Virtual Private Network

User Guide

Issue 01

Date 2024-03-27

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

1 Enterprise Edition VPN Gateway Management

1.1 Creating a VPN Gateway

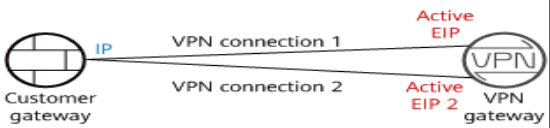
Scenario

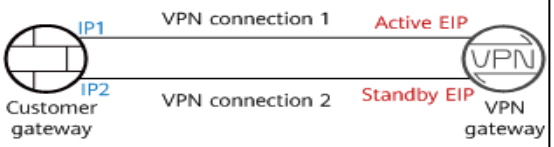
To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a VPN gateway before creating a VPN connection.

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		It is recommended that the VPN gateway uses the active-active mode. In this case, one VPN connection group is used.

Number of Customer Gateway IP Addresses	Recommended Networking	Description
2		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.

Notes and Constraints

- A VPN gateway of a non-GM specification cannot be changed to a VPN gateway of the GM specification.
- When an enterprise router is associated, pay attention to the upper limit of entries in the routing table of the enterprise router.
- Access via non-fixed IP addresses is available only for some regions. This function is supported only when **Billing Mode** is set to **Yearly/Monthly** and **Network Type** is set to **Public network**.

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**.
- An enterprise router has been created if you want to use it to connect to a VPN gateway. For details, see the enterprise router documentation.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select the desired region and project.

Step 3 On the homepage, choose **Networking** > **Virtual Private Network**.

Step 4 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.

Step 5 On the **VPN Gateways** page, click **Buy VPN Gateway**.

Step 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	• **Yearly/Monthly**: 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. • **Pay-per-use**: VPN gateways and VPN connection groups are billed by usage duration, and the billing cycle is 1 hour.	Yearly/Monthly Pay-per-use
Region	For low network latency and fast resource access, select the region nearest to your target users. Resources cannot be shared across regions.	AP-Singapore
Name	Specifies the name of a VPN gateway. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	vpngw-001
Network Type	• **Public network**: A VPN gateway establishes VPN connections through the Internet. • **Private network**: A VPN gateway establishes VPN connections through a private network.	Public network

Parameter	Description	Example Value
Associate With	• VPC Through a VPC, the VPN gateway sends messages to the customer gateway or servers in the local subnet. • Enterprise Router Through an enterprise router, the VPN gateway sends messages to the customer gateway or servers in the subnets of all VPCs connected to the enterprise router. **NOTE** In this scenario, pay attention to the upper limit of entries in the routing table of the enterprise router. If the number of routes advertised by the customer gateway and VPN gateway exceeds this upper limit, the enterprise router cannot learn the excess routes. As a result, traffic will fail to be forwarded between the VPN gateway and the customer gateway.	VPC
VPC	This parameter is available only when **Associate With** is set to **VPC**. Select a VPC.	vpc-001(192.168.0.0/16)
Enterprise Router	This parameter is available only when **Associate With** is set to **Enterprise Router**. Select an enterprise router.	er-001
Interconnection Subnet	This parameter is available only when **Associate With** is set to **VPC**. 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	This parameter is available only when **Associate With** is set to **VPC**. VPC subnets with which your on-premises data center needs to communicate through the customer gateway. • Select subnet Select subnets of the local VPC. • Enter CIDR block Enter subnets of the local VPC or subnets of the VPC that establishes a peering connection with the local VPC.	192.168.1.0/24,192.168.2.0/24
BGP ASN	BGP ASN of the VPN gateway, which must be different from that of the customer gateway.	64512

Parameter	Description	Example Value
Specification	Three options are available: **Professional 1**, **Professional 2**, and **GM**. Professional 1 and Professional 2 support access via non-fixed IP addresses only when **Billing Mode** is **Yearly/Monthly** and **Network Type** is set to **Public network**. For details about differences between these specifications, see **Specifications**.	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. • If two or more AZs are available, select two AZs. The VPN gateway deployed in two AZs has higher availability. You are advised to select the AZs where resources in the VPC are located. • If only one AZ is available, select this AZ.	AZ1, AZ2
VPN Connection Groups	This parameter is available only when **Billing Mode** is set to **Yearly/Monthly**. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway. • If an on-premises data center has only one egress gateway, all servers or user hosts in the data center connect to the Internet through this gateway. In this case, you need to configure a VPN connection group consisting of two VPN connections. That is, configure a VPN connection for each of the two EIPs of the VPN gateway to communicate with the egress gateway in the on-premises data center. • If an on-premises data center has two egress gateways, the servers or user hosts in the data center connect to the Internet through the two egress gateways. In this case, you need to configure two VPN connection groups, each of which consisting of two VPN connections. That is, configure a VPN connection for each of the two EIPs of each VPN gateway to communicate with both egress gateways in the on-premises data center.	10

Parameter	Description	Example Value
HA Mode	• **Active-active**: 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. • **Active/Standby**: 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.	Active-active
Active EIP	This parameter is available only when **Network Type** is set to **Public network**. EIP used by the VPN gateway to communicate with a customer gateway. • **Create Now**: Buy a new EIP. The billing mode of the new EIP is the same as that of the VPN gateway. • **Use existing**: Use an existing EIP. This EIP can share bandwidth with the EIPs of other network services.	Create Now
Billed By	This parameter is available only when **Billing Mode** is set to **Pay-per-use** and **Network Type** is set to **Public network**. A pay-per-use VPN gateway can be billed by bandwidth or by traffic. • **Bandwidth**: You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth. • **Traffic**: You need to specify a bandwidth limit and pay for the outbound traffic sent from your VPC.	Traffic

Parameter	Description	Example Value
Bandwidth (Mbit/s)	This parameter is available only when **Network Type** is set to **Public network** and **Active EIP** is set to **Create Now**. Bandwidth of the EIP, in Mbit/s. ● 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. 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. ● You can configure alarm rules on Cloud Eye to monitor the bandwidth. ● You can customize the bandwidth within the allowed range. ● Some regions support only 300 Mbit/s bandwidth by default. If higher bandwidth is required, apply for 300 Mbit/s bandwidth and then **submit a service ticket** for capacity expansion.	10 Mbit/s
Bandwidth Name	This parameter is available only when **Network Type** is set to **Public network**. EIP bandwidth name.	Vpngw-bandwidth1
Active EIP 2	This parameter is available only when the **Network Type** is set to **Public network** and **HA Mode** is set to **Active-active**. 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.	Create Now

Parameter	Description	Example Value
Standby EIP	This parameter is available only when the **Network Type** is set to **Public network** and **HA Mode** is set to **Active/Standby**. 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. **NOTE** When **Billing Mode** of the VPN gateway is **Pay-per-use** and the backup EIP is billed by traffic, you are advised to configure alarm rules on Cloud Eye to monitor the backup EIP. This prevents traffic fee overrun caused by VPN connection switching due to a fault of the active VPN connection. For details about how to configure alarm rules on Cloud Eye, see **Creating an Alarm Rule**.	Create Now
Billed By	This parameter is available only when **Billing Mode** is set to **Pay-per-use** and **Network Type** is set to **Public network**. A pay-per-use VPN gateway can be billed by bandwidth or by traffic. • **Bandwidth**: You need to specify a bandwidth limit and pay for the amount of time you use the bandwidth. • **Traffic**: You need to specify a bandwidth limit and pay for the outbound traffic sent from your VPC.	Traffic

