

# Virtual Private Network

## User Guide

**Issue** 01  
**Date** 2023-10-20



**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 Enterprise Edition VPN Gateway Management.....</b>  | <b>1</b>  |
| 1.1 Creating a VPN Gateway.....  | 1         |
| 1.2 Viewing a VPN Gateway.....   | 8         |
| 1.3 Modifying a VPN Gateway.....   | 9         |
| 1.4 Binding an EIP to a VPN Gateway.....   | 9         |
| 1.5 Unbinding an EIP from a VPN Gateway.....   | 10        |
| 1.6 Unsubscribing from a Yearly/Monthly VPN Gateway.....   | 10        |
| 1.7 Renewing a Yearly/Monthly VPN Gateway.....   | 11        |
| 1.8 Deleting a Pay-per-Use VPN Gateway.....  | 11        |
| <b>2 Customer Gateway Management of Enterprise Edition VPN.....</b>                              | <b>13</b> |
| 2.1 Creating a Customer Gateway.....   | 13        |
| 2.2 Viewing a Customer Gateway.....  | 15        |
| 2.3 Modifying a Customer Gateway.....  | 15        |
| 2.4 Deleting a Customer Gateway.....   | 15        |
| <b>3 Enterprise Edition VPN Connection Management.....</b>                                       | <b>17</b> |
| 3.1 Creating a VPN Connection.....   | 17        |
| 3.2 Viewing a VPN Connection.....  | 27        |
| 3.3 Modifying a VPN Connection.....  | 28        |
| 3.4 Deleting a VPN Connection.....   | 30        |
| <b>4 Enterprise Edition VPN Fee Management.....</b>  | <b>32</b> |
| 4.1 Changing the Billing Mode of a VPN Gateway from Pay-Per-Use to Yearly/Monthly.....           | 32        |
| 4.2 Increasing or Decreasing the Bandwidth of an EIP Billed on a Yearly/Monthly Basis.....       | 33        |
| 4.3 Increasing or Decreasing the VPN Connection Group Quota of a Yearly/Monthly VPN Gateway..... | 33        |
| <b>5 Monitoring.....</b>   | <b>35</b> |
| 5.1 Monitoring VPN.....  | 35        |
| 5.2 Metrics.....   | 35        |
| 5.3 Viewing Metrics.....   | 38        |
| 5.4 Creating Alarm Rules.....  | 40        |
| <b>6 Audit.....</b>  | <b>42</b> |
| 6.1 VPN Operations That Can Be Recorded by CTS.....  | 42        |
| 6.2 Querying CTS Traces.....   | 43        |

---

|   |           |
|---|-----------|
| <b>7 Permissions Management.....</b>                  | <b>44</b> |
| 7.1 Creating a User and Granting VPN Permissions..... | 44        |
| 7.2 VPN Custom Policies.....                          | 45        |
| <b>8 Quotas.....</b>                                  | <b>48</b> |

# 1 Enterprise Edition VPN Gateway Management

## 1.1 Creating a VPN Gateway

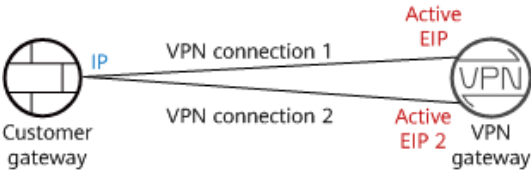
### Scenarios

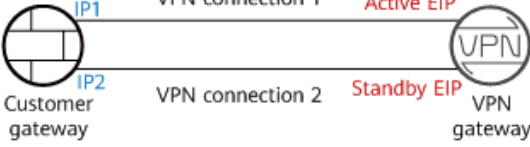
To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a VPN gateway before creating a VPN connection.

### Context

The recommended networking varies according to the number of customer gateway IP addresses, as described in [Table 1-1](#).

**Table 1-1** Networking

| Number of Customer Gateway IP Addresses | Recommended Networking  | Description  |
|---|---|--|
| 1                                       |  <p>The diagram illustrates a network setup where a 'Customer gateway' (represented by a circle with a grid) is connected to a 'VPN gateway' (represented by a circle with 'VPN' text) through two separate lines labeled 'VPN connection 1' and 'VPN connection 2'. The VPN gateway is also associated with two 'Active EIP' labels, 'Active EIP' and 'Active EIP 2', indicating an active-active configuration.</p> | <p>It is recommended that the VPN gateway uses the active-active mode. In this case, one VPN connection group is used.</p> |


| Number of Customer Gateway IP Addresses | Recommended Networking   | Description  |
|---|--|--|
| 2                                       |  <p>The diagram illustrates a network configuration where a customer gateway (left) is connected to a VPN gateway (right) via two separate VPN connections. The customer gateway has two IP addresses, IP1 and IP2. VPN connection 1 connects IP1 to the Active EIP of the VPN gateway. VPN connection 2 connects IP2 to the Standby EIP of the VPN gateway.</p> | It is recommended that the VPN gateway uses the active-standby mode. In this case, two VPN connection groups are used. |

- If your on-premises data center has only one customer gateway configured with only one IP address, it is recommended that the VPN gateway uses the active-active mode. In this mode, you need to create a VPN connection between each of the active EIP and active EIP 2 of the VPN gateway and the IP address of the customer gateway. In this scenario, only one VPN connection group is used.
- If your on-premises data center has two customer gateways or one customer gateway configured with two IP addresses, it is recommended that the VPN gateway uses the active-standby mode. In this mode, you need to create a VPN connection with each of the customer gateway IP addresses using the active and standby EIPs of the VPN gateway. In this scenario, two VPN connection groups are used.

## Prerequisites

- A VPC has been created. For details about how to create a VPC, see [Creating a VPC and Subnet](#).
- Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see [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. 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, click **Buy VPN Gateway**.
6. Set parameters as prompted and click **Next**.

[Table 1-2](#) lists the VPN gateway parameters.

**Table 1-2** Description of VPN gateway parameters

| Parameter              | Description  | Example Value                 |
|------------------------|--|-------------------------------|
| Billing Mode           | <ul style="list-style-type: none"><li>● <b>Yearly/Monthly:</b> You are billed by month or year when creating a VPN gateway. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway.</li><li>● <b>Pay-per-use:</b> VPN gateways and VPN connection groups are billed by usage duration, and the billing cycle is 1 hour.</li></ul> | Yearly/Monthly                |
| Region                 | For low network latency and fast resource access, select the region nearest to your target users.<br>Resources cannot be shared across regions.  | EU-Dublin                     |
| Name                   | Name of a VPN gateway.   | vpngw-001                     |
| Network Type           | <ul style="list-style-type: none"><li>● <b>Public network:</b> A VPN gateway communicates with a customer gateway in an on-premises data center through the Internet.</li><li>● <b>Private network:</b> A VPN gateway communicates with a customer gateway in an on-premises data center through a private network.</li></ul>  | Public network                |
| Associate With         | <ul style="list-style-type: none"><li>● VPC<br/>Through a VPC, the VPN gateway sends messages to the customer gateway or servers in the local subnet.</li></ul>  | VPC                           |
| VPC                    | Select a VPC.  | vpc-001(192.168.0.0/16)       |
| Interconnection Subnet | This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.   | 192.168.66.0/24               |
| Local Subnet           | VPC subnets with which your on-premises data center needs to communicate through the customer gateway. <ul style="list-style-type: none"><li>● Select subnet<br/>Select subnets of the local VPC.</li><li>● Enter CIDR block<br/>Enter subnets of the local VPC or subnets of the VPC that establishes a peering connection with the local VPC.</li></ul>                      | 192.168.1.0/24,192.168.2.0/24 |

