Virtual Private Network (VPN)
8.2.1
User Guide

Issue	02
Date	2023-04-30



HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions


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

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

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Overview **1**
1.1 What Is Virtual Private Network? 1
1.2 Advantages 2
1.3 Application Scenarios 3
1.4 Related Services 4
1.5 Feature List 5
1.6 Restrictions and Limitations 5
1.7 Accessing and Using VPN 6
2 Related Concepts **7**
2.1 IPsec VPN 7
2.2 Virtual Private Cloud (VPC) 8
3 Operation Process **9**
4 Getting Started **12**
4.1 Applying for a VPC 12
4.2 Creating a Subnet 18
4.3 Applying for a VPN 23
5 Creation **32**
5.1 Applying for a VPN 32
6 Managing a VPN Gateway **41**
7 Managing a VPN Connection **43**
8 Best Practice **45**
8.1 Using the IPsec VPN to Enable Communication Between a VPC and One or More Sites 45
8.2 Using the IPsec VPN to Enable Communication Between Two VPCs in Different Regions 49
9 FAQs **55**
9.1 What Types of VPNs Are Supported? 55
9.2 What Are the Differences Between VPN and Direct Connect? 55
9.3 Does the IPsec VPN Support Automatic Negotiation? 56
9.4 What Are the Reference Standards and Protocols for the IPsec VPN? 56
9.5 What Do I Do If VPN Connection Setup Fails? 57

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

9.6 How Can I Handle the Failure in Accessing the ECSs from My Data Center or LAN Even If the VPN Connection Has Been Set Up? 58
9.7 What Do I Do If I Cannot Access My Data Center or LAN from the ECSs After a VPN Connection Has Been Set Up? 59
9.8 Does a VPN Allow for Communication Between Two VPCs? 59
9.9 What Is the Limitation on the Number of Local and Remote Subnets of a VPN? 59
9.10 How Long Is Required for Issued VPN Configurations to Take Effect? 59
9.11 How Do I Log In to the VPN Console as a VDC Administrator or VDC Operator? 59

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

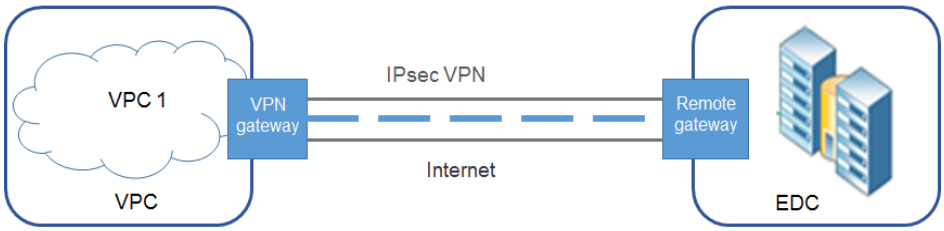
1 Overview

1.1 What Is Virtual Private Network?

A virtual private network (VPN) is a secure, encrypted communication tunnel established between a remote user and a virtual private cloud (VPC). This tunnel meets the industry standards and can seamlessly extend your data center to a VPC.

By default, an Elastic Cloud Server (ECS) or bare metal server (BMS) in a VPC cannot communicate with your data center or private network. To enable communication between them, use a VPN. If you are a remote user and you want to access the service resources of a VPC, you can use a VPN to connect to the VPC.

Figure 1-1 VPN structure



- VPN Gateway

  A VPN gateway is an egress gateway of a VPC. You can use a VPN gateway to enable encrypted communication between a VPC and your data center or between a VPC in one region and a VPC in another region. A VPN gateway works together with the remote gateway in the local center or a VPC in another region. Each local data center must have a remote gateway, and each VPC must have a VPN gateway. A VPN gateway can connect to one or more remote gateways. The VPN service allows you to set up VPN connections from one point to one point or from one point to multiple points.

- Remote Gateway

  Specifies the public IP address of a VPN in your data center or a VPC in another region. This IP address is used for communicating with ECSs or BMSs in a specified VPC.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- VPN Connection

  A VPN connection is an Internet-based IPsec encryption technology. With the special tunnel encryption technology, VPN connections use encrypted security services to establish confidential and secure communications tunnels between different networks.

  A VPN connection connects VPN gateways and remote gateways of user data center through establishing a secure and reliable encryption tunnel between them. Currently, only the Internet Protocol Security (IPsec) VPN is supported.

Networking Solution

Professional network hardware devices are used to establish an encrypted communication tunnel for network connectivity.

Functions

- **Extending your data center to the cloud**

  If you want to build an enterprise hybrid cloud architecture, connecting your local data center to cloud resources using an encrypted tunnel over the Internet, create a VPN connection.

- **Streamlining provisioning and management**

  You can provision and manage a VPN connection easily, and a newly created VPN connection takes effect immediately.

- **Extending your applications to the cloud**

  You can use a VPN to connect a VPC to your data center, extending your data center to the VPC rapidly.

Key Technologies

Key Technology	Description
Encryption Algorithm	AES-128, AES-192, and AES-256
Authentication Algorithm	SHA2-256, SHA2-384, and SHA2-512
Transfer Protocol	A variety of supported transfer protocols: ESP, AH, and AH-ESP
Version	Multiple supported versions: V1 and V2

1.2 Advantages

The VPN service is provided by professional devices, ensuring high VPN reliability. In addition, the VPN service enables you to rapidly and smoothly migrate your applications to the cloud, implementing hybrid cloud deployment and expanding the computing capabilities of applications.

- **Secure and reliable data**

  Professional Huawei devices are used to encrypt transmission data using Internet Key Exchange (IKE) and Internet Protocol Security (IPsec), and

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

provide a carrier-class reliability mechanism, ensuring the stable running of the VPN service concerning hardware, software, and links.

- **Seamless resource scaling up**

  The VPN service allows your local data center to connect to a VPC on the cloud. In this way, your businesses can be rapidly migrated to the cloud, achieving high scalability for your applications and businesses.

- **Low-cost connection**

  IPsec channels are set up over the Internet. Compared with traditional connection modes, VPN connections produce lower costs.

- **Convenient provisioning operation**

  The VPN service and its configuration take effect immediately. This enables you to rapidly and efficiently deploy the VPN service.

- **Flexible architecture**

  Riding on the long-term cooperation and close contact with carriers, Huawei provides you with professional one-step services.

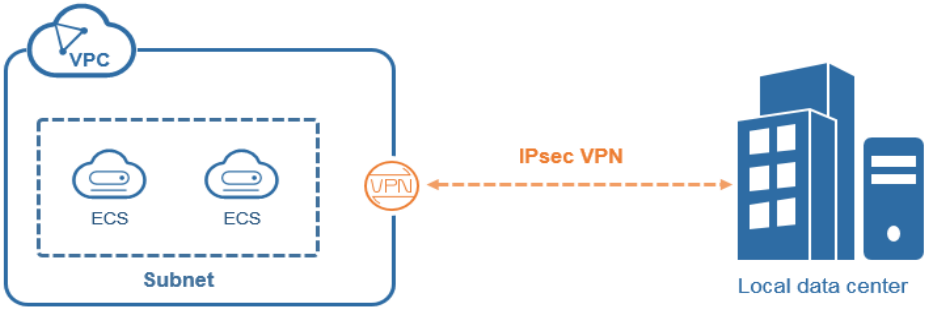
- **Professional O&M capabilities**

  VPN can meet your requirement for either hybrid cloud access or remote DR backup.

1.3 Application Scenarios

Deploying a VPN to Connect a VPC to a Local Data Center

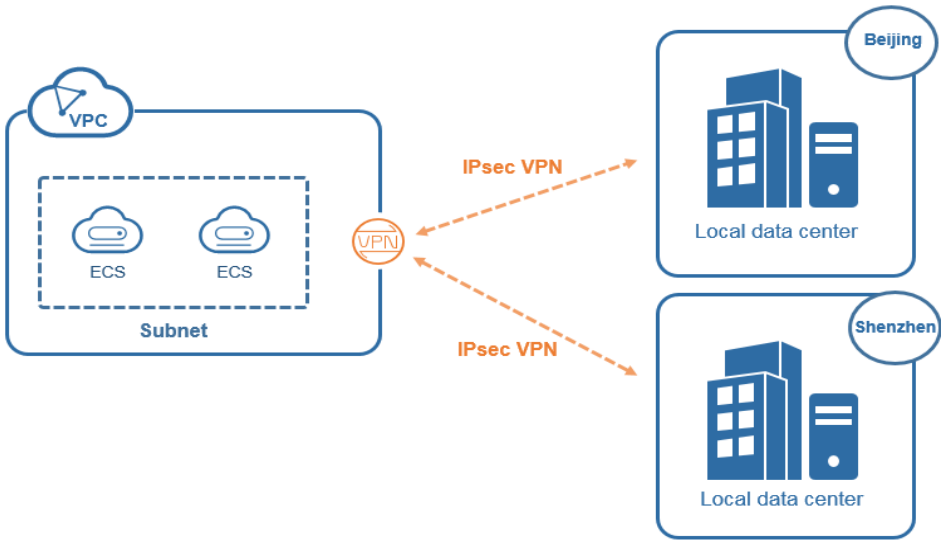
With the VPN between a VPC and your traditional data center, you can easily use the ECSs and block storage resources in the cloud. Applications can be migrated to the cloud and additional web servers can be created to increase the computing capacity on a network. In this way, a hybrid cloud is built, which reduces IT O&M costs and protects enterprise core data from being leaked.



Deploying a VPN to Connect a VPC to Multiple Local Data Centers

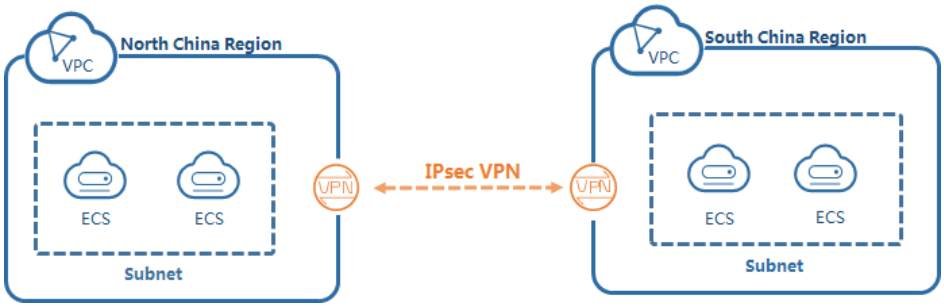
With VPN between VPC and multiple traditional data centers, you can easily use ECSs and block storage resources in the cloud. To connect multiple sites, ensure that the subnet CIDR blocks of each site involved in the VPN connection cannot overlap.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



Cross-Region Interconnection Between VPCs

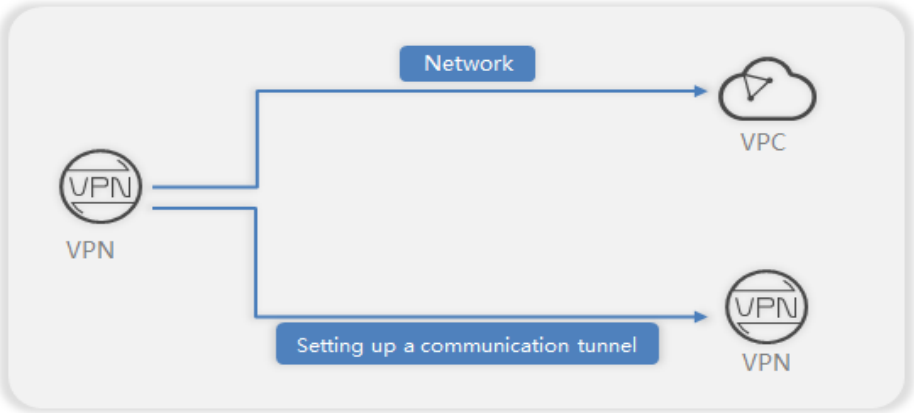
In this scenario, a VPN tunnel is established between two VPCs in different regions to enable mutual access between the two VPCs.



