Virtual Private Cloud

Connect with Customer Data Center

Product Documentation

Contents

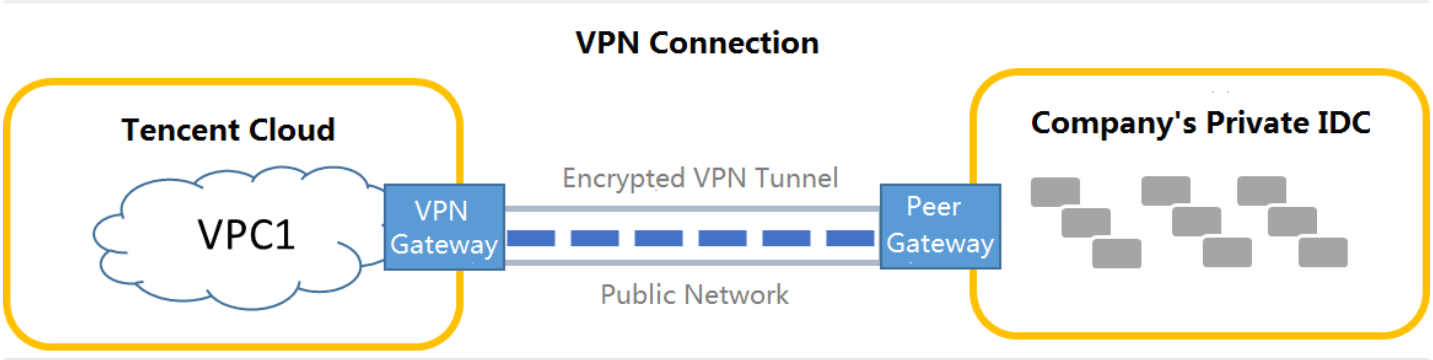
Connect with Customer Data Center VPN Connection

Last updated：2019-07-31 11:14:45

Overview

VPN connection is a method to connect your peer IDC and VPC through encrypted public network tunnel. As shown below, Tencent Cloud VPC VPN Connection consists of the following components:

- VPN gateway: Created VPC IPsec VPN gateway
- Customer gateway: IPsec VPN service gateway for IDC
- VPN tunnel: Encrypted IPsec VPN tunnel



VPN gateways can be established in the VPC. Multiple VPN tunnels can be established in each VPN gateway. Each VPN tunnel can connect to one local IDC. Please note that, **after a VPN connection is established, you need to configure related routing policies in the routing table to achieve communication.**

VPN Gateway

VPN gateway is an outbound gateway that establishes VPN connections in the VPC, and it is used in combination with a customer gateway (IPsec VPN service gateway for IDC). VPN gateway is mainly used to establish a secure and reliable encrypted network communication between Tencent Cloud VPC and external IDC. Implemented through software virtualization, Tencent Cloud NAT gateway uses master/slave hot backup to switch automatically when a single server suffers a failure, without affecting the normal operation of your businesses.

According to the upper limit of bandwidth, the VPN gateway comes with 5 settings: 5 Mbps, 10 Mbps, 20 Mbps, 50 Mbps and 100 Mbps. The setting of the bandwidth for the VPN gateway can be adjusted at any time, and takes effect immediately.

If you need BGP high defense to provide ultra-large bandwidth DDoS and CC defense for the VPN gateway, you can bind the high defense package to the VPN gateway for security protection.

Customer Gateway

Customer gateway refers to the IPsec VPN service gateway of IDC, which needs to be used along with the Tencent Cloud VPN gateway. Encrypted VPN network tunnels can be established between a VPN gateway and multiple customer gateways.

VPN Tunnel

After the VPN gateway and the customer gateway are established, VPN tunnels can be established for the encrypted communication between VPC and external IDC. VPN tunnels support IPsec encryption protocols, which can meet the needs of most VPN connections.

Since VPN tunnels run in the ISP's public network, the congestion or jitter of the public network may affect the quality of the VPN network. Therefore, the assurance of the SLA service agreement is unavailable. If your business is sensitive to delay and jitter, it is recommended to access the VPC via Direct Connect. For more information, please see Direct Connect.

The VPN tunnel on Tencent Cloud uses the Internet Key Exchange (IKE) protocol to establish a session when implementing IPsec. IKE is provided with a self-protection mechanism that can securely authenticate identities, distribute keys and establish IPSec sessions on unsecured networks.

The following configuration information is required when a VPN tunnel is established:

- Basic info
- Security Policy Database (SPD) policy
- IKE configuration (optional)
- IPsec configuration (optional)

The basic information, SPD policy, IKE configuration (optional) and IPsec configuration (optional) are described in details below.

