NAT Gateway

Public NAT Gateway Operation Guide

Product Documentation

Contents

Public NAT Gateway Operation Guide
Operation Overview

Last updated：2022-03-28 14:14:26

This document lists the common NAT gateway-related operations.

Common operations

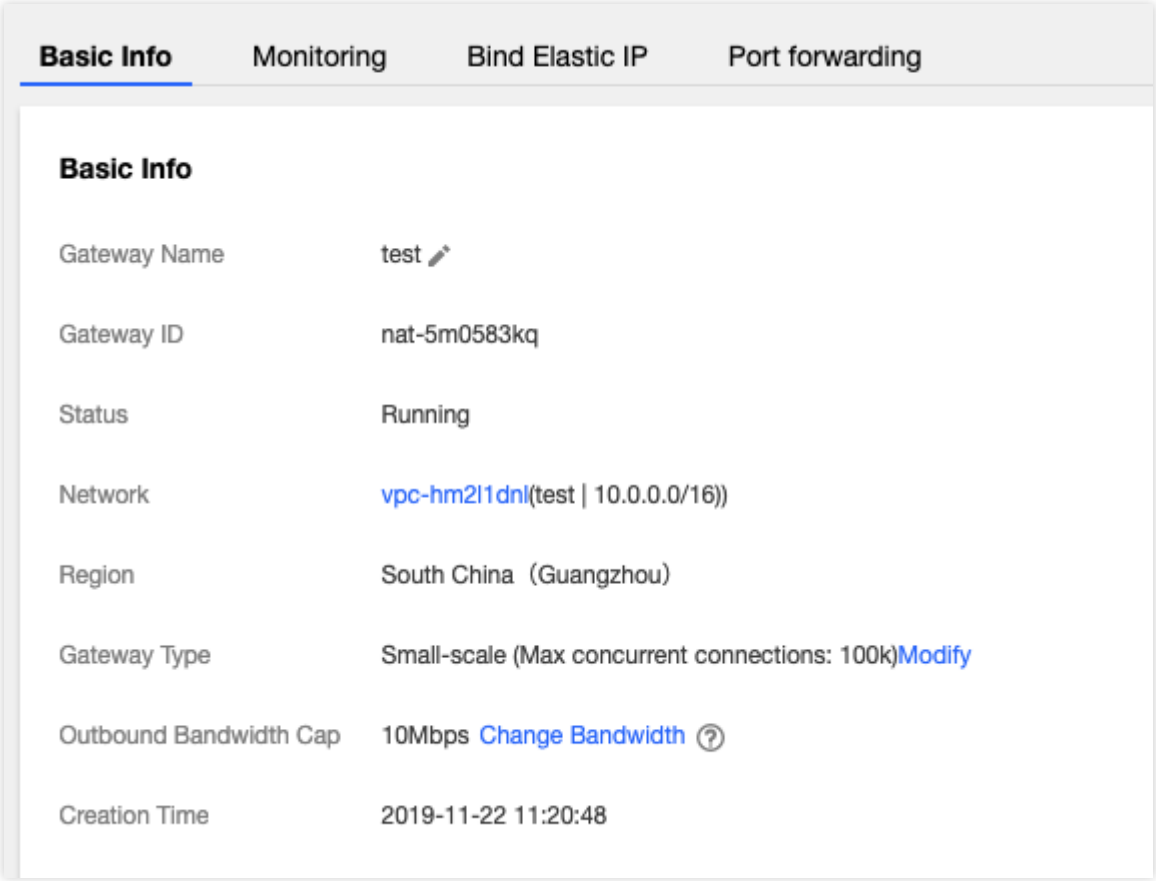
- Routing to NAT Gateway
- Modifying NAT Gateway Configuration
- Managing EIPs Bound to a NAT Gateway
- Managing SNAT Rules
- Managing Port Forwarding Rules
- Deleting NAT Gateway
- Configuring Alarm Policies
- Binding Anti-DDoS Pro Instance
- Adjusting Priorities of NAT Gateways & EIPs

Modifying NAT Gateway Configuration

Last updated：2021-12-10 11:09:43

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

1. Log in to the NAT Gateway 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：2022-05-20 11:02:14

After creating a NAT gateway, you can follow the directions to manage the EIPs of the gateway.

Directions

1. Log in to the **NAT Gateway console**.
2. Click the ID of the target NAT gateway to go to its details page.
3. Click the **Bind EIP** tab. On this tab, you can view the EIPs bound to the NAT gateway and manage them.

