

Alibaba Cloud

VPN Gateway User Guide

Document Version: 20220704

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.VPN gateways -----	06
2.Manage a VPN Gateway -----	07
2.1. Configure routes of a VPN Gateway -----	07
2.1.1. Route overview -----	07
2.2. Enable IPsec-VPN and SSL-VPN -----	07
2.3. Enable quick diagnostics -----	08
2.4. Upgrade a VPN gateway -----	12
2.5. Service-linked roles -----	13
2.5.1. AliyunServiceRoleForVpn -----	13
3.Manage a customer gateway -----	16
3.1. Create a customer gateway -----	16
3.2. Modify a customer gateway -----	17
3.3. Delete a customer gateway -----	17
4.Configure SSL-VPN -----	18
4.1. Configuration overview -----	18
4.2. Manage an SSL server -----	18
4.2.1. Modify an SSL server -----	18
4.2.2. Delete an SSL server -----	18
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 -----	19
4.3.3. Delete an SSL client certificate -----	19
4.4. Modify the maximum number of concurrent SSL connectio...-----	20
5.Configure IPsec-VPN connections -----	21
5.1. Overview -----	21
5.2. Manage an IPsec-VPN connection -----	22

5.2.1. Create an IPsec-VPN connection	22
5.2.2. Modify an IPsec-VPN connection	28
5.2.3. Download the configuration of an IPsec-VPN connectio... ..	28
5.2.4. View IPsec-VPN connection logs	28
5.2.5. Delete an IPsec-VPN connection	29
5.3. Configure local gateways	29
5.3.1. Configure H3C firewall	29
5.3.2. Configure strongSwan	31
5.3.3. Configure an IPsec-VPN connection through an SRX se... ..	34
5.3.4. Load the IPsec-VPN configuration to a Cisco firewall d... ..	36
6.IPsec-VPN servers	41
6.1. Configure IPsec-VPN servers	41
6.2. Create and manage IPsec servers	43
6.3. Configure a mobile client	45
6.4. Query IPsec-VPN server logs	46
7.Tag management	48
7.1. Overview	48
7.2. Attach tags	49
7.2.1. Attach tags to a VPN gateway	49
7.2.2. Attach tags to multiple VPN gateways at a time	50
7.3. Search VPN gateways by tag	51
7.4. Remove tags	52
7.4.1. Remove tags from a VPN gateway	52
7.4.2. Remove tags from multiple VPN gateways at a time	53
8.Manage quotas	55

1. VPN gateways

Features

VPN Gateway supports both IPsec-VPN connections and SSL-VPN connections.

- IPsec-VPN

IPsec-VPN connects networks based on routes. It facilitates the configuration and maintenance of VPN policies, and provides flexible traffic routing methods.

You can use the IPsec-VPN feature to establish a secure connection between a data center and a virtual private cloud (VPC) or between two VPCs. IPsec-VPN supports the IKEv1 and IKEv2 protocols. All gateway devices that support the two protocols can connect to VPN gateways on Alibaba Cloud.

You can use IPsec-VPN in different scenarios. For more information, see [Overview of IPsec-VPN](#).

- SSL-VPN

You can use the SSL-VPN feature to connect a client to applications or services that are deployed in a VPC. After you deploy applications or services in a VPC, you need only to import the required certificate to a client and initiate a connection to the VPC.

You can use SSL-VPN in different scenarios. For more information, see [SSL-VPN overview](#).

2. Manage a VPN Gateway

2.1. Configure routes of a VPN Gateway

2.1.1. Route overview

After you create an IPsec-VPN connection by using a VPN gateway, you must add a route to the VPN gateway.

Route-based IPsec-VPN allows you to route network traffic in multiple ways, and facilitates the configuration and maintenance of VPN policies.

You can add the following two types of route to a VPN gateway:

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

Policy-based routes

Policy-based routes forward traffic based on source and destination IP addresses.

For more information, see [Add a policy-based route entry](#).

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

Destination-based routes

Destination-based routes forward traffic to specified destination IP addresses.

For more information, see [Create a destination-based route](#).

2.2. Enable IPsec-VPN and SSL-VPN

You can enable IPsec-VPN and SSL-VPN when or after you create a VPN gateway.

Enable IPsec-VPN

- 1.
- 2.
3. On the **VPN Gateways** page, find the VPN gateway and click **Enable** next to **IPsec** in the **Gateway Status** column.
4. On the configurations page, select **Enable IPsec-VPN**, select the VPN Gateway Terms of Service check box, click **Buy Now**, and then complete the payment.

Enable SSL-VPN

- If your VPN gateway was created before January 20, 2018, update the VPN gateway to the latest version before you enable SSL-VPN for the VPN gateway.
- If your VPN gateway was created after January 20, 2018, you can enable SSL-VPN for the VPN gateway in the console.

- 1.
- 2.
3. On the **VPN Gateways** page, find the VPN gateway and click **Enable** next to **SSL** in the **Gateway Status** column.
4. On the configurations page, select **Enable SSL-VPN**, specify the number of SSL-VPN connections, select the VPN Gateway Terms of Service check box, click **Buy Now**, and then complete the payment.

2.3. Enable quick diagnostics

VPN gateways support the quick diagnostics feature that can be used to detect anomalies in VPN connections. The anomalies include configuration errors, quota issues, route conflicts, and network connectivity issues. This feature allows you to locate the cause of a VPN connection failure and troubleshoot the failure.

Prerequisites

- A VPN gateway is created and an IPsec-VPN connection is created for the VPN gateway before you enable the quick diagnostics feature. For more information, see [创建和管理VPN网关实例](#) and [Create an IPsec-VPN connection](#).

 **Note** The quick diagnostics feature is supported only in the following regions: .

- Make sure that your VPN gateway uses the latest version. Otherwise, you cannot use the quick diagnostics feature.

Context

You can use this feature to diagnose IPsec-VPN connections. However, it cannot be used to diagnose SSL-VPN connections. This feature allows you to diagnose the following items.

Item	Description
------	-------------

Item	Description
<p>Quota of IPsec-VPN connections supported by a VPN gateway</p>	<p>The system checks the number of IPsec-VPN connections created for a specified VPN gateway and the quota of IPsec-VPN connections supported by each VPN gateway under your Alibaba Cloud account. Then, the system calculates the ratio of created IPsec-VPN connections to the quota supported by each VPN gateway.</p> <ul style="list-style-type: none"> • If the ratio is not greater than 80%, the diagnostic result is normal. • If the ratio is greater than 80%, the diagnostic result is warning. <p>For example, the quota of IPsec-VPN connections supported by your VPN gateway is 10:</p> <ul style="list-style-type: none"> • If you have created eight IPsec-VPN connections for the VPN gateway, the diagnostic result of this item is normal. • If you have created nine IPsec-VPN connections for the VPN gateway, the diagnostic result of this item is warning. <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p> Note By default, each VPN gateway supports at most 10 IPsec-VPN connections.</p> <p>To increase the quota, go to the Quota Management page. For more information, see Manage quotas.</p> </div>
<p>Quota of policy-based routes supported by a VPN gateway</p>	<p>The system checks the number of policy-based routes created for a specified VPN gateway and the quota of policy-based routes supported by each VPN gateway under your Alibaba Cloud account. Then, the system calculates the ratio of created policy-based routes to the quota supported by each VPN gateway.</p> <ul style="list-style-type: none"> • If the ratio is not greater than 80%, the diagnostic result is normal. • If the ratio is greater than 80%, the diagnostic result is warning. <p>For example, the quota of policy-based routes supported by your VPN gateway is 20:</p> <ul style="list-style-type: none"> • If you have created 16 policy-based routes for the VPN gateway, the diagnostic result of this item is normal. • If you have created 17 policy-based routes for the VPN gateway, the diagnostic result of this item is warning. <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p> Note By default, each VPN gateway supports up to 20 policy-based routes.</p> <p>To increase the quota, go to the Quota Management page. For more information, see Manage quotas.</p> </div>

