Virtual Private Network

Service Overview

Issue	01
Date	2025-02-05

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

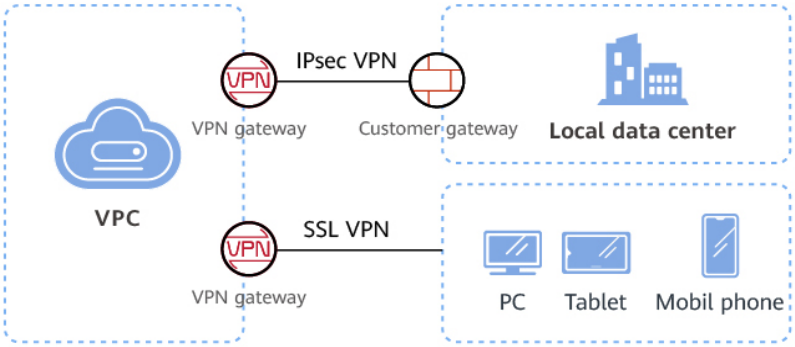
1 VPN Infographics

Getting to Know Huawei Cloud VPN

Secure, flexible,
and convenient communications over
easy-to-use encrypted connections

What Is Virtual Private Network?

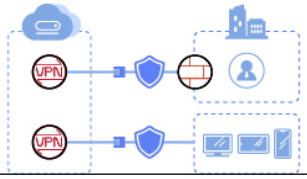
A Virtual Private Network (VPN) establishes secure, reliable, and cost-effective encrypted connections between your local network, data center, or terminals and a Huawei Cloud VPC.



Why Huawei Cloud VPN?

High Security

Data is encrypted using IKE/IPsec or SSL, and there are dedicated gateways for enhanced security.



High Availability

2 What Is VPN?

Overview

Virtual Private Network (VPN) establishes secure, reliable, and cost-effective encrypted connections between your on-premises network or data center and a virtual network on the cloud.

NOTE

Cross-border VPN connections cannot be established between the Chinese mainland and other regions.

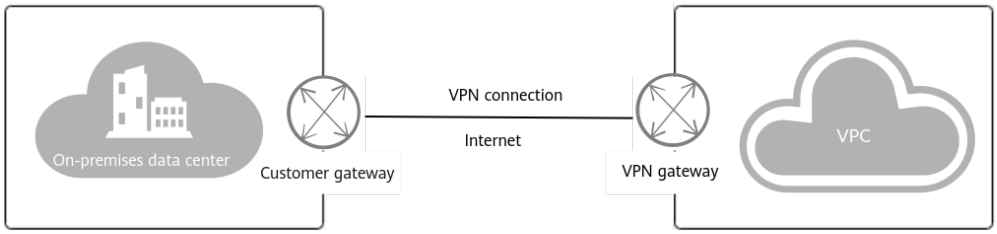
VPN falls into two categories: Site-to-Cloud VPN (S2C VPN) and Point-to-Cloud VPN (P2C VPN), which apply to different scenarios. S2C VPN uses the Internet Protocol Security (IPsec) protocol, and P2C VPN uses the Secure Sockets Layer (SSL) protocol.

S2C VPN involves three key components: VPN gateway, customer gateway, and VPN connection.

- A VPN gateway provides an Internet egress for a Virtual Private Cloud (VPC) to connect to a customer gateway in your on-premises data center.
- A VPN connection connects a VPN gateway to a customer gateway through encrypted tunnels, enabling communication between a VPC and your on-premises data center. This helps quickly establish a secure hybrid cloud environment.

Figure 2-1 shows the S2C VPN networking.

Figure 2-1 S2C VPN networking

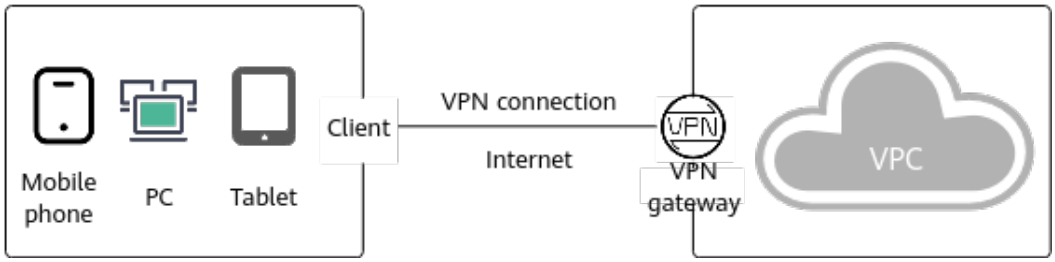


P2C VPN involves three key components: VPN gateway, server, and client.

- A VPN gateway provides an Internet egress for a VPC and is bound to a server.
- A server encapsulates and decapsulates data packets, and defines the port, encryption algorithm, and CIDR blocks for communicating with clients.
- A client establishes a VPN connection with a server to remotely access cloud resources or services.

Figure 2-2 shows the P2C VPN networking.

Figure 2-2 P2C VPN networking



Components

S2C VPN

- **VPN gateway**: a virtual gateway of VPN on the cloud. It establishes secure private connections with a customer gateway in your on-premises network or data center.
- **Customer gateway**: a resource that provides information to the cloud about your customer gateway device. It can be a physical device or software application in your on-premises data center.
- **VPN connection**: a secure channel between a VPN gateway and a customer gateway. VPN connections use the Internet Key Exchange (IKE) and IPsec protocols to encrypt the transmitted data.

P2C VPN

- **VPN gateway**: a virtual gateway of VPN on the cloud. It establishes secure private connections with clients.
- **Server**: a functional module of a virtual gateway. It provides SSL services for configuration management and client connection authentication.
- **Client**: VPN client software deployed on user terminals.

Accessing the VPN Service

You can access the VPN service through the web-based management console.

- If you have registered an account, log in to the management console and choose **Networking** > **Virtual Private Network** to log in to the VPN console.
- If you do not have an account, register one first by referring to "Signing up for a HUAWEI ID and Enabling Huawei Cloud Services" in **Preparations**.

3 Product Advantages

VPN has the following advantages:

- **High security**
  - Data is encrypted using IKE/IPsec or SSL, ensuring high data security.
  - A VPN gateway is exclusive to a tenant, isolating tenants from each other.
  - Multiple encryption algorithms such as AES and SM series algorithms are supported, meeting a range of security requirements.
  - Multiple authentication modes are supported, including certificate authentication and password authentication.
- **High availability**
  - A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.
  - Active-active gateways are deployed in different availability zones (AZs) to ensure AZ-level high availability.
  - High availability (HA) mode: S2C VPN supports active/standby and active-active modes. P2C VPN supports the active/standby mode.
- **Cost-effectiveness**
  - IPsec connections over the Internet provide a cost-effective alternative to Direct Connect.
  - A VPN gateway can be bound to elastic IP addresses (EIPs) that share bandwidth, reducing bandwidth costs.
  - The bandwidth can be adjusted when an EIP instance is created.
  - Access via non-fixed IP addresses reduces access costs in typical scenarios.
- **Easy to use**
  - A VPN gateway supports multiple connection modes, including policy-based, static routing, and BGP routing, to meet different access requirements of customer gateways.
  - A VPN gateway on the cloud can function as a VPN hub, enabling on-premises branch sites to access each other.

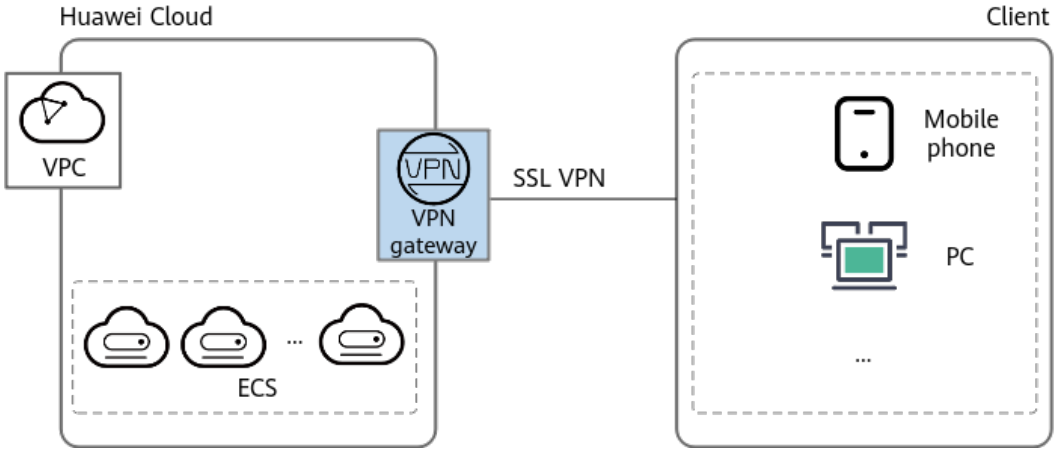
- A VPN connection can be created in a few simple steps on the VPN device in an on-premises data center and on the VPN console, and is ready to use immediately after being created.
- VPN can be used together with the enterprise router service, allowing enterprises to build more flexible cloud-based networks.
- Backup between VPN and Direct Connect is supported, and automatic failover is supported.
- Private VPN gateways are supported to encrypt traffic transmitted over Direct Connect connections, improving data transmission security.
- Terminals running different operating systems, including Windows, macOS, Linux, Android, and iOS, can access the cloud network to implement mobile office.
- Access via DNS domain names is supported, allowing users to use domain names to access cloud services.
- VPN users can be imported and deleted in batches, maximizing efficiency.
- In P2C VPN, you can manage and proactively disconnect connections.
- In S2C VPN, you can flexibly enable or disable branch interconnection to implement interconnection or isolation between customer gateways, respectively.

