Virtual Private Cloud

User Guide (ME-Abu Dhabi Region)

Issue	01
Date	2020-11-05

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 Service Overview 1
1.1 What Is Virtual Private Cloud? 1
1.2 Application Scenarios 2
1.3 VPC Connectivity 2
1.4 VPC and Other Services 3
1.5 Basic Concepts 4
1.5.1 Subnet 4
1.5.2 Elastic IP 4
1.5.3 Route Table 5
1.5.4 Security Group 7
1.5.5 VPC Peering Connection 8
1.5.6 Network ACL 10
1.5.7 Virtual IP Address 12
1.5.8 Region and AZ 14
2 Getting Started 16
2.1 Typical Application Scenarios 16
2.2 Configuring a VPC for ECSs That Do Not Require Internet Access 16
2.2.1 Overview 16
2.2.2 Step 1: Create a VPC 18
2.2.3 Step 2: Create a Subnet for the VPC 23
2.2.4 Step 3: Create a Security Group 26
2.2.5 Step 4: Add a Security Group Rule 28
2.3 Configuring a VPC for ECSs That Access the Internet Using EIPs 31
2.3.1 Overview 31
2.3.2 Step 1: Create a VPC 32
2.3.3 Step 2: Create a Subnet for the VPC 38
2.3.4 Step 3: Assign an EIP and Bind It to an ECS 41
2.3.5 Step 4: Create a Security Group 43
2.3.6 Step 5: Add a Security Group Rule 45
3 VPC and Subnet 49
3.1 Network Planning 49
3.2 VPC 52

3.2.1 Creating a VPC....52
3.2.2 Modifying a VPC....58
3.2.3 Deleting a VPC....58
3.2.4 Managing VPC Tags....59
3.2.5 Exporting VPC Information....60
3.3 Subnet....61
3.3.1 Creating a Subnet for the VPC....61
3.3.2 Modifying a Subnet....64
3.3.3 Deleting a Subnet....66
3.3.4 Managing Subnet Tags....66
3.4 IPv4 and IPv6 Dual-Stack Network....68
4 Security....70
4.1 Security Group....70
4.1.1 Security Group Overview....70
4.1.2 Default Security Groups and Security Group Rules....71
4.1.3 Security Group Configuration Examples....73
4.1.4 Creating a Security Group....76
4.1.5 Adding a Security Group Rule....77
4.1.6 Fast-Adding Security Group Rules....80
4.1.7 Replicating a Security Group Rule....81
4.1.8 Modifying a Security Group Rule....81
4.1.9 Deleting a Security Group Rule....82
4.1.10 Importing and Exporting Security Group Rules....82
4.1.11 Deleting a Security Group....83
4.1.12 Adding Instances to and Removing Them from a Security Group....83
4.1.13 Cloning a Security Group....84
4.1.14 Modifying a Security Group....85
4.1.15 Viewing the Security Group of an ECS....86
4.1.16 Changing the Security Group of an ECS....86
4.2 Network ACL....86
4.2.1 Network ACL Overview....87
4.2.2 Network ACL Configuration Examples....90
4.2.3 Creating a Network ACL....92
4.2.4 Adding a Network ACL Rule....93
4.2.5 Associating Subnets with a Network ACL....94
4.2.6 Disassociating a Subnet from a Network ACL....95
4.2.7 Changing the Sequence of a Network ACL Rule....95
4.2.8 Modifying a Network ACL Rule....96
4.2.9 Enabling or Disabling a Network ACL Rule....98
4.2.10 Deleting a Network ACL Rule....98
4.2.11 Exporting and Importing Network ACL Rules....99
4.2.12 Viewing a Network ACL....99

4.2.13 Modifying a Network ACL 100
4.2.14 Enabling or Disabling a Network ACL 100
4.2.15 Deleting a Network ACL 101
4.3 Differences Between Security Groups and Network ACLs 101
5 EIP 104
5.1 Assigning an EIP and Binding It to an ECS 104
5.2 Unbinding an EIP from an ECS and Releasing the EIP 106
5.3 Managing EIP Tags 107
5.4 Modifying EIP Bandwidth 109
5.5 Exporting EIP Information 109
6 Shared Bandwidth 110
6.1 Shared Bandwidth Overview 110
6.2 Assigning Shared Bandwidth 110
6.3 Adding EIPs to a Shared Bandwidth 111
6.4 Removing EIPs from a Shared Bandwidth 112
6.5 Modifying a Shared Bandwidth 112
6.6 Deleting a Shared Bandwidth 113
7 Route Table 114
7.1 Route Table Overview 114
7.2 Configuring an SNAT Server 117
7.3 Creating a Custom Route Table 120
7.4 Adding a Custom Route 121
7.5 Associating a Subnet with a Route Table 122
7.6 Changing the Route Table Associated with a Subnet 123
7.7 Viewing a Route Table 123
7.8 Deleting a Route Table 123
7.9 Modifying a Route 124
7.10 Deleting a Route 125
7.11 Replicating a Route 126
7.12 Exporting Route Table Information 126
8 VPC Peering Connection 127
8.1 VPC Peering Connection Creation Procedure 127
8.2 VPC Peering Connection Configuration Plans 129
8.3 Creating a VPC Peering Connection with Another VPC in Your Account 132
8.4 Creating a VPC Peering Connection with a VPC in Another Account 134
8.5 Viewing VPC Peering Connections 138
8.6 Modifying a VPC Peering Connection 138
8.7 Deleting a VPC Peering Connection 138
8.8 Viewing Routes Configured for a VPC Peering Connection 139
8.9 Deleting a VPC Peering Route 139
9 Virtual IP Address 141

9.1 Virtual IP Address Overview 141
9.2 Assigning a Virtual IP Address 144
9.3 Binding a Virtual IP Address to an EIP or ECS 144
9.4 Using an EIP to Access a Virtual IP Address 145
9.5 Using a VPN to Access a Virtual IP Address 145
9.6 Using a Direct Connect Connection to Access the Virtual IP Address 145
9.7 Using a VPC Peering Connection to Access the Virtual IP Address 146
9.8 Disabling Source and Destination Check (HA Load Balancing Cluster Scenario) 146
9.9 Releasing a Virtual IP Address 146

10 Monitoring 148
10.1 Supported Metrics 148
10.2 Viewing Metrics 150
10.3 Creating an Alarm Rule 151

11 FAQs 152
11.1 General 152
11.1.1 What Is a Quota? 152
11.2 VPC and Subnet 153
11.2.1 What Is Virtual Private Cloud? 153
11.2.2 Which CIDR Blocks Are Available to the VPC Service? 153
11.2.3 Can Subnets Communicate with Each Other? 154
11.2.4 What Subnet CIDR Blocks Are Available? 154
11.2.5 How Many Subnets Can I Create? 154
11.2.6 What Do I Do If a Subnet Cannot Be Deleted Because It Is Being Used by Other Resources? 154
11.3 EIP 155
11.3.1 Can I Bind an EIP to Multiple ECSs? 155
11.3.2 How Do I Access an ECS from the Internet After an EIP Is Bound to the ECS? 155
11.4 Bandwidth 155
11.4.1 What Is the Bandwidth Size Range? 155
11.5 Connectivity 155
11.5.1 Does a VPN Allow for Communication Between Two VPCs? 156
11.5.2 Why Cannot I Access the Internet or Internal Domain Names in the Cloud Through Domain Names When My ECS Has Multiple NICs? 156
11.5.3 What Are the Constraints Related to VPC Peering? 156
11.5.4 What Should I Do If VPCs Connected by a VPC Peering Connection Cannot Communicate with Each Other? 157
11.5.5 How Many VPC Peering Connections Can I Have? 157
11.5.6 What Are the Priorities of the Custom Route and EIP If Both Are Configured for an ECS to Enable the ECS to Access the Internet? 158
11.6 Routing 158
11.6.1 How Many Routes Can a Route Table Have? 158
11.6.2 What Are the Limitations of a Route Table? 158
11.6.3 Are There Different Routing Priorities for Direct Connect Connections and Custom Routes in the Same VPC? 158

11.6.4 Are There Different Routing Priorities of the VPN and Custom Routes in the Same VPC?.....158
11.7 Security.....158
11.7.1 Can I Change the Security Group of an ECS?.....158
11.7.2 How Many Security Groups Can I Have?.....158
11.7.3 How Do I Configure a Security Group for Multi-Channel Protocols?.....159
11.7.4 How Many Network ACLs Can I Have?.....159
11.7.5 Does a Security Group Rule or a Network ACL Rule Immediately Take Effect for Its Original Traffic After It Is Modified?.....159

A Change History.....161

1 Service Overview

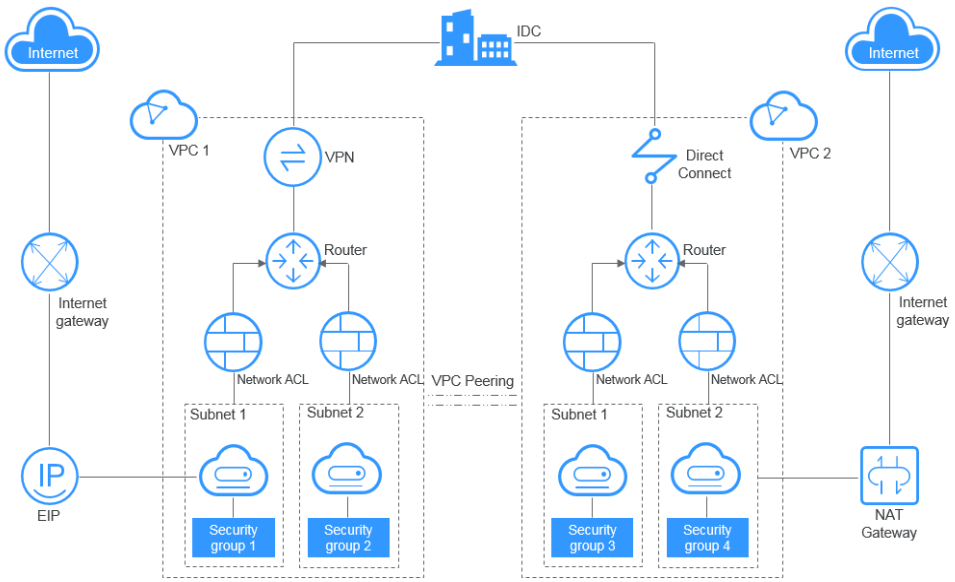
1.1 What Is Virtual Private Cloud?

Overview

The Virtual Private Cloud (VPC) service enables you to provision logically isolated, configurable, and manageable virtual networks for Elastic Cloud Servers (ECSs), improving cloud service security and simplifying network deployment.

Within your own VPC, you can create security groups and VPNs, configure IP address ranges, specify bandwidth sizes, manage the networks in the VPC, and make changes to these networks as needed, quickly and securely. You can also define rules for communication between ECSs in the same security group or in different security groups.

Figure 1-1 VPC components



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 perform operations on VPC resources directly. 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 the VPC service provided by the cloud system into a third-party system for secondary development, you can use an API to access the VPC service. For details, see the *Virtual Private Cloud API Reference*.

1.2 Application Scenarios

- Hosting web applications

  You can host web applications and websites in a VPC and use the VPC as a regular network. With EIPs, you can connect ECSs running your web applications to the Internet. A VPN gateway is used to establish a VPN tunnel between the web applications and the service system on the cloud, ensuring high-speed communication between the website and the service system.

- Hosting services that demand high security

  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 run database servers in subnets that are not publicly accessible. This arrangement ensures high security.

- Extending your corporate network into the cloud

  You can establish a VPN connection between a VPC and a traditional data center to use the ECSs and block storage resources. Applications can be migrated to the cloud and additional web servers can be quickly deployed as needed when there is a spike in demand for computing resources. This way, less money has to be spent on IT and O&M and data is kept safer than in a traditional arrangement. A VPC can span multiple AZs, protecting from single-points-of-failure and ensuring high availability for e-commerce systems.

1.3 VPC Connectivity

You can use EIPs, load balancers, NAT gateways, VPN connections, and Direct Connect connections to access the Internet if required.

- 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 the EIPs to the 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.

- Use NAT Gateways to Enable a Large Number of ECSs to Access the Internet

  When a large number of ECSs need to access the Internet, the public cloud system provides NAT gateways for the ECSs. With NAT gateways, you do not need to assign an EIP to each ECS, which reduces management costs incurred by an excessive number of EIPs. A NAT gateway offers both the SNAT and DNAT functions. 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. SNAT supports up to 1 million concurrent connections and 30,000 new connections. 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.

- Use ELB to Connect to 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 cluster mode and provides fault tolerance for your applications by automatically balancing traffic across multiple availability zones (AZs). You can also take advantage of deep integration with Auto Scaling (AS), which enables automatic scaling based on service traffic and ensures service stability and reliability.

- Use VPN or Direct Connect to Extend Your On-premises Data Center into the Cloud over the Internet

  For customers with equipment rooms in their on-premises data centers, not all businesses of the customers will be migrated to the cloud because the customers want to reuse their legacy devices and require smooth business evolution. Then, you can use VPN or Direct Connect to interconnect your VPC and on-premises data center. A VPN connection routes traffic through the Internet, which allows you to use a private network with the price of the public network. A Direct Connect connection is a dedicated, private network connection that provides you with more efficient data transmission and more consistent network experience than Internet-based connections.

1.4 VPC and Other Services

- ECS

  The VPC service provides an isolated virtual network for ECSs. You can configure and manage the network as required. There are multiple connectivity options for ECSs to access the Internet. You can also define rules for communication between ECSs in the same security group or in different security groups.

- ELB

  ELB uses the EIPs and bandwidths associated with the VPC service.

- Cloud Eye

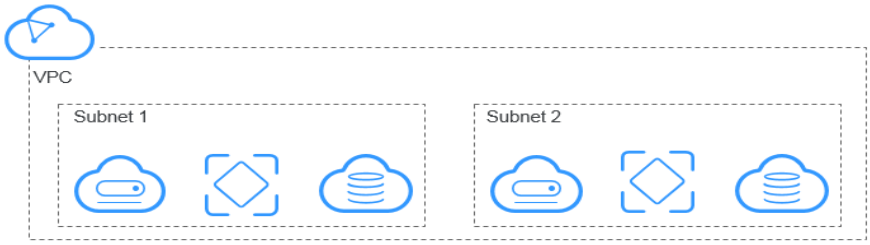
  You can use Cloud Eye to monitor the status of your VPCs without adding plug-ins.

1.5 Basic Concepts

1.5.1 Subnet

A subnet is a range of IP addresses in your VPC and provides IP address management and DNS resolution functions for ECSs in it. The IP addresses of all ECSs in a subnet belong to the subnet.

Figure 1-2 Subnet



By default, ECSs in all subnets of the same VPC can communicate with one another, but ECSs in different VPCs cannot.

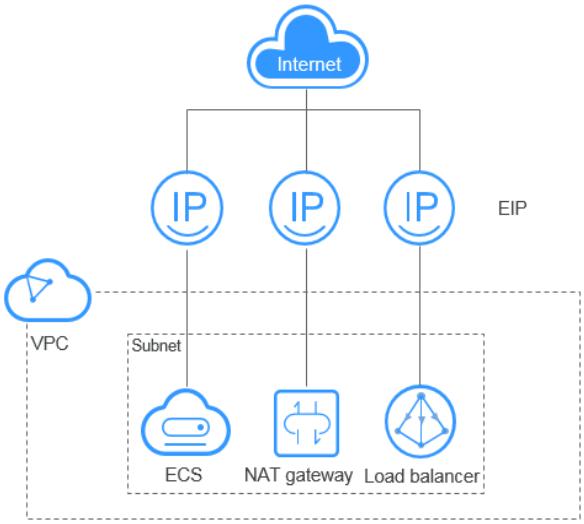
To enable ECSs in different VPCs but in the same region to communicate with one another, you can create a VPC peering connection. For details, see **1.5.5 VPC Peering Connection**.

1.5.2 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 1-3 Accessing the Internet using an EIP

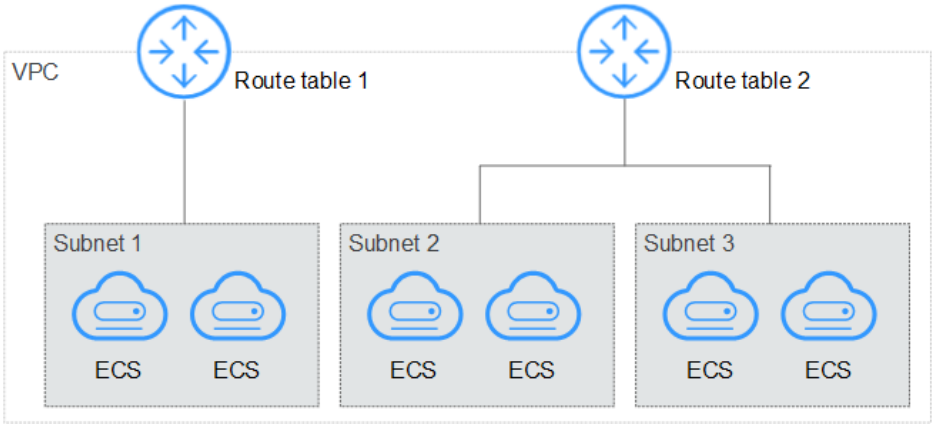


1.5.3 Route Table

Route Table

A route table contains a set of rules, called routes, that are used to control where inbound and outbound subnet traffic is forwarded within a VPC. Each subnet in a VPC must be associated with a route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Figure 1-4 Route Table



Default Route Table and Custom 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. You can add, delete, and modify routes in the default route table, but cannot delete the table. When you create a VPN connection, the default route table automatically delivers a route that cannot be deleted or

modified. If you want to modify or delete the route, you can associate your subnet with a custom route table and replicate the route to the custom route table to modify or delete it.

You can also create a custom route table and associate subnets that have the same routing requirements with this table. Custom route tables can be deleted if they are no longer required.

Route

A route is configured with the destination, next hop type, and next hop to determine where the network traffic is directed. Routes are classified into system routes and custom routes.

- System route: Routes that 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.

    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 route: A route that can be modified and deleted. 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 the network traffic is directed. **Table 1-1** lists the supported types of next hops.

Table 1-1 Next hop type

Next Hop Type	Description
ECS	Traffic intended for the destination is forwarded to an ECS in the VPC.
Extension NIC	Traffic intended for the destination is forwarded to the extension NIC of an ECS in the VPC.
VPN gateway	Traffic intended for the destination is forwarded to a VPN gateway.
Direct Connect gateway	Traffic intended for the destination is forwarded to a Direct Connect gateway.
NAT gateway	Traffic intended for the destination is forwarded to a NAT gateway.
VPC peering connection	Traffic intended for the destination is forwarded to a VPC peering connection.

Next Hop Type	Description
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.

NOTE

- When you add a custom route to a default route table, the next hop type cannot be set to VPN gateway.
- If you have to specify the destination when creating a service, a system route is delivered. If you do not need to specify a destination when creating a service, a custom route that can be modified or deleted is delivered automatically.

  For example, you do not need to specify a destination when creating a NAT gateway, the system automatically delivers a custom route that you can modify or delete. 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 a system route. If the route destination can be modified on the **Route Tables** page, the destination will be inconsistent with that configured remote subnet. To modify the destination, you can go to the specific service page to modify the remote subnet, then the route destination will be changed accordingly.

1.5.4 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. After a security group is created, you can create different access rules for the security group, these rules will apply to any ECS that the security group contains.

Your account automatically comes with a default security group. The default security group allows all outbound traffic, denies all inbound traffic, and allows all traffic between ECSs in the group. Your ECSs in this security group can communicate with each other already without adding additional rules.

Figure 1-5 illustrates how the default security group works.

Figure 1-5 Default security group

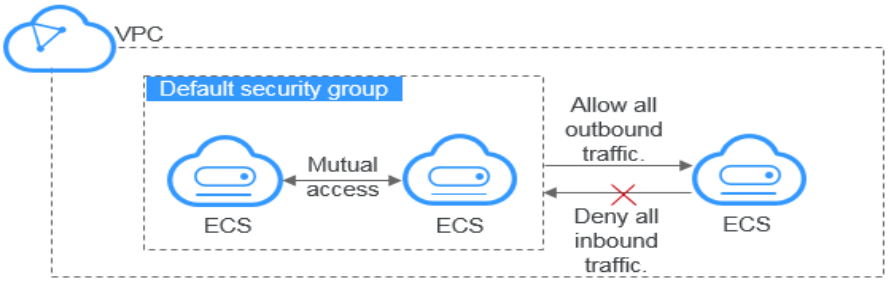


Table 1-2 describes the default rules for the default security group.

Table 1-2 Rules in the default security group

Direction	Protocol	Port/ Range	Source/ Destination	Description
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic.
Inbound	All	All	Source: the current security group (for example, sg-*xxxxx*)	Allows communication among ECSs within the security group and denies all inbound traffic (incoming data packets).
Inbound	TCP	22	Source: 0.0.0.0/0	Allows all IP addresses to access Linux ECSs over SSH.
Inbound	TCP	3389	Source: 0.0.0.0/0	Allows all IP addresses to access Windows ECSs over RDP.

You can also create custom security groups and rules as required.

NOTE

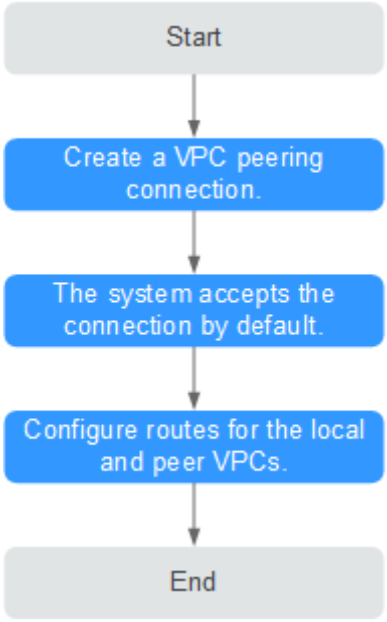
If two ECSs are in the same security group but in different VPCs, the ECSs cannot communicate with each other. To enable communications between the ECSs, use a VPC peering connection to connect the two VPCs first.

1.5.5 VPC Peering Connection

A VPC peering connection is a network connection between two VPCs in one region that enables you to route traffic between them using private IP addresses. ECSs in either VPC can communicate with each other just as if they were in the same region. You can create a VPC peering connection between your own VPCs, or between your VPC and another account's VPC within the same region. A VPC peering connection between VPCs in different regions will not take effect.

