

VPN Connections

Quick Start



Copyright Notice

©2013–2026 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Trademark Notice



This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies ("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Quick Start

IPSec VPN

Establishing a Connection Between VPC and IDC (SPD policy)

Getting Started

Step 1: Creating a VPN Gateway

Step 2: Creating a Customer Gateway

Step 3: Creating a VPN Channel

Step 4: Load the Configuration of the Local Gateway

Step 5: Configuring a Routing Table

Step 6: Activating a VPN Channel

Connecting VPC to IDC (Route Table)

Getting Started

Step 1: Creating a VPN Gateway

Step 2: Creating a Customer Gateway

Step 3: Creating a VPN Channel

Step 4: Local Gateway Configuration

Step 5: Configure a Routing Policy

Step 6: Activate a VPN Tunnel

Establishing a Connection Between VPC and IDC (Dynamic BGP)

Getting Started

Step 1: Create a CCN VPN Gateway

Step 2: Creating a Customer Gateway

Step 3: Creating a VPN Channel

Step 4: Local Gateway Configuration

Step 5: Activate the VPN Tunnel

SSL VPN

Connecting the Mobile Client to VPC

Directions

Step 1: Create an SSL VPN Gateway

Step 2: Create an SSL VPN Server

Step 3: Create an SSL VPN Client

Step 4: Configure the Tencent Cloud Routing Policy

Step 5: Configure the Mobile Client

Step 6: Test the Connection

Quick Start

IPSec VPN

Establishing a Connection Between VPC and IDC (SPD policy)

Getting Started

Last updated: 2024-09-20 16:00:51

This tutorial introduces how to establish VPN Connections between your on-premises IDC and VPC through a public encrypted channel. The following video presents a quick start guide for VPN Connections.

[观看视频](#)

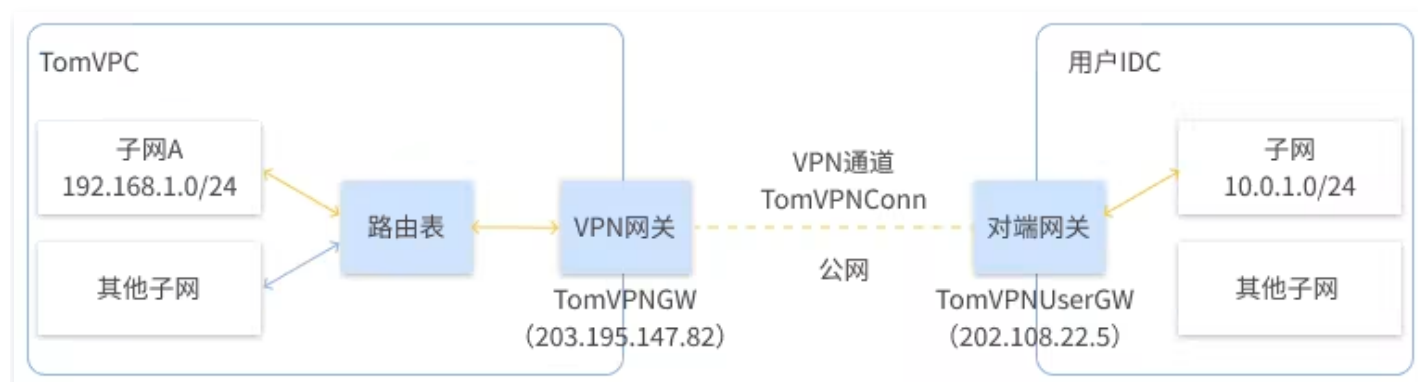
You need to complete the following steps to make the VPN Connections effective, as illustrated below.

ⓘ Note:

In the [Local Database Sync to Cloud](#) scenario, please use the VPN3.1 Gateway.

Example

By using IPsec VPN Connections, establish connectivity between Subnet A: 192.168.1.0/24 in TomVPC within your VPC in **Guangzhou** and the Subnet: 10.0.1.0/24 in your IDC. The public IP of the VPN Gateway in your IDC is 202.108.22.5 .



Operation Steps

Below is the flowchart of activating a VPN connection:



For detailed directions, see:

- [Step 1: Creating a VPN Gateway](#)
- [Step 2: Creating a Customer Gateway](#)
- [Step 3: Creating a VPN Channel](#)
- [Step 4: Load the Configuration of the Local Gateway](#)
- [Step 5: Configuring a Routing Table](#)
- [Step 6: Activating a VPN Channel](#)

Step 1: Creating a VPN Gateway

Last updated: 2024-09-20 16:01:12

This document describes how to create a VPN gateway. You can learn about the basic operations of the VPN gateway through the following video.

ⓘ Note:

The video introduces only the basic features of the VPN. Please refer to the actual console for the interface.

[观看视频](#)

Operation Steps

1. Log in to the [VPC console](#).
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Select the region, such as **Guangzhou** in the example, and click **New**.

ⓘ Note:

If **New** is greyed out and "No available VPC" is shown when hovering over it, please [create a VPC](#) first before creating a new VPN gateway.

4. Enter a name for the VPN gateway (e.g., TomVPNGw). Select the associate network, subordinate network, bandwidth cap, labels, and billing method, and click **Create**. After the VPN gateway is created, the system randomly assigns a public IP address, such as `203.195.147.82`.

ⓘ Note:

- Only new gateways but not existing gateways are supported on 200 Mbps, 500 Mbps, 1,000 Mbps and 3,000 Mbps bandwidths.
- If the VPN gateway uses 200 Mbps, 500 Mbps, 1,000 Mbps or 3,000 Mbps bandwidths, AES128+MD5 is recommended for VPN tunnel encryption.

新建VPN网关

×

网关名称

t

您还可以输入56个字符

所在地域

华南地区 (广州)

可用区

广州三区

协议类型

☒ IPsec ☐ SSL

带宽上限

5M

10M

20M

50M

100M

200M

500M

1000M

3000M

bps

关联网络

☐ 云联网 ☒ 私有网络

所属网络

标签

标签键	标签值	操作
请选择	请选择	×

添加

计费方式

☒ 按流量计费 ☐ 包年包月

总价

-(网关费用)

-(流量费用)

创建

取消

Note:
The labels are alternatively configured, please retain the default settings.

Reference

[Step 2: Creating the Peer Gateway](#)

[Step 3: Creating the VPN Tunnel](#)

[Step 4: Load the Configuration of the Local Gateway](#)

[Step 5: Configure the Route Table](#)

[Step 6: Activate the VPN Tunnel](#)

Step 2: Creating a Customer Gateway

Last updated: 2024-09-20 16:01:48

This article introduces how to create a Customer Gateway. You can watch the following video to understand the basic operations of a Customer Gateway.

[观看视频](#)

Operation Steps

Before creating a VPN channel, you need to create a customer gateway:

1. Log in to the [VPC console](#).
2. In the left directory, click **VPN Connections** > **Customer Gateway** to enter the management page.
3. Select the region, such as **Guangzhou** in the example, and click **New**.



4. Enter a name for the customer gateway (for example, TomVPNUserGw), the labels, and the public IP address of the IDC's VPN gateway, for example, `202.108.22.5`.

ⓘ Note:

The labels are alternatively configured, please retain the default settings.

