Virtual Private Network

Service Overview

Issue	01
Date	2024-03-06

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

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

Contents

1 What Is Virtual Private Network?

Overview

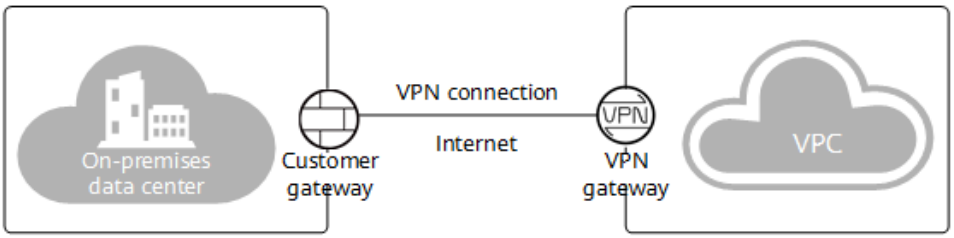
Virtual Private Network (VPN) establishes secure, reliable, and cost-effective encrypted connections between your on-premises network or data center and a virtual network on Huawei Cloud.

A VPN consists of a VPN gateway, a customer gateway, and one or more VPN connections.

- A VPN gateway provides an Internet egress for a 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 1-1 shows the VPN networking.

Figure 1-1 VPN networking



Components

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

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 "Registering a HUAWEI ID and Enabling Huawei Cloud Services" in **Preparations**.

2 Product Advantages

VPN has the following advantages:

- **High security**
  - Data is encrypted using IKE and IPsec, ensuring high data security.
  - A VPN gateway is exclusive to a tenant, isolating tenants from each other.
- **High availability**
  - A VPN gateway provides two elastic IP addresses (EIPs) 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.
  - Active/Standby mode: In normal cases, a VPN gateway communicates with a customer gateway through the active connection. If the active connection fails, traffic is automatically switched to the standby VPN connection. After the fault is rectified, traffic is switched back to the active VPN connection.
- **Cost-effectiveness**
  - IPsec connections over the Internet provide a cost-effective alternative to Direct Connect.
  - A VPN gateway can be bound to EIPs that share bandwidth, reducing bandwidth costs.
  - The bandwidth can be adjusted when an EIP instance is created.
- **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.

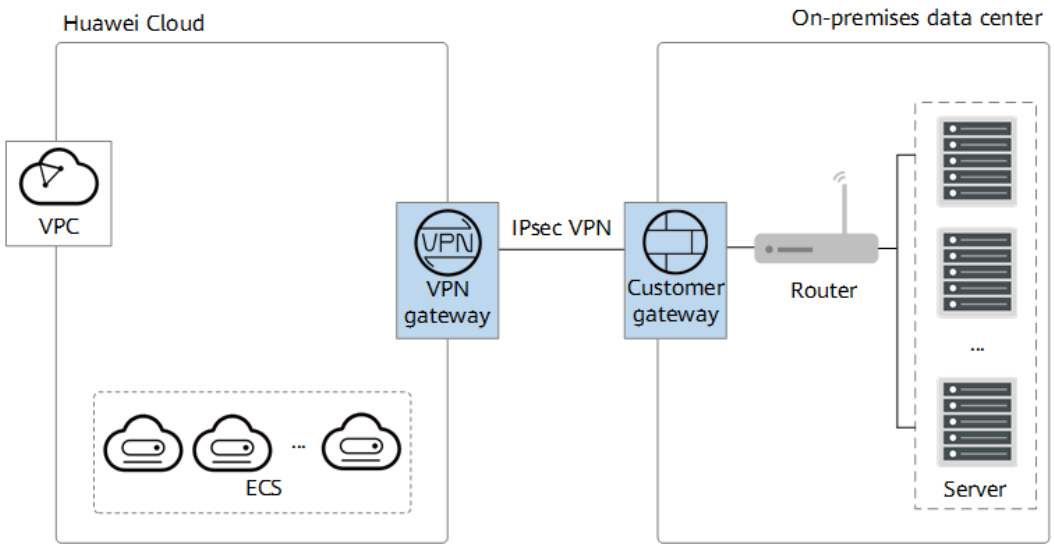
- Private VPN gateways are supported to encrypt traffic transmitted over Direct Connect connections, improving data transmission security.

