

Alibaba Cloud

VPN Gateway User Guide

Document Version: 20200916

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.What is VPN Gateway?	06
2.Manage a VPN Gateway	07
2.1. Create a VPN gateway	07
2.2. Modify a VPN Gateway	08
2.3. Configure routes of a VPN Gateway	08
2.3.1. VPN Gateway route overview	09
2.3.2. Add a policy-based route entry	09
2.3.3. Add a destination-based route	10
2.4. Enable IPsec-VPN and SSL-VPN	11
3.Manage a customer gateway	13
3.1. Create a customer gateway	13
3.2. Modify a customer gateway	13
3.3. Delete a customer gateway	14
4.Configure SSL-VPN	15
4.1. Configuration overview	15
4.2. Manage an SSL server	15
4.2.1. Create an SSL Server	15
4.2.2. Modify an SSL server	17
4.2.3. Delete an SSL server	17
4.3. Manage an SSL client certificate	18
4.3.1. Create an SSL client certificate	18
4.3.2. Download an SSL client certificate	18
4.3.3. Delete an SSL client certificate	19
4.4. Modify the number of concurrent SSL connections	19
5.Configure IPsec-VPN connections	20
5.1. Configuration overview	20

5.2. Manage an IPsec-VPN connection	21
5.2.1. Create an IPsec-VPN connection	21
5.2.2. Modify an IPsec-VPN connection	23
5.2.3. Download the configuration of an IPsec-VPN connec...	24
5.2.4. View IPsec-VPN connection logs	24
5.2.5. Delete an IPsec-VPN connection	25
5.3. Configure local gateways	25
5.3.1. Configure an IPsec-VPN connection through a USG s...	25
5.3.2. Configure H3C firewall	28
5.3.3. Configure strongSwan	30
5.3.4. Configure an IPsec-VPN connection through an SRX	32
5.3.5. Configure an IPsec-VPN connection through a Next-...	34
5.4. Establish a connection between two VPCs	39
5.5. Configure multi-site connections	43
6.Tag management	46
6.1. Overview	46
6.2. Attach tags	47
6.2.1. Attach tags to a VPN gateway	47
6.2.2. Attach tags to multiple VPN gateways at a time	48
6.3. Search VPN gateways by tag	49
6.4. Remove tags	50
6.4.1. Remove tags from a VPN gateway	50
6.4.2. Remove tags from multiple VPN gateways at a time	51
7.MTU notes	53
8.Manage quotas	54

1. What is VPN Gateway?

VPN Gateway is an Internet-based service that allows you to connect enterprise data centers, office networks, or Internet-facing terminals to Alibaba Cloud Virtual Private Cloud (VPC) networks through secure and reliable connections. VPN Gateway supports both IPsec-VPN connections and SSL-VPN connections.

IPsec-VPN

The route-based IPsec-VPN not only facilitates the configuration and maintenance of VPN policies, but also provides flexible traffic routing methods.

You can use IPsec-VPN to connect a VPC to an on-premises data center or connect two VPCs. 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, Ixia, and more.

IPsec-VPN can meet the demands of different scenarios. For more information, see [IPsec-VPN scenarios](#).

SSL-VPN

You can create an SSL-VPN connection to connect a remote client to applications and services deployed in a VPC. When the deployment is complete, you can achieve remote access just by loading the certificate in the client and initiating the connection.

SSL-VPN can meet the demands of different scenarios. For more information, see [SSL-VPN scenarios](#).

2. Manage a VPN Gateway

2.1. Create a VPN gateway

This topic describes how to create a VPN gateway. You must create a VPN gateway before you can use the IPsec-VPN and SSL-VPN services. After the VPN gateway is created, a public IP address is assigned to the VPN gateway.

Procedure

1. Log on to the [VPN gateway console](#).
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. On the **VPN Gateways** page, click **Create VPN Gateway**.
4. On the buy page, set the following parameters and click **Buy Now** to complete the payment.

Parameter	Description
Name	Enter a name for the VPN gateway. The name must be 2 to 128 characters in length and can contain letters, Chinese characters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter or Chinese character.
Region	Select the region where the VPN gateway is deployed. You can create IPsec-VPN connections on VPN gateways to connect an on-premises data center to a VPC network or connect two VPC networks. Make sure that the VPC network and the VPN gateway associated with the VPC network are deployed in the same region.
VPC	Select the VPC network to be associated with the VPN gateway.
Assign VSwitch	Specify whether to manually select a VSwitch for the VPN gateway. Valid values: <ul style="list-style-type: none"> ○ No: The VPN gateway is created and automatically attached a VSwitch in the VPC network. ○ Yes: The VPN gateway is created and attached to the manually specified VSwitch in the VPC network.
Peak Bandwidth	Specify the maximum bandwidth of the VPN gateway. The bandwidth is provided for data transfer over the Internet.
Billing Method	Select a billing method for the VPN gateway. VPN gateways support only the pay-by-data-transfer billing method.

Parameter	Description
IPsec-VPN	Specify whether to enable IPsec-VPN for the VPN gateway. After IPsec-VPN is enabled, you can create IPsec-VPN connections between an on-premises data center and a VPC network, or between two VPC networks.
SSL-VPN	Specify whether to enable SSL-VPN. SSL-VPN connections are point-to-site connections. SSL-VPN allows you to connect a client to Alibaba Cloud without configuring a gateway for the client.
SSL Connections	Specify the maximum number of concurrent SSL connections that the VPN gateway supports. <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #d9e1f2;">? Note This parameter is available only after SSL-VPN is enabled.</div>
Billing Cycle	Specify the subscription duration. VPN gateways support only the pay-by-hour billing method.



2.2. Modify a VPN Gateway

This topic describes how to modify a VPN Gateway. After you create a VPN Gateway, you can modify the name and description of the VPN Gateway.

Prerequisites

A VPN Gateway is created. For more information, see [Create a VPN gateway](#).

Procedure

1. Log on to the [VPC console](#).
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. Select the region of the target VPN Gateway.
4. On the **VPN Gateways** page, find the target VPN Gateway and click the  icon in the **Instance ID/Name** column to modify the instance name. The name must be 2 to 100 characters in length and can contain numbers, underscores (_) or hyphens (-). The name must start with a letter.
5. Click the  icon in the **Description** column to modify the description. The description must be 2 to 256 characters in length and cannot start with http:// or https://.

2.3. Configure routes of a VPN Gateway

2.3.1. VPN Gateway route overview

After you create an IPsec-VPN connection, you must manually add a VPN Gateway route.

The route-based IPsec-VPN enables you to easily configure and maintain VPN policies, and provides flexible ways for routing traffic.

You can add the following two types of routes for a VPN Gateway:

- Policy-based routes.
- Destination-based routes.

Policy-based route

If a policy-based route is used, traffic is forwarded based on both the source IP address and the destination IP address.

For more information, see [Add policy-based routes](#).

 **Note** Policy-based routes take precedence over destination-based routes.

Destination-based route

If a destination-based route is used, traffic is forwarded based only on the destination IP address.

For more information, see [Add Destination-based routes](#).



2.3.2. Add a policy-based route entry

This topic describes how to add a policy-based route entry after an IPsec-VPN connection is created. Policy-based routing (PBR) is a technique that routes packets based on source and destination IP addresses.

Procedure

1. Log on to the [VPN gateway console](#).
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. Select the region where the VPN gateway is deployed.
4. On the **VPN Gateways** page, find the target VPN gateway and click the instance ID in the **Instance ID/Name** column.
5. Click the **Policy-based Routing** tab, and then click **Add Route Entry**.
6. In the **Add Route Entry** dialog box, set the following parameters and click **OK**.

Parameter	Description
Destination CIDR Block	The CIDR block that you want to access.
Source CIDR Block	The CIDR block of the VPC network.
Next Hop Type	Select IPsec Connection.

Parameter	Description
Next Hop	Select an IPsec instance to create an IPsec-VPN connection.
Publish to VPC	<p>Specify whether to automatically publish new route entries to the VPC route table.</p> <ul style="list-style-type: none"> Yes (Recommended): automatically publishes new route entries to the VPC route table. No: does not automatically publish new route entries to the VPC route table. <p> Note If you select No, you must manually publish new route entries to the VPC route table.</p>
Weight	<p>Select a weight. Valid values:</p> <ul style="list-style-type: none"> 100: indicates that the priority of the route entry is high. 0: indicates that the priority of the route entry is low. <p> Note If two policy-based route entries are configured with the same destination CIDR block, you cannot set the weights of both route entries to 100.</p>



2.3.3. Add a destination-based route

This topic describes how to add a destination-based route. After you add a destination-based route, you can forward traffic by using the specified destination IP address.

Procedure


- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > VPN Gateways**.
4. Select the region where the VPN gateway is deployed.
5. On the **VPN Gateways** page, find the target VPN gateway and click the instance ID in the **Instance ID/Name** column.
6. On the **Destination-based Routing** tab, click **Add Route Entry**.
7. On the **Add Route Entry** page, configure a destination-based route, and then click **OK**. The following table describes the parameters.

Configuration	Description
Destination CIDR Block	Enter the private CIDR block to be accessed.
Next Hop Type	Select IPsec Connection.

Configuration	Description
Next Hop	Select the target IPsec-VPN connection instance.
Publish to VPC	<p>Select whether to publish the new route entry to the VPC route table.</p> <ul style="list-style-type: none"> ◦ Yes (Recommended): Publish the new route entry to the VPC route table. ◦ No: Do not publish the new route entry to the VPC route table. <p> Note If you select No, you must also publish the route entry in the destination-based route table after you add the destination-based route.</p>
Weight	<p>Select a weight. Valid values:</p> <ul style="list-style-type: none"> ◦ 100: high priority ◦ 0: low priority <p> Note Destination-based routes with the same destination CIDR block cannot be configured with a weight of 100 at the same time.</p>

2.4. Enable IPsec-VPN and SSL-VPN

This topic describes how to enable the SSL-VPN and IPsec-VPN functions. You can enable SSL-VPN and IPsec-VPN when you create a VPN Gateway or after you create it.

