Virtual Private Network

User Guide

Issue	01
Date	2025-07-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 S2C Enterprise Edition VPN

1.1 Enterprise Edition VPN Gateway Management

1.1.1 Creating a VPN Gateway

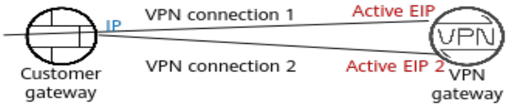
Scenario

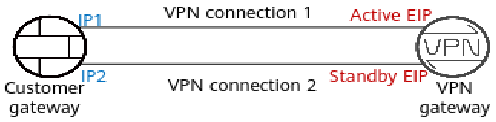
To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a VPN gateway before creating a VPN connection.

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	 IP VPN connection 1 Active EIP VPN Customer gateway VPN connection 2 Active EIP 2 VPN gateway	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	 IP1 VPN connection 1 Active EIP VPN IP2 Customer gateway VPN connection 2 Standby EIP VPN gateway	It is recommended that the VPN gateway uses the active/standby mode. In this case, two VPN connection groups are used.

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

Prerequisites

- A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.
- Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see **Security Group Rules**.
- 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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click **Buy S2C 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.	Ireland-Dublin
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. You are advised to select an AZ type based on the AZs where resources in the VPC are located. The following types of AZs are supported: ● General	*Set this parameter based on the site requirements.*
Name	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. When **AZ** is set to **HomeZones**, **Associate With** can only be set to **VPC**. ● 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**. Specify the 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
HA Mode	● Active-active – When **Associate With** is set to **VPC**, the outgoing traffic from the VPN gateway to the customer subnet is preferentially forwarded through the first VPN connection (VPN connection 1) set up between the customer subnet and an EIP. If VPN connection 1 fails, the outgoing traffic is automatically switched to the other VPN connection (VPN connection 2) set up with the customer subnet. After VPN connection 1 recovers, the outgoing traffic is still transmitted through VPN connection 2 and will not be switched back to VPN connection 1. – When **Associate With** is set to **Enterprise Router**, the outgoing traffic from the VPN gateway to the customer subnet is load balanced among all VPN connections set up with the customer subnet. ● Active/Standby The outgoing traffic from the VPN gateway to the customer subnet is preferentially transmitted through the VPN connection (VPN connection 1) set up between the customer subnet and the active EIP. If VPN connection 1 fails, the outgoing traffic is automatically switched to the other VPN connection (VPN connection 2) set up between the customer subnet and the standby EIP. After VPN connection 1 recovers, the outgoing traffic is automatically switched back to VPN connection 1.	Active-active
Specification	Two options are available: **Professional 1** and **Professional 2**.	Professional 1

Parameter	Description	Example Value
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
Bandwidth Name	This parameter is available only when **Network Type** is set to **Public network**. Specify the name of the EIP bandwidth. ● Bandwidth (Mbit/s): 5 ● When **Shared Bandwidth** is toggled on, you can select the name of the shared bandwidth. ● A maximum of 20 EIPs can be added to shared bandwidth. For details about how to apply for more quota, see **Increasing the Quota**.	Vpngw-bandwidth2

Parameter	Description	Example Value
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. **NOTE** When shared bandwidth is used, you can only use EIPs created now. ● **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**. Pay-per-use billing supports two billing modes: ● **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
Bandwidth (Mbit/s)	This parameter is available only when **Network Type** is set to **Public network**. 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.	10 Mbit/s

Parameter	Description	Example Value
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. **NOTE** When shared bandwidth is used, you can only create an EIP now, and the EIP cannot be changed after being created.	Create Now
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
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 **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, access subnet, and gateway IP address 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**. This parameter is supported only for some users.	*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**. This parameter is supported only for some users.	*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

Parameter	Description	Example Value
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
Gateway IP Address	This parameter is available only when **Associate With** is set to **VPC** and **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
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**.

----End

1.1.2 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. On the **S2C VPN Gateways** tab page, view the VPN gateway list.
6. Click the name of a VPN gateway to view its details.
   - For VPN gateways of the public network type, you can view their basic information, EIPs, tags, and routing information.
   - For VPN gateways of the private network type, you can view their basic information, advanced settings, and routing 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.

1.1.3 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the row that contains the target VPN gateway, and 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**.

Table 1-3 describes the parameters for modifying the VPN gateway.

Table 1-3 Parameters for modifying the VPN gateway

Parameter	Description	Modifiable or Not
Name	Name of a VPN gateway. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Y
EIP	To change an EIP, unbind it and bind a new one. If a VPN connection has been created for an EIP, the EIP cannot be unbound. **NOTE** ● Only the bandwidth size can be changed. ● The EIP name and type can be changed only on the EIP console.	Y
Local Subnet	VPC subnets with which your on-premises data center needs to communicate through the customer gateway.	Y
Billing Mode	The value can be **Yearly/ Monthly** or **Pay-per-use**.	Y
VPN Connection Groups	The number of VPN connection groups needs to be specified only when **Billing Mode** is set to **Yearly/ Monthly**.	Y
Region	For low network latency and fast resource access, select the region nearest to your target users. Resources cannot be shared across regions.	N

Parameter	Description	Modifiable or Not
Specification	Three options are available: **Basic**, **Professional 1** and **Professional 2**. Two options are available: **Professional 1** and **Professional 2**.	The supported specifications are subject to those displayed on the management console.
Associate With	The options include **VPC** and **Enterprise Router**.	N
Enterprise Router	The associated enterprise router needs to be specified only when **Associate With** is set to **Enterprise Router**.	N
VPC	VPC that the on-premises data center needs to access.	N
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	N
BGP ASN	BGP AS number.	N
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.	N

1.1.4 Changing the Specification of a VPN Gateway

Scenario

You can change the specification of a VPN gateway on the VPN gateway page. The following specification changes are subject to the console.

- The specification of a VPN gateway can be changed between Professional 1 and Professional 2.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the target VPN gateway, and choose **More** > **Change Specification** or click **Change Specification** in the **Operation** column.
6. Modify the gateway specification as prompted.

1.1.5 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the row that contains the target VPN gateway, and click **Bind EIP** in the **Operation** column.
   - If the VPN gateway uses the active-active mode, the VPN gateway can have an 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**.

1.1.6 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the row that contains the target VPN gateway, and click **Unbind EIP** or choose **More** > **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. Click **OK**.

   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.
   - The impact of shared bandwidth freezing on EIPs is subject to the EIP documentation. For details, see **Why My EIPs Are Frozen? How Do I Unfreeze My EIPs?**.

1.1.7 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the row that contains the target VPN gateway, and choose **More** > **Unsubscribe** in the **Operation** column.
6. Unsubscribe from the VPN gateway as prompted.

1.1.8 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the row that contains the target VPN gateway, and choose **More** > **Renew** or click **Renew** in the **Operation** column.
6. Complete the renewal as prompted.

1.1.9 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 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 **1.1.6 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the row that contains the VPN gateway to be deleted, and choose **More** > **Delete** in the **Operation** column.
6. Click **OK**.

NOTE

The impact of shared bandwidth freezing on EIPs is subject to the EIP documentation. For details, see **Why My EIPs Are Frozen? How Do I Unfreeze My EIPs?**.

1.1.10 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 management 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.

- You can only select existing keys and values from the drop-down list.
- You can select a maximum of 20 tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.
- You can use tags together with other types of filter criteria. The relationship between them is AND.

1.2 Customer Gateway Management of Enterprise Edition VPN

1.2.1 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

- Address groups cannot be used to configure the source and destination subnets in a policy on customer gateway devices.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ≡ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. On the **Customer Gateways** page, click **Create Customer Gateway**.
6. Set parameters as prompted and click **Create Now**.

   Table 1-4 lists the customer gateway parameters.

Table 1-4 Description of customer gateway parameters

Parameter	Description	Example Value
Name	Name of a customer gateway. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	cgw-001

Parameter	Description	Example Value
Identifier	● **IP Address**: Specify the IP address of the customer gateway. 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	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
Advanced Settings > Tags	Tag 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.

1.2.2 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. On the **Customer Gateways** page, 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.

1.2.3 Modifying a Customer Gateway

Scenario

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. On the **Customer Gateways** page, click ✎ next to the name of a customer gateway.
6. Enter a new name for the customer gateway and click **OK**.

   Table 1-5 describes the parameters related to customer gateway modification.

   Table 1-5 Parameters related to customer gateway modification

Parameter	Description	Modifiable or Not
Name	Name of a VPN connection. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Y
BGP ASN	BGP AS number.	N
Gateway IP Address	IP address used by the customer gateway to communicate with the VPN gateway. The value must be a static address.	N

1.2.4 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. On the **Customer Gateways** page, locate the customer gateway to delete, and click **Delete** in the **Operation** column.
6. Click **OK**.

1.2.5 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 management 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.
   - You can only select existing keys and values from the drop-down list.
   - You can select a maximum of 20 tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.
   - You can use tags together with other types of filter criteria. The relationship between them is AND.

1.3 Enterprise Edition VPN Connection Management

1.3.1 Creating VPN Connections

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.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connection** page, click **Create VPN Connection**.

   NOTE

   A VPN gateway can establish two VPN connections with a customer gateway using EIPs, improving reliability.
6. Set parameters as prompted and click **Buy Now**.

   Table 1-6 lists the VPN connection parameters.

Table 1-6 Description of VPN connection parameters

Parameter	Description	Example Value
Name	VPN connection name. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	vpn-001

Parameter	Description	Example Value
VPN Gateway	Name of the VPN gateway for which VPN connections are created. You can also click **Create VPN Gateway** to create a VPN gateway. For details about related parameters, see **Table 1-2**.	vpngw-001
VPN Gateway IP of Connection 1	● When **Network Type** is set to **Public network**, the value is the active EIP of the VPN gateway. ● When **Network Type** is set to **Private network**, the value is the active IP address of the VPN gateway. The same address of a VPN gateway cannot be repeatedly selected when you create VPN connections between the VPN gateway and the same customer gateway.	11.xx.xx.11
Customer Gateway of Connection 1	Select the customer gateway of connection 1. You can also click **Create Customer Gateway** to create a customer gateway. For details about related parameters, see **Table 1-4**. **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 Gateway IP of Connection 2	- When **Network Type** is set to **Public network** and **HA Mode** is set to **Active-active**, the value is active EIP 2 of the VPN gateway. - When **Network Type** is set to **Private network** and **HA Mode** is set to **Active-active**, the value is active IP address 2 of the VPN gateway. - When **Network Type** is set to **Public network** and **HA Mode** is set to **Active/Standby**, the value is the standby EIP of the VPN gateway. - When **Network Type** is set to **Private network** and **HA Mode** is set to **Active/Standby**, the value is the standby IP address of the VPN gateway. The VPN gateway IP address must be unique for each connection with a customer gateway.	11.xx.xx.12
Customer Gateway of Connection 2	Select the customer gateway of connection 2. You can also click **Create Customer Gateway** to create a customer gateway. For details about related parameters, see **Table 1-4**. **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 changing interconnection subnets, or backup between VPN 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** **NOTE** By default, the VPN type, customer subnet, branch interconnection setting (BGP routing mode), and policy rules (policy-based mode) of the two connections are the same.	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. ● If the interconnection subnet is associated with an ACL rule, ensure that the ACL rule permits the TCP port for traffic between all local and customer subnets. ● Address groups cannot be used to configure the source and destination subnets in a policy on customer gateway devices.	172.16.1.0/24,172.16.2.0/24
Branch Interconnection	This parameter is available only when **VPN Type** is set to **BGP routing**. ● Enabled ● Disabled This function is disabled by default. **NOTE** When this function is disabled, only local subnet routes are advertised.	Disabled

Parameter	Description	Example Value
Policy	This parameter is available only when **VPN Type** is set to **Policy-based**. Defines the data flow that enters the encrypted VPN connections 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. A maximum of five source CIDR blocks can be configured for a VPN connection. ● Destination CIDR Block The destination CIDR block must contain all the CIDR blocks of the customer subnets. A policy rule supports a maximum of 50 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
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, policies, and advanced settings for connection 1.	Set parameters based on the site requirements.

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 Tunnel Interface Address** to the tunnel interface address of the VPN gateway, which can reside only on the CIDR block 169.254.*x*.*x*/30 (except 169.254.195.*x*/30). Then, the system automatically sets **Customer Tunnel Interface Address** based on the value of **Local Tunnel Interface Address**. For example, when you set **Local Tunnel Interface Address** to **169.254.1.6/30**, the system automatically sets **Customer Tunnel Interface Address** to **169.254.1.5/30**. – When you set **VPN Type** to **BGP routing** and configure tunnel interface addresses in **Manually specify** mode, ensure that the local and remote tunnel interface addresses configured on the customer gateway device (the other end of the VPN connection) are the same as the values of **Customer Tunnel Interface Address** and **Local Tunnel Interface Address**, respectively. ● Automatically assign	Automatically assign

Parameter	Description	Example Value
	– By default, an IP address on the CIDR block 169.254.*x.x*/30 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 Connection** page. – When you set **VPN Type** to **BGP routing** and select **Automatically assign**, check the automatically assigned local and customer tunnel interface addresses after the VPN connection is created. Ensure that the local and remote tunnel interface addresses configured on the customer gateway device (the other end of the VPN connection) are the reverse of the settings on the cloud side.	
Local Tunnel Interface Address	This parameter is available only when **Interface IP Address Assignment** is set to **Manually specify**. Tunnel interface IP address of 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 of the customer gateway device.	N/A

Parameter	Description	Example Value
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.	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: ~ ! @ # $ % ^ ( ) - _ + = { } , . / : ;	Test@123
Confirm PSK	Enter the PSK again.	Test@123
Policy Settings	● **Default**: Use default IKE and IPsec policies. ● **Custom**: Use custom IKE and IPsec policies. For details about the policies, see **Table 1-7** and **Table 1-8**. **NOTE** When **Local ID** and **Customer ID** are set to **IP Address**, you can specify specific IP addresses as the local and customer IDs, which must be different.	Custom

Parameter	Description	Example Value
Tag	● Tag 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**.	-
Connection 2's Configuration	Determine whether to enable **Same as that of connection 1**. ● Enabled ● Disabled	Enabled

Table 1-7 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.) ● v2 The default value is **v2**.	v2
Negotiation Mode	This parameter is available only when **Version** is **v1**. ● Main ● Aggressive	Main
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 The default value is **SHA2-256**.	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 When this encryption algorithm is used, the IKE version can only be **v2**. The default value is **AES-128**.	AES-128
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**.	Group 15
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 peer 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 IP address of the VPN gateway. – You can configure a specific IP address as the local ID, which must be different from the customer ID.	IP Address
Customer ID	Authentication identifier of the customer gateway used in IPsec negotiation. The local ID configured on the customer gateway must be the same as the customer ID configured here. Otherwise, IPsec negotiation fails. ● **IP Address** (default) – The system automatically sets this parameter to the IP address of the customer gateway. – You can configure a specific IP address as the customer ID, which must be different from the local ID.	IP Address

Table 1-8 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 The default value is **SHA2-256**.	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 The default value is **AES-128**.	AES-128
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**.	DH group 15
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocol is 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

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**.

1.3.2 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.

5. On the **VPN 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**.

1.3.3 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connection** page, view the VPN connection list.
6. Click the name of a VPN connection to view its basic information, policy configuration, and tags.
   - When **VPN Type** is **Static routing**, the basic information includes the VPN connection information and health check information.
   - When **VPN Type** is **BGP routing**, the basic information includes the VPN connection information, health check information, and BGP peer information.
   - When **VPN Type** is **Policy-based**, the basic information includes the VPN connection information, policy rule information, and health check information.

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 unknown.

