NAT Gateway

User Guide

Issue	01
Date	2022-11-29

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

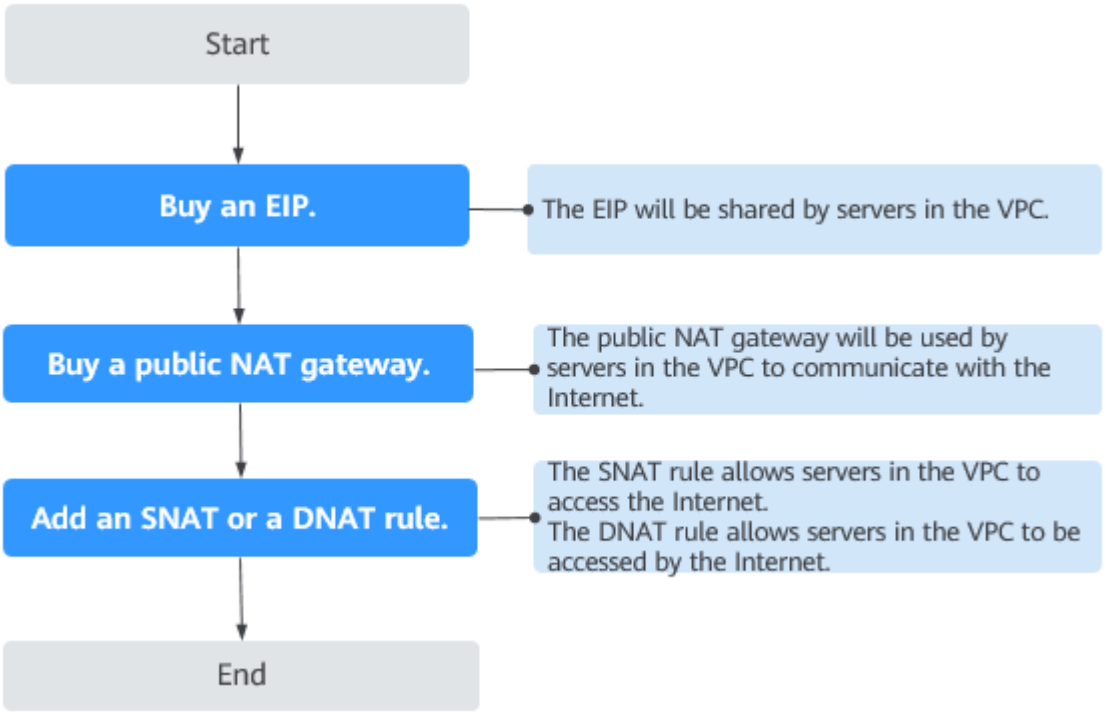
1 Public NAT Gateways

1.1 Public NAT Gateway Overview

Public NAT gateways provide network address translation with 20 Gbit/s of bandwidth for ECSs and BMSs in a VPC, or servers in on-premises data centers that connect to a VPC through Direct Connect or VPN, allowing these servers to share EIPs to access the Internet or provide services accessible from the Internet.

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

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

You can 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 you will buy a public NAT gateway are available.
- Traffic to the public NAT gateway needs to be allowed to pass through, that is, a route pointing to the public NAT gateway needs to be configured in the VPC. Therefore, when you buy a public NAT gateway, a default route 0.0.0.0/0 that points 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, you need to 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 **BuyPublic NAT Gateway**.
5. Configure the required parameters. For details, see **Table 1-1**.

Table 1-1 Parameter descriptions

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	The VPC that the public NAT gateway belongs to The selected VPC cannot be changed after you buy the public NAT gateway. **NOTE** Traffic to the public NAT gateway needs to be allowed to pass through, that is, a route pointing to the public NAT gateway needs to be configured in the VPC. Therefore, when you buy a public NAT gateway, a default route 0.0.0.0/0 that points 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, you need to 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.
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 you buy the public NAT gateway.
Type	The type of the public NAT gateway The type can be **Extra-large**, **Large**, **Medium**, and **Small**. 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 Enter up to 255 characters.
Tag	The public NAT gateway tag. A tag is a key-value pair. You can add up to 10 tags to each public NAT gateway. The tag key and value must meet the requirements listed in **Table 1-2**.

Table 1-2 Tag requirements

Parameter	Requirement
Key	• 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	• 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 these parameters are configured, the public NAT gateway price will be displayed. You can click **Pricing details** on the page to view pricing details.

6. Click **Submit** to create a public NAT gateway.

   It takes 1 to 5 minutes to create a public NAT gateway.

7. 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

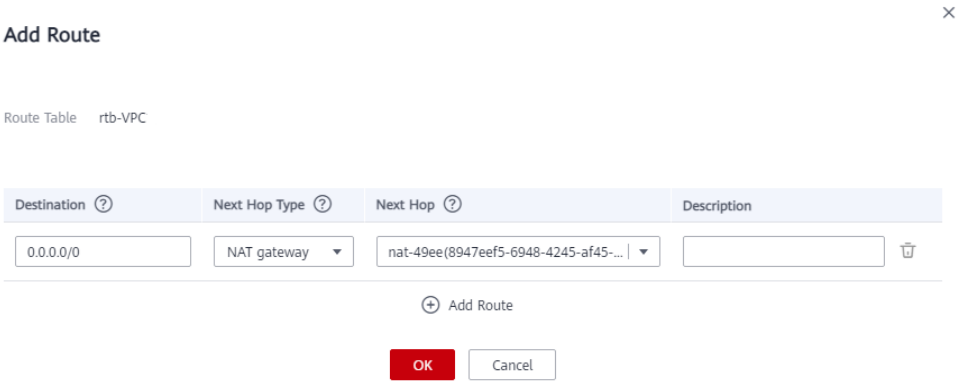
   If the custom route table quota is insufficient, **submit a service ticket** to increase the route table quota.

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 1-2 Add Route



8. Click **OK**.

1.2.2 Viewing a Public NAT Gateway

Scenarios

You can view information about a public NAT gateway.

Prerequisites

There is a public NAT gateway 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 target public NAT gateway.
5. View information about the public NAT gateway on the displayed page.

1.2.3 Modifying a Public NAT Gateway

Scenarios

You can modify the name, type, or description of a public NAT gateway.

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

Prerequisites

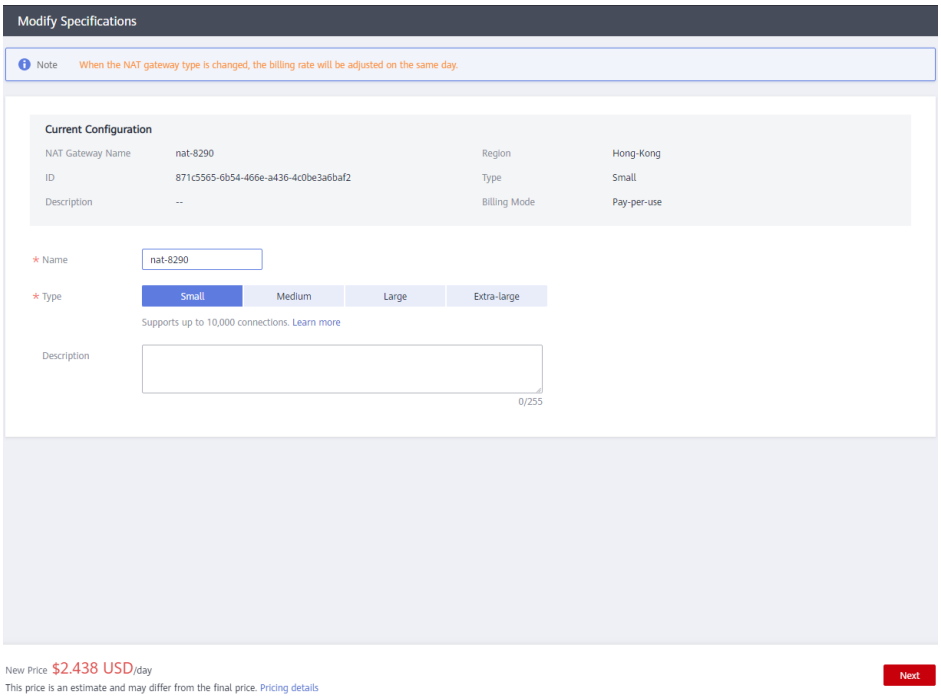
There is a public NAT gateway available.

