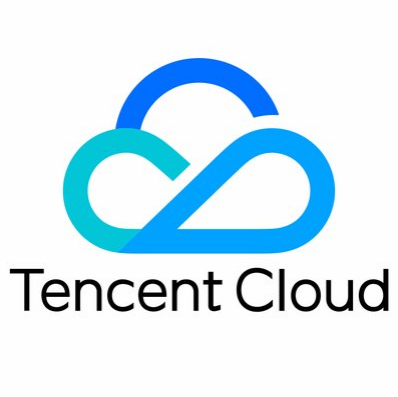
VPN Connections

Practice Tutorial



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

- Practice Tutorial
  - IPsec VPN
    - Resolve IDC and Cloud Resource IP Conflicts with VPN + CCN + NAT
    - Hybrid Cloud Primary/Backup Redundant Communication via DC (BGP Route) and VPN Connections (Static Route) (Automatic Switching)
    - Hybrid Cloud Primary/Secondary Communication (DC and VPN)
    - Connecting IDC to CCN
    - Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery
    - Dedicated private network traffic achieves encrypted communication through the Private Network VPN Gateway
      - Solution Overview
      - Dedicated private network traffic is encrypted through the Private Network VPN Gateway
    - Establishing a VPN Connection between Tencent Cloud and AzureChina
    - Connecting IDC with Cloud Resources (Dynamic BGP)
    - Local Gateway Configurations
      - Huawei Firewall Configuration
      - Hillstone Networks Firewall Configuration
      - Juniper Firewall Configuration
      - NSFOCUS Firewall Configuration
      - Configuring a Cisco Firewall
  - SSL VPN
    - SSL VPN Access Control Practice Guidelines (Okta)
    - Connecting Client to VPC

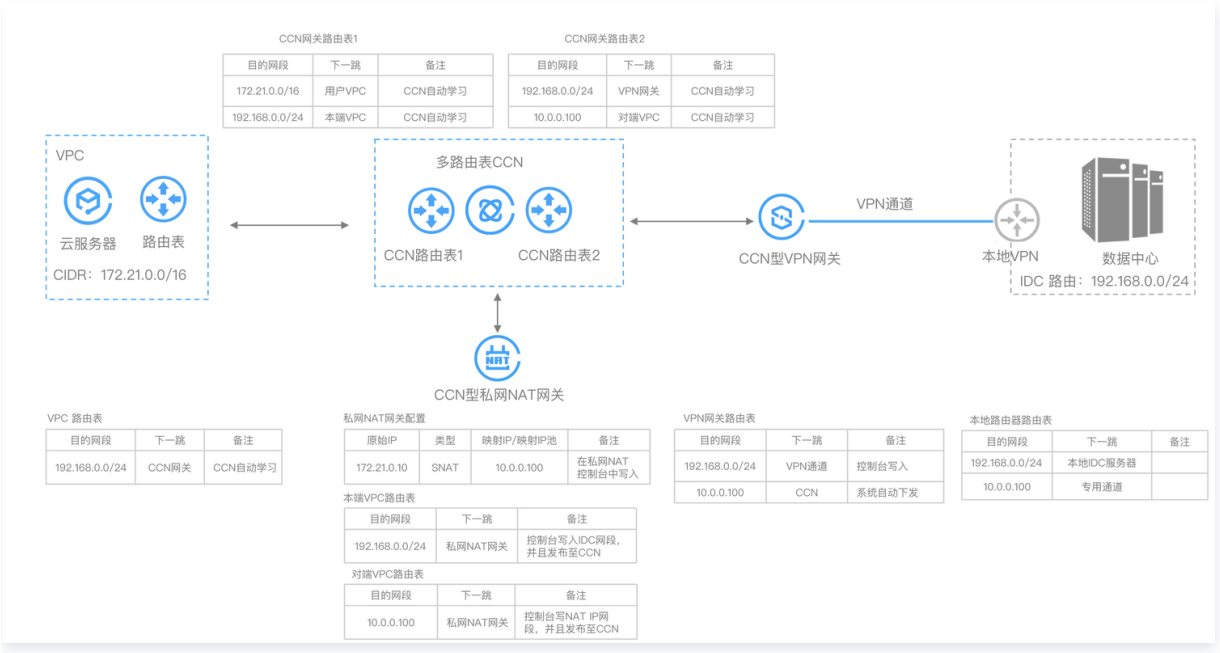
Practice Tutorial
IPsec VPN
Resolve IDC and Cloud Resource IP Conflicts with VPN + CCN + NAT

Last updated: 2024-09-26 10:31:36

Using VPN to connect IDC/third-party clouds and Tencent Cloud for resource access often causes IP conflicts. Replanning IP ranges is time-consuming and labor-intensive. This article guides you through solving these issues using VPN + CCN multiple route tables + Private NAT Gateway.

Business Scenario

Users can use VPN to connect Tencent Cloud with remote IDCs/third-party clouds for resource access, specifying IP addresses without conflicts via a Private Network VPN + NAT + CCN solution.



Operating Procedures

1. Create a CCN instance that supports multiple route tables and bind it to a VPC instance.
2. Create a CCN-type Private Network NAT instance and complete the rule settings.
3. Configure local/remote VPC routes and publish to CCN.
4. Configure NAT IP mapping rules.
5. Create a CCN-type VPN Gateway and its resources, and associate it with the CCN instance.

Prerequisites

- CCN multiple route tables feature enabled. To activate, please Submit a Ticket.
- Private Network NAT Gateway feature enabled. To activate, please Submit a Ticket.

Operation Steps

Step 1: create a CCN instance and associate it with your business VPC

1. Log in to the CCN console, click **Create**, and associate it with the business VPC. For details, refer to Creating a CCN Instance.

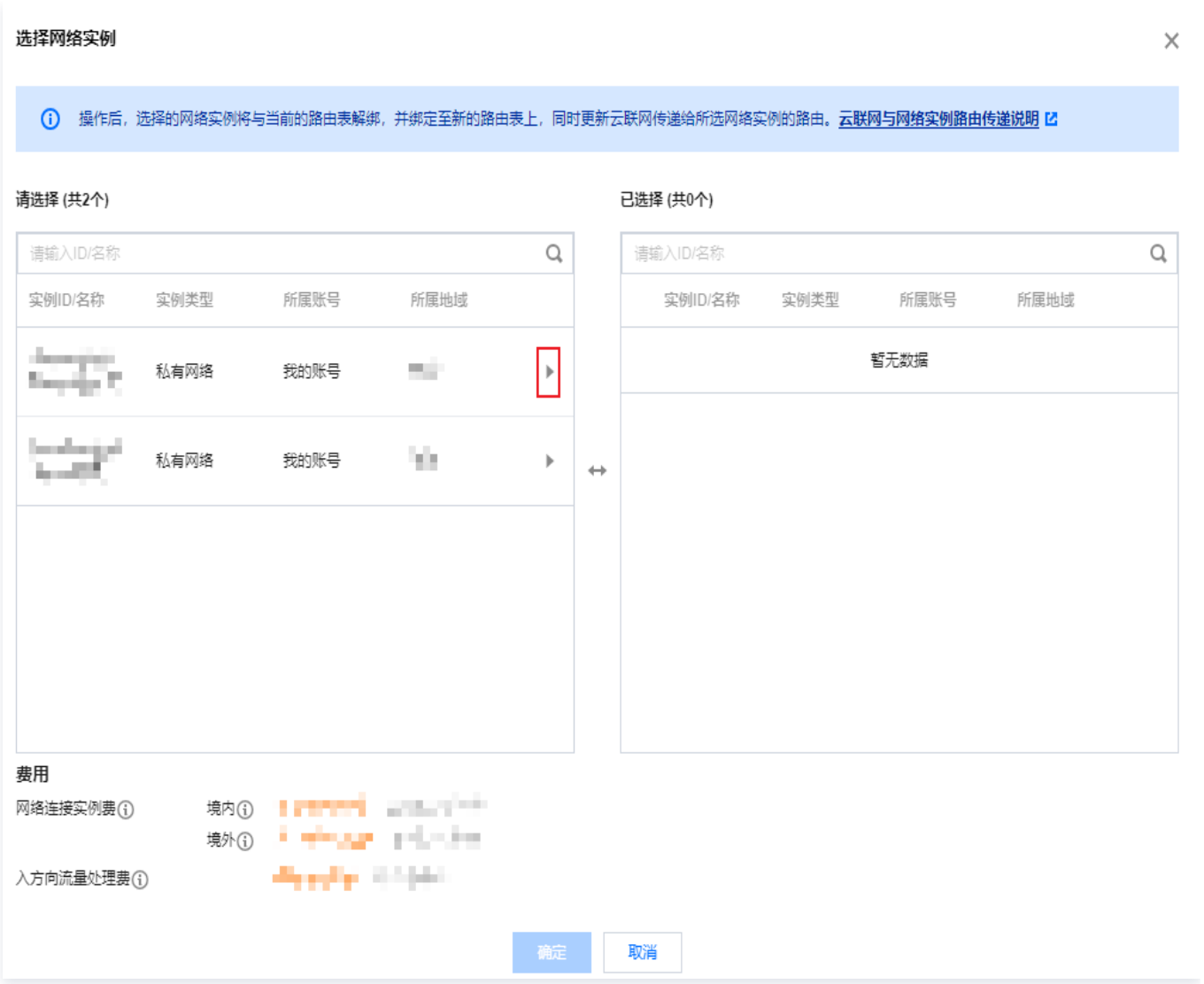
2. In the CCN instance list page, click the created **CCN ID**, then on the CCN instance details page, go to the **Route Table** tab, and click **Create Route Table** to create two CCN route tables.

> **Note**
> Ensure you have enabled the CCN multiple route table feature. If not, please Submit a Ticket to activate.

3. Add the business VPC to the CCN network route table 1.

3.1 In the left-side CCN route table list, select route table 1, and click **Bind Instance** to bind the business VPC instance.

3.2 In the **Bind Instance** tab, click **Bind Network Instance**, then on the **Select Network Instance** page, select the business VPC instance and click **OK**.



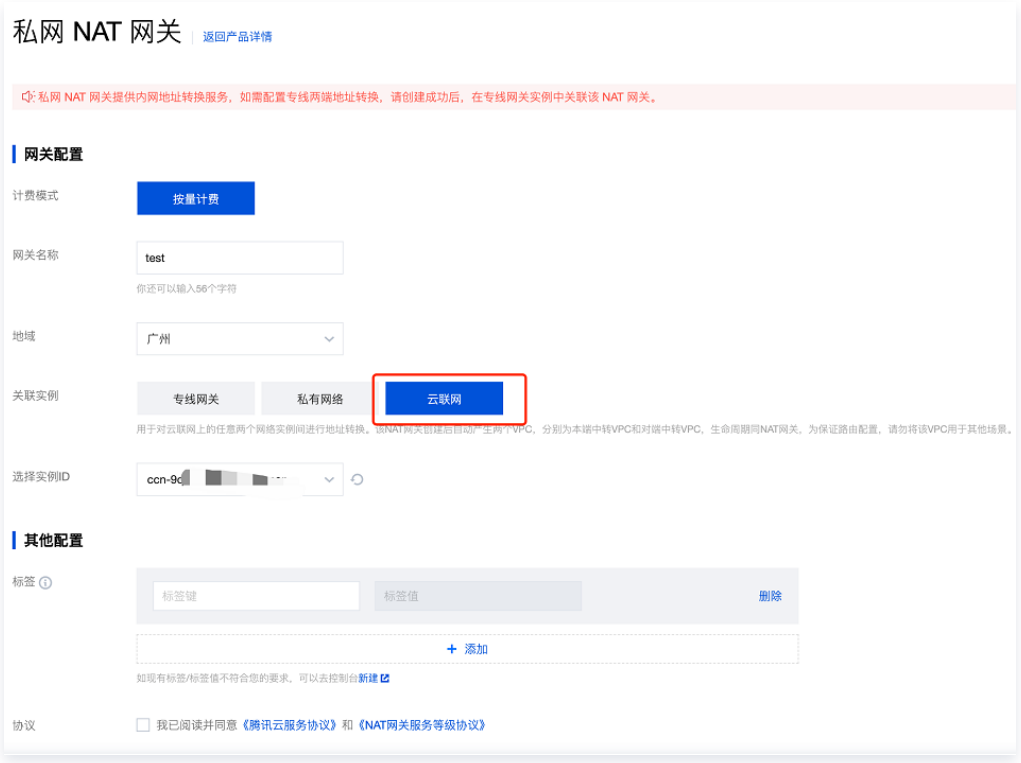
Added as follows:

Step 2: Create a CCN-type Private Network NAT and add it to the CCN multiple route tables.

In this step, you need to create a CCN-type Private Network NAT instance on the NAT side and associate the VPC attached to the Private Network NAT with the CCN multiple route tables.

1. Log in to the Private Network NAT Gateway Console, select the region and VPC at the top of the page, then click **Create**.
2. Complete the creation on the Private Network NAT purchase page following the interface prompts. Once created successfully, the local VPC instance and the remote VPC instance will be displayed automatically.

> **Note**
> Ensure that the Private Network NAT feature is enabled. If not, please Submit a Ticket to activate.



3. In the CCN Console, find the CCN instance created in Step 1, and on its details page, go to the **Route Table** tab, bind the local VPC of the NAT instance to route table 1 of the CCN instance.

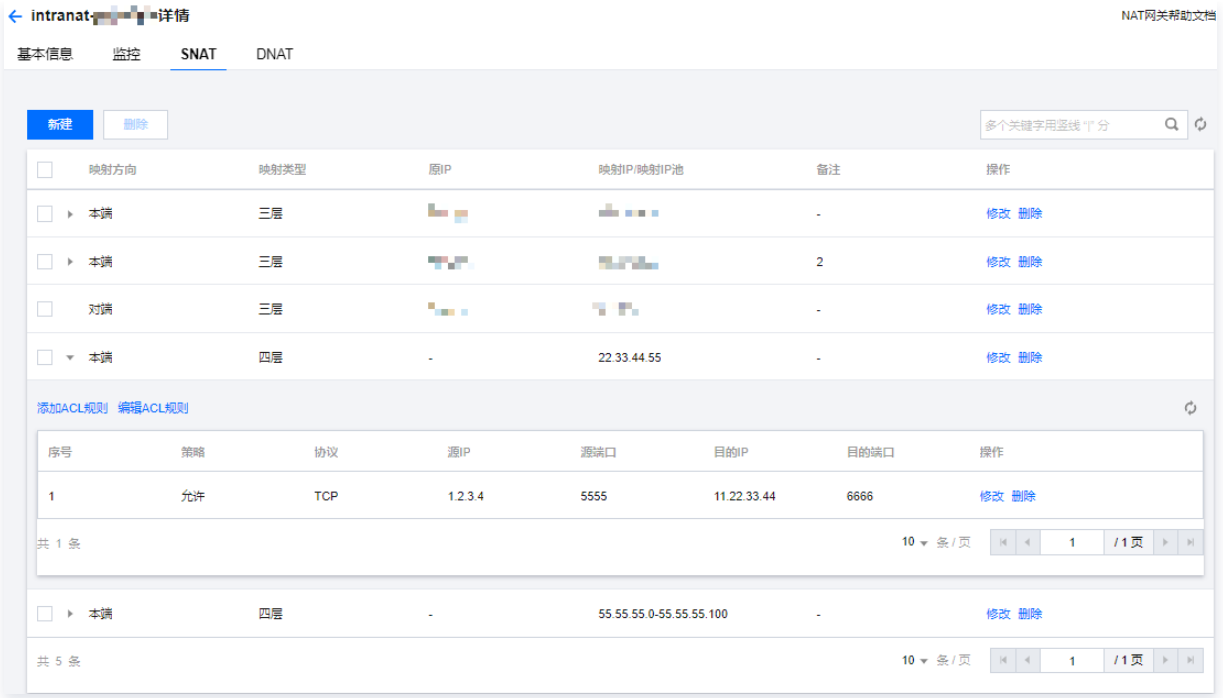
4. Set the route reception policy in CCN route table 1. For details, refer to Step 1, Step 3.

5. Similarly, bind the remote VPC of the NAT instance to route table 2 of the CCN instance and configure the route reception policy.

Step 3: Configure IP Mapping Rules

1. On the Private Network NAT Gateway instance details page, click the private network NAT instance ID created in Step 2, then on its details page click **SNAT**.
2. On the SNAT tab, click **Create** and follow the interface prompts to configure. Here we use the local Layer 4 rule as an example.

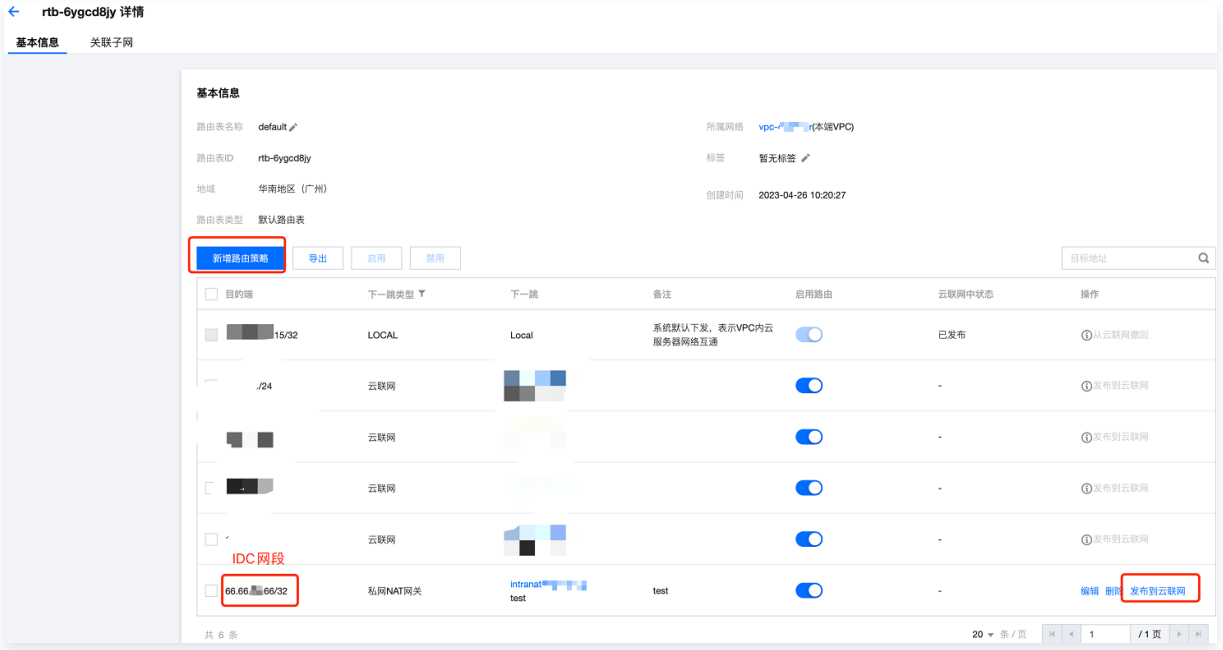
> **Note:**
> When the mapping type is Layer 4, you must configure and add ACL rules. For details, refer to Rule Overview or submit a ticket for consultation.



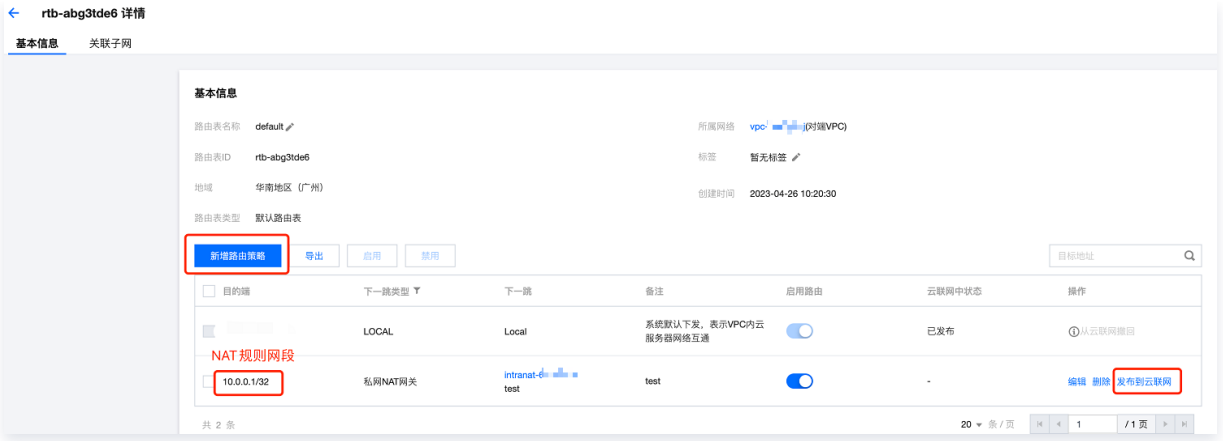
Step 4: Configure and publish VPC routing policies to CCN

In this step, you need to configure local/remote VPC routes on the VPC side and publish them to CCN.

1. Log in to the VPC Console, find the business VPC and click **VPC Instances**.
2. On the VPC instance details page, click **Route Table**, then on the basic information page of the default route table of the local VPC, click Add Routing Policy.
3. On the Add Route page, configure the destination end as the IDC network segment, the next hop type as Private Network NAT Gateway, and publish it to CCN.



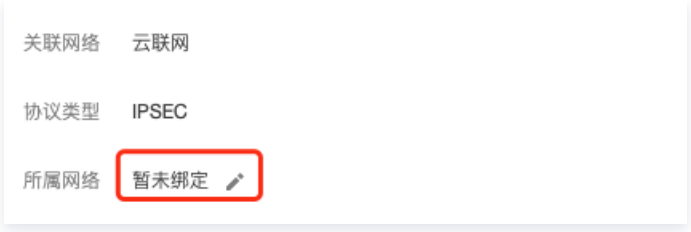
4. Similarly, add an entry to the default route table of the remote VPC as follows: the destination end is the NAT rule mapped IP route created in Step 3's Step 2, the next hop is Private Network NAT Gateway, then publish it to CCN.



Step 5: Create a CCN-type VPN gateway and its resources, and associate them with multiple CCN route tables.

1. Log in to VPC Console, in the left sidebar, click **VPN Connections** > **VPN Gateway**. After selecting the region and VPC, click **New**. For the associated network, choose "CCN". Follow the interface prompts to complete the creation of a CCN-type VPN Gateway. For detailed operations, refer to Creating a VPN Gateway.

2. In the VPN Gateway details page, bind the CCN instance created in Step 1.



3. In the CCN Instance > Route Table tab, add the VPN Gateway to the CCN Route Table 2, bind the VPN Gateway instance, and set up the route reception policy. For detailed steps, refer to Step 1's Step 3.
4. In the VPN side, create a Customer Gateway and create a VPN tunnel.
5. (Optional) Publish the route to CCN. Only if the VPN tunnel is SPD Policy-based, the routes need to be manually published to CCN in the VPN Gateway.
6. On the user IDC side, configure the firewall or local VPN.

Hybrid Cloud Primary/Backup Redundant Communication via DC (BGP Route) and VPN Connections (Static Route) (Automatic Switching)

Last updated: 2024-09-26 10:31:59

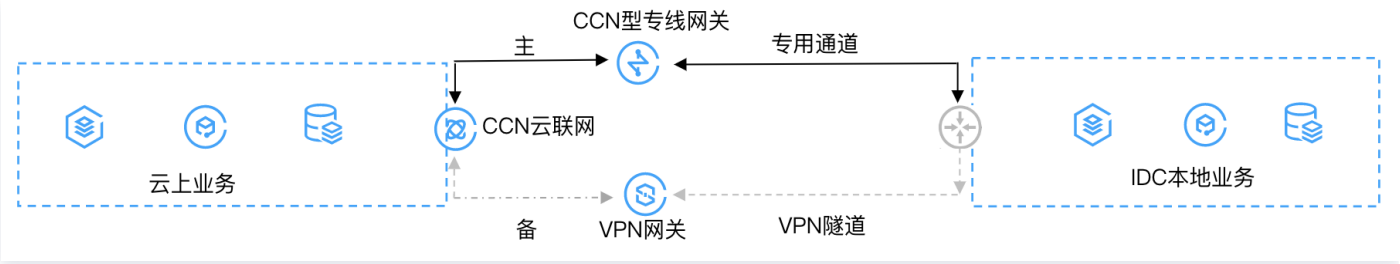
If your business is deployed in both a local data center and a Tencent Cloud VPC, you can connect them via DC or VPN Connections for intercommunication. To enhance business high-availability, you can set up both DC and VPN Connections services, with CCN configuring both links as primary and backup, achieving redundant communication.

> **Note:**
> When configuring primary and backup routes, the subnet mask length of the dedicated line should be greater than the subnet mask length of the VPN.

Business Scenario

As shown in the picture below, to achieve interaction between on-cloud and off-cloud businesses, you need to deploy network connection services for intercommunication. To achieve high-availability communication with automatic switching during failures, the deployment plan is as follows:

- DC (primary link): The local IDC connects to a CCN-type dedicated gateway through a physical dedicated line, achieving communication between the on-cloud and off-cloud businesses. When the physical dedicated line link is normal, all communication traffic between the IDC and the VPC is forwarded through the dedicated line.
- VPN Connections (backup link): The local IDC achieves communication with the Tencent Cloud VPC by establishing a CCN-type VPN secure tunnel. When the dedicated line link fails, traffic is automatically switched to this link, ensuring business availability.



Prerequisites

- Your local IDC gateway device should support the IPsec VPN feature and can act as a customer VPN gateway to establish an IPsec tunnel with the cloud-side VPN device.
- A CCN instance has been created, with ECMP and route overlapping features enabled.
- Dynamic BGP transmission feature has been enabled on the dedicated line side. For details, please contact online support.

Network Planning

Configuration Item			Sample value
Network Configurati	VPC information	Subnet CIDR block	192.168.1.0/24

on		Public IP of the VPN gateway	203.xx.xx.82
	IDC information	Subnet CIDR block	10.0.1.0/24
		Public IP of the gateway	202.xx.xx.5

Operation Steps

Step 1: Configure IDC to connect to the cloud via DC

1. Log in to DC Console, click Physical Dedicated Line in the left navigation bar, click **New**, create a physical dedicated line. For details, refer to Applying for Connection.
2. Click Dedicated Line Gateway in the left navigation bar, click **New**, create a CCN Type Dedicated Line Gateway. After creation, publish the segment pointing to CCN in its details (click Enable Auto Propagation). For detailed operations, refer to Creating Dedicated Line Gateway, Publish Network Segment to Cloud Connect Network.
3. Click **Dedicated Tunnels** > **Exclusive Virtual Interface** in the left navigation bar, click **New**, create an exclusive private channel. Here, you need to configure the channel name, select the dedicated line type, the created dedicated line gateway, Tencent Cloud's and the user's interconnect IP, choose the static routing mode, fill in the IDC communication segment, etc. After configuration, download the configuration guide and complete it on the IDC equipment. For detailed operations, refer to Exclusive Private Channel.

> **Note:**
> - For more detailed configurations, refer to Migrating IDC to the Cloud Through CCN.
> - To achieve physical dedicated line fault awareness and route auto-convergence, enable route health check.

Step 2: Connect IDC to VPC through a VPN connection

1. Log in to VPN Gateway Console, click **New**, create a CCN Type VPN Gateway. For details, refer to Creating VPN Gateway. After creation, associate the CCN instance in its details page. For detailed operations, refer to Associating CCN Instance.
2. Click Peer Gateway on the left navigation bar, configure the peer gateway (i.e., the logical object of the IDC side VPN gateway), and fill in the public IP address of the IDC side VPN gateway, such as 202.xx.xx.5. For detailed operations, refer to Creating Peer Gateway.
3. Click VPN Tunnel on the left navigation bar, click **New**, and create the VPN tunnel following the page guide to configure SPD policy, IKE, IPsec, and other parameters. For detailed configurations, refer to Creating VPN Tunnel. Configure the VPN tunnel information on the IDC local gateway device, ensuring the configuration matches the VPN tunnel information in Step 3, otherwise, the VPN tunnel will not connect properly.
4. In the route table tab of the gateway, configure routes pointing to the peer gateway (make sure the VPN routes are aggregate routes).

