

NAT Gateway

User Guide

Issue 01
Date 2025-01-10



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property 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 Cloud 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 Service Overview.....	1
1.1 What Is NAT Gateway?.....	1
1.2 NAT Gateway Advantages.....	4
1.3 Application Scenarios.....	5
1.4 NAT Gateway Specifications.....	9
1.5 Notes and Constraints.....	10
1.6 Permissions Management.....	11
1.7 Region and AZ.....	15
1.8 Basic Concepts.....	16
2 Getting Started.....	17
2.1 Using a Public NAT Gateway to Enable Servers to Share One or More EIPs to Access the Internet.....	17
2.2 Using a Public NAT Gateway to Enable Servers to Be Accessed by the Internet.....	21
2.3 Using a Private NAT Gateway to Connect Cloud and On-premises Networks.....	26
3 Public NAT Gateways.....	32
3.1 Overview of Public NAT Gateways.....	32
3.2 Creating a Public NAT Gateway.....	33
3.3 Managing Public NAT Gateways.....	35
3.4 Managing SNAT Rules.....	36
3.4.1 Adding an SNAT Rule.....	36
3.4.2 Modifying an SNAT Rule.....	38
3.4.3 Deleting an SNAT Rule.....	38
3.5 Managing DNAT Rules.....	38
3.5.1 Adding a DNAT Rule.....	38
3.5.2 Modifying a DNAT Rule.....	41
3.5.3 Deleting a DNAT Rule.....	41
3.5.4 Deleting DNAT Rules in Batches.....	42
3.5.5 Importing DNAT Rules by Using a Template and Exporting DNAT Rules	42
4 Private NAT Gateways.....	45
4.1 Overview of Private NAT Gateways.....	45
4.2 Creating a Private NAT Gateway.....	48
4.3 Managing Private NAT Gateways.....	50
4.4 Managing SNAT Rules.....	50

4.4.1 Adding an SNAT Rule.....	50
4.4.2 Modifying an SNAT Rule.....	52
4.4.3 Deleting an SNAT Rule.....	52
4.5 Managing DNAT Rules.....	52
4.5.1 Adding a DNAT Rule.....	52
4.5.2 Modifying a DNAT Rule.....	55
4.5.3 Deleting a DNAT Rule.....	55
4.6 Managing Transit IP Addresses.....	55
4.6.1 Assigning a Transit IP Address.....	56
4.6.2 Viewing a Transit IP Address.....	56
4.6.3 Releasing a Transit IP Address.....	57
4.7 Accessing On-Premises Data Centers or Other VPCs.....	57
5 Permissions Management.....	58
5.1 Creating a User and Granting NAT Gateway Permissions.....	58
5.2 NAT Gateway Custom Policies.....	59
6 Monitoring.....	62
6.1 Supported Metrics.....	62
6.2 Creating Alarm Rules.....	66
6.3 Viewing Metrics.....	67
7 FAQs.....	68
7.1 Public NAT Gateways.....	68
7.1.1 What Is the Relationship Between a VPC, Public NAT Gateway, EIP Bandwidth, and ECS?.....	68
7.1.2 How Does a Public NAT Gateway Offer High Availability?.....	68
7.2 Private NAT Gateways.....	68
7.2.1 How Do I Troubleshoot a Network Failure After a Private NAT Gateway Is Configured?.....	68
7.2.2 How Many Private NAT Gateways Can I Create in a VPC?.....	69
7.2.3 Can Private NAT Gateways Translate On-premises IP Addresses Connected to the Cloud Through Direct Connect?.....	69
7.2.4 What Are the Differences Between Private NAT Gateways and Public NAT Gateways?.....	69
7.2.5 Can a Private NAT Gateway Be Used Across Accounts?.....	70
7.3 SNAT Rules.....	70
7.3.1 Why Do I Need SNAT?.....	70
7.3.2 What Are SNAT Connections?.....	70
7.4 DNAT Rules.....	71
7.4.1 Why Do I Need DNAT?.....	71
7.4.2 Can I Modify DNAT Rules?.....	71
A Change History.....	72

1 Service Overview

1.1 What Is NAT Gateway?

NAT Gateway is a network address translation (NAT) service. It can be a public NAT gateway or a private NAT gateway.

Public NAT Gateways

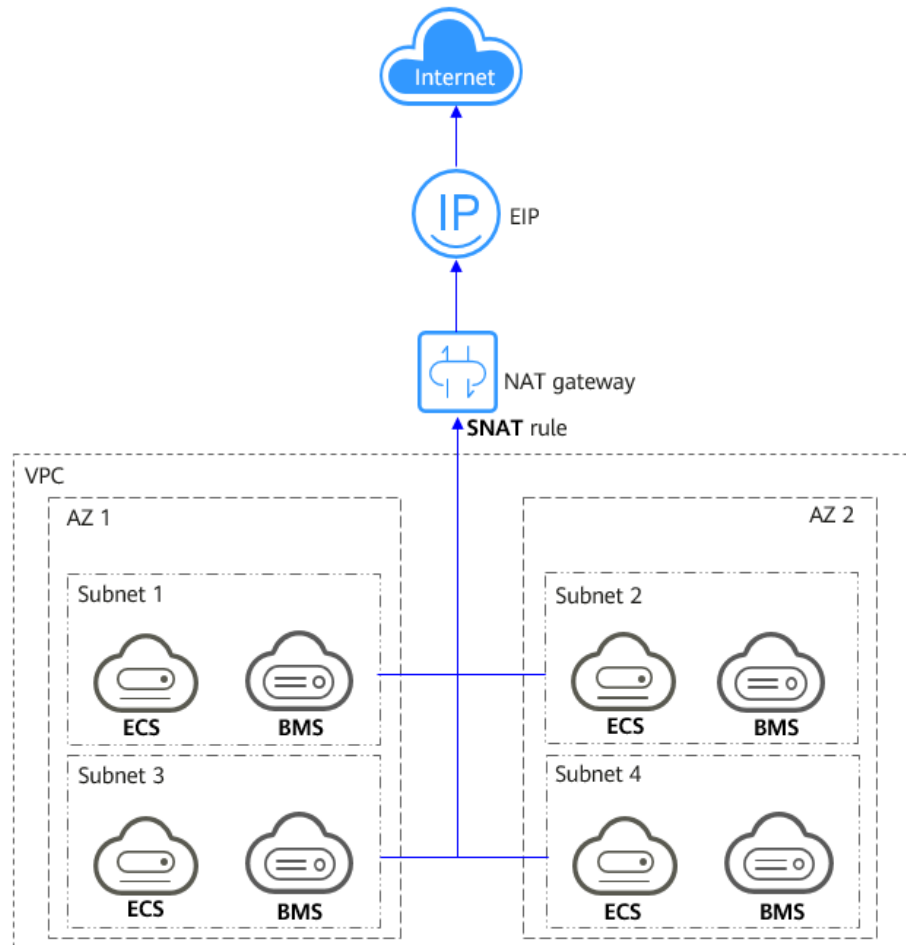
A public NAT gateway enables cloud and on-premises servers in a private subnet to share an EIP to access the Internet or provide services accessible from the Internet. Cloud servers are ECSs and BMSs in a VPC. On-premises servers are servers in on-premises data centers that connect to a VPC through Direct Connect or Virtual Private Network (VPN). A public NAT gateway supports up to 20 Gbit/s of bandwidth.

Public NAT gateways offer source NAT (SNAT) and destination NAT (DNAT).

- SNAT translates private IP addresses into EIPs so that traffic from a private network can go out to the Internet.

Figure 1-1 shows how an SNAT rule works.

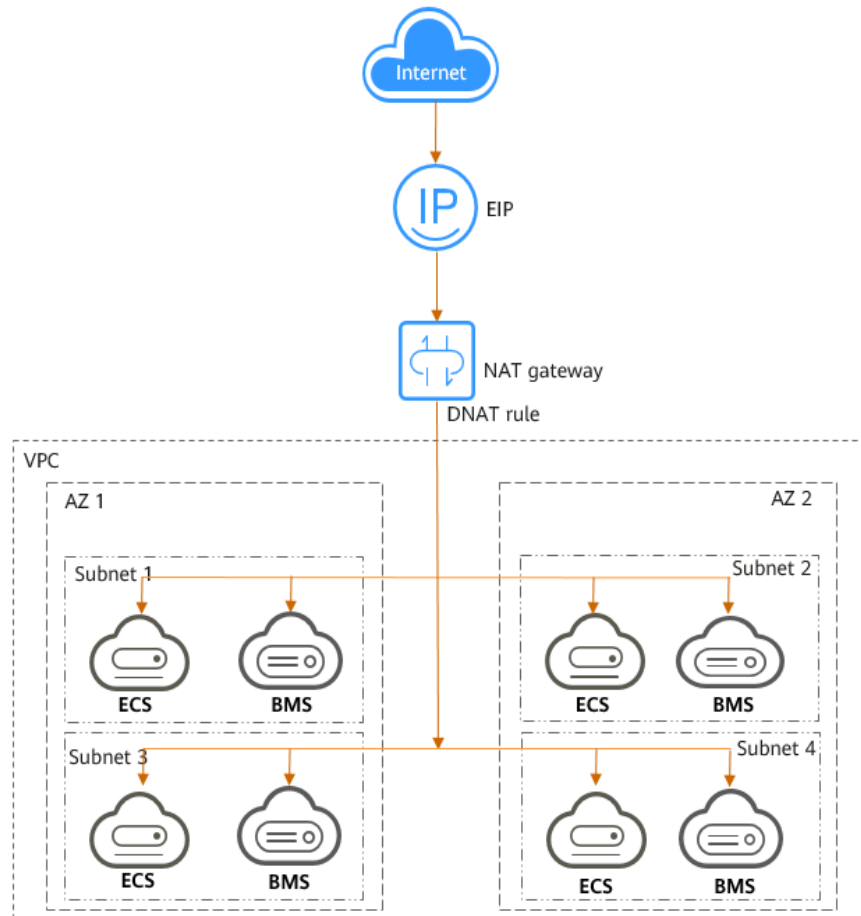
Figure 1-1 NAT gateway with an SNAT rule



- DNAT enables servers in a VPC, regardless of if they are in the same AZ, to share an EIP to provide services accessible from the Internet. With an EIP, a public NAT gateway forwards the Internet requests from only a specific port and over a specific protocol to a specific port of a server, or it can forward all requests to the server regardless of which port they originated on.

Figure 1-2 shows how a DNAT rule works.

Figure 1-2 NAT gateway with a DNAT rule



Private NAT Gateways

Private NAT gateways provide network address translation, allowing ECSs and BMSs in a VPC to communicate with servers in other VPCs or on-premises data centers. You can configure SNAT and DNAT rules for a NAT gateway to translate the source and destination IP addresses of originating packets into a transit IP address.

Specifically,

- SNAT enables servers in a VPC, regardless of if they are in the same AZ, to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers in a VPC, regardless of if they are in the same AZ, to share the same transit IP address to provide services accessible from on-premises data centers or other VPCs.

Transit Subnet

A transit subnet is a transit network and is the subnet to which the transit IP address belongs.

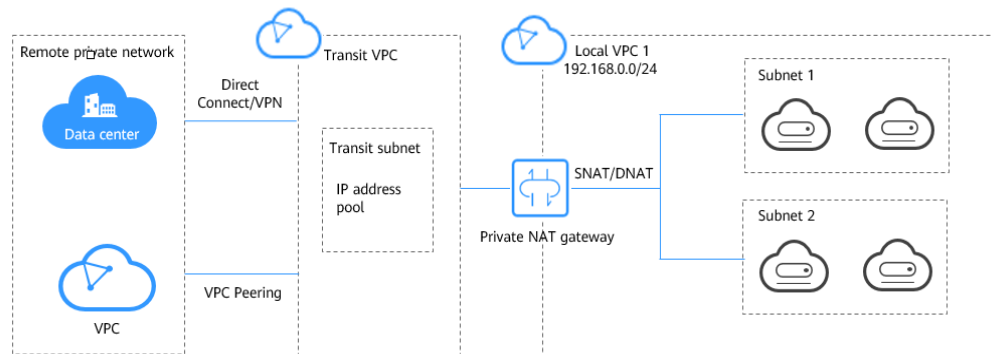
Transit IP Address

A transit IP address is a private IP address that can be assigned from a transit subnet. Cloud servers in your VPC can share a transit IP address to access on-premises networks or other VPCs.