| Parameter             | Description   | Example Value  |
|-----------------------|---|----------------|
| BGP ASN               | BGP ASN of the VPN gateway, which must be different from that of the customer gateway.  | 64512          |
| Specification         | Forwarding bandwidth and maximum number of VPN connection groups supported by the VPN gateway.<br>Two options are available: <b>Professional 1</b> and <b>Professional 2</b> .  | Professional 1 |
| AZ                    | An AZ is a geographic location with independent power supply and network facilities in a region. AZs in the same VPC are interconnected through private networks and are physically isolated. <ul style="list-style-type: none"><li>• If two or more AZs are available, select two AZs.<br/>The VPN gateway deployed in two AZs has higher availability. You are advised to select the AZs where resources in the VPC are located.</li><li>• If only one AZ is available, select this AZ.</li></ul> | AZ1, AZ2       |
| VPN Connection Groups | This parameter is available only when <b>Billing Mode</b> is set to <b>Yearly/Monthly</b> .<br>By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway. <ul style="list-style-type: none"><li>• When the VPN gateway uses the active-active mode, only one VPN connection group is used.</li><li>• When the VPN gateway uses the active-standby mode, two VPN connection groups are used.</li></ul>   | 10             |



| Parameter  | Description  | Example Value |
|------------|--|---------------|
| HA Mode    | <ul style="list-style-type: none"> <li>● <b>Active-active:</b> Both the active EIP and active EIP 2 establish a VPN connection with the customer gateway, but only one VPN connection is used for data transmission. When this VPN connection fails, traffic is switched to the other VPN connection.</li> <li>● <b>Active-standby:</b> Both the active and standby EIPs establish a VPN connection with the customer gateway. By default, traffic is transmitted only through the active link. If the active link fails, traffic is automatically switched to the standby link. After the active link recovers, traffic is switched back to the active link.</li> </ul> | Active-active |
| Active EIP | <p>This parameter is available only when <b>Network Type</b> is set to <b>Public network</b>.</p> <p>EIP used by the VPN gateway to communicate with a customer gateway.</p> <ul style="list-style-type: none"> <li>● <b>Create Now:</b> Buy a new EIP. The billing mode of the new EIP is the same as that of the VPN gateway.</li> <li>● <b>Use existing:</b> Use an existing EIP. This EIP can share bandwidth with the EIPs of other network services.</li> </ul>  | Create Now    |
| Billed By  | <p>This parameter is available only when <b>Billing Mode</b> is set to <b>Pay-per-use</b> and <b>Network Type</b> is set to <b>Public network</b>.</p> <p>A pay-per-use VPN gateway can be billed by bandwidth or by traffic.</p> <ul style="list-style-type: none"> <li>● <b>Bandwidth:</b> You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth.</li> <li>● <b>Traffic:</b> You need to specify a bandwidth limit and pay for the outbound traffic sent from your VPC.</li> </ul>  | Traffic       |

| Parameter          | Description   | Example Value    |
|--------------------|---|------------------|
| Bandwidth (Mbit/s) | <p>This parameter is available only when <b>Network Type</b> is set to <b>Public network</b> and <b>Active EIP</b> is set to <b>Create Now</b>.</p> <p>Bandwidth of the EIP, in Mbit/s.</p> <ul style="list-style-type: none"><li>All VPN connections created using the EIP share the bandwidth of the EIP. The total bandwidth consumed by all the VPN connections cannot exceed the bandwidth of the EIP.</li><li>If network traffic exceeds the bandwidth of the EIP, network congestion may occur and VPN connections may be interrupted. As such, ensure that you configure enough bandwidth.</li><li>You can configure alarm rules on Cloud Eye to monitor the bandwidth.</li><li>You can customize the bandwidth within the allowed range.</li></ul> | 10 Mbit/s        |
| Bandwidth Name     | <p>This parameter is available only when <b>Network Type</b> is set to <b>Public network</b>.</p> <p>EIP bandwidth name.</p>  | Vpngw-bandwidth1 |
| Active EIP 2       | <p>This parameter is available only when the <b>Network Type</b> is set to <b>Public network</b> and <b>HA Mode</b> is set to <b>Active-active</b>.</p> <p>A VPN gateway needs to be bound to a group of EIPs (active EIP and active EIP 2). You can plan the bandwidth and billing mode for each EIP. The EIPs can share bandwidth with the EIPs of other network services.</p>  | Create Now       |
| Standby EIP        | <p>This parameter is available only when the <b>Network Type</b> is set to <b>Public network</b> and <b>HA Mode</b> is set to <b>Active-standby</b>.</p> <p>A VPN gateway needs to be bound to a group of EIPs (active EIP and standby EIP). You can plan the bandwidth and billing mode for each EIP. The EIPs can share bandwidth with the EIPs of other network services.</p>  | Create Now       |

| Parameter          | Description  | Example Value              |
|--------------------|--|----------------------------|
| Billed By          | <p>This parameter is available only when <b>Billing Mode</b> is set to <b>Pay-per-use</b> and <b>Network Type</b> is set to <b>Public network</b>.</p> <p>A pay-per-use VPN gateway can be billed by bandwidth or by traffic.</p> <ul style="list-style-type: none"> <li>• <b>Bandwidth:</b> You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth.</li> <li>• <b>Traffic:</b> You need to specify a bandwidth limit and pay for the outbound traffic sent from your VPC.</li> </ul>  | Traffic                    |
| Bandwidth (Mbit/s) | <p>This parameter is available only when <b>Network Type</b> is set to <b>Public network</b> and <b>Active EIP 2</b> or <b>Standby EIP</b> is set to <b>Create Now</b>.</p> <p>Bandwidth of the EIP, in Mbit/s.</p> <ul style="list-style-type: none"> <li>• All VPN connections created using the EIP share the bandwidth of the EIP. The total bandwidth consumed by all the VPN connections cannot exceed the bandwidth of the EIP.</li> <li>• If network traffic exceeds the bandwidth of the EIP, network congestion may occur and VPN connections may be interrupted. As such, ensure that you configure enough bandwidth.</li> <li>• You can configure alarm rules on Cloud Eye to monitor the bandwidth.</li> <li>• You can customize the bandwidth within the allowed range.</li> </ul> | 10 Mbit/s                  |
| Bandwidth Name     | <p>This parameter is available only when <b>Network Type</b> is set to <b>Public network</b>.</p> <p>EIP bandwidth name.</p>   | Vpngw-bandwidth2           |
| Access VPC         | <ul style="list-style-type: none"> <li>• This parameter is available only when <b>Associate With</b> is set to <b>VPC</b> and <b>Network Type</b> is set to <b>Private network</b>.</li> </ul> <p>If a VPN gateway needs to connect to different VPCs in the southbound and northbound directions, set the VPC in the northbound direction as the access VPC. The VPC in the southbound direction is the VPC associated with the VPN gateway.</p>  | Same as the associated VPC |

| Parameter         | Description  | Example Value                      |
|-------------------|--|------------------------------------|
| Access Subnet     | <ul style="list-style-type: none"><li>This parameter is available only when <b>Associate With</b> is set to <b>VPC</b> and <b>Network Type</b> is set to <b>Private network</b>.</li></ul> By default, a VPN gateway uses the interconnection subnet to connect to the associated VPC. Set this parameter when another subnet needs to be used.  | Same as the interconnection subnet |
| Required Duration | This parameter is available only when <b>Billing Mode</b> is set to <b>Yearly/Monthly</b> .<br>If your account balance is sufficient and you select <b>Auto-renew</b> , the system automatically renews your service when the required duration elapses. <ul style="list-style-type: none"><li>Monthly subscription: Your service is automatically renewed on a per-month basis.</li><li>Yearly subscription: Your service is automatically renewed on a per-year basis.</li></ul> | 6                                  |


7. Confirm the order and click **Pay Now**.

## 1.2 Viewing a VPN Gateway


### Scenarios

After creating a VPN gateway, you can view its details.

