

NAT Gateway

User Guide

Issue 01
Date 2022-04-12



Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

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

Trademarks and Permissions



HUAWEI 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 Overview.....	1
1.1 What Is NAT Gateway?.....	1
1.2 Product Advantages.....	3
1.3 Application Scenarios.....	4
1.4 NAT Gateway Types.....	7
1.5 Notes and Constraints.....	8
1.6 NAT Gateway and Other Services.....	9
1.7 Permissions Management.....	9
1.8 Region and AZ.....	12
1.9 Basic Concepts.....	13
2 Getting Started.....	14
2.1 Using SNAT to Access the Internet.....	14
2.1.1 Overview	14
2.1.2 Step 1: Assign an EIP.....	15
2.1.3 Step 2: Create a NAT Gateway.....	15
2.1.4 Step 3: Add an SNAT Rule.....	16
2.1.5 Step 4: Verify the Result.....	18
2.2 Using DNAT to Provide Services Accessible from the Internet.....	18
2.2.1 Overview	18
2.2.2 Step 1: Assign an EIP.....	19
2.2.3 Step 2: Create a NAT Gateway.....	19
2.2.4 Step 3: Add a DNAT Rule.....	21
2.2.5 Step 4: Verify the Result.....	22
2.3 Using SNAT and DNAT Rules to Allow On-premises Servers to Communicate Over the Internet.....	23
2.3.1 Overview	23
2.3.2 Step 1: Create a Direct Connect Connection.....	23
2.3.3 Step 2: Assign an EIP.....	24
2.3.4 Step 3: Create a NAT Gateway.....	24
2.3.5 Step 4: Add an SNAT Rule.....	25
2.3.6 Step 5: Add a DNAT Rule.....	27
3 Managing NAT Gateways.....	29
3.1 Creating a NAT Gateway.....	29

3.2 Viewing a NAT Gateway.....	30
3.3 Modifying a NAT Gateway.....	31
3.4 Deleting a NAT Gateway.....	31
4 Managing SNAT Rules.....	32
4.1 Adding an SNAT Rule.....	32
4.2 Viewing an SNAT Rule.....	34
4.3 Modifying an SNAT Rule.....	35
4.4 Deleting an SNAT Rule.....	35
5 Managing DNAT Rules.....	36
5.1 Adding a DNAT Rule.....	36
5.2 Viewing a DNAT Rule.....	38
5.3 Modifying a DNAT Rule.....	38
5.4 Deleting a DNAT Rule.....	39
5.5 Deleting DNAT Rules in Batches.....	39
5.6 Importing and Exporting DNAT Rules Using Templates.....	40
6 Permissions Management.....	42
6.1 Creating a User and Granting NAT Gateway Permissions.....	42
6.2 NAT Gateway Custom Policies.....	43
7 Monitoring Management.....	46
7.1 Supported Metrics.....	46
7.2 Creating Alarm Rules.....	49
7.3 Viewing Metrics.....	51
8 FAQs.....	53
8.1 NAT Gateway.....	53
8.1.1 What Is the Relationship Between a VPC, NAT Gateway, EIP Bandwidth, and ECS?.....	53
8.1.2 How Does A NAT Gateway Offer High Availability?.....	53
8.1.3 Which Ports Cannot Be Accessed?.....	53
8.1.4 What Should I Do If I Fail to Access the Internet Through the NAT Gateway?.....	54
8.1.5 Can I Change the VPC for a NAT Gateway After It Is Created?.....	54
8.2 SNAT.....	54
8.2.1 Why Is SNAT Used?.....	54
8.2.2 What Are SNAT Connections?.....	54
8.2.3 What Is the Bandwidth of the NAT Gateway When a Server Accesses the Internet Through the NAT Gateway? Where Can I Configure the Bandwidth?.....	55
8.2.4 How Do I Resolve Packet Loss or Connection Failure Issues When Using a NAT Gateway?.....	55
8.2.5 What Are the Relationships and Differences Between the CIDR Blocks in a NAT Gateway and in an SNAT Rule?.....	55
8.3 DNAT.....	55
8.3.1 Why Is DNAT Used?.....	55
8.3.2 Can I Modify DNAT Rules?.....	55
8.3.3 What Should I Do If NAT Gateway Rules Become Invalid After ECS Specifications Are Changed?.....	56

A Change History..... 57

1 Overview

1.1 What Is NAT Gateway?

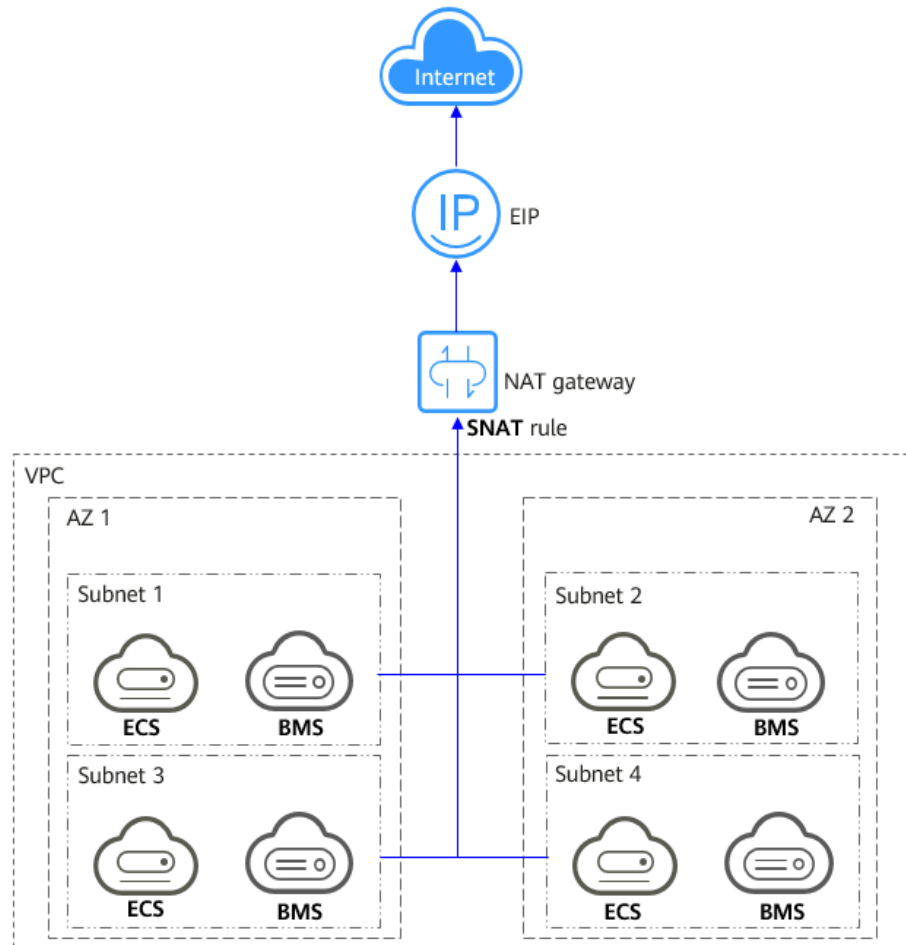
The NAT Gateway service provides network address translation (NAT) with 20 Gbit/s of bandwidth for Elastic Cloud Servers (ECSs) and Bare Metal Servers (BMSs) in a Virtual Private Cloud (VPC), or servers that connect to a VPC through Direct Connect or Virtual Private Network (VPN) in on-premises data centers, allowing these servers to share elastic IP addresses (EIPs) to access the Internet or to provide services accessible from the Internet.

NAT Gateway supports source NAT (SNAT) and destination NAT (DNAT).

- SNAT translates private IP addresses into EIPs, allowing servers in a VPC to share an EIP to access the Internet in a secure and efficient way.

