

Virtual Private Network

Troubleshooting

Issue 01
Date 2025-02-05



Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <https://www.huawei.com>

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

1 The State of a VPN Connection Is Not connected

Symptom

On the **Enterprise – VPN Connections** page of the VPN console, the state of a VPN connection is displayed as **Not connected**.



Possible Causes

- The configurations at the two ends of the VPN connection are incorrect.
- The security group configuration on the Huawei Cloud management console or the ACL configuration on the customer gateway device is incorrect.
- The IPsec VPN connection negotiation fails or the connection is disconnected.

Procedure

- Check the configurations at the two ends of the VPN connection.
 - Check whether the gateway IP addresses configured at the two ends of the VPN connection are reversed.
 - To check the active and standby EIPs of the VPN gateway, choose **Virtual Private Network > Enterprise – VPN Gateways** and view the IP addresses in the **Gateway IP Address** column.
 - To check the IP address of the customer gateway, choose **Virtual Private Network > Enterprise – Customer Gateways** and view the IP address in the **Gateway IP Address** column.
 - Check whether the IKE and IPsec policies at the two ends of the VPN connection are consistent.
 - To view the IKE and IPsec policy settings on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, locate the target VPN connection, and choose **More > Modify Policy Settings**.
 - Check whether the PSKs at the two ends of the VPN connection are the same.

- The PSK cannot be checked on the VPN console. If you are not sure whether the PSK configured on the VPN console is correct, you are advised to change it to be the same as that configured on the customer gateway device.
To change the PSK on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, locate the target VPN connection, and choose **More > Reset PSK**.
- If the policy-based mode is used, check whether the source and destination CIDR blocks in the policy rules at the two ends of the VPN connection are reversed.
To check policy rules on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, locate the target VPN connection, and click **Modify VPN Connection**.
- If the static routing mode is used and the NQA function is enabled on the VPN console, check whether tunnel interface IP addresses are correctly configured on the customer gateway device.
 - To check whether NQA is enabled on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, click the name of the target VPN connection, and view the value of **Link Detection** on the **Summary** tab page.
 - To check the tunnel interface IP addresses configured on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, click **Modify VPN Connection**, and view the values of **Local Interface IP Address** and **Customer Interface IP Address**. The local and remote interface IP addresses configured on the customer gateway device must be the same as the values of **Customer Interface IP Address** and **Local Interface IP Address** configured on the VPN console, respectively.
- If the BGP routing mode is used, check whether the BGP ASNs at the two ends of the VPN connection are reversed.
 - To check the BGP ASN of the VPN gateway, choose **Virtual Private Network > Enterprise – VPN Gateways**, click the VPN gateway name, and view the BGP ASN in the **Basic Information** area.
 - To check the BGP ASN of the customer gateway, choose **Virtual Private Network > Enterprise – Customer Gateways** and view the value in the **BGP ASN** column.
- Check the security group configuration on the Huawei Cloud management console and the ACL configuration on the customer gateway device.
 - Check whether the default security group on the Huawei Cloud management console permits the ports corresponding to the public IP addresses of the customer gateway.
To check the default security group on the Huawei Cloud management console, perform the following steps:
 - i. Choose **Virtual Private Network > Enterprise – VPN Gateways**, and click the name of the VPC associated with the VPN gateway.
 - ii. On the **Virtual Private Cloud** page, click the number in the **Route Tables** column.

- iii. On the **Route Tables** page, click the name of the route table.
- iv. Locate and click the next hop of the active or standby EIP of the VPN gateway.
- v. On the **Associated Security Groups** tab page, check whether the security group permits traffic of the ports.
- Verify that an ACL on the customer gateway device permits the ports corresponding to the active and standby EIPs of the VPN gateway.
- Check IPsec connection logs.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and select the desired region and project.
 - c. Click  in the upper left corner of the page, and choose **Networking > Virtual Private Network**.
 - d. In the navigation pane on the left, choose **Virtual Private Network > Enterprise - VPN Connections**.
 - e. On the **VPN Connection** page, locate the target VPN connection, and choose **More > View Logs** to view connection logs.