### Procedure

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, view the VPN gateway list.
6. Click the name of a VPN gateway to view its details.
  - For VPN gateways of the public network type, you can view their basic information and EIPs.
  - For VPN gateways of the private network type, you can view the basic information and advanced settings.

 NOTE


In the VPN gateway list, you can click  in the **Gateway IP Address** column of a VPN gateway to view the bandwidth and traffic of the VPN gateway.


## 1.3 Modifying a VPN Gateway

### Scenarios

You can modify basic information about a VPN gateway, including the name and local subnets.

### Procedure

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, and click **Modify Basic Information** in the **Operation** column.

To modify only the name of a VPN gateway, you can also click  next to the VPN gateway name.


6. Modify the name and local subnet of the VPN gateway as prompted.
7. Click **OK**.

## 1.4 Binding an EIP to a VPN Gateway

### Scenarios

You can bind an EIP to a VPN gateway that has been created.

### Procedure

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. Locate the row that contains the target VPN gateway, and choose **More > Bind EIP** in the **Operation** column.
  - If the VPN gateway uses the active-active mode, the VPN gateway can be bound to the active EIP and active EIP 2.
  - If the VPN gateway uses the active-standby mode, the VPN gateway can be bound to an active EIP and a standby EIP.


6. Select the desired EIP and click **OK**.

## 1.5 Unbinding an EIP from a VPN Gateway

### Scenarios

After creating a VPN gateway, you can unbind an EIP from it.

### Procedure

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 and click **Unbind EIP** in the **Operation** column.
  - If the VPN gateway uses the active-active mode, the VPN gateway can be unbound from the active EIP and active EIP 2.
  - If the VPN gateway uses the active-standby mode, the VPN gateway can be unbound from the active EIP and standby EIP.
6. In the displayed dialog box, click **Yes**.

#### NOTE

- An EIP that is in use by a VPN connection cannot be unbound from a VPN gateway.
- An EIP will continue to be billed after being unbound from a VPN gateway. If you no longer need an EIP, you are advised to release it.

## 1.6 Unsubscribing from a Yearly/Monthly VPN Gateway


### Scenarios

If a yearly/monthly VPN gateway is no longer required, you can unsubscribe from it.

#### NOTE

If a pay-per-use EIP is bound to a VPN gateway, the EIP is automatically unbound from the VPN gateway when you unsubscribe from the VPN gateway. After the EIP is unbound, it is retained. If the EIP is no longer used, you can release it after unsubscribing from the VPN gateway.

### Procedure

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, and choose **More > Unsubscribe** in the **Operation** column.
6. Unsubscribe the VPN gateway as prompted.

## 1.7 Renewing a Yearly/Monthly VPN Gateway

### Scenarios

You can renew a yearly/monthly VPN gateway that is about to expire.

### Procedure

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. In the **Operation** column, choose **More > Renew**.
6. Complete the renewal as prompted.

## 1.8 Deleting a Pay-per-Use VPN Gateway

### Scenarios

You can delete a pay-per-use VPN gateway that is no longer required.

### Restrictions and Limitations

- A VPN gateway that is being created, updated, or deleted cannot be deleted.
- If a VPN gateway has VPN connections configured, you need to delete all the VPN connections before deleting the VPN gateway.


For details about how to delete a VPN connection, see [Deleting a VPN Connection](#).

- If a VPN gateway is bound to an EIP billed in yearly/monthly mode, the EIP will be unbound from the VPN gateway when the VPN gateway is deleted. After the EIP is unbound, it is retained. If the EIP is no longer used, you can release it after deleting the gateway.
- If a VPN gateway is bound to an EIP billed in pay-per-use mode, the EIP will be released when the VPN gateway is deleted.

To retain such a pay-per-use EIP, unbind it before deleting the VPN gateway. For details about how to unbind an EIP, see [Unbinding an EIP from a VPN Gateway](#).

- If a VPN gateway is bound to an EIP that shares bandwidth with other EIPs, the EIP will be released and the shared bandwidth will be reserved when the VPN gateway is deleted.

## Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the navigation pane on the left, choose **Virtual Private Network > Enterprise - VPN Gateways**.
4. On the **VPN Gateways** page, locate the row that contains the target VPN gateway, and choose **More > Delete** in the **Operation** column.
5. In the displayed dialog box, click **Yes**.




# 2 Customer Gateway Management of Enterprise Edition VPN

## 2.1 Creating a Customer Gateway

### Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a customer gateway before creating a VPN connection.

### Procedure

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 - Customer Gateways**.
5. On the **Customer Gateways** page, click **Create Customer Gateway**.
6. Set parameters as prompted and click **Create Now**.

[Table 2-1](#) lists the customer gateway parameters.

**Table 2-1** Description of customer gateway parameters

| Parameter | Description                 | Example Value |
|-----------|-----------------------------|---------------|
| Name      | Name of a customer gateway. | cgw-001       |

| Parameter          | Description  | Example Value |
|--------------------|--|---------------|
| Routing Mode       | <p>Routing mode of the customer gateway.</p> <ul style="list-style-type: none"><li>• Select <b>Dynamic (BGP)</b> when <b>VPN Type</b> is set to <b>Route-based</b> and <b>Routing Mode</b> is set to <b>Dynamic (BGP)</b> for the VPN connection.<ul style="list-style-type: none"><li>– When selecting this option, ensure that the customer gateway supports dynamic BGP.</li><li>– The customer gateway can advertise a maximum of 100 BGP routes to the VPN gateway. If more than 100 BGP routes are advertised, the BGP peer relationship is disconnected, causing traffic interruption between the VPN gateway and customer gateway.</li></ul></li><li>• Select <b>Static</b> when <b>VPN Type</b> is set to <b>Route-based</b> and <b>Routing Mode</b> is set to <b>Static</b> for the VPN connection.</li><li>• You are advised to select <b>Static</b> when <b>VPN Type</b> is set to <b>Policy-based</b> for the VPN connection.</li></ul> | Static        |
| BGP ASN            | <p>This parameter is available only when <b>Routing Mode</b> is set to <b>Dynamic (BGP)</b>. Enter the ASN of your on-premises data center or private network.</p> <p>The BGP ASN of the customer gateway must be different from that of the VPN gateway.</p>  | 65000         |
| Gateway IP Address | <p>IP address used by the customer gateway to communicate with the VPN gateway. The value must be a static address.</p> <p>Ensure that UDP port 4500 is permitted in a firewall rule on the customer gateway in your on-premises data center or private network.</p>   | 1.2.3.4       |

7. (Optional) If there are two customer gateway IP addresses, repeat the preceding operations to configure the customer gateway with another IP address.

## Related Operations


You need to configure an IPsec VPN tunnel on the router or firewall in your on-premises data center.

