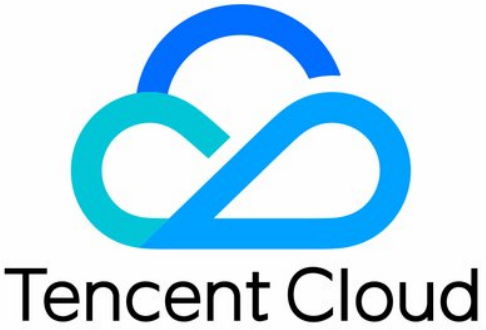
VPN Connections Operation Guide



Copyright Notice

Trademark Notice

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Operation Guide
VPN Gateway
IPSec VPN Gateway
Create IPSec VPN Gateway

Last updated: 2024-09-24 17:14:15

A VPN gateway is a VPN connection instance. Therefore, please create an IPsec VPN gateway before using a VPN connection to securely access the Tencent Cloud Virtual Private Cloud (VPC) from external networks. This document shows you how to create a VPN gateway in the console.

Prerequisites

To create a VPC-based VPN gateway, please create a VPC in the same region in advance. For details, refer to Create VPC.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. On the VPN Gateway management page, click **+Create New**.
4. In the pop-up **VPN Gateway Purchase Page**, configure the following gateway parameters.

> **Note:**
> - Only new gateways but not existing gateways are supported on 200 Mbps, 500 Mbps, 1,000 Mbps and 3,000 Mbps bandwidths.
> - If the VPN gateway uses 200 Mbps, 500 Mbps, 1,000 Mbps or 3,000 Mbps bandwidths, AES128+MD5 is recommended for VPN tunnel encryption.

Parameter name	Parameter Description
Billing Mode	Both Traffic Billing and Annual and Monthly Subscription are supported. Traffic billing is applicable to scenarios with significant bandwidth fluctuations; annual and monthly subscriptions are suitable for scenarios with relatively stable bandwidth.

Region	Select the region where the current gateway is located.
Availability Zone	Select the Availability Zone where the current gateway is located.
Protocol Type	IPSec and SSL protocols are supported.
Network Type	Both public networks and private networks are supported for resource access. If you need to use a private network type of VPN, please Submit a work order for consultation.
Associated Network	This parameter indicates whether you create a CCN-based VPN/VPN gateway or a VPC-based VPN/VPN gateway. • If you need to enable interconnection with multiple VPC networks or other dedicated networks via VPN Connections, you can select CCN. **Note:** You cannot associate the CCN-based VPN gateway with a CCN instance during its creation. You can associate a created VPN gateway to a CCN instance in the gateway details page. If you create a policy-based VPN tunnel, you also need to enable the route published to the CCN in the IDC IP range of the VPN gateway. • If you want to communicate with a single VPC by using a VPN connection, create a VPC-based VPN.
Virtual Private Cloud	Specify the VPC to be associated with the VPN gateway only when the associated network is VPC.
On-cloud subnet	Specify the outer address for external access of the VPN gateway. The address is allocated from the selected subnet.
Bandwidth Cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Gateway Name	Enter the VPN gateway name (up to 60 characters).

Tag	Tags mark VPN gateway resources so that these resources can be queried and managed efficiently. Tag is not a required configuration. You can decide whether to configure it according to your demand.
Gateway Name	Enter the VPN gateway name (up to 60 characters).

5. After completing the gateway parameter settings, click **Create** to start the VPN gateway creation. At this point, the **Status** is **Creating**. Wait about 1–2 minutes. The successfully created VPN gateway status is **Running**. The system assigns a Gateway Access IP to the VPN gateway.

Configure Cloud Routing Policy

Last updated: 2024-09-24 17:18:07

Prerequisites

Before configuring the VPN routing policy, ensure that the VPN gateway, customer gateway, and VPN tunnel have been set up.

Operation Steps

1. Log in to the VPC console.
2. In the left directory, click **Subnet**, select the relevant Region and VPC, and click the subnet's associated route table ID to go to the details page.
3. In the **Basic Information** tab, click **Add Routing Policy**.
4. In the pop-up box, enter the customer IDC subnet segment. Select **VPN Gateway** as the next hop type, choose the newly created VPN gateway as the next hop, and click **Create** to complete the subnet routing policy configuration.
5. In the left directory, select **VPN Connections** > **VPN Gateway**.
6. On the **VPN Gateway** page, select the Region and VPC, and click the VPN gateway instance ID to go to the details page.
7. On the **Instance Details** page, click the **Route Table** tab.
8. Click **Add Route** and configure the routing policy.

> **Note**
> - When adding routes to the VPN gateway route table, the list will display all VPN tunnels (i.e., all SPD policy-based and routing-type VPN tunnels) under the VPN gateway by default.
> - SPD policy-based tunnels do not require route additions (in version 3.0, routes need to be configured). Only add routes for routing-type tunnels based on your communication needs.

Configuration Item	Description
Destination	Enter the subnet segment of the customer network you want to access.

Next Hop Type	Supports both VPN Tunnel and CCN types. **Note:** If it is a CCN type VPN gateway, and the VPN gateway is associated with the CCN instance, the routing policies with **CCN** as the next hop will be automatically learned by the system and displayed in the route entries. Do not manually configure duplicate routes.
Next Hop	Select the specific next hop instance ID. • If the next hop type is a VPN tunnel, select the already created VPN tunnel. • If the next hop type is CCN, the system automatically displays the CCN instance associated with the VPN Gateway.
Weight	Select the weight value of the channel: • 0: High priority. • 100: Low priority. **Note:** For primary and secondary channel scenarios, select a high priority for the primary channel and a low priority for the secondary channel. For other scenarios, select the default value.
Add a line	Multiple routing policies can be added.
Delete	You can delete routing policies, except the last one.

9. After configuring the routing policy, click **Confirm**.
10. Other executable operations.
    10.1 Enable or disable the routing policy.

Note

- Disable routing policy: Click the icon on the right side of an enabled routing policy to disable it. Disabling a routing entry may cause business interruption. Please assess carefully before proceeding.

- Enable routing policy: Click the icon on the right side of a disabled routing policy to enable it.

10.2 Disabled routing policies can be deleted.

Note

Deleting a routing policy may affect business operations. Please evaluate carefully before proceeding.

Associating a CCN Instance

Last updated: 2024-09-25 10:53:04

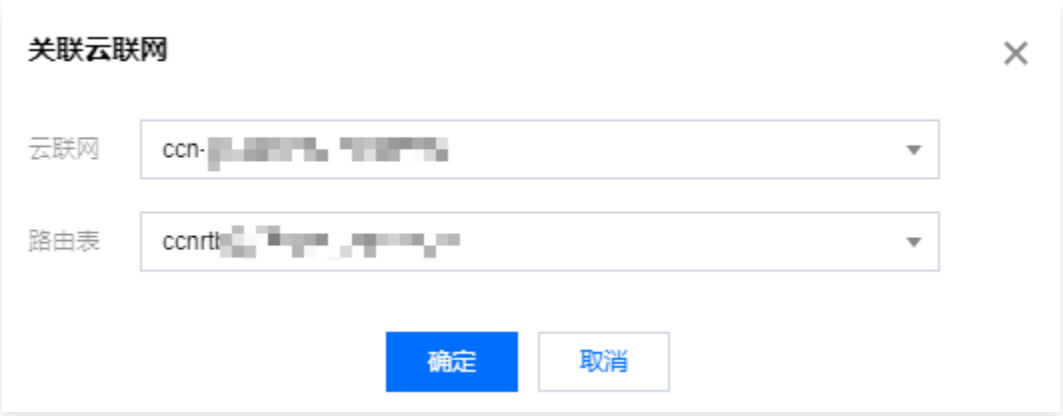
If you are creating a CCN-based VPN gateway, you need to associate the created VPN gateway to a CCN instance on the gateway details page.

Prerequisites

You have created a CCN-based IPsec VPN gateway.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click the ID of the target VPN gateway to go to the details page.
4. On the **Basic Information** tab of the gateway details page, click **Network** in the row, then click **Associate CCN** and select the CCN instance to be associated with and the corresponding route table in the pop-up dialog box.



5. Click **OK**.

Publishing IDC IP Ranges to CCN

Last updated: 2024-09-25 10:53:47

This document describes how to publish the IP range to CCN for connecting the VPN to the CCN.

> **Note:**
> If the communication mode of the VPN tunnel is "destination route", then you don't need to publish the IDC IP range to the CCN.

Prerequisites

- You have created a CCN-based IPsec VPN gateway and bound a CCN instance.
- The SPD policy has been configured in the VPN tunnel.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click the ID of the target VPN gateway to go to the details page.
4. Publish the IP range in the **Publish IP Range** tab on the details page in the CCN direction.

The IP range here is the IP range of the opposite gateway when configuring the SPD policy for the VPN tunnel.

Modifying IPSec VPN Gateways

Last updated: 2024-09-25 10:53:59

After a VPN gateway is created, the VPN gateway name, tag and bandwidth cap can be modified.

Operation Steps

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **VPN Gateway**.
3. On the **VPN Gateway** page, modify the gateway name.
   - Click the edit icon next to VPN Gateway name to modify the gateway name.
   - Click the gateway ID to enter the gateway details page, then click to rename the VPN gateway name.
4. Modify maximum bandwidth.

> **Note**
> - Modifying the bandwidth cap will change the fee to charge. Please evaluate the fee before the adjustment.
> - For versions before VPN 4.0, bandwidth adjustment is limited to specific ranges like [5,100] Mbps and [200,1000] Mbps. Cross-range adjustments are not supported.
> - VPN 4.0 supports full range bandwidth adjustments, which might take a few minutes to take effect.

- Monthly Subscription
  - In the VPN gateway instance list, find the instance whose bandwidth needs adjustment, and in the operation column click **More** > **Upgrade/Downgrade**.
  - On the upgrade page, select your new specifications, then click **Confirm**.
- Pay-as-you-go
  - Method I: In the VPN gateway instance list, find the instance to be upgraded. In the **Operation** column, click **Adjust Bandwidth** and select the new specification values.
  - Method II: Enter the instance details page, click **Bandwidth Cap** next to **Adjust Bandwidth** and select the new specification values.

