VPN Connections

Getting Started

Product Documentation

Contents

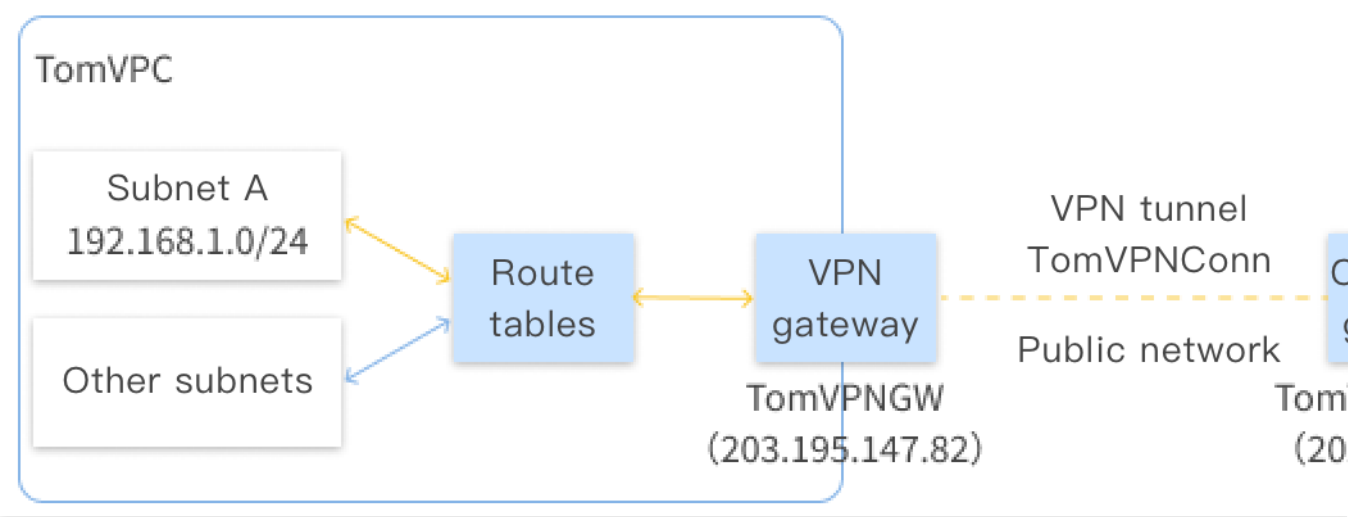
Getting Started
IPSec VPN
Establishing a Connection Between VPC and IDC (SPD policy)
Overview

Last updated：2024-01-09 14:20:07

You need to perform several steps to make a VPN connection effective. Then you can configure the IPsec VPN on the console in a self-service manner. An example is described below.

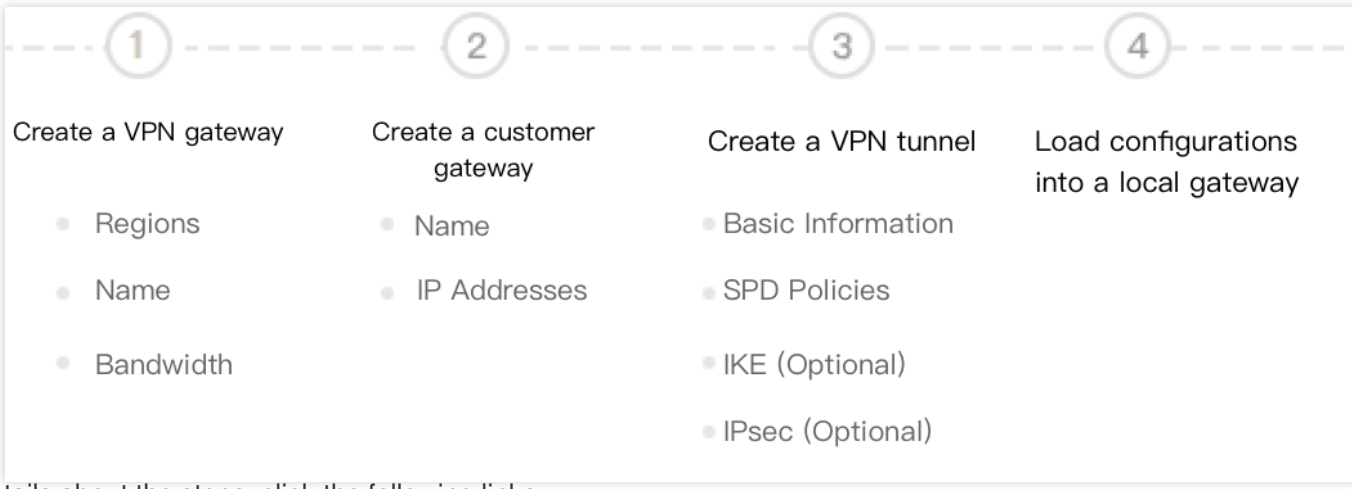
Example

Use an IPsec VPN connection to connect subnet A `192.168.1.0/24` in your VPC (TomVPC) in **Guangzhou** to the subnet `10.0.1.0/24` in your IDC. The public IP address of the VPN gateway in your IDC is `202.108.22.5`.



Directions

The flowchart of activating the VPN connection is shown below:



For details about the steps, click the following links:

Step 1: Create a VPN Gateway

Step 2: Create a Customer Gateway

Step 3: Create a VPN Tunnel

Step 4: Configure a Local Gateway

Step 5: Configure a Routing Policy

Step 6: Activate the VPN Tunnel

Step 1: Create a VPN Gateway

Last updated：2024-01-09 14:20:07

This document describes how to create a VPN gateway.

Directions

1. Log in to the VPC console.
2. Select **VPN Connections** > **VPN Gateway** in the left sidebar to enter the admin page.
3. Choose a region, for example, **Guangzhou**, and click **+Create**.

Note:

If the **+New** button is grayed out and “No VPC available” is displayed when the mouse hovers over it, create a VPC as instructed in Creating VPCs before creating the VPN gateway.

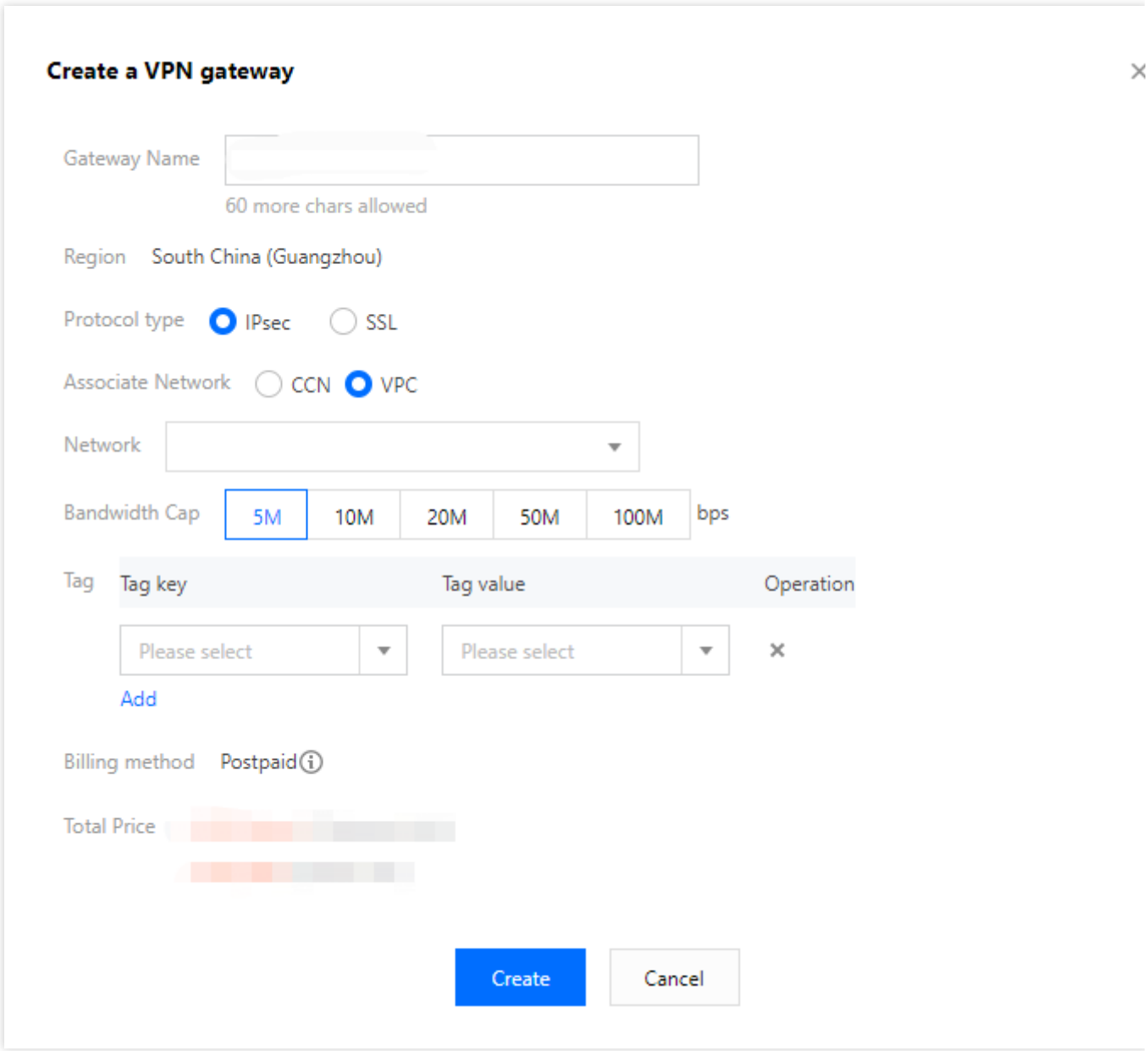
4. Enter a name for the VPN gateway, such as TomVPNGw. Select the associate network, subordinate network, bandwidth cap, labels, and billing method, and click **Create**. After the VPN gateway is created, the system randomly assigns a public IP address, such as `203.195.147.82`.