## 2.2 Viewing a Customer Gateway

### Scenarios

After creating a customer gateway, you can view its details.

### Procedure



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 – Customer Gateways**.
5. On the **Customer Gateway** page, view the customer gateway list.
6. Click the name of a customer gateway to view its details.
  - In the **Basic Information** area, you can view the name, ID, routing mode, BGP ASN, IP address, and VPN connection of the customer gateway.

## 2.3 Modifying a Customer Gateway

### Scenarios

After creating a customer gateway, you can modify its name.

### Procedure


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 – Customer Gateways**.
5. On the **Customer Gateway** page, click  next to the name of a customer gateway.
6. Enter a new name for the customer gateway and click **OK**.

## 2.4 Deleting a Customer Gateway

### Scenarios

You can delete a customer gateway that you have created.

## Procedure

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 – Customer Gateways**.
5. On the **Customer Gateway** page, locate the customer gateway to delete and click **Delete** in the **Operation** column.

Before deleting a customer gateway associated with a VPN connection, remove the customer gateway from the VPN connection.

6. Click **Yes**.


# 3 Enterprise Edition VPN Connection Management

## 3.1 Creating a VPN Connection

### Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, you need to create VPN connections after creating a VPN gateway and a customer gateway.

### Procedure

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 Connections**.
5. On the **VPN Connections** page, click **Buy VPN Connection**.

#### NOTE

For higher reliability, you are advised to create a VPN connection between each of the two EIPs of a VPN gateway and the IP address of a customer gateway.

6. Set parameters as prompted and click **Next**.  
**Table 3-1** lists the VPN connection parameters.

**Table 3-1** Description of VPN connection parameters

| Parameter | Description               | Example Value |
|-----------|---------------------------|---------------|
| Name      | Name of a VPN connection. | vpn-001       |

| Parameter          | Description  | Example Value                |
|--------------------|--|------------------------------|
| VPN Gateway        | Name of the VPN gateway for which the VPN connection is created.<br>You can also click <b>Create VPN Gateway</b> to create a VPN gateway. For details about related parameters, see <a href="#">Table 1-2</a> .  | vpngw-001                    |
| Gateway IP Address | IP address of the VPN gateway.<br>The same EIP of a VPN gateway cannot be repeatedly selected when you create VPN connections between the VPN gateway and the same customer gateway.   | Available gateway IP address |
| Customer Gateway   | Name of a customer gateway.<br>You can also click <b>Create Customer Gateway</b> to create a customer gateway. For details about related parameters, see <a href="#">Table 2-1</a> .<br><b>NOTE</b><br>If a customer gateway connects to multiple VPN gateways, the BGP ASNs and VPN types of the VPN gateways must be the same. | cgw-001                      |

| Parameter       | Description   | Example Value               |
|-----------------|---|-----------------------------|
| VPN Type        | <p>IPsec connection mode, which can be route-based or policy-based.</p> <ul style="list-style-type: none"><li>• Static routing<br/>Determines the data that enters the IPsec VPN tunnel based on the route configuration (local subnet and customer subnet).<br/>Application scenario:<br/>Communication between customer gateways</li><li>• BGP routing<br/>Determines the traffic that can enter the IPsec VPN tunnel based on BGP routes.<br/>Application scenario:<br/>Communication between customer gateways + Many or frequently changed interconnection subnets or backup between VPC and Direct Connect</li><li>• Policy-based<br/>Determines the data that enters the IPsec VPN tunnel based on the policy (between the customer network and VPC). Policy rules can be defined based on the source and destination CIDR blocks.<br/>Application scenario: Isolation between customer gateways</li></ul> | Static routing              |
| Customer Subnet | <p>Subnets in your on-premises data center that need to communicate with a VPC through the customer gateway.</p> <p>If there are multiple customer subnets, separate them with commas (,).</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>• A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached.</li><li>• Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.</li></ul>  | 172.16.1.0/24,172.16.2.0/24 |

| Parameter                       | Description   | Example Value        |
|---------------------------------|---|----------------------|
| Interface IP Address Assignment | <p>This parameter is available only when <b>VPN Type</b> is set to <b>Static routing</b> or <b>BGP routing</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>• Set interface IP addresses to the tunnel interface IP addresses used by the VPN gateway and customer gateway to communicate with each other.</li><li>• If the tunnel interface address of the customer gateway is fixed, select <b>Manually specify</b>, and set the tunnel interface address of the VPN gateway based on the tunnel interface address of the customer gateway.</li><li>• Manually specify<br/>Set <b>Local Interface IP Address</b> to the tunnel interface address of the VPN gateway, which can reside only on the 169.254.x.x/30 CIDR block (except 169.254.195.x/30). Then, the system automatically sets <b>Customer Interface IP Address</b> to a random value based on the setting of <b>Local Interface IP Address</b>.<br/>For example, when you set <b>Local Interface IP Address</b> to <b>169.254.1.6/30</b>, the system automatically sets the <b>Customer Interface IP Address</b> to <b>169.254.1.5/30</b>.</li><li>• Automatically assign<br/>By default, an IP address on the 169.254.x.x/30 CIDR block is assigned to the tunnel interface of the VPN gateway.<br/>To view the automatically assigned local and customer interface IP addresses, click <b>Modify VPN Connection</b> on the <b>VPN Connections</b> page.</li></ul> | Automatically assign |



| Parameter                         | Description  | Example Value |
|-----------------------------------|--|---------------|
| Local Tunnel Interface Address    | This parameter is available only when <b>Interface IP Address Assignment</b> is set to <b>Manually specify</b> .<br>Tunnel interface IP address configured on the VPN gateway.   | N/A           |
| Customer Tunnel Interface Address | This parameter is available only when <b>Interface IP Address Assignment</b> is set to <b>Manually specify</b> .<br>Tunnel interface IP address configured on the customer gateway device.   | N/A           |
| Link Detection                    | This parameter is available only when <b>VPN Type</b> is set to <b>Static routing</b> .<br><b>NOTE</b><br>When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, traffic will fail to be forwarded.<br>After this function is enabled, the VPN gateway automatically performs Network Quality Analysis (NQA) on the customer interface IP address of the customer gateway. | Selected      |
| PSK                               | The PSKs configured for the VPN gateway and customer gateway must be the same.<br>The PSK: <ul style="list-style-type: none"> <li>• Contains 8 to 128 characters.</li> <li>• Can contain only three or more types of the following characters: <ul style="list-style-type: none"> <li>- Digits</li> <li>- Uppercase letters</li> <li>- Lowercase letters</li> <li>- Special characters: ~ ! @ # \$ % ^ ( ) - _ + = { } , . / : ;</li> </ul> </li> </ul>  | Test@123      |
| Confirm PSK                       | Enter the PSK again.   | Test@123      |

| Parameter       | Description  | Example Value  |
|-----------------|--|--|
| Policy          | <p>This parameter is available only when <b>VPN Type</b> is set to <b>Policy-based</b>.</p> <p>Defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. By default, a maximum of five policy rules can be configured.</p> <ul style="list-style-type: none"> <li>● Source CIDR Block<br/>The source CIDR block must contain some CIDR blocks of the local subnets. <b>0.0.0.0/0</b> indicates any IP address.</li> <li>● Destination CIDR block<br/>The destination CIDR block must contain all the CIDR blocks of the customer subnets. A policy rule supports a maximum of five destination CIDR blocks, which are separated by commas (,).</li> </ul> <p><b>NOTE</b><br/>When <b>Associate With</b> is set to <b>VPC</b> for the VPN gateway and <b>VPN Type</b> is set to <b>Policy-based</b> for the VPN connection, do not set <b>Destination CIDR Block</b> to <b>0.0.0.0</b>. Otherwise, traffic may fail to be forwarded.</p> | <ul style="list-style-type: none"> <li>● Source CIDR block 1:<br/>192.168.1.0/24</li> <li>● Destination CIDR block 1:<br/>172.16.1.0/24,172.16.2.0/24</li> <li>● Source CIDR block 2:<br/>192.168.2.0/24</li> <li>● Destination CIDR block 2:<br/>172.16.1.0/24,172.16.2.0/24</li> </ul> |
| Policy Settings | <ul style="list-style-type: none"> <li>● <b>Default:</b> Use default IKE and IPsec policies.</li> <li>● <b>Custom:</b> Use custom IKE and IPsec policies. For details about the policies, see <a href="#">Table 3-2</a> and <a href="#">Table 3-3</a>.</li> </ul>  | Custom   |

