Network Cloud Services - Virtual Private Cloud

Foreword

- With ever-increasing online service requirements, enterprise networks require a long time to market, have high O&M costs, and are faced with high security risks. More and more enterprises are now deploying their online services using Huawei Virtual Private Cloud (VPC).
- Huawei VPC is an infrastructure networking service. It leverages secure tunneling technology to provide secure and isolated networking environments. This chapter introduces the Huawei VPC service.

Objectives

- After completing this course, you will:
  - Be familiar with the VPC service.
  - Understand the concepts, functions, and application scenarios of the VPC service.
  - Be able to create and manage VPCs.

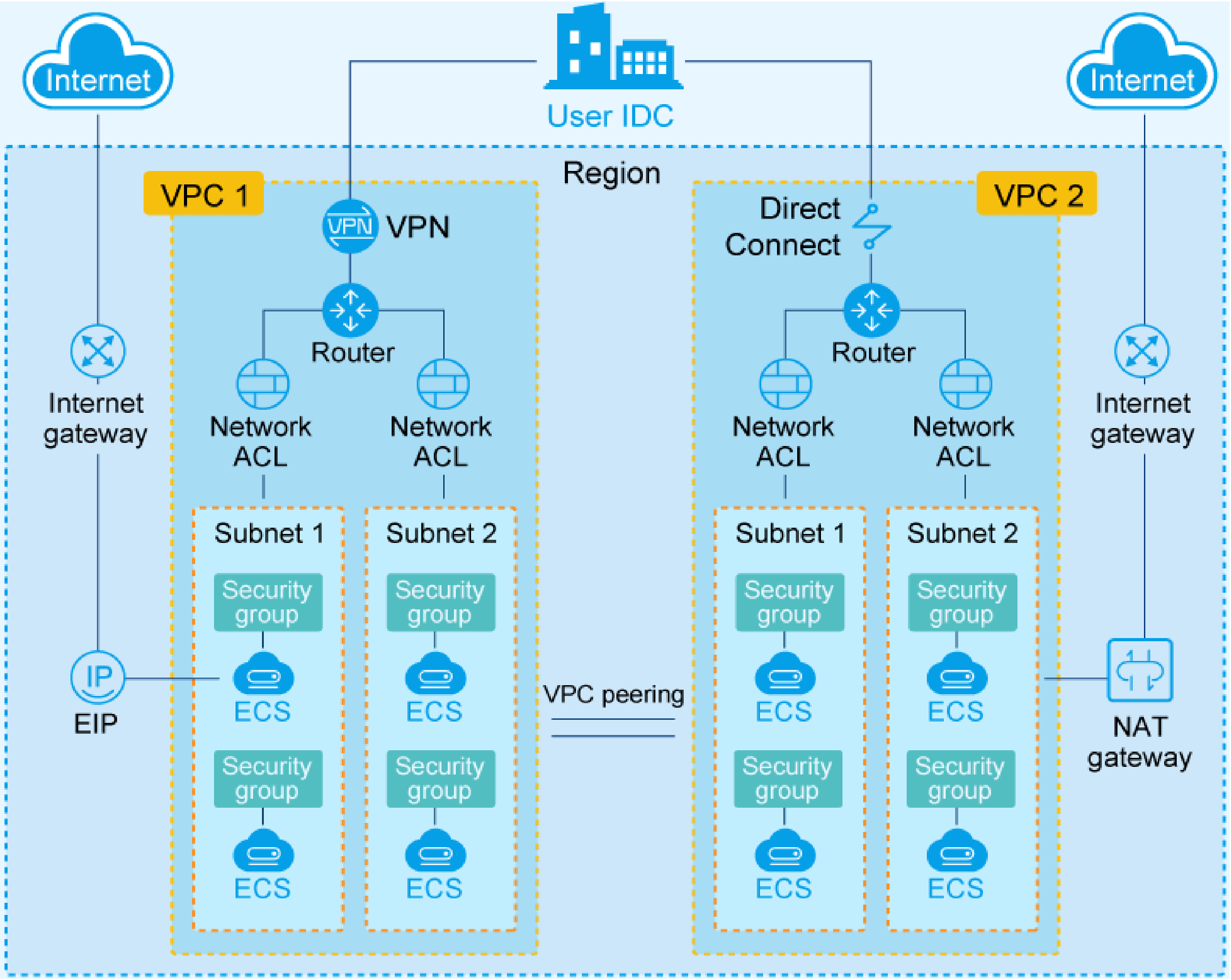
Contents

1. **VPC Overview**
2. VPC Concepts
3. VPC Application Scenarios
4. VPC Use and Management
5. VPC FAQs and Troubleshooting
6. Related Services of VPC

VPC Concept

A VPC is an isolated virtual network environment created on HUAWEI CLOUD. You have complete control over your virtual network, including creating subnets and security groups, assigning elastic IP addresses (EIPs), allocating bandwidth, and configuring DHCP.

VPC Product Architecture



VPC Product Advantages

Secure and Reliable

Private networks on the cloud are completely isolated.

You can create Elastic Cloud Servers (ECSs) that are in different availability zones, in the same VPC.

Flexible Configuration

Self-service network management frees you from routine network configurations

and allows flexible network deployment.