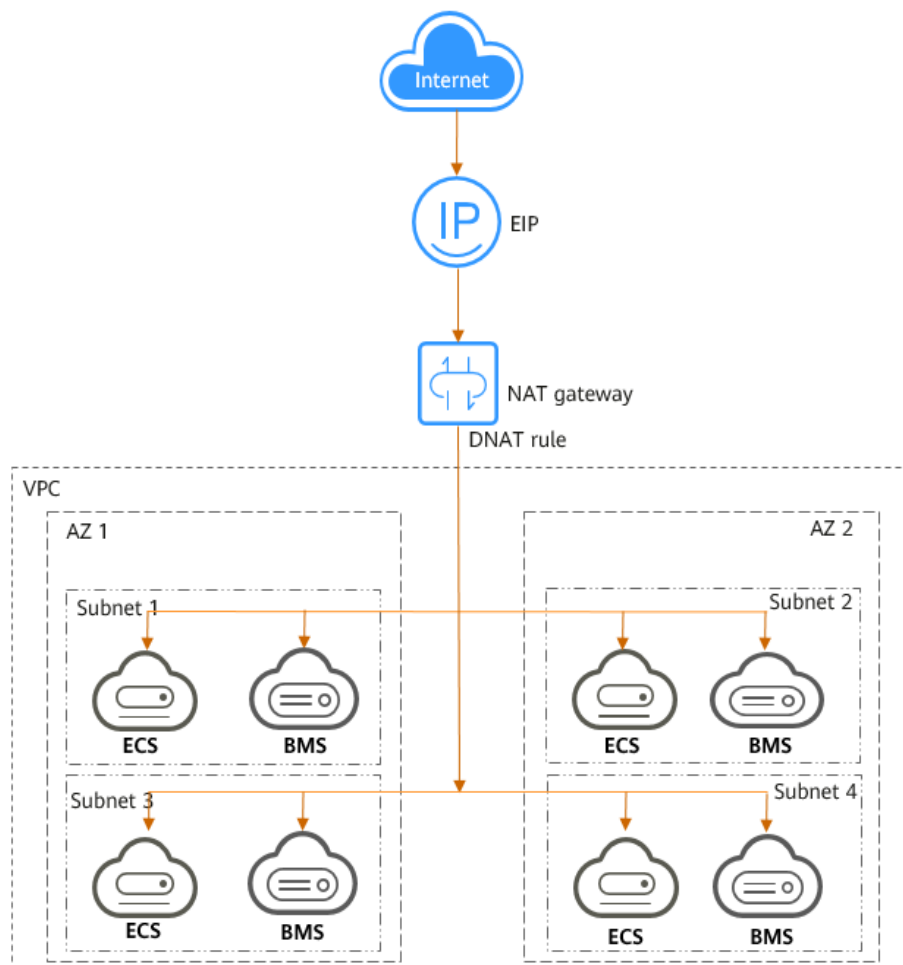
Figure 1-1 shows how an SNAT rule works.

Figure 1-1 NAT gateway with an SNAT rule



- DNAT enables servers in a VPC to share an EIP to provide services accessible from the Internet through IP address mapping or port mapping.

Figure 1-2 shows how a DNAT rule works.

Figure 1-2 NAT gateway with a DNAT rule

1.2 Product Advantages

The NAT Gateway service has the following highlights:

- Flexibility

A NAT gateway can be deployed flexibly across subnets and AZs. Any fault in a single AZ does not affect the service continuity of a NAT gateway. The type and EIP of a NAT gateway can be adjusted at any time.

- Easy of use

Multiple types of NAT gateways are available. You can use them after simple configuration. NAT Gateway supports easy operation and maintenance (O&M) and quick provisioning. They can run stably and reliably.

- Cost-effectiveness

Multiple servers can share an EIP. When you send data through a private IP address or provide services accessible from the Internet using a NAT gateway, the NAT gateway translates the private IP address to a public IP address. The NAT Gateway service helps you save money on EIPs and bandwidth.

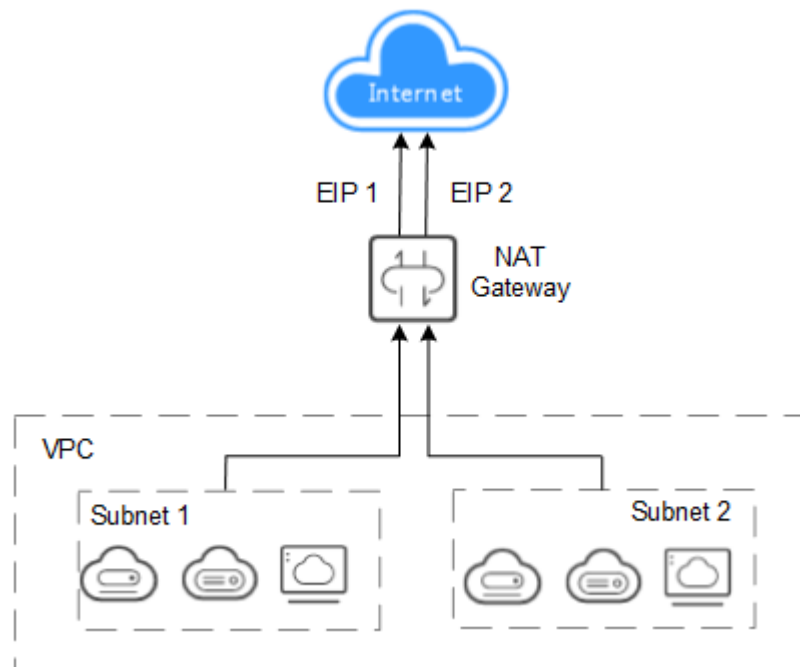
1.3 Application Scenarios

Using SNAT to Enable Servers to Access the Internet

If your servers in a VPC require Internet access, you can use SNAT to let the servers share one or more EIPs to access the Internet without exposing their IP addresses. In a VPC, each subnet corresponds to an SNAT rule, and each SNAT rule is configured with an EIP. NAT Gateway provides different types of NAT gateways that support different numbers of connections. You can create multiple SNAT rules to meet your service requirements.

Figure 1-3 shows how servers in a VPC access the Internet using SNAT.

Figure 1-3 Using SNAT to enable servers to access the Internet



Using DNAT to Allow Servers to Provide Services Accessible from the Internet

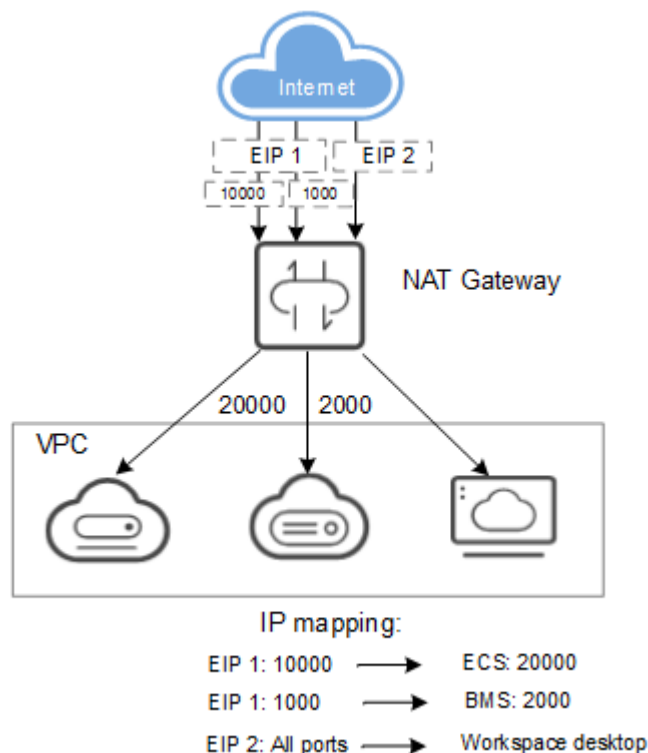
To allow your servers in a VPC to provide services accessible from the Internet, you can use DNAT.

You can associate an EIP with a DNAT rule. As requests with a specific protocol and port access the EIP, NAT Gateway only forwards requests to the port of the target server through the mapping between the ports. NAT Gateway can also forward requests on the EIP to your servers based on IP address mapping. NAT Gateway allows multiple servers to share an EIP, saving costs on bandwidth.

A DNAT rule is configured for one server. If there are multiple servers, you can create several DNAT rules to make the servers share one or more EIPs.

Figure 1-4 shows how servers in a VPC use DNAT to provide services accessible from the Internet. The servers shown in the following figure can be an ECS or BMS.

