Virtual Private Cloud

Service Overview

Issue	43
Date	2023-08-07

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Network Service Overview 1

1.1 Huawei Cloud Network Service Overview 1

1.2 Network Planning and Design 8

1.3 Network Security 15

1.4 Network Monitoring 18

2 What Is Virtual Private Cloud? 20

3 Product Advantages 23

4 Application Scenarios 26

5 Functions 32

6 Security 36

6.1 Shared Responsibilities 36

6.2 Identity Authentication and Access Control 37

6.3 Auditing and Logging 38

6.4 Risk Monitoring 38

7 Notes and Constraints 39

8 VPC and Other Services 40

9 Billing 42

10 Permissions 44

11 Basic Concepts 49

11.1 Subnet 49

11.2 Elastic IP 50

11.3 Route Table 50

11.4 Security Group 54

11.5 VPC Peering Connection 55

11.6 Network ACL 56

11.7 Virtual IP Address 58

11.8 Elastic Network Interface 60

11.9 Supplementary Network Interface 60

11.10 IP Address Group 61

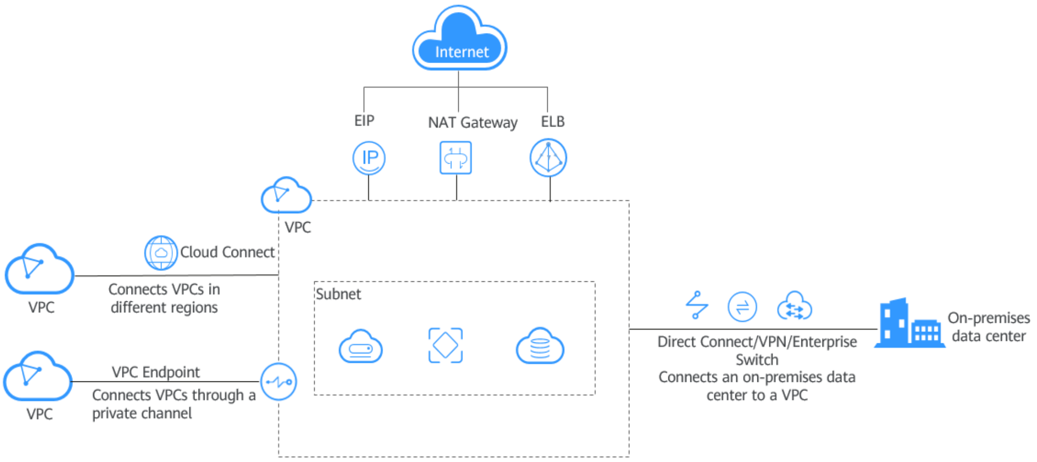
11.11 Region and AZ..62

1 Network Service Overview

1.1 Huawei Cloud Network Service Overview

Huawei Cloud provides various network services to help you build secure and scalable networks on the cloud, connect cloud and on-premises networks in a high-speed and reliable way, and connect your on-premises data center to the Internet.

Figure 1-1 Network services

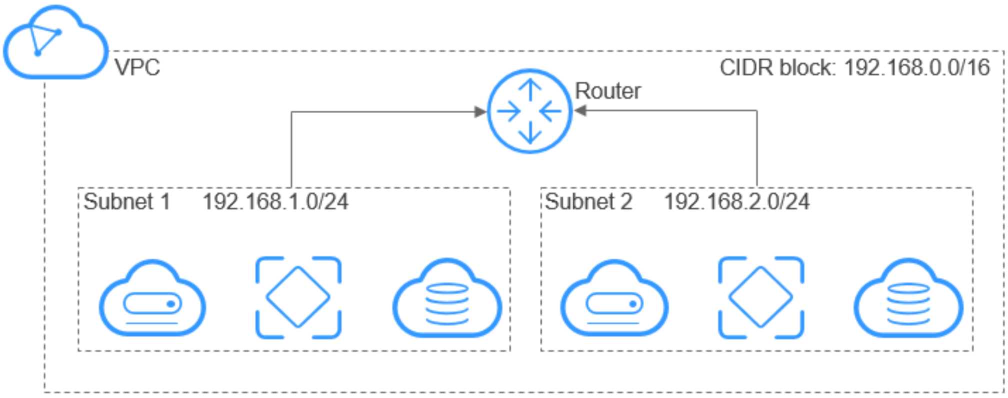

Internet
EIP
NAT Gateway
ELB
VPC
Cloud Connect
Connects VPCs in different regions
VPC
Subnet
VPC Endpoint
Connects VPCs through a private channel
VPC
Direct Connect/VPN/Enterprise Switch
Connects an on-premises data center to a VPC
On-premises data center

Virtual Private Cloud (VPC)

A VPC is logically isolated, configurable, and manageable virtual network for cloud servers, cloud containers, and cloud databases. It improves resource security and simplifies network deployment on the cloud.

Each VPC consists of a private CIDR block, route tables, and at least one subnet. When you create a VPC, you need to specify a CIDR block for the VPC and the system automatically generates a default route table for the VPC. All resources in a VPC must be deployed on subnets. The default route table ensures that all subnets in the VPC can communicate with each other.

Figure 1-2 VPC



VPC can work together with other network services for more flexible network connectivity.

- Connecting to the Internet

  Resources in a VPC can communicate with the Internet through **elastic IP addresses (EIPs)**. You can also use a NAT gateway to enable resources in a VPC to share an EIP.

- Connecting a VPC and an on-premises network

  Direct Connect, **Enterprise Switch**, or **VPN** can be used to connect a VPC to an on-premises data center.

- Connecting VPCs

  A **VPC peering connection** enables communication between two VPCs in the same region.

  Cloud Connect enables high-speed and stable communication between VPCs in different regions.

For details about VPC, see **What Is Virtual Private Cloud?**

Elastic IP (EIP)

The 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, load balancers, and NAT gateways.

You can also purchase the following for your EIPs:

- Shared bandwidth

  Shared bandwidth allows ECSs, BMSs, and load balancers that are bound with EIPs in the same region to share the same bandwidth.

- Shared data package

  A shared data package provides a quota for data usage. Shared data packages take effect immediately after your purchase. If you have subscribed to pay-per-use EIPs billed by traffic in a region and buy a shared data package in the same region, the EIPs will use the shared data package. After the package quota is used up or the package expires, the EIPs will continue to be billed on a pay-per-use basis.

- Bandwidth add-on package

  A bandwidth add-on package is used to temporarily increase the maximum bandwidth of a yearly/monthly EIP.

For details about EIP, see **What Are EIPs?**

NAT Gateway

Public NAT gateway

Public NAT gateways provide network address translation (NAT) with 20 Gbit/s of bandwidth for servers in a VPC, such as ECSs, Bare Metal Servers (BMSs), and Workspace desktops, or for servers that connect to a VPC through Direct Connect or VPN in on-premises data centers, allowing these servers to share EIPs to access the Internet or to provide services accessible from the Internet.

NAT gateways provide source NAT and destination NAT functions.

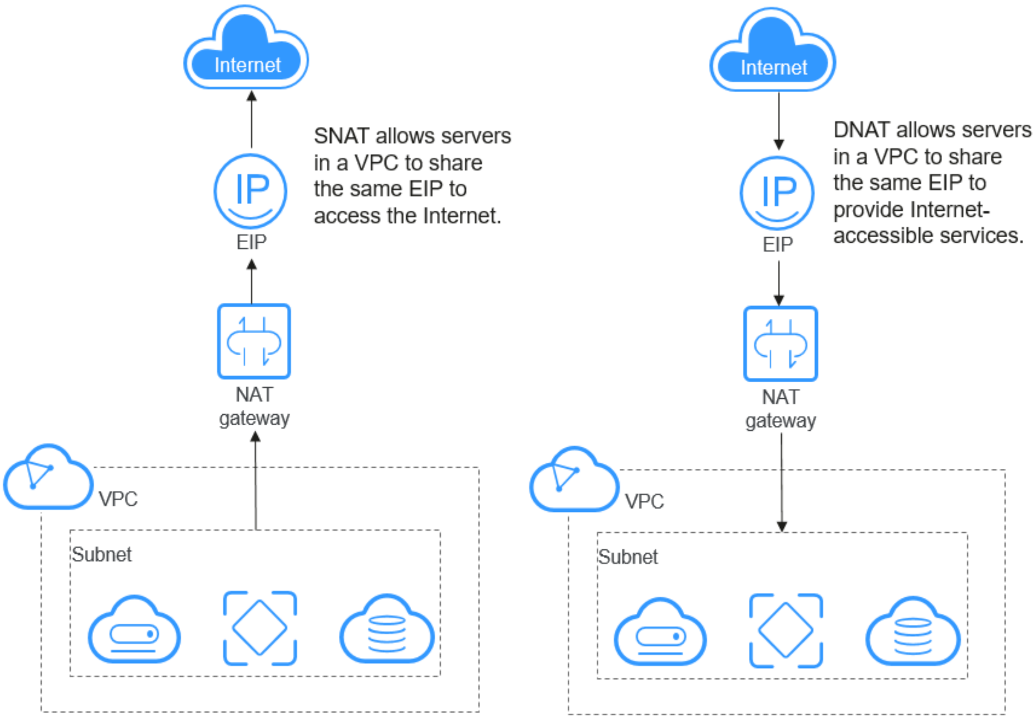
- Source NAT (SNAT)

  SNAT translates private IP addresses into EIPs, allowing servers in a VPC to share an EIP to access the Internet in a secure and efficient way.

- Destination NAT (DNAT)

  DNAT enables servers in a VPC to share an EIP to provide services accessible from the Internet through IP address mapping or port mapping.

Figure 1-3 Public NAT gateway


Internet
SNAT allows servers in a VPC to share the same EIP to access the Internet.
EIP
NAT gateway
VPC
Subnet
Internet
DNAT allows servers in a VPC to share the same EIP to provide Internet-accessible services.
EIP
NAT gateway
VPC
Subnet

Private NAT gateway

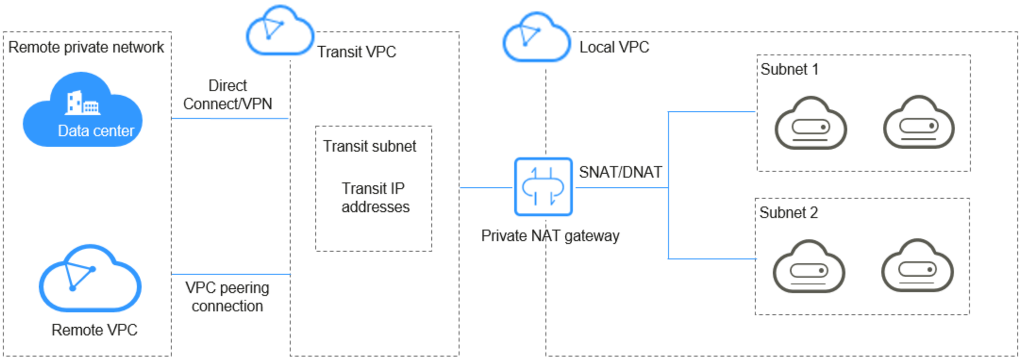
Private NAT gateways provide network address translation (NAT) for servers, such as ECSs, BMSs, and Workspace desktops, in a VPC, and allow multiple servers to share a private IP address to access or provide services accessible from an on-premises data center or a remote VPC.

A private NAT gateway translates IP addresses between your VPC and your on-premises data center or another VPC, allowing you to keep legacy networks unchanged after migrating some of your workloads to the cloud.

Private NAT gateways support SNAT and DNAT.

- SNAT allows multiple servers across AZs in a VPC to share the transit IP address to access an on-premises data center or a remote VPC.
- DNAT enables servers that share the same transit IP address in a VPC to provide services accessible from an on-premises data center or a remote VPC through IP address or port mapping.