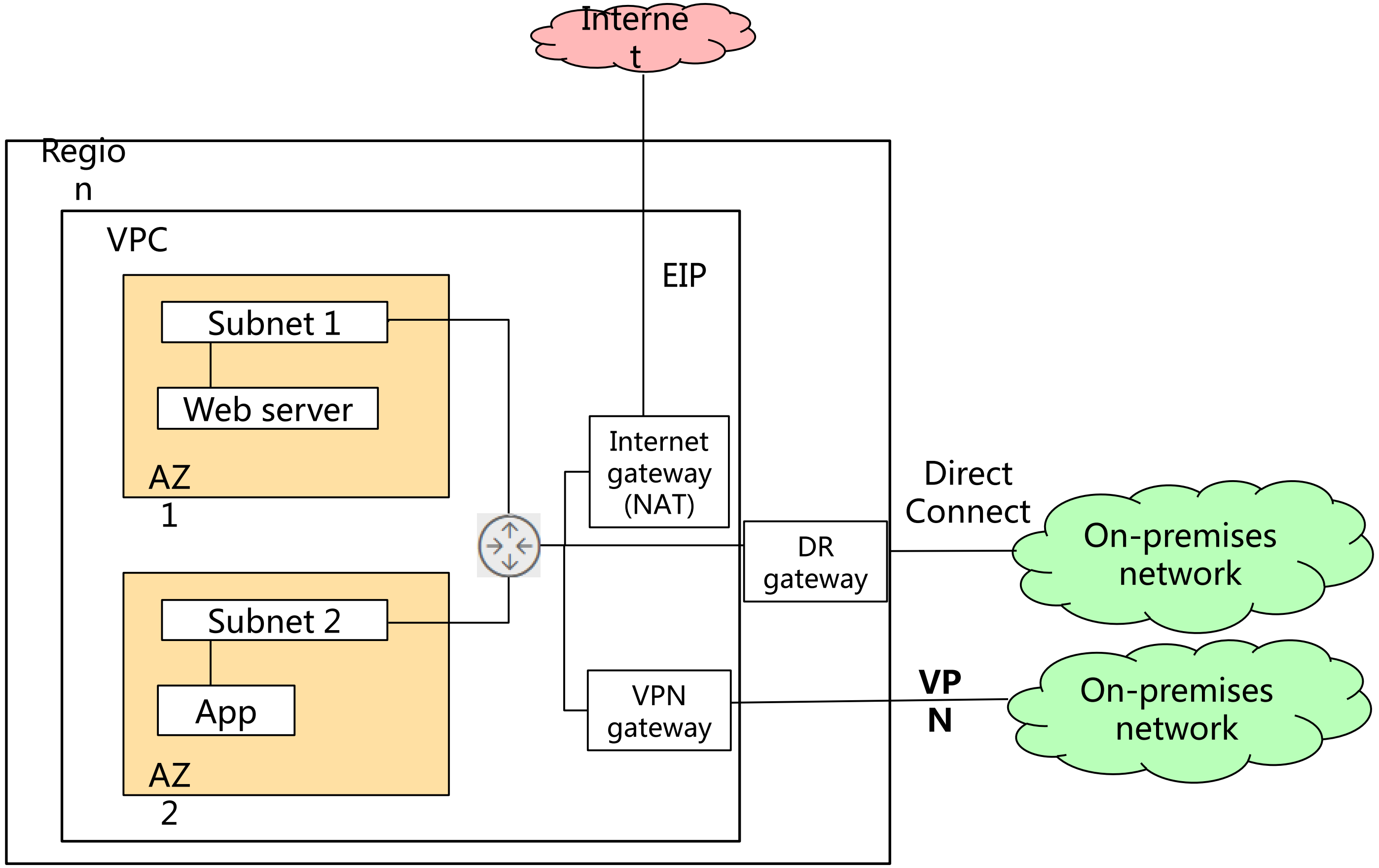
High-Speed Access

Dynamic BGP network connections enable seamless high-speed access to services on the cloud.

Interconnection

VPC peering enables interconnection between VPCs.

VPC Application Scenario – Large Internet Applications



VPC Application Scenarios

- **Hosting Universal Web Applications**
  - **Application scenarios**: Blogs and simple websites
  - **Characteristics**: You can host web applications and websites in a VPC and use the VPC as a common network. You can create a subnet and create ECSs in the subnet. You can also use EIPs to connect ECSs to the Internet for running web applications deployed on the ECSs.
- **Building Enterprise Hybrid Cloud**
  - **Application scenarios**: E-commerce websites
  - **Characteristics**: You can connect a VPC to your private cloud using a VPN connection. With a VPN connection between the VPC and your traditional data center, you can easily use the ECSs and block storage resources. Applications can be migrated to the cloud and additional web servers can be deployed to increase the computing capacity on a network. In this way, a hybrid cloud is built.
- **Hosting Security-Demanding Services**
  - **Application scenarios**: Security-demanding service systems
  - **Characteristics**: 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 and database servers in non-publically accessible subnets to ensure high security and meet requirements of security-demanding scenarios.

Function Description

- **Private Network Customization**

  You can customize private subnets in your VPC and deploy applications and other services in the subnets accordingly.

- **Flexible Security Policy Configuration**

  You can use security groups to divide ECSs in a VPC into different security zones and then configure different access control rules for each security zone. You can also create network ACLs to control traffic in and out of associated subnets, improving subnet security.

- **EIP Binding**

  You can assign an independent EIP in your VPC. The EIP can be bound to or unbound from an ECS as required. The binding and unbinding operations take effect immediately after the operations are performed.

- **Direct Connect/VPN Access**

  You can use a Direct Connect connection or VPN to connect your VPC with the corporate data center to form a hybrid network for smooth application migration to the cloud.

Contents

1. VPC Overview
2. **VPC Concepts**
3. VPC Application Scenarios
4. VPC Use and Management
5. VPC FAQs and Troubleshooting
6. Related Services of VPC

VPC Concepts

- Subnet
- EIP
- Bandwidth
- Security group
- VPN
- Remote gateway
- Remote subnet

Contents

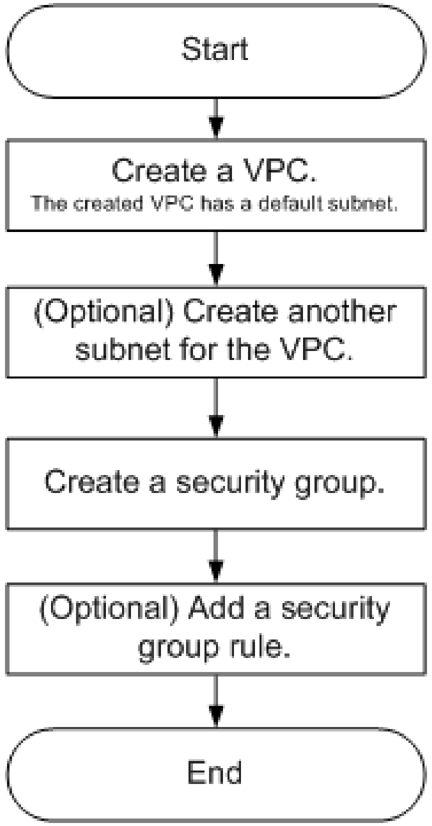
1. VPC Overview
2. VPC Concepts
3. **VPC Application Scenarios**
4. VPC Use and Management
5. VPC FAQs and Troubleshooting
6. Related Services of VPC

Typical VPC Application Scenarios

- Configuring a VPC for ECSs that do not require Internet access
- Configuring a VPC for ECSs that access the Internet using EIPs
- Configuring a VPC for ECSs that access the Internet using a VPN

VPC Configuration Procedure (1/2)

If your ECSs do not need to access the Internet (for example, the ECSs functioning as the database or server nodes for deploying a website), follow the procedure in the next slide to configure a VPC for the ECSs.



