NAT Gateway

Best Practices

Issue	01
Date	2022-08-30

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 Using a Public NAT Gateway and Direct Connect to Accelerate Internet Access

Scenarios

You need to connect your on-premises data center to Huawei Cloud using Direct Connect and then add SNAT rules to enable your on-premises servers to access the Internet through a public NAT gateway in a secure, reliable, and high-speed way, or add DNAT rules to enable your on-premises servers to provide services accessible from the Internet. This practice can be used in similar scenarios like Internet, games, e-commerce, and finance.

Solution Advantages

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

With SNAT and DNAT of the public NAT gateway, your servers can share an EIP for Internet access, saving costs on EIPs. You can change the public NAT gateway types and EIPs bound to it at any time. The configuration is simple and will take effect immediately.

Typical Topology

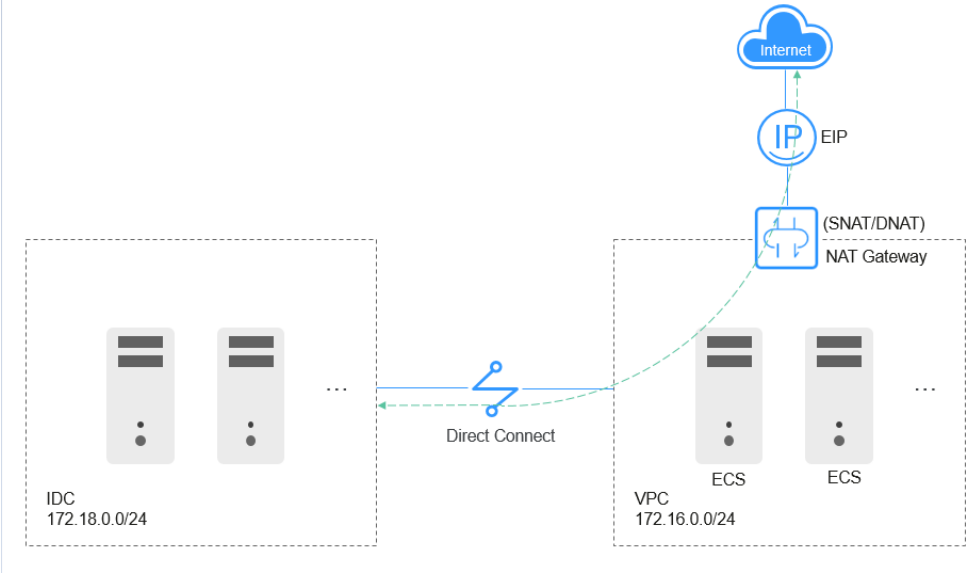
The network of your on-premises data center is 172.18.0.0/24.

The subnet of the VPC your on-premises data center will access is 172.16.0.0/24.

Implementation methods:

1. A Direct Connect connection is used to connect your on-premises data center to the VPC.
2. A public NAT gateway is created in the VPC, enabling Internet connectivity for your on-premises servers.

Figure 1-1 Network topology



Prerequisites

- The default route of your on-premises data center is available for configuring Direct Connect.
- The CIDR block of your on-premises data center does not overlap with the subnet CIDR block of the VPC. Otherwise, the communications between your on-premises data center and the VPC will fail.

Procedure

Step 1 Create a VPC.

For detailed operations, see **Creating a VPC**.

Step 2 Configure a Direct Connect connection.

Create a direct connection between your on-premises data center and the transit VPC (in the specified region). For details, see **Overview**.

NOTE

After the Direct Connect connection is created, configure routes in your on-premises data center as follows:

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

Step 3 Assign an EIP and configure a public NAT gateway.

1. Buy an EIP in the specified region. For details, see **Assigning an EIP**.
2. Create a public NAT gateway. For details, see **Creating a Public NAT Gateway**.
3. Add an SNAT rule by setting the CIDR block to that of the Direct Connect connection. For more details, see **Adding an SNAT Rule**.

