NAT Gateway

Service Overview

Issue	01
Date	2023-08-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 What Is NAT Gateway?

Public NAT gateways are used to provide NAT.

Public NAT Gateways

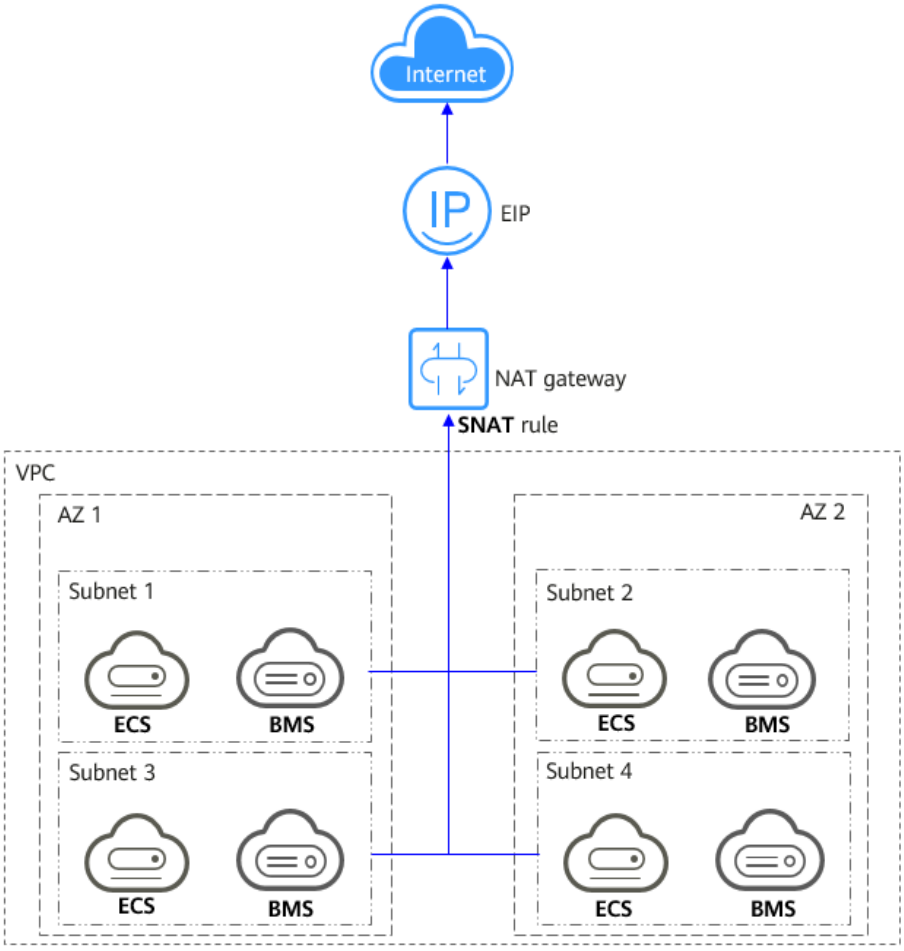
A public NAT gateway enables cloud and on-premises servers in a private subnet to share an EIP to access the Internet or provide services accessible from the Internet. Cloud servers are ECSs and BMSs in a VPC. On-premises servers are servers in on-premises data centers that connect to a VPC through Direct 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.