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, locate the row that contains the public NAT gateway you want to modify and click **Modify** in the **Operation** column.
5. Modify the name, type, or description of the public NAT gateway as needed.

   Figure 1-3 Modify Specifications



6. Click **OK**.

1.2.4 Deleting or Unsubscribing from a Public NAT Gateway

Scenarios

You can delete or unsubscribe from public NAT gateways that are no longer required to release resources and reduce costs.

NOTE

- To unsubscribe from a pay-per-use public NAT gateway, you only need to **delete the NAT gateway**.

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. 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, locate the row that contains the public NAT gateway you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **Yes**.

1.3 Managing SNAT Rules

1.3.1 Adding an SNAT Rule

Scenarios

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

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

Prerequisites

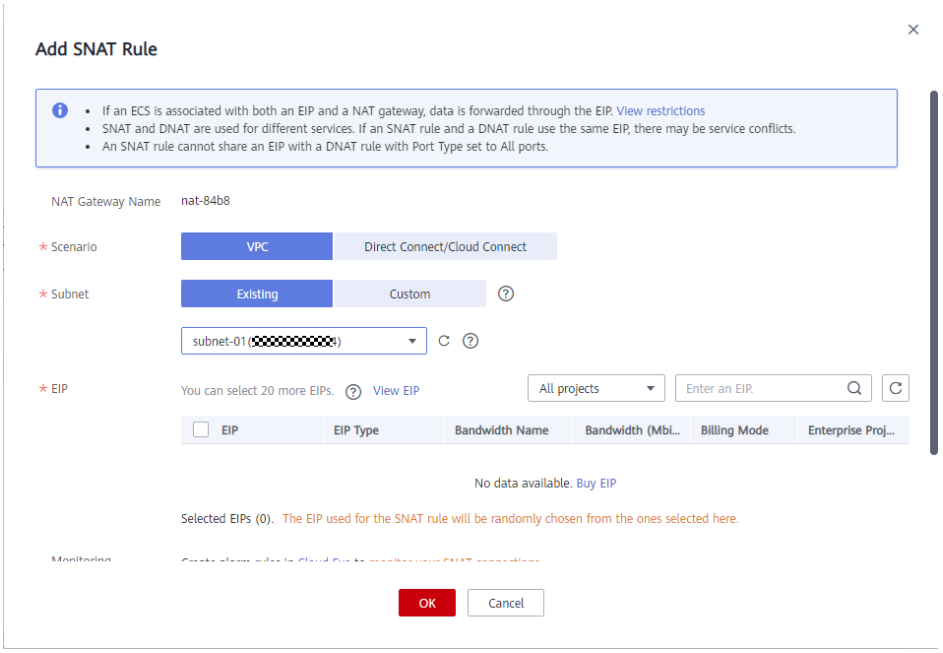
There is a public NAT gateway available.

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 that you want to add an SNAT rule for.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

Figure 1-4 Add SNAT Rule



6. Configure the required parameters. For details, see **Table 1-3**.

Table 1-3 Parameter descriptions

Parameter	Description
Scenario	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	• **Existing**: Select an existing subnet to enable servers in this subnet to use the SNAT rule to access the Internet. • **Custom**: Specify the CIDR block to a subset of a current VPC subnet or enter a server IP address so that the server can use the SNAT rule to access the Internet. **NOTE** When you select **Custom**, you can enter 0.0.0.0/0. Only a 32-bit server IP address is supported.

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 with **Port Type** set to **Specific port** of the current public NAT gateway, 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 at once. If you have selected multiple EIPs for an SNAT rule, an EIP will be chosen from your selection at random.
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	Supplementary information about the SNAT rule Enter up to 255 characters.

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.

1.3.2 Viewing an SNAT Rule

Scenarios

After you add an SNAT rule, you can view its details.

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.
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 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

You can modify SNAT rules as needed.

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.
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 target public NAT gateway.
5. On the **SNAT Rules** tab, locate the row that contains the SNAT rule you want to modify.
6. Click **Modify** in the **Operation** column.
7. In the displayed dialog box, modify the parameters as needed.
8. Click **OK**.

1.3.4 Deleting an SNAT Rule

Scenarios

You can delete SNAT rules that you no longer need.

Prerequisites

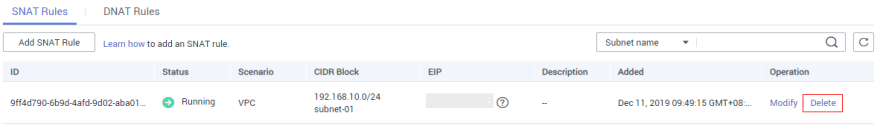
An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
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 target public NAT gateway.
5. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete 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 only one DNAT rule for each port on a server. One port can be mapped to only one EIP. If multiple servers need to provide services accessible from the Internet, create multiple DNAT rules.

Prerequisites

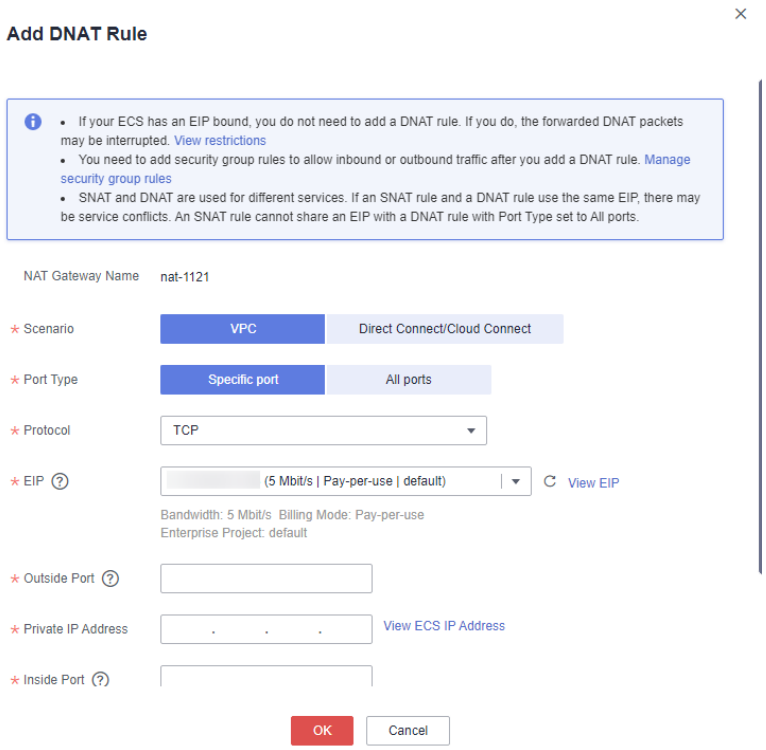
There is a public NAT gateway available.

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 that you want to add a DNAT rule for.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. Click **Add DNAT Rule**.

Figure 1-6 Add DNAT Rule



7. Configure the required parameters. For details, see **Table 1-4**.

Table 1-4 Parameter descriptions

Parameter	Description
Scenario	Select **VPC** if your servers in a VPC will use the DNAT rule to share the same EIP to provide services accessible from the Internet. **Direct Connect/Cloud Connect**: Select this scenario if servers in an on-premises data center connected to a VPC through Direct Connect or Cloud Connect will use the DNAT rule to provide services accessible from the Internet.
Port Type	The port type • **All ports**: This is effectively like having a regular EIP bound to your servers. All requests received by the gateway will be forwarded to your servers, regardless of what port or protocol was used. • **Specific port**: The public NAT gateway forwards requests to your servers only from the outside port and to the inside port configured here, and only if they use the right protocol.

Parameter	Description
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 has not been bound, has been bound to a DNAT rule with **Port Type** set to **Specific port** of the current public NAT gateway, or has been bound to an SNAT rule of the current public NAT gateway.
Outside Port	The port of the EIP 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	• 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 your on-premises data center or your 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. **NOTE** In the Direct Connect or Cloud Connect scenario, the private IP address can also be a virtual IP address or a private IP address of a load balancer. • Configure the port of **Private IP Address** if you select **Specific port** for **Port Type**.
Inside Port	The port of the server that uses the DNAT rule to provide services accessible from the Internet 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	Supplementary information about the DNAT rule Enter up to 255 characters.

8. Click **OK**.

Once the rule is created, its status changes to **Running**.

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.

1.4.2 Viewing a DNAT Rule

Scenarios

After you add a DNAT rule, you can view its details.