Transit VPC

A transit VPC is where a transit subnet belongs to.

Figure 1-3 Private NAT gateway



How Do I Access the NAT Gateway Service?

You can access the NAT Gateway service through the management console or using HTTPS-based APIs.

- **Management console**
Log in to the management console and choose **NAT Gateway** from the service list.
- **APIs**
If you need to integrate NAT Gateway on the cloud platform into your own system, use APIs to access NAT Gateway.

1.2 NAT Gateway Advantages

Advantages of Public NAT Gateways

- **Flexible deployment**
A NAT gateway can be shared across subnets and AZs, so that even if an AZ fails, the public NAT gateway can still run normally in another AZ. The specifications and EIP of a public NAT gateway can be changed at any time.
- **Ease of use**
Multiple NAT gateway specifications are available. Public NAT gateway configuration is simple, the operation & maintenance is easy, and they can be provisioned quickly. Once provisioned, they can run stably.
- **Cost-effectiveness**
Servers can share one EIP to connect to the Internet. You no longer need to configure one EIP for each server, which saves money on EIPs and bandwidth.

Advantages of Private NAT Gateways

- **Easier network planning**

Different departments in a large enterprise may have overlapping CIDR blocks, so the enterprise has to replan its network before migrating their workloads to the cloud. The replanning is time-consuming and stressful. The private NAT gateway eliminates the need to replan the network so that customers can retain their original network while migrating to the cloud.
- **Easy operation & maintenance**

Departments of a large enterprise usually have hierarchical networks for hierarchical organizations, rights- and domain-based management, and security isolation. Such hierarchical networks need to be mapped to a large-scale network for enabling communication between them. A private NAT gateway can map the CIDR block of each department to the same VPC CIDR block, which simplifies the management of complex networks.
- **Strong security**

Departments of an enterprise may need different levels of security. Private NAT gateways can expose the IP addresses and ports of only specified CIDR blocks to meet high security requirements. An industry regulation agency may require other organizations to use a specified IP address to access their regulation system. Private NAT gateways can help meet this requirement by mapping private IP addresses to that specified IP address.
- **Zero IP conflicts**

Isolated services of multiple departments usually use IP addresses from the same private CIDR block. After the enterprise migrates workloads to the cloud, IP address conflicts occur. Thanks to IP address mapping, the private NAT gateways allow for communication between overlapping CIDR blocks.

1.3 Application Scenarios

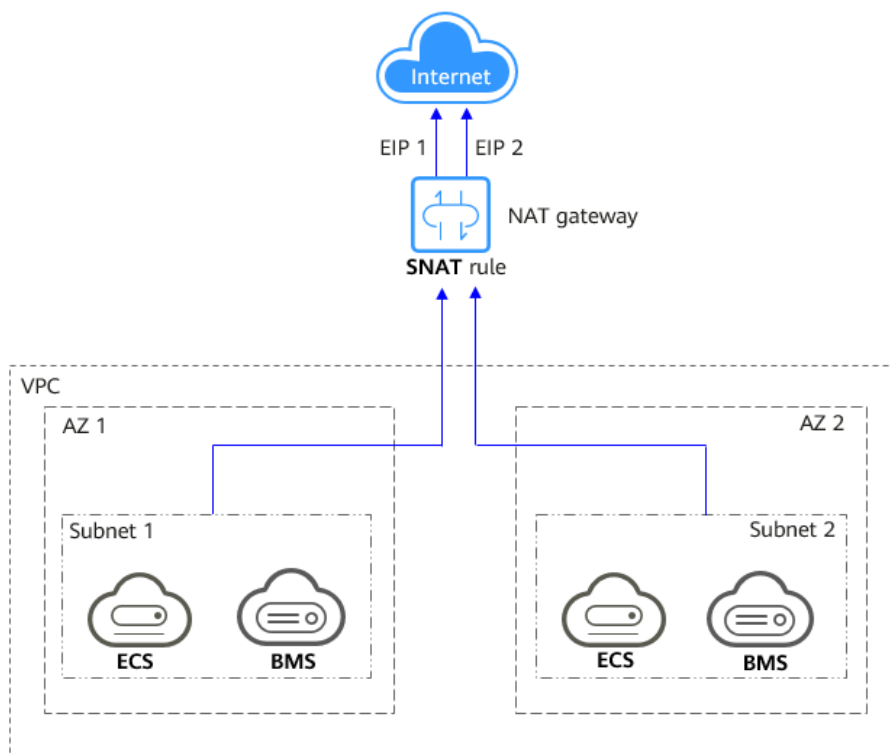
Public NAT Gateway

- **Allowing a private network to access the Internet using SNAT**

If your servers in a VPC need to access the Internet, you can configure SNAT rules to let these servers use EIPs to access the Internet without exposing their private IP addresses. You can configure only one SNAT rule for each subnet in a VPC and select one or more EIPs for each SNAT rule. Public NAT Gateway provides different numbers of connections, and you can create multiple SNAT rules to meet your service requirements.

Figure 1-4 shows how servers in a VPC access the Internet using SNAT.

Figure 1-4 Allowing a private network to access the Internet using SNAT



- **Allowing Internet users to access a service in a private network using DNAT**

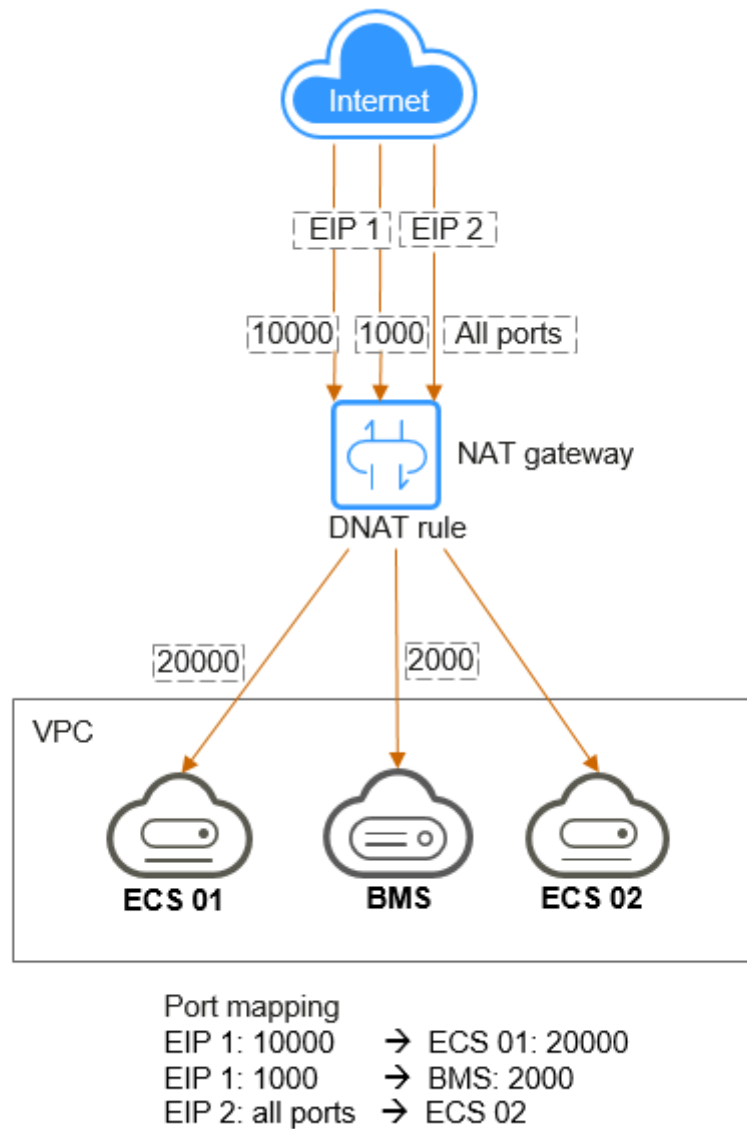
DNAT rules enable servers in a VPC to provide services accessible from the Internet.

After receiving requests from a specific port over a specific protocol, the public NAT gateway can forward the requests to a specific port of a server through port mapping. The public NAT gateway can also forward all requests destined for an EIP to a specific server through IP address mapping.

One DNAT rule can be configured for each server. If there are multiple servers, you can create multiple DNAT rules to map one or more EIPs to the private IP addresses of these servers.

Figure 1-5 shows how servers (ECSs or BMSs) in a VPC provide services accessible from the Internet using DNAT.

Figure 1-5 Allowing Internet users to access a service in a private network using DNAT

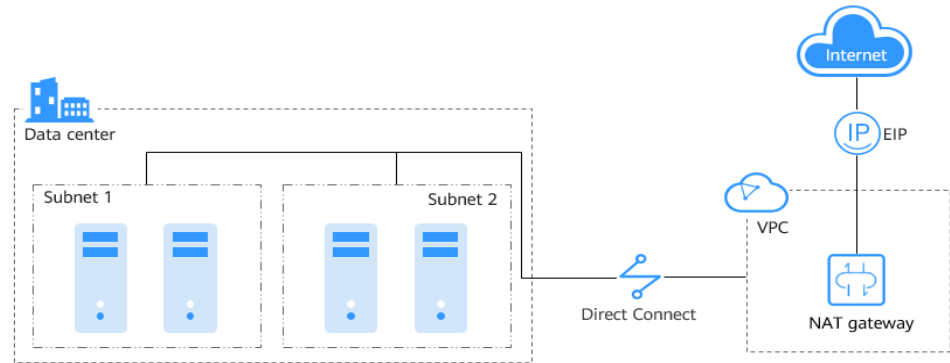


- **Allowing on-premises servers to communicate with the Internet**

In certain Internet, gaming, e-commerce, and financial scenarios, a large number of servers in a private cloud are connected to a VPC through Direct Connect or VPN. If such servers need secure, high-speed Internet access or need to provide services accessible from the Internet, you can deploy a NAT gateway and configure SNAT and DNAT rules to meet their requirements.

Figure 1-6 shows how to use SNAT and DNAT to provide high-speed Internet access or provide services accessible from the Internet.

Figure 1-6 Allowing on-premises servers to communicate with the Internet



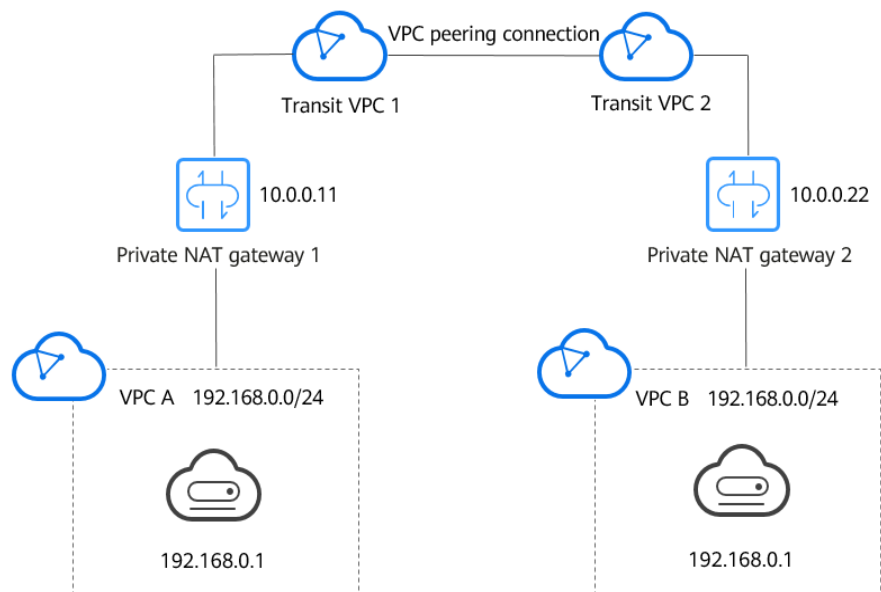
Private NAT Gateway

- **Connecting VPCs with overlapping CIDR blocks**

You can configure two private NAT gateways for two VPCs with overlapping CIDR blocks. Then, add SNAT and DNAT rules on the two private NAT gateways to enable servers in the two VPCs to use the transit IP addresses to communicate with each other.

