Virtual Private Network

FAQ

Issue 01
Date 2019-02-15
## Contents

1 How Many IPsec VPNs Can I Have? ................................................................. 1
2 Do IPsec VPNs Support Automatic Negotiation? ........................................... 2
3 What Are the Reference Standards and Protocols for the IPsec VPN? .................... 3
4 What Do I Do If VPN Connection Setup Fails? .............................................. 4
5 How Can I Handle the Failure in Accessing the ECSs from My Data Center or LAN Even If the VPN Has Been Set Up? .................................................. 5
6 What Do I Do If I Cannot Access My Data Center or LAN from the ECSs After a VPN Connection Has Been Set Up? .................................................. 6
7 Does a VPN Allow for Communication Between Two VPCs? ............................ 7
8 What Is the Limitation on the Number of Local and Remote Subnets of a VPN? .... 8
9 Why Is Not Connected Displayed as the Status for a Successfully Created VPN? .... 9
10 How Long Is Required for Issued VPN Configurations to Take Effect? ............... 10
11 How Do I Configure a Remote Device for a VPN? .......................................... 11
12 Which Remote VPN Devices Are Supported? ................................................. 13
13 What Can I Do If the VPN Connection Fails or the Network Speed of the VPN Connection Is Slow? .............................................................. 14
14 Are SSL VPNs Supported? ............................................................................ 15
15 What Is the VPN Quota? .............................................................................. 16
1 How Many IPsec VPNs Can I Have?

By default, a user can have a maximum of two IPsec VPNs. If your quota cannot fulfill your service requirements, submit a service ticket to increase the quota.
Do IPsec VPNs Support Automatic Negotiation?

Yes. IPsec VPNs support automatic negotiation.
What Are the Reference Standards and Protocols for the IPsec VPN?

The following standards and protocols are associated with the IPsec VPN:

- RFC 4301: Security Architecture for the Internet Protocol
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2857: The Use of HMAC-RIPemd-160-96 within ESP and AH
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and its use with IPsec
- RFC 3625: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3748: Extensible Authentication Protocol (EAP)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2) Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4322: Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC 4359: The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478: Repeated Authentication in Internet Key Exchange (IKEv2)
- RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2)
What Do I Do If VPN Connection Setup Fails?

1. Log in to the management console and choose **Virtual Private Network > VPN Connections**.

2. In the VPN connection list, locate the target VPN connection and click **View Policy** in the **Operation** column to view IKE and IPsec policy details about the VPN connection.

3. Check the IKE and IPsec policies to see whether the negotiation modes and encryption algorithms between the local and remote sides of the VPN are the same.
   
   a. If the IKE policy has been set up during phase one and the IPsec policy has not been enabled in phase two, the IPsec policies between the local and remote sides of the VPN may be inconsistent.

   b. If the Cisco physical device is used at the customer side, it is recommended that you use MD5. Then, you need to set **Authentication Mode** to MD5 in the IPsec policy for the VPN created on the cloud.

4. Check whether the ACL configurations are correct.
   
   If the subnets of your 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 data center subnet to permit 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. After the configuration is complete, ping the local and the remote side from each other to check whether the VPN connection is normal.
5 How Can I Handle the Failure in Accessing the ECSs from My Data Center or LAN Even If the VPN Has Been Set Up?

The security group denies the access from all sources by default. If you want to access your ECSs, modify the security group configuration and allow the access from the remote subnets.
What Do I Do If I Cannot Access My Data Center or LAN from the ECSs After a VPN Connection Has Been Set Up?

Check whether you have properly configured the firewall policies for the access from the public IP address of the cloud VPN to the public IP address of your data center or LAN. No policies are configured to limit the access by default.
Does a VPN Allow for Communication Between Two VPCs?

If the two VPCs are in the same region, you can use a VPC peering connection to enable communication between them.

If the two VPCs are in different regions, you can use a VPN to enable communication between the VPCs. The CIDR blocks of the two VPCs are the local and remote subnets, respectively.
What Is the Limitation on the Number of Local and Remote Subnets of a VPN?

The maximum number obtained by multiplying the number of local subnets and that of remote subnets cannot exceed 225.
Why Is Not Connected Displayed as the Status for a Successfully Created VPN?

After a VPN is created, its status changes to Normal only after the VMs or physical servers on the two sides of the VPN communicate with each other.

- **IKE v1:**
  - If no traffic goes through the VPN for a period of time, the VPN needs to be renegotiated. The negotiation time depends on the value of Lifecycle (s) in the IPsec policy. Generally, the value of Lifecycle (s) is 3600 (1 hour), indicating that the negotiation will be initiated in the fifty-fourth minute. If the negotiation succeeds, the connection remains to the next round of negotiation. If the negotiation fails, the status is set to be disconnected within one hour. The connection can be restored after the two sides of the VPN communicates with each other. The disconnection can be avoided by using a network monitoring tool, such as IP SLA, to generate packets.

