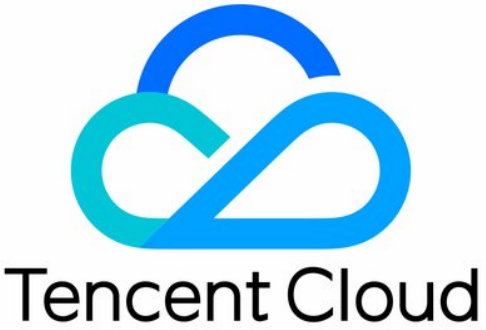
VPN Connections Troubleshooting



Copyright Notice

Trademark Notice

Service Notice

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

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

Contact Us

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

Contents

Troubleshooting
VPN Tunnel Unconnected

Last updated: 2024-09-26 10:42:36

Phenomenon Description

Using VPN Connections to establish communication between VPC and IDC, after configuration, the VPN tunnel status is **disconnected**.

Possible Reasons

An exception in tunnel status usually results from the following factors:

- No traffic to activate the tunnel
- The VPN gateway public IP is not connected
- The security policy is not correctly configured
- Inconsistent negotiation parameters and modes

Solutions

1. Log in to a CVM in the VPC and activate the tunnel by using the ping command to test the network connectivity of the private IP of the server on the customer IDC side.

   > **Note:**
   > To log in to CVM in VPC, refer to log in to Linux instance or log in to Windows instance.

   - If the ping is successful, the tunnel is activated. Check the VPN tunnel status. If it is connected, the problem is solved.
   - If the ping is unsuccessful, directly perform Step 2.
2. Please log into the IDC side VPN device, ping the public IP of the Tencent Cloud VPN gateway (assuming the VPN gateway public IP is 139.186.120.129) to see if it can be reached.

- If yes, please perform Step 4.
- If no, please perform Step 3.

```
[IDC_IPSec] ping 139.186.120.129
  PING 139.186.120.129: 56  data bytes, press CTRL_C to break
    Reply from 139.186.120.129: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 139.186.120.129: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 139.186.120.129: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 139.186.120.129: bytes=56 Sequence=4 ttl=255 time=70 ms
    Reply from 139.186.120.129: bytes=56 Sequence=5 ttl=255 time=60 ms

  --- 139.186.120.129 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/58/80 ms
```

3. Please check the public network connection status on the IDC side to see if it can connect to the internet normally.
   - If yes, please perform Step 4.
   - If no, after repairing the local network, check again if the VPN tunnel status is connected. If connected, the problem is solved, end; if not, continue to perform Step 4.
4. Check the security policy of the IDC side VPN device, whether it has allowed the public IP of the Tencent Cloud VPN gateway and the internal network addresses that need to be communicated.

```
display current-configuration configuration security-policy
//Take Huawei Firewall as an example here
```

- If yes, please perform Step 5.
- If not, please modify the security policy and open the VPN gateway IP on the Tencent Cloud side and the corresponding SPD policy. Then, check whether the VPN tunnel is connected. If so, the problem is solved. If not, please go to Step 5.

5. Check whether the negotiation parameters (including IKE and IPsec configurations) and negotiation modes (main/aggressive mode) of the VPN gateway on the Tencent Cloud side and the VPN device in the customer IDC are consistent.

> **Note**
> - The VPN channel cannot be established if any parameter is inconsistent.

- The default VPN configuration varies by devices and public cloud service providers.

Enter the VPN Gateway Console, click on the Instance ID to access the details page, and view in the "Advanced Settings" tab:

Device configuration parameters on the IDC side can be obtained through the following command. Take Huawei Firewall as an example here:

```
display current-configuration configuration ike profile
display current-configuration configuration ipsec  policy
```

- If they are consistent, please go to Step 6.
- If not, please modify corresponding parameters on both sides to ensure consistency. Then, check whether the VPN tunnel is connected. If so, the problem is solved. If not,

please go to Step 6.