- Creating a VPC peering connection between VPCs in your account

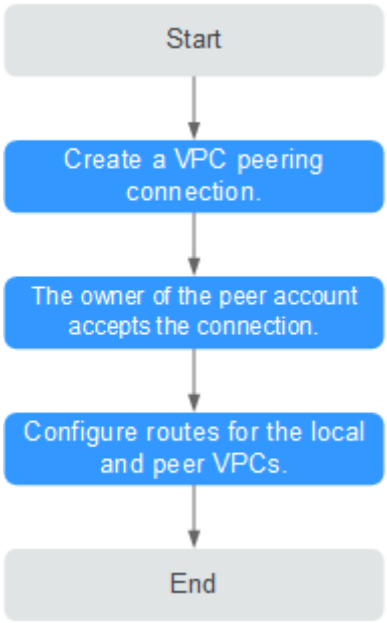
Figure 1-6 Creating a VPC peering connection between VPCs in your account



If you create a VPC peering connection between two VPCs in your account, the system automatically accepts the connection by default. You need to add routes for the local and peer VPCs to enable communication between the two VPCs.

- Creating a VPC peering connection with a VPC in another account

Figure 1-7 Creating a VPC peering connection with a VPC in another account



If you create a VPC peering connection between your VPC and a VPC that is in another account, the VPC peering connection will be in the **Awaiting acceptance** state. After the owner of the peer account accepts the connection, the connection status changes to **Accepted**. The owners of both

the local and peer accounts must configure the routes required by the VPC peering connection to enable communication between the two VPCs.

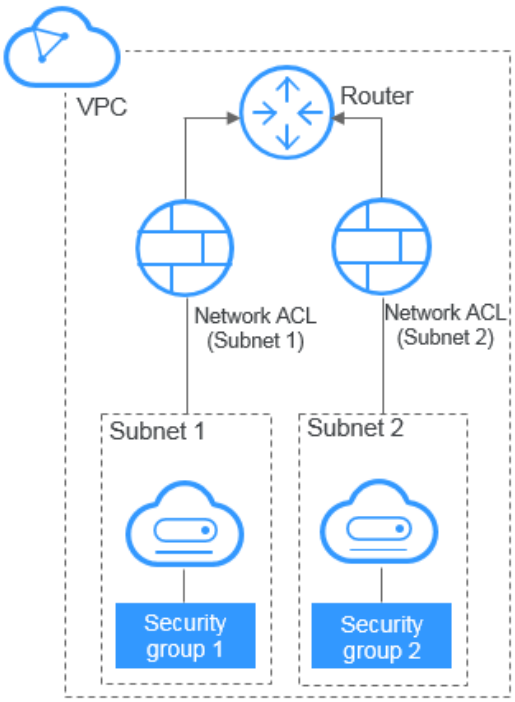
If the local and peer VPCs have overlapping CIDR blocks, the routes added for the VPC peering connection may be invalid. Before creating a VPC peering connection between two VPCs that have overlapping CIDR blocks, ensure that none of the subnets in the two VPCs overlap. In this case, the created VPC peering connection enables communication between two subnets in the two VPCs.

You can run the **ping** command to check whether the two VPCs can communicate with each other.

1.5.6 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, the network ACL can help you control traffic in and out of the subnets.

Figure 1-8 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 access control that is both comprehensive and fine-grained.

Network ACL Basics

- Your VPC does not come with a default network ACL, but you can create one and associate it with a 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 you send a request from your instance and the outbound traffic is allowed, 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 ones. **Table 1-3** shows the default network ACL rules. The default rules cannot be modified or deleted.

Table 1-3 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 one 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, 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 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.

1.5.7 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.

A virtual IP address can be bound to multiple ECSs deployed in active/standby mode. You can bind an EIP to the virtual IP address. When the EIP is accessed from the Internet, the virtual IP address has made it possible to either the active or standby ECS, making ECSs highly fault tolerant.

Networking

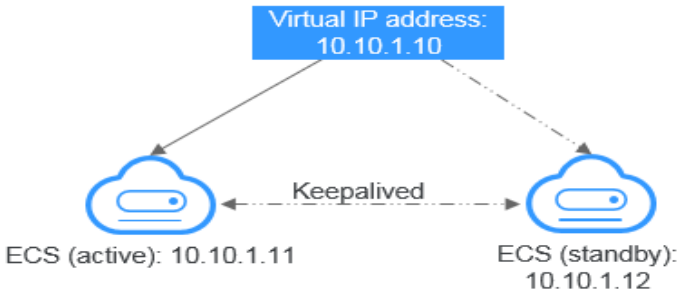
Virtual IP addresses are used for high availability as they make active/standby ECS switchover possible. This way if one ECS goes down for some reason, the other one can take over and services continue uninterrupted. ECSs can be configured for HA or as load balancing clusters.

- **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 1-9 Networking diagram of the HA mode

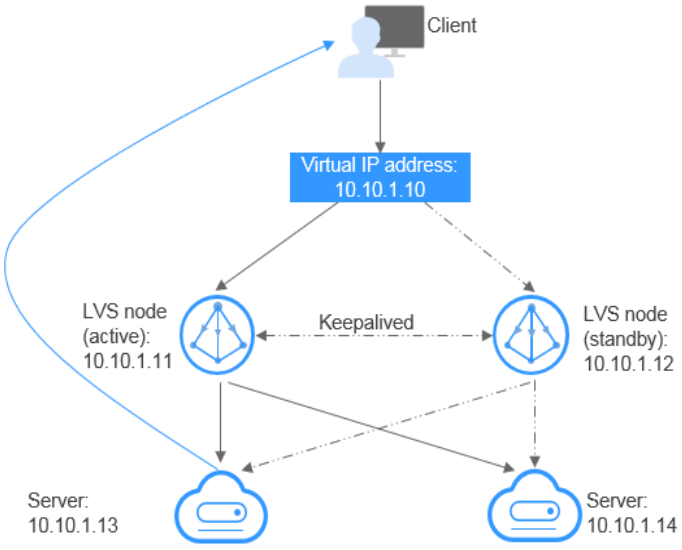


- In this configuration, a single virtual IP address is bound to two ECSs in the same subnet.
- Keepalived is then used to configure the two ECSs to work in the active/standby mode. Follow industry standards for configuring Keepalived. The details are not included here.

- **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 1-10 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.

1.5.8 Region and AZ

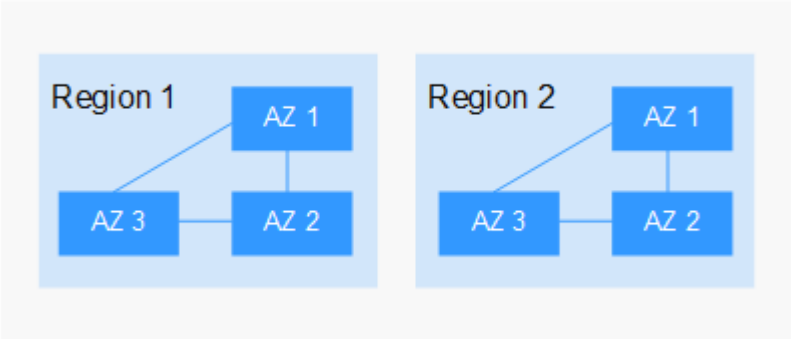
Concept

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

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in an AZ will not affect other AZs.

Figure 1-11 shows the relationship between regions and AZs.

Figure 1-11 Regions and AZs



Selecting a Region

Select a region closest to your target users for low network latency and quick access.

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 low 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**.

2 Getting Started

2.1 Typical Application Scenarios

A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

- If any of your ECSs, for example, ECSs that function as the database of server nodes for website deployment, do not need to access the Internet, you can configure a VPC for the ECSs by following the instructions described in **2.2 Configuring a VPC for ECSs That Do Not Require Internet Access**.
- If your ECSs need to access the Internet, you can configure EIPs for them. For example, the ECSs functioning as the service nodes for deploying a website need to be accessed by users over the Internet. Then, you can configure a VPC for these ECSs by following the instructions provided in **2.3 Configuring a VPC for ECSs That Access the Internet Using EIPs**.

2.2 Configuring a VPC for ECSs That Do Not Require Internet Access

2.2.1 Overview

If your ECSs do not require Internet access (for example, the ECSs functioning as the database nodes or server nodes for deploying a website), you can follow the procedure shown in **Figure 2-1** to configure a VPC for the ECSs.

Figure 2-1 Configuring the network

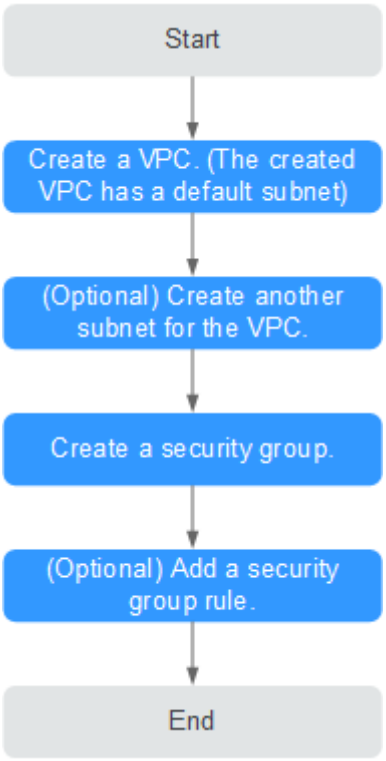


Table 2-1 describes the different tasks in the procedure for configuring the network.

Table 2-1 Configuration process description

Task	Description
Create a VPC.	This task is mandatory. After the VPC is created, you can create other required network resources in the VPC based on your service requirements.
Create another subnet for the VPC.	This task is optional. If the default subnet cannot meet your requirements, you can create one. The new subnet is used to assign IP addresses to NICs added to the ECS.
Create a security group.	This task is mandatory. You can create a security group and add ECSs in the VPC to the security group to improve ECS access security. After a security group is created, it has a default rule, which allows all outgoing data packets. ECSs in a security group can access each other without the need to add rules.

Task	Description
Add a security group rule.	This task is optional. If the default rule meets your service requirements, you do not need to add rules to the security group.

2.2.2 Step 1: Create a VPC

Scenarios

A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

Create a VPC by following the procedure provided in this section. Then, create subnets, security groups, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. Click **Create VPC**.
4. On the **Create VPC** page, set parameters as prompted.

   A default subnet will be created together with a VPC and you can also click **Add Subnet** to create more subnets for the VPC.

   Table 2-2 VPC parameter description

Parameter	Description	Example Value
Region	Specifies the desired region. Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	-

Parameter	Description	Example Value
Name	Specifies the VPC name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	VPC-001
IPv4 CIDR Block	Specifies the CIDR block of the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset of the CIDR block for the VPC (for multiple subnets in the VPC). The following CIDR blocks are supported: 10.0.0.0 – 10.255.255.255 172.16.0.0 – 172.31.255.255 192.168.0.0 – 192.168.255.255	192.168.0.0/16
Enterprise Project	When creating a VPC, you can add the VPC to an enabled enterprise project. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the *Enterprise Management User Guide*.	default
Advanced Settings	Click the drop-down arrow to set advanced VPC parameters, including tags.	Default
Tag	Specifies the VPC tag, which consists of a key and value pair. You can add a maximum of 10 tags to each VPC. The tag key and value must meet the requirements listed in **Table 2-4**.	• Key: vpc_key1 • Value: vpc-01

Table 2-3 Subnet parameter description

Parameter	Description	Example Value
Name	Specifies the subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
IPv4 CIDR Block	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set **IPv6 CIDR Block** to **Enable**. After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
Associated Route Table	Specifies the default route table to which the subnet will be associated. You can change the route table to a custom route table on the **Subnets** page.	Default
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including **Gateway** and **DNS Server Address**.	Default
Gateway	Specifies the gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1

Parameter	Description	Example Value
NTP Server Address	Specifies the IP address of the NTP server. This parameter is optional. You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If this parameter is left empty, no IP address of the NTP server is added. Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.	192.168.2.1
DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private network domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x

Parameter	Description	Example Value
DHCP Lease Time	Specifies the period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day/Hour If a DHCP lease time is changed, the new lease automatically takes effect when half of the current lease time has passed. To make the change take effect immediately, restart the ECS or log in to the ECS to cause the DHCP lease to automatically renew.	365 days
Tag	Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet. The tag key and value must meet the requirements listed in **Table 2-5**.	• Key: subnet_key1 • Value: subnet-01
Description	Provides supplementary information about the subnet. This parameter is optional. The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

Table 2-4 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for the same VPC and can be the same for different VPCs. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	vpc_key1

Parameter	Requirements	Example Value
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	vpc-01

Table 2-5 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each subnet. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	subnet_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	subnet-01

5. Confirm the current configuration and click **Create Now**.

2.2.3 Step 2: Create a Subnet for the VPC

Scenarios

A VPC comes with a default subnet. If the default subnet cannot meet your requirements, you can create one.

The subnet is configured with DHCP by default. When an ECS in this subnet starts, the ECS automatically obtains an IP address using DHCP.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. Click **Create Subnet**.
5. Set the parameters as prompted.

Table 2-6 Parameter descriptions

Parameter	Description	Example Value
VPC	Specifies the VPC for which you want to create a subnet.	-
Name	Specifies the subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
IPv4 CIDR Block	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set **IPv6 CIDR Block** to **Enable**. After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
Associated Route Table	Specifies the default route table to which the subnet will be associated. You can change the route table to a custom route table on the **Subnets** page.	Default
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including **Gateway** and **DNS Server Address**.	Default
Gateway	Specifies the gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1
DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private network domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x

Parameter	Description	Example Value
DHCP Lease Time	Specifies the period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day/Hour If a DHCP lease time is changed, the new lease automatically takes effect when half of the current lease time has passed. To make the change take effect immediately, restart the ECS or log in to the ECS to cause the DHCP lease to automatically renew.	365 days
NTP Server Address	Specifies the IP address of the NTP server. This parameter is optional. You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If this parameter is left empty, no IP address of the NTP server is added. Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.	192.168.2.1
Tag	Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet. The tag key and value must meet the requirements listed in **Table 2-7**.	• Key: subnet_key1 • Value: subnet-01
Description	Provides supplementary information about the subnet. This parameter is optional. The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Table 2-7 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each subnet. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	subnet_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	subnet-01

6. Click **OK**.

Precautions

When a subnet is created, there are five reserved IP addresses, which cannot be used. For example, in a subnet with CIDR block 192.168.0.0/24, the following IP addresses are reserved:

- 192.168.0.0: Network ID. This address is the beginning of the private IP address range and will not be assigned to any instance.
- 192.168.0.1: Gateway address.
- 192.168.0.253: Reserved for the system interface. This IP address is used by the VPC for external communication.
- 192.168.0.254: DHCP service address.
- 192.168.0.255: Network broadcast address.

If you configured the default settings under **Advanced Settings** during subnet creation, the reserved IP addresses may be different from the default ones, but there will still be five of them. The specific addresses depend on your subnet settings.

2.2.4 Step 3: Create a Security Group

Scenarios

To improve ECS access security, you can create security groups, define security group rules, and add ECSs in a VPC to different security groups. We recommend that you allocate ECSs that have different Internet access policies to different security groups.

Procedure

1. Log in to the management console.

2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click **Create Security Group**.
5. In the **Create Security Group** area, set the parameters as prompted. **Table 2-8** lists the parameters to be configured.

Table 2-8 Parameter description

Parameter	Description	Example Value
Name	Specifies the security group name. This parameter is mandatory. The security group name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces. **NOTE** You can change the security group name after a security group is created. It is recommended that you give each security group a different name.	sg-318b
Template	A template comes with default security group rules, helping you quickly create security groups. The following templates are provided: • **Custom**: This template allows you to create security groups with custom security group rules. • **General-purpose web server**: The security group that will be created using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389. • **All ports open**: The security group that will be created using this template includes default rules that allow inbound traffic on any port. Allowing inbound traffic on any port may pose security risks.	General-purpose web server
Description	Provides supplementary information about the security group. This parameter is optional. The security group description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. Click **OK**.

2.2.5 Step 4: Add a Security Group Rule

Scenarios

After a security group is created, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After ECSs are added to the security group, they are protected by the rules of that group.

- Inbound rules control incoming traffic to ECSs associated with the security group.
- Outbound rules control outgoing traffic from ECSs associated with the security group.

For details about the default security group rules, see **4.1.2 Default Security Groups and Security Group Rules**. For details about security group rule configuration examples, see **4.1.3 Security Group Configuration Examples**.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
5. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

   You can click **+** to add more inbound rules.

Table 2-9 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: specifies the network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: specifies the port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.	22, or 22-30
Type	Specifies the IP address type. • IPv4 • IPv6	IPv4

Parameter	Description	Example Value
Source	Specifies the source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses) • sg-abc (security group)	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.

   You can click **+** to add more outbound rules.

Table 2-10 Outbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: specifies the network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: specifies the port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30
Type	Specifies the IP address type. • IPv4 • IPv6	IPv4
Destination	Specifies the destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses) • sg-abc (security group)	0.0.0.0/0

Parameter	Description	Example Value
Description	Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **OK**.

Verification

After required security group rules are added, you can verify that the rules take effect. For example, you have deployed a website on ECSs. Users need to access your website over TCP (port 80), and you have added the security group rule shown in **Table 2-11**.

Table 2-11 Security group rule

Direction	Protocol	Port	Source
Inbound	TCP	80	0.0.0.0/0

Linux ECS

To verify the security group rule on a Linux ECS:

1. Log in to the ECS.
2. Run the following command to check whether TCP port 80 is listened:
   ```
   netstat -an | grep 80
   ```
   If command output shown in **Figure 2-2** is displayed, TCP port 80 is listened.

   Figure 2-2 Command output for the Linux ECS

   ```
   tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
   ```
3. Enter **http://***ECS EIP* in the address box of the browser and press **Enter**.
   If the requested page can be accessed, then the security group rule has taken effect.

Windows ECS

To verify the security group rule on a Windows ECS:

1. Log in to the ECS.
2. Choose **Start** > **Accessories** > **Command Prompt**.
3. Run the following command to check whether TCP port 80 is listened:
   ```
   netstat -an | findstr 80
   ```
   If command output shown in **Figure 2-3** is displayed, TCP port 80 is listened.

Figure 2-3 Command output for the Windows ECS

```
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
```

4. Enter **http://***ECS EIP* in the address box of the browser and press **Enter**.

   If the requested page can be accessed, then the security group rule has taken effect.

2.3 Configuring a VPC for ECSs That Access the Internet Using EIPs

2.3.1 Overview

If your ECSs need to access the Internet (for example, the ECSs functioning as the service nodes for deploying a website), you can follow the procedure shown in **Figure 2-4** to bind EIPs to the ECSs.

Figure 2-4 Configuring the network

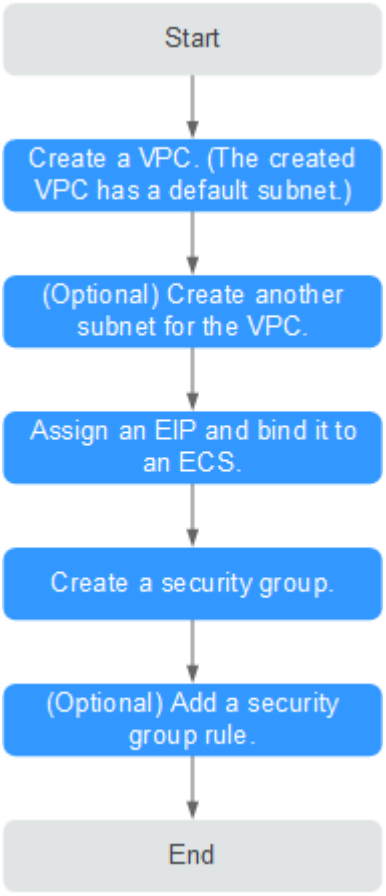


Table 2-12 describes the different tasks in the procedure for configuring the network.

Table 2-12 Configuration process description

Task	Description
Create a VPC.	This task is mandatory. A created VPC comes with a default subnet you specified. After the VPC is created, you can create other required network resources in the VPC based on your service requirements.
Create another subnet for the VPC.	This task is optional. If the default subnet cannot meet your requirements, you can create one. The new subnet is used to assign IP addresses to NICs added to the ECS.
Assign an EIP and bind it to an ECS.	This task is mandatory. You can assign an EIP and bind it to an ECS so that the ECS can access the Internet.
Create a security group.	This task is mandatory. You can create a security group and add ECSs in the VPC to the security group to improve ECS access security. After a security group is created, it has a default rule, which allows all outgoing data packets. ECSs in a security group can access each other without the need to add rules.
Add a security group rule.	This task is optional. If the default rule does not meet your service requirements, you can add security group rules.

2.3.2 Step 1: Create a VPC

Scenarios

A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

Create a VPC by following the procedure provided in this section. Then, create subnets, security groups, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. Click **Create VPC**.

4. On the **Create VPC** page, set parameters as prompted.

   A default subnet will be created together with a VPC and you can also click **Add Subnet** to create more subnets for the VPC.

   Table 2-13 VPC parameter description

Parameter	Description	Example Value
Region	Specifies the desired region. Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	-
Name	Specifies the VPC name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	VPC-001
IPv4 CIDR Block	Specifies the CIDR block of the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset of the CIDR block for the VPC (for multiple subnets in the VPC). The following CIDR blocks are supported: 10.0.0.0 – 10.255.255.255 172.16.0.0 – 172.31.255.255 192.168.0.0 – 192.168.255.255	192.168.0.0/16

Parameter	Description	Example Value
Enterprise Project	When creating a VPC, you can add the VPC to an enabled enterprise project. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the *Enterprise Management User Guide*.	default
Advanced Settings	Click the drop-down arrow to set advanced VPC parameters, including tags.	Default
Tag	Specifies the VPC tag, which consists of a key and value pair. You can add a maximum of 10 tags to each VPC. The tag key and value must meet the requirements listed in **Table 2-15**.	• Key: vpc_key1 • Value: vpc-01

Table 2-14 Subnet parameter description

Parameter	Description	Example Value
Name	Specifies the subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
IPv4 CIDR Block	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24

Parameter	Description	Example Value
IPv6 CIDR Block	Specifies whether to set **IPv6 CIDR Block** to **Enable**. After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
Associated Route Table	Specifies the default route table to which the subnet will be associated. You can change the route table to a custom route table on the **Subnets** page.	Default
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including **Gateway** and **DNS Server Address**.	Default
Gateway	Specifies the gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1

Parameter	Description	Example Value
NTP Server Address	Specifies the IP address of the NTP server. This parameter is optional. You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If this parameter is left empty, no IP address of the NTP server is added. Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.	192.168.2.1
DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private network domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x

Parameter	Description	Example Value
DHCP Lease Time	Specifies the period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day/Hour If a DHCP lease time is changed, the new lease automatically takes effect when half of the current lease time has passed. To make the change take effect immediately, restart the ECS or log in to the ECS to cause the DHCP lease to automatically renew.	365 days
Tag	Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet. The tag key and value must meet the requirements listed in **Table 2-16**.	• Key: subnet_key1 • Value: subnet-01
Description	Provides supplementary information about the subnet. This parameter is optional. The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

Table 2-15 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for the same VPC and can be the same for different VPCs. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	vpc_key1

Parameter	Requirements	Example Value
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	vpc-01

Table 2-16 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each subnet. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	subnet_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	subnet-01

5. Confirm the current configuration and click **Create Now**.

2.3.3 Step 2: Create a Subnet for the VPC

Scenarios

A VPC comes with a default subnet. If the default subnet cannot meet your requirements, you can create one.

