

Virtual Private Network

API Reference

Issue 01
Date 2025-07-30



Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

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 Before You Start

Overview

A Virtual Private Network (VPN) establishes an encrypted, Internet-based communication tunnel between your network and a Virtual Private Cloud (VPC). By default, Elastic Cloud Servers (ECSs) in a VPC cannot communicate with devices in your on-premises data center or private network. To enable communication between them, you can enable a VPN. There are two types of VPN services: Site-to-Cloud VPN (S2C VPN) and Point-to-Cloud VPN (P2C VPN). S2C VPN allows you to establish secure, reliable, and cost-effective encrypted connections between your on-premises network or data center and a virtual cloud network on Huawei Cloud. P2C VPN allows you to establish secure, reliable, and cost-effective encrypted connections between your office software and a virtual network on Huawei Cloud.

This document describes how to use application programming interfaces (APIs) to perform operations on VPNs, such as creating, querying, deleting, and updating VPNs. For details about all supported operations, see [API Overview](#).

If you plan to use APIs of the VPN service, ensure that you are familiar with concepts of VPN. For details, see [Service Overview](#) in the VPN product documentation.

API Calling

VPN supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS. For details, see [Calling APIs](#).

Endpoints

An endpoint is the request address for calling an API. Endpoints vary according to services and regions.

Constraints

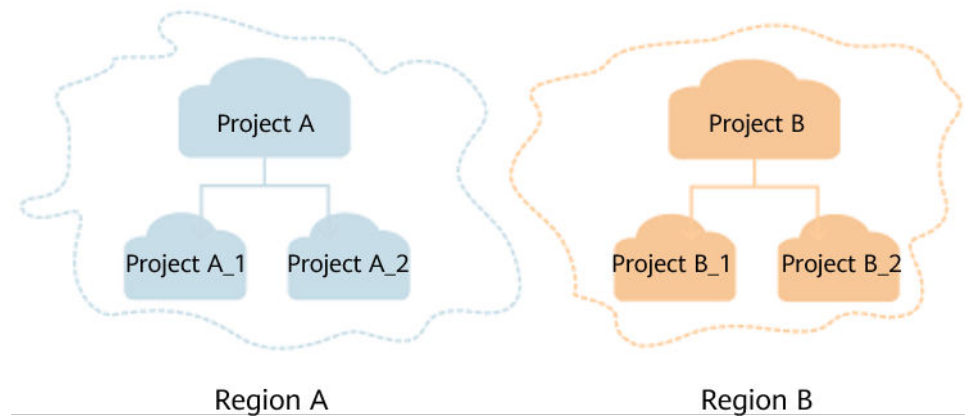
The number of VPN resources that you can create is determined by your quota. You can view or increase the quota by referring to [What Quotas Does a VPN Have?](#).

For more constraints, see description of each API.

Basic Concepts

- **Account**
An account is created upon successful registration. The account has full access permissions on all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity, and using it to perform routine management is not recommended. Instead, you are advised to create Identity and Access Management (IAM) users and grant routine management permissions to the users.
- **User**
You can use your account to create IAM users for routine management of specific cloud services. These users have their own identity credentials (such as passwords and access keys).
To view your account ID and IAM user ID, log in to the console, click your account in the upper right corner, and choose **My Credentials**. The account name, username, and password will be required for API authentication.
- **Region**
Regions are divided based on geographical locations and network latency. Public services, such as ECS, Elastic Volume Service (EVS), Object Storage Service (OBS), VPC, Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region.
Regions are classified into universal regions and dedicated regions.
 - A universal region provides universal cloud services for common tenants.
 - A dedicated region provides specific services for specific tenants.
- **Availability zone (AZ)**
An AZ comprises one or more physical data centers equipped with independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are connected using high-speed optical fibers, allowing you to build highly available systems across AZs.
- **Project**
Projects group and isolate resources (including compute, storage, and network resources) across physical regions. A default project is provided for each region. Users can be granted permissions to access all resources in a specific project. If you need more refined access control, create subprojects under a default project and create resources in subprojects. Then, you can assign users the permissions to access resources only in the specific subprojects.

Figure 1-1 Project isolation model



To view a project ID, log in to the console, click your account in the upper right corner, and choose **My Credentials**.

- Enterprise project

Enterprise projects group and manage resources across regions. Resources in different enterprise projects are logically isolated. An enterprise project can contain resources across multiple regions, and resources can be added to or removed from enterprise projects.

For more information about enterprise projects and how to obtain enterprise project IDs, see the [Enterprise Management User Guide](#).

2 API Overview

Table 2-1 lists the APIs provided by the VPN service. For details about API permissions, see [Permission Policies and Supported Actions](#).

Table 2-1 VPN APIs

API Type		Description
S2C VPN APIs	VPN Gateway	APIs for creating, querying, updating, and deleting S2C VPN gateways, and querying AZs of S2C VPN gateways.
	Customer Gateway	APIs for creating, querying, updating, and deleting customer gateways.
	VPN Connection	APIs for creating, querying, updating, and deleting VPN connections.
	VPN Connection Monitor	APIs for creating, querying, and deleting VPN connection health checks.
P2C VPN API	VPN Gateway	APIs for querying and modifying P2C VPN gateways, querying AZs of P2C VPN gateways, querying the P2C VPN connection list, and tearing down connections.
	Server	APIs for creating, querying, modifying, and exporting the client configuration on the server, as well as importing, querying, modifying, and deleting client CA certificates.
	User Management	APIs for creating, querying, modifying, and deleting VPN users, as well as changing and resetting user passwords; and APIs for creating/batch creating, querying, modifying, and deleting/batch deleting VPN user groups, adding VPN users to groups, removing VPN users from groups, and querying VPN users in groups.

API Type		Description
	Access Policy	APIs for creating, querying, modifying, and deleting VPN access policies.
Public Service APIs	VPN Quota	API for querying quotas.
	VPN Tag	APIs for querying, adding, and deleting tags.

3 Calling APIs

3.1 Request

This section describes the structure of a REST API request, and uses the IAM API for [creating an IAM user as an administrator](#) as an example to demonstrate how to call an API. The user token obtained by this API can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

{URI-scheme}://{Endpoint}/{resource-path}?{query-string}

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be separately transmitted.

Table 3-1 Parameters in a URI

Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use HTTPS.
Endpoint	Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions.
resource-path	Resource path of an API. Obtain the path from the URI of an API. For example, the resource-path of the API for obtaining a user token is /v3/auth/tokens .
query-string	(Optional) Query parameter. Ensure that a question mark (?) is included in front of each query parameter, which is in the format of <i>Parameter name=Parameter value</i> . For example, ?limit=10 indicates that a maximum of 10 data records can be queried.

 NOTE

To simplify the URI display, this document provides only the **resource-path** and request method in the URI of each API. The **URI-scheme** of all APIs is **https**, and the endpoints in a region are the same.

Request Methods

The HTTP protocol defines the following request methods for sending requests to a server.

Table 3-2 HTTP methods

Method	Description
GET	Requests a server to return specified resources.
PUT	Requests a server to update specified resources.
POST	Requests a server to add resources or perform special operations.
DELETE	Requests a server to delete a specified resource (for example, an object).
HEAD	Requests resource headers from a server.
PATCH	Requests a server to update part of specified resources. If the requested resource does not exist, the server may create a resource using the PATCH method.

For example, in the URI used to [create an IAM user as an administrator](#), the request method is POST. The request is as follows:

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-USER/users
```

Request Header

You can add additional fields, such as the fields required by a specified URI or HTTP method, to a request header. For example, to request authentication information, you can add **Content-Type** to specify the type of the request body.

For details about common request headers, see [Table 3-3](#).

Table 3-3 Common fields in request headers

Parameter	Description	Mandatory	Example
Host	Specifies the server to which a request is sent, which can be obtained from the URL of the service API. The value is in the format of <i>Host name:Port number</i> . If the port number is not specified, the default port is used. The default port number for https is 443 .	No This field is mandatory for access key (AK)/secret access key (SK) authentication.	code.test.com or code.test.com:443
Content-Type	Specifies the type (or format) of a message body. The default value <i>application/json</i> is recommended. Other values will be described in the specific APIs.	Yes	application/json
Content-Length	Specifies the length of a request body, in bytes.	No	3495
X-Project-Id	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .	No This field is mandatory for requests that use AK/SK authentication in the Dedicated Cloud (DeC) scenario or multi-project scenario.	e9993fc7*****baa340f9c0f4

Parameter	Description	Mandatory	Example
X-Auth-Token	Specifies a user token. A user token is carried in a response to the API for obtaining a user token. This API is the only one that does not require authentication. The value of X-Subject-Token in the response header is the token.	No This field is mandatory for token authentication.	The following is part of an example token: MIIPAgYJKoZIhvcNAQc-Co...ggg1BBIINPXsidG9rZ

 NOTE

APIs also support AK/SK authentication, which uses SDKs to sign a request. During the signature, the **Authorization** (signature authentication) and **X-Sdk-Date** (time when a request is sent) headers are automatically added to the request.

For details about AK/SK authentication, see [Authentication](#).

When the API used to **create an IAM user as an administrator** uses AK/SK authentication, the request with the header added is as follows:

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-USER/users
```

```
Content-Type: application/json
```

(Optional) Request Body

The response body is optional. A request body is generally sent in a structured format (for example, JSON or XML), which is specified by **Content-Type** in the request header. It is used to transfer content other than the request header. If the request body contains full-width characters, these characters must be coded in UTF-8.

Request bodies vary according to APIs. Some APIs do not require a request body, such as the APIs called using the GET and DELETE methods.

For the API used to **create an IAM user as an administrator**, you can obtain the request parameters and parameter description from the API request. The following provides an example request with a body included. Replace the values in bold with the actual ones.

- **accountid** is the ID of the account to which an IAM user belongs.
- **username** is the IAM username to be created.

- **email** is the email address of the IAM user.
- ********* is the login password of the IAM user.

POST https://iam.myhuaweicloud.eu/v3.0/OS-USER/users

Content-Type: application/json

X-Sdk-Date: 20240416T095341Z

Authorization: SDK-HMAC-SHA256 Access=*****, SignedHeaders=content-type;host;x-sdk-date,
Signature=*****

```
{
  "user": {
    "domain_id": "accountid",
    "name": "username",
    "password": "*****",
    "email": "email",
    "description": "IAM User Description"
  }
}
```

If all data required by an API request is available, you can send the request to call the API through [curl](#), [Postman](#), or coding. In the response to the API for obtaining a user token, **x-subject-token** carries a user token. You can use this token to authenticate the calling of other APIs.

3.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token authentication: Requests are authenticated using tokens.
- AK/SK authentication: Requests are encrypted using AK/SK pairs. AK/SK authentication is recommended as it is more secure than token authentication.

Token Authentication

NOTE

A token is valid for 24 hours. When using a token for authentication, cache it to avoid frequent calling.

A token is used to acquire temporary permissions. During API authentication using a token, the token is added to the request header to get permissions for calling the API. You can obtain a token by calling the API used to [obtain a user token](#).

A cloud service can be deployed as either a project-level service or global service.

- For a project-level service, you need to obtain a project-level token by setting **auth.scope** in the request body to **project**.
- For a global service, you need to obtain a global token by setting **auth.scope** in the request body to **domain**.

A project-level token is required for calling APIs of the VPN service. As such, set **auth.scope** in the request body to **project** when you call the API for [obtaining a user token](#).

```
{
  "auth": {
```

```
{
  "identity": {
    "methods": [
      "password"
    ],
    "password": {
      "user": {
        "name": "username",
        "password": "*****",
        "domain": {
          "name": "domainname"
        }
      }
    }
  },
  "scope": {
    "project": {
      "name": "xxxxxxx"
    }
  }
}
```

After obtaining a token, add the **X-Auth-Token** field specifying the token to the request header when calling other APIs. For example, when the token is **ABCDEFGF....**, add **X-Auth-Token: ABCDEFG....** to the request header as follows:

```
POST https://iam.myhuaweicloud.eu/v3.0/OS-USER/users
```

```
Content-Type: application/json
X-Auth-Token: ABCDEFG....
```

AK/SK Authentication

NOTE

AK/SK authentication supports API requests with a body size not larger than 12 MB. For API requests with larger sizes, use token authentication.

In AK/SK-based authentication, AK/SK is used to sign requests, and the signature is then added to the request header for authentication.

- AK: access key, which is a unique identifier used together with an SK to sign requests cryptographically.
- SK: secret access key, which is used together with an AK to sign requests cryptographically. It identifies a request sender and prevents the requests from being modified.

In AK/SK authentication, you can use an AK/SK to sign requests based on the signature algorithm or using the signing SDK. For details about how to sign requests and use the signing SDK, see [API Request Signing Guide](#).

NOTE

Different from the SDKs provided by services, the signing SDK is used only for signing.

3.3 Response

Status Code

After sending a request, you can receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a response. For more information, see [A.2 Status Codes](#).

If status code 201 is returned after the API used to [create an IAM user as an administrator](#) is called, the request is successful.

Response Header

Like a request, a response also has a header, for example, **Content-Type**.

The response header shown in [Figure 3-1](#) is returned for the API used to [create an IAM user as an administrator](#).

Figure 3-1 Response header for the API used to create an IAM user as an administrator

```
"X-Frame-Options": "SAMEORIGIN",
"X-IAM-ETag-id": "2562365939-d8f6f12921974cb097338ac11fceac8a",
"Transfer-Encoding": "chunked",
"Strict-Transport-Security": "max-age=31536000; includeSubdomains;",
"Server": "api-gateway",
"X-Request-Id": "af2953f2bcc67a42325a69a19e6c32a2",
"X-Content-Type-Options": "nosniff",
"Connection": "keep-alive",
"X-Download-Options": "noopen",
"X-XSS-Protection": "1; mode=block;",
"X-IAM-Trace-Id": "token_ null_af2953f2bcc67a42325a69a19e6c32a2",
"Date": "Tue, 21 May 2024 09:03:40 GMT",
"Content-Type": "application/json; charset=utf8"
```

Response Body

The response body is optional. A response body is generally returned in a structured format (for example, JSON or XML), which is specified by **Content-Type** in the response header. It is used to transfer content other than the response header.

The following provides part of the response body returned for the API used to [create an IAM user as an administrator](#).

```
{
  "user": {
    "id": "c131886aec...",
    "name": "IAMUser",
    "description": "IAM User Description",
    "areacode": "",
    "phone": "",
    "email": "***@***.com",
    "status": null,
    "enabled": true,
    "pwd_status": false,
    "access_mode": "default",
    "is_domain_owner": false,
    "xuser_id": "",
    "xuser_type": "",
    "password_expires_at": null,
    "create_time": "2024-05-21T09:03:41.000000",
    "domain_id": "d78cbac1.....",
    "xdomain_id": "30086000.....",
    "xdomain_type": ""
  }
}
```

```
    "default_project_id": null  
  }  
}
```

If an error occurs during API calling, an error code and an error message will be displayed. The following is an example of an error response body.

```
{  
  "error_msg": "Request body is invalid.",  
  "error_code": "IAM.0011"  
}
```

error_code specifies an error code, and **error_msg** describes the error.

4 API

4.1 S2C VPN APIs

4.1.1 S2C VPN Gateway

4.1.1.1 Creating a VPN Gateway

Function

This API is used to create a VPN gateway. Currently, only pay-per-use VPN gateways can be created.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/vpn-gateways

Table 4-1 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Request

- Request parameters

Table 4-2 Request parameters

Parameter	Type	Mandatory	Description
vpn_gateway	CreateVgwRequestBodyContent object	Yes	Specifies the VPN gateway object.

Table 4-3 CreateVgwRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies the name of a VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.). - If this parameter is not specified, a name in the format of vpngw-**** is automatically generated, for example, vpngw-a45b.
network_type	String	No	- Specifies the network type of the VPN gateway. A public VPN gateway (public) uses EIPs to connect to a customer gateway. A private VPN gateway (private) uses private IP addresses in a VPC to connect to a customer gateway. - The value can be public or private. - The default value is public.
attachment_type	String	No	- Specifies the association mode. - The value can be vpc or er. - The default value is vpc.
ip_version	String	No	- Specifies the IP protocol version of the VPN gateway. - The value is ipv4. - The default value is ipv4.

Parameter	Type	Mandatory	Description
er_id	String	No	- Specifies the ID of the enterprise router instance to which the VPN gateway connects. - The value is a UUID containing 36 characters. Set this parameter only when attachment_type is set to er. Either er_id or vpc_id must be specified.
vpc_id	String	No	- Function description: - When attachment_type is set to vpc, vpc_id specifies the ID of the service VPC associated with the VPN gateway. - When attachment_type is set to er, vpc_id specifies the ID of the access VPC used by the VPN gateway. In this case, any VPC ID can be used. - The value is a UUID containing 36 characters. When attachment_type is set to vpc, this parameter is mandatory. When attachment_type is set to er, this parameter is optional; if both vpc_id and access_vpc_id are set, the access_vpc_id value is used. Either vpc_id or er_id must be specified. You can obtain the VPC ID by querying VPCs.

Parameter	Type	Mandatory	Description
local_subnets	Array of String	No	- Specifies an IPv4 local subnet. This subnet is a cloud-side subnet that needs to communicate with an on-premises customer subnet through a VPN. A maximum of 50 local subnets can be specified for each VPN gateway. For example, a local subnet can be 192.168.52.0/24. - This parameter is mandatory only when attachment_type is set to vpc and ip_version is set to ipv4.
connect_subnet	String	No	- Specifies the ID of the VPC subnet used by the VPN gateway. - The value is a UUID containing 36 characters. When attachment_type is set to vpc, this parameter is mandatory. When attachment_type is set to er, this parameter is optional; if both connect_subnet and access_subnet_id are set, the access_subnet_id value is used. When attachment_type is set to er, the subnet must have at least two idle IP addresses. When attachment_type is set to vpc, the subnet must have at least four idle IP addresses if the values of access_subnet_id and connect_subnet are the same or must have at least two idle IP addresses if the values of access_subnet_id and connect_subnet are different.
bgp_asn	Long	No	- Specifies the BGP AS number of the VPN gateway. - The value ranges from 1 to 4294967295. - The default value is 64512.

Parameter	Type	Mandatory	Description
flavor	String	No	- Specifies the specification of the VPN gateway. For the value range, see the Specification parameter on the page for creating a VPN gateway on the VPN console. - Value range: - Professional1 - Professional2 - The default value is Professional1.
availability_zone_ids	Array of String	No	- Specifies the AZ where the VPN gateway is to be deployed. If this parameter is not specified, one or two AZs are automatically selected for the VPN gateway. Before specifying AZs, you need to query the available AZ list by referring to Querying the AZs of VPN Gateways, and determine the AZs supported for the VPN gateway based on the combination of parameters flavor, attachment_type, and ip_version. - Constraints: If two or more AZs are supported for the VPN gateway, specify two AZs. If only one AZ is supported for the VPN gateway, specify one AZ. If no AZ is supported, the VPN gateway cannot be created.
enterprise_project_id	String	No	- Specifies an enterprise project ID. - The value is a UUID (36 characters) or 0. - The default value is 0, indicating that the resource belongs to the default enterprise project.

Parameter	Type	Mandatory	Description
eip1	CreateRequestEip object	No	- Specifies the first EIP of the VPN gateway using the active-active mode or the active EIP of the VPN gateway using the active-standby mode. - Set this parameter only when network_type is set to public.
eip2	CreateRequestEip object	No	- Specifies the second EIP of the VPN gateway using the active-active mode or the standby EIP of the VPN gateway using the active-standby mode. - Set this parameter only when network_type is set to public.
access_vpc_id	String	No	- Specifies the ID of the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters. - By default, the value is the same as the value of vpc_id. You can obtain the VPC ID by querying VPCs.
access_subnet_id	String	No	- Specifies the ID of the subnet in the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters. When attachment_type is set to er, the subnet must have at least two idle IP addresses. When attachment_type is set to vpc, the subnet must have at least four idle IP addresses if the values of access_subnet_id and connect_subnet are the same or must have at least two idle IP addresses if the values of access_subnet_id and connect_subnet are different. - By default, the value is the same as the value of connect_subnet.

Parameter	Type	Mandatory	Description
ha_mode	String	No	- Specifies the HA mode of the gateway. The value can be active-active or active-standby. - Value range: active-active, active-standby - Default value: active-active
access_private_ip_1	String	No	- Specifies private IP address 1 of a private VPN gateway. Set this parameter if a private VPN gateway needs to use specified IP addresses. In active/standby gateway mode, the specified IP address is the active IP address. In active-active gateway mode, the specified IP address is active IP address 1. - Value range: allocatable IP addresses in the access subnet - This parameter must be specified together with access_private_ip_2, and the two parameters must have different values.
access_private_ip_2	String	No	- Specifies private IP address 2 of a private VPN gateway. Set this parameter if a private VPN gateway needs to use specified IP addresses. In active/standby gateway mode, the specified IP address is the standby IP address. In active-active gateway mode, the specified IP address is active IP address 2. - Value range: allocatable IP addresses in the access subnet - This parameter must be specified together with access_private_ip_1, and the two parameters must have different values.
tags	Array of VpnResourceTag objects	No	- Specifies a tag list. - A maximum of 20 tags can be specified.

Table 4-4 CreateRequestEip

Parameter	Type	Mandatory	Description
id	String	No	- Specifies an EIP ID. - The value is a UUID containing 36 characters. - Set this parameter only when an existing EIP is used. You can obtain the EIP ID by referring to Querying EIPs .
type	String	No	- Specifies the EIP type. - The value is a string of 0 to 36 characters. For the value range, see the type field in Table 7 in Assigning an EIP. The value 5_bgp is preferred if it is supported. - Set this parameter only when a new EIP is used. For more constraints, see the type field in Table 4 in Assigning an EIP.
charge_mode	String	No	- Specifies the billing mode of EIP bandwidth. - Value range: bandwidth: billed by bandwidth traffic: billed by traffic - This parameter is mandatory only when a new EIP not binding to shared bandwidth is created. - The default value is bandwidth.

Parameter	Type	Mandatory	Description
bandwidth_size	Integer	No	- Specifies the bandwidth (Mbit/s) of an EIP. The maximum EIP bandwidth varies according to regions and depends on the EIP service. You can submit a service ticket to increase the maximum EIP bandwidth under your account. - The value ranges from 1 to 1000. For details, see the EIP documentation. - This parameter is mandatory only when a new EIP not binding to shared bandwidth is created. The value cannot be greater than 300 when flavor is set to Professional1. The value cannot be greater than 1000 when flavor is set to Professional2.
bandwidth_name	String	No	- Specifies the bandwidth name of an EIP. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.). - This parameter is mandatory only when a new EIP not binding to shared bandwidth is created. - When a new EIP is used and this parameter is not set, an EIP bandwidth name in the format of vpngw-bandwidth-**** is automatically generated, for example, vpngw-bandwidth-e1fa.
bandwidth_id	String	No	- Specifies a bandwidth ID. You can specify existing shared bandwidth when creating an EIP. - The value is a UUID containing 36 characters. - This parameter is mandatory only when you want to bind shared bandwidth to an EIP.

Table 4-5 VpnResourceTag

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	Yes	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example requests

- a. Create a VPN gateway that uses existing EIPs and is associated with a VPC.

POST https://{Endpoint}/v5/{project_id}/vpn-gateways

```
{
  "vpn_gateway": {
    "vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "local_subnets": [
      "192.168.0.0/24", "192.168.1.0/24"
    ],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "eip1": {
      "id": "cff40e5e-demo-a8df-va86-7366077bf097"
    },
    "eip2": {
      "id": "d290f1ee-demo-a8df-va86-d701748f0851"
    }
  }
}
```

- b. Create a VPN gateway that uses new EIPs and is associated with an enterprise router.

POST https://{Endpoint}/v5/{project_id}/vpn-gateways

```
{
  "vpn_gateway": {
    "name": "vpngw-1234",
    "attachment_type": "er",
    "er_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "vpc_id": "584a238f-demo-a8df-va86-edca746f6277",
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "bgp_asn": 65533,
    "flavor": "Professional2",
    "availability_zone_ids": [
      "cn-south-1f",
      "cn-south-1e"
    ],
    "eip1": {
      "type": "5_bgp",

```

```
        "charge_mode": "bandwidth",
        "bandwidth_size": 1000,
        "bandwidth_name": "vpngw-bandwidth-1391"
      },
      "eip2": {
        "type": "5_bgp",
        "charge_mode": "bandwidth",
        "bandwidth_size": 1000,
        "bandwidth_name": "vpngw-bandwidth-1392"
      }
    }
  }
}
```

c. Create a private VPN gateway associated with a VPC.

POST https://{Endpoint}/v5/{project_id}/vpn-gateways

```
{
  "vpn_gateway": {
    "vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "local_subnets": [
      "192.168.0.0/24", "192.168.1.0/24"
    ],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "network_type": "private"
  }
}
```

Response

- Response parameters
- Returned status code 201: successful operation

Table 4-6 Parameters in the response body

Parameter	Type	Description
vpn_gateway	ResponseVpn Gateway object	Specifies the VPN gateway object.
request_id	String	Specifies a request ID.

Table 4-7 ResponseVpnGateway

Parameter	Type	Description
id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).

Parameter	Type	Description
network_type	String	- Specifies the network type of the VPN gateway. - The value can be public or private. - The default value is public.
attachment_type	String	- Specifies the association mode. - The value can be vpc or er.
ip_version	String	- Specifies the IP protocol version of the VPN gateway. - The value is ipv4.
er_id	String	Specifies the ID of the enterprise router instance to which the VPN gateway connects. This parameter is available only when attachment_type is set to er .
vpc_id	String	When attachment_type is set to vpc , vpc_id specifies the ID of the service VPC associated with the VPN gateway. This parameter is not returned when attachment_type is set to er . To view the ID of the access VPC used by the VPN gateway, check the access_vpc_id field.
local_subnets	Array of String	Specifies an IPv4 local subnet. This subnet is a cloud-side subnet that needs to communicate with an on-premises network through a VPN. An example subnet is 192.168.52.0/24. This parameter is returned only when attachment_type is set to vpc and ip_version is set to ipv4 .
connect_subnet	String	Specifies the ID of the VPC subnet used by the VPN gateway.
bgp_asn	Long	Specifies the BGP AS number of the VPN gateway.

Parameter	Type	Description
flavor	String	- Specifies the specification of the VPN gateway. For the value range, see the Specification parameter on the page for creating a VPN gateway on the VPN console. - Value range: v300: The maximum forwarding bandwidth is 300 Mbit/s. This value has been deprecated, but is retained for compatibility purposes. Using this value is not recommended. v1g: The maximum forwarding bandwidth is 1 Gbit/s. This value has been deprecated, but is retained for compatibility purposes. Using this value is not recommended. Professional1: The maximum forwarding bandwidth is 300 Mbit/s. Professional2: The maximum forwarding bandwidth is 1 Gbit/s.
connection_number	Integer	Specifies the maximum number of VPN connections supported for the VPN gateway.
used_connection_number	Integer	Specifies the number of VPN connections that have been used by the VPN gateway.
used_connection_group	Integer	Specifies the number of VPN connection groups that have been used by the VPN gateway. A connection group consists of two connections between a customer gateway and a VPN gateway. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway.
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID (36 characters) or 0.
access_vpc_id	String	- Specifies the ID of the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.

Parameter	Type	Description
access_subnet_id	String	- Specifies the ID of the subnet in the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.
ha_mode	String	- Specifies the HA mode of the gateway. The value can be active-active or active-standby. - Value range: active-active, active-standby - Default value: active-active
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-8 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

Table 4-9 PolicyTemplate

Parameter	Type	Description
ike_policy	IkePolicy object	Specifies the IKE policy object.
ipsec_policy	IpsecPolicy object	Specifies the IPsec policy object.

Table 4-10 IkePolicy

Parameter	Type	Description
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group14, group15, group16, group19, group20, group21, or disable.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.

Table 4-11 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group14, group15, group16, group19, group20, group21, or disable.
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.

- Example responses

- a. Response to the request for creating a VPN gateway that uses existing EIPs and is associated with a VPC

```
{
  "vpn_gateway": {
    "id": "134f9fb1-demo-a8df-va86-2040a5c13325",
    "name": "vpngw-9f24",
    "network_type": "public",
    "attachment_type": "vpc",
    "ip_version": "ipv4",
    "vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",
    "local_subnets": ["192.168.0.0/24"],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "bgp_asn": 64512,
    "flavor": "Professional1",
    "connection_number": 200,
    "used_connection_number": 0,
    "used_connection_group": 0,
    "enterprise_project_id": "0",
    "access_vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "ha_mode": "active-active"
  },
  "request_id": "7b37532a-d6e4-46b9-98dc-9169ec2ca58f"
}
```

- b. Response to the request for creating a VPN gateway that uses new EIPs and is associated with an enterprise router

```
{
  "vpn_gateway": {
    "id": "80ac167b-demo-a8df-va86-a9a2a23223b8",
    "name": "vpngw-1234",
    "network_type": "public",
    "attachment_type": "er",
    "ip_version": "ipv4",
    "er_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "bgp_asn": 65533,
    "flavor": "Professional2",
    "connection_number": 200,
    "used_connection_number": 0,
    "used_connection_group": 0,
    "enterprise_project_id": "0",
    "access_vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "ha_mode": "active-active"
  },
  "request_id": "cd71cade-bfbd-410b-b672-4bfe46cfc311"
}
```

- c. Response to the request for creating a private VPN gateway associated with a VPC

```
{
  "vpn_gateway": {
    "id": "80ac167b-demo-a8df-va86-a9a2a23223b8",
    "name": "vpngw-1234",
    "network_type": "private",
    "attachment_type": "vpc",
    "ip_version": "ipv4",
    "vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "local_subnets": ["192.168.0.0/24", "192.168.1.0/24"],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "bgp_asn": 65533,
    "flavor": "Professional2",
    "connection_number": 200,
    "used_connection_number": 0,
    "used_connection_group": 0,
    "enterprise_project_id": "0",
    "access_vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "ha_mode": "active-active"
  }
}
```

```
},  
"request_id": "cd71cade-bfbd-410b-b672-4bfe46cfc311"  
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.1.2 Querying a Specified VPN Gateway

Function

This API is used to query a VPN gateway with a specified gateway ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn-gateways/{vgw_id}

Table 4-12 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vgw_id	String	Yes	Specifies a VPN gateway ID.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/vpn-gateways/{vgw_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-13 Parameters in the response body

Parameter	Type	Description
vpn_gateway	ResponseVpnGateway object	Specifies the VPN gateway object.
request_id	String	Specifies a request ID.

Table 4-14 ResponseVpnGateway

Parameter	Type	Description
id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
network_type	String	- Specifies the network type of the VPN gateway. - The value can be public or private. - The default value is public.
status	String	- Specifies the status of the VPN gateway. - Value range: PENDING_CREATE: creating PENDING_UPDATE: updating PENDING_DELETE: deleting ACTIVE: normal FAULT: abnormal FREEZED: frozen
attachment_type	String	- Specifies the association mode. - The value is vpc or er.
ip_version	String	- Specifies the IP protocol version of the VPN gateway. - The value is ipv4.
er_id	String	Specifies the ID of the enterprise router instance to which the VPN gateway connects. This parameter is available only when attachment_type is set to er .

Parameter	Type	Description
er_attachment_id	String	Specifies the ID of the enterprise router attachment associated with the VPN gateway.
vpc_id	String	Specifies the ID of the service VPC associated with the VPN gateway. This parameter is available only when attachment_type is set to vpc .
local_subnets	Array of String	Specifies an IPv4 local subnet. This subnet is a cloud-side subnet that needs to communicate with an on-premises network through a VPN. An example subnet is 192.168.52.0/24. This parameter is returned only when attachment_type is set to vpc and ip_version is set to ipv4 .
connect_subnet	String	Specifies the ID of the VPC subnet used by the VPN gateway.
bgp_asn	Long	Specifies the BGP AS number of the VPN gateway.
flavor	String	- Specifies the specification of the VPN gateway. - Value range: Professional1: The maximum forwarding bandwidth is 300 Mbit/s. Professional2: The maximum forwarding bandwidth is 1 Gbit/s.
availability_zone_ids	Array of String	Specifies the AZ where the VPN gateway is deployed. This parameter is available when an AZ is specified. If no AZ is specified, this parameter is available only when the VPN gateway is in ACTIVE state.
public_border_group	String	Specifies a public border group.
connection_number	Integer	Specifies the maximum number of VPN connections supported for the VPN gateway.
used_connection_number	Integer	Specifies the number of VPN connections that have been used by the VPN gateway.

Parameter	Type	Description
used_connection_group	Integer	Specifies the number of VPN connection groups that have been used by the VPN gateway. A connection group consists of two connections between a customer gateway and a VPN gateway. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway.
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. If no enterprise project ID is specified during VPN gateway creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Note that 0 is not the ID of an existing enterprise project.
eip1	ResponseEip object	Specifies the first EIP of the VPN gateway using the active-active mode or the active EIP of the VPN gateway using the active/standby mode. This parameter is available when the VPN gateway is in ACTIVE state.
eip2	ResponseEip object	Specifies the second EIP of the VPN gateway using the active-active mode or the standby EIP of the VPN gateway using the active/standby mode. This parameter is available when the VPN gateway is in ACTIVE state.
created_at	String	- Specifies the time when the VPN gateway is created. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
applied_at	String	- Specifies the time when the VPN gateway takes effect. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Parameter	Type	Description
updated_at	String	- Specifies the last update time. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
access_vpc_id	String	- Specifies the ID of the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.
access_subnet_id	String	- Specifies the ID of the subnet in the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.
access_private_ip_1	String	Specifies a private IP address used by the VPN gateway to connect to a customer gateway when the network type is private network. This address is the first private IP address of the VPN gateway in active-active mode or the active private IP address of the VPN gateway in the active/standby mode. An example is 192.168.52.9. This parameter is available only when network_type is set to private.
access_private_ip_2	String	Specifies a private IP address used by the VPN gateway to connect to a customer gateway when the network type is private network. This address is the second private IP address of the VPN gateway in active-active mode or the standby private IP address of the VPN gateway in the active/standby mode. An example is 192.168.52.9. This parameter is available only when network_type is set to private.
ha_mode	String	- Specifies the HA mode of the gateway. The value can be active-active or active-standby. - Value range: active-active, active-standby - Default value: active-active
supported_flavors	Array of Strings	Specifies the specification to which the gateway can be upgraded.

Parameter	Type	Description
supported_features	Array of String	Specifies the features supported by the gateway.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-15 ResponseEip

Parameter	Type	Description
id	String	- Specifies an EIP ID. - The value is a UUID containing 36 characters. If the default enterprise project is used, 0 is returned.
ip_version	Integer	- Specifies the EIP version. - The value can only be 4, indicating IPv4 address.
ip_billing_info	String	- Specifies the EIP order information. This parameter is available only for yearly/monthly EIPs. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa
type	String	- Specifies the EIP type. - For the value range, see the type field in Table 7 in Assigning an EIP.
ip_address	String	- Specifies an EIP, that is, a public IPv4 address. - The value is an IPv4 address, for example, 88.***.***.11.
charge_mode	String	- Specifies the billing mode of EIP bandwidth. - Value range: bandwidth: billed by bandwidth traffic: billed by traffic

Parameter	Type	Description
bandwidth_id	String	- Specifies the bandwidth ID of an EIP. - The value is a UUID containing 36 characters.
bandwidth_size	Integer	- Specifies the bandwidth (Mbit/s) of an EIP. The maximum EIP bandwidth varies according to regions and depends on the EIP service. You can submit a service ticket to increase the maximum EIP bandwidth under your account. - The value ranges from 1 to 1000. For details, see the EIP documentation.
bandwidth_name	String	- Specifies the bandwidth name of an EIP. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
bandwidth_billing_info	String	- Specifies the EIP bandwidth order information. This parameter is available only for yearly/monthly EIPs. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa
share_type	String	- Specifies the bandwidth type. - Value range: PER: dedicated bandwidth WHOLE: shared bandwidth

Table 4-16 PolicyTemplate

Parameter	Type	Description
ike_policy	IkePolicy object	Specifies the IKE policy object.
ipsec_policy	IpsecPolicy object	Specifies the IPsec policy object.

Table 4-17 IkePolicy

Parameter	Type	Description
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group14, group15, group16, group19, group20, group21, or disable.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.

Table 4-18 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group14, group15, group16, group19, group20, group21, or disable.
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.

Table 4-19 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example responses
 - a. Example response to the request for querying a public VPN gateway associated with an enterprise router

```
{
  "vpn_gateway": {
    "id": "66ddeacb-demo-a8df-va86-9a414b5bd7d5",
    "name": "vpngw-5bd6",
    "network_type": "public",
    "status": "ACTIVE",
    "attachment_type": "er",
    "ip_version": "ipv4",
    "er_id": "c62fad0d-demo-a8df-va86-e06c4c351b9f",
    "bgp_asn": 64512,
    "flavor": "Professional1",
    "availability_zone_ids": ["cn-south-1f", "cn-south-1e"],
    "connection_number": 200,
    "used_connection_number": 0,
    "used_connection_group": 0,
    "enterprise_project_id": "0",
    "eip1": {
      "id": "0f6d1415-demo-a8df-va86-edb2ee97c9cc",
      "ip_version": 4,
      "type": "5_bgp",
      "ip_address": "88.***.***.251",
      "charge_mode": "bandwidth",
      "bandwidth_id": "e93767cc-demo-a8df-va86-bac2987f90a4",
      "bandwidth_size": 300,
      "bandwidth_name": "vpngw-bandwidth-10c3"
    },
    "eip2": {
      "id": "7b46b62f-demo-a8df-va86-6b8e44312416",
      "ip_version": 4,
      "type": "5_bgp",
      "ip_address": "88.***.***.102",
      "charge_mode": "bandwidth",
      "bandwidth_id": "bde3557e-demo-a8df-va86-629a3754ae07",
      "bandwidth_size": 300,
      "bandwidth_name": "vpngw-bandwidth-18bd"
    },
    "created_at": "2022-11-28T02:22:27.24Z",
    "updated_at": "2022-11-28T02:22:27.24Z",
    "access_vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "ha_mode": "active-active"
  }
}
```

```
    },  
    "request_id": "28b795f8-d431-4f1e-93ab-1c401a82b799"  
  }  
}
```

- b. Example response to the request for querying a private VPN gateway associated with a VPC

```
{  
  "vpn_gateway": {  
    "id": "66ddeacb-demo-a8df-va86-9a414b5bd7d5",  
    "name": "vpngw-5bd6",  
    "network_type": "private",  
    "status": "ACTIVE",  
    "attachment_type": "vpc",  
    "ip_version": "ipv4",  
    "vpc_id": "91a74241-demo-a8df-va86-9b5f98c66c8c",  
    "local_subnets": ["192.168.0.0/24"],  
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",  
    "bgp_asn": 64512,  
    "flavor": "Professional1",  
    "availability_zone_ids": ["cn-south-1f", "cn-south-1e"],  
    "connection_number": 200,  
    "used_connection_number": 0,  
    "used_connection_group": 0,  
    "enterprise_project_id": "0",  
    "created_at": "2022-11-28T02:22:27.24Z",  
    "updated_at": "2022-11-28T02:22:27.24Z",  
    "access_vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",  
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",  
    "access_private_ip_1": "192.168.146.45",  
    "access_private_ip_2": "192.168.146.77",  
    "ha_mode": "active-active"  
  },  
  "request_id": "28b795f8-d431-4f1e-93ab-1c401a82b799"  
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.1.3 Querying the VPN Gateway List

Function

This API is used to query the VPN gateway list.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn-gateways

Table 4-20 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Table 4-21 Parameter in a query request

Parameter	Type	Mandatory	Description
enterprise_project_id	Array	No	Specifies an enterprise project ID.

Request

- Request parameters
None
- Example requests
 - a. Query all VPN gateways.
GET https://{Endpoint}/v5/{project_id}/vpn-gateways
 - b. Query VPN gateways based on a specified enterprise project ID.
GET https://{Endpoint}/v5/{project_id}/vpn-gateways?
enterprise_project_id={enterprise_project_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-22 Parameters in the response body

Parameter	Type	Description
vpn_gateways	Array of ResponseVpnGateway objects	Specifies gateway information.
request_id	String	Specifies a request ID.

Table 4-23 ResponseVpnGateway

Parameter	Type	Description
id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
network_type	String	- Specifies the network type of the VPN gateway. - The value can be public or private. - The default value is public.
status	String	- Specifies the status of the VPN gateway. - Value range: PENDING_CREATE: creating PENDING_UPDATE: updating PENDING_DELETE: deleting ACTIVE: normal FAULT: abnormal FREEZED: frozen
attachment_type	String	- Specifies the association mode. - The value is vpc or er.
ip_version	String	- Specifies the IP protocol version of the VPN gateway. - The value is ipv4.
er_id	String	Specifies the ID of the enterprise router instance to which the VPN gateway connects. This parameter is available only when attachment_type is set to er .
er_attachment_id	String	Specifies the ID of the enterprise router attachment associated with the VPN gateway.
vpc_id	String	Specifies the ID of the service VPC associated with the VPN gateway. This parameter is returned only when attachment_type is set to vpc .

Parameter	Type	Description
local_subnets	Array of String	Specifies an IPv4 local subnet. This subnet is a cloud-side subnet that needs to communicate with an on-premises network through a VPN. An example subnet is 192.168.52.0/24. This parameter is returned only when attachment_type is set to vpc and ip_version is set to ipv4 .
connect_subnet	String	Specifies the ID of the VPC subnet used by the VPN gateway.
bgp_asn	Long	Specifies the BGP AS number of the VPN gateway.
flavor	String	- Specifies the specifications of the VPN gateway. - Value range: Professional1: The maximum forwarding bandwidth is 300 Mbit/s. Professional2: The maximum forwarding bandwidth is 1 Gbit/s.
availability_zone_ids	Array of String	Specifies the AZ where the VPN gateway is deployed. This parameter is available when an AZ is specified. If no AZ is specified, this parameter is available only when the VPN gateway is in ACTIVE state.
public_border_group	String	Specifies a public border group.
connection_number	Integer	Specifies the maximum number of VPN connections supported for the VPN gateway.
used_connection_number	Integer	Specifies the number of VPN connections that have been used by the VPN gateway.
used_connection_group	Integer	Specifies the number of VPN connection groups that have been used by the VPN gateway. A connection group consists of two connections between a customer gateway and a VPN gateway. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway.

Parameter	Type	Description
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. If no enterprise project ID is specified during VPN gateway creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Note that 0 is not the ID of an existing enterprise project.
eip1	ResponseEip object	Specifies the first EIP used by the VPN gateway. This parameter is available when the VPN gateway is in ACTIVE state.
eip2	ResponseEip object	Specifies the second EIP used by the VPN gateway. This parameter is available when the VPN gateway is in ACTIVE state.
created_at	String	- Specifies the time when the VPN gateway is created. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
applied_at	String	- Specifies the time when the VPN gateway takes effect. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
access_vpc_id	String	- Specifies the ID of the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.
access_subnet_id	String	- Specifies the ID of the subnet in the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.