新建对端网关

名称

您还可以输入60个字符

公网IP

标签

标签键	标签值	操作
请选择	请选择	

创建

取消

5. Click **Create** to continue.

Step 3: Creating a VPN Channel

Last updated: 2024-09-20 16:02:15

This document describes how to create a VPN tunnel. You can learn about VPN tunnel operations through the following video.

[观看视频](#)

Operation Steps

1. Log in to the [VPC console](#).
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel** to enter the management page.
3. Select the corresponding Region and VPC, such as **Guangzhou** and **TomVPC** in the example, then click **Create**.



4. VPN tunnel basic parameter configuration.

Basic configuration includes entering the tunnel name, selecting the gateway's region, network type, VPN gateway instance, peer gateway instance, pre-shared key, negotiation type, and communication mode. For the specific meaning of the parameters, please refer to [Creating a VPN Tunnel](#).

In this instance, the communication mode is SPD policy. The local network segment is

subnet A's segment `192.168.1.0/24` , and the remote network segment is `10.0.1.0/24` .

基本配置

VPN通道名称

您还可以输入60个字符

地域

广州

VPN网关类型

☒ 私有网络

☐ 云联网

私有网络

Test

VPN网关

Test

对端网关

☒ 选择已有

☐ 新建

tes

对端网关IP

1.1.1.0

协议类型

IKE/IPsec

预共享密钥

协商类型

☒ 流量协商

☐ 主动协商

☐ 被动协商

通信模式

☐ 目的路由

☒ SPD策略

通信模式选择后不可更改，请结合需求选择：网关下两种类型通道的目的网段重叠时，优先走通信模式为目的路由的通道

本端网段	对端网段	操作
		删除

+ 新增一行

标签

标签键

标签值

x

+ 添加

5. Configure the advanced settings.

In this step, you can set the advanced parameters, including DPD, health check, IKE, and IPsec. In this example, the default parameter values are used.

Note:

Make sure that the settings of IKE and IPsec on the cloud side are the same as those on the local side. Otherwise, the tunnel fails due to inconsistent protocol configurations.

高级配置

 配置IKE和IPSec时请确保云侧配置和本地配置一致、相匹配，以防因两端协议配置不一致而通道不通。

▲ DPD检测

开启DPD检测  ☒

DPD超时时间  30

DPD超时操作 

▼ 健康检测

▼ IKE配置

▼ IPsec 信息

创建

取消

6. Check your configuration, then click **Create**. After creation, return to the VPN tunnel list page, click **More**, select to download the configuration file, and complete the download.

Step 4: Load the Configuration of the Local Gateway

Last updated: 2024-09-20 16:02:39

After completing the first 3 steps, the configuration of the cloud VPN gateway and VPN tunnel has been finished. You need to continue configuring the VPN tunnel information on the "Local Gateway" on the IDC side. For more details, please refer to [Local Gateway Configuration](#). The "Local Gateway" on the IDC side refers to the IPsec VPN device on the IDC side, whose public IP is recorded under "Peer Gateway" in [step 2](#).

A local gateway is generally deployed in the following scenarios:

Note:

- Both of the following methods require that the VPN configuration on your "Local Gateway" matches the VPN tunnel information in [step 3](#), otherwise, the VPN tunnel will not be able to connect properly.
- You can view the configuration information of the VPN Connection on Tencent Cloud through the [VPN Connection Console](#), and download it via **Downloading Config File** to load it into the IPsec VPN Gateway of the local data center to complete the configuration.

- Establish a connection between Tencent Cloud and your local data center**

The local gateway is a network device with VPN feature, usually a data center exit router or firewall. You can configure VPN on this network device to complete the "Local Gateway" setup.

Note:

Configurations may vary with network device manufacturers (such as H3C and Cisco). Please configure the local gateway as needed.

- Establish a connection between Tencent Cloud and other public clouds**

The local gateway is the VPN gateway on your target public cloud. You need to operate on the VPN gateway on your target public cloud to complete the VPN configuration of the "Local Gateway". For specific configuration methods, please refer to the documentation of your target public cloud.

Step 5: Configuring a Routing Table

Last updated: 2024-09-20 16:03:00

By Step 4, we have successfully configured a VPN channel, but we still need to configure a routing policy to route the traffic from Subnet A to the VPN Gateway, enabling communication between the network segment in Subnet A and the network segment in the IDC.

1. Log in to the [VPC console](#).
2. In the left-side directory, click **Subnet**, select the corresponding region and VPC, such as **Guangzhou** and **TomVPC** as in the example, and click the route table ID associated with Subnet A to enter the details page.



3. Click **+Add Routing Policy**.



4. In the pop-up box, enter the destination network segment (**10.0.1.0/24**), select **VPN Gateway** as the next hop type, choose the newly created VPN Gateway **TomVPNGw** as the next hop, and click **create**.

新增路由

×

目的端	下一跳类型	下一跳	备注	操作
10.0.1.0/24	云服务器的公网IP	云服务器的公网IP①		✕
+新增一行				
① 路由策略用于控制子网内的流量走向				
NAT 网关 对等连接 专线网关 高可用虚拟IP VPN网关 云服务器的公网IP 云服务器				
创建 关闭				

Step 6: Activating a VPN Channel

Last updated: 2024-09-20 16:03:16

After configuring the Tencent Cloud VPN gateway, VPN channel, peer gateway, and user's local setup, you can use a Ping command to activate the channel and verify connectivity between Tencent Cloud and the user.

Ping an IP address in the peer IP range from Cloud Virtual Machine in the VPC.

- If the Ping action succeeds, Tencent Cloud connects to the user's VPN tunnel.
- If the Ping action fails, please check the customer's local setup. For technical support, please [submit a work order](#).

Connecting VPC to IDC (Route Table)

Getting Started

Last updated: 2024-09-20 16:03:41

This document describes how to quickly create a VPN connection and configure routing and forwarding policies with a route table to ensure the secure communication between VPC and IDC.

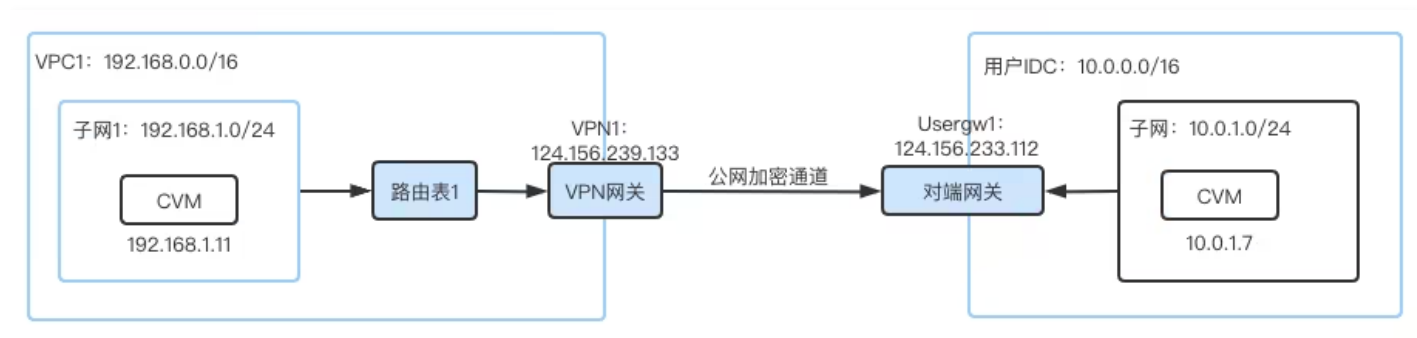
Step-by-Step Instructions

Below is the flowchart of activating a VPN connection:



Example

With an IPsec VPN connection, you can connect the subnet `192.168.1.0/24` in your VPC in Tokyo to the subnet `10.0.1.0/24` in your local IDC.



