Virtual Private Cloud

Service Overview

Issue 1

Date 2022-09-30

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Security Declaration

Vulnerability

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

Contents

1 What Is Virtual Private Cloud?

VPC Overview

Virtual Private Cloud (VPC) allows you to provision logically isolated virtual private networks for cloud resources, such as cloud servers, containers, and databases. You can create subnets, security groups, network ACLs, route tables, and more to manage cloud resources flexibly. You can also use EIPs to connect cloud resources in VPCs to the Internet, and use Direct Connect and VPN to connect on-premises data centers to VPCs to build a hybrid cloud network.

The VPC service uses network virtualization technologies, such as link redundancy, distributed gateway clusters, and multi-AZ deployment, to ensure network security, stability, and availability.

Product Architecture

The following describes the basics, security, connectivity, and O&M of VPCs.

Figure 1-1 VPC architecture

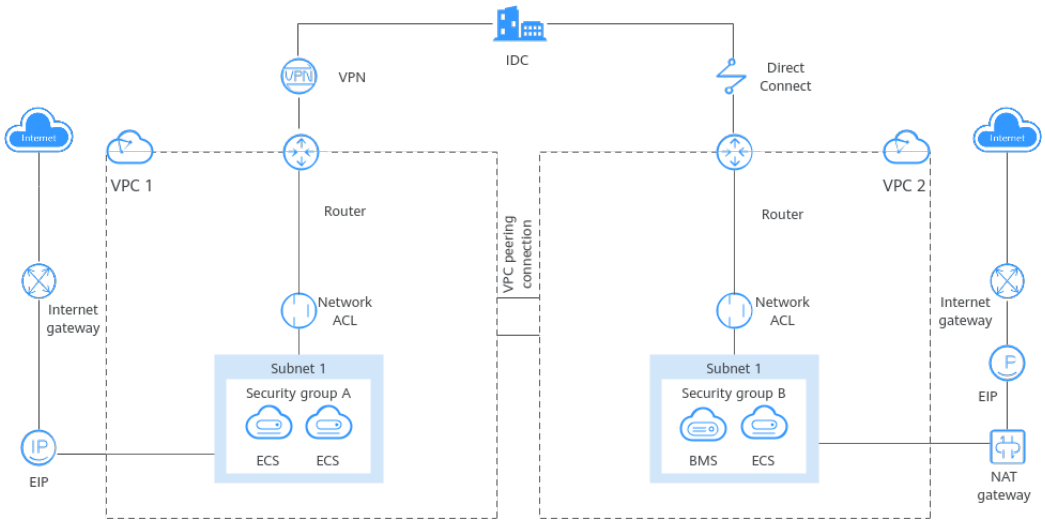


Table 1-1 Architecture description

Item	Brief	Details
VPC basics	A VPC is a logically isolated virtual private network. You can define a CIDR block for each VPC and add one or more subnets. You can also configure route tables to control where the traffic from your subnet is directed. VPCs are logically isolated from each other, but subnets in a VPC can communicate with each other by default.	• IPv4 CIDR block: When creating a VPC, you need to specify an IPv4 CIDR block for it. Supported IPv4 CIDR blocks are 10.0.0.0/8-24, 172.16.0.0/12-24, and 192.168.0.0/16-24. • Subnet: You can divide a VPC into one or more subnets as required to deploy your instances (such as cloud servers, containers, and databases). Private IP addresses are then assigned to your instances from the subnets where they are running. For more information, see **Subnet**. • Route table: Each VPC comes with a default route table that allows communications between subnets in a VPC. You can add routes to the default route table or create a route table to control traffic. For details, see **Route Tables and Routes**.
VPC security	Security groups and network ACLs protect the cloud resources deployed in a VPC.	• Security groups protect instances. You can add inbound and outbound rule to protect all the resources in a security group. For details about security groups, see **Security Groups and Security Group Rules**. • Network ACLs protect associated subnets. You can add inbound and outbound rule to protect all the resources in a subnet. For details, see **Network ACL Overview**. Network ACLs protect subnets, while security groups protect instances in a subnet. If both security group and network ACL rules are configured, traffic matches network ACL rules first and then security group rules. For details, see **What Is Access Control?**

Item	Brief	Details
VPC connectivity	You can combine VPC and other networking services to build networks to meet different requirements. • Use VPC peering connections or an enterprise router to connect different VPCs in the same region. • Use an EIP or NAT gateway to allow the instances in a VPC to the Internet. • Use Direct Connect or VPN to connect an on-premises data center to VPCs.	• Connecting VPCs in the same region – VPC peering connections: connect VPCs in a region in the same account or different accounts. For details, see **VPC Peering Connection Overview**. – Enterprise routers: connect multiple VPCs in the same region, as a high-performance centralized router. For details, see **What Is an Enterprise Router?** VPC peering connections are free of charge, while enterprise routers are not free. Compared with VPC peering connections, enterprise routers simplify the network structure and make it easy for scale-out and O&M. • Connecting a VPC to the Internet – EIPs: enable your cloud resources to communicate with the Internet. For details, see – Public NAT gateways: enables instances (such as ECSs or BMSs) in a VPC to share an EIP to communicate with the Internet. A public NAT gateway supports up to 20 Gbit/s of bandwidth. For details, see • Connecting an on-premises data center to a VPC – Direct Connect: allows you to establish a stable, high-speed, low-latency, secure, and dedicated network connection that connects your on-premises data center to the cloud. Direct Connect helps you build a flexible, scalable hybrid cloud computing environment. For details, see **What Is Direct Connect?**

Item	Brief	Details
		– VPN: establishes a secure, encrypted communication tunnel between your on-premises data center and your VPC. For details, see **What Is Virtual Private Network?** Compared with Direct Connect, VPN is cost-effective and can be quickly deployed.

Accessing the VPC Service

You can access the VPC service through the management console or using HTTPS-based APIs.

- Management console

  You can use the console to directly perform operations on VPC resources. To access the VPC service, log in to the management console**management console** and select **Virtual Private Cloud** from the console homepage.

- API

  If you need to integrate a VPC into a third-party system for secondary development, you can use APIs to access the VPC service. For details, see the **Virtual Private Cloud API Reference**.

2 Product Advantages

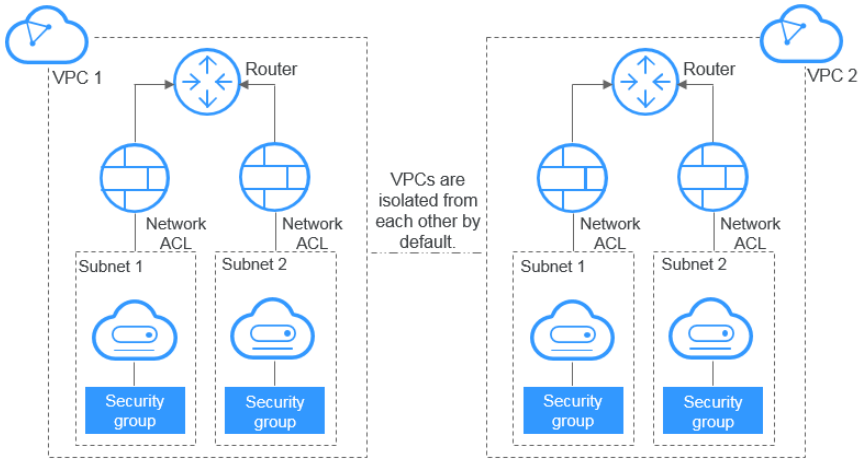
Flexible Configuration

You can create VPCs, add subnets, specify IP address ranges, configure DHCP, and set route tables. You can configure the same VPC for ECSs that are in different availability zones (AZs).

Secure and Reliable

VPCs are logically isolated through tunneling technologies. By default, different VPCs cannot communicate with each other. You can use network ACLs to protect subnets and use security groups to protect ECSs. They add additional layers of security to your VPCs, so your network is secure.

