

NAT Gateway

User Guide

Issue 01
Date 2022-11-29



Copyright © Huawei Technologies Co., Ltd. 2023. 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



HUAWEI 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 "Vul. Response Process". For details about the policy, see the following website:<https://www.huawei.com/en/psirt/vul-response-process>
For enterprise customers who need to obtain vulnerability information, visit:<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Allowing a Private Network to Access the Internet Using SNAT.....	1
1.1 Overview.....	1
1.2 Preparations.....	2
1.3 Step 1: Buy an EIP.....	2
1.4 Step 2: Buy a Public NAT Gateway.....	3
1.5 Step 3: Add an SNAT Rule.....	6
1.6 Step 4: Test the Connection.....	8
2 Allowing Internet Users to Access a Service in a Private Network Using DNAT... 11	11
2.1 Overview.....	11
2.2 Preparations.....	12
2.3 Step 1: Buy an EIP.....	12
2.4 Step 2: Buy a Public NAT Gateway.....	13
2.5 Step 3: Add a DNAT Rule.....	16
2.6 Step 4: Test the Connection.....	19
3 Allowing On-Premises Servers to Communicate with the Internet.....	22
3.1 Overview.....	22
3.2 Preparations.....	23
3.3 Step 1: Connect Your On-premises Data Center to the Cloud with Direct Connect.....	24
3.4 Step 2: Buy an EIP.....	24
3.5 Step 3: Buy a Public NAT Gateway.....	24
3.6 Step 4: Add an SNAT Rule.....	27
3.7 Step 5: Add a DNAT Rule.....	29
4 Using Private NAT Gateways to Enable Communications Between Cloud and On-premises Networks.....	33
4.1 Overview.....	33
4.2 Preparations.....	34
4.3 Step 1: Create a Service VPC and a Transit VPC.....	35
4.4 Step 2: Create a Direct Connect Connection.....	35
4.5 Step 3: Buy a Private NAT Gateway.....	35
4.6 Step 4: Add an SNAT Rule.....	38
4.7 Step 5: Add a Route.....	39
4.8 Step 6: Add a Security Group Rule.....	40

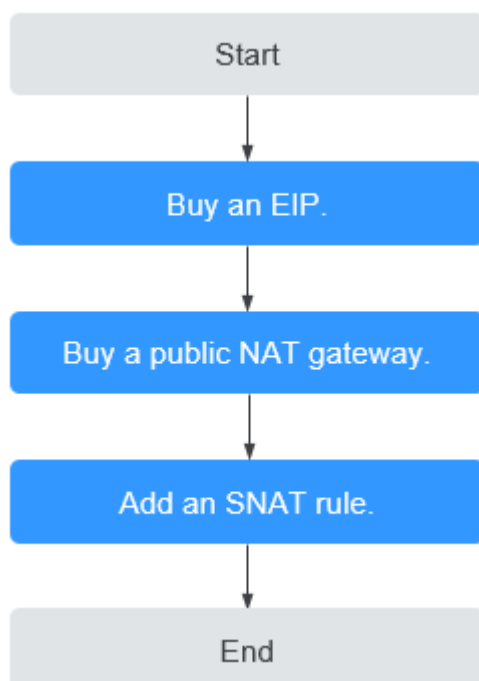
5 Using Multiple Public NAT Gateways Together in Performance-Demanding Scenarios.....	43
5.1 Overview.....	43
5.2 Preparations.....	44
5.3 Step 1: Create a VPC and Two Subnets.....	45
5.4 Step 2: Buy a Public NAT Gateway.....	45
5.5 Step 3: Check the Default Route.....	47
5.6 Step 4: Create a Route Table.....	47
5.7 Step 5: Buy Another Public NAT Gateway.....	48
5.8 Step 6: Add the Default Route.....	50
6 Change History.....	52

1 Allowing a Private Network to Access the Internet Using SNAT

1.1 Overview

If servers (ECSs and BMSs) without EIPs bound need to access the Internet, the servers can share one or more EIPs to access the Internet through a public NAT gateway. This method provides access without exposing their IP addresses.

Figure 1-1 Flowchart



1.2 Preparations

Before you use a public NAT gateway, complete operations described in this section.

Registering an Account and Completing Real-Name Authentication

Skip this part if you already have an account of Huawei Cloud and completed real-name authentication. If you do not have an account of Huawei Cloud, perform the following steps to create one:

1. Visit the [Huawei Cloud official website](#) and click **Register**.
2. On the displayed page, register an account as prompted.
After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in [Individual Real-Name Authentication](#).

NOTE

Real-name authentication is required only when your account purchases or uses resources in the Chinese Mainland regions.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For pricing details about public NAT gateways, see [Product Pricing Details](#).
- To top up an account, see [Topping Up an Account \(Prepaid Direct Customers\)](#).

1.3 Step 1: Buy an EIP

Scenarios

You can buy an EIP for your NAT gateway so that servers in a VPC can use this EIP to access the Internet.

NOTE

For details about the EIP pricing, see [Billing](#).

Procedure

For details, see [Assigning an EIP](#).

You do not need to bind the EIP to any server.

1.4 Step 2: Buy a Public NAT Gateway

Scenarios

Buy a public NAT gateway to enable your servers to access the Internet or provide services accessible from the Internet.

Prerequisites

- The VPC and subnet where your public NAT gateway will be deployed are available.
- 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.

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

Table 1-1 Descriptions of public NAT gateway parameters

Parameter	Description
Billing Mode	Public NAT gateways are billed on a pay-per-use 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.

Parameter	Description
VPC	<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	<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>
Specifications	<p>The specifications of the public NAT gateway</p> <p>The value can be Extra-large, Large, Medium, or Small. To view more details about specifications, click Learn more on the page.</p>
Enterprise Project	<p>The enterprise project that the public NAT gateway belongs to</p> <p>If an enterprise project has been configured, select the enterprise project. If you have not configured any enterprise project, select the default enterprise project.</p>
Description	<p>Supplementary information about the public NAT gateway</p> <p>Enter up to 255 characters. Angle brackets (<>) are not allowed.</p>
Tag	<p>The public NAT gateway tag. A tag is a key-value pair.</p> <p>You can add up to 10 tags to each public NAT gateway.</p> <p>The tag key and value must meet the requirements listed in Table 1-2.</p>

Table 1-2 Tag requirements


Parameter	Requirement
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each NAT gateway.• Can contain a maximum of 36 characters.• Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (), and slashes (/), and the first and last characters cannot be spaces.
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (), and slashes (/), and the first and last characters cannot be spaces.

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

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

After the public NAT gateway is created, check whether a default route (0.0.0.0/0) that points to the public NAT gateway exists in the default route table of the VPC where the public NAT gateway is. If no, add a route pointing to the public NAT gateway to the default route table, alternatively, create a custom route table and add the default route 0.0.0.0/0 pointing to the public NAT gateway to the table. The following describes how to add a route to a custom route table.

Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Networking**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. On the **Route Tables** page, click **Create Route Table** in the upper right corner.

VPC: Select the VPC to which the public NAT gateway belongs.

NOTE

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

- After the custom route table is created, click its name.
The **Summary** page is displayed.
- 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 1-2 Add Route

The screenshot shows the 'Add Route' dialog box. At the top, it says 'Add Route' with a close button (X). Below that, it indicates the 'Route Table' is 'rtb-VPC'. The main area contains a table with the following data:

Destination ?	Next Hop Type ?	Next Hop ?	Description
0.0.0.0/0	NAT gateway	nat-49ee(8947eef5-6948-4245-af45-...)	

Below the table, there is an 'Add Route' button with a plus sign. At the bottom, there are 'OK' and 'Cancel' buttons.

