



NAT Gateway

User Guide

Date **2020-01-02**

Contents

1 Overview.....	1
1.1 What Is NAT Gateway?.....	1
1.2 Product Advantages.....	4
1.3 Scenarios.....	5
1.4 NAT Gateway Specifications.....	8
1.5 Constraints and Limitations.....	9
1.6 Using NAT Gateway with Other Services.....	11
1.7 Billing	13
1.8 Permissions.....	13
1.9 Region and AZ.....	16
1.10 Basic Concepts.....	17
2 Getting Started.....	19
2.1 Allowing a Private Network to Access the Internet Using SNAT.....	19
2.1.1 Overview.....	19
2.1.2 Step 1: Assign an EIP.....	20
2.1.3 Step 2: Create a Public NAT Gateway.....	20
2.1.4 Step 3: Add an SNAT Rule.....	22
2.1.5 Step 4: Test the Connection.....	23
2.2 Allowing Internet Users to Access a Service in a Private Network Using DNAT.....	24
2.2.1 Overview.....	24
2.2.2 Step 1: Assign an EIP.....	25
2.2.3 Step 2: Create a Public NAT Gateway.....	25
2.2.4 Step 3: Add a DNAT Rule.....	27
2.2.5 Step 4: Test the Connection.....	29
2.3 Allowing On-Premises Servers to Communicate with the Internet.....	30
2.3.1 Overview.....	30
2.3.2 Step 1: Connect Your On-premises Data Center to the Cloud with Direct Connect.....	31
2.3.3 Step 2: Assign an EIP.....	31
2.3.4 Step 3: Create a Public NAT Gateway.....	32
2.3.5 Step 4: Add an SNAT Rule.....	34
2.3.6 Step 5: Add a DNAT Rule.....	35
2.4 Using Private NAT Gateways to Enable Communications Between Cloud and On-premises Networks.....	37

2.4.1 Overview.....	37
2.4.2 Step 1: Create a Service VPC and a Transit VPC.....	38
2.4.3 Step 2: Create a Direct Connect Connection.....	38
2.4.4 Step 3: Create a Private NAT Gateway.....	39
2.4.5 Step 4: Add an SNAT Rule.....	41
2.4.6 Step 5: Add a Route.....	42
2.4.7 Step 6: Add a Security Group Rule.....	43
2.5 Using Multiple Public NAT Gateways Together in Performance-Demanding Scenarios.....	44
2.5.1 Overview.....	44
2.5.2 Step 1: Create a VPC and Two Subnets.....	45
2.5.3 Step 2: Create a Public NAT Gateway.....	45
2.5.4 Step 3: Check the Default Route.....	47
2.5.5 Step 4: Create a Route Table.....	47
2.5.6 Step 5: Create Another Public NAT Gateway.....	48
2.5.7 Step 6: Add the Default Route.....	50
3 Public NAT Gateways.....	52
3.1 Public NAT Gateway Overview.....	52
3.2 Managing Public NAT Gateways.....	53
3.2.1 Creating a Public NAT Gateway.....	53
3.2.2 Viewing a Public NAT Gateway.....	55
3.2.3 Modifying a Public NAT Gateway.....	56
3.2.4 Deleting a Public NAT Gateway.....	56
3.3 Managing SNAT Rules.....	57
3.3.1 Adding an SNAT Rule.....	57
3.3.2 Viewing an SNAT Rule.....	58
3.3.3 Modifying an SNAT Rule.....	59
3.3.4 Deleting an SNAT Rule.....	59
3.4 Managing DNAT Rules.....	60
3.4.1 Adding a DNAT Rule.....	60
3.4.2 Viewing a DNAT Rule.....	61
3.4.3 Modifying a DNAT Rule.....	62
3.4.4 Deleting a DNAT Rule.....	62
3.4.5 Deleting DNAT Rules in Batches.....	63
3.4.6 Importing and Exporting DNAT Rules Using Templates.....	63
4 Private NAT Gateways.....	66
4.1 Private NAT Gateway Overview.....	66
4.2 Creating a Private NAT Gateway.....	67
4.2.1 Overview.....	67
4.2.2 Creating a Private NAT Gateway.....	68
4.2.3 Assigning a Transit IP Address.....	70
4.2.4 Adding an SNAT Rule.....	71
4.2.5 Adding a DNAT Rule.....	73

4.3 Managing Private NAT Gateways.....	76
4.3.1 Viewing a Private NAT Gateway.....	76
4.3.2 Modifying a Private NAT Gateway.....	76
4.3.3 Deleting a Private NAT Gateway.....	77
4.4 Managing SNAT Rules.....	77
4.4.1 Viewing an SNAT Rule.....	77
4.4.2 Modifying an SNAT Rule.....	78
4.4.3 Deleting an SNAT Rule.....	78
4.5 Managing DNAT Rules.....	79
4.5.1 Viewing a DNAT Rule.....	79
4.5.2 Modifying a DNAT Rule.....	79
4.5.3 Deleting a DNAT Rule.....	80
4.6 Managing Transit IP Addresses.....	80
4.6.1 Assigning a Transit IP Address.....	81
4.6.2 Viewing a Transit IP Address.....	81
4.6.3 Releasing a Transit IP Address.....	82
4.7 Accessing On-Premises Data Centers or Other VPCs.....	82
5 Permissions Management.....	83
5.1 Creating a User and Granting NAT Gateway Permissions.....	83
5.2 NAT Gateway Custom Policies.....	84
6 Monitoring.....	87
6.1 Supported Metrics.....	87
6.2 Creating Alarm Rules.....	91
6.3 Viewing Metrics.....	94
6.4 Viewing Metrics of Resources Using a NAT Gateway.....	94
7 FAQs.....	96
7.1 Public NAT Gateways.....	96
7.1.1 What Is the Relationship Between a VPC, Public NAT Gateway, EIP Bandwidth, and ECS?.....	96
7.1.2 How Does a Public NAT Gateway Offer High Availability?.....	96
7.1.3 Which Ports Cannot Be Accessed?.....	96
7.1.4 What Are the Differences Between Using a NAT Gateway and Using an EIP for an ECS?.....	97
7.1.5 What Should I Do If I Fail to Access the Internet Through a NAT Gateway?.....	97
7.1.6 Can I Change the VPC for a NAT Gateway?.....	97
7.1.7 What Is the Quota of the NAT Gateway?.....	97
7.1.8 Can I Update NAT Gateways and SNAT Rules?.....	98
7.1.9 Does NAT Gateway Support IPv6 Addresses?.....	98
7.1.10 What Security Policies Can I Configure to Implement Access Control If I Use a NAT Gateway?.....	98
7.1.11 What Can I Do If Connection Between My Servers and the Internet Fails After I Add SNAT and DNAT Rules?.....	98
7.2 Private NAT Gateways.....	106
7.2.1 How Do I Troubleshoot a Network Failure After a Private NAT Gateway Is Configured?.....	106
7.2.2 How Many Private NAT Gateways Can I Create in a VPC?.....	107