Parameter	Type	Description
access_private_ip_1	String	Specifies a private IP address used by the VPN gateway to connect to a customer gateway when the network type is private network. This address is the first private IP address of the VPN gateway in active-active mode or the active private IP address of the VPN gateway in the active/standby mode. An example is 192.168.52.9. This parameter is available only when network_type is set to private.
access_private_ip_2	String	Specifies a private IP address used by the VPN gateway to connect to a customer gateway when the network type is private network. This address is the second private IP address of the VPN gateway in active-active mode or the standby private IP address of the VPN gateway in the active/standby mode. An example is 192.168.52.9. This parameter is available only when network_type is set to private.
ha_mode	String	- Specifies the HA mode of the gateway. The value can be active-active or active-standby. - Value range: active-active, active-standby - Default value: active-active
supported_flavors	Array of Strings	Specifies the specification to which the gateway can be upgraded.
supported_features	Array of Strings	Specifies the features supported by the gateway.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-24 ResponseEip

Parameter	Type	Description
id	String	- Specifies an EIP ID. - The value is a UUID containing 36 characters. If the default enterprise project is used, 0 is returned.

Parameter	Type	Description
ip_version	Integer	- Specifies the EIP version. - The value can only be 4, indicating IPv4 address.
ip_billing_info	String	- Specifies the EIP order information. This parameter is available only for yearly/monthly EIPs. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484a
type	String	- Specifies the EIP type. - For the value range, see the type field in Table 7 in Assigning an EIP.
ip_address	String	- Specifies an EIP, that is, a public IPv4 address. - The value is an IPv4 address, for example, 88.***.***.11.
charge_mode	String	- Specifies the billing mode of EIP bandwidth. - Value range: bandwidth: billed by bandwidth traffic: billed by traffic
bandwidth_id	String	- Specifies the bandwidth ID of an EIP. - The value is a UUID containing 36 characters.
bandwidth_size	Integer	- Specifies the bandwidth (Mbit/s) of an EIP. The maximum EIP bandwidth varies according to regions and depends on the EIP service. You can submit a service ticket to increase the maximum EIP bandwidth under your account. - The value ranges from 1 to 1000. For details, see the EIP documentation.
bandwidth_name	String	- Specifies the bandwidth name of an EIP. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
bandwidth_billing_info	String	- Specifies the EIP bandwidth order information. This parameter is available only for yearly/monthly EIPs. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa
share_type	String	- Specifies the bandwidth type. - Value range: PER: dedicated bandwidth WHOLE: shared bandwidth

Table 4-25 PolicyTemplate

Parameter	Type	Description
ike_policy	IkePolicy object	Specifies the IKE policy object.
ipsec_policy	IpsecPolicy object	Specifies the IPsec policy object.

Table 4-26 IkePolicy

Parameter	Type	Description
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group14, group15, group16, group19, group20, group21, or disable.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.

Parameter	Type	Description
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.

Table 4-27 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group14, group15, group16, group19, group20, group21, or disable.
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.

Table 4-28 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (<code>_ . : = + - @</code>).

Parameter	Type	Description
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example responses

- a. Response to the request for querying all VPN gateways

```
{
  "vpn_gateways": [
    {
      "id": "8e1d0686-demo-a8df-va86-91f32fa1dfc8",
      "name": "vpngw-1af3",
      "network_type": "public",
      "status": "ACTIVE",
      "attachment_type": "vpc",
      "ip_version": "ipv4",
      "vpc_id": "91a74241-demo-a8df-va86-9b5f98c66c8c",
      "local_subnets": ["192.168.15.0/24"],
      "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
      "bgp_asn": 64512,
      "flavor": "Professional1",
      "availability_zone_ids": ["cn-south-1f", "cn-south-1e"],
      "connection_number": 200,
      "used_connection_number": 0,
      "used_connection_group": 0,
      "enterprise_project_id": "0",
      "eip1": {
        "id": "8ff5d6b5-demo-a8df-va86-b9d598033153",
        "ip_version": 4,
        "type": "5_bgp",
        "ip_address": "88.***.***.111",
        "charge_mode": "bandwidth",
        "bandwidth_id": "aa62f8f2-demo-a8df-va86-b05b2b999715",
        "bandwidth_size": 300,
        "bandwidth_name": "vpngw-bandwidth-13a3"
      },
      "eip2": {
        "id": "08e7e927-demo-a8df-va86-26a6394021eb",
        "ip_version": 4,
        "type": "5_bgp",
        "ip_address": "88.***.***.199",
        "charge_mode": "bandwidth",
        "bandwidth_id": "887d61f7-demo-a8df-va86-38ee8232e27c",
        "bandwidth_size": 300,
        "bandwidth_name": "vpngw-bandwidth-1afb"
      },
      "created_at": "2022-11-28T02:36:16.834Z",
      "updated_at": "2022-11-28T02:36:16.834Z",
      "access_vpc_id": "91a74241-demo-a8df-va86-9b5f98c66c8c",
      "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
      "ha_mode": "active-active"
    },
    {
      "id": "66ddeacb-demo-a8df-va86-9a414b5bd7d5",
      "name": "vpngw-2be4",
      "network_type": "public",
      "status": "ACTIVE",
      "attachment_type": "er",
      "ip_version": "ipv4",
      "er_id": "c62fad0d-demo-a8df-va86-e06c4c351b9f",
      "bgp_asn": 64512,
      "flavor": "Professional1",
    }
  ]
}
```

```
"availability_zone_ids": ["cn-south-1f", "cn-south-1e"],
"connection_number": 200,
"used_connection_number": 0,
"used_connection_group": 0,
"enterprise_project_id": "0",
"eip1": {
  "id": "0f6d1415-demo-a8df-va86-edb2ee97c9cc",
  "ip_version": 4,
  "type": "5_bgp",
  "ip_address": "88.***.***.251",
  "charge_mode": "bandwidth",
  "bandwidth_id": "e93767cc-demo-a8df-va86-bac2987f90a4",
  "bandwidth_size": 300,
  "bandwidth_name": "vpngw-bandwidth-10c3"
},
"eip2": {
  "id": "7b46b62f-demo-a8df-va86-6b8e44312416",
  "ip_version": 4,
  "type": "5_bgp",
  "ip_address": "88.***.***.102",
  "charge_mode": "bandwidth",
  "bandwidth_id": "bde3557e-demo-a8df-va86-629a3754ae07",
  "bandwidth_size": 300,
  "bandwidth_name": "vpngw-bandwidth-18bd",
},
"created_at": "2022-11-28T02:22:27.24Z",
"updated_at": "2022-11-28T02:22:27.24Z",
"access_vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",
"access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
"ha_mode": "active-active"
},{
  "id": "66ddeacb-demo-a8df-va86-9a414b5bd7d5",
  "name": "vpngw-5bd6",
  "network_type": "public",
  "status": "ACTIVE",
  "attachment_type": "vpc",
  "ip_version": "ipv4",
  "vpc_id": "c62fad0d-demo-a8df-va86-e06c4c351b9f",
  "local_subnets": [
    "192.168.0.0/24"
  ],
  "connect_subnet": "fd75bf7b--demo-a8df-va86-db13f03e299a",
  "bgp_asn": 64512,
  "availability_zone_ids": [
    "cn-north-7c"
  ],
  "connection_number": 200,
  "used_connection_number": 0,
  "used_connection_group": 0,
  "enterprise_project_id": "0",
  "ha_mode": "active-standby",
  "eip1": {
    "id": "0f6d1415-demo-a8df-va86-edb2ee97c9cc",
    "ip_version": 4,
    "type": "5_bgp",
    "ip_address": "88.***.***.251",
    "charge_mode": "bandwidth",
    "bandwidth_id": "e93767cc-demo-a8df-va86-bac2987f90a4",
    "bandwidth_size": 300,
    "bandwidth_name": "vpngw-bandwidth-10c3"
  },
  "eip2": {
    "id": "7b46b62f-demo-a8df-va86-6b8e44312416",
    "ip_version": 4,
    "type": "5_bgp",
    "ip_address": "88.***.***.102",
    "charge_mode": "bandwidth",
    "bandwidth_id": "bde3557e-demo-a8df-va86-629a3754ae07",
    "bandwidth_size": 300,
```

```
    "bandwidth_name": "vpngw-bandwidth-18bd"
  },
  "policy_template": {
    "ike_policy": {
      "encryption_algorithm": "aes-128",
      "dh_group": "group20",
      "authentication_algorithm": "sha2-256",
      "lifetime_seconds": 86400
    },
    "ipsec_policy": {
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "pfs": "group20",
      "lifetime_seconds": 3600
    }
  },
  "created_at": "2022-11-28T02:22:27.24Z",
  "updated_at": "2022-11-28T02:22:27.24Z",
  "access_vpc_id": "4d03fe2d--demo-a8df-va86-6def96440f2b",
  "access_subnet_id": "fd75bf7b--demo-a8df-va86-e-db13f03e299a"
}],
"request_id": "de1b6caf-d024-4dac-850e-645af40c84f3"
}
```

- b. Response to the request for querying VPN gateways based on a specified enterprise project ID

```
{
  "vpn_gateways": [ {
    "id": "8e1d0686-demo-a8df-va86-91f32fa1dfc8",
    "name": "vpngw-1af3",
    "network_type": "public",
    "status": "ACTIVE",
    "attachment_type": "vpc",
    "ip_version": "ipv4",
    "vpc_id": "91a74241-demo-a8df-va86-9b5f98c66c8c",
    "local_subnets": ["192.168.15.0/24"],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "bgp_asn": 64512,
    "flavor": "Professional1",
    "availability_zone_ids": ["cn-south-1f", "cn-south-1e"],
    "connection_number": 200,
    "used_connection_number": 0,
    "used_connection_group": 0,
    "enterprise_project_id": "7354dda9-demo-a8df-va86-a6b08fb92043",
    "eip1": {
      "id": "8ff5d6b5-demo-a8df-va86-b9d598033153",
      "ip_version": 4,
      "type": "5_bgp",
      "ip_address": "88.***.***.111",
      "charge_mode": "bandwidth",
      "bandwidth_id": "aa62f8f2-demo-a8df-va86-b05b2b999715",
      "bandwidth_size": 300,
      "bandwidth_name": "vpngw-bandwidth-13a3"
    },
    "eip2": {
      "id": "08e7e927-demo-a8df-va86-26a6394021eb",
      "ip_version": 4,
      "type": "5_bgp",
      "ip_address": "88.***.***.199",
      "charge_mode": "bandwidth",
      "bandwidth_id": "887d61f7-demo-a8df-va86-38ee8232e27c",
      "bandwidth_size": 300,
      "bandwidth_name": "vpngw-bandwidth-1afb"
    },
    "created_at": "2022-11-28T02:36:16.834Z",
    "updated_at": "2022-11-28T02:36:16.834Z",
    "access_vpc_id": "91a74241-demo-a8df-va86-9b5f98c66c8c",
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "ha_mode": "active-active"
  } ], {
  }
```

```
"id": "66ddeacb-demo-a8df-va86-9a414b5bd7d5",
"name": "vpngw-2be4",
"network_type": "private",
"status": "ACTIVE",
"attachment_type": "er",
"ip_version": "ipv4",
"er_id": "c62fad0d-demo-a8df-va86-e06c4c351b9f",
"bgp_asn": 64512,
"flavor": "Professional1",
"availability_zone_ids": ["cn-south-1f", "cn-south-1e"],
"connection_number": 200,
"used_connection_number": 0,
"used_connection_group": 0,
"enterprise_project_id": "7354dda9-demo-a8df-va86-a6b08fb92043",
"access_private_ip_1": "192.168.4.7",
"access_private_ip_2": "192.168.4.99",
"created_at": "2022-11-28T02:22:27.24Z",
"updated_at": "2022-11-28T02:22:27.24Z",
"access_vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",
"access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
"ha_mode": "active-active"
},{
  "id": "66ddeacb-demo-a8df-va86-9a414b5bd7d5",
  "name": "vpngw-5bd6",
  "network_type": "public",
  "status": "ACTIVE",
  "attachment_type": "vpc",
  "ip_version": "ipv4",
  "vpc_id": "c62fad0d-demo-a8df-va86-e06c4c351b9f",
  "local_subnets": [
    "192.168.0.0/24"
  ],
  "connect_subnet": "fd75bf7b--demo-a8df-va86-db13f03e299a",
  "bgp_asn": 64512,
  "availability_zone_ids": [
    "cn-north-7c"
  ],
  "connection_number": 200,
  "used_connection_number": 0,
  "used_connection_group": 0,
  "enterprise_project_id": "0",
  "ha_mode": "active-standby",
  "eip1": {
    "id": "0f6d1415-demo-a8df-va86-edb2ee97c9cc",
    "ip_version": 4,
    "type": "5_bgp",
    "ip_address": "88.***.***.251",
    "charge_mode": "bandwidth",
    "bandwidth_id": "e93767cc-demo-a8df-va86-bac2987f90a4",
    "bandwidth_size": 300,
    "bandwidth_name": "vpngw-bandwidth-10c3"
  },
  "eip2": {
    "id": "7b46b62f-demo-a8df-va86-6b8e44312416",
    "ip_version": 4,
    "type": "5_bgp",
    "ip_address": "88.***.***.102",
    "charge_mode": "bandwidth",
    "bandwidth_id": "bde3557e-demo-a8df-va86-629a3754ae07",
    "bandwidth_size": 300,
    "bandwidth_name": "vpngw-bandwidth-18bd"
  },
  "policy_template": {
    "ike_policy": {
      "encryption_algorithm": "aes-128",
      "dh_group": "group20",
      "authentication_algorithm": "sha2-256",
      "lifetime_seconds": 86400
    }
  },
}
```

```
    "ipsec_policy":{
      "authentication_algorithm":"sha2-256",
      "encryption_algorithm":"aes-128",
      "pfs":"group20",
      "lifetime_seconds":3600
    },
    "created_at":"2022-11-28T02:22:27.24Z",
    "updated_at":"2022-11-28T02:22:27.24Z",
    "access_vpc_id":"4d03fe2d--demo-a8df-va86-6def96440f2b",
    "access_subnet_id":"fd75bf7b--demo-a8df-va86-e-db13f03e299a"
  },
  "request_id": "bfa819a1-e824-4799-8e72-21a35dad97c9"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.1.4 Updating a VPN Gateway

Function

This API is used to update a VPN gateway with a specified gateway ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/vpn-gateways/{vgw_id}

Table 4-29 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vgw_id	String	Yes	Specifies the ID of a VPN gateway instance.

Request

- Request parameters

Table 4-30 Request parameters

Parameter	Type	Mandatory	Description
vpn_gateway	UpdateVgwRequestBodyContent object	Yes	Specifies the VPN gateway object.

Table 4-31 UpdateVgwRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies the name of a VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
local_subnets	Array of String	No	- Specifies an IPv4 local subnet. This subnet is a cloud-side subnet that needs to communicate with an on-premises network through a VPN. An example subnet is 192.168.52.0/24. - This parameter can be set only when attachment_type is set to vpc and ip_version is set to ipv4. A maximum of 50 local subnets can be configured for each VPN gateway.
eip_id_1	String	No	- Specifies the ID of the new EIP, which is used as the first EIP of the VPN gateway in active-active mode or the active EIP of the VPN gateway in active/standby mode. Before binding a new EIP, unbind the original EIP from the VPN gateway by referring to Updating an EIP. - The value is a UUID containing 36 characters. You can set this parameter only when network_type is set to public.

Parameter	Type	Mandatory	Description
eip_id_2	String	No	- Specifies the ID of the new EIP, which is used as the second EIP of the VPN gateway in active-active mode or the standby EIP of the VPN gateway in active/standby mode. Before binding a new EIP, unbind the original EIP from the VPN gateway by referring to Updating an EIP. - The value is a UUID containing 36 characters. You can set this parameter only when network_type is set to public.

Table 4-32 PolicyTemplate

Parameter	Type	Description
ike_policy	IkePolicy object	Specifies the IKE policy object.
ipsec_policy	IpsecPolicy object	Specifies the IPsec policy object.

Table 4-33 IkePolicy

Parameter	Type	Description
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group14, group15, group16, group19, group20, group21, or disable.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.

Parameter	Type	Description
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.

Table 4-34 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group14, group15, group16, group19, group20, group21, or disable.
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.

- Example requests
 - a. Updating a VPN gateway that does not support access via non-fixed IP addresses

```
PUT https://{Endpoint}/v5/{project_id}/vpn-gateways/{vgw_id}

{
  "vpn_gateway": {
    "name": "vpngw-4321",
    "local_subnets": [
      "192.168.0.0/24"
    ],
    "eip_id_1": "f1469b4a-demo-a8df-va86-bb7de91cf493",
    "eip_id_2": "6ad8e297-demo-a8df-va86-da0f885ccb98"
  }
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-35 Parameters in the response body

Parameter	Type	Description
vpn_gateway	ResponseVpnGateway object	Specifies the VPN gateway object.
request_id	String	Specifies a request ID.

Table 4-36 ResponseVpnGateway

Parameter	Type	Description
id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
network_type	String	- Specifies the network type of the VPN gateway. - The value can be public or private. - The default value is public.
attachment_type	String	- Specifies the association mode. - The value is vpc or er.
ip_version	String	- Specifies the IP protocol version of the VPN gateway. - The value is ipv4.
er_id	String	Specifies the ID of the enterprise router instance to which the VPN gateway connects. This parameter is available only when attachment_type is set to er .
vpc_id	String	- When attachment_type is set to vpc, vpc_id specifies the ID of the service VPC associated with the VPN gateway. - When attachment_type is set to er, vpc_id specifies the ID of the access VPC used by the VPN gateway.

Parameter	Type	Description
local_subnets	Array of String	Specifies a local subnet. This subnet is a cloud-side subnet that needs to communicate with an on-premises network through a VPN. An example subnet is 192.168.52.0/24. This parameter is returned only when attachment_type is set to vpc and ip_version is set to ipv4 .
connect_subnet	String	Specifies the ID of the VPC subnet used by the VPN gateway.
bgp_asn	Long	Specifies the BGP AS number of the VPN gateway.
flavor	String	- Specifies the specification of the VPN gateway. - Value range: Professional1: The maximum forwarding bandwidth is 300 Mbit/s. Professional2: The maximum forwarding bandwidth is 1 Gbit/s.
availability_zone_ids	Array of String	Specifies the AZ where the VPN gateway is deployed. This parameter is available when an AZ is specified. If no AZ is specified, this parameter is available only when the VPN gateway is in ACTIVE state.
connection_number	Integer	Specifies the maximum number of VPN connections supported for the VPN gateway.
used_connection_number	Integer	Specifies the number of VPN connections that have been used by the VPN gateway.
used_connection_group	Integer	Specifies the number of VPN connection groups that have been used by the VPN gateway. A connection group consists of two connections between a customer gateway and a VPN gateway. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway.

Parameter	Type	Description
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. If no enterprise project ID is specified during VPN gateway creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Note that 0 is not the ID of an existing enterprise project.
eip1	ResponseEip object	Specifies the first EIP of the VPN gateway in the active-active mode or the active EIP of the VPN gateway in the active/standby mode. This parameter is available when the VPN gateway is in ACTIVE state.
eip2	ResponseEip object	Specifies the second EIP of the VPN gateway in the active-active mode or the standby EIP of the VPN gateway in the active/standby mode. This parameter is available when the VPN gateway is in ACTIVE state.
created_at	String	- Specifies the time when the VPN gateway is created. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
access_vpc_id	String	- Specifies the ID of the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.
access_subnet_id	String	- Specifies the ID of the subnet in the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.

Parameter	Type	Description
access_private_ip_1	String	Specifies a private IP address used by the VPN gateway to connect to a customer gateway when the network type is private network. This address is the first private IP address of the VPN gateway in active-active mode or the active private IP address of the VPN gateway in the active/standby mode. An example is 192.168.52.9. This parameter is available only when network_type is set to private.
access_private_ip_2	String	Specifies a private IP address used by the VPN gateway to connect to a customer gateway when the network type is private network. This address is the second private IP address of the VPN gateway in active-active mode or the standby private IP address of the VPN gateway in the active/standby mode. An example is 192.168.52.9. This parameter is available only when network_type is set to private.
ha_mode	String	- Specifies the HA mode of the gateway. The value can be active-active or active-standby. - Value range: active-active, active-standby
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-37 ResponseEip

Parameter	Type	Description
id	String	- Specifies an EIP ID. - The value is a UUID containing 36 characters. If the default enterprise project is used, 0 is returned.
ip_version	Integer	- Specifies the EIP version. - The value can only be 4, indicating IPv4 address.

Parameter	Type	Description
ip_billing_info	String	- Specifies the EIP order information. This parameter is available only for yearly/monthly EIPs. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484a
type	String	- Specifies the EIP type. - For the value range, see the type field in Table 7 in Assigning an EIP.
ip_address	String	- Specifies an EIP, that is, a public IPv4 address. - The value is an IPv4 address, for example, 88.***.***.11.
charge_mode	String	- Specifies the billing mode of EIP bandwidth. - Value range: bandwidth: billed by bandwidth traffic: billed by traffic
bandwidth_id	String	- Specifies the bandwidth ID of an EIP. - The value is a UUID containing 36 characters.
bandwidth_size	Integer	- Specifies the bandwidth (Mbit/s) of an EIP. The maximum EIP bandwidth varies according to regions and depends on the EIP service. You can submit a service ticket to increase the maximum EIP bandwidth under your account. - The value ranges from 1 to 1000. For details, see the EIP documentation.
bandwidth_name	String	- Specifies the bandwidth name of an EIP. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.)

Parameter	Type	Description
bandwidth_billing_info	String	- Specifies the EIP bandwidth order information. This parameter is available only for yearly/monthly EIPs. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa
share_type	String	- Specifies the bandwidth type. - Value range: PER: dedicated bandwidth WHOLE: shared bandwidth

Table 4-38 PolicyTemplate

Parameter	Type	Description
ike_policy	IkePolicy object	Specifies the IKE policy object.
ipsec_policy	IpsecPolicy object	Specifies the IPsec policy object.

Table 4-39 IkePolicy

Parameter	Type	Description
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group14, group15, group16, group19, group20, group21, or disable.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.

Parameter	Type	Description
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.

Table 4-40 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group14, group15, group16, group19, group20, group21, or disable.
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.

Table 4-41 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (<code>_ . : = + - @</code>).

Parameter	Type	Description
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example responses

- a. Response to the request for updating a VPN gateway that does not support access via non-fixed IP addresses

```
{
  "vpn_gateway": {
    "id": "620d99b8-demo-a8df-va86-200b868f2d7d",
    "name": "vpngw-4321",
    "attachment_type": "vpc",
    "network_type": "public",
    "ip_version": "ipv4",
    "vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "local_subnets": [
      "192.168.0.0/24"
    ],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "bgp_asn": 64512,
    "flavor": "Professional1",
    "availability_zone_ids": ["cn-south-1f", "cn-south-1e"],
    "connection_number": 200,
    "used_connection_number": 0,
    "used_connection_group": 0,
    "enterprise_project_id": "0",
    "eip1": {
      "id": "f1469b4a-demo-a8df-va86-bb7de91cf493",
      "ip_version": 4,
      "type": "5_bgp",
      "ip_address": "88.***.***.102",
      "charge_mode": "bandwidth",
      "bandwidth_id": "cff40e5e-demo-a8df-va86-7366077bf097",
      "bandwidth_size": 300,
      "bandwidth_name": "vpngw-bandwidth-1391"
    },
    "eip2": {
      "id": "6ad8e297-demo-a8df-va86-da0f885ccb98",
      "ip_version": 4,
      "type": "5_bgp",
      "ip_address": "88.***.***.188",
      "charge_mode": "bandwidth",
      "bandwidth_id": "d290f1ee-demo-a8df-va86-d701748f0851",
      "bandwidth_size": 300,
      "bandwidth_name": "vpngw-bandwidth-1392"
    },
    "created_at": "2022-09-15T08:56:09.386Z",
    "updated_at": "2022-09-15T11:13:13.677Z",
    "access_vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "ha_mode": "active-active"
  },
  "request_id": "33a2b77a-65f9-4fa0-90bd-4bd42038eb41"
}
```

- b. Response returned when a VPN gateway being created fails to be updated

```
{
  "error_code": "VPN.0003",
}
```

```
"error_msg": "resource (type=GATEWAY, ID=ff9bdca6-demo-a8df-va86-e4bcc1ea52bc) is not ready, currently CREATING",  
"request_id": "abafe41c-7744-41af-bf3d-4452872af799"  
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.1.5 Changing the Specification of a Gateway

Function

This API is used to change the specification of a gateway. Currently, only pay-per-use gateways are supported.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/vpn-gateways/{vgw_id}/update-specification

Table 4-42 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vgw_id	String	Yes	Specifies the ID of a VPN gateway instance.

Request

- Request parameters

Table 4-43 Request parameters

Parameter	Type	Mandatory	Description
vpn_gateway	UpdateVgwSpecificationRequestBodyContent object	Yes	Specifies the VPN gateway object.

Table 4-44 UpdateVgwSpecificationRequestBodyContent

Parameter	Type	Mandatory	Description
flavor	String	Yes	- Specifies the new specification of the VPN gateway. - The value can be one of the following: Professional1, Professional2. For details about the value range supported by each gateway, see the supported_flavors field in the response to the request for 4.1.1.2 Querying a Specified VPN Gateway.

- Example request

POST https://{Endpoint}/v5/{project_id}/vpn-gateways/{vgw_id}/update-specification

```
{
  "vpn_gateway": {
  }
}
```

Response

- Response parameters

Returned status code 200: successful operation

Table 4-45 Parameters in the response body

Parameter	Type	Description
vpn_gateway	ResponseVpn Gateway object	Specifies the VPN gateway object.
request_id	String	Specifies a request ID.

Table 4-46 ResponseVpnGateway

Parameter	Type	Description
id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.

Parameter	Type	Description
name	String	- Specifies the name of a VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
network_type	String	- Specifies the network type of the VPN gateway. - The value can be public or private. - The default value is public.
attachment_type	String	- Specifies the association mode. - The value is vpc or er.
ip_version	String	- Specifies the IP protocol version of the VPN gateway. - The value is ipv4.
er_id	String	Specifies the ID of the enterprise router instance to which the VPN gateway connects. This parameter is available only when attachment_type is set to er .
vpc_id	String	- When attachment_type is set to vpc, vpc_id specifies the ID of the service VPC associated with the VPN gateway. - When attachment_type is set to er, vpc_id specifies the ID of the access VPC used by the VPN gateway.
local_subnets	Array of String	Specifies a local subnet. This subnet is a cloud-side subnet that needs to communicate with an on-premises network through a VPN. An example subnet is 192.168.52.0/24. This parameter is returned only when attachment_type is set to vpc .
connect_subnet	String	Specifies the ID of the VPC subnet used by the VPN gateway.
bgp_asn	Long	Specifies the BGP AS number of the VPN gateway.

Parameter	Type	Description
flavor	String	- Specifies the specification of the VPN gateway. - Value range: Professional1: The maximum forwarding bandwidth is 300 Mbit/s. Professional2: The maximum forwarding bandwidth is 1 Gbit/s.
availability_zone_ids	Array of String	Specifies the AZ where the VPN gateway is deployed. This parameter is available when an AZ is specified. If no AZ is specified, this parameter is available only when the VPN gateway is in ACTIVE state.
connection_number	Integer	Specifies the maximum number of VPN connections supported for the VPN gateway.
used_connection_number	Integer	Specifies the number of VPN connections that have been used by the VPN gateway.
used_connection_group	Integer	Specifies the number of VPN connection groups that have been used by the VPN gateway. A connection group consists of two connections between a customer gateway and a VPN gateway. By default, 10 VPN connection groups are included free of charge with the purchase of a VPN gateway.
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. If no enterprise project ID is specified during VPN gateway creation, 0 is returned, indicating that the resource belongs to the default enterprise project. Note that 0 is not the ID of an existing enterprise project.
eip1	ResponseEip object	Specifies the first EIP of the VPN gateway in the active-active mode or the active EIP of the VPN gateway in the active/standby mode. This parameter is available when the VPN gateway is in ACTIVE state.

Parameter	Type	Description
eip2	ResponseEip object	Specifies the second EIP of the VPN gateway in the active-active mode or the standby EIP of the VPN gateway in the active/standby mode. This parameter is available when the VPN gateway is in ACTIVE state.
created_at	String	- Specifies the time when the VPN gateway is created. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. This parameter is available when the VPN gateway is in ACTIVE state. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
access_vpc_id	String	- Specifies the ID of the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.
access_subnet_id	String	- Specifies the ID of the subnet in the access VPC used by the VPN gateway. - The value is a UUID containing 36 characters.
access_private_ip_1	String	Specifies a private IP address used by the VPN gateway to connect to a customer gateway when the network type is private network. This address is the first private IP address of the VPN gateway in active-active mode or the active private IP address of the VPN gateway in the active/standby mode. An example is 192.168.52.9. This parameter is available only when network_type is set to private.

Parameter	Type	Description
access_private_ip_2	String	Specifies a private IP address used by the VPN gateway to connect to a customer gateway when the network type is private network. This address is the second private IP address of the VPN gateway in active-active mode or the standby private IP address of the VPN gateway in the active/standby mode. An example is 192.168.52.9. This parameter is available only when network_type is set to private .
ha_mode	String	- Specifies the HA mode of the gateway. The value can be active-active or active-standby. - Value range: active-active, active-standby
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-47 ResponseEip

Parameter	Type	Description
id	String	- Specifies an EIP ID. - The value is a UUID containing 36 characters. If the default enterprise project is used, 0 is returned.
ip_version	Integer	- Specifies the EIP version. - The value can only be 4, indicating IPv4 address.
ip_billing_info	String	- Specifies the EIP order information. This parameter is available only for yearly/monthly EIPs. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa

Parameter	Type	Description
type	String	- Specifies the EIP type. - For the value range, see the type field in Table 7 in Assigning an EIP.
ip_address	String	- Specifies an EIP, that is, a public IPv4 address. - The value is an IPv4 address, for example, 88.***.***.11.
charge_mode	String	- Specifies the billing mode of EIP bandwidth. - Value range: bandwidth: billed by bandwidth traffic: billed by traffic
bandwidth_id	String	- Specifies the bandwidth ID of an EIP. - The value is a UUID containing 36 characters.
bandwidth_size	Integer	- Specifies the bandwidth (Mbit/s) of an EIP. The maximum EIP bandwidth varies according to regions and depends on the EIP service. You can submit a service ticket to increase the maximum EIP bandwidth under your account. - The value ranges from 1 to 1000. For details, see the EIP documentation.
bandwidth_name	String	- Specifies the bandwidth name of an EIP. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
bandwidth_billing_info	String	- Specifies the EIP bandwidth order information. This parameter is available only for yearly/monthly EIPs. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484a

Parameter	Type	Description
share_type	String	- Specifies the bandwidth type. - Value range: PER: dedicated bandwidth WHOLE: shared bandwidth

Table 4-48 PolicyTemplate

Parameter	Type	Description
ike_policy	IkePolicy object	Specifies the IKE policy object.
ipsec_policy	IpsecPolicy object	Specifies the IPsec policy object.

Table 4-49 IkePolicy

Parameter	Type	Description
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group14, group15, group16, group19, group20, group21, or disable.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.

Table 4-50 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, or sha2-256.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, or aes-128.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group14, group15, group16, group19, group20, group21, or disable.
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.

Table 4-51 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example response
 - a. Response to the request for updating a VPN gateway that does not support access via non-fixed IP addresses

```
{
  "vpn_gateway": {
    "id": "620d99b8-demo-a8df-va86-200b868f2d7d",
    "name": "vpngw-4321",
    "attachment_type": "vpc",
    "network_type": "public",
    "ip_version": "ipv4",
```

```
"vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
"local_subnets": [
  "192.168.0.0/24"
],
"connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
"bgp_asn": 64512,
"flavor": "Professional1",
"availability_zone_ids": ["cn-south-1f", "cn-south-1e"],
"connection_number": 200,
"used_connection_number": 0,
"used_connection_group": 0,
"enterprise_project_id": "0",
"eip1": {
  "id": "f1469b4a-demo-a8df-va86-bb7de91cf493",
  "ip_version": 4,
  "type": "5_bgp",
  "ip_address": "88.***.***.102",
  "charge_mode": "bandwidth",
  "bandwidth_id": "cff40e5e-demo-a8df-va86-7366077bf097",
  "bandwidth_size": 300,
  "bandwidth_name": "vpngw-bandwidth-1391"
},
"eip2": {
  "id": "6ad8e297-demo-a8df-va86-da0f885ccb98",
  "ip_version": 4,
  "type": "5_bgp",
  "ip_address": "88.***.***.188",
  "charge_mode": "bandwidth",
  "bandwidth_id": "d290f1ee-demo-a8df-va86-d701748f0851",
  "bandwidth_size": 300,
  "bandwidth_name": "vpngw-bandwidth-1392"
},
"created_at": "2022-09-15T08:56:09.386Z",
"updated_at": "2022-09-15T11:13:13.677Z",
"access_vpc_id": "0cf79a3f-demo-a8df-va86-d7ace626b0fa",
"access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
"ha_mode": "active-active"
},
"request_id": "33a2b77a-65f9-4fa0-90bd-4bd42038eb41"
}
```

- b. Response returned when a VPN gateway being created fails to be updated

```
{
  "error_code": "VPN.0003",
  "error_msg": "resource (type=GATEWAY, ID=ff9bdca6-demo-a8df-va86-e4bcc1ea52bc) is not ready, currently CREATING",
  "request_id": "abafe41c-7744-41af-bf3d-4452872af799"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.1.6 Deleting a VPN Gateway

Function

This API is used to delete a VPN gateway with a specified gateway ID. If a pay-per-use VPN gateway to be deleted is bound to yearly/monthly EIPs, unbind the EIPs first. Otherwise, the VPN gateway cannot be deleted.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/vpn-gateways/{vgw_id}

Table 4-52 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vgw_id	String	Yes	Specifies the ID of a VPN gateway instance.

Request

- Request parameters
None
- Example request
DELETE https://{Endpoint}/v5/{project_id}/vpn-gateways/{vgw_id}

Response

- Response parameters
Returned status code 204: successful deletion
- Example response
Response returned when a VPN gateway being created fails to be deleted

```
{
  "error_code": "VPN.0003",
  "error_msg": "resource (type=GATEWAY, ID=ff9bdca6-demo-a8df-va86-e4bcc1ea52bc) is not ready, currently CREATING",
  "request_id": "1d94a4e8-fdc2-7bfd-943e-19bfa9b234ac"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.1.7 Querying the AZs of VPN Gateways

Function

This API is used to query the AZs of VPN gateways.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn-gateways/availability-zones

Table 4-53 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/vpn-gateways/availability-zones

Response

- Response parameters
Returned status code 200: successful operation

Table 4-54 Parameters in the response body

Parameter	Type	Description
availability_zones	AvailabilityZones object	Specifies the list of AZs.
request_id	String	Specifies a request ID.

Table 4-55 AvailabilityZones

Parameter	Type	Description
professional1	VpnGatewayAvailabilityZones object	Indicates that the specification of VPN gateways is Professional1.
professional2	VpnGatewayAvailabilityZones object	Indicates that the specification of VPN gateways is Professional2.

The supported specification options are subject to the value range of the **Specification** parameter on the page for creating a VPN gateway on the VPN console.

Table 4-56 VpnGatewayAvailabilityZones

Parameter	Type	Description
vpc	Array of String	Specifies the list of AZs for VPN gateways associated with VPCs.
er	Array of String	Specifies the list of AZs for VPN gateways associated with enterprise routers.

• Example response

```
{
  "availability_zones": {
    "vpc": ["cn-south-1f"],
    "er": ["az1"]
  },
  "professional1": {
    "vpc": ["cn-south-1f", "cn-south-1e", "cn-south-1c"],
    "er": ["cn-south-1f"]
  },
  "vpc": ["cn-south-1f", "cn-south-1e", "cn-south-1c"],
  "er": ["cn-south-1f"]
},
"request_id": "b60309ab-812c-4269-9de4-fb9a65e6db16"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.1.8 Querying the Route Table of a VPN Gateway

Function

This API is used to query the route table of a VPN gateway with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn-gateways/{vgw_id}/routing-table

Table 4-57 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vgw_id	String	Yes	Specifies a VPN gateway ID.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/vpn-gateways/{vgw_id}/routing-table

Response

- Response parameters
Returned status code 200: successful query

Table 4-58 Parameters in the response body

Parameter	Type	Description
routing_table	Array of Route objects	Indicates the route table of a specified VPN gateway.
total_count	Long	Specifies the total number of routes on the gateway.
page_info	ResponsePageInfoV3	Specifies pagination information.

Table 4-59 Route

Parameter	Type	Description
destination	String	Specifies the destination address of a route.
nexthop	String	Specifies the next-hop IP address.
outbound_interface_ip	String	Specifies the IP address of the outbound interface.
origin	String	• Specifies the origin of a BGP route. • The value can be igp, egp, or incomplete.
as_path	String	Specifies the AS_Path of a BGP route.
med	Integer	Specifies the MED value of a BGP route.
nexthop_resource	NextHopResource object	Specifies the next hop resource of a route.

Table 4-60 NexthopResource

Parameter	Type	Description
id	String	Specifies the next-hop resource ID, which is in UUID format.
type	String	- Specifies the next-hop resource type. - The value can be er, vpn_gateway or vpn_connection.

Table 4-61 ResponsePageInfoV3

Parameter	Type	Description
current_count	Integer	Specifies the number of resources in the list.
next_marker	String	Specifies the marker value of the next page.

- Example response
 - a. Example response to the request for querying a public VPN gateway associated with an enterprise router

```
{
  "routing_table": [
    {
      "destination": "192.168.0.0/24",
      "nexthop": "192.168.0.240",
      "outbound_interface_ip": "192.168.0.240",
      "origin": "igp",
      "as_path": "64513",
      "med": 0,
      "nexthop_resource": {
        "id": "fd8e4220-cdcd-4c84-809e-09fd3148b24b",
        "type": "vpn_connection"
      }
    },
    {
      "destination": "222.69.222.1/32",
      "nexthop": "169.254.1.2",
      "outbound_interface_ip": "169.254.1.1",
      "origin": "igp",
      "as_path": "64513",
      "med": 0,
      "nexthop_resource": {
        "id": "e3c28cc1-fb34-4acd-97f9-29d8e42efe0f",
        "type": "vpn_gateway"
      }
    },
    {
      "destination": "222.69.222.2/32",
      "nexthop": "169.254.2.2",
      "outbound_interface_ip": "169.254.2.1",
      "origin": "igp",
      "as_path": "64513",
      "med": 0,
```

```
    "nexthop_resource": {  
      "id": "85d31993-f519-49ea-8d2e-7afeffb8ef5e",  
      "type": "vpn_connection"  
    }  
  },  
  "total_count": 3,  
  "page_info": {  
    "current_count": 3  
  }  
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.2 Customer Gateway

4.1.2.1 Creating a Customer Gateway

Function

This API is used to create a customer gateway to which a VPN gateway connects.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/customer-gateways

Table 4-62 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Request

- Request parameters

Table 4-63 Request parameters

Parameter	Type	Mandatory	Description
customer_gateway	CreateCgwRequestBodyContent object	Yes	Specifies the customer gateway object.

Table 4-64 CreateCgwRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies the name of a customer gateway. If this parameter is not specified, a name in the format of cgw-**** is automatically generated, for example, cgw-21a3. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
id_type	String	No	- Specifies the identifier type of a customer gateway. - The value is ip. - The default value is ip.
id_value	String	Yes	- Specifies the identifier of a customer gateway. - The value is a string of 1 to 128 characters. When id_type is set to ip, the value is an IPv4 address in dotted decimal notation, for example, 192.168.45.7.
bgp_asn	Long	No	- Specifies the BGP AS number of the customer gateway. - The value ranges from 1 to 4294967295. - Set this parameter only when id_type is set to ip.
tags	Array of VpnResourceTag object	No	- Specifies a tag list. - A maximum of 20 tags can be specified.

Table 4-65 VpnResourceTag

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	Yes	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example request
POST https://{Endpoint}/v5/{project_id}/vpn/customer-gateways

```
{
  "customer_gateway": {
    "name": "cgw-2abf",
    "id_type": "ip",
    "id_value": "10.***.***.21",
    "bgp_asn": 65000,
  }
}
```

Response

- Response parameters
Returned status code 201: successful creation

Table 4-66 Parameters in the response body

Parameter	Type	Description
customer_gateway	ResponseCustomerGateway object	Specifies the customer gateway object.
request_id	String	Specifies a request ID.

Table 4-67 ResponseCustomerGateway

Parameter	Type	Description
id	String	- Specifies the ID of a customer gateway. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a customer gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
id_type	String	- Specifies the identifier type of a customer gateway. - The value is ip.
id_value	String	Specifies the identifier of a customer gateway.
bgp_asn	Long	Specifies the BGP AS number of the customer gateway. This parameter is available only when id_type is set to ip .
created_at	String	- Specifies the time when the customer gateway is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ss.SSSZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ss.SSSZ</i>.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-68 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

Parameter	Type	Description
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example response

```
{
  "customer_gateway": {
    "id": "03c0aa3d-demo-a8df-va86-9d82473765d4",
    "name": "cgw-2abf",
    "id_type": "ip",
    "id_value": "10.***.***.21",
    "bgp_asn": 65000,
    "created_at": "2021-12-21T16:49:28.108+08:00",
    "updated_at": "2021-12-21T16:49:28.108+08:00"
  },
  "request_id": "7e0383bf-a7fb-461b-a926-baa8a795bf1a"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.2.2 Querying a Specified Customer Gateway

Function

This API is used to query a customer gateway with a specified gateway ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/customer-gateways/{customer_gateway_id}

Table 4-69 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
customer_gateway_id	String	Yes	Specifies a customer gateway ID.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/customer-gateways/{customer_gateway_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-70 Parameters in the response body

Parameter	Type	Description
customer_gateway	ResponseCustomerGateway object	Specifies the customer gateway object.
request_id	String	Specifies a request ID.

Table 4-71 ResponseCustomerGateway

Parameter	Type	Description
id	String	- Specifies the ID of a customer gateway. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a customer gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
id_type	String	- Specifies the identifier type of a customer gateway. - The value is ip.
id_value	String	Specifies the identifier of a customer gateway.
bgp_asn	Long	Specifies the BGP AS number of the customer gateway. This parameter is available only when id_type is set to ip .