- Click **OK**.

1.5 Step 3: Add an SNAT Rule

Scenarios

After creating a public NAT gateway, add an SNAT rule to enable your servers in a specific subnet to access the Internet through the same EIP.

One SNAT rule can be configured for only one subnet or CIDR block. If there are multiple subnets or CIDR blocks in a VPC, you can add multiple SNAT rules to allow servers to share EIPs.

Prerequisites

A public NAT gateway is available.

Procedure


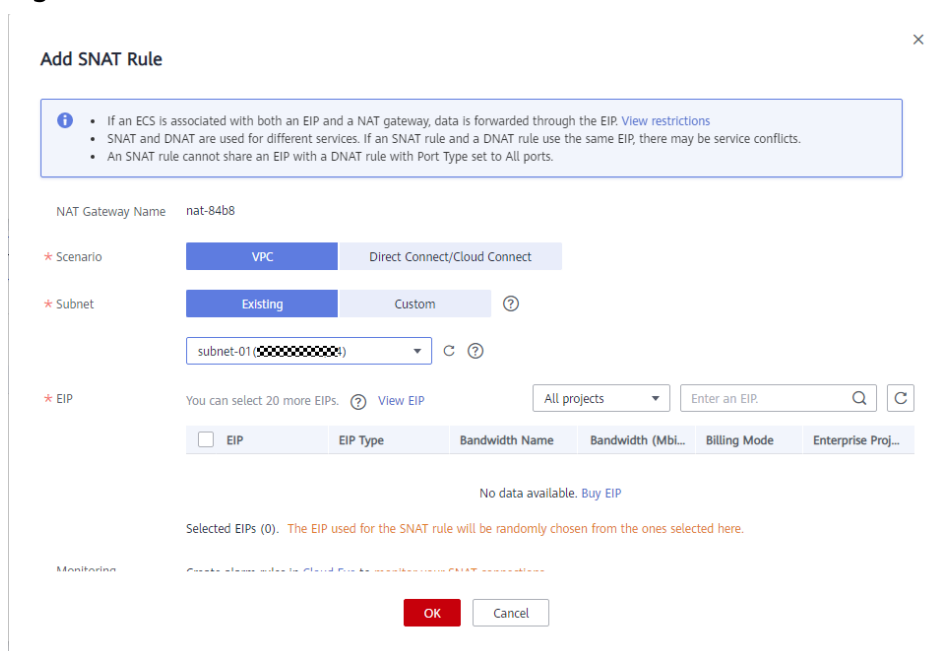
- Log in to the management console.
- Click  in the upper left corner and select the desired region and project.
- Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
- On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
- On the **SNAT Rules** tab, click **Add SNAT Rule**.

Figure 1-3 Add SNAT Rule



6. Configure required parameters. [Table 1-3](#) describes the parameters.

Table 1-3 Descriptions of SNAT rule parameters

Parameter	Description
Scenario	Select VPC if your servers in a VPC will use the SNAT rule to access the Internet.
Subnet	<ul style="list-style-type: none"> ● Existing: Select an existing subnet. ● Custom: Customize a CIDR block or enter a server IP address. <p>NOTE The customized CIDR block must be a subset of the VPC subnet CIDR block. You can configure a 32-bit host IP address. The NAT gateway takes effect only for this address.</p>
EIP	<p>The EIP used for accessing the Internet</p> <p>You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with Port Type set to Specific port, or has been bound to an SNAT rule of the current public NAT gateway.</p> <p>You can select up to 20 EIPs for an SNAT rule. If you have selected multiple EIPs for an SNAT rule, one EIP will be chosen randomly.</p>
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.

Parameter	Description
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

7. Click **OK**.

 **NOTE**

- You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.
- Each VPC can be associated with multiple public NAT gateways.
- Only one SNAT rule can be added for each VPC subnet.

1.6 Step 4: Test the Connection

Scenarios

After adding an SNAT rule, you can perform the following steps to verify the connection:

1. Verify that the SNAT rule has been added for the public NAT gateway.
2. Verify that servers that have no EIP bound can access the Internet through the NAT gateway.

Prerequisites

An SNAT rule has been added.

Verifying that the SNAT Rule Has Been Added


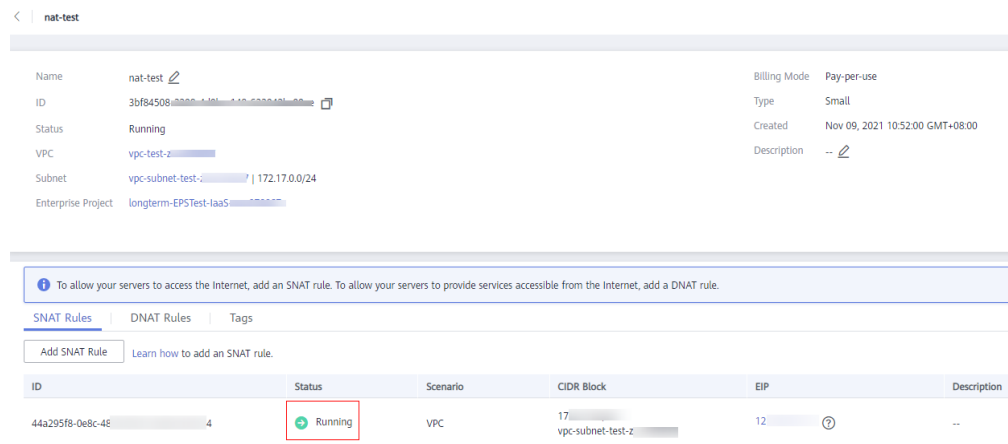
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
4. On the **Public NAT Gateways** page, click the name of the public NAT gateway.
5. In the **SNAT Rules** tab, view details about the SNAT rule.
If **Status** of the SNAT rule is **Running**, the SNAT rule has been created.

Figure 1-4 Checking the SNAT rule



Verifying that Servers Can Access the Internet Through the NAT Gateway



- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select the desired region and project.
- Step 3** Hover on  in the upper left corner to display **Service List** and choose **Compute > Elastic Cloud Server**.
- Step 4** Log in to the server.
- Step 5** Verify that the server can access the Internet.

