NAT Gateway

Best Practices

Issue	01
Date	2021-01-26



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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 Working with SNAT to Access the Internet Outside China from the Private Network..... 1

2 Using NAT Gateway and Direct Connect to Accelerate Internet Access.....4

3 Using Private NAT Gateway and Direct Connect to Enable Communication Between a VPC and an On-premises Data Center..... 8

4 Using NAT Gateway and VPC Peering to Enable Communication Between VPCs and Internet..... 12

 Copyright © Huawei Technologies Co., Ltd.

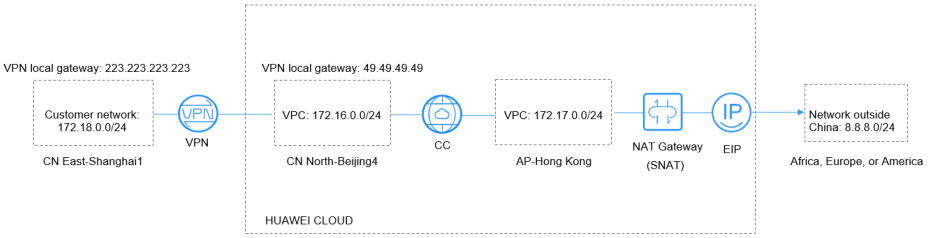
1 Working with SNAT to Access the Internet Outside China from the Private Network

Scenarios

This practice provides detailed operations for accessing the Internet outside China by using CC, VPN, and NAT Gateway.

Figure 1-1 shows the networking diagram.

Figure 1-1 Networking



NOTE

- In this practice, you can consider the VPC in CN East-Shanghai1 as the on-premises network.
- The network outside China is 8.8.8.0/24, and 8.8.8.8 is the only IP address for test.
- Your account must have permissions for cross-border network communication. If you do not have the permissions, you can authorize others to load the VPCs to a cloud connection.

Procedure

Step 1 Create VPCs.

For details, see **Creating a VPC**.

Ensure that the VPC CIDR blocks do not conflict with each other.

 Copyright © Huawei Technologies Co., Ltd.

- VPC in CN East-Shanghai1: 172.18.0.0/24
- VPC in CN North-Beijing4: 172.16.0.0/24
- VPC in AP-Hong Kong: 172.17.0.0/24

Step 2 Configure the VPN service.

Buy a VPN gateway and a VPN connection to connect networks in CN North-Beijing4 and CN East-Shanghai1.

For details, see **Buying a VPN Gateway** and **Buying a VPN Connection**.

- Gateway and subnet configuration for CN North-Beijing4:
  - Local subnets: 172.16.0.0/24, 172.17.0.0/24, and 8.8.8.0/24
  - Remote gateway: 223.223.223.223
  - Remote subnet: 172.18.0.0/24
- Gateway and subnet configuration for CN East-Shanghai1:
  - Local subnet: 172.18.0.0/24
  - Remote gateway: 49.49.49.49
  - Remote subnets: 172.16.0.0/24, 172.17.0.0/24, and 8.8.8.0/24

NOTE

When configuring the VPN connection between CN North-Beijing4 and CN East-Shanghai1, ensure that local subnets in CN North-Beijing4 and remote subnets in CN East-Shanghai1 contain the network outside China (8.8.8.0/24) so that this network can be pinged.

Step 3 Configure CC.

1. Create a cloud connection.

   For details, see **Creating a Cloud Connection**.
2. Load the VPCs.

   For details, see **Loading a Network Instance**.
3. Add custom CIDR blocks.

   For details, see **Adding a Custom CIDR block**.
   - Custom CIDR blocks for CN North-Beijing4: 172.18.0.0/24 and 172.16.0.0/24
   - Custom CIDR blocks for AP-Hong Kong: 172.17.0.0/24 and 8.8.8.0/24

   NOTE

   To enable communications among all nodes, you need to add all local subnets.
4. Buy a bandwidth package.

   The default inter-region bandwidth of a cloud connection is 10 kbit/s, which is used for testing connectivity only.

   For details, see **Buying a Bandwidth Package**.
5. Configure an inter-region bandwidth.

   For details, see **Configuring an Inter-Region Bandwidth**.

Step 4 Buy an ECS in CN North-Beijing4, CN East-Shanghai1, and AP-Hong Kong, respectively.

For details, see **Purchasing an ECS**.

 Copyright © Huawei Technologies Co., Ltd.

- Private IP address of the ECS in CN North-Beijing4: 172.16.0.3
- Private IP address of the ECS in CN East-Shanghai1: 172.18.0.3
- Private IP address of the ECS in AP-Hong Kong: 172.17.0.3

Step 5 Buy an EIP and configure a NAT gateway.

Buy an EIP in the AP-Hong Kong region, buy a NAT gateway, and create SNAT rules that include the following CIDR blocks:

For details, see **Assigning an EIP and Binding It to an ECS** and **Adding an SNAT Rule**.

- VPC CIDR block: 172.17.0.0/24
- Direct Connect/CC CIDR block: 172.18.0.0/24
- Direct Connect/CC CIDR block: 172.16.0.0/24

NOTE

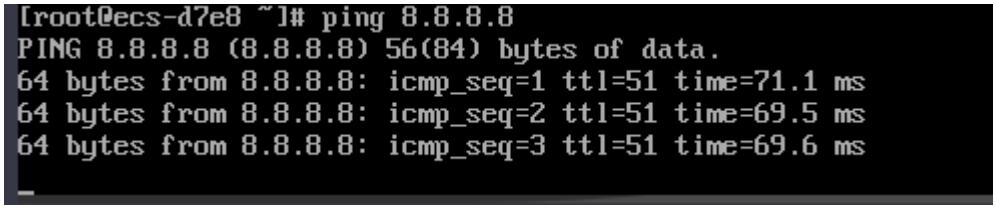
SNAT rules are to access to the Internet and ping the network outside China (8.8.8.0/24).