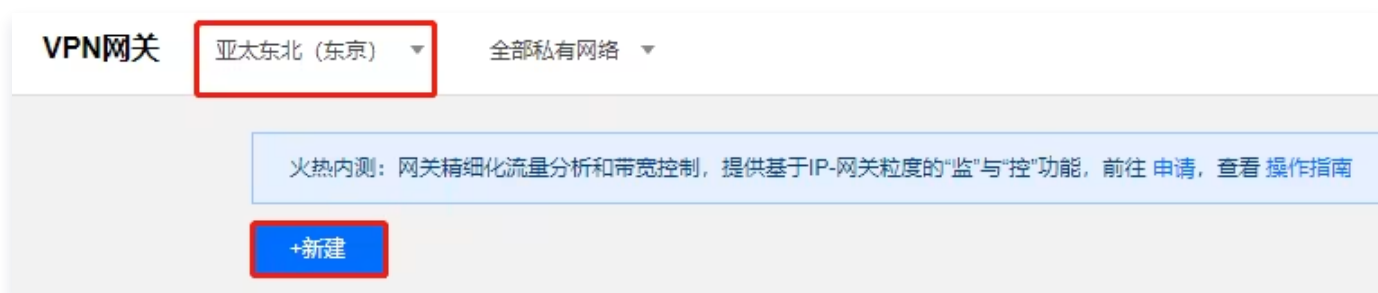
Step 1: Creating a VPN Gateway

Last updated: 2024-09-20 16:04:36

1. Log in to the [VPC console](#).
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Select the region, such as **Tokyo** in the example, and click **Create**.

Note:

If **New** is greyed out and "No available VPC" is shown when hovering over it, please [create a VPC](#) first before creating a new VPN gateway.



4. In the pop-up dialog box, enter the VPN gateway name (such as VPN1), choose VPC as the associated network, choose VPC1 as the network it belongs to, and select the bandwidth cap and billing method.

Note:

If the VPN gateway uses 200 Mbps, 500 Mbps, 1,000 Mbps or 3,000 Mbps bandwidths, AES128+MD5 is recommended for VPN tunnel encryption.

5. Click **Buy Now**. After the VPN gateway is created, the system assigns a public IP address randomly, such as: 124.156.239.133 .

Step 2: Creating a Customer Gateway

Last updated: 2024-09-20 16:04:55

1. Log in to the [VPC console](#).
2. In the left directory, click **VPN Connections** > **Customer Gateway** to enter the management page.
3. Select the region, such as **Tokyo** in the example, and click **Create**.
4. Enter the customer gateway name (e.g. Usergw1) and the public IP address of the customer VPN gateway, e.g. 124.156.223.112.

新建对端网关

名称

Usergw1

不能超过60个字符

公网IP

124

156

223

112

用户侧 ASN

-

64551

+

ASN 取值范围为1 - 4294967295，其中 139341,45090,58835 不可用。
一个对端网关仅能配置一个 ASN，即一个公网 IP 仅能配置一个 ASN

标签

标签键

标签值

+ 添加

键值粘贴板

确定

取消

5. Click **OK**, and the successfully created VPN tunnel is shown as below.

ID/名称	公网IP	通道个数	ASN	标签	操作
cgw-43...	43...	1	111		删除 编辑标签
cgw-43...	43...	1	222		删除 编辑标签

Step 3: Creating a VPN Channel

Last updated: 2024-09-24 17:06:44

1. Log in to the [VPC console](#).
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel** to enter the management page.
3. Select the corresponding Region and VPC, like **Tokyo** and **VPC1** in the example, click **+New**.
4. VPN Tunnel Basic Configuration Parameters.

Basic configurations include inputting the tunnel name, selecting the gateway's region, network type, VPN gateway instance, peer gateway instance, pre-shared key, negotiation type, and communication mode. For specific parameter definitions, please see [Create VPN Tunnel](#).

In this instance, the communication mode is destination routing.

基本配置

VPN通道名称

请输入通道名称

您还可以输入60个字符

地域

广州

VPN网关类型

☒ 私有网络

☐ 云联网

私有网络

to1-12345678901234567890

VPN网关

to1-12345678901234567890

对端网关

☒ 选择已有

☐ 新建

SH-12345678901234567890

对端网关IP

1.1.1.1

协议类型

IKE/IPsec

预共享密钥

协商类型

☒ 流量协商

☐ 主动协商

☐ 被动协商

通信模式

☒ 目的路由

☐ SPD策略

通信模式选择后不可更改，请结合需求选择；网关下两种类型通道的目的网段重叠时，优先走通信模式为目的路由的通道

标签

标签键

标签值

+ 添加

5. Configure the advanced settings.

In this step, you can set the advanced parameters, including DPD, health check, IKE, and IPsec. In this example, the default parameter values are used.

Note:

Make sure that the settings of IKE and IPsec on the cloud side are the same as those on the local side. Otherwise, the tunnel fails due to inconsistent protocol configurations.

高级配置

 配置IKE和IPSec时请确保云侧配置和本地配置一致、相匹配，以防因两端协议配置不一致而通道不通。

▲ DPD检测

开启DPD检测  ☒

DPD超时时间 

DPD超时操作 

▼ 健康检测

▼ IKE配置

▼ IPsec 信息

创建

取消

6. After successful creation, return to the VPN tunnel list page, click **More > Download Peer Configuration File** and complete the download.

ID/名称	监控	通道状态	健康状态	协议类型	通信类型	VPN网关	对端网关	关联网	预共享密钥	标签 (key:v...	操作
vpn-22		已联通	不支持	IKE/IPsec	动态 BGP 路由			ccr-37	123456		 
vpn-11		已联通	不支持	IKE/IPsec	动态 BGP 路由			ccn-37	123456		   

Step 4: Local Gateway Configuration

Last updated: 2024-09-24 17:07:09

After completing the first 3 steps, the configuration of the cloud VPN gateway and VPN tunnel has been finished. You need to continue configuring the VPN tunnel information on the "Local Gateway" on the IDC side. For more details, please refer to [Local Gateway Configuration](#). The "Local Gateway" on the IDC side refers to the IPsec VPN device on the IDC side, whose public IP is recorded under "Peer Gateway" in [step 2](#).

A local gateway is generally deployed in the following scenarios:

Note:

- Both of the following methods require that the VPN configuration on your "Local Gateway" matches the VPN tunnel information in [step 3](#), otherwise, the VPN tunnel will not be able to connect properly.
- You can view the configuration information of the VPN Connection on Tencent Cloud through the [VPN Connection Console](#), and download it via **Downloading Config File** to load it into the IPsec VPN Gateway of the local data center to complete the configuration.

- **Establish a connection between Tencent Cloud and your local data center**

The local gateway is a network device with VPN feature, usually a data center exit router or firewall. You can configure VPN on this network device to complete the "Local Gateway" setup.