Note:

200 Mbps, 500 Mbps, 1,000 Mbps, and 3,000 Mbps bandwidths are available only in the following availability zones: North China (Beijing), East China (Shanghai), South China (Guangzhou), Southwest China (Chengdu), Hong Kong, Macao and Taiwan regions of China(Hong Kong, China), and East China (Nanjing). To use the bandwidths, please submit a ticket.

Only new gateways can use 200 Mbps, 500 Mbps, 1,000 Mbps, and 3,000 Mbps bandwidths. Existing gateways cannot use the preceding bandwidths.

If the VPN gateway uses the 200 Mbps, 500 Mbps, 1,000 Mbps, or 3,000 Mbps bandwidth, we recommend that you use AES128+MD5 for VPN tunnel encryption.



Note:

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

References

Step 2: Create a Customer Gateway

Step 3: Create a VPN Tunnel

Step 4: Load the Configuration of the Local Gateway

Step 5: Configure a Routing Table

Step 6: Activate a VPN Tunnel

Step 2: Create a Customer Gateway

Last updated：2024-01-09 14:20:07

This file introduces how to create a customer gateway.

Directions

Before creating a VPN tunnel, you need to create a customer gateway.

1. Log in to the VPC console.

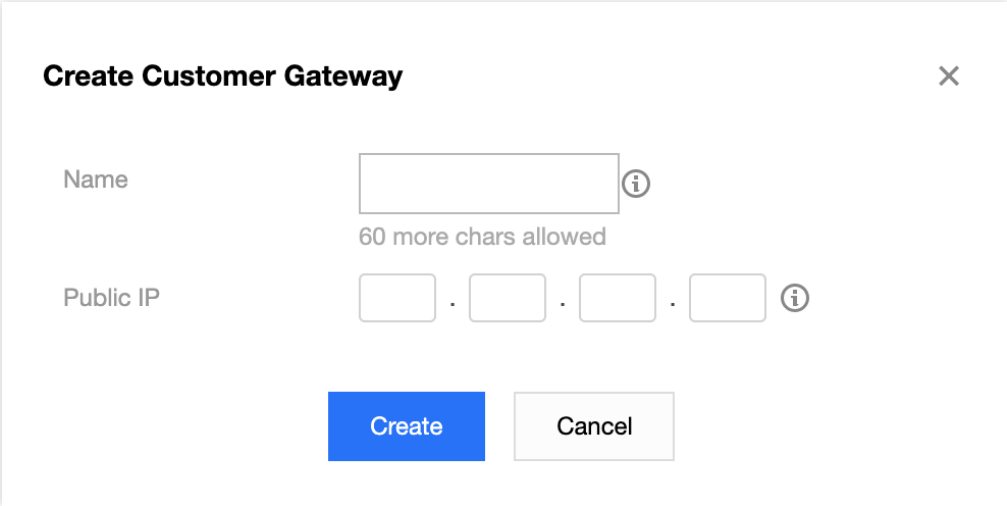
2. Click **VPN Connection** > **Customer Gateway** in the left directory to enter the admin page.

3. Choose a region, for example, **Guangzhou**, and click **+Create**.

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

Note:

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



5. Click **Create**.

Step 3: Create a VPN Tunnel

Last updated：2024-01-09 14:20:07

This document describes how to create a VPN tunnel.

Directions

1. Log in to the VPC console.
2. Select **VPN Connections** > **VPN Tunnel** in the left sidebar.
3. Choose the region where your VPC is located and your VPC, i.e. **Guangzhou** and `TomVPC` in this example, and click **+New**.
4. Configure the basic settings of the VPN tunnel.
The basic settings of a VPN tunnel include the tunnel name, region of the gateway, network type, VPN gateway instance, customer gateway instance, pre-shared key, negotiation type, and communication mode. For more information about the parameters, see Creating a VPN Tunnel.
In this example, the communication mode is **SPD policy**, the local IP range is the IP range `192.168.1.0/24` of subnet A, and the customer IP range is `10.0.1.0/24` .
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.
6. Check your configuration and click **Create**. After the tunnel is created, go to the VPN tunnel list page, click **More** next to the created tunnel, and choose **Download config file** to complete the download.

Step 4: Load the Configuration of the Local Gateway

Last updated：2024-01-09 14:20:07

After the first 3 steps, the VPN gateway and VPN tunnel on the Tencent Cloud are configured. Then, you need to configure the VPN tunnel on the local gateway of the IDC. For more information about local gateway, see Local Gateway Configurations. The local gateway refers to the IPsec VPN device on the IDC side. The public IP of this device is recorded in the “customer gateway” created in Step 2.

A local gateway is generally deployed in the following scenarios:

Note:

In both scenarios below, you should configure the same VPN tunnel on your local gateway as that configured in Step 3. Otherwise, the VPN tunnel cannot be connected.

You can view the VPN tunnel configurations in the VPN Tunnel console. You can also click **Download config file** to download the configuration information and upload it to the IPsec VPN gateway of the local IDC for configuration.

Connecting Tencent Cloud to a local IDC

A local gateway is a network device with the VPN feature and is generally an egress router or a firewall of an IDC. You can configure the VPN connection on the local gateway.

Note:

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

Connecting Tencent Cloud to another public cloud

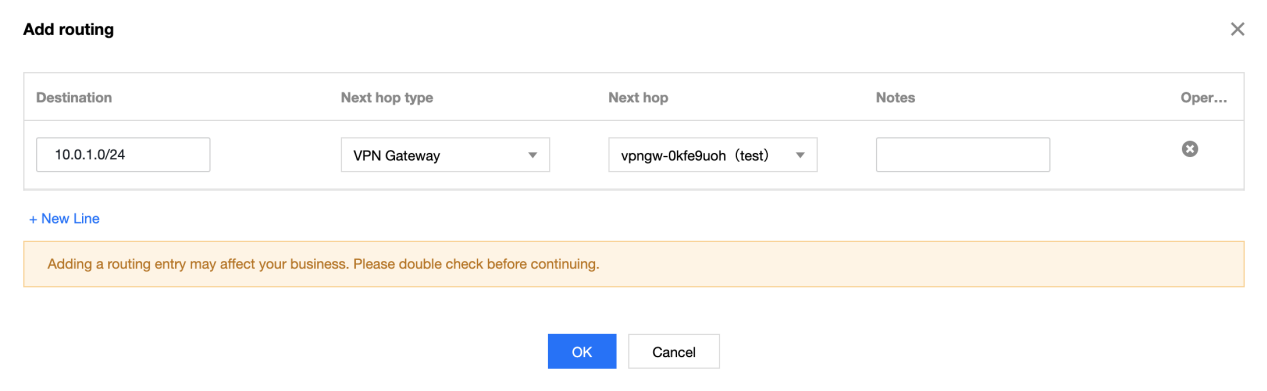
A local gateway is the VPN gateway on the target public cloud. You need to configure the VPN connection on the VPN gateway of the target public cloud. For more information about configuration method, see the documentation of the target public cloud.

Step 5: Configure a Routing Table

Last updated：2024-01-09 14:20:07

After you complete Step 4, the VPN tunnel is successfully configured. Next, you need to configure a route table to route the traffic of subnet A to the VPN gateway so that the IP range in subnet A can communicate with the IP range in the IDC.

1. Log in to the Virtual Private Cloud Console.
2. In the left sidebar, click **Subnet**. Choose the region where your VPC resides and your VPC, i.e. **Guangzhou** and `TomVPC` in this example, and click the associated route table of the subnet A to go to the details page.
3. Click **+ New**.
4. In the **Create Route Table** pop-up window, enter the destination IP range (`10.0.1.0/24`). Select **VPN Gateway** for **next hop type**, and the new VPN gateway `TomVPNGw` for **next hop**.



Step 6: Activate a VPN Tunnel

Last updated：2024-01-09 14:20:07

After configuring the Tencent Cloud VPN gateway, VPN tunnel, customer gateway, and users' local IDC, you can use a Ping command to activate the tunnel. The step is to verify whether Tencent Cloud connects to 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 IDC configuration. For technical support, please submit a ticket.

Connecting VPC to IDC (Destination route)

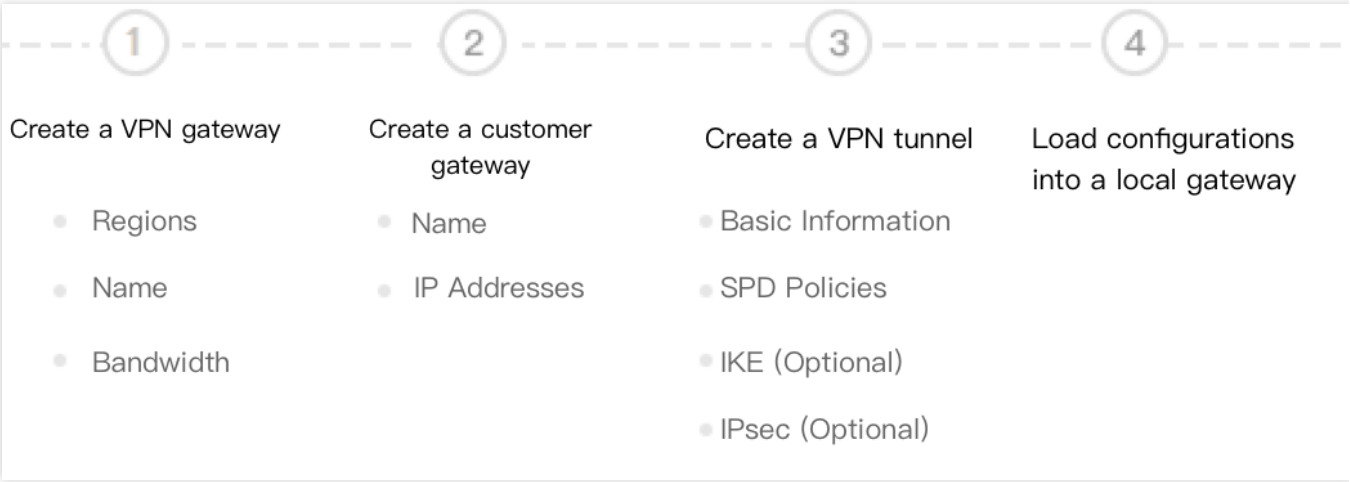
Overview

Last updated：2024-01-09 14:20:07

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.

