NAT Gateway

Product Documentation

Contents

NAT Gateway 3
- Product Introduction 3
  - Overview 3
  - Product Features 6
  - Use Cases 7
  - Product Specifications 8
  - Use Limits 9
  - Related Products 10
- Purchase Guide 12
  - Billing Overview 12
  - Purchase Method 15
- Quick Start 18
- Operation Guide 21
  - Configuring a Route Pointing to the NAT Gateway 21
  - Adjusting the Priority of NAT Gateway and EIP 22
  - Managing Port Forwarding Rules 24
    - Creating Port Forwarding Rules 24
    - Querying Port Forwarding Rules 25
  - Modifying NAT Gateway Configuration 26
  - Managing NATGW EIPs 27
  - Managing SNAT Rules 30
  - Viewing Monitoring Information 34
  - Setting Alarms 35
  - Deleting a NAT Gateway 36
- FAQs 37
  - Concepts 37
  - Function Category 39

Product Introduction
Overview

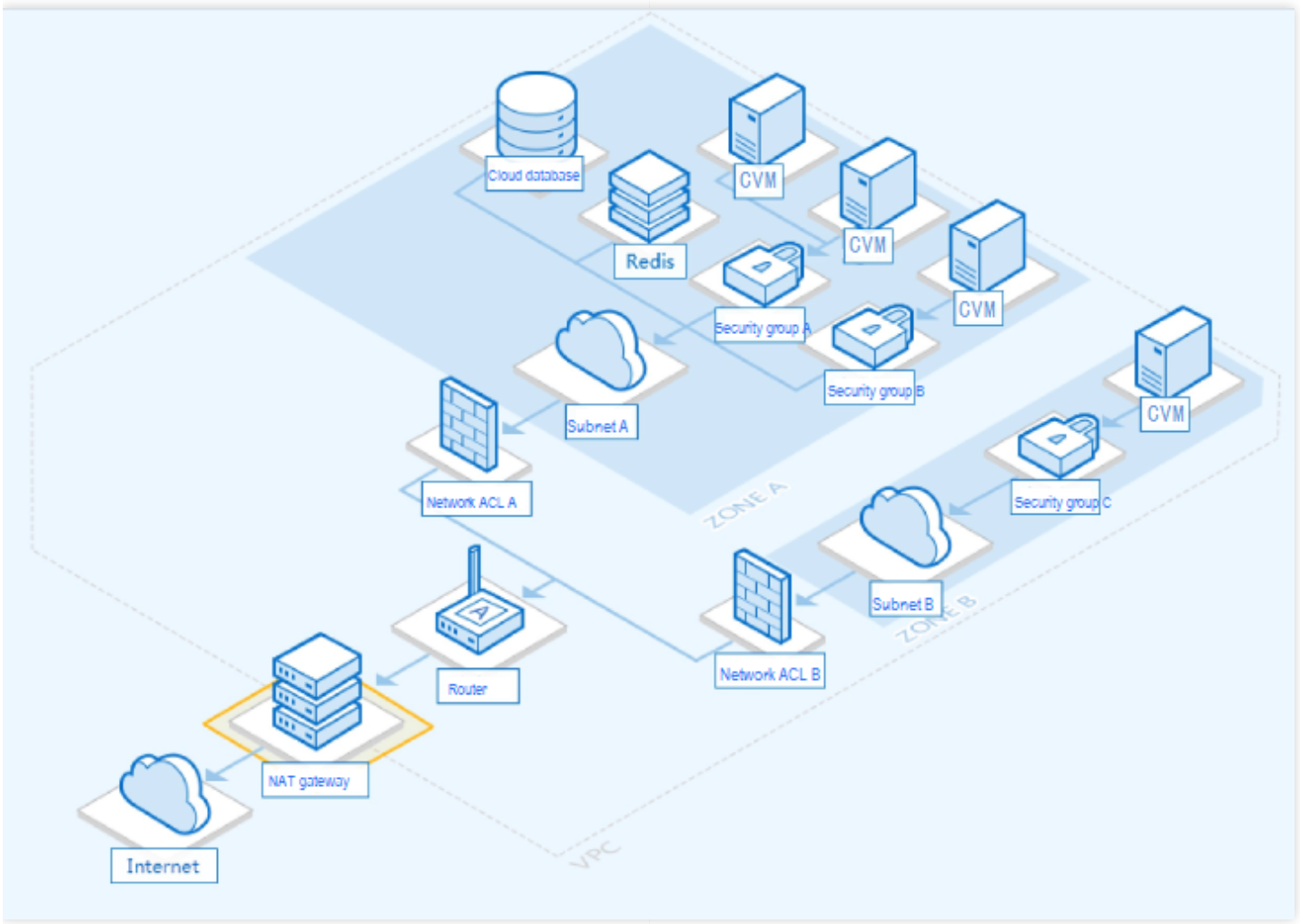
Introduction

NAT Gateway is a service that supports IP address translation and provides SNAT and DNAT capabilities, which can provide secure and high-performance internet access services for resources within a VPC. NAT Gateway supports up to 99.99% high availability, 5Gbps bandwidth, and more than 10 million concurrent connections. Its typical use cases are as follows:

- Large bandwidth, high availability public network egress services, such as web crawling and accessing public internet services.
- Secure public network egress services, for example: the CVM needs to communicate with the public network, but for security reasons, you do not want the CVM to be bound to a public IP address.

Network Topology

As shown in the figure below, when CVMs and other resources in a VPC send data packets outward through a NAT Gateway, the data first passes through the router and is routed according to the routing policy. Finally, the NAT Gateway uses the bound EIP address as the source IP address and sends the traffic to the internet.



Differences from Public Network Gateways

CVMs in a VPC can access the internet through a NAT Gateway or a public network gateway. The differences between the two gateways are shown in the following table.

Attribute	NAT Gateway	Public Gateway
Availability	Hot standby, automatic hot switch.	Manually switch the faulty gateway.
Public Network Bandwidth	Max. 5 Gbps.	Depends on the CVM network bandwidth.
Public network IP address	Up to 10 Elastic IPs can be bound.	1 EIP or common public IP.
Public Network Speed Limit	No	Depends on the CVM speed limit.

Attribute	NAT Gateway	Public Gateway
Maximum Connections	1 million.	500 thousand.
Private IP Address	Does not occupy the VPC user's private network IP.	Occupy IP in the subnet.
Security Group	NAT Gateway does not support security group binding, but security group binding can be performed on the backend CVM.	Supports security group binding.
Network ACL	NAT Gateway does not support network ACL binding, but you can bind network ACL to the subnet where the backend CVM is located.	Does not support binding network ACL, but you can bind network ACL to the subnet.

According to the chart above, NAT Gateway has the following strengths:

- Large capacity

Supports up to 10 million concurrent connections, 5 Gbps bandwidth, and 10 Elastic IPs to meet the demands of large-scale users.

- High Availability of the Hot Standby

Automatic switching of stand-alone failures realizes automatic disaster recovery compared to manual switching of public network gateways, ensuring 99.99% service availability.

- Cost Savings

Provides three configurations: high, medium, and low. Users can purchase on demand with elastic billing to save costs.

Product Features

NAT Gateway has multiple features including SNAT (Source Network Address Translation), DNAT (Destination Network Address Translation), traffic alarm, Bandwidth Package, automatic disaster recovery, etc.

SNAT

SNAT supports multiple CVMs under the same VPC to access the internet through the same public IP. The NAT Gateway can support a single-instance forwarding capacity of 5 Gbps.

DNAT

DNAT maps the private IP address, protocol, and port of CVMs within the VPC to the public IP address, protocol, and port, enabling services on CVMs to be accessed from the public network.

Traffic Alarms

You can set custom traffic alarms for VPN connections. When the metric value exceeds a certain threshold, an alarm is automatically triggered. The alarm message is sent via email and SMS to help you get an early warning of risks. Monitoring and alarm services are free of charge and can help you quickly locate problems when they occur.

Automatic Disaster Recovery

NAT Gateway supports hot standby and automatic disaster recovery. It can automatically switch when a stand-alone fails without any business awareness. The service availability is as high as 99.99%, ensuring the stable operation of your business.

Use Cases

Large Bandwidth and High Availability Public Network Access

NAT Gateway can meet the following user needs:

- Requires large bandwidth.
- Large Public IP usage.
- Deploys public network access with more services.

Secure public network access

NAT Gateway provides secure IP translation and can be used in the following scenarios:

- Hide the public IP addresses of hosts in the VPC to prevent exposure of their network deployment.
- It can communicate with the public network while hiding the IP.

Product Specifications

The NAT Gateway provides a variety of packages for you to choose from.

Configuration Type

The NAT Gateway supports binding 10 EIPs and provides three configuration types, which can meet the maximum burst traffic of 5 Gbps and 10 million concurrent connections:

- Small (up to 1 million connections)
- Medium (up to 3 million connections)
- Large (up to 10 million connections)

> Note:
>
> Due to standard protocol restrictions, for the same protocol, destination IP, destination port, the upper limit of the number of connections = number of bound EIPs x 55,000. To increase the number of connections, please add a new bound EIP or adjust the destination IP/port, destination IP/port.

