Alibaba Cloud
vpn gateway

IPsec-VPN Quick Start

Issue: 20190626

Legal disclaimer

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

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

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⛔ Danger: Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠ Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	ⓘ 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 overview

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

Prerequisites

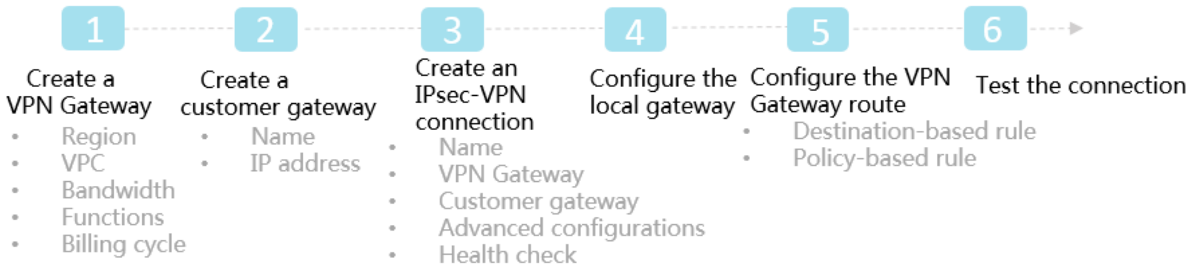
Before creating a site-to-site VPN connection, make sure the following conditions are met:

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

  IPsec-VPN supports IKEv1 and IKEv2 protocols. Devices that support these two protocols can connect to Alibaba Cloud VPN Gateway, including devices of Huawei , H3C, Hillstone, SANGFOR, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.
- A static public IP address is configured for the local gateway.
- The IP address ranges of the VPC and on-premises data center to be connected do not conflict with each other.

Procedure

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



1. Create a VPN Gateway

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

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

3. Create an IPsec connection

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

4. Configure the local gateway

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

5. Configure the VPN Gateway route

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

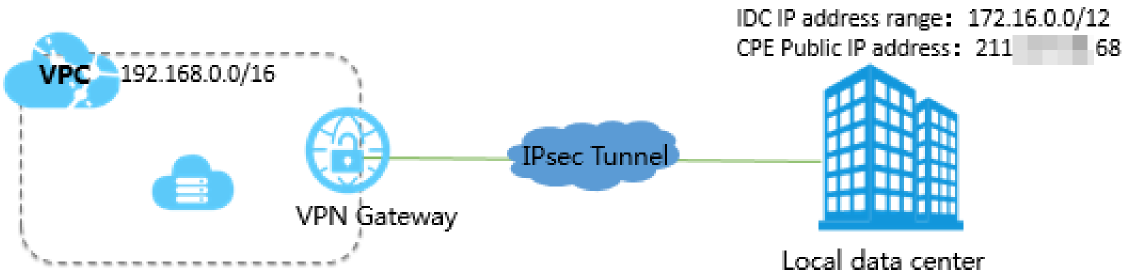
6. Test the connection

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

For more information, see *Establish a connection between a VPC and an on-premises data center*.

2 Establish a connection between a VPC and an on-premises data center

This topic describes how to create an IPsec-VPN connection between a VPC and an on-premises data center.


IDC IP address range: 172.16.0.0/12
CPE Public IP address: 211 [redacted] 68
VPC
192.168.0.0/16
VPN Gateway
IPsec Tunnel
Local data center

Prerequisites

Before you use the IPsec-VPN function to create a VPN connection between a VPC and an on-premises data center, make sure that the following conditions are met:

- The gateway device of the on-premises data center is normal. Alibaba Cloud VPN Gateway supports standard IKEv1 and IKEv2 protocols. Devices that support these two protocols can connect to Alibaba Cloud VPN Gateway, including devices of Huawei, H3C, Hillstone, SANGFOR, Cisco ASA, Juniper, SonicWall, Nokia, IBM, Ixia , and more.
- A static public IP address is configured for the gateway device of the on-premises data center.
- The CIDR blocks of the on-premises data center and the VPC to be connected 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. On the VPN Gateways page, click Create VPN Gateway.

4. On the purchase page, configure the VPN Gateway according to the following information and click Buy Now.

   - Name: Enter the name of the VPN Gateway.
   - Region: Select the region to which the VPN Gateway belongs.

     > Note:
     >
     > Make sure that the VPC and the VPN Gateway are in the same region.
   - VPC: Select the VPC to be connected.
   - Peak Bandwidth: Select a 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. The SSL-VPN feature allows you to connect to a VPC from a computer anywhere.
   - 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: Select the validity period of the purchase.
5. Go back to the VPN Gateways page to view the created VPN Gateway.

   The initial status of a VPN Gateway is Preparing. It changes to Normal in about two minutes. When it 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

To create a customer gateway, follow these steps:

1. In the left-side navigation pane, choose VPN > Customer Gateways.
2. Select a region.
3. On the Customer Gateways page, click Create Customer Gateway.

4. On the Create Customer Gateway page, configure the customer gateway according to the following information, and click OK.

   - Name: Enter a customer gateway name.
   - IP Address: Enter the public IP address of the local gateway.
   - Description: Enter a description of the customer gateway.

Step 3: Create an IPsec-VPN connection

To create an IPsec-VPN connection, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select a region.
3. On the IPsec Connections page, click Create IPsec Connection.
4. On the Create IPsec Connection page, configure the IPsec-VPN connection according to the following information and 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.
   - Pre-Shared Key: Enter a pre-shared key. This value must be the same as the one configured in the local gateway.

     Use the default configurations for other options.

Step 4: Configure the local gateway

To configure the local gateway, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select a region.
3. On the IPsec Connections page, find the target IPsec-VPN connection, and click Download Configuration in the Actions column.
4. Configure the local gateway accordingly. For more information, see *Local gateway configuration*.

   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 a route for the VPN Gateway

To configure a route of the VPN Gateway, follow these steps:

1. In the left-side navigation pane, choose VPN > VPN Gateways.
2. Select the region of the target VPN Gateway.
3. On the VPN Gateways page, find the target VPN Gateway and click the instance ID in the Instance ID/Name column.
4. On the Destination-based Routing page, click Add Route Entry.
5. On the Add Route Entry page, configure a destination-based route according to the following information, and click OK.
   - Destination CIDR Block: Enter the private CIDR block of the on-premises data center.
   - Next Hop: Select the target IPsec-VPN connection instance.
   - Publish to VPC: Select whether to publish the new route to the VPC route table. In this example, select Yes.
   - Weight: Select a weight. In this tutorial, select 100.

Step 6: Test the connection

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