Figure 1-4 Using DNAT to allow servers to provide services accessible from the Internet

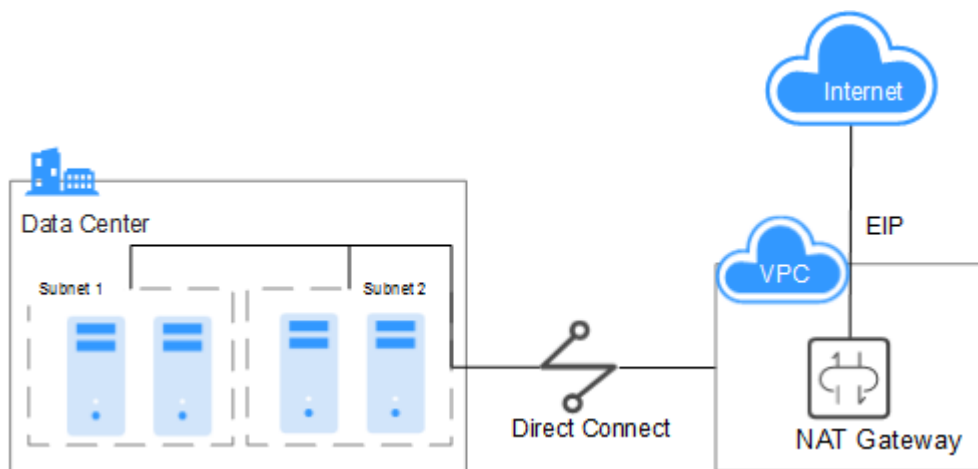


Using SNAT or DNAT to Communicate with the Internet at a High Speed

If a large number of servers in a private cloud or those connect to a VPC through Direct Connect or VPN need secure, high-speed Internet access or need to provide services accessible from the Internet, SNAT and DNAT provide this access. Typical scenarios include Internet, games, e-commerce, and finance across clouds.

Figure 1-5 shows how to communicate with the Internet at a high speed.

Figure 1-5 Using SNAT or DNAT to communicate with the Internet at a high speed



Configuring Highly Available System Using SNAT

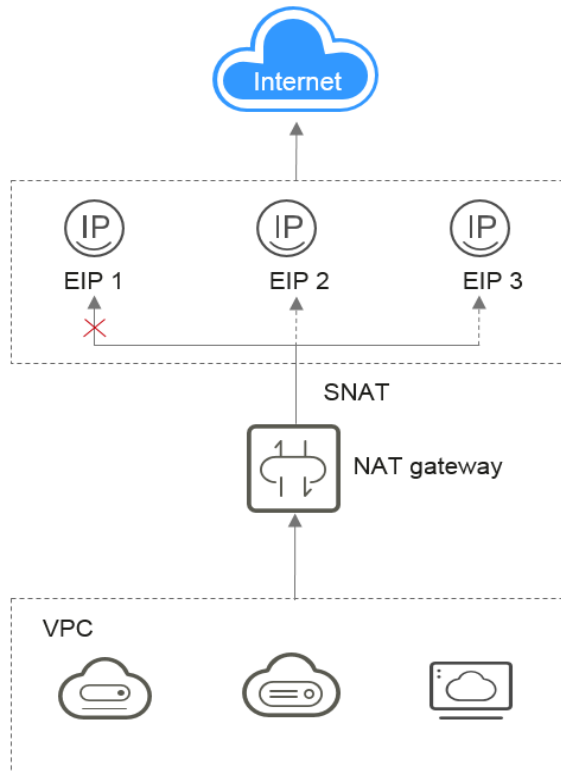
EIPs bound to resources may be attacked. To improve system reliability, you can add multiple EIPs when configuring an SNAT rule. If one EIP is attacked, another EIP can take over the job to ensure services continuity.

If an SNAT rule has multiple EIPs, the system randomly selects an EIP for servers that use the SNAT rule to access the Internet.

Up to 20 EIPs can be added to each SNAT rule. If EIPs added to an SNAT rule are blocked or unavailable due to attacks, delete them from the EIP pool.

Figure 1-6 shows the networking diagram.

Figure 1-6 Configuring highly available system using SNAT



1.4 NAT Gateway Types

A NAT gateway type specifies the maximum number of SNAT connections supported by a NAT gateway.

An SNAT connection consists of the source IP address, source port, destination IP address, destination port, and transmission-layer protocol. The source IP address refers to the EIP, and the source port refers to the EIP port. They will be used to access the destination IP address and port of the Internet. These five elements identify a connection as a unique session.

The data throughput of a NAT gateway is determined by the sum of the EIP bandwidths used by its DNAT rules. For example, if a NAT gateway has two DNAT rules, and their EIP bandwidths are 10 Mbit/s and 5 Mbit/s, respectively, the throughput of the NAT gateway is 15 Mbit/s.

Each NAT gateway supports up to 20 Gbit/s of bandwidth.

The timeout period of an SNAT connection using TCP is 600 seconds.

The timeout period of an SNAT connection using UDP is 300 seconds.

When creating a NAT gateway, select the type based on your service requirements. [Table 1-1](#) lists the NAT gateway types.

Table 1-1 NAT gateway types

Type	Maximum Number of SNAT Connections
Small	10,000
Medium	50,000
Large	200,000
Extra-large	1,000,000

 **NOTE**

- If the requests exceed the maximum connections allowed by your NAT gateway, your services will be adversely affected. To avoid this situation, create alarm rules for the SNAT connection in Cloud Eye.
- The DNAT rules of a NAT gateway are irrelevant to the NAT gateway type. A maximum of 200 DNAT rules can be added to a NAT gateway.

1.5 Notes and Constraints

When using a NAT gateway:

- Multiple rules for one NAT gateway can use the same EIP, but the rules for different NAT gateways must use different EIPs.
- Each VPC can only have one NAT gateway.
- Manually adding the default route for a VPC is not allowed.
- Each VPC subnet can only be used in one SNAT rule.
- SNAT and DNAT rules are designed for different functions. If SNAT and DNAT rules use the same EIP, resource preemption will occur. An SNAT rule cannot share an EIP with a DNAT rule with **Port Type** set to **All ports**.
- DNAT rules do not support the mapping between an EIP and a virtual IP address.
- If both an EIP and a NAT gateway are configured for a server, data will be forwarded through the EIP.
- When you add an SNAT rule, if the rule is used in the VPC scenario, the custom CIDR block must be a subset of the NAT gateway's VPC subnets. If the rule is used in the Direct Connect scenario, the custom CIDR block must be a CIDR block of a Direct Connect connection and cannot overlap with the NAT gateway's VPC subnets.
- After you perform operations on underlying resources of an ECS, for example, changing its specifications, the configured NAT gateway rules will become invalid. Delete the rules and recreate them for the new specifications.
- You can configure only one DNAT rule for each port of a server. One port can be mapped to only one EIP.

1.6 NAT Gateway and Other Services

Table 1-2 Related services

Interactive Function	Related Service	Reference
Local servers that need to access the Internet or provide services accessible from the Internet using a NAT gateway can connect to a VPC using Direct Connect.	Direct Connect	Using SNAT and DNAT Rules to Allow On-premises Servers to Communicate Over the Internet
Local servers that need to access the Internet or provide services accessible from the Internet using a NAT gateway can connect to a VPC through VPN connections.	Virtual Private Network (VPN)	Using SNAT and DNAT Rules to Allow On-premises Servers to Communicate Over the Internet
A NAT gateway enables cloud services (such as ECSs, BMSs, and Workspace desktops) to access the Internet or provide services that are accessible from the Internet.	ECS	Using SNAT to Access the Internet Using DNAT to Provide Services Accessible from the Internet

1.7 Permissions Management

You can use Identity and Access Management (IAM) to manage NAT Gateway permissions and control access to your resources. IAM provides identity authentication, permissions management, and access control.

You can create IAM users for your employees, and assign permissions to these users on a principle of least privilege (PoLP) basis to control their access to specific resource types. For example, you can create IAM users for software developers and assign specific permissions to allow them to use NAT Gateway resources but prevent them from being able to delete resources or perform any high-risk operations.

If your account does not require individual IAM users for permissions management, skip this section.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see the *Identity and Access Management User Guide*.

NAT Gateway Permissions

By default, new IAM users do not have any permissions assigned. To assign permissions to these new users, add them to one or more groups, and attach permissions policies or roles to these groups.

NAT Gateway is a project-level service deployed and accessed in specific physical regions. When assigning NAT Gateway permissions to a user group, specify region-specific projects where the permissions will take effect. If you select **All projects**, the permissions will be granted for all region-specific projects. When accessing NAT Gateway, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that provides only a limited number of service-level roles. When using roles to grant permissions, you also need to assign dependency roles. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization for securer access control. For example, you can grant NAT Gateway users only the permissions for managing a certain type of NAT gateways and SNAT rules. Most policies define permissions based on APIs. For the API actions supported by NAT Gateway, see section "Permissions Policies and Supported Actions" in the *NAT Gateway API Reference*.