The subnet is configured with DHCP by default. When an ECS in this subnet starts, the ECS automatically obtains an IP address using DHCP.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. Click **Create Subnet**.
5. Set the parameters as prompted.

Table 2-17 Parameter descriptions

Parameter	Description	Example Value
VPC	Specifies the VPC for which you want to create a subnet.	-
Name	Specifies the subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
IPv4 CIDR Block	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set **IPv6 CIDR Block** to **Enable**. After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
Associated Route Table	Specifies the default route table to which the subnet will be associated. You can change the route table to a custom route table on the **Subnets** page.	Default
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including **Gateway** and **DNS Server Address**.	Default
Gateway	Specifies the gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1
DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private network domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x

Parameter	Description	Example Value
DHCP Lease Time	Specifies the period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day/Hour If a DHCP lease time is changed, the new lease automatically takes effect when half of the current lease time has passed. To make the change take effect immediately, restart the ECS or log in to the ECS to cause the DHCP lease to automatically renew.	365 days
NTP Server Address	Specifies the IP address of the NTP server. This parameter is optional. You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If this parameter is left empty, no IP address of the NTP server is added. Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.	192.168.2.1
Tag	Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet. The tag key and value must meet the requirements listed in **Table 2-18**.	• Key: subnet_key1 • Value: subnet-01
Description	Provides supplementary information about the subnet. This parameter is optional. The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Table 2-18 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each subnet. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	subnet_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	subnet-01

6. Click **OK**.

Precautions

When a subnet is created, there are five reserved IP addresses, which cannot be used. For example, in a subnet with CIDR block 192.168.0.0/24, the following IP addresses are reserved:

- 192.168.0.0: Network ID. This address is the beginning of the private IP address range and will not be assigned to any instance.
- 192.168.0.1: Gateway address.
- 192.168.0.253: Reserved for the system interface. This IP address is used by the VPC for external communication.
- 192.168.0.254: DHCP service address.
- 192.168.0.255: Network broadcast address.

If you configured the default settings under **Advanced Settings** during subnet creation, the reserved IP addresses may be different from the default ones, but there will still be five of them. The specific addresses depend on your subnet settings.

2.3.4 Step 3: Assign an EIP and Bind It to an ECS

Scenarios

You can assign an EIP and bind it to an ECS so that the ECS can access the Internet.

Assigning an EIP

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, click **Assign EIP**.

4. Set the parameters as prompted.

Table 2-19 Parameter descriptions

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	N/A
EIP Type	**Dynamic BGP**: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP
Billed By	The following bandwidth types are available: • **Bandwidth**: You specify a maximum bandwidth and pay for the amount of time you use the bandwidth. This is suitable for scenarios with heavy or stable traffic. • **Traffic**: You specify a maximum bandwidth and pay for the total traffic you use. This is suitable for scenarios with light or sharply fluctuating traffic. • **Shared Bandwidth**: The bandwidth can be shared by multiple EIPs. This is suitable for scenarios with staggered traffic.	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	100
Bandwidth Name	The name of the bandwidth.	bandwidth
Tag	Specifies the EIP tags. Each tag contains a key and value pair. The tag key and value must meet the requirements listed in **Table 2-20**.	• Key: Ipv4_key1 • Value: 192.168.12.10

Parameter	Description	Example Value
Quantity	The number of EIPs you want to purchase.	1
Enterprise Project	The enterprise project to which the EIP belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the *Enterprise Management User Guide*.	default

Table 2-20 EIP tag requirements

Parameter	Requirement	Example Value
Key	• Cannot be left blank. • Must be unique for each EIP. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	Ipv4_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	192.168.12.10

5. Click **Create Now**.
6. Click **Submit**.

Binding an EIP

1. On the **EIPs** page, locate the row that contains the target EIP, and click **Bind**.
2. Select the instance to which you want to bind the EIP.
3. Click **OK**.

2.3.5 Step 4: Create a Security Group

Scenarios

To improve ECS access security, you can create security groups, define security group rules, and add ECSs in a VPC to different security groups. We recommend

that you allocate ECSs that have different Internet access policies to different security groups.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click **Create Security Group**.
5. In the **Create Security Group** area, set the parameters as prompted. **Table 2-21** lists the parameters to be configured.

Table 2-21 Parameter description

Parameter	Description	Example Value
Name	Specifies the security group name. This parameter is mandatory. The security group name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces. **NOTE** You can change the security group name after a security group is created. It is recommended that you give each security group a different name.	sg-318b
Template	A template comes with default security group rules, helping you quickly create security groups. The following templates are provided: • **Custom**: This template allows you to create security groups with custom security group rules. • **General-purpose web server**: The security group that will be created using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389. • **All ports open**: The security group that will be created using this template includes default rules that allow inbound traffic on any port. Allowing inbound traffic on any port may pose security risks.	General-purpose web server

Parameter	Description	Example Value
Description	Provides supplementary information about the security group. This parameter is optional. The security group description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. Click **OK**.

2.3.6 Step 5: Add a Security Group Rule

Scenarios

After a security group is created, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After ECSs are added to the security group, they are protected by the rules of that group.

- Inbound rules control incoming traffic to ECSs associated with the security group.
- Outbound rules control outgoing traffic from ECSs associated with the security group.

For details about the default security group rules, see **4.1.2 Default Security Groups and Security Group Rules**. For details about security group rule configuration examples, see **4.1.3 Security Group Configuration Examples**.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
5. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

   You can click **+** to add more inbound rules.

Table 2-22 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: specifies the network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP

Parameter	Description	Example Value
	Port: specifies the port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.	22, or 22-30
Type	Specifies the IP address type. • IPv4 • IPv6	IPv4
Source	Specifies the source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses) • sg-abc (security group)	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.

   You can click **+** to add more outbound rules.

Table 2-23 Outbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: specifies the network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: specifies the port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30
Type	Specifies the IP address type. • IPv4 • IPv6	IPv4

Parameter	Description	Example Value
Destination	Specifies the destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses) • sg-abc (security group)	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **OK**.

Verification

After required security group rules are added, you can verify that the rules take effect. For example, you have deployed a website on ECSs. Users need to access your website over TCP (port 80), and you have added the security group rule shown in **Table 2-24**.

Table 2-24 Security group rule

Direction	Protocol	Port	Source
Inbound	TCP	80	0.0.0.0/0

Linux ECS

To verify the security group rule on a Linux ECS:

1. Log in to the ECS.
2. Run the following command to check whether TCP port 80 is listened:
   ```
   netstat -an | grep 80
   ```
   If command output shown in **Figure 2-5** is displayed, TCP port 80 is listened.

   Figure 2-5 Command output for the Linux ECS

   ```
   tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
   ```
3. Enter **http://***ECS EIP* in the address box of the browser and press **Enter**.
   If the requested page can be accessed, then the security group rule has taken effect.

Windows ECS

To verify the security group rule on a Windows ECS:

1. Log in to the ECS.
2. Choose **Start** > **Accessories** > **Command Prompt**.
3. Run the following command to check whether TCP port 80 is listened:
   ```
   netstat -an | findstr 80
   ```
   If command output shown in **Figure 2-6** is displayed, TCP port 80 is listened.

   Figure 2-6 Command output for the Windows ECS

4. Enter **http://***ECS EIP* in the address box of the browser and press **Enter**.
   If the requested page can be accessed, then the security group rule has taken effect.

3 VPC and Subnet

3.1 Network Planning

Before creating your VPCs, determine how many VPCs, the number of subnets, and what IP address ranges or connectivity options you will need.

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. The communications on these different networks are completely isolated from each other, this is not the case for different AZs in the same VPC. Two networks in the same VPC should be able to communicate with each other even if they are in different AZs.

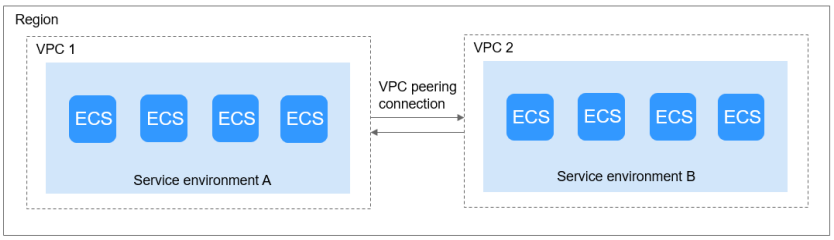
One VPC

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, you can use a VPC peering connection as shown in **Figure 3-1**.

Figure 3-1 VPC peering connection



Default VPC Quota

By default, you can create a maximum of five VPCs in your account. If this cannot meet your service requirements, request a quota increase. For details, see **11.1.1 What Is a Quota?**

How Do I Plan Subnets?

A subnet is a range of IP addresses in your VPC. All of the resources in a VPC must be deployed on subnets and the subnets on a VPC cannot overlap. Once a subnet has been created, its CIDR block cannot be modified.

The subnets used to deploy your resources must reside within your VPC, and the subnet masks used to define them can be between the netmask of its VPC CIDR block and /28 netmask.

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Subnet Planning

- We recommend that you create different subnets for different service modules in a VPC. For example, you can create different subnets for web, application, and database servers. A web server is in a publicly accessible subnet, and application and database servers are in non-publically accessible subnets. You can leverage network ACLs to help control access to the servers in each subnet.
- If you only need to plan subnets for VPCs, and communication between VPCs and on-premises data centers are not required, you can create subnets within any of the CIDR blocks listed above.
- If your VPC needs to communicate with an on-premises data center through VPN or Direct Connect, the VPC CIDR block cannot overlap with the CIDR block of the on-premises data center. Therefore, when creating a VPC or subnet, ensure that its CIDR block does not overlap with any CIDR block on the data center.
- When determining the size of a VPC or subnet CIDR block, ensure that the number of available IP addresses on the CIDR block meet your service requirements.

Default Subnet Quota

By default, you can create up to 100 subnets in your account. If you need more, submit a service ticket to request a quota increase. For details, see **11.1.1 What Is a Quota?**

How Do I Plan Routing Policies?

A route table contains a set of routes that are used to control where inbound and outbound subnet traffic is forwarded within a VPC. When you create a VPC, it automatically has a default route table, which enables internal communication within that VPC.

- If you do not need to explicitly control how each subnet routes inbound and outbound traffic, you can use the default route table.

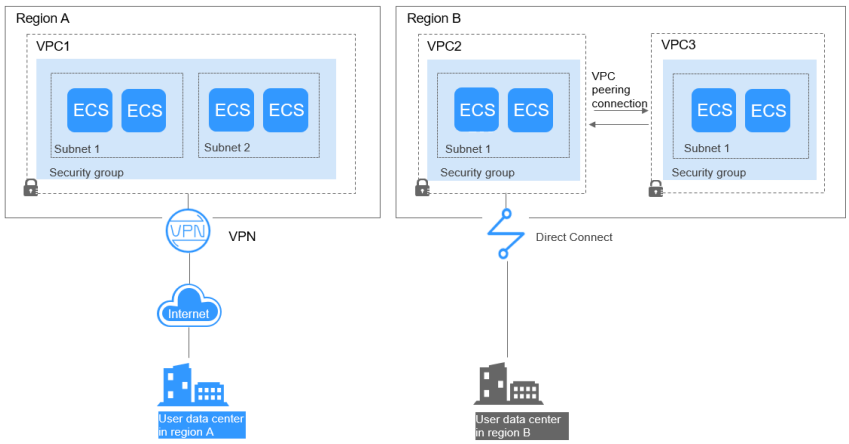
- If you need to explicitly control how each subnet routes inbound and outbound traffic in a VPC, you can add custom routes to the route table.

How Do I Connect to an On-Premises Data Center?

If you require interconnection between a VPC and an on-premises data center, ensure that the VPC does not have an overlapping IP address range with the on-premises data center to be connected.

Figure 3-2 shows that VPC 1 is in Region A and that VPC 2 and VPC 3 are in Region B. To connect to an on-premises data center, they can use a VPN, as VPC 1 does in Region A; or a Direct Connect connection, as VPC 2 does in Region B. VPC 2 connects to the data center through a Direct Connect connection, but to connect to another VPC in that region, like VPC 3, a VPC peering connection must be established.

Figure 3-2 Connections to on-premises data centers



When planning CIDR blocks for VPC 1, VPC 2, and VPC 3.

- The CIDR block of VPC 1 cannot overlap with the CIDR block of the on-premises data center in Region A.
- The CIDR block of VPC 2 cannot overlap with the CIDR block of the on-premises data center in Region B.
- The CIDR blocks of VPC 2 and VPC 3 cannot overlap.

How Do I Access 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 the EIPs to the 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.

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, the public cloud system provides 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 source network address translation (SNAT) and destination network address translation (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.

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 clusters. It provides fault tolerance for your applications by automatically balancing traffic across multiple AZs. You can also take advantage of deep integration with Auto Scaling (AS), which enables automatic scaling based on service traffic and ensures service stability and reliability.

3.2 VPC

3.2.1 Creating a VPC

Scenarios

A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

Create a VPC by following the procedure provided in this section. Then, create subnets, security groups, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. Click **Create VPC**.
4. On the **Create VPC** page, set parameters as prompted.

   A default subnet will be created together with a VPC and you can also click **Add Subnet** to create more subnets for the VPC.

Table 3-1 VPC parameter description

Parameter	Description	Example Value
Region	Specifies the desired region. Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	-
Name	Specifies the VPC name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	VPC-001
IPv4 CIDR Block	Specifies the CIDR block of the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset of the CIDR block for the VPC (for multiple subnets in the VPC). The following CIDR blocks are supported: 10.0.0.0 – 10.255.255.255 172.16.0.0 – 172.31.255.255 192.168.0.0 – 192.168.255.255	192.168.0.0/16
Enterprise Project	When creating a VPC, you can add the VPC to an enabled enterprise project. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the *Enterprise Management User Guide*.	default

Parameter	Description	Example Value
Advanced Settings	Click the drop-down arrow to set advanced VPC parameters, including tags.	Default
Tag	Specifies the VPC tag, which consists of a key and value pair. You can add a maximum of 10 tags to each VPC. The tag key and value must meet the requirements listed in **Table 3-3**.	• Key: vpc_key1 • Value: vpc-01

Table 3-2 Subnet parameter description

Parameter	Description	Example Value
Name	Specifies the subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
IPv4 CIDR Block	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set **IPv6 CIDR Block** to **Enable**. After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
Associated Route Table	Specifies the default route table to which the subnet will be associated. You can change the route table to a custom route table on the **Subnets** page.	Default

Parameter	Description	Example Value
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including **Gateway** and **DNS Server Address**.	Default
Gateway	Specifies the gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1
NTP Server Address	Specifies the IP address of the NTP server. This parameter is optional. You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If this parameter is left empty, no IP address of the NTP server is added. Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.	192.168.2.1

Parameter	Description	Example Value
DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private network domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
DHCP Lease Time	Specifies the period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day/Hour If a DHCP lease time is changed, the new lease automatically takes effect when half of the current lease time has passed. To make the change take effect immediately, restart the ECS or log in to the ECS to cause the DHCP lease to automatically renew.	365 days
Tag	Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet. The tag key and value must meet the requirements listed in **Table 3-4**.	• Key: subnet_key1 • Value: subnet-01

Parameter	Description	Example Value
Description	Provides supplementary information about the subnet. This parameter is optional. The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

Table 3-3 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for the same VPC and can be the same for different VPCs. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	vpc_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	vpc-01

Table 3-4 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each subnet. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	subnet_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	subnet-01

5. Confirm the current configuration and click **Create Now**.

3.2.2 Modifying a VPC

Scenarios

Change the VPC name and CIDR block.

If the VPC CIDR block conflicts with the CIDR block of a VPN created in the VPC, you can modify its CIDR block.

Notes and Constraints

When modifying the VPC CIDR block:

- The VPC CIDR block to be modified must be in the supported 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
- If the VPC has subnets, the VPC CIDR block to be modified must contain all subnet CIDR blocks.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Virtual Private Cloud**.
4. On the **Virtual Private Cloud** page, locate the row that contains the VPC to be modified and click **Edit CIDR Block** in the **Operation** column.
5. On the displayed page, modify parameters as prompted. You can change the VPC CIDR block.
6. Click **OK**.

3.2.3 Deleting a VPC

Scenarios

You can delete a VPC if the VPC is no longer required.

A VPC cannot be deleted if it contains subnets, Direct Connect connections, custom routes, VPC peering connections, or VPNs. To delete the VPC, you must first delete the following resources.

- Subnets. For details, see section **3.3.3 Deleting a Subnet**.
- VPNs. For details, see *Virtual Private Network User Guide*.
- Custom routes. For details, see section **7.10 Deleting a Route**.
- VPC peering connections. For details, see section **8.7 Deleting a VPC Peering Connection**.

Notes and Constraints

If there are any EIPs, the last VPC cannot be deleted.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Virtual Private Cloud**.
4. On the **Virtual Private Cloud** page, locate the row that contains the VPC to be deleted and click **Delete** in the **Operation** column.
5. Click **Yes** in the displayed dialog box.

3.2.4 Managing VPC Tags

Scenarios

A VPC tag identifies a VPC. Tags can be added to VPCs to facilitate VPC identification and management. You can add a tag to a VPC when creating the VPC, or you can add a tag to a created VPC on the VPC details page. A maximum of 10 tags can be added to each VPC.

A tag consists of a key and value pair. **Table 3-5** lists the tag key and value requirements.

Table 3-5 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for the same VPC and can be the same for different VPCs. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	vpc_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	vpc-01

Procedure

Search for VPCs by tag key and value on the page showing the VPC list.

1. Log in to the management console.
2. Under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Virtual Private Cloud**.
4. In the upper right corner of the VPC list, click **Search by Tag**.
5. In the displayed area, enter the tag key and value of the VPC you are looking for.

Both the tag key and value must be specified. The system automatically displays the VPCs you are looking for if both the tag key and value are matched.

6. Click **+** to add another tag key and value.

   You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for VPCs, the VPCs containing all specified tags will be displayed.

7. Click **Search**.

   The system displays the VPCs you are looking for based on the entered tag keys and values.

Add, delete, edit, and view tags on the Tags tab of a VPC.

1. Log in to the management console.
2. Under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Virtual Private Cloud**.
4. On the **Virtual Private Cloud** page, locate the VPC whose tags are to be managed and click the VPC name.

   The page showing details about the particular VPC is displayed.

5. Click the **Tags** tab and perform desired operations on tags.
   - View tags.

     On the **Tags** tab, you can view details about tags added to the current VPC, including the number of tags and the key and value of each tag.
   - Add a tag.

     Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.
   - Edit a tag.

     Locate the row that contains the tag you want to edit, and click **Edit** in the **Operation** column. Enter the new tag key and value, and click **OK**.
   - Delete a tag.

     Locate the row that contains the tag you want to delete, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

3.2.5 Exporting VPC Information

Scenarios

Information about all VPCs under your account can be exported as an Excel file to a local directory. This file records the names, ID, status, IP address ranges of VPCs, and the number of subnets.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Virtual Private Cloud**.
4. In the upper right corner of the VPC list, click  .

The system will automatically export information about all VPCs under your account in the current region. They will be exported in Excel format.

3.3 Subnet

3.3.1 Creating a Subnet for the VPC

Scenarios

A VPC comes with a default subnet. If the default subnet cannot meet your requirements, you can create one.

The subnet is configured with DHCP by default. When an ECS in this subnet starts, the ECS automatically obtains an IP address using DHCP.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. Click **Create Subnet**.
5. Set the parameters as prompted.

Table 3-6 Parameter descriptions

Parameter	Description	Example Value
VPC	Specifies the VPC for which you want to create a subnet.	-
Name	Specifies the subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
IPv4 CIDR Block	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set **IPv6 CIDR Block** to **Enable**. After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-

Parameter	Description	Example Value
Associated Route Table	Specifies the default route table to which the subnet will be associated. You can change the route table to a custom route table on the **Subnets** page.	Default
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including **Gateway** and **DNS Server Address**.	Default
Gateway	Specifies the gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1
DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private network domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
DHCP Lease Time	Specifies the period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day/Hour If a DHCP lease time is changed, the new lease automatically takes effect when half of the current lease time has passed. To make the change take effect immediately, restart the ECS or log in to the ECS to cause the DHCP lease to automatically renew.	365 days

Parameter	Description	Example Value
NTP Server Address	Specifies the IP address of the NTP server. This parameter is optional. You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If this parameter is left empty, no IP address of the NTP server is added. Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.	192.168.2.1
Tag	Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet. The tag key and value must meet the requirements listed in **Table 3-7**.	• Key: subnet_key1 • Value: subnet-01
Description	Provides supplementary information about the subnet. This parameter is optional. The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Table 3-7 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each subnet. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	subnet_key1

Parameter	Requirements	Example Value
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	subnet-01

6. Click **OK**.

Precautions

When a subnet is created, there are five reserved IP addresses, which cannot be used. For example, in a subnet with CIDR block 192.168.0.0/24, the following IP addresses are reserved:

- 192.168.0.0: Network ID. This address is the beginning of the private IP address range and will not be assigned to any instance.
- 192.168.0.1: Gateway address.
- 192.168.0.253: Reserved for the system interface. This IP address is used by the VPC for external communication.
- 192.168.0.254: DHCP service address.
- 192.168.0.255: Network broadcast address.

If you configured the default settings under **Advanced Settings** during subnet creation, the reserved IP addresses may be different from the default ones, but there will still be five of them. The specific addresses depend on your subnet settings.

3.3.2 Modifying a Subnet

Scenarios

Change the subnet name and DNS server address.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. In the subnet list, locate the target subnet and click its name.
5. On the subnet details page, modify required parameters.