Item	Description
<p>Quota of destination-based routes supported by a VPN gateway</p>	<p>The system checks the number of destination-based routes created for a specified VPN gateway and the quota of destination-based routes supported by each VPN gateway under your Alibaba Cloud account. Then, the system calculates the ratio of created destination-based routes to the quota supported by each VPN gateway.</p> <ul style="list-style-type: none"> • If the ratio is not greater than 80%, the diagnostic result is normal. • If the ratio is greater than 80%, the diagnostic result is warning. <p>For example, the quota of destination-based routes supported by your VPN gateway is 20:</p> <ul style="list-style-type: none"> • If you have created 16 destination-based routes for the VPN gateway, the diagnostic result of this item is normal. • If you have created 17 destination-based routes for the VPN gateway, the diagnostic result of this item is warning. <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p> Note By default, each VPN gateway supports at most 20 destination-based routes.</p> <p>To increase the quota, go to the Quota Management page. For more information, see Manage quotas.</p> </div>
<p>Route conflicts</p>	<p>The system checks a specified IPsec-VPN connection route and determines whether the route conflicts with any route in the route table of a specified VPN gateway. An IPsec-VPN connection route is a route whose next hop is an IPsec-VPN connection.</p> <ul style="list-style-type: none"> • If the destination CIDR block of the IPsec-VPN connection route is different from and does not overlap with the destination CIDR blocks of the routes in the route table, the diagnostic result is normal. • If the destination CIDR block of a route in the route table is the same as or contains that of the IPsec-VPN connection route, the diagnostic result is error. • If the destination CIDR block of the IPsec-VPN connection route contains that of a route in the route table, the diagnostic result is warning. <p>For example, the destination CIDR block of your IPsec-VPN connection route is 172.23.0.0/16 and the next hop is vco-1:</p> <ul style="list-style-type: none"> • If the route table of the VPN gateway has only one route with the destination CIDR block of 192.168.0.0/16, the diagnostic result is normal. • If the route table of the VPN gateway has a route with the destination CIDR block of 172.23.0.0/16 and next hop of vco-2, the diagnostic result is error. • If the route table of the VPN gateway has a route with the destination CIDR block of 172.23.1.0/24 and next hop of vco-3, the diagnostic result is warning.

Item	Description
Configuration consistency of IPsec-VPN connections	<p>The system checks whether the configurations of IPsec-VPN connections for a specified VPN gateway are the same those of an on-premises gateway device.</p> <ul style="list-style-type: none"> If the configurations are consistent, the diagnostic result is normal. If the configurations are inconsistent, the diagnostic result is error. <div style="background-color: #e0f2f7; padding: 5px;"> <p> Note If the quick diagnostics feature fails to obtain the configurations of IPsec-VPN connections for the on-premises gateway device, the diagnostic result is also normal.</p> </div>
Internet connectivity of customer gateways	<p>The system sends packets to test Internet connectivity.</p> <ul style="list-style-type: none"> If the packet loss rate is 0, the diagnostic result is normal. If the packet loss rate is 0 to 100% (excluding 0 and 100%), the diagnostic result is warning. If the packet loss rate is 100%, the diagnostic result is error.
Private network connectivity	<p>The system sends packets to test private network connectivity.</p> <ul style="list-style-type: none"> If the packet loss rate is 0, the diagnostic result is normal. If the packet loss rate is 0 to 100% (excluding 0 and 100%), the diagnostic result is warning. If the packet loss rate is 100%, the diagnostic result is error. <div style="background-color: #e0f2f7; padding: 5px;"> <p> Note To test private network connectivity, you must specify the source IP address and destination IP address. Otherwise, the connectivity test fails.</p> </div>

Procedure

- 1.
2. In the top navigation bar, select the region where the VPN gateway is deployed.
3. On the **VPN Gateways** page, choose  > **Quick Diagnostics** in the **Actions** column.
4. In the **Quick Diagnostics** dialog box, set the following parameters and click **Next**.

Parameter	Description
IPsec Connection	Select the IPsec-VPN connection that you want to diagnose.
Private Network Connectivity Check	
Source IP Address	Enter an IP address in a virtual private cloud (VPC). This IP address is used as the source IP address to test private network connectivity.
Destination IP Address	Enter an IP address of a data center. This IP address is used as the destination IP address to test private network connectivity.

5. In the **Diagnostic Result** section, view the diagnostic results of the IPsec-VPN connection.

2.4. Upgrade a VPN gateway

This topic describes how to upgrade a VPN gateway. After you upgrade a VPN gateway to the latest version, you can use more features. These features include BGP dynamic routing and Dead Peer Detection (DPD).

Descriptions

- It takes about 10 minutes to upgrade a VPN gateway. The VPN gateway remains unavailable during the upgrade process. Connections that are established to the VPN gateway are also interrupted. We recommend that you upgrade a VPN gateway during a network maintenance window to avoid service interruptions.
- If multiple CIDR blocks are specified for an IPsec-VPN connection and the IKE version is IKE V1, you must change IKE V1 to IKE V2 or create an IPsec-VPN connection for each of the CIDR blocks. Otherwise, the upgrade will fail.
- You can check whether your VPN gateway is already upgraded to the latest version based on the status of the **Upgrade** button.
 - If your VPN gateway uses the latest version, the **Upgrade** button is dimmed and unavailable. If you move the pointer over the **Upgrade** button, the console prompts that the VPN gateway is already upgraded to the latest version.

Newly created VPN gateways use the latest version by default.

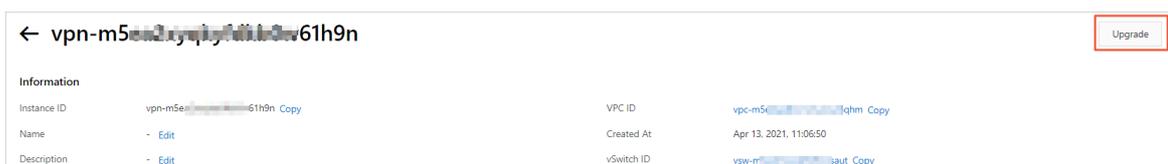
- If the **Upgrade** button is not dimmed, you can click it to upgrade the VPN gateway. For more information about how to upgrade a VPN gateway, see [Upgrade](#).

If your VPN gateway was created before March 21, 2019, the routes of the VPN gateway cannot be converted to the latest policy-based routes during the upgrade. After the VPN gateway is upgraded, you must configure routes for the VPN gateway to ensure network connectivity. For more information, see [Route overview](#).

If your VPN gateway was created after March 21, 2019, you do not need to configure routes after you upgrade the VPN gateway.

Upgrade

- 1.
- 2.
3. On the **VPN Gateways** page, find the VPN gateway that you want to upgrade and click its ID.
4. On the details page of the VPN gateway, click **Upgrade**.



5. In the **Upgrade VPN Gateway** dialog box, read and accept the upgrade agreement, and then click **OK**.

After you click **OK**, the system starts to upgrade the VPN gateway. Wait until the upgrade is completed.

2.5. Service-linked roles

2.5.1. AliyunServiceRoleForVpn

This topic describes the service-linked role AliyunServiceRoleForVpn. A VPN gateway can assume this role to access other cloud resources.

Background information

A service-linked role is a Resource Access Management (RAM) role that can be assumed by the linked service. A service can assume the service-linked role to access other cloud resources. Service-linked roles simplify the authorization process and prevent user errors. For more information, see [Service-linked roles](#).

Create the service-linked role AliyunServiceRoleForVpn

When you create a VPN gateway, the system automatically creates the service-linked role AliyunServiceRoleForVpn. This role contains a policy named AliyunServiceRolePolicyForVpn, which allows a VPN gateway to access other cloud resources. The policy contains the following content:

 **Note** If the service-linked role AliyunServiceRoleForVpn already exists, the system does not create it again.

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVSwitchAttributes"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:CreateNetworkInterface",
        "ecs:CreateSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:RevokeSecurityGroup",
        "ecs>DeleteSecurityGroup",
        "ecs:JoinSecurityGroup",
        "ecs:LeaveSecurityGroup",
        "ecs:DescribeSecurityGroups",
        "ecs:AttachNetworkInterface",
        "ecs:DetachNetworkInterface",
        "ecs>DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:CreateNetworkInterfacePermission",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs>DeleteNetworkInterfacePermission",
        "ecs:CreateSecurityGroupPermission",
        "ecs:AuthorizeSecurityGroupPermission",
        "ecs:RevokeSecurityGroupPermission",

```

```
"ecs:JoinSecurityGroupPermission",
"ecs>DeleteSecurityGroupPermission",
"ecs:LeaveSecurityGroupPermission",
"ecs:DescribeSecurityGroupPermissions",
"ecs:AttachNetworkInterfacePermissions",
"ecs:DetachNetworkInterfacePermissions",
"ecs:AssignPrivateIpAddresses",
"ecs:UnassignPrivateIpAddresses",
"ecs:DescribeNetworkInterfaceAttribute"
],
"Resource": "*",
"Effect": "Allow"
},
{
  "Action": "ram:DeleteServiceLinkedRole",
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ram:ServiceName": "vpn.aliyuncs.com"
    }
  }
}
]
}
```

Delete the service-linked role AliyunServiceRoleForVpn

You can delete the service-linked role AliyunServiceRoleForVpn only when no VPN gateway exists within your Alibaba Cloud account. For more information, see the following topics:

1. [创建和管理VPN网关实例](#)
2. [Delete a service-linked role](#)

FAQ

By default, an Alibaba Cloud account is authorized to create the service-linked role AliyunServiceRoleForVpn. If a RAM user wants to create the service-linked role, you must first use the Alibaba Cloud account to grant the required permissions to the RAM user.

You must create the following policy and attach it to the RAM user. Then, the RAM user can create the service-linked role AliyunServiceRoleForVpn. For more information, see [Create a custom policy](#) and [Grant permissions to a RAM role](#).