Table 1-3 lists all the system-defined roles and policies supported by NAT Gateway.

Table 1-3 System-defined roles and policies supported by NAT Gateway

Policy Name	Description	Type	Dependency
NAT FullAccess	All operations on NAT Gateway resources.	System-defined policy	N/A
NAT ReadOnly Access	Read-only permissions for all NAT Gateway resources.	System-defined policy	N/A
NAT Administrator	All operations on NAT Gateway resources.	System-defined role	All operations on NAT Gateway resources. To be granted this permission, users must also have the Tenant Guest permission.

Table 1-4 lists the common operations supported by each NAT Gateway system policy or role. Select the policies or roles as required.

Table 1-4 Common operations supported by each system-defined policy or role of NAT Gateway

Operation	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Creating a NAT gateway	√	x	√
Querying NAT gateways	√	√	√
Querying NAT gateway details	√	√	√
Updating a NAT gateway	√	x	√
Deleting a NAT gateway	√	x	√
Adding an SNAT rule	√	x	√
Viewing an SNAT rule	√	√	√
Modifying an SNAT rule	√	x	√
Deleting an SNAT rule	√	x	√
Adding a DNAT rule	√	x	√
Viewing a DNAT rule	√	√	√
Modifying a DNAT rule	√	x	√
Deleting a DNAT rule	√	x	√

 **NOTE**

To add or modify a DNAT rule, your account must have the **NAT FullAccess** permission or fine-grained permission **nat:dnatRules:create/nat:dnatRules:update**. After a DNAT rule is configured, add a security group rule to allow the Internet to access servers for which the DNAT rule is configured. Otherwise, the DNAT rule cannot take effect. Therefore, the **VPC FullAccess** permission or fine-grained permission **vpc:securityGroups:create** is required.

Helpful Links

- [What Is IAM?](#)
- [Creating a User and Granting NAT Gateway Permissions](#)

1.8 Region and AZ

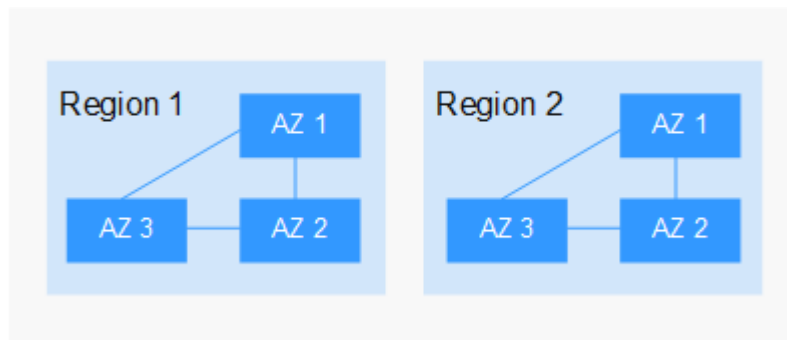
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

[Figure 1-7](#) shows the relationship between regions and AZs.

Figure 1-7 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

1.9 Basic Concepts

EIP

An EIP can be directly accessed over the Internet. A private IP address is an IP address on a local area network (LAN) and cannot be routed through the Internet.

An EIP is a static, public IP address. You can bind an EIP to an ECS in your subnet to enable the ECS in your VPC to communicate with the Internet through a fixed public IP address.

Each EIP can be used by only one ECS at a time.

SNAT Connections

An SNAT connection consists of the source IP address, source port, destination IP address, destination port, and transmission-layer protocol. The source IP address refers to the EIP, and the source port refers to the EIP port. They will be used to access the destination IP address and port of the Internet. These five elements identify a connection as a unique session.

DNAT Connections

A DNAT connection enables servers in a VPC to share an EIP to provide services accessible from the Internet through IP address or port mapping.

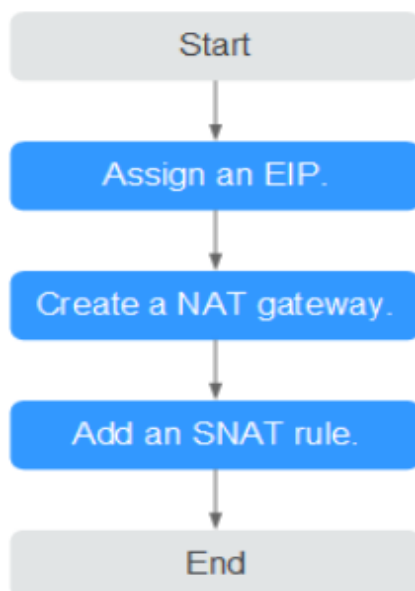
2 Getting Started

2.1 Using SNAT to Access the Internet

2.1.1 Overview

If servers (ECSs and BMSs) without EIPs bound need to access the Internet, the servers can share one or more EIPs to access the Internet through a NAT gateway. This method provides access without exposing their IP addresses. [Figure 2-1](#) illustrates the process.

Figure 2-1 Flowchart



2.1.2 Step 1: Assign an EIP

Scenarios

Assign an EIP and enable your servers in a VPC to access the Internet through a NAT gateway by sharing the EIP.

Procedure

For details, see the *Elastic IP User Guide*. After you assign an EIP, you do not need to bind it to a server here.

2.1.3 Step 2: Create a NAT Gateway

Scenarios

This section guides you on how to create a public NAT gateway to enable your servers to access the Internet or to provide services available from the Internet.

Prerequisites

- When creating a public NAT gateway, you must specify its VPC, subnet, and type.
- Ensure that the VPC does not have the default route.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click **Create Public NAT Gateway**.
4. Configure the parameters as prompted. For details, see [Table 2-1](#).

Table 2-1 Parameter descriptions of a public NAT gateway

Parameter	Description
Region	The region where the NAT gateway is located.
Name	The name of the NAT gateway. The name can contain a maximum of 64 characters and only digits, letters, underscores (_), and hyphens (-) are allowed.
VPC	The VPC that the NAT gateway belongs to. Select a VPC which is not used by any other NAT gateways and has no default route. You can change the VPC only when you are creating the NAT gateway. After the NAT gateway is created, you cannot modify the VPC.

Parameter	Description
Subnet	The subnet of the VPC that the NAT gateway belongs to. The subnet must have at least one available IP address. You can change the subnet only when you are creating the NAT gateway. After the NAT gateway is created, you cannot change the subnet.
Type	The type of the NAT gateway. The type can be Small , Medium , Large , and Extra-large . You can click Learn more on the page to view details about each type.
Enterprise Project	The enterprise project that the NAT gateway belongs to. If an enterprise project is configured for a NAT gateway, the NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, enterprise project default will be used.
Description	Supplementary information about the NAT gateway. The description can contain up to 255 characters.

- Click **Create Now**. Confirm the NAT gateway information on the displayed page.
- If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a NAT gateway.
- In the NAT gateway list, view the NAT gateway status.

2.1.4 Step 3: Add an SNAT Rule

Scenarios

After a NAT gateway is created, add SNAT rules. With an SNAT rule, your servers in a specified subnet can access the Internet by sharing the same EIP.

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

Prerequisites

A NAT gateway has been created.

Procedure

- Log in to the management console.
- Under **Network**, choose **NAT Gateway**.
- On the displayed page, click the name of the NAT gateway for which you want to add the SNAT rule.

4. On the **SNAT Rules** tab, click **Add SNAT Rule**.
5. Configure the parameters as prompted. [Table 2-2](#) describes the parameters.

Table 2-2 Parameter descriptions

Parameter	Condition	Description
Scenario	N/A	Select VPC if your servers in a VPC will use the SNAT rule to access the Internet. Different servers in a VPC can share the same EIP to access the Internet.
Type	This parameter is available only when you select VPC for Scenario .	You can set it to Subnet or Custom based on service requirements. Select Subnet if all servers in a VPC subnet need to access the Internet through the SNAT rule. Select Custom if only specific servers in a VPC subnet need to access the Internet through the SNAT rule.
Subnet	This parameter is available only when you select VPC for Scenario , and Subnet for Type .	The subnet in which servers can access the Internet through the SNAT rule.
CIDR Block	This parameter is available only when you select VPC for Scenario , and Custom for Type .	The CIDR block is a subset of the NAT gateway's VPC subnets. Servers whose IP addresses in the custom CIDR block can access the Internet through the SNAT rule.
EIP	N/A	The EIP used for accessing the Internet. You can select an EIP that either is not bound to any resource, has been bound to a DNAT rule with Port Type set to Specific port of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.
Monitoring	N/A	Alarm rules are created in Cloud Eye. The alarm rules help you monitor your SNAT connections and keep you informed of any changes in a timely manner.
Description	N/A	Supplementary information about the SNAT rule. The description can contain up to 255 characters.

