Virtual Private Network

API Reference-Enterprise

Issue	01
Date	2024-11-14

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

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. 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.

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 *Virtual Private Network User Guide*.

NOTE

There are two editions of VPN: Classic VPN and Enterprise Edition VPN. This document applies only to Enterprise Edition VPN.

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?" in the *Virtual Private Network User Guide*.

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.

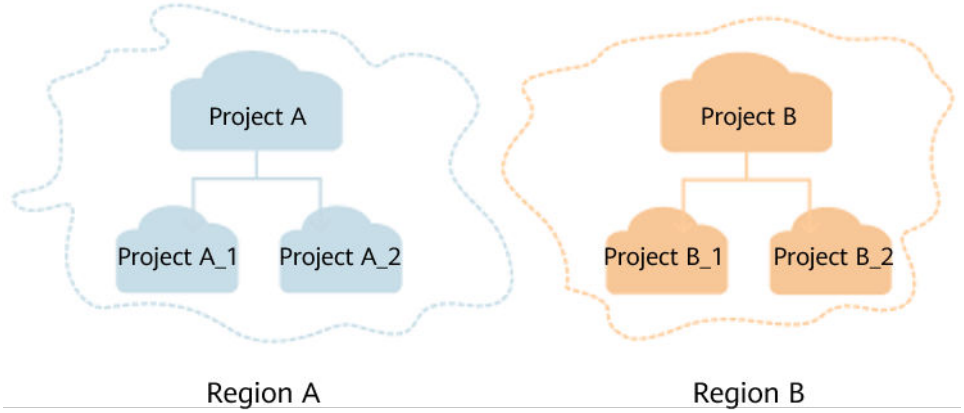
- Availability zone (AZ)

  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
Enterprise Edition API	**VPN Gateway**	APIs for creating, querying, updating, and deleting VPN gateways, and querying AZs of 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.
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 *Parameter name*=*Parameter value*. 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.cn-north-4.myhuaweicloud.com/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=**********
```

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 *Host name:Port number*. 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 *application/json* 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.cn-north-1.myhuaweicloud.com/v3.0/OS-USE//users
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date, Signature=**********
```

Request Body

This part 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.cn-north-4.myhuaweicloud.com/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": "xxxxxxxx"
        }
    }
  }
}
```

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 **ABCDEFJ....**, add **X-Auth-Token: ABCDEFJ....** to the request header as follows:

```
POST https://iam.cn-north-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

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.

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_[redacted]_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 Enterprise Edition VPN API

4.1.1 VPN Gateway

4.1.1.1 Creating a VPN Gateway

Function

This API is used to create a VPN gateway.

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**.

Parameter	Type	Mandatory	Description
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 .
local_subnets	Array of String	No	• Specifies a 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**.

Parameter	Type	Mandatory	Description
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 – GM For details about the features supported by different specifications, see "Product Specifications" in the *Virtual Private Network User Guide*. • 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. • 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.
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**.

Parameter	Type	Mandatory	Description
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**.
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**

Parameter	Type	Mandatory	Description
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.
type	String	No	• Specifies the EIP type. • The value is a string of 0 to 36 characters. • Set this parameter only when a new EIP is used.
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**. The value cannot be greater than 500 when **flavor** is set to **GM**.

Parameter	Type	Mandatory	Description
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**.

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 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	**ResponseVpnGateway** 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**.
certificate_id	String	• Specifies the certificate ID. • The value is a UUID containing 36 characters.
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 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. 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. **GM**: The maximum forwarding bandwidth is 500 Mbit/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",
      "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 private VPN gateway associated with a VPC


```
{
   "vpn_gateway": {
      "id": "80ac167b-demo-a8df-va86-a9a2a23223b8",
      "name": "vpngw-1234",
      "network_type": "private",
      "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": 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 (.).

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**.
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 can be **vpc** or **er**.
certificate_id	String	• Specifies a certificate ID. • The value is a UUID containing 36 characters.
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 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. **GM**: The maximum forwarding bandwidth is 500 Mbit/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 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.

Parameter	Type	Description
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 *yyyy-MM-ddTHH:mm:ssZ*.
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 *yyyy-MM-ddTHH:mm:ssZ*.
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**.
certificate_id	String	• Specifies the ID of the certificate used by the VPN gateway. This parameter is available only when **flavor** is set to **GM**. • 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 4-15 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.

Parameter	Type	Description
ip_billing_info	String	• Specifies the EIP order information. • The value is in the format of *order_id*:*product_id*:*region_id*:*project_id*, 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 "Assigning an EIP" in the *Elastic IP API Reference*.
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_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. • The value is in the format of *order_id*:*product_id*:*region_id*:*project_id*, for example: CS22********LIBIV:00301-******-0--0:br-iaas-odin1:0605768a**********c006c7e484aa

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 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",
```



```
      "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**.

Parameter	Type	Description
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 can be **vpc** or **er**.
certificate_id	String	• Specifies a certificate ID. • The value is a UUID containing 36 characters.
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**.
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.
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. **GM**: The maximum forwarding bandwidth is 500 Mbit/s.

Parameter	Type	Description
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 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 *yyyy-MM-ddTHH:mm:ssZ*.

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 *yyyy-MM-ddTHH:mm:ssZ*.
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**
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.
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 *order_id*:*product_id*:*region_id*:*project_id*, 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 "Assigning an EIP" in the *Elastic IP API Reference*.
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_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.

Parameter	Type	Description
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 *order_id*:*product_id*:*region_id*:*project_id*, for example: CS22********LIBIV:00301-******-0--0:br-iaas-odin1:0605768a**********c006c7e484aa

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 (_ . : = + - @).

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",
      "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_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_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",
      "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_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_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",
    "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_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_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",
      "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_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_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",
      "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",
    "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_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_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 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 can be set only when **attachment_type** is set to **vpc**. 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. • The value is a UUID containing 36 characters. You can set this parameter only when **network_type** is set to **public**.
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. • 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**.
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**.

Parameter	Type	Description
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.

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 can be **vpc**.
certificate_id	String	• Specifies a certificate ID. • The value is a UUID containing 36 characters.
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.
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. **GM**: The maximum forwarding bandwidth is 500 Mbit/s.

Parameter	Type	Description
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.
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.

Parameter	Type	Description
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 *yyyy-MM-ddTHH:mm:ssZ*.
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 *yyyy-MM-ddTHH:mm:ssZ*.
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**.

Parameter	Type	Description
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.
ip_billing_info	String	• Specifies the EIP order information. • The value is in the format of *order_id*:*product_id*:*region_id*:*project_id*, 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 "Assigning an EIP" in the *Elastic IP API Reference*.
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_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 *order_id*:*product_id*:*region_id*:*project_id*, for example: CS22********LIBIV:00301-******-0--0:br-iaas-odin1:0605768a**********c006c7e484aa

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**.

Parameter	Type	Description
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 4-40 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 (_ . : = + - @).
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",
        "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_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_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 **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": {
      "flavor": "Basic"
   }
}
```

Response

- Response parameters

  Returned status code 200: successful operation

Table 4-45 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 4-46 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 can be **vpc** or **er**.
certificate_id	String	• Specifies a certificate ID. • The value is a UUID containing 36 characters.
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. **GM**: The maximum forwarding bandwidth is 500 Mbit/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 *yyyy-MM-ddTHH:mm:ssZ*.
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 *yyyy-MM-ddTHH:mm:ssZ*.
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. • The value is in the format of *order_id*:*product_id*:*region_id*:*project_id*, 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 "Assigning an EIP" in the *Elastic IP API Reference*.

