

NAT Gateway

Getting Started

Issue 01
Date 2024-10-12



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property 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 Cloud 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 to Enable Servers to Share One or More EIPs to Access the Internet.....	1
2 Using a Public NAT Gateway to Enable Servers to Be Accessed by the Internet....	6
3 Using a Private NAT Gateway to Connect Cloud and On-premises Networks.....	13
4 Using Multiple Public NAT Gateways Together in Performance-Demanding Scenarios.....	20
4.1 Overview.....	20
4.2 Step 1: Create a VPC and Two Subnets.....	22
4.3 Step 2: Buy a Public NAT Gateway.....	22
4.4 Step 3: Check the Default Route.....	24
4.5 Step 4: Create a Route Table.....	24
4.6 Step 5: Buy Another Public NAT Gateway.....	25
4.7 Step 6: Add the Default Route.....	27

1 Using a Public NAT Gateway to Enable Servers to Share One or More EIPs to Access the Internet

Scenarios

If servers without EIPs need to access the Internet, they can share one or more EIPs to access the Internet through a public NAT gateway. This helps save EIP resources and protect servers from exposing their IP addresses.

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: Buy an EIP	Buy an EIP.
Step 2: Buy a Public NAT Gateway	Buy a public NAT gateway.
Step 3: Add an SNAT Rule	Add an SNAT rule for the public NAT gateway so that servers in specific CIDR blocks share the EIP you have assigned to access the Internet.
Step 4: Verify that the SNAT Rule Has Been Added	Check whether the SNAT rule has been added.
Step 5: Verify that Server Can Access the Internet Through the NAT Gateway	Verify that server in the CIDR block to which the SNAT rule is applied can access the Internet.

Preparations

Before using NAT gateways, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account.

- [Create a HUAWEI ID and enable Huawei Cloud services.](#)
- [Complete real-name authentication.](#)
- [Top up your account.](#)

Step 1: Buy an EIP

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.

Step 2: Buy a Public NAT Gateway

1. Go to the [Buy Public NAT Gateway](#) page.
2. On the **Buy Public NAT Gateway** page, configure required parameters.

Table 1-1 Descriptions of public NAT gateway parameters

Parameter	Example	Description
Region	CN North-Beijing4	The region where the public NAT gateway is located.
Billing Mode	Pay-per-use	The billing mode of the public NAT gateway.
Specifications	Small	The specifications of the public NAT gateway. The value can be Extra-large , Large , Medium , or Small . To view more details about specifications, click Learn more on the page.
Name	public-nat-01	The name of the public NAT gateway. Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.

Parameter	Example	Description
VPC	vpc-A	<p>The VPC that the public NAT gateway belongs to.</p> <p>The selected VPC cannot be changed after you buy the public NAT gateway.</p> <p>NOTE</p> <p>To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you buy a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you buy the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.</p>
Subnet	Subnet-A01	<p>The subnet that the public NAT gateway belongs to.</p> <p>The subnet must have at least one available IP address.</p> <p>The selected subnet cannot be changed after you buy the public NAT gateway.</p> <p>The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.</p>
Advanced Settings (Optional)	-	Click the drop-down arrow to configure advanced parameters of the public NAT gateway.
SNAT Connection TCP Timeout (s)	900	<p>The timeout period of a TCP connection established using the SNAT rule. If no data is exchanged within this period, the TCP connection will be closed.</p> <p>Value range: 40 to 7200</p>
SNAT Connection UDP Timeout (s)	300	<p>The timeout period of a UDP connection established using the SNAT rule. If no data is exchanged within this period, the UDP connection will be closed.</p> <p>Value range: 40 to 7200</p>

Parameter	Example	Description
SNAT Connection ICMP Timeout (s)	10	The timeout period of an ICMP connection established using the SNAT rule. If no data is exchanged within this period, the ICMP connection will be closed. Value range: 10 to 7200
TCP TIME_WAIT (s)	5	How long the side that actively closed the TCP connection is in the TIME_WAIT state. Value range: 0 to 1800
Description	Not required	Supplementary information about the public NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.
Tag	Not required	The identifier of the public NAT gateway. A tag is a key-value pair. You can add up to 20 tags to each public NAT gateway.

3. Click **Next**. On the page displayed, confirm the public NAT gateway specifications.
4. If you do not need to modify the information, click **Submit**.