  Check the value of **BGP Peer State**. If the value is **0**, the BGP peer relationship has not been established. If the value is **1**, the BGP peer relationship has been established. If the value is **2**, the BGP peer relationship is in unknown state.
- In the VPN connection list, dual connections to the same customer gateway are identified by ┌└. If such dual connections are displayed on different pages, ┌ and └ are also displayed on different pages.

  The dual-connection identifier will be unavailable if you sort VPN connections by any field in the VPN connection list. The identifier will be restored after you cancel field-based sorting.
- In the VPN connection list, you can locate the target VPN connection and choose **More** > **View Logs** to view IPsec negotiation logs of the VPN connection.

  If a VPN connection is in **Not connected** state, you can determine the cause of the disconnection based on the VPN connection log details. If the log does not show any exception but the VPN connection is still not connected, **submit a service ticket** for Huawei technical support.

1.3.4 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN 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 a VPN connection in BGP routing mode, you can enable or disable branch Interconnection on the **Modify VPN Connection** page.
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 1-9**.

Table 1-9 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.	• 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.
IKEv1 policy	Encryption Algorithm	The new settings take effect in the next negotiation period.	Locate the VPN connection to modify, and click **Modify VPN Configuration**.
	Authentication Algorithm		
	DH Algorithm		
	Negotiation Mode		
	Local ID		
	Customer ID		
	Lifetime (s)		

Item	Parameter	When New Settings Take Effect	How to Modify
	Version	The new settings take effect immediately.	
IKEv2 policy	Encryption Algorithm	The new settings take effect in the next negotiation period.	Locate the VPN connection to modify, and click **Modify VPN Configuration**.
	Authentication Algorithm		
	DH Algorithm		
	Lifetime (s)		
	Version	The new settings take effect immediately.	
	Local ID	The new settings take effect after the VPN connection is re-established.	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.	Locate the VPN connection to modify, and click **Modify VPN Configuration**.
	Authentication Algorithm		
	PFS		
	Lifetime (s)		
	Transfer Protocol	This parameter cannot be modified on the management console.	

Table 1-10 describes the parameters related to VPN connection modification.

Table 1-10 Parameters related to VPN connection modification

Parameter	Description	Modifiable or Not
Name	VPN connection name. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Y
Customer Gateway	Gateway used for communicating with a VPC through VPN.	Y
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC on Huawei Cloud.	Y
Policy Settings	There are IKE and IPsec policies.	Y
PSK	The PSKs configured for the VPN gateway and customer gateway must be the same.	Y
Billing Mode	● **Yearly/Monthly**: You are billed by month or year. 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.	The billing mode can only be changed from pay-per-use to yearly/monthly.
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	Y
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	Y
Branch Interconnection	This parameter is available only when **VPN Type** is set to **BGP routing**.	Y
VPN Gateway	VPN gateway that has been created.	N

Parameter	Description	Modifiable or Not
Gateway IP Address	IP address used by the customer gateway to communicate with the VPN gateway. The value must be a static address. Ensure that UDP port 4500 is permitted in a firewall rule on the customer gateway in your on-premises data center or private network.	N
Interface IP Address Assignment	Mode in which IP addresses of the local and customer interfaces are assigned. The options include **Manually specify** and **Automatically assign**.	N
Link Detection	This function is used for route reliability detection in multi-link scenarios. **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, VPN traffic will fail to be forwarded.	N

1.3.5 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connection** page, locate the row that contains the target VPN connection, and choose **More** > **Delete**.

6. Click **OK**.

1.3.6 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 management 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. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.
   - You can only select existing keys and values from the drop-down list.
   - You can select a maximum of 20 tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.
   - You can use tags together with other types of filter criteria. The relationship between them is AND.

1.4 Enterprise Edition VPN Fee Management

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and 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 usage 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.

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

Procedure

1. Log in to the management console.
2. Click ⌖ in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the name of a VPN gateway.
6. Click the **Elastic IPs** tab, and click **Change** next to **Bandwidth (Mbit/s)**.
7. On the **Modify Bandwidth** page, select your required bandwidth and click **Next**.
8. Click **Pay Now**.
   - If the bandwidth is increased, the new bandwidth takes effect immediately after you pay the extra fees.

– If the bandwidth is decreased, the new bandwidth takes effect only within the renewal period.

1.4.3 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.
- The new VPN connection group quota cannot be less than the number of connection groups in use.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Locate the row that contains the target VPN gateway, and choose **More** > **Change VPN Connection Group Quota**.
6. On the **Change VPN Connection Group Quota** page, set a new number of VPN connection groups and click **Next**.
7. If you increase the quota, click **Pay Now** to pay the extra fee. If you decrease the quota, click **OK**.

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

2 P2C VPN

2.1 P2C VPN Gateway Management

2.1.1 Creating a VPN Gateway

Scenario

P2C VPN allows users to securely access applications and services deployed in a VPC from local terminals. To use P2C VPN, you need to create a VPN gateway first.

Limitations and Constraints

You can create a maximum of 50 VPN gateways.

Prerequisites

- A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.
- Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see **Security Group Rules**.

Procedure

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab, and then click **Buy P2C VPN Gateway**.

Step 6 Set parameters as prompted and click **Buy Now**.

Table 2-1 describes the VPN gateway parameters.

Table 2-1 Description of VPN gateway parameters

Parameter	Description	Example Value
Region	For low network latency and fast resource access, select the region nearest to your target users. Resources cannot be shared across regions.	*Set this parameter based on the actual condition.*
Name	Enter the name of a VPN gateway.	p2c-vpngw-001
VPC	Select a VPC.	vpc-001(192.168.0.0/16)
Interconnection Subnet	Specify the subnet used by the VPN gateway to access the VPC. Ensure that the selected interconnection subnet has three or more assignable IP addresses.	192.168.66.0/24
Specification	Only **Professional 1** is supported. ● Maximum bandwidth: 300 Mbit/s ● Maximum number of VPN connections: 500	Professional 1
AZ	An availability zone (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
Connections	Ten VPN connections are included free of charge with the purchase of a VPN gateway. You can select or customize the number of required VPN connections. **NOTE** If you set the number of VPN connections to 10, all the 10 connections are free of charge.	10

Parameter	Description	Example Value
EIP	Set the EIP used by the VPN gateway to communicate with clients. ● **Create now**: Buy a new EIP. The billing mode of a new EIP is yearly/monthly. ● **Use existing**: Use an existing EIP. Only EIPs with dedicated bandwidth are supported. **NOTE** If an existing EIP is used, its billing mode can be pay-per-use or yearly/monthly.	Create now
EIP Type	This parameter is available only when a new EIP is created. **Dynamic BGP**: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails. For more information about EIP types, see **What Is Elastic IP?**.	Dynamic BGP
Billed By	This parameter is available only when a new EIP is created. Pay-per-use billing includes two modes: billed by bandwidth and billed 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.	Bandwidth
Bandwidth (Mbit/s)	This parameter is available only when a new EIP is created. Specify the bandwidth of the EIP. ● 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.	20 Mbit/s

Parameter	Description	Example Value
Bandwidth Name	This parameter is available only when a new EIP is created. Specify the name of the EIP bandwidth.	p2c-vpngw-bandwidth1
Advanced Settings > Tags	● A tag identifies a VPN resource. It 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**.	-
Usage Duration	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

----End

2.1.2 Modifying a VPN Gateway

Scenario

After creating a VPN gateway, you can modify its basic information, including its name and bandwidth.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.

- To modify the name of a VPN gateway, click ✎ on the right of the VPN gateway name, modify the name, and click **OK**.

- To modify the bandwidth of the bound EIP, click the VPN gateway name, click **Modify** on the right of **Bandwidth (Mbit/s)** in the **EIP** area on the **Basic Information** tab page, modify the bandwidth, and confirm the price.

----End

2.1.3 Viewing a VPN Gateway

Scenario

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

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.

Step 6 Click the name of a VPN gateway to view its details.

- When the client authentication mode is certificate authentication, you can view the following details:
  - **Basic Information** tab page: You can view basic information about the VPN gateway and EIP.
  - **Server** tab page: You can view the basic information, authentication information, and advanced settings of the server.
  - **Connections** tab page: You can view information about the VPN connections established with the server, including the ID, virtual address, actual address, establishment time, number of incoming bytes, number of outgoing bytes, number of incoming data packets, and number of outgoing data packets.
  - **Tags** tab page: You can view and manage the keys and values of tags created for the VPN gateway.
- When the client authentication mode is password authentication (local), you can view the following details:
  - **Basic Information** tab page: You can view basic information about the VPN gateway and EIP.
  - **Server** tab page: You can view the basic information, authentication information, and advanced settings of the server.
  - **User Management** tab page: You can view the created users and user groups.
  - **Access Policies** tab page: You can view the gateway policy information, including the name/ID, user group, destination CIDR block, description, and update time.

- **Connections** tab page: You can view information about the VPN connections established with the server, including the ID, virtual address, actual address, username, establishment time, number of incoming bytes, number of outgoing bytes, number of incoming data packets, and number of outgoing data packets.
- **Tags** tab page: You can view and manage the keys and values of tags created for the VPN gateway.

----End

2.1.4 Unsubscribing from a VPN Gateway

Scenario

You can unsubscribe from a VPN gateway if it is no longer required.

Limitations and Constraints

- The unsubscription operation is not supported for a VPN gateway that is being created, updated, or unsubscribed.
- If a VPN gateway is bound to a pay-per-use EIP, the EIP will be 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 required, you can release it after unsubscribing from the gateway.
- Unsubscribing from a VPN gateway will interrupt its VPN connections immediately.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and choose **More** > **Unsubscribe** in the **Operation** column.

Step 6 Unsubscribe from the VPN gateway as prompted.

----End

2.1.5 Binding an EIP to a VPN Gateway

Scenario

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

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

Step 4 Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.

Step 5 Locate the row that contains the target VPN gateway, and choose **More** > **Bind EIP** in the **Operation** column.

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

NOTE

After you bind an EIP, download the client configuration again.

----End

2.1.6 Unbinding an EIP from a VPN Gateway

Scenario

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

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.

Step 6 Locate the row that contains the target VPN gateway, and choose **More** > **Unbind EIP** in the **Operation** column.

Step 7 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.

----End

2.1.7 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 management console.

Prerequisites

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

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.

Step 6 Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a key value.

- You can only select existing keys and values from the drop-down list.
- You can select a maximum of 20 tags to search for VPN resources. If you select multiple tags, the relationship between them is OR.
- You can use tags together with other types of filter criteria. The relationship between them is OR.

----End

2.2 P2C VPN Server Management

2.2.1 Configuring a Server

Scenario

A server provides configuration management and connection authentication capabilities. After a P2C VPN gateway is created, you need to complete the server configuration for it.

Prerequisites

The VPN gateway where a server is to be deployed has been created.

Limitations and Constraints

- You can configure a server only when the VPN gateway is in **Normal** state.
- A VPN gateway can have only one server associated.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. Then, click **Configure Server** in the **Operation** column of the target VPN gateway, or click the name of the target VPN gateway and click the **Server** tab.

Step 6 Set parameters as prompted and click **OK**.

Table 2-2 describes the server parameters.

Table 2-2 Server parameters

Area	Parameter	Description	Example Value
Basic Information	Local CIDR Block	Destination CIDR block that clients need to access through the P2C VPN gateway. The CIDR block can be within or connected to a Huawei Cloud VPC. A maximum of 20 local CIDR blocks can be specified. The local CIDR block cannot be set to 0.0.0.0. The local CIDR block cannot overlap or conflict with the following special CIDR blocks: 0.0.0.0/8, 224.0.0.0/4, 240.0.0.0/4, and 127.0.0.0/8. ● 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. **NOTE** After the local CIDR block is modified, clients need to be reconnected.	192.168.0.0/24

Area	Parameter	Description	Example Value
	Client CIDR Block	CIDR block for assigning IP addresses to virtual NICs of clients. It cannot overlap with the local CIDR block or the CIDR blocks in the route table of the VPC where the VPN gateway is located. The client CIDR block must be in the format of dotted decimal notation/mask. The mask ranges from 16 to 26. When assigning an IP address to a client, the system assigns a smaller CIDR block with the mask of 30 to ensure proper network communication. As such, ensure that the number of available IP addresses in the specified client CIDR block is at least four times the number of VPN connections. The recommended client CIDR blocks vary according to the number of VPN connections. For details, see **Table 2-3**. **NOTE** After the client CIDR block is modified, clients need to be reconnected.	172.16.0.0/16
	Tunnel Type	Secure Sockets Layer (SSL) is a transport layer protocol used to establish a secure channel between a client and a server. The value is fixed at **OpenVPN (SSL)**.	OpenVPN (SSL)
Authentication Information	Server Certificate	SSL certificate of the server. Clients use this certificate to verify the server's identity. ● To use an uploaded certificate, select it from the drop-down list box. ● To upload a new certificate, choose **Upload** from the drop-down list box to go to the Cloud Certificate Manager (CCM) service page. Upload a server certificate as prompted. For details, see **Uploading an External Certificate to SCM**. ● It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. **NOTE** If you delete the referenced server certificate in CCM after configuring the server, the availability of the server certificate is not affected.	*Set this parameter based on the actual condition.*

Area	Parameter	Description	Example Value
	Client Authentication Mode	Mode in which the server verifies the client identity. The options include **Certificate authentication** and **Password authentication (local)**. ● Select **Certificate authentication**. – Click **Upload CA Certificate**, open the CA certificate file in PEM format as a text file, and copy the certificate content to the **Content** text box in the **Upload CA Certificate** dialog box. A maximum of 10 client CA certificates can be added. It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. Certificates using the RSA-2048 encryption algorithm have risks. Exercise caution when using such certificates. – After a CA certificate is verified, you can view its basic information, including the name, serial number, signature algorithm, issuer, subject, and expiration time. ● Select **Password authentication (local)**. – Click the **User Management** and **User Groups** tabs in sequence, and click **Create User Group**. – Click the **User Management** tab. On the **Users** tab page, click **Create User**. – Click the **Access Policies** tab, and click **Create Policy**.	*Set this parameter based on the actual condition.*
Advanced Settings	Protocol	Protocol used by P2C VPN connections. ● TCP (default)	TCP
	Port	Port used by P2C VPN connections. ● 443 (default) ● 1194	443

Area	Parameter	Description	Example Value
	Encryption Algorithm	Encryption algorithm used by P2C VPN connections. ● AES-128-GCM (default) ● AES-256-GCM	AES-128-GCM
	Authentication Algorithm	Authentication algorithm used by P2C VPN connections. ● When the encryption algorithm is AES-128-GCM, the authentication algorithm is SHA256. ● When the encryption algorithm is AES-256-GCM, the authentication algorithm is SHA384.	SHA256
	Compression	Whether to compress the transmitted data. By default, this function is disabled and cannot be modified.	Disabled
	Domain Name Access	Whether to enable domain name access. ● Valid DNS server address: – Not 0.0.0.0 – Non-loopback address. The loopback address range is 127.0.0.0 to 127.255.255.255. – Non-multicast address. The broadcast address range is 224.0.0.0 to 239.255.255.255. – Address not starting or ending with 0 – Non-duplicate DNS server address	Enabled

Table 2-3 Recommended client CIDR blocks

Number of VPN Connections	Recommended Client CIDR Block
10	CIDR blocks with the mask less than or equal to 26 Example: 10.0.0.0/26 and 10.0.0.0/25
20	CIDR blocks with the mask less than or equal to 25 Example: 10.0.0.0/25 and 10.0.0.0/24

Number of VPN Connections	Recommended Client CIDR Block
50	CIDR blocks with the mask less than or equal to 24 Example: 10.0.0.0/24 and 10.0.0.0/23
100	CIDR blocks with the mask less than or equal to 23 Example: 10.0.0.0/23 and 10.0.0.0/22
200	CIDR blocks with the mask less than or equal to 22 Example: 10.0.0.0/22 and 10.0.0.0/21
500	CIDR blocks with the mask less than or equal to 21 Example: 10.0.0.0/21 and 10.0.0.0/20

----End

2.2.2 Checking Server Information

Scenario

After a server is configured, you can view its configuration.

