

Alibaba Cloud vpn gateway

SSL-VPN Quick Start

Issue: 20181129

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 .
<i>Courier font</i>	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand / slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Tutorial overview.....	1
2 Linux client remote access.....	2
3 Windows client remote access.....	7
4 Mac client remote access.....	12

1 Tutorial overview

The tutorials illustrate how to use SSL-VPN to connect a VPC from a remote computer using the Linux, Windows, and Mac operating systems.

Prerequisites

Switch to the new VPC console.

Procedure

Follow these steps to access the VPC from the client using the SSL-VPN feature:

1. Create a VPN Gateway

Create a VPN Gateway with SSL-VPN enabled.

2. Create an SSL server

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

3. Create a client certificate

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

4. Configure the client

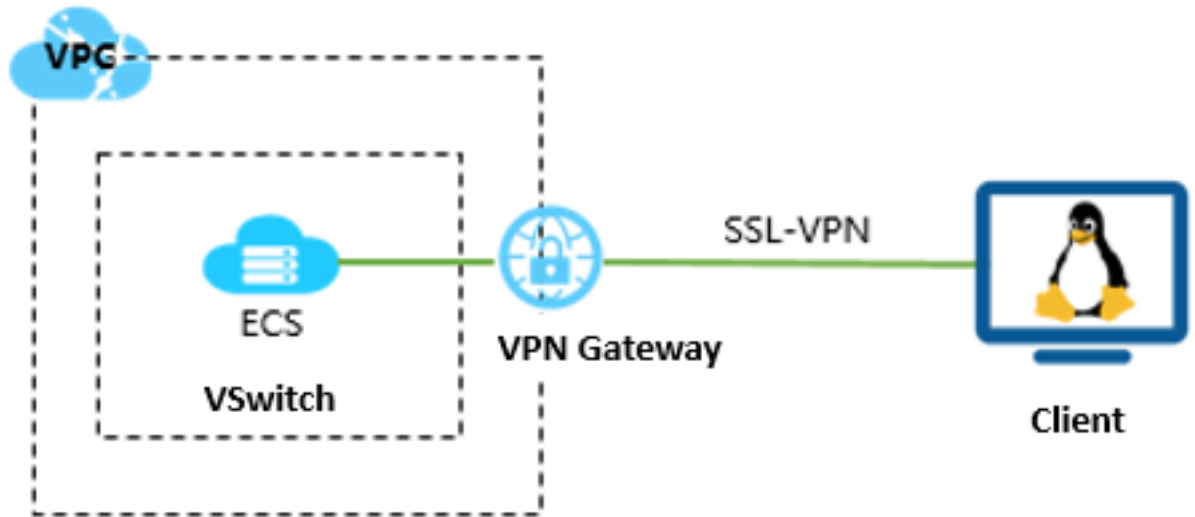
Download and install the client VPN software in the client, load the client certificate and configurations, and initiate the connection.

5. Configure security rules

Make sure the security group rules of the ECS instance allow remote access.

2 Linux client remote access

This document illustrates how to use SSL-VPN to connect a VPC from a remote computer of the Linux operating system.



Prerequisites

Before deploying the VPN Gateway, make sure that the following conditions are met:

- The IP address ranges of the VPC and the remote computer are not in conflict.
- The client can access the Internet.

Step 1: 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. On the purchase page, configure the VPN gateway and complete the payment. In this tutorial, the VPN gateway uses the following configurations:
 - **Region:** Select the region of the VPN gateway. In this tutorial, **China (Hangzhou)** is selected.



Note:

Make sure that the VPC and the VPN gateway are in the same region.

- **VPC:** Select the VPC to be connected.
- **Bandwidth specification:** Select a bandwidth specification. The bandwidth specification is the Internet bandwidth of the VPN gateway.
- **IPsec-VPN:** Select whether to enable the IPsec-VPN feature. The IPsec-VPN feature applies to site-to-site connections and can be enabled according to your actual needs.
- **SSL-VPN:** Select whether to enable the SSL-VPN feature. The SSL-VPN feature allows you to connect to a VPC from a single computer anywhere. In this tutorial, select **Enable**.
- **Concurrent SSL Connections:** Select the maximum number of clients you want to connect to simultaneously.