Maximum Public Network Outbound Bandwidth

The optional values of the maximum public network bandwidth of the NAT Gateway (unit: Mbps) are 10, 20, 50, 100, 200, 500, 1,000, 2,000, and 5,000.

Maximum Public Network Inbound Bandwidth

- The default maximum public network inbound bandwidth of the NAT Gateway is 5 Gbps, and setting a limit is not currently supported.
- The NAT Gateway traffic fee is calculated based on the maximum outbound bandwidth of the public network. The inbound bandwidth value of the public network has nothing to do with the fee.

Use Limits

Note the following when you use a NAT Gateway:

- When a user deletes a NAT Gateway, its EIP is disassociated, but the EIP is not released from the user account.
- Users cannot associate a security group with a NAT Gateway but can bind a security group to instances in a private subnet to control traffic in and out of these instances.
- Users cannot use network ACLs directly to control traffic in and out of a NAT Gateway but can use network ACLs to control traffic in and out of the subnet associated with the NAT Gateway.
- Users cannot route traffic to a NAT Gateway through a VPC peering connection, VPN connection, or Direct Connect because the resources on the other end of such connections cannot use a NAT Gateway.
  For example, all traffic from VPC 1 to the internet can be sent through the NAT Gateway. VPC 1 and VPC 2 have established a peering connection. All resources in VPC 2 can access all resources in VPC 1, but all resources in VPC 2 cannot access the internet through the NAT Gateway.
- NAT Gateway supports TCP, UDP, and ICMP protocols, but ESP and AH used by GRE tunnel and IPSec cannot use NAT Gateway and ALG-related technologies are not supported yet. This is determined by the features of the NAT Gateway itself and has nothing to do with the service provider. However, most internet applications are TCP applications, and TCP and UDP applications together account for 99% of internet application types.
- The resource limits supported by the NAT Gateway are shown in the following table.

Resources	Limit	Can request for high quota
Number of NAT Gateways Supported by Each VPC	3	No
Number of Elastic IPs Supported by Each NAT Gateway	10	Yes
Maximum Forwarding Capacity Supported by Each NAT Gateway	5Gbps	No
Maximum Port Forwarding Entries Per NAT Gateway	200	Yes

Related Products

This document will introduce you to network products related to NAT Gateway.

Elastic IP

NAT Gateway and EIP are two ways for CVMs to access the internet. You can choose one or both for the architecture design of your public network access.

Solution 1: Use only a NAT Gateway

The CVM is not bound to an EIP. Traffic accessing the internet is forwarded to the NAT Gateway through the private network and is not subject to the public network bandwidth limit at the time of purchase. The network traffic generated by the NAT Gateway does not occupy the public network bandwidth outlet of the CVM.

Solution 2: Use only an EIP

The CVM is only bound to an EIP and does not use a NAT Gateway. All internet access traffic is transferred out through the EIP and is subject to the public network bandwidth limit at the time of purchase.

Solution 3: Use both a NAT Gateway and an EIP

The CVM is bound to an EIP, and the subnet route accessing the internet traffic points to the NAT Gateway.

- All traffic from CVMs actively accessing the internet is only forwarded to the NAT Gateway through the private network. The return packet also passes through the NAT Gateway and returns to the CVM. This part of the traffic is subject to the public network bandwidth limit at the time of purchase.
- When traffic from the internet actively accesses the EIP of the CVM, the CVM return packets are uniformly returned through the EIP, and the generated public network outbound traffic is subject to the public network bandwidth limit at the time of purchase.
  For more information about EIP, see document Elastic IP Overview.

Other Products

For related product information, see the following table:

Product	Relationship with NAT Gateway
Cloud Virtual Machine	NAT Gateway and EIP are two ways for CVMs to access the internet.

Product	Relationship with NAT Gateway
Elastic IP	EIP and NAT Gateway are two ways for CVMs to access the internet.
Virtual Private Cloud	NAT Gateway is a sub-product of VPC.
Route Tables	After you create a NAT Gateway, you need to configure routing rules to direct subnet traffic to the NAT Gateway.
Public Gateway	The public network gateway is a CVM with a forwarding feature enabled, which supports NAT connect.
Network ACL	After the subnet where the NAT Gateway backend CVM is located is bound to the network ACL, the traffic in and out of the subnet can be precisely controlled.

Purchase Guide
Billing Overview

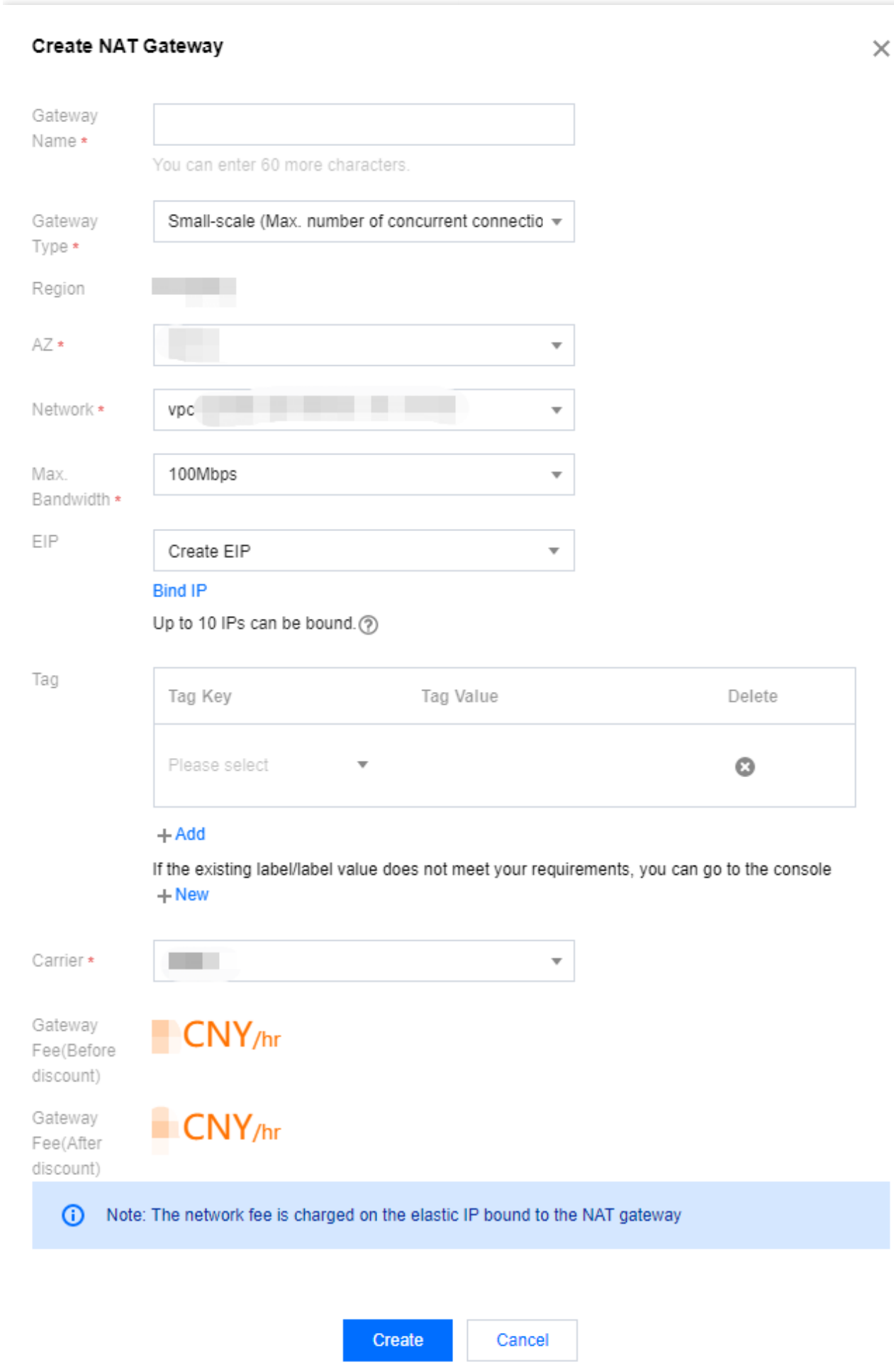
This document introduces the fee structure of the NAT Gateway.

Billing Description

The NAT Gateway service fee consists of two parts: gateway fee (billed by hour) and network fee (billed by traffic). The gateway fee is billed on the NAT Gateway, and the network fee is billed on the EIP bound to the NAT Gateway.

Gateway Inquiry

You can select different bandwidth specifications on the NAT Gateway purchase page to learn about the corresponding gateway fees.