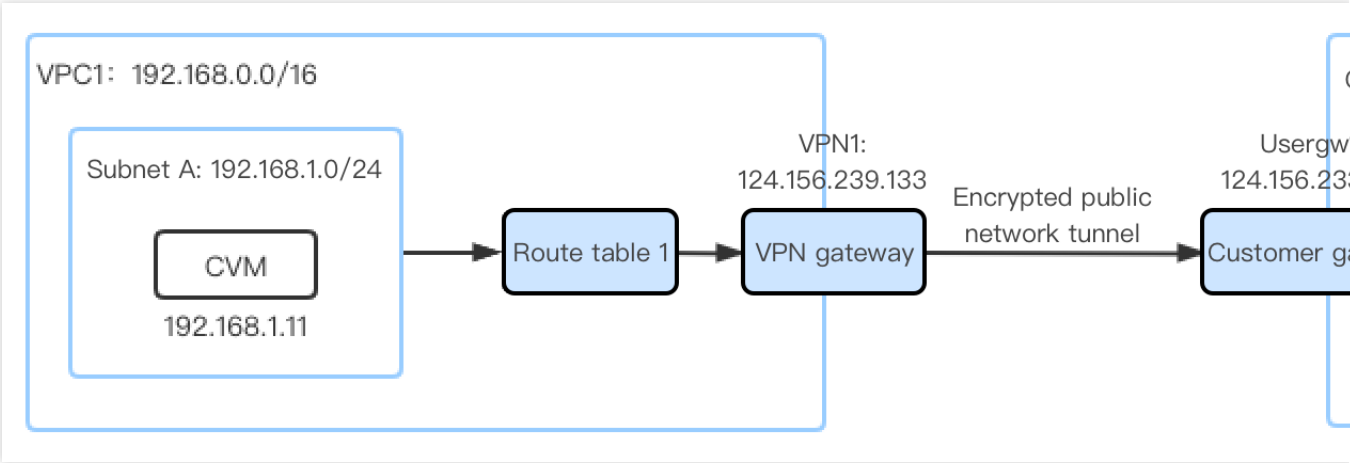
Directions

Below is the flowchart of activating a VPN connection:



Example

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



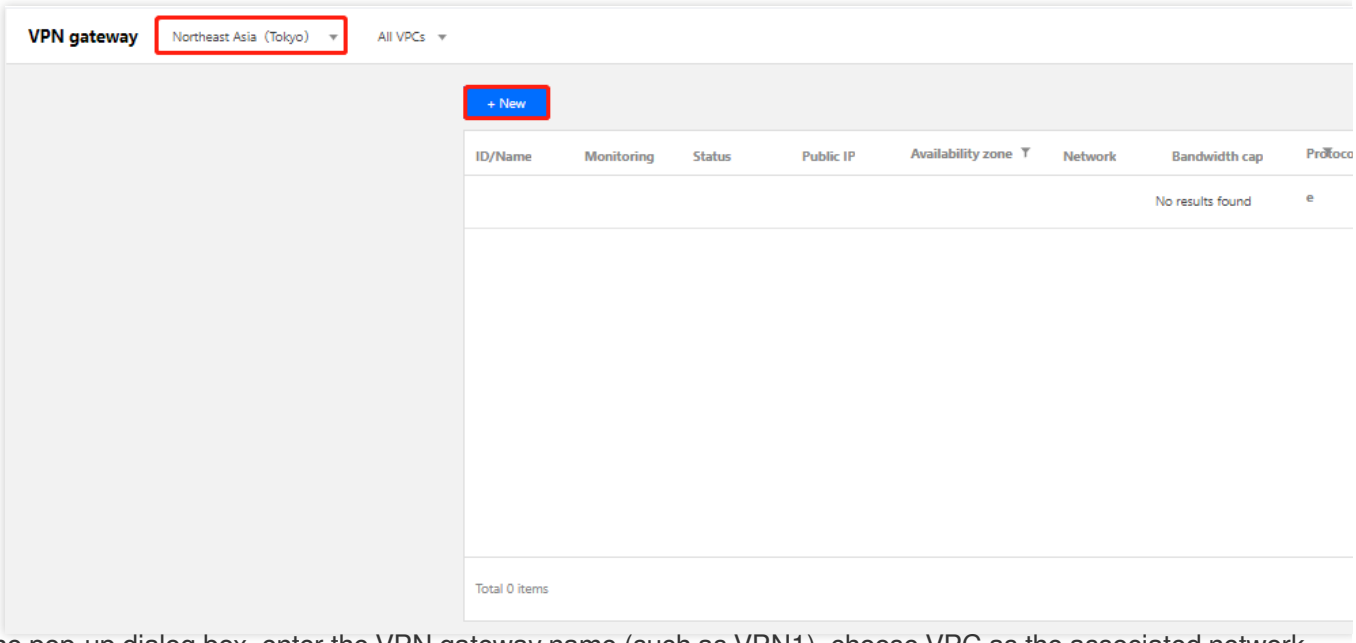
Step 1: Create a VPN Gateway

Last updated：2024-01-09 14:20:07

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Choose a region (**Tokyo** in this example), and click **+New**.

Note:

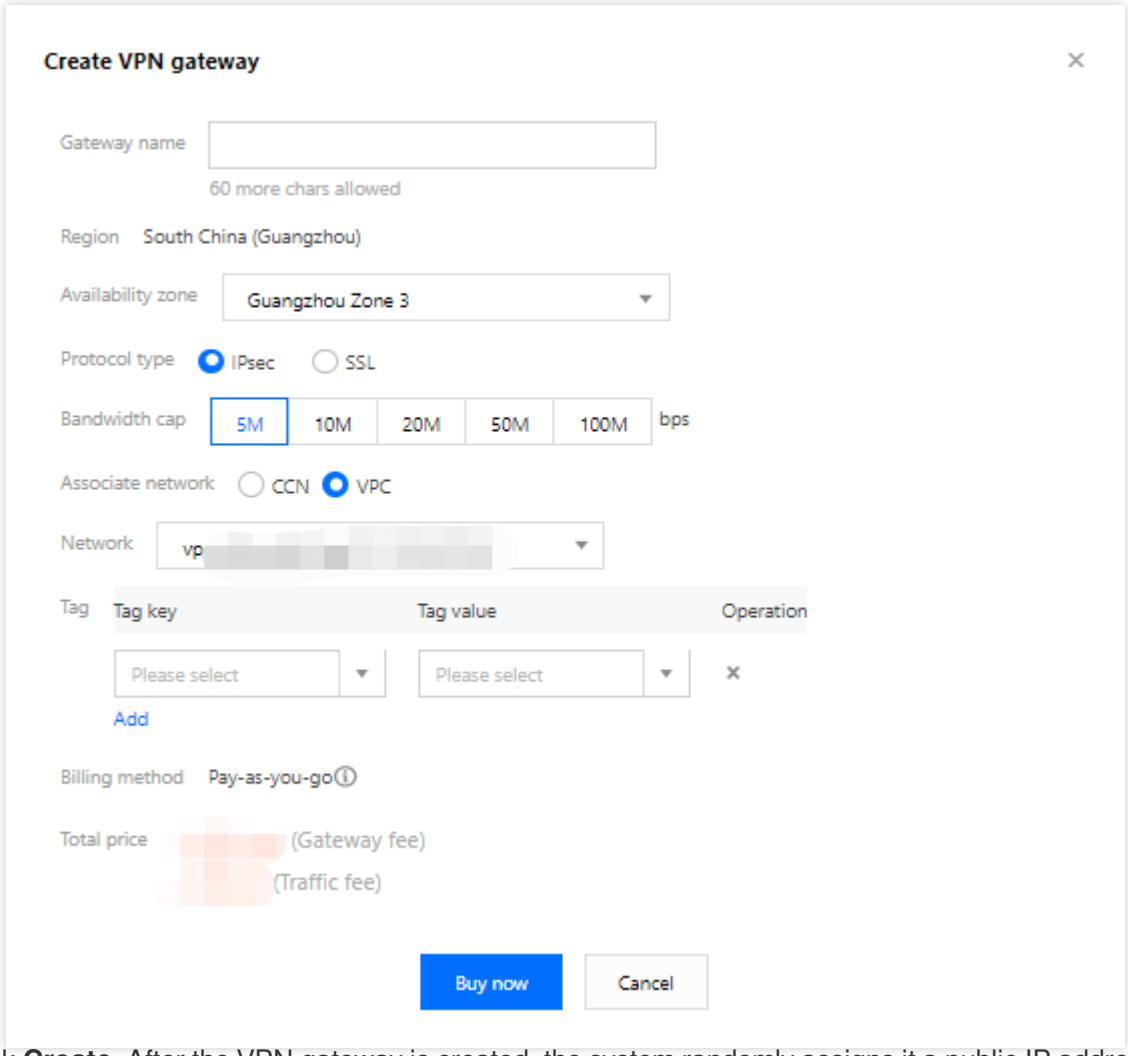
If the **+New** button is grayed out and “No VPC available” is displayed when the mouse hovers over it, create a VPC as instructed in Creating VPCs before creating the VPN gateway.