Check IPsec connection logs, and locate the fault based on the log keywords and error codes listed in [Table 1-1](#).

Table 1-1 Common causes of VPN disconnection

Category	Error Code	Description
IPsec VPN negotiation failure	phase1 proposal mismatch	IKE proposal parameters on both ends do not match.
	phase2 proposal or pfs mismatch	IPsec proposal parameters, PFS algorithms, or security ACLs on both ends do not match.
	responder dh mismatch	The DH algorithm of the responder does not match that of the initiator.
	initiator dh mismatch	The DH algorithm of the initiator does not match that of the responder.
	encapsulation mode mismatch	Encapsulation modes on both ends do not match.
	flow or peer mismatch	Security ACLs or IKE peer addresses on both ends do not match.
	version mismatch	IKE versions on both ends do not match.
	peer address mismatch	IKE peer addresses on both ends do not match.

Category	Error Code	Description
	config ID mismatch	No IKE peer with the specified ID is found.
	exchange mode mismatch	Negotiation modes on both ends do not match.
	authentication fail	The identity authentication fails.
	construct local ID fail	A local ID fails to be constructed.
	rekey no find old sa	The old SA fails to be found during renegotiation.
	rekey fail	The old SA is going offline during renegotiation.
	first packet limited	First packets are rate limited.
	unsupported version	The IKE version is not supported.
	malformed message	There is a malformed message.
	malformed payload	There is a malformed payload.
	critical drop	The critical payload is not recognized.
	cookie mismatch	The cookies do not match.
	invalid cookie	The cookie is invalid.
	invalid length	The packet length is invalid.
	unknown exchange type	The negotiation mode is unknown.
	uncritical drop	The non-critical payload is not identified.
	route limit	The number of imported routes reaches the upper limit.
	ip assigned fail	IP address assignment fails.
	eap authentication timeout	EAP authentication times out.
	eap authentication fail	EAP authentication fails.
	xauth authentication fail	XAUTH authentication fails.
	xauth authentication timeout	XAUTH authentication times out.

Category	Error Code	Description
	license or specification limited	There is license control.
	local address mismatch	The local IP address and interface IP address in IKE negotiation do not match.
	dynamic peers number reaches limitation	The number of IKE peers reaches the upper limit.
	ipsec tunnel number reaches limitation	The number of IPsec tunnels reaches the upper limit.
	netmask mismatch	The mask does not match the configured one after the IPsec mask filtering function is enabled.
	flow conflict	A data flow conflict exists.
	proposal mismatch or use sm in ikev2	IPsec proposals on both ends do not match or IKEv2 uses an SM algorithm.
	ikev2 not support sm in ipsec proposal ikev2	IKEv2 does not support the SM algorithm used in the IPsec proposal.
	no policy applied on interface	No policy is applied to an interface.
	nat detection fail	NAT detection fails.
	fragment packet limit	The number of fragments exceeds the upper limit.
	fragment packet reassemble timeout	Fragment reassembly times out.
IPsec VPN connection disconnection	dpd timeout	DPD detection times out.
	peer request	The remote end sends a message, asking the local end to tear down a tunnel.
	config modify or manual offline	The SA is automatically deleted due to configuration modification, or is manually deleted.
	phase1 hard expiry	In phase 1, hard timeout (no new SA negotiation succeeds) occurs.
	phase2 hard expiry	A hard timeout occurs in phase 2.
	heartbeat timeout	Heartbeat detection times out.