Note:

Configurations may vary with network device manufacturers (such as H3C and Cisco). Please configure the local gateway as needed.

- **Establish a connection between Tencent Cloud and other public clouds**

The local gateway is the VPN gateway on your target public cloud. You need to operate on the VPN gateway on your target public cloud to complete the VPN configuration of the "Local Gateway". For specific configuration methods, please refer to the documentation of your target public cloud.

Step 5: Configure a Routing Policy

Last updated: 2024-09-24 17:07:27

You can successfully configure a VPN tunnel after Step 4, but you still need to configure a subnet routing policy to route the traffic from Subnet 1 to the VPN gateway. Meanwhile, configure the VPN gateway routing policy to import the traffic that reaches the VPN gateway into the VPN tunnel. This way, the IP range in Subnet 1 can communicate with the IP range in the IDC.

1. Log in to the [VPC console](#).
2. In the left directory, click **Subnet**, select the corresponding region and VPC, such as **Tokyo** and **VPC1** in the example, click the **Route Table ID** associated with Subnet 1 to enter the details page.



ID/名称	所属网络	CIDR	可用区	关联路由表	子网广播	云服务器	可用IP	默认子网	创建时间	操作
sub-tes	vpc-	10	东京一区	rtb-kra0b1h default	☐	0	253	否	2021-01-21 11:05:42	删除 更多

3. In the **Basic Information** tab, click **Add Routing Policy**.



目的端	下一跳类型	下一跳	备注	启用路由
	LOCAL	Local	系统默认下发，表示 VPC 内云服务器网络互通	☒

共 1 条

4. In the pop-up box, enter the peer IDC subnet segment (**10.0.1.0/24**), select **VPN Gateway** for the next hop type, choose the newly created VPN gateway **VPN1** for the next hop, and click **Create** to complete the routing policy configuration for Subnet 1.



目的端	下一跳类型	下一跳	备注	启用路由	云联网中状态	操作
192.168.0.0/16	LOCAL	Local	系统默认下发，表示 VPC 内云服务器网络互通	☒	-	① 发布到云联网
10.0.1.0/24	VPN网关	vpngw-o4ao5usq VPN1		☒	-	编辑 删除 发布到云联网

5. In the left directory, select **VPN Connections > VPN Gateway**.
6. Click the ID of the VPN gateway instance to go to the details page.
7. In the **Instance details** page, click the **Route Table** tab to configure the routing policy for the VPN gateway.

8. Click **Add Route**, and fill out the following parameters in the pop-up dialog box:

- **Destination:** Enter the intranet subnet of the peer IDC that needs to communicate with the local VPC. In this example, enter `10.0.1.0/24`.
- **Next hop type:** VPN tunnel is the only option. No setting required.
- **Next Hop:** Select the VPN tunnel created in [Step 3](#).
- **Weight:** If there are 2 VPN tunnels between VPC and IDC, you can set the active/standby linkage according to the weight. In this example, the default weight value is 0.

新增路由

目的端	下一跳类型	下一跳	权重	操作
	VPN通道 ▾	无可用VPN通道 ▾	0	删除
+新增一行				

确定

取消

9. Click **Confirm** to complete the routing policy configuration for the VPN gateway.

VPN1 详情

查看 API Inspector

VPN连接帮助文档

基本信息

监控

路由表

新增路由								
目的端	通道状态	健康状态	下一跳	路由类型	权重	更新时间	启用路由	操作
10.0.1.0/24	可达	-	vpn-x-13eftq9n tunnel1	静态路由	0	2021-02-04 10:57:50	☒	删除

Step 6: Activate a VPN Tunnel

Last updated: 2024-09-24 17:07:44

You can use the CVM in the VPC to ping an IP address in the customer IP range to activate the VPN tunnel. A successful ping indicates that VPC and IDC can communicate with each other. For example, you can use the CVM in subnet 1 of VPC1 to ping the server IP address in the subnet of the customer IDC: ping 10.0.1.7.

Establishing a Connection Between VPC and IDC (Dynamic BGP)

Getting Started

Last updated: 2024-09-24 17:08:11

This chapter describes how to quickly create VPN Connections and use Dynamic BGP to ensure secure communication between VPC and the peer IDC.

⚠ Note:

Dynamic BGP is currently in beta. If you need to use it, you can submit a [ticket request](#).

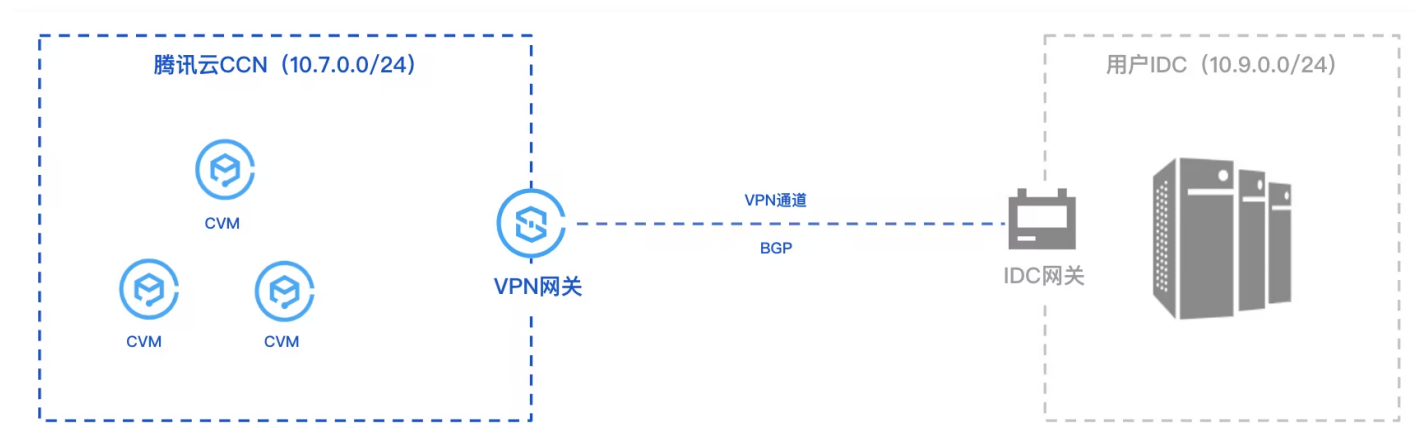
Step-by-Step Instructions

The flowchart is as follows:



Example

With IPsec VPN Connections, you can connect subnet A: 10.7.0.0/24 in your VPC in Seoul to the subnet: 10.9.0.0/24 in your local IDC.



Step 1: Create a CCN VPN Gateway

Last updated: 2026-08-10 15:09:51

1. Log in to the [VPC console](#).
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Select a region, such as **Seoul**, click **New**.

Note:

If **New** is greyed out and "No available VPC" is shown when hovering over it, please [create a VPC](#) first before creating a new VPN gateway.

4. In the pop-up creation dialog, enter the VPN gateway name (such as VPN1), choose the associated network as CCN, and set the bandwidth cap, BGP ASN, and billing method. For specific parameter information, refer to [Create IPsec VPN Gateway](#).

Note:

- Only VPN gateways with bandwidths of 200Mbps, 500Mbps, 1000Mbps, and 3000Mbps support dynamic BGP.
- AES128+MD5 is recommended for the VPN tunnel encryption protocol.

