

# Virtual Private Network

## FAQs

**Issue** 01  
**Date** 2023-10-11



**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

---

<b>1 Popular Questions.....</b>	<b>1</b>
1.1 What Devices Can Be Connected to Huawei Cloud Through a VPN?.....	1
1.2 What Are VPN Negotiation Parameters? What Are Their Default Values?.....	2
1.3 What Types of VPN Service Tickets Are There? How Do I Create a VPN Service Ticket?.....	4
1.4 Can I Deploy an Application on the Cloud and a Database in an On-premises Data Center and Connect Them Through a VPN?.....	6
1.5 Can I Visit Websites Across International Borders Using a VPN?.....	6
1.6 What Is a VPN Connection? How Do I Set the Number of VPN Connections When Buying a VPN Gateway?.....	7
1.7 Will I Be Notified If a VPN Connection Is Interrupted?.....	7
1.8 Are a Username and Password Required for Creating an IPsec VPN Connection?.....	7
1.9 What Are the Differences Between IPsec VPN and SSL VPN in Application Scenarios and Connection Modes?.....	8
1.10 Is an IPsec VPN Connection Automatically Established?.....	8
1.11 How Will I Be Charged for My Use of a VPN? Will I Be Charged for VPN Gateway EIPs?.....	9
1.12 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?.....	9
1.13 What VPN Resources Can Be Monitored?.....	9
1.14 In Which Direction Is the VPN Bandwidth Limited? What Is the Unit of Bandwidth?.....	10
1.15 How Is the Network Speed of a VPN Connection Tested?.....	10
1.16 Can a VPN Billed by Traffic Use a Shared Data Package?.....	12
1.17 How Do I Change the Billing Mode of a VPN Gateway from Pay-Per-Use to Yearly/Monthly?.....	12
1.18 What Are the Relationships Between a VPC, a VPN Gateway, and a VPN Connection?.....	13
1.19 What Are a Customer Gateway and a Customer Subnet in a VPN Connection?.....	13
1.20 How Many VPN Connections Do I Need to Connect Multiple On-premises Servers to the Cloud?.....	14
1.21 Does a VPN Allow for Communications Between Two VPCs?.....	14
1.22 What Are the Impacts of a VPN on an On-premises Network? What Are the Changes to the Route for Accessing an ECS?.....	15
1.23 Can I Connect a Network with Two Egresses to a VPC Through Two VPN Connections?.....	15
1.24 How Can I Prevent VPN Disconnections?.....	15
1.25 What Do I Do If a VPN Connection Fails to Be Established?.....	16
1.26 Can EIPs Be Used as VPN Gateway IP Addresses?.....	16
1.27 Why Is a VPN Connection Always in Not Connected State After Its Configuration Is Complete?.....	16
1.28 Do I Need to Configure ACL Rules on the Huawei Cloud Management Console After I Configure ACL Rules on the On-premises Gateway Device?.....	17

<b>2 General Consulting</b> .....	<b>18</b>
2.1 What Are the Typical Scenarios of IPsec VPN?.....	18
2.2 What Are a VPC, a VPN Gateway, and a VPN Connection?.....	18
2.3 What Are the Relationships Between a VPC, a VPN Gateway, and a VPN Connection?.....	19
2.4 What Is a VPN Connection? How Do I Set the Number of VPN Connections When Buying a VPN Gateway?.....	19
2.5 What Are a Customer Gateway and a Customer Subnet in a VPN Connection?.....	20
2.6 How Do I Plan CIDR Blocks for Access to a VPC Through a VPN Connection?.....	20
2.7 Is an IPsec VPN Connection Automatically Established?.....	20
2.8 What Types of VPN Service Tickets Are There? How Do I Create a VPN Service Ticket?.....	20
2.9 What Devices Can Be Connected to Huawei Cloud Through a VPN?.....	22
2.10 What Are VPN Negotiation Parameters? What Are Their Default Values?.....	23
2.11 Are a Username and Password Required for Creating an IPsec VPN Connection?.....	25
2.12 How Do I Allow Specific Hosts to Access a VPC Subnet Through a Created VPN Connection?.....	26
2.13 What VPN Resources Can Be Monitored?.....	26
2.14 Can EIPs Be Used as VPN Gateway IP Addresses?.....	27
2.15 Do I Need to Purchase EIPs for Hosts to Communicate with Each Other Through a VPN?.....	27
2.16 Are SSL VPNs Supported?.....	27
2.17 How Long Does It Take for Delivered VPN Configurations to Take Effect?.....	27
2.18 Does Huawei Cloud VPN Support IPv6 Addresses?.....	27
2.19 How Do I Determine My VPN Bandwidth?.....	27
2.20 Does a VPN Connection Support SM Series Cryptographic Algorithms?.....	28
2.21 Which IKE Version Should I Select When I Create a VPN Connection?.....	28
2.22 How Many Bits Do the DH Groups Used by Huawei Cloud VPN Have?.....	30
2.23 Can I Visit Websites Across International Borders Using a VPN?.....	30
2.24 Can I Deploy an Application on the Cloud and a Database in an On-premises Data Center and Connect Them Through a VPN?.....	31
2.25 What Are the Differences Between IPsec VPN and SSL VPN in Application Scenarios and Connection Modes?.....	31
2.26 How Will I Be Charged for My Use of a VPN? Will I Be Charged for VPN Gateway EIPs?.....	32
2.27 What Are the Differences Between Billing the VPN Gateway EIP Bandwidth by Bandwidth and by Traffic?.....	32
2.28 Can a VPN Billed by Traffic Use a Shared Data Package?.....	33
2.29 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?.....	33
2.30 Where Can I Add Routes to Customer Subnets on the VPN Console?.....	33
2.31 Will I Be Notified If a VPN Connection Is Interrupted?.....	33
2.32 What Do I Do If a VPN Connection Fails to Be Established?.....	33
2.33 In Which Direction Is the VPN Bandwidth Limited? What Is the Unit of Bandwidth?.....	34
2.34 Can I Restore a VPN Gateway or VPN Connection That Is Incorrectly Deleted?.....	34
<b>3 Networking and Application Scenarios</b> .....	<b>36</b>
3.1 Can I Visit Websites Across International Borders Using a VPN?.....	36
3.2 Can I Deploy an Application on the Cloud and a Database in an On-premises Data Center and Connect Them Through a VPN?.....	36

3.3 How Many VPN Connections Do I Need to Connect Multiple On-premises Servers to the Cloud?.....	37
3.4 What Are the Differences Between IPsec VPN and SSL VPN in Application Scenarios and Connection Modes?.....	37
3.5 Does a VPN Allow for Communications Between Two VPCs?.....	38
3.6 What Are the Impacts of a VPN on an On-premises Network? What Are the Changes to the Route for Accessing an ECS?.....	38
3.7 What Configurations Are Required at Both Ends of a VPN That Connects an On-premises Data Center to a VPC?.....	39
3.8 Can I Connect a Network with Two Egresses to a VPC Through Two VPN Connections?.....	39
3.9 Can I Connect Two VPCs in the Same Region Through a VPN?.....	39
3.10 How Can I Connect Two VPCs in the Same Region?.....	39
3.11 How Do I Enable Communications Between Two VPCs and an On-premises Network?.....	40
3.12 How Do I Connect Four Subnets?.....	40
3.13 Do I Need Two VPN Connections to Connect Four Subnets of Two Regions If Each Region Has Two Subnets?.....	41
3.14 Can I Access OBS Through a VPN?.....	41
3.15 How Do I Connect My Personal Computer to the Cloud Through a VPN?.....	42
3.16 How Do I Access Huawei Cloud ECSs at Home When My Enterprise Network Has Been Connected to Huawei Cloud Through a VPN?.....	42
3.17 How Do I Establish a VPN Connection Temporarily If No IPsec-Capable On-Premises Device Is Available After I Purchase a Huawei Cloud VPN Gateway and VPN Connection?.....	42
3.18 How Do I Select a Proper Region on the Cloud When I Buy a VPN Gateway?.....	42
<b>4 Billing and Payments.....</b>	<b>44</b>
4.1 How Will I Be Charged for My Use of a VPN? Will I Be Charged for VPN Gateway EIPs?.....	44
4.2 What Are the Differences Between Billing the VPN Gateway EIP Bandwidth by Bandwidth and by Traffic?.....	44
4.3 Can a VPN Billed by Traffic Use a Shared Data Package?.....	45
4.4 For How Many VPN Connections Will I Be Charged to Connect VPCs in Different Regions?.....	45
4.5 How Do I Change the Billing Mode of a VPN Gateway from Pay-Per-Use to Yearly/Monthly?.....	45
4.6 Will a Yearly/Monthly VPN Gateway Be Automatically Renewed?.....	46
4.7 Can I Unsubscribe from a Yearly/Monthly VPN Gateway?.....	46
4.8 When Will My VPN Resources Be Frozen? How Can I Unfreeze the VPN Resources?.....	46
4.9 How Are VPN Resources Billed and How Do I Use Coupons?.....	47
<b>5 Operations on the Console.....</b>	<b>48</b>
5.1 What Are the Relationships Between a VPC, a VPN Gateway, and a VPN Connection?.....	48
5.2 How Long Does It Take for Delivered VPN Configurations to Take Effect?.....	48
5.3 Why Is a VPN Connection Always in Not Connected State After Its Configuration Is Complete?.....	49
5.4 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?.....	49
5.5 What Information About a Created VPN Can Be Modified and What Information Cannot Be Modified?.....	49
5.6 Do I Need to Configure ACL Rules on the Huawei Cloud Management Console After I Configure ACL Rules on the On-premises Gateway Device?.....	51
5.7 What Do I Do If an Exception Occurs When I Add a Customer Subnet During VPN Connection Creation?.....	51

5.8 Where Can I Configure Routes to Customer Subnets on the VPN Console?.....	51
5.9 Can I Call APIs to Manage Huawei Cloud VPN Resources?.....	51
5.10 What Are a Customer Gateway and a Customer Subnet in a VPN Connection?.....	51
5.11 How Do I Disable PFS When Creating a VPN Connection?.....	52
5.12 How Many Local and Customer Subnets Can I Add to a VPN?.....	52
5.13 What Are the Precautions for Configuring the Local and Customer Subnets for a VPN Connection? .....	52
5.14 Why Is a VPN Connection in Not Connected State on the Management Console When It Is Already Available?.....	53
5.15 What Can I Do If a Message Is Displayed Indicating That the VPN Connection Does Not Exist After Negotiation Policies Are Modified?.....	53
5.16 What Is the Maximum Bandwidth Supported by a VPN Gateway?.....	53
5.17 Which IKE Version Should I Select When I Create a VPN Connection?.....	53
5.18 What Types of VPN Service Tickets Are There? How Do I Create a VPN Service Ticket?.....	55
5.19 Are a Username and Password Required for Creating an IPsec VPN Connection?.....	57
5.20 What VPN Resources Can Be Monitored?.....	57
5.21 Will I Be Notified If a VPN Connection Is Interrupted?.....	57
<b>6 VPN Negotiation and Interconnection.....</b>	<b>59</b>
6.1 What Devices Can Be Connected to Huawei Cloud Through a VPN?.....	59
6.2 What Are VPN Negotiation Parameters? What Are Their Default Values?.....	60
6.3 Is an IPsec VPN Connection Automatically Established?.....	62
6.4 How Do I Configure a VPN on an On-premises Device? (Example of Configuring VPN on a Huawei USG6600 Series Firewall).....	63
6.5 Does Huawei Cloud VPN Support Interconnection with a Customer Gateway Through a Domain Name?.....	64
6.6 How Many Tunnels Does My VPN Connection Have?.....	64
6.7 How Do I Allow Specific Hosts to Access a VPC Subnet Through a Created VPN Connection?.....	65
6.8 Do Huawei Cloud VPNs Have the DPD Function Enabled?.....	65
6.9 How Can I Use Security Groups to Prevent VPN Access to Some ECSs in a VPC to Implement Security Isolation?.....	65
6.10 Will a VPN Connection Be Re-established After Its Configuration Is Modified?.....	66
6.11 Why Cannot I Initiate Negotiation from Amazon Web Services to Huawei Cloud After They Are Interconnected?.....	66
6.12 How Do I Configure DPD for Interconnection with Huawei Cloud?.....	66
6.13 What Should I Do If My Firewall Cannot Receive Response Packets from the Huawei Cloud VPN Gateway in IKE Phase 1?.....	67
6.14 What Should I Do If My Firewall Cannot Receive Response Packets from a Huawei Cloud VPN Subnet?.....	67
6.15 How Many Bits Do the DH Groups Used by Huawei Cloud VPN Have?.....	68
<b>7 Connection or Ping Failure.....</b>	<b>69</b>
7.1 Why Is a VPN Connection Always in Not Connected State After Its Configuration Is Complete?.....	69
7.2 How Can I Prevent VPN Disconnections?.....	69
7.3 How Do I Quickly Restore an Interrupted IPsec VPN Connection?.....	70
7.4 What Will Happen If Traffic Exceeds the Bandwidth of a VPN Gateway?.....	71

7.5 Is an IPsec VPN Connection Automatically Established?.....	71
7.6 Why Cannot ECSs at the Two Ends of a Normal Cross-Region VPN Connection Ping Each Other?.....	71
7.7 Why Cannot Subnets at the Two Ends of a Normal VPN Connection Access Each Other?.....	71
7.8 What Do I Do If a VPN Connection Is Interrupted and a Message Indicating Data Flow Mismatch Is Displayed?.....	72
7.9 What Do I Do If a VPN Connection Is Interrupted and a Message Indicating DPD Timeout Is Displayed?.....	72
7.10 Why Is a VPN Connection in Not Connected State on the Management Console When It Is Already Available?.....	72
7.11 Will I Be Notified If a VPN Connection Is Interrupted?.....	72
7.12 What Do I Do If a VPN Connection Fails to Be Established?.....	73
7.13 What Should I Do If I Cannot Access the ECSs on the Cloud from My On-premises Data Center or LAN After the VPN Connection Has Been Set Up?.....	73
7.14 Why Is the State of a Successfully Created VPN Connection Displayed as Not Connected?.....	73
7.15 Do Huawei Cloud VPNs Have the DPD Function Enabled?.....	74
<b>8 Public Addresses.....</b>	<b>75</b>
8.1 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?.....	75
8.2 Can EIPs Be Used as VPN Gateway IP Addresses?.....	75
8.3 Do I Need to Purchase EIPs for Hosts to Communicate with Each Other Through a VPN?.....	75
8.4 Why Does an ECS Have EIP Access Information After I Enable a VPN?.....	75
8.5 Can My On-premises Gateway Have a Non-fixed Public IP Address?.....	76
<b>9 Route Configurations.....</b>	<b>77</b>
9.1 What Are a Customer Gateway and a Customer Subnet in a VPN Connection?.....	77
9.2 Where Can I Add Routes to Customer Subnets on the VPN Console?.....	77
9.3 Do I Need to Add a Route for an ECS with Multiple NICs to Reach the On-premises Network?.....	77
<b>10 Subnet Configurations.....</b>	<b>78</b>
10.1 What Are the Precautions for Configuring the Local and Customer Subnets for a VPN Connection?.....	78
10.2 How Many Local and Customer Subnets Can I Add to a VPN?.....	78
10.3 What Do I Do If an Exception Occurs When I Add a Customer Subnet During VPN Connection Creation?.....	79
10.4 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?.....	79
10.5 How Do I Plan CIDR Blocks for Access to a VPC Through a VPN Connection?.....	79
10.6 How Is a VPN Gateway IP Address Allocated?.....	79
<b>11 VPN Interesting Traffic.....</b>	<b>80</b>
11.1 Do I Need to Configure ACL Rules on the Huawei Cloud Management Console After I Configure ACL Rules on the On-premises Gateway Device?.....	80
11.2 How Do I Configure and Modify the Interesting Traffic of a VPN on the Cloud?.....	80
<b>12 Keeping VPN Connections Alive.....</b>	<b>81</b>
12.1 How Can I Prevent VPN Disconnections?.....	81
<b>13 Monitoring.....</b>	<b>82</b>
13.1 What VPN Resources Can Be Monitored?.....	82

---

13.2 Will I Be Notified If a VPN Connection Is Interrupted?.....	82
13.3 Can I View the Traffic of Each VPN Connection?.....	83
13.4 Will I Be Notified of Abnormal VPN Monitoring Results?.....	83
<b>14 Bandwidth and Network Speed.....</b>	<b>84</b>
14.1 How Is the Network Speed of a VPN Connection Tested?.....	84
14.2 In Which Direction Is the VPN Bandwidth Limited? What Is the Unit of Bandwidth?.....	86
14.3 How Do I Change the VPN Bandwidth?.....	86
14.4 What Will Happen If Traffic Exceeds the Bandwidth of a VPN Gateway?.....	86
14.5 Why Does the VPN Bandwidth Change Not Take Effect?.....	86
14.6 What Are the Differences Between the Bandwidth of a VPN Connection and That of a Direct Connect Connection?.....	87
14.7 How Do I Determine My VPN Bandwidth?.....	87
<b>15 Quotas.....</b>	<b>88</b>
15.1 What Quotas Does a VPN Have?.....	88
15.2 How Many VPN Gateways and VPN Connections Can I Create By Default?.....	88
15.3 How Do I Change My VPN Gateway and Connection Quotas?.....	88
15.4 How Many IPsec VPNs Can I Have?.....	89
<b>16 Account Permissions.....</b>	<b>90</b>
16.1 Are a Username and Password Required for Creating an IPsec VPN Connection?.....	90
16.2 What Should I Do If the System Displays a Message Indicating that I Do Not Have the Permissions to Create a VPN?.....	90
16.3 How Do I Determine that My Account Cannot Create a VPN Due to Insufficient Permissions?.....	91



# 1 Popular Questions

---

## 1.1 What Devices Can Be Connected to Huawei Cloud Through a VPN?

Huawei Cloud VPN supports the standard Internet Protocol Security (IPsec) protocol. A device in your on-premises data center can connect to Huawei Cloud if the device meets the following requirements:

1. Supports IPsec VPN.
2. Has a fixed public IP address, which can be statically configured, or translated through NAT in NAT traversal scenarios (your device is deployed behind a NAT gateway).

Most devices are routers and firewalls. For details about the interconnection configuration, see .

### NOTE

- Common home broadband routers, Windows hosts providing VPN services (such as L2TP), and personal mobile terminals cannot connect to Huawei Cloud through a VPN.
- The following products can connect to Huawei Cloud through VPNs:
  - Devices: Huawei firewalls and access routers (ARs), Hillstone firewalls, and Check Point firewalls
  - Cloud services: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS), and Microsoft Azure
  - Software: strongSwan
- The IPsec protocol is a standard IETF protocol. Devices that support IPsec can interconnect with Huawei Cloud through a VPN.

Most enterprise-class routers and firewalls support the IPsec protocol.
- Some devices support IPsec VPN only after you purchase required software licenses. Your on-premises data center administrator can check with the device vendor whether a license is required based on the device model.