Parameter	Description	Example Value
Bandwidth (Mbit/s)	This parameter is available only when **Network Type** is set to **Public network** and **Active EIP 2** or **Standby EIP** is set to **Create Now**. Bandwidth of the EIP, in Mbit/s. • 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. 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. • You can configure alarm rules on Cloud Eye to monitor the bandwidth. • You can customize the bandwidth within the allowed range. • Some regions support only 300 Mbit/s bandwidth by default. If higher bandwidth is required, apply for 300 Mbit/s bandwidth and then **submit a service ticket** for capacity expansion.	10 Mbit/s
Bandwidth Name	This parameter is available only when **Network Type** is set to **Public network**. EIP bandwidth name.	Vpngw-bandwidth2
Enterprise Project	Enterprise project to which the VPN belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The default project is **default**. For details about how to create and manage enterprise projects, see the *Enterprise Management User Guide*.	default

Parameter	Description	Example Value
Advanced Settings	Parameters under **Advanced Settings** are available only when **Network Type** is set to **Private network** and **Associate With** is set to **VPC**. • **Select**: This option applies to the scenario where VPCs of the same tenant are connected. Select the access VPC, access subnet, and gateway IP address of the current tenant. • **Enter**: This option applies to the scenario where a VPC of the current tenant is connected to that of another tenant. Enter the access project, access domain, access VPC, and access subnet of the other tenant.	Select
Access Project	This parameter is available only when you select **Enter** for **Advanced Settings**. Enter an access project ID. For details about how to obtain the project ID, see **How Do I Obtain an Enterprise Project ID**.	*Set this parameter based on the site requirements.*
Access Domain	This parameter is available only when you select **Enter** for **Advanced Settings**. Enter an access domain ID. For details about how to obtain the domain ID, see **Viewing or Modifying IAM User Information**.	*Set this parameter based on the site requirements.*
Access VPC	• This parameter is available only when **Associate With** is set to **Enterprise Router**. • This parameter is available only when **Associate With** is set to **VPC** and **Network Type** is set to **Private network**. 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.	Same as the associated VPC
Access Subnet	• This parameter is available only when **Associate With** is set to **Enterprise Router**. • This parameter is available only when **Associate With** is set to **VPC** and **Network Type** is set to **Private network**. 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

Parameter	Description	Example Value
Gateway IP Address	This parameter is available only when **Network Type** is set to **Private network**. • Self-assigned IP address (default) An IP address on the access subnet will be automatically assigned to the VPN gateway. You can view the automatically assigned IP address on the **VPN Gateways** page. • Manually-specified IP address Manually configure IP addresses on the access subnet for the VPN gateway. When you select **Select** for **Advanced Settings**, you can click **View In-Use IP Address** on the right to check the IP addresses in use. The refresh and fuzzy search functions are supported in the **View In-Use IP Address** dialog box. When **HA Mode** is set to **Active/Standby** for the VPN gateway, enter the active and standby IP addresses in sequence. When **HA Mode** is set to **Active-active** for the VPN gateway, enter the active IP address and active IP address 2 in sequence.	Self-assigned IP address
Tag	Specifies the identifier of a VPN resource. The value consists of a key and a value. A maximum of 20 tags can be added. You can select predefined tags or customize tags. To view predefined tags, click **View predefined tags**.	-
Required Duration	This parameter is available only when **Billing Mode** is set to **Yearly/Monthly**. If your account balance is sufficient and you select **Auto-renew**, the system automatically renews your service when the required duration elapses. • Monthly subscription: Your service is automatically renewed on a per-month basis. • Yearly subscription: Your service is automatically renewed on a per-year basis.	6

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

Step 8 (Optional) For a VPN gateway of the GM specification, upload the VPN gateway certificate after the VPN gateway is created. Otherwise, the VPN gateway cannot set up a VPN connection.

For details, see **Uploading Certificates for a VPN Gateway**.

----End

1.2 Viewing a VPN Gateway

Scenario

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. On the homepage, 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 a VPN gateway of the public network type, you can view the basic information and EIPs. If the VPN gateway specification is **Professional 1: non-fixed IP address** or **Professional 2: non-fixed IP address**, you can also view the policy template configuration.
   - For VPN gateways of the private network type, you can view the basic information and advanced settings.
   - For VPN gateways of the GM specification, you can view the basic information and certificate information.

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

Scenario

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

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

1.4 Modifying the Specification of a Yearly/Monthly VPN Gateway

Scenario

If the specification of a yearly/monthly VPN gateway of the public network type is **Professional 1** or **Professional 2**, you can upgrade the specification to enable the VPN gateway to support access via non-fixed IP addresses.

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 homepage, 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** > **Modify Specifications** in the **Operation** column.
6. Modify the gateway specification as prompted.

1.5 Modifying the Policy Template of a VPN Gateway

Scenario

If the specification of a VPN gateway is **Professional 1: non-fixed IP address** or **Professional 2: non-fixed IP address**, you can modify the policy template for 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. On the homepage, 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 **View/Modify Policy Template** in the **Operation** column. On the **Policy Template** tab page, click **Modify Policy Template** to modify the policy template.

   NOTE

   After the policy template is modified, the customer gateway with a non-fixed IP address must update the corresponding configuration (requiring manual modification) and connect to the VPN gateway again. Otherwise, the connection will be interrupted.

Table 1-3 Description of policy template parameters

Parameter		Description	Support for Modification
IKE Policy	Version	Version of the IKE protocol. The supported version is **v2**.	×
	Authentication Algorithm	Hash algorithm used for authentication. The following options are available: ● SHA2-256 ● SHA2-384 ● SHA2-512 The default algorithm is **SHA2-256**.	√
	Encryption Algorithm	Encryption algorithm. The following options are available: ● AES-256-GCM-16 ● AES-128(Insecure. Not recommended.) ● AES-192(Insecure. Not recommended.) ● AES-256(Insecure. Not recommended.) The default value is **AES-128**.	√

Parameter		Description	Support for Modification
	DH Algorithm	The following algorithms are supported: ● Group 14(Insecure. Not recommended.) ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 The default value is **Group 15**.	√
	Lifetime (s)	Lifetime of a security association (SA). An SA will be renegotiated when its lifetime expires. ● Unit: second ● Value range: **60** to **604800** The default value is **86400**.	√
	Local ID	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. By default, EIPs of the VPN gateways are used.	×
IPsec Policy	Authentication Algorithm	Hash algorithm used for authentication. The following options are available: ● SHA2-256 ● SHA2-384 ● SHA2-512 The default algorithm is **SHA2-256**.	√

Parameter		Description	Support for Modification
	Encryption Algorithm	Encryption algorithm. The following options are available: ● AES-256-GCM-16 ● AES-128(Insecure. Not recommended.) ● AES-192(Insecure. Not recommended.) ● AES-256(Insecure. Not recommended.) The default value is **AES-128**.	√
	PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: ● DH group 14(Insecure. Not recommended.) ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 ● Disable The default value is **DH group 15**.	√
	Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. Currently, ESP is supported.	×
	Lifetime (s)	Lifetime of an SA. An SA will be renegotiated when its lifetime expires. ● Unit: second ● Value range: **30** to **604800** The default value is **3600**.	√

6. Click **OK**.

1.6 Binding an EIP to a VPN Gateway

Scenario

You can bind EIPs 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. On the homepage, 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 click **Bind EIP** in the **Operation** column.
   - If the VPN gateway uses the active-active mode, the VPN gateway can have active EIP and active EIP 2 bound.
   - If the VPN gateway uses the active/standby mode, the VPN gateway can have an active EIP and a standby EIP bound.
6. Select the desired EIP and click **OK**.

