HUAWEI

Networking Services

HUAWEI CLOUD
EVERYTHING AS A SERVICE

Foreword

- Network resources play a vital role in setting up infrastructure on the cloud. These resources enable communications between instances and between applications. This lays a solid foundation for the rapid business growth.
- In this chapter, we will discuss basic networking services provided by Huawei Cloud. I hope you will acquire a better understanding of how to use these services.

Objectives

- Understand the basic concepts of Virtual Private Cloud (VPC) and be proficient in configuring cloud networks using VPC.
- Understand the concepts of security groups and network ACLs, and be proficient in using them to secure simple networks.
- Understand the basic functions of VPC peering connections and VPN connections, and be able to use them to enable communications between VPCs.
- Understand Elastic IP (EIP) and NAT Gateway, and be proficient in using them to connect a cloud server to the Internet.

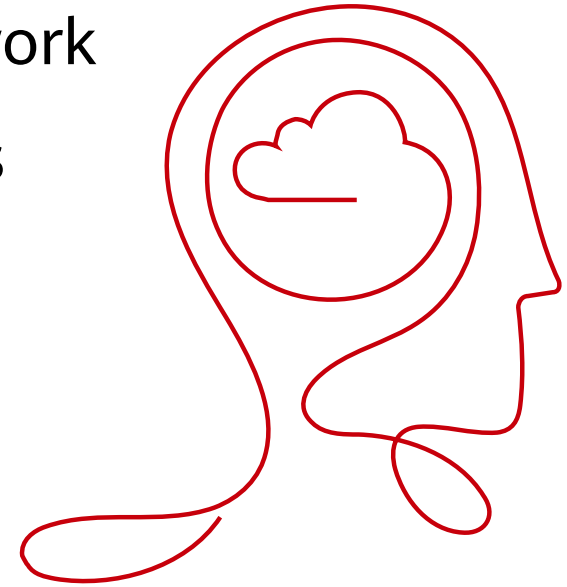
Contents

HUAWEI

Quiz

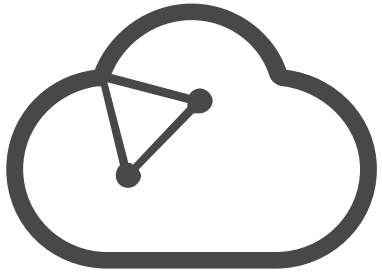
- Question: How do you create a private network on Huawei Cloud to enable communications between two ECSs?

- Answer: Use Huawei Cloud VPC.



VPC Overview

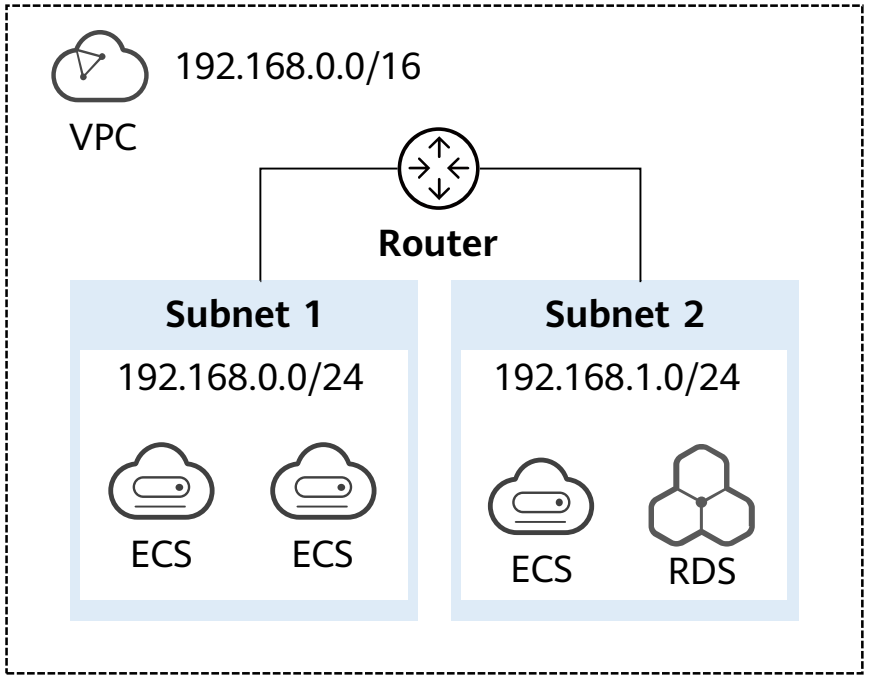
- Virtual Private Cloud (VPC) allows you to provision logically isolated virtual private networks for cloud resources, such as cloud servers, containers, and databases.



- "LANs" on the cloud
  - Resources in a VPC can communicate with each other.
  - Resources from different VPCs are isolated from each other.
- Custom IP address assignment and route configuration
- Core network security services

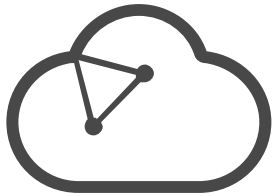
VPC Components

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



HUAWEI

Subnet



- You can define a CIDR block for each VPC.
- Resources in a VPC can communicate with each other.

