NAT Gateway

User Guide

Issue	01
Date	2020-07-18



HUAWEI TECHNOLOGIES CO., LTD.

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

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Public NAT Gateway 1
1.1 Public NAT Gateway Overview 1
1.2 Managing Public NAT Gateways 2
1.2.1 Buying a Public NAT Gateway 2
1.2.2 Viewing a Public NAT Gateway 4
1.2.3 Modifying a Public NAT Gateway 5
1.2.4 Deleting a Public NAT Gateway 6
1.3 Managing SNAT Rules 7
1.3.1 Adding an SNAT Rule 7
1.3.2 Viewing an SNAT Rule 9
1.3.3 Modifying an SNAT Rule 10
1.3.4 Deleting an SNAT Rule 10
1.4 Managing DNAT Rules 11
1.4.1 Adding a DNAT Rule 11
1.4.2 Viewing a DNAT Rule 14
1.4.3 Modifying a DNAT Rule 14
1.4.4 Deleting a DNAT Rule 15
1.4.5 Deleting DNAT Rules in Batches 15
1.4.6 Importing and Exporting DNAT Rules Using Templates 16
2 Private NAT Gateway (OBT) 19
2.1 Private NAT Gateway Overview 19
2.2 Managing Private NAT Gateways 20
2.2.1 Buying a Private NAT Gateway 20
2.2.2 Viewing a Private NAT Gateway 21
2.2.3 Modifying a Private NAT Gateway 22
2.2.4 Deleting a Private NAT Gateway 22
2.3 Managing SNAT Rules 23
2.3.1 Adding an SNAT Rule 23
2.3.2 Viewing an SNAT Rule 24
2.3.3 Modifying an SNAT Rule 25
2.3.4 Deleting an SNAT Rule 25
2.4 Managing DNAT Rules 26
2.4.1 Adding a DNAT Rule 26

 Copyright © Huawei Technologies Co., Ltd.

2.4.2 Viewing a DNAT Rule....28
2.4.3 Modifying a DNAT Rule....28
2.4.4 Deleting a DNAT Rule....29
2.5 Managing Transit Subnets....29
2.6 Connecting to an On-premises Data Center or a Remote VPC....31
3 Permissions Management....33
3.1 Creating a User and Granting NAT Gateway Permissions....33
3.2 NAT Gateway Custom Policies....34
4 Monitoring Management....37
4.1 Supported Metrics....37
4.2 Creating Alarm Rules....42
4.3 Viewing Metrics....43
A Change History....44

 Copyright © Huawei Technologies Co., Ltd.

1 Public NAT Gateway

1.1 Public NAT Gateway Overview

Public NAT gateways provide network address translation (NAT) with 10 Gbit/s of bandwidth for servers in a Virtual Private Cloud (VPC), such as Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), and Workspace desktops, or servers that connect to a VPC through Direct Connect or Virtual Private Network (VPN) in local data centers, allowing these servers to share elastic IP addresses (EIPs) to access the Internet or to provide services accessible from the Internet.

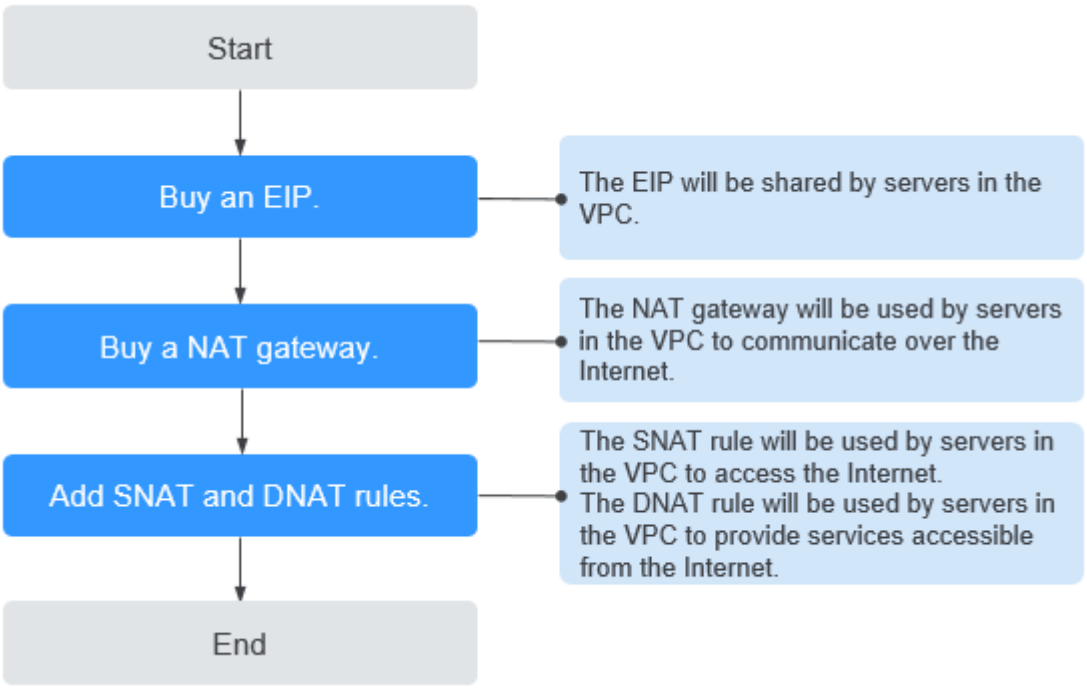
NOTE

Private NAT gateways are currently available for open beta test in regions **CN North-Beijing4**, **CN East-Shanghai1**, and **CN South-Guangzhou**. All NAT gateways refer to public NAT gateways in **Public NAT Gateway**.

The process of using a public NAT gateway is as follows:

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 Process of using a public NAT gateway



1.2 Managing Public NAT Gateways

1.2.1 Buying a Public NAT Gateway

Scenarios

This section describes how to buy a public NAT gateway to enable your servers to access the Internet or to provide services for external networks.

Prerequisites

- When buying a public NAT gateway, you must specify its VPC, subnet, and type.
- Check whether the default route (0.0.0.0/0) of the VPC has been used by other gateways. If the default route of the VPC has been used by other gateways, add another route for this gateway or add the default route to a new route table to be associated with the gateway after the gateway is created.