6. Collect the troubleshooting information above, and submit a ticket or contact the device manufacturer for assistance.

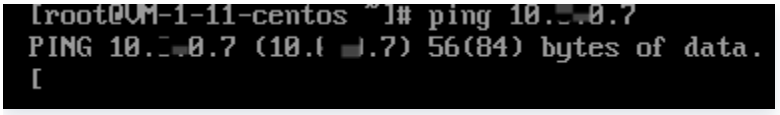
VPN Tunnel Connected Yet Private Network Unconnected

Last updated: 2024-09-26 10:42:55

Phenomenon Description

Use VPN Connections to establish communication between the VPC and IDC. The VPN tunnel status is **Connected**, but the private network cannot be connected. The phenomenon is as follows:
The VPN tunnel status is **Connected**:

The VPC side server cannot ping the private IP on the IDC side:



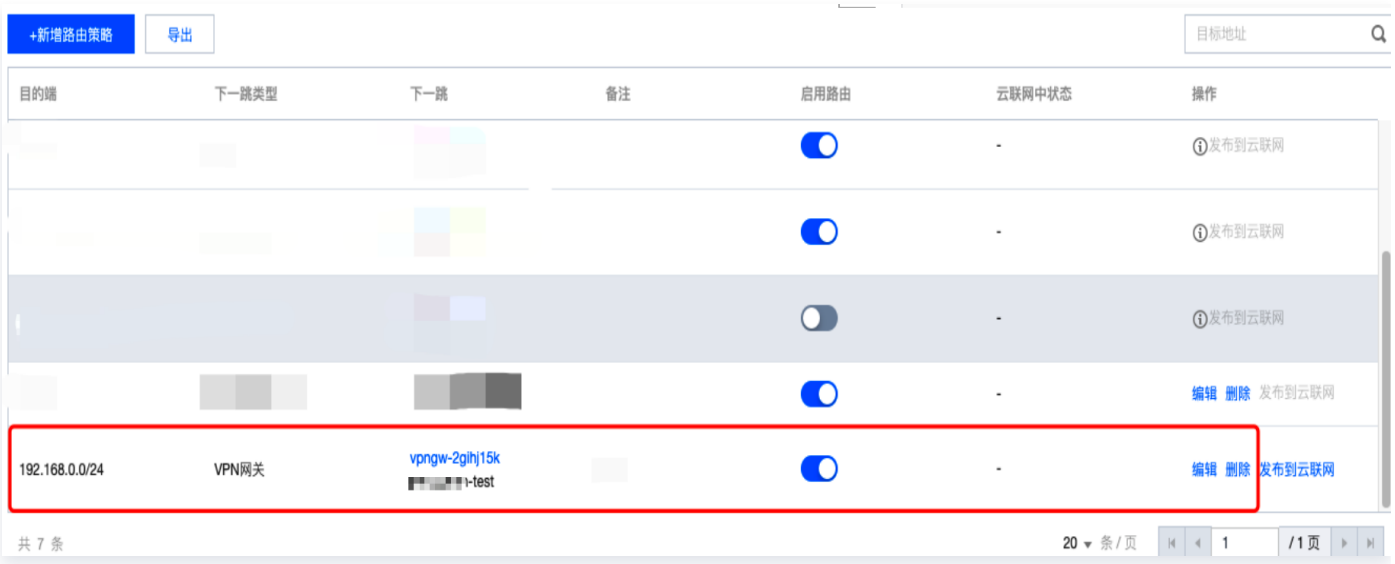
Possible Reasons

If the tunnel is in a normal status yet the private network cannot be connected, the possible causes are as follows:

- The VPC subnet route table has not added a route pointing to the private IP range on the IDC side
- The security policy on the VPC/IDC side does not make the corresponding source and destination IPs open to Internet
- The VPN gateway has not added a channel (routing type) pointing to the private IP range on the IDC side
- The firewall of the operating system of private network server on the VPC/IDC side does not allow the customer IP range to pass
- The SPD policy on the VPC/IDC side does not contain the source and destination IPs
- The VPN gateway has not configured a routing policy

Processing Procedures

1. Check the VPC subnet route table to see if there is a route whose destination is the private IP range on the IDC side and whose next hop address is the corresponding VPN gateway. Also, check whether the IDC side has a route whose destination is the VPC IP range and whose next hop is the corresponding VPN tunnel.
   Go to the VPC subnet route table, click the route table ID, and enter the details page to check:



   Execute the command on the IDC side to check the routing (take Huawei devices as an example):

```
display ip routing-table     //Check whether there is any route whose destination IP address is the cloud VPC IP range and whose next hop is the corresponding VPN tunnel
```

   - If so, proceed to Step 3.
   - If not, please complete the routing information according to business requirements before proceeding to Step 2.