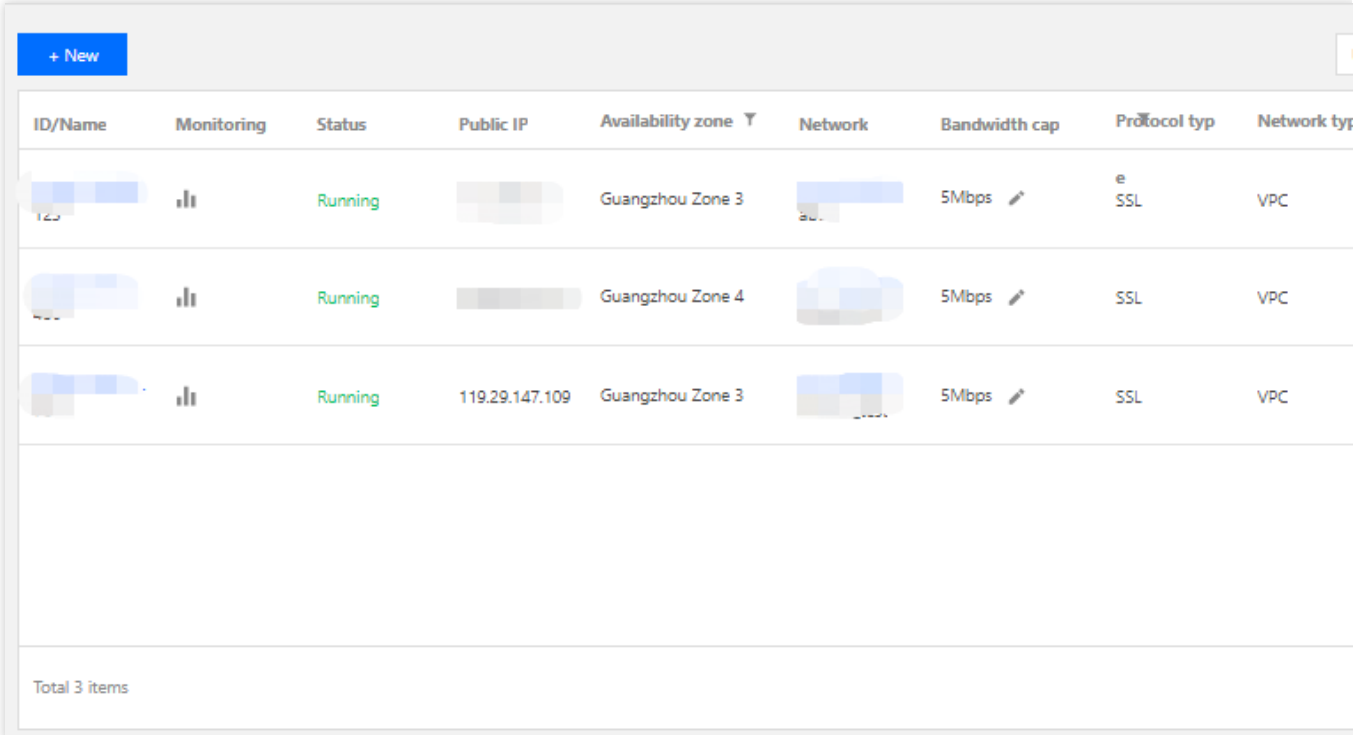
4. In the pop-up dialog box, enter the VPN gateway name (such as VPN1), choose VPC as the associated network, choose VPC1 as the network it belongs to, and select the bandwidth cap and billing method.

Note:

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



5. Click **Create**. After the VPN gateway is created, the system randomly assigns it a public IP address such as `119.29.147.109` .



Step 2: Create a Customer Gateway

Last updated：2024-01-09 14:20:07

1. Log in to the VPC console.
2. Click **VPN Connection** > **Customer Gateway** on the left sidebar to go to the management page.
3. Choose a region (**Tokyo** in this example), and click **+New**.
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` .
5. Click **Create**. A successfully created VPN tunnel is shown as below.

Step 3: Create a VPN Tunnel

Last updated：2024-01-09 14:20:07

1. Log in to the VPC console.
2. Select **VPN Connections** > **VPN Tunnel** in the left sidebar.
3. Choose a region and VPC (**Tokyo** and `VPC1` in this example) and click **+New**.
4. Configure the basic settings of the VPN tunnel.

The basic settings of a VPN tunnel include the tunnel name, region of the gateway, network type, VPN gateway instance, customer gateway instance, pre-shared key, negotiation type, and communication mode. For more information about the parameters, see Creating a VPN Tunnel.

In this example, the communication mode is **Destination route**.

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.

6. After you created the VPN tunnel successfully, return to the VPN tunnel list page. Click **More** and choose **Download config file** to complete the download.

Step 4: Configure a Local Gateway

Last updated：2024-01-09 14:20:07

After the first 3 steps, the VPN gateway and VPN tunnel on the Tencent Cloud are configured. Then, you need to configure the VPN tunnel on the local gateway of the IDC. For more information about local gateway, see Local Gateway Configurations. The local gateway refers to the IPsec VPN device on the IDC side. The public IP of this device is recorded in the “customer gateway” created in Step 2.

A local gateway is generally deployed in the following scenarios:

Note:

In both scenarios below, you should configure the same VPN tunnel on your local gateway as that configured in Step 3. Otherwise, the VPN tunnel cannot be connected.

You can view the VPN tunnel configurations in the VPN Tunnel console. You can also click **Download config file** to download the configuration information and upload it to the IPsec VPN gateway of the local IDC for configuration.

Connecting Tencent Cloud to a local IDC

A local gateway is a network device with the VPN feature and is generally an egress router or a firewall of an IDC. You can complete VPN settings on the local gateway.

Note:

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

Connecting Tencent Cloud to another public cloud

A local gateway is the VPN gateway of the target public cloud. You need to complete VPN settings on the VPN gateway of the target public cloud. For more information about configuration method, see the documentation of the target public cloud.

Step 5: Configure a Routing Policy

Last updated：2024-01-09 14:20:07

You can successfully configure a VPN tunnel after the aforementioned 4 steps, but you still need to configure a route table to route the traffic of the subnet A to the VPN gateway. Meanwhile, you need to configure the route table of the VPN gateway to import the traffic of the VPN gateway to the VPN tunnel. In this way, the IP range in subnet A can communicate with the IP range in the IDC.

1. Log in to the VPC console.
2. Click **Subnet** on the left sidebar and choose the corresponding region and VPC, such as **Tokyo** and `VPC1` in the example. Click the ID of the route table associated with subnet A to go to the details page.
3. Click **Add routing policy** on the “Basic Information” tab.
4. In the pop-up dialog box, enter the subnet IP range of the IDC (`10.0.1.0/24`). Choose **VPN gateway** as the “Next hop type” and choose the VPN gateway which has just been created, namely `VPN1` , as “Next hop”. Click **Create** to configure the route table of subnet A.
5. Click **VPN Connection** > **VPN Gateway** on the left sidebar.
6. Click the ID of the VPN gateway instance to go to the details page.
7. Click the **Route Table** tab on the “Instance Details” page to configure the routing policy of the VPN gateway.
8. Click **Add routing** and enter the following parameters in the pop-up dialog box:

Destination: enter the private network IP range of the customer IDC which needs to communicate with the local IDC. Enter `10.0.1.0/24` in this example.

Next hop type: VPN tunnel is the only option. No setting required.

Next hop: choose 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.

9. Click **OK** to complete the configuration of the VPN gateway route table.

Step 6: Activate a VPN Tunnel

Last updated：2024-01-09 14:20:07

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 A of VPC1 to ping the server IP address in the subnet of the customer IDC: ping 10.0.1.7.

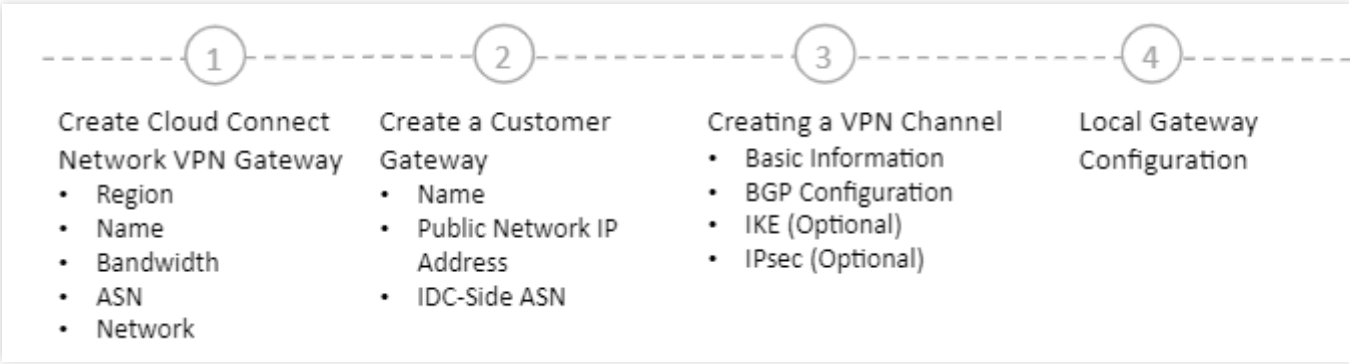
Connecting VPC to IDC (Dynamic BGP) Overview

Last updated：2024-08-15 16:18:44

This document describes how to quickly establish a VPN connection and use BGP for secure communication between the VPC and the peer IDC.