5. Click **Purchase Now**. After the VPN gateway is created, the system randomly assigns a public IP.

Step 2: Creating a Customer Gateway

Last updated: 2024-09-24 17:09:31

1. Log in to the [VPC console](#).
2. In the left directory, click **VPN Connections** > **Customer Gateway** to enter the management page.
3. Select the region, such as Seoul in the example, and click **New**.
4. Enter the customer gateway name (e.g. Usergw1) and the public IP address of the customer VPN gateway.

Note:

- The ASN value range is 1 – 4294967295, with 139341, 45090, and 58835 being unavailable.
- A customer gateway can only be configured with one ASN, meaning one public IP can only be configured with one ASN.

新建对端网关

×

名称 ⓘ
不能超过60个字符

公网IP ⓘ
· · ·

用户侧 ASN
- +
ASN 取值范围为1 - 4294967295, 其中 139341,45090,58835 不可用。
一个对端网关仅能配置一个 ASN, 即一个公网 IP 仅能配置一个 ASN

标签 ⓘ
标签键 标签值 ×
+ 添加 ⓘ 键值粘贴板

确定 取消

5. Click **OK**.

Step 3: Creating a VPN Channel

Last updated: 2024-09-24 17:09:47

1. Log in to the [VPC console](#).
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel**.
3. Select the appropriate region and VPC, click **Create**.
4. Basic configuration of the VPN tunnel.

The basic configuration includes entering the tunnel name, selecting the gateway region, network type, VPN gateway instance, peer gateway instance, preshared key, negotiation type, and communication mode. For detailed parameter descriptions, see [Create VPN Tunnel](#).

Search for the required CAM policy as needed, and click to complete policy association.

基本配置

VPN通道名称

您还可以输入60个字符

地域

广州

网络类型

☐ 私有网络
☒ 云联网

VPN网关

tes

对端网关

☒ 选择已有
☐ 新建

3

对端网关 IP

协议类型
IKE/IPsec

预共享密钥 ⓘ

协商类型

☒ 流量协商
☐ 主动协商
☐ 被动协商

通信模式

☐ 目的路由
☐ SPD策略
☒ 动态 BGP 路由

通信模式选择后不可更改，请结合需求选择；网关下两种类型通道的目的网段重叠时，优先走通信模式为目的路由的通道

您所关联的 VPN 网关 [vpngw-hsknf1m8](#) 未配置 ASN，请点击实例名称前往配置

BGP 隧道网段 ⓘ

169
/
30

云端 BGP 地址 ⓘ

16

用户端 BGP 地址 ⓘ

16

标签 ⓘ

标签键

标签值

×

+ 添加

键值粘贴板

5. Advanced Configuration.

In this step, you can configure advanced parameters such as DPD detection, IKE configuration, and IPsec information. In this example, the default configuration is used. After configuring, click **Create**.

! Note:

When configuring IKE and IPsec information, make sure that the cloud-side settings are consistent with the local settings to prevent tunnel failure due to protocol inconsistencies.

6. After creating successfully, return to the VPN tunnel list page, click **More**, select **Download Peer Configuration File** and complete the download.



Step 4: Local Gateway Configuration

Last updated: 2024-09-24 17:10:00

After completing the first three steps, the configuration of the cloud VPN gateway and VPN tunnel has been completed. You need to continue configuring the VPN tunnel information on the "Local Gateway" at the IDC side. For details, please refer to [Local Gateway Configuration](#). The "Local Gateway" on the IDC side is the IPsec VPN device on the IDC side, and the public IP of this device is recorded in [Step 2: Create a Peer Gateway](#) under the "Peer Gateway". A local gateway is generally deployed in the following scenarios:

Note

- Both methods require the VPN configuration on your "Local Gateway" to be consistent with the VPN tunnel information in [Step 3: Create a VPN Tunnel](#), otherwise, the VPN tunnel will not connect properly.
- The configuration information of the VPN tunnel on Tencent Cloud can be viewed through [VPN Tunnel Console](#), and the configuration file can be downloaded and imported into the IPsec VPN gateway of the local data center to complete the configuration.

• Integrate Tencent Cloud with the local data center

The local gateway is a network device with VPN feature, generally a data center exit router or firewall. You can configure the VPN on this network device to complete the configuration of the local gateway.

Note

Configurations may vary with network device manufacturers (such as H3C and Cisco). Please configure according to the specifics of the network equipment.

• Establish a connection between Tencent Cloud and other public clouds

The local gateway is the VPN gateway on your target public cloud. You need to operate on the VPN gateway on your target public cloud to complete the VPN configuration of the "Local Gateway". For specific configuration methods, please refer to the documentation of your target public cloud.

Step 5: Activate the VPN Tunnel

Last updated: 2024-09-24 17:10:14

After configuring the Tencent Cloud VPN gateway, VPN channel, peer gateway, and user's local setup, you can use a Ping command to activate the channel and verify connectivity between Tencent Cloud and the user.

Ping an IP address in the peer IP range from Cloud Virtual Machine in the VPC.

- If the Ping action succeeds, Tencent Cloud connects to the user's VPN tunnel.
- If the Ping action fails, please check the customer's local configuration. For technical support, please [submit a ticket](#).

SSL VPN

Connecting the Mobile Client to VPC

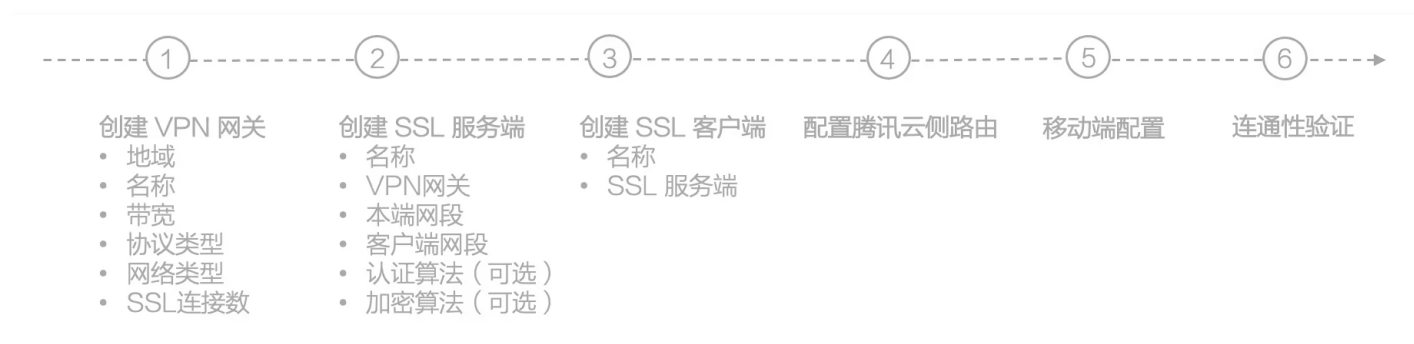
Directions

Last updated: 2024-09-24 17:11:16

This document describes how to quickly create an SSL VPN connection, and configure routing and forwarding policies with a route table to ensure the secure communication between the VPC and client.