**Table 3-2** IKE policy

| Parameter                | Description   | Example Value |
|--------------------------|---|---------------|
| Version                  | Version of the IKE protocol. The value can be one of the following: <ul style="list-style-type: none"><li>v1 (v1 has low security. If the device supports v2, v2 is recommended.)</li><li>v2</li></ul> The default value is <b>v2</b> .   | v2            |
| Negotiation Mode         | This parameter is available only when <b>Version</b> is <b>v1</b> . <ul style="list-style-type: none"><li>Main</li><li>Aggressive</li></ul>   | Main          |
| Authentication Algorithm | Hash algorithm used for authentication. The following options are available: <ul style="list-style-type: none"><li>SHA1(Insecure. Not recommended.)</li><li>MD5(Insecure. Not recommended.)</li><li>SHA2-256</li><li>SHA2-384</li><li>SHA2-512</li></ul> The default value is <b>SHA2-256</b> .   | SHA2-256      |
| Encryption Algorithm     | Encryption algorithm. The following options are available: <ul style="list-style-type: none"><li>3DES(Insecure. Not recommended.)</li><li>AES-128</li><li>AES-192</li><li>AES-256</li><li>AES-256-GCM-16</li></ul> When this encryption algorithm is used, the IKE version can only be <b>v2</b> .<br>The default value is <b>AES-128</b> . | AES-128       |

| Parameter    | Description   | Example Value |
|--------------|---|---------------|
| DH Algorithm | <p>The following algorithms are supported:</p> <ul style="list-style-type: none"><li>• Group 1(Insecure. Not recommended.)</li><li>• Group 2(Insecure. Not recommended.)</li><li>• Group 5(Insecure. Not recommended.)</li><li>• Group 14(Insecure. Not recommended.)</li><li>• Group 15</li><li>• Group 16</li><li>• Group 19</li><li>• Group 20</li><li>• Group 21</li></ul> <p>The default value is <b>Group 15</b>.</p>   | Group 14      |
| Lifetime (s) | <p>Lifetime of a security association (SA).<br/>An SA will be renegotiated when its lifetime expires.</p> <ul style="list-style-type: none"><li>• Unit: second</li><li>• The value ranges from <b>60</b> to <b>604800</b>.</li><li>• The default value is <b>86400</b>.</li></ul>   | 86400         |
| Local ID     | <p>Authentication identifier of the VPN gateway used in IPsec negotiation. The VPN gateway ID configured on the customer gateway must be the same as the local ID configured here. Otherwise, IPsec negotiation fails.</p> <ul style="list-style-type: none"><li>• IP Address (default value)<br/>The system automatically sets this parameter to the selected EIP of the VPN gateway.</li><li>• FQDN<br/>Set the full qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &amp;, &lt;, &gt;, [, ], \, ?, and spaces).</li></ul> | IP Address    |

| Parameter   | Description   | Example Value |
|-------------|---|---------------|
| Customer ID | <p>Authentication identifier of the customer gateway used in IPsec negotiation. The customer gateway ID configured on the customer gateway must be the same as the customer ID configured here. Otherwise, IPsec negotiation fails.</p> <ul style="list-style-type: none"><li>• IP Address (default value)<br/>The system automatically sets this parameter to the IP address of the customer gateway.</li><li>• FQDN<br/>Set the full qualified domain name (FQDN) to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &amp;, &lt;, &gt;, [, ], \, ?, and spaces).</li></ul> | IP Address    |

**Table 3-3** IPsec policy

| Parameter                | Description  | Example Value |
|--------------------------|--|---------------|
| Authentication Algorithm | <p>Hash algorithm used for authentication. The following options are available:</p> <ul style="list-style-type: none"><li>• SHA1(Insecure. Not recommended.)</li><li>• MD5(Insecure. Not recommended.)</li><li>• SHA2-256</li><li>• SHA2-384</li><li>• SHA2-512</li></ul> <p>The default value is <b>SHA2-256</b>.</p> | SHA2-256      |

| Parameter            | Description  | Example Value |
|----------------------|--|---------------|
| Encryption Algorithm | <p>Encryption algorithm. The following options are available:</p> <ul style="list-style-type: none"><li>• 3DES(Insecure. Not recommended.)</li><li>• AES-128</li><li>• AES-192</li><li>• AES-256</li><li>• AES-128-GCM-16</li><li>• AES-256-GCM-16</li></ul> <p>The default value is <b>AES-128</b>.</p>   | AES-128       |
| PFS                  | <p>Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms:</p> <ul style="list-style-type: none"><li>• Disable(Insecure. Not recommended.)</li><li>• DH group 1(Insecure. Not recommended.)</li><li>• DH group 2(Insecure. Not recommended.)</li><li>• DH group 5(Insecure. Not recommended.)</li><li>• DH group 14(Insecure. Not recommended.)</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></ul> <p>The default value is <b>DH group 15</b>.</p> | DH group 15   |
| Transfer Protocol    | <p>Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported:</p> <ul style="list-style-type: none"><li>• ESP</li></ul> <p>The default value is <b>ESP</b>.</p>   | ESP           |

| Parameter                 | Description  | Example Value |
|---------------------------|--|---------------|
| Lifetime (s)              | Lifetime of an SA.<br>An SA will be renegotiated when its lifetime expires. <ul style="list-style-type: none"><li>• Unit: second</li><li>• The value ranges from <b>30</b> to <b>604800</b>.</li><li>• The default value is <b>3600</b>.</li></ul> | 3600          |
| Packet Encapsulation Mode | The default value is <b>TUNNEL</b> .   | TUNNEL        |

 **NOTE**

An IKE policy specifies the encryption and authentication algorithms to use in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to use in the data transmission phase of an IPsec tunnel. The policy settings for VPN connections must be the same at the VPC and on-premises data center sides. If they are different, VPN negotiation will fail, causing the failure to establish VPN connections.

The following algorithms are not recommended because they are not secure enough:

- Authentication algorithms: SHA1 and MD5
  - Encryption algorithm: 3DES
  - DH algorithms: Group 1, Group 2, Group 5, and Group 14
7. Confirm the VPN connection configuration and click **Submit**.
  8. Repeat the preceding operations to create the other VPN connection.

For details about IP address configuration, see [Context](#).


For details about scenario-specific configuration examples, see [Administrator Guide](#).

## 3.2 Viewing a VPN Connection

### Scenarios

After creating a VPN connection, you can view its details.