A VPC can have one or more subnets.

- You can divide a VPC into one or more subnets.
- You can use subnets for refined network management.
- Traffic can be controlled in and out of subnets.
- You can customize routes for different networks.
- All resources must be created in subnets.

Subnets can be used for more refined network management.

Route Table

- A route table contains a set of routes that are used to control the traffic in and out of your subnets in a VPC.
- Each subnet can only be associated with one route table.

- Each VPC comes with a default route table.
- If you create a subnet in the VPC, the subnet is automatically associated 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 route table.

A route table contains a set of routes that are used to control the traffic in and out of your subnets in a VPC.

The default route table ensures that subnets in a VPC can communicate with each other.

HUAWEI

Exercise 1

- **Task 1**: Use the following settings to create a VPC (**vpc-demo-a**) and two subnets (**subnet-demo-0** and **subnet-demo-1**) and view the default route table configuration.

VPC
- Region: CN North-Beijing4
- Name: vpc-demo-a
- IPv4 CIDR Block: 192.168.0.0/16

Retain default values for other parameters.

Default Subnet
- AZ: AZ1
- Subnet Name: subnet-demo-0
- IPv4 CIDR Block: 192.168.0.0/24

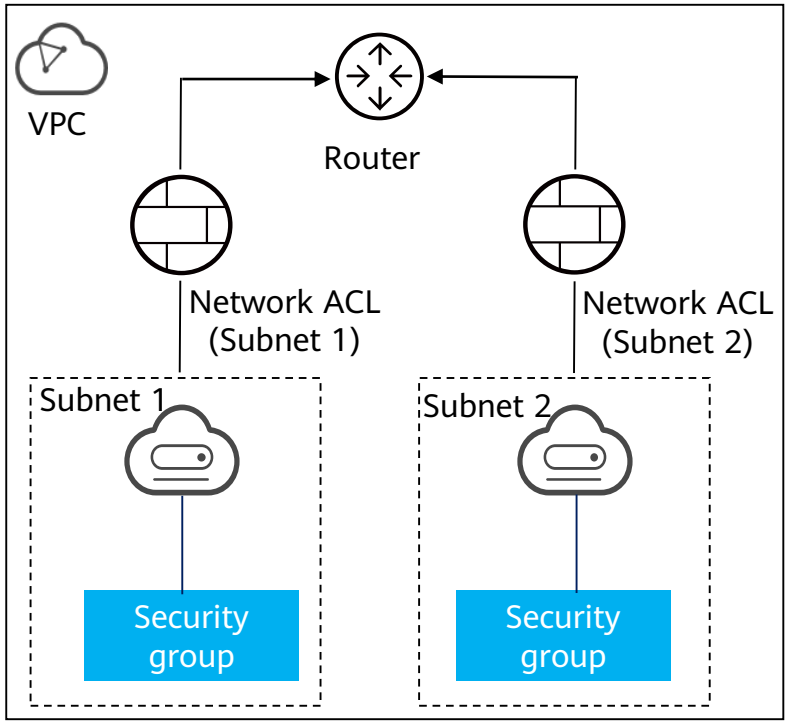
Subnet Setting1
- Subnet Name: subnet-demo-1
- IPv4 CIDR Block: 192.168.1.0/24

Retain default values for other parameters.

- **Task 2**: Create two ECSs (**ecs-demo-1** and **ecs-demo-2**) in **subnet-demo-0** and **subnet-demo-1**, respectively, and test network connectivity.
- **Question**: What might happen that could prevent **ecs-demo-1** and **ecs-demo-2** from communicating with each other?

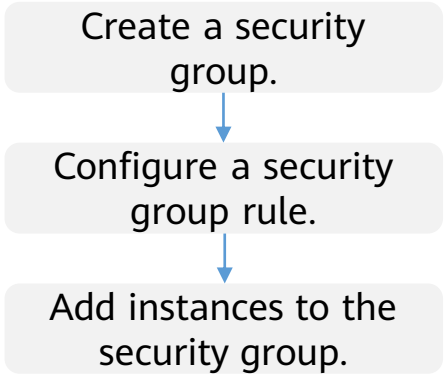
Access Control

- You can configure network ACLs and security groups to protect resources in a VPC.
  - Security groups protect instances and check traffic to and from instances.
  - Network ACLs protect subnets and only check traffic across subnets.



Security Group

- A security group is a logical group that you can use to configure access rules for, which will then will apply to all instances associated with this security group.
- A security group has inbound and outbound rules to control traffic that is allowed to reach or leave the instances associated with the security group.