Category	Error Code	Description
	re-auth timeout	The SA is deleted because the re-authentication times out.
	aaa cut user	The SA is deleted because the AAA module logs out the user.
	ip address syn failed	IP addresses fail to be synchronized.
	hard expiry triggered by port mismatch	Hard timeout occurs due to a NAT port number mismatch.
	kick old sa with same flow	The old SA is deleted when the same flow is transmitted.
	cpu table updated	When an SPU is removed and inserted, the SAs of CPUs other than the one on the SPU are deleted.
	flow overlap	The IP address in the encrypted data flow conflicts with the remote IP address.
	spi conflict	An SPI conflict occurs.
	phase1 sa replace	A new IKE SA replaces the old one.
	phase2 sa replace	A new IPsec SA replaces the old one.
	nhrp notify	The NHRP module notifies the device of SA deletion.
	receive backup delete info	The standby device receives an SA backup deletion message from the active device.
	eap delete old sa	When the peer device performs EAP authentication repeatedly, the local device deletes the old SA.
	receive invalid spi notify	The device receives an invalid SPI notification.
	dns resolution status change	The DNS resolution status is changed.
	ikev1 phase1-phase2 sa dependent offline	The device deletes the associated IPsec SA when deleting an IKEv1 SA.
	exchange timeout	Packet exchange times out.

Category	Error Code	Description
	hash gene adjusted	The hash factor is adjusted, causing the IPsec tunnel to be deleted.

If the fault persists after you verify the preceding configurations, contact Huawei engineers by [submitting a service ticket](#).

2 Ping Tests Between Cloud and On-premises Networks Fail

Symptom

- Servers in an on-premises data center cannot ping ECSs in a Huawei Cloud VPC.
- ECSs in a Huawei Cloud VPC cannot ping the servers in an on-premises data center.

Possible Causes

- The security group configuration on the Huawei Cloud management console is incorrect.
- The ACL rule associated with the interconnection subnet is incorrectly configured.
- The ACL configuration on the customer gateway device is incorrect.
- The route configuration on the customer gateway device is incorrect.

Procedure

- Check the security group configuration on the Huawei Cloud management console.
 - Verify that the default security group on the Huawei Cloud management console permits data flows destined for the customer subnet.
To check the default security group on the Huawei Cloud management console, perform the following steps:
 - i. Choose **Virtual Private Network > Enterprise – VPN Gateways**, and click the name of the VPC associated with the VPN gateway.
 - ii. Click the number of route tables corresponding to the VPC.
 - iii. On the **Route Tables** page, click the name of the route table.
 - iv. Locate and click the next hop of the active or standby EIP of the VPN gateway.
 - v. On the **Associated Security Groups** tab page, check the ports permitted by the security group.

- Verify that the default security group on the Huawei Cloud management console permits data flows originated from the customer subnet.
- Verify that the default security group on the Huawei Cloud management console permits data flows destined for the local subnet.
- Verify that the default security group on the Huawei Cloud management console permits data flows originated from the local subnet.
- Verify that a security group permits data flows from the ECSs on Huawei Cloud to the customer subnet.
To check whether such a security group has been configured, choose **Compute > Elastic Cloud Server**, click an ECS name, click the **Security Groups** tab, and click **Manage Rule**.
- Verify that a security group permits data flows from the customer subnet to the ECSs on Huawei Cloud.
- The ACL rule associated with the interconnection subnet is incorrectly configured.
 - Check whether the ACL rule associated with the interconnection subnet permits the ports between all local and customer subnets.
 - i. Choose **Virtual Private Network > Enterprise – VPN Gateways**, and click the name of target VPN gateway.
 - ii. In the **Basic Information** area, check and record the interconnection subnet.
 - iii. In the **Basic Information** area, click the name of the associated VPC.
 - iv. On the **Summary** tab page of the VPC, click the number of subnets in the **Networking Components** area.
 - v. Find the interconnection subnet in the subnet list, and click the ACL name in the **Network ACL** column.
 - vi. Permit the ports between all local and customer subnets.
- Check the ACL configuration on the customer gateway device.
 - Verify that an ACL rule on the customer gateway device permits data flows destined for the local subnet of the Huawei Cloud VPN gateway.
 - Verify that an ACL rule on the customer gateway device permits data flows originated from the local subnet of the Huawei Cloud VPN gateway.
To check the local subnet of the Huawei Cloud VPN gateway, choose **Virtual Private Network > Enterprise – VPN Gateways**, click the VPN gateway name, and view the value of **Local Subnet** in the **Basic Information** area.
- Check the route configuration on the customer gateway device.
 - Verify that the public network route is correctly configured. That is, the destination address is an EIP of the Huawei Cloud VPN gateway, and the next hop is the egress interface address of the customer gateway device.
 - Verify that the private network route is correctly configured. That is, the destination address is the local subnet of the Huawei Cloud VPN gateway, and the next hop is the egress interface address of the customer gateway device.
To check the local subnet of the Huawei Cloud VPN gateway, choose **Virtual Private Network > Enterprise – VPN Gateways**, click the VPN

