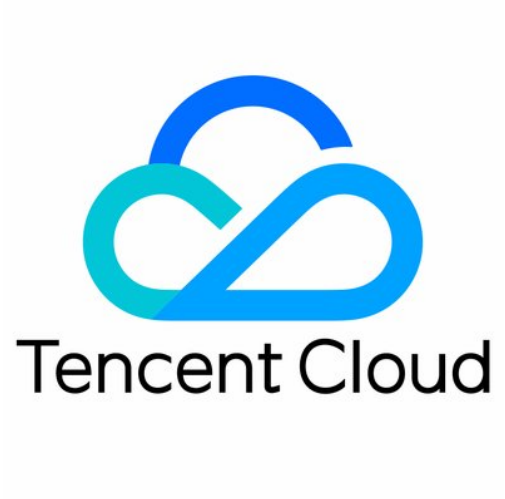
NAT Gateway

Operation Guide

Product Documentation



Contents

Operation Guide
Operation Overview

Last updated : 2020-08-19 10:40:13

This document describes some common operations for using NAT gateways (create and query port forwarding rules, manage EIPs, adjust configurations, and view bandwidth limit details) and the related products.

Common Operations

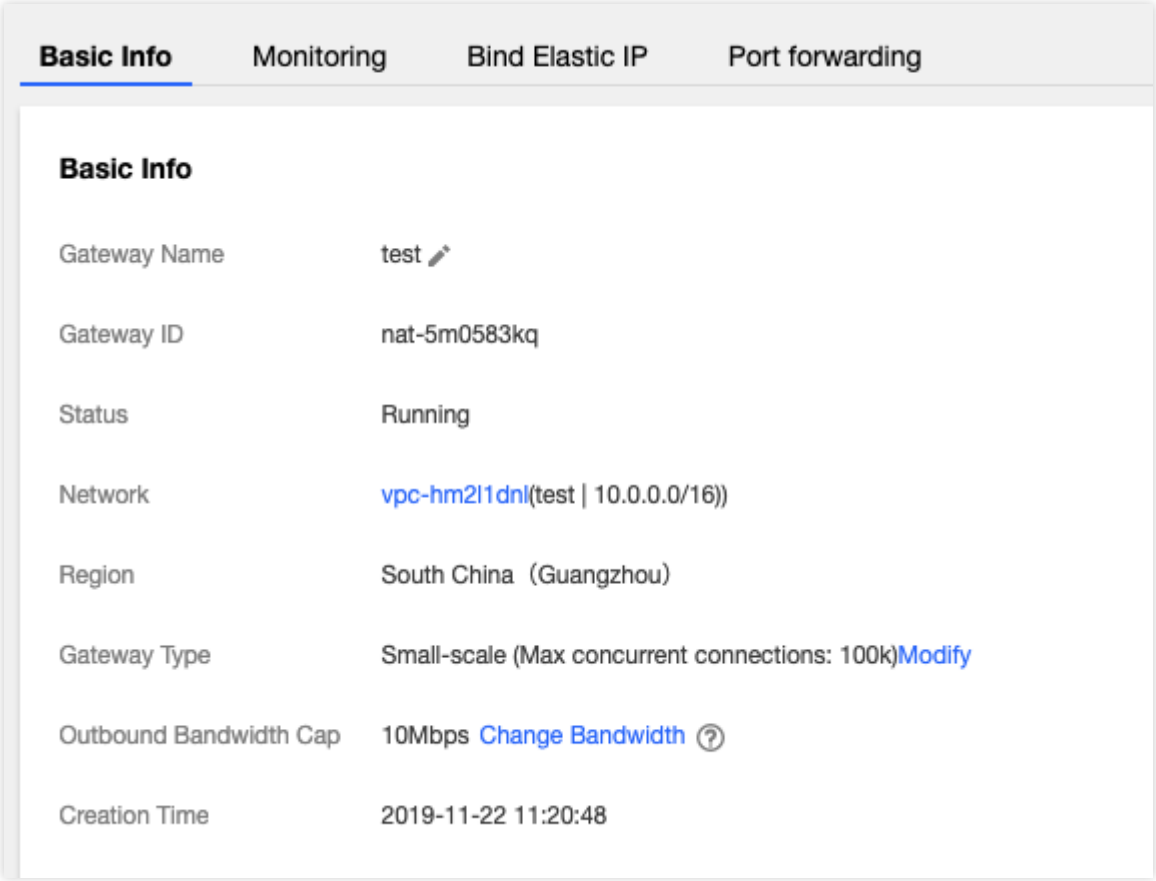
- Configuring a Route That Points to NAT Gateway
- Adjusting the Priorities of NAT Gateways and EIPs
- Creating a Port Forwarding Rule
- Querying a Port Forwarding Rule
- Modifying NAT Gateway Configuration
- Managing the EIPs Bound to a NAT Gateway
- Viewing NAT Gateway Monitoring Information
- Setting Alarms
- Deleting a NAT Gateway
- Enabling Gateway Traffic Monitoring and Control
- Setting Gateway Traffic Monitoring and Control
- Viewing Gateway Traffic Monitoring and Control
- Binding with an Anti-DDoS Pro Instance

Modifying NAT Gateway Configuration

Last updated : 2020-05-12 15:09:55

After creating a NAT gateway, you can modify its properties.

