VPN Connections

Troubleshooting

Product Documentation

Contents

Troubleshooting
VPN Tunnel Unconnected

Last updated：2024-01-09 14:20:07

Error description

A VPN connection is used to connect VPC to IDC, but the status of VPN tunnel is **Unconnected** after the configuration.

Possible causes

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 the CVM in the VPC, please see Logging in to Linux Instance or Logging in to a Windows Instance.
A successful ping indicates that the tunnel is activated. Check if the status of the VPN tunnel is “Connected”. If so, the problem is solved.
In case of a ping failure, please directly go to Step 2.
2. Log i
n to the VPN device
on the IDC side and use the ping command to test the network connectivity of the VPN gateway public IP on the Tencent Cloud side (suppose the VPN gateway public IP is 139.186.120.129) to see if the ping is successful or not.
If it is, please go to Step 4.
If not, please go to Step 3.

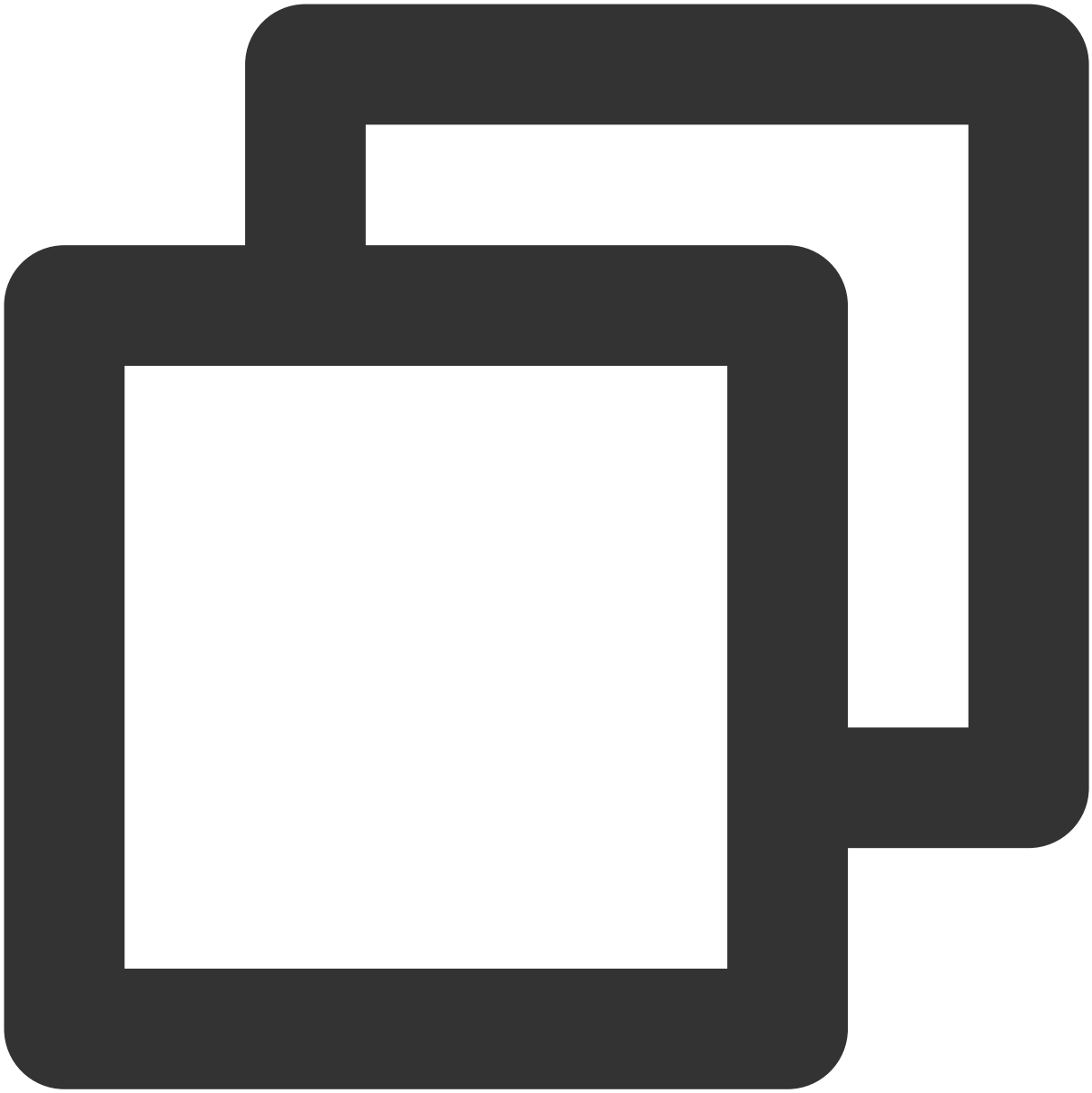
```