Start

Create a VPC.
The created VPC has a default subnet.

(Optional) Create another subnet for the VPC.

Create a security group.

(Optional) Add a security group rule.

End

VPC Configuration Procedure (2/2)

Task	Description	Mandatory
01 Create a VPC.	You must configure required parameters to create a VPC. The 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.	Yes
02 Create another subnet for the VPC.	If you need another subnet in addition to the default one, you can create a subnet in the VPC. The new subnet is used to assign IP addresses to NICs added to the ECS.	No
03 Create a security group.	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. If the default rule meets your service requirements, you do not need to add rules to the security group.	Yes
04 Add a security group rule.	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. If the default rule does not meet your service requirements, you can add a security group rule.	No

Contents

1. VPC Overview
2. VPC Concepts
3. VPC Application Scenarios
4. **VPC Use and Management**
5. VPC FAQs and Troubleshooting
6. Related Services of VPC

Common Operations

- VPC Common Operations
- Security Group Common Operations
- EIP Common Operations

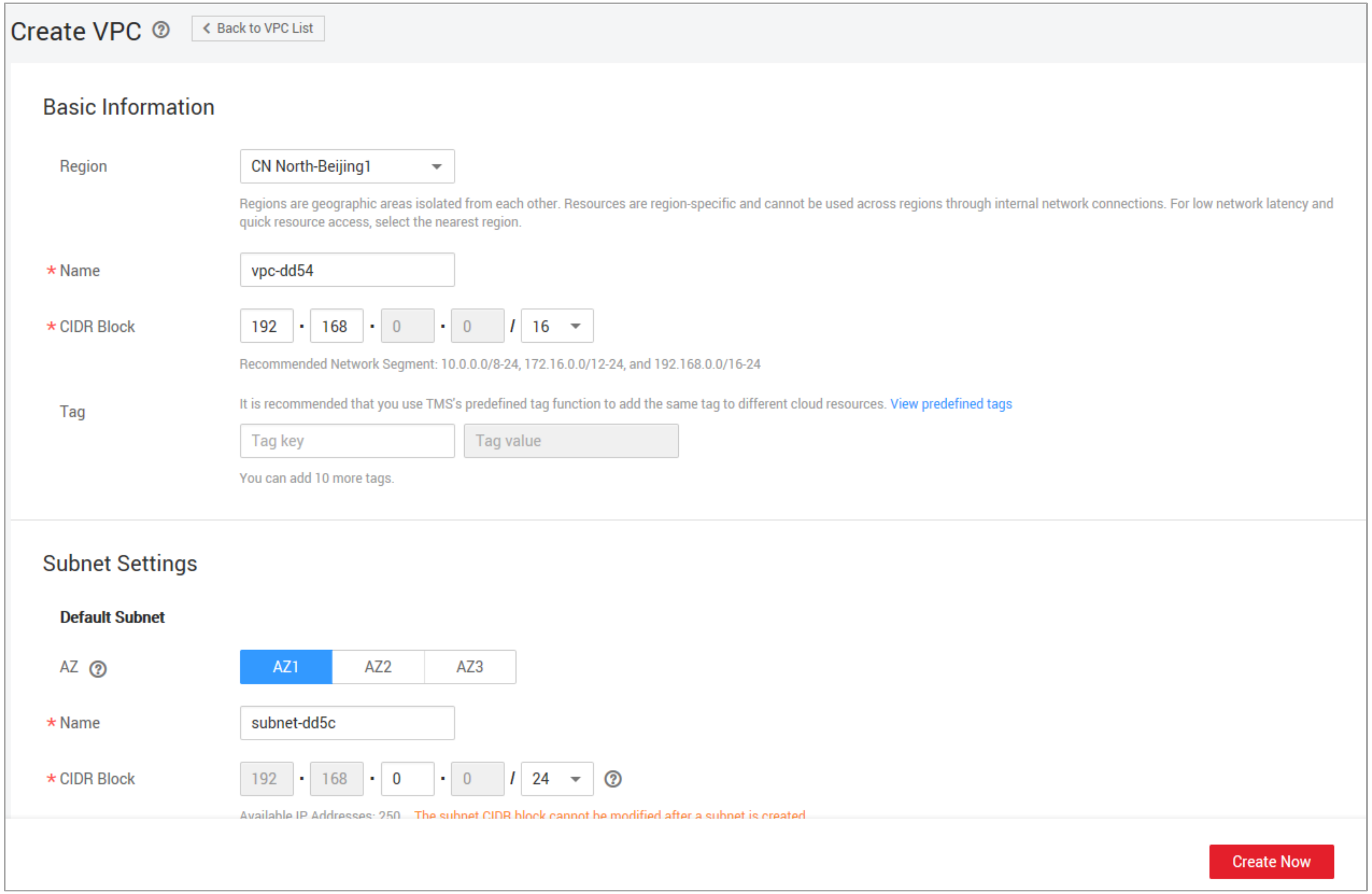
VPC Common Operations

- Creating a VPC
- Modifying a VPC
- Creating a subnet for the VPC
- Modifying a subnet
- Deleting a VPC

Creating a VPC

- **Scenario**
- A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required. Perform the following procedure to create a VPC. Then, create subnets, security groups, and VPNs, and assign EIPs based on your actual network requirements.
- **Procedure**
- Log in to the management console.
- On the console homepage, under **Network**, click **Virtual Private Cloud**.
- On the **Dashboard page**, click **Create VPC.**
- On the **Create VPC** page, set parameters as prompted.
- Click **Create Now**.

