

Copyright © Huawei Technologies Co., Ltd. 2020. 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 Product Specifications.....	7
1.5 Notes and Constraints.....	8
1.6 NAT Gateway and Other Services.....	9
1.7 Region and AZ.....	9
1.8 Basic Concepts.....	10
2 Getting Started.....	12
2.1 Using SNAT to Access the Internet.....	12
2.1.1 Overview	12
2.1.2 Step 1: Assign an EIP.....	13
2.1.3 Step 2: Create a Public NAT Gateway.....	13
2.1.4 Step 3: Add an SNAT Rule.....	15
2.1.5 Step 4: Verify the Result.....	16
2.2 Using DNAT to Provide Services Accessible from the Internet.....	17
2.2.1 Overview	17
2.2.2 Step 1: Assign an EIP.....	17
2.2.3 Step 2: Create a Public NAT Gateway.....	18
2.2.4 Step 3: Add a DNAT Rule.....	19
2.2.5 Step 4: Verify the Result.....	21
2.3 Using SNAT and DNAT Rules to Allow On-premises Servers to Communicate Over the Internet.....	21
2.3.1 Overview	21
2.3.2 Step 1: Create a Direct Connect Connection.....	22
2.3.3 Step 2: Assign an EIP.....	22
2.3.4 Step 2: Create a Public NAT Gateway.....	23
2.3.5 Step 4: Add an SNAT Rule.....	24
2.3.6 Step 5: Add a DNAT Rule.....	26
3 Managing NAT Gateways.....	29
3.1 Creating a NAT Gateway.....	29
3.2 Viewing a NAT Gateway.....	31

3.3 Modifying a NAT Gateway.....	31
3.4 Deleting a NAT Gateway.....	32
4 Managing SNAT Rules.....	33
4.1 Adding an SNAT Rule.....	33
4.2 Viewing an SNAT Rule.....	35
4.3 Modifying an SNAT Rule.....	36
4.4 Deleting an SNAT Rule.....	36
5 Managing DNAT Rules.....	38
5.1 Adding a DNAT Rule.....	38
5.2 Viewing a DNAT Rule.....	41
5.3 Modifying a DNAT Rule.....	41
5.4 Deleting a DNAT Rule.....	42
5.5 Deleting DNAT Rules in Batches.....	42
5.6 Importing and Exporting DNAT Rules Using Templates.....	43
6 Monitoring Management.....	46
6.1 Supported Metrics.....	46
6.2 Creating Alarm Rules.....	50
6.3 Viewing Metrics.....	51
7 FAQs.....	52
7.1 NAT Gateway.....	52
7.1.1 What Is the Relationship Between VPC, NAT Gateway, EIP Bandwidth, and ECS?.....	52
7.1.2 How Does A NAT Gateway Offer High Availability?.....	52
7.1.3 Which Ports Cannot Be Accessed?.....	52
7.1.4 What Can I Do If I Fail to Access the Internet Through the NAT Gateway?.....	53
7.1.5 Can I Change the VPC for a NAT Gateway After It Is Created?.....	53
7.1.6 What Is the Quota of the NAT Gateway?.....	53
7.2 SNAT.....	54
7.2.1 Why SNAT Is Used?.....	54
7.2.2 What Are SNAT Connections?.....	54
7.2.3 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
7.2.4 How Do I Resolve Packet Loss or Connection Failure Issues When Using a NAT Gateway?.....	55
7.2.5 What Are the Relationships and Differences Between the CIDR Blocks in a NAT Gateway and in an SNAT Rule?.....	55
7.3 DNAT.....	55
7.3.1 Why DNAT Is Used?.....	55
7.3.2 Does the DNAT Rule Support the Update Operation?.....	55
7.3.3 What Can I Do If NAT Gateway Rules Become Invalid After ECS Specifications Are Changed?.....	55
A Change History.....	56

1 Overview

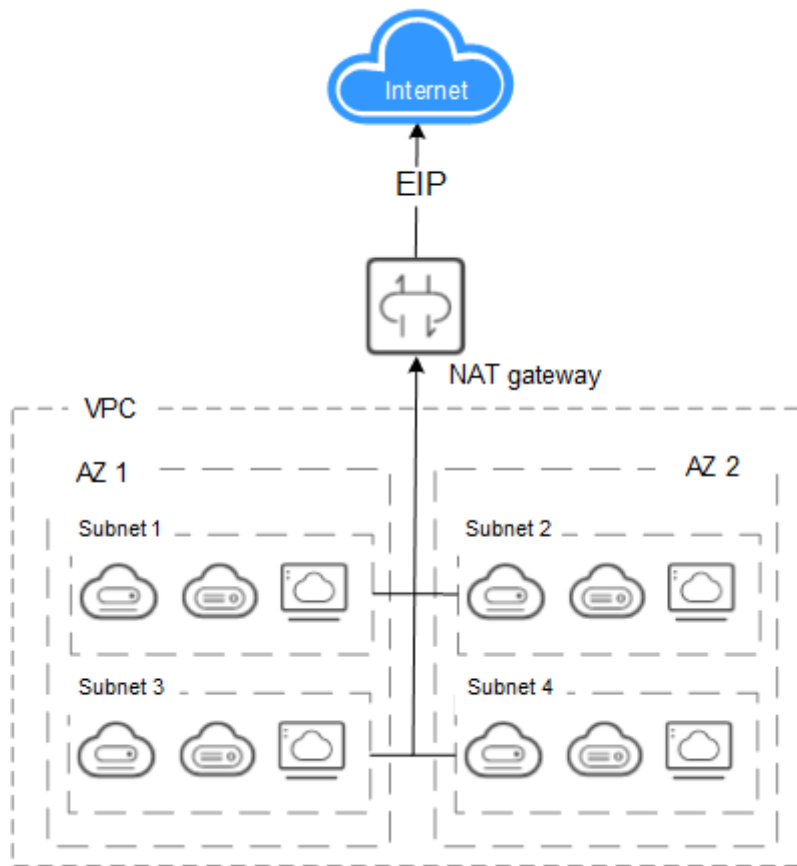
1.1 What Is NAT Gateway?

The NAT Gateway service provides the network address translation (NAT) function with 10 Gbit/s bandwidth for servers, such as Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), and Workspace desktops, in a Virtual Private Cloud (VPC), or servers that connect to a VPC through Direct Connect or Virtual Private Network (VPN) in local 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) functions.

- The SNAT function 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 the SNAT architecture.

