Elastic IP

Getting Started

Issue 01

Date 2024-12-11

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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

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

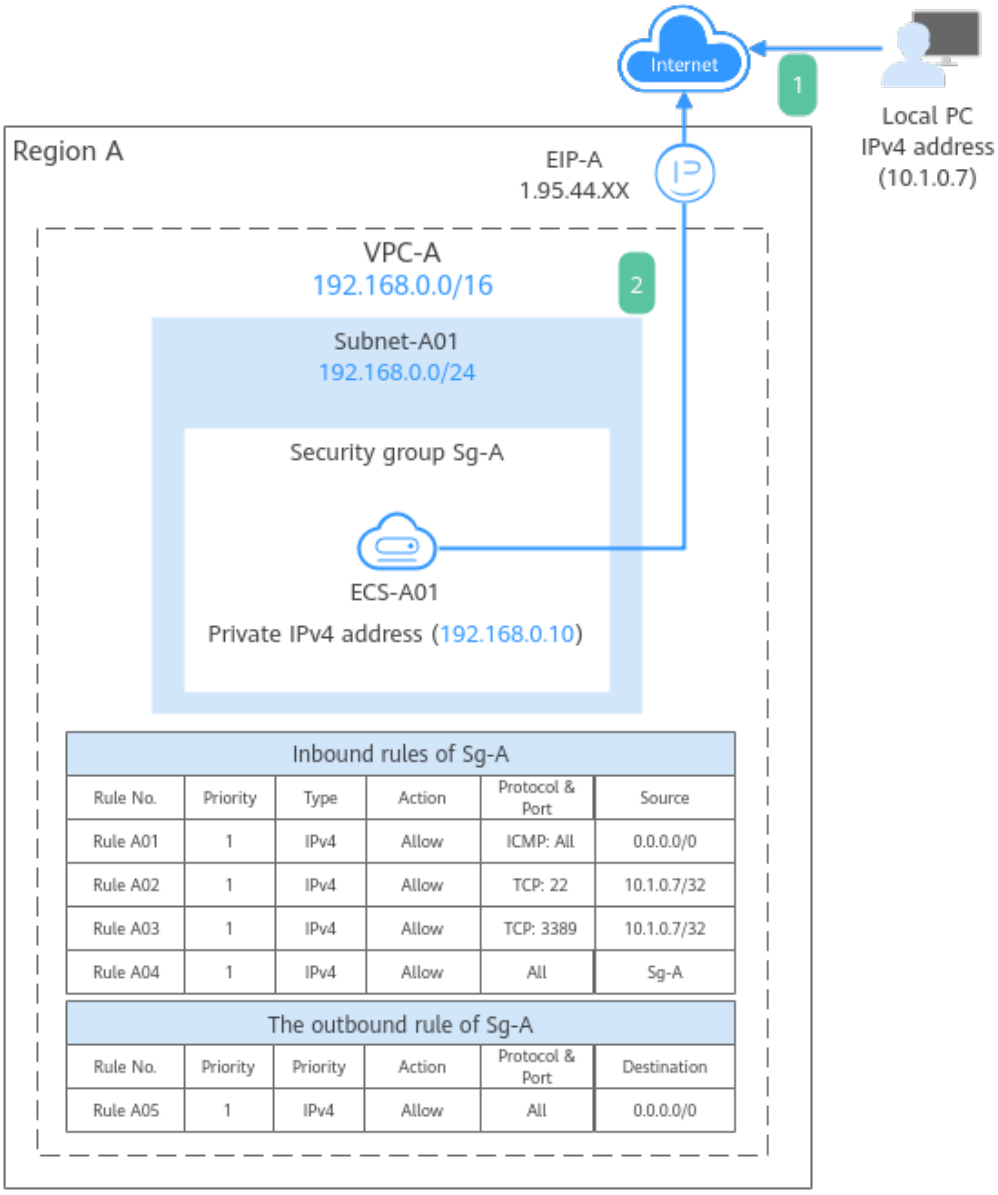
Contents

1 Setting Up a Network in a VPC and Enabling Internet Access Using an EIP

This topic describes how to create a VPC and an ECS to set up an IPv4 private network on the cloud and bind an EIP to the ECS to allow the ECS to access the Internet.