In the following figure, there are two transit VPCs and two private NAT gateways. Address 192.168.0.1 in VPC A is translated to 10.0.0.11, and the IP address 192.168.0.1 in VPC B is translated to 10.0.0.22. A VPC peering connection can then be established between the two transit VPCs to enable communication between them.

Figure 1-7 Connecting VPCs with overlapping CIDR blocks



- **Keeping the network topology while migrating workloads to the cloud, or accessing regulatory agencies from specific IP addresses**

Organizations may want to migrate their workloads to the cloud without making any changes to their existing network topology. They may also have to access regulatory agencies from specific IP addresses as required by these agencies. A private NAT gateway is a good choice.

The following figure represents an enterprise network where the subnets of different departments overlap. A private NAT gateway allows the enterprise to keep the existing network topology unchanged while migrating their workloads to the cloud. In this example, the private NAT gateway maps the IP address of each department to 10.0.0.33 so that each department can use 10.0.0.33 to securely access the regulatory agency.

1.4 NAT Gateway Specifications

The NAT gateway performance is determined by the maximum number of SNAT connections supported.

Public NAT Gateway

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address is the EIP, and the source port is the EIP port. An SNAT connection uniquely identifies a session.

Throughput is the total bandwidth of all EIPs in DNAT rules. For example, a public NAT gateway has two DNAT rules. The EIP bandwidth in the first DNAT rule is 10 Mbit/s, and that in the second DNAT rule is 5 Mbit/s. The throughput of the public NAT gateway will be 15 Mbit/s.

Select a public NAT gateway based on your service requirements. [Table 1-1](#) lists the public NAT gateway specifications.

Table 1-1 Public NAT gateway specifications

Specifications	SNAT Connections	Bandwidth	Queries Per Second (QPS)
Small	10,000	20 Gbit/s	10,000
Medium	50,000	20 Gbit/s	10,000
Large	200,000	20 Gbit/s	10,000
Extra-large	1,000,000	20 Gbit/s	10,000

NOTE

- The PPS of different NAT gateway specifications is the total PPS in both inbound and outbound directions.
- If the number of requests exceeds the maximum allowed connections of a public NAT gateway, services will be adversely affected. To avoid this situation, create alarm rules on the Cloud Eye console to monitor the number of SNAT connections.

Private NAT Gateway

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address is the transit IP address, and the source port is the port of the transit IP address.

Select a private NAT gateway based on your service requirements. [Table 1-2](#) lists the private NAT gateway specifications.

Table 1-2 Private NAT gateway specifications

Specifications	SNAT Connections	Bandwidth	QPS
Small	2,000	200 Mbit/s	6000
Medium	5,000	500 Mbit/s	9000
Large	20,000	2 Gbit/s	10,000
Extra-large	50,000	5 Gbit/s	10,000

NOTE

If the number of requests exceeds the maximum allowed connections of a private NAT gateway, services will be adversely affected. To avoid this situation, create alarm rules on the Cloud Eye console to monitor the number of SNAT connections.

1.5 Notes and Constraints

Public NAT Gateway

When using a public NAT gateway, note the following:

- Common restrictions
 - Rules on one public NAT gateway can use the same EIP, but rules on different NAT gateways must use different EIPs.
 - Each VPC can be associated with multiple public NAT gateways.
 - SNAT and DNAT rules can use the same EIP to save resources. However, when **Port Type** of a DNAT rule is set to **All ports**, the resource in the DNAT rule will preferentially use all ports of the EIP. So an SNAT rule cannot share an EIP with such a DNAT rule.
 - If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.
 - NAT Gateway supports TCP, UDP, and ICMP, but does not support application layer gateway (ALG)-related technologies. In addition, NAT Gateway does not support Encapsulating Security Payload (ESP) and Authentication Header (AH) used by Generic Routing Encapsulation (GRE) tunnels and Internet Protocol Security (IPsec). This is determined by the features of NAT Gateway.

- SNAT restrictions
 - Only one SNAT rule can be added for each VPC subnet.
 - When you add an SNAT rule in the VPC scenario, the custom CIDR block must be a subset of the NAT gateway's VPC subnets.
 - If an SNAT 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.
 - There is no limit on the number of SNAT rules that can be added on a public NAT gateway.
- DNAT restrictions
 - Only one DNAT rule can be configured for each port on a server. One port can be mapped to only one EIP.
 - A maximum of 200 DNAT rules can be added on a public NAT gateway.

Private NAT Gateway

When using a private NAT gateway, note the following:

- Common restrictions
 - Manually add routes in a VPC to connect it to a remote private network through a VPC peering connection, Direct Connect, or VPN connection.
 - The transit IP address and destination IP address cannot be in the same VPC.
 - SNAT and DNAT rules cannot share a transit IP address.
 - The total number of DNAT and SNAT rules that can be added on a private NAT gateway varies with the private NAT gateway specifications.
 - Small: 20 or less
 - Medium: 50 or less
 - Large: 200 or less
 - Extra-large: 500 or less
- SNAT restrictions
 - Only one SNAT rule can be added for each VPC subnet.
- DNAT restrictions
 - A DNAT rule with **Port Type** set to **All ports** cannot share a transit IP address with a DNAT rule with **Port Type** set to **Specific port**.

1.6 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.

With IAM, you can create IAM users and assign permissions to control their access to specific resources. 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, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see *Identity and Access Management User Guide*.

NAT Gateway Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

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. Cloud services depend on each other. 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 more secure access control. For example, the account administrator can grant users only permission to manage 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
NAT FullAccess	All operations on NAT Gateway resources.	System-defined policy
NAT ReadOnlyAccess	Read-only permissions for all NAT Gateway resources.	System-defined policy
NAT Administrator	All operations on NAT Gateway resources. To be granted this permission, users must also have the Tenant Guest permissions.	System-defined role

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	√
Creating a transit subnet	√	x	√
Querying transit subnets	√	√	√

Operation	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Querying details of a transit subnet	√	√	√
Modifying a transit subnet	√	x	√
Deleting a transit subnet	√	x	√
Assigning a transit IP address	√	x	√
Querying a transit IP address	√	√	√
Releasing a transit IP address	√	x	√

 NOTE

- Note the following when creating a DNAT rule:
 - If you set **Instance Type** to **Server** and select an ECS, you also need to obtain the **ECS ReadOnlyAccess** permissions or the fine-grained permissions for actions **ecs:cloudServers:get** and **ecs:cloudServers:list**. For details, see the *Elastic Cloud Server API Reference*.
 - If you set **Instance Type** to **Server** and select a BMS, you also need to obtain the **BMS ReadOnlyAccess** permissions or the fine-grained permissions for actions **bms:servers:get** and **bms:servers:list**. For details, see the *Bare Metal Server API Reference*.
 - If you create a DNAT rule on a private NAT gateway and select **Load balancer** for **Instance Type**, you need to obtain the **ELB ReadOnlyAccess** permissions or the fine-grained permissions for actions **elb:loadbalancers:get** and **elb:loadbalancers:list**. For details, see the *Elastic Load Balance API Reference*.
 - After a DNAT rule is created, add a security group rule to allow the Internet to access servers for which the DNAT rule is configured. Otherwise, the DNAT rule does not take effect. Obtain the **VPC FullAccess** permissions or the fine-grained permissions for action **vpc:securityGroups:create** by referring to the *Virtual Private Cloud API Reference*.
- To view metrics, obtain the **CES ReadOnlyAccess** permissions. For details, see the *Cloud Eye API Reference*.
- To view access logs, obtain the **LTS ReadOnlyAccess** permissions. For details, see the *Log Tank Service API Reference*.

1.7 Region and AZ

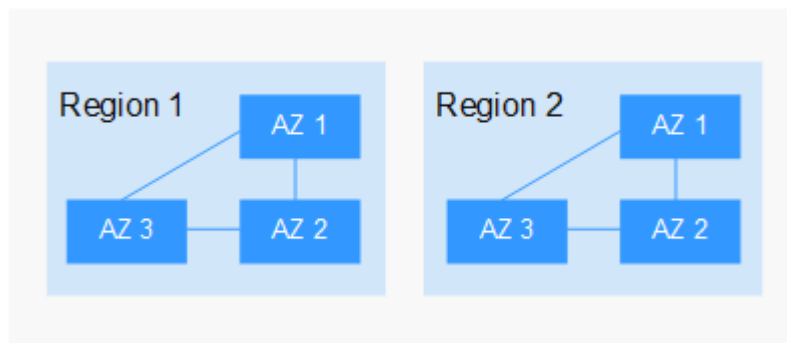
Concept

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 one AZ will not affect others.

Figure 1-8 shows the relationship between regions and AZs.

Figure 1-8 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](#).

1.8 Basic Concepts

EIP

An EIP is a static, public IP address.

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.

You can bind an EIP to an ECS in your subnet to enable the ECS to communicate with the Internet.

Each EIP can be used by only one ECS at a time. To enable servers in a VPC, regardless of if they are in the same AZ, to share an EIP, use a public NAT gateway.

SNAT Connections

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address and port are the IP address and port translated by SNAT. An SNAT connection uniquely identifies a session.

DNAT Connections

DNAT connections enable servers in a private network, regardless of if they are in the same AZ, to share an EIP to provide services accessible from the Internet.

2 Getting Started

2.1 Using a Public NAT Gateway to Enable Servers to Share One or More EIPs to Access the Internet

Scenarios

If servers without EIPs need to access the Internet, they can share one or more EIPs to access the Internet through a public NAT gateway. This helps save EIP resources and protect servers from exposing their IP addresses.

Operation Process

Procedure	Description
Step 1: Buy an EIP	Buy an EIP.
Step 2: Buy a Public NAT Gateway	Buy a public NAT gateway.
Step 3: Add an SNAT Rule	Add an SNAT rule for the public NAT gateway so that servers in specific CIDR blocks share the EIP you have assigned to access the Internet.
Step 4: Verify that the SNAT Rule Has Been Added	Check whether the SNAT rule has been added.
Step 5: Verify that Server Can Access the Internet Through the NAT Gateway	Verify that server in the CIDR block to which the SNAT rule is applied can access the Internet.

Step 1: Buy an EIP

1. On the **Assign EIP** page, set the EIP name to **EIP-A**.

You can configure other EIP parameters as required. For details, see .

Step 2: Buy a Public NAT Gateway

1. On the **Create Public NAT Gateway** page, configure required parameters.

Table 2-1 Descriptions of public NAT gateway parameters

Parameter	Example	Description
Region	CN North-Beijing4	The region where the public NAT gateway is located.
Specifications	Small	The specifications of the public NAT gateway. The value can be Extra-large , Large , Medium , or Small . To view more details about specifications, click Learn more on the page.
Name	public-nat-01	The name of the public NAT gateway. Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
VPC	vpc-A	The VPC that the public NAT gateway belongs to. The selected VPC cannot be changed after you create the public NAT gateway. NOTE To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.