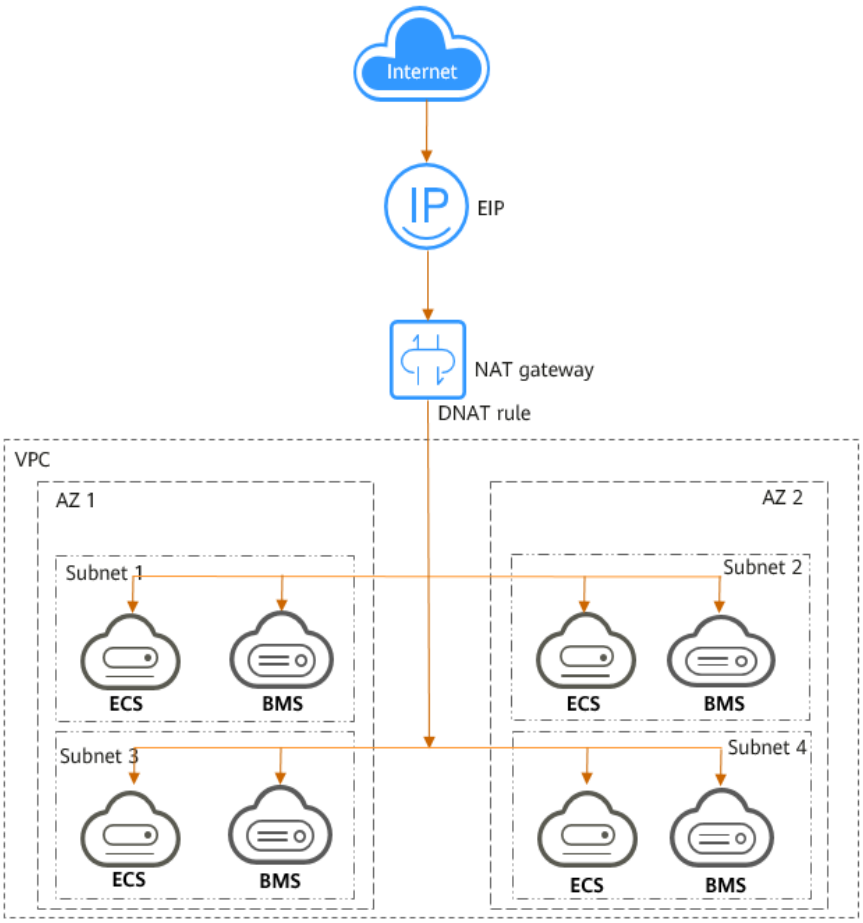
Figure 1-1 NAT gateway with an SNAT rule



- DNAT enables servers within an AZ or across AZs in a VPC to share an EIP to provide services accessible from the Internet. With an EIP, a 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 within one AZ or across AZs in a VPC to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers that share the same transit IP address in a VPC 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.

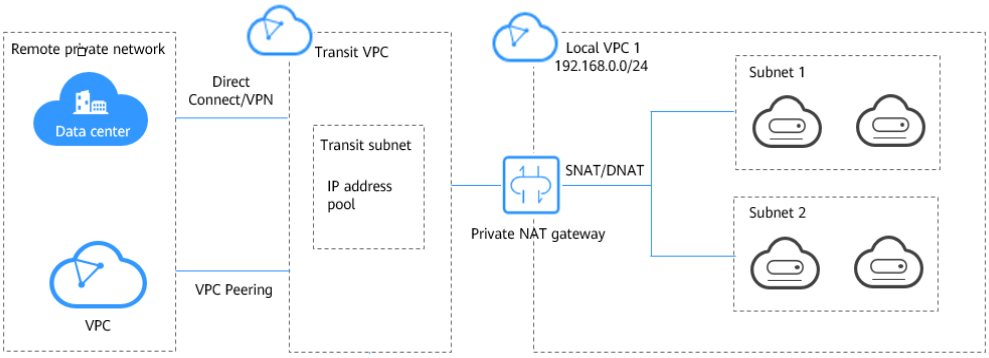
Transit IP Address

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

  Use APIs if you need to integrate NAT Gateway into your own system solution. For details, see the ***NAT Gateway API Reference***.

