Virtual Private Network

User Guide

Issue 01

Date 2025-09-17





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

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

Trademarks and Permissions

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

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:

https://www.huawei.com/en/psirt/vul-response-process

For vulnerability information, enterprise customers can visit the following web page:

https://securitybulletin.huawei.com/enterprise/en/security-advisory

1 Overview

1.1 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

VPN supports only non-inter-border connections.

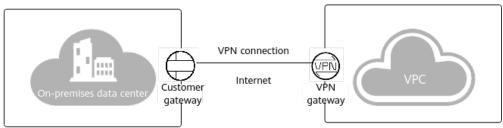
Site-to-Cloud VPN (S2C VPN) uses the Internet Protocol Security (IPsec) protocol and has two editions: Classic VPN and Enterprise Edition VPN.

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 onpremises 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**: 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.

1.2 Product Advantages

Enterprise Edition VPN has the following advantages:

High security

- Data is encrypted using IKE/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 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.
- 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 elastic IP addresses (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 policybased, 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 onpremises 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.

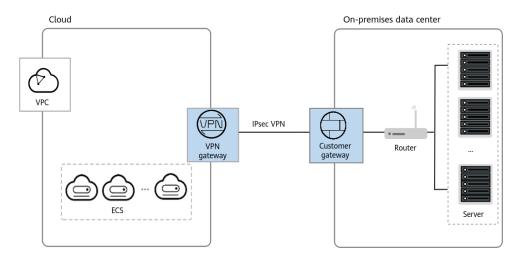
 In S2C VPN, you can flexibly enable or disable branch interconnection to implement interconnection or isolation between customer gateways, respectively.

1.3 Application Scenarios

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 1-2 shows the hybrid cloud deployment.

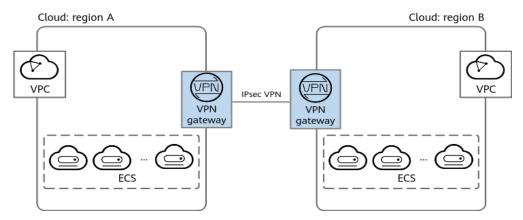
Figure 1-2 Hybrid cloud deployment



Inter-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 1-3**.

Figure 1-3 Inter-region interconnection between VPCs



Enterprise Branch Interconnection

A VPN gateway functions as a VPN hub to connect enterprise branches, as shown in **Figure 1-4**. This eliminates the need to configure VPN connections between every two branches.

Cloud

Branch 1

VPC

VPC

VPN

IPsec VPN

IPsec VPN

Customer gateway

Data center

Customer gateway

Data center

Data center

Data center

Figure 1-4 Enterprise branch interconnection

1.4 Product Specifications

Table 1-1 S2C VPN specifications

Item	Professional 1	Professional 2
Exclusive gateway resources	Supported	Supported
Dual connections	Supported	Supported
Active-active gateways	Supported	Supported
Active/Standby gateways	Supported	Supported
Policy-based mode	Supported	Supported
Routing mode: static routing	Supported	Supported
Routing mode: BGP routing	Supported	Supported
Maximum forwarding bandwidth	300 Mbit/s	1 Gbit/s
Maximum number of VPN connection groups	100	100
Private network	Supported	Supported
Supported regions	Subject to the regions available on the management console	Subject to the regions available on the management console

1.5 Quotas and Limitations

VPN Gateway

Table 1-2 Constraints on VPN gateways

VPN Type	Resource	Default Quota
Enterprise Edition VPN	VPN gateways per tenant in each region	 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.
	VPN connection groups per VPN gateway	100
	Local subnets per VPN gateway	50
	Number of BGP routes that can be accepted by VPN gateways of different specifications	 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 routes supported by a VPN gateway	10000
	Maximum number of ACL rules supported by VPN gateways of different specifications	Other specifications: A maximum of 300 ACL rules are supported for each IP address of a VPN gateway.

VPN Type	Resource	Default Quota
Classic VPN	VPN gateways per tenant in each region	2 Only one VPN gateway can be created for a VPC.

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

Customer Gateway

Table 1-3 Constraints on customer gateways

VPN Type	Resource	Default Quota
Enterprise Edition VPN	Customer gateways per tenant in each region	100

- 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 1-4 Constraints on VPN connections

VPN Type	Resource	Default Quota	How to Increase Quota
	Policy rules per VPN connection	5	The quotas cannot be
VPN	Customer subnets per VPN connection	50	increased.

VPN Type	Resource	Default Quota	How to Increase Quota
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 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.

For a VPN gateway of the Professional 1 or Professional 2 specification, a single IP address can be used to establish a maximum of 300 communications tunnels with customer gateways.

- In routing mode, each VPN connection occupies only one communications tunnel of the corresponding VPN gateway IP address.
- In policy-based 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.

For a VPN gateway of the Professional 1 or Professional 2 specification, a maximum of 300 source and destination subnet pairs are supported for each IP address used to establish connections with customer gateways.

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

If the number of communications tunnels occupied by VPN connections in different modes established by a single IP address of a VPN gateway of the Professional 1 or Professional 2 specification exceeds 300, 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.

1.6 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)

1.7 Differences between S2C Enterprise Edition VPN and Classic VPN

Table 1-5 Differences between Enterprise Edition VPN and Classic VPN

Category	Item Enterprise Edi VPN		Classic VPN
Tenant isolation	Tenant-exclusive Supported gateway		Not supported
Features	Policy-based mode	Supported	Supported
	Routing mode	Static routing and BGP routing	Not supported
	VPN hub	Supported	Not supported
	Enterprise router	Not supported	Not supported
	Network type	Public network and private network	Public network
Capacity	Number of subnets	Route-based mode: 50Policy-based mode: 5	Policy-based mode: 5
	For more information	, see Table 1-1.	
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

1.8 Permissions Management

1.8.1 IAM-based Permissions Management

If you need to assign different permissions to personnel in your enterprise to access your VPN resources created on the cloud service platform, 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 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 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.

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

For more information about IAM, see the *Identity and Access Management User Guide*.

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 1-6 lists all system-defined permissions for VPN.

Table 1-6 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. This role must be used together with the Tenant Guest and VPC Administrator roles in the same project. • 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 (recommende d)	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:li st" • "scm:cert:list" • "scm:cert:download"
VPN ReadOnlyAcce ss	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 1-7 lists the common operations supported by system-defined permissions for S2C VPN.

Table 1-7 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	√	√	√
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 	✓

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
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: × 	×

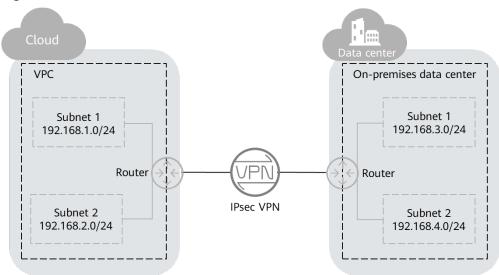
1.9 Basic Concepts

1.9.1 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. S2C VPN is an IPsec VPN technology on the cloud.

In the example shown in **Figure 1-5**, 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 1-5 IPsec VPN



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

1.9.2 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.

1.9.3 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.

1.9.4 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.

2 Getting Started

2.1 Configuring Enterprise Edition VPN to Connect an On-premises Data Center to a VPC

2.1.1 Overview

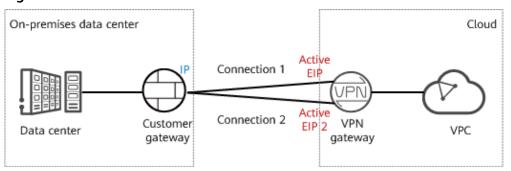
Scenario

To meet business development requirements, enterprise A needs to implement communication between its on-premises data center and its VPC. In this case, enterprise A can use the VPN service to create connections between the on-premises data center and the VPC.

• If the on-premises data center has only one customer gateway and this gateway can be configured with only one IP address, it is recommended that the VPN gateway use the active-active mode. **Figure 2-1** shows the networking.

In active-active mode, if connection 1 is faulty, traffic is automatically switched to connection 2 for transmission, without affecting enterprise services.

Figure 2-1 Active-active mode

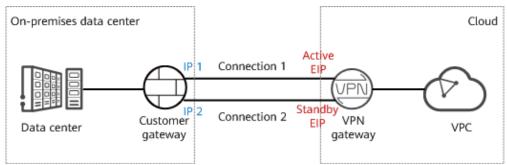


• If the on-premises data center has two customer gateways or has only one customer gateway that can be configured with two IP addresses, it is

recommended that the VPN gateway use the active/standby mode. **Figure 2-2** shows the networking.

In active/standby mode, connection 1 is the active link and connection 2 is the standby link. By default, traffic is transmitted only through the active link. If the active link fails, traffic is automatically switched to the standby link, without affecting enterprise services. After the active link recovers, traffic is switched back to the active link.

Figure 2-2 Active/Standby mode



Limitations and Constraints

- The customer gateway device must support standard IKE and IPsec protocols.
- The interconnection subnets of the on-premises data center neither overlap with those of the VPC nor contain 100.64.0.0/10 or 214.0.0.0/8.

If the VPC uses Direct Cloud or Cloud Connect connections to communicate with other VPCs, the on-premises data center subnets cannot overlap with those of these VPCs.

Data Plan

Table 2-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	192.168.0.0/16
VPN gateway	Interconnecti on subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	HA mode	Active-active

Category	Item	Data
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 11.xx.xx.11 • Active EIP 2: 11.xx.xx.12
VPN connectio n	Tunnel interface addresses under Connection 1's Configuratio n	The IP addresses are used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under Connection 2's Configuration	 Local tunnel interface address: 169.254.71.1/30 Customer tunnel interface address: 169.254.71.2/30
On- premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Gateway IP address	The gateway IP address is assigned by a carrier. In this example, the gateway IP address is: 22.xx.xx.22

Operation Process

Figure 2-3 shows the process of using the VPN service to enable communication between an on-premises data center and a VPC.

Figure 2-3 Operation process



N o.	Step	Description
1	Step 1: Creating a VPN Gateway	Bind two EIPs to the VPN gateway. If you have purchased EIPs, you can directly bind them to the VPN gateway.
2	Step 2: Creating a Customer Gateway	Configure the VPN device in the on-premises data center as the customer gateway.
3	Step 3: Creating VPN Connections	 Create two VPN connections between the VPN gateway (active EIP and active EIP 2) and the customer gateway. The connection mode, PSK, IKE policy, and IPsec policy settings of connection 2 must be the same as those of connection 1.
4	Step 4: Configuring the Customer Gateway Device	 The local and remote tunnel interface addresses configured on the customer gateway device must be the same as the customer and local tunnel interface addresses of the VPN connections, respectively. The connection mode, PSK, IKE policy, and IPsec policy settings on the customer gateway device must be same as those of the VPN connections.
5	Step 5: Verifying Network Connectivity	Log in to an ECS and run the ping command to verify the network connectivity.

Table 2-2 Operation process description

2.1.2 Step 1: Creating a VPN Gateway

Prerequisites

- A VPC has been created. For details about how to create a VPC, see the *Virtual Private Cloud User Guide*.
- Security group rules have been configured for ECSs in the VPC, and allow the
 customer gateway in the on-premises data center to access VPC resources. For
 details about how to configure security group rules, see the Virtual Private
 Cloud User Guide.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner, and choose > .
- Step 3 In the navigation pane on the left, choose Virtual Private Network > Enterprise VPN Gateways.

- Step 4 Click Buy S2C VPN Gateway.
- **Step 5** Set parameters as prompted, click **Create Now**, and complete the payment.
- **Step 6** The following describes only key parameters.

Table 2-3 Key VPN gateway parameters

Parameter	Description	Example Value
Region	Select the region nearest to you.	-
Name	Enter the name a VPN gateway.	vpngw-001
Network Type	 Public network: A VPN gateway communicates with a customer gateway in an on-premises data center through the Internet. Private network: A VPN gateway communicates with a customer gateway in an on-premises data center through a private network. 	Public network
Associate With	VPC: Through a VPC, the VPN gateway sends messages to the customer gateway or servers in the local subnet.	VPC
VPC	Select the VPC that needs to access the on-premises data center.	vpc-001(192.168.0.0/16
Interconne ction Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Specify the VPC subnet that needs to access the on-premises data center.	192.168.0.0/24
	You can manually enter a CIDR block or select a subnet from the drop-down list box.	
Specificati on	Select Professional 1 .	Professional 1
HA Mode	Select Active-active .	Active-active
Active EIP	You can buy a new EIP or use an existing	11.xx.xx.11
Active EIP 2	EIP.	11.xx.xx.12

----End

Verification

Check the created VPN gateway on the **VPN Gateways** page. The initial state of the VPN gateway is **Creating**. When the VPN gateway state changes to **Normal**, the VPN gateway is successfully created.

2.1.3 Step 2: Creating a Customer Gateway

Procedure

- Step 1 In the navigation pane on the left, choose Virtual Private Network > Enterprise Customer Gateways.
- **Step 2** On the **Customer Gateways** page, click **Create Customer Gateway**.
- **Step 3** Set parameters as prompted and click **Create Now**.

The following describes only key parameters.

Table 2-4 Customer gateway parameters

Parameter	Description	Example Value
Name	Name a customer gateway.	cgw-001
Identifier	Enter the IP address of the customer gateway.	IP Address, 22.xx.xx.22

----End

Verification

Check the created customer gateway on the **Customer Gateways** page.

2.1.4 Step 3: Creating VPN Connections

Procedure

- Step 1 In the navigation pane on the left, choose Virtual Private Network > Enterprise VPN Connections.
- **Step 2** On the **VPN Connection** page, click **Create VPN Connection**.
- **Step 3** Set VPN connection parameters as prompted and click **Buy Now**.

The following describes only key parameters.

Table 2-5 Description of VPN connection parameters

Parameter	Description	Example Value
Name	Enter the name of VPN connection 1.	vpn-001

Parameter	Description	Example Value
VPN Gateway	Select the VPN gateway created in 2.1.2 Step 1: Creating a VPN Gateway.	vpngw-001
VPN Gateway IP of Connection 1	Select the active EIP of the VPN gateway.	11.xx.xx.11
Customer Gateway of Connection 1	Select the customer gateway of connection 1.	cgw-001
VPN Gateway IP of Connection 2	Select active EIP 2 of the VPN gateway.	11.xx.xx.12
Customer Gateway of Connection 2	Select the customer gateway of connection 2.	cgw-001
VPN Type	Select Static routing .	Static routing
Customer Subnet	 Enter the subnet of the on-premises data center that needs to access the VPC. NOTE The customer subnet can overlap with the local subnet but cannot be the same as the local subnet. A customer subnet cannot be included in the existing subnets of the VPC associated with the VPN gateway. It also cannot be the destination address in the route table of the VPC associated with the VPN gateway. Customer subnets cannot be the reserved CIDR blocks of VPCs, for example, 100.64.0.0/10 or 214.0.0.0/8. If the interconnection subnet is associated with an ACL rule, ensure that the ACL rule permits the TCP port for traffic between all local and customer subnets. Address groups cannot be used to configure the source and destination subnets in a policy on customer gateway devices. 	172.16.0.0/16

Parameter	Description	Example Value
Connection 1's Configuration	Configure the IP address assignment mode of gateway interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	Set parameters based on the site requirements.
Interface IP Address Assignment	The options include Manually specify and Automatically assign.	Manually specify
Local Tunnel Interface Address	Specify the tunnel interface address of the VPN gateway. NOTE The local and remote interface addresses configured on the customer gateway device must be the same as the values of Customer Tunnel Interface IP Address and Local Tunnel Interface IP Address, respectively.	169.254.70.2/30
Customer Tunnel Interface Address	Specify the tunnel interface address of the customer gateway device.	169.254.70.1/30
Link Detection	This function is used for route reliability detection in multi-link scenarios. NOTE When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, VPN traffic will fail to be forwarded.	NQA enabled
PSK, Confirm PSK	Specify the negotiation key of the VPN connection. The PSKs configured on the VPN console and the customer gateway device must be the same.	Test@123
Policy Settings	Configure the IKE and IPsec policies, which define the encryption algorithms used by the VPN tunnel. The policy settings on the VPN console and the customer gateway device must be the same.	Default
Connection 2's Configuration	Determine whether to enable Same as that of connection 1.	Disabled

Parameter	Description	Example Value
Local Tunnel Interface Address	Specify the tunnel interface address of the VPN gateway.	169.254.71.2/30
Customer Tunnel Interface Address	Specify the tunnel interface address of the customer gateway device.	169.254.71.1/30

----End

Verification

Check the created VPN connection on the **VPN Connection** page. The initial state of the VPN connection is **Creating**. As the customer gateway device has not been configured, no VPN connection can be established. After about 2 minutes, the VPN connection state changes to **Not connected**.