**Note:**

You can only configure this option after you enables the SSL-VPN feature.

Basic Configuration	Region	China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)
		Hong Kong	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
		UAE (Dubai)	Germany (Frankfurt)	China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
		UK(London)					
	Name	<input type="text"/>					
	VPC	emr_test_vpc					
	Peak Bandwidth	10 Mbps		100 Mbps			
	Billing Method	Pay By Traffic					
VPN	IPsec-VPN	enable		disable			
	SSL-VPN	disable		enable			

5. Go back to the VPN Gateways page, select China (Hangzhou) region to view the created VPN Gateway.

The initial status of a VPN Gateway is Preparing. It changes to Normal in about 2 minutes.

When it changes to Normal, it indicates that the VPN Gateway is ready to use.

**Note:**

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

VPN Gateways											
Create VPN Gateway Refresh Custom			Instance ID ▾		Enter a name or ID						
Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Enable IPsec	Enable SSL	Concurrent SSL Connections	Description	Actions
vpn2	47.97.193.13		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 01/25/2018, 14:41:45 Created	Enabled	Enable SSL	-	-	Delete
vpn2	47.97.209.47		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 02/11/2018, 17:53:25 Created	Enabled	Enabled	5 Upgrade downgrade	-	Delete

Step 2: Create an SSL server

1. In the left-hand navigation pane, click **VPN > SSL Servers**.
2. Click **Create SSL Server**. In this tutorial, the configurations of the SSL server is as follows:
 - **Name:** Enter a name for the SSL server.
 - **VPN Gateway:** Select the created VPN Gateway.
 - **Local Network:** Enter the CIDR block of the network to be connected. Click **Add Local Network** to add multiple local networks. The local network can be the CIDR block of any VPC or VSwitch, or the CIDR block of the local network.
 - **Client Subnet:** Enter the IP addresses used by the client to connect the server in the form of CIDR block.
 - **Advanced Configuration:** Use the default advanced configuration.

SSL Servers

Create SSL Server Refresh Custom

Instance ID/Name	IP Address	VPN Gateway
vss-bp15prztev8lvop9b74d2server1	47.97.209.47	vpn-bp19uhlxmy47kqf5acwl

Create SSL Server

VPN Gateway
vpn2/vpn-bp111s8uqu8782z8ee43

Local Network
192.168.0.0/16

[Add Local Network](#)

Client Subnet
10.10.0.0/24

Note: The client subnet IP range cannot overlap the VPC VSwitch subnet IP range.

Advanced Configuration
☒

Protocol
UDP

Port
1194

Encryption Algorithm
AES-128-CBC

Enable Compression
No

OK Cancel

Step 3: Create a client certificate

1. In the left-side navigation pane, click **VPN > SSL Clients**.
2. Click **Create Client Certificate**.
3. On the **Create Client Certificate** page, enter a name, and then select the corresponding SSL server. Click **OK**.
4. On the **SSL Clients** page, find the created SSL client certificate, and then click **Download**.

SSL Clients					
<div>Create Client Certificate Refresh Custom</div>					
Instance ID/Name	SSL Server	Status	Created At	Expiration Date	Actions
u Client	vs2 server1	Normal	10/17/2018, 19:09:01	10/16/2021, 19:09:01	Download Delete

Step 4: Configure Linux clients

1. Run the following command to install the OpenVPN client.

```
yum install -y openvpn
```

2. Extract the client certificates downloaded in the step 3 and copy the certificates to the `/etc/openvpn/conf/` directory.
3. Run the following command to start the OpenVPN.

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

Step 5: Verify the connection

On the client, ping the private IP address of an ECS instance in the connected VPC network to verify the connection.