Table 3-8 Parameter descriptions

Parameter	Description	Example Value
Name	Specifies the subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private network domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
DHCP Lease Time	Specifies the period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day/Hour If a DHCP lease time is changed, the new lease automatically takes effect when half of the current lease time has passed. To make the change take effect immediately, restart the ECS or log in to the ECS to cause the DHCP lease to automatically renew.	365 days

3.3.3 Deleting a Subnet

Scenarios

You can delete a subnet to release network resources if the subnet is no longer required.

Prerequisites

Before deleting a subnet, ensure that any of the following resources using the subnet have been deleted.

You can view all resources of your account on the console homepage and check the resources that are in the subnet to be deleted. You must delete all resources in the subnet before deleting the subnet.

The resources may include:

- ECS
- Load balancer
- VPN
- Private IP address
- Custom route
- NAT gateway
- VPC endpoint and VPC endpoint service

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. On the **Subnets** page, locate the target subnet and click **Delete**.
5. Click **Yes** in the displayed dialog box.

3.3.4 Managing Subnet Tags

Scenarios

A subnet tag identifies a subnet. Tags can be added to subnets to facilitate subnet identification and administration. You can add a tag to a subnet when creating the subnet, or you can add a tag to a created subnet on the subnet details page. A maximum of 10 tags can be added to each subnet.

A tag consists of a key and value pair. **Table 3-9** lists the tag key and value requirements.

Table 3-9 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	• Cannot be left blank. • Must be unique for each subnet. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	subnet_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	subnet-01

Procedure

Search for subnets by tag key and value on the page showing the subnet list.

1. Log in to the management console.
2. Under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. In the upper right corner of the subnet list, click **Search by Tag**.
5. Enter the tag key of the subnet to be queried.

   Both the tag key and value must be specified. The system automatically displays the subnets you are looking for if both the tag key and value are matched.
6. Click **+** to add another tag key and value.

   You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for subnets, the subnets containing all specified tags will be displayed.
7. Click **Search**.

   The system displays the subnets you are looking for based on the entered tag keys and values.

Add, delete, edit, and view tags on the Tags tab of a subnet.

1. Log in to the management console.
2. Under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. In the subnet list, locate the target subnet and click its name.
5. On the subnet details page, click the **Tags** tab and perform desired operations on tags.
   - View tags.

     On the **Tags** tab, you can view details about tags added to the current subnet, including the number of tags and the key and value of each tag.

- Add a tag.

  Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.
- Edit a tag.

  Locate the row that contains the tag you want to edit, and click **Edit** in the **Operation** column. Enter the new tag key and value, and click **OK**.
- Delete a tag.

  Locate the row that contains the tag you want to delete, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

3.4 IPv4 and IPv6 Dual-Stack Network

Overview

IPv4 and IPv6 dual-stack allows your resources, such as ECSs, to use both IPv4 and IPv6 addresses for private and public network communication.

- Private IPv4 addresses can be used for private network access between ECSs.
- Private IPv4 addresses with EIPs bound can be used for Internet access.
- IPv6 addresses can be used for private network access between ECSs (in the same VPC) that have both IPv4 and IPv6 addresses.
- IPv6 addresses can be used to access IPv6 networks on the Internet.

Application Scenarios

If your application needs to provide services for users who use IPv6 clients, you can use IPv6 EIPs or the IPv4 and IPv6 dual-stack function.

If your application needs to both provide services for users who use IPv6 clients and analyze the access request data, you can only use the IPv4 and IPv6 dual-stack function.

If private network communication is required between your application systems or between your application system and another system (such as a database system), you can only use the IPv4 and IPv6 dual-stack function.

Basic Operations

NOTE

The basic operations for IPv4 and IPv6 dual-stack networks are the same as those for IPv4 networks. Only some parameters are different. You can check the console pages for details.

Creating an IPv6 Subnet

Create an IPv6 subnet by following the instructions provided in **3.3.1 Creating a Subnet for the VPC**. You must ensure that **Enable** is selected for **IPv6 CIDR Block**. An IPv6 CIDR block will be automatically assigned to the subnet. The IPv6 function cannot be disabled after the subnet is created. Currently, customizing IPv6 CIDR block is not supported.

Viewing In-Use IPv6 Addresses

In the subnet list, click the target subnet name. On the displayed page, view in-use IPv6 addresses on the **In-Use IP Addresses** tab.

Adding a Security Group Rule (IPv6)

Add a security group rule with **Type** set to **IPv6** and **Source** or **Destination** set to an IPv6 address or IPv6 CIDR block.

Adding a Network ACL Rule (IPv6)

Add a network ACL rule with **Type** set to **IPv6** and **Source** or **Destination** set to an IPv6 address or IPv6 CIDR block.

Adding a Route (IPv6)

Add a route with **Destination** set to an IPv6 address and **Next Hop** set to an IPv6 address or CIDR block. For details about how to add a route, see **7.4 Adding a Custom Route**. If the destination is an IPv6 CIDR block, the next hop can only be an IP address in the same VPC as the IPv6 CIDR block.

NOTE

If the destination is an IPv6 CIDR block, the next hop type can only be ECS, extension NIC, or virtual IP address. The next hop must also have IPv6 addresses.

4 Security

4.1 Security Group

4.1.1 Security Group Overview

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. After a security group is created, you can create different access rules for the security group, these rules will apply to any ECS that the security group contains.

Your account automatically comes with a default security group. The default security group allows all outbound traffic, denies all inbound traffic, and allows all traffic between ECSs in the group. Your ECSs in this security group can communicate with each other already without adding additional rules. You can directly use the default security group. For details, see **4.1.2 Default Security Groups and Security Group Rules**.

You can also create custom security groups to meet your specific service requirements. For details, see **4.1.4 Creating a Security Group**.

Security Group Basics

- Instances, such as servers and extension NICs, can be associated with one or more security groups.

  You can change the security groups that are associated with instances, such as servers or extension NICs. By default, when you create an instance, it is associated with the default security group of its VPC unless you specify another security group.
- Security group rules need be added to allow instances in the same security group to communicate with each other.
- Security groups are stateful. If you send a request from your instance and the outbound traffic is allowed, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Similarly, if inbound traffic

is allowed, responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

Security groups use connection tracking to track traffic to and from instances that they contain and security group rules are applied based on the connection status of the traffic to determine whether to allow or deny traffic. If a security group rule is added, deleted, or modified, or an instance in the security group is created or deleted, the connection tracking of all instances in the security group will be automatically cleared. In this case, the inbound or outbound traffic of the instance is considered as new connections, which need to match the inbound or outbound security group rules to ensure that the rules take effect immediately and the security of incoming traffic.

In addition, if the inbound or outbound traffic of an instance has no packets for a long time, the traffic is considered as new connections after the connection tracking times out, and the connections need to match the outbound and inbound 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.

NOTE

If two ECSs are in the same security group but in different VPCs, the ECSs cannot communicate with each other. To enable communications between the ECSs, use a VPC peering connection to connect the two VPCs first.

Security Group Rules

After a security group is created, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After ECSs are added to the security group, they are protected by the rules of that group.

Each security group has **default rules**. You can also customize security group rules. For details, see **4.1.5 Adding a Security Group Rule**.

Security Group Constraints

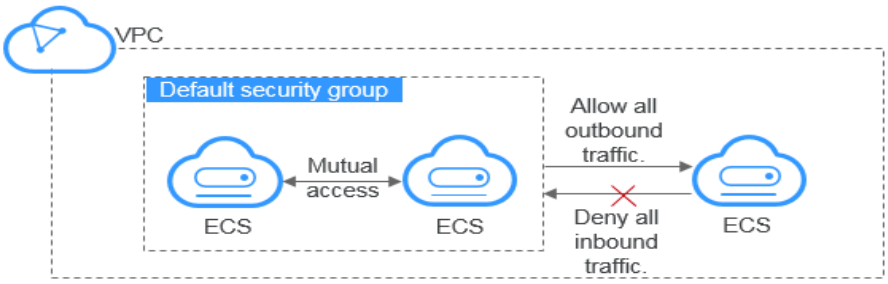
- By default, you can create up to 100 security groups in your cloud account.
- By default, each security group can have up to 50 security group rules.
- By default, an ECS or an ECS extension NIC can be added to a maximum of five security groups.
- A maximum of 20 instances can be added to a security group at a time.
- A security group can be associated with a maximum of 1000 instances.

4.1.2 Default Security Groups and Security Group Rules

Your account automatically comes with a default security group. The default security group allows all outbound traffic, denies all inbound traffic, and allows all traffic between ECSs in the group. Your ECSs in this security group can communicate with each other already without adding additional rules.

Figure 4-1 shows the default security group.

Figure 4-1 Default security group



NOTE

- You cannot delete the default security group, but you can modify the rules for the default security group.
- If two ECSs are in the same security group but in different VPCs, the ECSs cannot communicate with each other. To enable communications between the ECSs, use a VPC peering connection to connect the two VPCs first.

Table 4-1 describes the default rules for the default security group.

Table 4-1 Rules in the default security group

Direction	Protocol	Port/ Range	Source/ Destination	Description
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic.
Inbound	All	All	Source: the current security group (for example, sg-*xxxxx*)	Allows communication among ECSs within the security group and denies all inbound traffic (incoming data packets).
Inbound	TCP	22	Source: 0.0.0.0/0	Allows all IP addresses to access Linux ECSs over SSH.
Inbound	TCP	3389	Source: 0.0.0.0/0	Allows all IP addresses to access Windows ECSs over RDP.

4.1.3 Security Group Configuration Examples

Common security group configurations are presented here. The examples in this section allow all outgoing data packets by default. This section will only describe how to configure inbound rules.

- **Allowing External Access to a Specified Port**
- **Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network**
- **Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group**
- **Remotely Connecting to Linux ECSs Using SSH**
- **Remotely Connecting to Windows ECSs Using RDP**
- **Enabling Communication Between ECSs**
- **Hosting a Website on ECSs**
- **Enabling an ECS to Function as a DNS Server**
- **Uploading or Downloading Files Using FTP**

You can use the default security group or create a security group in advance. For details, see sections **4.1.4 Creating a Security Group** and **4.1.5 Adding a Security Group Rule**.

Allowing External Access to a Specified Port

- Example scenario:

  After services are deployed, you can add security group rules to allow external access to a specified port (for example, 1100).

- Security group rule:

Direction	Protocol	Port	Source
Inbound	TCP	1100	0.0.0.0/0

Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network

- Example scenario:

  Resources on an ECS in a security group need to be copied to an ECS associated with another security group. The two ECSs are in the same VPC. We recommend that you enable private network communication between the ECSs and then copy the resources.

- Security group configuration:

  Within a given VPC, ECSs in the same security group can communicate with one another by default. However, ECSs in different security groups cannot communicate with each other by default. To enable these ECSs to communicate with each other, you need to add certain security group rules.

You can add an inbound rule to the security groups containing the ECSs to allow access from ECSs in the other security group. The required rule is as follows.

Direction	Protocol/Application	Port	Source
Inbound	Used for communication through an internal network	Port or port range	ID of another security group

Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group

- Example scenario:

  To prevent ECSs from being attacked, you can change the port number for remote login and configure security group rules that allow only specified IP addresses to remotely access the ECSs.

- Security group configuration:

  To allow IP address **192.168.20.2** to remotely access Linux ECSs in a security group over the SSH protocol (port 22), you can configure the following security group rule.

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	IPv4 CIDR block or ID of another security group For example, 192.168.20.2/32

Remotely Connecting to Linux ECSs Using SSH

- Example scenario:

  After creating Linux ECSs, you can add a security group rule to enable remote SSH access to the ECSs.

  NOTE

  The default security group comes with the following rule. If you use the default security group, you do not need to add this rule again.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	SSH (22)	22	0.0.0.0/0

Remotely Connecting to Windows ECSs Using RDP

- Example scenario:

After creating Windows ECSs, you can add a security group rule to enable remote RDP access to the ECSs.

NOTE

The default security group comes with the following rule. If you use the default security group, you do not need to add this rule again.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	RDP (3389)	3389	0.0.0.0/0

Enabling Communication Between ECSs

- Example scenario:

  After creating ECSs, you need to add a security group rule so that you can run the **ping** command to test communication between the ECSs.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	ICMP	All	0.0.0.0/0

Hosting a Website on ECSs

- Example scenario:

  If you deploy a website on your ECSs and require that your website be accessed over HTTP or HTTPS, you can add rules to the security group used by the ECSs that function as the web servers.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	HTTP (80)	80	0.0.0.0/0
Inbound	HTTPS (443)	443	0.0.0.0/0

Enabling an ECS to Function as a DNS Server

- Example scenario:

  If you need to use an ECS as a DNS server, you must allow TCP and UDP access from port 53 to the DNS server. You can add the following rules to the security group associated with the ECS.

- Security group rules:

Direction	Protocol/ Application	Port	Source
Inbound	TCP	53	0.0.0.0/0
Inbound	UDP	53	0.0.0.0/0

Uploading or Downloading Files Using FTP

- Example scenario:

  If you want to use File Transfer Protocol (FTP) to upload files to or download files from ECSs, you need to add a security group rule.

  NOTE

  You must first install the FTP server program on the ECSs and check whether ports 20 and 21 are working properly.

- Security group rule:

Direction	Protocol/ Application	Port	Source
Inbound	TCP	20-21	0.0.0.0/0

4.1.4 Creating a Security Group

Scenarios

To improve ECS access security, you can create security groups, define security group rules, and add ECSs in a VPC to different security groups. We recommend that you allocate ECSs that have different Internet access policies to different security groups.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click **Create Security Group**.
5. In the **Create Security Group** area, set the parameters as prompted. **Table 4-2** lists the parameters to be configured.

Table 4-2 Parameter description

Parameter	Description	Example Value
Name	Specifies the security group name. This parameter is mandatory. The security group name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces. **NOTE** You can change the security group name after a security group is created. It is recommended that you give each security group a different name.	sg-318b
Template	A template comes with default security group rules, helping you quickly create security groups. The following templates are provided: • **Custom**: This template allows you to create security groups with custom security group rules. • **General-purpose web server**: The security group that will be created using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389. • **All ports open**: The security group that will be created using this template includes default rules that allow inbound traffic on any port. Allowing inbound traffic on any port may pose security risks.	General-purpose web server
Description	Provides supplementary information about the security group. This parameter is optional. The security group description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. Click **OK**.

4.1.5 Adding a Security Group Rule

Scenarios

After a security group is created, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After ECSs are added to the security group, they are protected by the rules of that group.

- Inbound rules control incoming traffic to ECSs associated with the security group.
- Outbound rules control outgoing traffic from ECSs associated with the security group.

For details about the default security group rules, see **4.1.2 Default Security Groups and Security Group Rules**. For details about security group rule configuration examples, see **4.1.3 Security Group Configuration Examples**.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
5. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

   You can click **+** to add more inbound rules.

Table 4-3 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: specifies the network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: specifies the port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.	22, or 22-30
Type	Specifies the IP address type. • IPv4 • IPv6	IPv4
Source	Specifies the source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses) • sg-abc (security group)	0.0.0.0/0

Parameter	Description	Example Value
Description	Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.
   You can click **+** to add more outbound rules.

   Table 4-4 Outbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: specifies the network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: specifies the port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30
Type	Specifies the IP address type. • IPv4 • IPv6	IPv4
Destination	Specifies the destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses) • sg-abc (security group)	0.0.0.0/0
Description	Provides supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **OK**.

Verification

After required security group rules are added, you can verify that the rules take effect. For example, you have deployed a website on ECSs. Users need to access

your website over TCP (port 80), and you have added the security group rule shown in **Table 4-5**.

Table 4-5 Security group rule

Direction	Protocol	Port	Source
Inbound	TCP	80	0.0.0.0/0

Linux ECS

To verify the security group rule on a Linux ECS:

1. Log in to the ECS.
2. Run the following command to check whether TCP port 80 is listened:
   ```
   netstat -an | grep 80
   ```
   If command output shown in **Figure 4-2** is displayed, TCP port 80 is listened.

   Figure 4-2 Command output for the Linux ECS

3. Enter **http://***ECS EIP* in the address box of the browser and press **Enter**.

   If the requested page can be accessed, then the security group rule has taken effect.

Windows ECS

To verify the security group rule on a Windows ECS:

1. Log in to the ECS.
2. Choose **Start** > **Accessories** > **Command Prompt**.
3. Run the following command to check whether TCP port 80 is listened:
   ```
   netstat -an | findstr 80
   ```
   If command output shown in **Figure 4-3** is displayed, TCP port 80 is listened.

   Figure 4-3 Command output for the Windows ECS

4. Enter **http://***ECS EIP* in the address box of the browser and press **Enter**.

   If the requested page can be accessed, then the security group rule has taken effect.

4.1.6 Fast-Adding Security Group Rules

Scenarios

You can add multiple security group rules with different protocols and ports at the same time.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
5. On the **Inbound Rules** tab, click **Fast-Add Rule**. In the displayed dialog box, select the protocols and ports you wish to add all at once.
6. On the **Outbound Rules** tab, click **Fast-Add Rule**. In the displayed dialog box, select required protocols and ports to add multiple rules at a time.
7. Click **OK**.

4.1.7 Replicating a Security Group Rule

Scenarios

Replicate an existing security group rule to generate a new rule. When replicating a security group rule, you can make changes so that it is not a perfect copy.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click the security group name.
5. On the displayed page, locate the row that contains the security group rule to be replicated, and click **Replicate** in the **Operation** column.

   You can also modify the security group rule as required to quickly generate a new rule.
6. Click **OK**.

4.1.8 Modifying a Security Group Rule

Scenarios

You can modify the port, protocol, and IP address of a security group rule to meet your specific requirements.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click the security group name.
5. On the displayed page, locate the row that contains the security group rule to be modified, and click **Modify** in the **Operation** column.

6. Modify the rule and click **Confirm**.

4.1.9 Deleting a Security Group Rule

Scenarios

If the source of an inbound security group rule or destination of an outbound security group rule needs to be changed, you need to first delete the security group rule and add a new one.

NOTE

Security group rules use whitelists. Deleting a security group rule may result in ECS access failures.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click the security group name.
5. If you do not need a security group rule, locate the row that contains the target rule, and click **Delete**.
6. Click **Yes** in the displayed dialog box.

Deleting multiple security group rules at once

You can also select multiple security group rules and click **Delete** above the security group rule list to delete multiple rules at a time.

4.1.10 Importing and Exporting Security Group Rules

Scenarios

If you want to quickly apply the rules of one security group to another, or if you want to modify multiple rules of the current security group at once, you can import or export existing rules.

Security group rules are imported or exported to an Excel file.

Notes and Constraints

When modifying exported security group rules, you can only modify existing fields in the exported file based on the template and cannot add new fields or modify the field names. Otherwise, the file will fail to be imported.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.

4. On the **Security Groups** page, click the security group name.
5. On the displayed page, export and import security group rules.
   - Click  to export all rules of the current security group to an Excel file.
   - Click  to import security group rules from an Excel file into the current security group.

4.1.11 Deleting a Security Group

Scenarios

You can delete a security group to release resources if the security group is no longer required.

Notes and Constraints

- The default security group cannot be deleted.
- If a security group is associated with resources other than servers and extension NICs, the security group cannot be deleted.

Prerequisites

- Before deleting a security group, ensure that the security group is not used by any cloud resource, such as ECS. If the security group is used by any cloud resource, release the corresponding cloud resource or change the security group used by the cloud resource, and then delete the security group.
- If the security group to be deleted has been associated with rules of another security group (**Source**), delete or modify the associated security group rules, and then delete the security group.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, locate the row that contains the target security group, click **More** in the **Operation** column, and click **Delete**.
5. Click **Yes** in the displayed dialog box.

4.1.12 Adding Instances to and Removing Them from a Security Group

Scenarios

After a security group is created, you can add instances, including servers and extension NICs, to the security group to protect the instances. If the instances are not required, you can also remove them from the security group.

You can add multiple instances to or remove them from a security group.

Adding Instances to a Security Group

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click **Manage Instance** in the **Operation** column.
5. On the **Servers** tab, click **Add** and add one or more servers to the current security group.
6. On the **Extension NICs** tab, click **Add** and add one or more extension NICs to the current security group.
7. Click **OK**.

Removing Instances from a Security Group

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click **Manage Instance** in the **Operation** column.
5. On the **Servers** tab, locate the target server and click **Remove** in the **Operation** column to remove the server from current security group.
6. On the **Extension NICs** tab, locate the target extension NIC and click **Remove** in the **Operation** column to remove the NIC from the current security group.
7. Click **Yes**.

Removing multiple instances from a security group

Select multiple servers and click **Remove** above the server list to remove the selected servers from the current security group all at once.

Select multiple extension NICs and click **Remove** above the extension NIC list to remove the selected extension NICs from the current security group all at once.

4.1.13 Cloning a Security Group

Scenarios

You can clone a security group from one region to another to quickly apply the security group rules to ECSs in another region.

You can clone a security group in the following scenarios:

- For example, you have security group **sg-A** in region A. If ECSs in region B require the same security group rules as those configured for security group **sg-A**, you can clone security group **sg-A** to region B, freeing you from creating a new security group in region B.
- If you need new security group rules, you can clone the original security group as a backup.

Notes and Constraints

In cross-region security group cloning, only rules whose source and destination are CIDR blocks and rules whose source and destination are the current security group will be cloned.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, locate the row that contains the target security group and choose **More** > **Clone** in the **Operation** column.
5. Set required parameters and click **OK**.

   You can then switch to the required region to view the cloned security group in the security group list.

4.1.14 Modifying a Security Group

Scenarios

Modify the name and description of a created security group.

Procedure

Method 1

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, locate the target security group and choose **More** > **Modify** in the **Operation** column.
5. Modify the name and description of the security group as required.
6. Click **OK**.

Method 2

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click the security group name.
5. On the displayed page, click  on the right of **Name** and edit the security group name.
6. Click **√** to save the security group name.
7. Click  on the right of **Description** and edit the security group description.
8. Click **√** to save the security group description.

4.1.15 Viewing the Security Group of an ECS

Scenarios

View inbound and outbound rules of a security group used by an ECS.

Procedure

1. Log in to the management console.
2. Log in to ManageOne as a VDC administrator or operator using a browser.

   URL: **https://***Address for accessing ManageOne Operation Portal*, for example, **https://console.demo.com**
3. Click  in the upper left corner, select a region, and choose **Computing** > **Elastic Cloud Server**.

   The **Elastic Cloud Server** page is displayed.
4. Under **Computing**, click **Elastic Cloud Server**.
5. On the **Elastic Cloud Server** page, click the name of the target ECS.
6. Click the **Security Groups** tab and view information about the security group used by the ECS.