2.1.5 Step 4: Configuring the Customer Gateway Device

Procedure

In this example, the customer gateway device is an AR router.

- **Step 1** Log in to the AR router.
- **Step 2** Enter the system view.

<AR651>system-view

Step 3 Configure an IP address for the WAN interface. In this example, the WAN interface of the AR router is GigabitEthernet 0/0/8.

[AR651]interface GigabitEthernet 0/0/8 [AR651-GigabitEthernet0/0/8]ip address 22.xx.xx.22 255.255.255.0 [AR651-GigabitEthernet0/0/8]quit

Step 4 Configure a default route.

[AR651]ip route-static 0.0.0.0 0.0.0.0 22.xx.xx.1

In this command, 22.xx.xx.1 is the gateway address of the AR router's public IP address. Replace it with the actual gateway address.

- **Step 5** Enable the SHA-2 algorithm to be compatible with the standard RFC algorithms. [AR651]IPsec authentication sha2 compatible enable
- Step 6 Configure an IPsec proposal.

[AR651]IPsec proposal hwproposal1 [AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256 [AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128 [AR651-IPsec-proposal-hwproposal1]quit

Step 7 Configure an IKE proposal.

```
[AR651]ike proposal 2
[AR651-ike-proposal-2]encryption-algorithm aes-128
[AR651-ike-proposal-2]dh group14
[AR651-ike-proposal-2]authentication-algorithm sha2-256
[AR651-ike-proposal-2]authentication-method pre-share
[AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
[AR651-ike-proposal-2]prf hmac-sha2-256
[AR651-ike-proposal-2]quit
```

Step 8 Configure IKE peers.

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]undo version 1
[AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer1]ike-proposal 2
[AR651-ike-peer-hwpeer1]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer1]remote-address 11.xx.xx.11
[AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer1]rsa signature-padding pss
[AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer1]quit
[AR651]ike peer hwpeer2
[AR651-ike-peer-hwpeer2]undo version 1
[AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer2]ike-proposal 2
[AR651-ike-peer-hwpeer2]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer2]remote-address 11.xx.xx.12
[AR651-ike-peer-hwpeer2]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer2]rsa signature-padding pss
[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer2]quit
```

The commands are described as follows:

- **pre-shared-key cipher**: configures a PSK, which must be the same as that configured on the VPN console.
- local-address: specifies the public IP address of the AR router.
- remote-address: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 9 Configure an IPsec profile.

```
[AR651]IPsec profile hwpro1
[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1
[AR651-IPsec-profile-hwpro1]proposal hwproposal1
[AR651-IPsec-profile-hwpro1]pfs dh-group14
[AR651-IPsec-profile-hwpro1]quit
[AR651]IPsec profile hwpro2
[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2
[AR651-IPsec-profile-hwpro2]proposal hwproposal1
[AR651-IPsec-profile-hwpro2]pfs dh-group14
[AR651-IPsec-profile-hwpro2]quit
```

Step 10 Configure virtual tunnel interfaces.

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 22.xx.xx.22
[AR651-Tunnel0/0/1] destination 11.xx.xx.11
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 22.xx.xx.22
[AR651-Tunnel0/0/2] destination 11.xx.xx.12
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

The commands are described as follows:

• interface Tunnel0/0/1 and interface Tunnel0/0/2: indicate the tunnel interfaces corresponding to the two VPN connections.

In this example, Tunnel0/0/1 establishes a VPN connection with the active EIP of the VPN gateway, and Tunnel0/0/2 establishes a VPN connection with active EIP 2 of the VPN gateway.

- **ip address**: configures an IP address for a tunnel interface on the AR router.
- **source**: specifies the public IP address of the AR router.
- **destination**: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 11 Configure NQA.

```
[AR651]nga test-instance IPsec_nga1 IPsec_nga1
[AR651-nga-IPsec_nga1-IPsec_nga1]test-type icmp
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
[AR651-nga-IPsec_nga2-IPsec_nga2]destination-address ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nga-IPsec_nga2-IPsec_nga2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nga-IPsec_nga2-IPsec_nga2]quit
```

The commands are described as follows:

nqa test-instance IPsec_nqa1 IPsec_nqa1 and nqa test-instance IPsec_nqa2
 IPsec_nqa2: configure two NQA test instances named IPsec_nqa1 and IPsec_nqa2.

In this example, the test instance <code>IPsec_nqa1</code> is created for the VPN connection to which the active EIP of the VPN gateway belongs; the test instance <code>IPsec_nqa2</code> is created for the VPN connection to which active EIP 2 of the VPN gateway belongs.

- destination-address: specifies the tunnel interface address of the VPN connection.
- **source-address**: specifies the tunnel interface address of the AR router.

Step 12 Configure association between the static route and NQA.

```
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/1 track nga IPsec_nga1 IPsec_nga1 [AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 track nga IPsec_nga2 IPsec_nga2
```

The parameters are described as follows:

- 192.168.0.0 indicates the local subnet of the VPC.
- **Tunnel** *x* and **IPsec_nqa** *x* in the same command correspond to the same VPN connection.

----End

Verification

Step 1 Log in to the management console.

- Step 2 Click in the upper left corner, and choose > .
- Step 3 In the navigation pane on the left, choose Virtual Private Network > Enterprise VPN Connections.

Verify that the states of the two VPN connections are both **Normal**.

----End

2.1.6 Step 5: Verifying Network Connectivity

Procedure

- **Step 1** Log in to the management console.
- **Step 2** Click on the upper left corner and select the desired region and project.
- **Step 3** Click **Service List** and choose **Compute > Elastic Cloud Server**.
- Step 4 Log in to an ECS.

Login using VNC on the management console is used as an example.

Step 5 Run the following command on the ECS:

ping 172.16.0.100

172.16.0.100 is the IP address of a server in the on-premises data center. Replace it with an actual server IP address.

If information similar to the following is displayed, the VPC on the cloud and the on-premises data center can communicate with each other.