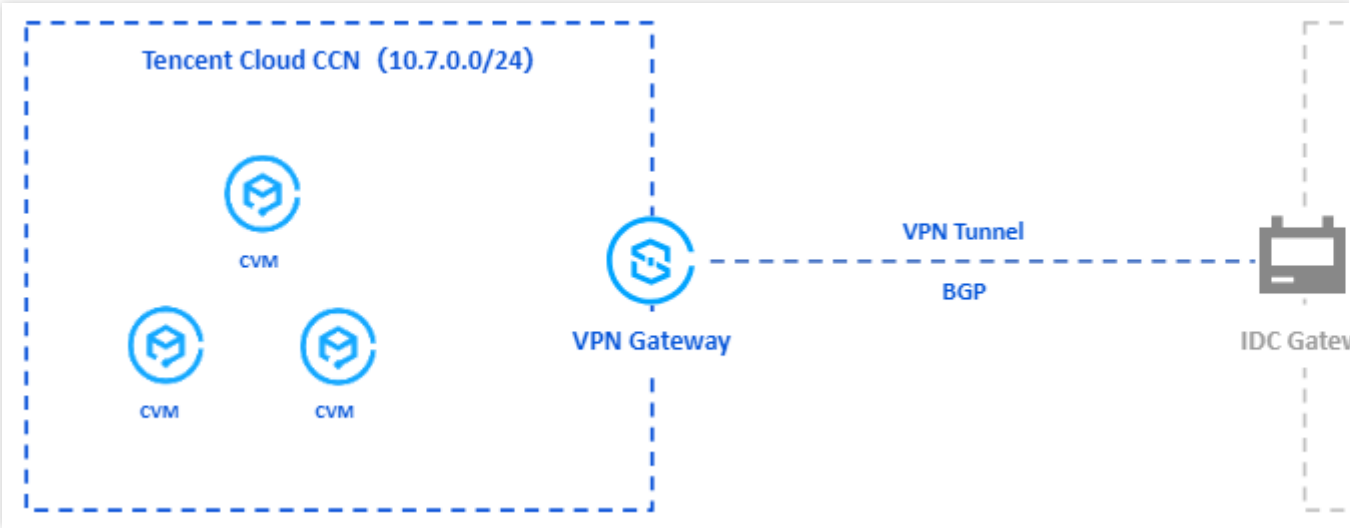
Step-by-Step Guide

The process diagram is as follows:



Sample Code

By establishing an IPsec VPN connection, you can connect subnet 1: 10.7.0.0/24 in your VPC in Seoul to subnet: 10.9.0.0/24 in your local IDC.



Step 1: Create a CCN VPN Gateway

Last updated：2024-08-15 16:18:04

1. Log in to the VPC console.
2. In the left navigation pane, choose **VPN Connection** > **VPN Gateway** to enter the management page.
3. Select a region, for example, Seoul, and click **Create**.

Note:

If **Create** appears grayed out, and hovering over it displays "No available VPC", please create a VPC before creating a VPN gateway.

4. In the pop-up dialog box, fill in the VPN gateway name (e.g., VPN1), select CCN as the associated network, and set the bandwidth cap, BGP ASN, billing method, etc.

Note:

Only VPN gateways with bandwidths of 200 Mbps, 500 Mbps, 1,000 Mbps, and 3,000 Mbps support dynamic BGP.
AES128+MD5 is recommended for VPN tunnel encryption.

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

Step 2: Create a Customer Gateway

Last updated：2024-08-15 16:15:44

1. Log in to the VPC console.
2. In the left navigation pane, choose **VPN Connection** > **Customer Gateway** to enter the management page.
3. Select a region, for example, Seoul, and click **Create**.
4. Fill in the customer gateway name (e.g., Usergw1) and the public IP address of the customer VPN gateway.

Note:

The ASN value range is from 1 to 4294967295, excluding 139341, 45090, and 58835.

A single customer gateway can be configured with only one ASN. That is, a public IP address can be configured with only one ASN.

5. click **OK**.

Step 3: Create a VPN Tunnel

Last updated：2024-08-15 16:15:12

1. Log in to the VPC console.
2. In the left navigation pane, choose **VPN Connection** > **VPN Tunnel**.
3. Select a region and VPC, and then click **Create**.
4. Set basic parameters of the VPN tunnel.

Basic configuration includes filling in the tunnel name and selecting the gateway region, network type, VPN gateway instance, customer gateway instance, preshared key, negotiation type, and communication mode. For the specific meanings of the parameters, see Creating a VPN Tunnel.

5. Set advanced parameters.

Advanced configuration includes DPD detection, IKE configuration, IPSec information, etc. This example uses the default configuration. After the configuration, click **Create**.

Note:

When configuring IKE and IPSec information, ensure that the configuration on the cloud side is consistent with the local configuration, thus preventing the tunnel from being disrupted due to inconsistent protocol configurations.

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

Step 4: Configure a Local Gateway

Last updated：2024-08-15 16:14:50

After the first 3 steps are completed, the configuration of the cloud VPN gateway and VPN tunnel is complete. You need to continue configuring the VPN tunnel information of the other side on the local gateway at the IDC side. For details, see Local Gateway Configurations. The local gateway on the IDC side is the IPsec VPN device at the IDC, and its public IP address is recorded in the customer gateway in Step 2: Create a Customer Gateway.

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 be consistent with the VPN tunnel information in Step 3: Create a VPN Tunnel; otherwise, the VPN tunnel cannot connect properly.

The VPN tunnel configuration information on Tecent Cloud can be viewed through the VPN tunnel console and imported by downloading the configuration file, which is then loaded into the IPsec VPN gateway of the local data center to complete the configuration.

Establishing connectivity between Tecent Cloud and the local data center

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

Note:

Configurations may vary according to the network device manufacturers (such as H3C and Cisco). Please configure according to the specific circumstances of the network devices.

Establishing connectivity between Tecent Cloud and other public clouds

The local gateway is the VPN gateway on your target public cloud. You need to operate the VPN gateway on the target public cloud to complete the VPN configuration for the local gateway. Please refer to the documentation of the target public cloud for specific configuration methods.

Step 6: Activate a VPN Tunnel

Last updated：2024-08-15 16:13:52

After configuring the VPN gateway, VPN tunnel, customer gateway, and user's local configuration on Tecent Cloud, you can use a ping command to activate the tunnel to verify whether Tecent Cloud connects to the user.

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

If the ping action succeeds, Tecent Cloud connects to the user's VPN tunnel.

If the ping action fails, check the customer's local configuration. For technical support, please submit a ticket.

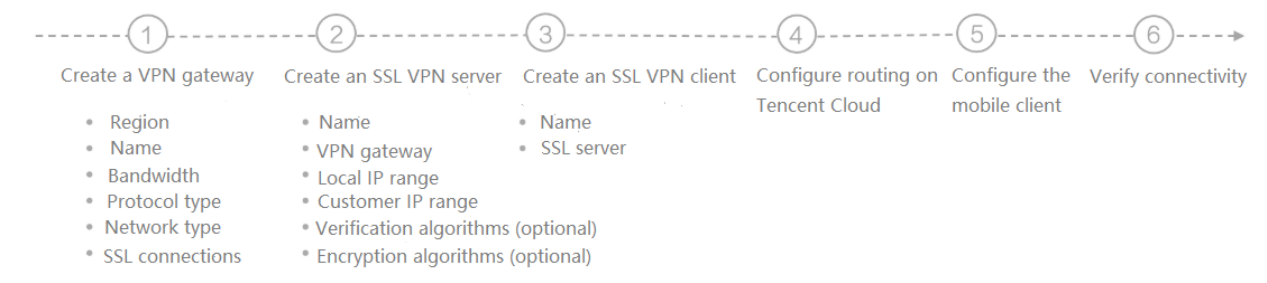
SSL VPN
Connecting the Mobile Client to VPC
Directions

Last updated：2024-01-09 14:20:07

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.

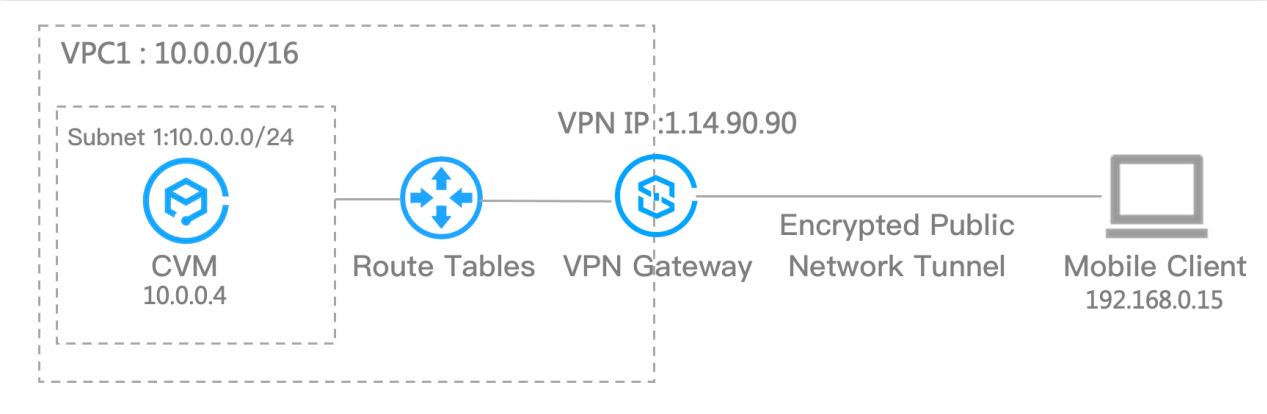
Directions

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



Example

Let's assume that you need to establish an SSL VPN connection to connect the subnet 1: `10.0.0.0/16` in your VPC in Guangdong Region 2 to the subnet: `192.168.0.0/16` in your mobile terminal.