2 Product 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.

3 Scenarios

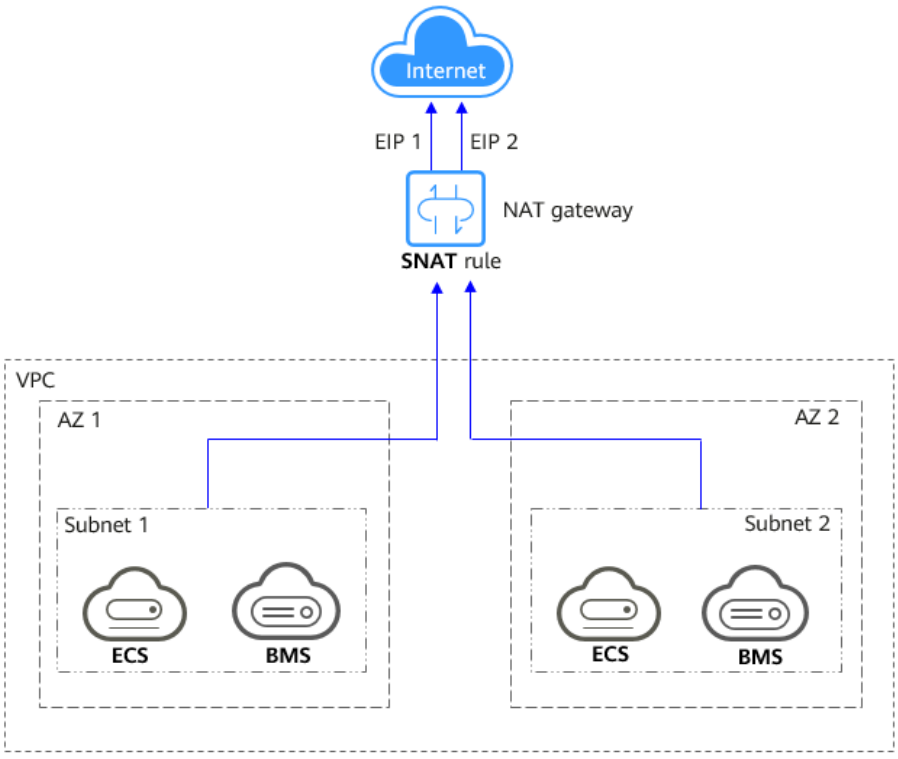
Public NAT Gateway

- **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 one or more 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 3-1 shows how servers in a VPC access the Internet using SNAT.

  Figure 3-1 Allowing a private network to access the Internet using SNAT



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

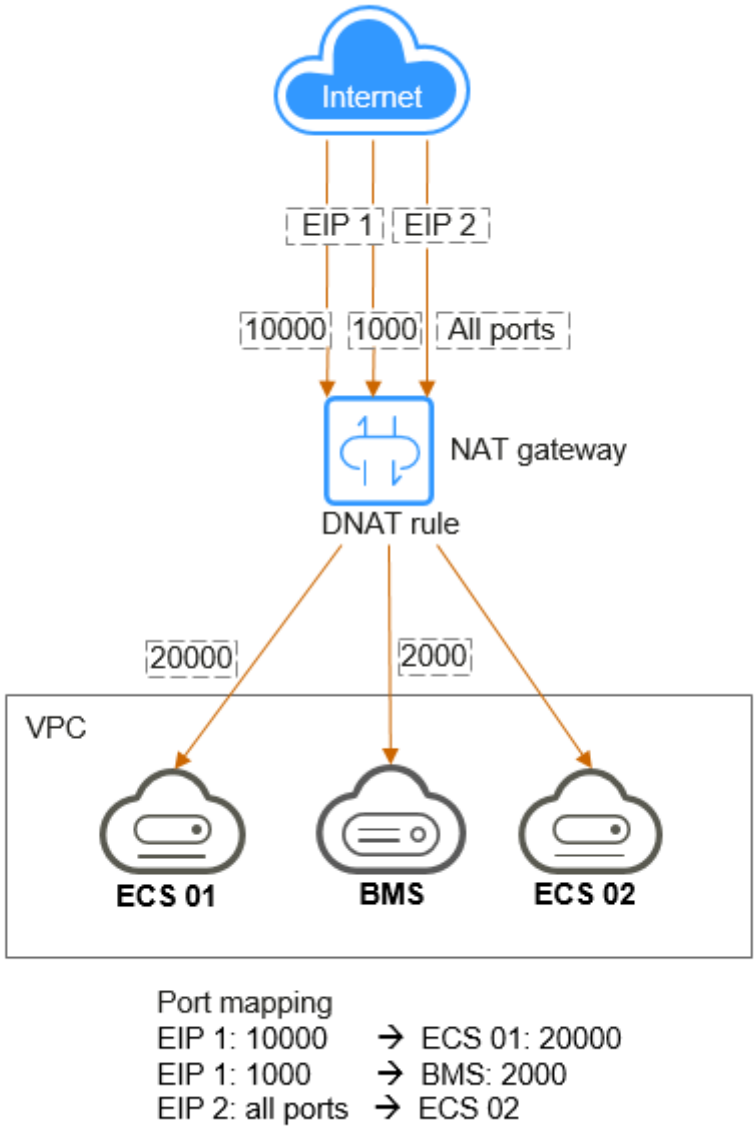
  DNAT rules enable servers in a VPC to provide services accessible from the Internet.