Figure 1-4 Private NAT gateway

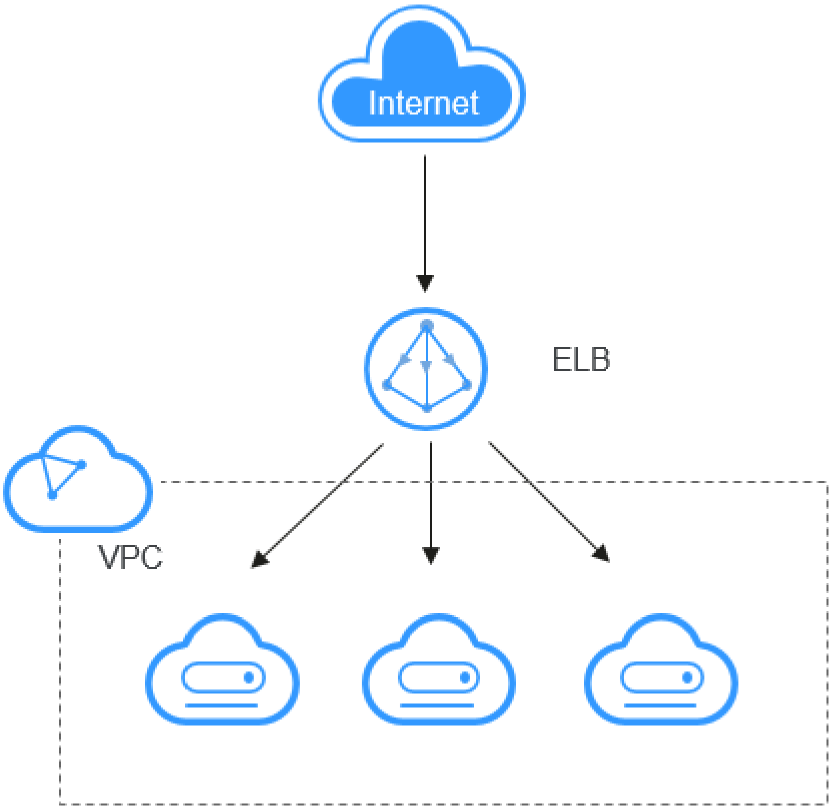


For details, see **What Is NAT Gateway?**

Elastic Load Balance (ELB)

ELB automatically distributes incoming traffic across multiple backend servers based on configured listening rules. ELB expands the capacities of your applications and improves their availability by eliminating single points of failure (SPOFs).

Figure 1-5 ELB



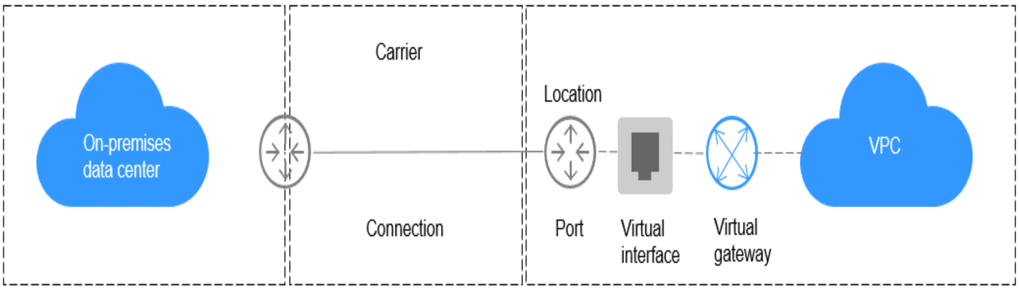
For details, see **What Is ELB?**

Direct Connect

Direct Connect allows you to establish a dedicated network connection between your on-premises data center and a VPC. With Direct Connect, you can easily build a secure and reliable hybrid cloud.

Direct Connect establishes a dedicated connection, and your data will not be transferred over the Internet.

Figure 1-6 Direct Connect



You can connect your data center to the cloud using either type of connection:

- Standard connection

  You have more than one connection terminated at different locations. These connections work as a backup for each other, improving the reliability of connections. If you can select only one carrier due to special requirements, you must configure different physical routes.

  A standard connection provides an exclusive port. You can create standard connections on the management console.

- Hosted connection

  You request a connection from a partner who has a line terminated at the Direct Connect location that is nearby to your on-premises data center.

  You share the port with others.

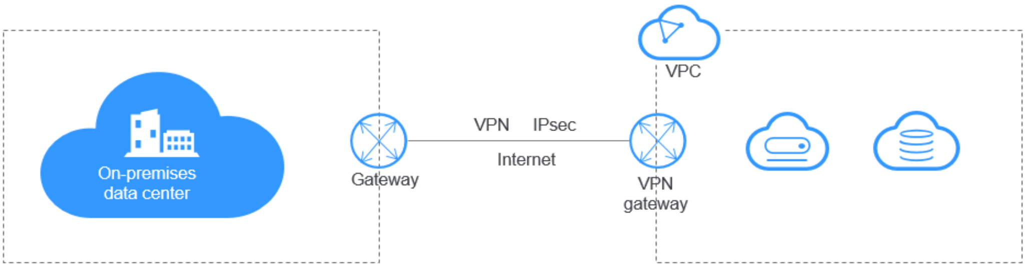
For details, see **What Is Direct Connect?**

VPN

VPN establishes a secure, encrypted communication tunnel between your data center and your VPC. With VPN, you can connect to a VPC and access the resources deployed there.

Different from Direct Connect, VPN establishes an encrypted tunnel that transfers data over the Internet.

Figure 1-7 Network topology



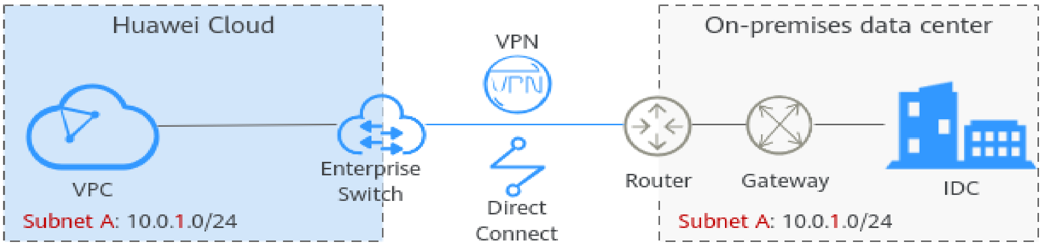
Enterprise Switch

Enterprise switches enable Layer 2 networking for VPCs, helping you to connect cloud and on-premises networks that are highly reliable, in a large scale, and of high performance.

Currently, enterprise switches only support Layer 2 connection gateways (L2CGs). An L2CG is a virtual tunnel gateway that can work with Direct Connect or VPN to establish network communications between cloud and on-premises networks at Layer 2. The gateway allows you to migrate workloads in data centers or private clouds to the cloud without changing subnets and IP addresses.

An enterprise switch is a tunnel gateway of a VPC and corresponds to the tunnel gateway of your data center. It can work together with Direct Connect or VPN to enable communications between a VPC and your data center at Layer 2. **Figure 1-8** shows the networking diagram. You need to connect a VPC subnet to the enterprise switch and specify the enterprise switch to establish a connection with the tunnel gateway of your on-premises data center so that the VPC subnet can communicate with the data center subnet at Layer 2.

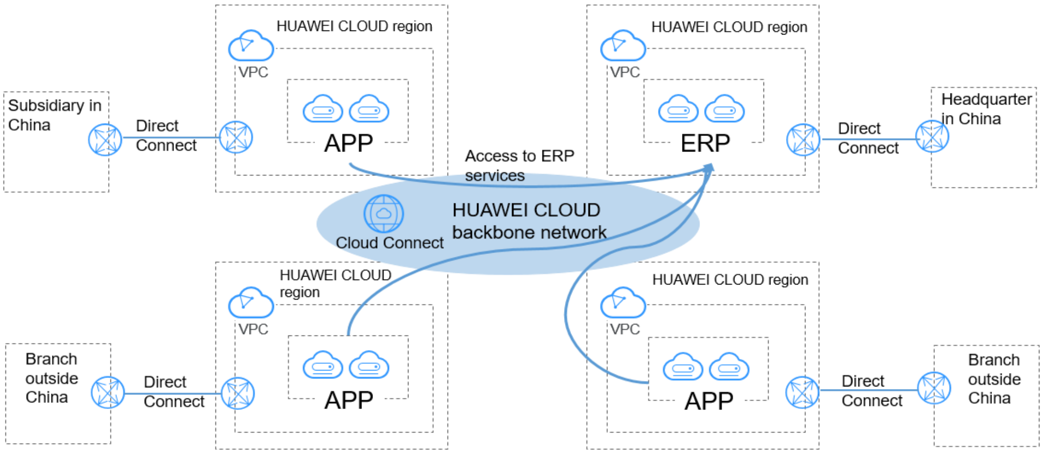
Figure 1-8 Layer 2 networking



Cloud Connect

Cloud Connect allows you to quickly build high-quality networks that can connect VPCs across regions and work with Direct Connect to connect VPCs and on-premises data centers. With Cloud Connect, you can build a globally connected cloud network with enterprise-class scalability and communications capabilities.

Figure 1-9 Network topology



VPC Endpoint (VPCEP)

The VPCEP service provides secure and private channels to connect your VPC to VPC endpoint services (cloud services or your private services) without having to use EIPs.

VPCEP applies to the following scenarios:

- Access to your private services in a VPC through a VPC endpoint service

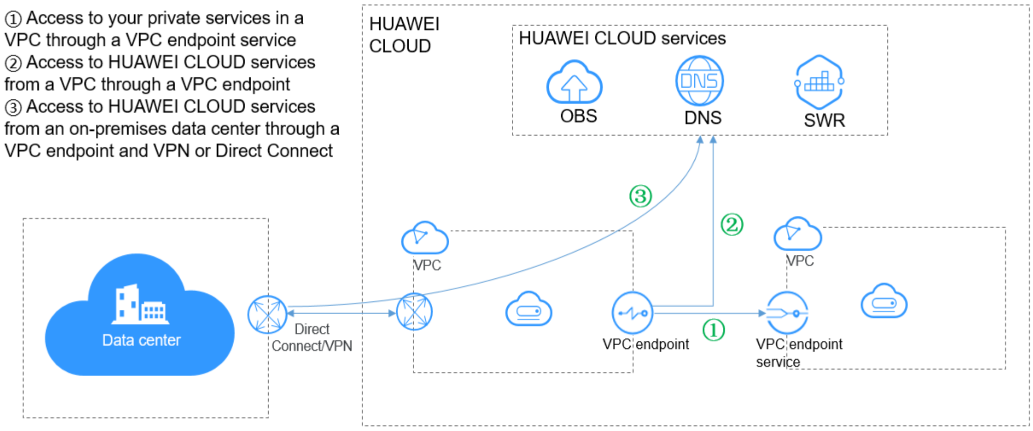
  You can create a VPC endpoint service to allow your services provided by ELB, ECS, and BMS in a VPC to be accessible.

  A service consumer uses a VPC endpoint to access the endpoint service.
- Access to cloud services from a VPC through a VPC endpoint

  You can create a VPC endpoint to access the VPC endpoint services.
- Access to cloud services from an on-premises data center through a VPC endpoint and VPN or Direct Connect

VPN or Direct Connect can work together with a VPC endpoint to allow access to cloud services, such as OBS, DNS, and SWR, from an on-premises data center.

Figure 1-10 VPC endpoint

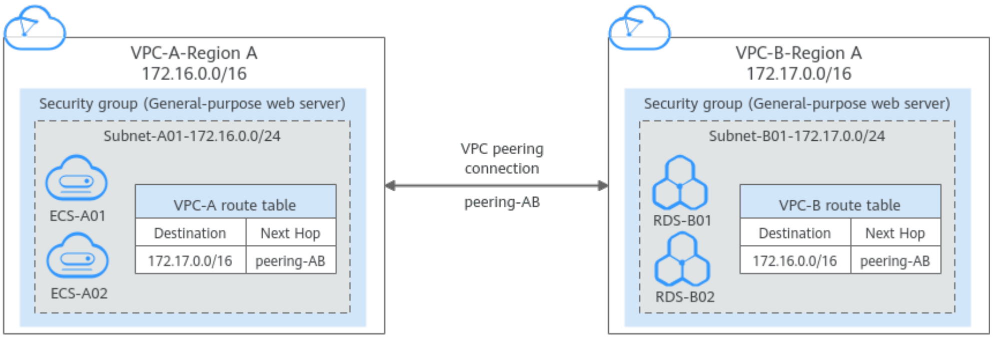

① Access to your private services in a VPC through a VPC endpoint service
② Access to HUAWEI CLOUD services from a VPC through a VPC endpoint
③ Access to HUAWEI CLOUD services from an on-premises data center through a VPC endpoint and VPN or Direct Connect
HUAWEI CLOUD
HUAWEI CLOUD services
OBS
DNS
SWR
③
②
VPC
VPC
Data center
Direct Connect/VPN
VPC endpoint
①
VPC endpoint service

VPC Peering

By default, VPCs cannot communicate with each other. A VPC peering connection enables two VPCs in the same region to 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. A VPC peering connection between VPCs in different regions will not take effect.

For details, see **VPC Peering Connection Overview** and **VPC Peering Connection Configuration Plans**.

Figure 1-11 VPC peering connection network diagram



VPC-A route table

Destination	Next Hop
172.17.0.0/16	peering-AB

VPC-B route table

Destination	Next Hop
172.16.0.0/16	peering-AB

For details about the differences between VPC peering connections and VPC endpoints, see **What Are the Differences Between VPC Endpoints and VPC Peering Connections?**

1.2 Network Planning and Design

When you deploy workloads on the cloud, you need to consider network isolation, scalability, and connectivity.