3 Application Scenarios

Hybrid Cloud Deployment

You can use a VPN to connect your on-premises data center to a VPC on the cloud and use the elastic and fast scaling capabilities of the cloud to expand application computing capabilities. **Figure 3-1** shows the hybrid cloud deployment.

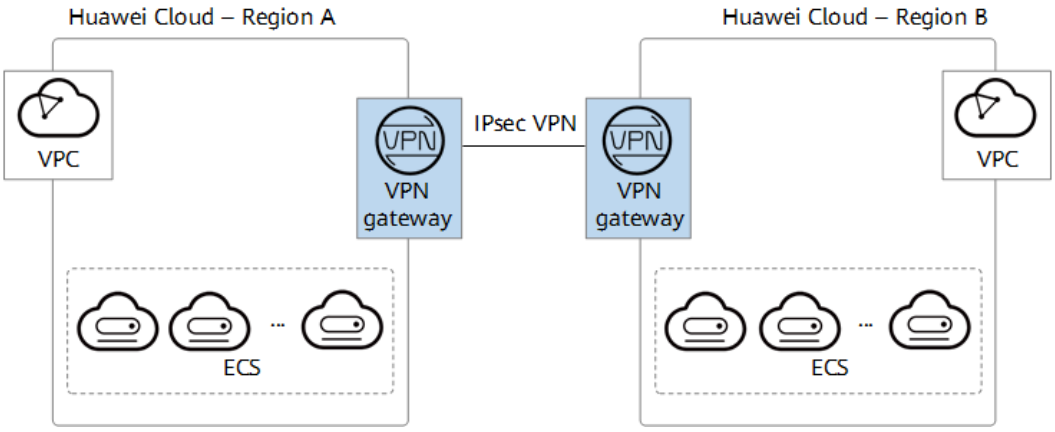
Figure 3-1 Hybrid cloud deployment



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 3-2**.

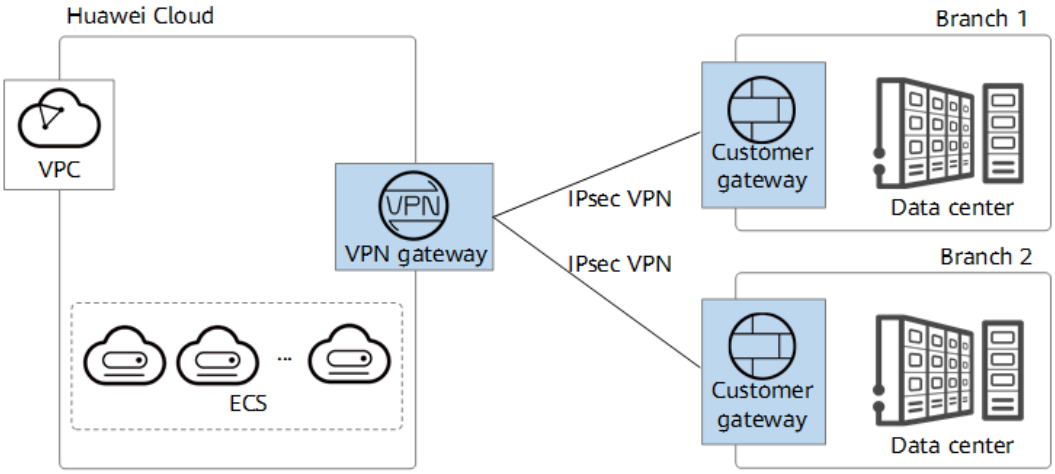
Figure 3-2 Cross-region interconnection between VPCs



Enterprise Branch Interconnection

A VPN gateway functions as a VPN hub to connect enterprise branches, as shown in **Figure 3-3**. This eliminates the need to configure VPN connections between every two branches.