On the **Public NAT Gateways** page, you can view the created public NAT gateway in the list.

Step 3: Add an SNAT Rule

1. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
2. On the **SNAT Rules** tab, click **Add SNAT Rule**.
3. Configure required parameters. [Table 1-2](#) describes the parameters.

Table 1-2 Descriptions of SNAT rule parameters

Parameter	Example	Description
Scenario	VPC	Select VPC if your servers in a VPC will use the SNAT rule to access the Internet. Different servers in a VPC can share the same EIP to access the Internet.
CIDR Block	Existing	The CIDR block is a subset of the NAT gateway's VPC subnets. Servers whose IP addresses in the CIDR block can access the Internet through the SNAT rule. Select a CIDR block from the drop-down list.
Public IP Address Type	EIP	The EIP used for accessing the Internet.

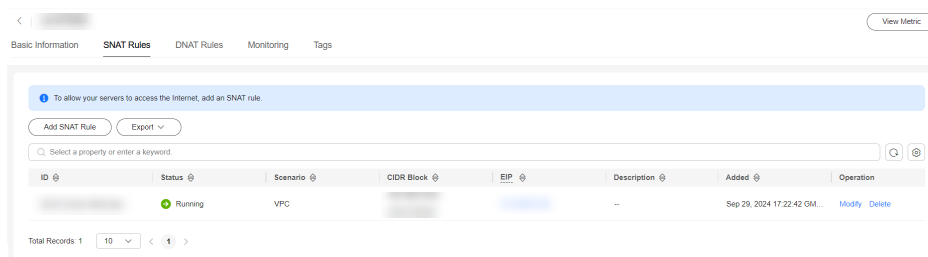
Parameter	Example	Description
Monitoring	-	You can create alarm rules on the Cloud Eye console to monitor your SNAT connections and keep informed of any changes in a timely manner.
Description	Not required	Supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

4. Click **OK**.

Step 4: Verify that the SNAT Rule Has Been Added

1. In the **SNAT Rules** tab, view details of the SNAT rule.
If **Status** of the SNAT rule is **Running**, the SNAT rule has been created.

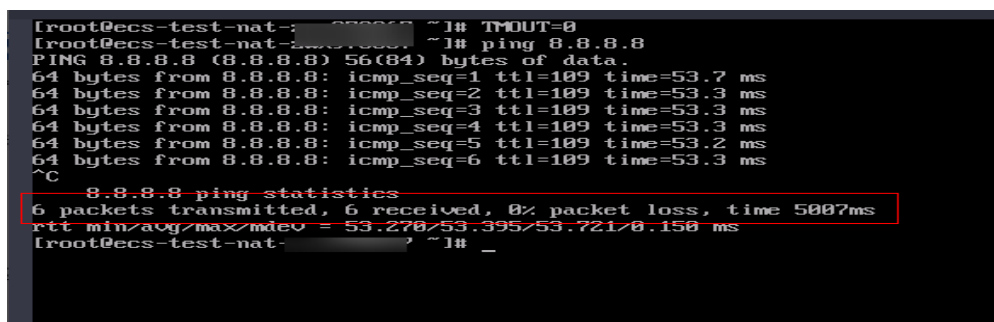
Figure 1-1 Verifying that the SNAT rule has been added



Step 5: Verify that Server Can Access the Internet Through the NAT Gateway

1. Go to the **ECS list** page.
2. Log in to the server to be verified.
3. Verify that the server can access the Internet.

Figure 1-2 Verification result



2 Using a Public NAT Gateway to Enable Servers to Be Accessed by the Internet

Scenarios

When one or more servers in a VPC need to provide services accessible from the Internet, you can add DNAT rules for a public NAT gateway, as introduced in this section.

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: Buy an EIP	Buy an EIP.
Step 2: Buy a Public NAT Gateway	Buy a public NAT gateway.
Step 3: Add a Default Route Pointing to the Public NAT Gateway	Add DNAT rules for the public NAT gateway so that servers in specific CIDR blocks share EIPs to access the Internet.
Step 4: Add a DNAT Rule	Add DNAT rules for the public NAT gateway so that servers in specific CIDR blocks share EIPs to access the Internet.
Step 5: Verify that the DNAT Rule Has Been Added	Check whether the DNAT rule has been added.
Step 6: Verify that Servers in a VPC Can Be Accessed from the Internet Through the NAT Gateway	Verify that servers for which the DNAT rules are applied can be accessed by a client on the Internet.