  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 3-2 shows how servers (ECSs or BMSs) in a VPC provide services accessible from the Internet using DNAT.

Figure 3-2 Allowing Internet users to access a service in a private network using DNAT

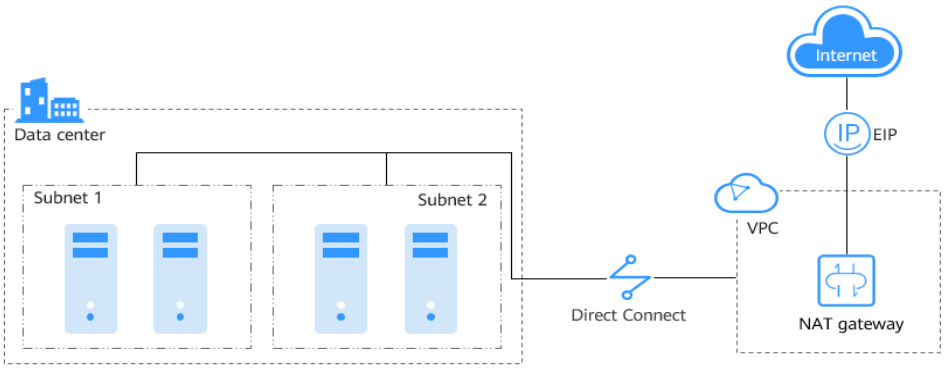


- **Allowing servers in an on-premises data center to communicate with the Internet**

  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 3-3 shows how to use SNAT and DNAT to provide high-speed Internet access or provide services accessible from the Internet.

Figure 3-3 Allowing servers in an on-premises data center to communicate with the Internet



- **Setting up a highly available system by adding multiple EIPs to an SNAT rule**

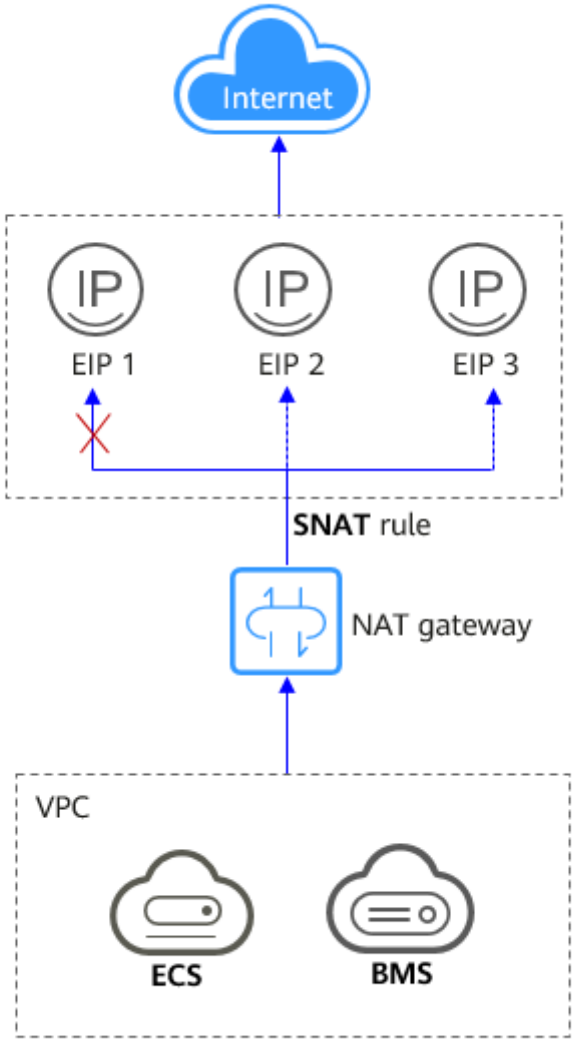
  EIPs may be attacked. To improve system reliability, you can bind multiple EIPs to an SNAT rule so that if one EIP is attacked, another EIP can be used to ensure service continuity.

  Each SNAT rule can have up to 20 EIPs. If an SNAT rule has multiple EIPs, the system randomly selects one EIP for servers to use to access the Internet.