[IDC_IPSec] ping 139.186.120.129
  PING 139.186.120.129: 56  data bytes, press CTRL_C to
    Reply from 139.186.120.129: bytes=56 Sequence=1 ttl
    Reply from 139.186.120.129: bytes=56 Sequence=2 ttl
    Reply from 139.186.120.129: bytes=56 Sequence=3 ttl
    Reply from 139.186.120.129: bytes=56 Sequence=4 ttl
    Reply from 139.186.120.129: bytes=56 Sequence=5 ttl

  --- 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. Check the connection status of the public network on the IDC side and see whether it can be connected to the Internet.

If it is, please go to Step 4.

If not, please check whether the VPN tunnel is connected after repairing the local network. If it is connected, the problem is solved. If not, please go to Step 4.

4. Check the security policy of the VPN device on the IDC side, and whether the public IP address of the VPN gateway on the Tencent Cloud side and the private IP address are open to Internet.



```
display current-configuration configuration security-policy      //Take Huawei Fire
```

If it is, please go to Step 5.

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

5. Chec

k whether the ne

gotiation 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.

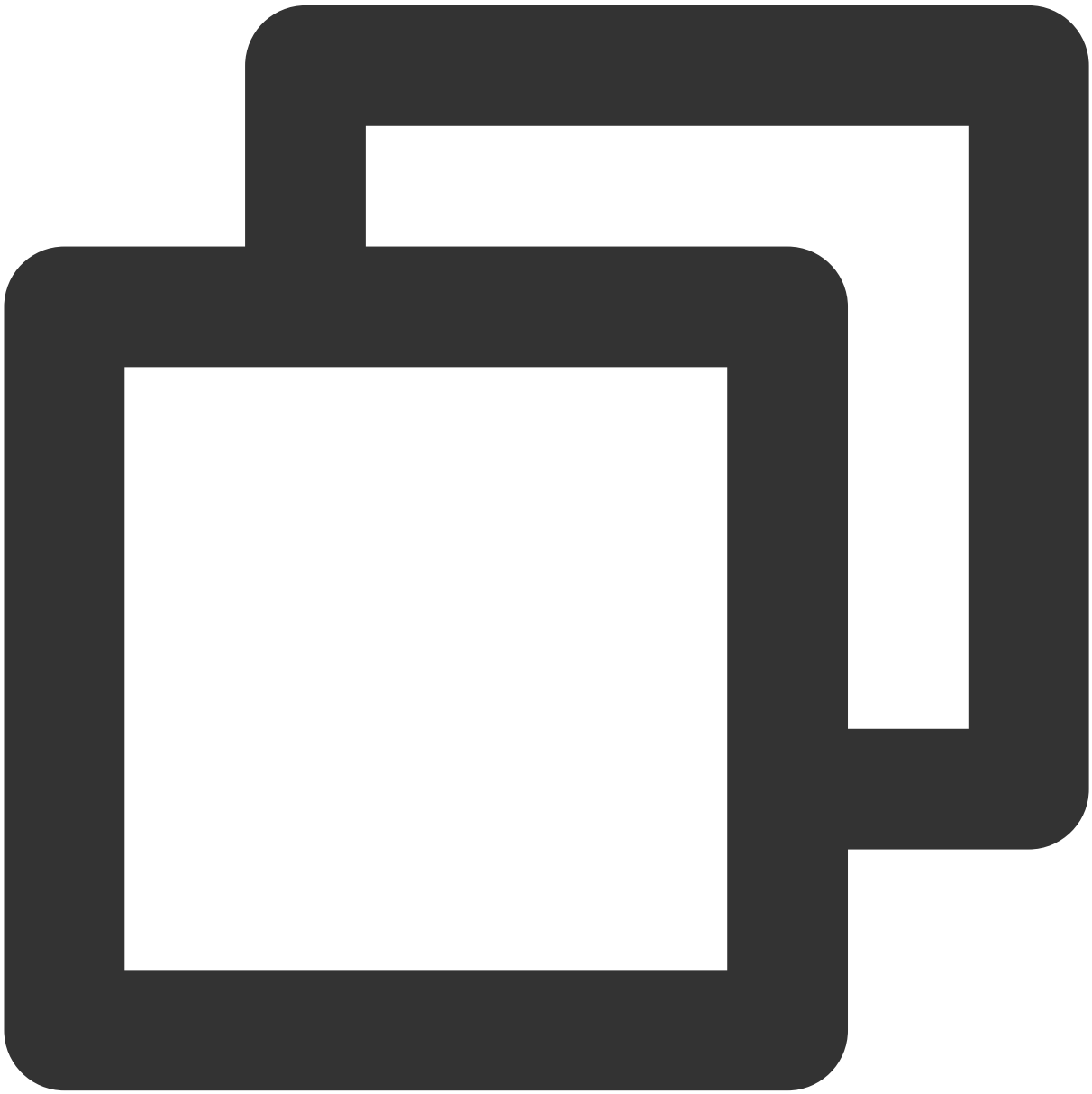
Note:

Inconsistency in any parameter can cause the failure to create a VPN tunnel.

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

Go to the VPN tunnel console. Click the instance ID to enter the details page, and check the consistency on the “Advanced Configuration” 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 the 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 troub

leshooting inf

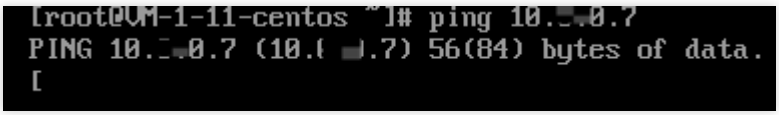
ormation above and submit a ticket or ask the device manufacturer for help.

VPN Tunnel Connected Yet Private Network Unconnected

Last updated：2024-01-09 14:20:07

Symptom

A VPN connection is used to connect a VPC to an IDC and the status of the VPN tunnel is **Linked**, but the private network cannot be connected.