Figure 1-5 Verification result

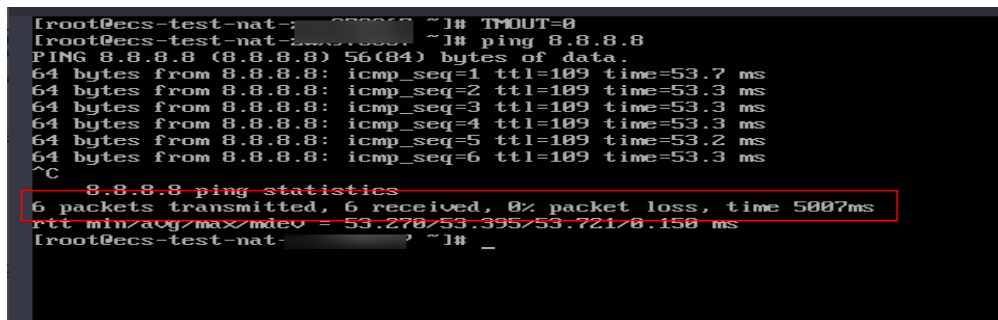


Figure 1-6 Deleting an SNAT rule

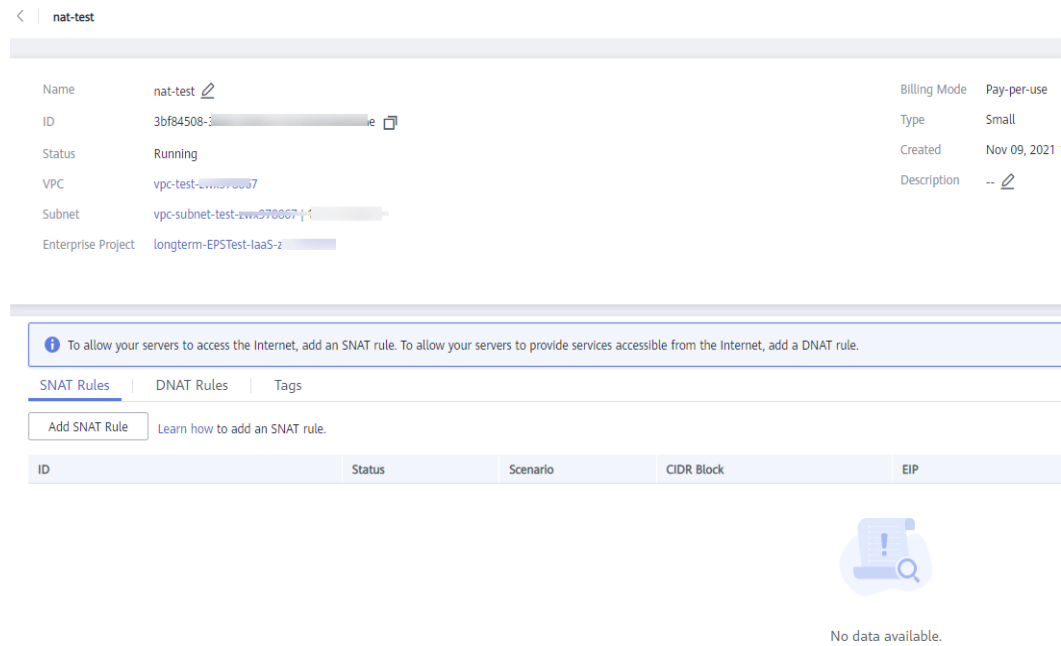
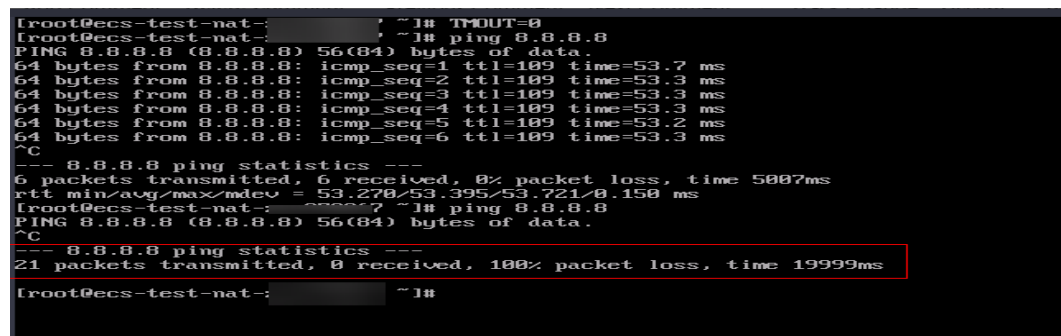


Figure 1-7 Failed to access the Internet



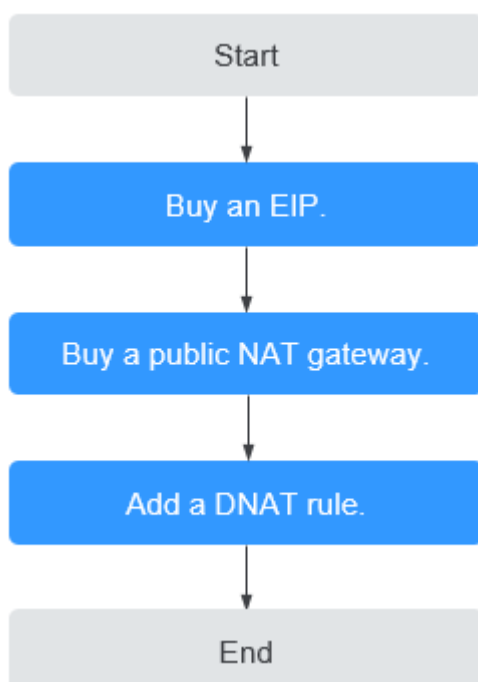
----End

2 Allowing Internet Users to Access a Service in a Private Network Using DNAT

2.1 Overview

When one or more servers (ECSs and BMSs) in a VPC need to provide services accessible from the Internet, you can add DNAT rules.

Figure 2-1 Flowchart



2.2 Preparations

Before you use a public NAT gateway, complete operations described in this section.

Registering an Account and Completing Real-Name Authentication

Skip this part if you already have an account of Huawei Cloud and completed real-name authentication. If you do not have an account of Huawei Cloud, perform the following steps to create one:

1. Visit the [Huawei Cloud official website](#) and click **Register**.
2. On the displayed page, register an account as prompted.
After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in [Individual Real-Name Authentication](#).

NOTE

Real-name authentication is required only when your account purchases or uses resources in the Chinese Mainland regions.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For pricing details about public NAT gateways, see [Product Pricing Details](#).
- To top up an account, see [Topping Up an Account \(Prepaid Direct Customers\)](#).

2.3 Step 1: Buy an EIP

Scenarios

You can buy an EIP for your NAT gateway so that servers in a VPC can use this EIP to provide services accessible from the Internet.

NOTE

For details about the EIP pricing, see [Billing](#).

Procedure

For details, see [Assigning an EIP](#).

You do not need to bind the EIP to any server.

2.4 Step 2: Buy a Public NAT Gateway

Scenarios

Buy a public NAT gateway to enable your servers to access the Internet or provide services accessible from the Internet.

Prerequisites

- The VPC and subnet where your public NAT gateway will be deployed are available.
- 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.

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 **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
4. On the displayed page, click **Buy Public NAT Gateway**.
5. Configure required parameters. For details, see [Table 2-1](#).

Table 2-1 Descriptions of public NAT gateway parameters

Parameter	Description
Billing Mode	Public NAT gateways are billed on a pay-per-use 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.

Parameter	Description
VPC	<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	<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>
Specifications	<p>The specifications of the public NAT gateway</p> <p>The value can be Extra-large, Large, Medium, or Small. To view more details about specifications, click Learn more on the page.</p>
Enterprise Project	<p>The enterprise project that the public NAT gateway belongs to</p> <p>If an enterprise project has been configured, select the enterprise project. If you have not configured any enterprise project, select the default enterprise project.</p>
Description	<p>Supplementary information about the public NAT gateway</p> <p>Enter up to 255 characters. Angle brackets (<>) are not allowed.</p>
Tag	<p>The public NAT gateway tag. A tag is a key-value pair.</p> <p>You can add up to 10 tags to each public NAT gateway.</p> <p>The tag key and value must meet the requirements listed in Table 2-2.</p>

Table 2-2 Tag requirements


Parameter	Requirement
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each NAT gateway.• Can contain a maximum of 36 characters.• Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (), and slashes (/), and the first and last characters cannot be spaces.
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (), and slashes (/), and the first and last characters cannot be spaces.

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

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

After the public NAT gateway is created, check whether a default route (0.0.0.0/0) that points to the public NAT gateway exists in the default route table of the VPC where the public NAT gateway is. If no, add a route pointing to the public NAT gateway to the default route table, alternatively, create a custom route table and add the default route 0.0.0.0/0 pointing to the public NAT gateway to the table. The following describes how to add a route to a custom route table.

Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Networking**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. On the **Route Tables** page, click **Create Route Table** in the upper right corner.