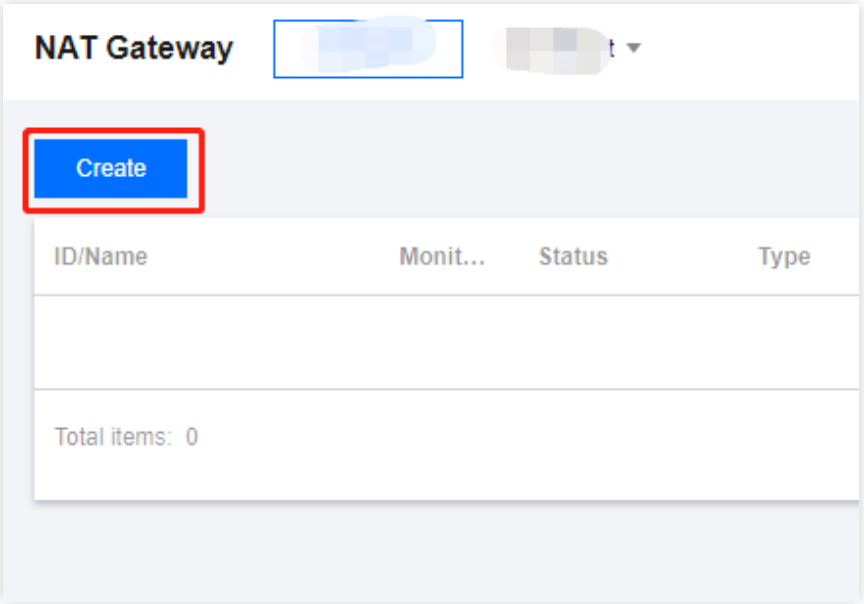

Create NAT Gateway
Gateway Name *
You can enter 60 more characters.
Gateway Type *
Small-scale (Max. number of concurrent connectio
Region
AZ *
Network *
vpc
Max. Bandwidth *
100Mbps
EIP
Create EIP
Bind IP
Up to 10 IPs can be bound.
Tag
Tag Key
Tag Value
Delete
Please select
Add
If the existing label/label value does not meet your requirements, you can go to the console
New
Carrier *
Gateway Fee(Before discount)
CNY/hr
Gateway Fee(After discount)
CNY/hr
Note: The network fee is charged on the elastic IP bound to the NAT gateway
Create
Cancel

Purchase Method

The following are the specific steps for purchasing a NAT Gateway.

1. Log in to the cloud console, select Cloud Services > VPC to enter the VPC console, and click NAT Gateway on the left.

2. Click Create in the upper left corner.



In the pop-up, enter or confirm the following parameters in sequence:

- Gateway name.
- Gateway type.
- AZ.
- Network: Select the VPC for the NAT Gateway service.
- Max. Bandwidth: Select according to your needs.
- EIP: Bind an EIP to the NAT Gateway. You can select an existing EIP or purchase and bind a new one.
- Carrier: Choose the carrier.

Create NAT Gateway

Gateway Name *

You can enter 60 more characters.

Gateway Type * Small-scale (Max. number of concurrent connectio

Region

AZ *

Network * vpc

Max. Bandwidth * 100Mbps

EIP Create EIP

Bind IP

Up to 10 IPs can be bound.

Tag

Tag Key	Tag Value	Delete
Please select		

+ Add

If the existing label/label value does not meet your requirements, you can go to the console

+ New

Carrier *

Gateway Fee(Before discount) CNY/hr

Gateway Fee(After discount) CNY/hr

Note: The network fee is charged on the elastic IP bound to the NAT gateway

Create Cancel

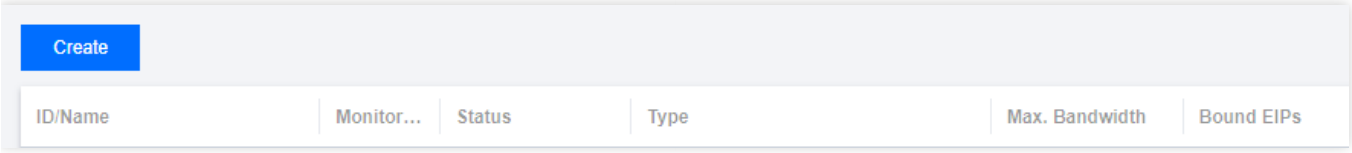
3. After selection, click Create to complete the purchase of the NAT Gateway.

Quick Start

You only need to complete the following two steps to access the internet through a NAT Gateway.

Step 1: Create a NAT Gateway

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway on the left.
2. Click Create in the upper left corner.



3. In the pop-up New dialog box, gateway parameters involved are:
Parameter description:

- Gateway Name: Customize the gateway name.
- Gateway Type: The gateway type supports small, medium, and large. Please set it according to the actual situation.
- AZ: Select the availability zone to which the NAT Gateway belongs.
- Network: Select the VPC to which the NAT gateway belongs.
- Max. Bandwidth: Select according to your needs.
- EIP: Bind an EIP to the NAT Gateway. You can select an existing EIP or purchase and bind a new one.
- Carrier: Select an ISP based on your actual situation.

Create NAT Gateway

Gateway Name *

You can enter 60 more characters

Gateway Type * Small (up to 1,000,000 connections)

Region

AZ *

Network *

Bandwidth * 100Mbps

EIP Create EIP

Bind EIP

Up to 10 IPs can be bound

Carrier *

The maximum number of EIPs that can be created under this carrier is 100, and 100 can still be created.

Tag

Tag Key	Tag Value	Delete
Please select		

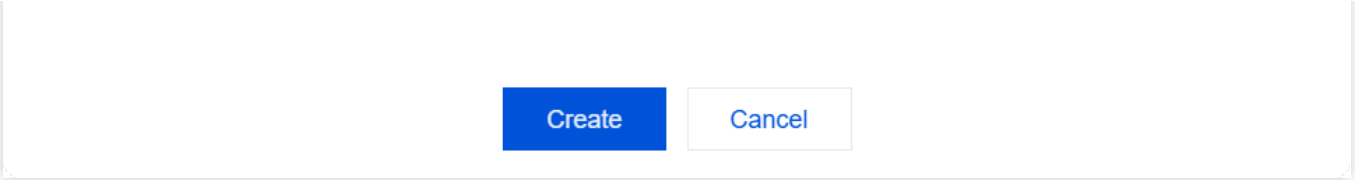
+ Add

If the existing tag or tag value does not meet your requirements, you can create a tag on the console.

Gateway Fee(Before discount)

Gateway Fee(After discount)

Note: The network fee is charged on the elastic IP bound to the NAT gateway.

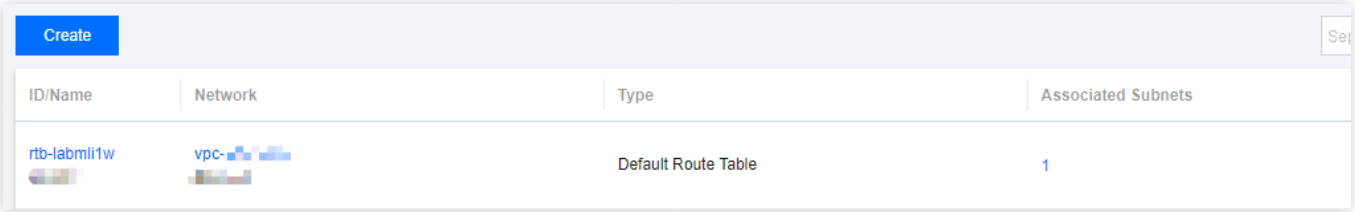


4. After the parameter settings are completed, click Create to create the NAT Gateway.

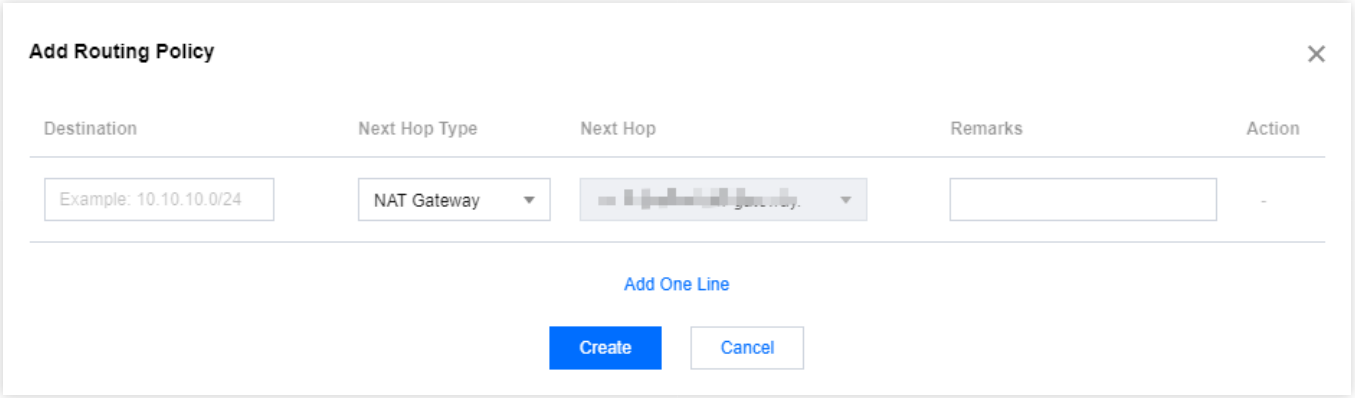
Step 2: Configure the route table associated with the subnet

After you create a NAT Gateway, you need to configure routing rules to direct subnet traffic to the NAT Gateway.