----End

Verification

After the configuration is complete, test the network connectivity.

Ping the gateway (8.8.8.8) from the ECS in CN East-Shanghai1.



 Copyright © Huawei Technologies Co., Ltd.

2 Using NAT Gateway and Direct Connect to Accelerate Internet Access

Scenarios

You need to connect your data center to HUAWEI CLOUD using Direct Connect and then configure SNAT rules of a NAT gateway to enable servers to access the Internet in a secure, reliable, and high-speed way, or configure DNAT rules to enable servers to provide services accessible from the Internet. Similar scenarios include Internet, games, e-commerce, and finance.

Solution Advantages

With Direct Connect, you can access a VPC on HUAWEI CLOUD with high-performance, low-latency, and secure networks. A Direct Connect connection supports a maximum of 10 Gbit/s bandwidth, meeting various bandwidth requirements.

With the SNAT and DNAT functions of the NAT gateway, multiple servers can share an EIP, effectively reducing costs. The NAT gateway specifications and bound EIPs can be adjusted at any time. The configuration is simple and will take effect immediately.

Typical Topology

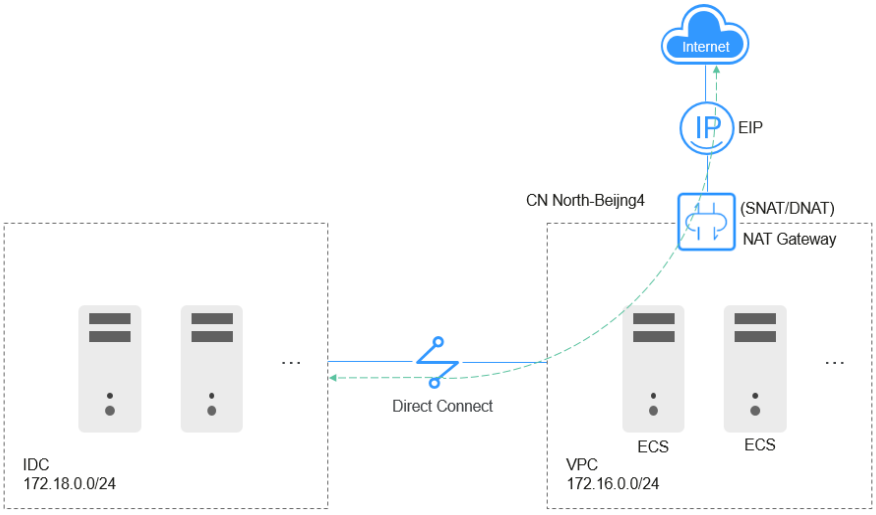
Assume that the network of your IDC is 172.18.0.0/24, the region of the VPC is **CN North-Beijng4**, and the VPC subnet is 172.16.0.0/24.

Implementation methods:

1. Use Direct Connect to connect your IDC to your VPC.
2. Create a NAT gateway in the VPC to connect to the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 Network topology



Prerequisites

- The default route of the IDC is available for configuring Direct Connect.
- The network CIDR block of the IDC does not overlap with the subnet CIDR block of the VPC on the cloud. Otherwise, the communication between the IDC and the VPC will fail.

Configuration Procedure

Step 1 Create VPCs.

For details, see **Creating a VPC**.

Step 2 Configure a Direct Connect connection.

Create a Direct Connect connection between the IDC and the cloud (**CN North-Beijing4** region). For details, see **Process Description**.

NOTE

When creating a Direct Connect connection, add the 0.0.0.0/0 CIDR block as the local subnet on the cloud when configuring the route.

- **Static**: Add the default route with 0.0.0.0/0 as the destination in the on-premises data center and set the next hop to the connection.
- **BGP**: The on-premises network can learn the default route using BGP.

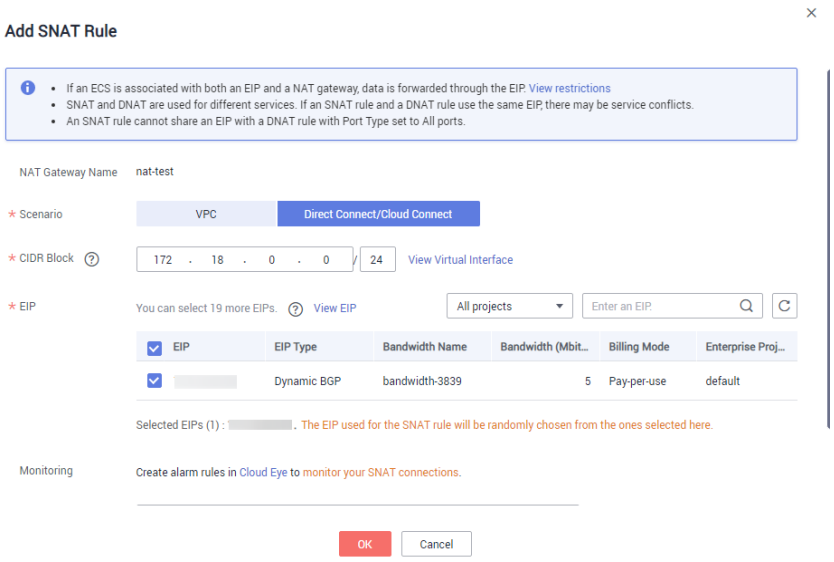
Step 3 Buy an EIP and configure a NAT gateway.