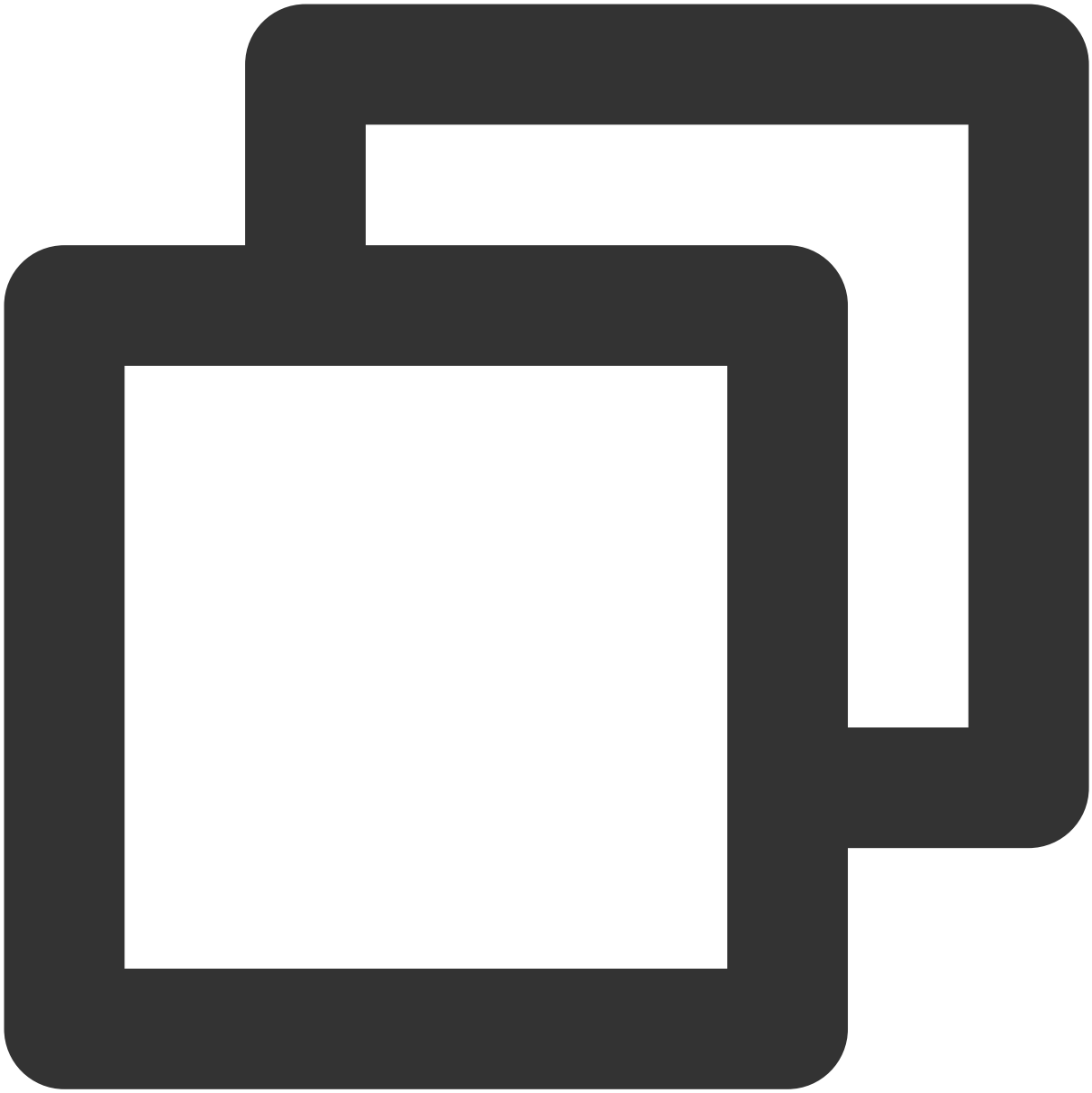


Possible Causes

If the tunnel is in a normal status yet the private network cannot be connected, the possible causes are as follows:
No routes directing to the private IP range in the IDC are added in the route table of the VPC subnet.
The security policy on the VPC/IDC side does not make the corresponding source and destination IPs open to Internet
No tunnels directing to the private IP range in the IDC are added to the VPN gateway (route-based gateway).
The firewall of the operating system of 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
No routing policies are configured in the VPN gateway.

Troubleshooting

1. Check whether the route table of the VPC subnet contains any route whose destination IP address is the private IP range on the IDC side and whose next hop address is the corresponding VPN gateway. Meanwhile, check whether there is any route on the IDC side whose destination IP address is the VPC IP range and whose next hop address is the corresponding VPN tunnel.
Go to the VPC subnet route table. Click the route table ID to enter the details page and check these aspects:
Execute the command on the IDC side to check the routing (take Huawei's device as an example):



```
display ip routing-table     //Check whether there is any route whose destination I
```

If so, please go to Step 3.