gateway name, and view the value of **Local Subnet** in the **Basic Information** area.

3 Packet Loss Occurs

Symptom

- Packet loss occurs when a server in an on-premises data center pings an ECS in a Huawei Cloud VPC.
- Packet loss occurs when an ECS in a Huawei Cloud VPC pings a server in an on-premises data center.

Procedure

- Check the customer-side networking and bandwidth.
 - Check whether the customer network has multiple egresses working in load balancing mode and whether traffic destined for Huawei Cloud is distributed to a non-VPN egress. Ensure that the traffic destined for Huawei Cloud is transmitted through the same egress.
 - Ping the IP address of the VPN gateway on Huawei Cloud and other public IP addresses (for example, 114.114.114.114) from the customer gateway to check the delay and packet loss rate on the public network. If the quality of the public network is poor, you are advised to seek help from the corresponding carrier.
 - Check whether traffic on the customer gateway device exceeds the bandwidth limit.
- Check the Huawei Cloud-side networking and bandwidth.
 - Check whether traffic exceeds the bandwidth of the Huawei Cloud VPN gateway.
 - i. Check the bandwidth of active and standby EIPs of the VPN gateway as follows: Choose **Virtual Private Network > Enterprise – VPN Gateways**, click the VPN gateway name, and check the value of **Bandwidth (Mbit/s)** in the **EIP** area.
 - ii. Check the actual bandwidth usage of the VPN gateway as follows: Choose **Virtual Private Network > Enterprise – VPN Gateways**, and click  in the **Public IP Address** column of the VPN gateway.

If traffic exceeds the bandwidth of the VPN gateway, increase the bandwidth.

- If the fault persists after you verify the preceding configurations, contact Huawei engineers by [submitting a service ticket](#).

4 Client Connection Failures

4.1 The Client Log Contains "Connection failed to establish within given time"

Applicable Client

Windows OpenVPN Connect

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
Connection failed to establish within given time
```

Possible Causes

- The client device cannot access the Internet.
- The existing client configuration file is inconsistent with that on the **Server** tab page of the VPN gateway.

Procedure

1. Try to access other Internet services on the client device.
If the access also fails, contact your carrier to rectify the network connectivity fault.
2. Log in to the Huawei Cloud management console.
3. Locate the target VPN gateway, and check whether the gateway address, server port, and protocol are the same as those in the client configuration file.
If not, download the client configuration file again or directly modify the client configuration file, and then use the new client configuration file to reconnect the client to the VPN gateway.

4.2 The Client Log Contains "Cannot load CA certificate file [[INLINE]](no entries were read)"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
Cannot load CA certificate file [[INLINE]](no entries were read)
```

Possible Causes

There is no client certificate or private key in the client configuration file.

Procedure

Copy the client certificate and private key to the client configuration file, and reconnect the client to the VPN gateway. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

4.3 The Client Log Contains "error:068000A8:asn1 encoding routines:wrong tag"

Applicable Client

- Linux
- Windows OpenVPN GUI
- Windows OpenVPN Connect

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
error:068000A8:asn1 encoding routines:wrong tag
```

Possible Causes

The client certificate and private key do not match.

Procedure

Copy the correct client certificate and private key to the client configuration file, and reconnect the client to the VPN gateway. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

4.4 The Client Log Contains "OpenSSL: error:0A000086:SSL routines::certificate verify failed"

Applicable Client

- Linux
- Windows OpenVPN GUI
- Windows OpenVPN Connect

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
OpenSSL: error:0A000086:SSL routines::certificate verify failed
```

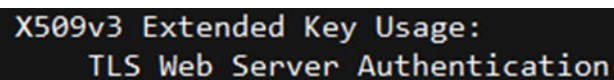
Possible Causes

The server certificate used by the VPN gateway does not contain the Extended Key Usage attribute. As a result, certificate verification fails.

