Alibaba Cloud
vpn gateway

User Guide

Issue: 20181130

Legal disclaimer

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

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

secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion , or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos , marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

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

Contents

1 Manage a VPN Gateway

Create a VPN Gateway to enable SSL-VPN and IPsec-VPN connectivity. After a VPN Gateway is created, a public IP is allocated to it.

Create a VPN gateway

Follow these steps to create a VPN gateway:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **VPN Gateways**.
3. On the **VPN Gateways** page, click **Create VPN Gateway**.
4. Configure the VPN gateway according to the following information, and click **Buy Now**.

Configuration	Description
Region	Select the region of the VPN Gateway. If you want to use IPsec-VPN to connect a VPC to a local data center or other VPCs, make sure that the VPN Gateway and the VPC are in the same region.
VPC	Select the VPC associated with the VPN Gateway.
Bandwidth	Select the Internet bandwidth of the VPN Gateway. The bandwidth specification is the Internet bandwidth of the VPN gateway.
IPsec-VPN	Enable IPsec-VPN. With IPsec-VPN enabled, you can create a site-to-site connection over the IPsec tunnel to connect a local data center to a VPC, or connect two VPCs.
SSL-VPN	Enable SSL-VPN. With SSL-VPN enabled, you can create a point-to-site connection. The client can directly access the VPC from a remote location without configuring a client gateway.
Purchase Duration	Select the purchase duration.
Auto renew	Select whether to enable auto renew: • If VPN Gateway is billed monthly, renewal cycle is month. • If VPN Gateway is billed yearly, the auto renewal cycle is year.

Edit a VPN gateway

Follow these steps to edit the name and description of a VPN gateway:

1. Log on to the VPC console.

2. In the left-side navigation pane, click **VPN** > **VPN Gateways**.
3. On the **VPN Gateways** page, select the region of the VPN Gateway.
4. Click **Edit** in the **Actions** column of the target VPN Gateway.

2 Manage a customer gateway

When using an IPsec-VPN connection to build a site-to-site connection, you must create a customer gateway. By creating a customer gateway, you can register the configurations of the local gateway to Alibaba Cloud. One customer gateway can be connected to multiple VPN Gateways.

Create a customer gateway

Follow these steps to create a customer gateway:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **Customer Gateways**.
3. Select the region of the customer gateway.

   The customer gateway and the VPN Gateway you are connecting must be in the same region.
4. On the **Customer Gateways** page, click **Create Customer Gateway**.
5. Configure the customer gateway according to the following information.

Configuration	Description
Name	The name of the customer gateway. The name can contain 2-128 English letters, numbers, hyphens, or underlines, and must start with English letters.
IP Address	The static public IP address configured for the gateway in the local data center.
Description	The description of the customer gateway. The description can contain from 2 to 256 characters and cannot begin with http:// or https://.

6. (Optional) Click **+Add** to add another customer gateway.
7. Click **OK**.

Edit a customer gateway

Follow these steps to edit the name and description of a customer gateway:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **Customer Gateways**.
3. Select the region of the target customer gateway.
4. Click **Edit** in the **Actions** column of the target customer gateway.
5. Modify the name and description of the customer gateway.

Delete a user gateway

Follow these steps to delete a customer gateway:

> **Note:**
> Before deleting a customer gateway, you must first delete the IPsec connection associated with the customer gateway.

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **Customer Gateways**.
3. Select the region of the target customer gateway.
4. Click **Delete** in the **Actions** column of the target customer gateway.
5. In the displayed dialog box, click **OK**.

3 Manage an IPsec connection

After creating a VPN Gateway and a customer gateway, you can create an IPsec connection. The IPsec connection allows you to connect the VPN Gateway and the customer gateway, thus establishing a VPN tunnel.

Create an IPsec connection

Follow these steps to create an IPsec connection:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **IPsec Connections**.
3. On the **IPsec Connections** page, select the region of the IPsec connection.
4. Click **Create IPsec connection**.
5. Configure the IPsec connection according to the following information and click **OK**.