Security group configuration process

Inbound rules of security group Sg-A				
Rules	**Priority**	**Action**	**Protocol & Port**	**Source**
Rule A1	1	Allow	ICMP: All	0.0.0.0/0
Rule A2	1	Allow	All	Sg-A
Outbound rules of Sg-A				
Rules	**Priority**	**Action**	**Protocol & Port**	**Source**
Rule A3	1	Allow	All	0.0.0.0/0

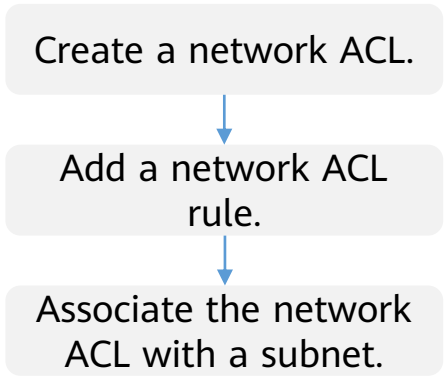
Sg-A rules

What do these rules mean?

HUAWEI

Network ACL

- A network ACL is an optional layer of security for your subnets. After you add inbound and outbound rules to a network ACL and associate subnets with it, you can control traffic in and out of the subnets.
- After a network ACL is associated with a subnet, the network ACL denies all traffic to and from this subnet by default until you add rules to allow traffic.
- A network ACL can be associated with multiple subnets. However, a subnet can be associated with only one network ACL.



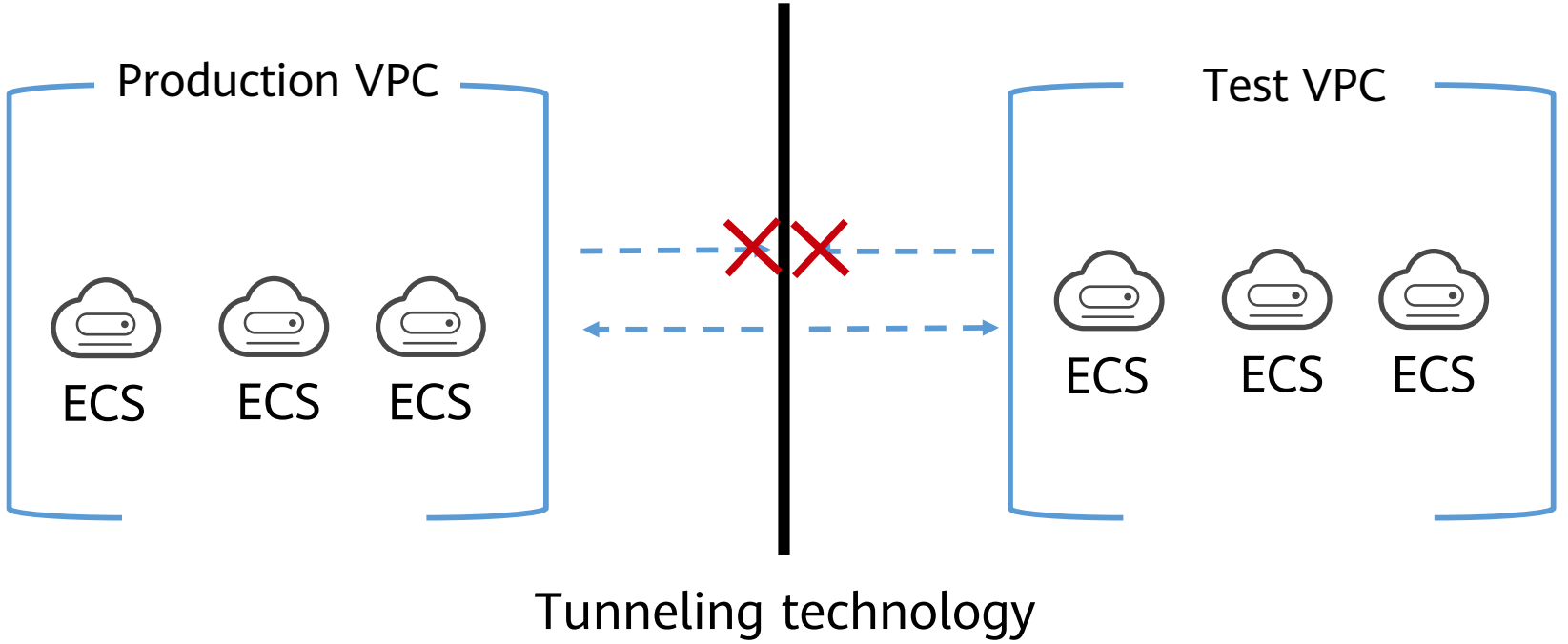
Network ACL configuration process

Direction	Action	Protocol	Source	Source Port Range	Destination	Destination Port Range
Inbound	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	80
Inbound	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	443
Outbound	Allow	All	0.0.0.0/0	All	0.0.0.0/0	All

Network ACL rules

VPC Application Scenario - Dedicated Networks on Cloud

- Each VPC represents a private network that is logically isolated from other VPCs. You can deploy your service system in a VPC on Huawei Cloud. If you have multiple service systems, for example, a production system and a test system, you can keep them isolated by deploying them in separate VPCs.



Exercise 2

- **Task 1**: Use the following settings to create a security group (**sg-demo**) and view its inbound and outbound rules. Then, use the new security group to replace the security group of the two ECSs in Exercise 1 and test network connectivity between the two ECSs.

  Security group
  - Name: sg-demo
  - Template: Fast-add rule
  - Inbound Rules: ICMP (All)

  Retain default values for other parameters.

