VPN Connections

FAQs

Product Documentation

Contents

FAQs
Concepts

Last updated：2021-09-03 18:03:30

What is a VPN connection?

A VPN connection is used to connect a customer IDC with a VPC through an encrypted tunnel over the public network. For more information, see Overview.

What is a VPN tunnel?

After VPN gateway and customer gateway are created, you can establish a VPN tunnel between the VPC and an external IDC for encrypted communication. For more information, see Overview.

What is a VPN gateway?

A VPN gateway is an egress gateway for VPC 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 and an external IDC. Tencent Cloud VPN gateway uses software virtualization and a dual-server hot backup architecture. When one server fails, automatic switchover helps ensure the normal operation of your businesses.

- Eight bandwidth caps are available for a VPN gateway: 5 Mbps, 10 Mbps, 20 Mbps, 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, and 1000 Mbps. You can adjust the bandwidth setting for a VPN gateway.
- You can bind an Anti-DDoS instance to a VPN gateway to defend against DDoS and CC attacks with high-bandwidth protection.

What is an IPsec VPN?

IPsec VPN is used to connect a customer IDC with a VPC through an encrypted tunnel over a public network. Tencent Cloud IPsec VPN connection consists of the following components:

- **VPN gateway**: an IPsec VPN gateway in a VPC. It is used with a customer gateway (IPsec VPN gateway on the IDC side) to establish an encrypted communication between the VPC and your IDC.
- **Customer gateway**: an IPsec VPN gateway on the IDC side that is mapped to the VPC. It is used with a VPN gateway. Each VPN gateway can create encrypted VPN tunnels with multiple customer gateways.
- **VPN tunnel**: an encrypted IPsec VPN tunnel over the public network. After the VPN gateway and customer gateway are created, you can establish a VPN tunnel between the VPC and an external

IDC for encrypted communication.

What are the limitations on using a VPN?

To use a VPN, take notice of the limitations on IP addresses of the VPN connection and the customer gateway. For more information, see Use Limits.

How many VPN gateways and VPN tunnels can I create?

The creation limit varies depending on the resources. For more information, see Quota Limit. To increase the limit, please submit a ticket.

Can a VPC connect to multiple IDCs through VPN connections?

Yes. You can create VPN gateways in a VPC and create multiple VPN tunnels for each VPN gateway. Each VPN tunnel connects the VPC to one local IDC.

Can two VPCs communicate with each other through a VPN connection?

Yes. You need to separately purchase VPN gateways and configure VPN tunnels and customer gateways in the two VPCs, but the configuration is complex. So we recommend using Cloud Connect Network (CCN) to connect two VPCs over the Tencent Cloud private network and help ensuring the communication quality.

How do I ensure the network quality between a VPC and a VPN-connected IDC?

- Because a VPC connects to an IDC through a VPN connection on the public network, latency, packet loss, or jitter on the public network may affect the VPN connection. If you require more stable communication, we recommend that you use Direct Connect.
- Tencent Cloud provides 24-hour monitoring on your VPN gateways and reports alarms for exceptions. OPS personnel are available for emergencies. You can also monitor the traffic of your VPN gateways and tunnels on the console in real time. In case of any exceptions, contact us promptly.

What are differences between Direct Connect and IPSec VPN connections?

- An IPsec VPN connection establishes an encrypted network connection between your IDC and VPCs based on the public network and IPsec protocol. You can purchase a VPN gateway and make it effective in just a few minutes. However, a VPN connection may be interrupted due to public network jitters or congestion. When your business does not require a high-quality network connection, the VPN connection is a cost-effective choice for rapid deployment.
- Direct Connect provides a network connection solution dedicated to your business. The configuration may take a longer time, but it can provide a highly reliable network connection.

When your businesses have a higher requirement for the network quality and security, this option fits in.

The table below lists their specific differences.