4.1.16 Changing the Security Group of an ECS

Scenarios

Change the security group associated with an ECS NIC.

Procedure

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Manage Network** > **Change Security Group**.

   The **Change Security Group** dialog box is displayed.
4. Select the target NIC and security group as prompted.

   You can select multiple security groups. In such a case, the access rules of all the selected security groups apply on the ECS. To create a security group, click **Create Security Group**.

   NOTE

   Using multiple security groups may deteriorate ECS network performance. You are suggested to select no more than five security groups.
5. Click **OK**.

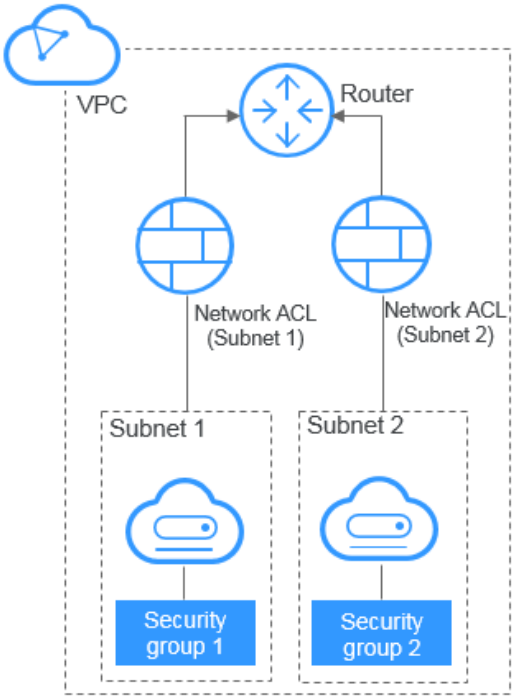
4.2 Network ACL

4.2.1 Network ACL Overview

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

Figure 4-4 shows how a network ACL works.

Figure 4-4 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 access control that is both comprehensive and fine-grained.

4.3 Differences Between Security Groups and Network ACLs summarizes the basic differences between security groups and network ACLs.

Network ACL Basics

- Your VPC does not come with a default network ACL, but you can create one and associate it with a 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 you send a request from your instance and the outbound traffic is allowed, 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 ones. **Table 4-6** shows the default network ACL rules. The default rules cannot be modified or deleted.

Table 4-6 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 one 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, 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 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.

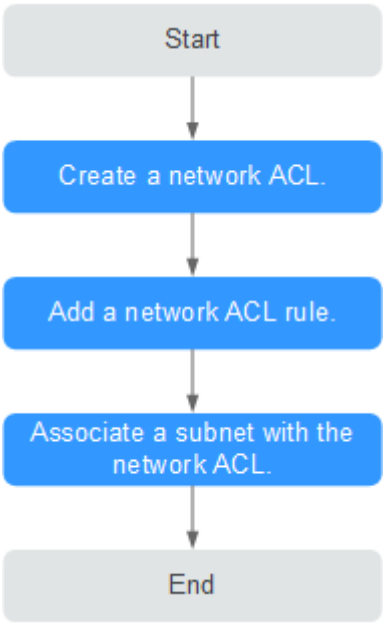
  Solution: You can add network ACL rules to control traffic between subnets.
- For frequently accessed applications, a security rule sequence may need to be adjusted to improve performance.

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

Network ACL Configuration Procedure

Figure 4-5 shows the procedure for configuring a network ACL.

Figure 4-5 Network ACL configuration procedure



1. Create a network ACL by following the steps described in **4.2.3 Creating a Network ACL**.

2. Add network ACL rules by following the steps described in **4.2.4 Adding a Network ACL Rule**.
3. Associate subnets with the network ACL by following the steps described in **4.2.5 Associating Subnets with a Network ACL**. After subnets are associated with the network ACL, the subnets will be protected by the configured network ACL rules.

4.2.2 Network ACL Configuration Examples

This section provides examples for configuring network ACLs.

- **Denying Access from a Specific Port**
- **Allowing Access from Specific Ports and Protocols**

Denying Access from a Specific Port

You might want to block TCP 445 to protect against the WannaCry ransomware attacks. You can add a network ACL rule to deny all incoming traffic from TCP port 445.

Network ACL Configuration

Table 4-7 lists the inbound rule required.

Table 4-7 Network ACL rules

Direction	Action	Protocol	Source	Source Port Range	Destination	Destination Port Range	Description
Inbound	Allow	All	0.0.0.0/0	1-65535	0.0.0.0/0	All	Allows all inbound traffic.
Inbound	Deny	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	445	Denies inbound traffic from any IP address through TCP port 445.

NOTE

By default, a network ACL denies all inbound traffic. You need to allow all inbound traffic if necessary.

Allowing Access from Specific Ports and Protocols

In this example, an ECS in a subnet is used as the web server, and you need to allow inbound traffic from HTTP port 80 and HTTPS port 443 and allow all outbound traffic regardless of the port. You need to configure both the network ACL rules and security group rules to allow the traffic.

Network ACL Configuration

Table 4-8 lists the inbound rule required.

Table 4-8 Network ACL rules

Direction	Action	Protocol	Source	Source Port Range	Destination	Destination Port Range	Description
Inbound	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	80	Allows inbound HTTP traffic from any IP address to ECSs in the subnet through port 80.
Inbound	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	443	Allows inbound HTTPS traffic from any IP address to ECSs in the subnet through port 443.
Outbound	Allow	All	0.0.0.0/0	All	0.0.0.0/0	All	Allows all outbound traffic from the subnet.

Security group configuration

Table 4-9 lists the inbound and outbound security group rules required.

Table 4-9 Security group rules

Direction	Protocol / Application	Port	Source/ Destination	Description
Inbound	TCP	80	Source: 0.0.0.0/0	Allows inbound HTTP traffic from any IP address to ECSs associated with the security group through port 80.
Inbound	TCP	443	Source: 0.0.0.0/0	Allows inbound HTTPS traffic from any IP address to ECSs associated with the security group through port 443.

Direction	Protocol / Application	Port	Source/ Destination	Description
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic from the security group.

A network ACL adds an additional layer of security. Even if the security group rules allow more traffic than that actually required, the network ACL rules allow only access from HTTP port 80 and HTTPS port 443 and deny other inbound traffic.

4.2.3 Creating a Network ACL

Scenarios

You can create a custom network ACL, but any newly created network ACL will be disabled by default. It will not have any inbound or outbound rules, or have any subnets associated. Each user can create up to 200 network ACLs by default.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. In the right pane displayed, click **Create Network ACL**.
5. In the displayed dialog box, enter network ACL information as prompted. **Table 4-10** lists the parameters to be configured.

   Table 4-10 Parameter descriptions

Parameter	Description	Example Value
Name	Specifies the network ACL name. This parameter is mandatory. The name contains a maximum of 64 characters, which may consist of letters, digits, underscores (_), and hyphens (-). The name cannot contain spaces.	fw-92d3
Description	Provides supplementary information about the network ACL. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. Click **OK**.

4.2.4 Adding a Network ACL Rule

Scenarios

Add an inbound or outbound rule based on your network security requirements.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, click **Add Rule** to add an inbound or outbound rule.

   You can click **+** to add more rules.

Table 4-11 Parameter descriptions

Parameter	Description	Example Value
Type	Specifies the network ACL type. This parameter is mandatory. You can select a value from the drop-down list. Currently, only **IPv4** and **IPv6** are supported.	IPv4
Action	Specifies the action in the network ACL. This parameter is mandatory. You can select a value from the drop-down list. Currently, the value can be **Allow** or **Deny**.	Allow
Protocol	Specifies the protocol supported by the network ACL. This parameter is mandatory. You can select a value from the drop-down list. The value can be **TCP**, **UDP**, **All**, or **ICMP**. If **ICMP** or **All** is selected, you do not need to specify port information.	TCP
Source	Specifies the source from which the traffic is allowed. The source can be an IP address or IP address range. The default value is **0.0.0.0/0**, which indicates that traffic from all IP addresses is allowed. For example: • xxx.xxx.xxx.xxx/32 (IP address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses)	0.0.0.0/0

Parameter	Description	Example Value
Source Port Range	Specifies the source port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, **1-100**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22, or 22-30
Destination	Specifies the destination to which the traffic is allowed. The destination can be an IP address or IP address range. The default value is **0.0.0.0/0**, which indicates that traffic to all IP addresses is allowed. For example: • xxx.xxx.xxx.xxx/32 (IP address) • xxx.xxx.xxx.0/24 (IP address range) • 0.0.0.0/0 (all IP addresses)	0.0.0.0/0
Destination Port Range	Specifies the destination port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, **1-100**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22, or 22-30
Description	Provides supplementary information about the network ACL rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. Click **OK**.

4.2.5 Associating Subnets with a Network ACL

Scenarios

On the page showing network ACL details, associate desired subnets with a network ACL. After a network ACL is associated with a subnet, the network ACL denies all traffic to and from the subnet until you add rules to allow traffic.

Procedure

1. Log in to the management console.

2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the displayed page, click the **Associated Subnets** tab.
6. On the **Associated Subnets** page, click **Associate**.
7. On the displayed page, select the subnets to be associated with the network ACL, and click **OK**.

NOTE

Subnets that have already been associated with network ACLs will not be displayed on the page for you to select. One-click subnet association and disassociation are not currently supported. Furthermore, a subnet can only be associated with one network ACL. If you want to reassociate a subnet that has already been associated with another network ACL, you must first disassociate the subnet from the original network ACL.

4.2.6 Disassociating a Subnet from a Network ACL

Scenarios

Disassociate a subnet from a network ACL when necessary.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the displayed page, click the **Associated Subnets** tab.
6. On the **Associated Subnets** page, locate the row that contains the target subnet and click **Disassociate** in the **Operation** column.
7. Click **Yes** in the displayed dialog box.

Disassociating subnets from a network ACL

Select multiple subnets and click **Disassociate** above the subnet list to disassociate the subnets from the current network ACL at a time.

4.2.7 Changing the Sequence of a Network ACL Rule

Scenarios

If multiple network ACL rules conflict, the rule in the front takes precedence. 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.

Procedure

1. Log in to the management console.

2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, locate the target rule, click **More** in the **Operation** column, and select **Insert Rule Above** or **Insert Rule Below**.
6. In the displayed dialog box, configure required parameters and click **OK**.

   The rule is inserted. The procedure for inserting an outbound rule is the same as that for inserting an inbound rule.

4.2.8 Modifying a Network ACL Rule

Scenarios

Modify an inbound or outbound network ACL rule based on your network security requirements.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule and click **Modify** in the **Operation** column. In the displayed dialog box, configure parameters as prompted. **Table 4-12** lists the parameters to be configured.

Table 4-12 Parameter descriptions

Parameter	Description	Example Value
Type	Specifies the network ACL type. This parameter is mandatory. You can select a value from the drop-down list. Currently, only **IPv4** and **IPv6** are supported.	IPv4
Action	Specifies the action in the network ACL. This parameter is mandatory. You can select a value from the drop-down list. Currently, the value can be **Allow** or **Deny**.	Allow

Parameter	Description	Example Value
Protocol	Specifies the protocol supported by the network ACL. This parameter is mandatory. You can select a value from the drop-down list. The value can be **TCP**, **UDP**, **All**, or **ICMP**. If **ICMP** or **All** is selected, you do not need to specify port information.	TCP
Source	Specifies the source from which the traffic is allowed. The source can be an IP address or IP address range. The default value is **0.0.0.0/0**, which indicates that traffic from all IP addresses is allowed. For example: ● xxx.xxx.xxx.xxx/32 (IP address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses)	0.0.0.0/0
Source Port Range	Specifies the source port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, **1-100**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22, or 22-30
Destination	Specifies the destination to which the traffic is allowed. The destination can be an IP address or IP address range. The default value is **0.0.0.0/0**, which indicates that traffic to all IP addresses is allowed. For example: ● xxx.xxx.xxx.xxx/32 (IP address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses)	0.0.0.0/0
Destination Port Range	Specifies the destination port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, **1-100**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22, or 22-30

Parameter	Description	Example Value
Description	Provides supplementary information about the network ACL rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

6. Click **Confirm**.

4.2.9 Enabling or Disabling a Network ACL Rule

Scenarios

Enable or disable an inbound or outbound rule based on your network security requirements.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule, and click **Enable** or **Disable** in the **Operation** column.
6. Click **Yes** in the displayed dialog box.

   The rule is enabled or disabled. The procedure for enabling or disabling an outbound rule is the same as that for enabling or disabling an inbound rule.

4.2.10 Deleting a Network ACL Rule

Scenarios

Delete an inbound or outbound rule based on your network security requirements.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule and click **Delete** in the **Operation** column.

6. Click **Yes** in the displayed dialog box.

Deleting multiple network ACL rules at a time

You can also select multiple network ACL rules and click **Delete** above the network ACL rule list to delete multiple rules at a time.

4.2.11 Exporting and Importing Network ACL Rules

Scenarios

You can export inbound and outbound rules of a specific network ACL as an Excel file then import these rules for another network ACL. Importing and exporting rules across regions are supported.

Exporting Network ACL Rules

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. Click  to export the inbound and outbound network ACL rules. The exported rules are stored in an Excel file. You need to download the file to a local directory.

Importing Network ACL Rules

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. Click  .
6. Select the Excel file containing the exported network ACL rules and click **Import** to import the rules.

4.2.12 Viewing a Network ACL

Scenarios

View details about a network ACL.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.

3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the displayed page, click the **Inbound Rules**, **Outbound Rules**, and **Associated Subnets** tabs one by one to view details about inbound rules, outbound rules, and subnet associations.

4.2.13 Modifying a Network ACL

Scenarios

Modify the name and description of a network ACL.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the displayed page, click on the right of **Name** and edit the network ACL name.
6. Click √ to save the new network ACL name.
7. Click on the right of Description and edit the network ACL description.
8. Click √ to save the new network ACL description.

4.2.14 Enabling or Disabling a Network ACL

Scenarios

After a network ACL is created, you may need to enable it based on network security requirements. You can also disable an enabled network ACL if need. Before enabling a network ACL, ensure that subnets have been associated with the network ACL and that inbound and outbound rules have been added to the network ACL.

When a network ACL is disabled, custom rules will become invalid. Disabling a network ACL may interrupt network traffic. For information about the default network ACL rules, see **Default Network ACL Rules**.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the row that contains the target network ACL in the right pane, click **More** in the **Operation** column, and click **Enable** or **Disable**.
5. Click **Yes** in the displayed dialog box.

4.2.15 Deleting a Network ACL

Scenarios

Delete a network ACL when it is no longer required.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate the target network ACL in the right pane, click **More** in the **Operation** column, and click **Delete**.
5. Click **Yes**.

   NOTE

   After a network ACL is deleted, associated subnets are disassociated and added rules are deleted from the network ACL.

4.3 Differences Between Security Groups and Network ACLs

You can configure security groups and network ACL to increase the security of ECSs in your VPC.

- Security groups operate at the ECS level.
- Network ACLs operate at the subnet level.

For details, see **Figure 4-6**.

Figure 4-6 Security groups and network ACLs

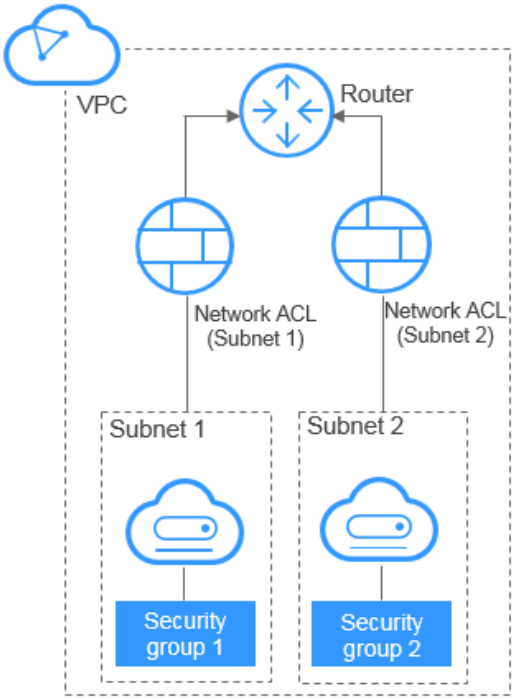


Table 4-13 describes the differences between security groups and network ACLs.

Table 4-13 Differences between security groups and network ACLs

Category	Security Group	Network ACL
Targets	Operates at the ECS level.	Operates at the subnet level.
Rules	Only supports **Allow** rules.	Supports **Allow** and **Deny** rules.
Priority	If security group rules conflict, the overlapping elements of these rules take effect.	If rules conflict, the rule with the highest priority takes effect.
Usage	Automatically applies to ECSs in the security group that is selected during ECS creation. You must select a security group when creating ECSs.	Applies to all ECSs in the subnets associated with the network ACL. Selecting a network ACL is not allowed during subnet creation. You must create a network ACL, associate subnets with it, add inbound and outbound rules, and enable network ACL. The network ACL then takes effect for the associated subnets and ECSs in the subnets.

Category	Security Group	Network ACL
Packets	Only packet filtering based on the 3-tuple (protocol, port, and peer IP address) is supported.	Only packet filtering based on the 5-tuple (protocol, source port, destination port, source IP address, and destination IP address) is supported.

5 EIP

5.1 Assigning an EIP and Binding It to an ECS

Scenarios

You can assign an EIP and bind it to an ECS so that the ECS can access the Internet.

Assigning an EIP

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, click **Assign EIP**.
4. Set the parameters as prompted.

Table 5-1 Parameter descriptions

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	N/A
EIP Type	**Dynamic BGP**: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP

Parameter	Description	Example Value
Billed By	The following bandwidth types are available: • **Bandwidth**: You specify a maximum bandwidth and pay for the amount of time you use the bandwidth. This is suitable for scenarios with heavy or stable traffic. • **Traffic**: You specify a maximum bandwidth and pay for the total traffic you use. This is suitable for scenarios with light or sharply fluctuating traffic. • **Shared Bandwidth**: The bandwidth can be shared by multiple EIPs. This is suitable for scenarios with staggered traffic.	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	100
Bandwidth Name	The name of the bandwidth.	bandwidth
Tag	Specifies the EIP tags. Each tag contains a key and value pair. The tag key and value must meet the requirements listed in **Table 5-2**.	• Key: Ipv4_key1 • Value: 192.168.12.10
Quantity	The number of EIPs you want to purchase.	1
Enterprise Project	The enterprise project to which the EIP belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the *Enterprise Management User Guide*.	default

Table 5-2 EIP tag requirements

Parameter	Requirement	Example Value
Key	• Cannot be left blank. • Must be unique for each EIP. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	Ipv4_key1
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	192.168.12.10

5. Click **Create Now**.
6. Click **Submit**.

Binding an EIP

1. On the **EIPs** page, locate the row that contains the target EIP, and click **Bind**.
2. Select the instance to which you want to bind the EIP.
3. Click **OK**.

5.2 Unbinding an EIP from an ECS and Releasing the EIP

Scenarios

If you no longer need an EIP, unbind it from the ECS and release the EIP to avoid wasting network resources.

Notes and Constraints

- You can only release unbound EIPs.
- You cannot buy an EIP that has been released if it is currently in use by another user.

Procedure

Unbinding a single EIP

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, locate the row that contains the target EIP, and click **Unbind**.

4. Click **Yes** in the displayed dialog box.

Releasing a single EIP

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, locate the row that contains the target EIP, click **More** and then **Release** in the **Operation** column.
4. Click **Yes** in the displayed dialog box.

Unbinding multiple EIPs at once

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, select the EIPs to be unbound.
4. Click the **Unbind** button located above the EIP list.
5. Click **Yes** in the displayed dialog box.

Releasing multiple EIPs at once

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, select the EIPs to be released.
4. Click the **Release** button located above the EIP list.
5. Click **Yes** in the displayed dialog box.

5.3 Managing EIP Tags

Scenarios

Tags can be added to EIPs to facilitate EIP identification and administration. You can add a tag to an EIP when assigning the EIP. Alternatively, you can add a tag to an assigned EIP on the EIP details page. A maximum of 10 tags can be added to each EIP.

A tag consists of a key and value pair. **Table 5-3** lists the tag key and value requirements.

Table 5-3 EIP tag requirements

Parameter	Requirement	Example Value
Key	• Cannot be left blank. • Must be unique for each EIP. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-).	Ipv4_key1

Parameter	Requirement	Example Value
Value	• Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	192.168.12.10

Procedure

Searching for EIPs by tag key and value on the page showing the EIP list

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. In the upper right corner of the EIP list, click **Search by Tag**.
4. In the displayed area, enter the tag key and value of the EIP you are looking for.

   You must specify both the tag key and value. The system will display the EIPs that contain the tag you specified.
5. Click **+** to add another tag key and value.

   You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for EIPs, the system will display the EIPs that contain all the tags you specified.
6. Click **Search**.

   The system displays the EIPs you are looking for based on the entered tag keys and values.

Adding, deleting, editing, and viewing tags on the Tags tab of an EIP

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, locate the EIP whose tags are to be managed, and click the EIP name.
4. On the page showing EIP details, click the **Tags** tab and perform desired operations on tags.
   - View tags.

     On the **Tags** tab, you can view details about tags added to the current EIP, including the number of tags and the key and value of each tag.
   - Add a tag.

     Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.
   - Edit a tag.

     Locate the row that contains the tag you want to edit, and click **Edit** in the **Operation** column. Enter the new tag key and value, and click **OK**.
   - Delete a tag.

     Locate the row that contains the tag you want to delete, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

5.4 Modifying EIP Bandwidth

Scenarios

Modify the EIP bandwidth name or size.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. Locate the row that contains the target EIP in the EIP list, click **More** in the **Operation** column, and select **Modify Bandwidth**.
4. Modify the bandwidth parameters as prompted.
5. Click **Next**.
6. Click **Submit**.

5.5 Exporting EIP Information

Scenarios

The information of all EIPs under your account can be exported in an Excel file to a local directory. The file records the ID, status, type, bandwidth name, and bandwidth size of EIPs.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Elastic IP**.
3. On the displayed page, click  in the upper right corner of the EIP list.

   The system will automatically export all EIPs in the current region of your account to an Excel file and download the file to a local directory.

6 Shared Bandwidth

6.1 Shared Bandwidth Overview

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.

When you host a large number of applications on the cloud, if each EIP uses an independent bandwidth, a lot of bandwidths are required, increasing O&M workload. If all EIPs share the same bandwidth, VPCs and the region-level bandwidth can be managed in a unified manner, simplifying O&M statistics and network operations cost settlement.