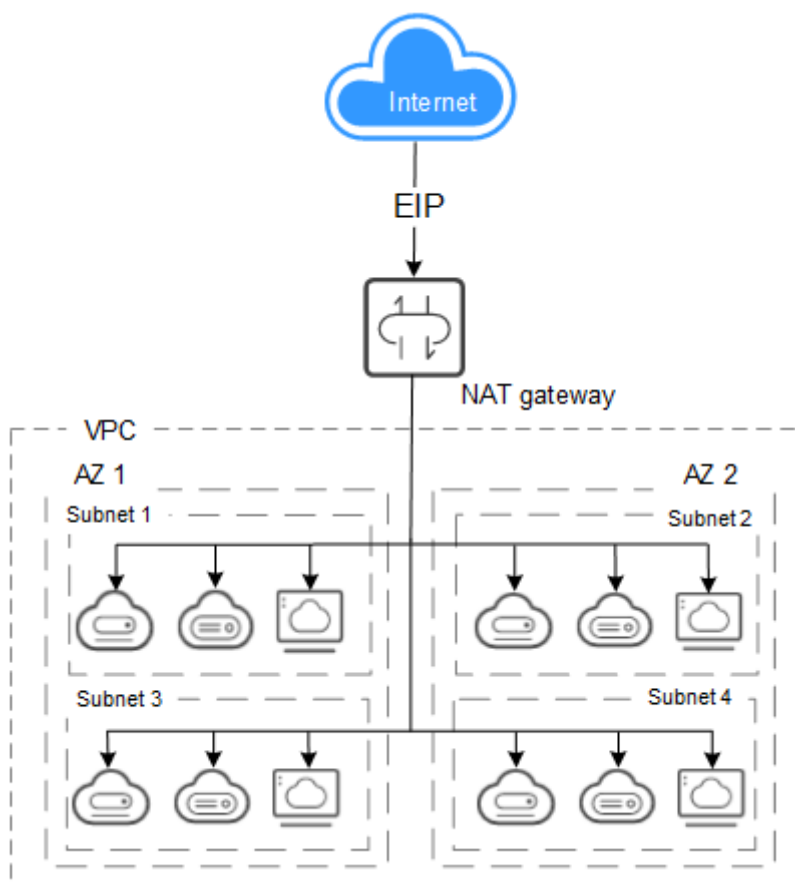
Figure 1-1 SNAT architecture



- The DNAT function 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 the DNAT architecture.

Figure 1-2 DNAT architecture



1.2 Product Advantages

The NAT Gateway service has the following highlights:

- Flexible deployment

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.

- Diversified and easy-to-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-effective

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 reduce costs in EIPs and bandwidth.

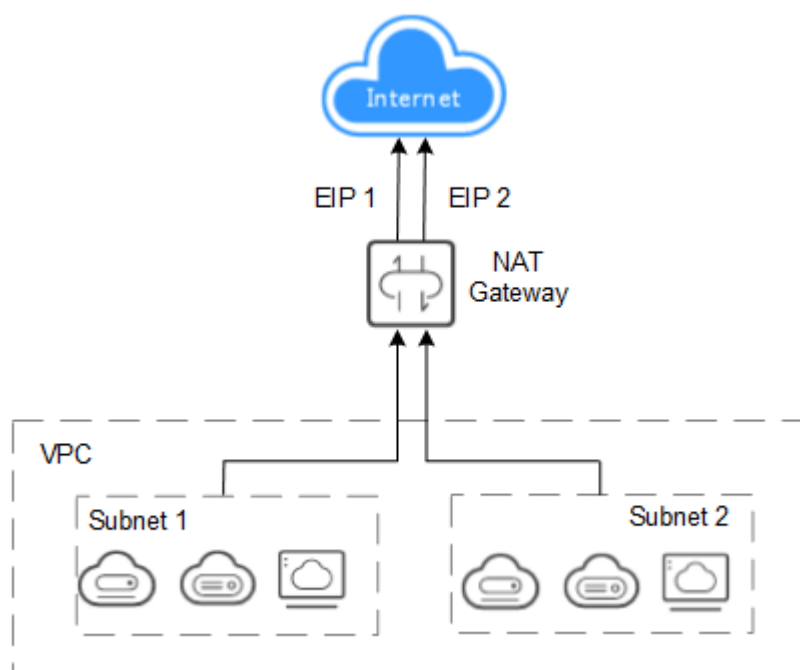
1.3 Application Scenarios

Using SNAT to Access the Internet

If your servers in the VPC require Internet access, you can use the SNAT function 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 one SNAT rule, and each SNAT rule is configured with one 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 access the Internet



Using DNAT to Provide Services Accessible from the Internet

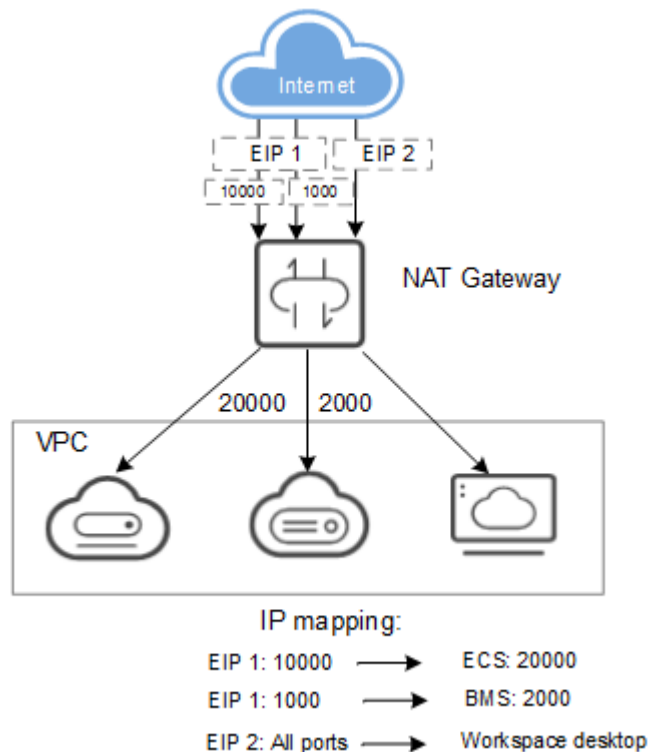
To allow your servers in a VPC to provide services for the Internet, you can use the DNAT function.

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

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 provide services accessible from the Internet using DNAT. The servers shown in the following figure can be an ECS, a BMS, or a Workspace desktop.

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

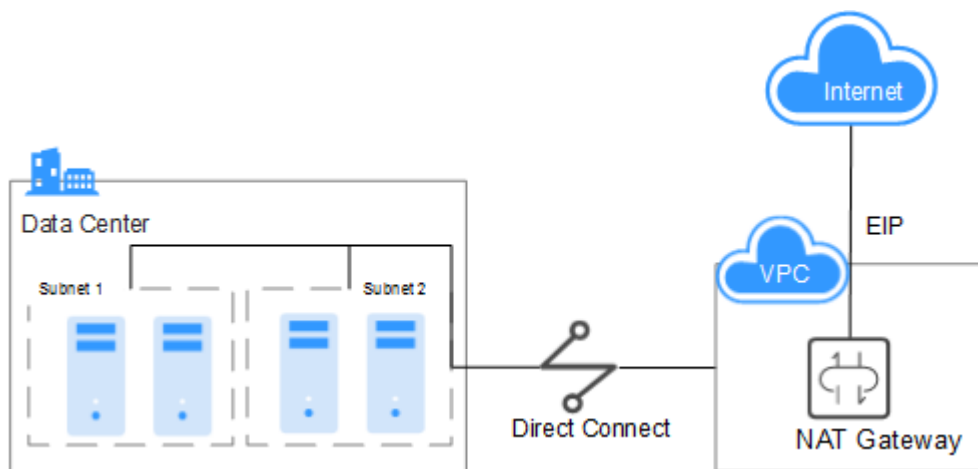


Using SNAT or DNAT to Communicate with the Internet in a High-Speed Way

If a large number of servers that in a private cloud or connect to a VPC through a Direct Connect or VPN connection need to securely access the Internet in a high speed way or to provide services accessible from the Internet, SNAT and DNAT can be used in such scenario. The similar scenarios include Internet, games, e-commerce, and finance.