Step 1: Create an SSL VPN Gateway

Last updated：2024-01-09 14:22:13

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.

Directions

1. Log in to the VPC console.
2. Select **VPN Connections** > **VPN Gateway** in the left sidebar to enter the admin page.
3. Click **+New**.
4. Configure the following gateway parameters in the pop-up window.

Parameter	Configuration
Gateway name	Enter the VPN gateway name (up to 60 characters).
Region	Display the region of the VPN gateway.
AZ	Select the availability zone.
Protocol Type	Select SSL.
Bandwidth cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Associated Network	Select the network type for accessing resources in the cloud. VPC is used as an example here.
Network	Select the VPC associated with the VPN gateway.
SSL VPN Connections	Set the number of SSL VPN connections on the mobile clients. **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.
Billing Mode	Bill-by-traffic is used by default.

5. Click **Create**.

Step 2: Create an SSL VPN Server

Last updated：2024-01-09 14:20:07

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. Select **VPN Connections** > **SSL VPN Server** in the left sidebar to enter the admin page.
3. Click **+New**.
4. Configure the following parameters in the pop-up window.

Parameter	Configuration
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.
Server 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.
Verification algorithm	Supported authentication algorithms: SHA1 and MD5.
Encryption algorithm	Supported encryption algorithms: AES-128-CBC, AES-192-CBC, and AES-256-CBC.
Compressed	No.
Verification 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. Click **Create**.

Step 3: Create an SSL VPN Client

Last updated：2024-01-09 14:20:07

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.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Client** in the left directory to enter the admin page.
3. Click **+New**.
4. Configure the following parameters in the pop-up window.

Parameter	Configuration
Name	Enter the SSL VPN server name (up to 60 characters)
Region	Displays the region of the SSL VPN server.
SSL VPN Server	Select an existing SSL VPN server.

5. Click **Create**. When the **Certificate Status** goes **Available**, the creation is completed.

Step 4: Configure the Tencent Cloud Routing Policy

Last updated：2024-01-09 14:20:07

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

Directions

1. Log in to the VPC console.
2. Click **Route Tables** on the left sidebar to enter the admin page.
3. Click **+New**.
4. Configure the following parameters in the pop-up window.

Parameter	Configuration
Destination	Enter the mobile client IP range
Next Hop Type	Select VPN Gateway
Next Hop	Select an existing VPN gateway

5. Click **Create**.

Step 5: Configure the Mobile Client

Last updated：2024-01-09 14:20:07

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

Directions

1. Download the SSL VPN client verification file assigned by Tencent Cloud. See Downloading SSL VPN Client Configuration.

Note:

The download SSL VPN client certificate can only be used for one local client.

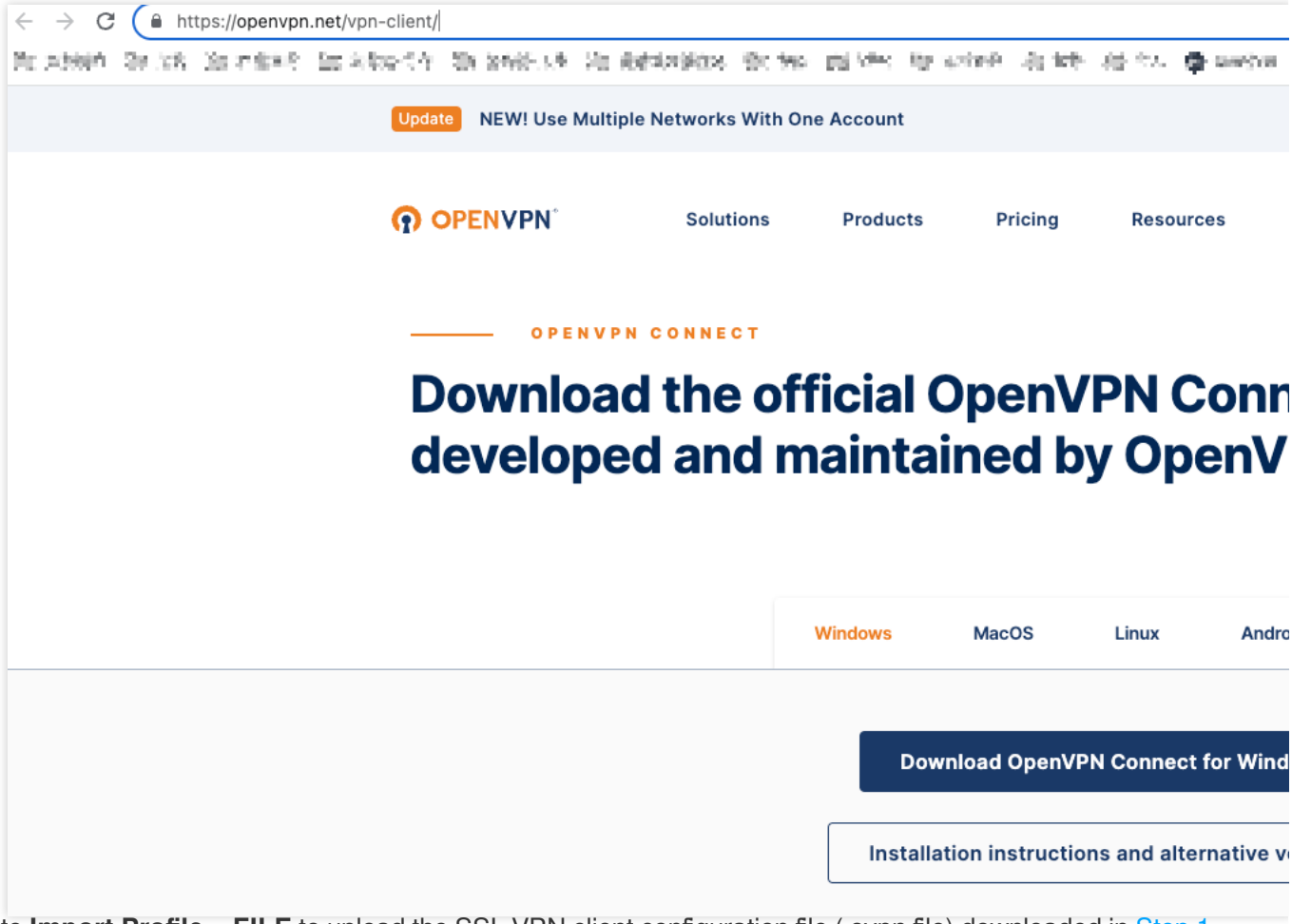
2. Download OpenVPN and install it on the mobile device.