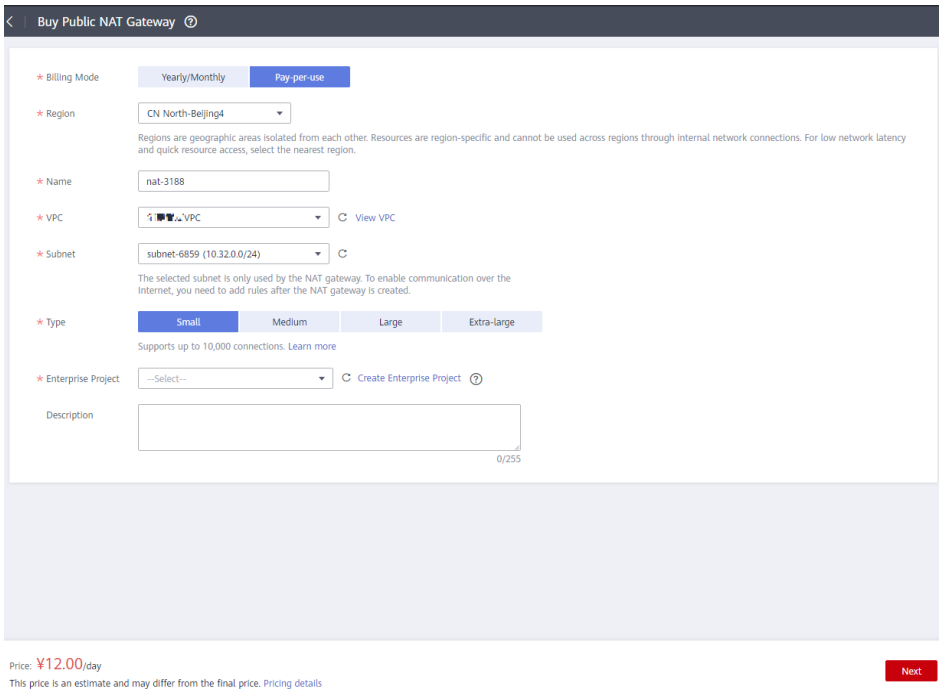
Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.

 Copyright © Huawei Technologies Co., Ltd.

4. On the displayed page, click **Buy Public NAT Gateway**.

Figure 1-2 Buy Public NAT Gateway



5. Set the parameters as prompted. For details, see **Table 1-1**.

Table 1-1 Parameter description

Parameter	Description
Region	The region where the public NAT gateway is located.
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.
Name	The name of the public NAT gateway. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The VPC that the public NAT gateway belongs to. Check whether the default route (0.0.0.0/0) of the VPC has been used by other gateways. If the default route of the VPC has been used by other gateways, add another route for this gateway or add the default route to a new route table to be associated with the gateway after the gateway is created. The selected VPC cannot be changed after the public NAT gateway is purchased.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
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.
Type	The type of the public NAT gateway. The type can be **Small**, **Medium**, **Large**, and **Extra-large**. You can click **Learn more** on the page to view details about each type.
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 do not specify an enterprise project, the **default** enterprise project will be used.
Description	Supplementary information about the public NAT gateway. The description can contain up to 255 characters.
Required Duration	The required duration of the public NAT gateway.

After these parameters are set, the public NAT gateway price will be displayed. You can click **Pricing details** on the page to view pricing details.

6. Click **Next**. The page for you to confirm the public NAT gateway specifications is displayed.
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, you can see the public NAT gateway status.

1.2.2 Viewing a Public NAT Gateway

Scenarios

After a public NAT gateway is created, you can view details about the gateway.

Prerequisites

A public NAT gateway has been created.

Procedure

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

 Copyright © Huawei Technologies Co., Ltd.

3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the target public NAT gateway.
5. View the public NAT gateway details on the displayed page.

1.2.3 Modifying a Public NAT Gateway

Scenarios

This section describes how to modify the name, type, or description of a public NAT gateway.

Increasing the size of the NAT gateway type does not affect services, but if you switch to a smaller NAT gateway, make sure the reduced capacity will still be enough to meet your service requirements.

The connections supported by a yearly/monthly NAT gateway cannot be decreased.

If you change the billing mode of a NAT gateway from yearly/monthly to pay-per-use, the pay-per-use billing mode takes effect only after the yearly/monthly billing mode expires. If you change the billing mode of a NAT gateway from pay-per-use to yearly/monthly, the new billing mode will take effect immediately.

Prerequisites

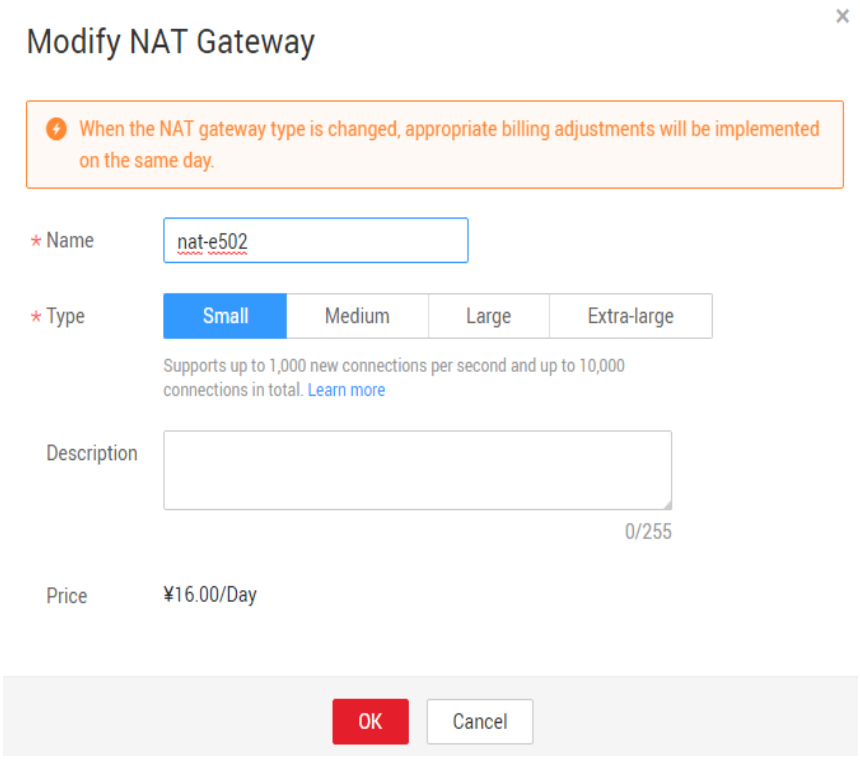
A public NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, locate the row that contains the target public NAT gateway and click **Modify** in the **Operation** column.
5. Modify the name, type, or description of the public NAT gateway as prompted.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-3 Modify NAT Gateway



6. Click **OK**.

1.2.4 Deleting a Public NAT Gateway

Scenarios

You can delete public NAT gateways that are no longer required to release resources, saving costs.

Prerequisites

All SNAT and DNAT rules created on the public NAT gateway have been deleted.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, locate the row that contains the target public NAT gateway and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **Yes**.

 Copyright © Huawei Technologies Co., Ltd.

1.3 Managing SNAT Rules

1.3.1 Adding an SNAT Rule

Scenarios

After the public NAT gateway is created, you need to add SNAT rules. With the SNAT rule, servers in a VPC subnet or servers that are connected to a VPC through Direct Connect or VPN can access the Internet by sharing an EIP.

Each SNAT rule is configured for one subnet. If there are multiple subnets in a VPC, you can create several SNAT rules to allow them to share EIPs.