1.4 Related Services

Figure 1-2 and Table 1-1 describe the relationship between VPN and other cloud services.

Figure 1-2 VPN-related services



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 1-1 Relationship between VPN and other cloud services

Service Name	Description
VPC	VPN builds a communication tunnel between VPC and a traditional data center, and therefore VPC will be used.

1.5 Feature List

Context

The CPUs supported by the service are provided by Intel, Hygon (AMD), Kunpeng, and Phytium. Intel and Hygon (AMD) CPUs use the x86 architecture, and Kunpeng and Phytium CPUs use the Arm architecture. For details about the features and functions supported by servers using different CPUs, see ***Huawei Cloud Stack 8.2.1 Infrastructure Service Feature List (Compute, Network, and Basic Management)***.

1.6 Restrictions and Limitations

Before using VPN, learn the restrictions described in **Table 1-2**.

Table 1-2 VPN restrictions

Item	Restriction
CIDR blocks of local subnet	CIDR blocks of local subnet must be in the private network segment.
CIDR blocks of remote subnet	• The remote subnet and the local subnet cannot have overlapping CIDR blocks. • The remote subnet and the subnet for VPC peering cannot have overlapping CIDR blocks. • CIDR blocks of remote subnet cannot be in the private network segment.
VPN gateway	Each VPN gateway can be associated with only one VPC.
VPN connection	• A VPN gateway can connect to multiple subnets in the associated VPC. • All VPN connections under the same VPN gateway cannot overlap. • The CIDR blocks of remote subnet connected to the same VPN cannot overlap. • The CIDR blocks of local subnets of all VPN connections under the same VPN gateway cannot overlap.

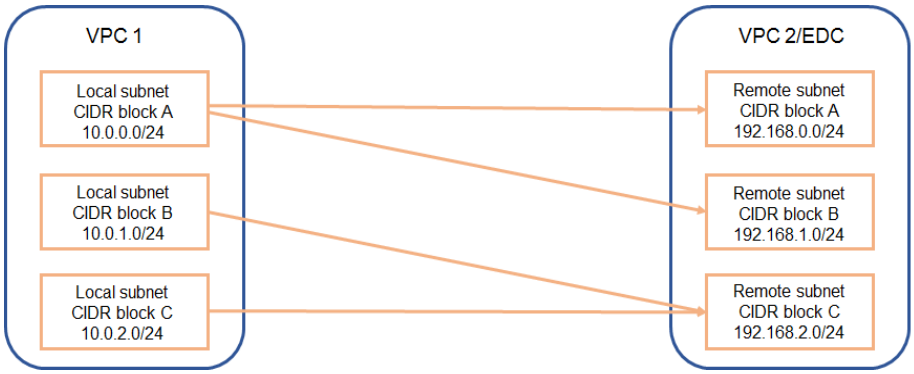
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Correct example:

VPN connection 1: CIDR block of local subnet is 10.0.0.0/24, and CIDR blocks of peering network are 192.168.0.0/24 and 192.168.1.0/24.

VPN connection 2: CIDR block of local subnet is 10.0.1.0/24, and CIDR block of peering network is 192.168.2.0/24.

VPN connection 3: CIDR block of local subnet is 10.0.2.0/24, and CIDR block of peering network is 192.168.2.0/24.



1.7 Accessing and Using VPN

Two methods are available:

- Web UI

  Log in to ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios) as a tenant, click ☰ in the upper left corner of the page, select a region and resource set, and select the cloud service.

- API

  Use this mode if you need to integrate this service into a third-party system for secondary development. For details, see the API reference of this service on **Operation Help Center**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Related Concepts

2.1 IPsec VPN

The Internet Protocol Security (IPsec) VPN is an encrypted tunneling technology that uses encrypted security services to establish confidential and secure communications tunnels between different networks.

In the example shown in **Figure 2-1**, you have created a VPC that has two subnets, 192.168.1.0/24 and 192.168.2.0/24, on the cloud. You also have two subnets, 192.168.3.0/24 and 192.168.4.0/24, on your router deployed in your data center. In this case, you can create an IPsec VPN to enable communication between subnets in your VPC and those in your physical data center.

Currently, the site-to-site VPN and hub-spoke VPN are supported. You need to set up VPNs in both your physical data center and the VPC to establish the VPN connection.

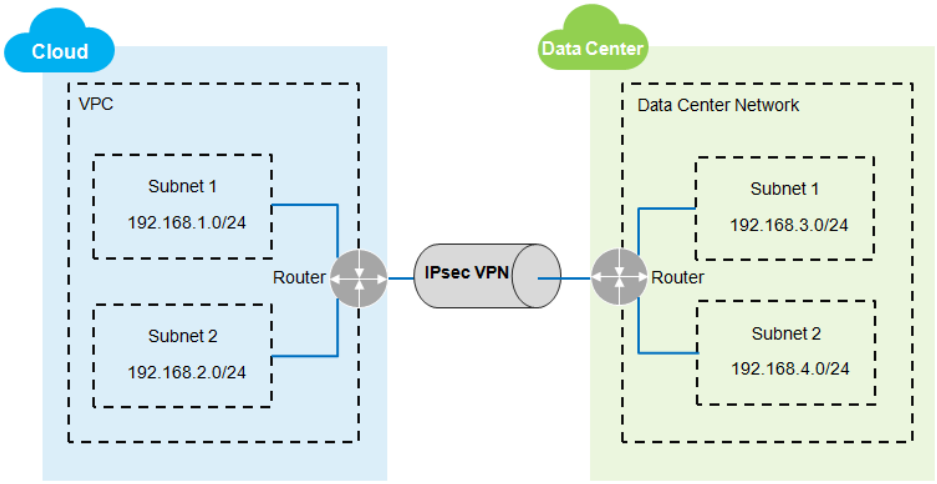
You must ensure that the VPN in your VPC and that in your data center use the same IKE and IPsec policy configurations. Before creating a VPN, familiarize yourself with the protocols described in **Table 2-1** and ensure that your device meets the requirements and configuration constraints of the involved protocols.

Table 2-1 Involved protocols

Parameter	Description	Limitations
RFC 2409	Defines the IKE protocol, which negotiates and verifies key information to safeguard VPN connections.	• Use the PSK to reach an IKE peer agreement. • Use the main mode to perform the negotiation.
RFC 4301	Defines the IPsec architecture, the security services that IPsec offers, and the collaboration between components.	Set up a VPN connection using the IPsec tunnel.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 2-1 IPsec VPN



2.2 Virtual Private Cloud (VPC)

The VPC service enables you to provision logically isolated, configurable, and manageable virtual networks for cloud servers, improving the security of resources in the system and simplifying network deployment. Cloud servers can be elastic cloud servers (ECSs) or bare metal servers (BMSs). For details, see **Operation Help Center** > **Network** > **Virtual Private Cloud** > **User Guide**.

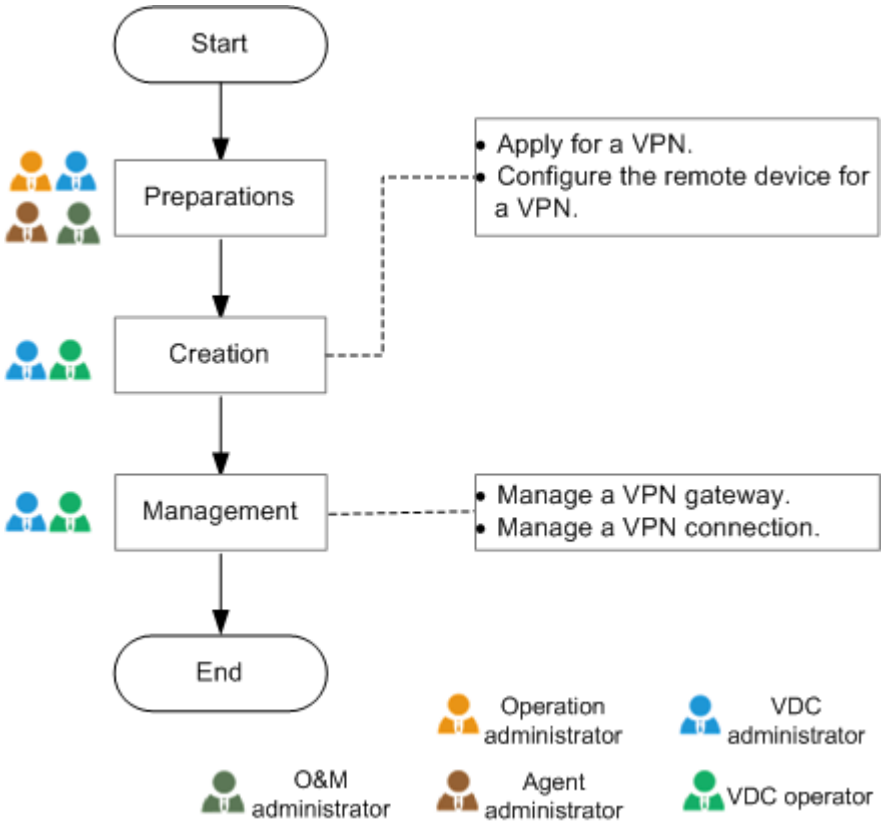
You can select IP address ranges, create subnets, customize security groups, and configure route tables as well as gateways in a VPC. This allows you to manage and modify your network securely and rapidly. You can also customize access rules and network ACLs to control instance access within a security group and across different security groups to enhance security of instances in the subnet.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Operation Process

This section describes the VPN operation process.