VPC: Select the VPC to which the public NAT gateway belongs.

NOTE

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

- After the custom route table is created, click its name.
The **Summary** page is displayed.
- 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 2-2 Add Route

The screenshot shows the 'Add Route' configuration window. At the top, it says 'Add Route' with a close button. Below that, it indicates the route table is 'rtb-VPC'. The main configuration area has four columns: 'Destination' (0.0.0.0/0), 'Next Hop Type' (NAT gateway), 'Next Hop' (nat-49ee(8947eef5-6948-4245-af45-...)), and 'Description'. Below the table is an 'Add Route' button with a plus icon, and 'OK' and 'Cancel' buttons at the bottom.

- Click **OK**.

2.5 Step 3: Add a DNAT Rule

Scenarios


After a public NAT gateway is created, add DNAT rules to allow servers in your VPC to provide services accessible from the Internet.

You can configure a DNAT rule for each port on a server. If multiple servers need to provide services accessible from the Internet, create multiple DNAT rules.

Prerequisites

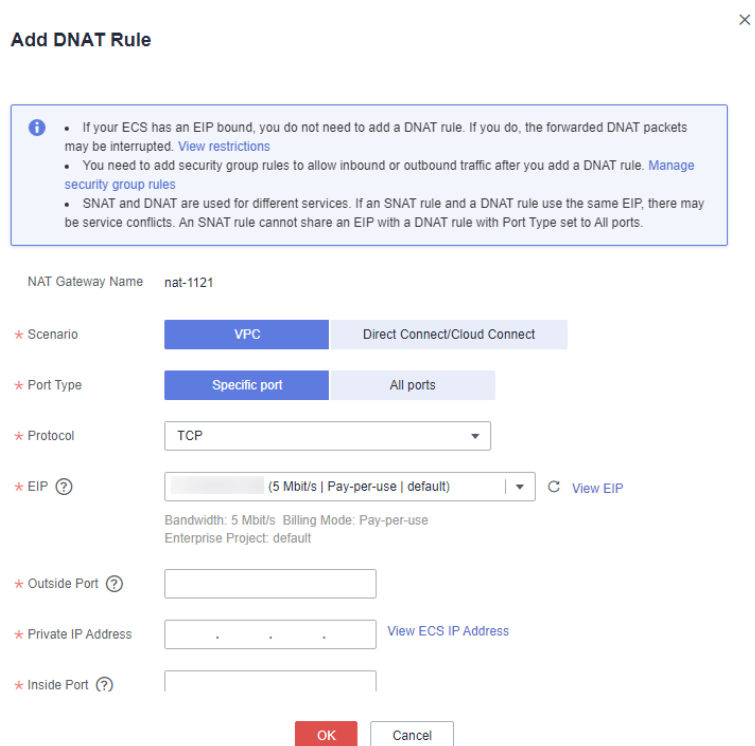
A public NAT gateway is available.

Procedure

- Log in to the management console.
- Click  in the upper left corner and select the desired region and project.
- Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
- On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
- On the public NAT gateway details page, click the **DNAT Rules** tab.

6. Click **Add DNAT Rule**.

Figure 2-3 Add DNAT Rule



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

Table 2-3 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	Select VPC if your servers in a VPC need to share an EIP to provide services accessible from the Internet.
Port Type	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	The protocol can be TCP or UDP. This parameter is available if you select Specific port for Port Type . If you select All ports , the value of this parameter is All by default.

Parameter	Description
EIP	The EIP of the public NAT gateway You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with Port Type set to Specific port , or has been bound to an SNAT rule of the current public NAT gateway.
Outside Port	The port of the EIP used by the NAT gateway for external communications This parameter is only available if you select Specific port for Port Type . Range: 1 to 65535 You can enter a specific port number or a port range, for example, 80 or 80-100.
Private IP Address	The IP address of the server in the NAT gateway's VPC and processes matching packets where requests will be forwarded to Configure the port of Private IP Address if you select Specific port for Port Type .
Inside Port	The port of the server over which the originating requests will be forwarded This parameter is only available if you select Specific port for Port Type . Range: 1 to 65535 You can enter a specific port number or a port range, for example, 80 or 80-100.
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

8. 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.

2.6 Step 4: Test the Connection

Scenarios


After adding a DNAT rule, you can perform the following steps to verify the connection:

1. Verify that the DNAT rule has been added for the public NAT gateway.
2. Check whether ECS 01 in the private network can be accessed by ECS 02 from the Internet through the NAT gateway (EIP 120.46.131.153 bound to the DNAT rule).

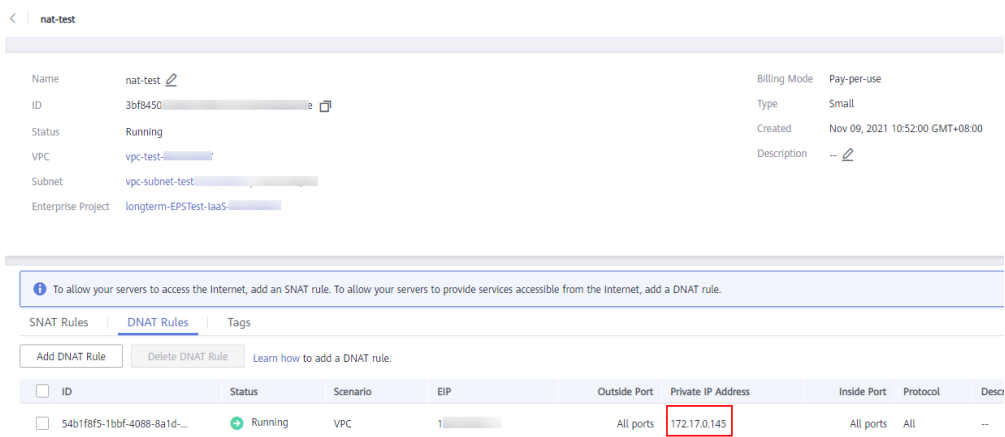
Prerequisites

A DNAT rule has been added.

Verifying that the DNAT Rule Has Been Added

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 **NAT Gateway**.
4. On the **Public NAT Gateways** page, click the name of the public NAT gateway.
5. In the **DNAT Rules** tab, view details about the DNAT rule and check whether the DNAT rule has been created.

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




The screenshot shows the details of a NAT Gateway named 'nat-test'. The status is 'Running'. Below the details is a table of DNAT Rules with one rule listed, having a status of 'Running' and a private IP address of 172.17.0.145.

ID	Status	Scenario	EIP	Outside Port	Private IP Address	Inside Port	Protocol	Desc
54b1f8f5-1bbf-4088-8a1d-...	Running	VPC	1	All ports	172.17.0.145	All ports	All	--

Verifying that Servers in a VPC Can Be Accessed from the Internet Through the NAT Gateway

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select the desired region and project.