> **Note:**
> - For more detailed configuration, please refer to Establishing a Connection from IDC to CCN.
> - Ensure VPN routes are aggregate routes, e.g., a Direct Connect gateway passing the IDC side routes 10.0.1.0/25 10.0.1.128/25 to CCN, and the VPN passing the IDC side route 10.0.1.0/24 to CCN.

Step 3: Configure an alarm policy

You can configure an alarm policy for linkages. When a linkage has an exception, alarm notifications are sent to you automatically via emails and SMS message, alerting you of the risks in advance.

1. Log in to the TCOP Alarm Policy Console.
2. Click **New**, fill in the policy name, select VPC / Network Detection for the policy type, choose a specific network detection instance as the alarm object, set up trigger conditions and alarm notifications, etc., and click **Finish** to complete.

Step 4: Switch between primary and secondary routes

When an exception alarm is received for the network probing of Direct Connect Gateway's primary path, your traffic will automatically be switched to the backup route of the VPN gateway.

Hybrid Cloud Primary/Secondary Communication (DC and VPN)

Last updated: 2024-09-26 10:32:36

If your business is deployed in both a local IDC and a Tencent Cloud VPC, you can connect them via Direct Connect or VPN. To improve the business availability, you set up both DC and VPN connections and configure them as the primary and secondary linkage for redundant communication. This document guides you through how to configure the DC and VPN connection as primary/secondary linkages to connect your IDC to the cloud.

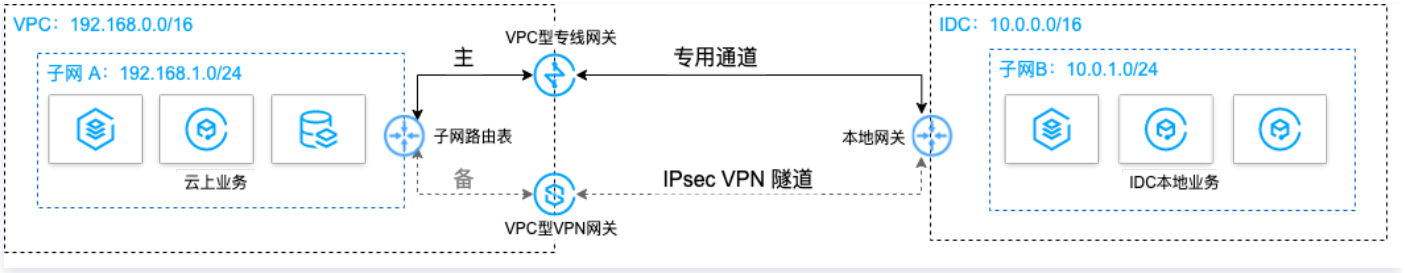
Note

- The route priority feature is currently in beta testing. If needed, please contact support online.
- The next hop type determines the route priority in the VPC route table. The default route priority sequence from high to low is CCN, direct connect gateway, VPN gateway, and others.
- Currently, the route priority cannot be adjusted in the console. If you want to adjust the route priority, please contact support online.
- Currently, automatic switching is not supported. When a fault occurs, you must manually switch the route in the VPC.

Business Scenario

You have deployed businesses in a Tencent Cloud VPC and an IDC. To interconnect them, you need to configure network connection services for high-availability communications as follows:

- Direct Connect (primary): connects the local IDC to a VPC-based direct connect gateway through a connection. When the connection linkage is normal, all data traffic between the IDC and the VPC is forwarded through the connection.
- VPN connection (secondary): establishes an IPsec VPN tunnel to interconnect the local IDC and the Tencent Cloud VPC. When the connection linkage fails, traffic will be forwarded using this linkage to ensure the business availability.



Prerequisites

- Your local IDC gateway device should support the IPsec VPN feature and can act as a customer gateway to create a VPN tunnel with the VPN gateway.
- The IDC gateway device has configured with a static IP address.
- Data preparation as follows:

Configuration Item			Sample value
Network Configuration	VPC information	Subnet CIDR block	192.168.1.0/24
		Public IP of the VPN gateway	203.xx.xx.82

	IDC information	Subnet CIDR block	10.0.1.0/24
		Public IP of the gateway	202.xx.xx.5

Directions

1. Configure IDC to VPC through DC
2. Configure IDC to VPC through a VPN connection
3. Configure network probes
4. Configure an alarm policy
5. Switch between primary and secondary routes

Directions

Step 1: Connect IDC to VPC through Direct Connect

1. Log in to the DC Console, click **Physical Dedicated Line** on the left sidebar to create a connection.
2. Click **Direct Connect Gateway** on the left sidebar to create a Direct Connect Gateway. In this case, we choose to connect to the VPC with a standard Direct Connect Gateway. If the IDC and VPC IP ranges conflict, you can also choose the NAT type.
3. Click **Exclusive Private Channel** on the left sidebar to create a dedicated channel. Here, you need to configure the channel name, choose the type of direct connection, the created Direct Connect Gateway, interconnect IPs on both Tencent Cloud and user sides, select static routing, enter the IDC IP range, etc. After configuration, download the configuration guide and complete the configuration on the IDC device.
4. In the route table associated with the VPC subnet for communication, configure a routing policy with the direct connect gateway as the next hop and IDC IP range as the destination.

> **Note**
> For more detailed configurations, see Quick Start for Dedicated Line Access.

Step 2: Connect IDC to VPC through a VPN connection

1. Log in to the VPN Gateway Console, click **Create** to create a VPN Gateway. In this case, associate the network with the VPC.
2. Click **Peer Gateway** on the left sidebar to configure the Peer Gateway (the logical object of the IDC-side VPN gateway). Enter the public IP address of the IDC-side VPN gateway, e.g., 202.xx.xx.5.
3. Click on the left navigation bar's **VPN Tunnel**, please configure SPD policies, IKE, IPsec, etc.
4. Configure the same VPN tunnel as the step 3 on the local gateway device of the IDC to ensure a normal connection.
5. In the route table associated with the VPC subnet for communication, configure a routing policy with the VPN gateway as the next hop and IDC IP range as the destination.

> **Note**
> For more detailed configurations, please refer to Establishing a VPC to IDC Connection (Routing Table).

Step 3: Configure network probes

> **Note**

> After the first two steps, there are two VPC routes to IDC. That is, both direct connect gateway and VPN gateway act as the next hop. By default, the direct connect gateway route has a higher priority, making it the primary path and the VPN gateway the secondary path.

To stay on top of the primary/secondary connection quality, configure two network probes separately to monitor the key metrics such as latency and packet loss rate and check the availability of primary/secondary routes.

1. Log in to the Network Detection Console.
2. Click **Create** to set up network detection. Fill in the name of the network detection, select VPC, subnet, detection target IP, and designate the source endpoint's next-hop route, such as a direct connect gateway.
3. Please perform Step 2 again, specifying the source-end next-hop route as the VPN gateway. Once configured, you can view the network probe latency and packet loss rate of the primary and secondary paths for DC and VPN connections.

> **Note**
> For more detailed configurations, please refer to Network Detection.

Step 4: Configure an alarm policy

You can configure an alarm policy for linkages. When a linkage has an exception, alarm notifications are sent to you automatically via emails and SMS message, alerting you of the risks in advance.

1. Log in to the TCOP section's Alarm Policy Console.
2. Click **Create**, fill in the policy name, for policy type select **VPC/Network Detection**, choose a specific network detection instance for the alarm object, configure trigger conditions and alarm notifications, and then click **Done**.

Step 5: Switch between primary and secondary routes

After receiving the exception alarms about the direct connect gateway, you need to manually disable the primary route, and forward traffic to the secondary route VPN gateway.

1. Log in to the Routing Table Console.
2. Click VPC Communication Subnet to associate Route Table ID, enter the route detail page, click  to disable the primary route to the direct connect gateway's next hop. Hence, VPC traffic to IDC will switch from the direct connect gateway to the VPN gateway.

Connecting IDC to CCN

Last updated: 2024-09-26 10:32:51

The VPN gateway for CCN can be associated with the Cloud Connect Network (CCN) to establish an encrypted communication between the IDC and CCN. This document introduces how to associate the VPN gateway for CCN with CCN.

Background

A VPN gateway for CCN can be associated with CCN. Each VPN gateway for CCN can establish multiple encrypted VPN tunnels, and each VPN tunnel can connect one local IDC.

The steps to associate the VPN gateway for CCN with CCN are as follows:

1. Create a VPN gateway for CCN: a VPN gateway is an egress gateway used by CCN to establish VPN connections along with the customer gateway.
2. Associate CCN instances: associate the created VPN gateway for CCN with CCN instances.
3. Create a customer gateway: a customer gateway is a logical object used to record the public IP address of the IPsec VPN gateway on the IDC side (a fixed public IP is required on the IDC side). It is used with a Tencent Cloud VPN gateway. One VPN gateway can establish encrypted VPN tunnels with multiple customer gateways.
4. Create a VPN tunnel: VPN tunnel supports IPsec encryption protocol to ensure secure data transmission.
5. Configure the VPN gateway route: after the VPN tunnel is successfully configured, you need to configure the VPN gateway route to the customer gateway.
6. IDC Local Configuration: Configure the VPN tunnel information of the other side (Tencent Cloud side) on the "local gateway" at the IDC side.
7. Enable the IDC IP segment: add the peer IP segment from the SPD policy to CCN.

Directions

Step 1: create a VPN gateway for CCN

1. Log in to the VPC console.
2. Choose **VPN Connection** > **VPN Gateway** in the left sidebar.
3. In the top navigation bar, select **region**, and on the "VPN Gateway" page, click **New**.
4. In the popped-up "Create VPN Gateway" window, enter the VPN gateway name (e.g., TomVPNGw), select the associated network, bandwidth limit, and billing method, then click **Create**. After the VPN gateway is created, the system will randomly assign a public IP, such as `203.195.147.82`.

> **Note**
> To create a VPN gateway for CCN in the specified availability zone, please submit a Ticket.

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	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	Select CCN here.
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.

Step 2: associate CCN instances

- You can associate an existing CCN instance by the following steps:

  1.1 Return to the **VPN Gateway** page, and in the VPN gateway list, click the created CCN VPN gateway ID.

  1.2 On the **Basic Information** page, click **Associate CCN** next to Associated Network, select the target CCN instance from the drop-down list, and click **Confirm**.

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

- You can associate a new CCN instance by the following steps:
  1.1 Click **CCN** on the left sidebar.
  1.2 On the "CCN" page, select **Region** at the top, then click **Create**.
  1.3 In the popped-up "Create CCN Instance" window, follow the steps and then click **Confirm**.
    1.3.1 Enter the CCN instance name, description, select billing mode, and service quality.
    1.3.2 Under "Associated Instances", select **VPN Gateway**, and the region and ID of the created CCN VPN gateway.

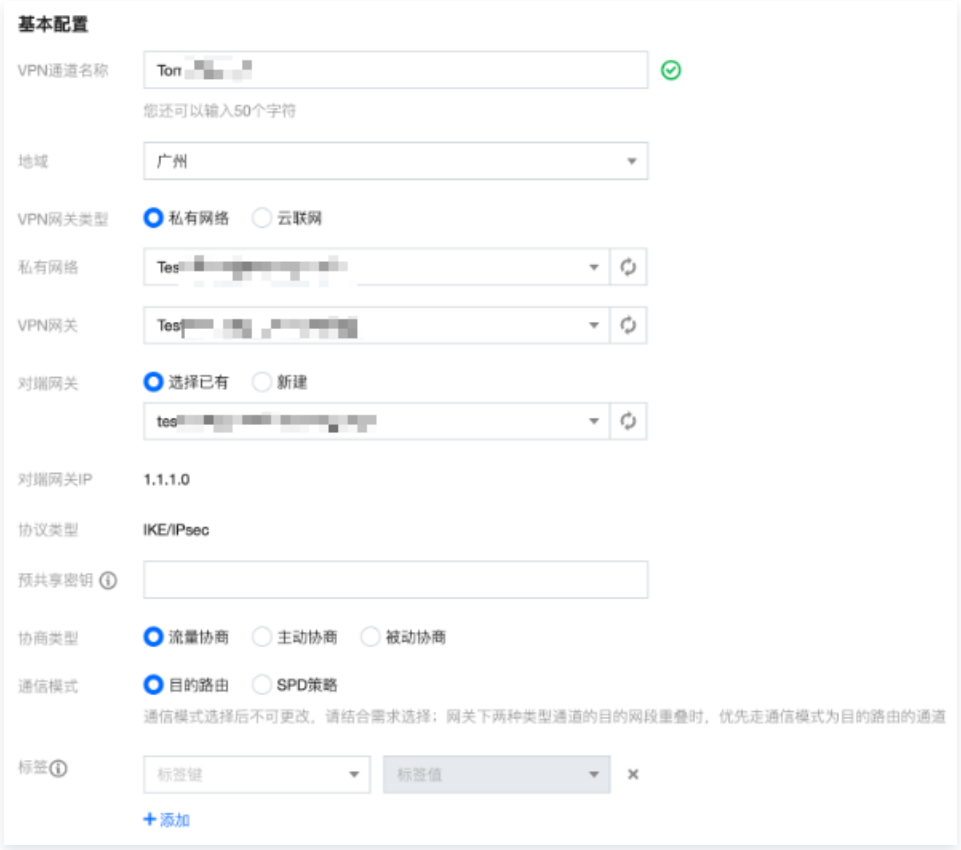
Step 3: create a customer gateway

1. Log in to the VPC console.
2. In the left sidebar, select **VPN Connections** > **Peer Gateway**.
3. On the "Peer Gateway" page, select **Region** at the top, and click **Create**.
4. In the popped-up "Create Peer Gateway" window, enter the peer gateway name and the public IP of the IDC VPN gateway, and click **Create**.

Step 4: create a VPN tunnel

1. Log in to the VPC console.
2. Choose **VPN Connections** > **VPN Tunnel** in the left sidebar.
3. At the top of the "VPN Tunnel" page, select **Region** and click **Create** to enter the "Create VPN Tunnel" page.
4. Configure the basic information about the VPN tunnel as prompted.

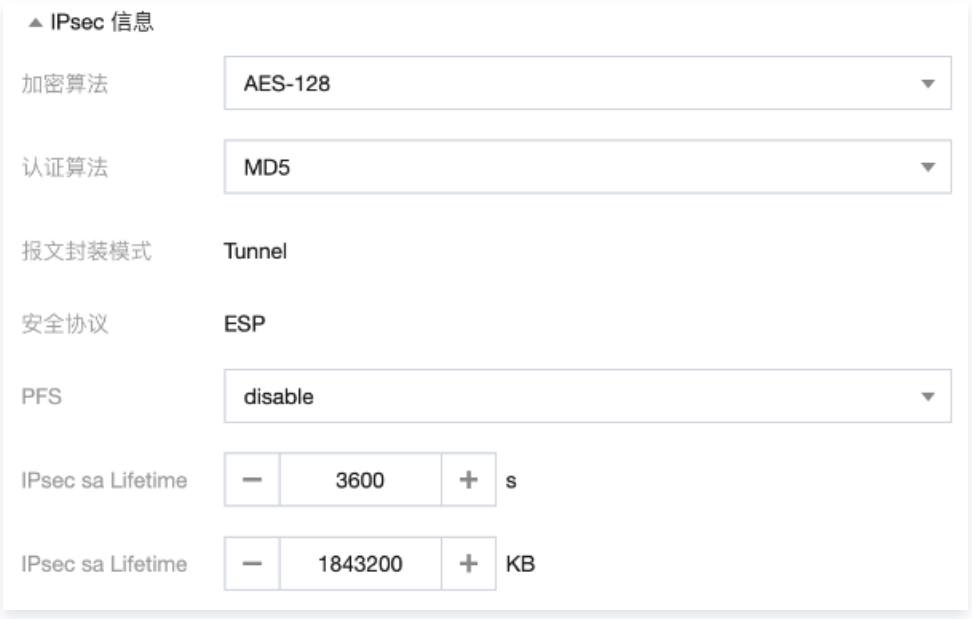
> **Note**
> - IDC IP ranges in each rule cannot overlap.
> - Rules for tunnels in the same gateway cannot overlap.
> - Peer IP ranges in the SPD policy can be added to CCN.



5. Configure DPD and health check options.
   - DPD Detection: Keep the default configuration, which is enabled by default. If modifications are needed, please refer to the interface parameters for configuration.
   - Health Check: Keep the default configuration, which is disabled by default.

6. (Optional) Configure IKE Parameters. If no advanced configuration is needed, you can directly click **Next**.

7. (Optional) Configure IPsec Parameters. If no configuration is needed, you can directly click **Complete**.



8. After completing the basic and advanced configurations, click **Create**.

   Once created, return to the VPN Tunnel list page, and under the operation column, click **More** > **Download Configuration File** and complete the download.

Step 5: configure the VPN gateway route

After the VPN tunnel configuration is complete, configure the VPN gateway route to the customer gateway.

1. Choose **VPN Connections** > **VPN Gateway** in the left sidebar, find the created VPN Gateway in the VPN Gateway list on the right, and click its name.
2. In the VPN Gateway details tab, click the **Route Table** tab, then click **Add Route**.

3. On the **Create Route** page, configure the route policy from the VPN Gateway to the peer gateway.

Configuration Item	Description
Destination	Enter the IDC IP range configured in the customer gateway for the public access.
Next Hop Type	The default value is VPN Tunnel.
Next Hop	Select a VPN tunnel that has been created.
Weight	Enter an integer within 0–100. The smaller the value, the higher the priority.

4. Click **OK**.

Step 6: configure the IDC devices

After completing the first 4 steps, the configuration of the VPN gateway and VPN tunnel on the cloud has been completed. You need to continue configuring the VPN tunnel information on the "Local Gateway" on the IDC side. For details, please refer to Local Gateway Configuration.

Step 7: enable IDC IP ranges

Note

- This step is only applicable to version 1.0 and 2.0 of the VPN Gateway. For version 3.0 of the VPN Gateway, this corresponds to the **Route Table** tab, as shown below.
- If you are using version 3.0 of the CCN Type VPN Gateway and the VPN Gateway has been associated with a CCN instance, the routing policy to **CCN** for next hop will be automatically learned and displayed in the routing entries. There is no need for manual configuration. Additionally, the routing policies configured in the VPN Gateway will be automatically synchronized to the CCN.

Version 3.0 VPN Gateway routing table **interface display:**

For VPN gateways v1.0 and v2.0, enable the IDC IP ranges as follows:

1. Log in to the VPC console.

2. Choose **VPN Connections** > **VPN Gateway** in the left sidebar.
3. Click the ID of the CCN Type VPN Gateway in the VPN Gateway list.
4. In the VPN Gateway details page, choose the **IDC IP Range** tab, and enable the target IP range.

Result Verification

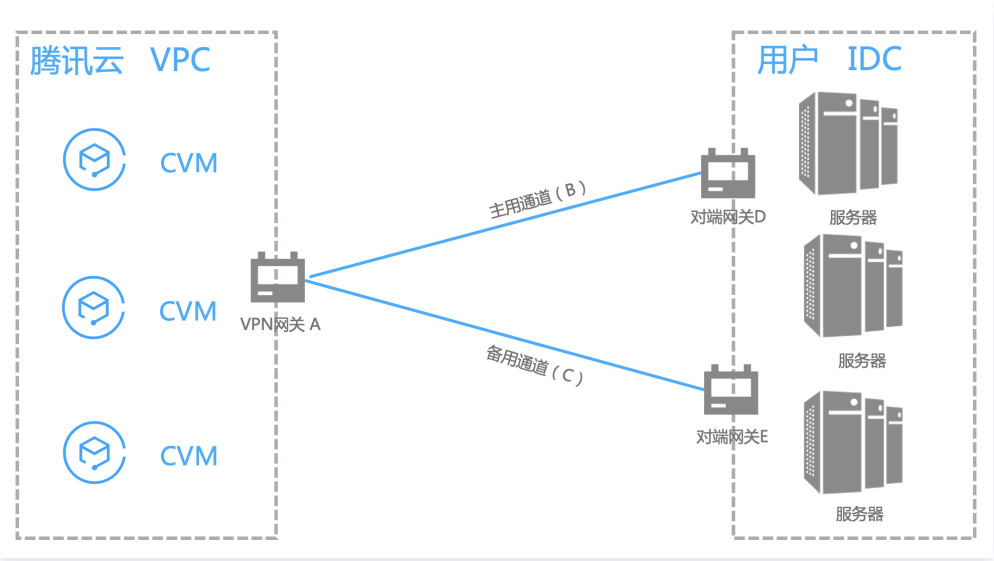
1. Log in to the VPC console.
2. Choose **CCN** in the left sidebar.
3. In the CCN list page, click the ID of the CCN instance associated with the CCN Type VPN Gateway.
4. On the CCN details page, select the **routing table** tab. If the enabled network segment is in the routing table, and the "status" is valid, and the "next hop" is a CCN-type VPN gateway, then the association is successful.

Connecting IDC to a Single Tencent Cloud VPC for Primary/Secondary Disaster Recovery

Last updated: 2024-09-26 10:33:08

Tencent Cloud VPN Connections are highly available. When a user's IDC connects to the cloud through primary and secondary VPN tunnels, and the primary tunnel fails, the business automatically switches to the secondary tunnel, ensuring the sustainability of operations and improving business reliability. This document uses the example of connecting an IDC to a single Tencent Cloud VPC for primary/secondary disaster recovery.

Disaster Recovery Scheme



The user's IDC only needs to connect with a single Tencent Cloud VPC. On the user's IDC side, the user can deploy two IPsec VPN devices to establish IPSec VPN tunnels with the Tencent Cloud VPC VPN. The routes in the VPN gateway's route table will have two routes with the same destination, and the primary/secondary tunnel effect is achieved through priority control. In case of a failure, the route can automatically switch.

Prerequisites

You have created a VPC network on the Tencent Cloud side.

Configuration Process

1. Creating a VPN Gateway
2. Creating a Customer Gateway
3. Create VPN Tunnel (Primary/Secondary)
4. IDC-Side Configuration
5. Configure VPN Gateway Routes
6. Configure Channel Health Check
7. Configure VPC Routing Policies
8. Activate VPN Tunnel

Operation Steps

Step 1: Create VPN Gateway

> **Note**
> This document uses version 3.0 of the VPN gateway as an example.

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. In the pop-up **Create VPN Gateway** dialog box, configure the following gateway parameters.

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	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	Select VPC here.
Virtual Private Cloud	You need to specify the VPC to be associated with the VPN gateway only when the network type is VPC.
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.

5. After completing the gateway parameter settings, click **Create** to start the creation of the VPN gateway.
   The **Status** will be **Creating** for about 1-2 minutes. Once successfully created, the VPN gateway status will be **Running**, and the system will assign a public IP to the VPN gateway.

Step 2: Create a Customer Gateway

Create a customer gateway D on the Tencent Cloud side.

1. In the left sidebar, choose **VPN Connections** > **Customer Gateway**.
2. On the **Customer Gateway** management page, select the region and click **New**.
3. 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.

- Name: Enter the name of the customer gateway.
- Public IP: Enter the public IP address of the VPN gateway on the IDC side.

4. Click **OK**.

Create a customer gateway E on the Tencent Cloud side.

Repeat steps 1 to 4 for creating customer gateway A.

Step 3: Create a VPN Tunnel (Primary and Backup)

After the VPN gateway and customer gateway are created, you need to create two VPN tunnels between the VPN gateway and the IDC side, one as the primary tunnel and the other as the backup tunnel.

Create the primary tunnel B

1. In the left sidebar, choose **VPN Connections** > **VPN Tunnel**.
2. On the **VPN Tunnel** management page, select the region and click **New**.
3. Fill in the VPN tunnel information on the pop-up page. For specific parameter configuration, refer to New VPN Tunnel. Choose "Destination Routing" for the communication mode.
4. Click **Create**.

Create Backup Tunnel C

Repeat Step 1 to Step 4 of creating Primary Tunnel B. For the communication mode, select "Destination Routing".

Step 4: IDC-side Configuration

After completing the first three steps, the configuration of the VPN gateway and VPN tunnel on Tencent Cloud is complete. Next, configure the other side of the VPN tunnel on the IDC side's **Local Gateway**. Refer to Local Gateway Configuration for details. The "Local Gateway" on the IDC side is the IPsec VPN device on the IDC side, and its public IP is recorded in the "Customer Gateway" in Step 2.

> ⚠ **Note**
> Both the primary and backup VPN tunnels on the IDC-side VPN gateway need to be configured.

Step 5: configure the VPN gateway route

Up to Step 4, the primary and backup VPN tunnels have been configured. You need to configure the VPN gateway route to the VPN tunnel in the VPN console.

1. In the left navigation bar, choose **VPN Connections** > **VPN Gateway**, and in the right VPN gateway list, find VPN Gateway A created in Step 1 and click its name.
2. In the details tab of VPN Gateway A, click the **Route Table** tab, and click **Add Route**.

3. On the **Add Route** page, configure the routing policy from VPN Gateway A to VPN Tunnel B and VPN Tunnel C.

Configuration Item	Description
Destination	Enter the IP range of the remote network to be accessed, which is the IP range provided by the IDC side for public access.
Next Hop Type	The system auto-fills **VPN Tunnel**.
Next Hop	Select a VPN tunnel that has been created.
Weight	• Enter 0 for VPN Tunnel B. • Enter 100 for VPN Tunnel C. Enter an integer within 0–100. The smaller the value, the higher the priority.

4. Click **OK**.

Step 6: Configuring Tunnel Health Check

After completing the VPN gateway route configuration, configure the health check for the VPN tunnel (this needs to be configured for both primary and backup tunnels).

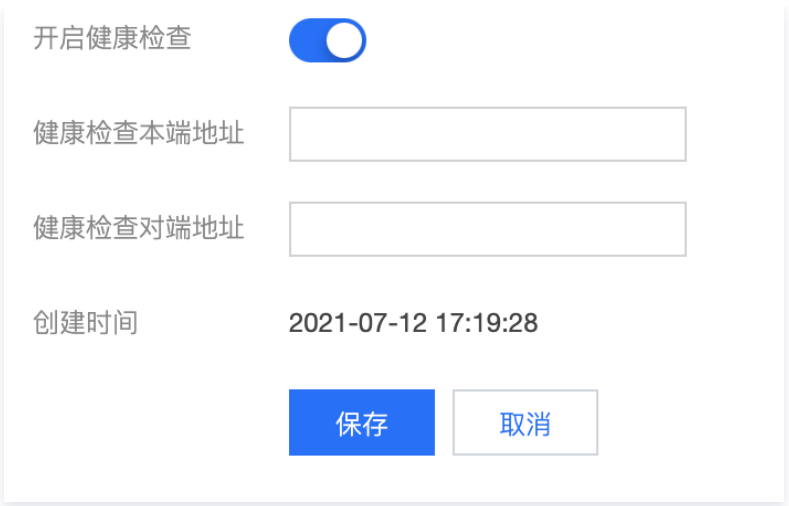
> **Note**

> When the health check triggers a switch between primary and backup tunnels, there may be a brief business interruption. Don't worry, the business will return to normal 1-2 seconds after the switch completes.

Primary Tunnel B Health Check Configuration

1. In the left sidebar, select **VPN Connections** > **VPN Tunnel**, find the created VPN tunnel in the right-side VPN tunnel list, and then click the VPN tunnel name.
2. In the **Basic Information** tab of the tunnel, click **Edit**.

3. Turn on the health check switch, input the **Health Check Local Address** and **Health Check Remote Address**, and then click **Save**.



