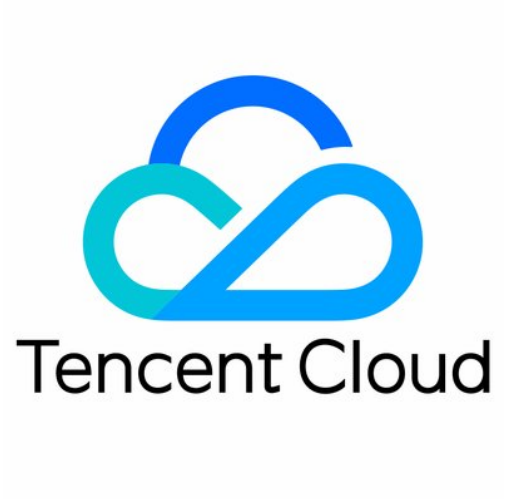
VPN Connections

Product Introduction

Product Documentation



Contents

Product Introduction

Overview

Last updated：2024-08-15 16:25:41

VPN Connections aims to create a secure network connection over the public network. It can securely connect the customer IDC to the private office network and the Tencent Cloud VPC through an encrypted tunnel over the public network.

Note:

Tencent Cloud's VPN Connections are provided in compliance with national policies and regulations, and do not offer Internet access capabilities. It is prohibited to circumvent network censorship to access foreign networks through technical means. Additionally, no proxy feature is provided.

Tencent Cloud's VPN supports both IPsec and SSL network security protocols. In the following sections, we refer to VPN connections utilizing the IPsec protocol as IPsec VPNs, and those employing the SSL protocol as SSL VPNs.

Tencent Cloud's IPSec VPN supports access to cloud resources via both public and private networks. In the following sections, we refer to VPN connections that access cloud resources over the public network as public VPNs, and those that access cloud resources through a private network as private VPNs.

Note:

If you require the use of a private VPN, submit a ticket for consultation.

IPsec VPN

Tencent Cloud VPN Connections consists of the following components:

VPN gateway: an IPsec VPN gateway.

VPN gateway for VPC: if you need to communicate with a single VPC, you can connect to the VPC via the VPN gateway for VPC.

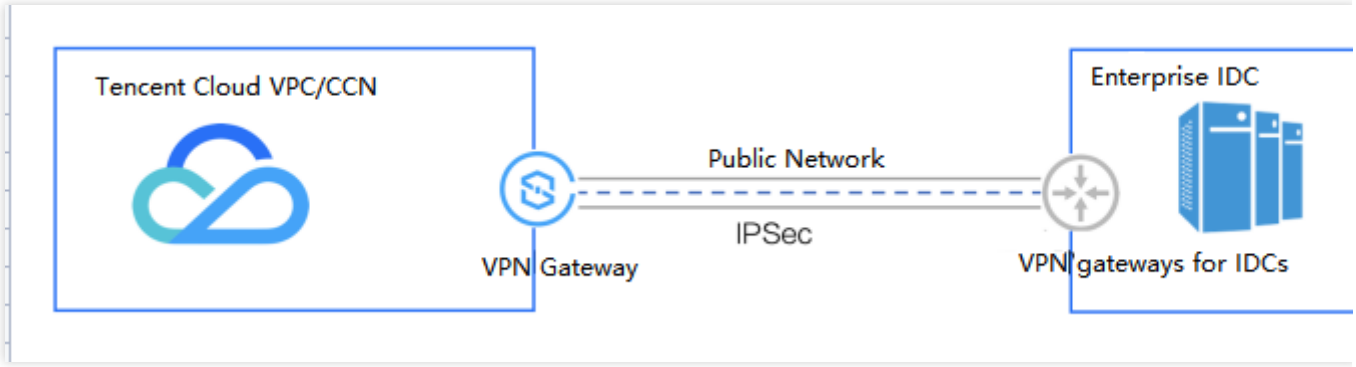
VPN gateway for CCN: if you need to communicate with multiple VPCs, you can connect to CCN via the VPN gateway for CCN to realize traffic interconnection.

Note:

Each VPN gateway can create multiple VPN tunnels, each of which can connect the VPC to a local IDC.

Customer gateway: a logical object that records the fixed public IP address of the IPsec VPN gateway on the IDC side.

VPN tunnel: an encrypted IPsec VPN tunnel.



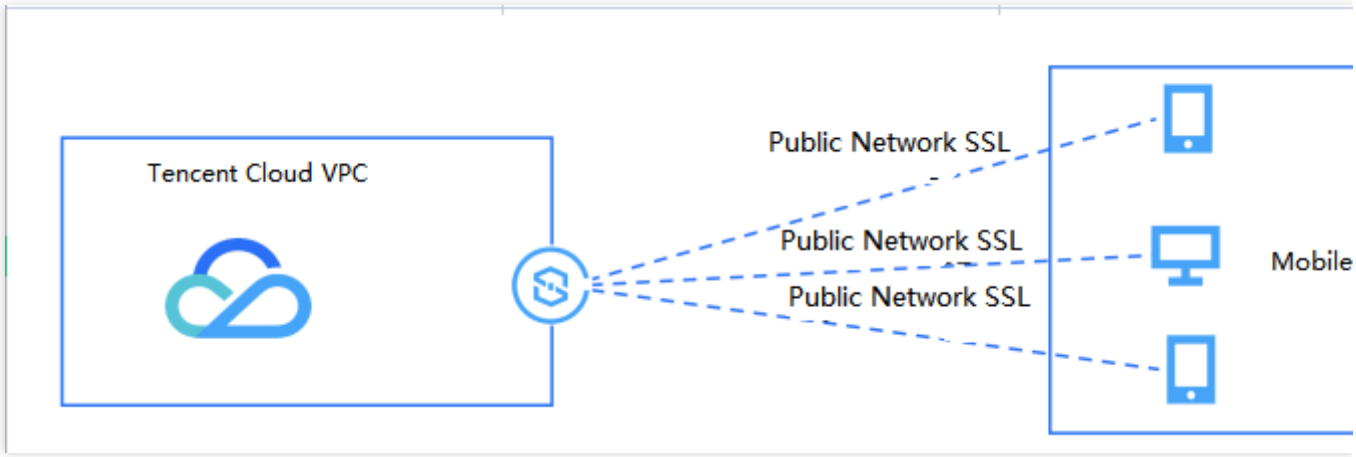
SSL VPN

Tencent Cloud SSL VPN Connections consists of the following components:

SSL VPN gateway: a VPN gateway using the SSL protocol

SSL VPN server: a service module that provides SSL services and is used to encapsulate and de-encapsulate data packets and negotiate the communication port, encryption algorithm, and IP ranges for interconnection.

SSL VPN client: a VPN client that is deployed on user terminals and is considered a logical instance on Tencent Cloud.



Components

Last updated：2024-08-15 16:25:04

Tencent Cloud VPN supports the virtual network connections using IPSec and SSL protocols. It realizes a full connection among IDC, private office network, mobile client, and Tencent Cloud VPC/CCN.

IPsec VPN

IPSec VPN Gateway

An IPSec VPN gateway is an egress gateway for VPC or CCN to establish a VPN connection. It is used with a customer gateway (IPsec VPN gateway on the IDC side) to establish an encrypted communication between a Tencent Cloud VPC or CCN and an external IDC. Tencent Cloud VPN gateway uses software virtualization and an active-active hot backup architecture. When one server fails, automatic switchover helps ensure the normal operation of your businesses.
Eight supported bandwidth caps of VPN gateway: 5 Mbps, 10 Mbps, 20 Mbps, 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1,000 Mbps and 3,000 Mbps.
If you need Anti-DDoS Pro to defend against DDoS and CC attacks with high-bandwidth protection, you can bind it to the VPN gateway.

Customer Gateway

A customer gateway is a logical object accompanied by a Tencent Cloud VPN gateway to record the fixed public IP address of the IPsec VPN gateway on the IDC side. Each VPN gateway can create encrypted VPN tunnels with multiple customer gateways.