- Step 3** Hover on  in the upper left corner to display **Service List** and choose **Compute > Elastic Cloud Server**.
- Step 4** Log in to ECS 02 with an EIP bound.
- Step 5** 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 2-4 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-~]#
```

Figure 2-5 Deleting a DNAT rule

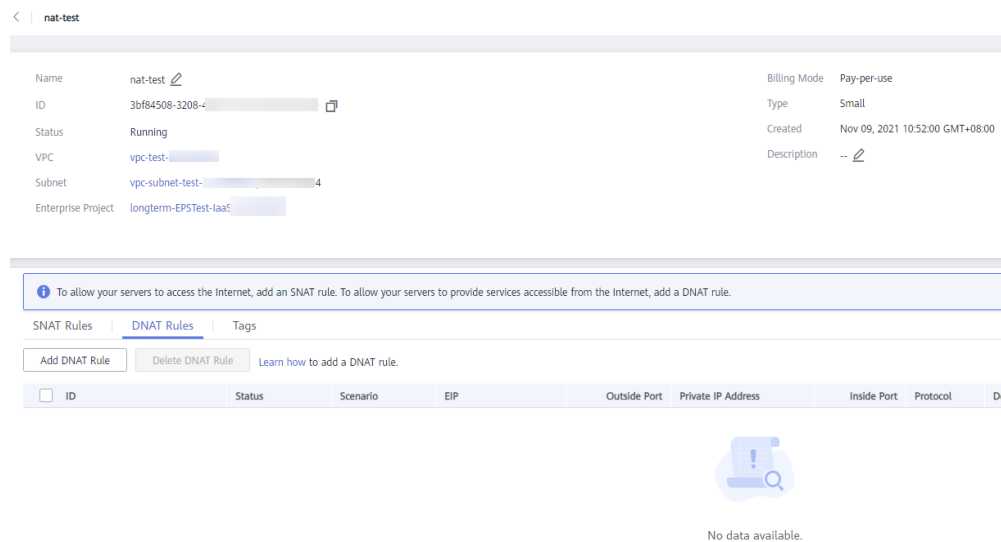


Figure 2-6 Failed to be accessed from the Internet

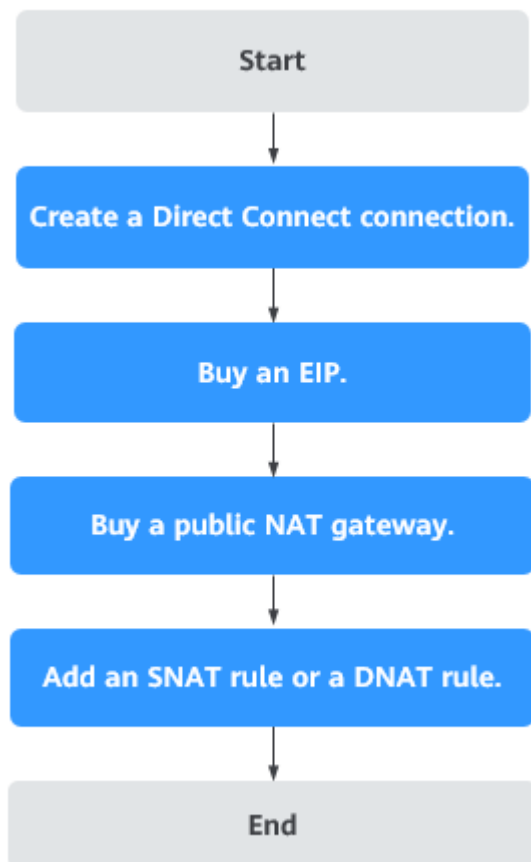
```
[root@ecs- ~]# ping 120.46.131.153
PING 120.46.131.153 (120.46.131.153) 56(84) bytes of data.
^C
--- 120.46.131.153 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5104ms
[root@ecs- ~]#
```

----End

3 Allowing On-Premises Servers to Communicate with the Internet

3.1 Overview

You need to first create a Direct Connect or VPN connection to connect your servers in the on-premises data center to the cloud, and then buy public NAT gateways and configure SNAT rules to allow servers in your data center to access the Internet or to provide services accessible from the Internet. [Figure 3-1](#) shows how servers in an on-premises data center communicate with the Internet.

Figure 3-1 Servers in an on-premises data center communicating with the Internet

3.2 Preparations

Before you use a public NAT gateway, complete operations described in this section.

Registering an Account and Completing Real-Name Authentication

Skip this part if you already have an account of Huawei Cloud and completed real-name authentication. If you do not have an account of Huawei Cloud, perform the following steps to create one:

1. Visit the [Huawei Cloud official website](#) and click **Register**.
2. On the displayed page, register an account as prompted.
After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in [Individual Real-Name Authentication](#).

NOTE

Real-name authentication is required only when your account purchases or uses resources in the Chinese Mainland regions.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For pricing details about public NAT gateways, see [Product Pricing Details](#).
- To top up an account, see [Topping Up an Account \(Prepaid Direct Customers\)](#).

3.3 Step 1: Connect Your On-premises Data Center to the Cloud with Direct Connect

Scenarios

Create a Direct Connect connection to link your on-premises data center to a VPC. Then deploy a public NAT gateway in the VPC to allow your on-premises servers to communicate with the Internet.

Procedure

For details on how to enable Direct Connect, see the *Direct Connect User Guide*.

3.4 Step 2: Buy an EIP

Scenarios

Buy an EIP for a NAT gateway to allow servers that are connected to the cloud using Direct Connect to communicate with the Internet.

Procedure

For details, see [Assigning an EIP](#).

You do not need to bind the EIP to any server.

3.5 Step 3: Buy a Public NAT Gateway

Scenarios

Buy a public NAT gateway.

Prerequisites

- You have created the VPC and subnet required for buying a public NAT gateway.
- 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.

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 **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
4. On the displayed page, click **Buy Public NAT Gateway**.
5. Configure required parameters. For details, see [Table 3-1](#).

Table 3-1 Descriptions of public NAT gateway parameters

Parameter	Description
Billing Mode	Public NAT gateways are billed on a pay-per-use 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 you buy the public NAT gateway. NOTE 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.

Parameter	Description
Subnet	The subnet 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 specifications of the public NAT gateway The value can be Small , Medium , Large , or Extra-large .
Enterprise Project	The enterprise project that the public NAT gateway belongs to If an enterprise project has been configured, select the 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.


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

6. Click **Next**. On the page displayed, confirm the public NAT gateway specifications.
7. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a public NAT gateway.
8. In the public NAT gateway list, check the gateway status.

After the public NAT gateway is created, check whether a default route (0.0.0.0/0) that points to the public NAT gateway exists in the default route table of the VPC where the public NAT gateway is. If no, add a route pointing to the public NAT gateway to the default route table, alternatively, create a custom route table and add the default route 0.0.0.0/0 pointing to the public NAT gateway to the table. The following describes how to add a route to a custom route table.

Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.

2. Click  in the upper left corner and select the desired region and project.
3. Under **Networking**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. On the **Route Tables** page, click **Create Route Table** in the upper right corner.

VPC: Select the VPC to which the public NAT gateway belongs.

NOTE

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

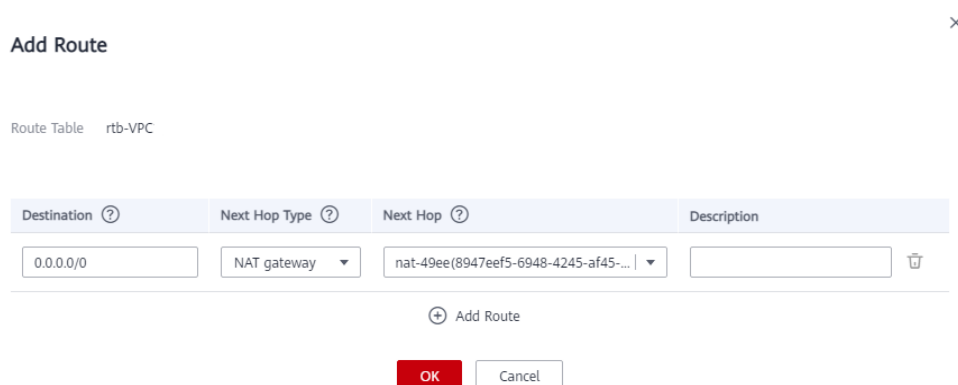
6. After the custom route table is created, click its name.
The **Summary** page is displayed.
7. Click **Add Route** and configure parameters as follows:

Destination: Set it to **0.0.0.0/0**.

Next Hop Type: Select **NAT gateway**.

Next Hop: Select the created NAT gateway.

Figure 3-2 Add Route



The screenshot shows the 'Add Route' dialog box. At the top, it says 'Add Route' with a close button (X). Below that, it indicates 'Route Table rtb-VPC'. The main area contains a table with the following columns: Destination, Next Hop Type, Next Hop, and Description. The 'Destination' field contains '0.0.0.0/0', 'Next Hop Type' is a dropdown menu set to 'NAT gateway', 'Next Hop' is a dropdown menu set to 'nat-49ee(8947eef5-6948-4245-af45-...)', and 'Description' is empty. Below the table is an 'Add Route' button with a plus sign. At the bottom, there are 'OK' and 'Cancel' buttons.

8. Click **OK**.

3.6 Step 4: Add an SNAT Rule

Scenarios