Note:

- Local Address: Enter the IP address on Tencent Cloud side that initiates the health check request to the IDC. This IP address cannot be an IP address within the VPC.
- Remote Address: Enter the IP address at the IDC side that responds to the Tencent Cloud health check request. This IP address should be different from the Tencent Cloud address to avoid IP conflicts.
- When Tencent Cloud initiates a health check request, and the request reaches the IDC through the tunnel, and finds a health check response IP address, it indicates that the tunnel health is normal. If not, it indicates an anomaly.

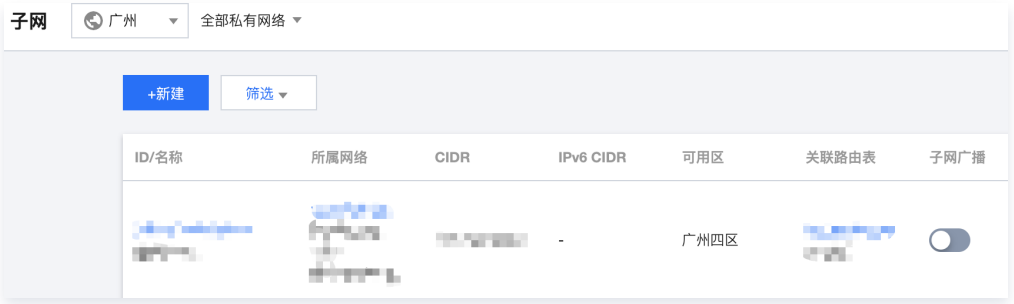
Backup Tunnel C Health Check Configuration

Repeat steps 1 to 3 of the primary tunnel health check configuration; the health check connections should not be the same as those of the primary tunnel.

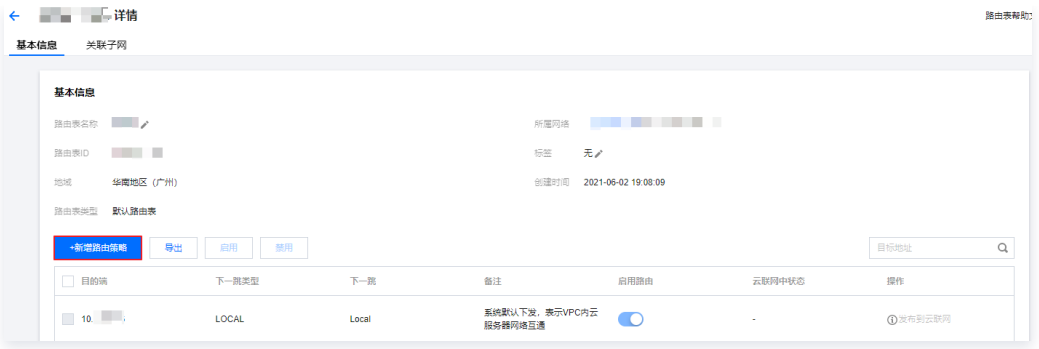
Step 7: Configure the VPC Routing Policy

As of Step 5, the primary and backup VPN tunnels have been successfully configured. You need to configure the VPC routing policy to route the traffic from the subnet to the VPN gateway so that the IP range in the subnet can communicate with the IP range in the IDC.

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. Click **Add a Routing Policy**.



4. In the pop-up box, enter the destination IP range, select **VPN Gateway** as the next hop type, choose the newly created VPN gateway as the next hop, and click **Create**.

Step 8: Activate the VPN Tunnel

Use the CVM in the VPC to ping the IP of the opposite IP range to activate the VPN tunnel. A successful ping indicates that the VPC and IDC can communicate properly.
When the VPN route table detects that the route to the primary VPN Tunnel B is unreachable, the system automatically switches the traffic to VPN Tunnel C, ensuring high availability for your business.

Dedicated private network traffic achieves encrypted communication through the Private Network VPN Gateway Solution Overview

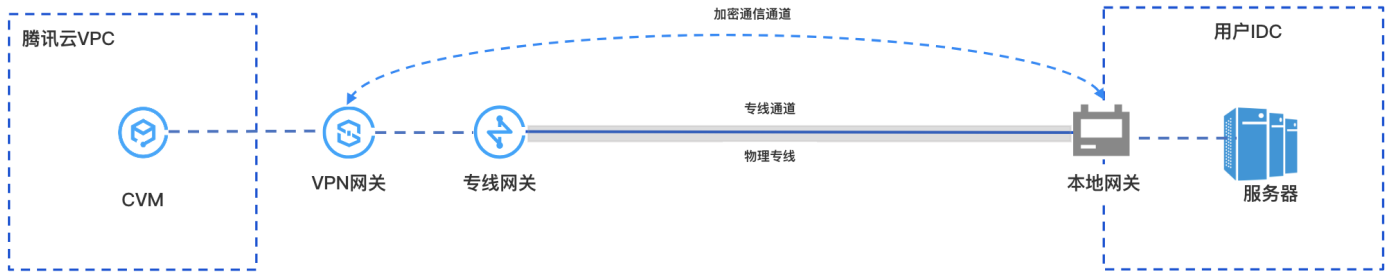
Last updated: 2024-09-26 10:33:28

Note:

- The Private Network VPN Gateway IP address belongs to the Tenant VPC.
- Private Network VPN currently supports only VPC-based VPNs. CCN-type VPN gateways are not supported.
- Dynamic BGP is not currently supported for Private Network VPN.
- To use private network type VPN, please submit a work order for consultation.

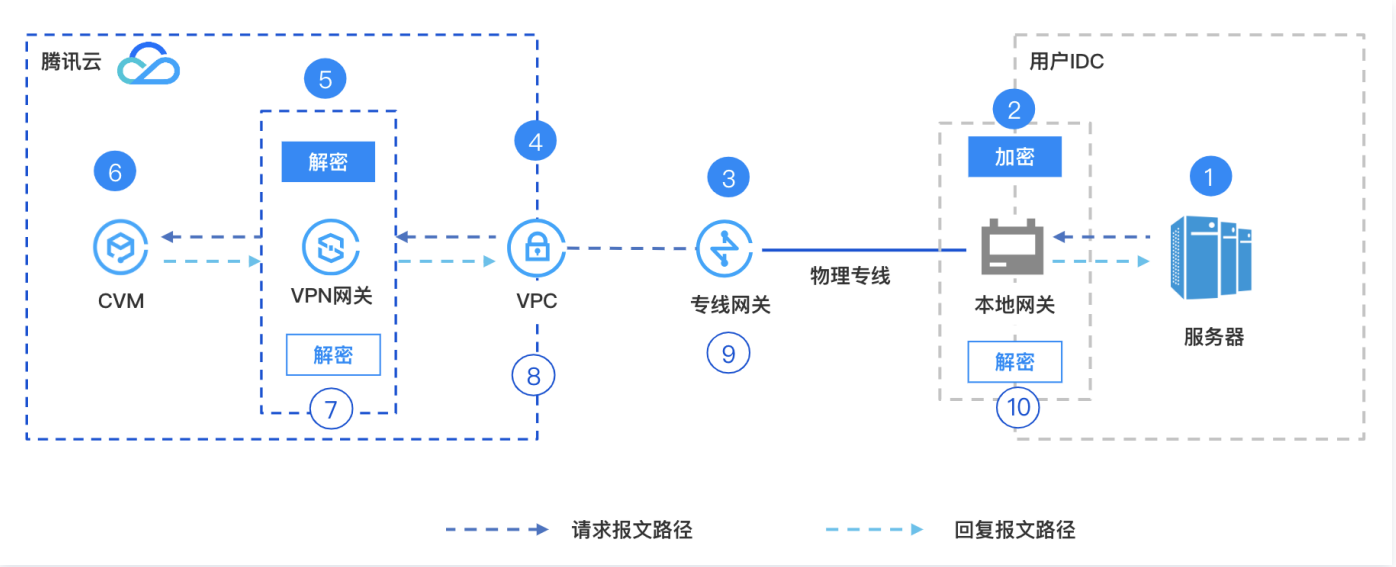
Scenario Description

After establishing private network communication between the local data center (IDC) and the VPC on the cloud through a physical dedicated line, the Private Network VPN Gateway can establish an encrypted communication channel with the local gateway device through the existing private network connection. You can configure relevant routes to guide the traffic between the local IDC and the VPC that needs to be interconnected into the encrypted communication channel, achieving encrypted communication of private network traffic.



Private Network Traffic Encryption Communication Principle

To help you understand, the following examples illustrate the process of traffic encryption for Private Network VPN.



Serial number	Forwarding Object	Description
①	User IDC Server	The customer initiates an access request, and the request packet is routed to the IDC local gateway.
②	IDC Local Gateway	The local gateway encrypts and encapsulates the request packet, then forwards the encapsulated packet to the Cloud Direct Connect Gateway based on the configured route.
③	Direct Connect Gateway	After receiving the encapsulated request packet, the Direct Connect Gateway forwards it to the VPC.
④	Virtual Private Cloud	After receiving the encapsulated Request Message, the Virtual Private Cloud forwards it to the Private Network VPN Gateway.
⑤	VPN Gateway	1. The Private Network VPN Gateway receives the encapsulated Request Message and decrypts it. 2. The Private Network VPN Gateway traverses the routing table based on the decrypted message's destination address and forwards the Request Message to the Cloud Virtual Machine.
⑥	Cloud Virtual Machine (CVM)	1. The Cloud Virtual Machine receives the decrypted Request Message, responds to it, and sends a Response Message to the client. 2. The Cloud Virtual Machine queries the routing table based on the Response Message's destination address and forwards the Response Message to the VPN Gateway.
⑦	VPN Gateway	1. The Private Network VPN Gateway encrypts the Response Message after receiving it. 2. The VPN Gateway queries the routing table based on the encrypted Response Message's destination IP address and forwards the Response Message to the Virtual Private Cloud.
⑧	Virtual Private Cloud	After receiving the encrypted Response Message, the Virtual Private Cloud queries the routing table and forwards the encrypted Response Message to the Direct Connect Gateway.

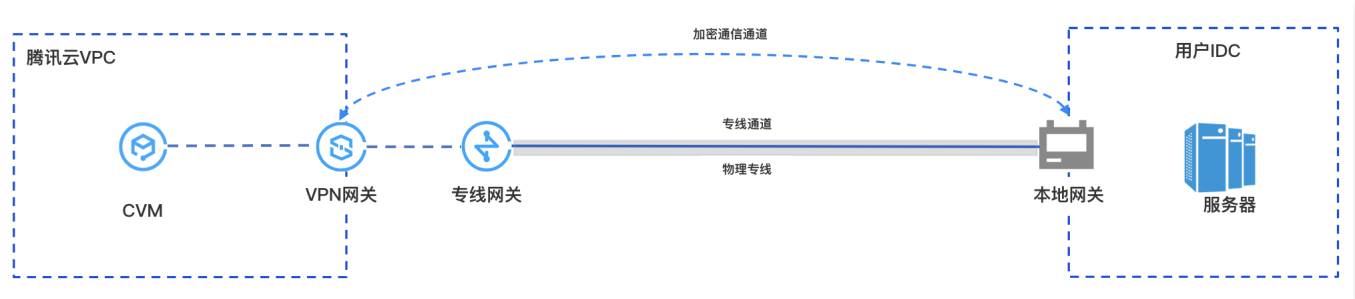
⑨	Direct Connect Gateway	The Direct Connect Gateway receives the encrypted Response Message, queries the routing table, and forwards the encrypted Response Message to the IDC Local Gateway.
⑩	IDC Local Gateway	1. After the IDC Local Gateway receives the Response Message, it decrypts the Response Message. 2. The Local Gateway device queries the route table based on the destination IP address of the decrypted Response Message and forwards the Response Message to the Server.

Dedicated private network traffic is encrypted through the Private Network VPN Gateway

Last updated: 2024-09-26 10:33:44

After establishing private network communication between the local data center (IDC) and the VPC on the cloud through a physical dedicated line, the Private Network VPN Gateway can establish an encrypted communication channel with the local gateway device through the existing private network connection. You can configure relevant routes to guide the traffic between the local IDC and the VPC that needs to be interconnected into the encrypted communication channel, achieving encrypted communication of private network traffic.

Business Scenario



Use Limits

- Currently, the Private Network VPN only supports VPC-type VPNs, and CCN-type VPNs are not supported yet.
- Private Network VPN currently does not support dynamic BGP routing.
- Only supported in VPN v4.0.

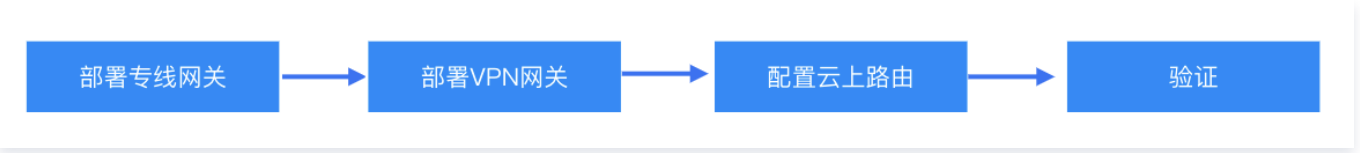
Network Planning

Configuration Object	IP Range Planning	IP addresses and Notes
VPC	10.7.0.0/16	• CVM:10.7.6.10 • Private Network VPN Gateway IP: 10.7.6.15 **Note:** Private Network VPN Gateway IP belongs to the tenant VPC.
Direct Connect Gateway	195.168.0.0/29	• VLAN ID:1234 • Tencent Cloud Primary IP1: 195.168.0.3/29 • Tencent Cloud Primary IP2: 195.168.0.2/29 • Customer Edge IP: 195.168.0.1/29.
Local Gateway	195.168.0.0/24	• Local Gateway IP for connection with Cloud-based VPN Connections: 195.168.0.6 • IP Range connected with Direct Connect Gateway: 195.168.0.1/29
Local IDC Server	133.168.0.0/16	Client address: 133.168.0.3/32

Prerequisites

- You have created a VPC.
- Physical dedicated line has been constructed and connected.
- You have applied for Private Network VPN permissions. If you need to use it, please submit a work order.
- IDC-side equipment is ready.

Configuration Process



Step 1: Deploy Dedicated Line Service

Step 1: Create a VPC-type dedicated line gateway

1. Log in to the DC Console, and click on **Dedicated Line Gateways** in the left navigation bar.
2. At the top of the **Direct Connect Gateway** page, choose the region and VPC, then click **New**.
3. In the **Create a Dedicated Line Gateway** dialog box, configure the gateway details and click **Confirm** upon completion.

Field	Meaning
Name	Enter a name for the direct connect gateway.
Availability Zone	Select the AZ supported by the region.
Associated Network	Select VPC.
Network Location	Associate with the created VPC instance, vpc-xxx.

Step 2: Create a dedicated tunnel for the dedicated line

1. Log in to DC - Dedicated Tunnel console.
2. In the left navigation bar, click **Dedicated Tunnel** > **Exclusive Private Channel**. At the top of the page, click **New** and configure the name, dedicated line type, access network, region, associated Direct Connect Gateway, and other basic configurations. Once completed, click **Next**.

Field	Meaning
Dedicated tunnel name	Dedicated tunnel name.
Direct Connection Type	Select "My Dedicated Line"
Connection	Select the ready physical dedicated line.
Access network	Select VPC.
Gateway	Select the region where the target VPC instance is located, such as Guangzhou.

Region	
Direct Connect Gateway	Associate the Private Network Dedicated Line Gateway created in Step 1.

3. On the **Advanced Configuration** page, configure the following parameters.

Field	Meaning
VLAN ID	Configure the planned VLAN, e.g., 1234. One VLAN corresponds to one channel, with a range of values [0,3000).
Bandwidth	The maximum bandwidth of the exclusive channel cannot exceed the bandwidth of the associated physical dedicated line. Under the postpaid model after the 95th percentile for the month, the "bandwidth" parameter does not represent the billing bandwidth.
Tencent Cloud Boundary IP1	Configure the planned Edge Interconnect IP on the Tencent Cloud side of the physical dedicated line, e.g., `195.168.0.3/29` Do not use the following IP ranges or addresses: `169.254.0.0/16`, `127.0.0.0/8`, `255.255.255.255/32`, `224.0.0.0/8` – `239.255.255.255/32`, `240.0.0.0/8` – `255.255.255.254/32`.
Tencent Cloud Boundary IP2	Configure the planned Standby Border Interconnect IP, e.g., `195.168.0.2/29`. In the event of a failure of the primary border IP, the standby IP is automatically activated to ensure the normal operation of your service. If Tencent Cloud Edge IP has a mask of 30 or 31, standby IP configuration is not supported.
User Boundary IP	Configure the cloud IP on the IDC side used to interconnect with the dedicated line, e.g., `195.168.0.1/29`.
Routing mode	Select BGP Routing.
Health examination	Health checks are enabled by default. For details, see Dedicated Tunnel Health Check.
Check Mode	Select BFD Mode.
Health Check Interval	Interval between two health checks.
Number of health checks	Route switching occurs after the specified number of consecutive health check failures.
BGP ASN	Enter the BGP neighbor ASN on the CPE side. Note that the Tencent Cloud ASN is 45090. If this field is left empty, a random ASN will be assigned.
BGP keys	Enter the MD5 value of the BGP neighbor. The default is "tencent", leave empty to indicate no BGP key is required. The BGP key does not support 6 special characters including ? & space" \ +.

4. Click **Submit**.

Step 2: Deploy VPN Service

Step 1. Create a Private Network VPN Gateway

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. In the pop-up **Create VPN Gateway** dialog box, configure the following gateway parameters.

Parameter name	Parameter Description
Billing Mode	Select bill-by-traffic. Private Network VPN does not support annual and monthly subscriptions.
Gateway Name	Enter the VPN gateway name (up to 60 characters).
Region	Display the region of the VPN gateway.
Protocol Type	Select IPSEC.
Network Type	Select "Private Network".
Associated Network	Here, select VPC. Private Network VPN does not support CCN.
On-cloud subnet	Select the subnet created on the VPC side. The Private Network VPN Gateway IP address belongs to the tenant VPC and is allocated from this subnet.
Bandwidth Cap	Select 5M.
Network	Specify the VPC to be associated with the VPN gateway only when the associated network is VPC.
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 **Create** to start creating the VPN gateway.

Step 2. Create a Customer Gateway

1. In the left sidebar, choose **VPN Connections** > **Customer Gateway**.
2. On the **Customer Gateway** management page, select the region and click **New**.
3. Enter the name of the customer gateway. For Private Network IP, enter the private network IP of the local gateway device at the IDC side (195.168.0.6).
4. Click **Create**.

Step 3. Create a VPN Tunnel

1. In the left sidebar, choose **VPN Connections** > **VPN Tunnel**.
2. On the **VPN Tunnel** management page, select the region and click **New**.
3. Fill in the VPN tunnel information on the pop-up page.

   This section only introduces key parameter configurations. For other configurations, please refer to Create VPN Tunnel.

Parameter name	Parameter Description
Name of the channel	Enter the channel name.
Network Type	Select VPC.
Virtual Private Cloud	Select the created VPC instance.
VPN Gateway	Select the private VPN gateway created in Step 1.
Customer Gateway	Select the customer gateway created in Step 2.
Pre-shared Key	Set it to 123456.
Negotiation Type	Select "Traffic Negotiation".
Communication Mode	Select "Destination Routing".
Advanced Configuration	Select the current default value.

4. Click **Create**.

Step 4. Completing the IDC local configuration as instructed in Huawei NE Series Routers

After completing the first three steps, the configuration of the VPN gateway and VPN tunnel on Tencent Cloud is completed. Continue to configure the VPN tunnel information on the IDC side with the **local gateway**. For details, refer to Local Gateway Configuration. The "local gateway" on the IDC side is the IPsec VPN device, and its private IP address is recorded in the customer gateway created in Step 2.

Step 3: Configure the Cloud Routing

After completing the above configuration, an encrypted communication channel can be established between the local gateway device and the VPN gateway. You also need to configure routing for the cloud network instance to direct traffic from both the cloud and on-premises into the VPN encrypted communication channel.

Step 1. Configure the Definition route for the VPC on the Cloud

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. Click **Create a routing policy,** and configure the route to the VPN gateway in the pop-up window.

Parameter name	Description
Destination Address	Enter the local IDC subnet, for example, `133.168.0.3/32`.
Next Hop Type	Select "Private VPN Gateway".
Next Hop	Select the VPN Gateway created in Step 1 of Deploying the VPN, vpngw-xxxx.

4. Click **+Add a line** to configure the routing policy to the Direct Connect Gateway.

Parameter name	Description
Destination Address	Enter the VPN IP address of the local gateway device, e.g., `195.168.0.6`.
Next Hop Type	Select **Direct Connect Gateway**.
Next Hop	Select the Direct Connect Gateway created in Step 1 of Deploying the Direct Connect Gateway, dcg-xxxx.

5. Click **Create**.

Step 2. Configure the VPN Gateway Route

> **Note:**
> To direct VPC traffic to the off-cloud encrypted communication tunnel of the VPN Gateway, you need to add a route for the local IDC segment in the VPN Gateway.

1. Click **VPN Connections** in the left navigation bar > **VPN Gateway**.
2. On the **VPN Gateway** page, select the Region and VPC, and click the VPN gateway instance ID to go to the details page.
3. On the **Instance Details** page, click the **Route Table** tab, then click **Add Route** to 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.

Configuration Item	Description
Destination	Enter the local IDC segment, e.g., 133.168.0.3/32.
Next Hop Type	Unselectable, default is "VPN tunnel".
Next Hop	Select the VPN Tunnel created during VPN deployment.
Weight	Set the tunnel weight value to 0.

	• 0: High priority. • 100: Low priority.

4. After configuring the routing policy, click **Confirm**.

Step 4: Business Validation

After completing the above configurations, encrypted private network communication between the local IDC and the VPC is established. Test the private network connectivity and verify that the traffic is encrypted through the VPN Gateway.

1. Testing connectivity

   Log in to the CVM instance and use the **Ping** command to access the server in the local IDC segment.
2. Encryption Validation

   In the VPN Console, check the VPN tunnel traffic monitoring. Traffic indicates successful encryption.

Establishing a VPN Connection between Tencent Cloud and AzureChina

Last updated: 2025-05-30 14:30:43

We recommend establishing a VPN connection between two public clouds to transmit traffic over a private network. This improves network security and reduces risk exposure.

> **Note:**
> To establish a VPN connection, you need to create Tencent Cloud services and Azure China cloud resources. Therefore, the steps outlined in the tutorial may not be up to date.This article's third-party tutorial comes from Tencent Cloud Product "User Practices" Collection, for learning and reference purposes only.

This article provides you with a third-party tutorial on establishing VPN Connection between Tencent Cloud and AzureChina. You can refer to the tutorial to related practical operations.

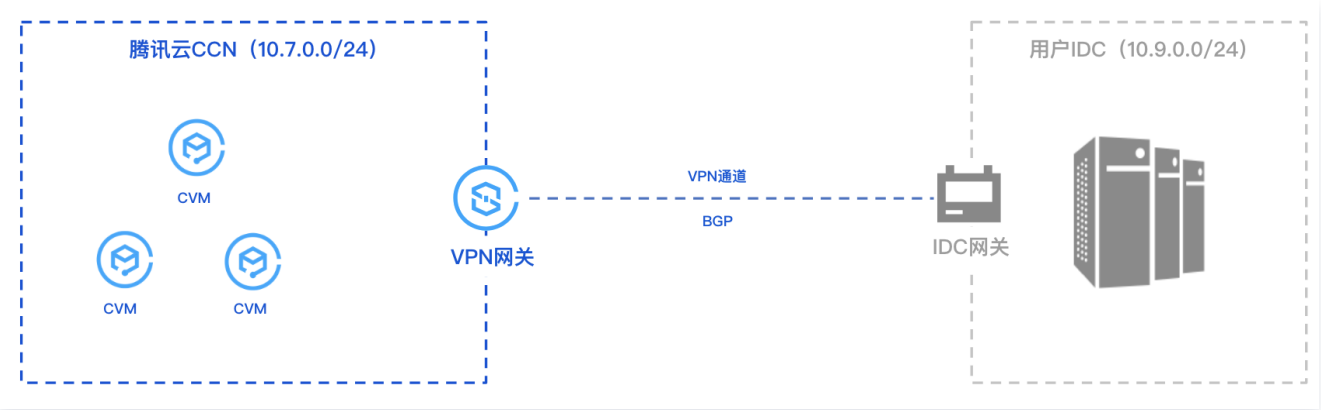
Connecting IDC with Cloud Resources (Dynamic BGP)

Last updated：2024-09-26 10:35:01

This document introduces how to use VPN's Dynamic BGP to connect IDC and cloud resources, enabling business communication.

Business Scenario

Some of the user's business is deployed on the cloud, using VPN Connections to connect IDC to the cloud network, and communicate via BGP.



Operating Procedures

1. Create a CCN instance.
2. Create a CCN-type VPN Gateway and bind the created CCN instance.
3. Create a peer gateway and specify the IDC-side ASN.
4. Create a VPN tunnel and configure BGP parameters.
5. IDC local configuration.

Operation Steps

This guide introduces only the necessary configuration steps and their parameters during the operation. For details on other parameters, please refer to the specific operation documents.

Step 1: Create a CCN Instance

You need to create the required CCN instance in the CCN Console. For specific operations, see Creating a CCN Instance.

Step 2: Create a CCN-type VPN Gateway

1. Log in to the VPN Gateway Console, and on the VPN gateway page, click **Create**.
2. Configure CCN Gateway Parameters on the VPN Purchase Page.
   - Region: Select Seoul.
   - Network Type: Select CCN.
   - Bandwidth: Select specifications of 200Mbps or above.
   - BGP ASN: Tencent side VPN gateway ASN number, default 64551, value range is 1 – 4294967295, where 139341, 45090, 58835 are unavailable.

3. On the VPN gateway details page, click **Associated Network** on the right side of **Associate CCN**, in the pop-up of **Associate CCN**, bind Step One created cloud connectivity instance.

Step 3: create a customer gateway

1. Log in to Peer Gateway Console, on the right peer gateway page, click **Create**.
2. On the **Create Peer Gateway** page, configure the IP address for public network access on the IDC side and the planned ASN, see details in Create Peer Gateway.

Step Four: Create BGP Routing VPN Tunnel

1. Log in to VPN Tunnel Console, on the right VPN tunnel page, click **Create**.
2. On the new VPN tunnel page, configure the basic parameters of the tunnel according to actual situations, and continue with subsequent configurations after completion.

Parameters	Description
Network Type	Select CCN.
VPN Gateway	Choose the CCN type VPN gateway that has been configured with ASN.
Customer Gateway	Choose the peer gateway that has been configured with ASN.
Communication Mode	Choose Dynamic BGP Routing.
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 Address	The BGP IP address for cloud-user interconnection.
Customer-side BGP Address	Cannot be modified, automatically assigned user end BGP interconnection address. After manually modifying the cloud BGP address, this parameter is automatically updated.

Step 5: IDC Local Gateway Configuration

After completing the first 4 steps, the configuration of the VPN gateway and VPN tunnel on the cloud has been completed. You need to continue configuring the VPN tunnel information on the "Local Gateway" on the IDC side. For details, please refer to Local Gateway Configuration.

> **Note:**
> The "Local Gateway" on the IDC side refers to the IPsec VPN equipment on the IDC side. The public IP of this equipment is recorded in the created "Peer Gateway".

Local Gateway Configurations
Huawei Firewall Configuration

Last updated: 2024-09-26 10:35:15

When using IPSec VPN to establish a connection between Tencent Cloud VPC and the user's IDC, after configuring the Tencent Cloud VPN gateway, you also need to configure the VPN on the gateway device at the user's local IDC site. This article introduces the configuration of Huawei firewall.

> **Note:**
> This article uses Huawei USG series firewalls as an example to introduce the IPSec VPN configuration process. For more detailed information and other business services, please contact the manufacturer for corresponding model equipment configuration guidance.