Figure 2-1 Secure and reliable



Seamless Interconnectivity

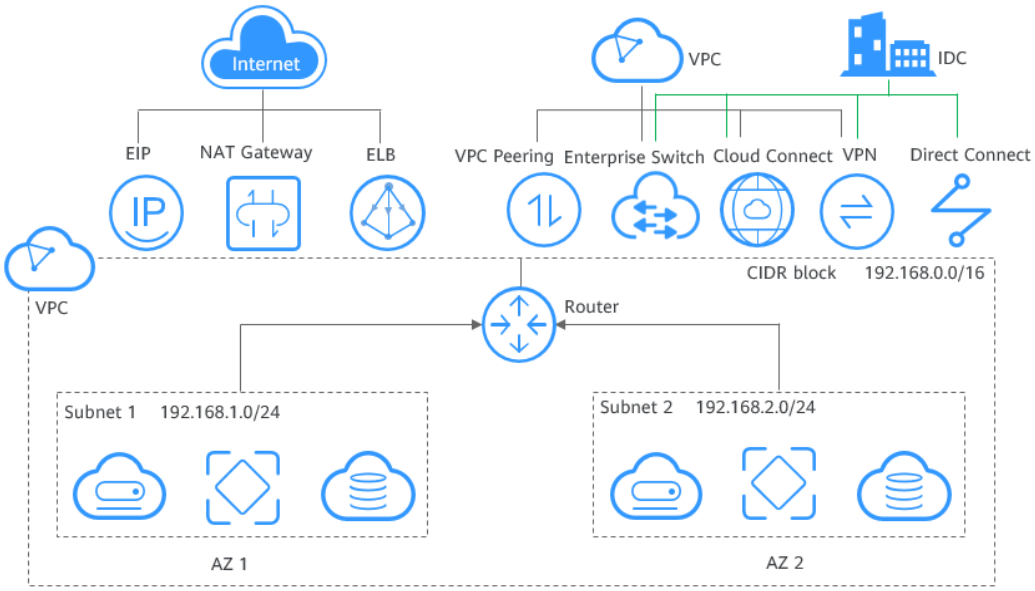
By default, instances in a VPC cannot access the Internet. You can use EIPs, NAT gateways, Direct Connect connections, VPN connections, and load balancers to enable access to or from the Internet.

By default, instances in different VPCs cannot communicate with each other. You can create a VPC peering connection to enable the instances in the two VPCs in the same region to communicate with each other using private IP addresses.

You can use a Layer 2 connection gateway (L2CG) provided by our Enterprise Switch service to establish network communication between the cloud and on-premises networks, and migrate data center or private cloud services to the cloud without changing subnets.

Multiple connectivity options are available to meet diverse service requirements for the cloud, enabling you to deploy enterprise applications with ease and lower enterprise IT operation and maintenance (O&M) costs.

Figure 2-2 Interconnectivity



High-Speed Access

Dynamic BGP is used to provide access to various carrier networks. You can establish over 20 dynamic BGP connections to different carriers. Dynamic BGP connections enable real-time failovers based on preset routing protocols, ensuring high network stability, low network latency, and smooth access to services on the cloud.

Advantage Comparison

Table 2-1 lists the advantages of a VPC over a traditional IDC.

Table 2-1 Comparison between a VPC and a traditional IDC

Item	VPC	Traditional IDC
Deployment cycle	• You do not need to perform complex engineering deployment, including engineering planning and cabling. • You can determine your networks, subnets, and routes on Huawei Cloud based on service requirements.	You need to set up networks and perform tests. The entire process takes a long time and requires professional technical support.
Total cost	Huawei Cloud provides flexible billing modes for network services. You can select whichever one best fits your business needs. There are no upfront costs and network O&M costs, reducing the total cost of ownership (TCO).	You need to invest heavily in equipment rooms, power supply, construction, and hardware materials. You also need professional O&M teams to ensure network security. Asset management costs increase with any change in business requirements.
Flexibility	Huawei Cloud provides a variety of network services for you to choose from. If you need more network resources (for instance, if you need more bandwidth), you can expand resources on the fly.	You have to strictly comply with the network plan to complete the service deployment. If there are changes in your service requirements, it is difficult to dynamically adjust the network.
Security	VPCs are logically isolated from each other. You can use security features such as network ACLs and security groups, and even security services like Advanced Anti-DDoS (AAD) to protect your cloud resources.	The network is insecure and difficult to maintain. You need professional technical personnel to ensure network security.

3 Application Scenarios

Dedicated Networks on Cloud

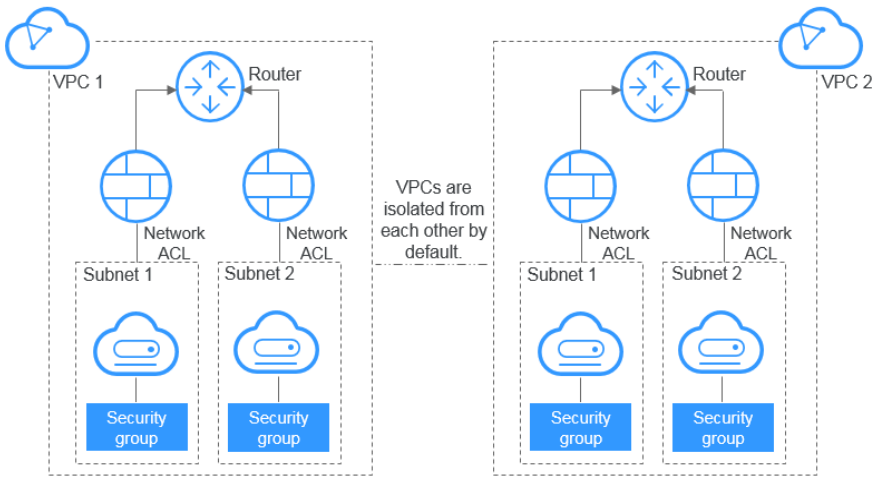
Scenario

Each VPC represents a private network and is logically isolated from other VPCs. You can deploy your service system in a VPC so it will have a private network environment on Huawei Cloud. If you have multiple service systems, for example, a production system and a test system, you can deploy them in two different VPCs to keep them isolated. If you want to establish communication between these two VPCs, you can create a VPC peering connection to link them.

Related Services

ECS

Figure 3-1 Dedicated networks on cloud



Web Application or Website Hosting

Scenario

You can host web applications and websites in a VPC and use the VPC as a regular network. With EIPs or NAT gateways, you can connect ECSs running your web

applications to the Internet. You can use load balancers to evenly distribute traffic across multiple ECSs.

Cloud resources in a VPC can use the following cloud services to connect to the Internet.