5. On the "Gateway List" interface, click **Edit Tag** or enter the gateway details page and click  to modify the Tag.

Deleting IPSec VPN Gateway

Last updated: 2024-09-25 10:54:12

You can delete VPN gateways that are no longer used.

Prerequisites

- The associated VPN tunnels have been deleted. For detailed directions, see Deleting VPN Tunnel.
- The associated customer gateways have been deleted. For detailed directions, see Deleting Customer Gateways.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. On the "VPN Gateway" page, find the VPN gateway to be deleted, click **Delete** on the right side of the gateway's operation column, and in the pop-up dialog, click **OK**.

> **Note**
> Note that all the associated connections will be immediately interrupted after the VPN gateway is deleted.

Viewing IPSec VPN Gateway

Last updated: 2024-09-25 10:54:25

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click the ID of the target VPN gateway to go to the details page.
4. View the details of the VPN gateway.
   - Viewing basic information

     Click on the specific instance name in the VPN gateway instance list to view the gateway details under the **Basic Information** tab, such as name, gateway ID, public IP, status, ASN, associated network, billing mode, etc.
   - View the route table

     Click on the specific instance name in the VPN gateway instance list to view the gateway routing details under the **Route Table** tab, such as destination, channel status, health status, next hop, route type, priority, and AS Path.
   - Viewing Monitoring Information

     Click on the specific instance name in the VPN gateway instance list to view the gateway monitoring metrics under the **Monitoring** tab, such as external bandwidth out, external bandwidth in, packet count out, packet count in, external traffic out, etc.
5. View BGP Session

   Click **View BGP Session** in the action column of the VPN gateway instance list to display BGP session details in a pop-up dialog, such as cloud-side BGP address, cloud-side ASN, user-side BGP address, associated VPN channel, and session duration.

SSL VPN Gateway
Creating an SSL VPN gateway

Last updated: 2024-09-25 10:54:40

An SSL VPN gateway works as the egress of an SSL VPN connection on the VPC side. It helps establish secure and reliable encrypted network communication between Tencent Cloud VPC and mobile clients.

Prerequisites

A VPC has been created. See Creating VPC for more details.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. On the VPN Gateway management page, click **New**.
4. On the pop-up **VPN Gateway Purchase** page, configure the following gateway parameters.

Parameter name	Parameter Description
Billing Mode	The SSL VPN currently only supports traffic-based billing.
Region	Display the region of the VPN gateway.
Availability Zone	Select the Availability Zone where the current gateway is located.
Protocol Type	IPSec and SSL protocols are supported.
Network Type	• This parameter specifies whether you create a CCN-based VPN/VPN gateway or a VPC-based VPN/VPN gateway. If you want to use a VPN connection to enable interconnection with multiple VPCs or other Direct Connect networks, create a CCN-based VPN. **Note:**

	> You cannot associate the CCN-based VPN gateway with a CCN instance during its creation. You can associate a created VPN gateway to a CCN instance in the gateway details page. If you create a policy-based VPN tunnel, you also need to enable the route published to the CCN in the IDC IP range of the VPN gateway. • If you want to communicate with a single VPC by using a VPN connection, create a VPC-based VPN.
Virtual Private Cloud	Select the specific VPC to which the VPN gateway will be associated if the associated network is a VPC. For CCN instances, the gateway needs to be bound on the details page after creation. For more details, see Associating a CCN Instance.
Bandwidth Cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Number of SSL Connections	Selecting "SSL" for **Protocol Type** requires configuration of this item. The number of SSL connections supported is related to the gateway. For more details, see Usage Restrictions.
Gateway Name	Enter the VPN gateway name (up to 60 characters).
Tag	Tags mark VPN gateway resources so that these resources can be queried and managed efficiently. Tag is not a required configuration. You can decide whether to configure it according to your demand.

5. After completing the gateway parameter settings, click **Purchase Now**.

Associating a CCN Instance

Last updated: 2024-09-25 10:55:10

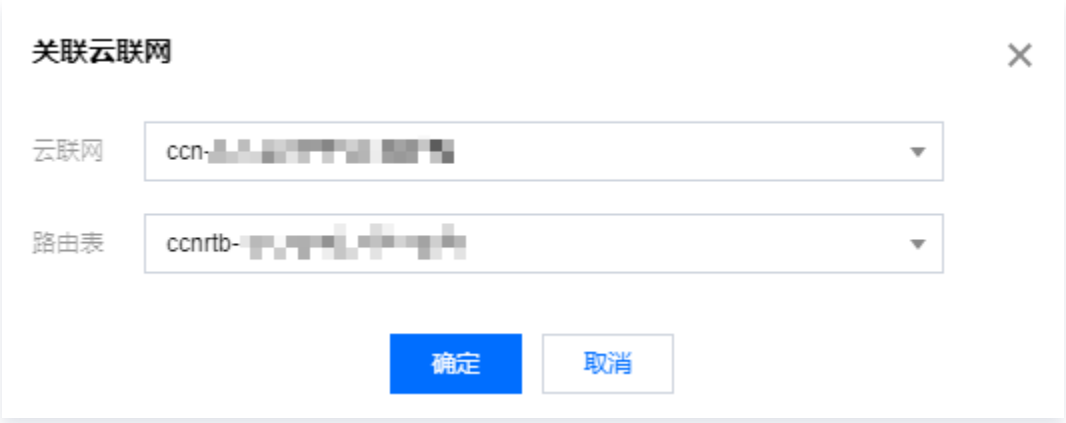
If you are creating a CCN-based VPN gateway, you need to associate the created VPN gateway to a CCN instance on the details page of the gateway.

Prerequisites

You have created a CCN-based SSL VPN gateway.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. Click the ID of the target VPN gateway to go to the details page.
4. On the **Basic Information** tab of the gateway details page, click **Network** in the row, then click **Associate CCN** and select the CCN instance to be associated with and the corresponding route table in the pop-up dialog box.



5. Click **OK**.

Modifying SSL VPN Gateways

Last updated: 2024-09-25 10:55:38

You can modify the name, tag, and bandwidth cap of a created SSL VPN gateway.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. On the **VPN Gateway** page, modify the gateway name.
   - Click the edit icon next to the name of the VPN gateway using the **SSL** protocol to modify the gateway name.
   - Click on the gateway ID to enter the gateway details page, click on the next to the gateway name to make modifications.
4. Modify maximum bandwidth.

> **Note**
> - Modifying the bandwidth cap will change the fee to charge. Please evaluate the fee before the adjustment.
> - The adjustment of the VPN gateway bandwidth is limited to [5,100] Mbps and [200,1000] Mbps.
> - The bandwidth 1000 Mbps can not be downgraded.

- Method I: In the VPN gateway instance list, find the instance whose bandwidth needs adjustment, click **Adjust Bandwidth** in the Action column, and select the new specification values.
- Method II: Enter the instance details page, click **Bandwidth Cap** next to **Adjust Bandwidth** and select the new specification values.

Deleting SSL VPN Gateways

Last updated: 2024-09-25 10:55:50

You can delete SSL VPN gateways that are no longer used.

Prerequisites

- The SSL VPN servers mounted to the gateways have been deleted. For directions, see Deleting SSL VPN Server.
- The SSL VPN clients mounted to the gateways have been deleted. For directions, see Deleting SSL VPN Client.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. In the "VPN Gateway" page, find the SSL VPN Gateway to delete, then click **Delete** in the action column, and click **OK** in the pop-up dialog.

> ⚠ **Note:**
> Note that all the associated connections will be immediately interrupted after the VPN gateway is deleted.

Viewing SSL VPN Gateways

Last updated: 2024-09-25 10:56:02

Viewing VPN Gateways

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **VPN Gateway** to enter the management page. This page displays information such as the SSL VPN gateway ID, name, status, public IP, network, and bandwidth cap.

3. Click the specific SSL VPN **gateway ID** to enter the SSL VPN gateway details page.
4. View details of the SSL VPN gateway.

Setting the Display Columns for VPN Gateway List

If you need to customize the display columns of the VPN gateway list, click the ⚙ next to the search box on the right, select the fields to display, and then click **OK**.

Search for the required CAM policy as needed, and click to complete policy association.

VPN Tunnel
Creating VPN Tunnel

Last updated: 2024-09-25 10:56:15

VPN Tunnel is a public network encrypted channel used in VPN Connections for transmitting data packets. Tencent Cloud's VPN Tunnel uses the Internet Key Exchange (IKE) protocol to establish sessions in IPsec. IKE features a self-protection mechanism that ensures secure identity authentication, key distribution, and IPsec session establishment over insecure networks. This document introduces how to create a VPN Tunnel through the "Console." You can also manage your VPN Tunnels via API or SDK. For details, refer to API Documentation. Establishing a VPN Tunnel involves the following configuration information:

- Basic Info
- Channel Mode
- IKE Configuration (optional)
- IPsec Configuration (optional)

Background

- Destination Routes
  This communication specifies which network segments within the IDC can communicate with the network of the VPN Gateway using the routing policy. After creating the tunnel, you need to configure the corresponding routing policy in the VPN Gateway's routing table. For details, refer to Create VPN Gateway Routes.
- SPD Policy.