After a public NAT gateway is created, add SNAT rules for it. With SNAT rules, servers that are connected to a VPC using Direct Connect can access the Internet by sharing an EIP.

Each SNAT rule is configured for only one CIDR block. If servers that are connected to a VPC using Direct Connect are in multiple CIDR blocks, you can create multiple SNAT rules to allow the servers to share EIPs.

Prerequisites

A public NAT gateway is available.

Procedure


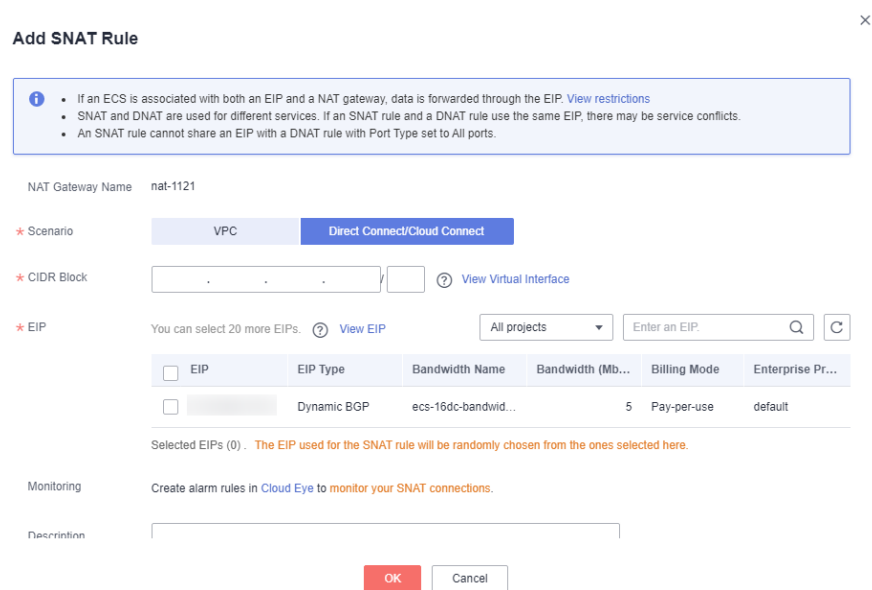
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
4. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

Figure 3-3 Add SNAT Rule



Add SNAT Rule

Info

- If an ECS is associated with both an EIP and a NAT gateway, data is forwarded through the EIP. [View restrictions](#)
- 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.

NAT Gateway Name: nat-1121

* Scenario: VPC Direct Connect/Cloud Connect

* CIDR Block: [View Virtual Interface](#)

* EIP: You can select 20 more EIPs. [View EIP](#) All projects Enter an EIP

<input type="checkbox"/> EIP	EIP Type	Bandwidth Name	Bandwidth (Mb...)	Billing Mode	Enterprise Pr...
<input type="checkbox"/>	Dynamic BGP	ecs-16dc-bandwid...	5	Pay-per-use	default

Selected EIPs (0). The EIP used for the SNAT rule will be randomly chosen from the ones selected here.

Monitoring: Create alarm rules in [Cloud Eye](#) to monitor your SNAT connections.

Description:

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

Table 3-2 Descriptions of SNAT rule parameters

Parameter	Description
Scenario	Select Direct Connect/Cloud Connect if your on-premises servers or servers in another VPC need to access the Internet.
CIDR Block	The CIDR block of the servers in the on-premises data center or in another VPC

Parameter	Description
EIP	The EIP used for accessing the Internet You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with Port Type set to Specific port , or has been bound to an SNAT rule of the current public NAT gateway. You can select up to 20 EIPs for an SNAT rule. If you have selected multiple EIPs for an SNAT rule, one EIP will be chosen randomly.
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	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

7. Click **OK**.
8. View details in the SNAT rule list.

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

NOTE

- You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.
- Each VPC can be associated with multiple public NAT gateways.
- Only one SNAT rule can be added for each VPC subnet.

3.7 Step 5: Add a DNAT Rule

Scenarios


After a public NAT gateway is created, add DNAT rules to allow servers in your on-premises data center to provide services accessible from the Internet.

You can configure a DNAT rule for each port on a server. If there are multiple servers, you can create multiple DNAT rules.

Prerequisites

A public NAT gateway 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. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
4. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. Click **Add DNAT Rule**.

Figure 3-4 Add DNAT Rule

Add DNAT Rule

Info:

- If your ECS has an EIP bound, you do not need to add a DNAT rule. If you do, the forwarded DNAT packets may be interrupted. [View restrictions](#)
- You need to add security group rules to allow inbound or outbound traffic after you add a DNAT rule. [Manage security group rules](#)
- 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.

NAT Gateway Name: nat-1121

* Scenario: VPC Direct Connect/Cloud Connect

* Port Type: Specific port All ports

* Protocol: TCP

* EIP: (5 Mbit/s | Pay-per-use | default) [View EIP](#)

Bandwidth: 5 Mbit/s Billing Mode: Pay-per-use Enterprise Project: default

* Outside Port:

* Private IP Address: [View Virtual Interface](#)

* Inside Port:

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

Table 3-3 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	Select Direct Connect/Cloud Connect if servers in your on-premises data center or in another VPC need to provide services accessible from the Internet.

Parameter	Description
Port Type	<p>The port type</p> <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	<p>The protocol can be TCP or UDP.</p> <p>This parameter is available if you select Specific port for Port Type. If you select All ports, the value of this parameter is All by default.</p>
EIP	<p>The EIP of the public NAT gateway</p> <p>You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with Port Type set to Specific port, or has been bound to an SNAT rule of the current public NAT gateway.</p>
Outside Port	<p>The port of the EIP used by the NAT gateway for external communications</p> <p>This parameter is only available if you select Specific port for Port Type.</p> <p>Range: 1 to 65535</p> <p>You can enter a specific port number or a port range, for example, 80 or 80-100.</p>
Private IP Address	<p>The IP address of the server that processes matching packets where requests will be forwarded to</p> <p>This IP address is used by local servers that are connected to a VPC through Direct Connect or servers in another VPC to provide services accessible from the Internet through DNAT. Configure the port of Private IP Address if you select Specific port for Port Type.</p> <p>This IP address is used by the server to provide services accessible from the Internet through DNAT.</p>
Inside Port	<p>The port of the server over which the originating requests will be forwarded</p> <p>This parameter is only available if you select Specific port for Port Type.</p> <p>Range: 1 to 65535</p> <p>You can enter a specific port number or a port range, for example, 80 or 80-100.</p>

Parameter	Description
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

8. Click **OK**.
9. View details in the DNAT rule list.
If **Status** is **Running**, the rule has been added.

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.

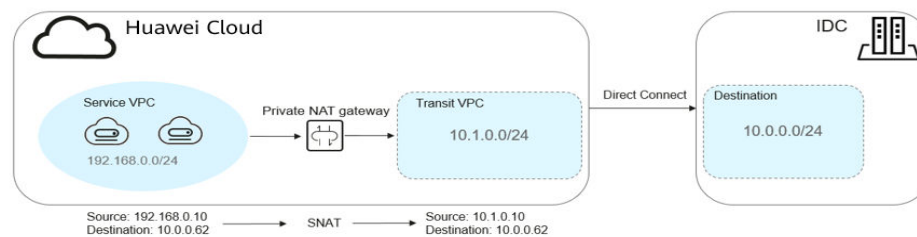
4 Using Private NAT Gateways to Enable Communications Between Cloud and On-premises Networks

4.1 Overview

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 4-1 Networking diagram

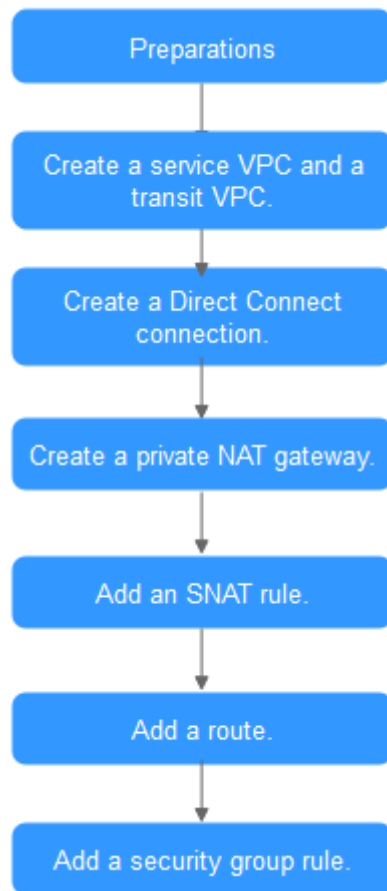