1. Log in to the Virtual Private Cloud Console.
2. In the list, click the ID of the desired NAT gateway to go to its details page, where you can perform the following operations.
   - Change the name of the gateway.
   - Change the gateway type. Once made, this change takes effect immediately. Changing the gateway type does not lead to network disconnection.
   - Change the outbound bandwidth cap.
   - Add a label for permission management.

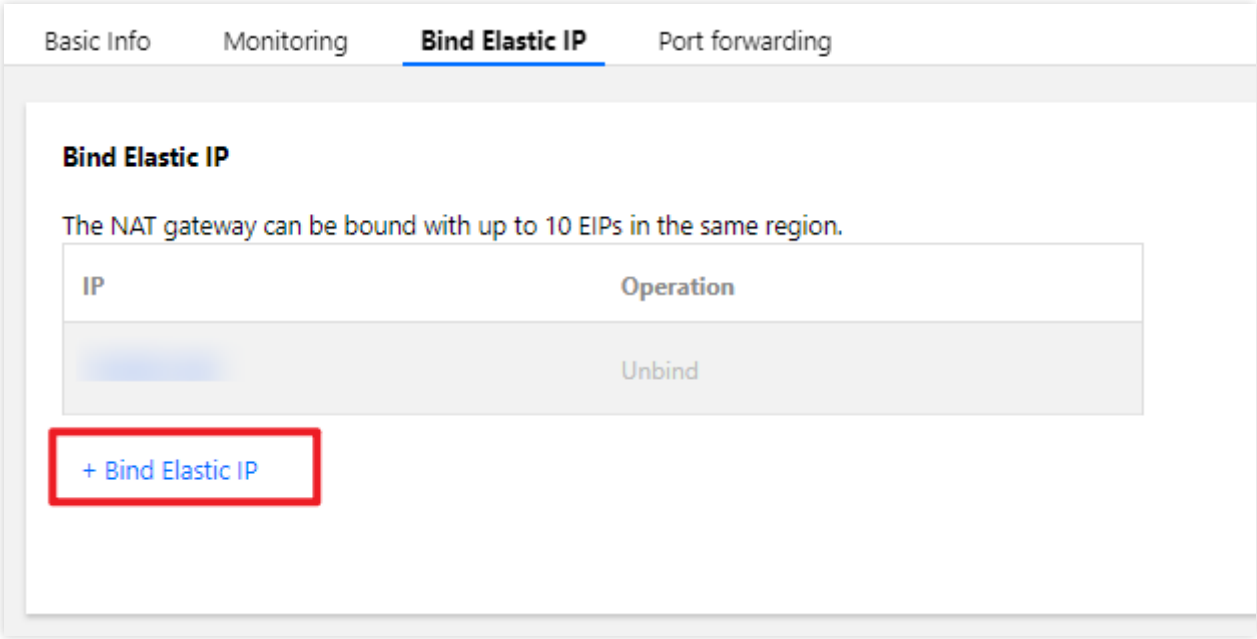


Managing EIPs of NAT Gateway

Last updated : 2020-01-16 11:26:38

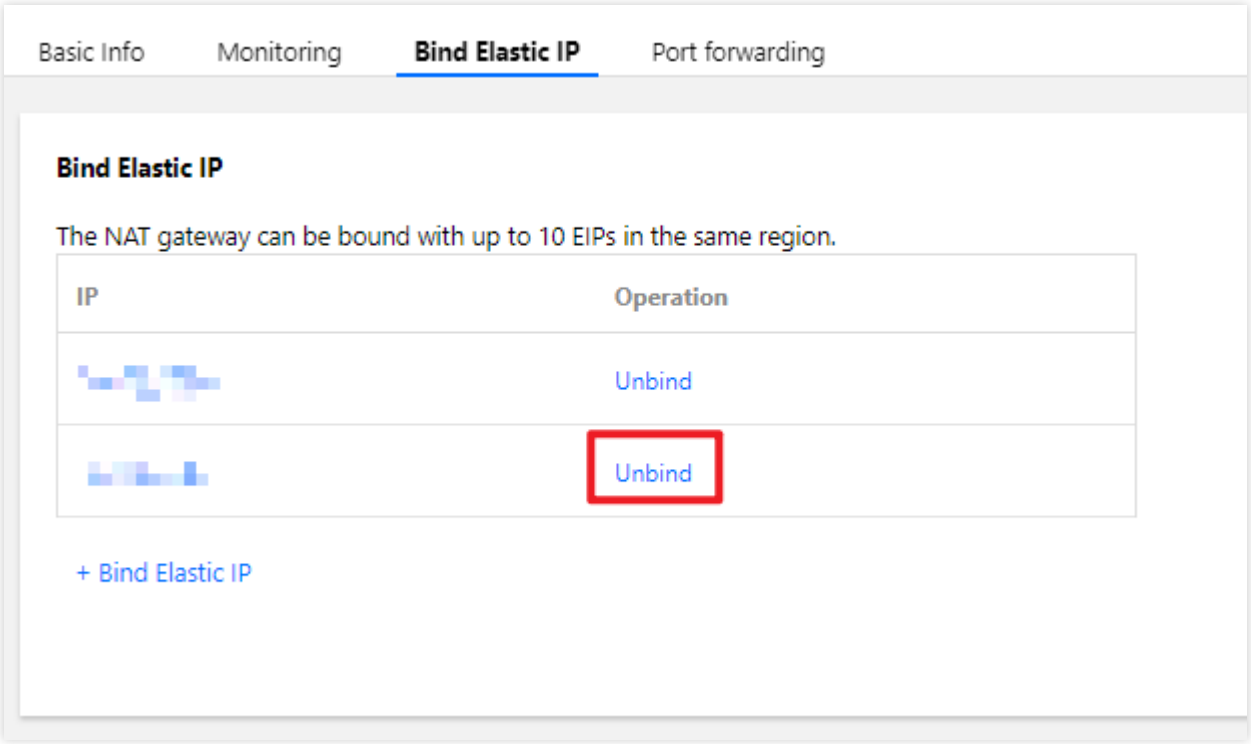
After creating a NAT gateway, you can manage the EIPs of the gateway by completing the steps below.

1. Log in to Tencent Cloud Console and choose **Products** > **Virtual Private Cloud* to open the VPC console. Then, click **NAT Gateway** in the left sidebar.
2. In the list, click the ID of the desired NAT gateway to go to its details page.