Figure 3-3 Enterprise branch interconnection



4 Notes and Constraints

Table 4-1 Notes and constraints

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**.
	Customer gateways per tenant in each region	100	**Submit a service ticket**.
	VPN connection groups per VPN gateway	100	This quota cannot be increased.
	Local subnets per VPN gateway	50	This quota cannot be increased.
	Policy rules per VPN connection	5	This quota cannot be increased.
	Customer subnets per VPN connection	50	This quota cannot be increased.

VPN Type	Resource	Default Quota	How to Increase Quota
	Number of BGP routes that a VPN gateway can receive from a customer gateway through a connection	100	This quota cannot be increased.

5 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)

6 Security

6.1 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.

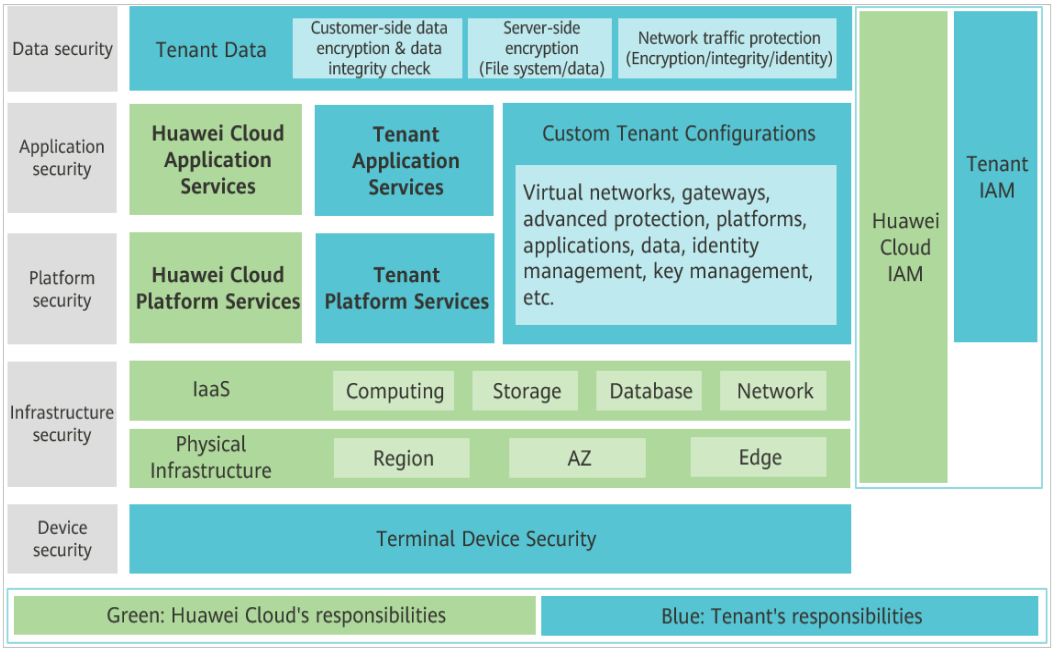
Figure 6-1 shows the responsibilities shared by you (tenants) and Huawei Cloud.

- **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 6-1 Shared responsibility model of Huawei Cloud



6.2 Identity Authentication and Access Control

A 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 6-2 Identity and access management

6.3 Data Protection Technologies

- IPsec 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 IPsec VPN connection, you can configure data encryption and authentication algorithms in an IPsec policy.