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_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 *order_id*:*product_id*:*region_id*:*project_id*, for example: CS22********LIBIV:00301-******-0--0:br-iaas-odin1:0605768a**********c006c7e484aa

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",
        "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_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_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.

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.
gm	**VpnGatewayAvailabilityZones** object	Indicates that the specification of VPN gateways is GM.

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.

- Example response

```
{
   "availability_zones": {
          "vpc": ["cn-south-1f"],
          "er": []
      },
      "professional1": {
          "vpc": ["cn-south-1f", "cn-south-1e", "cn-south-1c"],
          "er": ["cn-south-1f"]
      },
      "professional2": {
          "vpc": ["cn-south-1f", "cn-south-1e", "cn-south-1c"],
          "er": ["cn-south-1f"]
      },
     "gm": {
          "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 Uploading Certificates for a VPN Gateway

Function

This API is used to upload certificates and private keys for a VPN gateway of the GM specification.

Calling Method

For details, see **3 Calling APIs**.

URI

POST /v5/{project_id}/vpn-gateways/{vgw_id}/certificate

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 the ID of a VPN gateway of the GM specification.

Request

- Request parameters

Table 4-58 CreateVpnGatewayCertificateRequestBody

Parameter	Type	Mandatory	Description
certificate	**CreateVpnGatewayCertificateRequestBodyContent** object	Yes	Specifies the VPN gateway certificate object.

Table 4-59 CreateVpnGatewayCertificateRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	• Specifies the certificate name of a VPN gateway. • The value is a string of 3 to 63 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, **cert-a45b**.
certificate	String	Yes	• Specifies a signature certificate. • The value is a string of 1 to 4096 characters. The certificate must be a non-CA certificate of the SM type.
private_key	String	Yes	• Specifies the private key of the SM signature certificate. • The value is a string of 1 to 4096 characters. The value matches the public key of the signature certificate.
certificate_chain	String	Yes	• Specifies the content of a CA certificate. • The value is a string of 1 to 8192 characters. The certificate must be an SM CA certificate.
enc_certificate	String	Yes	• Specifies an encryption certificate. • The value is a string of 1 to 4096 characters. The certificate must be a non-CA certificate of the SM type.
enc_private_key	String	Yes	• Specifies the private key of the SM encryption certificate. • The value is a string of 1 to 4096 characters. The value matches the public key of the encryption certificate.

- Example request


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

{
   "certificate": {
      "name": "cert-dce7",
      "certificate": "-----BEGIN CERTIFICATE-----******-----END CERTIFICATE-----",
      "private_key": "-----BEGIN EC PRIVATE KEY-----*******-----END EC PRIVATE KEY-----",
      "enc_certificate": "-----BEGIN CERTIFICATE-----********-----END CERTIFICATE-----",
      "enc_private_key": "-----BEGIN EC PRIVATE KEY-----********-----END EC PRIVATE KEY-----",
      "certificate_chain": "-----BEGIN CERTIFICATE-----******-----END CERTIFICATE-----"
   }
}
```

Response

- Response parameters

  Returned status code 201: successful operation

Table 4-60 Parameters in the response body

Parameter	Type	Description
certificate	**VpnGatewayCertificateConfig** object	Specifies the VPN gateway certificate object.
request_id	String	Specifies a request ID.

Table 4-61 VpnGatewayCertificateConfig

Parameter	Type	Description
id	String	• Specifies the certificate ID of a VPN gateway. • The value is a UUID containing 36 characters.
name	String	• Specifies the certificate name of a VPN gateway. • The value is a string of 3 to 63 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.
issuer	String	• Specifies the issuer of the SM signature certificate. • The value is a string of 1 to 256 characters.

Parameter	Type	Description
signature_algorithm	String	• Specifies the signature algorithm of the SM signature certificate. • The value is a string of 1 to 64 characters.
certificate_serial_number	String	• Specifies the serial number of the SM signature certificate. • The value is a string of 1 to 64 characters.
certificate_subject	String	• Specifies the subject of the signature certificate. • The value is a string of 1 to 256 characters.
certificate_expire_time	String	• Specifies the time when the SM signature certificate expires.
certificate_chain_serial_number	String	• Specifies the serial number of the CA certificate. • The value is a string of 1 to 64 characters.
certificate_chain_subject	String	• Specifies the subject of the CA certificate. • The value is a string of 1 to 256 characters.
certificate_chain_expire_time	String	• Specifies the time when the CA certificate expires.
enc_certificate_serial_number	String	• Specifies the serial number of the SM encryption certificate. • The value is a string of 1 to 64 characters.
enc_certificate_subject	String	• Specifies the subject of the encryption certificate. • The value is a string of 1 to 256 characters.
enc_certificate_expire_time	String	• Specifies the time when the SM encryption certificate expires.
created_at	String	• Specifies the creation time.

- Example response

```
{
    "certificate": {
        "id": "73f072d8-demo-a8df-va86-2a755d95636f",
        "name": "cert-dce7",
        "vgw_id": "c7f1d3e3-0476-4a71-95a7-3ce8cbb969de",
```



```
      "issuer": "C=CN,ST=Beijing,L=HaiDian,O=GMCert.org,CN=GMCert GM Root CA - 01",
      "signature_algorithm": "SM3WITHSM2",
      "certificate_serial_number": "16548506527294397241",
      "certificate_subject": "C=CN,ST=beijing,L=beijing,O=huawei,OU=vpn,CN=hwcloud-vpn",
      "certificate_expire_time": "2024-02-20T15:41:39+08:00",
      "certificate_chain_serial_number": "12369133709000538078",
      "certificate_chain_subject": "C=CN,ST=Beijing,L=HaiDian,O=GMCert.org,CN=GMCert GM Root CA
- 01",
      "certificate_chain_expire_time": "2039-07-11T20:31:33+08:00",
      "enc_certificate_serial_number": "16548506527294397242",
      "enc_certificate_subject": "C=CN,ST=beijing,L=beijing,O=huawei,OU=vpn,CN=hwcloud-vpn",
      "enc_certificate_expire_time": "2024-02-20T15:43:26+08:00",
      "created_at": "2023-03-30T10:47:16.657+08:00"
   }
}
```


Status Codes

For details, see **A.2 Status Codes**.