Table 3-1 Accessing the Internet

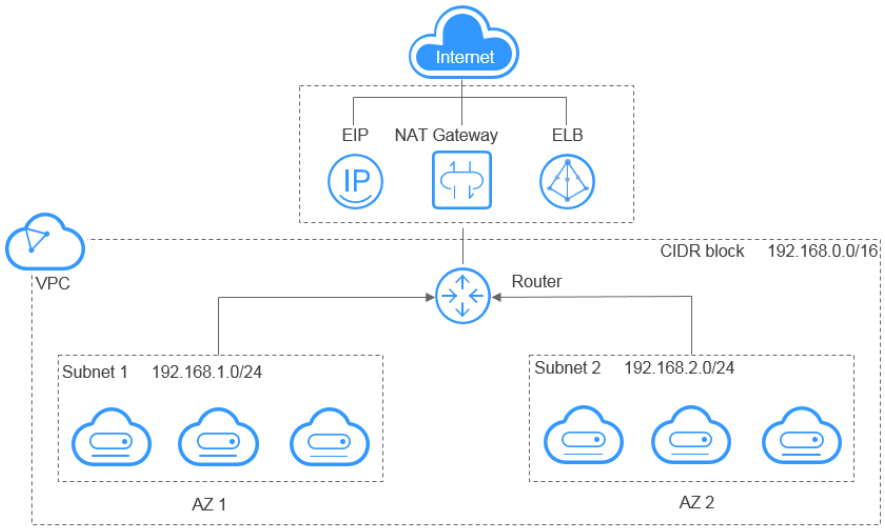
Cloud Service	Application Scenario	Description	Related Operations
EIP	Single ECS accesses the Internet.	You can assign an EIP and bind it to an ECS so that the ECS can access the Internet or provide services accessible from the Internet. You can unbind the EIP from the ECS to disable access at any time. You can use shared bandwidth and shared data packages to streamline costs.	**Elastic IP**
NAT Gateway	Multiple ECSs share an EIP to access the Internet.	A NAT gateway offers both source network address translation (SNAT) and destination network address translation (DNAT). SNAT allows multiple ECSs in the same VPC to share EIPs to access the Internet. In this way, you can reduce management costs and prevent the EIPs of ECSs from being exposed to the Internet. DNAT uses port-level data forwarding. It maps EIP ports to ECS ports so that the ECSs in a VPC can share the same EIP and bandwidth to provide Internet-accessible services. However, DNAT does not balance traffic.	**Using SNAT to Access the Internet** **Using DNAT to Provide Services Accessible from the Internet**

Cloud Service	Application Scenario	Description	Related Operations
ELB	Evenly distribute incoming traffic across multiple ECSs in high-concurrency scenarios, such as e-commerce.	Load balancers evenly distribute traffic across multiple backend ECSs (at Layer 4 or Layer 7). You can bind EIPs to ECSs to allow access from the Internet. ELB expands the capabilities and improves availability of your applications by eliminating single points of failures.	What Is Elastic Load Balance?

Related Services

ECS, EIP, NAT Gateway, and ELB

Figure 3-2 Web application or website hosting



Web Application Access Control

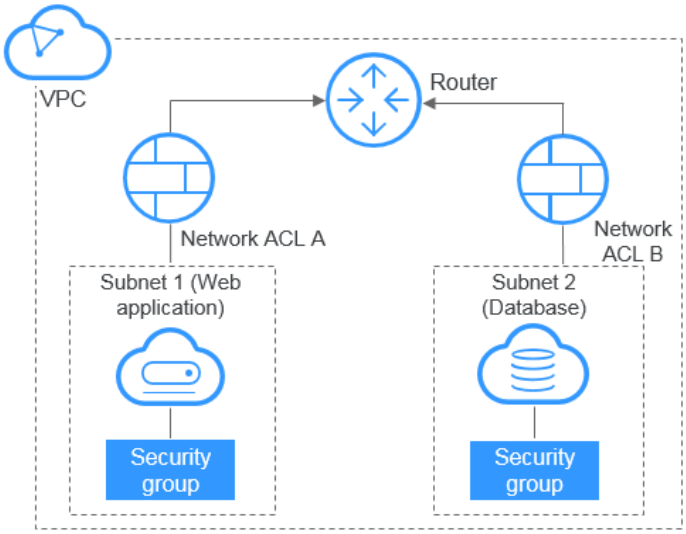
Scenario

You can create a VPC and security groups to host multi-tier web applications in different security zones. You can associate web servers and database servers with different security groups and configure different access control rules for security groups. You can launch web servers in a publicly accessible subnet. But then, to ensure security, you can run database servers in subnets that are not publicly accessible.

Related Services

ECS

Figure 3-3 Web application access control



VPC Connectivity Options

Scenario

You can use the following cloud services to allow two VPCs to communicate with each other.

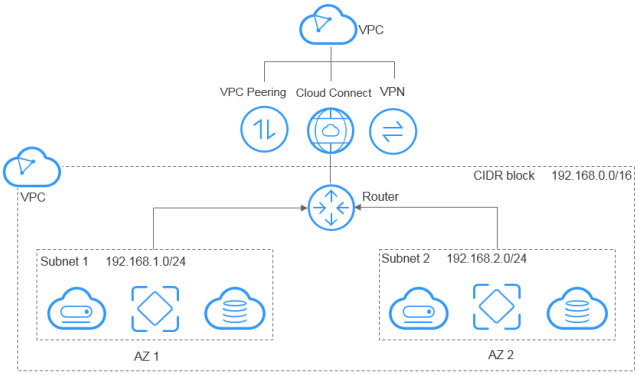
Table 3-2 Connecting VPCs

Cloud Service	Application Scenario	Description	Related Operations
VPC Peering	Connect VPCs in the same region.	You can request a VPC peering connection with another VPC in your account or in another account, but the two VPCs must be in the same region. VPC peering connections are free.	**Creating a VPC Peering Connection with Another VPC in Your Account** **Creating a VPC Peering Connection with a VPC in Another Account**
VPN	Use VPN to connect VPCs across regions at a low cost.	VPN uses an encrypted communications tunnel to connect VPCs in different regions and sends traffic over the Internet. It is inexpensive, easy to configure, and easy to use. However, the quality of VPN connections depends on the quality of your Internet connections.	-

Related Services

ECS, Cloud Connect, and VPN

Figure 3-4 VPC connectivity options



Hybrid Cloud Deployment

Scenario

If you have an on-premises data center and you do not want to migrate all of your services to the cloud, you can build a hybrid cloud, which will let you keep core data in your data center.

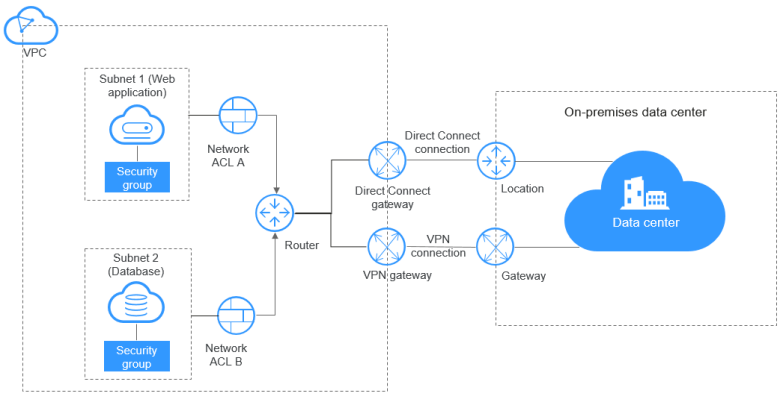
Table 3-3 Connecting to an on-premises data center

Cloud Service	Application Scenario	Description	Related Operations
VPN	Use VPN to connect a VPC to an on-premises data center at a low cost.	VPN uses an encrypted communications tunnel to connect a VPC on the cloud to an on-premises data center and sends traffic over the Internet. It is inexpensive, easy to configure, and easy to use. However, the quality of VPN connections depends on the quality of your Internet connections.	-
Direct Connect	Use a physical connection to connect a VPC to an on-premises data center.	Direct Connect provides physical connections between VPCs and data centers. It features low latency and is very secure. Direct Connect is a good choice if you have strict requirements on network transmission quality.	**Accessing Multiple VPCs Using a Connection**

Related Services

ECS, Cloud Connect, Direct Connect, and VPN

Figure 3-5 Hybrid cloud deployment



4 Functions

Table 4-1 lists common VPC functions.

Before using the VPC service, you should be familiar with the basic concepts, such as subnets, route tables, security groups, and EIPs. This will make it easier to understand VPC functions.

Table 4-1 Common VPC functions

Category	Function	Description
VPC and Subnet	VPC	A VPC provides an isolated virtual network for your cloud resources. You can flexibly configure and manage the network. You can create VPCs, modify basic information about VPCs, delete VPCs, and export the VPC list. For details, see **Creating a VPC**.
	Subnet	A subnet is a unique CIDR block with a range of IP addresses in your VPC. All resources in a VPC must be deployed on subnets. You can create subnets, modify subnet information, and delete subnets. For details, see **Creating a VPC**.
	Route Table	A route table contains routes, which determine where traffic is directed. When you create a VPC, the system automatically creates a default route table. The route table ensures that all subnets in the VPC can communicate with each other. You can also add custom routes to control where traffic is directed. You can add, query, modify, and delete routes. For details, see **Route Table Overview**.