Binding EIPs

Note：

- Loads are automatically balanced if the NAT gateway is bound to multiple EIPs.
- Currently, you can bind the existing EIPs only. To bind more EIPs, create them first in the Public IP console.

1. Click **Bind EIP** on the top of the tab.

2. In the **Select IP** drop-down list, select the EIP or EIPs to be bound, and then click **OK**.
3. Click **OK**.

Adjusting the bandwidth of the EIP

1. Find the target EIP, click **Adjust bandwidth** under the operation column.

2. Adjust the bandwidth of the target in the pop-up window, and then click **OK**.

Unbinding EIPs

Note：
When the NAT gateway is bound with only one EIP, the unbinding is not supported.

1. Find the target EIP, click **Unbind** under the operation column.

2. In the **Confirm unbinding** pop-up window, click **OK**.

Routing to NAT Gateway

Last updated：2022-03-28 14:52:30

After the NAT Gateway is created, you need to configure routing policies to direct the subnet traffic to the NAT Gateway.
There are two options:

- Method 1: Configure in the **NAT Gateway** console
- Method 2: Configure in the **Route Table** console

Directions

Method 1: Configure in the NAT Gateway console

1. Log in to the **NAT Gateway console**.
2. In the NAT gateway list, click the VPC ID of the target NAT gateway.

3. Click **Subnet** in the VPC details page.

4. In the **Subnets** list, find the subnet that needs to access the internet and click the route table ID.
5. Click **+New routing policies** on the **Basic Information** page.

6. In the **Add route** box, enter the destination (public IP range), select **NAT gateway** in **Next hop type** and choose an existing NAT gateway.

7. Click **Create** to complete.

Method 2: Configure in the Route Table console

1. Log in to the VPC console and click **Route Tables** on the left sidebar.
2. Locate the route table associated with the subnet that needs to access the Internet, and click its **ID**/**Name** to enter the details page.

3. Click **+New routing policies** on the **Basic Information** page.

4. In the **Add route** box, enter the destination (public IP range), select **NAT gateway** in **Next hop type** and choose an existing NAT gateway.

5. Click **Create** to complete.

Managing SNAT Rules

Last updated：2022-07-22 19:10:52

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

Assume that a NAT gateway is bound with EIPs including EIP1, EIP2, EIP3, and EIP4. The load balancer distributes the access traffic to these EIPs for CVM access to the public network. If EIP1, EIP2 and EIP3 are added to the SNAT address pool, CLB will distribute the access traffic to the three EIPs, and CVM will use them to access the public network. The CVMs that do not have a SNAT rule configured can access the public network through all EIPs bound to the NAT.

Note：

- When the load on a CVM instance surges, one EIP may not be enough to support huge access traffic, so you can choose to configure multiple EIPs.
- In a NAT gateway, an EIP can be set in the SNAT rule and port forwarding rule at the same time. See Creating Port Forwarding Rule.

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

Rule Limits

- When an EIP is disassociated from a NAT gateway, the SANT rule is also deleted if the EIP is the only EIP.
- If the subnet configured for a SNAT rule does not exist, the SNAT rule is deleted as well.
- If the CVM configured for a SNAT rule does not exist, the SNAT rule is also deleted if this is the last CVM; otherwise, the CVM is deleted from the SNAT rule.
- Restricted by standard protocols, for the NAT gateways with the same protocol/destination IP/destination port, the number of maximum connections = the number of bound EIPs × 55000. To increase the number of connections, bind new EIPs or adjust the destination IP/port.

