VPN Connections

FAQs

Product Documentation

Contents

FAQs
Concepts

Last updated：2024-01-09 14:20:07

What is an IPsec VPN?

IPsec VPN is used to connect 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.

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.

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	Network latency is unstable. An IPsec VPN connection accesses the network over the Internet,

	unstable latency caused by network congestion or failure bypass.	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.
High 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.

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.

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

A VPC connects to an IDC through a VPN connection in the public network. Therefore, latency, packet loss, or jitter in the public network may affect the VPN connection. If you require highly stable communication, we recommend that you use Direct Connect.
Tencent Cloud provides 24-hour monitoring for 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 in the console in real time. If exceptions occur, submit a ticket.

Can I access the Internet through a VPN connection?

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

Can I use VPN Connections without a public IP?

If you use an IPsec VPN connection, you must have a public IP.
If you don't have a public IP, you can try using an SSL VPN connection to connect your LAN and the cloud environment. To check whether an SSL VPN connection can meet your requirements, see Directions.
Note:
Using an IPSec VPN connection requires the customer gateway to have a fixed IP address.
An SSL VPN gateway doesn't require that the customer gateway have a fixed public IP address. It is an egress gateway through which the VPC establishes an SSL VPN connection and is used together with the SSL VPN client (mobile client). For more information, see Directions.

What is a customer gateway?

A customer gateway is a logical object that records the VPN gateway on the edge of the peer IDC.

What is an SPD policy? Why do I need to configure the local and peer IP ranges?

A Security Policy Database (SPD) policy consists of a series of SPD rules that determine the IP ranges in a VPC or CCN and the IP ranges in an IDC that can communicate with each other.
Therefore, the local and peer IP ranges must be configured for an SPD policy. The local gateway settings specify the IP ranges of the Tencent Cloud VPN gateway. The IP ranges cannot overlap with each other. The customer gateway settings specify the public network IP ranges of the local customer gateway that is interconnected with Tencent Cloud.

What is an SSL VPN client?

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

Scenarios

Last updated：2024-01-09 14:20:07

What do I do when an employee leaves the company or a project team, or when I need to temporarily revoke an employee's permissions?

You can disable the corresponding certificate on the SSL VPN client page. For more information, see Managing SSL VPN Client Certificate.

Can I remotely connect to my VPC over a VPN connection?

Yes. Tencent Cloud provides SSL VPN that allows you to remotely access the resources and services in your VPC by using a computer or mobile phone. That is, you can connect to your VPC by using SSL VPN. For more information, see Connecting the Mobile Client to VPC > Directions.

Can I access the internet over an SSL VPN connection?

No. This is not supported.

Can multiple IDCs communicate with each other by using a VPN gateway?

Yes. You can use **VPN for Cloud Connect Network (CCN)** to allow multiple IDCs that do not require access to cloud resources to communicate with each other. In this case, each IDC uses its own IPsec VPN devices to access the VPN gateway for CCN, without being associated with a CCN instance, for traffic forwarding.

Can multiple IDCs communicate with a VPC by using a VPN gateway?

Yes. You can create a VPN gateway for CCN and associate the gateway with a CCN instance. In this case, each IDC uses its own IPsec VPN devices to access the VPN gateway for CCN to communicate with a VPC.

Can I implement redundant communication by using a DC connection as the primary connection and a VPN connection as the secondary connection?

Yes. You can create a VPC-based Direct Connect (DC) gateway and a VPC-based VPN gateway. Then, you can create a DC connection and a VPN connection. Based on the VPC route priority, the DC connection serves as the primary connection and the VPN connection serves as the secondary connection. This allows you to implement

redundant communication. For more information, see Hybrid Cloud Primary/Secondary Communication (DC and VPN).

How do I implement primary/secondary disaster recovery?

You can use Tencent Cloud VPN Connections to implement primary/secondary disaster recovery. To be specific, you can create two IPsec VPN tunnels (route table) and configure the subnet routing, gateway routing, as well as routing weights. For more information, see Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery.