## 1.2 What Are VPN Negotiation Parameters? What Are Their Default Values?

Table 1-1 VPN negotiation parameters

Protocol	Parameter	Value
IKE	Authentication Algorithm	<ul style="list-style-type: none"><li>• MD5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• SHA2-256 (default value)</li><li>• SHA2-384</li><li>• SHA2-512</li></ul>
	Encryption Algorithm	<ul style="list-style-type: none"><li>• 3DES (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• AES-128 (default value)</li><li>• AES-192</li><li>• AES-256</li><li>• AES-256-GCM-16</li></ul>
	DH Algorithm	<ul style="list-style-type: none"><li>• Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 14 (default value)</li><li>• Group 16</li><li>• Group 19</li><li>• Group 20</li><li>• Group 21</li></ul>
	Version	<ul style="list-style-type: none"><li>• v1 (not recommended due to security risks)</li><li>• v2 (default value)</li></ul>

Protocol	Parameter	Value
	Lifetime (s)	<b>86400</b> (default value) Unit: second Value range: <b>60</b> to <b>604800</b>
	Local ID	<ul style="list-style-type: none"><li>IP Address The local IP address is automatically displayed as the EIP of the VPN gateway, removing the need to manually configure it.</li><li>FQDN</li></ul> By default, the local ID type is IP address and the local ID value is the EIP of the VPN gateway.
	Customer ID	<ul style="list-style-type: none"><li>IP Address</li><li>FQDN</li></ul> By default, the customer ID type is IP address and the customer ID value is the public IP address of the customer gateway.
IPsec	Authentication Algorithm	<ul style="list-style-type: none"><li>SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>MD5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>SHA2-256 (default value)</li><li>SHA2-384</li><li>SHA2-512</li></ul>
	Encryption Algorithm	<ul style="list-style-type: none"><li>AES-128 (default value)</li><li>AES-192</li><li>AES-256</li><li>3DES (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>AES-256-GCM-16</li></ul>

Protocol	Parameter	Value
	PFS	<ul style="list-style-type: none"><li>• DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 14 (default value)</li><li>• DH group 15</li><li>• DH group 16</li><li>• DH group 19</li><li>• DH group 20</li><li>• DH group 21</li><li>• Disable</li></ul>
	Transfer Protocol	<ul style="list-style-type: none"><li>• ESP (default value)</li></ul>
	Lifetime (s)	<b>3600</b> (default value) Unit: second Value range: <b>30</b> to <b>604800</b>

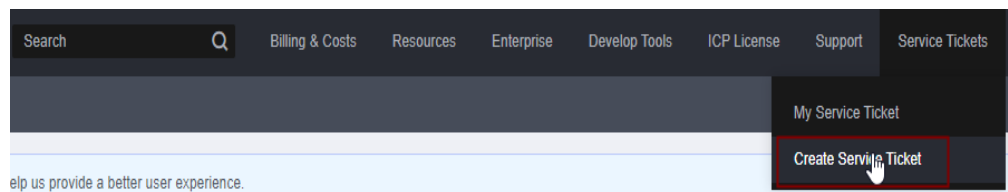
 **NOTE**

- Perfect Forward Secrecy (PFS) is a security feature.  
IKE negotiation has two phases, phase one and phase two. The key of phase two (IPsec SA) is derived from the key generated in phase one. Once the key in phase one is disclosed, the security of the IPsec VPN may be adversely affected. To improve the key security, IKE provides PFS. When PFS is enabled, an additional DH exchange will be performed during IPsec SA negotiation to generate a new IPsec SA key, improving IPsec SA security.
- For security purposes, PFS is enabled on Huawei Cloud by default. Ensure that PFS is also enabled on the gateway device in your on-premises data center and the PFS settings on both ends are the same. Otherwise, the negotiation will fail.
- The default traffic-based lifetime of an IPsec SA is 1,843,200 KB and cannot be changed for the Huawei Cloud VPN. This parameter is not involved in negotiation and has no impact on the establishment of an IPsec SA.

## 1.3 What Types of VPN Service Tickets Are There? How Do I Create a VPN Service Ticket?

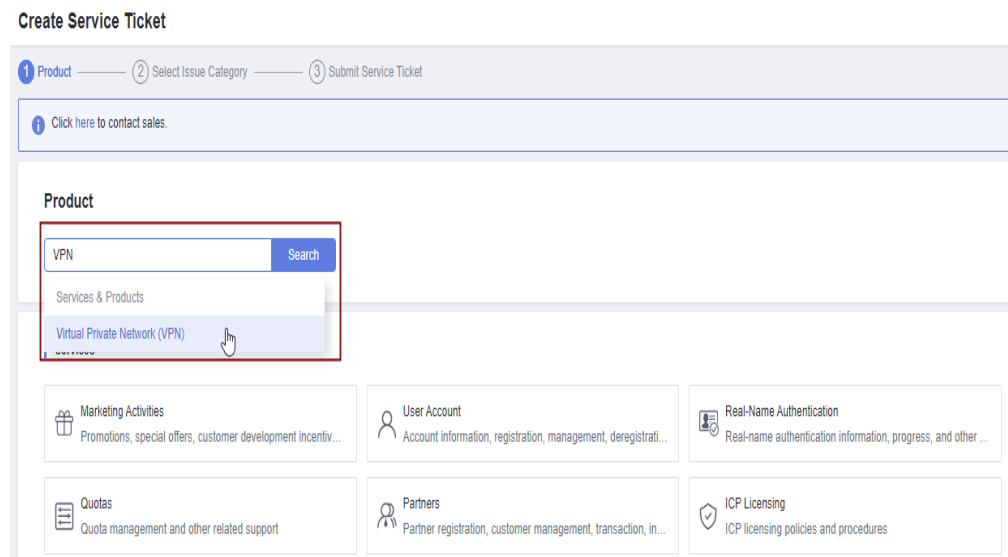
1. Log in to the management console.
2. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket**.

Figure 1-1 Create Service Ticket



3. Search for VPN and select **Virtual Private Network (VPN)**.

Figure 1-2 Selecting Virtual Private Network (VPN)



4. Select an issue category.

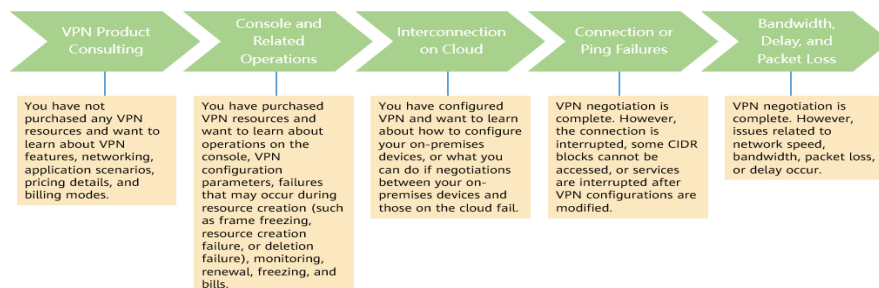
Figure 1-3 Select Issue Category



**NOTE**

When you , select an issue category to facilitate problem handling.

**Figure 1-4** Issue category and classification basis



## 1.4 Can I Deploy an Application on the Cloud and a Database in an On-premises Data Center and Connect Them Through a VPN?

Yes.

A VPN connects a VPC and an on-premises data center.

After a VPN is set up, service traffic can be transmitted between the VPC and on-premises data center. For an application server on the cloud, access to an on-premises database is logically the same as access to other hosts in the same LAN. Given this, it is feasible to use a VPN to connect an application on the cloud to a database in an on-premises data center.

This is a typical IPsec VPN scenario.

Additionally, there are no limitations on the service initiator. That is, service requests can be initiated from the cloud or the on-premises data center.

**NOTICE**

- After a VPN is set up, check the network latency and packet loss rate to ensure smooth service running.
- It is recommended that you run the ping command to check the packet loss and network latency details.

## 1.5 Can I Visit Websites Across International Borders Using a VPN?

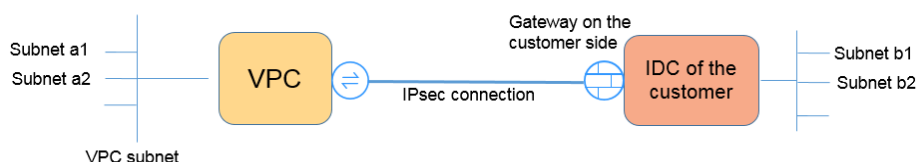
No.

VPN connects a VPC and the network of an on-premises data center, that is, site-to-site connection.

## 1.6 What Is a VPN Connection? How Do I Set the Number of VPN Connections When Buying a VPN Gateway?

A Huawei Cloud VPN connection is an IPsec connection established between a VPN gateway on the cloud and an independent public IP address of an on-premises data center. You can configure multiple local subnets (VPC subnets) and customer subnets (on-premises subnets) for one VPN connection.

The number of VPN connections to be created is determined by the number of on-premises data centers. Each VPN connection can connect a VPC to only one on-premises data center.




### NOTE

In the preceding figure, if subnets a1 and a2 on Huawei Cloud need to communicate with subnets b1 and b2 on the on-premises network, you only need to create one VPN connection, with source CIDR blocks set to a1 and a2 and destination CIDR blocks set to b1 and b2.

## 1.7 Will I Be Notified If a VPN Connection Is Interrupted?

The VPN connection status can be monitored. After a VPN connection is created, the VPN service reports the connection status information to Cloud Eye, but does not send alarm notifications to you. To receive notifications, create alarm rules and enable **Alarm Notification** on the Cloud Eye console.

To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

## 1.8 Are a Username and Password Required for Creating an IPsec VPN Connection?

No. Huawei Cloud IPsec VPN uses a pre-shared key (PSK) for authentication. The PSK is configured on a VPN gateway, and a connection will be established after VPN negotiation is complete. Therefore, no username or password is required for creating an IPsec VPN connection. Generally, SSL, PPTP, and L2TP VPNs use usernames and passwords for authentication.

**NOTE**

IPsec XAUTH provides extended authentication for IPsec VPN. It requires users to enter their usernames and passwords during VPN negotiation.

Huawei Cloud VPN does not support IPsec XAUTH.

## 1.9 What Are the Differences Between IPsec VPN and SSL VPN in Application Scenarios and Connection Modes?

### Application Scenarios

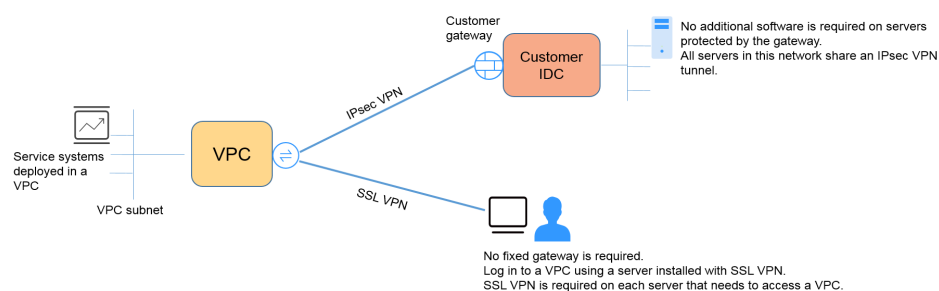
IPsec VPN connects two LANs, such as a branch and its headquarters, or an on-premises data center and a VPC.

SSL VPN connects a client to a LAN. For example, the portable computer of an employee on a business trip accesses the internal network of the company.

### Connection Modes

IPsec VPN requires fixed gateways, such as firewalls or routers, at both ends. The administrator needs to configure gateways at both ends to enable them to complete IPsec VPN negotiation.

SSL VPN requires a specific client program installed on hosts. Users need to enter usernames and password to connect the hosts to SSL servers.

**NOTE**

Huawei Cloud supports only IPsec VPN.

## 1.10 Is an IPsec VPN Connection Automatically Established?

Yes. An IPsec VPN connection is automatically established.



## 1.11 How Will I Be Charged for My Use of a VPN? Will I Be Charged for VPN Gateway EIPs?

VPNs are billed by the following items on a yearly/monthly or pay-per-use basis.

- VPN gateway
- VPN connection

By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway. You can purchase additional VPN connections if required.

- EIP bandwidth of a VPN gateway

The VPN gateway bandwidth can be billed by traffic or bandwidth.

- a. A yearly/monthly VPN gateway can only be billed by bandwidth. The price of a yearly/monthly VPN gateway includes the price of the VPN connections that can be created for the gateway and the bandwidth price.
- b. The billing cycle of the pay-per-use billing mode is 1 hour. When you create a pay-per-use VPN gateway, the system prompts you to create VPN connections. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway. If more connection groups are required, you need to purchase them.

### NOTE

A VPN gateway cannot share a bandwidth with an EIP bound to an ECS.

## 1.12 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?

If a pay-per-use EIP is bound to a pay-per-use VPN gateway, deleting the VPN gateway will also delete the bound EIP.

To retain such a pay-per-use EIP, unbind it before deleting the VPN gateway.

## 1.13 What VPN Resources Can Be Monitored?

### VPN gateway

The following bandwidth information of a VPN gateway IP address can be monitored: inbound traffic, inbound bandwidth, outbound traffic, outbound bandwidth, and outbound bandwidth usage.


To view the monitoring information, click  in the **Gateway IP Address** column in the VPN gateway list.

### VPN connection

The following information about a VPN connection can be monitored: VPN connection status, average link round-trip time (RTT), maximum link RTT, link

packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate.

To monitor average link RTT, maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate, click the VPN connection name and click **Add** in the **Health Check** area on the **Summary** tab page to add health check items.

To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

## 1.14 In Which Direction Is the VPN Bandwidth Limited? What Is the Unit of Bandwidth?

Your purchased VPN gateway bandwidth applies to the outbound direction of Huawei Cloud. To achieve a balance between bandwidths in the inbound and outbound directions, the bandwidth in the inbound direction is limited as follows:

- If the purchased bandwidth is 10 Mbit/s or less, the bandwidth in the inbound direction is limited to 10 Mbit/s.
- If the purchased bandwidth is greater than 10 Mbit/s, the bandwidth in the inbound direction is the same as the purchased bandwidth.

The unit of bandwidth is Mbit/s and that of traffic is GB.

## 1.15 How Is the Network Speed of a VPN Connection Tested?

Test environment: A VPN connection has been created. ECSs have been created on the local subnets of VPCs at the two ends of the VPN connection. The ECSs can ping each other.

**When the bandwidth of a purchased VPN gateway is 200 Mbit/s:**

1. When the ECSs at the two ends of the VPN connection run Windows, iPerf3 and FileZilla (a free FTP application for file upload and download) are used to test the network speed. The test result is 180 Mbit/s, meeting requirements.

### NOTE

The TCP-based FTP protocol has a congestion control mechanism, and the IPsec protocol adds new headers to original packets. As such, it is normal in the industry, to have a network speed deviation of about 10%.

**Figure 1-5** shows the result of testing the 200 Mbit/s bandwidth on the iPerf3 client.

**Figure 1-5** Test result for 200 Mbit/s bandwidth (iPerf3 client)

```
C:\Windows>iperf3 -c 10.1.0.180 -i 1 -w 1M
Connecting to host 10.1.0.180, port 5201
[ 4] local 192.168.0.75 port 49212 connected to 10.1.0.180 port 5201
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-1.01   sec  17.1 MBytes  142 Mbits/sec
[ 4]  1.01-2.00   sec  30.0 MBytes  253 Mbits/sec
[ 4]  2.00-3.01   sec  19.8 MBytes  165 Mbits/sec
[ 4]  3.01-4.01   sec  23.2 MBytes  194 Mbits/sec
[ 4]  4.01-5.00   sec  18.9 MBytes  161 Mbits/sec
[ 4]  5.00-6.01   sec  26.2 MBytes  219 Mbits/sec
[ 4]  6.01-7.01   sec  18.4 MBytes  153 Mbits/sec
[ 4]  7.01-8.01   sec  23.2 MBytes  195 Mbits/sec
[ 4]  8.01-9.00   sec  21.1 MBytes  180 Mbits/sec
[ 4]  9.00-10.01  sec  21.0 MBytes  174 Mbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 4]  0.00-10.01  sec  219 MBytes  183 Mbits/sec      sender
[ 4]  0.00-10.01  sec  219 MBytes  183 Mbits/sec      receiver

iperf Done.
```

**Figure 1-6** shows the result of testing the 200 Mbit/s bandwidth on the iPerf3 server.

**Figure 1-6** Test result for 200 Mbit/s bandwidth (iPerf3 server)

```
Server listening on 5201
-----
Accepted connection from 192.168.0.75, port 49211
[ 5] local 10.1.0.180 port 5201 connected to 192.168.0.75 port 49212
[ ID] Interval           Transfer     Bandwidth
[ 5]  0.00-1.00   sec  15.1 MBytes  127 Mbits/sec
[ 5]  1.00-2.01   sec  30.2 MBytes  252 Mbits/sec
[ 5]  2.01-3.00   sec  19.7 MBytes  166 Mbits/sec
[ 5]  3.00-4.01   sec  23.6 MBytes  197 Mbits/sec
[ 5]  4.01-5.01   sec  18.6 MBytes  156 Mbits/sec
[ 5]  5.01-6.00   sec  26.3 MBytes  222 Mbits/sec
[ 5]  6.00-7.01   sec  18.4 MBytes  153 Mbits/sec
[ 5]  7.01-8.01   sec  23.4 MBytes  196 Mbits/sec
[ 5]  8.01-9.01   sec  21.5 MBytes  180 Mbits/sec
[ 5]  9.01-10.00  sec  20.4 MBytes  173 Mbits/sec
[ 5] 10.00-10.07  sec   1.32 MBytes  162 Mbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 5]  0.00-10.07  sec   0.00 Bytes    0.00 bits/sec      sender
[ 5]  0.00-10.07  sec  219 MBytes  182 Mbits/sec      receiver
-----
```

2. When the ECSs at the two ends of the VPN connection run CentOS 7, iPerf3 is used to test the network speed. The test result is 180 Mbit/s, meeting requirements.
3. When the ECS functioning as a server runs CentOS 7 and the ECS functioning as a client runs Windows, iPerf3 and FileZilla are used to test the network speed. The test result is 20 Mbit/s, failing to meet requirements.

This is because TCP implementations on Windows and Linux are different.

**Figure 1-7** shows the result of using iPerf3 to test the network speed between two ECSs running different operating systems.

Figure 1-7 Test result on iPerf3

```
C:\Windows>iperf3 -c 10.1.0.182 -i 1 -w 1M
Connecting to host 10.1.0.182, port 5201
[ 41] local 192.168.0.75 port 49426 connected to 10.1.0.182 port 5201
[ ID] Interval           Transfer     Bandwidth
[ 41] 0.00-1.00 sec      4.38 MBytes  36.7 Mbits/sec
[ 41] 1.00-2.00 sec      4.50 MBytes  37.7 Mbits/sec
[ 41] 2.00-3.00 sec      5.12 MBytes  43.0 Mbits/sec
[ 41] 3.00-4.00 sec      1.75 MBytes  14.7 Mbits/sec
[ 41] 4.00-5.00 sec      2.12 MBytes  17.8 Mbits/sec
[ 41] 5.00-6.00 sec      3.25 MBytes  27.3 Mbits/sec
[ 41] 6.00-7.00 sec      2.12 MBytes  17.8 Mbits/sec
[ 41] 7.00-8.00 sec      1.25 MBytes  10.5 Mbits/sec
[ 41] 8.00-9.00 sec      2.25 MBytes  18.9 Mbits/sec
[ 41] 9.00-10.00 sec     2.38 MBytes  19.9 Mbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 41] 0.00-10.00 sec    29.1 MBytes  24.4 Mbits/sec  sender
[ 41] 0.00-10.00 sec    28.2 MBytes  23.6 Mbits/sec  receiver

iperf Done.
```

When the bandwidth of a purchased VPN gateway is 1000 Mbit/s:

 NOTE

Some regions support only 300 Mbit/s bandwidth by default. If higher bandwidth is required, apply for 300 Mbit/s bandwidth and then for capacity expansion.