1. Buy an EIP in the **CN North-Beijing4** region. For details, see **Assigning an EIP**.
2. Buy a NAT gateway. For details, see **Buying a NAT Gateway**.
3. Add an SNAT rule with the CIDR block set to that of the Direct Connect connection. For details, see **Adding an SNAT Rule**.

   Set **CIDR Block** to 172.18.0.0/24 and select an EIP.

 Copyright © Huawei Technologies Co., Ltd.

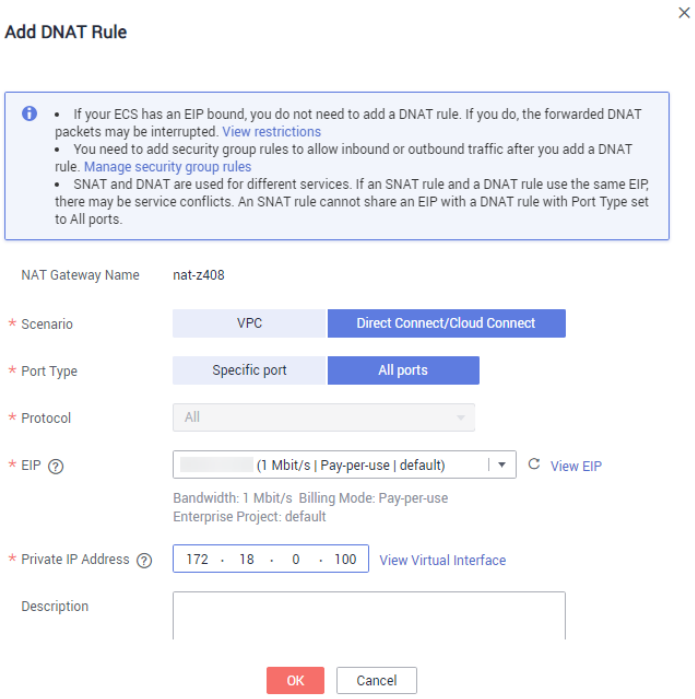
Figure 2-2 Add SNAT Rule



4. Add a DNAT rule. For details, see **Adding a DNAT Rule**.

   Configure the protocol and port type. **All ports** is used as an example. Set **Private IP Address** to 172.18.0.100 and select an EIP.

Figure 2-3 Add DNAT Rule



NOTE

SNAT and DNAT are used for different services. If an SNAT rule and a DNAT rule use the same EIP, there may be service conflicts. An SNAT rule cannot share an EIP with a DNAT rule with **Port Type** set to **All ports**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Configuration Verification

After the configuration is complete, test the network connectivity.

Ping an external IP address, for example, 114.114.114.114, from a server in the IDC.

 Copyright © Huawei Technologies Co., Ltd.

3 Using Private NAT Gateway and Direct Connect to Enable Communication Between a VPC and an On-premises Data Center

Scenarios

The following diagram shows that ECSs in a VPC communicate with an on-premises IDC using Direct Connect and a private NAT gateway.

NOTE

The following configuration is used as an example.

Solution Advantages

In the hybrid cloud scenario, you need to specify a private IP address for compute instances in a VPC to communicate with the on-premises network that meets security compliance requirements.

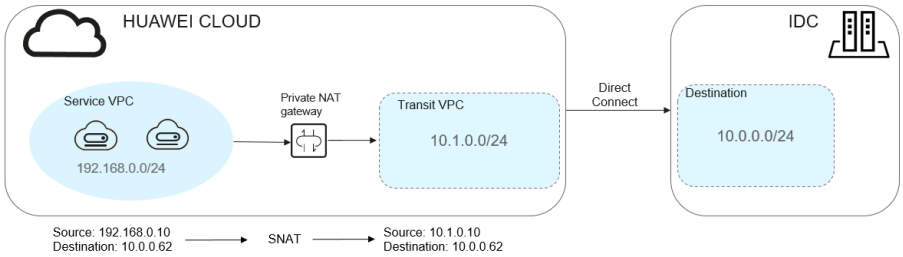
Typical Topology

Assume that the CIDR block of the IDC is 10.0.0.0/24 and the subnet of the transit VPC in the region **CN North-Beijing4** is 10.1.0.0/24.

Implementation methods:

1. Connect the transit VPC to the IDC using Direct Connect (VPC Peering is used in the test environment where Direct Connect is unavailable).
2. Create a private NAT gateway to connect the service VPC to the transit VPC.

Figure 3-1 Network topology



 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- The network CIDR block of the IDC does not overlap with the subnet CIDR block of the transit VPC on the cloud. Otherwise, the communication between the IDC and the transit VPC will fail.
- You have determined the private CIDR block in the transit VPC for performing NAT for resources in the service VPC.

Procedure

Step 1 Create a service VPC and a transit VPC.

For details, see **Creating a VPC**.