Note:

Make sure that the security rule of the ECS instance allow remote access. For more information, see [Typical applications of security group rules](#).

Add Security Group Rule ? Add security group rules

NIC: Internal Network

Rule Direction: Ingress

Action: Allow

Protocol Type: All

* Port Range: -1/-1

Priority: 1

Authorization Type: CIDR

* Authorization Objects: 10.10.0.0/24

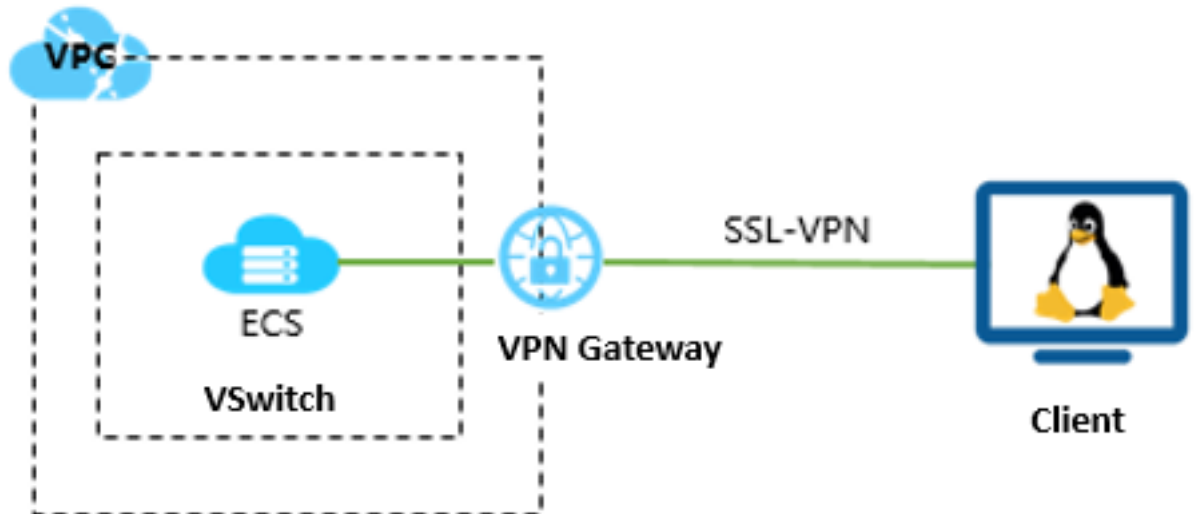
Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK Cancel

3 Windows client remote access

This document illustrates how to use SSL-VPN to connect a VPC from a remote computer with the Windows operating system.



Prerequisites

Before deploying the VPN gateway, make sure that the following conditions are met:

- The IP address ranges of the VPC and the remote computer are not in conflict.
- The client can access the Internet.

Step 1: 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. On the purchase page, configure the VPN gateway and complete the payment. In this tutorial, the VPN gateway uses the following configurations:
 - **Region:** Select the region of the VPN gateway. In this tutorial, **China (Hangzhou)** is selected.



Note:

Make sure that the VPC and the VPN gateway are in the same region.

- **VPC:** Select the VPC to be connected.
- **Bandwidth specification:** Select a bandwidth specification. The bandwidth specification is the Internet bandwidth of the VPN gateway.
- **IPsec-VPN:** Select whether to enable the IPsec-VPN feature. The IPsec-VPN feature applies to site-to-site connections and can be enabled according to your actual needs.
- **SSL-VPN:** Select whether to enable the SSL-VPN feature. The SSL-VPN feature allows you to connect to a VPC from a single computer anywhere. In this tutorial, select **Enable**.
- **Concurrent SSL Connections:** Select the maximum number of clients you want to connect to simultaneously.

**Note:**

You can only configure this option after you enables the SSL-VPN feature.