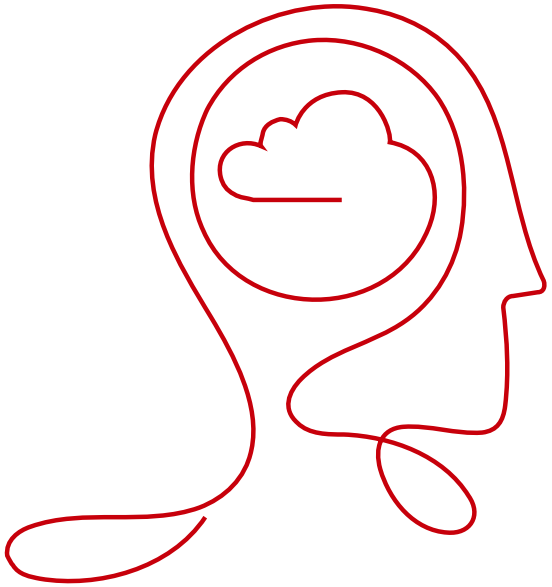
- **Task 2**: Delete all rules except **ICMP (All)** from **sg-demo** and test network connectivity between the two ECSs again.

Contents

HUAWEI

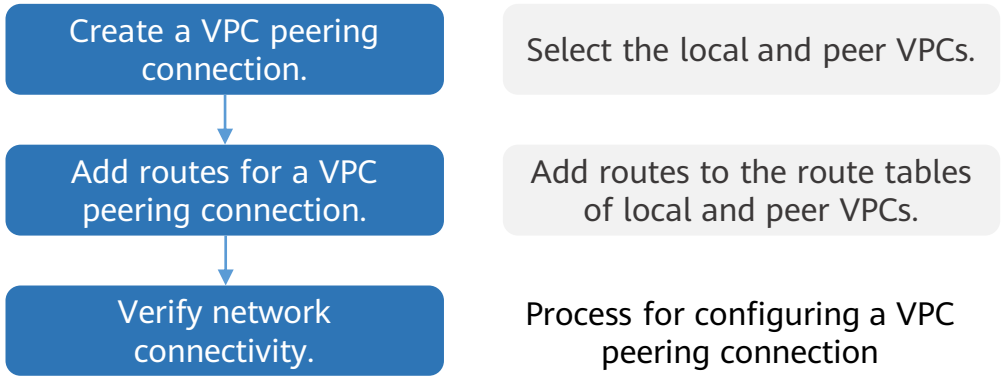
Quiz

- **Question**: Can two ECSs in different VPCs in the same region communicate with each other using private IP addresses?
- **Answer**: Yes, they can. You can create a VPC peering connection to connect the two VPCs.



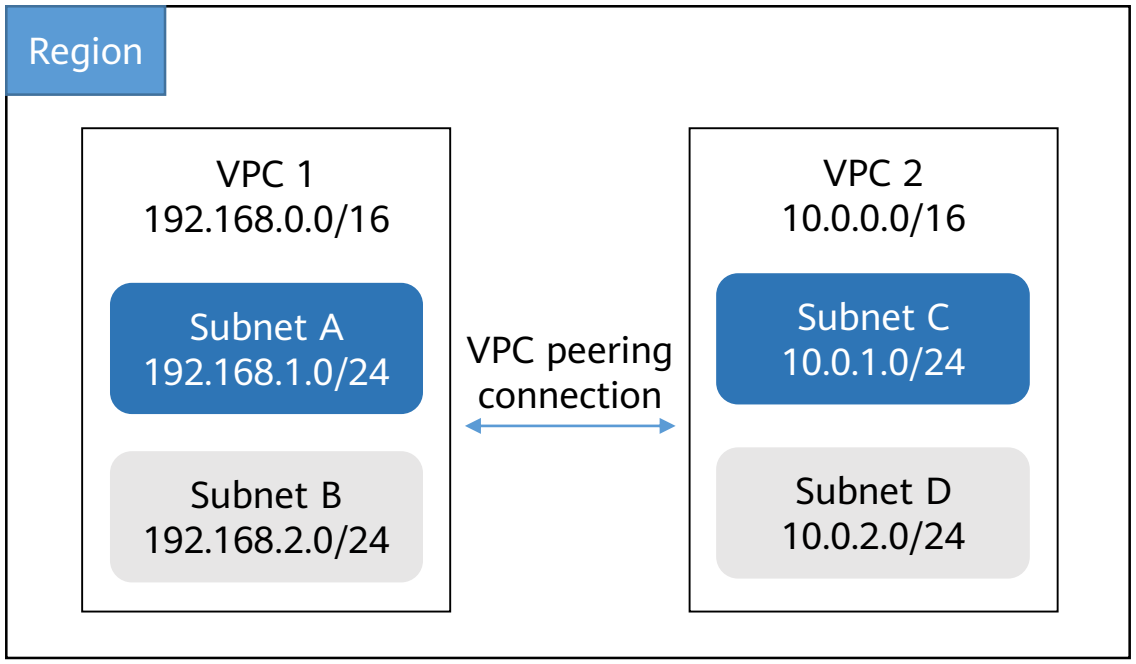
VPC Peering Connection Overview

- A VPC peering connection is a network connection between two VPCs. Different VPCs cannot communicate with each other by default, but you can connect them with a VPC peering connection if needed.