Preparations

Before using NAT gateways, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account.

- [Create a HUAWEI ID and enable Huawei Cloud services.](#)
- [Complete real-name authentication.](#)
- [Top up your account.](#)

Step 1: Buy an EIP

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.

Step 2: Buy a Public NAT Gateway

1. Go to the [Buy Public NAT Gateway](#) page.
2. On the **Buy Public NAT Gateway** page, configure required parameters.

Table 2-1 Descriptions of public NAT gateway parameters

Parameter	Example	Description
Region	CN North-Beijing4	The region where the public NAT gateway is located.
Billing Mode	Pay-per-use	The billing mode of the public NAT gateway.
Specifications	Small	The specifications of the public NAT gateway. The value can be Extra-large , Large , Medium , or Small . To view more details about specifications, click Learn more on the page.
Name	public-nat-01	The name of the public NAT gateway. Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.

Parameter	Example	Description
VPC	vpc-A	<p>The VPC that the public NAT gateway belongs to.</p> <p>The selected VPC cannot be changed after you buy the public NAT gateway.</p> <p>NOTE</p> <p>To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you buy a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you buy the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.</p>
Subnet	Subnet-A01	<p>The subnet that the public NAT gateway belongs to.</p> <p>The subnet must have at least one available IP address.</p> <p>The selected subnet cannot be changed after you buy the public NAT gateway.</p> <p>The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.</p>
Advanced Settings (Optional)	-	Click the drop-down arrow to configure advanced parameters of the public NAT gateway.
SNAT Connection TCP Timeout (s)	900	<p>The timeout period of a TCP connection established using the SNAT rule. If no data is exchanged within this period, the TCP connection will be closed.</p> <p>Value range: 40 to 7200</p>
SNAT Connection UDP Timeout (s)	300	<p>The timeout period of a UDP connection established using the SNAT rule. If no data is exchanged within this period, the UDP connection will be closed.</p> <p>Value range: 40 to 7200</p>

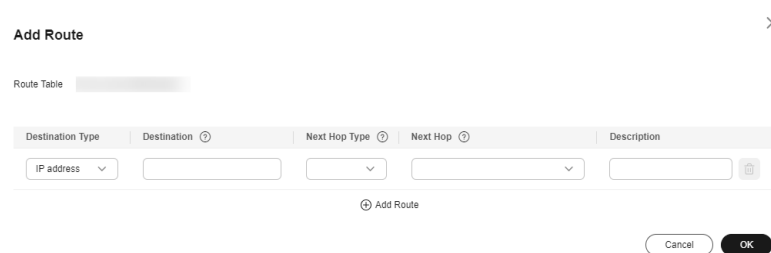
Parameter	Example	Description
SNAT Connection ICMP Timeout (s)	10	The timeout period of an ICMP connection established using the SNAT rule. If no data is exchanged within this period, the ICMP connection will be closed. Value range: 10 to 7200
TCP TIME_WAIT (s)	5	How long the side that actively closed the TCP connection is in the TIME_WAIT state. Value range: 0 to 1800
Description	Not required	Supplementary information about the public NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.
Tag	Not required	The identifier of the public NAT gateway. A tag is a key-value pair. You can add up to 20 tags to each public NAT gateway.

3. Click **Next**. On the page displayed, confirm the public NAT gateway specifications.
4. If you do not need to modify the information, click **Submit**.
On the **Public NAT Gateways** page, you can view the created public NAT gateway in the list.

Step 3: Add a Default Route Pointing to the Public NAT Gateway

1. Go to the [route table list](#) page.
2. On the **Route Tables** page, click **Create Route Table** in the upper right corner.
VPC: Select the VPC that the public NAT gateway belongs to.
3. After the custom route table is created, click its name. The **Summary** page is displayed.
4. Click **Add Route** and configure parameters as follows:
Destination: Set it to **0.0.0.0/0**.
Next Hop Type: Select **NAT gateway**.
Next Hop: Select the created NAT gateway.

Figure 2-1 Add Route



5. Click **OK**.

Step 4: Add a DNAT Rule

1. Go to the [public NAT gateway list](#) page.
2. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. Click **Add DNAT Rule**.
5. Configure required parameters. For details, see [Table 2-2](#).