The VPN gateway bandwidth is shared by all of its VPN connections. To fully use the large bandwidth of 1000 Mbit/s, deploy multiple ECSs with high specifications as the forwarding performance of a single ECS is limited. ECSs with their NICs supporting the bandwidth of 2 Gbit/s or higher are recommended.

**Conclusions:** Based on the preceding test results, bandwidths of Huawei Cloud VPN gateways meet requirements. To fully use your purchased bandwidth, you are advised to use servers running the same operating system and using NICs meeting certain requirements at the two ends of a VPN connection.

## 1.16 Can a VPN Billed by Traffic Use a Shared Data Package?

No.

The VPN service is billed independently and cannot use shared data packages.


## 1.17 How Do I Change the Billing Mode of a VPN Gateway from Pay-Per-Use to Yearly/Monthly?

### Prerequisites

- The pay-per-use VPN gateway is billed by bandwidth.
- To change the billing mode of a VPN gateway billed by traffic from pay-per-use to yearly/monthly, first change the VPN gateway from being billed by traffic to being billed by bandwidth and then from pay-per-use to yearly/monthly.

## Procedure

Perform the following operations:

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking > Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
5. On the **VPN Gateways** page, locate the row that contains the target VPN gateway, choose **More > Change Billing Mode** in the **Operation** column.
6. In the **Change Billing Mode** dialog box, click **OK**.

### NOTE

The billing mode of a VPN gateway cannot be changed from yearly/monthly to pay-per-use and the VPN gateway bandwidth included in the yearly/monthly subscription cannot be decreased.

7. Confirm the VPN gateway information, set a renewal duration, and click **Pay**.
8. On the payment page, confirm the order information, select a coupon or discount, select a payment method, and click **Pay**.

### NOTE

Changing the billing mode of a VPN gateway from pay-per-use to yearly/monthly will not affect your services.

## 1.18 What Are the Relationships Between a VPC, a VPN Gateway, and a VPN Connection?

- A VPC is a private network on the cloud. Multiple VPCs can be created in the same region while they are isolated from each other. A VPC can be divided into multiple subnets.
- A VPN gateway is created in a VPC and is the access point of a VPN connection. One Huawei Cloud VPC can have multiple VPN gateways, and one VPN gateway can have multiple VPN connections.
- A VPN connection is created for a VPN gateway and connects a VPC to an on-premises data center (or a VPC in another region).

### NOTE

The number of VPN connections is irrelevant to the number of local subnets or the number of customer subnets. It is only related to the number of on-premises data centers (or VPCs in other regions) to be connected to your VPC. The created VPN connections are displayed in the VPN connection list. You can also view the number of VPN connections created for each VPN gateway.

## 1.19 What Are a Customer Gateway and a Customer Subnet in a VPN Connection?

A VPN connection is created on Huawei Cloud. As such, a subnet of a Huawei Cloud VPC is a local subnet, and a VPN gateway created on Huawei Cloud is a

local gateway. The subnet and gateway in an on-premises data center connected to the VPC are a customer subnet and a customer gateway, respectively.

A customer gateway's IP address is a public IP address.

## 1.20 How Many VPN Connections Do I Need to Connect Multiple On-premises Servers to the Cloud?

Huawei Cloud VPN uses IPsec VPN technology. It connects a VPC on the cloud and your on-premises data center. Therefore, the number of VPN connections is irrelevant to the number of servers to be connected to the cloud, but to the number of data centers where the servers are located.

Two EIPs can be bound to a VPN gateway for communication with a customer gateway.

- If an on-premises data center has only one egress gateway, all servers or hosts in the data center connect to the Internet through this gateway. In this case, you need to configure a VPN connection group consisting of two VPN connections. That is, configure a VPN connection for each of the two EIPs of the VPN gateway to communicate with the egress gateway in the on-premises data center.
- If an on-premises data center has two egress gateways, the servers or user hosts in the data center connect to the Internet through the two egress gateways. In this case, you need to configure two VPN connection groups, each of which consisting of two VPN connections. That is, configure a VPN connection for each of the two EIPs of each VPN gateway to communicate with both egress gateways in the on-premises data center.

## 1.21 Does a VPN Allow for Communications Between Two VPCs?

- If the two VPCs are in the same region, use a VPC peering connection to connect them.
- If the two VPCs are in different regions, use a VPN to connect them. The operations are as follows:
  - a. Create a VPN gateway for each VPC, and create a VPN connection between the two VPN gateways.
  - b. For the VPN connection, set the customer gateway to the EIP of the peer VPN gateway.
  - c. For the VPN connection, set the customer subnet to the subnet of the peer VPC.
  - d. Set the same pre-shared keys (PSKs) and algorithms for the two VPCs.

## 1.22 What Are the Impacts of a VPN on an On-premises Network? What Are the Changes to the Route for Accessing an ECS?

When configuring a VPN, you need to perform the following operations on the gateway in your on-premises data center:

- Configure IKE and IPsec policies.
- Set the connection mode to route-based or policy-based.
- Check the route configuration on the gateway to ensure that traffic destined for a Huawei Cloud VPC can be routed to the correct outbound interface (interface having an IPsec policy bound).

## 1.23 Can I Connect a Network with Two Egresses to a VPC Through Two VPN Connections?

Yes.

## 1.24 How Can I Prevent VPN Disconnections?

VPN connections are renegotiated when the IPsec SA lifetime is about to expire or the data transmitted through a VPN connection exceeds 20 GB. Usually, renegotiation does not interrupt VPN connections.

Most disconnections are caused by incorrect configurations at the two ends of the VPN connection or renegotiation failures due to Internet exceptions.

Common causes of disconnections are as follows:

- ACLs at both ends of the VPN connection do not match.
- SA lifetime settings at both ends of the VPN connection are different.
- Dead Peer Detection (DPD) is not configured on the device in your on-premises data center.
- Configuration is modified when the VPN connection is in use.
- Jitter occurs on the carrier's network.

As such, ensure that the following VPN configurations are correct to keep VPN connections alive:

- At the two ends of the VPN connection, the local and remote subnet configurations are reversed.
- SA lifetime settings at both ends of the VPN connection are the same.
- DPD is enabled on the on-premises gateway device, and the number of detection times is 3 or more.
- Parameters are modified at both ends of the VPN connection during the use of the VPN connection.

- Set TCP MAX-MSS to 1300 for the on-premises gateway device.
- The bandwidth of the on-premises gateway device is large enough for the VPN connection.
- VPN connection negotiation can be triggered by both ends and active negotiation has been enabled on the on-premises gateway device.

## 1.25 What Do I Do If a VPN Connection Fails to Be Established?

1. Log in to the management console and choose **Virtual Private Network > Enterprise - VPN Connections**.
2. In the VPN connection list, locate the target VPN connection, and choose **More > Modify Policy Settings** on the right to view IKE and IPsec policies of the VPN connection.
3. Check the IKE and IPsec policies to see whether the negotiation modes and encryption algorithms at both ends of the VPN connection are the same.  
If the IKE SA has been set up in phase 1 but no IPsec SA has been established in phase 2, the IPsec policies at both ends of the VPN connection may be inconsistent.
4. Check whether the ACL rules are correct.  
If the subnets of your on-premises data center are 192.168.3.0/24 and 192.168.4.0/24, and the VPC subnets are 192.168.1.0/24 and 192.168.2.0/24, configure the ACL rules for each on-premises subnet to allow the communication with the VPC subnets. The following provides an example of ACL configurations:

```
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
```
5. Ping the two ends of the VPN connection from each other to check whether the VPN connection is normal.

## 1.26 Can EIPs Be Used as VPN Gateway IP Addresses?

No.

When you create a VPN gateway, its IP address is automatically assigned. This IP address has preset configurations and can be used for interconnection with a VPC. However, an EIP cannot be used for interconnection with a VPC.

## 1.27 Why Is a VPN Connection Always in Not Connected State After Its Configuration Is Complete?

The configuration may be incorrect.

1. At the two ends (cloud and on-premises data center) of the VPN connection, ensure that the pre-shared keys (PSKs) and negotiation information are



consistent, the local and remote subnets are reversed, and the local and remote gateways are also reversed.

2. Ensure that routes, NAT, and security policies are correctly configured on the device in your on-premises data center.

## 1.28 Do I Need to Configure ACL Rules on the Huawei Cloud Management Console After I Configure ACL Rules on the On-premises Gateway Device?

You need to configure policy rules (ACL rules) for a VPN connection on the Huawei Cloud management console only when **VPN Type** is set to **Policy-based**.

# 2 General Consulting

---

## 2.1 What Are the Typical Scenarios of IPsec VPN?

A VPN is a point-to-point connection that implements private network access between two points.

- Applicable scenarios:
  - A VPN is created between different regions of Huawei Cloud to enable cross-region VPC communications.
  - A VPN is created between VPCs of Huawei Cloud and another public cloud, for example, Alibaba Cloud.
  - A VPN is created between a VPC of Huawei Cloud and your on-premises data center.
  - A VPN hub is used together with VPC peering connections and Cloud Connect connections to enable communications between an on-premises data center and multiple VPCs on the cloud.
  - A VPN is used together with source NAT to enable access to specific IP addresses across clouds.
- Not applicable scenarios:
  - A VPN cannot be used to connect VPCs in the same region of Huawei Cloud. It is recommended that you use VPC peering connections to enable communications between VPCs in the same region.
  - A VPN cannot be used between Huawei Cloud and your home network that uses PPPoE dial-up.
  - A VPN cannot be used between Huawei Cloud and 4G/5G routers.
  - A VPN cannot be used between Huawei Cloud and your personal terminals.

## 2.2 What Are a VPC, a VPN Gateway, and a VPN Connection?

VPC enables you to create private, isolated virtual networks. You can use VPN to securely access ECSs in VPCs.

A VPN gateway is an egress gateway for a VPC. With a VPN gateway, you can create a secure, reliable, and encrypted connection between a VPC and an on-premises data center or between two VPCs in different regions.

A VPN connection is a secure and reliable IPsec encrypted communications tunnel established between a VPN gateway and the customer gateway in an on-premises data center.

To create a VPN on the cloud, perform the following operations:

1. Create a VPN gateway. You need to specify the VPC to be connected, as well as the bandwidth and EIPs of the VPN gateway.
2. Create a VPN connection. You need to specify the gateway EIP used to connect to the customer gateway, subnets, and negotiation policies.

## 2.3 What Are the Relationships Between a VPC, a VPN Gateway, and a VPN Connection?

- A VPC is a private network on the cloud. Multiple VPCs can be created in the same region while they are isolated from each other. A VPC can be divided into multiple subnets.
- A VPN gateway is created in a VPC and is the access point of a VPN connection. One Huawei Cloud VPC can have multiple VPN gateways, and one VPN gateway can have multiple VPN connections.
- A VPN connection is created for a VPN gateway and connects a VPC to an on-premises data center (or a VPC in another region).

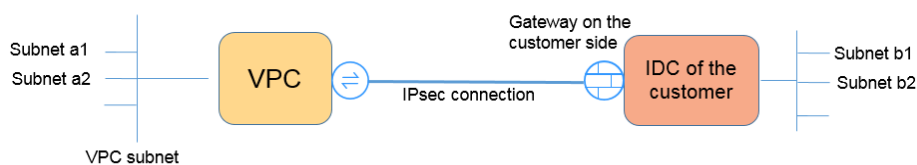
### NOTE

The number of VPN connections is irrelevant to the number of local subnets or the number of customer subnets. It is only related to the number of on-premises data centers (or VPCs in other regions) to be connected to your VPC. The created VPN connections are displayed in the VPN connection list. You can also view the number of VPN connections created for each VPN gateway.

## 2.4 What Is a VPN Connection? How Do I Set the Number of VPN Connections When Buying a VPN Gateway?

A Huawei Cloud VPN connection is an IPsec connection established between a VPN gateway on the cloud and an independent public IP address of an on-premises data center. You can configure multiple local subnets (VPC subnets) and customer subnets (on-premises subnets) for one VPN connection.

The number of VPN connections to be created is determined by the number of on-premises data centers. Each VPN connection can connect a VPC to only one on-premises data center.

**NOTE**

In the preceding figure, if subnets a1 and a2 on Huawei Cloud need to communicate with subnets b1 and b2 on the on-premises network, you only need to create one VPN connection, with source CIDR blocks set to a1 and a2 and destination CIDR blocks set to b1 and b2.

## 2.5 What Are a Customer Gateway and a Customer Subnet in a VPN Connection?

A VPN connection is created on Huawei Cloud. As such, a subnet of a Huawei Cloud VPC is a local subnet, and a VPN gateway created on Huawei Cloud is a local gateway. The subnet and gateway in an on-premises data center connected to the VPC are a customer subnet and a customer gateway, respectively.

A customer gateway's IP address is a public IP address.

## 2.6 How Do I Plan CIDR Blocks for Access to a VPC Through a VPN Connection?

- The CIDR blocks of a VPC cannot conflict with on-premises CIDR blocks.
- To avoid conflicts with cloud service addresses, do not use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3, or 100.64.0.0/10 for your on-premises network.

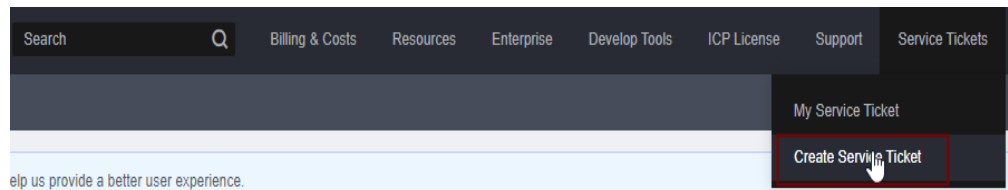
## 2.7 Is an IPsec VPN Connection Automatically Established?

Yes. An IPsec VPN connection is automatically established.

## 2.8 What Types of VPN Service Tickets Are There? How Do I Create a VPN Service Ticket?

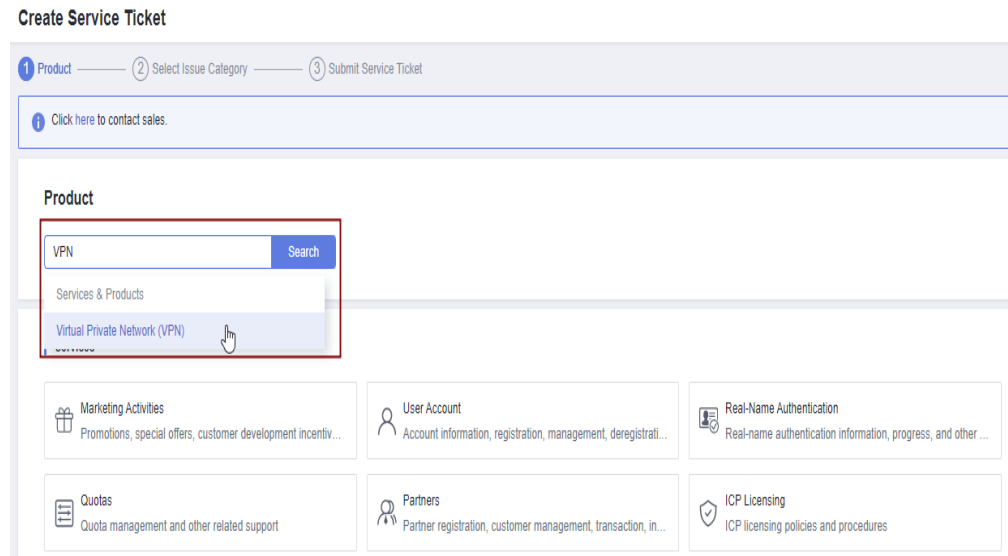
1. Log in to the management console.
2. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket**.

Figure 2-1 Create Service Ticket



- 3. Search for VPN and select Virtual Private Network (VPN).

Figure 2-2 Selecting Virtual Private Network (VPN)



- 4. Select an issue category.

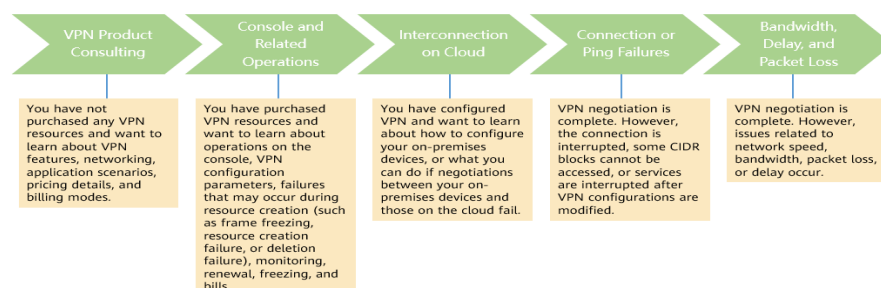
Figure 2-3 Select Issue Category



**NOTE**

When you , select an issue category to facilitate problem handling.

**Figure 2-4** Issue category and classification basis



## 2.9 What Devices Can Be Connected to Huawei Cloud Through a VPN?

Huawei Cloud VPN supports the standard Internet Protocol Security (IPsec) protocol. A device in your on-premises data center can connect to Huawei Cloud if the device meets the following requirements:

1. Supports IPsec VPN.
2. Has a fixed public IP address, which can be statically configured, or translated through NAT in NAT traversal scenarios (your device is deployed behind a NAT gateway).

Most devices are routers and firewalls. For details about the interconnection configuration, see .

**NOTE**

- Common home broadband routers, Windows hosts providing VPN services (such as L2TP), and personal mobile terminals cannot connect to Huawei Cloud through a VPN.
- The following products can connect to Huawei Cloud through VPNs:
  - Devices: Huawei firewalls and access routers (ARs), Hillstone firewalls, and Check Point firewalls
  - Cloud services: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS), and Microsoft Azure
  - Software: strongSwan
- The IPsec protocol is a standard IETF protocol. Devices that support IPsec can interconnect with Huawei Cloud through a VPN.

Most enterprise-class routers and firewalls support the IPsec protocol.

- Some devices support IPsec VPN only after you purchase required software licenses. Your on-premises data center administrator can check with the device vendor whether a license is required based on the device model.

