ALIBABA CLOUD

Alibaba Cloud

VPN Gateway

SSL-VPN Quick Start

Document Version: 20210908

Alibaba Cloud

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

Table of Contents

1.Overview of SSL-VPN

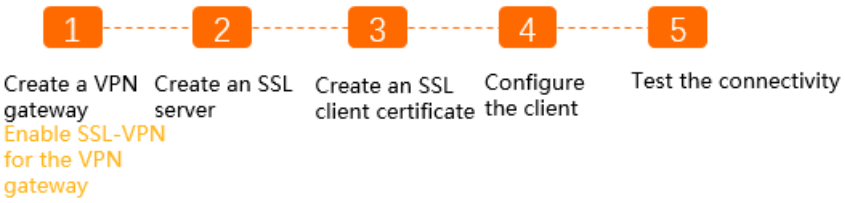
SSL-VPN allows clients to connect to a virtual private cloud (VPC) and access applications and services that are deployed in the VPC in a secure manner. This topic describes how to use SSL-VPN.

Prerequisites

Before you use SSL-VPN to establish a connection between a client and a VPC, make sure that the following prerequisites are met:

- The private CIDR block of the client and the private CIDR block of the VPC do not overlap. Otherwise, the client and the VPC cannot communicate with each other.
- The client can access the Internet.
- You have read and understand the security group rules that apply to the Elastic Compute Service (ECS) instances in the VPC, and the security rules allow the client to access cloud resources. For more information, see Query security group rules.

Procedure



1. Create a VPN gateway.

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

2. Create an SSL server.

   On the SSL server, specify the private CIDR block that the client needs to access and the CIDR block that is used by the client.

3. Create an SSL client certificate

   Create and download a client certificate based on the SSL server configuration.

4. Configure the client.

   Download and install VPN software on the client, load the SSL client certificate, and then initiate an SSL-VPN connection.

5. Test the connectivity.

   Open the CLI on the client, and run the **ping** command to ping an ECS instance in the VPC.

Basic scenarios

Connect a client to a VPC

2.Connect a client to a VPC

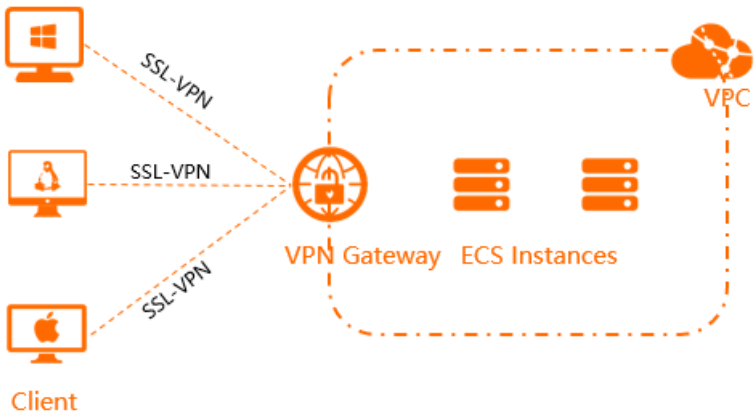
This topic describes how to connect a client to a virtual private cloud (VPC) by using SSL-VPN.

Prerequisites

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, create an Alibaba Cloud account.
- The private CIDR block of the client and the private CIDR block of the VPC do not overlap. Otherwise, the client and the VPC cannot communicate with each other.
- The client can access the Internet.
- You have read and understand the security group rules that apply to the ECS instances in the VPC, and the security group rules allow gateway devices in the data center to access cloud resources. For more information, see Query security group rules.

Context

The scenario in the following figure is used as an example to describe how Linux, Windows, and Mac clients connect to a VPC by using SSL-VPN.



Step 1: Create a VPN gateway

1. Log on to the VPN gateway console.
2. On the **VPN Gateways** page, click **Create VPN Gateway**.
3. On the buy page, set the parameters of the VPN gateway, click **Buy Now**, and then complete the payment.
   - **Name**: Enter a name for the VPN gateway.
   - **Region**:Select the region where you want to deploy the VPN gateway.