Figure 2-2 Add DNAT Rule

Add DNAT Rule

Public NAT Gateway Name: nat-example For servers in your on-premises data center

* Scenario: **VPC** Direct Connect/Cloud Connect

* Port Type: **Specific port** All ports

* Protocol: TCP

* Public IP Address Type: **EIP** Global EIP

Bandwidth: 1 Mbit/s Billing Mode: Yearly/Monthly Enterprise Project: default

* Outside Port: Example: 22 or 22-30

* Instance Type: **Server** Virtual IP address Custom

Specify filter criteria.

Name	Status	Private IP Address	VPC	Enterprise Project

* NIC: --Select--

* Inside Port: Example: 22 or 22-30

Description: 0/255

Cancel OK

Table 2-2 Descriptions of DNAT rule parameters

Parameter	Example	Description
Scenario	VPC	Select VPC if your servers in a VPC will use the DNAT rule to provide services accessible from the Internet. Different servers in a VPC can share the same EIP to provide services accessible from the Internet.

Parameter	Example	Description
Port Type	Specific port	The port type. <ul style="list-style-type: none">• All ports: All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.• Specific port: Only requests received from a specified port over a specified protocol will be forwarded to the specified port on the server.
Protocol	TCP	The protocol can be TCP or UDP. This parameter is available if you select Specific port for Port Type . If you select All ports , this parameter is All by default.
Public IP Address Type	EIP	The EIP of the public NAT gateway.
Outside Port	80-100	The port of the EIP used by the NAT gateway. The port number ranges from 1 to 65535. You can enter a specific port number or a port range, for example, 80 or 80-100.
Instance Type	Server	The instance type for which the DNAT rules are applied.
NIC	-	The network interface of the server.
Inside Port	80-100	The port of the server that provides services accessible from the Internet through the DNAT rule. This parameter is available if you select Specific port for Port Type . The port number ranges from 1 to 65535. You can enter a specific port number or a port range, for example, 80 or 80-100.
Description	Not required	Supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. Click **OK**.

NOTICE

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect. For details, see [Adding a Security Group Rule](#).

Step 5: Verify that the DNAT Rule Has Been Added

1. In the **DNAT Rules** tab, view details of the DNAT rule and check whether the DNAT rule has been created.

If **Status** of the SNAT rule is **Running**, the SNAT rule has been created.

Step 6: Verify that Servers in a VPC Can Be Accessed from the Internet Through the NAT Gateway

1. Go to the [ECS list](#) page.
2. Log in to ECS 02 with an EIP bound.
3. On ECS 02, ping the EIP (120.46.131.153) to check whether ECS 01 on the private network can be accessed by ECS 02 on the public network through the NAT gateway.

Figure 2-3 Verification result

```
[root@ecs-~]# ping 120.46.131.153
PING 120.46.131.153 (120.46.131.153) 56(84) bytes of data:
64 bytes from 120.46.131.153: icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 120.46.131.153: icmp_seq=2 ttl=58 time=0.939 ms
64 bytes from 120.46.131.153: icmp_seq=3 ttl=58 time=0.905 ms
64 bytes from 120.46.131.153: icmp_seq=4 ttl=58 time=0.896 ms
64 bytes from 120.46.131.153: icmp_seq=5 ttl=58 time=0.906 ms
64 bytes from 120.46.131.153: icmp_seq=6 ttl=58 time=0.889 ms
64 bytes from 120.46.131.153: icmp_seq=7 ttl=58 time=0.860 ms
64 bytes from 120.46.131.153: icmp_seq=8 ttl=58 time=0.905 ms
64 bytes from 120.46.131.153: icmp_seq=9 ttl=58 time=0.886 ms
^C
--- 120.46.131.153 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8137ms
rtt min/avg/max/mdev = 0.860/0.930/1.192/0.102 ms
[root@ecs-~]#
```

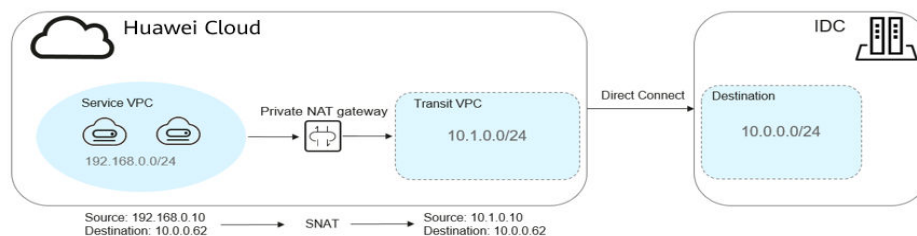
3 Using a Private NAT Gateway to Connect Cloud and On-premises Networks

Scenarios

You can use a private NAT gateway to enable communications between cloud and on-premises networks.