Parameter	Type	Description
created_at	String	- Specifies the time when the customer gateway is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-72 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example response

```
{
  "customer_gateway": {
    "id": "03c0aa3d-demo-a8df-va86-9d82473765d4",
    "name": "cgw-ba08",
    "id_type": "ip",
    "id_value": "10.***.***.21",
    "bgp_asn": 65000,
    "created_at": "2021-12-21T16:49:28.108+08:00",
    "updated_at": "2021-12-21T16:49:28.108+08:00"
  },
  "request_id": "8111d315-5024-45c9-8ee3-5ef676edb0d1"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.2.3 Querying the Customer Gateway List

Function

This API is used to query the customer gateway list.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/customer-gateways

Table 4-73 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Table 4-74 Parameter in a query request

Parameter	Type	Mandatory	Description
limit	Integer	No	- Specifies the number of records returned on each page during pagination query. - The value ranges from 0 to 200. - The default value is 200.
marker	String	No	- Specifies the start flag for querying the current page. If this parameter is left blank, the first page is queried. The marker for querying the next page is the next_marker in the page_info object returned on the current page. - This parameter must be used together with limit.

Request

- Request parameters
None

- Example request
GET https://{Endpoint}/v5/{project_id}/customer-gateways?limit={limit}&marker={marker}

Response

- Response parameters
Returned status code 200: successful query

Table 4-75 Parameters in the response body

Parameter	Type	Description
customer_gateways	Array of ResponseCustomerGateway objects	Specifies the customer gateway object.
total_count	Long	Specifies the total number of a tenant's customer gateways.
page_info	PageInfo object	Specifies pagination information.
request_id	String	Specifies a request ID.

Table 4-76 ResponseCustomerGateway

Parameter	Type	Description
id	String	• Specifies the ID of a customer gateway. • The value is a UUID containing 36 characters.
name	String	• Specifies the name of a customer gateway. • The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
id_type	String	• Specifies the identifier type of a customer gateway. • The value is ip.
id_value	String	Specifies the identifier of a customer gateway.
bgp_asn	Long	Specifies the BGP AS number of the customer gateway. This parameter is available only when id_type is set to ip .

Parameter	Type	Description
created_at	String	- Specifies the time when the customer gateway is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-77 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (<code>_ . : = + - @</code>).
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (<code>_ . : = + - @</code>).

Table 4-78 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	Integer	Specifies the number of resources in the list. If the value of current_count is less than the value of limit in the query request, the current page is the last page.

- Example response

```
{
  "customer_gateways": [{
    "id": "e67d6e27-demo-a8df-va86-be9a0f0168e9",
    "name": "cgw-a45b",
    "id_type": "ip",
    "id_value": "100.***.***.81",
    "bgp_asn": 65588,
    "created_at": "2022-11-28T07:36:24.923Z",
    "updated_at": "2022-11-28T07:36:24.923Z"
  }, {
    "id": "312067bb-demo-a8df-va86-09dc941bbffc",
    "name": "cgw-21a3",
    "id_value": "123*****456",
    "created_at": "2022-11-28T06:25:01.937Z",
    "updated_at": "2022-11-28T06:25:01.937Z"
  }],
  "total_count": 2,
  "page_info": {
    "next_marker": "2022-11-28T06:25:01.937Z",
    "current_count": 2
  },
  "request_id": "82a108d9-0929-42e9-adb7-e146c04c587c"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.2.4 Updating a Customer Gateway

Function

This API is used to update a customer gateway with a specified gateway ID. Only the gateway name can be updated. To modify other parameters, you need to create another customer gateway.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/customer-gateways/{customer_gateway_id}

Table 4-79 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
customer_gateway_id	String	Yes	Specifies a customer gateway ID.

Request

- Request parameters

Table 4-80 Request parameters

Parameter	Type	Mandatory	Description
customer_gateway	UpdateCgwRequestBodyContent object	Yes	Specifies the customer gateway object.

Table 4-81 UpdateCgwRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies a gateway name. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).

- Example request

PUT https://{Endpoint}/v5/{project_id}/customer-gateways/{customer_gateway_id}

```
{
  "customer_gateway": {
    "name": "cgw-f846",
  }
}
```

Response

- Response parameters
Returned status code 200: successful update

Table 4-82 Parameters in the response body

Parameter	Type	Description
customer_gateway	ResponseCustomerGateway object	Specifies the customer gateway object.
request_id	String	Specifies a request ID.

Table 4-83 ResponseCustomerGateway

Parameter	Type	Description
id	String	- Specifies the ID of a customer gateway. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a customer gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
id_type	String	- Specifies the identifier type of a customer gateway. - The value is ip.
id_value	String	Specifies the identifier of a customer gateway.
bgp_asn	Long	Specifies the BGP AS number of the customer gateway. This parameter is available only when id_type is set to ip .
created_at	String	- Specifies the time when the customer gateway is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ss.SSSZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ss.SSSZ</i>.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-84 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

Parameter	Type	Description
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example response

```
{
  "customer_gateway": {
    "id": "03c0aa3d-demo-a8df-va86-9d82473765d4",
    "name": "cgw-f846",
    "id_type": "ip",
    "id_value": "10.***.***.21",
    "bgp_asn": 65533,
    "created_at": "2021-12-21T16:49:28.108Z",
    "updated_at": "2021-12-21T16:49:28.108Z"
  },
  "request_id": "96718f4a-f57a-4e1f-8d05-7d5e903c8d90"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.2.5 Deleting a Customer Gateway

Function

This API is used to delete a customer gateway with a specified gateway ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/customer-gateways/{customer_gateway_id}

Table 4-85 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
customer_gateway_id	String	Yes	Specifies a customer gateway ID.

Request

- Request parameters
None
- Example request
DELETE https://{Endpoint}/v5/{project_id}/customer-gateways/{customer_gateway_id}

Response

- Response parameters
Returned status code 204: successful deletion
- Example response
Response returned when a customer gateway that has been created and has VPN connections fails to be deleted
DELETE https://{Endpoint}/v5/{project_id}/customer-gateways/{customer_gateway_id}
{
 "error_code": "VPN.0001",
 "error_msg": "invalid request: customer gateway 575c1722-demo-a8df-va86-dd7f41876332 has connection",
 "request_id": "c923ac44-1890-48d5-a004-5be6432cf361"
}

Status Codes

For details, see [A.2 Status Codes](#).

4.1.3 VPN Connection

4.1.3.1 Creating a VPN Connection

Function

This API is used to create a VPN connection that connects a VPN gateway to a customer gateway.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/vpn-connection

Table 4-86 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Request

- Request parameters

Table 4-87 Request parameters

Parameter	Type	Mandatory	Description
vpn_connection	CreateVpnConnectionRequestBodyContent object	Yes	Specifies the VPN connection object.

Table 4-88 CreateVpnConnectionRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies the name of a VPN connection. If this parameter is not specified, a name in the format of vpn-**** is automatically generated, for example, vpn-13be. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
vgw_id	String	Yes	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters. You can obtain the VPN gateway ID by querying the VPN gateway list.

Parameter	Type	Mandatory	Description
vgw_ip	String	Yes	- Function description: - When network_type of the VPN gateway is set to public, set vgw_ip to the EIP IDs of the VPN gateway. - When network_type of the VPN gateway is set to private, set vgw_ip to the private IP addresses of the VPN gateway. - The value is a UUID containing 36 characters or an IPv4 address in dotted decimal notation (for example, 192.168.45.7). You can obtain the EIP IDs or private IP addresses of the VPN gateway by querying information about the VPN gateway.
style	String	No	- Specifies the connection mode. - Value range: policy: policy-based mode static: static routing mode bgp: BGP routing mode - The default value is static.
cgw_id	String	Yes	- Specifies a customer gateway ID. - The value is a UUID containing 36 characters.
peer_subnets	Array of String	No	- Specifies an IPv4 customer subnet. - Constraints: - Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets. - A maximum of 50 customer subnets can be configured for each VPN connection.

Parameter	Type	Mandatory	Description
tunnel_local_address	String	No	- Specifies the tunnel interface address configured on the VPN gateway in route-based mode, for example, 169.254.76.1/30. - Constraints: - The first 16 bits must be 169.254, and the value cannot be 169.254.195.xxx. - The mask length must be 30, and the address must be in the same CIDR block as the value of tunnel_peer_address. - The address needs to be a host address in a CIDR block.
tunnel_peer_address	String	No	- Specifies the tunnel interface address configured on the customer gateway device in route-based mode, for example, 169.254.76.2/30. - Constraints: - The first 16 bits must be 169.254, and the value cannot be 169.254.195.xxx. - The mask length must be 30, and the address must be in the same CIDR block as the value of tunnel_local_address. - The address needs to be a host address in a CIDR block.
enable_nqa	Boolean	No	- Specifies whether to enable the network quality analysis (NQA) function. - The value can be true or false. - The default value is false. - Set this parameter only when style is set to static.

Parameter	Type	Mandatory	Description
enable_hub	Boolean	No	- Specifies whether to enable branch interconnection. - The value can be true or false. - The default value is false. - Set this parameter only when style is set to BGP.
psk	String	No	- Specifies a pre-shared key. - The value is a string of 8 to 128 characters, which must contain at least three types of the following: uppercase letters, lowercase letters, digits, and special characters (~!@#\$%^()-_+={ },./:;).
policy_rules	Array of PolicyRule object	No	Specifies IPv4 policy rules. A maximum of five policy rules can be specified. This parameter is mandatory only when style is set to policy and ip_version of the VPN gateway is set to ipv4 .
ikepolicy	IkePolicy object	No	Specifies the Internet Key Exchange (IKE) policy object.
ipsecpolicy	IpsecPolicy object	No	Specifies the Internet Protocol Security (IPsec) policy object.
ha_role	String	No	- This parameter is optional when you create a connection for a VPN gateway in active-active mode. When you create a connection for a VPN gateway in active-standby mode, master indicates the active connection, and slave indicates the standby connection. - The default value is master. - Constraints: In active/standby mode, this field must be set to master for the connection established using the active EIP or active private IP address of the VPN gateway, and must be set to slave for the connection established using the standby EIP or standby private IP address of the VPN gateway.

Parameter	Type	Mandatory	Description
tags	Array of VpnResourceTag object	No	- Specifies a tag list. - A maximum of 20 tags can be specified.

Table 4-89 PolicyRule

Parameter	Type	Mandatory	Description
source	String	No	- Specifies a source CIDR block. The IP protocol version (IPv4) of the CIDR block must be the same as that of the VPN gateway. - The value of source in each policy rule must be unique.
destination	Array of String	No	- Specifies a destination CIDR block. The IP protocol version (IPv4) of the CIDR block must be the same as that of the VPN gateway. An example IPv4 CIDR block is 192.168.52.0/24. - A maximum of 50 destination CIDR blocks can be configured in each policy rule.

Table 4-90 IkePolicy

Parameter	Type	Mandatory	Description
ike_version	String	No	- Specifies the IKE version. - Value range: v1 and v2 - Default value: v2

Parameter	Type	Mandatory	Description
phase1_negotiation_mode	String	No	- Specifies the negotiation mode. - Value range: main: ensures high security during negotiation. aggressive: ensures fast negotiation and a high negotiation success rate. - The default value is main. - This parameter is mandatory only when the IKE version is v1.
authentication_algorithm	String	No	- Specifies an authentication algorithm. - Value range: sha2-512, sha2-384, sha2-256, sha1, md5 Exercise caution when using sha1 and md5 as they have low security. - Default value: sha2-256
encryption_algorithm	String	No	- Specifies an encryption algorithm. - Value range: aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, 3des Exercise caution when using 3des, aes-128, aes-192, and aes-256 as they have low security. - Default value: aes-128
dh_group	String	No	- Specifies the DH group used for key exchange in phase 1. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, or group21. Exercise caution when using group1, group2, group5, or group14 as they have low security. - The default value is group15.

Parameter	Type	Mandatory	Description
authentication_method	String	No	- Specifies the authentication method used during IKE negotiation. - Value range: pre-share: pre-shared key - The default value is pre-share.
lifetime_seconds	Integer	No	- Specifies the security association (SA) lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds. - The default value is 86400.
local_id_type	String	No	- Specifies the local ID type. - The value is ip. - The default value is ip.
local_id	String	No	- Specifies the local ID. - Constraints: When local_id_type is set to ip, this parameter is optional. If it is set, the value must be an IPv4 address.
peer_id_type	String	No	- Specifies the peer ID type. - The value is ip. - The default value is ip.
peer_id	String	No	- Specifies the peer ID. - Constraints: When local_id_type is set to ip, this parameter is optional. If it is set, the value must be an IPv4 address.
dpd	Dpd object	No	Specifies the dead peer detection (DPD) object.

Table 4-91 Dpd

Parameter	Type	Mandatory	Description
timeout	Integer	No	- Specifies the interval for retransmitting DPD packets. - The value ranges from 2 to 60, in seconds. - The default value is 15.
interval	Integer	No	- Specifies the DPD idle timeout period. - The value ranges from 10 to 3600, in seconds. - The default value is 30.
msg	String	No	- Specifies the format of DPD packets. - Value range: seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash. - The default value is seq-hash-notify.

Table 4-92 IpsecPolicy

Parameter	Type	Mandatory	Description
authentication_algorithm	String	No	- Specifies an authentication algorithm. - Value range: sha2-512, sha2-384, sha2-256, sha1, md5 Exercise caution when using sha1 and md5 as they have low security. - Default value: sha2-256

Parameter	Type	Mandatory	Description
encryption_algorithm	String	No	- Specifies an encryption algorithm. - Value range: aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, 3des Exercise caution when using 3des, aes-128, aes-192, and aes-256 as they have low security. - Default value: aes-128
pfs	String	No	- Specifies the DH key group used by Perfect Forward Secrecy (PFS). - The value can be group1, group2, group5, group14, group15, group16, group19, group20, group21, or disable. Exercise caution when using group1, group2, group5, or group14 as they have low security. - The default value is group15.
transform_protocol	String	No	- Specifies the transfer protocol. - Value range: esp: encapsulating security payload protocol - The default value is esp.
lifetime_seconds	Integer	No	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds. - The default value is 3600.
encapsulation_mode	String	No	- Specifies the packet encapsulation mode. - Value range: tunnel: encapsulates packets in tunnel mode. - The default value is tunnel.

Table 4-93 VpnResourceTag

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	Yes	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example requests

- a. Create a VPN connection in static routing mode.

POST https://{Endpoint}/v5/{project_id}/vpn-connection

```
{
  "vpn_connection": {
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",
    "peer_subnets": [
      "192.168.44.0/24"
    ],
    "psk": "abcd****"
  }
}
```

- b. Create a VPN connection in policy-based mode.

POST https://{Endpoint}/v5/{project_id}/vpn-connection

```
{
  "vpn_connection": {
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",
    "style": "policy",
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",
    "peer_subnets": [
      "192.168.44.0/24"
    ],
    "psk": "abcd****",
    "policy_rules": [{
      "source": "10.0.0.0/24",
      "destination": [
        "192.168.0.0/24"
      ]
    }]
  }
}
```

- c. Create a VPN connection in BGP routing mode.

POST https://{Endpoint}/v5/{project_id}/vpn-connection

```
{
  "vpn_connection": {
    "name": "vpn-1655",
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",
    "style": "bgp",
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",
    "peer_subnets": [
      "192.168.44.0/24"
    ],
    "tunnel_local_address": "169.254.56.225/30",
    "tunnel_peer_address": "169.254.56.226/30",
    "psk": "abcd****",
    "ikepolicy": {
      "ike_version": "v2",
      "authentication_algorithm": "sha2-512",
      "encryption_algorithm": "aes-256",
      "dh_group": "group16",
      "lifetime_seconds": 172800,
      "local_id": "123****",
      "peer_id": "456****",
      "dpd": {
        "timeout": 30,
        "interval": 60,
        "msg": "seq-notify-hash"
      }
    },
    "ipsecpolicy": {
      "authentication_algorithm": "sha2-512",
      "encryption_algorithm": "aes-256",
      "pfs": "group16",
      "transform_protocol": "esp",
      "lifetime_seconds": 7200,
      "encapsulation_mode": "tunnel"
    }
  }
}
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-94 Parameters in the response body

Parameter	Type	Description
vpn_connection	ResponseVpnConnection object	Specifies the VPN connection object.
request_id	String	Specifies a request ID.

Table 4-95 ResponseVpnConnection

Parameter	Type	Description
id	String	• Specifies a VPN connection ID. • The value is a UUID containing 36 characters.

Parameter	Type	Description
name	String	- Specifies the name of a VPN connection. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
vgw_id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
vgw_ip	String	- Specifies an EIP ID or private IP address of the VPN gateway. - The value is a UUID containing 36 characters or an IPv4 address in dotted decimal notation (for example, 192.168.45.7).
style	String	- Specifies the connection mode. - Value range: POLICY: policy-based mode STATIC: static routing mode BGP: BGP routing mode
cgw_id	String	- Specifies a customer gateway ID. - The value is a UUID containing 36 characters.
peer_subnets	Array of String	Specifies an IPv4 customer subnet. This parameter is not returned when attachment_type of the VPN gateway is set to ER and style is set to BGP or POLICY .
tunnel_local_address	String	Specifies the tunnel interface address configured on the VPN gateway in route-based mode. This parameter is valid only when style is STATIC or BGP .
tunnel_peer_address	String	Specifies the tunnel interface address configured on the customer gateway device in route-based mode. This parameter is valid only when style is STATIC or BGP .
enable_hub	Boolean	- Specifies whether branch interconnection is enabled. - The value can be true or false.

Parameter	Type	Description
enable_nqa	Boolean	- Specifies whether NQA is enabled. This parameter is returned only when style is STATIC. - The value can be true or false.
policy_rules	Array of PolicyRule objects	Specifies IPv4 policy rules, which are returned only when style is set to POLICY and ip_version of the VPN gateway is set to ipv4 .
ikepolicy	IkePolicy object	Specifies the IKE policy object.
ipsecpolicy	IpsecPolicy object	Specifies the IPsec policy object.
created_at	String	- Specifies the time when the VPN connection is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. The value must be the same as the enterprise project ID of the VPN gateway specified by vgw_id.
ha_role	String	- For a VPN gateway in active-standby mode, master indicates the active connection, and slave indicates the standby connection. For a VPN gateway in active-active mode, the value of ha_role can only be master. - The default value is master.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-96 PolicyRule

Parameter	Type	Description
rule_index	Integer	- Specifies a rule ID. - The value ranges from 0 to 50.

Parameter	Type	Description
source	String	Specifies a source CIDR block.
destination	Array of String	Specifies a destination CIDR block. An example IPv4 CIDR block is 192.168.52.0/24. A maximum of 50 destination CIDR blocks can be returned for each policy rule.

Table 4-97 IkePolicy

Parameter	Type	Description
ike_version	String	- Specifies the IKE version. - The value can be v1 or v2.
phase1_negotiation_mode	String	- Specifies the negotiation mode. This parameter is available only when the IKE version is v1. - Value range: main: ensures high security during negotiation. aggressive: ensures fast negotiation and a high negotiation success rate.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, or group21.
authentication_method	String	- Specifies the authentication method used during IKE negotiation. - Value range: pre-share: pre-shared key

Parameter	Type	Description
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.
local_id_type	String	- Specifies the local ID type. - The value is ip.
local_id	String	Specifies the local ID. When local_id_type is set to ip , the local ID specified when the VPN connection is created or updated is returned. If no local ID is specified, the VPN gateway IP address corresponding to the VPN connection is returned.
peer_id_type	String	- Specifies the peer ID type. - The value is ip.
peer_id	String	Specifies the peer ID. When peer_id_type is set to ip , the peer ID specified when the VPN connection is created or updated is returned. If no peer ID is specified, the IP address of the customer gateway is returned.
dpd	Dpd object	Specifies the DPD object.

Table 4-98 Dpd

Parameter	Type	Description
timeout	Integer	- Specifies the interval for retransmitting DPD packets. - The value ranges from 2 to 60, in seconds.
interval	Integer	- Specifies the DPD idle timeout period. - The value ranges from 10 to 3600, in seconds.

Parameter	Type	Description
msg	String	- Specifies the format of DPD packets. - Value range: seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash.

Table 4-99 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, group21, or disable.
transform_protocol	String	- Specifies the transfer protocol. - Value range: esp: encapsulating security payload protocol
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.
encapsulation_mode	String	- Specifies the packet encapsulation mode. - Value range: tunnel: encapsulates packets in tunnel mode.

Table 4-100 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example responses
 - a. Response to the request for creating a VPN connection in static routing mode

```
{
  "vpn_connection": {
    "id": "98c5af8a-6ee2-4482-99a2-ae2280a6f4c3",
    "name": "vpn-b2cb",
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",
    "style": "STATIC",
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",
    "peer_subnets": ["192.168.44.0/24"],
    "tunnel_local_address": "169.254.56.225/30",
    "tunnel_peer_address": "169.254.56.226/30",
    "enable_nqa": false,
    "ikepolicy": {
      "ike_version": "v2",
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "dh_group": "group15",
      "authentication_method": "pre-share",
      "lifetime_seconds": 86400,
      "local_id_type": "ip",
      "local_id": "10.***.***.134",
      "peer_id_type": "ip",
      "peer_id": "88.***.***.164",
      "dpd": {
        "timeout": 15,
        "interval": 30,
        "msg": "seq-hash-notify"
      }
    },
    "ipsecpolicy": {
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "pfs": "group15",
      "transform_protocol": "esp",
      "lifetime_seconds": 3600,
      "encapsulation_mode": "tunnel"
    },
    "created_at": "2022-11-26T13:41:34.626Z",
    "updated_at": "2022-11-26T13:41:34.626Z",
    "enterprise_project_id": "0",
    "ha_role": "master"
  }
}
```

```
},  
"request_id": "f91082d4-6d49-479c-ad1d-4e552a9f5cae"  
}
```

b. Response to the request for creating a connection in policy-based mode

```
{  
  "vpn_connection": {  
    "id": "98c5af8a-demo-a8df-va86-ae2280a6f4c3",  
    "name": "vpn-799d",  
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",  
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",  
    "style": "POLICY",  
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",  
    "peer_subnets": ["192.168.44.0/24"],  
    "tunnel_local_address": "169.254.56.225/30",  
    "tunnel_peer_address": "169.254.56.226/30",  
    "policy_rules": [{  
      "rule_index": 1,  
      "source": "10.0.0.0/24",  
      "destination": [  
        "192.168.44.0/24"  
      ]  
    }],  
    "ikepolicy": {  
      "ike_version": "v2",  
      "authentication_algorithm": "sha2-256",  
      "encryption_algorithm": "aes-128",  
      "dh_group": "group15",  
      "authentication_method": "pre-share",  
      "lifetime_seconds": 86400,  
      "local_id_type": "ip",  
      "local_id": "10.***.***.134",  
      "peer_id_type": "ip",  
      "peer_id": "88.***.***.164",  
      "dpd": {  
        "timeout": 15,  
        "interval": 30,  
        "msg": "seq-hash-notify"  
      }  
    },  
    "ipsecpolicy": {  
      "authentication_algorithm": "sha2-256",  
      "encryption_algorithm": "aes-128",  
      "pfs": "group15",  
      "transform_protocol": "esp",  
      "lifetime_seconds": 3600,  
      "encapsulation_mode": "tunnel"  
    },  
    "created_at": "2022-11-26T13:41:34.626Z",  
    "updated_at": "2022-11-26T13:41:34.626Z",  
    "enterprise_project_id": "0",  
    "ha_role": "master"  
  },  
  "request_id": "f91082d4-6d49-479c-ad1d-4e552a9f5cae"  
}
```

c. Response to the request for creating a VPN connection in BGP routing mode

```
{  
  "vpn_connection": {  
    "id": "98c5af8a-demo-a8df-va86-ae2280a6f4c3",  
    "name": "vpn-1655",  
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",  
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",  
    "style": "BGP",  
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",  
    "peer_subnets": ["192.168.44.0/24"],  
    "tunnel_local_address": "169.254.56.225/30",  
    "tunnel_peer_address": "169.254.56.226/30",  
    "ikepolicy": {  
      "ike_version": "v2",  
      "authentication_algorithm": "sha2-256",  
      "encryption_algorithm": "aes-128",  
      "dh_group": "group15",  
      "authentication_method": "pre-share",  
      "lifetime_seconds": 86400,  
      "local_id_type": "ip",  
      "local_id": "10.***.***.134",  
      "peer_id_type": "ip",  
      "peer_id": "88.***.***.164",  
      "dpd": {  
        "timeout": 15,  
        "interval": 30,  
        "msg": "seq-hash-notify"  
      }  
    },  
    "ipsecpolicy": {  
      "authentication_algorithm": "sha2-256",  
      "encryption_algorithm": "aes-128",  
      "pfs": "group15",  
      "transform_protocol": "esp",  
      "lifetime_seconds": 3600,  
      "encapsulation_mode": "tunnel"  
    },  
    "created_at": "2022-11-26T13:41:34.626Z",  
    "updated_at": "2022-11-26T13:41:34.626Z",  
    "enterprise_project_id": "0",  
    "ha_role": "master"  
  },  
  "request_id": "f91082d4-6d49-479c-ad1d-4e552a9f5cae"  
}
```

```
{
  "ike_version": "v2",
  "authentication_algorithm": "sha2-512",
  "encryption_algorithm": "aes-256",
  "dh_group": "group16",
  "authentication_method": "pre-share",
  "lifetime_seconds": 172800,
  "local_id": "123***",
  "peer_id": "456***",
  "dpd": {
    "timeout": 30,
    "interval": 60,
    "msg": "seq-notify-hash"
  },
  "ipsecpolicy": {
    "authentication_algorithm": "sha2-512",
    "encryption_algorithm": "aes-256",
    "pfs": "group16",
    "transform_protocol": "esp",
    "lifetime_seconds": 7200,
    "encapsulation_mode": "tunnel"
  },
  "created_at": "2022-11-26T13:41:34.626Z",
  "updated_at": "2022-11-26T13:41:34.626Z",
  "enterprise_project_id": "0",
  "ha_role": "master"
},
"request_id": "f91082d4-6d49-479c-ad1d-4e552a9f5cae"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.3.2 Creating VPN Connections in Batches

Function

This API is used to create one or two VPN connections for a VPN gateway in batches.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/vpn-connections/batch-create

Table 4-101 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Request

- Request parameters

Table 4-102 Request parameters

Parameter	Type	Mandatory	Description
vpn_connections	Array of CreateVpnConnectionRequestBodyContent object	Yes	Specifies the vpn_connection object array. One or two VPN connections can be created at a time.

Table 4-103 CreateVpnConnectionRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies the name of a VPN connection. If this parameter is not specified, a name in the format of vpn-**** is automatically generated, for example, vpn-13be. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
vgw_id	String	Yes	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters. When two VPN connections are to be created, the values of vgw_id must be the same. You can obtain the VPN gateway ID by querying the VPN gateway list.

Parameter	Type	Mandatory	Description
vgw_ip	String	Yes	- Function description: - When network_type of the VPN gateway is set to public, set vgw_ip to the EIP IDs of the VPN gateway. - When network_type of the VPN gateway is set to private, set vgw_ip to the private IP addresses of the VPN gateway. - The value is a UUID containing 36 characters or an IPv4 address in dotted decimal notation (for example, 192.168.45.7). You can obtain the EIP IDs or private IP addresses of the VPN gateway by querying information about the VPN gateway.
style	String	No	- Specifies the connection mode. - Value range: policy: policy-based mode static: static routing mode bgp: BGP routing mode - The default value is static.
cgw_id	String	Yes	- Specifies a customer gateway ID. - The value is a UUID containing 36 characters.
peer_subnets	Array of String	No	- Specifies an IPv4 customer subnet. - Constraints: - This parameter is not required when attachment_type of the VPN gateway is set to er and style is set to policy or bgp. In other scenarios, this parameter is mandatory. - Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets. - A maximum of 50 customer subnets can be configured for each VPN connection.

Parameter	Type	Mandatory	Description
tunnel_local_address	String	No	- Specifies the tunnel interface address configured on the VPN gateway in route-based mode, for example, 169.254.76.1/30. - Constraints: - The first 16 bits must be 169.254, and the value cannot be 169.254.195.xxx. - The mask length must be 30, and the address must be in the same CIDR block as the value of tunnel_peer_address. - The address needs to be a host address in a CIDR block.
tunnel_peer_address	String	No	- Specifies the tunnel interface address configured on the customer gateway device in route-based mode, for example, 169.254.76.2/30. - Constraints: - The first 16 bits must be 169.254, and the value cannot be 169.254.195.xxx. - The mask length must be 30, and the address must be in the same CIDR block as the value of tunnel_local_address. - The address needs to be a host address in a CIDR block.
enable_nqa	Boolean	No	- Specifies whether NQA is enabled. - The value can be true or false. - The default value is false. - Set this parameter only when style is set to static.
enable_hub	Boolean	No	- Specifies whether branch interconnection is enabled. - The value can be true or false. - The default value is false. - Set this parameter only when style is set to BGP.

Parameter	Type	Mandatory	Description
psk	String	No	- Specifies a pre-shared key. - The value is a string of 8 to 128 characters, which must contain at least three types of the following: uppercase letters, lowercase letters, digits, and special characters (~!@#\$%^()-_+={ } , / ;).
policy_rules	Array of PolicyRule object	No	Specifies IPv4 policy rules. A maximum of five policy rules can be specified. This parameter is mandatory only when style is set to policy and ip_version of the VPN gateway is set to ipv4 .
ikepolicy	IkePolicy object	No	Specifies the IKE policy object.
ipsecpolicy	IpsecPolicy object	No	Specifies the IPsec policy object.
ha_role	String	No	- This parameter is optional when you create a connection for a VPN gateway in active-active mode. When you create a connection for a VPN gateway in active/standby mode, master indicates the active connection, and slave indicates the standby connection. - The default value is master. - Constraints: In active/standby mode, this field must be set to master for the connection established using the active EIP or active private IP address of the VPN gateway, and must be set to slave for the connection established using the standby EIP or standby private IP address of the VPN gateway.
tags	Array of VpnResourceTag object	No	- Specifies a tag list. - A maximum of 20 tags can be specified.

Table 4-104 PolicyRule

Parameter	Type	Mandatory	Description
source	String	No	- Specifies a source CIDR block. The IP protocol version (IPv4) of the CIDR block must be the same as that of the VPN gateway. - The value of source in each policy rule must be unique.
destination	Array of String	No	- Specifies a destination CIDR block. The IP protocol version (IPv4) of the CIDR block must be the same as that of the VPN gateway. An example IPv4 CIDR block is 192.168.52.0/24. - A maximum of 50 destination CIDR blocks can be configured in each policy rule.

Table 4-105 IkePolicy

Parameter	Type	Mandatory	Description
ike_version	String	No	- Specifies the IKE version. - Value range: v1 and v2 - Default value: v2
phase1_negotiation_mode	String	No	- Specifies the negotiation mode. - Value range: main: ensures high security during negotiation. aggressive: ensures fast negotiation and a high negotiation success rate. - The default value is main. - This parameter is mandatory only when the IKE version is v1.

Parameter	Type	Mandatory	Description
authentication_algorithm	String	No	- Specifies an authentication algorithm. - Value range: sha2-512, sha2-384, sha2-256, sha1, md5 Exercise caution when using sha1 and md5 as they have low security. - Default value: sha2-256
encryption_algorithm	String	No	- Specifies an encryption algorithm. - Value range: aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, 3des Exercise caution when using 3des, aes-128, aes-192, and aes-256 as they have low security. - Default value: aes-128
dh_group	String	No	- Specifies the DH group used for key exchange in phase 1. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, or group21. Exercise caution when using group1, group2, group5, or group14 as they have low security. - The default value is group15.
authentication_method	String	No	- Specifies the authentication method used during IKE negotiation. - Value range: pre-share: pre-shared key - The default value is pre-share.

Parameter	Type	Mandatory	Description
lifetime_seconds	Integer	No	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds. - The default value is 86400.
local_id_type	String	No	- Specifies the local ID type. - The value is ip. - The default value is ip.
local_id	String	No	- Specifies the local ID. - Constraints: When local_id_type is set to ip, this parameter is optional. If it is set, the value must be an IPv4 address.
peer_id_type	String	No	- Specifies the peer ID type. - The value is ip. - The default value is ip.
peer_id	String	No	- Specifies the peer ID. - Constraints: When local_id_type is set to ip, this parameter is optional. If it is set, the value must be an IPv4 address.
dpd	Dpd object	No	Specifies the DPD object.

Table 4-106 Dpd

Parameter	Type	Mandatory	Description
timeout	Integer	No	- Specifies the interval for retransmitting DPD packets. - The value ranges from 2 to 60, in seconds. - The default value is 15.

Parameter	Type	Mandatory	Description
interval	Integer	No	- Specifies the DPD idle timeout period. - The value ranges from 10 to 3600, in seconds. - The default value is 30.
msg	String	No	- Specifies the format of DPD packets. - Value range: seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash. - The default value is seq-hash-notify.

Table 4-107 IpsecPolicy

Parameter	Type	Mandatory	Description
authentication_algorithm	String	No	- Specifies an authentication algorithm. - Value range: sha2-512, sha2-384, sha2-256, sha1, md5 Exercise caution when using sha1 and md5 as they have low security. - Default value: sha2-256

Parameter	Type	Mandatory	Description
encryption_algorithm	String	No	- Specifies an encryption algorithm. - Value range: aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, 3des Exercise caution when using 3des , aes-128 , aes-192 , and aes-256 as they have low security. - Default value: aes-128
pfs	String	No	- Specifies the DH key group used by PFS. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, group21, or disable. Exercise caution when using group1, group2, group5, or group14 as they have low security. - The default value is group15.
transform_protocol	String	No	- Specifies the transfer protocol. - Value range: esp: encapsulating security payload protocol - The default value is esp.
lifetime_seconds	Integer	No	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds. - The default value is 3600.
encapsulation_mode	String	No	- Specifies the packet encapsulation mode. - Value range: tunnel: encapsulates packets in tunnel mode. - The default value is tunnel.

Table 4-108 VpnResourceTag

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	Yes	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example request

- a. Create VPN connections in static routing mode in batches.

POST https://{Endpoint}/v5/{project_id}/vpn-connections/batch-create

```
{
  "vpn_connections": [
    {
      "vgw_ip": "0d0f4af1-42b9-41eb-97b9-b4d41a0bf9c4",
      "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
      "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
      "peer_subnets": [
        "192.168.2.0/24"
      ],
      "psk": "abcd****"
    },
    {
      "vgw_ip": "1fb97767-d780-4d8b-83bb-6f878f662005",
      "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
      "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
      "peer_subnets": [
        "192.168.2.0/24"
      ],
      "psk": "abcd****"
    }
  ]
}
```

- b. Create VPN connections in policy-based mode in batches.

POST https://{Endpoint}/v5/{project_id}/vpn-connections/batch-create

```
{
  "vpn_connections": [
    {
      "vgw_ip": "0d0f4af1-42b9-41eb-97b9-b4d41a0bf9c4",
      "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
      "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
      "style": "policy",
      "peer_subnets": [
        "192.168.2.0/24"
      ],
      "psk": "abcd****"
    }
  ]
}
```

```
"policy_rules": [
  {
    "source": "10.0.0.0/24",
    "destination": [
      "192.168.0.0/24"
    ]
  }
],
{
  "vgw_ip": "1fb97767-d780-4d8b-83bb-6f878f662005",
  "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
  "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
  "style": "policy",
  "peer_subnets": [
    "192.168.2.0/24"
  ],
  "psk": "abcd****",
  "policy_rules": [
    {
      "source": "10.0.0.0/24",
      "destination": [
        "192.168.0.0/24"
      ]
    }
  ]
}
]
```

c. Create VPN connections in BGP routing mode in batches.

POST https://{Endpoint}/v5/{project_id}/vpn-connections/batch-create

```
{
  "vpn_connections": [
    {
      "name": "vpn-1655",
      "vgw_ip": "0d0f4af1-42b9-41eb-97b9-b4d41a0bf9c4",
      "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
      "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
      "style": "bgp",
      "peer_subnets": [
        "192.168.2.0/24"
      ],
      "tunnel_local_address": "169.254.56.225/30",
      "tunnel_peer_address": "169.254.56.226/30",
      "psk": "abcd****",
      "ikepolicy": {
        "ike_version": "v2",
        "authentication_algorithm": "sha2-512",
        "encryption_algorithm": "aes-256",
        "dh_group": "group16",
        "lifetime_seconds": 172800,
        "local_id": "123***",
        "peer_id": "456***",
        "dpd": {
          "timeout": 30,
          "interval": 60,
          "msg": "seq-notify-hash"
        }
      },
      "ipsecpolicy": {
        "authentication_algorithm": "sha2-512",
        "encryption_algorithm": "aes-256",
        "pfs": "group16",
        "transform_protocol": "esp",
        "lifetime_seconds": 7200,
        "encapsulation_mode": "tunnel"
      }
    }
  ],
}
```

```
{
  "name": "vpn-1341",
  "vgw_ip": "1fb97767-d780-4d8b-83bb-6f878f662005",
  "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
  "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
  "style": "bgp",
  "peer_subnets": [
    "192.168.2.0/24"
  ],
  "tunnel_local_address": "169.254.56.225/30",
  "tunnel_peer_address": "169.254.56.226/30",
  "psk": "abcd****",
  "ikepolicy": {
    "ike_version": "v2",
    "authentication_algorithm": "sha2-512",
    "encryption_algorithm": "aes-256",
    "dh_group": "group16",
    "lifetime_seconds": 172800,
    "local_id": "123****",
    "peer_id": "456****",
    "dpd": {
      "timeout": 30,
      "interval": 60,
      "msg": "seq-notify-hash"
    }
  },
  "ipsecpolicy": {
    "authentication_algorithm": "sha2-512",
    "encryption_algorithm": "aes-256",
    "pfs": "group16",
    "transform_protocol": "esp",
    "lifetime_seconds": 7200,
    "encapsulation_mode": "tunnel"
  }
}
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-109 Parameters in the response body

Parameter	Type	Description
vpn_connections	Array of CreateResponseVpnConnection object	Specifies the vpn_connections object array.
request_id	String	Specifies a request ID.

Table 4-110 CreateResponseVpnConnection

Parameter	Type	Description
id	String	- Specifies a VPN connection ID. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a VPN connection. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
vgw_id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
vgw_ip	String	- Specifies an EIP ID or private IP address of the VPN gateway. - The value is a UUID containing 36 characters or an IPv4 address in dotted decimal notation (for example, 192.168.45.7).
style	String	- Specifies the connection mode. - Value range: POLICY: policy-based mode STATIC: static routing mode BGP: BGP routing mode
cgw_id	String	- Specifies a customer gateway ID. - The value is a UUID containing 36 characters.
peer_subnets	Array of String	Specifies an IPv4 customer subnet. This parameter is not returned when attachment_type of the VPN gateway is set to ER and style is set to BGP or POLICY .
tunnel_local_address	String	Specifies the tunnel interface address configured on the VPN gateway in route-based mode. This parameter is valid only when style is STATIC or BGP .
tunnel_peer_address	String	Specifies the tunnel interface address configured on the customer gateway device in route-based mode. This parameter is valid only when style is STATIC or BGP .

Parameter	Type	Description
enable_nqa	Boolean	- Specifies whether NQA is enabled. This parameter is returned only when style is STATIC. - The value can be true or false.
policy_rules	Array of PolicyRule objects	Specifies IPv4 policy rules, which are returned only when style is set to POLICY and ip_version of the VPN gateway is set to ipv4 .
ikepolicy	IkePolicy object	Specifies the IKE policy object.
ipsecpolicy	IpsecPolicy object	Specifies the IPsec policy object.
created_at	String	- Specifies the time when the VPN connection is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. The value must be the same as the enterprise project ID of the VPN gateway specified by vgw_id.
ha_role	String	- For a VPN gateway in active/standby mode, master indicates the active connection, and slave indicates the standby connection. For a VPN gateway in active-active mode, the value of ha_role can only be master. - The default value is master.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-111 PolicyRule

Parameter	Type	Description
source	String	Specifies a source CIDR block.

Parameter	Type	Description
destination	Array of String	Specifies a destination CIDR block. An example IPv4 CIDR block is 192.168.52.0/24. A maximum of 50 destination CIDR blocks can be returned for each policy rule.

Table 4-112 IkePolicy

Parameter	Type	Description
ike_version	String	- Specifies the IKE version. - The value can be v1 or v2.
phase1_negotiation_mode	String	- Specifies the negotiation mode. This parameter is available only when the IKE version is v1. - Value range: main: ensures high security during negotiation. aggressive: ensures fast negotiation and a high negotiation success rate.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, or group21.
authentication_method	String	- Specifies the authentication method used during IKE negotiation. - Value range: pre-share: pre-shared key
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.

Parameter	Type	Description
local_id_type	String	- Specifies the local ID type. - The value is ip.
local_id	String	Specifies the local ID. When local_id_type is set to ip , the local ID specified when the VPN connection is created or updated is returned. If no local ID is specified, the VPN gateway IP address corresponding to the VPN connection is returned.
peer_id_type	String	- Specifies the peer ID type. - The value is ip.
peer_id	String	Specifies the peer ID. When peer_id_type is set to ip , the peer ID specified when the VPN connection is created or updated is returned. If no peer ID is specified, the IP address of the customer gateway is returned.
dpd	Dpd object	Specifies the DPD object.

Table 4-113 Dpd

Parameter	Type	Description
timeout	Integer	- Specifies the interval for retransmitting DPD packets. - The value ranges from 2 to 60, in seconds.
interval	Integer	- Specifies the DPD idle timeout period. - The value ranges from 10 to 3600, in seconds.
msg	String	- Specifies the format of DPD packets. - Value range: seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash.

Table 4-114 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, group21, or disable.
transform_protocol	String	- Specifies the transfer protocol. - Value range: esp: encapsulating security payload protocol
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.
encapsulation_mode	String	- Specifies the packet encapsulation mode. - Value range: tunnel: encapsulates packets in tunnel mode.

Table 4-115 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (<code>_ . : = + - @</code>).