Basic Configuration	Region	China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)
		Hong Kong	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
		UAE (Dubai)	Germany (Frankfurt)	China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
		UK(London)					
	Name	<input type="text"/>					
	VPC	emr_test_vpc					
	Peak Bandwidth	10 Mbps		100 Mbps			
	Billing Method	Pay By Traffic					
Advanced Configuration	IPsec-VPN	enable		disable			
	SSL-VPN	disable		enable			

5. Go back to the VPN Gateways page, select China (Hangzhou) region to view the created VPN Gateway.

The initial status of a VPN Gateway is Preparing. It changes to Normal in about 2 minutes.

When it changes to Normal, it indicates that the VPN Gateway is ready to use.

**Note:**

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

VPN Gateways											
Create VPN Gateway Refresh Custom			Instance ID ▾		Enter a name or ID						
Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Enable IPsec	Enable SSL	Concurrent SSL Connections	Description	Actions
vpn2	47.97.193.13		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 01/25/2018, 14:41:45 Created	Enabled	Enable SSL	-	-	Delete
vpn2	47.97.209.47		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 02/11/2018, 17:53:25 Created	Enabled	Enabled	5 Upgrade downgrade	-	Delete

Step 2: Create an SSL server

1. In the left-hand navigation pane, click **VPN > SSL Servers**.
2. Click **Create SSL Server**. In this tutorial, the configurations of the SSL server is as follows:
 - **Name:** Enter a name for the SSL server.
 - **VPN Gateway:** Select the created VPN Gateway.
 - **Local Network:** Enter the CIDR block of the network to be connected. Click **Add Local Network** to add multiple local networks. The local network can be the CIDR block of any VPC or VSwitch, or the CIDR block of the local network.
 - **Client Subnet:** Enter the IP addresses used by the client to connect the server in the form of CIDR block.
 - **Advanced Configuration:** Use the default advanced configuration.

SSL Servers

Create SSL Server Refresh Custom

Instance ID/Name	IP Address	VPN Gateway
vss-bp15prztev8lvop9b74d2server1	47.97.209.47	vpn-bp19uhlxmy47kqf5acwl

Create SSL Server

VPN Gateway
vpn2/vpn-bp111s8uqu8782z8ee43

Local Network
192.168.0.0/16

[Add Local Network](#)

Client Subnet
10.10.0.0/24

Note: The client subnet IP range cannot overlap the VPC VSwitch subnet IP range.

Advanced Configuration
☒

Protocol
UDP

Port
1194

Encryption Algorithm
AES-128-CBC

Enable Compression
No

OK Cancel

Step 3: Create a client certificate

1. In the left-side navigation pane, click **VPN > SSL Clients**.
2. Click **Create Client Certificate**.
3. On the **Create Client Certificate** page, enter a name, and then select the corresponding SSL server. Click **OK**.
4. On the **SSL Clients** page, find the created SSL client certificate, and then click **Download**.

SSL Clients					
<div> <div>Create Client Certificate</div> <div>Refresh</div> <div>Custom</div> </div>					
Instance ID/Name	SSL Server	Status	Created At	Expiration Date	Actions
u Client	vs 2 server1	Normal	10/17/2018, 19:09:01	10/16/2021, 19:09:01	<div>Download</div> <div>Delete</div>