1. In the sidebar on the left side of the VPC console, click Route Table.
2. In the route table list, click the route table ID associated with the subnet that needs to access the internet to enter the route table details page, then click Add Routing Policy in the routing policy.



3.Enter the destination (the public IP address segment to be accessed) in the pop-up box, select NAT Gateway for the next hop type, and select the created NAT Gateway ID for the next hop.

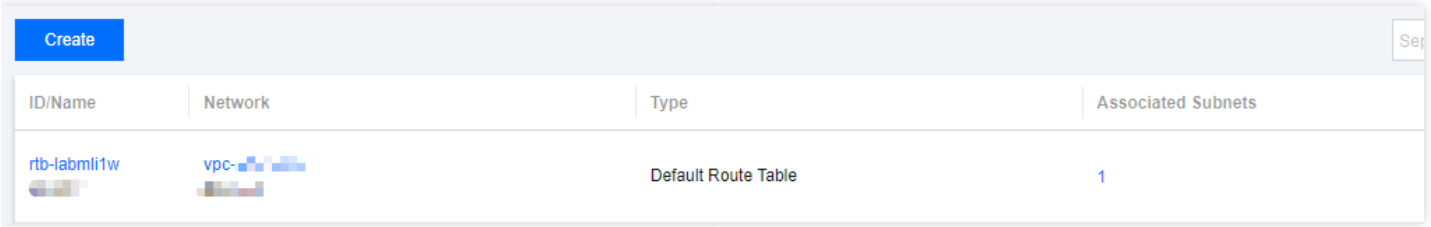


4.Click Create, and after the above configuration is completed, the traffic from the CVM in the subnet associated with this route table will be directed to the NAT Gateway when the CVM accesses the internet.

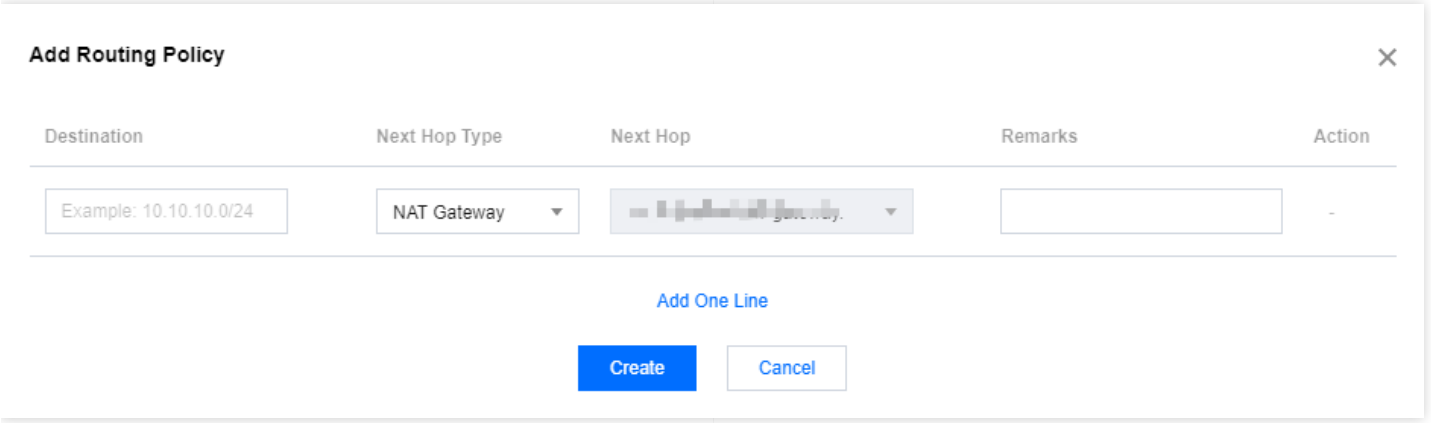
Operation Guide
Configuring a Route Pointing to the NAT Gateway

After you create a NAT Gateway, you need to configure routing rules to direct subnet traffic to the NAT Gateway.

1. In the sidebar on the left side of the VPC console, click Route Table.
2. In the route table list, click the route table ID associated with the subnet that needs to access the internet to enter the route table details page, then click Add Routing Policy in the routing policy.



3. Enter the destination in the pop-up box, select NAT Gateway for the next hop type, and select the created NAT Gateway ID for the next hop.



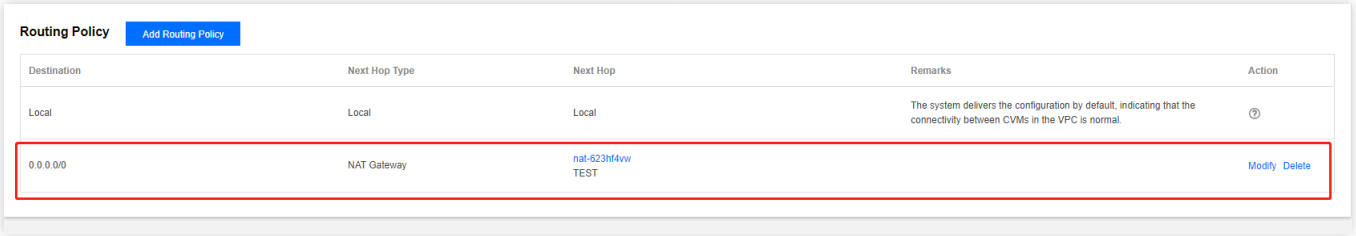
4. Click Create, and after the above configuration is completed, the traffic from the CVM in the subnet associated with this route table will be directed to the NAT Gateway when the CVM accesses the internet.

Adjusting the Priority of NAT Gateway and EIP

When a subnet is associated with a NAT gateway, and the CVM in the subnet has a public network 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 network IP. However, you can set a routing policy to allow the CVM to access the Internet through its public network IP.

Directions

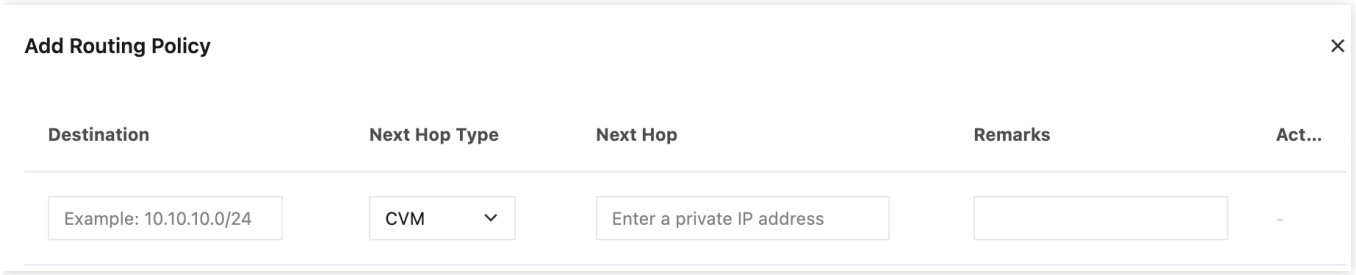
1. View the routing table associated with the subnet where the CVM is located. Ensure that a routing policy that points to the NAT gateway exists so that CVMs in the subnet that have no public network IP can still access the Internet through the NAT gateway.



2. Add a new routing policy with the Next Hop Type as Public Network IP of Cloud Virtual Machine and enter the Destination.
   - Destination: Enter the specific public network IP range or default route (0.0.0.0/0, default route indication: if the destination is not in the routing table, default route for all data packets) to be accessed by the service.
   - Next Hop Type: CVM.

     Note:

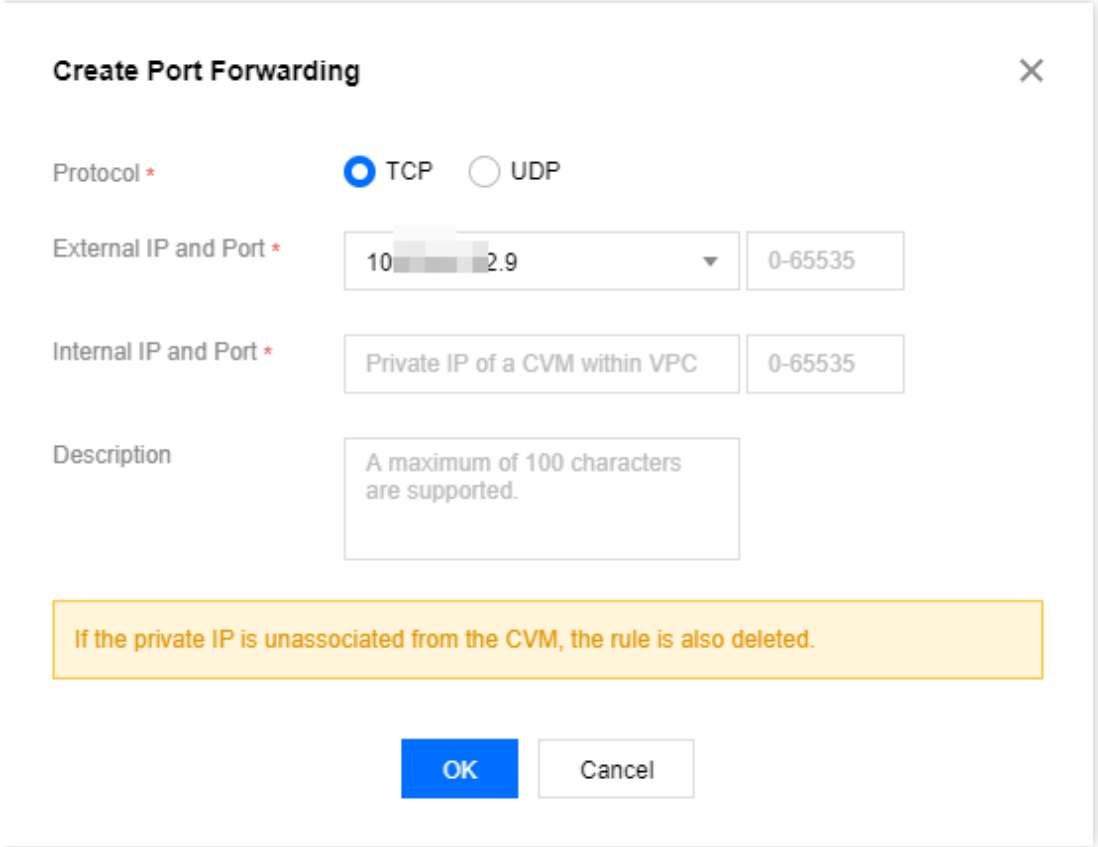
     - This routing policy, when configured with routing rules that have the same destination as the original ones pointing to the NAT Gateway, CVM, and public network gateway, always matches this route preferentially.
     - This routing policy will affect all subnets associated with this route table (please confirm the impact of this operation). Specifically, cloud servers within these subnets that have public IP addresses (or elastic IPs) will access the Internet via their public IPs instead of through the NAT Gateway.
     - Cloud servers within the subnets associated with this route table that do not have public IP addresses can still access the Internet via the NAT Gateway and will not be affected.


Add Routing Policy
Destination
Next Hop Type
Next Hop
Remarks
Act...
Example: 10.10.10.0/24
CVM
Enter a private IP address
-

Managing Port Forwarding Rules
Creating Port Forwarding Rules

The port forwarding table is a configuration table on the NAT Gateway. It is used to configure the DNAT feature on the NAT Gateway, which maps the private IP address, protocol, and port of CVMs within the VPC to the public IP address, protocol, and port, enabling resources on CVMs to be accessed from the public network.
The following will introduce you in detail how to create port forwarding rules.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the sidebar on the left.
2. In the list, click the NAT Gateway ID that needs to be modified to enter the details page, and click Port Forwarding in the tab.
3. Click Create, select the protocol, external IP port, and internal IP port, and click OK.



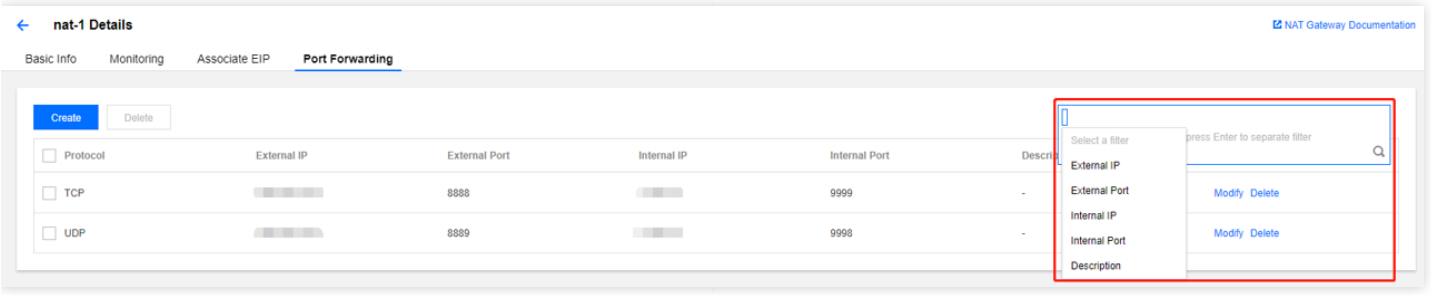
Querying Port Forwarding Rules

The following will introduce you in detail how to query port forwarding rules.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the left sidebar.

2. In the list, click the NAT Gateway ID you want to query to enter the details page and select Port Forwarding.

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

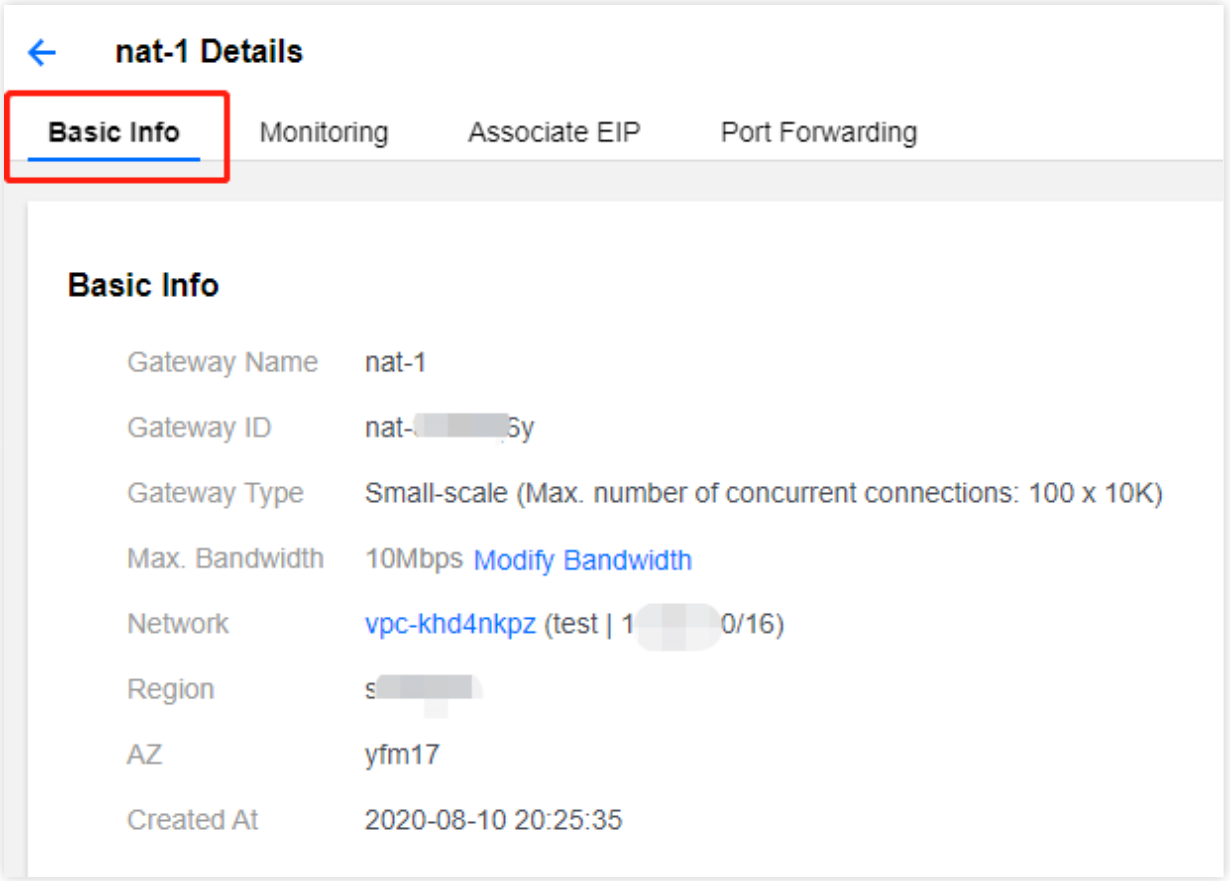


Modifying NAT Gateway Configuration

After you create a NAT Gateway, you can modify its attributes.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the sidebar on the left.
2. In the list, click the NAT Gateway ID that needs to be modified to enter the details page. On the Basic Information page of the details page, you can complete the following operations.

- Modify the custom name of the gateway.
- Change the NAT Gateway type.
- Modify maximum bandwidth.