6. Click **OK**.

 **NOTE**

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

2.1.5 Step 4: Verify the Result

Scenarios

After you add an SNAT rule to a NAT gateway, you can verify that the SNAT rule has been added successfully.

Prerequisites

An SNAT rule has been added.

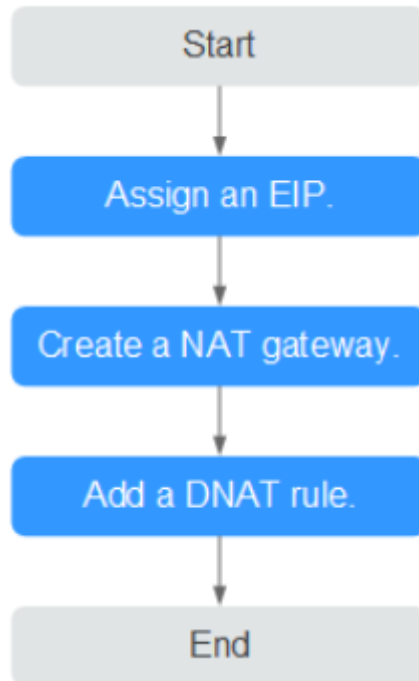
Procedure

1. Log in to the management console.
2. Under **Network**, click **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. In the SNAT rule list, you can view details about the SNAT rule. If **Status** is **Running**, the SNAT rule has been added successfully.

2.2 Using DNAT to Provide Services Accessible from the Internet

2.2.1 Overview

When one or more servers (ECSs and BMSs) in a VPC are required to provide services accessible from the Internet, you can add DNAT rules. [Figure 2-2](#) illustrates the process.

Figure 2-2 Flowchart

2.2.2 Step 1: Assign an EIP

Scenarios

Assign an EIP and enable servers in a VPC to provide services accessible from the Internet using a NAT gateway by sharing the EIP.

Procedure

For details, see the *Elastic IP User Guide*. After you assign an EIP, you do not need to bind it to a server here.

2.2.3 Step 2: Create a NAT Gateway

Scenarios

This section guides you on how to create a public NAT gateway to enable your servers to access the Internet or to provide services available from the Internet.

Prerequisites

- When creating a public NAT gateway, you must specify its VPC, subnet, and type.
- Ensure that the VPC does not have the default route.

Procedure

1. Log in to the management console.

2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click **Create Public NAT Gateway**.
4. Configure the parameters as prompted. For details, see [Table 2-3](#).

Table 2-3 Parameter descriptions of a public NAT gateway

Parameter	Description
Region	The region where the NAT gateway is located.
Name	The name of the NAT gateway. The name can contain a maximum of 64 characters and only digits, letters, underscores (_), and hyphens (-) are allowed.
VPC	The VPC that the NAT gateway belongs to. Select a VPC which is not used by any other NAT gateways and has no default route. You can change the VPC only when you are creating the NAT gateway. After the NAT gateway is created, you cannot modify the VPC.
Subnet	The subnet of the VPC that the NAT gateway belongs to. The subnet must have at least one available IP address. You can change the subnet only when you are creating the NAT gateway. After the NAT gateway is created, you cannot change the subnet.
Type	The type of the NAT gateway. The type can be Small , Medium , Large , and Extra-large . You can click Learn more on the page to view details about each type.
Enterprise Project	The enterprise project that the NAT gateway belongs to. If an enterprise project is configured for a NAT gateway, the NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, enterprise project default will be used.
Description	Supplementary information about the NAT gateway. The description can contain up to 255 characters.

5. Click **Create Now**. Confirm the NAT gateway information on the displayed page.
6. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a NAT gateway.
7. In the NAT gateway list, view the NAT gateway status.

2.2.4 Step 3: Add a DNAT Rule

Scenarios

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

You can configure a DNAT rule for each port of a server. If multiple servers need to provide services accessible from the Internet, create multiple DNAT rules.

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the NAT gateway for which you want to add the DNAT rule.
4. On the NAT gateway details page, click the **DNAT Rules** tab.
5. Click **Add DNAT Rule**.
6. Configure the parameters as prompted. For details, see [Table 2-4](#).

Table 2-4 Parameter descriptions

Parameter	Description
Scenario	Select VPC if your servers in a VPC will use the DNAT rule to provide services accessible from the Internet. Different servers in a VPC can share the same EIP to provide services accessible from the Internet.
Port Type	The port type. You can select All ports or Specific port . <ul style="list-style-type: none"> • All ports: This is equivalent to assigning an EIP to a server. Any requests on the EIP will be forwarded by the NAT gateway to your server based on IP address mapping. • Specific port: The NAT gateway only forwards requests with a specific protocol and port on the EIP to the corresponding port of the target server.
Protocol	The protocol can be TCP or UDP. This parameter is available if you select Specific port for Port Type . If you select All ports , the value of this parameter will be All by default.

Parameter	Description
EIP	The EIP that will be used by the server to provide services accessible from the Internet. You can select an EIP that either is not bound to any resource, has been bound to a DNAT rule with Port Type set to Specific port of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.
Outside Port	The port of the EIP. This parameter is available if you select Specific port for Port Type . The value ranges from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Private IP Address	The private IP address of the server that provides services accessible from the Internet through the DNAT rule.
Inside Port	The port of the server that provides services accessible from the Internet through the DNAT rule. This parameter is available if you select Specific port for Port Type . The value ranges from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Description	Supplementary information about the DNAT rule. The description can contain up to 255 characters.

7. Click **OK**.

2.2.5 Step 4: Verify the Result

Scenarios

After you add a DNAT rule to a NAT gateway, you can verify that the DNAT rule has been added successfully.

Prerequisites

A DNAT rule has been added.

Procedure

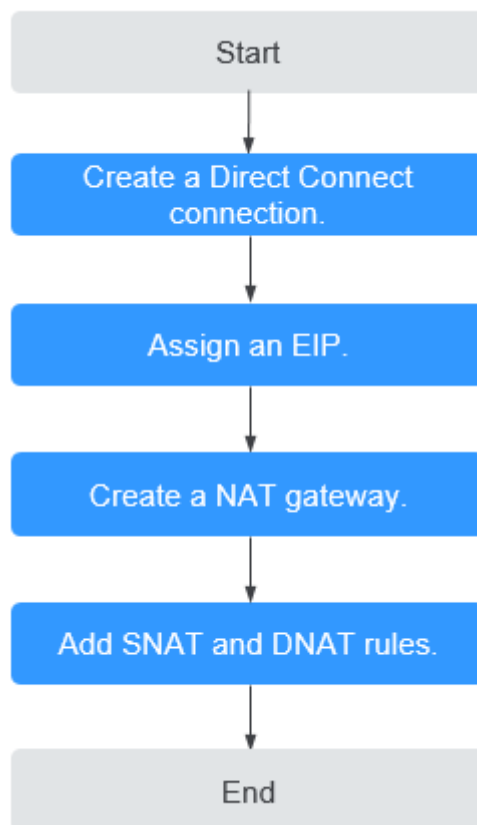
1. Log in to the management console.
2. Under **Network**, click **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. In the DNAT rule list, you can view details about the DNAT rule. If **Status** is **Running**, the DNAT rule has been added successfully.

2.3 Using SNAT and DNAT Rules to Allow On-premises Servers to Communicate Over the Internet

2.3.1 Overview

If servers in your data center need to access the Internet or to provide services accessible from the Internet, NAT Gateway provides you with high-quality network services. You need to first create a Direct Connect or VPN connection to connect your servers in an on-premises data center to the cloud, and then create NAT gateways and configure SNAT rules to communicate over the Internet. [Figure 2-3](#) illustrates the process.

Figure 2-3 Flowchart



2.3.2 Step 1: Create a Direct Connect Connection

Scenarios

Create a Direct Connect connection for connecting a VPC to your data center before enabling your servers in the data center to access the Internet or to provide services accessible from the Internet through NAT gateways.

Procedure

For details on how to enable Direct Connect, see the *Direct Connect User Guide*.

2.3.3 Step 2: Assign an EIP

Scenarios

You can assign an EIP, which can work together with a NAT gateway to allow servers that are connected to a public cloud system using Direct Connect or VPN to access the Internet or to provide services accessible from the Internet.