Category	Function	Description
	Virtual IP Address	A virtual IP address can be shared among multiple ECSs. You can configure both private and virtual IP addresses for an ECS, and you can access the ECS through either IP address. A virtual IP address has the same network access capability as a private IP address. If you require high availability, you can use virtual IP addresses because they support active/standby ECS switchover. You can assign and release virtual IP addresses, bind a virtual IP address to an EIP or ECS, and access a virtual IP address through an EIP, a VPN, Direct Connect, or VPC peering connection. For details, see **Virtual IP Address Overview**.
	IPv4 and IPv6 Dual-Stack Network	IPv4 and IPv6 dual stack allows your resources to use both the IPv4 and IPv6 addresses for private and public network communication. You can create an IPv4/IPv6 dual-stack network or add an IPv6 subnet to a VPC to form a dual-stack network. For details, see **IPv4 and IPv6 Dual-Stack Network**.
Access Control	Security Group	A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted within a VPC. You can create a security group and define different access rules to protect the ECSs that it contains. You can create and delete security groups, add, replicate, modify, delete, import or export security group rules, view the security group of an ECS, change the security group of an ECS, and add cloud resources to or remove them from a security group. For details, see **Security Group Overview**.
	Network ACL	A network ACL is an optional layer of security for your subnets. You can associate one or more subnets with a network ACL to control traffic in and out of the subnets. You can create, view, modify, delete, enable, disable network ACLs, associate subnets with or disassociate them from network ACLs, and add, modify, change the sequence of, enable, disable, and delete network ACL rules. For details, see **Network ACL Overview**.

Category	Function	Description
EIP and Bandwidth	EIP	The Elastic IP (EIP) service enables you to use static public IP addresses and scalable bandwidths to connect your cloud resources to the Internet. You can assign EIPs, bind EIPs to cloud resources, unbind EIPs from cloud resources, release EIPs, modify EIP bandwidth, and upgrade static BGP to dynamic BGP. For details, see **EIP Overview**.
	Shared bandwidth	Shared bandwidth allows multiple EIPs to share the same bandwidth. All ECSs, BMSs, and load balancers that have EIPs bound in the same region can share a bandwidth. You can assign, modify, delete a shared bandwidth, add EIPs to a shared bandwidth, and remove EIPs from a shared bandwidth. For details, see **Shared Bandwidth Overview**.
Resource Interconnection	VPC Peering Connection	A VPC peering connection is a network connection between two VPCs. A VPC peering connection allows two VPCs communicate with each other using private IP addresses as if they were in the same VPC. You can create a VPC peering connection between your own VPCs, or between your VPC and a VPC of another account within the same region. However, you cannot create a VPC peering connection between VPCs in different regions. You can create a VPC peering connection with another VPC in your account or with a VPC in another account. You can also view, modify, and delete VPC peering connections. For details, see **VPC Peering Connection Overview**.
Monitoring	Viewing Metrics	You can view the bandwidth and EIP usage of the VPC service through Cloud Eye, create and set alarm rules, and customize the monitored objects and notification policies without adding plug-ins. For details, see **Supported Metrics**.
Auditing	Viewing Audit Logs	With CTS, you can record operations performed on the VPC service for further query, audit, and backtracking purposes. You can view and export operation records of the last seven days on the CTS console.

Category	Function	Description
Tag	Tag Management	Tags help you identify and manage cloud resources. You can manage VPC tags, subnet tags, and tags.
Permissions	Permissions Management	You can use Identity and Access Management (IAM) to implement fine-grained permissions management for your VPCs, allowing enterprises to set different access permissions based on organizations and responsibilities. You can create an IAM user, grant permissions to the user, and create custom VPC policies.

5 Notes and Constraints

Table 5-1 lists the quotas about VPC resources. Some default quotas can be increased.

You can log in to the console to view default quotas. For details, see **How Do I View My Quotas?**

Table 5-1 VPC resource quotas

Resource	Adjustable
Maximum number of VPCs per region	Yes
Maximum number of subnets per region	Yes
Maximum number of security groups per region	Yes
Maximum number of security group rules per region	Yes
Maximum number of per region	Yes
Maximum number of route tables that can be associated with a VPC in a region	Yes
Maximum number of routes per route table in a region	No
Maximum number of VPC peering connections per region	No
Maximum number of VPC flow logs per region	No

6 VPC and Other Services

Figure 6-1 shows the relationship between VPC and other services.

Figure 6-1 VPC and other services

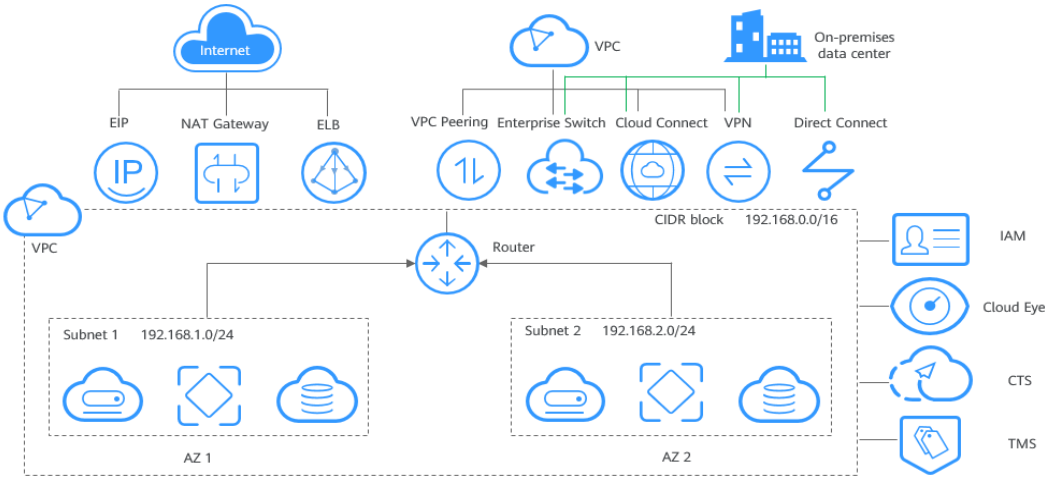


Table 6-1 Related services

Interactive Function	Service	Reference
Secure networks for ECSs.	Elastic Cloud Server (ECS)	Adding a Security Group Rule
Connect ECSs in a VPC to the Internet.	Elastic IP (EIP)	Connecting ECSs in a VPC to the Internet Using EIPs
	NAT Gateway	Using SNAT to Access the Internet
Connect a VPC to a local data center.	Virtual Private Network (VPN)	Virtual Private Network

Interactive Function	Service	Reference
	Direct Connect	**Direct Connect**
Distribute incoming traffic to multiple ECSs in a VPC.	Elastic Load Balance (ELB)	**Elastic Load Balance**
Assign different permissions to employees in your enterprise to access your VPC resources.	Identity and Access Management (IAM)	**Identity and Access Management**
Check the bandwidth and traffic usage.	Cloud Eye	**Viewing Metrics**
Record VPC-related operations for later query, audit, and backtracking.	Cloud Trace Service (CTS)	**Viewing Audit Logs**
Tags identify VPC resources for purposes of easy categorization and quick search.	Tag Management Service (TMS)	**Managing EIP Tags**

7 Billing

VPC provides a wide range of cloud resources. Some are free, while some are not. **Table 7-1** describes how these resources are billed.