VPN Tunnel

After the VPN gateway and customer gateway are created, you can establish a VPN tunnel between the VPC or CCN and an external IDC for encrypted communication. Currently, a VPN tunnel supports the IPsec encryption protocol, which can meet the requirements of most VPN connections.
VPN tunnels support not only static routing communication methods such as destination routing and SPD policies, but also dynamic BGP routing communication. Currently, dynamic BGP routing communication is in a grayscale upgrade. If you need to use this feature, submit a ticket for a request.
A VPN tunnel runs on an ISP's public network, therefore, congestion or jitter on the public network may affect the VPN performance. If your business is sensitive to latency and jitter, we recommend that you connect the VPC or CCN via Direct Connect. For more information, see Direct Connect.

SSL VPN

SSL VPN Gateway

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.

If you need Anti-DDoS Pro to defend against DDoS and CC attacks with high-bandwidth protection, you can bind it to the VPN gateway.

SSL VPN Server

The SSL VPN server is a service module in VPN gateway, which is used to encapsulate and de-encapsulate data packets. The configuration parameters include server IP range, client IP range, communication protocol, port and algorithm, etc. For details, see Creating the SSL VPN Server.

SSL VPN Client

The SSL VPN client provides a certificate for connecting the mobile device to the server. Only through a two-way certificate authentication can the client be connected to the server.

Application Scenarios

Last updated：2024-08-15 16:24:19

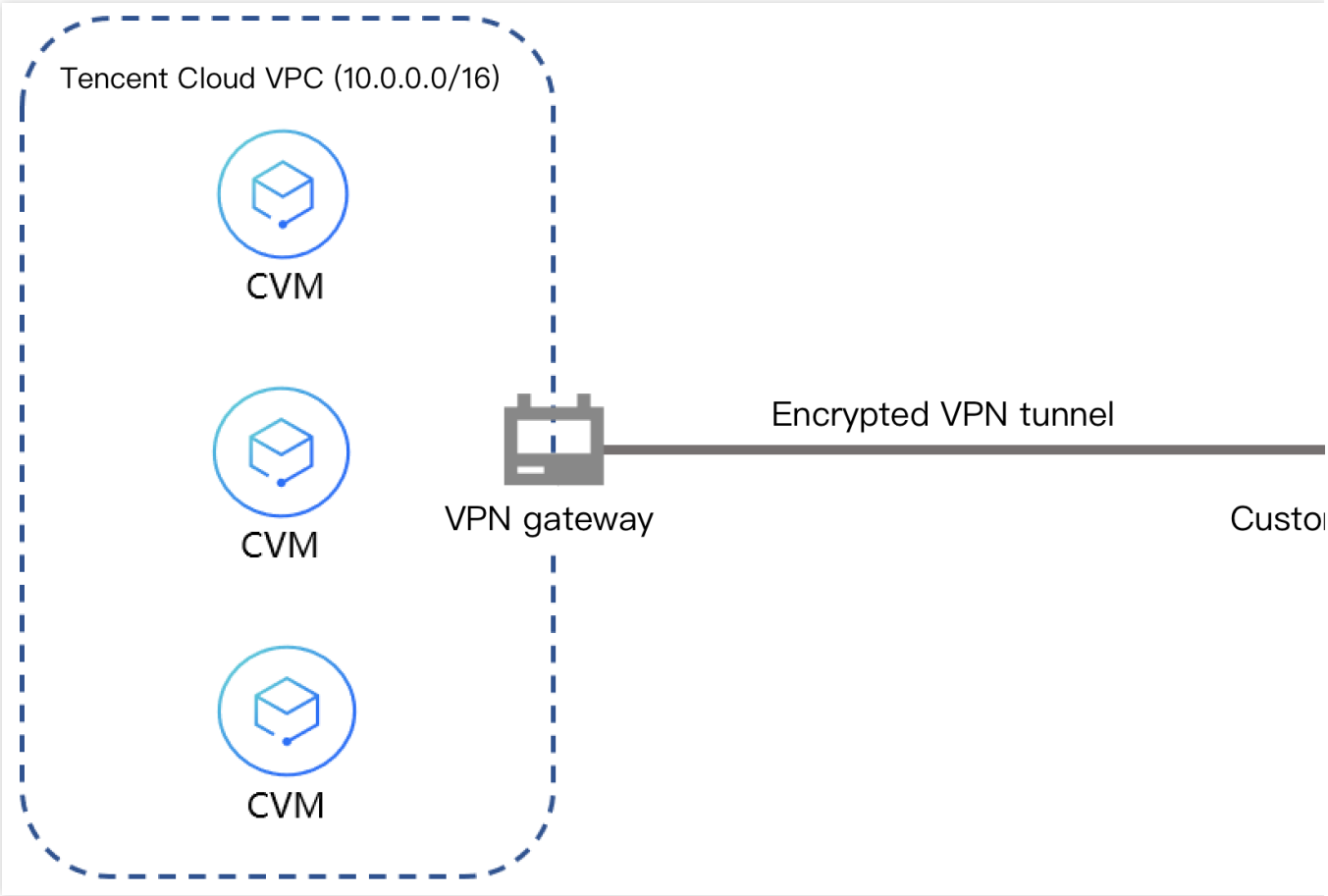
Tencent Cloud VPN Connections provides Internet-based remote network connection services. As an important component of a VPN connection, a VPN gateway can enable secure site-to-site access by creating a secure encrypted IPsec or SSL tunnel with the customer IDC, mobile client, and private office network.

Use Cases of IPSec VPN

VPN has two routing and forwarding methods:
Matching the source and destination IP ranges of data flow based on the SPD policy-based routing, and forwarding according to the set forwarding policy. Routing cannot be realized through this method, so traffic cannot be forwarded, but the first, fourth and sixth communication scenarios can be realized.
By configuring the VPN route table, you can route and forward data packets based on the destination IP range. This method is called destination routing, and all the following communication scenarios can be realized with this method. The sixth scenario can not only be realized through SPD policy-based routing alone but also through SPD policy-based routing and destination routing at the same time.
Note:
The "customer gateway" in the following figures means the logical object that records the public IP address of the IPsec VPN device on the IDC side. Each customer gateway corresponds to the IPsec VPN device on the IDC side.