1.7 Unbinding an EIP from a VPN Gateway

Scenario

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

Notes and Constraints

An EIP that is in use by a VPN connection cannot be unbound from a 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. On the homepage, 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 active EIP and active EIP 2 can be unbound from the VPN gateway.
   - If the VPN gateway uses the active/standby mode, the active EIP and standby EIP can be unbound from the VPN gateway.

6. In the displayed dialog box, click **Yes**.

   NOTE

   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.

1.8 Unsubscribing from a Yearly/Monthly VPN Gateway

Scenario

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

Notes and Constraints

- You can unsubscribe from a VPN gateway only when it is in normal state.
- 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. On the homepage, 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.

1.9 Renewing a Yearly/Monthly VPN Gateway

Scenario

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. On the homepage, 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.

1.10 Deleting a Pay-per-Use VPN Gateway

Scenario

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

Notes and Constraints

- The delete operation is not supported for a VPN gateway that is being created, updated, or 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 **3.5 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 **1.7 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. On the homepage, 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** > **Delete** in the **Operation** column.
6. In the displayed dialog box, click **Yes**.

1.11 Uploading Certificates for a VPN Gateway

Scenario

When creating a VPN gateway of the GM specification, you need to upload certificates for it to establish VPN connections with a customer gateway. In

addition, configure the alarm function on the Cloud Eye console for such a VPN gateway. For details, see **Creating an Alarm Rule to Monitor an Event**.

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 homepage, 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 a VPN gateway of the GM specification, and choose **More** > **View/Upload Certificate** in the **Operation** column.
6. Click **Upload Certificate** and set parameters as prompted.

   Table 1-4 describes the parameters for uploading certificates for a VPN gateway.

   Table 1-4 Parameters for uploading certificates for a VPN gateway

Parameter	Description	Example Value
Certificate Name	User-defined name.	certificate-001
Signature Certificate	Certificate used for signature authentication to ensure data validity and non-repudiation. Open the PEM signature certificate file (with the extension .pem) as a text file, and copy the content in the file to this text box. Enter both a signature certificate and its issuing CA certificate.	-----BEGIN CERTIFICATE----- *Signature certificate* -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- *CA certificate* -----END CERTIFICATE-----
Signature Private Key	Private key used to decrypt the data that is encrypted by a signature certificate. Open the signature private key file (with the extension .key) as a text file, and copy the private key to this text box.	-----BEGIN EC PRIVATE KEY----- *Signature private key* -----END EC PRIVATE KEY-----

Parameter	Description	Example Value
Encryption Certificate	Certificate used to encrypt data transmitted over VPN connections to ensure data confidentiality and integrity. The CA that issues the encryption certificate must be the same as the CA that issues the signature certificate. Open the PEM encryption certificate file (with the extension .pem) as a text file, and copy the content in the file to this text box.	-----BEGIN CERTIFICATE----- *Encryption certificate* -----END CERTIFICATE-----
Encryption Private Key	Private key used to decrypt the data that is encrypted by an encryption certificate. Open the encryption private key file (with the extension .key) as a text file, and copy the private key to this text box.	-----BEGIN EC PRIVATE KEY----- *Encryption private key* -----END EC PRIVATE KEY-----

1.12 Replacing Certificates of a VPN Gateway

Scenario

When certificates of a VPN gateway of the GM specification expire or become invalid, you need to replace the certificates.

After certificates of a VPN gateway are replaced, the customer gateway must use the corresponding new CA certificate to renegotiate with the VPN gateway. Otherwise, VPN connections will be disconnected.

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 homepage, 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 a VPN gateway of the GM specification, and choose **More** > **View/Upload Certificate** in the **Operation** column.
6. Click **Replace** and set parameters as prompted.

Table 1-5 describes the parameters for replacing certificates of a VPN gateway.

Table 1-5 Parameters for replacing certificates of a VPN gateway

Parameter	Description	Example Value
Certificate Name	This parameter cannot be modified.	The value must be the same as the original certificate name.
New Signature Certificate	Certificate used for signature authentication to ensure data validity and non-repudiation. Open the PEM signature certificate file (with the extension .pem) as a text file, and copy the content in the file to this text box. Enter both a signature certificate and its issuing CA certificate.	-----BEGIN CERTIFICATE----- *Signature certificate* -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- *CA certificate* -----END CERTIFICATE-----
New Signature Private Key	Private key used to decrypt the data that is encrypted by a signature certificate. Open the signature private key file (with the extension .key) as a text file, and copy the private key to this text box.	-----BEGIN EC PRIVATE KEY----- *Signature private key* -----END EC PRIVATE KEY-----
New Encryption Certificate	Certificate used to encrypt data transmitted over VPN connections to ensure data confidentiality and integrity. The CA that issues the encryption certificate must be the same as the CA that issues the signature certificate. Open the PEM encryption certificate file (with the extension .pem) as a text file, and copy the content in the file to this text box.	-----BEGIN CERTIFICATE----- *Encryption certificate* -----END CERTIFICATE-----

Parameter	Description	Example Value
New Encryption Private Key	Private key used to decrypt the data that is encrypted by an encryption certificate. Open the encryption private key file (with the extension .key) as a text file, and copy the private key to this text box.	-----BEGIN EC PRIVATE KEY----- *Encryption private key* -----END EC PRIVATE KEY-----

7. Select "I have read and understand the preceding risk, and would like to replace the certificates anyway." and click **OK**.

1.13 Searching for VPN Gateways by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the VPN console.

Prerequisites

You have added tags to VPN resources. For details, see **Adding Tags to Cloud Resources**.

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 homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click **Search by Tag** in the upper right corner, select the desired tag key and value, and click **Search**.
   - You can only select keys and values from the drop-down lists.
   - You can add a maximum of 20 tags to search for VPN resources.

2 Customer Gateway Management of Enterprise Edition VPN

2.1 Creating a Customer Gateway

Scenario

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.

Notes and Constraints

- The identifier of a customer gateway that uses SM series cryptographic algorithms can only be a gateway IP address, which must be a static IP address.
- A customer gateway identified by a full qualified domain name (FQDN) supports VPN connections only in policy template mode.