Prerequisites

A server has been configured.

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 Click ≡ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

- **Basic Information** area: You can view the server ID, local CIDR block, client CIDR block, tunnel type, and server status.
- **Authentication Information** area: You can view the server certificate information and client authentication mode.
- **Advanced Settings** area: You can view the protocol, port, encryption algorithm, authentication algorithm, compression function status, and domain name access information.

----End

2.2.3 Modifying a Server

Scenario

You can modify the server configuration.

NOTE

- If you specify a client IP address and then modify the client CIDR block of the server, the client needs to reconnect to the server and the specified IP address will be cleared.
- If you modify advanced settings such as the protocol and port, you need to download the new client configuration file and import it to the clients for the modification to take effect.

Precautions

- After the port or encryption algorithm is changed, clients are disconnected. You need to download the new client configuration file to reconnect them.
- Exercise caution when adding, deleting, or modifying the local CIDR block of a VPN gateway, client CIDR block of a VPN connection, client authentication type, and access policy, since these operations may interrupt the network.

Modifying a Server

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the VPN gateway list, locate the target VPN gateway, and click **View Server** in the **Operation** column.

- Click ✎ next to **Basic Information** to change the local or client CIDR block.
- Click **Replace** in the **Operation** column of the server certificate to replace it.
- Click ✎ on the right of **Client Authentication Mode** to change the client authentication mode.
- Click ✎ next to **Advanced Settings** to modify the port, encryption algorithm, or domain name access configuration.

⚠ CAUTION

After a DNS server address is changed, the new address takes effect when a client reconnects to the cloud.

Step 6 Click **OK**.

----End

Changing the Authentication Mode

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the VPN gateway list, locate the target VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Change the client authentication mode in either of the following ways:

- When **Client Authentication Mode** is set to **Password authentication (local)**, click ✎ on the right of **Password authentication (local)**. In the **Modify Client Authentication Mode** dialog box, change the value of **Client Authentication Mode** to **Certificate authentication** and click **OK**.

  Before changing the authentication mode to **Certificate authentication**, ensure that users, user groups, and policies have been deleted.

- When **Client Authentication Mode** is set to **Certificate authentication**, click ✎ on the right of **Certificate authentication**. In the **Modify Client Authentication Mode** dialog box, change the value of **Client Authentication Mode** to **Password authentication (local)** and click **OK**.

  Before changing the authentication mode to **Password authentication (local)**, ensure that CA certificates have been deleted.

⚠ CAUTION

After the authentication mode is changed, the original connections are interrupted.

----End

2.2.4 Uploading a Server Certificate

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **Configure Server** in the **Operation** column.

Step 6 On the **Server** tab page, click **Upload** in the **Server Certificate** drop-down list box. The **Cloud Certificate Manager** page is displayed.

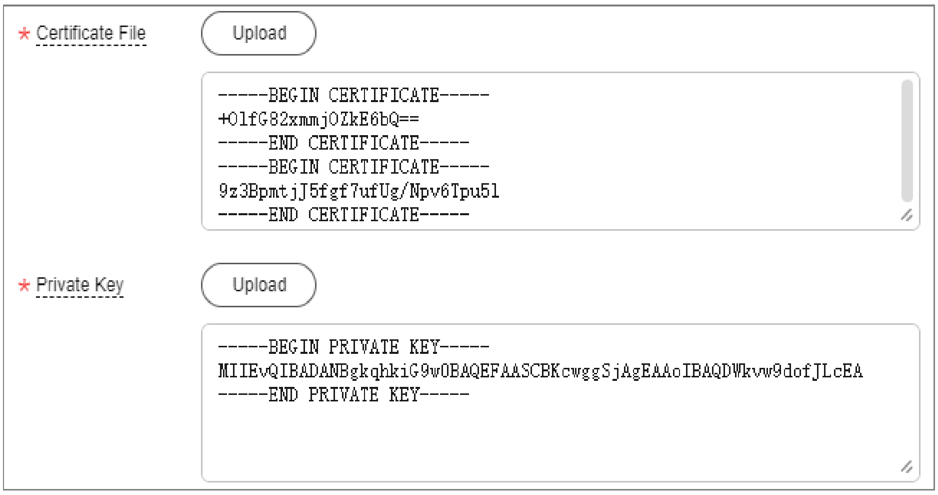
Step 7 On the **SSL Certificate Manager** page, click the **Hosted Certificates** tab, click **Upload Certificate**, and enter related information as prompted.

Table 2-4 describes the parameters for uploading a certificate.

Table 2-4 Parameters for uploading an international standard certificate

Parameter	Description
Certificate standard	Select **International**.
Certificate Name	User-defined name of a certificate.
Enterprise Project	Select the enterprise project to which the SSL certificate is to be added.
Certificate File	Use a text editor (such as Notepad++) to open the certificate file in CER or CRT format to be uploaded, and copy the certificate content to this text box. You need to upload a combined certificate file that contains both the server certificate content and CA certificate content. The CA certificate content must be pasted below the server certificate content. **NOTE** If you do not have a certificate, you can generate a self-issued certificate and upload it. For details, see **Using Easy-RSA to Issue Certificates (Server and Client Sharing a CA Certificate)**. For the format of the certificate file content to be uploaded, see **Figure 2-1**.
Private Key	Use a text editor (such as Notepad++) to open the certificate file in KEY format to be uploaded, and copy the private key content to this text box. You only need to upload the private key of the server certificate. For the format of the private key content to be uploaded, see **Figure 2-1**.

Figure 2-1 Format of the certificate content to be uploaded



* Certificate File

Upload

```
-----BEGIN CERTIFICATE-----
+OlfG82xmmjOZkE6bQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
9z3BpmtjJ5fgf7ufUg/Npv6Tpu5l
-----END CERTIFICATE-----
```

* Private Key

Upload

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDWkvw9dofJLcEA
-----END PRIVATE KEY-----
```

NOTE

The common name (CN) of a server certificate must be in the domain name format.

Step 8 Click **Submit**. The certificate is uploaded.

Step 9 In the certificate list, verify that the certificate status is **Hosted**.

----End

2.2.5 Modifying a Server Certificate

Precautions

After the server certificate is replaced, clients are disconnected. You need to download the new client configuration file to reconnect them.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 On the **Server** tab page, click **Replace** in the **Operation** column of the server certificate. The **Replace Server Certificate** dialog box is displayed.

Step 7 Select a server certificate, and click **OK**.

----End

2.2.6 Uploading a Client CA Certificate

Scenario

You need to upload a client CA certificate only when **Client Authentication Mode** is set to **Certificate authentication**.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **Configure Server** or **View Server** in the **Operation** column.

Step 6 On the **Server** tab page, choose **Certificate authentication** from the **Client Authentication Mode** drop-down list box, and click **Upload CA Certificate**.

Step 7 Set parameters as prompted.

Table 2-5 Parameters for uploading a CA certificate

Parameter	Description	Example Value
Name	This parameter can be modified.	ca-cert-server
Content	Use a text editor (such as Notepad++) to open the signature certificate file in PEM format, and copy the certificate content to this text box. **NOTE** ● It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. ● Certificates using the RSA-2048 encryption algorithm have risks. Exercise caution when using such certificates.	-----BEGIN CERTIFICATE----- MIIDoTCCAomgAwIBAgIUZAxA/ 2WlDFidbH9QfedbwYHrmQQw DQYJKoZIhvcNAQEL BQAwYDELMAkGA1UEBhMCQ0 4xCzAJBgNVBAgMAkJKMQswC- QYDVQQHDAJCSjEPMA0G -----END CERTIFICATE-----

Step 8 Click **OK**.

NOTE

A maximum of 10 client CA certificates can be added.

----End

2.2.7 Deleting a Client CA Certificate

Scenario

You can delete a CA certificate that has been uploaded when **Client Authentication Mode** is set to **Certificate authentication**.

Precautions

After a CA certificate is deleted, clients cannot connect to the server. Exercise caution when deleting a CA certificate.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 On the **Server** tab page, click **Delete** in the **Operation** column of a client CA certificate.

Step 7 In the **Delete CA Certificate** dialog box, click **OK**.

----End

2.2.8 Creating a User and User Group

Scenario

You can create users and user groups only when **Client Authentication Mode** is set to **Password authentication (local)**.

Limitations and Constraints

- Each user can establish a maximum of five connections.
- A maximum of 500 users can be created on a VPN gateway.

Creating a User

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **Configure Server** or **View Server** in the **Operation** column.

Step 6 On the **Server** tab page, set **Client Authentication Mode** to **Password authentication (local)** and click **OK**.

Step 7 Choose **User Management** > **Users**, and click **Create User**.

Table 2-6 describes the parameters.

Table 2-6 Parameters for creating a user

Parameter	Description
Name	The value can contain a maximum of 64 characters, including letters, digits, periods (.), underscores (_), and hyphens (-). **NOTE** Do not use the following usernames that are reserved in the system: ● **L3SW_** (prefix) ● **link** ● **Cascade** ● **SecureNAT** ● **localbridge** ● **administrator** (case-insensitive)
Description	Enter description information as needed.
Password	● The value contains 8 to 32 characters. ● The value must contain at least two types of the following characters: uppercase letters, lowercase letters, digits, and special characters including `~!@#$%^&*()-_=+|[{}];:'",<.>/? and spaces. ● The password cannot be the username or the reverse of the username. **NOTE** For account security purposes, you are advised to change the password periodically.
Confirm Password	Reenter the password.

Parameter	Description
User Group	Select the user group to which the user belongs. **NOTE** ● A user that is not added to any user group cannot access resources on the cloud. ● If no access policy is configured for the selected user group, the user will be unable to access resources on the cloud.
Specify Client IP Address	Determine whether to specify a client IP address. ● Enabled The existing connection of the specified IP address will be interrupted. ● Disabled **CAUTION** ● The specified IP address cannot be the same as the gateway IP address of the client address pool. ● The specified IP address must be the first host address in a CIDR block with a 30-bit mask. ● The specified IP address cannot be the same as the IP address that has been specified for another user. ● The specified IP address must be in the client address pool.

Step 8 Click **OK**.

The **Users** tab page is displayed, showing the user information, including the name/ID, user group, creation time, and static IP address.

----End

NOTE

The maximum number of users that can be added is the maximum number of connections supported by the corresponding VPN gateway.

Creating a User Group

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **Configure Server** or **View Server** in the **Operation** column.

Step 6 On the **Server** tab page, set **Client Authentication Mode** to **Password authentication (local)** and click **OK**.

Step 7 Choose **User Management** > **User Groups**. Click **Create User Group**, enter the name and description, and click **OK**.

----End

NOTE

- The name of a user group must be unique.
- A maximum of 50 user groups are supported.
- Currently, the quota of user groups cannot be modified.
- After creating a user group, you need to configure an access policy for accessing resources on the cloud.

Adding a User to a User Group

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **Configure Server** or **View Server** in the **Operation** column.

Step 6 On the **Server** tab page, set **Client Authentication Mode** to **Password authentication (local)** and click **OK**.

Step 7 Add a user to a user group using either of the following methods:

- Add a user on the **Users** tab page.
  a. Choose **User Management** > **Users**, and click **Create User**.
  b. Set parameters as prompted.

     Select the user group to which the user is to be added.

     NOTE

     If you do not select a user group when creating a user, you can click **Modify** in the **Operation** column of the user to select a user group.
  c. Click **OK**.
- Add a user on the **User Groups** tab page.
  a. Choose **User Management** > **User Groups**. Click **Create User Group**, enter the name and description, and click **OK**.
  b. Locate the row that contains the created user group, and click **Add User** in the **Operation** column.
  c. In the **Add User** dialog box, select one or more users, click ›, and click **OK**.

----End

2.2.9 Modifying a User or User Group

Scenario

You can modify a user or user group that has been created when **Client Authentication Mode** is set to **Password authentication (local)**.

Precautions

After the user group to which a user belongs is modified, the original connection is interrupted. Exercise caution when modifying a user group.

Modifying a User

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Choose **User Management** > **Users**. Locate the row that contains the target user, and click **Modify** in the **Operation** column. In the **Modify User** dialog box, you can modify the description or user group, and determine whether to specify a client IP address.

When a client IP address is specified, all connections of the current user and the connection of the new IP address will be disconnected.

NOTE

For account security purposes, you are advised to change the password periodically.

----End

Modifying a User Group

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Choose **User Management** > **User Groups**. Click **Modify** in the **Operation** column of the target user group, and modify the name and description.

⚠ CAUTION

The default user group cannot be modified or deleted.

----End

2.2.10 Deleting a User or User Group

Scenario

You can delete a user or user group that has been created when **Client Authentication Mode** is set to **Password authentication (local)**.

Precautions

After a user is deleted, the user is disconnected and cannot be connected again. Exercise caution when deleting a user.

Deleting a User

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Choose **User Management** > **Users**. Click **Delete** in the **Operation** column of the target user.

Step 7 In the **Delete User** dialog box, click **OK**.

----End

Removing a User from a User Group

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Choose **User Management** > **User Groups**. Click the name of a user group to go to the user list page.

Step 7 Click **Remove** in the **Operation** column of the user to be removed from the user group.

Step 8 In the **Remove User** dialog box, click **OK**.

⚠ CAUTION

After being removed, a user cannot access resources on the cloud.

----End

Deleting a User Group

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Choose **User Management** > **User Groups**. Click **Delete** in the **Operation** column of the target user group.

Step 7 In the **Delete User Group** dialog box, click **OK**.

⚠ CAUTION

- After the user group is deleted, users in the user group cannot access resources on the cloud.
- The default user group cannot be modified or deleted.

----End

2.2.11 Creating an Access Policy

Scenario

You can create an access policy when the client authentication mode is **Password authentication (local)**.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **Configure Server** in the **Operation** column.

Step 6 On the **Server** tab page, set **Client Authentication Mode** to **Password authentication (local)** and click **OK**.

Step 7 Click the **Access Policies** tab, click **Create Policy**, set the policy name, destination CIDR block, description, and user group, and click **OK**.

NOTE

- A maximum of 10 destination CIDR blocks can be configured in a single policy.
- A maximum of 100 access policies are supported.

----End

2.2.12 Modifying an Access Policy

Scenario

You can modify an access policy when the client authentication mode is **Password authentication (local)**.

Precautions

Modifying an access policy may interrupt the network. Exercise caution when performing this operation.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Click the **Access Policies** tab, click **Modify** in the **Operation** column of the target policy, and modify the name, destination CIDR block, description, and user group as required.

----End

2.2.13 Deleting an Access Policy

Scenario

You can delete an access policy when the client authentication mode is **Password authentication (local)**.

Precautions

After an access policy is deleted, users in the user group associated with this policy cannot access related resources on the cloud. Exercise caution when deleting an access policy.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Click the **Access Policies** tab, and click **Delete** in the **Operation** column of the target policy.

Step 7 In the **Delete Policy** dialog box, click **OK**.

----End

2.2.14 Resetting the Password of a User

Scenario

You can reset the password of a user that has been created when **Client Authentication Mode** is set to **Password authentication (local)**.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Choose **User Management** > **Users**. Click **Reset Password** in the **Operation** column of the target user.

Step 7 In the **Reset Password** dialog box, enter a new password, reenter it, and click **OK**.

NOTE

For account security purposes, you are advised to change the password periodically.

----End

2.2.15 Importing Users in Batches

Scenario

You can import users in batches when the client authentication mode is **Password authentication (local)**.

Limitations and Constraints

- This operation is supported only on Windows operating systems.
- A maximum of 500 users can be created on a VPN gateway.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Choose **User Management** > **Users**, and click **Import User**.

Step 7 In the **Import User** dialog box, click **Download Template**, and configure the downloaded .xlsx template file.

Enter names, passwords, user group names, and static IP addresses in the template file.

NOTE

If a static IP address is specified for a user in the template, the user's client uses this static IP address, and no IP address will be automatically assigned to this user.

Step 8 Click **Select File** and upload the template file.

If the template content is incorrect, the system displays the message "Invalid file content". In this case, you need to modify the template file and import it again.

NOTE

- The size of the file to be uploaded cannot exceed 50 KB.
- Only .xlsx files (Excel 2007 or later) can be uploaded.
- The table header in the file to be uploaded must be the same as that in the downloaded template file.

  The system may be unable to identify the imported template content. Therefore, you are advised not to modify the original content in the template file.
- A maximum of 500 user records are supported in the file to be uploaded.

Step 9 Click **OK**. Users are imported in batches.

----End

2.2.16 Deleting Users in Batches

Scenario

You can delete users in batches when the client authentication mode is **Password authentication (local)**.

Precautions

After a user is deleted, the user is disconnected and cannot be connected again. Exercise caution when deleting a user.

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 Click ≡ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Choose **User Management** > **Users**, select the user to be deleted, and click **Delete User**.

Step 7 In the **Delete User** dialog box, click **OK**.

----End

2.2.17 Viewing a VPN connection

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 Click ≡ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Click the **Connections** tab, and view details about the current connection, including the ID, virtual address, actual address, time when the connection is established, and operation.

NOTE

The **Username** column is available on the **Connections** tab page only when the client authentication mode is set to **Password authentication (local)**.

----End

2.2.18 Tearing Down a VPN Connection

Limitations and Constraints

Only when a VPN gateway is in normal states, you can tear down its connections.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Click the **Connections** tab, locate the target VPN connection, and click **Tear Down** in the **Operation** column.

> ⚠ CAUTION
>
> Exercise caution when tearing down a connection because doing so will disconnect the corresponding VPN client. To prevent the client from going online again, reset the password.

Step 7 Click **OK**. The disconnection request is delivered, and the VPN connection will be torn down.

----End

2.2.19 Viewing VPN Connection Logs

Scenario

After the VPN logging function is enabled, you can view the logs of a specified VPN connection.

Prerequisites

The Log Tank Service (TLS) has been enabled. For details, see **Getting Started with TLS**.

Procedure

- Creating a log group
  1. Log in to the management console.
  2. Click 📍 in the upper left corner and select the desired region and project.
  3. Click ☰ in the upper left corner of the page, and choose **Management & Governance** > **Log Tank Service**.
  4. Create a log group. For details, see **Managing Log Groups**.
- Creating a log stream
  1. Log in to the management console.
  2. Click 📍 in the upper left corner and select the desired region and project.

  c. Click ☰ in the upper left corner of the page, and choose **Management & Governance** > **Log Tank Service**.

  d. Create a log stream. For details, see **Managing Log Streams**.

- Configuring the connection log function
  a. Log in to the management console.
  b. Click 📍 in the upper left corner and select the desired region and project.
  c. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
  d. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
  e. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
  f. Click the **Connections** tab. The VPN connection details page is displayed.
  g. In the **Connection Log** area, click **Configure Connection Log**.
  h. In the dialog box that is displayed, toggle on **Collect Logs**.
  i. Select the target log group and log stream, and click **OK**.

     On the **Connections** tab page, you can view the configured connection log.

- Viewing connection logs
  a. Log in to the management console.
  b. Click 📍 in the upper left corner and select the desired region and project.
  c. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
  d. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
  e. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
  f. Click the **Connections** tab. The VPN connection details page is displayed.
  g. In the **Connection Log** area, click **View Log Details**. The LTS page is displayed.
  h. In the log group list, click ^ on the left of the target log group to view log stream details.
  i. Click a log stream name to view log details, including the time and log content.

     The log format is as follows:

```
$p2c_vgw_id $connection_id $client_public_ip $client_private_ip $client_user_name $event_type
$event_timestamp
```

Table 2-7 Description of the log format

Parameter	Description
p2c_vgw_id	Gateway ID
connection_id	Connection ID
client_public_ip	Actual address
client_private_ip	Virtual address
client_user_name	Username
event_type	Online/Offline event type
event_timestamp	Timestamp

You can search for logs by keyword on the log stream details page on the LTS console.

2.2.20 Updating the VPN Connection Log Configuration

Prerequisites

The VPN connection log function has been configured. For details, see **Configuring the Connection Log Function**.

Precautions

After the connection log configuration is updated, the previously reported connection logs cannot be viewed in the new log group or log stream. Exercise caution when performing this operation.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Click the **Connections** tab. The VPN connection details page is displayed.

Step 7 In the **Connection Log** area, click **Configure Connection Log**.

Step 8 In the dialog box that is displayed, select a new log group and a new log stream.

Step 9 Click **OK**.

The **Connections** tab page is displayed, showing the new connection log configuration.

----End

2.2.21 Deleting the VPN Connection Log Configuration

Precautions

After the connection log configuration is deleted, connection logs cannot be reported. Exercise caution when performing this operation.

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 Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

Step 5 Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.

Step 6 Click **Connections**. The VPN connection details page is displayed.

Step 7 In the **Connection Log** area, click **Configure Connection Log**.

Step 8 In the dialog box that is displayed, toggle off **Collect Logs**.

Step 9 Click **OK**.

----End

2.3 P2C VPN Client Management

2.3.1 Client Configuration Precautions

Limitations and Constraints

- When a VPN client connects to multiple servers, ensure that the client CIDR blocks configured for the servers do not overlap with each. Otherwise, the client may be assigned the same IP address for connecting to different servers, causing connection failures.
- A client can establish only one VPN connection with a VPN gateway.
- If DNS has been configured on the operating system where the OpenVPN client is installed and DNS is also configured for a P2C VPN gateway, the later will inherit or overwrite the former. As a result, domain names in the DNS

configuration of the operating system will fail to be resolved, causing access failures.

High-Risk Operation Warning

Before configuring a client, exercise caution when adding, deleting, or modifying the local subnet of a VPN gateway and the customer subnet or policy configuration of a VPN connection, because these operations may cause network interruption.

List of Supported Operating Systems

Table 2-8 List of supported operating systems

Operating System Type	Operating System Version	Client Version	Operation Guide
Windows	Windows 10 or later	- OpenVPN GUI 2.6 or later - OpenVPN Connect 3.4.4 or later	**2.3.2 Configuring a Windows Client**
Linux	- Ubuntu 24.10 - Ubuntu 22.04 (Jammy)	- 24.10: OpenVPN 2.6 or later - 22.04: OpenVPN 2.5 or earlier	**Ubuntu**
	- CentOS 7.9 - CentOS 8 - CentOS Stream 9	- 7.9 and 8: OpenVPN 2.4.12 - Stream 9: OpenVPN 2.5 or later	**CentOS**
	Debian 12	OpenVPN 2.5 or later	**Debian**
	Red Hat Enterprise Linux 9.5	OpenVPN 2.5 or later	**Redhat**
	openSUSE 15.5	OpenVPN 2.5 or later	**OpenSUSE**
macOS	-	- Tunnelblick 3.8.8d - OpenVPN Connect 3.4.4.4629	**2.3.4 Configuring a macOS Client**

Operating System Type	Operating System Version	Client Version	Operation Guide
Android	-	OpenVPN Connect APK 3.3.2 or later	**2.3.5 Configuring an Android Client**
iOS	-	OpenVPN Connect 3.4.0	**2.3.6 Configuring an iOS Client**

2.3.2 Configuring a Windows Client

Version Requirements

Table 2-9 lists the client versions supported by Windows.

Table 2-9 Version requirements

Client Type	OpenVPN Version	Operation Guide
OpenVPN GUI	2.6 or later	**OpenVPN GUI**
OpenVPN Connect	3.4.4 or later	**OpenVPN Connect**

OpenVPN GUI

Step 1 Download the OpenVPN GUI installation package and install it as prompted.

The installation package varies according to the Windows operating system as follows:

- For a 32-bit Windows operating system, download the **Windows 32-bit MSI installer**.
- For a 64-bit Windows operating system, download the **Windows 64-bit MSI installer**.
- For a 64-bit Windows ARM-based operating system, download the **Windows ARM64 MIS installer**.

Step 2 Download the client configuration file.

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

5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

Step 3 Decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 4 Open the **client_config.ovpn** file using Notepad or Notepad++.

Step 5 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

Step 6 Save the .ovpn configuration file.

Step 7 Click **OpenVPN GUI** in the Start menu to start the client.

The message "OpenVPN GUI is already running. Right click on the tray icon to start." is displayed in the lower right corner.

Step 8 Right-click the icon on the Windows taskbar, and choose **Import** > **Import file**.

Import the .ovpn configuration file.

When the message "File imported successfully." is displayed in the lower right corner, the file is imported.

Step 9 In the **Open** dialog box, select the configuration file with the client certificate and private key added, and click **Open**.

Step 10 Right-click the icon on the Windows taskbar, and choose **Connect**.

----End

OpenVPN Connect

Step 1 Download OpenVPN Connect from the OpenVPN official website, and install it as prompted.

Step 2 Download the client configuration file.

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.

3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

Step 3 Add configuration information.

You can add configuration information using either of the following methods:

- **Method 1: Import the configuration file (with the client certificate and private key added).**
  a. Decompress **client_config.zip** to a specified directory, for example, **D:\**.

     After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

  b. Open the **client_config.ovpn** file using Notepad or Notepad++.
  c. Add the client certificate and private key to the file.

     Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

  d. Save the .ovpn configuration file.
  e. Start the OpenVPN Connect client.
  f. Import the .ovpn configuration file.

- **Method 2: Use the original configuration file (without the client certificate and private key) and a USB key.**
  a. Initialize a USB key.

     The following uses Longmai's mToken GM3000 administrator tool (v2.2.19.619) as an example to describe how to create a USB key. When the USB key is successfully initialized, remove and insert the USB key.

  b. Import the client certificate to the USB key.
  c. Use the USB key to establish a VPN connection.

     In OpenVPN Connect, import the configuration file without the client CA certificate and private key from the USB key, and click **CONNECT**.

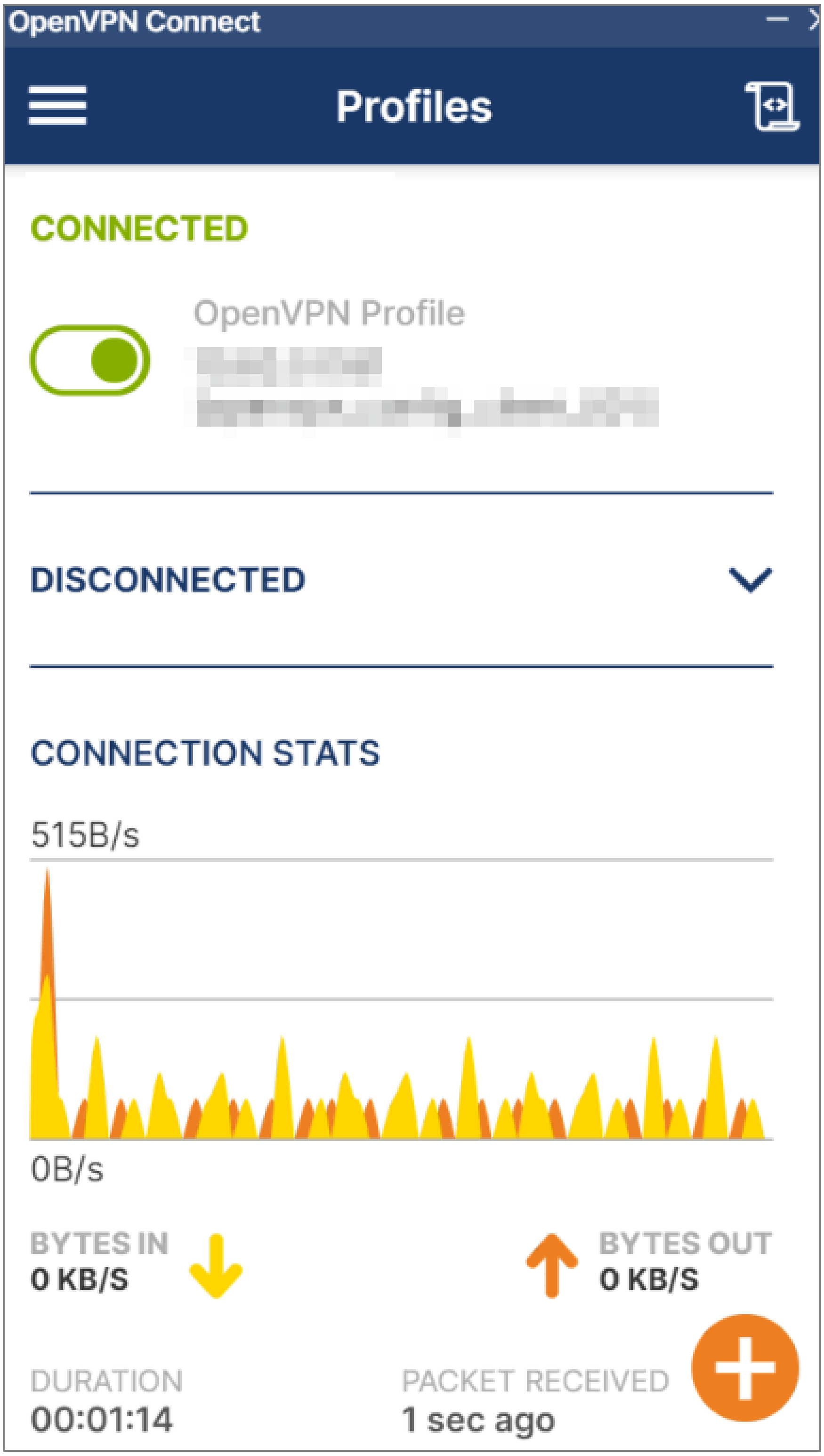
NOTE

- When the connection is being established, do not remove the USB key.
- After the connection is established, it will not be interrupted if you remove the USB key, and you can tear down this connection manually. However, the connection will fail to be re-established after you remove the USB key.

Step 4 Establish a VPN connection.

If information similar to the following is displayed, the connection is successfully established.

Figure 2-2 Connection established



CONNECTED

OpenVPN Profile

[redacted]

DISCONNECTED

CONNECTION STATS

515B/s

0B/s

BYTES IN
0 KB/S

BYTES OUT
0 KB/S

DURATION
00:01:14

PACKET RECEIVED
1 sec ago

----End

2.3.3 Configuring a Linux Client

2.3.3.1 Ubuntu

Version Requirements

Table 2-10 lists the client versions supported by Ubuntu.

Table 2-10 Version requirements

Ubuntu Version	OpenSSL Version	OpenVPN Version	Operation Guide
24.10	3.3.1	Versions later than 2.5	**Ubuntu 24.10**
22.04 (Jammy)	1.1.1	2.5 or later	**Ubuntu 22.04 (Jammy)**

Ubuntu 24.10

Step 1 Log in to the Ubuntu system as the **root** user and open the CLI.

Step 2 Run the following command to back up the original configuration file of the system:

cp -a /etc/apt/sources.list.d/ubuntu.sources /etc/apt/sources.list.d/ubuntu.sources.bak

Step 3 Install APT repositories.

1. Run the following command to configure APT repositories:

   vim /etc/apt/sources.list.d/ubuntu.sources

2. Enter the following content in the command window:

```
Types: deb
URIs: https://xxx.cn/ubuntu/
Suites: oracular oracular-updates oracular-backports
Components: main restricted universe multiverse
Signed-By: /usr/share/keyrings/ubuntu-archive-keyring.gpg

Types: deb
URIs: https://xxx.cn/ubuntu/
Suites: oracular-security
Components: main restricted universe multiverse
Signed-By: /usr/share/keyrings/ubuntu-archive-keyring.gpg
```

   NOTE

   Replace ***https://xxx.cn/*** with the actual source.

3. Press **Esc**, enter **:wq**, and press **Enter**.

   The system saves the configuration and exits the editor.

Step 4 Run the following command to check the current OpenVPN version:

openvpn --version

Information similar to the following is displayed:

```
OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AEAD] [DCO]
library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
```

- If the OpenVPN version is displayed, go to **5**.
- If no OpenVPN version is displayed, perform the following operations to install OpenVPN:

  a. Run the following command to install OpenVPN:

  apt install -y openvpn

  A download progress bar is displayed. When the download progress reaches 100%, the installation is complete.

  The following information is displayed:

  ```
  Installing:
    openvpn

  Suggested packages:
    openvpn-dco-dkms  openvpn-systemd-resolved  easy-rsa
  ...
  ...
  ...
  No services need to be restarted.