4.1.1.9 Querying VPN Gateway Certificate Details

Function

This API is used to query imported certificates of 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}/certificate

Table 4-62 Parameter description

Parameter	Type	Description
project_id	String	Specifies a project ID.
vgw_id	String	Specifies the ID of a VPN gateway instance.

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v5/{project_id}/vpn-gateways/{vgw_id}/certificate

Response

- Response parameters

  Returned status code 200: successful query

Table 4-63 Parameters in the response body

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

Table 4-64 VpnGatewayCertificate

Parameter	Type	Description
id	String	• Specifies the certificate ID of a VPN gateway. • The value is a UUID containing 36 characters.
name	String	• Specifies the certificate name of a VPN gateway. • The value is a string of 3 to 63 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
project_id	String	• Specifies the project ID of a tenant. • The value is a string of 1 to 64 characters.
vgw_id	String	• Specifies a VPN gateway ID. • The value is a UUID containing 36 characters.
status	String	• Specifies the gateway certificate status. • The value can be **BOUND**, **FAULT**, or **BINDING**.
issuer	String	• Specifies the issuer of the SM signature certificate. • The value is a string of 1 to 256 characters.
signature_algorithm	String	• Specifies the signature algorithm of the SM signature certificate. • The value is a string of 1 to 64 characters.

Parameter	Type	Description
certificate_serial_number	String	• Specifies the serial number of the SM signature certificate. • The value is a string of 1 to 64 characters.
certificate_subject	String	• Specifies the subject of the signature certificate. • The value is a string of 1 to 256 characters.
certificate_expire_time	String	• Specifies the time when the SM signature certificate expires.
certificate_chain_serial_number	String	• Specifies the serial number of the CA certificate. • The value is a string of 1 to 64 characters.
certificate_chain_subject	String	• Specifies the subject of the CA certificate. • The value is a string of 1 to 256 characters.
certificate_chain_expire_time	String	• Specifies the time when the CA certificate expires.
enc_certificate_serial_number	String	• Specifies the serial number of the SM encryption certificate. • The value is a string of 1 to 64 characters.
enc_certificate_subject	String	• Specifies the subject of the encryption certificate. • The value is a string of 1 to 256 characters.
enc_certificate_expire_time	String	• Specifies the time when the SM encryption certificate expires.
created_at	String	• Specifies the creation time.
updated_at	String	• Specifies the update time.

- Example response

```
{
   "certificate":
      {
         "id": "18b81966-demo-a8df-va86-51db2ae6cfbd",
         "name": "cert-ces-test",
         "project_id": "06057689f680d5762f7fc008c77b8891",
         "vgw_id": "b1e94931-demo-a8df-va86-ec906c458ba7",
         "status": "BOUND",
         "issuer": "C=CN,ST=Beijing,L=HaiDian,O=GMCert.org,CN=GMCert GM Root CA - 01",
```



```
        "signature_algorithm": "SM3WITHSM2",
        "certificate_serial_number": "16548506527294397241",
        "certificate_subject": "C=CN,ST=beijing,L=beijing,O=huawei,OU=vpn,CN=hwcloud-vpn",
        "certificate_expire_time": "2023-03-21T07:41:39Z",
        "certificate_chain_serial_number": "12369133709000538078",
        "certificate_chain_subject": "C=CN,ST=Beijing,L=HaiDian,O=GMCert.org,CN=GMCert GM Root
CA - 01",
        "certificate_chain_expire_time": "2023-03-21T01:31:33Z",
        "enc_certificate_serial_number": "16548506527294397242",
        "enc_certificate_subject": "C=CN,ST=beijing,L=beijing,O=huawei,OU=vpn,CN=hwcloud-vpn",
        "enc_certificate_expire_time": "2023-03-21T07:43:26Z",
        "created_at": "2023-03-14T07:48:13.705Z",
        "updated_at": "2023-03-14T07:48:13.887Z"
    }
}
```


Status Codes

For details, see **A.2 Status Codes**.

4.1.1.10 Updating Certificate Information of a VPN Gateway

Function

This API is used to update the certificate information of a tenant's VPN gateway of the GM specification, including the certificate name, signature certificate, signature private key, encryption certificate, encryption private key, and CA certificate chain.

Calling Method

For details, see **3 Calling APIs**.

URI

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

Table 4-65 Parameter in a request

Parameter	Type	Description
project_id	String	Specifies a project ID.
vgw_id	String	Specifies the ID of a VPN gateway instance.
certificate_id	String	Specifies the certificate ID of a VPN gateway.

Request

- Request parameters

Table 4-66 UpdateVpnGatewayCertificateRequestBody

Parameter	Type	Mandatory	Description
certificate	**UpdateVpnGatewayCertificateRequestBodyContent** object	Yes	Specifies the VPN gateway certificate object.

Table 4-67 UpdateVpnGatewayCertificateRequestBodyContent

Parameter	Type	Mandatory	Description
name	String	No	• Specifies the certificate name of a VPN gateway. • The value is a string of 3 to 63 characters, which can contain digits, letters, underscores (_), hyphens (-), and periods (.).
certificate	String	No	• Specifies the content of the SM signature certificate. This parameter is optional if only the certificate name is to be updated. • The value is a string of 1 to 4096 characters.
private_key	String	No	• Specifies the private key of the SM signature certificate. This parameter is optional if only the certificate name is to be updated. • The value is a string of 1 to 4096 characters.
certificate_chain	String	No	• Specifies the content of the CA certificate. This parameter is optional if only the certificate name is to be updated. • The value is a string of 1 to 8192 characters.

Parameter	Type	Mandatory	Description
enc_certificate	String	No	• Specifies the content of the SM encryption certificate. This parameter is optional if only the certificate name is to be updated. • The value is a string of 1 to 4096 characters.
enc_private_key	String	No	• Specifies the private key of the SM encryption certificate. This parameter is optional if only the certificate name is to be updated. • The value is a string of 1 to 4096 characters.

- Example request

```
POST https://{Endpoint}/v5/{project_id}/vpn-gateways/{vgw_id}/certificate/{certificate_id}

{
   "certificate": {
      "name": "cert-dce7",
      "certificate": "-----BEGIN CERTIFICATE-----******-----END CERTIFICATE-----",
      "private_key": "-----BEGIN EC PRIVATE KEY-----*******-----END EC PRIVATE KEY-----",
      "enc_certificate": "-----BEGIN CERTIFICATE-----********-----END CERTIFICATE-----",
      "enc_private_key": "-----BEGIN EC PRIVATE KEY-----********-----END EC PRIVATE KEY-----",
      "certificate_chain": "-----BEGIN CERTIFICATE-----******-----END CERTIFICATE-----"
   }
}
```

Response

- Response parameters

  Returned status code 200: successful operation

  Table 4-68 Parameters in the response body

Parameter	Type	Description
certificate	**VpnGatewayCertificateConfig** object	Specifies the VPN gateway certificate object.
request_id	String	Specifies a request ID.