- Lowered Bandwidth Costs

  Region-level bandwidth sharing and multiplexing reduce bandwidth usage and O&M costs.
- Easy to Manage

  Region-level bandwidth sharing and multiplexing simplify O&M statistics, management, and operations cost settlement.
- Flexible Operations

  You can add EIPs that are billed on a pay-per-use basis to a shared bandwidth or remove them from a shared bandwidth regardless of the instances to which they are bound.

6.2 Assigning Shared Bandwidth

Scenarios

Assign a shared bandwidth for use with EIPs.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.

3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the upper right corner, click **Assign Shared Bandwidth**. On the displayed page, configure parameters as prompted.

   Table 6-1 Parameter descriptions

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	N/A
Bandwidth	The bandwidth size in Mbit/s. The maximum bandwidth can be 300 Mbit/s.	10
Enterprise Project	The enterprise project to which the EIP belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the *Enterprise Management User Guide*.	default
Bandwidth Name	The name of the shared bandwidth.	Bandwidth-001

5. Click **Create Now**.

6.3 Adding EIPs to a Shared Bandwidth

Scenarios

Add EIPs to a shared bandwidth and the EIPs can then share that bandwidth. You can add multiple EIPs to a shared bandwidth at the same time.

Notes and Constraints

- After an EIP is added to a shared bandwidth, the original bandwidth used by the EIP will become invalid and the EIP will start to use the shared bandwidth.
- The EIP's original dedicated bandwidth will be deleted.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the shared bandwidth to which you want to add EIPs. In the **Operation** column, choose **Add Public IP Address**, and select the EIPs to be added.
5. Click **OK**.

6.4 Removing EIPs from a Shared Bandwidth

Scenarios

Remove EIPs that are no longer required from a shared bandwidth if needed.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the bandwidth from which EIPs are to be removed, choose **More** > **Remove Public IP Address** in the **Operation** column, and select the EIPs to be removed in the displayed dialog box.
5. Click **OK**.

6.5 Modifying a Shared Bandwidth

Scenarios

You can modify the name and size of a shared bandwidth, which takes effect immediately.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the shared bandwidth you want to modify, click **Modify Bandwidth** in the **Operation** column, and modify the bandwidth settings.
5. Click **Next**.

6. Click **Submit**.

6.6 Deleting a Shared Bandwidth

Scenarios

Delete a shared bandwidth when it is no longer required.

Prerequisites

Before deleting a shared bandwidth, remove all the EIPs associated with it. For details, see **6.4 Removing EIPs from a Shared Bandwidth**.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the shared bandwidth you want to delete, click **More** in the **Operation** column, and then click **Delete**.
5. In the displayed dialog box, click **Yes**.

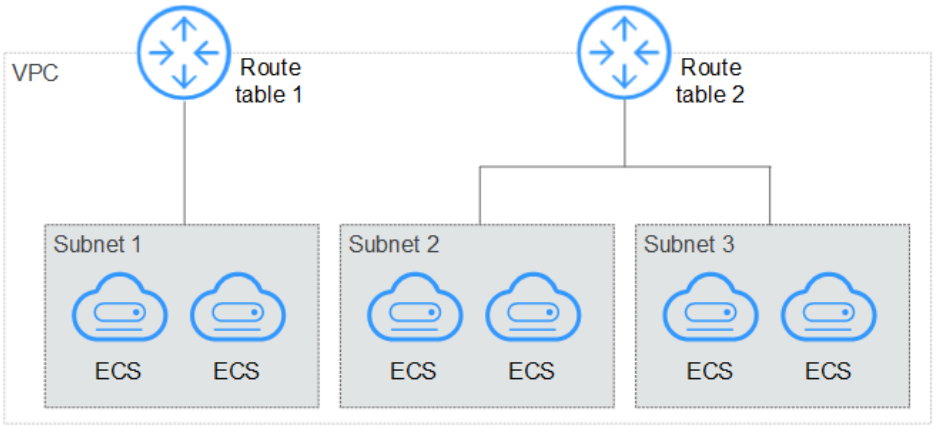
7 Route Table

7.1 Route Table Overview

Route Table

A route table contains a set of rules, called routes, that are used to control where inbound and outbound subnet traffic is forwarded within a VPC. Each subnet in your VPC must be associated with a route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Figure 7-1 Route table



Default Route Table and Custom Route Table

When you create a VPC, the system automatically generates a default route table for the VPC. After a subnet is created, the subnet automatically associates with the default route table. 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 or Direct Connect connection, the default route table automatically delivers a route that cannot be deleted or modified. You can associate the subnet with the custom route table or replicate the route to the custom route table, and then add, modify, or delete the route in the custom route table.

You can use the default route table or create a custom route table for a subnet and then associate the custom route table with the subnet. You can delete the custom route table if it is no longer required.

NOTE

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

For details about how to create a custom route table, see section **7.3 Creating a Custom Route Table**.

Route

A route, that is a routing rule, is configured with the destination, next hop type, and next hop to determine where the network traffic is directed. Routes are classified into system routes and custom routes.

- System route: Routes that 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.

    NOTE

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

- Custom route: A route that can be modified and deleted. 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 the network traffic is directed. **Table 7-1** lists the supported types of next hops.

Table 7-1 Next hop type

Next Hop Type	Description
ECS	Traffic intended for the destination is forwarded to an ECS in the VPC.
Extension NIC	Traffic intended for the destination is forwarded to the extension NIC of an ECS in the VPC.
VPN gateway	Traffic intended for the destination is forwarded to a VPN gateway.
Direct Connect gateway	Traffic intended for the destination is forwarded to a Direct Connect gateway.
NAT gateway	Traffic intended for the destination is forwarded to a NAT gateway.

Next Hop Type	Description
VPC peering connection	Traffic intended for the destination is forwarded to a VPC peering connection.
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.
VPC endpoint	Traffic intended for the destination is forwarded to a VPC endpoint.

NOTE

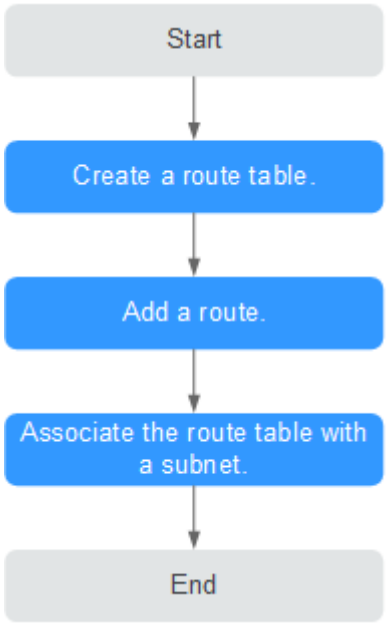
- When you add a custom route to a default route table, the next hop type cannot be set to VPN gateway or Direct Connect gateway.
- If you have to specify the destination when creating a service, a system route is delivered. If you do not need to specify a destination when creating a service, a custom route that can be modified or deleted is delivered automatically.

  For example, you do not need to specify a destination when creating a NAT gateway, the system automatically delivers a custom route that you can modify or delete. However, when you create a VPN gateway or Direct Connect gateway, you need to specify the remote subnet, that is, the destination of a route. In this case, the system delivers a system route. If the route destination can be modified on the **Route Tables** page, the destination will be inconsistent with that configured remote subnet. To modify the destination, you can go to the specific service page to modify the remote subnet, then the route destination will be changed accordingly.

Custom Route Table Configuration Process

Figure 7-2 shows the process of creating and configuring a custom route table.

Figure 7-2 Route table configuration process



1. For details about how to create a custom route table, see **7.3 Creating a Custom Route Table**.
2. For details about how to add a custom route, see **7.4 Adding a Custom Route**.
3. For details about how to associate a subnet with a route table, see **7.5 Associating a Subnet with a Route Table**. After the association, the routes in the route table control the routing for the subnet.

Notes and Constraints

- A maximum of 10 route tables, including the default one, can be created for each VPC.
- A maximum of 200 routes can be added to each route table.
- The default route table cannot be deleted.
- The system route cannot be modified or deleted.
- The routes delivered by the VPN and Direct Connect services to the default route table cannot be modified or deleted.
- The gateway VPC endpoint routes delivered by the VPC Endpoint service to the default route table cannot be modified, replicated, or deleted. In addition, a gateway VPC endpoint route in the custom route table cannot be modified or deleted.
- When you add a custom route to a default route table, the next hop type cannot be set to VPN gateway or Direct Connect gateway.

7.2 Configuring an SNAT Server

Scenarios

To use the route table function provided by the VPC service, you need to configure SNAT on an ECS to enable other ECSs that do not have EIPs bound in a VPC to access the Internet through this ECS.

The configured SNAT takes effect for all subnets in a VPC.

Prerequisites

- You have an ECS where SNAT is to be configured.
- The ECS where SNAT is to be configured runs the Linux OS.
- The ECS where SNAT is to be configured has only one network interface card (NIC).

Differences Between SNAT Servers and NAT Gateways

The NAT Gateway service provides network address translation (NAT) for servers, such as ECSs, BMSs, and Workspace desktops, in a VPC or servers that connect to a VPC through Direct Connect or VPN in local data centers. A NAT gateway allows these servers to access the Internet using EIPs or to provide services for the Internet.

The NAT Gateway service is easier to configure and use than SNAT. This service can be flexibly deployed across subnets and AZs and supports different NAT

gateway specifications. You can click **NAT Gateway** under **Network** on the management console to try this service.

For details, see the *NAT Gateway User Guide*.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Computing**, click **Elastic Cloud Server**.
3. On the displayed page, locate the target ECS in the ECS list and click the ECS name to switch to the page showing ECS details.
4. On the displayed ECS details page, click the **NICs** tab.
5. Click the NIC IP address. In the displayed area showing the NIC details, disable the source/destination check function.

   By default, the source/destination check is enabled. When this check is enabled, the system checks whether source IP addresses contained in the packets sent by ECSs are correct. If the IP addresses are incorrect, the system does not allow the ECSs to send the packets. This mechanism prevents packet spoofing, thereby improving system security. If SNAT is used, the SNAT server needs to forward packets. This mechanism prevents the packet sender from receiving returned packets. Therefore, you need to disable the source/destination check for SNAT servers.
6. Bind an EIP.
   - Bind an EIP with the private IP address of the ECS. For details, see **5.1 Assigning an EIP and Binding It to an ECS**.
   - Bind an EIP with the virtual IP address of the ECS. For details, see **9.3 Binding a Virtual IP Address to an EIP or ECS**.
7. On the ECS console, use the remote login function to log in to the ECS where you plan to configure SNAT.
8. Run the following command and enter the password of user **root** to switch to user **root**:

   su - root
9. Run the following command to check whether the ECS can successfully connect to the Internet:

   NOTE

   Before running the command, you must disable the response iptables rule on the ECS where SNAT is configured and enable the security group rules.

   ping www.google.com

   The ECS can access the Internet if the following information is displayed:

```
[root@localhost ~]# ping www.google.com
PING www.a.shifen.com (xxx.xxx.xxx.xxx) 56(84) bytes of data.
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=1 ttl=51 time=9.34 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=2 ttl=51 time=9.11 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=3 ttl=51 time=8.99 ms
```

10. Run the following command to check whether IP forwarding of the Linux OS is enabled:

    cat /proc/sys/net/ipv4/ip_forward

    In the command output, **1** indicates it is enabled, and **0** indicates it is disabled. The default value is **0**.

- If IP forwarding in Linux is enabled, go to step **13**.
- If IP forwarding in Linux is disabled, perform step **11** to enable IP forwarding in Linux.

Many OSs support packet routing. Before forwarding packets, OSs change source IP addresses in the packets to OS IP addresses. Therefore, the forwarded packets contain the IP address of the public sender so that the response packets can be sent back along the same path to the initial packet sender. This method is called SNAT. The OSs need to keep track of the packets where IP addresses have been changed to ensure that the destination IP addresses in the packets can be rewritten and that packets can be forwarded to the initial packet sender. To achieve these purposes, you need to enable the IP forwarding function and configure SNAT rules.

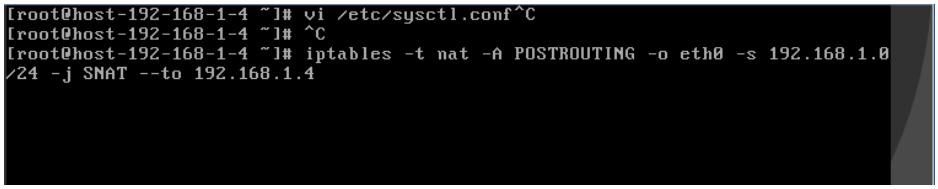
11. Use the vi editor to open the **/etc/sysctl.conf** file, change the value of **net.ipv4.ip_forward** to **1**, and enter **:wq** to save the change and exit.
12. Run the following command to make the change take effect:

    sysctl -p /etc/sysctl.conf
13. Configure SNAT.

    Run the following command to enable all ECSs on the network segment (for example, 192.168.1.0/24) to access the Internet using the SNAT function: **Figure 7-3** shows the example command.

    iptables -t nat -A POSTROUTING -o eth0 -s subnet -j SNAT --to nat-instance-ip

    Figure 7-3 Configuring SNAT

    NOTE

    - To ensure that the rule will not be lost after the restart, write the rule into the **/etc/rc.local** file.
      1. Run the following command to switch to the **/etc/sysctl.conf** file:

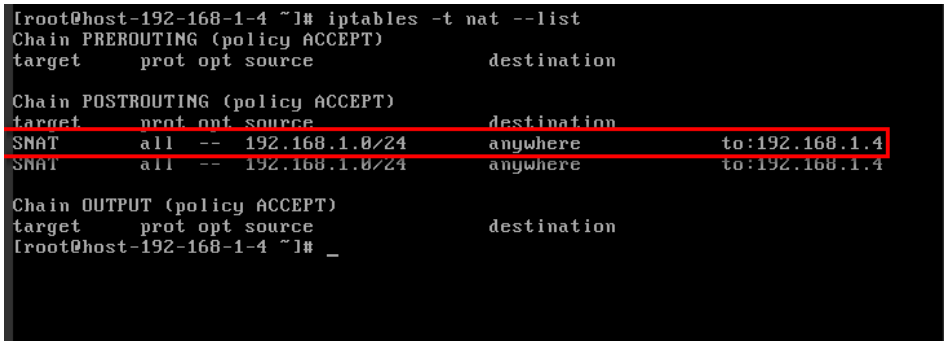
         vi /etc/rc.local
      2. Perform **14** to configure SNAT.
      3. Run the following command to save the configuration and exit:

         :wq
      4. Run the following command to add the execute permission for the **rc.local** file:

         # chmod +x /etc/rc.local
    - To ensure that the configuration takes effect, run the **iptables -L** command to check whether the configured rules conflict with each other.
14. Run the following command to check whether the operation is successful: If information similar to **Figure 7-4** (for example, 192.168.1.0/24) is displayed, the operation was successful.

    iptables -t nat --list

Figure 7-4 Verifying configuration



15. Add a route. For details, see section **7.4 Adding a Custom Route**.

    Set the destination to **0.0.0.0/0**, and the next hop to the private or virtual IP address of the ECS where SNAT is deployed. For example, the next hop is **192.168.1.4**.

After these operations are complete, if the network communication still fails, check your security group and network ACL configuration to see whether required traffic is allowed.

7.3 Creating a Custom Route Table

Scenarios

You can create a custom route table if you do not want to use the default one.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the upper right corner, click **Create Route Table**. On the displayed page, configure parameters as prompted.

Table 7-2 Parameter descriptions

Parameter	Description	Example Value
Name	Specifies the name of the route table. This parameter is mandatory. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	rtb-001
VPC	Specifies the VPC to which the route table belongs. This parameter is mandatory.	vpc-001

Parameter	Description	Example Value
Description	Provides supplementary information about the route table. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-
Route Settings	Specifies the route information. This parameter is optional. You can add a route when creating the route table or after the route table is created. For details, see **7.4 Adding a Custom Route**. You can click **+** to add more routes.	-

5. Click **OK**.

   A message is displayed. You can determine whether to associate the route table with subnets immediately as prompted. If you want to associate immediately, perform the following operations:

   a. Click **Associate Subnet**. The **Associated Subnets** page is displayed.
   b. Click **Associate Subnet** and select the target subnets to be associated.
   c. Click **OK**.

7.4 Adding a Custom Route

Scenarios

Each route table contains a default system route, which indicates that ECSs in a VPC can communicate with each other. You can add custom routes as required to forward the traffic destined for the destination to the specified next hop.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the route table list, click the name of the route table to which you want to add a route.
5. Click **Add Route** and set parameters as prompted.

   You can click **+** to add more routes.

Table 7-3 Parameter descriptions

Parameter	Description	Example Value
Destination	Specifies the destination CIDR block. The destination of each route must be unique. The destination cannot overlap with any subnet CIDR block in the VPC.	192.168.0.0/16
Next Hop Type	Set the type of the next hop. For details about the supported resource types, see **Table 7-1**. **NOTE** When adding a custom route to or modifying a custom route in a default route table, the next hop type cannot be set to VPN gateway or Direct Connect gateway.	ECS
Next Hop	Set the next hop. The resources in the drop-down list box are displayed based on the selected next hop type.	ecs-001
Description	Provides supplementary information about the route. This parameter is optional. The route description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

6. Click **OK**.

7.5 Associating a Subnet with a Route Table

Scenarios

After a route table is associated with a subnet, the routes in the route table control the routing for the subnet and apply to all cloud resources in the subnet. Determine the impact on services before performing this operation.

Notes and Constraints

A subnet can only be associated with one route table.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the route table list, locate the row that contains the target route table and click **Associate Subnet** in the **Operation** column.
5. Select the subnet to be associated.

6. Click **OK**.

7.6 Changing the Route Table Associated with a Subnet

Scenarios

You can change the route table associated with the subnet to another one in the VPC. If the route table for a subnet is changed, routes in the new route table will apply to all cloud resources in the subnet. Determine the impact on services before performing this operation.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the route table list, click the name of the target route table.
5. On the **Associated Subnets** tab page, click **Change Route Table** in the **Operation** column and select a new route table as prompted.
6. Click **OK**.

   After the route table for a subnet is changed, routes in the new route table will apply to all cloud resources in the subnet.

7.7 Viewing a Route Table

Scenarios

You can view the basic information, routes, and associated subnets of a route table.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the route table list, click the name of the target route table.

7.8 Deleting a Route Table

Scenarios

You can delete custom route tables but cannot delete the default route table.

Prerequisites

Before deleting a route table, ensure that no subnet has been associated with the custom route table. If there is an associated subnet, associate the subnet with

another route table by clicking **Change Route Table** and then delete the custom route table.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the route table list, locate the row that contains the route table to be deleted and click **Delete** in the **Operation** column.
5. Click **Yes**.

7.9 Modifying a Route

Scenarios

Modify a route.

Notes and Constraints

- The system route cannot be modified.
- The routes delivered by the VPN, Direct Connect services to the default route table cannot be modified. The route of a gateway VPC endpoint delivered by a VPC endpoint to the default route table cannot be modified. In addition, the route of a gateway VPC endpoint in the custom route table cannot be modified.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the route table list, click the name of the target route table.
5. Locate the row that contains the route to be modified and click **Modify** in the **Operation** column.
6. Modify the route information in the displayed dialog box.

Table 7-4 Parameter descriptions

Parameter	Description	Example Value
Destination	Specifies the destination CIDR block. The destination of each route must be unique. The destination cannot overlap with any subnet CIDR block in the VPC.	192.168.0.0/16

Parameter	Description	Example Value
Next Hop Type	Set the type of the next hop. For details about the supported resource types, see Table 7-1. **NOTE** When adding a custom route to or modifying a custom route in a default route table, the next hop type cannot be set to VPN gateway or Direct Connect gateway.	ECS
Next Hop	Set the next hop. The resources in the drop-down list box are displayed based on the selected next hop type.	ecs-001
Description	Provides supplementary information about the route. This parameter is optional. The route description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

7. Click **OK**.

7.10 Deleting a Route

Scenarios

Delete a custom route if it is no longer required.

Notes and Constraints

- The system route cannot be deleted.
- The routes delivered by the VPN, Direct Connect services to the default route table cannot be deleted. The route of a gateway VPC endpoint delivered by a VPC endpoint to the default route table cannot be deleted. In addition, the route of a gateway VPC endpoint in the custom route table cannot be deleted.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the route table list, click the name of the target route table.
5. Locate the row that contains the route to be deleted and click **Delete** in the **Operation** column.
6. Click **Yes**.

7.11 Replicating a Route

Scenarios

You can replicate a created route as required.

Notes and Constraints

- The gateway VPC endpoint routes delivered by the VPC Endpoint service to the default route table cannot be replicated.
- The routes delivered by the VPN service to the default route table cannot be replicated.
- The routes delivered to the default route table by the Direct Connect service that is enabled by call or email cannot be replicated.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the route table list, locate the row that contains the target route table and click **Replicate Route** in the **Operation** column.
5. Select the target route table and then the route to be replicated as prompted.

   The routes listed on the page are those that do not exist in the target route table. You can select one or more routes to replicate to the target route table.
6. Click **OK**.

7.12 Exporting Route Table Information

Scenarios

Information about all route tables under your account can be exported as an Excel file to a local directory. This file records the name, ID, VPC, type, and number of associated subnets of the route tables.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the displayed page, click  in the upper right of the route table list.

   The system will automatically export information about all route tables under your account in the current region as an Excel file to a local directory.

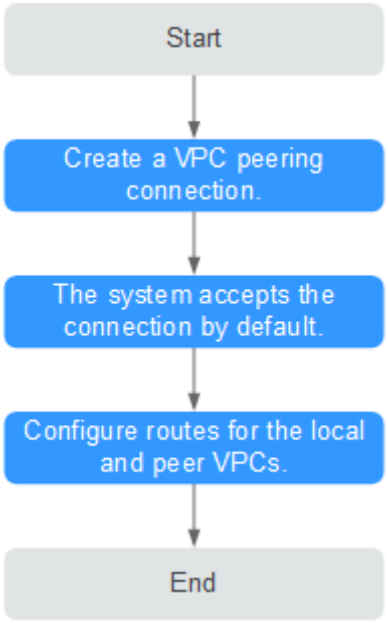
8 VPC Peering Connection

8.1 VPC Peering Connection Creation Procedure

A VPC peering connection is a network connection between two VPCs in one region that enables you to route traffic between them using private IP addresses. ECSs in either VPC can communicate with each other just as if they were in the same region. You can create a VPC peering connection between your own VPCs, or between your VPC and another account's VPC within the same region. A VPC peering connection between VPCs in different regions will not take effect.