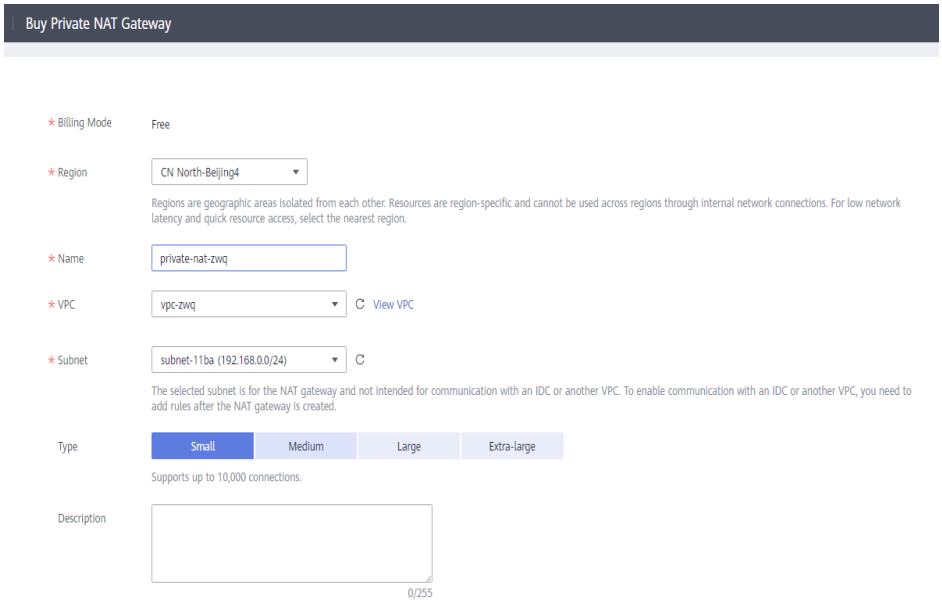
Step 2 Create a Direct Connect connection.

Create a Direct Connect connection between the IDC and the cloud (**CN North-Beijing4** region). For details, see **Direct Connect User Guide**.

Step 3 Create and configure a private NAT gateway.

1. Create a private NAT gateway in the **CN North-Beijing4** region and select the service VPC.

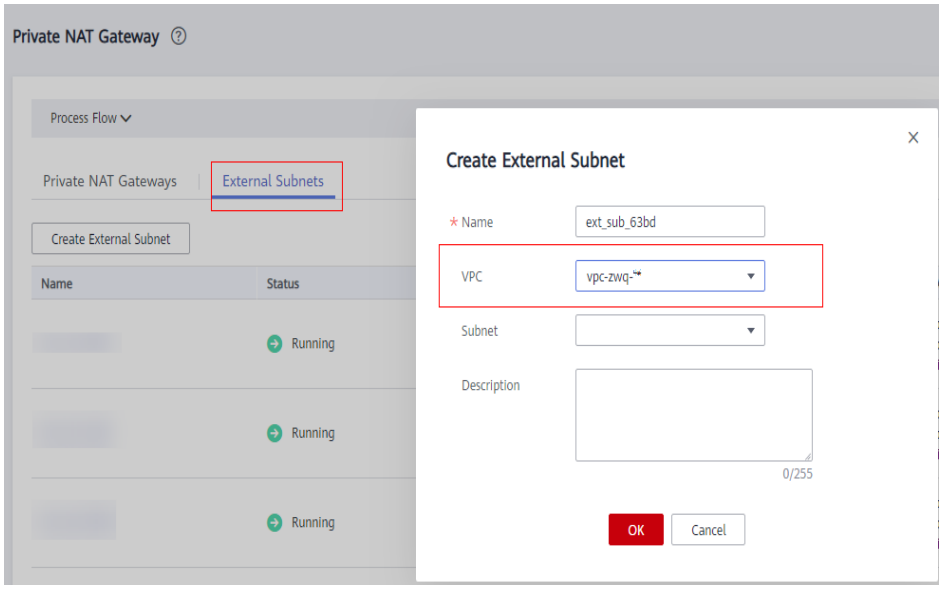
   Figure 3-2 Buy Private NAT Gateway

2. Create an external subnet in the transit VPC.

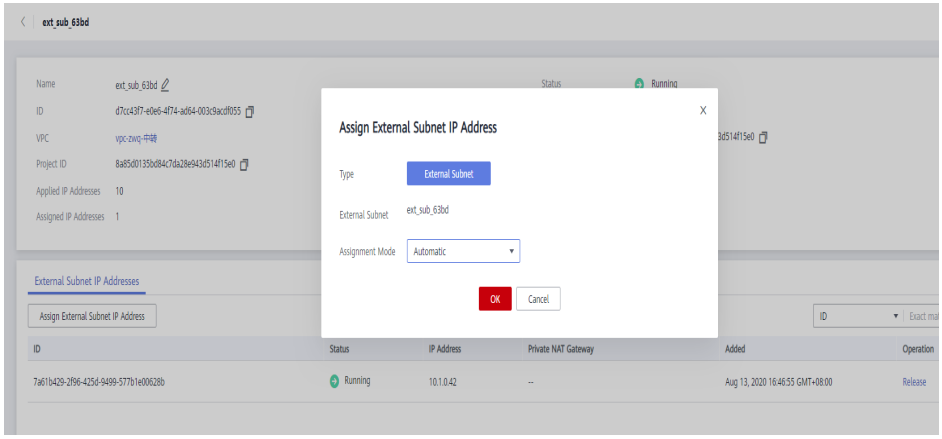
 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 Create External Subnet