Table 4-69 VpnGatewayCertificateConfig

Parameter	Type	Description
id	String	• Specifies the certificate ID of a VPN gateway. • The value is a UUID containing 36 characters.
name	String	• Specifies the certificate name of a VPN gateway. • The value is a string of 3 to 63 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.
issuer	String	• Specifies the issuer of the SM signature certificate. • The value is a string of 1 to 256 characters.
signature_algorithm	String	• Specifies the signature algorithm of the SM signature certificate. • The value is a string of 1 to 64 characters.
certificate_serial_number	String	• Specifies the serial number of the SM signature certificate. • The value is a string of 1 to 64 characters.
certificate_subject	String	• Specifies the subject of the SM signature certificate. • The value is a string of 1 to 256 characters.
certificate_expire_time	String	• Specifies the time when the SM signature certificate expires.
certificate_chain_serial_number	String	• Specifies the serial number of the SM CA certificate. • The value is a string of 1 to 64 characters.
certificate_chain_subject	String	• Specifies the subject of the SM CA certificate. • The value is a string of 1 to 256 characters.

Parameter	Type	Description
certificate_chain_expire_time	String	• Specifies the time when the SM CA certificate expires.
enc_certificate_serial_number	String	• Specifies the serial number of the SM encryption certificate. • The value is a string of 1 to 64 characters.
enc_certificate_subject	String	• Specifies the subject of the SM encryption certificate. • The value is a string of 1 to 256 characters.
enc_certificate_expire_time	String	• Specifies the time when the SM encryption certificate expires.
created_at	String	• Specifies the creation time.

- Example response

```
{
   "certificate": {
      "id": "73f072d8-demo-a8df-va86-2a755d95636f",
      "name": "cert-dce7",
      "vgw_id": "c7f1d3e3-0476-4a71-95a7-3ce8cbb969de",
      "issuer": "C=CN,ST=Beijing,L=HaiDian,O=GMCert.org,CN=GMCert GM Root CA - 01",
      "signature_algorithm": "SM3WITHSM2",
      "certificate_serial_number": "16548506527294397241",
      "certificate_subject": "C=CN,ST=beijing,L=beijing,O=huawei,OU=vpn,CN=hwcloud-vpn",
      "certificate_expire_time": "2024-02-20T15:41:39+08:00",
      "certificate_chain_serial_number": "12369133709000538078",
      "certificate_chain_subject": "C=CN,ST=Beijing,L=HaiDian,O=GMCert.org,CN=GMCert GM Root CA
- 01",
      "certificate_chain_expire_time": "2039-07-11T20:31:33+08:00",
      "enc_certificate_serial_number": "16548506527294397242",
      "enc_certificate_subject": "C=CN,ST=beijing,L=beijing,O=huawei,OU=vpn,CN=hwcloud-vpn",
      "enc_certificate_expire_time": "2024-02-20T15:43:26+08:00",
      "created_at": "2023-03-30T10:47:16.657+08:00"
   }
}
```

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 4-70 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 4-71 Request parameters

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

Table 4-72 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. • Value range: – ip – fqdn • The default value is **ip**.

Parameter	Type	Mandatory	Description
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. When **id_type** is set to **fqdn**, the value is a string of characters that can contain uppercase letters, lowercase letters, digits, and special characters. Spaces and the following special characters are not supported: & < > [ ] \ ?.
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**.
ca_certificate	**CaCertificateRequest** object	No	• Specifies the CA certificate of the customer gateway. This parameter is mandatory when you create a customer gateway that uses SM series cryptographic algorithms.
tags	Array of **VpnResourceTag** object	No	• Specifies a tag list. • A maximum of 20 tags can be specified.

Table 4-73 CaCertificateRequest

Parameter	Type	Mandatory	Description
id	String	No	• Specifies a certificate ID. • The value is a UUID containing 36 characters.

Parameter	Type	Mandatory	Description
content	String	No	• Specifies the content in the CA certificate of the customer gateway. • The value is a string of 1 to 8192 characters.

Table 4-74 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,
        "ca_certificate": {
            "content":"******"
        }
    }
}
```

Response

- Response parameters

  Returned status code 201: successful creation

Table 4-75 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 4-76 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 (_), and hyphens (-).
id_type	String	• Specifies the identifier type of a customer gateway. • Value range: – ip – fqdn
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**.
ca_certificate	**CaCertificate** object	Specifies the CA certificate information of the customer gateway. This parameter is available only when the customer gateway has a CA certificate bound.
created_at	String	• Specifies the time when the customer gateway is created. • The UTC time format is *yyyy-MM-ddTHH:mm:ss.SSSZ*.
updated_at	String	• Specifies the last update time. • The UTC time format is *yyyy-MM-ddTHH:mm:ss.SSSZ*.

Parameter	Type	Description
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-77 CaCertificate

Parameter	Type	Description
id	String	Specifies a certificate ID.
serial_number	String	Specifies the serial number of the certificate.
signature_algorithm	String	Specifies the signature algorithm.
issuer	String	Specifies the certificate issuer.
subject	String	Specifies the certificate subject.
expire_time	String	Specifies the time when the certificate expires.
is_updatable	boolean	Indicates whether the certificate content can be updated.

Table 4-78 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-2abf",
    "id_type": "ip",
```



```
        "id_value": "10.***.***.21",
        "bgp_asn": 65000,
        "ca_certificate": {
            "serial_number": "14257156674311863338",
            "signature_algorithm": "SM3WITHSM2",
            "issuer": "C=CN,O=a0002,CN=XXX",
            "subject": "C=CN,O=a0002,CN=XXX",
            "expire_time": "2024-05-22T07:34:22Z",
            "is_updatable": true
        },
        "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 4-79 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

  None

- Example request

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


Response

- Response parameters

  Returned status code 200: successful query

  Table 4-80 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 4-81 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. • Value range: – ip – fqdn
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**.
ca_certificate	CaCertificate object	Specifies the CA certificate information of the customer gateway. This parameter is available only when the customer gateway has a CA certificate bound.

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

Table 4-82 CaCertificate

Parameter	Type	Description
id	String	Specifies a certificate ID.
serial_number	String	Specifies the serial number of the certificate.
signature_algorithm	String	Specifies the signature algorithm.
issuer	String	Specifies the certificate issuer.
subject	String	Specifies the certificate subject.
expire_time	String	Specifies the time when the certificate expires.
is_updatable	boolean	Indicates whether the certificate content can be updated.

Table 4-83 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-ba08",
      "id_type": "ip",
      "id_value": "10.***.***.21",
      "bgp_asn": 65000,
      "ca_certificate": {
         "serial_number": "14257156674311863338",
         "signature_algorithm": "SM3WITHSM2",
         "issuer": "C=CN,O=a0002,CN=XXX",
         "subject": "C=CN,O=a0002,CN=XXX",
         "expire_time": "2024-05-22T07:34:22Z",
         "is_updatable": true
      },
      "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 4-84 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 4-85 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 4-86 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 4-87 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. • Value range: – ip – fqdn
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**.
ca_certificate	**CaCertificate** object	Specifies the CA certificate information of the customer gateway. This parameter is available only when the customer gateway has a CA certificate bound.

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

Table 4-88 CaCertificate

Parameter	Type	Description
id	String	Specifies a certificate ID.
serial_number	String	Specifies the serial number of the certificate.
signature_algorithm	String	Specifies the signature algorithm.
issuer	String	Specifies the certificate issuer.
subject	String	Specifies the certificate subject.
expire_time	String	Specifies the time when the certificate expires.
is_updatable	boolean	Indicates whether the certificate content can be updated.

Table 4-89 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 (_ . : = + - @).

Table 4-90 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,
      "ca_certificate": {
          "serial_number": "14257156674311863338",
          "signature_algorithm": "SM3WITHSM2",
          "issuer": "C=CN,O=a0002,CN=XXX",
          "subject": "C=CN,O=a0002,CN=XXX",
          "expire_time": "2024-05-22T07:34:22Z",
          "is_updatable": true
      },
      "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",
      "ca_certificate": null,
      "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 and certificate 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 4-91 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 4-92 Request parameters

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

Table 4-93 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 (.).
ca_certificate	CaCertificateRequest object	No	• Specifies the CA certificate of the customer gateway.

Table 4-94 CaCertificateRequest

Parameter	Type	Mandatory	Description
id	String	No	• Specifies a certificate ID. • The value is a UUID containing 36 characters.
content	String	No	• Specifies the content in the CA certificate of the customer gateway. • The value is a string of 1 to 8192 characters.

- Example request

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

{
   "customer_gateway": {
      "name": "cgw-f846",
      "ca_certificate": {
         "content":"******"
      }
   }
}
```