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. 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 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

You can modify DNAT rules as needed.

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. 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 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 DNAT rule you want to modify and click **Modify** in the **Operation** column.
7. In the displayed dialog box, modify the parameters as needed.
8. Click **OK**.

1.4.4 Deleting a DNAT Rule

Scenarios

You can delete a DNAT rule that you no longer need.

Prerequisites

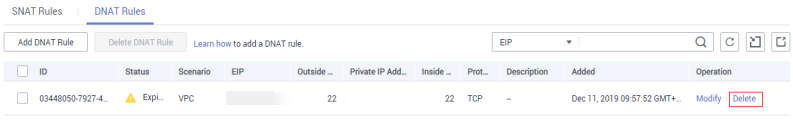
A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. 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 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 DNAT rule you want to delete 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

You can delete DNAT rules that you no longer need.

Prerequisites

DNAT rules have 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. 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 target public NAT gateway.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
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, create multiple DNAT rules.

Prerequisites

There is a public NAT gateway 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**.

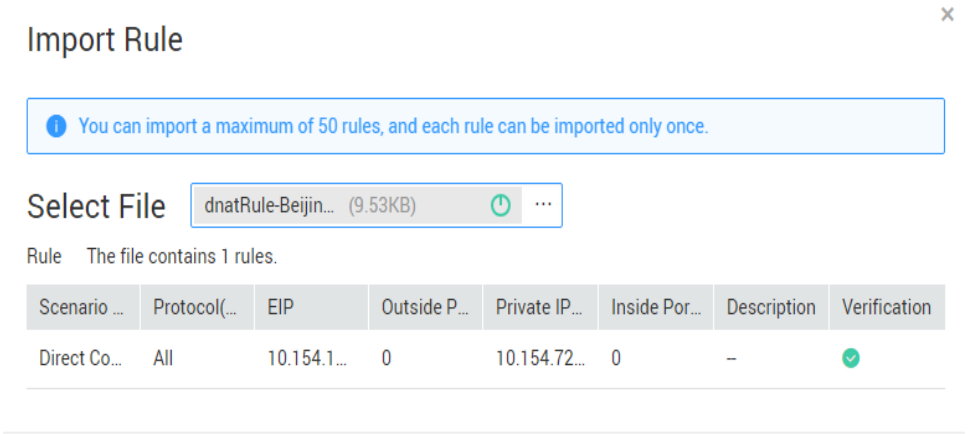
   The **Public NAT Gateway** page is displayed.
4. On the displayed page, click the name of the public NAT gateway that you want to add a DNAT rule for.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. On the displayed page, click **Import Rule** and then **Download Template**.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

Table 1-5 Parameter descriptions

Parameter	Description
Scenario	The following two scenarios are available: • **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**: Select this scenario if servers in an on-premises data center connected to a VPC through Direct Connect or Cloud Connect will use the DNAT rule to provide services accessible from the Internet.
Protocol	The protocol can be **TCP**, **UDP**, or **All**.
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 only available if you select **Specific port** for **Port Type**. You can enter a specific 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 your on-premises data center or your 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 private IP address port if you set **Protocol** to **TCP** or **UDP**.
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 on-premises data center or the user's private port. • This parameter is only available if you select **Specific port** for **Port Type**. The number of inside and outside ports must match.
Description	Supplementary information about the DNAT rule. You can enter up to 255 characters.

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

   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.

2 Private NAT Gateways

2.1 Private NAT Gateway Overview

Private NAT Gateways

Private NAT gateways provide private address translation services for ECSs and BMSs in a VPC. You can configure SNAT and DNAT rules to translate the source and destination IP addresses into transit IP addresses, so that servers in the VPC can communicate with other VPCs or on-premises data centers.

Specifically:

- SNAT enables multiple servers across AZs in a VPC to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers that share the same transit IP address in a VPC to provide services accessible from on-premises data centers or other VPCs.

Transit Subnet

A transit subnet functions as a transit network. You can configure a transit IP address for the transit subnet so that servers in a local VPC can share the transit IP address to access on-premises data centers or other VPCs.

Transit VPC

The transit VPC is the VPC that the transit subnet is a part of.

Figure 2-1 Private NAT gateway

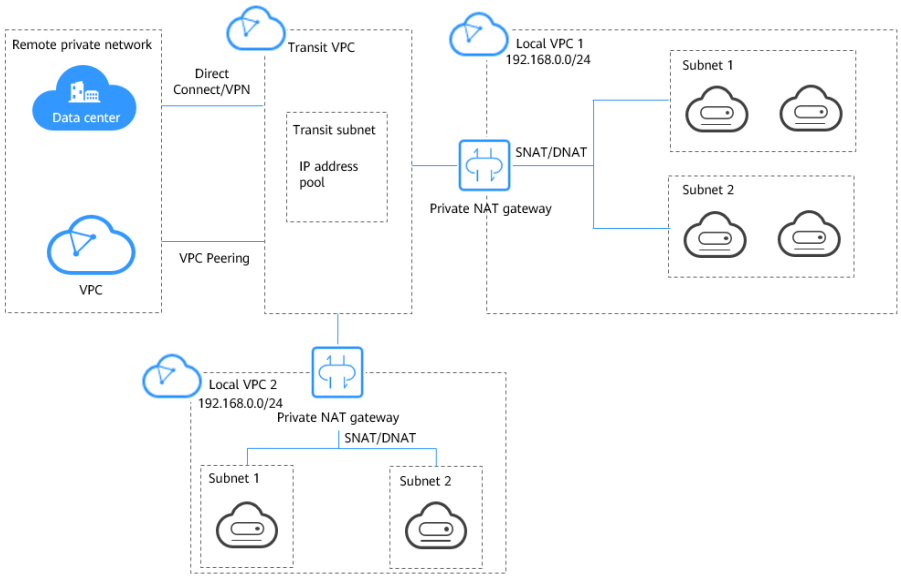


Figure 2-1 shows two ways a private NAT gateway can be deployed.

- **Communications between VPCs with overlapping CIDR blocks**

  Normally, VPCs with overlapping CIDR blocks cannot communicate with each other. But with private NAT gateways, you can configure SNAT and DNAT rules to translate the private IP addresses in the VPCs to transit IP addresses and establish cross-VPC communications.

- **Using a specific IP address to access a remote private network**

  A private NAT gateway lets you use a specific IP address to access an on-premises data center or a VPC on a remote private network. The on-premises data center connects to the transit VPC through Direct Connect or VPN. The VPC is connected to the transit VPC through a VPC Peering connection. In the figure, VPC 1 uses a private NAT gateway to access the remote private network. To do this, SNAT rules need to be configured to translate the private IP address in VPC 1 into specific IP addresses that can communicate with the private network, on the left.

  NOTE

  - Private NAT gateways are free for a limited time in the following regions: CN East-Shanghai2, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg, and LA-Mexico City2.
  - Private NAT gateways are billed in the following regions: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok, AP-Singapore, and CN Southwest-Guiyang1.

Advantages

- Easier network planning

  After migrating some of their workloads from on-premises data centers to the cloud, an enterprise may want to preserve their internal network communications unchanged. Private NAT gateways can translate the IP addresses of your cloud servers to transit IP addresses in the transit VPC. That way, the servers can communicate with on-premises data centers or other

VPCs. The enterprise does not have to reconstruct any of their services and the network planning is much simpler.

- Zero IP conflicts

  Two private NAT gateways can translate IP addresses of two VPCs with an overlapping CIDR block to two transit IP addresses, so that servers in the two VPCs can use the transit IP addresses to communicate with each other.

- Strong security

  A private NAT gateway can map private IP addresses to IP addresses that are specified by enterprise security requirements. In this way, enterprises can choose which IP addresses are used to access different agencies, which can improve security.