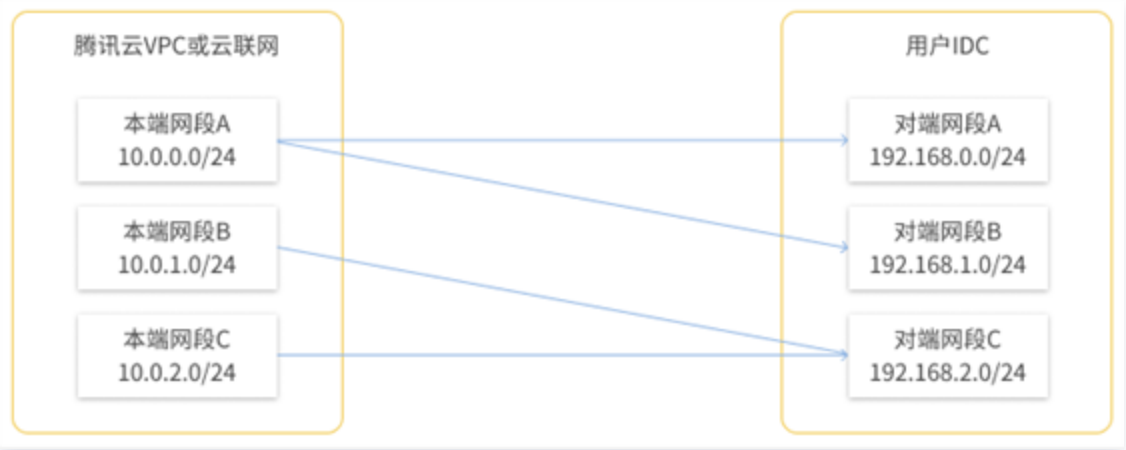
> **Note**
> - SPD (Security Policy Database) Policy consists of a series of SPD Rules and specifies which segments in the VPC or CCN can communicate with segments in the IDC. Each SPD Rule includes a Local Network Segment CIDR and at least one Remote Network Segment CIDR. One Local Network Segment CIDR and one Remote Network Segment CIDR form a matching pair. Multiple **Matches** can exist under one SPD Rule.
> - Tencent Cloud VPN gateway negotiates with the peer gateway device sequentially according to the **Matching Relationship**. You need to ensure that your peer gateway device supports negotiation based on the matching relationship, such as using the also keyword in StrongSwan configuration.
> - The maximum number of matching relationships formed by all SPD Rules under the same VPN gateway is **200**. Otherwise, it is recommended to use **Route-**

based VPN Connections.

- The matching relationships of the rules in all channels under the same VPN gateway cannot overlap, that is, in a group of matching relationships, the local IP range and the remote IP range cannot overlap at the same time.
- It is recommended that the **SPD policy configured in Tencent Cloud** should be symmetrical with the SPD policy configured in the peer gateway device. That is, in the SPD policy configuration in Tencent Cloud, the local network segment is `10.11.12.0/24`, and the remote network segment is `192.168.1.0/24`; in the SPD policy configuration of the peer gateway device, the local network segment is `192.168.1.0/24`, and the remote network segment is `10.11.12.0/24`.
- After configuring the SPD Policy, the VPN gateway will automatically push routes, and there is no need to add routes in the VPN gateway.

Example:

As shown in the figure below, the following SPD Rules already exist under a VPN gateway:



- SPD Rule 1: Local Network Segment is `10.0.0.0/24`, Peer Network Segment is `192.168.0.0/24`, `192.168.1.0/24`, with two matching relationships.
- SPD Rule 2: Local Network Segment is `10.0.1.0/24`, Peer Network Segment is `192.168.2.0/24`, with one matching relationship.
- SPD rule 3: Local network segment `10.0.2.0/24`, Peer network segment `192.168.2.0/24`, has a matching relationship.

Their matching relationships are respectively:

- `10.0.0.0/24` ----- `192.168.0.0/24`
- `10.0.0.0/24` ----- `192.168.1.0/24`
- `10.0.1.0/24` ----- `192.168.2.0/24`
- `10.0.2.0/24` ----- `192.168.2.0/24`

These four matching relationships cannot overlap with each other, i.e., their local network segments and peer network segments cannot overlap simultaneously.

- If a new matching relationship is added `10.0.0.0/24` ----- `192.168.1.0/24`, it cannot be added to the SPD rule due to the overlap with existing matching relationships.
- If a new matching relationship `10.0.1.0/24` ----- `192.168.1.0/24` is added and does not overlap with the existing 3 matching relationships, it can be added to the SPD rule.

Prerequisites

- Created VPN Gateway and Peer Gateway.
- Please ensure that your created VPN tunnels do not exceed the quota. Refer to Limits for adjusting the quota.

Operation Steps

1. Log in to the VPC console.
2. click **VPN Connections** in the left navigation bar > **VPN Tunnels** to enter the management page.
3. On the **VPN Tunnel** management page, click **New**.
4. In the **New VPN Tunnel** dialog, configure VPN tunnel Basic Information.

   4.1 **Basic Information Configuration**

   This step mainly configures the channel name, network, associated VPN gateway, peer gateway, shared key, negotiation type, communication mode, etc.

Parameter name	Description
Name of the channel	For defining the channel name, the character length is 60.
Region	The region of the VPN gateway associated with the VPN tunnel you want to create.
Network Type	The VPN gateway supports two types of networks: **VPC** and **CCN**. If you need to use the BGP feature, please choose **CCN**.
Virtual Private Cloud	Only when the VPN gateway type is VPC, you need to select the VPC to which the VPN gateway belongs. This parameter does not apply to CCN type.
VPN Gateway	Select the VPN gateway instance from the list.
Customer	Records the public IP for external access on the IDC side.

Gateway	Select the existing customer gateway instance. If not, you can click **New** to create one quickly.
Customer Gateway IP	The public IP address of the customer gateway.
Protocol Type	Default is IKE/IPsec.
Pre-shared Key	Used for identity authentication between the local and customer gateways. Both parties must use the same pre-shared key.
Negotiation Type	• Traffic Negotiation: After creating the tunnel, negotiation starts with the customer gateway when there is inbound traffic. • Proactive Negotiation: Initiate negotiation to the customer gateway after creating the tunnel. • Passive Negotiation: Wait for the customer gateway to initiate negotiation.
Communication Mode	Supports three types: Destination Routing, SPD Policy, and Dynamic BGP Routing. **Note:** • For static routing scenarios, it is recommended to use **Destination Routing**. Before using SPD Policy mode, you can first understand SPD Policy principles. • Dynamic BGP Routing is in canary release. To try it out, please submit a Ticket.
Customer Gateway ASN	Displays the IDC-side ASN configured in the customer gateway, which cannot be modified.
BGP Neighbor	BGP tunnel segment used for communication between the cloud and the customer side. This segment must be within the `169.254.128.0/17` range.
Cloud BGP	BGP IP address for interconnection between the cloud and the IDC side. Please avoid conflicts with the VPC segment and it is

Address	recommended to use the default allocated address.
Customer-side BGP Address	Automatically allocated address for customer-side BGP interconnection, which cannot be modified.
Tag	Tags mark VPN gateway resources so that these resources can be queried and managed efficiently. Tag is not a required configuration. You can decide whether to configure it according to your demand.

4.2 Advanced Configuration

This step mainly configures DPD Detection, health check, IKE, and IPSec.

Configure DPD Detection

Parameter name	Description
Enable DPD Detection	DPD Detection on/off switch, used to check if the other side is alive. It is enabled by default. The local side actively sends DPD request messages to the other side. If the response message is not received within the specified timeout period, it is considered that the other side is offline, and corresponding actions are taken after the timeout.
DPD Timeout	DPD overall detection timeout. Default is 30 seconds, range is 30 to 60 seconds.
DPD Timeout Actions	• Disconnect: Clear the current SA and break the current VPN tunnel. • Retry: Re-establish connection with the peer.

Health Check Configuration

Parameter name	Description
Enable Health Check	Health checks are used for primary and backup channel scenarios. For specifics, refer to Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery. If this does not apply to you, there is no need to enable this feature (disabled by default). Otherwise, enable this feature and configure the local and peer addresses for health checks below. For details, see Configuring Health Check. **Note:**

	Once you enable health checks and create the channel, the system will immediately start detecting the VPN tunnel health via NQA. If the VPN tunnel is not connected or the peer address you configured does not respond to NQA detection, the system will consider it unhealthy after multiple detection failures and will temporarily interrupt traffic until the VPN tunnel restores health.
Local Health Check Address	This parameter needs to be set only when the health check feature is enabled. You can use the IP address assigned by the system or specify one. **Note:** The specified address must not conflict with the VPC, CCN, or IDC private network address or segment, and must not conflict with the peer health check address. Multicast, broadcast, and local loop addresses cannot be used.
Peer Health Check Address	This parameter needs to be set only when the health check feature is enabled. You can use the IP address assigned by the system or specify one. **Note:** The specified address must not conflict with the VPC or CCN private network addresses or segments, and it must not conflict with the local health check address. Multicast, broadcast, and loopback addresses are not allowed.

IKE Configuration

Configuration Item	Description
Version	IKE V1,IKE V2.
Identity Authen	Default Pre-shared Key.

tication Method	
Encryption Algorithm	Supported encryption algorithms: AES-128, AES-192, AES-256, 3DES, DES, SM4. AES-128 is recommended.
Authentication Algorithm	Supported authentication algorithms: MD5, SHA1, SHA256, AES-383, SHA512, SM3. MD5 is recommended.
Negotiation Mode	Supports both main and aggressive modes. The difference is that aggressive mode can send more information with fewer packets, allowing quicker connection establishment, but it sends the security gateway identity in plain text. When using aggressive mode, parameters like Diffie-Hellman and PFS cannot be negotiated and require compatible configurations on both ends.
Local ID	Supports IP Address and FQDN (Fully Qualified Domain Name), with IP Address as the default.
Remote ID	Supports IP Address and FQDN, with IP Address as the default.
DH group	DH Group used for IKE key exchange. The security of the key exchange increases with the size of the DH Group, but the exchange time also increases. DH1: DH Group using 768-bit Modular Exponential (MODP) algorithm. DH2: DH Group using 1024-bit MODP Algorithm. DH5: DH Group using 1536-bit MODP Algorithm. DH14: DH Group using 2048-bit MODP Algorithm. Dynamic VPN does not support this option. DH24: DH Group using 2048-bit MODP Algorithm with a 256-bit prime order subgroup.
IKE SA Lifetime	Unit: seconds. Set the IKE Security Proposal's SA lifetime. Before the set lifetime expires, another SA is negotiated to replace the old SA. Until the new SA negotiation is complete, the old SA is still used. Once the new SA is established, it will be used immediately, and the old SA will be automatically cleared after the lifetime expires.