Prerequisites

Please ensure that you have created a VPN within Tencent Cloud VPC and completed the VPN tunnel configuration.

Data Preparations

An example of IPsec VPN configuration data in this document is as follows:

Configuration Item	Sample value
Network Configuration	VPC information
Public IP of the VPN gateway	159.75.**.242
IDC information	Intranet CIDR
Public IP of the gateway	120.235.**.76
Upstream public network port	GE1/0/2
Downstream public network port	GE1/0/1
IPsec Connection Configuration	IKE Configuration
Identity Authentication Method	Pre-shared Key
PSK	123456
Encryption Algorithm	AES-128
Authentication Algorithm	MD5
Negotiation Mode	main
Local ID	IP Address:120.235.225.76
Remote ID	IP Address:159.75.41.242
DH group	DH2
IKE SA Lifetime	86400
IPSec Information	Encryption Algorithm

Authentication Algorithm	MD5
Message Encapsulation Mode	Tunnel
Security Protocol	ESP
PFS	disable
IPsec sa Lifetime	3600s

Operation Steps

1. Configure the interface IP address and add the interface to the secure zone.

```
  [HUAWEI] interface GigabitEthernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] ip address 172.16.0.1 16 /*Internal network gateway
address*/
  [HUAWEI-GigabitEthernet1/0/1] quit
  [HUAWEI] interface GigabitEthernet 1/0/2
  [HUAWEI-GigabitEthernet1/0/2] ip address 120.235.**.76 24
  [HUAWEI-GigabitEthernet1/0/2] service-manage ping permit /*Allow cloud to ping public
network detection*/
  [HUAWEI-GigabitEthernet1/0/2] quit
  [HUAWEI] interface tunnel 1
  [HUAWEI-Tunnel1] ip address unnumbered interface GigabitEthernet1/0/2
  [HUAWEI-Tunnel1] tunnel-protocol ipsec
  [HUAWEI-Tunnel1] service-manage ping permit
  [HUAWEI-Tunnel1] quit
  [HUAWEI] firewall zone trust
  [HUAWEI-zone-trust] add interface GigabitEthernet 1/0/1 /*Add interface to firewall
secure zone*/
  [HUAWEI-zone-trust] quit
  [HUAWEI] firewall zone untrust
  [HUAWEI-zone-untrust] add interface GigabitEthernet 1/0/2
  [HUAWEI-zone-untrust] add interface tunnel 1
  [HUAWEI-zone-untrust] quit
```

2. Configure inter-domain security policy.

```
  [HUAWEI] security-policy
  [HUAWEI-policy-security] rule name 1 /*Plaintext cross-domain policy*/
  [HUAWEI-policy-security-rule-1] source-zone untrust
  [HUAWEI-policy-security-rule-1] destination-zone trust
  [HUAWEI-policy-security-rule-1] source-address 10.1.1.0 24
  [HUAWEI-policy-security-rule-1] destination-address 172.16.0.0 16
  [HUAWEI-policy-security-rule-1] action permit
  [HUAWEI-policy-security-rule-1] quit
  [HUAWEI-policy-security] rule name 2 /*Plaintext cross-domain policy*/
  [HUAWEI-policy-security-rule-2] source-zone trust
  [HUAWEI-policy-security-rule-2] destination-zone untrust
  [HUAWEI-policy-security-rule-2] source-address 172.16.0.0 16
  [HUAWEI-policy-security-rule-2] destination-address 10.1.1.0 24
  [HUAWEI-policy-security-rule-2] action permit
  [HUAWEI-policy-security-rule-2] quit
```

```
[HUAWEI-policy-security] rule name 3 /*Encrypted cross-domain policy*/
[HUAWEI-policy-security-rule-3] source-zone local
[HUAWEI-policy-security-rule-3] destination-zone untrust
[HUAWEI-policy-security-rule-3] source-address 120.235.**.76 32
[HUAWEI-policy-security-rule-3] destination-address 159.75.**.242 32
[HUAWEI-policy-security-rule-3] action permit
[HUAWEI-policy-security-rule-3] quit
[HUAWEI-policy-security] rule name 4 /*Encrypted cross-domain policy*/
[HUAWEI-policy-security-rule-4] source-zone untrust
[HUAWEI-policy-security-rule-4] destination-zone local
[HUAWEI-policy-security-rule-4] source-address 159.75.**.242 32
[HUAWEI-policy-security-rule-4] destination-address 120.235.**.76 32
[HUAWEI-policy-security-rule-4] action permit
[HUAWEI-policy-security-rule-4] quit
```

3. Configure Access Control List, define the data flow to be protected.

```
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255 destination 172.16.0.0
0.0.255.255
[HUAWEI-acl-adv-3000] quit
```

4. Configure IPSec security protocol.

```
[HUAWEI] ipsec proposal tran1
[HUAWEI-ipsec-proposal-tran1] transform esp
[HUAWEI-ipsec-proposal-tran1] encapsulation-mode tunnel
[HUAWEI-ipsec-proposal-tran1] esp authentication-algorithm md5
[HUAWEI-ipsec-proposal-tran1] esp encryption-algorithm aes-128
[HUAWEI-ipsec-proposal-tran1] quit
```

5. Create IKE security protocol.

```
[HUAWEI] ike proposal 1
[HUAWEI-ike-proposal-1] encryption-algorithm aes-128
[HUAWEI-ike-proposal-1] authentication-algorithm md5
[HUAWEI-ike-proposal-1] dh group2
[HUAWEI-ike-proposal-1] quit
```

6. Configure IKE policies.

```
[HUAWEI] ike peer tencent
[HUAWEI-ike-peer-asa] undo version 2
[HUAWEI-ike-peer-asa] exchange-mode main
[HUAWEI-ike-peer-asa] ike-proposal 1
[HUAWEI-ike-peer-asa] remote-address 159.75.**.242   //Tencent's public address
[HUAWEI-ike-peer-asa] pre-shared-key 123456
[HUAWEI-ike-peer-asa] quit
```

7. Configure IPSec policies.

```
[HUAWEI] ipsec policy map1 1 isakmp
[HUAWEI-ipsec-policy-isakmp-map1-1] security acl 3000
[HUAWEI-ipsec-policy-isakmp-map1-1] proposal tran1
[HUAWEI-ipsec-policy-isakmp-map1-1] ike-peer tencent
[HUAWEI-ipsec-policy-isakmp-map1-1] quit
```

8. Apply IPSec policies on the Tunnel interface.

```
[HUAWEI] interface Tunnel 1
[HUAWEI-Tunnel1] ipsec policy map1
[HUAWEI-Tunnel1] quit
```

9. Configure inner layer routing to direct traffic to the tunnel port.

```
[HUAWEI] ip route-static 10.1.1.0 24 tunnel 1
```

10. Configure outer layer outbound routing.

    For example: the upper gateway is 120.235.**.1

```
[HUAWEI] ip route-static 0.0.0.0 0.0.0.0 120.235.**.1
```

Hillstone Networks Firewall Configuration

Last updated: 2024-09-26 10:35:32

When establishing a connection from Tencent Cloud VPC to a user IDC using IPsec VPN, after configuring the Tencent Cloud VPN gateway, you also need to configure the VPN on the gateway device at the user IDC local site. This document uses Hillstone Firewall as an example to demonstrate how to configure VPN at the local site.

Note:

- This document uses the SG-6000-VM01 model and SG6000-CloudEdge-5.5R7P9 version firewall for demonstration. Other versions may have slightly different interfaces, but the overall configuration logic is the same.
- All IP addresses, interfaces, and other parameter values in this document are examples. Please use actual values during configuration.

Prerequisites

Please ensure that you have created a VPN in Tencent Cloud VPC and completed the VPN tunnel configuration.

Data Preparations

IPsec VPN configuration data examples in this document are as follows:

Configuration Item			Sample value
Network Configuration	VPC information	Subnet CIDR block	10.1.1.0/24
		Public IP of the VPN gateway	159.xx.xx.242
	IDC information	Intranet CIDR block	172.16.0.0/16
		Public IP of the gateway	120.xx.xx.76
IPsec Connection Configuration	IKE Configuration	Version	IKEV1
		Identity Authentication Method	Preshared key, for example 123456
		Encryption Algorithm	DES
		Authentication Algorithm	MD5
		Negotiation Mode	main
		Local ID	IP Address:120.xx.xx.76
		Remote ID	IP Address:159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec Configuration	Encryption Algorithm	AES-128
		Authentication Algorithm	MD5
		Message Encapsulation Mode	Tunnel

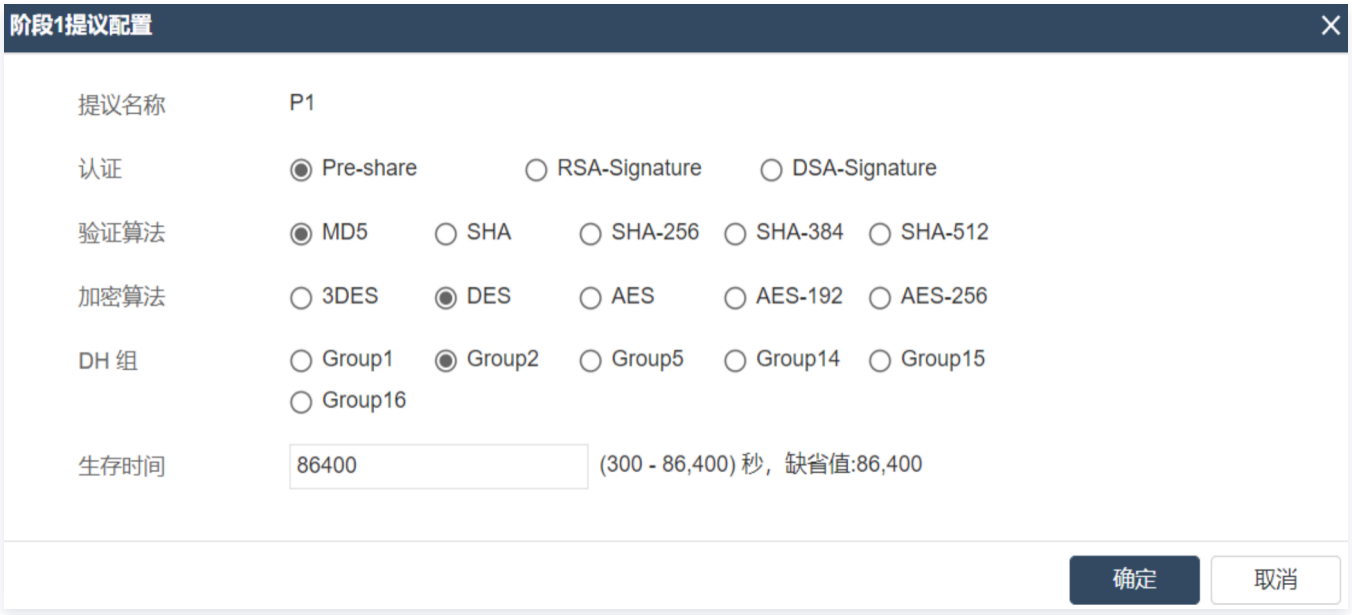
		Security Protocol	ESP
		PFS	disable
		IPsec SA Lifetime (s)	3600s
		IPsec SA Lifetime (KB)	1843200KB

Operation Steps

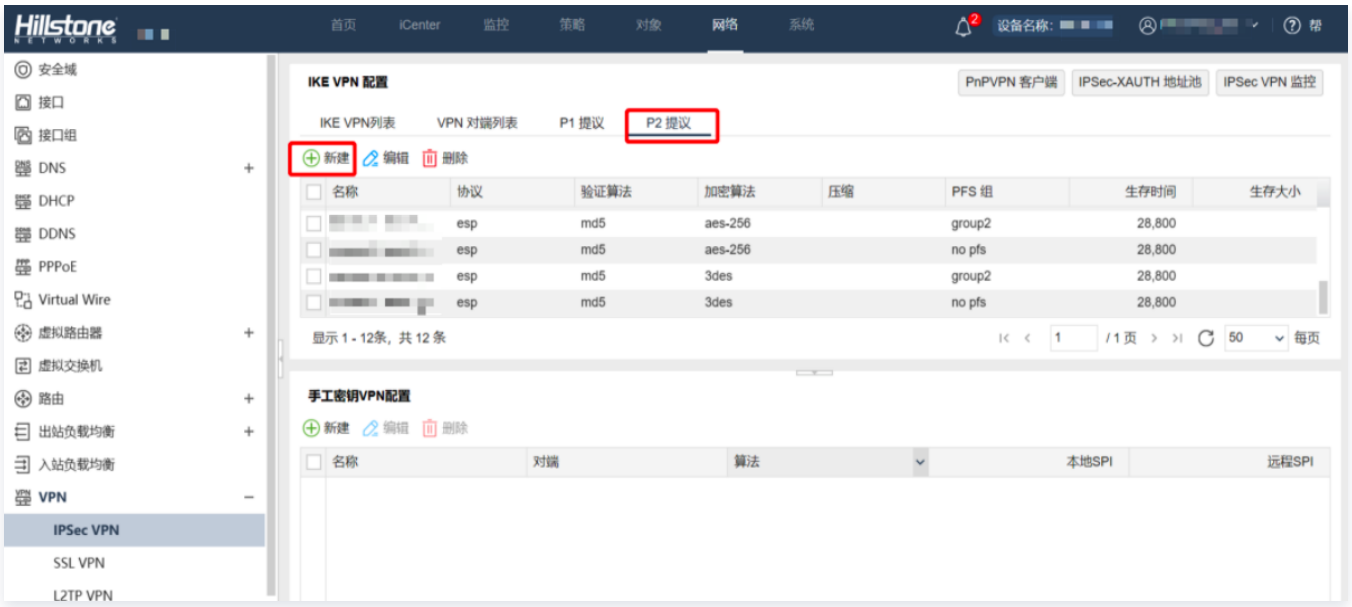
Applicable to VPN with SPD Policy Forwarding

1. Log in to the Hillstone Firewall Web interface, select **Network** > **VPN** > **IPsec VPN** > **P1 Proposal**, in the **P1 Proposal** interface, click **New**.

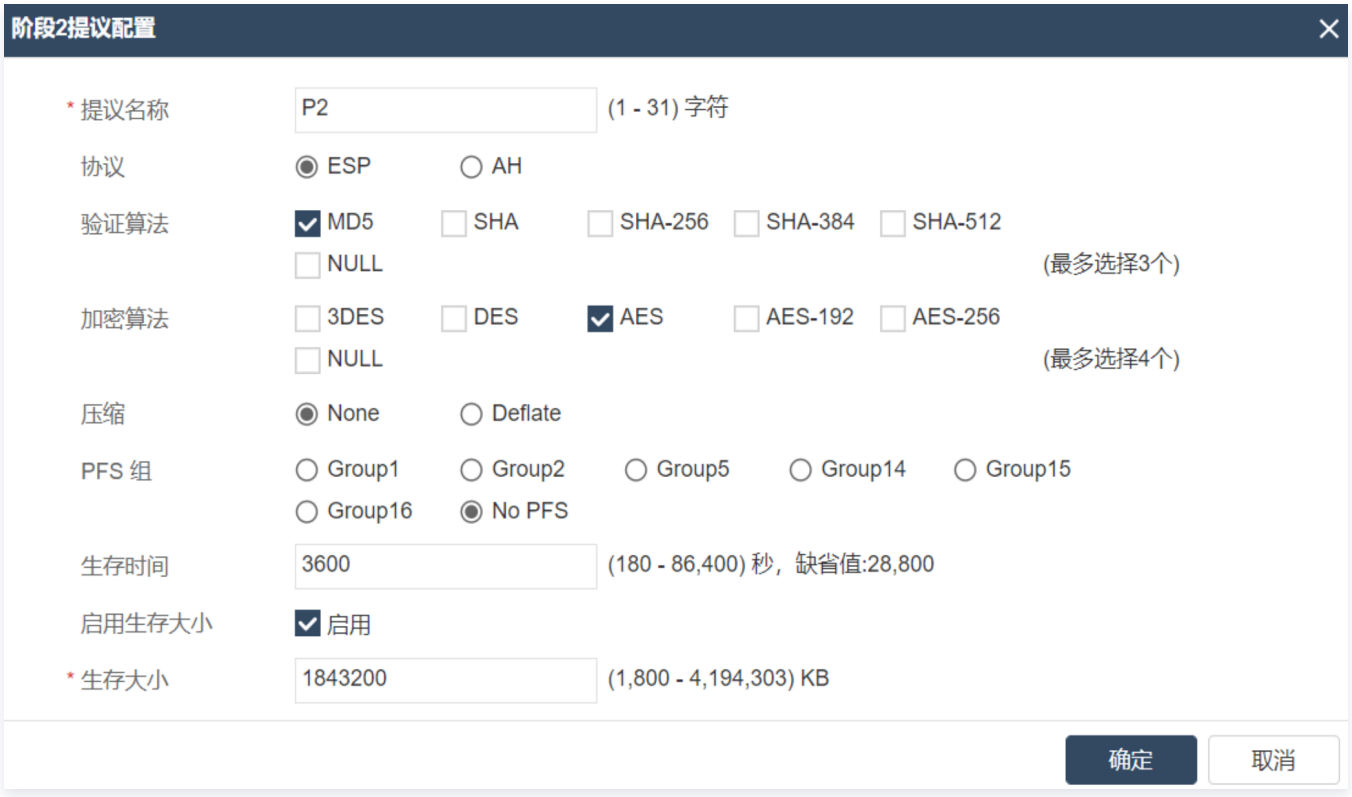
2. In the popped-up **Phase 1 Proposal Configuration** interface, configure the IKE protocol of IDC according to the IKE protocol information of Tencent Cloud VPN Connections, and click **OK**.



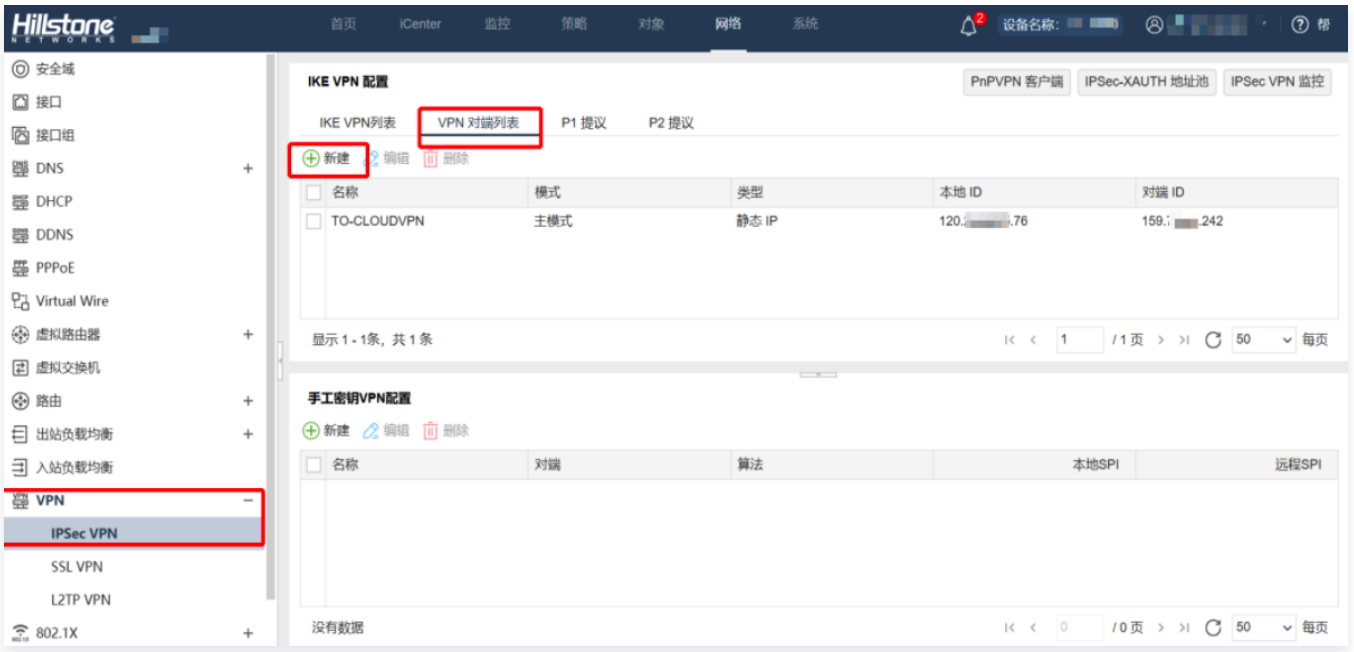
3. Select the **P2 Proposal** tab, and click **New**.



4. In the popped-up **Phase 2 Proposal Configuration** interface, configure the IPsec protocol of IDC according to the IPsec protocol information of Tencent Cloud VPN Connections, and click **OK**.



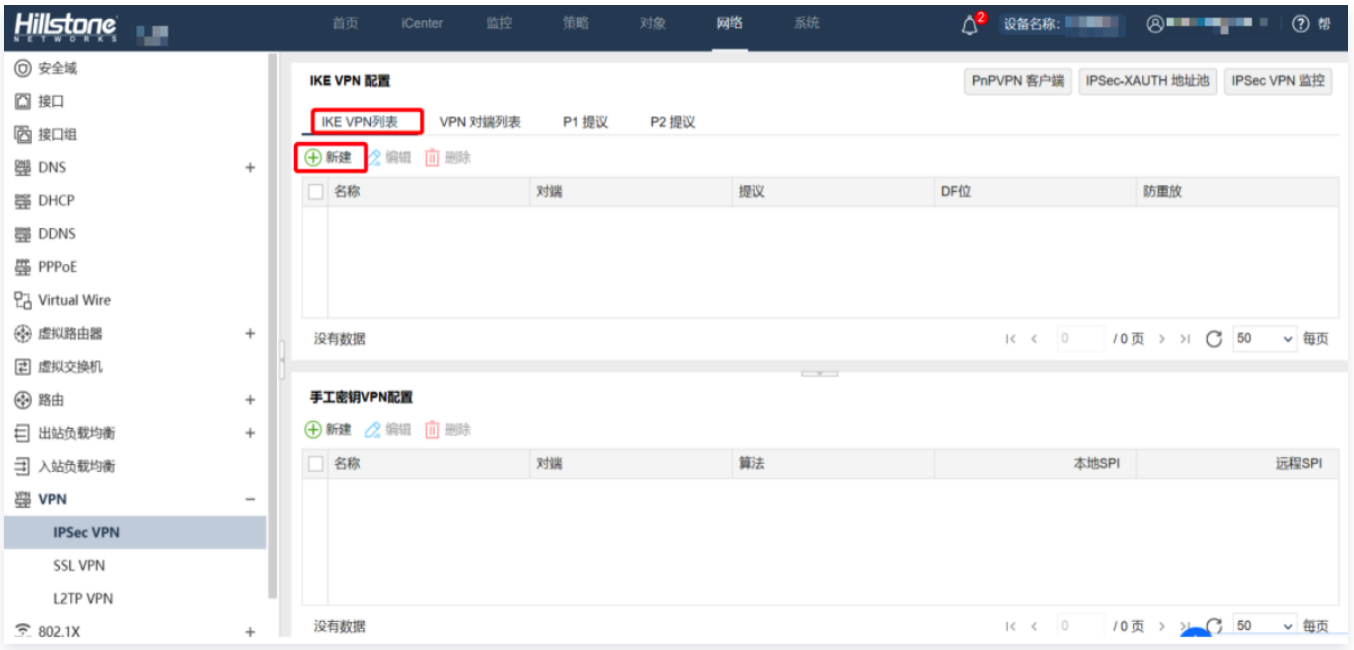
5. Select the **VPN Peer List** tab, and click **New**.



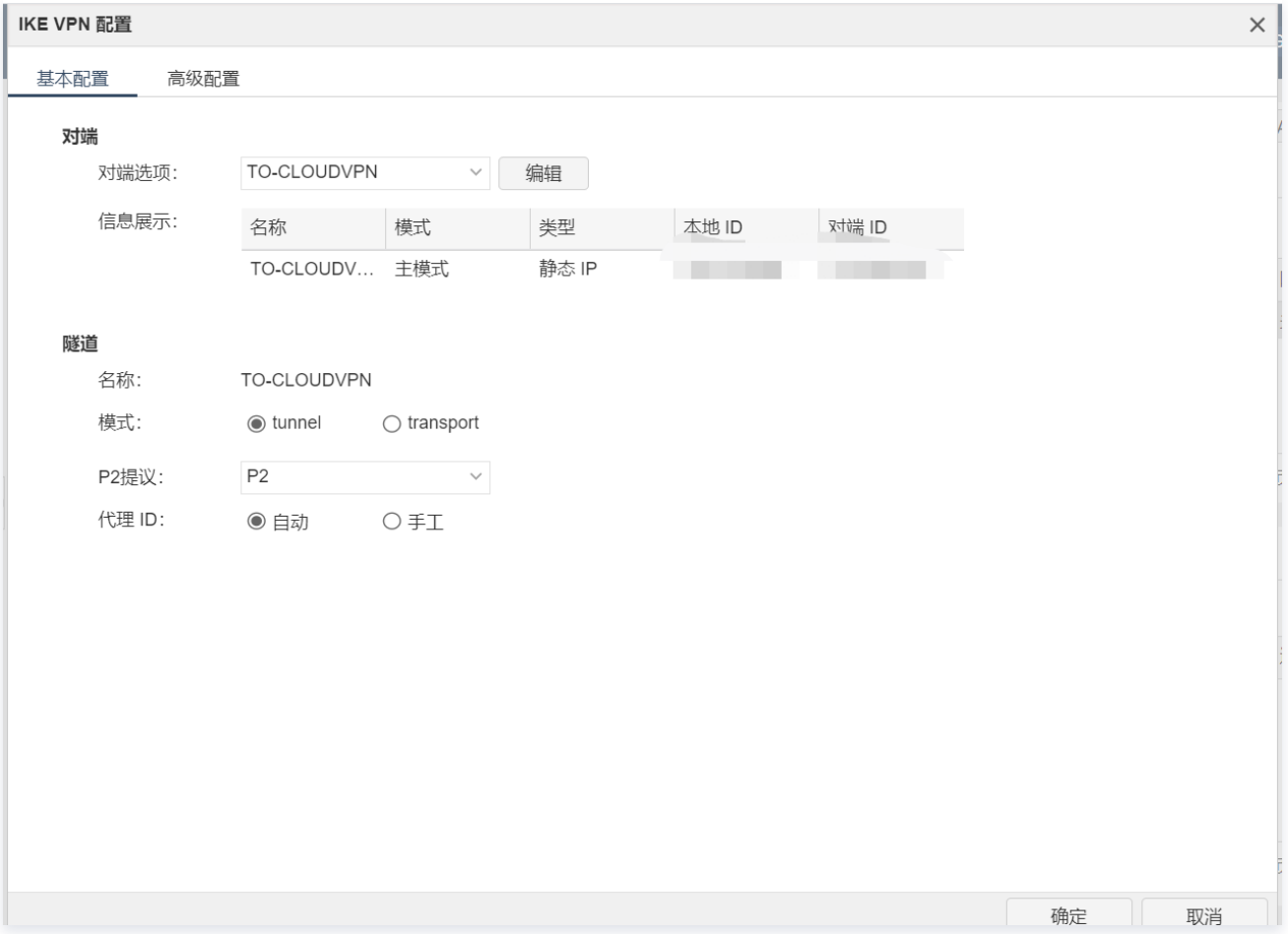
6. In the pop-up VPN peer **configurationinterface**, configure the relevant parameters of the VPN peer, and click **OK**.