3. Click **Associate EIP**, and then choose to bind or unbind an EIP on this page.
   - Binding an EIP
     Click **Bind EIP**, choose the EIP to be bound in the drop-down box, and click **Save**.



   - Unbinding an EIP
     Click **Unbind** in the **Operation** column for the EIP that is to be unbound.

> At least one EIP must be retained.



Managing SNAT Rules

Last updated : 2021-08-24 10:02:13

You can bind EIPs to the NAT Gateway and assign them to different CVMs based on SNAT rules for the public network access.

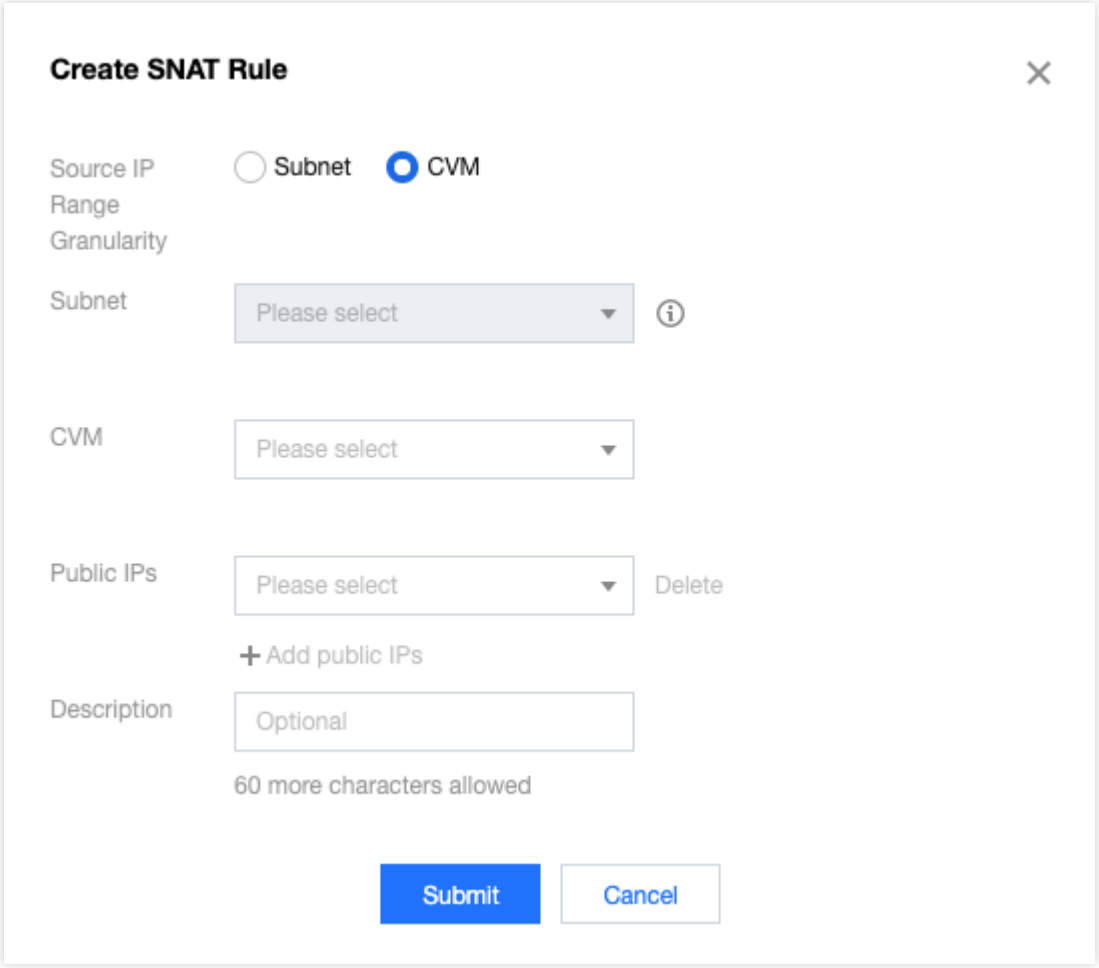
Assume a NAT Gateway is bound with EIPs including EIP1, EIP2, EIP3, and EIP4, they will automatically share the public network access traffic. If you add EIP1, EIP2, and EIP3 to the SNAT address pool, these in the address pool will be used to access the public network and share the access traffic.

