NAT Gateway

# Best Practices

| | |
|---|---|
| **Issue** | 01 |
| **Date** | 2026-06-24 |

HUAWEI

**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.

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

## Scenarios

You can add SNAT or DNAT rules to a public NAT gateway to enable a large number of on-premises servers connected to a VPC using Direct Connect to access the Internet or provide services accessible from the Internet, in a secure, reliable, and high-speed manner. This practice can be used in similar scenarios across sectors like Internet, gaming, e-commerce, and finance.

## Solution Advantages

With Direct Connect, you can access a VPC on Huawei Cloud over high-performance, low-latency, and secure networks. A Direct Connect connection supports up to 10 Gbit/s of bandwidth, meeting your service 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 type of the public NAT gateway and EIPs bound to it at any time. The configuration is simple and will take effect immediately.

## Typical Topology

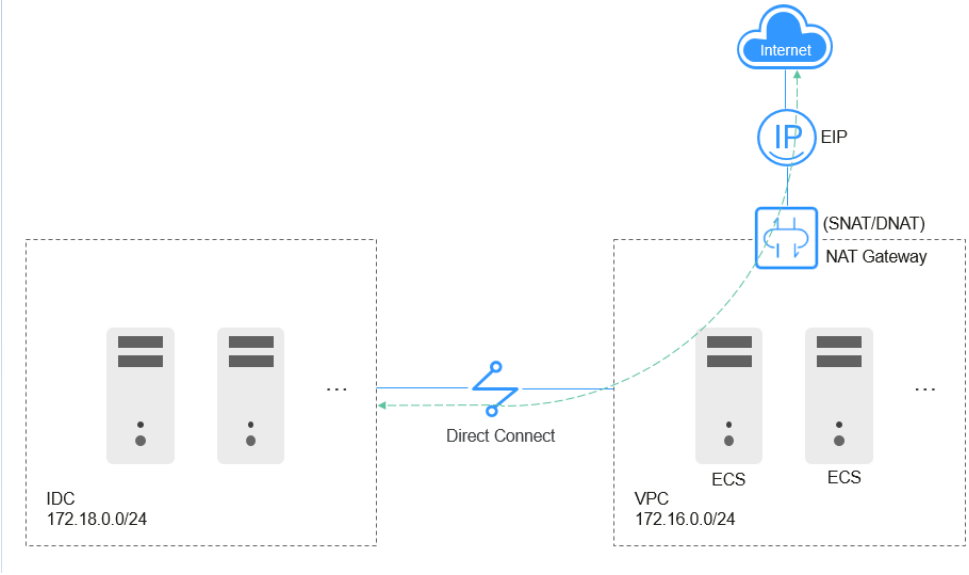
The CIDR block of your on-premises data center is 172.18.0.0/24, which will access the VPC. The CIDR block of the VPC is 172.16.0.0/24.

Implementation procedure:

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

**Figure 1-1** Networking diagram




## 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 cannot overlap with that of the VPC; otherwise, the communications between your on-premises data center and the VPC will fail.

## Procedure

**Step 1** **Create a VPC with a subnet.**

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

**Step 2** Configure a Direct Connect connection.

Create a Direct Connect connection between your on-premises data center and the VPC (in the specified region). For details, see .

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 Direct Connect connection.
- **BGP**: The on-premises network can learn the default route using BGP.

**Step 3** Buy an EIP and configure a public NAT gateway.

1. Buy an EIP in the specified region. For details, see **Assigning an EIP**.
2. Buy a public NAT gateway. For details about how to configure other parameters, see **Creating a Public NAT Gateway**.
3. Add an SNAT rule and set the CIDR block to that of the Direct Connect connection. For more details, see **Adding an SNAT Rule**.

   Set the CIDR block to **172.18.0.0/24** and select the EIP assigned in step **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 rules 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

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 a Public NAT Gateway and VPC Peering to Enable Communications Between VPCs and the Internet

## Scenarios

There are two VPCs in the same region: VPC A and VPC B. VPC A has a subnet (**subnet A**), and VPC B has a subnet (**subnet B**). You can create a public NAT gateway in subnet A, and add SNAT and DNAT rules to enable servers in subnet A to access and be accessed from the Internet. Then you can create a VPC peering connection to connect subnet B in VPC B to subnet A in VPC A. In this way, servers in subnet B can use the public NAT gateway in subnet A to access and be accessed from the Internet. You do not need to configure another public NAT gateway for subnet B.

## Solution Advantages

Only one public NAT gateway needs to be configured. Servers in the two VPCs can use 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 procedure:

1. Create a NAT gateway in VPC A, and add SNAT and DNAT rules.
2. Create a VPC peering connection between subnet A and subnet B, enabling servers in subnet B to use the public NAT gateway in subnet A to access and be accessed from the Internet.

## 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.

- At least one pair of subnets in the two VPCs does not have overlapping CIDR blocks.

## Configuring a Public NAT Gateway

**Step 1** Buy a public NAT gateway.

Select VPC A for **VPC**. For details about how to configure other parameters, see **Creating a Public NAT Gateway**.

**Step 2** Add SNAT rules.

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 3** Add DNAT rules.

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 more details, see **Adding a DNAT Rule**.
2. Add a DNAT rule for subnet B. Set **Scenario** to **Direct Connect/Cloud Connect** and enter an IP address of a server in subnet B for **Private IP Address**.

**----End**

## Creating a VPC Peering Connection

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

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

**Step 2** Create a VPC peering connection between subnet A and subnet B.

For detailed operations, see **Creating a VPC Peering Connection to Connect Two VPCs in the Same Account**.

NOTE

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

In addition to the existing local and peer routes, you also need to add a route to the route table of VPC B. Set **Destination** to **0.0.0.0/0** and **Next Hop** to the VPC peering connection between VPC A and VPC B.

**----End**

## Testing Network Connectivity

Test the network connectivity.

Log in to a server in subnet B and ping its EIP. If the following information is displayed, the network is connected.

```
[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 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. If the following information is displayed, the network is connected.

```
[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 ~]#
```

# 3 Using an Enterprise Router to Enable Multiple VPCs to Share a NAT Gateway

You can use an enterprise router to enable multiple VPCs to share a NAT gateway. This allows you to use the NAT gateway to control outbound traffic more efficiently, reduce resource overhead, and simplify network management.

For details, see **Allowing VPCs to Share an EIP to Access the Internet Using Enterprise Router and NAT Gateway**.