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

Figure 1-5 Using SNAT and DNAT to communicate with the Internet in a high-speed way



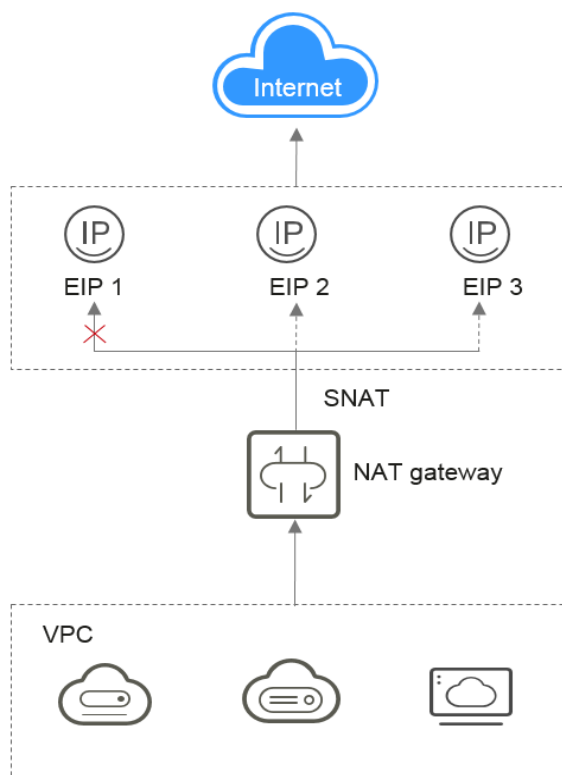
Configuring Highly Available System Using SNAT

EIPs that 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, services can use another EIP to ensure service running.

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

A maximum of 20 EIPs can be added to each SNAT rule. If EIPs added to an SNAT rule are blocked or unavailable due to attacks, you need to manually delete them from the EIP pool.

Figure 1-6 shows the networking diagram.

Figure 1-6 Configuring highly available system using SNAT

1.4 Product Specifications

The specification refers to 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 and source port are the EIP and port translated by SNAT to access the destination IP address and port of a public network. With these five elements, a connection can be distinguished as a unique session.

The data throughput of a NAT gateway is determined by the sum of EIP bandwidths used by its DNAT rules. For example, a NAT gateway has two DNAT rules. If the bandwidth of the EIP bound to one rule is 10 Mbit/s and that bound to the other is 5 Mbit/s, the throughput of the NAT gateway is 15 Mbit/s.

Each NAT gateway supports up to 10 Gbit/s forwarding 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 proper type based on your service requirements. [Table 1-1](#) lists the NAT gateway specifications.

Table 1-1 NAT Gateway type

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 allowed connections of your NAT gateway, your services will be adversely affected. To avoid this situation, you are advised to create alarm rules for the SNAT connection in Cloud Eye.
- The number of DNAT rules that you can add for a NAT gateway has no relationship with the NAT gateway type. A maximum of 200 DNAT rules can be added for each NAT gateway.

1.5 Notes and Constraints

Observe the following 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 reuse 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.
- The custom CIDR block configured when adding an SNAT rule must be a subset of the VPC subnet CIDR blocks.
- The custom CIDR block must be a CIDR block of a Direct Connect connection and cannot conflicts with VPC's existing subnet CIDR blocks.
- When you perform operations on underlying resources of an ECS, for example, changing its specifications, the configured NAT gateway rules become invalid. You need to delete the rules and reconfigure them.

1.6 NAT Gateway and Other Services

Table 1-2 Related services

Interactive Function	Related Service	Reference
Local servers that connect to a VPC using Direct Connect can access the Internet or provide services that are accessible from the Internet using a NAT gateway.	Direct Connect	Using SNAT and DNAT Rules to Allow On-premises Servers to Communicate Over the Internet
Local servers that connect to a VPC using VPN can access the Internet or provide services that are accessible from the Internet using a NAT gateway.	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 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

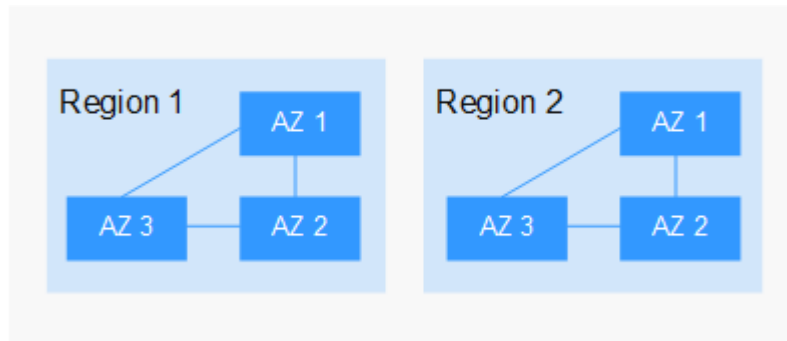
1.7 Region and AZ

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 an AZ will not affect other AZs.

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 low 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 low 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](#).

1.8 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) in the public cloud system 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 and source port are the EIP and port translated by SNAT to access the destination IP address and port of a public network. With these five elements, a connection can be distinguished 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 mapping or port mapping.

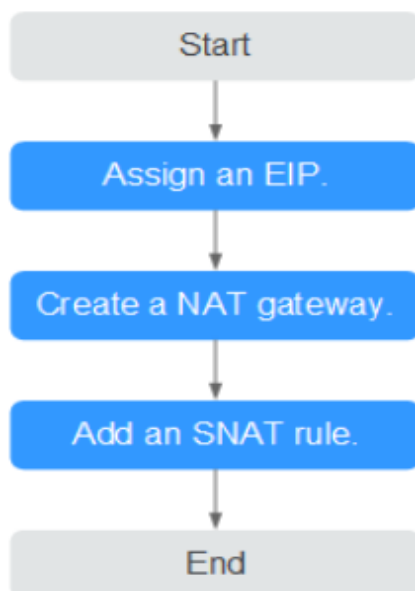
2 Getting Started

2.1 Using SNAT to Access the Internet

2.1.1 Overview

If your servers (ECSs, BMSs, and desktops) without EIPs bound need to access the Internet, the servers can share one or more EIPs to access the Internet through a NAT gateway without exposing their IP addresses. [Figure 2-1](#) shows the required operations.

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 Public 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 for external networks.

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**, click **NAT Gateway**.
3. On the displayed page, click **Create Public NAT Gateway**.