2. Check if communication has resumed normally, that is, log in to a server in VPC/IDC, ping the internal IP of the peer server.

> **Note**
> To log in to the CVM in the VPC, please refer to logging in to Linux Instance or logging in to Windows Instance.

   - If so, communication is normal, the issue is resolved, and the process ends.
   - If not, please proceed to Step 3.

3. Check whether the security group associated with the server in the VPC and the network ACL associated with the subnet allow traffic from the on-premises IDC, and also check if the IDC side allows traffic from the cloud-based VPC.
   Go to the VPC server security group interface, click on the security group ID, enter the "Security Group Rules" page to check:

   Go to the VPC subnet ACL rules, click on the **network ACL ID**, enter the "Basic Information" page, click on the "Inbound Rules" tab to check:

   Check the security policies on the IDC side (taking Huawei Firewall as an example):

```
display current-configuration configuration security-policy
```

   - If they do, please go to Step 5.
   - If not, please allow the private IP ranges that need to communicate in the security group/Network ACL/IDC side security devices, and then go to Step 4.

4. Check whether the communication is restored, i.e. log in to a server in the VPC/IDC and ping the private IP of the peer server.
   - If so, communication is normal, the issue is resolved, and the process ends.
   - If not, please go to Step 5.

5. Check respectively the operating system built-in firewalls of the V
   PC cloud server and the IDC internal server, and whether they have policies to allow the peer network segment.
   For Linux servers, check the firewall with: `iptables --list`

For Windows servers, check the firewall via Control Panel/System and Security/Windows Firewall/Allowed Apps

- If they do, please go to Step 7.
- If not, please allow the business network segments that need to be connected in the firewall of the internal server, and then go to Step 6.

6. Check whether the communication is restored, i.e. log in to a server in the VPC/IDC and ping the private IP of the peer server.
   - If so, communication is normal, the issue is resolved, and the process ends.
   - If not, please go to Step 7.
7. Check separately whether the SPD policies of the VPN tunnels on both the VPC and IDC sides include the required internal network segments.
   Go to VPC-side SPD Policy, click on the VPN tunnel ID, go to the "Basic Information" page to check the SPD policy:

IDC-side SPD policy check (using Huawei firewall as an example):

```
display current-configuration configuration acl
```

   - If so, please go to Step 8.
   - If not, please add the missing SPD policies and then go to Step 8.
8. Check whether the routing table of the VPN gateway contains the corresponding routing policies. Go to the VPN gateway, click on the VPN gateway ID, go to the "Routing Table" page to check the routing policies.

   - If so, please go to Step 9.

- If not, set the next hop on the VPN gateway > Routing tab, and then go to Step 9.

9. Checkwhether the communication is restored, i.e. log in to a server in the VPC/IDC and ping the private IP of the peer server.
   - If so, communication is normal, the issue is resolved, and the process ends.
   - If not, please go to Step 10.
10. Please collect the above information and submit a work order or contact the equipment manufacturer for follow-up.

Error Description of IPSec VPN Negotiation Failure

Last updated: 2024-09-26 10:43:18

Negotiation Stage	Error message	Description
IKE Negotiation	no match proposal	The IKE policy configured on the cloud side and client side are inconsistent. Please check.
	DH group not supported	The DH Group configured on the client side is not supported by the cloud side. Please modify your local configuration.
	responder no peer config found by ID payload	The cloud side configuration of the **Local Identifier** and the **Peer Identification** are inconsistent with the client side, causing the responder to not reply.
	initiator no peer config found by ID payload	The cloud side configuration of the **Local Identifier** and the **Peer Identification** are inconsistent with the client side, causing the requester to not reply.
	received xxx error notify	The cloud side received a negotiation failure message from the client side.
IPSec Negotiation	DH group xxx not supported	The DH Group configured on the client side is not supported by the cloud side. Please modify your local DH group.
	reponder no matching CHILD_SA config for TS	The TS configuration on the cloud side and client side are inconsistent. Please check.
	no matching proposal, configured xxx, received xxx	The child configuration on the cloud side and client side do not match.
	received xxx error notify in the payload	The cloud side received a negotiation failure message from the client side.