3. Click the created external subnet and assign an IP address from it.

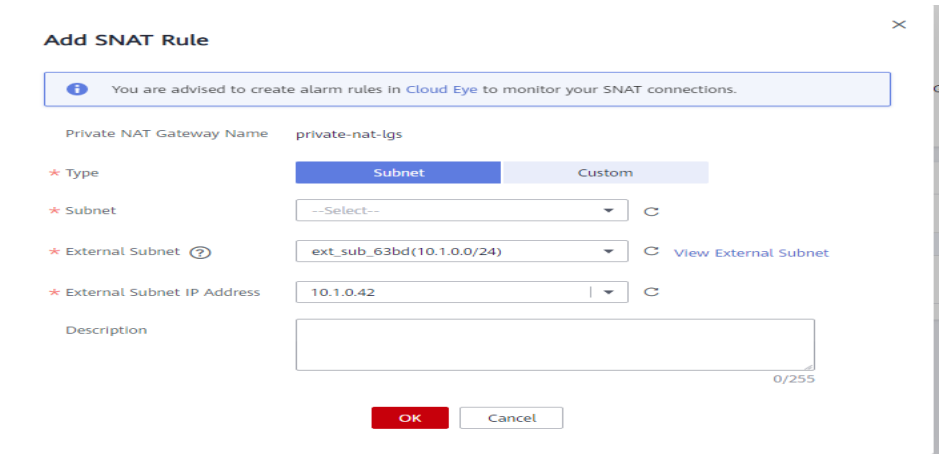
Figure 3-4 Assign External Subnet IP Address



4. In the private NAT gateway list, click the created NAT gateway name, and add an SNAT rule. Set **Subnet** to the subnet in which the address mapping needs to be performed in the service VPC, and set **External Subnet** and **External Subnet IP Address** to those created in the previous step.

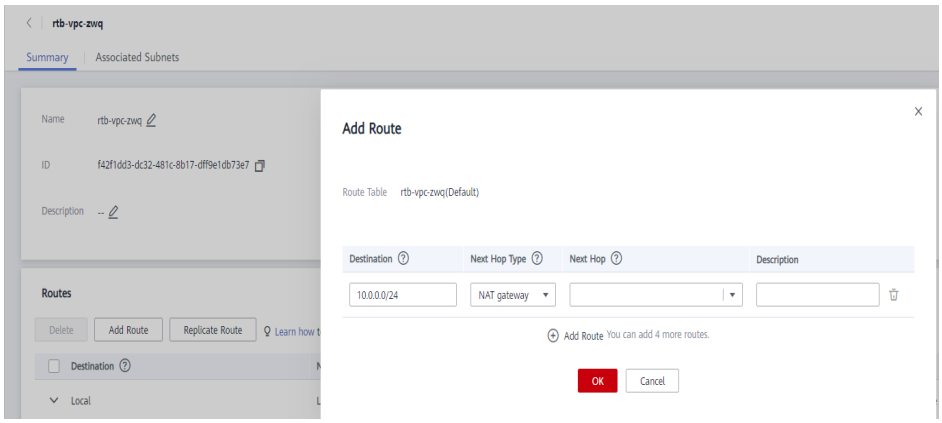
 Copyright © Huawei Technologies Co., Ltd.

Figure 3-5 Add SNAT Rule



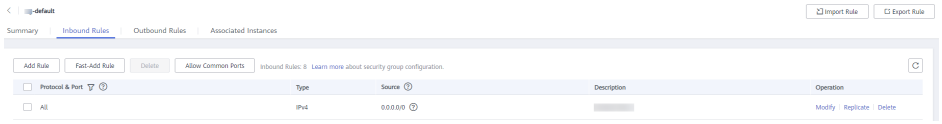
5. Add a route pointing to the private NAT gateway for the service VPC and set the destination to the private CIDR block of the IDC.

Figure 3-6 Adding a route



6. Add an inbound security group rule to allow traffic to the destination.

Figure 3-7 Adding an inbound security group rule



----End

Verification

After the configuration is complete, test the network connectivity.

Log in to the ECS in the service VPC and ping the private IP address of the IDC.

```
[root@ecs-zwq ~]# ping 10.0.0.62
PING 10.0.0.62 (10.0.0.62) 56(84) bytes of data.
64 bytes from 10.0.0.62: icmp_seq=1 ttl=64 time=1.08 ms
64 bytes from 10.0.0.62: icmp_seq=2 ttl=64 time=0.507 ms
64 bytes from 10.0.0.62: icmp_seq=3 ttl=64 time=0.455 ms
```

 Copyright © Huawei Technologies Co., Ltd.

4 Using NAT Gateway and VPC Peering to Enable Communication Between VPCs and Internet

Scenarios

VPC A and VPC B are in the same region. A NAT gateway is configured for subnet A in VPC A and you can add SNAT and DNAT rules to enable communication with the Internet. Subnet B connects to the subnet A through a VPC peering connection and uses the NAT gateway of subnet A to communicate with the Internet.

Solution Advantages

Only one NAT gateway needs to be configured. Servers in the two VPCs can communicate with the Internet through the same NAT gateway, saving resources.