Process for configuring a VPC peering connection

- After a VPC peering connection is created, you need to add routes for the local and peer VPCs to enable communications between them.
- VPC peering connections are free and easy to configure.
- VPCs connected by VPC peering connections can communicate with each other over a private network instead of the Internet.



HUAWEI

Exercise 3

- **Task 1**: Use the following settings to create the second VPC (**vpc-demo-b**) and create the third ECS (**ecs-demo-3)** in **vpc-demo-b**. Test network connectivity between **ecs-demo-1** and **ecs-demo-3**. *(Note: ECSs are associated with the same security group and trust each other.)*

VPC
- Region: CN North-Beijing4
- Name: vpc-demo-b
- IPv4 CIDR Block: 192.168.0.0/16

Default Subnet
- AZ: AZ1
- Subnet Name: subnet-demo-2
- IPv4 CIDR Block: 192.168.2.0/24

Retain default values for other parameters.

- **Task 2**: Create a VPC peering connection between **vpc-demo-a** and **vpc-demo-b**, add routes to the route tables of **vpc-demo-a** and **vpc-demo-b**, and test network connectivity between **ecs-demo-1** and **ecs-demo-3** again.

Quiz

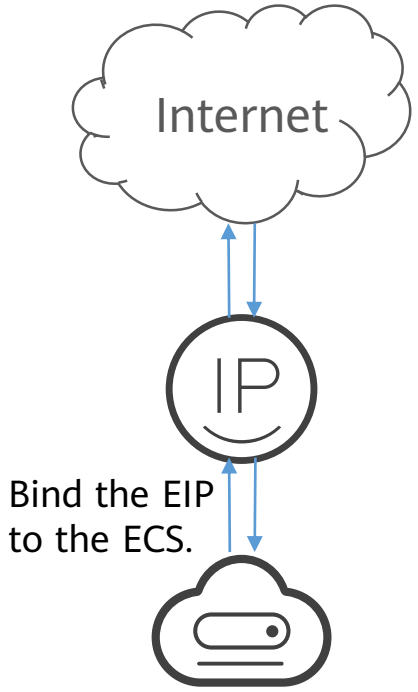
- **Question**: How can you enable an ECS to connect to the Internet?
- **Answer**: You can assign an EIP and bind it to the ECS so that the ECS can access the Internet.

Elastic IP (EIP) Overview

- EIP provides static public IP addresses and scalable bandwidths that enable your cloud resources to communicate with the Internet.

EIP
Public IP address:
19.205.67.7
Bandwidth: 5 Mbit/s

ECS
Private IP address:
192.168.0.56



- EIPs can be bound to or unbound from many cloud resources but only one cloud resource at any given time.
- Flexible billing modes: There are yearly/monthly and pay-per-use billing modes. Pay-per-use EIPs can be billed by bandwidth or by traffic. 95th percentile bandwidth billing (enhanced) and resource packages are also supported for saving costs.
- Bandwidths can be flexibly adjusted.

Exercise 4

- **Task 1**: Test the connectivity between **ecs-demo-0** and the Internet when no EIP is bound to **ecs-demo-0**. (for example, ping **www.huaweicloud.com** to check network connectivity.)
- **Task 2**: Assign an EIP using the following settings, bind it to **ecs-demo-0**, and test the connectivity between **ecs-demo-2** and the Internet.

  - Billing Mode: Pay-per-use
  - Region: CN North-Beijing4
  - EIP Type: Dynamic BGP
  - Billed By: Bandwidth
  - Bandwidth (Mbit/s): 5

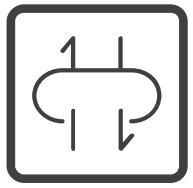
  Retain default values for other parameters.

Quiz

- **Question**: If multiple ECSs need to connect to the Internet, do I need to apply for multiple EIPs?
- **Answer**: That is one solution, but you can also try a public NAT gateway.

NAT Gateway

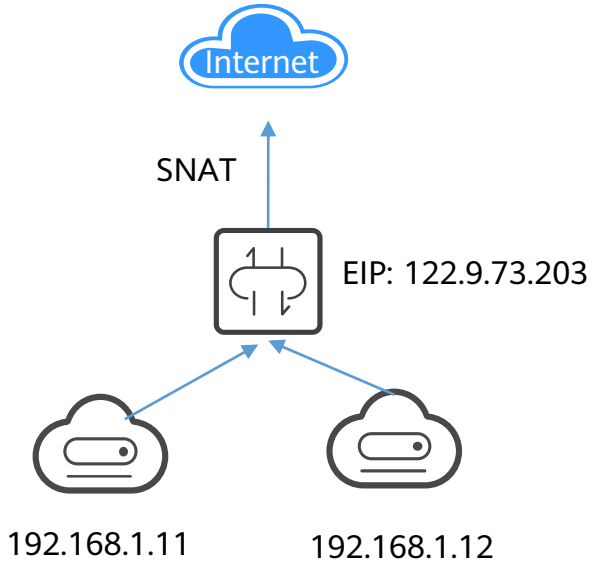
- Public and private NAT gateways are used to provide network address translation (NAT) in different scenarios. Public NAT gateways support source network address translation (SNAT) and destination network address translation (DNAT).
  - SNAT enables multiple servers to share an EIP to access the Internet.
  - DNAT enables multiple servers to share an EIP to provide services accessible from the Internet.