Configuration	Description
Name	Enter the name of the IPsec connection. The name can contain 2-128 English letters, numbers, hyphens, or underscores, and must start with English letters.
VPN Gateway	Select the VPN Gateway to connect.
Customer Gateway	Select the customer gateway to connect.
Local Network	Enter the IP address range of the VPC to be connected with the local data center, which is used for second-stage negotiation. You can enter multiple IP address ranges and separate them by commas. For example, 192.168.1.0/24, 192.168.2.0/24. **Note:** If multiple IP address ranges are entered, the IKEv2 must be selected.
Remote Network	Enter the IP address range of the local data center to be connected with the VPC. This is used for second-stage negotiation. You can enter multiple IP address ranges and separate them by commas. For example, 172.10.1.0/24,172.10.2.0/24. **Note:** If multiple IP address ranges are entered, the IKEv2 must be selected.

Configuration	Description
Effective Immediately	Choose whether to delete the established IPsec tunnel and restart the negotiation. • Yes: Start the negotiation immediately once the configuration is complete. • No: Start the negotiation only when there is incoming traffic.
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 enter a specific 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	Select the negotiation mode of the IKEv1. • Main mode: The negotiation process features high security. • Aggressive mode: The negotiation is fast and the success rate of negotiation is high. After the negotiation succeeds, the information transmission security is the same for the two modes.
Encryption Algorithm	Select an encryption algorithm used by first-stage negotiation from the following options: aes, aes192, aes256, des, and 3des.
Authentication Algorithm	Select an authentication algorithm used by first-stage negotiation from the following options: sha1 or md5.
DH Group	Select a Diffie-Hellman key exchange algorithm used by first-stage negotiation.
SA Life Cycle (seconds)	Set the SA lifecycle for the first-stage negotiation. The default value is 86,400 seconds.
LocalId	It is the identification of the VPN Gateway used for the first-stage 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.
RemoteId	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 RemoteId in the FQDN format, we

Configuration	Description
	recommend that you change the negotiation mode to the aggressive mode.
Advanced Configuration: IPSec Configuration	
Encryption Algorithm	Select the encryption algorithm of second-stage negotiation from the following options: aes, aes192, aes256, des, or 3des.
Authentication Algorithm	Select an authentication algorithm used by second-stage negotiation from the following options: sha1 or md5.
DH Group	Select a Diffie-Hellman key exchange algorithm used by second-stage negotiation. • 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 the second-stage negotiation. The default value is 86,400 seconds.

Download the configuration

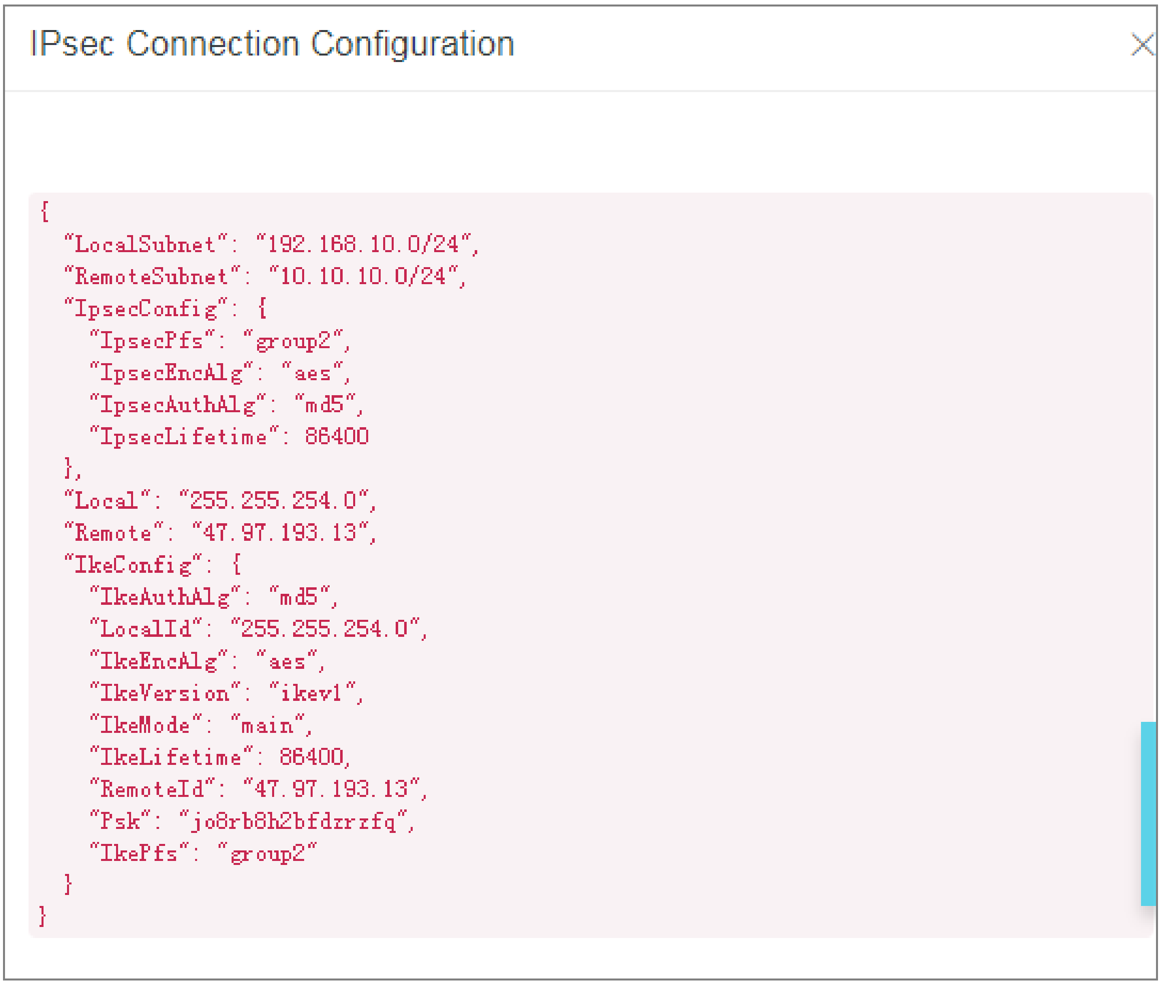
After the IPsec connection is configured and the negotiation succeeds, you can download the IPsec connection configuration and configure the local gateway. For more information, see *Configure H3C firewallConfigure strongSwan*.