```
Reply from xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=27ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=27ms TTL=245
```

----End

2.2 Configuring S2C Classic VPN to Connect an Onpremises Data Center to a VPC

2.2.1 Buying a VPN Gateway

Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, buy a VPN gateway first.

Prerequisites

A VPC has been created. For details about how to create a VPC, see .

• Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see .

Procedure

- 1. Log in to the management console.
- 2. Click \bigcirc in the upper left corner and select the desired region and project.
- 3. Click Service List and choose Networking > Virtual Private Network.
- 4. On the console homepage, under **Network**, click **Virtual Private Cloud**.
- In the navigation pane on the left, choose Virtual Private Network > Classic
 VPN Gateways.

If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.

- 6. On the VPN Gateways page, click Create VPN Gateway.
- 7. Configure parameters based on Table 2-6, and click Create NowNext.

Table 2-6 Description of VPN gateway parameters

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	
Name	Name of a VPN gateway.	vpngw-001
VPC	Name of the VPC to which the VPN gateway connects.	vpc-001
Туре	VPN type. IPsec is selected by default.	IPsec
Reliability	Only Active-active is supported.	Active-active
Bandwidth (Mbit/s)	The bandwidth of the VPN gateway. The bandwidth is shared by all VPN connections created for the VPN gateway. The total bandwidth size used by all VPN connections created for a VPN gateway cannot exceed the VPN gateway bandwidth size.	10

Table 2-7 Description of VPN connection parameters

Parameter	Description	Example Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created.	vpcgw-001
Local Subnet	 VPC subnets that will access your on-premises network through a VPN. You can set the local subnet using either of the following methods: Select subnet: Select the subnets that need to access your onpremises data center or private network. Specify CIDR block: Enter the CIDR blocks that need to access your on-premises data center or private network. 	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC. In active-active mode, you can enter two remote gateway addresses.	N/A
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnet cannot overlap with CIDR blocks involved in existing VPC peering, Direct Connect, or Cloud Connect connections created for the local VPC.	192.168.3.0/24, 192.168.4.0/24
PSK	PSKs configured at both ends of a VPN connection must be the same. The PSK: Contains 6 to 128 characters. Can contain only: Digits Letters Special characters: ~ `! @ # \$ % ^ () + = [] { } . / :;	Test@123
Confirm PSK	Enter the PSK again.	Test@123

Parameter	Description	Example Value
Advanced Settings	Default: Use default IKE and IPsec policies.	Custom
	Custom: Use custom IKE and IPsec policies. For details, see Table 2-8 and Table 2-9.	

Table 2-8 IKE policy

Parameter	Description	Example Value
Authenticati on Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5(Insecure. Not recommended.) • SHA1(Insecure. Not recommended.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is SHA2-256.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES(Insecure. Not recommended.) The default algorithm is AES-128.	AES-128

Parameter	Description	Example Value
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported:	Group 14
	Group 1(Insecure. Not recommended.)	
	Group 2(Insecure. Not recommended.)	
	Group 5(Insecure. Not recommended.)	
	Group 14	
	Group 15	
	Group 16	
	Group 19	
	Group 20	
	• Group 21	
	The default value is Group 14 .	
	DH algorithms configured at both ends of a VPN connection must be the same. Otherwise, the negotiation will fail.	
Version	Version of the IKE protocol. The value can be one of the following:	v2
	v1 (not recommended due to security risks)	
	• v2	
	The default value is v2 .	
Lifetime (s)	Lifetime of an SA, in seconds	86400
	An SA will be renegotiated when its lifetime expires.	
	The default value is 86400 .	

Table 2-9 IPsec policy

Parameter	Description	Example Value
Authenticatio n Algorithm	Hash algorithm used for authentication. The following algorithms are supported: SHA1(Insecure. Not recommended.) MD5(Insecure. Not recommended.) SHA2-256 SHA2-384 SHA2-512 The default algorithm is SHA2-256.	SHA2-256

Parameter	Description	Example Value
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES(Insecure. Not recommended.) The default algorithm is AES-128.	AES-128
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: DH group 1(Insecure. Not recommended.) DH group 2(Insecure. Not recommended.) DH group 5(Insecure. Not recommended.) DH group 14 DH group 15 DH group 16 DH group 19 DH group 20 DH group 21 The default algorithm is DH group 14 .	DH group 14
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • ESP • AH • AH-ESP The default protocol is ESP.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is 3600 .	3600

8. Confirm the VPN gateway information and click **Submit**.

2.2.2 Buying a VPN Connection

Scenarios

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

Procedure

- 1. Log in to the management console.
- 2. Click $^{\circ}$ in the upper left corner and select the desired region and project.
- 3. Click Service List and choose Networking > Virtual Private Network.
- 4. On the console homepage, under **Network**, click **Virtual Private Cloud**.
- In the navigation pane on the left, choose Virtual Private Network > Classic
 VPN Connections.

If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.

- 6. On the VPN Connections page, click Create VPN Connection.
- 7. Configure the parameters as prompted and click **Create Now**. **Table 2-10** describes the VPN connection parameters.

Table 2-10 Description of VPN connection parameters

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	N/A
Name	Name of a VPN connection.	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created.	vpcgw-001
Local Subnet	VPC subnets that will access your on- premises network through a VPN. You can set the local subnet using either of the following methods:	192.168.1.0/24, 192.168.2.0/24
	Select subnet: Select the subnets that need to access your on-premises data center or private network.	
	Specify CIDR block: Enter the CIDR blocks that need to access your onpremises data center or private network.	

Parameter	Description	Example Value
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC. In active-active mode, you can enter two remote gateway addresses.	N/A
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnet cannot overlap with CIDR blocks involved in existing VPC peering, Direct Connect, or Cloud Connect connections created for the local VPC.	192.168.3.0/24, 192.168.4.0/24
PSK	Private key shared by two ends of a VPN connection for negotiation. PSKs configured at both ends of the VPN connection must be the same. The PSK: Contains 6 to 128 characters. Can contain only: Digits Letters Special characters: ~ `! @ # \$ % ^ () + = [] { } . / :;	Test@123
Confirm PSK	Enter the PSK again.	Test@123
Advanced Settings	 Default: Use default IKE and IPsec policies. Existing: Use existing IKE and IPsec policies. Custom: including IKE Policy and IPsec Policy, which specifies the encryption and authentication algorithms of a VPN tunnel. For details, see Table 2-11 and Table 2-12. 	Custom

Table 2-11 IKE policy

Parameter	Description	Example Value
Authenticatio n Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5(Insecure. Not recommended.) • SHA1(Insecure. Not recommended.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is SHA1. The default algorithm is SHA2-256.	SHA1 SHA2-256
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES(Insecure. Not recommended.) The default algorithm is AES-128.	AES-128
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported: Group 1(Insecure. Not recommended.) Group 2(Insecure. Not recommended.) Group 5(Insecure. Not recommended.) Group 14 Group 15 Group 16 Group 19 Group 20 Group 21 The default algorithm is Group 14 .	Group 5 Group 14

Parameter	Description	Example Value
Version	Version of the IKE protocol. The value can be one of the following:	v2
	 v1 (not recommended due to security risks) 	
	• v2	
	The default value is v2 .	
Lifetime (s)	Lifetime of an SA, in seconds	86400
	An SA will be renegotiated when its lifetime expires.	
	The default value is 86400 .	
Negotiation Mode	This parameter is available only when Version is set to v1 . You can set Negotiation Mode to Main or Aggressive .	Main
	The default mode is Main .	

Table 2-12 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported:	SHA1 SHA2-256
	SHA1(Insecure. Not recommended.)	
	 MD5(Insecure. Not recommended.) 	
	• SHA2-256	
	• SHA2-384	
	• SHA2-512	
	The default algorithm is SHA2-256 .	
Encryption Algorithm	Encryption algorithm. The following algorithms are supported:	AES-128
	• AES-128	
	• AES-192	
	• AES-256	
	3DES(Insecure. Not recommended.)	
	The default algorithm is AES-128.	

Parameter	Description	Example Value
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: DH group 1 (Insecure. Not recommended.) DH group 2 (Insecure. Not recommended.) DH group 5 (Insecure. Not recommended.) DH group 14 DH group 15 DH group 16 DH group 19 DH group 20 DH group 21 The default algorithm is DH group 14.	DH group 5 DH group 14
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • AH • ESP • AH-ESP The default protocol is ESP.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is 3600 .	3600

□ NOTE

An IKE policy specifies the encryption and authentication algorithms to be used in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to be used in the data transmission phase of an IPsec tunnel. The IKE and IPsec policies must be the same at both ends of a VPN connection. If they are different, the VPN connection cannot be set up.

8. Click **Submit**.

3 Management

3.1 Enterprise Edition S2C VPN

3.1.1 Enterprise Edition VPN Gateway Management

3.1.1.1 Creating a VPN Gateway

Scenario

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

Context

The recommended networking varies according to the number of customer gateway IP addresses, as described in **Table 3-1**.

Table 3-1 Networking

Number of Custome r Gateway IP Addresse s	Recommended Networking	Description
1	Customer gateway VPN connection 2 Active EIP VPN Active EIP VPN gateway	It is recommended that the VPN gateway uses the active-active mode. In this case, one VPN connection group is used.

Number of Custome r Gateway IP Addresse s	Recommended Networking	Description
2	Customer VPN connection 1 Active EIP Customer VPN connection 2 Standby EIP VPN gateway gateway	It is recommended that the VPN gateway uses the active/standby mode. In this case, two VPN connection groups are used.

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

Prerequisites

- A VPC has been created. For details about how to create a VPC, see the *Virtual Private Cloud User Guide*.
- Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the Virtual Private Cloud User Guide.

- **Step 1** Log in to the management console.
- **Step 2** Click in the upper left corner and select the desired region and project.
- Step 3 Click in the upper left corner, and choose > .
- **Step 4** In the navigation pane on the left, choose **Virtual Private Network > Enterprise VPN Gateways**.
- Step 5 Click Buy S2C VPN Gateway.
- **Step 6** Set parameters as prompted and click **Create Now**.

Table 3-2 lists the VPN gateway parameters.

Table 3-2 Description of VPN gateway parameters

Paramete r	Description	Example Value
Region	For low network latency and fast resource access, select the region nearest to your target users.	Select a region as required.
	Resources cannot be shared across regions.	
Name	Name of a VPN gateway. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	vpngw-001
Network Type	 Public network: A VPN gateway establishes VPN connections through the Internet. Private network: A VPN gateway establishes VPN connections through a private network. 	Public network
Associate With	VPC Through a VPC, the VPN gateway sends messages to the customer gateway or servers in the local subnet.	VPC
VPC	Select a VPC.	vpc-001(192.168. 0.0/16)
Interconn ection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.66.0/24
Local Subnet	Specify the VPC subnets with which your onpremises data center needs to communicate through the customer gateway. Select subnet Select subnets of the local VPC. Enter CIDR block Enter subnets of the local VPC or subnets of the VPC that establishes a peering connection with the local VPC.	192.168.1.0/24,19 2.168.2.0/24
BGP ASN	BGP ASN of the VPN gateway, which must be different from that of the customer gateway.	64512

Paramete r	Description	Example Value
HA Mode	 Active-active When Associate With is set to VPC, the outgoing traffic from the VPN gateway to the customer subnet is preferentially forwarded through the first VPN connection (VPN connection 1) set up between the customer subnet and an EIP. If VPN connection 1 fails, the outgoing traffic is automatically switched to the other VPN connection (VPN connection 2) set up with the customer subnet. After VPN connection 1 recovers, the outgoing traffic is still transmitted through VPN connection 2 and will not be switched back to VPN connection 1. Active/Standby The outgoing traffic from the VPN gateway to the customer subnet is preferentially transmitted through the VPN connection (VPN connection 1) set up between the customer subnet and the active EIP. If VPN connection 1 fails, the outgoing traffic is automatically switched to the other VPN connection (VPN connection 2) set up between the customer subnet and the standby EIP. After VPN connection 1 recovers, the outgoing traffic is automatically switched back to VPN connection 1. 	Active-active
Specificati on	Two options are available: Professional 1 and Professional 2 .	Professional 1
Shared Bandwidt h	When Billing Mode is set to Pay-per-use , the shared bandwidth is disabled by default.	Disabled
EIP Type	Select the type of the EIP to be bound to the VPN gateway.	Set this parameter based on the site requirements.
Bandwidt h Name	Specify the name of the EIP bandwidth.	Vpngw- bandwidth2

Paramete r	Description	Example Value
Active EIP	 EIP used by the VPN gateway to communicate with a customer gateway. Create now: Create an EIP. Use existing: Use an existing EIP. This EIP can share bandwidth with the EIPs of other network services. 	Create Now
Bandwidt h (Mbit/s)	 Bandwidth of the EIP, in Mbit/s. All VPN connections created using the EIP share the bandwidth of the EIP. The total bandwidth consumed by all the VPN connections cannot exceed the bandwidth of the EIP. If network traffic exceeds the bandwidth of the EIP, network congestion may occur and VPN connections may be interrupted. As such, ensure that you configure enough bandwidth. You can configure alarm rules on Cloud Eye to monitor the bandwidth. You can customize the bandwidth within the allowed range. 	10 Mbit/s
Active EIP 2	A VPN gateway needs to be bound to a group of EIPs (active EIP and active EIP 2). You can plan the bandwidth for each EIP. The EIPs can share bandwidth with the EIPs of other network services.	Create Now
Standby EIP	A VPN gateway needs to be bound to a group of EIPs (active EIP and standby EIP). You can plan the bandwidth for each EIP. The EIPs can share bandwidth with the EIPs of other network services. NOTE When Billing Mode of the VPN gateway is Pay-peruse and the backup EIP is billed by traffic, you are advised to configure alarm rules on Cloud Eye to monitor the backup EIP. This prevents traffic fee overrun caused by VPN connection switching due to a fault of the active VPN connection. For details about how to configure alarm rules on Cloud Eye, see the Elastic IP User Guide.	Create Now
Enterprise Project	Enterprise project to which the VPN belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The default project is default .	default

Paramete r	Description	Example Value
Access VPC	If a VPN gateway needs to connect to different VPCs in the southbound and northbound directions, set the VPC in the northbound direction as the access VPC. The VPC in the southbound direction is the VPC associated with the VPN gateway.	Same as the associated VPC
Access Subnet	By default, a VPN gateway uses the interconnection subnet to connect to the associated VPC. Set this parameter when another subnet needs to be used.	Same as the interconnection subnet

----End

3.1.1.2 Viewing a VPN Gateway

Scenario

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

Procedure

- 1. Log in to the management console.
- 2. Click in the upper left corner and select the desired region and project.
- 3. Click **i** in the upper left corner, and choose > .
- 4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise VPN Gateways**.
- 5. On the **S2C VPN Gateways** tab page, view the VPN gateway list.
- 6. Click the name of a VPN gateway to view its details.
 - For VPN gateways of the public network type, you can view their basic information, EIPs, tags, and routing information.
 - For VPN gateways of the private network type, you can view their basic information, advanced settings, and routing information.

3.1.1.3 Modifying a VPN Gateway

Scenario

You can modify basic information about a VPN gateway, including the name and local subnet.

Procedure

1. Log in to the management console.

- 2. Click in the upper left corner and select the desired region and project.
- 3. Click in the upper left corner, and choose > .
- 4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise VPN Gateways**.
- 5. Locate the row that contains the target VPN gateway, and click **Modify Basic Information** in the **Operation** column.

To modify only the name of a VPN gateway, you can also click $\stackrel{\checkmark}{=}$ on the right of the VPN gateway name.

- 6. Modify the name and local subnet of the VPN gateway as prompted.
- 7. Click **OK**.

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

Table 3-3 Parameters for modifying the VPN gateway

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

Parameter	Description	Modifiable or Not
Specification	Two options are available: Professional 1 and Professional 2.	The supported specifications are subject to those displayed on the management console.
Associate With	Select VPC .	N
VPC	VPC that the on-premises data center needs to access.	N
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	N
BGP ASN	BGP AS number.	N
AZ	An AZ is a geographic location with independent power supply and network facilities in a region. AZs in the same VPC are interconnected through private networks and are physically isolated. If two or more AZs are available, select two AZs. The VPN gateway deployed in two AZs has higher availability. You are advised to select the AZs where resources in the VPC are located. If only one AZ is available, select this AZ.	N

3.1.1.4 Binding an EIP to a VPN Gateway

Scenario

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

Procedure

1. Log in to the management console.

- 2. Click $^{ extstyle ex$
- 3. Click in the upper left corner, and choose > .
- In the navigation pane on the left, choose Virtual Private Network > Enterprise - VPN Gateways.
- 5. Locate the row that contains the target VPN gateway, and click **Bind EIP** in the **Operation** column.
 - If the VPN gateway uses the active-active mode, the VPN gateway can have an active EIP and active EIP 2 bound.
 - If the VPN gateway uses the active/standby mode, the VPN gateway can have an active EIP and a standby EIP bound.
- 6. Select the desired EIP and click **OK**.

3.1.1.5 Unbinding an EIP from a VPN Gateway

Scenario

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

Notes and Constraints

An EIP that is in use by a VPN connection cannot be unbound from a VPN gateway.

Procedure

- 1. Log in to the management console.
- 2. Click $^{ extstyle ex$
- 3. Click in the upper left corner, and choose > .
- 4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise VPN Gateways**.
- 5. Locate the row that contains the target VPN gateway, and click **Unbind EIP** or choose **More** > **Unbind EIP** in the **Operation** column.
 - If the VPN gateway uses the active-active mode, the active EIP and active EIP 2 can be unbound from the VPN gateway.
 - If the VPN gateway uses the active/standby mode, the active EIP and standby EIP can be unbound from the VPN gateway.
- 6. Click OK.

3.1.1.6 Deleting a VPN Gateway

Scenario

You can delete a VPN gateway that is no longer required.

Notes and Constraints

- The delete operation is not supported for a VPN gateway that is being created, updated, or deleted.
- If a VPN gateway is bound to an EIP billed in pay-per-use mode, the EIP will be released when the VPN gateway is deleted.
 - To retain such a pay-per-use EIP, unbind it before deleting the VPN gateway. For details about how to unbind an EIP, see 3.1.1.5 Unbinding an EIP from a VPN Gateway.
- If a VPN gateway is bound to an EIP that shares bandwidth with other EIPs, the EIP will be released and the shared bandwidth will be reserved when the VPN gateway is deleted.

Procedure

- 1. Log in to the management console.
- 2. Click in the upper left corner and select the desired region and project.
- 3. Click in the upper left corner, and choose > .
- 4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise VPN Gateways**.
- 5. Locate the row that contains the VPN gateway to be deleted, and choose **More** > **Delete** in the **Operation** column.
- 6. Click OK.
 - ∩ NOTE

The impact of shared bandwidth freezing on EIPs is subject to the EIP documentation.

3.1.1.7 Searching for VPN Gateways by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the management console.

Prerequisites

You have added tags to VPN resources.

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

- 5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.
 - You can only select existing keys and values from the drop-down list.
 - You can select a maximum of 20 tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.
 - You can use tags together with other types of filter criteria. The relationship between them is AND.

3.1.2 Customer Gateway Management of Enterprise Edition VPN

3.1.2.1 Creating a Customer Gateway

Scenario

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

Notes and Constraints

