

VPN Connections

Getting Started

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Getting Started

Connecting VPC to IDC (SPD Policy)

Overview

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 a VPN Tunnel

Connecting VPC to IDC (Route Table)

Overview

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 a VPN Tunnel

Getting Started

Connecting VPC to IDC (SPD Policy)

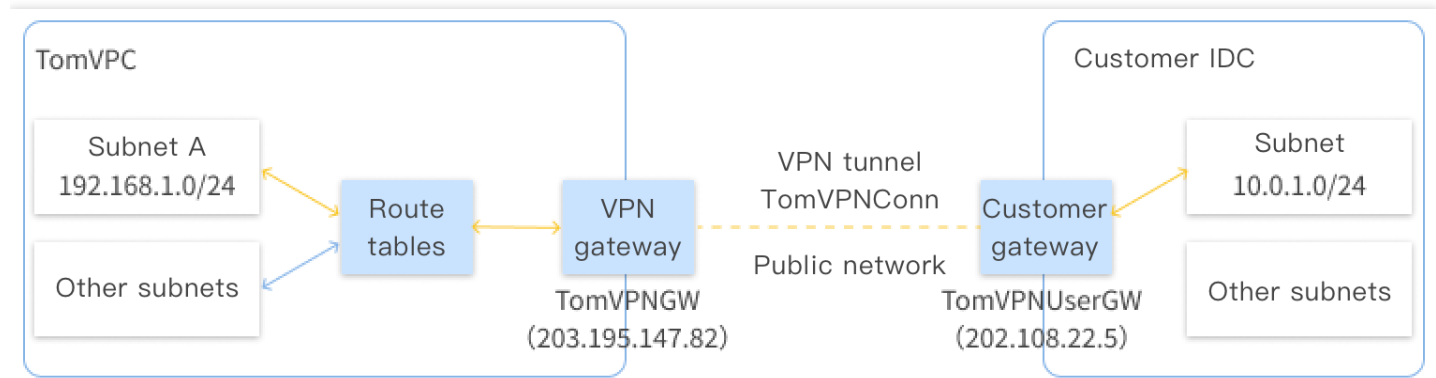
Overview

Last updated : 2021-06-15 11:08:46

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.

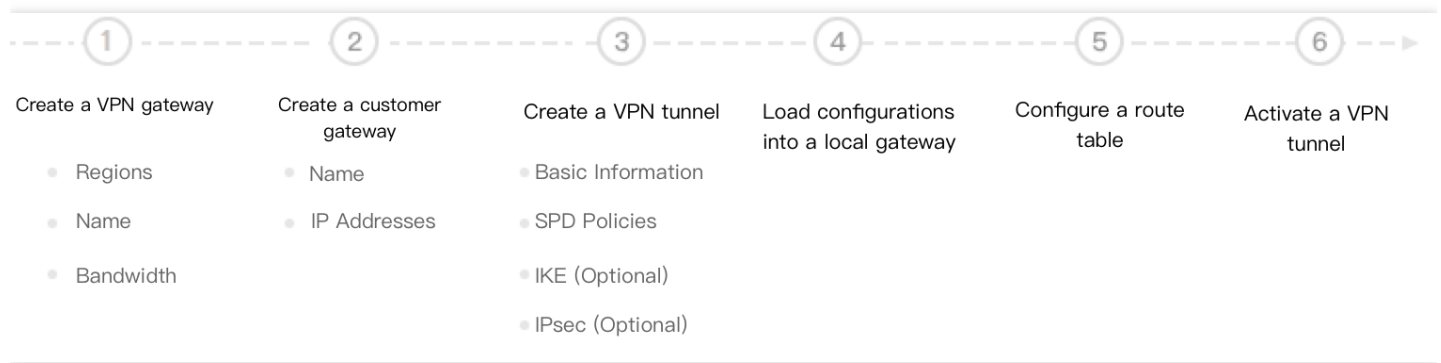
Example

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 : 2021-03-09 17:55:26

1. Log in to [VPC Console](#).
2. In the left sidebar, choose **VPN Connection** -> **VPN Gateway** to go to the management page.
3. Choose a region (**Guangzhou** in this example), and click **+New**.

Note :

If the **+New** button is grayed out, and prompts “No available VPC” when you hover over it, [create a VPC](#) before creating the VPN gateway.

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


Create a VPN gateway ×

Gateway Name
60 more chars allowed

Region South China (Guangzhou)

Network

Bandwidth Cap bps

Billing method Postpaid 

Total Price **0.078 USD/hour** (Gateway fee) | **0.12 USD/GB** (Traffic fee)

Step 2: Create a Customer Gateway

Last updated : 2021-03-09 17:52:15

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

1. Log in to [VPC Console](#).
2. In the left sidebar, choose **VPN Connection** > **Customer Gateway** to go to the management page.
3. Choose a region, i.e. **Guangzhou** in this example, and click **New**.
4. Enter the name of the customer gateway (for example, TomVPNUserGw) and the public IP address (for example, 202.108.22.5) of the VPN gateway of the IDC.