Figure 3-1 VPN operation process



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-1 VPN operation process

Operation	Description and Reference	Operator and UI Portal
Preparations	Preparations for VPN creation are as follows: • Obtain the VDC administrator account or VDC operator account. If no such an account is available, contact the operation administrator for creating a VDC and VDC administrator, and then use the VDC administrator account to create a VDC operator account. For details, see **Operation Help Center** > **Operation** > **VDC Tenant Modeling**. • Create and configure an external network. For details, see **Operation Help Center** > **Operation** > **VDC Tenant Modeling** > **Dividing External Networks (Huawei Cloud Stack Scenario)**. • Create a VPC and its subnets. For details, see "Creation" > "Applying for a VPC" in **Operation Help Center** > **Network** > **Virtual Private Cloud** > **User Guide**.	ManageOne Operation Portal (ManageOne Operation Management Portal in B2B scenarios): operation administrator ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC administrator • Agent administrator ManageOne Maintenance Portal: O&M administrator
Creation	Create a basic service network and apply for a VPN. For details, see **5.1 Applying for a VPN**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC administrator • VDC operator
Management	Manage VPN gateways based on service requirements. You can view, modify, or delete the VPN gateways. For details, see **6 Managing a VPN Gateway**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC administrator • VDC operator

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Operation	Description and Reference	Operator and UI Portal
	Manage VPN connections based on service requirements. You can view, modify, delete, or extend the required duration of VPN connections. For details, see **7 Managing a VPN Connection**.	ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios): • VDC administrator • VDC operator

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 Getting Started

4.1 Applying for a VPC

Context

A VPC provides an isolated virtual network for ECSs. You can configure and manage your network as required. This section describes how to create a VPC. You can create subnets, security groups, and other network resources as required by following the instructions provided in subsequent sections.

Prerequisites

You have divided external networks and allocated an external network to the tenant.

- You have created a VPC external network and have allocated it to the tenant. For details, see **Operation Help Center** > **VDC Tenant Modeling** > **Dividing External Networks (Huawei Cloud Stack Scenario)**.
- You have also created an EIP external network, set a resource tag for the external network, created subnets, and allocated the external network to the tenant if you will create subnet 2 that can communicate with the extranet. For details, see **Operation Help Center** > **VDC Tenant Modeling** > **Dividing External Networks (Huawei Cloud Stack Scenario)** > **Configuring an External Network** and **Allocating Resources**.
- You have created an IPv6 subnet pool if you have deployed the dual stack (IPv4 & IPv6) in the system and intend to create a dual-stack VPC and subnets. For details, see **Operation Help Center** > **VDC Tenant Modeling** > **Dividing External Networks (Huawei Cloud Stack Scenario)** > **Configuring IPv6 Settings**.
- You have obtained the permission to apply for VPCs. If the system displays a message indicating that you do not have the required permission, contact the administrator to assign the permission.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Procedure

Step 1 **Log in to the VPN console as a VDC administrator or a VDC operator.**

Step 2 Click  on the left of the main menu, select a region and resource set, and choose **Network** > **Virtual Private Cloud**.

Step 3 In the navigation pane on the left, choose **Virtual Private Cloud** > **My VPCs**.

Step 4 Click **Apply for VPC**.

Step 5 In the displayed **Select Service** dialog box, click **Apply Now**.

Step 6 Set the parameters as prompted. A default subnet will be created together with a VPC.

Set the VPC parameters described in **Table 4-1** and set the subnet parameters described in **Table 4-2**.

Table 4-1 VPC parameters

Parameter	Description	Example Value
Region	The current region and project are displayed by default. To change them, use the selector in the upper left corner of the page.	az1.dc1(test)
Name	Specifies the VPC name. The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	VPC-001
External Network	Select an AZ from the first drop-down list, and select an external network for the VPC from the second drop-down list. If no external networks are available, contact the administrator to configure external networks as described in "Prerequisites".	az0.dc0 net-01
Primary CIDR Block	Specifies the CIDR block of the VPC. The CIDR block of a subnet must be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset of the CIDR block for the VPC (for multiple subnets in the VPC).	192.168.0.0/16
Required Duration	Specifies the required duration for a VPC.	1 year

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-2 Subnet parameters

Parameter	Description	Example Value
Name	Specifies the name of the subnet. The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Subnet-f03c
DHCP	Specifies whether to enable DHCP. • If DHCP is enabled for a subnet, when a cloud server in the subnet starts up, the cloud server automatically obtains, through DHCP, the IP address assigned by the system or specified by you when the cloud server is created. • If DHCP is disabled for a subnet, when a cloud server in the subnet starts up, the cloud server cannot automatically obtain the IP address assigned by the system or specified by you when the cloud server is created. In this case, you need to manually assign an IP address to the cloud server. If a cloud server is not assigned an IP address, it cannot communicate with others. You are not advised to disable DHCP.	Enabled
Type	If you have deployed the dual stack (IPv4 & IPv6) in the system, you need to select a network type first. If you have deployed only IPv4 in the system, configure the subnet parameters directly by referring to **Table 4-3**. • IPv4 Specifies the IPv4 subnet. You can set parameters by referring to **Table 4-3**. • IPv4&IPv6 Specifies that the subnet has both IPv4 and IPv6 address ranges. You can set parameters by referring to **Table 4-3** and **Table 4-4**.	IPv4

Table 4-3 Parameters for configuring an IPv4 subnet

Parameter	Description	Example Value
CIDR Block	Specifies the IP address range of the subnet.	192.168.0.0/24
Gateway	Specifies the gateway address of the subnet.	192.168.0.1

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Allocation Pools	Specifies the range of IP addresses that can be automatically assigned to NICs if you choose to automatically assign an IP address when creating a cloud server or adding a NIC to a cloud server. This parameter is optional. The IP address range of the allocation pool must be within the subnet CIDR block. To reserve some IP addresses in a subnet so that they will not be automatically assigned to NICs, configure an allocation pool. When configuring the allocation pool, enter an IP address range that does not contain these IP addresses. **NOTE** • If a VPC requires two or more allocation pools, click **Add Allocation Pool**. • When creating a cloud server or adding a NIC to a cloud server, if you manually assign an IP address to the NIC, you can specify an IP address that belongs to the subnet but does not belong to the allocation pool.	192.168.0.2-192.168.0.221 192.168.0.225-192.168.0.251
DNS Server Address 1	Specifies the IP address of an associated DNS server. This parameter is optional.	192.168.71.3
DNS Server Address 2	Specifies the IP address of an associated DNS server. This parameter is optional. **NOTE** If the DNS server addresses are left blank, the subnet is not associated with any DNS server. When using only one DNS server address, enter it into **DNS Server Address 1**. To add a DNS server address, click **Add DNS Server Address**.	192.168.72.3
NTP Server Address 1	Specifies the IP address of an associated NTP server. This parameter is optional.	192.168.32.65
NTP Server Address 2	Specifies the IP address of an associated NTP server. This parameter is optional. **NOTE** If the IPv4 & IPv6 dual-stack service is deployed, the NTP server address can be an IPv4 address or an IPv6 address.	192.168.32.66

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Static Route Switch	If this switch is set to **OFF**, static routes will not be configured for cloud servers in the subnet. If this switch is set to **ON**, the configured static routes will be injected to those cloud servers by using the DHCP function of the subnet. • **Destination**: specifies the destination IP address range of the static route. • **Next Hop**: specifies the next-hop IP address of the static route. **NOTE** When you need to add more static routes for cloud servers in a subnet, click **Add Static Route**. You can configure up to five static routes at a time.	• Destination: 10.10.0.0/24 • Next Hop: 192.168.20.2

Table 4-4 Parameters for configuring an IPv6 subnet

Parameter	Description	Example Value
Advanced Settings	You can use the default IPv6 subnet configuration or configure advanced settings. If you enable **Advanced Settings**, you need to configure additional parameters of the IPv6 subnet.	Enabled
Address Mode	Only **dhcpv6-stateful** is available. In this mode, all IP addresses and other stateless configurations (such as DNS and NTP) are managed to implement fine-grained management and allocation of IP addresses.	dhcpv6-stateful
CIDR Block	This parameter is optional. Enter a valid subnet CIDR block, which must be within the displayed available CIDR block. The text format of an IPv6 address is *xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx*. Each *x* is a hexadecimal digit, which represents a 4-bit binary number. Leading zeroes can be omitted during configuration. **NOTE** • If the IPv6 mode is **dhcpv6-stateful**, the prefix length ranges from 64 to 124 bits. • In the displayed available CIDR block, **::** represents a string of consecutive 0 bits. For example, **fc00::** in the available CIDR block **fc00::/32** represents **fc00:0000:0000:0000:0000:0000:0000:0000**. **fc00::/32** starts at address **fc00:0000:0000:0000:0000:0000:0000:0000** and ends at **fc00:0000:ffff:ffff:ffff:ffff:ffff:ffff**.	fc00:0000:00ff:0000:0000:0000:0000:0000/64

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Gateway	Specifies the gateway address of the subnet.	fc00:0000:00ff:0000:0000:0000:0000:0001
Allocation Pools	Specifies the range of IP addresses that can be automatically assigned to NICs if you choose to automatically assign an IP address when creating a cloud server or adding a NIC to a cloud server. This parameter is optional. The IP address range of the allocation pool must be within the subnet CIDR block. To reserve some IP addresses in a subnet so that they will not be automatically assigned to NICs, configure an allocation pool. When configuring the allocation pool, enter an IP address range that does not contain these IP addresses. **NOTE** • If a VPC requires two or more allocation pools, click **Add Allocation Pool**. • When creating a cloud server or adding a NIC to a cloud server, if you manually assign an IP address to the NIC, you can specify an IP address that belongs to the subnet but does not belong to the allocation pool.	fc00:0000:00ff:0000:0000:0000:0001-fc00:0000:00ff:0000:0000:0000:0f30
DNS Server Address 1	Specifies the IP address of an associated DNS server. This parameter is optional.	N/A
DNS Server Address 2	Specifies the IP address of an associated DNS server. This parameter is optional. **NOTE** If the DNS server addresses are left blank, the subnet is not associated with any DNS server. When using only one DNS server address, enter it into **DNS Server Address 1**. To add a DNS server address, click **Add DNS Server Address**.	N/A

Step 7 Check the VPC settings and perform either of the following operations:

- Click **Apply Now** to apply for the VPC.
- Click **Add to Cart** and submit the application later.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.2 Creating a Subnet

Context

This section describes how to create a subnet for a VPC. Cloud servers in this subnet can communicate with each other at Layer 3.

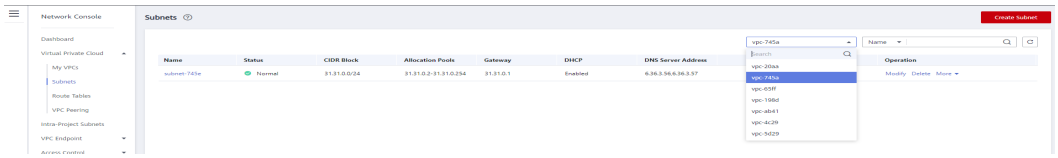
Procedure

Step 1 **Log in to the VPN console as a VDC administrator or a VDC operator.**

Step 2 In the navigation pane under **Network Console**, choose **Virtual Private Cloud** > **Subnets**.

Step 3 In the filter box above the subnet list, locate the VPC for which a subnet is to be created, and click **Create Subnet**.

Figure 4-1 Searching for a VPC



Step 4 In the **Create Subnet** dialog box, set parameters as prompted.