IPSec Information Configuration

Configuration Item	Description
Encryption Algorithm	Supported encryption algorithms: AES-128, AES-192, AES-256, 3DES, DES, SM4.
Authentication Algorithm	Supported authentication algorithms: MD5, SHA1, SHA256, SHA384, SHA512, SM3.
Message Encapsulation Mode	Tunnel.
Security Protocol	ESP.
PFS	Supports disable, DH-GROUP1, DH-GROUP2, DH-GROUP5, DH-GROUP14, and DH-GROUP24.
IPsec SA lifetime(s)	Unit: seconds.
IPsec SA lifetime(KB)	Unit: KB.

5. If advanced configuration is not needed, you can directly click **create**.

Viewing VPN Tunnels

Last updated: 2024-09-25 10:56:26

After the VPN tunnel is created, you can view the tunnel details on the VPN Tunnel management page.

Operation Steps

1. Log in to the VPC console.
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel** to enter the management page.
3. On the **VPN Tunnel** management page, click the tunnel instance to enter the VPN Tunnel details page.

- **Basic Info**

  The **Basic Info** tab displays information such as Name, Tunnel ID, Protocol Type, Network, Shared Key, Negotiation Type, DPD parameters, and Pass-through Mode.
- **Advanced Configuration Information**

  The **Advanced Information** tab displays IKE and IPSec related configuration information such as Encryption Algorithm, Authentication Algorithm, etc.

Configuring health check

Last updated: 2024-09-25 10:56:37

Tencent Cloud VPN Connections provides a complete solution to guarantee the high availability of your business. Not only the VPN gateway itself supports a high availability, but also primary/secondary tunnels are supported. The VPN gateway uses health check to identify the tunnel status and triggers the traffic switch between the primary and secondary tunnels based on their status. This document describes how to configure health check.

> **Note**
> We recommend you use a route-based tunnel for health check. If you use an SPD policy-based tunnel, you need to configure an SPD policy for `0.0.0.0/0`.

Health Check Principle

The monitoring check of the VPN tunnel uses the NQA mechanism and defaults to using Ping. The VPN gateway periodically uses the local address of the health check to Ping (encrypted within the tunnel) the peer address to determine its connectivity. After multiple consecutive Ping failures, the VPN gateway determines that the tunnel connectivity is abnormal and will switch the main channel traffic to the backup channel. At this time, the peer gateway also needs a similar mechanism to switch the traffic to the backup channel concurrently. Therefore, you need to configure or use the system to automatically allocate two IP addresses that can Ping each other within the tunnel for health checks. The subnets of these two addresses should not conflict with the VPC or IDC subnets.

Prerequisites

- Created VPN Gateway and Configured Peer Gateway, and the VPN gateway is version 3.0 or above.
- Business scenarios require primary and backup channels.
- You have planned health check addresses or use the addresses automatically assigned by the system.
- Health check has been enabled on the client side.

Configuring the Health Checks When Creating VPN Tunnels

This section only introduces the parameters for health checks. For other steps for creating a VPN tunnel, see Creating a VPN Tunnel.

1. Log in to the VPC console.
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel** to enter the management page.

3. In the **VPN Tunnel** management page, click **Create**.
4. In the pop-up **Create VPN Tunnel** dialog box, after completing the basic configuration, enable health check and configure the health check IP and NQA in **Advanced Configuration**.

> **Note:**
> - It is not recommended to modify the local address for health checks.
> - Avoid IP conflicts when modifying the peer address for health checks.

Parameters	Description
Health Check Local Address	It defaults to an IP within the range of `169.254.128.0/17`. You can also specify an available IP outside the VPC, but it must be outside the VPC range, within `224.0.0.0` to `239.255.255.255`, or `0.0.0.0`.
Health Check Remote Address	It defaults to an IP within the range of `169.254.128.0/17`. You can also specify an available on-premises IP.
ICMP	NQA.
Health Check Interval	Interval between two Tencent Cloud health checks. Range [1000ms, 5000ms], default 5000ms, unit ms.
Number of health checks	Number of route switches executed after a health check failure. Range of check counts [3, 8], default value 3.
Health check latency	Detection timeout time. Range [10ms – 5000ms], default value 150ms.

5. After configuring, click **Create**. The health check configuration takes effect immediately after the tunnel is created.

Configuring the Health Check After Creating VPN Tunnels

You can also configure health check on the VPN tunnel details page after the tunnel is created.

> **Note**

> After configuring the health check this way, your business may experience brief interruptions. We recommend using the first method.

1. Log in to the VPC console.
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel** to enter the management page.
3. In the **VPN Tunnels** management page, locate and click the target VPN tunnel instance, then click the specific instance name and click **Basic Information** tab, then click **Edit**.
4. Enable the health check and configure the relevant parameters.

> **Note:**
> - It is not recommended to modify the local address for health checks.
> - Avoid IP conflicts when modifying the health check remote address.

Parameters	Description
Health Check Local Address	It defaults to an IP within the range of `169.254.128.0/17`. You can also specify an available IP outside the VPC, but it must be outside the VPC range, within `224.0.0.0` to `239.255.255.255`, or `0.0.0.0`.
Health Check Remote Address	It defaults to an IP within the range of `169.254.128.0/17`. You can also specify an available on-premises IP.
ICMP	NQA.
Health Check Interval	Interval between two Tencent Cloud health checks. Range [1000ms, 5000ms], default 5000ms, unit ms.
Number of health checks	Number of route switches executed after a health check failure. Range of check counts [3, 8], default value 3.
Health check latency	Detection timeout time. Range [10ms – 5000ms], default value 150ms.

5. We recommend you select **Destination route** for the communication mode. If **Destination Route** is unavailable, we recommend you enter `0.0.0.0/0` for the local and peer IP ranges

in the SPD policy to ensure that the communication between the local and peer health check IPs is encrypted based on the VPN tunnel.

6. Click **OK**.

Generate Peer End Configuration

Last updated: 2024-09-25 10:57:24

After the local VPN tunnel is configured, you can generate a configuration file for your local VPN setup. After copying the content, you can directly configure your local VPN.

Prerequisites

A VPN tunnel has been created.

Operation Steps

1. log in to the VPN tunnel console and enter the management page.
2. On the "VPN Connections" management page, click **More** on the right side of the tunnel instance and select **Generate Peer End Configuration.**
3. In the pop-up **Channel Configuration** page, copy the configuration content and configure it locally according to your actual situation.

Viewing Tunnel Logs

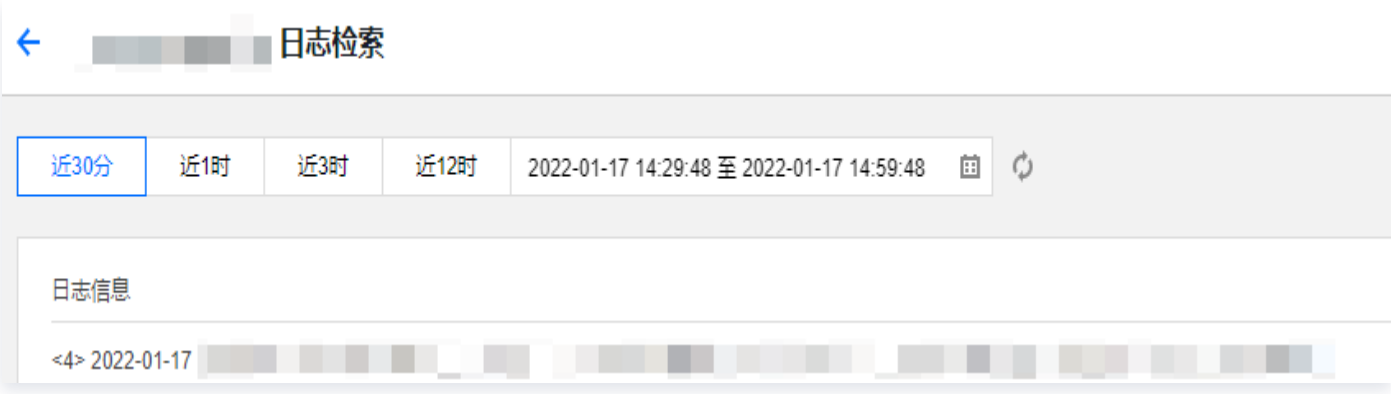
Last updated: 2024-09-25 10:57:39

You can query logs on the VPN tunnel management page and troubleshoot failures during the VPN tunnel connection according to the log information.

Directions

1. Log in to the VPC console.
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel** to enter the management page.
3. On the **VPN Tunnel** management page, click **More** on the right side of the channel instance > **Logs** to enter the log retrieval page.

4. On the **Log Retrieval** page, you can view log details and select logs from different time periods to view.



Modify a VPN tunnel

Last updated: 2024-09-25 10:57:52

After a VPN tunnel is created, you can modify the basic information of it, such as the tunnel name, pre-shared key, tag information, and SPD policy, as well as advanced configurations such as IKE configuration and IPsec configuration. You can also reset all the configurations of the VPN tunnel.

Systems impact

The reset operation will interrupt data transmission over the existing VPN tunnel and reestablish the connection. Please get ready for network change in advance.

Directions

1. Log in to the VPC console.
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel** to enter the management page.
3. On the "VPN Tunnel" management page, click the VPN tunnel instance ID that needs to be modified to enter the details page.
4. On the "Basic Information" page, click the edit icon in the picture to modify the VPN tunnel name, pre-shared password, tag information, and SPD policy rules. After modification, click **Confirm**.

   You can also modify the tunnel name and pre-shared key by clicking the edit icon on the VPN tunnel list page, as shown in the figure below.

5. Click the **Advanced Information** tab to modify the IKE Configuration and IPsec Configuration in **Advanced Information**. After modification, click **Confirm**.
6. Click **Reset** to reset all tunnel configurations. Please be aware of the risks and proceed with caution.