Advantage	Direct Connect	IPsec VPN Connection
Stable network latency	Network latency is stable and guaranteed. A Direct Connect instance accesses the network through dedicated links, and supports fixed routes, removing the pain of unstable latency caused by network congestion or failure bypass.	Network latency is unstable. An IPsec VPN connection accesses the network over the Internet, which may be exposed to bypass due to network congestion.
Highly reliable disaster recovery access	Access devices and network forwarding devices are deployed in distributed clusters to ensure high reliability of all links. It also supports dual-line access with protection to provide more than 99.95% of uptime.	Features a dual-server hot backup architecture with high availability at the gateway layer. However, it cannot provide the same network availability as dedicated lines due to the unreliable Internet links.
Large bandwidth	It provides a bandwidth of up to 10 Gbps for each link. You can have multiple 10 Gbps links for network load balancing, so it can theoretically support unlimited bandwidth.	A single IPsec VPN gateway supports a bandwidth of up to 1 Gbps and a VPC can have multiple VPN gateways, which can meet the need for a VPN connection larger than 1 Gbps.
High security	Dedicated network links offer strong security without data leakage risks, satisfying the demanding network connection requirements of the finance and government sectors.	Network transmission is encrypted using IKE pre-shared key, which can satisfy the security requirements for most network transmission.
Network address translation	It supports configuring the network address translation service on gateways, as well as IP mapping on the two sides of Direct Connect and IP port mapping on the VPC side, to avoid address conflict in case of interconnection among multiple networks.	Not supported.

Can I access the Internet through a VPN connection?

No. VPN gateways only provide access to VPCs but not to the Internet.

Features

Last updated : 2021-07-27 17:58:18

How does a VPN gateway work? How about its availability?

- A VPN gateway uses the network functions virtualization (NFV) and an active-active hot backup mechanism. When one server fails, automatic switchover helps ensure the normal operation of your businesses.
- Because a VPN tunnel runs on the public network, congestion, jitter, or delay on the public network may affect the VPN network. If your business is sensitive to delay and jitter, we recommend using the Direct Connect.

Why does the monitoring data displayed on the VPN gateway and VPN tunnel sometimes differ?

Currently, VPN gateway and VPN tunnel collect data at a different interval. The statistical granularity of the VPN gateway is 1 minute, and that of the VPN tunnel is 10 seconds. Therefore, the statistical data shown on the monitoring page of the VPN gateway may be different from that of the VPN tunnel.

How can I configure a VPN?

You can fully configure the IPsec VPN on the console. For more information, see Getting Started Overview.

How can I create a VPN gateway?

You can log in to the VPC console to create a VPN gateway as instructed in Step 1: Create a VPN Gateway.

How can I create a VPN tunnel?

You can log in to the VPC console to create a VPN gateway as instructed in Step 3: Create a VPN Tunnel.

How can I query the VPN connection monitoring data?

You can log in to the VPC console to query the VPN connection monitoring data as instructed in Viewing Monitoring Data.

How can I set a VPN connection alarm?

You can log in to the VPC console to set a VPN connection alarm as instructed in Setting Alarms.

How can I query the VPN gateway details?

You can log in to the VPC console to query the VPN gateway details as instructed in Viewing a VPN Gateway.

How can I modify the VPN tunnel configuration?

You can log in to the VPC console to modify the VPN tunnel configuration as instructed in Modifying VPN Tunnel.

How can I bind an Anti-DDoS instance?

You can log in to the Anti-DDoS Pro console to bind an Anti-DDoS instance as instructed in Binding an Anti-DDoS Instance.

Why can’t I create a VPN connection that supports more than 100 MB?

- This feature is unavailable in certain regions, which can be checked in the console.
- The A5 route is not configured.
- This feature is not enabled. Please submit a ticket to enable it.

How can I configure health check?

1. Ensure that the customer gateway is a routing gateway.
2. Configure health check in the Tencent Cloud console.

> Note :
>
> - Create the primary and secondary VPN tunnels before configuring health check to avoid affecting your business.
> - The IP addresses of the VPN gateway and the customer gateway do not conflict. If the two IP addresses belong to one IP range, there is no need to configure a separate route to specify the customer gateway.

3. Configure the VPN gateway route and set its priority.

Why does the fee still be automatically deducted even when the VPN tunnel is not connected or has been deleted?

The outbound traffic of the VPN gateway will be charged. Delete the unused VPN gateway to avoid fee deduction.

Billing

Last updated : 2019-12-03 18:56:31

Why can’t I renew or upgrade VPN gateways?

A VPN gateway cannot be renewed and upgraded at the same time. If you have an unpaid renewal or upgrade order, other renewal or upgrade operations cannot be performed. The system invalidates unpaid renewal or upgrade orders at 24:00 every day, after which you must re-submit your order.