4 Application Scenarios

Access from Terminals to a VPC

You can use client software on terminals such as PCs and mobile phones to remotely access resources in a VPC, as shown in **Figure 4-1**.

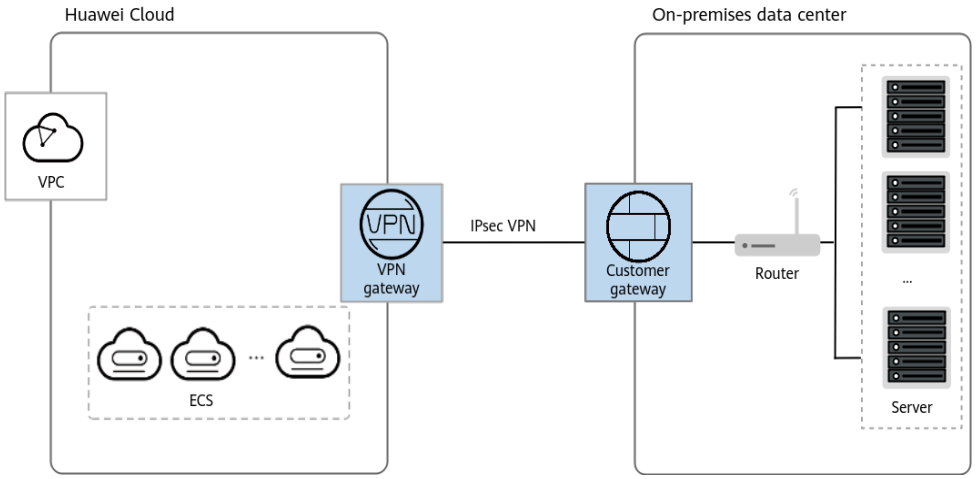
Figure 4-1 Remote access from terminals to a VPC



Hybrid Cloud Deployment

You can use a VPN to connect your on-premises data center to a VPC and use the elastic and fast scaling capabilities of the cloud to expand application computing capabilities. **Figure 4-2** shows the hybrid cloud deployment.

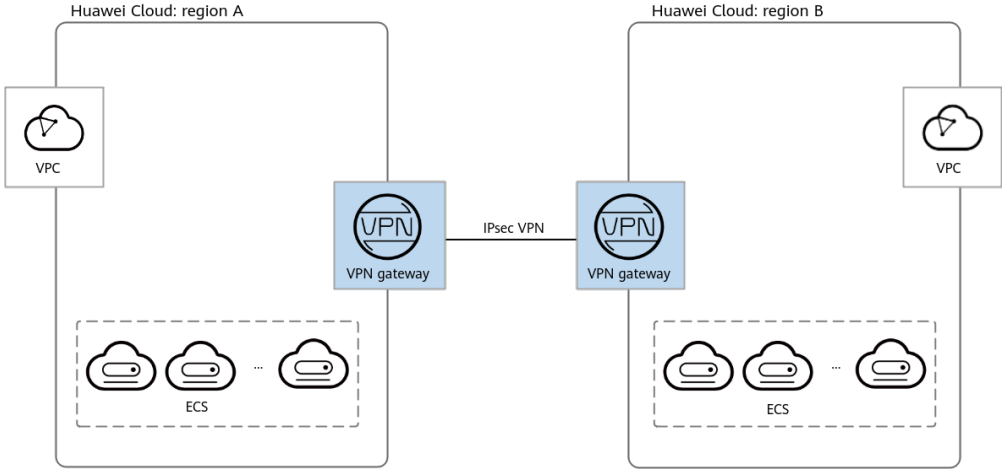
Figure 4-2 Hybrid cloud deployment



Cross-Region Interconnection Between VPCs

With VPNs, you can connect VPCs in different regions to enable connectivity between user services in these regions, as shown in **Figure 4-3**.

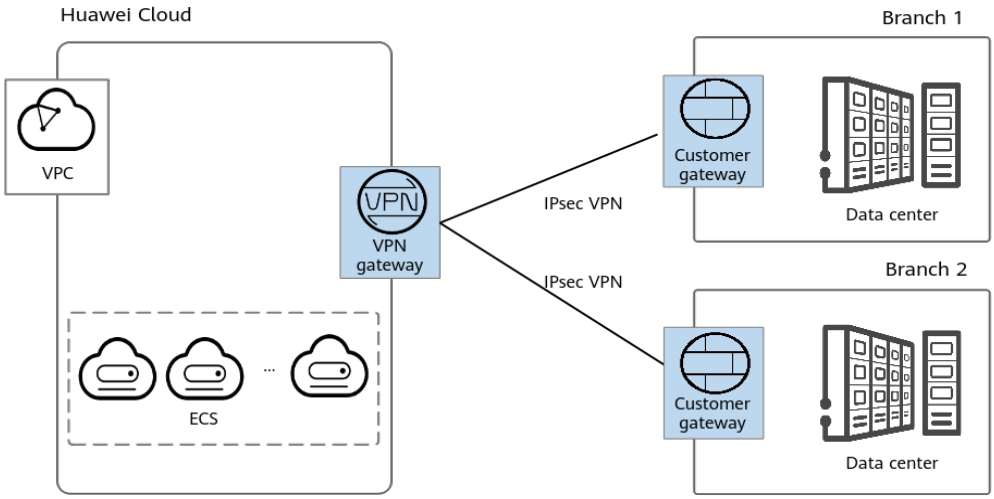
Figure 4-3 Cross-region interconnection between VPCs



Enterprise Branch Interconnection

A VPN gateway functions as a VPN hub to connect enterprise branches, as shown in **Figure 4-4**. This eliminates the need to configure VPN connections between every two branches.

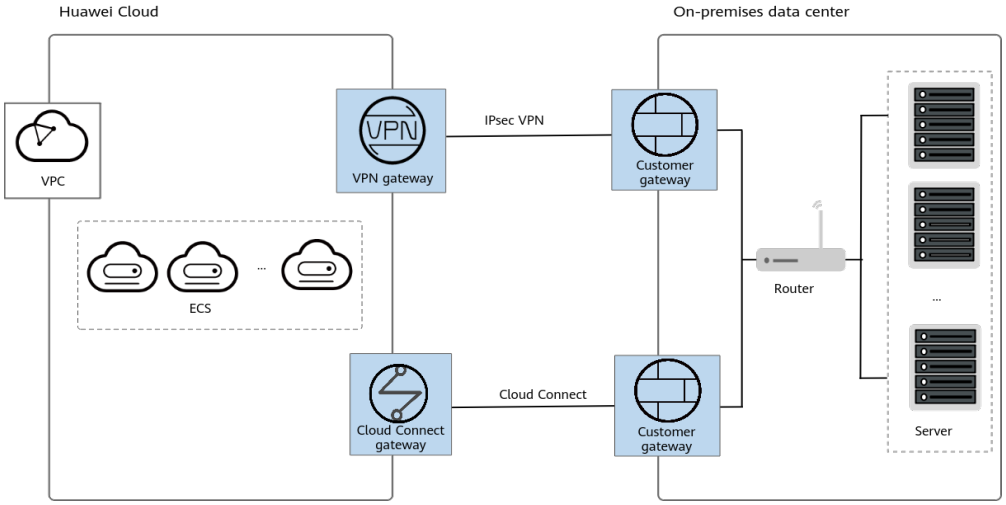
Figure 4-4 Enterprise branch interconnection



Backup Between VPN and Direct Connect

For high reliability purposes, you can connect your on-premises data center to a VPC on the cloud through Direct Connect and VPN that back up each other, as shown in **Figure 4-5**.