Basic Information

Protocol type: IKE/IPsec
Pre-shared private key: The pre-shared private key is a Unicode string used to verify L2TP/IPSec connections. The local and peer must use the same pre-shared private key.

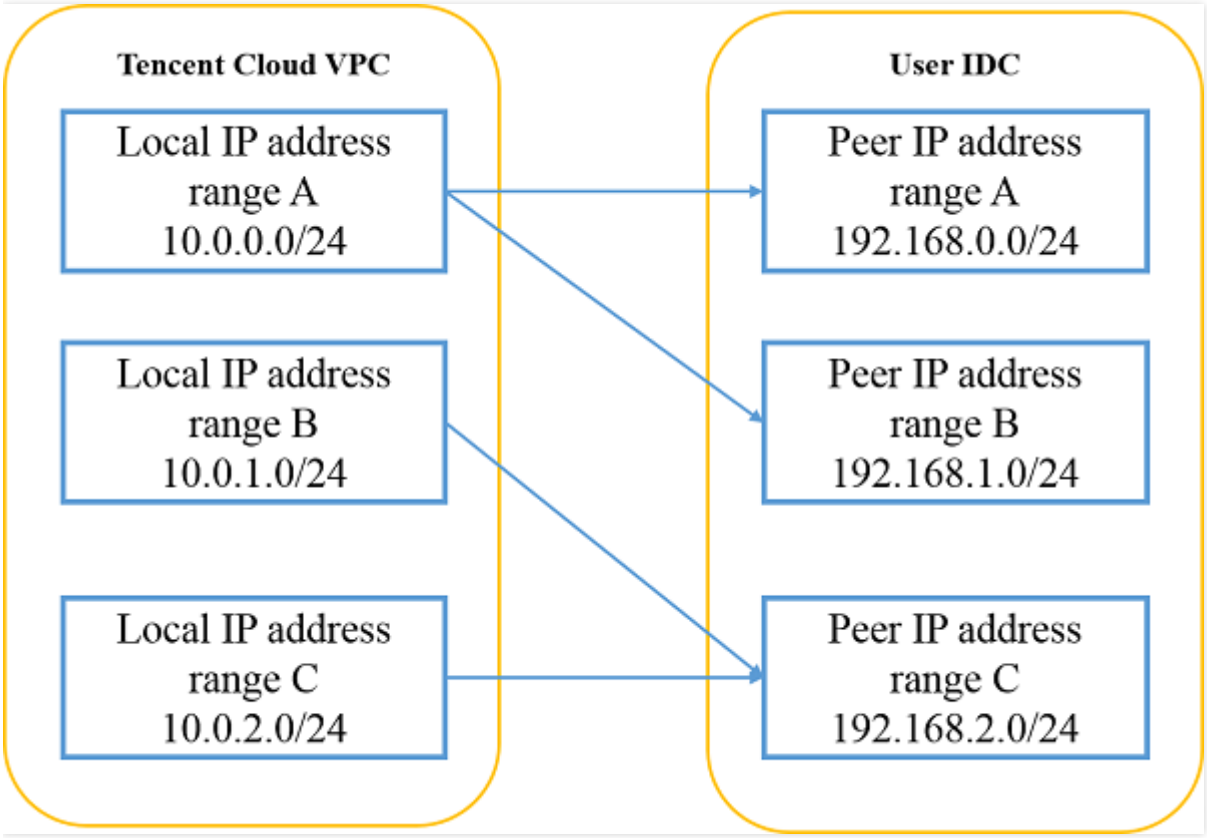
Security Policy Database (SPD) Policy

The Security Policy Database (SPD) policy consists of a series of SPD rules, and each of which is used to specify which IP address ranges of the VPC can communicate with which IP address ranges of the IDC.

- Each SPD policy is used for a local and multiple peer IP address ranges. The local IP address range and the peer ones cannot overlap.
- The local IP address ranges for a collection of policies cannot overlap.
- Several peer IP address ranges for one local IP address range cannot overlap.
- The peer IP address range and the VPC IP address range cannot overlap.

Here is a correct instance:

SPD policy 1: The local IP address range is `10.0.0.0/24`, and the peer IP address range is `192.168.0.0/24` / `192.168.1.0/24`.
SPD policy 2: The local IP address range is `10.0.1.0/24`, and the peer IP address range is `192.168.2.0/24`.
SPD policy 3: The local IP address range is `10.0.2.0/24`, and the peer IP address range is `192.168.2.0/24`.