Create Customer Gateway ✕

Name ⓘ
60 more chars allowed

Public IP . . . ⓘ

5. Click **Create**.

Step 3: Create a VPN Tunnel

Last updated : 2021-03-09 17:50:06

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

1. Log in to [VPC Console](#).
2. In the left sidebar, choose **VPN Connection** > **VPN Tunnel** to go to the management page.
3. Select the region (such as Guangzhou) and VPC (such as TomVPC), and click **+New**.
4. Enter a name for the tunnel (for example, TomVPNConn), select the VPN gateway `TomVPNGw` and the customer gateway `TomVPNUserGw`, enter the pre-shared key (for example, `123456`), and click **Next**.

The screenshot shows the 'Create VPN Tunnel' form in the Tencent Cloud console. The form includes the following fields and options:

- Tunnel Name ***: A text input field with the placeholder 'Please enter a tunnel name' and a note '60 more chars allowed'.
- Region**: A grid of buttons for various regions, with 'South China (Guangzhou)' selected. Other regions include East China (Shanghai), North China (Beijing), Southwest China (Chengdu), Southwest China (Chongqing), Southeast Asia (Singapore), Asia Pacific (Bangkok), South Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Tokyo), Western US (Silicon Valley), Eastern US (Virginia), North America (Toronto), Europe (Frankfurt), and Europe (Moscow).
- Virtual Private Cloud ***: A dropdown menu showing 'vpc-s1e2bu0d (test2 | 192.168.0.0/16)'.
- VPN Gateway ***: A dropdown menu showing 'test(test2)'.
- Customer Gateway ***: Radio buttons for 'Select existing' (selected) and 'Create', followed by a dropdown menu.
- Customer Gateway IP**: A field with a hyphen '-'.
- Protocol type**: A dropdown menu showing 'IKE/IPsec'.
- Pre-shared key ***: A text input field with the placeholder 'Please enter a pre-shared key' and a help icon.

5. Enter an SPD policy to limit the communication between local IP ranges and customer IP ranges. In this example, the local IP range is `192.168.1.0/24` of subnet A, and the customer IP range is

10.0.1.0/24 . Then, click **Next**.

SPD policy: It is used to specify which IP ranges in the VPC and IDC can communicate with each other. The rules in all tunnels under the same VPN gateway cannot overlap. [Click to view details.](#)

Local VPC 192.168.0.0/16

Rules ⓘ	Local IP address range	Peer IP range	Operation
Rules 1	<input type="text" value="192.168.1.0/24"/>	<input type="text" value="10.0.1.0/24"/>	Delete
+ New line			

[Back](#)

[Next](#)

[Cancel](#)

6. (Optional) Configure IKE parameters. Click **Next** if no advanced configuration is required.

IKE Configuration

Version	IKE V1	
ID verification methods	Pre-shared key	
Encryption algorithm	3DES	▼
Verification algorithm	MD5	▼
Negotiation model	main	▼
Local identifier	IP Address	▼ 123.207.16.14
Remote ID	IP Address	▼ 122.233.211.11
DH group	DH1	▼ ⓘ
IKE SA Lifetime	86400	s

[Back](#)

7. (Optional) Configure IPsec parameters. Click **Complete** if no configuration is required.

IPSec Information

Encryption algorithm	3DES	
Verification algorithm	MD5	
Packet encapsulation mode	Tunnel	
Security protocol	ESP	
PFS	disable	
IPsec sa Lifetime(s)	3600	s
IPsec sa Lifetime(KB)	1843200	KB

[Back](#)

8. After the VPN tunnel is successfully created, return to the VPN tunnel list page and click **Download config file** to complete the download.

ID/Name	Monitoring	Status	Customer Gateway	Network	Pre-shared key	Operation
vpn-x-o4p7blog ss		Non-linked	cgw-7s54ktdl 122.233.211.11(122.233.211.11)	vpc-s1e2bu0d test2	aaa	Reset More Delete Download config file Edit Tags

Step 4: Configure a Local Gateway

Last updated : 2021-07-05 10:51:32

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 Policy

Last updated : 2021-06-15 11:11:43

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**.

Add routing ✕

Destination	Next hop type	Next hop	Notes	Oper...
<input type="text" value="10.0.1.0/24"/>	<input style="border: none; background-color: #f0f0f0;" type="text" value="VPN Gateway"/>	<input style="border: none; background-color: #f0f0f0;" type="text" value="vpngw-0kfe9uoh (test)"/>	<input type="text"/>	<input type="button" value="✕"/>

[+ New Line](#)

Adding a routing entry may affect your business. Please double check before continuing.

Step 6: Activate a VPN Tunnel

Last updated : 2019-12-03 18:24:36

Ping an IP address in the customer IP range from a CVM in the VPC to activate the VPN tunnel.

For example, `ping 10.0.1.1` from a CVM in subnet A of `TomVPC` .