Figure 4-5 Backup between VPN and Direct Connect



5 Product Specifications

5.1 S2C VPN

NOTE

- The specification of a VPN gateway can be changed between Basic and Professional 1.
- The specification of a VPN gateway can be changed between Professional 1 and Professional 2.
- The specification of a VPN gateway cannot be changed from Professional 1 supporting access via non-fixed IP addresses to Professional 1 or from Professional 2 supporting access via non-fixed IP addresses to Professional 2.
- The specification of a VPN gateway cannot be changed to Professional 3 or changed from Professional 3 to another one.

The preceding specification changes are subject to the console.

Table 5-1 S2C VPN specifications

Item	Basic	Professional 1	Professional 1: Supporting Access via Non-fixed IP Addresses	Professional 2	Professional 2: Supporting Access via Non-fixed IP Addresses	GM	Professional 3
Exclusive gateway resources	Supported	Supported	Supported	Supported	Supported	Supported	Supported

Item	Basic	Professional 1	Professional 1: Supporting Access via Non-fixed IP Addresses	Professional 2	Professional 2: Supporting Access via Non-fixed IP Addresses	GM	Professional 3
Dual connections	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Active-active gateways	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Active/Standby gateways	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Policy-based mode	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Routing mode: static routing	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Routing mode: BGP routing	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Policy template mode	Not supported	Not supported	Supported	Not supported	Supported	Not supported	Supported
Maximum forwarding bandwidth	100 Mbit/s	300 Mbit/s	300 Mbit/s	1 Gbit/s	1 Gbit/s	500 Mbit/s	5000Mbps

Item	Basic	Professional 1	Professional 1: Supporting Access via Non-fixed IP Addresses	Professional 2	Professional 2: Supporting Access via Non-fixed IP Addresses	GM	Professional 3
Maximum number of VPN connection groups	10	100	100	100	100	100	300
Interconnection with an enterprise router	Not supported	Supported	Supported	Supported	Supported	Supported	Supported
Private network	Not supported	Supported	Not supported	Supported	Not supported	Supported	Supported
Access via non-fixed IP addresses	Not supported	Not supported	Supported	Not supported	Supported	Not supported	Not supported
Supported regions	Subject to the regions available on the management console	Subject to the regions available on the management console	Subject to the regions available on the management console	Subject to the regions available on the management console	Subject to the regions available on the management console	Subject to the regions available on the management console	Subject to the regions available on the management console

5.2 P2C VPN

Table 5-2 P2C VPN specifications

Item	Professional 1
Exclusive gateway resources	Supported
Maximum forwarding bandwidth	300 Mbit/s
Maximum number of VPN connections	500
Supported regions	Subject to the regions available on the management console

6 Quotas and Constraints

6.1 S2C VPN

VPN Gateway

Table 6-1 Constraints on VPN gateways

VPN Type	Resource	Default Quota	How to Increase Quota
Enterprise Edition VPN	VPN gateways per tenant in each region	50 • If you have only one VPC, you can create a maximum of 50 VPN gateways for the VPC. • If you have multiple VPCs, you can create a maximum of 50 VPN gateways for all these VPCs.	**Submit a service ticket**.

VPN Type	Resource	Default Quota	How to Increase Quota
	VPN connection groups per VPN gateway	100 If a VPN gateway supports access via non-fixed IP addresses, it supports a total of 100 VPN connection groups for access via non-fixed IP addresses and access via fixed IP addresses.	This quota cannot be increased.
	Local subnets per VPN gateway	50	This quota cannot be increased.

VPN Type	Resource	Default Quota	How to Increase Quota
	Number of BGP routes that can be accepted by gateways of different specifications	100 • Maximum number of BGP routes that can be accepted by a VPN gateway of the Basic or GM specification: 100 • Maximum number of BGP routes that can be accepted by a VPN gateway of the Professional 1 specification: 200 • Maximum number of BGP routes that can be accepted by a VPN gateway of the Professional 2 specification: 300 • Maximum number of BGP routes that can be accepted by a VPN gateway of the Professional 3 specification: 500	This quota cannot be increased.
	Maximum number of routes supported by a VPN gateway	10000	This quota cannot be increased.
Classic VPN	VPN gateways per tenant in each region	2 Only one VPN gateway can be created for a VPC.	**Submit a service ticket**.

- By default, the maximum length of TCP packets supported by a VPN gateway is 1300 bytes.

Customer Gateway

Table 6-2 Constraints on customer gateways

VPN Type	Resource	Default Quota	How to Increase Quota
Enterprise Edition VPN	Customer gateways per tenant in each region	100	**Submit a service ticket**.

- Enable NAT traversal on the customer gateway based on the networking.
  - If the customer gateway is connected to the Internet through a NAT device, enable NAT traversal on the customer gateway.
  - If the customer gateway is directly connected to the Internet, you do not need to enabled NAT traversal on the customer gateway.
- Dead Peer Detection (DPD) must be enabled on a customer gateway.
- A customer gateway must support IPsec tunnel interfaces and be configured with a corresponding security policy.
- When Network Quality Analysis (NQA) is enabled for a connection in static routing mode, the IPsec tunnel interface of a customer gateway must have an IP address and be able to respond to ICMP requests.
- It is recommended that the maximum segment size (MSS) of TCP packets be set to a value less than 1399 on a customer gateway, so as to prevent fragmentation caused by addition of an IPsec header.

VPN Connection

Table 6-3 Constraints on VPN connections

VPN Type	Resource	Default Quota	How to Increase Quota
Enterprise Edition VPN	Policy rules per VPN connection	5	The quotas cannot be increased.
	Customer subnets per VPN connection	50	
Classic VPN	VPN connections per tenant in each region	12	This quota cannot be increased.

- In multi-subnet scenarios, you are advised to use VPN connections in routing mode. For a VPN connection in policy-based or policy template mode, a VPN

gateway creates a communications tunnel for each pair of the local and customer subnets by default. If there are multiple local or customer subnets for a VPN connection in policy-based or policy template mode, multiple communications tunnels are created.

Each IP address of a VPN gateway supports a maximum of 100 communications tunnels for connecting to customer gateways.

- In routing mode, each VPN connection occupies only one communications tunnel of the corresponding VPN gateway IP address.
- In policy-based or policy template mode, each VPN connection occupies *M* x *N* communications tunnels of the corresponding VPN gateway IP address. *M* indicates the number of local subnets, and *N* indicates the number of customer subnets.

If the number of communications tunnels occupied by all VPN connections in different modes established by a single gateway IP address has reached 100, excess VPN connections will fail to be created.

- When creating a VPN connection in policy-based mode and adding multiple policy rules, ensure that the source and destination CIDR blocks in different policy rules do not overlap. Otherwise, data flows may be incorrectly matched or IPsec tunnels may flap.

6.2 P2C VPN

P2C VPN Gateway

Table 6-4 Constraints on P2C VPN gateways

VPN Type	Resource	Default Quota	How to Increase Quota
Enterprise Edition VPN	VPN gateways per tenant in each region	50	The quotas cannot be increased.
	Servers associated with a single VPN gateway	1	

P2C VPN gateways support only EIPs with dedicated bandwidth, but not EIPs with shared bandwidth.

P2C VPN Server

Table 6-5 Constraints on P2C VPN servers

VPN Type	Resource	Default Quota	How to Increase Quota
Enterprise Edition VPN	Client CA certificates per server	10	The quotas cannot be increased.
	Local CIDR blocks per server	20	

- If you modify the protocol, port, authentication algorithm, or encryption algorithm, you need to download the client configuration again.
- The local subnet cannot be set to 0.0.0.0.
- The local CIDR block cannot overlap or conflict with the following special CIDR blocks: 0.0.0.0/8, 224.0.0.0/4, 240.0.0.0/4, and 127.0.0.0/8.
- Each user can establish a maximum of five connections.
- A maximum of 500 users can be created on a VPN gateway.
- The maximum number of users that can be configured is the maximum number of connections of the gateway.
- A maximum of 50 user groups are supported.
- A maximum of 10 destination CIDR blocks can be configured in a single policy.

  A maximum of 100 access policies are supported.
- Only when a VPN gateway is in a normal state, its connections can be torn down. If a VPN gateway is in faulty, updating, deleting, or frozen state, its connections cannot be torn down.