The following figure shows how a private NAT gateway enables ECSs in a VPC to communicate with your on-premises data center that has been connected to the cloud using Direct Connect.

Figure 3-1 Networking diagram



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 Service VPC and a Transit VPC	Create a service VPC and a transit VPC.
Step 2: Create a VPC Peering Connection	Create a VPC peering connection to connect your local data center to a transit VPC.
Step 3: Buy a Private NAT Gateway	Buy a private NAT gateway.

Procedure	Description
Step 5: Add an SNAT Rule	After the private NAT gateway is created, add an SNAT rule so that servers in the VPC can share a transit IP address to access on-premises data centers or other VPCs.
Step 6: Add a Route	You can add a route and configure the destination, next hop type, and next hop in the routes to determine where network traffic is directed.
Step 7: Add a Security Group Rule	Add an inbound security group rule to allow traffic to servers in the destination VPC.

Preparations

Before using NAT gateways, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account.

- [Create a HUAWEI ID and enable Huawei Cloud services.](#)
- [Complete real-name authentication.](#)
- [Top up your account.](#)

Step 1: Create a Service VPC and a Transit VPC

A VPC provides an isolated virtual network for ECSs. You can configure and manage your network as required.

You need to create two VPCs, one for your services, and one as the transit VPC.

For details, see [Creating a VPC](#).

Step 2: Create a VPC Peering Connection

Create a Direct Connect connection to link your on-premises data center to the cloud (the **CN-Hong Kong** region). In this example, a VPC peering connection is used.

Create a VPC peering connection to connect your local data center to a transit VPC. For details, see [VPC Peering Connection](#).

NOTE

For details about how to use Direct Connect to connect your data center (the destination VPC in the VPC peering connection) to the transit VPC, see [Overview](#).

Step 3: Buy a Private NAT Gateway

1. Go to the [Buy Private NAT Gateway](#) page.
2. On the [Buy Private NAT Gateway](#) page, configure required parameters.

Figure 3-2 Buy Private NAT Gateway

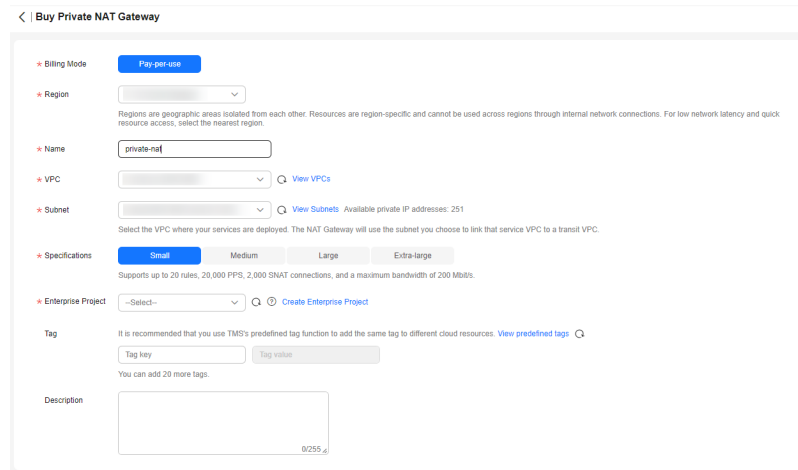


Table 3-1 Descriptions of private NAT gateway parameters

Parameter	Example	Description
Billing Mode	Pay-per-use	The billing mode of the private NAT gateway.
Region	CN-Hong Kong	The region where the private NAT gateway is located.
Name	private-nat-01	The name of the private NAT gateway. Enter up to 64 characters including only digits, letters, underscores (_), and hyphens (-).
VPC	vpc-A	The service VPC that the private NAT gateway belongs to. The selected VPC cannot be changed after the private NAT gateway is purchased.
Subnet	Subnet-A01	The subnet that the private NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the private NAT gateway is purchased.
Specifications	Small	The specifications of the private NAT gateway.