```
{
  "Statement": [
    {
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "vpn.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```

Why am I unable to create the service-linked role AliyunServiceRoleForVpn by using a RAM user?

References

[创建和管理VPN网关实例](#)

3. Manage a customer gateway

3.1. Create a customer gateway

This topic describes how to create a customer gateway. You can use a customer gateway to establish an IPsec-VPN connection between a virtual private cloud (VPC) and a data center or between two VPCs. After you create a customer gateway, you can update the information about a gateway device in the data center to Alibaba Cloud. Then, you can connect the customer gateway to a VPN gateway. A customer gateway can connect to multiple VPN gateways.

Procedure

- 1.
- 2.
3. In the top navigation bar, select the region where you want to create the customer gateway.

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

4. On the **Customer Gateways** page, click **Create Customer Gateway**.
5. On the **Create Customer Gateway** page, set the following parameters and click **OK**.

Parameter	Description
Name	Enter a name for the customer gateway.
IP Address	Enter the static public IP address of the gateway device in the data center.
ASN	<p>Enter the autonomous system number (ASN) of the gateway device in the data center. Valid values: 1 to 4294967295.</p> <p>You can enter the ASN in two segments and separate the first 16 bits from the following 16 bits with a period (.). Enter the number in each segment in the decimal format.</p> <p>For example, if you enter 123.456, the ASN is 8061384. The ASN is calculated by using the following formula: $123 \times 65536 + 456 = 8061384$.</p> <div data-bbox="550 1556 1380 1836" style="background-color: #e6f2ff; padding: 10px;"> <p> Note</p> <ul style="list-style-type: none"> ◦ This parameter is required when the VPN gateway has dynamic BGP enabled. ◦ We recommend that you use a private ASN to establish a connection with Alibaba Cloud over BGP. Refer to the relevant documentation for the private ASN range. </div>

Parameter	Description
Description	Enter a description for the customer gateway. You can click + below the Description field to create multiple customer gateways at a time.

Related information

- [CreateCustomerGateway](#)

3.2. Modify a customer gateway

This topic describes how to modify the name and description of a customer gateway.

Procedure

- 1.
- 2.
- 3.
4. On the **Customer Gateways** page, find the customer gateway, click [✎](#) in the **Instance ID/Name** column. In the dialog box that appears, enter a new name and click **OK**.
5. Click [✎](#) in the **Description** column. In the dialog box that appears, enter a new description and click **OK**.

Related information

- [ModifyCustomerGatewayAttribute](#)

3.3. Delete a customer gateway

This topic describes how to delete a customer gateway.

Procedure

- 1.
- 2.
- 3.
4. On the **Customer Gateways** page, find the customer gateway that you want to delete, and then click **Delete** in the **Actions** column.
5. In the **Delete Customer Gateway** message, 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.

4.2. Manage an SSL server

4.2.1. Modify an SSL server

After you create an SSL server, you can modify its configurations.

Procedure

- 1.
- 2.
- 3.
4. On the **SSL Servers** page, find the SSL server that you want to manage and click **Modify** in the **Actions** column.
5. On the **Edit SSL Server** page, modify the name, server CIDR block, client CIDR block, and advanced settings of the SSL server, and then click **OK**.

For more information about the parameters on the buy page, see [创建SSL服务端](#).

4.2.2. Delete an SSL server

This topic describes how to delete an SSL server.

Procedure

- 1.
- 2.
- 3.
4. On the **SSL Servers** page, find the SSL server that you want to delete and click **Delete** in the **Actions** column.
5. In the **Delete SSL Server** message, click **OK**.

4.3. Manage an SSL client certificate

4.3.1. Create an SSL client certificate

After you create an SSL server, you must create an SSL client certificate based on the configuration of the SSL server.

Prerequisites

An SSL server is created. For more information, see [创建SSL服务端](#).

Procedure

- 1.
- 2.
- 3.
4. On the **SSL Clients** page, click **Create Client Certificate**.
5. In the **Create Client Certificate** panel, set the following parameters and click **OK**.

Parameter	Description
Name	Enter a name for the SSL client certificate. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter.
SSL Server	Select the SSL server that you want to associate with the SSL client certificate.

4.3.2. Download an SSL client certificate

This topic describes how to download an SSL client certificate. You can download an SSL client certificate in the VPN Gateway console.

Prerequisites

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

Procedure

- 1.
- 2.
- 3.
4. On the **SSL Clients** page, find the SSL client certificate that you want to download 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.
4. On the **SSL Clients** page, find the SSL client certificate that you want to delete, and click **Delete** in the **Actions** column.
5. In the **Delete Client Certificate** dialog box, click **OK**.

4.4. Modify the maximum number of concurrent SSL connections

This topic describes how to modify the maximum number of concurrent SSL connections that a VPN gateway supports.

Procedure

- 1.
2. In the top navigation bar, select the region where the VPN gateway that you want to manage is created.
3. On the **VPN Gateway** page, find the VPN gateway that you want to manage.
 - To increase the maximum number of concurrent SSL connections, click **Upgrade** in the **Concurrent SSL Connections** column.
 - To reduce the maximum number of concurrent SSL connections, click **Downgrade** in the **Concurrent SSL Connections** column.
4. In the **SSL Connections:** section, specify a new maximum number and complete the payment.

5. Configure IPsec-VPN connections

5.1. Overview

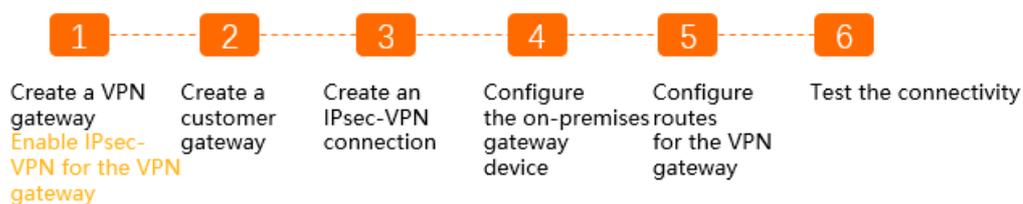
This topic describes how to connect a virtual private cloud (VPC) to a data center through IPsec-VPN.

Prerequisites

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

- The gateway device in the data center supports the IKEv1 and IKEv2 protocols.
IPsec-VPN supports the IKEv1 and IKEv2 protocols. All gateway devices that support the two protocols can connect to VPN gateways on Alibaba Cloud.
- A static public IP address is assigned to the gateway device in the data center.
- The CIDR block of the data center does not overlap with the CIDR block of the VPC.
- You must make sure that the security group rules applied to the Elastic Compute Service (ECS) instances in the VPC allow gateway devices in the data center to access cloud resources. For more information, see [Query security group rules](#).

Procedure



1. Create a VPN gateway

You must enable the IPsec-VPN feature after you create the VPN gateway. You can establish more than one IPsec-VPN connection to each VPN gateway.

2. Create a customer gateway

You must load the configuration of the gateway device in the data center to a customer gateway on Alibaba Cloud.

3. Create an IPsec-VPN connection

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

4. Configure the gateway device in the data center

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

5. Add routes to the VPN gateway

You must add routes to the VPN gateway and advertise these routes to the VPC route table. Then, the VPC and the data center can communicate with each other. For more information, see [Route overview](#).

6. Verify the connectivity

Log on to an ECS instance that is not assigned a public IP address in the VPC. Then, run the `ping` command to ping the private IP address of a server that resides in the 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 between the two gateways to encrypt data transmission.

Prerequisites

- A VPN gateway is created. For more information, see [创建和管理VPN网关实例](#).
- A customer gateway is created. For more information, see [Create a customer gateway](#).

Context

When you create an IPsec-VPN connection, you can enable or disable the following features:

- **DPD**: the dead peer detection (DPD) feature.

After you enable DPD, the initiator of the IPsec-VPN connection sends DPD packets to check the existence and availability of the peer. If no response is received from the peer within a specified period of time, the connection fails. The ISAKMP Security Association (SA), IPsec SA, and IPsec tunnel are deleted. This feature is enabled by default.

- **NAT Traversal**: the network address translation (NAT) traversal feature.