Console Page for VPC Creation



Basic Information

Region: CN North-Beijing1

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Name: vpc-dd54

* CIDR Block: 192 . 168 . 0 . 0 / 16

Recommended Network Segment: 10.0.0.0/8-24, 172.16.0.0/12-24, and 192.168.0.0/16-24

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

You can add 10 more tags.

Subnet Settings

Default Subnet

AZ: AZ1 | AZ2 | AZ3

* Name: subnet-dd5c

* CIDR Block: 192 . 168 . 0 . 0 / 24

Available IP Addresses: 250 The subnet CIDR block cannot be modified after a subnet is created.

VPC Configuration Parameters

Parameter	Description	Example Value
Region	Specifies the desired region. Regions are geographic areas isolated from each other. Resources are specific to a region and cannot be used across regions through internal network connections. Select the nearest region for quick resource access and low network latency.	CN North-Beijing1
Name	Specifies the VPC name.	VPC-001
CIDR Block	Specifies the CIDR block for 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 (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	Specifies the enterprise project to which the VPC belongs. By default, the VPC belongs to the **Default** project.	Default
Tag	Specifies the VPC tag, which consists of a key and value pair. You can add a maximum of ten tags to each VPC.	• Key: vpc_key1 • Value: vpc-01
Name (Subnet Settings)	Specifies the subnet name.	Subnet
CIDR Block (Subnet Settings)	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR range.	192.168.0.0/24
Gateway	Specifies the gateway address of the subnet.	192.168.0.1
DNS Server Address	The external DNS server address is used by default. If you need to change the DNS server address, ensure that the configured DNS server address is available.	192.168.1.0
Tag (Subnet Settings)	Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of ten tags to each subnet.	• Key: subnet_key1 • Value: subnet-01

Creating a subnet for the VPC

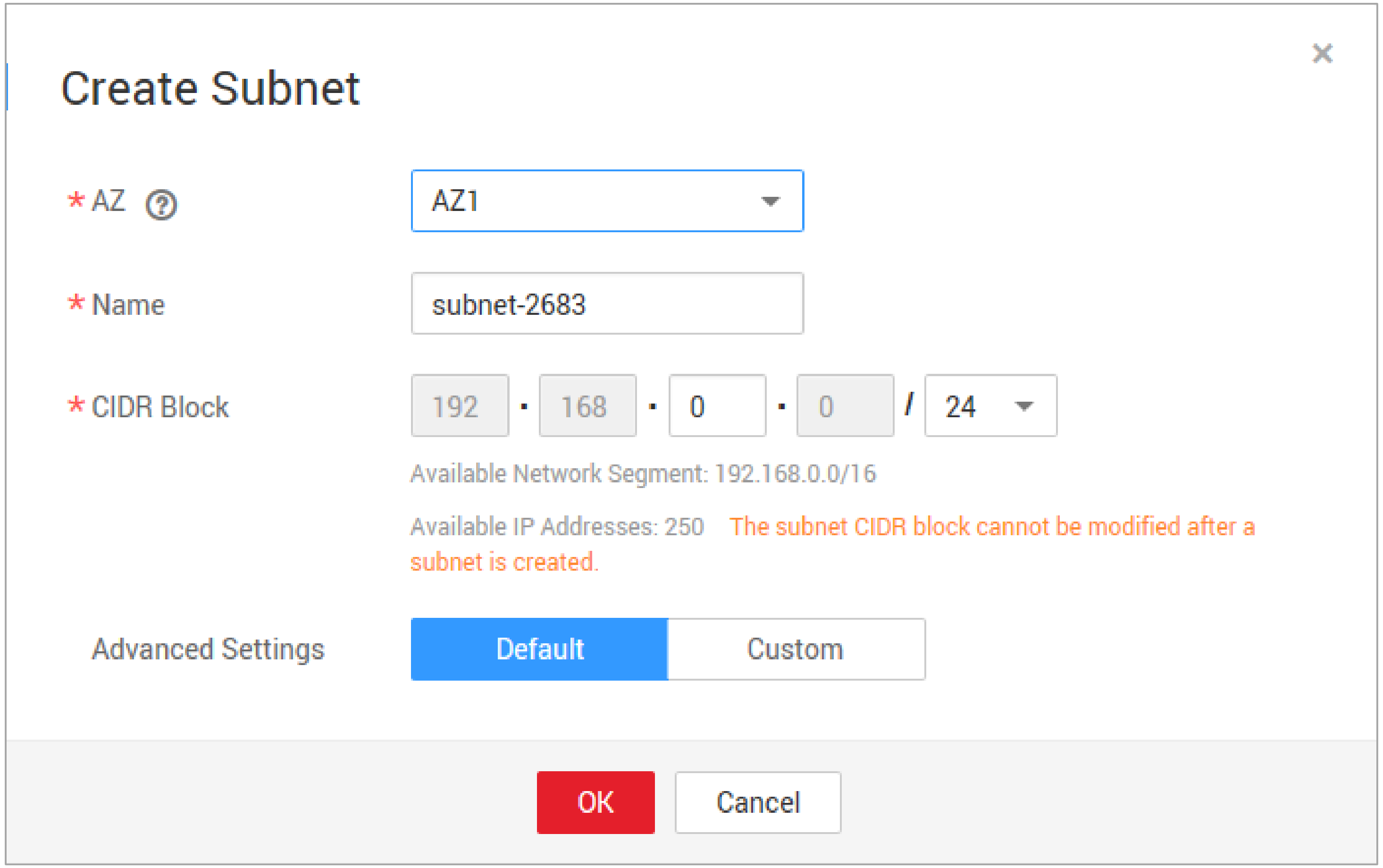
- **Scenario**

  A subnet is automatically created when you create a VPC. If required, you can create another subnet in the VPC.

- **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, select the VPC for which a subnet is to be created.
  4. On the **Subnets** page, click **Create Subnet**.
  5. In the **Create Subnet** area, set parameters as prompted.
  6. Click **OK**.

Console Page for Subnet Creation



Create Subnet

* AZ: AZ1

* Name: subnet-2683

* CIDR Block: 192 . 168 . 0 . 0 / 24

Available Network Segment: 192.168.0.0/16

Available IP Addresses: 250 The subnet CIDR block cannot be modified after a subnet is created.