 **Note** If you want to enable SSL-VPN for a VPN Gateway created before January 20, 2018, you need to open a ticket. For a VPN Gateway created after January 20, 2018, you can enable the SSL-VPN function in the console directly.

Enable IPsec-VPN

To enable IPsec-VPN, follow these steps:

1. Log on to the [VPC console](#).
2. In the left-side navigation pane, choose **VPN > VPN Gateways**.
3. Select the region of the target VPN Gateway.
4. On the **VPN Gateways** page, find the target VPN Gateway and click **Enable IPsec after IPsec** in the **Gateway Status** column.
5. On the purchase page, complete the payment.

Enable SSL-VPN

To enable SSL-VPN, follow these steps:

1. Log on to the [VPC console](#).

2. Log on to the [VPC console](#).
3. In the left-side navigation pane, choose **VPN > VPN Gateways**.
4. Select the region of the target VPN Gateway.
5. On the **VPN Gateways** page, find the target VPN Gateway and click **Enable SSL after SSL** in the **Gateway Status** column.
6. On the purchase page, complete the payment.

3. Manage a customer gateway

3.1. Create a customer gateway

When you use an IPsec-VPN connection to connect a VPC to an on-premises data center or connect two VPCs, you must 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.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, click **VPN > Customer Gateways**.
4. Select the region to which the target customer gateway belongs.

 **Note** The customer gateway and the VPN Gateway you are connecting must be in the same region.

5. On the **Customer Gateways** page, click **Create Customer Gateway**.
6. On the **Create Customer Gateway** page, configure the customer gateway according to the following information.

Configuration	Description
Name	The name of the customer gateway. The name must be 2 to 128 letters in length and can contain numbers, hyphens, or underscores. It must start with a letter.
IP Address	The static public IP address configured for the gateway device of the on-premises data center.
Description	The description of the customer gateway. The description must be 2 to 256 characters in length. It cannot begin with http:// or https://.

7. Optional. Click **+Add** to add another customer gateway.
8. Click **OK**.

3.2. Modify a customer gateway

This topic describes how to modify a customer gateway. After creating a customer gateway, you can modify the name and the description of the customer gateway.

Prerequisites

A customer gateway is created. For more information, see [Create a customer gateway](#).

Procedure

- 1.
- 2.
3. In the left-side navigation pane, click **VPN > Customer Gateways**.
4. Select the region to which the target customer gateway belongs.
5. On the **Customer Gateways** page, find the target customer gateway and click the



icon in the **Instance ID/Name** column to modify the name of the customer gateway. The name must be 2 to 100 characters in length and can contain numbers, underscores (_) or hyphens (-). The name must start with a letter.

6. Click the



icon in the **Description** column to modify the description of the customer gateway. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.

3.3. Delete a customer gateway

This topic describes how to delete a customer gateway.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, click **VPN > Customer Gateways**.
4. Select the region where the customer gateway is deployed.
5. On the **Customer Gateways** page, find the target customer gateway, and click **Delete** in the **Actions** column.
6. In the displayed dialog box, click **OK**.

4. Configure SSL-VPN

4.1. Configuration overview

This topic describes how to use the SSL-VPN function to connect a remote client to a VPC.

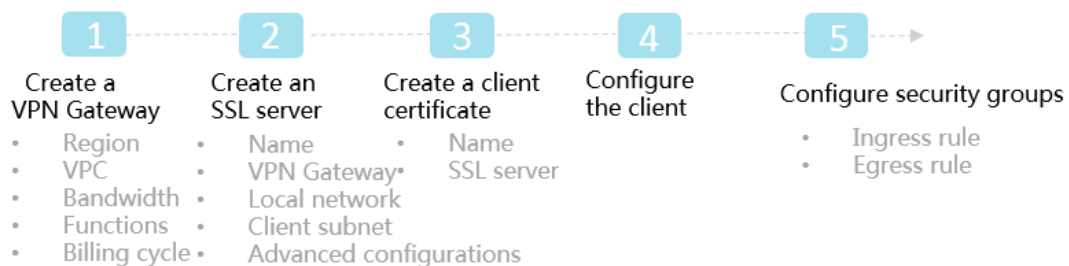
Prerequisites

The following conditions must be met before you deploy a VPN Gateway:

- The client and the VPC are not using the same private CIDR block.
- The client is able to access the Internet.

Procedure

The following figure illustrates the work flow of how to connect a client to a VPC by using the SSL-VPN function.



1. Create a VPN Gateway

Create a VPN Gateway and enable the SSL-VPN function.

2. Create an SSL server

Specify the IP address range of the SSL server and the IP address range used by the client.

3. Create a client certificate

Create the client certificate according to server configurations, and then download the client certificate and configurations.

4. Configure the client

Download and install client VPN software in the client, load the client certificate and configurations, and initiate the connection.

5. Configure security groups

Make sure that the security group rules of ECS instances in the VPC allow remote access.

4.2. Manage an SSL server

4.2.1. Create an SSL Server



This topic describes how to create an SSL server. To use the SSL-VPN to establish point-to-site connections, you must create an SSL server.


Prerequisites

You have created a VPN gateway and have SSL-VPN enabled. For more information, see [Create a VPN gateway](#).

Procedure

1. Log on to the [VPN gateway console](#).
2. In the left-side navigation pane, click **VPN > SSL Servers**.
3. On the top of the page, select the region of the SSL server.
4. On the **SSL Servers** page, click **Create SSL Server**.
5. In the **Create SSL Server** dialog box that appears, configure the SSL server according to the following information, and then click **OK**.

Parameter	Description
Name	<p>Enter a name for the SSL server.</p> <p>The name must be 2 to 128 characters in length and can contain letters, digits, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.</p>
VPN Gateway	<p>Select a VPN gateway that you want to associate with the SSL server.</p> <p>Ensure that SSL-VPN is enabled.</p>
Local Network	<p>Enter the CIDR blocks used in the connections by the client through SSL-VPN. This value can be the CIDR blocks of a VPC network, a VSwitch, an on-premises data center connected to a VPC through a leased line, or a cloud service such as ApsaraDB for RDS or Object Storage Service (OSS).</p> <p>Click +Add Local Network to add more local networks.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> Note The subnet mask of the local network must be 8-32 bits.</p> </div>
Client Subnet	<p>The CIDR blocks from which an IP address will be allocated to the virtual network interface of the client. This value is not the existing internal CIDR blocks of the client. When the client accesses the local end, the client uses the IP address allocated from the client subnet by the VPN Gateway to access the local network.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> Note The client and the local end cannot use the same CIDR block.</p> </div>
Advanced Configuration	
Protocol	The protocol used by the SSL connection. Valid values: UDP or TCP.
Port	The port used by the SSL connection. Default value: 1194.

Parameter	Description
Encryption Algorithm	The encryption algorithm used by the SSL connection. Valid values: AES-128-CBC, AES-192-CBC and AES-256-CB
Enable Compression	Enable or disable compression.
Two-factor Authentication	<p>Enable or disable two-factor authentication You must select an IDaaS instance after you enable two-factor authentication.</p> <p>By default, you can use the username and password of IDaaS for two-factor authentication. You can configure AD authentication. After you configure AD authentication, SSL-VPN can process the AD authentication feature.</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfcfcf;"> <p> Note</p> <ul style="list-style-type: none"> ◦ The VPN gateways that support two-factor authentication must be created at a time later than 00:00 on March 5, 2020. ◦ When you use the two-factor authentication for the first time, you must authorize the VPN gateway to access the IDaaS instance before you create the SSL server. </div>

Related information

- [CreateSslVpnServer](#)

4.2.2. Modify an SSL server

This topic describes how to modify an SSL server. After an SSL server is created, you can modify the name, local network, client subnet, and advanced configuration of the SSL server.

Prerequisites

An SSL server is created. For more information, see [Create an SSL server](#).

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > SSL Servers**.
4. In the top navigation bar, select the region where you want to create the SSL server.
5. On the **SSL Servers** page, find the target SSL server, and click **Edit** in the **Actions** column.
6. On the **Edit SSL Server** page, modify the name, local network, client subnet, and advanced configuration of the SSL server, and click **OK**.

4.2.3. Delete an SSL server

This topic describes how to delete an SSL server.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > SSL Servers**.
4. In the top navigation bar, select the region where you want to create the SSL server.
5. On the **SSL Servers** page, find the target SSL server and click **Delete** in the **Actions** column.
6. In the displayed dialog box, click **OK**.

4.3. Manage an SSL client certificate

4.3.1. Create an SSL client certificate

This topic describes how to create an SSL client certificate. After creating an SSL server, you need to create an SSL client certificate.

Prerequisites

An SSL server is created. For more information, see [Create an SSL Server](#).

Context

Each user can retain up to 50 SSL client certificates. To increase the quota, open a ticket.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, click **VPN > SSL Clients**.
4. Select the target region.
5. On the **SSL Clients** page, click **Create Client Certificate**.
6. On the **Create Client Certificate** page, configure the client certificate according to the following information, and click **OK**.

Configuration	Description
Name	The name of the SSL client certificate. The name must be 2 to 128 characters in length and can contain numbers, hyphens, and underscores. It must start with a letter.
SSL Server	The associated SSL server.

4.3.2. Download an SSL client certificate

This topic describes how to download an SSL client certificate. To use the SSL-VPN function, you need to load an SSL client certificate to your client. After creating an SSL client certificate, you can download the certificate.

Prerequisites

An SSL client certificate is created. For more information, see [Create an SSL client certificate](#).

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > SSL Clients**.
4. Select the region where the SSL client is deployed.
5. On the **SSL Clients** page, find the target client certificate and click **Download** in the **Actions** column.

4.3.3. Delete an SSL client certificate

This topic describes how to delete an SSL client certificate.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > SSL Clients**.
4. Select the region where the SSL client is deployed.
5. On the **SSL Clients** page, find the target SSL client certificate, and click **Delete** in the **Actions** column.
6. In the displayed dialog box, click **OK**.

4.4. Modify the number of concurrent SSL connections

You can modify the number of clients simultaneously connected to a VPN Gateway according to your business needs.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > VPN Gateways**.
4. Select the region where the VPN gateway is deployed.
5. On the **VPN Gateways** page, find the target VPN Gateway.
 - To increase the number of concurrent SSL connections, click **Upgrade** in the **Concurrent SSL Connections** column.
 - To reduce the number of concurrent SSL connections, click **Downgrade** in the **Concurrent SSL Connections** column.
6. On the **Configuration Upgrade** area, select a new number of SSL connections and complete the payment.