VPN通道
华南地区（广州）
全部私有网络
VPN 通道帮助文档
+新建
多个关键字用竖线"|"分隔，多个过滤标签用回车键分隔
ID/名称
监控
通道状态
健康状态
对端网关
所属网络
预共享密钥
操作
已联通
未联通
未联通
重置
更多
确认重置此VPN通道?
重置操作会中断现有vpn通道数据传输并重新建立连接，请提前做好网络变更准备。
重置
取消

Deleting a VPN Channel

Last updated: 2024-09-25 10:58:15

You can delete VPN tunnels that are no longer used.

Operation Steps

1. Log in to the VPC console.
2. In the left-side menu, click **VPN Connections** > **VPN Tunnel** to enter the management page.
3. On the "VPN Tunnel" management page, click **More** on the right side of the Channel instance > **Delete**.

4. In the confirmation dialog box, click **OK** to complete the operation.

Customer Gateway
Creating a Customer Gateway

Last updated：2024-09-25 11:01:24

The customer gateway records the IPsec VPN gateway IP address of the IDC, which is the other end of the VPN tunnel connection apart from the Tencent Cloud VPN gateway. This document explains how to create a customer gateway on the Tencent Cloud side.

Operation Steps

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **Customer Gateway** to enter the management page.
3. On the "Customer Gateway" management page, select the region and click **Create**.
4. Enter the name of the customer gateway and public IP. Public IP refers to the static public IP of the VPN gateway device of the customer IDC. Configure tags according to demand.

5. Click **Confirm** to complete. The created customer gateway is shown in the following figure.

Viewing Customer Gateways

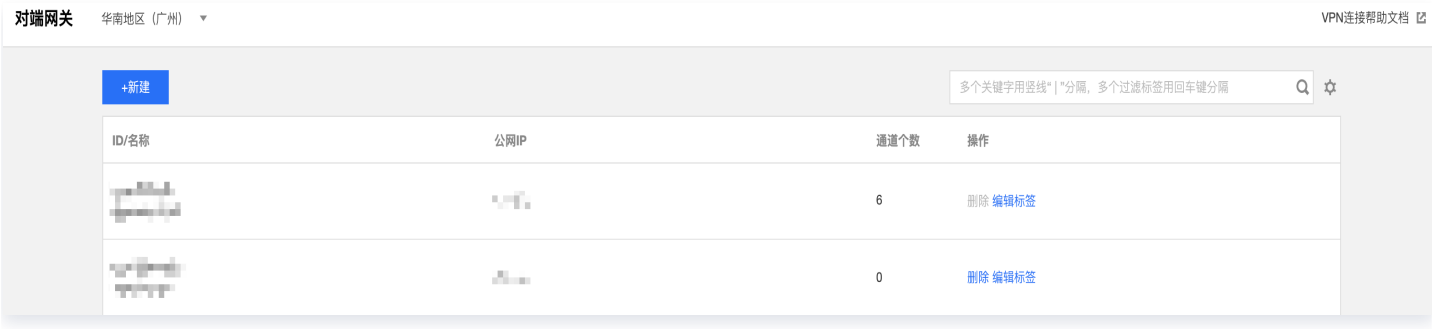
Last updated：2024-09-26 10:13:55

Follow the directions below to view details of the created customer gateways.

Directions.

1. Log in to the VPC console.
2. Click **VPN Connections** > **Peer Gateway** in the left directory to enter the Management Page. Search and view the required peer gateway information, including ID/Name, Public IP, Number of Channels, etc.

Search for the required CAM policy as needed, and click to complete policy association.



Modifying Customer Gateways

Last updated: 2024-09-26 10:15:17

After creating a customer gateway, you can modify its name.

Directions.

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **Customer Gateway** to enter the management page.
3. On the "Customer Gateway" management page, click the edit icon next to the customer gateway name to make modifications. After modifying, click **Confirm**.
4. Click **Edit Tag** on the right to edit the tag information.

Deleting a Customer Gateway

Last updated: 2024-09-26 10:15:29

If you do not use the customer gateway anymore and haven't created any VPN tunnels, you can delete the customer gateway.

Directions.

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **Customer Gateway** to enter the management page.
3. On the "Customer Gateway" management page, click **Delete** on the right side of the customer gateway instance to be deleted.
4. In the confirmation dialog box, click **OK** to complete the operation.

SSL VPN Server
Creating an SSL Server

Last updated: 2024-09-26 10:20:59

After creating the SSL VPN gateway, you need to create an SSL server on Tencent Cloud to provide SSL services for users.

Directions

1. Log in to the VPC console.
2. In the left sidebar, click **VPN Connections** > **SSL Server** to access the management page.

> **Note**
> A VPN gateway supports only one associated SSL server. For details, see Usage Limitations.

3. In the SSL server management page, click **New**.
4. In the pop-up **New SSL Server** dialog box, configure the following parameters.

> **Note**
> In a Windows system, if your OpenVPN client is version 3.4.0 or above, you need to configure encryption and authentication algorithms for the SSL server configuration, with the authentication algorithm supporting only SHA1.

Parameter name	Parameter Description
Name	Enter the SSL VPN server name (up to 60 characters).
Region	Display the region of the SSL VPN server.
VPN Gateway	Select an existing VPN gateway.
Cloud IP Range	The cloud network segment is the IP address range in the VPC to which your created VPN gateway belongs. Do not overlap with other segments.

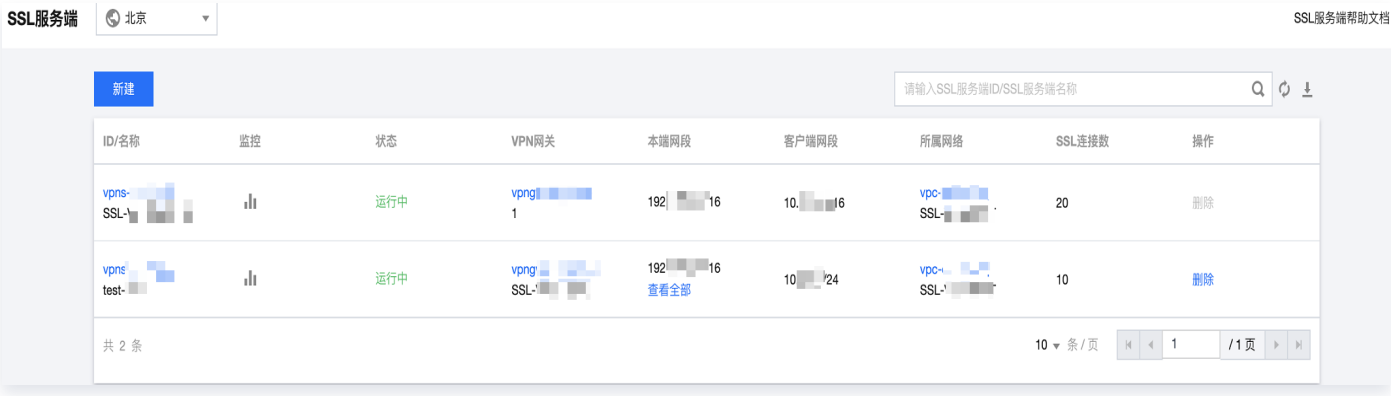
Client IP Range	The client subnet is the network segment allocated for client communication with the cloud. It must not overlap with the cloud network segment or your local network segment, and the address pool mask must be less than or equal to 24.
Protocol	Transmission protocol of the server.
Port	Enter the SSL VPN server port used for data forwarding.
Authentication Algorithm	Supported authentication algorithms: SHA1 and MD5.
Encryption Algorithm	Supported encryption algorithms: AES-128-CBC, AES-192-CBC, and AES-256-CBC.
Compressed	No.
Authentication Method	Certificate verification and Certificate verification + Identity verification are available. In this example, certificate verification is used. • Certificate verification: In this verification method, the SSL VPN server can be accessed through all SSL VPN client connections by default. • Certificate verification + Identity verification: In this verification method, only connections that are allowed by the access control policy can be established. You can configure the access control policy for specific user groups or all users. If you select this option, you must select an EIAM application.

5. After completing the Gateway settings, click **OK**.

Viewing the SSL VPN Server

Last updated：2024-09-26 10:22:16

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the Management Page.
   This page displays the SSL VPN server ID, name, status, VPN gateway, local network segment, client subnet, and other information.



3. Click the specific SSL **VPN server ID** to enter the SSL VPN Server Details Page. On this page, you can view the SSL VPN server's basic information and configuration information.

Deleting an SSL server

Last updated: 2024-09-26 10:25:20

You can delete the SSL VPN servers that are no longer used.

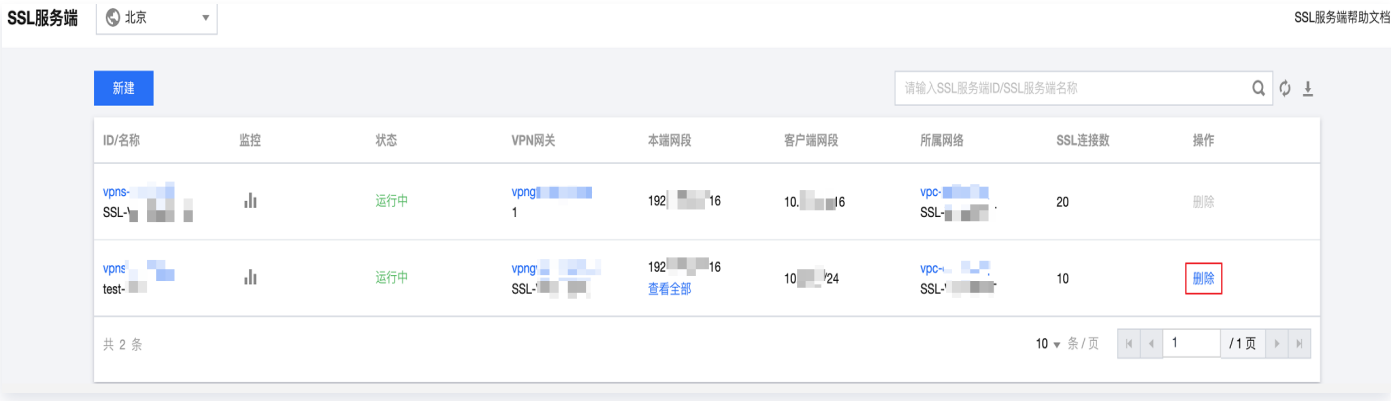
Prerequisites

The SSL VPN clients associated with the SSL VPN server have been deleted.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **SSL VPN Server** in the left directory to enter the admin page.
3. On the **SSL VPN Server** page, find the SSL server you need to delete, then click **Delete** in the action column, and click **Confirm** in the pop-up dialog.