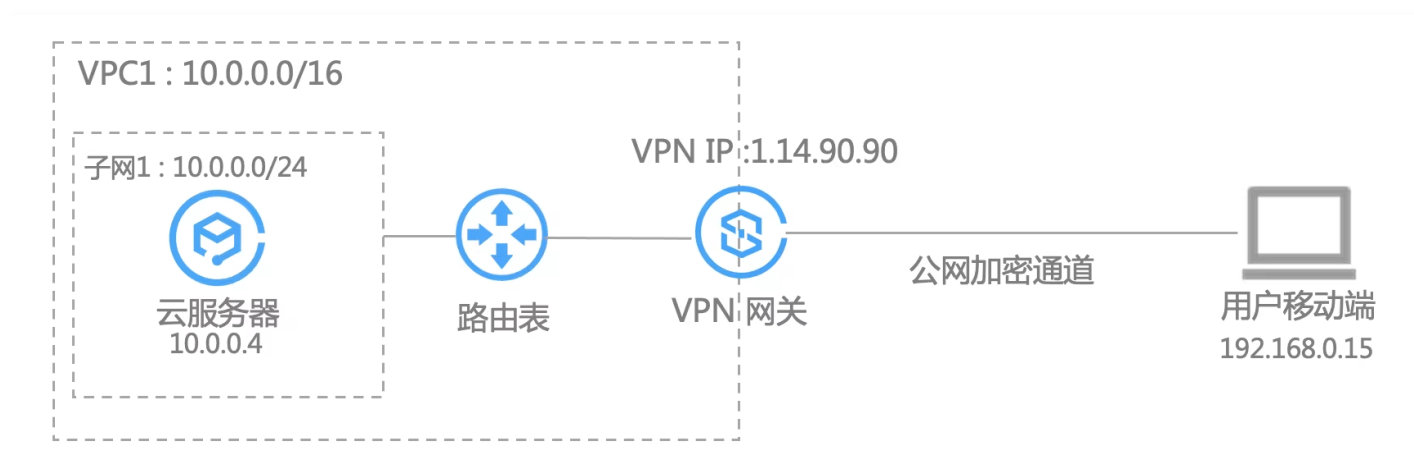
Step-by-Step Instructions

See below for the flowchart of activating an SSL VPN connection:



Example

Through SSL VPN Connections, connect your subnet 1: `10.0.0.0/16` in the VPC VPC in Guangdong 2 Zone with your mobile subnet: `192.168.0.0/16`.



Step 1: Create an SSL VPN Gateway

Last updated: 2024-09-24 17:11:30

An SSL VPN gateway is an egress gateway for VPC to establish an SSL VPN connection. It is used with an SSL VPN client (on mobile devices) to establish an encrypted communication between a Tencent Cloud VPC and a mobile client.

Operation Steps

1. Log in to the [VPC console](#).
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. On the VPN Gateway management page, click **New**.
4. In the pop-up **Create VPN Gateway** dialog box, configure the following gateway parameters.

Parameter name	Parameter Description
Billing Mode	The SSL VPN currently only supports traffic-based billing.
Region	Display the region of the VPN gateway.
Availability Zone	Select the Availability Zone where the current gateway is located.
Protocol Type	IPSec and SSL protocols are supported.
Network Type	• This parameter specifies whether you create a CCN-based VPN/VPN gateway or a VPC-based VPN/VPN gateway. If you want to use a VPN connection to enable interconnection with multiple VPCs or other Direct Connect networks, create a CCN-based VPN.  Note: You cannot associate the CCN-based VPN gateway with a CCN instance during its creation. You can associate a created VPN gateway to a CCN instance in the gateway details page. If you create a policy-based VPN tunnel, you also need to enable the

	route published to the CCN in the IDC IP range of the VPN gateway. If you want to communicate with a single VPC by using a VPN connection, create a VPC-based VPN.
VPC	Select the specific VPC to which the VPN gateway will be associated if the associated network is a VPC. For CCN instances, the gateway needs to be bound on the details page after creation. For more details, see Associating a CCN Instance .
Bandwidth Cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Number of SSL Connections	Selecting "SSL" for Protocol Type requires configuration of this item. The number of SSL connections supported is related to the gateway. For more details, see Usage Restrictions. Note: This number indicates the maximum number of clients allowed for simultaneous connection, that is, the maximum number of clients that the gateway can be associated with. After the gateway is created, this parameter cannot be modified. Therefore, set this parameter with caution.
Gateway Name	Enter the VPN gateway name (up to 60 characters).
Tag	Tags mark VPN gateway resources so that these resources can be queried and managed efficiently. Tag is not a required configuration. You can decide whether to configure it according to your demand.

5. After completing the gateway parameter settings, click **Purchase Now**.

Step 2: Create an SSL VPN Server

Last updated: 2024-09-24 17:11:47

This document describes how to create an SSL VPN server on Tencent Cloud to provide SSL services for clients.

Directions

1. Log in to the [VPC console](#).
2. In the left sidebar, click **VPN Connections** > **SSL Server** to access the management page.
3. On the SSL Server management page, click Create.
4. In the **Create SSL Server** dialog that appears, configure the following parameters.

Note:

In a Windows system, if your OpenVPN client is version 3.4.0 or above, you need to configure encryption and authentication algorithms for the SSL server configuration, with the authentication algorithm supporting only SHA1.

×

- ### 基本配置

您还可以输入60个字符

广州

请选择VPN网关

请输入云端网段

+新增一行

请输入客户端网段

UDP

1194

NONE

NONE

否

☒ 证书认证 ☐ 证书认证 + 身份认证

取消

Parameter name	Parameter Description
----------------	-----------------------

Name	Enter the SSL VPN server name (up to 60 characters).
Region	Display the region of the SSL VPN server.
VPN Gateway	Select an existing VPN gateway.
Cloud IP Range	Specify the IP range on Tencent Cloud that the mobile client can access, that is, the IP range of your VPC.
Client IP Range	Enter the IP range that is assigned to the mobile client for communication. The IP range must not conflict with the VPC CIDR block of Tencent or your local IP range.
Protocol	Transmission protocol of the server.
Port	Enter the SSL VPN server port used for data forwarding.
Authentication Algorithm	Supported authentication algorithms: SHA1 and MD5.
Encryption Algorithm	Supported encryption algorithms: AES-128-CBC, AES-192-CBC, and AES-256-CBC.
Compressed	No.
Authentication Method	Certificate verification and Certificate verification + Identity verification are available. In this example, certificate verification is used. • Certificate verification: In this verification method, the SSL VPN server can be accessed through all SSL VPN client connections by default. • Certificate verification + Identity verification: In this verification method, only connections that are allowed by the access control policy can be established. You can configure the access control policy for specific user groups or all users. If you select this option, you must select an EIAM application.

5. After completing the Gateway settings, click **OK**.

Step 3: Create an SSL VPN Client

Last updated: 2024-09-24 17:12:01

This document describes how to create an SSL VPN client on Tencent Cloud. The SSL VPN client records the information about the SSL certificate assigned by Tencent Cloud to the client. SSL certificate is used for mutual authentication between the server and the mobile client. You can download the certificate to the mobile terminal and configure it to OpenVPN for communication with Tencent Cloud.

Operation Steps

1. Log in to the [VPC console](#).
2. In the left directory, click **VPN Connections** > **SSL Clients** to enter the management page.
3. In the SSL Client management page, click **New**.
4. In the pop-up **SSL Client** dialog box, configure the following parameters.