Table 4-5 Parameter description

Parameter	Description	Example Value
VPC	Specifies the name of the VPC to which the subnet belongs.	vpc-9cce
Name	Specifies the name of the subnet. The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Subnet

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
DHCP	Specifies whether to enable DHCP. • If DHCP is enabled for a subnet, when a cloud server in the subnet starts up, the cloud server automatically obtains, through DHCP, the IP address assigned by the system or specified by you when the cloud server is created. • If DHCP is disabled for a subnet, when a cloud server in the subnet starts up, the cloud server cannot automatically obtain the IP address assigned by the system or specified by you when the cloud server is created. In this case, you need to manually assign an IP address to the cloud server. If a cloud server is not assigned an IP address, it cannot communicate with others. You are not advised to disable DHCP. **NOTE** After a subnet is created, the DHCP status for the subnet cannot be changed.	Enabled
Type	If you have deployed the dual stack (IPv4 & IPv6) in the system, you need to select a network type first. If you have deployed only IPv4 in the system, configure the subnet parameters directly by referring to **Table 4-6**. • IPv4 If you select **IPv4**, set the parameters by referring to **Table 4-6**. • IPv4&IPv6 If you select **IPv4&IPv6**, set the parameters by referring to **Table 4-6** and **Table 4-7**.	IPv4

Table 4-6 IPv4 address settings

Parameter	Description	Example Value
CIDR Block	Specifies the IP address range of the subnet.	192.168.0.0/24
Gateway	Specifies the gateway address of the subnet.	192.168.0.1

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Allocation Pools	Specifies the range of IP addresses that can be automatically assigned to NICs if you choose to automatically assign an IP address when creating a cloud server or adding a NIC to a cloud server. This parameter is optional. The IP address range of the allocation pool must be within the subnet CIDR block. To reserve some IP addresses in a subnet so that they will not be automatically assigned to NICs, configure an allocation pool. When configuring the allocation pool, enter an IP address range that does not contain these IP addresses. **NOTE** • If a VPC requires two or more allocation pools, click **Add Allocation Pool**. • When creating a cloud server or adding a NIC to a cloud server, if you manually assign an IP address to the NIC, you can specify an IP address that belongs to the subnet but does not belong to the allocation pool.	192.168.0.2-192.168.0.221 192.168.0.225-192.168.0.251
DNS Server Address 1	Specifies the IP address of an associated DNS server. This parameter is optional.	192.168.71.3
DNS Server Address 2	Specifies the IP address of an associated DNS server. This parameter is optional. **NOTE** If the DNS server addresses are left blank, the subnet is not associated with any DNS server. When using only one DNS server address, enter it into **DNS Server Address 1**. To add a DNS server address, click **Add DNS Server Address**. A maximum of five DNS server addresses can be added. If you run **neutron subnet-update --dns-nameserver**, a message is displayed, indicating that only five DNS server addresses can be added.	192.168.72.3
NTP Server Address 1	Specifies the IP address of an associated NTP server. This parameter is optional.	192.168.32.65
NTP Server Address 2	Specifies the IP address of an associated NTP server. This parameter is optional. **NOTE** An NTP server supports only IPv4 addresses.	192.168.32.66

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Static Route Switch	If this switch is set to **OFF**, static routes will not be configured for cloud servers in the subnet. If this switch is set to **ON**, the configured static routes will be injected to those cloud servers by using the DHCP function of the subnet. • **Destination**: specifies the destination IP address range of the static route. • **Next Hop**: specifies the next-hop IP address of the static route. **NOTE** When you need to add more static routes for cloud servers in a subnet, click **Add Static Route**. You can configure up to five static routes at a time.	• Destination: 10.10.0.0/24 • Next Hop: 192.168.20.2

Table 4-7 IPv6 address settings

Parameter	Description	Example Value
Advanced Settings	You can use the default IPv6 subnet configuration or configure advanced settings. If you enable **Advanced Settings**, you need to configure additional parameters of the IPv6 subnet.	Enabled
Address Mode	Only **dhcpv6-stateful** is available. In this mode, all IP addresses and other stateless configurations (such as DNS and NTP) are managed to implement fine-grained management and allocation of IP addresses.	dhcpv6-stateful

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
CIDR Block	This parameter is optional. Enter a valid subnet CIDR block, which must be within the displayed available CIDR block. The text format of an IPv6 address is *xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx*. Each *x* is a hexadecimal digit, which represents a 4-bit binary number. Leading zeroes can be omitted during configuration. **NOTE** • If the IPv6 mode is **dhcpv6-stateful**, the prefix length ranges from 64 to 124 bits. • In the displayed available CIDR block, **::** represents a string of consecutive 0 bits. For example, **fc00::** in the available CIDR block **fc00::/32** represents **fc00:0000:0000:0000:0000:0000:0000:0000**. **fc00::/32** starts at address **fc00:0000:0000:0000:0000:0000:0000:0000** and ends at **fc00:0000:ffff:ffff:ffff:ffff:ffff:ffff**.	fc00:0000:00ff:0000:0000:0000:0000:0000/64
Gateway	Specifies the gateway address of the subnet.	fc00:0000:00ff:0000:0000:0000:0000:0001
Allocation Pools	Specifies the range of IP addresses that can be automatically assigned to NICs if you choose to automatically assign an IP address when creating a cloud server or adding a NIC to a cloud server. This parameter is optional. The IP address range of the allocation pool must be within the subnet CIDR block. To reserve some IP addresses in a subnet so that they will not be automatically assigned to NICs, configure an allocation pool. When configuring the allocation pool, enter an IP address range that does not contain these IP addresses. **NOTE** • If a VPC requires two or more allocation pools, click **Add Allocation Pool**. • When creating a cloud server or adding a NIC to a cloud server, if you manually assign an IP address to the NIC, you can specify an IP address that belongs to the subnet but does not belong to the allocation pool.	fc00:0000:00ff:0000:0000:0000:0001-fc00:0000:00ff:0000:0000:0000:0f30
DNS Server Address 1	Specifies the IP address of an associated DNS server. This parameter is optional.	N/A

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
DNS Server Address 2	Specifies the IP address of an associated DNS server. This parameter is optional. **NOTE** If the DNS server addresses are left blank, the subnet is not associated with any DNS server. When using only one DNS server address, enter it into **DNS Server Address 1**. To add a DNS server address, click **Add DNS Server Address**. A maximum of five DNS server addresses can be added. If you run **neutron subnet-update --dns-nameserver**, a message is displayed, indicating that only five DNS server addresses can be added.	N/A

Step 5 Click **OK**.

Step 6 Check after the creation.

1. Click the name of the subnet.
2. Click **IP Addresses**, and check whether the IP address for the DHCP service exists.
   - If yes, the creation is successful.
   - If no, the DHCP server is not ready and cannot provide the DHCP service. Contact technical support for assistance.

----End

4.3 Applying for a VPN

By default, ECSs in a VPC cannot communicate with your data center or private network. To enable communication between them, use a VPN.

To use a VPN, you must first create one in your VPC and update the access control rules, including security group rules and network ACL rules.

You can apply for a VPN on the VPN page.

Related operations will be described in this section.

NOTICE

All ECSs in the local subnets of a VPN must be in the private cloud system.

Context

A VPN gateway is an egress gateway in your VPC for establishing an IPsec VPN. It is used to establish a secure, reliable, and encrypted communications channel between your VPC and external data center. A VPN connection is an encrypted

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

communications channel established between the VPN gateway in your VPC and that in an external data center. Currently, only IPsec VPN connections are supported. You must first create a VPN gateway and then a VPN connection. Multiple VPN connections can be created for a VPN gateway.

Prerequisites

- You have created VPN external networks. For details, visit **Operation Help Center** and choose **Operation** > **VDC Tenant Modeling** > **Dividing External Networks** > **Configuring an External Network**.
- You have allocated an external network to the tenant. For details, see **Operation Help Center** > **Operation** > **VDC Tenant Modeling** > **Dividing External Networks (Huawei Cloud Stack Scenario)** > **Allocating Resources** > **Allocating an External Network to a VDC Tenant**.
- You have created a VPC and subnets for network communication with a remote user.
- VPN-QoS has been enabled.

  NOTE

  - If VPN QoS is enabled, the parameters including bandwidth name and bandwidth size are displayed. You need to configure these parameters when creating a VPN gateway.
  - If VPN QoS is disabled, the parameters including bandwidth name and bandwidth size are not displayed. You do not need to configure these parameters when creating a VPN gateway.

Creating a VPN Gateway

Step 1 Log in to ManageOne as a VDC administrator or VDC operator using a browser.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**.

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**.

URL of the unified portal: **https://***Domain name of the ManageOne unified portal*, for example, **https://console.demo.com/moserviceaccesswebsite/unifyportal#/home**. On the homepage, choose **Self-service Cloud Service Center** to go to ManageOne Operation Portal.

You can log in using a password or a USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click  in the upper left corner of the main menu, select a region and resource set, and choose **Network** > **Virtual Private Network**.

Step 3 In the navigation pane on the left, choose **Virtual Private Network** > **VPN Gateway**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 4 On the displayed **VPN Gateway** page, click **Create VPN Gateway** to display the **Create VPN Gateway** page.

Step 5 Set parameters as prompted, and click **Create Now**.

Table 4-8 Parameters for creating a VPN gateway

Parameter	Description	Example Value
Region and Project	The current region and project are displayed by default. To change them, use the selector in the upper left corner of the page.	East region
Name	Specifies the name of the VPN gateway.	vpngw-001
VPC	Specifies the name of the VPC to which the VPN has access. If there are no available VPCs that you want, click **View VPC** to go to the VPC page. Then, click **Apply for VPC** to apply for a VPC.	vpc-001
External Network/ Subnet	Specifies the VPN external networks and subnets. If there are no external networks available, contact the administrator to configure external networks.	vpn_external_network(group1) vpntest2(192.168.30.0/24)
Assignment Mode	Specifies the mode for assigning a local gateway IP address. You can select an assignment mode based on your needs. • **Automatic**: indicates that the system automatically assigns an IP address from the **Allocation Pools**. • **Manual**: indicates that you can assign an IP address from the subnet for the external network.	Manual

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Local Gateway	Specifies the IP address of the local gateway. The IP address is obtained from the subnet selected for **External Network/Subnet** (a VPN gateway parameter). The IP address varies with the value of **Assignment Mode**. • If you select **Automatic** for **Assignment Mode**, the system automatically assigns the local gateway IP address. • If you select **Manual** for **Assignment Mode**, you need to manually configure the local gateway IP address.	192.168.30.2
Bandwidth Name	The bandwidth name can contain only letters, digits, underscores (_), hyphens (-), and dots (.).	bandwidth-ea49
Bandwidth (Mbit/s)	Specifies the bandwidth size (in Mbit/s) of the local VPN gateway. The bandwidth limits only the traffic in the egress direction. When you use a VPN connection, if the network traffic exceeds the VPN connection bandwidth, network congestion occurs and the VPN connection is interrupted. Plan sufficient bandwidth in advance to avoid the VPN connection interruption failure.	5 Mbit/s
Description	Specifies the description of the VPN gateway. This parameter is optional.	N/A

----End

Creating a VPN Connection

Step 1 **Log in to the VPN console as a VDC administrator or a VDC operator.**

Step 2 In the navigation pane on the left, choose **Virtual Private Network** > **VPN Connection**.