- Creating a VPC peering connection between VPCs in your account

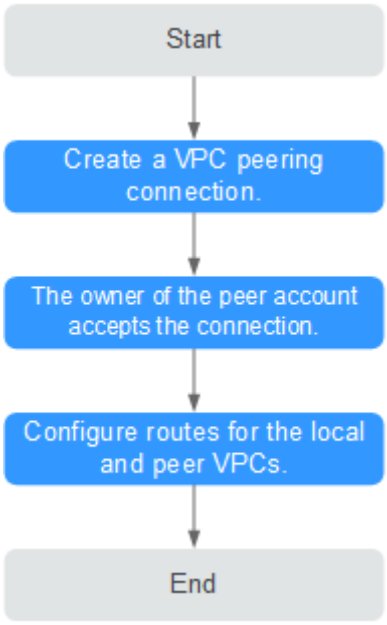
  Figure 8-1 Creating a VPC peering connection between VPCs in your account

  If you create a VPC peering connection between two VPCs in your account, the system automatically accepts the connection by default. You need to add routes for the local and peer VPCs to enable communication between the two VPCs.

- Creating a VPC peering connection with a VPC in another account

  Figure 8-2 Creating a VPC peering connection with a VPC in another account

  If you create a VPC peering connection between your VPC and a VPC that is in another account, the VPC peering connection will be in the **Awaiting acceptance** state. After the owner of the peer account accepts the connection, the connection status changes to **Accepted**. The owners of both the local and peer accounts must configure the routes required by the VPC peering connection to enable communication between the two VPCs.

  If the local and peer VPCs have overlapping CIDR blocks, the routes added for the VPC peering connection may be invalid. Before creating a VPC peering connection between two VPCs that have overlapping CIDR blocks, ensure that none of the subnets in the two VPCs overlap. In this case, the created VPC peering connection enables communication between two subnets in the two VPCs.

  You can run the **ping** command to check whether the two VPCs can communicate with each other.

Notes and Constraints

- VPC peering connections created between VPCs that have overlapping subnet CIDR blocks may not take effect.
- You cannot have more than one VPC peering connection between the same two VPCs at the same time.
- You cannot create a VPC peering connection between VPCs in different regions.
- You cannot use the EIPs in a VPC of a VPC peering connection to access resources in the other VPC. For example, VPC A is peered with VPC B, VPC B has EIPs that can be used to access the Internet, you cannot use EIPs in VPC B to access the Internet from VPC A.
- To request a VPC peering connection with a VPC of another tenant, the peer tenant must accept the request to activate the connection. If you request a

VPC peering connection with a VPC of your own, the system automatically accepts the request to activate the connection.

- After a VPC peering connection is established, the local and peer tenants must add routes in the local and peer VPCs to enable communication between the two VPCs.
- VPC A is peered with both VPC B and VPC C. If VPC B and VPC C have overlapping CIDR blocks, routes with the same destinations cannot be configured for VPC A.
- To ensure security, do not accept VPC peering connections from unknown tenants.
- Either owner of a VPC in a peering connection can delete the VPC peering connection at any time. If a VPC peering connection is deleted by one of its owners, all information about this connection will be automatically deleted immediately, including routes added for the VPC peering connection.
- If two VPCs in a VPC peering connection have overlapping CIDR blocks, the peering connection can only enable communication between two subnets in the two VPCs. If subnets in the two VPCs of a VPC peering connection have overlapping CIDR blocks, the peering connection will not take effect. When creating a VPC peering connection, ensure that the VPCs involved do not contain overlapping subnets.
- You cannot delete a VPC for which VPC peering connection routes have been configured.

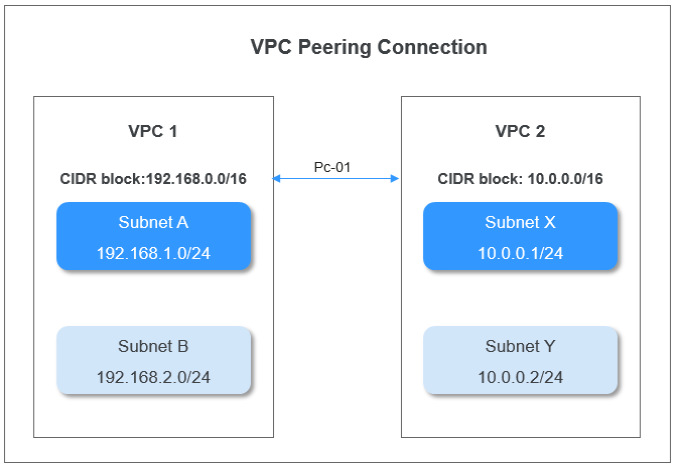
8.2 VPC Peering Connection Configuration Plans

To enable two VPCs to communicate with each other, you can create a VPC peering connection between them. As long as the two VPCs do not overlap, you can configure routes that point to entire VPCs for the VPC peering connection. If the two VPCs have overlapping CIDR blocks, you can only configure routes that point to specific subnets of the VPCs for the VPC peering connection.

- Configurations with Routes to Entire VPCs
  - There can be two or more VPCs peered together using VPC peering connections.
  - Regardless of how many VPCs are connected, if you need to configure routes that point to entire VPCs in a VPC peering connection, none of the VPCs involved in the connection can have overlapping CIDR blocks. Otherwise, the VPC peering connection will be unable to take effect because the routes will be unreachable.
  - The destination of the route that points to an entire VPC is the CIDR block of the peer VPC, and the next hop is the VPC peering connection ID.

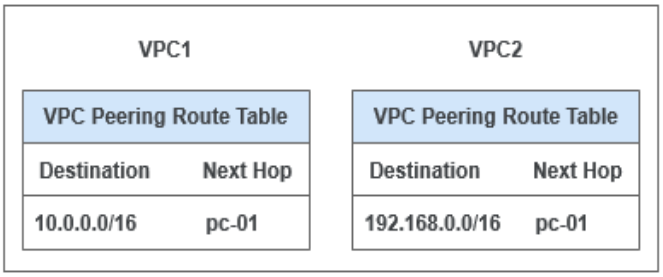
  If VPC 1 and VPC 2 have different CIDR blocks, you can create a VPC peering connection route that points to the entire VPC. **Figure 8-3** shows a VPC peering connection created between two VPCs.

Figure 8-3 VPC peering connection between VPC 1 and VPC 2



Routes are required to enable communication between VPC 1 and VPC 2 in the figure. **Figure 8-4** shows the routes configured for the VPC peering connection between VPC 1 and VPC 2. After the routes are configured, VPC 1 and VPC 2 can communicate with each other.

Figure 8-4 Route table for the VPC peering connection between VPC 1 and VPC 2



- Configurations with Routes to Specific Subnets

  If VPCs connected by a VPC peering connection have overlapping CIDR blocks, the peering connection can only enable communication between specific (non-overlapping) subnets in the VPCs. If subnets in the two VPCs of a VPC peering connection have overlapping CIDR blocks, the peering connection will not take effect. When creating a VPC peering connection, ensure that the VPCs involved do not contain overlapping subnets.

  For example, VPC 1 and VPC 2 have matching CIDR blocks, but the subnets in the two VPCs do not overlap. A VPC peering connection can be created between pairs of subnets that do not overlap with each other. The route table is used to control the specific subnets that the VPC peering connection is created for. **Figure 8-5** shows a VPC peering connection created between two subnets. Routes are required to enable communication between Subnet A in VPC 1 and Subnet X in VPC 2 in the figure.

Figure 8-5 VPC peering connection between Subnet A and Subnet X

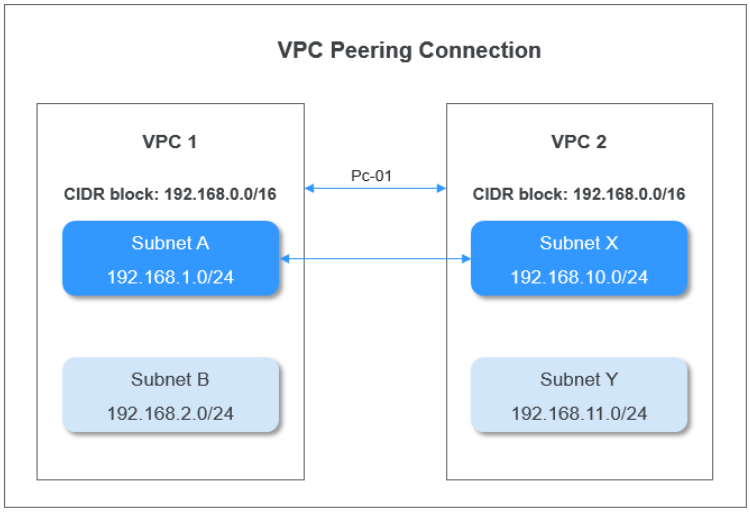
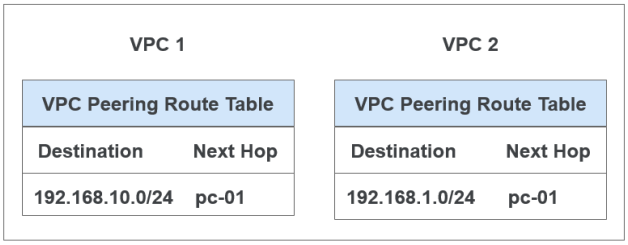


Figure 8-6 shows the routes configured for the VPC peering connection between Subnet A and Subnet X. After the routes are configured, Subnet A and Subnet X can communicate with each other.

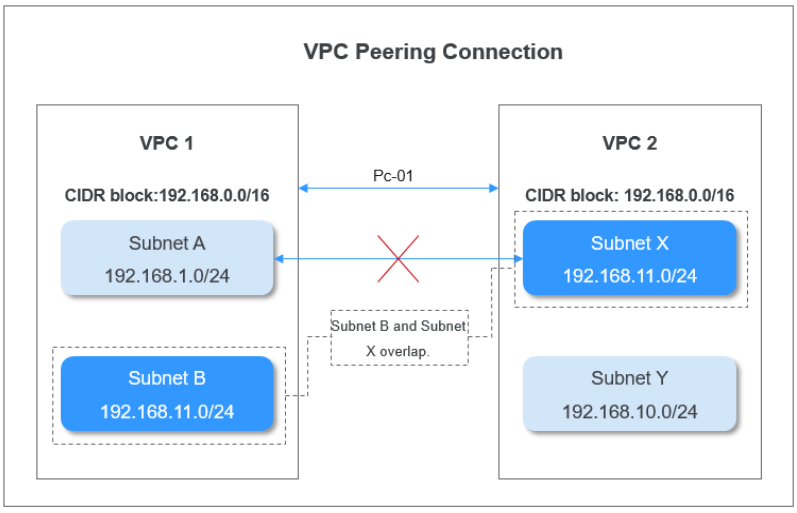
Figure 8-6 Route table for the VPC peering connection between Subnet A and Subnet X



If two VPCs have overlapping subnets, the VPC peering connection created between the two subnets does not take effect, and the subnets cannot communicate with each other.

As shown in Figure 8-7, Subnet B and Subnet X have matching CIDR blocks. Therefore, subnet A preferentially accesses subnet B that is in its same VPC and a VPC peering connection cannot be created between Subnet A and Subnet X.

Figure 8-7 Invalid VPC peering connection



If peering connections are used to link VPC 1 to multiple VPCs, for example, VPC 2, VPC 3, and VPC 4, the subnet CIDR blocks of VPC 1 cannot overlap with those of VPC 2, VPC 3, and VPC 4. If VPC 2, VPC 3, and VPC 4 have overlapping subnets, a VPC peering connection can be created between only one of these overlapping subnets and a subnet of VPC 1. If a VPC peering connection is created between a subnet and the other *N* subnets, none of the subnets can have overlapping CIDR blocks.

8.3 Creating a VPC Peering Connection with Another VPC in Your Account

Scenarios

To create a VPC peering connection, first create a request to peer with another VPC. You can request a VPC peering connection with another VPC in your account, but the two VPCs must be in the same region. The system automatically accepts the request.

Prerequisites

Two VPCs in the same region have been created.

Creating a VPC Peering Connection

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the right pane displayed, click **Create VPC Peering Connection**.
5. Configure parameters as prompted. You must select **My account** for **Account**. **Table 8-1** lists the parameters to be configured.

Table 8-1 Parameter descriptions

Parameter	Description	Example Value
Name	Specifies the name of the VPC peering connection. The name contains a maximum of 64 characters, which consist of letters, digits, hyphens (-), and underscores (_).	peering-001
Local VPC	Specifies the local VPC. You can select one from the drop-down list.	vpc_01
Local VPC CIDR Block	Specifies the CIDR block for the local VPC.	192.168.10.0/24
Account	Specifies the account to which the peer VPC belongs. • **My account**: The VPC peering connection will be created between two VPCs, in the same region, in your account. • **Another account**: The VPC peering connection will be created between your VPC and a VPC in another account, in the same region.	My account
Peer Project	Specifies the peer project name. The project name of the current project is used by default.	aaa
Peer VPC	Specifies the peer VPC. You can select one from the drop-down list if the VPC peering connection is created between two VPCs in your own account.	vpc_02
Peer VPC CIDR Block	Specifies the CIDR block for the peer VPC. The local and peer VPCs cannot have matching or overlapping CIDR blocks. Otherwise, the routes added for the VPC peering connection may not take effect.	192.168.2.0/24

6. Click **OK**.

Adding Routes for a VPC Peering Connection

If you request a VPC peering connection with another VPC in your own account, the system automatically accepts the request. To enable communication between the two VPCs, you need to add local and peer routes on the **Route Tables** page for the VPC peering connection.

1. On the console homepage, under **Network**, click **Virtual Private Cloud**.
2. In the navigation pane on the left, choose **Route Tables**.
3. Search for or create a route table for the local VPC and add the local route. **Table 8-2** describes the route parameters.

   Table 8-2 Parameter descriptions

Parameter	Description	Example Value
Destination	Specifies the CIDR block of the peer VPC or peer subnet.	192.168.2.0/24
Next Hop Type	Specifies the next hop type. Select **VPC peering connection**.	VPC peering connection
Next Hop	Specifies the next hop address. Select the name of the current VPC peering connection.	peering-001
Description	Provides supplementary information about the route. This parameter is optional. The route description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

4. Search for or create a route table for the peer VPC and add the peer route.

After a VPC peering connection is created, the two VPCs can communicate with each other through private IP addresses. You can run the **ping** command to check whether the two VPCs can communicate with each other. Before running the **ping** command, ensure that the security group allows inbound ICMP traffic. For details, see **4.1.5 Adding a Security Group Rule**.

If two VPCs cannot communicate with each other, check the configuration by following the instructions provided in **11.5.4 What Should I Do If VPCs Connected by a VPC Peering Connection Cannot Communicate with Each Other?**

8.4 Creating a VPC Peering Connection with a VPC in Another Account

Scenarios

The VPC service also allows you to create a VPC peering connection with a VPC in another account. The two VPCs must be in the same region. If you request a VPC

peering connection with a VPC in another account in the same region, the owner of the peer account must accept the request to activate the connection.

Creating a VPC Peering Connection

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the right pane displayed, click **Create VPC Peering Connection**.
5. Configure parameters as prompted. You must select **Another account** for **Account**.

Table 8-3 Parameter descriptions

Parameter	Description	Example Value
Name	Specifies the name of the VPC peering connection. The name contains a maximum of 64 characters, which consist of letters, digits, hyphens (-), and underscores (_).	peering-002
Local VPC	Specifies the local VPC. You can select one from the drop-down list.	vpc_01
Account	Specifies the account to which the VPC to peer with belongs. • **My account**: The VPC peering connection will be created between two VPCs, in the same region, in your account. • **Another account**: The VPC peering connection will be created between your VPC and a VPC in another account, in the same region.	Another account
Peer Project ID	This parameter is available only when **Another account** is selected. For details about how to obtain the peer project ID, see **Obtaining the Peer Project ID**.	N/A

Parameter	Description	Example Value
Peer VPC ID	This parameter is available only when **Another account** is selected. For details about how to obtain the peer VPC ID, see **Obtaining the Peer VPC ID**.	65d062b3-40fa-4204-8181-3538f527d2ab

6. Click **OK**.

Accepting a VPC Peering Connection Request

To request a VPC peering connection with a VPC in another account, the owner of the peer account must accept the request to activate the connection.

1. The owner of the peer account logs in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the list of requests to be handled, locate the row that contains the target VPC peering connection and click **Accept Request** in the **Operation** column.
5. Click **Yes** in the displayed dialog box.

Refusing a VPC Peering Connection

The owner of the peer account can reject any VPC peering connection request that they receive. If a VPC peering connection request is rejected, the connection will not be established. You must delete the rejected VPC peering connection request before creating a VPC peering connection between the same VPCs as those in the rejected request.

1. The owner of the peer account logs in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the list of requests to be handled, locate the row that contains the target VPC peering connection and click **Reject Request** in the **Operation** column.
5. Click **Yes** in the displayed dialog box.

Adding Routes for a VPC Peering Connection

If you request a VPC peering connection with a VPC in another account, the owner of the peer account must accept the request. To enable communication between the two VPCs, the owners of both the local and peer accounts need to add routes on the **Route Tables** page for the VPC peering connection. The owner of the local account can add only the local route because the owner does not have the required permission to perform operations on the peer VPC. The owner of the peer account must add the peer route. The procedure for adding a local route and a peer route is the same.

1. On the console homepage, under **Network**, click **Virtual Private Cloud**.

2. In the navigation pane on the left, choose **Route Tables**.
3. Search for or create a route table for the local VPC and add the local route. **Table 8-4** describes the route parameters.

   Table 8-4 Parameter descriptions

Parameter	Description	Example Value
Destination	Specifies the CIDR block for the peer VPC.	192.168.3.0/24
Next Hop Type	Specifies the next hop type. Select **VPC peering connection**.	VPC peering connection
Next Hop	Specifies the next hop address. Select the name of the current VPC peering connection.	peering-002
Description	Provides supplementary information about the route. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

4. Click **OK**.

   The routes are added for the VPC peering connection.

After a VPC peering connection is created, the two VPCs can communicate with each other through private IP addresses. You can run the **ping** command to check whether the two VPCs can communicate with each other. Before running the **ping** command, ensure that the security group allows inbound ICMP traffic. For details, see **4.1.5 Adding a Security Group Rule**.

If two VPCs cannot communicate with each other, check the configuration by following the instructions provided in **11.5.4 What Should I Do If VPCs Connected by a VPC Peering Connection Cannot Communicate with Each Other?**

Obtaining the Peer Project ID

1. The owner of the peer account logs in to the management console.
2. Select **My Credentials** from the username drop-down list.
3. On the **Projects** tab, obtain the required project ID.

Obtaining the Peer VPC ID

1. The owner of the peer account logs in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Virtual Private Cloud**.
4. Click the target VPC name and view VPC ID on the VPC details page.

8.5 Viewing VPC Peering Connections

Scenarios

The owners of both the local and peer accounts can view information about the created VPC peering connections and those that are still waiting to be accepted.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the displayed pane on the right, view information about the VPC peering connections. You can search for specific VPC peering connections by connection status or by name.
5. Click the VPC peering connection name. On the displayed page, view detailed information about the VPC peering connection.

8.6 Modifying a VPC Peering Connection

Scenarios

The owners of both the local and peer accounts can modify a VPC peering connection in any state. The VPC peering connection name can be changed.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the displayed pane on the right, view information about the VPC peering connections. You can search for specific VPC peering connections by connection status or by name.
5. Locate the target VPC peering connection and click **Modify** in the **Operation** column. In the displayed dialog box, modify information about the VPC peering connection.
6. Click **OK**.

8.7 Deleting a VPC Peering Connection

Scenarios

The owners of both the local and peer accounts can delete a VPC peering connection in any state. After a VPC peering connection is deleted, routes configured for the connection will be automatically deleted as well.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the displayed pane on the right, view information about the VPC peering connections. You can search for specific VPC peering connections by connection status or by name.
5. Locate the target VPC peering connection and click **Delete** in the **Operation** column.
6. Click **Yes** in the displayed dialog box.

8.8 Viewing Routes Configured for a VPC Peering Connection

Scenarios

After routes are added for a VPC peering connection, the owners of both the local and peer accounts can view information about the routes on the page showing details about the VPC peering connection.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. Locate the target VPC peering connection in the connection list.
5. Click the name of the VPC peering connection to switch to the page showing details about the connection.
6. On the displayed page, click the **Local Routes** tab and view information about the local route added for the VPC peering connection.
7. On the page showing details about the VPC peering connection, click the **Peer Routes** tab and view information about the peer route added for the VPC peering connection.

8.9 Deleting a VPC Peering Route

Scenarios

After routes are added for a VPC peering connection, the owners of both the local and peer accounts can delete the routes on the **Route Tables** page.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.

3. In the navigation pane on the left, choose **Route Tables**.
4. Locate the target route table in the route table list.
5. Click the name of the target route table to go to the route table details page.
6. Locate the row that contains the route to be deleted and click **Delete** in the **Operation** column.
7. Click **Yes** in the displayed dialog box.

9 Virtual IP Address

9.1 Virtual IP Address Overview

What Is a 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.

A virtual IP address can be bound to multiple ECSs deployed in active/standby mode. You can bind an EIP to the virtual IP address. When the EIP is accessed from the Internet, the virtual IP address has made it possible to either the active or standby ECS, making ECSs highly fault tolerant.

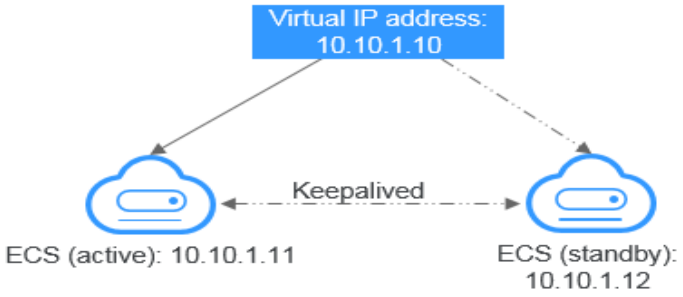
Networking

Virtual IP addresses are used for high availability as they 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 9-1 Networking diagram of the HA mode

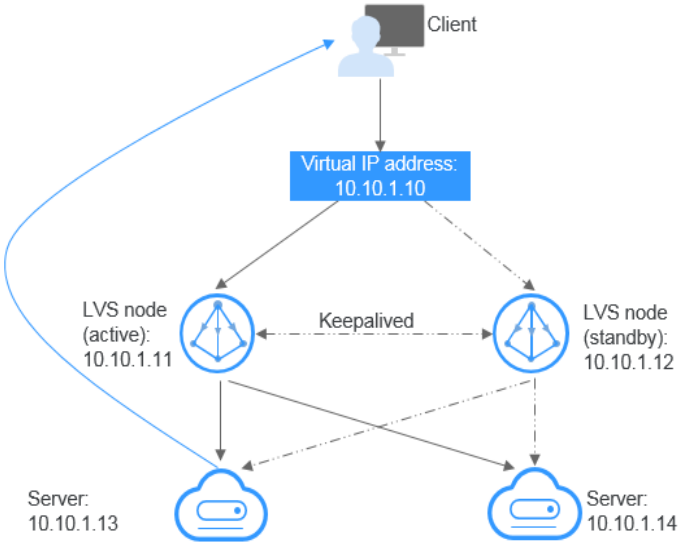


  - In this configuration, a single virtual IP address is bound to two ECSs in the same subnet.
  - Keepalived is then used to configure the two ECSs to work in the active/standby mode. Follow industry standards for configuring Keepalived. The details are not included here.