Procedure

1. Check and verify that the generated server certificate contains the Extended Key Usage attribute, as shown in [Figure 4-1](#).

Figure 4-1 Extended Key Usage



```
X509v3 Extended Key Usage:
  TLS Web Server Authentication
```

- A server certificate generated by the Easy-RSA shell command `./easyrsa build-server-full` contains this attribute by default.

- A server certificate issued through OpenSSL does not contain this attribute. You need to add **extendedKeyUsage = serverAuth** to the server certificate file.
- 2. Host the server certificate containing this attribute in the CCM, replace the server certificate with a correct one on the **Server** tab page of the VPN gateway, and reconnect the client to the VPN gateway.

4.5 The Client Log Contains "TLS Error: TLS handshake failed"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
TLS Error: TLS handshake failed
```

Possible Causes

The certificate and private key in the client configuration file do not match the client CA certificate imported on the **Server** tab page of the VPN gateway.

Procedure

1. Check whether the imported client CA certificate is correct.
If the certificate and private key in the configuration file do not match the imported client CA certificate, import the correct CA certificate on the **Server** tab page of the VPN gateway, delete the incorrect CA certificate, and reconnect the client to the VPN gateway.
2. Check whether the certificate and private key in the configuration file are correct.
If the certificate and private key in the configuration file do not match, copy the correct client certificate content and private key to the client configuration file, and reconnect the client to the VPN gateway.

4.6 The Client Log Contains "Options error: Unrecognized option or missing or extra parameter(s) in XXX: disable-dco"

Applicable Client

Linux

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
Options error: Unrecognized option or missing or extra parameter(s) in XXX: disable-dco
```

Possible Causes

The OpenVPN client software earlier than 2.6 is used, which cannot identify the **disable-dco** configuration item.

Procedure

1. Log in to the Huawei Cloud management console.
2. Download the client configuration. The **client_config.ovpn** file is generated.
3. Open the **client_config.ovpn** file, and add a comment character (#) in front of the **disable-dco** configuration item.
4. Save the configuration file, and reconnect the client to the VPN gateway through the new configuration.

4.7 The Client Log Contains "TCP: connect to [AF_INET] *.*.*.*:**** failed: Unknown error"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
TCP: connect to [AF_INET] *.*.*.*:**** failed: Unknown error
```

Possible Causes

- The client device cannot access the Internet.
- The protocol or port number in the client configuration file is different from that configured on the **Server** tab page of the VPN gateway.

Procedure

1. Try to access other Internet services on the client device.
If the access also fails, contact your carrier to rectify the network connectivity fault.
2. Log in to the Huawei Cloud management console.
3. Locate the target VPN gateway, and check whether the server protocol and port are the same as those in the client configuration file.

If not, download the client configuration file again or directly modify the client configuration file, and then use the new client configuration file to reconnect the client to the VPN gateway.

4.8 The Client Log Contains "AUTH: Received control message: AUTH_FAILED"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
AUTH: Received control message: AUTH_FAILED
```

Possible Causes

- The username and password did not match.
- The user account is locked after the user entered incorrect passwords for five consecutive times.
- If a static IP address has been configured for the user, the client can set up only one connection.

Procedure

1. Log in to the Huawei Cloud management console.
2. Check the username and password for logging in to the client.
If the account is locked due to multiple incorrect password attempts, wait for about 5 minutes and then use the correct username and password for login.
3. Check whether a static IP address has been configured for the user.
Click **View Server** in the **Operation** column of the corresponding VPN gateway, choose **User Management > Users**, and check whether a static IP address has been configured for the user.