7.2.3 Can I Increase the Numbers of SNAT and DNAT Rules Supported by a Private NAT Gateway?..... 107

7.2.4 Can an SNAT Rule and a DNAT Rule of a Private NAT Gateway Share the Same Transit IP Address?
..... 107

7.2.5 Can Private NAT Gateways Translate On-premises IP Addresses Connected to the Cloud Through
Direct Connect?..... 107

7.2.6 What Are the Differences Between Private NAT Gateways and Public NAT Gateways?..... 107

7.2.7 Can a Private NAT Gateway Be Used Across ?..... 108

7.3 SNAT Rules..... 108

7.3.1 Why Do I Need SNAT?..... 108

7.3.2 What Are SNAT Connections?..... 108

7.3.3 What Is the Bandwidth of a NAT Gateway That Is Used by Servers to Access the Internet? How Do I
Configure the Bandwidth?..... 108

7.3.4 How Do I Resolve Packet Loss or Connection Failure Issues When Using a NAT Gateway?..... 109

7.3.5 What Should I Do If My ECS Fails to Access a Server on the Public Network Through a NAT
Gateway?..... 109

7.3.6 What Are the Relationships and Differences Between the CIDR Blocks in a NAT Gateway and in an
SNAT Rule?..... 110

7.4 DNAT Rules..... 110

7.4.1 Why Do I Need DNAT?..... 110

7.4.2 Can I Modify DNAT Rules?..... 110

A Change History..... 111

1 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

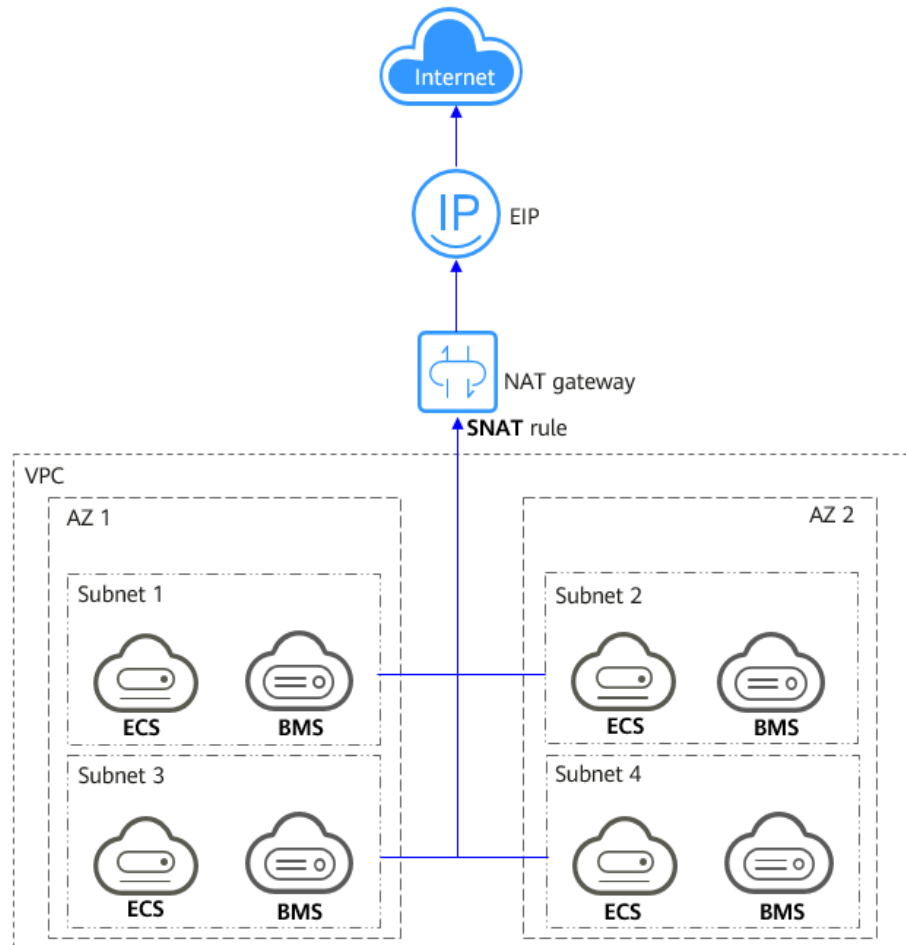
A public NAT gateway enables cloud and on-premises servers in a private subnet to share an EIP to access the Internet or provide services accessible from the Internet. Cloud servers are ECSs and BMSs in a VPC. On-premises servers are servers in on-premises data centers that connect to a VPC through Direct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