Response

- Response parameters

  Returned status code 200: successful update

Table 4-95 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 4-96 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. • Value range: – ip – fqdn
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 *yyyy-MM-ddTHH:mm:ss.SSSZ*.
updated_at	String	• Specifies the last update time. • The UTC time format is *yyyy-MM-ddTHH:mm:ss.SSSZ*.
ca_certificate	**CaCertificate** object	Specifies the CA certificate information of the customer gateway. This parameter is available only when the customer gateway has a CA certificate bound.

Parameter	Type	Description
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-97 CaCertificate

Parameter	Type	Description
id	String	Specifies a certificate ID.
serial_number	String	Specifies the serial number of the certificate.
signature_algorithm	String	Specifies the signature algorithm.
issuer	String	Specifies the certificate issuer.
subject	String	Specifies the certificate subject.
expire_time	String	Specifies the time when the certificate expires.
is_updatable	boolean	Indicates whether the certificate content can be updated.

Table 4-98 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-f846",
    "id_type": "ip",
```



```
        "id_value": "10.***.***.21",
        "bgp_asn": 65533,
        "ca_certificate": {
            "serial_number": "14257156674311863338",
            "signature_algorithm": "SM3WITHSM2",
            "issuer": "C=CN,O=a0002,CN=XXX",
            "subject": "C=CN,O=a0002,CN=XXX",
            "expire_time": "2024-05-22T07:34:22Z",
            "is_updatable": true
        },
        "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 4-99 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 4-100 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 4-101 Request parameters

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

Table 4-102 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 **flavor** is set to **GM** for the VPN gateway, ensure that certificates have been imported for the VPN gateway. 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 **policy-template**: policy template mode • The default value is **static**.
cgw_id	String	Yes	• Specifies a customer gateway ID. • The value is a UUID containing 36 characters. When **flavor** is set to **GM** for the VPN gateway, ensure that a certificate has been imported for the customer gateway.

Parameter	Type	Mandatory	Description
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.
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, 169.254.76.2/30. • 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**.
psk	String	No	• Specifies a pre-shared key. This parameter is mandatory when **flavor** is not set to **GM** for the VPN gateway. • 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.

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

Table 4-103 PolicyRule

Parameter	Type	Mandatory	Description
rule_index	Integer	No	• Specifies a rule ID, which is used to identify the sequence in which the rule is configured. You are advised not to set this parameter. • The value ranges from 0 to 50. • The value of **rule_index** in each policy rule must be unique. The value of **rule_index** in **ResponseVpnConnection** may be different from the value of this parameter. This is because if multiple destination CIDR blocks are specified, the VPN service generates a rule for each destination CIDR block.
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 4-104 IkePolicy

Parameter	Type	Mandatory	Description
ike_version	String	No	• Specifies the IKE version. • Value range: When **flavor** is set to **GM** for the VPN gateway, the value can only be **v1**. In other scenarios, the value can be **v1** or **v2**. • Default value: When **flavor** is set to **GM** for the VPN gateway, the default value is **v1**. In other scenarios, the default value is **v2**.
phase1_negotiation_mode	String	No	• Specifies the negotiation mode. • Value range: When **flavor** is set to **GM** for the VPN gateway, the value can only be **main**. In other scenarios, the value can be **main** or **aggressive**. **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: When **flavor** is set to **GM** for the VPN gateway, the value can only be **sm3**. In other scenarios, the value can be **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**. Exercise caution when using **sha1** and **md5** as they have low security. • Default value: When **flavor** is set to **GM** for the VPN gateway, the default value is **sm3**. In other scenarios, the default value is **sha2-256**.
encryption_algorithm	String	No	• Specifies an encryption algorithm. • Value range: When **flavor** is set to **GM** for the VPN gateway, the value can only be **sm4**. In other scenarios, the value can be **aes-256-gcm-16**, **aes-128-gcm-16**, **aes-256**, **aes-192**, **aes-128**, or **3des**. Exercise caution when using **3des** as it has low security. • Default value: When **flavor** is set to **GM** for the VPN gateway, the default value is **sm4**. In other scenarios, the default value is **aes-128**.

Parameter	Type	Mandatory	Description
dh_group	String	No	• Specifies the DH group used for key exchange in phase 1. You do not need to set this parameter when **flavor** is set to **GM** for the VPN gateway. • 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 **digital-envelope-v2**: SM digital envelope • Default value: **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. You do not need to set this parameter when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn • The default value is **ip**.

Parameter	Type	Mandatory	Description
local_id	String	No	• Specifies the local ID. You do not need to set this parameter when **flavor** is set to **GM** for the VPN gateway. • The value can contain a maximum of 255 case-sensitive characters, including letters, digits, and special characters (excluding & < > [ ] \). Spaces are not supported. Set this parameter when **local_id_type** is set to **fqdn**. The value must be the same as that of **peer_id** on the peer device.
peer_id_type	String	No	• Specifies the peer ID type. You do not need to set this parameter when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn • The default value is **ip**.
peer_id	String	No	• Specifies the peer ID. You do not need to set this parameter when **flavor** is set to **GM** for the VPN gateway. • The value can contain a maximum of 255 case-sensitive characters, including letters, digits, and special characters (excluding & < > [ ] \). Spaces are not supported. Set this parameter when **peer_id_type** is set to **fqdn**. The value must be the same as that of **local_id** on the peer device.
dpd	**Dpd** object	No	Specifies the dead peer detection (DPD) object.