IKE Configuration

Configuration Item	Description
Version	IKE V1
Authentication method	Default pre-shared private key
Authentication algorithm	Authentication algorithm. MD5 and SHA1 are supported
Negotiation mode	Support main mode and aggressive mode The difference is that more information can be sent with fewer packets in aggressive mode, which results in a quicker connection establishment. The downside is that the identity of security gateway has to be sent in plain text. When using aggressive mode, configuration parameters such as Diffie-Hellman and PFS may not be negotiated. Therefore, it's critical that their configurations are compatible on both sides
Local identity	Support IP address and Fully Qualified Domain Name (FQDN)
Peer identity	Support IP address and FQDN
DH group	Specify the DH group used during IKE. The security of key exchange increases with the expansion of the DH group, but the exchange time also increases Group1: DH group using 768-bit modular exponential (MODP) algorithm Group2: DH group using 1024-bit MODP algorithm Group5: DH group using 1536-bit MODP algorithm Group14: DH group using 2048-bit MODP algorithm. Dynamic VPN is not supported for this option Group24: DH group using 2048-bit MODP algorithm with a 256-bit prime order subgroup. Group VPN is not supported for this option

Configuration Item	Description
IKE SA Lifetime	Set the SA lifetime of the IKE security proposal (in sec). Before the expiration of the set lifetime, another SA is negotiated in advance to replace the old SA. The old SA is still used until the negotiation on the new SA is finished. The new SA is used immediately upon its establishment, and the old SA is cleared automatically after its lifetime has expired

Ipsec Information

Configuration Item	Description
Encryption algorithm	Support 3DES, AES-128, AES-192, AES-256, DES
Authentication algorithm	Support MD5 and SHA1
Message encapsulation mode	Tunnel
Security protocol	ESP
PFS	Support disable, dh-group1, dh-group2, dh-group5, dh-group14 and dh-group24
IPsec SA lifetime (s)	In sec
IPsec SA lifetime (KB)	In KB

Service Limits

VPN Connection Constraints

For VPN connections, please note that:

- After the VPN parameters are configured, **you need to add the routing policy for the VPN gateway in the routing table associated with the subnet**, so that the access requests from CVMs within the subnet to peer IP address range can reach the customer gateway through the VPN tunnel.
- After the routing table is configured, **you need to ping the IP of the peer IP address range using the CVM of VPC to activate this VPN tunnel.**

- The stability of VPN connection depends on the performance of public network provided by ISPs. We cannot guarantee relevant service level under an SLA contract.

Resource	Limit
Number of VPN gateways per VPC	10
Number of customer gateways in a region	20
Number of VPN tunnels per customer gateway	10
Number of VPN tunnels that can be created in a VPN	20
Number of SPDs per VPN tunnel	10
Number of peer IP address ranges per SPD	50

IP Address Constraints for Customer Gateway

The following IP addresses are not supported for the customer gateway:

- Multicast addresses all starting with 0 or 225/224.
- Loopback addresses: 127.x.x.x/8.
- Addresses with host bits all being 0 or 1, for example:
  a. Addresses starting with 1-126 in Class A, such as 1-126.0.0.0 and 1-126.255.255.255.
  b. Addresses starting with 128-191 in Class B, such as 128-191.x.0.0 and 128-191.x.255.255.
  c. Addresses starting with 192-223 in Class C, such as 192-223.x.x.0 and 192-223.x.x.255.
- Internal service addresses: 169.254.x.x/16;

Billing Method

VPN tunnel and customer gateway are free of charge.
VPN gateway will be charged by hour. Its unit price already includes the cost of IDC bandwidth, so CVM does not need to purchase network bandwidth again. The specific expenses are shown in the following table:

Region	Mainland China	Hong Kong, Korea, Frankfurt, Silicon Valley, Virginia, Mumbai,Tokyo,Moscow	Singapore, Toronto, Bangkok
Price (USD/hour)	0.078	0.088	0.12

For more information regarding the prices of VPC services, refer to VPC Price Overview.