If not, please complete the routing information according to business requirements before going to Step 2.

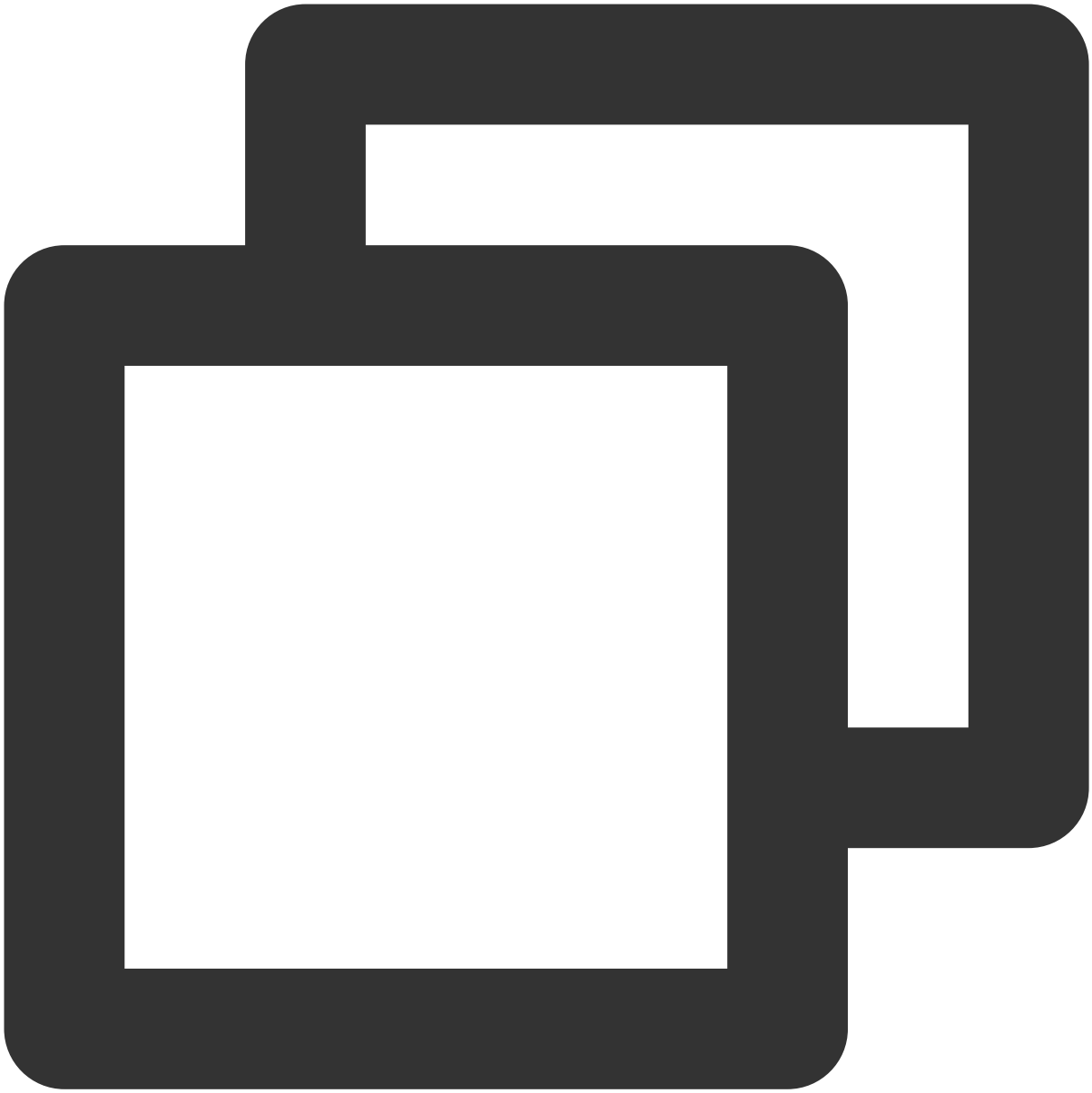
2.