Parameter	Example	Description
Subnet	Subnet-A01	The subnet that the public NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after you create the public NAT gateway. The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.
Advanced Settings (Optional)	-	Click the drop-down arrow to configure advanced parameters of the public NAT gateway.
SNAT Connection TCP Timeout (s)	900	The timeout period of a TCP connection established using the SNAT rule. If no data is exchanged within this period, the TCP connection will be closed. Value range: 40 to 7200
SNAT Connection UDP Timeout (s)	300	The timeout period of a UDP connection established using the SNAT rule. If no data is exchanged within this period, the UDP connection will be closed. Value range: 40 to 7200
SNAT Connection ICMP Timeout (s)	10	The timeout period of an ICMP connection established using the SNAT rule. If no data is exchanged within this period, the ICMP connection will be closed. Value range: 10 to 7200
TCP TIME_WAIT (s)	5	How long the side that actively closed the TCP connection is in the TIME_WAIT state. Value range: 0 to 1800
Description	Not required	Supplementary information about the public NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.
Tag	Not required	The identifier of the public NAT gateway. A tag is a key-value pair. You can add up to 20 tags to each public NAT gateway.

2. Click **Create Now**. On the page displayed, confirm the public NAT gateway specifications.
3. If you do not need to modify the information, click **Submit**.

On the **Public NAT Gateways** page, you can view the created public NAT gateway in the list.

Step 3: Add an SNAT Rule

1. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
2. On the **SNAT Rules** tab, click **Add SNAT Rule**.
3. Configure required parameters. [Table 2-2](#) describes the parameters.

Table 2-2 Descriptions of SNAT rule parameters

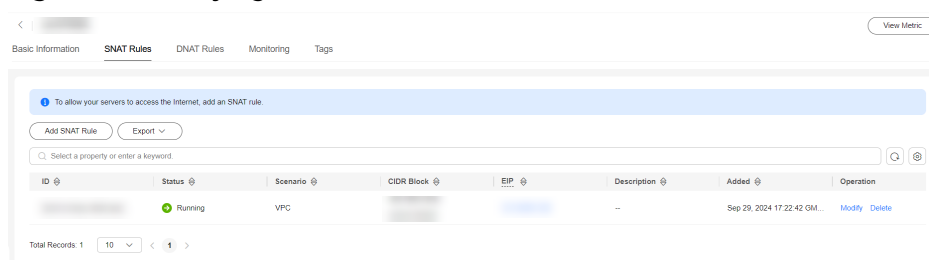
Parameter	Example	Description
Scenario	VPC	Select VPC if your servers in a VPC will use the SNAT rule to access the Internet. Different servers in a VPC can share the same EIP to access the Internet.
CIDR Block	Existing	The CIDR block is a subset of the NAT gateway's VPC subnets. Servers whose IP addresses in the CIDR block can access the Internet through the SNAT rule. Select a CIDR block from the drop-down list.
Public IP Address Type	EIP	The EIP used for accessing the Internet.
Monitoring	-	You can create alarm rules on the Cloud Eye console to monitor your SNAT connections and keep informed of any changes in a timely manner.
Description	Not required	Supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

4. Click **OK**.

Step 4: Verify that the SNAT Rule Has Been Added

1. In the **SNAT Rules** tab, view details of the SNAT rule.
If **Status** of the SNAT rule is **Running**, the SNAT rule has been created.

Figure 2-1 Verifying that the SNAT rule has been added



Step 5: Verify that Server Can Access the Internet Through the NAT Gateway

1. Log in to the server to be verified.
2. Verify that the server can access the Internet.

Figure 2-2 Verification result

```
[root@ecs-test-nat-20070007 ~]# TMOU=0
[root@ecs-test-nat-20070007 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=53.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=109 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=109 time=53.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=109 time=53.3 ms
^C
 8.8.8.8 ping statistics:
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 53.270/53.395/53.721/0.150 ms
[root@ecs-test-nat-20070007 ~]#
```

2.2 Using a Public NAT Gateway to Enable Servers to Be Accessed by the Internet

Scenarios

When one or more servers in a VPC need to provide services accessible from the Internet, you can add DNAT rules for a public NAT gateway, as introduced in this section.

Operation Process

Procedure	Description
Step 1: Buy an EIP	Buy an EIP.
Step 2: Buy a Public NAT Gateway	Buy a public NAT gateway.
Step 3: Add a Default Route Pointing to the Public NAT Gateway	Add a route table.
Step 4: Add a DNAT Rule	Add DNAT rules for the public NAT gateway so that servers in specific CIDR blocks share EIPs to access the Internet.
Step 5: Verify that the DNAT Rule Has Been Added	Check whether the DNAT rule has been added.
Step 6: Verify that Servers in a VPC Can Be Accessed from the Internet Through the NAT Gateway	Verify that servers for which the DNAT rules are applied can be accessed by a client on the Internet.

Step 1: Buy an EIP

1. On the **Assign EIP** page, set the EIP name to **EIP-A**.
You can configure other EIP parameters as required. For details, see .

Step 2: Buy a Public NAT Gateway

1. On the **Create Public NAT Gateway** page, configure required parameters.

Table 2-3 Descriptions of public NAT gateway parameters

Parameter	Example	Description
Region	CN North-Beijing4	The region where the public NAT gateway is located.
Specifications	Small	The specifications of the public NAT gateway. The value can be Extra-large , Large , Medium , or Small . To view more details about specifications, click Learn more on the page.
Name	public-nat-01	The name of the public NAT gateway. Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
VPC	vpc-A	The VPC that the public NAT gateway belongs to. The selected VPC cannot be changed after you create the public NAT gateway. NOTE To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.

Parameter	Example	Description
Subnet	Subnet-A01	The subnet that the public NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after you create the public NAT gateway. The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.
Advanced Settings (Optional)	-	Click the drop-down arrow to configure advanced parameters of the public NAT gateway.
SNAT Connection TCP Timeout (s)	900	The timeout period of a TCP connection established using the SNAT rule. If no data is exchanged within this period, the TCP connection will be closed. Value range: 40 to 7200
SNAT Connection UDP Timeout (s)	300	The timeout period of a UDP connection established using the SNAT rule. If no data is exchanged within this period, the UDP connection will be closed. Value range: 40 to 7200
SNAT Connection ICMP Timeout (s)	10	The timeout period of an ICMP connection established using the SNAT rule. If no data is exchanged within this period, the ICMP connection will be closed. Value range: 10 to 7200
TCP TIME_WAIT (s)	5	How long the side that actively closed the TCP connection is in the TIME_WAIT state. Value range: 0 to 1800
Description	Not required	Supplementary information about the public NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.
Tag	Not required	The identifier of the public NAT gateway. A tag is a key-value pair. You can add up to 20 tags to each public NAT gateway.

2. Click **Create Now**. On the page displayed, confirm the public NAT gateway specifications.
3. If you do not need to modify the information, click **Submit**.

On the **Public NAT Gateways** page, you can view the created public NAT gateway in the list.

Step 3: Add a Default Route Pointing to the Public NAT Gateway

1. On the **Route Tables** page, click **Create Route Table** in the upper right corner.
VPC: Select the VPC that the public NAT gateway belongs to.
2. After the custom route table is created, click its name. The **Summary** page is displayed.
3. Click **Add Route** and configure parameters as follows:
Destination: Set it to **0.0.0.0/0**.
Next Hop Type: Select **NAT gateway**.
Next Hop: Select the created NAT gateway.

Figure 2-3 Add Route

4. Click **OK**.

Step 4: Add a DNAT Rule

1. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
2. On the public NAT gateway details page, click the **DNAT Rules** tab.
3. Click **Add DNAT Rule**.
4. Configure required parameters. For details, see [Table 2-4](#).

Table 2-4 Descriptions of DNAT rule parameters

Parameter	Example	Description
Scenario	VPC	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.

Parameter	Example	Description
Port Type	Specific port	The port type. <ul style="list-style-type: none">• All ports: All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.• Specific port: Only requests received from a specified port over a specified protocol will be forwarded to the specified port on the server.
Protocol	TCP	The protocol can be TCP or UDP. This parameter is available if you select Specific port for Port Type . If you select All ports , this parameter is All by default.
Public IP Address Type	EIP	The EIP of the public NAT gateway.
Outside Port	80-100	The port of the EIP used by the NAT gateway. The port number ranges from 1 to 65535. You can enter a specific port number or a port range, for example, 80 or 80-100.
Instance Type	Server	The instance type for which the DNAT rules are applied.
NIC	-	The network interface of the server.
Inside Port	80-100	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 port number ranges from 1 to 65535. You can enter a specific port number or a port range, for example, 80 or 80-100.
Description	Not required	Supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

5. Click **OK**.

NOTICE

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect. For details, see .

Step 5: Verify that the DNAT Rule Has Been Added

1. In the **DNAT Rules** tab, view details of the DNAT rule and check whether the DNAT rule has been created.

If **Status** of the SNAT rule is **Running**, the SNAT rule has been created.

Step 6: Verify that Servers in a VPC Can Be Accessed from the Internet Through the NAT Gateway

1. Log in to ECS 02 with an EIP bound.
2. On ECS 02, ping the EIP (120.46.131.153) to check whether ECS 01 on the private network can be accessed by ECS 02 on the public network through the NAT gateway.

Figure 2-4 Verification result

```
[root@ecs-~]# ping 120.46.131.153
PING 120.46.131.153 (120.46.131.153) 56(84) bytes of data.
64 bytes from 120.46.131.153: icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 120.46.131.153: icmp_seq=2 ttl=58 time=0.939 ms
64 bytes from 120.46.131.153: icmp_seq=3 ttl=58 time=0.905 ms
64 bytes from 120.46.131.153: icmp_seq=4 ttl=58 time=0.896 ms
64 bytes from 120.46.131.153: icmp_seq=5 ttl=58 time=0.906 ms
64 bytes from 120.46.131.153: icmp_seq=6 ttl=58 time=0.889 ms
64 bytes from 120.46.131.153: icmp_seq=7 ttl=58 time=0.860 ms
64 bytes from 120.46.131.153: icmp_seq=8 ttl=58 time=0.905 ms
64 bytes from 120.46.131.153: icmp_seq=9 ttl=58 time=0.886 ms
^C
--- 120.46.131.153 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8137ms
rtt min/avg/max/mdev = 0.860/0.930/1.192/0.102 ms
[root@ecs-~]#
```

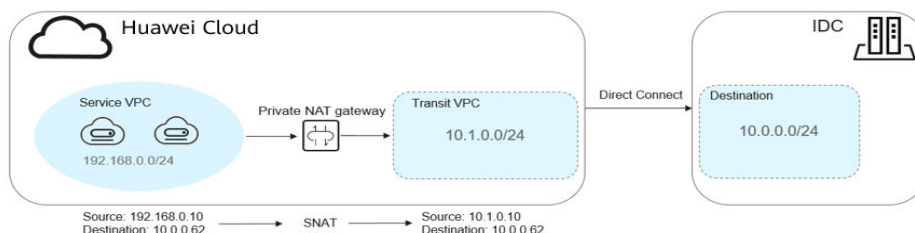
2.3 Using a Private NAT Gateway to Connect Cloud and On-premises Networks

Scenarios

You can use a private NAT gateway to enable communications between cloud and on-premises networks.

The following figure shows how a private NAT gateway enables ECSs in a VPC to communicate with your on-premises data center that has been connected to the cloud using Direct Connect.

Figure 2-5 Networking diagram



Operation Process

Procedure	Description
Step 1: Create a Service VPC and a Transit VPC	Create a service VPC and a transit VPC.
Step 2: Create a VPC Peering Connection	Create a VPC peering connection to connect your local data center to a transit VPC.
Step 3: Buy a Private NAT Gateway	Buy a private NAT gateway.
Step 4: Assign a Transit IP Address	Assign a transit IP address so that cloud servers in a VPC can use the same transit IP address.
Step 5: Add an SNAT Rule	After the private NAT gateway is created, add an SNAT rule so that servers in the VPC can share a transit IP address to access on-premises data centers or other VPCs.
Step 6: Add a Route	You can add a route and configure the destination, next hop type, and next hop in the routes to determine where network traffic is directed.
Step 7: Add a Security Group Rule	Add an inbound security group rule to allow traffic to servers in the destination VPC.