This document describes how to create and manage a SNAT rule.

Creating a SNAT Rule

1. Log in to the VPC console.
2. Choose **NAT Gateway** on the left sidebar to go to the **NAT Gateway** page.
3. Click the **ID/Name** of the target gateway to enter its details page.
4. Select the **SNAT Rule** tab.
5. Click **Create**.
6. In the **Create SNAT Rule** dialog box, configure a SNAT rule as follows:
   - **Source IP Range Granularity**: select **Subnet** or **CVM**.
     - Subnet: when **Subnet** is selected, the associated route table of the subnet must point to the NAT Gateway, allowing CVMs in the subnet to access the public network based on the SNAT rule.
     - CVM: when **CVM** is selected, the route table associated with the subnet where the CVM instance resides must point to the NAT Gateway. Only the selected CVM instances can access the public network based on the SNAT rule.
   - **Subnet**: select a subnet or the subnet where the CVM instance resides.
   - **CVM**: select CVM instances from the drop-down list if **CVM** is selected for **Source IP Range Granularity**.
   - **Public IP**: assign EIP for the public network access.

- **Description**: enter the descriptive information, which cannot exceed 60 characters.



7. After the configuration is completed, click **Submit**.

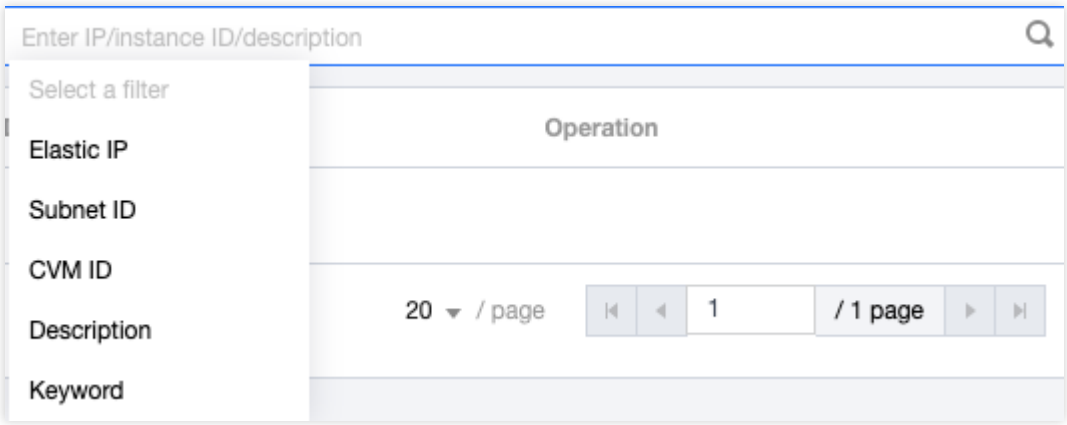
Editing a SNAT Rule

> Note :
> Please note that changing the public IP of an existing SNAT rule may cause business interruption, which will be resumed after reconnection.

1. Select the SNAT Rule tab and click **Edit** on the right of a SNAT rule.
2. Modify the public IP address or description, and click **Submit**.
3. Click the pencil icon next to **Description** of the selected SNAT rule to directly modify its description.

