Virtual Private Network

User Guide

Date 2019-02-22
## 5.7 Does a VPN Allow for Communication Between Two VPCs?

5.8 What Is the Limitation on the Number of Local and Remote Subnets of a VPN?

5.9 Why Is Not Connected Displayed as the Status for a Successfully Created VPN?

5.10 How Long Is Required for Issued VPN Configurations to Take Effect?

5.11 How Do I Configure a Remote Device for a VPN?

5.12 Which Remote VPN Devices Are Supported?

5.13 What Can I Do If the VPN Fails or the Network Speed of the VPN Is Slow?

5.14 Are SSL VPNs Supported?

### A Change History

---

2019-02-22
1.1 Virtual Private Network

A Virtual Private Network (VPN) establishes an encrypted communications tunnel between a user and a Virtual Private Cloud (VPC). With VPN, you can connect to a VPC and access service resources in it.

By default, ECSs in a VPC cannot communicate with your data center or private network. To enable communication between them, use a VPN connection.

1.2 IPsec VPN

The Internet Protocol Security (IPsec) VPN is an encrypted tunneling technology that uses encrypted security services to establish confidential and secure communication tunnels between different networks.

In the example shown in Figure 1-1, you have created a VPC that has two subnets, 192.168.1.0/24 and 192.168.2.0/24, on the cloud. You also have two subnets, 192.168.3.0/24 and 192.168.4.0/24 on your router deployed in your data center. In this case, you can create an IPsec VPN to enable communication between subnets in your VPC and those in your data center.

Currently, the site-to-site VPN and hub-spoke VPN are supported. You need to set up VPNs in both your data center and the VPC to establish the VPN connection.

You must ensure that the VPN in your VPC and that in your data center use the same Internet Key Exchange (IKE) and IPsec policy configurations. Before creating a VPN, familiarize yourself with the protocols described in Table 1-1 and ensure that your device meets the requirements and configuration constraints of the involved protocols.

Table 1-1 Involved protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
<th>Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2409</td>
<td>Defines the IKE protocol, which negotiates and verifies key information to safeguard VPN connections.</td>
<td>• Use the pre-shared key (PSK) to reach an IKE peer agreement. • Use the main mode for negotiation.</td>
</tr>
</tbody>
</table>
### Protocol Description

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
<th>Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 4301</td>
<td>Defines the IPsec architecture, the security services that IPsec offers, and the collaboration between components.</td>
<td>Set up a VPN connection using the IPsec tunnel.</td>
</tr>
</tbody>
</table>

#### Figure 1-1 IPsec VPN

![IPsec VPN Diagram](image1.png)

### 1.3 Application Scenarios

With the VPN between the VPC and your traditional data center, you can easily use the ECSs and block storage resources provided by the cloud platform. Applications can be migrated to the cloud and additional web servers can be deployed to increase the computing capacity on a network. In this way, a hybrid cloud is built, which reduces IT O&M costs and protects enterprise core data from being leaked.

The VPN service allows an IPsec VPN to be created between multiple local gateways in different VPCs and the same remote gateway.

#### Figure 1-2 VPN created between multiple local gateways and the same remote gateway

![VPN Diagram](image2.png)
As shown in Figure 1-2, two IPsec VPNs are created. One IPsec VPN is created between local gateway 1.1.1.1 and remote gateway 3.1.1.1. Local subnet Subnet1 (192.168.1.0/24) in VPC1 communicates with remote subnet (192.168.3.0/24) through this VPN. The other IPsec VPN is created between local subnet 2.1.1.1 and remote subnet 3.1.1.1. Local subnet Subnet2 (192.168.2.0/24) communicates with remote subnet (192.168.3.0/24) through this VPN. In this scenario, the IP addresses in subnets Subnet1 and Subnet2 cannot overlap.

1.4 VPN Reference Standards and Protocols

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)
2 Getting Started

2.1 Creating a VPC

Scenarios

A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

Create a VPC by following the procedure provided in this section. Then, create subnets, security groups, and VPNs, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
4. On the Dashboard page, click Create VPC.
5. On the Create VPC page, set parameters as prompted.
   During VPC creation, a default subnet will be created and you can also click Add Subnet to create more subnets for the VPC.

Table 2-1 VPC parameter description

<table>
<thead>
<tr>
<th>Category</th>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>Region</td>
<td>Specifies the desired region. Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.</td>
<td>eu-de</td>
</tr>
<tr>
<td>Basic Information</td>
<td>Name</td>
<td>Specifies the VPC name.</td>
<td>VPC-001</td>
</tr>
</tbody>
</table>
## Getting Started