- Name: Fill in the VPN peer name in the self-definition, for example, TO-CLOUDVPN
- Peer IP Address: Fill in the Public IP address of Tencent Cloud VPN Gateway
- Local IP: Fill in the Public IP address of the local IDC
- Peer IP: Fill in the Public IP address of the IDC VPN Gateway
- Proposal 1: Select the P1 proposal created in Step 2
- Preshared Key: Fill in the preshared key consistent with the basic configuration of the Tencent Cloud VPN channel, such as 123456 in this example

7. Select the **IKE VPN List** tab, and click **New**.



8. In the popped-up **IKE VPN Configuration** interface, perform the basic and advanced configuration of IKE VPN, and after completion, click **OK**.
   - Basic Configuration



   - Peer Option: Select the VPN peer created in Step 6
   - P2 Proposal: Select the P2 proposal created in Step 4
   - Proxy ID: Select **Automatic**

- Advanced Configuration: Check to set **Automatic Connection** as **Enabled**

9. Select **Network** > **Security Domain**, click **Create** to configure the security domain.

10. In the popped-up **Security Domain Configuration** interface, configure the following parameters, and after completion, click **OK**.
    - Security Domain Name: self-defined name, e.g., **VPNhub**
    - Virtual Router: by default selected as **trust-vr**

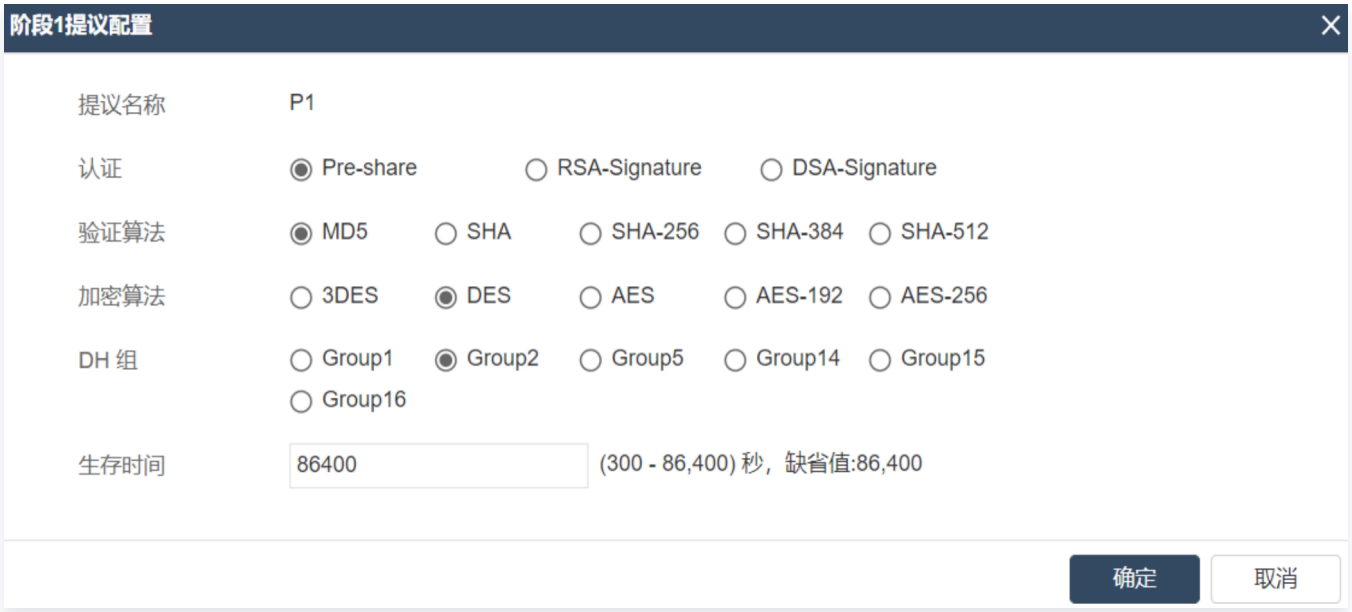
11. Select **Policy** > **Policy**, click **Create**, configure policies as per the following parameter guide, and after completion click **OK**.

- Source Information:
  - Security Domain: Select **trust**
  - Address: Fill in the **IDC local subnet and mask**, e.g., 172.16.0.0/16
- Destination Information:
  - Security Domain: Select **VPNHub**
  - Address: Fill in the **Tencent Cloud VPN backend subnet and mask**, e.g., 10.1.1.0/24
- Service: Select **any**
- Action: Select **Secure Connection**, **Tunnel** select the VPN peer created in Step 6, e.g., TO-CLOUDVPN, check **Two-way VPN Policy**

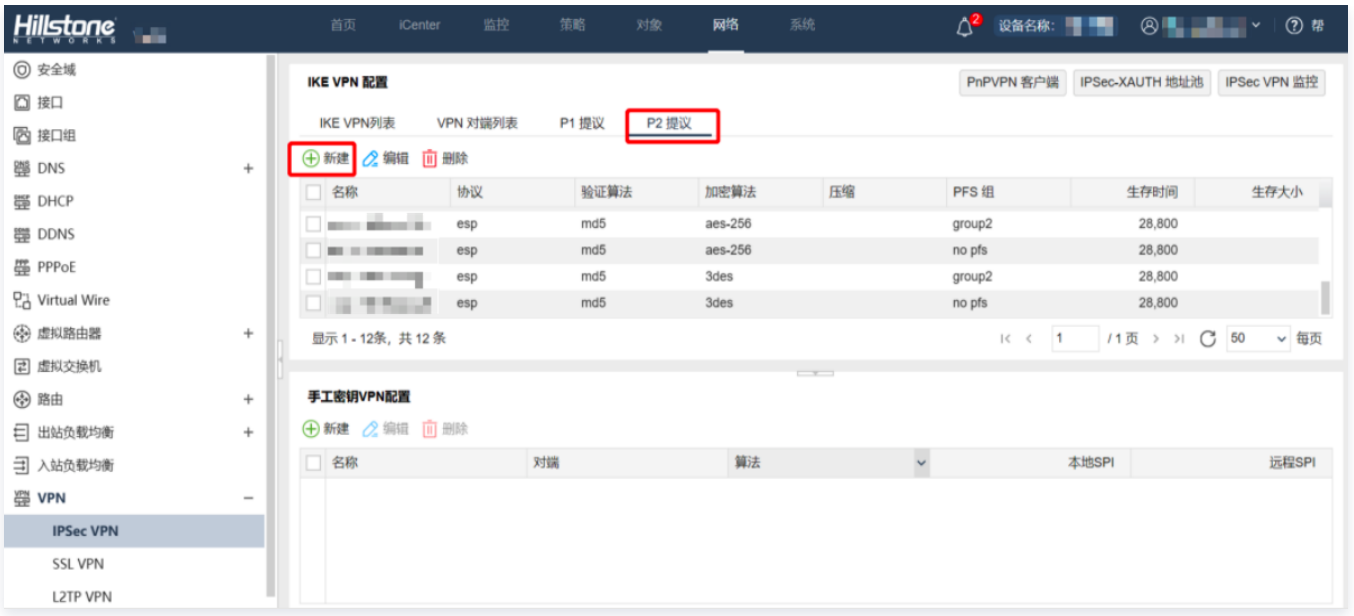
Applicable to route-based VPNs

1. Log in to the Hillstone firewall web interface, select **Network** > **VPN** > **IPsec VPN** > **P1 Proposal**. In the **P1 Proposal** interface, click **New**.

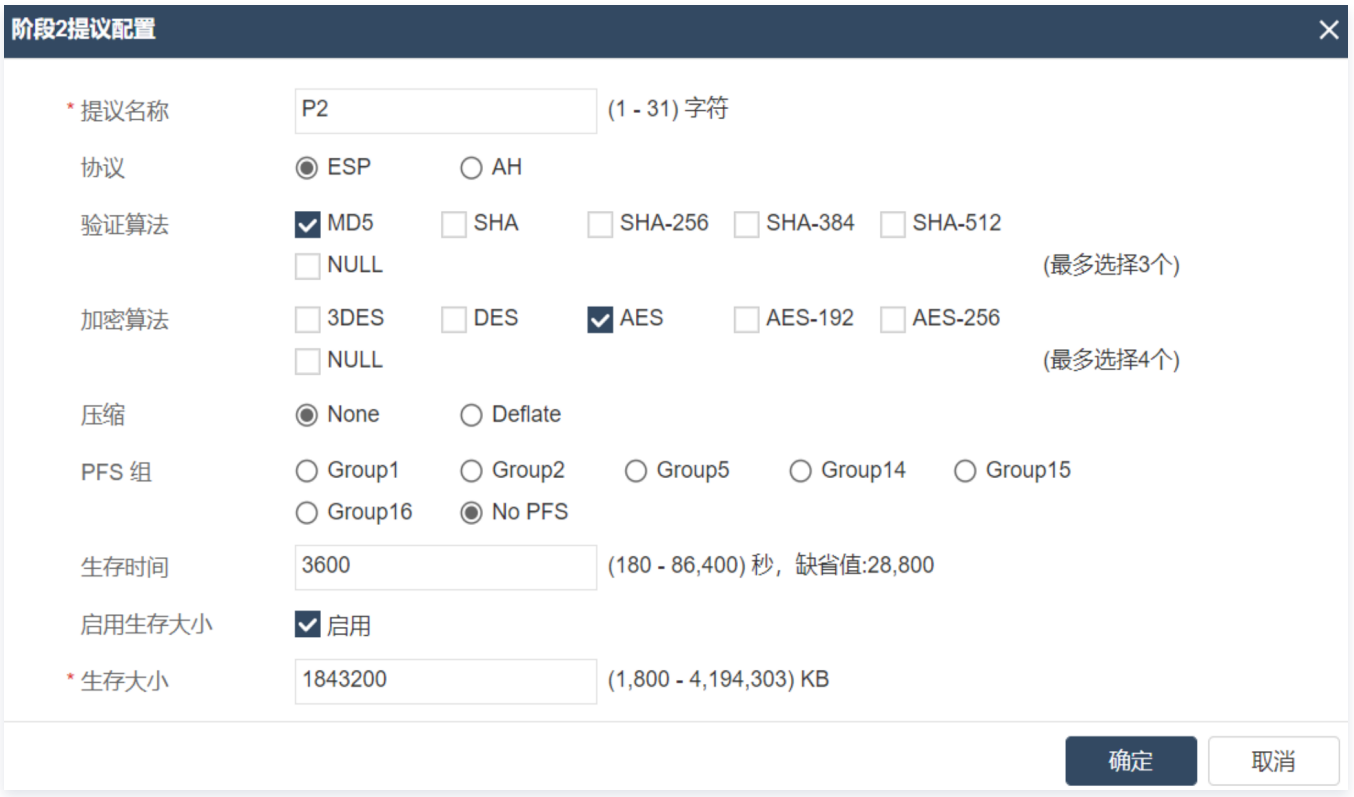
2. In the popped-up **Phase 1 Proposal Configuration** interface, configure the IKE protocol of IDC according to the IKE protocol information of Tencent Cloud VPN Connections, and click **OK**.



3. Select the **P2 Proposal** tab, and click **New**.



4. In the popped-up **Phase 2 Proposal Configuration** interface, configure the IPsec protocol of IDC according to Tencent Cloud VPN Connections' IPsec protocol information, and click **OK**

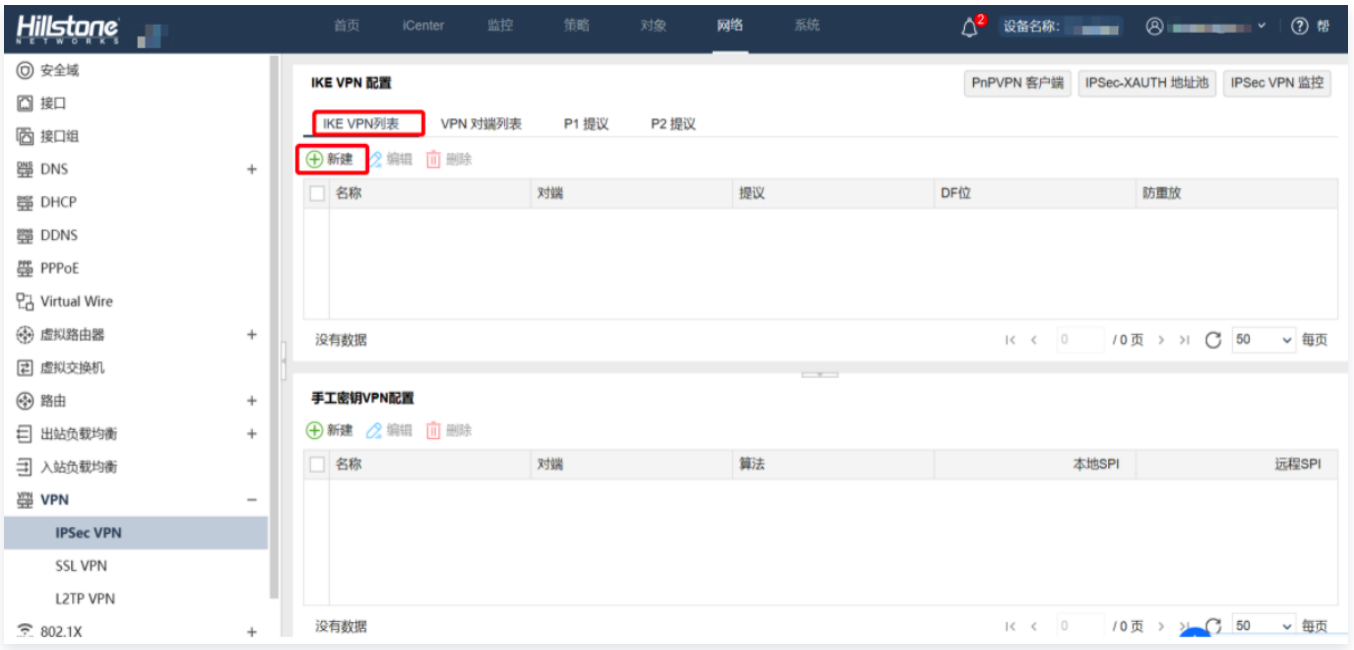


5. Select the **VPN Peer List** tab, and click **New**.

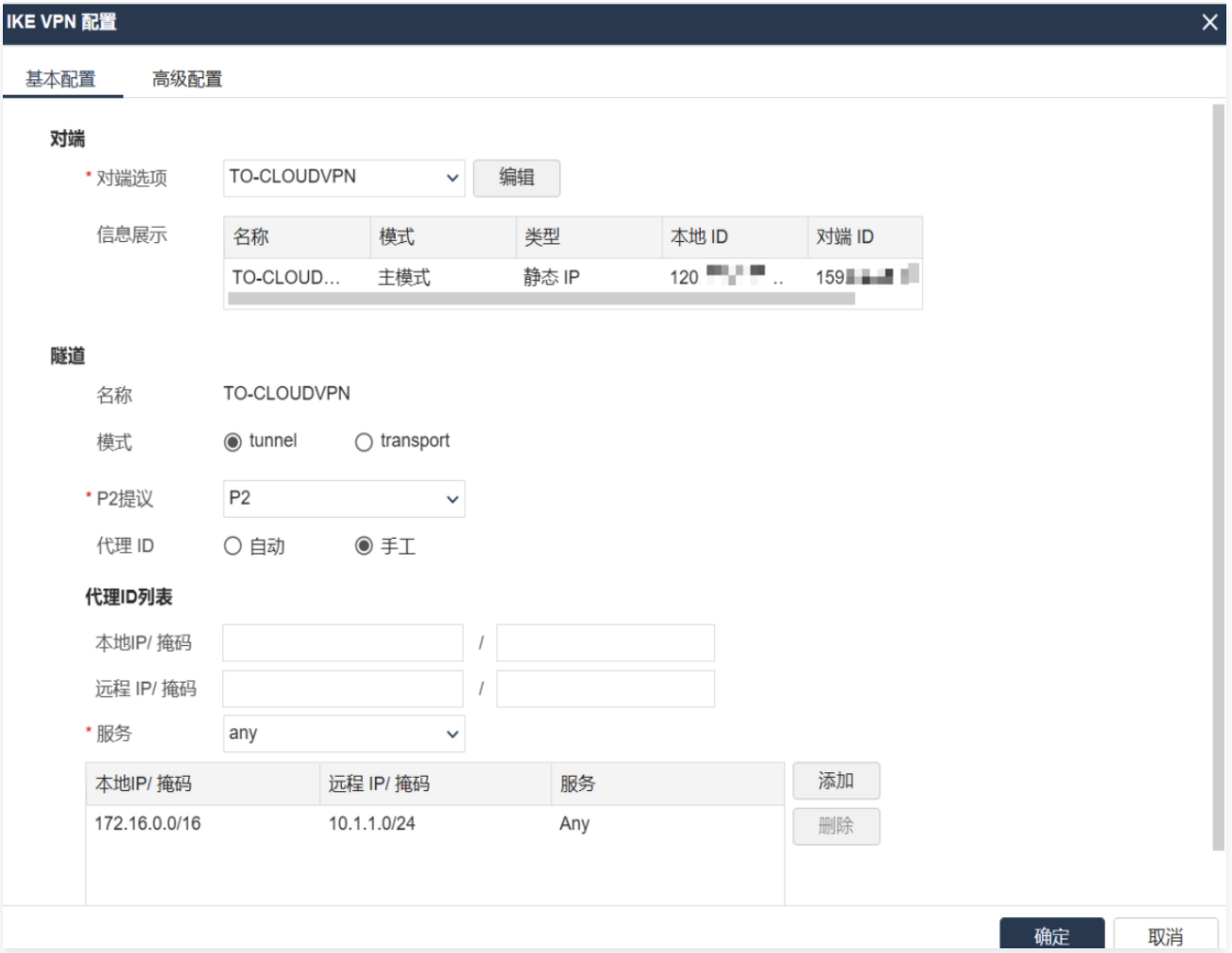
6. In the pop-up VPN Peer</1.1>**Configuration** interface, configure the related parameters of the VPN peer, and click **OK**.

- Name: Fill in the VPN peer name in the self-definition, for example, TO-CLOUDVPN
- Peer IP Address: Fill in the Public IP address of Tencent Cloud VPN Gateway
- Local IP: Fill in the Public IP address of the local IDC
- Peer IP: Fill in the Public IP address of the IDC VPN Gateway
- Proposal 1: Select the P1 proposal created in Step 2
- Preshared Key: Fill in the preshared key consistent with the basic configuration of the Tencent Cloud VPN channel, such as 123456 in this example

7. Select the **IKE VPN List** tab, and click **New**.



8. In the popped-up **IKE VPN Configuration** interface, perform the basic and advanced configuration of IKE VPN, and after completion, click **OK**.
   - Basic Configuration



   - Peer Option: Select the VPN peer created in Step 6
   - P2 Proposal: Select the P2 proposal created in Step 4

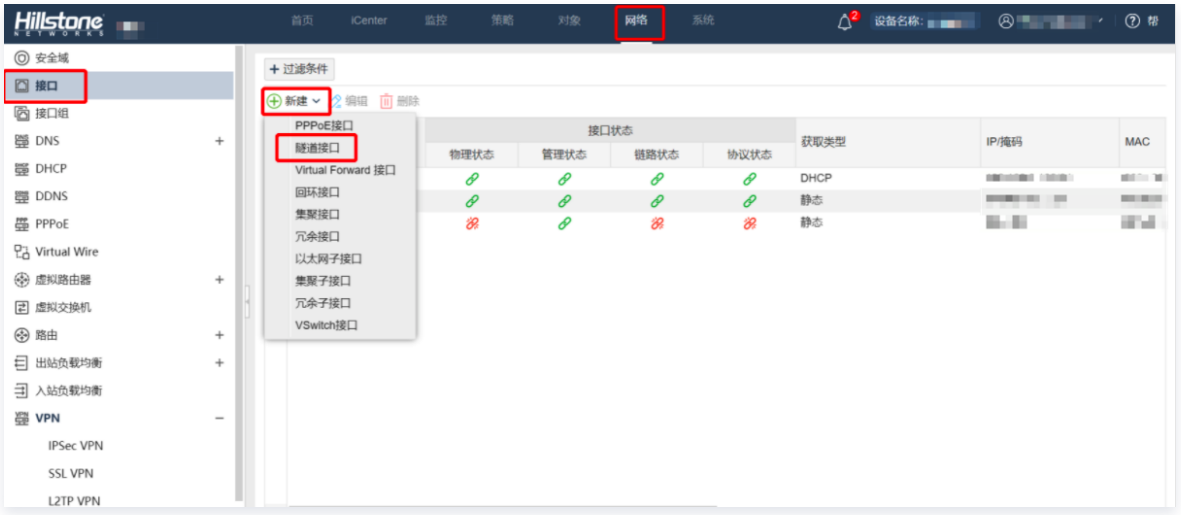
- Proxy ID: Select **Manual**. In the **Proxy ID List**, enter the private network segment of the local IDC in **Local IP/Mask**, and enter the private network segment of the Tencent Cloud VPC in **Remote IP/Mask**, then click **Add**
- Advanced Configuration: Check to set **Automatic Connection** as **Enabled**

9. Select **Network** > **Security Domain**, and click **New** to configure the security domain.

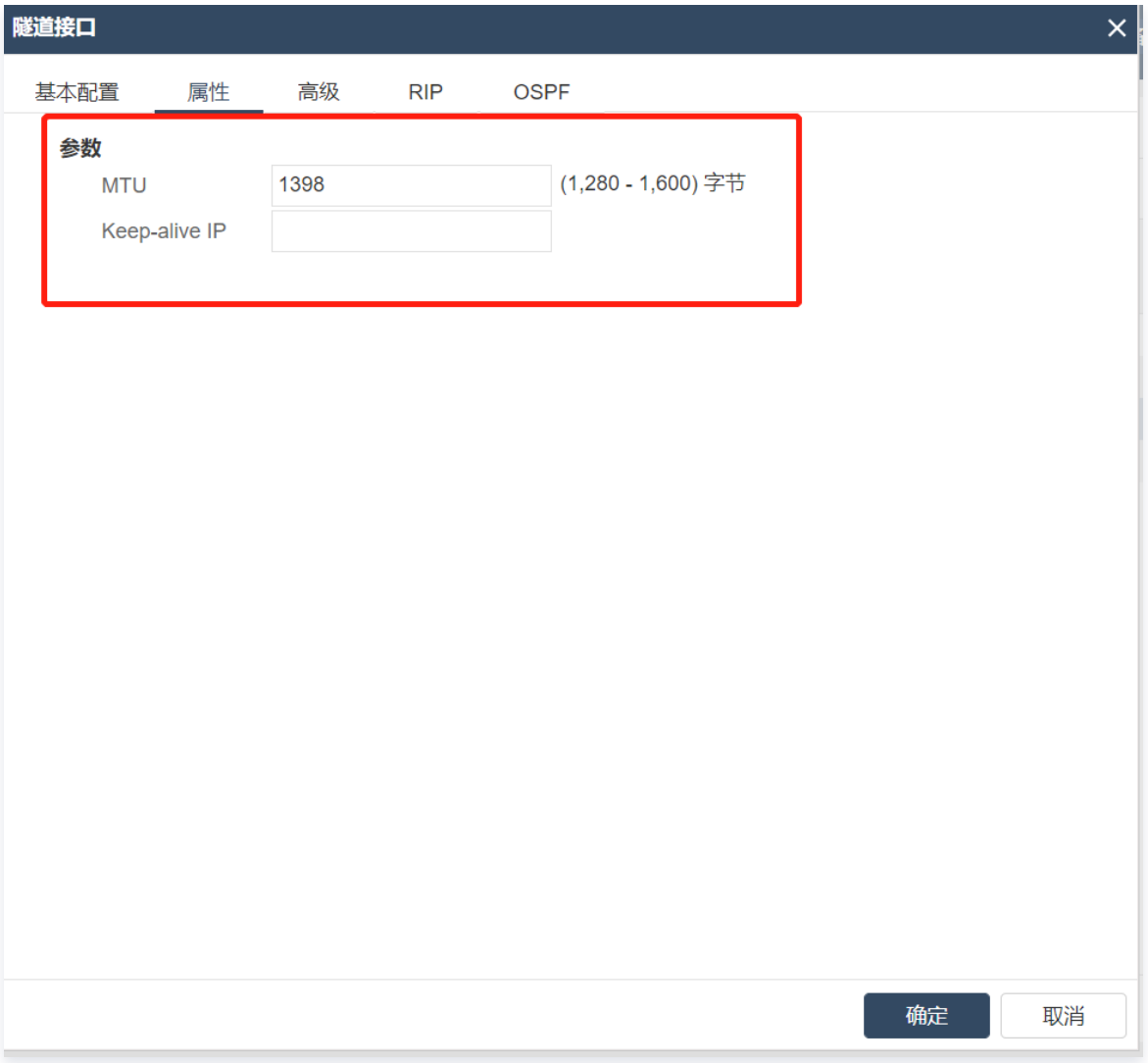
10. In the popped-up **Security Domain Configuration** interface, configure the following parameters, and after completion, click **OK**.
    - Security Domain Name: self-defined name, e.g., **VPNhub**

- Virtual Router: by default selected as **trust-vr**

11. Select **Network** > **Interface**, and click **New** > **Tunnel Interface**.



12. In the popped-up **Tunnel Interface** dialog box, configure the relevant parameters of the tunnel interface.
    - Interface Name: Enter **tunnelX**, where X ranges from 1 to 64, e.g., tunnel1
    - Security Domain: Select the security domain created in Step 10
    - Tunnel Type: Select **IPsec VPN**
    - VPN Name: Select the peer VPN name created in Step 6



13. Select **Policy** > **Policy**, click **Create** to configure the policy.

14. Select **Network** > **Routes**, click **New** to configure upstream and downstream routes separately. After completion, click **OK**.
    - Upstream Route: Set the destination address to the Tencent Cloud VPC IP range, and the next hop to the tunnel interface created in Step 12, in this case tunnel1.

- Downstream Route: Configure the firewall downstream interface route.

Juniper Firewall Configuration

Last updated: 2024-09-26 10:39:27

When establishing a connection from Tencent Cloud VPC to the user's IDC using IPsec VPN, after configuring the Tencent Cloud VPN gateway, you need to configure VPN settings on the gateway device at the local site of the user IDC. This document uses a Juniper firewall as an example to show how to configure VPN at the local site.

Note:
- Supports Juniper SRX Series Firewalls and vSRX Series Virtual Firewalls, all versions are supported.
- All IP addresses, interfaces, and other parameter values in this document are for example purposes only. Please use actual values during specific configuration.

Prerequisites

Please make sure you have created a VPN</1> within Tencent Cloud VPC within Tencent Cloud VPC<1> and completed the <3>VPN tunnel configuration</3>.