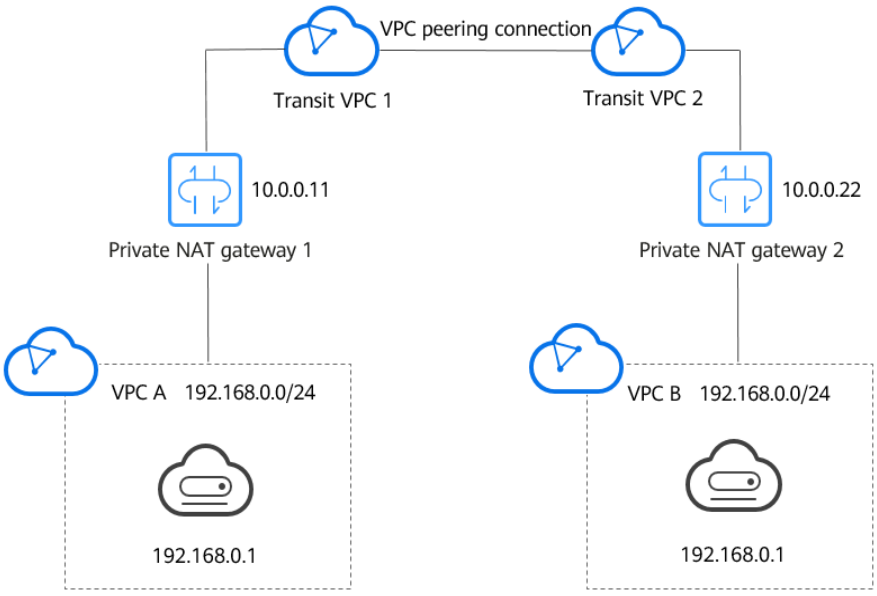
Scenarios

- Connecting VPCs with overlapping CIDR blocks

  You can configure two private NAT gateways for two VPCs with overlapping CIDR blocks, and then add SNAT and DNAT rules on the two private NAT gateways to enable the servers in the two VPCs to use the transit IP addresses to communicate with each other.

  In the following figure, there are two transit VPCs and two private NAT gateways. Address 192.168.0.1 in VPC A is translated to 10.0.0.11, and the IP address 192.168.0.1 in VPC B is translated to 10.0.0.22. A VPC peering connection can then be established between the two transit VPCs to enable communication between them.

  Figure 2-2 Connecting VPCs with overlapping CIDR blocks



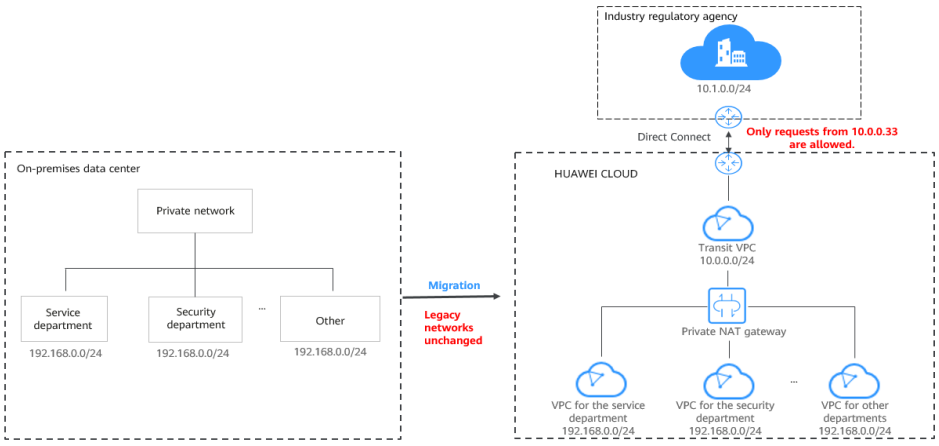
- Migrating workloads to the cloud without changing the network topology or accessing regulatory agencies from specific IP addresses

  Organizations may want to migrate their workloads to the cloud without making any changes to their existing network topology. They may also have

to access regulatory agencies from specific IP addresses as required by these agencies. A private NAT gateway is a good choice.

The following figure represents an enterprise network where the subnets of different departments overlap. A private NAT gateway allows the enterprise to keep the existing network topology unchanged while migrating their workloads to the cloud. In this example, the private NAT gateway maps the IP address of each department to 10.0.0.33 so that each department can use 10.0.0.33 to securely access the regulatory agency.

Figure 2-3 Migrating workloads to the cloud without changing the network topology or accessing regulatory agencies from specific IP addresses



Differences Between Public and Private NAT Gateways

Public NAT gateways use SNAT rules to map private IP addresses to EIPs, so that servers in a VPC can share an EIP to access the Internet. DNAT rules enable the servers to share an EIP to provide services accessible from the Internet.

Private NAT gateways use SNAT rules to map private IP addresses to transit IP addresses, so that servers in a VPC can access on-premises data centers or other VPCs. DNAT rules enable the servers to share the transit IP address to provide services accessible from the private network.

Table 2-1 describes the differences between public and private NAT gateways.

Table 2-1 Differences between public and private NAT gateways

Item	Public NAT Gateway	Private NAT Gateway
Function	Connects a private network to the Internet	Connects private network to each other
SNAT	Enables access to the Internet	Enables access to on-premises data centers or other VPCs
DNAT	Allows servers to provide services accessible from the Internet	Allows servers to provide services accessible from on-premises data centers or other VPCs in private networks

Item	Public NAT Gateway	Private NAT Gateway
Communications media	EIP	Transit IP address

Helpful Links

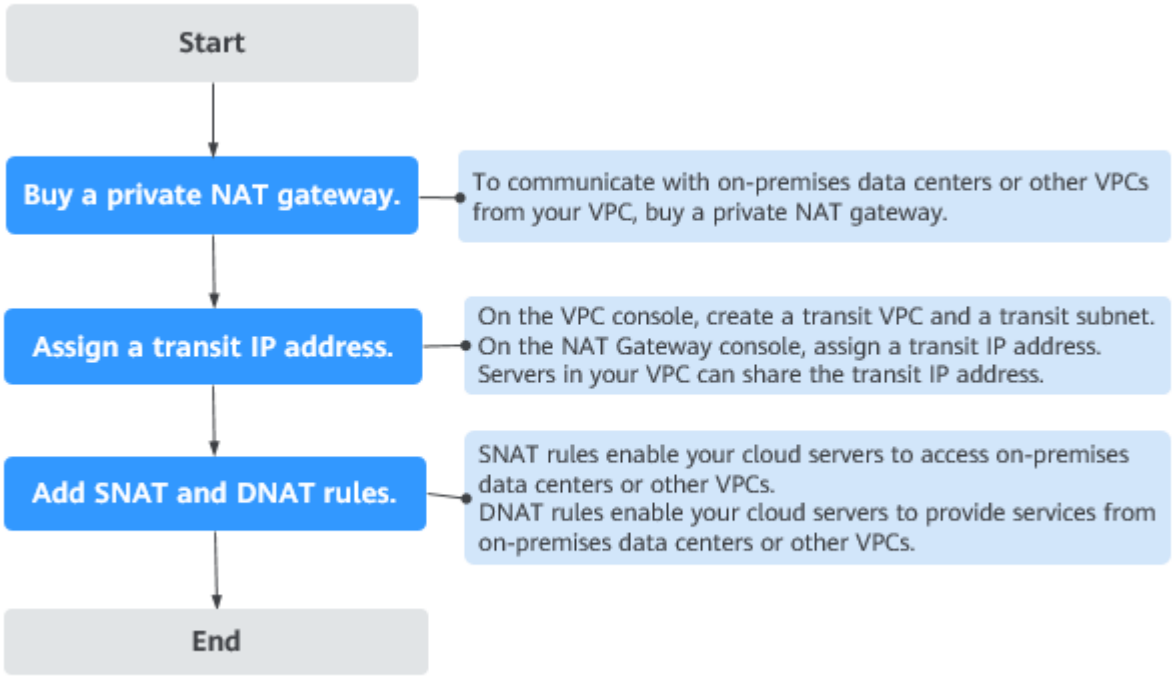
Using Private NAT Gateways to Enable Communications Between Cloud and On-premises Networks

2.2 Buying a Private NAT Gateway

2.2.1 Overview

This section describes how to buy a private NAT gateway.

Figure 2-4 Process for deploying a private NAT gateway



After you configure the private NAT gateway, see **Accessing On-premises Data Centers or Other VPCs** to learn how to connect to on-premises data centers or other VPCs.

2.2.2 Buying a Private NAT Gateway

Scenarios

You can buy a private NAT gateway to enable servers in your VPC to access or provide services accessible from on-premises data centers and other VPCs.

NOTE

- Private NAT gateways are free for a limited time in the following regions: CN East-Shanghai2, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg, and LA-Mexico City2.
- Private NAT gateways are billed in the following regions: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok, AP-Singapore, and CN Southwest-Guiyang1.

CAUTION

When you buy a private NAT gateway, you must specify its VPC, subnet, and type.