<table>
<thead>
<tr>
<th>Category</th>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>CIDR Block</td>
<td>Specifies the CIDR block for the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset (for multiple subnets in the VPC). The following CIDR blocks are supported: 10.0.0.0 – 10.255.255.255 172.16.0.0 – 172.31.255.255 192.168.0.0 – 192.168.255.255</td>
<td>192.168.0.0/16</td>
</tr>
<tr>
<td>Basic Information</td>
<td>Tag</td>
<td>Specifies the VPC tag, which consists of a key and value pair. You can add a maximum of ten tags to each VPC. The tag key and value must meet the requirements listed in Table 2-2.</td>
<td>• Key: vpc_key1  • Value: vpc-01</td>
</tr>
<tr>
<td>Subnet Settings</td>
<td>Name</td>
<td>Specifies the subnet name.</td>
<td>Subnet</td>
</tr>
<tr>
<td>Subnet Settings</td>
<td>CIDR Block</td>
<td>Specifies the CIDR block for the subnet. This value must be within the VPC CIDR range.</td>
<td>192.168.0.0/24</td>
</tr>
<tr>
<td>Subnet Settings</td>
<td>Gateway</td>
<td>Specifies the gateway address of the subnet.</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>Subnet Settings</td>
<td>DNS Server Address</td>
<td>The external DNS server address is used by default. If you need to change the DNS server address, ensure that the configured DNS server address is available.</td>
<td>192.168.1.0</td>
</tr>
<tr>
<td>Subnet Settings</td>
<td>NTP Server Address</td>
<td>Specifies the NTP server IP address. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (.).</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>Subnet Settings</td>
<td>Tag</td>
<td>Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of ten tags to each subnet. The tag key and value must meet the requirements listed in Table 2-3.</td>
<td>• Key: subnet_key 1  • Value: subnet-01</td>
</tr>
</tbody>
</table>

### Table 2-2 VPC tag key and value requirements

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirements</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>• Cannot be left blank.</td>
<td>vpc_key1</td>
</tr>
</tbody>
</table>
### Table 2-3 Subnet tag key and value requirements

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirements</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
<td>• Cannot be left blank.</td>
<td>subnet_key1</td>
</tr>
<tr>
<td></td>
<td>• Must be unique for each subnet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can contain a maximum of 36 characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can contain only the following character types:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Uppercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Lowercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Digits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Special characters, including hyphens (−) and underscores (_)</td>
<td></td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>• Can contain a maximum of 43 characters.</td>
<td>subnet-01</td>
</tr>
<tr>
<td></td>
<td>• Can contain only the following character types:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Uppercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Lowercase letters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Digits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>− Special characters, including hyphens (−) and underscores (_)</td>
<td></td>
</tr>
</tbody>
</table>
6. The external DNS server address is used by default. If you need to change the DNS server address, select Custom for Advanced Settings and configure the DNS server addresses. You must ensure that the configured DNS server addresses are available.

7. Click Create Now.

2.2 Creating a Subnet for the VPC

Scenarios

You can add subnets during VPC creation. If required, you can also create subnets for an existing VPC.

The created subnet is configured with DHCP by default. After an ECS using this VPC starts, the ECS automatically obtains an IP address using DHCP.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. In the navigation pane on the left, click Virtual Private Cloud.
5. On the Virtual Private Cloud page, locate the VPC for which a subnet is to be created and click the VPC name.
6. On the displayed Subnets tab, click Create Subnet.
7. In the Create Subnet area, set parameters as prompted.

Figure 2-1 Create Subnet

<table>
<thead>
<tr>
<th>Create Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>CIDR Block</strong></td>
</tr>
</tbody>
</table>

Available CIDR Block: 192.168.0.0/16
Available IP Addresses: 256
The CIDR block cannot be modified after the subnet has been created.

Advanced Settings: Default, Custom

OK, Cancel

Table 2-4 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the subnet name.</td>
<td>Subnet</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>CIDR Block</td>
<td>Specifies the CIDR block for the subnet. This value must be within the VPC CIDR range.</td>
<td>192.168.0.0/24</td>
</tr>
<tr>
<td>Gateway</td>
<td>Specifies the gateway address of the subnet.</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>NTP Server Address</td>
<td>Specifies the NTP server IP address. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</td>
<td>192.168.2.1</td>
</tr>
</tbody>
</table>
| Tag                  | Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of ten tags to each subnet. The tag key and value must meet the requirements listed in Table 2-5. | • Key: subnet_key1  
• Value: subnet-01 |
| DNS Server Address   | The external DNS server address is used by default. If you need to change the DNS server address, ensure that the configured DNS server address is available. | 192.168.1.0   |

**Table 2-5 Subnet tag key and value requirements**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirements</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Key       | • Cannot be left blank.  
• Must be unique for each subnet.  
• Can contain a maximum of 36 characters.  
• Can contain only the following character types:  
  − Uppercase letters  
  − Lowercase letters  
  − Digits  
  − Special characters, including hyphens (-) and underscores (_) | subnet_key1 |
| Value     | • Can contain a maximum of 43 characters.  
• Can contain only the following character types:  
  − Uppercase letters  
  − Lowercase letters  
  − Digits  
  − Special characters, including hyphens (-) and underscores (_) | subnet-01 |
8. The external DNS server address is used by default. If you need to change the DNS server address, select **Custom** for **Advanced Settings** and configure the DNS server addresses. You must ensure that the configured DNS server addresses are available.