Parameter	Example	Description
Enterprise Project	default	The enterprise project that the private NAT gateway belongs to. If you have not configured any enterprise project, select the default enterprise project. You can configure the enterprise project to which the private network NAT gateway belongs only after the enterprise project function is enabled for you.
Tag	Not required	The private NAT gateway tag. A tag is a key-value pair. You can add up to 20 tags to each private NAT gateway.
Description	Not required	Supplementary information about the private NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.

3. Click **Buy Now**.
4. In the private NAT gateway list, check the gateway status.

Step 4: Assign a Transit IP Address

1. On the **Private NAT Gateways** page, click **Transit IP Addresses < Assign Transit IP Address**.

Figure 3-3 Assigning a transit IP address

Assign Transit IP Address [X]

Transit VPC [dropdown] [Q]

Transit Subnets [dropdown] [Q]

Transit IP Address Automatic Manual

Enterprise Project [--Select--] [Q] [Create Enterprise Project](#) [?]

Tag It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) [Q]

Tag key [input] Tag value [input]

You can add 20 more tags.

[Cancel] [OK]

2. Configure required parameters. For details, see [Table 3-2](#).

Table 3-2 Parameter descriptions of a transit IP address

Parameter	Example	Description
Transit VPC	-	The VPC to which the transit IP address belongs.
Transit Subnets	-	A transit subnet is a transit network and is the subnet to which the transit IP address belongs. The subnet must have at least one available IP address.
Transit IP Address	Automatic	The transit IP address can be assigned in either of the following ways: Automatic: The system automatically assigns a transit IP address. Manual: You need to manually assign a transit IP address.
Enterprise Project	default	The enterprise project to which the transit IP address belongs.
Tag	Not required	The transit IP address tag, which consists of a key and value pair. You can add up to 20 tags to each transit IP address.

3. Click **OK**.

Step 5: Add an SNAT Rule

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add an SNAT rule.
3. On the **SNAT Rules** tab, click **Add SNAT Rule**.
4. Configure required parameters. For details, see [Table 3-3](#).

Table 3-3 Descriptions of SNAT rule parameters

Parameter	Example	Description
Subnet	Existing	The subnet type of the SNAT rule. Select Existing or Custom . Select a subnet where IP address translation is required in the service VPC.
Monitoring	-	You can create alarm rules to watch the number of SNAT connections.
Transit IP Address	-	The transit IP address you assigned in Step 4: Assign a Transit IP Address .

Parameter	Example	Description
Description	Not required	Supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

- Click **OK**.
- View details in the SNAT rule list. If **Status** is **Running**, the rule has been added.

Step 6: Add a Route

- Go to the [route table list](#) page.
- In the route table list, click the name of the route table associated the service VPC.
- Click **Add Route** and configure required parameters.

Table 3-4 Route parameters

Parameter	Example	Description
Destination	10.0.0.0/24	The destination CIDR block. Set it to the CIDR block used by your on-premises data center.
Next Hop Type	NAT gateway	Type of the next hop.
Next Hop	private-nat-01	Set Next Hop to the private NAT gateway.
Description	Not required	(Optional) Supplementary information about the route. Enter up to 255 characters. Angle brackets (<>) are not allowed.

- Click **OK**.

Step 7: Add a Security Group Rule

- Go to the [security group list](#) page.
- Locate the target security group and click **Manage Rules** in the **Operation** column.
The page for configuring security group rules is displayed.
- On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, configure required parameters.
You can click + to add more inbound rules.

Table 3-5 Description of inbound rule parameters

Parameter	Example	Description
Priority	1	Priority of a rule. A smaller value indicates a higher priority.
Action	Allow	<p>Allow or Deny</p> <ul style="list-style-type: none"> • If the Action is set to Allow, access from the source is allowed to ECSs in the security group over specified ports. • If the Action is set to Deny, access from the source is denied to ECSs in the security group over specified ports.
Protocol & Port	TCP	Protocol: Network protocol. The value can be All, TCP, UDP, ICMP, or GRE .
	22 or 22-30	Port: The port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.
Source	0.0.0.0/0	<p>Source of the security group rule. The value can be a single IP address, an IP address group, or a security group, to allow access from the specified IP address, IP address group, or instances in another security group.</p> <p>For more information about IP address groups, see IP Address Group Overview.</p>
Description	Not required	<p>(Optional) Supplementary information about the security group rule.</p> <p>Enter up to 255 characters. Angle brackets (<>) are not allowed.</p>