Parameter	Type	Description
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

– Example response

i. Response to the request for creating VPN connections in static routing mode in batches

```
{
  "vpn_connections": [
    {
      "id": "cf91c03c-9679-495f-a201-3622a1aec817",
      "name": "vpn-b8fa",
      "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
      "vgw_ip": "0d0f4af1-42b9-41eb-97b9-b4d41a0bf9c4",
      "style": "STATIC",
      "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
      "peer_subnets": [
        "192.168.2.0/24"
      ],
      "tunnel_local_address": "169.254.12.37/30",
      "tunnel_peer_address": "169.254.12.38/30",
      "enable_nqa": false,
      "policy_rules": [],
      "ikepolicy": {
        "ike_version": "v2",
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "dh_group": "group15",
        "authentication_method": "pre-share",
        "lifetime_seconds": 86400,
        "local_id_type": "ip",
        "local_id": "10.***.***.173",
        "peer_id_type": "ip",
        "peer_id": "2.***.***.2",
        "dpd": {
          "interval": 30,
          "timeout": 15,
          "msg": "seq-hash-notify"
        }
      },
      "ipsecpolicy": {
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "pfs": "group15",
        "transform_protocol": "esp",
        "lifetime_seconds": 3600,
        "encapsulation_mode": "tunnel"
      },
      "created_at": "2025-02-21T03:53:23.557Z",
      "updated_at": "2025-02-21T03:53:23.557Z",
      "enterprise_project_id": "0",
      "ha_role": "master",
      "tags": [],
      "policy_rules_v6": []
    },
    {
      "id": "64c09578-a23c-4d9d-9c64-56b2f9a74695",
      "name": "vpn-ec21",

```

```
"vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
"vgw_ip": "1fb97767-d780-4d8b-83bb-6f878f662005",
"style": "STATIC",
"cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
"peer_subnets": [
  "192.168.2.0/24"
],
"tunnel_local_address": "169.254.60.229/30",
"tunnel_peer_address": "169.254.60.230/30",
"enable_nqa": false,
"policy_rules": [],
"ikepolicy": {
  "ike_version": "v2",
  "authentication_algorithm": "sha2-256",
  "encryption_algorithm": "aes-128",
  "dh_group": "group15",
  "authentication_method": "pre-share",
  "lifetime_seconds": 86400,
  "local_id_type": "ip",
  "local_id": "215.***.***.55",
  "peer_id_type": "ip",
  "peer_id": "2.***.***.2",
  "dpd": {
    "interval": 30,
    "timeout": 15,
    "msg": "seq-hash-notify"
  }
},
"ipsecpolicy": {
  "authentication_algorithm": "sha2-256",
  "encryption_algorithm": "aes-128",
  "pfs": "group15",
  "transform_protocol": "esp",
  "lifetime_seconds": 3600,
  "encapsulation_mode": "tunnel"
},
"created_at": "2025-02-21T03:53:23.226Z",
"updated_at": "2025-02-21T03:53:23.226Z",
"enterprise_project_id": "0",
"ha_role": "master",
"tags": [],
"policy_rules_v6": []
}
],
"request_id": "3c53db019753c69323303c198af58a85"
}
```

- ii. Response to the request for creating VPN connections in policy-based mode in batches

```
{
  "vpn_connections": [
    {
      "id": "db06a7cb-e3b5-4c8c-b682-40ed54e8eb54",
      "name": "vpn-ed37",
      "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
      "vgw_ip": "1fb97767-d780-4d8b-83bb-6f878f662005",
      "style": "POLICY",
      "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
      "peer_subnets": [
        "192.168.2.0/24"
      ],
      "tunnel_local_address": "169.254.44.197/30",
      "tunnel_peer_address": "169.254.44.198/30",
      "policy_rules": [
        {
          "rule_index": 1,
          "source": "192.168.37.0/24",
          "destination": [
            "192.168.2.0/24"
          ]
        }
      ]
    }
  ]
}
```

```
    }  
  },  
  "ikepolicy": {  
    "ike_version": "v2",  
    "authentication_algorithm": "sha2-256",  
    "encryption_algorithm": "aes-128",  
    "dh_group": "group15",  
    "authentication_method": "pre-share",  
    "lifetime_seconds": 86400,  
    "local_id_type": "ip",  
    "local_id": "215.***.***.55",  
    "peer_id_type": "ip",  
    "peer_id": "2.***.***.2",  
    "dpd": {  
      "interval": 30,  
      "timeout": 15,  
      "msg": "seq-hash-notify"  
    }  
  },  
  "ipsecpolicy": {  
    "authentication_algorithm": "sha2-256",  
    "encryption_algorithm": "aes-128",  
    "pfs": "group15",  
    "transform_protocol": "esp",  
    "lifetime_seconds": 3600,  
    "encapsulation_mode": "tunnel"  
  },  
  "created_at": "2025-02-21T03:59:50.341Z",  
  "updated_at": "2025-02-21T03:59:50.341Z",  
  "enterprise_project_id": "0",  
  "ha_role": "master",  
  "tags": [],  
  "policy_rules_v6": []  
},  
{  
  "id": "9f5220fd-f674-420c-9df7-6b6420a3ae99",  
  "name": "vpn-d0c2",  
  "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",  
  "vgw_ip": "0d0f4af1-42b9-41eb-97b9-b4d41a0bf9c4",  
  "style": "POLICY",  
  "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",  
  "peer_subnets": [  
    "192.168.2.0/24"  
  ],  
  "tunnel_local_address": "169.254.192.61/30",  
  "tunnel_peer_address": "169.254.192.62/30",  
  "policy_rules": [  
    {  
      "rule_index": 1,  
      "source": "192.168.37.0/24",  
      "destination": [  
        "192.168.2.0/24"  
      ]  
    }  
  ],  
  "ikepolicy": {  
    "ike_version": "v2",  
    "authentication_algorithm": "sha2-256",  
    "encryption_algorithm": "aes-128",  
    "dh_group": "group15",  
    "authentication_method": "pre-share",  
    "lifetime_seconds": 86400,  
    "local_id_type": "ip",  
    "local_id": "10.***.***.173",  
    "peer_id_type": "ip",  
    "peer_id": "2.***.***.2",  
    "dpd": {  
      "interval": 30,  
      "timeout": 15,
```

```
        "msg": "seq-hash-notify"
      }
    },
    "ipsecpolicy": {
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "pfs": "group15",
      "transform_protocol": "esp",
      "lifetime_seconds": 3600,
      "encapsulation_mode": "tunnel"
    },
    "created_at": "2025-02-21T03:59:50.651Z",
    "updated_at": "2025-02-21T03:59:50.651Z",
    "enterprise_project_id": "0",
    "ha_role": "master",
    "tags": [],
    "policy_rules_v6": []
  }
},
"request_id": "81237dad5e1338b1818cd6582781b610"
}
```

iii. Response to the request for creating VPN connections in BGP routing mode in batches

```
{
  "vpn_connections": [
    {
      "id": "5ddf5d02-c746-4075-be4b-95e9213e1c3c",
      "name": "vpn-1655",
      "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
      "vgw_ip": "0d0f4af1-42b9-41eb-97b9-b4d41a0bf9c4",
      "style": "BGP",
      "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
      "peer_subnets": [
        "192.168.2.0/24"
      ],
      "tunnel_local_address": "169.254.56.225/30",
      "tunnel_peer_address": "169.254.56.226/30",
      "enable_hub": false,
      "policy_rules": [],
      "ikepolicy": {
        "ike_version": "v2",
        "authentication_algorithm": "sha2-512",
        "encryption_algorithm": "aes-256",
        "dh_group": "group16",
        "authentication_method": "pre-share",
        "lifetime_seconds": 172800,
        "local_id": "123****",
        "peer_id": "456****",
        "dpd": {
          "interval": 60,
          "timeout": 30,
          "msg": "seq-notify-hash"
        }
      },
      "ipsecpolicy": {
        "authentication_algorithm": "sha2-512",
        "encryption_algorithm": "aes-256",
        "pfs": "group16",
        "transform_protocol": "esp",
        "lifetime_seconds": 7200,
        "encapsulation_mode": "tunnel"
      },
      "created_at": "2025-02-21T06:50:25.238Z",
      "updated_at": "2025-02-21T06:50:25.238Z",
      "enterprise_project_id": "0",
      "ha_role": "master",
      "tags": [],
      "policy_rules_v6": []
    },
  ],
}
```

```
{
  "id": "bb3632dd-f517-4e94-96b7-977c70d28966",
  "name": "vpn-1341",
  "vgw_id": "8030f6d6-32a8-4d20-a7f8-50a7a826e2f8",
  "vgw_ip": "1fb97767-d780-4d8b-83bb-6f878f662005",
  "style": "BGP",
  "cgw_id": "12f3577a-cbd8-4602-b68c-ecbf792fcec5",
  "peer_subnets": [
    "192.168.2.0/24"
  ],
  "tunnel_local_address": "169.254.56.225/30",
  "tunnel_peer_address": "169.254.56.226/30",
  "enable_hub": false,
  "policy_rules": [],
  "ikepolicy": {
    "ike_version": "v2",
    "authentication_algorithm": "sha2-512",
    "encryption_algorithm": "aes-256",
    "dh_group": "group16",
    "authentication_method": "pre-share",
    "lifetime_seconds": 172800,
    "local_id": "123***",
    "peer_id": "456***",
    "dpd": {
      "interval": 60,
      "timeout": 30,
      "msg": "seq-notify-hash"
    }
  },
  "ipsecpolicy": {
    "authentication_algorithm": "sha2-512",
    "encryption_algorithm": "aes-256",
    "pfs": "group16",
    "transform_protocol": "esp",
    "lifetime_seconds": 7200,
    "encapsulation_mode": "tunnel"
  },
  "created_at": "2025-02-21T06:50:25.5Z",
  "updated_at": "2025-02-21T06:50:25.5Z",
  "enterprise_project_id": "0",
  "ha_role": "master",
  "tags": [],
  "policy_rules_v6": []
},
  "request_id": "938ea2bba48836a429c741bd6f7627a4"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.3.3 Querying a Specified VPN Connection

Function

This API is used to query a VPN connection with a specified connection ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn-connection/{vpn_connection_id}

Table 4-116 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_connection_id	String	Yes	Specifies a VPN connection ID.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}

Response

- Response parameters
Returned status code 200: successful operation

Table 4-117 Parameters in the response body

Parameter	Type	Description
vpn_connection	ResponseVpnConnection object	Specifies the VPN connection object.
request_id	String	Specifies a request ID.

Table 4-118 ResponseVpnConnection

Parameter	Type	Description
id	String	- Specifies a VPN connection ID. - The value is a UUID containing 36 characters.

Parameter	Type	Description
name	String	- Specifies the name of a VPN connection. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
status	String	- Specifies the status of the VPN connection. - Value range: ERROR: abnormal ACTIVE: normal DOWN: not connected PENDING_CREATE: creating PENDING_UPDATE: updating PENDING_DELETE: deleting FREEZED: frozen UNKNOWN: unknown
vgw_id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
vgw_ip	String	- Specifies an EIP ID or private IP address of the VPN gateway. - The value is a UUID containing 36 characters or an IPv4 address in dotted decimal notation (for example, 192.168.45.7).
style	String	- Specifies the connection mode. - Value range: POLICY: policy-based mode STATIC: static routing mode BGP: BGP routing mode
cgw_id	String	- Specifies a customer gateway ID. - The value is a UUID containing 36 characters.
peer_subnets	Array of String	Specifies an IPv4 customer subnet. This parameter is not returned when attachment_type of the VPN gateway is set to ER and style is set to BGP or POLICY .

Parameter	Type	Description
tunnel_local_address	String	Specifies the tunnel interface address configured on the VPN gateway in route-based mode. This parameter is valid only when style is STATIC or BGP .
tunnel_peer_address	String	Specifies the tunnel interface address configured on the customer gateway device in route-based mode. This parameter is valid only when style is STATIC or BGP .
enable_nqa	Boolean	- Specifies whether NQA is enabled. This parameter is returned only when style is STATIC. - The value is true or false.
enable_hub	Boolean	- Specifies whether branch interconnection is enabled. This parameter is returned only when style is BGP. - The value is true or false.
policy_rules	Array of PolicyRule objects	Specifies IPv4 policy rules, which are returned only when style is set to POLICY and ip_version of the VPN gateway is set to ipv4 .
ikepolicy	IkePolicy object	Specifies the IKE policy object.
ipsecpolicy	IpsecPolicy object	Specifies the IPsec policy object.
created_at	String	- Specifies the time when the VPN connection is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. The value must be the same as the enterprise project ID of the VPN gateway specified by vgw_id.

Parameter	Type	Description
connection_monitor_id	String	- Specifies the ID of a VPN connection monitor. This parameter is available only when a connection monitor is created for a VPN connection. - The value is a UUID containing 36 characters.
ha_role	String	- For a VPN gateway in active-standby mode, master indicates the active connection, and slave indicates the standby connection. For a VPN gateway in active-active mode, the value of ha_role can only be master. - The default value is master.
tags	Array of VpnResourceTag objects	Specifies a tag list.
bgp_peer	BgpPeer object	Specifies BGP peer information.

Table 4-119 PolicyRule

Parameter	Type	Description
source	String	Specifies a source CIDR block.
destination	Array of String	Specifies a destination CIDR block. An example IPv4 CIDR block is 192.168.52.0/24. A maximum of 50 destination CIDR blocks can be returned for each policy rule.

Table 4-120 IkePolicy

Parameter	Type	Description
ike_version	String	- Specifies the IKE version. - The value can be v1 or v2.

Parameter	Type	Description
phase1_negotiation_mode	String	- Specifies the negotiation mode. This parameter is available only when the IKE version is v1. - Value range: main: ensures high security during negotiation. aggressive: ensures fast negotiation and a high negotiation success rate.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, or group21.
authentication_method	String	- Specifies the authentication method used during IKE negotiation. - Value range: pre-share: pre-shared key
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.
local_id_type	String	- Specifies the local ID type. - Value range: - ip -
local_id	String	Specifies the local ID. When local_id_type is set to ip , the local ID specified when the VPN connection is created or updated is returned. If no local ID is specified, the VPN gateway IP address corresponding to the VPN connection is returned.

Parameter	Type	Description
peer_id_type	String	- Specifies the peer ID type. - The value is ip.
peer_id	String	Specifies the peer ID. When peer_id_type is set to ip , the peer ID specified when the VPN connection is created or updated is returned. If no peer ID is specified, the IP address of the customer gateway is returned.
dpd	Dpd object	Specifies the DPD object.

Table 4-121 Dpd

Parameter	Type	Description
timeout	Integer	- Specifies the interval for retransmitting DPD packets. - The value ranges from 2 to 60, in seconds.
interval	Integer	- Specifies the DPD idle timeout period. - The value ranges from 10 to 3600, in seconds.
msg	String	- Specifies the format of DPD packets. - Value range: seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash.

Table 4-122 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.

Parameter	Type	Description
pfs	String	- Specifies the DH key group used by PFS. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, group21, or disable.
transform_protocol	String	- Specifies the transfer protocol. - Value range: esp: encapsulating security payload protocol
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.
encapsulation_mode	String	- Specifies the packet encapsulation mode. - Value range: tunnel: encapsulates packets in tunnel mode.

Table 4-123 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

Table 4-124 BgpPeer

Parameter	Type	Description
peer_ip_addresses	String	Specifies the address of a BGP peer.

Parameter	Type	Description
peer_asn	Integer	Specifies the AS number of a BGP peer.
state	String	Specifies the status of a peer.
state_duration	String	Specifies the connection duration.
num_received_routes	Integer	Specifies the number of received routes.
num_message_received	Integer	Specifies the number of received messages.
num_message_sent	Integer	Specifies the number of sent messages.

- Example response

```
{
  "vpn_connection": {
    "id": "98c5af8a-demo-a8df-va86-ae2280a6f4c3",
    "name": "vpn-1655",
    "status": "DOWN",
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",
    "style": "POLICY",
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",
    "peer_subnets": ["192.168.0.0/24"],
    "tunnel_local_address": "169.254.56.225/30",
    "tunnel_peer_address": "169.254.56.226/30",
    "policy_rules": [{
      "rule_index": 1,
      "source": "10.0.0.0/24",
      "destination": [
        "192.168.0.0/24"
      ]
    }],
    "ikepolicy": {
      "ike_version": "v2",
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "dh_group": "group15",
      "authentication_method": "pre-share",
      "lifetime_seconds": 86400,
      "local_id_type": "ip",
      "local_id": "10.***.***.134",
      "peer_id_type": "ip",
      "peer_id": "88.***.***.164",
      "dpd": {
        "timeout": 15,
        "interval": 30,
        "msg": "seq-hash-notify"
      }
    },
    "ipsecpolicy": {
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "pfs": "group15",
      "transform_protocol": "esp",
      "lifetime_seconds": 3600,
      "encapsulation_mode": "tunnel"
    },
    "created_at": "2022-11-26T13:41:34.626Z",
    "updated_at": "2022-11-26T13:41:34.626Z",
    "enterprise_project_id": "0",
  }
}
```

```
    "ha_role": "master",
    "tags": [],
    "policy_rules_v6": [],
    "bgp_peer": {
      "peer_ip_address": "169.254.173.1",
      "peer_asn": 64516,
      "state": "established",
      "state_duration": "3d01h34m24s",
      "num_received_routes": 5,
      "num_message_received": 15541,
      "num_message_sent": 15516
    },
    "request_id": "f91082d4-6d49-479c-ad1d-4e552a9f5cae"
  }
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.3.4 Querying the VPN Connection List

Function

This API is used to query the VPN connection list.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn-connection

Table 4-125 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Table 4-126 Parameter in a query request

Parameter	Type	Mandatory	Description
vgw_ip	String	No	Specifies an EIP ID or private IP address of a VPN gateway.
vgw_id	String	No	Specifies a VPN gateway ID.
enterprise_project_id	Array	No	Specifies an enterprise project ID.

Parameter	Type	Mandatory	Description
limit	Integer	No	- Specifies the number of records returned on each page during pagination query. - The value ranges from 0 to 200. - The default value is 200.
marker	String	No	- Specifies the start flag for querying the current page. If this parameter is left blank, the first page is queried. The marker for querying the next page is the next_marker in the page_info object returned on the current page. - This parameter must be used together with limit.

Request

- Request parameters
None
- Example requests
 - Query all VPN connections.
GET https://{Endpoint}/v5/{project_id}/vpn-connection
 - Query VPN connections of a specified vgw_ip.
GET https://{Endpoint}/v5/{project_id}/vpn-connection?
vgw_ip={vgw_ip}&limit={limit}&marker={marker}
 - Query VPN connections of a specified VPN gateway instance.
GET https://{Endpoint}/v5/{project_id}/vpn-connection?
vgw_id={vgw_id}&limit={limit}&marker={marker}

Response

- Response parameters
Returned status code 200: successful operation

Table 4-127 Parameters in the response body

Parameter	Type	Description
vpn_connections	Array of ResponseVpnConnection objects	Specifies the VPN connection object.
page_info	PageInfo object	Specifies pagination information.

Parameter	Type	Description
request_id	String	Specifies a request ID.
total_count	Long	Specifies the total number of a tenant's connections.

Table 4-128 ResponseVpnConnection

Parameter	Type	Description
id	String	- Specifies a VPN connection ID. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a VPN connection. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
status	String	- Specifies the status of the VPN connection. - Value range: ERROR: abnormal ACTIVE: normal DOWN: not connected PENDING_CREATE: creating PENDING_UPDATE: updating PENDING_DELETE: deleting FREEZED: frozen UNKNOWN: unknown
vgw_id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
vgw_ip	String	- Specifies an EIP ID or private IP address of the VPN gateway. - The value is a UUID containing 36 characters or an IPv4 address in dotted decimal notation (for example, 192.168.45.7).

Parameter	Type	Description
style	String	- Specifies the connection mode. - Value range: POLICY: policy-based mode STATIC: static routing mode BGP: BGP routing mode
cgw_id	String	- Specifies a customer gateway ID. - The value is a UUID containing 36 characters.
peer_subnets	Array of String	Specifies an IPv4 customer subnet. This parameter is not returned when attachment_type of the VPN gateway is set to ER and style is set to BGP or POLICY .
tunnel_local_address	String	Specifies the tunnel interface address configured on the VPN gateway in route-based mode. This parameter is valid only when style is STATIC or BGP .
tunnel_peer_address	String	Specifies the tunnel interface address configured on the customer gateway device in route-based mode. This parameter is valid only when style is STATIC or BGP .
enable_nqa	Boolean	- Specifies whether NQA is enabled. This parameter is returned only when style is STATIC. - The value is true or false.
enable_hub	Boolean	- Specifies whether branch interconnection is enabled. This parameter is returned only when style is BGP. - The value is true or false.
policy_rules	Array of PolicyRule objects	Specifies IPv4 policy rules, which are returned only when style is set to POLICY and ip_version of the VPN gateway is set to ipv4 .
ikepolicy	IkePolicy object	Specifies the IKE policy object.
ipsecpolicy	IpssecPolicy object	Specifies the IPsec policy object.

Parameter	Type	Description
created_at	String	- Specifies the time when the VPN connection is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. The value must be the same as the enterprise project ID of the VPN gateway specified by vgw_id.
connection_monitor_id	String	- Specifies the ID of a VPN connection monitor. This parameter is available only when a connection monitor is created for a VPN connection. - The value is a UUID containing 36 characters.
ha_role	String	- For a VPN gateway in active-standby mode, master indicates the active connection, and slave indicates the standby connection. For a VPN gateway in active-active mode, the value of ha_role can only be master. - The default value is master.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-129 PolicyRule

Parameter	Type	Description
source	String	Specifies a source CIDR block.
destination	Array of String	Specifies a destination CIDR block. An example IPv4 CIDR block is 192.168.52.0/24. A maximum of 50 destination CIDR blocks can be returned for each policy rule.

Table 4-130 IkePolicy

Parameter	Type	Description
ike_version	String	- Specifies the IKE version. - The value can be v1 or v2.
phase1_negotiation_mode	String	- Specifies the negotiation mode. This parameter is available only when the IKE version is v1. - Value range: main: ensures high security during negotiation. aggressive: ensures fast negotiation and a high negotiation success rate.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, or group21.
authentication_method	String	- Specifies the authentication method used during IKE negotiation. - Value range: pre-share: pre-shared key
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.
local_id_type	String	- Specifies the local ID type. - The value is ip.

Parameter	Type	Description
local_id	String	Specifies the local ID. When local_id_type is set to ip , the local ID specified when the VPN connection is created or updated is returned. If no local ID is specified, the VPN gateway IP address corresponding to the VPN connection is returned.
peer_id_type	String	- Specifies the peer ID type. - The value is ip.
peer_id	String	Specifies the peer ID. When peer_id_type is set to ip , the peer ID specified when the VPN connection is created or updated is returned. If no peer ID is specified, the IP address of the customer gateway is returned.
dpd	Dpd object	Specifies the DPD object.

Table 4-131 Dpd

Parameter	Type	Description
timeout	Integer	- Specifies the interval for retransmitting DPD packets. - The value ranges from 2 to 60, in seconds.
interval	Integer	- Specifies the DPD idle timeout period. - The value ranges from 10 to 3600, in seconds.
msg	String	- Specifies the format of DPD packets. - Value range: seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash.

Table 4-132 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
pfs	String	- Specifies the DH key group used by PFS. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, group21, or disable.
transform_protocol	String	- Specifies the transfer protocol. - Value range: esp: encapsulating security payload protocol
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.
encapsulation_mode	String	- Specifies the packet encapsulation mode. - Value range: tunnel: encapsulates packets in tunnel mode.

Table 4-133 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (<code>_ . : = + - @</code>).

Parameter	Type	Description
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

Table 4-134 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	Integer	Specifies the number of resources in the list. If the value of current_count is less than the value of limit in the query request, the current page is the last page.

- Example responses
 - a. Response to the request for querying all VPN connections

```
{
  "vpn_connections": [{
    "id": "228a68f0-demo-a8df-va86-a9919a3ea3de",
    "name": "vpn-56ea",
    "status": "DOWN",
    "vgw_id": "ba90819b-demo-a8df-va86-3a01622856a5",
    "vgw_ip": "3ea3b006-demo-a8df-va86-ae180ae07885",
    "style": "STATIC",
    "cgw_id": "537d9c26-demo-a8df-va86-99364a410f00",
    "peer_subnets": [
      "192.168.1.0/24"
    ],
    "tunnel_local_address": "169.254.149.2/30",
    "tunnel_peer_address": "169.254.149.1/30",
    "enable_nqa": true,
    "ikepolicy": {
      "ike_version": "v2",
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "dh_group": "group15",
      "authentication_method": "pre-share",
      "lifetime_seconds": 86400,
      "local_id_type": "ip",
      "local_id": "10.1.1.216",
      "peer_id_type": "ip",
      "peer_id": "10.0.1.67",
      "dpd": {
        "timeout": 15,
        "interval": 30,
        "msg": "seq-hash-notify"
      }
    }
  ]
}
```

```
"ipsecpolicy": {
  "authentication_algorithm": "sha2-256",
  "encryption_algorithm": "aes-128",
  "pfs": "group15",
  "transform_protocol": "esp",
  "lifetime_seconds": 3600,
  "encapsulation_mode": "tunnel"
},
"created_at": "2022-12-11T13:59:59.633Z",
"updated_at": "2022-12-11T13:59:59.633Z",
"enterprise_project_id": "0"
},
{
  "id": "a4df33ca-demo-a8df-va86-410a7dd6973f",
  "name": "vpn-15ea",
  "status": "DOWN",
  "vgw_id": "02217fb1-demo-a8df-va86-806ea291a8f2",
  "vgw_ip": "f5acac2c-demo-a8df-va86-72b819a5f525",
  "style": "POLICY",
  "cgw_id": "10a4496f-demo-a8df-va86-7510f4b2af33",
  "tunnel_local_address": "169.254.77.169/30",
  "tunnel_peer_address": "169.254.77.170/30",
  "policy_rules": [{
    "source": "10.0.0.0/24",
    "destination": [
      "192.168.44.0/24"
    ]
  }],
  "ikepolicy": {
    "ike_version": "v2",
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "dh_group": "group15",
    "authentication_method": "pre-share",
    "lifetime_seconds": 3600,
    "local_id_type": "ip",
    "local_id": "88 ***.***.167",
    "peer_id_type": "ip",
    "peer_id": "10.***.***.21",
    "dpd": {
      "interval": 30,
      "timeout": 15,
      "msg": "seq-hash-notify"
    }
  },
  "ipsecpolicy": {
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "pfs": "group15",
    "transform_protocol": "esp",
    "lifetime_seconds": 3600,
    "encapsulation_mode": "tunnel"
  },
  "created_at": "2022-12-09T07:24:27.674Z",
  "updated_at": "2022-12-09T07:24:27.674Z",
  "enterprise_project_id": "0",
  "ha_role": "master"
}
},
"page_info": {
  "next_marker": "2022-12-09T07:24:27.674Z",
  "current_count": 2
},
"request_id": "1d94a4e8-fdc2-7bfd-943e-19bfa9b234ac",
"total_count": 2
}
```

- b. Response to the request for querying VPN connections with a specified vgw_ip

```
{
  "vpn_connections": [
    {
      "id": "8fa335dd-demo-a8df-va86-78bb55a8bb04",
      "name": "vpn-2acd",
      "status": "DOWN",
      "vgw_id": "02217fb1-demo-a8df-va86-806ea291a8f2",
      "vgw_ip": "f5acac2c-demo-a8df-va86-72b819a5f525",
      "style": "STATIC",
      "cgw_id": "eba04567-demo-a8df-va86-5b0352f89af0",
      "peer_subnets": [
        "192.168.44.0/24"
      ],
      "tunnel_local_address": "169.254.58.225/30",
      "tunnel_peer_address": "169.254.58.226/30",
      "enable_nqa": false,
      "ikepolicy": {
        "ike_version": "v2",
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "dh_group": "group15",
        "authentication_method": "pre-share",
        "lifetime_seconds": 3600,
        "local_id_type": "ip",
        "local_id": "88.***.***.167",
        "peer_id_type": "ip",
        "peer_id": "10.***.***.9",
        "dpd": {
          "timeout": 15,
          "interval": 30,
          "msg": "seq-hash-notify"
        }
      },
      "ipsecpolicy": {
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "pfs": "group15",
        "transform_protocol": "esp",
        "lifetime_seconds": 3600,
        "encapsulation_mode": "tunnel"
      },
      "created_at": "2022-12-11T14:24:25.115Z",
      "updated_at": "2022-12-11T14:24:25.115Z",
      "enterprise_project_id": "0"
    },
    {
      "id": "a4df33ca-demo-a8df-va86-410a7dd6973f",
      "name": "vpn-15ea",
      "status": "DOWN",
      "vgw_id": "02217fb1-demo-a8df-va86-806ea291a8f2",
      "vgw_ip": "f5acac2c-demo-a8df-va86-72b819a5f525",
      "style": "POLICY",
      "cgw_id": "10a4496f-demo-a8df-va86-7510f4b2af33",
      "tunnel_local_address": "169.254.77.169/30",
      "tunnel_peer_address": "169.254.77.170/30",
      "policy_rules": [
        {
          "source": "10.0.0.0/24",
          "destination": [
            "192.168.44.0/24"
          ]
        }
      ],
      "ikepolicy": {
        "ike_version": "v2",
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "dh_group": "group15",
        "authentication_method": "pre-share",
```

```
        "lifetime_seconds": 3600,
        "local_id_type": "ip",
        "local_id": "88.***.***.167",
        "peer_id_type": "ip",
        "peer_id": "10.***.***.21",
        "dpd": {
            "interval": 30,
            "timeout": 15,
            "msg": "seq-hash-notify"
        }
    },
    "ipsecpolicy": {
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "pfs": "group15",
        "transform_protocol": "esp",
        "lifetime_seconds": 3600,
        "encapsulation_mode": "tunnel"
    },
    "created_at": "2022-12-11T13:59:59.633Z",
    "updated_at": "2022-12-11T13:59:59.633Z",
    "enterprise_project_id": "0",
    "ha_role": "master"
}
],
"page_info": {
    "next_marker": "2022-12-11T13:59:59.633Z",
    "current_count": 2
},
"request_id": "1d94a4e8-fdc2-7bfd-943e-19bfa9b234ac",
"total_count": 12
}
```

- c. Response to the request for querying VPN connections of a specified VPN gateway instance

```
{
  "vpn_connections": [
    {
      "id": "8fa335dd-demo-a8df-va86-78bb55a8bb04",
      "name": "vpn-2acd",
      "status": "DOWN",
      "vgw_id": "02217fb1-demo-a8df-va86-806ea291a8f2",
      "vgw_ip": "f5acac2c-demo-a8df-va86-72b819a5f525",
      "style": "STATIC",
      "cgw_id": "eba04567-demo-a8df-va86-5b0352f89af0",
      "peer_subnets": [
        "192.168.44.0/24"
      ],
      "tunnel_local_address": "169.254.58.225/30",
      "tunnel_peer_address": "169.254.58.226/30",
      "enable_nqa": false,
      "ikepolicy": {
        "ike_version": "v2",
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "dh_group": "group15",
        "authentication_method": "pre-share",
        "lifetime_seconds": 3600,
        "local_id_type": "ip",
        "local_id": "88.***.***.167",
        "peer_id_type": "ip",
        "peer_id": "10.***.***.9",
        "dpd": {
          "timeout": 15,
          "interval": 30,
          "msg": "seq-hash-notify"
        }
      },
      "ipsecpolicy": {
        "authentication_algorithm": "sha2-256",

```

```
        "encryption_algorithm": "aes-128",
        "pfs": "group15",
        "transform_protocol": "esp",
        "lifetime_seconds": 3600,
        "encapsulation_mode": "tunnel"
    },
    "created_at": "2022-12-11T14:24:25.115Z",
    "updated_at": "2022-12-11T14:24:25.115Z",
    "enterprise_project_id": "0",
    "ha_role": "master"
},
{
    "id": "a4df33ca-demo-a8df-va86-410a7dd6973f",
    "name": "vpn-15ea",
    "status": "DOWN",
    "vgw_id": "02217fb1-demo-a8df-va86-806ea291a8f2",
    "vgw_ip": "f5acac2c-demo-a8df-va86-72b819a5f525",
    "style": "POLICY",
    "cgw_id": "10a4496f-demo-a8df-va86-7510f4b2af33",
    "tunnel_local_address": "169.254.77.169/30",
    "tunnel_peer_address": "169.254.77.170/30",
    "policy_rules": [
        {
            "source": "10.0.0.0/24",
            "destination": [
                "192.168.44.0/24"
            ]
        }
    ],
    "ikepolicy": {
        "ike_version": "v2",
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "dh_group": "group15",
        "authentication_method": "pre-share",
        "lifetime_seconds": 3600,
        "local_id_type": "ip",
        "local_id": "88.***.***.167",
        "peer_id_type": "ip",
        "peer_id": "10.***.***.21",
        "dpd": {
            "interval": 30,
            "timeout": 15,
            "msg": "seq-hash-notify"
        }
    },
    "ipsecpolicy": {
        "authentication_algorithm": "sha2-256",
        "encryption_algorithm": "aes-128",
        "pfs": "group15",
        "transform_protocol": "esp",
        "lifetime_seconds": 3600,
        "encapsulation_mode": "tunnel"
    },
    "created_at": "2022-12-11T13:59:59.633Z",
    "updated_at": "2022-12-11T13:59:59.633Z",
    "enterprise_project_id": "0",
    "ha_role": "master"
}
],
"page_info": {
    "next_marker": "2022-12-11T13:59:59.633Z",
    "current_count": 2
},
"request_id": "1d94a4e8-fdc2-7bfd-943e-19bfa9b234ac",
"total_count": 12
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.3.5 Updating a VPN Connection

Function

This API is used to update a VPN connection with a specified connection ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/vpn-connection/{vpn_connection_id}

Table 4-135 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_connection_id	String	Yes	Specifies a VPN connection ID.

Request

- Request parameters

Table 4-136 Request parameters

Parameter	Type	Mandatory	Description
vpn_connection	UpdateVpnConnectionRequestBodyContent object	Yes	Specifies the VPN connection object.

Table 4-137 UpdateVpnConnectionRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies the name of a VPN connection. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
cgw_id	String	No	- Specifies a customer gateway ID. - The value is a UUID containing 36 characters.
peer_subnets	Array of String	No	- Specifies an IPv4 customer subnet. - Constraints: - Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets. - A maximum of 50 customer subnets can be configured for each VPN connection.
tunnel_local_address	String	No	- Specifies the tunnel interface address configured on the VPN gateway in route-based mode, for example, 169.254.76.1/30. - Constraints: - The first 16 bits must be 169.254, and the value cannot be 169.254.195.xxx. - The mask length must be 30, and the address must be in the same CIDR block as the value of tunnel_peer_address. - The address needs to be a host address in a CIDR block.

Parameter	Type	Mandatory	Description
tunnel_peer_address	String	No	- Specifies the tunnel interface address configured on the customer gateway device in route-based mode, for example, 169.254.76.1/30. - Constraints: The first 16 bits must be 169.254, and the value cannot be 169.254.195.xxx. The mask length must be 30, and the address must be in the same CIDR block as the value of tunnel_local_address. The address needs to be a host address in a CIDR block.
enable_hub	Boolean	No	- Specifies whether branch interconnection is enabled. - The value can be true or false. - The default value is false. - Set this parameter only when style is set to BGP.
psk	String	No	- Specifies a pre-shared key. When the IKE version is v2 and only this parameter is modified, the modification does not take effect. - The value is a string of 8 to 128 characters, which must contain at least three types of the following: uppercase letters, lowercase letters, digits, and special characters (~!@#\$%^()-_+= { } , . / ;) .
policy_rules	Array of PolicyRule object	No	Specifies IPv4 policy rules. A maximum of five policy rules can be specified. This parameter is mandatory only when style is set to policy and ip_version of the VPN gateway is set to ipv4 .
ikepolicy	UpdateIkePolicy object	No	Specifies the IKE policy object.
ipsecpolicy	UpdateIpsecPolicy object	No	Specifies the IPsec policy object.

Table 4-138 PolicyRule

Parameter	Type	Mandatory	Description
source	String	No	- Specifies a source CIDR block. The IP protocol version (IPv4) of the CIDR block must be the same as that of the VPN gateway. - The value of source in each policy rule must be unique.
destination	Array of String	No	- Specifies a destination CIDR block. The IP protocol version (IPv4) of the CIDR block must be the same as that of the VPN gateway. An example IPv4 CIDR block is 192.168.52.0/24. - A maximum of 50 destination CIDR blocks can be configured in each policy rule.

Table 4-139 UpdateIkePolicy

Parameter	Type	Mandatory	Description
ike_version	String	No	- Specifies the IKE version. - Value range: v1 and v2 - Default value: v2
phase1_negotiation_mode	String	No	- Specifies the negotiation mode. - Value range: main: ensures high security during negotiation. aggressive: ensures fast negotiation and a high negotiation success rate. - This parameter takes effect only for IKEv1.

Parameter	Type	Mandatory	Description
authentication_algorithm	String	No	- Specifies an authentication algorithm. The modification of this field takes effect only after SAs in phase 1 are aged. - Value range: sha2-512, sha2-384, sha2-256, sha1, md5 Exercise caution when using sha1 and md5 as they have low security.
encryption_algorithm	String	No	- Specifies an encryption algorithm. The modification of this field takes effect only after SAs in phase 1 are aged. - Value range: aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, 3des Exercise caution when using 3des , aes-128 , aes-192 , and aes-256 as they have low security.
dh_group	String	No	- Specifies the DH group used for key exchange in phase 1. The modification of this field takes effect only after SAs in phase 1 are aged. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, or group21. Exercise caution when using group1 , group2 , group5 , or group14 as they have low security.
lifetime_seconds	Integer	No	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. The modification of this field takes effect only after SAs in phase 1 are aged. - The value ranges from 60 to 604800, in seconds.

Parameter	Type	Mandatory	Description
local_id_type	String	No	- Specifies the local ID type. - The value is ip.
local_id	String	No	- Specifies the local ID. - Constraints: When local_id_type is set to ip, this parameter is optional. If it is set, the value must be an IPv4 address.
peer_id_type	String	No	- Specifies the peer ID type. - The value is ip.
peer_id	String	No	- Specifies the peer ID. - Constraints: When local_id_type is set to ip, this parameter is optional. If it is set, the value must be an IPv4 address.
dpd	UpdateDpd object	No	Specifies the DPD object.

Table 4-140 UpdateDpd

Parameter	Type	Mandatory	Description
timeout	Integer	No	- Specifies the interval for retransmitting DPD packets. - The value ranges from 2 to 60, in seconds. The default value is 15.
interval	Integer	No	- Specifies the DPD idle timeout period. - The value ranges from 10 to 3600, in seconds. The default value is 30.

Parameter	Type	Mandatory	Description
msg	String	No	- Specifies the format of DPD packets. - Value range: seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash. The default value is seq-hash-notify.

Table 4-141 UpdatelpsecPolicy

Parameter	Type	Mandatory	Description
authentication_algorithm	String	No	- Specifies an authentication algorithm. Exercise caution when using SHA1 and MD5 as they have low security. The modification of this field takes effect only after SAs in phase 2 are aged. - Value range: sha2-512, sha2-384, sha2-256, sha1, md5
encryption_algorithm	String	No	- Specifies an encryption algorithm. Exercise caution when using 3des, aes-128, aes-192, and aes-256 as they have low security. The modification of this field takes effect only after SAs in phase 2 are aged. - Value range: aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, 3des

Parameter	Type	Mandatory	Description
pfs	String	No	- Specifies the DH key group used by PFS. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, group21, or disable. The default value is group15. Exercise caution when using group1, group2, group5, or group14 as they have low security.
transform_protocol	String	No	- Specifies the transfer protocol. - Value range: esp: encapsulating security payload protocol The default value is esp.
lifetime_seconds	Integer	No	- Specifies the lifetime of a tunnel established over an IPsec connection. The modification of this field takes effect only after SAs in phase 2 are aged. - The value ranges from 30 to 604800, in seconds. The default value is 3600.
encapsulation_mode	String	No	- Specifies the packet encapsulation mode. - Value range: tunnel: encapsulates packets in tunnel mode. The default value is tunnel.

- Example requests

- a. Update the customer subnet.

```
PUT https://{Endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}
```

```
{
  "vpn_connection": {
    "peer_subnets": [
      "192.168.1.0/24"
    ]
  }
}
```

- b. Update a policy rule.

```
PUT https://{Endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}
```

```
{
  "vpn_connection": {
    "policy_rules": [{

```

```
        "source": "10.0.0.0/24",
        "destination": [
            "192.168.1.0/24"
        ]
    }
}
```

c. Update the SA lifetime.

PUT https://{Endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}

```
{
  "vpn_connection": {
    "ikepolicy": {
      "lifetime_seconds": 3600
    },
    "ipsecpolicy": {
      "lifetime_seconds": 3600
    }
  }
}
```

d. Update the connection name.

PUT https://{Endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}

```
{
  "vpn_connection": {
    "name": "vpn_connection_name"
  }
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-142 Parameters in the response body

Parameter	Type	Description
vpn_connection	ResponseVpnConnection object	Specifies the VPN connection object.
request_id	String	Specifies a request ID.

Table 4-143 ResponseVpnConnection

Parameter	Type	Description
id	String	• Specifies a VPN connection ID. • The value is a UUID containing 36 characters.

Parameter	Type	Description
name	String	- Specifies the name of a VPN connection. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
vgw_id	String	- Specifies a VPN gateway ID. - The value is a UUID containing 36 characters.
vgw_ip	String	- Specifies an EIP ID or private IP address of the VPN gateway. - The value is a UUID containing 36 characters or an IPv4 address in dotted decimal notation (for example, 192.168.45.7).
style	String	- Specifies the connection mode. - Value range: POLICY: policy-based mode STATIC: static routing mode BGP: BGP routing mode
cgw_id	String	- Specifies a customer gateway ID. - The value is a UUID containing 36 characters.
peer_subnets	Array of String	Specifies an IPv4 customer subnet. This parameter is not returned when attachment_type of the VPN gateway is set to ER and style is set to BGP or POLICY .
tunnel_local_address	String	Specifies the tunnel interface address configured on the VPN gateway in route-based mode. This parameter is valid only when style is STATIC or BGP .
tunnel_peer_address	String	Specifies the tunnel interface address configured on the customer gateway device in route-based mode. This parameter is valid only when style is STATIC or BGP .
enable_nqa	Boolean	- Specifies whether NQA is enabled. This parameter is returned only when style is STATIC. - The value can be true or false.

Parameter	Type	Description
enable_hub	Boolean	- Specifies whether branch interconnection is enabled. This parameter is returned only when style is BGP. - The value can be true or false.
policy_rules	Array of PolicyRule objects	Specifies IPv4 policy rules, which are returned only when style is set to POLICY and ip_version of the VPN gateway is set to ipv4 .
ikepolicy	IkePolicy object	Specifies the IKE policy object.
ipsecpolicy	IpsecPolicy object	Specifies the IPsec policy object.
created_at	String	- Specifies the time when the VPN connection is created. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
enterprise_project_id	String	- Specifies an enterprise project ID. - The value is a UUID containing 36 characters. The value must be the same as the enterprise project ID of the VPN gateway specified by vgw_id.
connection_monitor_id	String	- Specifies the ID of a VPN connection monitor. This parameter is available only when a connection monitor is created for a VPN connection. - The value is a UUID containing 36 characters.
ha_role	String	- For a VPN gateway in active-standby mode, master indicates the active connection, and slave indicates the standby connection. For a VPN gateway in active-active mode, the value of ha_role can only be master. - The default value is master.
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-144 PolicyRule

Parameter	Type	Description
source	String	Specifies a source CIDR block.
destination	Array of String	Specifies a destination CIDR block. An example IPv4 CIDR block is 192.168.52.0/24. A maximum of 50 destination CIDR blocks can be returned for each policy rule.