- **Isolation**

  Isolation is the basic requirement for network planning and design. By default, VPCs are isolated from each other and cannot communicate with each other over a private network no matter whether they are in the same region.

  Generally, different workloads are in different VPCs. Different departments or environments (such as development, test, and production) use different VPCs.

  You can create multiple subnets in a VPC for workloads with different requirements and configure network ACLs to ensure security between subnets.

- **Scalability**

  Consider network scalability from the following aspects as workload requirements constantly change over time:

  – Reserve sufficient IP addresses for capacity expansion.

  – Create VPCs for **connectivity**.

- **Connectivity**

  Network connectivity is closely related to network isolation and scalability. You need to consider network connectivity between:

  – A VPC and the Internet

  – VPCs in the same region and in different regions

  – An on-premises data center and a VPC

The preceding sections describe some basic principles of network planning. For details about the concepts of regions, see **Region and AZ**. The following describes network planning and design in terms of VPC planning, subnet planning, Internet connectivity, connectivity between VPCs and between an on-premises data center and a VPC.

How Do I Determine How Many VPCs I Need?

VPCs are region-specific. By default, networks in VPCs in different regions or even in the same region are not connected.

- One VPC

  If your services do not require network isolation, a single VPC should be enough.

- Multiple VPCs

If you have multiple service systems in a region and each service system requires an isolated network, you can create a separate VPC for each service system.

If you require network connectivity between separate VPCs in the same account or in different accounts, you can use VPC peering connections or Cloud Connect.

- If two VPCs are in the same region, use a **VPC peering connection**.
- If two VPCs are in different regions, use **Cloud Connect**.

NOTE

By default, you can create a maximum of five VPCs in each region. If this cannot meet your service requirements, request a quota increase. For details, see **How Do I Apply for a Higher Quota?**

The following table lists the private CIDR blocks that you can specify when creating a VPC. Consider the following when selecting a VPC CIDR block:

- Number of IP addresses: Reserve sufficient IP addresses in case of business growth.
- IP address range: Avoid IP address conflicts if you need to connect a VPC to an on-premises data center or connect two VPCs.

Table 1-1 lists the supported VPC CIDR blocks.

Table 1-1 VPC CIDR blocks

VPC CIDR Block	IP Address Range	Maximum Number of IP Addresses
10.0.0.0/8-24	10.0.0.0-10.255.255.255	2^24-2=16777214
172.16.0.0/12-24	172.16.0.0-172.31.255.255	2^20-2=1048574
192.168.0.0/16-24	192.168.0.0-192.168.255.255	2^16-2=65534

How Do I Plan Subnets?

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 between 16 to 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 10.0.3.0/24 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?**

When planning subnets, consider the following:

- You create different subnets for different modules in a VPC. For example, in VPC-A, you can create subnet A01 for web services, subnet A02 for management services, and subnet A03 for data services. You can leverage network ACLs to control access to each subnet.

- If your VPC needs to communicate with an on-premises data center through VPN or Direct Connect, ensure that the VPC subnet and the CIDR block used for communication in the data center do not overlap.

How Do I Plan Routing Policies?

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. A route table contains a set of routes that are used to determine where network traffic from your subnets in a VPC is directed. The default route table ensures that subnets in a VPC can communicate with each other.

If you do not want to use the default route table, you can now create a custom route table and associate it with the subnets. The custom route table associated with a subnet affects only the outbound traffic. The default route table controls the inbound traffic.

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: Routes that are automatically added by the system and cannot be modified or deleted. System routes allow instances in a VPC to communicate with each other.
- Custom routes: Routes that can be modified and deleted. The destination of a custom route cannot overlap with that of a system route.

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

Connecting VPCs

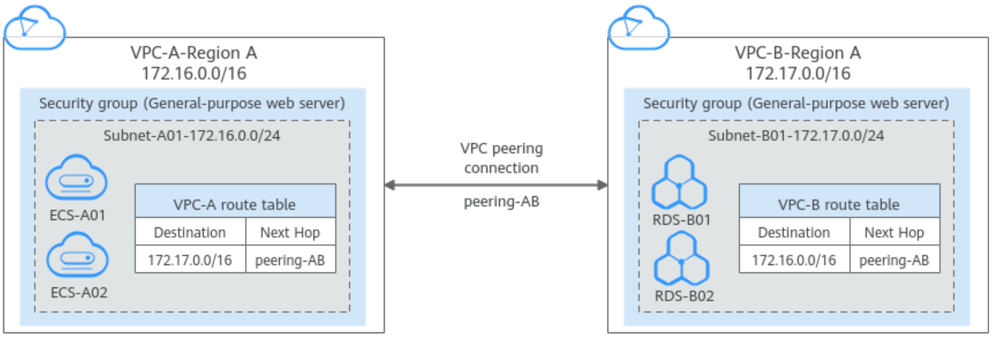
You can use the following to connect two VPCs.

- **VPC Peering**

  A VPC peering connection is a networking connection between two VPCs and enables 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. For details, see **VPC Peering Connection Overview**.

  If the local and peer VPCs have overlapping CIDR blocks, the VPC peering connection may not take effect.

Figure 1-12 VPC peering connection network diagram



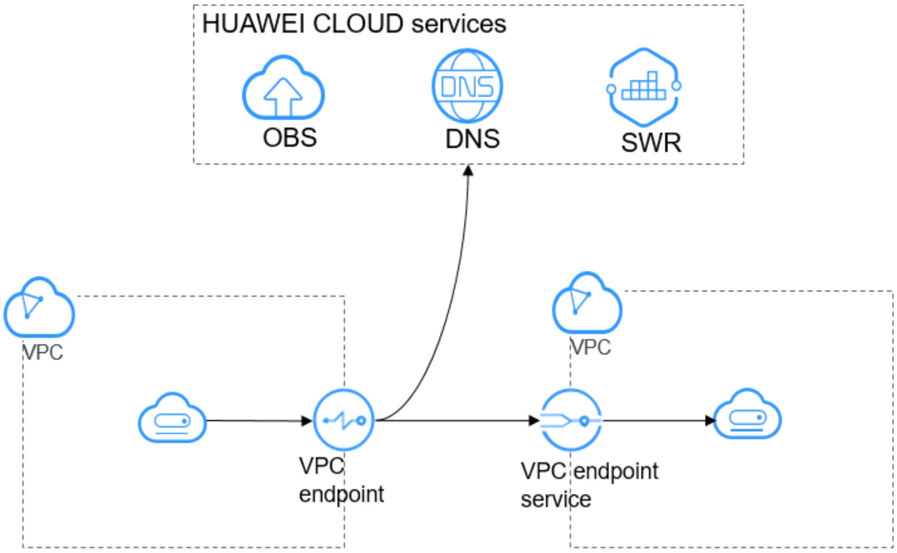
- **VPC endpoint**

  The VPCEP service provides secure and private channels to allow your resources in a VPC to be accessible from other VPCs. In addition, you can access Huawei Cloud services, such as OBS, SWR, and DNS, through VPC endpoints over the private network.

  VPCEP allows you to access cloud resources or other cloud services in a VPC that is configured as a VPC endpoint service. The access is unidirectional, which is more secure and private.

  For details, see **What Is VPC Endpoint?**

Figure 1-13 Using the VPCEP service to access services across VPCs in a unidirectional way

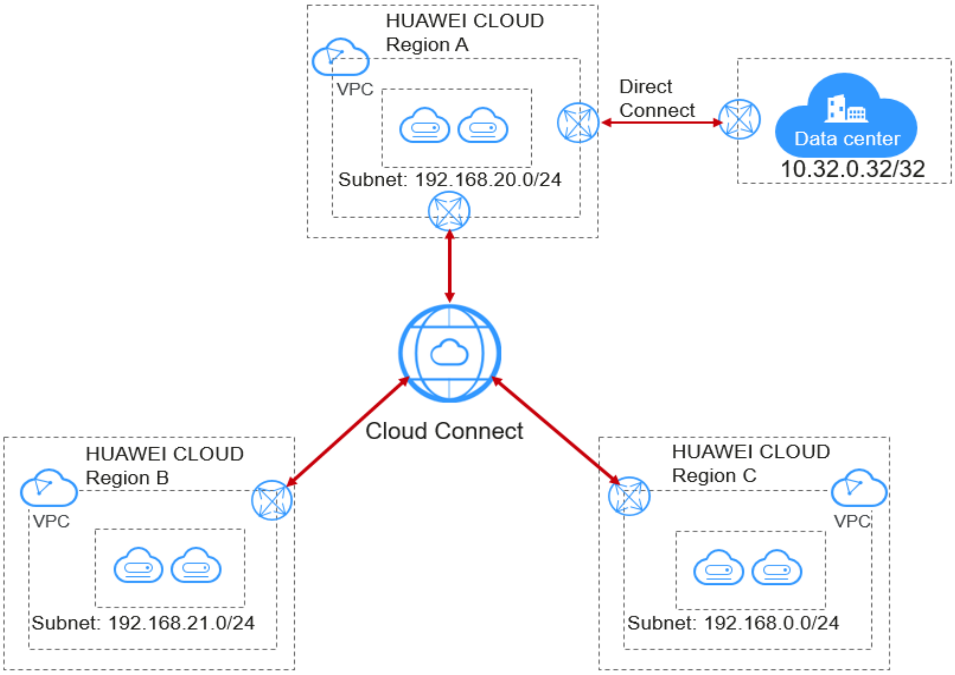


- **Cloud Connect**

  Cloud Connect allows you to quickly build high-quality networks that can connect VPCs across regions and work with Direct Connect to connect VPCs and on-premises data centers. With Cloud Connect, you can build a globally connected cloud network with enterprise-class scalability and communications capabilities.

  The CIDR blocks of VPCs connected by a cloud connection cannot overlap. Otherwise, network communications will fail. For details, see **What Is Cloud Connect?**

Figure 1-14 Connecting VPCs across regions

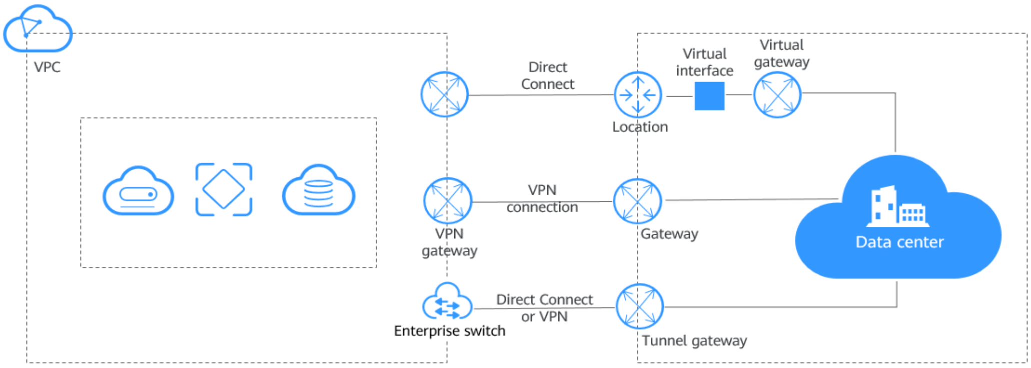


Connecting a VPC to an On-premises Data Center

If your VPC needs to communicate with your on-premises data center, you can use Direct Connect or VPN together with an L2CG.

- Direct Connect establishes a dedicated connection, and your data will not be transferred over the Internet.
- VPN establishes an encrypted tunnel that transfers data over the Internet.
- Enterprise switches only support Layer 2 connection gateways (L2CGs) now. An L2CG is a virtual tunnel gateway that can work with Direct Connect or VPN to establish network communications between cloud and on-premises networks at Layer 2. The gateway allows you to migrate workloads in data centers or private clouds to the cloud without changing subnets and IP addresses.