Preparations

Before using NAT gateways, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account.

- .
- .
- .

Step 1: Create a Service VPC and a Transit VPC

A VPC provides an isolated virtual network for ECSs. You can configure and manage your network as required.

You need to create two VPCs, one for your services, and one as the transit VPC.

For details, see .

Step 2: Create a VPC Peering Connection

Create a Direct Connect connection to link your on-premises data center to the cloud (the region). In this example, a VPC peering connection is used.

Create a VPC peering connection to connect your local data center to a transit VPC. For details, see .

NOTE

For details about how to use Direct Connect to connect your data center (the destination VPC in the VPC peering connection) to the transit VPC, see .

Step 3: Buy a Private NAT Gateway

1. On the **Create Private NAT Gateway** page, configure required parameters.

Table 2-5 Descriptions of private NAT gateway parameters

Parameter	Description
Region	The region where the private NAT gateway is located.
Name	The name of the private NAT gateway. Enter up to 64 characters including only digits, letters, underscores (_), and hyphens (-).
VPC	The service VPC that the private NAT gateway belongs to. The selected VPC cannot be changed after the private NAT gateway is created.
Subnet	The subnet that the private NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the private NAT gateway is created.
Specifications	The specifications of the private NAT gateway.
Enterprise Project	The enterprise project that the private NAT gateway belongs to. If you have not configured any enterprise project, select the default enterprise project. You can configure the enterprise project to which the private network NAT gateway belongs only after the enterprise project function is enabled for you.
Tag	The private NAT gateway tag. A tag is a key-value pair. You can add up to 20 tags to each private NAT gateway.

Parameter	Description
Description	Supplementary information about the private NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.

2. Click **Create Now**.
3. In the private NAT gateway list, check the gateway status.

Step 4: Assign a Transit IP Address

1. On the **Private NAT Gateways** page, click **Transit IP Addresses < Assign Transit IP Address**.
2. Configure required parameters. For details, see [Table 2-6](#).

Table 2-6 Parameter descriptions of a transit IP address

Parameter	Example	Description
Transit VPC	-	The VPC to which the transit IP address belongs.
Transit Subnets	-	A transit subnet is a transit network and is the subnet to which the transit IP address belongs. The subnet must have at least one available IP address.
Transit IP Address	Automatic	The transit IP address can be assigned in either of the following ways: Automatic: The system automatically assigns a transit IP address. Manual: You need to manually assign a transit IP address.
Enterprise Project	default	The enterprise project to which the transit IP address belongs.
Tag	Not required	The transit IP address tag, which consists of a key and value pair. You can add up to 20 tags to each transit IP address.

3. Click **OK**.

Step 5: Add an SNAT Rule

1. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add an SNAT rule.
2. On the **SNAT Rules** tab, click **Add SNAT Rule**.
3. Configure required parameters. For details, see [Table 2-7](#).

Table 2-7 Descriptions of SNAT rule parameters

Parameter	Example	Description
Subnet	Existing	The subnet type of the SNAT rule. Select Existing or Custom . Select a subnet where IP address translation is required in the service VPC.
Monitoring	-	You can create alarm rules to watch the number of SNAT connections.
Transit IP Address	-	The transit IP address you assigned in Step 4: Assign a Transit IP Address .
Description	Not required	Supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

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

Step 6: Add a Route

1. In the route table list, click the name of the route table associated the service VPC.
2. Click **Add Route** and configure required parameters.

Table 2-8 Route parameters

Parameter	Example	Description
Destination	10.0.0.0/24	The destination CIDR block. Set it to the CIDR block used by your on-premises data center.
Next Hop Type	NAT gateway	Type of the next hop.
Next Hop	private-nat-01	Set Next Hop to the private NAT gateway.
Description	Not required	(Optional) Supplementary information about the route. Enter up to 255 characters. Angle brackets (<>) are not allowed.

3. Click **OK**.

Step 7: Add a Security Group Rule

1. Locate the target security group and click **Manage Rules** in the **Operation** column.

The page for configuring security group rules is displayed.

2. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, configure required parameters.

You can click + to add more inbound rules.

Table 2-9 Description of inbound rule parameters

Parameter	Example	Description
Priority	1	Priority of a rule. A smaller value indicates a higher priority.
Action	Allow	Allow or Deny <ul style="list-style-type: none"> • If the Action is set to Allow, access from the source is allowed to ECSs in the security group over specified ports. • If the Action is set to Deny, access from the source is denied to ECSs in the security group over specified ports.
Protocol & Port	TCP	Protocol: Network protocol. The value can be All, TCP, UDP, ICMP, or GRE .
	22 or 22-30	Port: The port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.
Source	0.0.0.0/0	Source of the security group rule. The value can be a single IP address, an IP address group, or a security group, to allow access from the specified IP address, IP address group, or instances in another security group.
Description	Not required	(Optional) Supplementary information about the security group rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

3. Click **OK**.

3 Public NAT Gateways

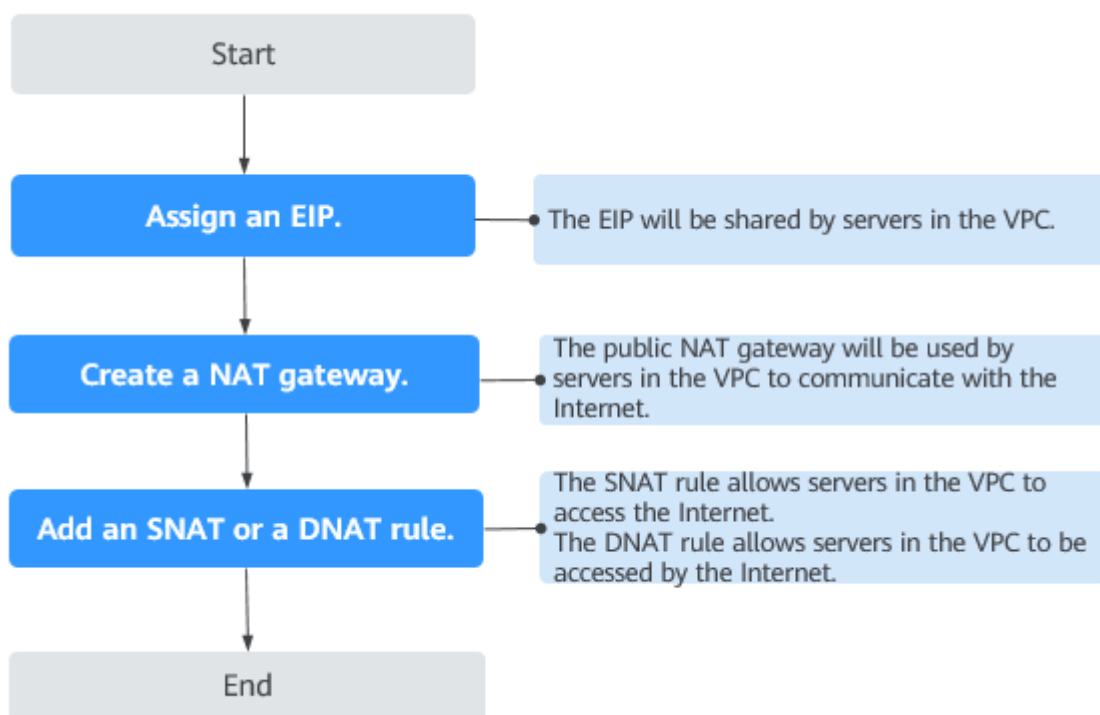
3.1 Overview of Public NAT Gateways

Public NAT gateways provide network address translation (NAT) with 20 Gbit/s of bandwidth for servers in a VPC or for servers in on-premises data centers that connect to a VPC through Direct Connect or VPN.

Public NAT gateways allow multiple servers to share an EIP to access the Internet or to provide services accessible from the Internet.

The process of using a public NAT gateway is as follows.

Figure 3-1 Process of using a public NAT gateway



3.2 Creating a Public NAT Gateway

Scenarios

a public NAT gateway to enable your servers to access the Internet or provide services accessible from the Internet.

Notes and Constraints

- Rules on one public NAT gateway can use the same EIP, but rules on different NAT gateways must use different EIPs.
- Each VPC can be associated with multiple public NAT gateways.
- SNAT and DNAT rules can use the same EIP to save resources. However, when **Port Type** of a DNAT rule is set to **All ports**, the resource in the DNAT rule will preferentially use all ports of the EIP. So an SNAT rule cannot share an EIP with such a DNAT rule.
- If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.

Prerequisites

- The VPC and subnet where your public NAT gateway will be deployed are available.
- To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.

Procedure


1. Log in to the management console.
2. In the upper left corner of the page, click  to expand the service list and choose **Network > NAT Gateway**.
The **Public NAT Gateways** page is displayed.
3. On the displayed page, click **Public NAT Gateway**.
4. Configure required parameters. For details, see [Table 3-1](#).

Table 3-1 Descriptions of public NAT gateway parameters

Parameter	Description
Region	The region where the public NAT gateway is located.
Specifications	The specifications of the public NAT gateway. The value can be Small , Medium , Large , or Extra-large . You can click Learn more on the page to view details of each specification.
Name	The name of the public NAT gateway. Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
VPC	The VPC that the public NAT gateway belongs to. The selected VPC cannot be changed after the public NAT gateway is created. NOTE To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully create: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.
Subnet	The subnet that the public NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the public NAT gateway is created. The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.
Advanced Settings (Optional)	Click the drop-down arrow to configure advanced parameters of the public NAT gateway, such as Description .
Description	Supplementary information about the public NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.

5. Click **Create Now**. On the page displayed, confirm the public NAT gateway specifications.
6. Click **Submit**.
It takes 1 to 5 minutes to create a public NAT gateway.
7. In the public NAT gateway list, you can see the gateway status.

NOTE

After the public NAT gateway is created, check whether a default route (0.0.0.0/0) that points to the public NAT gateway exists in the default route table of the VPC where the public NAT gateway is. If no, add a route pointing to the public NAT gateway to the default route table, alternatively, create a custom route table and add the default route 0.0.0.0/0 pointing to the public NAT gateway to the table.

FAQ

What Should I Do If the Number of NAT Gateway Connections Exceeds the Upper Limit?

- If the number of requests exceeds the maximum allowed connections of a public NAT gateway, services will be adversely affected. To avoid this situation, create alarm rules on the Cloud Eye console to monitor the number of SNAT connections.
- If the number of requests exceeds the maximum allowed connections of a NAT gateway, you are advised to update the NAT gateway by referring to [Managing Public NAT Gateways](#).

Does Changing NAT Gateway Specifications Interrupt Services?

Using a public NAT gateway of more robust specifications does not affect services, but if you switch to a public NAT gateway of less robust specifications, ensure that its capacity can still be enough to meet your service requirements.

3.3 Managing Public NAT Gateways

Scenarios


After a public NAT gateway is created, you can modify the name, specifications, or description of it. You can also delete public NAT gateways that are no longer needed to release resources.

Using a public NAT gateway of more robust specifications does not affect services, but if you switch to a public NAT gateway of less robust specifications, ensure that its capacity can still be enough to meet your service requirements.


NOTE

- If you downgrade a NAT gateway, make sure that the new specification can meet your service requirements.
- Upgrading a NAT gateway does not affect services.

Modifying a Public NAT Gateway

1. Log in to the management console.
2. In the upper left corner of the page, click  to expand the service list and choose **Network > NAT Gateway**.
The **Public NAT Gateways** page is displayed.
3. Locate the row that contains the public NAT gateway you want to modify and click **Modify** in the **Operation** column.
4. Modify the name, specifications, or description of the public NAT gateway.