Parameter name	Parameter Description
SSL VPN Server	Select the created SSL VPN server.
Region	Display the region of the SSL VPN server.
Mode	• Single creation: Users can directly create one SSL Client. • Batch creation: Download the batch creation template. After filling in the relevant parameters, click Select Files to upload.
Name	Enter the SSL VPN server name (up to 60 characters).

5. After configuring the SSL Client parameters, click **OK**. When the **Status** shows **Available**, the creation is complete.

Step 4: Configure the Tencent Cloud Routing Policy

Last updated: 2024-09-24 17:12:15

This document describes how to configure the routing and forwarding policies for the mobile client to access Tencent Cloud VPC.

Operation Steps

1. Log in to the [VPC console](#).
2. In the left menu, click **Route Table** to enter the Management Console.
3. In the route table management page, click **New**.
4. In the popped-up **New Route** dialog box, configure the following parameters.
- Search for the required CAM policy as needed, and click to complete policy association.

新建路由表

名称

您还可以输入60个字符

所属网络

标签

标签键

标签值

x

+ 添加

键值粘贴板

路由策略

①

路由策略用于控制子网内的流量走向，操作帮助请参考配置路由策略。

目的端	下一跳类型	下一跳	备注	操作
Local	LOCAL	Local	系统默认下发，表示 VPC 内云服务...	-
如 10.0.0.0/16	云服务器的公网IP	云服务器的公网IP ①		✖

+新增一行

创建

关闭

Parameter name	Parameter Description
Destination	Enter the network segment where the user's mobile terminal is located
Next Hop Type	Select the VPN Gateway

Next Hop	For the next hop, select the specific VPN Gateway instance you have created
----------	---

5. After completing the parameter settings, click **Create**.

Step 5: Configure the Mobile Client

Last updated: 2024-09-24 17:12:29

Now, you need to configure the SSL VPN client certificate on the mobile client.

Directions

1. Download the SSL client authentication files assigned to customers for connecting with Tencent Cloud from the Tencent Cloud side. For more details, see [Download SSL Client Configuration](#).

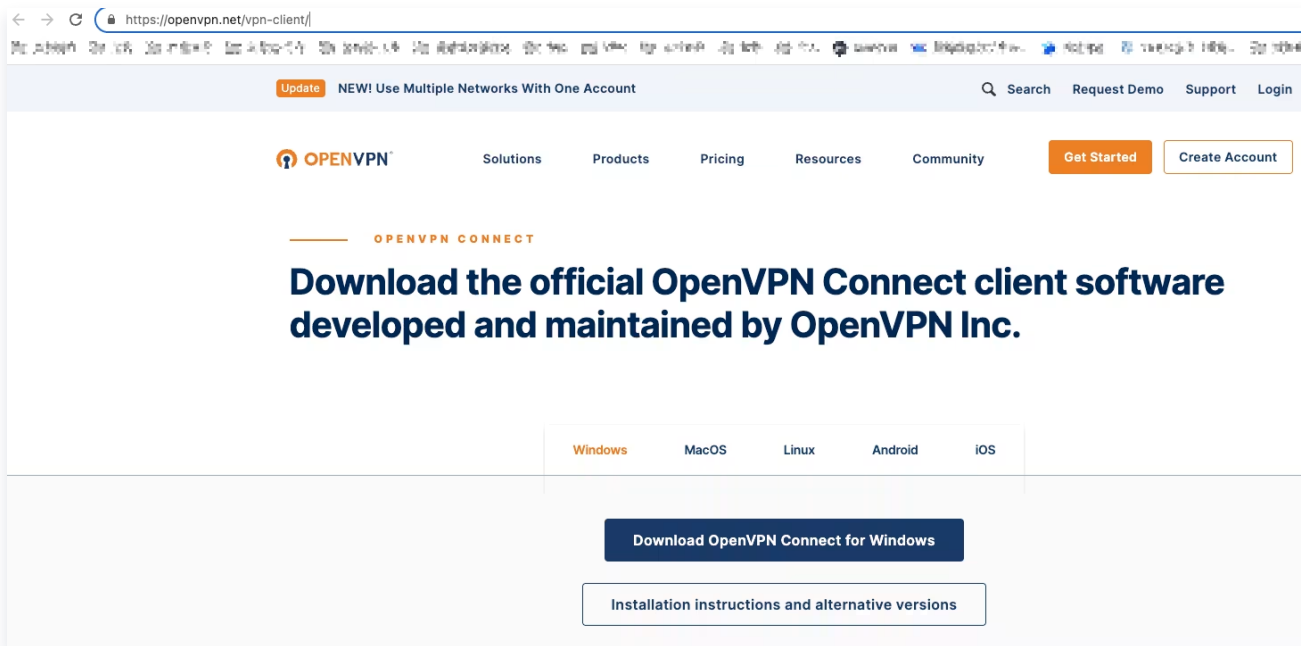
Note:

The downloaded SSL client certificate only supports one local client and does not support multiple clients simultaneously.

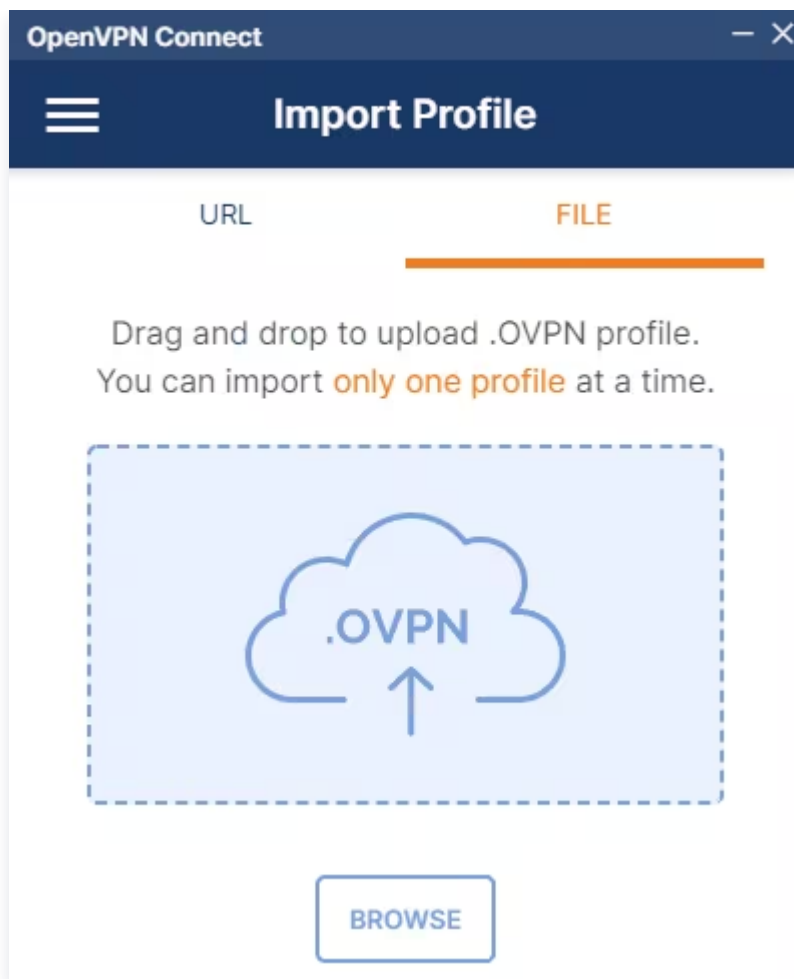
2. Download OpenVPN and the local mobile version of OpenVPN