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 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. Configure the required parameters. For details, see **Table 2-2**.

Table 2-2 Parameter descriptions

Parameter	Parameter descriptions
Billing Mode	Private NAT gateways are billed on a pay-per-use basis.
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 VPC that the private NAT gateway belongs to The selected VPC cannot be changed after the private NAT gateway is purchased.

Parameter	Parameter descriptions
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: **Extra-large**, **Large**, **Medium**, and **Small**. For details about types, see **NAT Gateway 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. If you do not specify an enterprise project, the **default** enterprise project will be used.
Description	Supplementary information about the private NAT gateway Enter up to 255 characters.

7. Click **Buy Now**.

Helpful Links

Managing Private NAT Gateways

2.2.3 Assigning a Transit IP Address

Scenarios

After a private NAT gateway is created, assign a transit IP address, so that servers in your VPC can share the transit IP address to communicate with on-premises data centers or other VPCs.

Prerequisites

- There are transit VPCs and transit subnets available.
- A Direct Connect connection has been created with the VPC CIDR block **0.0.0.0/0** configured. For details, see **Create a Virtual Gateway**.

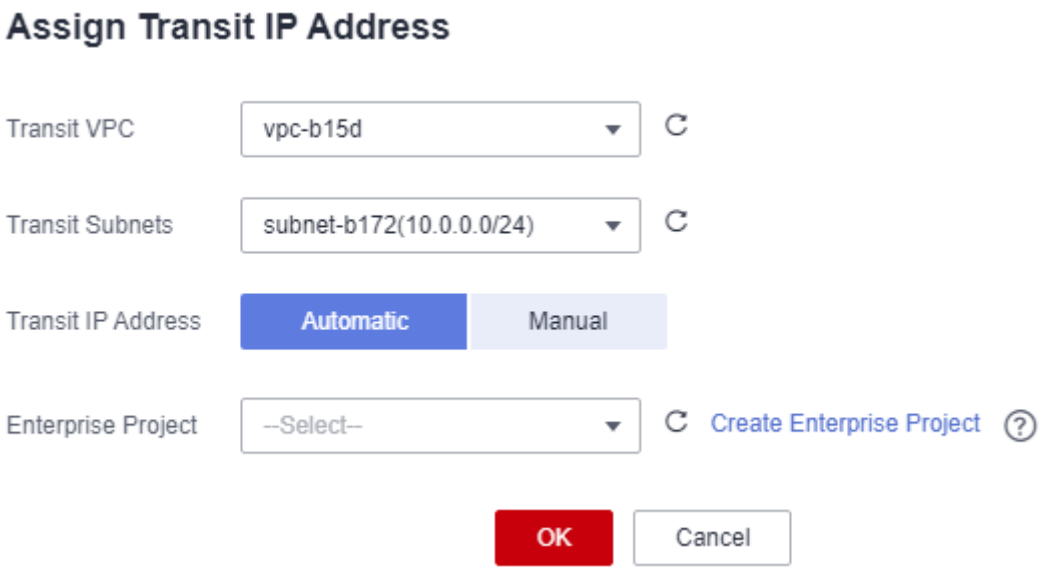
Procedure

1. Log in to the management console.

2. Click in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **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 **Private NAT Gateway** page, click **Transit IP Addresses**.

Figure 2-5 Assign Transit IP Address



6. Configure required parameters. For details, see **Table 2-3**.

Table 2-3 Parameter descriptions of a transit IP address

Parameter	Description
Transit VPC	The VPC to which the transit IP address belongs.
Transit Subnet	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**.

Parameter	Description
Enterprise Project	Specifies the enterprise project to which the transit IP address belongs.

7. Click **OK**.

2.2.4 Adding an SNAT Rule

Scenarios

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

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

Prerequisites

- There is a private NAT gateway available.
- There are transit IP addresses available.
- A Direct Connect connection has been created with the VPC CIDR block **0.0.0.0/0** configured. 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. Click **Service List** in the upper left corner. Under **Networking**, select **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 that you want to add an SNAT rule for.
6. On the **SNAT Rules** tab, click **Add SNAT Rule**.
7. Configure required parameters. For details, see **Table 2-4**.

Figure 2-6 Add SNAT Rule

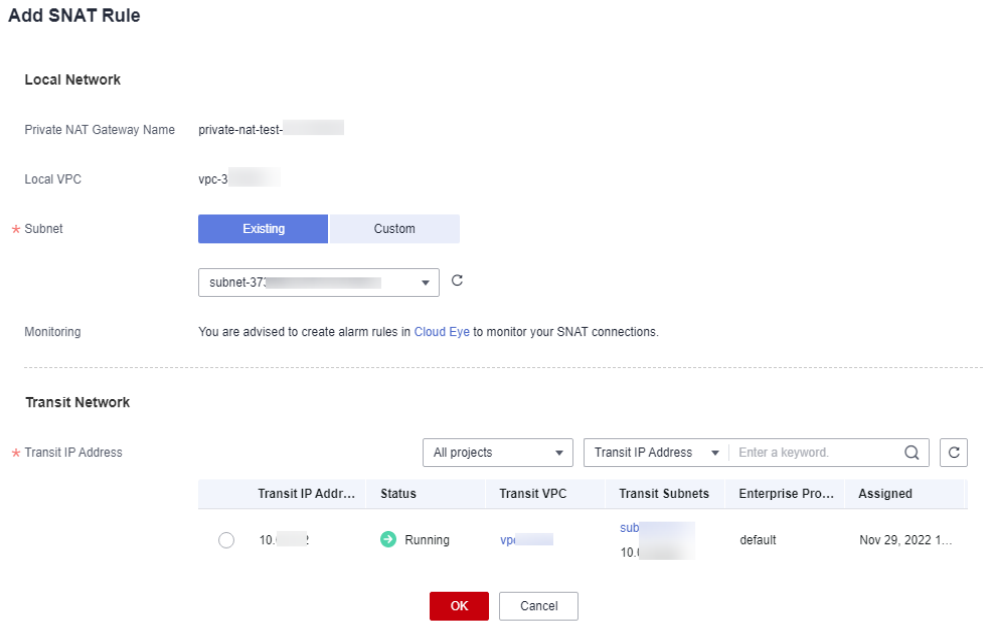


Table 2-4 Parameter descriptions of an SNAT rule

Parameter	Description
Subnet	Specifies 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	Select the created transit IP address.
Description	Provides supplementary information about the SNAT rule. You can enter up to 255 characters.

8. Click **OK**.

NOTE

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

Helpful Links

Managing SNAT Rules

2.2.5 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 on-premises servers or other VPCs.

A DNAT rule needs to be configured for each port on a server that needs to be made accessible. If multiple ports on a server or multiple servers need to provide services accessible from on-premises servers or other VPCs, multiple DNAT rules need to be configured.

Prerequisites

- There is a private NAT gateway available.
- There are transit IP addresses 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 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 that you want to add a DNAT rule for.
6. On the private NAT gateway details page, click the **DNAT Rules** tab.
7. Click **Add DNAT Rule**.

   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.
8. Configure the required parameters. For details, see **Table 2-5**.