### Procedure

1. Click  in the upper left corner and select the desired region and project.
2. Click **Service List** and choose **Networking > Virtual Private Network**.
3. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Connections**.
4. On the **VPN Connections** page, view the VPN connection list.

- Click the name of a VPN connection to view its basic information and policy configuration.

 **NOTE**


- 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.
- In the VPN connection list, you can locate the target VPN connection and click **View Metric** to view monitoring information about the VPN connection.

## 3.3 Modifying a VPN Connection

### Scenarios

A VPN connection is an encrypted communications channel established between a VPN gateway in a VPC and a customer gateway in your on-premises data center. You can modify a VPN connection when required.

### Procedure

- Log in to the management console.
- Click  in the upper left corner and select the desired region and project.
- Click **Service List** and choose **Networking > Virtual Private Network**.
- In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Connections**.
- On the **VPN Connections** page, locate the VPN connection to modify, and click **Modify VPN Connection**.
- Modify VPN connection parameters as prompted.
- Click **OK**.

---

 **CAUTION**

If you change the PSK or modify the IKE or IPsec policy of a VPN connection, ensure that the new configurations are consistent with those on the customer gateway. Otherwise, the VPN connection will be interrupted.

---

Only some of the parameters take effect immediately after being modified, as described in [Table 3-4](#).



**Table 3-4** Time when new parameter settings take effect

| Item               | Parameter                | When New Settings Take Effect  | How to Modify   |
|--------------------|--------------------------|--|---|
| -                  | PSK                      | <ul style="list-style-type: none"> <li>When IKEv1 is used, the new setting takes effect in the next negotiation period.</li> <li>When IKEv2 is used, the new setting takes effect after the VPN connection is re-established.</li> </ul> | <ul style="list-style-type: none"> <li>When IKEv1 is used: Locate the VPN connection to modify, choose <b>More &gt; Reset PSK</b> on the right, and change the PSK as prompted.</li> <li>When IKEv2 is used: <ol style="list-style-type: none"> <li>Delete the current VPN connection.</li> <li>Create a new VPN connection.</li> </ol> </li> </ul> |
| IKE policy (IKEv1) | Encryption Algorithm     | The new settings take effect in the next negotiation period.   | Locate the VPN connection to modify, and click <b>Modify VPN Configuration</b> .  |
|                    | Authentication Algorithm |  |   |
|                    | DH Algorithm             |  |   |
|                    | Negotiation Mode         |  |   |
|                    | Local ID                 |  |   |
|                    | Customer ID              |  |   |
|                    | Lifetime (s)             |  |   |
|                    | Version                  | The new settings take effect immediately.  |   |
| IKE policy (IKEv2) | Encryption Algorithm     | The new settings take effect in the next negotiation period.   | Locate the VPN connection to modify, and click <b>Modify VPN Configuration</b> .  |

| Item         | Parameter                | When New Settings Take Effect  | How to Modify  |
|--------------|--------------------------|--|--|
|              | Authentication Algorithm |  |  |
|              | DH Algorithm             |  |  |
|              | Lifetime (s)             |  |  |
|              | Version                  | The new settings take effect immediately.                                |  |
|              | Local ID                 | The new settings take effect after the VPN connection is re-established. |  |
|              | Custom ID                |  |  |
| IPsec policy | Encryption Algorithm     | The new settings take effect in the next negotiation period.             | Locate the VPN connection to modify, and click <b>Modify VPN Configuration</b> . |
|              | Authentication Algorithm |  |  |
|              | PFS                      |  |  |
|              | Lifetime (s)             |  |  |
|              | Transfer Protocol        | Currently, this parameter cannot be modified on the management console.  |  |


## 3.4 Deleting a VPN Connection

### Scenarios

If a VPN connection is no longer required, you can delete it to release network resources.

### Procedure

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 Connections**.
5. On the **VPN Connections** page, choose **More > Delete** in the **Operation** column of a VPN connection.
6. In the displayed dialog box, click **Yes**.

# 4 Enterprise Edition VPN Fee Management

---

## 4.1 Changing the Billing Mode of a VPN Gateway from Pay-Per-Use to Yearly/Monthly

### Procedure

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. Locate a pay-per-use VPN gateway, and choose **More > Change Billing Mode** in the **Operation** column.
  - You can change the billing mode of the VPN gateway and bound EIPs to yearly/monthly simultaneously. Alternatively, you can only change the billing mode of the VPN gateway to yearly/monthly, and retain the billing mode of the bound EIPs as pay-per-use.

Only when the EIPs bound to a VPN gateway are billed by bandwidth in pay-per-use mode, you can change the billing modes of the VPN gateway and EIPs to yearly/monthly simultaneously.
  - Billing formula change

Assume that  $X$  VPN connection groups are in use before the billing mode is changed to yearly/monthly. Then, after the billing mode is changed, the billing formula changes to: Fee of the VPN gateway + Fee of  $(X - 10)$  VPN connection groups.
6. In the **Change Billing Mode** dialog box, click **OK**.
7. Confirm the VPN gateway information and set a renewal duration.
8. Click **Pay**.
9. On the payment page, confirm the order information, select a coupon or discount, and select the payment method.


10. Click **Pay**.

 **NOTE**

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

## 4.2 Increasing or Decreasing the Bandwidth of an EIP Billed on a Yearly/Monthly Basis

### Procedure


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. Click the name of a VPN gateway.
6. Click the **Elastic IPs** tab, and click **Change** next to **Bandwidth (Mbit/s)**.
7. On the **Modify Bandwidth** page, select your required bandwidth and click **Next**.
8. Click **Pay Now**.
  - If the bandwidth is increased, the new bandwidth takes effect immediately after you pay the extra fees.
  - If the bandwidth is decreased, the new bandwidth takes effect only within the renewal period.

## 4.3 Increasing or Decreasing the VPN Connection Group Quota of a Yearly/Monthly VPN Gateway

### Scenarios

You can change the VPN connection group quota for Enterprise Edition VPN gateways whose specifications are not basic.

### Procedure

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. Locate the row that contains the target VPN gateway, and choose **More > Change VPN Connection Group Quota**.

6. On the **Change VPN Connection Group Quota** page, set a new number of VPN connection groups and click **Next**.
7. If you increase the quota, click **Pay Now** to pay the extra fee. If you decrease the quota, click **OK**.

The new quota of VPN connection groups takes effect immediately, and you are charged the extra fee or refunded accordingly.

# 5 Monitoring

## 5.1 Monitoring VPN

Cloud Eye lets you keep a close eye on the performance and resource utilization of VPNs, ensuring VPN reliability and availability. You can use Cloud Eye to automatically monitor VPNs in real time and manage alarms and notifications, so that you can keep track of VPN performance metrics.

## 5.2 Metrics

### Description

This section describes monitored metrics reported by VPN to Cloud Eye as well as their namespaces and dimensions. You can use the Cloud Eye management console to query the metrics of the monitored objects and alarms generated for VPN.