Table 4-145 IkePolicy

Parameter	Type	Description
ike_version	String	- Specifies the IKE version. - The value can be v1 or v2.
phase1_negotiation_mode	String	- Specifies the negotiation mode. This parameter is available only when the IKE version is v1. - Value range: main: ensures high security during negotiation. aggressive: ensures fast negotiation and a high negotiation success rate.
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
dh_group	String	- Specifies the DH group used for key exchange in phase 1. - The value can be group1, group2, group5, group14, group15, group16, group19, group20, or group21.
authentication_method	String	- Specifies the authentication method used during IKE negotiation. - Value range: pre-share: pre-shared key

Parameter	Type	Description
lifetime_seconds	Integer	- Specifies the SA lifetime. When the lifetime expires, an IKE SA is automatically updated. - The value ranges from 60 to 604800, in seconds.
local_id_type	String	- Specifies the local ID type. - The value is ip.
local_id	String	Specifies the local ID. When local_id_type is set to ip , the local ID specified when the VPN connection is created or updated is returned. If no local ID is specified, the VPN gateway IP address corresponding to the VPN connection is returned.
peer_id_type	String	- Specifies the peer ID type. - The value can be ip or any.
peer_id	String	Specifies the peer ID. When peer_id_type is set to ip , the peer ID specified when the VPN connection is created or updated is returned. If no peer ID is specified, the IP address of the customer gateway is returned. When peer_id_type is set to any , this parameter is not returned.
dpd	Dpd object	Specifies the DPD object.

Table 4-146 Dpd

Parameter	Type	Description
timeout	Integer	- Specifies the interval for retransmitting DPD packets. - The value ranges from 2 to 60, in seconds.
interval	Integer	- Specifies the DPD idle timeout period. - The value ranges from 10 to 3600, in seconds.

Parameter	Type	Description
msg	String	- Specifies the format of DPD packets. - Value range: seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash.

Table 4-147 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	- Specifies an authentication algorithm. - The value can be sha2-512, sha2-384, sha2-256, sha1, or md5.
encryption_algorithm	String	- Specifies an encryption algorithm. - The value can be aes-256-gcm-16, aes-128-gcm-16, aes-256, aes-192, aes-128, or 3des.
pfs	String	Specifies the DH key group used by PFS. The value can be group1, group2, group5, group14, group15, group16, group19, group20, group21, or disable.
transform_protocol	String	- Specifies the transfer protocol. - Value range: esp: encapsulating security payload protocol
lifetime_seconds	Integer	- Specifies the lifetime of a tunnel established over an IPsec connection. - The value ranges from 30 to 604800, in seconds.
encapsulation_mode	String	- Specifies the packet encapsulation mode. - Value range: tunnel: encapsulates packets in tunnel mode.

Table 4-148 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example responses
 - a. Response to the request for updating a VPN connection

```
{
  "vpn_connection": {
    "id": "98c5af8a-demo-a8df-va86-ae2280a6f4c3",
    "name": "vpn-1655",
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",
    "style": "POLICY",
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",
    "peer_subnets": ["192.168.1.0/24"],
    "tunnel_local_address": "169.254.56.225/30",
    "tunnel_peer_address": "169.254.56.226/30",
    "policy_rules": [{
      "source": "10.0.0.0/24",
      "destination": [
        "192.168.1.0/24"
      ]
    }],
  },
  "ikepolicy": {
    "ike_version": "v2",
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "dh_group": "group15",
    "authentication_method": "pre-share",
    "lifetime_seconds": 86400,
    "local_id_type": "ip",
    "local_id": "10.***.***.134",
    "peer_id_type": "ip",
    "peer_id": "88.***.***.164",
    "dpd": {
      "timeout": 15,
      "interval": 30,
      "msg": "seq-hash-notify"
    }
  },
  "ipsecpolicy": {
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "pfs": "group15",
    "transform_protocol": "esp",
    "lifetime_seconds": 3600,
    "encapsulation_mode": "tunnel"
  },
}
```

```
"created_at": "2022-11-26T13:41:34.626Z",
"updated_at": "2022-11-26T13:41:34.626Z",
"enterprise_project_id": "0",
"ha_role": "master"
},
"request_id": "f91082d4-6d49-479c-ad1d-4e552a9f5cae"
}
```

b. Response returned when a frozen VPN connection fails to be updated

```
{
  "error_code": "VPN.0001",
  "error_msg": "invalid request: ILLEGAL not allowed update vpnConnection",
  "request_id": "8c833634-4560-7897-7740-a7462f5bcbd4"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.3.6 Deleting a VPN Connection

Function

This API is used to delete a VPN connection with a specified connection ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/vpn-connection/{vpn_connection_id}

Table 4-149 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_connection_id	String	Yes	Specifies a VPN connection ID.

Request

- Request parameters
None
- Example request
DELETE https://{Endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}

Response

- Response parameters
Returned status code 204: successful deletion
- Example response
Response returned when a frozen VPN connection fails to be deleted
DELETE https://{Endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}

```
{
  "error_code": "VPN.0001",
  "error_msg": "invalid request: ILLEGAL not allowed delete vpnConnection",
  "request_id": "76b771cb-3b2a-151a-5bed-fdf5df12ff82"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.3.7 Querying VPN Connection Logs

Function

This API is used to query logs of a VPN connection with a specified connection ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn-connection/{vpn_connection_id}/log

Table 4-150 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_connection_id	String	Yes	Specifies a VPN connection ID.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}/log

Response

- Response parameters
Returned status code 200: successful operation

Table 4-151 Parameters in the response body

Parameter	Type	Description
logs	Array of Log objects	Specifies the log object.
request_id	String	Specifies a request ID.

Table 4-152 Log

Parameter	Type	Description
time	Integer	• Specifies the timestamp.
raw_message	String	• Specifies log information.

- Example response

```
{
  "logs": [
    {
      "time": 1735024112,
      "raw_message": "2024-12-24T07:08:32.730275+00:00 host-xx-xx-xx-xx ipsec_ike[30085]:
[xx.xx.xx.xx] IPSec tunnel negotiation fails. (IfIndex=[207], PolicyName=[], SeqNum=[0],
PeerAddress=[xx.xx.xx.xx], PeerPort=[500], Reason=[version mismatch])"
    }
  ],
  "request_id": "f15d2c621593f2018c23eb1d49e3605e"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.4 VPN Connection Monitoring

4.1.4.1 Creating a VPN Connection Monitor

Function

This API is used to create a VPN connection monitor to perform health check between gateways. After a VPN connection monitor is created, the VPN gateway sends probe packets to the customer gateway to collect statistics about the round-trip delay and packet loss rate, thereby monitoring quality of VPN connections between the gateways.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/connection-monitors

Table 4-153 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Request

- Request parameters

Table 4-154 Request parameters

Parameter	Type	Mandatory	Description
connection_monitor	CreateConnectionMonitorRequestBodyContent object	Yes	Specifies the connection_monitor object.

Table 4-155 CreateConnectionMonitorRequestBodyContent

Parameter	Type	Mandatory	Description
vpn_connection_id	String	Yes	Specifies the ID of the VPN connection to be monitored. You can obtain VPN connection IDs by querying the VPN connection list .

- Example request
POST https://{Endpoint}/v5/{project_id}/connection-monitors

```
{
  "connection_monitor": {
    "vpn_connection_id": "cae286f2-demo-a8df-va86-e22416ca1220"
  }
}
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-156 Parameters in the response body

Parameter	Type	Description
connection_monitor	ConnectionMonitorInfo object	Specifies the connection_monitor object.
request_id	String	Specifies a request ID.

Table 4-157 ConnectionMonitorInfo

Parameter	Type	Description
id	String	- Specifies the ID of a VPN connection monitor. - The value is a UUID containing 36 characters.
vpn_connection_id	String	- Specifies the ID of the VPN connection to be monitored. - The value is a UUID containing 36 characters.
type	String	- Specifies the type of objects to be monitored. - The value can only be gateway.
source_ip	String	Specifies the source address to be monitored.
destination_ip	String	Specifies the destination address to be monitored.
proto_type	String	- Specifies the protocol used by NQA. - The value can only be icmp.

- Example response

```
{
  "connection_monitor":{
    "id":"76f64229-demo-a8df-va86-3907e2815b6d",
    "vpn_connection_id":"cae286f2-demo-a8df-va86-e22416ca1220",
    "type":"gateway",
    "source_ip":"88.***.***.60",
    "destination_ip":"88.***.***.32",
    "proto_type":"icmp"
  },
  "request_id": "bd37d16d-387c-41ab-a180-01b649f73590"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.4.2 Querying a VPN Connection Monitor

Function

This API is used to query a VPN connection monitor with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/connection-monitors/{connection_monitor_id}

Table 4-158 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
connection_monitor_id	String	Yes	Specifies the ID of a VPN connection monitor.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/connection-monitors/{connection_monitor_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-159 Parameters in the response body

Parameter	Type	Description
connection_monitor	ConnectionMonitorInfo object	Specifies the connection_monitor object.
request_id	String	Specifies a request ID.

Table 4-160 ConnectionMonitorInfo

Parameter	Type	Description
id	String	- Specifies the ID of a VPN connection monitor. - The value is a UUID containing 36 characters.
status	String	- Specifies the status of the VPN connection monitor. - Value range: ACTIVE: normal PENDING_CREATE: creating PENDING_DELETE: deleting
vpn_connection_id	String	- Specifies the ID of the VPN connection to be monitored. - The value is a UUID containing 36 characters.
type	String	- Specifies the type of objects to be monitored. - The value can only be gateway.
source_ip	String	Specifies the source address to be monitored.
destination_ip	String	Specifies the destination address to be monitored.
proto_type	String	- Specifies the protocol used by NQA. - The value can only be icmp.

- Example response

```
{
  "connection_monitor": {
    "id": "76f64229-demo-a8df-va86-3907e2815b6d",
    "status": "ACTIVE",
    "vpn_connection_id": "cae286f2-demo-a8df-va86-e22416ca1220",
    "type": "gateway",
    "source_ip": "88.***.***.60",
    "destination_ip": "88.***.***.32",
    "proto_type": "icmp"
  },
  "request_id": "6d212bc0-ecb1-457b-977b-5e815fce658d"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.4.3 Querying the List of VPN Connection Monitors

Function

This API is used to query the list of VPN connection monitors.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/connection-monitors

Table 4-161 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Table 4-162 Parameter in a query request

Parameter	Type	Mandatory	Description
vpn_connection_id	String	No	Specifies a VPN connection ID.
enterprise_project_id	Array	No	Specifies an enterprise project ID.

Request

- Request parameters
None
- Example requests
 - Query all VPN connection monitors.
GET https://{Endpoint}/v5/{project_id}/connection-monitors
 - Query VPN monitors based on a specified VPN connection ID.
GET https://{Endpoint}/v5/{project_id}/connection-monitors?
vpn_connection_id={vpn_connection_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-163 Parameters in the response body

Parameter	Type	Description
connection_monitors	Array of ConnectionMonitorInfo objects	Specifies the connection_monitor object.
request_id	String	Specifies a request ID.

Table 4-164 ConnectionMonitorInfo

Parameter	Type	Description
id	String	- Specifies the ID of a VPN connection monitor. - The value is a UUID containing 36 characters.
status	String	- Specifies the status of the VPN connection monitor. - Value range: ACTIVE: normal PENDING_CREATE: creating PENDING_DELETE: deleting
vpn_connection_id	String	- Specifies the ID of the VPN connection to be monitored. - The value is a UUID containing 36 characters.
type	String	- Specifies the type of objects to be monitored. - The value can only be gateway.
source_ip	String	Specifies the source address to be monitored.
destination_ip	String	Specifies the destination address to be monitored.
proto_type	String	- Specifies the protocol used by NQA. - The value can only be icmp.

- Example responses
 - a. Response to the request for querying all VPN connection monitors

```
{
  "connection_monitors": [
    {
      "id": "76f64229-demo-a8df-va86-3907e2815b6d",
      "status": "ACTIVE",
```

```
{
  "vpn_connection_id": "2342adf2-demo-a8df-va86-12aq511s0917",
  "type": "gateway",
  "source_ip": "88.***.***.60",
  "destination_ip": "88.***.***.32",
  "proto_type": "icmp"
},
{
  "id": "85t53318-demo-a8df-va86-zq9312525f6t",
  "status": "ACTIVE",
  "vpn_connection_id": "cae286f2-demo-a8df-va86-e22416ca1220",
  "type": "gateway",
  "source_ip": "89.***.***.21",
  "destination_ip": "88.***.***.12",
  "proto_type": "icmp"
}
],
"request_id": "531f8b2c-ec55-45d8-90a3-ed922f7d63c"
}
```

- b. Response to the request for querying monitors based on a specified VPN connection ID

```
{
  "connection_monitors": [
    {
      "id": "76f64229-demo-a8df-va86-3907e2815b6d",
      "status": "ACTIVE",
      "vpn_connection_id": "2342adf2-demo-a8df-va86-12aq511s0917",
      "type": "gateway",
      "source_ip": "88.***.***.60",
      "destination_ip": "88.***.***.32",
      "proto_type": "icmp"
    }
  ],
  "request_id": "05ab9b58-9b4c-4cee-8113-4b0f325f1dfc"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.1.4.4 Deleting a VPN Connection Monitor

Function

This API is used to delete a VPN connection monitor with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/connection-monitors/{connection_monitor_id}

Table 4-165 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
connection_monitor_id	String	Yes	Specifies the ID of a VPN connection monitor.

Request

- Request parameters
None
- Example request
DELETE https://{Endpoint}/v5/{project_id}/connection-monitors/{connection_monitor_id}

Response

- Response parameters
Returned status code 204: successful deletion
- Example response
None

Status Codes

For details, see [A.2 Status Codes](#).

4.2 P2C VPN APIs

4.2.1 P2C VPN Gateway

4.2.1.1 Querying a P2C VPN Gateway

Function

This API is used to query a P2C VPN gateway with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}

Table 4-166 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-167 Parameters in the response body

Parameter	Type	Description
p2c_vpn_gateway	p2c_vpn_gateway object	Specifies the VPN gateway object.
request_id	String	Specifies a request ID.

Table 4-168 p2c_vpn_gateway

Parameter	Type	Description
id	String	- Specifies the ID of a P2C VPN gateway. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a P2C VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).

Parameter	Type	Description
status	String	- Specifies the status of the P2C VPN gateway. - Value range: PENDING_CREATE: creating PENDING_UPDATE: updating PENDING_DELETE: deleting ACTIVE: normal FAULT: abnormal FROZEN: frozen
vpc_id	String	Specifies the ID of the VPC to which the P2C VPN gateway connects.
connect_subnet	String	Specifies the ID of the VPC subnet used by the P2C VPN gateway.
flavor	String	- Specifies the specification of the P2C VPN gateway. - Value range: Professional1
availability_zone_ids	Array of strings	Specifies the list of AZs.
eip	ResponseEipInfo object	Indicates information about the EIP bound to the gateway.
max_connection_number	Integer	- Specifies the maximum number of concurrent online client connections. - Value range: 1–500
current_connection_number	Integer	Specifies the number of current client connections.
enterprise_project_id	String	Specifies an enterprise project ID.
tags	Array of VpnResourceTag objects	Specifies a tag list.
order_id	String	Specifies an order ID.
admin_state_up	Boolean	- Specifies the frozen status. - Value range: true: not frozen false: frozen

Parameter	Type	Description
frozen_effect	Integer	- Specifies whether a frozen resource can be deleted. - Value range: 0: A resource is not frozen. 1: A resource can be deleted after being frozen. 2: A resource cannot be deleted after being frozen.
version	string	Specifies the gateway version.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
applied_at	String	- Specifies the time when the VPN gateway takes effect. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-169 ResponseEipInfo

Parameter	Type	Description
id	String	- Specifies an EIP ID. - The value is a UUID containing 36 characters.
ip_version	Integer	- Specifies the EIP version. - The value can only be 4, indicating IPv4 address.
ip_billing_info	String	- Specifies the EIP order information. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa
type	String	- Specifies the EIP type. - For the value range, see the type field in Table 7 in Assigning an EIP.

Parameter	Type	Description
ip_address	String	- Specifies an EIP, that is, a public IPv4 address. - The value is an IPv4 address, for example, 88.***.***.11.
charge_mode	String	- Specifies the billing mode of EIP bandwidth. - Value range: bandwidth: billed by bandwidth traffic: billed by traffic
bandwidth_id	String	- Specifies the bandwidth ID of an EIP. - The value is a UUID containing 36 characters.
bandwidth_size	Integer	- Specifies the bandwidth (Mbit/s) of an EIP. The maximum EIP bandwidth varies according to regions and depends on the EIP service. You can submit a service ticket to increase the maximum EIP bandwidth under your account. - The value ranges from 1 to 1000. For details, see the EIP documentation.
bandwidth_name	String	- Specifies the bandwidth name of an EIP. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
bandwidth_billing_info	String	- Specifies the EIP bandwidth order information. - The value is in the format of <i>order_id:product_id:region_id:project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa
share_type	String	- Specifies the bandwidth sharing type. - Value range: PER: dedicated bandwidth

Table 4-170 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters, which can contain letters, digits, spaces, and the following special characters: _ . : = + - @. However, the value cannot start or end with a space or start with _sys_.
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters, which can contain letters, digits, spaces, and the following special characters: _ . : / = + - @.

• Example response

```
{
  "p2c_vpn_gateway": {
    "id": "6d526e5f-a0c6-44b6-a785-000000000000",
    "name": "p2c-vpngw-0000",
    "status": "ACTIVE",
    "vpc_id": "05b9d7de-9acd-4a05-b497-1a3c75afaa0a",
    "connect_subnet": "1948ce22-ddc5-4fb6-87b8-dfcc9b176b51",
    "flavor": "Professional1",
    "availability_zone_ids": [
      "cn-south-1f",
      "cn-south-1e"
    ],
    "eip": {
      "id": "f0bac06a-88a7-4d37-8e2e-c37691ee4ba2",
      "ip_version": 4,
      "ip_billing_info": "CS*****JWT1O:OFFI*****5078:cn-south-1:47190474*****98781092d16c",
      "type": "5_youxuanbgp",
      "ip_address": "215.***.***.120",
      "charge_mode": "bandwidth",
      "bandwidth_id": "3456471c-9dac-40f6-8344-daca14fbd81e",
      "bandwidth_size": 20,
      "bandwidth_name": "p2c-vpngw-bandwidth-bd61",
      "bandwidth_billing_info": "CS*****JWT1O:OFFI*****5078:cn-south-1:47190474*****98781092d16c",
      "share_type": "PER"
    },
    "max_connection_number": 10,
    "current_connection_number": 0,
    "enterprise_project_id": "0",
    "tags": [],
    "order_id": "CS*****JWT1O",
    "admin_state_up": true,
    "frozen_effect": 0,
    "created_at": "2024-06-14T10:24:12.147Z",
    "updated_at": "2024-06-14T10:24:12.147Z"
  },
  "request_id": "2ddd2f6107a8164ce6f6268bd991e57c"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.1.2 Querying the P2C VPN Gateway List

Function

This API is used to query the P2C VPN gateway list.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways

Table 4-171 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Table 4-172 Parameter in a query request

Parameter	Type	Mandatory	Description
limit	Integer	No	Specifies the number of records returned on each page during pagination query.
marker	String	No	- Specifies the start flag for querying the current page. If this parameter is left blank, the first page is queried. The marker for querying the next page is the next_marker in the page_info object returned on the current page. - This parameter must be used together with limit.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways

Response

- Response parameters
Returned status code 200: successful query

Table 4-173 Parameters in the response body

Parameter	Type	Description
p2c_vpn_gateways	Array of p2c_vpn_gateway objects	Specifies the gateway information list.
total_count	Integer	Specifies the total number of gateways.
page_info	PageInfo object	Specifies the pagination query information.
request_id	string	Specifies a request ID.

Table 4-174 p2c_vpn_gateway

Parameter	Type	Description
id	String	- Specifies the ID of a P2C VPN gateway. - The value is a UUID containing 36 characters.
name	String	- Specifies the name of a P2C VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
status	String	- Specifies the status of the P2C VPN gateway. - Value range: PENDING_CREATE: creating PENDING_UPDATE: updating PENDING_DELETE: deleting ACTIVE: normal FAULT: abnormal FROZEN: frozen
vpc_id	String	Specifies the ID of the VPC to which the P2C VPN gateway connects.
connect_subnet	String	Specifies the ID of the VPC subnet used by the P2C VPN gateway.

Parameter	Type	Description
flavor	String	- Specifies the specification of the P2C VPN gateway. - Value range: Professional1
availability_zone_ids	Array of strings	Specifies the list of AZs.
eip	ResponseEipInfo object	Indicates information about the EIP bound to the gateway.
max_connection_number	Integer	- Specifies the maximum number of concurrent online client connections. - Value range: 1-500
current_connection_number	Integer	Specifies the number of current client connections.
enterprise_project_id	String	Specifies an enterprise project ID.
tags	Array of VpnResourceTag objects	Specifies a tag list.
order_id	String	Specifies an order ID.
admin_state_up	Boolean	- Specifies the frozen status. - Value range: true: not frozen false: frozen
frozen_effect	Integer	- Specifies whether a frozen resource can be deleted. - Value range: 0: A resource is not frozen. 1: A resource can be deleted after being frozen. 2: A resource cannot be deleted after being frozen.
version	string	Specifies the gateway version.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Parameter	Type	Description
applied_at	String	- Specifies the time when the VPN gateway takes effect. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-175 ResponseEipInfo

Parameter	Type	Description
id	String	- Specifies an EIP ID. - The value is a UUID containing 36 characters.
ip_version	Integer	- Specifies the EIP version. - The value can only be 4, indicating IPv4 address.
ip_billing_info	String	- Specifies the EIP order information. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa
type	String	- Specifies the EIP type. - For the value range, see the type field in Table 7 in Assigning an EIP.
ip_address	String	- Specifies an EIP, that is, a public IPv4 address. - The value is an IPv4 address, for example, 88.***.***.11.
charge_mode	String	- Specifies the billing mode of EIP bandwidth. - Value range: bandwidth: billed by bandwidth traffic: billed by traffic
bandwidth_id	String	- Specifies the bandwidth ID of an EIP. - The value is a UUID containing 36 characters.

Parameter	Type	Description
bandwidth_size	Integer	- Specifies the bandwidth (Mbit/s) of an EIP. The maximum EIP bandwidth varies according to regions and depends on the EIP service. You can submit a service ticket to increase the maximum EIP bandwidth under your account. - The value ranges from 1 to 1000. For details, see the EIP documentation.
bandwidth_name	String	- Specifies the bandwidth name of an EIP. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
bandwidth_billing_info	String	- Specifies the EIP bandwidth order information. - The value is in the format of <i>order_id.product_id.region_id.project_id</i>, for example: CS22*****LIBIV:00301-*****-0--0:br-iaas-odin1:0605768a*****c006c7e484aa
share_type	String	- Specifies the bandwidth type. - Value range: PER: dedicated bandwidth

Table 4-176 VpnResourceTag

Parameter	Type	Description
key	String	- Specifies a tag key. - The value is a string of 1 to 128 characters, which can contain letters, digits, spaces, and the following special characters: _ . : = + - @. However, the value cannot start or end with a space or start with _sys_.
value	String	- Specifies a tag value. - The value is a string of 0 to 255 characters, which can contain letters, digits, spaces, and the following special characters: _ . : / = + - @.

Table 4-177 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	Integer	Specifies the number of resources in the list.

- Example response

```
{
  "p2c_vpn_gateways": [
    {
      "id": "6d526e5f-a0c6-44b6-a785-7e0ef7c9eb76",
      "name": "p2c-vpngw-0001",
      "status": "ACTIVE",
      "vpc_id": "05b9d7de-9acd-4a05-b497-1a3c75afaa0a",
      "connect_subnet": "1948ce22-ddc5-4fb6-87b8-dfcc9b176b51",
      "flavor": "Professional1",
      "availability_zone_ids": [
        "cn-south-1f",
        "cn-south-1e"
      ],
      "eip": {
        "id": "f0bac06a-88a7-4d37-8e2e-c37691ee4ba2",
        "ip_version": 4,
        "ip_billing_info": "CS*****JWT1O:OFFI*****5078:cn-south-1:47190474*****98781092d16c",
        "type": "5_youxuanbgp",
        "ip_address": "215.***.***.120",
        "charge_mode": "bandwidth",
        "bandwidth_id": "3456471c-9dac-40f6-8344-daca14fbd81e",
        "bandwidth_size": 20,
        "bandwidth_name": "p2c-vpngw-bandwidth-bd61",
        "bandwidth_billing_info": "CS*****JWT1O:OFFI*****5078:cn-south-1:47190474*****98781092d16c",
        "share_type": "PER"
      },
      "max_connection_number": 10,
      "current_connection_number": 0,
      "enterprise_project_id": "0",
      "tags": [],
      "order_id": "CS2406141822JWT1O",
      "admin_state_up": true,
      "frozen_effect": 0,
      "created_at": "2024-06-14T10:24:12.147Z",
      "updated_at": "2024-06-14T10:24:12.147Z"
    },
    {
      "id": "10d176c7-aed8-4766-9180-a47e536c64d0",
      "name": "p2c-vpngw-0002",
      "status": "ACTIVE",
      "vpc_id": "01ffa178-9be5-4457-ba5b-874c01cfc872",
      "connect_subnet": "be0d53dd-55a1-4e73-9002-54297e1a4c43",
      "flavor": "Professional1",
      "availability_zone_ids": [
        "cn-south-1f",
        "cn-south-1e"
      ],
      "eip": {
        "id": "106a269c-c8c1-425e-9f92-f6abcb4dc7b1",
        "ip_version": 4,
```

```
{
  "type": "5_bgp",
  "ip_address": "10.83.51.162",
  "charge_mode": "bandwidth",
  "bandwidth_id": "beeababf-57aa-469e-8fc8-e6f01554711c",
  "bandwidth_size": 20,
  "bandwidth_name": "p2c-vpngw-bandwidth-4455",
  "share_type": "PER"
},
{
  "max_connection_number": 10,
  "current_connection_number": 0,
  "enterprise_project_id": "0",
  "tags": [],
  "order_id": "CS*****JWT1O",
  "admin_state_up": true,
  "frozen_effect": 0,
  "created_at": "2024-06-14T10:01:39.654Z",
  "updated_at": "2024-06-15T01:59:40.39Z"
}
],
"total_count": 2,
"page_info": {
  "current_count": 2
},
"request_id": "6a88ffb594cdb382ac2c321bc6cbbe13"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.1.3 Modifying a P2C VPN Gateway

Function

This API is used to modify a P2C VPN gateway with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}

Table 4-178 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.

Request

- Request parameters

Table 4-179 Request parameters

Parameter	Type	Mandatory	Description
p2c_vpn_gateway	UpdateP2cVgwRequestBodyContent object	Yes	Specifies the P2C VPN gateway object.

Table 4-180 UpdateP2cVgwRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies the name of a P2C VPN gateway. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
eip_id	String	No	- Specifies the ID of a valid EIP, which is the new EIP to be bound to a P2C VPN gateway. Before binding a new EIP, unbind the original EIP from the VPN gateway by referring to Updating an EIP. - The value is a UUID containing 36 characters.

- Example request

```
PUT https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}
```

```
{
  "p2c_vpn_gateway": {
    "name": "p2c-vpngw-0003",
    "eip_id": "d9d85143-e1e1-427a-9994-d8b8fd9ebe3f"
  }
}
```

Response

- Response parameters

Returned status code 200: successful operation

Table 4-181 Parameters in the response body

Parameter	Type	Description
p2c_vpn_gateway	ResponseP2cVgw object	Specifies the P2C VPN gateway object.
request_id	String	Specifies a request ID.

Table 4-182 ResponseP2cVgw

Parameter	Type	Description
id	String	- Specifies the ID of a P2C VPN gateway. - The value is a UUID containing 36 characters.

- Example response

```
{
  "p2c_vpn_gateway": {
    "id": "10d176c7-aed8-4766-9180-a47e536c64d0"
  },
  "request_id": "b19ba5a0be8f7b7f664b14596f8f35db"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.1.4 Querying the AZs of P2C VPN Gateways

Function

This API is used to query the AZs of P2C VPN gateways.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/availability-zones

Table 4-183 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Table 4-184 Parameter in a query request

Parameter	Type	Mandatory	Description
flavor	String	No	- Specifies the specification of the P2C VPN gateway. - Value range: Professional1

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/availability-zones?flavor=Professional1

Response

- Response parameters
Returned status code 200: successful operation

Table 4-185 Parameters in the response body

Parameter	Type	Description
availability_zones	Array of strings	Specifies the list of AZs.
request_id	String	Specifies a request ID.

- Example response

```
{
  "availability_zones": [
    "cn-south-1f",
    "cn-south-1e"
  ],
  "request_id": "c63d850876bcd11776cce57914"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.1.5 Querying the Connections of a P2C VPN Gateway

Function

This API is used to query the connections of a P2C VPN gateway with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections

Table 4-186 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.

Table 4-187 Parameter in a query request

Parameter	Type	Mandatory	Description
limit	Integer	No	Specifies the number of records returned on each page during pagination query.
offset	Integer	No	Specifies the offset for pagination query.

Request

- Request parameters
None
- Example requests

1. Query the connection list in non-pagination mode.

GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections

2. Query the connection list in pagination mode.

GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections?limit=10&offset=0

Response

- Response parameters
Returned status code 200: successful query

Table 4-188 Parameters in the response body

Parameter	Type	Description
connections	Array of Connection objects	Specifies connection information.
total_count	Long	Specifies the total number of connections.
request_id	String	Specifies a request ID.

Table 4-189 Connection

Parameter	Type	Description
connection_id	String	- Specifies a connection ID. - The value is a UUID containing 36 characters.
client_virtual_ip	String	Specifies the virtual IP address assigned to a client for establishing a connection.
client_ip	String	Specifies the public IP address that a client accesses.
client_username	String	Specifies a client username.
inbound_packets	Long	Specifies the number of inbound packets.
outbound_packets	Long	Specifies the number of outbound packets.
inbound_bytes	Long	Specifies the number of inbound bytes.
outbound_bytes	Long	Specifies the number of outbound bytes.
connection_established_time	String	- Specifies the time when a client connection is established. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Parameter	Type	Description
timestamp	String	- Specifies the timestamp in the statistics about traffic transmitted over the connection. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

- Example response

```
{
  "connections": [
    {
      "connection_id": "10293371-114e-4d2a-878e-c6a616d0ec0e",
      "client_virtual_ip": "36.***.***.149",
      "client_ip": "100.***.***.100",
      "client_user_name": "1111",
      "inbound_packets": 13,
      "outbound_packets": 24,
      "inbound_bytes": 4185,
      "outbound_bytes": 10480,
      "connection_established_time": "2024-06-17T02:58:27.213Z",
      "timestamp": "2024-06-17T02:58:48Z"
    },
    {
      "connection_id": "6ade9de6-b19e-4b87-874d-f4880be317c1",
      "client_virtual_ip": "36.***.***.145",
      "client_ip": "100.***.***.100",
      "client_user_name": "1111",
      "inbound_packets": 13,
      "outbound_packets": 38,
      "inbound_bytes": 4185,
      "outbound_bytes": 15804,
      "connection_established_time": "2024-06-17T02:58:12.413Z",
      "timestamp": "2024-06-17T02:58:48Z"
    }
  ],
  "total_count": 2,
  "request_id": "6844f73ab1dd713d369b88904a935bd6"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.1.6 Tearing Down a Connection of a P2C VPN Gateway

Function

This API is used to tear down a connection of a specified P2C VPN gateway based on the connection ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections/
{connection_id}/disconnect

Table 4-190 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.
connection_id	String	Yes	Specifies a connection ID of a P2C VPN gateway.

- Example request
POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections/{connection_id}/disconnect

Response

- Response parameters
Returned status code 200: successful operation

Table 4-191 Parameters in the response body

Parameter	Type	Description
request_id	String	Specifies a request ID.

- Example response

```
{
  "request_id": "c63d850876bcd9bdfbd11776cce57914"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2 Server

4.2.2.1 Creating a VPN Server

Function

This API is used to create a VPN server.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers

Table 4-192 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.

Table 4-193 Parameters in the request header

Parameter	Type	Mandatory	Description
X-Client-Token	String	No	- Specifies the ID of an idempotent request. - The value is a UUID containing 36 characters.

Request

- Request parameters

Table 4-194 Request parameters

Parameter	Type	Mandatory	Description
vpn_server	CreateServerRequest object	Yes	Specifies the to-be-created server object.

Table 4-195 CreateServerRequest

Parameter	Type	Mandatory	Description
tunnel_protocol	String	No	- Specifies a tunnel protocol. - Value range: SSL - The default value is SSL.
client_cidr	String	Yes	- Specifies a client CIDR block. A virtual IP address on this CIDR block will be assigned to a client for establishing a connection. - The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24. - Constraints: - The client CIDR block cannot conflict with the routes in the default route table of the VPC to which the gateway belongs. - The client CIDR block cannot conflict with any local CIDR block of the server. - The number of available IP addresses in the client CIDR block must be greater than four times the maximum number of gateway connections. - The client CIDR block cannot be 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, 240.0.0.0/4, or 169.254.0.0/16.

Parameter	Type	Mandatory	Description
local_subnets	Array of strings	Yes	- Specifies the list of local CIDR blocks. A local CIDR block is a destination CIDR block on the cloud to be accessed by client CIDR blocks through a VPN. - The value is in the format of dotted decimal notation/mask, for example, 10.10.1.0/24. - Constraints: - There must be at least one local CIDR block. By default, a maximum of 20 local CIDR blocks are supported. - The local CIDR block cannot be 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, or 240.0.0.0/4.
client_auth_type	String	No	- Specifies the client authentication mode. - Value range: CERT: certificate authentication LOCAL_PASSWORD: password authentication (local) - The default value is LOCAL_PASSWORD.
server_certificate	server_certificate object	No	Specifies a server certificate. This parameter is mandatory when SSL is used as the tunnel protocol. It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096.

Parameter	Type	Mandatory	Description
client_ca_certificates	Array of client_ca_certificate objects	No	- Specifies the list of client CA certificates, which are used to authenticate client certificates. - Constraints: - This parameter is mandatory when SSL is used as the tunnel protocol and the client authentication mode is certificate authentication. - When the client authentication mode is certificate authentication, you must upload at least one client CA certificate. A maximum of 10 client CA certificates can be uploaded.
ssl_options	ssl_options object	No	Specifies SSL options. This parameter is mandatory when SSL is used as the tunnel protocol.
dns_servers	Array of strings	No	- Specifies the DNS server list. A maximum of two DNS servers are supported. - The value is in dotted decimal notation, for example, 172.16.1.1.

Table 4-196 server_certificate

Parameter	Type	Mandatory	Description
id	String	Yes	Specifies a certificate ID, which is the ID of a certificate uploaded in the Cloud Certificate Manager (CCM).

Table 4-197 client_ca_certificate

Parameter	Type	Mandatory	Description
name	String	No	- Specifies a certificate name. If this parameter is left blank, the system automatically generates a certificate name. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
content	String	Yes	- Specifies the certificate content. It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. - Format: -----BEGIN CERTIFICATE----- ***** ***** -----END CERTIFICATE-----

Table 4-198 ssl_options

Parameter	Type	Mandatory	Description
protocol	String	No	- Specifies a protocol. - Value range: TCP - The default value is TCP.
port	Integer	No	- Specifies a port number. - Value range: 443 1194 - The default value is 443.
encryption_algorithm	String	No	- Specifies an encryption algorithm. - Value range: - AES-128-GCM - AES-256-GCM - The default value is AES-128-GCM.

Parameter	Type	Mandatory	Description
is_compressed	Boolean	No	- Specifies whether to compress data. - Value range: - true - false - The default value is false.

- Example requests

1. Create a VPN server in certificate authentication mode.

POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers

```
{
  "vpn_server": {
    "tunnel_protocol": "SSL",
    "client_cidr": "172.16.0.1/24",
    "local_subnets": [
      "10.16.0.0/24",
      "10.16.1.0/24"
    ],
    "client_auth_type": "CERT",
    "server_certificate": {
      "id": "scs*****3922"
    },
    "client_ca_certificates": [
      {
        "name": "client_ca_8sux3d",
        "content": "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----"
      }
    ],
    "ssl_options": {
      "protocol": "TCP",
      "port": 443,
      "encryption_algorithm": "AES-128-GCM",
      "is_compressed": false
    }
  }
}
```

2. Create a VPN server in password authentication mode.

```
{
  "vpn_server": {
    "tunnel_protocol": "SSL",
    "client_cidr": "172.16.0.1/24",
    "local_subnets": [
      "10.16.0.0/24",
      "10.16.1.0/24"
    ],
    "client_auth_type": "LOCAL_PASSWORD",
    "server_certificate": {
      "id": "scs1716171403922"
    },
    "ssl_options": {
      "protocol": "TCP",
      "port": 443,
      "encryption_algorithm": "AES-128-GCM",
      "is_compressed": false
    }
  }
}
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-199 Parameters in the response body

Parameter	Type	Description
vpn_server	vpn_server object	Specifies the VPN server object.
request_id	String	Specifies a request ID.

Table 4-200 vpn_server

Parameter	Type	Description
id	String	• Specifies the ID of a VPN server. • The value is a UUID containing 36 characters.

- Example response

```
{
  "vpn_server": {
    "id": "2407a20d-0bf7-4530-ba9a-7ffa0cedfa3b"
  },
  "request_id": "b19ba5a0be8f7b7f664b14596f8f35db"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.2 Querying a VPN Server Based on a Specified Gateway ID

Function

This API is used to query a VPN server based on a specified P2C VPN gateway ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers

Table 4-201 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers

Response

- Response parameters
Returned status code 200: successful query

Table 4-202 Parameters in the response body

Parameter	Type	Description
vpn_servers	Array of ShowServerResponse objects	Specifies server list information.
total_count	integer	Specifies the total number of records.
page_info	PageInfo	Specifies pagination query information.
request_id	String	Specifies a request ID.

Table 4-203 ShowServerResponse

Parameter	Type	Description
id	String	- Specifies the ID of a VPN server. - The value is a UUID containing 36 characters.

Parameter	Type	Description
p2c_vgw_id	String	- Specifies the ID of a P2C VPN gateway. - The value is a UUID containing 36 characters.
client_cidr	String	- Specifies a client CIDR block. A virtual IP address on this CIDR block will be assigned to a client for establishing a connection. - The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24.
local_subnets	Array of strings	- Specifies the list of local CIDR blocks. - The value is in the format of dotted decimal notation/mask, for example, 10.10.1.0/24.
client_auth_type	String	- Specifies the client authentication mode. - Value range: CERT: certificate authentication LOCAL_PASSWORD: password authentication (local)
tunnel_protocol	String	- Specifies a tunnel protocol. - Value range: SSL
server_certificate	server_certificate object	Specifies server certificate information.
client_ca_certificates	Array of QueryClientCaCertificateBody objects	Specifies the list of client CA certificates, which are used to authenticate client certificates.
ssl_options	ssl_options object	Specifies SSL options.
dns_servers	Array of strings	- Specifies the DNS server list. - The value is in dotted decimal notation, for example, 172.16.1.1.

Parameter	Type	Description
status	String	- Specifies the server status. - Value range: PENDING_CREATE: creating PENDING_UPDATE: updating ACTIVE: normal FAULT: abnormal FROZEN: frozen
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-204 server_certificate

Parameter	Type	Description
id	String	Specifies a certificate ID, which is the ID of a certificated uploaded in the CCM. This parameter is left empty if the certificate is deleted from the CCM.
name	String	Specifies a certificate name, which is the name of a certificated uploaded in the CCM.
issuer	String	- Specifies the issuer of a certificate. - The value is a string of 1 to 256 characters.
subject	String	- Specifies the subject of a certificate. - The value is a string of 1 to 256 characters.
serial_number	String	- Specifies the serial number of a certificate. - The value is a string of 1 to 64 characters.
expiration_time	String	- Specifies the expiration time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Parameter	Type	Description
signature_algorithm	String	- Specifies the signature algorithm of a certificate. - The value is a string of 1 to 64 characters.

Table 4-205 QueryClientCaCertificateBody

Parameter	Type	Description
id	String	- Specifies a certificate ID. - The value is a UUID containing 36 characters.
name	String	- Specifies a certificate name. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
issuer	String	- Specifies the issuer of a certificate. - The value is a string of 1 to 256 characters.
subject	String	- Specifies the subject of a certificate. - The value is a string of 1 to 256 characters.
serial_number	String	- Specifies the serial number of a CA certificate. - The value is a string of 1 to 64 characters.
expiration_time	String	- Specifies the expiration time of a certificate. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
signature_algorithm	String	- Specifies the signature algorithm of a certificate. - The value is a string of 1 to 64 characters.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Parameter	Type	Description
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-206 ssl_options

Parameter	Type	Description
protocol	string	- Specifies a protocol. - Value range: TCP
port	integer	- Specifies a port number. - Value range: 443 1194
encryption_algorithm	string	- Specifies an encryption algorithm. - Value range: - AES-128-GCM - AES-256-GCM
authentication_algorithm	string	- Specifies an authentication algorithm. - Value range: - SHA256 - SHA384
is_compressed	boolean	- Specifies whether to compress data. By default, data is not compressed. - Value range: - true - false

Table 4-207 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	integer	Specifies the number of resources in the current list.

- Example response

```
{
  "vpn_servers": [
    {
      "id": "2407a20d-0bf7-4530-ba9a-7ffa0cedfa3b",
      "p2c_vgw_id": "3b5b64e4-2927-4062-acf6-05b0b842bbfe",
      "client_cidr": "1.1.0.0/16",
      "local_subnets": [
        "192.168.12.0/24",
        "192.168.1.0/24"
      ],
      "client_auth_type": "LOCAL_PASSWORD",
      "tunnel_protocol": "SSL",
      "server_certificate": {
        "id": "scs1716171403922",
        "name": "lsh-newcert",
        "issuer": "C=CN,ST=beijing,L=haidian,O=lesaas,OU=root,CN=www.***.com",
        "subject": "C=CN,ST=beijing,L=haidian,O=server,OU=server,CN=www.***.com",
        "serial_number": "310325804134830162280305057622726926320418980636",
        "expiration_time": "2024-06-19T02:15:26Z",
        "signature_algorithm": "SHA256WITHRSA"
      },
      "client_ca_certificates": [],
      "ssl_options": {
        "protocol": "TCP",
        "port": 443,
        "encryption_algorithm": "AES-128-GCM",
        "authentication_algorithm": "SHA256",
        "is_compressed": false
      },
      "status": "ACTIVE",
      "created_at": "2024-06-14T01:14:56.802Z",
      "updated_at": "2024-06-14T08:53:22.855Z"
    }
  ],
  "request_id": "3378c265585ffb8aac68ec39a2db67a1"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.3 Modifying a VPN Server

Function

This API is used to modify a VPN server with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}

Table 4-208 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Request

- Request parameters

Table 4-209 Request parameters

Parameter	Type	Mandatory	Description
vpn_server	UpdateServerRequest object	Yes	Specifies the to-be-updated VPN server object.

Table 4-210 UpdateServerRequest

Parameter	Type	Mandatory	Description
client_cidr	String	No	- Specifies a client CIDR block. A virtual IP address on this CIDR block will be assigned to a client for establishing a connection. - The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24. - Constraints: - The client CIDR block cannot conflict with the routes in the default route table of the VPC to which the gateway belongs. - The client CIDR block cannot conflict with any local CIDR block of the server. - The number of available IP addresses in the client CIDR block must be greater than four times the maximum number of gateway connections. - The client CIDR block cannot be 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, 240.0.0.0/4, or 169.254.0.0/16.
local_subnets	Array of strings	No	- Specifies the list of local CIDR blocks. A local CIDR block is a destination CIDR block on the cloud to be accessed by client CIDR blocks through a VPN. - The value is in the format of dotted decimal notation/mask, for example, 10.10.1.0/24. - Constraints: - There must be at least one local CIDR block. By default, a maximum of 20 local CIDR blocks are supported. - The local CIDR block cannot be 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, or 240.0.0.0/4.