Scenario 1: communication between VPC and IDC

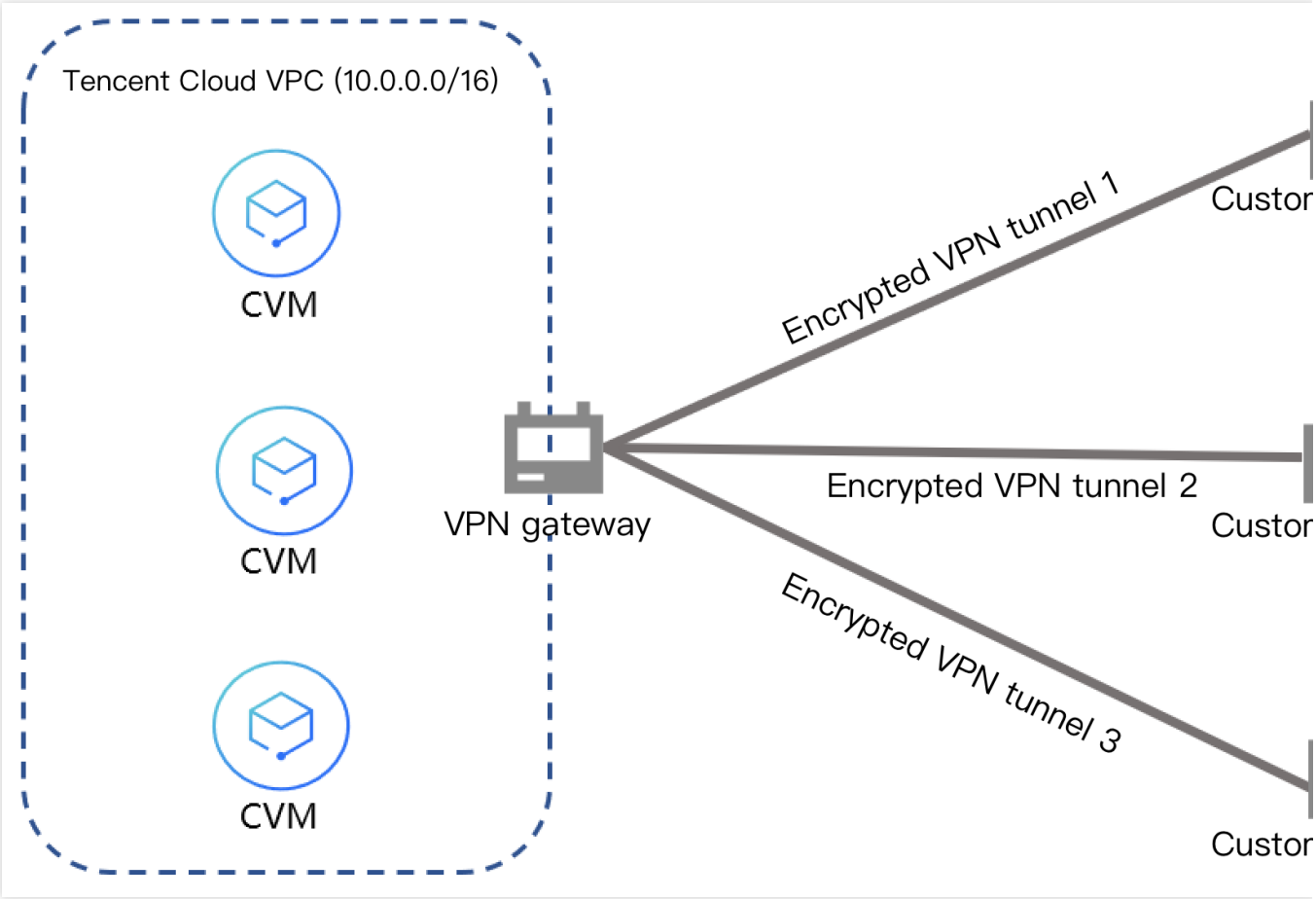
VPN Connections enables the communication between VPC and IDC



Scenario 2: traffic interconnection between a single VPC and multiple IDCs

Multiple IDCs connect to each other in the VPN connection-based migration-to-cloud scenario.

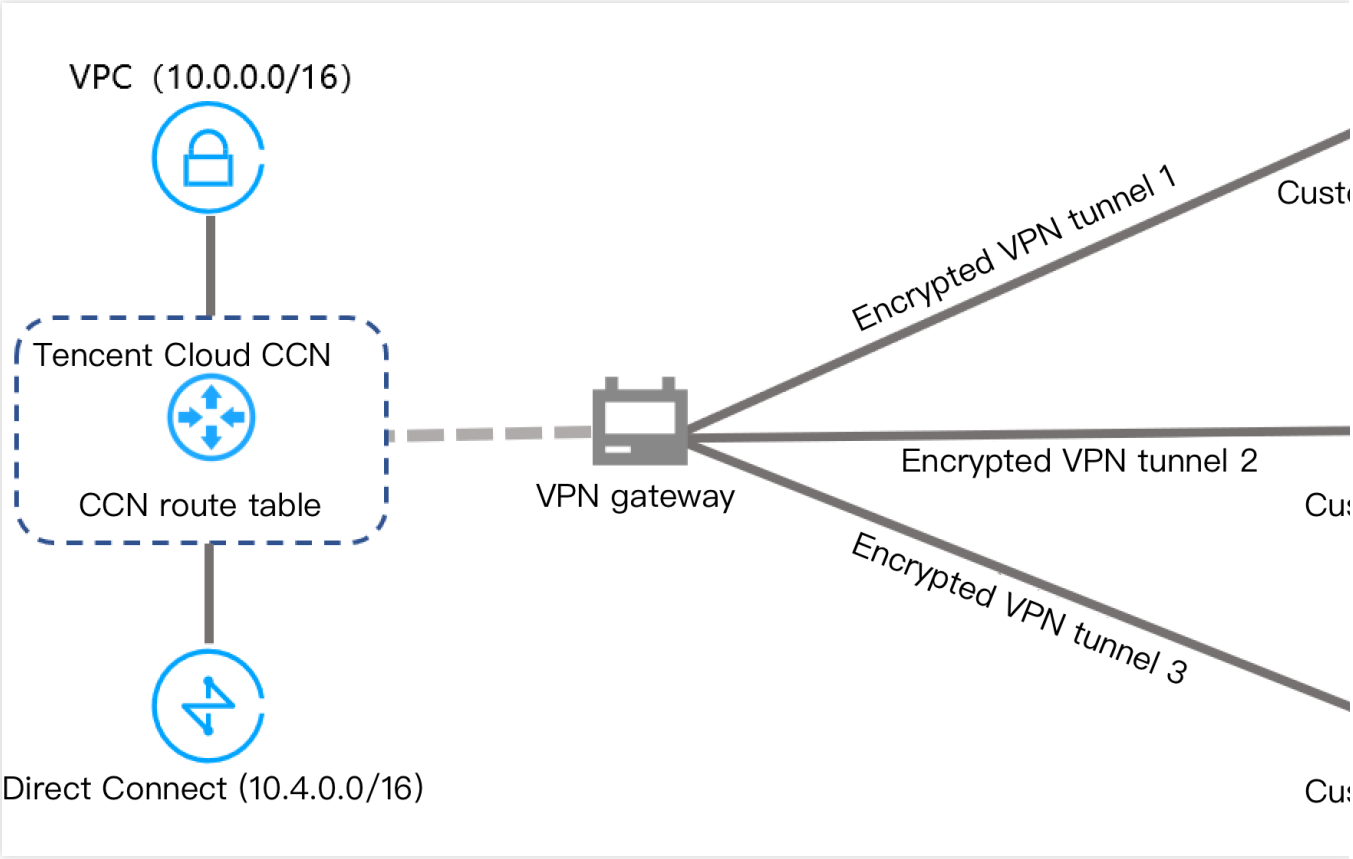
Scenario description: the customer IDC-1, IDC-2, and IDC-3 are connected to Tencent Cloud VPN gateway for VPC via their respective IPsec VPN device. They can not only access various resources in the VPC of the VPN gateway but also connect to each other through Tencent Cloud VPN gateway, thus enabling secure communication between VPC and the customer IDC-1, IDC-2, and IDC-3.