Procedure

For details, see the *Elastic IP User Guide*. After you assign an EIP, you do not need to bind it to a server here.

2.3.4 Step 3: Create a NAT Gateway

Scenarios

This section guides you on how to create a public NAT gateway to enable your servers to access the Internet or to provide services available from the Internet.

Prerequisites

- When creating a public NAT gateway, you must specify its VPC, subnet, and type.
- Ensure that the VPC does not have the default route.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
3. On the displayed page, click **Create Public NAT Gateway**.
4. Configure the parameters as prompted. For details, see [Table 2-5](#).

Table 2-5 Parameter descriptions of a public NAT gateway

Parameter	Description
Region	The region where the NAT gateway is located.
Name	The name of the NAT gateway. The name can contain a maximum of 64 characters and only digits, letters, underscores (_), and hyphens (-) are allowed.

Parameter	Description
VPC	The VPC that the NAT gateway belongs to. Select a VPC which is not used by any other NAT gateways and has no default route. You can change the VPC only when you are creating the NAT gateway. After the NAT gateway is created, you cannot modify the VPC.
Subnet	The subnet of the VPC that the NAT gateway belongs to. The subnet must have at least one available IP address. You can change the subnet only when you are creating the NAT gateway. After the NAT gateway is created, you cannot change the subnet.
Type	The type of the NAT gateway. The type can be Small , Medium , Large , and Extra-large . You can click Learn more on the page to view details about each type.
Enterprise Project	The enterprise project that the NAT gateway belongs to. If an enterprise project is configured for a NAT gateway, the NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, enterprise project default will be used.
Description	Supplementary information about the NAT gateway. The description can contain up to 255 characters.

5. Click **Create Now**. Confirm the NAT gateway information on the displayed page.
6. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a NAT gateway.
7. In the NAT gateway list, view the NAT gateway status.

2.3.5 Step 4: Add an SNAT Rule

Scenarios

After a NAT gateway is created, you can add SNAT rules for it. With SNAT rules, servers that are connected to a VPC using Direct Connect can access the Internet by sharing an EIP.

An SNAT rule is configured for one CIDR block. If servers that are connected to a VPC using Direct Connect are in multiple CIDR blocks, you can create several SNAT rules to make the servers share one or more EIPs.

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the NAT gateway for which you want to add the SNAT rule.
4. On the **SNAT Rules** tab, click **Add SNAT Rule**.
5. Configure the parameters as prompted. For details, see [Table 2-6](#).

Table 2-6 Parameter descriptions

Parameter	Description
Scenario	Select Direct Connect if servers in your data center need to access the Internet. The servers in your data center that are connected to a VPC through Direct Connect or VPN can access the Internet through the SNAT rule.
CIDR Block	On-premises servers whose IP address in this CIDR block can access the Internet through the SNAT rule.
EIP	The EIP used for accessing the Internet. You can select an EIP that either is not bound to any resource, has been bound to a DNAT rule with Port Type set to Specific port of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.
Monitoring	Alarm rules are created in Cloud Eye. The alarm rules help you monitor your SNAT connections and keep you informed of any changes in a timely manner.
Description	Supplementary information about the SNAT rule. The description can contain up to 255 characters.

6. Click **OK**.
7. View details in the SNAT rule list. If **Status** is **Running**, the rule has been added.

NOTE

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

2.3.6 Step 5: Add a DNAT Rule

Scenarios

After a NAT gateway is created, you can add DNAT rules to allow servers in your on-premises data center to provide services accessible from the Internet.

You can configure a DNAT rule for each port of a server. If there are multiple servers, you can create several DNAT rules to make the servers share one or more EIPs.

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the NAT gateway for which you want to add the DNAT rule.
4. On the NAT gateway details page, click the **DNAT Rules** tab.
5. Click **Add DNAT Rule**.
6. Configure the parameters as prompted. For details, see [Table 2-7](#).

Table 2-7 Parameter descriptions

Parameter	Description
Scenario	Select Direct Connect if servers in your data center need to access the Internet. Servers in your data center that connected to a VPC using Direct Connect or VPN can provide services accessible from the Internet through the DNAT rule.
Port Type	The port type. You can select All ports or Specific port . <ul style="list-style-type: none"> • All ports: This is equivalent to assigning an EIP to a server. Any requests on the EIP will be forwarded by the NAT gateway to your server based on IP address mapping. • Specific port: The NAT gateway only forwards requests with a specific protocol and port on the EIP to the corresponding port of the target server.
Protocol	The protocol can be TCP or UDP. This parameter is available if you select Specific port for Port Type . If you select All ports , the value of this parameter will be All by default.

Parameter	Description
EIP	The EIP that will be used by the server to provide services accessible from the Internet. You can select an EIP that either is not bound to any resource, has been bound to a DNAT rule with Port Type set to Specific port of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.
Outside Port	The port of the EIP. This parameter is available if you select Specific port for Port Type . The value ranges from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Private IP Address	The IP address of the server in the local data center or the user's private IP address. With DNAT, a server using this private IP address in your data center that is connected to a VPC through Direct Connect or VPN can provide services accessible from the Internet.
Inside Port	The port of the server that provides services accessible from the Internet through the DNAT rule. This parameter is available if you select Specific port for Port Type . The value ranges from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Description	Supplementary information about the DNAT rule. The description can contain up to 255 characters.

7. Click **OK**.
8. View details in the DNAT rule list. If **Status** is **Running**, the rule has been added.

3 Managing NAT Gateways

3.1 Creating a NAT Gateway

Scenarios

This section guides you on how to create a public NAT gateway to enable your servers to access the Internet or to provide services available from the Internet.

Prerequisites

- When creating a public NAT gateway, you must specify its VPC, subnet, and type.
- Ensure that the VPC does not have the default route.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click **Create Public NAT Gateway**.
4. Configure the parameters as prompted. For details, see [Table 3-1](#).

Table 3-1 Parameter descriptions of a public NAT gateway

Parameter	Description
Region	The region where the NAT gateway is located.
Name	The name of the NAT gateway. The name can contain a maximum of 64 characters and only digits, letters, underscores (_), and hyphens (-) are allowed.

Parameter	Description
VPC	The VPC that the NAT gateway belongs to. Select a VPC which is not used by any other NAT gateways and has no default route. You can change the VPC only when you are creating the NAT gateway. After the NAT gateway is created, you cannot modify the VPC.
Subnet	The subnet of the VPC that the NAT gateway belongs to. The subnet must have at least one available IP address. You can change the subnet only when you are creating the NAT gateway. After the NAT gateway is created, you cannot change the subnet.
Type	The type of the NAT gateway. The type can be Small , Medium , Large , and Extra-large . You can click Learn more on the page to view details about each type.
Enterprise Project	The enterprise project that the NAT gateway belongs to. If an enterprise project is configured for a NAT gateway, the NAT gateway belongs to this enterprise project. If you do not specify an enterprise project, enterprise project default will be used.
Description	Supplementary information about the NAT gateway. The description can contain up to 255 characters.

5. Click **Create Now**. Confirm the NAT gateway information on the displayed page.
6. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a NAT gateway.
7. In the NAT gateway list, view the NAT gateway status.

3.2 Viewing a NAT Gateway

Scenarios

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

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.

2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. View the NAT gateway details on the displayed page.

3.3 Modifying a NAT Gateway

Scenarios

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

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

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, locate the row that contains the target NAT gateway and click **Modify** in the **Operation** column.
4. Modify the name, type, or description of the NAT gateway as prompted.
5. Click **OK**.

3.4 Deleting a NAT Gateway

Scenarios

You can delete NAT gateways to release resources.

Prerequisites

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

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, locate the row that contains the target NAT gateway and click **Delete** in the **Operation** column.
4. In the displayed dialog box, click **Yes**.

4 Managing SNAT Rules

4.1 Adding an SNAT Rule

Scenarios

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

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

Prerequisites

- A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the NAT gateway for which you want to add the SNAT rule.
4. On the **SNAT Rules** tab, click **Add SNAT Rule**.
5. Configure the parameters as prompted. For details, see [Table 4-1](#).