  No containers need to be restarted.

  No user sessions are running outdated binaries.

  No VM guests are running outdated hypervisor (qemu) binaries on this host.
  ```

  b. Run the following command again to check the OpenVPN version:

  openvpn --version

  Information similar to the following is displayed:

  ```
  OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/
  PKTINFO] [AEAD] [DCO]
  library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
  ```

Step 5 Download the client configuration file on a Windows system.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

Step 6 Decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 7 Open the **client_config.conf** file using Notepad or Notepad++.

Step 8 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

Step 9 Save the .conf configuration file.

Step 10 Upload the .conf configuration file to the Ubuntu system using Xftp (a file transfer tool). In this example, the file is uploaded to the **/opt/** directory.

Step 11 On Ubuntu, run the following command to go to the directory where the client configuration file is stored:

cd /opt/

Step 12 Run the following command to start the OpenVPN client and connect to the VPN gateway:

openvpn --config /opt/openvpn_config_user-01.conf

If the following information in bold is displayed, the OpenVPN connection is successfully established:

```
2025-02-27 19:22:41 Note: Kernel support for conf-dco missing, disabling data channel offload.
2025-02-27 19:22:41 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
[MH/PKTINFO] [AEAD] [DCO]
2025-02-27 19:22:41 library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
...
...
...
2025-02-27 19:22:42 Initialization Sequence Completed
...
...
```

Step 13 Run the following command to verify the connectivity:

ping XX.XX.XX.XX

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----End

Ubuntu 22.04 (Jammy)

Step 1 Log in to the Ubuntu system as the **root** user and open the CLI.

Step 2 Run the following command to install the OpenVPN client:

```
yum install -y openvpn
```

Step 3 Download the client configuration file on a Windows system.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.
6. Decompress **client_config.zip** to a specified directory, for example, **D:\**.

   After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
7. Open the **client_config.conf** file using Notepad or Notepad++.
8. Add the client certificate and private key to the file.

   Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

   ```
   <cert>
   -----BEGIN CERTIFICATE-----
   Client certificate content
   -----END CERTIFICATE-----
   </cert>

   <key>
   -----BEGIN PRIVATE KEY-----
   Client private key
   -----END PRIVATE KEY-----
   </key>
   ```
9. (Optional) Comment out **disable-dco**. Perform this step only when OpenVPN 2.5 or earlier is used.
   a. Press **Ctrl+F** to search for and locate **disable-dco**.
   b. Enter **#** in front of the line where **disable-dco** is located to comment out the line.

      ```
      …
      …
      # disable-dco
      …
      …
      ```
10. Save the .conf configuration file.

Step 4 Upload the .conf configuration file to the Ubuntu system using Xftp. In this example, the file is uploaded to the **/etc/openvpn/conf/** directory.

Step 5 On Ubuntu, run the following command to go to the directory where the client configuration file is stored:

```
cd /etc/openvpn/conf/
```

Step 6 Run the following command to start the OpenVPN client and connect to the VPN gateway:

openvpn --config /etc/openvpn/conf/config.conf --daemon

NOTE

On Linux, you are advised not to modify the DNS configuration of the operating system after starting OpenVPN. Otherwise, the new DNS configuration of the operating system will be overwritten by the DNS configuration of the OpenVPN client when OpenVPN is started next time.

----End

2.3.3.2 CentOS

Version Requirements

Table 2-11 lists the client versions supported by CentOS.

Table 2-11 Version requirements

CentOS Version	OpenSSL Version	OpenVPN Version
7.9	1.1.1	2.4.12
8	1.1.1	2.4.12
Stream 9	3.2.2	2.5 or later

Procedure

Step 1 Log in to the CentOS system as the **root** user and open the CLI.

Step 2 Run the following command to back up the original configuration file of the system:

cp -a /etc/yum.repos.d/epel.repo /etc/yum.repos.d/epel.repo.backup

Step 3 Install the EPEL repository.

- CentOS 7.9

  Run the following command to install the EPEL repository:

  yum install -y epel-release

  If the following information is displayed, the EPEL repository is successfully installed:

  ```
  Last metadata expiration check: 0:00:14 ago on Wed 05 Mar 2025 05:53:17 PM CST.
  ...
  ...
  ...
  Installed:
    epel-release-8-11.el8.noarch

  Complete!
  ```

- CentOS 8 or Stream 9

  a. Run the following command to configure the EPEL repository:

     vim /etc/yum.repos.d/epel.repo

b. Enter the following content in the command window:

```
[epel]
name=epel
baseurl=https://xxx.cn/epel/8/Everything/x86_64/
gpgcheck=0
gpgkey=https://xxx.cn/epel/RPM-GPG-KEY-EPEL-8
```

NOTE

- **8** indicates the CentOS version. Change it to the actual version number.
- Replace ***https://xxx.cn/*** with the actual source.

c. Press **Esc**, enter **:wq**, and press **Enter**.

The system saves the configuration and exits the editor.

Step 4 Run the following command to check the current OpenSSL version:

openssl version

The following information is displayed:

```
OpenSSL 1.1.1k
```

- If the OpenSSL version is 1.1.1k or later, go to 5.
- If the OpenSSL version is earlier than 1.1.1k, perform the following operations to install OpenSSL:

a. Run the following command to install OpenSSL 1.1.1k:

yum install -y openssl11 openssl11-devel

If the following information is displayed, OpenSSL 1.1.1k is successfully installed:

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
...
...
...
Is this ok [y/d/N]: y     # Enter y.
...
...
...
Installed:
  openssl11.x86_64 1:1.1.1k-7.el7

Complete!
```

b. Run the following command again to check the OpenSSL version:

openssl11 version

The following information is displayed:

```
OpenSSL 1.1.1k
```

Step 5 Run the following command to check the current OpenVPN version:

openvpn --version

The following information is displayed:

```
OpenVPN 2.4.12 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AEAD] built on Nov 10 2023
library versions: OpenSSL 1.1.1k FIPS 25 Mar 2021, LZO 2.08
```

- If the OpenVPN version is displayed, go to 6.

- If no OpenVPN version is displayed, perform the following operations to install OpenVPN:

  Install OpenVPN. The installation command varies according to the CentOS version.

  - CentOS 7.9

    NOTE

    CentOS 7.9 supports only OpenVPN 2.4.12.

    i. On Windows, download the OpenVPN client installation package (**openvpn-2.4.12-2.el8.rpm**).

    ii. Upload the downloaded .rpm installation package to a directory on CentOS using Xftp. In this example, the file is uploaded to the **/opt/** directory.

    iii. On CentOS, run the following command to go to the directory where the installation package is stored:

       cd /opt/

    iv. Run the following command to install OpenVPN:

       yum install ./openvpn-2.4.12-2.el8.x86_64.rpm

       If the following information in bold is displayed, OpenVPN is successfully installed:

```
Loaded plugins: fastestmirror
Examining openvpn-2.4.12-2.el8.x86_64.rpm: openvpn-2.4.12-2.el8.x86_64
Marking openvpn-2.4.12-2.el8.x86_64.rpm to be installed
...
...
...
Is this ok [y/d/N]: y        # Enter y.
...
...
...
Installed:
  openvpn.x86_64 0:2.4.12-2.el8

Complete!
```

    v. Run the following command again to check the OpenVPN version:

       openvpn --version

       Information similar to the following is displayed:

```
OpenVPN 2.4.12 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Nov 10 2023
library versions: OpenSSL 1.1.1k FIPS 25 Mar 2021, LZO 2.08
```

  - CentOS 8 or CentOS Stream 9

    i. On CentOS, run the following command to install OpenVPN:

       yum install openvpn

       If the following information in bold is displayed, OpenVPN is successfully installed:

```
CentOS-8 - Base                              28 kB/s | 3.9 kB     00:00
...
...
...
Is this ok [y/N]: y            # Enter y.
...
...
...
Installed:
 openvpn-2.4.12-2.el8.x86_64            pkcs11-helper-1.22-7.el8.x86_64

Complete!
```

ii. Run the following command again to check the OpenVPN version:

openvpn --version

Information similar to the following is displayed:

```
OpenVPN 2.4.12 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Nov 10 2023
library versions: OpenSSL 1.1.1k FIPS 25 Mar 2021, LZO 2.08
```

Step 6 Download the client configuration file on a Windows system.

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.
6. Decompress **client_config.zip** to a specified directory, for example, **D:\**.

   After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
7. Open the **client_config.conf** file using Notepad or Notepad++.
8. Add the client certificate and private key to the file.

   Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

9. (Optional) Comment out **data-ciphers** and **disable-dco**.

   NOTE

   Comment out **data-ciphers** only when OpenVPN 2.4.12 is used.

   Comment out **disable-dco** only when OpenVPN 2.5 or earlier is used.

   a. Press **Ctrl+F** to search for and locate **data-ciphers** and **disable-dco**.

   b. Enter **#** in front of the lines where **data-ciphers** and **disable-dco** are located to comment out the lines.

```
...
......
# data-ciphers AES-XXX-GCM      # Comment out this line only on CentOS 7.9 and CentOS 8.
......
......
# disable-dco                # Comment out this line only on CentOS 7.9, CentOS 8, and CentOS
```

```
Stream 9.
......
...
```

10. Save the .conf configuration file.

Step 7 Upload the .conf configuration file to the CentOS system using Xftp. In this example, the file is uploaded to the **/opt/** directory.

Step 8 On CentOS, run the following command to go to the directory where the client configuration file is stored:

cd /opt/

Step 9 Run the following command to start the OpenVPN client and connect to the VPN gateway:

openvpn --config /opt/openvpn_config_user-01.conf

If the following information in bold is displayed, the OpenVPN connection is successfully established:

```
Tue Feb 25 19:24:04 2025 OpenVPN 2.4.12 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Nov 10 2023
...
...
...
Tue Feb 25 19:24:06 2025 WARNING: this configuration may cache passwords in memory -- use the auth-
nocache option to prevent this
Tue Feb 25 19:24:06 2025 Initialization Sequence Completed
```

Step 10 Run the following command to verify the connectivity:

ping XX.XX.XX.XX

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----End

2.3.3.3 Debian

Version Requirements

Table 2-12 lists the client versions supported by Debian.

Table 2-12 Version requirements

Debian Version	OpenSSL Version	OpenVPN Version
12.0.0	1.1.1	2.5 or later

High-Risk Operation Warning

Before configuring a client, exercise caution when adding, deleting, or modifying the local subnet of a VPN gateway and the customer subnet or policy configuration of a VPN connection, because these operations may cause network interruption.

Procedure

Step 1 Log in to the Debian system as the **root** user and open the CLI.

Step 2 Run the following command to back up the original configuration file of the system:

cp -a /etc/apt/sources.list /etc/apt/sources.list.bak

Step 3 Install APT repositories.

1. Run the following command to configure APT repositories:

   vi /etc/apt/sources.list

2. Enter the following content in the command window:

```
deb https://xxx.cn/debian/ bullseye contrib main

deb-src https://xxx.cn/debian/ bullseye contrib main

# Software update sources

deb https://xxx.cn/debian-security/ bullseye-security main contrib

deb-src https://xxx.cn/debian-security/ bullseye-security main contrib

# Security update sources

deb https://xxx.cn/debian/ bullseye-updates main contrib

deb-src https://xxx.cn/debian/ bullseye-updates main contrib
```

   NOTE

   Replace ***https://xxx.cn/*** with the actual source.

3. Press **Esc**, enter **:wq**, and press **Enter**.

   The system saves the configuration and exits the editor.

Step 4 Run the following command to check the version information:

openvpn --version

The following information is displayed:

```
OpenVPN 2.5.1 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AEAD] built on May 14 2021
library versions: OpenSSL 1.1.1w  11 Sep 2023, LZO 2.10
```

- If the OpenVPN version is displayed, go to 5.
- If no OpenVPN version is displayed, perform the following operations to install OpenVPN:

  a. Run the following command to install OpenVPN:

     apt install -y openvpn

     A download progress bar is displayed. When the download progress reaches 100%, the installation is complete.

     The following information is displayed:

     ```
     Reading package lists... Done
     Building dependency tree... Done
     Reading state information... Done
     ...
     ...
     ...
     Unpacking openvpn (2.5.1-3) ...
     Setting up openvpn (2.5.1-3) ...
     Processing triggers for man-db (2.11.2-2) ...
     ```

  b. Run the following command again to check the version information:

     openvpn --version

     The following information is displayed:

     ```
     OpenVPN 2.5.1 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/
     PKTINFO] [AEAD] built on May 14 2021
     library versions: OpenSSL 1.1.1w  11 Sep 2023, LZO 2.10
     ```

Step 5 Download the client configuration file on a Windows system.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

Step 6 Decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 7 Open the **client_config.conf** file using Notepad or Notepad++.

Step 8 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
```

```
-----END PRIVATE KEY-----
</key>
```

Step 9 (Optional) Comment out **disable-dco**. Perform this step only when OpenVPN 2.5 or earlier is used.

1. Press **Ctrl+F** to search for and locate **disable-dco**.
2. Enter **#** in front of the line where **disable-dco** is located to comment out the line.