Prerequisites

- A public NAT gateway has been created.
- A Direct Connect connection has been created. Its VPC CIDR block has been set to **0.0.0.0/0** when you configure the virtual gateway. For details, see **Creating a Virtual Gateway**.

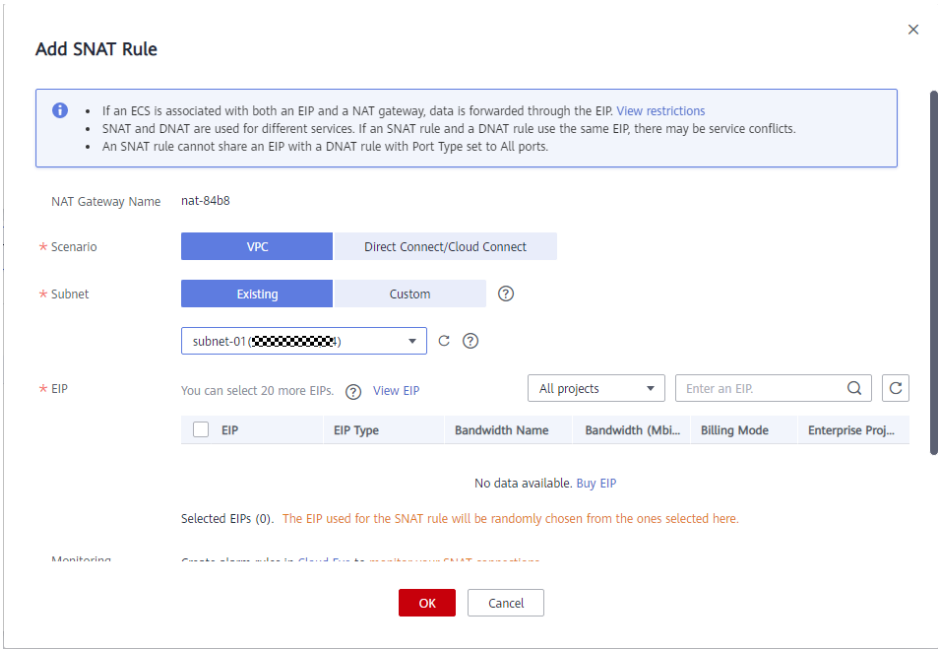
Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the public NAT gateway for which you want to add the SNAT rule.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-4 Add SNAT Rule



6. Specify the parameters as prompted. For details, see **Table 1-2**.

Table 1-2 Parameter descriptions

Parameter	Condition	Description
Scenario	N/A	The scenarios where the SNAT rule is used. Select **VPC** if your servers in a VPC need to access the Internet. Select **Direct Connect/Cloud Connect** if the servers that are connected to a VPC through Direct Connect or VPN in your data center need to access the Internet.
Subnet	This parameter is available only when you select **VPC** for **Scenario**.	Select a subnet or enter a CIDR block in which servers can access the Internet through the SNAT rule.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Condition	Description
EIP	• This parameter is available when you select **VPC** for **Scenario**. • This parameter is available when you select **Direct Connect/Cloud Connect** for **Scenario**.	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 with **Port Type** set to **Specific port** of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway. You can select multiple EIPs at once. Up to 20 EIPs can be selected for each SNAT rule. The EIP used for the SNAT rule is randomly chosen from the ones you select when you add the rule.
Monitoring	N/A	Alarm rules are created in Cloud Eye. The alarm rules help you monitor your SNAT connections and keep you informed of any changes in a timely manner.
Description	N/A	Supplementary information about the public NAT gateway. The description can contain up to 255 characters.

7. Click **OK**.

   NOTE

   You can add multiple SNAT rules for a NAT gateway to suite your service requirements.

1.3.2 Viewing an SNAT Rule

Scenarios

After you add an SNAT rule to a public NAT gateway, you can view the details about the SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

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

 Copyright © Huawei Technologies Co., Ltd.

3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the target public NAT gateway.
5. In the SNAT rule list, view the details about the SNAT rule.

1.3.3 Modifying an SNAT Rule

Scenarios

After an SNAT rule is added, you can modify parameters in the SNAT rule as required.

Prerequisites

An SNAT rule has been added for 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. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the target public NAT gateway.
5. On the SNAT Rules tab, locate the row that contains the target SNAT rule to be modified.
6. Click **Modify** in the **Operation** column.
7. In the displayed dialog box, modify the required parameters.
8. Click **OK**.

1.3.4 Deleting an SNAT Rule

Scenarios

Delete the SNAT rules that you no longer need.

Prerequisites

An SNAT rule has been added for the public NAT gateway.

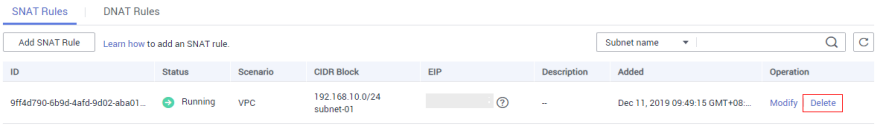
Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the target public NAT gateway.

 Copyright © Huawei Technologies Co., Ltd.

5. In the SNAT rule list, locate the row that contains the target SNAT rule and click **Delete** in the **Operation** column.

   Figure 1-5 Deleting an SNAT Rule

6. In the displayed dialog box, click **Yes**.

1.4 Managing DNAT Rules

1.4.1 Adding a DNAT Rule

Scenarios

After a public NAT gateway is created, you can 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 of a server. If multiple servers need to provide services accessible from the Internet, you need to create multiple DNAT rules.

Prerequisites

A NAT gateway has been created.

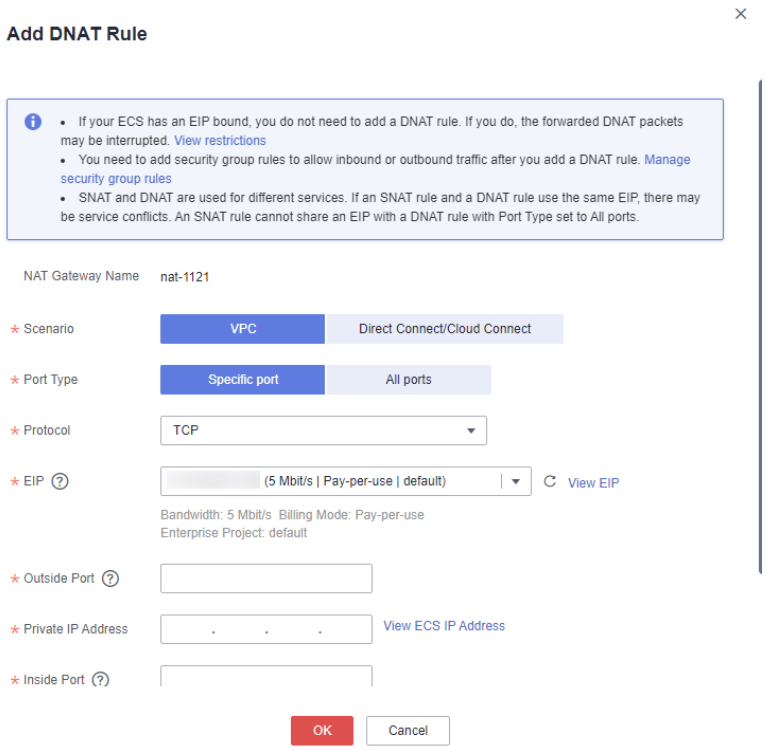
Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the public NAT gateway for which you want to add the DNAT rule.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. Click **Add DNAT Rule**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-6 Add DNAT Rule



NOTICE

You need to add security group rules to allow inbound or outbound traffic after you add a DNAT rule. Otherwise, the DNAT rule does not take effect.