Windows client

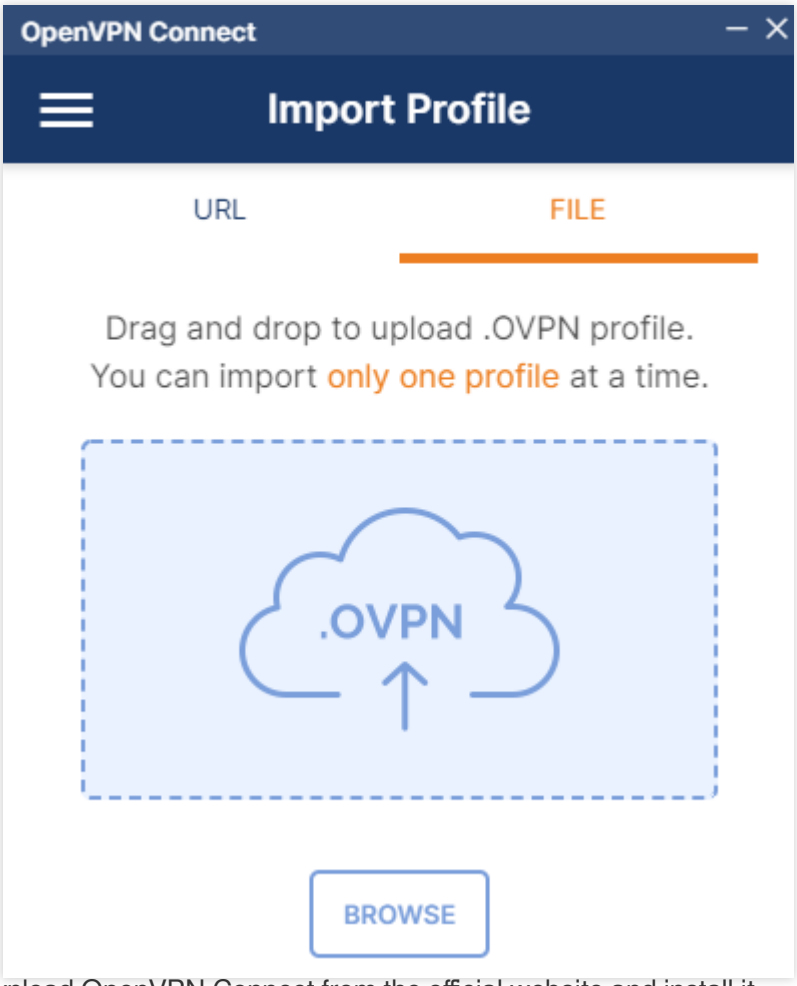
MAC client

Linux client

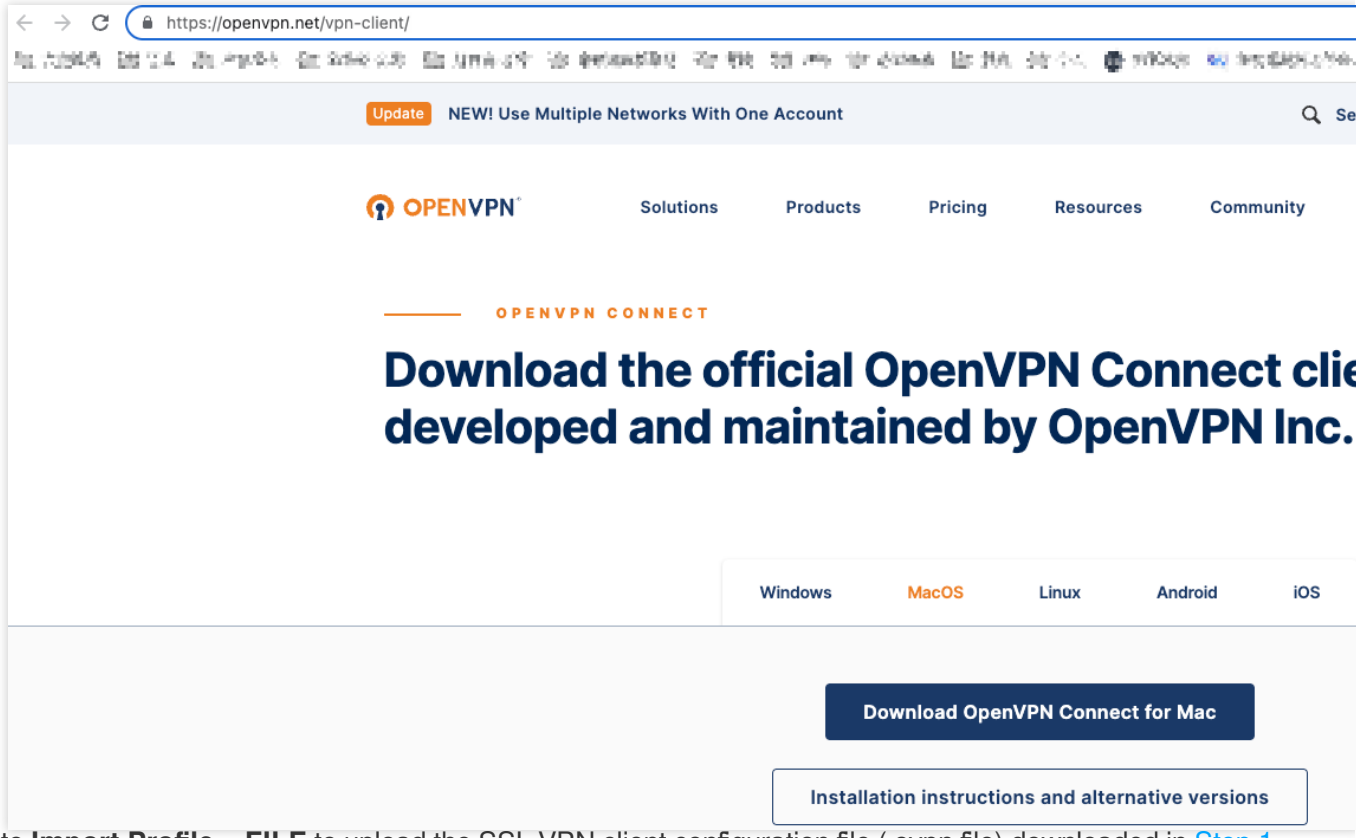
1. Download OpenVPN Connect from the official website and install it.



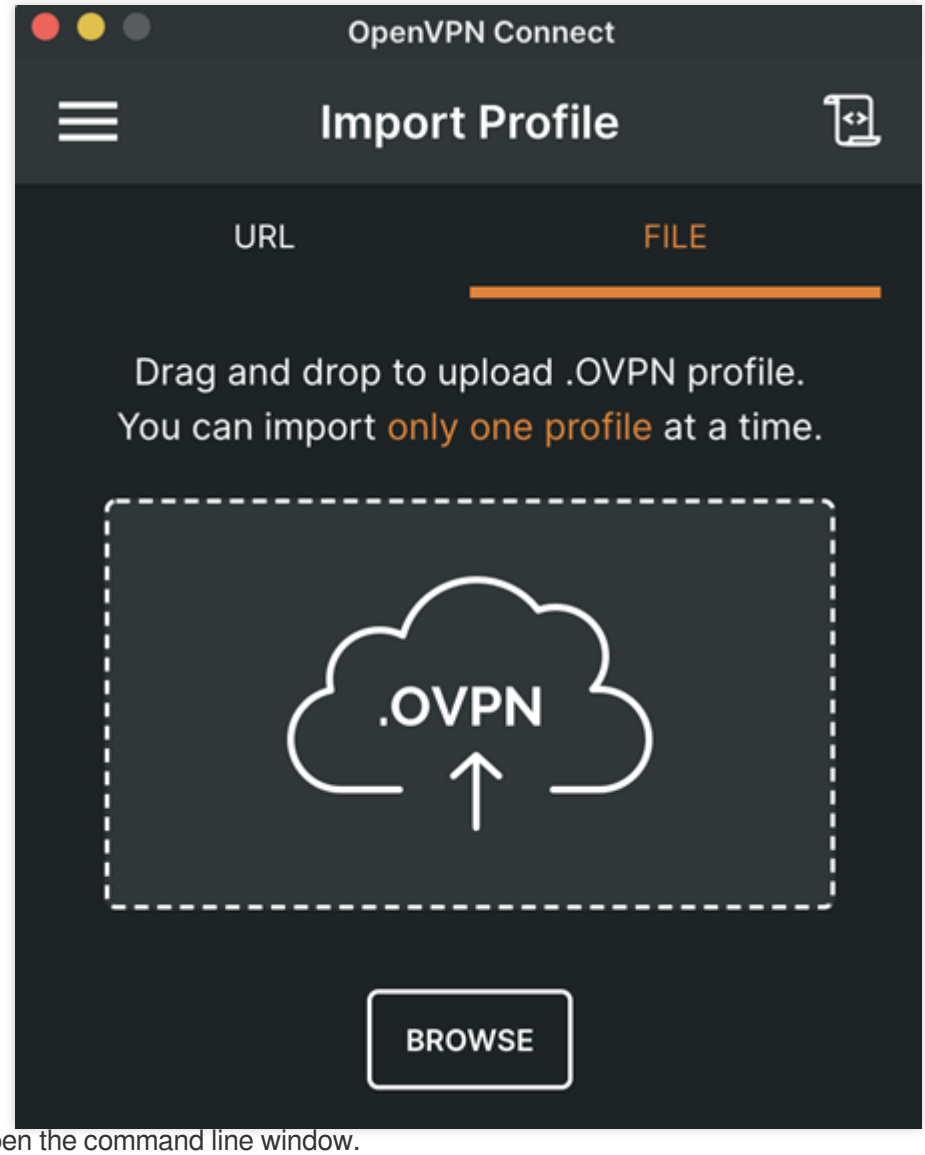
2. Go to **Import Profile** > **FILE** to upload the SSL VPN client configuration file (.ovpn file) downloaded in Step 1.



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

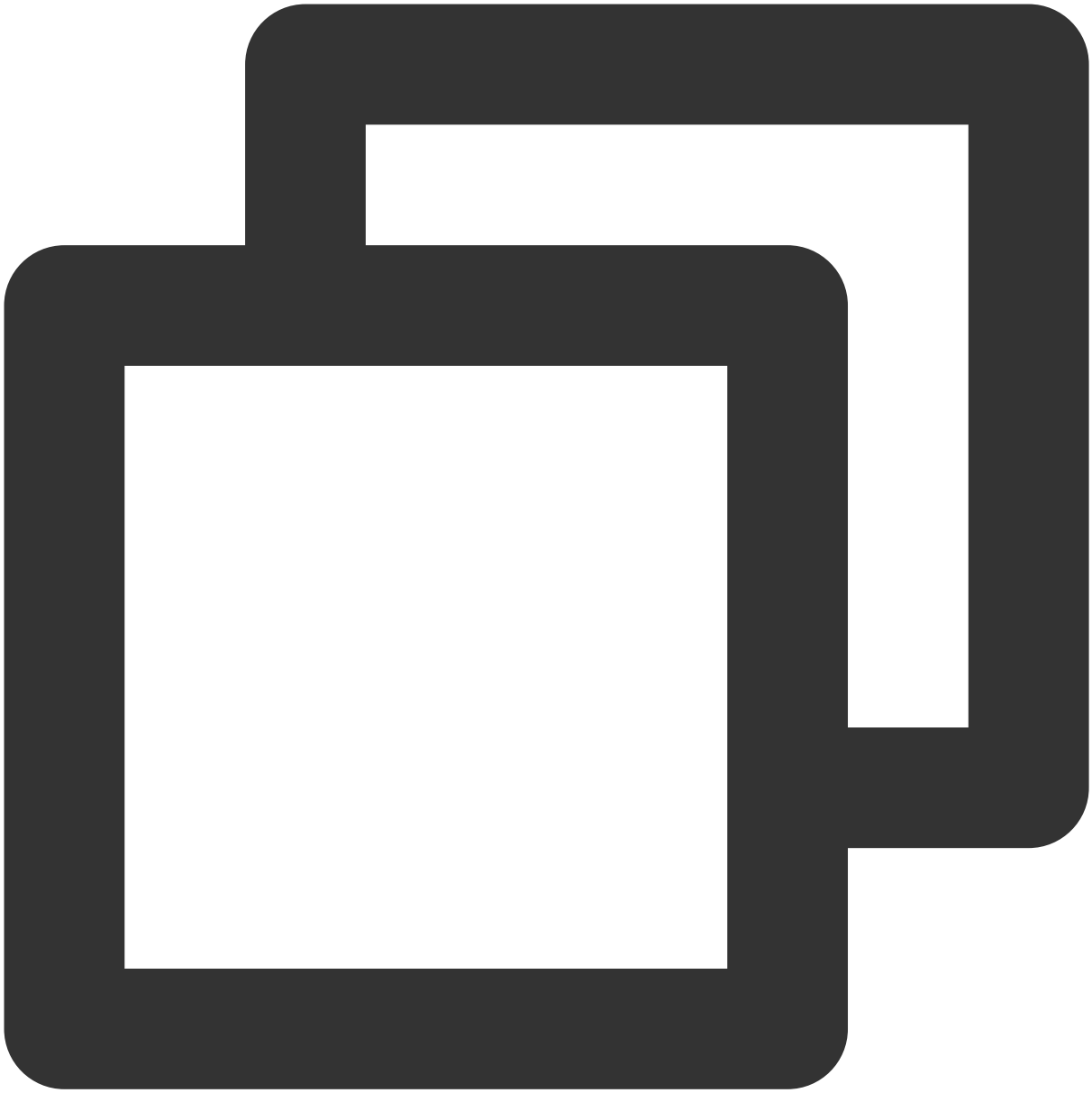


2. Go to **Import Profile** > **FILE** to upload the SSL VPN client configuration file (.ovpn file) downloaded in Step 1.