9. Click **OK**.

**Precautions**

After a subnet is created, five IP addresses in the subnet will be reserved and cannot be used. For example, in a subnet with CIDR block 192.168.0.0/24, the following IP addresses are reserved:

- 192.168.0.0: Network address.
- 192.168.0.1: Gateway address.
- 192.168.0.253: Reserved for the system interface. This IP address is used by the VPC for external communication.
- 192.168.0.254: DHCP service address.
- 192.168.0.255: Network broadcast address.

If you set **Advanced Settings** to **Custom** during subnet creation, the reserved IP addresses may be different from the preceding default ones. The system will reserve five IP addresses based on your subnet settings.

**2.3 Creating a VPN**

**Overview**

By default, ECSs in a VPC cannot communicate with your data center or private network. To enable communication between them, use a VPN. You need to create a VPN in your VPC and update the security group rules.

**Description of a Simple IPsec VPN Intranet Topology**

In Figure 2-2, a VPC has two subnets: 192.168.1.0/24 and 192.168.2.0/24. On your router deployed in your physical data center, you also have two subnets: 192.168.3.0/24 and 192.168.4.0/24. You can create a VPN to enable subnets in your VPC to communicate with those in your data center.
Currently, the site-to-site VPN and hub-spoke VPN are supported. You need to set up VPNs in both your data center and the VPC to establish the VPN connection.

Ensure that the VPN in your VPC and that in your data center use the same Internet Key Exchange (IKE) and IPsec policy configurations. Before creating a VPN, familiarize yourself with the protocols described in Table 2-6 and ensure that your device meets the requirements and configuration constraints of the involved protocols.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2409</td>
<td>Defines the IKE protocol, which negotiates and verifies key information to safeguard VPNs.</td>
<td>• Use the pre-shared key (PSK) to reach an IKE peer agreement. • Use the main mode and aggressive mode for negotiation.</td>
</tr>
<tr>
<td>RFC 4301</td>
<td>Defines the IPsec architecture, the security services that IPsec offers, and the collaboration between components.</td>
<td>Use the IPsec tunnel to set up a VPN.</td>
</tr>
</tbody>
</table>

**Scenarios**

Perform the following procedure to create a VPN that sets up a secure, isolated communication tunnel between your data center and cloud services.

**Procedure**

1. Log in to the management console.
2. Click in the upper left corner and select a region and project.
3. On the console homepage, under **Network**, click **Virtual Private Network**.
4. On the **Virtual Private Network** page, click **Create VPN**.

5. Set the parameters as prompted and click **Create Now**.

**Figure 2-3 Creating a VPN**

**Table 2-7 Basic parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>Specifies the desired region. Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.</td>
<td>eu-de</td>
</tr>
<tr>
<td>VPC</td>
<td>Specifies the VPC name.</td>
<td>VPC-001</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the VPN name.</td>
<td>VPN-001</td>
</tr>
<tr>
<td>PSK</td>
<td>Specifies the pre-shared key. The value is a string of 6 to 128 characters. This parameter value must be the same for the VPN in the VPC and that in the data center.</td>
<td>Test@123</td>
</tr>
<tr>
<td>Confirm PSK</td>
<td>Specifies the confirm pre-shared key.</td>
<td>Test@123</td>
</tr>
</tbody>
</table>
| Tag        | Specifies the VPN tag, which consists of a key and value pair. You can add a maximum of ten tags to each VPN. The tag key and value must meet the requirements listed in Table 2-8. | Key: vpn_key1  
Value: vpn-01  |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Local Subnet    | Specifies the VPC subnets or CIDR blocks that need to communicate with your data center or private network.  
- **Select subnet**: If you select this option, you can then select the subnets that need to communicate with your data center.  
- **Specify CIDR block**: If you select this option, you can then enter the CIDR blocks that need to communicate with your data center. | 192.168.1.0/24, 192.168.2.0/24 |
| Remote Gateway  | Specifies the public IP address of the VPN in your data center or on the private network. This IP address is used for communicating with the VPN in the VPC.                                                    | N/A                           |
| Remote Subnet   | Specifies the subnets of your data center or private network for communicating with the VPC. The remote and local subnets cannot have overlapping or matching CIDR blocks. The remote subnet CIDR block cannot overlap with CIDR blocks involved in existing VPC peering connections created for the local VPC. | 192.168.3.0/24, 192.168.4.0/24 |
| Advanced Settings|  
- **Default**: uses default IKE and IPsec policies.  
- **Existing**: uses existing IKE and IPsec policies. This option is available only after you have created IKE and IPsec policies.  
- **Custom**: uses custom IKE and IPsec policies. For details about the policies, see Table 2-9 and Table 2-10. | Custom                        |