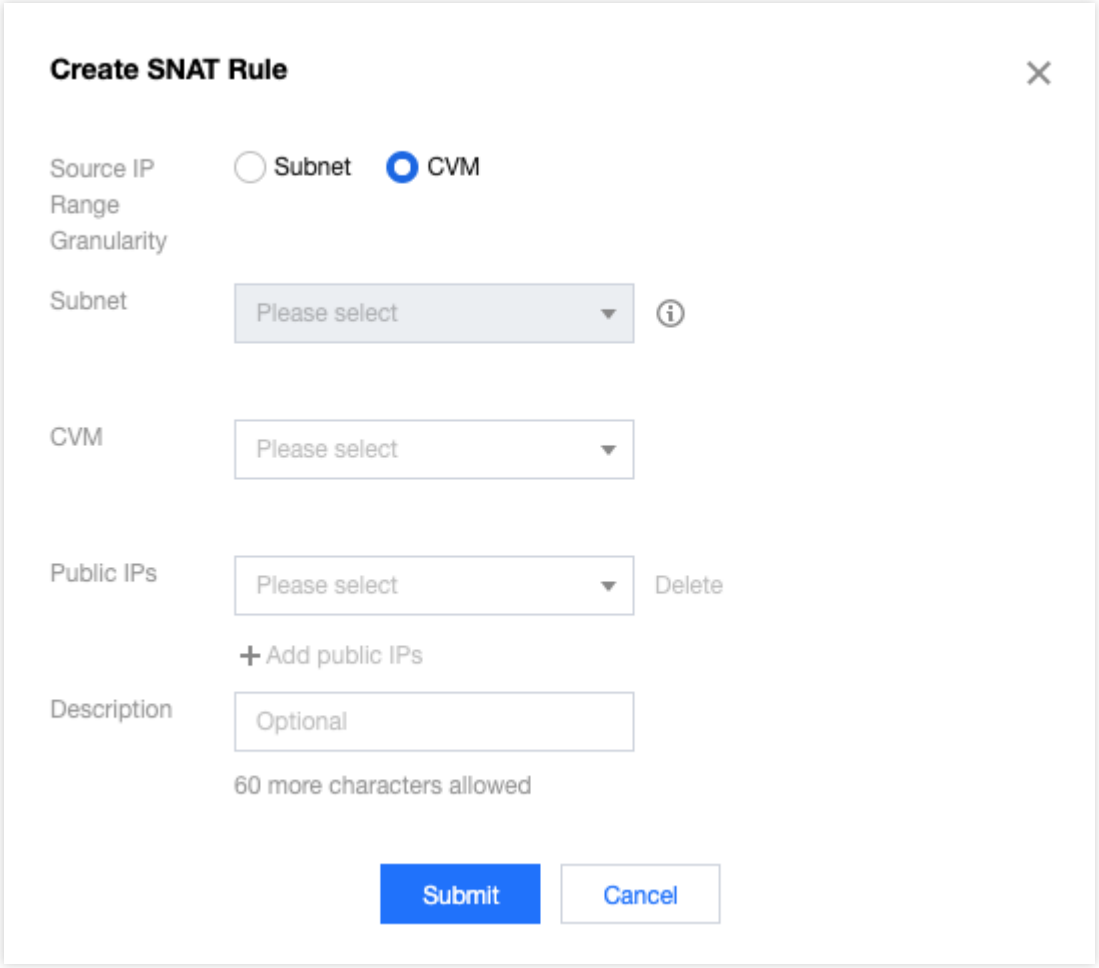
Prerequisites

Before creating a SNAT rule, make sure the route table where the subnet resides points to the corresponding NAT gateway. See Routing to NAT Gateway.

Creating a SNAT Rule

1. Log in to the NAT Gateway console.
2. Click the ID of the target NAT gateway to go to its details page.
3. Select the **SNAT rule** tab and enter the SNAT rule management page.
4. Click **Create**.
5. 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 resides must point to the NAT gateway. Only the selected CVMs can access the public network based on the SNAT rule. The CVMs that do not have a SNAT rule configured can access the public network through all EIPs bound to the NAT.
   - 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 with up to 60 characters.



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

Modifying 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. On the SNAT rule tab, click **Edit** on the right side of SNAT rule entry to enter the dialog box.

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 search box at the top right of the SNAT rule tab, click to select the following filters, and enter the corresponding parameter values in the input 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**

1. Click **Delete** to the right of the SNAT rule entry on the SNAT rule tab.
2. Click **Confirm** to delete the selected SNAT rule.

- **Batch delete SNAT rules**

1. On the SNAT rule tab, check several SNAT rules and click **Delete** at the top.

2. In the pop-up window, click **Delete**.

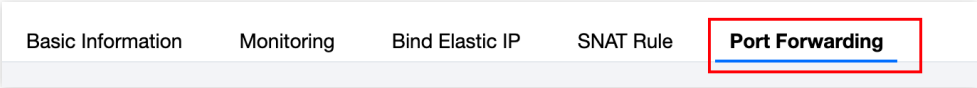
Managing Port Forwarding Rules
Creating Port Forwarding Rule

Last updated：2022-03-28 14:14:26

A port forwarding table configures the DNAT feature on the NAT gateway. It maps the combination of **[private IP, protocol and port]** of a CVM in the VPC to a combination of **[public IP, protocol and port]** 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.