  If any EIP is blocked or attacked, manually remove it from the EIP pool.

  Figure 3-4 shows a highly available system using an SNAT rule of a public NAT gateway.

Figure 3-4 Using the SNAT rule of a public NAT gateway to build a highly available system



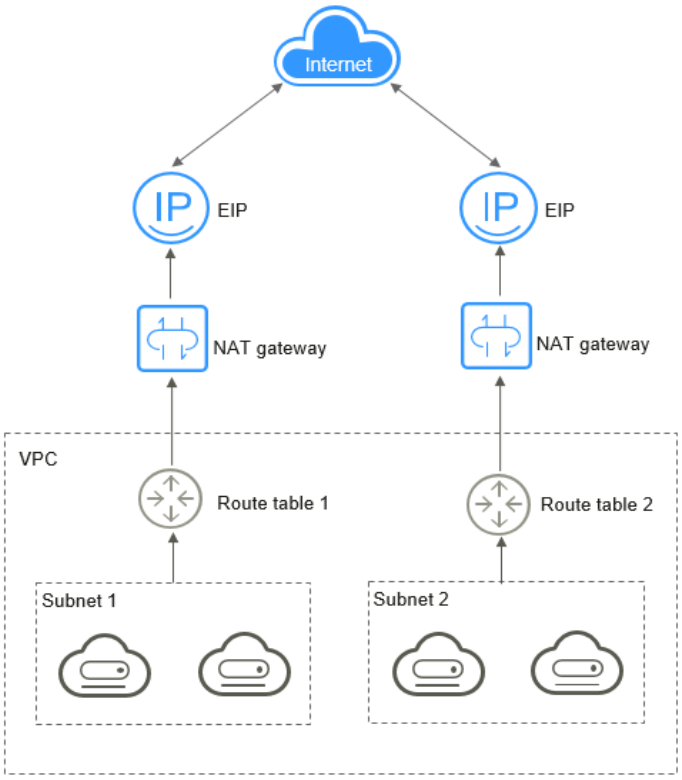
- **Using multiple NAT gateways together**

  If a single NAT gateway bottlenecks your services, for example, if there are over one million SNAT connections, or if the maximum bandwidth of 20 Gbit/s cannot meet service requirements, you can use multiple ones.

  To use multiple NAT gateways together, associate route tables of the VPC subnets with these public NAT gateways.

  Figure 3-5 shows how multiple public NAT gateways are used to overcome the performance bottleneck.

Figure 3-5 Using multiple public NAT gateways together



NOTE

- The system does not add a default route for a public NAT gateway. You need to add a route pointing to the public NAT gateway to the corresponding route table.
- Each public NAT gateway has an associated route table. The number of public NAT gateways that can be created in a VPC is determined by the number of route tables for the VPC.

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.

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

The default timeout period of an SNAT connection over TCP is 900 seconds.

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

Select a public NAT gateway based on your service requirements. **Table 4-1** lists the public NAT gateway specifications.

Table 4-1 Public NAT gateway specifications

Specifications	Maximum Number of SNAT Connections	Bandwidth	Packets per Second (PPS)
Small	10,000	20 Gbit/s	2,000,000
Medium	50,000	20 Gbit/s	2,000,000
Large	200,000	20 Gbit/s	2,000,000
Extra-large	1,000,000	20 Gbit/s	2,000,000

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.
- The DNAT rules of a public NAT gateway are irrelevant to the NAT gateway specifications. Up to 200 DNAT rules can be added to a public NAT gateway.

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 4-2** lists the private NAT gateway specifications.

Table 4-2 Private NAT gateway specifications

Specifications	Maximum Number of SNAT Connections	Bandwidth	PPS	Number of NAT Rules (SNAT Rules +DNAT Rules)
Small	2,000	200 Mbit/s	20,000	20
Medium	5,000	500 Mbit/s	50,000	50
Large	20,000	2 Gbit/s	200,000	200
Extra-large	50,000	5 Gbit/s	500,000	500

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.