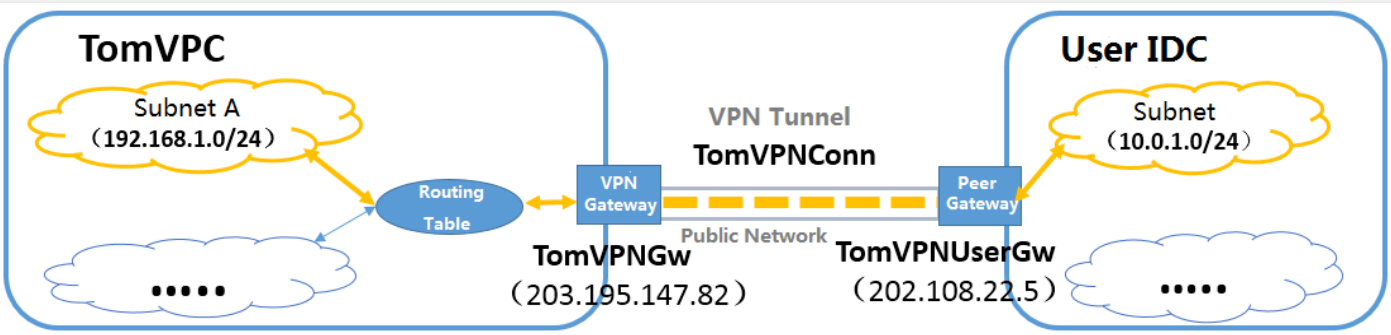
Operation Instructions

Quick Start

IPsec VPN can be fully customized in the console. You need to complete the following steps to allow the VPN connection to take effect :

1) Create VPN gateway
2) Create customer gateway
3) Create VPN tunnel
4) Load the configuration file in self-built IPsec VPN gateway
5) **Configure the routing table**
6) **Enable VPN tunnel**

Example:
Through IPsec VPN, connect the subnet A `192.168.1.0/24` in your VPC ("TomVPC") in **Guangzhou** with the subnet `10.0.1.0/24` in your IDC, and the public IP of the VPN gateway in IDC is `202.108.22.5` .



You need to complete the following steps:

Step 1: Create VPN Gateway

1) Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Routing Table".
2) Click "VPN Connection" -> "VPN Gateway" tab in the left navigation bar.
3) Select **Guangzhou** in which VPC "myVPC" resides and the VPC `TomVPC` at the top of the list, and then click "New".
4) Enter the name of VPN gateway (such as TomVPNGw), select the appropriate bandwidth configuration and make the payment. Then, the VPN gateway is created. After that, the system randomly assigns a public IP, e.g. `203.195.147.82` .

Step 2: Create Customer Gateway

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

1) Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Routing Table".
2) Click "VPN Connection" -> "Customer Gateway" tab in the left navigation bar.
3) Select the region "**Guangzhou**" at the top of the list, and then click "New".
4) Enter the name of customer gateway (such as TomVPNUserGw) and the public IP of VPN gateway of IDC `202.108.22.5` .
5) Click "Create", and you can view the new customer gateway in the customer gateway list.

Step 3: Create VPN Tunnel

Create a VPN tunnel by following the steps below:

1) Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Routing Table".
2) Click "VPN Connection" -> "VPN Tunnel" tab in the left navigation bar.
3) Select **Guangzhou** in which VPC "myVPC" resides and the VPC `TomVPC` at the top of the list, and then click "New".
4) Enter the name of tunnel (such as TomVPNConn), select the VPN gateway `TomVPNGw` and the customer gateway `TomVPNUserGw` , and then enter the pre-shared key (such as `123456`).
5) Enter the SPD policy to limit the communication between which local IP address ranges and which peer IP address ranges. The local IP address range in this example is the IP address range of subnet A `192.168.1.0 / 24` , and the peer IP address range is `10.0.1.0 / 24` . Then, click "Next".
6) (Optional) Step 3: Configure IKE parameters. If you do not need advanced configurations, click "Next".
7) (Optional) Step 4: Configure IPsec parameters. If you do not need these parameters, click "Finish" to complete the configuration.
8) Click to complete the creation of VPN tunnel, and download the configuration file.

Step 4: Load the Configuration File in Self-built IPsec VPN Gateway

To achieve network interconnection among VPN tunnels, you need to load and configure the configuration files generated in Step 3 in your own IPsec VPN gateway.

Step 5: Modify Routing Table

After the completion of Step 4, we have successfully configured a VPN tunnel. However, since the traffic of subnet A has not been routed to the VPN gateway yet, CVMs in the IP address range of subnet A still cannot communicate with servers in the IP address range of IDC.

1) Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Routing Table".

2) Click "Subnet" in the left navigation bar. Select **Guangzhou** in which VPC "myVPC" resides and the VPC `TomVPC` at the top of the list. Click the ID of the routing table associated with subnet A to go to the details page of the routing table.
3) Click "Edit" button, and then click "New line". Enter the destination IP address range (`10.0.1.0/24`), select the "VPN Gateway" as the next hop type, and then select the VPN gateway `TomVPNGw` you just created.
4) Click "Save" to complete the outbound routing settings of subnet that requires communication.