P2C VPN Client

In the Windows operating system, the reconnection time of the OpenVPN GUI client is longer than that of the OpenVPN Connect client in exception scenarios. Therefore, the OpenVPN Connect client is recommended.

7 Reference Standards and Protocols

The following standards and protocols are associated with VPN:

- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
- RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2)Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308: Cryptographic Suites for IPsec
- RFC 5282: Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
- RFC 6989: Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)

- RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7321: Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 8247: Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 4271: A Border Gateway Protocol 4 (BGP-4)

8 Differences between S2C Enterprise Edition VPN and Classic VPN

Table 8-1 Differences between Enterprise Edition VPN and Classic VPN

Category	Item	Enterprise Edition VPN	Classic VPN
Tenant isolation	Tenant-exclusive gateway	Supported	Not supported
Features	Policy-based mode	Supported	Supported
	Routing mode	Static routing and BGP routing	Not supported
	VPN hub	Supported	Not supported
	Enterprise router	Supported	Not supported
	Network type	Public network and private network	Public network
Capacity	Number of subnets	• Route-based mode: 50 • Policy-based mode: 5	Policy-based mode: 5
	For more information, see **Table 5-1**.		
Reliability	Gateway protection mode	Active/Standby or active-active	-
	Cross-AZ gateway deployment	Supported	Not supported
	Active-active VPN connections	Supported	Not supported
	Backup with Direct Connect	Supported	Not supported

9 Security

9.1 Shared Responsibility

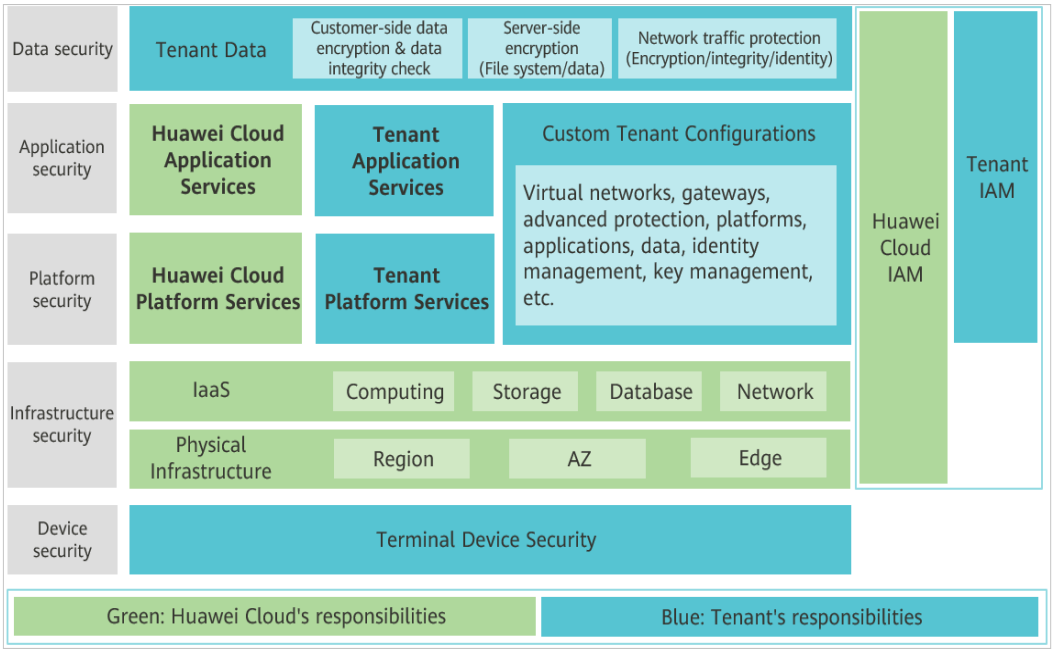
Huawei Cloud guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To address emerging challenges to cloud security and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive security system that is compliant with laws, regulations, and industry standards for cloud services in different regions and industries, by leveraging Huawei's security ecosystem and unique advantages in software and hardware.

You (tenants) and Huawei Cloud both have the responsibilities to ensure security, as shown in **Figure 9-1**.

- **Huawei Cloud**: Ensures the security of cloud services. Huawei Cloud is responsible for the security of its IaaS, PaaS, and SaaS cloud services, as well as the physical environments of the Huawei Cloud data centers where these services are deployed. Huawei Cloud is committed not only to the security and performance of its infrastructure, cloud services, and technologies, but also to the overall cloud O&M security and, more broadly, the security compliance.
- **Tenants**: Ensure secure use of cloud services. Your responsibility is to use the IaaS, PaaS, and SaaS cloud services securely, and effectively manage the security configurations you have customized for virtual firewalls, API gateways, advanced security services, cloud services, user data, identity and key management, and the operating systems for virtual networks, virtual hosts, and guest virtual machines (VMs).

The **Huawei Cloud Security White Paper** details the ideas and measures for building Huawei Cloud security system, including cloud security strategies, shared responsibility model, security compliance and privacy protection, security organization and personnel, infrastructure security, tenant services and security, engineering security, O&M security, and ecosystem security.

Figure 9-1 Shared responsibility model of Huawei Cloud



9.2 Identity Authentication and Access Control

An S2C VPN connection supports authentication of a customer gateway using a pre-shared key (PSK).

The identity authentication succeeds and the VPN connection can be set up only when the PSK configured on the customer gateway is the same as that configured for the VPN connection.

Figure 9-2 Identity and access management

9.3 Data Protection Technologies

- S2C VPN is a tunneling technology that provides IP-layer security using the IKE/IPsec protocol suite. It ensures confidentiality and integrity of IP data packets and prevents them from being intercepted, disclosed, or tampered with on insecure networks (such as the Internet).
- When creating an S2C VPN connection, you can configure data encryption and authentication algorithms in a policy.

  Table 9-1 lists the algorithms recommended for S2C VPN in descending order of security.

Table 9-1 Parameters for configuring an S2C VPN policy

Parameter		Description
IKE Policy	Version	• v2 • v1 (v1 has low security. If the device supports v2, v2 is recommended. For VPN connections set up using SM series cryptographic algorithms, only v1 is supported.) The default value is **v2**.
	Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA2-512 • SHA2-384 • SHA2-256 • MD5(Insecure. Not recommended.) • SHA1(Insecure. Not recommended.) By default, the SHA2-256 algorithm is used.
	Encryption Algorithm	The following encryption algorithms are supported: • AES-256-GCM-16 (supported only by Enterprise Edition VPN) • AES-128-GCM-16 (supported only by Enterprise Edition VPN) • AES-256(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • 3DES(Insecure. Not recommended.) The default value is **AES-128**.

Parameter		Description
	DH Algorithm	The following algorithms are supported: ● Group 21 ● Group 20 ● Group 19 ● Group 16 ● Group 15 ● Group 14(Insecure. Not recommended.) ● Group 5(Insecure. Not recommended.) ● Group 2(Insecure. Not recommended.) ● Group 1(Insecure. Not recommended.) By default, Group 15 is used.
IPsec Policy	Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: ● SHA2-512 ● SHA2-384 ● SHA2-256 ● MD5(Insecure. Not recommended.) ● SHA1(Insecure. Not recommended.) By default, the SHA2-256 algorithm is used.
	Encryption Algorithm	The following encryption algorithms are supported: ● AES-256-GCM-16 ● AES-128-GCM-16 ● AES-256(Insecure. Not recommended.) ● AES-192(Insecure. Not recommended.) ● AES-128(Insecure. Not recommended.) ● 3DES(Insecure. Not recommended.) The default value is **AES-128**.

- P2C VPN uses the SSL/TLS protocol for encryption to ensure data confidentiality and integrity and prevent the data from being intercepted, disclosed, or tampered with on insecure networks (such as the Internet).

Table 9-2 lists the commercial cryptographic algorithms supported by P2C VPN.

Table 9-2 Parameters for configuring algorithms used in P2C VPN

Parameter	Description
Authentication Algorithm	• SHA2-384 • SHA384
Encryption Algorithm	• AES-256-GCM-16 • AES-128-GCM-16

PFS

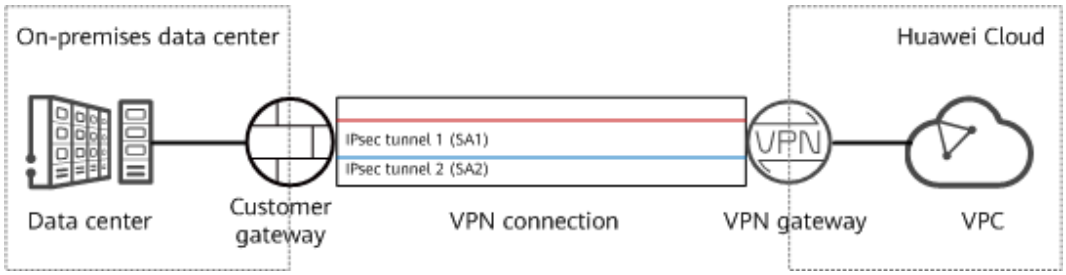
Perfect Forward Secrecy (PFS) ensures that the compromise of the keys of an IPsec tunnel does not affect the security of other tunnels by leveraging that the keys of these tunnels are irrelevant to each other. By default, the PFS function is enabled for S2C VPN.