- Multiple servers can share the same EIP.
- A NAT gateway can be shared across subnets and AZs.
- Multiple specifications of NAT gateways are available.

NAT Gateway - SNAT

- SNAT only translates source IP addresses in packets. It is mainly used to enable servers on a private network to access the Internet.

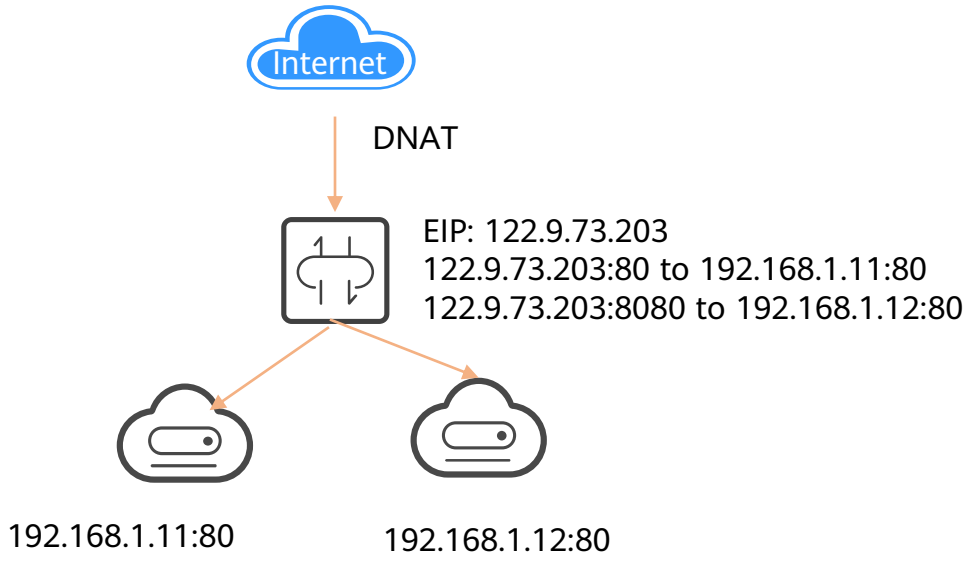


Mandatory parameters in an SNAT rule

- **Scenario**: You can select **VPC** or **Direct Connect/Cloud Connect**.
- **Subnet**: You can select an existing subnet, customize a CIDR block, or enter a server IP address.
- **EIP**: You can select up to 20 EIPs.

NAT Gateway - DNAT

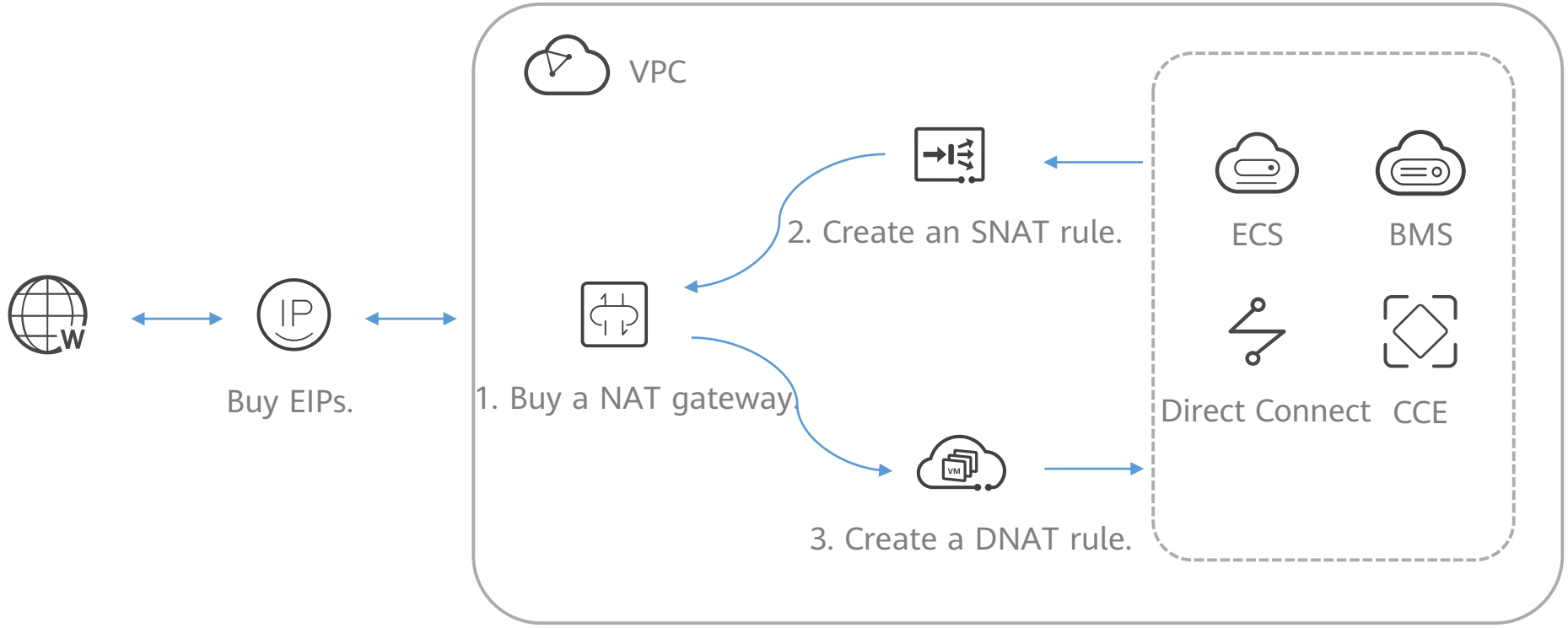
- DNAT only translates destination IP addresses and ports in packets. This enables Internet users to access services deployed on a private network.