After you enable NAT traversal, the initiator does not check the UDP ports during IKE negotiations and can automatically discover NAT gateway devices along the IPsec tunnel. This feature is enabled by default.

- **BGP**: the Border Gateway Protocol (BGP) dynamic routing feature.

After you enable BGP routing, the VPN gateway can automatically learn routes by using BGP. This reduces network maintenance costs and network configuration errors. This feature is disabled by default.

- **Health Check**: the health check feature.

You can configure health checks to check the connectivity of IPsec-VPN connections and detect issues at the earliest opportunity. This feature is disabled by default.

Note

- If you use a VPN gateway of the latest version, you can use DPD, NAT traversal, BGP dynamic routing, and health checks. Otherwise, you cannot use the preceding features.
- You cannot disable BGP dynamic routing after you enable it.

Procedure

- 1.
- 2.
- 3.
4. On the **IPsec Connections** page, click **Create IPsec Connection**.
5. On the **Create IPsec Connection** page, configure the IPsec-VPN connection based on the following information and click **OK**.

Parameter	Description
Name	Enter a name for the IPsec-VPN connection. The name must be 2 to 128 characters in length and can contain digits, hyphens (-), and underscores (_). It must start with a letter.
VPN Gateway	Select the standard VPN gateway to be connected through the IPsec-VPN connection.
Customer Gateway	Select the customer gateway to be connected through the IPsec-VPN connection.

Parameter	Description
Routing Mode	<p>Select a routing mode. Default value: Destination Routing Mode.</p> <ul style="list-style-type: none">◦ Destination Routing Mode: forwards traffic to specified destination IP addresses. <p>After you create an IPsec-VPN connection, you must add destination-based routes to the route table of the VPN gateway. For more information, see Manage destination-based routes.</p> <ul style="list-style-type: none">◦ Protected Data Flows: forwards traffic based on source and destination IP addresses. <p>If you select Protected Data Flows when you create an IPsec-VPN connection, you must configure Local Network and Remote Network. After you complete the configurations, the system automatically adds policy-based routes to the route table of the VPN gateway.</p> <p>After the system adds policy-based routes to the route table of the VPN gateway, the routes are not advertised by default. You must manually advertise the routes to the VPC.</p> <div data-bbox="552 869 1385 1339" style="background-color: #e0f2f7; padding: 10px;"><p> Note</p><ul style="list-style-type: none">◦ If you use an earlier version of VPN Gateway, you do not need to select a routing mode. After you create an IPsec-VPN connection, you must manually add destination-based routes or policy-based routes to the VPN gateway. For more information, see Route overview.◦ Do not create a route that meets the following conditions: The destination CIDR block is 100.64.0.0/10 or one of its subnets. The next hop is an IPsec-VPN connection. If you create such a route, one of the following errors occurs: The status of the IPsec-VPN connection cannot be displayed in the console. The negotiations of the IPsec-VPN connection fail.</div>

Parameter	Description
Local Network	<p>Enter the CIDR block on the VPC side. The CIDR block is used in Phase 2 negotiations.</p> <p>Click + next to the field to add multiple CIDR blocks on the VPC side.</p> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p> Note You can add multiple CIDR blocks only if IKEv2 is used.</p> </div>
Remote Network	<p>Enter the CIDR block on the data center side. This CIDR block is used in Phase 2 negotiations.</p> <p>Click + next to the field to add multiple CIDR blocks on the data center side.</p> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p> Note You can add multiple CIDR blocks only if IKEv2 is used.</p> </div>
Effective Immediately	<p>Specify whether to immediately start negotiations.</p> <ul style="list-style-type: none"> ◦ Yes: starts connection negotiations after the configuration is completed. ◦ No: starts negotiations when inbound traffic is detected.
Pre-Shared Key	<p>Enter the pre-shared key that is used for identity authentication between the VPN gateway and the data center. The key must be 1 to 100 characters in length.</p> <p>If you do not specify a pre-shared key, the system randomly generates a 16-bit string as the pre-shared key. After you create an IPsec-VPN connection, you can click Edit to view the pre-shared key that is generated by the system. For more information, see Modify an IPsec-VPN connection.</p> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p> Notice The pre-shared key of the IPsec-VPN connection must be the same as the authentication key of the data center. Otherwise, you cannot establish a connection between the data center and the VPN gateway.</p> </div>
Advanced Configuration: IKE Configurations	
Version	<p>Select an IKE version.</p> <ul style="list-style-type: none"> ◦ ikev1 ◦ ikev2 <p>IKEv1 and IKEv2 are supported. Compared with IKEv1, IKEv2 simplifies the SA negotiation process and provides better support for scenarios in which multiple CIDR blocks are used. We recommend that you select IKEv2.</p>

Parameter	Description
Negotiation Mode	<p>Select a negotiation mode.</p> <ul style="list-style-type: none"> ◦ main: This mode offers higher security during negotiations. ◦ aggressive: This mode is faster and has a higher success rate. <p>Connections negotiated in both modes ensure the same level of security for data transmission.</p>
Encryption Algorithm	Select the encryption algorithm that is used in Phase 1 negotiations. Supported algorithms are aes , aes192 , aes256 , des , and 3des .
Authentication Algorithm	Select the authentication algorithm that is used in Phase 1 negotiations. Supported algorithms are sha1 , md5 , sha256 , sha384 , and sha512 .
DH Group	<p>Select the DH key exchange algorithm that is used in Phase 1 negotiations. The following DH groups are supported:</p> <ul style="list-style-type: none"> ◦ group1: DH group 1 ◦ group2: DH group 2 ◦ group5: DH group 5 ◦ group14: DH group 14
SA Life Cycle (seconds)	Specify the lifecycle of the SA after Phase 1 negotiations succeed. Unit: seconds. Default value: 86400 . Valid values: 0 to 86400 .
LocalId	Specify the identifier of the VPN gateway that is used in Phase 1 negotiations. The default value is the public IP address of the VPN gateway. If you set LocalId to a fully qualified domain name (FQDN), we recommend that you set Negotiation Mode to aggressive .
Remoteld	Specify the identifier of the customer gateway that is used in Phase 1 negotiations. The default value is the public IP address of the customer gateway. If you set Remoteld to an FQDN, we recommend that you set Negotiation Mode to aggressive .
Advanced Configuration: IPsec Configurations	
Encryption Algorithm	Select the encryption algorithm that is used in Phase 2 negotiations. Supported algorithms are aes , aes192 , aes256 , des , and 3des .
Authentication Algorithm	Select the authentication algorithm that is used in Phase 2 negotiations. Supported algorithms are sha1 , md5 , sha256 , sha384 , and sha512 .

Parameter	Description
DH Group	<p>Select the DH key exchange algorithm that is used in Phase 2 negotiations. Standard VPN gateways support the following values:</p> <ul style="list-style-type: none"> ◦ disabled: does not use a DH key exchange algorithm. <ul style="list-style-type: none"> ▪ For clients that do not support perfect forward secrecy (PFS), select disabled. ▪ If you select a value other than disabled, the PFS feature is enabled by default, which requires a key update for every renegotiation. Therefore, you must also enable PFS for the client. ◦ group1: DH group 1 ◦ group2: DH group 2 ◦ group5: DH group 5 ◦ group14: DH group 14
SA Life Cycle (seconds)	Specify the lifecycle of the SA after Phase 2 negotiations succeed. Unit: seconds. Default value: 86400 . Valid values: 0 to 86400 .
DPD	Specify whether to enable the DPD feature. This feature is enabled by default.
NAT Traversal	Specify whether to enable the NAT traversal feature. This feature is enabled by default.
BGP Configuration	
Tunnel CIDR Block	<p>Enter the CIDR block of the IPsec tunnel.</p> <p>The CIDR block must fall within 169.254.0.0/16. The subnet mask of the CIDR block must be 30 bits in length.</p>
Local BGP IP address	<p>Enter the BGP IP address on the VPC side.</p> <p>This IP address must fall within the CIDR block of the IPsec tunnel.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #d9e1f2;"> <p> Note Make sure that the BGP IP addresses on the VPC side and on the data center side do not conflict with each other.</p> </div>
Local ASN	<p>Enter the autonomous system number (ASN) on the VPC side. Valid values: 1 to 4294967295. Default value: 45104.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #d9e1f2;"> <p> Note We recommend that you use a private ASN to establish a connection with Alibaba Cloud over BGP. Refer to the relevant documentation for the valid range of a private ASN.</p> </div>
Health Check	
Destination IP	Enter the IP address on the data center side that the VPC can communicate with through the IPsec-VPN connection.

Parameter	Description
Source IP	Enter the IP address on the VPC side that the data center can communicate with through the IPsec-VPN connection.
Retry Interval	Specify the interval between two consecutive health checks. Unit: seconds.
Number of Retries	Specify the maximum number of health check retries.

