

Virtual Private Network

Troubleshooting

Issue 01
Date 2023-10-23



Copyright © Huawei Technologies Co., Ltd. 2023. 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.

Contents

1 The State of a VPN Connection Is Not connected.....	1
2 Ping Tests Between Cloud and On-premises Networks Fail.....	4
3 Packet Loss Occurs.....	6
4 Classic VPN.....	8
4.1 Common Check Items.....	8
4.2 Common Configuration Issues and Solutions.....	9

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.

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 traffic of UDP ports 500 and 4500 originated from the public IP address 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 traffic of UDP ports 500 and 4500 originated from the active and standby EIPs of the VPN gateway.

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 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. 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 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** and click **More > Manage Network > Security Group Rule Configuration** in the **Operation** column.

- Verify that a security group permits data flows from the customer subnet to the ECSs on Huawei Cloud.
- 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 Classic VPN

4.1 Common Check Items

VPN connections fail or cannot be pinged 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 Configurations of the Firewall on Your Local Network and the Security Group on Huawei 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 Configurations of the Firewall on Your Local Network and the Security Group on Huawei Cloud

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

Checking the Firewall Route Table

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

- Ensure that a route table contains the 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 to 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 non-Huawei 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.

4.2 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](#).