7. Set the parameters as prompted. For details, see **Table 1-3**.

Table 1-3 Parameter descriptions

Parameter	Description
Scenario	**VPC**: The servers in a VPC can share an EIP to provide services accessible from the Internet through the DNAT rule. **Direct Connect/Cloud Connect**: Servers in your data center connected to a VPC using Direct Connect or Cloud Connect can provide services accessible from the Internet through the DNAT rule.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Port Type	The port type. You can select **All ports** or **Specific port**. • **All ports**: This is equivalent to assigning an EIP to a server. Any requests on the EIP will be forwarded by the NAT gateway to your server based on IP address mapping. • **Specific port**: The public NAT gateway only forwards requests with a specific protocol and port on the EIP to the corresponding port of the target 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**, this parameter is **All** by default.
EIP	The EIP that will be used by the server to provide services accessible from the Internet. You can select an EIP that either is not bound to any resource, has been bound to a DNAT rule with **Port Type** set to **Specific port** of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.
Outside Port	The port of the EIP. This parameter is available if you select **Specific port** for **Port Type**. The port number must range from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Private IP Address	• In a VPC scenario, set this parameter to the IP address of the server in a VPC. This IP address is used by the server to provide services accessible from the Internet through DNAT. • In a Direct Connect scenario, set this parameter to IP address of the server in the local data center or the user's private IP address. This IP address is used by local servers that are connected to a VPC through Direct Connect or Cloud Connect to provide services accessible from the Internet through DNAT. • Configure the port of **Private IP Address** if you select **Specific port** for **Port Type**.
Inside Port	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 must range from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Description	Supplementary information about the DNAT rule. The description can contain up to 255 characters.

 Copyright © Huawei Technologies Co., Ltd.

8. After the configuration is complete, click **OK**. Once the rule is created, its status changes to **Running**.

1.4.2 Viewing a DNAT Rule

Scenarios

After you add a DNAT rule to a public NAT gateway, you can view the details about the DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the target public NAT gateway.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, view the details about the DNAT rule.

1.4.3 Modifying a DNAT Rule

Scenarios

After a DNAT rule is added, you can modify parameters in the DNAT rule as required.

Prerequisites

A public DNAT rule has been added for the 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. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the target public NAT gateway.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, locate the row that contains the target DNAT rule and click **Modify** in the **Operation** column.
7. In the displayed dialog box, modify the required parameters.
8. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

1.4.4 Deleting a DNAT Rule

Scenarios

Delete a DNAT rule that you no longer need.

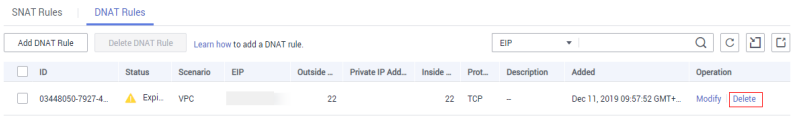
Prerequisites

A public DNAT rule has been added for the 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. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the target public NAT gateway.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, locate the row that contains the target DNAT rule and click **Delete** in the **Operation** column.

   Figure 1-7 Deleting a DNAT rule

7. In the displayed dialog box, click **Yes**.

1.4.5 Deleting DNAT Rules in Batches

Scenarios

Delete the DNAT rules that you no longer need.

Prerequisites

DNAT rules have been added for 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. Under **Network**, click **NAT Gateway**.
   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the target public NAT gateway.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.

 Copyright © Huawei Technologies Co., Ltd.

6. In the DNAT rule list, select the target DNAT rules and click **Delete DNAT Rule**.
7. In the displayed dialog box, click **Yes**.

1.4.6 Importing and Exporting DNAT Rules Using Templates

Scenarios

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

A DNAT rule is configured for one server. If there are multiple servers, you need to create multiple DNAT rules.

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   Switch to the public NAT gateway page.
4. On the displayed page, click the name of the public NAT gateway for which you want to add the DNAT rule.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. On the displayed page, click **Import Rule** and then **Download Template**.
7. Fill in DNAT rule parameters based on the table heading in the template. For details, see **Table 1-4**.

Table 1-4 Parameter descriptions

Parameter	Description
Scenario	**VPC**: The servers in a VPC can share an EIP to provide services accessible from the Internet through the DNAT rule. **Direct Connect/Cloud Connect**: On-premises servers that are connected to a VPC through Direct Connect or Cloud Connect can provide services accessible from the Internet through the DNAT rule.

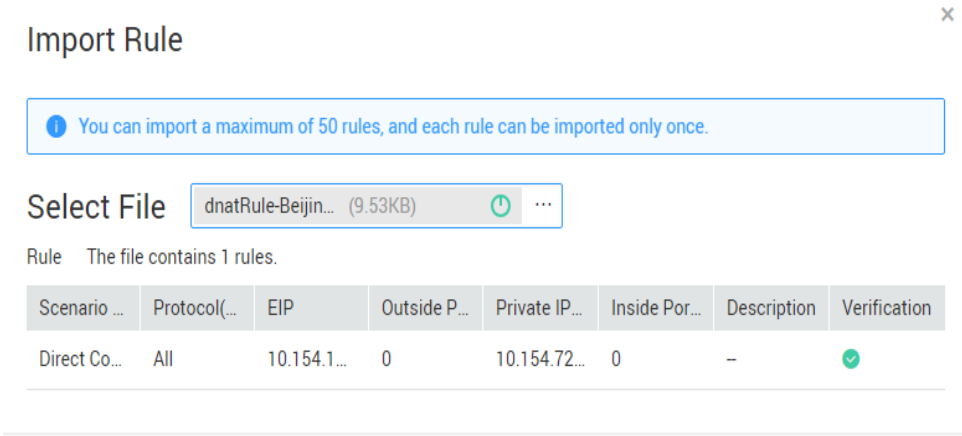
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Port Type	The port type. You can select **All ports** or **Specific port**. • **All ports**: This is equivalent to assigning an EIP to a server. Any requests on the EIP will be forwarded by the NAT gateway to your server based on IP address mapping. • **Specific port**: indicates the port mapping method. The public NAT gateway only forwards requests with a specific protocol and port on the EIP to the corresponding port of the target 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**, this parameter is **All** by default.
EIP	The EIP that will be used by the server to provide services accessible from the Internet. Only EIPs that have not been bound or that have been bound to a DNAT rule in the current VPC are available for selection.
Outside Port	The EIP port. This parameter is available if you select **Specific port** for **Port Type**. You can enter a single port number or a port range, for example, 80 or 80-100.
Private IP Address	• In a VPC scenario, set this parameter to the IP address of the server in a VPC. This IP address is used by the server to provide services accessible from the Internet through DNAT. • In a Direct Connect scenario, set this parameter to IP address of the server in the local data center or the user's private IP address. This IP address is used by local servers that are connected to a VPC through Direct Connect or Cloud Connect to provide services accessible from the Internet through DNAT. • Configure the port of **Private IP Address** if you select **Specific port** for **Port Type**.
Inside Port	• In a VPC scenario, set this parameter to the port of the server in a VPC. • In a Direct Connect scenario, set this parameter to the port of the server in the local data center or the user's private port. • This parameter is available if you select **Specific port** for **Port Type**. The number of inside and outside ports must match.