5.2.2. Modify an IPsec-VPN connection

After you create an IPsec-VPN connection, you can modify its configurations.

Procedure

- 1.
- 2.
- 3.
4. On the **IPsec Connections** page, find the IPsec-VPN connection that you want to manage, and click **Edit** in the **Actions** column.
5. On the **Modify IPsec Connections** page, modify the name, advanced configurations, CIDR block, and then click **OK**.

For more information about the parameters, see [Create an IPsec-VPN connection](#).

5.2.3. Download the configuration of an IPsec-VPN connection

After you create an IPsec-VPN connection, you can download its configuration.

Procedure

- 1.
- 2.
- 3.
4. On the **IPsec Connections** page, find the IPsec-VPN connection that you want to manage and choose **> Download Configuration** in the **Actions** column.

What's next

After you download the configuration of an IPsec-VPN connection, you can load the configuration to an on-premises gateway device. For more information, see [Configure a gateway device in a data center](#).

5.2.4. View IPsec-VPN connection logs

This topic describes how to view IPsec-VPN connection logs that are generated within the last month to troubleshoot connection errors. The time range of a log is set to 10 minutes.

Procedure

- 1.
- 2.
- 3.
4. On the **IPsec Connections** page, find the IPsec-VPN connection that you want to manage and choose **> View Logs** in the **Actions** column.
5. In the **IPsec Connection Logs Dialog Box**, set the time range and view the log.

5.2.5. Delete an IPsec-VPN connection

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

Procedure

- 1.
- 2.
- 3.
4. On the **IPsec Connections** page, find the IPsec-VPN connection that you want to delete, and click **Delete** in the **Actions** column.
5. In the **Are you sure that you want to delete the following resources?** message, click **OK**.

5.3. Configure local gateways

5.3.1. 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 [建立VPC到本地数据中心的连接](#).
- 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:

- o 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

- o 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.

5.3.2. Configure strongSwan

When you use IPsec-VPN to establish a site-to-site connection, you must configure the gateway device in the data center after you configure the VPN gateway on Alibaba Cloud. The following example shows you how to load the configuration of a VPN gateway to a data center. strongSwan is used in the example.

Prerequisites

- An IPsec-VPN connection is created. For more information, see [建立VPC到本地数据中心的连接](#).
- The configuration of the IPsec-VPN connection is downloaded. For more information, see [Download the configuration of an IPsec-VPN connection](#).

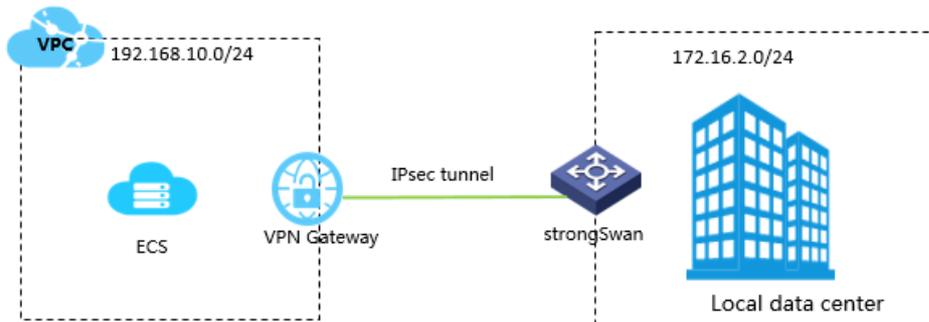
The following table shows the configuration of the IPsec-VPN connection in this example.

Protocol	Parameter	Example
IKE	Authentication algorithm	sha1
	Encryption algorithm	aes
	DH group	group2
	IKE version	ikev1
	Lifecycle	86400
	Negotiation mode	main
	Pre-shared key (PSK)	123456
IPsec	Authentication algorithm	sha1
	Encryption algorithm	aes
	DH group	group2
	Lifecycle	86400

Description

The following scenario is used as an example in this topic. The data center and Alibaba Cloud VPC are connected by using IPsec VPN:

- The CIDR block of the Alibaba Cloud VPC is 192.168.10.0/24.
- The CIDR block of the data center is 172.16.2.0/24.
- The public IP address of strongSwan is 59.XX.XX.70.



Step 1: Install strongSwan

1. Run the following command to install strongSwan:

```
# yum install strongswan
```

2. Run the following command to query the version of strongSwan that you installed:

```
# strongswan version
```

Step 2: Configure strongSwan

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

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

2. Refer to the following configuration to modify the *ipsec.conf* file:

```
# ipsec.conf - strongSwan IPsec configuration file
# basic configuration
config setup
    uniqueids=never
conn %default
    authby=psk # enables pre-shared key authentication
    type=tunnel
conn tomyidc
    keyexchange=ikev1 # the version of the IKE protocol that is used by the
IPsec-VPN connection
    left=59.XX.XX.70
    leftsubnet=172.16.2.0/24 # the CIDR block of the data center
    leftid=59.XX.XX.70 # the public IP address of the gateway in the data cen
ter
    right=119.XX.XX.125
    rightsubnet=192.168.10.0/24 # the CIDR block of the VPC
    rightid=119.XX.XX.125 # the IP address of the VPN gateway
    auto=route
    ike=aes-sha1-modp1024 # the encryption algorithm, authentication algorithm,
and DH group of the IKE protocol
    ikelifetime=86400s # the lifecycle of the IKE protocol
    esp=aes-sha1-modp1024 # the encryption algorithm, authentication algorithm,
and DH group of the IPsec protocol
    lifetime=86400s # the lifecycle of the IPsec protocol
    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 in the code:

```
59.XX.XX.70 119.XX.XX.125 : PSK 123456 # 123456 is the pre-shared key for the IPs
ec-VPN connection. The data center and the VPN gateway must use the same pre-shared
key.
```

4. Enable system forwarding:

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

For more information, see [Configurations for different scenarios](#).

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

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

6. Configure two routes in the data center. One route is used to transmit data from the data center client to the strongSwan gateway. The other route is used to transmit data from the strongSwan gateway to the data center client.

Note If you have created more than three IPsec-VPN connections by using strongSwan, you must modify the configuration in `/etc/strongswan/strongswan.d/charon.conf`. You must delete the annotator before the `max_ikev1_exchanges = 3` command to enable the command, and modify the parameter in the command to a value that is greater than the number of connections you have created.

For example, if you have created four connections using strongSwan, you can change the command to `max_ikev1_exchanges = 5`.

5.3.3. 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
```

5.3.4. Load the IPsec-VPN configuration to a Cisco firewall device

When you use IPsec-VPN to establish a site-to-site connection, you must load the IPsec-VPN configuration to the gateway device that is deployed in the data center after you configure the VPN gateway on Alibaba Cloud. This topic provides an example on how to load the IPsec-VPN configuration to a Cisco firewall device that is deployed in a data center.

Context

The following table describes the network configurations of the virtual private cloud (VPC) and the data center in this example.

Parameter		Example
VPC	CIDR blocks of the vSwitches	192.168.10.0/24 and 192.168.11.0/24
	Public IP address of the VPN gateway	47.XX.XX.161
Data center	Private CIDR block	10.10.10.0/24
	Public IP address of the Cisco firewall device	124.XX.XX.171

Note If you want to connect multiple CIDR blocks of a data center to a VPC, we recommend that you create an equivalent number of IPsec-VPN connections and add routes to the VPN gateway on Alibaba Cloud.

Configure IKEv1 VPN

Prerequisites:

- An IPsec-VPN connection is created in a VPC on Alibaba Cloud. 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 following configuration is used in this example.

Protocol	Parameter	Example
IKE	Authentication algorithm	SHA-1
	Encryption algorithm	AES-128
	DH group	group 2
	IKE version	IKE v1
	Lifecycle	86400
	Negotiation mode	main
	PSK	123456
IPsec	Authentication algorithm	SHA-1
	Encryption algorithm	AES-128
	DH group	group 2
	IKE version	IKE v1
	Lifecycle	86400

Protocol	Parameter	Example
	Negotiation mode	esp

1. Log on to the command-line interface of the firewall device.
2. Create an ISAKMP policy.

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

3. Set the pre-shared key.

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

4. Specify the IPsec protocol.

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

5. Create network access control lists (ACLs) to specify the inbound and outbound traffic flows to be encrypted.

 **Note** If multiple CIDR blocks are configured on the firewall device, you must create a network ACL 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 0.0.0.255 192.168.11.0 0.0.0.255
```

6. Create an IPsec policy.

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

7. Apply the IPsec policy.

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

8. Configure static routes

```
ip route 192.168.10.0 255.255.255.0 47.XX.XX.161
ip route 192.168.11.0 255.255.255.0 47.XX.XX.161
```

9. Test the connectivity.

You can use a host on Alibaba Cloud and a host in the data center to test the connectivity.

Configure IKEv2 VPN

Prerequisites:

- An IPsec-VPN connection is created in a VPC on Alibaba Cloud. 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 following configuration is used in this example.

Protocol	Parameter	Example
IKE	Authentication algorithm	SHA-1
	Encryption algorithm	AES-128
	DH group	group 2
	IKE version	IKE v2
	Lifecycle	86400
	PRF algorithm	SHA-1
	PSK	123456
IPsec	Authentication algorithm	SHA-1
	Encryption algorithm	AES-128
	DH group	group 2
	IKE version	IKE v2
	Lifecycle	86400
	Negotiation mode	esp

1. Log on to the command-line interface of the firewall device.
2. Specify the algorithm that is used in IKE Phase 1 negotiations.

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

3. Create an IKEv2 policy and set an IKEv2 proposal.

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

4. Set the pre-shared key.

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

5. Configure identity verification.