Step 3 On the **VPN Connection** page, click **Create VPN Connection**. The **Select Service** dialog box is displayed.

Step 4 Click Apply Now. The **Create VPN Connection** page is displayed.

Step 5 Set parameters as prompted.

Table 4-9, **Table 4-10**, and **Table 4-11** describe the parameters.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-9 Basic information

Parameter	Description	Example Value
Region and Project	The current region is automatically displayed on the page. You can change the region in the upper left corner of the page.	East region
Name	Specifies the VPN connection name.	vpn-001
VPN Gateway	Specifies the VPN gateway used by the VPN connection. If there are no VPN gateways available, click **Create VPN Gateway** to create a VPN gateway.	vpcgw-001
Local Subnet	Specifies the VPC subnets that need to communicate with your data center or private network. **NOTE** You can also add other CIDR blocks.	subnet-da(192.168.0.0/24)
Remote Gateway	Specifies the public IP address of the VPN in your data center or on the private network. This IP address is used for communicating with ECSs or BMSs in a specified VPC.	10.88.88.88
Remote Subnet	Specifies the subnets of your data center or private network for communicating with the VPC. Enter the subnet and mask. If multiple subnets and masks are available, separate them with commas (,). **NOTE** The remote subnet and the local subnet cannot have overlapping CIDR blocks. The remote subnet and the subnet for VPC peering cannot have overlapping CIDR blocks. Example: If VPC1 and VPC2 reside in different regions and they need to communicate with each other using a VPN, VPC1 and VPC2 cannot have any overlapping subnet CIDR block. If they do, you cannot apply for a VPN connection.	192.168.3.0/24,192.168.4.0/24
PSK	Specifies the pre-shared key, which is the password shared by the two ends to set up an IPsec VPN connection. Its value consists of 6 to 128 characters and must not contain spaces or the following characters: < > & ? * ' " PSKs configured at both ends of a VPN connection must be the same.	N/A

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Confirm PSK	Enter the pre-shared key again.	N/A
Required Duration	Specifies the validity period for a VPN.	1 year
Advanced Settings	You can select **Default configuration** or **Custom configuration**. If you select **Custom configuration**, set parameters based on **Table 4-10** and **Table 4-11**.	Default configuration

Table 4-10 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Specifies the hash algorithm for authentication. The value can be: • **SHA2-256**: indicates a one-way hash function designed by NIST. Its hash value is 256 bits long, and its maximum hash value length is close to 264 bits. SHA2-256 uses an internal structure of eight 32-bit words, and is more suitable for 32-bit CPUs. • **SHA2-384**: indicates a one-way hash function designed by NIST. Its hash value is 384 bits long, and its maximum hash value length is close to 2128 bits. • **SHA2-512**: indicates a one-way hash function designed by NIST. Its hash value is 512 bits long, and its maximum hash value length is close to 2128 bits. SHA2-512 is not widely supported by software. **NOTE** VPN supports various algorithms, which provide different levels of security and performance. The higher the security is, the lower the performance is.	SHA2-256

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Encryption Algorithm	Specifies the algorithm for encryption. The value can be: • **AES-128**: The key length is 128 bits, and the number of encryption rounds is 10. • **AES-192**: The key length is 192 bits, and the number of encryption rounds is 14. • **AES-256**: The key length is 256 bits, and the number of encryption rounds is 14. **NOTE** • Advanced Encryption Standard (AES) is a block encryption standard adopted by the U.S. federal government. It is a symmetric encryption algorithm. • Different algorithms provide different levels of security and performance. The higher the security is, the lower the performance is.	AES-128
DH Algorithm	Specifies the Diffie-Hellman key exchange algorithm. The value can be: • **Group2**: indicates the DH group using the 1024-bit MODP algorithm. • **Group5**: indicates the DH group using the 1536-bit MODP algorithm. • **Group14**: indicates the DH group using the 2048-bit MODP algorithm. It is not supported by dynamic VPN. **NOTE** Different algorithms provide different levels of security and performance. The higher the security is, the lower the performance is.	Group5
Version	Specifies the version of the IKE protocol. The value can be: • **v1**: This version will be used only when the peer device does not support v2. • **v2**: This version is an improved version of v1 and is recommended.	v1
Lifecycle (s)	Specifies the lifetime of the security association (SA), in seconds. The SA will be renegotiated if its lifetime expires.	86400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-11 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Specifies the hash algorithm for authentication. The value can be: • **SHA2-256**: indicates a one-way hash function designed by NIST. Its hash value is 256 bits long, and its maximum hash value length is close to 264 bits. SHA2-256 uses an internal structure of eight 32-bit words, and is more suitable for 32-bit CPUs. • **SHA2-384**: indicates a one-way hash function designed by NIST. Its hash value is 384 bits long, and its maximum hash value length is close to 2128 bits. • **SHA2-512**: indicates a one-way hash function designed by NIST. Its hash value is 512 bits long, and its maximum hash value length is close to 2128 bits. SHA2-512 is not widely supported by software. **NOTE** VPN supports various algorithms, which provide different levels of security and performance. The higher the security is, the lower the performance is.	SHA2-256
Encryption Algorithm	Specifies the algorithm for encryption. The value can be: • **AES-128**: The key length is 128 bits, and the number of encryption rounds is 10. • **AES-192**: The key length is 192 bits, and the number of encryption rounds is 14. • **AES-256**: The key length is 256 bits, and the number of encryption rounds is 14. **NOTE** • Advanced Encryption Standard (AES) is a block encryption standard adopted by the U.S. federal government. It is a symmetric encryption algorithm. • Different algorithms provide different levels of security and performance. The higher the security is, the lower the performance is.	AES-128
PFS	Stands for Perfect Forward Secrecy, which is used to configure the IPsec tunnel negotiation. The value can be **Group 2**, **Group 5**, or **Group 14**. **Group 2** and **Group 5** are not recommended due to low security.	Group 14

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Transfer Protocol	Specifies the security protocol used for IPsec to transmit and encapsulate user data. The supported protocols are AH, ESP, and AH-ESP. • AH provides the integrity check function but does not provide the encryption function. • ESP provides both the integrity check function and the encryption function. • AH-ESP provides both the integrity check function and the encryption function, with higher security.	ESP
Lifecycle (s)	Specifies the lifetime of the security association (SA), in seconds. The SA will be renegotiated if its lifetime expires.	3600

NOTE

- The IKE policy specifies the encryption and authentication algorithms to use in the negotiation phase of an IPsec tunnel. The IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to use in the data transmission phase of an IPsec tunnel. These parameters must be the same between the VPN in your VPC and that in your data center. If they are different, the VPN tunnel cannot be set up.
- Due to the symmetry of the tunnel, you also need to configure the IPsec VPN on your router or network ACL in the data center.
- For the protocols supported by VPN connections, see **9.4 What Are the Reference Standards and Protocols for the IPsec VPN?**

Step 6 Check your parameter settings.

- You can click **Add to Cart** and submit the application later.
- You can click **Create Now** to create a VPN connection.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Creation

5.1 Applying for a VPN

By default, ECSs in a VPC cannot communicate with your data center or private network. To enable communication between them, use a VPN.

To use a VPN, you must first create one in your VPC and update the access control rules, including security group rules and network ACL rules.

You can apply for a VPN on the VPN page.

Related operations will be described in this section.

NOTICE

All ECSs in the local subnets of a VPN must be in the private cloud system.

Context

A VPN gateway is an egress gateway in your VPC for establishing an IPsec VPN. It is used to establish a secure, reliable, and encrypted communications channel between your VPC and external data center. A VPN connection is an encrypted communications channel established between the VPN gateway in your VPC and that in an external data center. Currently, only IPsec VPN connections are supported. You must first create a VPN gateway and then a VPN connection. Multiple VPN connections can be created for a VPN gateway.

Prerequisites

- You have created VPN external networks. For details, visit **Operation Help Center** and choose **Operation** > **VDC Tenant Modeling** > **Dividing External Networks** > **Configuring an External Network**.
- You have allocated an external network to the tenant. For details, see **Operation Help Center** > **Operation** > **VDC Tenant Modeling** > **Dividing External Networks (Huawei Cloud Stack Scenario)** > **Allocating Resources** > **Allocating an External Network to a VDC Tenant**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- You have created a VPC and subnets for network communication with a remote user.
- VPN-QoS has been enabled.

  NOTE

  - If VPN QoS is enabled, the parameters including bandwidth name and bandwidth size are displayed. You need to configure these parameters when creating a VPN gateway.
  - If VPN QoS is disabled, the parameters including bandwidth name and bandwidth size are not displayed. You do not need to configure these parameters when creating a VPN gateway.

Creating a VPN Gateway

Step 1 Log in to ManageOne as a VDC administrator or VDC operator using a browser.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**.

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**.

URL of the unified portal: **https://***Domain name of the ManageOne unified portal*, for example, **https://console.demo.com/moserviceaccesswebsite/unifyportal#/home**. On the homepage, choose **Self-service Cloud Service Center** to go to ManageOne Operation Portal.

You can log in using a password or a USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click  in the upper left corner of the main menu, select a region and resource set, and choose **Network** > **Virtual Private Network**.

Step 3 In the navigation pane on the left, choose **Virtual Private Network** > **VPN Gateway**.

Step 4 On the displayed **VPN Gateway** page, click **Create VPN Gateway** to display the **Create VPN Gateway** page.

Step 5 Set parameters as prompted, and click **Create Now**.

Table 5-1 Parameters for creating a VPN gateway

Parameter	Description	Example Value
Region and Project	The current region and project are displayed by default. To change them, use the selector in the upper left corner of the page.	East region

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Name	Specifies the name of the VPN gateway.	vpngw-001
VPC	Specifies the name of the VPC to which the VPN has access. If there are no available VPCs that you want, click **View VPC** to go to the VPC page. Then, click **Apply for VPC** to apply for a VPC.	vpc-001
External Network/ Subnet	Specifies the VPN external networks and subnets. If there are no external networks available, contact the administrator to configure external networks.	vpn_external_network(group1) vpntest2(192.168.30.0/24)
Assignment Mode	Specifies the mode for assigning a local gateway IP address. You can select an assignment mode based on your needs. ● **Automatic**: indicates that the system automatically assigns an IP address from the **Allocation Pools**. ● **Manual**: indicates that you can assign an IP address from the subnet for the external network.	Manual
Local Gateway	Specifies the IP address of the local gateway. The IP address is obtained from the subnet selected for **External Network/Subnet** (a VPN gateway parameter). The IP address varies with the value of **Assignment Mode**. ● If you select **Automatic** for **Assignment Mode**, the system automatically assigns the local gateway IP address. ● If you select **Manual** for **Assignment Mode**, you need to manually configure the local gateway IP address.	192.168.30.2
Bandwidth Name	The bandwidth name can contain only letters, digits, underscores (_), hyphens (-), and dots (.).	bandwidth-ea49

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Bandwidth (Mbit/s)	Specifies the bandwidth size (in Mbit/s) of the local VPN gateway. The bandwidth limits only the traffic in the egress direction. When you use a VPN connection, if the network traffic exceeds the VPN connection bandwidth, network congestion occurs and the VPN connection is interrupted. Plan sufficient bandwidth in advance to avoid the VPN connection interruption failure.	5 Mbit/s
Description	Specifies the description of the VPN gateway. This parameter is optional.	N/A

----End

Creating a VPN Connection

Step 1 **Log in to the VPN console as a VDC administrator or a VDC operator.**

Step 2 In the navigation pane on the left, choose **Virtual Private Network** > **VPN Connection**.