5. Configure IPsec-VPN connections

5.1. Configuration 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:

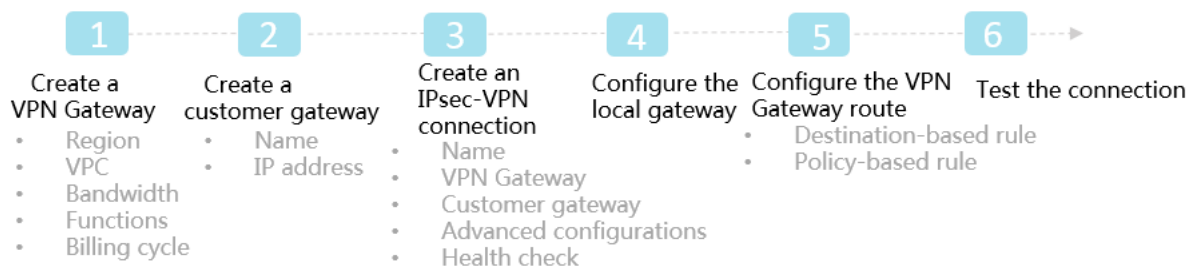
- The protocols IKEv1 and IKEv2 are supported by the gateway device of the on-premises data center.

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](#).

5.2. Manage an IPsec-VPN connection


5.2.1. Create an IPsec-VPN connection

This topic describes how to create an IPsec-VPN connection. After you create a VPN Gateway and a customer gateway, you can create an IPsec-VPN connection to establish an encrypted communication tunnel.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > IPsec Connections**.
4. Select a region.
5. On the **IPsec Connections** page, click **Create IPsec Connection**.
6. On the **Create IPsec Connection** page, configure the IPsec-VPN connection according to the following information and click **OK**.

Configuration	Description
Name	Enter the name of the IPsec-VPN connection. The name must be 2 to 128 characters in length and can contain letters, numbers, hyphens, or underscores. It must start with a letter.
VPN Gateway	Select the VPN Gateway to connect.
Customer Gateway	Select the customer gateway to connect.
Local Network	Enter the CIDR block of the VPC to be connected with the on-premises data center. This parameter is used for phase two negotiation.
+ Add Local Network	Add multiple CIDR blocks of the VPC to be connected with the on-premises data center. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> ? Note If multiple CIDR blocks are entered, the IKEv2 version must be selected. </div>

Configuration	Description
Remote Network	Enter the CIDR block of the on-premises data center to be connected with the VPC. This parameter is used for phase two negotiation.
+ Add Remote Network	<p>Add multiple CIDR blocks of the on-premises data center to be connected with the VPC.</p> <div style="border: 1px solid #ccc; background-color: #e0f2f1; padding: 5px; margin-top: 10px;"> <p> Note If multiple CIDR blocks are entered, the IKEv2 version must be selected.</p> </div>
Effective Immediately	<p>Indicates whether the IPsec-VPN connection takes effect immediately.</p> <ul style="list-style-type: none"> ◦ Yes: Start the negotiation immediately once the configuration is complete. ◦ No: Start the negotiation only when traffic is detected in the tunnel.
Advanced Configuration: IKE Configurations	
Pre-Shared Key	Enter the pre-shared key used for the authentication between the VPN Gateway and the customer gateway. By default, it is an automatically generated value. But you can also specify a pre-shared key.
Version	Select the IKE version to use. Compared with IKEv1, IKEv2 simplifies the SA negotiation process and provides better support for multiple-CIDR-block scenarios. We recommend that you select the IKE V2 protocol.
Negotiation Mode	<p>Select the negotiation mode of the IKEv1.</p> <ul style="list-style-type: none"> ◦ Main mode: The negotiation process features high security. ◦ Aggressive mode: The negotiation is fast and the success rate of negotiation is high. <p>After the negotiation succeeds, the information transmission security is the same for the two modes.</p>
Encryption Algorithm	Select an encryption algorithm used by phase one negotiation. Valid values: aes, aes192, aes256, des, 3des.
Encryption Algorithm	Select an authentication algorithm used by phase one negotiation. Valid values: sha1, md5, sha256, sha384, sha512.
DH Group	Select a Diffie-Hellman key exchange algorithm used by phase one negotiation.
SA Life Cycle (seconds)	Set the SA lifecycle for phase one negotiation. The default value is 86,400 seconds.
LocalId	It is the identification of the VPN Gateway used for phase one negotiation. The default value is the public IP address of the VPN Gateway. If you set the LocalId in the FQDN format, we recommend that you change the negotiation mode to the aggressive mode.

Configuration	Description
Remoteld	It is the identification of the customer gateway used for the first-stage negotiation. The default value is the public IP address of the customer gateway. If you set the Remoteld in the FQDN format, we recommend that you change the negotiation mode to the aggressive mode.
Advanced Configuration: IPsec Configurations	
Encryption Algorithm	Select the encryption algorithm of phase two negotiation. Valid values: aes, aes192, aes256, des, 3des.
Authentication Algorithm	Select an authentication algorithm used by phase two negotiation. Valid values: sha1, md5, sha256, sha384, sha512.
DH Group	Select a Diffie-Hellman key exchange algorithm used by phase two negotiation. <ul style="list-style-type: none"> ◦ If you select any group that are not disabled, the PFS feature is enabled by default (perfect forward secrecy), so the key must be updated for each renegotiation and PFS must be enabled on the client. ◦ For clients that do not support PFS, select Disabled.
SA Life Cycle (seconds)	Set the SA lifecycle for phase two negotiation. Default value: 86,400s.
Health Check	
Destination IP	The IP address of the on-premises data center that the VPC can communicate with through the IPsec-VPN connection.
Source IP	The IP address of the VPC that the on-premises data center can communicate with through the IPsec-VPN connection.
Retry Interval	The length of time before a health check is retried. Unit: second.
Retry Times	The number of times to attempt sending health check packets.

5.2.2. Modify an IPsec-VPN connection

This topic describes how to modify an IPsec-VPN connection. After creating an IPsec-VPN connection, you can modify its name, advanced configuration, and health check.

Prerequisites

An IPsec-VPN connection is created. For more information, see [Create an IPsec-VPN connection](#).

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > IPsec Connections**.

4. Select the region where you want to create the IPsec-VPN connection.
5. On the **IPsec Connections** page, find the target connection and click **Edit** in the **Actions** column.
6. On the **Modify IPsec Connections** page, modify the name, advanced configuration, and health check of the IPsec-VPN connection, and then click **OK**.

5.2.3. Download the configuration of an IPsec-VPN connection


After the IPsec connection is configured and the negotiation succeeds, you can download the IPsec connection configuration and configure the local gateway.

Prerequisites

Make sure an IPsec-VPN connection is created. For more information, see [Create an IPsec-VPN connection](#).

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > IPsec Connections**.
4. Select the region where you want to create the IPsec-VPN connection.
5. On the **IPsec Connections** page, find the target IPsec-VPN connection, and click **Download Configuration** in the **Actions** column.

 **Note** The RemoteSubnet and LocalSubnet in the downloaded configuration are opposite to the local network and the remote network when you create 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, whereas from the perspective of the on-premises data center, the remote network is the VPC and the local network is the on-premises data center.

5.2.4. View IPsec-VPN connection logs

This topic describes how to view the historical logs of an IPsec-VPN connection of up to the previous month. You can also analyze these logs to troubleshoot IPsec-VPN connection errors. The time range for log query is 10 minutes.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > IPsec Connections**.
4. Select the region where you want to create the IPsec-VPN connection.
5. On the **IPsec Connections** page, find the target IPsec-VPN connection, and click **View Logs** in the **Actions** column.

6. On the IPsec Connection Logs page, set the time range and view the corresponding logs.

5.2.5. Delete an IPsec-VPN connection

This topic describes how to delete an IPsec-VPN connection.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, choose **VPN > IPsec Connections**.
4. Select the region where you want to create the IPsec-VPN connection.
5. On the IPsec Connections page, find the target IPsec-VPN connection, and click **Delete** in the **Actions** column.
6. In the displayed dialog box, click **OK**.

5.3. Configure local gateways

5.3.1. Configure an IPsec-VPN connection through a USG series Next-Generation Firewall device (Huawei)

This topic describes how to configure an IPsec-VPN connection through a USG series Next-Generation Firewall device from Huawei (known as USG series Huawei device) to connect an on-premises data center. When you use IPsec-VPN to establish a site-to-site connection, you need to configure your local gateway devices after configuring Alibaba Cloud VPN Gateway.

Alibaba Cloud VPN Gateway supports the standard IKEv1 and IKEv2 protocols. Therefore, all devices that support these two protocols can connect to Alibaba Cloud VPN Gateway (such as devices from Huawei, H3C, Hillstone, Sangfor, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia).

The following sections take a USG series device from Huawei as an example to describe the network scenario and the following table describes the corresponding network configurations.

Network configuration		Example value
VPC	CIDR block of the VSwitch	192.168.10.0/24, 192.168.11.0/24
	Public IP address of the VPN Gateway	47.xx.xx.10
On-premises data center	CIDR block of the intranet	10.10.10.0/24
	Public IP address of the firewall	124.xx.xx.215/26
	Upstream Internet interface	10GE1/0/0
	Downstream intranet interface	10GE1/0/1

Note If the on-premises data center is associated with multiple CIDR blocks that need to connect with a VPC, we recommend that you create an equivalent number of IPsec-VPN connections on Alibaba Cloud so that each CIDR block of the on-premises data center is connected with a VPC CIDR block.

Configure an IKEv1 VPN

Prerequisites

- An IPsec-VPN connection is created in an Alibaba Cloud VPC. For more information, see [Create an IPsec-VPN connection](#).
- The configuration of the IPsec-VPN connection is downloaded. The configurations in the following table are used in this example.