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 homepage, 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 **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	Specifies the name of a customer gateway. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	cgw-001
Identifier	• **IP Address**: Specify the IP address of the customer gateway. • **FQDN**: Enter an FQDN. The value is a string of 1 to 128 case-sensitive characters, including letters, digits, and special characters (excluding & < > [ ] \). Spaces are not supported. If the customer gateway does not have a fixed IP address, select **FQDN**. Ensure that UDP port 4500 is permitted in a firewall rule on the customer gateway in your on-premises data center or private network.	• IP Address, 1.2.3.4 • FQDN, cgw-fqdn
BGP ASN	This parameter is available only when **Identifier** is set to **IP Address**. Enter the ASN of your on-premises data center or private network. The BGP ASN of the customer gateway must be different from that of the VPN gateway.	65000
CA certificate (optional)	For a customer gateway that uses SM series cryptographic algorithms, you need to upload a CA certificate for it to establish VPN connections with a VPN gateway. • To upload a new certificate, manually enter a value starting with -----BEGIN CERTIFICATE----- and ending with **-----END CERTIFICATE-----**. • To use an uploaded certificate, select the certificate. Pay attention to the time when the certificate will expire.	-----BEGIN CERTIFICATE----- *CA certificate* -----END CERTIFICATE-----
Tag	Specifies the identifier of a VPN resource. The value consists of a key and a value. A maximum of 20 tags can be added. You can select predefined tags or customize tags. To view predefined tags, click **View predefined tags**.	-

7. (Optional) If there are two customer gateways, repeat the preceding operations to configure the other customer gateway with a different identifier.

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

Scenario

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. On the homepage, 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, identifier, ID, BGP ASN, and VPN connection of the customer gateway.
   - In the **CA Certificate** area, you can view the certificate SN, signature algorithm, expiration time, issuer, and subject, and add or replace the CA certificate. (If the customer gateway uses SM series cryptographic algorithms, you need to add a CA certificate.)

2.3 Modifying a Customer Gateway

Scenario

After creating a customer gateway, you can modify its name. For a customer gateway that uses SM series cryptographic algorithms, you can also add or replace its CA certificate.

For details about how to add or replace a CA certificate, see **2.5 Uploading a Certificate for a Customer Gateway** and **2.6 Replacing the Certificate of 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. On the homepage, 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

Scenario

You can delete a customer gateway that you have created.

Notes and Constraints

Before deleting a customer gateway associated with a VPN connection, remove the customer gateway from the 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. On the homepage, 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.
6. Click **Yes**.

2.5 Uploading a Certificate for a Customer Gateway

Scenario

For a customer gateway that uses SM series cryptographic algorithms, you need to upload a CA certificate for it to establish VPN connections with a 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. On the homepage, 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 the name of the target customer gateway.
6. In the **CA Certificate** area, click **Add**.

7. Set parameters and click **OK**.

   Table 2-2 describes the parameters for uploading a CA certificate for a customer gateway.

   Table 2-2 Parameters for uploading a CA certificate for a customer gateway

Parameter	Description	Example Value
Upload a certificate	CA certificate of the customer gateway.	-----BEGIN CERTIFICATE----- *CA certificate* -----END CERTIFICATE-----
Use an uploaded certificate	Select an uploaded certificate. Pay attention to the time when the certificate will expire.	-

2.6 Replacing the Certificate of a Customer Gateway

Scenario

When the CA certificate of a customer gateway that uses SM series cryptographic algorithms expires or becomes invalid, you need to replace the CA certificate.

After the CA certificate is replaced, the customer gateway needs to use the SM certificate issued based on the new CA certificate to renegotiate with the VPN gateway. Otherwise, VPN connections will be disconnected.

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 homepage, 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 the name of the target customer gateway.
6. In the **CA Certificate** area, click **Replace**.
7. Set parameters as prompted.

   Table 2-3 describes the parameters for replacing the CA certificate of a customer gateway.

Table 2-3 Parameters for replacing the CA certificate of a customer gateway

Parameter	Description	Example Value
Upload a certificate	CA certificate of the customer gateway.	-----BEGIN CERTIFICATE----- *CA certificate* -----END CERTIFICATE-----
Use an uploaded certificate	Select an uploaded certificate. Pay attention to the time when the certificate will expire.	-

8. Select "I have read and understand the preceding risk, and would like to replace the CA certificate anyway." and click **OK**.

2.7 Searching for Customer Gateways by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the VPN console.

Prerequisites

You have added tags to VPN resources. For details, see **Adding Tags to Cloud Resources**.

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 homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. Click **Search by Tag** in the upper right corner, select the desired tag key and value, and click **Search**.
   - You can only select keys and values from the drop-down lists.
   - You can add a maximum of 20 tags to search for VPN resources.

3 Enterprise Edition VPN Connection Management

3.1 Creating a VPN Connection

Scenario

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.

Notes and Constraints

- When creating a VPN connection in static routing mode, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection before enabling NQA. Otherwise, traffic will fail to be forwarded.
- When creating a VPN connection in policy-based mode and adding multiple policy rules, ensure that the source and destination CIDR blocks in the rules do not overlap. Otherwise, data flows may be incorrectly matched or IPsec tunnels may flap.

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 homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connection** 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 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	Specifies the name of a VPN connection. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created. You can also click **Create VPN Gateway** to create a VPN gateway. For details about related parameters, see **Table 1-2**. If you use a VPN gateway of the GM specification and no certificate has been bound to the VPN gateway, click **Upload Certificate** to upload certificates. Otherwise, VPN connections cannot be set up.	vpngw-001
Gateway IP Address	IP address of the VPN gateway. 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. You can also click **Create Customer Gateway** to create a customer gateway. For details about related parameters, see **Table 2-1**. If you use a customer gateway that supports SM series cryptographic algorithms and no CA certificate has been bound to the customer gateway, upload a CA certificate by referring to **2.5 Uploading a Certificate for a Customer Gateway**. Otherwise, VPN connections cannot be set up. **NOTE** 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	IPsec connection mode, which can be route-based or policy-based. • Static routing Determines the data that enters the IPsec VPN tunnel based on the route configuration (local subnet and customer subnet). **Application scenario: Communication between customer gateways** • BGP routing Determines the traffic that can enter the IPsec VPN tunnel based on BGP routes. **Application scenario: Communication between customer gateways + Many or frequently changed interconnection subnets or backup between VPC and Direct Connect** • Policy-based 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. **Application scenario: Isolation between customer gateways** • Policy template The VPN gateway passively responds to the IPsec connection requests from the customer gateway. After authenticating the customer gateway, the VPN gateway accepts the policy rules defined on the customer gateway based on source and destination CIDR blocks. **Application scenario: The customer gateway uses a non-fixed IP address.**	Static routing

Parameter	Description	Example Value
Customer Subnet	Customer-side subnet that needs to access the VPC on the cloud through VPN connections. If there are multiple customer subnets, separate them with commas (,). **NOTE** • The customer subnet can overlap with the local subnet but cannot be the same as the local subnet. • A customer subnet cannot be included in the existing subnets of the VPC associated with the VPN gateway. It also cannot be the destination address in the route table of the VPC associated with the VPN gateway. • Customer subnets cannot be the reserved CIDR blocks of VPCs, for example, 100.64.0.0/10 or 214.0.0.0/8.	172.16.1.0/24,172.16.2.0/24