Data Preparations

The IPsec VPN configuration examples in this document are as follows:

Configuration Item			Sample value
Network Configuration	VPC information	Subnet CIDR block	10.1.1.0/24
		Public IP of the VPN gateway	159.xx.xx.242
	IDC information	Internal network CIDR	172.16.0.0/16
		Gateway Public IP	120.xx.xx.76
IPsec Connection Configuration	IKE Configuration	Version	IKEV1
		Identity Authentication Method	Pre-shared Key
		Encryption Algorithm	AES-128
		Authentication Algorithm	MD5
		Negotiation Mode	main
		Local ID	IP Address:120.xx.xx.76
		Remote ID	IP Address:159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec Configuration	Encryption Algorithm	AES-128
		Authentication Algorithm	MD5

		Message Encapsulation Mode	Tunnel
		Security Protocol	ESP
		PFS	disable
		IPsec sa Lifetime	3600s

Operation Steps

Applicable to VPNs based on SPD policy forwarding

1. log in to the firewall device command line interface.

```
ssh -p 22 root@172.16.0.1
# Use the SSH command to log in to the firewall command line interface
root@SRX1> configure
Entering configuration mode
# After logging in, it's in operational mode. Type "configure" to enter configuration
mode
[edit]
root@SRX1#
# "#" indicates that you have entered Configuration Mode
root@SRX1# commit
commit complete
# Changes made in Configuration Mode will not take effect immediately. You must use the
"commit" command for the changes to be saved and take effect
```

2. Configure firewall network interfaces, security zones, and address book information.

```
set interfaces ge-0/0/x unit 0 family inet address 172.16.0.1/16
# Define the IP address for internal interface ge-0/0/x. Please replace with actual
interface and IP
set interfaces ge-0/0/y unit 0 family inet address 120.xx.xx.76/30
# Define the IP address for external interface ge-0/0/y. Please replace with actual
interface and IP
set security zones security-zone trust interfaces ge-0/0/x.0
# Bind ge-0/0/x to the internal security zone (trust) connected to the internal
business zone. Please replace with actual interface
set security zones security-zone untrust interfaces ge-0/0/y.0  host-inbound-traffic
system-services ike
# Bind ge-0/0/y to the external security zone (untrust) connected to the external WAN,
and enable IKE service, indicating that this zone can establish a VPN
set security zones security-zone untrust address-book address vpn-peer_subnet
10.1.1.0/24
# Define the address book for the business addresses of the VPN peer to be accessed,
for subsequent access policy referencing. The name can be self-defined
set security zones security-zone trust address-book address vpn-local_subnet
172.16.0.0/16
```

```
# Define the local business address book for subsequent access policy referencing. The
name can be self-defined
```

3. Configure IKE policies.

```
set security ike proposal ike-proposal-cfgr authentication-method pre-shared-keys
# Define the IPSEC VPN authentication method (this example uses shared key mode: pre-
shared-keys). Note that "ike-proposal-cfgr" is a user-defined name and will be
referenced in subsequent settings
set security ike proposal ike-proposal-cfgr dh-group group2
# Define the IKE DH group
set security ike proposal ike-proposal-cfgr authentication-algorithm md5
# Define the IKE authentication algorithm
set security ike proposal ike-proposal-cfgr encryption-algorithm aes-128-cbc
# Define the IKE encryption algorithm
set security ike proposal ike-proposal-cfgr lifetime-seconds 86400
# Define the IKE lifetime, range: (180～86400 seconds)
set security ike policy ike-policy-cfgr mode main
# Specify the IKE mode
set security ike policy ike-policy-cfgr proposals ike-proposal-cfgr
# Define the IKE policies, you need to call the algorithm definitions named in the
previous steps
set security ike policy ike-policy-cfgr pre-shared-key ascii-text "TestPassword"
# Define the Key, note that the key cannot contain: "@","+","-","=" characters
```

4. Configure the IKE gateway, including the outgoing interface and protocol version.

```
set security ike gateway ike-gate-cfgr ike-policy ike-policy-cfgr
# Call the previously defined IKE policy naming
set security ike gateway ike-gate-cfgr address 159.xx.xx.242
# Define the gateway address information for IKE (the public address of the remote VPN)
set security ike gateway ike-gate-cfgr local-identity inet 120.xx.xx.76
set security ike gateway ike-gate-cfgr remote-identity inet 159.xx.xx.242
# Define the VPN identifier. You can use FQDN or IP addresses. In this example, use the
local and remote IP addresses
set security ike gateway ike-gate-cfgr external-interface ge-0/0/y
# Bind the VPN interface, which is the local public exit
set security ike gateway ike-gate-cfgr version v1-only
# Define the version of IKE, v1
```

5. Configure IPsec policies.

```
set security ipsec proposal ipsec-proposal-cfgr protocol esp
# Define the encryption protocol for the IPSEC phase
set security ipsec proposal ipsec-proposal-cfgr authentication-algorithm hmac-md5-96
# Define the authentication algorithm for the IPSEC phase
set security ipsec proposal ipsec-proposal-cfgr encryption-algorithm aes-128-cbc
# Define the encryption algorithm for the IPSEC phase
set security ipsec proposal ipsec-proposal-cfgr lifetime-seconds 3600
# Define the lifetime for the IPSEC phase (range: 180～86400)
```

```
set security ipsec policy ipsec-policy-cfgr proposals ipsec-proposal-cfgr
# Call the previously defined IPSEC algorithm definitions
```

6. Apply IPsec policies.

```
set security ipsec vpn ipsec-vpn-cfgr ike gateway ike-gate-cfgr
# Call the previously defined IKE gateway configuration
set security ipsec vpn ipsec-vpn-cfgr ike ipsec-policy ipsec-policy-cfgr
# Call the previously defined IPsec policies configuration
set security ipsec vpn ipsec-vpn-cfgr establish-tunnels immediately
# Configure VPN to establish the tunnel immediately, rather than waiting for traffic to
trigger
set routing-options static route 10.1.1.0/24 next-hop x.x.x.x
# For policy-based VPN, configure the route for the remote segment to be sent out from
the public network interface, x.x.x.x is the next hop address of the device's public
network interface
```

7. Configure outbound policies.

```
set security policies from-zone trust to-zone vpn policy trust-to-untrust_any_permit
match source-address vpn-local_subnet
set security policies from-zone trust to-zone vpn policy trust-to-untrust_any_permit
match destination-address vpn-peer_subnet
set security policies from-zone trust to-zone vpn policy trust-to-untrust_any_permit
match application any
set security policies from-zone untrust to-zone trust policy trust-to-
untrust_any_permit then permit tunnel ipsec-vpn ipsec-vpn-cfgr
set security policies from-zone untrust to-zone trust policy trust-to-
untrust_any_permit then permit tunnel pair-policy untrust-to-trust_any_permit
# Define access policies; this policy is for local network segments accessing VPN
peer’s business segments (trust to untrust), specify the IPSEC VPN Channel. Set
specific access permissions according to actual business access needs
```

8. Configure inbound policies.

```
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit
match source-address vpn-peer_subnet
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit
match destination-address vpn-local_subnet
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit
match application any
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit
then permit tunnel ipsec-vpn ipsec-vpn-cfgr
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit
then permit tunnel pair-policy trust-to-untrust_any_permit
# Define access policies; this policy is for remote VPN segments accessing local
business segments (untrust to trust), specify the IPSEC VPN Channel. Set specific
access permissions according to actual business access needs
```

9. Save configuration.

```
root@SRX1# commit
commit complete
# Changes made in Configuration Mode will not take effect immediately. You must use the
"commit" command for the changes to be saved and take effect
```

Applicable to routing-based VPN

1. log in to the firewall device command line interface.

```
ssh -p 22 root@172.16.0.1
# Use the SSH command to log in to the firewall command line interface
root@SRX1> configure
Entering configuration mode
# After logging in, it's in operational mode. Type "configure" to enter configuration
mode
[edit]
root@SRX1#
# "#" indicates that you have entered Configuration Mode
root@SRX1# commit
commit complete
# Changes made in Configuration Mode will not take effect immediately. You must use the
"commit" command for the changes to be saved and take effect
```

2. Configure firewall network interfaces, security zones, and address book information.

```
set interfaces ge-0/0/x unit 0 family inet address 172.16.0.1/16
# Define the IP address for internal interface ge-0/0/x. Please replace with actual
interface and IP
set interfaces ge-0/0/y unit 0 family inet address 120.xx.xx.76/30
# Define the IP address for external interface ge-0/0/y. Please replace with actual
interface and IP
set interfaces st0 unit 0 family inet mtu 1398
# Define the tunnel interface. By default, no IP address is set. The parameter after
the unit of the tunnel interface needs to be specified. One unit number can bind one
VPN tunnel. The sequence number range: 0-16385. Also, set the tunnel interface MTU to
1398
set security zones security-zone trust interfaces ge-0/0/x.0
# Bind ge-0/0/x to the internal security zone (trust) connected to the internal
business zone
set security zones security-zone untrust interfaces ge-0/0/y.0  host-inbound-traffic
system-services ike
# Bind ge-0/0/y to the external security zone (untrust), connect to the external WAN,
and enable IKE service, indicating that this zone can establish a VPN
set security zones security-zone vpn interfaces st0.0
# Bind the channel interface to the VPN zone (vpn) as a logical channel for connecting
the IPSEC VPN, used for subsequent routing and access policies
set security zones security-zone vpn address-book address vpn-peer_subnet 10.1.1.0/24
```

```
# Define the address book for the business addresses of the VPN peer to be accessed,
for subsequent access policy referencing. The name can be self-defined
set security zones security-zone trust address-book address vpn-local_subnet
172.16.0.0/16
# Define the local business address book for subsequent access policy referencing. The
name can be self-defined
```

3. Configure IKE policies.

```
set security ike proposal ike-proposal-cfgr authentication-method pre-shared-keys
# Define the IPSEC VPN authentication method (this example uses shared key mode: pre-
shared-keys). Note that "ike-proposal-cfgr" is a user-defined name and will be
referenced in subsequent settings
set security ike proposal ike-proposal-cfgr dh-group group2
# Define the IKE DH group
set security ike proposal ike-proposal-cfgr authentication-algorithm md5
# Define the IKE authentication algorithm
set security ike proposal ike-proposal-cfgr encryption-algorithm aes-128-cbc
# Define the IKE encryption algorithm
set security ike proposal ike-proposal-cfgr lifetime-seconds 86400
# Define the IKE lifetime, range: (180-86400 seconds)
set security ike policy ike-policy-cfgr mode main
set security ike policy ike-policy-cfgr proposals ike-proposal-cfgr
set security ike policy ike-policy-cfgr pre-shared-key ascii-text "TestPassword"
# Define the IKE policies, specify the mode and the key, you need to call the algorithm
definitions named in the previous steps. Note that the key cannot contain the
characters: "@", "+", "-", "="
```

4. Configure the IKE gateway, including the outgoing interface and protocol version.

```
set security ike gateway ike-gate-cfgr ike-policy ike-policy-cfgr
# Call the previously defined IKE policy naming
set security ike gateway ike-gate-cfgr address 159.xx.xx.242
# Define the gateway address information for IKE (the public address of the remote VPN)
set security ike gateway ike-gate-cfgr local-identity inet 120.xx.xx.76
set security ike gateway ike-gate-cfgr remote-identity inet 159.xx.xx.242
Define the VPN identifier. You can use FQDN or IP addresses. In this example, use the
remote and local IP addresses
set security ike gateway ike-gate-cfgr external-interface ge-0/0/y
# Bind the VPN interface, which is the local public exit
set security ike gateway ike-gate-cfgr version v1-only
# Define the version of IKE, v1
```

5. Configure IPsec policies.

```
set security ipsec proposal ipsec-proposal-cfgr protocol esp
# Define the encryption protocol for the IPSEC phase
set security ipsec proposal ipsec-proposal-cfgr authentication-algorithm hmac-md5-96
# Define the authentication algorithm for the IPSEC phase
set security ipsec proposal ipsec-proposal-cfgr encryption-algorithm aes-128-cbc
```

```
# Define the encryption algorithm for the IPSEC phase
set security ipsec proposal ipsec-proposal-cfgr lifetime-seconds 3600
# Define the lifetime for the IPSEC phase
set security ipsec policy ipsec-policy-cfgr proposals ipsec-proposal-cfgr
# Call the previously defined IPSEC algorithm definitions
set security ipsec vpn ipsec-vpn-cfgr ike proxy-identity local 172.16.0.0/16
set security ipsec vpn ipsec-vpn-cfgr ike proxy-identity remote 10.1.1.0/24
Set the TS (Traffic Selector) or SPD configuration, default is 0.0.0.0/0. If the peer
also specifies a segment, it needs to match the peer
set security ipsec vpn ipsec-vpn-cfgr bind-interface st0.0
# Bind the VPN tunnel interface
```

6. Apply IPsec policies.

```
set security ipsec vpn ipsec-vpn-cfgr ike gateway ike-gate-cfgr
# Call the previously defined IKE gateway configuration
set security ipsec vpn ipsec-vpn-cfgr ike ipsec-policy ipsec-policy-cfgr
# Call the previously defined IPsec policies configuration
set security ipsec vpn ipsec-vpn-cfgr establish-tunnels immediately
# Configure VPN to establish the tunnel immediately, rather than waiting for traffic to
trigger
set routing-options static route 10.1.1.0/24 next-hop st0.0
# Configure the remote Business IP Segment, forward through the Virtual Channel
Interface
```

7. Configure outbound policies.

```
set security policies from-zone trust to-zone vpn policy trust-to-vpn_any_permit match
source-address vpn-local_subnet
set security policies from-zone trust to-zone vpn policy trust-to-vpn_any_permit match
destination-address vpn-peer_subnet
set security policies from-zone trust to-zone vpn policy trust-to-vpn_any_permit match
application any
set security policies from-zone trust to-zone vpn policy trust-to-vpn_any_permit then
permit
# Define access policies; this policy is for local network segments accessing VPN
peer's business segments (trust to vpn). Set specific access permissions according to
actual business access needs
```

8. Configure inbound policies.

```
set security policies from-zone vpn to-zone trust policy vpn-to-trust_any_permit match
source-address vpn-peer_subnet
set security policies from-zone vpn to-zone trust policy vpn-to-trust_any_permit match
destination-address vpn-local_subnet
set security policies from-zone vpn to-zone trust policy vpn-to-trust_any_permit match
application any
set security policies from-zone vpn to-zone trust policy vpn-to-trust_any_permit then
permit
```

```
# Define access policies; this policy is for VPN remote segments accessing local
business segments (vpn to trust). Set specific access permissions according to actual
business access needs
```

9. Save configuration.

```
root@SRX1# commit
commit complete
Changes made in Configuration Mode will not take effect immediately. You must use the
"commit" command for the changes to be saved and take effect
```

NSFOCUS Firewall Configuration

Last updated: 2024-09-26 10:39:55

When establishing a connection from Tencent Cloud VPC to User IDC using IPsec VPN, after configuring the Tencent Cloud VPN gateway, you also need to configure the VPN on the gateway device at the local site of the User IDC. This document uses the NSFOCUS firewall as an example to demonstrate how to configure VPN at the local site.

Note:

- This document uses the NFNX3-V2000TX model with firewall version 603.168 for demonstration. Other versions may have slight interface differences, but the overall configuration logic is consistent.
- This document only supports the configuration of the IKEv1 protocol.
- All IP addresses, interfaces, and other parameter values in this document are for example purposes only. Please use actual values when configuring.

Prerequisites

Please ensure you have created a VPN inside Tencent Cloud VPC and completed the VPN tunnel configuration.

Data Preparations

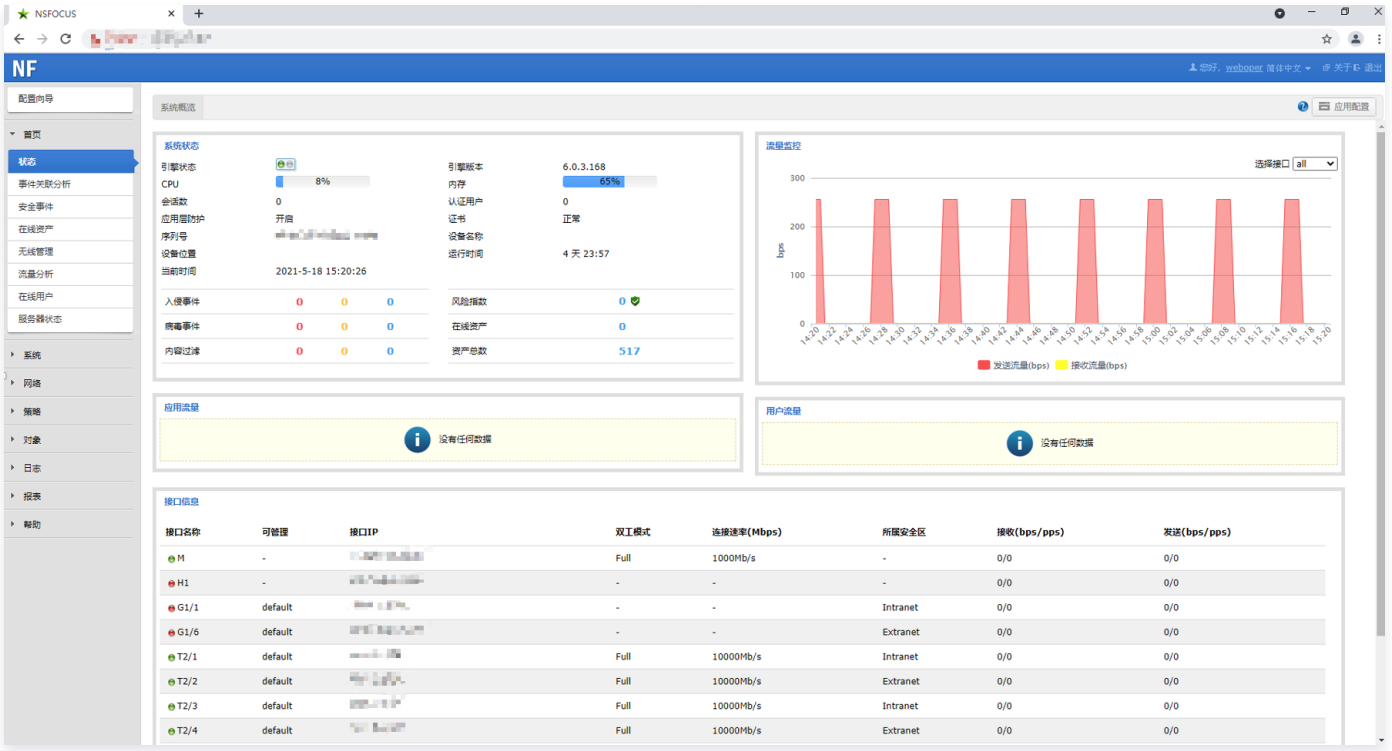
The IPsec VPN configuration data example in this document is as follows:

Configuration Item			Sample value
Network Configuration	VPC information	Subnet CIDR block	10.1.1.0/24
		Public IP of the VPN gateway	159.xx.xx.242
	IDC information	Intranet CIDR block	172.16.0.0/16
		Public IP of the gateway	120.xx.xx.76
IPsec Connection Configuration	IKE Configuration	Version	IKEV1
		Identity Authentication Method	Pre-shared Key
		PSK	tencent@123
		Encryption Algorithm	AES-128
		Authentication Algorithm	MD5
		Negotiation Mode	main
		Local ID	IP Address:120.xx.xx.76
		Remote ID	IP Address:159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec Configuration	Encryption Algorithm	AES-128
		Authentication Algorithm	MD5

		Message Encapsulation Mode	Tunnel
		Security Protocol	ESP
		PFS	disable
		IPsec SA Lifetime (s)	3600s

Operation Steps

1. Use weboper to log in to the NSFOCUS Management Interface.



2. Select **Networking** > **Interfaces** from the left sidebar, then click **New** on the IPsec Interfaces page.
3. On the **New** page, configure the IPsec-related information, then click **Confirm**.

- Interface Type: Select VPN.
- Subtype: Select IPsec.
- Interface Name: Cannot be modified, the system fills it by default.
- Secure Zone: Select **DMZ**.
  To ensure that data from the IPsec interface to the intranet is not blocked by security policies, keep the default option **DMZ**.
- IPv4: Select the local VPC segment, i.e., the example value 10.1.1.1/24 of the VPC subnet CIDR during **Data Preparations**.

4. Select **Networking** > **IPSEC** > **IPSEC Tunnel** from the left sidebar.
5. In the **Phase 1** tab, configure the IKE protocol information for the IDC side based on Tencent Cloud VPN Connections' IKE protocol information.

*Required items.

- Tunnel Name: Enter the tunnel name.
- Local Interface: Select the planned local interface.
- HA Line: Select the HA line.
- IP Addresses: Select the IP address of the server where IPsec is located.
- Client Type: Select **Gateway Client**.
- Authentication Method: Select **Preshared Key**.
- Preshared Key: Set the preshared key.

6. (Optional) Advanced Options Configuration.
   If you have higher requirements for IPsec policies, such as authentication algorithms, encryption algorithms, ISAKMP-SA lifetime, etc., you need to perform advanced configurations.

This section only provides a description of the main parameters.

- Local/Peer ID Type:
  - IPv4: Enter the address in standard IPv4 format.
  - Domain Name: The character count should be less than or equal to 30 characters and can only include letters, numbers, underscores, periods, and @.
  - Username: Currently, only user email addresses are supported, for example: xxxx@nsfocus.com.
- DH Group: The DH group used by the IPsec VPN tunnel.
- Authentication Algorithm: Specify the security authentication algorithm, such as MD5.
- Encryption Algorithm: Specify the encryption algorithm.

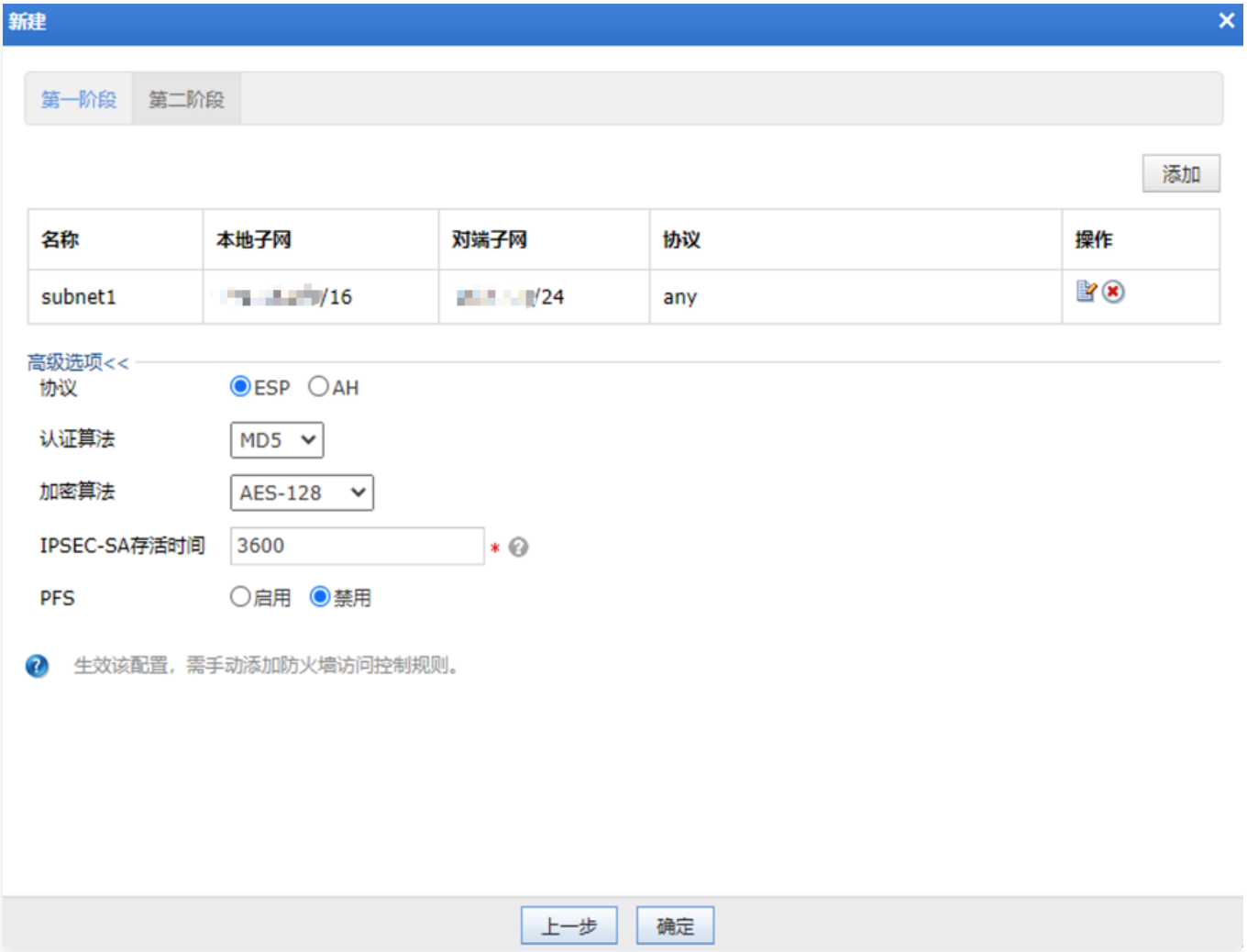
> **Note**
> If the authentication method in Step 5 selected **Preshared Key**, options include DES, 3DES, AES-128, AES-192, AES-256, and BLOWFISH. Please select according to actual needs.

7. After configuring the **Phase 1**, click **Next**.
8. In the **Phase 2** tab, configure the IPsec protocol on the IDC side according to the Tencent Cloud VPN Connections' IPsec protocol information.

> **Note**
> There should be no overlapping subnets.

8.1 In the **Phase 2** tab, click **Add**.
8.2 In **Local Subnet**, enter the local IDC subnet and mask, for example, 172.16.0.0/16.
8.3 In **Peer Subnet**, enter the Tencent Cloud VPN backend subnet and mask, for example, 10.1.1.0/24.
8.4 Select **Protocol** as **any**.
8.5 Advanced Configuration.
- Select **Protocol** as **ESP**
- Select **Authentication Algorithm** as **MD5**
- Select **Encryption Algorithm** as **AES-128**
- Set **IPSEC-SA Lifetime** to 3600
- Set **PFS** to disabled

8.6 Click **OK**.



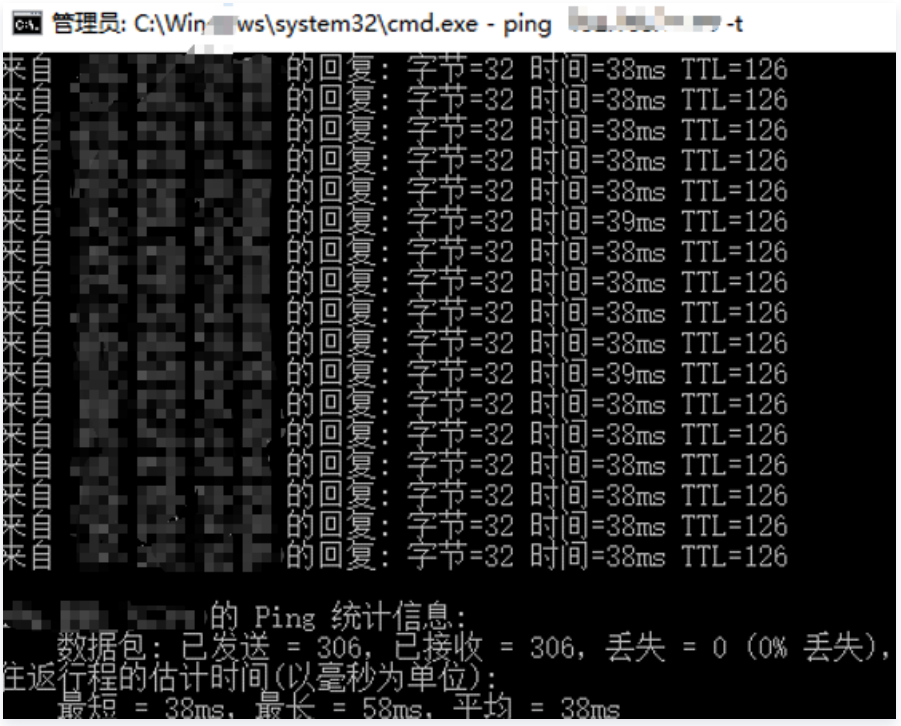
9. Test the connectivity between NSFOCUS and Tencent Cloud.
- After NSFOCUS and Tencent Cloud VPN establish the tunnel, a corresponding tunnel information entry is automatically generated on the NSFOCUS side.

隧道名	本地IP	对端地址	本地子网	对端子网	当前隧道状态	建立时间
tencent					ipsec隧道已建立	2021-05-06 10:45:05
tencent					ipsec隧道已建立	2021-05-06 10:45:05

- You can view the connection status on the Tencent Cloud VPN side.

ID/名称	监控	状态	对端网关	所属网络	预共享密钥	操作
ceshi		已联通	cgw	vpc 测试		重置 更多

- On the NSFOCUS side, use the Ping command to ping the CVM within the Tencent Cloud VPC, and it should pass normally.