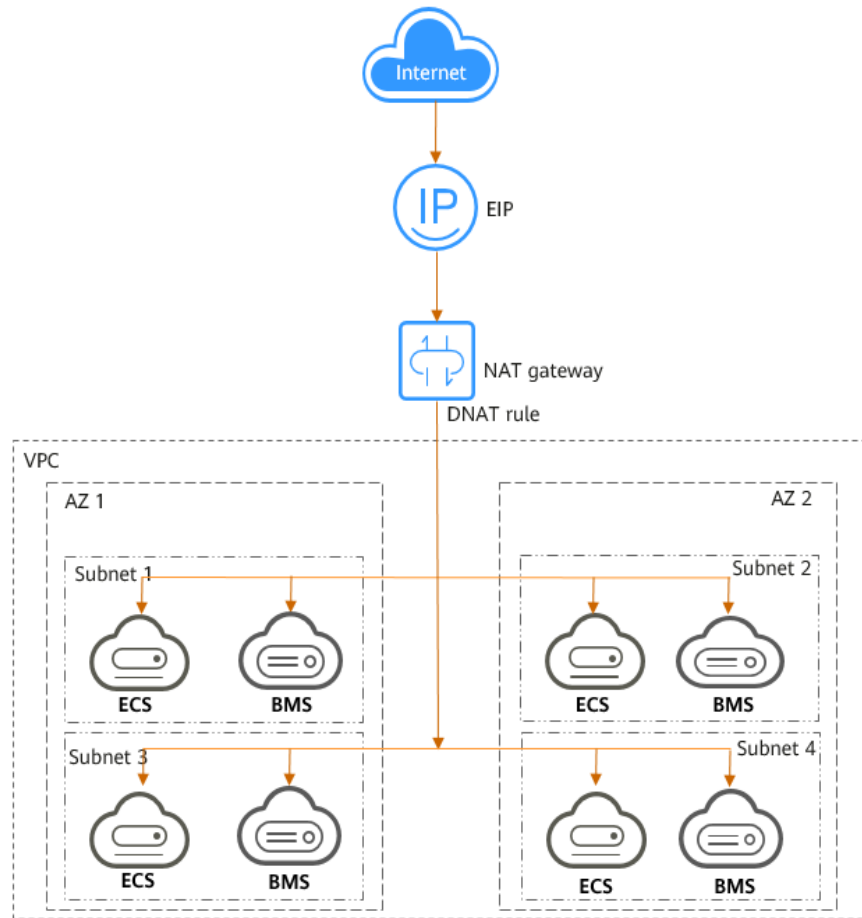
Figure 1-1 NAT gateway with an SNAT rule



- DNAT enables servers 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.

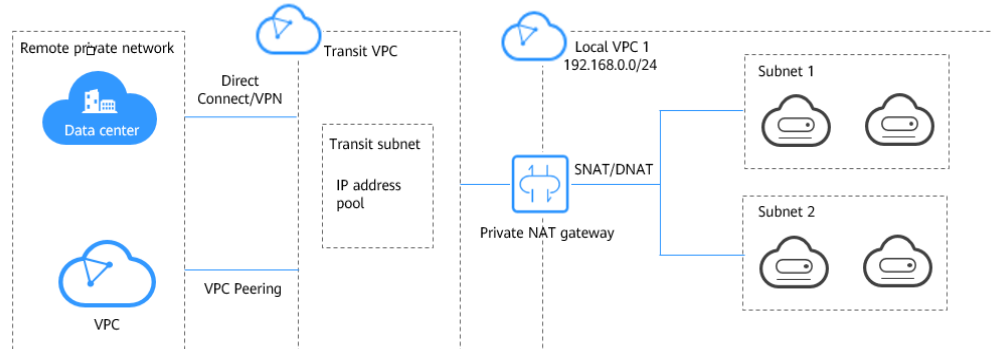
Transit IP Address

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*.

1.2 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.

1.3 Scenarios

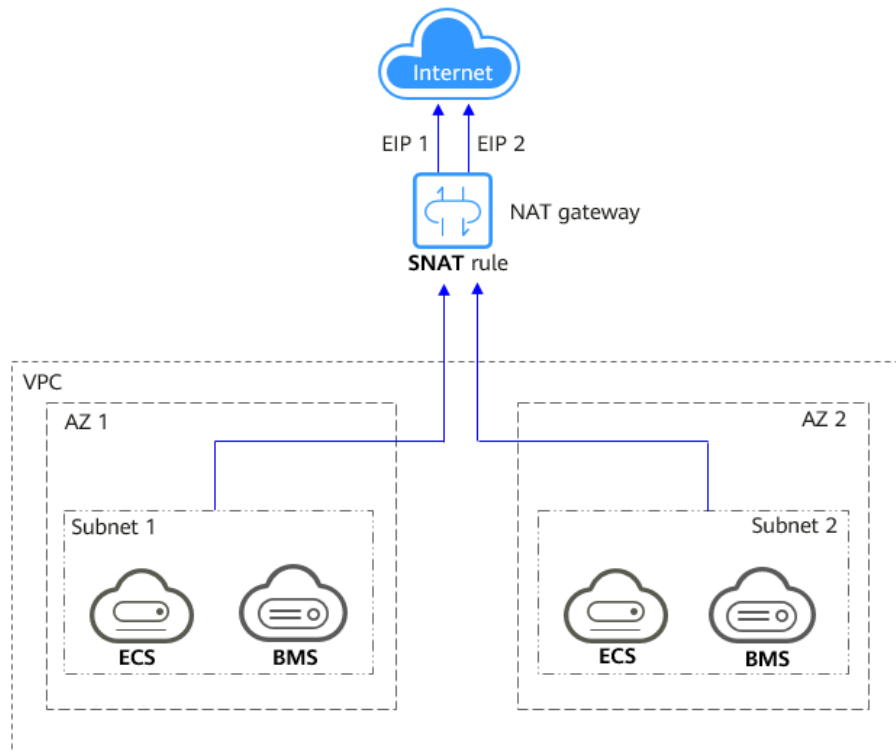
Public NAT Gateway

- **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 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**