> **Note**
> Note that all the associated connections will be immediately interrupted after the SSL VPN server is deleted.



Export SSL VPN server list

Last updated：2024-09-26 10:25:33

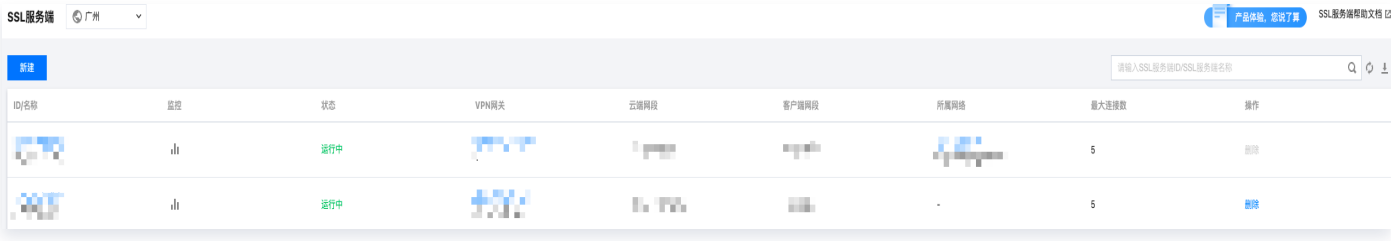
Once the SSL VPN server is created, if you need to export the SSL VPN server configuration information, you can perform this operation on the SSL VPN server. This document describes how to export the SSL VPN server configuration information.

Prerequisites

You've created an SSL VPN server.

Operation Steps

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the admin page.
3. On the SSL service management page, click the next to the search box to export.



SSO Authentication

Last updated: 2024-09-26 10:25:46

If you download the SSL VPN client configuration from the self-service portal, you can enable SSO authentication on the SSL VPN server.

> **Note**
> Currently, the SSO authentication feature is in beta testing. If you need it, please submit a ticket.

Prerequisites

- The Identity Provider has been applied for in CAM.
- The VPN version is 4.0.

Enabling the feature while creating an SSL VPN server

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the management page.
3. In the SSL server management page, click **New**.
4. In the pop-up **New SSL VPN Server** dialog box, select **authentication method** as **Certificate Authentication** + **Identity Authentication** and then select the EIAM application.

Parameter name	Parameter Description
Protocol	Transmission protocol of the server.
Port	Enter the SSL VPN server port used for data forwarding.
Authentication Algorithm	Supported authentication algorithms: SHA1 and MD5.
Encryption Algorithm	Supported encryption algorithms: AES-128-CBC, AES-192-CBC, and AES-256-CBC.

Compressed	No.
Authentication Method	• Certificate verification: In this verification method, the SSL VPN server can be accessed through all SSL VPN client connections by default. • Certificate Authentication + Identity Authentication: Use the CAM Identity Provider for SSO authentication. You need to select the created Identity Provider.
Identity Provider	The current Identity Provider is Tencent Cloud Certificate Authority M. For more details, see the Identity Provider user guide.
Access Control	SSL VPN Server access control switch.

5. **Access control** can be **enabled** as needed. For details, see Enable Access Control.

Enabling the feature after creating an SSL VPN server

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the management page.
3. In the SSL VPN Server management page, click the specific instance name.
4. On the instance details page, in the **Basic Information** tab, click **Edit** in the **Server Configuration** section.
5. Select **Authentication Method** as **Certificate Authentication** + **Identity Authentication**, choose a provider, and then click **Save**.

Enabling Access Control

Last updated: 2024-09-26 10:26:03

To guarantee your business security, SSL VPN provides the SSL VPN server access control feature, making your link more secure.

Prerequisites

An IdP has been created in the CAM Create an Identity Provider.

Must-Knows

- After enabling access control, you need to configure the corresponding access policy after the server is created, otherwise, the server will reject all connections.
- If you select **Certificate Authentication** as the authentication method, the SSL VPN server will accept all connections by default.

Enable access control when creating the SSL VPN server

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the management page.
3. In the SSL server management page, click **New**.
4. In the pop-up **New SSL VPN Server** dialog box, enable access control while enabling identity authentication and configure the relevant parameters.

> **Note:**
> If you enable access control, you need to configure the access control policy after the server is created, otherwise, the server will reject all connections.

Parameter name	Parameter Description
Authentication Method	• Certificate verification: In this verification method, the SSL VPN server can be accessed through all SSL VPN client connections by default. • Certificate Authentication + Identity Authentication: This authentication method only allows connections that are permitted by the access policy. You can configure the access policy for specific user groups or all users. After selecting this option, you need to choose the corresponding identity provider, currently, it is Tencent Cloud Certificate Authority M.
Identity Provider	The current Identity Provider is Tencent Cloud Certificate Authority M. For more details, see the Identity Provider user guide.

Enable access control after creating the SSL VPN server

> **Note:**
> If you enable access control, you need to configure the corresponding access policy after the server is created, otherwise, the server will reject all connections.

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the management page.

3. In the SSL VPN Server management page, click the specific instance name.
4. In the **Basic Information** tab on the instance details page, configure the authentication policy on the server.

Disabling Access Control

Last updated: 2024-09-26 10:26:17

> **Note:**
> If you disable access control, all access policies you have configured will be cleared, and the server will accept all connections by default.

Disable Access Control when creating the SSL VPN Server

1. Log in to the VPC console.
2. In the left sidebar, click **VPN Connections** > **SSL Server** to access the management page.
3. In the SSL server management page, click **New**.
4. In the popup **New SSL VPN Server** dialog, select **Access Control** as **Disabled** when configuring other parameters.
5. After configuring other parameters, please click **OK**.

Disable Access Control after creating the SSL VPN Server

1. Log in to the VPC console.
2. In the left sidebar, click **VPN Connections** > **SSL Server** to access the management page.
3. In the SSL VPN Server management page, click the specific instance name.
4. On the instance details page, in the **Basic Information** tab, disable **Access Control** in the **Server Configuration** section.

Configuring an access control policy

Last updated: 2024-09-26 10:26:33

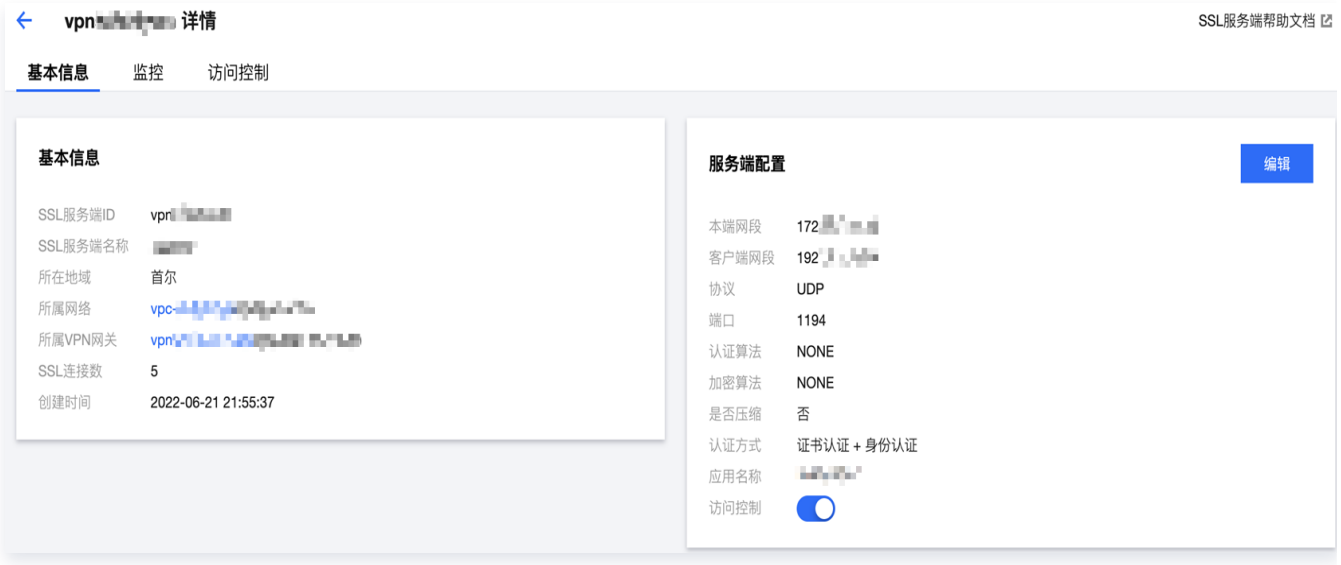
To guarantee your business security, SSL VPN provides the SSL VPN server access control feature for you to manage your SSL VPN servers in a fine-grained manner.

> **Note**
> Currently, only SSO authentication-enabled SSL VPN servers support the access control feature. For more information, see SSO Authentication.

Prerequisites

- An IdP has been created in CAM
- In the VPN Console, SSL server "certificate authentication + identity authentication" and access control have been enabled simultaneously.
  - Option 1. Enable the feature while creating an SSL VPN server.

  - Option 2: Enable the feature after creating an SSL VPN server.



> **Note**
>
> - If you select **certificate authentication** as the verification method, the SSL VPN server can be accessed through all client connections by default, that is, any client can connect to it.
> - If you enable access control, you need to configure the access policy after the SSL VPN server is created; otherwise, the server will reject all connections.

Configuring an access control policy

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the management page.
3. In the SSL VPN Server management page, click the specific instance name.