Advanced Settings: [✓ Default] Custom

Subnet Configuration Parameters

Parameter	Description	Example Value
Name	Specifies the subnet name.	Subnet
CIDR Block	Specifies the CIDR block for the subnet. This value must be within the VPC CIDR range.	192.168.0.0/24
Gateway	Specifies the gateway address of the subnet.	192.168.0.1
DNS Server Address	The external DNS server address is used by default. If you need to change the DNS server address, ensure that the configured DNS server address is available.	192.168.1.0
Tag	Specifies the subnet tag, which consists of a key and value pair. You can add a maximum of ten tags to each subnet.	• Key: subnet_key1 • Value: subnet-01

Security Group Common Operations

- Creating a security group
- Adding a security group rule
- Deleting a security group rule
- Deleting a security group

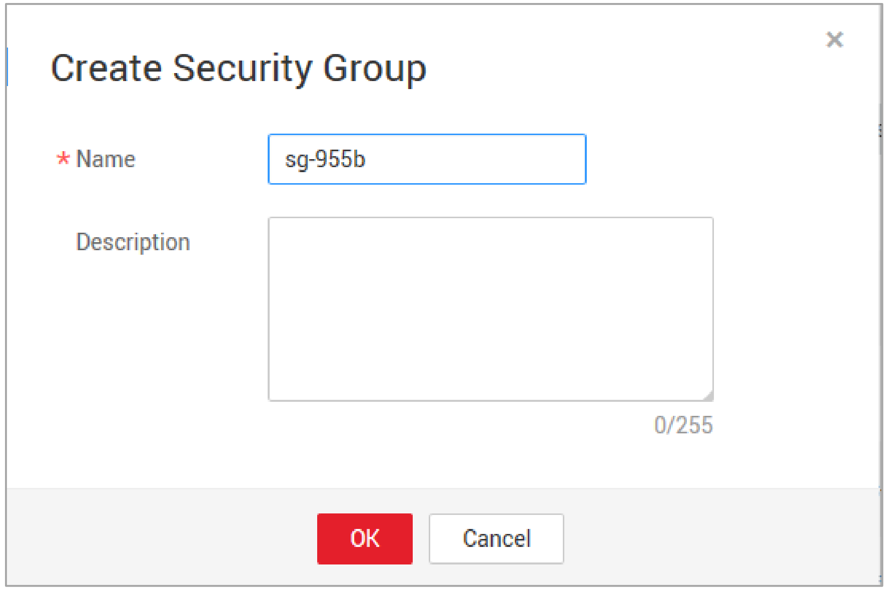
Creating a Security Group

- **Scenario**

  To improve ECS access security, you can create a security group, define security group rules, and add ECSs in the VPC to the security group. 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, click **Security Group**.
  4. On the **Security Group** page, click **Create Security Group**.
  5. In the **Create Security Group** area, set parameters as prompted.
  6. Click **OK**



Create Security Group

* Name: sg-955b

Description:

0/255

Creating a Security Group Rule (1/2)

- **Scenario**
  After a security group is created, it has default rules. You can add new inbound and outbound rules to the security group.
  Inbound rules control incoming traffic to ECSs in the security group.
  Outbound rules control outgoing traffic from ECSs in the security group.
- **Default security group rules**

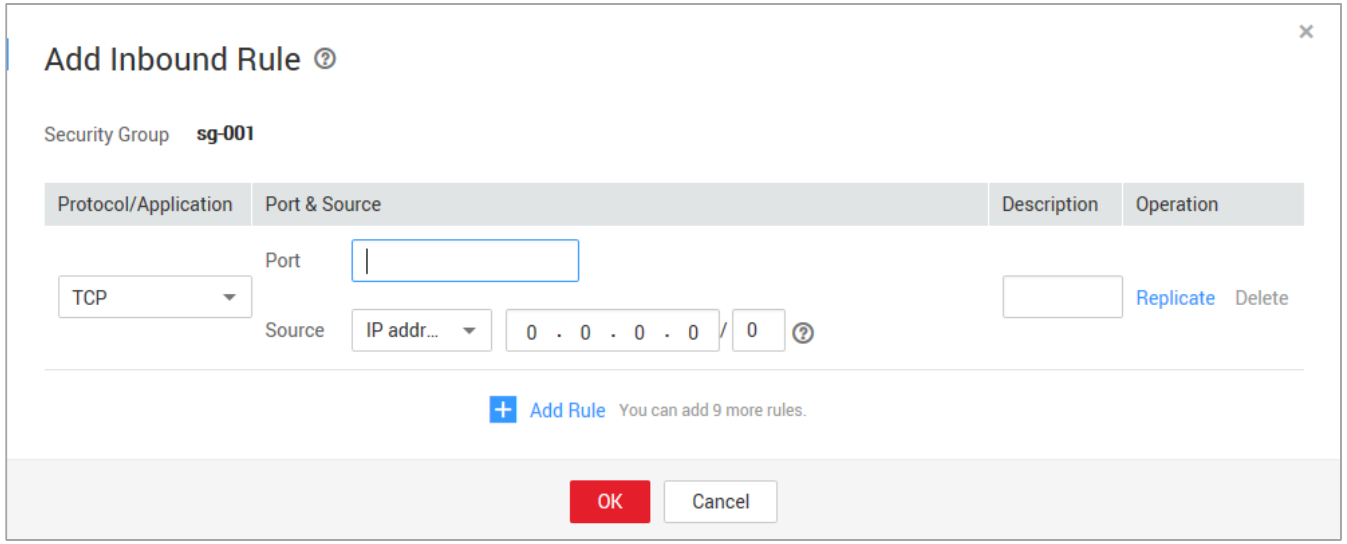
Transfer Direction	Protocol	Port/Range	Source/Destination	Description
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic.
Inbound	All	All	Source: Current security group ID (for example, sg-*xxxxx*)	Allow inbound traffic from ECSs added to the same security group.
Inbound	TCP	22	Source: 0.0.0.0/0	Allows all IP addresses to access Linux ECSs over SSH.
Inbound	TCP	3389	Source: 0.0.0.0/0	Allow all IP addresses to access Windows ECSs over RDP.