Parameter	Description	Example Value
Interface IP Address Assignment	This parameter is available only when **VPN Type** is set to **Static routing** or **BGP routing**. **NOTE** • Set interface IP addresses to the tunnel interface IP addresses used by the VPN gateway and customer gateway to communicate with each other. • If the tunnel interface address of the customer gateway is fixed, select **Manually specify**, and set the tunnel interface address of the VPN gateway based on the tunnel interface address of the customer gateway. • Manually specify Set **Local Interface IP Address** 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 **Customer Interface IP Address** to a random value based on the setting of **Local Interface IP Address**. For example, when you set **Local Interface IP Address** to **169.254.1.6/30**, the system automatically sets the **Customer Interface IP Address** to **169.254.1.5/30**. • Automatically assign By default, an IP address on the 169.254.x.x/30 CIDR block is assigned to the tunnel interface of the VPN gateway. To view the automatically assigned local and customer interface IP addresses, click **Modify VPN Connection** on the **VPN Connections** page.	Automatically assign

Parameter	Description	Example Value
Local Tunnel Interface Address	This parameter is available only when **Interface IP Address Assignment** is set to **Manually specify**. Tunnel interface IP address configured on the VPN gateway.	N/A
Customer Tunnel Interface Address	This parameter is available only when **Interface IP Address Assignment** is set to **Manually specify**. Tunnel interface IP address configured on the customer gateway device.	N/A
Link Detection	This parameter is available only when **VPN Type** is set to **Static routing**. **NOTE** 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. After this function is enabled, the VPN gateway automatically performs Network Quality Analysis (NQA) on the customer interface IP address of the customer gateway. For details about NQA, see **Huawei Cloud VPN NQA**.	Selected
PSK	The PSKs configured for the VPN gateway and customer gateway must be the same. The PSK: • Contains 8 to 128 characters. • Can contain only three or more types of the following characters: – Digits – Uppercase letters – Lowercase letters – Special characters: ~ ! @ # $ % ^ ( ) - _ + = { } , . / : ; **NOTE** This parameter is not available for VPN connections set up using SM series cryptographic algorithms.	Test@123

Parameter	Description	Example Value
Confirm PSK	Enter the PSK again. **NOTE** This parameter is not available for VPN connections set up using SM series cryptographic algorithms.	Test@123
Policy	This parameter is available only when **VPN Type** is set to **Policy-based**. 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. • Source CIDR Block The source CIDR block must contain some CIDR blocks of the local subnets. **0.0.0.0/0** indicates any IP address. • Destination CIDR Block 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 (,).	• Source CIDR block 1: 192.168.1.0/24 • Destination CIDR block 1: 172.16.1.0/24,172.16.2.0/24 • Source CIDR block 2: 192.168.2.0/24 • Destination CIDR block 2: 172.16.1.0/24,172.16.2.0/24
Policy Settings	• **Default**: Use default IKE and IPsec policies. • **Custom**: Use custom IKE and IPsec policies. For details about the policies, see **Table 3-2** and **Table 3-3**.	Custom
Policy Template	Configure the policy template only when **VPN Type** is set to **Policy template**. The policy template cannot be modified here. For details about the modification, see **1.5 Modifying the Policy Template of a VPN Gateway**.	-

Parameter	Description	Example Value
Tag	Specifies the identifier of a VPN resource. The value consists of a key and a value. A maximum of 20 tags can be added. You can select predefined tags or customize tags. To view predefined tags, click **View predefined tags**.	-

Table 3-2 IKE policy

Parameter	Description	Example Value
Version	Version of the IKE protocol. The value can be one of the following: • v1 (v1 has low security. If the device supports v2, v2 is recommended.) The IKE version can only be **v1** for VPN connections set up using SM series cryptographic algorithms. • v2 The default value is **v1** for VPN connections set up using SM series cryptographic algorithms. The default value is **v2** for VPN connections that are not set up using SM series cryptographic algorithms.	v2
Negotiation Mode	This parameter is available only when **Version** is **v1**. • Main Only **Main** is available if a VPN gateway of the GM specification is selected. • Aggressive	Main

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following options are available: • SHA1(Insecure. Not recommended.) • MD5(Insecure. Not recommended.) • SHA2-256 • SHA2-384 • SHA2-512 • SM3 This authentication algorithm is available only for VPN connections set up using an SM series cryptographic algorithm. In this case, the IKE version can only be **v1**. The default value is **SM3** for VPN connections set up using SM series cryptographic algorithms. The default value is **SHA2-256** for VPN connections that are not set up using SM series cryptographic algorithms.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following options are available: • 3DES(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-256(Insecure. Not recommended.) • AES-256-GCM-16 When this encryption algorithm is used, the IKE version can only be **v2**. • SM4 This encryption algorithm is available only for VPN connections set up using an SM series cryptographic algorithm. In this case, the IKE version can only be **v1**. The default value is **SM4** for VPN connections set up using SM series cryptographic algorithms. The default value is **AES-128** for VPN connections that are not set up using SM series cryptographic algorithms.	AES-128

Parameter	Description	Example Value
DH Algorithm	The following algorithms are supported: • Group 1(Insecure. Not recommended.) • Group 2(Insecure. Not recommended.) • Group 5(Insecure. Not recommended.) • Group 14(Insecure. Not recommended.) • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 The default value is **Group 15**. **NOTE** This parameter is not available for VPN connections set up using SM series cryptographic algorithms.	Group 14
Lifetime (s)	Lifetime of a security association (SA). An SA will be renegotiated when its lifetime expires. • Unit: second • The value ranges from **60** to **604800**. • The default value is **86400**.	86400

Parameter	Description	Example Value
Local ID	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. • IP Address (default value) The system automatically sets this parameter to the selected EIP of the VPN gateway. • FQDN Set the FQDN to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). **NOTE** This parameter is not available for VPN connections set up using SM series cryptographic algorithms.	IP Address
Customer ID	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. • IP Address (default value) The system automatically sets this parameter to the IP address of the customer gateway. • FQDN Set the FQDN to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces). **NOTE** This parameter is not available for VPN connections set up using SM series cryptographic algorithms.	IP Address

Table 3-3 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following options are available: • SHA1(Insecure. Not recommended.) • MD5(Insecure. Not recommended.) • SHA2-256 • SHA2-384 • SHA2-512 • SM3 Select this authentication algorithm for VPN connections set up using SM series cryptographic algorithms. The default value is **SM3** for VPN connections set up using SM series cryptographic algorithms. The default value is **SHA2-256** for VPN connections that are not set up using SM series cryptographic algorithms.	SHA2-256

Parameter	Description	Example Value
Encryption Algorithm	Encryption algorithm. The following options are available: • 3DES(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-256(Insecure. Not recommended.) • AES-128-GCM-16 • AES-256-GCM-16 • SM4 This encryption algorithm is used only by VPN connections set up using SM series cryptographic algorithms. The default value is **SM4** for VPN connections set up using SM series cryptographic algorithms. The default value is **AES-128** for VPN connections that are not set up using SM series cryptographic algorithms.	AES-128