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

Procedure

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

Table 3-4 lists the customer gateway parameters.

Table 3-4 Description of customer gateway parameters

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

Parameter	Description	Example Value
Identifier	IP Address: Specify the IP address of the customer gateway. Ensure that UDP port 4500 is permitted in a firewall rule on the customer gateway in your on-premises data center or private network.	IP Address, 1.2.3.4FQDN, cgw-fqdn
BGP ASN	Enter the ASN of your on-premises data center or private network. The BGP ASN of the customer gateway must be different from that of the VPN gateway.	65000

7. (Optional) If there are two customer gateways, repeat the preceding operations to configure the other customer gateway with a different identifier.

Related Operations

You need to configure an IPsec VPN tunnel on the router or firewall in your onpremises data center.

3.1.2.2 Viewing a Customer Gateway

Scenario

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

Procedure

- 1. Log in to the management console.
- 2. Click \bigcirc in the upper left corner and select the desired region and project.
- 3. Click in the upper left corner, and choose > .
- 4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise Customer Gateways**.
- 5. On the **Customer Gateways** page, view the customer gateway list.
- 6. Click the name of a customer gateway to view its details.
 - In the Basic Information area, you can view the Name, Identifier, ID, BGP ASN, and VPN Connection of the customer gateway.

3.1.2.3 Modifying a Customer Gateway

Scenario

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

Procedure

- 1. Log in to the management console.
- 2. Click \bigcirc in the upper left corner and select the desired region and project.
- 3. Click in the upper left corner, and choose > .
- 4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise Customer Gateways**.
- 5. On the **Customer Gateways** page, click next to the name of a customer gateway.
- Enter a new name for the customer gateway and click OK.
 Table 3-5 describes the parameters related to customer gateway modification.

Table 3-5 Parameters related to customer gateway modification

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

3.1.2.4 Deleting a Customer Gateway

Scenario

You can delete a customer gateway that you have created.

Notes and Constraints

Before deleting a customer gateway associated with a VPN connection, remove the customer gateway from the VPN connection.

- 1. Log in to the management console.
- 2. Click $^{ extstyle ex$
- 3. Click in the upper left corner, and choose > .

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

3.1.2.5 Searching for Customer Gateways by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the management console.

Prerequisites

You have added tags to VPN resources.

Procedure

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

3.1.3 Enterprise Edition VPN Connection Management

3.1.3.1 Creating VPN Connections

Scenario

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

Notes and Constraints

When creating a VPN connection in static routing mode, ensure that the
customer gateway supports ICMP and is correctly configured with the
customer interface IP address of the VPN connection before enabling NQA.
Otherwise, traffic will fail to be forwarded.

Procedure

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

A VPN gateway can establish two VPN connections with a customer gateway using EIPs, improving reliability.

6. Set parameters as prompted and click **Create Now**.

Table 3-6 lists the VPN connection parameters.

Table 3-6 Description of VPN connection parameters

Parameter	Description	Example Value
Name	VPN connection name. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	vpn-001
VPN Gateway	Name of the VPN gateway for which VPN connections are created.	vpngw-001
	You can also click Create VPN Gateway to create a VPN gateway. For details about related parameters, see Table 3-2 .	
VPN Gateway IP of Connection 1	When Network Type is set to Public network , the value is the active EIP of the VPN gateway.	11.xx.xx.11
	When Network Type is set to Private network , the value is the active IP address of the VPN gateway.	
	The same address of a VPN gateway cannot be repeatedly selected when you create VPN connections between the VPN gateway and the same customer gateway.	

Parameter	Description	Example Value
Customer Gateway of Connection 1	Select the customer gateway of connection 1. You can also click Create Customer Gateway to create a customer gateway. For details about related parameters, see Table 3-4 . NOTE If a customer gateway connects to multiple VPN gateways, the BGP ASNs and VPN types of the VPN gateways must be the same.	cgw-001
VPN Gateway IP of Connection 2	 When Network Type is set to Public network and HA Mode is set to Active-active, the value is active EIP 2 of the VPN gateway. When Network Type is set to Private network and HA Mode is set to Active-active, the value is active IP address 2 of the VPN gateway. When Network Type is set to Public network and HA Mode is set to Active/Standby, the value is the standby EIP of the VPN gateway. When Network Type is set to Private network and HA Mode is set to Active/Standby, the value is the standby IP address of the VPN gateway. The VPN gateway IP address must be unique for each connection with a customer gateway. 	11.xx.xx.12
Customer Gateway of Connection 2	Select the customer gateway of connection 2. You can also click Create Customer Gateway to create a customer gateway. For details about related parameters, see Table 3-4 . NOTE If a customer gateway connects to multiple VPN gateways, the BGP ASNs and VPN types of the VPN gateways must be the same.	cgw-001

Parameter	Description	Example Value
VPN Type	IPsec connection mode, which can be route-based or policy-based.	Static routing
	Static routing Determines the data that enters the IPsec VPN tunnel based on the route configuration (local subnet and customer subnet).	
	Application scenario: Communication between customer gateways	
	BGP routing Determines the traffic that can enter the IPsec VPN tunnel based on BGP routes.	
	Application scenario: Communication between customer gateways, many or frequently changing interconnection subnets, or backup between VPN and Direct Connect	
	Policy-based Determines the data that enters the IPsec VPN tunnel based on the policy (between the customer network and VPC). Policy rules can be defined based on the source and destination CIDR blocks.	
	Application scenario: Isolation between customer gateways	
	NOTE By default, the VPN type, customer subnet, branch interconnection setting (BGP routing mode), and policy rules (policy-based mode) of the two connections are the same.	

Parameter	Description	Example Value
Customer Subnet	Customer-side subnet that needs to access the VPC on the cloud through VPN connections.	172.16.1.0/24,172.1 6.2.0/24
	If there are multiple customer subnets, separate them with commas (,).	
	NOTE	
	 The customer subnet can overlap with the local subnet but cannot be the same as the local subnet. 	
	 A customer subnet cannot be included in the existing subnets of the VPC associated with the VPN gateway. It also cannot be the destination address in the route table of the VPC associated with the VPN gateway. 	
	 Customer subnets cannot be the reserved CIDR blocks of VPCs, for example, 100.64.0.0/10 or 214.0.0.0/8. 	
	 If the interconnection subnet is associated with an ACL rule, ensure that the ACL rule permits the TCP port for traffic between all local and customer subnets. 	
	 Address groups cannot be used to configure the source and destination subnets in a policy on customer gateway devices. 	
Branch Interconnectio n	This parameter is available only when VPN Type is set to BGP routing.	Disabled
	Enabled	
	Disabled	
	This function is disabled by default.	
	NOTE When this function is disabled, only local subnet routes are advertised.	

Parameter	Description	Example Value
Policy	This parameter is available only when VPN Type is set to Policy-based .	• Source CIDR block 1: 192.168.1.0/24
	Defines the data flow that enters the encrypted VPN connections between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. By default, a maximum of five policy rules can be configured. • Source CIDR Block The source CIDR block must contain some CIDR blocks of the local subnets. 0.0.0/0 indicates any IP address. A maximum of five source CIDR blocks can be configured for a VPN connection. • Destination CIDR Block The destination CIDR blocks of the customer subnets. A policy rule supports a maximum of 50 destination CIDR blocks, which are separated by commas (,).	 Destination CIDR block 1: 172.16.1.0/24,17 2.16.2.0/24 Source CIDR block 2: 192.168.2.0/24 Destination CIDR block 2: 172.16.1.0/24,17 2.16.2.0/24
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, policies, and advanced settings for connection 1.	Set parameters based on the site requirements.

Parameter	Description	Example Value
Interface IP Address Assignment	This parameter is available only when VPN Type is set to Static routing or BGP routing. NOTE Set interface IP addresses to the tunnel interface IP addresses used by the VPN gateway and customer gateway to communicate with each other. If the tunnel interface address of the customer gateway is fixed, select Manually specify, and set the tunnel interface address of the VPN gateway based on the tunnel interface address of the customer	Automatically assign
	gateway. • Manually specify	
	- Set Local Tunnel Interface Address to the tunnel interface address of the VPN gateway, which can reside only on the CIDR block 169.254.x.x/30 (except 169.254.195.x/30). Then, the system automatically sets Customer Tunnel Interface Address based on the value of Local Tunnel Interface Address. For example, when you set Local Tunnel Interface Address to 169.254.1.6/30, the system automatically sets Customer Tunnel Interface Address to 169.254.1.5/30.	
	 When you set VPN Type to BGP routing and configure tunnel interface addresses in Manually specify mode, ensure that the local and remote tunnel interface addresses configured on the customer gateway device (the other end of the VPN connection) are the same as the values of Customer Tunnel Interface Address and Local Tunnel Interface Address, respectively. Automatically assign 	

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

Parameter	Description	Example Value
Link Detection	This parameter is available only when VPN Type is set to Static routing. NOTE When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, traffic will fail to be forwarded. After this function is enabled, the VPN gateway automatically performs Network Quality Analysis (NQA) on the customer interface IP address of the customer gateway.	Selected
PSK	The PSKs configured for the VPN gateway and customer gateway must be the same. The PSK: Contains 8 to 128 characters. Can contain only three or more types of the following characters: Digits Uppercase letters Lowercase letters Special characters: ~! @ #\$ % ^() + = {}, . /:;	Test@123
Confirm PSK	Enter the PSK again.	Test@123
Policy Settings	 Default: Use default IKE and IPsec policies. Custom: Use custom IKE and IPsec policies. For details about the policies, see Table 3-7 and Table 3-8. NOTE When Local ID and Customer ID are set to IP Address, you can specify specific IP addresses as the local and customer IDs, which must be different. 	Custom
Connection 2's Configuration	Determine whether to enable Same as that of connection 1. • Enabled • Disabled	Enabled

Table 3-7 IKE policy

Parameter	Description	Example Value
Version	Version of the IKE protocol. The value can be one of the following:	v2
	• v1 (v1 has low security. If the device supports v2, v2 is recommended.)	
	• v2	
	The default value is v2 .	
Negotiation Mode	This parameter is available only when Version is v1 .	Main
	Main	
	Aggressive	
Authentication Algorithm	Hash algorithm used for authentication. The following options are available:	SHA2-256
	SHA1(Insecure. Not recommended.)	
	MD5(Insecure. Not recommended.)	
	• SHA2-256	
	• SHA2-384	
	• SHA2-512	
	The default value is SHA2-256 .	
Encryption Algorithm	Encryption algorithm. The following options are available:	AES-128
	3DES(Insecure. Not recommended.)	
	AES-128(Insecure. Not recommended.)	
	AES-192(Insecure. Not recommended.)	
	AES-256(Insecure. Not recommended.)	
	• AES-128-GCM-16	
	AES-256-GCM-16 When this encryption algorithm is used, the IKE version can only be v2.	
	The default value is AES-128 .	

Parameter	Description	Example Value
DH Algorithm	 The following algorithms are supported: Group 1(Insecure. Not recommended.) Group 2(Insecure. Not recommended.) Group 5(Insecure. Not recommended.) Group 14(Insecure. Not recommended.) Group 15 Group 16 Group 19 Group 20 	Group 15
	• Group 21 The default value is Group 15 .	
Lifetime (s)	Lifetime of a security association (SA). An SA will be renegotiated when its lifetime expires. • Unit: second • The value ranges from 60 to 604800. • The default value is 86400.	86400
Local ID	Authentication identifier of the VPN gateway used in IPsec negotiation. The peer ID configured on the customer gateway must be the same as the local ID configured here. Otherwise, IPsec negotiation fails. IP Address (default value) The system automatically sets this parameter to the IP address of the VPN gateway. You can configure a specific IP address as the local ID, which must be different from the customer ID.	IP Address

Parameter	Description	Example Value
Customer ID	Authentication identifier of the customer gateway used in IPsec negotiation. The local ID configured on the customer gateway must be the same as the customer ID configured here. Otherwise, IPsec negotiation fails.	IP Address
	• IP Address (default)	
	 The system automatically sets this parameter to the IP address of the customer gateway. 	
	 You can configure a specific IP address as the customer ID, which must be different from the local ID. 	

Table 3-8 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following options are available:	SHA2-256
	SHA1 (Insecure. Not recommended.)	
	MD5(Insecure. Not recommended.)	
	• SHA2-256	
	• SHA2-384	
	• SHA2-512	
	The default value is SHA2-256 .	

Parameter	Description	Example Value
Encryption Algorithm	Encryption algorithm. The following options are available:	AES-128
	3DES(Insecure. Not recommended.)	
	AES-128(Insecure. Not recommended.)	
	AES-192(Insecure. Not recommended.)	
	AES-256(Insecure. Not recommended.)	
	• AES-128-GCM-16	
	• AES-256-GCM-16	
	The default value is AES-128 .	
PFS	Algorithm used by the Perfect forward secrecy (PFS) function.	DH group 15
	PFS supports the following algorithms:	
	 Disable(Insecure. Not recommended.) 	
	DH group 1(Insecure. Not recommended.)	
	DH group 2(Insecure. Not recommended.)	
	DH group 5(Insecure. Not recommended.)	
	DH group 14(Insecure. Not recommended.)	
	DH group 15	
	DH group 16	
	DH group 19	
	DH group 20	
	DH group 21	
	The default value is DH group 15 .	
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocol is supported: ESP	ESP
	The default value is ESP .	

Parameter	Description	Example Value
Lifetime (s)	Lifetime of an SA.	3600
	An SA will be renegotiated when its lifetime expires.	
	Unit: second	
	• The value ranges from 30 to 604800 .	
	The default value is 3600 .	

□ NOTE

An IKE policy specifies the encryption and authentication algorithms to use in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to use in the data transmission phase of an IPsec tunnel. The policy settings for VPN connections must be the same at the VPC and on-premises data center sides. If they are different, VPN negotiation will fail, causing the failure to establish VPN connections.

The following algorithms are not recommended because they are not secure enough:

- Authentication algorithms: SHA1 and MD5
- Encryption algorithms: 3DES, AES-128, AES-192, and AES-256
 Because some customer devices do not support secure encryption algorithms, the default encryption algorithm of VPN connections is still AES-128. You are advised to use a more secure encryption algorithm if customer devices support secure encryption algorithms.
- DH algorithms: Group 1, Group 2, Group 5, and Group 14
- 7. Confirm the VPN connection configuration and click **Submit**.

3.1.3.2 Configuring Health Check

Scenario

After VPN connections are created, you can configure health check to enable the VPN gateway to send probe packets to the customer gateway to collect statistics about the round-trip time and packet loss rate of physical links. The statistics help you learn about the VPN connection quality. The Cloud Eye service monitors the round-trip time and packet loss rate of VPN links. For details, see Metrics.

- 1. Log in to the management console.
- 2. Click in the upper left corner and select the desired region and project.
- 3. Click in the upper left corner, and choose > .
- 4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise VPN Connections**.
- 5. On the **VPN Connection** page, click the name of the target VPN connection. On the **Summary** tab page, click **Add** in the **Health Check** area.

6. In the Add Health Check dialog box, click OK.

3.1.3.3 Viewing a VPN Connection

Scenario

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

Procedure

- 1. Log in to the management console.
- 2. Click in the upper left corner and select the desired region and project.
- 3. Click in the upper left corner, and choose > .
- 4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise VPN Connections**.
- 5. On the **VPN Connection** page, view the VPN connection list.
- 6. Click the name of a VPN connection to view its basic information, policy configuration, and tags.
 - When VPN Type is Static routing, the basic information includes the VPN connection information and health check information.
 - When VPN Type is BGP routing, the basic information includes the VPN connection information, health check information, and BGP peer information.
 - When VPN Type is Policy-based, the basic information includes the VPN connection information, policy rule information, and health check information.

MOTE

- In the VPN connection list, locate the target VPN connection, and choose More > Modify Policy Settings on the right to view IKE and IPsec policies of the VPN connection.
- In the VPN connection list, you can locate the target VPN connection and click **View Metric** to view monitoring information about the VPN connection.
 - Check the value of **VPN Connection Status**. If the value is **0**, the VPN connection is not connected. If the value is **1**, the VPN connection is connected. If the value is **2**, the VPN connection status is unknown.
 - Check the value of **BGP Peer State**. If the value is **0**, the BGP peer relationship has not been established. If the value is **1**, the BGP peer relationship has been established. If the value is **2**, the BGP peer relationship is in unknown state.
- In the VPN connection list, dual connections to the same customer gateway are
 - identified by \sqsubseteq . If such dual connections are displayed on different pages, \sqcap and \sqsubseteq are also displayed on different pages.
 - The dual-connection identifier will be unavailable if you sort VPN connections by any field in the VPN connection list. The identifier will be restored after you cancel field-based sorting.
- In the VPN connection list, you can locate the target VPN connection and choose More
 View Logs to view IPsec negotiation logs of the VPN connection.
 - If a VPN connection is in **Not connected** state, you can determine the cause of the disconnection based on the VPN connection log details.

3.1.3.4 Modifying a VPN Connection

Scenario

A VPN connection is an encrypted communications channel established between a VPN gateway in a VPC and a customer gateway in your on-premises data center. You can modify a VPN connection when required.

Procedure

- 1. Log in to the management console.
- 2. Click in the upper left corner and select the desired region and project.
- 3. Click in the upper left corner, and choose > .
- In the navigation pane on the left, choose Virtual Private Network > Enterprise - VPN Connections.
- 5. On the **VPN Connection** page, locate the VPN connection to modify, and click **Modify VPN Connection** or **Modify Policy Settings**.
- 6. Modify VPN connection parameters as prompted.
 - For a VPN connection in BGP routing mode, you can enable or disable branch Interconnection on the **Modify VPN Connection** page.
- 7. Click OK.

<u>A</u> CAUTION

If you change the PSK or modify the IKE or IPsec policy of a VPN connection, ensure that the new configurations are consistent with those on the customer gateway. Otherwise, the VPN connection will be interrupted.

Only some of the parameters take effect immediately after being modified, as described in **Table 3-9**.

Table 3-9 Time when new parameter settings take effect

Item	Parame ter	When New Settings Take Effect	How to Modify
-	PSK	 When IKEv1 is used, the new setting takes effect in the next negotiation period. When IKEv2 is used, the new setting takes effect after the VPN connection is re-established. 	 When IKEv1 is used: Locate the VPN connection to modify, choose More > Reset PSK on the right, and change the PSK as prompted. When IKEv2 is used: 1. Delete the current VPN connection. 2. Create a new VPN connection.
IKEv1 policy	Encrypt ion Algorit hm	The new settings take effect in the next negotiation period.	Locate the VPN connection to modify, and click Modify VPN Configuration .
	Authen tication Algorit hm		
	DH Algorit hm		
	Negotia tion Mode		
	Local ID		
	Custom er ID		
	Lifetim e (s)		
	Version	The new settings take effect immediately.	
IKEv2 policy	Encrypt ion Algorit hm	The new settings take effect in the next negotiation period.	Locate the VPN connection to modify, and click Modify VPN Configuration .

Item	Parame ter	When New Settings Take Effect	How to Modify
	Authen tication Algorit hm		
	DH Algorit hm		
	Lifetim e (s)		
	Version	The new settings take effect immediately.	
	Local ID	The new settings take effect after the VPN connection is re-established.	Delete the current VPN connection.
	Custom er ID		2. Create a new VPN connection.