Mandatory parameters in a DNAT rule

- **Scenario**: You can select **VPC** or **Direct Connect/Cloud Connect**.
- **Port Type**: You can select **Specific port** or **All ports**.
- **Protocol**: You can select **TCP** or **UDP**.
- **EIP**: Select an EIP used for Internet access.
- **Outside Port**: This parameter is only available if **Specific port** is selected for **Port Type**.
- **Private IP Address**: Specify the private IP address of an ECS in the same VPC of the NAT gateway.
- **Inside Port**: Specify a port of the ECS.

Public NAT Gateway - Configuration Overview



HUAWEI

Exercise 5

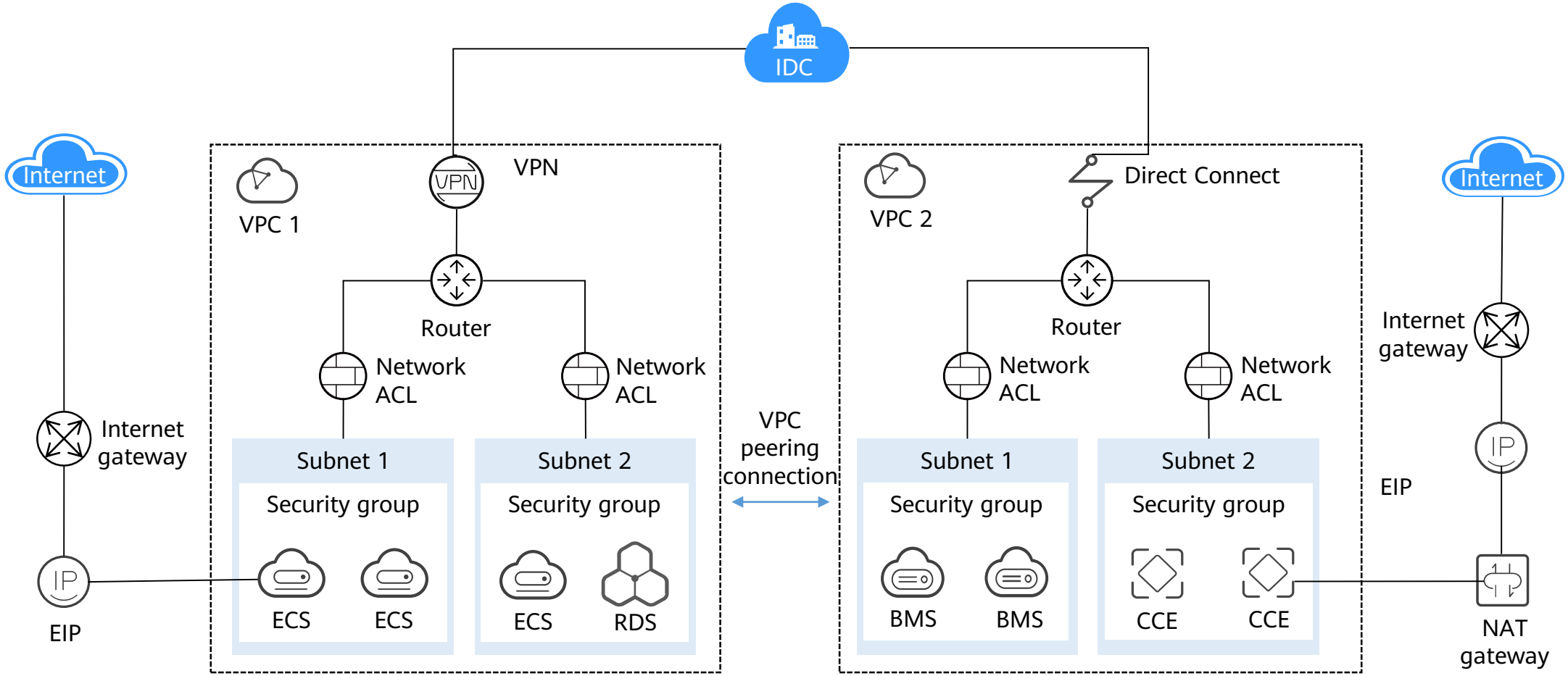
- **Task 1**: Create a public NAT gateway using the following settings:
  - **Billing Mode**: **Pay-per-use**
  - **Region**: **CN North-Beijing4**
  - **Name**: **nat-demo**
  - **VPC**: **vpc-demo-a**
  - **Subnet**: **subnet-demo-0**
  - **Specifications**: **Small**