Table 7-1 VPC resource billing

Resource	Billing Description
VPC	Free
Subnet	Free
Route table	Free
VPC peering connection	Free
Elastic network interface	Free
Supplementary network interface	Free
Security group	Free
Network ACL	Free
VPC flow log	Free

Resource	Billing Description
EIP and bandwidth	If you use EIPs and bandwidths, you need to pay for their prices. • EIP reservation price If your pay-per-use EIP has no instance bound, you will be billed for the EIP reservation price. • Fixed bandwidth: – EIP bandwidth prices: bandwidth prices of yearly/monthly EIPs and pay-per-use EIPs (by bandwidth); traffic price of pay-per-use EIPs (by traffic) – Shared bandwidth price For details, see **EIP Billing**.
VPC endpoint	If you use VPC endpoints, you need to pay for them. For details, see **VPC Endpoint Billing**.

NOTE

Currently, free resources are not billed. You will be notified in advance if the billing starts.

8 Permissions

If you need to assign different permissions to personnel in your enterprise to access your VPCs, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you to securely access your Huawei Cloud resources.

With IAM, you can create IAM users, and assign permissions to control their access to specific resources. For example, if you want some software developers in your enterprise to use VPCs but do not want them to delete VPCs or perform any other high-risk operations, you can grant permissions to use VPCs but not permissions to delete them.

If your HUAWEI ID does not require IAM for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information, see **IAM Service Overview**.

VPC 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.

VPC 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 VPCs in the selected projects. If you set **Scope** to **All resources**, users have permissions for VPCs in all region-specific projects. When accessing VPCs, the users need to switch to the authorized region.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. When you grant permissions using roles, you also need to attach dependent roles. Roles are not ideal for fine-grained authorization and least privilege access.
- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain

conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant VPC users only the permissions for managing a certain type of resources. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by VPC, see **Permissions Policies and Supported Actions**.

Table 8-1 lists all the system-defined permissions for VPC.

Table 8-1 System-defined permissions for VPC

Policy Name	Description	Policy Type	Dependencies
VPC FullAccess	Full permissions for VPC	System-defined policy	To use the VPC flow log function, users must also have the **LTS ReadOnlyAccess** permission.
VPC ReadOnlyAccess	Read-only permissions on VPC.	System-defined policy	None
VPC Administrator	Most permissions on VPC, excluding creating, modifying, deleting, and viewing security groups and security group rules. To be granted this permission, users must also have the **Tenant Guest** permission.	System-defined role	**Tenant Guest** policy, which must be attached in the same project as **VPC Administrator**.

Table 8-2 lists the common operations supported by system-defined permissions for VPC.

Table 8-2 Common operations supported by system-defined permissions

Operation	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
Creating a VPC	Not supported	Supported	Supported
Modifying a VPC	Not supported	Supported	Supported
Deleting a VPC	Not supported	Supported	Supported

Operation	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
Viewing VPC information	Supported	Supported	Supported
Creating a subnet	Not supported	Supported	Supported
Viewing subnet information	Supported	Supported	Supported
Modifying a subnet	Not supported	Supported	Supported
Deleting a subnet	Not supported	Supported	Supported
Creating a security group	Not supported	Not supported	Supported
Viewing security group information	Supported	Not supported	Supported
Modifying a security group	Not supported	Not supported	Supported
Deleting a security group	Not supported	Not supported	Supported
Adding a security group rule	Not supported	Not supported	Supported
Viewing a security group rule	Supported	Not supported	Supported
Modifying a security group rule	Not supported	Not supported	Supported
Deleting a security group rule	Not supported	Not supported	Supported
Creating a network ACL	Not supported	Supported	Supported
Viewing a network ACL	Supported	Supported	Supported

Operation	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
Modifying a network ACL	Not supported	Supported	Supported
Deleting a network ACL	Not supported	Supported	Supported
Adding a network ACL rule	Not supported	Supported	Supported
Modifying a network ACL rule	Not supported	Supported	Supported
Deleting a network ACL rule	Not supported	Supported	Supported
Creating a VPC peering connection	Not supported	Supported	Supported
Modifying a VPC peering connection	Not supported	Supported	Supported
Deleting a VPC peering connection	Not supported	Supported	Supported
Querying a VPC peering connection	Supported	Supported	Supported
Accepting a VPC peering connection request	Not supported	Supported	Supported
Rejecting a VPC peering connection request	Not supported	Supported	Supported
Creating a route table	Not supported	Supported	Supported
Deleting a route table	Not supported	Supported	Supported
Modifying a route table	Not supported	Supported	Supported

Operation	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
Associating a route table with a subnet	Not supported	Supported	Supported
Adding a route	Not supported	Supported	Supported
Modifying a route	Not supported	Supported	Supported
Deleting a route	Not supported	Supported	Supported
Creating a VPC flow log	Not supported	Supported	Supported
Viewing a VPC flow log	Supported	Supported	Supported
Enabling or disabling a VPC flow log	Not supported	Supported	Supported
Deleting a VPC flow log	Not supported	Supported	Supported

Helpful Links

- What Is IAM?
- Creating a User and Granting VPC Permissions
- Permissions Policies and Supported Actions

9 Basic Concepts

9.1 Subnet

A subnet is a unique CIDR block with a range of IP addresses in a VPC. All resources in a VPC must be deployed on subnets.

- By default, all instances in different subnets of the same VPC can communicate with each other and the subnets can be located in different AZs. If you have a VPC with two subnets in it and they are located in different AZs, they can communicate with each other by default.
- After a subnet is created, its CIDR block cannot be modified. Subnets in the same VPC cannot overlap.

  When you create a VPC, a default subnet will be created together. If you need more subnets, see **Creating a Subnet for the VPC**.

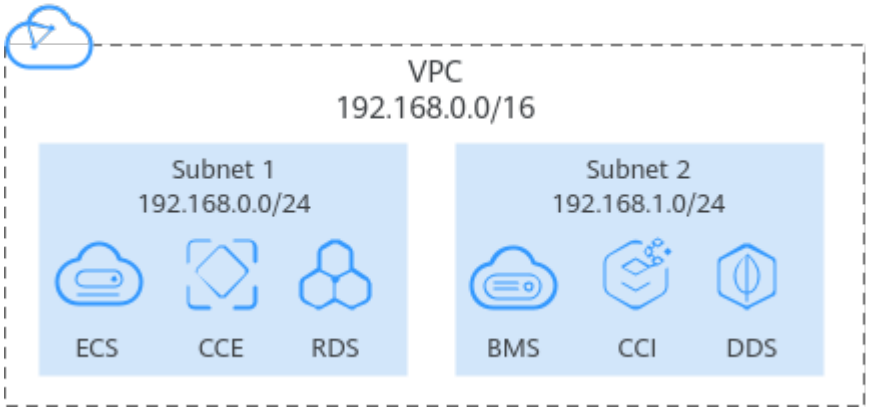
  A subnet mask can be between the netmask of its VPC CIDR block and /28 netmask. If a VPC CIDR block is 10.0.0.0/16, its subnet mask can be between 16 and 28.

  For example, if the CIDR block of VPC-A is 10.0.0.0/16, you can specify 10.0.0.0/24 for subnet A01, 10.0.1.0/24 for subnet A02, and 10.0.2.0/24 for subnet A03.

  NOTE

  By default, you can create a maximum of 100 subnets in each region. If this cannot meet your service requirements, request a quota increase by referring to **How Do I Apply for a Higher Quota?**

Figure 9-1 Subnet

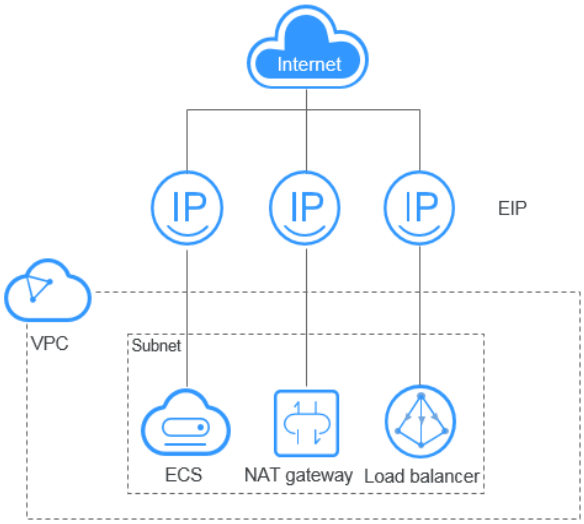


9.2 Elastic IP

The Elastic IP (EIP) service enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, NAT gateways, or load balancers.