```
crypto ikev2 profile ipsecpro64_v2
match identity remote address 47.XX.XX.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. Specify the IPsec protocol.

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

7. Create network ACLs to specify the inbound and outbound traffic flows to be encrypted.

 **Note** If multiple CIDR blocks are configured on the firewall device, you must create a network ACL 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 0.0.0.255 192.168.11.0 0.0.0.255
```

8. Create an IPsec policy.

```
crypto map ipsecpro64_v2 10 ipsec-isakmp
set peer 47.XX.XX.161
set transform-set ipsecpro64_v2
set pfs group2
set ikev2-profile ipsecpro64_v2
match address 100
```

9. Apply the IPsec policy.

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

10. Configure static routes

```
ip route 192.168.10.0 255.255.255.0 47.XX.XX.161
ip route 192.168.11.0 255.255.255.0 47.XX.XX.161
```

11. Test the connectivity.

You can use a host on Alibaba Cloud and a host in the data center to test the connectivity.

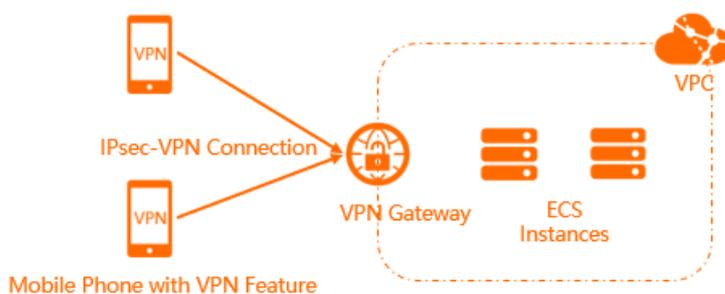
6.IPsec-VPN servers

6.1. Configure IPsec-VPN servers

VPN Gateway allows you to configure IPsec-VPN servers. Then, you can establish an IPsec-VPN connection to Alibaba Cloud by using the built-in VPN feature of your mobile client. After you establish an IPsec-VPN connection, you can use your mobile client to communicate with the resources on Alibaba Cloud.

Scenarios

IPsec-VPN servers allow you to establish end-to-site IPsec connections by using the built-in VPN feature of your mobile client. After you establish an IPsec-VPN connection, you can use your mobile client to communicate with resources on Alibaba Cloud through a secure VPN tunnel.



Limits

- IPsec-VPN servers are supported only in the following regions: .
- IPsec-VPN servers support only mobile clients that run the iOS operating system.
- You can create only one IPsec-VPN server for each VPN gateway.
- If you create an IPsec-VPN server and an SSL-VPN server for the same VPN gateway, both the IPsec-VPN server and SSL-VPN server consume the SSL connection quota of the VPN gateway.

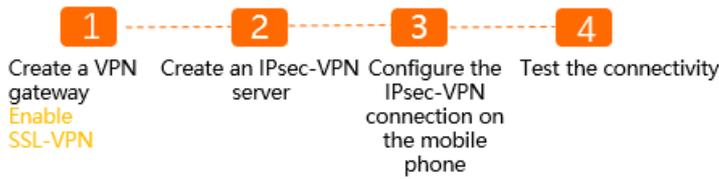
For example, the SSL connection quota that you purchase for a VPN gateway is 20, and the SSL-VPN server is connected to 5 clients. In this case, the IPsec-VPN server can be connected to at most 15 clients.

Prerequisites

Before you use an IPsec-VPN server, make sure that the following prerequisites are met:

- A virtual private cloud (VPC) is created in the region where you want to create the IPsec-VPN server. For more information, see [Create an IPv4 VPC](#).
- Your mobile client can access the Internet.
- Your mobile client runs the iOS operating system.
- The security group rules of your Elastic Compute Service (ECS) instances allow requests from the mobile client. For more information, see [Query security group rules](#) and [Add a security group rule](#).

Procedure



1. Create a VPN gateway

Create a VPN gateway and enable the SSL-VPN feature.

2. Create an IPsec-VPN server

On the IPsec-VPN server, specify the CIDR block that the mobile client wants to access and the CIDR block of the mobile client.

3. Set the IPsec-VPN connection on the mobile client

Specify the VPN gateway information on the mobile client and establish an IPsec-VPN connection.

4. Verify network connectivity

After you establish an IPsec-VPN connection between the mobile client and VPN gateway, you can verify the connectivity by connecting to a cloud resource from the mobile client.

For more information about how to use an IPsec-VPN server, see [Connect an iOS device to a VPN gateway by using the built-in VPN software](#).

References

- After you create an IPsec-VPN server, you can query the log of the IPsec-VPN server to troubleshoot errors. For more information, see [Query IPsec-VPN server logs](#).
- For more information about how to manage an IPsec-VPN server, see:
 - [创建和管理VPN网关实例](#)
 - [Create and manage IPsec servers](#)
 - [Configure a mobile client](#)

What is the difference between an IPsec-VPN server and an SSL-VPN server?

Item	IPsec-VPN server	SSL-VPN server
Scenarios	Provides end-to-site connections.	Provides end-to-site connections.
Client mode	Allows mobile clients to establish IPsec-VPN connections to Alibaba Cloud.	Allows computers to establish SSL-VPN connections to Alibaba Cloud.
Connection mode	Allows mobile clients to establish IPsec-VPN connections to Alibaba Cloud by using the built-in VPN feature.	Allows computers to establish SSL-VPN connections to Alibaba Cloud by using OpenVPN.
Encryption method	IPsec protocol	SSL certificate

6.2. Create and manage IPsec servers

You can establish an IPsec-VPN connection between an IPsec server and Alibaba Cloud by using the built-in VPN feature of your mobile phone that runs iOS. This topic describes how to create, modify, and delete an IPsec server.

Prerequisites

- You understand the limits of and prerequisites for IPsec servers. For more information, see [Limits](#) and [Prerequisites](#).
- A VPN gateway is created and the SSL-VPN feature is enabled for the VPN gateway. For more information, see [创建和管理VPN网关实例](#).

Create an IPsec server

-
-
- In the top navigation bar, select the region where you want to create the IPsec server.

Regions that support IPsec servers

- On the **IPsec-VPN Server** page, click **Create IPsec-VPN Server**.