Step 3 On the **VPN Connection** page, click **Create VPN Connection**. The **Select Service** dialog box is displayed.

Step 4 Click Apply Now. The **Create VPN Connection** page is displayed.

Step 5 Set parameters as prompted.

Table 5-2, **Table 5-3**, and **Table 5-4** describe the parameters.

Table 5-2 Basic information

Parameter	Description	Example Value
Region and Project	The current region is automatically displayed on the page. You can change the region in the upper left corner of the page.	East region
Name	Specifies the VPN connection name.	vpn-001
VPN Gateway	Specifies the VPN gateway used by the VPN connection. If there are no VPN gateways available, click **Create VPN Gateway** to create a VPN gateway.	vpcgw-001

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Local Subnet	Specifies the VPC subnets that need to communicate with your data center or private network. **NOTE** You can also add other CIDR blocks.	subnet-da(192.168.0.0/24)
Remote Gateway	Specifies the public IP address of the VPN in your data center or on the private network. This IP address is used for communicating with ECSs or BMSs in a specified VPC.	10.88.88.88
Remote Subnet	Specifies the subnets of your data center or private network for communicating with the VPC. Enter the subnet and mask. If multiple subnets and masks are available, separate them with commas (,). **NOTE** The remote subnet and the local subnet cannot have overlapping CIDR blocks. The remote subnet and the subnet for VPC peering cannot have overlapping CIDR blocks. Example: If VPC1 and VPC2 reside in different regions and they need to communicate with each other using a VPN, VPC1 and VPC2 cannot have any overlapping subnet CIDR block. If they do, you cannot apply for a VPN connection.	192.168.3.0/24,192.168.4.0/24
PSK	Specifies the pre-shared key, which is the password shared by the two ends to set up an IPsec VPN connection. Its value consists of 6 to 128 characters and must not contain spaces or the following characters: < > & ? * ' " PSKs configured at both ends of a VPN connection must be the same.	N/A
Confirm PSK	Enter the pre-shared key again.	N/A
Required Duration	Specifies the validity period for a VPN.	1 year
Advanced Settings	You can select **Default configuration** or **Custom configuration**. If you select **Custom configuration**, set parameters based on **Table 5-3** and **Table 5-4**.	Default configuration

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-3 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Specifies the hash algorithm for authentication. The value can be: • **SHA2-256**: indicates a one-way hash function designed by NIST. Its hash value is 256 bits long, and its maximum hash value length is close to 264 bits. SHA2-256 uses an internal structure of eight 32-bit words, and is more suitable for 32-bit CPUs. • **SHA2-384**: indicates a one-way hash function designed by NIST. Its hash value is 384 bits long, and its maximum hash value length is close to 2128 bits. • **SHA2-512**: indicates a one-way hash function designed by NIST. Its hash value is 512 bits long, and its maximum hash value length is close to 2128 bits. SHA2-512 is not widely supported by software. **NOTE** VPN supports various algorithms, which provide different levels of security and performance. The higher the security is, the lower the performance is.	SHA2-256
Encryption Algorithm	Specifies the algorithm for encryption. The value can be: • **AES-128**: The key length is 128 bits, and the number of encryption rounds is 10. • **AES-192**: The key length is 192 bits, and the number of encryption rounds is 14. • **AES-256**: The key length is 256 bits, and the number of encryption rounds is 14. **NOTE** • Advanced Encryption Standard (AES) is a block encryption standard adopted by the U.S. federal government. It is a symmetric encryption algorithm. • Different algorithms provide different levels of security and performance. The higher the security is, the lower the performance is.	AES-128

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
DH Algorithm	Specifies the Diffie-Hellman key exchange algorithm. The value can be: • **Group2**: indicates the DH group using the 1024-bit MODP algorithm. • **Group5**: indicates the DH group using the 1536-bit MODP algorithm. • **Group14**: indicates the DH group using the 2048-bit MODP algorithm. It is not supported by dynamic VPN. **NOTE** Different algorithms provide different levels of security and performance. The higher the security is, the lower the performance is.	Group5
Version	Specifies the version of the IKE protocol. The value can be: • **v1**: This version will be used only when the peer device does not support v2. • **v2**: This version is an improved version of v1 and is recommended.	v1
Lifecycle (s)	Specifies the lifetime of the security association (SA), in seconds. The SA will be renegotiated if its lifetime expires.	86400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 5-4 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Specifies the hash algorithm for authentication. The value can be: • **SHA2-256**: indicates a one-way hash function designed by NIST. Its hash value is 256 bits long, and its maximum hash value length is close to 264 bits. SHA2-256 uses an internal structure of eight 32-bit words, and is more suitable for 32-bit CPUs. • **SHA2-384**: indicates a one-way hash function designed by NIST. Its hash value is 384 bits long, and its maximum hash value length is close to 2128 bits. • **SHA2-512**: indicates a one-way hash function designed by NIST. Its hash value is 512 bits long, and its maximum hash value length is close to 2128 bits. SHA2-512 is not widely supported by software. **NOTE** VPN supports various algorithms, which provide different levels of security and performance. The higher the security is, the lower the performance is.	SHA2-256
Encryption Algorithm	Specifies the algorithm for encryption. The value can be: • **AES-128**: The key length is 128 bits, and the number of encryption rounds is 10. • **AES-192**: The key length is 192 bits, and the number of encryption rounds is 14. • **AES-256**: The key length is 256 bits, and the number of encryption rounds is 14. **NOTE** • Advanced Encryption Standard (AES) is a block encryption standard adopted by the U.S. federal government. It is a symmetric encryption algorithm. • Different algorithms provide different levels of security and performance. The higher the security is, the lower the performance is.	AES-128
PFS	Stands for Perfect Forward Secrecy, which is used to configure the IPsec tunnel negotiation. The value can be **Group 2**, **Group 5**, or **Group 14**. **Group 2** and **Group 5** are not recommended due to low security.	Group 14

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Transfer Protocol	Specifies the security protocol used for IPsec to transmit and encapsulate user data. The supported protocols are AH, ESP, and AH-ESP. • AH provides the integrity check function but does not provide the encryption function. • ESP provides both the integrity check function and the encryption function. • AH-ESP provides both the integrity check function and the encryption function, with higher security.	ESP
Lifecycle (s)	Specifies the lifetime of the security association (SA), in seconds. The SA will be renegotiated if its lifetime expires.	3600

NOTE

- The IKE policy specifies the encryption and authentication algorithms to use in the negotiation phase of an IPsec tunnel. The IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to use in the data transmission phase of an IPsec tunnel. These parameters must be the same between the VPN in your VPC and that in your data center. If they are different, the VPN tunnel cannot be set up.
- Due to the symmetry of the tunnel, you also need to configure the IPsec VPN on your router or network ACL in the data center.
- For the protocols supported by VPN connections, see **9.4 What Are the Reference Standards and Protocols for the IPsec VPN?**

Step 6 Check your parameter settings.

- You can click **Add to Cart** and submit the application later.
- You can click **Create Now** to create a VPN connection.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 Managing a VPN Gateway

Step 1 **Log in to the VPN console as a VDC administrator or a VDC operator.**

Step 2 In the navigation pane on the left, choose **Virtual Private Network** > **VPN Gateway**.

Manage a VPN gateway by referring to **Table 6-1**.

Table 6-1 Operations

Operation	Procedure
Viewing a VPN gateway	On the **VPN Gateway** page, view a VPN gateway. **NOTE** After HUAWEI CLOUD Stack is upgraded, if you create VPNs without enabling VPN QoS before the upgrade, the names specified for VPN gateways will become blank.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Operation	Procedure
Modifying a VPN gateway	**NOTE** A VPN gateway is an egress gateway in your VPC for establishing an IPsec VPN. It is used to establish a secure, reliable, and encrypted communications channel between your VPC and external data center. You can modify the name and bandwidth size of a VPN gateway as required. ● Modifying the basic information of a VPN gateway 1. On the **VPN Gateway** page, locate the row containing the target VPN gateway, click **Modify Basic Information** in the **Operation** column, and change the name and description as prompted. 2. Click **OK**. ● Changing the bandwidth size of a VPN gateway 1. On the **VPN Gateway** page, locate the row containing the target VPN gateway, click **More** in the **Operation** column, choose **Modify Bandwidth**, and reconfigure the parameters as required. 2. Click **OK**. **NOTE** The modified bandwidth limits only the traffic in the egress direction.
Deleting a VPN gateway	**NOTE** ● You can delete a VPN gateway to release network resources if it is no longer required. ● A VPN gateway cannot be deleted if it is being used by a VPN connection. Delete the VPN connection before deleting the VPN gateway. 1. On the **VPN Gateway** page, locate the row containing the target VPN gateway, click **More** in the **Operation** column, and choose **Delete**. 2. In the displayed dialog box, click **OK**.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7 Managing a VPN Connection

Step 1 **Log in to the VPN console as a VDC administrator or a VDC operator.**

Step 2 In the navigation pane on the left, choose **Virtual Private Network** > **VPN Connection**.

Manage a VPN connection by referring to **Table 7-1**.

Table 7-1 Operations

Operation	Procedure
Viewing a VPN connection	1. On the **VPN Connection** page, view a VPN connection. 2. On the **VPN Connection** page, click **Policy Details** in the **Operation** column to view IKE and IPsec policy details about the VPN connection.
Modifying a VPN connection	**NOTE** • A VPN connection is an encrypted communications channel established between the VPN gateway in your VPC and that in an external data center. You can modify a VPN connection as required. • If the VPN gateway associated with the VPN connection is added as the next hop of a route in the custom route table, modifying the remote subnet of the VPN connection will delete the route from the custom route table and have the route automatically added to the default route table. 1. On the **VPN Connection** page, locate the row containing the target VPN connection, click **Modify**, and reconfigure the parameters as required. 2. Click **OK**.
Deleting a VPN connection	1. On the **VPN Connection** page, locate the row containing the target VPN connection, click **More**, and choose **Delete**. 2. In the displayed dialog box, click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Operation	Procedure
Extending the required duration of a VPN connection	**NOTE** If you want to continue using a VPN connection that has expired, you can extend the required duration of the VPN connection. 1. On the **VPN Connection** page, locate the row containing the target VPN connection, click **More**, and choose **Extend**. 2. Select or specify a required duration, and click **OK**.