Figure 1-1 shows the architecture of an IPv4 network. In this network, security group **Sg-A** protects ECS **ECS-A01** in it. You can configure security group rules to control access to and from **ECS-A01**.

Figure 1-1 The architecture of an IPv4 network



1. To allow users to remotely log in to **ECS-A01** from the local PC (IP address: 10.1.0.7) and perform operations on this ECS, you need to configure the following inbound rules:
   - Rule A01: allows the local PC to ping **ECS-A01** in **VPC-A** over all ICMP ports to test network connectivity.
   - Rules A02: allow the local PC to remotely log in to **ECS-A01** over TCP port 22 if the ECS runs Linux.
   - Rules A03: allow the local PC to remotely log in to **ECS-A01** over TCP port 3389 if the ECS runs Windows.
   - Rule A04: allows ECSs in **Sg-A** to communicate with each other.
2. To allow **ECS-A01** to access the Internet, you need to EIP **EIP-A** to it and add outbound rule A05.

Precautions

The network planning in this topic is only for your reference. Once a VPC and subnet are created, the CIDR blocks cannot be changed. Before creating VPCs, determine how many VPCs, the number of subnets, and what CIDR blocks or connectivity options you will need.

For details, see **VPC and Subnet Planning Suggestions**.

Operation Process

Procedure	Description
Preparations	Before using cloud services, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account.
Step 1: Create a VPC and Subnet	Create a VPC with an IPv4 CIDR block and create a subnet in the VPC. • VPC IPv4 CIDR block: 192.168.0.0/16 • Subnet IPv4 CIDR block: 192.168.0.0/24
Step 2: Buy an ECS	Buy an ECS in the subnet you have created and configure security group rules for the ECS.
Step 3: Buy an EIP and Bind It to ECS-A01	Buy an EIP and bind it to the ECS so that the ECS can access the Internet.
Step 4: Test Network Connectivity	To test ECS connectivity, you can: 1. Log in to the ECS from the local PC. 2. Access the Internet from the ECS using an EIP.

Preparations

Before creating resources such as VPCs and ECSs, you need to sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account. Ensure that your account has sufficient balance.

1. You have created a HUAWEI ID, enabled Huawei Cloud services, and completed real-name authentication.

   If you already have a HUAWEI ID, skip this part. If you do not have a HUAWEI ID, perform the following operations to create one:

   a. **Sign up for a HUAWEI ID and enable Huawei Cloud services**.

   b. Complete **real-name authentication**.