How do I use Tencent Cloud VPN Connections? How do I choose between IPsec VPN and SSL VPN?

Tencent Cloud VPN Connections supports both the IPsec and SSL network security protocols.
You can use IPsec VPN for site-to-site connections. For more information, see IPSec VPN.
You can use SSL VPN for client-to-site connections. For more information, see Connecting the Mobile Client to VPC.

Does Tencent Cloud VPN Connections support internet access acceleration?

No. Tencent Cloud VPN Connections does not support internet access acceleration. If you want to accelerate internet access, see Anycast Internet Acceleration.

Can I use Tencent Cloud VPN Connections to access a hotel system that runs on Tencent Cloud from hotels in six regions?

Yes. You can use SSL VPN in this scenario. If you have higher security requirements, you can configure access control. For more information, see SSL VPN Access Control and Portal Login Guide.

Can I use Tencent Cloud VPN Connections to visit Google?

No. Tencent Cloud VPN Connections provides services in compliance with national laws and regulations, and does not provide the internet access or proxy service. You are not allowed to technically circumvent internet censorship to visit banned websites.

Can I use Tencent Cloud VPN Connections to access Tencent Cloud without a public IP address?

Yes. You can use SSL VPN in this scenario.

Can I use Tencent Cloud VPN Connections for non-Tencent Cloud products?

Yes. Tencent Cloud VPN Connections is developed based on the standard IKE and IPsec protocols. Therefore, it is compatible with all VPN devices and services in compliance with the protocols.

Does Tencent Cloud VPN Connections support primary/secondary disaster recovery based on ECMP?

No. Tencent Cloud VPN Connections does not support Equal-Cost Multipath Routing (ECMP). However, you can use Tencent Cloud VPN Connections to implement primary/secondary disaster recovery in the following way: Create two IPsec VPN tunnels (route table) and configure the subnet routing, gateway routing, as well as routing weights. For more information, see Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery.

How can I configure a VPN connection?

You can fully configure an IPsec VPN connection on the console. For more information, see 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.

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

Yes. You can separately purchase VPN gateways and configure VPN tunnels and customer gateways in the two VPCs, but the configuration is complex. We recommend that you use Cloud Connect Network (CCN). CCN connects two VPCs by using the private network of Tencent to ensure the quality of communication.

Can I use Tencent Cloud VPN Connections for the proxy service?

Tencent Cloud VPN Connections provides services in compliance with national laws and regulations, and does not provide the internet access or proxy service.

Generic class

Last updated：2024-01-09 14:20:07

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.

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.

Billing

Last updated：2024-01-09 14:20:07

What's the billing mode for VPN connections?

VPN tunnels and customer gateways are free of charge, but VPN gateways are charged.
VPN gateways can be billed in pay-as-you-go mode. For more information, see Billing Overview.

For more information about VPC pricing, see Purchase Guide.

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.

Will I receive a reminder when my VPN gateway expires?

For more information, please see Expiration Notifications.

Is an SSL VPN connection still charged after it is terminated?

After an SSL VPN connection is terminated, no traffic fees will be incurred. However, the VPN gateway instance fee and SSL connection fee are fixed and will also be charged. Please delete any resources that you no longer need in time.

Why is a VPN connection charged immediately after it is created?

The billing items vary based on the VPN product type:
The billing items of IPsec VPN include the gateway instance and public network traffic. A fixed fee is charged for the gateway instance.
The billing items of SSL VPN include the gateway instance, SSL connections, and public network traffic. Fixed fees are charged for the gateway instance and SSL connections, and the public network traffic is charged in pay-as-you-go mode.
For more information about billing, see Billing Overview.

Why is a pay-as-you-go VPN connection still charged after it is deleted?