Each EIP can be used by only one cloud resource at a time.

Figure 9-2 Accessing the Internet using an EIP



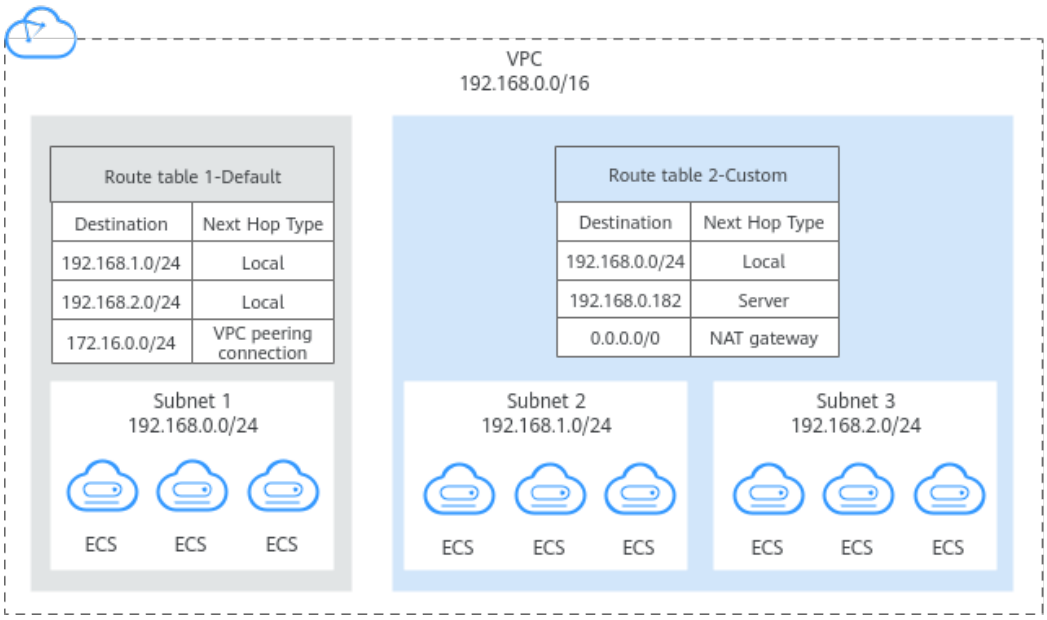
9.3 Route Table

Route Tables

A route table contains a set of routes that are used to determine where network traffic from your subnets in a VPC is directed. Each subnet must be associated with a route table. A subnet can only be associated with one route table, but you can associate multiple subnets with the same route table.

Both IPv4 and IPv6 routes are supported.

Figure 9-3 Route tables



- Default route table: When you create a VPC, the system automatically generates a default route table for the VPC. If you create a subnet in the VPC, the subnet automatically associates with the default route table. The default route table ensures that subnets in a VPC can communicate with each other.
  - You can add routes to, delete routes from, and modify routes in the default route table, but cannot delete the table.
  - When you create a VPC endpoint, VPN or Direct Connect connection, the default route table automatically delivers a route that cannot be deleted or modified.
- Custom route table: If you do not want to use the default route table, you can create a custom route table and associate it with the subnet. Custom route tables can be deleted if they are no longer required.

  The custom route table associated with a subnet affects only the outbound traffic. The default route table of a subnet controls the inbound traffic.

NOTE

To use a custom route table, you need to submit a service ticket. You need to click **Increase quota** on the **Create Route Table** page or choose **More** > **Service Tickets** > **Create Service Ticket** in the upper right corner of the page. For more information, see **Submitting a Service Ticket**.

Route

You can add routes to default and custom route tables and configure the destination, next hop type, and next hop in the routes to determine where network traffic is directed. Routes are classified into system routes and custom routes.

- System routes: These routes are automatically added by the system and cannot be modified or deleted.

After a route table is created, the system automatically adds the following system routes to the route table, so that instances in a VPC can communicate with each other.

- Routes whose destination is 100.64.0.0/10 or 198.19.128.0/20.
- Routes whose destination is a subnet CIDR block.

  If you enable IPv6 when creating a subnet, the system automatically assigns an IPv6 CIDR block to the subnet. Then, you can view IPv6 routes in its route table. Example destinations of subnet CIDR blocks are as follows:

  - IPv4: 192.168.2.0/24
  - IPv6: 2407:c080:802:be7::/64

  NOTE

  In addition to the preceding system routes, the system automatically adds a route whose destination is 127.0.0.0/8. This is the local loopback address.

- Custom routes: These are routes that you can add, modify, and delete. The destination of a custom route cannot overlap with that of a system route.

  You can add a custom route and configure the destination, next hop type, and next hop in the route to determine where network traffic is directed. **Table 9-1** lists the supported types of next hops.

  You cannot add two routes with the same destination to a VPC route table even if their next hop types are different. The route priority depends on the destination. According to the longest match routing rule, the destination with a higher matching degree is preferentially selected for packet forwarding.

Table 9-1 Next hop type

Next Hop Type	Description	Supported Route Table
Server	Traffic intended for the destination is forwarded to an ECS in the VPC.	• Default route table • Custom route table
Extension NIC	Traffic intended for the destination is forwarded to the extension NIC of an ECS in the VPC.	• Default route table • Custom route table
BMS user-defined network	Traffic intended for the destination is forwarded to a BMS user-defined network.	• Custom route table
Direct Connect gateway	Traffic intended for the destination is forwarded to a Direct Connect gateway.	Custom route table

Next Hop Type	Description	Supported Route Table
NAT gateway	Traffic intended for the destination is forwarded to a NAT gateway.	• Default route table • Custom route table
VPC peering connection	Traffic intended for the destination is forwarded to a VPC peering connection.	• Default route table • Custom route table
Virtual IP address	Traffic intended for the destination is forwarded to a virtual IP address and then sent to active and standby ECSs to which the virtual IP address is bound.	• Default route table • Custom route table
VPC endpoint	Traffic intended for the destination is forwarded to a VPC endpoint.	• Default route table • Custom route table
Cloud container	Traffic intended for the destination is forwarded to a cloud container.	• Default route table • Custom route table
Enterprise router	Traffic intended for the destination is forwarded to an enterprise router.	• Default route table • Custom route table
Cloud firewall	Traffic intended for the destination is forwarded to a cloud firewall.	• Default route table • Custom route table

NOTE

If you specify the destination when creating a resource, a system route is delivered. If you do not specify a destination when creating a resource, a custom route that can be modified or deleted is delivered.

For example, when you create a NAT gateway, the system automatically delivers a custom route without a specific destination (0.0.0.0/0 is used by default). In this case, you can change the destination. However, when you create a VPN gateway, you need to specify the remote subnet, that is, the destination of a route. In this case, the system delivers this system route. Do not modify the route destination on the **Route Tables** page. If you do, the destination will be inconsistent with the configured remote subnet. To modify the route destination, go to the specific resource page and modify the remote subnet, then the route destination will be changed accordingly.