**Table 2-8 VPN tag key and value requirements**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- Cannot be left blank.  
- Must be unique for the same VPN and can be the same for different VPNs.  
- Contains a maximum of 36 characters.  
- Can contain only the following character types: | vpn_key1       |
### Parameter | Requirement | Example Value
--- | --- | ---
Value | Can contain a maximum of 43 characters. Can contain only the following character types: - Uppercase letters - Lowercase letters - Digits - Special characters, including hyphens (-) and underscores (_) | vpn-01

Table 2-9 IKE policy

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Algorithm</td>
<td>Specifies the authentication hash algorithm. The value can be SHA1, SHA2-256, SHA2-384, SHA2-512, or MD5.</td>
<td>SHA1</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>Specifies the encryption algorithm. The value can be AES-128, AES-192, AES-256, or 3DES. The 3DES algorithm is not recommended because it is risky.</td>
<td>AES-128</td>
</tr>
<tr>
<td>DH Algorithm</td>
<td>Specifies the Diffie-Hellman key exchange algorithm. The value can be Group 1, Group 2, Group 5, Group 14, Group 15, Group 16, Group 19, Group 20, or Group 21. The DH group security level from the highest to lowest is as follows: Group 21 &gt; Group 20 &gt; Group 19 &gt; Group 16 &gt; Group 15 &gt; Group 14 &gt; Group 5 &gt; Group 2 &gt; Group 1.</td>
<td>Group 5</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the version of the IKE protocol. The value can be v1 or v2.</td>
<td>v1</td>
</tr>
<tr>
<td>Lifecycle (s)</td>
<td>Specifies the lifetime of the security association (SA), in seconds. The SA will be renegotiated if its lifetime expires.</td>
<td>86400</td>
</tr>
<tr>
<td>Negotiation Mode</td>
<td>If the IKE policy version is v1, the negotiation mode can be configured. The value can only be Main.</td>
<td>Main</td>
</tr>
</tbody>
</table>
Table 2-10 IPsec policy

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Algorithm</td>
<td>Specifies the authentication hash algorithm. The value can be SHA1, SHA2-256, SHA2-384, SHA2-512, or MD5.</td>
<td>SHA1</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>Specifies the encryption algorithm. The value can be AES-128, AES-192, AES-256, or 3DES. The 3DES algorithm is not recommended because it is risky.</td>
<td>AES-128</td>
</tr>
<tr>
<td>PFS</td>
<td>Specifies the perfect forward secrecy (PFS), which is used to configure the IPsec tunnel negotiation. This function enables two parties to exchange the DH keys during the phase-two negotiation, improving key security. It is recommended that you enable this function. You can disable this function by selecting Disable from the drop-down list. The PFS used at the two sides of a VPN must be the same. Otherwise, the negotiation will fail. If you disable this function on the console, you also need to disable it at the remote side of the VPN. The value can be DH group 1, DH group 2, DH group 5, DH group 14, DH group 15, DH group 16, DH group 19, DH group 20, or DH group 21. The PFS group security level from the highest to lowest is as follows: DH group 21 &gt; DH group 20 &gt; DH group 19 &gt; DH group 16 &gt; DH group 15 &gt; DH group 14 &gt; DH group 5 &gt; DH group 2 &gt; DH group 1.</td>
<td>DH group 5</td>
</tr>
<tr>
<td>Transfer Protocol</td>
<td>Specifies the security protocol used for IPsec to transmit and encapsulate user data. The value can be AH, ESP, or AH-ESP.</td>
<td>ESP</td>
</tr>
<tr>
<td>Lifecycle (s)</td>
<td>Specifies the lifetime of the SA, in seconds. The SA will be renegotiated if its lifetime expires.</td>
<td>3600</td>
</tr>
</tbody>
</table>
**NOTE**
The IKE policy specifies the encryption and authentication algorithms to use in the negotiation phase of an IPsec tunnel. The IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to use in the data transmission phase of an IPsec tunnel. These parameters must be the same between the VPN in your VPC and that in your data center. If they are different, the VPN cannot be set up.

6. Click **Submit**.

After the IPsec VPN is created, a public network egress IP address is assigned to the IPsec VPN. The IP address is the local gateway address of a created VPN on the network console. When configuring the remote tunnel in your data center, you must set the remote gateway address to this IP address.

**Figure 2-4** Gateway egress IP address

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>VPC</th>
<th>Local Gateway</th>
<th>Local Subnet</th>
<th>Remote Gateway</th>
<th>Remote Subnet</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn-abcd</td>
<td>Not cr</td>
<td>ident1</td>
<td>45.29.100.63</td>
<td>172.16.25.0/24</td>
<td>192.168.0.24</td>
<td>192.168.0.24</td>
<td>View Policy</td>
</tr>
</tbody>
</table>

7. Due to the symmetry of the tunnel, you also need to configure the IPsec VPN on your router or firewall in the data center.
   - For details about the VPN configuration, see 5.11 How Do I Configure a Remote Device for a VPN?.
   - For a list of protocols supported by VPN connections, see 5.3 What Are the Reference Standards and Protocols for the IPsec VPN?.
   - For a list of supported VPN devices, see 5.12 Which Remote VPN Devices Are Supported?.