Querying SNAT Rules

1. In the top-right corner search box of the SNAT Rule tab, click to select a filter and enter the corresponding parameter value in the text box.



2. Click the search icon to filter results.
3. Click the **Subnet/CVM ID** to view the resource details.

Deleting SNAT Rules

You can delete SNAT rules if CVM can access the public network without a specified EIP.

- **Delete a single SNAT rule**
  i. Select the SNAT Rule tab and click **Delete** on the right of the target SNAT rule.
  ii. Click **Confirm** to delete the selected SNAT rule.
- **Batch delete SNAT rules**
  i. On the SNAT Rule tab, select SNAT rules and click **Delete** at the top of the list.
  ii. In the pop-up window, click **Delete** to complete the deletion.

Managing Port Forwarding Rules
Creating Port Forwarding Rule

Last updated：2020-02-24 14:33:46

A port forwarding table is a configuration table on a NAT gateway that is used to configure the DNAT feature on the NAT gateway. It maps the **[private IP, protocol and port]** collection of a CVM in the VPC to another **[public IP, protocol and port]** collection in the public network, so that resources on the CVM can be accessed from the public network.
You can create port forwarding rules by completing the steps below.

1. Log in to the Virtual Private Cloud Console.

2. In the list, click the ID of the desired NAT gateway to go to its details page. Click **Port Forwarding** tab.

3. Click **New**, select the protocol, external and internal IP ports, and click **OK**.

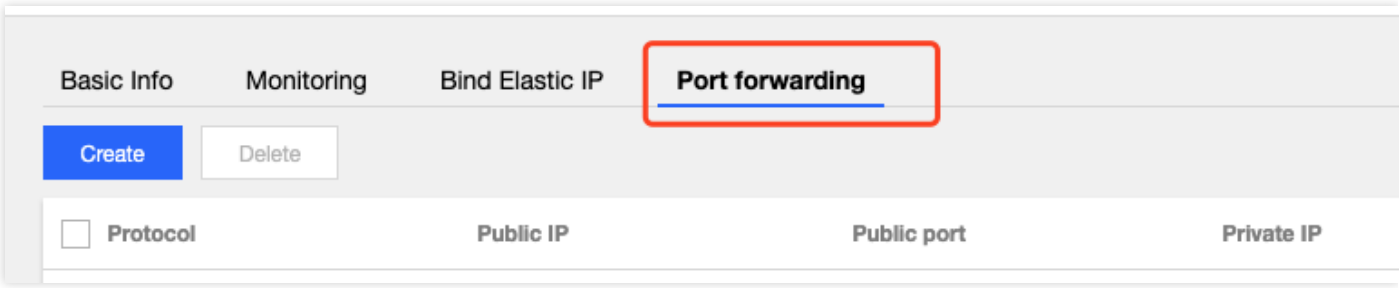
> The internal IP address only supports the private IP address of a CVM within the VPC.

Querying Port Forwarding Rule

Last updated : 2020-02-21 09:35:48

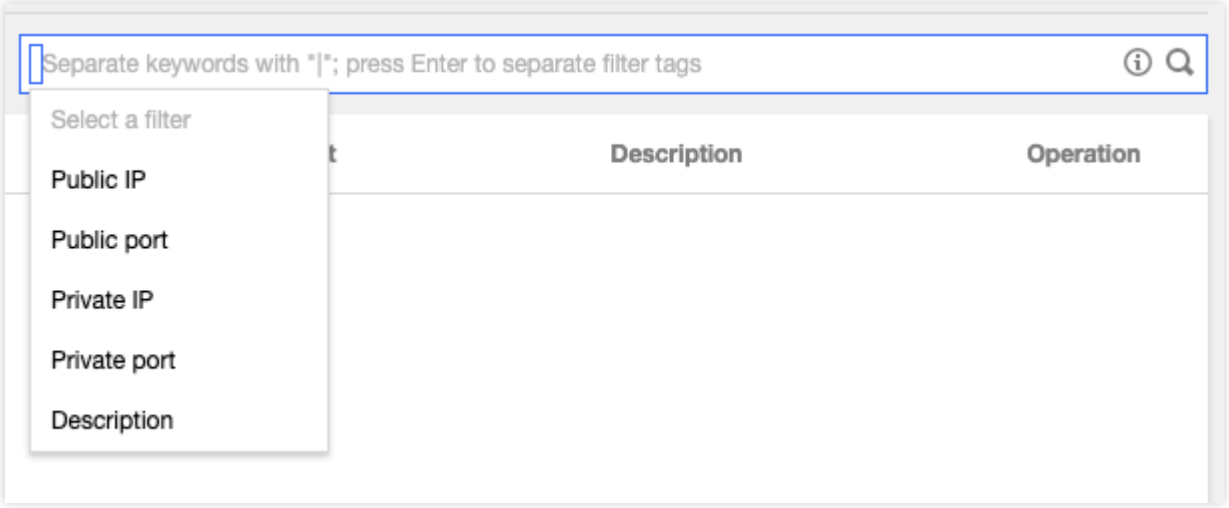
You can query port forwarding rules by completing the steps below.