Parameter	Type	Mandatory	Description
server_certificate	server_certificate object	No	Specifies a server certificate. It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096.
ssl_options	ssl_options object	No	Specifies SSL options.
client_auth_type	String	No	- Specifies the client authentication mode. - Value range: CERT: certificate authentication LOCAL_PASSWORD: password authentication (local)
dns_servers	Array of strings	No	- Specifies the DNS server list. A maximum of two DNS servers are supported. - The value is in dotted decimal notation, for example, 172.16.1.1.

Table 4-211 server_certificate

Parameter	Type	Mandatory	Description
id	String	Yes	Specifies a certificate ID, which is the ID of a certificated uploaded in the CCM.

Table 4-212 ssl_options

Parameter	Type	Mandatory	Description
protocol	String	No	- Specifies a protocol. - Value range: TCP - The default value is TCP.

Parameter	Type	Mandatory	Description
port	Integer	No	- Specifies a port number. - Value range: 443 1194 - The default value is 443.
encryption_algorithm	String	No	- Specifies an encryption algorithm. - Value range: - AES-128-GCM - AES-256-GCM - The default value is AES-128-GCM.

- Example request

PUT https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}

```
{
  "vpn_server": {
    "client_cidr": "192.168.10.0/24",
    "local_subnets": [
      "172.16.0.0/24",
      "172.16.1.0/24"
    ],
    "server_certificate": {
      "id": "scs1717051012106"
    },
    "ssl_options": {
      "protocol": "TCP",
      "port": 443,
      "encryption_algorithm": "AES-128-GCM"
    },
    "client_auth_type": "CERT"
  }
}
```

Response

- Response parameters

Returned status code 200: successful operation

Table 4-213 Parameters in the response body

Parameter	Type	Description
request_id	string	Specifies a request ID.

- Example response

```
{
  "request_id": "c63d850876bcd9bdfbd11776cce57914"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.4 Exporting the Client Configuration Corresponding to a VPN Server

Function

This API is used to export client configuration information based on a specified VPN server ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-config/export

Table 4-214 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Request

- Request parameters

Table 4-215 Request parameters

Parameter	Type	Mandatory	Description
os_type	String	No	- Specifies the OS type. - Value range: Windows Linux MacOS Android iOS - The default value is Windows.

- **Example request**
POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-config/export

```
{
  "os_type": "Windows"
}
```

Response

- **Response parameters**
Returned status code 200: successful query

Table 4-216 Parameters in the response body

Parameter	Type	Description
client_config	string	Specifies client configuration.

- **Example response**

```
{
  "client_config": "client\\ndev tun\\nproto tcp\\nremote 215.xx.xx.99 443\\nresolv-retry infinite\\nnobind
\\npersist-key\\npersist-tun\\nremote-cert-tls server\\ndata-ciphers AES-128-GCM\\nauth SHA256\\nverb
3\\nauth-user-pass\\n<ca>\\n-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----\\n</ca>\\n\\n
\\nreneg-sec 0\\n# Add a comment character (#) in front of disable-dco when OpenVPN 2.5 or earlier
is used.\\ndisable-dco\\n"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.5 Querying All VPN Servers of a Tenant

Function

This API is used to query all VPN servers of a tenant.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn-servers

Table 4-217 Parameter description

Parameter	Type	Manda tory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Table 4-218 Parameter in a query request

Parameter	Type	Mandatory	Description
limit	Integer	No	Specifies the number of records returned on each page during pagination query.
marker	String	No	- Specifies the start flag for querying the current page. If this parameter is left blank, the first page is queried. The marker for querying the next page is the next_marker in the page_info object returned on the current page. - This parameter must be used together with limit.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/vpn-servers

Response

- Response parameters
Returned status code 200: successful query

Table 4-219 Parameters in the response body

Parameter	Type	Description
vpn_servers	Array of ShowServerResponse objects	Specifies VPN server information.
total_count	Integer	Specifies the total number of VPN servers under the current tenant.
page_info	PageInfo object	Specifies pagination query information.
request_id	String	Specifies a request ID.

Table 4-220 ShowServerResponse

Parameter	Type	Description
id	String	- Specifies the ID of a VPN server. - The value is a UUID containing 36 characters.
p2c_vgw_id	String	- Specifies the ID of a P2C VPN gateway. - The value is a UUID containing 36 characters.
client_cidr	String	- Specifies a client CIDR block. A virtual IP address on this CIDR block will be assigned to a client for establishing a connection. - The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24.
local_subnets	Array of strings	- Specifies the list of local CIDR blocks. - The value is in the format of dotted decimal notation/mask, for example, 10.10.1.0/24.
client_auth_type	String	- Specifies the client authentication mode. - Value range: CERT: certificate authentication LOCAL_PASSWORD: password authentication (local)
tunnel_protocol	String	- Specifies a tunnel protocol. - Value range: SSL
server_certificate	server_certificate object	Specifies server certificate information.
client_ca_certificates	Array of QueryClientCaCertificateBody objects	Specifies the list of client CA certificates, which are used to authenticate client certificates.
ssl_options	ssl_options object	Specifies SSL options.
dns_servers	Array of strings	- Specifies the DNS server list. - The value is in dotted decimal notation, for example, 172.16.1.1.

Parameter	Type	Description
status	String	- Specifies the server status. - Value range: PENDING_CREATE: creating PENDING_UPDATE: updating ACTIVE: normal FAULT: abnormal FROZEN: frozen
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-221 server_certificate

Parameter	Type	Description
id	String	Specifies a certificate ID, which is the ID of a certificated uploaded in the CCM. This parameter is left empty if the certificate is deleted from the CCM.
name	String	Specifies a certificate name, which is the name of a certificated uploaded in the CCM.
issuer	String	- Specifies the issuer of a certificate. - The value is a string of 1 to 256 characters.
subject	String	- Specifies the subject of a certificate. - The value is a string of 1 to 256 characters.
serial_number	String	- Specifies the serial number of a certificate. - The value is a string of 1 to 64 characters.
expiration_time	String	- Specifies the expiration time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Parameter	Type	Description
signature_algorithm	String	- Specifies the signature algorithm of a certificate. - The value is a string of 1 to 64 characters.

Table 4-222 QueryClientCaCertificateBody

Parameter	Type	Description
id	String	- Specifies a certificate ID. - The value is a UUID containing 36 characters.
name	String	- Specifies a certificate name. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
issuer	String	- Specifies the issuer of a certificate. - The value is a string of 1 to 256 characters.
subject	String	- Specifies the subject of a certificate. - The value is a string of 1 to 256 characters.
serial_number	String	- Specifies the serial number of a CA certificate. - The value is a string of 1 to 64 characters.
expiration_time	String	- Specifies the expiration time of a certificate. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
signature_algorithm	String	- Specifies the signature algorithm of a certificate. - The value is a string of 1 to 64 characters.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Parameter	Type	Description
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-223 ssl_options

Parameter	Type	Description
protocol	string	- Specifies a protocol. - Value range: TCP
port	integer	- Specifies a port number. - Value range: 443 1194
encryption_algorithm	string	- Specifies an encryption algorithm. - Value range: - AES-128-GCM - AES-256-GCM
authentication_algorithm	string	- Specifies an authentication algorithm. - Value range: - SHA256 - SHA384
is_compressed	boolean	- Specifies whether to compress data. By default, data is not compressed. - Value range: - true - false

Table 4-224 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	Integer	Specifies the number of resources in the list.

– Example response

```
{
  "vpn_servers": [
    {
      "id": "3f7e48ca-cd3c-4ce2-a277-674382ce44ea",
      "p2c_vgw_id": "10d176c7-aed8-4766-9180-a47e536c64d0",
      "client_cidr": "173.16.1.0/24",
      "local_subnets": [
        "172.16.0.0/24",
        "172.16.1.0/24"
      ],
      "client_auth_type": "CERT",
      "tunnel_protocol": "SSL",
      "server_certificate": {
        "id": "scs1698803781642",
        "name": "p2cvpn_test",
        "issuer": "CN=p2cvpn.test",
        "subject": "CN=p2cvpn.server",
        "serial_number": "109258411809374886820602321558250159914",
        "expiration_time": "2026-01-22T06:26:18Z",
        "signature_algorithm": "SHA256WITHRSA"
      },
      "client_ca_certificates": [
        {
          "id": "2f291995-9582-4ce8-a7f4-e1b7742e6e0c",
          "name": "client_ca_sdk_test_1",
          "issuer": "CN=p2cvpn.test",
          "subject": "CN=p2cvpn.test",
          "serial_number": "218730615113252363388323617489459159151767515623",
          "expiration_time": "2033-10-17T06:21:25Z",
          "signature_algorithm": "SHA256WITHRSA",
          "created_at": "2024-06-15T01:59:46.612Z",
          "updated_at": "2024-06-15T01:59:46.612Z"
        }
      ],
      "ssl_options": {
        "protocol": "TCP",
        "port": 443,
        "encryption_algorithm": "AES-128-GCM",
        "authentication_algorithm": "SHA256",
        "is_compressed": false
      },
      "status": "ACTIVE",
      "created_at": "2024-06-15T01:59:46.612Z",
      "updated_at": "2024-06-15T02:01:16.606Z"
    },
    {
      "id": "3840e9ea-84be-4ff9-ad26-817829ba16ed",
      "p2c_vgw_id": "30dfb9cd-eeb0-4937-a7a5-4bc08184090b",
      "client_cidr": "173.17.0.0/24",
      "local_subnets": [
        "172.16.0.0/24",
        "172.16.1.0/24"
      ],
      "client_auth_type": "LOCAL_PASSWORD",
      "tunnel_protocol": "SSL",
      "server_certificate": {
        "id": "scs1698803781642",
        "name": "p2cvpn_test",
        "issuer": "CN=p2cvpn.test",
        "subject": "CN=p2cvpn.server",
        "serial_number": "109258411809374886820602321558250159914",
        "expiration_time": "2026-01-22T06:26:18Z",
        "signature_algorithm": "SHA256WITHRSA"
      },
      "client_ca_certificates": [],
      "ssl_options": {
        "protocol": "TCP",
        "port": 443,
```

```
        "encryption_algorithm": "AES-128-GCM",
        "authentication_algorithm": "SHA256",
        "is_compressed": false
      },
      "status": "ACTIVE",
      "created_at": "2024-06-15T02:01:19.87Z",
      "updated_at": "2024-06-15T02:01:19.87Z"
    }
  ],
  "total_count": 2,
  "page_info": {
    "current_count": 2
  },
  "request_id": "2b16014544fff455b50ef3f1e62bbe35"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.6 Verifying a Client CA Certificate

Function

This API is used to verify the validity of a client CA certificate.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/client-ca-certificates/check

Table 4-225 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Request

Request parameters

Table 4-226 Request parameters

Parameter	Type	Mandatory	Description
client_ca_certificate	client_ca_certificate object	Yes	Specifies client CA certificate information.

Table 4-227 client_ca_certificate

Parameter	Type	Mandatory	Description
name	String	No	- Specifies a certificate name. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
content	String	Yes	- Specifies the certificate content. - Format: -----BEGIN CERTIFICATE----- ***** ***** -----END CERTIFICATE-----

- Example request
POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/client-ca-certificates/check

```
{
  "client_ca_certificate": {
    "name": "client_ca_8sux3d",
    "content": "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----"
  }
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-228 Parameters in the response body

Parameter	Type	Description
name	String	- Specifies a certificate name. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
issuer	String	- Specifies the issuer of a certificate. - The value is a string of 1 to 256 characters.
subject	String	- Specifies the subject of a certificate. - The value is a string of 1 to 256 characters.
serial_number	String	- Specifies the serial number of a CA certificate. - The value is a string of 1 to 64 characters.
expiration_time	String	- Specifies the expiration time of a certificate. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
signature_algorithm	String	- Specifies the signature algorithm of a certificate. - The value is a string of 1 to 64 characters.

- Example response

Response returned when verification succeeds:

```
{
  "name": "client_ca_8sux3d",
  "issuer": "CN=xxx",
  "subject": "CN=xxx",
  "serial_number": "621079609299744022526309164429940520767604766768",
  "expiration_time": "2033-08-05T11:52:34Z",
  "signature_algorithm": "SHA256WITHRSA"
}
```

Response returned when verification fails:

```
{
  "error_code": "VPN.0072",
  "error_msg": "Certificate client_ca_8sux3d has expired.",
  "request_id": "b012532f51675c0ffdcfb2868669bd4e"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.7 Uploading a Client CA Certificate

Function

This API is used to upload a client CA certificate.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates

Table 4-229 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Table 4-230 Parameters in the request header

Parameter	Type	Mandatory	Description
X-Client-Token	String	No	- Specifies the ID of an idempotent request. - The value is a UUID containing 36 characters.

Request

- Request parameters

Table 4-231 Request parameters

Parameter	Type	Mandatory	Description
client_ca_certificate	client_ca_certificate object	Yes	Specifies client CA certificate information.

Table 4-232 client_ca_certificate

Parameter	Type	Mandatory	Description
name	String	No	- Specifies a certificate name. If this parameter is left blank, the system automatically generates a certificate name. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
content	String	Yes	- Specifies the certificate content. It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. - Format: -----BEGIN CERTIFICATE----- ***** ***** -----END CERTIFICATE-----

- Example request
POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates

```
{
  "client_ca_certificate": {
    "name": "client_ca_8sux3d",
    "content": "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----"
  }
}
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-233 Parameters in the response body

Parameter	Type	Description
client_ca_certificate	client_ca_certificate object	Specifies the client CA certificate object.
request_id	String	Specifies a request ID.

Table 4-234 client_ca_certificate

Parameter	Type	Description
id	String	- Specifies the ID of a client CA certificate. - The value is a UUID containing 36 characters.

– Example response

```
{
  "client_ca_certificate": {
    "id": "4e3a364f-1213-4a37-917e-d494aeada34e"
  },
  "request_id": "4114fdd9ca33e22936ece75b97d7a363"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.8 Querying a Client CA Certificate

Function

This API is used to query a client CA certificate with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}

Table 4-235 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
client_ca_certificate_id	String	Yes	Specifies the ID of a client CA certificate.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-236 Parameters in the response body

Parameter	Type	Description
client_ca_certificate	QueryClientCaCertificateBody object	Specifies the client CA certificate object.
request_id	string	Specifies a request ID.

Table 4-237 QueryClientCaCertificateBody

Parameter	Type	Description
id	String	• Specifies a certificate ID. • The value is a UUID containing 36 characters.
name	String	• Specifies a certificate name. • The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).
issuer	String	• Specifies the issuer of a certificate. • The value is a string of 1 to 256 characters.
subject	String	• Specifies the subject of a certificate. • The value is a string of 1 to 256 characters.
serial_number	String	• Specifies the serial number of a CA certificate. • The value is a string of 1 to 64 characters.

Parameter	Type	Description
expiration_time	String	- Specifies the expiration time of a certificate. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
signature_algorithm	String	- Specifies the signature algorithm of a certificate. - The value is a string of 1 to 64 characters.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the last update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

– Example response

```
{
  "client_ca_certificate": {
    "id": "ab80b8f6-6d67-4bdb-ba39-e8dd9419e64e",
    "name": "ca-cert-55f7",
    "issuer": "CN=xxx",
    "subject": "CN=xxx",
    "serial_number": "218730615113252363388323617489459159151767515623",
    "expiration_time": "2033-10-17T06:21:25Z",
    "signature_algorithm": "SHA256WITHRSA",
    "created_at": "2024-06-17T02:46:22.327Z",
    "updated_at": "2024-06-17T02:46:22.327Z"
  },
  "request_id": "29d83bb1-5349-4af5-9fa6-672af3daf4d1"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.9 Modifying a Client CA Certificate

Function

This API is used to update a client CA certificate with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}

Table 4-238 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
client_ca_certificate_id	String	Yes	Specifies the ID of a client CA certificate.

Request

- Request parameters

Table 4-239 Request parameters

Parameter	Type	Mandatory	Description
client_ca_certificate	client_ca_certificate object	Yes	Specifies the client CA certificate object.

Table 4-240 client_ca_certificate

Parameter	Type	Mandatory	Description
name	String	No	- Specifies a certificate name. - The value is a string of 1 to 64 characters, which can contain digits, letters, underscores (_), and hyphens (-).

– Example request

```
PUT https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}
```

```
{
  "client_ca_certificate": {
    "name": "client_ca_update"
  }
}
```

Response

- Response parameters

Returned status code 200: successful operation

Table 4-241 Parameters in the response body

Parameter	Type	Description
request_id	string	Specifies a request ID.

- Example response

```
{
  "request_id": "c63d850876bcd9bdfbd11776cce57914"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.10 Deleting a Client CA Certificate

Function

This API is used to delete a client CA certificate with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}

Table 4-242 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
client_ca_certificate_id	String	Yes	Specifies the ID of a client CA certificate.

Request

- Request parameters
None
- Example request

DELETE https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}

Response

- Response parameters
Returned status code 204: successful deletion

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.11 Modifying the Connection Log Configuration of a P2C VPN Gateway

Function

This API is used to modify the connection log configuration of a P2C VPN gateway with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config

Table 4-243 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.

Request

- Request parameters

Table 4-244 Request parameters

Parameter	Type	Mandatory	Description
log_config	UpdateVpnLogConfigRequestBodyContent object	Yes	Specifies the log_config object.

Table 4-245 UpdateVpnLogConfigRequestBodyContent

Parameter	Type	Mandatory	Description
log_group_id	String	Yes	Specifies a log group ID, which is obtained from the Log Tank Service (LTS).
log_stream_id	String	Yes	Specifies a log stream ID, which is obtained from LTS.

- Example request
PUT https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config

```
{
  "log_config": {
    "log_group_id": "05c4052d-8d14-488f-aa00-19fea5a25fdd",
    "log_stream_id": "d9d85143-e1e1-427a-9994-d8b8fd9ebe3f"
  }
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-246 Parameters in the response body

Parameter	Type	Description
log_config	ConnectionsLogConfig object	Specifies the log_config object.
request_id	String	Specifies a request ID.

Table 4-247 ConnectionsLogConfig

Parameter	Type	Description
log_group_id	String	Specifies a log group ID, which is obtained from LTS.
log_stream_id	String	Specifies a log stream ID, which is obtained from LTS.

- Example response

```
{
  "log_config": {
    "log_group_id": "05c4052d-8d14-488f-aa00-19fea5a25fdd",
    "log_stream_id": "d9d85143-e1e1-427a-9994-d8b8fd9ebe3f"
  },
  "request_id": "b19ba5a0be8f7b7f664b14596f8f35db"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.12 Querying the Connection Log Configuration of a P2C VPN Gateway

Function

This API is used to query the connection log configuration of a P2C VPN gateway with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config

Table 4-248 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config

Response

- Response parameters
Returned status code 200: successful query

Table 4-249 Parameters in the response body

Parameter	Type	Description
log_config	log_config object	Specifies the log_config object.
request_id	String	Specifies a request ID.

Table 4-250 log_config

Parameter	Type	Description
log_group_id	String	Specifies the ID of the log group to which the connection logs of the P2C VPN gateway belong.
log_stream_id	String	Specifies the ID of the log stream to which the connection logs of the P2C VPN gateway belong.

- Example response

```
{
  "log_config": {
    "log_group_id": "05c4052d-8d14-488f-aa00-19fea5a25fdd",
    "log_stream_id": "d9d85143-e1e1-427a-9994-d8b8fd9ebe3f"
  },
  "request_id": "2ddd2f6107a8164ce6f6268bd991e57c"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.2.13 Deleting the Connection Log Configuration of a P2C VPN Gateway

Function

This API is used to delete the connection log configuration of a P2C VPN gateway with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config

Table 4-251 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
p2c_vgw_id	String	Yes	Specifies the ID of a P2C VPN gateway instance.

Request

- Request parameters
None
- Example request
DELETE https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config

Response

- Response parameters
Returned status code 204: successful deletion

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3 User Management

4.2.3.1 Creating a VPN User

Function

This API is used to create a VPN user on a specified VPN server.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users

Table 4-252 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Table 4-253 Parameters in the request header

Parameter	Type	Mandatory	Description
X-Client-Token	String	No	- Specifies the ID of an idempotent request. - The value is a UUID containing 36 characters.

Request

- Request parameters

Table 4-254 Request parameters

Parameter	Type	Mandatory	Description
user	CreateVpnUserRequestBodyContent object	Yes	Specifies the to-be-created VPN user object.

Table 4-255 CreateVpnUserRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	Yes	- Specifies a username. - The value is a string of 4 to 32 characters, which can contain letters, digits, periods (.), underscores (_), and hyphens (-)

Parameter	Type	Mandatory	Description
password	String	Yes	• Specifies a password for the user. • Constraints: – 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.
description	String	No	• Specifies user description. • The value is a string of 0 to 64 characters, which can contain letters, digits, and underscores (_).
user_group_id	String	No	• Specifies the ID of the user group to which the user belongs. • The value is a UUID containing 36 characters.

Parameter	Type	Mandatory	Description
static_ip	String	No	- Specifies the static IP address of a client. - The value is an IPv4 address in dotted decimal notation (for example, 192.168.0.5) or disable. - The default value is disable, indicating that a client IP address is randomly allocated. - Constraints: - The value must be within the client CIDR block. - The value cannot be the gateway IP address of the client CIDR block. For example, if the client CIDR block is 192.168.0.0/24, 192.168.0.1 cannot be configured as a client address. - The value must be the first host address in a CIDR block with a 30-bit mask. For example, for the CIDR block 192.168.10.4/30 with four IP addresses, you can only specify 192.168.10.5 as a client address. - The value cannot be the same as the IP address of another user.

– Example request

POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users

```
{
  "user": {
    "name": "user001",
    "password": "*****",
    "description": "UserDescription1",
    "user_group_id": "yWYnJt0R-Q0a7-R4QW-tFXX-QfundEqrR27W"
  }
}
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-256 Parameters in the response body

Parameter	Type	Description
user	user object	Specifies the VPN user object.
request_id	String	Specifies a request ID.

Table 4-257 user

Parameter	Type	Description
id	String	- Specifies the ID of a VPN user. - The value is a UUID containing 36 characters.

- Example response

```
{
  "user": {
    "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d"
  },
  "request_id": "b19ba5a0be8f7b7f664b14596f8f35db"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.2 Creating VPN Users in Batches

Function

This API is used to create VPN users in batches on a specified VPN server.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/batch-create

Table 4-258 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Parameter	Type	Mandatory	Description
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Table 4-259 Parameters in the request header

Parameter	Type	Mandatory	Description
X-Client-Token	String	No	- Specifies the ID of an idempotent request. - The value is a UUID containing 36 characters.

Request

- Request parameters

Table 4-260 Request parameters

Parameter	Type	Mandatory	Description
users	Array of CreateVpnUser objects	Yes	Specifies the list of VPN users to be created.

Table 4-261 CreateVpnUser

Parameter	Type	Mandatory	Description
name	String	No	- Specifies a username. - The value is a string of 4 to 32 characters, which can contain letters, digits, periods (.), underscores (_), and hyphens (-)

Parameter	Type	Mandatory	Description
password	String	No	• Specifies a password for a user. • Constraints: – 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.
description	String	No	• Specifies user description. • The value is a string of 0 to 64 characters, which can contain letters, digits, and underscores (_).
user_group_name	String	No	• Specifies the name of the user group to which users belong. • Constraints: – The value is a string of 1 to 64 characters, which can contain letters, digits, underscores (_), and hyphens (-). – The value must be the name of an existing user group.

Parameter	Type	Mandatory	Description
static_ip	String	No	- Specifies the static IP address of a client. - The value is an IPv4 address in dotted decimal notation (for example, 192.168.0.5) or disable. - The default value is disable, indicating that a client IP address is randomly allocated. - Constraints: - The value must be within the client CIDR block. - The value cannot be the gateway IP address of the client CIDR block. For example, if the client CIDR block is 192.168.0.0/24, 192.168.0.1 cannot be configured as a client address. - The value must be the first host address in a CIDR block with a 30-bit mask. For example, for the CIDR block 192.168.10.4/30 with four IP addresses, you can only specify 192.168.10.5 as a client address. - The value cannot be the same as the IP address of another user.

– Example request

POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users

```
{
  "users": [
    {
      "name": "user1",
      "password": "*****",
      "description": "UserDescription1",
      "user_group_name": "default"
    },
    {
      "name": "user2",
      "password": "*****",
      "description": "UserDescription2",
      "user_group_name": "UserGroup1"
    }
  ]
}
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-262 Parameters in the response body

Parameter	Type	Description
invalid_users	Arrays of InvalidVpnUser Object	Specifies the list of invalid VPN users. If the invalid_users parameter is not empty, all users fail to be created in batches. You need to correct parameter settings in the request and try again.
request_id	String	Specifies a request ID.

Table 4-263 InvalidVpnUser

Parameter	Type	Description
name	String	Specifies a username.
description	String	Specifies user description.
user_group_name	String	Specifies the name of the user group to which the user belongs.
static_ip	String	Specifies the static IP address of the client.
cause	String	Specifies the cause.

- Example response
Response of successful batch creation:

```
{
  "invalid_users": [],
  "request_id": "b19ba5a0be8f7b7f664b14596f8f35db"
}
```

Response to a request that contains invalid users:

```
{
  "invalid_users": [
    {
      "name": "USER1",
      "description": "UserDescription",
      "user_group_name": "default",
      "cause": "Duplicate user name."
    },
    {
      "name": "USER2",
      "description": "UserDescription",
      "user_group_name": "default",
      "cause": "Password length invalid."
    }
  ],
}
```

```
"request_id": "49b52ed16992baa4650d093b512a59b6"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.3 Querying a VPN User

Function

This API is used to query information about a VPN user with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}

Table 4-264 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
user_id	String	Yes	Specifies a user ID.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-265 Parameters in the response body

Parameter	Type	Description
user	VpnUser object	Specifies the VPN user object.
request_id	String	Specifies a request ID.

Table 4-266 VpnUser

Parameter	Type	Description
id	String	- Specifies a user ID. - The value is a UUID containing 36 characters.
name	String	Specifies a username.
description	String	Specifies user description.
user_group_id	String	- Specifies the ID of the user group to which the user belongs. - The value is a UUID containing 36 characters.
user_group_name	String	Specifies the name of the user group to which the user belongs.
static_ip	String	- Specifies the static IP address of a client. - The value is an IPv4 address in dotted decimal notation (for example, 192.168.0.5) or disable.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

• Example response

```
{
  "user": {
    "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d",
    "name": "user001",
    "description": "UserDescription1",
    "user_group_id": "yWYnJt0R-Q0a7-R4QW-tFXX-QfundEqrR27W",
    "user_group_name": "user-group1",
    "created_at": "2024-06-17T06:53:46.302Z",
    "updated_at": "2024-06-17T06:53:46.302Z"
  },
}
```

```
}
  "request_id": "926a0edb3bf432943e2399b700173add"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.4 Querying the VPN User List

Function

This API is used to query the user list based on a specified VPN server ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users

Table 4-267 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	Yes	Specifies the ID of a VPN server.

Table 4-268 Parameter in a query request

Parameter	Type	Mandatory	Description
limit	Integer	No	Specifies the number of records returned on each page during pagination query.
marker	String	No	- Specifies the start flag for querying the current page. If this parameter is left blank, the first page is queried. The marker for querying the next page is the next_marker in the page_info object returned on the current page. - This parameter must be used together with limit.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users

Response

- Response parameters
Returned status code 200: successful query

Table 4-269 Parameters in the response body

Parameter	Type	Description
users	Array of VpnUser objects	Specifies user list information.
total_count	Integer	Specifies the total number of users on the current VPN server.
page_info	PageInfo object	Specifies pagination query information.
request_id	String	Specifies a request ID.

Table 4-270 VpnUser

Parameter	Type	Description
id	String	- Specifies a user ID. - The value is a UUID containing 36 characters.
name	String	Specifies a username.
description	String	Specifies user description.
user_group_id	String	- Specifies the ID of the user group to which the user belongs. - The value is a UUID containing 36 characters.
user_group_name	String	Specifies the name of the user group to which the user belongs.
static_ip	String	- Specifies the static IP address of a client. - The value is an IPv4 address in dotted decimal notation (for example, 192.168.0.5) or disable.

Parameter	Type	Description
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-271 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	Integer	Specifies the number of resources in the list.

• Example response

```
{
  "users": [
    {
      "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d",
      "name": "user001",
      "description": "UserDescription1",
      "user_group_id": "yWYnJt0R-Q0a7-R4QW-tFXX-QfundEqrR27W",
      "user_group_name": "user-group1",
      "created_at": "2024-06-17T06:53:46.302Z",
      "updated_at": "2024-06-17T06:53:46.302Z"
    },
    {
      "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d",
      "name": "user002",
      "description": "UserDescription2",
      "user_group_id": "yWYnJt0R-Q0a7-R4QW-tFXX-QfundEqrR27W",
      "user_group_name": "user-group1",
      "created_at": "2024-06-17T06:53:46.302Z",
      "updated_at": "2024-06-17T06:53:46.302Z"
    }
  ],
  "total_count": 2,
  "page_info": {
    "current_count": 2
  },
  "request_id": "b04b68fb4d548344e0bc4b34dbd6f6e7"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.5 Modifying a VPN User

Function

This API is used to modify a VPN user with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}

Table 4-272 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
user_id	String	Yes	Specifies a user ID.

Request

- Request parameters

Table 4-273 Request parameters

Parameter	Type	Mandatory	Description
user	UpdateVpnUserRequestBodyContent object	Yes	Specifies the to-be-modified VPN user object.

Table 4-274 UpdateVpnUserRequestBodyContent

Parameter	Type	Mandatory	Description
description	String	No	- Specifies user description. - The value is a string of 0 to 64 characters, which can contain letters, digits, and underscores (_).
user_group_id	String	No	- Specifies the ID of the user group to which the user belongs. - The value is a UUID containing 36 characters.
static_ip	String	No	- Specifies the static IP address of a client. - The value is an IPv4 address in dotted decimal notation (for example, 192.168.0.5) or disable. - Constraints: - The value must be within the client CIDR block. - The value cannot be the gateway IP address of the client CIDR block. For example, if the client CIDR block is 192.168.0.0/24, 192.168.0.1 cannot be configured as a client address. - The value must be the first host address in a CIDR block with a 30-bit mask. For example, for the CIDR block 192.168.10.4/30 with four IP addresses, you can only specify 192.168.10.5 as a client address. - The value cannot be the same as the IP address of another user.

- Example request**
PUT https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}

```
{
  "user": {
    "description": "UserDescription-update",
    "user_group_id": "PTnsQAbZ-KOGW-mCzt-C9Sk-rMM3TcNjQ8wY"
  }
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-275 Parameters in the response body

Parameter	Type	Description
user	VpnUser object	Specifies the VPN user object.
request_id	String	Specifies a request ID.

Table 4-276 VpnUser

Parameter	Type	Description
id	String	• Specifies a user ID. • The value is a UUID containing 36 characters.
name	String	Specifies a username.
description	String	Specifies user description.
user_group_id	String	• Specifies the ID of the user group to which the user belongs. • The value is a UUID containing 36 characters.
user_group_name	String	Specifies the name of the user group to which the user belongs.
static_ip	String	• Specifies the static IP address of a client. • The value is an IPv4 address in dotted decimal notation (for example, 192.168.0.5) or disable.
created_at	String	• Specifies the creation time. • The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	• Specifies the update time. • The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

– Example response

```
{
  "user": {
    "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d",
```

```
    "name": "1111",
    "description": "UserDescription-update",
    "user_group_id": "PTnsQAbZ-KOgW-mCzt-C9Sk-rMM3TcNjQ8wY",
    "user_group_name": "user-group2",
    "created_at": "2024-06-17T06:53:46.302Z",
    "updated_at": "2024-06-17T08:45:20.973Z"
  },
  "request_id": "380562b4bda6dfe116c42e707d8e9110"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.6 Deleting a VPN User

Function

This API is used to delete a VPN user with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}

Table 4-277 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
user_id	String	Yes	Specifies a user ID.

Request

- Request parameters
None
- Example request
DELETE https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}

Response

- Response parameters
Returned status code 204: successful deletion

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.7 Deleting VPN Users in Batches

Function

This API is used to delete VPN users with specified IDs in batches.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/batch-delete

Table 4-278 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Request

- Request parameters

Table 4-279 Request parameters

Parameter	Type	Mandatory	Description
users	Array of OpVpnUser objects	Yes	Specifies the list of VPN users to be deleted.

Table 4-280 OpVpnUser

Parameter	Type	Mandatory	Description
id	String	Yes	- Specifies a user ID. - The value is a UUID containing 36 characters.

- Example request
POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/batch-delete

```
{
  "users": [
    {
      "id": "cc975b1d-ed5-448d-a47d-9dbf11f5d842"
    },
    {
      "id": "30ad347e-e36e-42bd-a36b-c38f8ecc8bda"
    }
  ]
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-281 Parameters in the response body

Parameter	Type	Description
request_id	String	Specifies a request ID.

- Example response

```
{
  "request_id": "c63d850876bcd8bdfbd11776cce57914"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.8 Changing the Password of a VPN User

Function

This API is used to change the password of a specified VPN user.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/password

Table 4-282 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
user_id	String	Yes	Specifies the ID of a VPN user.

Request

- Request parameters

Table 4-283 Request parameters

Parameter	Type	Mandatory	Description
old_password	String	Yes	Specifies the old password.
new_password	String	Yes	- Specifies a new password for the user. - Constraints: - 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. - The new password must be different from the latest five old passwords.

- **Example request**
PUT https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/password

```
{
  "old_password": "stringst-old",
  "new_password": "stringst-new"
}
```

Response

- **Response parameters**
Returned status code 200: successful operation

Table 4-284 Parameters in the response body

Parameter	Type	Description
request_id	String	Specifies a request ID.

- **Example response**

```
{
  "request_id": "c63d850876bcd9bdfbd11776cce57914"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.9 Resetting the Password of a VPN User

Function

This API is used to reset the password of a specified VPN user.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/reset-password

Table 4-285 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Parameter	Type	Mandatory	Description
user_id	String	Yes	Specifies the ID of a VPN user.

Request

- Request parameters

Table 4-286 Request parameters

Parameter	Type	Mandatory	Description
new_password	String	Yes	- Specifies a new password for the user. - Constraints: - 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. - The new password must be different from the latest five old passwords.

- Example request

```
POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/reset-password
{
  "new_password": "stringst-new"
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-287 Parameters in the response body

Parameter	Type	Description
request_id	String	Specifies a request ID.

- Example response

```
{
  "request_id": "c63d850876bcd9bdfbd11776cce57914"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.10 Creating a VPN User Group

Function

This API is used to create a VPN user group on a specified VPN server.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups

Table 4-288 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Table 4-289 Parameters in the request header

Parameter	Type	Mandatory	Description
X-Client-Token	String	No	• Specifies the ID of an idempotent request. • The value is a UUID containing 36 characters.

Request

- Request parameters

Table 4-290 Request parameters

Parameter	Type	Mandatory	Description
user_group	CreateVpnUserGroupRequestBodyContent object	Yes	Specifies the to-be-created VPN user group object.

Table 4-291 CreateVpnUserGroupRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	Yes	- Specifies a user group name. - The value is a string of 1 to 64 characters, which can contain letters, digits, underscores (_), and hyphens (-). - A user group name must be unique.
description	String	No	- Specifies user group description. - The value is a string of 0 to 64 characters, which can contain uppercase letters, lowercase letters, digits, and the following special characters: `~!@#\$%^&*()-_+=\ []{};:","<.>/?

– Example request

```
POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups
{
  "user_group": {
    "name": "user-group1",
    "description": "UserGroup1"
  }
}
```

Response

- Response parameters
- Returned status code 201: successful operation

Table 4-292 Parameters in the response body

Parameter	Type	Description
user_group	user_group object	Specifies the user group object.
request_id	String	Specifies a request ID.

Table 4-293 user_group

Parameter	Type	Description
id	String	- Specifies the ID of a VPN user group. - The value is a UUID containing 36 characters.

- Example response

```
{
  "user_group": {
    "id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8"
  },
  "request_id": "94d271493e144135423e7377e40127cf"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.11 Querying a VPN User Group

Function

This API is used to query information about a VPN user group with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}

Table 4-294 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
group_id	String	Yes	Specifies the ID of a user group.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}

Response

- Response parameters
Returned status code 200: successful query

Table 4-295 Parameters in the response body

Parameter	Type	Description
user_group	VpnUserGroup object	Specifies the VPN user group object.
request_id	String	Specifies a request ID.

Table 4-296 VpnUserGroup

Parameter	Type	Description
id	String	- Specifies the ID of a VPN user group. - The value is a UUID containing 36 characters.
name	String	Specifies the name of a user group.
description	String	Specifies user group description.
type	String	- Specifies the type of a user group. - Value range: Default: default user group Custom: custom user group

Parameter	Type	Description
user_number	Integer	Specifies the number of users.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

– Example response

```
{
  "user_group": {
    "id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
    "name": "user-group1",
    "description": "UserGroup1",
    "type": "Custom",
    "user_number": 0,
    "created_at": "2024-06-17T09:48:27.548Z",
    "updated_at": "2024-06-17T09:48:27.548Z"
  },
  "request_id": "6735d32bb3e35e9154caba1dbc6c2dc6"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.12 Querying the VPN User Group List

Function

This API is used to query the list of user groups on a specified server.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups

Table 4-297 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Parameter	Type	Mandatory	Description
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Table 4-298 Parameter in a query request

Parameter	Type	Mandatory	Description
limit	Integer	No	Specifies the number of records returned on each page during pagination query.
marker	String	No	- Specifies the start flag for querying the current page. If this parameter is left blank, the first page is queried. The marker for querying the next page is the next_marker in the page_info object returned on the current page. - This parameter must be used together with limit.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups

Response

- Response parameters
Returned status code 200: successful query

Table 4-299 Parameters in the response body

Parameter	Type	Description
user_groups	Array of VpnUserGroup objects	Specifies the user group list object.
total_count	Integer	Specifies the total number of user groups.
page_info	PageInfo object	Specifies pagination query information.
request_id	String	Specifies a request ID.

Table 4-300 VpnUserGroup

Parameter	Type	Description
id	String	- Specifies the ID of a VPN user group. - The value is a UUID containing 36 characters.
name	String	Specifies the name of a user group.
description	String	Specifies user group description.
type	String	- Specifies the type of a user group. - Value range: Default: default user group Custom: custom user group
user_number	Integer	Specifies the number of users.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-301 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	Integer	Specifies the number of resources in the list.

– Example response

```
{
  "user_groups": [
    {
      "id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
      "name": "user-group1",
      "description": "UserGroup1",
      "type": "Custom",
      "user_number": 0,
      "created_at": "2024-06-17T09:48:27.548Z",
      "updated_at": "2024-06-17T09:48:27.548Z"
    },
    {
      "id": "0748b24e-cbd3-474e-9546-8586e8f2b5c6",
      "name": "default",
```

```
        "description": "Default user group",
        "type": "Default",
        "user_number": 0,
        "created_at": "2024-06-17T03:45:25.879Z",
        "updated_at": "2024-06-17T03:45:25.879Z"
      }
    ],
    "total_count": 2,
    "page_info": {
      "current_count": 2
    },
    "request_id": "1ae5c7648497d3d90824985367da954a"
  }
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.13 Modifying a VPN User Group

Function

This API is used to modify a VPN user group with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}

Table 4-302 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
group_id	String	Yes	Specifies the ID of a user group.

Request

- Request parameters

Table 4-303 Request parameters

Parameter	Type	Mandatory	Description
user_group	UpdateVpnUserGroupRequestBodyContent object	Yes	Specifies the to-be-modified VPN user group object.

Table 4-304 UpdateVpnUserGroupRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	- Specifies a user group name. - The value is a string of 1 to 64 characters, which can contain uppercase letters, lowercase letters, digits, and the following special characters: `~!@#\$%^&*()-_+=\ [{ }];:","<.>/? - A user group name must be unique.
description	String	No	- Specifies user group description. - The value is a string of 0 to 64 characters, which can contain uppercase letters, lowercase letters, digits, and the following special characters: `~!@#\$%^&*()-_+=\ [{ }];:","<.>/?

– Example request

```
PUT https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}

{
  "user_group": {
    "name": "user-group1-update",
    "description": "UserGroup1-update"
  }
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-305 Parameters in the response body

Parameter	Type	Description
user_group	VpnUserGroup object	Specifies the VPN user group object.
request_id	String	Specifies a request ID.

Table 4-306 VpnUserGroup

Parameter	Type	Description
id	String	- Specifies the ID of a VPN user group. - The value is a UUID containing 36 characters.
name	String	Specifies the name of a user group.
description	String	Specifies user group description.
type	String	- Specifies the type of a user group. - Value range: Default: default user group Custom: custom user group
user_number	Integer	Specifies the number of users.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

– Example response

```
{
  "user_group": {
    "id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
    "name": "user-group1-update",
    "description": "UserGroup1-update",
    "type": "Custom",
    "user_number": 0,
    "created_at": "2024-06-17T09:48:27.548Z",
    "updated_at": "2024-06-17T09:59:03.318Z"
  },
  "request_id": "6735d32bb3e35e9154caba1dbc6c2dc6"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.14 Deleting a VPN User Group

Function

This API is used to delete a VPN user group with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}

Table 4-307 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
group_id	String	Yes	Specifies the ID of a user group.

Request

- Request parameters
None
- Example request
DELETE https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}

Response

- Response parameters
Returned status code 204: successful deletion

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.15 Adding a VPN User to a Group

Function

This API is used to add a VPN user to a specified user group.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/add-users

Table 4-308 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
group_id	String	Yes	Specifies the ID of a VPN user group.

Request

- Request parameters

Table 4-309 Request parameters

Parameter	Type	Mandatory	Description
users	Array of OpVpnUser objects	Yes	Specifies the VPN user list.

Table 4-310 OpVpnUser

Parameter	Type	Mandatory	Description
id	String	Yes	- Specifies the ID of a VPN user. - The value is a UUID containing 36 characters.

- Example request
POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/add-users

```
{
  "users": [
```

```
{
  "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d"
},
{
  "id": "a609eecb-3fa6-4d6d-a8c3-256a12d02b6c"
}
]
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-311 Parameters in the response body

Parameter	Type	Description
request_id	String	Specifies a request ID.

– Example response

```
{
  "request_id": "63c49a90467d1ee8a111e587eaedac1f"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.16 Removing a VPN User from a Group

Function

This API is used to remove a VPN user from a specified user group.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/remove-users

Table 4-312 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Parameter	Type	Mandatory	Description
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
group_id	String	Yes	Specifies the ID of a VPN user group.