### 2.4 Configuring Security Group Policies

#### 2.4.1 Creating a Security Group

**Scenarios**

To improve ECS access security, you can create a security group, define security group rules, and add ECSs in the VPC to the security group. We recommend that you allocate ECSs that have different Internet access policies to different security groups.

**Procedure**

1. Log in to the management console.
2. Click 🗺 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control > Security Groups**.
5. On the **Security Groups** page, click **Create Security Group**.
6. In the **Create Security Group** area, set the parameters as prompted. Table 2-11 lists the parameters to be configured.
Table 2-11 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the security group name. This parameter is mandatory. The security group name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces. <strong>NOTE</strong> You can change the security group name after a security group is created. It is recommended that you use different names for different security groups.</td>
<td>sg-318b</td>
</tr>
<tr>
<td>Description</td>
<td>Provides supplementary information about the security group. This parameter is optional. The security group description can contain a maximum of 255 characters and cannot contain angle brackets (&lt; or &gt;).</td>
<td>N/A</td>
</tr>
</tbody>
</table>

7. Click OK.
2.4.2 Adding a Security Group Rule

Scenarios

After a security group is created, you can add rules to the security group. A rule applies either to inbound traffic (ingress) or outbound traffic (egress). After ECSs are added to the security group, they are protected by the security group rules.

- Inbound rules control incoming traffic to ECSs associated with the security group.
- Outbound rules control outgoing traffic from ECSs associated with the security group.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
4. In the navigation pane on the left, choose Access Control > Security Groups.
5. On the Security Groups page, locate the target security group and click Manage Rule in the Operation column to switch to the page for managing inbound and outbound rules.
6. On the inbound rule tab, click Add Rule. In the displayed dialog box, set required parameters to add an inbound rule.
   You can click + to add more inbound rules.

![Figure 2-6 Add Inbound Rule](image)

Table 2-12 Inbound rule parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Specifies the network protocol. Currently, the value can be All, TCP, UDP, ICMP, GRE, or others.</td>
<td>TCP</td>
</tr>
<tr>
<td>Port &amp; Port</td>
<td>specifies the port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.</td>
<td>22 or 22-30</td>
</tr>
</tbody>
</table>
7. On the outbound rule tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.
   You can click + to add more outbound rules.

**Figure 2-7 Add Outbound Rule**

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td><strong>Source</strong>: specifies the source of the security group rule. The value can be another security group, a CIDR block, or a single IP address. Example: xxx.xxx.xxx.xxx/32 (IPv4 address) xxx.xxx.xxx.0/24 (subnet) 0.0.0.0/0 (any IP address)</td>
<td>0.0.0.0/0 default</td>
</tr>
<tr>
<td>Description</td>
<td>Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (&lt; or &gt;).</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Specifies the network protocol. Currently, the value can be <strong>All</strong>, <strong>TCP</strong>, <strong>UDP</strong>, <strong>ICMP</strong>, <strong>GRE</strong>, or others.</td>
<td>TCP</td>
</tr>
<tr>
<td>Port &amp; Destination</td>
<td><strong>Port</strong>: specifies the port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535. <strong>Destination</strong>: specifies the destination of the security group rule. The value can be another security group, a CIDR block, or a single IP address. Example:</td>
<td>22 or 22-30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.0.0.0/0 default</td>
</tr>
</tbody>
</table>
### 2.4.3 Deleting a Security Group Rule

#### Scenarios

If the source of an inbound security group rule or destination of an outbound security group rule needs to be changed, you can first delete the security group rule and add a new one.

> **NOTE**  
Security group rules use the whitelist mechanism. After security group rules are deleted, ECS access failures may occur. You must exercise caution when deleting security group rules.

#### Procedure

1. Log in to the management console.
2. Click ⚡ in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control > Security Groups**.
5. On the **Security Groups** page, click the security group name.
6. If you do not need a security group rule, locate the row that contains the target rule, and click **Delete**.
7. Click Yes in the displayed dialog box.

**Delete Multiple Security Group Rules at a Time.**

You can also select multiple security group rules and click **Delete** above the security group rule list to delete multiple rules at a time.
3.1 Configuring the Remote Device for a VPN

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.

The following sections use Huawei USG6600 series V100R001C30SPC300 and Cisco 2900 series 15.0 firewalls as examples to describe how to configure the remote device for a VPN.

3.2 Configuring the VPN on a Cisco 2900 Firewall

This section describes how to configure the IPsec VPN on a Cisco 2900 series 15.0 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 93.188.242.110, 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. Configure the Internet Security Association and Key Management Protocol (ISAKMP) policy.
   
   ```
   crypto isakmp policy 1
   authentication pre-share
   encryption aes 256
   hash sha
   group 5
   lifetime 3600
   ```
3. Configure the pre-shared key.
   