2. You need to ensure that your account has sufficient balance. If it does not, **top up your account**.

Step 1: Create a VPC and Subnet

1. Go to the **Create VPC** page.

2. On the **Create VPC** page, set parameters as needed.
   In this example, you need to create a VPC and a subnet.

Figure 1-2 Creating a VPC

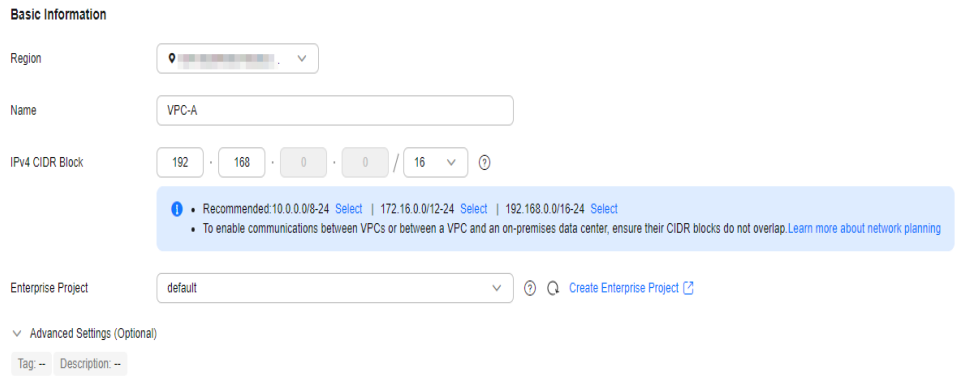


Figure 1-3 Setting a subnet

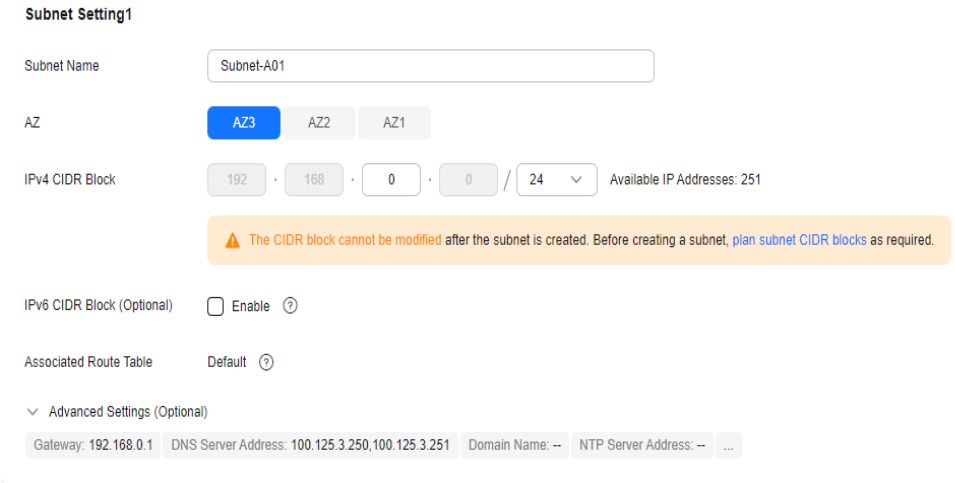


Table 1-1 VPC parameters

Parameter	Example Value	Description
Region	CN-Hong Kong	The region where the VPC is created. Select the region nearest to you to ensure the lowest possible latency. The VPC, ECS, and EIP used in this example must be in the same region. The region cannot be changed after the VPC is created.
Name	VPC-A	The VPC name. Set it to **VPC-A**. The name can be modified after **VPC-A** is created.

Parameter	Example Value	Description
IPv4 CIDR Block	192.168.0.0/16	The IPv4 CIDR block of **VPC-A**. You are advised to select from the following CIDR blocks: • 10.0.0.0/8-24: The IP address ranges from 10.0.0.0 to 10.255.255.255, and the netmask ranges from 8 to 24. • 172.16.0.0/12-24: The IP address ranges from 172.16.0.0 to 172.31.255.255, and the netmask ranges from 12 to 24. • 192.168.0.0/16-24: The IP address ranges from 192.168.0.0 to 192.168.255.255, and the netmask ranges from 16 to 24. The IPv4 CIDR block cannot be changed after **VPC-A** is created.
Enterprise Project	default	The enterprise project by which VPCs are centrally managed. Select an existing enterprise project for **VPC-A**. The enterprise project cannot be changed after **VPC-A** is created.
Advanced Settings (Optional) > Tag	Not required	The tag that is used to classify and identify resources. Add tags to **VPC-A** as required. After **VPC-A** is created, you can edit tags added to **VPC-A**.
Advanced Settings (Optional) > Description	Not required	Supplementary information about **VPC-A**. Enter a description as required. The description can be modified after **VPC-A** is created.

Table 1-2 Subnet parameters

Parameter	Example Value	Description
AZ	AZ4	A geographic location with independent power supply and network facilities in a region. Each region contains multiple AZs. AZs are physically isolated but connected through an internal network. Subnets of a VPC can be located in different AZs without affecting communications. You can select any AZ in a region. If **Edge** is displayed, select an edge AZ based on your service requirements. If **Edge** is not displayed, you do not need to set the subnet AZ, which does not affect your service running. An ECS and its VPC can be in different AZs. For example, you can select AZ1 for the ECS and AZ3 for its VPC subnet. The AZ cannot be changed after **Subnet-A01** is created. You can select an AZ for a subnet only in certain regions. See the available regions on the management console.
Subnet Name	Subnet-A01	The subnet name. Set it to **Subnet-A01**. The name can be modified after **Subnet-A01** is created.
IPv4 CIDR Block	192.168.0.0/24	The IPv4 CIDR block of **Subnet-A01**, which is a unique CIDR block with a range of IP addresses in **VPC-A**. The CIDR block cannot be changed after **Subnet-A01** is created.
IPv6 CIDR Block (Optional)	Disabled	Whether to assign IPv6 addresses. You can enable or disable this option after **Subnet-A01** is created.