Table 4-105 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 4-106 IpsecPolicy

Parameter	Type	Mandatory	Description
authentication_algorithm	String	No	• Specifies an authentication algorithm. • Value range: When **flavor** is set to **GM** for the VPN gateway, the value can only be **sm3**. In other scenarios, the value can be **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**. Exercise caution when using **sha1** and **md5** as they have low security. • Default value: When **flavor** is set to **GM** for the VPN gateway, the default value is **sm3**. In other scenarios, the default value is **sha2-256**.
encryption_algorithm	String	No	• Specifies an encryption algorithm. • Value range: When **flavor** is set to **GM** for the VPN gateway, the value can only be **sm4**. In other scenarios, the value can be **aes-256-gcm-16**, **aes-128-gcm-16**, **aes-256**, **aes-192**, **aes-128**, or **3des**. Exercise caution when using **3des** as it has low security. • Default value: When **flavor** is set to **GM** for the VPN gateway, the default value is **sm4**. In other scenarios, the default value is **aes-128**.

Parameter	Type	Mandatory	Description
pfs	String	No	• Specifies the DH key group used by Perfect Forward Secrecy (PFS). You do not need to set this parameter when **flavor** is set to **GM** for the VPN gateway. • 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 4-107 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": [{
         "rule_index": 1,
         "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"
      }
   }
}
```

d. Create a VPN connection in static routing mode, which is set up using SM series cryptographic algorithms.

   Prerequisites:

   A VPN gateway of the GM specification has been created, and SM certificates have been imported for it. You have obtained the **vgw_id** value of this VPN gateway.

   A customer gateway that uses an SM series cryptographic algorithm has been created, and a certificate has been imported for it. You have obtained the **cgw_id** value of this customer gateway.