Figure 2-2 Create Public NAT Gateway

The screenshot displays the 'Create Public NAT Gateway' configuration interface. It includes the following elements:

- Region:** A dropdown menu set to 'G42'. A note below states: 'Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.'
- Name:** A text input field containing 'nat-fbat'.
- VPC:** A dropdown menu set to 'vpc-d2e7'. A link 'View VPC' is present. A note below states: 'Only VPCs without NAT gateways and default routes can be selected.'
- Subnet:** A dropdown menu set to 'subnet-d329 (192.168.0.0/24)'. A link is present. A note below states: 'The selected subnet is only used by the NAT gateway. To enable communication over the Internet, you need to add rules after the NAT gateway is created.'
- Type:** Radio buttons for 'Small', 'Medium', 'Large', and 'Extra-large'. 'Small' is selected. A note below states: 'Supports up to 10,000 connections. Learn more.'
- Enterprise Project:** A dropdown menu set to '--Select--'. A link 'Create Enterprise Project' is present.
- Description:** A text area with a character count of '0/255'.
- Tag:** A section with a note: 'It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags'. It contains 'Tag key' and 'Tag value' input fields. A note below states: 'You can add 10 more tags.'

4. Set the parameters as prompted. For details, see [Table 2-1](#).

Table 2-1 Parameter description

Parameter	Description
Region	Specifies the region where the NAT gateway is located.
Name	Specifies the name of the NAT gateway. The value is a string of 1 to 64 characters consisting of digits, letters, underscores (_), and hyphens (-).
VPC	Specifies the VPC to which the NAT gateway belongs. 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	Specifies the subnet of the VPC to which the NAT gateway belongs. 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	Specifies the type of the NAT gateway. The value can be Small , Medium , Large , and Extra-large . You can click Learn more on the page to view details about each type.
Enterprise Project	Specifies the enterprise project to which the NAT gateway belongs. 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, the default enterprise project will be used.
Description	Provides supplementary information about the NAT gateway. The description can contain a maximum of 255 characters.

5. Click **Create Now**. The page for you to confirm the NAT gateway specifications is displayed.
6. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a NAT gateway.
7. On the **NAT Gateway** homepage, check the NAT gateway status.

2.1.4 Step 3: Add an SNAT Rule

Scenarios

After the NAT gateway is created, you need to 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 make multiple servers share more EIPs.

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, click **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. Set the parameters as prompted. [Table 2-2](#) describes the parameters.

Table 2-2 Parameter description

Parameter	Condition	Description
Scenario	N/A	Select VPC when your servers in a VPC need to use the SNAT rule to access the Internet. Servers in the VPC can share one EIP to access the Internet.
Type	This parameter is available when you select VPC for Scenario .	You can set it to Subnet or Custom based on service requirements. Select Subnet when all servers in a VPC subnet need to access the Internet through the SNAT rule. Select Custom when specific servers in a VPC subnet need to access the Internet through the SNAT rule.
Subnet	This parameter is available when you select VPC for Scenario , and Subnet for Type .	Specifies the subnet in which servers can access the Internet through the SNAT rule.

Parameter	Condition	Description
CIDR Block	This parameter is available when you select VPC for Scenario , and Custom for Type .	Specifies a CIDR block that is a subset of a VPC subnet CIDR block. Servers whose IP addresses in the custom CIDR block can access the Internet through the SNAT rule.
EIP	This parameter is available when you select VPC for Scenario .	Specifies the EIP used for accessing the Internet. You can only select an EIP that has not been bound, 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	Create alarm rules in Cloud Eye. The alarm rules help you monitor your SNAT connections in a timely manner.
Description	N/A	Provides supplementary information about the SNAT rule. The description can contain a maximum of 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

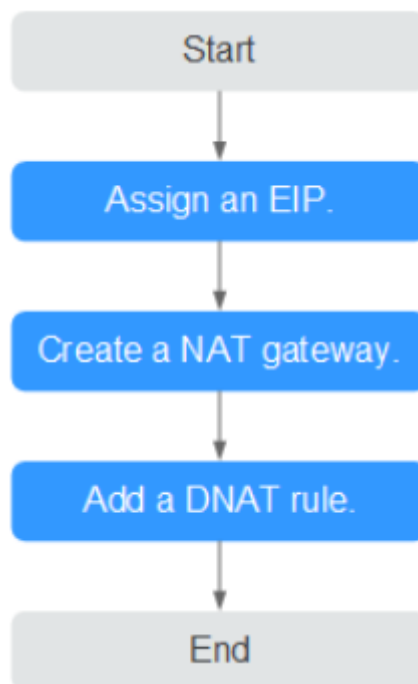
1. Log in to the management console.
2. Under **Network**, click **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. In the SNAT rule list, you can view details about the SNAT rule. If **Status** is **Running**, the SNAT rule has been added successfully.

2.2 Using DNAT to Provide Services Accessible from the Internet

2.2.1 Overview

When one or more servers (ECSs, BMSs, and Workspace desktops) in a VPC are required to provide services accessible from the Internet, you can add DNAT rules. [Figure 2-3](#) shows the required operations.

Figure 2-3 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 Public 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 for external networks.

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**, click **NAT Gateway**.
3. On the displayed page, click **Create Public NAT Gateway**.

Figure 2-4 Create Public NAT Gateway

The screenshot shows the 'Create Public NAT Gateway' configuration page. The fields are as follows:

- Region:** G42
- Name:** nat-float
- VPC:** vpc-d2e7
- Subnet:** subnet-d329 (192.168.0.0/24)
- Type:** Small (selected), Medium, Large, Extra-large
- Enterprise Project:** --Select--
- Description:** 0/255
- Tag:** Tag key, Tag value

A 'Create Now' button is located at the bottom right of the form.

4. Set the parameters as prompted. For details, see [Table 2-3](#).

Table 2-3 Parameter description

Parameter	Description
Region	Specifies the region where the NAT gateway is located.

Parameter	Description
Name	Specifies the name of the NAT gateway. The value is a string of 1 to 64 characters consisting of digits, letters, underscores (_), and hyphens (-).
VPC	Specifies the VPC to which the NAT gateway belongs. 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	Specifies the subnet of the VPC to which the NAT gateway belongs. 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	Specifies the type of the NAT gateway. The value can be Small , Medium , Large , and Extra-large . You can click Learn more on the page to view details about each type.
Enterprise Project	Specifies the enterprise project to which the NAT gateway belongs. 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, the default enterprise project will be used.
Description	Provides supplementary information about the NAT gateway. The description can contain a maximum of 255 characters.

5. Click **Create Now**. The page for you to confirm the NAT gateway specifications is displayed.
6. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a NAT gateway.
7. On the **NAT Gateway** homepage, check 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, you need to create multiple DNAT rules.

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, click **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. Set the parameters as prompted. For details, see [Table 2-4](#).

Table 2-4 Parameter description

Parameter	Description
Scenario	Select VPC when your servers in a VPC need to share one EIP to provide services accessible from the Internet.
Port Type	Specifies the port type, including All ports and Specific port . <ul style="list-style-type: none"> • All ports: indicates the IP mapping method. This method 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: indicates the port mapping method. The NAT gateway forwards the requests with 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.
EIP	Specifies the EIP that will be used by the server to provide services accessible from the Internet. You can only select an EIP that has not been bound, 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	Specifies the port of the EIP. This parameter is available if you select Specific port for Port Type . The value ranges from 1 to 65535. The value can be a single port number or a port range, for example, 80 or 80-100.