Windows client

1. Download OpenVPN Connect from the official website and install it.

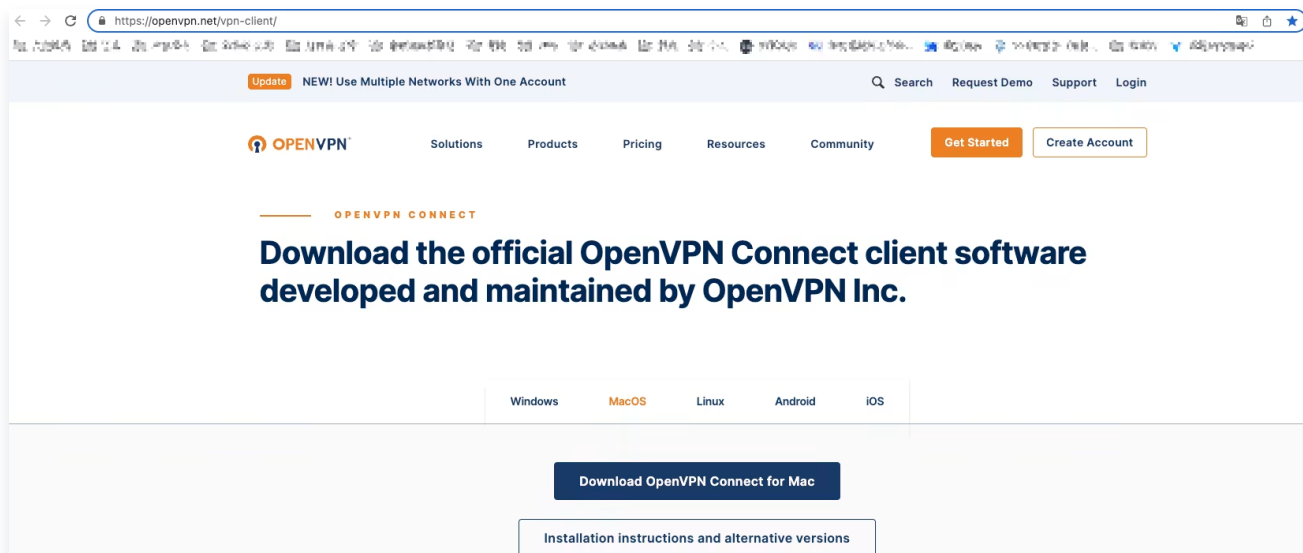


2. After the SSL client is installed, select the "FILE" page in the "Import Profile" menu, and upload the SSL client configuration file (.ovpn format) downloaded in [Step 1](#).

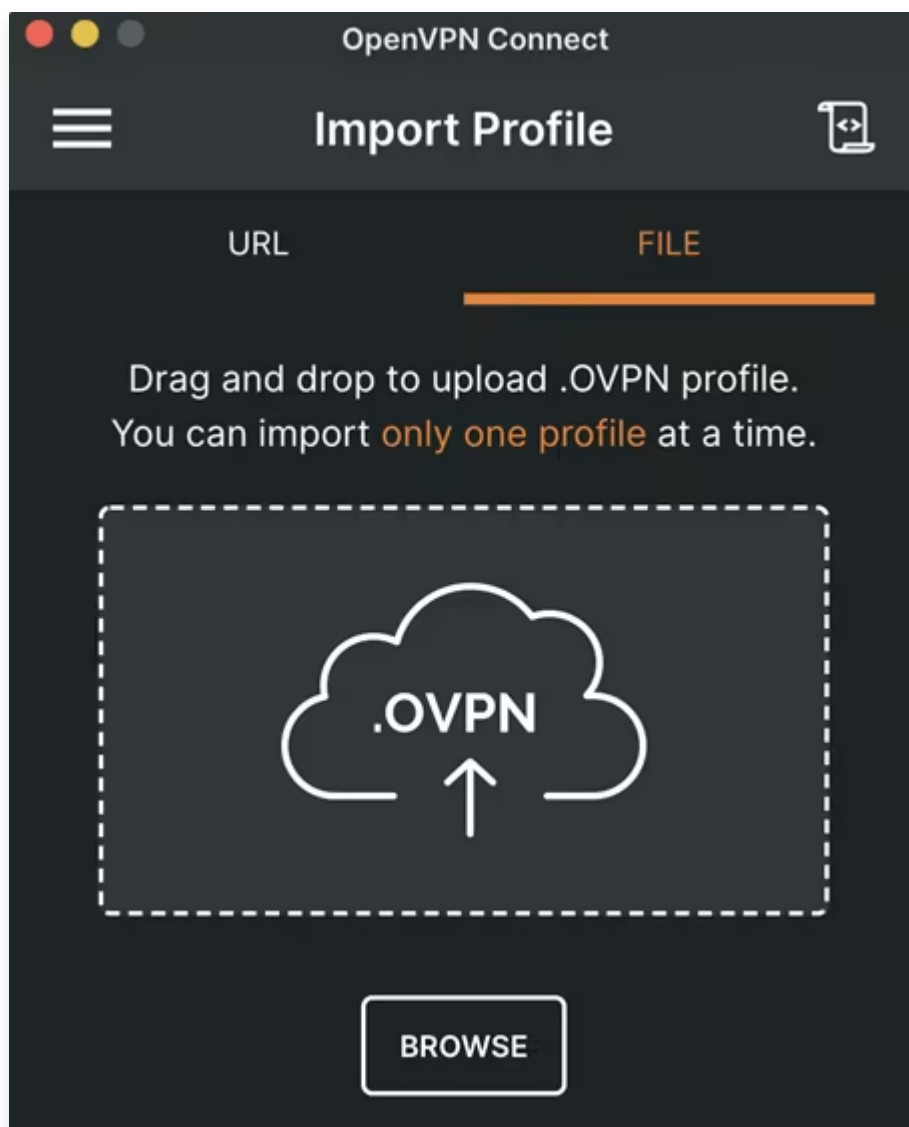


MAC client

1. Download OpenVPN Connect from the official website and install it.



2. After the SSL client is installed, select the "FILE" page in the "Import Profile" menu, and upload the SSL client configuration file (.ovpn format) downloaded in [Step 1](#).



Linux client

1. Open the command line window.
2. Run the following command to install OpenVPN Connect.

- CentOS distribution

```
yum install -y openvpn
```

- Ubuntu distribution

```
sudo apt-get install openvpn
```

3. Unzip and copy the SSL client certificate downloaded in [Step 1](#) to the `/etc/openvpn/conf/` directory.

Go to the `/etc/openvpn/conf/` directory and execute the following command to establish VPN Connections.

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

Step 6: Test the Connection

Last updated: 2024-09-24 17:12:43

After establishing SSL VPN Connections between Tencent Cloud and the user's mobile terminal, the Ping command can be used to test the connection.

For example, use a CVM within the VPC to ping an IP in the mobile terminal's network segment. If the ping is successful, it indicates that the VPC and the mobile terminal can communicate normally.