- **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 9-2 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.
  - Check whether the source/destination check is disabled on the active and standby LVS ECSs. For details, see **9.8 Disabling Source and Destination Check (HA Load Balancing Cluster Scenario)**.

If you bind an ECS to a virtual IP address on the management console, the source/destination check is automatically disabled. If you bind an ECS to a virtual IP address by calling APIs, you need to manually disable the source/destination check.

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.

Notes and Constraints

- Virtual IP addresses are not recommended when multiple NICs in the same subnet are configured on an ECS. It is too easy for there to be route conflicts on the ECS, which would cause communication failure using the virtual IP address.
- A virtual IP address can only be bound to ECSs in the same subnet.
- IP forwarding must be disabled on the standby ECS. Perform the following operations to confirm whether the IP forwarding is disabled on the standby ECS:

  a. Log in to standby ECS and run the following command to check whether the IP forwarding is enabled:

     cat /proc/sys/net/ipv4/ip_forward

     In the command output, **1** indicates it is enabled, and **0** indicates it is disabled. The default value is **0**.

     - If the command output is **1**, perform **b** and **c** to disable the IP forwarding.
     - If the command output is **0**, no further action is required.

  b. Use the vi editor to open the **/etc/sysctl.conf** file, change the value of **net.ipv4.ip_forward** to **0**, and enter **:wq** to save the change and exit. You can also use the **sed** command to modify the configuration. A command example is as follows:

     sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf

  c. Run the following command to make the change take effect:

     sysctl -p /etc/sysctl.conf

- The virtual IP address can use only the default security group, which cannot be changed to a custom security group.

- It is recommended that no more than eight virtual IP addresses be bound to an ECS.
- It is recommended that no more than 10 ECSs be bound to a virtual IP address.

9.2 Assigning a Virtual IP Address

Scenarios

If an ECS requires a virtual IP address or if a virtual IP address needs to be reserved, you can assign a virtual IP address from the subnet.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. In the subnet list, click the name of the subnet where a virtual IP address is to be assigned.
5. Click the **IP Addresses** tab and click **Assign Virtual IP Address**.
6. Select a virtual IP address assignment mode.
   - **Automatic**: The system assigns an IP address automatically.
   - **Manual**: You can specify an IP address.
7. Select **Manual** and enter a virtual IP address.
8. Click **OK**.

You can then query the assigned virtual IP address in the IP address list.

9.3 Binding a Virtual IP Address to an EIP or ECS

Scenarios

You can bind a virtual IP address to an EIP so that you can access the ECSs can be deployed in active/standby mode for improve fault tolerance.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. In the subnet list, click the name of the subnet that the virtual IP address belongs to.
5. Click the **IP Addresses** tab, locate the row that contains the target virtual IP address, and click **Bind to EIP** or **Bind to Server** in the **Operation** column.
6. Select the desired EIP, or ECS and its NIC.

NOTE

- If the ECS has multiple NICs, bind the virtual IP address to the primary NIC.
- Multiple virtual IP addresses can be bound to an ECS NIC.

7. Click **OK**.

9.4 Using an EIP to Access a Virtual IP Address

Prerequisites

- You have configured the ECS networking based on **Networking** and ensure that the ECS has been bound with a virtual IP address.
- You have assigned an EIP.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. Locate the row that contains the EIP to be bound to the virtual IP address, and click **Bind** in the **Operation** column.
4. Select the target virtual IP address and click **OK**.

9.5 Using a VPN to Access a Virtual IP Address

Procedure

1. Configure the ECS networking based on **Networking**.
2. Create a VPN.

The VPN can be used to access the virtual IP address of the ECS.

9.6 Using a Direct Connect Connection to Access the Virtual IP Address

Procedure

1. Configure the ECS networking based on **Networking**.
2. Create a Direct Connect connection.

The created Direct Connect connection can be used to access the virtual IP address of the ECS.

9.7 Using a VPC Peering Connection to Access the Virtual IP Address

Procedure

1. Configure the ECS networking based on **Networking**.
2. Create a VPC peering connection.

The VPC peering connection can be used to access the virtual IP address of the ECS.

9.8 Disabling Source and Destination Check (HA Load Balancing Cluster Scenario)

1. Log in to the management console.
2. Under **Computing**, click **Elastic Cloud Server**.
3. In the ECS list, click the ECS name.
4. On the displayed ECS details page, click the **NICs** tab.
5. Check that **Source/Destination Check** is disabled.

9.9 Releasing a Virtual IP Address

Scenarios

If you no longer need a virtual IP address or a reserved virtual IP address, you can release it to avoid wasting resources.

Prerequisites

Before deleting a virtual IP address, ensure that the virtual IP address has been unbound from the following resources:

- ECS
- EIP
- CCE cluster

Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. In the subnet list, click the name of the subnet that the virtual IP address belongs to.
5. Click the **IP Addresses** tab, locate the row that contains the virtual IP address to be released, click **More** in the **Operation** column, and select **Release**.

6. Click **Yes** in the displayed dialog box.

10 Monitoring

10.1 Supported Metrics

Description

This section describes the namespace, list, and dimensions of EIP and bandwidth metrics on Cloud Eye. You can use APIs or the Cloud Eye console to query the metrics of the monitored metrics and alarms generated for EIP and bandwidth.

Namespace

SYS.VPC

Monitoring Metrics

Table 10-1 EIP and Bandwidth metrics

Metric	Metric Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic (Previously called "Upstream Bandwidth") Unit: bit/s	≥ 0 bit/s	Object: Bandwidth or EIP Dimension[a]: bandwidth_id, publicip_id	1 minute

Metric	Metric Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic (Previously called "Downstream Bandwidth") Unit: bit/s	≥ 0 bit/s	Object: Bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage of outbound bandwidth in the unit of percent.	0% to 100%	Object: Bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute
up_stream	Outbound Traffic	Network traffic going out of the cloud platform (Previously called "Upstream Traffic") Unit: byte	≥ 0 bytes	Object: Bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute
down_stream	Inbound Traffic	Network traffic going into the cloud platform (Previously called "Downstream Traffic") Unit: byte	≥ 0 bytes	Object: Bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute

Metric	Metric Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)

a: If a service has multiple dimensions, all dimensions are mandatory when you use APIs to query the metrics.
• Query a monitoring metric: dim.0=bandwidth_id,530cd6b0-86d7-4818-837f-935f6a27414d&dim.1=publicip_id,3773b058-5b4f-4366-9035-9bbd9964714a
• Query monitoring metrics in batches:
"dimensions": [
{
"name": "bandwidth_id",
"value": "530cd6b0-86d7-4818-837f-935f6a27414d"
}
{
"name": "publicip_id",
"value": "3773b058-5b4f-4366-9035-9bbd9964714a"
}
],					

Dimensions

Key	Value
publicip_id	EIP ID
bandwidth_id	Bandwidth ID

10.2 Viewing Metrics

Scenarios

View related metrics to see bandwidth and EIP usage information.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Management & Deployment**, click **Cloud Eye**.
3. Click **Cloud Service Monitoring** on the left of the page, and choose **Elastic IP and Bandwidth**.

4. Locate the row that contains the target bandwidth or EIP and click **View Metric** in the **Operation** column to check the bandwidth or EIP monitoring information.

   You can view data during the last one, three, or twelve hours.

10.3 Creating an Alarm Rule

Scenarios

You can configure alarm rules to customize the monitored objects and notification policies. You can learn VPC statuses at any time.

Procedure

1. Log in to the management console.
2. On the console homepage, under **Management & Deployment**, click **Cloud Eye**.
3. In the left navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
4. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters to create an alarm rule, or modify an existing alarm rule.
5. After the parameters are set, click **Create**.

   After the alarm rule is created, the system automatically notifies you if an alarm is triggered for the VPC service.

   NOTE

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

11 FAQs

11.1 General

11.1.1 What Is a Quota?

What Is a Quota?

A quota limits the quantity of a resource available to users, thereby preventing spikes in the usage of the resource. For example, a VPC quota limits the number of VPCs that can be created.

You can also request for an increase in quota if an existing quota cannot meet your service requirements.

How Do I View My Quotas?

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click .

   The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

The system does not support online quota adjustment. If you need to adjust a quota, call the hotline or send an email to the customer service mailbox. Customer service personnel will timely process your request for quota adjustment and inform you of the real-time progress by making a call or sending an email.

Before dialing the hotline number or sending an email, make sure that the following information has been obtained:

- Account name, project name, and project ID, which can be obtained by performing the following operations:

  Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the account name, project name, and project ID on the **My Credentials** page.
- Quota information, which includes:
  - Service name
  - Quota type
  - Required quota

If you need to adjust a quota, contact the administrator.

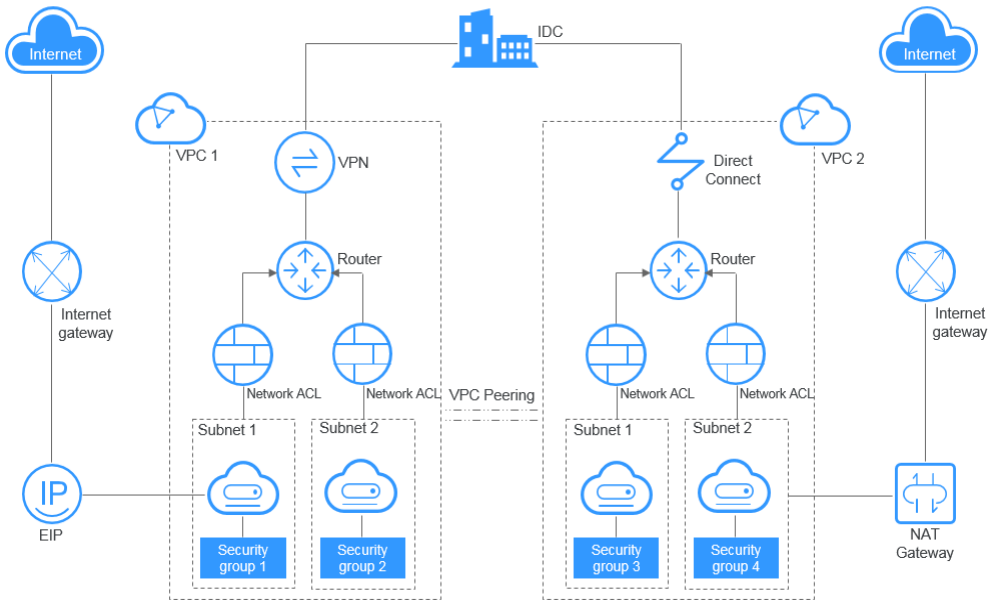
11.2 VPC and Subnet

11.2.1 What Is Virtual Private Cloud?

The Virtual Private Cloud (VPC) service enables you to provision logically isolated, configurable, and manageable virtual networks for Elastic Cloud Servers (ECSs), improving cloud service security and simplifying network deployment.

Within your own VPC, you can create security groups and VPNs, configure IP address ranges, specify bandwidth sizes, manage the networks in the VPC, and make changes to these networks as needed, quickly and securely. You can also define rules for communication between ECSs in the same security group or in different security groups.

Figure 11-1 Product Architecture



11.2.2 Which CIDR Blocks Are Available to the VPC Service?

The VPC service supports the following CIDR blocks:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

11.2.3 Can Subnets Communicate with Each Other?

Subnets in the same VPC can communicate with each other while subnets in different VPCs cannot communicate with each other by default. However, you can create VPC peering connections to enable subnets in different VPCs to communicate with each other.

NOTE

If a subnet is associated with a network ACL, configure network ACL rules to allow the communication between subnets.

11.2.4 What Subnet CIDR Blocks Are Available?

A subnet CIDR block must be included in its VPC CIDR block. Supported VPC CIDR blocks are **10.0.0.0/8–24**, **172.16.0.0/12–24**, and **192.168.0.0/16–24**. The allowed block size of a subnet is between the netmask of its VPC CIDR block and /28 netmask.

11.2.5 How Many Subnets Can I Create?

Each account can have a maximum of 100 subnets. If the number of subnets cannot meet your service requirements, request a quota increase. For details, see **11.1.1 What Is a Quota?**

11.2.6 What Do I Do If a Subnet Cannot Be Deleted Because It Is Being Used by Other Resources?

The VPC service allows you to create private, isolated virtual networks. In a VPC, you can manage private IP address ranges, subnets, and gateways. ECSs, BMSs, databases, and some other applications can use subnets created in VPCs.

A subnet cannot be deleted if it is being used by other resources.

You can view all resources of your account on the console homepage and check the resources that are in the subnet to be deleted. You must delete all resources in the subnet before deleting the subnet.

The resources may include:

- ECS
- Load balancer
- VPN
- Private IP address
- Custom route
- NAT gateway
- VPC endpoint and VPC endpoint service

11.3 EIP

11.3.1 Can I Bind an EIP to Multiple ECSs?

Each EIP can be bound to only one ECS at a time.

Multiple ECSs cannot share the same EIP. An ECS and its bound EIP must be in the same region. If you want multiple ECSs in the same VPC to share an EIP, you have to use a NAT gateway. For more information, see *NAT Gateway User Guide*.

11.3.2 How Do I Access an ECS from the Internet After an EIP Is Bound to the ECS?

Each ECS is automatically added to a security group after being created to ensure its security. The security group denies access traffic from the Internet by default (except TCP traffic from port 22 through SSH to the Linux OS and TCP traffic from port 3389 through RDP to the Windows OS). To allow external access to ECSs in the security group, add an inbound rule to the security group.

You can set **Protocol** to **TCP**, **UDP**, **ICMP**, or **All** as required on the page for creating a security group rule.

- If the ECS needs to be accessible over the Internet and the IP address used to access the ECS over the Internet has been configured on the ECS, or the ECS does not need to be accessible over the Internet, set **Source** to the IP address range containing the IP address that is allowed to access the ECS over the Internet.
- If the ECS needs to be accessible over the Internet and the IP address used to access the ECS over the Internet has not been configured on the ECS, it is recommended that you retain the default setting **0.0.0.0/0** for **Source**, and then set **Port Range** to improve network security.
- Allocate ECSs that have different Internet access policies to different security groups.

  NOTE

  The default source IP address **0.0.0.0/0** indicates that all IP addresses can access ECSs in the security group.

11.4 Bandwidth

11.4.1 What Is the Bandwidth Size Range?

The bandwidth ranges from 1 Mbit/s to 300 Mbit/s.

11.5 Connectivity

11.5.1 Does a VPN Allow for Communication Between Two VPCs?

If the two VPCs are in the same region, you can use a VPC peering connection to enable communication between them.

If the two VPCs are in different regions, you can use a VPN to enable communication between the VPCs. The CIDR blocks of the two VPCs are the local and remote subnets, respectively.

11.5.2 Why Cannot I Access the Internet or Internal Domain Names in the Cloud Through Domain Names When My ECS Has Multiple NICs?

When an ECS has more than one NIC, if different DNS server addresses are configured for the subnets used by the NICs, the ECS cannot access the Internet or internal domain names in the cloud.

You can rectify this fault by configuring the same DNS server address for the subnets used by the same ECS. You can perform the following steps to modify DNS server addresses of subnets in a VPC:

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. In the subnet list, locate the target subnet and click its name.
5. On the subnet details page, change the DNS server address of the subnet.
6. Click **OK**.

11.5.3 What Are the Constraints Related to VPC Peering?

- VPC peering connections created between VPCs that have overlapping subnet CIDR blocks may not take effect.
- You cannot have more than one VPC peering connection between the same two VPCs at the same time.
- You cannot create a VPC peering connection between VPCs in different regions.
- You cannot use the EIPs in a VPC of a VPC peering connection to access resources in the other VPC. For example, VPC A is peered with VPC B, VPC B has EIPs that can be used to access the Internet, you cannot use EIPs in VPC B to access the Internet from VPC A.
- To request a VPC peering connection with a VPC of another tenant, the peer tenant must accept the request to activate the connection. If you request a VPC peering connection with a VPC of your own, the system automatically accepts the request to activate the connection.
- After a VPC peering connection is established, the local and peer tenants must add routes in the local and peer VPCs to enable communication between the two VPCs.

- VPC A is peered with both VPC B and VPC C. If VPC B and VPC C have overlapping CIDR blocks, routes with the same destinations cannot be configured for VPC A.
- To ensure security, do not accept VPC peering connections from unknown tenants.
- Either owner of a VPC in a peering connection can delete the VPC peering connection at any time. If a VPC peering connection is deleted by one of its owners, all information about this connection will be automatically deleted immediately, including routes added for the VPC peering connection.
- If two VPCs in a VPC peering connection have overlapping CIDR blocks, the peering connection can only enable communication between two subnets in the two VPCs. If subnets in the two VPCs of a VPC peering connection have overlapping CIDR blocks, the peering connection will not take effect. When creating a VPC peering connection, ensure that the VPCs involved do not contain overlapping subnets.
- You cannot delete a VPC for which VPC peering connection routes have been configured.

11.5.4 What Should I Do If VPCs Connected by a VPC Peering Connection Cannot Communicate with Each Other?

1. Check whether a VPC peering connection has been successfully created for the two VPCs, especially, whether the VPC IDs are correctly configured.
2. Check whether routes that point to the CIDR block (or portion of the CIDR block) of the other VPC have been configured.
3. Check whether routes configured for the VPC peering connection are correct. If VPCs in a VPC peering connections have overlapping CIDR blocks, you can only add routes to enable communication between two subnets in the two VPCs.
4. Check whether the VPCs in the VPC peering connection contain overlapping subnets.
5. Check whether required security group rules have been configured for the ECSs that need to communicate with each other and whether restriction rules have been added to the iptables or firewall used by the ECSs.
6. If a message indicating that this route already exists is displayed when you add routes for a VPC peering connection, check whether the destination of a VPN, Direct Connect, or VPC peering connection route already exists.
7. If the route destination of the VPC peering connection overlap with that of a Direct Connect or VPN connection, the route may be invalid.
8. If VPCs in a VPC peering connection cannot communicate with each other after all these possible faults have been rectified, contact the administrator.

11.5.5 How Many VPC Peering Connections Can I Have?

You can have a maximum of 50 VPC peering connections in one region. Accepted VPC peering connections consume the quota of both owners of a VPC peering connection. A VPC peering connection in the pending approval state only consumes the quota of only the requester.

11.5.6 What Are the Priorities of the Custom Route and EIP If Both Are Configured for an ECS to Enable the ECS to Access the Internet?

The priority of an EIP is higher than that of a custom route.

11.6 Routing

11.6.1 How Many Routes Can a Route Table Have?

Each route table can contain a maximum of 200 routes by default, including routes added for Direct Connect and VPC peering connections.

11.6.2 What Are the Limitations of a Route Table?

- The ECS providing SNAT must have the **Unbind IP from MAC** function enabled.
- The destination of each route in a route table must be unique. The next hop must be a private IP address or a virtual IP address in the VPC. Otherwise, the route table will not take effect.
- If a virtual IP address is set to be the next hop in a route, EIPs bound with the virtual IP address in the VPC will become invalid.

11.6.3 Are There Different Routing Priorities for Direct Connect Connections and Custom Routes in the Same VPC?

No. Direct Connect connections and custom routes are used in different scenarios. Therefore, there is no routing priority competition between them.

11.6.4 Are There Different Routing Priorities of the VPN and Custom Routes in the Same VPC?

The routing priority of custom routes and that of VPNs are the same.

11.7 Security

11.7.1 Can I Change the Security Group of an ECS?

Yes. Log in to the ECS console, switch to the page showing ECS details, and change the security group of the ECS.

11.7.2 How Many Security Groups Can I Have?

Each account can have a maximum of 100 security groups and 5000 security group rules.

When creating an ECS, you can select multiple security groups (no more than five is recommended).

11.7.3 How Do I Configure a Security Group for Multi-Channel Protocols?

ECS Configuration

The TFTP daemon determines whether the configuration file specifies the port range. If you use the TFTP configuration file that allows the data channel ports to be configurable, it is a best practice to configure a small range of ports that are not listened on.

Security Group Configuration

You can configure both port 69 and the data channel ports used by TFTP for the security group. In RFC1350, the TFTP protocol specifies that ports available to data channels range from 0 to 65535. However, not all these ports are used by the TFTP daemon processes of different applications. Therefore, you can configure a small range of ports for the TFTP daemon.

The following figure provides an example of the security group rule configuration if the ports used by data channels range from 60001 to 60100.

Figure 11-2 Security group rules

Type	Protocol	Port/Range	Source
IPv4	All	All	sg-test
IPv4	UDP	60001-60100	0.0.0.0/0

11.7.4 How Many Network ACLs Can I Have?

You can have a maximum of 200 network ACLs. It is recommended that you configure a maximum of 20 inbound or outbound rules for each network ACL. If more than 20 inbound or outbound rules are configured, the forwarding performance will deteriorate.

11.7.5 Does a Security Group Rule or a Network ACL Rule Immediately Take Effect for Its Original Traffic After It Is Modified?

- Security groups are stateful. Responses to outbound traffic are allowed to go in to the instance regardless of inbound security group rules, and vice versa. Security groups use connection tracking to track traffic information about traffic to and from instances. If a security group rule is added, deleted, or modified, or an instance in the security group is created or deleted, the connection tracking of all instances in the security group will be automatically cleared. In this case, the inbound or outbound traffic of the instance is considered as new connections, which need to match the inbound or outbound security group rules to ensure that the rules take effect immediately and the security of incoming traffic.
- A modified network ACL rule will not immediately take effect for its original traffic. You need to interrupt the original traffic for about 120 seconds for the new rule to take effect for the traffic. To ensure that the traffic is immediately

interrupted after the rule is changed, it is recommended that you configure security group rules.

A Change History

Release Date	Description
2020-11-05	This issue is the first official release.