----End

8 Best Practice

8.1 Using the IPsec VPN to Enable Communication Between a VPC and One or More Sites

Scenario

The Internet Protocol Security (IPsec) VPN is an encrypted tunneling technology that uses encrypted security services to establish confidential and secure communications tunnels between different networks. In this scenario, the IPsec VPN is used to enable secure and reliable communication between cloud servers in a VPC and one or more data centers.

Configuration Process

Figure 8-1 shows the process for configuring a VPN to enable communication between a VPC and one site. **Figure 8-2** shows the process for configuring multiple VPNs to enable communication between a VPC and multiple sites. The former is similar to the latter. The only difference is that in the latter, you need to apply for multiple VPNs and ensure that the parameter settings of each VPN are identical to the parameter settings of its peer VPN in a data center.

The tunnel has a symmetric structure. Therefore, the IPsec VPN authentication and encryption algorithms configured in the cloud must be the same as the authentication and encryption algorithms configured on the VPN gateway in the data center. Otherwise, the VPN connection cannot be established.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 8-1 Process for configuring a VPN to enable communication between a VPC and one site

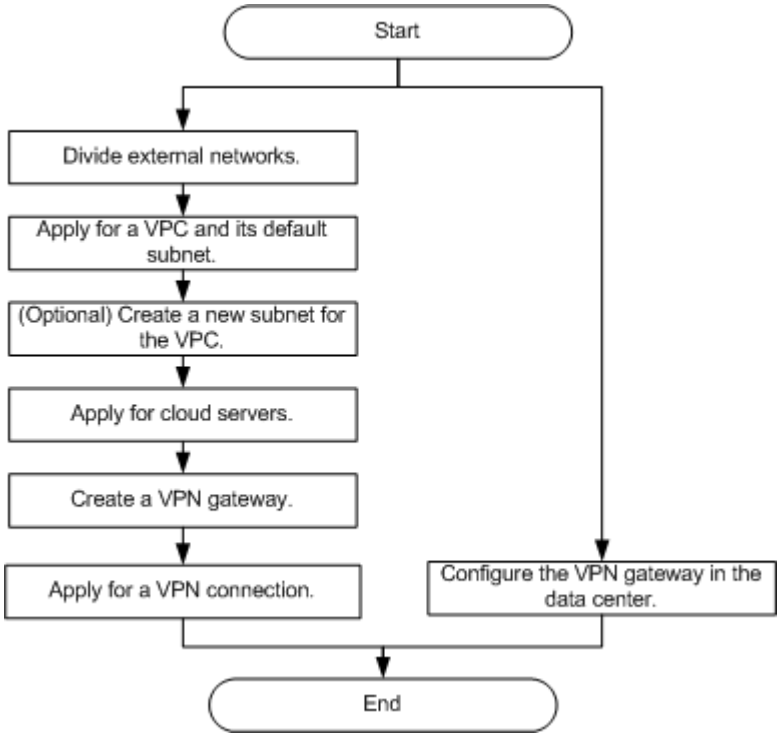
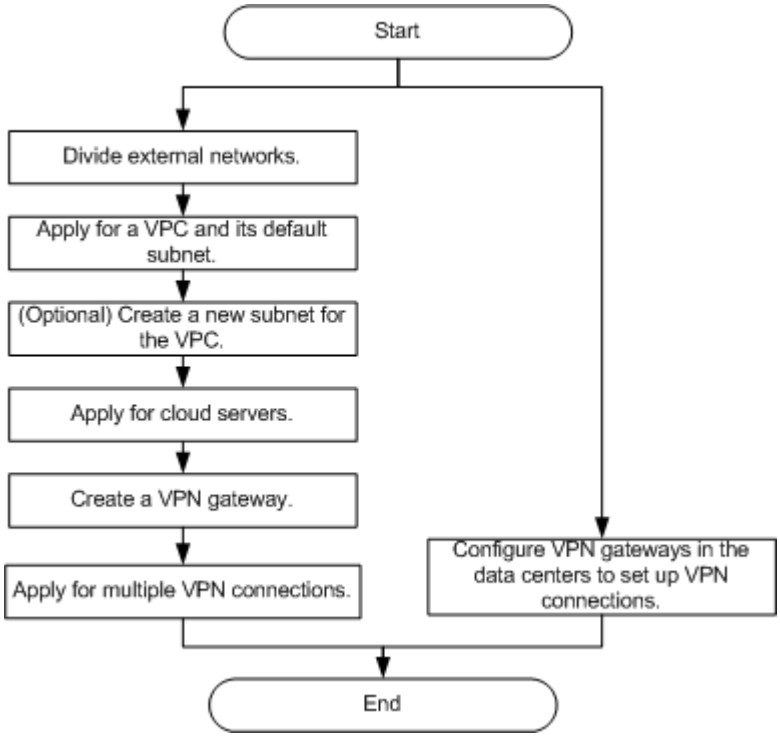


Figure 8-2 Process for configuring multiple VPNs to enable communication between a VPC and multiple sites



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Configuration Operations

Step 1 Divide external networks. Specifically, create and configure external networks.

For details, see **Operation Help Center** > **Operation** > **VDC Tenant Modeling** > **Dividing External Networks (Huawei Cloud Stack Scenario)**.

Step 2 Apply for a VPC and its default subnet.

For details, see "Creation" > "Applying for a VPC" in **Operation Help Center** > **Network** > **Virtual Private Cloud** > **User Guide**.

Step 3 Create a subnet for the VPC.

For details, see "VPC and Subnet" > "Subnet" > "Creating a Subnet" in **Operation Help Center** > **Network** > **Virtual Private Cloud** > **User Guide**.

Step 4 Apply for cloud servers.

For details about how to apply for an ECS, see "Creating an ECS" > "Applying for an ECS" in **Operation Help Center** > **Compute** > **Elastic Cloud Server** > **User Guide**.

For details about how to apply for a BMS, see "Creating a BMS" > "Applying for a BMS" in **Operation Help Center** > **Compute** > **Bare Metal Server** > **User Guide**.

Step 5 Create a VPN gateway.

1. **Log in to the VPN console as a VDC administrator or a VDC operator.**
2. Choose **Virtual Private Network** > **VPN Gateway** and click **Create VPN Gateway**.
3. On the **Create VPN Gateway** page, set parameters as prompted.

Table 8-1 Parameters for creating a VPN gateway

Parameter	Example Value
Region and Project	East region
Name	vpngw-001
VPC	VPC-001
External Network/ Subnet	vpn_external_network(group1) vpntest2(192.168.30.0/24)
Assignment Mode	Manual
Local Gateway	192.168.30.1
Bandwidth Name	bandwidth-ea49
Bandwidth (Mbit/s)	5 Mbit/s
Description	N/A

Step 6 Create a VPN connection.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Connection**, and click **Create VPN Connection**.
2. In the displayed dialog box, click **Apply Now**.
3. On the **Create VPN Connection** page, set parameters as prompted.

   Table 8-2, **Table 8-3**, and **Table 8-4** describe the parameters.

Table 8-2 Basic information

Parameter	Example Value
Region and Project	East region
Name	vpn-001
VPN Gateway	vpcgw-001
Local Subnet	192.168.10.0/24,192.168.2.0/24
Remote Gateway	10.1.1.1
Remote Subnet	10.10.1.0/24
PSK	N/A
Confirm PSK	N/A
Required Duration	One year
Advanced Settings	Customized configuration

Table 8-3 IKE policy

Parameter	Example Value
Authentication Algorithm	SHA2-256
Encryption Algorithm	AES-128
DH Algorithm	Group5
Version	v1
Lifecycle (s)	86400

Table 8-4 IPsec policy

Parameter	Example Value
Authentication Algorithm	SHA2-256
Encryption Algorithm	AES-128
PFS	Group5

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value
Transfer Protocol	ESP
Lifecycle (s)	3600

Step 7 Access servers of the user data center from ECSs to verify the result.

----End

Enabling communication between a VPC and multiple sites

Create multiple VPN connections one after another as described in **Step 5** to **Step 7**.

NOTE

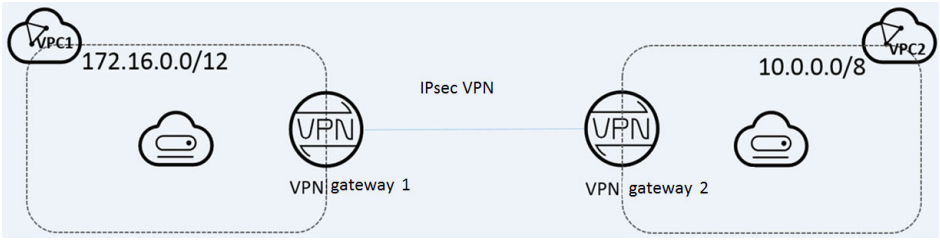
- All VPN connections under the same VPN gateway cannot overlap.
- The CIDR blocks of remote subnets connected to the same VPN cannot overlap.
- The CIDR blocks of local subnets of all VPN connections under the same VPN gateway cannot overlap.

8.2 Using the IPsec VPN to Enable Communication Between Two VPCs in Different Regions

Scenario

To enable communication between two VPCs (for example, VPC1 and VPC2) in different regions, you can set up an IPsec VPN between the two VPCs. **Figure 8-3** shows the user service scenario.

Figure 8-3 User service scenario

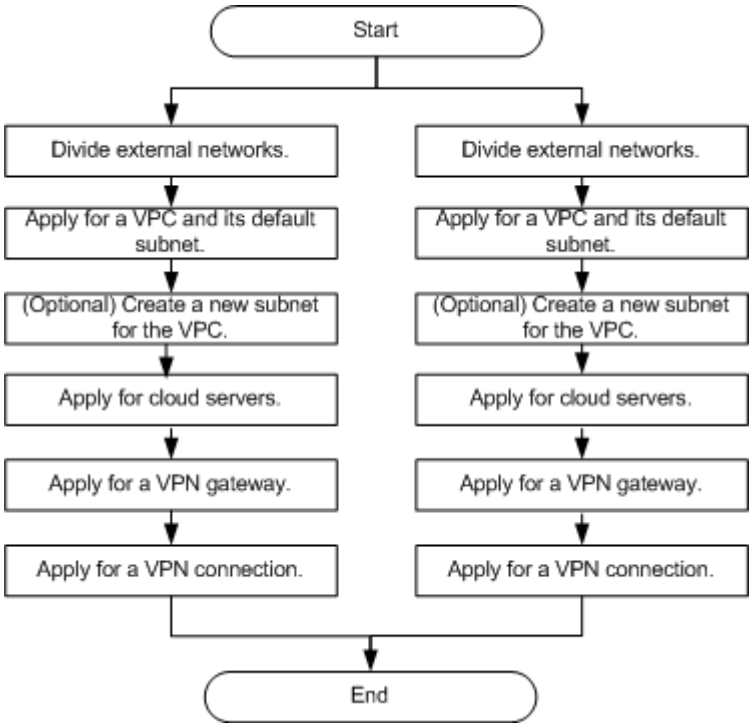


Configuration Process

Figure 8-4 shows the configuration process. The tunnel has a symmetric structure. Therefore, the IPsec VPN authentication and encryption algorithms configured in VPC1 must be the same as those configured in VPC2. Otherwise, the VPN connection cannot be established.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 8-4 Configuration plan



Procedure

Step 1 Divide external networks for VPC1. Specifically, create and configure external networks.