Figure 2-7 Add DNAT Rule

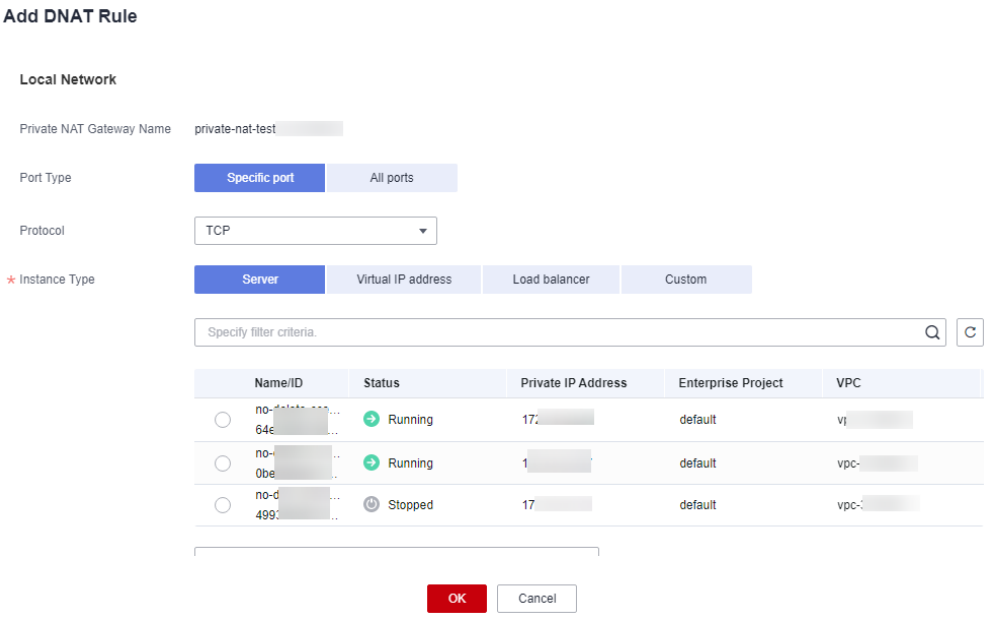


Table 2-5 Parameter descriptions

Parameter	Description
Local Network	
Port Type	The port type The type can be: • **Specific port**: The private NAT gateway forwards requests to your servers only from the outside port and to the inside port configured here, and only if they use the right protocol. • **All ports**: This is effectively like having a transit IP address bound to your servers. All requests received by the gateway will be forwarded to your servers, regardless of what port or protocol was used.
Protocol	The protocol can be TCP or UDP If you select **All ports**, this parameter is **All** by default. This parameter is only available if you select **Specific port** for **Port Type**.
Instance Type	The type of instance that will be providing services accessible from on-premises data centers or other VPCs Possible types are: • **Server** • **Virtual IP address** • **Load balancer** • **Custom**

Parameter	Description
NIC	The NIC of the server This parameter is only available if you set **Instance Type** to **Server**.
IP Address	The IP address of the server that will be providing services accessible from on-premises data centers or other VPCs. This parameter is only available if you set **Instance Type** to **Custom**.
Internal Port	The port of the instance Range: 1 to 65535 This parameter is only available if you select **Specific port** for **Port Type**.
Transit Network	
Transit IP Address	The transit IP address used to access on-premises data centers or other VPCs You can select a transit IP address that either is not bound to any resource, or has been bound to a DNAT rule for the current private NAT gateway where **Port Type** is set to **Specific port**.
Transit IP Address Port	The port of the transit IP address Supported range: 1 to 65535 This parameter is only available if you select **Specific port** for **Port Type**.
Description	Supplementary information about the DNAT rule Enter up to 255 characters.

9. Click **OK**.

   Once the rule is created, its status changes to **Running**.

Helpful Links

Managing DNAT Rules

2.3 Managing Private NAT Gateways

2.3.1 Viewing a Private NAT Gateway

Scenarios

You can view information about a private NAT gateway.

Prerequisites

There is a private NAT gateway 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 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.
6. View information about the private NAT gateway on the displayed page.

2.3.2 Modifying a Private NAT Gateway

Scenarios

You can modify the name, type, or description of a private NAT gateway.

Prerequisites

There is a private NAT gateway 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 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 private NAT gateway you want to modify and click **Modify** in the **Operation** column.
6. Modify the name, type, or description of the private NAT gateway as needed.
7. Confirm your modification and click **OK**.

   You can view information about the modified NAT gateway in the private NAT gateway list.

2.3.3 Deleting a Private NAT Gateway

Scenarios

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

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. Click **Service List** in the upper left corner. Under **Networking**, select **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 private NAT gateway you want to delete and click **Delete** in the **Operation** column.
6. In the displayed dialog box, click **Yes**.

2.4 Managing SNAT Rules

2.4.1 Viewing an SNAT Rule

Scenarios

After you add an SNAT rule, you can view its details.

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.
3. Click **Service List** in the upper left corner. Under **Networking**, select **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.
6. In the SNAT rule list, view the details about the SNAT rule.

2.4.2 Modifying an SNAT Rule

Scenarios

You can modify an SNAT rule as needed.

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.
3. Click **Service List** in the upper left corner. Under **Networking**, select **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.
6. On the **SNAT Rules** tab, locate the row that contains the SNAT rule you want to modify.
7. Click **Modify** in the **Operation** column.
8. In the displayed dialog box, modify the parameters as needed.
9. Click **OK**.

2.4.3 Deleting an SNAT Rule

Scenarios

You can delete SNAT rules that you no longer need.

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.
3. Click **Service List** in the upper left corner. Under **Networking**, select **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.
6. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.
7. In the displayed dialog box, click **Yes**.

2.5 Managing DNAT Rules

2.5.1 Viewing a DNAT Rule

Scenarios

After you add a DNAT rule, you can view its details.

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. Click **Service List** in the upper left corner. Under **Networking**, select **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.
6. On the private NAT gateway details page, click the **DNAT Rules** tab.
7. In the DNAT rule list, view the details about the DNAT rule.

2.5.2 Modifying a DNAT Rule

Scenarios

You can modify a DNAT rule as needed.

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. Click **Service List** in the upper left corner. Under **Networking**, select **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.
6. On the private NAT gateway details page, click the **DNAT Rules** tab.
7. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.
8. In the displayed dialog box, modify the parameters as needed.
9. Click **OK**.

2.5.3 Deleting a DNAT Rule

Scenarios

You can delete a DNAT rule that you no longer need.

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. Click **Service List** in the upper left corner. Under **Networking**, select **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.
6. On the private NAT gateway details page, click the **DNAT Rules** tab.
7. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.
8. In the displayed dialog box, click **Yes**.

2.6 Managing Transit IP Addresses

2.6.1 Assigning a Transit IP Address

Scenarios

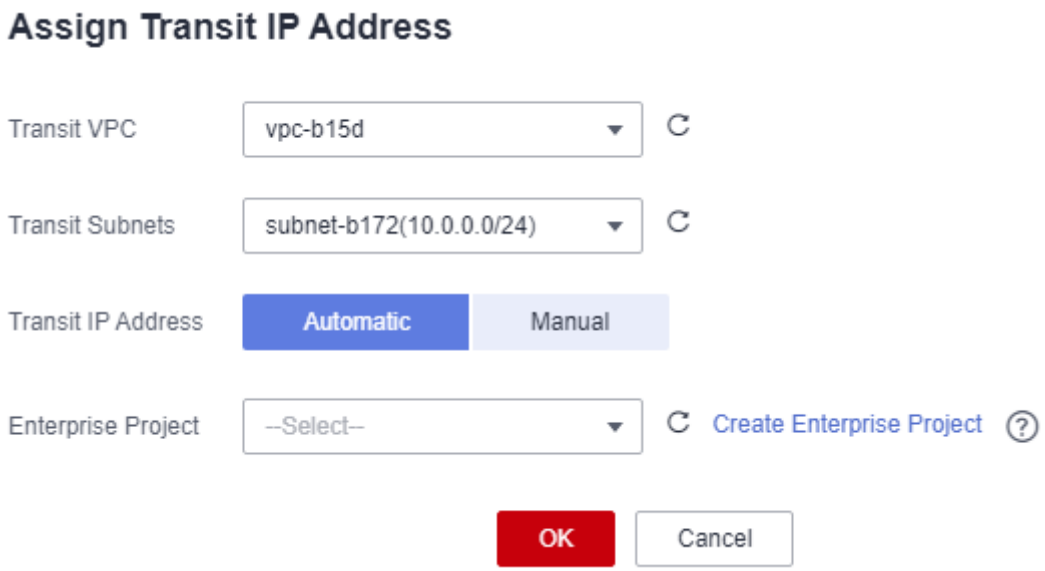
Servers in a VPC all use the same transit IP address in the transit subnet to access or provide services accessible from on-premises data centers or other VPCs.

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**.

   The NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. On the **Private NAT Gateway** page, click **Transit IP Addresses**.

   Figure 2-8 Assign Transit IP Address



6. Configure required parameters. For details, see **Table 2-6**.

   Table 2-6 Parameter descriptions of a transit IP address

Parameter	Description
Transit VPC	The VPC to which the transit IP address belongs.
Transit Subnet	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.

Parameter	Description
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.

7. Click **OK**.

2.6.2 Viewing a Transit IP Address

Scenarios

You can view details about the transit IP addresses assigned to you.

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 NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. Click the **Transit IP Addresses** tab and then click the target transit IP address.
6. On the page displayed, view details about the assigned transit IP addresses.