4. On the instance details page, click **Access Control**, and click **Add Policy**.

5. Configure the access control policy in the pop-up dialog box.

Parameter name	Parameter Description
Destination	Enter the local IP range, i.e., IP range for accessing the cloud. **Note:** The destination IP range needs to be in the same IP range as the local IP range. If you change the local IP range, you need to modify the destination address of the access control.
Access permission	• Specific User Group: This access control policy applies to the specified user group. After selecting this option, you need to configure the access group ID. • All Users: This access control policy applies to all users. **Note:** You can choose to configure the access policy for a specific user group or all users. The specific user group can come from the user group configuration in the Identity Authentication Platform.
Access group ID	The access group ID corresponds to the user group in the EIAM application and supports multi-selection. After selecting the access group ID, this access control policy will apply to the specified user group.

Remarks	Enter the policy remarks, which are required and make it easier for you to find the policy.

6. Click **OK**.
   After the configuration, the SSL VPN server will accept connections from users in the specified user group.

Delete Access Control Policy

> **Note**
> - After deleting the access control policy, clients in the user group specified in this policy will no longer be able to access the SSL VPN server.
> - If the Access Control Policy is Delete All, the SSL service will reject all client access by default. To allow access, you can configure additional access policies or change the authentication method to **Certificate authentication**.

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the management page.
3. On the SSL VPN server management page, click the specific instance name. Go to the **Access Control** tab and delete the corresponding policy.
   - Batch deletion: In the policy list, select the policies you want to delete, then click **Batch Deletion**.
   - Single deletion: In the action column of the policy you want to delete, click **Delete**.
4. In the pop-up dialog, click **OK**.

Editing an Access Control Policy

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL VPN Server** to enter the management page.
3. On the SSL VPN server management page, click the specific instance name. Go to the **Access Control** tab, locate the specific policy action column, and click **Editing**. Modify the relevant parameters according to your actual needs.

4. Click **OK**.

SSL VPN Client
Creating an SSL Client

Last updated: 2024-09-26 10:26:57

After creating the SSL VPN gateway and server, you need to create an SSL VPN client certificate on Tencent Cloud. This certificate records the information about the SSL certificate assigned by Tencent Cloud to the client, and is used for mutual authentication between the server and the mobile client. You can download the certificate to the mobile terminal and use it to communicate with Tencent Cloud through OpenVPN.

Operation Steps

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL Clients** to enter the management page.
3. In the SSL Client management page, click **New**.
4. In the pop-up **New SSL Client** dialog box, configure the following parameters.

Parameter name	Parameter Description
SSL VPN Server	Select the created SSL VPN server.

Region	Display the region of the SSL VPN server.
Mode	• Single creation: Users can directly create one SSL Client. • Batch creation: Download the **batch creation template**. After filling in the relevant parameters, click **Select Files** to upload.
Name	Enter the SSL VPN server name (up to 60 characters).

5. After configuring the SSL VPN client parameters, click **Create** to initiate the SSL client creation. When the **Status** becomes **Available**, the creation is complete.

Viewing SSL VPN Client

Last updated: 2024-09-26 10:27:09

You can view details of the created SSL VPN client on the SSL VPN client page.

Prerequisites

You've created an SSL Client.

Viewing SSL VPN Client

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL Clients** to enter the management page.\nThis page displays information such as the SSL Client ID, Name, connected SSL VPN Server, Certificate Effective Time, Certificate Expiry Time, Recent Connection Time, Last Connection Time, Client Private Network IP, Certificate Status, Enable Certificate Switch, and Operation Column.

   Click **SSL Server ID** to redirect to the connected SSL VPN Server and view the server information.

Deleting an SSL Client

Last updated: 2024-09-26 10:27:22

You can delete the SSL VPN client certificate on the SSL VPN client page.

> **Note:**
> Batch deletion of SSL Clients is only supported in VPN4.0.

Prerequisites

- You've created an SSL VPN server.
- You've created an SSL Client.

Deleting the SSL VPN Client Certificate

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL Clients** to enter the admin page.
   - Single Deletion: In the operation column of the instance to be deleted, click **Delete**
   - Batch Deletion: Select the instances to be deleted in bulk, and then click the **Delete** button above.

> **Note:**
> Note that all the associated connections will be immediately interrupted after the SSL VPN client certificate is deleted.

Downloading SSL VPN Client Configuration

Last updated: 2024-09-26 10:27:44

After successfully creating an SSL VPN client, you can download the client configuration for connecting to the SSL VPN server on the SSL VPN client management page. Two-way authentication will be performed when you use OpenVPN or a compatible VPN client to connect to the SSL VPN server through the downloaded client configuration. To guarantee your communication security, only after two-way authentication is passed can you access Tencent Cloud resources (such as CVM instances in a VPC) associated with the SSL VPN server gateway from the mobile client.

Downloading the SSL VPN Client Configuration as a Tenant Admin

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL Client** to enter the management page.
3. Download SSL Client Configuration.

- Single Download: Click **Download Configuration** on the row of the target SSL Client certificate instance, and select the download format in the pop-up dialog box.
- Batch Download: Select the instances to be downloaded, then click **Download Configuration** at the top, and choose the download format in the pop-up dialog box. You need to distribute the downloaded configuration files to users who need to connect to Tencent Cloud via SSL VPN Connections (e.g., your company employees). They must use this file to configure OpenVPN or a compatible VPN client to interconnect with the Tencent Cloud VPC. For detailed directions, see Mobile Configuration.

> **Note**
> Do not disclose the configuration file to unrelated personnel to prevent asset loss. If a configuration file is leaked, promptly disable the SSL Client. For details, see Disable SSL Client Certificates.

Downloading the SSL VPN Client Configuration on the Self-Service Portal

If identity verification is enabled when you create an SSL VPN server, the mobile client user (such as an employee in your company) can download the configuration file required by OpenVPN or a compatible VPN client on their own. In addition, Tencent Cloud uses an authentication mechanism to guarantee the security throughout the entire download process.

Prerequisites

- The tenant administrator has already created Identity and Access Management user groups, added the corresponding users and configured application permissions for the user groups. For detailed operations, please refer to the EIAM product documentation.
- The tenant admin has created an SSL Server in the VPN console, which supports identity authentication.
- The tenant admin has distributed the ID of the SSL VPN server with identity verification enabled to you (as a user). If you don't have the ID, contact your admin to get it.

Operation Steps

The following steps should be performed by the mobile terminal user (e.g., your company employees) on their own.

1. Log in to Tencent Cloud Client VPN Self-Service Portal.

> **Note**
> We recommend you use the latest version of Chrome.

1.1 Enter the previously distributed SSL server instance ID in the input box of the SSL Server ID row, then click **Next** to enter the log in to interface.

1.2 Perform identity verification.

Click  to perform SAML authentication, then click **Go to SAML for authentication** to log in. You need to use the authentication method specified by your tenant administrator. For example, the tenant administrator

- VPN 3.0 and 3.1 versions: If the tenant administrator specifies authentication by connecting to your enterprise account system in EIAM, you will see the domain account login page of your enterprise in the browser. Please enter your domain account for authentication. If the administrator specifies another method such as WeCom, you need to authenticate using the corresponding account.
- VPN 4.0 version: The identity verification relies on the CAM role configuration, supporting mainstream third-party IdPs based on SAML 2.0. For more details, please refer to the SSL VPN Access Control Guide (Okta)

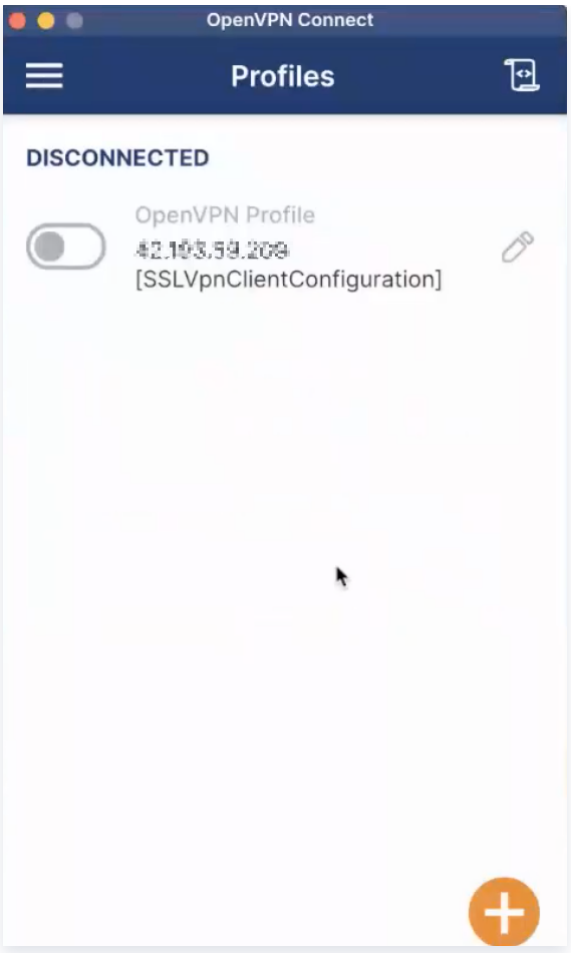
> **Note**
> EIAM is no longer maintained. Please use it with caution.

2. Download the SSL VPN client configuration file and client.

2.1 Find the SSL client configuration file you need to download in the **Download SSL Client Configuration File** section, click **Download**.

2.2 In the **Download SSL VPN client** section, find and download the appropriate SSL VPN client software. After downloading, please install the client.

3. After installing the SSL VPN client, upload the downloaded configuration file. Then, the client will automatically connect to the SSL VPN server.



Start, Stop, and Update SSL Client Certificates

Last updated: 2024-09-26 10:27:59

The SSL client certificates created in the SSL client are enabled by default. This article describes how to enable/disable certificates individually or in batches and update certificates.

Enabling the SSL VPN Client Certificate

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL Client** to enter the management page.
   - Enable Individually:
     - Option 1: In the row of the specific SSL client instance, click **Enable Certificate** > **OK**.
     - Option 2: Select a specific SSL client instance, click the top **Enable Certificate** > **OK**.
   - Enable in Batch: Select multiple SSL client instances, click the top **Enable Certificate** > **OK**.