Typical Topology

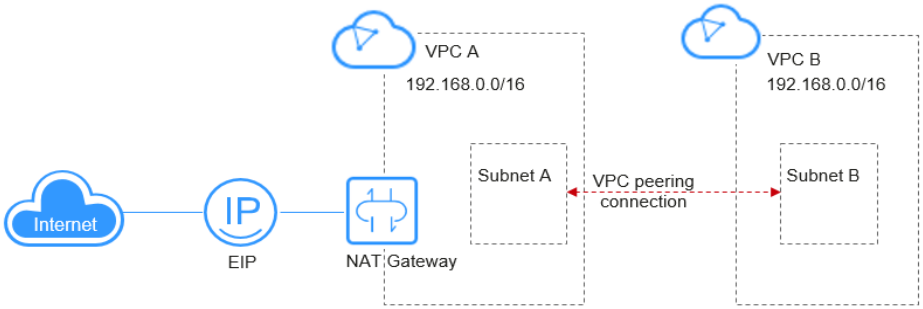
The CIDR block of VPC A is 192.168.0.0/16 and that of subnet A is 192.168.1.0/24. The CIDR block of VPC B is 192.168.0.0/16 and that of subnet B is 192.168.2.0/24.

Implementation methods:

1. Use a VPC peering connection to connect subnet A in VPC A to subnet B in VPC B.
2. Create a NAT gateway in VPC A. Then subnet B can use the NAT gateway to communicate the Internet.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 Network topology



Prerequisites

- If VPCs connected by a VPC peering connection have overlapping CIDR blocks, the connection can only enable communication between specific (non-overlapping) subnets in the VPCs.
- The subnets of the two VPCs do not overlap with each other.

Procedure

Step 1 Create VPC A, VPC B, subnet A, and subnet B.

For details, see **Creating a VPC**.

Step 2 Create a VPC peering connection.

Create a VPC peering connection between subnet A and subnet B. For details, see **Creating a VPC Peering Connection with Another VPC in Your Account**.

NOTE

The local VPC is VPC A, and the peer VPC is VPC B.

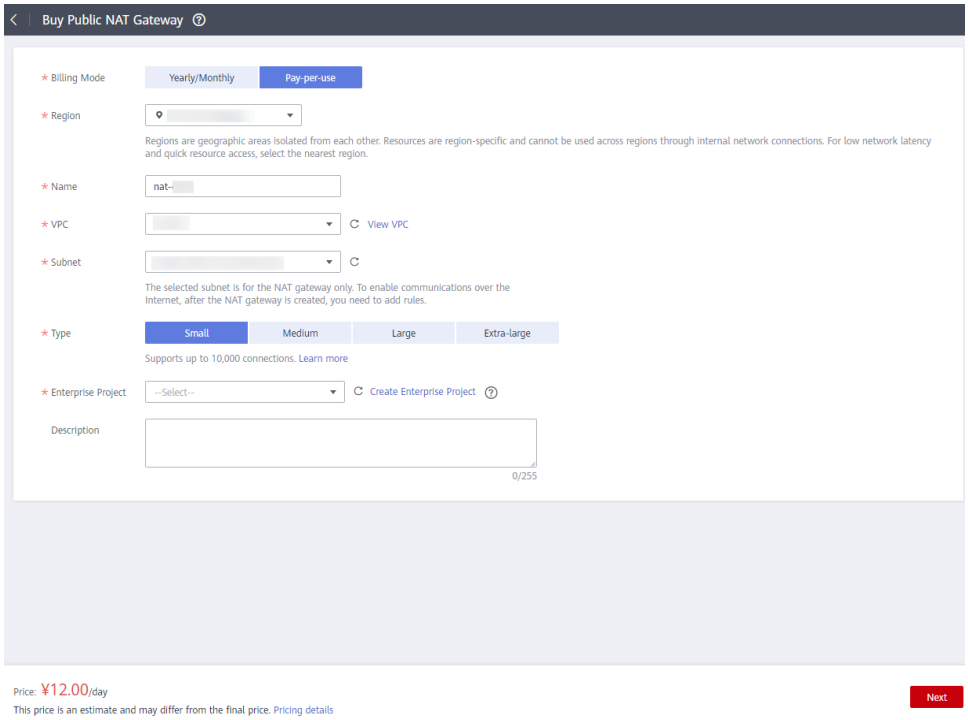
In addition to the local and peer routes, you need to add another peer route with destination set to 0.0.0.0/0.

Step 3 Buy a public NAT gateway.

Buy a public network NAT gateway with **VPC** set to VPC A. For details, see **Buying a Public NAT Gateway**.

 Copyright © Huawei Technologies Co., Ltd.

