Virtual Private Network

Troubleshooting

Issue	01
Date	2021-06-30



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. 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


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 Common Check Items.....1
2 Common Configuration Issues and Solutions.....3

 Copyright © Huawei Technologies Co., Ltd.

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 Interzone 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.
- Ensure that the local subnet of one side is the same as the remote subnet of the other side and the remote subnet of one side is the same as the local subnet of the other side.

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.

 Copyright © Huawei Technologies Co., Ltd.

- 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 iteration. VPN traffic is sent from the public network interface. Therefore, the next hop must be the gateway address provided by the carrier.

     The following uses the Cisco device as an example.

     IP route: *192.168.1.0; 255.255.255.0; a.b.c.d*

     192.168.1.0/24 is the CIDR block of a VPC on HUAWEI CLOUD and *a.b.c.d* is the gateway address provided by the carrier.

Checking the Firewall Interzone Policy

- From a trust zone to an untrust zone: Allows access from your local network to the VPC subnet on the cloud.
- From an untrust zone to a 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.

 Copyright © Huawei Technologies Co., Ltd.

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 value of PFS on the cloud and that off the cloud 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**.

 Copyright © Huawei Technologies Co., Ltd.