Figure 1-15 Connecting a VPC to an on-premises data center



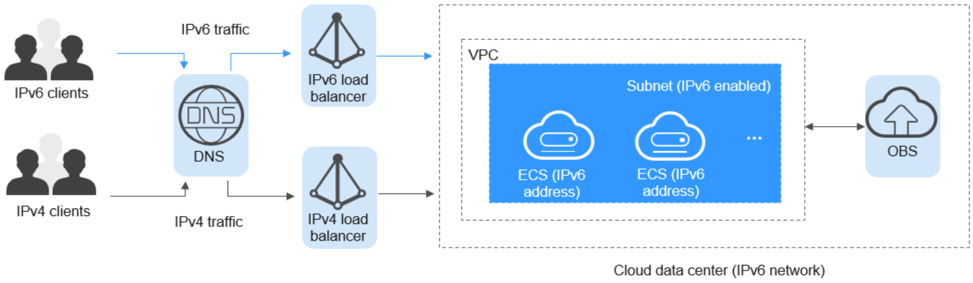
Connecting to the Internet

- **Use EIPs to enable a small number of ECSs to access the Internet.**

  When only a few ECSs need to access the Internet, you can bind EIPs to these ECSs. This will provide them with Internet access. You can also dynamically unbind the EIPs from the ECSs and bind them to NAT gateways and load balancers instead, which will also provide Internet access. The process is not complicated. Different EIPs in the same region can share a bandwidth, reducing your bandwidth costs.

  You can obtain both IPv4 and IPv6 addresses for private or Internet communication if you enable IPv4 and IPv6 dual stack or IPv6 EIP.

  Figure 1-16 IPv4 and IPv6 dual stack

  For more information about EIP, see **EIP Overview**.

- **Use a NAT gateway to enable a large number of ECSs to access the Internet.**

  When a large number of ECSs need to access the Internet, you can use NAT gateways for your ECSs. With NAT gateways, you do not need to assign an EIP to each ECS. NAT gateways reduce costs as you do not need so many EIPs. NAT gateways offer both SNAT and DNAT. SNAT allows multiple ECSs in the same VPC to share one or more EIPs to access the Internet. SNAT prevents the EIPs of ECSs from being exposed to the Internet. DNAT can implement 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.

  For more information, see **NAT Gateway User Guide**.

- **Use ELB to access the Internet If there are a large number of concurrent requests.**

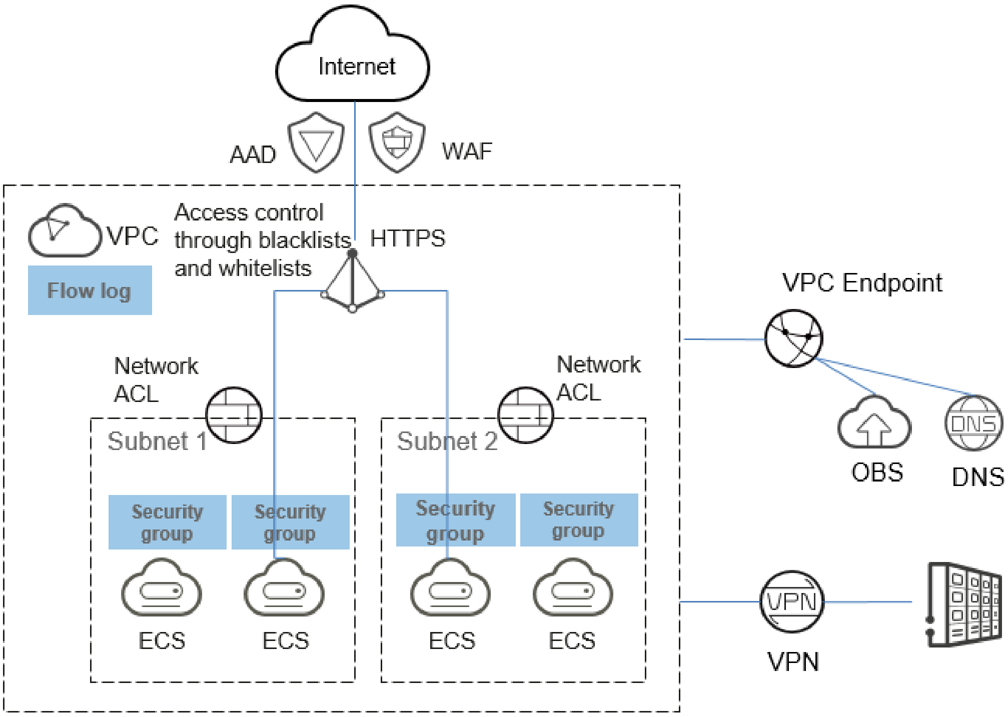
  In high-concurrency scenarios, such as e-commerce, you can use load balancers provided by the ELB service to evenly distribute incoming traffic across multiple ECSs, allowing a large number of users to concurrently access your business system or application. ELB is deployed in the cluster mode. It provides fault tolerance for your applications by automatically balancing traffic across multiple AZs. ELB deeply integrates with the Auto Scaling (AS) service, which enables automatic scaling based on service traffic and ensures service stability and reliability.

  For more information, see **Elastic Load Balance User Guide**.

1.3 Network Security

Huawei Cloud provides a wide range of security services and functions to secure your resources.

The following figure shows how Huawei Cloud security services and functions protect your resources.



Advanced Anti-DDoS (AAD) and Web Application Firewall (WAF)

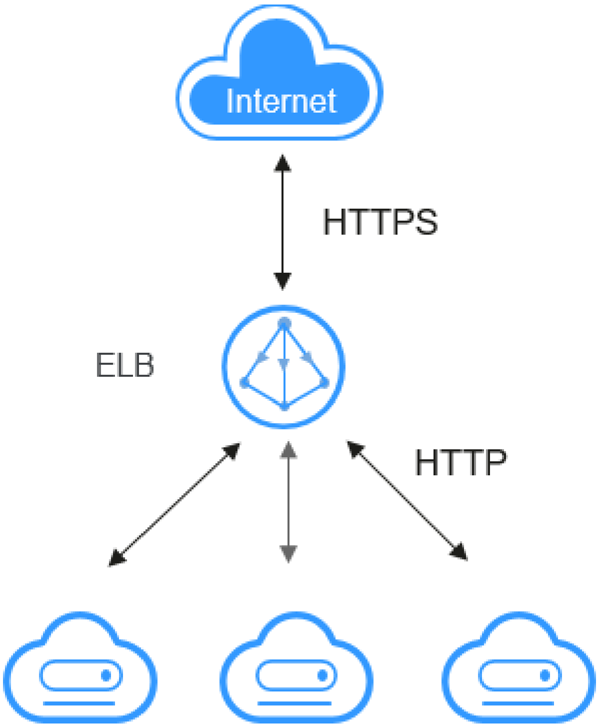
- **AAD** ensures the continuity of important enterprise services. AAD offers high-defense IP addresses to provide services in place of the original server IP addresses for external systems. The malicious attacks targeting the origin servers can be diverted for scrubbing to ensure the stable running of mission-critical workloads. This service can be used to protect servers on Huawei Cloud, other clouds, and on-premises data centers.
- **WAF** keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

ELB

ELB can handle **HTTPS requests** and support SSL certificates and access logins at Layer 7.

In addition, you can configure blacklist and whitelist to manage access permissions. For details, see **Access Control**.

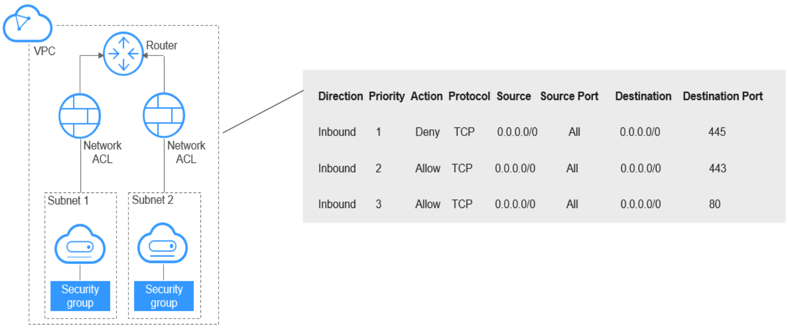
Figure 1-17 HTTPS requests



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. For details, see **Network ACL Overview**.

Figure 1-18 Network ACL



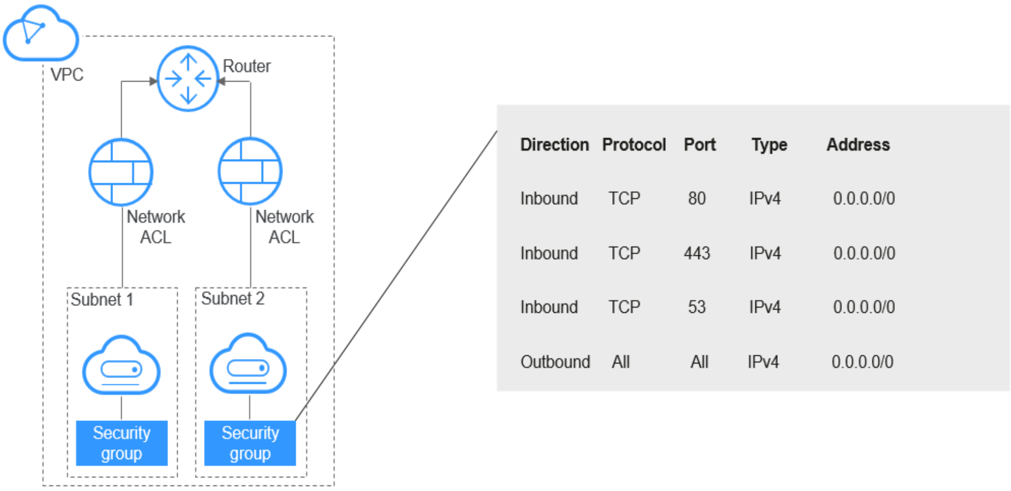
Direction	Priority	Action	Protocol	Source	Source Port	Destination	Destination Port
Inbound	1	Deny	TCP	0.0.0.0/0	All	0.0.0.0/0	445
Inbound	2	Allow	TCP	0.0.0.0/0	All	0.0.0.0/0	443
Inbound	3	Allow	TCP	0.0.0.0/0	All	0.0.0.0/0	80

Security Group

A security group implements access control for ECSs that have the same security protection requirements in a VPC. You can define inbound and outbound rules to control traffic to and from the ECSs in a security group, making your VPC more secure. For details, see **Security Group Overview**.

Security groups operate at the ECS level, whereas network ACLs operate at the subnet level. You can use network ACLs together with security groups to implement access control that is both comprehensive and fine-grained.

Figure 1-19 Security group



Direction	Protocol	Port	Type	Address
Inbound	TCP	80	IPv4	0.0.0.0/0
Inbound	TCP	443	IPv4	0.0.0.0/0
Inbound	TCP	53	IPv4	0.0.0.0/0
Outbound	All	All	IPv4	0.0.0.0/0

VPC Flow Log

A VPC flow log records information about traffic going to and from your VPC. VPC flow logs help you monitor network traffic, analyze network attacks, and determine whether security group and network ACL rules require modification.

You can create flow logs to record traffic information about VPCs, subnets, or NICs to identify attack traffic or traffic discarded by security groups or network ACLs. You can view flow logs on the LTS console or in OBS buckets. These flow logs can be analyzed by mainstream log analysis tools. For details, see **VPC Flow Log Overview**.

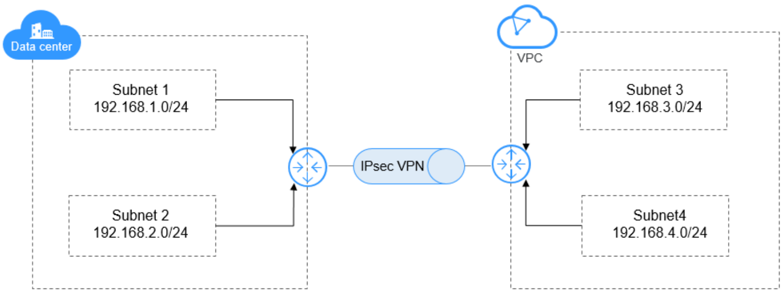
The following is an example flow log record:

```
<version> <project-id> <interface-id>  <srcaddr>      <dstaddr>       <srcport>   <dstport>   <protocol>
<packets>  <bytes>  <start>      <end>       <action>   <log-status>
1         *          *          192.168.0.59   192.168.0.218   22         39074      6          20         3997
1588743886   1588744486  ACCEPT     OK
1         *          *          192.168.0.59   192.168.0.218   22         39082      6          20         3997
1588743886   1588744486  ACCEPT     OK
1         *          *          192.168.0.218  192.168.0.59    39074      22         6          26         4033
1588743886   1588744486  ACCEPT     OK
1         *          *          192.168.0.218  192.168.0.59    39082      22         6          24         4117
1588743886   1588744486  ACCEPT     OK
```

VPN

VPN establishes a secure, encrypted communication tunnel between your on-premises data center and your VPC, quickly extending resources from your data center to Huawei Cloud.