Request

- Request parameters

Table 4-313 Request parameters

Parameter	Type	Mandatory	Description
users	Array of OpVpnUser objects	Yes	Specifies the VPN user list.

Table 4-314 OpVpnUser

Parameter	Type	Mandatory	Description
id	String	Yes	- Specifies the ID of a VPN user. - The value is a UUID containing 36 characters.

- Example request
POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/remove-users

```
{
  "users": [
    {
      "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d"
    }
  ]
}
```

Response

- Response parameters
Returned status code 201: successful operation

Table 4-315 Parameters in the response body

Parameter	Type	Description
request_id	String	Specifies a request ID.

– Example response

```
{
  "request_id": "254ee8ac1d39c2a0ec6200447b676e18"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.3.17 Querying VPN Users in a Group

Function

This API is used to query information about users in a VPN user group with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/users

Table 4-316 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
group_id	String	Yes	Specifies the ID of a user group.

Table 4-317 Parameter in a query request

Parameter	Type	Mandatory	Description
limit	Integer	No	Specifies the number of records returned on each page during pagination query.
marker	String	No	- Specifies the start flag for querying the current page. If this parameter is left blank, the first page is queried. The marker for querying the next page is the next_marker in the page_info object returned on the current page. - This parameter must be used together with limit.

Request

- Request parameters

None

- Example request

```
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/users
```

Response

- Response parameters

Returned status code 200: successful query

Table 4-318 Parameters in the response body

Parameter	Type	Description
users	Array of VpnUserInGroup objects	Specifies the user group list object.
total_count	integer	Specifies the total number of users.
page_info	PageInfo object	Specifies pagination query information.
request_id	String	Specifies a request ID.

Table 4-319 VpnUserInGroup

Parameter	Type	Description
id	String	- Specifies a user ID. - The value is a UUID containing 36 characters.
name	String	Specifies a username.
description	String	Specifies user description.

Table 4-320 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	Integer	Specifies the number of resources in the list.

– Example response

```
{
  "users": [
    {
      "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d",
      "name": "user1",
      "description": "User1's description"
    }
  ],
  "total_count": 1,
  "page_info": {
    "current_count": 1
  },
  "request_id": "146c67110e52963d5bf62785aede7308"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.4 Access Policy

4.2.4.1 Creating a VPN Access Policy

Function

This API is used to create an access policy on a specified VPN server.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies

Table 4-321 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Table 4-322 Parameters in the request header

Parameter	Type	Mandatory	Description
X-Client-Token	String	No	- Specifies the ID of an idempotent request. - The value is a UUID containing 36 characters.

Request

- Request parameters

Table 4-323 Request parameters

Parameter	Type	Mandatory	Description
access_policy	CreateVpnAccessPolicyRequestBodyContent object	Yes	Specifies the to-be-created VPN access policy object.

Table 4-324 CreateVpnAccessPolicyRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	Yes	Specifies the name of an access policy.
user_group_id	String	Yes	- Specifies the ID of a VPN user group. - The value is a UUID containing 36 characters.
description	String	No	Specifies access policy description.
dest_ip_cidrs	Array of strings	Yes	- Specifies the list of destination CIDR blocks. - The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24. - There must be at least one CIDR block. A maximum of 10 CIDR blocks are supported.

– Example request

POST https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies

```
{
  "access_policy": {
    "name": "policy-001",
    "user_group_id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
    "description": "AccessPolicy1",
    "dest_ip_cidrs": [
      "172.16.0.0/24",
      "172.16.1.0/24"
    ]
  }
}
```

Response

- Response parameters

Returned status code 201: successful operation

Table 4-325 Parameters in the response body

Parameter	Type	Description
access_policy	access_policy object	Specifies the access policy object.
request_id	String	Specifies a request ID.

Table 4-326 access_policy

Parameter	Type	Description
id	String	- Specifies the ID of an access policy. - The value is a UUID containing 36 characters.

- Example response

```
{
  "access_policy": {
    "id": "4f746482-a575-4e1f-9e80-5f6f69ff8588"
  },
  "request_id": "1663cd8cacbb3497ebc88877e5a3ad89"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.4.2 Querying a VPN Access Policy

Function

This API is used to query a VPN access policy with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}

Table 4-327 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
policy_id	String	Yes	Specifies the ID of an access policy.

Request

- Request parameters
None

- **Example request**
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}

Response

- **Response parameters**
Returned status code 200: successful query

Table 4-328 Parameters in the response body

Parameter	Type	Description
access_policy	VpnAccessPolicy object	Specifies the VPN access policy object.
request_id	String	Specifies a request ID.

Table 4-329 VpnAccessPolicy

Parameter	Type	Description
id	String	• Specifies the ID of an access policy. • The value is a UUID containing 36 characters.
name	String	Specifies the name of an access policy.
user_group_id	String	• Specifies the ID of the associated user group. • The value is a UUID containing 36 characters.
user_group_name	String	Specifies the name of the associated user group.
description	String	Specifies access policy description.
dest_ip_cidrs	Array of String	• Specifies the list of destination CIDR blocks. • The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24.
created_at	String	• Specifies the creation time. • The UTC time format is yyyy-MM-ddTHH:mm:ssZ.
updated_at	String	• Specifies the update time. • The UTC time format is yyyy-MM-ddTHH:mm:ssZ.

- Example response

```
{
  "access_policy": {
    "id": "4f746482-a575-4e1f-9e80-5f6f69ff8588",
    "name": "policy-001",
    "user_group_id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
    "user_group_name": "user-group1",
    "description": "AccessPolicy1",
    "dest_ip_cidrs": [
      "172.16.0.0/24",
      "172.16.1.0/24"
    ],
    "created_at": "2024-06-17T13:32:19.57Z",
    "updated_at": "2024-06-17T13:32:19.57Z"
  },
  "request_id": "85657002f01c35576606003cc36114ab"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.4.3 Querying the VPN Access Policy List

Function

This API is used to query the list of VPN access policies on a VPN server with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies

Table 4-330 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.

Table 4-331 Parameter in a query request

Parameter	Type	Mandator y	Description
limit	Integer	No	Specifies the number of records returned on each page during pagination query.
marker	String	No	- Specifies the start flag for querying the current page. If this parameter is left blank, the first page is queried. The marker for querying the next page is the next_marker in the page_info object returned on the current page. - This parameter must be used together with limit.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies

Response

- Response parameters
Returned status code 200: successful query

Table 4-332 Parameters in the response body

Parameter	Type	Description
access_policies	Array of VpnAccessPolicy objects	Specifies the access policy list object.
total_count	Integer	Specifies the total number of access policies.
page_info	PageInfo object	Specifies pagination query information.
request_id	String	Specifies a request ID.

Table 4-333 VpnAccessPolicy

Parameter	Type	Description
id	String	- Specifies the ID of an access policy. - The value is a UUID containing 36 characters.
name	String	Specifies the name of an access policy.
user_group_id	String	- Specifies the ID of the associated user group. - The value is a UUID containing 36 characters.
user_group_name	String	Specifies the name of the associated user group.
description	String	Specifies access policy description.
dest_ip_cidrs	Array of String	- Specifies the list of destination CIDR blocks. - The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24.
created_at	String	- Specifies the creation time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	- Specifies the update time. - The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

Table 4-334 PageInfo

Parameter	Type	Description
next_marker	String	Specifies the marker of the next page. The value is the time when the last resource in the last query response was created.
current_count	Integer	Specifies the number of resources in the list.

- Example response

```
{
  "access_policies": [
    {
      "id": "4f746482-a575-4e1f-9e80-5f6f69ff8588",
      "name": "policy-001",
      "user_group_id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
      "user_group_name": "user-group1",
```

```
{
  "description": "AccessPolicy1",
  "dest_ip_cidrs": [
    "172.16.0.0/24",
    "172.16.1.0/24"
  ],
  "created_at": "2024-06-17T13:32:19.57Z",
  "updated_at": "2024-06-17T13:32:19.57Z"
},
{
  "total_count": 1,
  "page_info": {
    "current_count": 1
  },
  "request_id": "02b5b35cab4c2963d1d89560f50017b9"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.4.4 Modifying a VPN Access Policy

Function

This API is used to modify a VPN access policy with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}

Table 4-335 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
policy_id	String	Yes	Specifies the ID of an access policy.

Request

- Request parameters

Table 4-336 Request parameters

Parameter	Type	Mandatory	Description
access_policy	UpdateVpnAccessPolicyRequestBodyContent object	Yes	Specifies the to-be-modified access policy object.

Table 4-337 UpdateVpnAccessPolicyRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	Specifies the name of an access policy.
user_group_id	String	No	- Specifies the ID of the associated user group. - The value is a UUID containing 36 characters.
description	String	No	Specifies access policy description.
dest_ip_cidrs	Array of strings	No	- Specifies the list of destination CIDR blocks. - The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24. - There must be at least one CIDR block. A maximum of 10 CIDR blocks are supported.

– Example request

PUT https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}

```
{
  "access_policy": {
    "name": "policy-001-update",
    "user_group_id": "efb92c43-c2e9-44c0-b2e5-5b980f0ca90a",
    "description": "AccessPolicy1-update",
    "dest_ip_cidrs": [
      "192.168.12.0/24",
      "192.168.1.0/24"
    ]
  }
}
```

Response

- Response parameters
Returned status code 200: successful operation

Table 4-338 Parameters in the response body

Parameter	Type	Description
access_policy	VpnAccessPolicy object	Specifies the VPN access policy object.
request_id	String	Specifies a request ID.

Table 4-339 VpnAccessPolicy

Parameter	Type	Description
id	String	• Specifies the ID of an access policy. • The value is a UUID containing 36 characters.
name	String	Specifies the name of an access policy.
user_group_id	String	• Specifies the ID of the associated user group. • The value is a UUID containing 36 characters.
user_group_name	String	Specifies the name of the associated user group.
description	String	Specifies access policy description.
dest_ip_cidrs	Array of String	• Specifies the list of destination CIDR blocks. • The value is in the format of dotted decimal notation/mask, for example, 192.168.1.0/24.
created_at	String	• Specifies the creation time. • The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.
updated_at	String	• Specifies the update time. • The UTC time format is <i>yyyy-MM-ddTHH:mm:ssZ</i>.

– Example response

```
{
  "access_policy": {
    "id": "36f3f232-9204-4774-be20-84cc94da8535",
```

```
{
  "name": "policy-001-update",
  "user_group_id": "efb92c43-c2e9-44c0-b2e5-5b980f0ca90a",
  "user_group_name": "UserGroupA",
  "description": "AccessPolicy1-update",
  "dest_ip_cidrs": [
    "192.168.12.0/24",
    "192.168.1.0/24"
  ],
  "created_at": "2024-06-14T08:59:45.598Z",
  "updated_at": "2024-06-14T09:01:59.539Z"
},
"request_id": "2e4cc58a4ea5fe69f62d6d8943b5f99b"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.2.4.5 Deleting a VPN Access Policy

Function

This API is used to delete a VPN access policy with a specified ID.

Calling Method

For details, see [3 Calling APIs](#).

URI

DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}

Table 4-340 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
vpn_server_id	String	Yes	Specifies the ID of a VPN server.
policy_id	String	Yes	Specifies the ID of an access policy.

Request

- Request parameters
None
- Example request
DELETE https://{Endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}

Response

- Response parameters
Returned status code 204: successful deletion

Status Codes

For details, see [A.2 Status Codes](#).

4.3 Public Service APIs

4.3.1 VPN Quota

4.3.1.1 Querying Quotas

Function

This API is used to query VPN resource quotas of a tenant, including VPN gateways, customer gateways, and VPN connections.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/vpn/quotas

Table 4-341 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/vpn/quotas

Response

- Response parameters
Returned status code 200: successful query

Table 4-342 Parameters in the response body

Parameter	Type	Description
quotas	Quotas object	Specifies the quotas object.
request_id	String	Specifies a request ID.

Table 4-343 Quotas

Parameter	Type	Description
resources	Array of QuotaInfo objects	Specifies the resources object.

Table 4-344 QuotaInfo

Parameter	Type	Description
type	String	- Specifies a resource type. - Value range: customer_gateway: customer gateway vpn_connection: Enterprise Edition VPN connection vpn_gateway: Enterprise Edition VPN gateway
quota	Integer	Specifies the quota upper limit.
used	Integer	Specifies the number of resources in use.

- Example response

```
{
  "quotas": {
    "resources": [
      {
        "type": "customer_gateway",
        "quota": 100,
        "used": 13
      },
      {
        "type": "vpn_connection",
        "quota": 5000,
        "used": 306
      },
      {
        "type": "vpn_gateway",
        "quota": 50,
        "used": 23
      }
    ]
  },
}
```

```
}
  "request_id": "9aeb7f73-e1b6-42eb-96ad-b68aef8186e3"
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.3.2 VPN Tag

4.3.2.1 Querying the Resource Instance List

Function

This API is used to query resource instances based on tags.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/{resource_type}/resource-instances/filter

Table 4-345 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
resource_type	String	Yes	- Specifies the resource type. - The value can be one of the following: vpn-gateway, customer-gateway, vpn-connection, p2c-vpn-gateways.

Table 4-346 Parameter in a query request

Parameter	Type	Mandatory	Description
limit	Integer	No	- Specifies the number of records to be queried. - The value ranges from 1 to 1000. - The default value is 1000.

Parameter	Type	Mandatory	Description
offset	Integer	No	- Specifies the index position. The query starts from the (<i>offset value</i> + 1)th data record. - The minimum value is 0. - The default value is 0.

Request

- Request parameters

Table 4-347 Request parameters

Parameter	Type	Mandatory	Description
without_any_tag	Boolean	No	When this parameter is set to true, all resources without tags are queried. In this case, the tags field is ignored. If this parameter is set to false or is not specified, all resources are queried or resources are filtered by "tags" or "matches".
tags	Array of Tag objects	No	- Specifies a tag list. - A maximum of 20 tags can be specified.
matches	Array of Match objects	No	Specifies a search field, including a key and a value. The match key is the field to be matched, for example, resource_name. The match value is the value to be matched. The key is a fixed dictionary value.

Table 4-348 Tag

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a tag key. - The value is a string of 1 to 128 characters.

Parameter	Type	Mandatory	Description
values	Array of String	Yes	- Specifies the value list of a tag. If values is an empty list, it indicates any_value. The relationship between values is OR. - The value is a string of 0 to 255 characters. - A maximum of 20 values can be specified.

Table 4-349 Match

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a match key. - The value is resource_name.
value	String	Yes	- Specifies a match value. - The value is a string of 0 to 255 characters.

- Example request

POST https://{Endpoint}/v5/{project_id}/{resource_type}/resource-instances/filter

```
{
  "tags": [{
    "key": "key1",
    "values": [
      "value1",
      "value2"
    ]
  },
  {
    "key": "key2",
    "values": [
      "value1",
      "value2"
    ]
  }
],
  "matches": [{
    "key": "resource_name",
    "value": "resource1"
  }],
  "without_any_tag": "false"
}
```

Response

- Response parameters

Returned status code 200: successful query

Table 4-350 Parameters in the response body

Parameter	Type	Description
resources	Array of Resource objects	Indicates the resource object list.
total_count	Integer	Indicates the total number of records.

Table 4-351 Resource

Parameter	Type	Description
resource_id	String	Indicates a resource ID.
resource_detail	object	Specifies resource details. This parameter is reserved for extension and is left empty by default.
tags	Array of ResourceTag objects	Specifies a tag list.
resource_name	String	Indicates a resource name.

Table 4-352 ResourceTag

Parameter	Type	Description
key	String	Indicates a tag key.
value	String	Indicates a tag value.

- Example response

```
{
  "resources": [{
    "resource_id": "134f9fb1-demo-a8df-va86-2040a5c13325",
    "resource_name": "resoucee1",
    "tags": [{
      "key": "key1",
      "value": "value1"
    }]
  }],
  "total_count": 1000
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.3.2.2 Querying the Number of Resource Instances

Function

This API is used to query the number of resource instances based on tags.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/{resource_type}/resource-instances/count

Table 4-353 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
resource_type	String	Yes	- Specifies the resource type. - The value can be one of the following: vpn-gateway, customer-gateway, vpn-connection, p2c-vpn-gateways.

Request

- Request parameters

Table 4-354 Request parameters

Parameter	Type	Mandatory	Description
without_any_tag	Boolean	No	When this parameter is set to true, all resources without tags are queried. In this case, the tags field is ignored. If this parameter is set to false or is not specified, all resources are queried or resources are filtered by "tags" or "matches".
tags	Array of Tag objects	No	- Specifies a tag list. - A maximum of 20 tags can be specified.

Parameter	Type	Mandatory	Description
matches	Array of Match objects	No	Specifies a search field, including a key and a value. The match key is the field to be matched, for example, resource_name. The match value is the value to be matched. The key is a fixed dictionary value.

Table 4-355 Tag

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a tag key. - The value is a string of 1 to 128 characters.
values	Array of String	Yes	- Specifies the value list of a tag. If values is an empty list, it indicates any_value. The relationship between values is OR. - The value is a string of 0 to 255 characters. - A maximum of 20 values can be specified.

Table 4-356 Match

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a match key. - The value is resource_name.
value	String	Yes	- Specifies a match value. - The value is a string of 0 to 255 characters.

- Example request

```
POST https://{Endpoint}/v5/{project_id}/{resource_type}/resource-instances/count
{
  "tags": [{
    "key": "key1",
    "values": [
      "value1",
      "value2"
    ]
  }]
```

```
    ],  
    {  
      "key": "key2",  
      "values": [  
        "value1",  
        "value2"  
      ]  
    }  
  ],  
  "matches": [{  
    "key": "resource_name",  
    "value": "resource1"  
  }],  
  "without_any_tag": "false"  
}
```

Response

- Response parameters
Returned status code 200: successful query

Table 4-357 Parameters in the response body

Parameter	Type	Description
total_count	Integer	Indicates the total number of records.

- Example response

```
{  
  "total_count": 1000  
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.3.2.3 Adding Resource Tags in Batches

Function

This API is used to add tags to a specified instance in batches.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create

Table 4-358 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
resource_type	String	Yes	- Specifies the resource type. - The value can be one of the following: vpn-gateway, customer-gateway, vpn-connection, p2c-vpn-gateways.
resource_id	String	Yes	Indicates a resource ID.

Request

- Request parameters

Table 4-359 Request parameters

Parameter	Type	Mandatory	Description
tags	Array of ResourceTag objects	Yes	- Specifies a tag list. - A maximum of 20 tags can be specified.

Table 4-360 ResourceTag

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	No	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- **Example request**
POST https://{Endpoint}/v5/{project_id}/{resource_type}/{resource_id}/tags/create
{
 "tags": [{
 "key": "key1",
 "value": "value1"
 }]
}

Response

- **Response parameters**
Returned status code 204: Tags are successfully added.

Status Codes

For details, see [A.2 Status Codes](#).

4.3.2.4 Deleting Resource Tags in Batches

Function

This API is used to delete tags from a specified instance in batches.

Calling Method

For details, see [3 Calling APIs](#).

URI

POST /v5/{project_id}/{resource_type}/{resource_id}/tags/delete

Table 4-361 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
resource_type	String	Yes	• Specifies the resource type. • The value can be one of the following: vpn-gateway, customer-gateway, vpn-connection, p2c-vpn-gateways.
resource_id	String	Yes	Indicates a resource ID.

Request

- Request parameters

Table 4-362 Request parameters

Parameter	Type	Mandatory	Description
tags	Array of ResourceTag objects	Yes	- Specifies a tag list. - A maximum of 20 tags can be specified.

Table 4-363 ResourceTag

Parameter	Type	Mandatory	Description
key	String	Yes	- Specifies a tag key. - The value is a string of 1 to 128 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).
value	String	No	- Specifies a tag value. - The value is a string of 0 to 255 characters that can contain digits, letters, Spanish characters, Portuguese characters, spaces, and special characters (_ . : = + - @).

- Example request

```
DELETE https://{Endpoint}/v5/{project_id}/{resource_type}/{resource_id}/tags/delete
{
  "tags": [{
    "key": "key1",
    "value": "value1"
  }]
}
```

Response

- Response parameters
Returned status code 204: Tags are successfully deleted.

Status Codes

For details, see [A.2 Status Codes](#).

4.3.2.5 Querying Resource Tags

Function

This API is used to query tags of a specified instance.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/{resource_type}/{resource_id}/tags

Table 4-364 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
resource_type	String	Yes	- Specifies the resource type. - The value can be one of the following: vpn-gateway, customer-gateway, vpn-connection, p2c-vpn-gateways.
resource_id	String	Yes	Indicates a resource ID.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/{resource_type}/{resource_id}/tags

Response

- Response parameters
Returned status code 200: successful query

Table 4-365 Parameters in the response body

Parameter	Type	Description
tags	Array of ResourceTag objects	Specifies the list of resource tags.

Table 4-366 ResourceTag

Parameter	Type	Description
key	String	Specifies a tag key.
value	String	Specifies a tag value.

- Example response

```
{
  "tags": [
    {
      "key": "key1",
      "value": "value1"
    }
  ]
}
```

Status Codes

For details, see [A.2 Status Codes](#).

4.3.2.6 Querying Project Tags

Function

This API is used to query all tags of a specified resource type in a specified project of a tenant.

Calling Method

For details, see [3 Calling APIs](#).

URI

GET /v5/{project_id}/{resource_type}/tags

Table 4-367 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies a project ID. You can obtain the project ID by referring to A.1 Obtaining the Project ID .
resource_type	String	Yes	• Specifies the resource type. • The value can be one of the following: vpn-gateway, customer-gateway, vpn-connection, p2c-vpn-gateways.

Request

- Request parameters
None
- Example request
GET https://{Endpoint}/v5/{project_id}/{resource_type}/tags

Response

- Response parameters
Returned status code 200: successful query

Table 4-368 Parameters in the response body

Parameter	Type	Description
tags	Array of ResourceTag objects	Specifies the list of resource tags.

Table 4-369 ResourceTag

Parameter	Type	Description
key	String	Indicates a tag key.
values	Array of String	Indicates a tag value.

- Example response

```
{
  "tags": [
    {
      "key": "key1",
      "values": ["value1"]
    }
  ]
}
```

Status Codes

For details, see [A.2 Status Codes](#).

5 Application Examples

5.1 Example 1: Creating an S2C VPN Gateway

Scenario

This section describes how to create an S2C VPN gateway by calling an API.

Prerequisites

- You have created a VPC. For details, see [Creating a VPC](#).
- You have determined the region where the VPN gateway is to be deployed and obtained the endpoint for calling APIs based on the region.
- You have obtained a user token if you need to use token authentication. In addition, you need to add **X-Auth-Token** to the request header when calling an API. For details about token authentication, see [Authentication](#).

NOTE

The token obtained through IAM is valid for only 24 hours. When using a token for authentication, cache it to avoid frequent calling.

Data Preparation

Table 5-1 Key parameters in the request for creating a VPN gateway

Parameter	Description	Example Value
vpc_id	Specifies the ID of the VPC to which the VPN gateway connects.	cb4a631d-demo-a8df-va86-ca3fa348c36c
local_subnets	Specifies the local CIDR block.	192.168.0.0/24,192.168.1.0/24

Parameter	Description	Example Value
connect_subnet	Specifies the ID of the VPC subnet used by the VPN gateway.	f5741286-demo-a8df-va86-2c82bd9ee114
eip1.id	Specifies the ID of the active EIP used by the VPN gateway.	cff40e5e-demo-a8df-va86-7366077bf097
eip2.id	Specifies the ID of the standby EIP used by the VPN gateway.	d290f1ee-demo-a8df-va86-d701748f0851

Procedure

1. Create a VPN gateway associated with a VPC.

- a. Send **POST** https://{endpoint}/v5/{project_id}/vpn-gateways.
- b. Add **X-Auth-Token** to the request header.
- c. Specify the following parameters in the request body:

```
{
  "vpn_gateway": {
    "vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "local_subnets": [
      "192.168.0.0/24", "192.168.1.0/24"
    ],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "eip1": {
      "id": "cff40e5e-demo-a8df-va86-7366077bf097"
    },
    "eip2": {
      "id": "d290f1ee-demo-a8df-va86-d701748f0851"
    }
  }
}
```

- d. Check the response.

- The request is successful if the following response is displayed. In the response, **id** indicates a VPN gateway ID.

```
{
  "vpn_gateway": {
    "id": "620d99b8-demo-a8df-va86-200b868f2d7d",
    "name": "vpngw-3caf",
    "network_type": "public",
    "attachment_type": "vpc",
    "vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "local_subnets": ["192.168.0.0/24", "192.168.1.0/24"],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "bgp_asn": 64512,
    "access_vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "flavor": "Professional1",
    "used_connection_number": 0,
    "used_connection_group": 0,
    "enterprise_project_id": "0"
  },
  "request_id": "4a739f5c-edb7-4122-b31f-b77fb1b94857"
}
```

2. Query details about the VPN gateway.
 - a. Send **GET** `https://{endpoint}/v5/{project_id}/vpn-gateways/{vgw_id}`.
 - b. Add **X-Auth-Token** to the request header.
 - c. Check the response.
- The request is successful if the following response is displayed. In the response, **id** indicates a VPN gateway ID.

```
{
  "vpn_gateway": {
    "id": "620d99b8-demo-a8df-va86-200b868f2d7d",
    "name": "vpngw-3caf",
    "network_type": "public",
    "status": "ACTIVE",
    "attachment_type": "vpc",
    "vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "local_subnets": [
      "192.168.0.0/24", "192.168.1.0/24"
    ],
    "connect_subnet": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "access_vpc_id": "cb4a631d-demo-a8df-va86-ca3fa348c36c",
    "access_subnet_id": "f5741286-demo-a8df-va86-2c82bd9ee114",
    "bgp_asn": 64512,
    "flavor": "Professional1",
    "availability_zone_ids": [
      "cn-south-1f", "cn-south-1e"
    ],
    "used_connection_number": 0,
    "used_connection_group": 0,
    "enterprise_project_id": "0",
    "eip1": {
      "id": "cff40e5e-demo-a8df-va86-7366077bf097",
      "ip_version": 4,
      "type": "5_bgp",
      "ip_address": "88.***.***.8",
      "charge_mode": "bandwidth",
      "bandwidth_id": "593a1a79-demo-a8df-va86-64ec45fb23f6",
      "bandwidth_size": 300,
      "bandwidth_name": "vpngw-bandwidth-1391"
    },
    "eip2": {
      "id": "d290f1ee-demo-a8df-va86-d701748f0851",
      "ip_version": 4,
      "type": "5_bgp",
      "ip_address": "88.***.***.6",
      "charge_mode": "bandwidth",
      "bandwidth_id": "0abb9d55-demo-a8df-va86-b7500ac2a338",
      "bandwidth_size": 300,
      "bandwidth_name": "vpngw-bandwidth-1392"
    },
    "created_at": "2022-09-15T08:56:09.386Z",
    "updated_at": "2022-09-15T11:13:13.677Z"
  },
  "request_id": "d099a7dc-ea71-45a6-a75b-dccbfe17d438"
}
```

5.2 Example 2: Creating a Customer Gateway

Scenario

This section describes how to create a customer gateway by calling APIs.

Prerequisites

You have obtained a user token if you need to use token authentication. In addition, you need to add **X-Auth-Token** to the request header when calling an API. For details about token authentication, see [Authentication](#).

NOTE

The token obtained through IAM is valid for only 24 hours. When using a token for authentication, cache it to avoid frequent calling.

Data Preparation

Table 5-2 Key parameters in the request for creating a customer gateway

Parameter	Description	Example Value
name	Specifies a customer gateway name.	stub-customer-gateway-id-1
route_mode	Specifies the gateway routing mode.	static
ip	Specifies the IP address of the customer gateway.	10.12.13.21

Procedure

1. Create a customer gateway.
 - a. Send **POST** **https://{endpoint}/v5/{project_id}/customer-gateways**.
 - b. Add **X-Auth-Token** to the request header.
 - c. Specify the following parameters in the request body:

```
{
  "customer_gateway": {
    "name": "cgw-3ebf",
    "id_type": "ip",
    "id_value": "10.***.***.21"
  }
}
```
 - d. Check the response.
 - The request is successful if the following response is displayed. In the response, **id** indicates a customer gateway ID.

```
{
  "customer_gateway": {
    "id": "03c0aa3d-demo-a8df-va86-9d82473765d4",
    "name": "cgw-3ebf",
    "id_type": "ip",
    "id_value": "10.***.***.21",
    "created_at": "2021-12-21T16:49:28.108+08:00",
    "updated_at": "2021-12-21T16:49:28.108+08:00"
  },
  "request_id": "e55783ba-5cc8-40c1-ad81-12cce6f773d2"
}
```
2. Query details about the customer gateway.

- a. Send **GET** `https://{endpoint}/v5/{project_id}/customer-gateways/{customer_gateway_id}`.
- b. Add **X-Auth-Token** to the request header.
- c. Check the response.
 - The request is successful if the following response is displayed. In the response, **id** indicates a customer gateway ID.

```
{
  "customer_gateway": {
    "id": "03c0aa3d-demo-a8df-va86-9d82473765d4",
    "name": "cgw-3ebf",
    "id_type": "ip",
    "id_value": "10.***.***.21",
    "created_at": "2021-12-21T16:49:28.108+08:00",
    "updated_at": "2021-12-21T16:49:28.108+08:00"
  },
  "request_id": "8cf476c4-c3d4-4516-bfbc-01e2473e549b"
}
```

5.3 Example 3: Creating Dual VPN Connections

Scenario

This section describes how to create dual VPN connections by calling APIs.

Prerequisites

- You have created a VPN gateway. For details, see [4.1.1.1 Creating a VPN Gateway](#).
- You have created a customer gateway. For details, see [4.1.2.1 Creating a Customer Gateway](#).
- You have obtained a user token if you need to use token authentication. In addition, you need to add **X-Auth-Token** to the request header when calling an API. For details about token authentication, see [Authentication](#).

NOTE

The token obtained through IAM is valid for only 24 hours. When using a token for authentication, cache it to avoid frequent calling.

Data Preparation

Table 5-3 Key parameters in the request for creating a VPN connection

Parameter	Description	Example Value
vgw_id	Specifies a VPN gateway ID.	8030f6d6-demo-4d20-a7f8-50a7a826e2f8
vgw_ip1	Specifies the ID of EIP 1 of the VPN gateway.	e4d7930f-demo-4cbf-b78a-b004416c7485
vgw_ip2	Specifies the ID of EIP 2 of the VPN gateway.	1fb97767-demo-4d8b-83bb-6f878f662005

Parameter	Description	Example Value
cgw_id	Specifies a customer gateway ID.	8916effb-demo-42d8-83d7-4517567d3d26
peer_subnets	Specifies a customer subnet.	192.168.44.0/24
psk	Specifies a pre-shared key.	abcd****

Procedure

1. Create a VPN connection in static routing mode for a VPN gateway associated with a VPC.

- a. Send **POST** `https://{endpoint}/v5/{project_id}/vpn-connections/batch-create`.
- b. Add **X-Auth-Token** to the request header.
- c. Specify the following parameters in the request body:

```
{
  "vpn_connections": [
    {
      "vgw_ip": "e4d7930f-demo-4cbf-b78a-b004416c7485",
      "cgw_id": "8916effb-demo-42d8-83d7-4517567d3d26",
      "vgw_id": "8030f6d6-demo-4d20-a7f8-50a7a826e2f8",
      "peer_subnets": [
        "192.168.44.0/24"
      ],
      "psk": "abcd****"
    },
    {
      "vgw_ip": "1fb97767-demo-4d8b-83bb-6f878f662005",
      "cgw_id": "8916effb-demo-42d8-83d7-4517567d3d26",
      "vgw_id": "8030f6d6-demo-4d20-a7f8-50a7a826e2f8",
      "peer_subnets": [
        "192.168.44.0/24"
      ],
      "psk": "abcd****"
    }
  ]
}
```

- d. Check the response.

- The request is successful if the following response is displayed. In the response, **id** indicates a VPN connection ID.

```
{
  "vpn_connections": [
    {
      "id": "18be2aa1-demo-410f-832e-4d8ba13b4c5d",
      "name": "vpn-22b6",
      "vgw_id": "8030f6d6-demo-4d20-a7f8-50a7a826e2f8",
      "vgw_ip": "e4d7930f-demo-4cbf-b78a-b004416c7485",
      "style": "STATIC",
      "cgw_id": "8916effb-demo-42d8-83d7-4517567d3d26",
      "peer_subnets": [
        "192.168.44.0/24"
      ],
      "tunnel_local_address": "169.254.135.49/30",
      "tunnel_peer_address": "169.254.135.50/30",
      "enable_nqa": false,
      "policy_rules": [],
      "ikepolicy": {

```

```
    "ike_version": "v2",
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "dh_group": "group15",
    "authentication_method": "pre-share",
    "lifetime_seconds": 86400,
    "local_id_type": "ip",
    "local_id": "10.***.***.128",
    "peer_id_type": "ip",
    "peer_id": "188.***.***.189",
    "dpd": {
      "interval": 30,
      "timeout": 15,
      "msg": "seq-hash-notify"
    }
  },
  "ipsecpolicy": {
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "pfs": "group15",
    "transform_protocol": "esp",
    "lifetime_seconds": 3600,
    "encapsulation_mode": "tunnel"
  },
  "created_at": "2025-03-17T12:25:21.369Z",
  "updated_at": "2025-03-17T12:25:21.369Z",
  "enterprise_project_id": "0",
  "ha_role": "master",
  "tags": [],
  "policy_rules_v6": []
},
{
  "id": "c7e617bd-877f-demo-8af0-44b5f8598116",
  "name": "vpn-e41c",
  "vgw_id": "8030f6d6-demo-4d20-a7f8-50a7a826e2f8",
  "vgw_ip": "1fb97767-demo-4d8b-83bb-6f878f662005",
  "style": "STATIC",
  "cgw_id": "8916effb-demo-42d8-83d7-4517567d3d26",
  "peer_subnets": [
    "192.168.44.0/24"
  ],
  "tunnel_local_address": "169.254.73.253/30",
  "tunnel_peer_address": "169.254.73.254/30",
  "enable_nqa": false,
  "policy_rules": [],
  "ikepolicy": {
    "ike_version": "v2",
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "dh_group": "group15",
    "authentication_method": "pre-share",
    "lifetime_seconds": 86400,
    "local_id_type": "ip",
    "local_id": "215.***.***.55",
    "peer_id_type": "ip",
    "peer_id": "188.***.***.189",
    "dpd": {
      "interval": 30,
      "timeout": 15,
      "msg": "seq-hash-notify"
    }
  },
  "ipsecpolicy": {
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "pfs": "group15",
    "transform_protocol": "esp",
    "lifetime_seconds": 3600,
    "encapsulation_mode": "tunnel"
  }
}
```

```
    },
    "created_at": "2025-03-17T12:25:21.678Z",
    "updated_at": "2025-03-17T12:25:21.678Z",
    "enterprise_project_id": "0",
    "ha_role": "master",
    "tags": [],
    "policy_rules_v6": []
  }
],
"request_id": "a923f31456941e12c5fc9a663a6e630e"
}
```

2. Query details about the VPN connection.

- a. Send **GET** `https://{endpoint}/v5/{project_id}/vpn-connection/{vpn_connection_id}`.
 - b. Add **X-Auth-Token** to the request header.
 - c. Check the response.
- The request is successful if the following response is displayed. In the response, **id** indicates a VPN connection ID.

```
{
  "vpn_connection": {
    "id": "98c5af8a-demo-a8df-va86-ae2280a6f4c3",
    "name": "vpn-1655",
    "status": "DOWN",
    "vgw_id": "b32d91a4-demo-a8df-va86-e907174eb11d",
    "vgw_ip": "0c464dad-demo-a8df-va86-c22bb0eb0bde",
    "style": "STATIC",
    "cgw_id": "5247ae10-demo-a8df-va86-dd36659a7f5d",
    "peer_subnets": ["192.168.44.0/24"],
    "tunnel_local_address": "169.254.56.225/30",
    "tunnel_peer_address": "169.254.56.226/30",
    "enable_nqa": false,
    "ikepolicy": {
      "ike_version": "v2",
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "dh_group": "group15",
      "authentication_method": "pre-share",
      "lifetime_seconds": 86400,
      "local_id_type": "ip",
      "local_id": "10.***.***.134",
      "peer_id_type": "ip",
      "peer_id": "88.***.***.164",
      "dpd": {
        "timeout": 15,
        "interval": 30,
        "msg": "seq-hash-notify"
      }
    },
    "ipsecpolicy": {
      "authentication_algorithm": "sha2-256",
      "encryption_algorithm": "aes-128",
      "pfs": "group15",
      "transform_protocol": "esp",
      "lifetime_seconds": 3600,
      "encapsulation_mode": "tunnel"
    },
    "created_at": "2022-11-26T13:41:34.626Z",
    "updated_at": "2022-11-26T13:41:34.626Z",
    "enterprise_project_id": "0",
    "request_id": "104c5608-b68b-462c-af17-ead2fb5ccee4"
  }
}
```

```
{
  "id": "18be2aa1-demo-410f-832e-4d8ba13b4c5d",
  "name": "vpn-22b6",
  "status": "DOWN",
  "vgw_id": "8030f6d6-demo-4d20-a7f8-50a7a826e2f8",
  "vgw_ip": "e4d7930f-demo-4cbf-b78a-b004416c7485",
  "style": "STATIC",
  "cgw_id": "8916effb-demo-42d8-83d7-4517567d3d26",
  "peer_subnets": [
    "192.168.44.0/24"
  ],
  "tunnel_local_address": "169.254.135.49/30",
  "tunnel_peer_address": "169.254.135.50/30",
  "enable_nqa": false,
  "policy_rules": [],
  "ikepolicy": {
    "ike_version": "v2",
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "dh_group": "group15",
    "authentication_method": "pre-share",
    "lifetime_seconds": 86400,
    "local_id_type": "ip",
    "local_id": "10.***.***.128",
    "peer_id_type": "ip",
    "peer_id": "188.***.***.189",
    "dpd": {
      "interval": 30,
      "timeout": 15,
      "msg": "seq-hash-notify"
    }
  },
  "ipsecpolicy": {
    "authentication_algorithm": "sha2-256",
    "encryption_algorithm": "aes-128",
    "pfs": "group15",
    "transform_protocol": "esp",
    "lifetime_seconds": 3600,
    "encapsulation_mode": "tunnel"
  },
  "created_at": "2025-03-17T12:25:21.369Z",
  "updated_at": "2025-03-17T12:25:21.369Z",
  "enterprise_project_id": "0",
  "ha_role": "master",
  "tags": [],
  "policy_rules_v6": [],
  "eip_id": "e4d7930f-7038-4cbf-b78a-b004416c7485",
  "type": "ROUTE",
  "route_mode": "STATIC"
},
"request_id": "62dc155a7353037f0a1ccc569016a3e9"
}
```

5.4 Example 4: Creating a VPN Connection Monitor

Scenario

This section describes how to create a VPN connection monitor by calling APIs.

Prerequisites

- You have created a VPN connection. For details, see [4.1.3.1 Creating a VPN Connection](#).

- You have obtained a user token if you need to use token authentication. In addition, you need to add **X-Auth-Token** to the request header when calling an API. For details about token authentication, see [Authentication](#).

NOTE

The token obtained through IAM is valid for only 24 hours. When using a token for authentication, cache it to avoid frequent calling.

Data Preparation

Table 5-4 Key parameters in the request for creating a VPN connection monitor

Parameter	Description	Example Value
vpn_connection_id	Specifies the ID of the VPN connection to be monitored.	cae286f2-demo-a8df-va86-e22416ca1220

Procedure

- Create a VPN connection monitor.
 - Send **POST https://{endpoint}/v5/{project_id}/connection-monitors**.
 - Add **X-Auth-Token** to the request header.
 - Specify the following parameters in the request body:

```
{
  "connection_monitor": {
    "vpn_connection_id": "cae286f2-demo-a8df-va86-e22416ca1220"
  }
}
```
 - Check the response.
 - The request is successful if the following response is displayed. In the response, **id** indicates the ID of a VPN connection monitor.

```
{
  "connection_monitor": {
    "id": "76f64229-demo-a8df-va86-3907e2815b6d",
    "vpn_connection_id": "cae286f2-demo-a8df-va86-e22416ca1220",
    "type": "gateway",
    "source_ip": "88.***.***.60",
    "destination_ip": "192.***.***.0",
    "proto_type": "icmp"
  },
  "request_id": "54af23d8-989e-445d-bb48-0a9da33d7f0f"
}
```
- Query details about the VPN connection monitor.
 - Send **GET https://{endpoint}/v5/{project_id}/connection-monitors/{connection_monitor_id}**.
 - Add **X-Auth-Token** to the request header.
 - Check the response.
 - The request is successful if the following response is displayed. In the response, **id** indicates the ID of a VPN connection monitor.

```
{
  "connection_monitor": {
```

```
{
  "id": "76f64229-demo-a8df-va86-3907e2815b6d",
  "status": "ACTIVE",
  "vpn_connection_id": "cae286f2-demo-a8df-va86-e22416ca1220",
  "type": "gateway",
  "source_ip": "88.***.***.60",
  "destination_ip": "192.***.***.0",
  "proto_type": "icmp"
},
"request_id": "72d05395-0637-4f93-9844-b4979e9d7bdc"
}
```

5.5 Example 5: Creating a Server

Scenario

This section describes how to create a VPN server by calling an API.

Prerequisites

- You have created a yearly/monthly P2C VPN gateway.
- You have purchased or uploaded a server certificate in the CCM. For details, see [Purchasing an SSL Certificate](#) or [Uploading an External Certificate](#).
- You have determined the endpoint for calling APIs.
- You have obtained a user token if you need to use token authentication. In addition, you need to add **X-Auth-Token** to the request header when calling an API. For details about token authentication, see [Authentication](#).

NOTE

The token obtained through IAM is valid for only 24 hours. When using a token for authentication, cache it to avoid frequent calling.

Data Preparation

A VPN server supports two authentication modes: certificate authentication and password authentication.

Table 5-5 Key parameters in a request for creating a VPN server in certificate authentication mode

Parameter	Description	Example Value
p2c_vgw_id	Specifies the ID of the P2C VPN gateway that has been created.	595210dc-7998-4ba3-aeb9-516fbcf7853c
client_cidr	Specifies a client CIDR block.	100.10.1.0/24
local_subnets	Specifies the list of local CIDR blocks.	192.168.0.0/24,192.168.1.0/24
server_certificate_id	Specifies a server certificate ID, which can be obtained from the CCM.	scs1717051012106

Parameter	Description	Example Value
client_ca_certificate.content	Specifies the content of client CA certificates.	-----BEGIN CERTIFICATE----- *****-----END CERTIFICATE-----

Table 5-6 Key parameters in a request for creating a VPN server in password authentication mode

Parameter	Description	Example Value
p2c_vgw_id	Specifies the ID of the P2C VPN gateway that has been created.	dea8c4fb-be5c-4d50-be9a-f9a5f3a9afc6
client_cidr	Specifies a client CIDR block.	100.10.2.0/24
local_subnets	Specifies the list of local CIDR blocks.	192.168.0.0/24,192.168.1.0/24
server_certificate.id	Specifies a server certificate ID, which can be obtained from the CCM.	scs1717051012106

Procedure

1. Create a VPN server.
 - a. Send **POST** https://{endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers. {p2c_vgw_id} specifies the ID of the created P2C VPN gateway.
 - b. Add **X-Auth-Token** to the request header.
 - c. Set parameters in the request body.

In certificate authentication mode, the input parameters are as follows:

```
{
  "vpn_server": {
    "tunnel_protocol": "SSL",
    "client_cidr": "100.10.1.0/24",
    "local_subnets": [
      "192.168.0.0/24",
      "192.168.1.0/24"
    ],
    "client_auth_type": "CERT",
    "server_certificate": {
      "id": "scs1717051012106"
    },
    "client_ca_certificates": [
      {
        "content": "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----"
      }
    ],
    "ssl_options": {
      "protocol": "TCP",
      "port": 443,
      "encryption_algorithm": "AES-128-GCM",
```

```
    "is_compressed": false
  }
}
```

In password authentication mode, the input parameters are as follows:

```
{
  "vpn_server": {
    "tunnel_protocol": "SSL",
    "client_cidr": "100.10.2.0/24",
    "local_subnets": [
      "192.168.0.0/24",
      "192.168.1.0/24"
    ],
    "client_auth_type": "LOCAL_PASSWORD",
    "server_certificate": {
      "id": "scs1717051012106"
    },
    "ssl_options": {
      "protocol": "TCP",
      "port": 443,
      "encryption_algorithm": "AES-128-GCM",
      "is_compressed": false
    }
  }
}
```

- d. Check the response.

The request is successful if the following response is displayed. In the response, **id** specifies the ID of the created VPN server.