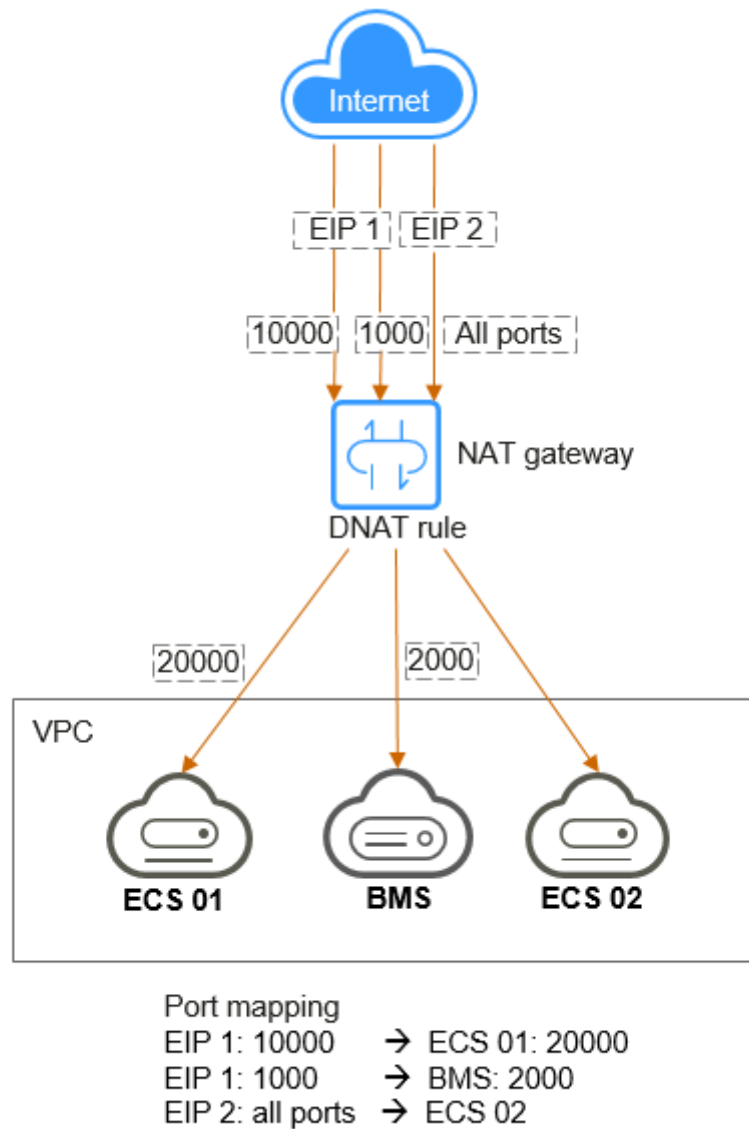
DNAT rules enable servers in a VPC to provide services accessible from the Internet.

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

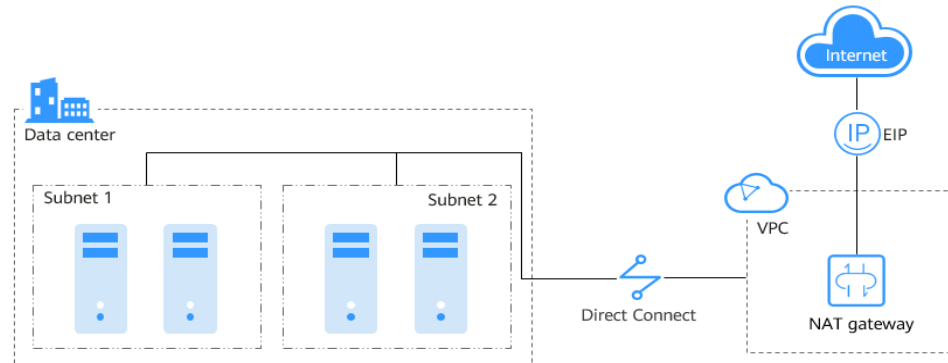


- **Allowing on-premises servers to communicate with the Internet**

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



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	Maximum Number of SNAT Connections	Bandwidth
Small	10,000	20 Gbit/s
Medium	50,000	20 Gbit/s
Large	200,000	20 Gbit/s
Extra-large	1,000,000	20 Gbit/s

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	Maximum Number of SNAT Connections	Bandwidth
Small	2,000	200 Mbit/s
Medium	5,000	500 Mbit/s
Large	20,000	2 Gbit/s
Extra-large	50,000	5 Gbit/s

 **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 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 have only one NAT gateway.
 - Each VPC can be associated with multiple public NAT gateways.
 - SNAT and DNAT rules cannot use the same EIP.
 - If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.
 - Some carriers will block the following ports for security reasons. It is recommended that you do not use the following ports.

Proto col	Port
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996

Protocol	Port
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

- 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
 - DNAT rules cannot map virtual IP addresses to EIPs.
 - 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 Using NAT Gateway with Other Services

Figure 1-7 shows the relationship between NAT Gateway and other services.