For details, see **Operation Help Center** > **Operation** > **VDC Tenant Modeling** > **Dividing External Networks (Huawei Cloud Stack Scenario)**.

Step 2 Apply for VPC1 and its default subnet.

For details, see "Creation" > "Applying for a VPC" in **Operation Help Center** > **Network** > **Virtual Private Cloud** > **User Guide**.

Step 3 Create a subnet for VPC1.

For details, see "VPC and Subnet" > "Subnet" > "Creating a Subnet" in **Operation Help Center** > **Network** > **Virtual Private Cloud** > **User Guide**.

Step 4 Apply for cloud servers in VPC1.

For details about how to apply for an ECS, see "Creating an ECS" > "Applying for an ECS" in **Operation Help Center** > **Compute** > **Elastic Cloud Server** > **User Guide**.

For details about how to apply for a BMS, see "Creating a BMS" > "Applying for a BMS" in **Operation Help Center** > **Compute** > **Bare Metal Server** > **User Guide**.

Step 5 Create a VPN gateway for VPC1.

1. **Log in to the VPN console as a VDC administrator or a VDC operator.**
2. Choose **Virtual Private Network** > **VPN Gateway** and click **Create VPN Gateway**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3. On the **Create VPN Gateway** page, set parameters as prompted.

Table 8-5 Parameters for configuring VPN gateway 1

Parameter	Example Value
Region and Project	Huadong 1
Name	vpngw-001
VPC	VPC1
External Network/ Subnet	net-001 vpntest2(192.168.30.0/24)
Assignment Mode	Manual
Local Gateway	172.16.**.149
Bandwidth Name	bandwidth-ea49
Bandwidth (Mbit/s)	5 Mbit/s
Description	N/A

Step 6 Create a VPN connection for VPC1.

1. In the navigation pane on the left, choose **Virtual Private Network** > **VPN Connection**, and click **Create VPN Connection**.
2. In the displayed dialog box, click **Apply Now**.
3. On the **Create VPN Connection** page, set parameters as prompted.
   Table 8-6, **Table 8-7**, and **Table 8-8** describe the parameters.

Table 8-6 Basic information

Parameter	Example Value
Region and Project	Huadong 1
Name	vpn-001
VPN Gateway	vpcgw-001
Local Subnet	172.16.0.0/12
Remote Gateway	192.168.**.143
Remote Subnet	10.0.0.0/8
PSK	N/A
Confirm PSK	N/A
Required Duration	One year
Advanced Settings	Customized IKE and IPsec policies

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 8-7 IKE policy

Parameter	Example Value
Authentication Algorithm	SHA2-256
Encryption Algorithm	AES-128
DH Algorithm	Group5
Version	v1
Lifecycle (s)	86400

Table 8-8 IPsec policy

Parameter	Example Value
Authentication Algorithm	SHA2-256
Encryption Algorithm	AES-128
PFS	Group5
Transfer Protocol	ESP
Lifecycle (s)	3600

Step 7 Repeat **Step 1** to **Step 4** to create external networks, VPC2 and its default subnet, (optional) a new subnet for VPC2, and cloud servers in VPC2.

Step 8 Create a VPN gateway for VPC2.

Table 8-9 describes the parameters for configuring VPN gateway 2.

Table 8-9 Parameters for configuring VPN gateway 2

Parameter	Example Value
Region and Project	Huadong 2
Name	vpngw-002
VPC	VPC2
External Network/Subnet	net-002 vpntest2(133.*.*.0/24)
Assignment Mode	Manual
Local Gateway	172.17.**.143
Bandwidth Name	bandwidth-ea49
Bandwidth (Mbit/s)	5 Mbit/s

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value
Description	N/A

Step 9 Create a VPN connection for VPC2.

Table 8-10, **Table 8-11**, and **Table 8-12** describe the parameters for configuring a VPN connection.

Table 8-10 Basic information

Parameter	Example Value
Region and Project	Huadong 2
Name	vpn-002
VPN Gateway	vpcgw-002
Local Subnet	10.0.0.0/8
Remote Gateway	192.168.**.149
Remote Subnet	172.16.0.0/12
PSK	N/A
Confirm PSK	N/A
Required Duration	One year
Advanced Settings	Set parameters as required. For details, see **Table 8-11** and **Table 8-12**.

Table 8-11 IKE policy

Parameter	Example Value
Authentication Algorithm	SHA2-256
Encryption Algorithm	AES-128
DH Algorithm	Group5
Version	v1
Lifecycle (s)	86400

Table 8-12 IPsec policy

Parameter	Example Value
Authentication Algorithm	SHA2-256

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Example Value
Encryption Algorithm	AES-128
PFS	Group5
Transfer Protocol	ESP
Lifecycle (s)	3600

Step 10 Access an ECS in VPC2 from an ECS in VPC1 to test the configuration result.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

9 FAQs

9.1 What Types of VPNs Are Supported?

Currently, the system supports only IPsec VPNs.

9.2 What Are the Differences Between VPN and Direct Connect?

- IPsec VPN uses the public network, IKE protocol, and IPsec protocol to establish an encrypted communication tunnel between a traditional data center and a VPC to connect networks. IPsec VPN can meet most network transmission security requirements. You can purchase, validate, and configure a VPN gateway in a few minutes. The IPsec VPN connection is usually established over the Internet. Therefore, it may be interrupted due to Internet quality issues including Internet jitter or link congestion in peak hours. The IPsec VPN connection is applicable to services that do not require high network connection quality. It is a cost-effective choice for fast deployment.
- Direct Connect provides a dedicated network connection solution for users. A dedicated connection channel is set up to achieve high reliability, high security, and high quality for network connections. Therefore, no data leakage risk exists. Direct Connect is applicable to services that require high network quality and network security, such as those for finance, government, and enterprise. However, to set up a direct connection takes a long time and its cost is relatively high. `

Table 9-1 Performance comparison between VPN and Direct Connect

Item	VPN	Direct Connect
Security	High	Ultra-high
Access channel	Interconnection network, such as the Internet or e-Government extranet	Physical connection of a carrier or internal network of a data center

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Item	VPN	Direct Connect
Price	The price of VPN is less than that of Direct Connect.	
Bandwidth	Determined by public network.	Determined by the connection capability of Direct Connect itself.
Latency	In common scenarios, the latency of VPN is greater than that of Direct Connect.	
Time required to provision the service	Takes effect immediately.	Determined by the construction progress of the carrier.

9.3 Does the IPsec VPN Support Automatic Negotiation?

The IPsec VPN tunnel works in passive mode, which triggers automatic negotiation only when traffic sent by the local end passes through the tunnel.

9.4 What Are the Reference Standards and Protocols for the IPsec VPN?

The following standards and protocols are associated with the IPsec VPN:

- RFC 4301: Security Architecture for the Internet Protocol
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and its use with IPsec
- RFC 3625: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3748: Extensible Authentication Protocol (EAP)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- 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)

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- RFC 4322: Opportunistic Encryption using the Internet Key Exchange (IKE)
- RFC 4359: The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4478: Repeated Authentication in Internet Key Exchange (IKEv2)
- RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2)

9.5 What Do I Do If VPN Connection Setup Fails?

1. Check whether the parameters listed in **Table 9-2**, **Table 9-3**, and **Table 9-4** are consistent between the cloud VPN and the peer VPN.

Table 9-2 Basic parameters

Parameter	Description	Example Value
PSK	Specifies the pre-shared key. The value can contain 6 to 128 characters PSKs set at both ends of a VPN connection must be the same.	N/A

Table 9-3 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Specifies the hash authentication algorithm. The supported algorithms are SHA2-256, SHA2-384, SHA2-512.	SHA2-256
Encryption Algorithm	Specifies the encryption algorithm. The supported algorithms are AES-128, AES-192, AES-256.	AES-128
DH Algorithm	Specifies the Diffie-Hellman key exchange algorithm. The value can be **group2**, **group5**, or **group14**.	Group5
Version	Specifies the version of the IKE protocol. The value can be **v1** or **v2**.	v1
Lifecycle (s)	Specifies the lifetime of the security association (SA), in seconds. The SA will be renegotiated if its lifetime expires.	86400

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 9-4 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Specifies the hash authentication algorithm. The supported algorithms are SHA2-256, SHA2-384, SHA2-512.	SHA2-256
Encryption Algorithm	Specifies the encryption algorithm. The supported algorithms are AES-128, AES-192, AES-256.	AES-128
PFS	Stands for Perfect Forward Secrecy, which is used to configure the IPsec tunnel negotiation.	Group5
Transfer Protocol	Specifies the security protocol used for IPsec to transmit and encapsulate user data. The supported protocols are AH, ESP, and AH-ESP.	ESP
Lifecycle (s)	Specifies the lifetime of the security association (SA), in seconds. The SA will be renegotiated if its lifetime expires.	3600

2. Check whether the ACL configurations are correct.

If the subnets of your 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, set the ACL rules for each data center subnet to permit the 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
```

9.6 How Can I Handle the Failure in Accessing the ECSs from My Data Center or LAN Even If the VPN Connection Has Been Set Up?

The security group denies the access from all sources by default. If you want to access your ECSs, modify the security group configuration and allow the access from the peer subnets. For details, see "Security Group" in **Operation Help Center** > **Network** > **Virtual Private Cloud** > **User Guide**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

9.7 What Do I Do If I Cannot Access My Data Center or LAN from the ECSs After a VPN Connection Has Been Set Up?

Check whether you have properly configured the firewall policies for the access from the public IP address of the cloud VPN to the public IP address of your data center or LAN. No policies are configured to limit the access by default.

9.8 Does a VPN Allow for Communication Between Two VPCs?

Two VPCs in the same region cannot be connected using a VPN. In this case, they can be connected using a VPC peering connection. Two VPCs in different regions can be connected using a VPN.

9.9 What Is the Limitation on the Number of Local and Remote Subnets of a VPN?

The product of the number of local subnets and that of remote subnets cannot exceed 255.

9.10 How Long Is Required for Issued VPN Configurations to Take Effect?

The time required for VPN configurations to take effect increases linearly with the number obtained by multiplying the number of local subnets and that of remote subnets.

9.11 How Do I Log In to the VPN Console as a VDC Administrator or VDC Operator?

Step 1 Log in to ManageOne as a VDC administrator or VDC operator using a browser.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**.

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**.

URL of the unified portal: **https://***Domain name of the ManageOne unified portal*, for example, **https://console.demo.com/moserviceaccesswebsite/unifyportal#/home**. On the homepage, choose **Self-service Cloud Service Center** to go to ManageOne Operation Portal.

You can log in using a password or a USB key.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click  in the upper left corner of the main menu, select a region and resource set, and choose **Network** > **Virtual Private Network**.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.