   ```
   crypto isakmp key ******* address 93.188.242.110 (******* indicates the pre-shared key.)
   ```
4. Configure the IPsec security protocol.

```plaintext
crypto ipsec transform-set ipsecpro64 esp-aes 256 esp-sha-hmac
mode tunnel
```

5. Configure an ACL and define the data flow to be protected.

```plaintext
access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 100 permit ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 100 permit ip 192.168.4.0 0.0.0.255 192.168.2.0 0.0.0.255
```

6. Configure the IPsec policy.

```plaintext
crypto map vnpip64 10 ipsec-isakmp
set peer 93.188.242.110
set transform-set ipsecpro64
set pfs group5
match address 100
```

7. Apply the IPsec policy on the target interface.

```plaintext
interface g0/0
crypto map vnpip64
```

8. 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.

```
3.3 Configuring the VPN on a Huawei USG6600 Series Firewall

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 93.188.242.110, which can be obtained from the local gateway parameters of the IPsec VPN in the VPC.

**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 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
   sa duration 3600
   ```
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.)
   ike-proposal 64
   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.

3.4 Viewing a VPN

Scenarios

You can view details about an existing VPN.

Procedure

1. Sign up and log in to the management console.
2. Click in the upper left corner and select a region and project.
4. On the displayed Virtual Private Network page, view the target VPN. Table 3-1 describes the VPN status.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Indicates that the VPN is successfully created and communication with the local data center through the VPN is normal.</td>
</tr>
<tr>
<td>Not connected</td>
<td>Indicates that the VPN is successfully created but has not been used for communication with the local data center.</td>
</tr>
<tr>
<td>Creating</td>
<td>Indicates that the VPN is being created.</td>
</tr>
</tbody>
</table>

```
root@psl-benh:/home/ubuntu# ifconfig
eth0 Link encap:Ethernet  HWaddr 52:54:70:ba:bf:dc
inet addr:192.168.3.2  Bcast:192.168.3.255  Mask:255.255.255.0
inet addr:fe80::200:97ff:feba:bfcc/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:128 errors:0 dropped:0 overruns:0 frame:0
TX packets:174 errors:0 dropped:0 overruns:0 carrier:0
collisions:0  txqueuelen:1000
RX bytes:86956 (85.84 KB)  TX bytes:86956 (85.84 KB)

root@psl-benh:/home/ubuntu# ping 192.168.1.2
PING 192.168.1.2 (192.168.12.1): 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=62 time=4.55 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=62 time=4.27 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=62 time=4.28 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=62 time=4.24 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=62 time=4.21 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=62 time=4.23 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=62 time=4.21 ms
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6000ms
rtt min/avg/max/mdev = 0.676/4.554/4.554/1.250 ms
```
### 3.5 Modifying a VPN

#### Scenarios

If the VPN network information conflicts the VPC network information or you need to adjust VPN configurations, you can modify a VPN.

#### Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select a region and project.
3. On the console homepage, under **Network**, click **Virtual Private Network**.
4. On the **Virtual Private Network** page, locate the target VPN and click **Modify**.
5. In the displayed dialog box, set parameters as prompted.

![Figure 3-1 Modifying a VPN](image)

6. Click **OK**.
3.6 Deleting a VPN

Scenarios

You can delete a VPN to release network resources if the VPN is no longer required.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select a region and project.
4. On the Virtual Private Network page, locate the target VPN and click Delete.
5. Click Yes in the displayed dialog box.

3.7 Managing VPN Tags

Application Scenarios

A VPN tag identifies a VPN. Tags can be added to VPNs to facilitate VPN identification and administration. You can add a tag to a VPN when creating the VPN. Alternatively, you can add a tag to a created VPN on the VPN details page. A maximum of ten tags can be added to each VPN.

A tag consists of a key and value pair. Table 3-2 lists the tag key and value requirements.

Table 3-2 VPN tag key and value requirements

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
</table>
| Key       | • Cannot be left blank.  
           | • Must be unique for the same VPN and can be the same for different VPNs.  
           | • Contains a maximum of 36 characters.  
           | • Can contain only the following character types:  
           |   - Uppercase letters  
           |   - Lowercase letters  
           |   - Digits  
           |   - Special characters, including hyphens (-) and underscores (_) | vpn_key1 |
| Value     | • Can contain a maximum of 43 characters.  
           | • Can contain only the following character types:  
           |   - Uppercase letters  
           |   - Lowercase letters  
<pre><code>       |   - Digits | vpn-01 |
</code></pre>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Requirement</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>− Special characters, including hyphens (-) and underscores (_)</td>
<td></td>
</tr>
</tbody>
</table>

## Procedure

### Search for VPNs by Tag Key and Value on the Page Showing the VPN List.

1. Log in to the management console.
2. Click  in the upper left corner and select a region and project.
4. In the upper right corner of the VPN list, click Search by Tag.
5. In the displayed area, enter the tag key and value of the VPN you are looking for. Both the tag key and value must be specified.
6. Click + to add the entered tag key and value. You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for VPCs, the VPCs containing all specified tags will be displayed.
7. Click Search. The system displays the VPNs you are looking for based on the entered tag keys and values.