Parameter	Description	Example Value
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: ● Disable(Insecure. Not recommended.) ● DH group 1(Insecure. Not recommended.) ● DH group 2(Insecure. Not recommended.) ● DH group 5(Insecure. Not recommended.) ● DH group 14(Insecure. Not recommended.) ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 The default value is **DH group 15**. **NOTE** ● This parameter is not available for VPN connections set up using SM series cryptographic algorithms. ● When a VPN gateway and customer gateway use an SM series cryptographic algorithm to set up VPN connections, ensure that the PFS function is disabled on the customer gateway. Otherwise, VPN connections cannot be set up.	DH group 15
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: ● ESP The default value is **ESP**.	ESP

Parameter	Description	Example Value
Lifetime (s)	Lifetime of an SA. An SA will be renegotiated when its lifetime expires. • Unit: second • The value ranges from **30** to **604800**. • The default value is **3600**.	3600
Packet Encapsulation Mode	The default value is **TUNNEL**.	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 algorithms: 3DES, AES-128, AES-192, and AES-256

  Because some customer devices do not support secure encryption algorithms, the default encryption algorithm of VPN connections is still AES-128. You are advised to use a more secure encryption algorithm if customer devices support secure encryption algorithms.
- 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 Configuring Health Check

Scenario

After VPN connections are created, you can configure health check to enable the VPN gateway to send probe packets to the customer gateway to collect statistics about the round-trip time and packet loss rate of physical links. The statistics help you learn about the VPN connection quality. The Cloud Eye service monitors the round-trip time and packet loss rate of VPN links. For details, see **Metrics**.

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 homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connection** page, click the name of the target VPN connection. On the **Summary** tab page, click **Add** in the **Health Check** area.
6. In the **Add Health Check** dialog box, click **OK**.

3.3 Viewing a VPN Connection

Scenario

After creating a VPN connection, 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. On the homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connection** page, view the VPN connection list.
6. 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.

  Check the value of **VPN Connection Status**. If the value is **0**, the VPN connection is not connected. If the value is **1**, the VPN connection is connected. If the value is **2**, the VPN connection status is not reported in the last 180 seconds.

3.4 Modifying a VPN Connection

Scenario

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

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. On the homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connection** page, locate the VPN connection to modify, and click **Modify VPN Connection** or **Modify Policy Settings**.
6. Modify VPN connection parameters as prompted.

   For VPN connections in policy template mode, you can modify the policy settings on the **VPN Gateways** page, instead of on the **VPN Connection** page. For details, see **1.5 Modifying the Policy Template of a VPN Gateway**.
7. 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	• When IKEv1 is used, the new setting takes effect in the next negotiation period. • When IKEv2 is used, the new setting takes effect after the VPN connection is re-established. **NOTE** This parameter is not available for VPN connections set up using SM series cryptographic algorithms.	• When IKEv1 is used: Locate the VPN connection to modify, choose **More** > **Reset PSK** on the right, and change the PSK as prompted. • When IKEv2 is used: 1. Delete the current VPN connection. 2. Create a new VPN connection.

<table>
<tr><th>Item</th><th>Parameter</th><th>When New Settings Take Effect</th><th>How to Modify</th></tr>
<tr><td rowspan="8">IKE policy (IKEv1)</td><td>Encryption Algorithm</td><td rowspan="7">The new settings take effect in the next negotiation period.
NOTE
• The following parameters cannot be modified for VPN connections set up using SM series cryptographic algorithms: Encryption Algorithm, Authentication Algorithm, and Negotiation Mode.
• The following parameters are not available for VPN connections set up using SM series cryptographic algorithms: DH Algorithm, Local ID, and Customer ID.</td><td rowspan="8">Locate the VPN connection to modify, and click Modify VPN Configuration.</td></tr>
<tr><td>Authentication Algorithm</td></tr>
<tr><td>DH Algorithm</td></tr>
<tr><td>Negotiation Mode</td></tr>
<tr><td>Local ID</td></tr>
<tr><td>Customer ID</td></tr>
<tr><td>Lifetime (s)</td></tr>
<tr><td>Version</td><td>The new settings take effect immediately.
NOTE
This parameter is not available for VPN connections set up using SM series cryptographic algorithms.</td></tr>
<tr><td rowspan="5">IKE policy (IKEv2)</td><td>Encryption Algorithm</td><td rowspan="4">The new settings take effect in the next negotiation period.</td><td rowspan="5">Locate the VPN connection to modify, and click Modify VPN Configuration.</td></tr>
<tr><td>Authentication Algorithm</td></tr>
<tr><td>DH Algorithm</td></tr>
<tr><td>Lifetime (s)</td></tr>
<tr><td>Version</td><td>The new settings take effect immediately.</td></tr>
</table>

Item	Parameter	When New Settings Take Effect	How to Modify
	Local ID	The new settings take effect after the VPN connection is re-established.	1. Delete the current VPN connection. 2. Create a new VPN connection.
	Customer ID		
IPsec policy	Encryption Algorithm	The new settings take effect in the next negotiation period. **NOTE** • **Encryption Algorithm** and **Authentication Algorithm** cannot be modified for VPN connections set up using SM series cryptographic algorithms. • The **PFS** parameter is not available for VPN connections set up using SM series cryptographic algorithms.	Locate the VPN connection to modify, and click **Modify VPN Configuration**.
	Authentication Algorithm		
	PFS		
	Lifetime (s)		
	Transfer Protocol	Currently, this parameter cannot be modified on the management console.	

3.5 Deleting a VPN Connection

Scenario

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. On the homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. On the **VPN Connection** page, choose **More** > **Delete** in the **Operation** column of a VPN connection.
6. In the displayed dialog box, click **Yes**.

3.6 Searching for VPN Connections by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the VPN console.

Prerequisites

You have added tags to VPN resources. For details, see **Adding Tags to Cloud Resources**.

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 homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. Click **Search by Tag** in the upper right corner, select the desired tag key and value, and click **Search**.
   - You can only select keys and values from the drop-down lists.
   - You can add a maximum of 20 tags to search for VPN resources.

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. On the homepage, choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the target 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. On the **Change Subscription** page that is displayed, confirm the information about the VPN gateway and configure the 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. On the homepage, 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

Notes and Constraints

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. On the homepage, 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 Classic VPN Gateway Management

5.1 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** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
5. View information about your VPN gateway.

5.2 Modifying a VPN Gateway

1. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
2. Click **OK**.

Modifying Basic Information About a VPN Gateway

Scenario

You can modify the name and description of a 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** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
5. Locate the row that contains the VPN gateway that you want to modify, and choose **More** > **Modify Basic Information** in the **Operation** column.
6. Modify the VPN gateway name or description as required.

   NOTE

   The name of a VPN gateway can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
7. Click **OK**.

Modifying VPN Gateway Bandwidth

Scenario

When the bandwidth of a VPN gateway cannot meet your service requirements, you can modify the VPN gateway bandwidth.

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** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
5. On the **VPN Gateways** page, locate the row that contains the target VPN gateway and choose **More** > **Modify Bandwidth** in the **Operation** column.
6. Modify the bandwidth as required.
7. Click **Submit**.