Parameter	Description
Private IP Address	Specifies the private IP address of the server that provides services accessible from the Internet through the DNAT rule.
Inside Port	Specifies 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. The value can be a single port number or a port range, for example, 80 or 80-100.
Description	Provides supplementary information about the DNAT rule. The description can contain a maximum of 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

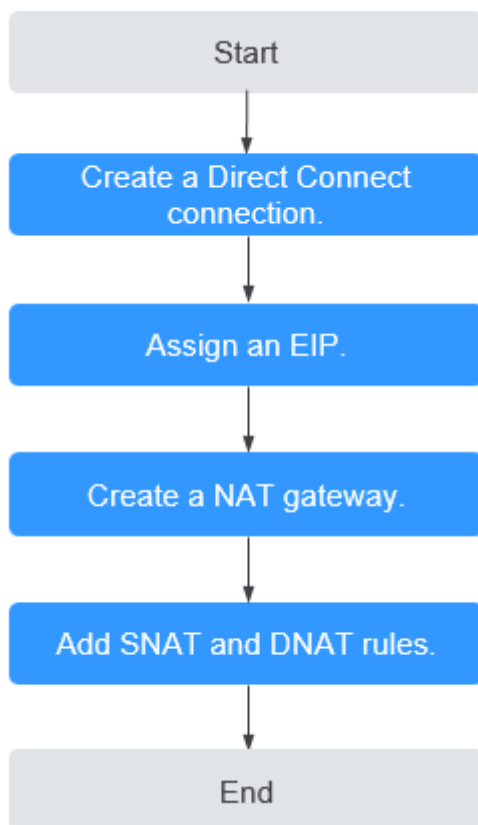
1. Log in to the management console.
2. Under **Network**, click **NAT Gateway**.
3. On the displayed page, click the name of the target NAT gateway.
4. In the DNAT rule list, you can view details about the DNAT rule. If **Status** is **Running**, the DNAT rule has been added successfully.

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 2-5](#) shows the required operations.

Figure 2-5 Flowchart



2.3.2 Step 1: Create a Direct Connect Connection

Scenarios

You need to 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 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 2: Create a Public 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 for external networks.

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**, click **NAT Gateway**.
3. On the displayed page, click **Create Public NAT Gateway**.

Figure 2-6 Create Public NAT Gateway

The screenshot displays the 'Create Public NAT Gateway' configuration interface. It includes the following fields and options:

- Region:** G42
- Name:** nat-float
- VPC:** vpc-d2e7
- Subnet:** subnet-d329 (192.168.0.0/24)
- Type:** Small (selected), Medium, Large, Extra-large
- Enterprise Project:** --Select--
- Description:** 0/255
- Tag:** Tag key, Tag value

A 'Create Now' button is located at the bottom right of the form.

4. Set the parameters as prompted. For details, see [Table 2-5](#).

Table 2-5 Parameter description

Parameter	Description
Region	Specifies the region where the NAT gateway is located.

Parameter	Description
Name	Specifies the name of the NAT gateway. The value is a string of 1 to 64 characters consisting of digits, letters, underscores (_), and hyphens (-).
VPC	Specifies the VPC to which the NAT gateway belongs. 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	Specifies the subnet of the VPC to which the NAT gateway belongs. 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	Specifies the type of the NAT gateway. The value can be Small , Medium , Large , and Extra-large . You can click Learn more on the page to view details about each type.
Enterprise Project	Specifies the enterprise project to which the NAT gateway belongs. 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, the default enterprise project will be used.
Description	Provides supplementary information about the NAT gateway. The description can contain a maximum of 255 characters.

5. Click **Create Now**. The page for you to confirm the NAT gateway specifications is displayed.
6. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a NAT gateway.
7. On the **NAT Gateway** homepage, check 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**, click **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**.

Figure 2-7 Add SNAT Rule

Add SNAT Rule

Info:

- If an ECS is associated with both an EIP and a NAT gateway, data is forwarded through the EIP. [View restrictions](#)
- SNAT and DNAT are used for different services. If an SNAT rule and a DNAT rule use the same EIP, there may be service conflicts.
- An SNAT rule cannot share an EIP with a DNAT rule with Port Type set to All ports.

NAT Gateway Name: nat-1121

* Scenario: VPC Direct Connect/Cloud Connect

* CIDR Block: [View Virtual Interface](#)

* EIP: You can select 20 more EIPs. [View EIP](#) All projects Enter an EIP

<input type="checkbox"/> EIP	EIP Type	Bandwidth Name	Bandwidth (Mb...)	Billing Mode	Enterprise Pr...
<input type="checkbox"/>	Dynamic BGP	ecs-16dc-bandwid...	5	Pay-per-use	default

Selected EIPs (0). **The EIP used for the SNAT rule will be randomly chosen from the ones selected here.**

Monitoring: [Create alarm rules in Cloud Eye to monitor your SNAT connections.](#)

Description:

5. Specify the parameters as prompted. For details, see [Table 2-6](#).

Table 2-6 Parameter description

Parameter	Description
Scenario	Select Direct Connect when 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	Specifies that local servers whose IP address in this CIDR block can access the Internet through the SNAT rule.

Parameter	Description
EIP	Specifies the EIP used for accessing the Internet. You can only select an EIP that has not been bound, 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	Create alarm rules in Cloud Eye. The alarm rules help you monitor your SNAT connections in a timely manner.
Description	Provides supplementary information about the SNAT rule. The description can contain a maximum of 255 characters.

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

 **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 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**, click **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**.

Figure 2-8 Add DNAT Rule

6. Set the parameters as prompted. For details, see [Table 2-7](#).

Table 2-7 Parameter description

Parameter	Description
Scenario	Select Direct Connect when 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	Specifies the port type, including All ports and Specific port . <ul style="list-style-type: none"> • All ports: indicates the IP mapping method. This method 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: indicates the port mapping method. The NAT gateway forwards the requests with 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	Specifies the EIP that will be used by the server to provide services accessible from the Internet. You can only select an EIP that has not been bound, 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	Specifies the port of the EIP. This parameter is available if you select Specific port for Port Type . The value ranges from 1 to 65535. The value can be a single port number or a port range, for example, 80 or 80-100.
Private IP Address	Specifies 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	Specifies 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. The value can be a single port number or a port range, for example, 80 or 80-100.
Description	Provides supplementary information about the DNAT rule. The description can contain a maximum of 255 characters.

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

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 for external networks.