```
...
...
# disable-dco
...
...
```

Step 10 Save the .conf configuration file.

Step 11 Upload the .conf configuration file to the Debian system using Xftp. In this example, the file is uploaded to the **/opt/** directory.

Step 12 Run the following command to go to the directory where the installation package is stored:

cd /opt/

Step 13 Run the following command to start the OpenVPN client and connect to the VPN gateway:

openvpn --config /opt/openvpn_config_user-01.conf

If the following information in bold is displayed, the OpenVPN connection is successfully established:

```
2025-02-28 11:34:35 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
[MH/PKTINFO] [AEAD] built on May 14 2021
2025-02-28 11:34:35 library versions: OpenSSL 1.1.1w  11 Sep 2023, LZO 2.10
...
...
...
2025-02-28 11:34:37 Initialization Sequence Completed
```

Step 14 Run the following command to verify the connectivity:

ping XX.XX.XX.XX

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----End

2.3.3.4 Red Hat Enterprise Linux

Version Requirements

Table 2-13 lists the client versions supported by Red Hat Enterprise Linux.

Table 2-13 Version requirements

Red Hat Enterprise Linux Version	OpenSSL Version	OpenVPN Version
9.5	1.1.1 or later	2.5 or later

Procedure

Step 1 On Windows, **download lib64pkcs11-helper1**.

Step 2 Upload the downloaded .rpm installation package to a directory on Red Hat Enterprise Linux using Xftp. In this example, the file is uploaded to the **/opt/** directory.

Step 3 Log in to the Red Hat Enterprise Linux system as the **root** user and open the CLI.

Step 4 Run the following command to go to the directory where the installation package is stored:

cd /opt/

Step 5 Run the following command to install lib64pkcs11-helper1:

yum install lib64pkcs11-helper1-1.30.0-1-omv2390.x86_64.rpm

If the following information is displayed, lib64pkcs11-helper1 is successfully installed:

```
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to
register.
...
...
...
Installed:
  lib64pkcs11-helper1-1.30.0-1.x86_64

Complete!
```

Step 6 Run the following command to check the OpenVPN version:

openvpn --version

The following information is displayed:

```
OpenVPN 2.5.11 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AEAD] built on Jul 18 2024
library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
```

- If the OpenVPN version is displayed, go to **4**.
- If no OpenVPN version is displayed, perform the following operations to install OpenVPN:

a. On Windows, **download OpenVPN**.

b. Upload the downloaded .rpm installation package to a directory on Red Hat Enterprise Linux using Xftp. In this example, the file is uploaded to the **/opt/** directory.

c. Run the following command to install OpenVPN:

yum install openvpn-2.5.11-1.el9.x86_64.rpm

If the following information in bold is displayed, OpenVPN is successfully installed:

```
Updating Subscription Management repositories.
Unable to read consumer identity
...
...
...
Is this ok [y/N]: y                    # Enter y.
...
...
...
Installed:
  openvpn-2.5.11-1.el9.x86_64

Complete!
```

d. Run the following command again to check the OpenVPN version:

openvpn --version

Information similar to the following is displayed:

```
OpenVPN 2.5.11 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
[MH/PKTINFO] [AEAD] built on Jul 18 2024
library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
```

Step 7 Download the client configuration file on a Windows system.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

Step 8 Decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 9 Open the **client_config.conf** file using Notepad or Notepad++.

Step 10 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>
```

```
<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

Step 11 (Optional) Comment out **disable-dco**. Perform this step only when OpenVPN 2.5 or earlier is used.

1. Press **Ctrl+F** to search for and locate **disable-dco**.
2. Enter **#** in front of the line where **disable-dco** is located to comment out the line.

```
...
...
# disable-dco
...
...
```

Step 12 Save the .conf configuration file.

Step 13 Upload the .conf configuration file to the Red Hat Enterprise Linux system using Xftp. In this example, the file is uploaded to the **/opt/** directory.

Step 14 Run the following command to go to the directory where the client configuration file is stored:

cd /opt/

Step 15 Run the following command to start the OpenVPN client and connect to the VPN gateway:

openvpn --config /opt/openvpn_config_user-01.conf

If the following information in bold is displayed, the OpenVPN connection is successfully established:

```
2025-02-27 22:18:30 OpenVPN 2.5.11 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Jul 18 2024
2025-02-27 22:18:30 library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
...
...
...
2025-02-27 22:18:32 Initialization Sequence Completed
```

Step 16 Run the following command to verify the connectivity:

ping XX.XX.XX.XX

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----End

2.3.3.5 openSUSE

Version Requirements

Table 2-14 lists the client versions supported by openSUSE.

Table 2-14 Version requirements

openSUSE Version	OpenSSL Version	OpenVPN Version
15.5	1.1.1	2.5 or later

Procedure

Step 1 Log in to the CentOS system as the **root** user and open the CLI.

Step 2 Configure Zypper repositories.

1. Run the following command to back up the original configuration file of the system:

   mkdir /etc/zypp/repos.d/repo_bakmv /etc/zypp/repos.d/*.repo /etc

   /zypp/repos.d/repo_bak/mv /etc/zypp/repos.d/*.repo /etc/zypp/repos.d/repo_bak/

2. Configure the image source.

   NOTE

   The image source configuration varies according to the client version. For details, see the Zypper repository configuration documents.

Step 3 Run the following command to check the version information:

openvpn --version

The following information is displayed:

```
OpenVPN 2.5.6 x86_64-suse-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AEAD] built on Mar 16 2022
library versions: OpenSSL 1.1.1l  24 Aug 2021 SUSE release 150500.15.4, LZO 2.10
```

- If the OpenVPN version is displayed, go to 4.
- If no OpenVPN version is displayed, perform the following operations to install OpenVPN:
  a. Run the following command to install OpenVPN:

     zypper install openvpn

     If the following information is displayed, OpenVPN is successfully installed:

     ```
     Loading repository data...
     ...
     ...
     ...
     Continue? [y/n/v/...? shows all options] (y): y            # Enter y.
     ...
     ...
     ...
     (1/1) Installing: openvpn-2.5.6-150400.3.6.1.x86_64 ......................................[done]
     ```

b. Run the following command again to check the version information:

openvpn --version

Information similar to the following is displayed:

```
OpenVPN 2.5.6 x86_64-suse-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/
PKTINFO] [AEAD] built on Mar 16 2022
library versions: OpenSSL 1.1.1l  24 Aug 2021 SUSE release 150500.15.4, LZO 2.10
```

Step 4 Download the client configuration file on a Windows system.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

Step 5 Decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 6 Open the **client_config.conf** file using Notepad or Notepad++.

Step 7 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

Step 8 (Optional) Comment out **disable-dco**. Perform this step only when OpenVPN 2.5 or earlier is used.

1. Press **Ctrl+F** to search for and locate **disable-dco**.
2. Enter **#** in front of the line where **disable-dco** is located to comment out the line.

```
...
...
# disable-dco
...
...
```

Step 9 Save the .conf configuration file.

Step 10 Upload the .conf configuration file to the openSUSE system using Xftp. In this example, the file is uploaded to the **/opt/** directory.

Step 11 On openSUSE, run the following command to go to the directory where the client configuration file is stored:

cd /opt/

Step 12 Run the following command to start the OpenVPN client and connect to the VPN gateway:

openvpn --config /opt/openvpn_config_user-01.conf

If the following information in bold is displayed, the OpenVPN connection is successfully established:

```
2025-02-27 14:09:26 OpenVPN 2.5.6 x86_64-suse-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Mar 16 2022
2025-02-27 14:09:26 library versions: OpenSSL 1.1.1l  24 Aug 2021 SUSE release 150500.15.4, LZO 2.10
...
...
...
2025-02-27 14:09:28 Initialization Sequence Completed
```

Step 13 Run the following command to verify the connectivity:

ping XX.XX.XX.XX

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----End

2.3.4 Configuring a macOS Client

Client Version Requirements

Table 2-15 lists the client versions supported by macOS.

Table 2-15 Client version requirements

Client Type	Client Version	Operation Guide
OpenVPN Connect	3.4.4.4629	**OpenVPN Connect**
Tunnelblick	3.8.8d	**Tunnelblick**

OpenVPN Connect

Step 1 Visit the OpenVPN official website, and **download the OpenVPN Connect installer** based on the hardware of your device.

Step 2 Install OpenVPN Connect as prompted.

Step 3 Download the client configuration file.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

Step 4 Decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 5 Open the **client_config.ovpn** file using TextEdit.

Step 6 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

Step 7 Save the .ovpn configuration file.

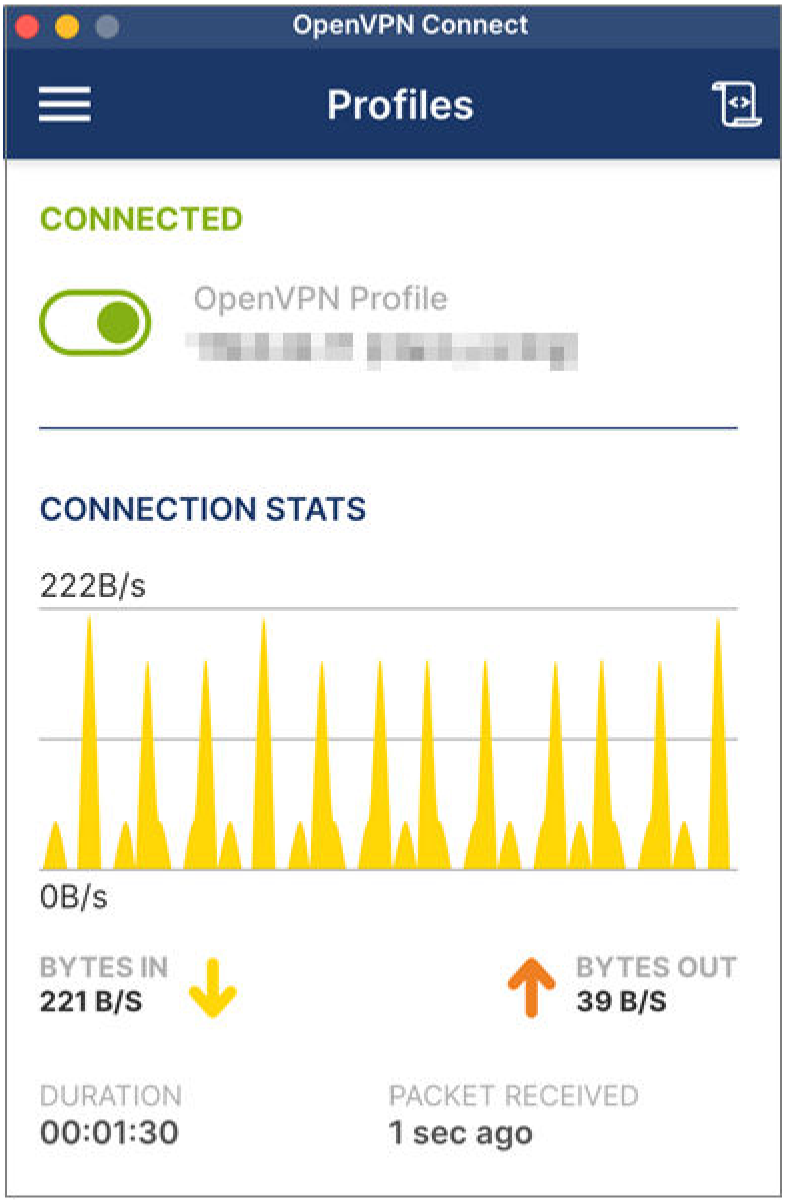
Step 8 Start the OpenVPN Connect client.

Step 9 Import the .ovpn configuration file and enter the configuration information.

Step 10 Establish a VPN connection.

If information similar to the following is displayed, the connection is successfully established.

Figure 2-3 Connection established



OpenVPN Connect

Profiles

CONNECTED

OpenVPN Profile

[redacted]

CONNECTION STATS

222B/s

0B/s

BYTES IN
221 B/S

BYTES OUT
39 B/S

DURATION
00:01:30

PACKET RECEIVED
1 sec ago

----End

Tunnelblick

Step 1 Download Tunnelblick from the official website.

Download the software of a required release. An official release is recommended. You are advised to download the software in DMG format.

Step 2 Install Tunnelblick as prompted.

Step 3 Download the client configuration file.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.

3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

Step 4 Decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 5 Open the **client_config.ovpn** file using TextEdit.

Step 6 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

Step 7 Comment out **disable-dco**.

1. Press **Command+F** to search for and locate **disable-dco**.
2. Enter **#** in front of the line where **disable-dco** is located to comment out the line.

   ```
   ...
   ...
   # disable-dco
   ...
   ...
   ```

Step 8 Save the .ovpn configuration file.

Step 9 Start the Tunnelblick client.

Step 10 Import the .ovpn configuration file.

Step 11 Establish a VPN connection.

----End

2.3.5 Configuring an Android Client

Procedure

Step 1 Download the **OpenVPN client (Android)** and install it.

Step 2 Download the client configuration file.

- Method 1: Download the client configuration file on a PC.
- Method 2: Download the client configuration file on a mobile phone.

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

   NOTE

   If you download the client configuration file on a PC, you need to upload the file to the Android system.

Step 3 On your PC, decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 4 Open the **client_config.ovpn** file using Notepad or Notepad++.

Step 5 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

Step 6 Save the .ovpn configuration file.

NOTE

If you perform subsequent operations on Android, you need to upload the .ovpn configuration file that has been configured on the PC to the Android system.

Step 7 Start the OpenVPN client.

- Method 1: Start the client on your PC.
- Method 2: Start the client on your mobile phone.

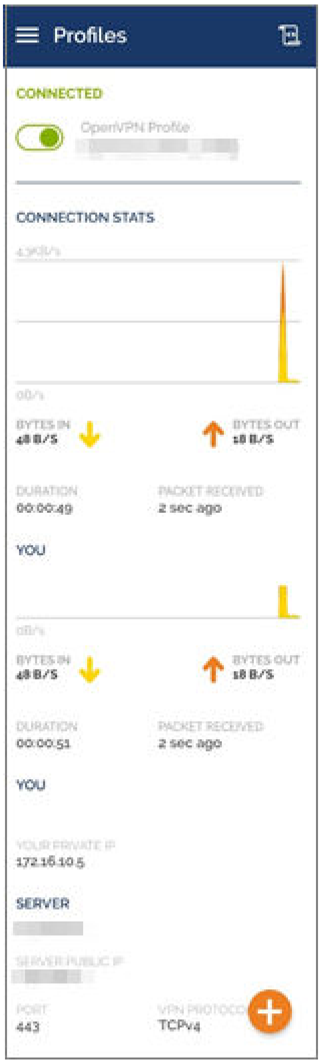
Step 8 Import the .ovpn configuration file.

Step 9 Establish a VPN connection.

A connection request is displayed on the app screen. Tap **OK**.

If information similar to the following is displayed, the connection is successfully established.

Figure 2-4 Connection established



Profiles

CONNECTED

OpenVPN Profile

[redacted]

CONNECTION STATS

4.9KB/s

0B/s

BYTES IN 48 B/S

BYTES OUT 18 B/S

DURATION 00:00:49

PACKET RECEIVED 2 sec ago

YOU

0B/s

BYTES IN 48 B/S

BYTES OUT 18 B/S

DURATION 00:00:51

PACKET RECEIVED 2 sec ago

YOU

YOUR PRIVATE IP 172.16.10.5

SERVER

[redacted]

SERVER PUBLIC IP

[redacted]

PORT 443

VPN PROTOCOL TCPv4

----End

2.3.6 Configuring an iOS Client

Procedure

Step 1 Search for "OpenVPN Connect" in the App Store, download the software, and install it.

Step 2 Download the client configuration file.

- **Method 1: Download the client configuration file on a PC.**
- **Method 2: Download the client configuration file on a mobile phone.**

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.

3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.

   The downloaded client configuration file is **client_config.zip**.

   NOTE

   If you download the client configuration file on a PC, you need to upload the file to the Android system.

Step 3 On your PC, decompress **client_config.zip** to a specified directory, for example, **D:\**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

Step 4 Open the **client_config.ovpn** file using Notepad or Notepad++.

Step 5 Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

Step 6 Save the .ovpn configuration file.

NOTE

If you perform subsequent operations on iOS, you need to upload the .ovpn configuration file that has been configured on the PC to the iOS system.

Step 7 Start the OpenVPN Connect client.

- Method 1: Start the client on your PC.
- Method 2: Start the client on your mobile phone.

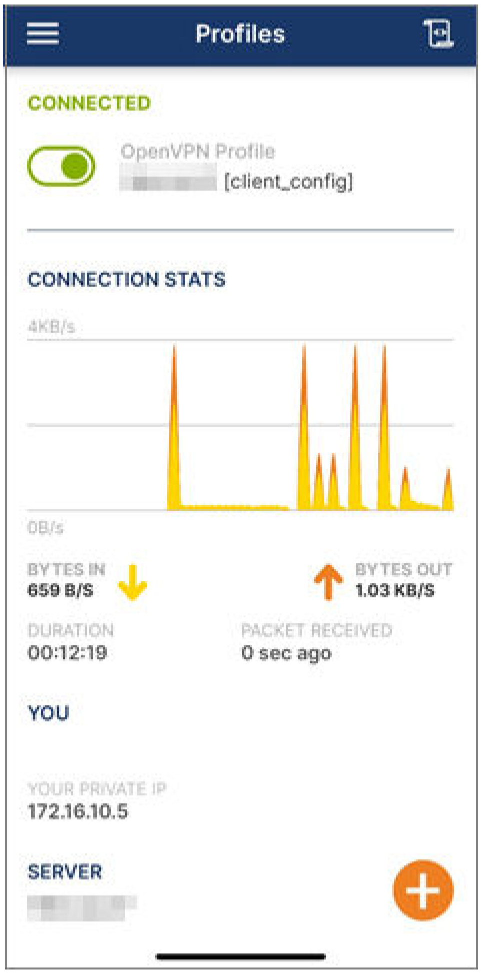
Step 8 Import the .ovpn configuration file.

Add the client configuration as prompted.

Step 9 Establish a VPN connection.

If information similar to the following is displayed, the connection is successfully established.

Figure 2-5 Connection established



CONNECTED

OpenVPN Profile
[redacted] [client_config]

CONNECTION STATS

BYTES IN 659 B/S

BYTES OUT 1.03 KB/S

DURATION 00:12:19

PACKET RECEIVED 0 sec ago

YOU

YOUR PRIVATE IP 172.16.10.5

SERVER [redacted]

----End

2.4 P2C VPN Fee Management

2.4.1 Increasing or Decreasing the VPN Connection Quota of a Yearly/Monthly 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 ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.
6. Locate the row that contains the target VPN gateway, and choose **More** > **Change VPN Connection Quota**.

7. In the **Change VPN Connection Quota** dialog box, select **Increase** or **Decrease**, and click **Yes**.
8. Select a desired number of connections, and click **Next**.
9. Confirm the information, and click **Pay Now**.

NOTE

- In yearly/monthly billing mode, a maximum of 500 connections are supported.
- If you increase the number of VPN connections for a gateway, the new quota takes effect immediately, and you will be charged the extra fee.
- If you decrease the VPN connection quota, you need to set a renewal period and pay for the renewal. The new quota will be available in the new renewal period.

  If the number of connections in use exceeds the new connection quota in the new renewal period, new connections cannot be created. As such, set a proper connection quota.

3 Monitoring

3.1 Monitoring VPN

Monitoring is the key to ensuring VPN performance, reliability, and availability. You can determine VPN resource usage based on monitoring data. The cloud platform provides Cloud Eye to help you obtain the running statuses of your VPNs. You can use Cloud Eye to automatically monitor VPNs in real time and manage alarms and notifications, so that you can know VPN performance metrics in a timely manner.

3.2 Metrics (S2C 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 3-1 Metrics supported for Enterprise Edition VPN gateways

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
gateway_send_pkt_rate	Outbound Packet Rate	Average number of data packets leaving the cloud per second.	≥ 0	pps	N/A	Gateway	1 minute
gateway_recv_pkt_rate	Inbound Packet Rate	Average number of data packets entering the cloud per second.	≥ 0	pps	N/A	Gateway	1 minute
gateway_send_rate	Outbound Bandwidth	Average volume of traffic leaving the cloud per second.	0-1	bps	1024(IEC)	Gateway	1 minute
gateway_recv_rate	Inbound Bandwidth	Average volume of traffic entering the cloud per second.	0-1	bps	1024(IEC)	Gateway	1 minute
gateway_send_rate_usage	Outbound Bandwidth Usage	Bandwidth utilization for traffic leaving the cloud.	0-100	percentage(%)	N/A	Gateway	1 minute
gateway_recv_rate_usage	Inbound Bandwidth Usage	Bandwidth utilization for traffic entering the cloud.	0-100	percentage(%)	N/A	Gateway	1 minute

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
gateway_connection_num	Number of Connections	Number of VPN connections.	≥ 0	count	N/A	Gateway	1 minute

Table 3-2 Enterprise Edition VPN connection metrics

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	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	N/A	VPN connection	15s
tunnel_max_latency	Maximum Tunnel RTT	Maximum round-trip time on the tunnel between the VPN gateway and customer gateway.	0~5000	ms	N/A	VPN connection	15s
tunnel_packet_loss_rate	Tunnel Packet Loss Rate	Packet loss rate on the tunnel between the VPN gateway and customer gateway.	0~100	percentage(%)	N/A	VPN connection	15s
link_average_latency	Average Link RTT	Average round-trip time on the physical link between the VPN gateway and customer gateway.	0~5000	ms	N/A	VPN connection	15s

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
link_max_latency	Maximum Link RTT	Maximum round-trip time on the physical link between the VPN gateway and customer gateway.	0~5000	ms	N/A	VPN connection	15s
link_packet_loss_rate	Link Packet Loss Rate	Packet loss rate on the physical link between the VPN gateway and customer gateway.	0~100	percentage(%)	N/A	VPN connection	15s
connection_status	VPN Connection Status	Status of a VPN connection: **0**: not connected **1**: connected **2**: unknown	0, 1, or 2	N/A	N/A	VPN connection	1 minute
bgp_peer_status	BGP Peer State	State of a BGP peer connection. **0**: not connected **1**: connected **2**: unknown	0, 1, or 2	N/A	N/A	VPN connection	1 minute
recv_pkt_rate	Packet Receive Rate	Average number of data packets received per second.	≥ 0	pps	N/A	VPN connection	1 minute
send_pkt_rate	Packet Send Rate	Average number of data packets sent per second.	≥ 0	pps	N/A	VPN connection	1 minute
recv_rate	Traffic Receive Rate	Average volume of traffic received per second.	0-1	bps	1024(IEC)	VPN connection	1 minute
send_rate	Traffic Send Rate	Average volume of traffic sent per second.	0-1	bps	1024(IEC)	VPN connection	1 minute

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	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	N/A	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	N/A	SA of a VPN connection	1 minute
sa_recv_rate	SA Traffic Receive Rate	Average volume of traffic received over an SA per second.	0-1	bps	1024(IEC)	SA of a VPN connection	1 minute
sa_send_rate	SA Traffic Send Rate	Average volume of traffic sent over an SA per second.	0-1	bps	1024(IEC)	SA of a VPN connection	1 minute

Dimensions

key	Value
evpn_connection_id	Enterprise Edition S2C VPN connection
evpn_sa_id	SAs of an Enterprise Edition S2C VPN connection
evpn_gateway_id	Enterprise Edition S2C VPN gateway

3.3 Metrics (P2C 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 3-3 Metrics supported for Enterprise Edition VPN gateways

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
gateway_send_pkt_rate	Outbound Packet Rate	Average number of data packets leaving the cloud per second.	≥ 0	pps	N/A	Gateway	1 minute
gateway_recv_pkt_rate	Inbound Packet Rate	Average number of data packets entering the cloud per second.	≥ 0	pps	N/A	Gateway	1 minute
gateway_send_rate	Outbound Bandwidth	Average volume of traffic leaving the cloud per second.	0-1	bps	1024(IEC)	Gateway	1 minute
gateway_recv_rate	Inbound Bandwidth	Average volume of traffic entering the cloud per second.	0-1	bps	1024(IEC)	Gateway	1 minute

Metric ID	Metric Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
gateway_send_rate_usage	Outbound Bandwidth Usage	Bandwidth utilization for traffic leaving the cloud.	0-100	percentage(%)	N/A	Gateway	1 minute
gateway_recv_rate_usage	Inbound Bandwidth Usage	Bandwidth utilization for traffic entering the cloud.	0-100	percentage(%)	N/A	Gateway	1 minute
gateway_connection_num	Number of Connections	Number of VPN connections.	≥ 0	count	N/A	Gateway	1 minute

Dimensions

key	Value
p2c_vpn_gateway_id	Enterprise Edition **P2C VPN** gateway

3.4 Event Monitoring (S2C Enterprise Edition VPN)

Description

Event monitoring provides the functions of reporting and querying event data and generating alarms. You can search for event monitoring and alarm information generated for VPN on the Cloud Eye console.

Namespace

SYS.VPN

Table 3-4 VPN event monitoring

Event Name	Event ID	Event Severity	Description	Handling Suggestion	Impact
Certificate to expire in 1 day	VPNCertificatePreExpire1Day	Emergency	An SM certificate is about to expire.	Replace the certificate as soon as possible.	None
Certificate to expire in 3 days	VPNCertificatePreExpire3Days	Emergency	An SM certificate is about to expire.	Replace the certificate as soon as possible.	None
Certificate to expire in 7 days	VPNCertificatePreExpire7Days	Emergency	An SM certificate is about to expire.	Replace the certificate as soon as possible.	None
Certificate to expire in 15 days	VPNCertificatePreExpire15Days	Major	An SM certificate is about to expire.	Replace the certificate as soon as possible.	None
Certificate to expire in 30 days	VPNCertificatePreExpire30Days	Major	An SM certificate is about to expire.	Replace the certificate as soon as possible.	None
Certificate to expire in 60 days	VPNCertificatePreExpire60Days	Major	An SM certificate is about to expire.	Replace the certificate as soon as possible.	None
Certificate expired	VPNCertificateExpire	Emergency	An SM certificate has expired.	Replace the certificate as soon as possible.	Services are interrupted.

3.5 Viewing Metrics

Scenarios

View the VPN connection status and usages of bandwidth and EIP. You can view data of the last 1, 3, 12, or 24 hours, or last 7 days.

Support for Metrics

Table 3-5 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 Gateway Metrics

- Viewing metrics on the VPN console
  1. Log in to the management console.
  2. Click 📍 in the upper left corner and select the desired region and project.
  3. Click ☰ in the upper left corner of the management console, and choose **Networking** > **Virtual Private Network**.
  4. View metrics. The operations vary according to the VPN type.
     - S2C Enterprise Edition VPN: Choose **Virtual Private Network** > **Enterprise – VPN Gateways** > **S2C VPN Gateways**, and click 🖥 in the **Gateway IP Address** column of a VPN gateway. You can view metrics of two EIPs separately.

       The metrics are EIP metrics, including **Outbound Bandwidth**, **Inbound Bandwidth**, **Inbound Bandwidth Usage**, **Outbound Bandwidth Usage**, **Outbound Traffic**, and **Inbound Traffic**.
     - P2C VPN: Choose **Virtual Private Network** > **Enterprise – VPN Gateways** > **P2C VPN Gateways**, and click 🖥 in the **Gateway IP Address** column of a VPN gateway.

       The metrics are EIP metrics, including **Outbound Bandwidth**, **Inbound Bandwidth**, **Inbound Bandwidth Usage**, **Outbound Bandwidth Usage**, **Outbound Traffic**, and **Inbound Traffic**.
- Viewing metrics on the Cloud Eye console
  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**.
  5. View metrics. The operations vary according to the VPN type.
     - S2C Enterprise Edition VPN: Select **S2C VPN Gateway** from the drop-down list. On the **Resources** tab page, click **View Metric** in the **Operation** column.

       The VPN gateway metrics include **Outbound Packet Rate**, **Inbound Bandwidth**, **Outbound Bandwidth**, **Inbound Bandwidth Usage**, **Number of Connections**, **Outbound Bandwidth Usage**, and **Inbound Packet Rate**.
     - P2C VPN: Select **P2C VPN Gateway** from the drop-down list. On the **Resources** tab page, click **View Metric** in the **Operation** column.

       The VPN gateway metrics include **Number of Connections**, **Inbound Packet Rate**, **Inbound Bandwidth**, **Inbound Bandwidth Usage**, **Outbound Bandwidth**, **Outbound Packet Rate**, and **Outbound Bandwidth Usage**.

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 in the upper left corner of the management console, and choose **Networking** > **Virtual Private Network**.
  d. View metrics.
     - S2C Enterprise Edition VPN: Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **View Metric** under the name of a VPN connection.

       The metrics include the following:
       - VPN Connection Status
       - Average Link RTT, Maximum Link RTT, Link Packet Loss Rate

         These metrics are displayed only after the health check function is enabled. To enable this function, click the name of a VPN connection and add health check items on the **Summary** tab page.
       - Average Tunnel RTT, Maximum Tunnel RTT, Tunnel Packet Loss Rate

         These metrics are displayed only when **VPN Type** is set to **Static routing** and the NQA function is enabled.
- 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. View metrics.
     - S2C Enterprise Edition VPN
       1) Select **S2C VPN Connection** from the drop-down list.
       2) On the **Resources** tab page, click **View Metric** in the **Operation** column to view VPN connection metrics.

          The metrics include the following:

          - VPN Connection Status, Packet Receive Rate, Packet Send Rate, Traffic Receive Rate, Traffic Send Rate

          - Average Link RTT, Maximum Link RTT, Link Packet Loss Rate

          These metrics are displayed only after the health check function is enabled. To enable this function, click the name of a VPN connection and add health check items on the **Summary** tab page.

- Average Tunnel RTT, Maximum Tunnel RTT, Tunnel Packet Loss Rate

These metrics are displayed only when **VPN Type** is set to **Static routing** and the NQA function is enabled.

3.6 Creating a Monitoring Alarm Rule

Scenarios

You can create monitoring alarm rules to customize monitored objects and notification policies, so that you can be well-informed of the VPN service status.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner of the management console, and choose **Management & Governance** > **Cloud Eye**.
4. Choose **Cloud Service Monitoring** > **Virtual Private Network VPN**, and configure alarm rules for different types of alarms as required.
   - Alarms related to VPN gateways in S2C Enterprise Edition VPN: Select **S2C VPN Gateway** from the drop-down list. On the **Resources** tab page, choose **More** > **Create Alarm Rule** in the **Operation** column.
   - Alarms related to VPN connections in S2C Enterprise Edition VPN: Select **S2C VPN Connection** from the drop-down list. On the **Resources** tab page, choose **More** > **Create Alarm Rule** in the **Operation** column.
   - Alarms related to VPN gateways in P2C VPN: Select **P2C VPN Gateway** from the drop-down list. On the **Resources** tab page, choose **More** > **Create Alarm Rule** in the **Operation** column.
5. Configure an alarm rule.
   - **Associate template**: By default, the alarm template **Virtual Private Network Alarm Template** is available. You can use this default template without creating a new one.
   - **Configure manually**: Create a custom alarm policy. After the policy is created, it is available in the **Associate template** drop-down list box.
6. Click **Create**.

   After the monitoring alarm rule is created, you will receive a notification once an alarm is generated.

   NOTE

   For more information about VPN alarm rules, see the ***Cloud Eye User Guide***.

3.7 Creating an Event Alarm Rule

Scenarios

You can create event alarm rules to customize the event monitoring scope and notification policies, so that you can be well-informed of the VPN service status.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner of the management console, and choose **Management & Governance** > **Cloud Eye**.
4. Click **Event Monitoring** from the navigation pane.
5. Click **Create Alarm Rule** in the upper right corner. The **Create Alarm Rule** page is displayed.
6. Configure an event alarm rule by referring to **Table 3-6**.

Table 3-6 Alarm parameters

Parameter	Description
Name	The system automatically generates a name. You can also change the name.
Alarm Type	Select **Event**.
Event Type	Select **System event**.
Event Source	Select **Virtual Private Network**.
Monitoring Scope	Select **All resources**.
Method	Set this parameter as required.
Alarm Policy	You are advised to select **Certificate to expire in 1 day**, **Certificate to expire in 3 days**, and **Certificate to expire in 7 days** so that the system will send alarm notifications seven days, three days, and one day before the certificate expires.
Notified By	Set this parameter as required. **NOTE** Alarm notifications are sent by the Simple Message Notification (SMN) service, which may incur a small amount of fees.

7. Click **Create**.

   After the event alarm rule is created, you will receive a notification once an alarm is generated.

4 Audit

4.1 Key Operations That Can Be Recorded by CTS

Table 4-1 Operations related to S2C Enterprise Edition VPN 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
Updating the specification of a pay-per-use VPN gateway	vpn-gateway	updatePostpaidVgwSpecification

Operation	Resource Type	Trace Name
Creating a VPN connection	vpn-connection	createVpnConnection
Updating a VPN connection	vpn-connection	updateVpnConnection
Deleting a VPN connection	vpn-connection	deleteVpnConnection
Creating a resource tag	instance	batchCreateResourceTags
Deleting a resource tag	instance	batchDeleteResourceTags
Querying the customer gateway list	customer-gateway	listCgws
Querying a customer gateway	customer-gateway	showCgw
Querying resource tags	instance	showResourceTags
Querying project tags	instance	listProjectTags
Querying resource instances by tag	instance	listResourcesByTags
Querying the number of resource instances by tag	instance	countResourcesByTags
Querying a VPN gateway	vpn-gateway	showVgw
Querying the AZs of VPN gateways	vpn-gateway	listExtendedAvailabilityZones
Querying the route table of a specified VPN gateway	vpn-gateway	showVpnGatewayRoutingTable
Querying the VPN connection list	vpn-connection	listVpnConnections
Querying a VPN connection	vpn-connection	showVpnConnection
Querying the VPN gateway list	vpn-connection	listVgws

Operation	Resource Type	Trace Name
Querying a VPN connection monitor	vpn-connection	showConnectionMonitor
Querying the VPN connection monitor list	vpn-connection	listConnectionMonitors
Querying quotas of a specified tenant	quota	showQuotasInfo
Querying VPN connection logs	vpn-connection	queryVpnConnectionLog
Creating VPN connections in batches	vpn-connection	batchCreateVpnConnection

Table 4-2 Operations related to P2C VPN that can be recorded by CTS

Operation	Resource Type	Trace Name
Subscribing to resources	p2c-vpn-gateway	subscribeP2cVgw
Updating the specification of a yearly/monthly VPN gateway	p2c-vpn-gateway	updateP2cVgwSpecification
Changing the resource status (frozen or unfrozen)	p2c-vpn-gateway	updateP2cVgwStatus
Unsubscribing from resources	p2c-vpn-gateway	unsubscribeP2cVgw
Updating a P2C VPN gateway	p2c-vpn-gateway	updateP2cVgw
Creating an SSL server	vpn-server	createVpnServer
Modifying an SSL server	vpn-server	updateVpnServer
Creating a VPN user	vpn-user	createVpnUser

Operation	Resource Type	Trace Name
Modifying a VPN user	vpn-user	updateVpnUser
Changing the password of a VPN user	vpn-user	updateVpnUserPassword
Resetting the password of a VPN user	vpn-user	resetVpnUserPassword
Deleting a VPN user	vpn-user	deleteVpnUser
Creating a VPN user group	vpn-user-group	createVpnUserGroup
Modifying a VPN user group	vpn-user-group	updateVpnUserGroup
Adding a user to a VPN user group	vpn-user-group	addVpnUsersToGroup
Removing a user from a VPN user group	vpn-user-group	removeVpnUsersToGroup
Creating a VPN access policy	vpn-access-policy	createVpnAccessPolicy
Modifying a VPN access policy	vpn-access-policy	updateVpnAccessPolicy
Deleting a VPN access policy	vpn-access-policy	deleteVpnAccessPolicy
Downloading the client configuration file	vpn-server	exportClientConfig
Importing a client CA certificate	vpn-server	importClientCa
Modifying a client CA certificate	vpn-server	updateClientCa
Deleting a client CA certificate	vpn-server	deleteClientCa
Creating resource tags in batches	p2c-vpn-gateway	batchCreateResourceTags
Deleting resource tags in batches	p2c-vpn-gateway	batchDeleteResourceTags

Operation	Resource Type	Trace Name
Querying the P2C VPN gateway list	p2c-vpn-gateway	listP2cVgws
Querying a P2C VPN gateway with a specified ID	p2c-vpn-gateway	showP2cVgw
Querying the AZs of a P2C VPN gateway	p2c-vpn-gateway	listP2cVgwAvailabilityZones
Querying the connections of a P2C VPN gateway	p2c-vpn-gateway	listP2cVgwConnections
Querying tags of a specific instance	p2c-vpn-gateway	listTagsForResource
Querying the tags of all resources owned by a tenant in a specified project	p2c-vpn-gateway	listTags
Querying the VPN access policy list	vpn-access-policy	listVpnAccessPolicies
Querying a VPN access policy	vpn-access-policy	showVpnAccessPolicy
Querying server information on a gateway	vpn-server	listVpnServersByVgw
Querying a client CA certificate	vpn-server	showClientCa
Querying information about all servers of a tenant	vpn-server	listVpnServersByProject
Querying the VPN user list	vpn-user	listVpnUsers
Querying a VPN user	vpn-user	showVpnUser
Querying the VPN user group list	vpn-user	listVpnUserGroups
Querying a VPN user group	vpn-user	showVpnUserGroup

Operation	Resource Type	Trace Name
Querying VPN users in a group	vpn-user	listVpnUsersInGroup
Creating VPN users in batches	vpn-user	batchCreateVpnUsers
Deleting VPN users in batches	vpn-user	batchDeleteVpnUsers
Creating or updating the connection log configuration	p2c-vpn-gateway	updateVpnConnectionsLogConfig
Deleting the connection log configuration	p2c-vpn-gateway	deleteVpnConnectionsLogConfig
Querying the connection log configuration	p2c-vpn-gateway	showVpnConnectionsLogConfig
Tearing down connections of a P2C VPN gateway	p2c-vpn-gateway	disconnectP2cVgwConnection

4.2 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**.

5 Permissions Management

5.1 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 users only the permissions required to perform a given task based on their job responsibilities.
- 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 meets your permissions requirements, you can skip this section.

This section describes the procedure for granting permissions (see **Figure 5-1**).

Prerequisites

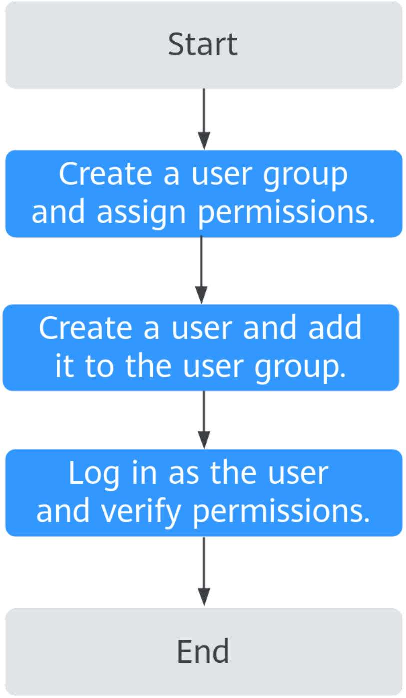
You have learned about the permissions supported by VPN (see **Permission Management**), and determined the permissions to be granted to a user group. Before granting permissions of other services, learn about all **permissions** supported by IAM.

NOTE

The authentication feature of S2C VPN is bound to the enterprise project feature. If the enterprise project feature is not enabled for a user account, authentication cannot be performed for this user account.

Process Flow

Figure 5-1 Process of granting VPN permissions


Start
Create a user group and assign permissions.
Create a user and add it to the user group.
Log in as the user and verify permissions.
End

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console and attach the **VPN FullAccess** 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 the **S2C VPN Gateways** tab, and click **Buy S2C VPN Gateway** to create a VPN gateway. If the VPN gateway is successfully created, the **VPN FullAccess** policy has already taken effect.

   – Click **Service List** and choose **Networking** > **Virtual Private Network**. On the **Enterprise – VPN Gateways** page, click the **P2C VPN Gateways** tab, and click **Buy P2C VPN Gateway** in the upper right corner to create a VPN gateway. If the VPN gateway is successfully created, the **VPN FullAccess** policy has already taken effect.

   – Select any service except the VPN service in **Service List**. Assume that the current policy contains only **VPN FullAccess**. If a message appears indicating that you have insufficient permissions to access the service, the **VPN FullAccess** policy has already taken effect.

5.2 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.

  You need to add the following dependent actions. If they are not added, an exception may occur when you delete a VPN gateway.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpn:vpnGateways:delete"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "vpc:subNetworkInterfaces:update",
                "vpc:routeTables:update",
                "vpc:subnets:delete",
                "vpc:publicIps:list",
                "vpc:publicIps:delete",
                "vpc:vpcs:get",
                "vpc:routeTables:get",
                "vpc:ports:get",
                "vpc:ports:delete",
                "vpc:publicIps:update",
                "vpc:subnets:get",
                "vpc:bandwidths:list",
                "vpc:publicIps:get",
                "vpc:vpcs:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "er:instances:get",
                "er:instances:list"
            ]
        }
    ]
}
```