Figure 1-20 Establishing an encrypted communication tunnel

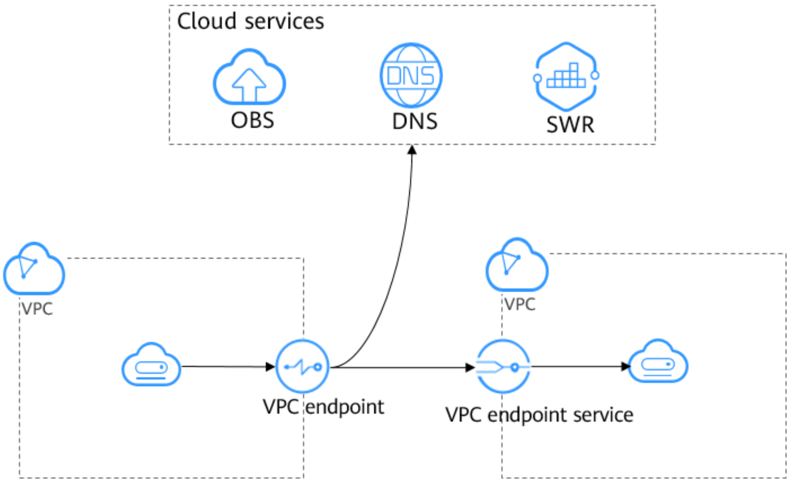


VPCEP

VPCEP provides secure and private channels to connect your VPCs to VPC endpoint services, including Huawei Cloud services or your private services, without having to use EIPs.

The access is unidirectional.

Figure 1-21 Establishing a private channel



1.4 Network Monitoring

Huawei Cloud monitors the following network resources:

EIP and Bandwidth

By monitoring the inbound bandwidth, outbound bandwidth, bandwidth usage, inbound traffic, and outbound traffic, you can know the quality of the EIP and bandwidth in real time. In addition, you can set alarm rules to automatically generate alarms when a metric exceeds the threshold, ensuring network quality.

For details, see **Supported Metrics**.

Traffic in a VPC

A VPC flow log records information about traffic going to and from your VPC. VPC flow logs help you monitor network traffic, analyze network attacks, and determine whether security group and network ACL rules require modification.

You can create flow logs to record traffic information about VPCs, subnets, or NICs to identify attack traffic or traffic discarded by security groups or network ACLs. You can view flow logs on the LTS console or in OBS buckets. These flow logs can be analyzed by mainstream log analysis tools.

The following is an example flow log record:

```
<version> <project-id> <interface-id>  <srcaddr>      <dstaddr>       <srcport>   <dstport>   <protocol>
<packets>  <bytes>  <start>      <end>       <action>   <log-status>
1         *           *              192.168.0.59   192.168.0.218   22         39074       6          20         3997
1588743886   1588744486  ACCEPT     OK
1         *           *              192.168.0.59   192.168.0.218   22         39082       6          20         3997
1588743886   1588744486  ACCEPT     OK
1         *           *              192.168.0.218  192.168.0.59    39074       22         6          26         4033
1588743886   1588744486  ACCEPT     OK
1         *           *              192.168.0.218  192.168.0.59    39082       22         6          24         4117
1588743886   1588744486  ACCEPT     OK
```

2 What Is Virtual Private Cloud?

Overview

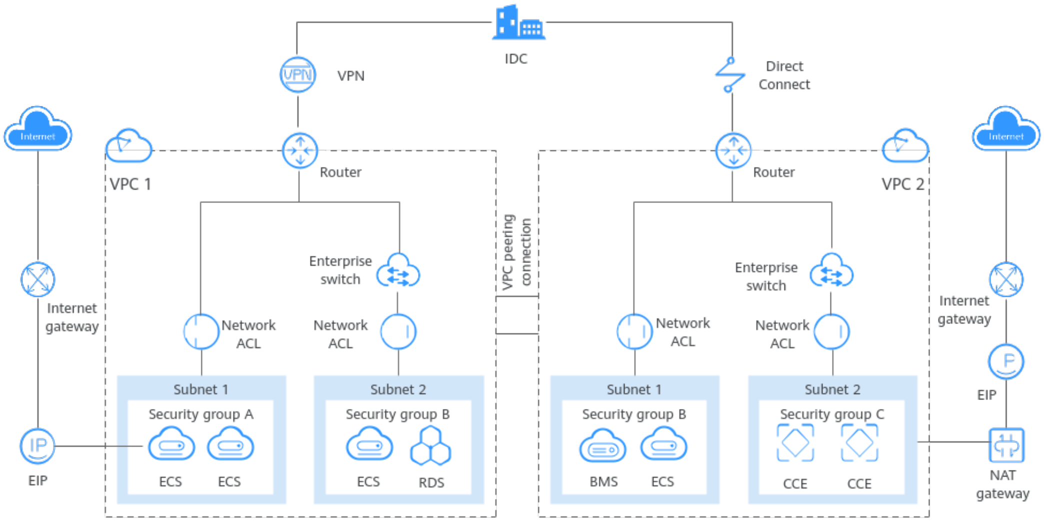
The Virtual Private Cloud (VPC) service enables you to provision logically isolated virtual private networks for cloud resources, such cloud servers, containers, and databases. You can create custom subnets, security groups, network ACLs, and assign EIPs and bandwidths. With Direct Connect or Virtual Private Network (VPN), you can connect your VPCs to an on-premises data center.

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 product architecture consists of VPC components, security features, and VPC connectivity options.

Figure 2-1 Architecture



VPC Components

Each VPC consists of a private CIDR block, route tables, and at least one subnet.

- Private CIDR blocks: When creating a VPC, you need to specify the private CIDR block used by the VPC. The VPC service supports the following CIDR blocks: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, and 192.168.0.0 – 192.168.255.255
- Subnets: Cloud resources, such as cloud servers and databases, must be deployed in subnets. After you create a VPC, you can divide the VPC into one or more subnets. Each subnet must be within the VPC. For more information, see **Subnet**.
- Route tables: When you create a VPC, the system automatically generates a default route table. The route table ensures that all subnets in the VPC can communicate with each other. If the routes in the default route table cannot meet application requirements (for example, if there is an ECS without an elastic IP address (EIP) bound that needs to access the Internet), you can create a custom route table. For more information, see **Route Table Overview**.

Security Features

Security groups and network ACLs ensure the security of cloud resources deployed in a VPC. A security group acts as a virtual firewall and has a collection of access control rules for cloud resources, such as cloud servers, containers, and databases, that have the same security requirements and that are mutually trusted. After a security group is created, you can create various access rules for the security group, these rules will apply to all cloud resources added to this security group. For more information, see **Security Group Overview**. A network ACL can be associated with subnets that have the same access control requirements. You can add rules to precisely control inbound and outbound traffic at the subnet level. For more information, see **Network ACL Overview**.

VPC Connectivity

Huawei Cloud provides multiple VPC connectivity options to meet different requirements. For details, see **Application Scenarios**.

- VPC Peering allows two VPCs in the same region to communicate with each other using private IP addresses.
- Elastic IP or NAT Gateway allows ECSs in a VPC to communicate with the Internet.
- Virtual Private Network (VPN), Cloud Connect, or Direct Connect can connect a VPC to your data center.

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** 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**.

3 Product Advantages

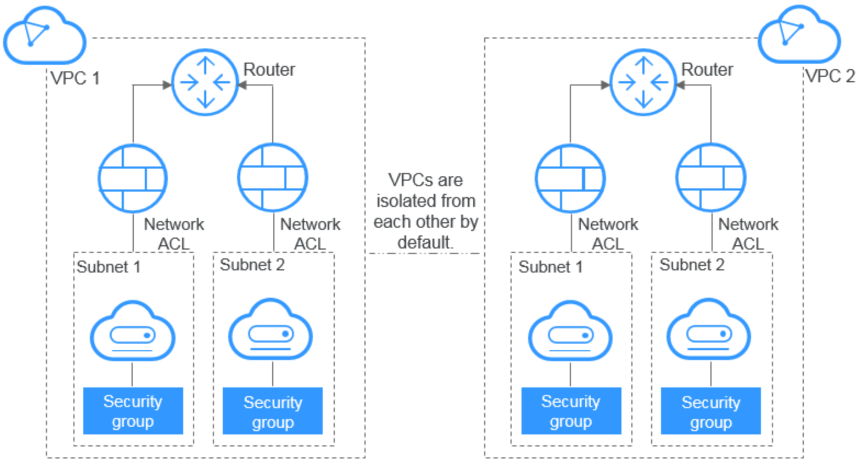
Flexible Configuration

You can create VPCs, add subnets, specify IP address ranges, and configure DHCP and 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 3-1 Secure and Reliable



Seamless Interconnectivity

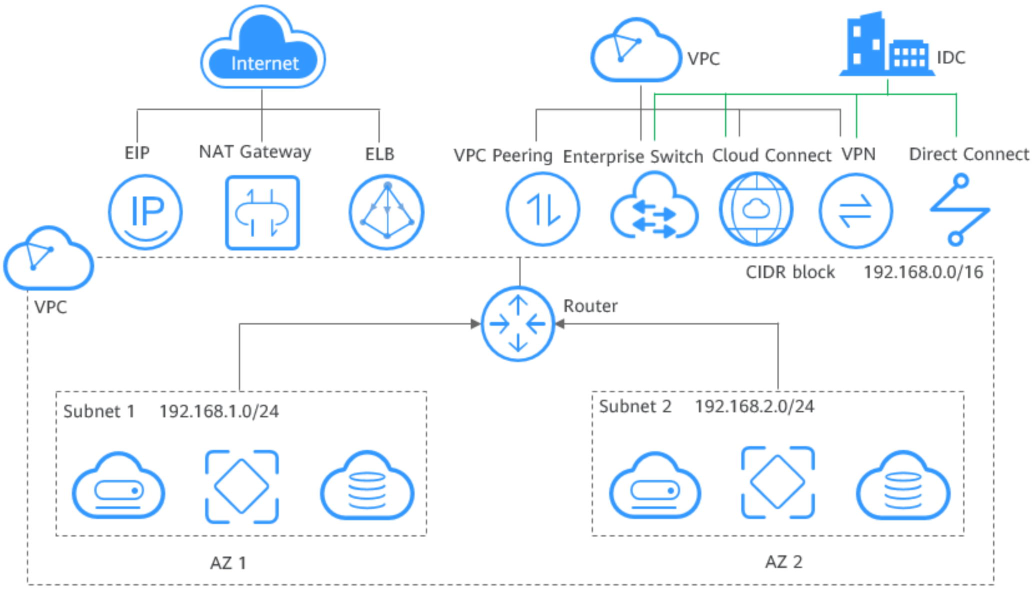
By default, instances in a VPC cannot access the Internet. You can use EIPs, load balancers, NAT gateways, VPN connections, and Direct Connect connections to enable access to or from the Internet.

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 3-2 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 3-1 lists the advantages of a VPC over a traditional IDC.

Table 3-1 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.

4 Application Scenarios

Dedicated Networks on Cloud

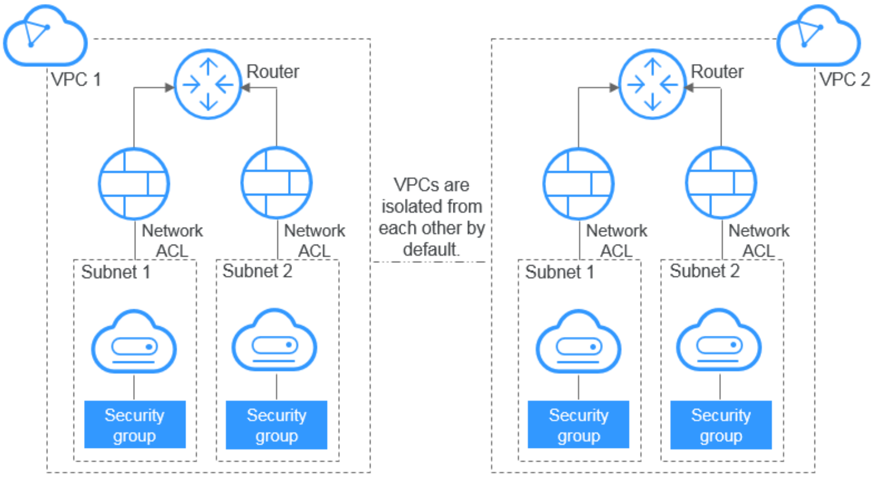
Scenario

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 4-1 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 provided by the ELB service to evenly distribute traffic across multiple ECSs.