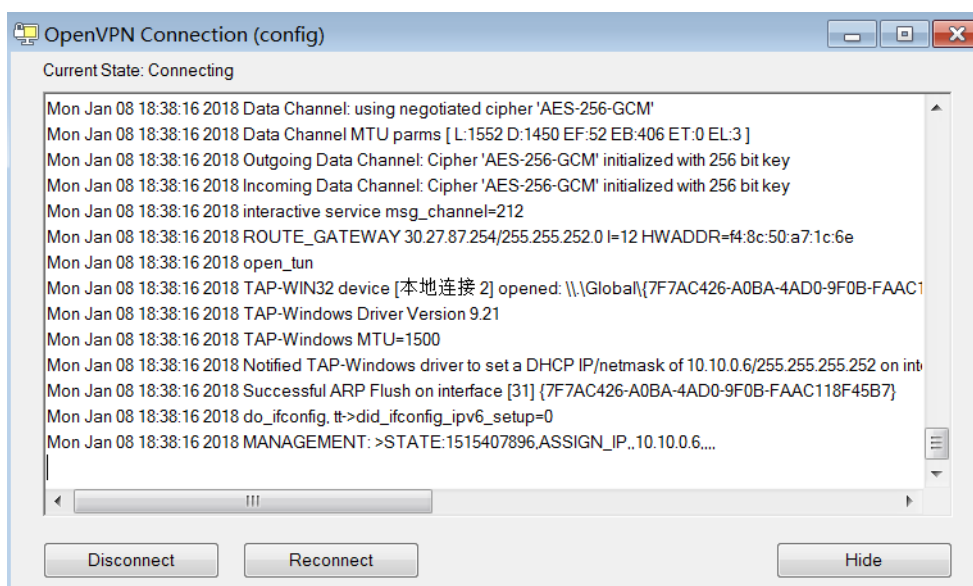
Step 4: Configure Windows clients



Note:

You need to run the client as an administrator.

1. Download and install the OpenVPN client.
2. Extract the client certificates downloaded in step 3 and copy the certificates to the `/etc/openvpn/conf/` directory.
3. Click **Connect** to initiate the connection.



Step 5: Verify the connection

On the client, ping the private IP address of an ECS instance in the connected VPC network to verify the connection.

**Note:**

Make sure that the security rule of the ECS instance allow remote access. For more information, see [Add security group rules](#).

Add Security Group Rule ⓘ Add security group rules

NIC: Internal Network ▼

Rule Direction: Ingress ▼

Action: Allow ▼

Protocol Type: All ▼

* Port Range: -1/-1 ⓘ

Priority: 1 ⓘ

Authorization Type: CIDR ▼

* Authorization Objects: 10.10.0.0/24 ⓘ
Tutorial

Description:

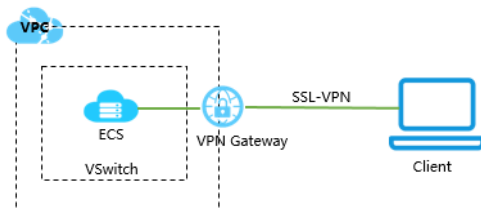
It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK

Cancel

4 Mac client remote access

This document illustrates how to use SSL-VPN to connect a VPC from a client of the Mac operating system.



Prerequisites

Before deploying the VPN gateway, make sure that the following conditions are met:

- The IP address ranges of the VPC and the remote computer are not in conflict.
- The client can access the Internet.

Step 1: 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. On the purchase page, configure the VPN gateway and complete the payment. In this tutorial, the VPN Gateway uses the following configurations:

- **Region:** Select the region of the VPN Gateway. In this tutorial, **China (Hangzhou)** is selected.



Note:

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

- **VPC:** Select the VPC to be connected.
- **Bandwidth specification:** Select a bandwidth specification. The bandwidth specification is the Internet bandwidth of the VPN Gateway.
- **IPsec-VPN:** Select whether to enable the IPsec-VPN feature. The IPsec-VPN feature applies to site-to-site connections and can be enabled according to your actual needs.
- **SSL-VPN:** Select whether to enable the SSL-VPN feature. The SSL-VPN feature allows you to connect to a VPC from a single computer anywhere. In this tutorial, select **Enable**.

- **Concurrent SSL Connections:** Select the maximum number of clients you want to connect to simultaneously.

**Note:**

You can only configure this option after you enable the SSL-VPN feature.

Basic Configuration	Region	China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)
		Hong Kong	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
		UAE (Dubai)	Germany (Frankfurt)	China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
		UK(London)					
	Name	<input type="text"/>					
	VPC	emr_test_vpc					
	Peak Bandwidth	10 Mbps		100 Mbps			
	Billing Method	Pay By Traffic					
Duration	IPsec-VPN	enable		disable			
	SSL-VPN	disable		enable			

5. Go back to the VPN Gateways page, select China (Hangzhou) region to view the created VPN Gateway.

The initial status of a VPN Gateway is Preparing. It changes to Normal in about 2 minutes.