### Add, Delete, Edit, and View Tags on the Tags Tab of a VPN.

1. Log in to the management console.
2. Click  in the upper left corner and select a region and project.
4. On the Virtual Private Network page, locate the VPN whose tags are to be managed and click the VPN name.
   The page showing details about the particular VPN is displayed.
5. Click the Tags tab and perform desired operations on tags.
   − View tags. On the Tags tab, you can view details about tags added to the current VPN, including the number of tags and the key and value of each tag.
   − Add a tag. Click Add Tag in the upper left corner. In the displayed dialog box, enter the key and value of the tag to be added, and click OK.
   − Edit a tag. Locate the row that contains the tag to be edited and click Edit in the Operation column. In the Edit Tag dialog box, change the tag value and click OK.
   − Delete a tag. Locate the row that contains the tag to be deleted, and click Delete in the Operation column. In the displayed Delete Tag dialog box, click Yes.
4 VPN Best Practice

4.1 Connecting to a VPC Through a VPN

Scenarios

By default, ECSs in a VPC cannot communicate with your data center or private network. To enable communication between them, use a VPN. After a VPN is created, configure the security group and check the connectivity between the local and remote networks to ensure that the VPN is available. VPNs can be classified into the following two types:

- **Site-to-site VPN**: The local side is a VPC on the public cloud platform, and the remote side is the user data center. A site-to-site VPN establishes a communication tunnel between a user data center and a single VPC.

- **Hub-and-spoke VPN**: The local side is multiple VPCs on the public cloud platform, and the remote side is the user data center. A hub-and-spoke VPN establishes a communication tunnel between a user data center and multiple VPCs.

Ensure that the following requirements are met when configuring a VPN:

- The local and remote subnets cannot overlap.
- Different local subnets cannot overlap.
- The local and remote sides use the same IKE policy.
- The local and remote sides use the same IPsec policy.
- The local and remote subnet and gateway parameters must be symmetric.
- The local and remote sides use the same PSK.
- The security group used by ECSs in the VPC allows traffic from and to the remote side.
- 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.

Prerequisites

You have created the VPC and subnet required by the VPN.

Procedure

1. On the management console, select the appropriate IKE and IPsec policies to create a VPN.
2. Check the IP address pools for the local and remote subnets.
In Figure 4-1, a VPC has two subnets: 192.168.1.0/24 and 192.168.2.0/24. On your router deployed in your physical data center, you also have two subnets: 192.168.3.0/24 and 192.168.4.0/24. You can create a VPN to enable subnets in your VPC to communicate with those in your data center.

**Figure 4-1 IPsec VPN**

The IP address pools for the local and remote subnets cannot overlap with each other. For example, if the local VPC has two subnets, 192.168.1.0/24 and 192.168.2.0/24, the IP address pool for the remote subnets cannot contain these two subnets.

3. Configure security group rules for the VPC.

4. Check the security group of the VPC.

   The security group must allow packets from the VPN to pass. You can run the `ping` command to check whether the security group of the VPC allows packets from the VPN to pass.

5. Check the remote LAN configuration (network configuration of the remote data center).

   A route must be configured for the remote LAN to enable VPN traffic to be forwarded to network devices on the LAN. If the VPN traffic cannot be forwarded to the network devices, check whether the remote LAN has policies configured to refuse the traffic.
5.1 How Many IPsec VPNs Can I Have?
By default, a user can have a maximum of five IPsec VPNs. If your quota cannot fulfill your service requirements, submit a service ticket to increase the quota.

5.2 Do IPsec VPNs Support Automatic Negotiation?
The IPsec VPN tunnel works in passive mode, which triggers automatic negotiation only when traffic sent by the local end passes through the tunnel.

5.3 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
5.4 What Do I Do If VPN Setup Fails?

1. Log in to the management console and click **Virtual Private Network**.
2. In the VPN list, locate the target VPN and click **View Policy** in the **Operation** column to view IKE and IPsec policy details about the VPN.
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.

5.5 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.
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?

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.

5.7 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.

5.8 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 2500.

5.9 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.
5.10 How Long Is Required for Issued VPN Configurations to Take Effect?

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.

5.11 How Do I Configure a Remote Device for a VPN?

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.XX.XX, 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
   17:20:502017/03/09
   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
   sa duration 3600
   ```
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.)
   ike-proposal 64
5. Create an IPsec protocol.

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

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