5.3 Deleting a Pay-per-Use VPN Gateway

Scenarios

If a VPN gateway is no longer required, you can delete it to release network resources as long as it has no VPN connections configured.

If it has any connections configured, delete the connections first.

NOTE

If you create a pay-per-use VPN gateway, a VPN connection will be created together with the gateway. If you delete all VPN connections created for a pay-per-use VPN gateway, the VPN gateway will be automatically deleted. For details, see **6.3 Deleting 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. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
4. 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**.

6 Classic VPN Connection Management

6.1 Viewing a VPN Connection

Scenarios

After creating a VPN connection, 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** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic** and click the **VPN Connections** tab.
5. View the VPN connection information. You can also locate the row that contains the target VPN connection, and click **View Policy** in the **Operation** column to view IKE and IPsec policy details of the VPN connection.

6.2 Modifying a VPN Connection

Scenarios

A VPN connection is an encrypted communications channel established between the VPN gateway in your VPC and that in an on-premises data center. The VPN connection can be modified after creation.

CAUTION

If you modify the advanced settings, network communications may be interrupted. Exercise caution when performing this operation.

Modifying the PSK only will not delete the current VPN connection. The new PSK takes effect during IKE renegotiation after the IKE lifetime expires.

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** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic** and click the **VPN Connections** tab.
5. Locate the row that contains the target VPN connection, and click **Modify** in the **Operation** column.
6. In the displayed **Modify VPN Connection** dialog box, modify parameters as required.

   NOTE

   The name of a VPN gateway can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
7. Click **OK**.

6.3 Deleting a VPN Connection

Scenarios

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

When you delete the last VPN connection of a pay-per-use VPN gateway, the associated VPN gateway will also be deleted.

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** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic** and click the **VPN Connections** tab.

5. Locate the row that contains the target VPN connection, and choose **More** > **Delete** in the **Operation** column.
6. In the displayed dialog box, click **Yes**.

7 Classic VPN Management (LA-Mexico City1/LA-Sao Paulo1)

7.1 Viewing Purchased VPNs

Scenarios

You can view details about an existing VPN.

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. On the displayed **Virtual Private Network** page, view the target VPN. **Table 7-1** describes the VPN status.

Table 7-1 VPN status

Status	Description
Normal	The VPN is successfully created, and the on-premises data center can access the VPC properly.
Not connected	The VPN is successfully created but has not been used for communication with the on-premises data center.
Creating	The VPN is being created.
Updating	VPN information is being updated.
Deleting	The VPN is being deleted.
Abnormal	The VPN is abnormal.
Frozen	The VPN is frozen.

7.2 Modifying a Purchased VPN

Scenarios

If VPN network information conflicts with VPC network information or needs to be adjusted based on the latest network environment, you can modify the VPN.

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. On the **Virtual Private Network** page, locate the target VPN and click **Modify**.
5. In the displayed dialog box, modify parameters as required.
6. Click **OK**.

7.3 Deleting a VPN

Scenarios

You can delete a VPN if it is no longer required.

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. On the **Virtual Private Network** page, locate the target VPN and click **Delete**.
5. In the displayed dialog box, click **Yes**.

8 Classic VPN Fee Management

8.1 Changing a Pay-Per-Use VPN Gateway from Being Billed by Bandwidth to Being Billed by Traffic or the Other Way Around

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** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic** and click the **VPN Gateways** tab.
5. On the **VPN Gateways** page, locate the row that contains the target VPN gateway.
6. Choose **More** > **Modify Bandwidth** in the **Operation** column.
7. On the **Modify Bandwidth** page, set **Billed By** to **Bandwidth** in the **Modify Specifications** area.
8. Click **Submit**.

9 Monitoring

9.1 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.

9.2 Metrics (Enterprise Edition VPN)

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 9-1 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.	≥ 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.	≥ 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.	≥ 0	Gateway	1 minute

Table 9-2 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

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
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
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	Status of a VPN connection: **0**: not connected **1**: connected **2**: unknown	0, 1, or 2	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.	0~1G bit/s	VPN connection	1 minute
send_rate	Traffic Send Rate	Average volume of traffic sent per second.	0~1G bit/s	VPN connection	1 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
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
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.	0~1G bit/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.	0~1G bit/s	SA of a VPN connection	1 minute

Dimensions

key	Value
evpn_connection_id	S2C VPN Connection
evpn_sa_id	S2C VPN Connection - S2C VPN Connection SA
evpn_gateway_id	S2C VPN Gateway

9.3 Metrics (Classic VPN)

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 9-3 Metrics supported for Classic VPN gateways

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic (previously called "Upstream Bandwidth"). Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic (previously called "Downstream Bandwidth"). Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage of outbound bandwidth, in percentage. Outbound bandwidth usage = Outbound bandwidth/Purchased bandwidth	0-100%	Bandwidth or EIP	1 minute
downstream_bandwidth_usage	Inbound Bandwidth Usage	Usage of inbound bandwidth, in percentage. Inbound bandwidth usage = Inbound bandwidth/Purchased bandwidth **NOTE** • Up to 10 Mbit/s inbound bandwidth is provided by Huawei Cloud for some sites that purchase an inbound bandwidth of less than 10 Mbit/s. As such, the inbound bandwidth usage may be greater than 100%. • If you change the bandwidth of an EIP in use, there is a delay of 5–10 minutes for the metrics to update for the new bandwidth.	0-100%	Bandwidth or EIP	1 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
up_stream	Outbound Traffic	Outbound network traffic (previously called "Upstream Traffic") Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute
down_stream	Inbound Traffic	Inbound network traffic (previously called "Downstream Traffic") Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute

Table 9-4 Metrics supported for Classic VPN connections

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
connection_status	VPN Connection Status	Status of a VPN connection: **0**: not connected **1**: connected	0 or 1	VPN connection	5 minutes

Dimensions

key	Value
vpn_connection_id	VPN Connections

9.4 Viewing Metrics

Scenarios

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

Support for Metrics

Table 9-5 Support for metrics

Metric Name	Support	Enabled by Default?
VPN Connection Status	Supported by both Enterprise Edition VPN and Classic VPN	Yes
• Average Link RTT • Maximum Link RTT • Link Packet Loss Rate • Packet Receive Rate • Packet Send Rate • Traffic Receive Rate • Traffic Send Rate • SA Packet Receive Rate • SA Packet Send Rate • SA Traffic Receive Rate • SA Traffic Send Rate	Supported only by Enterprise Edition VPN	No You can click the name of a VPN connection and add a health check item on the **Summary** tab page.
• Average Tunnel RTT • Maximum Tunnel RTT • Tunnel Packet Loss Rate	Supported only by Enterprise Edition VPN	Yes 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**.

   For Classic VPN, choose **Virtual Private Network** > **Classic**, and click the **VPN Connections** tab.

e. Click  to view VPN connection information.

   For Classic VPN, locate the target VPN connection, and choose **Operation** > **View Metric**.

   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.

     For Classic VPN, click the **VPN Connections** 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**.

     For Classic VPN, choose **Virtual Private Network** > **Classic**, and click the **VPN Gateways** tab.

  e. Locate the target VPN connection, and click the **View Metric** icon in the **Gateway IP Address** column.