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

Table 4-1 Accessing the Internet

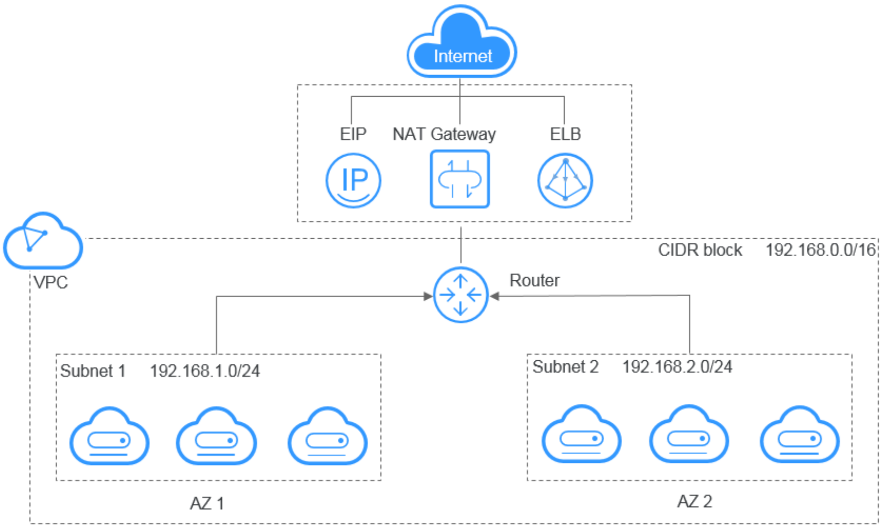
Cloud Service	Application Scenario	Description	Related Operations
EIP	Single ECS accesses the Internet.	You can assign an EIP and bind it to an ECS so that the ECS can access the Internet or provide services accessible from the Internet. You can unbind the EIP from the ECS to disable access at any time. 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 4-2 Web application or website hosting



Web Application Access Control

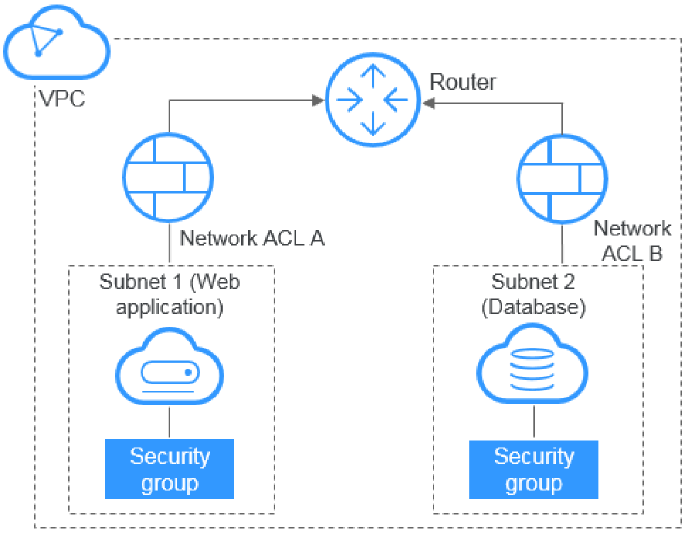
Scenario

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 4-3 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 4-2 Connecting VPCs

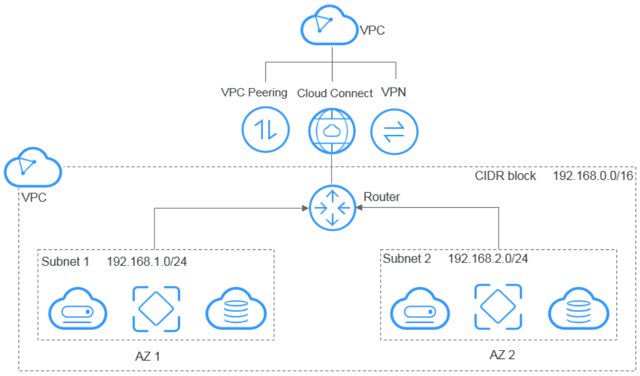
Cloud Service	Application Scenario	Description	Related Operations
VPC Peering	Connect VPCs in the same region.	You can request a VPC peering connection with another VPC in your account or in another account, but the two VPCs must be in the same region. VPC peering connections are free.	**Creating a VPC Peering Connection with Another VPC in Your Account** **Creating a VPC Peering Connection with a VPC in Another Account**
Cloud Connect	Connect VPCs in different regions.	Cloud Connect allows you to connect two VPCs in the same account or in different accounts even if they are in different regions.	**Communication Between VPCs Across Regions**

Cloud Service	Application Scenario	Description	Related Operations
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.	**Connecting to a VPC Through a VPN**

Related Services

ECS, Cloud Connect, and VPN

Figure 4-4 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.

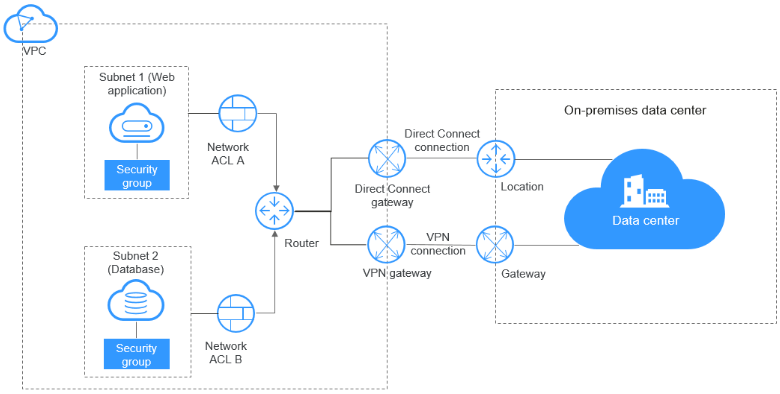
Table 4-3 Connecting to an on-premises data center

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.	**Connecting to a VPC Through a VPN** **Using an Enterprise Switch to Allow an On-premise Data Center and a VPC to Communicate at Layer 2**
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** **Using an Enterprise Switch to Allow an On-premise Data Center and a VPC to Communicate at Layer 2**

Related Services

Cloud Connect, ECS, Direct Connect, and VPN

Figure 4-5 Hybrid cloud deployment



5 Functions

Table 5-1 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 5-1 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, add a secondary CIDR block to a VPC, remove a secondary CIDR block from a VPC, 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**.
	VPC Flow Log	A VPC flow log records information about the traffic going to and from a VPC. VPC flow logs help you monitor network traffic, analyze network attacks, and determine whether security group and network ACL rules require modification. You can create, view, enable, disable, and delete VPC flow logs. For details, see **VPC Flow Log Overview**.
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**.

Category	Function	Description
	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**.
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**.

Category	Function	Description
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.
Tag	Tag Management	Tags help you identify and manage cloud resources. You can manage VPC tags, subnet tags, and EIP 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.

6 Security

6.1 Shared Responsibilities

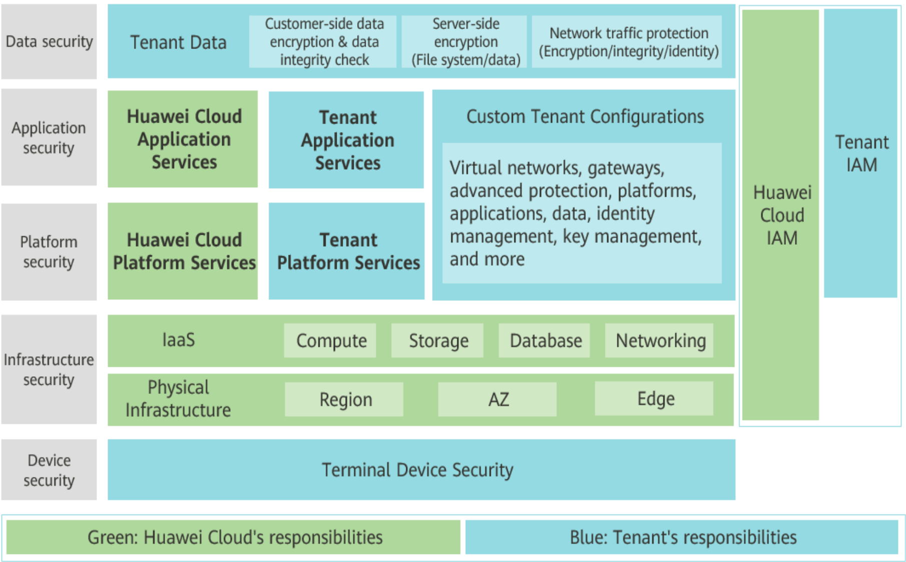
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 6-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 6-1 Huawei Cloud shared security responsibility model


Data security
Tenant Data
Customer-side data encryption & data integrity check
Server-side encryption (File system/data)
Network traffic protection (Encryption/integrity/identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Custom Tenant Configurations
Virtual networks, gateways, advanced protection, platforms, applications, data, identity management, key management, and more
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
IaaS
Compute
Storage
Database
Networking
Physical Infrastructure
Region
AZ
Edge
Device security
Terminal Device Security
Huawei Cloud IAM
Tenant IAM
Green: Huawei Cloud's responsibilities
Blue: Tenant's responsibilities

6.2 Identity Authentication and Access Control

Identity Authentication

Identity and Access Management (IAM) enables you to easily manage users and control their access to Huawei Cloud services and resources.

You can use IAM to control access to your VPC resources. IAM permissions define which actions on your cloud resources are allowed or denied.

After creating an IAM user, the administrator needs to add it to a user group and grant the permissions required by VPC to the user group. Then, all users in this group automatically inherit the granted permissions.

- **IAM Functions**
- **Permissions**

Access Control

- **Security Groups**

  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 within a VPC. After a security group is created, you can create various access rules for the security group, these rules will apply to all cloud resources added to this security group.

  You can create and delete security groups, add, replicate, modify, delete, import or export security group rules, view or change the security group of an ECS, and add ECSs to or remove them from a security group.

  You can define access rules for a security group. Then these rules will apply to all cloud resources added to this security group.

  For details, see **Security Group Overview**.

- **Network ACLs**

  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, add, modify, change the sequence of, enable, disable, and delete network ACL rules.

  You can define network ACL rules to control traffic in and out of the subnets.

  For details, see **Network ACL Overview**.

6.3 Auditing and Logging

Auditing

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

After CTS is enabled, it can record VPC operations.

- If you want to enable and configure CTS, refer to **CTS Getting Started**.
- If you want to know supported operations on VPCs, refer to **Supported VPC Operations**.
- If you want to view traces, refer to **Viewing Traces**.

Logging

A VPC flow log records information about traffic going to and from your VPC. VPC flow logs help you monitor network traffic, analyze network attacks, and determine whether security group and network ACL rules require modification.

- **VPC Flow Log Overview**
- **Creating a VPC Flow Log**

6.4 Risk Monitoring

Cloud Eye is a multi-dimensional resource monitoring platform. You can use Cloud Eye to monitor the utilization of service resources, track the running status of cloud services, configure alarm rules and notifications, and quickly respond to resource changes.

With Cloud Eye, you can view the bandwidth and EIP usage. You can also create alarm rules and configure monitoring thresholds and alarm notifications. This will ensure you learn about VPC resource status in a timely manner.

- **What Is Cloud Eye?**
- **Supported Metrics**
- **Viewing Metrics**

7 Notes and Constraints

Table 7-1 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 7-1 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 network ACLs per region	**Yes**
Maximum number of IP address groups 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

8 VPC and Other Services

Figure 8-1 shows the relationship between VPC and other services.

Figure 8-1 VPC and other services

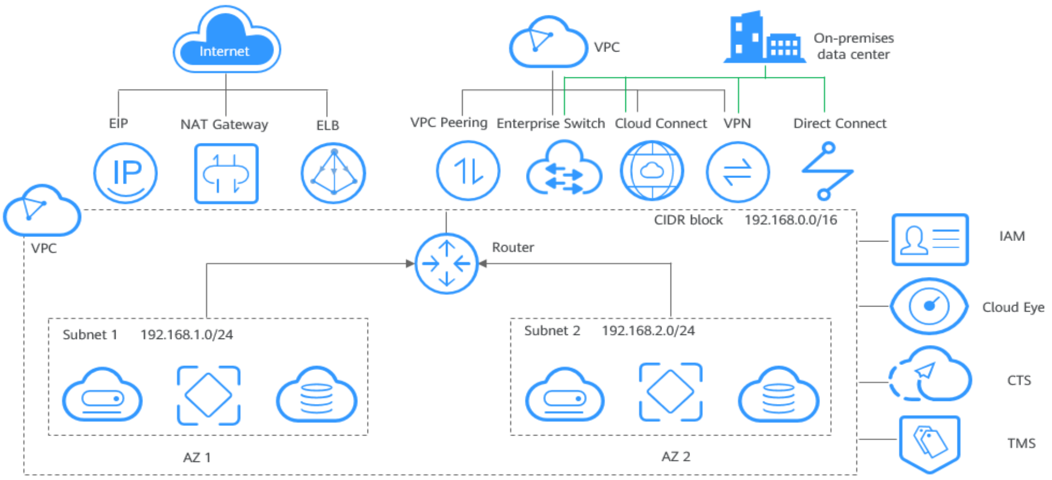


Table 8-1 Related services

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**

9 Billing

Table 9-1 describes the billing details of VPC and its related resources.