Deleting a Public NAT Gateway

1. Log in to the management console.
2. In the upper left corner of the page, click  to expand the service list and choose **Network > NAT Gateway**.
The **Public NAT Gateways** page is displayed.
3. On the displayed page, locate the public NAT gateway that you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, enter **DELETE**.
5. Click **OK**.

3.4 Managing SNAT Rules

3.4.1 Adding an SNAT Rule

Scenarios

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

One SNAT rule takes effect for only one subnet. If there are multiple subnets in a VPC, create multiple SNAT rules to allow servers in them to share EIPs.

Notes and Constraints

- Only one SNAT rule can be added for each VPC subnet.
- When you add an SNAT rule in the VPC scenario, the custom CIDR block must be a subset of the NAT gateway's VPC subnets.
- If an SNAT 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.
- There is no limit on the number of SNAT rules that can be added on a public NAT gateway.

Adding an SNAT Rule


1. Log in to the management console.
2. In the upper left corner of the page, click  to expand the service list and choose **Network > NAT Gateway**.
The **Public NAT Gateways** page is displayed.
3. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
4. On the **SNAT Rules** tab, click **Add SNAT Rule**.
5. Configure required parameters. For details, see [Table 3-2](#).

Table 3-2 Descriptions of SNAT rule parameters

Parameter	Description
Scenario	The scenarios where the SNAT rule is used Select VPC if your servers in a VPC need to access the Internet. Select Direct Connect if servers in your on-premises data center need to access the Internet.
CIDR Block	In a VPC scenario, specify a VPC subnet to enable servers in that subnet to access the Internet using the SNAT rule. In a Direct Connect scenario, specify a CIDR block of your data center to enable your servers to access the Internet using the SNAT rule.
Public IP Address Type	The EIP used for accessing the Internet You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with Port Type set to Specific port , or has been bound to an SNAT rule of the current public NAT gateway.
Monitoring	You can create alarm rules on the Cloud Eye console to monitor your SNAT connections and keep informed of any changes in a timely manner.
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. Click **OK**.

 **NOTE**

- You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.
- Only one SNAT rule can be added for each VPC subnet.

3.4.2 Modifying an SNAT Rule

Scenarios

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

Note that modifying an SNAT rule may interrupt your services.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click the name of the public NAT gateway.
3. On the **SNAT Rules** tab, locate the SNAT rule you want to modify.
4. Click **Modify** in the **Operation** column.
5. In the displayed dialog box, modify parameters as needed.
6. Click **OK**.

3.4.3 Deleting an SNAT Rule

Scenarios

You can delete SNAT rules that are no longer needed.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click the name of the public NAT gateway.
3. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.
4. Enter **DELETE** in the displayed dialog box and click **OK**.

3.5 Managing DNAT Rules

3.5.1 Adding a DNAT Rule

Scenarios

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

Only one DNAT rule can be configured for each port on 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.

Restrictions and Limitations

- Only one DNAT rule can be configured for each port on a server. One port can be mapped to only one EIP.
- A maximum of 200 DNAT rules can be added on a public NAT gateway.

Procedure


1. Log in to the management console.
2. In the upper left corner of the page, click  to expand the service list and choose **Network > NAT Gateway**.
The **Public NAT Gateways** page is displayed.
3. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. Click **Add DNAT Rule**.
6. Configure required parameters. For details, see [Table 3-3](#).

Table 3-3 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	Select VPC if your servers in a VPC will use the DNAT rule to share the same EIP to provide services accessible from the Internet. Direct Connect : Select this scenario if your on-premises servers will use the DNAT rule to provide services accessible from the Internet.
Port Type	The port type <ul style="list-style-type: none">• All ports: All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.• Specific port: Only requests received from a specified port over a specified protocol will be forwarded to the specified port on the 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 is All by default.

Parameter	Description
Public IP Address Type	<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 has not been bound, has been bound to a DNAT rule of the current public NAT gateway with Port Type set to Specific port, or has been bound to an SNAT rule of the current public NAT gateway.</p>
Outside Port	<p>The port of the EIP used by the NAT gateway for external communications</p> <p>This parameter is only available if you select Specific port for Port Type. Range: 1 to 65535</p> <p>You can enter a specific port number or a port range, for example, 80 or 80-100.</p>
Instance Type	<p>The type of the instance that will be providing services accessible from the Internet. Possible values are:</p> <ul style="list-style-type: none"> • Server • Virtual IP address • Custom
NIC	<p>The NIC of the server. This parameter is available if you set Instance Type to Server.</p>
Private IP Address	<ul style="list-style-type: none"> • In a VPC scenario, set this parameter to the private IP address of a server in the NAT gateway's VPC. The server will provide services accessible from the Internet through DNAT. • In a Direct Connect scenario, set this parameter to IP address of the server in your on-premises data center or your private IP address. This IP address is used by on-premises servers that are connected to a VPC through Direct Connect 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>The port of the server over which the originating requests will be forwarded</p> <p>This parameter is only available if you select Specific port for Port Type.</p> <p>Range: 1 to 65535</p> <p>You can enter a specific port number or a port range, for example, 80 or 80-100.</p>
Description	<p>Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.</p>

7. Click **OK**.
Once the rule is created, its status changes to **Running**.

NOTICE

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect.

3.5.2 Modifying a DNAT Rule

Scenarios

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

Note that modifying a DNAT rule may interrupt your services.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click the name of the public NAT gateway.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.
5. In the displayed dialog box, modify parameters as needed.
6. Click **OK**.

3.5.3 Deleting a DNAT Rule

Scenarios

You can delete DNAT rules that are no longer needed.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click the name of the public NAT gateway.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.

5. Enter **DELETE** in the displayed dialog box and click **OK**.

3.5.4 Deleting DNAT Rules in Batches

Scenarios

Delete DNAT rules that you no longer need.

Prerequisites

DNAT rules have been added.

Procedure

1. Log in to the management console.
2. Click the name of the public NAT gateway.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list, select DNAT rules that you no longer need and click **Delete DNAT Rule**.
5. In the displayed dialog box, click **OK**.

3.5.5 Importing DNAT Rules by Using a Template and Exporting DNAT Rules

Scenarios

When adding DNAT rules in different environments or migrating DNAT rules between NAT gateways, you can import and export DNAT rules to simplify and accelerate the DNAT rule configuration.

Importing DNAT Rules

1. Log in to the management console.
2. On the displayed page, click the name of the public NAT gateway to which you want to import DNAT rules.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. On the displayed page, click **Import**. In the displayed **Import Rule** dialog box, click **Download Template**.
5. Fill in DNAT rule parameters based on the table heading in the template. For details, see [Table 3-4](#).

Table 3-4 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	<p>The following two scenarios are available:</p> <ul style="list-style-type: none"> • VPC: The servers in a VPC will share an EIP to provide services accessible from the Internet through the DNAT rule. • Direct Connect: Select this scenario if your on-premises servers will use the DNAT rule to provide services accessible from the Internet.
Protocol	The value can be TCP , UDP , or All .
EIP	<p>The EIP that will be used by the server to provide publicly accessible services</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>The EIP port</p> <p>This parameter is only available if Specific port is selected for Port Type.</p> <p>You can enter a specific 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 private IP address of a server in the NAT gateway's VPC. The server will provide services accessible from the Internet through DNAT. • In a Direct Connect scenario, set this parameter to IP address of the server in your on-premises data center or your private IP address. This IP address is used by on-premises servers that are connected to a VPC through Direct Connect to provide services accessible from the Internet through DNAT. • Configure the private IP address port if Protocol is set to TCP or UDP.
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 on-premises data center or the user's private port. • This parameter is only available if Specific port is selected for Port Type. <p>The number of inside and outside ports must match.</p>
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. After filling in the template, click **Select File**, select the local template, and click **Import**.
7. View the imported DNAT rules.
If their **Status** is **Running**, the DNAT rules have been added.

Exporting DNAT Rules

1. Log in to the management console.
2. On the displayed page, click the name of the public NAT gateway from which you want to export DNAT rules.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list, select the rules to be exported and click **Export**.
 - a. **Export all data to an XLSX file:** The system automatically exports the basic information of all the DNAT rules in the current region as an Excel file to a local directory.
 - b. **Export selected data to an XLSX file:** The system automatically exports the basic information of the selected DNAT rules in the current region as an Excel file to a local directory.

4 Private NAT Gateways

4.1 Overview of Private NAT Gateways

Private NAT Gateways

Private NAT gateways provide private address translation services for ECSs and BMSs in a VPC. You can configure SNAT and DNAT rules to translate the source and destination IP addresses into transit IP addresses, so that servers in the VPC can communicate with other VPCs or on-premises data centers.

Specifically:

- SNAT enables servers in a VPC, regardless of if they are in the same AZ, to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers in a VPC, regardless of if they are in the same AZ, to share a transit IP address to provide services accessible from on-premises data centers or other VPCs.

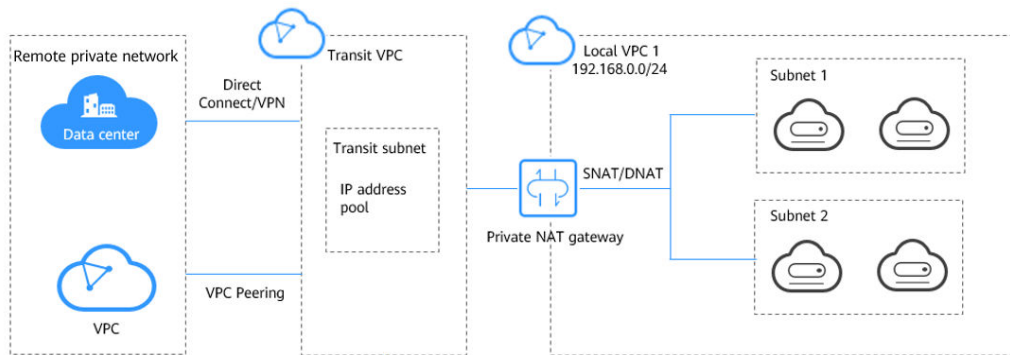
Transit Subnet

A transit subnet functions as a transit network. You can configure a transit IP address for the transit subnet so that servers in a local VPC can share the transit IP address to access on-premises data centers or other VPCs.

Transit VPC

The transit VPC is the VPC that the transit subnet is a part of.

Figure 4-1 Private NAT gateway



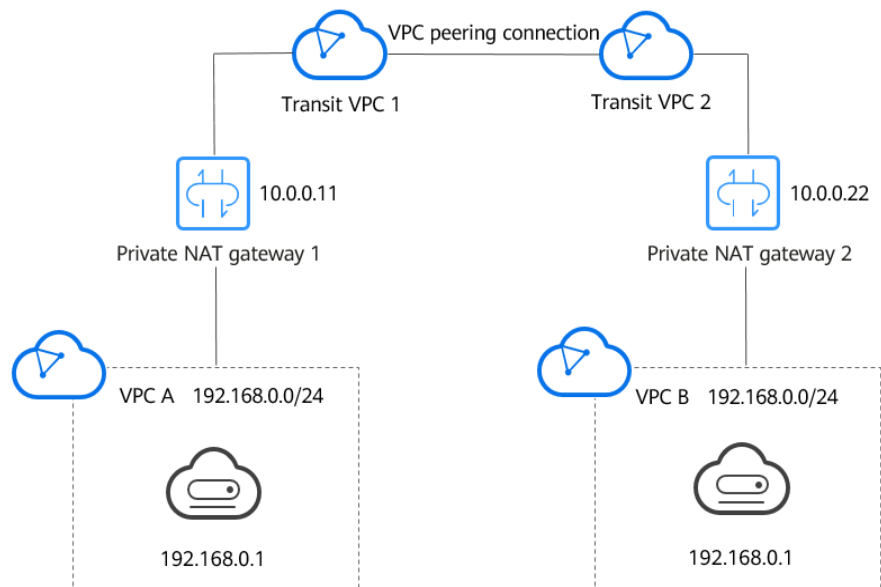
Application Scenarios

- Connecting VPCs with overlapping CIDR blocks

You can configure two private NAT gateways for two VPCs with overlapping CIDR blocks. Then, add SNAT and DNAT rules on the two private NAT gateways to enable servers in the two VPCs to use the transit IP addresses to communicate with each other.