Protocol	Configuration	Example value
IKE	Authentication Algorithm	SHA-1
	Encryption Algorithm	AES-128
	DH Group	group 2
	IKE Version	IKE v1
	SA Life Cycle	86400
	Negotiation Mode	main
IPsec	PSK	123456
	Authentication Algorithm	SHA-1
	Encryption Algorithm	AES-128
	DH Group	group 2
	IKE Version	IKE v1
	SA Life Cycle	86400
	Negotiation Mode	esp

Procedure

To load customer gateway configurations to the USG series Huawei device, follow these steps:

1. Go to the Huawei firewall management page. Choose **Network > Interface > Interface List**. Add the upstream Internet interface 10GE1/0/0 to the untrust security zone and set the public IP address; add the downstream intranet interface 10GE1/0/1 to the trust security zone, and then set the private IP address.
2. Choose **Policy > Security Policy > Add** to create a security policy.
3. Choose **Network > IPsec > IPsec Policy List > Add**. Configure the peer site according to the following information:

- **Local Interface:** Select the upstream Internet interface. In this example, select 10GE1/0/0.
 - **Peer Address:** Enter the public IP address of the VPN Gateway. In this example, enter 47.xx.xx.10.
 - **Pre-Shared Key:** The pre-shared key is the same as the PSK at the Alibaba Cloud side. In this example, enter 123456.
4. On the **Data Flow to Be Encrypted** page, click **Add**. Add the data flow to be encrypted for all VSwitch CIDR blocks in the VPC according to the following information:
 - **Source Address/Address-Set:** Enter the private IP address segment of the on-premises data center. In this example, enter 10.10.10.0/24.
 - **Destination Address/Address-Set:** Enter the VSwitch IP address segment of the VPC. In this example, enter 192.168.10.0/24 and 192.168.11.0/24.
 5. On the **IKE/IPsec Protocol** page, click **Advanced**. Configure IKE protocol parameters based on the IPsec-VPN connection configurations that you downloaded.
 6. On the **IPsec Parameters** page, configure the IPsec protocol parameters based on the IPsec connection configurations that you downloaded.
 7. Choose **Network > Route > Static Route > Static Route List > Add** to configure static routes for the firewall. When you add a default route, the next hop is the public IP address of the firewall. When you add a route to the VPC, the next hop is the public IP address of the VPN Gateway.

Configure an IKEv2 VPN

Prerequisites

- An IPsec-VPN connection is created in the Alibaba Cloud VPC.
- The configuration of the IPsec-VPN connection is downloaded. The configurations in the following table are used in this example.

Protocol	Configuration	Example value
IKE	Authentication Algorithm	SHA-1
	Encryption Algorithm	AES-128
	DH Group	group 2
	IKE Version	IKE v2
	SA Life Cycle	86400
	PRF Algorithm	SHA-1
	PSK	123456
	Authentication Algorithm	SHA-1
	Encryption Algorithm	AES-128
	DH Group	group 2

IPsec Protocol	Configuration	Example value
	IKE Version	Ike v2
	SA Life Cycle	86400
	Negotiation Mode	esp

Procedure

To load customer gateway configurations to USG series Huawei device, follow these steps:

- Go to the Huawei firewall management page. Choose **Network > Interface > Interface List**. Add the upstream Internet interface 10GE1/0/0 to the untrust security zone and set the public IP address; add the downstream intranet interface 10GE1/0/1 to the trust security zone, and then set the private IP address.
- Choose **Policy > Security Policy > Add** to create a security policy.
- Choose **Network > IPsec > IPsec Policy List > Add**. Configure the peer site according to the following information:
 - Local Interface:** Select the firewall upstream Internet interface. In this example, select 10GE1/0/0.
 - Peer Address:** Enter the public IP address of the Alibaba Cloud VPN Gateway. In this example, enter 47.xx.xx. 10.
 - Pre-Shared Key:** The pre-shared key is the same as the PSK at the Alibaba Cloud side. In this example, enter 123456.
- On the **Data Flow to Be Encrypted** page, click **Add**. Add the data flow to be encrypted for all VSwitch CIDR blocks in the VPC according to the following information:
 - Source Address/Address-Set:** Enter the private IP address segment of the on-premises data center. In this example, enter 10.10.10.0/24.
 - Destination Address/Address-Set:** Enter the VSwitch IP address segment of the VPC. In this example, enter 192.168.10.0/24 and 192.168.11.0/24.
- On the **IKE/IPSec Protocol** page, click **Advanced**. Configure IKE parameters based on the IPsec-VPN connection configurations that you downloaded.
- On the **IPsec Parameters** page, configure the IPsec protocol parameters based on the IPsec connection that you downloaded.
- Choose **Network > Route > Static Route > Static Route List > Add** to configure static routes for the firewall. Among them, when you add a default route, the next one is the public network IP of the firewall; when adding a route to a VPC, jump to the public IP of the VPN gateway.

5.3.2. Configure H3C firewall

When using IPsec-VPN to create a site-to-site connection, you must configure the local gateway according to the IPsec connection configured for the Alibaba Cloud VPN Gateway. This document takes H3C firewall as an example to show how to configure the VPN settings.

Prerequisites

- Make sure you have configured IPsec connections. For more information, see [Establish a connection between a VPC and an on-premises data center](#).
- After you create an IPsec-VPN connection, download the configurations of the IPsec-VPN connection. For more information, see [Create an IPsec-VPN connection](#).

In this tutorial, the configurations of the IPsec-VPN connection are as follows:

○ IPsec-VPN configuration

Configurations		Value
IKE	Authentication Algorithm	sha1
	Encryption Algorithm	aes
	DH Group	group2
	IKE Version	ikev1
	SA Life Cycle (seconds)	86400
	Negotiation Mode	main
	PSK	h3c
IPsec	Authentication Algorithm	sha1
	Encryption Algorithm	aes
	DH Group	group2
	IKE Version	ikev1
	SA Life Cycle (seconds)	86400

○ Network configurations

Configuration		Value
VPC	Private CIDR block	192.168.10.0/24
	Public IP address of VPN Gateway	101.xxx.xxx.127
On-premises data center	Private CIDR block	192.168.66.0/24
	Public IP address of local gateway	122.xxx.xxx.248
	Uplink public port	Reth 1
	Downlink private port	G 2/0/10

Procedure

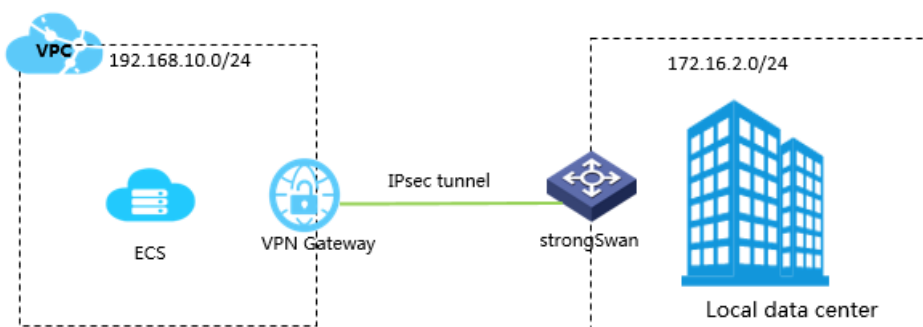
1. Log on to the firewall Web page and choose **Network > VPN > IPsec > Policy**.
2. Configure the H3C firewall IPsec policy based on the IPsec configurations of the Alibaba Cloud VPN Gateway. Click **Add** in the **Protected Data Stream** list, set the IP address range of the on-premises data center as the source IP address and the IP address range of the VPC as the destination IP address.
3. Choose **IKE Proposal > Create**. Configure the IKE proposal according to the IKE configurations of the Alibaba Cloud VPN Gateway.
4. Choose **Network > VPN > IPsec > Policy**.
5. Select the new IPsec policy and click **Advanced Configuration**.
Configure the IPsec protocol according to the information of the IPsec connection configured for the Alibaba Cloud VPN Gateway.
6. Choose **Policy > Security Policy > Create** to create the uplink security policy and downlink security policy.
7. Choose **Network > Route > Static Route**.
8. Add the default route, set the uplink interface as the next hop of the outbound traffic. In this tutorial, no configuration is required.

5.3.3. Configure strongSwan

When using IPsec-VPN to create a site-to-site connection, you must configure the local gateway according to the IPsec connection configured for the Alibaba Cloud VPN gateway. This article takes strongswan as an example to show you how to load a VPN configuration in a local site.

This document takes strongSwan as an example to show how to configure the VPN settings. The configurations used in this tutorial are as follows:

- The IP address range of the Alibaba Cloud VPC is 192.168.10.0/24.
- The IP address range of the local data center is 172.16.2.0/24.
- The public IP of strongSwan is 59.110.165.70.



Prerequisites

- Make sure you have configured IPsec connections. For more information, see [Establish a connection between a VPC and an on-premises data center](#).
- After you create an IPsec connection, download the configurations of the created IPsec connection. For more information, see [Create an IPsec-VPN connection](#).

Install strongSwan

1. Run the following command to install strongSwan.

```
# yum install strongSwan
```

2. Run the following to view the installed software version.

```
# strongswan version
```

Configure strongSwan

1. Run the following command to open the *ipsec.conf* file.

```
# vi /etc/strongswan/ipsec.conf
```

2. Refer to the following configurations to update the *ipsec.conf* file.

```
# ipsec.conf - strongSwan IPsec configuration file
# basic configuration
config setup
    uniqueids=never
conn %default
    authby=psk
    type=tunnel
conn tomyidc
    keyexchange=ikev1
    left=59.110.165.70
    leftsubnet=172.16.2.0/24
    leftid=59.110.165.70 (Public IP of the loca gateway)
    right=119.23.227.125
    rightsubnet=192.168.10.0/24
    rightid=119.23.227.125 (Public IP of the VPN Gateway)
    auto=route
    ike=aes-sha1-modp1024
    ikelifetime=86400s
    esp=aes-sha1-modp1024
    lifetime=86400s
    type=tunnel
```

3. Configure the *ipsec.secrets* file.

- i. Run the following command to open the configuration file.

```
# vi /etc/strongswan/ipsec.secrets
```

- ii. Add the following configuration.

```
59.110.165.70 119.23.227.125 : PSK yourpassword
```

4. Enable system forwarding.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

For more configuration examples for different scenarios, see [Configuration examples for different scenarios](#).