8. After filling in the template, click **Import Rule**, select the template, and click **Import**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-8 Import Rule



9. View details in the DNAT rule list. If **Status** is **Running**, the rules have been added.
10. On the **DNAT Rules** tab page, click **Export Rule** to export the configured DNAT rule template.

 Copyright © Huawei Technologies Co., Ltd.

2 Private NAT Gateway (OBT)

2.1 Private NAT Gateway Overview

Private NAT gateways provide network address translation (NAT) for servers, such as ECSs, BMSs, and Workspace desktops, in a VPC, and allow multiple servers to share a private IP address to access or provide services accessible from an on-premises data center or a remote VPC.

A private NAT gateway allows network address translation between two VPCs or between a VPC and an on-premises network with no matter large, small, or overlapping network ranges. A private NAT gateway lets you avoid having to reconstruct services. It makes it safer and less expensive to migrate services to the cloud.

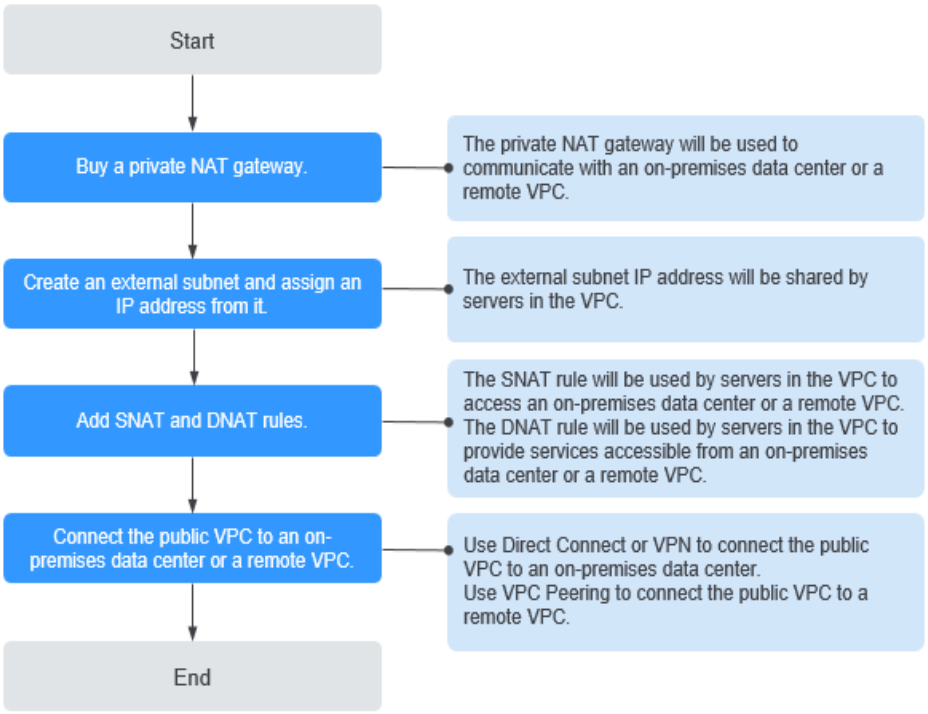
NOTE

Private NAT gateways are currently available for open beta test in regions **CN North-Beijing4**, **CN East-Shanghai1**, and **CN South-Guangzhou**.

The process of using a private NAT gateway is as follows:

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 Process of using a private NAT gateway



2.2 Managing Private NAT Gateways

2.2.1 Buying a Private NAT Gateway

Scenarios

You can buy a private NAT gateway and use it to access or provide services accessible from your on-premises data center or remote VPC.

NOTE

Private NAT gateways are currently available for open beta test in regions **CN North-Beijing4**, **CN East-Shanghai1**, and **CN South-Guangzhou**.

Prerequisites

- When buying a private NAT gateway, you must specify its VPC, subnet, and type.
- Ensure that the VPC does not have a default route. (This restriction does not apply to the **CN North-Beijing4** region.)

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

Copyright © Huawei Technologies Co., Ltd.

The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click **Buy Private NAT Gateway**.
6. Set the parameters as prompted. For details, see **Table 2-1**.

Table 2-1 Parameter descriptions

Parameter	Parameter descriptions
Region	The region where the private NAT gateway is located.
Name	The name of the private NAT gateway. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The 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 VPC 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.
Type	The type of the private NAT gateway. Four types of private NAT gateways are available, small, medium, large, and extra-large. For details, see **Product Specifications**.
Enterprise Project	The enterprise project that the private NAT gateway belongs to. If an enterprise project is configured for a private NAT gateway, the private NAT gateway belongs to this enterprise project.
Description	Supplementary information about the private NAT gateway. The description can contain up to 255 characters.

7. Click **Buy Now**.

2.2.2 Viewing a Private NAT Gateway

Scenarios

After a private NAT gateway is created, you can view details about the gateway.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A private NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the target private NAT gateway.
6. View the private NAT gateway details on the displayed page.

2.2.3 Modifying a Private NAT Gateway

Scenarios

This section describes how to modify the name, type, or description of a private NAT gateway.

Prerequisites

A private NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, locate the row that contains the target private NAT gateway and click **Modify** in the **Operation** column.
6. Modify the name, type, or description of the private NAT gateway as prompted.

2.2.4 Deleting a Private NAT Gateway

Scenarios

You can delete private NAT gateways that are no longer required to release resources, saving costs.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

All SNAT and DNAT rules created on the private NAT gateway have been deleted.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, locate the row that contains the target private NAT gateway and click **Delete** in the **Operation** column.
6. In the displayed dialog box, click **Yes**.

2.3 Managing SNAT Rules

2.3.1 Adding an SNAT Rule

Scenarios

After the private NAT gateway is created, you need to add SNAT rules. An SNAT rule allows all or some servers in a VPC subnet to access your on-premises data center or remote VPC by sharing a transit IP address.