5 Constraints and Limitations

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, an SNAT rule cannot share an EIP with a DNAT rule whose **Port Type** is set to **All ports**, because the resource in the DNAT rule will preferentially use all ports of the EIP.
  - The public NAT gateway does not translate IP addresses for Enterprise Edition VPN.
  - If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.
  - After you perform operations on backend resources, such as changing the specifications of an ECS, the existing NAT gateway rules will become invalid. Delete the rules and create some new rules for the ECS of the new specifications.
  - Private IP addresses used by load balancers cannot be selected when you add DNAT rules on public NAT gateways for Internet communications.
  - Some carriers will block the following ports for security reasons. It is recommended that you do not use the following ports.

Protocol	Port
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

NOTE

- The system does not add a default route for a public NAT gateway. You need to add a route pointing to the public NAT gateway to the corresponding route table.
- Each public NAT gateway has an associated route table. The number of public NAT gateways that can be created in a VPC is determined by the number of route tables for the VPC.

- 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.
  - 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**.

6 Using NAT Gateway with Other Services

Figure 6-1 shows the relationship between NAT Gateway and other services.

Figure 6-1 Relationship between NAT Gateway and other services

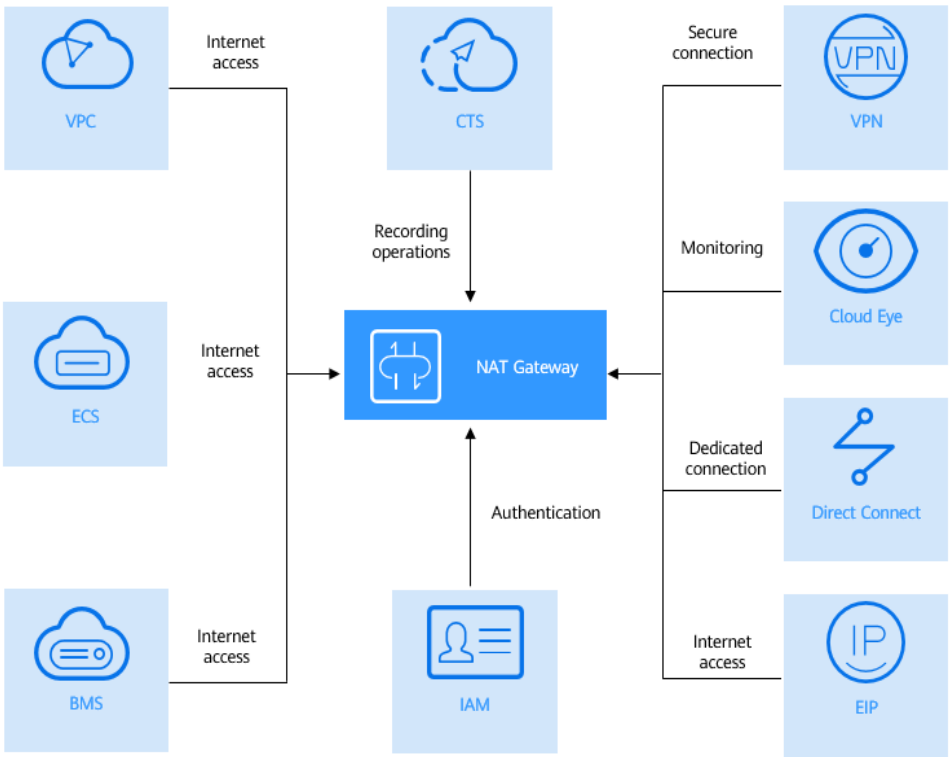


Table 6-1 Related services

Cloud Service	Interaction	Reference
Direct Connect	On-premises servers connected to a VPC through Direct Connect can use a public NAT gateway to communicate with the Internet.	**Allowing On-Premises Servers to Communicate with the Internet**
Virtual Private Network (VPN)	A VPN establishes an encrypted, Internet-based communication tunnel between your on-premises network and a VPC. This ensures secure access to the Internet through a public NAT gateway.	**Allowing On-Premises Servers to Communicate with the Internet**
ECS and BMS	ECSs and BMSs can use a public NAT gateway to communicate with the Internet.	**Allowing a Private Network to Access the Internet Using SNAT** **Allowing Internet Users to Access a Service in a Private Network Using DNAT**
VPC	ECSs in a VPC can connect to the Internet.	**Allowing a Private Network to Access the Internet Using SNAT**
Elastic IP (EIP)	With a public NAT gateway, servers in a VPC can share an EIP to access the Internet or provide Internet-accessible services.	**Allowing a Private Network to Access the Internet Using SNAT** **Allowing Internet Users to Access a Service in a Private Network Using DNAT**
Cloud Eye	You can view NAT gateway monitoring data on the Cloud Eye console.	**Viewing Metrics**
Identity and Access Management (IAM)	If you need to assign different permissions to employees in your enterprise to control their access to your NAT Gateway resources, IAM is a good choice for fine-grained permissions management.	**Identity and Access Management**

