
  “Local”: “255.255.254.0”,
  “Remote”: “47.97.193.13”,
  “IkeConfig”: {
    “IkeAuthAlg”: “md5”,
    “LocalId”: “255.255.254.0”,
    “IkeEncAlg”: “aes”,
    “IkeVersion”: “ikev1”,
    “IkeMode”: “main”,
    “IkeLifetime”: 86400,
    “RemoteId”: “47.97.193.13”,
    “Psk”: “jo8rb8h2bfdzrzfq”,
    “IkePfs”: “group2”
  }
}
```

Step 5: Test the connectivity

Log on to an ECS instance that does not have a public IP address in the target Alibaba Cloud VPC. Then, ping the private IP address of a host in your on-premises data center to test if the VPC and the on-premises data center can communicate with each other.