2.6.3 Releasing a Transit IP Address

Scenarios

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

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 NAT gateway console is displayed.
4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateway**.
5. In the **Transit IP Addresses** area, locate the transit IP address you want to release, and click **Release** in the **Operation** column.
6. Click **Yes**.

NOTE

If a transit IP address has been associated with an SNAT or DNAT rule, it cannot be released. To release such a transit IP address, delete all rules associated with it first.

2.7 Accessing On-Premises Data Centers or Other VPCs

Accessing On-Premises Data Centers

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

For a higher quality connection, use Direct Connect. For details, see **Overview**.

For more cost-effective connectivity, use VPN. For details, see **Overview.**

Accessing Other VPCs

You can use VPC Peering to connect the transit VPC to other VPCs.

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

3 Permissions Management

3.1 Creating a User and Granting NAT Gateway Permissions

This section describes how to use **IAM** to implement fine-grained permissions control for your NAT Gateway resources. 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 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.

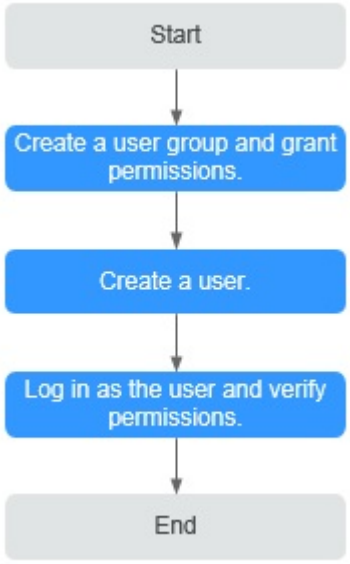
This section describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