Managing NATGW EIPs

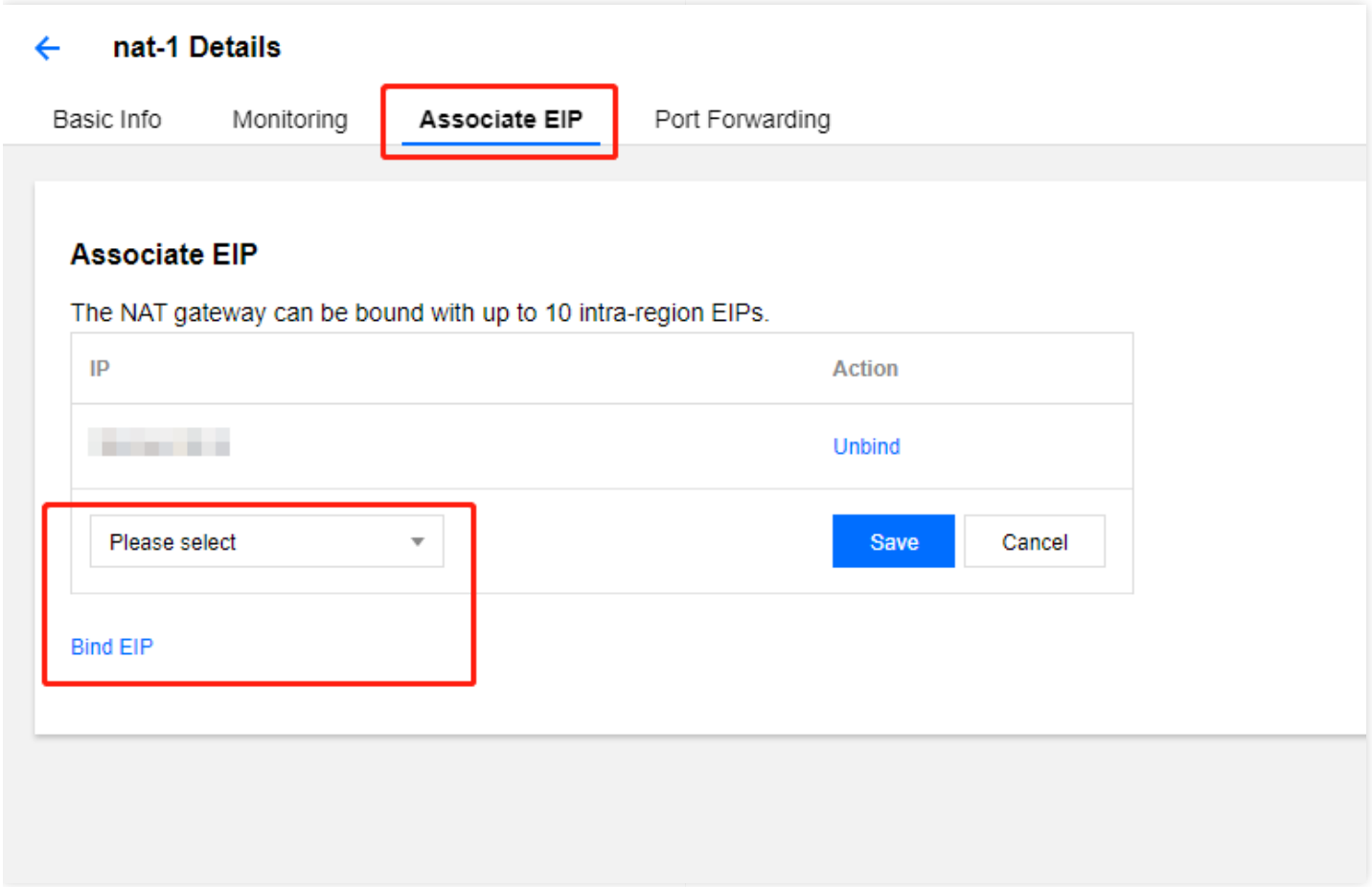
After creating a NATGW, you can manage the EIPs of the NATGW. The following section describes the management method in detail.

1. Log in to the VPC console.
2. In the left directory, click NATGW to go to the NATGW List page.
3. Click a gateway ID in the list to go to the details page.
4. Select the EIP Association tab, on which you can choose to bind or unbind an EIP.

Bind an EIP

> Note:
>
> When a NATGW is bound to multiple EIPs, the system automatically performs load balancing.

Click Bind EIP, select the EIP to be bound in the dropdown list, and click Save.

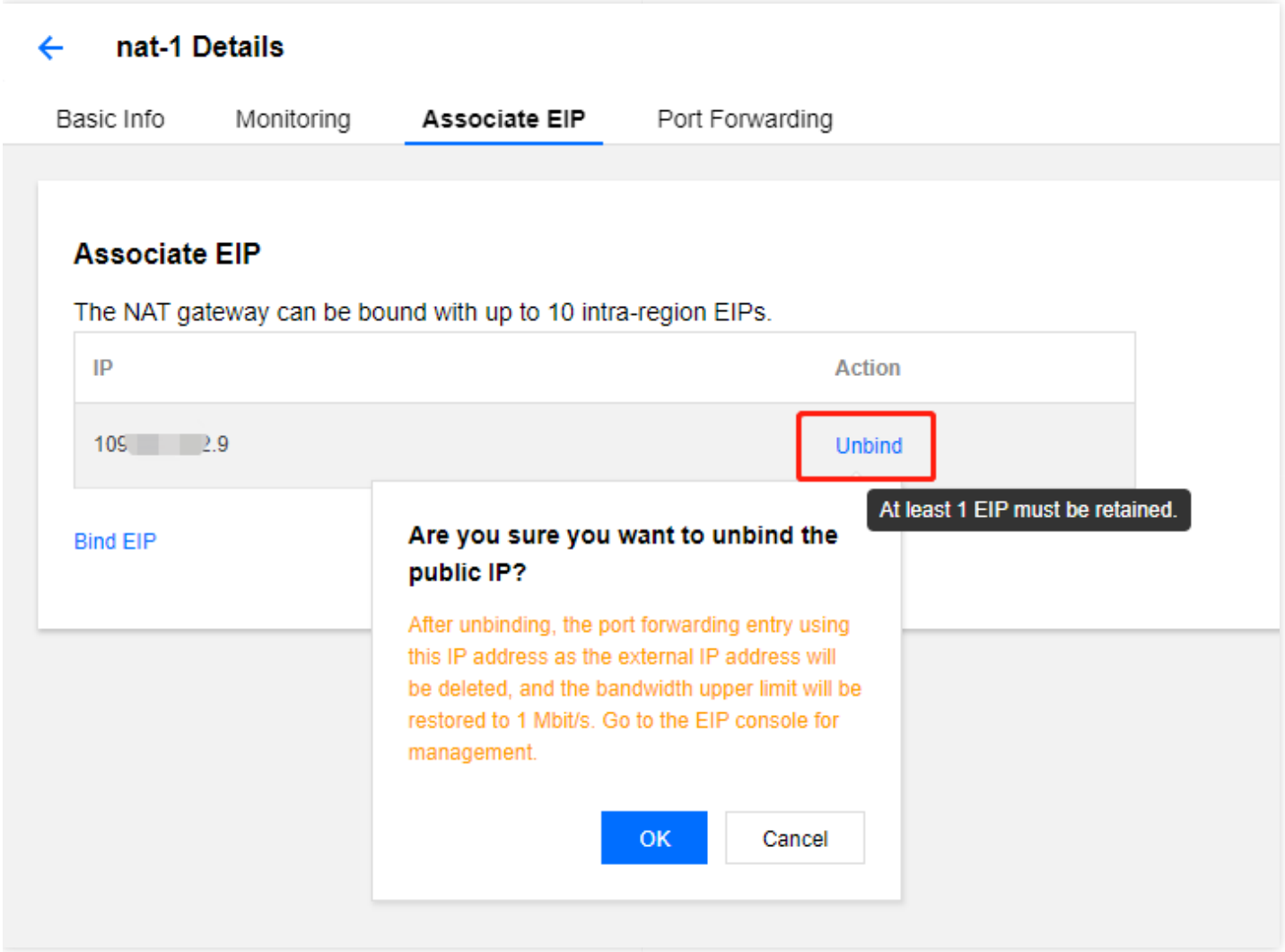


Unbinding an EIP

> Note:

> A NATGW should be bound to at least one EIP.

In the Operation column of the EIP that needs to be unbound, click Unbind.



Setting Active/Standby EIPs

> Note:
>
> 1. When a NATGW is bound to only one EIP, it does not support setting a standby IP. When a NATGW is bound to two or more EIPs, it supports setting a standby IP.
>
> 2. Multiple active EIPs and only one standby EIP can be set.

1. In the Operation column of the line where the corresponding EIP is located, click Set to Standby IP.
2. Click OK in the pop-up box to complete the standby IP settings.
3. When you no longer need a standby IP, you can restore the EIP to the active IP. In the Operation column of the EIP, click Restore to Active IP.

4. Click OK in the pop-up box to complete the active IP restoration.

Actual Forwarding Logic of Active/Standby EIPs

EIPs have corresponding health detections. When the health of the active EIP is detected to be abnormal:

- If there are EIPs in standby status and the number of available EIPs is greater than or equal to 1, data plane forwarding will be stopped for the abnormal EIP. An "(Abnormal)" suffix will be added to the abnormal EIP, while the processing logic and suffix of the original EIP in the "Standby" status remain unchanged.
- If there are EIPs in standby status and the number of available EIPs is zero, data plane forwarding will be stopped for the abnormal EIP. An "(Abnormal)" suffix will be added to the abnormal EIP, while the data plane of the original EIP in the "Standby" status will start forwarding, and its suffix will change to "(Standby, in use)".