In the following figure, there are two transit VPCs and two private NAT gateways. Address 192.168.0.1 in VPC A is translated to 10.0.0.11, and the IP address 192.168.0.1 in VPC B is translated to 10.0.0.22. A VPC peering connection can then be established between the two transit VPCs to enable communication between them.

Figure 4-2 Connecting VPCs with overlapping CIDR blocks



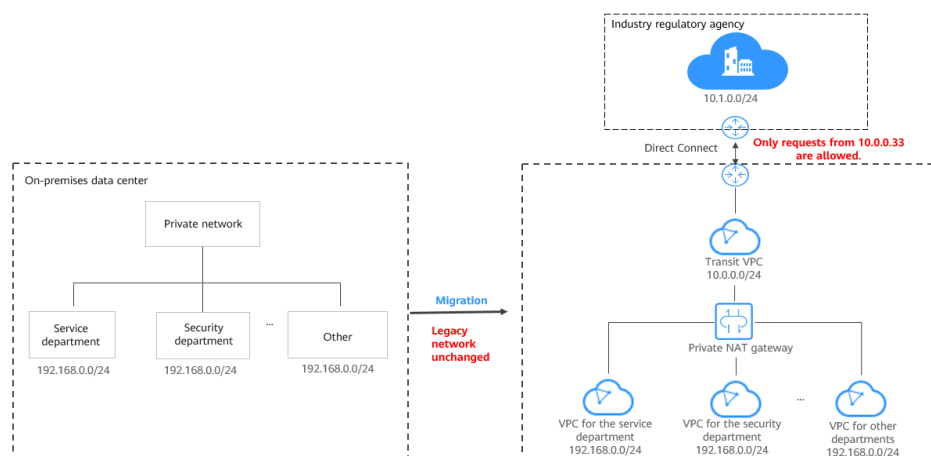
- Migrating workloads to the cloud without changing the network topology or accessing regulatory agencies from specific IP addresses

Organizations may want to migrate their workloads to the cloud without making any changes to their existing network topology. They may also have

to access regulatory agencies from specific IP addresses as required by these agencies. A private NAT gateway is a good choice.

The following figure represents an enterprise network where the subnets of different departments overlap. A private NAT gateway allows the enterprise to keep the existing network topology unchanged while migrating their workloads to the cloud. In this example, the private NAT gateway maps the IP address of each department to 10.0.0.33 so that each department can use 10.0.0.33 to securely access the regulatory agency.

Figure 4-3 Migrating workloads to the cloud without changing the network topology or accessing regulatory agencies from specific IP addresses



Differences Between Public and Private NAT Gateways

Public NAT gateways use SNAT rules to map private IP addresses to EIPs, so that servers in a VPC can share an EIP to access the Internet. DNAT rules enable the servers to share an EIP to provide services accessible from the Internet.

Private NAT gateways use SNAT rules to map private IP addresses to transit IP addresses, so that servers in a VPC can access on-premises data centers or other VPCs. DNAT rules enable the servers to share the transit IP address to provide services accessible from the private network.

Table 4-1 describes the differences between public and private NAT gateways.

Table 4-1 Differences between public and private NAT gateways

Item	Public NAT Gateway	Private NAT Gateway
Function	Connects a private network to the Internet	Connects private networks
SNAT	Enables access to the Internet	Enables access to on-premises data centers or other VPCs
DNAT	Allows servers to provide services accessible from the Internet	Allows servers to provide services accessible from on-premises data centers or other VPCs in private networks

Item	Public NAT Gateway	Private NAT Gateway
IP type for communication	EIP	Transit IP address

Process for Deploying a Private NAT Gateway

The process for deploying a private NAT gateway is as follows:

Figure 4-4 Process for deploying a private NAT gateway



If you want to use a private NAT gateway to connect your VPC to on-premises data centers or other VPCs, refer to [Accessing On-premises Data Centers or Other VPCs](#).

4.2 Creating a Private NAT Gateway

Scenarios

You need a private NAT gateway to enable servers in your VPC to access or provide services accessible from on-premises data centers and other VPCs.

Notes and Constraints

- Manually add routes in a VPC to connect it to a remote private network through a VPC peering connection, Direct Connect, or VPN connection.
- SNAT and DNAT rules cannot share a transit IP address.
- The total number of DNAT and SNAT rules that can be added on a private NAT gateway varies with the private NAT gateway specifications.
 - Small: 20 or less
 - Medium: 50 or less
 - Large: 200 or less
 - Extra-large: 500 or less

CAUTION

When you create a private NAT gateway, you must specify its VPC, subnet, and specifications.

Procedure


1. Log in to the management console.
2. In the upper left corner of the page, click  to expand the service list and choose **Network > NAT Gateway**.
The NAT Gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, click **Create Private NAT Gateway**.
5. Configure required parameters. For details, see [Table 4-2](#).

Table 4-2 Descriptions of private NAT gateway parameters

Parameter	Description
Region	The region where the private NAT gateway is located.
Name	The name of the private NAT gateway. Enter up to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.
VPC	The VPC that the private NAT gateway belongs to. The selected VPC cannot be changed after the private NAT gateway is created.
Subnet	The subnet that the private NAT gateway belongs to. The subnet must have at least one available IP address. The selected subnet cannot be changed after the private NAT gateway is created.
Specifications	The specifications of the private NAT gateway. The value can be Extra-large , Large , Medium , or Small . For details about specifications, see NAT Gateway Specifications .
Description	Supplementary information about the private NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. Click **Create Now**.

Other Operations

- [Assigning a Transit IP Address](#)
- [Adding an SNAT Rule](#)

- [Adding a DNAT Rule](#)
- [Managing Private NAT Gateways](#)

4.3 Managing Private NAT Gateways

After a private NAT gateway is created, you can manage it in a unified manner, including modifying and deleting the private NAT gateway.

Modifying a Private NAT Gateway

Modify the name, specifications, or description of a private NAT gateway.

1. Log in to the management console.
2. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
3. On the displayed page, locate the row that contains the private NAT gateway you want to modify and click **Modify** in the **Operation** column.
4. Modify the name, specifications, or description of the private NAT gateway.
5. Click **Next**.
6. Confirm the modification and click **Submit**.

Deleting a Private NAT Gateway

Delete private NAT gateways that are no longer required to release resources.

NOTE

All SNAT and DNAT rules created on the private NAT gateway have been deleted. For details about how to delete SNAT and DNAT rules, see [Deleting an SNAT Rule](#) and [Deleting a DNAT Rule](#).

1. Log in to the management console.
2. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
3. On the **Private NAT Gateways** page, locate the private NAT gateway that you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, enter **DELETE**.
5. Click **OK**.

4.4 Managing SNAT Rules

4.4.1 Adding an SNAT Rule

Scenarios

After the private NAT gateway is created, add an SNAT rule so that some or all servers in a VPC subnet can share a transit IP address to access on-premises data centers or other VPCs.

Notes and Constraints

Only one SNAT rule can be added for each VPC subnet.

Prerequisites

- A private NAT gateway is available.
- A transit IP address is available.

Procedure

1. Log in to the management console.
2. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
3. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add an SNAT rule.
4. On the **SNAT Rules** tab, click **Add SNAT Rule**.
5. Configure required parameters. For details, see [Table 4-3](#).

Table 4-3 Parameter descriptions of an SNAT rule

Parameter	Description
Subnet	The subnet type of the SNAT rule. Select Existing or Custom . Select a subnet where IP address translation is required in the service VPC.
Monitoring	You can create alarm rules using Cloud Eye after your SNAT connection has been created.
Transit IP Address	Select the created transit IP address.
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. Click **OK**.

NOTE

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

Helpful Links

[Managing SNAT Rules](#)

4.4.2 Modifying an SNAT Rule

Scenarios

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

Note that modifying an SNAT rule may interrupt your services.

Prerequisites

An SNAT rule has been added.

Procedure

1. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
2. On the **SNAT Rules** tab, locate the SNAT rule you want to modify.
3. Click **Modify** in the **Operation** column.
4. In the displayed dialog box, modify parameters as needed.
5. Click **OK**.

4.4.3 Deleting an SNAT Rule

Scenarios

You can delete SNAT rules that are no longer needed.

Prerequisites

An SNAT rule has been added.

Procedure

1. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
2. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.
3. In the displayed dialog box, click **OK**.

4.5 Managing DNAT Rules

4.5.1 Adding a DNAT Rule

Scenarios

After a private NAT gateway is created, you can add DNAT rules to allow servers in your VPC to provide services accessible from on-premises servers or other VPCs.

A DNAT rule needs to be configured for each port on a server that needs to be made accessible. If multiple ports on a server or multiple servers need to provide services accessible from on-premises servers or other VPCs, multiple DNAT rules need to be configured.

Notes and Constraints

A DNAT rule with **Port Type** set to **All ports** cannot share a transit IP address with a DNAT rule with **Port Type** set to **Specific port**.

Prerequisites

- A private NAT gateway is available.
- A transit IP address is available.

Procedure

1. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add a DNAT rule.
2. On the private NAT gateway details page, click the **DNAT Rules** tab.
3. Click **Add DNAT Rule**.

NOTICE

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect.

4. Configure required parameters. For details, see [Table 4-4](#).

Table 4-4 Descriptions of DNAT rule parameters

Parameter	Description
Local Network	
Port Type	The port type The type can be: <ul style="list-style-type: none">• Specific port: The private NAT gateway only forwards requests to your servers from the outside port and to the inside port configured here, and only if they use the right protocol.• All ports: All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.

Parameter	Description
Protocol	The protocol can be TCP or UDP If you select All ports , the value of this parameter is All by default. This parameter is only available if you select Specific port for Port Type .
Instance Type	The type of instance that will provide services accessible from on-premises data centers or other VPCs Possible types are: <ul style="list-style-type: none"> • Server • Virtual IP address • Load balancer • Custom
NIC	The NIC of the server This parameter is only available if you set Instance Type to Server .
IP Address	The IP address of the server that will provide services accessible from on-premises data centers or other VPCs. This parameter is only available if you set Instance Type to Custom .
Internal Port	The port of the instance Range: 1 to 65535 This parameter is only available if you select Specific port for Port Type .
Transit Network	
Transit IP Address	The transit IP address used to access on-premises data centers or other VPCs You can select a transit IP address that is not bound to any resource, has been bound to a DNAT rule for the current private NAT gateway where Port Type is set to Specific port , or has been bound to an SNAT rule of the current private NAT gateway.
Transit IP Address Port	The port of the transit IP address Supported range: 1 to 65535 This parameter is only available if you select Specific port for Port Type .
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

5. Click **OK**.

Once the rule is created, its status changes to **Running**.

Helpful Links

[Managing DNAT Rules](#)

4.5.2 Modifying a DNAT Rule

Scenarios

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

Note that modifying an SNAT rule may interrupt your services.

Prerequisites

A DNAT rule has been added.

Procedure

1. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
2. On the private NAT gateway details page, click the **DNAT Rules** tab.
3. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.
4. In the displayed dialog box, modify parameters as needed.
5. Click **OK**.

4.5.3 Deleting a DNAT Rule

Scenarios

You can delete DNAT rules that are no longer needed.

Prerequisites

A DNAT rule has been added.

Procedure

1. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
2. On the private NAT gateway details page, click the **DNAT Rules** tab.
3. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, click **OK**.