  Common commercial cryptographic algorithms are supported. The recommended algorithms are listed as follows in descending order of security:

  - Encryption algorithms:
    - AES-256-GCM-16
    - AES-128-GCM-16
    - AES-256
    - AES-192
    - AES-128
  - Authentication algorithms:
    - SHA2-512
    - SHA2-384
    - SHA2-256

PFS

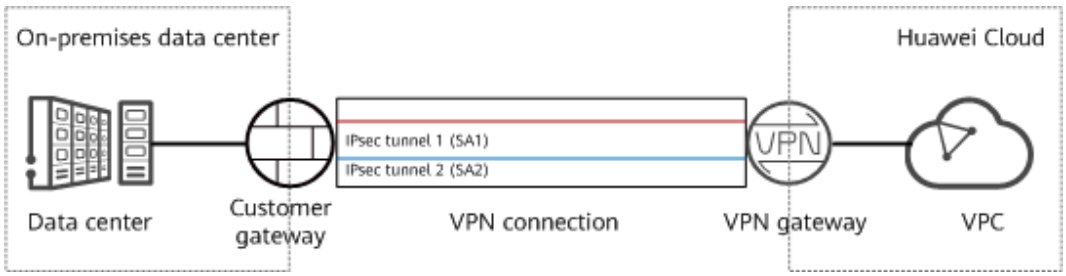
Perfect Forward Secrecy (PFS) ensures that the compromise of the keys of an IPsec tunnel does not affect the security of other tunnels by leveraging that the keys of these tunnels are irrelevant to each other. By default, PFS is enabled for the VPN service.

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

Common PFS algorithms are supported. The recommended algorithms are as follows:

- DH group 15
- DH group 16
- DH group 19
- DH group 20
- DH group 21

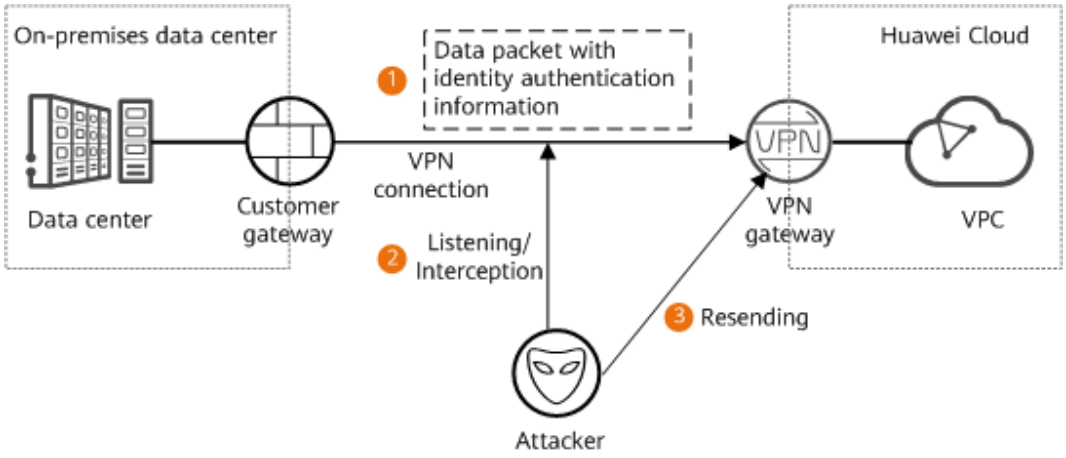
Figure 6-3 PFS



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.