Follow these steps to download the IPsec connection configuration:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **IPsec Connections**.
3. On the **IPsec Connections** page, select the region of the target IPsec connection.
4. Click **Download Config** in the **Actions** column of the target IPsec connection.

   The RemoteSubnet and LocalSubnet in the download configuration are opposite to the local network and the remote network when creating an IPsec connection. From the perspective of VPN Gateway, the remote network is the local IDC and the local network is the VPC; while from the perspective of local IDC, the remote network is the VPC and the local network is the local IDC.

   For example, if you set the local network to 192.168.0.0/16 and the remote network to 10.0.0.0/8 in an IPsec connection, the downloaded IPsec connection configuration is as follows:



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

Edit an IPsec connection

Follow these steps to edit an IPsec connection:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **IPsec Connections**.
3. On the **IPsec Connections** page, select the region of the target IPsec connection.
4. Click **Edit** in the **Actions** column of the target IPsec connection.

Delete an IPsec connection

Follow these steps to delete an IPsec connection:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **IPsec Connections**.
3. On the **IPsec Connections** page, select the region of the target IPsec connection.
4. Click **Delete** in the **Actions** column of the target IPsec connection.
5. In the displayed dialog box, click **OK**.

View IPsec connection logs

You can view the IPsec connection logs in the previous month. You can troubleshoot IPsec connection errors by analyzing the connection logs. The maximum time range is 10 minutes.

Follow these steps to view IPsec connection logs:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **IPsec Connections**.
3. On the **IPsec Connections** page, select the region of the target IPsec connection.
4. Click **View Logs** in the **Actions** column of the target IPsec connection.
5. On the displayed page, configure the time range of the logs to view.

4 Manage an SSL server

To create a point-to-site connection, you must create an SSL server to specify the network that you want to connect.

Create an SSL server

Follow these steps to create an SSL server:

1. In the left-side navigation pane, click **VPN** > **SSL Servers**.
2. On the **SSL Servers** page, select a region.
3. Click **Create SSL Server**.
4. Configure the SSL server according to the following information, and click **OK**.