IPsec policy	Encrypt ion Algorit hm	The new settings take effect in the next negotiation period.	Locate the VPN connection to modify, and click Modify VPN Configuration .
	Authen tication Algorit hm		
	PFS		
	Lifetim e (s)		
	Transfer Protoco l	This parameter cannot be modified on the management console.	

Table 3-10 describes the parameters related to VPN connection modification.

Table 3-10 Parameters related to VPN connection modification

Parameter	Description	Modifiable or Not
Name	VPN connection name. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Υ

Parameter	Description	Modifiable or Not
Customer Gateway	Gateway used for communicating with a VPC through VPN.	Υ
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC.	Υ
Policy Settings	There are IKE and IPsec policies.	Υ
PSK	The PSKs configured for the VPN gateway and customer gateway must be the same.	Υ
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	Υ
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	Υ
Branch Interconnection	This parameter is available only when VPN Type is set to BGP routing .	Υ
VPN Gateway	VPN gateway that has been created.	N
Gateway IP Address	IP address used by the customer gateway to communicate with the VPN gateway. The value must be a static address. Ensure that UDP port 4500 is permitted in a firewall rule	N
	on the customer gateway in your on-premises data center or private network.	
Interface IP Address Assignment	Mode in which IP addresses of the local and customer interfaces are assigned. The options include Manually specify and Automatically assign.	N

3.1.3.5 Deleting a VPN Connection

Scenario

If a VPN connection is no longer required, you can delete it to release network resources.

Procedure

- 1. Log in to the management console.
- 2. Click in the upper left corner and select the desired region and project.
- 3. Click \blacksquare in the upper left corner, and choose > .
- In the navigation pane on the left, choose Virtual Private Network > Enterprise - VPN Connections.
- 5. On the **VPN Connection** page, locate the row that contains the target VPN connection, and choose **More** > **Delete**.
- 6. Click OK.

3.1.3.6 Searching for VPN Connections by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the management console.

Prerequisites

You have added tags to VPN resources.

Procedure

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

3.2 Classic S2C VPN

3.2.1 Classic VPN Gateway Management

3.2.1.1 Viewing a VPN Gateway

Scenarios

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

Procedure

- 1. Log in to the management console.
- 2. Click $^{ extstyle ex$
- 3. Click Service List and choose Networking > Virtual Private Network.
- 4. On the console homepage, under **Network**, click **Virtual Private Cloud**.
- In the navigation pane on the left, choose Virtual Private Network.
 If Enterprise Edition VPN is available for the selected region, choose Virtual Private Network > Classic.
- 6. View VPN gateway information.

3.2.1.2 Modifying a VPN Gateway

- 1. Log in to the management console.
- 2. Click \bigcirc in the upper left corner and select the desired region and project.
- 3. Click **Service List** and choose **Networking** > **Virtual Private Network**.
- 4. On the console homepage, under **Network**, click **Virtual Private Cloud**.
- In the navigation pane on the left, choose Virtual Private Network.
 If Enterprise Edition VPN is available for the selected region, choose Virtual Private Network > Classic.
- 6. On the **VPN Gateways** page, locate the row that contains the target VPN gateway and click **Modify** in the **Operation** column.
- 7. On the Classic page, click the **VPN Gateways** tab.
 - Locate the row that contains the target VPN gateway, and choose More >
 Modify Bandwidth in the Operation column.
 - Locate the row that contains the target VPN gateway, and choose More >
 Modify Basic Information in the Operation column.
 - Locate the row that contains the target VPN gateway, and choose More > Modify Specifications in the Operation column.
- 8. Modify the VPN gateway bandwidth, name, or description as required.
- 9. Modify the VPN gateway name or description as required.

10. Click **OK**.

3.2.1.3 Deleting a VPN Gateway

Scenarios

If a VPN gateway is no longer required, you can delete it to release network resources as long as it has no VPN connections configured.

If it has any connections configured, delete the connections first.

Procedure

- 1. Log in to the management console.
- In the navigation pane on the left, choose Virtual Private Network > Classic VPN Gateways.

If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.

- 3. Locate the row that contains the target VPN gateway, and choose **More** > **Delete** in the **Operation** column.
 - If Enterprise Edition VPN is available for the selected region, locate the row that contains the target VPN gateway, and choose **More** > **Delete**.
- 4. In the displayed dialog box, click **Yes**.

3.2.2 Classic VPN Connection Management

3.2.2.1 Viewing a VPN Connection

Scenarios

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

Procedure

- 1. Log in to the management console.
- 2. Click \bigcirc in the upper left corner and select the desired region and project.
- 3. Click **Service List** in the upper left corner, and choose > **Virtual Private Network**.
- 4. On the console homepage, under **Network**, click **Virtual Private Cloud**.
- In the navigation pane on the left, choose Virtual Private Network > Classic
 VPN Connections.

If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**. Then, click the **VPN Connections** tab.

6. View the VPN connection information. You can also locate the row that contains the target VPN connection, and click **View Policy** in the **Operation** column to view IKE and IPsec policy details of the VPN connection.

3.2.2.2 Modifying a VPN Connection

Scenarios

A VPN connection is an encrypted communications channel established between the VPN gateway in your VPC and that in an on-premises data center. The VPN connection can be modified after creation.

↑ CAUTION

If you modify the advanced settings, network communications may be interrupted. Exercise caution when performing this operation.

Changing the PSK only will not delete the current VPN connection. The new PSK takes effect during IKE renegotiation after the IKE lifetime expires.

Procedure

- 1. Log in to the management console.
- 2. Click \bigcirc in the upper left corner and select the desired region and project.
- 3. Click Service List and choose Networking > Virtual Private Network.
- 4. On the console homepage, under **Network**, click **Virtual Private Cloud**.
- In the navigation pane on the left, choose Virtual Private Network > Classic
 VPN Connections.

If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**. Then, click the **VPN Connections** tab.

- 6. Locate the row that contains the target VPN connection, and click **Modify** in the **Operation** column.
- 7. In the displayed **Modify VPN Connection** dialog box, modify parameters as required.

□ NOTE

The name of a VPN gateway can contain only letters, digits, underscores (_), hyphens (-), and periods (.).

8. Click **OK**.

3.2.2.3 Deleting a VPN Connection

Scenarios

If a VPN connection is no longer required, you can delete it to release network resources.

Procedure

- 1. Log in to the management console.
- 2. Click $^{\bigcirc}$ in the upper left corner and select the desired region and project.

- 3. Click Service List and choose Networking > Virtual Private Network.
- 4. On the console homepage, under **Network**, click **Virtual Private Cloud**.
- In the navigation pane on the left, choose Virtual Private Network > Classic
 VPN Connections.
 - If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**. Then, click the **VPN Connections** tab.
- 6. Locate the row that contains the target VPN connection, and choose **More** > **Delete** in the **Operation** column.
- 7. In the displayed dialog box, click Yes.

3.3 Monitoring

3.3.1 Metrics (S2C Enterprise Edition VPN)

Description

This section describes monitored metrics reported by VPN to Cloud Eye as well as their namespaces and dimensions. You can use the Cloud Eye management console to query the metrics of the monitored objects and alarms generated for VPN.

Namespace

SYS.VPN

Metrics

Table 3-11 Metrics supported for Enterprise Edition VPN gateways

Metric ID	Metr ic Nam e	Description	Val ue Ran ge	Uni t	Con vers ion Rul e	Moni tore d Obje ct (Dim ensi on)	Monitor ing Interval (Raw Data)
gateway_se nd_pkt_rat e	Outb ound Packe t Rate	Average number of data packets leaving the cloud per second.	≥ 0	pps	N/A	Gate way	1 minute
gateway_re cv_pkt_rate	Inbou nd Packe t Rate	Average number of data packets entering the cloud per second.	≥ 0	pps	N/A	Gate way	1 minute

Metric ID	Metr ic Nam e	Description	Val ue Ran ge	Uni t	Con vers ion Rul e	Moni tore d Obje ct (Dim ensi on)	Monitor ing Interval (Raw Data)
gateway_se nd_rate	Outb ound Band width	Average volume of traffic leaving the cloud per second.	0-1	bps	102 4(IE C)	Gate way	1 minute
gateway_re cv_rate	Inbou nd Band width	Average volume of traffic entering the cloud per second.	0-1	bps	102 4(IE C)	Gate way	1 minute
gateway_se nd_rate_us age	Outb ound Band width Usag e	Bandwidth utilization for traffic leaving the cloud.	0-1 00	per cen tag e(%)	N/A	Gate way	1 minute
gateway_re cv_rate_usa ge	Inbou nd Band width Usag e	Bandwidth utilization for traffic entering the cloud.	0-1 00	per cen tag e(%)	N/A	Gate way	1 minute
gateway_c onnection_ num	Num ber of Conn ectio ns	Number of VPN connections.	≥ 0	cou nt	N/A	Gate way	1 minute

Table 3-12 Enterprise Edition VPN connection metrics

Metric ID	Metric Name	Description	Valu e Ran ge	Uni t	Con ver sio n Rul e	Moni tored Obje ct (Dim ensio n)	Monito ring Interva I (Raw Data)
tunnel_av erage_late ncy	Average Tunnel RTT	Average round-trip time on the tunnel between the VPN gateway and customer gateway.	0~5 000	ms	N/A	VPN conn ectio n	15s
tunnel_m ax_latency	Maximu m Tunnel RTT	Maximum round- trip time on the tunnel between the VPN gateway and customer gateway.	0~5 000	ms	N/A	VPN conn ectio n	15s
tunnel_pa cket_loss_ rate	Tunnel Packet Loss Rate	Packet loss rate on the tunnel between the VPN gateway and customer gateway.	0~1 00	per cen tag e(%)	N/A	VPN conn ectio n	15s
link_avera ge_latenc y	Average Link RTT	Average round-trip time on the physical link between the VPN gateway and customer gateway.	0~5 000	ms	N/A	VPN conn ectio n	15s
link_max_l atency	Maximu m Link RTT	Maximum round- trip time on the physical link between the VPN gateway and customer gateway.	0~5 000	ms	N/A	VPN conn ectio n	15s
link_packe t_loss_rate	Link Packet Loss Rate	Packet loss rate on the physical link between the VPN gateway and customer gateway.	0~1 00	per cen tag e(%)	N/A	VPN conn ectio n	15s
connectio n_status	VPN Connect ion Status	Status of a VPN connection: 0: not connected 1: connected 2: unknown	0, 1, or 2	N/A	N/A	VPN conn ectio n	1 minute

Metric ID	Metric Name	Description	Valu e Ran ge	Uni t	Con ver sio n Rul e	Moni tored Obje ct (Dim ensio n)	Monito ring Interva l (Raw Data)
recv_pkt_r ate	Packet Receive Rate	Average number of data packets received per second.	≥ 0	pps	N/A	VPN conn ectio n	1 minute
send_pkt_ rate	Packet Send Rate	Average number of data packets sent per second.	≥ 0	pps	N/A	VPN conn ectio n	1 minute
recv_rate	Traffic Receive Rate	Average volume of traffic received per second.	0-1	bps	102 4(IE C)	VPN conn ectio n	1 minute
send_rate	Traffic Send Rate	Average volume of traffic sent per second.	0-1	bps	102 4(IE C)	VPN conn ectio n	1 minute
sa_send_p kt_rate	SA Packet Send Rate	Average number of data packets sent over an SA per second.	≥ 0	pps	N/A	SA of a VPN conn ectio n	1 minute
sa_recv_p kt_rate	SA Packet Receive Rate	Average number of data packets received over an SA per second.	≥ 0	pps	N/A	SA of a VPN conn ectio n	1 minute
sa_recv_ra te	SA Traffic Receive Rate	Average volume of traffic received over an SA per second.	0-1	bps	102 4(IE C)	SA of a VPN conn ectio n	1 minute
sa_send_r ate	SA Traffic Send Rate	Average volume of traffic sent over an SA per second.	0-1	bps	102 4(IE C)	SA of a VPN conn ectio n	1 minute

Dimensions

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

3.3.2 Metrics (S2C Classic VPN)

Description

This section describes monitored metrics reported by VPN to Cloud Eye as well as their namespaces and dimensions. You can use the Cloud Eye management console to query the metrics of the monitored objects and alarms generated for VPN.

Namespace

SYS.VPC

Metrics

Table 3-13 Metrics supported for Classic VPN connections

Metric ID	Metric Name	Description	Value Range	Uni t	Co nve rsio n Rul e	Monit ored Object (Dime nsion)	Monitor ing Interval (Raw Data)
conne ction_s tatus	VPN Conne ction Status	Status of a VPN connection: 0: not connected 1: connected	0 or 1	N/A	N/ A	VPN connec tion	5 minutes

Dimensions

key	Value
vpn_connection_id	S2C Classic VPN connection

3.3.3 Viewing Metrics

Scenarios

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

Support for Metrics

Table 3-14 Support for metrics

Metric Name	Support	Enabled by Default?
VPN Connection Status	Supported by both Enterprise Edition VPN and Classic VPN	Yes
 Average Link RTT Maximum Link RTT Link Packet Loss Rate Packet Receive Rate Packet Send Rate Traffic Receive Rate Traffic Send Rate SA Packet Receive Rate SA Packet Send Rate SA Traffic Receive Rate SA Traffic Receive Rate SA Traffic Receive Rate SA Traffic Send Rate 	Supported only by Enterprise Edition VPN	No You can click the name of a VPN connection and add a health check item on the Summary tab page.
 Average Tunnel RTT Maximum Tunnel RTT Tunnel Packet Loss Rate 	Supported only by Enterprise Edition VPN	Yes Private network monitoring metrics are supported only when a VPN connection uses the static routing mode and has NQA enabled.

Viewing VPN Gateway Metrics

- Viewing metrics on the VPN console
 - a. Log in to the management console.
 - b. Click on in the upper left corner and select the desired region and project.
 - c. Click in the upper left corner of the management console, and choose **Networking > Virtual Private Network**.
 - d. Choose Virtual Private Network > Enterprise VPN Gateways.
 - e. Locate the target VPN connection, and click the icon in the **Gateway** IP Address column.

You can view data of the last 1, 3, 12, or 24 hours, or a customized time range.

- Viewing metrics on the Cloud Eye console
 - a. Log in to the management console.
 - b. Click $^{\bigcirc}$ in the upper left corner and select the desired region and project.
 - c. Click Service List and choose Management & Governance > Cloud Eye.
 - d. Choose Cloud Service Monitoring > Virtual Private Network.
 - e. Click **View Metric** in the **Operation** column of the target VPN gateway to view its status.

You can view data of the last 1, 3, 12, or 24 hours, or last 7 days.

Viewing VPN Connection Metrics

- Viewing metrics on the VPN console
 - a. Log in to the management console.
 - b. Click \bigcirc in the upper left corner and select the desired region and project.
 - c. Click in the upper left corner of the management console, and choose **Networking > Virtual Private Network**.
 - d. View metrics.
 - S2C Enterprise Edition VPN: Choose Virtual Private Network >

Enterprise – VPN Connections, and click View Metric under the name of a VPN connection.

The metrics include the following:

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

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

- Viewing metrics on the Cloud Eye console
 - a. Log in to the management console.
 - b. Click in the upper left corner and select the desired region and project.
 - c. Click **Service List** and choose **Management & Governance** > **Cloud Eye**.
 - d. Choose Cloud Service Monitoring > Virtual Private Network.
 - e. View metrics.
 - Enterprise Edition VPN: On the S2C VPN Connection page, locate the target VPN connection, and click View Metric in the Operation column to view the VPN connection status.
 - Classic VPN: Click the VPN Connections tab, locate the target VPN connection, and click View Metric in the Operation column to view the VPN connection status.

You can view data of the last 1, 3, 12, or 24 hours, or last 7 days.

3.3.4 Creating a Monitoring Alarm Rule

Scenarios

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

Procedure

- 1. Log in to the management console.
- 2. Click \bigcirc in the upper left corner and select the desired region and project.
- 3. Click in the upper left corner of the management console, and choose Management & Governance > Cloud Eye.
- 4. Choose Cloud Service Monitoring > Virtual Private Network VPN, click Create Alarm Rule, and configure alarm rules for different types of alarms as required.
 - Alarms related to VPN gateways in S2C Enterprise Edition VPN: Click the S2C VPN Gateway tab, and click Create Alarm Rule in the Operation column of a VPN gateway.
 - Alarms related to VPN connections in S2C Enterprise Edition VPN: Click the S2C VPN Connection tab, and click Create Alarm Rule in the Operation column of a VPN connection.
- 5. Click **Create**.

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

◯ NOTE

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

3.4 Audit

3.4.1 Key Operations That Can Be Recorded by CTS

Table 3-15 Operations related to S2C Enterprise Edition VPN that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a customer gateway	customer- gateway	createCgw
Updating a customer gateway	customer- gateway	updateCgw
Deleting a customer gateway	customer- gateway	deleteCgw
Creating a VPN gateway	vpn-gateway	createVgw
Updating a VPN gateway	vpn-gateway	updateVgw
Deleting a VPN gateway	vpn-gateway	deleteVgw
Updating the VPN gateway status	vpn-gateway	updateResourceState
Updating the specification of a pay-per-use VPN gateway	vpn-gateway	updatePostpaidVgwSpecification
Creating a VPN connection	vpn-connection	createVpnConnection
Updating a VPN connection	vpn-connection	updateVpnConnection
Deleting a VPN connection	vpn-connection	deleteVpnConnection
Creating a resource tag	instance	batchCreateResourceTags
Deleting a resource tag	instance	batchDeleteResourceTags
Querying the customer gateway list	customer- gateway	listCgws

Operation	Resource Type	Trace Name
Querying a customer gateway	customer- gateway	showCgw
Querying resource tags	instance	showResourceTags
Querying project tags	instance	listProjectTags
Querying resource instances by tag	instance	listResourcesByTags
Querying the number of resource instances by tag	instance	countResourcesByTags
Querying a VPN gateway	vpn-gateway	showVgw
Querying the route table of a specified VPN gateway	vpn-gateway	showVpnGatewayRoutingTable
Querying the VPN connection list	vpn-connection	listVpnConnections
Querying a VPN connection	vpn-connection	showVpnConnection
Querying the VPN gateway list	vpn-connection	listVgws
Querying a VPN connection monitor	vpn-connection	showConnectionMonitor
Querying the VPN connection monitor list	vpn-connection	listConnectionMonitors
Querying quotas of a specified tenant	quota	showQuotasInfo
Querying VPN connection logs	vpn-connection	queryVpnConnectionLog
Creating VPN connections in batches	vpn-connection	batchCreateVpnConnection

3.5 Permissions Management

3.5.1 Creating a User and Granting VPN Permissions

Use the Identity and Access Management (IAM) service to implement fine-grained permissions control over your VPN resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing VPN resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Grant the permission to perform professional and efficient O&M on your VPN resources to other accounts or cloud services.

If your account meets your permissions requirements, you can skip this section.

This section describes the procedure for granting permissions (see Figure 3-1).

Prerequisites

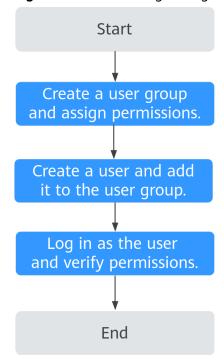
You have learned about the permissions supported by VPN, and determined the permissions to be granted to a user group. Before granting permissions of other services, learn about all permissions supported by IAM.

■ NOTE

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

Process Flow

Figure 3-1 Process of granting VPN permissions



- Create a user group and assign permissions to it.
 Create a user group on the IAM console and attach the VPN FullAccess policy to the group.
- Create a user and add it to the user group.
 Create a user on the IAM console and add the user to the group created in 1.
- Log in and verify permissions.
 Log in to the management console as the created user. Switch to the authorized region and verify the permissions.
 - Click Service List and choose Networking > Virtual Private Network.
 On the Enterprise VPN Gateways page, click Buy S2C VPN Gateway to create a VPN gateway. If the VPN gateway is successfully created, the VPN FullAccess policy has already taken effect.
 - Click Service List and choose Networking > Virtual Private Network >
 Classic. Click Create VPN Gateway to create a VPN gateway. If the VPN
 gateway is successfully created, the VPN FullAccess policy has already
 taken effect.
 - Select any service except the VPN service in Service List. Assume that the current policy contains only VPN FullAccess. If a message appears indicating that you have insufficient permissions to access the service, the VPN FullAccess policy has already taken effect.

3.5.2 VPN Custom Policies

Custom policies can be created to supplement the system-defined policies of VPN. You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see "Creating a Custom Policy" in the *Identity and Access Management User Guide*. The following section contains examples of common VPN custom policies.

Example VPN custom policy

Example 1: Grant permission to delete VPN gateways.

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

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

• Example 2: Deny VPN connection deletion.

]

A policy with only "Deny" permissions must be used together with other policies. If the permissions granted to an IAM user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the **VPN FullAccess** policy to a user but also forbid the user from deleting VPN connections. Create a custom policy for denying VPN connection deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on VPN except deleting VPN connections. The following is an example of a deny policy:

```
{
"Version": "1.1",
```

```
"Statement": [
{
    "Effect": "Deny",
    "Action": [
    "vpn:vpnGateways:delete"
    ]
    }
]
```

• Example 3: defining multiple actions in a policy

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

```
"Version": "1.1",
  "Statement": [
     {
        "Effect": "Allow",
        "Action": [
           "vpn:vpnGateways:create",
           "vpn:vpnConnections:create",
           "vpn:customerGateways:create"
     },
        "Effect": "Deny",
        "Action": [
           "vpn:vpnGateways:delete",
           "vpn:vpnConnections:delete",
           "vpn:customerGateways:create"
       ]
     },
        "Effect": "Allow",
        "Action": [
           "vpc:vpcs:list",
           "vpc:subnets:get"
       ]
     }
  ]
}
```

4 Best Practice

4.1 Enterprise Edition S2C VPN

4.1.1 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active-Active Mode)

4.1.1.1 Overview

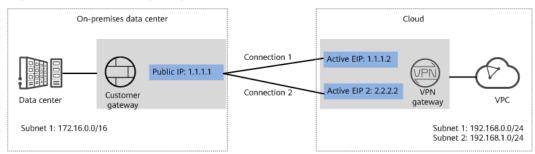
Scenario

VPN can be used to enable communication between an on-premises data center and ECSs in a VPC.

Networking

In this example, a group of VPN connections are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

Figure 4-1 Networking diagram



Solution Advantages

- 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 VPN gateways can be deployed in different AZs to ensure AZ-level high availability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same.
 That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

4.1.1.2 Planning Networks and Resources

Data Plan

Table 4-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	192.168.0.0/24192.168.1.0/24
VPN gateway	Interconnecti on subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	HA mode	Active-active
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2

Category	Item	Data
VPN connectio n	Tunnel interface addresses under Connection 1's Configuratio n	IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under Connection 2's Configuration	 Local tunnel interface address: 169.254.71.1/30 Customer tunnel interface address: 169.254.71.2/30
On- premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is as follows: 1.1.1.1
IKE and	PSK	Test@123
IPsec policies	IKE policy	 Version: v2 Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 DH algorithm: Group 15 Lifetime (s): 86400 Local ID: IP address Peer ID: IP address
	IPsec policy	 Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 PFS: DH Group15 Transfer protocol: ESP Lifetime (s): 3600

4.1.1.3 Procedure

Prerequisites

- Cloud side
 - A VPC has been created. For details about how to create a VPC, see the Virtual Private Cloud User Guide.
 - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.
- Data center side
 - IPsec has been configured on the VPN device in the on-premises data center

Procedure

VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

- **Step 1** Log in to the management console.
- **Step 2** Click **Service List** and choose **Networking** > **Virtual Private Network**.
- **Step 3** Configure a VPN gateway.
 - Choose Virtual Private Network > Enterprise VPN Gateways, and click Buy S2C VPN Gateway.
 - 2. Set parameters as prompted.

Table 4-2 only describes the key parameters for creating a VPN gateway.

Table 4-2 Description of VPN gateway parameters

Paramete r	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select Public network .	Public network
Associate With	Select VPC .	VPC
VPC	VPC to which the interconnection subnet belongs.	vpc-001(192.168.0. 0/16)
Interconn ection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24

Paramete r	Description	Value
Local Subnet	This parameter is available only when Associate With is set to VPC .	192.168.0.0/24,192. 168.1.0/24
	 Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. 	
	 Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center. 	
BGP ASN	BGP AS number.	64512
HA Mode	Select Active-active .	Active-active
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure the customer gateway.

- 1. Choose Virtual Private Network > Enterprise Customer Gateways, and click Create Customer Gateway.
- 2. Set parameters as prompted.

Table 4-3 only describes the key parameters for creating a customer gateway.

Table 4-3 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Identifier	IP address used by the customer gateway to communicate with the VPN gateway.	1.1.1.1
	Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	

Step 5 Configure VPN connections.

- Choose Virtual Private Network > Enterprise VPN Connections, and click Create VPN Connection.
- Set VPN connection parameters and click **Buy Now**.
 Table 4-4 describes the key parameters for creating VPN connections.

Table 4-4 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select Static routing .	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC. - A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. - Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	Set parameters based on the site requirements.
Interface IP Address Assignment	 Manually specify In this example, select Manually specify. Automatically assign 	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.70.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.71.1/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	NQA enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default
Connection 2's Configuration	Determine whether to enable Same as that of connection 1. NOTE If you disable Same as that of connection 1, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.70.2/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device.

----End

Verification

- About 5 minutes later, check states of the VPN connections.
 Choose Virtual Private Network > Enterprise VPN Connections. The states of the two VPN connections are both Normal.
- Verify that servers in the on-premises data center and ECSs in the VPC subnet can ping each other.

4.1.2 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active/Standby Mode)

4.1.2.1 Overview

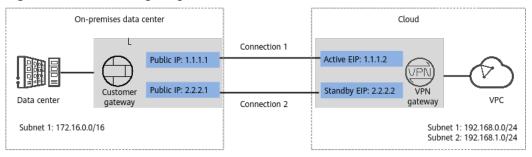
Scenario

VPN can be used to enable communication between an on-premises data center and ECSs in a VPC.

Networking

In this example, two VPN connections working in active/standby mode are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

Figure 4-2 Networking diagram



Solution Advantages

- 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/Standby mode: 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 original active VPN connection. Traffic leaving the cloud is preferentially transmitted through the active EIP, allowing you to determine the VPN connection through which traffic is transmitted.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same.
 That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.

• The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

4.1.2.2 Planning Networks and Resources

Data Plan

Table 4-5 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	192.168.0.0/24192.168.1.0/24
VPN gateway	Interconnecti on subnet VPN gateway and VPC. Ensure that the sele interconnection subnet has four or more as: IP addresses. 192.168.2.0/24	
	HA mode	Active/Standby
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Standby EIP: 2.2.2.2
VPN Tunnel interface addresses under Connection 1's Configuration		IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.70.1/30 • Customer tunnel interface address: 169.254.70.2/30
	Tunnel interface addresses under Connection 2's Configuration	 Local tunnel interface address: 169.254.71.1/30 Customer tunnel interface address: 169.254.71.2/30

Category	Item	Data
On- premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP addresses are as follows: • 1.1.1.1 • 2.2.2.1
IKE and	PSK	Test@123
IPsec policies	IKE policy	 Version: v2 Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 DH algorithm: Group 15 Lifetime (s): 86400 Local ID: IP address Peer ID: IP address
	IPsec policy	 Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 PFS: DH Group15 Transfer protocol: ESP Lifetime (s): 3600

4.1.2.3 Procedure

Prerequisites

- Cloud side
 - A VPC has been created. For details about how to create a VPC, see the Virtual Private Cloud User Guide.
 - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.
- Data center side
 - IPsec has been configured on the VPN device in the on-premises data center.

Procedure

VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

- **Step 1** Log in to the management console.
- **Step 2** Click **Service List** and choose **Networking** > **Virtual Private Network**.
- **Step 3** Configure a VPN gateway.
 - Choose Virtual Private Network > Enterprise VPN Gateways, and click Buy S2C VPN Gateway.
 - 2. Set parameters as prompted.

Table 4-6 only describes the key parameters for creating a VPN gateway.

Table 4-6 Description of VPN gateway parameters

Paramete r	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select Public network .	Public network
Associate With	Select VPC .	VPC
VPC	VPC to which the interconnection subnet belongs.	vpc-001(192.168.0. 0/16)
Interconn ection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	This parameter is available only when Associate With is set to VPC. - Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. - Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192. 168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select Active/Standby .	Active/Standby
Active EIP	Active EIP used by the VPN gateway to access the on-premises data center.	1.1.1.2
Standby EIP	Standby EIP used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure the customer gateway.

- 1. Choose Virtual Private Network > Enterprise Customer Gateways, and click Create Customer Gateway.
- 2. Set parameters as prompted.

Table 4-7 only describes the key parameters for creating a customer gateway.

Table 4-7 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Identifier	IP address used by the customer gateway to communicate with the VPN gateway.	1.1.1.1
	Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	

Step 5 Configure VPN connections.

- 1. Choose Virtual Private Network > Enterprise VPN Connections, and click Create VPN Connection.
- Set VPN connection parameters and click **Buy Now**.
 Table 4-8 only describes the key parameters for creating VPN connections.

Table 4-8 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Standby EIP of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	2.2.2.1
VPN Type	Select Static routing .	Static routing

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC.	172.16.0.0/16
	 A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. 	
	 Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets. 	
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	Set parameters based on the site requirements.
Interface IP Address Assignment	 Manually specify In this example, select Manually specify. Automatically assign 	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	NQA enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

Parameter	Description	Value
Connection 2's Configuration	Determine whether to enable Same as that of connection 1. NOTE If you disable Same as that of connection 1, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device.

----End

Verification

- About 5 minutes later, check states of the VPN connections.
 Choose Virtual Private Network > Enterprise VPN Connections. The states of the two VPN connections are both Available.
- Verify that servers in the on-premises data center and ECSs in the VPC subnet can ping each other.

4.1.3 Connecting Multiple On-premises Branch Networks Through a VPN Hub

4.1.3.1 Overview

Scenario

To meet service requirements, enterprise A needs to implement communication between its two on-premises data centers.

Networking

Figure 4-3 shows the networking where the VPN service is used to connect the two on-premises data centers.

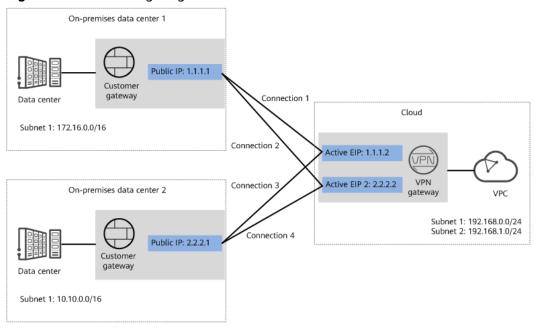


Figure 4-3 Networking diagram

Solution Advantages

- A VPN gateway on the cloud can function as a VPN hub to enable communication between on-premises branch sites. This eliminates the need to configure VPN connections between every two sites.
- A VPN gateway provides two IP addresses to establish dual independent VPN connections with each customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection, ensuring reliability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same.
 That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

4.1.3.2 Planning Networks and Resources

Data Plan

Table 4-9 Data plan

Category	Item	Data	
VPC	Subnet that needs to access the on-premises data centers	192.168.0.0/24192.168.1.0/24	
VPN Interconne on subnet		This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24	
	HA Mode	Active-active	
	EIPs are automatically generated when you them. By default, a VPN gateway uses two this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2		
On- premises data center 1	Subnet that needs to access the VPC	172.16.0.0/16	
Customer gateway in on- premises data center 1	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is as follows: 1.1.1.1	
VPN connectio ns of on- premises data center 1	Tunnel interface addresses under Connection 1's Configuration	 IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. Local tunnel interface address: 169.254.70.1/30 Customer tunnel interface address: 169.254.70.2/30 	

Category	Item	Data	
	Tunnel interface addresses under Connection 2's Configuratio n	 Local tunnel interface address: 169.254.71.1/30 Customer tunnel interface address: 169.254.71.2/30 	
On- premises data center 2	Subnet that needs to access the VPC	10.10.0.0/16	
Customer gateway in on- premises data center 2	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is as follows: 2.2.2.1	
VPN connectio ns of on- premises data center 2	Tunnel interface addresses under Connection 1's Configuratio n	IP addresses used to establish an IPsec tunnel between a VPN gateway and a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • Local tunnel interface address: 169.254.72.1/30 • Customer tunnel interface address: 169.254.72.2/30	
	Tunnel interface addresses under Connection 2's Configuration	 Local tunnel interface address: 169.254.73.1/30 Customer tunnel interface address: 169.254.73.2/30 	
IKE and	PSK	Test@123	
IPsec policies	IKE policy	 Authentication algorithm: SHA2-256 Encryption algorithm: AES-128 DH algorithm: Group 15 Version: v2 Lifetime (s): 86400 Local ID: IP address Peer ID: IP address 	

Category	Item	Data	
	IPsec policy	Authentication algorithm: SHA2-256	
		Encryption algorithm: AES-128	
		PFS: DH Group15	
		Transfer protocol: ESP	
		• Lifetime (s): 3600	

4.1.3.3 Procedure

Prerequisites

- Cloud side
 - A VPC has been created. For details about how to create a VPC, see the Virtual Private Cloud User Guide.
 - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.
- Data center side
 - IPsec has been configured on the VPN devices in the two on-premises data centers.
 - The remote subnets of the VPN device in on-premises data center 1 must contain the local subnet of the VPC and the subnet to be interconnected in on-premises data center 2. The remote subnets of the VPN device in on-premises data center 2 must contain the local subnet of the VPC and the subnet to be interconnected in on-premises data center 1.

Procedure

VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Configure a VPN gateway.

- Choose Virtual Private Network > Enterprise VPN Gateways, and click Buy S2C VPN Gateway.
- 2. Set parameters as prompted.

Table 4-10 only describes the key parameters for creating a VPN gateway.

Table 4-10 Description of VPN gateway parameters

Paramete r	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select Public network .	Public network

Paramete r	Description	Value
Associate With	Select VPC .	VPC
VPC	VPC that the on-premises data centers need to access.	vpc-001(192.168.0. 0/16)
Local Subnet	VPC subnets that the on-premises data centers need to access.	192.168.0.0/24,192. 168.1.0/24
Interconn ection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select Active-active .	Active-active
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 2 Configure customer gateways.

- 1. Choose Virtual Private Network > Enterprise Customer Gateways, and click Create Customer Gateway.
- 2. Set parameters as prompted.

Table 4-11 only describes the key parameters for creating a customer gateway.

Table 4-11 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw1
Identifier	IP address used by the customer gateway in on-premises data center 1 to communicate with the VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

3. Repeat the preceding operations to configure the customer gateway (2.2.2.1) in on-premises data center 2.

Step 3 Configure VPN connections between the cloud side and on-premises data center 1.

- Choose Virtual Private Network > Enterprise VPN Connections, and click Create VPN Connection.
- 2. Set VPN connection parameters and click **Buy Now**.

Table 4-12 only describes the key parameters for creating VPN connections.

Table 4-12 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-001
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	1.1.1.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	1.1.1.1
VPN Type	Select Static routing .	Static routing
Customer Subnet	Subnet in on-premises data center 1 that needs to access the VPC. - A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. - Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	Set parameters based on the site requirements.

Parameter	Description	Value
Interface IP Address Assignment	 Manually specify In this example, select Manually specify. Automatically assign 	Manually specify
Local Tunnel	Tunnel interface IP address of the	160 254 70 1/20
Interface Address	VPN gateway.	169.254.70.1/30
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.70.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	NQA enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default
Connection 2's Configuration	Determine whether to enable Same as that of connection 1. NOTE If you disable Same as that of connection 1, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2/30

Step 4 Configure VPN connections between the cloud side and on-premises data center 2.

- Choose Virtual Private Network > Enterprise VPN Connections, and click Create VPN Connection.
- Set VPN connection parameters and click **Buy Now**.
 Table 4-13 only describes the key parameters for creating VPN connections.

Table 4-13 Description of VPN connection parameters

Parameter	Description	Value
Name	VPN connection name.	vpn-002
VPN Gateway	VPN gateway for which VPN connections are created.	vpngw-001
VPN Gateway IP of Connection 1	Active EIP of the VPN gateway.	1.1.1.2
Customer Gateway of Connection 1	Customer gateway of connection 1.	2.2.2.1
VPN Gateway IP of Connection 2	Active EIP 2 of the VPN gateway.	2.2.2.2
Customer Gateway of Connection 2	Customer gateway of connection 2.	2.2.2.1
VPN Type	Select Static routing .	Static routing
Customer Subnet	 Subnet in on-premises data center 2 that needs to access the VPC. A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets. 	10.10.0.0/16
Connection 1's Configuration	Configure the IP address assignment mode of tunnel interfaces, local tunnel interface address, customer tunnel interface address, link detection, PSK, confirm PSK, and policies for connection 1.	Set parameters based on the site requirements.
Interface IP Address Assignment	 Manually specify In this example, select Manually specify. Automatically assign 	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address of the VPN gateway.	169.254.72.1/30

Parameter	Description	Value
Customer Tunnel Interface Address	Tunnel interface IP address of the customer gateway device.	169.254.72.2/30
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	NQA enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device in onpremises data center 2.	Test@123
Policy Settings	The policy settings must be the same as those configured on the customer gateway device in onpremises data center 2.	Default
Connection 2's Configuration	Determine whether to enable Same as that of connection 1. NOTE If you disable Same as that of connection 1, you are advised to use the same settings as connection 1 for connection 2, except the local and customer tunnel interface addresses.	Disabled
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.73.1/30
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.73.2/30

Step 5 Configure customer gateway devices in on-premises data centers 1 and 2.

The configuration procedures may vary according to the type of the customer gateway device.

----End

Verification

About 5 minutes later, check states of the VPN connections.
 Choose Virtual Private Network > Enterprise - VPN Connections. The states of the four VPN connections are all Normal.

• Verify that servers in on-premises data center 1 and servers in on-premises data center 2 can ping each other.

4.2 Classic S2C VPN

4.2.1 Connecting an On-Premises Data Center to a VPC Through a VPN

Scenarios

By default, ECSs in a VPC cannot communicate with devices in your on-premises data center or private network. To enable communication between them, you can configure VPN. After that, you need to configure security group rules and check subnet connectivity to ensure that the VPN is available. VPNs can be classified into the following two types:

- A site-to-site VPN functions as a communication tunnel between a VPC and a single on-premises data center.
- By contrast, a hub-and-spoke VPN is between a VPC and multiple onpremises data centers.

Pay attention to the following when you configure a VPN:

- The local and remote subnets cannot conflict.
- The IKE policies, IPsec policies, and PSKs configured on the cloud and in the on-premises data center must be the same.
- The parameters configured for the local and remote subnets and gateways must be symmetric.
- Security group rules permit access to and from the ECSs in the VPC.
- The status of a VPN changes to **Normal** only after ECSs and on-premises servers access each other.

Prerequisites

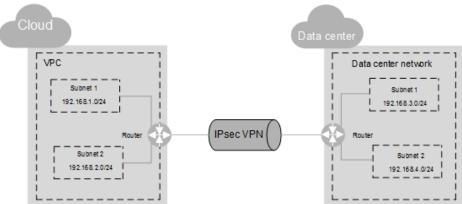
You have created the VPC and subnets that the on-premises data center wants to access.

Procedure

- 1. On the management console, select the appropriate IKE and IPsec policies to create a VPN.
- 2. Check the IP address pools for the local and remote subnets.

 In **Figure 4-4**, the VPC has subnets 192.168.1.0/24 and 192.168.2.0/24. Your on-premises data center has subnets 192.168.3.0/24 and 192.168.4.0/24. You can set up a VPN to connect these subnets.

Figure 4-4 IPsec VPN



The IP address pools for the local subnets cannot overlap with those for the remote subnets. Like in this example, the IP address pool for the remote subnets cannot contain the two subnets of the VPC.

- 3. Configure security group rules for the ECSs to allow packets from and to the on-premises data center over the VPN.
- 4. Ping the ECSs from the on-premises data center to verify that the security group allows packets from and to the on-premises data center over the VPN.
- 5. Check the on-premises network configuration.

A route must be configured for the on-premises network to enable traffic to be forwarded to network devices on the network over the VPN. If the data transmitted through the VPN cannot be forwarded to the network devices, check whether the remote LAN has rules configured to refuse the traffic.

5 Troubleshooting

5.1 The State of a VPN Connection Is Not connected

Symptom

On the **Enterprise – VPN Connections** page of the VPN console, the state of a VPN connection is displayed as **Not connected**.

Possible Causes

- The configurations at the two ends of the VPN connection are incorrect.
- The security group configuration on the management console or the ACL configuration on the customer gateway device is incorrect.
- The IPsec VPN connection negotiation fails or the connection is disconnected.

Procedure

- Check the configurations at the two ends of the VPN connection.
 - Check whether the gateway IP addresses configured at the two ends of the VPN connection are reversed.
 - To check the active and standby EIPs of the VPN gateway, choose Virtual Private Network > Enterprise – VPN Gateways and view the IP addresses in the Gateway IP Address column.
 - To check the IP address of the customer gateway, choose Virtual
 Private Network > Enterprise Customer Gateways and view the
 IP address in the Identifier column.
 - Check whether the IKE and IPsec policies at the two ends of the VPN connection are consistent.
 - To view the IKE and IPsec policy settings on the VPN console, choose Virtual Private Network > Enterprise – VPN Connections, locate the target VPN connection, and choose More > Modify Policy Settings.

- Check whether the PSKs at the two ends of the VPN connection are the same.
 - The PSK cannot be checked on the VPN console. If you are not sure whether the PSK configured on the VPN console is correct, you are advised to change it to be the same as that configured on the customer gateway device.
 - To change the PSK on the VPN console, choose **Virtual Private Network > Enterprise VPN Connections**, locate the target VPN connection, and choose **More > Reset PSK**.
- If the policy-based mode is used, check whether the source and destination CIDR blocks in the policy rules at the two ends of the VPN connection are reversed.
 - To check policy rules on the VPN console, choose **Virtual Private Network > Enterprise VPN Connections**, locate the target VPN connection, and click **Modify VPN Connection**.
- If the static routing mode is used and the NQA function is enabled on the VPN console, check whether tunnel interface IP addresses are correctly configured on the customer gateway device.
 - To check whether NQA is enabled on the VPN console, choose
 Virtual Private Network > Enterprise VPN Connections, click the name of the target VPN connection, and view the value of Link
 Detection on the Summary tab page.
 - To check the tunnel interface IP addresses configured on the VPN console, choose Virtual Private Network > Enterprise VPN Connections, click Modify VPN Connection, and view the values of Local Interface IP Address and Customer Interface IP Address. The local and remote interface IP addresses configured on the customer gateway device must be the same as the values of Customer Interface IP Address and Local Interface IP Address configured on the VPN console, respectively.