```
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"
      ]
   }
}
```

Response

- Response parameters

Returned status code 201: successful operation

Table 4-108 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 4-109 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 (_), 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 **POLICY-TEMPLATE**: policy template mode
cgw_id	String	• Specifies a customer gateway ID. • The value is a UUID containing 36 characters.
peer_subnets	Array of String	Specifies a customer subnet.

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 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 *yyyy-MM-ddTHH:mm:ssZ*.
updated_at	String	• Specifies the last update time. • The UTC time format is *yyyy-MM-ddTHH:mm:ssZ*.
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**.

Parameter	Type	Description
tags	Array of VpnResourceTag objects	Specifies a tag list.

Table 4-110 PolicyRule

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

Table 4-111 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 **sm3**, **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.
encryption_algorithm	String	• Specifies an encryption algorithm. • The value can be **sm4**, **aes-256-gcm-16**, **aes-128-gcm-16**, **aes-256**, **aes-192**, **aes-128**, or **3des**.

Parameter	Type	Description
dh_group	String	• Specifies the DH group used for key exchange in phase 1. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • 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 **digital-envelope-v2**: SM digital envelope
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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn
local_id	String	Specifies the local ID. When **local_id_type** is set to **ip**, the VPN gateway IP address corresponding to the VPN connection is returned. When **local_id_type** is set to **fqdn**, the local ID specified during VPN connection creation or update is returned. This parameter is not available when **flavor** is set to **GM** for the VPN gateway.
peer_id_type	String	• Specifies the peer ID type. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn

Parameter	Type	Description
peer_id	String	Specifies the peer ID. When **peer_id_type** is set to **ip**, the IP address of the customer gateway is returned. When **peer_id_type** is set to **fqdn**, the peer ID specified during VPN connection creation or update is returned. This parameter is not available when **flavor** is set to **GM** for the VPN gateway.
dpd	**Dpd** object	Specifies the DPD object.

Table 4-112 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 4-113 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	• Specifies an authentication algorithm. • The value can be **sm3**, **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.
encryption_algorithm	String	• Specifies an encryption algorithm. • The value can be **sm4**, **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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • 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 4-114 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": "sha2-512",
            "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 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 4-115 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 4-116 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 4-117 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).
style	String	• Specifies the connection mode. • Value range: **POLICY**: policy-based mode **STATIC**: static routing mode **BGP**: BGP routing mode **POLICY-TEMPLATE**: policy template mode
cgw_id	String	• Specifies a customer gateway ID. • The value is a UUID containing 36 characters.

Parameter	Type	Description
peer_subnets	Array of String	Specifies a customer subnet.
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**.
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 *yyyy-MM-ddTHH:mm:ssZ*.
updated_at	String	• Specifies the last update time. • The UTC time format is *yyyy-MM-ddTHH:mm:ssZ*.
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.

Parameter	Type	Description
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 4-118 PolicyRule

Parameter	Type	Description
rule_index	Integer	• Specifies a rule ID. • The value ranges from 0 to 50.
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 4-119 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 **sm3**, **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.

Parameter	Type	Description
encryption_algorithm	String	• Specifies an encryption algorithm. • The value can be **sm4**, **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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • 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 **digital-envelope-v2**: SM digital envelope
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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn
local_id	String	Specifies the local ID. When **local_id_type** is set to **ip**, the VPN gateway IP address corresponding to the VPN connection is returned. When **local_id_type** is set to **fqdn**, the local ID specified during VPN connection creation or update is returned. This parameter is not available when **flavor** is set to **GM** for the VPN gateway.

Parameter	Type	Description
peer_id_type	String	• Specifies the peer ID type. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn
peer_id	String	Specifies the peer ID. When **peer_id_type** is set to **ip**, the IP address of the customer gateway is returned. When **peer_id_type** is set to **fqdn**, the peer ID specified during VPN connection creation or update is returned. This parameter is not available when **flavor** is set to **GM** for the VPN gateway.
dpd	**Dpd** object	Specifies the DPD object.

Table 4-120 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 4-121 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	• Specifies an authentication algorithm. • The value can be **sm3**, **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.
encryption_algorithm	String	• Specifies an encryption algorithm. • The value can be **sm4**, **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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • 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 4-122 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


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


Status Codes

For details, see **A.2 Status Codes**.

4.1.3.3 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 4-123 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 4-124 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.
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.

Parameter	Type	Mandatory	Description
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

  a. Query all VPN connections.
  ```
  GET https://{Endpoint}/v5/{project_id}/vpn-connection
  ```

  b. Query VPN connections of a specified vgw_ip.
  ```
  GET https://{Endpoint}/v5/{project_id}/vpn-connection?
  vgw_ip={vgw_ip}&limit={limit}&marker={marker}
  ```

  c. 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 4-125 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.
request_id	String	Specifies a request ID.
total_count	Long	Specifies the total number of a tenant's connections.

Table 4-126 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).
style	String	• Specifies the connection mode. • Value range: **POLICY**: policy-based mode **STATIC**: static routing mode **BGP**: BGP routing mode **POLICY-TEMPLATE**: policy template mode
cgw_id	String	• Specifies a customer gateway ID. • The value is a UUID containing 36 characters.

Parameter	Type	Description
peer_subnets	Array of String	Specifies a customer subnet.
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**.
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 *yyyy-MM-ddTHH:mm:ssZ*.
updated_at	String	• Specifies the last update time. • The UTC time format is *yyyy-MM-ddTHH:mm:ssZ*.
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.

Parameter	Type	Description
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 4-127 PolicyRule

Parameter	Type	Description
rule_index	Integer	• Specifies a rule ID. • The value ranges from 0 to 50.
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 4-128 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 **sm3**, **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.

Parameter	Type	Description
encryption_algorithm	String	• Specifies an encryption algorithm. • The value can be **sm4**, **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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • 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 **digital-envelope-v2**: SM digital envelope
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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn
local_id	String	Specifies the local ID. When **local_id_type** is set to **ip**, the VPN gateway IP address corresponding to the VPN connection is returned. When **local_id_type** is set to **fqdn**, the local ID specified during VPN connection creation or update is returned. This parameter is not available when **flavor** is set to **GM** for the VPN gateway.

Parameter	Type	Description
peer_id_type	String	• Specifies the peer ID type. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn
peer_id	String	Specifies the peer ID. When **peer_id_type** is set to **ip**, the IP address of the customer gateway is returned. When **peer_id_type** is set to **fqdn**, the peer ID specified during VPN connection creation or update is returned. This parameter is not available when **flavor** is set to **GM** for the VPN gateway.
dpd	**Dpd** object	Specifies the DPD object.

Table 4-129 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 4-130 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	• Specifies an authentication algorithm. • The value can be **sm3**, **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.
encryption_algorithm	String	• Specifies an encryption algorithm. • The value can be **sm4**, **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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • 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 4-131 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 (_ . : = + - @).

Table 4-132 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": [{
                "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": 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": [
        {
          "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": 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": [
            {
               "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": 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**.

4.1.3.4 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 4-133 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 4-134 Request parameters

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

Table 4-135 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 a 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**. – 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.
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. This parameter cannot be updated when **flavor** is set to **GM** for the VPN gateway. • 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 4-136 PolicyRule

Parameter	Type	Mandatory	Description
rule_index	Integer	No	• Specifies a rule ID, which is used to identify the sequence in which the rule is configured. You are advised not to set this parameter. • The value ranges from 0 to 50. • The value of **rule_index** in each policy rule must be unique. The value of **rule_index** in **ResponseVpnConnection** may be different from the value of this parameter. This is because if multiple destination CIDR blocks are specified, the VPN service generates a rule for each destination CIDR block.
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 4-137 UpdateIkePolicy

Parameter	Type	Mandatory	Description
ike_version	String	No	• Specifies the IKE version. • Value range: – When **flavor** is set to **GM** for the VPN gateway, the value can only be **v1**. – In other scenarios, the value can be **v1** or **v2**. • Default value: – When **flavor** is set to **GM** for the VPN gateway, the default value is **v1**. – In other scenarios, the default value is **v2**.
phase1_negotiation_mode	String	No	• Specifies the negotiation mode. • Value range: When **flavor** is set to **GM** for the VPN gateway, the value can only be **main**. In other scenarios, the value can be **main** or **aggressive**. **main**: ensures high security during negotiation. **aggressive**: ensures fast negotiation and a high negotiation success rate. • This parameter takes effect only for IKEv1.
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: – When **flavor** is set to **GM** for the VPN gateway, the value can only be **sm3**. – In other scenarios, the value can be **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**. Exercise caution when using **sha1** and **md5** as they have low security.

Parameter	Type	Mandatory	Description
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: When **flavor** is set to **GM** for the VPN gateway, the value can only be **sm4**. In other scenarios, the value can be **aes-256-gcm-16**, **aes-128-gcm-16**, **aes-256**, **aes-192**, **aes-128**, or **3des**. Exercise caution when using **3des** as it has 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. This parameter cannot be modified when **flavor** is set to **GM** for the VPN gateway. • 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.
local_id_type	String	No	• Specifies the local ID type. This parameter cannot be modified when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn

Parameter	Type	Mandatory	Description
local_id	String	No	• Specifies the local ID. This parameter cannot be modified when **flavor** is set to **GM** for the VPN gateway. • The value can contain a maximum of 255 case-sensitive characters, including letters, digits, and special characters (excluding & < > [ ] \). Spaces are not supported. Set this parameter when **local_id_type** is set to **fqdn**. The value must be the same as that of **peer_id** on the peer device.
peer_id_type	String	No	• Specifies the peer ID type. This parameter cannot be modified when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn
peer_id	String	No	• Specifies the peer ID. This parameter cannot be modified when **flavor** is set to **GM** for the VPN gateway. • The value can contain a maximum of 255 case-sensitive characters, including letters, digits, and special characters (excluding & < > [ ] \). Spaces are not supported. Set this parameter when **peer_id_type** is set to **fqdn**. The value must be the same as that of **local_id** on the peer device.
dpd	**UpdateDpd** object	No	Specifies the DPD object.

Table 4-138 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.
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 4-139 UpdateIpsecPolicy

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: When **flavor** is set to **GM** for the VPN gateway, the value can only be **sm3**. In other scenarios, the value can be **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.

Parameter	Type	Mandatory	Description
encryption_algorithm	String	No	• Specifies an encryption algorithm. Exercise caution when using 3DES as it has low security. The modification of this field takes effect only after SAs in phase 2 are aged. • Value range: When **flavor** is set to **GM** for the VPN gateway, the value can only be **sm4**. In other scenarios, the value can be **aes-256-gcm-16**, **aes-128-gcm-16**, **aes-256**, **aes-192**, **aes-128**, or **3des**.
pfs	String	No	• Specifies the DH key group used by PFS. This parameter does not take effect and cannot be modified when **flavor** is set to **GM** for the VPN gateway. • 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.

Parameter	Type	Mandatory	Description
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": [{
         "rule_index": 1,
         "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 4-140 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 4-141 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 (_), 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 **POLICY-TEMPLATE**: policy template mode
cgw_id	String	• Specifies a customer gateway ID. • The value is a UUID containing 36 characters.
peer_subnets	Array of String	Specifies a customer subnet.

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 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 *yyyy-MM-ddTHH:mm:ssZ*.
updated_at	String	• Specifies the last update time. • The UTC time format is *yyyy-MM-ddTHH:mm:ssZ*.
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.

Parameter	Type	Description
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 4-142 PolicyRule

Parameter	Type	Description
rule_index	Integer	• Specifies a rule ID. • The value ranges from 0 to 50.
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 4-143 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 **sm3**, **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.

Parameter	Type	Description
encryption_algorithm	String	• Specifies an encryption algorithm. • The value can be **sm4**, **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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • 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 **digital-envelope-v2**: SM digital envelope
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. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – fqdn
local_id	String	Specifies the local ID. When **local_id_type** is set to **ip**, the VPN gateway IP address corresponding to the VPN connection is returned. This parameter is not available when **flavor** is set to **GM** for the VPN gateway.

Parameter	Type	Description
peer_id_type	String	• Specifies the peer ID type. This parameter is not available when **flavor** is set to **GM** for the VPN gateway. • Value range: – ip – any – fqdn
peer_id	String	Specifies the peer ID. When **peer_id_type** is set to **ip**, the IP address of the customer gateway is returned. This parameter is not available when **flavor** is set to **GM** for the VPN gateway.
dpd	**Dpd** object	Specifies the DPD object.

Table 4-144 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 4-145 IpsecPolicy

Parameter	Type	Description
authentication_algorithm	String	• Specifies an authentication algorithm. • The value can be **sm3**, **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, or **md5**.
encryption_algorithm	String	• Specifies an encryption algorithm. • The value can be **sm4**, **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 4-146 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 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": [{
         "rule_index": 1,
         "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**.

4.1.3.5 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 4-147 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**.

4.1.4 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 4-148 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 4-149 Request parameters

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

Table 4-150 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 4-151 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 4-152 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 4-153 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**.
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 4-154 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 4-155 ConnectionMonitorInfo

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

Parameter	Type	Description
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 4-156 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 4-157 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

  a. Query all VPN connection monitors.