1. Log in to Tencent Cloud Console and choose **Products** > **Virtual Private Cloud* to open the VPC console. Then, click **NAT Gateway** in the left sidebar.
2. In the NAT gateway list, click the ID of the NAT gateway to be queried to go to its details page. Then, select **Port Forwarding**.



3. In the search box, select a resource attribute value or enter a keyword to query the corresponding port forwarding rule.

> Be sure to check whether a NAT gateway routing policy has been added to the route table associated with the subnet where the instance resides.



Configuring a Route Pointing to NAT Gateway

Last updated : 2021-08-18 15:50:36

After creating a NAT gateway, you need to configure routing rules to direct the subnet traffic to the NAT gateway.

1. Click **Route Table** in the left sidebar of VPC Console.
2. In the route table list, click the route table ID/name associated with the subnet that needs to access the internet.
3. Click **+ New routing policies**.
4. In the pop-up window that appears, enter the destination (the public network access IP range), select **NAT Gateway** for **Next Hop Type**, and then select the created VPN gateway ID for **Next Hop**.
5. After you click **Create** to complete the configuration, the traffic generated when the CVM in the subnet associated with the route table accesses the Internet will be directed to the NAT gateway.

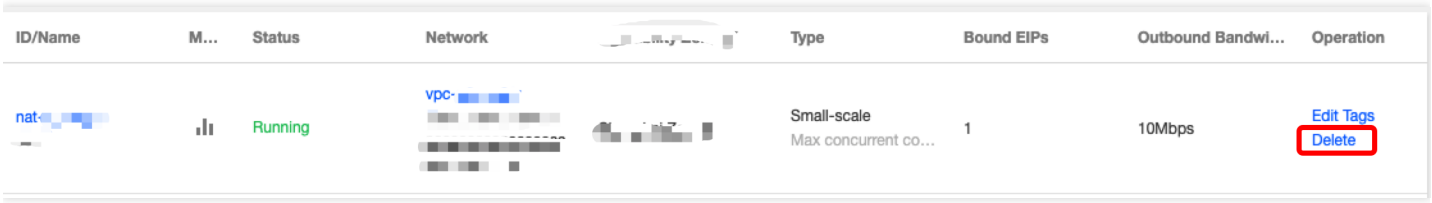
Deleteing NAT Gateway

Last updated : 2020-05-12 15:09:55

> Deleting a NAT gateway also deletes the gateway's routing table and all of its routing policies. This interrupts any requests to and from the public network. Therefore, make the necessary preparations in advance.

To delete a NAT gateway:

1. Log in to the Virtual Private Cloud Console.
2. Locate the desired NAT gateway and click the corresponding **Delete** button. Click **Delete** again to confirm the operation.