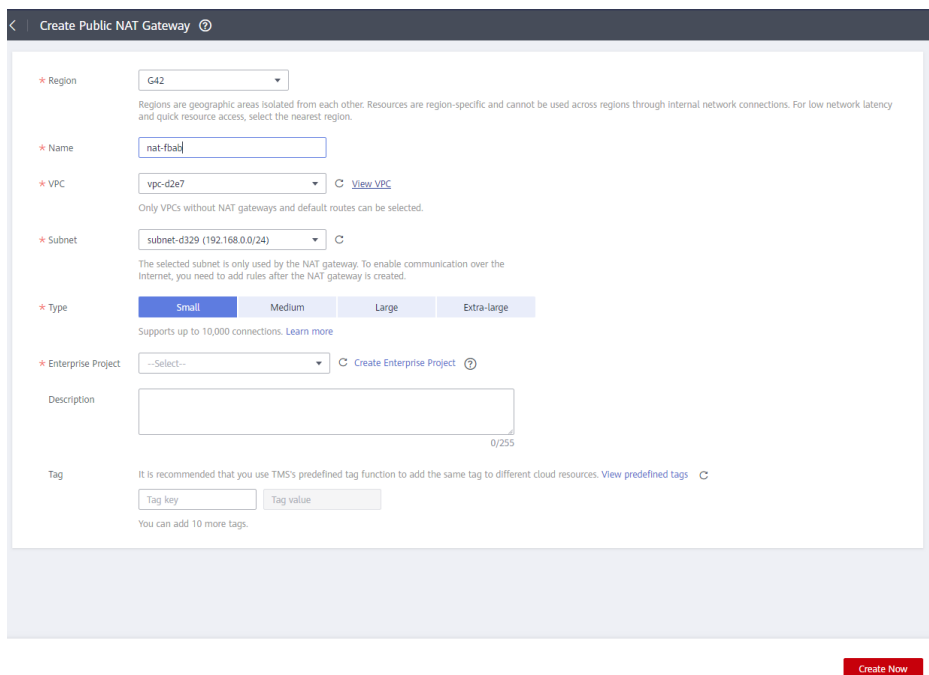
Prerequisites

- 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**, click **NAT Gateway**.
3. On the displayed page, click **Create Public NAT Gateway**.

Figure 3-1 Create Public NAT Gateway



4. Set the parameters as prompted. For details, see [Table 3-1](#).

Table 3-1 Parameter description

Parameter	Description
Region	Specifies the region where the NAT gateway is located.
Name	Specifies the name of the NAT gateway. The value is a string of 1 to 64 characters consisting of digits, letters, underscores (_), and hyphens (-).
VPC	Specifies the VPC to which the NAT gateway belongs. 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	Specifies the subnet of the VPC to which the NAT gateway belongs. 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	Specifies the type of the NAT gateway. The value can be Small , Medium , Large , and Extra-large . You can click Learn more on the page to view details about each type.

Parameter	Description
Enterprise Project	Specifies the enterprise project to which the NAT gateway belongs. 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, the default enterprise project will be used.
Description	Provides supplementary information about the NAT gateway. The description can contain a maximum of 255 characters.

5. Click **Create Now**. The page for you to confirm the NAT gateway specifications is displayed.
6. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a NAT gateway.
7. On the **NAT Gateway** homepage, check 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**, click **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 guides you on how to modify the name, type, or description of a NAT gateway.

The increase of the NAT gateway type does not affect service running. If you decrease the NAT gateway type, ensure that the NAT gateway type can meet your service requirements after the decrease.

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, click **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.

Figure 3-2 Modify NAT Gateway

Modify Specifications

Current Configuration			
NAT Gateway Name	nat-b188	Region	G42
ID	87e286f8-91b3-4d09-8208-1f603c2c7577	Type	Small
Description	--		

* Name

* Type Small Medium Large Extra-large

Supports up to 10,000 connections. [Learn more](#)

Description

0/255

5. Click **Next**.
6. Click **Submit**.

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**, click **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 the NAT gateway is created, you need to 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 one or more EIPs.

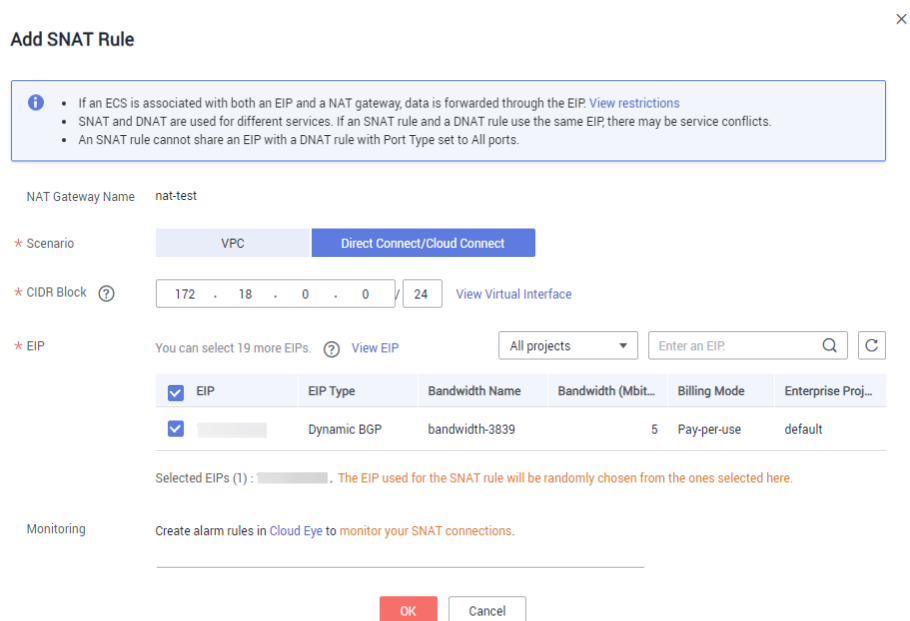
Prerequisites

- A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, click **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**.

Figure 4-1 Add SNAT Rule



5. Specify the parameters as prompted. For details, see [Table 4-1](#).

Table 4-1 Parameter description

Parameter	Condition	Description
Scenario	N/A	Specifies the scenarios in which the SNAT rule is used. Select VPC when your servers in a VPC need to access the Internet. Select Direct Connect when the servers that are connected to a VPC through Direct Connect or VPN in your data center need to access the Internet.
Type	This parameter is available when you select VPC for Scenario .	You can set it to Subnet or Custom based on service requirements. Select Subnet when all servers in a VPC subnet need to access the Internet through the SNAT rule. Select Custom when specific servers in a VPC subnet need to access the Internet through the SNAT rule.
Subnet	This parameter is available when you select VPC for Scenario , and Subnet for Type .	Specifies the subnet in which servers can access the Internet through the SNAT rule.

Parameter	Condition	Description
EIP	<ul style="list-style-type: none"> This parameter is available when you select VPC for Scenario. This parameter is available when you select Direct Connect for Scenario. 	<p>Specifies the EIP used for accessing the Internet.</p> <p>You can only select an EIP that has not been bound, 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 a time. A maximum of 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>
CIDR Block	<ul style="list-style-type: none"> This parameter is available when you select VPC for Scenario, and Custom for Type. This parameter is available when you select Direct Connect for Scenario. 	<p>In the VPC scenario, specify a VPC subnet to enable the servers whose IP addresses in that subnet to access the Internet through the SNAT rule.</p> <p>In the 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	<p>Create alarm rules in Cloud Eye.</p> <p>The alarm rules help you monitor your SNAT connections in a timely manner.</p>
Description	N/A	<p>Provides supplementary information about the NAT gateway. The description can contain a maximum of 255 characters.</p>

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**, click **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**, click **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 target SNAT rule to be modified.
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**, click **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.