### Namespace

SYS.VPN

### Metrics

**Table 5-1** Metrics supported for Enterprise Edition VPN gateways

| Metric ID             | Metric Name          | Description  | Value Range  | Monitored Object | Monitoring Interval (Raw Data) |
|-----------------------|----------------------|--|--------------|------------------|--------------------------------|
| gateway_send_pkt_rate | Outbound Packet Rate | Average number of data packets leaving the cloud per second. | $\geq 0$ pps | Gateway          | 1 minute                       |

| Metric ID               | Metric Name              | Description   | Value Range  | Monitored Object | Monitoring Interval (Raw Data) |
|-------------------------|--------------------------|---|--------------|------------------|--------------------------------|
| gateway_recv_pkt_rate   | Inbound Packet Rate      | Average number of data packets entering the cloud per second. | $\geq 0$ pps | Gateway          | 1 minute                       |
| gateway_send_rate       | Outbound Bandwidth       | Average volume of traffic leaving the cloud per second.       | 0–1 Gbit/s   | Gateway          | 1 minute                       |
| gateway_recv_rate       | Inbound Bandwidth        | Average volume of traffic entering the cloud per second.      | 0–1 Gbit/s   | Gateway          | 1 minute                       |
| gateway_send_rate_usage | Outbound Bandwidth Usage | Bandwidth utilization for traffic leaving the cloud.          | 0–100%       | Gateway          | 1 minute                       |
| gateway_recv_rate_usage | Inbound Bandwidth Usage  | Bandwidth utilization for traffic entering the cloud.         | 0–100%       | Gateway          | 1 minute                       |
| gateway_connection_num  | Number of Connections    | Number of VPN connections.                                    | $\geq 0$     | Gateway          | 1 minute                       |

**Table 5-2** Enterprise Edition VPN connection metrics

| Metric ID              | Metric Name        | Description   | Value Range | Monitored Object | Monitoring Interval (Raw Data) |
|------------------------|--------------------|---|-------------|------------------|--------------------------------|
| tunnel_average_latency | Average Tunnel RTT | Average round-trip time on the tunnel between the VPN gateway and customer gateway. | 0–5000 ms   | VPN connection   | 1 minute                       |
| tunnel_max_latency     | Maximum Tunnel RTT | Maximum round-trip time on the tunnel between the VPN gateway and customer gateway. | 0–5000 ms   | VPN connection   | 1 minute                       |



| Metric ID               | Metric Name             | Description   | Value Range | Monitored Object       | Monitoring Interval (Raw Data) |
|-------------------------|-------------------------|---|-------------|------------------------|--------------------------------|
| tunnel_packet_loss_rate | Tunnel Packet Loss Rate | Packet loss rate on the tunnel between the VPN gateway and customer gateway.  | 0–100 %     | VPN connection         | 1 minute                       |
| link_average_latency    | Average Link RTT        | Average round-trip time on the physical link between the VPN gateway and customer gateway.  | 0–5000 ms   | VPN connection         | 1 minute                       |
| link_max_latency        | Maximum Link RTT        | Maximum round-trip time on the physical link between the VPN gateway and customer gateway.  | 0–5000 ms   | VPN connection         | 1 minute                       |
| link_packet_loss_rate   | Link Packet Loss Rate   | Packet loss rate on the physical link between the VPN gateway and customer gateway.   | 0–100 %     | VPN connection         | 1 minute                       |
| connection_status       | VPN Connection Status   | VPN connection state:<br><b>0</b> : A VPN connection is in <b>Not connected</b> state.<br><b>1</b> : A VPN connection is in <b>Connected</b> state. | 0 or 1      | VPN connection         | 1 minute                       |
| recv_pkt_rate           | Packet Receive Rate     | Average number of data packets received per second.   | ≥ 0 pps     | VPN connection         | 1 minute                       |
| send_pkt_rate           | Packet Send Rate        | Average number of data packets sent per second.   | ≥ 0 pps     | VPN connection         | 1 minute                       |
| recv_rate               | Traffic Receive Rate    | Average volume of traffic received per second.  | 0~1Gbit/s   | VPN connection         | 1 minute                       |
| send_rate               | Traffic Send Rate       | Average volume of traffic sent per second.  | 0~1Gbit/s   | VPN connection         | 1 minute                       |
| sa_send_pkt_rate        | SA Packet Send Rate     | Average number of data packets sent over an SA per second.  | ≥ 0 pps     | SA of a VPN connection | 1 minute                       |

| Metric ID        | Metric Name             | Description  | Value Range | Monitored Object       | Monitoring Interval (Raw Data) |
|------------------|-------------------------|--|-------------|------------------------|--------------------------------|
| sa_recv_pkt_rate | SA Packet Receive Rate  | Average number of data packets received over an SA per second. | ≥ 0 pps     | SA of a VPN connection | 1 minute                       |
| sa_recv_rate     | SA Traffic Receive Rate | Average volume of traffic received over an SA per second.      | 0~1Gbit/s   | SA of a VPN connection | 1 minute                       |
| sa_send_rate     | SA Traffic Send Rate    | Average volume of traffic sent over an SA per second.          | 0~1Gbit/s   | SA of a VPN connection | 1 minute                       |

## Dimensions

| key                | Value                                      |
|--------------------|--|
| vpn_connection_id  | VPN Connections                            |
| evpn_connection_id | S2C VPN Connection                         |
| evpn_sa_id         | S2C VPN Connection - S2C VPN Connection SA |
| evpn_gateway_id    | S2C VPN Gateway                            |

## 5.3 Viewing Metrics

### Scenarios

View the VPN connection status and usages of bandwidth and EIP.



### Support for Metrics

**Table 5-3** Support for metrics

| Metric Name           | Support  | Enabled by Default? |
|-----------------------|--|---------------------|
| VPN Connection Status | Supported by both Enterprise Edition VPN and Classic VPN | Yes                 |


| Metric Name   | Support                                  | Enabled by Default?  |
|---|--|--|
| <ul style="list-style-type: none"><li>• Average Link RTT</li><li>• Maximum Link RTT</li><li>• Link Packet Loss Rate</li><li>• Packet Receive Rate</li><li>• Packet Send Rate</li><li>• Traffic Receive Rate</li><li>• Traffic Send Rate</li><li>• SA Packet Receive Rate</li><li>• SA Packet Send Rate</li><li>• SA Traffic Receive Rate</li><li>• SA Traffic Send Rate</li></ul> | Supported only by Enterprise Edition VPN | No<br>You can click the name of a VPN connection and add a health check item on the <b>Summary</b> tab page.                         |
| <ul style="list-style-type: none"><li>• Average Tunnel RTT</li><li>• Maximum Tunnel RTT</li><li>• Tunnel Packet Loss Rate</li></ul>   | Supported only by Enterprise Edition VPN | Yes<br>Private network monitoring metrics are supported only when a VPN connection uses the static routing mode and has NQA enabled. |

## Viewing VPN Connection Metrics

- Viewing metrics on the VPN console
  - a. Log in to the management console.
  - b. Click  in the upper left corner and select the desired region and project.
  - c. Click **Service List** and choose **Networking > Virtual Private Network**.
  - d. Choose **Virtual Private Network > Enterprise – VPN Connections**.
  - e. Click  to view VPN connection information.



Only the VPN connection status can be viewed. For other metrics, [view them on the Cloud Eye console](#).

You can view data of the last 1, 3, 12, or 24 hours, or last 7 days.
- Viewing metrics on the Cloud Eye console

- a. Log in to the management console.
- b. Click  in the upper left corner and select the desired region and project.
- c. Click **Service List** and choose **Management & Governance > Cloud Eye**.
- d. Choose **Cloud Service Monitoring > Virtual Private Network**.
- e. Click the **S2C VPN Connection** tab, locate the target VPN connection, and click **View Metric** in the **Operation** column.

You can view data of the last 1, 3, 12, or 24 hours, or last 7 days.