Configuration	Description
Name	The name of the SSL server. The name can contain 2-128 English letters, numbers, hyphens, or underlines, and must start with English letters.
VPN Gateway	The associated VPN gateway. Make sure that you have enabled the SSL-VPN function.
Local Network	The local network is the IP address range to be accessed by the client through SSL-VPN. It can be the IP address range of a VPC, a VSwitch, a local data center connected to a VPC through a leased line, or a cloud service such as RDS or OSS. Click **Add Local Network** to add more local networks. **Note:** The subnet mask of the local network must be /16 to /29.
Client Subnet	The client subnet is the IP address range of which an IP address will be allocated to the virtual network card of the client. The client uses the allocated IP address to access the local network. It is not the existing intranet IP address range of the client. **Note:** Make sure that the client subnet and the local network do not conflict with each other.
Advanced Configuration	
Protocol	The protocol used by the SSL connection: UDP or TCP. We recommend that you use the UDP protocol.

Configuration	Description
Port	The port used by the SSL connection. The default value is 1194.
Encryption Algorithm	The encryption algorithm used by the SSL connection: AES-128-CBC , AES-192-CBC, or AES-256-CBC
Enable Compression	Whether to enable compression.

Edit an SSL server

Follow these steps to edit an SSL server:

1. In the left-side navigation pane, click **VPN** > **SSL Servers**.
2. On the **SSL Servers** page, select the region of the target SSL server.
3. Click **Edit** in the **Actions** column of the target SSL server.

Delete an SSL server

Follow these steps to delete an SSL server:

1. In the left-side navigation pane, click **VPN** > **SSL Servers**.
2. On the **SSL Servers** page, select the region of the target SSL server.
3. Click **Delete** in the **Actions** column of the target SSL server.
4. In the displayed dialog box, click **OK**.

5 Manage an SSL client

Before enabling the SSL-VPN feature to build a site-to-site connection, you must create a client certificate.

Create client certificates

Follow these steps to create client certificates:

1. In the left-side navigation pane, click **VPN** > **SSL Clients**.
2. On the **SSL Clients** page, select a region.
3. Click **Create Client Certificate**.
4. Configure the client certificate according to the following information.

Configuration	Description
Name	The name of the SSL client certificate. The name can contain from 2 to 128 characters. It must begin with English letters, and can contain numbers, hyphens, and underlines.
SSL Server	The associated SSL server.

Download client certificates

Follow these steps to download the client certificates:

1. In the left-side navigation pane, click **VPN** > **SSL Clients**.
2. On the **SSL Clients** page, select the region of the target client certificate.
3. Click **Download** in the **Actions** column of the target client certificate.

Delete client certificates

Follow these steps to delete client certificates:

1. In the left-side navigation pane, click **VPN** > **SSL Clients**.
2. On the **SSL Clients** page, select the region of the target client certificate.
3. Click **Delete** in the **Actions** column of the target client certificate.
4. In the displayed dialog box, click **OK**.

6 Enable SSL-VPN and IPsec-VPN

If you do not enable SSL-VPN or IPsec-VPN when creating the VPN Gateway, you can enable it later.

Note:
To enable the SSL-VPN function of a VPN Gateway created before January 20, 2018, submit a ticket. For a VPN Gateway created after January 20, 2018, you can enable the function on the console directly.

Enable IPsec-VPN

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **VPN Gateways**.
3. Select the region of the target VPN Gateway.
4. Click **Enable** in the **Enable IPsec** column of the target VPN Gateway.
5. On the purchase page, complete the payment.

Enable SSL-VPN

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **VPN Gateways**.
3. Select the region of the target VPN Gateway.
4. Click **Enable** in the **Enable SSL** column of the target VPN Gateway.
5. On the purchase page, complete the payment.

7 Modify the bandwidth of a VPN gateway

You can modify the bandwidth of a VPN gateway anytime and the modification takes effect immediately.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **VPN Gateways**.
3. Select the region of the target VPN Gateway.
4. Click **Modify Configuration** in the **Bandwidth** column of the target VPN Gateway.
5. On the purchase page, select a new bandwidth specification and complete the payment process.

8 Modify the number of SSL connections

You can modify the number of clients connected to a VPN gateway at the same time according to your business needs.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VPN** > **VPN Gateways**.
3. Select the region of the target VPN Gateway.
4. Click **Modify Configuration** in the **Concurrent SSL Connections** column of the target VPN Gateway.
5. On the purchase page, select a new number of SSL connections and complete the payment process.