     For Classic VPN, locate the target VPN gateway, and click **View Metric** in the **Operation** column to view the IP monitoring data of the VPN gateway.

     You can view data of the last 1, 3, 12, or 24 hours, or a customized time range.

- 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.

9.5 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. For Classic VPN, configure alarm rules on the **VPN 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.
   - By default, Classic VPN provides an alarm template named **Virtual Private Network Alarm Template**. You can use this default template without creating a new one.

     If the alarm policy in the default alarm template does not meet your requirements, you can create a custom alarm template by clicking **Create Custom Template**. 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**.

10 Audit

10.1 VPN Operations That Can Be Recorded by CTS

NOTE

Cloud Trace Service (CTS) is not supported in LA-Mexico City1 and LA-Sao Paulo1 regions.

Table 10-1 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

Operation	Resource Type	Trace Name
Updating a VPN connection	vpn-connection	updateVpnConnection
Deleting a VPN connection	vpn-connection	deleteVpnConnection
Uploading a gateway certificate	vgw-certificate	createVgwCertificate
Replacing a gateway certificate	vgw-certificate	updateVgwCertificate
Creating a resource tag	instance	createResourceTag
Deleting a resource tag	instance	deleteResourceTag

Table 10-2 Classic VPN operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a VPN connection	VpnConnection	createVpnConnection
Updating a VPN connection	VpnConnection	updateVpnConnection
Deleting a VPN connection	VpnConnection	deleteVpnConnection
Creating a VPN gateway	VpnGw	createVpnGw
Updating a VPN gateway	VpnGw	updateVpnGw
Deleting a VPN gateway	VpnGw	deleteVpnGw

10.2 Querying CTS Traces

After you enable CTS and the management tracker is created, CTS starts recording operations performed on VPN resources. You can view the operation records in the last seven days on the CTS console.

For details about how to view audit logs, see **Querying Real-Time Traces**.

11 Permissions Management

11.1 Creating a User and Granting VPN Permissions

Use the **Identity and Access Management (IAM)** service to implement fine-grained permissions control over 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.

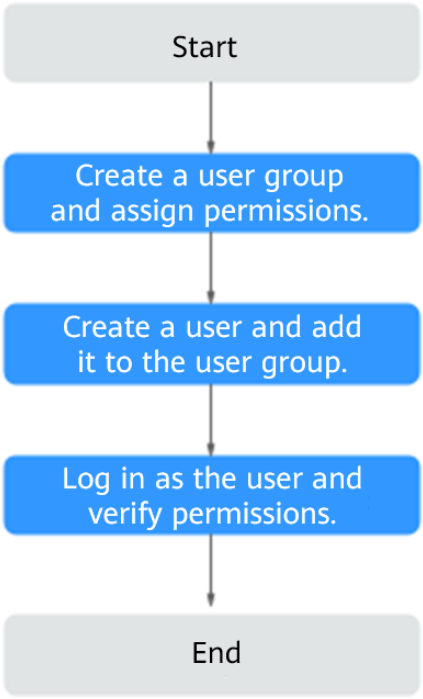
This section describes the procedure for granting permissions (see **Figure 11-1**).

Prerequisites

Learn about the permissions (see **Permissions Management**) supported by VPN and choose policies or roles based on your requirements. To grant permissions for other services, learn about all **system-defined permissions** supported by VPN.

Process Flow

Figure 11-1 Process of 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 a user and add it to the 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.

11.2 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: Grant permission to delete VPN gateways.

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

- Example 2: Deny VPN connection deletion.

  A policy with only "Deny" permissions must be used together with other policies. If the permissions granted to an IAM user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  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"
            ]
        }
    ]
}
```


12 Quotas

What Is a Quota?

Quotas put limits on the quantities and capacities 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

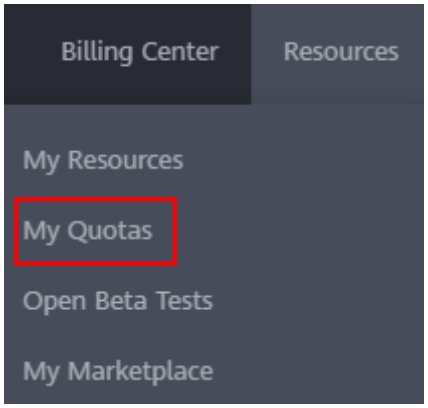
- Classic VPN resources include Classic VPN gateways and Classic VPN connections.
- VPN resources include VPN gateways, VPN connection groups, and customer gateways.

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

How Do I View My Quotas?

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

Figure 12-1 My Quotas



4. View the used and total quota of each type of resources on the displayed page.

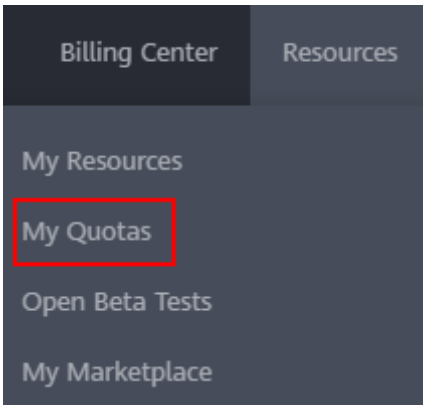
   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. Choose **Resources** > **My Quotas** in the upper right corner of the page.

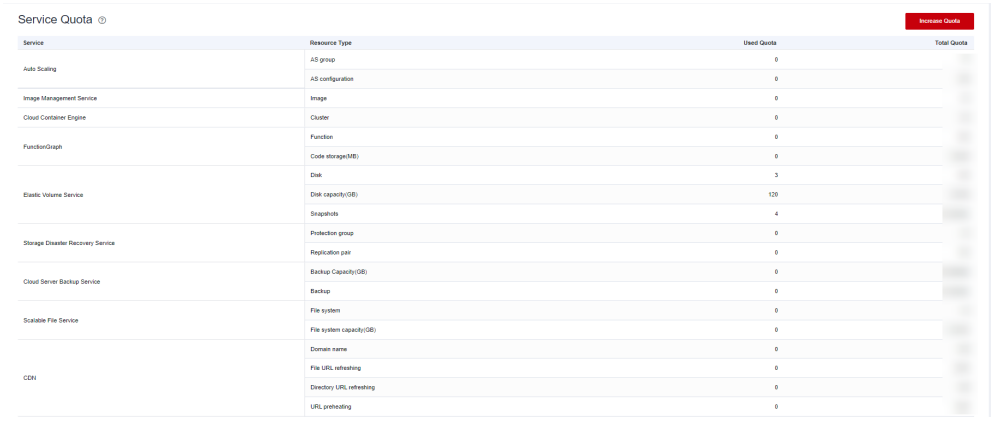
   The **Service Quota** page is displayed.

   Figure 12-2 My Quotas



3. Click **Increase Quota** in the upper right corner of the page.

   Figure 12-3 Applying for a higher quota



4. On the **Create Service Ticket** page, configure parameters as required.

   In the **Problem Description** area, enter the required quota and the reason for the quota adjustment.

5. Select the agreement and click **Submit**.