## 2.10 What Are VPN Negotiation Parameters? What Are Their Default Values?

Table 2-1 VPN negotiation parameters

Protocol	Parameter	Value
IKE	Authentication Algorithm	<ul style="list-style-type: none"><li>• MD5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• SHA2-256 (default value)</li><li>• SHA2-384</li><li>• SHA2-512</li></ul>
	Encryption Algorithm	<ul style="list-style-type: none"><li>• 3DES (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• AES-128 (default value)</li><li>• AES-192</li><li>• AES-256</li><li>• AES-256-GCM-16</li></ul>
	DH Algorithm	<ul style="list-style-type: none"><li>• Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 14 (default value)</li><li>• Group 16</li><li>• Group 19</li><li>• Group 20</li><li>• Group 21</li></ul>
	Version	<ul style="list-style-type: none"><li>• v1 (not recommended due to security risks)</li><li>• v2 (default value)</li></ul>

Protocol	Parameter	Value
	Lifetime (s)	<b>86400</b> (default value) Unit: second Value range: <b>60</b> to <b>604800</b>
	Local ID	<ul style="list-style-type: none"><li>IP Address The local IP address is automatically displayed as the EIP of the VPN gateway, removing the need to manually configure it.</li><li>FQDN</li></ul> By default, the local ID type is IP address and the local ID value is the EIP of the VPN gateway.
	Customer ID	<ul style="list-style-type: none"><li>IP Address</li><li>FQDN</li></ul> By default, the customer ID type is IP address and the customer ID value is the public IP address of the customer gateway.
IPsec	Authentication Algorithm	<ul style="list-style-type: none"><li>SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>MD5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>SHA2-256 (default value)</li><li>SHA2-384</li><li>SHA2-512</li></ul>
	Encryption Algorithm	<ul style="list-style-type: none"><li>AES-128 (default value)</li><li>AES-192</li><li>AES-256</li><li>3DES (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>AES-256-GCM-16</li></ul>



Protocol	Parameter	Value
	PFS	<ul style="list-style-type: none"><li>• DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 14 (default value)</li><li>• DH group 15</li><li>• DH group 16</li><li>• DH group 19</li><li>• DH group 20</li><li>• DH group 21</li><li>• Disable</li></ul>
	Transfer Protocol	<ul style="list-style-type: none"><li>• ESP (default value)</li></ul>
	Lifetime (s)	<b>3600</b> (default value) Unit: second Value range: <b>30</b> to <b>604800</b>

 **NOTE**

- Perfect Forward Secrecy (PFS) is a security feature.  
IKE negotiation has two phases, phase one and phase two. The key of phase two (IPsec SA) is derived from the key generated in phase one. Once the key in phase one is disclosed, the security of the IPsec VPN may be adversely affected. To improve the key security, IKE provides PFS. When PFS is enabled, an additional DH exchange will be performed during IPsec SA negotiation to generate a new IPsec SA key, improving IPsec SA security.
- For security purposes, PFS is enabled on Huawei Cloud by default. Ensure that PFS is also enabled on the gateway device in your on-premises data center and the PFS settings on both ends are the same. Otherwise, the negotiation will fail.
- The default traffic-based lifetime of an IPsec SA is 1,843,200 KB and cannot be changed for the Huawei Cloud VPN. This parameter is not involved in negotiation and has no impact on the establishment of an IPsec SA.

## 2.11 Are a Username and Password Required for Creating an IPsec VPN Connection?

No. Huawei Cloud IPsec VPN uses a pre-shared key (PSK) for authentication. The PSK is configured on a VPN gateway, and a connection will be established after VPN negotiation is complete. Therefore, no username or password is required for

creating an IPsec VPN connection. Generally, SSL, PPTP, and L2TP VPNs use usernames and passwords for authentication.

 **NOTE**

IPsec XAUTH provides extended authentication for IPsec VPN. It requires users to enter their usernames and passwords during VPN negotiation.

Huawei Cloud VPN does not support IPsec XAUTH.

## 2.12 How Do I Allow Specific Hosts to Access a VPC Subnet Through a Created VPN Connection?

Restrictions in the on-premises data center:

- Access control policies on the VPN device
- ACL rules on the router or switch

Restrictions at the cloud side:

- Security group rules that permit access only from specified IP addresses
- ACL rules

 **NOTE**

You are advised not to change the local or customer subnet to control access.

## 2.13 What VPN Resources Can Be Monitored?

### VPN gateway


The following bandwidth information of a VPN gateway IP address can be monitored: inbound traffic, inbound bandwidth, outbound traffic, outbound bandwidth, and outbound bandwidth usage.

To view the monitoring information, click  in the **Gateway IP Address** column in the VPN gateway list.

### VPN connection

The following information about a VPN connection can be monitored: VPN connection status, average link round-trip time (RTT), maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate.

To monitor average link RTT, maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate, click the VPN connection name and click **Add** in the **Health Check** area on the **Summary** tab page to add health check items.

To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

## 2.14 Can EIPs Be Used as VPN Gateway IP Addresses?

No.

When you create a VPN gateway, its IP address is automatically assigned. This IP address has preset configurations and can be used for interconnection with a VPC. However, an EIP cannot be used for interconnection with a VPC.

## 2.15 Do I Need to Purchase EIPs for Hosts to Communicate with Each Other Through a VPN?

If your on-premises hosts need to access an ECS on the cloud through a VPN, you do not need to purchase any EIPs for the ECS.

If an ECS needs to provide services accessible from the Internet, you need to purchase an EIP for the ECS.

## 2.16 Are SSL VPNs Supported?

SSL VPNs are not supported.

## 2.17 How Long Does It Take for Delivered VPN Configurations to Take Effect?

It takes 1–5 minutes for the VPN configurations to take effect.

### NOTE

After VPN configurations take effect, configure your gateway device on your on-premises network to complete tunnel negotiation with the VPN gateway on Huawei Cloud.

## 2.18 Does Huawei Cloud VPN Support IPv6 Addresses?

No.

Huawei Cloud VPN supports only IPv4 addresses.

## 2.19 How Do I Determine My VPN Bandwidth?

Consider the following when you determine the bandwidth:

- Amount of data transmitted over a VPN tunnel in a period of time (Reserve enough bandwidth to prevent link congestion.)
- Egress bandwidths at the two ends of a VPN connection: The egress bandwidth at the cloud side must be less than that at the on-premises side.

## 2.20 Does a VPN Connection Support SM Series Cryptographic Algorithms?

No.

Use the algorithms provided on the Huawei Cloud management console for VPN negotiation. Additionally, ensure that the two ends of a VPN connection use the same algorithms.

## 2.21 Which IKE Version Should I Select When I Create a VPN Connection?

Huawei Cloud recommends IKEv2 because IKEv1 is not secure. In addition, IKEv2 outperforms IKEv1 in connection negotiation and establishment, authentication methods, dead peer detection (DPD) timeout processing, and security association (SA) timeout processing.

Huawei Cloud will not support IKEv1 soon.

### Introduction to IKEv1 and IKEv2

- As a hybrid protocol, IKEv1 brings some security and performance defects due to its complexity. As such, it has become a bottleneck in the IPsec system.
- IKEv2 addresses the issues of IKEv1 while retaining basic functions of IKEv1. IKEv2 is more simplified, efficient, secure, and robust than IKEv1. Additionally, IKEv2 is defined by RFC 4306 in a single document, whereas IKEv1 are defined in multiple documents. By minimizing core functions and default password algorithms, IKEv2 greatly improves interoperability between different IPsec VPNs.

### Security Risks of IKEv1

- The cryptographic algorithms supported by IKEv1 have not been updated for more than 10 years. In addition, IKEv1 does not support strong cryptographic algorithms such as AES-GCM and ChaCha20-Poly1305. For IKEv1, the E (Encryption) bit in the ISALMP header specifies that the payloads following the ISALMP header are encrypted, but any data integrity verification of those payloads is handled by a separate hash payload. This separation of encryption from data integrity protection prevents the use of authenticated encryption (AES-GCM) with IKEv1.
- IKEv1 is vulnerable to DoS amplification attacks and half-open connection attacks. After responding to spoofed packets, the responder maintains initiator-responder relationships, consuming a large number of system resources.  
This defect is inherent to IKEv1 and is addressed in IKEv2.
- The aggressive mode of IKEv1 is not secure. In this mode, information packets are not encrypted, posing risks of information leakage. There are also brute-force attacks targeting at the aggressive mode, such as man-in-the-middle attacks.

## Differences Between IKEv1 and IKEv2

- **Negotiation process**

- IKEv1 is complex and consumes a large amount of bandwidth. IKEv1 SA negotiation consists of two phases. In IKEv1 phase 1, an IKE SA is established in either main mode or aggressive mode. Main mode requires three exchanges between peers totaling six ISAKMP messages, whereas aggressive mode requires two exchanges totaling three ISAKMP messages. Aggressive mode is faster, but does not provide identity protection for peers as key exchange and identity authentication are performed simultaneously. In IKEv1 phase 2, IPsec SAs are established through three ISAKMP messages in quick mode.
- Compared with IKEv1, IKEv2 simplifies the SA negotiation process. IKEv2 requires only two exchanges, totaling four messages, to establish an IKE SA and a pair of IPsec SAs. To create multiple pairs of IPsec SAs, only one additional exchange is needed for each additional pair of SAs.

 **NOTE**

For IKEv1 negotiation, its main mode involves nine (6+3) messages, and its aggressive mode involves six (3+3) messages. In contrast, IKEv2 negotiation requires only four (2+2) messages.

- **Authentication methods**

- Only IKEv1 (requiring an encryption card) supports digital envelope authentication (HSS-DE).
- IKEv2 supports Extensible Authentication Protocol (EAP) authentication. IKEv2 can use an AAA server to remotely authenticate mobile and PC users and assign private IP addresses to these users. IKEv1 does not provide this function and must use L2TP to assign private IP addresses.
- Only IKEv2 supports IKE SA integrity algorithms.

- **DPD timeout processing**

- Only IKEv1 supports the **retry-interval** parameter. If a device sends a DPD packet but receives no reply within the specified retry-interval, the device records a DPD failure event. When the number of DPD failure events reaches 5, both the IKE SA and IPsec SAs are deleted. IKE SA negotiation will start again only when there is traffic to be transmitted over the IPsec tunnel.
- In IKEv2, the retransmission interval increases from 1, 2, 4, 8, 16, 32 to 64, in seconds. If no reply is received within eight consecutive transmissions, the peer end is considered dead, and the IKE SA and IPsec SAs are deleted.

- **IKE SA timeout processing and IPsec SA timeout processing**

In IKEv2, the IKE SA soft lifetime is 9/10 of the IKE SA hard lifetime plus or minus a random number. This reduces the likelihood that two ends initiate renegotiation simultaneously. Therefore, you do not manually set the soft lifetime in IKEv2.

## Advantages of IKEv2 over IKEv1

- Simplifies the SA negotiation process, improving efficiency.
- Fixes many cryptographic security vulnerabilities, improving security.

- Supports EAP authentication, improving authentication flexibility and scalability.

EAP is an authentication protocol that supports multiple authentication methods. The biggest advantage of EAP is its scalability. That is, new authentication methods can be added without changing the original authentication system. EAP authentication has been widely used in dial-up access networks.

- Employs an Encrypted Payload on basis of ESP. This payload contains both an encryption algorithm and a data integrity algorithm. AES-GCM ensures confidentiality, integrity, and authentication, and works well with IKEv2.

## 2.22 How Many Bits Do the DH Groups Used by Huawei Cloud VPN Have?

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Higher DH group numbers are usually more secure, but more time is required to calculate the key.

**Table 2-2** lists the number of bits corresponding to the DH groups used by VPN.

**Table 2-2** Number of bits corresponding to each DH group

DH Group	Modulus
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	256 bits (ECP)
20	384 bits (ECP)
21	521 bits (ECP)

### NOTE

The following DH algorithms have security risks and are not recommended: DH group 1, DH group 2, and DH group 5.

## 2.23 Can I Visit Websites Across International Borders Using a VPN?

No.

VPN connects a VPC and the network of an on-premises data center, that is, site-to-site connection.

## 2.24 Can I Deploy an Application on the Cloud and a Database in an On-premises Data Center and Connect Them Through a VPN?

Yes.

A VPN connects a VPC and an on-premises data center.

After a VPN is set up, service traffic can be transmitted between the VPC and on-premises data center. For an application server on the cloud, access to an on-premises database is logically the same as access to other hosts in the same LAN. Given this, it is feasible to use a VPN to connect an application on the cloud to a database in an on-premises data center.

This is a typical IPsec VPN scenario.

Additionally, there are no limitations on the service initiator. That is, service requests can be initiated from the cloud or the on-premises data center.

---

### NOTICE

- After a VPN is set up, check the network latency and packet loss rate to ensure smooth service running.
  - It is recommended that you run the ping command to check the packet loss and network latency details.
- 

## 2.25 What Are the Differences Between IPsec VPN and SSL VPN in Application Scenarios and Connection Modes?

### Application Scenarios

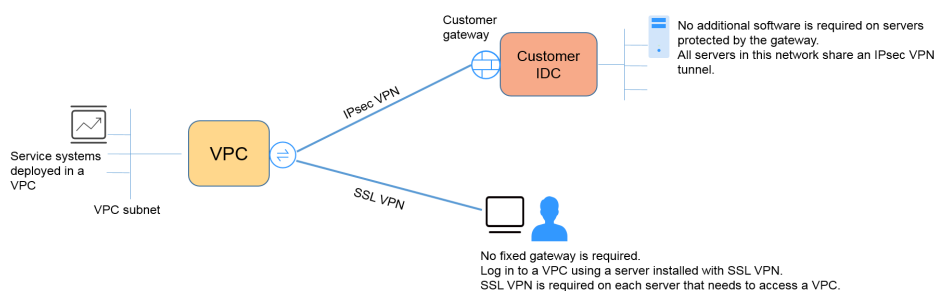
IPsec VPN connects two LANs, such as a branch and its headquarters, or an on-premises data center and a VPC.

SSL VPN connects a client to a LAN. For example, the portable computer of an employee on a business trip accesses the internal network of the company.

### Connection Modes

IPsec VPN requires fixed gateways, such as firewalls or routers, at both ends. The administrator needs to configure gateways at both ends to enable them to complete IPsec VPN negotiation.

SSL VPN requires a specific client program installed on hosts. Users need to enter usernames and password to connect the hosts to SSL servers.

**NOTE**

Huawei Cloud supports only IPsec VPN.

## 2.26 How Will I Be Charged for My Use of a VPN? Will I Be Charged for VPN Gateway EIPs?

VPNs are billed by the following items on a yearly/monthly or pay-per-use basis.

- VPN gateway
- VPN connection

By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway. You can purchase additional VPN connections if required.

- EIP bandwidth of a VPN gateway

The VPN gateway bandwidth can be billed by traffic or bandwidth.

- a. A yearly/monthly VPN gateway can only be billed by bandwidth. The price of a yearly/monthly VPN gateway includes the price of the VPN connections that can be created for the gateway and the bandwidth price.
- b. The billing cycle of the pay-per-use billing mode is 1 hour. When you create a pay-per-use VPN gateway, the system prompts you to create VPN connections. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway. If more connection groups are required, you need to purchase them.

**NOTE**

A VPN gateway cannot share a bandwidth with an EIP bound to an ECS.

## 2.27 What Are the Differences Between Billing the VPN Gateway EIP Bandwidth by Bandwidth and by Traffic?

The VPN gateway EIP bandwidth can be billed by bandwidth or by traffic.

The differences are as follows:

- Billed by bandwidth: The billing cycle is 1 hour. The generated fee depends on the bandwidth.



- Billed by traffic: The fee is calculated based on the outgoing traffic of a VPC generated every hour, which is not affected by the bandwidth.

## 2.28 Can a VPN Billed by Traffic Use a Shared Data Package?

No.

The VPN service is billed independently and cannot use shared data packages.

## 2.29 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?

If a pay-per-use EIP is bound to a pay-per-use VPN gateway, deleting the VPN gateway will also delete the bound EIP.


To retain such a pay-per-use EIP, unbind it before deleting the VPN gateway.

## 2.30 Where Can I Add Routes to Customer Subnets on the VPN Console?

When a VPN connection is created, routes to customer subnets are automatically delivered.

## 2.31 Will I Be Notified If a VPN Connection Is Interrupted?

The VPN connection status can be monitored. After a VPN connection is created, the VPN service reports the connection status information to Cloud Eye, but does not send alarm notifications to you. To receive notifications, create alarm rules and enable **Alarm Notification** on the Cloud Eye console.

To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

## 2.32 What Do I Do If a VPN Connection Fails to Be Established?

1. Log in to the management console and choose **Virtual Private Network > Enterprise – VPN Connections**.
2. In the VPN connection list, locate the target VPN connection, and choose **More > Modify Policy Settings** on the right to view IKE and IPsec policies of the VPN connection.
3. Check the IKE and IPsec policies to see whether the negotiation modes and encryption algorithms at both ends of the VPN connection are the same.

If the IKE SA has been set up in phase 1 but no IPsec SA has been established in phase 2, the IPsec policies at both ends of the VPN connection may be inconsistent.

4. Check whether the ACL rules are correct.

If the subnets of your on-premises data center are 192.168.3.0/24 and 192.168.4.0/24, and the VPC subnets are 192.168.1.0/24 and 192.168.2.0/24, configure the ACL rules for each on-premises subnet to allow the communication with the VPC subnets. The following provides an example of ACL configurations:

```
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
```

5. Ping the two ends of the VPN connection from each other to check whether the VPN connection is normal.

## 2.33 In Which Direction Is the VPN Bandwidth Limited? What Is the Unit of Bandwidth?

Your purchased VPN gateway bandwidth applies to the outbound direction of Huawei Cloud. To achieve a balance between bandwidths in the inbound and outbound directions, the bandwidth in the inbound direction is limited as follows:

- If the purchased bandwidth is 10 Mbit/s or less, the bandwidth in the inbound direction is limited to 10 Mbit/s.
- If the purchased bandwidth is greater than 10 Mbit/s, the bandwidth in the inbound direction is the same as the purchased bandwidth.

The unit of bandwidth is Mbit/s and that of traffic is GB.

## 2.34 Can I Restore a VPN Gateway or VPN Connection That Is Incorrectly Deleted?

- A yearly/monthly VPN gateway or VPN connection cannot be restored.
- A pay-per-use VPN gateway can be restored only when the following conditions are met:
  - The VPN gateway was deleted within 24 hours.
  - Both EIPs bound to the VPN gateway have not been unbound.
  - The VPC or enterprise router interconnected with the VPN gateway is available. If the VPC or enterprise router does not exist, restore the VPC or enterprise router first.
  - Your account is normal and is not in arrears or frozen.
- A VPN connection of a pay-per-use VPN gateway can be restored only when the following conditions are met:
  - The VPN gateway and customer gateway are available. If one of them does not exist, restore it first.
  - Your account is normal and is not in arrears or frozen.

The health check configuration of a pay-per-use VPN connection cannot be restored even after the VPN connection is restored. Therefore, you need to reconfigure the health check function.

# 3 Networking and Application Scenarios

---

## 3.1 Can I Visit Websites Across International Borders Using a VPN?

No.

VPN connects a VPC and the network of an on-premises data center, that is, site-to-site connection.

## 3.2 Can I Deploy an Application on the Cloud and a Database in an On-premises Data Center and Connect Them Through a VPN?

Yes.

A VPN connects a VPC and an on-premises data center.

After a VPN is set up, service traffic can be transmitted between the VPC and on-premises data center. For an application server on the cloud, access to an on-premises database is logically the same as access to other hosts in the same LAN. Given this, it is feasible to use a VPN to connect an application on the cloud to a database in an on-premises data center.

This is a typical IPsec VPN scenario.

Additionally, there are no limitations on the service initiator. That is, service requests can be initiated from the cloud or the on-premises data center.