     > **Note** Make sure that the VPC and the VPN gateway are deployed in the same region.

   - **VPC**:Select the VPC to be associated with the VPN gateway.
   - **Specify VSwitch**: Specify whether to create the VPN gateway in a vSwitch of the VPC. **No** is selected in this example.

     If you select **Yes**, you must specify a **vSwitch**.

- **Peak Bandwidth**: Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s. The bandwidth is used for data transfer over the Internet.
- **Traffic**: By default, the VPN gateway uses the pay-by-data-transfer billing method. For more information, see Pay-as-you-go.
- **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway. In this example, **Disable** is selected.
- **SSL-VPN**: Specify whether to enable SSL-VPN for the VPN gateway. In this example, **Enable** is selected.
- **SSL connections**: Specify the maximum number of concurrent SSL-VPN connections that the VPN gateway supports.

  > **Note** This parameter is available only after you enable the SSL-VPN feature.

- **Duration**: By default, the VPN gateway is billed on an hourly basis.

4. Return to the **VPN Gateways** page to view the VPN gateway that you created.

   The newly created VPN gateway is in the **Preparing** state. The VPN gateway changes to the **Normal** state after about 1 to 5 minutes. After the VPN gateway changes to the **Normal** state, the VPN gateway is ready for use.

Step 2: Create an SSL server

1. In the left-side navigation pane, choose **Interconnections > VPN > SSL Servers**.
2. In the top navigation bar, select the region where you want to create the SSL server.

   > **Note** Make sure that the SSL server and the VPN gateway that you created are deployed in the same region.

3. On the **SSL Server** page, click **Create SSL Server**.
4. In the **Create SSL Server** panel, set the following parameters and click **OK**.
   - **Name**: Enter a name for the SSL server.
   - **VPN Gateway**: Select that VPN gateway that you created.
   - **Local Network**: Enter the CIDR block of the network to which you want to connect. Click **Add Local Network** to add more CIDR blocks. You can add the CIDR block of a VPC, a vSwitch, or an on-premises network.
   - **Client Subnet**: Enter the CIDR block that the client uses to connect to the SSL server.

> **Notice**
>
> - Make sure that the CIDR block of the destination network and the client CIDR block do not overlap with each other.
> - 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.
>
> 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, to ensure that an IP address can be allocated to your client, you must 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.

- **Advanced Configuration**: Use default advanced configurations.

For more information, see Create an SSL server.

Step 3: Create and download an SSL client certificate

1. In the left-side navigation pane, choose **Interconnections > VPN > SSL Clients**.
2. On the **SSL Client** page, click **Create Client Certificate**.
3. In the **Create Client Certificate** panel, enter a name for the SSL client certificate, select an SSL server, and then click **OK**.
4. On the **SSL Client** page, find the SSL client certificate that you created and click **Download** in the **Actions** column.

   The SSL client certificate is downloaded to your on-premises device.

Step 4: Configure the client

The following section describes how to configure Linux, Mac, and Windows clients.

- Linux client
  i. Run the following command to install OpenVPN:

  ```
  yum install -y openvpn
  ```

  ii. Decompress the SSL client certificate package that you downloaded and copy the SSL client certificate to */etc/openvpn/conf/*.

  iii. Go to the */etc/openvpn/conf/* directory and run the following command to start the OpenVPN client:

  ```
  openvpn --config /etc/openvpn/conf/config.ovpn --daemon
  ```

- Windows client
  i. Download and install the OpenVPN client.