4. Click **OK**.

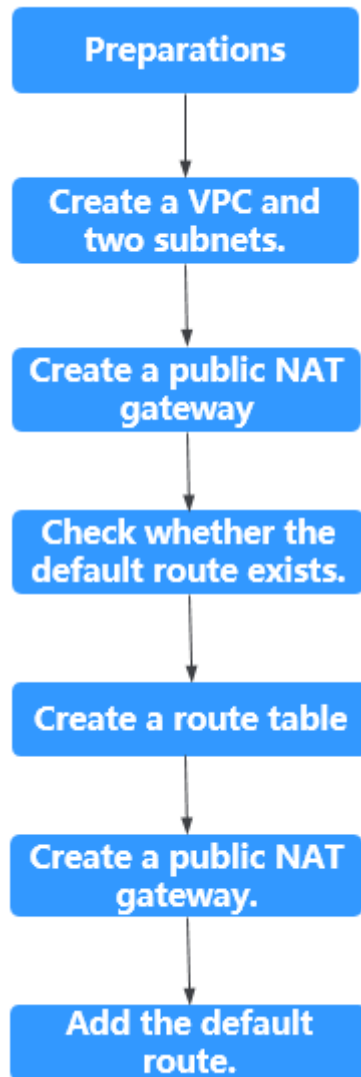
4 Using Multiple Public NAT Gateways Together in Performance-Demanding Scenarios

4.1 Overview

A single NAT gateway supports up to one million SNAT connections and 20 Gbit/s of bandwidth. If one NAT gateway cannot meet your requirements, you can use multiple NAT gateways.

This topic describes how to deploy multiple public NAT gateways.

Figure 4-1 Procedure



Preparations

Before using NAT gateways, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account.

- [Create a HUAWEI ID and enable Huawei Cloud services.](#)
- [Complete real-name authentication.](#)
- [Top up your account.](#)

4.2 Step 1: Create a VPC and Two Subnets

Scenarios

A VPC provides an isolated virtual network for ECSs. You can configure and manage your network as required.

Create one VPC and two subnets.

Procedure

For details, see [Creating a VPC](#).

4.3 Step 2: Buy a Public NAT Gateway



Scenarios

Buy a public NAT gateway.

Prerequisites

A VPC is available.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click  to expand the service list and choose **Networking > NAT Gateway**.

The **Public NAT Gateways** page is displayed.

4. On the displayed page, click **Buy Public NAT Gateway**.
5. Configure required parameters. For details, see [Table 4-1](#).

Select the VPC and subnet you created in [Step 1: Create a VPC and Two Subnets](#) for **VPC** and **Subnet**.

Table 4-1 Descriptions of public NAT gateway parameters

Parameter	Description
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.
Region	The region where the public NAT gateway is located

Parameter	Description
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed.
VPC	The VPC that the public NAT gateway belongs to The selected VPC cannot be changed after the public NAT gateway is purchased.
Subnet	The subnet of the VPC that the public NAT gateway belongs to The subnet must have at least one available IP address. The selected subnet cannot be changed after the public NAT gateway is purchased. The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.
Specifications	The public NAT gateway specifications The value can be Small , Medium , Large , or Extra-large . To view more details about specifications, click Learn more on the page.
Enterprise Project	The enterprise project that the public NAT gateway belongs to If an enterprise project is configured for a public NAT gateway, the public NAT gateway belongs to this enterprise project. If you have not configured any enterprise project, select the default enterprise project.
Advanced Settings	Click the drop-down arrow to configure advanced parameters of the public NAT gateway, such as Description .
Description	Supplementary information about the public NAT gateway Enter up to 255 characters. Angle brackets (<>) are not allowed.

After you configure the parameters, the public NAT gateway price will be displayed. To view more pricing details about public NAT gateways, click **Pricing details** on the page.

6. Click **Next**. On the page displayed, confirm the public NAT gateway specifications.
7. Click **Submit**.

It takes 1 to 6 minutes to create a public NAT gateway.


8. In the list, view the status of the public NAT gateway.

4.4 Step 3: Check the Default Route

Scenarios

After the public NAT gateway is purchased, go to the route table list, locate the default route table of the VPC where you deploy the public NAT gateway, and check whether there is a default route with the next hop set to the public NAT gateway.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the route table list, click the name of the default route table of the VPC.
6. Go to the route table details page and check whether the default route pointing to the public NAT gateway.