  When the active EIP is recovered:
- The data plane of the active EIP resumes forwarding first, then the standby EIP stops data plane forwarding, and the suffix is restored to its original status.

Managing SNAT Rules

When a NATGW is bound to multiple EIPs, you can create SNAT rules to specify the EIPs for public network access for CVMs in different business groups.
For example, when a NATGW is bound to multiple EIPs such as EIP1, EIP2, EIP3, and EIP4, the system automatically performs load balancing to access the public network among all bound EIPs. If EIP1, EIP2, and EIP3 are added to the SNAT address pool, the system uses the EIPs in the SNAT address pool to access the public network and automatically performs load balancing on the EIPs in the SNAT address pool. CVMs without SNAT rules configured can access the public network through all EIPs bound to NAT.

> Note:
>
> When the load on the CVM instance surges, one EIP may not be able to support the huge amount of traffic. In this case, multiple EIPs can be configured to share the traffic.
>
> NATGW supports using the same EIP to configure both SNAT rules and port forwarding rules. For detailed information about port forwarding rules, see Managing Port Forwarding Rules.

This document describes how to create and manage SNAT rules.

SNAT Rule Limits

- When a NATGW disassociates an EIP, if the EIP is the only EIP in the SNAT rule, the SNAT rule is deleted at the same time; if the EIP is not the only EIP in the SNAT rule, the EIP is deleted from the SNAT rule.
- If the subnet used in the SNAT rule does not exist, the SNAT rule is deleted at the same time.
- If the CVM used in the SNAT rule does not exist, the CVM is deleted from the SNAT rule at the same time. If the CVM is the last CVM in the SNAT rule, the SNAT rule is deleted at the same time.
- Due to standard protocol limits, for the same protocol/destination IP address/destination port, the upper limit of the number of connections = number of bound EIPs x 55,000. To increase the number of connections, add a new bound EIP or adjust the destination IP address/port.
- The description of the rule limit switch for cloud resources accessing the public network through the NATGW is as follows:
    - Disabled by default: When no SNAT rules are configured, all cloud resources pointing to the NATGW can access the public network through all EIPs on the NATGW. When SNAT rules are configured, specified cloud resources can access the public network through specified EIPs, while other cloud resources without SNAT rules configured can access the public network through all EIPs on the NATGW.
    - After enabling: Only cloud resources configured with SNAT rules are allowed to access the public network through the NATGW; other cloud resources are not allowed to access the public network through the NATGW.

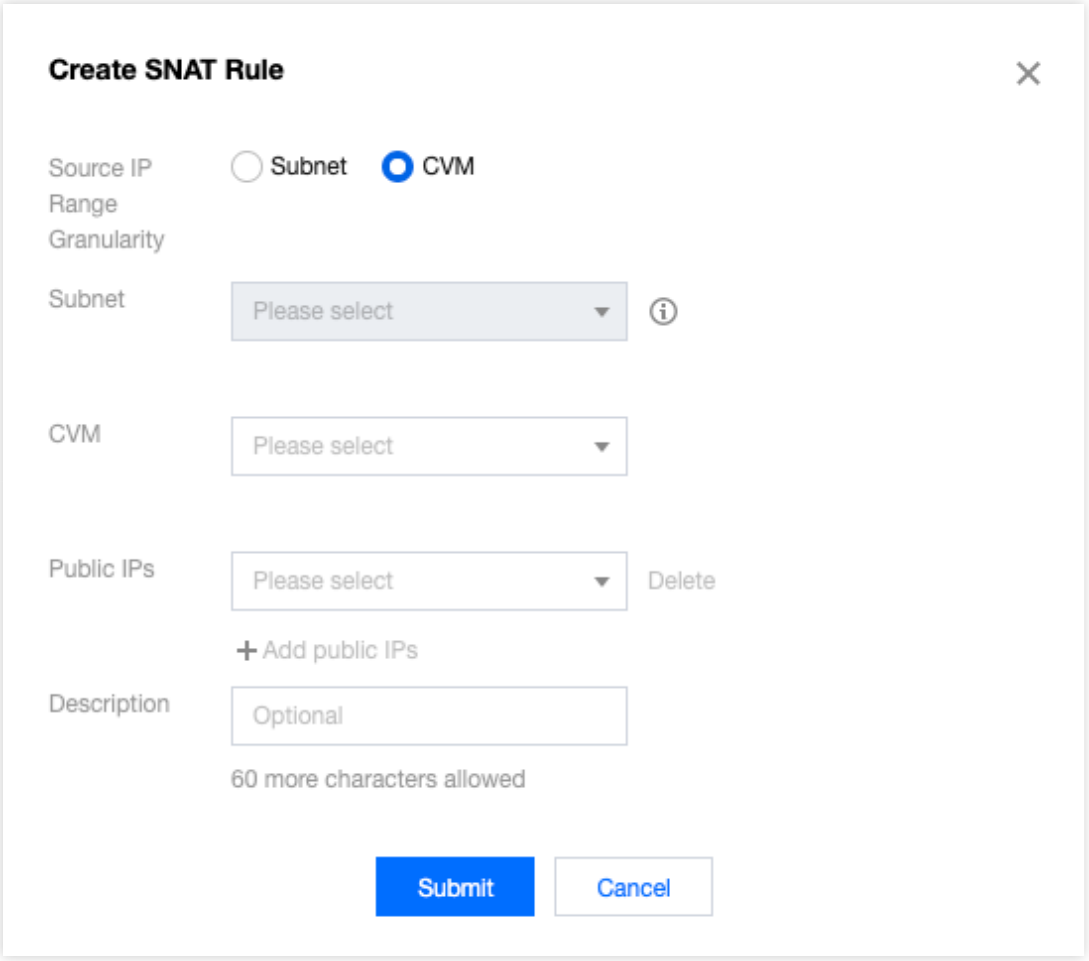
- When an EIP is in the standby status, it does not support binding to SNAT rules. Only the active EIP supports binding.
- EIPs that are bound to SNAT rules cannot be set to standby EIPs.

Prerequisites

Before creating an SNAT rule, ensure that the route table of the subnet points to the corresponding NATGW. For detailed operations, see Configuring a Route Pointing to the NATGW.

Creating an SNAT Rule

1. Log in to the VPC console.
2. In the left directory, click NATGW to go to the NATGW List page.
3. Click a gateway ID in the list to go to the details page.
4. Select the SNAT Rule tab to go to the SNAT Rule Management page.
5. Click Create, and the SNAT Rule Creation dialog box pops up.
6. Set the SNAT rule.
    - Source IP Range Granularity: Supports subnet and CVM granularity.
        - Subnet: When a subnet is selected, the route table associated with the subnet should point to the NATGW, and all CVMs in the subnet access the public network according to the SNAT rules.
        - CVM: When a CVM is selected, the route table associated with the subnet where the CVM is located should point to the NATGW. Only the selected CVM can access the public network according to the SNAT rules. CVMs without SNAT rules configured can access the public network through all EIPs bound to NAT.
    - Subnet: Select a subnet or the subnet to which the CVM belongs.
    - CVM: A CVM should be specified only when the source IP range granularity is CVM. Multiple CVMs can be added.
    - Public IP Address: Specify the EIP for public network access.
    - Description: Custom description information, supporting up to 60 characters.



7. After the SNAT rule parameter settings are completed, click Submit.

Editing an SNAT Rule

> Note:
>
> Modifying public IP addresses in the existing SNAT rules may cause the original business connection to be interrupted, which can be restored after reconnection. Proceed with caution.

1. On the SNAT Rule tab, click Edit on the right of the SNAT rule entry, and an editing dialog box pops up.
2. Modify the public IP address or description in the SNAT rule, and click Submit to complete the modification.
3. Click the edit icon next to the description in the SNAT rule to modify it directly.

Querying SNAT Rules

1. In the search box in the upper right corner of the SNAT Rule tab, click to select the following filter

conditions and enter the corresponding parameter values in the input box.
2. Click the search icon for a quick search.
3. Click a subnet/CVM ID to redirect to the corresponding resource details page.

Deleting an SNAT Rule

If you do not need to specify an EIP for the CVM to access the public network, you can delete the SNAT rule.