Creating a Security Group Rule (2/2)

- **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 **Security Group**.
4. On the **Security Group** 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** or **Outbound Rules** tab, click **Add Rule** to add an inbound or outbound rule.

Console Page for Security Group Rule Creation

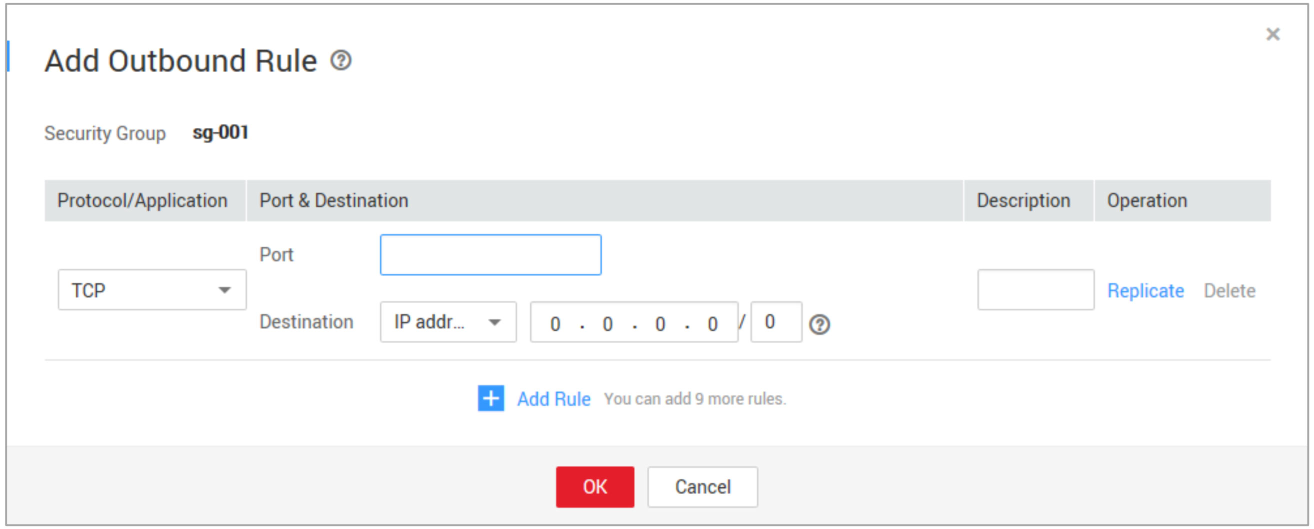


Add Inbound Rule

Security Group sg-001

Protocol/Application	Port & Source	Description	Operation
TCP	Port Source IP addr... 0 . 0 . 0 . 0 / 0		Replicate Delete

Add Rule You can add 9 more rules.



Add Outbound Rule

Security Group sg-001

Protocol/Application	Port & Destination	Description	Operation
TCP	Port Destination IP addr... 0 . 0 . 0 . 0 / 0		Replicate Delete

Add Rule You can add 9 more rules.

Security Group Rule Configuration Parameters

Parameter	Description	Example Value
Protocol	Specifies the network protocol for which the security group rule takes effect.	TCP
Port & Source (Inbound)	**Port**: specifies the port or port range for which the security group rule takes effect. The value ranges from **1** to **65535**.	22 or 22-30
	Source: specifies the source of the security group rule. The value can be another security group, a CIDR block, or a single IP address. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (CIDR block) • 0.0.0.0/0 (any IP address)	0.0.0.0/0 default
Port & Destination (Outbound)	**Port**: specifies the port or port range for which the security group rule takes effect. The value ranges from **1** to **65535**.	22 or 22-30
	Source: specifies the source of the security group rule. The value can be another security group, a CIDR block, or a single IP address. For example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (CIDR block) • 0.0.0.0/0 (any IP address)	0.0.0.0/0 default
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

EIP Common Operations

- Assigning an EIP and binding it to an ECS
- Querying and modifying bandwidth

Assigning an EIP and Binding It to an ECS (1/3)

- **Scenario**

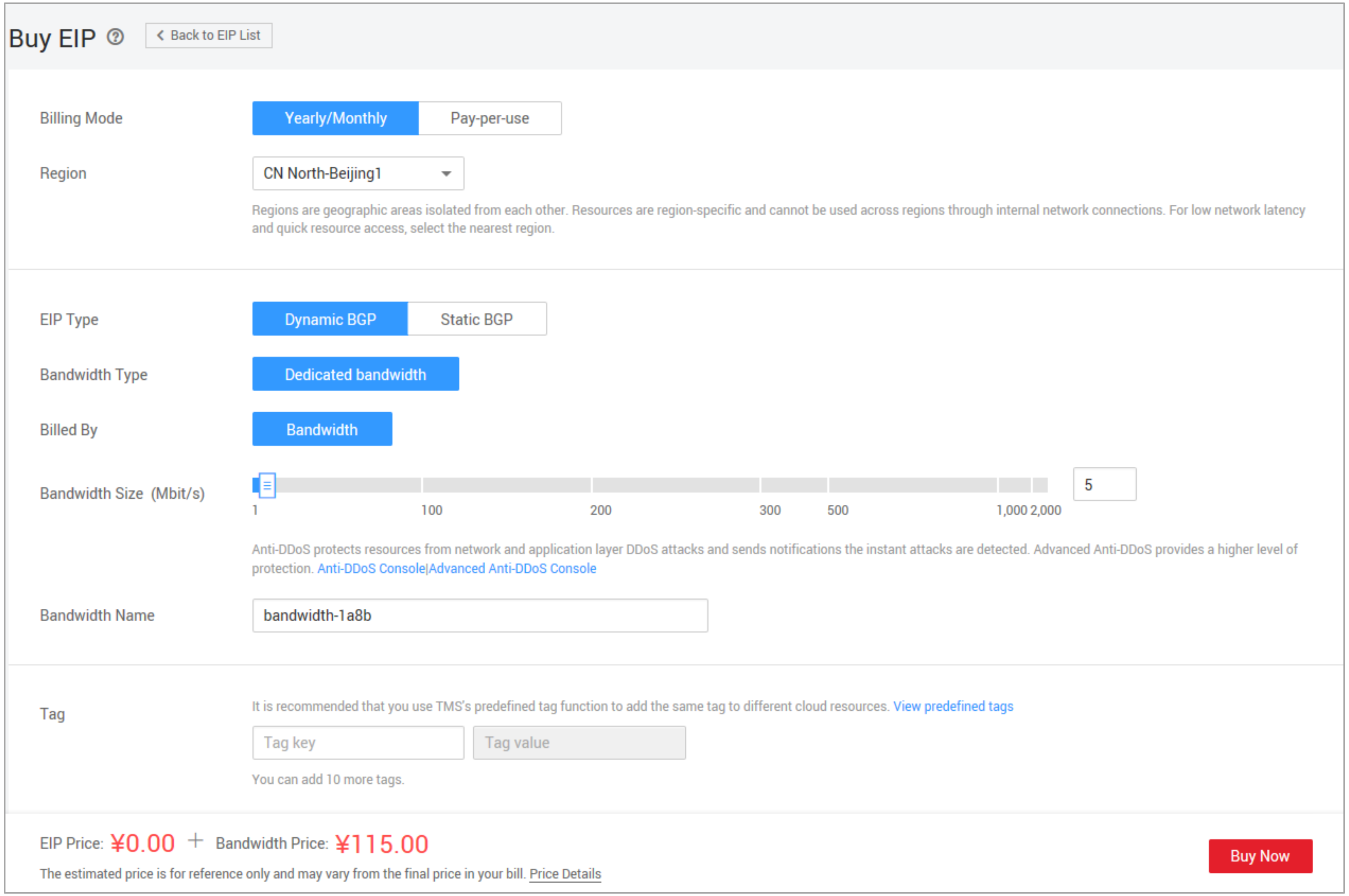
  You can assign an EIP and bind it to an ECS to enable the ECS to access the Internet.