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

Process Flow

Figure 3-1 Process for granting NAT Gateway permissions



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

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

2. **Create an IAM user and add it to a 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 have insufficient permissions to perform the operation, the **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 **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.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For operation 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 deny policy 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 Gateway **FullAccess** policy to a user but also forbid 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 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"
    }
  ]
}
```


4 Managing NAT Gateway Tags

Scenarios

A NAT gateway tag identifies the NAT gateway. Tags can be added to NAT gateways to facilitate NAT gateway identification and administration. You can add a tag to a NAT gateway when creating the NAT gateway. Alternatively, you can add a tag to a created NAT gateway on the NAT gateway details page. A maximum of ten tags can be added to each NAT gateway.

NOTE

Only public NAT gateways support tag management.

A tag consists of a key and value pair. **Table 4-1** lists the tag key and value requirements.

Table 4-1 Tag requirements

Parameter	Requirement
Key	• 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	• 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.

Procedure

Search for public NAT gateways by tag key or tag value on the page listing the public NAT gateways.

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
3. In the upper right corner of the public NAT gateway list, click **Search by Tag**.
4. In the displayed area, enter the tag key and tag value of the public NAT gateway you are searching for. Both the tag key and value must be specified.
5. Click **+** to specify additional tag keys and values.

   You can add a maximum of ten tags to refine your search results. If you add more than one tag to search for public NAT gateways, the tags are automatically joined with AND.
6. Click **Search**.

   The system displays the public NAT gateways you are searching for based on the entered tag keys and tag values.

Add, delete, edit, and view tags of a public NAT gateway on the Tags tab.

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
3. In the public NAT gateway list, locate the public NAT gateway whose tags you want to manage and click its name.

   The page showing details about the public NAT gateway is displayed.
4. Click the **Tags** tab and perform desired operations on tags.
   - View a tag.

     On the **Tags** tab, you can view tag details of the current public NAT gateway, including the number of tags and the key and value of each tag.
   - Add a tag.

     Click **Add Tag** in the upper left corner. In the displayed dialog box, enter the key and value of the tag to be added, and click **OK**.

     NOTE

     You can use the predefined tags as prompted to simplify tag adding operations. For details, see **Predefined Tags**.
   - Modify a tag.

     Locate the row that contains the tag to be edited and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, change the tag value and click **OK**.
   - Delete a tag.

     Locate the row that contains the tag to be deleted and click **Delete** in the **Operation** column. In the displayed **Delete Tag** dialog box, click **Yes**.

5 Monitoring

5.1 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

Table 5-1 Public NAT gateway metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway Unit: Count	≥ 0	Public NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bits/s	Public NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
outbound_bandwidth	Outbound Bandwidth	Outbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bits/s	Public NAT gateway	1 minute
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: Count	≥ 0	Public NAT gateway	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: Count	≥ 0	Public NAT gateway	1 minute
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Public NAT gateway	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Public NAT gateway	1 minute
snat_connection_ratio	SNAT Connection Usage	SNAT connection usage of the NAT gateway The maximum number of connections is the number of connections allowed by a NAT gateway type. For details, see **NAT Gateway Types**. Unit: Percent	≥ 0	Public NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
inbound_bandwidth_ratio	Inbound Bandwidth Usage	Inbound bandwidth usage of servers using the SNAT function. The maximum bandwidth supported by a public NAT gateway is 20 Gbit/s. Unit: Percent	≥ 0	Public NAT gateway	1 minute
outbound_bandwidth_ratio	Outbound Bandwidth Usage	Outbound bandwidth usage of servers using the SNAT function The maximum bandwidth supported by a public NAT gateway is 20 Gbit/s. Outbound bandwidth usage = Used bandwidth/Maximum bandwidth of the public NAT gateway x 100%. Unit: Percent **NOTE** This metric is used to monitor the performance of public NAT gateways instead of the EIP bandwidth.	≥ 0	Public NAT gateway	1 minute

Table 5-2 Private NAT gateway metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway Unit: Count	≥ 0	Private NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥0 bit/s	Private NAT gateway	1 minute
outbound_bandwidth	Outbound Bandwidth	Outbound bandwidth of servers using the SNAT function Unit: bit/s	≥0 bit/s	Private NAT gateway	1 minute
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: Count	≥ 0	Private NAT gateway	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: Count	≥ 0	Private NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Private NAT gateway	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Private NAT gateway	1 minute

Dimensions

Key	Value
nat_gateway_id	Public NAT gateway ID
vpc_nat_gateway_id	Private NAT gateway ID

5.2 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**, select **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.

6. On the **Create Alarm Rule** page, follow the prompts to configure the parameters.

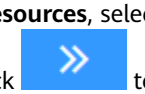
   a. Set the alarm rule name and description.

   Table 5-3 Configuring the alarm rule name and description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: **alarm-b6al**
Description	(Optional) Provides supplementary information about the alarm rule.

   b. Select an object to be monitored and set alarm rule parameters.

   Table 5-4 Parameters

Parameter	Description	Example Value
Resource Type	Specifies the type of the resource the alarm rule is created for.	NAT Gateway
Dimension	Specifies the metric dimension of the selected resource type.	Public NAT Gateway
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select **Resource groups** or **Specific resources**. **NOTE** • If **Resource groups** is selected and any resource in the group meets the alarm policy, an alarm is triggered. • If you select **Specific resources**, select one or more resources and click  to add them to the box on the right.	Specific resources
Method	There are two options: **Use template** or **Create manually**.	Create manually
Template	Specifies the template to be used. You can select a default alarm template or customize a template.	N/A

Parameter	Description	Example Value
Alarm Policy	Specifies the policy for triggering an alarm. If you set **Resource Type** to **Website Monitoring**, **Log Monitoring**, **Custom Monitoring**, or a specific cloud service, whether to trigger an alarm depends on whether the metric data in consecutive periods reaches the threshold. For example, Cloud Eye triggers an alarm if the raw data of the SNAT connections of the monitored object is 8000 or more for three consecutive 1-minute periods.	N/A
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major

c. Configure the alarm notification.

Table 5-5 Alarm notification parameters

Parameter	Description
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Object	Specifies the object that receives alarm notifications. You can select the account contact or a topic. • **Account contact** is the mobile phone number and email address of the registered account. • A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it. For details, see the **Cloud Eye User Guide**.
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00-20:00.
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

7. 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 configure alarm rules, see **Creating Alarm Rules**.

5.3 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

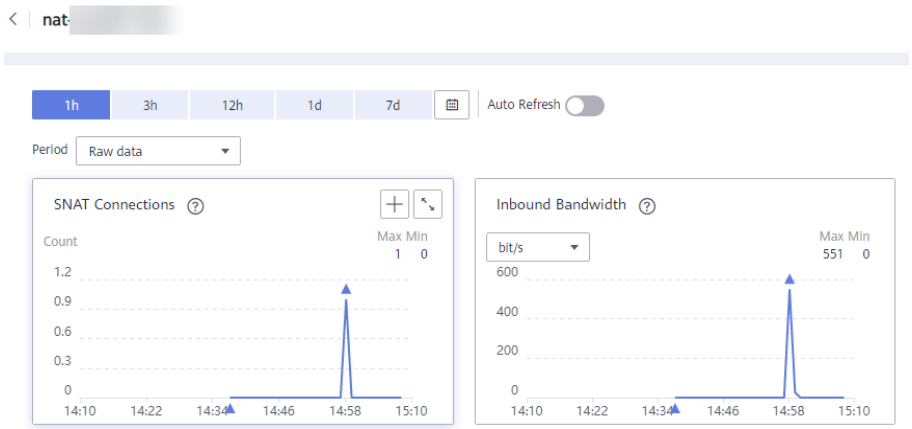
This section describes how to view NAT Gateway metrics.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the target region.
3. Under **Management & Deployment**, select **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 5-1 Viewing metrics



5.4 Viewing Metrics of Resources Using a NAT Gateway

Scenarios

You can view metrics details of resources using a specific NAT gateway. The resources can be ECSs or BMSs.

Procedure

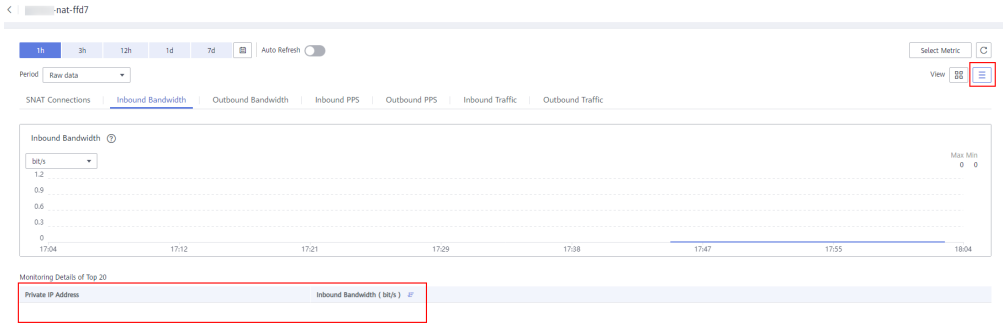
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.
4. Click the name of the NAT gateway whose metrics you want to view.
5. On the displayed page, choose the **Monitoring** tab and click **View Details**.

   On the Cloud Eye console, view metrics of the NAT Gateway.
6. Configure a time range for metrics to be viewed.
7. Click  in the upper right corner of the page to switch the display mode.
8. Select a metric to be viewed and click a specific time point in the displayed graph.

   In the lower part of the page, you can view the metric details of resources at the time point.

Figure 5-2 Viewing metrics



6 Auditing

6.1 Key Operations Recorded by CTS

You can use CTS to record operations on NAT Gateway for query, auditing, and backtracking.

Table 6-1 lists public NAT gateway operations that can be recorded by CTS.

Table 6-1 Public NAT gateway operations

Operation	Resource Type	Trace
Creating a public NAT gateway	natgateway	createNatGateway
Modifying a public NAT gateway	natgateway	updateNatGateway
Deleting a public NAT gateway	natgateway	deleteNatGateway
Creating a DNAT rule	dnatrule	createDnatRule
Modifying a DNAT rule	dnatrule	updateDnatRule
Deleting a DNAT rule	dnatrule	deleteDnatRule
Creating an SNAT rule	snatrule	createSnatRule
Modifying an SNAT rule	snatrule	updateSnatRule
Deleting an SNAT rule	snatrule	deleteSnatRule

6.2 Viewing Traces

Scenarios

CTS records the operations performed on NAT Gateway and allows you to view the operation records of the last seven days on the CTS console. This topic describes how to query these records.

Procedure

1. Log in to the management console.
2. In the upper left corner of the page, click and select the desired region and project.
3. Under **Management & Deployment**, click **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Specify the filters used for querying traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

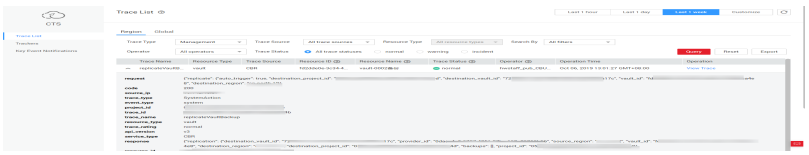
     Select a filter from the drop-down list.

     If you select **Trace name** for **Search By**, select a specific trace name.

     If you select **Resource ID** for **Search By**, select or enter a specific resource ID.

     If you select **Resource name** for **Search By**, select or enter a specific resource name.
   - **Operator**: Select a specific operator (at the user level rather than the tenant level).
   - **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.
   - Time range: You can query traces generated at any time range of the last seven days.
6. Click on the left of the required trace to expand its details.

   Figure 6-1 Expanding trace details

7. Click **View Trace** in the **Operation** column to view trace details.

Figure 6-2 View Trace

For details about key fields in the trace, see section "Trace Structure" in the ***Cloud Trace Service User Guide***.

A Change History

Released On	Description
2022-11-29	This is the twenty-second official release, which incorporates the following changes: Deleted the content of managing transit subnets in **Overview**, **Buying a Private NAT Gateway**, **Assigning a Transit IP Address**, **Adding an SNAT Rule**, **Adding a DNAT Rule**, **Assigning a Transit IP Address**, **Viewing a Transit IP Address**, and **Releasing a Transit IP Address** 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.
2022-08-30	This issue is the twentieth official release, which incorporates the following change: Added **Viewing Metrics of Resources Using a NAT Gateway**.
2022-07-27	This issue is the twentieth official release, which incorporates the following change: Deleted FAQ "What Is the Quota of Public NAT Gateways?" The numbers of DNAT rules and the number of SNAT rules supported by a NAT gateway are not quotas.
2022-06-15	This issue is the nineteenth official release, which incorporates the following change: Modified billing of private NAT gateways since the OBT of private NAT gateways ends.
2022-04-21	This issue is the eighteenth official release, which incorporates the following change: • Added **Adding a Default Route Pointing to the Public NAT Gateway**.

Released On	Description
2022-01-19	This issue is the seventeenth official release, which incorporates the following changes: • Added **Managing Transit IP Addresses**. • Added FAQs about private NAT gateways.
2021-12-29	This issue is the sixteenth official release, which incorporates the following change: • Added **Managing NAT Gateway Tags**.
2021-12-09	This issue is the fifteenth official release, which incorporates the following change: Updated Step 4: Test the Connection in **Configuring DNAT Rules to Enable Servers to Provide Services Accessible from the Internet**.
2021-11-12	This issue is the fourteenth official release, which incorporates the following change: Added **Auditing**.
2021-10-28	This is the thirteenth official release, which incorporates the following changes: • Added **Creating a User and Granting NAT Gateway Permissions**. • Added **NAT Gateway Custom Policies**.
2020-11-10	This issue is the twelfth official release, which incorporates the following change: Added the private NAT gateway function.
2020-06-24	This issue is the eleventh official release, which incorporates the following changes: • Modified FAQ "What Are the Differences Between an ECS Using a NAT Gateway and an ECS Having an EIP Bound?" • Added FAQ "Can I Change the VPC Selected When I Create a NAT Gateway?"
2020-05-08	This issue is the tenth official release, which incorporates the following change: Added description about SNAT rules and DNAT rules based on console changes.
2019-12-23	This issue is the ninth 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?"

Released On	Description
2019-11-05	This issue is the eighth official release, which incorporates the following change: Added the SNAT HA scenario.
2019-08-30	This issue is the seventh official release, which incorporates the following changes: ● Updated sections in "Overview". ● Added FAQs.
2019-03-30	This issue is the sixth 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.
2018-10-30	This issue is the fifth official release, which incorporates the following changes: ● Added the inter-cloud high-speed Internet access scenario. ● Optimized the document structure.
2018-07-30	This issue is the fourth official release, which incorporates the following changes: ● Added content in section "Monitoring". ● Supported the **All ports** type in a DNAT rule.
2018-06-08	This issue is the third official release, which incorporates the following change: Added an FAQ "Which Ports Cannot Be Accessed?"
2018-05-04	This issue is the second official release, which incorporates the following change: Added content about DNAT.
2018-04-20	This issue is the first official release.