Table 4-1 Parameter descriptions

Parameter	Condition	Description
Scenario	N/A	<p>The scenarios where the SNAT rule is used.</p> <p>Select VPC if your servers in a VPC need to access the Internet.</p> <p>Select Direct Connect if the servers that are connected to a VPC through Direct Connect in your data center need to access the Internet.</p>
Type	This parameter is available only when you select VPC for Scenario .	<p>You can set it to Subnet or Custom based on service requirements.</p> <p>Select Subnet if all servers in a VPC subnet need to access the Internet through the SNAT rule.</p> <p>Select Custom if only specific servers in a VPC subnet need to access the Internet through the SNAT rule.</p>
Subnet	This parameter is available only when you select VPC for Scenario , and Subnet for Type .	The subnet in which servers can access the Internet through the SNAT rule.
EIP	<ul style="list-style-type: none"> This parameter is available only when you select VPC for Scenario. This parameter is available only when you select Direct Connect for Scenario. 	<p>The EIP used for accessing the Internet.</p> <p>You can select an EIP that either is not bound to any resource, has been bound to a DNAT rule with Port Type set to Specific port of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.</p> <p>You can select multiple EIPs at once. Up to 20 EIPs can be selected for each SNAT rule. The EIP used for the SNAT rule is randomly chosen from the ones you select when you add the rule.</p>

Parameter	Condition	Description
CIDR Block	<ul style="list-style-type: none">This parameter is available only when you select VPC for Scenario, and Custom for Type.This parameter is available only when you select Direct Connect for Scenario.	<p>In a VPC scenario, specify a VPC subnet to enable the servers whose IP addresses in the subnet to access the Internet through the SNAT rule.</p> <p>In a Direct Connect scenario, specify a CIDR block of your data center to enable your servers to access the Internet through the SNAT rule.</p>
Monitoring	N/A	Alarm rules are created in Cloud Eye. The alarm rules help you monitor your SNAT connections and keep you informed of any changes in a timely manner.
Description	N/A	Supplementary information about the NAT gateway. The description can contain up to 255 characters.

6. Click **OK**.

 **NOTE**

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

4.2 Viewing an SNAT Rule

Scenarios

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

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. In the SNAT rule list, view the details about the SNAT rule.

4.3 Modifying an SNAT Rule

Scenarios

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

Prerequisites

An SNAT rule has been added for the NAT gateway.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. On the **SNAT Rules** tab, locate the row that contains the SNAT rule you want to modify.
5. Click **Modify** in the **Operation** column.
6. In the displayed dialog box, modify the required parameters.
7. Click **OK**.

4.4 Deleting an SNAT Rule

Scenarios

Delete the SNAT rules that you no longer need.

Prerequisites

An SNAT rule has been added for the NAT gateway.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. In the SNAT rule list, locate the row that contains the target SNAT rule and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **Yes**.

5 Managing DNAT Rules

5.1 Adding a DNAT Rule

Scenarios

After a 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 of 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

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the NAT gateway for which you want to add the DNAT rule.
4. On the NAT gateway details page, click the **DNAT Rules** tab.
5. Click **Add DNAT Rule**.

NOTICE

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

6. Configure the parameters as prompted. For details, see [Table 5-1](#).

Table 5-1 Parameter descriptions

Parameter	Description
Scenario	<p>VPC: Servers in the VPC can share an EIP to provide services accessible from the Internet through the DNAT rule.</p> <p>Direct Connect: Servers in your data center that are connected to a VPC using Direct Connect or VPN can provide services accessible from the Internet through the DNAT rule.</p>
Port Type	<p>The port type. You can select All ports or Specific port.</p> <ul style="list-style-type: none"> • All ports: This is equivalent to assigning an EIP to a server. Any requests on the EIP will be forwarded by the NAT gateway to your server based on IP address mapping. • Specific port: The NAT gateway only forwards requests with a specific protocol and port on the EIP to the corresponding port of the target server.
Protocol	<p>The protocol can be TCP or UDP. This parameter is available if you select Specific port for Port Type. If you select All ports, the value of this parameter will be All by default.</p>
EIP	<p>The EIP that will be used by the server to provide services accessible from the Internet.</p> <p>You can select an EIP that either is not bound to any resource, has been bound to a DNAT rule with Port Type set to Specific port of the current NAT gateway, or has been bound to an SNAT rule of the current NAT gateway.</p>
Outside Port	<p>The port of the EIP. This parameter is available if you select Specific port for Port Type. The value ranges from 1 to 65535.</p> <p>You can enter a single port number or a port range, for example, 80 or 80-100.</p>
Private IP Address	<ul style="list-style-type: none"> • 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 the IP address of the server in the local data center or the user's private IP address. This IP address is used by local servers that are connected to a VPC through Direct Connect or VPN to provide services accessible from the Internet through DNAT. • Configure the port of Private IP Address if you select Specific port for Port Type.

Parameter	Description
Inside Port	The port of the server that provides services accessible from the Internet through the DNAT rule. This parameter is available if you select Specific port for Port Type . The value ranges from 1 to 65535. You can enter a single port number or a port range, for example, 80 or 80-100.
Description	Supplementary information about the DNAT rule. The description can contain up to 255 characters.

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

5.2 Viewing a DNAT Rule

Scenarios

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

Prerequisites

A DNAT rule has been added.

Procedure

- Log in to the management console.
- Under **Network**, choose **NAT Gateway**.
- On the displayed page, click the name of the target NAT gateway.
- On the NAT gateway details page, click the **DNAT Rules** tab.
- In the DNAT rule list, view the details about the DNAT rule.

5.3 Modifying a DNAT Rule

Scenarios

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

Prerequisites

A DNAT rule has been added for the NAT gateway.

Procedure

- Log in to the management console.

2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. On the NAT gateway details page, click the **DNAT Rules** tab.
5. Locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.
6. In the displayed dialog box, modify the required parameters.
7. Click **OK**.

5.4 Deleting a DNAT Rule

Scenarios

Delete a DNAT rule that you no longer need.

Prerequisites

A DNAT rule has been added for the NAT gateway.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. On the NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.
6. In the displayed dialog box, click **Yes**.

5.5 Deleting DNAT Rules in Batches

Scenarios

Delete the DNAT rules that you no longer need.

Prerequisites

DNAT rules have been added for the NAT gateway.

Procedure

1. Log in to the management console.
2. Under **Network**, click **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. On the NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, select the target DNAT rules and click **Delete DNAT Rule**.

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

5.6 Importing and Exporting DNAT Rules Using Templates

Scenarios

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

You can configure a DNAT rule for each port of a server. If multiple servers need to provide services accessible from the Internet, create multiple DNAT rules.

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, choose **NAT Gateway**.
3. On the displayed page, click the name of the NAT gateway for which you want to add the DNAT rule.
4. On the NAT gateway details page, click the **DNAT Rules** tab.
5. On the displayed page, click **Import Rule** and then **Download Template**.
6. Fill in DNAT rule parameters based on the table heading in the template. For details, see [Table 5-2](#).

Table 5-2 Parameter descriptions

Parameter	Description
Scenario	<p>VPC: Servers in the VPC can share an EIP to provide services accessible from the Internet through the DNAT rule.</p> <p>Direct Connect: Servers in your data center that are connected to a VPC using Direct Connect or VPN can provide services accessible from the Internet through the DNAT rule.</p>
Port Type	<p>The port type. You can select All ports or Specific port.</p> <ul style="list-style-type: none">• All ports: This is equivalent to assigning an EIP to a server. Any requests on the EIP will be forwarded by the NAT gateway to your server based on IP address mapping.• Specific port: The NAT gateway only forwards requests with a specific protocol and port on the EIP to the corresponding port of the target server.

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 , the value of this parameter will be All by default.
EIP	The EIP that will be used by the server to provide services accessible from the Internet. Only EIPs that have not been bound or that have been bound to a DNAT rule in the current VPC are available for selection.
Outside Port	The EIP port. This parameter is available if you select Specific port for Port Type . You can enter a single port number or a port range, for example, 80 or 80-100.
Private IP Address	<ul style="list-style-type: none">• 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 the IP address of the server in the local data center or the user's private IP address. This IP address is used by local servers that are connected to a VPC through Direct Connect or VPN to provide services accessible from the Internet through DNAT.
Inside Port	<ul style="list-style-type: none">• In a VPC scenario, set this parameter to the port of the server in a VPC.• In a Direct Connect scenario, set this parameter to the port of the server in the local data center or the user's private port.• This parameter is available if you select Specific port for Port Type. The number of inside and outside ports must match.

7. After filling in the template, click **Import Rule**, select the template, and click **Import**.
8. View details in the DNAT rule list. If **Status** is **Running**, the rules have been added.
9. On the **DNAT Rules** tab page, click **Export Rule** to export the configured DNAT rule template.