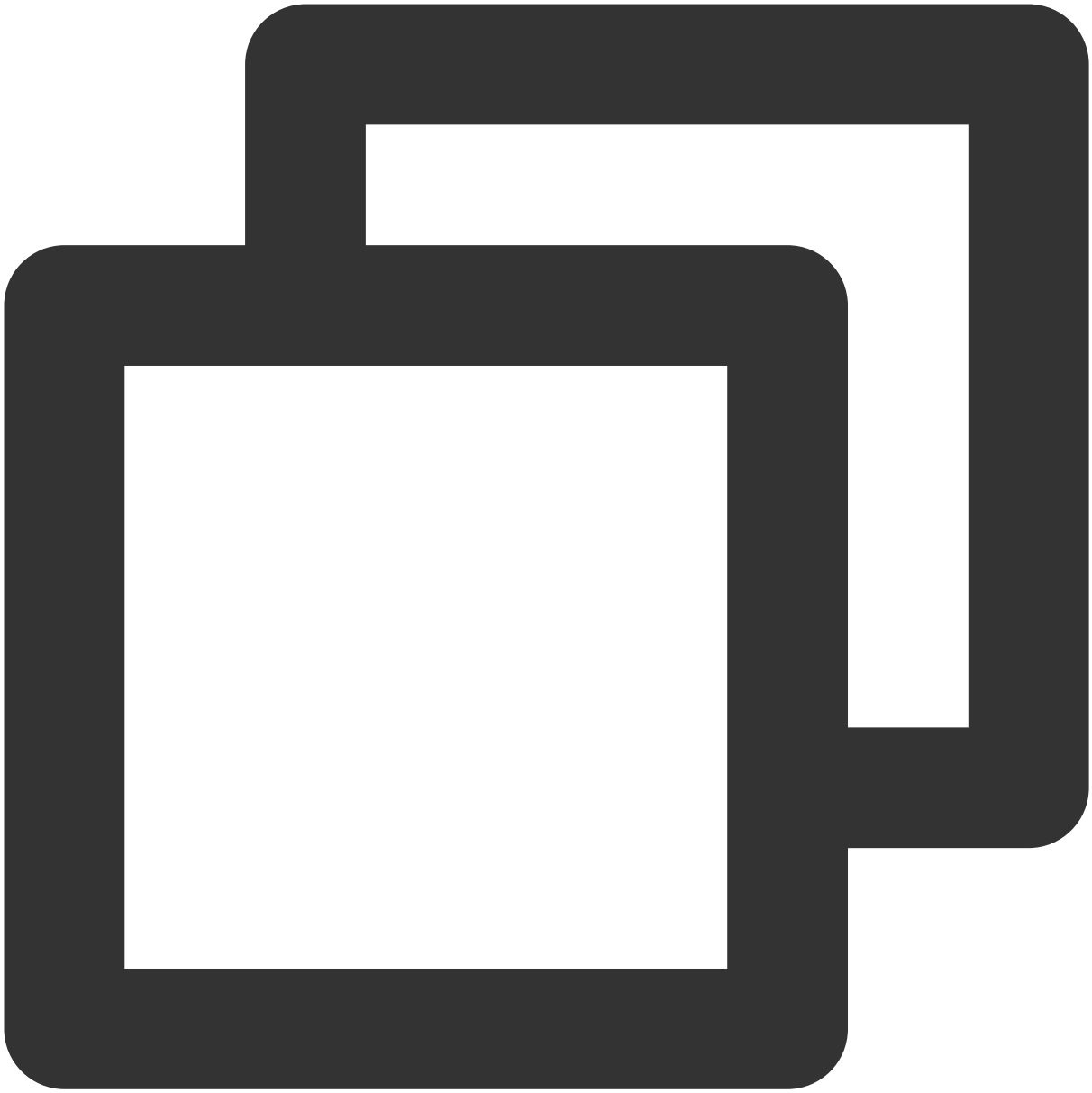
1. Open the command line window.
2. Run the following command to install OpenVPN Connect.

CentOS distribution



```
yum install -y openvpn
```

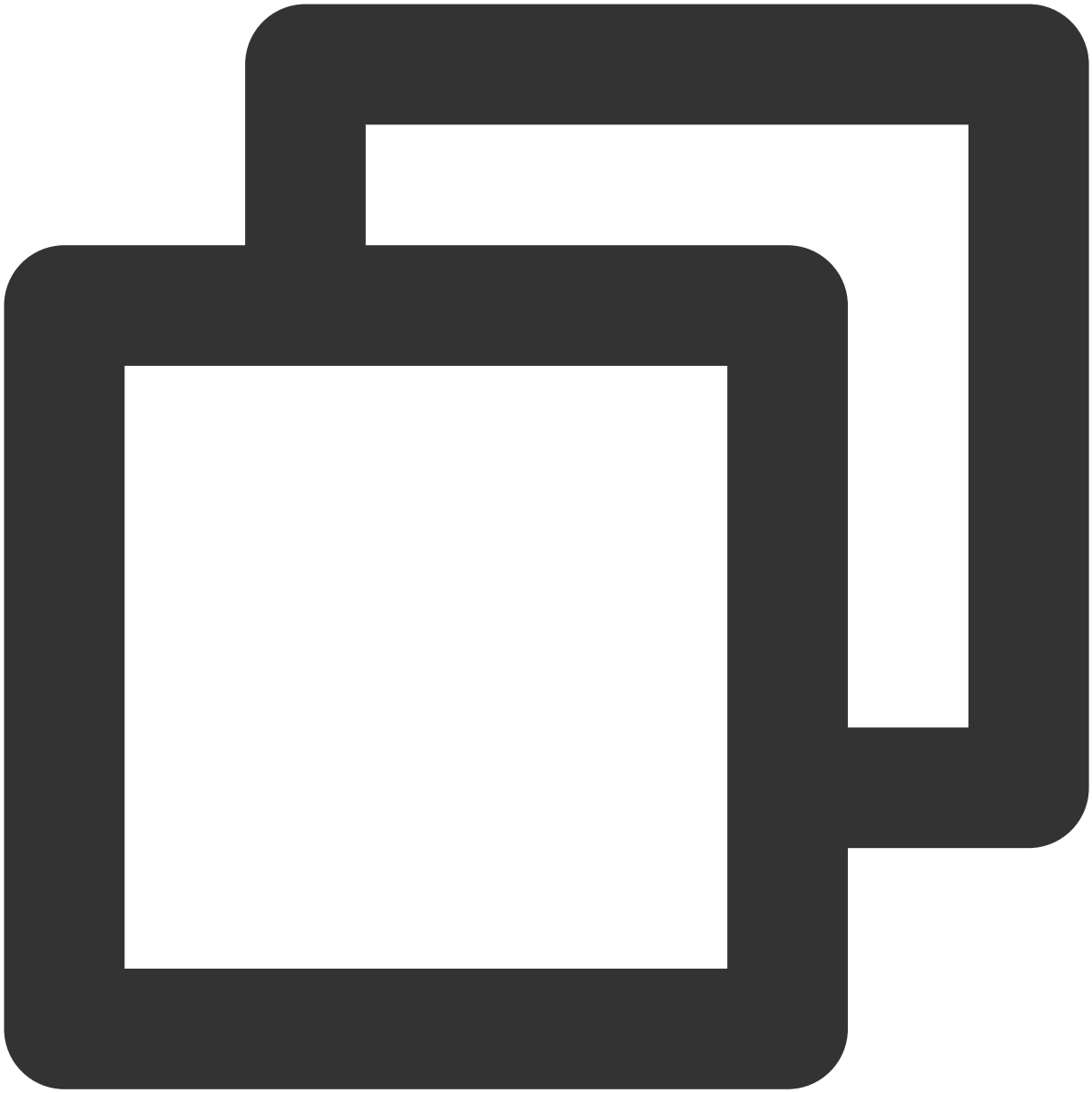
Ubuntu distribution



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

3. Unzip the SSL VPN client certificate from the package downloaded in Step 1 and copy it to the `/etc/openvpn/conf/` directory.

Enter the `/etc/openvpn/conf/` directory and run the following command to establish a VPN connection.



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

Step 6: Test the Connection

Last updated：2024-01-09 14:20:07

After establishing the SSL VPN connection between Tencent Cloud and the client, you can use `ping` to test it. For example, you can use the CVM in the VPC to `ping` an IP address in the mobile client IP range. If the pinging succeeds, the VPC and IDC can communicate with each other.