## Viewing VPN Gateway Metrics

- Viewing metrics on the VPN console (recommended)
  - a. Log in to the management console.
  - b. Click  in the upper left corner and select the desired region and project.
  - c. Click **Service List** and choose **Networking > Virtual Private Network**.
  - d. Choose **Virtual Private Network > Enterprise – VPN Gateways**.
  - e. Locate the target VPN connection, and click the **View Metric** icon in the **Gateway IP Address** column.
- Viewing metrics on the Cloud Eye console
  - a. Log in to the management console.
  - b. Click  in the upper left corner and select the desired region and project.
  - c. Click **Service List** and choose **Management & Governance > Cloud Eye**.
  - d. Choose **Cloud Service Monitoring > Virtual Private Network**.
  - e. On the **S2C VPN Gateway** tab page, locate the target VPN gateway, and click **View Metric** in the **Operation**.


You can view data of the last 1, 3, 12, or 24 hours, or last 7 days.

## 5.4 Creating Alarm Rules

### Scenarios

You can configure alarm rules on the Cloud Eye console to keep track of your VPN status at any time.

### Procedure

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 **Management & Governance > Cloud Eye**.

4. Choose **Cloud Service Monitoring > Virtual Private Network**, locate the target VPN connection, and click **Create Alarm Rule** in the **Operation** column.

For VPN, configure alarm rules on the **Dedicated Connections** tab page.

- By default, VPN does not provide any alarm templates. You need to click **Create Custom Template** to create a template first. Then, choose **Cloud Service Monitoring > Virtual Private Network** and click **Create Alarm Rule** to configure an alarm rule.

5. Click **Create**.

After the alarm rule is created, if you have enabled **Alarm Notification** and configured required parameters, you will receive notifications once an alarm is triggered.

 **NOTE**

For more information about VPN alarm rules, see the [Cloud Eye User Guide](#).

# 6 Audit

## 6.1 VPN Operations That Can Be Recorded by CTS

**Table 6-1** Enterprise Edition VPN operations that can be recorded by CTS



| Operation                             | Resource Type    | Trace Name          |
|---------------------------------------|------------------|---------------------|
| Creating a customer gateway           | customer-gateway | createCgw           |
| Updating a customer gateway           | customer-gateway | updateCgw           |
| Deleting a customer gateway           | customer-gateway | deleteCgw           |
| Creating a VPN gateway                | vpn-gateway      | createVgw           |
| Updating a VPN gateway                | vpn-gateway      | updateVgw           |
| Deleting a VPN gateway                | vpn-gateway      | deleteVgw           |
| Creating a yearly/monthly VPN gateway | vpn-gateway      | CreatePrePaidVgw    |
| Updating the VPN gateway status       | vpn-gateway      | UpdateResourceState |
| Creating a VPN connection             | vpn-connection   | createVpnConnection |
| Updating a VPN connection             | vpn-connection   | updateVpnConnection |

| Operation                 | Resource Type  | Trace Name          |
|---------------------------|----------------|---------------------|
| Deleting a VPN connection | vpn-connection | deleteVpnConnection |

## 6.2 Querying CTS Traces

When CTS is enabled, the system starts recording operations performed on VPN resources. You can view the operation records of the last seven days on the CTS management console.

### Procedure

- Step 1** Log in to the management console.
- Step 2** In the navigation pane on the left, click  and choose **Management & Governance > Cloud Trace Service**.
- Step 3** In the navigation pane, choose **Trace List**.
- Step 4** Specify the search criteria as needed.
  - **Search time range:** In the upper right corner, select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
  - **Trace Type, Trace Source, Resource Type, and Search By:** Select a filter from the drop-down list.
    - If you select **Resource ID** for **Search By**, specify a resource ID.
    - If you select **Data** for **Trace Type**, you can only filter traces by tracker.
  - **Operator:** Select one or more operators from the drop-down list.
  - **Trace Status:** Select one of **All trace statuses**, **Normal**, **Warning**, and **Incident**.
- Step 5** Click **Query**.
- Step 6** Click  on the left of a trace to expand its details.
- Step 7** Click **View Trace** in the **Operation** column to view detailed content of a trace.

----End

# 7 Permissions Management

---

## 7.1 Creating a User and Granting VPN Permissions

This topic describes how to use [IAM](#) to implement fine-grained permissions control for your VPN resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing VPN resources.
- Grant only the permissions required for users to perform a specific task.
- Grant the permission to perform professional and efficient O&M on your VPN resources to other Huawei Cloud accounts or cloud services.

If your Huawei Cloud account does not need individual IAM users, skip this topic.

This section describes the procedure for granting permissions (see [Figure 7-1](#)).

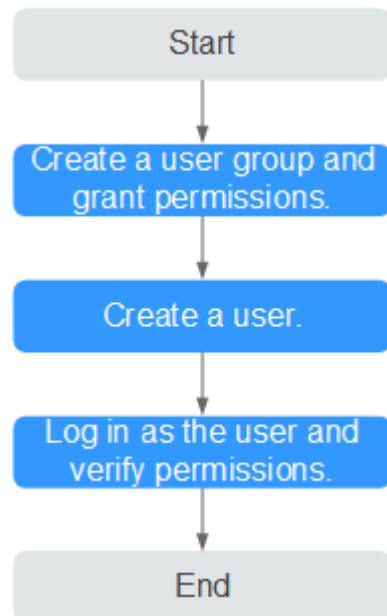
### Prerequisites

Learn about the permissions (see [Permissions Management](#)) supported by VPN and choose policies or roles based on your requirements. For system permissions of other cloud services, see [System Permissions](#).



## Process Flow

**Figure 7-1** Process for granting VPN permissions



1. **Create a user group and assign permissions** to it.  
Create a user group on the IAM console and attach the **VPN Administrator** policy to the group.
2. **Create an IAM user** and add it to a user group.  
Create a user on the IAM console and add the user to the group created in **1**.
3. **Log in** and verify permissions.  
Log in to the management console as the created user. Switch to the authorized region and verify the permissions.
  - Click **Service List** and choose **Networking > Virtual Private Network**. On the **Enterprise - VPN Gateways** page, click **Buy VPN Gateway** in the upper right corner. If the VPN gateway is successfully created, the **VPN Administrator** policy has already taken effect.
  - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **VPN Administrator** policy has already taken effect.

## 7.2 VPN Custom Policies

Custom policies can be created to supplement the system-defined policies of VPN.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). The following section contains examples of common VPN custom policies.

## Example VPN custom policy

- Example 1: Allowing users to delete VPN gateways

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpn:vpnGateways:delete"
      ]
    }
  ]
}
```

- Example 2: Denying users to delete a VPN connection

A policy with only Deny permissions must be used in conjunction with other policies to take effect. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used if you need to assign permissions of the **VPN FullAccess** policy to a user but also forbid the user from deleting VPN connections. Create a custom policy for denying VPN connection deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on VPN except deleting VPN connections. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "vpn:vpnGateways:delete"
      ]
    }
  ]
}
```

- Example 3: defining multiple actions in a policy

A custom policy can contain actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpn:vpnGateways:create",
        "vpn:vpnConnections:create",
        "vpn:customerGateways:create"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "vpn:vpnGateways:delete",
        "vpn:vpnConnections:delete",
        "vpn:customerGateways:create"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "vpc:vpcs:list",

```

```
    "vpc:subnets:get"  
  }  
]  
}
```

# 8 Quotas

---

## What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

## Resource Types

- VPN resources include VPN gateways, VPN connection groups, and customer gateways.

The total quota of each resource type varies according to regions.