---

### NOTICE

- After a VPN is set up, check the network latency and packet loss rate to ensure smooth service running.
  - It is recommended that you run the ping command to check the packet loss and network latency details.
-

### 3.3 How Many VPN Connections Do I Need to Connect Multiple On-premises Servers to the Cloud?

Huawei Cloud VPN uses IPsec VPN technology. It connects a VPC on the cloud and your on-premises data center. Therefore, the number of VPN connections is irrelevant to the number of servers to be connected to the cloud, but to the number of data centers where the servers are located.

Two EIPs can be bound to a VPN gateway for communication with a customer gateway.

- If an on-premises data center has only one egress gateway, all servers or hosts in the data center connect to the Internet through this gateway. In this case, you need to configure a VPN connection group consisting of two VPN connections. That is, configure a VPN connection for each of the two EIPs of the VPN gateway to communicate with the egress gateway in the on-premises data center.
- If an on-premises data center has two egress gateways, the servers or user hosts in the data center connect to the Internet through the two egress gateways. In this case, you need to configure two VPN connection groups, each of which consisting of two VPN connections. That is, configure a VPN connection for each of the two EIPs of each VPN gateway to communicate with both egress gateways in the on-premises data center.

### 3.4 What Are the Differences Between IPsec VPN and SSL VPN in Application Scenarios and Connection Modes?

#### Application Scenarios

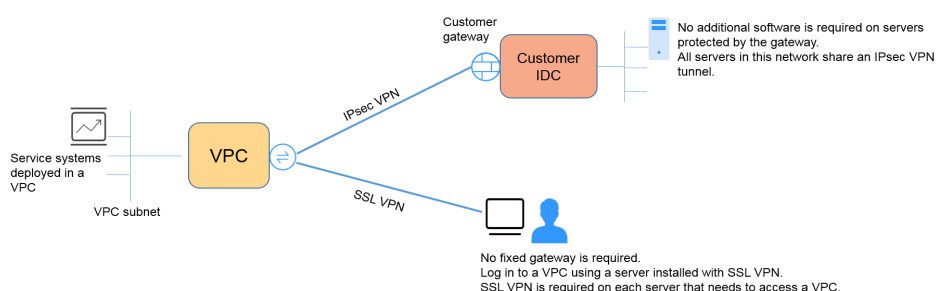
IPsec VPN connects two LANs, such as a branch and its headquarters, or an on-premises data center and a VPC.

SSL VPN connects a client to a LAN. For example, the portable computer of an employee on a business trip accesses the internal network of the company.

#### Connection Modes

IPsec VPN requires fixed gateways, such as firewalls or routers, at both ends. The administrator needs to configure gateways at both ends to enable them to complete IPsec VPN negotiation.

SSL VPN requires a specific client program installed on hosts. Users need to enter usernames and password to connect the hosts to SSL servers.

**NOTE**

Huawei Cloud supports only IPsec VPN.

### 3.5 Does a VPN Allow for Communications Between Two VPCs?

- If the two VPCs are in the same region, use a VPC peering connection to connect them.
- If the two VPCs are in different regions, use a VPN to connect them. The operations are as follows:
  - a. Create a VPN gateway for each VPC, and create a VPN connection between the two VPN gateways.
  - b. For the VPN connection, set the customer gateway to the EIP of the peer VPN gateway.
  - c. For the VPN connection, set the customer subnet to the subnet of the peer VPC.
  - d. Set the same pre-shared keys (PSKs) and algorithms for the two VPCs.

### 3.6 What Are the Impacts of a VPN on an On-premises Network? What Are the Changes to the Route for Accessing an ECS?

When configuring a VPN, you need to perform the following operations on the gateway in your on-premises data center:

- Configure IKE and IPsec policies.
- Set the connection mode to route-based or policy-based.
- Check the route configuration on the gateway to ensure that traffic destined for a Huawei Cloud VPC can be routed to the correct outbound interface (interface having an IPsec policy bound).

### 3.7 What Configurations Are Required at Both Ends of a VPN That Connects an On-premises Data Center to a VPC?

To implement the VPN interconnection, create a VPN on the cloud and configure the VPN device in the on-premises data center.

- Create a VPN on the cloud.
  - Buy a VPN gateway, and configure the billing mode, bandwidth, and interconnected VPC.
  - Create a customer gateway and configure the routing mode.
  - Buy a VPN connection, and configure the gateway IP addresses and subnets at both ends, as well as negotiation policies.
- Configure the VPN device in the on-premises data center.
  - a. Configure the public IP address used by the on-premises data center to connect to the cloud, and complete the configurations of IPsec negotiation phase 1 and phase 2 on the VPN device.
  - b. Configure routes, NAT, and security policies on the VPN device.

### 3.8 Can I Connect a Network with Two Egresses to a VPC Through Two VPN Connections?

Yes.

### 3.9 Can I Connect Two VPCs in the Same Region Through a VPN?

No.

You can use a VPC peering connection or Cloud Connect connection to connect two VPCs in the same region.

### 3.10 How Can I Connect Two VPCs in the Same Region?

You can use a VPC peering connection or Cloud Connect connection to connect two VPCs in the same region. VPC peering can only connect VPCs in the same region; Cloud Connect can also connect VPCs in different regions.

## 3.11 How Do I Enable Communications Between Two VPCs and an On-premises Network?

### Network Topology

IDC-VPC 1-VPC 2



IDC indicates an on-premises data center. A VPN connection is established between VPC 1 and the IDC.

### Procedure

1. Check whether the two VPCs are in the same region.
  - If so, use a VPC peering connection or Cloud Connect connection to connect the two VPCs. Such a connection is free of charge.
  - If not, use a Cloud Connect connection to connect the two VPCs. You need to pay for the Cloud Connect bandwidth.
2. Establish a VPN connection between the IDC and one VPC (VPC 1 in this example).

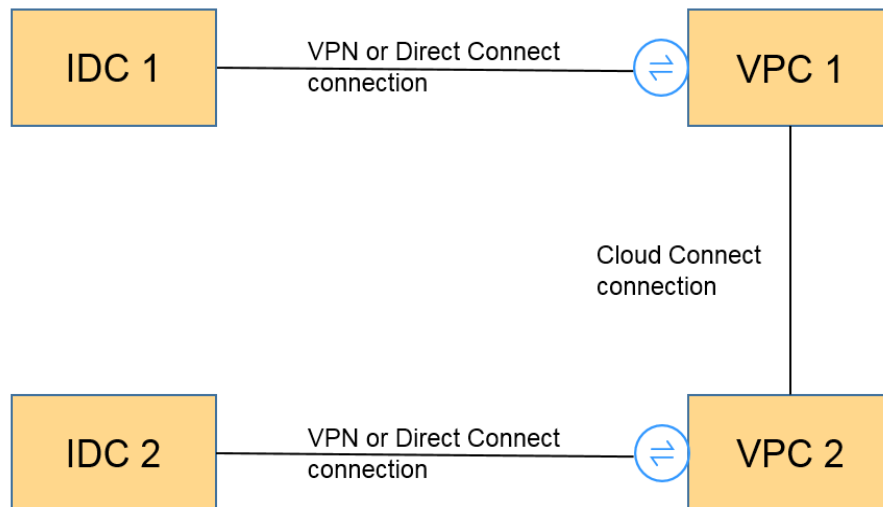
In the on-premises data center, set subnets of VPC 1 and VPC 2 as remote subnets. The local subnet of VPC 1 must contain the subnet connected through a VPC peering connection or Cloud Connect connection. The subnet route of the VPC peering connection or Cloud Connect connection needs to destine for the on-premises subnet.

## 3.12 How Do I Connect Four Subnets?

[Figure 3-1](#) shows the network topology.



**Figure 3-1** Network topology



1. Use a VPN connection or Direct Connect connection to connect IDC 1 to VPC 1.
2. Use a Cloud Connect connection to connect VPC 1 to VPC 2. (You can also use a VPC peering connection to connect VPC 1 to VPC 2 if they are in the same region.)
3. Use a VPN connection or Direct Connect connection to connect VPC 2 to IDC 2.
4. Update VPN subnets, Cloud Connect subnet routes, and Direct Connect subnet routes. Then, the four subnets are reachable to reach other.

### 3.13 Do I Need Two VPN Connections to Connect Four Subnets of Two Regions If Each Region Has Two Subnets?

No.

Only one VPN connection is required between two regions. The subnets can all be added to the VPN connection.

In this scenario, if you attempt to create a second VPN connection, the management console displays a message indicating that a conflict occurs because the two connections have the same customer gateway address.

### 3.14 Can I Access OBS Through a VPN?

Yes.

1. With the help of the VPC endpoint service, you can access OBS through a VPN. You need to create two VPC endpoints for the private DNS server and OBS of Huawei Cloud, respectively.

2. Configure the private DNS server and routes in your on-premises data center.

### 3.15 How Do I Connect My Personal Computer to the Cloud Through a VPN?

Common home broadband routers, Windows hosts providing VPN services (such as L2TP), and personal mobile terminals cannot connect to Huawei Cloud through a VPN.

To use Huawei Cloud VPN, on-premises devices must support the standard IPsec protocol.

### 3.16 How Do I Access Huawei Cloud ECSs at Home When My Enterprise Network Has Been Connected to Huawei Cloud Through a VPN?

A Huawei Cloud VPN is an IPsec VPN that connects an on-premises LAN to a VPC on the cloud. Your home network is not a part of your enterprise LAN, so you cannot directly connect to the VPC on the cloud at home.

If your host at home needs to access VPC resources on the cloud, your host can directly access the EIP of the corresponding service. Alternatively, your host can connect to the LAN of your enterprise through SSL VPN (if supported), and then access VPC resources on the cloud through the LAN.

### 3.17 How Do I Establish a VPN Connection Temporarily If No IPsec-Capable On-Premises Device Is Available After I Purchase a Huawei Cloud VPN Gateway and VPN Connection?

To establish a VPN connection with Huawei Cloud, you must have an on-premises device that supports the standard IPsec protocol and have a fixed public IP address.

If the preceding requirements are not met, you can install third-party IPsec software on a host to temporarily connect to Huawei Cloud.

Recommended third-party IPsec software includes strongSwan, Openswan, and GreenBow. For details about the interconnection, see .

### 3.18 How Do I Select a Proper Region on the Cloud When I Buy a VPN Gateway?

You can select a VPC in any region when you buy a VPN gateway.

It is recommended that you select the region nearest to your on-premises data center to minimize the impact of the Internet on the VPN.

- To connect to multiple VPCs in the same region, you can use VPN and Direct Connect.
- To connect to multiple VPCs in different regions, you can use VPN and Cloud Connect.

# 4 Billing and Payments

---

## 4.1 How Will I Be Charged for My Use of a VPN? Will I Be Charged for VPN Gateway EIPs?

VPNs are billed by the following items on a yearly/monthly or pay-per-use basis.

- VPN gateway
- VPN connection

By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway. You can purchase additional VPN connections if required.

- EIP bandwidth of a VPN gateway

The VPN gateway bandwidth can be billed by traffic or bandwidth.

- a. A yearly/monthly VPN gateway can only be billed by bandwidth. The price of a yearly/monthly VPN gateway includes the price of the VPN connections that can be created for the gateway and the bandwidth price.
- b. The billing cycle of the pay-per-use billing mode is 1 hour. When you create a pay-per-use VPN gateway, the system prompts you to create VPN connections. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway. If more connection groups are required, you need to purchase them.

### NOTE

A VPN gateway cannot share a bandwidth with an EIP bound to an ECS.

## 4.2 What Are the Differences Between Billing the VPN Gateway EIP Bandwidth by Bandwidth and by Traffic?

The VPN gateway EIP bandwidth can be billed by bandwidth or by traffic.

The differences are as follows:

- Billed by bandwidth: The billing cycle is 1 hour. The generated fee depends on the bandwidth.
- Billed by traffic: The fee is calculated based on the outgoing traffic of a VPC generated every hour, which is not affected by the bandwidth.

### 4.3 Can a VPN Billed by Traffic Use a Shared Data Package?

No.

The VPN service is billed independently and cannot use shared data packages.

### 4.4 For How Many VPN Connections Will I Be Charged to Connect VPCs in Different Regions?

VPNs can be used to connect VPCs in different regions. The VPN bandwidth and connections of each region will be billed independently. Therefore, when calculating the estimated fees, you need to check the total number of regions and their connection relationships.

For example, assume that Region A needs to establish a VPN connection with Region B and Region C, respectively. The VPN gateway of Region A has two connections; the VPN gateway of Region B has one connection; and the VPN gateway of Region C has one connection.

In this case, you will be charged for four VPN connections.


### 4.5 How Do I Change the Billing Mode of a VPN Gateway from Pay-Per-Use to Yearly/Monthly?

#### Prerequisites

- The pay-per-use VPN gateway is billed by bandwidth.
- To change the billing mode of a VPN gateway billed by traffic from pay-per-use to yearly/monthly, first change the VPN gateway from being billed by traffic to being billed by bandwidth and then from pay-per-use to yearly/monthly.

#### Procedure

Perform the following operations:

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** and choose **Networking > Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.

5. On the **VPN Gateways** page, locate the row that contains the target VPN gateway, choose **More > Change Billing Mode** in the **Operation** column.
6. In the **Change Billing Mode** dialog box, click **OK**.

 **NOTE**

The billing mode of a VPN gateway cannot be changed from yearly/monthly to pay-per-use and the VPN gateway bandwidth included in the yearly/monthly subscription cannot be decreased.

7. Confirm the VPN gateway information, set a renewal duration, and click **Pay**.
8. On the payment page, confirm the order information, select a coupon or discount, select a payment method, and click **Pay**.

 **NOTE**

Changing the billing mode of a VPN gateway from pay-per-use to yearly/monthly will not affect your services.

## 4.6 Will a Yearly/Monthly VPN Gateway Be Automatically Renewed?

Yes.

Huawei Cloud will automatically collect renewal fees from your balance.

A yearly/monthly VPN gateway needs to be prepaid. To ensure that your connection is normal, top up your account if your balance is not enough.

## 4.7 Can I Unsubscribe from a Yearly/Monthly VPN Gateway?

Yes.

On the **VPN Gateways** page, locate the row that contains the VPN gateway you want to unsubscribe and choose **More > Delete** in the **Operation** column. After you unsubscribe from a yearly/monthly VPN gateway, all VPN connections created for the gateway will also be deleted and cannot be recovered.

After the unsubscription, the remaining prepaid fees will be refunded.

## 4.8 When Will My VPN Resources Be Frozen? How Can I Unfreeze the VPN Resources?

- If pay-per-use VPN resources are in arrears, the resources enter the grace period, during which you can still access and use the resources. If the grace period ends and you have not paid off the arrears, the resources enter the retention period, during which the resources are frozen. Frozen resources are unavailable and cannot be modified or deleted. If the retention period ends and you still have not topped up your account and paid off the arrears, the resources will be released and cannot be restored. To ensure that resources

are available, top up your account and pay off the arrears before the resources expire.

- Frozen VPN resources will become available after you renew them or top up your account.

## 4.9 How Are VPN Resources Billed and How Do I Use Coupons?

A VPN gateway can be billed on a pay-per-use or yearly/monthly basis.

- Pay-per-use: Fees are deducted from the account balance based on the resource usage.
- Yearly/Monthly: The subscription must be paid for in advance.

If you have a Huawei Cloud coupon, you can use it to top up you account, as long as the coupon is valid. You can then use the new balance in your account to pay for your resources.

Yearly/monthly resources are cost-effective.

Huawei Cloud contract users need to select **Download Contract and Pay** on the console.

# 5 Operations on the Console

---

## 5.1 What Are the Relationships Between a VPC, a VPN Gateway, and a VPN Connection?

- A VPC is a private network on the cloud. Multiple VPCs can be created in the same region while they are isolated from each other. A VPC can be divided into multiple subnets.
- A VPN gateway is created in a VPC and is the access point of a VPN connection. One Huawei Cloud VPC can have multiple VPN gateways, and one VPN gateway can have multiple VPN connections.
- A VPN connection is created for a VPN gateway and connects a VPC to an on-premises data center (or a VPC in another region).

### NOTE

The number of VPN connections is irrelevant to the number of local subnets or the number of customer subnets. It is only related to the number of on-premises data centers (or VPCs in other regions) to be connected to your VPC. The created VPN connections are displayed in the VPN connection list. You can also view the number of VPN connections created for each VPN gateway.

## 5.2 How Long Does It Take for Delivered VPN Configurations to Take Effect?

It takes 1–5 minutes for the VPN configurations to take effect.

### NOTE

After VPN configurations take effect, configure your gateway device on your on-premises network to complete tunnel negotiation with the VPN gateway on Huawei Cloud.



## 5.3 Why Is a VPN Connection Always in Not Connected State After Its Configuration Is Complete?

The configuration may be incorrect.

1. At the two ends (cloud and on-premises data center) of the VPN connection, ensure that the pre-shared keys (PSKs) and negotiation information are consistent, the local and remote subnets are reversed, and the local and remote gateways are also reversed.
2. Ensure that routes, NAT, and security policies are correctly configured on the device in your on-premises data center.

## 5.4 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?

If a pay-per-use EIP is bound to a pay-per-use VPN gateway, deleting the VPN gateway will also delete the bound EIP.

To retain such a pay-per-use EIP, unbind it before deleting the VPN gateway.

## 5.5 What Information About a Created VPN Can Be Modified and What Information Cannot Be Modified?

- VPN gateway
  - You can modify the following information:
    - Name
    - Local subnet
    - Active and standby EIPs
      - To modify the active or standby EIP, unbind the original EIP and bind a new one.  
If a VPN connection has been created for an EIP, the EIP cannot be unbound.
      - For details about how to modify EIP attributes, such as the name, type, and bandwidth, see the [EIP service documentation](#).
  - You cannot modify the following information:
    - Region
    - Association mode
    - VPC
    - Interconnection subnet

- BGP ASN
- Billing mode (yearly/monthly or pay-per-use)
- Specification
- AZ
- Number of VPN connection groups  
The number of VPN connection groups needs to be specified only when **Billing Mode** is set to **Yearly/Monthly**.
- Customer gateway
  - You can modify the following information:
    - Name
  - You cannot modify the following information:
    - Routing mode
    - BGP ASN  
The BGP ASN needs to be specified only when **Routing Mode** is set to **Dynamic (BGP)**.
    - Public IP address
- VPN connection
  - You can modify the following information:
    - Name
    - Local interface address
    - Customer gateway
    - Customer subnet
    - Policy configuration, including IKE and IPsec policies
    - PSK
  - You cannot modify the following information:
    - VPN gateway
    - EIP
    - VPN type (route-based or policy-based)
    - Routing mode (static or BGP)  
The routing mode needs to be specified only when **VPN Type** is set to **Route-based**.
    - Link detection configuration  
The link detection configuration is available only when **VPN Type** is set to **Route-based**.

- Policy configuration, including the source and destination CIDR blocks  
The policy configuration is available only when **VPN Type** is set to **Route-based**.

## 5.6 Do I Need to Configure ACL Rules on the Huawei Cloud Management Console After I Configure ACL Rules on the On-premises Gateway Device?

You need to configure policy rules (ACL rules) for a VPN connection on the Huawei Cloud management console only when **VPN Type** is set to **Policy-based**.

## 5.7 What Do I Do If an Exception Occurs When I Add a Customer Subnet During VPN Connection Creation?

Check whether this customer subnet is involved in a route of a VPC peering, Cloud Connect, or Direct Connect connection. If so, a route conflict occurs and you need to delete the route and create a new one to prevent the conflict.