Each SNAT rule is configured for one subnet. If there are multiple subnets in a VPC, you can create several SNAT rules to allow them to share transit IP addresses.

Prerequisites

- A private NAT gateway has been created.
- A Direct Connect connection has been created. Its VPC CIDR block has been set to **0.0.0.0/0** when you configure the virtual gateway. For details, see **Create a Virtual Gateway**.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the private NAT gateway for which you want to add the SNAT rule.

Copyright © Huawei Technologies Co., Ltd.

6. On the **SNAT Rules** tab, click **Add SNAT Rule**.
7. Specify the parameters as prompted. For details, see **Table 2-2**.

Table 2-2 Parameter descriptions

Parameter	Description
Type	You can set it to **Subnet** or **Custom** based on service requirements. • Select **Subnet** if all servers in a VPC subnet need to access an on-premises data center or a remote VPC through the SNAT rule. • Select **Custom** if specific servers in a VPC subnet need to access an on-premises data center or a remote VPC through the SNAT rule.
Subnet	The subnet in which servers can access an on-premises data center or a remote VPC through the SNAT rule.
Transit Subnet	A subnet that does not in the VPC selected when you create the private NAT gateway.
Transit IP Address	The transit IP address that is used to access an on-premises data center or a remote VPC. You can select a transit IP address that either is not bound to any resource, has been bound to a DNAT rule with **Port Type** set to **Specific port** of the current private NAT gateway, or has been bound to an SNAT rule of the current private NAT gateway.
Description	Supplementary information about the private NAT gateway. The description can contain up to 255 characters.

8. Click **OK**.

NOTE

You can add multiple SNAT rules for a private NAT gateway to suite your service requirements.

2.3.2 Viewing an SNAT Rule

Scenarios

After you add an SNAT rule to a private NAT gateway, you can view the details about the SNAT rule.

Prerequisites

An SNAT rule has been added.

Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the target private NAT gateway.
6. In the SNAT rule list, view the details about the SNAT rule.

2.3.3 Modifying an SNAT Rule

Scenarios

After an SNAT rule is added, you can modify parameters in the SNAT rule as required.

Prerequisites

An SNAT rule has been added for 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. Under **Network**, click **NAT Gateway**.
   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the target private NAT gateway.
6. On the **SNAT Rules** tab, locate the row that contains the target SNAT rule to be modified.
7. Click **Modify** in the **Operation** column.
8. In the displayed dialog box, modify the required parameters.
9. Click **OK**.

2.3.4 Deleting an SNAT Rule

Scenarios

Delete the SNAT rules that you no longer need.

Prerequisites

An SNAT rule has been added for the private NAT gateway.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the target private NAT gateway.
6. In the SNAT rule list, locate the row that contains the target SNAT rule and click **Delete** in the **Operation** column.
7. In the displayed dialog box, click **Yes**.

2.4 Managing DNAT Rules

2.4.1 Adding a DNAT Rule

Scenarios

After a private NAT gateway is created, you can add DNAT rules to allow servers in your VPC to provide services accessible from an on-premises server or a remote VPC.

You can configure a DNAT rule for each port of a server. If multiple servers need to provide services accessible from an on-premises server or a remote VPC, you need to create multiple DNAT rules.

Prerequisites

A private NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the private NAT gateway for which you want to add the DNAT rule.
6. On the private NAT gateway details page, click the **DNAT Rules** tab.
7. Click **Add DNAT Rule**.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

You need to add security group rules to allow inbound or outbound traffic after you add a DNAT rule. Otherwise, the DNAT rule does not take effect.

8. Set the parameters as prompted. For details, see **Table 2-3**.

Table 2-3 Parameter descriptions

Parameter	Description
Port Type	The port type. You can select **All ports** or **Specific port**. • **All ports**: If you select this option, a transit IP address is configured for your servers. Any requests on the transit IP address will be forwarded to your servers based on the IP address mapping. • **Specific port**: The NAT gateway only forwards requests with a specific protocol and port on the transit IP address to the corresponding port of the target server.
Protocol	The protocol can be TCP or UDP. If you select **All ports**, this parameter is **All** by default. This parameter is available if you select **Specific port** for **Port Type**.
Transit Subnet	A subnet that does not in the VPC selected when you create the private NAT gateway.
Transit IP Address	The transit IP address that is used to access an on-premises data center or a remote VPC. You can select a transit IP address that either is not bound to any resource, has been bound to a DNAT rule with **Port Type** set to **Specific port** of the current private NAT gateway, or has been bound to an SNAT rule of the current private NAT gateway.
External port	The port of the transit IP address. The port number must range from 1 to 65535. This parameter is available if you select **Specific port** for **Port Type**.
Instance Type	The type of the instance that provides services accessible from an on-premises server or a remote VPC. • Server • Virtual IP address • Load balancer
NIC	The NIC of the server. This parameter is available if you set **Instance Type** to **Server**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Internal Port	The port of the instance. The port number must range from 1 to 65535. This parameter is available if you select **Specific port** for **Port Type**.
Description	Supplementary information about the DNAT rule. The description can contain up to 255 characters.

9. After the configuration is complete, click **OK**. Once the rule is created, its status changes to **Running**.

2.4.2 Viewing a DNAT Rule

Scenarios

After you add a DNAT rule to a private NAT gateway, you can view the details about the DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.
   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the target private NAT gateway.
6. On the NAT gateway details page, click the **DNAT Rules** tab.
7. In the DNAT rule list, view the details about the DNAT rule.

2.4.3 Modifying a DNAT Rule

Scenarios

After a DNAT rule is added, you can modify parameters in the DNAT rule as required.

Prerequisites

A DNAT rule has been added for the private NAT gateway.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the target private NAT gateway.
6. On the NAT gateway details page, click the **DNAT Rules** tab.
7. In the DNAT rule list, locate the row that contains the target DNAT rule and click **Modify** in the **Operation** column.
8. In the displayed dialog box, modify the required parameters.
9. Click **OK**.

2.4.4 Deleting a DNAT Rule

Scenarios

Delete a DNAT rule that you no longer need.

Prerequisites

A DNAT rule has been added for 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. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the displayed page, click the name of the target private NAT gateway.
6. On the NAT gateway details page, click the **DNAT Rules** tab.
7. In the DNAT rule list, locate the row that contains the target DNAT rule and click **Delete** in the **Operation** column.
8. In the displayed dialog box, click **Yes**.

2.5 Managing Transit Subnets

A transit IP address assigned from a transit subnet is shared by servers in a VPC to access or provide services accessible from an on-premises server or a remote VPC.

 Copyright © Huawei Technologies Co., Ltd.

Creating a Transit Subnet

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. Click the **Transit Subnets** tab and then **Create Transit Subnet**.
6. Set the parameters as prompted. For details, see **Table 2-4**.

Table 2-4 Parameter descriptions

Parameter	Description
Name	The transit subnet name. The name can include up to 64 characters and can include digits, letters, underscores (_), and hyphens (-).
VPC	The public VPC that the transit subnet belongs to.
Subnet	The transit subnet to be created.
Description	Supplementary information about the transit subnet. The description can contain up to 255 characters.