4.6 Managing Transit IP Addresses

4.6.1 Assigning a Transit IP Address

Scenarios

Servers in a VPC can use the same transit IP address to access or provide services accessible from on-premises data centers or other VPCs.

Procedure

1. Log in to the management console.
2. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
3. On the **Private NAT Gateways** page, click **Transit IP Addresses**.
4. Configure required parameters. For details, see [Table 4-5](#).

Table 4-5 Parameter descriptions of a transit IP address

Parameter	Description
Transit VPC	VPC to which the transit IP address is located.
Transit Subnets	A transit subnet is a transit network and is the subnet to which the transit IP address belongs. The subnet must have at least one available IP address.
Transit IP Address	The transit IP address can be assigned in either of the following ways: Automatic: The system automatically assigns a transit IP address. Manual: You need to manually assign a transit IP address.
IP Address	This parameter is only available when you set Transit IP Address to Manual . Click View In-Use IP Address to view in-use IP addresses in the selected subnet.
Tag	The private NAT gateway tag. A tag is a key-value pair. You can add up to 20 tags to each private NAT gateway.

5. Click **OK**.

4.6.2 Viewing a Transit IP Address

Scenarios

You can view details about the transit IP addresses assigned to you.

Procedure

1. Click the **Transit IP Addresses** tab and then click the transit IP address.
2. On the page displayed, view details of the assigned transit IP address.
You can view the transit VPC, transit subnet, and private NAT gateway associated with the transit IP address.

4.6.3 Releasing a Transit IP Address

Scenarios

You can release a transit IP address that is no longer needed.

Procedure

1. In the **Transit IP Addresses** tab, locate the transit IP address you want to release and click **Release** in the **Operation** column.
2. Click **OK**.

NOTE

If a transit IP address has been associated with an SNAT or DNAT rule, it cannot be released. To release such a transit IP address, delete all rules associated with it first.

4.7 Accessing On-Premises Data Centers or Other VPCs

Accessing On-Premises Data Centers

You can use Direct Connect or VPN to connect the transit VPC to your on-premises data centers.

For a higher quality connection, use Direct Connect. For details, see *Direct Connect User Guide*.

For more cost-effective connectivity, use VPN. For details, see *Virtual Private Network User Guide*.

Accessing Other VPCs

You can use VPC Peering to connect the transit VPC to other VPCs.

For details, see *Virtual Private Cloud User Guide*.

5 Permissions Management

5.1 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 a cloud service to perform efficient O&M on your NAT Gateway resources.

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

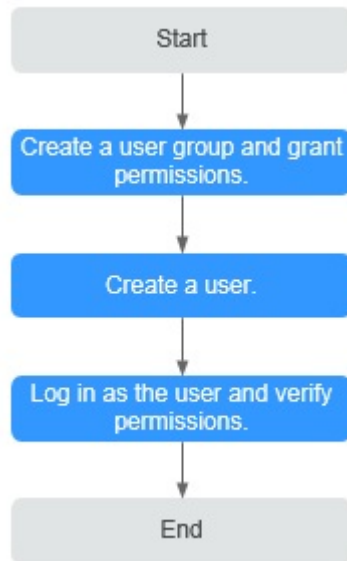
This section describes the procedure for granting permissions (see [Figure 5-1](#)).

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 [Permission Description](#).

Process Flow

Figure 5-1 Process for granting NAT Gateway permissions



1. Create and authorize a user group.
Create a user group on the IAM console and attach the **NATReadOnlyAccess** 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 **NATReadOnlyAccess** 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 **NATReadOnlyAccess** policy has already taken effect.

5.2 NAT Gateway Custom Policies

You can create custom policies to supplement system-defined policies of NAT Gateway. For the actions that can be added to custom policies, see section "Permissions Policies and Supported Actions" in *NAT Gateway API Reference*.

To create a custom policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For operation details, see section "Creating a Custom Policy" in *Identity and Access Management User Guide*. The following section contains examples of common NAT Gateway custom policies.

Example Policies

- Example 1: Grant permissions to create and delete a NAT gateway.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "nat:natGateways:create",
        "nat:natGateways:delete"
      ]
    }
  ]
}
```

- Example 2: Grant permissions to deny NAT gateway deletion.

A policy with only "Deny" permissions must be used together with other policies. 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"
    }
  ]
}
```



```
]
}
```

6 Monitoring

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

Metrics

Table 6-1 Public 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	Public NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bits/s	Public 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	Public NAT gateway	1 minute
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: count	≥ 0	Public NAT gateway	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: count	≥ 0	Public NAT gateway	1 minute
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Public NAT gateway	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Public 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 NAT gateway specifications. Unit: percent	≥ 0	Public NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
inbound_bandwidth_ratio	Inbound Bandwidth Usage	<p>Inbound bandwidth usage of servers using the SNAT function</p> <p>The maximum bandwidth supported by a public NAT gateway is 20 Gbit/s. Inbound bandwidth usage = Used bandwidth/Maximum bandwidth of the public NAT gateway × 100%.</p> <p>Unit: percent</p> <p>NOTE This metric is used to monitor the performance of public NAT gateways instead of the EIP bandwidth.</p>	≥ 0	Public NAT gateway	1 minute
outbound_bandwidth_ratio	Outbound Bandwidth Usage	<p>Outbound bandwidth usage of servers using the SNAT function</p> <p>The maximum bandwidth supported by a public NAT gateway is 20 Gbit/s. Outbound bandwidth usage = Used bandwidth/Maximum bandwidth of the public NAT gateway × 100%.</p> <p>Unit: percent</p> <p>NOTE This metric is used to monitor the performance of public NAT gateways instead of the EIP bandwidth.</p>	≥ 0	Public NAT gateway	1 minute

Table 6-2 Private 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	Private NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bit/s	Private NAT gateway	1 minute
outbound_bandwidth	Outbound Bandwidth	Outbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bit/s	Private NAT gateway	1 minute
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: count	≥ 0	Private NAT gateway	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: count	≥ 0	Private NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Private NAT gateway	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Private NAT gateway	1 minute

Dimensions

Key	Value
nat_gateway_id	Public NAT gateway
vpc_nat_gateway_id	Private NAT gateway

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**, 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 specify required parameters.
5. Click **Next** and specify rule parameters as prompted.

6. Click **Finish**.

After the alarm rule is set, the system automatically notifies you when an alarm is triggered.

 **NOTE**

For more details, see [Creating Alarm Rules](#).

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. In the upper left corner, select the target region.
3. Under **Management & Deployment**, select **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring > NAT Gateway**.
5. 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, or twelve hours.

7 FAQs

7.1 Public NAT Gateways

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

- A VPC is a secure, isolated, logical network environment.
- A public NAT gateway enables ECSs in a 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 an instance running in a VPC and uses a public NAT gateway to access the Internet.

7.1.2 How Does a Public NAT Gateway Offer High Availability?

The backend of a public NAT gateway supports automatic disaster recovery through hot standby, thereby reducing risks and improving availability.


7.2 Private NAT Gateways

7.2.1 How Do I Troubleshoot a Network Failure After a Private NAT Gateway Is Configured?


Checking Security Group Rules

If the traffic to and from the ECS port is denied in the security group, add rules to the security group to allow the port traffic.

Step 1 Log in to the management console.

- Step 2** Click  in the upper left corner and select the desired region and project.
- Step 3** Choose **Compute > Elastic Cloud Server**.
- Step 4** In the ECS list, click the name of the ECS for which you will check the security group rules.
- Step 5** Click the **Security Groups** tab and view security group rules.
- Step 6** Check whether you have configured inbound and outbound rules to allow traffic to and from the ECS port.
- If yes, go to [Checking Whether Default Route Pointing to the Private NAT Gateway Is Configured in the Route Table](#).
 - If no, go to [Step 7](#).
- Step 7** Click **Manage Rule**. On the displayed page, click **Inbound Rules** or **Outbound Rules** to add an inbound rule and outbound rule that allow traffic to and from the ECS port.
- End

Checking Whether Default Route Pointing to the Private NAT Gateway Is Configured in the Route Table

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select the desired region and project.
- Step 3** Under **Networking**, click **Virtual Private Cloud**.
- Step 4** In the navigation pane on the left, choose **Route Tables**.
- Step 5** In the route table list, click the name of the route table associated with the VPC to which the private NAT gateway belongs.
- Step 6** Check whether the route pointing to the private NAT gateway is configured in the route list.
- End

7.2.2 How Many Private NAT Gateways Can I Create in a VPC?

You can create a maximum of 10 private NAT gateways in a VPC.

7.2.3 Can Private NAT Gateways Translate On-premises IP Addresses Connected to the Cloud Through Direct Connect?

Yes. When you are creating a DNAT rule and select **Custom** for **Instance Type**, you can add an on-premises IP address.

7.2.4 What Are the Differences Between Private NAT Gateways and Public NAT Gateways?

Private NAT gateways perform NAT between private IP addresses and resolve the following problems:

- Private IP address conflicts
- Access from specified addresses

Public NAT gateways perform NAT between private IP addresses and public IP addresses and have the following advantages:

- Secure: Only shared EIPs, instead of all EIPs of servers, are exposed to the Internet.
- Cost-effective: EIPs and bandwidth are shared, saving network infrastructure costs.

7.2.5 Can a Private NAT Gateway Be Used Across Accounts?

Private NAT gateways cannot be used across accounts. However, you can use a VPC peering connection to connect the transit VPCs of two accounts. In this way, the two VPCs where the private NAT gateways of the two accounts are deployed can communicate with each other.

7.3 SNAT Rules

7.3.1 Why Do I Need SNAT?

Public NAT gateways: 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 public IP address is preferable and more practical. This can be done using SNAT.

Private NAT gateways: Different departments of a large enterprise may have a large number of overlapping CIDR blocks. After the enterprise migrates its workloads to the cloud, those departments will not be able to communicate with each other. In this case, SNAT can be used to translate the IP addresses of multiple ECSs in a department into a transit IP address for accessing other departments. In other scenarios where high security is required, an industry regulation agency may require other organizations to use a specified IP address to access the regulation system. In this case, SNAT can translate the IP addresses of multiple servers in an organization to one transit IP address, that is, the specified IP address.

7.3.2 What Are SNAT Connections?

The number of SNAT connections is the number of active connections created by a NAT gateway when it performs SNAT. An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. An SNAT connection uniquely identifies a session. The source IP address and port are the IP address and port translated by SNAT.

SNAT supports three protocols: TCP, UDP, and ICMP. A NAT gateway supports up to 55,000 concurrent connections to each destination IP address and port. If any of the destination IP address, port number, and protocol (TCP, UDP, or ICMP) changes, you can create another 55,000 connections. You can run the **netstat** command on an ECS to obtain the number of connections in the **ESTABLISHED**

state, but this number reflects only the number of connections established to this ECS, and due to the impact of connection timeout, connection reuse, and other issues, this number may be different from the number of SNAT connections maintained by the NAT gateway. Assume that an ECS creates 100 connections to a fixed destination every second and there are no interrupted TCP connections, 55,000 connections will be used up in about 10 minutes. 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.

7.4 DNAT Rules

7.4.1 Why Do I Need DNAT?

In a public NAT gateway, DNAT enables servers in a VPC to share an EIP to provide services accessible from the Internet through IP address mapping or port mapping. For details, see [Adding a DNAT Rule](#).

In a private NAT gateway, DNAT enables servers, regardless of if they are in the same AZ, to share the same transit IP address to provide services accessible from on-premises data centers or other VPCs. For details, see section "Adding a DNAT Rule" under "Managing Private NAT Gateways" in *NAT Gateway User Guide*.

7.4.2 Can I Modify DNAT Rules?

You can modify DNAT rules. For both public and private NAT gateways, DNAT rules can be modified.

A Change History

Released On	Description
2024-04-15	This issue is the first official release.