Scenario 3: communication among multiple IDCs via a VPN gateway

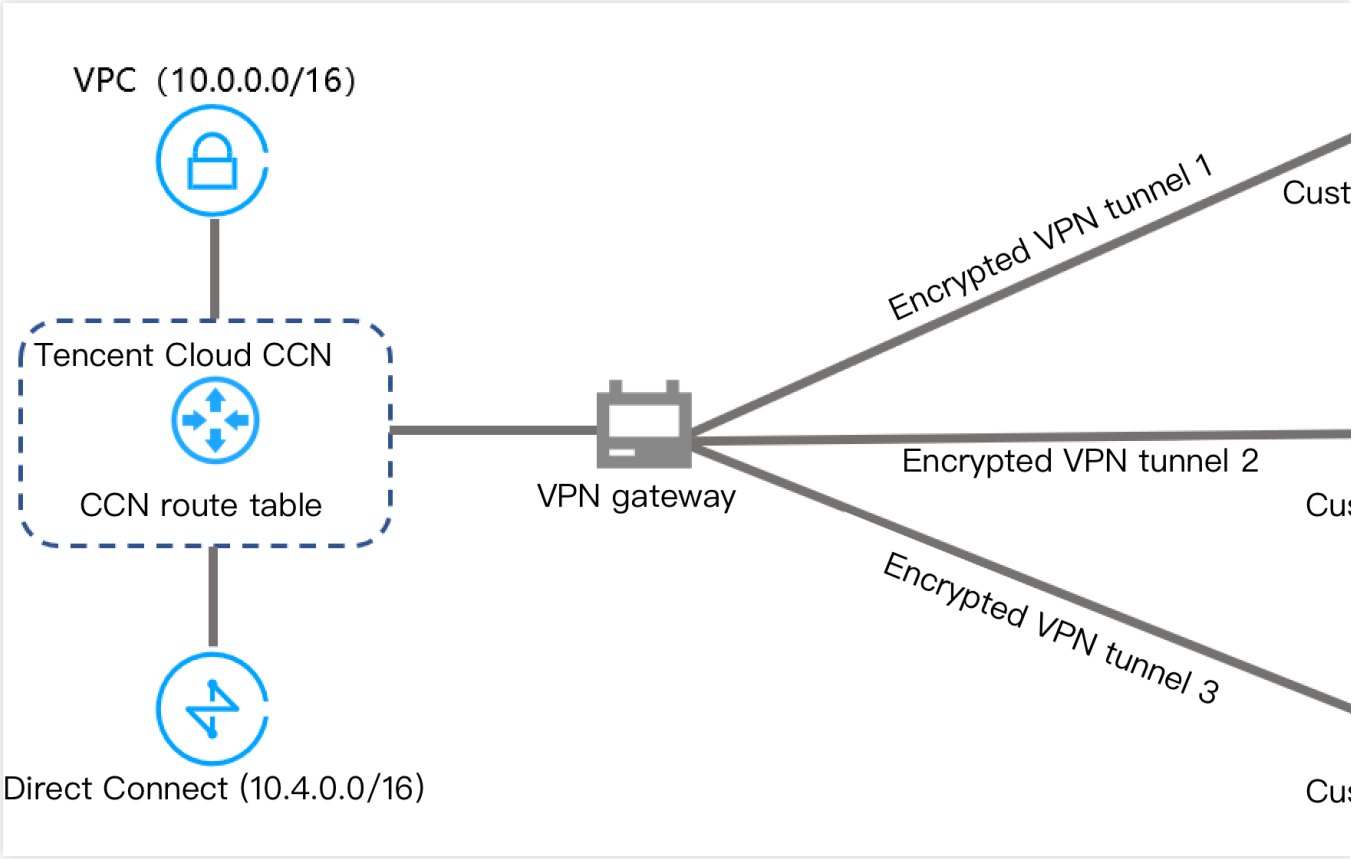
Multiple IDCs can communicate with each other via the VPN for Cloud Connect Network (CCN) if they don't need to access cloud resources.

Scenario description: the customer IDC-1, IDC-2, and IDC-3 are connected to Tencent Cloud VPN gateway for CCN via their respective IPsec VPN device. They communicate with each other only via Tencent Cloud VPN gateway without the need to access the public cloud resources of Tencent Cloud. In this case, customers can create a VPN gateway for CCN which is not associated with CCN.



Scenario 4: traffic interconnection between multiple IDCs and multiple cloud networks

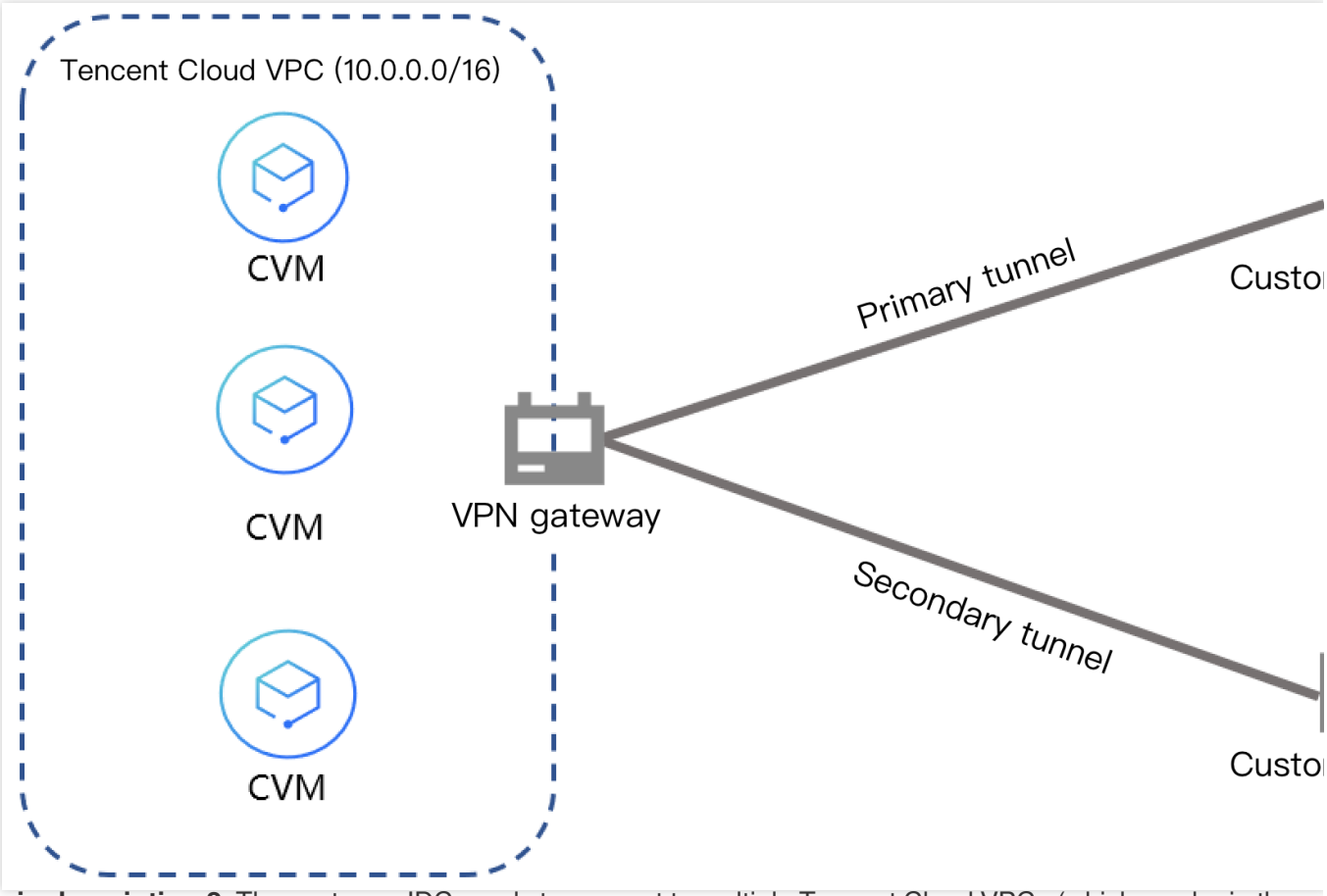
Scenario description: the customer IDC-1, IDC-2, and IDC-3 are connected to Tencent Cloud VPN gateway for CCN via their respective IPsec VPN device. They can communicate with each other via Tencent Cloud VPN gateway and access CCN-associated VPC and direct connect networks via CCN. In this case, customers can create a VPN gateway for CCN and associate it with CCN to realize traffic interconnection.