- **Procedure**

Assign an EIP.

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 **Elastic IP**.
4. On the **Elastic IP** page, click **Buy EIP**.
5. In the displayed dialog box, set parameters as prompted.
6. Click **Buy Now**.

Assigning an EIP and Binding It to an ECS (2/3)



Buy EIP

Billing Mode: **Yearly/Monthly** | Pay-per-use

Region: CN North-Beijing1

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

EIP Type: **Dynamic BGP** | Static BGP

Bandwidth Type: **Dedicated bandwidth**

Billed By: **Bandwidth**

Bandwidth Size (Mbit/s): 5

Anti-DDoS protects resources from network and application layer DDoS attacks and sends notifications the instant attacks are detected. Advanced Anti-DDoS provides a higher level of protection. Anti-DDoS Console|Advanced Anti-DDoS Console

Bandwidth Name: bandwidth-1a8b

Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

You can add 10 more tags.

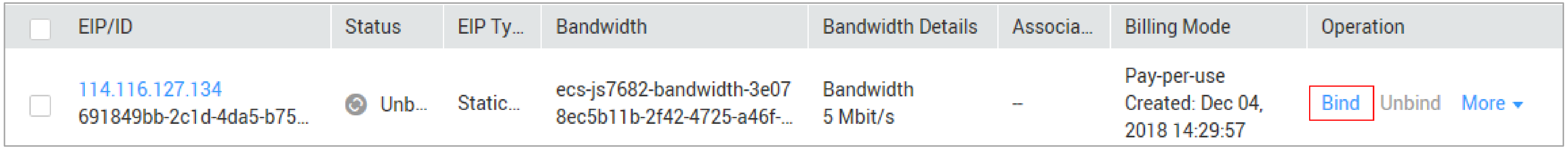
EIP Price: ¥0.00 + Bandwidth Price: ¥115.00

The estimated price is for reference only and may vary from the final price in your bill. Price Details

Assigning an EIP and Binding It to an ECS (3/3)

Bind an EIP.

1. On the **Elastic IP** page, locate the row that contains the target EIP, and click **Bind** in the **Operation** column.
2. Select the desired instance.
3. Click **OK**



□	EIP/ID	Status	EIP Ty...	Bandwidth	Bandwidth Details	Associa...	Billing Mode	Operation
□	114.116.127.134 691849bb-2c1d-4da5-b75...	Unb...	Static...	ecs-js7682-bandwidth-3e07 8ec5b11b-2f42-4725-a46f-...	Bandwidth 5 Mbit/s	--	Pay-per-use Created: Dec 04, 2018 14:29:57	Bind Unbind More ▾

Querying and Modifying Bandwidth (1/2)