When it changes to Normal, it indicates that the VPN Gateway is ready to use.

**Note:**

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

VPN Gateways											
Create VPN Gateway Refresh Custom			Instance ID ▾ Enter a name or ID								
Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Enable IPsec	Enable SSL	Concurrent SSL Connections	Description	Actions
vpn2	47.97.193.13		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 01/25/2018, 14:41:45 Created	Enabled	Enable SSL	-	-	Delete
vpn1	47.97.209.47		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 02/11/2018, 17:53:25 Created	Enabled	Enabled	5 Upgrade downgrade	-	Delete

Step 2: Create an SSL server

1. In the left-hand navigation pane, click **VPN > SSL Servers**.
2. Click **Create SSL Server**. In this tutorial, the configurations of the SSL server is as follows:
 - **Name:** Enter a name for the SSL server.
 - **VPN Gateway:** Select the created VPN Gateway.
 - **Local Network:** Enter the CIDR block of the network to be connected. Click **Add Local Network** to add multiple local networks. The local network can be the CIDR block of any VPC or VSwitch, or the CIDR block of the local network.
 - **Client Subnet:** Enter the IP addresses used by the client to connect the server in the form of CIDR block.
 - **Advanced Configuration:** Use the default advanced configuration.

SSL Servers

Create SSL Server Refresh Custom

Instance ID/Name	IP Address	VPN Gateway
vss-bp15przlev8lvop9b74d2server1	47.97.209.47	vpn-bp19uhkxny47kqrf5acwl

Create SSL Server

VPN Gateway
vpn2/vpn-bp111s8uqu8782zf8ee43

Local Network
192.168.0.0/16

[Add Local Network](#)

Client Subnet
10.10.0.0/24

Note: The client subnet IP range cannot overlap the VPC/VSwitch subnet IP range.

Advanced Configuration
☒

Protocol
UDP

Port
1194

Encryption Algorithm
AES-128-CBC

Enable Compression
No

OK Cancel

Step 3: Create a client certificate

1. In the left-side navigation pane, click **VPN > SSL Clients**.
2. Click **Create Client Certificate**.
3. On the **Create Client Certificate** page, enter a name, and then select the corresponding SSL server. Click **OK**.
4. On the **SSL Clients** page, find the created SSL client certificate, and then click **Download**.

SSL Clients					
Create Client Certificate Refresh Custom					
Instance ID/Name	SSL Server	Status	Created At	Expiration Date	Actions
u Client	vs 2 server1	● Normal	10/17/2018, 19:09:01	10/16/2021, 19:09:01	Download Delete

Step 4: Configure Mac clients

1. Run the following command to install the OpenVPN client.

```
brew install openvpn
```

**Note:**

Make sure that Homebrew is already installed.

2. Make a copy of the default configuration, and then run the following command to delete the default configuration:
 - a. Run the following command to copy the downloaded certificates to the configuration folder:

```
rm /usr/local/etc/openvpn/*
```
 - b. Run the following command to copy the file to the configuration directory:

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

`cert_location` is the path of the certificate downloaded in step 3. For example: `/Users/example/Downloads/certs6.zip`
 - c. Run the following command to extract the certificate:

```
cd /usr/local/certificates
```

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

- d. Run the following command to initiate the connection:

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

Step 5: Verify the connection

On the client, ping the private IP address of an ECS instance in the connected VPC network to verify the connection.



Note:

Make sure that the security rule of the ECS instance allow remote access. For more information, see [Typical applications of security group rules](#).

Add Security Group Rule ? Add security group rules

NIC: Internal Network

Rule Direction: Ingress

Action: Allow

Protocol Type: All

* Port Range: -1/-1

Priority: 1

Authorization Type: CIDR

* Authorization Objects: 10.10.0.0/24

Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK

Cancel