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.9 The Client Log Contains "AUTH_FAILED"

Applicable Client

Windows OpenVPN Connect

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
AUTH_FAILED
```

Possible Causes

- The username and password did not match.
- The user entered incorrect passwords for five consecutive times, and the user account is locked.
- The certificate and private key in the client configuration file do not match the client CA certificate imported on the **Server** tab page of the VPN gateway.
- If a static IP address has been configured for the user, the client can set up only one connection.

Procedure

1. Check the username and password for logging in to the client.
If the account is locked due to multiple incorrect password attempts, wait for about 5 minutes and then use the correct username and password for login.
2. Check whether the imported client CA certificate is correct.
If the certificate and private key in the configuration file do not match the imported client CA certificate, import the correct CA certificate on the **Server** tab page of the VPN gateway, delete the incorrect CA certificate, and reconnect the client to the VPN gateway.
3. Check whether the certificate and private key in the configuration file are correct.
If the certificate and private key in the configuration file do not match, copy the correct client certificate content and private key to the client configuration file, and reconnect the client to the VPN gateway.
4. Check whether a static IP address has been configured for the user.
Click **View Server** in the **Operation** column of the corresponding VPN gateway, choose **User Management > Users**, and check whether a static IP address has been configured for the user.

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

5 Successful Client Connection but Unavailable Services

5.1 A Client Cannot Ping an ECS IP Address

Symptom

A client is connected to a P2C VPN gateway, but cannot ping an ECS IP address.

Possible Causes

- Ping detection is disabled on the client device or ECS.
- Ping detection packets are denied by a security group of the ECS.
- The local CIDR block of the VPN gateway does not contain the IP address of the ECS to be accessed.
- The user group to which the user belongs is not configured, or the user group is not configured with the corresponding access policy.
- After the specified IP address of a client is changed and the client automatically reconnects to the server, the route to the local subnet is not generated in the routing table on the Windows operating system.

Procedure

- Check whether ping detection is disabled in an access control policy of the client device or ECS.
If so, modify the policy to permit ping detection. For the Windows operating system, you also need to modify the inbound rules of the firewall to permit ICMPv4-In.
- Verify that the inbound and outbound rules in the ECS's security group permit ICMP packets.
- On the **Server** tab page of the VPN gateway, change the local CIDR block to include the IP address of the ECS to be accessed. Then, disconnect the client, reconnect it, and run the following command to check whether the client device receives the route advertised by the VPN gateway:

- Windows operating system: **route print** command
- Linux operating system: **ip route show all** command
- On the user management page of the server, configure the user group to which the user belongs or configure an access policy for the user group.
- Check the local CIDR block and client address pool configured on the server.
 - Local CIDR block: 192.168.1.XX
 - Client address pool: 172.16.0.0

On the client, check whether the route to the local CIDR block is generated.

- If the route is generated, the IP address assigned to the client is 172.16.0.5.

The command output is as follows:

```
IPv4 Routing Table
=====
Active Routes:
Network Destination    Netmask          Gateway         Interface  Metric
-----
192.168.1.XX          255.255.255.0    172.16.0.0     172.16.0.5  281
192.168.2.XX          255.255.255.0    172.16.0.0     172.16.0.5  281
192.168.3.XX          255.255.255.0    172.16.0.0     172.16.0.5  281
=====
```

- If the route is not generated, disconnect the client and reconnect it.

5.2 Packet Loss Occurs During Service Access

Symptom

A client is connected to a P2C VPN gateway, but packet loss occurs during service access.

Possible Causes

- Service traffic bursts or continuously exceeds the bandwidth of the VPN gateway instance.
- The bandwidth of the EIP bound to the VPN gateway is insufficient.
- The quality of the Internet is poor.

Procedure

1. Go to the traffic monitoring view from the VPN gateway list page, and check whether traffic bursts or continuously approaches the bandwidth specification of the VPN gateway.
2. On the **Basic Information** page of the VPN gateway, view the EIP bandwidth, and check whether traffic exceeds the EIP bandwidth based on the traffic information in the traffic monitoring view.
If the traffic exceeds the EIP bandwidth, increase the EIP bandwidth.
3. Ping the public IP address of the VPN gateway from the client to detect the Internet link quality.
If the quality of the Internet link is poor, contact the carrier to resolve the problem.

6 S2C Classic VPN

6.1 Common Check Items

VPN connections or ping operations fail when configurations (such as the negotiation policy, firewall, route table, interzone policy, NAT configuration, and security group) are incorrect.

Check the following configurations.

- [Checking the Negotiation Information on Both Sides of a VPN Connection](#)
- [Checking the Firewall Configuration on Your Local Network and the Security Group Configuration on the Cloud](#)
- [Checking the Firewall Route Table](#)
- [Checking the Firewall Inter-zone Policy](#)
- [Checking the NAT Configurations on the Firewall](#)

Checking the Negotiation Information on Both Sides of a VPN Connection

- Ensure that the PSKs of the two sides are the same.
- Ensure the IKE policies and the IPsec policies of the two sides are the same.
- Local and remote subnets are matched pairs.

Checking the Firewall Configuration on Your Local Network and the Security Group Configuration on the Cloud

- Ensure that data packets from your network to the VPC subnet on Huawei Cloud are permitted.
- Ensure that data packets from the VPC subnet on Huawei Cloud to your network are permitted.

Checking the Firewall Route Table

Verify that there is a route to the VPC subnet on Huawei Cloud.

- Ensure that a route table contains a route to the target network on Huawei Cloud.

- Ensure that the forwarding table of the route works properly.

 **NOTE**

Incorrect route configurations:

1. The destination CIDR block is different from the VPC CIDR block. In this case, traffic destined for Huawei Cloud cannot be routed to the public network interface configured with the IPsec policy.
2. The outbound interface rather than the next hop is specified when configuring a static route.

On an Ethernet network, the outbound interface cannot learn the ARP entries from the remote side, leading to route forwarding failure.

3. The VPN gateway address on Huawei Cloud is specified as the next hop of the route.

Some third-party devices do not support automatic route recursion. VPN traffic is sent from the public network interface. Therefore, the next hop must be the gateway address provided by the carrier.

Checking the Firewall Inter-zone Policy

- From the Trust zone to the Untrust zone: Allows access from your local network to the VPC subnet on the cloud.
- From the Untrust zone to the Trust zone: Allows access from the VPC on the cloud to your local network.

Checking the NAT Configurations on the Firewall

Check whether the local VPN gateway is behind the NAT device (usually the border firewall). That is, the outbound interface of the VPN gateway uses a private IP address, and then it is translated into a public IP address by the NAT device.

This scenario is also called IPsec NAT traversal.

6.2 Common Configuration Issues and Solutions

- Inconsistent PSKs: PSK update takes effect in the next IKE negotiation. Ensure that the PSKs at both ends are the same.
- Inconsistent negotiation policies: Check the authentication algorithm, encryption algorithm, version, DH algorithm, and negotiation mode in the IKE policy, and the authentication algorithm, encryption algorithm, encapsulation format, and PFS algorithm in the IPsec policy. Ensure the PFSs at both ends are the same. By default, the PFS configuration is disabled on some devices.
- Interesting traffic: Check the ACL configurations at both ends. The actual IP address and mask must be used.
- NAT configuration: Do not perform NAT on the on-premises subnet that used to access the cloud.
- Security policies: Allow all protocols used by the on-premises subnet to access the cloud subnet, and allow two public IP addresses to communicate on UDP port 500 and UDP port 4500 using ESP or AH.
- Route configurations: Set the outbound interface for accessing the cloud subnet to the tunnel interface or IPsec negotiation interface. Ensure that the next-hop ARP resolution of the outbound interface is reachable.

For more information, see [Connection or Ping Failure](#).