Configuring a Cisco Firewall

Last updated: 2024-09-26 10:40:10

When using IPsec VPN to establish a connection from Tencent Cloud VPC to a user IDC, after configuring the Tencent Cloud VPN gateway, you also need to configure the VPN on the gateway device at the user's local IDC site. This document uses a Cisco firewall as an example to introduce how to configure the VPN at the local site.

Note

- This document provides general configuration for Cisco ASA series firewalls, supported by all versions.
- All IP addresses, interfaces, and other parameter values in this document are for illustration purposes only. Please replace them with actual values during configuration.

Prerequisites

Please ensure that you have created a VPN within Tencent Cloud VPC and completed the VPN tunnel configuration.

Data Preparations

An example of IPsec VPN configuration data in this document is as follows:

Configuration Item			Sample value
Network Configuration	VPC information	Subnet CIDR block	10.1.1.0/24
		Public IP of the VPN gateway	159.xx.xx.242
	IDC information	Intranet CIDR	172.16.0.0/16
		Public IP of the gateway	120.xx.xx.76
IPsec Connection Configuration	IKE Configuration	Version	IKEV1
		Identity Authentication Method	Pre-shared Key
		PSK	tencent@123
		Encryption Algorithm	AES-128
		Authentication Algorithm	MD5
		Negotiation Mode	main
		Local ID	IP Address:120.xx.xx.76
		Remote ID	IP Address:159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec Configuration	Encryption Algorithm	AES-128
		Authentication Algorithm	MD5
		Message Encapsulation Mode	Tunnel
		Security Protocol	ESP

		PFS	disable
		IPsec SA Lifetime (s)	3600s
		IPsec SA Lifetime (KB)	1843200KB
Firewall Configuration	Interface Information	Nameif	outside

Operation Steps

Applicable to VPNs forwarded based on SPD policy (IKEv1)

1. Log in to the firewall device command interface.

```
   ssh -p admin@10.XX.XX.56

# Log in to the firewall configuration interface via SSH command.

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# Enter account password to access user mode.

ASA>
ASA> en
Password:

# Enter 'enable' and the configured enable password to access privileged mode. This
mode supports viewing only.

ASA# conf t
ASA(config)#

# Type "config ter" to enter global mode for firewall configuration.
```

2. Configure the firewall interface.
   Configure the firewall interface to connect to Tencent Cloud End in global mode.

```
   interface GigabitEthernet0/0
   nameif outside  # Define the security domain name of the port.
   security-level 0  # Define the security domain level of the port.
   ip address 120.XX.XX.76 255.255.255.252  # Configure the public IP address of the
local VPN tunnel.
```

3. Configure ISAKMP policy.

```
   crypto ikev1 enable outside  # Enable IKE on the external interface.
   crypto ikev1 policy 10  # Define parameters for the first stage of IKEv1
negotiation, with a sequence number of 10. The smaller the number, the higher the
priority, ranging from 1 to 65535.
   authentication pre-share  # Configure the authentication method as a pre-shared key.
   encryption AES-128  # Configure the encryption algorithm for the data packet
encapsulation of the first stage of negotiation, default is AES-128.
   hash MD5  # Specify the hashing algorithm for IKE policy as MD5, default is SHA.
   group 2  # Specify the Diffie-Hellman group for the IKE policy as group 2, default
is group 2
   lifetime 86400  # Specify the SA lifetime, default is 86400 seconds.
```

4. Configure the pre-shared password.

```
   tunnel-group 159.XX.XX.242 type ipsec-l2l  # Create an IPsec tunnel group, type is
point-to-point.
   tunnel-group 159.XX.XX.242 ipsec-attributes  # Configure the tunnel group attributes
and specify the pre-shared key.
   ikev1 pre-shared-key tencent@123  # The key can be 1-128 characters, letters,
numbers, or strings.
```

5. Configure IPsec security protocol.

```
   crypto ipsec ikev1 transform-set TS esp-aes esp-md5-hmac  # Specify the encryption
algorithm and hash algorithm for the IPsec Phase 2 negotiation.
```

6. Configure ACL.

```
   access-list INTERESTING extended permit ip 172.XX.XX.0 255.255.0.0 10.1.1.0
255.255.255.0  # Configure ACL to capture data flow on the VPN channel.
```

7. Configure IPsec policies.

```
   crypto map CMAP 1 match address INTERESTING  # Invoke the ACL to allow data packets
from source or destination segments that meet the ACL to flow through the VPN channel.
   crypto map CMAP 1 set peer 159.XX.XX.242  # Forward the traffic protected by IPsec
to the peer VPN public address, in this case, Tencent Cloud VPN public address.
   crypto map CMAP 1 set ikev1 transform-set TS  # Configure the IKEv1 protocol for the
encryption map entry.
   crypto map CMAP 1 set security-association lifetime seconds 3600  # Configure the
lifetime of the encryption key.
```

8. Enable IPsec policies.

```
   crypto map CMAP interface outside  # Apply the configured encryption map to the
external interface.
```

```
```

9. Configure static routing.

```
   route outside 10.1.1.0 255.255.255.0 159.XX.XX.242 1  # Route the data segment to be
encrypted to the IPsec tunnel and configure the next hop as the public IP address of
the VPN tunnel peer.
```

10. Test VPN connectivity.
    Execute the ping command to test VPN connectivity.

Suitable for route-based VPN (IKEv1)

1. Log in to the firewall device command interface.

```
   ssh -p admin@10.XX.XX.56

# Log in to the firewall configuration interface via SSH command.

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# Enter account password to access user mode.

ASA>
ASA> en
Password:

# Enter 'enable' and the configured 'enable password' to access privileged mode. This
mode supports viewing only.

ASA# conf t
ASA(config)#

# Type "config ter" to enter global mode for firewall configuration.
```

2. Configure the firewall interface.
   Configure the firewall interface to connect to Tencent Cloud End in global mode

```
   interface GigabitEthernet0/0
   nameif outside  # Define the security domain name of the port.
   security-level 0  # Define the security domain level of the port.
   ip address 120.XX.XX.76 255.255.255.252  # Configure the public IP address of the
local VPN tunnel.
```

3. Configure ISAKMP policy.

```
    crypto ikev1 policy 10  # Define parameters for the first stage of IKEv1
negotiation, with a sequence number of 10. The smaller the number, the higher the
priority, ranging from 1 to 65535.
    authentication pre-share  # Configure the authentication method as a pre-shared
key.
    encryption AES-128  # Configure the encryption algorithm for the data packet
encapsulation of the first stage of negotiation, default is AES-128.
    hash MD5  # Specify the hashing algorithm for IKE policy as MD5, default is SHA.
    group 2  # Specify the Diffie-Hellman group for the IKE policy as group 2, default
is group 2
    lifetime 86400  # Specify the SA lifetime, default is 86400 seconds.
```

4. Configure the pre-shared password.

```
   tunnel-group 159.XX.XX.242 type ipsec-l2l  # Create an IPsec tunnel group, type is
point-to-point.
   tunnel-group 159.XX.XX.242 ipsec-attributes  # Configure the tunnel group attributes
and specify the pre-shared key.
    ikev1 pre-shared-key tencent@123  # The key can be 1-128 characters, letters,
numbers, or strings.
```

5. Configure IPsec security protocol.

```
   crypto ipsec ikev1 transform-set TS esp-aes esp-md5-hmac  # Specify the encryption
algorithm and hash algorithm for the IPsec Phase 2 negotiation.
```

6. Configure IPsec policies.

```
   crypto ipsec profile PROFILE1
   set ikev1 transform-set TS  # Specify the IKEv1 IPsec security proposals for the
crypto map entry
   set security-association lifetime kilobytes 1843200  # Set the number of bytes that
can be transferred between VPNs during the SA lifetime.
   set security-association lifetime seconds 3600  # Set the lifetime of the encryption
key. The default kilobyte value is 4,608,000; the default lifetime is 28,800 seconds.
```

7. Enable IPsec policies.

```
   interface Tunnel100
   tunnel source interface outside  # Configure the update source of the VPN as the
outside interface.
   tunnel destination 159.XX.XX.242  # Configure the public IP address of the remote
VPN, which is the Tencent Cloud VPN public IP address in this case.
   tunnel mode ipsec ipv4  # Configure the protocol used by the tunnel interface.
   tunnel protection ipsec profile PROFILE1  # Apply the IPsec policy to protect the
data passing through the tunnel interface.
```

8. Configure static routing.

```
   route vti 10.1.1.0 255.255.255.0 159.XX.XX.242  # Direct the data packets to be
encrypted to the tunnel interface.
```

9. Test VPN connectivity.
   Execute the ping command to test VPN connectivity.

Suitable for SPD policy-based routing VPN (IKEv2)

1. Log in to the firewall device command interface.

```
   ssh -p admin@10.XX.XX.56

# Log in to the firewall configuration interface via SSH command.

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# Enter account password to access user mode.

ASA>
ASA> en
Password:
```

```
# Enter 'enable' and the configured 'enable password' to access privileged mode. This
mode supports viewing only.

ASA# conf t
ASA(config)#

# Type "config ter" to enter global mode for firewall configuration.
```

2. Configure the firewall interface.
   Configure the firewall interface to connect to Tencent Cloud End in global mode.

```
   interface GigabitEthernet0/0
   nameif outside  # Define the security domain name of the port.
   security-level 0  # Define the security domain level of the port.
   ip address 120.XX.XX.76 255.255.255.252  # Configure the public IP address of the
local VPN tunnel.
```

3. Configure ISAKMP policy.

```
   crypto ikev2 enable outside  # Enable IKEv2 on the external interface.
   crypto ikev2 policy 10  # Define parameters for the first stage of IKEv2
negotiation, with a sequence number of 10. The smaller the number, the higher the
priority, ranging from 1 to 65535.
   authentication pre-share  # Configure the authentication method as a pre-shared key.
   encryption AES-128  # Configure the encryption algorithm for the data packet
encapsulation of the first stage of negotiation, default is AES-128.
   integrity MD5  # Specify the hashing algorithm for the IKE policy as MD5, default is
SHA.
   group 2  # Specify the Diffie-Hellman group for the IKE policy as group 2, default
is group 2.
   prf sha  # Set the encryption algorithm.
   lifetime seconds 86400  # Set the SA lifetime, default is 86400 seconds.
```

4. Configuration Group Policy

```
   group-policy group_policy internal  # Set group policy for the device.
   group-policy group_policy attributes  # Set group policy attributes.
   vpn-tunnel-protocol ikev2  # Configure the VPN tunnel to use the IKEv2 protocol.
```

5. Configure the pre-shared password.

```
   tunnel-group 159.XX.XX.242 type ipsec-l2l  # Create an IPsec tunnel group, type is
point-to-point.
   tunnel-group 159.XX.XX.242 general-attributes default-group-policy group_policy  #
Call the group policy of Back Definition.
   tunnel-group 159.XX.XX.242 ipsec-attributes  # Configure the tunnel group attributes
and specify the pre-shared key.
```

```
   ikev2 remote-authentication pre-shared-key tencent@123
   ikev2 local-authentication pre-shared-key tencent@123  # The key can be 1-128
characters, letters, numbers, or strings.
```

6. Configure IPsec security protocol.

```
   crypto ipsec ikev2 ipsec-proposal ikev2_proposal  # Configure the encryption
algorithm and hash algorithm for the IPsec Phase 2 negotiation.
   protocol esp encryption aes-128  # Configure the encryption algorithm.
   protocol esp integrity sha-1  # Configure the integrity check algorithm.
```

7. Configure ACL.

```
   access-list INTERESTING extended permit ip 172.XX.XX.0 255.255.0.0 10.1.1.0
255.255.255.0  # Configure ACL to capture data flow on the VPN channel.
```

8. Configure IPsec policies.

```
   crypto map CMAP 1 match address INTERESTING  # Invoke the ACL to allow data packets
from source or destination segments that meet the ACL to flow through the VPN channel.
   crypto map CMAP 1 set peer 159.XX.XX.242  # Forward the traffic protected by IPsec
to the peer VPN public address, in this case, Tencent Cloud VPN public address.
   crypto map CMAP 1 set ikev2 ipsec-proposal ikev2_proposal  # Configure the IKEv2
security protocol for the encryption map entry.
   crypto map CMAP 1 set security-association lifetime seconds 3600  # Configure the
lifetime of the encryption key.
   crypto map CMAP 1 set security-association lifetime kilobytes 1843200  # Set the
amount of traffic that can be transferred between VPNs within the SA lifetime. The
default is 4,608,000 kilobytes; the default lifetime is 28,800 seconds.
```

9. Enable IPsec policies.

```
   crypto map CMAP interface outside  # Apply the configured encryption map to the
external interface.
```

10. Configure static routing.

```
    route outside 10.1.1.0 255.255.255.0 159.XX.XX.242 1  # Route the data segment to
be encrypted to the IPsec tunnel and configure the next hop as the public IP address of
the VPN tunnel peer.
```

11. Test VPN connectivity.
    Execute the ping command to test VPN connectivity.

Suitable for route-based VPN (IKEv2)

1. Log in to the firewall device command interface.

```
   ssh -p admin@10.XX.XX.56

# Log in to the firewall configuration interface via SSH command.

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# Enter account password to access user mode.

ASA>
ASA> en
Password:

# Enter 'enable' and the configured 'enable password' to access privileged mode. This
mode supports viewing only.

ASA# conf t
ASA(config)#

# Type "config ter" to enter global mode for firewall configuration.
```

2. Configure the firewall interface.
   In global mode, configure the firewall interface and Tunnel interface to connect to Tencent Cloud.

```
   interface GigabitEthernet0/0
   nameif outside  # Define the security domain name of the port.
   security-level 0  # Define the security level of the port's security domain.
   ip address 120.XX.XX.76 255.255.255.252  # Configure the public IP address for
connecting to Tencent Cloud VPN.
   interface Tunnel100
   nameif vti
   ip address 172.XX.XX.2 255.255.255.0  # This IP address is used to activate the
Tunnel interface.
```

```
```

3. Configure ISAKMP policy.

```
   crypto ikev2 policy 1  # Define parameters for the first stage of IKEv2 negotiation,
with a sequence number of 1. The smaller the number, the higher the priority, ranging
from 1 to 65535.
   encryption AES-128  # Configure the encryption algorithm for the data packet
encapsulation in the first stage of negotiation, default is AES-128.
   integrity MD5  # Configure the hash algorithm for the IKE policy as MD5, default is
SHA.
   group 2  # Configure the Diffie-Hellman group for the IKE policy as group 2, default
is group 2.
   prf sha  # Configure the encryption algorithm.
   lifetime seconds 86400  # Configure the SA lifetime, default is 86400 seconds.
```

4. Configuration Group Policy

```
   group-policy group_policy internal  # Set group policy for the device.
   group-policy group_policy attributes  # Set group policy attributes.
   vpn-tunnel-protocol ikev2  # Configure the VPN tunnel to use the IKEv2 protocol.
```

5. Configure the pre-shared password.

```
   tunnel-group 159.XX.XX.242 type ipsec-l2l  # Create an IPsec tunnel group, type is
point-to-point.
   tunnel-group 159.XX.XX.242 general-attributes default-group-policy group_policy  #
Call the group policy of Back Definition.
   tunnel-group 159.XX.XX.242 ipsec-attributes  # Configure the tunnel group attributes
and specify the pre-shared key.
   ikev2 remote-authentication pre-shared-key tencent@123
   ikev2 local-authentication pre-shared-key tencent@123  # The key can be 1-128
characters, letters, numbers, or strings.
```

6. Configure IPsec security protocol.

```
   crypto ipsec ikev2 ipsec-proposal ikev2_proposal  # Configure the encryption
algorithm and hash algorithm for IPsec Phase 2 negotiation.
   protocol esp encryption aes-128  # Configure the encryption algorithm.
   protocol esp integrity sha-1  # Configure the integrity check algorithm.
```

7. Configure IPsec policies.

```
   crypto ipsec profile PROFILE1
   set ikev2 ipsec-proposal ikev2_proposal  # Set the IKEv2 security protocol for the
encryption map entry.
```

```
    set security-association lifetime kilobytes 1843200  # Set the number of bytes that
can be transferred between VPNs during the SA lifetime.
    set security-association lifetime seconds 3600  # Set the lifetime of the encryption
key. The default kilobyte value is 4,608,000; the default lifetime is 28,800 seconds.
```

8. Enable IPsec policies.

```
    interface Tunnel100
    tunnel source interface outside  # Configure the update source of the VPN as the
outside interface.
    tunnel destination 159.XX.XX.242  # Configure the public IP address of the remote
VPN, which is the Tencent Cloud VPN public IP address in this case.
    tunnel mode ipsec ipv4  # Configure the protocol used by the tunnel interface.
    tunnel protection ipsec profile PROFILE1  # Apply the IPsec policy to protect the
data passing through the tunnel interface.
```

9. Configure static routing.

```
    route vti 10.1.1.0 255.255.255.0 159.XX.XX.242  # Direct the data packets to be
encrypted to the tunnel interface.
```

10. Test VPN connectivity.

Execute the ping command to test VPN connectivity.

SSL VPN
SSL VPN Access Control Practice Guidelines (Okta)

Last updated: 2024-09-26 10:41:29

This article introduces how to use a third-party IDP (Okta) and SSL VPN to implement access control, enhancing your business security.

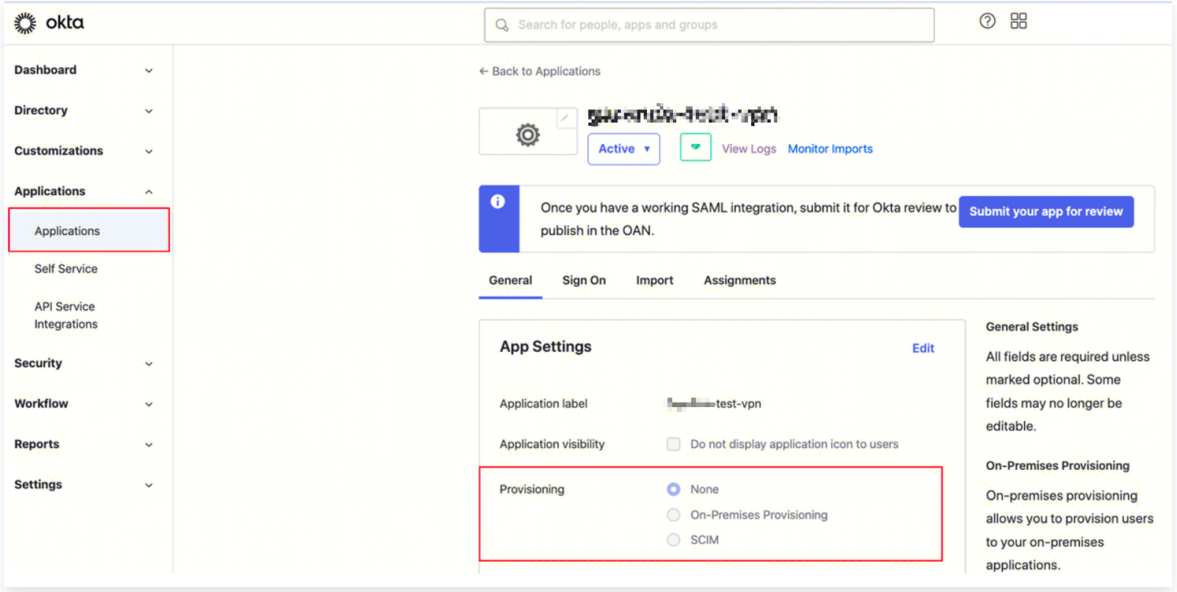
Note:
- Currently, the SSO identity authentication feature is in beta testing. To use it, please submit a Ticket Application.
- Support for mainstream third-party IDPs based on SAML 2.0, such as Okta.
- Supported Version: VPN 4.0.

Directions

Step 1: (Tenant Administrator) IDP Configuration (Okta)

Okta is a third-party IDP system. This section only introduces key parameter configurations. For detailed steps, please refer to the Okta official website or the Okta Single Sign-On Guide to Tencent Cloud.
This step configures the trust relationship between Okta and Tencent Cloud to make them mutually trusted.

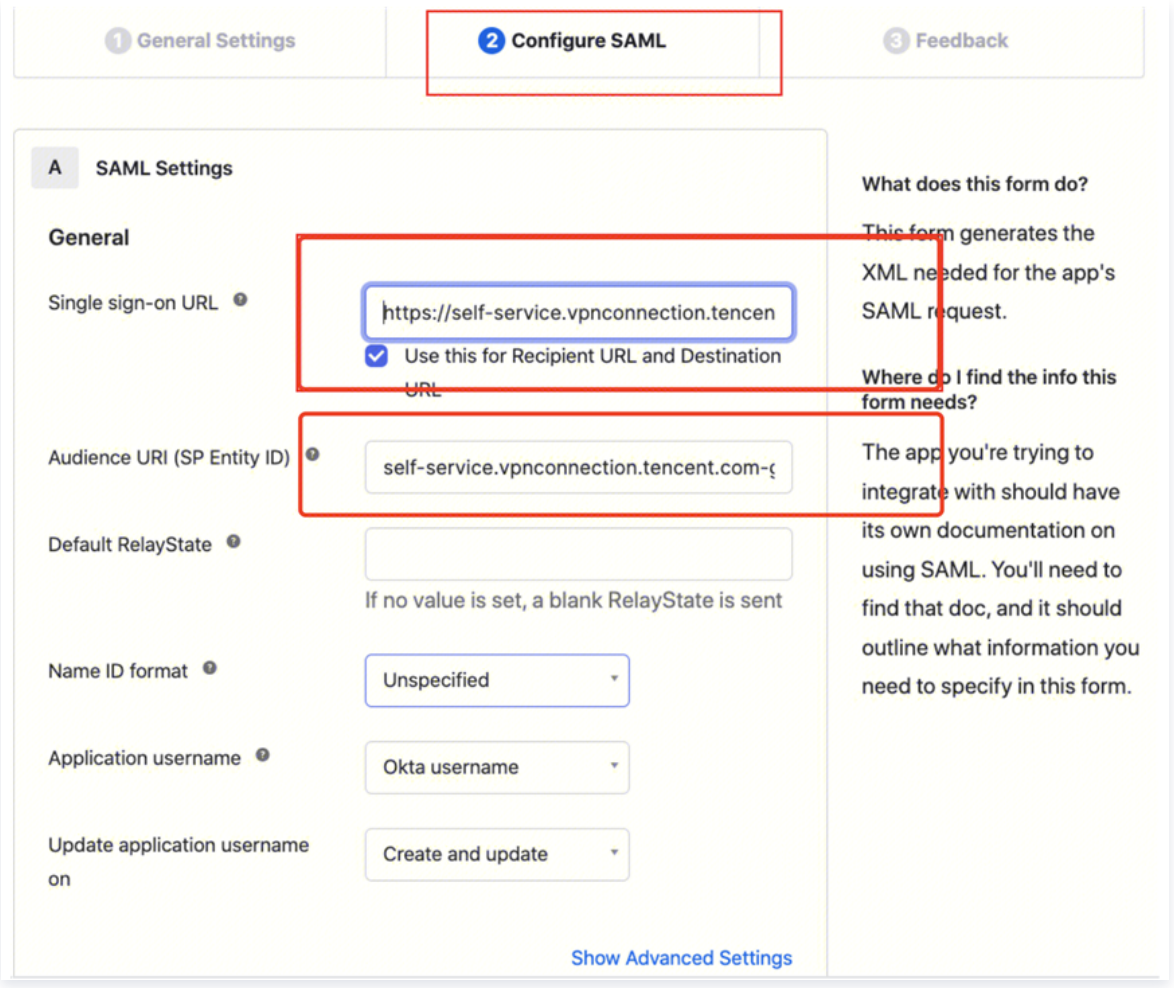
1. Log in to Okta Official Website and create an Okta application.
2. Go to the Applications page, click the application name, and then click **Edit** on the General tab.



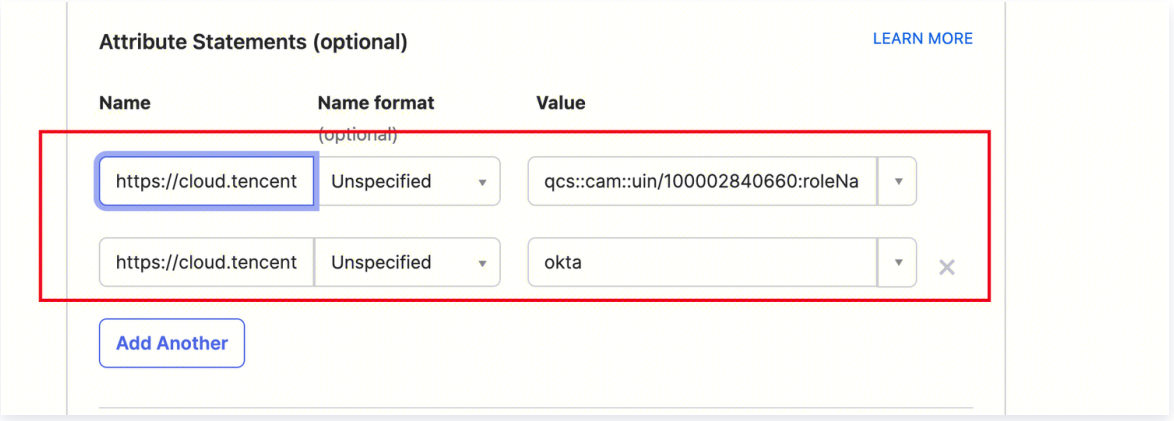
3. On the Configure SAML page, configure the Single Sign-On URL and Audience URL (SP Entity ID).

Note:

- Single Sign-On URL: `https://self-service.vpnconnection.tencent.com/api/auth/sso-v2/saml`. This value is fixed.
- Audience URI (SP Entity ID): Tencent Cloud Client VPN Self-Service Portal.



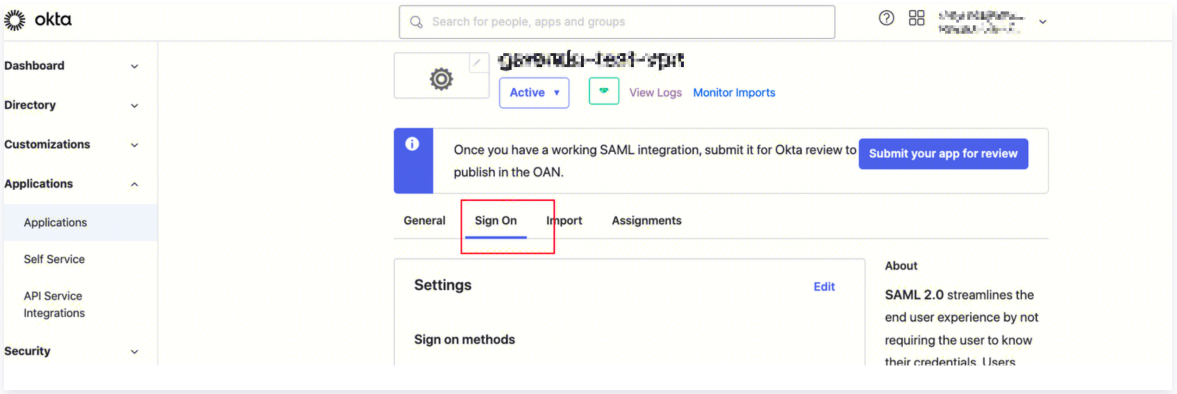
4. On the Configure SAML page, add the following information under ATTRIBUTE STATEMENTS in the GENERAL section.