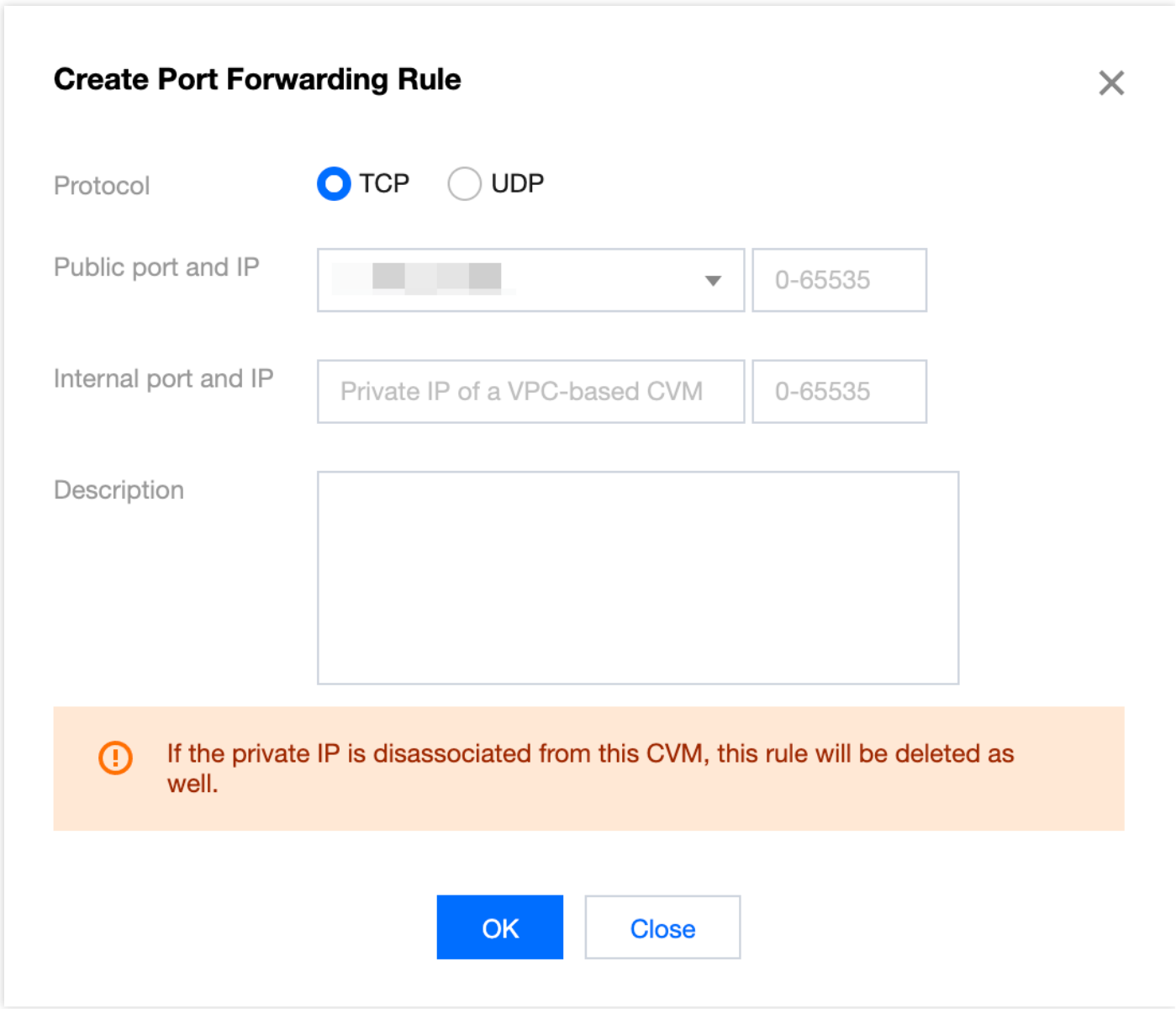
> Note：
> In a NAT gateway, an EIP can be set in the SNAT rule and port forwarding rule at the same time. See Managing SNAT Rules.

1. Log in to the **NAT Gateway console**.
2. In the list, click the ID of the target NAT gateway to go to its details page. Click **Port Forwarding** tab.