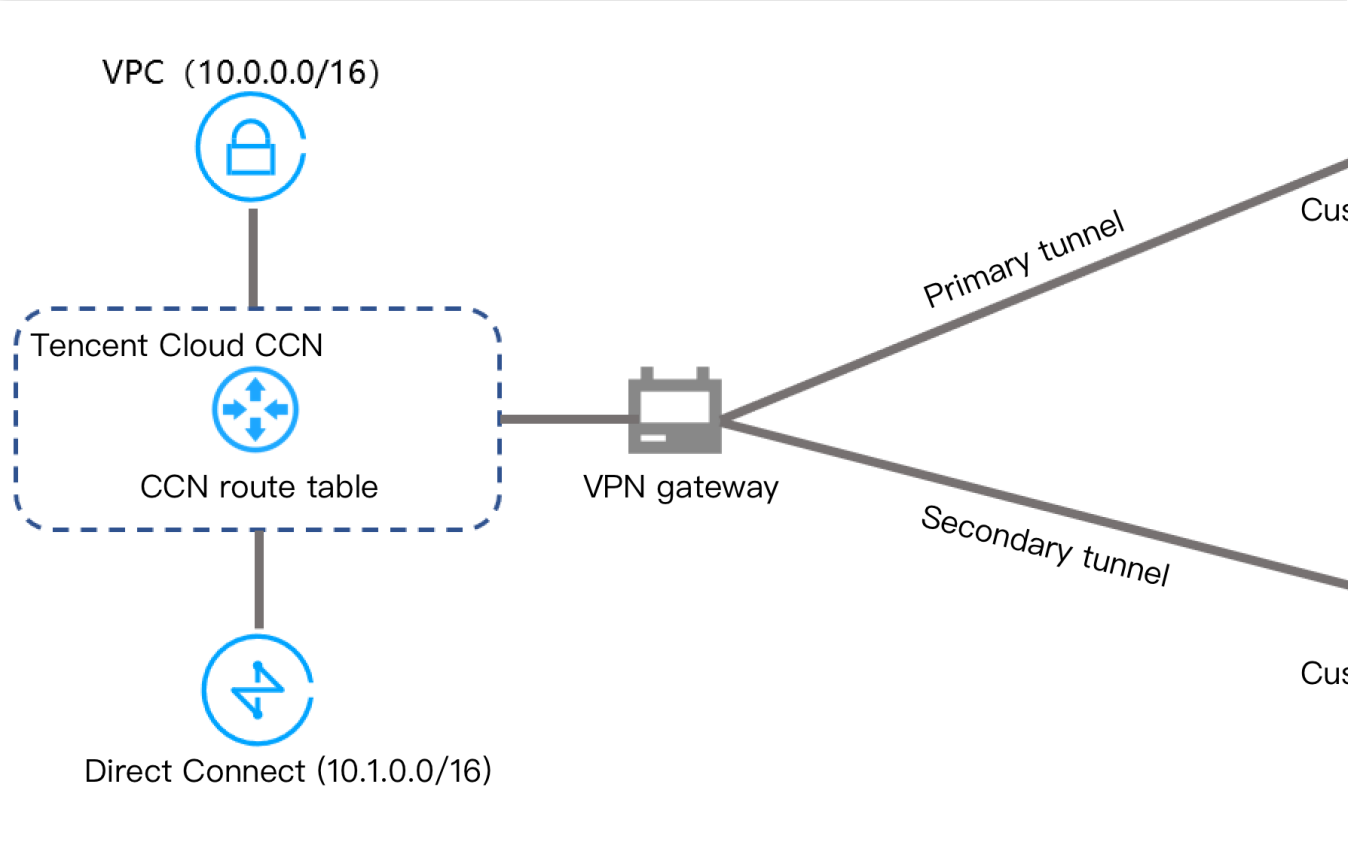
Scenario 5: IDC realizes active/standby cloud disaster recovery through active/standby VPN tunnels

If the customer IDC migrates to cloud via active/standby VPN tunnels, when the active tunnel fails, the business will be automatically switched over to the standby tunnel, thus ensuring business sustainability and reliability.

Scenario description 1: The customer IDC only needs to connect to a single Tencent Cloud VPC. On the customer IDC side, the customer can deploy 2 IPsec VPN devices that respectively create IPSec VPN tunnels with Tencent Cloud VPN gateway for VPC. The VPN gateway route table configures 2 routes that share the same destination port, and the active/standby tunnel mechanism will be effective through priority control. In case of failure, the routes can be switched over automatically.



Scenario description 2: The customer IDC needs to connect to multiple Tencent Cloud VPCs (which can be in the same region or different regions) and direct connect networks. On the customer IDC side, the customer can deploy 2 IPsec VPN devices that respectively create IPSec VPN tunnels with Tencent Cloud VPN gateway for CCN. The VPN gateway route table can configure 2 routes that share the same destination port, and the active/standby tunnel mechanism will be effective through priority control. In case of failure, the routes can be switched over automatically.

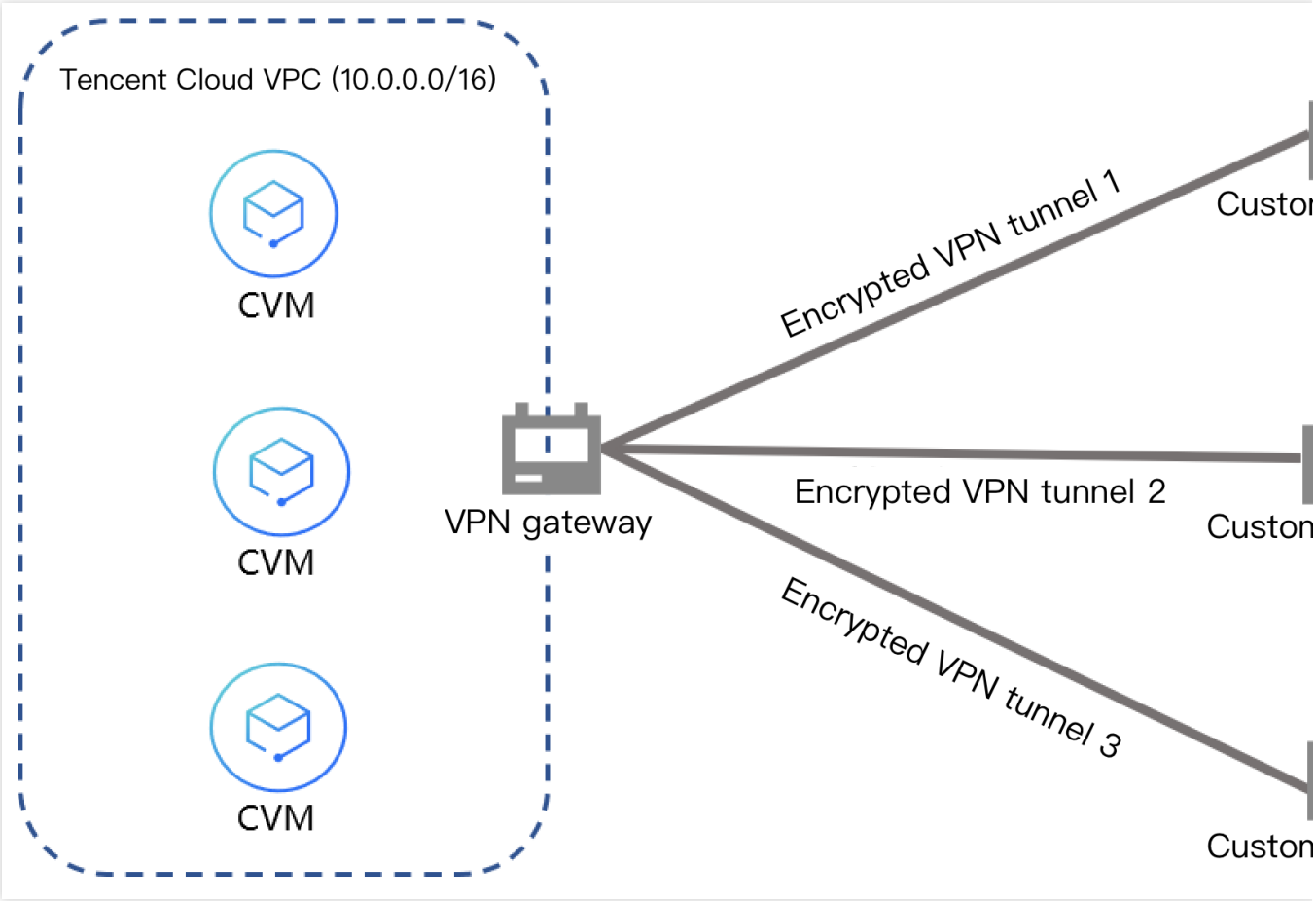


Scenario 6: communication between a single VPC and multiple IDCs via multiple VPN tunnels

This communication scenario is similar to the second scenario. The difference between them is that in this scenario, the customer IDC-1, IDC-2, and IDC-3 only need to communicate with VPC and don't need to communicate with each other.