Figure 1-7 Relationship between NAT Gateway and other services

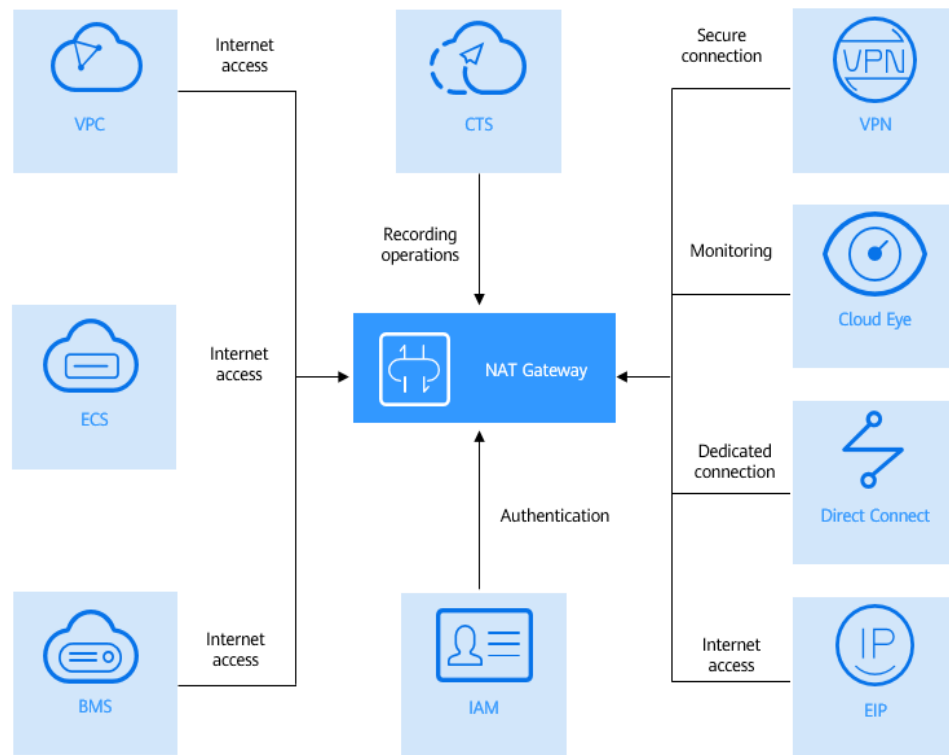


Table 1-3 Related services

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

Cloud Service	Interaction	Reference
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.	<i>Identity and Access Management User Guide</i>
Cloud Trace Service (CTS)	With CTS, you can record operations on NAT Gateway for later query, audit, and backtracking.	<i>Cloud Trace Service User Guide</i>

1.7 Billing

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.

 **NOTE**

Currently, private NAT gateways are free of charge.

Billing Modes

 **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.

1.8 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.

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 the *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. 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 1-4 lists all the system-defined roles and policies supported by NAT Gateway.

Table 1-4 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 1-5 lists the common operations supported by each NAT Gateway system policy or role. Select the policies or roles as required.

Table 1-5 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	√	√	√

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

 NOTE

- Note the following when creating a DNAT rule:
 - DNAT rule permissions cannot be managed by enterprise project.
 - 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*.
- To query predefined tags, obtain the **TMS Administrator** permissions. For details, see the *Tag Management Service API Reference*.

Helpful Links

- [Creating a User and Granting NAT Gateway Permissions](#)

1.9 Region and AZ

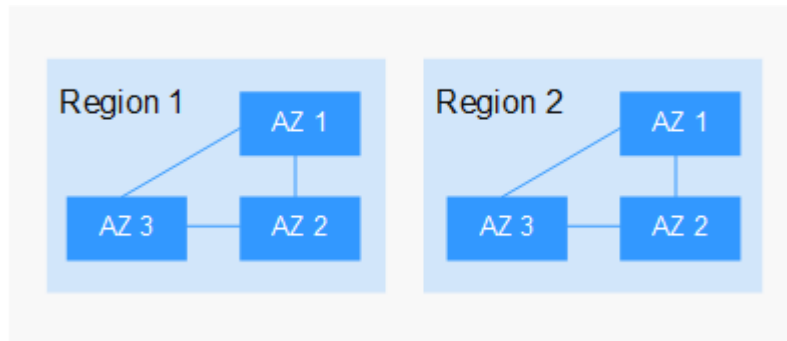
Concept

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](#).

1.10 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 in your subnet to enable the 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.

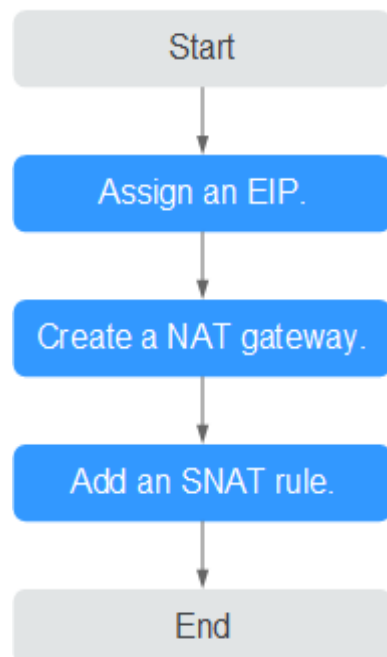
2 Getting Started

2.1 Allowing a Private Network to Access the Internet Using SNAT

2.1.1 Overview

If servers (ECSs and BMSs) without EIPs bound need to access the Internet, the servers can share one or more EIPs to access the Internet through a NAT gateway. This method provides access without exposing their IP addresses.

Figure 2-1 Flowchart



2.1.2 Step 1: Assign an EIP

Scenarios

You can assign an EIP for your NAT gateway so that servers in a VPC can use this EIP to access the Internet.

Procedure

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

You do not need to bind the EIP to any server.

2.1.3 Step 2: Create a Public NAT Gateway

Scenarios

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

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. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create NAT Gateway**.
4. Configure required parameters. For details, see [Table 2-1](#).

Table 2-1 Descriptions of public NAT gateway parameters

Parameter	Description
Region	The region where the public NAT gateway is located

Parameter	Description
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed.
VPC	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.
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 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.
Specifications	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.
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** to create a public NAT gateway.
It takes 1 to 6 minutes to create a public NAT gateway.
7. In the list, view the status of the public NAT gateway.