3. Click **Create**, specify the **Protocol**, **Public port and IP** and **Internal port and IP**, and click **OK**.

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

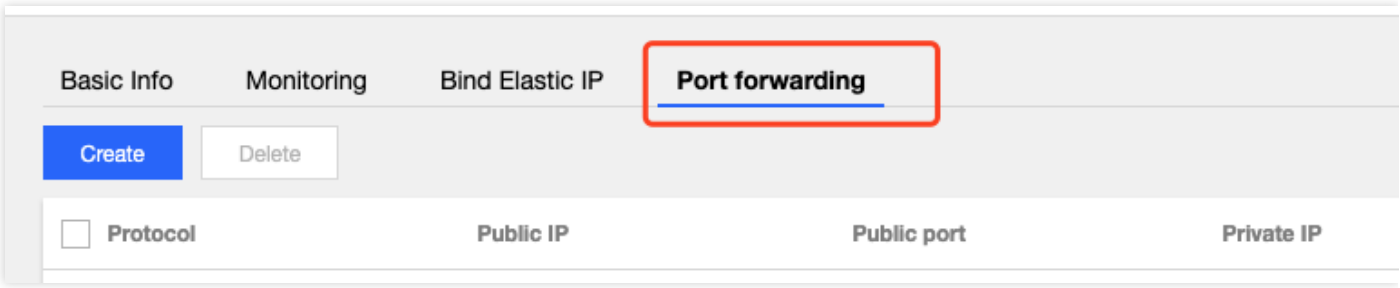


Querying Port Forwarding Rule

Last updated：2021-12-13 16:09:46

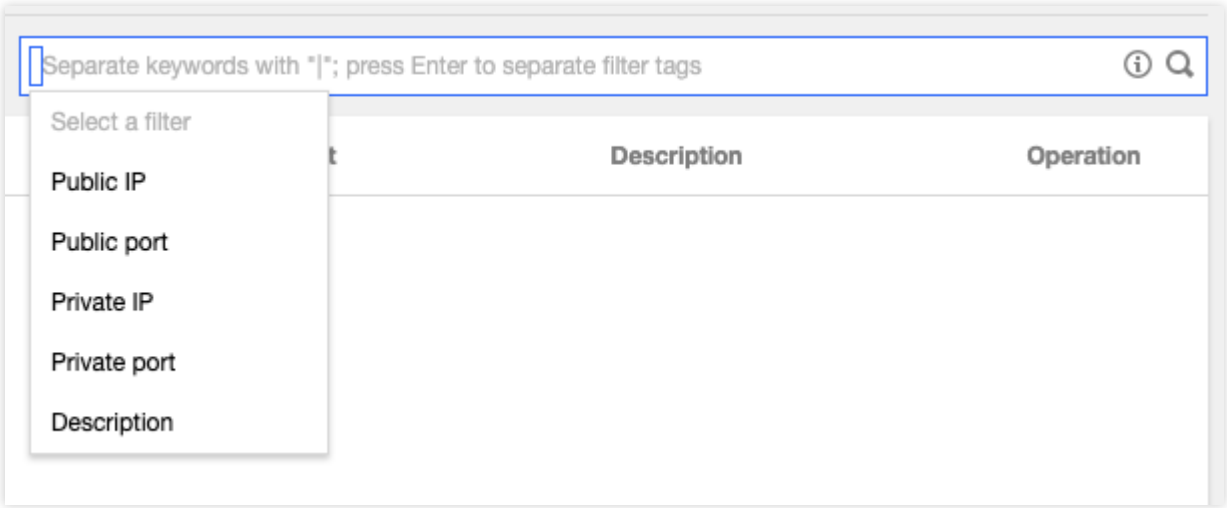
You can query port forwarding rules by completing the steps below.

1. Log in to NAT gateway Console
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.

> Note：
> 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.



Public NAT Usage Limits

Last updated：2023-08-03 16:33:11

This document describes the usage rules and limits of NAT gateways.

> Note：
> NAT Gateway supports TCP, UDP and ICMP, while ESP and AH for the GRE tunnel and IPSec cannot be used for the NAT Gateway, and ALG technologies are not supported. This is specific to NAT Gateway and irrelevant to service providers. Nevertheless, these supported protocols can mostly meet your application demands.