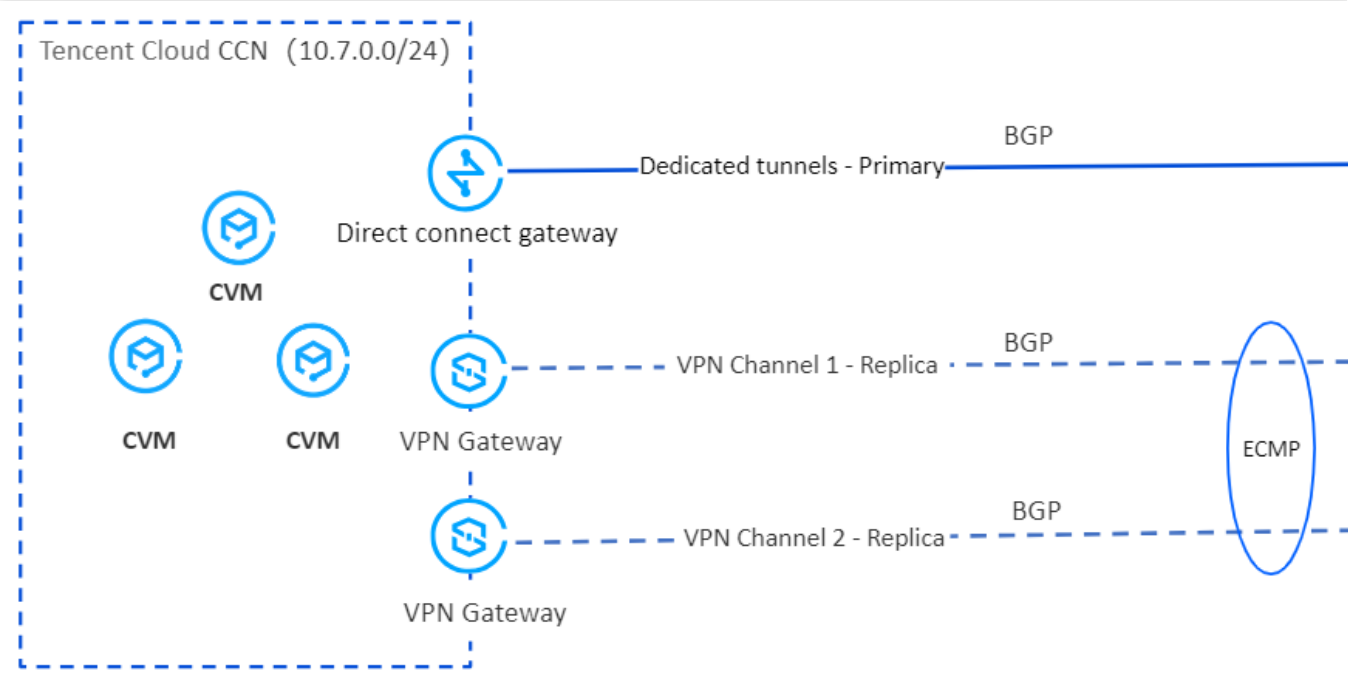
In terms of this scenario, we recommend that SPD policy-based routing method be used to create the VPC > IDC1, VPC > IDC2, and VPC > IDC3 rules.

If the destination routing method is used alone, IDC-1, IDC-2, and IDC-3 can communicate with each other, which does not conform to the communication scenario. You can configure the VPC > IDC1 and VPC > IDC2 rules when using the SPD policy-based routing method, and then configure in the route table a routing policy whose destination IP range is IDC3. As SPD policy-based routing has higher priority over destination routing, this communication scenario can also be realized.



Scenario 7: A VPN Gateway and a DC Gateway Realize Primary/Secondary Disaster Recovery

This communication scenario is akin to Scenario 5, with the distinction lying in the utilization of the dynamic BGP for orchestrating a primary DC + a standby VPN to achieve disaster recovery redundancy. Within this framework, the two VPN gateways are configured in an ECMP relationship. Under normal circumstances, service traffic flows through the dedicated channel; in the event of a failure, traffic is automatically rerouted to the VPN. Once normalcy is restored, service traffic seamlessly switches back to the DC.



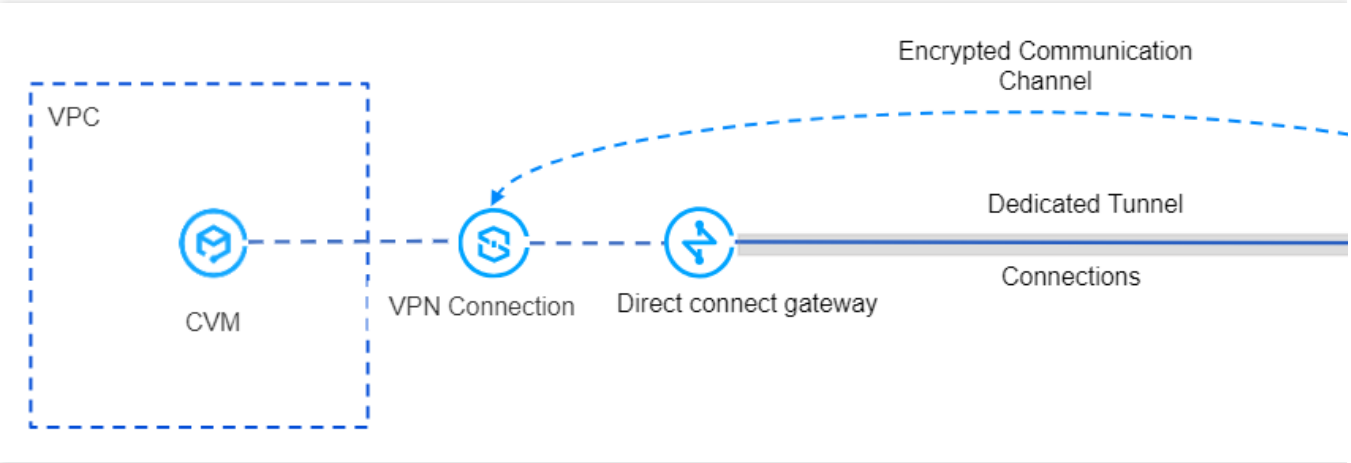
Scenario 8: A VPN Gateway and a DC Gateway Realize Encrypted Private Network Traffic Communication

Upon establishing private network communication between the local IDC and the cloud-based VPC via a physical DC, the private VPN gateway can create an encrypted communication channel with the local gateway device through the established private network connection. You may guide the traffic to be communicated between the local IDC and the VPC, into the encrypted communication channel through pertinent routing configuration, thereby achieving the encrypted communication of private network traffic.

Note:

In this scenario, the IP address of the private VPN gateway belongs to the tenant's VPC.