Each IPsec VPN connection consists of at least one IPsec tunnel, each of which uses an independent set of keys to protect user traffic.

S2C VPN supports the following algorithms:

- DH group 1 (This algorithm is insecure. Exercise caution when using it.)
- DH group 2 (This algorithm is insecure. Exercise caution when using it.)
- DH group 5 (This algorithm is insecure. Exercise caution when using it.)
- DH group 14
- DH group 15
- DH group 16
- DH group 19
- DH group 20
- DH group 21

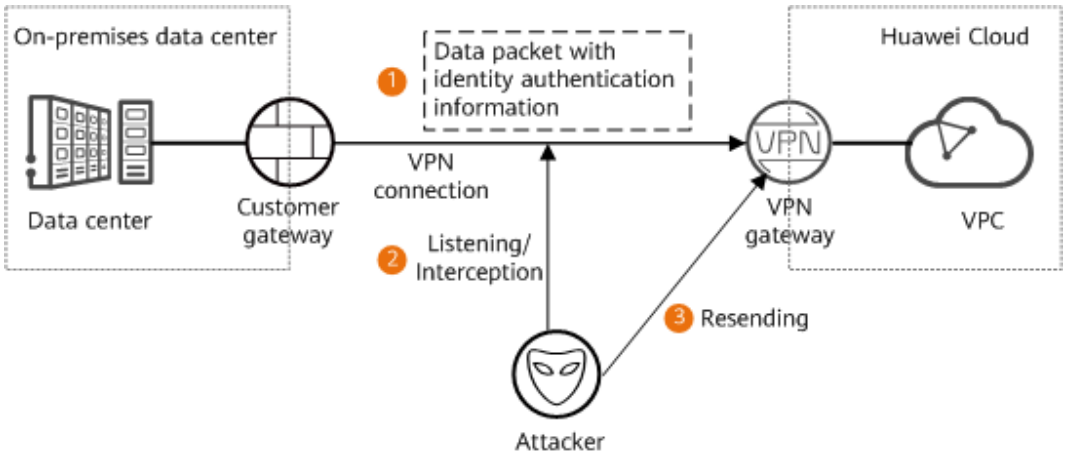
Figure 9-3 PFS



Anti-replay

Anti-replay uses sequence numbers to protect IPsec encrypted packets against replay attacks, which are initiated by repeatedly sending intercepted data packets. By default, the anti-replay function is enabled for the VPN service.

Figure 9-4 Replay attack

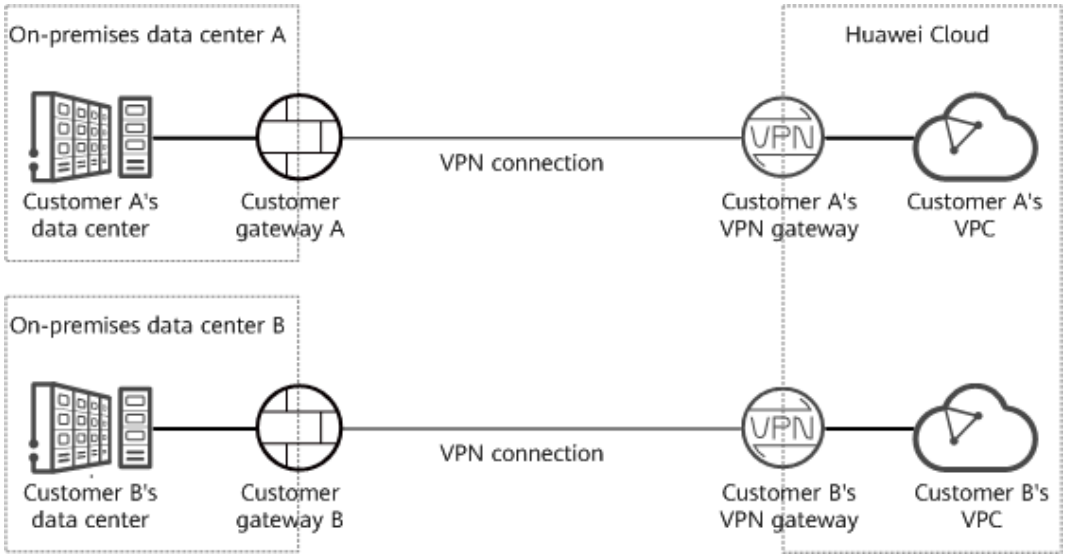


Resource Isolation

A VPN gateway is exclusive to a tenant. As such, tenants are isolated from each, ensuring tenant data security.

This feature is supported only by Enterprise Edition VPN.

Figure 9-5 Data isolation

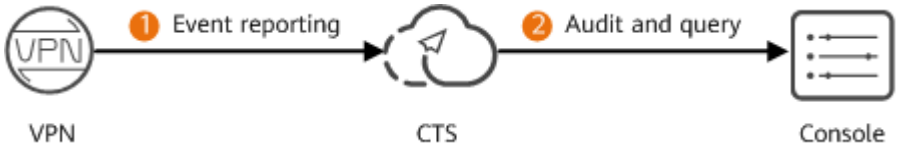


As shown in the figure, a failure of customer A's VPN gateway has no impact on customer B's VPN gateway.

9.4 Audit and Logs

VPN records the create, delete, and modify operations performed on all resources initiated by your account, and sends the records to Cloud Trace Service (CTS) in log files for query, audit, and source tracing.

Figure 9-6 Audit and logs

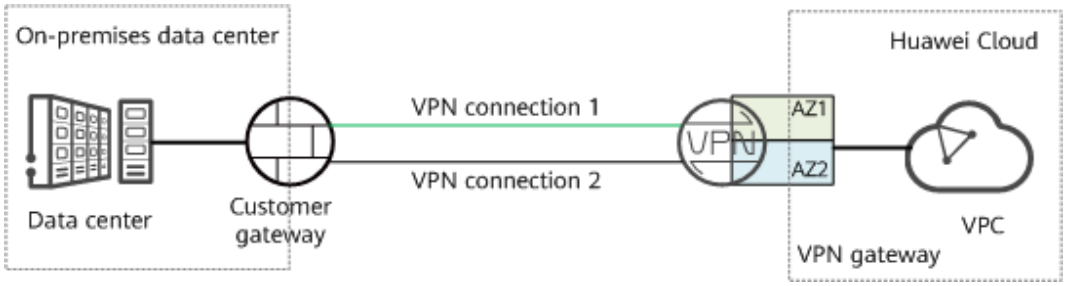


9.5 Service Resilience

VPN provides the dual-AZ disaster recovery function. You can create a VPN gateway in two AZs in the same region, and create a VPN connection between the customer gateway and each AZ.

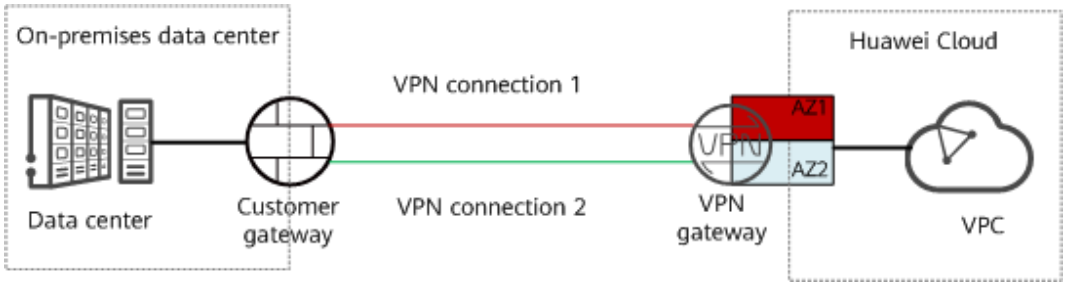
Dual-AZ disaster recovery is supported only by Enterprise Edition VPN, but not Classic VPN.

Figure 9-7 Scenario where services are running properly



If the VPN gateway or VPN connection in an AZ is faulty, traffic is automatically switched to the other VPN connection, ensuring normal service running.