A VPN connection is hourly postpaid in pay-as-you-go billing mode (billed hourly; time less than an hour is counted as an hour). If you use a connection during 12:02–13:20, fees will be incurred for two hours (12:00–13:00 and 13:00–14:00). In addition, the billing time in pay-as-you-go mode is not fixed and may be delayed; for example, fees for 13:00–14:00 may be billed after 14:00 or 15:00.

Do I need to pay for VPN tunnels and customer gateways?

VPN tunnels and customer gateways can be used for free.

Why cannot I delete an overdue gateway?

You can delete an overdue gateway only after you delete the resources associated with the gateway.

If I use an SSL VPN connection only from 8:00 to 12:00 in the morning, is the connection charged for other time periods?

In time periods with no traffic, only the VPN gateway instance fee and the SSL connection fee are charged.

How do I enable auto-renewal?

In the Tencent Cloud console, click **Cost** in the upper right corner, and click **Renewal management** in the left sidebar. On the **Auto Renewal** tab, enable auto-renewal for required resources.

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.

Can I upgrade or downgrade my VPN gateway configurations?

In terms of quota, the VPN gateway bandwidth can only be adjusted in specific bandwidth ranges. Please properly plan the bandwidth for your business.
Pay-as-you-go: The VPN gateway bandwidth can only be adjusted in the current bandwidth range ([5 Mbps, 100 Mbps] or [200 Mbps, 1000 Mbps]). Cross-range adjustment is not supported.
The bandwidth of 1000 Mbps SSL VPN gateways and 3000 Mbps IPsec VPN gateways cannot be downgraded. Please properly plan the bandwidth for your business.

About IPsec gateways

Last updated：2024-01-09 14:20:07

VPN Gateway
VPN Tunnel

Why am I unable to delete a VPN gateway?

You can delete a VPN gateway only after you delete the VPN tunnel resources that are associated with the VPN gateway. For more information, see Deleting SSL VPN Gateways.

What does a 50 Mbps bandwidth cap mean?

A bandwidth cap for a VPN gateway is the maximum outbound bandwidth from the VPN gateway to the Internet.

Why is the data upload speed only 2 Mbps while the gateway bandwidth is 50 Mbps?

The data upload speed also varies based on your Internet access speed, in addition to the bandwidth specification that you purchased.

Can I change an IPsec VPN gateway to an SSL VPN gateway?

No, you cannot change the VPN gateway type.

Does a VPN gateway support bandwidth configuration adjustment?

Currently, you can adjust the bandwidth configuration only within some specifications, such as [20 Mbps, 100 Mbps] and [200 Mbps, 1000 Mbps]. For example, you can increase the bandwidth cap from 50 Mbps to 100 Mbps. If you want to increase the bandwidth cap from 100 Mbps to 200 Mbps, you must create a gateway that supports a bandwidth specification of 200 Mbps.

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 does a VPN gateway work? How about its availability?

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

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 IPSec VPN Gateway.

Why am I unable to ping a VPN tunnel that is in the connected state?

If the tunnel is in a normal status yet the private network cannot be connected, the possible causes are as follows:
No routes directing to the private IP range in the IDC are added in the route table of the VPC subnet.
The security policy on the VPC/IDC side does not allow access to the corresponding source and destination IPs.
No tunnels directing to the private IP range in the IDC are added to the VPN gateway (route-based gateway).
The firewall of the operating system of the private network server on the VPC/IDC side does not allow the IP addresses in the customer IP range to pass.
The SPD policy on the VPC/IDC side does not contain the source and destination IPs.
No routing policies are configured on the VPN gateway.
For more information, see VPN Tunnel Connected Yet Private Network Unconnected.

Why is a VPN tunnel in the unconnected state?

The possible causes are as follows:
No traffic exists to activate the tunnel.
The public IP address of the VPN gateway is not connected.
The security policy is not correctly configured.
Inconsistent negotiation parameters and modes exist.
For more information, see VPN Tunnel Unconnected.

Why does my gateway suddenly fail when it is in use?