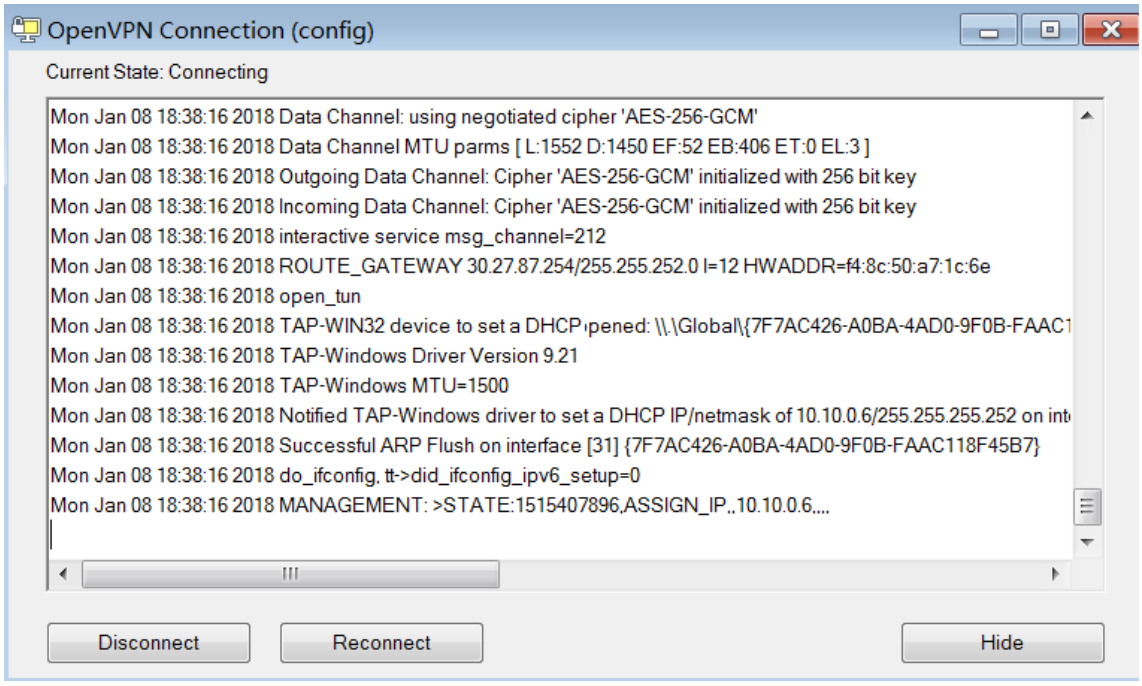
  Download OpenVPN.

  ii. Decompress the downloaded SSL client certificate package and copy the SSL client certificate to

the *OpenVPN\config* directory.

In this example, the certificate is copied to the *C:\Program Files\OpenVPN\config* directory. You must copy the certificate to the directory where the OpenVPN client is installed.

iii. Start the OpenVPN client and click **Connect** to initiate a connection.



- Mac client

  i. Run the following command to install OpenVPN:

  ```
  brew install openvpn
  ```

  > **Note** Make sure that homebrew is installed before you install OpenVPN.

  ii. Copy the SSL client certificate package that you downloaded in Step 3 to the configuration directory of the OpenVPN client and decompress the package. Then, initiate an SSL-VPN connection.

  a. Back up all configuration files in the */usr/local/etc/openvpn* folder.

  b. Run the following command to delete the configuration files of the OpenVPN client:

  ```
  rm /usr/local/etc/openvpn/*
  ```

  c. Run the following command to copy the downloaded SSL client certificate package to the configuration directory of the OpenVPN client:

  ```
  cp cert_location /usr/local/etc/openvpn/
  ```

  In the preceding command, replace `cert_location` with the directory to which the SSL client certificate package is downloaded in Step 3. For example: */Users/example/Downloads/certs6.zip*.

d. Run the following command to decompress the SSL client certificate package:

```
cd /usr/local/etc/openvpn/
unzip /usr/local/etc/openvpn/certs6.zip
```

e. Run the following command to initiate a connection:

```
sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
```

Step 5: Test the connectivity

1. Open the CLI on the client.
2. To test the connectivity, you can run the **ping** command to access an Elastic Compute Service (ECS) instance in the VPC.