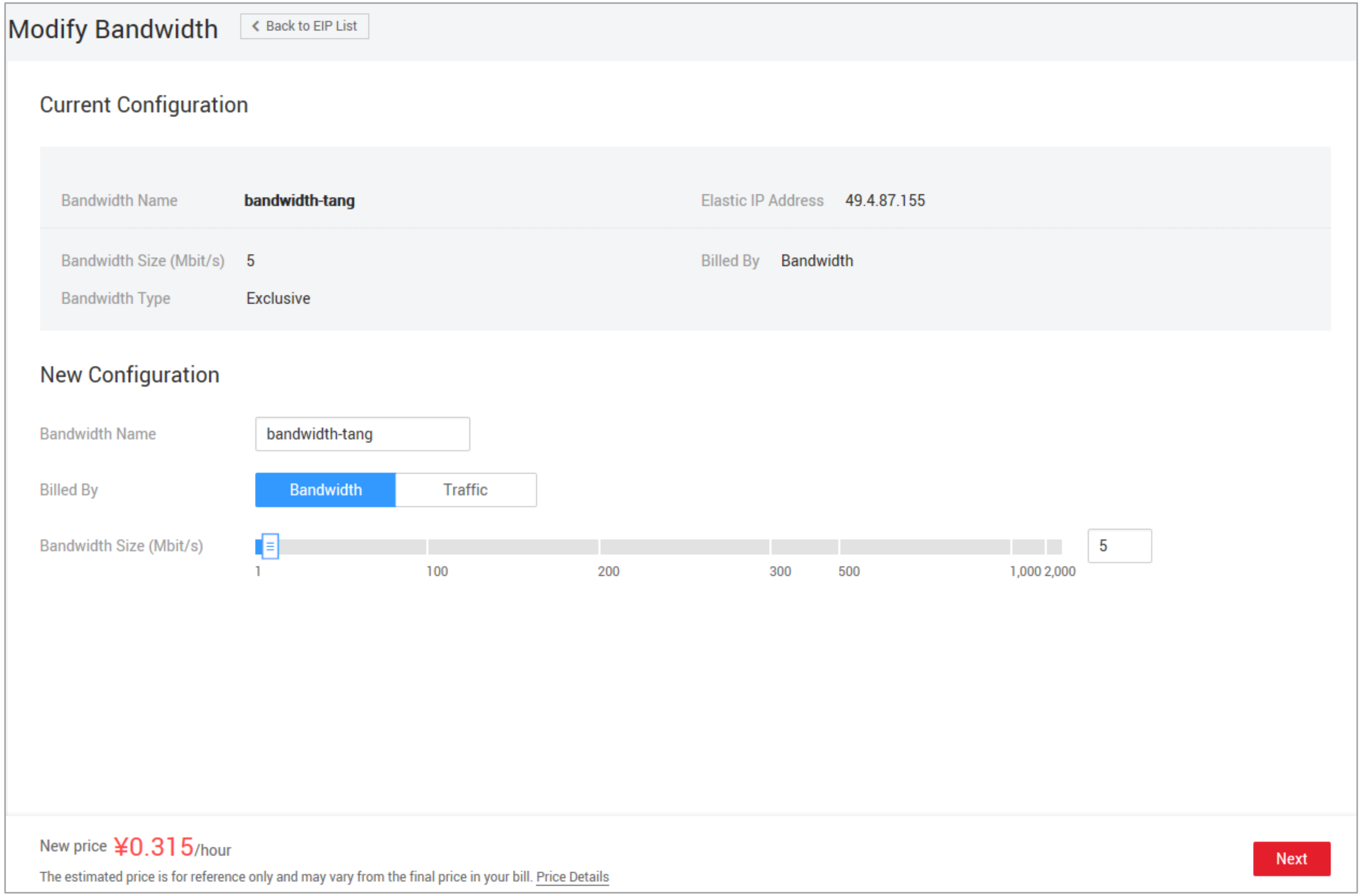
- **Scenario**

  Modify the name and size of the EIP bandwidth.

- **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 **Elastic IP**.
4. Locate the row that contains the target EIP in the EIP list, click **More** in the **Operation** column, and select **Modify Bandwidth**.
5. Modify bandwidth parameters as prompted.
6. Click **OK**

Querying and Modifying Bandwidth (2/2)



Modify Bandwidth

Current Configuration

Bandwidth Name	**bandwidth-tang**	Elastic IP Address	49.4.87.155
Bandwidth Size (Mbit/s)	5	Billed By	Bandwidth
Bandwidth Type	Exclusive		

New Configuration

Bandwidth Name: bandwidth-tang

Billed By: Bandwidth | Traffic

Bandwidth Size (Mbit/s): 5

New price ¥0.315/hour

The estimated price is for reference only and may vary from the final price in your bill. Price Details

Contents

1. VPC Overview
2. VPC Concepts
3. VPC Application Scenarios
4. VPC Use and Management
5. **VPC FAQs and Troubleshooting**
6. Related Services of VPC

VPC FAQs

- **Will I Be Charged for Using the VPC Service?**
  The VPC service is free of charge itself. However, you are charged for the bandwidth or VPN used in the VPC.
- **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
- **Can Subnets Communicate with Each Other?**
  Subnets belong to VPCs. Subnets in the same VPC can communicate with each other. 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.
- **Can I Modify the CIDR Block of a Subnet?**
  The subnet CIDR block cannot be modified after a subnet is created.
- **How Many Subnets Can I Create?**
  By default, one tenant can create a maximum of 100 subnets. If the number of subnets cannot meet your service requirements, submit a service ticket to increase the quota.
- **What Is the Bandwidth Size Range?**
  The bandwidth size ranges from 1 Mbit/s to 2000 Mbit/s.
- **What Bandwidth Types Does the VPC Service Support?**
  The VPC service supports the dedicated bandwidth and shared bandwidth. The dedicated bandwidth can be used by only one EIP, whereas the shared bandwidth can be shared by multiple EIPs.

Contents

1. VPC Overview
2. VPC Concepts
3. VPC Application Scenarios
4. VPC Use and Management
5. VPC FAQs and Troubleshooting
6. **Related Services of VPC**

Related Services

- **ECS**

  A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required. The VPC service provides multiple connectivity options for ECSs to access the Internet. You can also customize the ECS access rules within a security group and between security groups to improve ECS security.

- **ELB**

  ELB uses the EIP and bandwidth provided by the VPC service.

- **Cloud Eye**

  After the VPC service becomes available to you, you can use Cloud Eye to view status of monitored objects of the service without requiring additional plug-ins to be installed.

- **Cloud Trace Service (CTS)**

  With CTS, you can record operations performed on the VPC service for further query, audit, and backtrack purposes.

Quiz

Which of the Following Functions Are Provided by HUAWEI CLOUD VPC?

A. Customizing CIDR blocks

B. Customizing access control policies

C. Accessing the Internet using EIPs

D. Connecting a local data center using a VPN or Direct Connect connection

Quiz

Which of the Following Functions Are Provided by HUAWEI CLOUD VPC?

A. Customizing CIDR blocks

B. Customizing access control policies

C. Accessing the Internet using EIPs

D. Connecting a local data center using a VPN or Direct Connect connection

Summary

- Introduces the HUAWEI CLOUD VPC service.
- Introduces the concepts, functions, and application scenarios of the VPC service.
- Illustrates how to create and manage VPCs.

Recommendations

- **Huawei learning website:**

  http://support.huawei.com/learning/en/newindex.html

- HUAWEI CLOUD official websites

  https://www.huaweicloud.com/en-us/ (China)

  https://intl.huaweicloud.com/?locale=en-us (International)

Acronyms

Acronym	Full Name
AZ	Availability Zone
BGP	Border Gateway Protocol
DNS	Domain Name Server
EIP	Elastic Internet Protocol
IPsec	Internet Protocol Security
VPN	Virtual Private Network
IGW	Integration Gateway
NAT	Network Address Translation

Thank You

www.huawei.com