Figure 4-2 Deleting an SNAT Rule

The screenshot shows the 'SNAT Rules' management page. At the top, there are tabs for 'SNAT Rules' and 'DNAT Rules'. Below the tabs, there is a search bar labeled 'Subnet name' and a search icon. A table lists the SNAT rules with the following columns: ID, Status, Scenario, CIDR Block, EIP, Description, Added, and Operation. The first row contains the following data: ID: 9ff4d790-6b9d-4afd-9d02-aba01..., Status: Running (with a green checkmark icon), Scenario: VPC, CIDR Block: 192.168.10.0/24 subnet-01, EIP: (with a question mark icon), Description: --, Added: Dec 11, 2019 09:49:15 GMT+08:..., and Operation: Modify, Delete (with the 'Delete' button highlighted in red).

ID	Status	Scenario	CIDR Block	EIP	Description	Added	Operation
9ff4d790-6b9d-4afd-9d02-aba01...	Running	VPC	192.168.10.0/24 subnet-01		--	Dec 11, 2019 09:49:15 GMT+08:...	Modify Delete

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

Prerequisites

A NAT gateway has been created.

Procedure

1. Log in to the management console.
2. Under **Network**, click **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**.

Figure 5-1 Add DNAT Rule

Add DNAT Rule
×

Info

- If your ECS has an EIP bound, you do not need to add a DNAT rule. If you do, the forwarded DNAT packets may be interrupted. [View restrictions](#)
- You need to add security group rules to allow inbound or outbound traffic after you add a DNAT rule. [Manage security group rules](#)
- SNAT and DNAT are used for different services. If an SNAT rule and a DNAT rule use the same EIP, there may be service conflicts. An SNAT rule cannot share an EIP with a DNAT rule with Port Type set to All ports.

NAT Gateway Name: nat-1121

★ Scenario: VPC Direct Connect/Cloud Connect

★ Port Type: Specific port All ports

★ Protocol: TCP

★ EIP ?: (5 Mbit/s | Pay-per-use | default) C View EIP

Bandwidth: 5 Mbit/s Billing Mode: Pay-per-use
Enterprise Project: default

★ Outside Port ?:

★ Private IP Address: View ECS IP Address

★ Inside Port ?:

OK
Cancel

NOTICE

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

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

Table 5-1 Parameter description

Parameter	Description
Scenario	<p>VPC: indicates that the servers in a VPC can share one EIP to provide services accessible from the Internet through the DNAT rule.</p> <p>Direct Connect: indicates that 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>

Parameter	Description
Port Type	<p>Specifies the port type, including All ports and Specific port.</p> <ul style="list-style-type: none"> • All ports: indicates the IP mapping method. This method 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: indicates the port mapping method. The NAT gateway forwards the requests with 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>Specifies the EIP that will be used by the server to provide services accessible from the Internet.</p> <p>You can only select an EIP that has not been bound, 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>Specifies 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>The value can be 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 the 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 the Direct Connect scenario, set this parameter to 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.
Inside Port	<p>Specifies the port of the server that provides services for 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.</p> <p>The value can be a single port number or a port range, for example, 80 or 80-100.</p>

Parameter	Description
Description	Provides supplementary information about the DNAT rule. The description can contain a maximum of 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**, click **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.
- Under **Network**, click **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.
- 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.

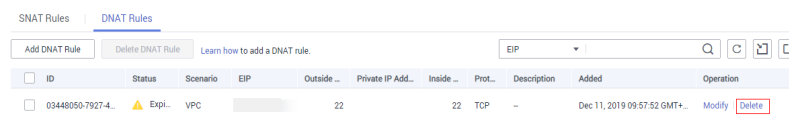
Prerequisites

A DNAT rule has been added for the NAT gateway.

Procedure

1. Log in to the management console.
2. Under **Network**, 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, locate the row that contains the target DNAT rule and click **Delete** in the **Operation** column.

Figure 5-2 Deleting a DNAT rule



ID	Status	Scenario	EIP	Outside ...	Private IP Add...	Inside ...	Prot...	Description	Added	Operation
03448050-7927-4...	▲ Expi...	VPC		22		22	TCP	-	Dec 11, 2019 09:57:52 GMT+	Modify Delete

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**.

- 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, you need to create multiple DNAT rules.

Prerequisites

A NAT gateway has been created.

Procedure

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

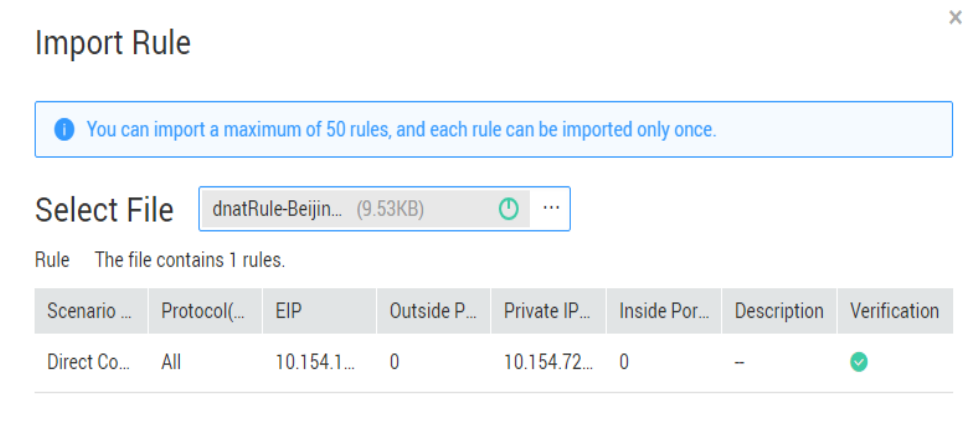
Table 5-2 Parameter description

Parameter	Description
Scenario	<p>VPC: indicates that the servers in a VPC can share one EIP to provide services accessible from the Internet through the DNAT rule.</p> <p>Direct Connect: indicates that 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>

Parameter	Description
Port Type	<p>Specifies the port type, including All ports and Specific port.</p> <ul style="list-style-type: none"> • All ports: indicates the IP mapping method. This method 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: indicates the port mapping method. The NAT gateway forwards the requests with 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>Specifies the EIP that will be used by the server to provide services accessible from the Internet.</p> <p>Only EIPs that have not been bound or that have been bound to a DNAT rule in the current VPC are available for selection.</p>
Outside Port	<p>Specifies the EIP port. This parameter is available if you select Specific port for Port Type.</p> <p>The value can be 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 the 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 the 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 the VPC scenario, set this parameter to the port of the server in a VPC. • In the 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. <p>The number of inside and outside ports must match.</p>