Use Rules

Note the following when using NAT Gateway:

- After a NAT Gateway is deleted, the associated EIPs are disassociated but not released.
- A NAT Gateway cannot be associated with security groups. However, you can bind security groups to instances within the VPC subnet to control their inbound and outbound traffic.
- The inbound and outbound traffic of the NAT Gateway cannot be directly controlled by the network ACL. Instead, you can use network ACL to control the traffic of the subnet associated with the NAT Gateway.
- You cannot use VPC peering connection or VPN connection to route traffic to a NAT Gateway.
  For example, a NAT Gateway enables traffic from VPC1 to the Internet, and VPC1 establishes a peering connection with VPC2. In this case, all the resources within VPC2 can access VPC1, but cannot access the Internet through the NAT Gateway.

Rule Limits

- When an EIP is disassociated from a NAT gateway, the SANT rule is also deleted if the EIP is the only EIP.
- If the subnet configured for a SNAT rule does not exist, the SNAT rule is deleted as well.
- If the CVM configured for a SNAT rule does not exist, the SNAT rule is also deleted if this is the last CVM; otherwise, the CVM is deleted from the SNAT rule.
- Restricted by standard protocols, for the NAT gateways with the same protocol/destination IP/destination port, the number of maximum connections = the number of bound EIPs × 55000. To increase the number of connections, bind new EIPs or adjust the destination IP/port.

Service Quota

The following table lists the restrictions on the supported resources for the NAT Gateway. For limits on other VPC resources, see Quota Limit.

Resource	Limit
Number of NAT Gateways per VPC	3
Number of EIPs per NAT Gateway	10
Maximum forwarding capability per NAT Gateway	5 Gbps
Maximum number of forwarding rules per NAT Gateway	200
Number of SNAT rules per NAT Gateway	200

NAT Gateway Flow Logs

Last updated：2022-07-22 19:36:42

NAT Gateway provides the flow log collection feature to collect and analyze NAT Gateway traffic and generate logs and analysis charts. This helps you stay informed of cross-region communication and quickly locate and solve problems based on the logs, thus improving the business availability and Ops efficiency.

Note：

- The flow log feature is in beta test. To try it out, submit a ticket for application.
- The Flow Log service is free of charge, but the data stored in CLS will be charged at the standard prices of CLS.
- The flow log data is stored in CLS. Make sure that you have granted the Flow Log service permissions to access CLS before querying log data in CLS.

Directions

1. Log in to the VPC console and select **Flow Logs** > **Log List** in the left sidebar.
2. Select the region in the top-left corner of the **Flow Logs** page and click **+Create**.
3. Configure the following parameters in the **Create flow log** window.

Field	Description
Name	The name of the flow log.
Collection range	Select “NAT Gateway”.
NAT gateway	The information about the NAT gateway.
Collection type	Specify the type of traffic to be collected by the flow log: All traffic, or the traffic rejected or accepted by security groups or ACL.
Logset	Specify the storage location in CLS for flow logs. If you already have a logset, select it directly; otherwise, keep **Created by system** selected, so that the system will create one for you. You can also click **Create** to create one in the CLS console.

Log topic	Specify the minimum dimension of log storage, which is used to distinguish between different types of logs, such as `Accept` log. If you already have a log topic, select it directly; otherwise, keep **Created by system** selected, so that the system will create one for you. You can also go to the CLS console to create one. Note For more information on how to configure a logset, log topic, and index, see Creating Logsets and Log Topics.
Tag key	Click **Advanced options** to enter or select a tag key for the identification and management of the flow log.
Tag value	Click **Advanced options** to enter or select a tag value. It can also be left empty.

4. Click **OK**.

Note
You can view the record of a newly created flow log in CLS after six minutes upon the creation (one minute for the capture window and five minutes for data publishing).

5. After about six minutes, click **Storage location** or **View** to enter the **Search and analysis** page of the CLS service, select the region and time period for which to view logs, and click **Search and analyze** to view the logs.

Below are sample logs:

Note：
For fields description, see Flow Log Record. For log analysis, see Quick Analysis.

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.