- If the BGP routing mode is used, check whether the BGP ASNs at the two ends of the VPN connection are reversed.
 - To check the BGP ASN of the VPN gateway, choose Virtual Private Network > Enterprise - VPN Gateways, click the VPN gateway name, and view the BGP ASN in the Basic Information area.
 - To check the BGP ASN of the customer gateway, choose Virtual Private Network > Enterprise - Customer Gateways and view the value in the BGP ASN column.
- Check the security group configuration on the management console and the ACL configuration on the customer gateway device.
 - Check whether the default security group on the management console permits the ports corresponding to the public IP addresses of the customer gateway.
 - To check the default security group on the management console, perform the following steps:
 - Choose Virtual Private Network > Enterprise VPN Gateways, and click the name of the VPC associated with the VPN gateway.

- ii. On the **Virtual Private Cloud** page, click the number in the **Route Tables** column.
- iii. On the Route Tables page, click the name of the route table.
- iv. Locate and click the next hop of the active or standby EIP of the VPN gateway.
- v. On the **Associated Security Groups** tab page, check whether the security group permits traffic of the ports.
- Verify that an ACL on the customer gateway device permits the ports corresponding to the active and standby EIPs of the VPN gateway.
- Check IPsec connection logs.
 - a. Log in to the management console.
 - b. Click in the upper left corner and select the desired region and project.
 - c. Click in the upper left corner, and choose > .
 - d. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise VPN Connections**.
 - e. On the **VPN Connection** page, locate the target VPN connection, and choose **More** > **View Logs** to view connection logs.

Check IPsec connection logs, and locate the fault based on the log keywords and error codes listed in **Table 5-1**.

Table 5-1 Common causes of VPN disconnection

Catego ry	Error Code	Description
IPsec VPN	phase1 proposal mismatch	IKE proposal parameters on both ends do not match.
negotia tion failure	phase2 proposal or pfs mismatch	IPsec proposal parameters, PFS algorithms, or security ACLs on both ends do not match.
	responder dh mismatch	The DH algorithm of the responder does not match that of the initiator.
	initiator dh mismatch	The DH algorithm of the initiator does not match that of the responder.
	encapsulation mode mismatch	Encapsulation modes on both ends do not match.
	flow mismatch	Security ACLs on both sides do not match.
	version mismatch	IKE versions on both ends do not match.

Catego ry	Error Code	Description
	peer address mismatch	IKE peer addresses on both ends do not match.
	config ID mismatch	No IKE peer with the specified ID is found.
	exchange mode mismatch	Negotiation modes on both ends do not match.
	authentication fail	The identity authentication fails.
	construct local ID fail	A local ID fails to be constructed.
	rekey no find old sa	The old SA fails to be found during renegotiation.
	rekey fail	The old SA is going offline during renegotiation.
	first packet limited	First packets are rate limited.
	unsupported version	The IKE version is not supported.
	malformed message	There is a malformed message.
	malformed payload	There is a malformed payload.
	critical drop	The critical payload is not recognized.
	cookie mismatch	The cookies do not match.
	invalid cookie	The cookie is invalid.
	invalid length	The packet length is invalid.
	short packet	Packets are ultra-short.
	unknown exchange type	The negotiation mode is unknown.
	uncritical drop	The non-critical payload is not identified.
	route limit	The number of imported routes reaches the upper limit.
	ip assigned fail	IP address assignment fails.
	eap authentication timeout	EAP authentication times out.
	eap authentication fail	EAP authentication fails.
	xauth authentication fail	XAUTH authentication fails.

Catego ry	Error Code	Description
	xauth authentication timeout	XAUTH authentication times out.
	license or specification limited	There is license control.
	local address mismatch	The local IP address and interface IP address in IKE negotiation do not match.
	dynamic peers number reaches limitation	The number of IKE peers reaches the upper limit.
	ipsec tunnel number reaches limitation	The number of IPsec tunnels reaches the upper limit.
	netmask mismatch	The mask does not match the configured one after the IPsec mask filtering function is enabled.
	flow confict	A data flow conflict exists.
	proposal mismatch or use sm in ikev2	IPsec proposals on both ends do not match or IKEv2 uses an SM algorithm.
	ikev2 not support sm in ipsec proposal ikev2	IKEv2 does not support the SM algorithm used in the IPsec proposal.
	no policy applied on interface	No policy is applied to an interface.
	nat detection fail	NAT detection fails.
	fragment packet limit	The number of fragments exceeds the upper limit.
	fragment packet reassemble timeout	Fragment reassembly times out.
	peer cert is expired	The peer certificate has expired.
	peer cert is revoked by CRL	The peer certificate is revoked.
	sa with same user exists	The SA is the same as that of another user.
	max transmit reached	The number of retransmitted packets reaches the maximum.

Catego ry	Error Code	Description
IPsec	dpd timeout	DPD detection times out.
VPN connect ion disconn	peer request	The remote end sends a message, asking the local end to tear down a tunnel.
ection	config modify or manual offline	The SA is automatically deleted due to configuration modification, or is manually deleted.
	phase1 hard expiry	In phase 1, hard timeout (no new SA negotiation succeeds) occurs.
	phase2 hard expiry	A hard timeout occurs in phase 2.
	heartbeat timeout	Heartbeat detection times out.
	peer address switch	The peer address is changed.
	re-auth timeout	The SA is deleted because the reauthentication times out.
	aaa cut user	The SA is deleted because the AAA module logs out the user.
	ip address syn failed	IP addresses fail to be synchronized.
	hard expiry triggered by port mismatch	Hard timeout occurs due to a NAT port number mismatch.
	kick old sa with same flow	The old SA is deleted when the same flow is transmitted.
	cpu table updated	When an SPU is removed and inserted, the SAs of CPUs other than the one on the SPU are deleted.
	flow overlap	The IP address in the encrypted data flow conflicts with the remote IP address.
	spi conflict	An SPI conflict occurs.
	admin down	The VPN tunnel status is admin down.
	forward down	The fwd group goes down.
	sa with same user exists	The SA is the same as that of another user.
	reset sa by ike user	A user resets the SA.

Catego ry	Error Code	Description
	phase1 sa replace	A new IKE SA replaces the old one.
	phase2 sa replace	A new IPsec SA replaces the old one.
	manual offline	The connection is manually torn down.
	nhrp notify	The NHRP module notifies the device of SA deletion.
	receive backup delete info	The standby device receives an SA backup deletion message from the active device.
	eap delete old sa	When the peer device performs EAP authentication repeatedly, the local device deletes the old SA.
	receive invalid spi notify	The device receives an invalid SPI notification.
	dns resolution status change	The DNS resolution status is changed.
	ikev1 phase1-phase2 sa dependent offline	The device deletes the associated IPsec SA when deleting an IKEv1 SA.
	exchange timeout	Packet exchange times out.
	hash gene adjusted	The hash factor is adjusted, causing the IPsec tunnel to be deleted.

5.2 Ping Tests Between Cloud and On-premises Networks Fail

Symptom

- Servers in an on-premises data center cannot ping ECSs in a VPC.
- ECSs in a VPC cannot ping the servers in an on-premises data center.

Possible Causes

- The security group configuration on the management console is incorrect.
- The ACL rule associated with the interconnection subnet is incorrectly configured.
- The ACL configuration on the customer gateway device is incorrect.

• The route configuration on the customer gateway device is incorrect.

Procedure

- Check the security group configuration on the management console.
 - Verify that the default security group on the management console permits data flows destined for the customer subnet.
 - To check the default security group on the management console, perform the following steps:
 - Choose Virtual Private Network > Enterprise VPN Gateways, and click the name of the VPC associated with the VPN gateway.
 - ii. Click the number of route tables corresponding to the VPC.
 - iii. On the Route Tables page, click the name of the route table.
 - iv. Locate and click the next hop of the active or standby EIP of the VPN gateway.
 - v. On the **Associated Security Groups** tab page, check the ports permitted by the security group.
 - Verify that the default security group on the management console permits data flows originated from the customer subnet.
 - Verify that the default security group on the management console permits data flows destined for the local subnet.
 - Verify that the default security group on the management console permits data flows originated from the local subnet.
 - Verify that a security group permits data flows from the ECSs to the customer subnet.
 - To check whether such a security group has been configured, choose **Compute > Elastic Cloud Server**, click an ECS name, click the **Security Groups** tab, and click **Manage Rule**.
 - Verify that a security group permits data flows from the customer subnet to the ECSs.
- The ACL rule associated with the interconnection subnet is incorrectly configured.
 - Check whether the ACL rule associated with the interconnection subnet permits the ports between all local and customer subnets.
 - Choose Virtual Private Network > Enterprise VPN Gateways, and click the name of target VPN gateway.
 - ii. In the **Basic Information** area, check and record the interconnection subnet.
 - iii. In the **Basic Information** area, click the name of the associated VPC.
 - iv. On the **Summary** tab page of the VPC, click the number of subnets in the **Networking Components** area.
 - v. Find the interconnection subnet in the subnet list, and click the ACL name in the **Network ACL** column.
 - vi. Permit the ports between all local and customer subnets.
- Check the ACL configuration on the customer gateway device.

- Verify that an ACL rule on the customer gateway device permits data flows destined for the local subnet of the VPN gateway.
- Verify that an ACL rule on the customer gateway device permits data flows originated from the local subnet of the VPN gateway.

To check the local subnet of the VPN gateway, choose **Virtual Private Network** > **Enterprise** - **VPN Gateways**, click the VPN gateway name, and view the value of **Local Subnet** in the **Basic Information** area.

- Check the route configuration on the customer gateway device.
 - Verify that the public network route is correctly configured. That is, the
 destination address is an EIP of the VPN gateway, and the next hop is the
 egress interface address of the customer gateway device.
 - Verify that the private network route is correctly configured. That is, the
 destination address is the local subnet of the VPN gateway, and the next
 hop is the egress interface address of the customer gateway device.

To check the local subnet of the VPN gateway, choose **Virtual Private Network > Enterprise - VPN Gateways**, click the VPN gateway name, and view the value of **Local Subnet** in the **Basic Information** area.

5.3 Packet Loss Occurs

Symptom

- Packet loss occurs when a server in an on-premises data center pings an ECS in a VPC.
- Packet loss occurs when an ECS in a VPC pings a server in an on-premises data center.

Procedure

- Check the customer-side networking and bandwidth.
 - Check whether the customer network has multiple egresses working in load balancing mode and whether traffic destined for the cloud is distributed to a non-VPN egress. Ensure that the traffic destined for the cloud is transmitted through the same egress.
 - Ping the IP address of the VPN gateway at the cloud side and other public IP addresses (for example, 114.114.114.114) from the customer gateway to check the delay and packet loss rate on the public network.
 If the quality of the public network is poor, you are advised to seek help from the corresponding carrier.
 - Check whether traffic on the customer gateway device exceeds the bandwidth limit.
- Check the cloud-side networking and bandwidth.
 - Check whether traffic exceeds the bandwidth of the VPN gateway.
 If traffic exceeds the bandwidth of the VPN gateway, increase the bandwidth.

6 FAQS

6.1 Enterprise Edition VPN

6.1.1 What Are the Typical Scenarios of IPsec VPN?

A VPN is a point-to-point connection that implements private network access between two points.

- Applicable scenarios:
 - A VPN is created between different regions to enable cross-region VPC communications.
 - A VPN hub is used together with VPC peering connections and Cloud Connect connections to enable communications between an on-premises data center and multiple VPCs on the cloud.
 - A VPN is used together with source NAT to enable access to specific IP addresses across clouds.
- Not applicable scenarios:
 - A VPN cannot be used to connect VPCs in the same region. It is recommended that you use VPC peering connections to enable communications between VPCs in the same region.
 - A VPN cannot be used between the cloud and your home network that uses PPPoE dial-up.
 - A VPN cannot be used between the cloud and 4G/5G routers.
 - A VPN cannot be used between the cloud and your personal terminals.

6.1.2 What Are a VPC, a VPN Gateway, and a VPN Connection?

VPC enables you to create private, isolated virtual networks. You can use VPN to securely access ECSs in VPCs.

A VPN gateway is an egress gateway for a VPC. With a VPN gateway, you can create a secure, reliable, and encrypted connection between a VPC and an on-premises data center or between two VPCs in different regions.

A VPN connection is a secure and reliable IPsec encrypted communications tunnel established between a VPN gateway and the customer gateway in an on-premises data center.

To create a VPN on the cloud, perform the following operations:

- 1. Create a VPN gateway. You need to specify the VPC to be connected, as well as the bandwidth and EIPs of the VPN gateway.
- 2. Create a VPN connection. You need to specify the gateway EIP used to connect to the customer gateway, subnets, and negotiation policies.

6.1.3 How Do I Plan CIDR Blocks for Access to a VPC Through a VPN Connection?

- The CIDR blocks of a VPC cannot conflict with on-premises CIDR blocks.
- To avoid conflicts with cloud service addresses, do not use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3, or 100.64.0.0/10 for your on-premises network.

6.1.4 Is an IPsec VPN Connection Automatically Established?

Yes. An IPsec VPN connection is automatically established.

6.1.5 What Are VPN Negotiation Parameters? What Are Their Default Values?

Table 6-1 VPN negotiation parameters

Protocol	Parameter	Value
IKE	Version	 v1 (v1 has low security. If the device supports v2, v2 is recommended.) v2 (default value)
	Negotiation Mode	Main (default value)Aggressive
	Authentication Algorithm	MD5 (This algorithm is insecure. Exercise caution when using this algorithm.)
		 SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.)
		SHA2-256 (default value)
		• SHA2-384
		• SHA2-512

Protocol	Parameter	Value
	Encryption Algorithm	 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) AES-128 (default value) AES-192 (This algorithm is insecure. Exercise caution when using this algorithm.) AES-256 (This algorithm is insecure. Exercise caution when using this algorithm.)
	DH Algorithm	 Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) Group 14 (default value) Group 15 Group 16 Group 19 Group 20 Group 21
	Lifetime (s)	86400 (default value) Unit: second Value range: 60 to 604800
	Local ID	 IP Address The local IP address is automatically displayed as the EIP of the VPN gateway, removing the need to manually configure it. FQDN By default, the local ID type is IP address and the local ID value is the EIP of the VPN gateway.

Protocol	Parameter	Value
	Customer ID	 IP Address FQDN By default, the customer ID type is IP address and the customer ID value is the public IP address of the customer gateway.
IPsec	Authentication Algorithm	 SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) SHA2-256 (default value) SHA2-384 SHA2-512
	Encryption Algorithm	 AES-128 (default value) AES-192 (This algorithm is insecure. Exercise caution when using this algorithm.) AES-256 (This algorithm is insecure. Exercise caution when using this algorithm.) 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) AES-128-GCM-16 AES-256-GCM-16

Protocol	Parameter	Value
	PFS	DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.)
		DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.)
		 DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.)
		DH group 14 (default value)
		DH group 15
		DH group 16
		DH group 19
		DH group 20
		DH group 21
		 Disable (not recommended due to security risks)
	Transfer Protocol	ESP (default value)
	Lifetime (s)	3600 (default value)
		Unit: second
		Value range: 30 to 604800

™ NOTE

- Perfect Forward Secrecy (PFS) is a security feature.
 - IKE negotiation has two phases, phase one and phase two. The key of phase two (IPsec SA) is derived from the key generated in phase one. Once the key in phase one is disclosed, the security of the IPsec VPN may be adversely affected. To improve the key security, IKE provides PFS. When PFS is enabled, an additional DH exchange will be performed during IPsec SA negotiation to generate a new IPsec SA key, improving IPsec SA security.
- For security purposes, PFS is enabled on the cloud side by default. Ensure that PFS is also enabled on the gateway device in your on-premises data center and the PFS settings on both ends are the same. Otherwise, the negotiation will fail.
- The default traffic-based lifetime of an IPsec SA is 1,843,200 KB on the cloud side and cannot be changed for the VPN. This parameter is not involved in negotiation and has no impact on the establishment of an IPsec SA.

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

No. IPsec VPN uses a pre-shared key (PSK) for authentication. The PSK is configured on a VPN gateway, and a connection will be established after VPN negotiation is complete. Therefore, no username or password is required for

creating an IPsec VPN connection. Generally, SSL, PPTP, and L2TP VPNs use usernames and passwords for authentication.

□ NOTE

IPsec XAUTH provides extended authentication for IPsec VPN. It requires users to enter their usernames and passwords during VPN negotiation.

Currently, VPN does not support IPsec XAUTH.

6.1.7 What VPN Resources Can Be Monitored?

VPN gateway

The following bandwidth information of a VPN gateway IP address can be monitored: inbound traffic, inbound bandwidth, outbound traffic, outbound bandwidth, and outbound bandwidth usage.

VPN connection

The following information about a VPN connection can be monitored: VPN connection status, average link round-trip time (RTT), maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate.

To monitor average link RTT, maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate, click the VPN connection name and click **Add** in the **Health Check** area on the **Summary** tab page to add health check items. Private network metrics can be configured only when the VPN connection uses the static routing mode and the NQA function is enabled.

6.1.8 Can EIPs Be Used as VPN Gateway IP Addresses?

Yes.

When creating a VPN gateway, you can bind EIPs as the gateway IP addresses.

6.1.9 Which IKE Version Should I Select When I Create a VPN Connection?

IKEv2 is recommended because IKEv1 is not secure. In addition, IKEv2 outperforms IKEv1 in connection negotiation and establishment, authentication methods, dead peer detection (DPD) timeout processing, and security association (SA) timeout processing.

IKEv2 will be widely used, and IKEv1 will gradually phase out.

Introduction to IKEv1 and IKEv2

- As a hybrid protocol, IKEv1 brings some security and performance defects due to its complexity. As such, it has become a bottleneck in the IPsec system.
- IKEv2 addresses the issues of IKEv1 while retaining basic functions of IKEv1. IKEv2 is more simplified, efficient, secure, and robust than IKEv1. Additionally, IKEv2 is defined by RFC 4306 in a single document, whereas IKEv1 are defined in multiple documents. By minimizing core functions and default password

algorithms, IKEv2 greatly improves interoperability between different IPsec VPNs

Security Risks of IKEv1

- The cryptographic algorithms supported by IKEv1 have not been updated for more than 10 years. In addition, IKEv1 does not support strong cryptographic algorithms such as AES-GCM and ChaCha20-Poly1305. For IKEv1, the E (Encryption) bit in the ISALMP header specifies that the payloads following the ISALMP header are encrypted, but any data integrity verification of those payloads is handled by a separate hash payload. This separation of encryption from data integrity protection prevents the use of authenticated encryption (AES-GCM) with IKEv1.
- IKEv1 is vulnerable to DoS amplification attacks and half-open connection attacks. After responding to spoofed packets, the responder maintains initiator-responder relationships, consuming a large number of system resources.

This defect is inherent to IKEv1 and is addressed in IKEv2.

 The aggressive mode of IKEv1 is not secure. In this mode, information packets are not encrypted, posing risks of information leakage. There are also bruteforce attacks targeting at the aggressive mode, such as man-in-the-middle attacks.

Differences Between IKEv1 and IKEv2

Negotiation process

- IKEv1 is complex and consumes a large amount of bandwidth. IKEv1 SA negotiation consists of two phases. In IKEv1 phase 1, an IKE SA is established in either main mode or aggressive mode. Main mode requires three exchanges between peers totaling six ISAKMP messages, whereas aggressive mode requires two exchanges totaling three ISAKMP messages. Aggressive mode is faster, but does not provide identity protection for peers as key exchange and identity authentication are performed simultaneously. In IKEv1 phase 2, IPsec SAs are established through three ISAKMP messages in quick mode.
- Compared with IKEv1, IKEv2 simplifies the SA negotiation process. IKEv2 requires only two exchanges, totaling four messages, to establish an IKE SA and a pair of IPsec SAs. To create multiple pairs of IPsec SAs, only one additional exchange is needed for each additional pair of SAs.

□ NOTE

For IKEv1 negotiation, its main mode involves nine (6+3) messages, and its aggressive mode involves six (3+3) messages. In contrast, IKEv2 negotiation requires only four (2+2) messages.

Authentication methods

- Only IKEv1 (requiring an encryption card) supports digital envelope authentication (HSS-DE).
- IKEv2 supports Extensible Authentication Protocol (EAP) authentication.
 IKEv2 can use an AAA server to remotely authenticate mobile and PC users and assign private IP addresses to these users. IKEv1 does not provide this function and must use L2TP to assign private IP addresses.

Only IKEv2 supports IKE SA integrity algorithms.

• DPD timeout processing

- Only IKEv1 supports the retry-interval parameter. If a device sends a DPD packet but receives no reply within the specified retry-interval, the device records a DPD failure event. When the number of DPD failure events reaches 5, both the IKE SA and IPsec SAs are deleted. IKE SA negotiation will start again only when there is traffic to be transmitted over the IPsec tunnel.
- In IKEv2, the retransmission interval increases from 1, 2, 4, 8, 16, 32 to 64, in seconds. If no reply is received within eight consecutive transmissions, the peer end is considered dead, and the IKE SA and IPsec SAs are deleted.

IKE SA timeout processing and IPsec SA timeout processing

In IKEv2, the IKE SA soft lifetime is 9/10 of the IKE SA hard lifetime plus or minus a random number. This reduces the likelihood that two ends initiate renegotiation simultaneously. Therefore, you do not manually set the soft lifetime in IKEv2.

Advantages of IKEv2 over IKEv1

- Simplifies the SA negotiation process, improving efficiency.
- Fixes many cryptographic security vulnerabilities, improving security.
- Supports EAP authentication, improving authentication flexibility and scalability.
 - EAP is an authentication protocol that supports multiple authentication methods. The biggest advantage of EAP is its scalability. That is, new authentication methods can be added without changing the original authentication system. EAP authentication has been widely used in dial-up access networks.
- Employs an Encrypted Payload on basis of ESP. This payload contains both an encryption algorithm and a data integrity algorithm. AES-GCM ensures confidentiality, integrity, and authentication, and works well with IKEv2.

6.1.10 What Do I Do If a VPN Connection Fails to Be Established?

- Log in to the management console, and choose Virtual Private Network > Enterprise - VPN Connections.
- In the VPN connection list, locate the target VPN connection, and choose
 More > Modify Policy Settings on the right to view IKE and IPsec policies of
 the VPN connection.
- 3. Check the IKE and IPsec policies to see whether the negotiation modes and encryption algorithms at both ends of the VPN connection are the same.

 If the IKE SA has been set up in phase 1 but no IPsec SA has been established in phase 2, the IPsec policies at both ends of the VPN connection may be inconsistent.
- 4. Check whether the ACL configurations are correct.

 If the subnets of your on-premises data center are 192.168.3.0/24 and 192.168.4.0/24, and the VPC subnets are 192.168.1.0/24 and 192.168.2.0/24,

configure the ACL rules for each on-premises subnet to allow communication with the VPC subnets. The following provides an example of ACL configurations:

```
rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255 rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255 rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
```

Ping the two ends of the VPN connection from each other to check whether the VPN connection is normal.

6.2 Classic VPN

6.2.1 What Are the Differences Between the Application Scenarios and Connection Modes of IPsec and SSL VPNs?

Scenarios

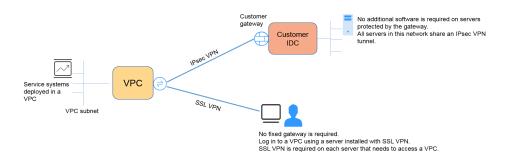
IPsec VPN connects two LANs, such as a branch and its headquarters (or a VPC), or an on-premises data center and a VPC.

SSL VPN connects a client to a LAN. For example, the portable computer of an employee on a business trip accesses the internal network of the company.

Connection Modes

IPsec VPN requires fixed gateways, such as firewalls or routers, at both ends. The administrator needs to configure gateways at both ends to complete IPsec VPN negotiation.

SSL VPN needs to install a specified client software on the server, then the server connects to the SSL device through the username and password.



Currently, only IPsec VPN is supported; SSL VPN is not supported.

6.2.2 Where Can I Add Routes on the VPN Console to Reach the Remote Subnets?

When a VPN connection is created, routes are automatically delivered to reach the remote subnets.

6.2.3 Will I Be Notified If a VPN Connection Is Interrupted?

The VPN connection status can be monitored. After a VPN connection is created, the VPN service reports the connection status information to Cloud Eye, but does not automatically send alarm notifications to you. To receive notifications, create alarm rules and enable **Alarm Notification** on the Cloud Eye console.

After a VPN connection is created, you can locate the row that contains the VPN connection and choose **Operation** > **View Metric** to view the VPN connection status.

6.2.4 How Many VPN Connections Do I Need to Connect to Multiple On-premises Servers?

VPN uses the IPsec technology to connect your on-premises data center to a VPC on the cloud. As such, the number of VPN connections is related to the number of data centers where the servers to be connected to the cloud are located, but not to the number of servers.

In most cases, one on-premises data center has one public gateway. All servers connect to the Internet through this gateway. Therefore, you only need to configure one VPN connection to allow communications between the VPC and your on-premises data center.

6.2.5 What Are the Impacts of a VPN on an On-premises Network? What Are the Changes to the Route for Accessing an ECS?

When you configure a VPN, perform the following operations on the on-premises gateway:

- 1. Configure IKE and IPsec policies.
- 2. Specify the to-be-protected traffic (ACL rules).
- 3. Check the route configuration on the gateway to ensure that traffic destined for a VPC can be routed to the correct outbound interface (interface having an IPsec policy bound).

After the VPN configuration is complete, only the interesting traffic enters the VPN tunnel.

For example, before a VPN is created, on-premises users access the ECS through the EIP bound to the ECS. After a VPN is created, data flows matching the ACL rules access the private IP address of the ECS through the VPN tunnel.

6.2.6 How Do I Replace a Direct Connect Connection with a VPN?

- 1. Ensure that the on-premises gateway supports IPsec VPN.
- 2. Create a VPN gateway and a VPN connection on the cloud. Select the VPC to which the Direct Connect connection uses for the VPN gateway.

NOTICE

When creating a VPN connection, configure its remote subnet as follows to avoid routing conflicts.

- Delete the virtual interface of the Direct Connect connection first and then configure the VPN connection.
- Divide the remote subnet into two subnets and configure the VPN connection. After the Direct Connect connection is deleted, configure the VPN connection again.

6.2.7 How Do I Access ECSs at Home When My Enterprise Network Has Been Connected to the Cloud Through a VPN?

A VPN is an IPsec VPN that connects a VPC on the cloud and an on-premises local area network (LAN).

The home network is not a part of the LAN of your enterprise and cannot be directly connected to the VPC on the cloud.

If your host at home needs to access VPC resources on the cloud, your host can directly access the EIP of the cloud service or connect to the LAN of your enterprise through SSL VPN (if your enterprise supports SSL access) and then access VPC resources on the cloud through the LAN.

6.2.8 How Do I Configure DPD for Interconnection with the Cloud?

By default, DPD is enabled on the cloud side and cannot be disabled.

Configure DPD as follows:

- DPD-type: on-demand
- DPD idle-time: 30s
- DPD retransmit-interval: 15s
- DPD retry-limit: 3
- DPD msg: seq-hash-notify

The **DPD msg** format at both ends of the VPN connection must be the same, but the DPD type, idle time, retransmission interval, and retry limit can be different.

6.2.9 Why Is Not Connected Displayed as the Status for a Successfully Created VPN Connection?

After a VPN connection is created, its status changes to **Normal** only after servers at both ends of the VPN connection communicate with each other.

• IKE v1:

If no traffic goes through the VPN connection for a period of time, the VPN connection needs to be renegotiated. The negotiation time depends on the value of **Lifetime (s)** in the IPsec policy. Generally, **Lifetime (s)** is set to **3600** (1 hour), indicating that the negotiation will be initiated in the fifty-fourth

minute. If the negotiation succeeds, the connection remains to the next round of negotiation. If the negotiation fails, the VPN connection status changes to **Not Connected** within one hour. The connection can be restored only after the two ends of the VPN connection communicate with each other. The disconnection can be avoided by using a network monitoring tool, such as IP SLA, to generate packets.

• IKE v2: If no traffic goes through the VPN connection for a period of time, the VPN connection remains in the connected status.

A Change History

Released On	Description
2025-09-17	This issue is the third official release. Added information about Enterprise Edition VPN.
2022-05-25	This issue is the second official release. Added Monitoring.
2020-08-30	This issue is the first official release.