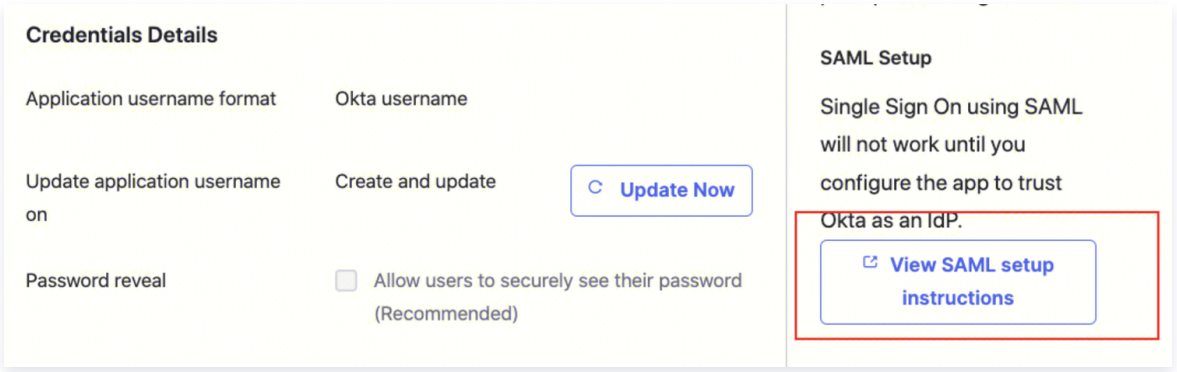
Name	Value
`https://cloud.tencent.com/SAML/Attributes/Role`	qcs::cam::uin/{AccountID}:roleName/{RoleName},qcs::cam::uin/{AccountID}:saml-provider/{ProviderName}

`https://cloud.tencent.com/SAML/Attributes/RoleSessionName`	okta

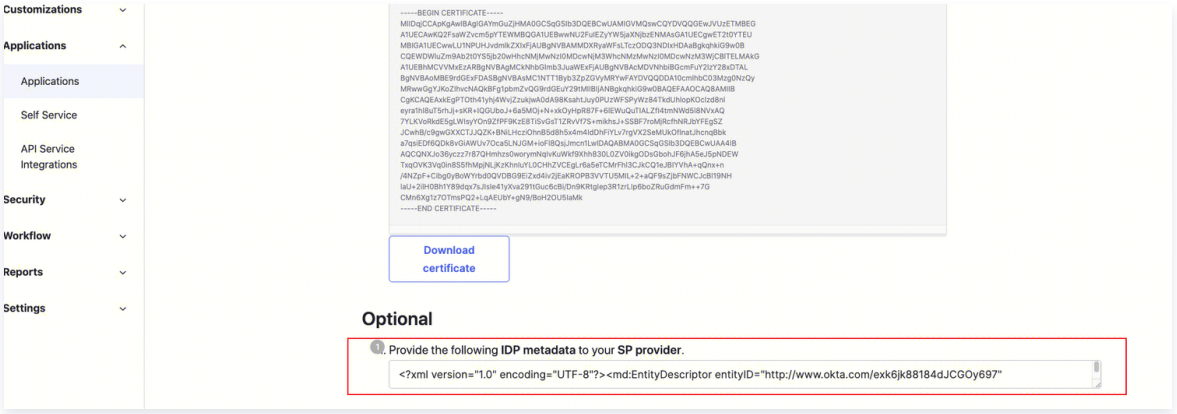
5. On the Sign-On tab, generate and download the SAML-Metadata file of the IDP.



click View SAML setup instructions.



click Download certificate , the downloaded file needs to be uploaded when configuring the identity on Tencent Cloud Certificate Authority M



Step 2: (Tenant Administrator) CAM Identity Configuration

1. Log in to the CAM console, select IdPs > Role SSO and click **Create New Provider** .

2. On the Create IdP page, select the provider type as SAML and configure the provider information, then click **Next**.

- IdP Name: Enter an IdP name.
- Remarks: Enter your memo for the current IdP.
- Metadata Document: This is the file downloaded in Step 1: (Tenant Administrator) IDP Configuration (Okta). You need to upload the SAML-Metadata data document downloaded in the IDP configuration to the Metadata Document field. The metadata document will be successfully uploaded after validation.

Step 3: (Tenant Administrator) VPN Resource Configuration

Create SSL VPN Gateway

1. Log in to the VPC console, select **VPN Connections** > **VPN Gateway** on the left sidebar to enter the management page.
2. On the VPN gateway management page, click **New** and configure the SSL VPN gateway on the **Create VPN Gateway** page based on the interface parameters.

Create SSL Server

1. Select **VPN Connections** > **SSL Server** on the left sidebar to enter the management page.
2. On the SSL server management page, click **New** and configure the SSL server on the **Create SSL Server** dialog based on the interface parameters.

- Authentication Method: The default authentication method allows the SSL server to be fully accessible by the SSL client.
- Identity Provider: The current Identity Provider is Tencent Cloud Certificate Authority M. For more details, see the Identity Provider Usage Guide.

Step 4: (Tenant) Download the SSL client configuration file and SSL client from the Client VPN portal

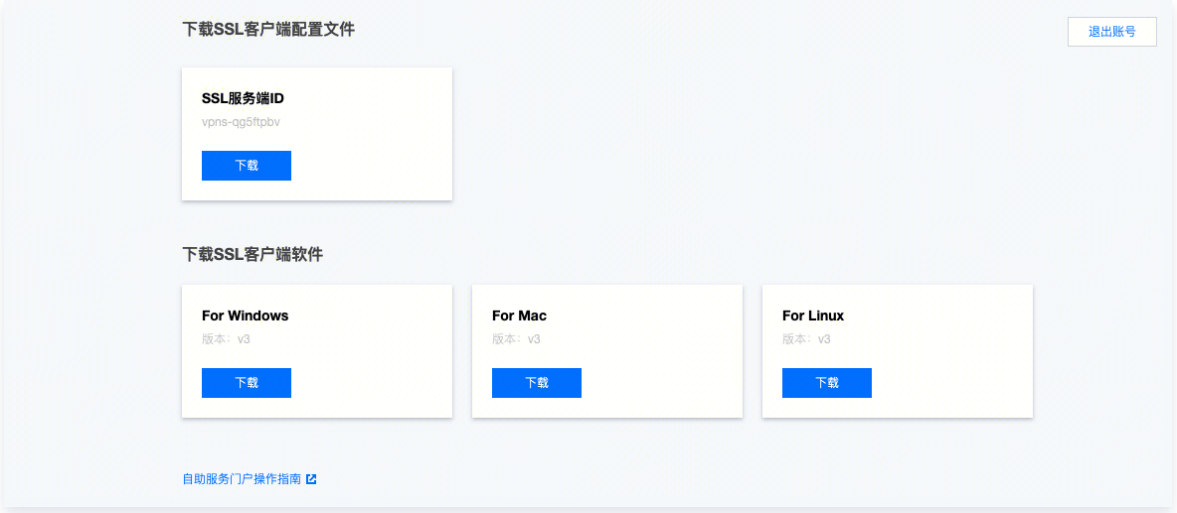
1. Access the Tencent Cloud Client VPN Self-Service Portal through your local browser.
2. In the input field under the SSL Server ID column, enter the created SSL Server ID, then click **Next** to start SSO authentication.

   If you do not have or are unsure about the SSL Server ID, contact the tenant administrator.

3. After clicking **Proceed to Authenticate (SAML)**, you need to complete the authentication process specified by your administrator.

   If you do not have an account or encounter issues during the authentication process, contact your tenant administrator. After you complete authentication and successfully log in, you will be automatically logged in to your business system.
   Search for the required CAM policy as needed, and click to complete policy association.

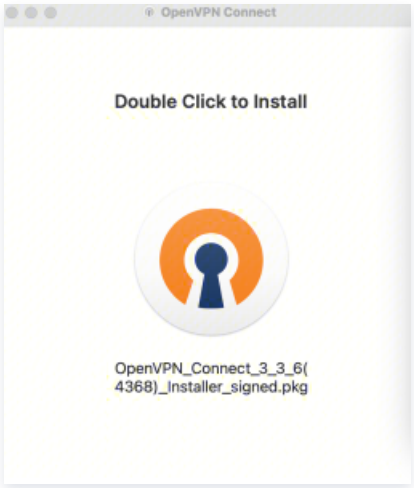
4. In the **Download SSL Client Configuration File** section, find the client configuration file you need and click **Download**.



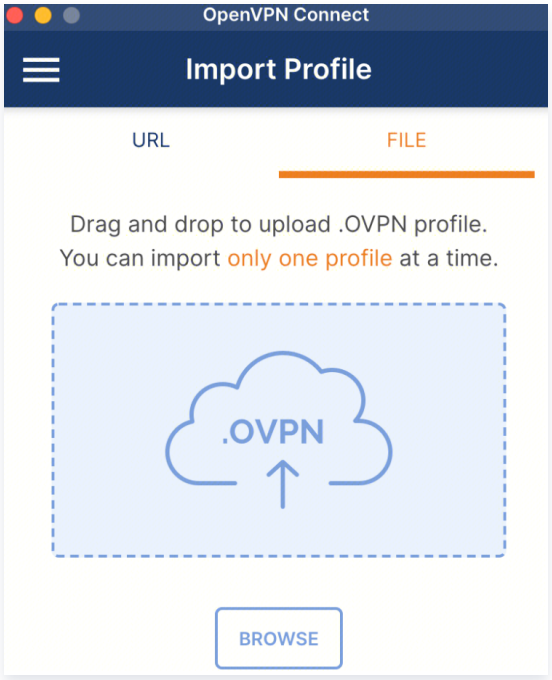
Step 5: (Tenant) SSL Client Installation and Connection

> **Note:**
> For the OpenVPN client, use version 3.4.0 or above.

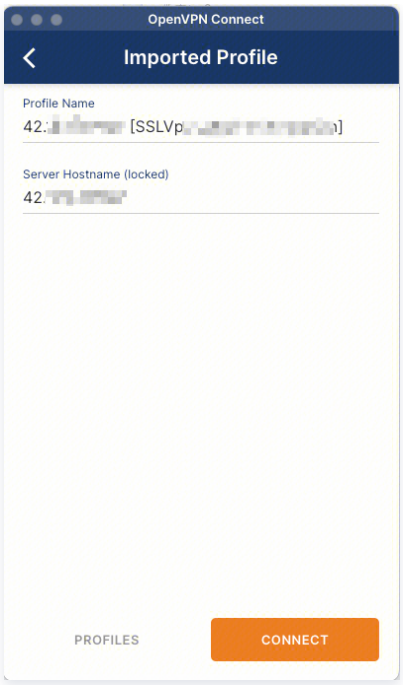
1. Decompress the installation package locally and double-click the installer to install the client as prompted.



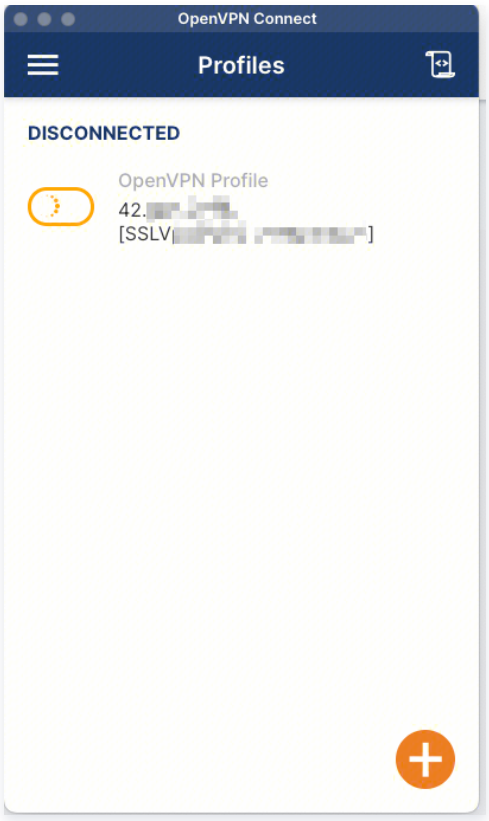
2. After installing the SSL client, select the "Import Profile" menu and go to the "FILE" page to upload the downloaded SSL client configuration file (.ovpn format).



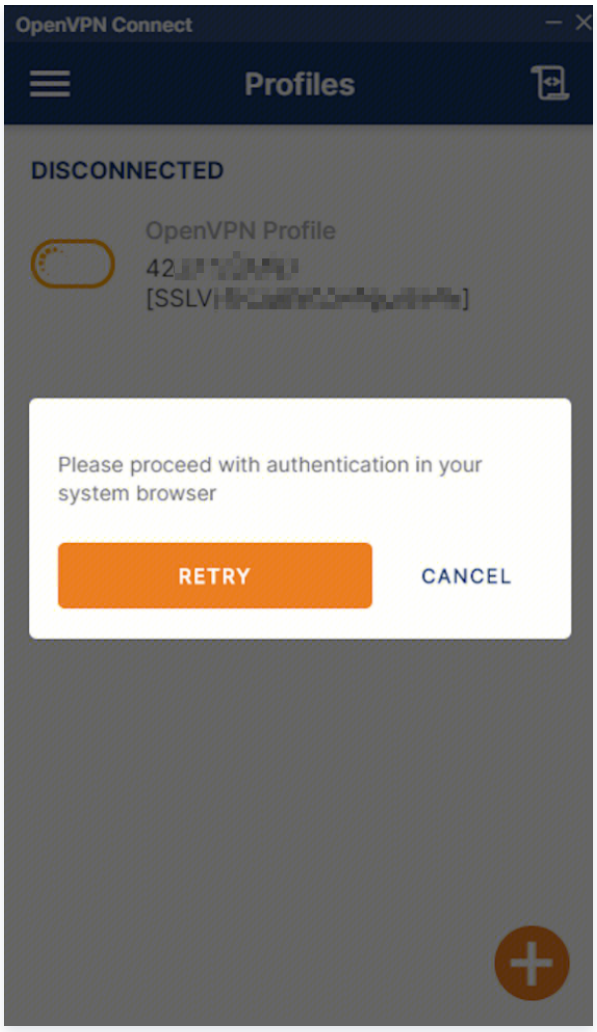
3. After the upload is successful, select Connect to proceed.



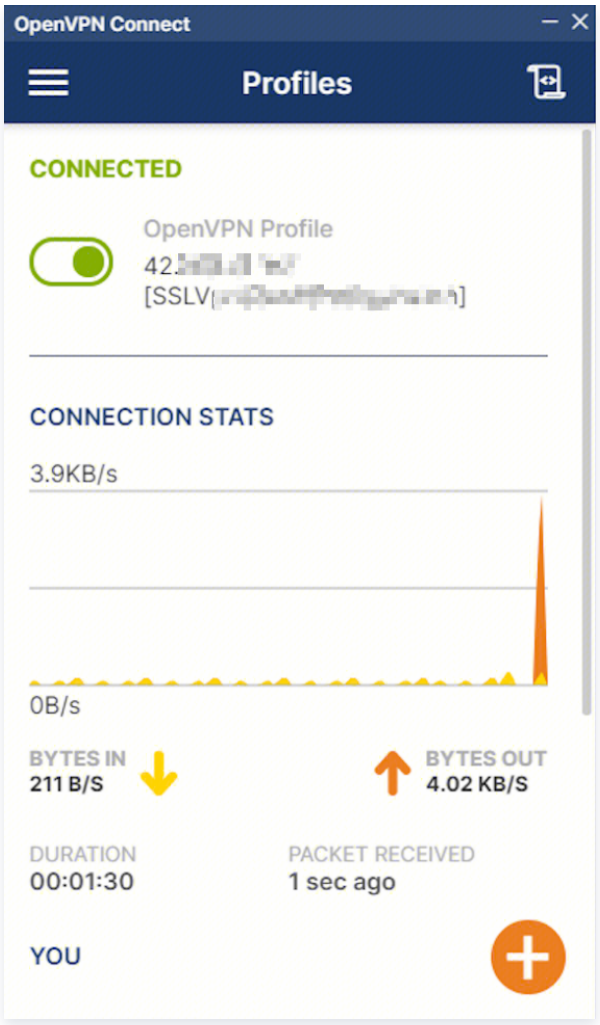
4. Profiles connecting, please wait.



5. Verify the login information.



6. The connection is successful.



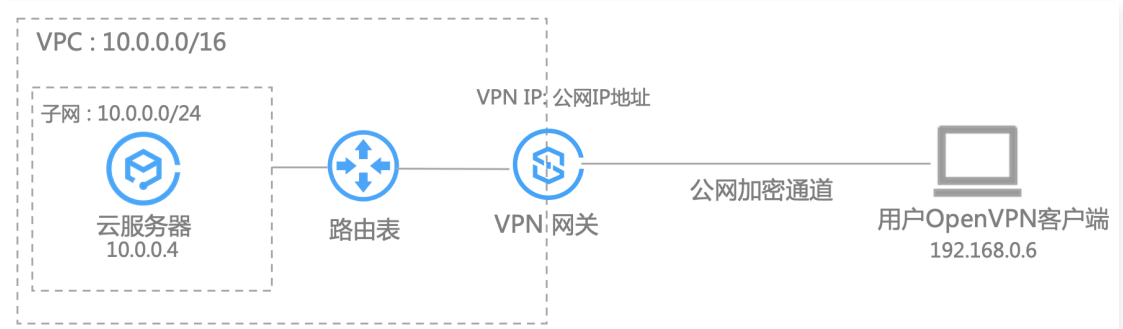
Connecting Client to VPC

Last updated: 2024-09-26 10:41:54

This article introduces how Windows, Mac, and Linux clients use SSL VPN Connections with VPC.

Background

Using the scenario below as an example, this article explains how Windows, Mac, and Linux clients use SSL VPN Connections with VPC.



VPC路由表			SSL 服务端配置	
目的端	下一跳类型	下一跳	本端网段	10.0.0.0/16
10.0.0.0/16	Local	Local	客户端网段	192.168.0.0/16
192.168.0.0/16	VPN网关	vpngw-12345678		

Configuration Process

The process diagram for clients connecting via SSL VPN Connections with VPC is shown below:

Step 1: Create an SSL VPN Gateway

1. Log in to the VPC console.
2. In the left directory, click **VPN Connections** > **VPN Gateway** to enter the admin page.
3. On the VPN Gateway management page, click **New**.
4. In the pop-up dialog for creating a new VPN Gateway, configure the following parameters.

Parameter name	Parameter Description
Gateway Name	Enter the VPN gateway name (up to 60 characters).
Region	Display the region of the VPN gateway.
Availability Zone	Select the Availability Zone where the current gateway is located.

Protocol Type	Select SSL.
Bandwidth Cap	Set a reasonable bandwidth cap for the VPN gateway according to the actual application scenarios.
Associated Network	Indicates that you are creating a VPC type VPN.
Network	Select the VPC associated with the VPN gateway.
Number of SSL Connections	The number of connected clients: One SSL client allows only one user connection and does not support multiple clients connected to the same SSL client.
Billing Mode	SSL VPN is billed based on traffic by default.

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

Step 2: Create 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.

> **Note**
> A VPN gateway supports associating with only one SSL server. For more details, please refer to Usage Limitations.

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

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	Tencent Cloud IP ranges accessed by mobile clients.
Client IP Range	Enter the IP range that is assigned to the mobile client for communication. The IP range must not conflict with the VPC CIDR block of Tencent or your local IP range.
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.

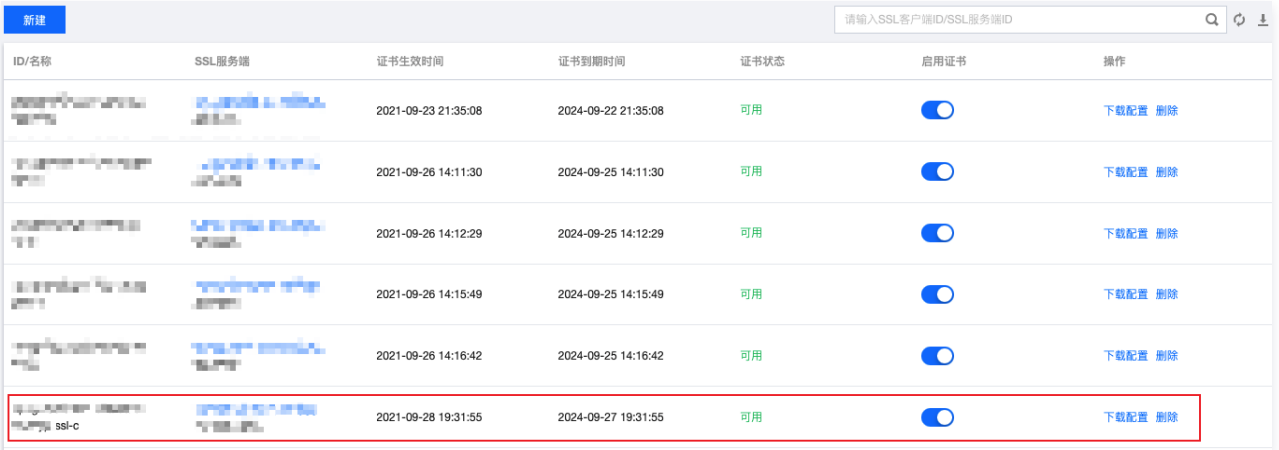
5. After completing the gateway parameter settings, click **Create**.

Step 3: Create an SSL VPN Client

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

5. After configuring the SSL client parameters, click **Confirm**. When the certificate status becomes available, it indicates the creation is complete.
6. In the SSL Client page, find the created client certificate, and then click **Download Configuration** in the action column.

> **Note**
> Each SSL client allows only one user connection. Multiple clients connected to the same SSL client are not supported.



Step 4: Configure VPC routing

1. Log in to the VPC console.
2. Click Route Tables on the left sidebar to enter the admin page.
3. In the list, click the routing table ID that needs modification to enter the details page. If you need to create a routing table, refer to Create a custom routing table.
4. Click **Add Routing Policy** and configure the routing policy in the popup window.

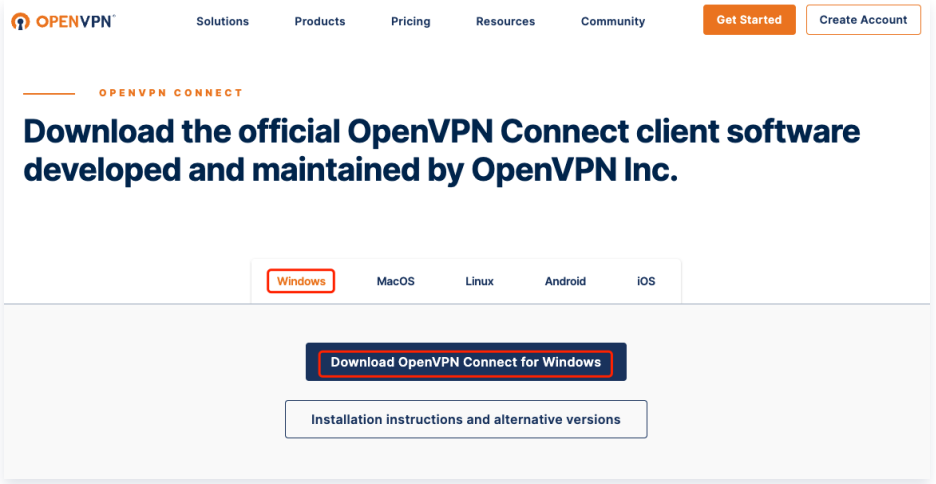
Parameter name	Parameter Description
Destination	Please fill in the client subnet configured in Step 2: Create an SSL VPN Server.
Next Hop Type	Select the VPN gateway.
Next Hop	For the next hop, select the specific SSL VPN Gateway Instance created.

Step 5: Configure the client

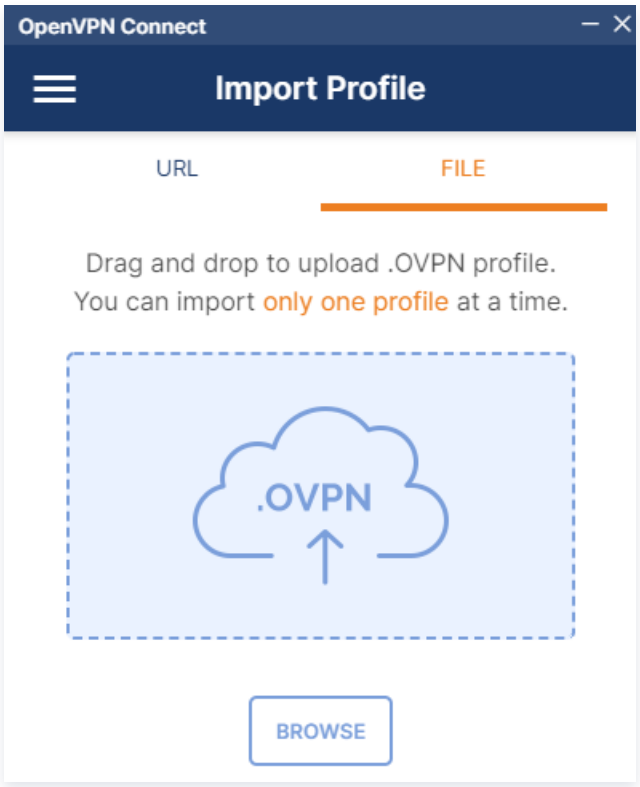
The following content introduces how to configure Windows, Mac, and Linux clients.

Windows client

1. First, download and install OpenVPN Connect from the official OpenVPN download page.

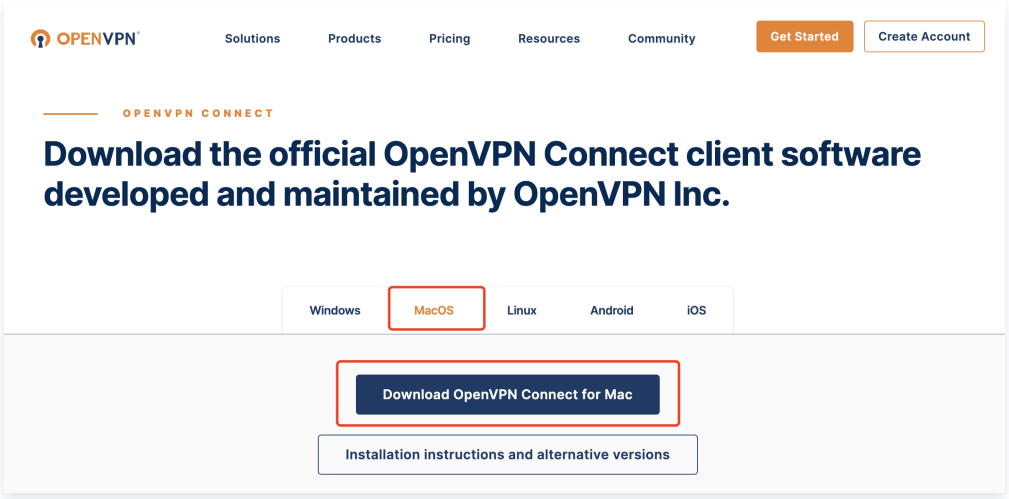


2. After installing the SSL client, select "Import Profile" from the "FILE" page and upload the SSL client configuration file (.ovpn format) downloaded in Step 3.



MAC client

1. First, download and install OpenVPN Connect from the official OpenVPN download page.



2. After installing the SSL client, select "Import Profile" from the "FILE" page and upload the SSL client configuration file (.ovpn format) downloaded in Step 3.

Linux client

1. Open the command line window.
2. Run the following command to install the OpenVPN client.
   CentOS distribution

```
yum install -y openvpn
```

   Ubuntu distribution

```
sudo apt-get install openvpn
```

3. Unzip the SSL client certificate downloaded in Step 3 and copy it to the /etc/openvpn/ directory.
4. Enter the /etc/openvpn/ directory and run the following command to establish VPN connections.

```
openvpn --config /etc/openvpn/config.ovpn --daemon
```

Step 6: Test connectivity

After establishing SSL VPN connections between Tencent Cloud and the user's mobile device, use the ping command to test connectivity.
For example, use a CVM within the VPC to ping the IP in the client subnet. If the ping is successful, it means the VPC and the client can communicate normally.