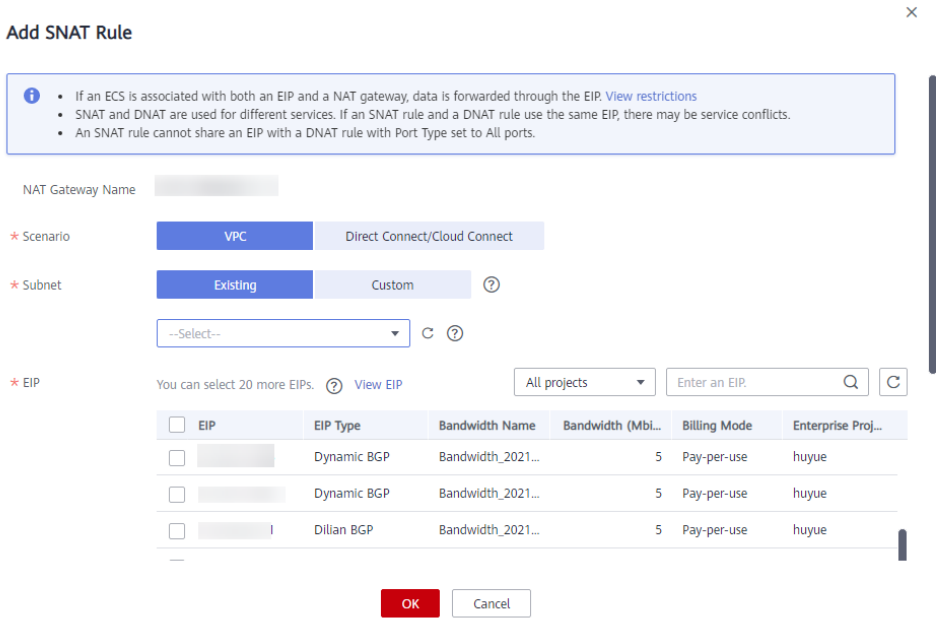
Figure 4-2 Buy Public NAT Gateway



Step 4 Add an SNAT rule.

1. Select **VPC** for **Scenario** and subnet A for **Subnet**. For details, see **Adding an SNAT Rule**.

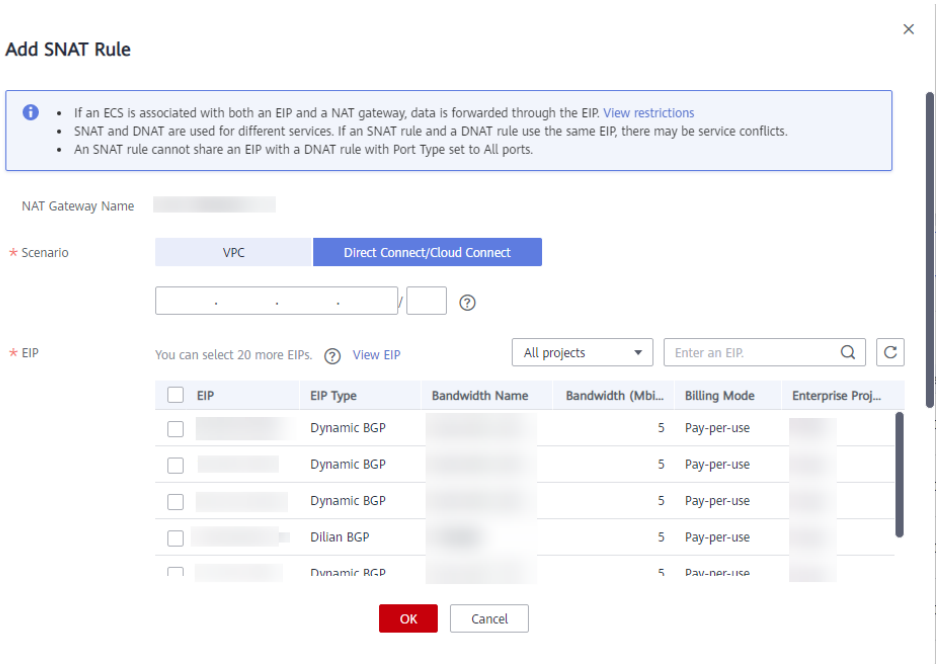
   Figure 4-3 Add SNAT Rule



2. Add an SNAT rule for subnet B. Set **Scenario** to **Direct Connect/Cloud Connect** and enter the CIDR block of subnet B.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-4 Add SNAT Rule