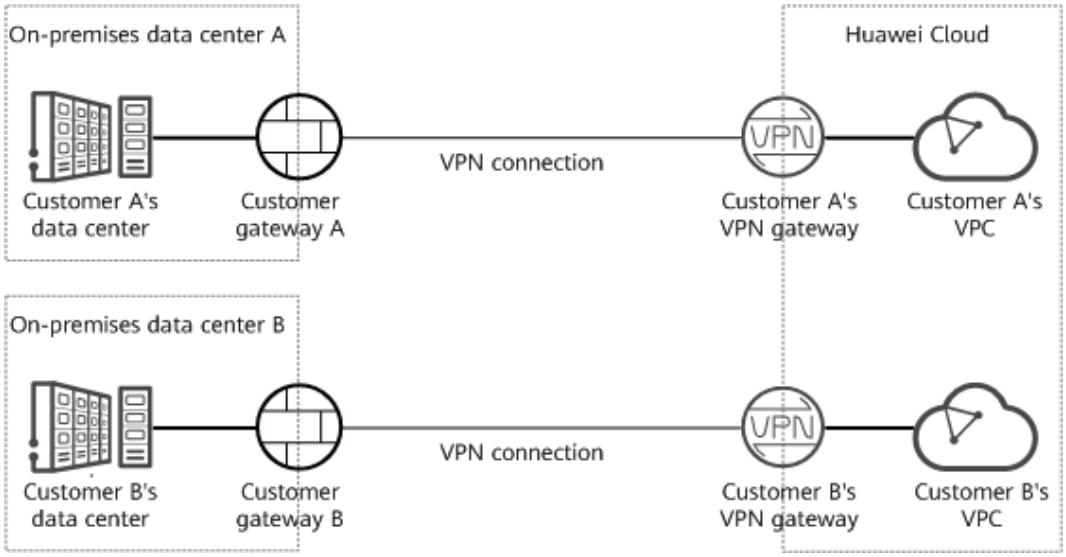
Figure 6-4 Replay attack



Resource Isolation

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

Figure 6-5 Data isolation

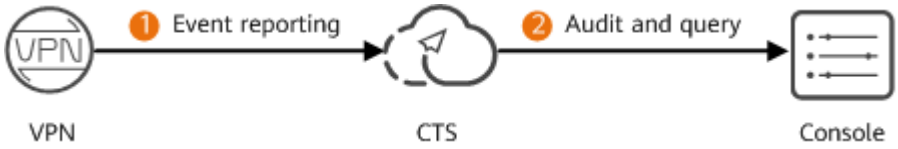


As shown in the figure, a failure of customer A's VPN gateway has no impact on customer B's VPN gateway.

6.4 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.

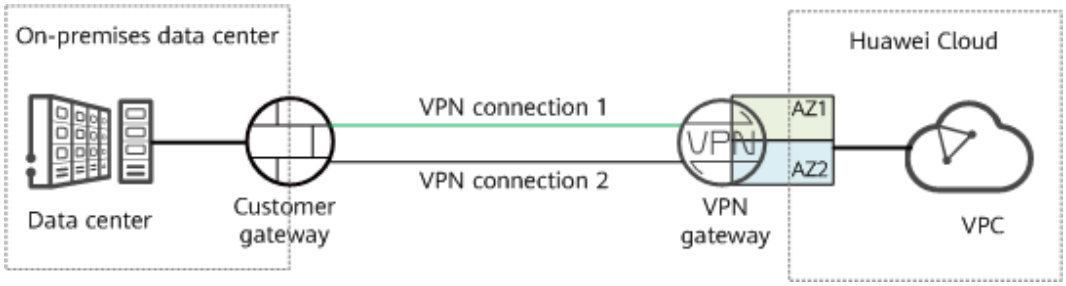
Figure 6-6 Audit and logs



6.5 Service Resilience

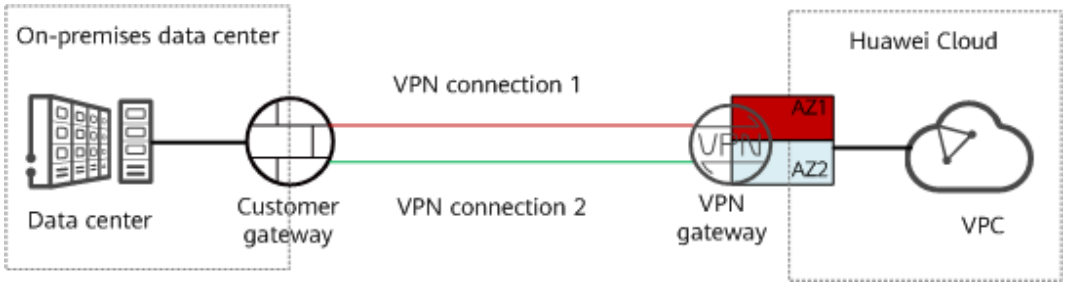
VPN provides the dual-AZ disaster recovery function. You can create a VPN gateway in two AZs in the same region, and create a VPN connection between the customer gateway and each AZ.