Table 9-1 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
IP address group	Free
Security group	Free
Network ACL	Free
VPC flow log	Free
EIP and bandwidth	If you use EIPs and bandwidth, you need to pay for their prices. ● EIP: reservation price ● Fixed bandwidth: price of dedicated bandwidth, shared bandwidth, and shared data package 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.

10 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 (for example, **ap-southeast-1**) in the specified regions (for example, **CN-Hong Kong**), 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 10-1 lists all the system-defined permissions for VPC.

Table 10-1 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 10-2 lists the common operations supported by system-defined permissions for VPC.

Table 10-2 Common operations supported by system-defined permissions

Operation	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Creating a VPC	x	√	√
Modifying a VPC	x	√	√
Deleting a VPC	x	√	√

Operation	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Viewing VPC information	√	√	√
Creating a subnet	x	√	√
Viewing subnet information	√	√	√
Modifying a subnet	x	√	√
Deleting a subnet	x	√	√
Creating a security group	x	x	√
Viewing security group information	√	x	√
Modifying a security group	x	x	√
Deleting a security group	x	x	√
Adding a security group rule	x	x	√
Viewing a security group rule	√	x	√
Modifying a security group rule	x	x	√
Deleting a security group rule	x	x	√
Creating a network ACL	x	√	√
Viewing a network ACL	√	√	√

Operation	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Modifying a network ACL	x	√	√
Deleting a network ACL	x	√	√
Adding a network ACL rule	x	√	√
Modifying a network ACL rule	x	√	√
Deleting a network ACL rule	x	√	√
Creating a VPC peering connection	x	√	√
Modifying a VPC peering connection	x	√	√
Deleting a VPC peering connection	x	√	√
Querying a VPC peering connection	√	√	√
Accepting a VPC peering connection request	x	√	√
Rejecting a VPC peering connection request	x	√	√
Creating a route table	x	√	√
Deleting a route table	x	√	√
Modifying a route table	x	√	√

Operation	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Associating a route table with a subnet	x	√	√
Adding a route	x	√	√
Modifying a route	x	√	√
Deleting a route	x	√	√
Creating a VPC flow log	x	√	√
Viewing a VPC flow log	√	√	√
Enabling or disabling a VPC flow log	x	√	√
Deleting a VPC flow log	x	√	√

Helpful Links

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

11 Basic Concepts

11.1 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**.

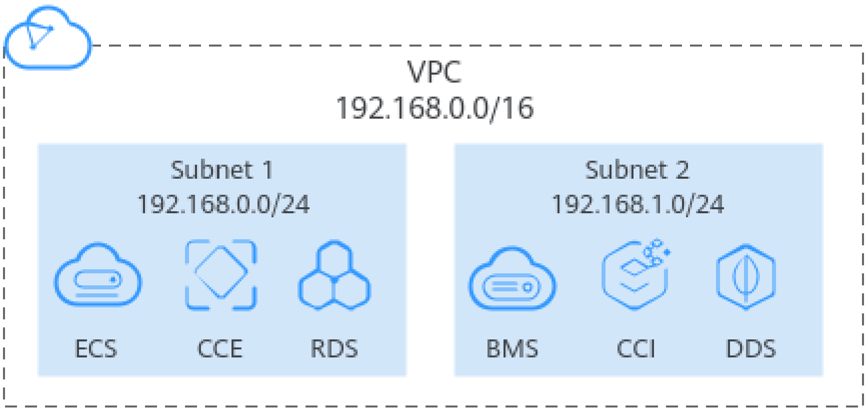
  A subnet mask can be between the netmask of its VPC CIDR block and /28 netmask. If a VPC CIDR block is 10.0.0.0/16, its subnet mask can between 16 to 28.

  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 10.0.3.0/24 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 11-1 Subnet

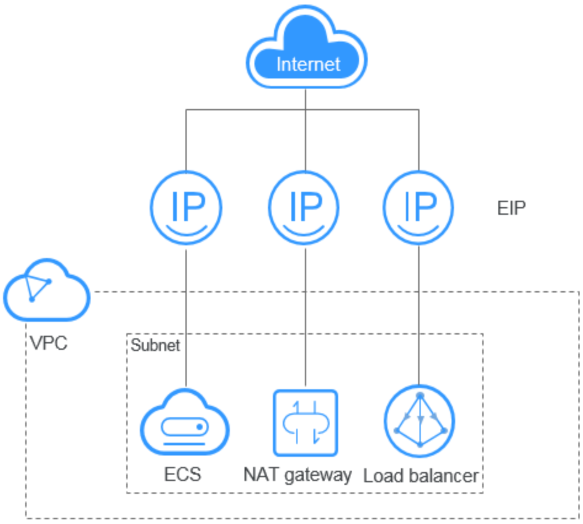


11.2 Elastic IP

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 11-2 Accessing the Internet using an EIP



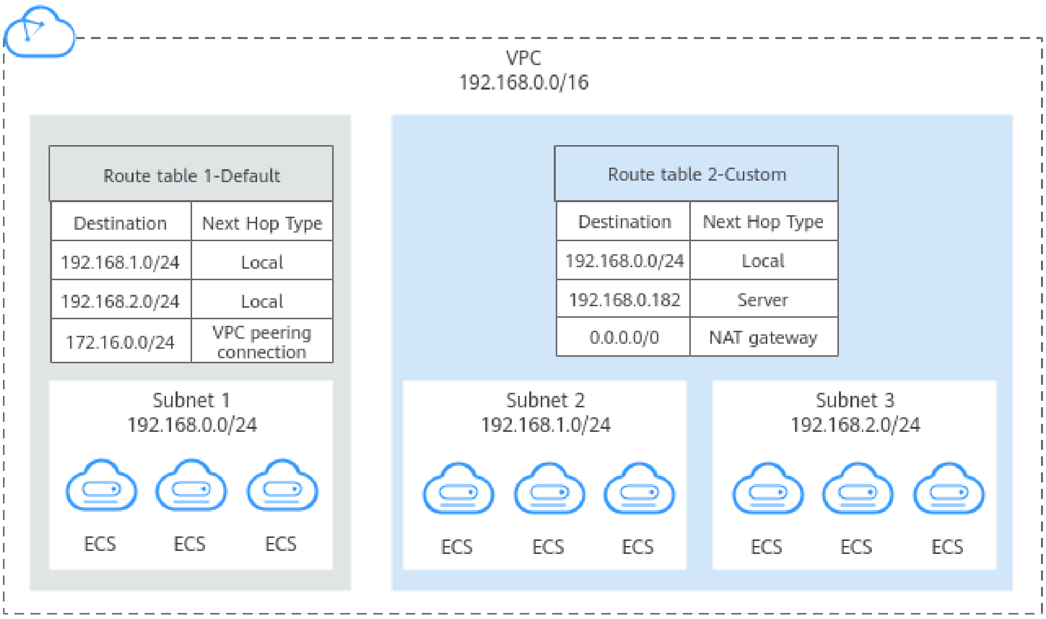
11.3 Route Table

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 11-3 Route tables



Route table 1-Default

Destination	Next Hop Type
192.168.1.0/24	Local
192.168.2.0/24	Local
172.16.0.0/24	VPC peering connection

Route table 2-Custom

Destination	Next Hop Type
192.168.0.0/24	Local
192.168.0.182	Server
0.0.0.0/0	NAT gateway

- 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 VPN, Cloud Connect, 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 11-1** 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 11-1 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.	● Default route table ● Custom route table
VPN gateway	Traffic intended for the destination is forwarded to a VPN gateway.	Custom route table

Next Hop Type	Description	Supported Route Table
Direct Connect gateway	Traffic intended for the destination is forwarded to a Direct Connect gateway.	Custom route table
Cloud connection	Traffic intended for the destination is forwarded to a cloud connection.	Custom route table
Supplementary network interface	Traffic intended for the destination is forwarded to the supplementary network interface of an ECS in the VPC.	● Default route table ● Custom 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.

11.4 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 create various access rules for the security group and these rules will apply to all cloud resources added to this security group.

Like whitelists, security group rules work as follows:

- Inbound rules control incoming traffic to instances in the security group.

  If an inbound request matches the source in an inbound security group rule with **Action** set to **Allow**, the request is allowed and other requests are denied.

  By default, you do not need to configure deny rules in the inbound direction because requests that do not match allow rules will be denied.

- Outbound rules control outgoing traffic from instances in the security group.

  If the destination of an outbound security group rule with **Action** set to **Allow** is 0.0.0.0/0, all outbound requests are allowed.

  0.0.0.0/0 represents all IPv4 addresses.

  ::/0 represents all IPv6 addresses.

Table 11-2 uses custom security group sg-AB as an example to describe its inbound and outbound rules in detail.

Table 11-2 Rules in security group sg-AB

Direction	Action	Type	Protocol & Port	Source/ Destination	Description
Inbound	Allow	IPv4	All	Source: sg-AB	Allows ECSs in the security group to communicate with each other.
Inbound	Allow	IPv4	TCP: 22	Source: 0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 22 (SSH) for remotely logging in to Linux ECSs.

Direction	Action	Type	Protocol & Port	Source/ Destination	Description
Inbound	Allow	IPv4	TCP: 3389	Source: 0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 3389 (RDP) for remotely logging in to Windows ECSs.
Inbound	Allow	IPv4	TCP: 80	Source: 10.5.6.30/32	Allows IP address 10.5.6.30 to access ECSs in the security group over port 80.
Outbound	Allow	IPv4	All	Destination: 0.0.0.0/0	Allows access from ECSs in the security group to any IPv4 address over any port.
Outbound	Allow	IPv6	All	Destination: ::/0	Allows access from ECSs in the security group to any IPv6 address over any port.

11.5 VPC Peering Connection

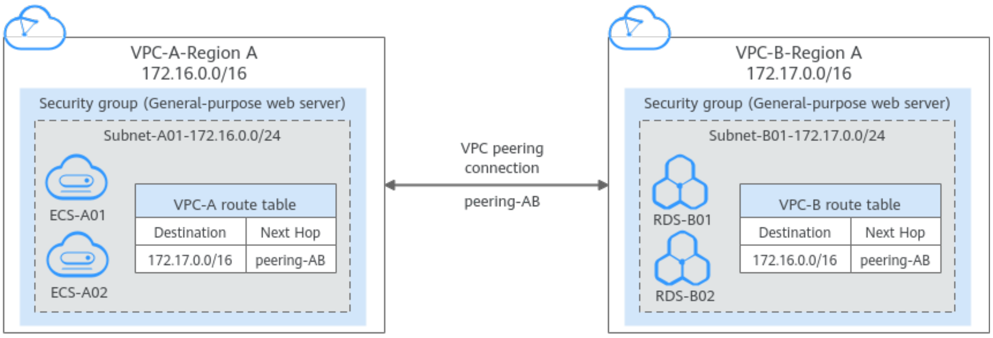
A VPC peering connection is a networking connection that connects two VPCs for them to communicate using private IP addresses. The VPCs to be peered can be in the same account or different accounts, but must be in the same region.

- If you want to connect VPCs in different regions, use **Cloud Connect**.
- You can use VPC peering connections to build different networks. For details, see **VPC Peering Connection Usage Examples**.

Figure 11-4 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.

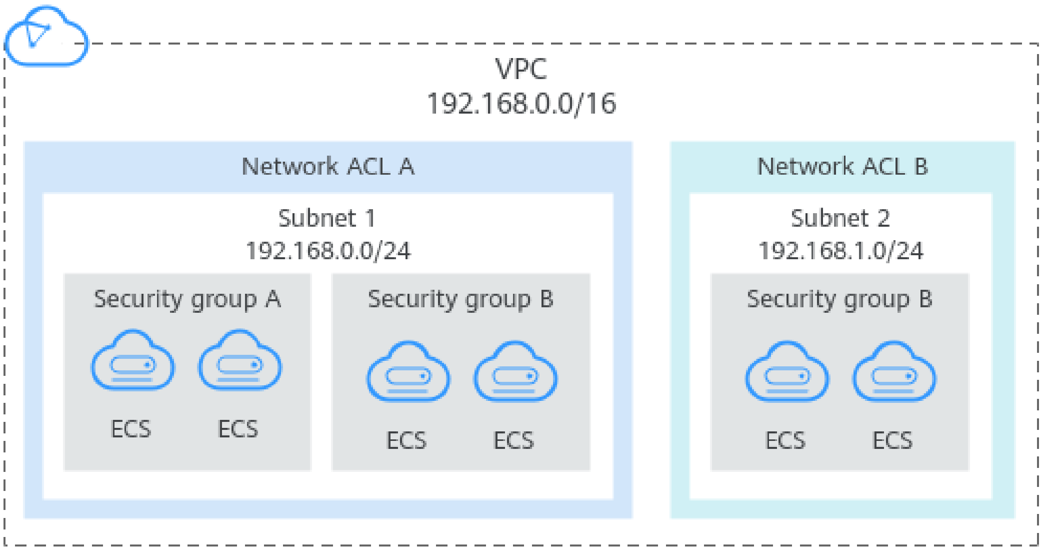
Figure 11-4 VPC peering connection network diagram



11.6 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 11-5 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.