## 5.8 Where Can I Configure Routes to Customer Subnets on the VPN Console?

When a VPN connection is created, routes to customer subnets are automatically delivered.

## 5.9 Can I Call APIs to Manage Huawei Cloud VPN Resources?

Yes.

## 5.10 What Are a Customer Gateway and a Customer Subnet in a VPN Connection?

A VPN connection is created on Huawei Cloud. As such, a subnet of a Huawei Cloud VPC is a local subnet, and a VPN gateway created on Huawei Cloud is a local gateway. The subnet and gateway in an on-premises data center connected to the VPC are a customer subnet and a customer gateway, respectively.

A customer gateway's IP address is a public IP address.

## 5.11 How Do I Disable PFS When Creating a VPN Connection?

- Huawei Cloud  
In the VPN connection configuration, set **PFS** in the IPsec policy to **Disable**. By default, PFS is enabled on Huawei Cloud.
- Customer gateway in your on-premises data center  
By default, PFS is disabled on some vendors' devices. For details about how to disable PFS, see the corresponding product documentation.

### NOTE

Ensure that the PFS settings on the Huawei Cloud and the customer gateway are consistent. Otherwise, the negotiation will fail.

For security purposes, you are advised to enable PFS on both Huawei Cloud and the customer gateway.

## 5.12 How Many Local and Customer Subnets Can I Add to a VPN?

- You can configure a maximum of 50 local subnets for each VPN gateway.
- You can configure a maximum of 50 customer subnets for each VPN connection.

## 5.13 What Are the Precautions for Configuring the Local and Customer Subnets for a VPN Connection?

- The number of local subnets and the number of customer subnets are limited. If the number of local or customer subnets exceeds the upper limit, aggregate the subnets.
  - Maximum number of local subnets for each VPN gateway: 50
  - Maximum number of customer subnets for each VPN connection: 50
- The local subnet cannot include the CIDR block of the remote subnet. The remote subnet can include the CIDR block of the local subnet.
- There are routes pointing to the local subnets in the VPC where the VPN gateway resides.
- If there are two connections (connection A and connection B) created for a VPN gateway, and the remote subnet of connection A is within that of connection B, when the destination network to be accessed belongs to the overlapped CIDR block, the connection created first is matched first, regardless of the connection status. (Mask length match is not used for the policy-based VPN.)

## 5.14 Why Is a VPN Connection in Not Connected State on the Management Console When It Is Already Available?

There is a certain delay in updating the VPN connection state on the management console.

If the service access is normal, the VPN connection has been established. The state of the VPN connection will be updated to **Connected** after several minutes.

## 5.15 What Can I Do If a Message Is Displayed Indicating That the VPN Connection Does Not Exist After Negotiation Policies Are Modified?

This problem is caused by the page refresh interval.

When you modify advanced policy settings, the system deletes the VPN connection and then creates one. If the page temporarily displays a message indicating that the connection is being deleted or created, do not create the same connection with the same local subnet, customer subnet, and customer gateway again.

If the page remains in the connection deleting or creating state for a long time, .

## 5.16 What Is the Maximum Bandwidth Supported by a VPN Gateway?

The maximum bandwidth supported by a VPN gateway is 1 Gbit/s.

## 5.17 Which IKE Version Should I Select When I Create a VPN Connection?

Huawei Cloud recommends IKEv2 because IKEv1 is not secure. In addition, IKEv2 outperforms IKEv1 in connection negotiation and establishment, authentication methods, dead peer detection (DPD) timeout processing, and security association (SA) timeout processing.

Huawei Cloud will not support IKEv1 soon.

### Introduction to IKEv1 and IKEv2

- As a hybrid protocol, IKEv1 brings some security and performance defects due to its complexity. As such, it has become a bottleneck in the IPsec system.
- IKEv2 addresses the issues of IKEv1 while retaining basic functions of IKEv1. IKEv2 is more simplified, efficient, secure, and robust than IKEv1. Additionally, IKEv2 is defined by RFC 4306 in a single document, whereas IKEv1 are defined

in multiple documents. By minimizing core functions and default password algorithms, IKEv2 greatly improves interoperability between different IPsec VPNs.

## Security Risks of IKEv1

- The cryptographic algorithms supported by IKEv1 have not been updated for more than 10 years. In addition, IKEv1 does not support strong cryptographic algorithms such as AES-GCM and ChaCha20-Poly1305. For IKEv1, the E (Encryption) bit in the ISALMP header specifies that the payloads following the ISALMP header are encrypted, but any data integrity verification of those payloads is handled by a separate hash payload. This separation of encryption from data integrity protection prevents the use of authenticated encryption (AES-GCM) with IKEv1.
- IKEv1 is vulnerable to DoS amplification attacks and half-open connection attacks. After responding to spoofed packets, the responder maintains initiator-responder relationships, consuming a large number of system resources.

This defect is inherent to IKEv1 and is addressed in IKEv2.

- The aggressive mode of IKEv1 is not secure. In this mode, information packets are not encrypted, posing risks of information leakage. There are also brute-force attacks targeting at the aggressive mode, such as man-in-the-middle attacks.

## Differences Between IKEv1 and IKEv2

- **Negotiation process**
  - IKEv1 is complex and consumes a large amount of bandwidth. IKEv1 SA negotiation consists of two phases. In IKEv1 phase 1, an IKE SA is established in either main mode or aggressive mode. Main mode requires three exchanges between peers totaling six ISAKMP messages, whereas aggressive mode requires two exchanges totaling three ISAKMP messages. Aggressive mode is faster, but does not provide identity protection for peers as key exchange and identity authentication are performed simultaneously. In IKEv1 phase 2, IPsec SAs are established through three ISAKMP messages in quick mode.
  - Compared with IKEv1, IKEv2 simplifies the SA negotiation process. IKEv2 requires only two exchanges, totaling four messages, to establish an IKE SA and a pair of IPsec SAs. To create multiple pairs of IPsec SAs, only one additional exchange is needed for each additional pair of SAs.

### NOTE

For IKEv1 negotiation, its main mode involves nine (6+3) messages, and its aggressive mode involves six (3+3) messages. In contrast, IKEv2 negotiation requires only four (2+2) messages.

- **Authentication methods**
  - Only IKEv1 (requiring an encryption card) supports digital envelope authentication (HSS-DE).
  - IKEv2 supports Extensible Authentication Protocol (EAP) authentication. IKEv2 can use an AAA server to remotely authenticate mobile and PC users and assign private IP addresses to these users. IKEv1 does not provide this function and must use L2TP to assign private IP addresses.

- Only IKEv2 supports IKE SA integrity algorithms.
- **DPD timeout processing**
  - Only IKEv1 supports the **retry-interval** parameter. If a device sends a DPD packet but receives no reply within the specified retry-interval, the device records a DPD failure event. When the number of DPD failure events reaches 5, both the IKE SA and IPsec SAs are deleted. IKE SA negotiation will start again only when there is traffic to be transmitted over the IPsec tunnel.
  - In IKEv2, the retransmission interval increases from 1, 2, 4, 8, 16, 32 to 64, in seconds. If no reply is received within eight consecutive transmissions, the peer end is considered dead, and the IKE SA and IPsec SAs are deleted.
- **IKE SA timeout processing and IPsec SA timeout processing**

In IKEv2, the IKE SA soft lifetime is 9/10 of the IKE SA hard lifetime plus or minus a random number. This reduces the likelihood that two ends initiate renegotiation simultaneously. Therefore, you do not manually set the soft lifetime in IKEv2.

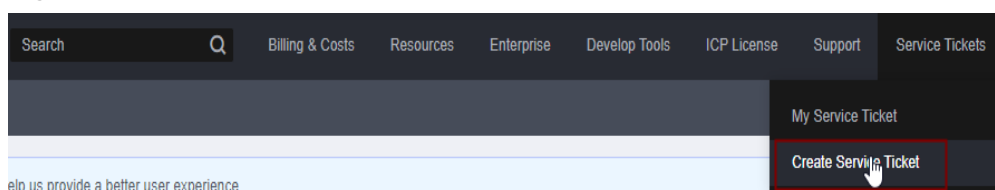
## Advantages of IKEv2 over IKEv1

- Simplifies the SA negotiation process, improving efficiency.
- Fixes many cryptographic security vulnerabilities, improving security.
- Supports EAP authentication, improving authentication flexibility and scalability.
- EAP is an authentication protocol that supports multiple authentication methods. The biggest advantage of EAP is its scalability. That is, new authentication methods can be added without changing the original authentication system. EAP authentication has been widely used in dial-up access networks.
- Employs an Encrypted Payload on basis of ESP. This payload contains both an encryption algorithm and a data integrity algorithm. AES-GCM ensures confidentiality, integrity, and authentication, and works well with IKEv2.

## 5.18 What Types of VPN Service Tickets Are There? How Do I Create a VPN Service Ticket?

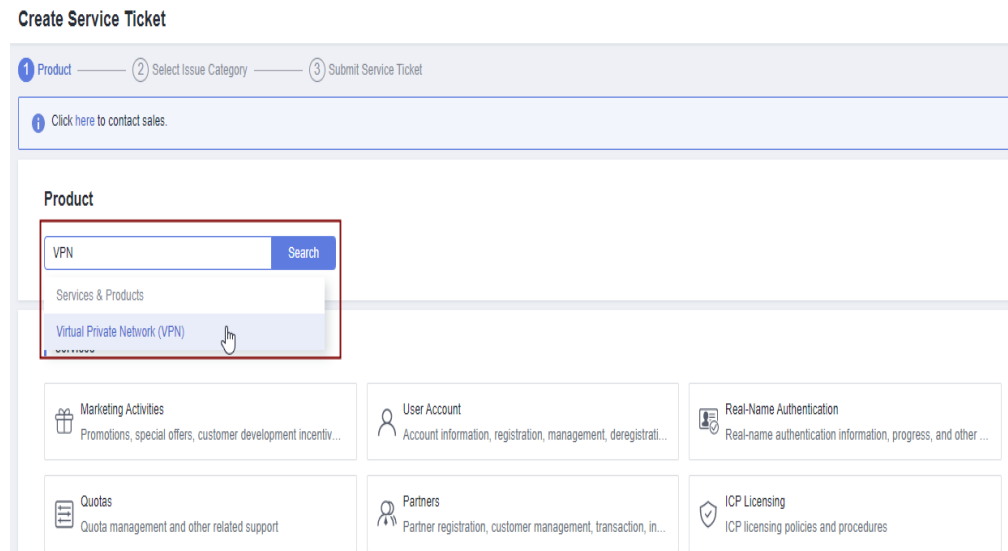
1. Log in to the management console.
2. In the upper right corner of the management console, choose **Service Tickets** > **Create Service Ticket**.

Figure 5-1 Create Service Ticket



3. Search for **VPN** and select **Virtual Private Network (VPN)**.

**Figure 5-2 Selecting Virtual Private Network (VPN)**



4. Select an issue category.

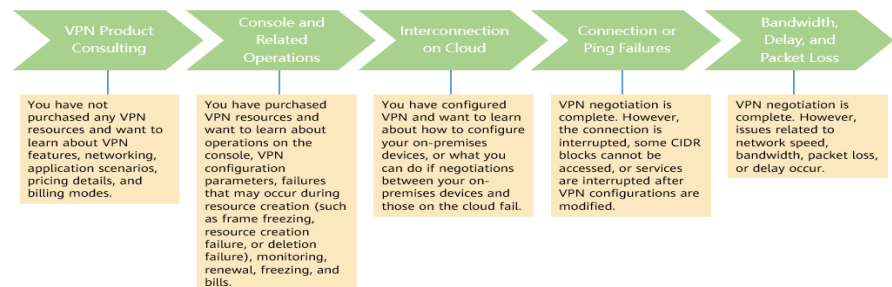
**Figure 5-3 Select Issue Category**



**NOTE**

When you , select an issue category to facilitate problem handling.

**Figure 5-4 Issue category and classification basis**





## 5.19 Are a Username and Password Required for Creating an IPsec VPN Connection?

No. Huawei Cloud IPsec VPN uses a pre-shared key (PSK) for authentication. The PSK is configured on a VPN gateway, and a connection will be established after VPN negotiation is complete. Therefore, no username or password is required for creating an IPsec VPN connection. Generally, SSL, PPTP, and L2TP VPNs use usernames and passwords for authentication.

### NOTE

IPsec XAUTH provides extended authentication for IPsec VPN. It requires users to enter their usernames and passwords during VPN negotiation.

Huawei Cloud VPN does not support IPsec XAUTH.

## 5.20 What VPN Resources Can Be Monitored?

### VPN gateway


The following bandwidth information of a VPN gateway IP address can be monitored: inbound traffic, inbound bandwidth, outbound traffic, outbound bandwidth, and outbound bandwidth usage.

To view the monitoring information, click  in the **Gateway IP Address** column in the VPN gateway list.

### VPN connection


The following information about a VPN connection can be monitored: VPN connection status, average link round-trip time (RTT), maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate.

To monitor average link RTT, maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate, click the VPN connection name and click **Add** in the **Health Check** area on the **Summary** tab page to add health check items.

To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

## 5.21 Will I Be Notified If a VPN Connection Is Interrupted?

The VPN connection status can be monitored. After a VPN connection is created, the VPN service reports the connection status information to Cloud Eye, but does not send alarm notifications to you. To receive notifications, create alarm rules and enable **Alarm Notification** on the Cloud Eye console.

To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

# 6 VPN Negotiation and Interconnection

---

## 6.1 What Devices Can Be Connected to Huawei Cloud Through a VPN?

Huawei Cloud VPN supports the standard Internet Protocol Security (IPsec) protocol. A device in your on-premises data center can connect to Huawei Cloud if the device meets the following requirements:

1. Supports IPsec VPN.
2. Has a fixed public IP address, which can be statically configured, or translated through NAT in NAT traversal scenarios (your device is deployed behind a NAT gateway).

Most devices are routers and firewalls. For details about the interconnection configuration, see .

### NOTE

- Common home broadband routers, Windows hosts providing VPN services (such as L2TP), and personal mobile terminals cannot connect to Huawei Cloud through a VPN.
- The following products can connect to Huawei Cloud through VPNs:
  - Devices: Huawei firewalls and access routers (ARs), Hillstone firewalls, and Check Point firewalls
  - Cloud services: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS), and Microsoft Azure
  - Software: strongSwan
- The IPsec protocol is a standard IETF protocol. Devices that support IPsec can interconnect with Huawei Cloud through a VPN.

Most enterprise-class routers and firewalls support the IPsec protocol.
- Some devices support IPsec VPN only after you purchase required software licenses. Your on-premises data center administrator can check with the device vendor whether a license is required based on the device model.

## 6.2 What Are VPN Negotiation Parameters? What Are Their Default Values?

Table 6-1 VPN negotiation parameters

Protocol	Parameter	Value
IKE	Authentication Algorithm	<ul style="list-style-type: none"><li>• MD5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• SHA2-256 (default value)</li><li>• SHA2-384</li><li>• SHA2-512</li></ul>
	Encryption Algorithm	<ul style="list-style-type: none"><li>• 3DES (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• AES-128 (default value)</li><li>• AES-192</li><li>• AES-256</li><li>• AES-256-GCM-16</li></ul>
	DH Algorithm	<ul style="list-style-type: none"><li>• Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• Group 14 (default value)</li><li>• Group 16</li><li>• Group 19</li><li>• Group 20</li><li>• Group 21</li></ul>
	Version	<ul style="list-style-type: none"><li>• v1 (not recommended due to security risks)</li><li>• v2 (default value)</li></ul>

Protocol	Parameter	Value
	Lifetime (s)	<b>86400</b> (default value) Unit: second Value range: <b>60</b> to <b>604800</b>
	Local ID	<ul style="list-style-type: none"><li>IP Address The local IP address is automatically displayed as the EIP of the VPN gateway, removing the need to manually configure it.</li><li>FQDN</li></ul> By default, the local ID type is IP address and the local ID value is the EIP of the VPN gateway.
	Customer ID	<ul style="list-style-type: none"><li>IP Address</li><li>FQDN</li></ul> By default, the customer ID type is IP address and the customer ID value is the public IP address of the customer gateway.
IPsec	Authentication Algorithm	<ul style="list-style-type: none"><li>SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>MD5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>SHA2-256 (default value)</li><li>SHA2-384</li><li>SHA2-512</li></ul>
	Encryption Algorithm	<ul style="list-style-type: none"><li>AES-128 (default value)</li><li>AES-192</li><li>AES-256</li><li>3DES (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>AES-256-GCM-16</li></ul>

Protocol	Parameter	Value
	PFS	<ul style="list-style-type: none"><li>• DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.)</li><li>• DH group 14 (default value)</li><li>• DH group 15</li><li>• DH group 16</li><li>• DH group 19</li><li>• DH group 20</li><li>• DH group 21</li><li>• Disable</li></ul>
	Transfer Protocol	<ul style="list-style-type: none"><li>• ESP (default value)</li></ul>
	Lifetime (s)	<b>3600</b> (default value) Unit: second Value range: <b>30</b> to <b>604800</b>

 **NOTE**

- Perfect Forward Secrecy (PFS) is a security feature.  
IKE negotiation has two phases, phase one and phase two. The key of phase two (IPsec SA) is derived from the key generated in phase one. Once the key in phase one is disclosed, the security of the IPsec VPN may be adversely affected. To improve the key security, IKE provides PFS. When PFS is enabled, an additional DH exchange will be performed during IPsec SA negotiation to generate a new IPsec SA key, improving IPsec SA security.
- For security purposes, PFS is enabled on Huawei Cloud by default. Ensure that PFS is also enabled on the gateway device in your on-premises data center and the PFS settings on both ends are the same. Otherwise, the negotiation will fail.
- The default traffic-based lifetime of an IPsec SA is 1,843,200 KB and cannot be changed for the Huawei Cloud VPN. This parameter is not involved in negotiation and has no impact on the establishment of an IPsec SA.

## 6.3 Is an IPsec VPN Connection Automatically Established?

Yes. An IPsec VPN connection is automatically established.

## 6.4 How Do I Configure a VPN on an On-premises Device? (Example of Configuring VPN on a Huawei USG6600 Series Firewall)

VPN settings on the device in your on-premises data center must be consistent with those on the cloud. Otherwise, the VPN cannot be established.

To set up a VPN, you also need to configure an IPsec VPN tunnel on the router or firewall in your on-premises data center. The configuration method varies according to your network device in use. For details, see the configuration guide of your network device.

The following uses a Huawei USG6600 series firewall running V100R001C30SPC300 as an example to describe how to configure a VPN on an on-premises device.

Assume that the subnets of an on-premises data center are 192.168.3.0/24 and 192.168.4.0/24, and the public IP address of the IPsec tunnel egress in the on-premises data center is 1.1.1.2. The subnets of a VPC are 192.168.1.0/24 and 192.168.2.0/24, and the public IP address of the IPsec tunnel egress in the VPC is 1.1.1.1.

### Procedure

1. Log in to the command line interface (CLI) of the firewall.
2. Check firewall version information.

```
display version
17:20:502017/03/09
Huawei Versatile Security Platform Software
Software Version: USG6600 V100R001C30SPC300 (VRP (R) Software, Version 5.30)
```
3. Create an ACL.

```
acl number 3065 vpn-instance vpn64
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
q
```
4. Create an IKE proposal.

```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```
5. Create an IKE peer and bind it to the created IKE proposal. The peer IP address is 1.1.1.1.