Cloud Service	Interaction	Reference
Cloud Trace Service (CTS)	With CTS, you can record operations on NAT Gateway for later query, audit, and backtracking.	Cloud Trace Service

7 Billing (Public NAT Gateway)

Billing Items

Public NAT gateways are billed based on the public NAT gateway specifications and the usage duration.

Four specifications of public NAT gateways are available: small, medium, large, and extra-large.

For pricing details, see **NAT Gateway Price Calculator**.

Billing Modes

Public NAT gateways are billed by day.

NOTE

The billing cycle of a pay-per-use (day) gateway is from 08:00 on the previous day to 08:00 on the next day. Any period less than one day is counted as one day.

For example, if you purchased a public NAT gateway at 6:00:00 on November 29, 2022 and deleted it at 7:59:59 on November 30, 2022, you will be charged for two days.

Configuration Changes

If the NAT gateway specifications are changed, the NAT gateway with more robust specifications will be billed on that day.

Unsubscription

To unsubscribe from a pay-per-use public NAT gateway, you only need to **delete it**.

8 Billing (Private NAT Gateway)

This section describes the billing details about private NAT gateways.

Billing Items

Private NAT gateways are billed based on the private NAT gateway specifications and the usage duration.

Four specifications of private NAT gateways are available: small, medium, large, and extra-large.

Billing Modes

Private NAT gateways are billed by hour.

Configuration Changes

New specifications take effect immediately upon change. You are then charged based on the new specifications.

Unsubscription

To unsubscribe from a pay-per-use private NAT gateway, you only need to **delete it**.

9 Permissions

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

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

If your account does not require individual IAM users for permissions management, 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 **What Is IAM?**

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. 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 **Permissions Policies and Supported Actions**.

Table 9-1 lists all the system-defined roles and policies supported by NAT Gateway.

Table 9-1 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** permission.	System-defined role

Table 9-2 lists the common operations supported by each NAT Gateway system policy or role. Select the policies or roles as required.

Table 9-2 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	√	√	√

Operation	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
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	√
Deleting DNAT rules in one batch	√	x	√
Importing DNAT rules using templates	√	x	√
Exporting DNAT rules using templates	√	√	√
Creating a transit subnet	√	x	√
Querying transit subnets	√	√	√
Querying details about a transit subnet	√	√	√
Modifying a transit subnet	√	x	√
Deleting a transit subnet	√	x	√
Assigning a transit IP address	√	x	√

Operation	NAT FullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Querying a transit IP address	√	√	√
Releasing a transit IP address	√	x	√

NOTE

- Note the following when creating a NAT gateway:
  - To create a yearly/monthly NAT gateway, you also need to obtain the **BSS Administrator** permissions of the Billing Center. For details, see the *Billing Center User Guide*.
- 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*.

NOTE

- 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*.
- To query predefined tags, obtain the **TMS Administrator** permissions. For details, see the *Tag Management Service API Reference*.

Helpful Links

- **What Is IAM?**
- **Creating a User and Granting NAT Gateway Permissions**
- **Permissions Policies and Supported Actions**

10 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.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. to support high-availability systems.

Selecting a Region

If your target users are in Europe, select the **EU-Dublin** region.

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.

11 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. If you want ECSs in the same VPC to share an EIP, you have to use a NAT gateway. For more information, see the **NAT Gateway User Guide**.

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 is the EIP, and the source port is the EIP port. An SNAT connection uniquely identifies a session.

DNAT Connections

DNAT connections enable servers in a private network to share an EIP to provide services accessible from the Internet.

12 Change History

Released On	Description
2022-11-29	This issue is the second official release, which incorporates the following change: Added the pay-per-use (day) billing cycle for public NAT gateways in **Billing (Public NAT Gateway)**.
2022-08-30	This issue is the first official release.