Figure 6-7 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 6-8 Failover scenario



7 Permission Management

If you need to assign different permissions to employees in your enterprise to access your VPN resources 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 Huawei Cloud 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, you may skip over this topic.

IAM is free. You pay only for the resources in your account. For more information about IAM, see **What Is IAM?**.

VPN Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

VPN is a project-level service deployed in specific physical regions. To assign VPN permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing VPN, the users need to switch to a region where they have been authorized to use this service.

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, you can grant VPN users only the permissions required for managing a certain type of ECSs.

Table 7-1 lists all system-defined roles and permissions supported by VPN.

Table 7-1 VPN system-defined roles and permissions

System Role/ Policy Name	Description	Dependency
VPN Administrator	All operations on VPN resources. Users with this permission 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	Full permissions for VPN.	To perform the following operations, you need to configure the **VPC Administrator** and **Tenant Guest** permissions in addition to the **VPN FullAccess** permission: • Creating VPN connections
VPN ReadOnlyAccess	Read-only permissions on VPN resources. Users who have these permissions can only view information about VPN resources.	N/A

Table 7-2 lists the common operations supported by each system-defined policy of VPN. Select the permissions as needed.

Table 7-2 Common operations supported by **VPN Administrator**

Operation	VPN Administrator	VPN FullAccess	VPN ReadOnlyAccess
Creating a VPN gateway	Supported	√	×
Viewing a VPN gateway	Supported	√	√
Modifying a VPN gateway	Supported	√	×
Deleting a VPN gateway	Supported	√	×
Creating a VPN connection	Supported	×	×
Viewing a VPN connection	Supported	√	√
Modifying a VPN connection	Supported	×	×
Deleting a VPN connection	Supported	×	×
Creating a customer gateway	√	√	×
Viewing a customer gateway	√	√	√
Modifying a customer gateway	√	√	×
Deleting a customer gateway	√	√	×

Helpful Links

- **What Is IAM?**
- **Creating a User and Granting VPN Permissions**

8 VPN and Other Services

Figure 8-1 shows VPN-related services.