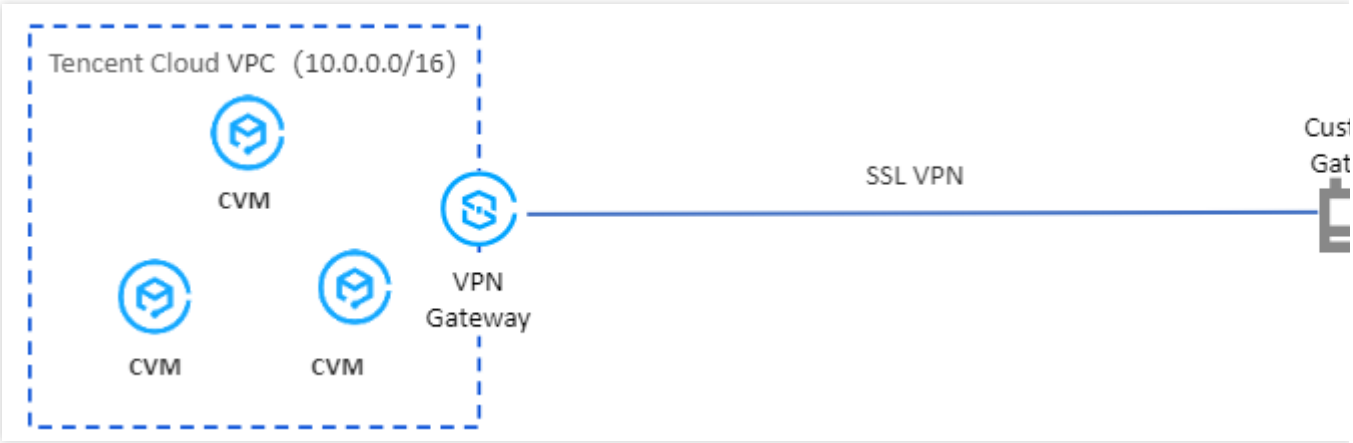
Currently, the private VPN only supports VPC-based VPNs, with CCN-based VPNs not yet supported.



Use Cases of SSL VPN

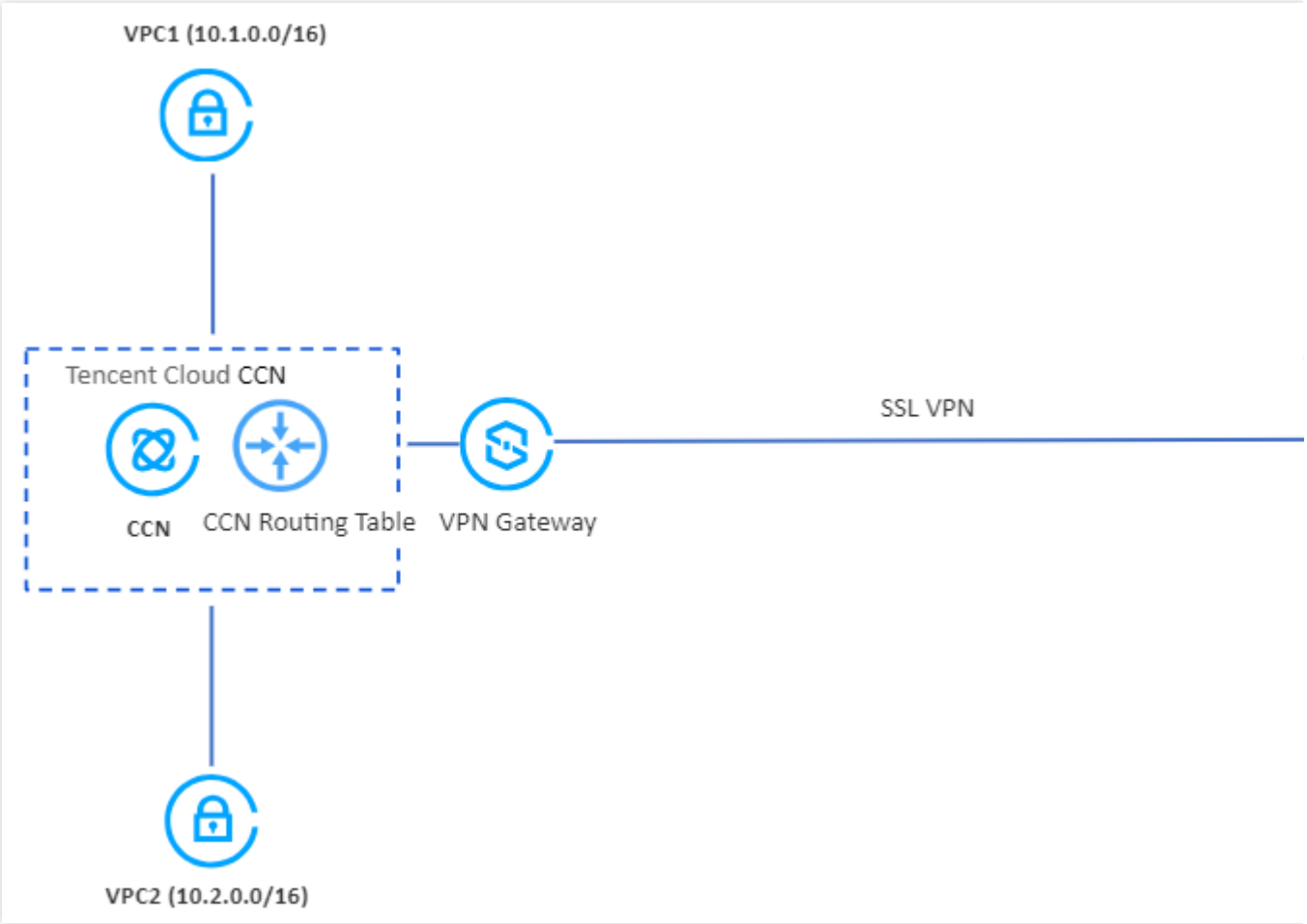
Scenario 1: Remote Access to a Single VPC from Mobile Devices

Users can establish a connection to resources within a single VPC in the cloud via an SSL VPN, enabling remote access from PCs or mobile devices.



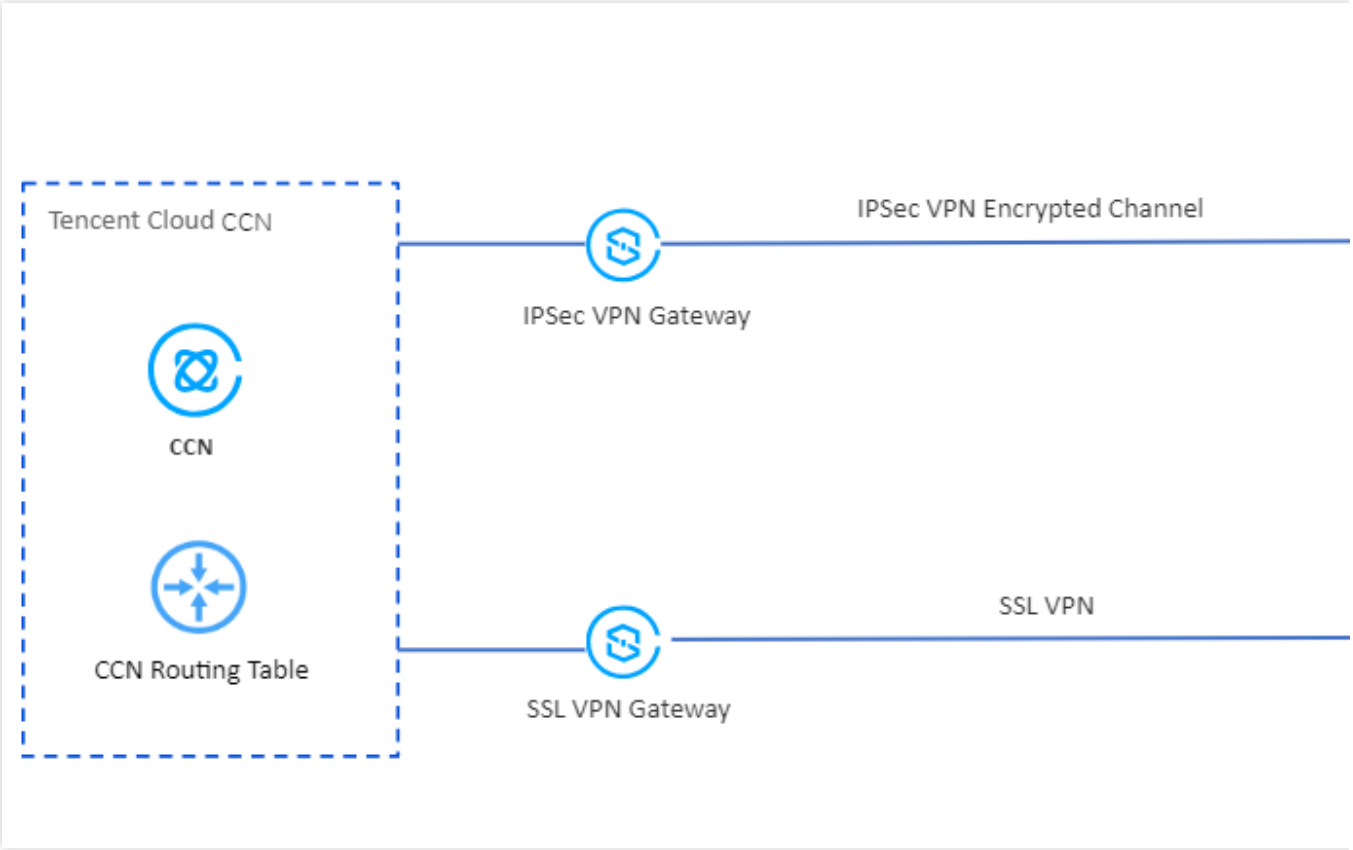
Scenario 2: Remote Access to Multiple VPCs from Remote Devices