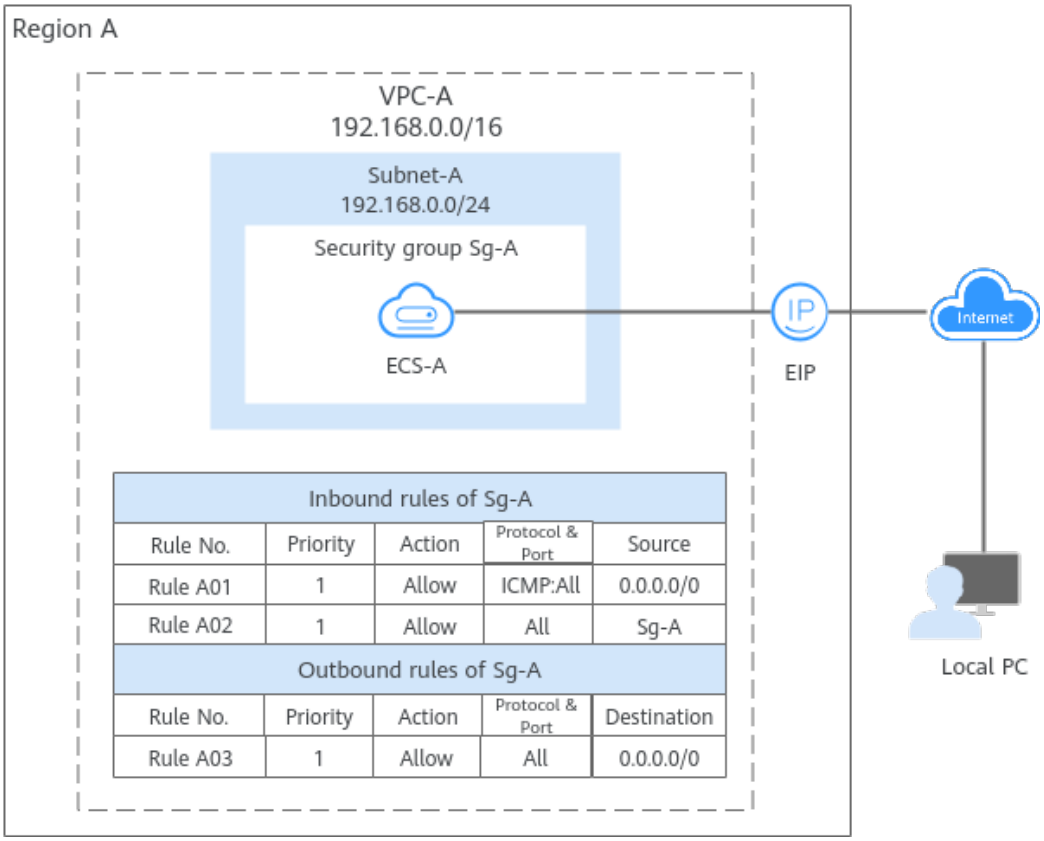
9.4 Security Group

A security group is a collection of access control rules for cloud resources, such as cloud servers, containers, and databases, that have the same security protection requirements and that are mutually trusted. After a security group is created, you can configure access rules that will apply to all cloud resources added to this security group.

Each security group can have both inbound and outbound rules. You need to specify the source, port, and protocol for each inbound rule and specify the destination, port, and protocol for each outbound rule to control the inbound and outbound traffic to and from the instances in the security group. As shown in Figure 9-4, you have a VPC (**VPC-A**) with a subnet (**Subnet-A**) in region A. An ECS (**ECS-A**) is running in **Subnet-A** and associated with security group **Sg-A**.

- Security group **Sg-A** has a custom inbound rule to allow ICMP traffic to **ECS-A** from your PC over all ports. However, the security group does not contain rules that allow SSH traffic to **ECS-A** so you cannot remotely log in to **ECS-A** from your PC.
- If **ECS-A** needs to access the Internet through an EIP, the outbound rule of **Sg-A** must allow all traffic from **ECS-A** to the Internet.

Figure 9-4 Security group architecture



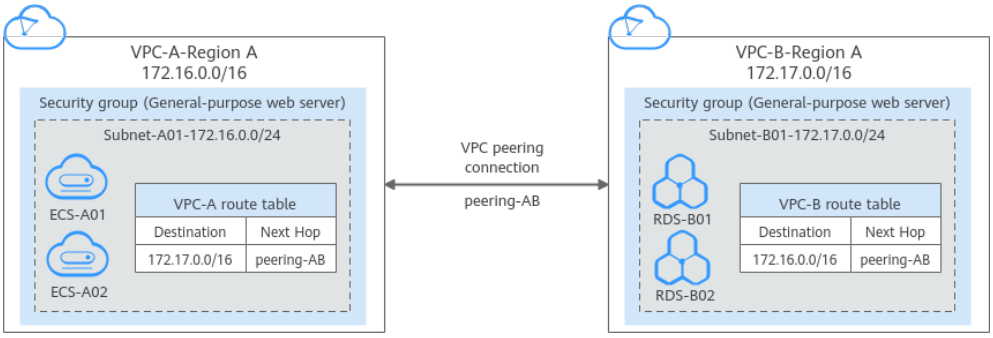
9.5 VPC Peering Connection

A VPC peering connection is a networking connection that connects two VPCs for them to communicate using private IP addresses. The VPCs to be peered can be in the same account or different accounts, but must be in the same region.

Figure 9-5 shows an application scenario of VPC peering connections.

- There are two VPCs (VPC-A and VPC-B) in region A that are not connected.
- Service servers (ECS-A01 and ECS-A02) are in VPC-A, and database servers (RDS-B01 and RDS-B02) are in VPC-B. The service servers and database servers cannot communicate with each other.
- You need to create a VPC peering connection (peering-AB) between VPC-A and VPC-B so the service servers and database servers can communicate with each other.

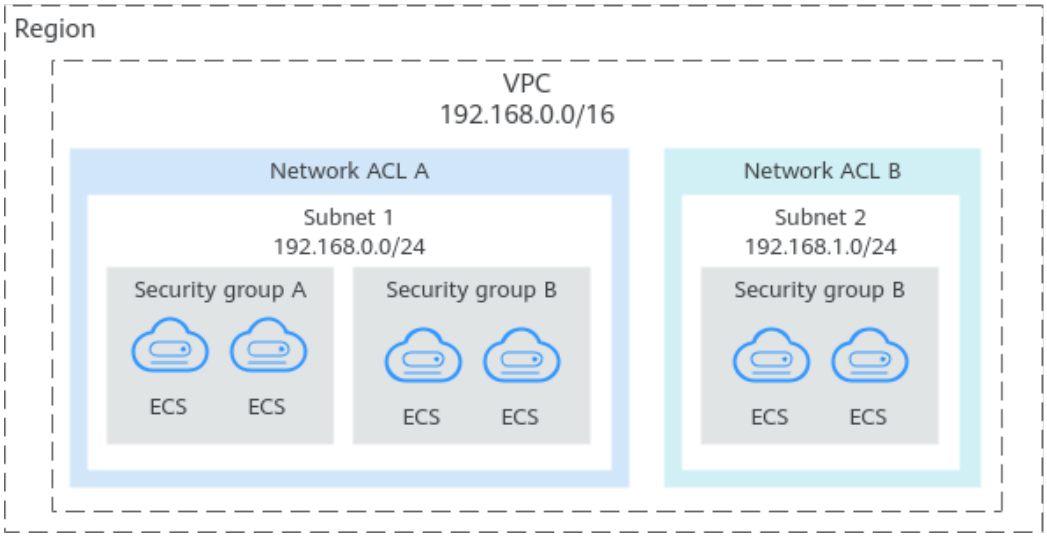
Figure 9-5 VPC peering connection network diagram



9.6 Network ACL

A network ACL is an optional layer of security for your subnets. After you associate one or more subnets with a network ACL, you can control traffic in and out of the subnets.

Figure 9-6 Security groups and network ACLs



Similar to security groups, network ACLs control access to subnets and add an additional layer of defense to your subnets. Security groups only have the "allow" rules, but network ACLs have both "allow" and "deny" rules. You can use network ACLs together with security groups to implement comprehensive and fine-grained access control.

9.7 Virtual IP Address

A virtual IP address can be shared among multiple ECSs. An ECS can have a private and a virtual IP address, which allows your users to access the ECS through either IP address.