```
ike peer vpnikepeer_64
pre-shared-key ***** (***** indicates a pre-shared key.)
ike-proposal 64
undo version 2
remote-address vpn-instance vpn64 1.1.1.1
sa binding vpn-instance vpn64
q
```
6. Configure an IPsec proposal.

```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
```

- ```
esp authentication-algorithm sha1
q
```
7. Configure an IPsec policy and bind the IPsec proposal to it.  
IPsec policy vpnIPsec64 1 isakmp  
security acl 3065  
pfs dh-group5  
ike-peer vpnikepeer\_64  
proposal IPsecpro64  
local-address 1.1.1.2  
q
  8. Apply the IPsec policy to the corresponding sub-interface.  
interface GigabitEthernet0/0/2.64  
IPsec policy vpnIPsec64  
q
  9. Test connectivity.  
Test the connectivity between your ECS on the cloud and a host in your on-premises data center, as shown in [Figure 6-1](#).

**Figure 6-1** Connectivity test

```
root@i-psybqhh:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:7c:ba:bf:cc
          inet addr:192.168.3.2  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:7cff:feba:bfcc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2304 (2.3 KB)  TX bytes:3404 (3.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1296 (1.2 KB)  TX bytes:1296 (1.2 KB)

root@i-psybqhh:/home/ubuntu# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data:
64 bytes from 192.168.1.2: icmp_req=1 ttl=62 time=4.55 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=62 time=1.27 ms
64 bytes from 192.168.1.2: icmp_req=3 ttl=62 time=1.25 ms
64 bytes from 192.168.1.2: icmp_req=4 ttl=62 time=0.871 ms
64 bytes from 192.168.1.2: icmp_req=5 ttl=62 time=0.886 ms
64 bytes from 192.168.1.2: icmp_req=6 ttl=62 time=0.676 ms
64 bytes from 192.168.1.2: icmp_req=7 ttl=62 time=1.06 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.676/1.510/4.554/1.258 ms
```

## 6.5 Does Huawei Cloud VPN Support Interconnection with a Customer Gateway Through a Domain Name?

No. Huawei Cloud VPN supports interconnection with a customer gateway only through the public IP address of the customer gateway.

## 6.6 How Many Tunnels Does My VPN Connection Have?

Number of tunnels in a VPN connection = Number of local subnets x Number of customer subnets



- An IPsec tunnel is in Active state when data traffic is transmitted between two subnets at the two ends of the IPsec tunnel.
- A VPN connection is in Connected state as long as one of its tunnels is in Active state.

## 6.7 How Do I Allow Specific Hosts to Access a VPC Subnet Through a Created VPN Connection?

Restrictions in the on-premises data center:

- Access control policies on the VPN device
- ACL rules on the router or switch

Restrictions at the cloud side:

- Security group rules that permit access only from specified IP addresses
- ACL rules

### NOTE

You are advised not to change the local or customer subnet to control access.

## 6.8 Do Huawei Cloud VPNs Have the DPD Function Enabled?

Yes.

By default, the dead peer detection (DPD) function is enabled for Huawei Cloud VPNs to detect the state of the IKE process in an on-premises data center.

After three consecutive detection failures, the IKE process in the on-premises data center is considered abnormal, and the tunnel on the cloud is automatically deleted.

The DPD protocol does not require that the peer end also be configured with DPD, but it requires that the peer end be able to respond to DPD detections. To ensure consistent tunnel states at the two ends, it is recommended that you enable DPD on your on-premises gateway to detect the IKE process state of the VPN service on Huawei Cloud.

### NOTE

Deleting the tunnel in the case of DPD detection failures will not affect service stability.

## 6.9 How Can I Use Security Groups to Prevent VPN Access to Some ECSs in a VPC to Implement Security Isolation?

You can configure security groups to allow access only to specific CIDR blocks or ECSs in a VPC through a VPN.

**Configuration example:** Prevent the customer subnet 192.168.1.0/24 from accessing ECSs in the VPC subnet 10.1.0.0/24.

**Procedure:**

1. Create security groups 1 and 2.
2. Configure security group 1 to deny access from subnet 192.168.1.0/24.
3. Configure security group 2 to permit access from subnet 192.168.1.0/24.
4. Associate ECSs in subnet 10.1.0.0/24 with security group 1 and associate other ECSs in the VPC with security group 2.

## 6.10 Will a VPN Connection Be Re-established After Its Configuration Is Modified?

A VPN connection consists of local subnets, customer subnets, customer gateway, pre-shared keys (PSKs), IKE negotiation policy, and IPsec negotiation policy. A VPN connection is modified if any of the following happens:

- If the local and customer subnets are modified, the connection ID will remain unchanged. If not all subnets are updated, the established tunnel between subnets will not be re-established.
- If the IP address of the customer gateway is changed, the connection ID will remain unchanged, but the VPN connection will be re-established.
- If only the PSKs are changed, the connection ID and status will remain unchanged. The PSK will be checked again during renegotiation. If the PSKs do not match, the renegotiation fails.
- If a negotiation policy is modified (PSK verification is required), the connection ID will be changed and the connection needs to be re-established.

## 6.11 Why Cannot I Initiate Negotiation from Amazon Web Services to Huawei Cloud After They Are Interconnected?

After a VPN connection is established between Amazon Web Services (AWS) and Huawei Cloud, AWS works in Response mode and does not initiate negotiation. As such, SA establishment will not be triggered when an AWS EC2 accesses a Huawei Cloud ECS.

According to the AWS document, negotiation can be initiated only from the customer side (in this case, Huawei Cloud).

## 6.12 How Do I Configure DPD for Interconnection with Huawei Cloud?

By default, DPD is enabled on Huawei Cloud and cannot be disabled.

You can configure DPD as follows:

- DPD-type: on-demand
- DPD idle-time: 30s
- DPD retransmit-interval: 15s
- DPD retry-limit: 3
- DPD msg: seq-hash-notify

The **DPD msg** format at both ends of the VPN connection must be the same, but the DPD type, idle time, retransmission interval, and retry limit can be different.

## 6.13 What Should I Do If My Firewall Cannot Receive Response Packets from the Huawei Cloud VPN Gateway in IKE Phase 1?

1. Check whether the public IP addresses of the two ends can communicate with each other by running the ping command. By default, the VPN gateway EIPs on Huawei Cloud can be pinged.
2. Verify that the on-premises gateway (firewall) and Huawei Cloud VPN gateway can exchange packets with UDP ports 500 and 4500.
3. Verify that the source port number is not translated when the on-premises gateway accesses the VPN gateway on Huawei Cloud. In a NAT traversal scenario, ensure that the source port number is not changed after NAT traversal.
4. Verify that IKE negotiation parameter settings are consistent at the two ends of the VPN.

In a NAT traversal scenario, set the customer ID type to IP address and the value to the post-NAT public IP address of the on-premises gateway.

## 6.14 What Should I Do If My Firewall Cannot Receive Response Packets from a Huawei Cloud VPN Subnet?

1. Check the routes, security policies, NAT configuration, interesting traffic, and negotiation policies for phase 2 negotiation on the on-premises gateway device.
  - Route configurations: Route the data for accessing cloud subnets to tunnels.
  - Security policies: Allow traffic from on-premises subnets to cloud subnets.
  - NAT policies: Do not perform source NAT on the traffic originated from on-premises subnets to cloud subnets.
  - Interesting traffic: The interesting traffic configurations at both ends are reversed at the two ends of a VPN connection. The address object name cannot be used for the interesting traffic configured using IKEv2.
  - Negotiation policies: Ensure the negotiations policies, especially PFS, at both ends are the same.
2. After confirming that both phase 1 and phase 2 negotiations are normal, ensure that the security groups on the cloud permit ICMP packets originated from on-premises subnets to cloud subnets.

## 6.15 How Many Bits Do the DH Groups Used by Huawei Cloud VPN Have?

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Higher DH group numbers are usually more secure, but more time is required to calculate the key.

**Table 6-2** lists the number of bits corresponding to the DH groups used by VPN.

**Table 6-2** Number of bits corresponding to each DH group

| DH Group | Modulus        |
|----------|----------------|
| 1        | 768 bits       |
| 2        | 1024 bits      |
| 5        | 1536 bits      |
| 14       | 2048 bits      |
| 15       | 3072 bits      |
| 16       | 4096 bits      |
| 19       | 256 bits (ECP) |
| 20       | 384 bits (ECP) |
| 21       | 521 bits (ECP) |

### NOTE

The following DH algorithms have security risks and are not recommended: DH group 1, DH group 2, and DH group 5.

# 7 Connection or Ping Failure

---

## 7.1 Why Is a VPN Connection Always in Not Connected State After Its Configuration Is Complete?

The configuration may be incorrect.

1. At the two ends (cloud and on-premises data center) of the VPN connection, ensure that the pre-shared keys (PSKs) and negotiation information are consistent, the local and remote subnets are reversed, and the local and remote gateways are also reversed.
2. Ensure that routes, NAT, and security policies are correctly configured on the device in your on-premises data center.

## 7.2 How Can I Prevent VPN Disconnections?

VPN connections are renegotiated when the IPsec SA lifetime is about to expire or the data transmitted through a VPN connection exceeds 20 GB. Usually, renegotiation does not interrupt VPN connections.

Most disconnections are caused by incorrect configurations at the two ends of the VPN connection or renegotiation failures due to Internet exceptions.

Common causes of disconnections are as follows:

- ACLs at both ends of the VPN connection do not match.
- SA lifetime settings at both ends of the VPN connection are different.
- Dead Peer Detection (DPD) is not configured on the device in your on-premises data center.
- Configuration is modified when the VPN connection is in use.
- Jitter occurs on the carrier's network.

As such, ensure that the following VPN configurations are correct to keep VPN connections alive:

- At the two ends of the VPN connection, the local and remote subnet configurations are reversed.

- SA lifetime settings at both ends of the VPN connection are the same.
- DPD is enabled on the on-premises gateway device, and the number of detection times is 3 or more.
- Parameters are modified at both ends of the VPN connection during the use of the VPN connection.
- Set TCP MAX-MSS to 1300 for the on-premises gateway device.
- The bandwidth of the on-premises gateway device is large enough for the VPN connection.
- VPN connection negotiation can be triggered by both ends and active negotiation has been enabled on the on-premises gateway device.

## 7.3 How Do I Quickly Restore an Interrupted IPsec VPN Connection?

1. If negotiation cannot be triggered, check connectivity between the public IP addresses of gateways at both ends of the IPsec VPN connection. For example, you can run the ping command to check the connectivity. By default, the Huawei Cloud VPN gateway responds to ICMP packets.
2. If connectivity is normal, check whether link switching occurs between outbound interfaces. That is, check whether the traffic for access to the Huawei Cloud VPN gateway is forwarded out from a non-negotiated interface.
3. If traffic is forwarded through the correct link, change the PSKs at both ends of the IPsec VPN connection to trigger re-negotiation.
4. If re-negotiation fails, check whether the negotiation policies configured at both ends are consistent and whether the interesting traffic configurations at both ends are reversed (same number of configurations and same subnets).
5. If the negotiation policies and interesting traffic configurations are correct, disable the VPN connection on the on-premises device. After the VPN connection state on Huawei Cloud changes to **Not connected**, enable the VPN connection on the on-premises device and trigger a data flow.
6. If negotiation still fails, perform the following operations:
  - a. Record the negotiation policies, PSK, local subnets, customer gateway, and customer subnets of the VPN connection configured on Huawei Cloud.
  - b. Use the existing VPN gateway to create another VPN connection. The negotiation policies, PSK, and local subnets are the same as those of the original VPN connection. The customer gateway and customer subnets can be configured randomly.
  - c. After the new VPN connection is created, delete the original VPN connection, and change the customer gateway and customer subnets of the new VPN connection to be the same as those of the original VPN connection.
  - d. Trigger the negotiation again.

If the fault persists, to Huawei Cloud customer service.

## 7.4 What Will Happen If Traffic Exceeds the Bandwidth of a VPN Gateway?

The VPN gateway bandwidth applies to traffic in the outbound direction of a VPC. If outbound traffic in the VPC exceeds the bandwidth, network congestion will occur, some subnets cannot be accessed, or even the VPN connection will be interrupted due to VPN detection timeout.

In this case, you are advised to increase the VPN gateway bandwidth.

### NOTE

The maximum bandwidth of a VPN is 1 Gbit/s.

## 7.5 Is an IPsec VPN Connection Automatically Established?

Yes. An IPsec VPN connection is automatically established.

## 7.6 Why Cannot ECSs at the Two Ends of a Normal Cross-Region VPN Connection Ping Each Other?

By default, a security group permits outbound traffic with any port number. To allow inbound traffic, add inbound rules to the security group. Ensure that the security group associated with the ECS that needs to receive ping packets allows inbound ICMP requests.

## 7.7 Why Cannot Subnets at the Two Ends of a Normal VPN Connection Access Each Other?

The VPN connection is normal, indicating that the negotiation parameters at both ends of the VPN connection are correct. You need to perform the following operations:

- Verify that routes to the VPN device in your on-premises data center are correctly configured.
- Verify that inter-subnet data exchange is allowed on the VPN device.
- Verify that NAT is not performed on the on-premises subnets that need to access the cloud.
- Verify that mutual access between the public IP addresses of the VPN gateway and customer gateway is permitted.

## 7.8 What Do I Do If a VPN Connection Is Interrupted and a Message Indicating Data Flow Mismatch Is Displayed?

This is usually caused by an ACL mismatch between the VPN gateway on the cloud and the customer gateway in your on-premises data center.

1. Verify that at the two ends of the VPN connection, the local and remote subnets are reversed and the ACL configurations are also reversed.
2. Use the subnet/mask format when you configure interesting traffic in your on-premises data center. Do not use the address object mode since it may cause incompatibility issues.

## 7.9 What Do I Do If a VPN Connection Is Interrupted and a Message Indicating DPD Timeout Is Displayed?

This happens because there is no data exchange over the VPN connection. When the SA lifetime ends, the VPN connection is deleted as the peer end does not respond to the dead peer detection (DPD).

### Solution

1. Enable DPD on the on-premises gateway device, and verify that data flows from both ends can trigger connection establishment.
2. Deploy a ping shell script on the servers at both ends. Alternatively, configure a keepalive function (for example, NQA on Huawei devices) on the on-premises gateway device to keep the connection alive.

## 7.10 Why Is a VPN Connection in Not Connected State on the Management Console When It Is Already Available?


There is a certain delay in updating the VPN connection state on the management console.

If the service access is normal, the VPN connection has been established.

## 7.11 Will I Be Notified If a VPN Connection Is Interrupted?

The VPN connection status can be monitored. After a VPN connection is created, the VPN service reports the connection status information to Cloud Eye, but does not send alarm notifications to you. To receive notifications, create alarm rules and enable **Alarm Notification** on the Cloud Eye console.



To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

## 7.12 What Do I Do If a VPN Connection Fails to Be Established?

1. Log in to the management console and choose **Virtual Private Network > Enterprise - VPN Connections**.
2. In the VPN connection list, locate the target VPN connection, and choose **More > Modify Policy Settings** on the right to view IKE and IPsec policies of the VPN connection.
3. Check the IKE and IPsec policies to see whether the negotiation modes and encryption algorithms at both ends of the VPN connection are the same.  
If the IKE SA has been set up in phase 1 but no IPsec SA has been established in phase 2, the IPsec policies at both ends of the VPN connection may be inconsistent.
4. Check whether the ACL rules are correct.  
If the subnets of your on-premises data center are 192.168.3.0/24 and 192.168.4.0/24, and the VPC subnets are 192.168.1.0/24 and 192.168.2.0/24, configure the ACL rules for each on-premises subnet to allow the communication with the VPC subnets. The following provides an example of ACL configurations:

```
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
```
5. Ping the two ends of the VPN connection from each other to check whether the VPN connection is normal.

## 7.13 What Should I Do If I Cannot Access the ECSs on the Cloud from My On-premises Data Center or LAN After the VPN Connection Has Been Set Up?

The security group denies access from all sources by default. If you want to access your ECSs, configure security group rules to permit access from your on-premises subnets.

## 7.14 Why Is the State of a Successfully Created VPN Connection Displayed as Not Connected?

There is a delay in updating the state of a VPN connection on the management console. Please refresh the page in about 2 minutes.

## 7.15 Do Huawei Cloud VPNs Have the DPD Function Enabled?

Yes.

By default, the dead peer detection (DPD) function is enabled for Huawei Cloud VPNs to detect the state of the IKE process in an on-premises data center.

After three consecutive detection failures, the IKE process in the on-premises data center is considered abnormal, and the tunnel on the cloud is automatically deleted.

The DPD protocol does not require that the peer end also be configured with DPD, but it requires that the peer end be able to respond to DPD detections. To ensure consistent tunnel states at the two ends, it is recommended that you enable DPD on your on-premises gateway to detect the IKE process state of the VPN service on Huawei Cloud.

### NOTE

Deleting the tunnel in the case of DPD detection failures will not affect service stability.

DPD can detect exceptions in the IKE process at the peer end in time and reset the tunnel to ensure tunnel synchronization between the two ends. After a tunnel is deleted, if there is traffic transmitted over the tunnel, the tunnel can be re-established through negotiation.

# 8 Public Addresses

---

## 8.1 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?

If a pay-per-use EIP is bound to a pay-per-use VPN gateway, deleting the VPN gateway will also delete the bound EIP.

To retain such a pay-per-use EIP, unbind it before deleting the VPN gateway.

## 8.2 Can EIPs Be Used as VPN Gateway IP Addresses?

No.

When you create a VPN gateway, its IP address is automatically assigned. This IP address has preset configurations and can be used for interconnection with a VPC. However, an EIP cannot be used for interconnection with a VPC.

## 8.3 Do I Need to Purchase EIPs for Hosts to Communicate with Each Other Through a VPN?

If your on-premises hosts need to access an ECS on the cloud through a VPN, you do not need to purchase any EIPs for the ECS.

If an ECS needs to provide services accessible from the Internet, you need to purchase an EIP for the ECS.

## 8.4 Why Does an ECS Have EIP Access Information After I Enable a VPN?

A possible cause is that the ECS has an EIP bound before the VPN is used. In this scenario, you can access the ECS through both the VPN and the EIP.

To allow only hosts on the VPN to access the ECS, unbind the EIP from the ECS after the VPN connection is established.

## 8.5 Can My On-premises Gateway Have a Non-fixed Public IP Address?

No.

To connect your on-premises data center to Huawei Cloud through a VPN, your on-premises gateway must have a fixed public IP address. This public IP address can be statically configured, or translated through NAT in NAT traversal scenarios (your device is deployed behind a NAT gateway).

### NOTE

Common home broadband routers, Windows hosts providing VPN services (such as L2TP), and personal mobile terminals cannot connect to Huawei Cloud through a VPN.

# 9 Route Configurations

---

## 9.1 What Are a Customer Gateway and a Customer Subnet in a VPN Connection?

A VPN connection is created on Huawei Cloud. As such, a subnet of a Huawei Cloud VPC is a local subnet, and a VPN gateway created on Huawei Cloud is a local gateway. The subnet and gateway in an on-premises data center connected to the VPC are a customer subnet and a customer gateway, respectively.

A customer gateway's IP address is a public IP address.

## 9.2 Where Can I Add Routes to Customer Subnets on the VPN Console?

When a VPN connection is created, routes to customer subnets are automatically delivered.

## 9.3 Do I Need to Add a Route for an ECS with Multiple NICs to Reach the On-premises Network?

- If the primary network interface card (NIC) is used to establish a VPN connection with the on-premises network, no route needs to be added.
- If a non-primary NIC is used to establish a VPN connection with the on-premises network, add a route to the on-premises network with the gateway address of the non-primary NIC as the next hop.

# 10 Subnet Configurations

---

## 10.1 What Are the Precautions for Configuring the Local and Customer Subnets for a VPN Connection?

- The number of local subnets and the number of customer subnets are limited. If the number of local or customer subnets exceeds the upper limit, aggregate the subnets.
  - Maximum number of local subnets for each VPN gateway: 50
  - Maximum number of customer subnets for each VPN connection: 50
- The local subnet cannot include the CIDR block of the remote subnet. The remote subnet can include the CIDR block of the local subnet.
- There are routes pointing to the local subnets in the VPC where the VPN gateway resides.
- If there are two connections (connection A and connection B) created for a VPN gateway, and the remote subnet of connection A is within that of connection B, when the destination network to be accessed belongs to the overlapped CIDR block, the connection created first is matched first, regardless of the connection status. (Mask length match is not used for the policy-based VPN.)

## 10.2 How Many Local and Customer Subnets Can I Add to a VPN?

- You can configure a maximum of 50 local subnets for each VPN gateway.
- You can configure a maximum of 50 customer subnets for each VPN connection.

## 10.3 What Do I Do If an Exception Occurs When I Add a Customer Subnet During VPN Connection Creation?

Check whether this customer subnet is involved in a route of a VPC peering, Cloud Connect, or Direct Connect connection. If so, a route conflict occurs and you need to delete the route and create a new one to prevent the conflict.

## 10.4 Can the EIP of a VPN Gateway Be Retained After the VPN Gateway Is Deleted?

If a pay-per-use EIP is bound to a pay-per-use VPN gateway, deleting the VPN gateway will also delete the bound EIP.

To retain such a pay-per-use EIP, unbind it before deleting the VPN gateway.

## 10.5 How Do I Plan CIDR Blocks for Access to a VPC Through a VPN Connection?

- The CIDR blocks of a VPC cannot conflict with on-premises CIDR blocks.
- To avoid conflicts with cloud service addresses, do not use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3, or 100.64.0.0/10 for your on-premises network.

## 10.6 How Is a VPN Gateway IP Address Allocated?

VPN gateway IP addresses of Huawei Cloud are a group of IP addresses planned before VPN gateways are purchased. These IP addresses are preset with VPN configurations.

When you buy a VPN gateway, the system randomly assigns an IP address and binds it to the VPC you selected. This IP address can be bound to only one VPC.

You cannot change the IP address of a VPN gateway as this IP address has preset configurations. When a VPN gateway is deleted, the binding relationship between the gateway IP address and the gateway VPC is released. When a new VPN gateway is purchased, the system randomly allocates a new gateway IP address.

# 11 VPN Interesting Traffic

---

## 11.1 Do I Need to Configure ACL Rules on the Huawei Cloud Management Console After I Configure ACL Rules on the On-premises Gateway Device?

You need to configure policy rules (ACL rules) for a VPN connection on the Huawei Cloud management console only when **VPN Type** is set to **Policy-based**.

## 11.2 How Do I Configure and Modify the Interesting Traffic of a VPN on the Cloud?

The number of rules that specify interesting traffic is the product of the number of local subnets and the number of customer subnets. For example, when there are local subnets A and B and customer subnets C, D, and E, the following six rules need to be configured to specify interesting traffic:

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

If you modify the local or customer subnets on the management console, the interesting traffic configuration is automatically updated. That is, ACL rules on the cloud are modified.



# 12 Keeping VPN Connections Alive

---

## 12.1 How Can I Prevent VPN Disconnections?

VPN connections are renegotiated when the IPsec SA lifetime is about to expire or the data transmitted through a VPN connection exceeds 20 GB. Usually, renegotiation does not interrupt VPN connections.

Most disconnections are caused by incorrect configurations at the two ends of the VPN connection or renegotiation failures due to Internet exceptions.

Common causes of disconnections are as follows:

- ACLs at both ends of the VPN connection do not match.
- SA lifetime settings at both ends of the VPN connection are different.
- Dead Peer Detection (DPD) is not configured on the device in your on-premises data center.
- Configuration is modified when the VPN connection is in use.
- Jitter occurs on the carrier's network.

As such, ensure that the following VPN configurations are correct to keep VPN connections alive:

- At the two ends of the VPN connection, the local and remote subnet configurations are reversed.
- SA lifetime settings at both ends of the VPN connection are the same.
- DPD is enabled on the on-premises gateway device, and the number of detection times is 3 or more.
- Parameters are modified at both ends of the VPN connection during the use of the VPN connection.
- Set TCP MAX-MSS to 1300 for the on-premises gateway device.
- The bandwidth of the on-premises gateway device is large enough for the VPN connection.
- VPN connection negotiation can be triggered by both ends and active negotiation has been enabled on the on-premises gateway device.

# 13 Monitoring

---

## 13.1 What VPN Resources Can Be Monitored?

### VPN gateway


The following bandwidth information of a VPN gateway IP address can be monitored: inbound traffic, inbound bandwidth, outbound traffic, outbound bandwidth, and outbound bandwidth usage.

To view the monitoring information, click  in the **Gateway IP Address** column in the VPN gateway list.

### VPN connection


The following information about a VPN connection can be monitored: VPN connection status, average link round-trip time (RTT), maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate.

To monitor average link RTT, maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate, click the VPN connection name and click **Add** in the **Health Check** area on the **Summary** tab page to add health check items.

To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

## 13.2 Will I Be Notified If a VPN Connection Is Interrupted?

The VPN connection status can be monitored. After a VPN connection is created, the VPN service reports the connection status information to Cloud Eye, but does not send alarm notifications to you. To receive notifications, create alarm rules and enable **Alarm Notification** on the Cloud Eye console.

To view the status of a VPN connection, click  in the **Monitoring** column of the VPN connection.

### **13.3 Can I View the Traffic of Each VPN Connection?**

No. VPN traffic is monitored on a per-VPN gateway basis. You can view the inbound and outbound traffic as well as the inbound and outbound bandwidths of a VPN gateway, but cannot view the traffic statistics of a specific VPN connection.

### **13.4 Will I Be Notified of Abnormal VPN Monitoring Results?**

Yes.

You can configure, on the Simple Message Notification (SMN) and Cloud Eye consoles, to receive notifications if abnormal VPN monitoring results occur.

# 14 Bandwidth and Network Speed

## 14.1 How Is the Network Speed of a VPN Connection Tested?

Test environment: A VPN connection has been created. ECSs have been created on the local subnets of VPCs at the two ends of the VPN connection. The ECSs can ping each other.

**When the bandwidth of a purchased VPN gateway is 200 Mbit/s:**

1. When the ECSs at the two ends of the VPN connection run Windows, iPerf3 and FileZilla (a free FTP application for file upload and download) are used to test the network speed. The test result is 180 Mbit/s, meeting requirements.

### NOTE

The TCP-based FTP protocol has a congestion control mechanism, and the IPsec protocol adds new headers to original packets. As such, it is normal in the industry, to have a network speed deviation of about 10%.

**Figure 14-1** shows the result of testing the 200 Mbit/s bandwidth on the iPerf3 client.

**Figure 14-1** Test result for 200 Mbit/s bandwidth (iPerf3 client)

```
C:\Windows>iperf3 -c 10.1.0.180 -i 1 -w 1M
Connecting to host 10.1.0.180, port 5201
[ 41] local 192.168.0.75 port 49212 connected to 10.1.0.180 port 5201
[ ID] Interval           Transfer     Bandwidth
[ 41] 0.00-1.01   sec    17.1 MBytes  142 Mbits/sec
[ 41] 1.01-2.00   sec    30.0 MBytes  253 Mbits/sec
[ 41] 2.00-3.01   sec    19.8 MBytes  165 Mbits/sec
[ 41] 3.01-4.01   sec    23.2 MBytes  194 Mbits/sec
[ 41] 4.01-5.00   sec    18.9 MBytes  161 Mbits/sec
[ 41] 5.00-6.01   sec    26.2 MBytes  219 Mbits/sec
[ 41] 6.01-7.01   sec    18.4 MBytes  153 Mbits/sec
[ 41] 7.01-8.01   sec    23.2 MBytes  195 Mbits/sec
[ 41] 8.01-9.00   sec    21.1 MBytes  180 Mbits/sec
[ 41] 9.00-10.01  sec    21.0 MBytes  174 Mbits/sec
-----
[ ID] Interval           Transfer     Bandwidth
[ 41] 0.00-10.01  sec    219 MBytes  183 Mbits/sec
[ 41] 0.00-10.01  sec    219 MBytes  183 Mbits/sec
iperf Done.
```

Figure 14-2 shows the result of testing the 200 Mbit/s bandwidth on the iPerf3 server.

Figure 14-2 Test result for 200 Mbit/s bandwidth (iPerf3 server)

```
Server listening on 5201
-----
Accepted connection from 192.168.0.75, port 49211
[ 5] local 10.1.0.180 port 5201 connected to 192.168.0.75 port 49212
[ ID] Interval      Transfer    Bandwidth
[ 5] 0.00-1.00    sec 15.1 MBytes 127 Mbits/sec
[ 5] 1.00-2.01    sec 30.2 MBytes 252 Mbits/sec
[ 5] 2.01-3.00    sec 19.7 MBytes 166 Mbits/sec
[ 5] 3.00-4.01    sec 23.6 MBytes 197 Mbits/sec
[ 5] 4.01-5.01    sec 18.6 MBytes 156 Mbits/sec
[ 5] 5.01-6.00    sec 26.3 MBytes 222 Mbits/sec
[ 5] 6.00-7.01    sec 18.4 MBytes 153 Mbits/sec
[ 5] 7.01-8.01    sec 23.4 MBytes 196 Mbits/sec
[ 5] 8.01-9.01    sec 21.5 MBytes 180 Mbits/sec
[ 5] 9.01-10.00   sec 20.4 MBytes 173 Mbits/sec
[ 5] 10.00-10.07  sec 1.32 MBytes 162 Mbits/sec
-----
[ ID] Interval      Transfer    Bandwidth
[ 5] 0.00-10.07   sec 0.00 Bytes 0.00 bits/sec
[ 5] 0.00-10.07   sec 219 MBytes 182 Mbits/sec
-----
sender
receiver
```

2. When the ECSs at the two ends of the VPN connection run CentOS 7, iPerf3 is used to test the network speed. The test result is 180 Mbit/s, meeting requirements.
3. When the ECS functioning as a server runs CentOS 7 and the ECS functioning as a client runs Windows, iPerf3 and FileZilla are used to test the network speed. The test result is 20 Mbit/s, failing to meet requirements.

This is because TCP implementations on Windows and Linux are different.

Figure 14-3 shows the result of using iPerf3 to test the network speed between two ECSs running different operating systems.

Figure 14-3 Test result on iPerf3

```
C:\Windows>iperf3 -c 10.1.0.182 -i 1 -w 1M
Connecting to host 10.1.0.182, port 5201
[ 4] local 192.168.0.75 port 49426 connected to 10.1.0.182 port 5201
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-1.00    sec 4.38 MBytes 36.7 Mbits/sec
[ 4] 1.00-2.00    sec 4.50 MBytes 37.7 Mbits/sec
[ 4] 2.00-3.00    sec 5.12 MBytes 43.0 Mbits/sec
[ 4] 3.00-4.00    sec 1.75 MBytes 14.7 Mbits/sec
[ 4] 4.00-5.00    sec 2.12 MBytes 17.8 Mbits/sec
[ 4] 5.00-6.00    sec 3.25 MBytes 27.3 Mbits/sec
[ 4] 6.00-7.00    sec 2.12 MBytes 17.8 Mbits/sec
[ 4] 7.00-8.00    sec 1.25 MBytes 10.5 Mbits/sec
[ 4] 8.00-9.00    sec 2.25 MBytes 18.9 Mbits/sec
[ 4] 9.00-10.00   sec 2.38 MBytes 19.9 Mbits/sec
-----
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-10.00   sec 29.1 MBytes 24.4 Mbits/sec
[ 4] 0.00-10.00   sec 28.2 MBytes 23.6 Mbits/sec
-----
iperf Done.
```

**When the bandwidth of a purchased VPN gateway is 1000 Mbit/s:**

**NOTE**

Some regions support only 300 Mbit/s bandwidth by default. If higher bandwidth is required, apply for 300 Mbit/s bandwidth and then for capacity expansion.

The VPN gateway bandwidth is shared by all of its VPN connections. To fully use the large bandwidth of 1000 Mbit/s, deploy multiple ECSs with high specifications

as the forwarding performance of a single ECS is limited. ECSs with their NICs supporting the bandwidth of 2 Gbit/s or higher are recommended.

**Conclusions: Based on the preceding test results, bandwidths of Huawei Cloud VPN gateways meet requirements. To fully use your purchased bandwidth, you are advised to use servers running the same operating system and using NICs meeting certain requirements at the two ends of a VPN connection.**

## 14.2 In Which Direction Is the VPN Bandwidth Limited? What Is the Unit of Bandwidth?

Your purchased VPN gateway bandwidth applies to the outbound direction of Huawei Cloud. To achieve a balance between bandwidths in the inbound and outbound directions, the bandwidth in the inbound direction is limited as follows:

- If the purchased bandwidth is 10 Mbit/s or less, the bandwidth in the inbound direction is limited to 10 Mbit/s.
- If the purchased bandwidth is greater than 10 Mbit/s, the bandwidth in the inbound direction is the same as the purchased bandwidth.

The unit of bandwidth is Mbit/s and that of traffic is GB.

## 14.3 How Do I Change the VPN Bandwidth?

1. In the VPN gateway list, click the name of a VPN gateway. The gateway details page is displayed.
2. In the **EIP** area, click **Change** next to **Bandwidth**.
3. Change the EIP bandwidth.

## 14.4 What Will Happen If Traffic Exceeds the Bandwidth of a VPN Gateway?

The VPN gateway bandwidth applies to traffic in the outbound direction of a VPC. If outbound traffic in the VPC exceeds the bandwidth, network congestion will occur, some subnets cannot be accessed, or even the VPN connection will be interrupted due to VPN detection timeout.

In this case, you are advised to increase the VPN gateway bandwidth.

### NOTE

The maximum bandwidth of a VPN is 1000 Mbit/s.

## 14.5 Why Does the VPN Bandwidth Change Not Take Effect?

There is a delay for the VPN bandwidth change to take effect.

Test the bandwidth 5 minutes after you change the bandwidth.

 NOTE

Changing the VPN bandwidth will not interrupt services on networks.

## 14.6 What Are the Differences Between the Bandwidth of a VPN Connection and That of a Direct Connect Connection?

### Concepts

- The bandwidth of a Direct Connect connection is the bandwidth of the physical connection created by a user.
- The bandwidth of a VPN connection applies to the outbound direction of Huawei Cloud.

### Maximum Bandwidth

- By default, the maximum bandwidth of a Direct Connect connection is 1000 Mbit/s. When you create a connection on the management console and set **Port Type** to **10GE single-mode optical port**, the maximum bandwidth is 10 Gbit/s.
- The maximum bandwidth of a VPN is 1000 Mbit/s.

### Network Quality

- A Direct Connect user has a dedicated connection with high network quality.
- VPN connections share the bandwidth of their VPN gateway. That is, the total bandwidth of VPN connections cannot exceed the bandwidth of the corresponding VPN gateway. The network quality will be affected by the Internet quality.

## 14.7 How Do I Determine My VPN Bandwidth?

Consider the following when you determine the bandwidth:

- Amount of data transmitted over a VPN tunnel in a period of time (Reserve enough bandwidth to prevent link congestion.)
- Egress bandwidths at the two ends of a VPN connection: The egress bandwidth at the cloud side must be less than that at the on-premises side.

# 15 Quotas

---

## 15.1 What Quotas Does a VPN Have?

### Resource Types

VPN resources include VPN gateways, VPN connections, and customer gateways. The total quota of each resource type varies according to regions.

## 15.2 How Many VPN Gateways and VPN Connections Can I Create By Default?

By default, each user can create a maximum of 50 VPN gateways and 100 customer gateways. Each VPN gateway can have a maximum of 100 connection groups. When two EIPs of a VPN gateway are connected to the same public IP address of a customer gateway, one VPN connection group is used. When two EIPs of a VPN gateway are connected to two customer gateways or two public IP addresses of the same customer gateway, two VPN connection groups are used.

Before purchasing VPN gateways, check your available quota. If the quota is insufficient, to increase the quota.

## 15.3 How Do I Change My VPN Gateway and Connection Quotas?

1. Log in to the management console, and choose **Service Tickets > Create Service Ticket** in the menu bar.
2. On the **Create Service Ticket** page, click **Quotas** in the **Services** area.
3. Click **Quota Application** under **Issue Categories**.
4. Click **Create Now**.

Enter required information and click **Submit**.



## 15.4 How Many IPsec VPNs Can I Have?

By default, each user can create a maximum of 50 VPN gateways and 100 customer gateways. Each VPN gateway can have a maximum of 100 connection groups. When two EIPs of a VPN gateway are connected to the same public IP address of a customer gateway, one VPN connection group is used. When two EIPs of a VPN gateway are connected to two customer gateways or two public IP addresses of the same customer gateway, two VPN connection groups are used.

Before purchasing VPN gateways, check your available quota. If the quota is insufficient, to increase the quota.

# 16 Account Permissions

---

## 16.1 Are a Username and Password Required for Creating an IPsec VPN Connection?

No. Huawei Cloud IPsec VPN uses a pre-shared key (PSK) for authentication. The PSK is configured on a VPN gateway, and a connection will be established after VPN negotiation is complete. Therefore, no username or password is required for creating an IPsec VPN connection. Generally, SSL, PPTP, and L2TP VPNs use usernames and passwords for authentication.

### NOTE

IPsec XAUTH provides extended authentication for IPsec VPN. It requires users to enter their usernames and passwords during VPN negotiation.

Huawei Cloud VPN does not support IPsec XAUTH.

## 16.2 What Should I Do If the System Displays a Message Indicating that I Do Not Have the Permissions to Create a VPN?

- Check whether your account is an IAM account.
- Ensure that your IAM account has the **VPC Administrator**, **Tenant Guest**, and **VPN Administrator** permissions.

If your IAM account does not have VPC operation operations, log in to the IAM console using a Huawei Cloud account, and grant the permissions to your IAM account. For details, see [Creating a User Group and Assigning Permissions](#) and [Adding Users to or Removing Users from a User Group](#).

## 16.3 How Do I Determine that My Account Cannot Create a VPN Due to Insufficient Permissions?

- The VPN gateways and connections created by a Huawei Cloud account are invisible to IAM user accounts.
- A message will be displayed indicating that the system is busy if you create a VPN gateway or connection using an IAM user account.

For details about the permissions required for creating a VPN connection, see [What Should I Do If the System Displays a Message Indicating that I Do Not Have the Permissions to Create a VPN?](#)