```
{
  "vpn_server": {
    "id": "0e325fb6-83b9-4004-a343-8b6fc714a5d9"
  },
  "request_id": "bf23a5884def9be4576cff33e4dd78d5"
}
```

2. Query VPN server information.

- a. Send **GET** https://{endpoint}/v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers. **{p2c_vgw_id}** specifies the ID of the created P2C VPN gateway.
- b. Add **X-Auth-Token** to the request header.
- c. Check the response.

If the **status** value of the server is **PENDING_CREATE**, the server is being created. If the **status** value of the server is **ACTIVE**, the server has been created.

The response in certificate authentication mode is as follows:

```
{
  "vpn_servers": [
    {
      "id": "b26c9c74-5bb9-4df8-8b98-ecf2051e3482",
      "p2c_vgw_id": "595210dc-7998-4ba3-aeb9-516fbcf7853c",
      "client_cidr": "100.10.1.0/24",
      "local_subnets": [
        "192.168.0.0/24",
        "192.168.1.0/24"
      ],
      "client_auth_type": "CERT",
      "tunnel_protocol": "SSL",
      "server_certificate": {
        "id": "scs1717051012106",
        "name": "test-05304",
        "issuer": "C=CN,ST=beijing,L=haidian,O=lesaas,OU=root,CN=www.root.huawei.com",

```

```
    "subject":  
    "C=CN,ST=beijing,L=haidian,O=server,OU=server,CN=www.server.huawei.com",  
    "serial_number": "350612543125953290200975245211283057292471206725",  
    "expiration_time": "2024-06-29T06:39:46Z",  
    "signature_algorithm": "SHA256WITHRSA"  
  },  
  "client_ca_certificates": [  
    {  
      "id": "7e971612-f720-4d31-88b5-fc6280b88e36",  
      "name": "ca-cert-123e",  
      "issuer": "C=CN,ST=JS,L=NJ,O=NYS,OU=N10,CN=test.huawei.com",  
      "subject": "C=CN,ST=JS,L=NJ,O=NYS,OU=N10,CN=testCA.huawei.com",  
      "serial_number": "1591942200161",  
      "expiration_time": "2033-11-06T11:39:14Z",  
      "signature_algorithm": "SHA256WITHRSA",  
      "created_at": "2024-06-18T12:19:17.978Z",  
      "updated_at": "2024-06-18T12:19:17.978Z"  
    }  
  ],  
  "ssl_options": {  
    "protocol": "TCP",  
    "port": 443,  
    "encryption_algorithm": "AES-128-GCM",  
    "authentication_algorithm": "SHA256",  
    "is_compressed": false  
  },  
  "status": "ACTIVE",  
  "created_at": "2024-06-18T12:19:17.978Z",  
  "updated_at": "2024-06-18T12:19:17.978Z"  
},  
"request_id": "68188a14243b1b54d0b45a82d9123b98"  
}
```

The response in password authentication mode is as follows:

```
{  
  "vpn_servers": [  
    {  
      "id": "0e325fb6-83b9-4004-a343-8b6fc714a5d9",  
      "p2c_vgw_id": "dea8c4fb-be5c-4d50-be9a-f9a5f3a9afc6",  
      "client_cidr": "100.10.2.0/24",  
      "local_subnets": [  
        "192.168.0.0/24",  
        "192.168.1.0/24"  
      ],  
      "client_auth_type": "LOCAL_PASSWORD",  
      "tunnel_protocol": "SSL",  
      "server_certificate": {  
        "id": "scs1717051012106",  
        "name": "test-05304",  
        "issuer": "C=CN,ST=beijing,L=haidian,O=lesaas,OU=root,CN=www.root.huawei.com",  
        "subject":  
        "C=CN,ST=beijing,L=haidian,O=server,OU=server,CN=www.server.huawei.com",  
        "serial_number": "350612543125953290200975245211283057292471206725",  
        "expiration_time": "2024-06-29T06:39:46Z",  
        "signature_algorithm": "SHA256WITHRSA"  
      },  
      "client_ca_certificates": [],  
      "ssl_options": {  
        "protocol": "TCP",  
        "port": 443,  
        "encryption_algorithm": "AES-128-GCM",  
        "authentication_algorithm": "SHA256",  
        "is_compressed": false  
      },  
      "status": "ACTIVE",  
      "created_at": "2024-06-18T12:21:54.889Z",  
      "updated_at": "2024-06-18T12:21:54.889Z"  
    }  
  ],  
}
```

```
"request_id": "f8e64d41466085f06383dc59ffb28230"
}
```

5.6 Example 6: Creating a User and a User Group

Scenario

This section describes how to create a VPN user and a user group by calling APIs.

Prerequisites

- You have created a P2C VPN gateway.
- You have created a VPN server and set the authentication mode of the server to password authentication. For details, see [Creating a Server](#).
- You have determined the endpoint for calling APIs.
- You have obtained a user token if you need to use token authentication. In addition, you need to add **X-Auth-Token** to the request header when calling an API. For details about token authentication, see [Authentication](#).

NOTE

The token obtained through IAM is valid for only 24 hours. When using a token for authentication, cache it to avoid frequent calling.

Calling the APIs related to users and user groups is an asynchronous process. The configuration takes effect after a period of time. If you frequently perform operations on users or user groups within a short period of time, the queue may be congested due to limited performance, and the error message "VPN.0030, The system is busy, please try later." is returned. In this case, you need to wait for a while before calling the APIs again.

Data Preparation

Table 5-7 Key parameter in the request for creating a user group

Parameter	Description	Example Value
vpn_server_id	Specifies the ID of a VPN server.	0e325fb6-83b9-4004-a343-8b6fc714a5d9

Table 5-8 Key parameter in the request for creating a user

Parameter	Description	Example Value
vpn_server_id	Specifies the ID of a VPN server.	0e325fb6-83b9-4004-a343-8b6fc714a5d9

Procedure

1. Create a user group.

- a. Send **POST** `https://{endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups`. `{vpn_server_id}` specifies the ID of the created VPN server.
- b. Add **X-Auth-Token** to the request header.
- c. Specify the following parameters in the request body:

```
{
  "user_group": {
    "name": "user-group1",
    "description": "UserGroup1"
  }
}
```

- d. Check the response.
 - The request is successful if the following response is displayed. In the response, **id** specifies the ID of the created user group.

```
{
  "user_group": {
    "id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8"
  },
  "request_id": "94d271493e144135423e7377e40127cf"
}
```

2. Query the user group.

- a. Send **GET** `https://{endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}`. `{group_id}` specifies the ID of the created user group.
- b. Add **X-Auth-Token** to the request header.
- c. Check the response.

```
{
  "user_group": {
    "id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
    "name": "user-group1",
    "description": "UserGroup1",
    "type": "Custom",
    "user_number": 0,
    "created_at": "2024-06-17T09:48:27.548Z",
    "updated_at": "2024-06-17T09:48:27.548Z"
  },
  "request_id": "6735d32bb3e35e9154caba1dbc6c2dc6"
}
```

3. Create a user.

- a. Send **POST** `https://{endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users`. `{vpn_server_id}` specifies the ID of the created VPN server.
- b. Add **X-Auth-Token** to the request header.
- c. Specify the following parameters in the request body:

```
{
  "user": {
    "name": "user001",
    "password": "Qwerasdf",
    "description": "User1",
    "user_group_id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8"
  }
}
```

- d. Check the response.
 - The request is successful if the following response is displayed. In the response, **id** specifies the ID of the created user.

```
{
  "user": {
    "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d"
  },
  "request_id": "b19ba5a0be8f7b7f664b14596f8f35db"
}
```

4. Query the user.

- a. Send **GET** `https://{endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}`. `{vpn_server_id}` specifies the ID of the created VPN server. `{user_id}` specifies the ID of the created user.
- b. Add **X-Auth-Token** to the request header.
- c. Check the response.

```
{
  "user": {
    "id": "41ad472e-d3e4-482b-8f00-7b2c1bfc4b7d",
    "name": "user001",
    "description": "User1",
    "user_group_id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
    "user_group_name": "user-group1",
    "created_at": "2024-06-17T06:53:46.302Z",
    "updated_at": "2024-06-17T06:53:46.302Z"
  },
  "request_id": "926a0edb3bf432943e2399b700173add"
}
```

5.7 Example 7: Creating an Access Policy

Scenario

This section describes how to create an access policy by calling an API.

Prerequisites

- You have created a P2C VPN gateway.
- You have created a VPN server and set the authentication mode of the server to password authentication. For details, see [Creating a Server](#).
- You have determined the endpoint for calling APIs.
- You have obtained a user token if you need to use token authentication. In addition, you need to add **X-Auth-Token** to the request header when calling an API. For details about token authentication, see [Authentication](#).

NOTE

The token obtained through IAM is valid for only 24 hours. When using a token for authentication, cache it to avoid frequent calling.

Calling the APIs related to access policies is an asynchronous process. The configuration takes effect after a period of time. If you frequently perform operations on access policies within a short period of time, the queue may be congested due to limited performance, and the error message "VPN.0030, The system is busy, please try later." is returned. In this case, you need to wait for a while before calling the APIs again.

Data Preparation

Table 5-9 Key parameters in the request for creating an access policy

Parameter	Description	Example Value
vpn_server_id	Specifies the ID of a VPN server.	0e325fb6-83b9-4004-a343-8b6fc714a5d9
user_group_id	Specifies the ID of a user group.	7625fd92-2e20-4e4d-8c56-66f110fbfaa8

Procedure

1. Create an access policy.
 - a. Send **POST** **https://{endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies**. {vpn_server_id} specifies the ID of the created VPN server.
 - b. Add **X-Auth-Token** to the request header.
 - c. Specify the following parameters in the request body:

```
{
  "access_policy": {
    "name": "policy-001",
    "user_group_id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
    "description": "AccessPolicy1",
    "dest_ip_cidrs": [
      "172.16.0.0/24",
      "172.16.1.0/24"
    ]
  }
}
```

- d. Check the response.
 - The request is successful if the following response is displayed. In the response, **id** specifies the ID of the created user group.

```
{
  "access_policy": {
    "id": "4f746482-a575-4e1f-9e80-5f6f69ff8588"
  },
  "request_id": "1663cd8cacbb3497ebc88877e5a3ad89"
}
```

2. Query the access policy.
 - a. Send **GET** **https://{endpoint}/v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}**. {vpn_server_id} specifies the ID of the created VPN server. {policy_id} specifies the ID of the created access policy.
 - b. Add **X-Auth-Token** to the request header.
 - c. Check the response.

```
{
  "access_policy": {
    "id": "4f746482-a575-4e1f-9e80-5f6f69ff8588",
    "name": "policy-001",
    "user_group_id": "7625fd92-2e20-4e4d-8c56-66f110fbfaa8",
    "user_group_name": "user-group1",
    "description": "AccessPolicy1",
  }
}
```

```
{  "dest_ip_cidrs": [
    "172.16.0.0/24",
    "172.16.1.0/24"
  ],
  "created_at": "2024-06-17T13:32:19.57Z",
  "updated_at": "2024-06-17T13:32:19.57Z",
},
  "request_id": "85657002f01c35576606003cc36114ab"
}
```

6 Permissions and Supported Actions

6.1 Introduction

You can use Identity and Access Management (IAM) for fine-grained permissions management of your VPN resources. If your Huawei Cloud account does not need individual IAM users, you can skip this section.

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

You can grant users permissions using [Roles](#) and [Policies](#). Roles are provided by IAM to define service-based permissions that match users' job responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

NOTE

Policy-based authorization is useful if you want to allow or deny the access to an API.

An account has permissions to call all APIs. An IAM user under the account can call specific APIs only after being assigned the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user wants to query the VPN gateway list using an API, the user must be granted permissions that allow the **vpn:vpnGateways:list** action.

Supported Actions

VPN provides system-defined policies that can be directly used in IAM. You can also create custom policies to supplement system-defined policies for more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions controlling the operations that users can perform
- APIs called by policies

- Actions supported by policies. They are specific operations that are allowed or denied.
- IAM or enterprise projects on which actions take effect. Policies that contain actions supporting both IAM and enterprise projects can be used and take effect in both IAM and Enterprise Management. Policies that contain actions supporting only IAM projects can be assigned to user groups and take effect only in IAM. Such policies will not take effect if they are assigned to user groups in Enterprise Management. For details about the differences between IAM and enterprise management, see [Differences Between IAM and Enterprise Management](#).

VPN supports the following actions that can be defined in custom policies:

[Example] [VPN gateway](#), including actions supported by VPN gateway APIs, such as the APIs for creating, querying, updating, and deleting VPN gateways, as well as querying the VPN gateway list.

 NOTE

The check mark (√) indicates that an action is supported. The cross symbol (x) indicates that an action is not supported.

6.2 Actions Supported by S2C VPN

6.2.1 VPN Gateway

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a VPN gateway	POST /v5/{project_id}/vpn-gateways	vpn:vpnGateways:create	- er:instances:list - er:instances:get - vpc:vpcs:list - vpc:vpcs:get - vpc:subnets:get - vpc:subnets:list - vpc:subnets:create - vpc:subnets:delete - vpc:subNetworkInterfaces:update - vpc:publicIps:create - vpc:publicIps:delete - vpc:publicIps:update - vpc:publicIps:get - vpc:publicIps:list - vpc:ports:create - vpc:quotas:list - vpc:bandwidths:list - vpc:ports:get - vpc:ports:delete - vpc:routeTables:update - vpc:routeTables:get	√	√

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
			vpc:bandwidths:get		
Querying a VPN gateway	GET /v5/{project_id}/vpn-gateways/{vgw_id}	vpn:vpnGateways:get	- vpc:publicips:get - vpc:publicips:list - vpc:bandwidths:list - er:instances:list - er:instances:get - vpc:vpcs:list - vpc:vpcs:get - vpc:subnets:get - vpc:subnets:list	√	√
Querying the VPN gateway list	GET /v5/{project_id}/vpn-gateways	vpn:vpnGateways:list	- vpc:publicips:get - vpc:publicips:list - vpc:bandwidths:list - er:instances:list - er:instances:get - vpc:vpcs:list - vpc:vpcs:get - vpc:subnets:get - vpc:subnets:list	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Updating a VPN gateway	PUT /v5/{project_id}/vpn-gateways/{vgw_id}	vpn:vpnGateways:update	- er:instances:list - er:instances:get - vpc:vpcs:list - vpc:vpcs:get - vpc:subnets:get - vpc:subnets:list - vpc:subnets:delete - vpc:subNetworkInterfaces:update - vpc:publicIps:delete - vpc:publicIps:update - vpc:publicIps:get - vpc:publicIps:list - vpc:bandwidths:list - vpc:ports:get - vpc:routeTables:update - vpc:routeTables:get	√	√

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Deleting a VPN gateway	DELETE /v5/{project_id}/vpn-gateways/{vgw_id}	vpn:vpnGateways:delete	- er:instances:list - er:instances:get - vpc:vpcs:list - vpc:vpcs:get - vpc:subnets:get - vpc:subnets:delete - vpc:subNetworkInterfaces:update - vpc:publicIps:delete - vpc:publicIps:update - vpc:publicIps:get - vpc:publicIps:list - vpc:bandwidths:list - vpc:ports:get - vpc:ports:delete - vpc:routeTables:update - vpc:routeTables:get	√	√
Querying the AZs of VPN gateways	GET /v5/{project_id}/vpn-gateways/availability-zones	vpn:vpnGatewayAvailabilityZone:list	-	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Querying the AZs of VPN gateways (V5.1)	GET /v5.1/{project_id}/vpn-gateways/availability-zones	vpn:vpnGatewayAvailabilityZone:list	-	√	×
Importing certificates for a VPN gateway	POST /v5/{project_id}/vpn-gateways/{vgw_id}/certificate	vpn:vpnGateways:importCertificate	-	√	√
Querying certificates of a VPN gateway	GET /v5/{project_id}/vpn-gateways/{vgw_id}/certificate	vpn:vpnGateways:getCertificate	-	√	√
Updating certificates of a VPN gateway	PUT /v5/{project_id}/vpn-gateways/{vgw_id}/certificate/{certificate_id}	vpn:vpnGateways:updateCertificate	-	√	√
Querying the route table of a VPN gateway	GET /v5/{project_id}/vpn-gateways/{vgw_id}/routing-table	vpn:vpnGateways:getRoutingTable	-	√	√

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Changing the specification of a pay-per-use VPN gateway	POST /v5/{project_id}/vpn-gateways/{vgw_id}/update-specification	vpn:vpnGateways:updatePostpaidSpecification	- er:instances:list - er:instances:get - vpc:vpcs:list - vpc:vpcs:get - vpc:subnets:get - vpc:subnets:list - vpc:subnets:delete - vpc:subNetworkInterfaces:update - vpc:publicIps:delete - vpc:publicIps:update - vpc:publicIps:get - vpc:publicIps:list - vpc:bandwidths:list - vpc:ports:get - vpc:routeTables:update - vpc:routeTables:get	√	√

6.2.2 Customer Gateway

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a customer gateway	POST /v5/{project_id}/customer-gateways	vpn:customerGateways:create	-	√	x
Querying details about a customer gateway	GET /v5/{project_id}/customer-gateways/{customer_gateway_id}	vpn:customerGateways:get	-	√	x
Querying the customer gateway list	GET /v5/{project_id}/customer-gateways	vpn:customerGateways:list	-	√	x
Updating a customer gateway	PUT /v5/{project_id}/customer-gateways/{customer_gateway_id}	vpn:customerGateways:update	-	√	x
Deleting a customer gateway	DELETE /v5/{project_id}/customer-gateways/{customer_gateway_id}	vpn:customerGateways:delete	-	√	x

6.2.3 VPN Connection

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a VPN connection	POST /v5/{project_id}/vpn-connection	vpn:vpnConnections:create	ces:metricData:list ces:currentRegionSupportedMetrics:list vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:subnets:list vpc:subNetworkInterfaces:update vpc:publicIps:get vpc:publicIps:list vpc:bandwidths:list vpc:ports:get vpc:routeTables:update vpc:routeTables:get	√	√
Querying the VPN connection list	GET /v5/{project_id}/vpn-connection	vpn:vpnConnections:list	vpc:publicIps:get vpc:publicIps:list vpc:bandwidths:list er:instances:list er:instances:get vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:subnets:list	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Querying details about a VPN connection	GET /v5/{project_id}/vpn-connection/{vpn_connection_id}	vpn:vpnConnections:get	vpc:publicIps:get vpc:publicIps:list vpc:bandwidths:list er:instances:list er:instances:get vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:subnets:list	√	√
Updating a VPN connection	PUT /v5/{project_id}/vpn-connection/{vpn_connection_id}	vpn:vpnConnections:update	vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:subnets:list vpc:subNetworkInterfaces:update vpc:publicIps:get vpc:publicIps:list vpc:bandwidths:list vpc:ports:get vpc:routeTables:update vpc:routeTables:get	√	√

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Deleting a VPN connection	DELETE /v5/{project_id}/vpn-connection/{vpn_connection_id}	vpn:vpnConnections:delete	ces:metricData:list ces:currentRegionSupportedMetrics:list vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:subNetworkInterfaces:update vpc:publicIps:get vpc:publicIps:list vpc:bandwidths:list vpc:ports:get vpc:routeTables:update vpc:routeTables:get	√	√

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating VPN connections in batches	POST /v5/{project_id}/vpn-connections/batch-create	vpn:vpnConnections:batchCreate	ces:metricData:list ces:currentRegionSupportedMetrics:list vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:subnets:list vpc:subNetworkInterfaces:update vpc:publicIps:get vpc:publicIps:list vpc:bandwidths:list vpc:ports:get vpc:routeTables:update vpc:routeTables:get	√	√
Querying VPN connection logs	GET /v5/{project_id}/vpn-connection/{vpn_connection_id}/log	vpn:vpnConnections:getLog	-	√	√

6.2.4 VPN Connection Monitor

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a VPN connection monitor	POST /v5/{project_id}/connection-monitors	vpn:connectionMonitors:create	-	√	√
Querying the VPN connection monitor list	GET /v5/{project_id}/connection-monitors	vpn:connectionMonitors:list	-	√	x
Deleting a VPN connection monitor	DELETE /v5/{project_id}/connection-monitors/{connection_monitor_id}	vpn:connectionMonitors:delete	-	√	√
Querying a VPN connection monitor	GET /v5/{project_id}/connection-monitors/{connection_monitor_id}	vpn:connectionMonitors:get	-	√	√

6.3 Actions Supported by P2C VPN

6.3.1 VPN Gateway

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Subscribing to a yearly/monthly P2C VPN gateway	POST /v5/{project_id}/p2c-vpn-gateways/subscribe/{order_id}	vpn:p2cVpnGateway:subscribe	vpn:system:listAvailabilityZones vpc:vpcs:list vpc:subnets:get vpc:bandwidths:list vpc:publicips:create vpc:publicips:delete vpc:publicips:update vpc:publicips:list vpc:quotas:list	√	×
Changing the specification of a yearly/monthly VPN gateway	PUT /v5/{project_id}/p2c-vpn-gateways/update-specification/{order_id}	vpn:p2cVpnGateway:updateSpecification	-	√	×
Updating a P2C VPN gateway	PUT /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}	vpn:p2cVpnGateway:update	vpc:publicips:create vpc:publicips:delete vpc:publicips:update vpc:publicips:get vpc:publicips:list vpc:bandwidths:list	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Querying details about a P2C VPN gateway	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}	vpn:p2cVpnGateway:get	vpc:publicIps:get	√	×
Querying the P2C VPN gateway list	GET /v5/{project_id}/p2c-vpn-gateways	vpn:p2cVpnGateway:list	vpc:publicIps:get	√	×
Querying the P2C VPN connection list	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections	vpn:p2cVpnGateway:listConnections	-	√	×
Disconnecting a connection of a P2C VPN gateway	POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections/{connection_id}/disconnect	vpn:p2cVpnGateway:disconnectConnection	-	√	×

6.3.2 Server

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a P2C VPN server	POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers	vpn:p2cVpnGateway:createServer	scm:cert:get scm:cert:list scm:cert:download vpc:publicIps:get vpc:routeTables:update vpc:subnets:get	√	x
Querying server information on a gateway	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers	vpn:p2cVpnGateway:listServers	-	√	x
Updating server information on a specified gateway	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}	vpn:p2cVpnGateway:updateServer	scm:cert:get scm:cert:list scm:cert:download vpc:publicIps:get vpc:routeTables:update vpc:subnets:get	√	x
Exporting the client configuration information corresponding to a server	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-config/export	vpn:p2cVpnGateway:exportClientConfig	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Verifying the validity of CA certificates	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/client-ca-certificates/check	vpn:system:checkClientCaCertificate	-	√	x
Importing client CA certificates	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates	vpn:p2cVpnGateway:importClientCa	-	√	x
Modifying a client CA certificate	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:updateClientCa	-	√	x
Querying a client CA certificate	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:getClientCa	-	√	x
Deleting a client CA certificate	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:deleteClientCa	-	√	x
Querying information about all servers of a tenant	GET /v5/{project_id}/vpn-servers	vpn:p2cVpnGateway:listAllServers	-	√	x

Permis sion	API	Action	Dependencies	IAM Proj ect	En ter pri se Pr oje ct
Discon necting connec tions of a P2C VPN gatewa y	POST /v5/{project_id}/ p2c-vpn-gateways/ {p2c_vgw_id}/ connections/ {connection_id}/ disconnect	vpn:p2cVpn Gateway:di sconnectCo nnection	-	√	x
Updati ng the P2C VPN connec tion log configu ration	PUT /v5/{project_id}/p2c- vpn-gateways/ {p2c_vgw_id}/log-config	vpn:p2cVpn Gateway:u pdateConn ectionsLog Config	-	√	x
Queryi ng the P2C VPN connec tion log configu ration	GET /v5/{project_id}/p2c- vpn-gateways/ {p2c_vgw_id}/log-config	vpn:p2cVpn Gateway:g etConnecti onsLogConf ig	-	√	x
Deletin g the P2C VPN connec tion log configu ration	DELETE /v5/{project_id}/ p2c-vpn-gateways/ {p2c_vgw_id}/log-config	vpn:p2cVpn Gateway:d eleteConne ctionsLogC onfig	-	√	x

6.3.3 User Management

Permis sion	API	Action	Dependencies	IAM Proj ect	En ter pri se Pr oje ct
Creatin g a VPN user	POST /v5/{project_id}/ p2c-vpn-gateways/vpn- servers/{vpn_server_id}/ users	vpn:p2cVpn User:create	-	√	x
Creatin g VPN users in batche s	POST /v5/{project_id}/ p2c-vpn-gateways/vpn- servers/{vpn_server_id}/ users/batch-create	vpn:p2cVpn User:batch Create	-	√	x
Queryi ng the VPN user list	GET /v5/{project_id}/p2c- vpn-gateways/vpn- servers/{vpn_server_id}/ users	vpn:p2cVpn User:list	-	√	x
Modifi ing a VPN user	PUT /v5/{project_id}/p2c- vpn-gateways/vpn- servers/{vpn_server_id}/ users/{user_id}	vpn:p2cVpn User:updat e	-	√	x
Queryi ng a VPN user	GET /v5/{project_id}/p2c- vpn-gateways/vpn- servers/{vpn_server_id}/ users/{user_id}	vpn:p2cVpn User:get	-	√	x
Deletin g a VPN user	DELETE /v5/{project_id}/ p2c-vpn-gateways/vpn- servers/{vpn_server_id}/ users/{user_id}	vpn:p2cVpn User:delete	-	√	x
Deletin g VPN users in batche s	POST /v5/{project_id}/ p2c-vpn-gateways/vpn- servers/{vpn_server_id}/ users/batch-delete	vpn:p2cVpn User:batch Delete	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Changing the password of a VPN user	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/password	vpn:p2cVpn User:updatePassword	-	√	x
Resetting the password of a VPN user	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/reset-password	vpn:p2cVpn User:resetPassword	-	√	x
Creating a VPN user group	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups	vpn:p2cVpn Gateway:createUserGroup	-	√	x
Querying the VPN user group list	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups	vpn:p2cVpn Gateway:listUserGroup	-	√	x
Modifying a VPN user group	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpn Gateway:updateUserGroup	-	√	x
Querying a VPN user group	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpn Gateway:getUserGroup	-	√	x
Deleting a VPN user group	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpn Gateway:deleteUserGroup	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Adding VPN users to a group	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/add-users	vpn:p2cVpnGateway:addUsers	-	√	x
Removing VPN users from a group	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/remove-users	vpn:p2cVpnGateway:removeUsers	-	√	x
Querying VPN users in a group	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/users	vpn:p2cVpnGateway:listUsersInGroup	-	√	x

6.3.4 Access Policy

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a VPN access policy	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies	vpn:p2cVpnGateway:createAccessPolicy	-	√	x
Querying the VPN access policy list	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies	vpn:p2cVpnGateway:listAccessPolicies	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Modifying a VPN access policy	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:updateAccessPolicy	-	√	x
Querying a VPN access policy	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:getAccessPolicy	-	√	x
Deleting a VPN access policy	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:deleteAccessPolicy	-	√	x

6.4 Actions Supported by Public Service APIs

6.4.1 VPN Quota

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Querying VPN quotas	GET /v5/{project_id}/vpn/quotas	vpn:quota:list	-	√	x

6.4.2 VPN Tag

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a resource tag	POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create	vpn:resourceInstanceTags:create	-	√	√
Deleting tags of a resource	POST /v5/{project_id}/{resource_type}/{resource_id}/tags/delete	vpn:resourceInstanceTags:delete	-	√	√
Querying the list of tags for a specific type of resources	GET /v5/{project_id}/{resource_type}/tags	vpn:resourceTypeTags:list	-	√	x
Querying the resource instance list	POST /v5/{project_id}/{resource_type}/resource-instances/filter	vpn:resourceInstances:list	-	√	x
Querying the resource tag list	GET /v5/{project_id}/{resource_type}/{resource_id}/tags	vpn:resourceInstanceTags:list	-	√	√
Querying the number of resource instances	POST /v5/{project_id}/{resource_type}/resource-instances/count	vpn:resourceInstances:count	-	√	x

A Appendixes

A.1 Obtaining the Project ID

Scenario

A project ID is required by some URLs used for calling APIs. You can obtain the project ID using either of the following methods:

- Obtaining the project ID by calling an API
- Obtaining the project ID from the console

Obtaining the Project ID by Calling an API

You can obtain the project ID by calling the API used to [query project information](#).

The API for obtaining the project ID is **GET https://{IAM endpoint}/v3/projects**. For details about API authentication, see [Authentication](#).

The following is an example response. The value of **id** is the project ID.

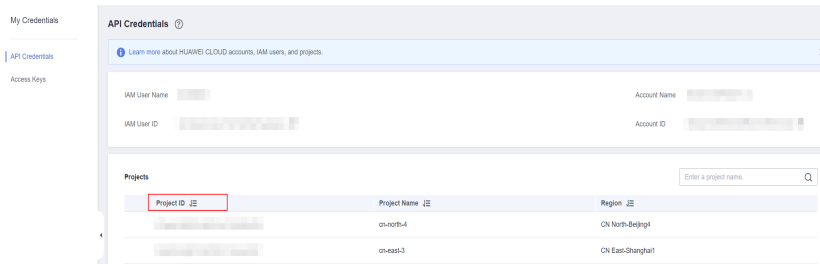
```
{
  "projects": [
    {
      "domain_id": "65382450e8f64ac0870cd180d14e684b",
      "is_domain": false,
      "parent_id": "65382450e8f64ac0870cd180d14e684b",
      "name": "project_name",
      "description": "",
      "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
      },
      "id": "a4a5d4098fb4474fa22cd05f897d6b99",
      "enabled": true
    }
  ],
  "links": {
    "next": null,
    "previous": null,
    "self": "https://www.example.com/v3/projects"
  }
}
```

```
}  
}
```

Obtaining the Project ID from the Console

- Perform the following operations:
1. Log in to the management console.
 2. Click your username in the upper right corner, and choose **My Credentials**.
On the **API Credentials** page, view the project ID in the project list.

Figure A-1 Viewing the project ID



A.2 Status Codes

Table A-1 Status codes returned upon successful operations

Status Code	Type	Description
200	OK	Successful GET or PUT operations
201	Created	Successful POST operations
204	No Content	Successful DELETE operations

Table A-2 Status codes returned upon exceptions

Status Code	Type	Description
400	Bad Request	The server fails to process the request.
401	Unauthorized	A username and password are required for access to the requested page.
403	Forbidden	Access to the requested page is forbidden.
404	Not Found	The requested page is not found.
405	Method Not Allowed	The method specified in the request is not allowed.

Status Code	Type	Description
406	Not Acceptable	The response generated by the server could not be accepted by the client.
407	Proxy Authentication Required	Processing the request requires authentication by a proxy server.
408	Request Timeout	The request times out.
409	Conflict	The request cannot be processed due to a conflict.
500	Internal Server Error	The request is not completed due to a service exception.
501	Not Implemented	The request is not completed because the server does not support the requested function.
502	Bad Gateway	The request is not completed because the server receives an invalid response from the upstream server.
503	Service Unavailable	The request is not completed because the service is unavailable.
504	Gateway Timeout	A gateway timeout error occurs.

A.3 Error Codes

Description

If an error occurs when an API is called, error information is returned. This section describes the error information for VPN APIs (excluding native OpenStack APIs).

Response Format

```
{
  "code": "VPN.0001",
  "message": "invalid request:xxx"
}
```

Error Code Description

If an error code starting with **APIGW** is returned when you call an API, rectify the fault by referring to the instructions provided in [Error Codes](#).

Module	Status Code	Error Code	Error Information	Handling Measure
Common	400	VPN.0001	invalid request:xxx	Contact technical support.
	500	VPN.0002	server error: xxx	Contact technical support.
	403	VPN.0003	Authentication failed: xxx	Obtain the required permissions.
	404	VPN.0004	resource not found	Check whether the resource ID is correct or whether the resource exists under the tenant.
	400	VPN.0030	The system is busy, please try later.	Try again later.
	400	VPN.0031	Repeated operation.	Try again later.
P2C VPN	400	VPN.0070	The key algorithm of the certificate %s is not supported.	Import a certificate with a supported key algorithm.
	400	VPN.0071	The signature algorithm of the certificate %s is not supported.	Import a certificate with a supported signature algorithm.
	400	VPN.0072	Certificate %s has expired.	Import a valid client CA certificate.
	400	VPN.0073	Certificate %s has not taken effect.	Import a valid certificate.
	400	VPN.0074	The format of the certificate %s is invalid.	Import a correct certificate.
	400	VPN.0075	The content of the certificate %s is invalid.	Import a correct certificate.
	400	VPN.0076	Certificate %s is not a CA certificate.	Import a correct certificate.

Module	Status Code	Error Code	Error Information	Handling Measure
	400	VPN.0077	Duplicate certificate: %s.	Delete the duplicate certificate.
	400	VPN.0078	Invalid format of the CRL %s.	Import a correct CRL.
	400	VPN.0079	Invalid content of the CRL %s.	Import a correct CRL.
	400	VPN.0080	Invalid date of the CRL %s.	Import a correct CRL.
	400	VPN.0500	VPC %s is not found.	Check whether the VPC ID is correct.
	400	VPN.0501	Interconnection subnet %s is not found.	Check whether the subnet ID is correct.
	400	VPN.0502	Interconnection subnet %s has insufficient available IP addresses.	Use a subnet with sufficient available IP addresses.
	400	VPN.0503	Interconnection subnet %s does not belong to the VPC %s.	Use a subnet of the specified VPC.
	400	VPN.0504	The number of connections exceeds the upper limit defined by the specification.	Enter a proper number of connections.
	400	VPN.0505	Gateway resources are insufficient.	Contact technical support.
	400	VPN.0506	The gateway is being created, please try again later.	Try again later.

Module	Status Code	Error Code	Error Information	Handling Measure
	400	VPN.0507	The gateway is being updated, please try again later.	Try again later.
	400	VPN.0508	The gateway is being deleted.	Try again later.
	404	VPN.0509	The gateway does not exist.	Check whether the gateway ID is correct.
	500	VPN.0510	The gateway status is abnormal.	Contact technical support.
	500	VPN.0511	The gateway is not ready.	Try again later.
	400	VPN.0512	The gateway already has an EIP bound.	Do not bind an EIP repeatedly.
	400	VPN.0513	Insufficient gateway quota.	Delete unnecessary gateways or apply for a higher gateway quota.
	400	VPN.0514	Two AZs must be specified.	Specify two AZs.
	400	VPN.0515	Duplicate AZs.	Specify a different AZ.
	400	VPN.0550	The EIP bandwidth exceeds the upper limit defined by the specification.	Enter a proper EIP bandwidth.
	400	VPN.0551	EIP %s is not found.	Check whether the EIP ID is correct.
	400	VPN.0552	EIP %s is frozen.	Use an available EIP.
	400	VPN.0553	EIP %s has been bound to an instance.	Use an available EIP.

Module	Status Code	Error Code	Error Information	Handling Measure
	400	VPN.0554	EIP %s does not have exclusive bandwidth.	Use an EIP with exclusive bandwidth.
	400	VPN.0555	EIP %s does not belong to a center.	Use the EIP of a center.
	400	VPN.0556	EIP type %s is invalid.	Use a correct EIP type.
	400	VPN.0557	EIPs of the type %s have been sold out.	Use an available EIP type.
	400	VPN.0558	Incomplete EIP parameters.	Ensure that all necessary EIP parameters are set.
	400	VPN.0559	EIP parameter conflict.	Enter either an EIP ID or other EIP parameters.
	400	VPN.0560	EIP quota not enough.	Increase the EIP quota or release idle EIPs.
	400	VPN.0561	EIP quota not found.	Contact technical support.
	400	VPN.0562	The current gateway version does not support %s feature.	Contact technical support.
	404	VPN.0563	The connection does not exist.	Enter a correct connection ID.
	400	VPN.1100	The server certificate cannot be empty.	Enter server certificate information.
	400	VPN.1101	At least one client CA certificate is required.	Ensure that at least one client CA certificate is available.

Module	Status Code	Error Code	Error Information	Handling Measure
	400	VPN.1102	The number of servers exceeds the upper limit.	Do not create multiple servers for a gateway.
	400	VPN.1103	CIDR block %s is invalid.	Enter a valid CIDR block.
	400	VPN.1104	CIDR block %s is unavailable.	Enter an available CIDR block.
	400	VPN.1105	The number of local subnets exceeds the upper limit.	Enter 20 or fewer local CIDR blocks.
	400	VPN.1106	Duplicate local subnet: %s.	Delete the duplicate local CIDR block.
	400	VPN.1107	The mask length of the client CIDR block must in the range of 16 to 26.	Enter a proper client CIDR block.
	400	VPN.1108	The number of IP addresses in the client CIDR block is less than the number of IP addresses required by gateway connections.	Enter a proper client CIDR block.
	400	VPN.1109	The client CIDR block conflicts with the VPC route %s.	Enter a proper client CIDR block.
	400	VPN.1110	The status of server certificate %s is abnormal.	Check the certificate status.

Module	Status Code	Error Code	Error Information	Handling Measure
	400	VPN.1111	The number of client CA certificates exceeds the upper limit.	Import 10 or fewer client CA certificates.
	400	VPN.1112	Server certificate %s is not found.	Check whether the server certificate ID is correct.
	400	VPN.1113	The server is being created, please try again later.	Try again later.
	400	VPN.1114	The server is being updated, please try again later.	Try again later.
	404	VPN.1115	Client CA certificate %s does not exist.	Check whether the client CA certificate ID is correct.
	404	VPN.1116	The server does not exist.	Check whether the server ID is correct.
	500	VPN.1117	The server status is abnormal.	Contact technical support.
	400	VPN.1118	The local CIDR block cannot be empty.	Enter a local CIDR block.
	400	VPN.1119	The client CIDR block conflicts with the local CIDR block %s.	Enter a proper client CIDR block.
	400	VPN.1120	Client CRL %s not found.	Enter a correct client CRL ID.
	400	VPN.1121	Gateway not bind eip.	Bind an EIP to the gateway and try again.
	400	VPN.1122	There are users on the server. Delete them first.	Delete users and try again.

Module	Status Code	Error Code	Error Information	Handling Measure
	400	VPN.1123	There are user groups on the server. Delete them first.	Delete user groups and try again.
	400	VPN.1124	There are access policies on the server. Delete them first.	Delete access policies and try again.
	400	VPN.1125	There are client CA certificates on the server. Delete them first.	Delete client CA certificates and try again.
	400	VPN.1300	The user group name already exists.	Enter a user group name that does not exist.
	404	VPN.1301	The user group does not exist.	Enter a correct user group ID.
	400	VPN.1302	The username already exists.	Enter a username that does not exist.
	404	VPN.1303	The user does not exist.	Enter a correct user ID.
	400	VPN.1304	The user %s has been added to another user group.	Check whether the user needs to be added to the current user group. If so, remove the user from the original user group first.
	400	VPN.1305	The user %s is not in the current user group.	Check whether the ID of the user to be removed is correct.
	400	VPN.1306	The number of user groups exceeds the upper limit (50).	Check the number of user groups. Ensure that the number of user groups does not exceed the upper limit.

Module	Status Code	Error Code	Error Information	Handling Measure
	400	VPN.1307	The number of users exceeds the upper limit.	Check the number of users, which cannot exceed the maximum number of gateway connections.
	400	VPN.1308	The password complexity does not meet requirements.	Enter a more complex password.
	400	VPN.1309	The password cannot be the username or the reverse of the username.	Enter a password that does not contain the username or the reverse of the username.
	400	VPN.1310	The password contains invalid characters.	Enter a password that contains only uppercase letters, lowercase letters, digits, and the following special characters: '~!@#\$%^&*()-_+=\ []{};,:<.>/? and spaces.
	400	VPN.1311	The new password cannot be the same as the old one.	Enter a password that is different from historical passwords.
	400	VPN.1312	The old password is incorrect.	Enter the correct password.
	400	VPN.1313	The user group has been associated with an access policy. Delete the access policy first.	Delete the associated access policy before deleting the user group.
	400	VPN.1314	The password is weak.	Enter a strong password.
	400	VPN.1315	Duplicate user %s.	Do not enter duplicate user IDs.

Module	Status Code	Error Code	Error Information	Handling Measure
	400	VPN.1316	Operations on the default user group are not allowed.	Do not perform operations on the default user group.
	400	VPN.1317	The username is unavailable.	Enter a correct username.
	400	VPN.1318	User list is empty.	Ensure that the user list is not empty.
	400	VPN.1400	The number of access policies exceeds the upper limit (100).	Check the number of access policies. Ensure that the number of access policies does not exceed the upper limit.
	400	VPN.1401	The access policy does not exist.	Enter a correct access policy ID.
	400	VPN.1402	The number of destination CIDR blocks exceeds the upper limit.	Enter a maximum of 10 destination CIDR blocks.
	400	VPN.1403	The destination CIDR block %s is invalid.	Enter a valid destination CIDR block.
	400	VPN.1404	Duplicate destination CIDR block %s	Do not enter duplicate destination CIDR blocks.
	400	VPN.1801	You have orders in progress and cannot perform the current operation.	Try again after the current order is finished.

B Change History

Table B-1 Change History

Released On	Description
2024-04-03	This issue is the first official release.