Connecting VPC to IDC (Route Table)

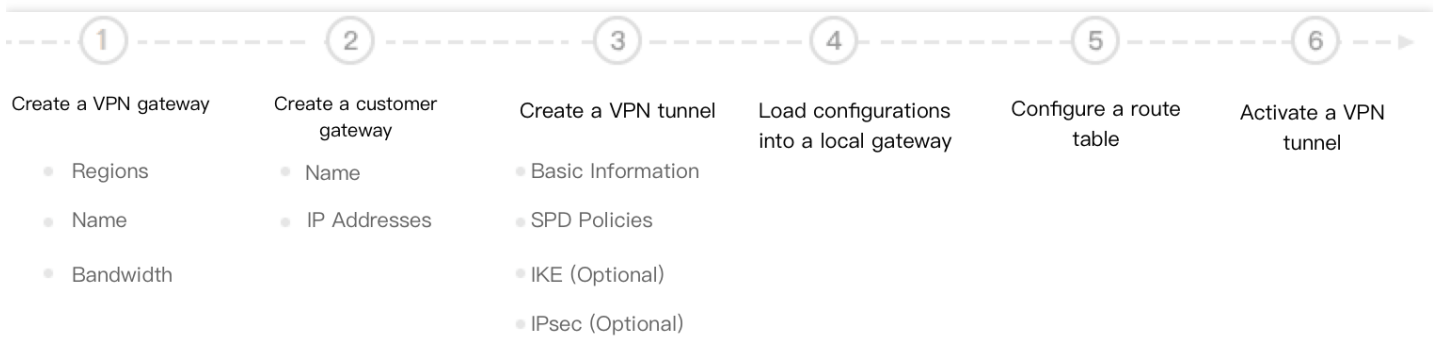
Overview

Last updated : 2021-06-15 10:31:20

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.

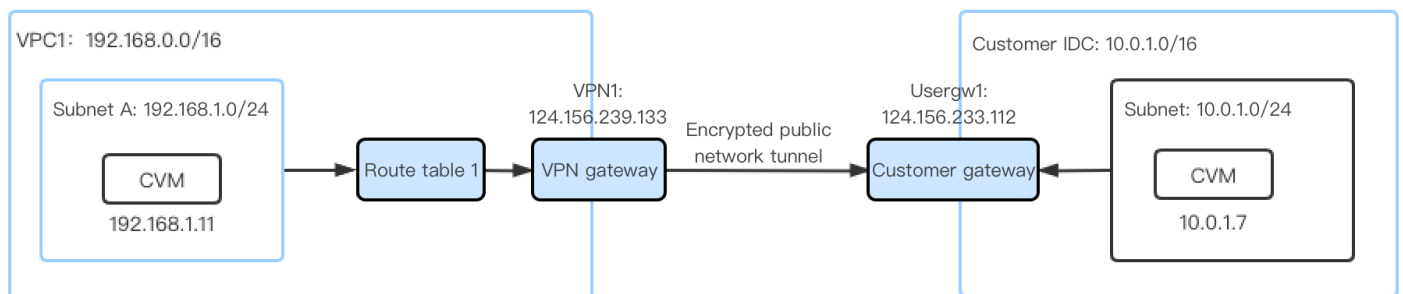
Directions

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 : 2021-06-15 10:32:16

1. Log in to the [VPC console](#).
2. Click **VPN Connection** > **VPN Gateway** on the left sidebar to go to the management 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](#) 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 type, choose **VPC1** as the specific network, and select the bandwidth cap and billing method.
5. Click **Create**. After the VPN gateway is created, the system randomly assigns it a public IP address such as 124.156.239.133 .

Step 2: Create a Customer Gateway

Last updated : 2021-06-15 10:32:55

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 : 2021-06-15 10:33:56

1. Log in to the [VPC console](#).
2. Click **VPN Connection** > **VPN Tunnel** on the left sidebar to go to the management page.
3. Choose a region and VPC (**Tokyo** and **VPC1** in this example) and click **+New**.
4. Enter the tunnel name (e.g. **tunnel1**). Choose the VPN gateway **VPN1** and the customer gateway **UserGw1**, enter the pre-shared key (e.g. **123456**), and click **Next**.

Note :

Health check is optional and is disabled by default. If it is enabled, please enter the VPN gateway IP address (an available IP not included in the primary CIDR block of the VPC), and the customer gateway IP (an available IP in the IDC IP range).

5. On the **SPD Policy** page, configure both the VPN gateway and customer gateway IP as **0.0.0.0/0**, and click **Next**.
6. (Optional) Configure IKE parameters. Click **Next** if no advanced configuration is required.
7. (Optional) Configure IPsec parameters. Click **Complete** if no configuration is required.
8. After the VPN tunnel is successfully created, 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 : 2021-07-05 10:55:12

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 : 2021-06-15 11:12:53

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 : 2021-06-15 10:35:32

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.