Step 6: Enable VPN Tunnel

To activate the VPN tunnel, you need to ping the IP of the peer IP address range using the CVM of VPC. For example: use the CVM within the subnet A of `TomVPC` to ping `10.0.1.1` .

Viewing Monitoring Data

You can view the monitoring data of VPN tunnels and VPN gateways.

1) Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Routing Table".
2) Click "VPN Connection" -> "VPN Gateway" or "VPN Tunnel" tab in the left navigation bar.
3) Click the icon in "Monitoring" column on the list page to view the monitoring data.

Setting the Alarm

VPN tunnel provides alarm feature:

1) Log in to Tencent Cloud Console, click "Cloud Products" -> "Monitor & Management" -> "Cloud Monitor" in the top navigation bar, and select "My Alarms" -> "Alarm Policy" in the left navigation bar, and then click "Add Alarm Policy".
2) Enter the alarm "Policy Name", select "VPN Tunnel" in Policy Type, and then add alarm triggering condition.
3) **Associate alarm objects**: Select the alarm receiver group, and when it is saved, you can view the set alarm polices in Policy List.

4. **View the alarm information**: When the alarm is triggered, you can receive a notification sent via SMS/email/internal message. You can also view it in "My Alarms" -> "Alarm List" in the left navigation bar.

Viewing the Details of VPN Gateway

1) Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Routing Table".
2) Click "VPN Connection" -> "VPN Gateway" tab in the left navigation bar.

3) Click "VPN Gateway ID" to go to the details page of VPN gateway to view the information of VPN gateway.

Modify VPN Tunnel Configuration

1) Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Routing Table".
2) Click "VPN Connection" -> "VPN Tunnel" tab in the left navigation bar.
3) Click "VPN Gateway ID" to go to the details page of VPN gateway to view the information of VPN gateway.
4) You can modify the basic information and SPD policy in the basic information page, or you can modify the IKE and Ipsec configurations in "Advanced Configuration".

Binding High Defense Package

1. Log in to Tencent Cloud Console, click "Security" -> "Dayu Distributed Defense" in the navigation bar, and select BGP High Defense Package on the left navigation bar.
   ii. Select an existing high defense package instance, click "Change Device" and select the VPN gateway that needs defense.
   iii. Click "OK" to associate the high defense package feature to this VPN gateway.

API Overview

You can use APIs to configure and manage your VPN connections. For more APIs relevant to VPC, please see Overview of All VPC APIs.

VPN-related APIs

Feature	Action ID	Description
Query price of VPN gateway	InquiryVpnPrice	Query the price of a VPN gateway.
Purchase VPN gateway	CreateVpn	Purchase a VPN gateway.
Modify properties of VPN gateway	ModifyVpnGw	Modify the information of a specified VPN gateway, such as the name.
Query VPN gateway list	DescribeVpnGw	Query the information of a VPN gateway based on user information, such as the ID and name of the VPN gateway.

Feature	Action ID	Description
Renew VPN gateway	RenewVpn	Renew a VPN gateway.

Customer Gateway-related APIs

Feature	Action ID	Description
Create customer gateway	AddUserGw	Create a customer gateway to be connected.
Delete customer gateway	DeleteUserGw	Delete a specified customer gateway.
Modify name of customer gateway	ModifyUserGw	Modify the name of a customer gateway.
Query customer gateway list	DescribeUserGw	Query the information of a customer gateway based on user information, such as the ID and name of the customer gateway.
Obtain information about supported customer gateway vendors	DescribeUserGwVendor	Query information on customer gateway vendors supported by Tencent Cloud VPN.

VPN Tunnel-related APIs

Feature	Action ID	Description
Create VPN tunnel	AddVpnConn	Create a encrypted VPN tunnel to connect VPC to other network resources.
Delete VPN tunnel	DeleteVpnConn	Delete a specified VPN tunnel.
Modify VPN tunnel	ModifyVpnConn	Modify the information of a specified VPN tunnel, such as the name.
Query VPN tunnel list	DescribeVpnConn	Query the information of a tunnel based on user information, such as the ID and name of the VPN tunnel.
Download VPN tunnel configuration	GetVpnConnConfig	Download the configuration of a VPN tunnel to make adjustments to it.

Feature	Action ID	Description
Obtain monitoring data of VPN tunnel	DescribeVpnConnMonitor	Obtain the monitoring data of a VPN tunnel.