```plaintext
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.

```plaintext
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.

---

5.12 Which Remote VPN Devices Are Supported?

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 5-1 lists the supported Huawei USG6xxx and USG9xxx firewalls.

Table 5-1 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>USG6306/6308/6330/6350/6350/6360/6370/6380/6390/6507/6530/6550/6570:2048</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 5.3 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 5.4 What Do I Do If VPN Setup Fails? or contact customer service.

5.13 What Can I Do If the VPN Fails or the Network Speed of the VPN 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.

5.14 Are SSL VPNs Supported?

Currently, the VPN service does not support the SSL VPNs.
## Change History

<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
</table>
| 2019-02-22   | This release incorporates the following changes:  
Updated the region description in Table 2-7. |
| 2019-02-18   | Accepted in OTC-4.0/Agile-02.2019 |
| 2019-02-11   | This release incorporates the following changes:  
- Deleted content about the firewall version from section 2.3 Creating a VPN.  
- Added Table 3-1.  
- Updated the tag key and value requirements in Table 2-8 and Table 3-2.  
- Updated content about searching for VPNs by tag key and value in section 3.7 Managing VPN Tags.  
- Adjusted the column width. |
| 2019-02-02   | This release incorporates the following changes:  
- Updated a figure in section 3.5 Modifying a VPN.  
- Updated the content in section 3.7 Managing VPN Tags based on the latest console page.  
- Updated section 2.4 Configuring Security Group Policies.  
- Updated sections 5.9 Why Is Not Connected Displayed as the Status for a Successfully Created VPN? and 5.11 How Do I Configure a Remote Device for a VPN?.  
- Added the negotiation mode in section Table 2-9. |
| 2019-01-30   | This release incorporates the following changes:  
- Added parameter **NTP Server Address** to section Table 2-1.  
- Sorted the DH algorithm values to display them in order in section Table 2-9.  
- Sorted the PFS values to display them in order in section Table 2-10.  
- Added description to show how to query the firewall |
<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>version in section 5.</td>
</tr>
<tr>
<td></td>
<td>• Added the supported network protocols to the tables listing inbound and outbound rules in section 2.4.2 Adding a Security Group Rule.</td>
</tr>
<tr>
<td></td>
<td>• Modified the description of parameter Port &amp; Source in the tables listing inbound and outbound rules in section 2.4.2 Adding a Security Group Rule.</td>
</tr>
<tr>
<td></td>
<td>• Added section 3.3 Configuring the VPN on a Huawei USG6600 Series Firewall.</td>
</tr>
<tr>
<td>2019-01-23</td>
<td>This release incorporates the following changes:</td>
</tr>
<tr>
<td></td>
<td>• Changed VPN connection to VPN.</td>
</tr>
<tr>
<td></td>
<td>• Changed OK to Yes in section 3.6 Deleting a VPN.</td>
</tr>
<tr>
<td></td>
<td>• Updated figures in sections Figure 2-3, Figure 2-4, and Figure 3-1.</td>
</tr>
<tr>
<td></td>
<td>• Modified the title in sections 3.4 Viewing a VPN and 3.5 Modifying a VPN.</td>
</tr>
<tr>
<td></td>
<td>• Added parameter Region and option Specify CIDR block to parameter Local Subnet in section Table 2-7.</td>
</tr>
<tr>
<td></td>
<td>• Added description about the DH group security level and description about the supported DH groups when the firewall version is V1 or V5 to section Table 2-9.</td>
</tr>
<tr>
<td></td>
<td>• Added description about the PFS group security level and description about the supported DH groups when the firewall version is V1 or V5 to section Table 2-10.</td>
</tr>
<tr>
<td></td>
<td>• Updated section 5.4 What Do I Do If VPN Setup Fails?.</td>
</tr>
<tr>
<td></td>
<td>• Added sections 5.13 What Can I Do If the VPN Fails or the Network Speed of the VPN Is Slow? and 5.14 Are SSL VPNs Supported?.</td>
</tr>
<tr>
<td>2019-01-02</td>
<td>This release incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>Added description about the PFS function to the section for configuring the IPsec policy of a VPN.</td>
</tr>
<tr>
<td>2018-04-30</td>
<td>This issue is the eighth official release, which incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>Added description about how to add tags during VPN creation.</td>
</tr>
<tr>
<td>2017-08-30</td>
<td>This issue is the seventh official release, which incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>Added description about VPC and subnet tags.</td>
</tr>
<tr>
<td>2017-07-30</td>
<td>This issue is the sixth official release, which incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added the best practice.</td>
</tr>
<tr>
<td></td>
<td>• Added description about the multi-project feature.</td>
</tr>
<tr>
<td>2017-04-28</td>
<td>This issue is the fifth official release, which incorporates the following change:</td>
</tr>
<tr>
<td>Release Date</td>
<td>What's New</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Changed the maximum number obtained by multiplying the number of local subnets and that of remote subnets of a VPN to <strong>2500</strong>.</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>This issue is the fourth official release, which incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added an example illustrating how to configure the remote device of a VPN.</td>
</tr>
<tr>
<td>2017-01-20</td>
<td>This issue is the third official release, which incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added description about the IPsec VPN created between multiple local gateways in different VPCs and the same remote gateway</td>
</tr>
<tr>
<td>2016-12-30</td>
<td>This issue is the second official release, which incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added FAQs.</td>
</tr>
<tr>
<td>2016-10-19</td>
<td>This issue is the first official release.</td>
</tr>
</tbody>
</table>