6 Permissions Management

6.1 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 an account or cloud service to perform efficient O&M on your NAT Gateway resources.

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

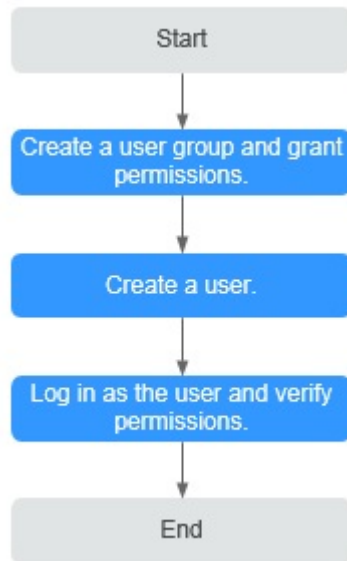
This section describes the procedure for granting permissions (see [Figure 6-1](#)).

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 [Permissions](#).

Process Flow

Figure 6-1 Process for granting NAT Gateway permissions



1. Create and authorize a user group.
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 **Create 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.

6.2 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 section "Permissions Policies and Supported Actions" in the *NAT Gateway API Reference*.

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 "Fine-Grained Policy Management" > "Creating a Custom Policy" in the *Identity and Access Management User Guide*. 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"
    }
  ]
}
```

```
]
}
```

7 Monitoring Management

7.1 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 7-1 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	NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bits/s	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	NAT gateway	1 minute
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: Count	≥ 0	NAT gateway	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: Count	≥ 0	NAT gateway	1 minute
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	NAT gateway	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	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. . Unit: Percent	≥ 0	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 NAT gateway is 20 Gbit/s. Unit: Percent	≥ 0	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 NAT gateway is 20 Gbit/s. Outbound bandwidth usage = Used bandwidth / Maximum bandwidth of the NAT gateway x 100%. Unit: Percent NOTE This metric is used to monitor the performance of NAT gateways instead of the EIP bandwidth.	≥ 0	NAT gateway	1 minute

Dimensions

Key	Value
nat_gateway_id	NAT gateway ID

7.2 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. Under **Management & Deployment**, select **Cloud Eye**.
3. In the left navigation pane, choose **Alarm Management > Alarm Rules**.
4. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters to create an alarm rule, or modify an existing alarm rule.
5. On the **Create Alarm Rule** page, follow the prompts to configure the parameters.
 - a. Set the alarm rule name and description.


Table 7-2 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-b6a1
Description	(Optional) Provides supplementary information about the alarm rule.

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

Table 7-3 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

Parameter	Description	Example Value
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select Resource groups or Specific resources . NOTE <ul style="list-style-type: none"> 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.	-
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.	-
Alarm Severity	Specifies the alarm severity, which can be Critical, Major, Minor , or Informational .	Major

c. Configure the alarm notification.

Table 7-4 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.

Parameter	Description
Notification Object	<p>Specifies the object that receives alarm notifications. You can select the account contact or a topic.</p> <ul style="list-style-type: none"> • 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	<p>Cloud Eye sends notifications only within the validity period specified in the alarm rule.</p> <p>If Validity Period is set to 08:00-20:00, Cloud Eye sends notifications only within 08:00-20:00.</p>
Trigger Condition	<p>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.</p>

6. After the parameters are set, click **Create**.
After the alarm rule is set, the system automatically notifies you when an alarm is triggered.

 **NOTE**

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

7.3 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. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring > NAT Gateway**.
4. 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.

8 FAQs

8.1 NAT Gateway

8.1.1 What Is the Relationship Between a VPC, NAT Gateway, EIP Bandwidth, and ECS?

- A VPC is a secure, isolated, logical network environment.
- A NAT gateway enables ECSs in the VPC to access the Internet.
- EIP is a service that provides valid static IP addresses on the Internet. The throughput of a VPC is determined by the EIP bandwidth.
- An ECS is a running instance in the VPC and uses the NAT gateway to access the Internet.

8.1.2 How Does A NAT Gateway Offer High Availability?

The backend of a NAT gateway supports automatic disaster recovery through hot standby and works with Cloud Eye to report alarms, thereby reducing risks and improving availability.

8.1.3 Which Ports Cannot Be Accessed?

Some carriers will block the following ports for security reasons. It is recommended that you do not use the following ports.

Protocol	Ports Not Supported
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

8.1.4 What Should I Do If I Fail to Access the Internet Through the NAT Gateway?

If your server cannot access the Internet through the NAT gateway, you may have configured the VPC route table incorrectly. Perform the following steps to reset the route table:

1. Locate the route table associated with the subnet in the VPC.
2. Check whether the route table contains the route to the NAT gateway. If not, add the route.
3. Ensure that the destination address of the route to be added contain the target address.

8.1.5 Can I Change the VPC for a NAT Gateway After It Is Created?

No.

You can select a VPC when creating a NAT gateway and cannot change the VPC for the NAT gateway after it is created.

8.2 SNAT

8.2.1 Why Is SNAT Used?

Besides requiring services provided by the system, some ECSs also need to access the Internet to obtain information or download software. However, assigning a public IP address to each ECS consumes already-limited IPv4 addresses, incurs additional costs, and may increase the attack surface in a virtual environment. Enabling multiple ECSs to share a single public IP address is preferable and more practical. This can be done using SNAT.

8.2.2 What Are SNAT Connections?

An SNAT connection consists of the source IP address, source port, destination IP address, destination port, and transmission-layer protocol. These five elements identify a connection as a unique session. The source IP address refers to the EIP, and the source port refers to the EIP port. They will be used to access the destination IP address and port of the Internet.

SNAT supports three protocols: TCP, UDP, and ICMP. A NAT gateway supports up to 55,000 concurrent connections for each destination IP address and port. If any of the destination IP address, port number, and protocol (TCP/UDP/ICMP) changes, you can create another 55,000 connections. The number of connections you query on an ECS may be different from the actual number of SNAT connections. (You can run the **netstat** command to query the number of connections.) Assume that an ECS creates 100 connections to a fixed destination every second. 55,000 connections will be used up in about 10 minutes without considering the dropped idle connections. As a result, new connections cannot be established.

If there is no data packet passing through the SNAT connection for a long time, the connection will be timed out. Therefore, to prevent connection interruption, initiate more data packets or use TCP to maintain connections. In addition, to prevent service interruption caused by insufficient connections, use Cloud Eye to monitor the number of SNAT connections and set appropriate alarm rules.

8.2.3 What Is the Bandwidth of the NAT Gateway When a Server Accesses the Internet Through the NAT Gateway? Where Can I Configure the Bandwidth?

NAT Gateway SNAT translates a private IP address to a public IP address by binding EIPs to servers in a VPC. When a server accesses the Internet through the NAT gateway, the bandwidth is related to the bandwidth of the EIP assigned to you.

8.2.4 How Do I Resolve Packet Loss or Connection Failure Issues When Using a NAT Gateway?

If packet loss or connection failures occur on a server that uses the NAT gateway to access the Internet, you can check the SNAT connections on the Cloud Eye console. If the number of SNAT connections exceeds that the NAT gateway type supports, there will be packet loss or connection failures. If the number of connections exceeds the upper limit, change the NAT gateway type.

8.2.5 What Are the Relationships and Differences Between the CIDR Blocks in a NAT Gateway and in an SNAT Rule?

When creating a NAT gateway, you must specify the VPC and subnet CIDR block for the NAT gateway. This CIDR block can only be used by the system.

When you are creating an SNAT rule with **Scenario** set to **VPC**, configure a subnet CIDR block for the VPC so that servers in the subnet can access the Internet through the SNAT rule.

When you are creating an SNAT rule with **Scenario** set to **Direct Connect**, configure the CIDR block of a local data center or another VPC so that ECSs in the CIDR block can access the Internet through the SNAT rule.

8.3 DNAT

8.3.1 Why Is DNAT Used?

DNAT enables servers in a VPC to share an EIP to provide services accessible from the Internet. For details, see [Adding a DNAT Rule](#).

8.3.2 Can I Modify DNAT Rules?

You can modify DNAT rules.

8.3.3 What Should I Do If NAT Gateway Rules Become Invalid After ECS Specifications Are Changed?

If the ECS specifications are changed, the configured rules will become invalid. You will need to delete the rules and recreate them.

A Change History

Released On	Description
2022-04-12	This issue is the first official release.