Assigning a Transit IP Address

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Under **Network**, click **NAT Gateway**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. Click the **Transit Subnets** tab and then click the target subnet name.

   The transit subnet details page is displayed.
6. Click **Assign Transit IP Address** and set parameters as prompted.

Table 2-5 Parameter descriptions

Parameter	Description
Assignment Mode	The assignment mode of the transit IP address. • Automatic • Manual

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IP Address	This parameter is available when **Assignment Mode** is set to **Manual**. This IP address must be included in the transit subnet.

Other Operations

Modifying a Transit Subnet

You can modify the name, description, and total number of IP addresses of transit subnet.

1. On the **Transit Subnets** tab page, locate the row that contains the target subnet, and click **Modify** or choose **More** > **Apply to Change the Number of IP Addresses** in the **Operation** column.
2. Click **OK**.

Deleting a Transit Subnet

You can delete a transit subnet if you no longer need it.

After the transit subnet is deleted, instances in the corresponding VPCs can no longer communicate with others through the private NAT gateway.

1. Locate the row that contains the transit subnet to be deleted and click the **Delete** in the **Operation** column.
2. Click **Yes**.

Releasing a Transit IP Address

You can release a transit IP address if you no longer need it.

1. In the transit IP address list on the transit subnet details page, locate the row that contains the target transit IP address and click **Release** in the **Operation** column.
2. Click **Yes**.

2.6 Connecting to an On-premises Data Center or a Remote VPC

Connecting to an On-premises Data Center

You can use Direct Connect or VPN to connect the public VPC to your on-premises data center.

For high-quality connections, use Direct Connect. For details, see **Enabling Direct Connect**.

For cost-effective connections, use VPN. For details, see **Enabling a VPN**.

Copyright © Huawei Technologies Co., Ltd.

Connecting to a Remote VPC

You can use VPC Peering to connect the public VPC to a remote VPC if they are both in the same region.

For details, see **VPC Peering Connection Overview** .

Copyright © Huawei Technologies Co., Ltd.

3 Permissions Management

3.1 Creating a User and Granting NAT Gateway Permissions

This topic describes how to use IAM to implement fine-grained permissions control for your NAT Gateway. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing NAT Gateway resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a HUAWEI CLOUD account or cloud service to perform efficient O&M on your NAT Gateway resources.

If your HUAWEI CLOUD account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions (see **Figure 3-1**).

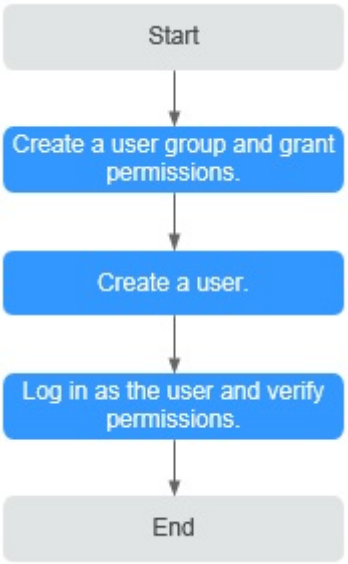
Prerequisites

Learn about the permissions supported by NAT Gateway and choose policies or roles according to your requirements. For NAT Gateway system permissions, see **Permissions Management**. For the permissions of other services, see **System Permissions**.

 Copyright © Huawei Technologies Co., Ltd.

Process Flow

Figure 3-1 Process for granting NAT Gateway permissions



1. **Create a user group and assign permissions to it.**

   Create a user group on the IAM console, and attach the **NAT ReadOnlyAccess** policy to the group.

2. **Create an IAM user and add it to the user group.**

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the management console as the created user.

   Switch to the authorized region and verify the permissions.

   - Choose **Service List** > **NAT Gateway**. Then click **Buy NAT Gateway**. If a message appears indicating that you do not have sufficient permissions to perform the operation, the **NAT ReadOnlyAccess** policy has already taken effect.
   - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **NAT ReadOnlyAccess** policy has already taken effect.

3.2 NAT Gateway Custom Policies

Custom policies can be created to supplement the system-defined policies of NAT Gateway. For the actions that can be added to custom policies, see **Permissions Policies and Supported Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.

 Copyright © Huawei Technologies Co., Ltd.

- JSON: Edit JSON policies from scratch or based on an existing policy.

  For details, see **Creating a Custom Policy**. The following section contains examples of common NAT Gateway custom policies.

Example Policies

- Example 1: Allowing users to create and delete NAT gateways

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "nat:natGateways:create",
                "nat:natGateways:delete"
            ]
        }
    ]
}
```

- Example 2: Denying NAT gateway deletion

  A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **NAT FullAccess** policy to a user but you want to prevent the user from deleting NAT gateways. Create a custom policy for denying NAT gateway deletion, and attach both policies to the group to which the user belongs. Then the user can perform all operations on NAT gateways except deleting NAT gateways. The following is an example of a deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "nat:natGateways:delete"
            ],
            "Effect": "Deny"
        }
    ]
}
```

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "nat:natGateways:update",
        "nat:natGateways:create"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:vpcs:update"
      ],
      "Effect": "Allow"
```

 Copyright © Huawei Technologies Co., Ltd.