Figure 9-8 Failover scenario



10 IAM-based Permissions Management

If you need to assign different permissions to personnel in your enterprise to access your VPN resources purchased on Huawei Cloud, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific Huawei Cloud resources. For example, some software developers in your enterprise need to use VPN resources but should not be allowed to delete them or perform any high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using VPN resources.

If your Huawei Cloud account does not need individual IAM users for permissions management, skip this section, which has no impact on using functions of VPN.

IAM is a free service. You only pay for the resources in your account.

For more information about IAM, see **IAM Service Overview**.

VPN Permissions

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.

VPN is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for VPN in the selected projects. If you set **Scope** to **All resources**, users have permissions for VPN in all region-specific projects. When accessing VPN, the users need to switch to the authorized region.

You can grant permissions by using roles or policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. There are only a limited number of roles for granting permissions to users. Some roles depend other roles to take

effect. When you assign such roles to users, remember to assign the roles they depend on. However, roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: a type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, administrators can grant IAM users only permissions to manage VPN resources of a certain type.

Table 10-1 lists all system-defined permissions for VPN.

Table 10-1 System-defined permissions for VPN

System Role/ Policy Name	Description	Dependency
VPN Administrator (not recommended)	Administrator permissions for VPN. Users with these permissions can perform all operations on VPN. Users with these permissions have the **VPC Administrator** and **Tenant Guest** permissions by default. • **VPC Administrator**: project-level policy, which is selected in the same project as **VPN Administrator**. • **Tenant Guest**: project-level policy, which is selected in the same project as **VPN Administrator**.	-
VPN FullAccess (recommended)	Full permissions for VPN. **NOTE** All actions that are used to query list information do not support authorization based on enterprise projects. You need to configure actions in the IAM view separately.	The actions of global services and the region-level actions cannot be configured in the same policy. As such, the following global actions are added: • "tms:predefineTags:list" • "scm:cert:list" • "scm:cert:get" • "scm:cert:download"

System Role/ Policy Name	Description	Dependency
VPN ReadOnlyAccess	Read-only permissions on VPN resources. Users who have these permissions can only view information about VPN resources. **NOTE** All actions that are used to query list information do not support authorization based on enterprise projects. You need to configure actions in the IAM view separately.	The actions of global services and the region-level actions cannot be configured in the same policy. As such, the following global actions are added: • "tms:predefineTags:list" • "scm:cert:list" • "scm:cert:get"

Table 10-2 lists the common operations supported by system-defined permissions for S2C VPN.

Table 10-2 Common operations supported by system-defined permissions for S2C VPN

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
Creating a VPN gateway	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×
Viewing a VPN gateway	√	√	√
Querying the VPN gateway list	√	√	√
Updating a VPN gateway	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×
Deleting a VPN gateway	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×
Creating a VPN connection	√	• Enterprise Edition VPN: √ • Classic VPN: √	×
Viewing a VPN connection	√	√	√

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
Querying the VPN connection list	√	√	√
Updating a VPN connection	√	• Enterprise Edition VPN: √ • Classic VPN: √	×
Deleting a VPN connection	√	• Enterprise Edition VPN: × • Classic VPN: √	×
Creating a customer gateway	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	×
Viewing a customer gateway	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	√
Querying the customer gateway list	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	√
Updating a customer gateway	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	×
Deleting a customer gateway	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	×
Creating a VPN connection monitor	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×
Querying a VPN connection monitor	√	• Enterprise Edition VPN: √ • Classic VPN: ×	√
Querying the VPN connection monitor list	√	• Enterprise Edition VPN: √ • Classic VPN: ×	√
Deleting a VPN connection monitor	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×

Table 10-3 lists the common operations supported by system-defined permissions for P2C VPN.

Table 10-3 Common operations supported by system-defined permissions for P2C VPN

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
Subscribing to a yearly/monthly P2C VPN gateway	√	√	×
Changing the specification of a yearly/monthly P2C VPN gateway	√	√	×
Updating a P2C VPN gateway	√	√	×
Querying details about a P2C VPN gateway	√	√	√
Querying the P2C VPN gateway list	√	√	√
Querying the P2C VPN connection list	√	√	√
Creating a VPN server	√	× The actions of global services and the region-level actions cannot be configured in the same policy. As such, the following global actions are added: scm:cert:get scm:cert:list scm:cert:download	×
Querying server information on a gateway	√	√	√

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
Updating server information on a specified gateway	√	× The actions of global services and the region-level actions cannot be configured in the same policy. As such, the following global actions are added: scm:cert:get scm:cert:list scm:cert:download	×
Exporting the client configuration information corresponding to a server	√	√	×
Verifying the validity of CA certificates	√	√	√
Importing a client CA certificate	√	√	×
Modifying a client CA certificate	√	√	×
Querying a client CA certificate	√	√	√
Deleting a client CA certificate	√	√	×
Querying information about all servers of a tenant	√	√	√
Creating a VPN user	√	√	×
Querying the VPN user list	√	√	√

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
Modifying a VPN user	√	√	×
Querying a VPN user	√	√	√
Deleting a VPN user	√	√	×
Changing the password of a VPN user	√	√	×
Resetting the password of a VPN user	√	√	×
Creating a VPN user group	√	√	×
Querying the VPN user group list	√	√	√
Modifying a VPN user group	√	√	×
Querying a VPN user group	√	√	√
Deleting a VPN user group	√	√	×
Adding VPN users to a group	√	√	×
Deleting VPN users from a group	√	√	×
Querying VPN users in a group	√	√	√
Creating a VPN access policy	√	√	×
Querying the VPN access policy list	√	√	√
Modifying a VPN access policy	√	√	×

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
Querying a VPN access policy	√	√	√
Deleting a VPN access policy	√	√	×
Querying the AZs of P2C VPN gateways	√	√	√
Adding resource tags in batches	√	√	×
Deleting resource tags in batches	√	√	×
Querying resource instances by resource tag	√	√	√
Querying the number of resource instances	√	√	√
Querying resource tags by resource instance	√	√	√
Querying the resource tag list	√	√	√

Helpful Links

- IAM Service Overview
- Creating a User and Granting VPN Permissions

10.1 Actions Supported by S2C VPN

10.1.1 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 (V5)	GET /v5/{project_id}/vpn-gateways/availability-zones	vpn:vpnGatewayAvailabilityZone:list	-	√	×
Querying the AZs of VPN gateways (V5.1)	GET /v5.1/{project_id}/vpn-gateways/availability-zones	vpn:vpnGatewayAvailabilityZone:list	-	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Importing certificates for a VPN gateway	POST /v5/{project_id}/vpn-gateways/{vgw_id}/certificate	vpn:vpnGateways:importCertificate	-	√	√
Querying certificates of a VPN gateway	GET /v5/{project_id}/vpn-gateways/{vgw_id}/certificate	vpn:vpnGateways:getCertificate	-	√	√
Updating certificates of a VPN gateway	PUT /v5/{project_id}/vpn-gateways/{vgw_id}/certificate/{certificate_id}	vpn:vpnGateways:updateCertificate	-	√	√

10.1.2 Customer Gateway

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a customer gateway	POST /v5/{project_id}/customer-gateways	vpn:customerGateways:create	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
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

10.1.3 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	√	√

10.1.4 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

10.2 Actions Supported by P2C VPN

10.2.1 VPN Gateway

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Subscribing to a yearly/monthly P2C VPN gateway	POST /v5/{project_id}/p2c-vpn-gateways/subscribe/{order_id}	vpn:p2cVpnGateway:subscribe	vpn:system:listAvailabilityZones vpc:vpcs:list vpc:subnets:get vpc:bandwidths:list vpc:publicIps:create vpc:publicIps:delete vpc:publicIps:update vpc:publicIps:list	√	×
Changing the specification of a yearly/monthly VPN gateway	PUT /v5/{project_id}/p2c-vpn-gateways/update-specification/{order_id}	vpn:p2cVpnGateway:updateSpecification	-	√	×
Updating a P2C VPN gateway	PUT /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}	vpn:p2cVpnGateway:update	vpc:publicIps:create vpc:publicIps:delete vpc:publicIps:update vpc:publicIps:get vpc:publicIps:list vpc:bandwidths:list	√	×

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Querying details about a P2C VPN gateway	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}	vpn:p2cVpnGateway:get	vpc:publicIps:get	√	×
Querying the P2C VPN gateway list	GET /v5/{project_id}/p2c-vpn-gateways	vpn:p2cVpnGateway:list	vpc:publicIps:get	√	×
Querying the P2C VPN connection list	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections	vpn:p2cVpnGateway:listConnections	-	√	×
Disconnecting a connection of a P2C VPN gateway	POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections/{connection_id}/disconnect	vpn:p2cVpnGateway:disconnectConnection	-	√	×