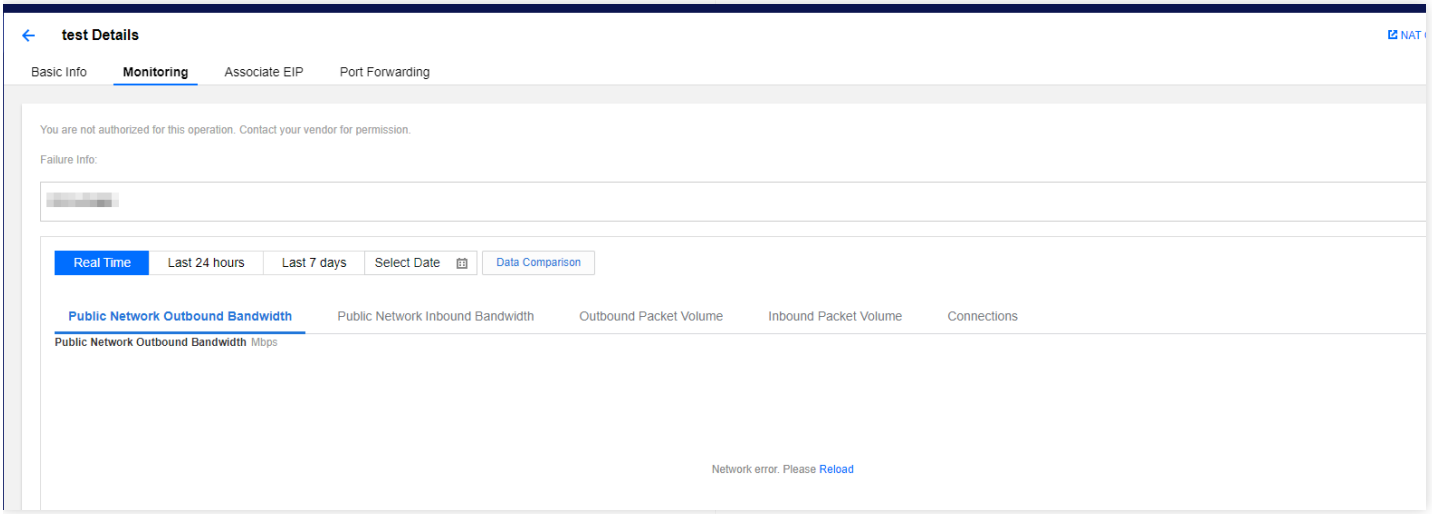
- Single-rule deletion
  - On the SNAT Rule tab, click Delete on the right of the SNAT rule entry.
  - Click OK to delete the SNAT rule.

- Batch deletion
  - On the SNAT Rule tab, select multiple SNAT rules and click Delete above.
  - In the pop-up dialog box, click Delete to complete the batch deletion.

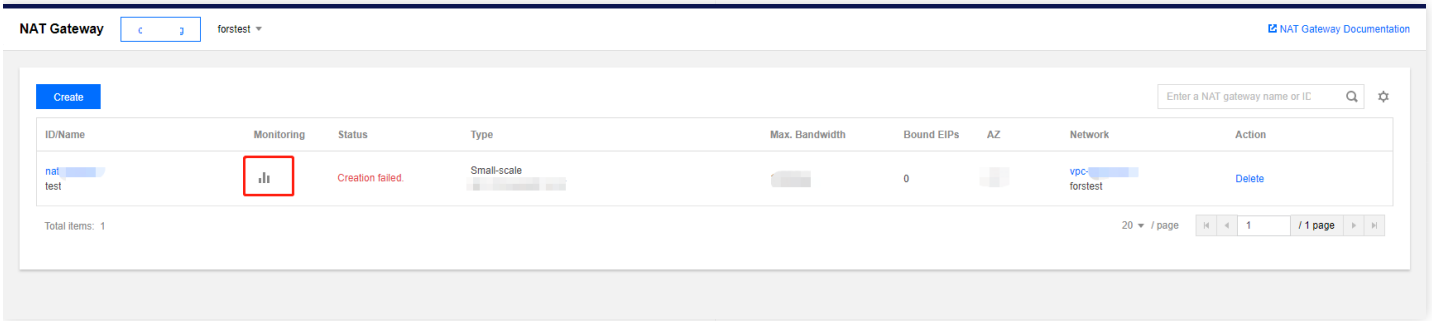
Viewing Monitoring Information

After you create a NAT Gateway, you can view monitoring information and export data through the console.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the sidebar on the left.
2. In the NAT Gateway list, click the gateway ID you want to view to enter the details page and click the Monitoring tab to view the monitoring information.



3. You can also click the monitor icon in the NAT Gateway entry you want to view in the NAT Gateway list to view the monitoring information.



Setting Alarms

You can set alarms for NAT gateways to monitor the status of NAT gateways.

1. Log in to the Cloud Monitor console.

2. In the directory on the left, select Alarm Configuration > Alarm Policy to enter the alarm policy configuration page, and click Create.

3. Enter the name of the alarm policy, select NAT Gateway as the policy type, select the alarm object, set the alarm policy, select the alarm receiving group and alarm channel, and click Complete. You can view the set alarm policy in the alarm policy list.

   > Note:
   >
   > After an alarm policy is created, you need to unbind all resources before you can delete it.

4. Viewing an Alarm Message
   When an alarm condition is triggered, you will receive an alarm through the selected alarm channel (SMS/email/message center), or you can click Alarm History in the left directory to view it.

Deleting a NAT Gateway

> Note:
>
> When you delete it, the route table containing this NAT Gateway and related routing policies will be deleted together, and internet forwarding requests will be interrupted immediately. Please be prepared for network interruption.

You can delete a NAT Gateway at any time if you decide that you do not need it.

1. Log in to the cloud console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console, and click NAT Gateway in the sidebar on the left.
2. Find the NAT Gateway you want to delete in the list, click Delete in the Action column, and click OK in the pop-up.

FAQs
Concepts

1. What Is NATGW?

When the private and public networks are isolated, NATGW translates the private IP addresses and public IP addresses in the VPC to enable the private network to access the Internet. NATGW supports a maximum burst traffic of 5 Gbps and 10 million concurrent connections. At the same time, as a high-availability gateway, NATGW achieves dual-host hot standby and automatic switch when a single machine fails without business perception. NATGW is a gateway that translates private IP addresses and public IP addresses in the VPC. It is a way for cloud resources without public IP addresses in VPCs to access the Internet (but it does not support active Internet access to VPCs).

2. What Is the Difference Between NATGW and Public Network Gateway?

NATGW and public network gateway are both used for CVMs in VPCs to access the Internet, but there are some differences between them.

3. What Are the Configuration Types of NATGW?

NATGW supports binding 10 EIPs and provides three configuration types: small (maximum 1 million connections), medium (maximum 3 million connections), and large (maximum 10 million connections).

4. What Are the Key Features of NATGW?

The main features of NATGW include SNAT, DNAT, high performance, high availability, monitoring details display, and gateway refined flow control.

5. What Are the Constraints of Using NATGW?

NATGW has its usage constraints. For example, deleting a NATGW will disassociate its EIP, but will not release the EIP from the user account.

6. What Is the Network Topology of NATGW?

When resources such as CVMs in the VPC send data packets through NATGW, the data first passes through the router and is routed according to the routing policy.

7. What Is the Main Feature of NATGW?

It supports SNAT and DNAT.

8. What Is an EIP?

An EIP address is a static IP address designed specifically for dynamic cloud computing. It is a fixed public IP address in a certain region. With EIPs, users can quickly map an address to another NATGW in their

account to isolate instance failures.

9. What Is a Region?

Regions in the cloud platform are completely isolated from each other, ensuring maximum stability and fault tolerance between different regions. We will gradually increase the supply of regions to cover more nodes. It is recommended that users select the region closest to their customers to reduce access latency and improve download speed.

10. How to Select a Region Suitable for Users?

The region selection follows the following principles:

- Principle of proximity to users
- Select the CVM region based on users' geographical location. The closer the CVM is to the accessing clients, the lower the access latency and the higher the access speed will be.
- Principle of intra-region private network communication
  The private network is interconnected within the same region and is isolated across different regions. Users requiring private network communication between multiple CVMs should select the same CVM region. CVMs within the same region can communicate through the private network. CVMs across different regions should communicate through the public network instead of the private network.

11. What Is the Degree of Isolation Between AZs?

Each AZ operates on its own independent, physically distinct infrastructure and is designed to be highly reliable. Common points of failure, like generators and cooling equipment, are not shared between AZs. Additionally, they are physically independent of each other, so even extremely rare disasters such as fires, tornadoes, or floods would only affect a single AZ.

12. How Many NATGWs Can Be Created?

Different resources have different creation quantity limits.

Function Category

How to Use a NAT Gateway and an EIP?

- A NAT Gateway is a gateway that translates private IP addresses and public IP addresses in a VPC. It is an entry and exit for public network traffic in a VPC.
- NAT Gateway and EIP are two ways for CVMs to access the internet. You can choose one or both of them for the user's architecture design of public network access.

Where Can I Find More Information About Security?

The cloud platform provides various network and security services such as security groups, encrypted log-in, and EIP to ensure that your instances can provide services internally and externally safely, efficiently, and freely. For more information about CVM security, see Network and Security Overview.

How Do I Prevent Others From Viewing My System?

Users have full control over the visibility of your system, and CVMs allow users to place running instances into any security group of the user's choice. Using the security group console interface, users can specify inter-group communications and which IP subnets on the network can communicate with CVMs.

How to Troubleshoot Security Issues?

If you suspect a security hazard or adverse event, see Cloud Workload Protection to resolve the security issue.

The route table configures a subnet to access the public network through a NAT Gateway, but the CVMs in the subnet are configured with EIPs. Do these CVMs access the public network through the NAT Gateway or the EIP?

When there are multiple routing policies in a route table, the following routing priority applies from high to low:

- Traffic within a VPC.
- Most precise routing.
- Public IP address.