5. Run the following command to start the strongSwan service.

```
# systemctl enable strongswan
# systemctl start strongswan
```

6. Configure two routings in strongSwan. One is used to route the requests destined for the IDC client to strongSwan. The other one is used to route the requests destined for strongSwan to your IDC client.

5.3.4. Configure an IPsec-VPN connection through an SRX series Services Gateway firewall device from Juniper

This topic takes an SRX series Services Gateway firewall device from Juniper as an example to show how to configure the VPN settings to connect an on-premises data center to Alibaba Cloud VPC. When using IPsec-VPN to create a site-to-site connection, you must configure the local gateway according to the IPsec-VPN connection configured for the Alibaba Cloud VPN Gateway.

Prerequisites

- An IPsec-VPN connection is created in an Alibaba Cloud VPC. For more information, see [Create an IPsec-VPN connection](#).
- The configuration of the IPsec-VPN connection is downloaded. For more information, see [Download the configuration of an IPsec-VPN connection](#).

The IPsec-VPN connection configurations in the following table are used in this example.

o IPsec protocol

Configuration		Example value
IKE	Authentication Algorithm	md5
	Encryption Algorithm	3des
	DH Group	group2
	IKE Version	IKE v1
	SA Life Cycle	86400
	Negotiation Mode	main
	PSK	123456
IPsec	Authentication Algorithm	md5
	Encryption Algorithm	des
	DH Group	group2
	IKE Version	IKE v1
	SA Life Cycle	28800

o Network configurations

Network configuration		Example value
VPC	CIDR block of the VSwitch	192.168.1.0/24
	Public IP address of the gateway	47.xxx.xxx.56
On-premises data center	CIDR block of the intranet	192.168.18.0/24
	Public IP address of the gateway	122.xxx.xxx.248

Procedure

To load customer gateway configurations to the Juniper firewall device, follow these steps:

1. Log on to the CLI of the firewall device.
2. Configure the basic network, security zone, and address book.

```
set security zones security-zone trust address-book address net-cfgr_192-168-18-0--24 192.168.18
.0/24
set security zones security-zone vpn address-book address net-cfgr_192-168-1-0--24 192.168.1.0/
24
```

3. Configure IKE policies.

```
set security ike policy ike-policy-cfgr mode main
set security ike policy ike-policy-cfgr pre-shared-key ascii-text "123456"
```

4. Configure the IKE gateway, outbound interface, and protocol version.

```
set security ike gateway ike-gate-cfgr ike-policy ike-policy-cfgr
set security ike gateway ike-gate-cfgr address 47.xxx.xxx.56
set security ike gateway ike-gate-cfgr external-interface ge-0/0/3
set security ike gateway ike-gate-cfgr version v1-only
```

5. Configure IPsec policies.

```
set security ipsec policy ipsec-policy-cfgr proposal-set standard
```

6. Apply IPsec policies.

```
set security ipsec vpn ipsec-vpn-cfgr ike gateway ike-gate-cfgr
set security ipsec vpn ipsec-vpn-cfgr ike ipsec-policy ipsec-policy-cfgr
set security ipsec vpn ipsec-vpn-cfgr bind-interface st0.0
set security ipsec vpn ipsec-vpn-cfgr establish-tunnels immediately
set security ipsec policy ipsec-policy-cfgr perfect-forward-secrecy keys group2
```

7. Configure outbound policies.

```
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr match source-address net-
cfgr_192-168-18-0--24
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr match destination-address
net-cfgr_192-168-1-0--24
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr match application any
set security policies from-zone trust to-zone vpn policy trust-vpn-cfgr then permit
```

8. Configure inbound policies.


```
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr match source-address net-
cfgr_192-168-1-0--24
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr match destination-address
net-cfgr_192-168-18-0--24
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr match application any
set security policies from-zone vpn to-zone trust policy vpn-trust-cfgr then permit
```

5.3.5. Configure an IPsec-VPN connection through a Next-Generation Firewall (NGFW) device (Cisco)

This topic takes a Next-Generation Firewall (NGFW) device from Cisco as an example to show how to configure the VPN settings to connect an on-premises data center to Alibaba Cloud VPC. When using IPsec-VPN to create a site-to-site connection, you must configure the local gateway according to the IPsec-VPN connection configured for the Alibaba Cloud VPN Gateway.

The following table lists the network configurations of the VPC and the on-premises data center used in this example.

Configuration		Example value
VPC	VSwitch CIDR block	192.168.10.0/24, 192.168.11.0/24
	Public IP address of the gateway	47. xxx. xxx.161
On-premises data center	Intranet CIDR block	10.10.10.0/24
	Public IP address of the firewall	124. xxx. xxx.171

 **Note** If the on-premises data center is associated with multiple CIDR blocks that need to connect with a VPC, we recommend that you create an equivalent number of IPsec-VPN connections on Alibaba Cloud so that each CIDR block of the on-premises data center is connected with a VPC CIDR block.

Configure an IKEv1 VPN

Prerequisites

- An IPsec-VPN connection is created in an Alibaba Cloud VPC. For more information, see [Create an IPsec-VPN connection](#).
- The configuration of the IPsec-VPN connection is downloaded. For more information, see [Download the configuration of an IPsec-VPN connection](#). The configurations in the following table are used in this example.

Protocol	Configuration	Example value
IKE	Authentication Algorithm	SHA-1
	Encryption Algorithm	AES-128
	DH Group	group 2
	IKE Version	IKE v1
	SA Life Cycle	86400
	Negotiation Mode	main
	PSK	123456
	Authentication Algorithm	SHA-1

Protocol	Configuration	Example value
IPsec	Authentication Algorithm	AES-128
	DH Group	group 2
	IKE Version	IKE v1
	SA Life Cycle	86400
	Negotiation Mode	esp

Procedure

To load customer gateway configurations to the NGFW device from Cisco, follow these steps:

1. Log on to the CLI of the NGFW device.
2. Configure the isakmp policy.

```
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. Configure the pre-shared key.

```
crypto isakmp key 123456 address 47.xxx.xxx. 161
```

4. Configure the IPsec protocol.

```
crypto ipsec transform-set ipsecpro64 esp-aes esp-sha-hmac
mode tunnel
```

5. Configure the Access Control List (ACL) and define the data flow to be protected.

 **Note** If multiple CIDR blocks are configured in the local gateway device, you need to add ACL policies for each CIDR block.

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

6. Configure IPsec policies.

```
crypto map ipsecpro64 10 ipsec-isakmp
set peer 47.xxx.xxx. 161
set transform-set ipsecpro64
set pfs group2
match address 100
```

7. Apply IPsec policies.

```
interface g0/0
crypto map ipsecpro64
```

8. Configure static routes.

```
ip route 192.168.10.0 255.255.255.0 47.xxx.xxx. 161
ip route 192.168.20.0 255.255.255.0 47.xxx.xxx. 161
```

9. Test the connectivity.

You can perform a connectivity test by using a host in Alibaba Cloud that is connected to a host in your on-premises data center.

Configure an IKEv2 VPN

Prerequisites

- An IPsec-VPN connection is created in an Alibaba Cloud VPC. For more information, see [Create an IPsec-VPN connection](#).
- The configurations of the IPsec-VPN connection are downloaded. For more information, see [Download the configuration of an IPsec-VPN connection](#). The configurations in the following table are used in this example.

Protocol	Configuration	Example value
IKE	Authentication Algorithm	SHA-1
	Encryption Algorithm	AES-128
	DH Group	group 2
	IKE Version	IKE v2
	SA Life Cycle	86400
	PRF Algorithm	SHA-1
	PSK	123456
	Authentication Algorithm	SHA-1
	Encryption Algorithm	AES-128
	DH Group	group 2

IPsec Protocol	Configuration	Example value
	IKE Version	IKE v2
	SA Life Cycle	86400
	Negotiation Mode	esp

Procedure

To load customer gateway configurations to the NGFW device from Cisco, follow these steps:

1. Log on to the CLI of the NGFW device.
2. Configure the phase one IKE algorithm.

```
crypto ikev2 proposal daemon
encryption aes-cbc-128
integrity sha1
group 2
```

3. Configure IKE v2 policies and apply the proposal.

```
crypto ikev2 policy ipsecpro64_v2
proposal daemon
```

4. Configure the pre-shared key.

```
crypto ikev2 keyring ipsecpro64_v2
peer vpngw
address 47.xxx.xxx. 161
pre-shared-key 0 123456
```

5. Configure the identity authentication.

```
crypto ikev2 profile ipsecpro64_v2
match identity remote address 47.xxx.xxx. 161 255.255.255.255
identity local address 10.10.10.1
authentication remote pre-share
authentication local pre-share
keyring local ipsecpro64_v2
```

6. Configure the IPsec security protocol.

```
crypto ipsec transform-set ipsecpro64_v2 esp-aes esp-sha-hmac
mode tunnel
```

7. Configure the ACL (access control list) and define the data stream to be protected.

Note If multiple CIDR blocks are configured in the local gateway device, you need to add ACL policies for each CIDR block.

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

8. Configure IPsec policies.

```
crypto map ipsecpro64_v2 10 ipsec-isakmp
set peer 47.xxx.xxx. 161
set transform-set ipsecpro64_v2
set ikev2-profile ipsecpro64_v2
match address 100
```

9. Apply IPsec policies.