  ```
  GET https://{Endpoint}/v5/{project_id}/connection-monitors
  ```

  b. 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 4-158 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 4-159 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-ede922f7d63c"
}
```


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 4-160 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 Public Service APIs

4.2.1 VPN Quota

4.2.1.1 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 4-161 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**.

Request

- Request parameters
  None
- Example request


```
GET https://{Endpoint}/v5/{project_id}/vpn/quotas
```

Response

- Response parameters

  Returned status code 200: successful query

  Table 4-162 Parameters in the response body

Parameter	Type	Description
quotas	**Quotas** object	Specifies the quotas object.
request_id	String	Specifies a request ID.

  Table 4-163 Quotas

Parameter	Type	Description
resources	Array of **QuotaInfo** objects	Specifies the resources object.

  Table 4-164 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**.

4.2.2 VPN Tag

4.2.2.1 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 4-165 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**.
resource_type	String	Yes	• Specifies the resource type. • The value can be one of the following: **vpn-gateway**, **customer-gateway**, **vpn-connection**.

Table 4-166 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.
offset	Integer	No	• Specifies the index position. The query starts from the (*offset value* + 1)th data record. • The minimum value is 0. • The default value is 0.

Request

- Request parameters

Table 4-167 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 4-168 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 sting of 0 to 255 characters. • A maximum of 20 values can be specified.

Table 4-169 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 sting 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 4-170 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 4-171 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 4-172 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": "resouece1",
      "tags": [{
         "key": "key1",
         "value": "value1"
      }]
   }],
   "total_count": 1000
}
```

Status Codes

For details, see **A.2 Status Codes**.

4.2.2.2 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 4-173 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**.

Request

- Request parameters

Table 4-174 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 4-175 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 sting of 0 to 255 characters. • A maximum of 20 values can be specified.

Table 4-176 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 sting 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 4-177 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**.

4.2.2.3 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 4-178 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**.
resource_type	String	Yes	• Specifies the resource type. • The value can be one of the following: **vpn-gateway**, **customer-gateway**, **vpn-connection**.
resource_id	String	Yes	Indicates a resource ID.

Request

- Request parameters

Table 4-179 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 4-180 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**.

4.2.2.4 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 4-181 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**.
resource_id	String	Yes	Indicates a resource ID.

Request

- Request parameters

Table 4-182 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 4-183 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**.

4.2.2.5 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 4-184 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**.
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 4-185 Parameters in the response body

Parameter	Type	Description
tags	Array of **ResourceTag** objects	Specifies the list of resource tags.

Table 4-186 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**.

4.2.2.6 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 4-187 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**.

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 4-188 Parameters in the response body

Parameter	Type	Description
tags	Array of **ResourceTag** objects	Specifies the list of resource tags.

  Table 4-189 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 a VPN Gateway

Scenario

This section describes how to create a VPN gateway by calling an API.

Prerequisites

- You have created a VPC. For details, see "Creating a VPC" in the *Virtual Private Cloud User Guide*.
- 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" in the *Virtual Private Cloud API Reference*.

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_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_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" in the *Virtual Private Cloud API Reference*.

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 a VPN Connection

Scenario

This section describes how to create a VPN connection 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" in the *Virtual Private Cloud API Reference*.

  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.	b32d91a4-demo-a8df-va86-e907174eb11d
vgw_ip	Specifies an EIP ID of the VPN gateway.	0c464dad-demo-a8df-va86-c22bb0eb0bde

Parameter	Description	Example Value
cgw_id	Specifies a customer gateway ID.	5247ae10-demo-a8df-va86-dd36659a7f5d
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-connection**.
   b. Add **X-Auth-Token** to the request header.
   c. Specify the following parameters in the request body:

```
{
    "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****"
    }
}
```

   d. 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",
        "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": "f74da97d-aa27-4f62-a87c-a33b5706964b"
}
```


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"
}
```


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" in the *Virtual Private Cloud API Reference*.

  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

1. Create a VPN connection monitor.
   a. Send **POST https://{endpoint}/v5/{project_id}/connection-monitors**.
   b. Add **X-Auth-Token** to the request header.
   c. Specify the following parameters in the request body:

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

   d. 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"
}
```

2. Query details about the VPN connection monitor.
   a. Send **GET https://{endpoint}/v5/{project_id}/connection-monitors/{connection_monitor_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 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"
}
```


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 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" in the *IAM User Guide*.

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

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:bandwidths:list • vpc:ports:get • vpc:ports:delete • vpc:routeTables:update • vpc:routeTables:get	√	√

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
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:routeTables:update • vpc:routeTables:get	√	√
Querying the AZs of VPN gateways	GET /v5/{project_id}/vpn-gateways/availability-zones	vpn:vpnGatewayAvailabilityZone:list	-	√	×

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	√	√

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	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
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	-	√	x
Querying a VPN connection monitor	GET /v5/{project_id}/connection-monitors/{connection_monitor_id}	vpn:connectionMonitors:get	-	√	x

6.3 Actions Supported by Public Service APIs

6.3.1 VPN Quota

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Querying VPN quotas	GET /v5/{project_id}/vpn/quotas	vpn:quota:list	-	√	×

6.3.2 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	-	√	x
Deleting tags of a resource	POST /v5/{project_id}/{resource_type}/{resource_id}/tags/delete	vpn:resourceInstanceTags:delete	-	√	x
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	-	√	x
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" in the *Virtual Private Cloud API Reference*.

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.

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.
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.

Status Code	Type	Description
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.

Module	Status Code	Error Code	Error Information	Handling Measure
	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.1318	User list is empty.	Ensure that the user list is not empty.	

B Change History

Table B-1 Change History

Released On	Description
2024-11-14	This issue is the first official release.