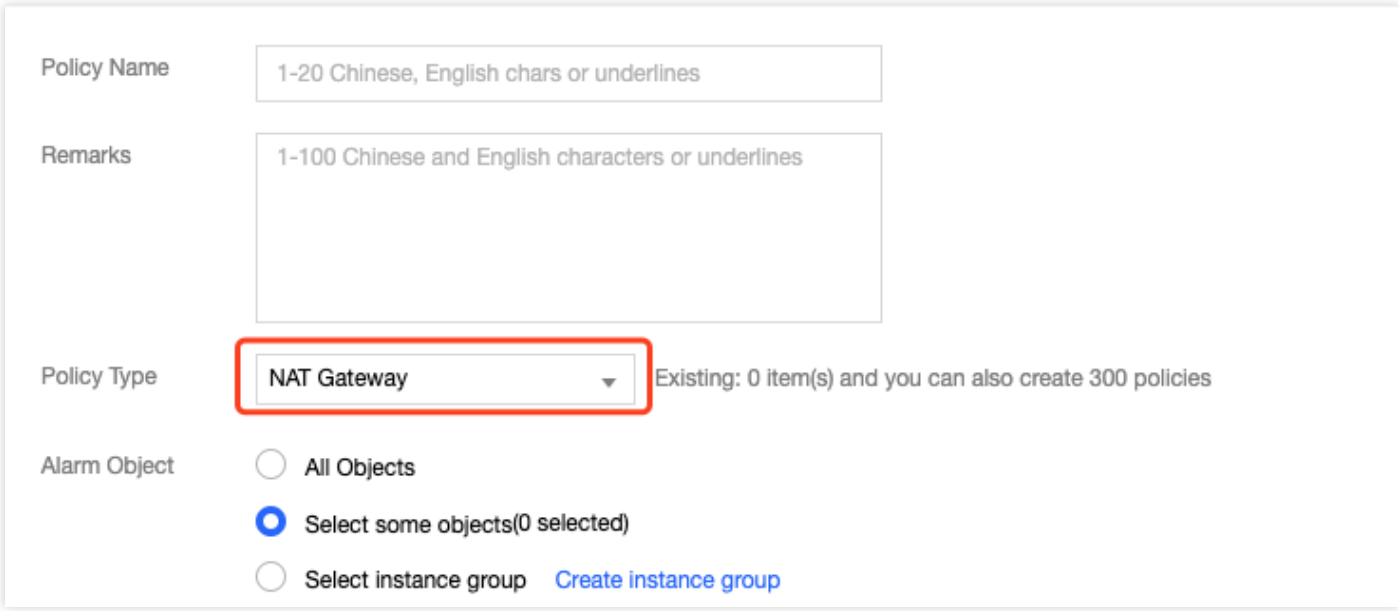
1. Purchase an Anti-DDoS Pro instance.
2. For detailed instructions on how to configure Anti-DDoS Pro for a NAT gateway, see Getting Started with Anti-DDoS Pro.

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：2022-07-22 19:10:52

After creating a NAT gateway, you can view and export its monitoring information in the console.

1. Log in to the NAT Gateway console.
2. In the NAT gateway list, click the ID of the desired NAT gateway to enter the details page.
3. Select the **Monitoring** tab.

- Click . Click **Export data** or **Export image** to save the information to your local device.
- Click  to display the chart in full screen mode.
- Click  to configure an alarm.

4. (Optional) You can also click the “View monitoring data” button that corresponds to the desired NAT gateway to view its monitoring information.

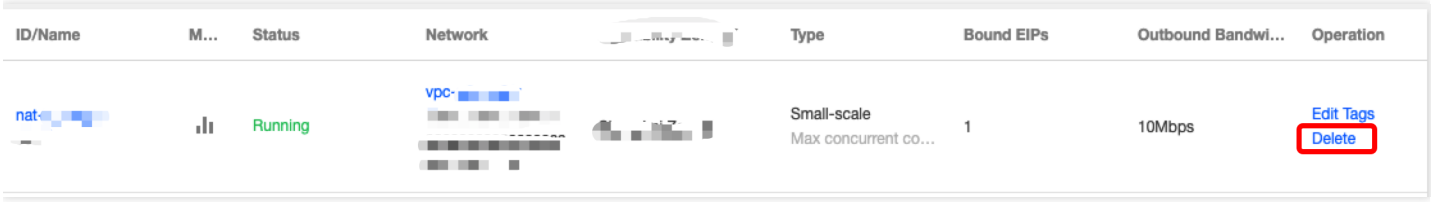
Deleting NAT Gateway

Last updated：2022-02-08 12:01:02

Note：
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 NAT Gateway Console.
2. Locate the desired NAT gateway and click the corresponding **Delete** button. Click **Delete** again to confirm the operation.



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.