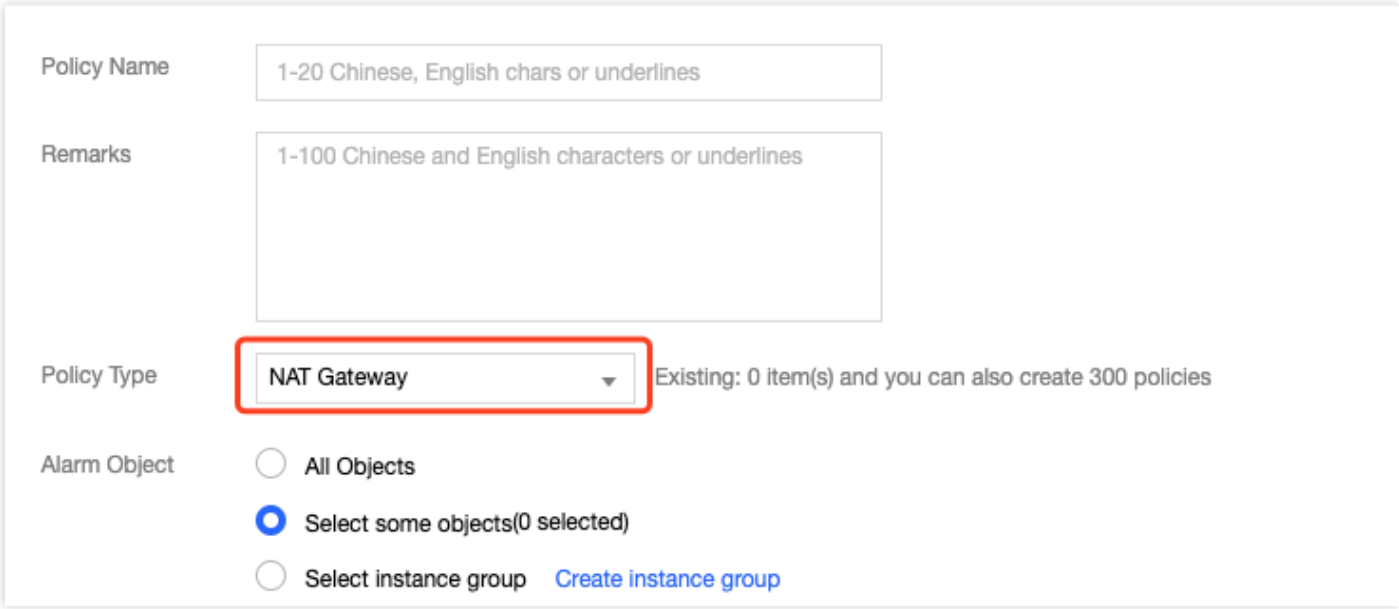


Monitoring and Alarms
Setting Alarms

Last updated : 2021-08-06 09:51:35

You can set an alarm for your NAT Gateway to monitor its status.

1. Log in to the Cloud Monitoring Console.
2. In the left sidebar, choose **Alarm Configuration** -> **Alarm Policy** to go to the **Alarm Policy** page, and then click **Add**.
3. Enter a name and remarks for the alarm policy. Select **NAT Gateway** for **Policy Type**. Configure the alarm object, triggering condition, and alarm channels. You can optionally input the URL that can be accessed by the public network as the callback API address, so Cloud Monitoring will push the alarm information to this address in time.



4. Click **Complete**. Then, you can view the alarm policy that you configured in the alarm list.

> Note :
> To delete an alarm policy, you must first unbind all resources from it.

5. When the alarm condition is triggered, you will receive an alarm notification via SMS, email, or in Message Center according to the alarm channel you configured. You can also select **Alarm List** in the left sidebar to view alarms. For more information, see Creating Alarm Policies.

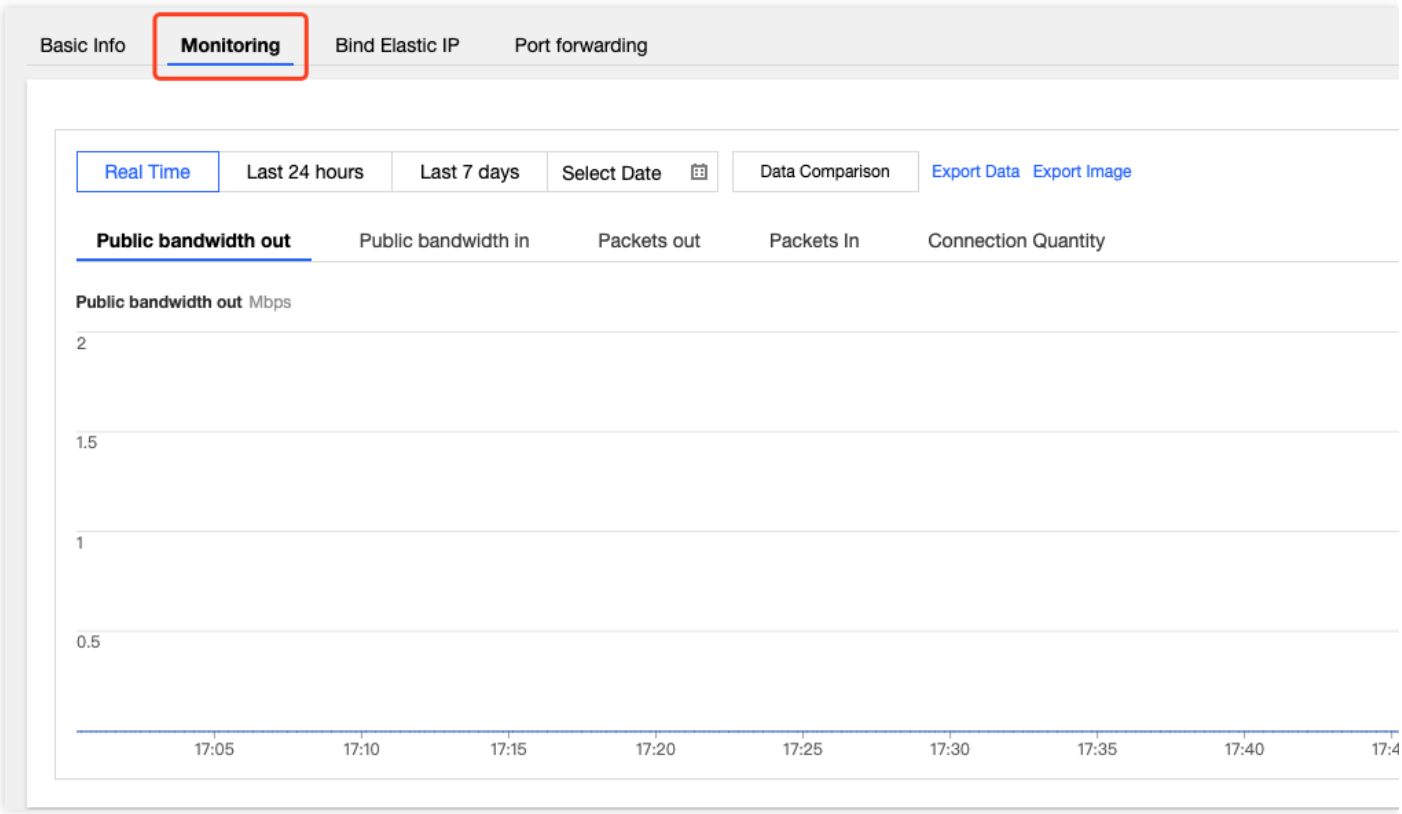
Note :
Packet loss caused by bandwidth glitches may not be reflected on the bandwidth view, because the minimum granularity for bandwidth statistics is 10 seconds (total traffic in 10 seconds/10 seconds).