10.2.2 Server

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a P2C VPN server	POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers	vpn:p2cVpnGateway:createServer	scm:cert:get scm:cert:list scm:cert:download vpc:publicIps:get vpc:routeTables:update vpc:subnets:get	√	x
Querying server information on a gateway	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/vpn-servers	vpn:p2cVpnGateway:listServers	-	√	x
Updating server information on a specified gateway	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}	vpn:p2cVpnGateway:updateServer	scm:cert:get scm:cert:list scm:cert:download vpc:publicIps:get vpc:routeTables:update vpc:subnets:get	√	x
Exporting the client configuration information corresponding to a server	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-config/export	vpn:p2cVpnGateway:exportClientConfig	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Verifying the validity of CA certificates	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/client-ca-certificates/check	vpn:system:checkClientCaCertificate	-	√	x
Importing client CA certificates	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates	vpn:p2cVpnGateway:importClientCa	-	√	x
Modifying a client CA certificate	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:updateClientCa	-	√	x
Querying a client CA certificate	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:getClientCa	-	√	x
Deleting a client CA certificate	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/client-ca-certificates/{client_ca_certificate_id}	vpn:p2cVpnGateway:deleteClientCa	-	√	x
Querying information about all servers of a tenant	GET /v5/{project_id}/vpn-servers	vpn:p2cVpnGateway:listAllServers	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Disconnecting connections of a P2C VPN gateway	POST /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/connections/{connection_id}/disconnect	vpn:p2cVpnGateway:disconnectConnection	-	√	x
Updating the P2C VPN connection log configuration	PUT /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config	vpn:p2cVpnGateway:updateConnectionsLogConfig	-	√	×
Querying the P2C VPN connection log configuration	GET /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config	vpn:p2cVpnGateway:getConnectionsLogConfig	-	√	×
Deleting the P2C VPN connection log configuration	DELETE /v5/{project_id}/p2c-vpn-gateways/{p2c_vgw_id}/log-config	vpn:p2cVpnGateway:deleteConnectionsLogConfig	-	√	×

10.2.3 User Management

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a VPN user	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users	vpn:p2cVpnUser:create	-	√	x
Creating VPN users in batches	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/batch-create	vpn:p2cVpnUser:batchCreate	-	√	x
Querying the VPN user list	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users	vpn:p2cVpnUser:list	-	√	x
Modifying a VPN user	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}	vpn:p2cVpnUser:update	-	√	x
Querying a VPN user	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}	vpn:p2cVpnUser:get	-	√	x
Deleting a VPN user	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}	vpn:p2cVpnUser:delete	-	√	x
Deleting VPN users in batches	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/batch-delete	vpn:p2cVpnUser:batchDelete	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Changing the password of a VPN user	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/password	vpn:p2cVpnUser:updatePassword	-	√	x
Resetting the password of a VPN user	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/users/{user_id}/reset-password	vpn:p2cVpnUser:resetPassword	-	√	x
Creating a VPN user group	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups	vpn:p2cVpnGateway:createUserGroup	-	√	x
Querying the VPN user group list	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups	vpn:p2cVpnGateway:listUserGroup	-	√	x
Modifying a VPN user group	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpnGateway:updateUserGroup	-	√	x
Querying a VPN user group	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpnGateway:getUserGroup	-	√	x
Deleting a VPN user group	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}	vpn:p2cVpnGateway:deleteUserGroup	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Adding VPN users to a group	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/add-users	vpn:p2cVpnGateway:addUsers	-	√	x
Removing VPN users from a group	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/remove-users	vpn:p2cVpnGateway:removeUsers	-	√	x
Querying VPN users in a group	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/groups/{group_id}/users	vpn:p2cVpnGateway:listUsersInGroup	-	√	x

10.2.4 Access Policy

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Creating a VPN access policy	POST /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies	vpn:p2cVpnGateway:createAccessPolicy	-	√	x
Querying the VPN access policy list	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies	vpn:p2cVpnGateway:listAccessPolicies	-	√	x

Permission	API	Action	Dependencies	IAM Project	Enterprise Project
Modifying a VPN access policy	PUT /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:updateAccessPolicy	-	√	x
Querying a VPN access policy	GET /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:getAccessPolicy	-	√	x
Deleting a VPN access policy	DELETE /v5/{project_id}/p2c-vpn-gateways/vpn-servers/{vpn_server_id}/access-policies/{policy_id}	vpn:p2cVpnGateway:deleteAccessPolicy	-	√	x

10.3 Actions Supported by Public Service APIs

10.3.1 VPN Quota

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

10.3.2 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

11 VPN and Other Services

Figure 11-1 shows VPN-related services.

Figure 11-1 VPN and related services

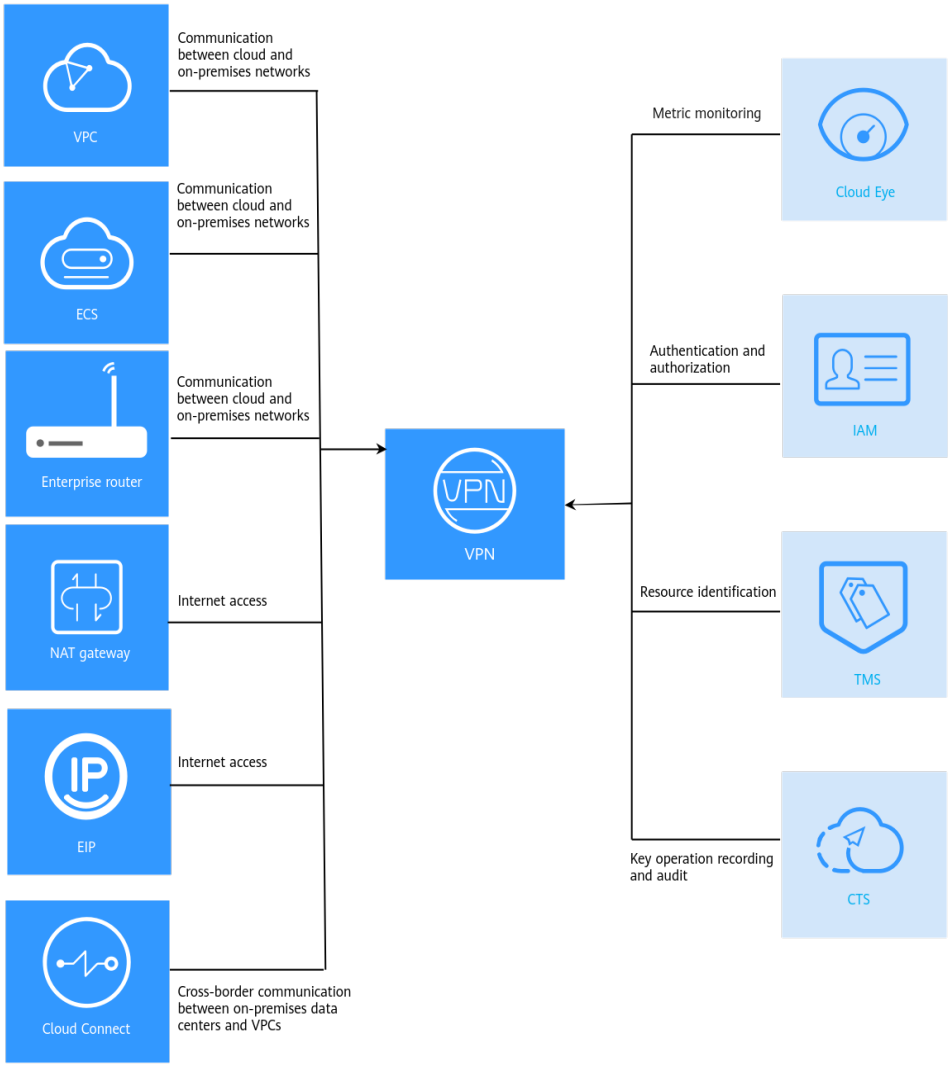


Table 11-1 Related services

Related Service	Function	Reference
Virtual Private Cloud (VPC)	Allows you to create a virtual private cloud to which your on-premises data center is to be connected.	**VPC**
Elastic Cloud Server (ECS)	Allows you to create security groups, add security group rules, and add ECSs to the security groups, improving ECS access security.	**ECS**
Enterprise Router (ER)	Connects an on-premises data center to the cloud through a VPN and Direct Connect that back up each other. This service is supported only by Enterprise Edition VPN gateways, but not Classic VPN gateways.	**Enterprise Router**
Network address translation (NAT) gateway	Allows servers in an on-premises data center to access the Internet or provide services that are accessible from the Internet.	**NAT Gateway**
Elastic IP address (EIP)	Allows a VPN gateway to communicate with a customer gateway through a public network. This service is supported only by Enterprise Edition VPN, but not Classic VPN.	**EIP**
Cloud Connect	Works together with VPN to enable stable network communications between your on-premises data center and VPCs in different regions.	**Cloud Connect**
Cloud Eye	Monitors VPN resources and allows you to view metrics.	**Cloud Eye**