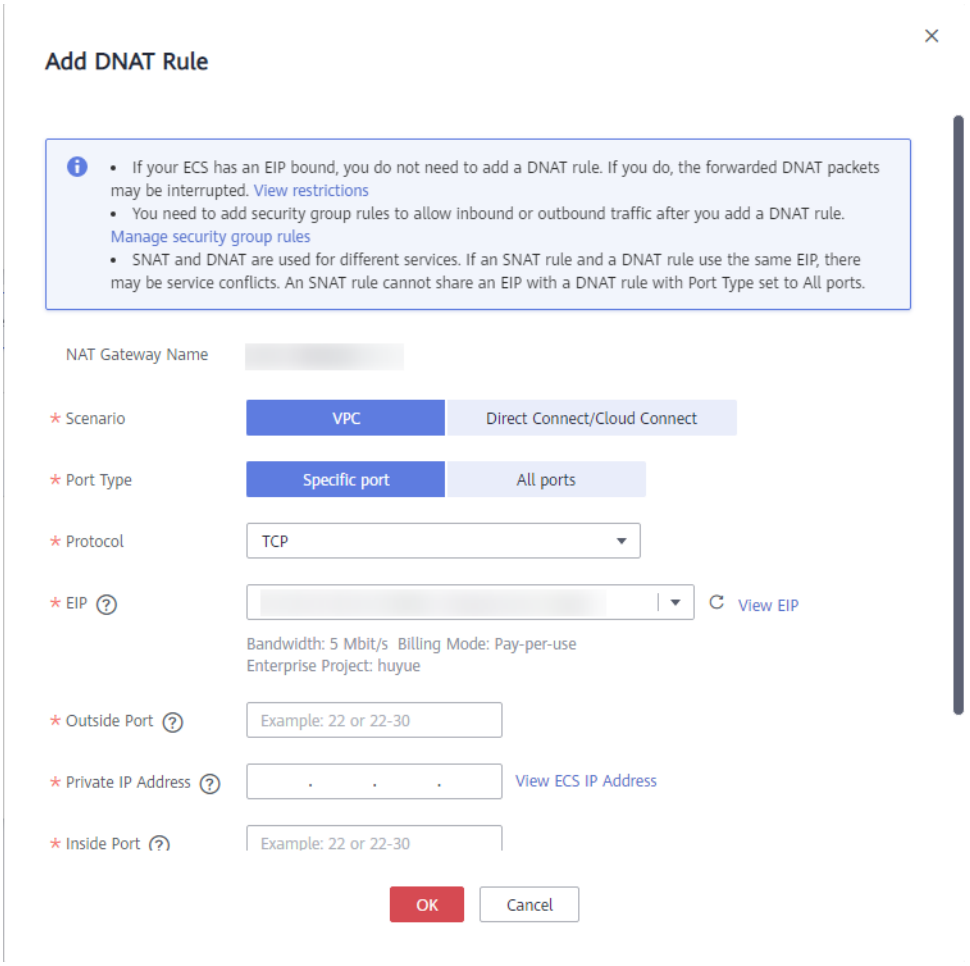


Step 5 Add a DNAT rule.

1. Add a DNAT rule for subnet A. Set **Scenario** to **VPC** and enter the IP address of the server in subnet A for **Private IP Address**. For details, see **Adding a DNAT Rule**.

 Copyright © Huawei Technologies Co., Ltd.

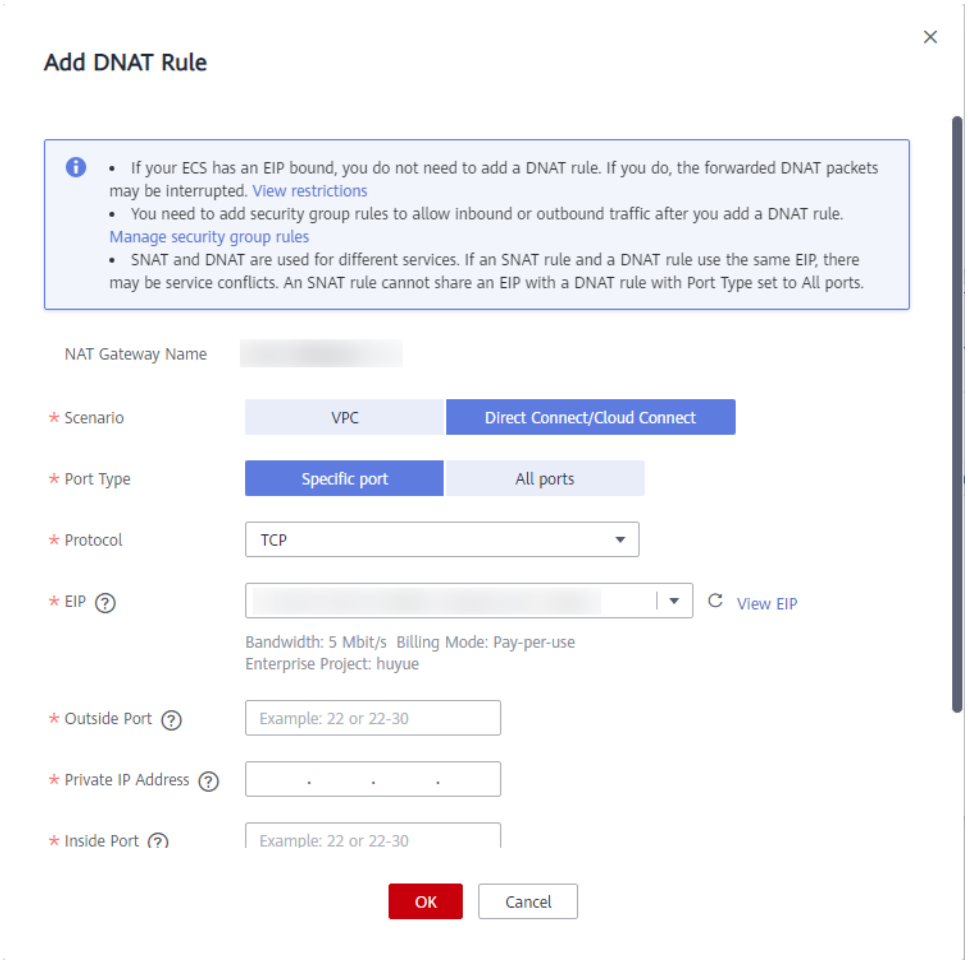
Figure 4-5 Add DNAT Rule



2. Add a DNAT rule for subnet B. Set **Scenario** to **Direct Connect/Cloud Connect** and enter the CIDR block of subnet B for **Private IP Address**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-6 Add DNAT Rule



----End

Verification

After the configuration is complete, test the network connectivity.

Log in to a server in subnet B to ping a public IP address.

```
[root@ecs-2670 ~]# ping www.baidu.com
PING www.a.shifen.com (14.215.177.39) 56(84) bytes of data.
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=1 ttl=54 time=5.74 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=2 ttl=54 time=5.44 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=3 ttl=54 time=5.33 ms
^C
--- www.a.shifen.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 5.332/5.507/5.742/0.182 ms
```

Log in to a server that does not belong to VPC A and VPC B. Use the curl command to check whether subnet B can communicate with the Internet through the DNAT rule with EIP associated.

 Copyright © Huawei Technologies Co., Ltd.

```
[root@ecs-cf5f ~]# curl
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
</ul>
<hr>
</body>
</html>
[root@ecs-cf5f ~]# curl
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
</ul>
<hr>
</body>
</html>
[root@ecs-cf5f ~]#
```

 Copyright © Huawei Technologies Co., Ltd.