You can use either IP address to enable layer 2 and layer 3 communications in a VPC, access a different VPC using peering connections, and access cloud servers through EIPs, Direct Connect connections, and VPN connections.

You can bind a virtual IP address to ECSs deployed in the active/standby pair, and then bind an EIP to the virtual IP address. Virtual IP addresses can work together with Keepalived to ensure high availability and disaster recovery. If the active ECS is faulty, the standby ECS automatically takes over services from the active one.

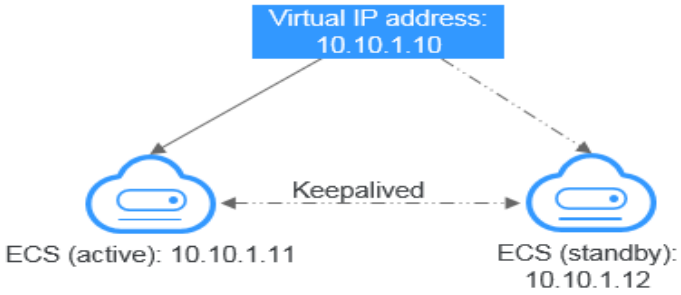
Networking

Virtual IP addresses are used for high availability and can work together with Keepalived to make active/standby ECS switchover possible. This way if one ECS goes down for some reason, the other one can take over and services continue uninterrupted. ECSs can be configured for HA or as load balancing clusters.

- **Networking mode 1**: HA

  To improve service availability and eliminate single points of failure, you can deploy ECSs in the active/standby pair or deploy one active ECS and multiple standby ECSs. And then, you can bind the same virtual IP address to these ECSs. If the active ECS becomes faulty, a standby ECS takes over services from the active ECS and services continue uninterrupted.

Figure 9-7 Networking diagram of the HA mode

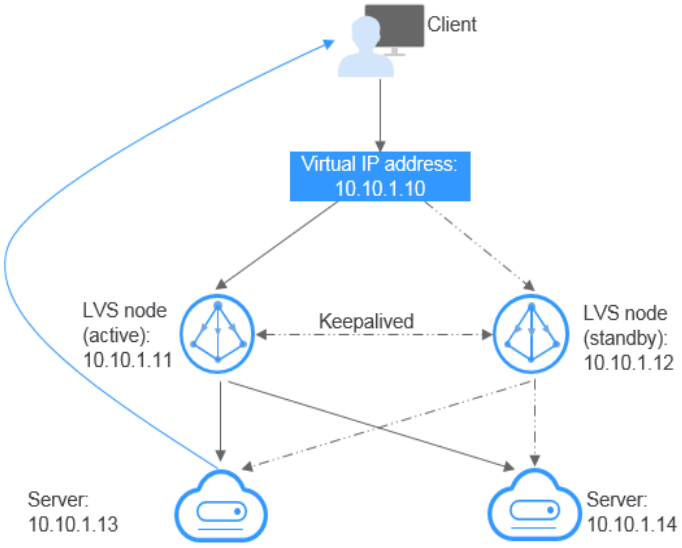


  - As shown in the above figure, bind a virtual IP address to two ECSs in the same subnet.
  - Configure Keepalived for the two ECSs to work in the active/standby pair. Follow industry standards for configuring Keepalived. The details are not included here.

- **Networking mode 2**: HA load balancing cluster

  If you want to build a high-availability load balancing cluster, use Keepalived and configure LVS nodes as direct routers.

  Figure 9-8 HA load balancing cluster



  - Bind a single virtual IP address to two ECSs.
  - Configure the two ECSs as LVS nodes working as direct routers and use Keepalived to configure the nodes in the active/standby pair. The two ECSs will evenly forward requests to different backend servers.
  - Configure two more ECSs as backend servers.
  - Disable the source/destination check for the two backend servers.

  Follow industry standards for configuring Keepalived. The details are not included here.

Application Scenarios

- Accessing the virtual IP address through an EIP

  If your application has high availability requirements and needs to provide services through the Internet, it is recommended that you bind an EIP to a virtual IP address.

- Using a VPN, Direct Connect, or VPC peering connection to access a virtual IP address

  To ensure high availability and access to the Internet, use a VPN for security and Direct Connect for a stable connection. A VPC peering connection is needed so that two VPCs in the same region can communicate with each other.

9.8 Elastic Network Interface

An elastic network interface (referred to as a network interface in this documentation) is a virtual network card. You can create and configure network interfaces and attach them to your instances (ECSs and BMSs) to obtain flexible and highly available network configurations.

Network Interface Types

- A primary network interface is created together with an instance by default, and cannot be detached from the instance.
- An extended network interface is created on the **Network Interfaces** console, and can be attached to or detached from an instance.

Application Scenarios

- Flexible migration

  You can detach a network interface from an instance and then attach it to another instance. The network interface retains its private IP address, EIP, and security group rules. In this way, service traffic on the faulty instance can be quickly migrated to the standby instance, implementing quick service recovery.

- Traffic management

  You can attach multiple network interfaces that belong to different subnets in a VPC to the same instance, and configure the network interfaces to carry the private network traffic, public network traffic, and management network traffic of the instance. You can configure access control policies and routing policies for each subnet, and configure security group rules for each network interface to isolate networks and service traffic.

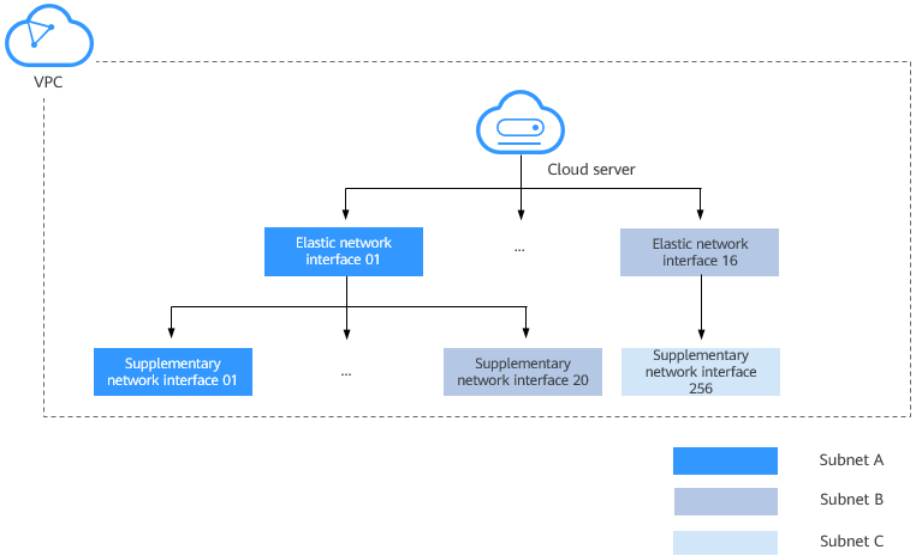
9.9 Supplementary Network Interface

Supplementary network interfaces are a supplement to elastic network interfaces. If the number of elastic network interfaces that can be attached to your ECS cannot meet your requirements, you can use supplementary network interfaces, which can be attached to VLAN subinterfaces of elastic network interfaces.

Application Scenarios

Supplementary network interfaces are attached to VLAN subinterfaces of elastic network interfaces. **Figure 9-9** shows the networking diagram.

Figure 9-9 Supplementary network interface networking diagram



The number of elastic network interfaces that can be attached to each ECS is limited. If this limit cannot meet your requirements, you can attach supplementary network interfaces to elastic network interfaces.

- You can attach supplementary network interfaces that belong to different subnets in the same VPC to an ECS. Each supplementary network interface has its private IP address and EIP for private or Internet communication.
- You can security group rules for supplementary network interfaces for network isolation.

9.10 Region and AZ

Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an

AZ, computing, network, storage, and other resources are logically divided into multiple clusters. to support high-availability systems.

Selecting a Region

If your target users are in Europe, select the **EU-Dublin** region.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