Related Service	Function	Reference
Identity and Access Management (IAM)	Allows you to assign different permissions to different users. It enables fine grained control over your VPN resources.	**Identity and Access Management**
Tag Management Service (TMS)	Identifies VPNs to facilitate classification and search.	**Tag Management Service**
Cloud Trace Service (CTS)	Records operations performed on VPN.	**Cloud Trace Service**

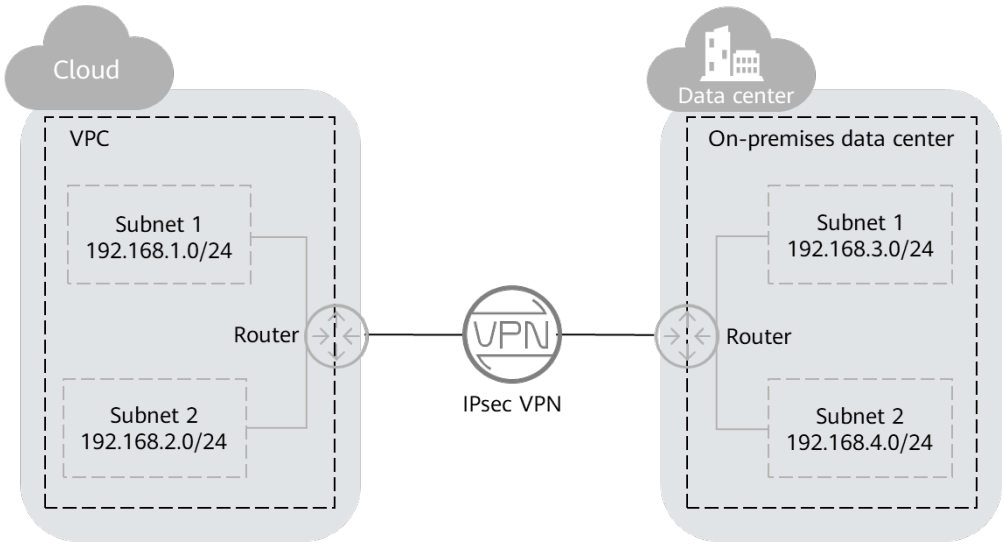
12 Basic Concepts

12.1 IPsec VPN

Internet Protocol Security (IPsec) VPN uses a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between different networks.

In the example shown in **Figure 12-1**, assume that you have created a VPC with two subnets (192.168.1.0/24 and 192.168.2.0/24) on the cloud, and the router in your on-premises data center also has two subnets (192.168.3.0/24 and 192.168.4.0/24). In this case, you can create a VPN to connect the VPC subnets and the data center subnets.

Figure 12-1 IPsec VPN



Site-to-site VPN is supported to enable communication between VPC subnets and on-premises data center subnets.

12.2 SSL VPN

SSL VPN is a virtual private network technology using the SSL protocol. It allows remote users to securely access intranet resources of enterprises through encrypted channels.

12.3 VPN Gateway

A VPN gateway is a virtual gateway of VPN on the cloud. It establishes secure private connections with a customer gateway in your on-premises network or data center. A VPN gateway needs to work with a customer gateway in your on-premises data center.

12.4 VPN Connection

A VPN connection is a secure channel between a VPN gateway and a customer gateway. VPN connections use the IKE and IPsec protocols to encrypt the transmitted data.

A VPN connection uses the IKE and IPsec protocols to encrypt transmitted data, ensuring data security and reliability.

12.5 VPN Gateway Bandwidth

The bandwidth you purchased for a VPN gateway refers to outbound bandwidth, that is, bandwidth for traffic sent from a VPC on the cloud to a customer gateway in an on-premises data center.

- If the purchased bandwidth is 10 Mbit/s or less, the inbound bandwidth is limited to 10 Mbit/s.
- If the purchased bandwidth is greater than 10 Mbit/s, the inbound bandwidth is the same as the EIP bandwidth.

If your VPN gateway is billed by traffic on a pay-per-use basis, the bandwidth size of the VPN gateway does not affect the total price. But it is recommended that you set the bandwidth size based on actual requirements to prevent a large amount of traffic caused by program errors or malicious access.

12.6 Local Subnet

Local subnets are VPC subnets that need to communicate with an on-premises network through VPN. When you buy a VPN gateway, you can set **Local Subnet** to either of the following options:

- **Select subnet**: Select subnets from the drop-down list. This is recommended if all subnets that require VPN communication are in the VPC.
- **Enter CIDR block**: Enter a subnet using CIDR notation (example: 192.168.0.0/16). If multiple subnets are specified, separate them by a comma

(,). This is recommended if the CIDR blocks requiring VPN communication are not in the VPC to which the VPN gateway belongs. For example, CIDR blocks (such as 0.0.0.0/0) that are connected using a VPC peering are not in the VPC to which the VPN gateway belongs.

12.7 Customer Gateway

A customer gateway can be a physical device or software application in your on-premises data center. A customer gateway is a resource that provides information on the management console about your customer gateway device.

12.8 Customer Subnet

Customer subnets are subnets in an on-premises data center that access a VPC on the cloud through a VPN. You need to enter subnets using CIDR notation (example: 192.168.0.0/16), and with each entry separated by a comma.

After configuring a customer subnet, you do not need to add a route for it. The VPN service will automatically deliver routes pointing to the customer subnet.

NOTE

A customer subnet cannot be set to a Class D or Class E IP address or an IP address starting with 127.

12.9 PSK

A pre-shared key (PSK) is a key configured for a VPN connection on the cloud. It is used for IKE negotiation between VPN devices at both ends of a VPN connection. Ensure that the PSK configurations at both ends of the VPN connection are the same. Otherwise, the IKE negotiation will fail.

Reference link:

Are a Username and Password Required for Creating an IPsec VPN Connection?

12.10 Region and AZ

Concepts

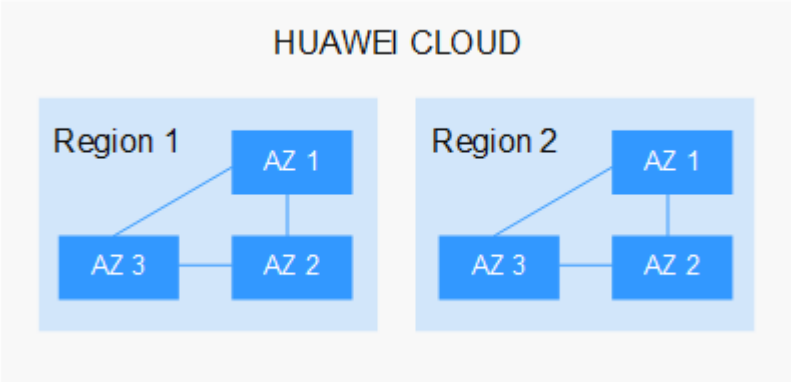
Regions and availability zones (AZs) identify the locations of data centers. You can create resources in regions and AZs.

- Regions are divided based on geographical locations and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions fall into two types: universal and dedicated. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.

- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, compute, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers, allowing you to build cross-AZ high-availability systems.

Figure 12-2 shows the relationship between regions and AZs.

Figure 12-2 Regions and AZs



Currently, Huawei Cloud provides services in many regions around the world. You can select regions and AZs as required. For more information, see **Huawei Cloud Global Regions**.

Selecting a Region

When selecting a region, consider the following:

- Geographical location

  You are advised to select a region close to you or your target users to reduce network latency and improve the access speed.

  - If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If your target users are in Africa, select the **AF-Johannesburg** region.
  - If your target users are in Latin America, select the **LA-Santiago** region.

    NOTE

    The **LA-Santiago** region is located in Chile.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When selecting a region to deploy resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For robust DR, deploy resources in different AZs within the same region.
- For a low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more information, see **Regions and Endpoints**.