Viewing Monitoring Information

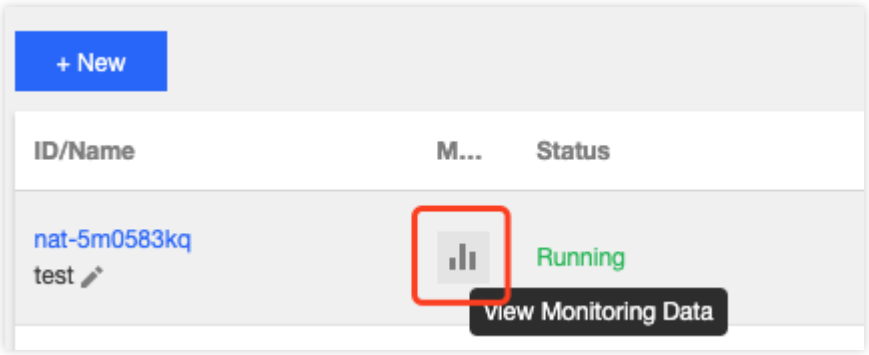
Last updated : 2020-05-12 15:09:55

Once a NAT gateway is created, you can use the console to view and export its monitoring information.

1. Log in to the Virtual Private Cloud Console.
2. In the NAT gateway list, click the ID of the desired NAT gateway. The gateway details page appears.
3. Click **Monitoring** to display monitoring information. Click **Export Data** or **Export Image** to save the information to your local device.



4. You can also click **View Monitoring Data** that corresponds to the desired NAT gateway to view its monitoring information, as shown in the following figure:



Binding with Anti-DDoS Pro

Last updated : 2020-03-04 17:49:45

You can bind an Anti-DDoS Pro instance to a NAT gateway to defend against DDoS attacks.

1. Purchase an Anti-DDoS Pro instance.
2. For detailed instructions on how to configure Anti-DDoS Pro for a NAT gateway, see Getting Started with Anti-DDoS Pro.

Adjusting the Priorities of NAT Gateways and EIPs

Last updated : 2020-02-24 14:27:29

Description of NAT Gateway and EIP Priorities

When a subnet is associated with a NAT gateway, and the CVM in the subnet has a public IP address (or an EIP), the CVM accesses the Internet through the NAT gateway by default because the priority of the exact match route is higher than that of the public IP address. However, you can set a routing policy to allow the CVM to access the Internet through its public IP address.

Directions

1. View the route table associated with the subnet where the CVM resides. Ensure that a routing policy that points to the NAT gateway exists so that CVMs in the subnet that have no public IP addresses can still access the Internet through the NAT gateway.

2. Add a routing policy with the next hop type set to the public IP of the CVM, and enter the destination.
   - Destination: Enter the specific public network range that your service needs to access or the default route (that is, 0.0.0.0/0, which indicates that the destination is not in the route table and all data packets are transmitted in the default route).
   - Next Hop Type: Public IP address of the CVM.

- When the routing policy is configured with the same destination as the routing rules that are directed to the NAT gateway, the CVM, and the public gateway, this route will be matched first.
- This routing policy affects all subnets associated with the route table, in which case please evaluate the impact of the operation. In other words, CVMs in these subnets that have public IP addresses (or elastic IP addresses) will access the Internet through their respective public IP address instead of the NAT gateway.
- In the subnet associated with the route table, CVMs that have no public IP addresses can still access the Internet through the NAT gateway without being affected.