Check whether the c

ommunication is back to normal. In other words, log in to a server in the VPC/IDC and use the ping command to test the connectivity of the private IP of the peer server.

Note:

To log in to the CVM in the VPC, please see Logging in to Linux Instance or Logging in to a Windows Instance.
If it is, the problem is solved.
If not, please go to Step 3
3. Check
whether the sec
urity group associated with the server in the VPC and the network ACL associated with the subnet allow the traffic from the local IDC to pass through. Meanwhile, check whether the IDC allows the traffic from the cloud VPC to pass through.
Go to the server security group in VPC page. Click the security group ID to enter the “Security Group Rule” page to check:
Go to VPC subnet ACL rule, click the network ACL ID to enter the “Basic Info” page, and click “Inbound Rule” tab to check:
Security policy check on the IDC side (take Huawei Firewall as an example here):



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

If they do, please go to Step 5.

If not, please make the private IP ranges of the security devices on the security group/network ACL/IDC side open to Internet, and then go to Step 4.

4. Chec

k whether th

e communication is back to normal. In other words, log in to a server in the VPC/IDC and use the ping command to test the connectivity of the private IP of the peer server.

If it is, the problem is solved.

If not, please go to Step 5.

5. Ch

eck whether t

he CVM instance in the VPC and the firewall of the operating system of the server on the private network in the IDC have the policy to open the peer IP range to internet.

Checking the firewall on a Linux server: `iptables --list`

Checking the firewall on a Windows server: **Control Panel** > **System and Security** > **Windows Defender Firewall** > **Allow an app through Windows Firewall**

If they do, please go to Step 7.

If not, please enable the Internet connectivity of the business which needs to be connected in the private network firewall, and then go to Step 6.

6. Check

whether the co

mmunication is back to normal. In other words, log in to a server in the VPC/IDC and use the ping command to test the connectivity of the private IP of the peer server.

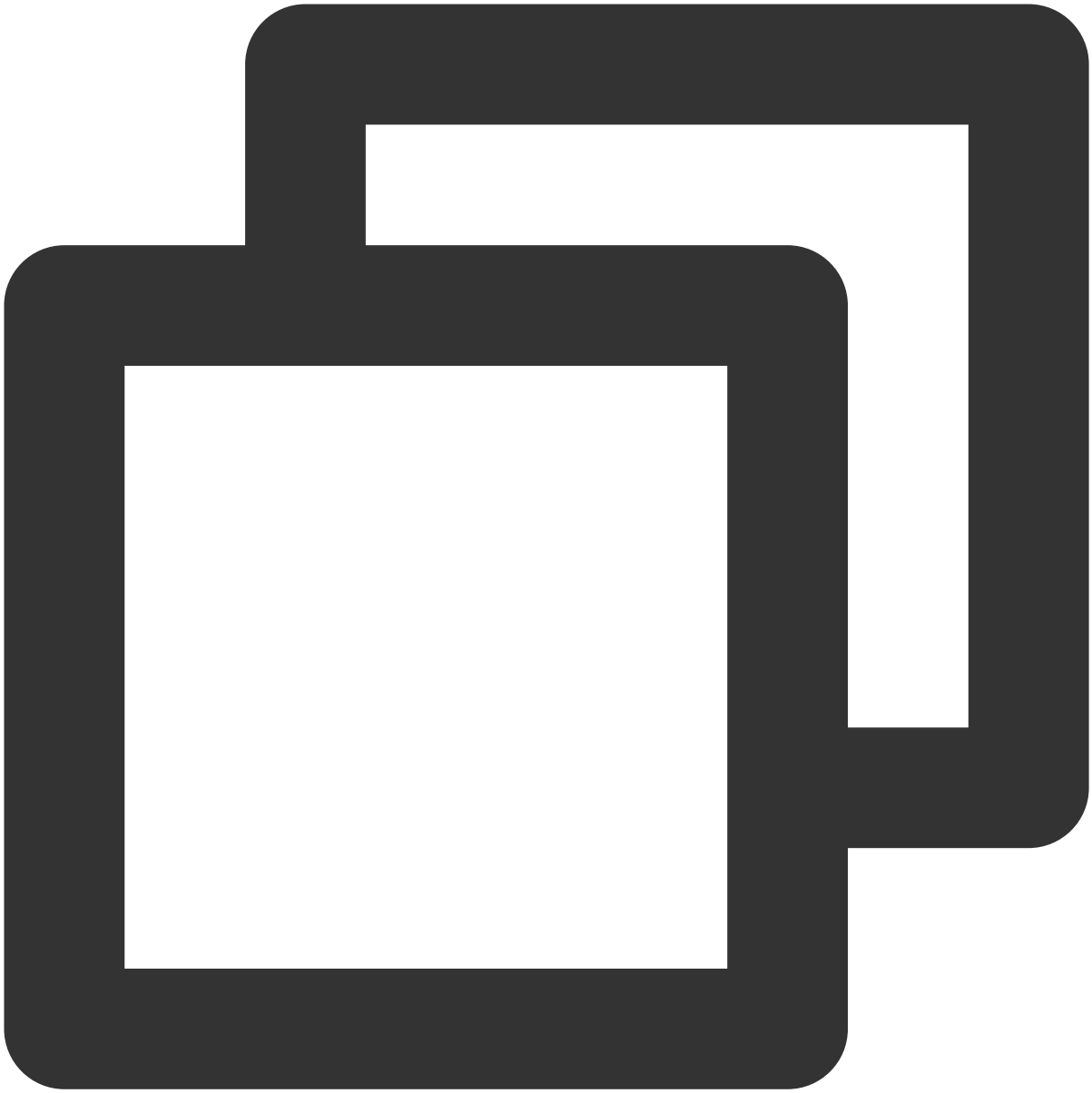
If it is, the problem is solved.

If not, please go to Step 7.