```
interface g0/1
crypto map ipsecpro64_v2
```

10. Configure static routes.

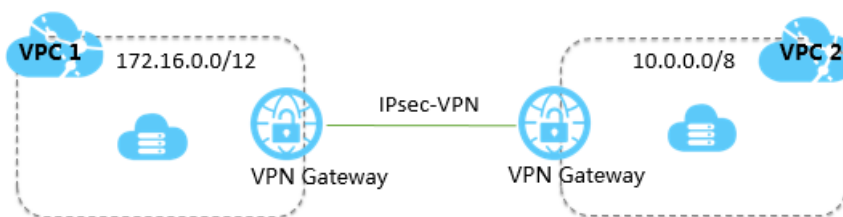
```
ip route 192.168.10.0 255.255.255.0 47.xxx.xxx. 161
ip route 192.168.20.0 255.255.255.0 47.xxx.xxx. 161
```

11. Test the connectivity.

You can perform a connectivity test by using a host in Alibaba Cloud that is connected to a host in your on-premises data center.


5.4. Establish a connection between two VPCs

This topic describes how to create an IPsec-VPN connection to connect two VPCs.



Two VPCs under the same account (labeled VPC1 and VPC2) are used as an example in this topic. The procedure of connecting two VPCs under different accounts is the same as that of connecting two VPCs under the same account. The only difference is that if you want to connect a VPC with another VPC that is under a different account, you must obtain the public IP address of the peer VPN Gateway and use this IP address to create a customer gateway.

VPC name	VPC CIDR block	VPC ID	ECS instance name
VPC1	172.16.0.0/12	vpc-xxxxz0	ECS1
VPC2	10.0.0.0/8	vpc-xxxxut	ECS2

 **Note** VPN Gateway enables communication by creating an encrypted tunnel over the Internet, which means the communication performance depends on the quality of the Internet connection. If you have high requirements regarding the communication quality, you can use Cloud Enterprise Network (CEN). For more information, see [CEN network planning](#).


Before you begin

Make sure the IP address ranges of the two VPCs 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**.
 - o **Name:** Enter a name for the VPN Gateway.
 - o **Region:** Select a region for the VPN Gateway.

 **Note** Make sure that the VPC and the VPN Gateway are in the same region.

- o **VPC:** Select the VPC to be connected.
- o **Peak Bandwidth:** Select a peak bandwidth. The bandwidth is the Internet bandwidth of the VPN Gateway.
- o **IPsec-VPN:** Select whether to enable the IPsec-VPN feature.
- o **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.
- o **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.

- o **Billing Cycle:** Select a billing cycle.
5. Repeat the preceding steps to create a VPN Gateway for the other VPC.

The status of the newly created VPN gateway is in preparation and will change to Normal in approximately two minutes. When it changes to Normal, it indicates that the VPN Gateway is ready for use. When the VPN gateway is created, the system automatically assigns two public IP addresses.

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

Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Enable IPsec	Enable SSL	Concurrent SSL Connections	Description	Actions
vpn-878-xxxxxqu vpn2	47.13		vpc-bp1tmsmbx 8edvypwhs1h webVPC	Normal	10Mbps Modify Configuration	Billing by Traffic Usage 01/25/2018, 14:41:45 Created	Enabled	Enable SSL	-	-	Delete
vpn-477k-xxxxxny 47kq	47.47		vpc-bp1tmsmbx 8edvypwhs1h webVPC	Normal	10Mbps Modify Configuration	Billing by Traffic Usage 02/11/2018, 17:53:25 Created	Enabled	Enabled	5	Modify Configuration	Delete

In this example, the public IP addresses assigned are 121.XXX.XX.143 and 118.XXX.XX.149, as shown in the following table.

VPC	VPN Gateway	IP address
Name: VPC1 ID: vpc-xxxxz0 IP address range: 172.16.0.0/12	vpn-xxxxxqwj	118.xxx.xx.149
Name: VPC2 ID: vpc-xxxxut IP address range: 10.0.0.0/8	vpn-xxxxxl5z	121.xxx.xx.143

Step 2: Create two customer gateways

To create a customer gateway, follow these steps:

1. In the left-side navigation pane, choose **VPN > Customer Gateways**.
2. Select the region in which you want to create a customer gateway.
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**.
 - o **Name:** Enter a name for the customer gateway.
 - o **IP Address:** Enter the public IP address of the local gateway.
 - o **Description:** Enter a description for the customer gateway.
5. Repeat the preceding steps to create another customer gateway by using the public IP address of the other VPN Gateway.

After creating two customer Gateways, the relationship among VPCs, VPN Gateways, and customer gateways is as follows:

VPC	VPN Gateway	IP address	Customer Gateway
Name: VPC1 ID: vpc-xxxxz0 IP address range: 172.16.0.0/12	vpn-xxxxxqwj	121.xxx.xx.143	user_VPC1
Name: PC2 ID: vpc-xxxxt IP address range: 10.0.0.0/8	vpn-xxxxxl5z	118.xxx.xx.149	user_VPC

Step 3: Create two IPsec-VPN connections

After creating the VPN Gateways and the customer gateways, you must create two IPsec-VPN connections to build the VPN channels:

1. In the left-side navigation pane, choose **VPN > IPsec Connections**.
2. Select the region in which you want to create an IPsec connection.
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 connection.
 - **VPN Gateway:** Select the created VPN Gateway. In this example, select the VPN Gateway `vpn-xxxxxqwj` of VPC1.
 - **Customer Gateway:** Select the created customer gateway. In this example, select the customer gateway `user_VPC2` of VPC2.
 - **Local Network:** Enter the CIDR block of the VPC to which the selected VPN Gateway belongs. In this example, enter the CIDR block `172.16.0.0/12` of VPC1.
 - **Remote Network:** Enter the CIDR block of the peer VPC. In this example, enter the CIDR block `10.0.0.0/8` of VPC2.
 - **Effective Immediately:** Select whether to start the negotiation immediately.
 - **Yes:** Start the negotiation immediately once the configuration is complete.
 - **No:** Start the negotiation only when traffic is detected in the tunnel.
 - **Pre-Shared Key:** Enter a pre-shared key. In this example, enter `1234567`. This value must be the same as that configured in the other IPsec-VPN connection.
 - **Health Check:** Enable health checks and enter the destination IP address, source IP address, retry interval, and number of retries.
Use the default settings for other parameters.
5. Repeat the preceding steps to create an IPsec-VPN connection for the other VPC.

Step 4: Configure a route for each VPN Gateway

To configure a route for a VPN Gateway, follow these steps:

1. In the left-side navigation pane, choose **VPN > VPN Gateways**.
2. Select the region to which the target VPN Gateway belongs.
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 the destination-based route according to the following information and click **OK**.
 - **Destination CIDR Block:** Enter the private CIDR block of VPC2.
 - **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 example, select **100**.
6. Repeat the preceding steps to configure a route for the other VPN Gateway.

Step 5: Test the connection

Log on to ECS1, and then ping the private IP address of ECS2 to check whether the connection is established.