NOTE

When the first public NAT gateway in a VPC is created, the default route (0.0.0.0/0) is automatically created in the default route table. If the default route already exists in the VPC, add a new route and set the next hop to the created public NAT gateway.

4.5 Step 4: Create a Route Table

Scenarios

Each public NAT gateway requires its unique route table. Create the second route table for the VPC.


NOTE

If the custom route table quota is insufficient, [create a service ticket](#) to increase the route table quota.

Prerequisites

A route table can be created in the VPC.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the upper right corner, click **Create Route Table**. On the displayed page, configure required parameters.

Table 4-2 Parameter descriptions

Parameter	Description	Example Value
Name	(Mandatory) The name of the route table Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. Spaces are not allowed.	rtb-001
VPC	(Mandatory) The VPC that the route table belongs to	vpc-001
Description	(Optional) Supplementary information about the route table Enter up to 255 characters. Angle brackets (<>) are not allowed.	N/A
Route Settings	Routes contained in the route table You can add a route when creating the route table or after the route table is created. You can click + to add more routes.	N/A

6. Click **OK**.
A message indicating that subnets can now be associated with the created route table is displayed. Perform the following steps to associate the other subnet of the VPC with the route table:
 - a. Click **Associate Subnet**.
The **Associated Subnets** tab is displayed.
 - b. Click **Associate Subnet** and select the second subnet created in [Step 1: Create a VPC and Two Subnets](#).
 - c. Click **OK**.

4.6 Step 5: Buy Another Public NAT Gateway



Scenarios

Buy another public NAT gateway in the service VPC.

Prerequisites

The second route table has been created for the VPC and has been associated with the second subnet of the VPC.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click  to expand the service list and choose **Networking > NAT Gateway**.

The **Public NAT Gateways** page is displayed.

4. On the displayed page, click **Buy Public NAT Gateway**.
5. Configure required parameters. For details, see [Table 4-3](#).

Select the VPC and the other subnet you created in [Step 1: Create a VPC and Two Subnets](#) for **VPC** and **Subnet**.

Table 4-3 Descriptions of public NAT gateway parameters

Parameter	Description
Billing Mode	public NAT gateway are billed on a pay-per-use or yearly/monthly basis.
Region	The region where the public NAT gateway is located
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed.
VPC	The VPC that the public NAT gateway belongs to The selected VPC cannot be changed after the public NAT gateway is purchased.
Subnet	The subnet of the VPC that the public NAT gateway belongs to The subnet must have at least one available IP address. The selected subnet cannot be changed after the public NAT gateway is purchased. The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.
Specifications	The public NAT gateway specifications The value can be Small , Medium , Large , or Extra-large . To view more details about specifications, click Learn more on the page.

Parameter	Description
Enterprise Project	The enterprise project that the public NAT gateway belongs to If an enterprise project is configured for a public NAT gateway, the public NAT gateway belongs to this enterprise project. If you have not configured any enterprise project, select the default enterprise project.
Description	Supplementary information about the public NAT gateway Enter up to 255 characters. Angle brackets (<>) are not allowed.


6. Click **Next**. On the page displayed, confirm the public NAT gateway specifications.
7. Click **Submit**.
It takes 1 to 6 minutes to create a public NAT gateway.
8. In the list, view the status of the public NAT gateway.

4.7 Step 6: Add the Default Route

Scenarios

If the VPC already has one or more NAT gateways configured, a route table must be created for the second public NAT gateway. You need to add the default route (0.0.0.0/0) with the next hop set to the second public NAT gateway in the new route table you have created.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the route table list, click the name of the route table to which you want to add a route.
6. Click **Add Route** and configure required parameters.


You can click  to add more routes.

Table 4-4 Parameter descriptions

Parameter	Description	Example Value
Destination	The destination CIDR block The destination of each route must be unique. The destination cannot overlap with any subnet in the VPC.	0.0.0.0/0
Next Hop Type	Type of the next hop	NAT gateway
Next Hop	Set the next hop. The resources in the drop-down list box are displayed based on the selected next hop type.	N/A
Description	(Optional) Supplementary information about the route Enter up to 255 characters. Angle brackets (<>) are not allowed.	N/A

7. Click **OK**.