Users can establish a connection to resources across multiple VPCs in the cloud via a CCN-based SSL VPN, enabling remote access from PCs or mobile devices.



Scenario 3: Access to IDC Resources via a VPN from Mobile Devices

Through the CCN, users can associate IPSec VPN gateways and SSL VPN gateways, enabling remote access to resources and services within their own IDC using PCs or mobile devices.



Use Limits

Last updated：2024-08-15 16:23:28

VPN Connections

Note the following when using a VPN connection:
After configuring VPN parameters, you need to add routing policies for your VPN gateway in the route table associated with the subnet, so that network requests from CVMs in the subnet to access the peer IP range can reach the customer gateway through the VPN tunnel.
For a VPN gateway v1.0, after configuring the route table, you need to ping an IP address in the peer IP range from a CVM in the VPC to activate the VPN tunnel.
The stability of the VPN connection depends on the ISP's public network.
The VPN connection only supports the PSK authentication method rather than CA authentication.
SPD or route IP ranges of the VPN connection cannot be specified as the following IP ranges:
Multicast addresses that are all 0, all 225, or start with 224.
Loopback addresses: 127.x.x.x/8.
IPv6 IP ranges.

VPN Gateway

VPN Connections is a region-level service, but you can also connect to your VPN gateway in any region over the internet.
You cannot specify a public IP or the ISP of the public IP for the VPN gateway. IPv6 and anycast IP addresses are also not supported.
The bandwidth allocated by Tencent Cloud for inbound and outbound traffic is equivalent to the bandwidth purchased by the user.
Currently, only VPN 4.0 gateways with specifications of 200 Mbps, 500 Mbps, 1,000 Mbps and 3,000 Mbps support the dynamic BGP feature.
Routing priority: Static routing > dynamic BGP routing.
Private VPN: Only VPC type IPSec VPN 4.0 version is supported. If you need to use a private VPN, submit a ticket for consultation.

Customer Gateway

You must specify the IP address of the customer gateway. The public IP of the customer gateway cannot be the following IP addresses:
Multicast addresses that are all 0, all 225, or start with 224.
Loopback addresses: 127.x.x.x/8.
IP Addresses with host bits being all 0 or all 1, for example:
Class-A IP addresses that start with 1-126, such as `1-126.0.0.0` and `1-126.255.255.255`.
Class-B IP addresses that start with 128-191, such as `128-191.x.0.0` and `128-191.x.255.255`.
Class-C IP addresses that start with 192-223, such as `192-223.x.x.0` and `192-223.x.x.255`.
Internal service addresses: `169.254.x.x/16`.
IPv6 addresses.
If you use an IPsec VPN connection to interconnect resources in two VPCs, the VPCs are each other's customer gateway, and their IP ranges cannot overlap.

SSL VPN Server

The server supports only UDP but not TCP.
To modify information such as port, authentication method, and encryption algorithm, you need to download the client configuration again.
The client and local IP ranges cannot overlap.
Identity verification relies on an EIAM application and cannot be directly interconnected with other identity providers (IdPs) for verification. You can use EIAM to interconnect with the verification source of your enterprise. You can also select a verification method supported by EIAM, such as SMS, WeCom, and AD. Currently, identity verification is in beta test. To try it out, submit a ticket for application.
You can use CAM if identity verification is enabled.

SSL VPN Client

You need to prepare the client on your own. An SSL VPN connection supports the open-source OpenVPN client or other compatible commercial clients.
Each client can use only one SSL client configuration certificate. You cannot use the same certificate for multiple clients.
Supported OpenVPN versions: 2.4.8–3.x.
Identity verification is supported only by OpenVPN 3.x or other compatible clients.
In a Windows environment, should your client's OpenVPN be version 3.4.0 or higher, it becomes imperative to configure both encryption and authentication algorithms for the SSL server setup. It is noteworthy that the authentication algorithm exclusively supports SHA1.

In a single operation, up to 100 SSL clients can be created in bulk.

Resource Limits

Limits on IPsec VPN

Note:

The private VPN gateway currently does not support dynamic BGP routing.

Resource	VPN Limit
VPC IPsec VPN gateways per region per account	10
CCN IPsec VPN gateways per region per account	10
Customer gateways in one region	20
VPN tunnels supported by one customer gateway	20 **Note：** The number of VPN tunnels supported by a customer gateway is the quota for the account. Only one VPN tunnel can be established between a pair of customer gateway and VPN gateway.
VPN tunnels that can be created on one VPN gateway	20
SPDs in a VPN tunnel	10
Peer IP ranges supported by a SPD	50
Routes supported by each VPN gateway route table	1,000
Number of routes can be added at one time on the console	10
Dynamic BGP-learned routing entries supported by each VPN gateway	500
Routing entries sent via the dynamic BGP for each VPN tunnel	10,000
BGP ASN	The default value is 64,551, with an allowable range from 1 to 4,294,967,295. Notably, the numbers 139,341, 45,090

	and 58,835 are unavailable for use.

Limits on SSL VPN

Resource	Limit
VPC SSL VPN Gateways per Region per Account	10
SSL VPN servers that can be created for an SSL VPN gateway	1
Local IP ranges that can be added on an SSL VPN server	5
Client IP ranges that can be added on an SSL VPN server	1 **Note：** To ensure that all your clients can be assigned an IP address, we recommend you specify a client IP range containing IP addresses more than the SSL VPN connections.
Validity period of the SSL VPN client certificate	In 3
SSL VPN connections	A [5,100] Mbps SSL VPN gateway can sustain up to 100 SSL VPN connections. A 200/500 Mbps SSL VPN gateway can sustain up to 500 SSL VPN connections. A 1,000 Mbps SSL VPN gateway can sustain up to 1,000 SSL VPN connections. **Note：** The maximum number of SSL VPN connections is the number of connections to the client. Once it is configured, it cannot be modified. Therefore, plan an appropriate value before configuration. The number of clients that can be connected to an SSL VPN gateway is also contingent upon the number of SSL connections configured at the time of creation. For instance, if you set up the gateway with five connections, then the maximum number of clients that can be connected to this gateway is five.

Related products

Last updated：2024-01-09 14:20:07

For information about products related to VPN connections, see the table below:

Product name	Description
VPC	VPN connection is used to connect customer IDC with a VPC through an encrypted tunnel over the public network.
Anti-DDoS Pro	Anti-DDoS Pro instance can be bound to a VPN gateway to defend against DDoS and CC attacks with high-bandwidth protection.
Direct Connect	If your business is sensitive to delay and jitter, we recommend that you access a VPC via Direct Connect.
Route Table	You need to add routing policies for your VPN gateway in the route table associated with a subnet, so that network requests can reach the customer gateway through the VPN tunnel.
CCN	VPN gateway for CCN can be associated with CCN to establish an encrypted communication between the IDC and CCN.