```
root@i-1234567890:~# ping 10.0.100.100
PING 10.0.182.100 (10.0.182.100) 56(84) bytes of data:
64 bytes from 10.0.100.100: icmp_seq=1 ttl=62 time=3.41 ms
64 bytes from 10.0.100.100: icmp_seq=2 ttl=62 time=2.40 ms
64 bytes from 10.0.100.100: icmp_seq=3 ttl=62 time=2.32 ms
64 bytes from 10.0.100.100: icmp_seq=4 ttl=62 time=2.43 ms
.
--- 10.0.100.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.327/2.646/3.414/0.445 ms
```

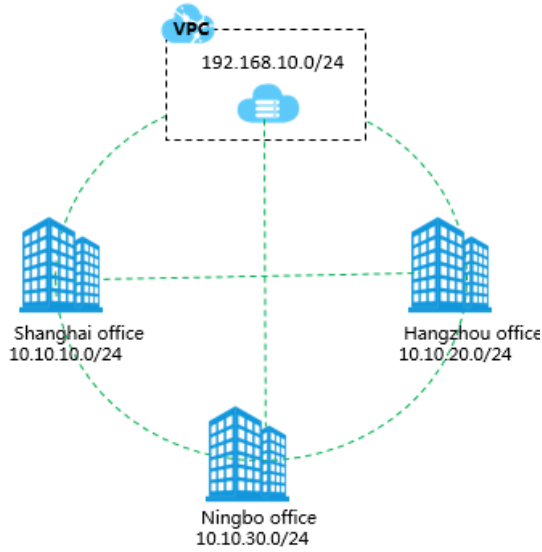
5.5. Configure multi-site connections

You can create IPsec-VPN connections between multiple sites and locations. With the VPN-Hub function, the connected sites can communicate with the connected VPC, and also communicate with each of the other sites. VPN-Hub meets the needs of large enterprises to establish intranet communications between different sites.

VPN-Hub overview

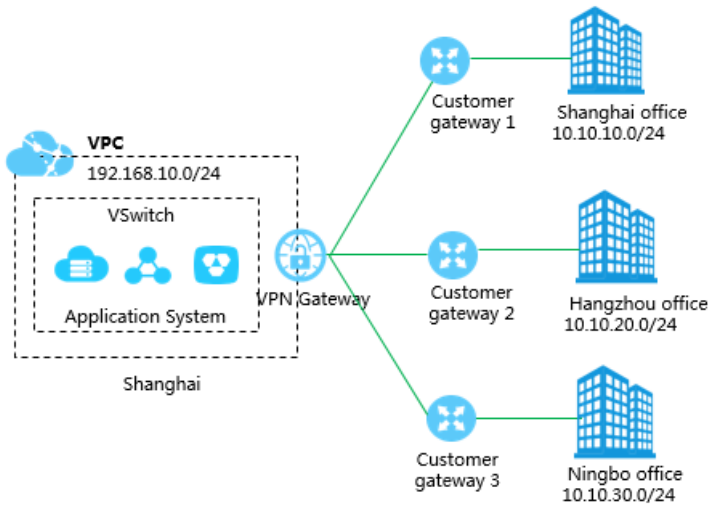
The VPN-Hub function is enabled by default. To achieve multi-site connections, you must create corresponding IPsec-VPN connections. A VPN Gateway can have up to ten IPsec-VPN connections. Therefore, you can connect up to ten office sites with one VPN Gateway.

The following scenario is used to illustrate connecting office sites in the cities of Shanghai, Hangzhou, and Ningbo. Before you begin, make sure that you have obtained the public IP address of the gateway device for each office site.



As shown in the following figure, to connect the three office sites (Shanghai, Hangzhou, and Ningbo), you only need to create a VPN Gateway and three customer gateways, and establish three IPsec-VPN connections.

Note Make sure the IP address ranges of all the connected sites do not conflict with each other.



Step 1: Create a VPN Gateway

Create a VPN Gateway in the region to which the VPC belongs. Three IPsec-VPN connections will be established for the VPN Gateway and are connected to the office sites in Shanghai, Hangzhou, and Ningbo. For more information, see [Create a VPN gateway](#).

Note Make sure that the IPsec-VPN function is enabled.

Step 2: Create an IPsec-VPN connection to the Shanghai office

1. Create a customer gateway and register the public IP address of the local gateway device to Alibaba Cloud to establish an IPsec-VPN connection.

The IP address of the customer gateway is the public IP address of the gateway device of the Shanghai office. For more information, see [Create a customer gateway](#).

2. Create an IPsec-VPN connection.

Create an IPsec connection to connect the VPN Gateway and the customer gateway. For more information, see [Create an IPsec-VPN connection](#).

3. Load VPN configurations to the gateway device of the local office site.

Load VPN configurations according to the requirements on the gateway device of the local office site. For more information, see [Local gateway configuration](#).

Step 3: Create additional IPsec-VPN connections for the other two sites

Follow the same procedures in the Step 2 to create two IPsec connections for the Hangzhou office and the Ningbo office.

Step 4: Configure the VPN Gateway route

To configure the VPN Gateway route, 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, select the region of the VPN Gateway.
4. Find the target VPN Gateway, and click the instance ID in the **Instance ID/Name** column.
5. On the **Destination-based Routing** page, click **Add Route Entry**.
6. Configure three route entries according to the following information and then click **OK**.
 - **Destination CIDR Block:** Enter the private CIDR block to be accessed.
 - **Next Hop:** Select the target IPsec-VPN connection instance.
 - **Publish to VPC:** Select whether to publish the new route to the VPC route table.
 - **Weight:** Select a weight.

The following are the destination-based routes configured in this example:

Destination CIDR Block	Next Hop	Publish to VPC	Weight
10.10.10.0/24	IPsec-VPN connection instance 1	Yes	100
10.10.20.0/24	IPsec-VPN connection instance 2	Yes	100
10.10.30.0/24	IPsec-VPN connection instance 3	Yes	100

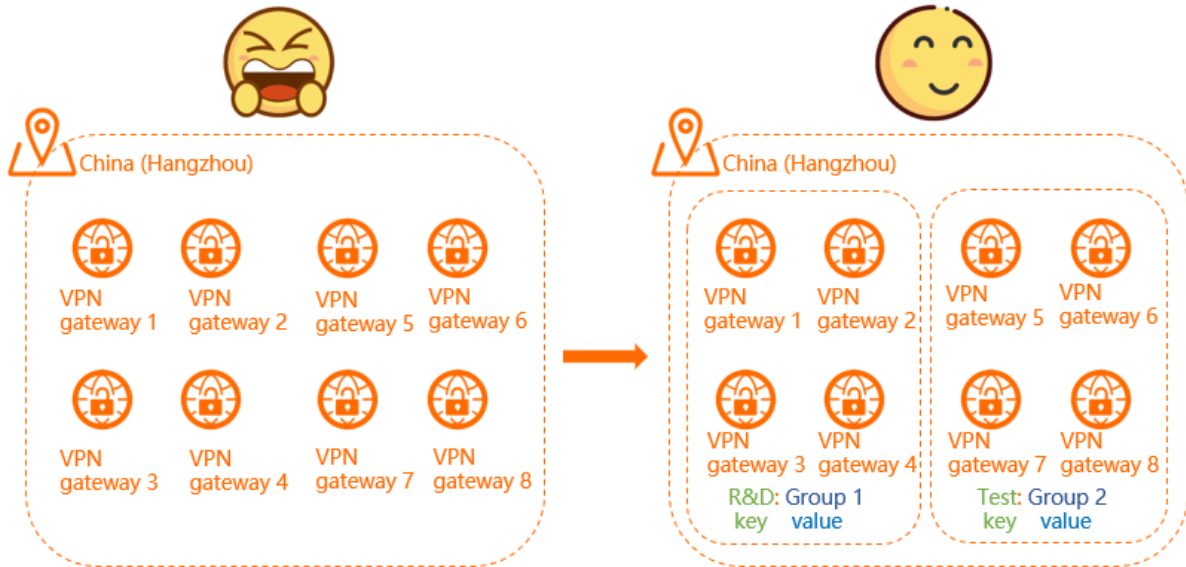
The IPsec-VPN connections to the three office sites have now been established. Each office site can now communicate with the VPC and can communicate with the other office sites over their intranet.

6.Tag management

6.1. Overview

You can label and classify VPN gateways by attaching tags to them. Using tags can help facilitate resource search and management.

Features



As shown in the preceding figure, it is difficult to manage a large number of VPN gateways. You can use tags to group VPN gateways. This allows you to search and filter VPN gateways in a more efficient way.

A tag is a label that you can attach to a VPN gateway. Each tag is composed of a key-value pair. Before you use tags to manage VPN gateways, note that:

- The keys of tags that are attached to the same VPN gateway must be unique.
- Tags must be attached to VPN gateways.
- Tag information is not shared across regions.

For example, in the China (Shanghai) region, you cannot view tags of instances that are created in the China (Hangzhou) region.

- You can modify the key and value of a tag, or remove the tag. If you delete a VPN gateway, all the tags that are attached to it are removed.

Limits

You can attach up to 20 tags to each VPN gateway. You cannot increase the quota limit.

Manage tags

The following table lists the operations that you can perform to manage tags.

Operation	Console	API
Attach tags	Attach tags to a VPN gateway	TagResources
	Attach tags to multiple VPN gateways at a time	
Search VPN gateways by tag	Search VPN gateways by tag	ListTagResources
Remove tags	Remove tags from a VPN gateway	UntagResources
	Remove tags from multiple VPN gateways at a time	

6.2. Attach tags

6.2.1. Attach tags to a VPN gateway

After you attach tags to VPN gateways, you can search and filter the VPN gateways by tag. This topic describes how to attach tags to a VPN gateway.

Context


You can attach up to 20 tags to each VPN gateway. Before you start, note that:

- The keys of tags that are attached to the same VPN gateway must be unique.
- Tags must be attached to VPN gateways.
- Tag information is not shared across regions.

For example, in the China (Shanghai) region, you cannot view tags of instances that are created in the China (Hangzhou) region.

- You can modify the key and value of a tag, or remove the tag. If you delete a VPN gateway, all the tags that are attached to it are removed.

Procedure

1. Log on to the [VPN gateway console](#).
2. In the top navigation bar, select the region where the VPN gateway is deployed.
3. On the **VPN Gateways** page, find the VPN gateway to which you want to attach tags, move the pointer over the  icon in the **Tags** column, and click **Add** in the message that appears.
4. In the **Configure Tags** dialog box, set the following parameters, and click **OK**.

Parameter	Description