- **IKE v2:** If no traffic goes through the VPN for a period of time, the VPN remains in the connected status.
The time required for VPN configurations to take effect increases linearly with the number obtained by multiplying the number of local subnets and that of remote subnets.
Due to the symmetry of the tunnel, the VPN parameters configured on the cloud must be the same as those configured in your own data center. If they are different, a VPN cannot be established.

To set up a VPN, you also need to configure the IPsec VPN on the router or firewall in your own data center. The configuration method may vary depending on your network device in use. For details, see the configuration guide of your network device.

This section describes how to configure the IPsec VPN on a Huawei USG6600 series V100R001C30SPC300 firewall for your reference.

For example, the subnets of the data center are 192.168.3.0/24 and 192.168.4.0/24, the subnets of the 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 XXX.XXX.XXX.XXX, which can be obtained from the local gateway parameters of the IPsec VPN in the VPC.

### Procedure

1. Log in to the CLI of the firewall.
2. Check firewall version information.
   ```
   display version
   17:20:50 03/09
   Huawei Versatile Security Platform Software
   Software Version: USG6600 V100R001C30SPC300(VRP (R) Software, Version 5.30)
   ```
3. Create an access control list (ACL) and bind it to the target VPN instance.
   ```
   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
   ```
4. Create an IKE proposal.
   ```
   ike proposal 64
dh group5
   authentication-algorithm sha1
   integrity-algorithm hmac-sha2-256
   ```
5. Create an IKE peer and reference the created IKE proposal. The peer IP address is 93.188.242.110.

   ike peer vpnikepeer_64
   pre-shared-key ******** (******** specifies the pre-shared key.)
   undo version 2
   remote-address vpn-instance vpn64 93.188.242.110
   sa binding vpn-instance vpn64

6. Create an IPsec protocol.

   ipsec proposal ipsecpro64
   encapsulation-mode tunnel
   esp authentication-algorithm sha1

7. Create an IPsec policy and reference the IKE policy and IPsec proposal.

   ipsec policy vpnipsec64 1 isakmp
   security acl 3065
   pfs dh-group5
   ike-peer vpnikepeer_64
   proposal ipsecpro64
   local-address xx.xx.xx.xx

8. Apply the IPsec policy to the subinterface.

   interface GigabitEthernet0/0/2.64
   ipsec policy vpnipsec64

9. Test the connectivity.

   After you perform the preceding operations, you can test the connectivity between your ECSs in the cloud and the hosts in your data center. For details, see the following figure.
Most devices that meet IPsec VPN standard and reference protocol requirements can be used as the remote VPN devices, for example, Cisco ASA firewalls, Huawei USG6xxx series firewalls, USG9xxx series firewalls, Hillstone firewalls, and Cisco ISR routers. Table 12-1 lists the supported Huawei USG6xxx and USG9xxx firewalls.

**Table 12-1 Huawei VPN devices**

<table>
<thead>
<tr>
<th>Supported Remote VPN Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huawei USG6000 series</td>
<td>USG6320/6310/6510-SJJ</td>
</tr>
<tr>
<td></td>
<td>USG6306/6308/6330/6350/6360/6370/6380/6390/6507/6530/6550/6570/2048</td>
</tr>
<tr>
<td></td>
<td>USG6620/6630/6650/6660/6670/6680</td>
</tr>
<tr>
<td>Huawei USG9000 series</td>
<td>USG9520/USG9560/USG9580</td>
</tr>
</tbody>
</table>

Other devices that meet the requirements in the reference protocols described in section 3 *What Are the Reference Standards and Protocols for the IPsec VPN?* can also be deployed. However, some devices may fail to add because of inconsistent protocol implementation methods of these devices. If the connection setup fails, rectify the fault by following the instructions provided in section 4 *What Do I Do If VPN Connection Setup Fails?* or contact customer service.
What Can I Do If the VPN Connection Fails or the Network Speed of the VPN Connection Is Slow?

You can perform the following steps to handle the issues:

1. Check the ECS specifications. Rate limiting is not performed for the VPN ingress on the cloud, so the issue may be caused by the ECS specifications.
2. Rate limiting has been configured for the VPN egress on the cloud. Check whether your bandwidth has reached or exceeded the maximum limit allowed.
3. Check your local network to see whether the network speed is slow.
4. Check whether packets sent between the two sides of the VPN have been lost.
14 Are SSL VPNs Supported?

Currently, the VPN service does not support the SSL VPNs. If you need an SSL VPN, you can buy the image for the SSL VPN in the HUAWEI CLOUD Marketplace.
What Is a Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users. For example, the VPN quotas limit the number of VPN gateways and VPN connections that you can create. You can also request more quotas if you need them.

This section describes how to view the VPN resource usage and the total quotas in a specified region.

How Do I View My Quota?

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose Resources > My Quota.
   The Service Quota page is displayed.

   **Figure 15-1 My Quota**

4. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, click Increase Quota to adjust it.
How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose Resources > My Quota.
   The Service Quota page is displayed.

   **Figure 15-2** My Quota

   ![My Quota](image)

3. Click Increase Quota.
4. On the Create Service Ticket page, configure parameters as required.
   In Problem Description area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select I have read and agree to the Tenant Authorization Letter and Privacy Statement and click Submit.