In this example, the CIDR block of your on-premises data center is 10.0.0.0/24. The subnet of the transit VPC in the **CN-Hong Kong** region is 10.1.0.0/24.

How networks are connected to each other

1. Your on-premises data center is connected to the transit VPC using Direct Connect.
2. The VPC where your services are deployed is connected to the transit VPC using a private NAT gateway.

This following figure shows the procedure.

Figure 4-2 Procedure

4.2 Preparations

Before you use a public NAT gateway, complete operations described in this section.

Registering an Account and Completing Real-Name Authentication

Skip this part if you already have an account of Huawei Cloud and completed real-name authentication. If you do not have an account of Huawei Cloud, perform the following steps to create one:

1. Visit the [Huawei Cloud official website](#) and click **Register**.
2. On the displayed page, register an account as prompted.
After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in [Individual Real-Name Authentication](#).

NOTE

Real-name authentication is required only when your account purchases or uses resources in the Chinese Mainland regions.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For pricing details about public NAT gateways, see [Product Pricing Details](#).
- To top up an account, see [Topping Up an Account \(Prepaid Direct Customers\)](#).

4.3 Step 1: Create a Service VPC and a Transit VPC

Scenarios

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

Procedure

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

4.4 Step 2: Create a Direct Connect Connection

Scenarios

Create a Direct Connect connection to link your on-premises data center to the cloud (the **CN-Hong Kong** region).

Procedure

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](#).

4.5 Step 3: Buy a Private NAT Gateway

Scenarios

To enable communications between your service VPC and a remote private network or VPC, buy a private NAT gateway.

Prerequisites

You have determined the transit IP addresses to be used for NAT in the transit 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 **NAT Gateway**. In the navigation pane on the left, choose **Private NAT Gateways**. The **Private NAT Gateways** page is displayed.
4. Click **Buy Private NAT Gateway** in the upper right corner.
5. Configure required parameters. For details, see [Table 4-1](#).

Table 4-1 Descriptions of private NAT gateway parameters

Parameter	Description
Billing Mode	The billing mode of the private NAT gateway
Region	The region where the private NAT gateway is located
Name	The name of the private NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed.
VPC	The service VPC that the private NAT gateway belongs to The selected VPC cannot be changed after the private NAT gateway is purchased.
Subnet	The subnet of the service VPC The subnet must have at least one available IP address. The selected subnet cannot be changed after the private NAT gateway is purchased.
Specifications	The specifications of the private NAT gateway The value can be Small , Medium , Large , or Extra-large .
Description	Supplementary information about the private NAT gateway Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. Click **Buy Now**.
7. In the private NAT gateway list, check the gateway status.
8. On the **Private NAT Gateways** page, click **Transit IP Addresses**.

Figure 4-3 Assign Transit IP Address

Assign Transit IP Address

The screenshot shows a configuration dialog titled "Assign Transit IP Address". It contains the following elements:

- Transit VPC:** A dropdown menu with "vpc-b15d" selected and a refresh icon.
- Transit Subnets:** A dropdown menu with "subnet-b172(10.0.0.0/24)" selected and a refresh icon.
- Transit IP Address:** Two radio buttons, "Automatic" (selected) and "Manual".
- Enterprise Project:** A dropdown menu with "--Select--" and a refresh icon, followed by a link "Create Enterprise Project" with a help icon.
- Buttons:** A red "OK" button and a white "Cancel" button.

9. Configure required parameters. For details, see [Table 4-2](#).

Table 4-2 Parameter descriptions of a transit IP address

Parameter	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	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.
IP Address	This parameter is only available when you set Transit IP Address to Manual .
Enterprise Project	Specifies the enterprise project to which the transit IP address belongs.

10. Set **Transit IP Address** to **Automatic** and click **OK**.

4.6 Step 4: Add an SNAT Rule

Scenarios

After the private NAT gateway is created, add an SNAT rule so that some or all servers in a VPC subnet can share a transit IP address to access on-premises data centers or other VPCs.

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 **NAT Gateway**. In the navigation pane on the left, choose **Private NAT Gateways**. The **Private NAT Gateways** page is displayed.
4. In the private NAT gateway list, click the name of the private NAT gateway that you want to add an SNAT rule for.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

Figure 4-4 Add SNAT Rule

Add SNAT Rule

Local Network

Private NAT Gateway Name private-nat-test-

Local VPC vpc-3

* Subnet Existing Custom

Monitoring You are advised to create alarm rules in [Cloud Eye](#) to monitor your SNAT connections.

Transit Network

* Transit IP Address

Transit IP Addr...	Status	Transit VPC	Transit Subnets	Enterprise Pro...	Assigned
<input type="radio"/> 10.0.0.0/24	<input checked="" type="checkbox"/> Running	vpc-3	sub-10.0.0.0/24	default	Nov 29, 2022 1...

6. Configure required parameters. For details, see [Table 4-3](#).

Table 4-3 Description

Parameter	Description
Subnet	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 3: Buy a Private NAT Gateway
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

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

4.7 Step 5: Add a Route

Scenarios

After the private NAT gateway is configured, add a route in the route table of the service VPC to point to the private 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 route table associated the service VPC.
6. Click **Add Route** and configure required parameters.