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

Figure 5-3 Import Rule



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

6 Monitoring Management

6.1 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

Monitoring Metrics

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
snat_connection	SNAT connections	Specifies the number of SNAT connections of the measurement object. Unit: Count	≥ 0	Measurement object: Active NAT gateway node Dimension: nat_gateway_id	1 minute

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
snat_connection	Monitoring Details of Top 20	Specifies the IP addresses of top 20 servers that occupy the largest number of SNAT connections. Unit: Count	≥ 0	Measurement object: NAT gateway Dimension: nat_gateway_id	1 minute
inbound_bandwidth	Inbound bandwidth	Specifies the inbound bandwidth of servers using the SNAT function. Unit: bit/s	≥ 0 bit/s	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute
inbound_bandwidth	Monitoring Details of Top 20	Specifies the IP addresses of top 20 servers using the SNAT function that occupy the most inbound bandwidth. Unit: bit/s	≥ 0 bit/s	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_bandwidth	Outbound bandwidth	Specifies the outbound bandwidth of servers using the SNAT function. Unit: bit/s	≥ 0 bit/s	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
outbound_bandwidth	Monitoring Details of Top 20	Specifies the IP addresses of top 20 servers using the SNAT function that occupy the most outbound bandwidth. Unit: bit/s	≥ 0 bit/s	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute
inbound_pps	Inbound PPS	Specifies the inbound PPS of servers using the SNAT function. Unit: Count	≥ 0	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute
inbound_pps	Monitoring Details of Top 20	Specifies the IP addresses of top 20 servers using the SNAT function that occupy the most inbound PPS. Unit: Count	≥ 0	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_pps	Outbound PPS	Specifies the outbound PPS of servers using the SNAT function. Unit: Count	≥ 0	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
outbound_pps	Monitoring Details of Top 20	Specifies the IP addresses of top 20 servers using the SNAT function that occupy the most outbound PPS. Unit: Count	≥ 0	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute
inbound_traffic	Inbound traffic	Specifies the inbound traffic of servers using the SNAT function. Unit: byte	≥0 bytes	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute
inbound_traffic	Monitoring Details of Top 20	Specifies the IP addresses of top 20 servers using the SNAT function that occupy the most inbound traffic. Unit: byte	≥0 bytes	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute
outbound_traffic	Outbound traffic	Specifies the outbound traffic of servers using the SNAT function. Unit: byte	≥0 bytes	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute

Metric	Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
outbound_traffic	Monitoring Details of Top 20	Specifies the IP addresses of top 20 servers using the SNAT function that occupy the most outbound traffic. Unit: byte	≥0 bytes	Measurement object: NAT gateway and servers using the SNAT function Dimension: nat_gateway_id	1 minute

Dimensions

Key	Value
nat_gateway_id	NAT gateway ID

6.2 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**, click **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. 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*.

6.3 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

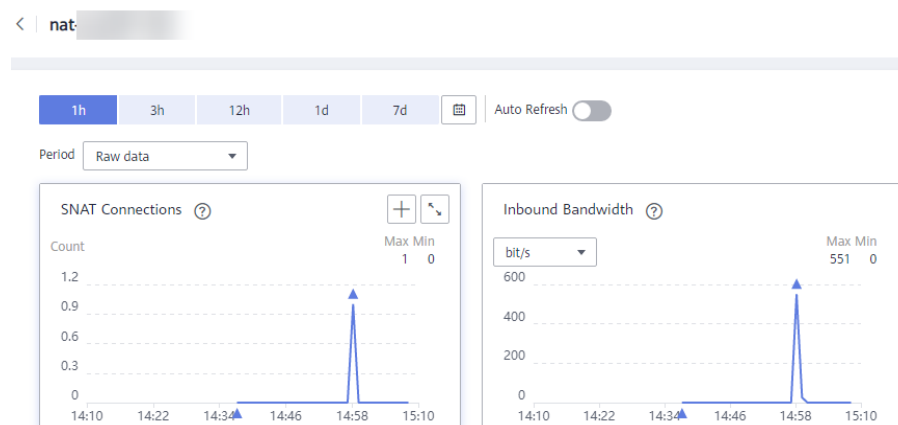
This section describes how to view NAT Gateway metrics.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, click **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.

Figure 6-1 Viewing metrics



7 FAQs

7.1 NAT Gateway

7.1.1 What Is the Relationship Between 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.

7.1.2 How Does A NAT Gateway Offer High Availability?

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

7.1.3 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	Port Not Supported
TCP	42, 135, 137, 138, 139, 444, 445, 593, 1025, 1068, 1434, 3127, 3128, 3129, 3130, 4444, 4789, 5554, 5800, 5900, and 9996
UDP	135 to 139, 1026, 1027, 1028, 1068, 1433, 1434, 4789, 5554, and 9996

7.1.4 What Can 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 not set the VPC route table correctly. 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.

7.1.5 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.



7.1.6 What Is the Quota of the NAT Gateway?

What Is the Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users. For example, the quota can limit the maximum number of EIPs that can be associated with an SNAT rule. You can apply for increasing quotas if necessary.

This section describes how to view the used NAT Gateway quota and the total NAT Gateway quota in a specified region.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click  .
The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

The system does not support online quota adjustment. If you need to adjust a quota, call the hotline or send an email to the customer service mailbox. Customer service personnel will timely process your request for quota adjustment and inform you of the real-time progress by making a call or sending an email.

Before dialing the hotline number or sending an email, make sure that the following information has been obtained:

- Account name, project name, and project ID, which can be obtained by performing the following operations:
Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the account name, project name, and project ID on the **My Credentials** page.
- Quota information, which includes:
 - Service name
 - Quota type
 - Required quota

If you need to adjust a quota, contact the administrator.

7.2 SNAT

7.2.1 Why SNAT Is 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 for a virtual environment. Therefore, enabling multiple ECSs to share one public IP address is a preferable and more feasible method. This can be done using SNAT.

7.2.2 What Are SNAT Connections?

An SNAT connection consists of the source IP address, source port, destination IP address, destination port, and transmission-layer protocol. With these five elements, a connection can be distinguished as a unique session. The source IP address and source port are the EIP and port translated by SNAT to access the destination IP address and port of a public network.

SNAT supports three protocols: TCP, UDP, and ICMP. NAT Gateway supports a maximum of 55000 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, connections cannot be created.

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, you need to initiate more data packets or use TCP to maintain connections. In addition, to prevent service interruption caused by insufficient connections, you are advised to use Cloud Eye to monitor the number of SNAT connections and set proper alarms.

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

The SNAT function of NAT Gateway 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 EIP bandwidth you created.

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

If packet loss or connection failure occurs on the 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 the specification limit of the NAT gateway, packet loss or connection failure occurs. If the number of connections exceeds the upper limit, modify the NAT gateway specifications.

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

When creating an SNAT rule with **Scenario** set to **Direct Connect**, you need to 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.

7.3 DNAT

7.3.1 Why DNAT Is Used?

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

7.3.2 Does the DNAT Rule Support the Update Operation?

No.

7.3.3 What Can 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 need to delete the rules and reconfigure them.

A Change History

Released On	Description
2020-07-30	This issue is the first official release.