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. The following describes how to add a route to a custom route table.

Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the **Route Tables** page, click **Create Route Table** in the upper right corner.
VPC: Select the VPC to which the public NAT gateway belongs.
5. After the custom route table is created, click its name.
The **Summary** page is displayed.
6. 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.
7. Click **OK**.

2.1.4 Step 3: Add an SNAT Rule

Scenarios

After creating a public NAT gateway, add an SNAT rule to enable your servers in a specific subnet to access the Internet through the same EIP.

One SNAT rule can be configured for only one subnet or CIDR block. If there are multiple subnets or CIDR blocks in a VPC, you can add multiple SNAT rules to allow servers to share EIPs.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** 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. [Table 2-2](#) describes the parameters.

Table 2-2 Descriptions of SNAT rule parameters

Parameter	Description
Scenario	Select VPC if your servers in a VPC will use the SNAT rule to access the Internet.
CIDR Block	The CIDR block is a subset of the NAT gateway's VPC subnets Servers whose IP addresses in the CIDR block can use the SNAT rule to access the Internet.
EIP	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.
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.

2.1.5 Step 4: Test the Connection

Scenarios

After adding an SNAT rule, you can perform the following steps to verify the connection:

1. Verify that the SNAT rule has been added for the public NAT gateway.
2. Verify that servers that have no EIP bound can access the Internet through the NAT gateway.

Prerequisites

An SNAT rule has been added.

Verifying that the SNAT Rule Has Been Added

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
3. On the **Public NAT Gateways** page, click the name of the public NAT gateway.

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

Verifying that Servers Can Access the Internet Through the NAT Gateway

- Step 1** Log in to the management console.
- Step 2** Log in to the server.
- Step 3** Verify that the server can access the Internet.

Figure 2-2 Verification result

```
[root@ecs-test-nat-~]# TMOU=0
[root@ecs-test-nat-~]# 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-~]#
```

Figure 2-3 Failed to access the Internet

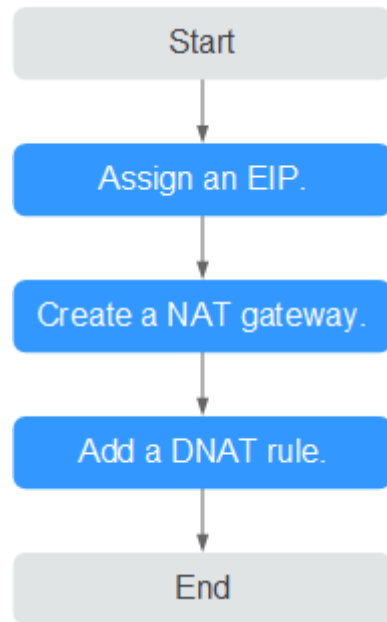
```
[root@ecs-test-nat-~]# TMOU=0
[root@ecs-test-nat-~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=53.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=53.3 ms
64 bytes from 8.8.8.8: 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-~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
^C
-- 8.8.8.8 ping statistics --
21 packets transmitted, 0 received, 100% packet loss, time 19999ms
[root@ecs-test-nat-~]#
```

----End

2.2 Allowing Internet Users to Access a Service in a Private Network Using DNAT

2.2.1 Overview

When one or more servers (ECSs and BMSs) in a VPC need to provide services accessible from the Internet, you can add DNAT rules.

Figure 2-4 Flowchart

2.2.2 Step 1: Assign an EIP

Scenarios

You can buy an EIP for your NAT gateway so that servers in a VPC can use this EIP to provide services accessible from the Internet.

Procedure

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

You do not need to bind the EIP to any server.

2.2.3 Step 2: Create a Public NAT Gateway

Scenarios

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

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. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create NAT Gateway**.
4. Configure required parameters. For details, see [Table 2-3](#).

Table 2-3 Descriptions of public NAT gateway parameters

Parameter	Description
Region	The region where the public NAT gateway is located
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed.
VPC	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.
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 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.

Parameter	Description
Specifications	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.
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** to create a public NAT gateway.
It takes 1 to 6 minutes to create a public NAT gateway.
7. In the list, view the status of the public NAT gateway.

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. The following describes how to add a route to a custom route table.

Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the **Route Tables** page, click **Create Route Table** in the upper right corner.
VPC: Select the VPC to which the public NAT gateway belongs.
5. After the custom route table is created, click its name.
The **Summary** page is displayed.
6. 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.
7. Click **OK**.

2.2.4 Step 3: Add 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.

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

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** 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 2-4](#).

Table 2-4 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	Select VPC if your servers in a VPC need to share an EIP 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.
EIP	The EIP of the public NAT gateway 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.

Parameter	Description
Instance Type	The type of the instance that will be providing services accessible from the Internet. Possible values are: <ul style="list-style-type: none"> • Server • Virtual IP address • Custom
NIC	The NIC of the server. This parameter is available if you set Instance Type to Server .
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

7. 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.

2.2.5 Step 4: Test the Connection

Scenarios

After adding a DNAT rule, you can perform the following steps to verify the connection:

1. Verify that the DNAT rule has been added for the public NAT gateway.
2. Check whether ECS 01 in the private network can be accessed by ECS 02 from the Internet through the NAT gateway (EIP 120.46.131.153 bound to the DNAT rule).

Prerequisites

A DNAT rule has been added.

Verifying that the DNAT Rule Has Been Added

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
3. On the **Public NAT Gateways** page, click the name of the public NAT gateway.
4. In the **DNAT Rules** tab, view details about the DNAT rule and check whether the DNAT rule has been created.
If **Status** of the DNAT rule is **Running**, the DNAT rule has been created.