  Set **Next Hop** of the default route (0.0.0.0/0) of **vpc-demo-a** to the public NAT gateway.
- **Task 2**: Unbind the EIP in exercise 4 and use the EIP to create an SNAT rule. Check whether **ecs-demo-1** and **ecs-demo-2** can use the same EIP to access the Internet (by pinging https://www.huaweicloud.com/intl/en-us/).

Extended Questions

- **Question 1**: A VPC peering connection can connect two VPCs in the same region, but how do I establish a network connection between two VPCs in different regions?
- **Question 2**: How do I establish connections between an on-premises data center and a virtual network on Huawei Cloud?

How Networking Services Work Together

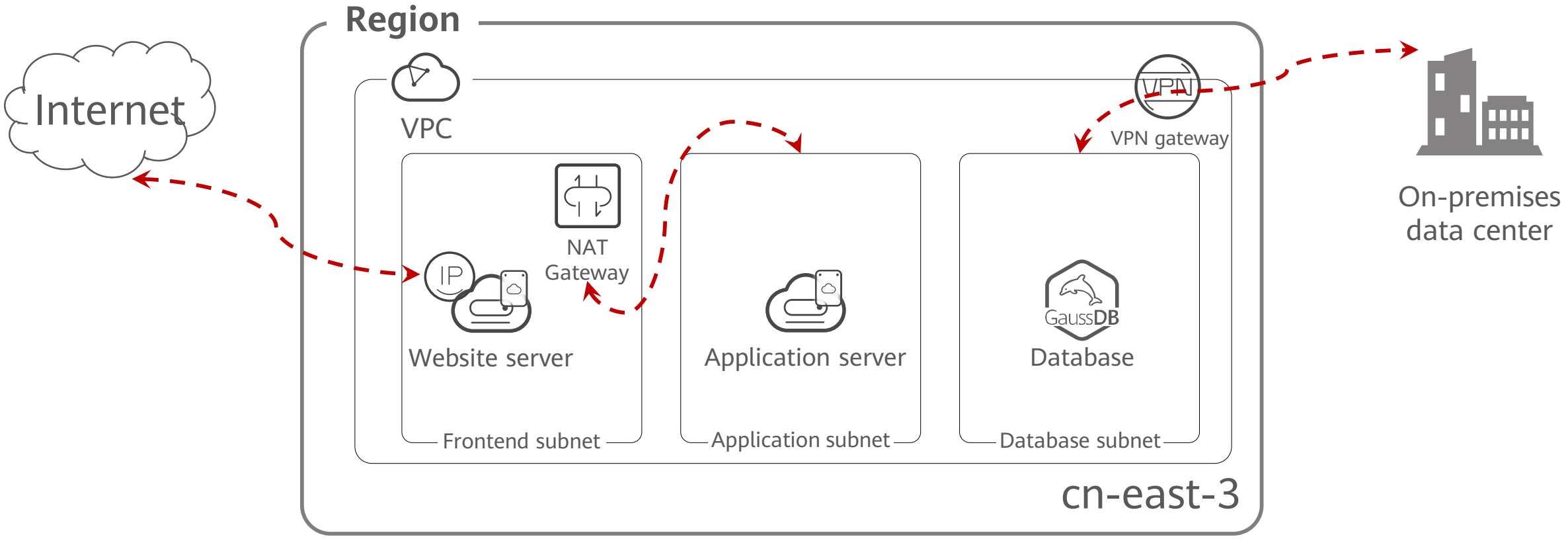


HUAWEI

Contents

HUAWEI

Networking Service Best Practices



HUAWEI

Summary

- This chapter discussed what a VPC is and how to create one. We covered how to enable communications between VPCs using VPC peering connections and how to secure VPC using security groups and network ACLs. This chapter also explained how to use EIP and NAT Gateway to allow ECSs to access the Internet.

Quiz

1. (Single-answer question) Which of the following networking cloud services can enable an ECS to access the Internet? ( )

   A. Virtual Private Cloud (VPC)

   B. VPC Peering Connection

   C. Elastic IP (EIP)

   D. NAT Gateway

2. (True or false) Two mutually trusted ECSs in the same security group cannot communicate with each other. One possible cause is that they are in different VPCs.

Recommendations

- Huawei Cloud websites
  - Huawei Cloud: https://www.huaweicloud.com/intl/en-us/
  - Huawei Cloud Developer Institute: https://edu.huaweicloud.com/intl/en-us/

Huawei Cloud
Developer Institute

Thank You.

HUAWEI CLOUD
EVERYTHING AS A SERVICE