Parameter	Example Value	Description
Associated Route Table	Default	The default route table that **Subnet-A01** is associated with. Each VPC comes with a default route table. Subnets in the VPC are then automatically associated with the default route table. The default route table has a preset system route that allows subnets in a VPC to communicate with each other. After **Subnet-A01** is created, you can create a custom route table and associate **Subnet-A01** with it.
Advanced Settings (Optional) > Gateway	192.168.0.1	The gateway address of **Subnet-A01**. You are advised to retain the default address. The gateway address cannot be changed after **Subnet-A01** is created.
Advanced Settings (Optional) • DNS Server Address • Domain Name • NTP Server Address • IPv4 DHCP Lease Time	Not required	The parameters are configured for the **ECS-A01** in **VPC-A**. In this example, retain the default values or leave them blank. You can change the values after **Subnet-A01** is created.
Advanced Settings (Optional) > Tag	Not required	The tag that is used to classify and identify resources. Add tags to **Subnet-A01** as required. After **Subnet-A01** is created, you can edit the tags added to **Subnet-A01**.
Advanced Settings (Optional) > Description	Not required	Supplementary information about **Subnet-A01**. Enter a description as required. The description can be modified after **Subnet-A01** is created.

3. Click **Create Now**.

   You will be redirected to the VPC list, where you can find **VPC-A** you have created.

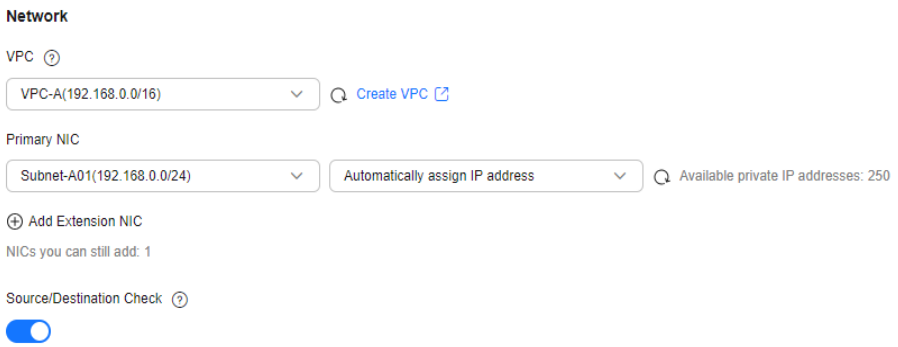
Step 2: Buy an ECS

1. Go to the **Buy ECS** page.
2. On the **Buy ECS** page, set parameters as required.

   In this example, set the ECS name to **ECS-A01** and configure other parameters as follows:

   - **Network**: Select **VPC-A** and **Subnet-A01** you have created.

     Figure 1-4 Network settings

   - **Security Group**: Create security group **Sg-A** and add inbound and outbound rules to it. Each security group comes with system rules. You need to check and modify the rules as required to ensure that all rules in **Table 1-3** are added.