Tag Key	You can select or enter a tag key. The tag key must be 1 to 64 characters in length and cannot start with <code>aliyun</code> or <code>acs:</code> . It cannot contain <code>http://</code> or <code>https://</code> .

Parameter	Description
Tag Value	You can select or enter a tag value. The tag value must be 1 to 128 characters in length and cannot start with <code>al</code> <code>iyun</code> or <code>acs:</code> . It cannot contain <code>http://</code> or <code>https://</code> .

Related information

- [TagResources](#)

6.2.2. Attach tags to multiple VPN gateways at a time

After you attach tags to VPN gateways, you can search and filter the VPN gateways by tag. This topic describes how to attach tags to multiple VPN gateways at a time.

Context

You can attach up to 20 tags to each VPN gateway. Before you start, note that:

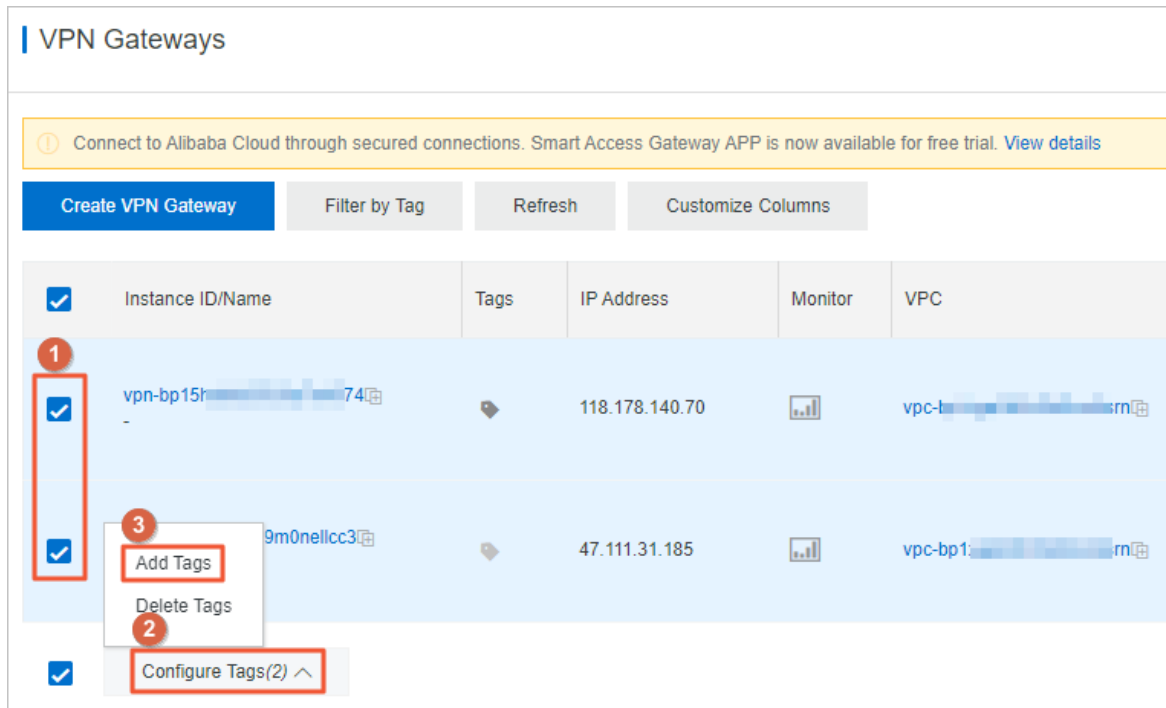
- The keys of tags that are attached to the same VPN gateway must be unique.
- Tags must be attached to VPN gateways.
- Tag information is not shared across regions.

For example, in the China (Shanghai) region, you cannot view tags of instances that are created in the China (Hangzhou) region.

- You can modify the key and value of a tag, or remove the tag. If you delete a VPN gateway, all the tags that are attached to it are removed.

Procedure

1. Log on to the [VPN gateway console](#).
2. In the top navigation bar, select the region where the VPN gateway is deployed.
3. On the VPN Gateways page, select the VPN gateways to which you want to attach tags, and choose **Configure Tags > Add Tags**.



- In the **Configure Tags for Multiple Resources** dialog box, set the following parameters, and click **OK**.

Parameter	Description
Tag Key	You can select or enter a tag key. The tag key must be 1 to 64 characters in length and cannot start with <code>aliyun</code> or <code>acs:</code> . It cannot contain <code>http://</code> or <code>https://</code> .
Tag Value	You can select or enter a tag value. The tag value must be 1 to 128 characters in length and cannot start with <code>aliyun</code> or <code>acs:</code> . It cannot contain <code>http://</code> or <code>https://</code> .

Related information

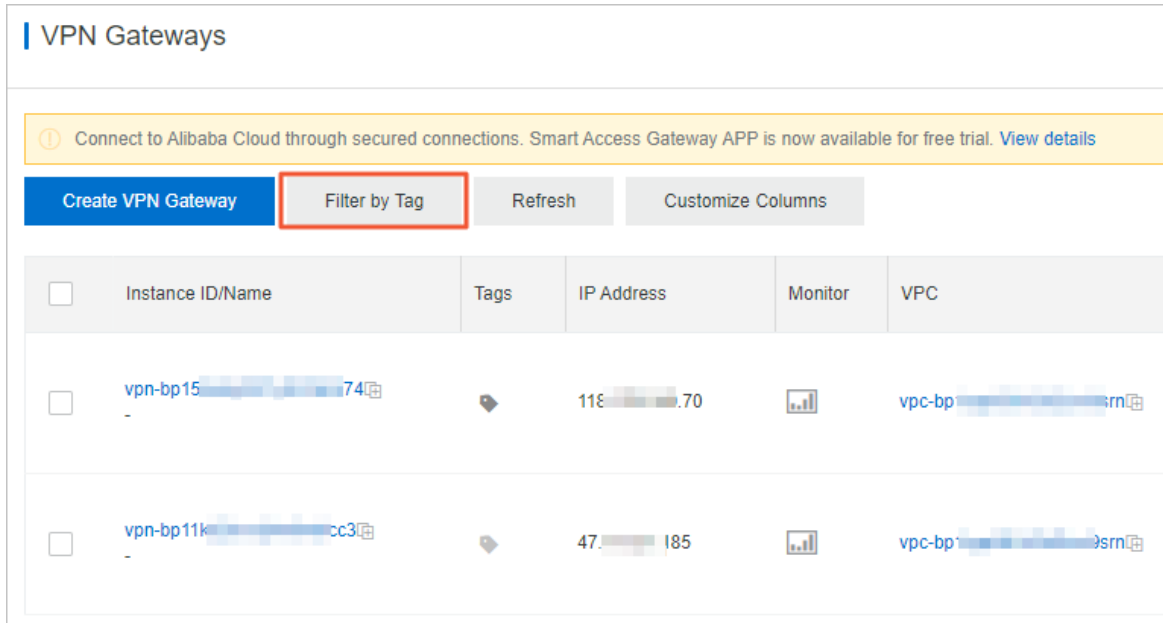
- [TagResources](#)

6.3. Search VPN gateways by tag

This topic describes how to search VPN gateways by using tags.

Procedure

- Log on to the [VPN gateway console](#).
- In the top navigation bar, select the region where the VPN gateway is deployed.
- On the **VPN Gateways** page, click the **Filter by Tag** tab.



- In the Filter by Tag dialog box, select or enter a tag key and a tag value, and click Search. You can select or enter a key-value pair, or a tag key. Up to 20 tags can be specified for each search.

Related information

- [ListTagResources](#)

6.4. Remove tags

6.4.1. Remove tags from a VPN gateway



You can remove tags that you no longer need from VPN gateways. This topic describes how to remove tags from a VPN gateway.

Context

Before you remove a tag, note that:

- You can remove up to 20 tags at a time.
- If a tag is attached to more than one VPN gateway and you remove the tag from a VPN gateway, the other VPN gateways still hold the tag.

Procedure

- Log on to the [VPN gateway console](#).
- In the top navigation bar, select the region where the VPN gateway is deployed.
- On the VPN Gateways page, find the VPN gateway from which you want to remove tags, move the pointer over the  image in the Tags column, and click Edit in the message that appears.
- In the Configure Tags dialog box, click the  icon on the right side to remove a tag. You can also attach tags to a VPN gateway in this dialog box.

- Click OK.

Related information

- [UnTagResources](#)

6.4.2. Remove tags from multiple VPN gateways at a time

You can remove tags that you no longer need from VPN gateways. This topic describes how to remove tags from multiple VPN gateways at a time.

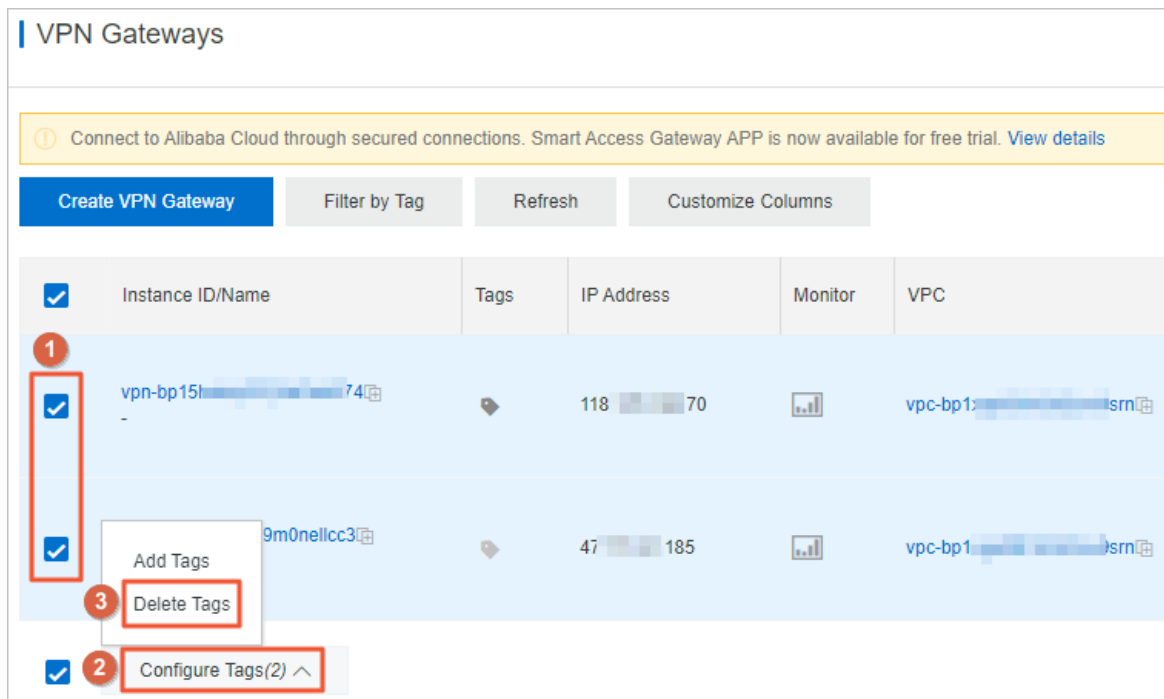
Context


Before you remove tags, note that:

- You can remove up to 20 tags at a time.
- If a tag is attached to more than one VPN gateway and you remove the tag from a VPN gateway, the other VPN gateways still hold the tag.

Procedure

- Log on to the [VPN gateway console](#).
- In the top navigation bar, select the region where the VPN gateway is deployed.
- On the **VPN Gateways** page, select the VPN gateways from which you want to remove tags, and choose **Configure Tags > Delete Tags**.



- In the **Delete Tags for Multiple Resources** dialog box, click the  icon on the right side to remove a tag.
- Click OK.

Related information

- [UnTagResources](#)

7.MTU notes

The maximum transmission unit (MTU) is the size (in bytes) of the largest packet supported by the network layer protocol (such as TCP), with headers and data included.

Network packets sent over IPsec tunnels are encrypted and then encapsulated in external packets for routing. Because an encapsulated internal packet itself must fit the MTU of the corresponding external packet, the MTU of the internal packet must be smaller.

Gateway MTU and system MTU

You must configure the MTU limit of the local VPN Gateway to not more than 1,400 bytes. We recommend that you set the MTU to 1,400 bytes.

For TCP traffic, the maximum length of data that can be carried by each packet segment can be negotiated by the sender and receiver when they communicate based on the maximum segment size (MSS).

8. Manage quotas

You can query the number of remaining resources in your quota through the VPC console. If the remaining quota number is insufficient for your requirements, you can open a ticket to apply for an increase to your quota.

Procedure

- 1.
- 2.
3. In the left-side navigation pane, click **Quota Management**.
4. On the **Quota Management** page, click the **VPN Gateway** tab to view the quota usage of VPN Gateways under your account.
5. To increase your resource quota, click **Apply** in the **Actions** column.
 - **Quantity for Application:** the number of resources you require. You must enter a number that is greater than the current quota. For more information about the resource limits of NAT Gateway, see [使用限制](#).
 - **Reason for Application:** your reason for applying for an increase to your quota. We recommend that you include details about your specific scenario.
 - **Mobile/Landline Phone Number:** the mobile or landline phone number of the person to contact.
 - **Email:** the email address of the person to contact.
6. Click **OK**. The system then determines whether the quota application is reasonable. If the system determines the request is unreasonable, the application enters the **Rejected** state. If the application is reasonable, the application status enters the **Approved** state and the quota is automatically upgraded to the specified quota number.

To view the history of quota applications, click **Application History** in the **Application History** column.