The possible causes are as follows:
The public IP address that you access is under Internet censorship and is blocked due to regulation compliance.

You have modified the local settings, such as the protocol, or new protocol parameters are automatically enabled during local upgrade but the parameters are not configured on Tencent Cloud.
Access to Tencent Cloud is prohibited by the local firewall.
Negotiation parameter values, such as SA lifetime, are inconsistent.
The VPN tunnel is deleted.

Why do I need to configure an SPD policy?

An SPD policy specifies the IP ranges in the network in which the VPN gateway resides and the IP ranges in the IDC that can communicate with each other.

Note:

The IP ranges specified in an SPD policy must not overlap with those specified in another SPD policy of the same VPN gateway.

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. For more information, see Configuring Health Checks.

Note:

Create primary and secondary VPN tunnels before you configure health check, to avoid impacts on your business. We recommend that you do not configure health check without primary and secondary VPN tunnels.
Ensure that the IP addresses of the VPN gateway and the customer gateway do not conflict. If the two IP addresses belong to the same 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 is the tunnel in the "unhealthy" status?

The ping test of IP that you configured for health check failed. Please check the configuration.

Do VPNs support the aggresive mode?

No.

How do I configure an SPD policy? Can I enter any peer IP range?

An SPD policy specifies the IP ranges in the network in which the VPN gateway resides and the IP ranges in the IDC that can communicate with each other. A peer IP range is a subset of accessible public IP ranges and cannot overlap with the IP ranges that are specified in other SPD policies of the same VPN gateway.

Do the local and peer IP ranges in an SPD policy for an SPD policy-based VPN tunnel need to follow specific sequence requirements?

No sequence requirements are imposed for the local and peer IP ranges in an SPD policy.

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 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.

What are the mappings between the local and peer IP ranges in an SPD policy?

For more information, see SPD policy in Creating a VPN Tunnel.

About SSL

Last updated：2024-01-09 14:20:07

How do I specify the local and peer IP ranges when I create an SSL VPN server?

Tencent Cloud IP range: Enter the Tencent Cloud IP range to be accessed by mobile clients, which is the IP range of the subnet in which your VPN gateway resides. For example, enter 10.0.0.0/24, 10.0.0.0/26, 10.0.0.0/28, or 10.0.0.0/30 for the 10.0.0.0/18 subnet.
Client IP range: Enter the IP range that the SSL VPN gateway assigns to the client for communication with Tencent Cloud. You can enter any IP range whose subnet mask is less than or equal to 24. Take note that the IP range must not conflict with the VPC CIDR of Tencent Cloud or your local private network.

Why does the SSL connection fail?

1. The public network connection failed. Check the connectivity of the public network.
2. The public IP address is invalid. You cannot use a cross-border public IP address to access cloud resources.
3. Subnet routing is not configured. For more information about how to configure subnet routing, see Step 4: Configure the Tencent Cloud Routing Policy.
4. The SSL client certificate is used by multiple users. Only one user can use the SSL client certificate.

Can I change the number of SSL connections?

No. You must plan the number of SSL connections in advance.

Does an SSL VPN require fixed public IP addresses?

No. SSL VPN connections do not require fixed IP addresses on the user side. An SSL VPN allows Windows, MAC, and Linux clients, as well as mobile phones that use OpenVPN, to connect to instances on Tencent Cloud VPCs.

Can I switch an SSL VPN to an IPsec VPN?

No, you cannot change the VPN gateway type.

Can multiple clients use the same certificate?

No, each SSL client configuration certificate can be used only by one client.

What is the maximum number of SSL connections allowed?

The maximum number of SSL connections allowed varies based on the bandwidth specification. A bandwidth specification of [5 Mbps, 100 Mbps] supports up to 100 SSL connections. A bandwidth specification of [200 Mbps, 500 Mbps] supports up to 500 SSL connections. A bandwidth specification of 1000 Mbps supports up to 1000 SSL connections.