     Figure 1-5 Inbound rules of **Sg-A**

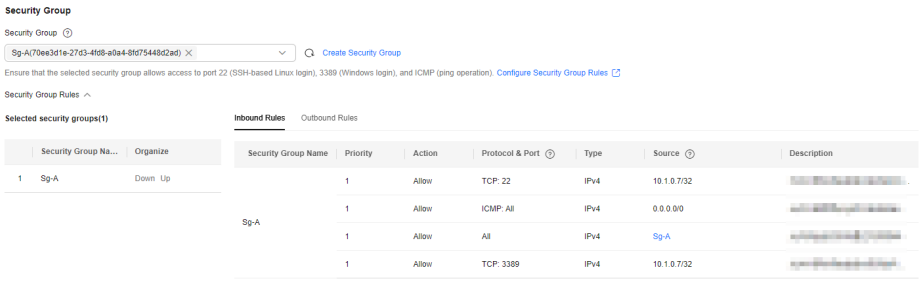
     

     Figure 1-6 The outbound rule of **Sg-A**

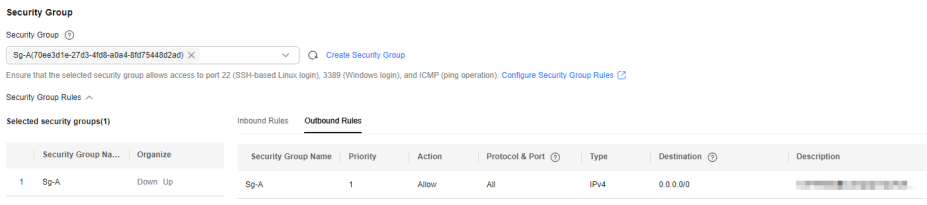
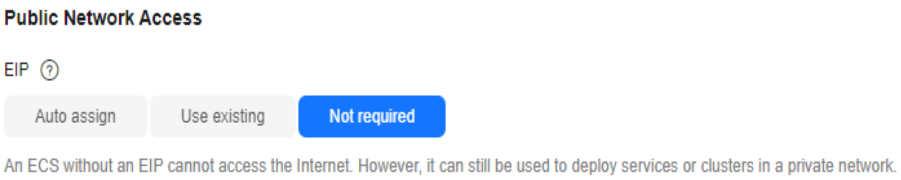
     

Table 1-3 Sg-A rules

Direction	Action	Type	Protocol & Port	Source/ Destination	Description
Inbound	Allow	IPv4	TCP: 22	Source: 10.1.0.7/32	Allows the local PC (10.1.0.7/32) to remotely log in to Linux **ECS-A01** over SSH port 22.
Inbound	Allow	IPv4	TCP: 3389	Source: 10.1.0.7/32	Allows the local PC (10.1.0.7/32) to remotely log in to Windows **ECS-A01** over RDP port 3389.
Inbound	Allow	IPv4	ICMP: All	Source: 0.0.0.0/0	Allows ping traffic to **ECS-A01** in **VPC-A** over all ICMP ports to test network connectivity.
Inbound	Allow	IPv4	All	Source: current security group (**Sg-A**)	Allows the ECSs in **Sg-A** to communicate with each other.
Outbound	Allow	IPv4	All	Destination: 0.0.0.0/0	Allows **ECS-A01** in **Sg-A** to access the Internet.

- **EIP**: Select **Not required**.

Figure 1-7 Selecting **Not required**



Configure other ECS parameters s as required. For details, see **Purchasing a Custom ECS**.

3. Click **Create**.

   Return to the ECS list to view **ECS-A01** you have bought.

Step 3: Buy an EIP and Bind It to ECS-A01

1. Go to the **Buy EIP** page.
2. On the **Buy EIP** page, set the EIP name to **EIP-A**.

   You can configure other EIP parameters as required. For details, see **Buying an EIP**.

3. Click **Next**.

   Return to the EIP list to view **EIP-A** you have assigned.

4. In the EIP list, locate **EIP-A** and click **Bind** in the **Operation** column.

   The **Bind EIP** dialog box is displayed.

5. In the displayed dialog box, select **ECS-A01** and click **OK**.

   Return to the EIP list. You can see that **ECS-A01** is displayed in the **Associated Instance** column in the EIP list.

Step 4: Test Network Connectivity

1. Use the local PC to remotely log in to **ECS-A01**.

   Multiple methods are available for logging in to an ECS. For details, see **Logging In to an ECS**.

2. Run the following command to test the network connectivity between **ECS-A01** and Internet:

   ping *IPv4 EIP or Domain name*

   Example command:

   ping support.huaweicloud.com

   If information similar to the following is displayed, **ECS-A01** can communicate with the Internet.

```
[root@ecs-a01 ~]# ping support.huaweicloud.com
PING hcdnw.cbg-notzj.c.cdnhwc2.com (203.193.226.103) 56(84) bytes of data.
64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=1 ttl=51 time=2.17 ms
64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=2 ttl=51 time=2.13 ms
64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=3 ttl=51 time=2.10 ms
64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=4 ttl=51 time=2.09 ms
...
--- hcdnw.cbg-notzj.c.cdnhwc2.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.092/2.119/2.165/0.063 ms
```