Figure 8-1 VPN and related services

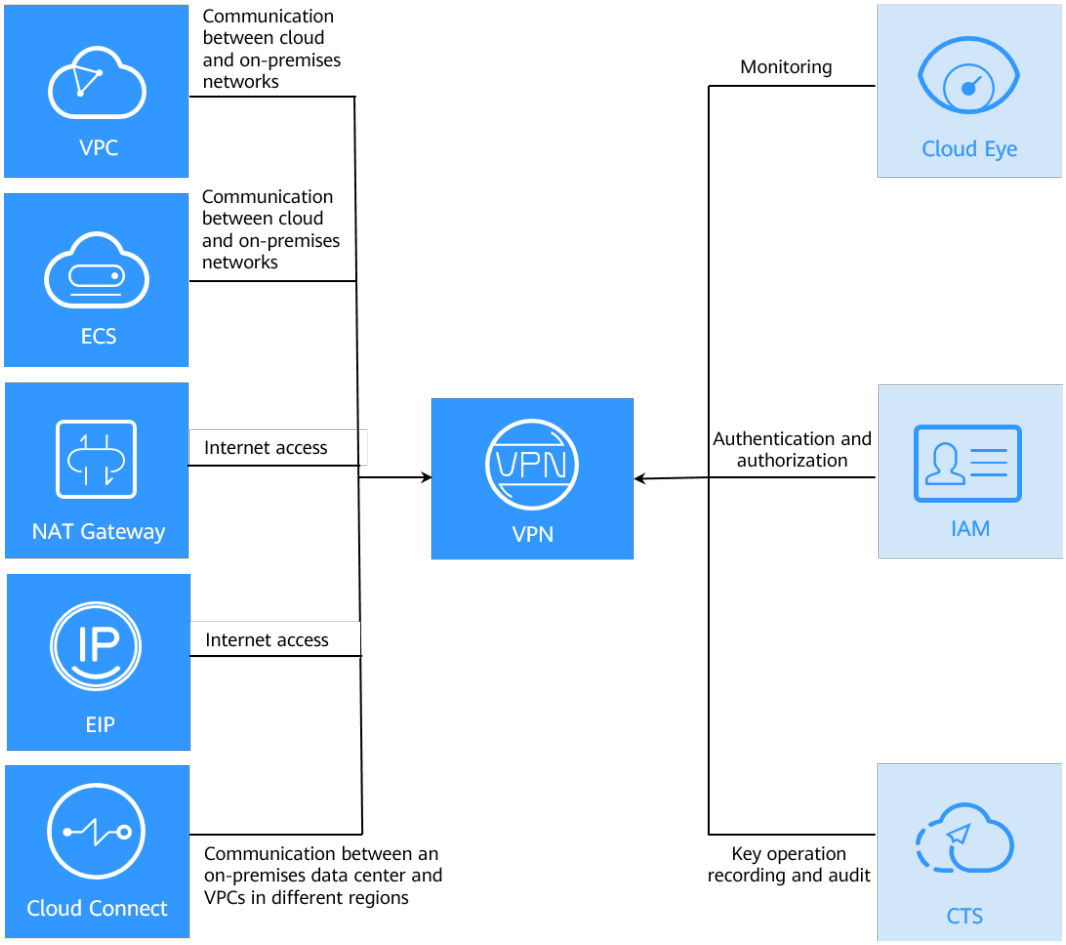


Table 8-1 Related services

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**
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 VPN.	**Elastic IP**
Cloud Connect	Works together with VPN to enable stable network communications between your on-premises data center and VPCs in different regions.	-
Cloud Eye	Monitors VPN resources and allows you to view metrics.	**Cloud Eye**
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**
Cloud Trace Service (CTS)	Records operations performed on VPN.	**Cloud Trace Service**

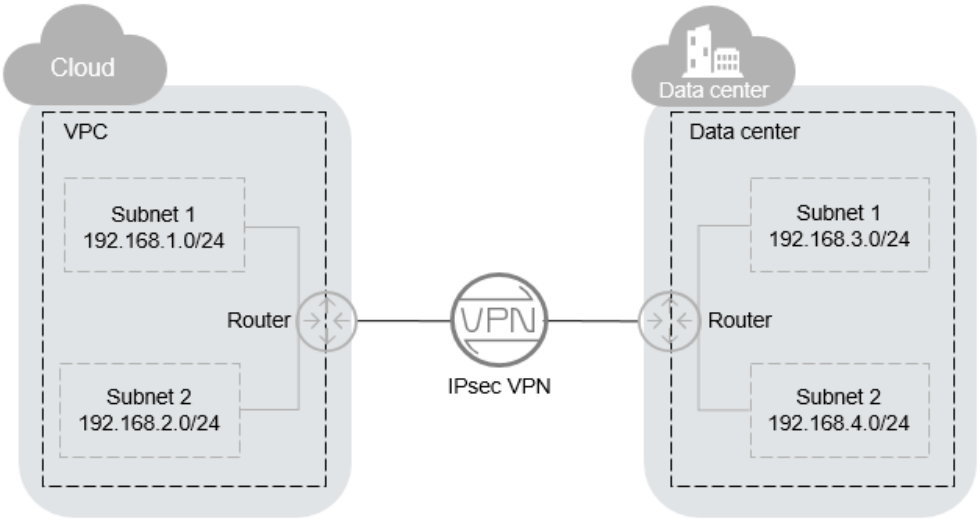
9 Basic Concepts

9.1 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 9-1**, 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 9-1 IPsec VPN



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

9.2 VPN Gateway

A VPN gateway is a virtual gateway of a VPN on Huawei 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.

9.3 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.

9.4 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.

9.5 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.

9.6 Customer Gateway

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

9.7 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.

9.8 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.