- On the **Create IPsec-VPN Server** page, set the following parameters and click **OK**.

Parameter	Description
Name	<p>Enter a name for the IPsec 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.</p>
VPN Gateway	<p>Select the VPN gateway with which you want to associate the IPsec server.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #d9e1f2;"> <p> Note After you create an IPsec server, you cannot change the associated VPN gateway.</p> </div>
Local Network	<p>Enter the CIDR block that the client needs to access over the IPsec-VPN connection.</p> <p>The CIDR block can be the CIDR block of a virtual private cloud (VPC), a vSwitch, or a data center that is connected to a VPC through an Express Connect circuit.</p> <p>Click Add Local Network to add more CIDR blocks.</p>

Parameter	Description
Client Subnet	<p>Enter the CIDR block from which an IP address is allocated to the virtual network interface controller (NIC) of the client. Do not enter the private CIDR block of the client. When the client accesses the destination network through an IPsec-VPN connection, the VPN gateway allocates an IP address from the client CIDR block to the client.</p> <div style="background-color: #e1f5fe; padding: 10px;"> <p> Notice</p> <ul style="list-style-type: none"> ◦ Make sure that the client CIDR block does not overlap with the destination CIDR block or the CIDR blocks of vSwitches in the VPC. ◦ Make sure that the number of IP addresses that the client CIDR block provides is at least four times the number of SSL-VPN connections to the VPN gateway. <p>For example, if you specify 192.168.0.0/24 as the client CIDR block, the system first divides a subnet CIDR block with a subnet mask of 30 from 192.168.0.0/24. 192.168.0.4/30, which provides up to four IP addresses, is used as the subnet CIDR block in this example. Then, the system allocates an IP address from 192.168.0.4/30 to the client and uses the other three IP addresses to ensure network communication. In this case, one client consumes four IP addresses. Therefore, make sure that the number of IP addresses that the client CIDR block provides is at least four times the number of SSL-VPN connections to the VPN gateway.</p> </div>
Pre-Shared Key	<p>Enter the pre-shared key of the IPsec server. The key is used for authentication between the IPsec server and the client. The key must be 1 to 100 characters in length.</p> <p>If you do not specify a pre-shared key, the system generates a random 16-bit string as the pre-shared key. After you create an IPsec server, you can click Edit to view the pre-shared key that is generated by the system. For more information, see Modify an IPsec server.</p> <div style="background-color: #e1f5fe; padding: 10px;"> <p> Notice The authentication key of the client must be the same as the pre-shared key of the IPsec server. Otherwise, you cannot establish a connection between the client and the IPsec server.</p> </div>
Effective Immediately	<p>Specify whether to immediately start negotiations.</p> <ul style="list-style-type: none"> ◦ Yes: starts negotiations after the configuration is completed. ◦ No: starts negotiations when inbound traffic is detected.
Advanced Configuration: IKE Configurations	

Parameter	Description
Version	<p>Select the version of the IKE protocol.</p> <ul style="list-style-type: none"> ◦ ikev1 ◦ ikev2 <p>IKEv1 and IKEv2 are supported. Compared with IKEv1, IKEv2 simplifies the negotiation process and provides better support for scenarios where multiple subnets are used. We recommend that you select IKEv2.</p>
LocalId	<p>Enter the identifier of the IPsec server. You can enter an IP address or a value that is in Fully Qualified Domain Name (FQDN) format. The default value is the public IP address of the VPN gateway.</p>
RemoteId	<p>Enter the identifier of the client. You can enter an IP address or a value that is in FQDN format. This parameter is left empty by default.</p>

Modify an IPsec server

- 1.
 - 2.
 - 3.
 4. On the **IPsec-VPN Server** page, find the IPsec server that you want to manage, and click **Edit** in the **Actions** column.
 5. On the **Edit IPsec-VPN Server** page, modify the configurations of the IPsec server and click **OK**.
- For more information about the parameters, see [Create an IPsec server](#).

Delete an IPsec server

When you delete an IPsec server, the IPsec server is automatically disconnected from clients.

- 1.
- 2.
- 3.
4. On the **IPsec-VPN Server** page, find the IPsec server that you want to delete and click **Delete** in the **Actions** column.
5. In the **Delete IPsec-VPN Server** message, confirm the information and click **OK**.

References

- [CreateIpsecServer](#): creates an IPsec server.
- [ListIpsecServers](#): queries IPsec servers.
- [UpdateIpsecServer](#): modifies the configurations of an IPsec server.
- [DeleteIpsecServer](#): deletes an IPsec server.

6.3. Configure a mobile client

After you create an IPsec-VPN server, you must configure a mobile client before you can establish IPsec-VPN connections between the mobile client and Alibaba Cloud.

Prerequisites

Before you start, make sure that the following requirements are met:

- An IPsec-VPN server is created. For more information, see [Create and manage IPsec servers](#).
- The following information is obtained in the VPN Gateway console:
 - The public IP address of the VPN gateway that is associated with the IPsec-VPN server.
 - The version of the IKE protocol used by the IPsec-VPN server.
 - The pre-shared key used by the IPsec-VPN server.

Configure an iOS client

IPsec-VPN servers support only mobile phones that run an iOS operating system. In this topic, iOS 14 is used as an example to describe how to configure a mobile client.

1. Open **Settings** on your mobile phone.
2. Choose **General > VPN > Add VPN Configuration**.
3. On the **Add Configurations** page, set the following parameters.
 - **Type**: Select a VPN protocol.
The IKE version that you set for this parameter must be the same as that of the IPsec-VPN server.
 - **Description**: Enter a description for the VPN.
 - **Server**: Enter the public IP address of the VPN gateway to which you want to connect by using the mobile client.
 - **Remote ID**: Enter the public IP address of the VPN gateway to which you want to connect by using the mobile client.
 - **Local ID**: Enter the identifier of the mobile client. You can leave this parameter empty.
 - **User Authentication**: Select **None**.
 - **Use Certificate**: Turn off the switch.
 - **Secret**: Enter the secret that is used for identity verification between the IPsec-VPN server and the mobile client. An IPsec-VPN connection can be established only when both ends use the same secret.
In this example, the pre-shared key of the IPsec-VPN server is used.
 - **Proxy**: Select **Off**.
4. Click **Done**.
5. On the **VPN** page, select the VPN configuration and turn on the **Status** switch.
If the status displays **Connected**, it indicates that the IPsec-VPN connection is established.

6.4. Query IPsec-VPN server logs

You can troubleshoot errors of an IPsec-VPN server by querying its logs.

Context

The system automatically retains the logs that were generated within the last month for an IPsec-VPN server. You can query logs in batches. You can query a log with a duration of at most 10 minutes.

Procedure

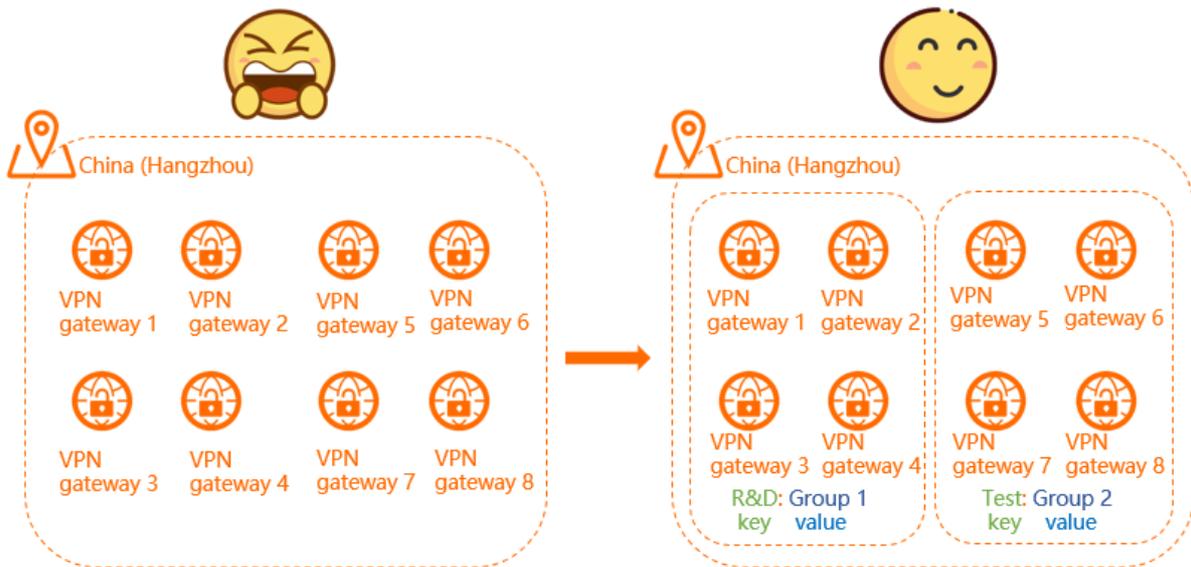
- 1.
- 2.
- 3.
4. On the **IPsec-VPN Server** page, find the IPsec-VPN server that you want to manage, and click **View Logs** in the **Actions** column.
5. On the **IPsec-VPN Server Logs** page, query logs by specifying the period of time when the logs are generated.

7.Tag management

7.1. 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	

7.2. Attach tags

7.2.1. 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.
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>aliyun</code> or <code>acs:</code> . It cannot contain <code>http://</code> or <code>https://</code> .

Related information

- [TagResources](#)

7.2.2. 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:

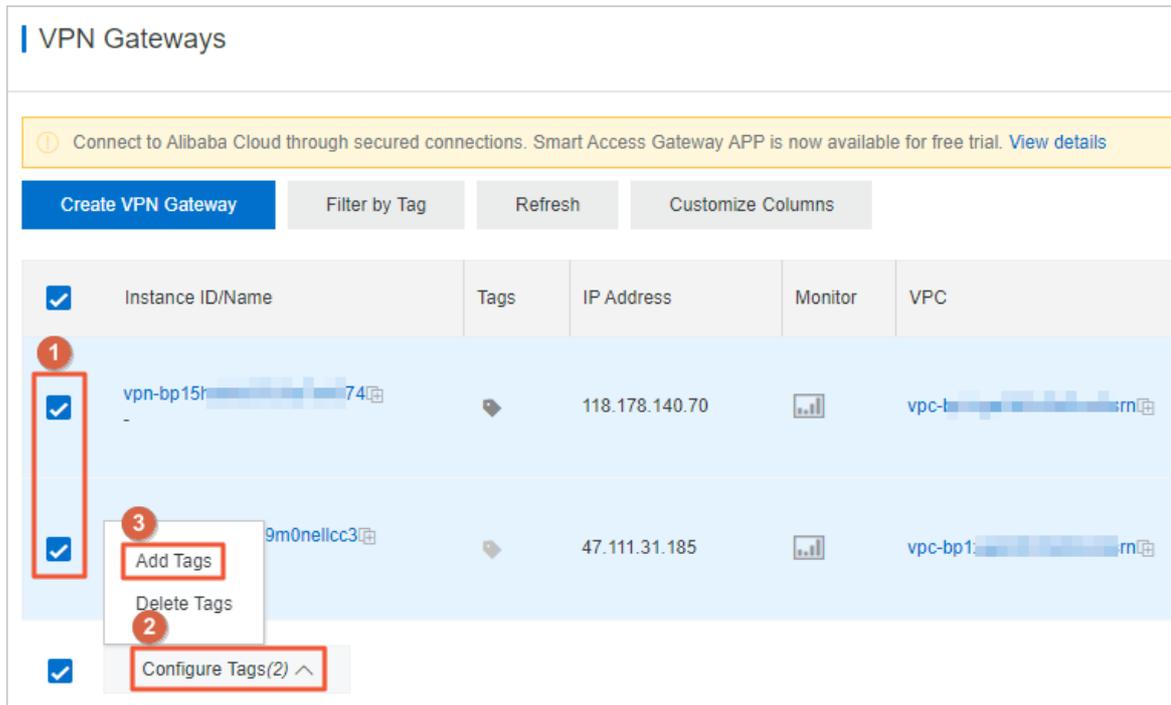
- The keys of tags that are attached to the same VPN gateway must be unique.
- Tags must be attached to VPN gateways.
- Tag information is not shared across regions.

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.
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**.



4. 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

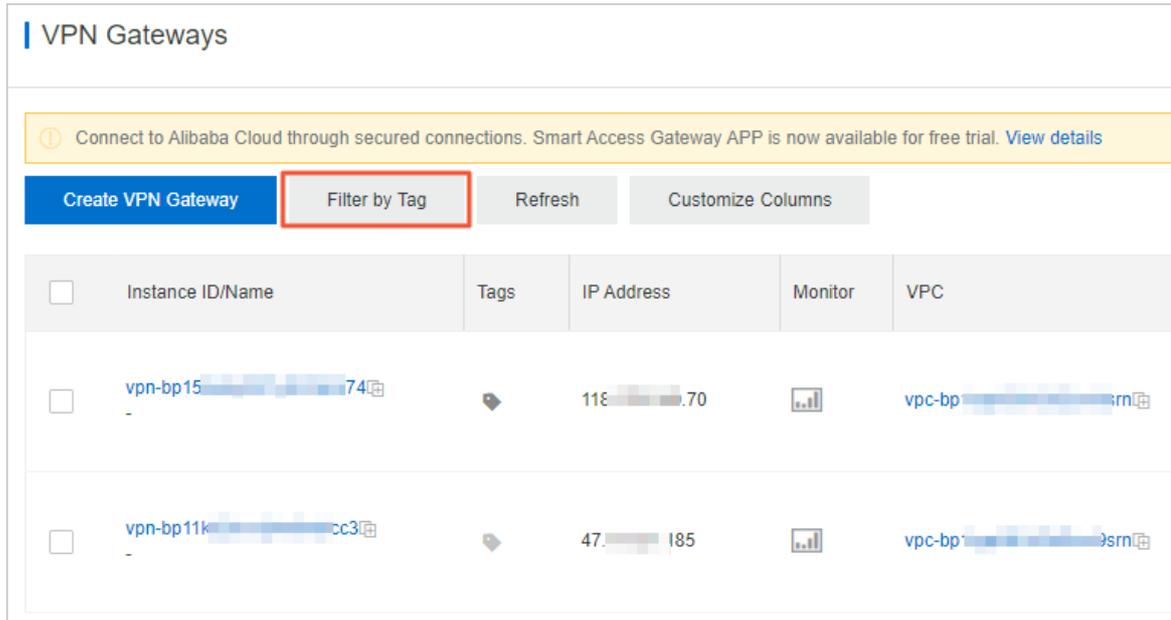
- [TagResources](#)

7.3. Search VPN gateways by tag

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

Procedure

- 1.
2. In the top navigation bar, select the region where the VPN gateway is deployed.
3. On the **VPN Gateways** page, click the **Filter by Tag** tab.



4. 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

- [List Tag Resources](#)

7.4. Remove tags

7.4.1. 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

- 1.
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 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.
4. 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.

5. Click **OK**.

Related information

- [UnTagResources](#)

7.4.2. 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.

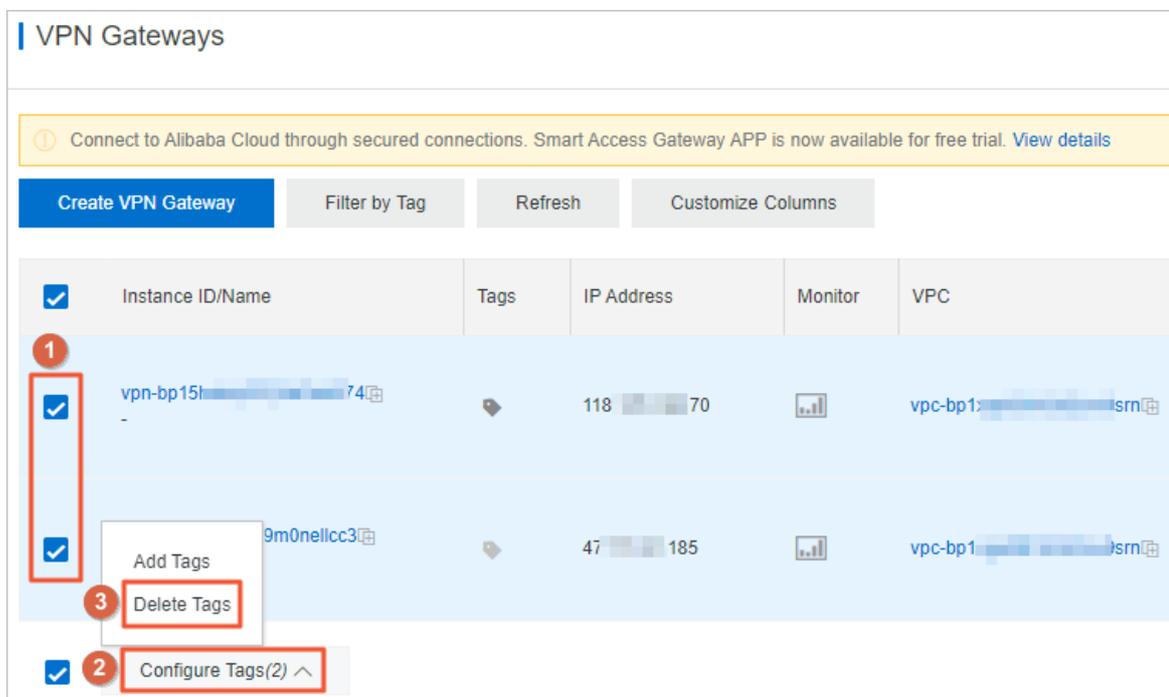
Context

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

- 1.
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 from which you want to remove tags, and choose **Configure Tags > Delete Tags**.



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

Related information

- [UnTagResources](#)

8. Manage quotas

This topic describes how to query the quota usage of a cloud resource in the VPN Gateway console. If the remaining quota of a resource cannot meet your business requirements, you can apply for a quota increase.

Procedure

- 1.
2. In the left-side navigation pane, choose **O&M and Monitoring > Quota Management**.
3. On the **Quota Management** page, click the **VPN Gateways** tab to view the quota usage.
4. To request a quota increase, click **Submit Application** in the **Actions** column.
 - **Requested Value**: the number of resources that you require. The number must be greater than the current quota. For more information about default quota limits, see [使用限制](#).
 - **Reason**: the reason for the application, including business scenarios and necessity.
 - **Email**: the email address of the applicant.
5. Click **OK**.

The system automatically reviews your application. You can check whether your application is approved based on the application state: **Rejected** or **Approved**. After your application is approved, the quota is increased to the specified quantity.

To view the quota increase history, click **History** in the **Actions** column.