Disabling the SSL VPN Client Certificate

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL Client** to enter the management page.
   - Disable Individually:
     - Option 1: In the row of the specific SSL client instance, click **Disable Certificate** > **OK**.
     - Option 2: Select a specific SSL client instance, click the top **Disable Certificate** > **OK**.

- Disable in Batch: Select multiple SSL client instances, click the top **Disable Certificate** > **OK**.

Updating SSL Client Certificates

> **Note:**
> - After updating the SSL client certificates, your business may be interrupted. Please perform the operation during off-peak business hours.
> - After updating the SSL client certificates, please download the SSL client certificates and locally replace the old certificates, then reconnect.

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **SSL Clients** to enter the admin page.
   - Disable Individually:
     - Method 1: In the action column of the SSL client instance row, click **Renew Certificate** > **OK**.
     - Method 2: Select a specific SSL client instance, click **Renew Certificate** at the top > **OK**.
   - Bulk Disable: Select multiple SSL client instances, click **Renew Certificate** at the top > **OK**.

Billing configuration
Monthly Subscription VPN Renewal

Last updated：2024-09-26 10:28:13

The Monthly Subscription VPN Gateway is a prepaid model. To avoid any impact on your business due to overdue payment of the VPN Gateway, please renew your VPN Gateway in a timely manner.

Directions

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. On the "VPN Gateway" page, click **More** in the action column on the right side of the VPN gateway instance you wish to renew > **Renew**.
4. In the pop-up renewal page, select the renewal period and click **OK** after confirming the details.

5. You can also click to enable the **auto-renewal** mode. If your account balance is sufficient, it will automatically renew for one month.

Switching from Annual and Monthly Subscription to Pay-as-You-Go

Last updated: 2024-09-26 10:28:41

Annual and monthly subscriptions are suitable for scenarios with stable bandwidth, while pay-as-you-go is more suitable for scenarios with significant bandwidth fluctuations. If you wish to change the billing mode to metered billing, refer to the following steps.

Must-Knows

- Only the annual and monthly subscription billing mode can be converted to pay-as-you-go. Once switched to pay-as-you-go, it cannot revert back to the annual and monthly subscription billing mode.
- The conversion from annual and monthly subscription to pay-as-you-go will take effect after the current gateway expires.

Operation Steps

1. Log in to the VPC console.
2. Click **VPN Connections** > **VPN Gateway** in the left directory to enter the admin page.
3. On the "VPN Gateway" management page, click **more** in the operation column on the right side of the VPN Gateway that needs to be switched to pay-as-you-go > **Switch to Pay-as-You-Go**.

4. Please carefully read the following notes. After confirming that everything is correct, click **OK** to complete the operation.

Binding an Anti-DDoS Instance

Last updated: 2024-09-26 10:29:00

Anti-DDoS New Version

For configuration guidance on the new version of Anti-DDoS, please refer to DDoS Protection Pack.

Anti-DDoS Legacy Version

1. Log in to Anti-DDoS Management Console, select **Legacy** > **Anti-DDoS Pro** > **Asset List**, and choose the region.
   - If your Anti-DDoS Pro instance is a single IP instance, select the **Single IP instance** tab.
   - If your Anti-DDoS Pro instance is a shared package, select the **Shared package** tab.
2. Find the Anti-DDoS Pro instance you need to bind in the list, click **Bind Device** in the action column of that instance.
3. In the pop-up box, select the type of associated device and the associated machine. Choose **VPN Gateway** as the associated device type and select the VPN gateway you need to associate from the list.
4. After selecting, click **OK**.

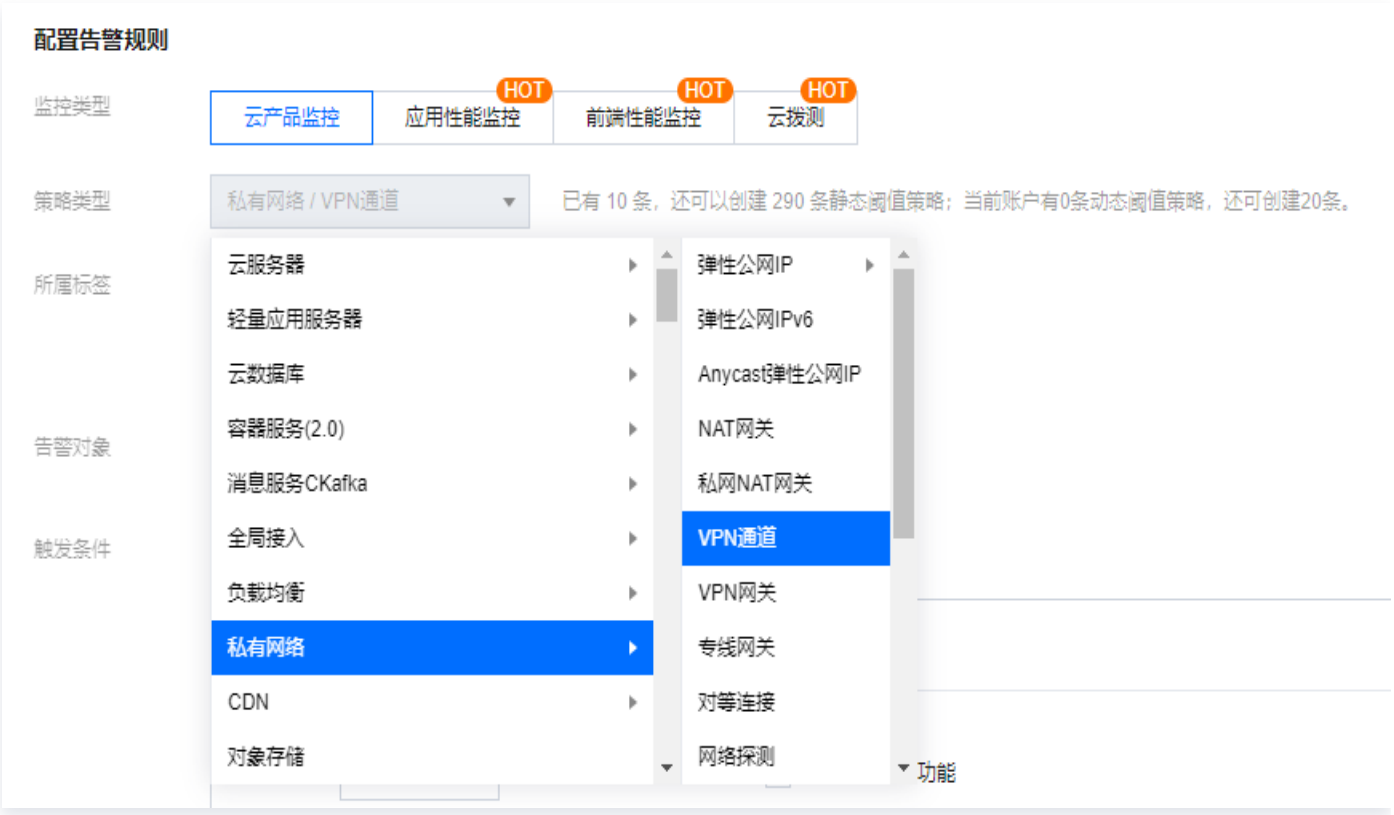
Configuring Alarm Policies Setting Alarms

Last updated: 2024-09-26 10:29:38

You can customize traffic alarms for VPN connections. When a metric value exceeds its threshold, alarm notifications are sent to you automatically via email and SMS. Alarm services are free of charge, helping you quickly locate problems.

Operation Steps

1. Log in to TCOP Console.
2. Click **Alert Management** > **Policy Management** in the left-side menu to enter the management page, then click **New Policy**.
3. Fill in the alarm policy name, choose the policy type as **VPC** > **VPN Tunnel**, select **Alert Object**, set the **Trigger Condition**, then click **Next: Configure Alarm Notification**.



Configuration Type	Configuration Item	Description
Alarm Rule	Alarm Object	• If you select Instance ID, the alarm policy will be associated with the selected instance.

Configuration		• If you select the instance group, the alarm policy will be associated with the selected instance group. • If you select all objects, the alarm policy will be associated with all instances under the current account.
	Trigger Condition	An alarm trigger condition is a semantic condition composed of metrics, comparative relationship, threshold, statistical granularity, and lasting N monitoring data points. You can set the metrics and event alert trigger conditions according to your business needs, configuring alert metrics, statistical granularity, alert thresholds, alert classification, and alert frequency. You can also directly use the trigger condition templates and predefined trigger conditions. Refer to Configure Alarm Trigger Condition.
Alarm Notification Configuration	Using alarm notification template	Support selecting system preset notification templates and user-defined notification templates. Each alarm policy can bind up to three notification templates. Refer to Alarm Notification.

4. On the **Configure Alarm Notification** page, select **Notification Template**, then click **Finish**
5. View alarm information
   When the alarm condition is triggered, you will receive an alarm notification through the selected alert channels (SMS/Email/WeChat, etc.). You can also click **Alert History** in the left-side menu to view. For more alarm-related information, refer to Alarm Configuration.

Viewing Monitoring Data

Last updated: 2024-09-26 10:30:01

With VPN tunnels and VPN gateways, you can view monitoring data, and quickly locate failures if they occur. The monitoring service is free of additional charges.

VPN Gateway

1. Log in to the VPC console.
2. Click **VPN Connections** in the left navigation bar > **VPN Gateway**.
3. Select the region and VPC, click in the VPN Gateway monitoring column you want to view in the list to see the monitoring data. You can also click the gateway ID to enter the details page and view it on the **SNAT Monitoring** tab.

VPN Tunnel

1. Log in to the VPC console.
2. Click **VPN Connections** in the left navigation bar > **VPN Tunnel**.
3. Select the region and VPC, click in the VPN Tunnel monitoring column you want to view in the list to see the monitoring data.

Reference

- VPN Gateway Monitoring Metrics
- VPN Tunnel Monitoring Metrics