```
    }
  ]
}
```

4 Monitoring Management

4.1 Supported Metrics

Description

This section describes metrics reported by NAT Gateway to Cloud Eye as well as their namespaces, monitoring metrics, and dimensions. You can use the management console or the APIs provided by Cloud Eye to query the metrics generated for NAT Gateway.

Namespace

SYS.NAT

Metrics

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway Unit: Count	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute
snat_connection	Monitoring Details of Top 20	IP addresses of the top 20 servers that occupy the most SNAT connections Unit: Count	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bit/s	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
inbound_bandwidth	Monitoring Details of Top 20	IP addresses of the top 20 servers using the SNAT function and occupying the most inbound bandwidth Unit: bit/s	≥ 0 bit/s	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_bandwidth	Outbound Bandwidth	Outbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bit/s	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_bandwidth	Monitoring Details of Top 20	IP addresses of the top 20 servers using the SNAT function and occupying the most outbound bandwidth Unit: bit/s	≥ 0 bit/s	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute

Copyright © Huawei Technologies Co., Ltd.

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: Count	≥ 0	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
inbound_pps	Monitoring Details of Top 20	IP addresses of the top 20 servers using the SNAT function and occupying the most inbound PPS Unit: Count	≥ 0	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: Count	≥ 0	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_pps	Monitoring Details of Top 20	IP addresses of the top 20 servers using the SNAT function and occupying the most outbound PPS Unit: Count	≥ 0	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute

Copyright © Huawei Technologies Co., Ltd.

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
inbound_traffic	Monitoring Details of Top 20	IP addresses of the top 20 servers using the SNAT function and occupying the most inbound traffic Unit: byte	≥ 0 bytes	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_traffic	Monitoring Details of Top 20	IP addresses of the top 20 servers using the SNAT function and occupying the most outbound traffic Unit: byte	≥ 0 bytes	Measurement object: NAT gateway using the SNAT function Dimension: nat_gateway_id	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
snat_connection_ratio	SNAT Connection Usage	Percentage of used SNAT connections. The maximum number of SNAT connections varies depending on the NAT gateway type, which can be 10,000, 50,000, 200,000, or 1,000,000. Unit: Percent	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute
snat_connection_ratio	Monitoring Details of Top 20	IP addresses of the top 20 servers with the most usage rate of SNAT connections Unit: Percent	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute
inbound_bandwidth_ratio	Inbound Bandwidth Usage	Inbound traffic usage rate of servers using the SNAT function. The maximum bandwidth of a NAT gateway is 20 Gbit/s. Unit: Percent	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute
inbound_bandwidth_ratio	Monitoring Details of Top 20	IP addresses of the top 20 servers using the SNAT function and with the most usage rate of inbound bandwidth Unit: Percent	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute

Copyright © Huawei Technologies Co., Ltd.

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
outbound_bandwidth_ratio	Outbound Bandwidth Usage	Outbound traffic usage rate of servers using the SNAT function. The maximum bandwidth of a NAT gateway is 20 Gbit/s. Unit: Percent	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute
outbound_bandwidth_ratio	Monitoring Details of Top 20	IP addresses of the top 20 servers using the SNAT function and with the most usage rate of outbound bandwidth Unit: Percent	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute

Dimensions

Key	Value
nat_gateway_id	NAT gateway ID

4.2 Creating Alarm Rules

Scenarios

You can set NAT gateway alarm rules to customize the monitored objects and notification policies. Then, you can learn NAT gateway running status in a timely manner.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Management & Deployment**, click **Cloud Eye**.
4. In the left navigation pane, choose **Alarm Management** > **Alarm Rules**.
5. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters to create an alarm rule, or modify an existing alarm rule.

 Copyright © Huawei Technologies Co., Ltd.

6. After the parameters are set, click **Create**.

   After the alarm rule is set, the system automatically notifies you when an alarm is triggered.

NOTE

For more information about how to set alarm rules, see *Cloud Eye User Guide*.

4.3 Viewing Metrics

Prerequisites

- The NAT gateway is running properly and SNAT rules have been created.
- It can take a period of time to obtain and transfer the monitoring data. Therefore, wait for a while and then check the data.

Scenarios

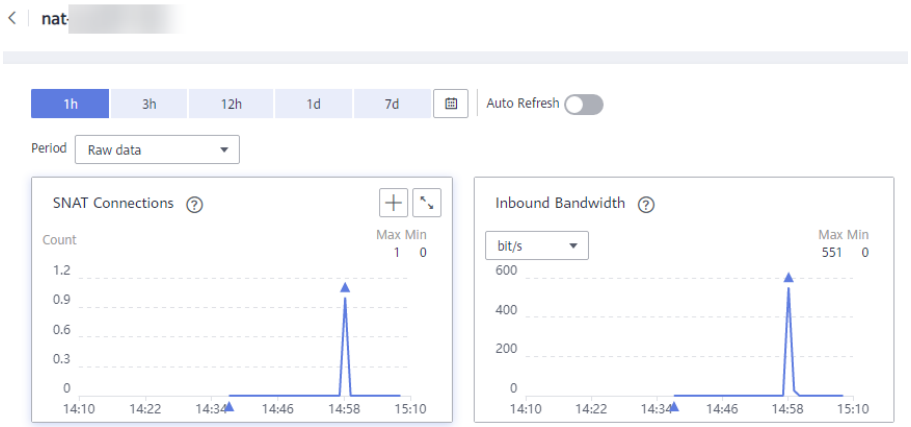
This section describes how to view NAT Gateway metrics.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the target region.
3. Under **Management & Deployment**, click **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **NAT Gateway**.
5. Locate the row that contains the target metric and click **View Metric** in the **Operation** column to check detailed information.

   You can view data of the last one, three, 12, or 24 hours, or last 7 days.

Figure 4-1 Viewing metrics



 Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2020-07-18	This issue is the nineteenth official release, which incorporates the following change: Added the private NAT gateway function.
2020-06-24	This issue is the eighteenth official release, which incorporates the following change: • Modified FAQ "What Are the Differences Between an ECS Using a NAT Gateway and an ECS Binding to an EIP?" • Added FAQ "Can I Change the VPC Selected When I Create a NAT Gateway?"
2020-05-26	This issue is the seventeenth official release, which incorporates the following change: Added scenario "Using Multiple NAT Gateways Together" in region **CN North-Beijing4**.
2020-05-08	This issue is the sixteenth official release, which incorporates the following change: Add description about SNAT rules and DNAT rules based on console changes.
2020-02-10	This issue is the fifteenth official release, which incorporates the following change: Changed the NAT system policy names.
2020-01-20	This issue is the fourteenth official release, which incorporates the following change: Modified contents in section "Permissions Management".

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2019-12-23	This issue is the thirteenth official release, which incorporates the following change: Added FAQ "What Are the Relationships and Differences Between the CIDR Blocks in a NAT Gateway and in an SNAT Rule?"
2019-12-03	This issue is the twelfth official release, which incorporates the following change: Updated section "Permissions Management" based on the IAM console.
2019-11-05	This issue is the eleventh official release, which incorporates the following change: Added the SNAT HA scenario.
2019-08-30	This issue is the tenth official release, which incorporates the following change: • Updated sections in "Overview". • Added FAQs.
2019-05-30	This issue is the ninth official release, which incorporates the following change: Added section **Permissions Management**.
2019-03-26	This issue is the eighth official release, which incorporates the following changes: • Added description that DNAT rules can be imported and exported using templates. • Added description that DNAT rules can be deleted in batches. • Added description about the DNAT rule. • Added description that the NAT Gateway service supports the enterprise project.
2018-01-30	This issue is the seventh official release, which incorporates the following changes: • Supported adding a maximum of 20 EIPs to one SNAT rule. • Supported configuring a port range for a DNAT rule. • Supported the modification of SNAT and DNAT rules.
2018-10-30	This issue is the sixth official release, which incorporates the following changes: • Added the inter-cloud high-speed Internet access scenario. • Optimized the document structure.

Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2018-07-30	This issue is the fifth official release, which incorporates the following changes: ● Supported the **All ports** type in a DNAT rule. ● Added section "Monitoring".
2018-04-30	This issue is the fourth official release, which incorporates the following change: Added DNAT description.
2018-03-30	This issue is the third official release, which incorporates the following change: Added a case to troubleshoot internet connection failure.
2018-01-30	This issue is the second official release, which incorporates the following changes: ● Modified the description of NAT Gateway deployment advantages. ● Added restrictions on the naming rules and description for creating a NAT gateway.
2017-12-18	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.