Verifying that Servers in a VPC Can Be Accessed from the Internet Through the NAT Gateway

- Step 1** Log in to the management console.
- Step 2** Log in to ECS 02 with an EIP bound.
- Step 3** 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 2-5 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-~]#
```

Figure 2-6 Failed to be accessed from the Internet

```
[root@ecs-~]# ping 120.46.131.153
PING 120.46.131.153 (120.46.131.153) 56(84) bytes of data.
^C
--- 120.46.131.153 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5104ms
[root@ecs-~]#
```

----End

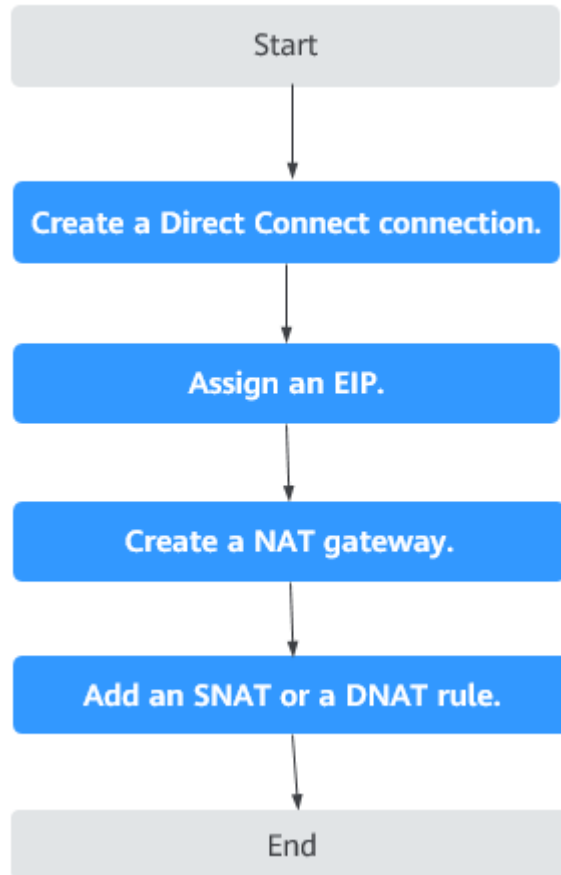
2.3 Allowing On-Premises Servers to Communicate with the Internet

2.3.1 Overview

You need to first create a Direct Connect or VPN connection to connect your servers in the on-premises data center to the cloud, and then create public NAT gateways and configure SNAT or DNAT rules to allow servers in your data center to access the Internet or to provide services accessible from the Internet. [Figure](#)

2-7 shows how servers in an on-premises data center communicate with the Internet.

Figure 2-7 Servers in an on-premises data center communicating with the Internet



2.3.2 Step 1: Connect Your On-premises Data Center to the Cloud with Direct Connect

Scenarios

Create a Direct Connect connection to link your on-premises data center to a VPC. Then deploy a public NAT gateway in the VPC to allow your on-premises servers to communicate with the Internet.

Procedure

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

2.3.3 Step 2: Assign an EIP

Scenarios

Buy an EIP for a NAT gateway to allow servers that are connected to the cloud using Direct Connect to communicate with the Internet.

Procedure

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

You do not need to bind the EIP to any server.

2.3.4 Step 3: Create a Public NAT Gateway

Scenarios

Create a public NAT gateway.

Prerequisites

- You have created the VPC and subnet required for creating a public NAT gateway.
- 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. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create NAT Gateway**.
4. Configure required parameters. For details, see [Table 2-5](#).

Table 2-5 Descriptions of public NAT gateway parameters

Parameter	Description
Region	The region where the public NAT gateway is located
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed.

Parameter	Description
VPC	<p>The VPC that the public NAT gateway belongs to The selected VPC cannot be changed after you create the public NAT gateway.</p> <p>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.</p>
Subnet	<p>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.</p>
Specifications	<p>The specifications of the public NAT gateway The value can be Small, Medium, Large, or Extra-large.</p>
Description	<p>Supplementary information about the public NAT gateway Enter up to 255 characters. Angle brackets (<>) are not allowed.</p>

5. Click **Create Now**. On the page displayed, confirm the public NAT gateway specifications.
6. If you do not need to modify the information, click **Submit**.
It takes 1 to 5 minutes to create a public NAT gateway.
7. In the public NAT gateway list, check the gateway status.
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. The following describes how to add a route to a custom route table.

Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the **Route Tables** page, click **Create Route Table** in the upper right corner.
VPC: Select the VPC to which the public NAT gateway belongs.
5. After the custom route table is created, click its name.
The **Summary** page is displayed.
6. 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.
7. Click **OK**.

2.3.5 Step 4: Add an SNAT Rule

Scenarios

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

Each SNAT rule is configured for only one CIDR block. If servers that are connected to a VPC using Direct Connect are in multiple CIDR blocks, you can create multiple SNAT rules to allow the servers to share EIPs.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** 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 2-6](#).

Table 2-6 Descriptions of SNAT rule parameters

Parameter	Description
Scenario	Select Direct Connect if your on-premises servers need to access the Internet.
CIDR Block	The CIDR block of the servers in the on-premises data center
EIP	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.
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. Click **OK**.
7. View details in the SNAT rule list.

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

 **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.

2.3.6 Step 5: Add a DNAT Rule

Scenarios

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

You can configure a DNAT rule for each port on a server. If there are multiple servers, you can create multiple DNAT rules.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** 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 2-7](#).

Table 2-7 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	Select Direct Connect if servers in your on-premises data center need 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.
EIP	The EIP of the public NAT gateway 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.