Network ACL Basics

- Your VPC does not come with a network ACL, but you can create a network ACL and associate it with a VPC subnet if required. By default, each network ACL denies all inbound traffic to and outbound traffic from the associated subnet until you add rules.
- You can associate a network ACL with multiple subnets. However, a subnet can only be associated with one network ACL at a time.
- Each newly created network ACL is in the **Inactive** state until you associate subnets with it.
- Network ACLs are stateful. If the network ACL allows outbound traffic and you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound network ACL rules. Similarly, if inbound traffic is allowed, responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

  The timeout period of connection tracking varies according to the protocol. The timeout period of a TCP connection in the established state is 600s, and the timeout period of an ICMP connection is 30s. For other protocols, if packets are received in both directions, the connection tracking timeout period is 180s. If one or more packets are received in one direction but no packet is received in the other direction, the connection tracking timeout period is 30s. For protocols other than TCP, UDP, and ICMP, only the IP address and protocol number are tracked.

Default Network ACL Rules

By default, each network ACL has preset rules that allow the following packets:

- Packets whose source and destination are in the same subnet.
- Broadcast packets with the destination 255.255.255.255/32, which is used to configure host startup information.
- Multicast packets with the destination 224.0.0.0/24, which is used by routing protocols.
- Metadata packets with the destination 169.254.169.254/32 and TCP port number 80, which is used to obtain metadata.
- Packets from CIDR blocks that are reserved for public services (for example, packets with the destination 100.125.0.0/16).
- A network ACL denies all traffic in and out of a subnet excepting the preceding packets. **Table 11-3** shows the default rules. You cannot modify or delete the default rules.

Table 11-3 Default network ACL rules

Direction	Priority	Action	Protocol	Source	Destination	Description
Inbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all inbound traffic.
Outbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all outbound traffic.

Rule Priorities

- Each network ACL rule has a priority value where a smaller value corresponds to a higher priority. Any time two rules conflict, the rule with the higher priority is the one that gets applied. The rule whose priority value is an asterisk (*) has the lowest priority.
- If multiple network ACL rules conflict, only the rule with the highest priority takes effect. If you need a rule to take effect before or after a specific rule, you can insert that rule before or after the specific rule.

Application Scenarios

- If the application layer needs to provide services for users, traffic must be allowed to reach the application layer from all IP addresses. However, you also need to prevent illegal access from malicious users.

Solution: You can add network ACL rules to deny access from suspect IP addresses.

- How can I isolate ports with identified vulnerabilities? For example, how do I isolate port 445 that can be exploited by WannaCry worm?

  Solution: You can add network ACL rules to deny access traffic from a specific port and protocol, for example, TCP port 445.

- No defense is required for the communication within a subnet, but access control is required for communication between subnets.

  Solution: You can add network ACL rules to control traffic between subnets.

- For frequently accessed applications, a security rule sequence may need to be adjusted to improve performance.

  Solution: A network ACL allows you to adjust the rule sequence so that frequently used rules are applied before other rules.

11.7 Virtual IP Address

A virtual IP address can be shared among multiple ECSs. An ECS can have both private and virtual IP addresses, and you can access the ECS through either IP address. A virtual IP address has the same network access capabilities as a private IP address, including layer 2 and layer 3 communication in VPCs, access between VPCs using VPC peering connections, as well as access through EIPs, VPN connections, and Direct Connect connections.

You can bind ECSs deployed in active/standby mode with the same virtual IP address, 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.

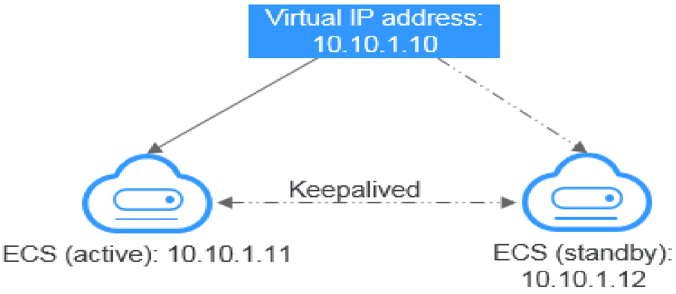
Networking

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

  If you want to improve service availability and avoid single points of failure, you can deploy ECSs in the active/standby mode or deploy one active ECS and multiple standby ECSs. In this arrangement, the ECSs all use the same virtual IP address. If the active ECS becomes faulty, a standby ECS takes over services from the active ECS and services continue uninterrupted.

Figure 11-6 Networking diagram of the HA mode

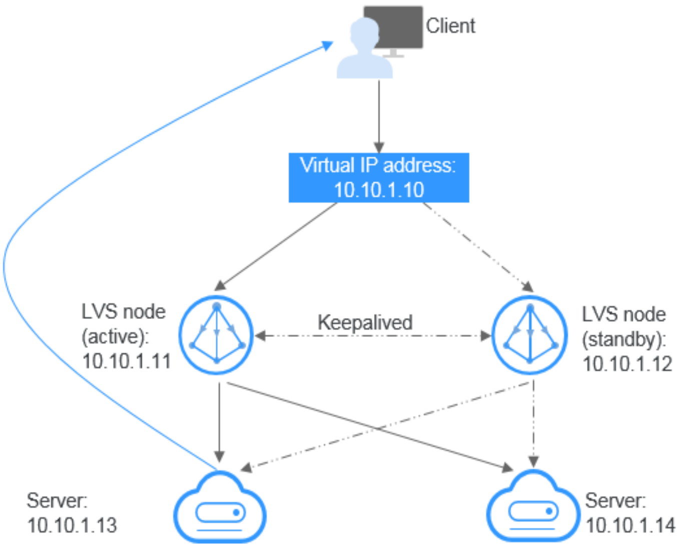


- In this configuration, a single virtual IP address is bound to two ECSs in the same subnet.
- Keepalived is then used to configure the two ECSs to work in the active/ standby mode. Follow industry standards for configuring Keepalived. The details are not included here.

- **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 11-7 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 mode. 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. The VPC peering connection is needed so that the VPCs in the same region can communicate with each other.

11.8 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.
- A supplementary 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.

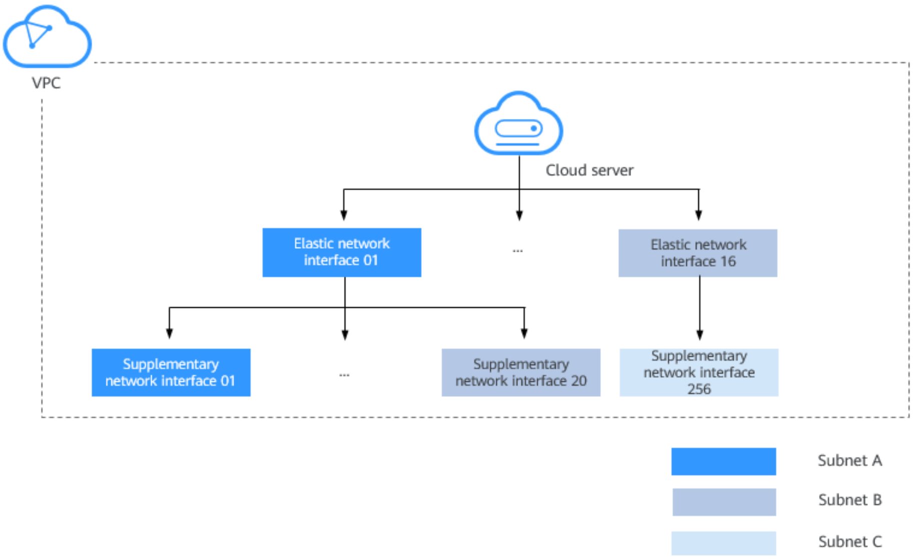
11.9 Supplementary Network Interface

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 11-8** shows the networking diagram.

Figure 11-8 Supplementary network interface networking diagram


VPC
Cloud server
Elastic network interface 01
...
Elastic network interface 16
Supplementary network interface 01
...
Supplementary network interface 20
Supplementary network interface 256
Subnet A
Subnet B
Subnet C

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.

11.10 IP Address Group

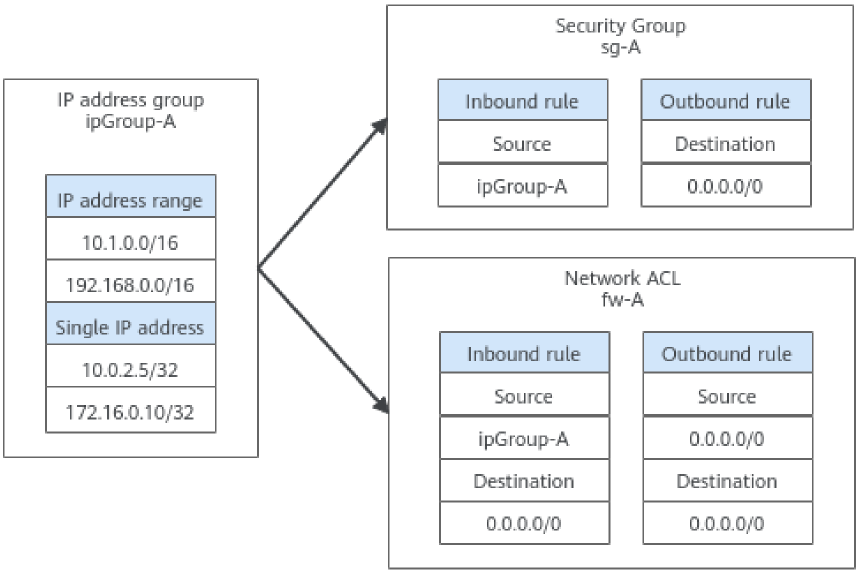
An IP address group is a collection of IP addresses. It can be associated with security groups and network ACLs to simplify IP address configuration and management.

You can add IP address ranges and IP addresses that need to be managed in a unified manner to an IP address group. An IP address group can work together with different cloud resources. **Table 11-4** lists the resources that can be associated with an IP address group.

Table 11-4 Resources that can be associated with an IP address group

Resource	Description	Example
Security group	The **Source** or **Destination** of a security group rule can be set to **IP address group**.	As shown in **Figure 11-9**, the inbound rule of security group sg-A uses IP address group ipGroup-A as the source.
Network ACL	The **Source** or **Destination** of a network ACL is set to **IP address group**.	As shown in **Figure 11-9**, the inbound rule of network ACL fw-A uses IP address group ipGroup-A as the source.

Figure 11-9 Using IP address group



11.11 Region and AZ

Concept

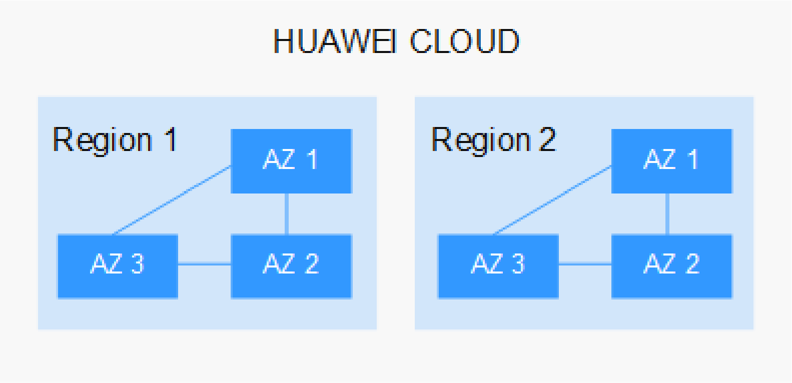
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- 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. AZs within a region are interconnected using high-speed optical fibers, to support cross-AZ high-availability systems.

Figure 11-10 shows the relationship between regions and AZs.

Figure 11-10 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see **Huawei Cloud Global Regions**.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  It is recommended that you select the closest region for lower network latency and quick access.

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

    NOTE

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

- Resource price

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

Selecting an AZ

When 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.

Regions and Endpoints

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