   Set **CIDR Block** to **172.18.0.0/24** and select the EIP assigned in **1**.

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

   Configure the protocol and port type. Set **Private IP Address** to **172.18.0.100** and select an EIP.

   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

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 your on-premises data center.

2 Using Public NAT Gateway and VPC Peering to Enable Communication Between VPCs and the Internet

Scenarios

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

Solution Advantages

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

Typical Topology

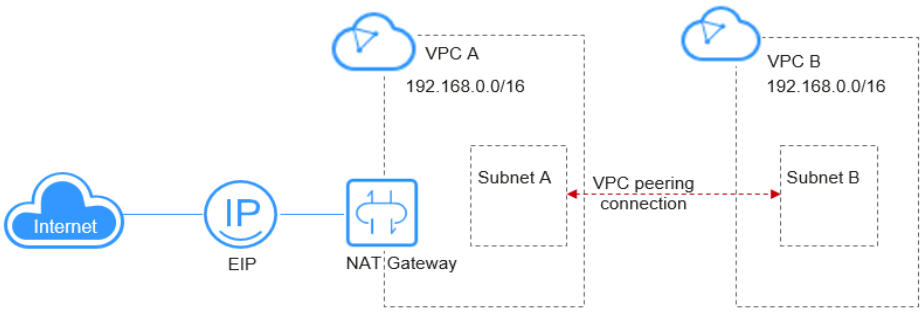
The CIDR block of VPC A is 192.168.0.0/16 and that of subnet A is 192.168.1.0/24.

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. A VPC peering connection is used to connect subnet A in VPC A to subnet B in VPC B.
2. A public NAT gateway is created in VPC A, and subnet B can use the public NAT gateway to communicate the Internet.

Figure 2-1 Network topology



Prerequisites

- If VPCs connected by a VPC peering connection have overlapping CIDR blocks, the connection can only enable communications between specific (non-overlapping) subnets in the VPCs.
- All 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 detailed operations, see **Creating a VPC**.

Step 2 Create a VPC peering connection.

Create a VPC peering connection between subnet A and subnet B. For detailed operations, 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.

Add a route in the route table of VPC B. Set **Destination** to **0.0.0.0/0** and **Next Hop** to the created VPC peering connection between VPC A and VPC B.

Step 3 Buy a public NAT gateway.

Buy a public NAT gateway with **VPC** set to VPC A. For details about how to configure other parameters, see **Creating a Public NAT Gateway**.

Step 4 Add an SNAT rule.

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

Step 5 Add a DNAT rule.

1. Add a DNAT rule for subnet A. Select **VPC** for **Scenario** and enter an IP address of a server in subnet A for **Private IP Address**. For details about how to configure other parameters, see **Adding a DNAT Rule**.

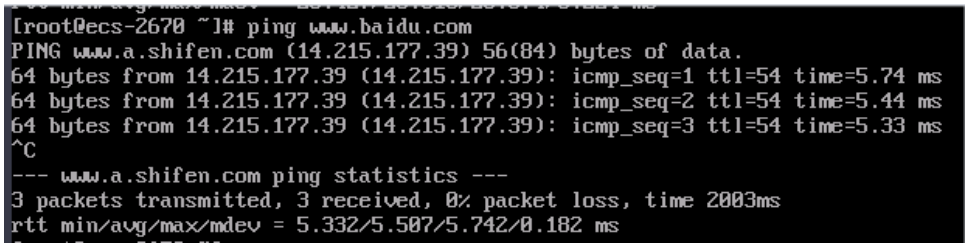
2. Add a DNAT rule for subnet B. Set **Scenario** to **Direct Connect/Cloud Connect** and enter the CIDR block of subnet B for **Private IP Address**.

----End

Verification

After the configuration is complete, test the network connectivity.

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



Log in to a server that can access the Internet and is not deployed in VPC A or VPC B. Use **curl** to check whether the server can communicate with subnet B via the EIP associated with the DNAT rule configured for subnet B.


```
[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 ~]#
```