7. Check whether the proxy identity (SPD policy) of VPN tunnels on the VPC and IDC sides contains private IP ranges that need to be interconnected.

Go to the SPD policy page in the VPC console. Click the **VPN tunnel ID** to enter the **Basic information** page, and you can check the SPD policy:

SPD policy check on the IDC side (take Huawei Firewall as an example here):



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

If it is, please go to Step 8.

If not, please add the missing SPD policies and go to Step 8

8. Ch

eck whether

the route table of the VPN gateway contains the required routing policy. On the **VPN gateway** page, click the ID of the target VPN gateway to enter the **Route table** page, and you can check the routing policies.

If so, please go to Step 9.

If not, specify the next hop on the **Route** tab and perform step 9.

9. C

heck whether

the communication is back to normal. In other words, log in to a server in the VPC/IDC and use the ping command to test the connectivity of the private IP of the peer server.

If it is, the problem is solved.

If not, please go to Step 10.

10. Colle

ct the trouble

shooting information above and submit a ticket or ask the device manufacturer for help.

IPSec VPN Error Description for Negotiation Failure

Last updated：2024-08-15 16:02:23

Negotiation Phase	Error Prompt	Description
IKE negotiation	no match proposal	The IKE policies configured on the cloud side and the 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 **local identifier** and **peer identifier** configured on the cloud side are inconsistent with those configured on the client side, resulting in no response from the responder.
	initiator no peer config found by ID payload	The **local identifier** and **peer identifier** configured on the cloud side are inconsistent with those configured on the client side, resulting in no response from the requester.
	received xxx error notify	The cloud side received a message of negotiation failure 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 configurations on the cloud side and the client side are inconsistent. Please check.
	no matching proposal, configured xxx, received xxx	The child configurations on the cloud side and the client side do not match.
	received xxx error notify in the payload	The cloud side received a message of negotiation failure from the client side.