- 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 the actions of one or multiple services that are of the same type (global or project-level). The following is an example policy containing multiple actions.

```
{
    "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"
            ]
        }
    ]
}
```

6 Tag Management

6.1 Scenario

VPN tags are used to identify VPN resources, facilitating VPN resource identification and management. You can add tags for a VPN resource when you create the VPN resource. Alternatively, you add tags for an existing VPN resource on the resource details page. A maximum of 20 tags can be added for each VPN resource.

NOTE

Only S2C Enterprise Edition VPN and P2C VPN support VPN tag management.

A tag consists of a key and a value. **Table 6-1** describes the requirements on the keys and values of VPN tags.

Table 6-1 Requirements on the keys and values of VPN tags

Parameter	Requirement	Example Value
Key	● Cannot be left blank. ● Must be unique for the same VPN. ● Can contain a maximum of 128 characters. ● Can contain only the following types of characters: – Digits – Spaces – Letters – Special characters, including _ . : - = + @ ● Cannot start or end with a space or start with **_sys_**.	vpn_key1

Parameter	Requirement	Example Value
Value	● Can contain a maximum of 255 characters. ● Can contain only the following types of characters: – Digits – Spaces – Letters – Special characters, including . : - = + @ / _	vpn-01

6.2 S2C Enterprise Edition VPN

6.2.1 Searching for Resources by Tag

Context

You can search for VPN gateways, customer gateways, and VPN connections based on the tag keys and values that have been added for these VPN resources.

Procedure

Searching for VPN gateways in S2C Enterprise Edition VPN by tag

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.

   The system displays the VPN gateways that match the selected tag key and value.

   – You can only select existing keys and values from the drop-down list.

   – You can select multiple tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.

   – You can use tags together with other types of filter criteria. The relationship between them is AND.

Searching for customer gateways in S2C Enterprise Edition VPN by tag

1. Log in to the management console.

2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.

   The system displays the customer gateways that match the selected tag key and value.

   – You can only select existing keys and values from the drop-down list.

   – You can select multiple tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.

   – You can use tags together with other types of filter criteria. The relationship between them is AND.

Searching for VPN connections in S2C Enterprise Edition VPN by tag

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.

   The system displays the VPN connections that match the selected tag key and value.

   – You can only select existing keys and values from the drop-down list.

   – You can select multiple tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.

   – You can use tags together with other types of filter criteria. The relationship between them is AND.

6.2.2 Managing Tags

Context

You can add, delete, modify, and view tags of VPN resources.

Procedure

- **Managing tags of VPN gateways in S2C Enterprise Edition VPN**

  a. Log in to the management console.

  b. Click 📍 in the upper left corner and select the desired region and project.

c. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

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

e. Click the name of the target VPN gateway. The VPN gateway details page is displayed.

f. Click the **Tags** tab, and add, delete, modify, or view tags of the VPN gateway.

   ▪ Add a tag.

     Click **Add Tag**. In the **Add Tag** dialog box, enter the key and value of a tag to be added, and click **OK**.

   ▪ Modify a tag.

     Click **Edit** in the **Operation** column of the tag to be modified. In the **Edit Tag** dialog box, change the tag value and click **OK**.

   ▪ Delete a tag.

     Click **Delete** in the **Operation** column of the tag to be deleted. In the **Delete Tag** dialog box, click **OK**.

   ▪ View tags.

     On the **Tags** page, view tag details, including the number of new tags that can be created and the key and value of each existing tag.

- **Managing tags of customer gateways in S2C Enterprise Edition VPN**

a. Log in to the management console.

b. Click 📍 in the upper left corner and select the desired region and project.

c. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

d. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.

e. Click the name of the target customer gateway. The customer gateway details page is displayed.

f. In the **Tags** area, add, delete, modify, or view tags of the customer gateway.

   ▪ Add a tag.

     Click **Add**. In the **Add Tag** dialog box, enter the key and value of a tag to be added, and click **OK**.

   ▪ Modify a tag.

     Click **Edit** in the **Operation** column of the tag to be modified. In the **Edit Tag** dialog box, change the tag value and click **OK**.

   ▪ Delete a tag.

     Click **Delete** in the **Operation** column of the tag to be deleted. In the **Delete Tag** dialog box, click **OK**.

    - View tags.

      In the **Tags** area, view tag details, including the number of new tags that can be created and the key and value of each existing tag.

- **Managing tags of VPN connections in S2C Enterprise Edition VPN**

  a. Log in to the management console.

  b. Click 📍 in the upper left corner and select the desired region and project.

  c. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.

  d. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.

  e. Click the name of the target VPN connection. The VPN connection details page is displayed.

  f. Click the **Tags** tab, and add, delete, modify, or view tags of the VPN connection.

    - Add a tag.

      Click **Add Tag**. In the **Add Tag** dialog box, enter the key and value of a tag to be added, and click **OK**.

    - Modify a tag.

      Click **Edit** in the **Operation** column of the tag to be modified. In the **Edit Tag** dialog box, change the tag value and click **OK**.

    - Delete a tag.

      Click **Delete** in the **Operation** column of the tag to be deleted. In the **Delete Tag** dialog box, click **OK**.

    - View tags.

      On the **Tags** page, view tag details, including the number of new tags that can be created and the key and value of each existing tag.

6.3 P2C VPN

6.3.1 Searching for Resources by Tag

Context

You can search for VPN gateways based on the tag keys and values that have been added for them.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.

3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.
6. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value to search for the target VPN gateway.
   - You can only select existing keys and values from the drop-down list.
   - You can select multiple tags to search for VPN resources. If you select multiple tags, the relationship between them is OR.
   - You can use tags together with other types of filter criteria. The relationship between them is OR.

6.3.2 Managing Tags

Context

You can add, delete, modify, and view tags of VPN resources.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Click ☰ in the upper left corner, and choose **Networking** > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab. The P2C VPN gateway list is displayed.
6. Click the name of the target VPN gateway. The VPN gateway details page is displayed.
7. Click the **Tags** tab, and add, delete, modify, or view tags of the VPN gateway.
   - Add a tag.

     Click **Add Tag**. In the **Add Tag** dialog box, enter the key and value of a tag to be added, and click **OK**.
   - Modify a tag.

     Click **Edit** in the **Operation** column of the tag to be modified. In the **Edit Tag** dialog box, change the tag value and click **OK**.
   - Delete a tag.

     Click **Delete** in the **Operation** column of the tag to be deleted. In the **Delete Tag** dialog box, click **OK**.
   - View tags.

     On the **Tags** tab page, view tag details, including the number of new tags that can be created and the key and value of each existing tag.

7 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

- S2C Enterprise Edition VPN resources include VPN gateways, VPN connection groups, and customer gateways.
- P2C VPN resources include only VPN gateways.

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

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