Figure 4-5 Add Route

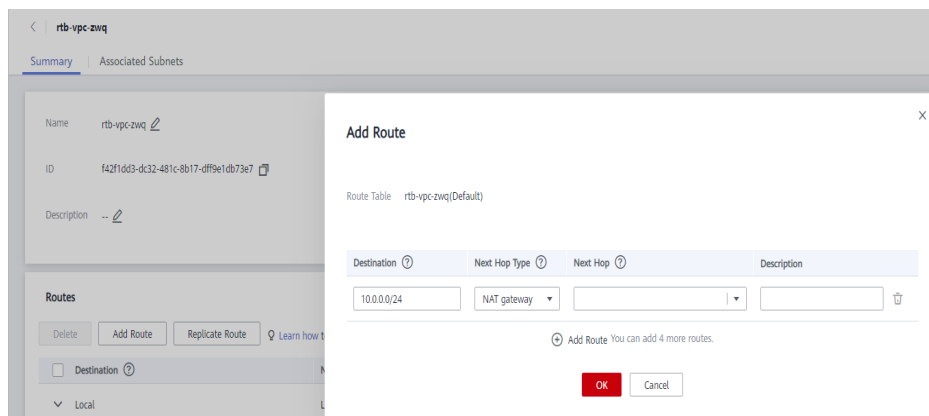


Table 4-4 Parameter descriptions

Parameter	Description
Destination	The destination CIDR block Set it to the CIDR block used by your on-premises data center.
Next Hop Type	Set it to NAT gateway .
Next Hop	Set Next Hop to the private NAT gateway.
Description	(Optional) Supplementary information about the route Enter up to 255 characters. Angle brackets (< or >) are not allowed.


7. Click **OK**.

4.8 Step 6: Add a Security Group Rule

Scenarios

Add an inbound security group rule to allow traffic to servers in the destination 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 **Access Control > Security Groups**. The security group list is displayed.

5. Locate the row that contains the target security group, and click **Manage Rule** in the **Operation** column.

The page for configuring security group rules is displayed.

6. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, configure required parameters.

You can click + to add more inbound rules.

Figure 4-6 Add Inbound Rule

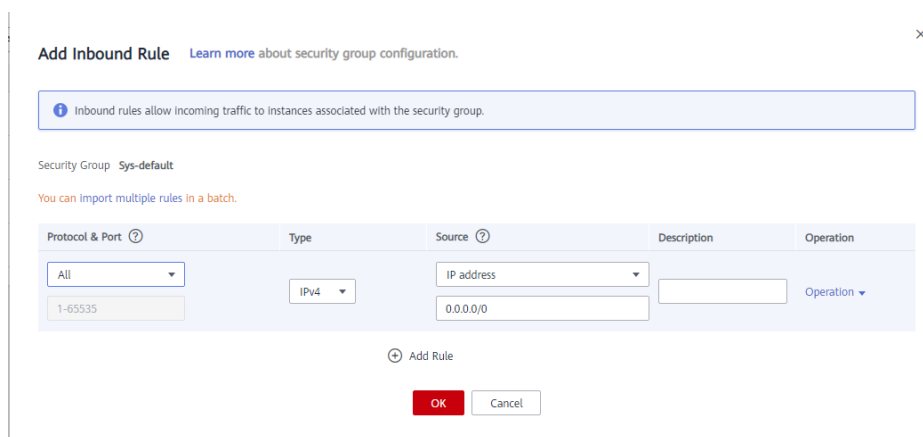


Table 4-5 Inbound rule parameter descriptions

Parameter	Description	Example Value
Protocol & Port	Protocol: network protocol The protocol can be All , TCP , UDP , ICMP , or GRE .	TCP
	Port: the port or port range over which the traffic can reach your ECS Supported range: 1 to 65535	22 or 22-30
Type	The IP address type. This parameter is available after the IPv6 function is enabled. <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4

Parameter	Description	Example Value
Source	<p>The source of the security group rule</p> <p>The source can be an IP address, an IP address group, or a security group to allow access from IP addresses or instances in another security group. For example:</p> <ul style="list-style-type: none"> • <i>xxx.xxx.xxx.xxx/32</i> (an IPv4 address) • <i>xxx.xxx.xxx.0/24</i> (a subnet) • 0.0.0.0/0 (all IP addresses) • sg-abc (a security group) <p>For more information about IP address groups, see IP Address Group Overview.</p>	0.0.0.0/0
Description	<p>(Optional) Supplementary information about the security group rule</p> <p>Enter up to 255 characters. Angle brackets (< or >) are not allowed.</p>	N/A

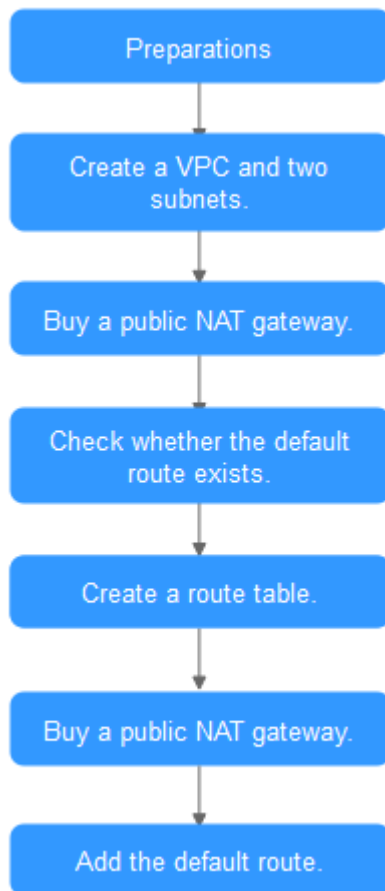
7. Click **OK**.

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

5.1 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 5-1 Procedure

5.2 Preparations

Before you use a public NAT gateway, complete operations described in this section.

Registering an Account and Completing Real-Name Authentication

Skip this part if you already have an account of Huawei Cloud and completed real-name authentication. If you do not have an account of Huawei Cloud, perform the following steps to create one:

1. Visit the [Huawei Cloud official website](#) and click **Register**.
2. On the displayed page, register an account as prompted.
After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in [Individual Real-Name Authentication](#).

NOTE

Real-name authentication is required only when your account purchases or uses resources in the Chinese Mainland regions.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For pricing details about public NAT gateways, see [Product Pricing Details](#).
- To top up an account, see [Topping Up an Account \(Prepaid Direct Customers\)](#).

5.3 Step 1: Create a VPC and Two Subnets

Scenarios

Create one VPC and two subnets.

Procedure

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

5.4 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. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
4. On the displayed page, click **Buy Public NAT Gateway**.
5. Configure required parameters. For details, see [Table 5-1](#).
Select the VPC and subnet you created in [Step 1: Create a VPC and Two Subnets](#) for **VPC** and **Subnet**.

Table 5-1 Descriptions of public NAT gateway parameters

Parameter	Description
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.

Parameter	Description
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.
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.

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** to create a public NAT gateway.

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


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

5.5 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.

5.6 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 5-2 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 (< or >) 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**.

5.7 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. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

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

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

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

Table 5-3 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** to create a public NAT gateway.
It takes 1 to 6 minutes to create a public NAT gateway.
8. In the list, view the status of the public NAT gateway.

5.8 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 5-4 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 (< or >) are not allowed.	N/A

7. Click **OK**.

6 Change History

Released On	What's New
2022-11-29	<p>This issue is the fourth official release, which incorporates the following change:</p> <p>Updated Step 3: Buy a Private NAT Gateway and Step 4: Add an SNAT Rule to match the newly released UI. The new UI does not have the Transit Subnets tab, but allows you to select a transit VPC and transit subnet when assigning a transit IP address.</p>
2022-08-05	<p>This issue is the third official release, which incorporates the following change:</p> <p>Updated the real-name authentication requirements in the following sections:</p> <ul style="list-style-type: none">• Preparations• Preparations• Preparations• Preparations• Preparations
2020-05-08	<p>This issue is the second official release, which incorporates the following change:</p> <p>Added description about SNAT rules and DNAT rules based on console changes.</p>
2018-11-16	<p>This issue is the first official release.</p>