Instance Type	The type of the instance that will be providing services accessible from the Internet. Possible values are: <ul style="list-style-type: none"> • Server • Virtual IP address • Custom
NIC	The NIC of the server. This parameter is available if you set Instance Type to Server .
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

7. 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.

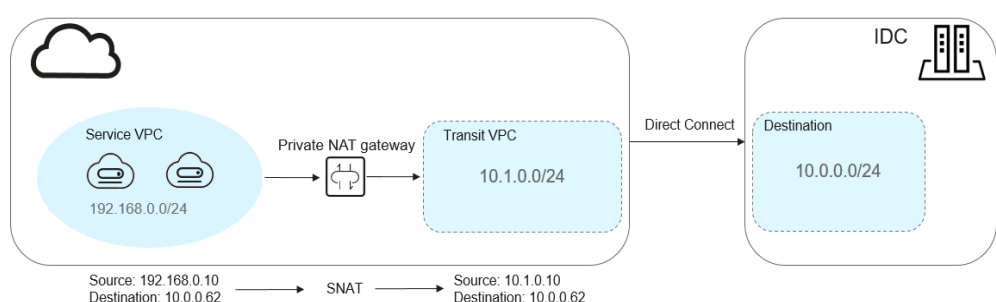
2.4 Using Private NAT Gateways to Enable Communications Between Cloud and On-premises Networks

2.4.1 Overview

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 2-8 Networking diagram



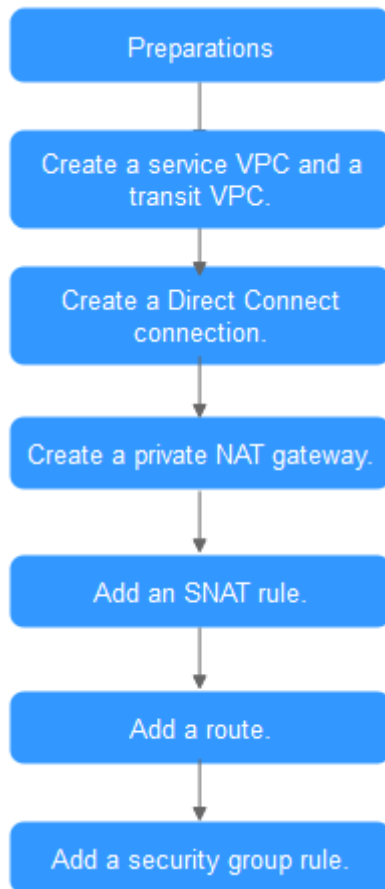
In this example, the CIDR block of your on-premises data center is 10.0.0.0/24. The subnet of the transit VPC in the region is 10.1.0.0/24.

How networks are connected to each other

1. Your on-premises data center is connected to the transit VPC using Direct Connect.
2. The VPC where your services are deployed is connected to the transit VPC using a private NAT gateway.

This following figure shows the procedure.

Figure 2-9 Procedure



2.4.2 Step 1: Create a Service VPC and a Transit VPC

Scenarios

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

Procedure

For details, see section "Creating a VPC" in the *Virtual Private Cloud User Guide*.

2.4.3 Step 2: Create a Direct Connect Connection

Scenarios

Create a Direct Connect connection to link your on-premises data center to the cloud (the region).

Procedure

Create a VPC peering connection to connect your local data center to a transit VPC. For details, see section "VPC Peering Connection" in the *Virtual Private Cloud User Guide*.

 **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 section "Overview" in the *Direct Connect User Guide*.

2.4.4 Step 3: Create a Private NAT Gateway

Scenarios

To enable communications between your service VPC and a remote private network or VPC, create a private NAT gateway.

Prerequisites

You have determined the transit IP addresses to be used for NAT in the transit VPC.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**. In the navigation pane on the left, choose **Private NAT Gateways**. The **Private NAT Gateways** page is displayed.
4. Click **Create Private NAT Gateway** in the upper right corner.
5. Configure required parameters. For details, see [Table 2-8](#).

Table 2-8 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 (_), and hyphens (-) are allowed.
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 of the service VPC The subnet must have at least one available IP address. The selected subnet cannot be changed after the private NAT gateway is created.

Parameter	Description
Specifications	The specifications of the private NAT gateway The value can be Small, Medium, Large, or Extra-large.
Description	Supplementary information about the private NAT gateway Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. Click **Create Now**.
7. In the private NAT gateway list, check the gateway status.
8. On the **Private NAT Gateways** page, click **Transit IP Addresses**.

Figure 2-10 Assign Transit IP Address

Assign Transit IP Address ×

Transit VPC C

Transit Subnets C

Transit IP Address Automatic Manual

Tag It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) C

You can add 10 more tags.

OK
Cancel

9. Configure required parameters. For details, see [Table 2-9](#).

Table 2-9 Parameter descriptions of a transit IP address

Parameter	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.

Parameter	Description
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 .

10. Set **Transit IP Address** to **Automatic** and click **OK**.

2.4.5 Step 4: Add 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.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**. In the navigation pane on the left, choose **Private NAT Gateways**. The **Private NAT Gateways** page is displayed.
4. In the private NAT gateway list, click the name of the private NAT gateway that you want to add an SNAT rule for.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

Figure 2-11 Add SNAT Rule

- Configure required parameters. For details, see .

Table 2-10 Description

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 to watch the number of SNAT connections.
Transit IP Address	The transit IP address you assigned in Step 3: Create a Private NAT Gateway
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

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

2.4.6 Step 5: Add a Route

Scenarios

After the private NAT gateway is configured, add a route in the route table of the service VPC to point to the private NAT gateway.

Procedure


- Log in to the management console.
- Click  in the upper left corner and select the desired region and project.
- Click **Service List** in the upper left corner. Under **Network**, select **Virtual Private Cloud**.
- In the navigation pane on the left, choose **Route Tables**.
- In the route table list, click the name of the route table associated the service VPC.
- Click **Add Route** and configure required parameters.

Table 2-11 Parameter descriptions

Parameter	Description
Destination	The destination CIDR block Set it to the CIDR block used by your on-premises data center.
Next Hop Type	Set it to NAT gateway .
Next Hop	Set Next Hop to the private NAT gateway.
Description	(Optional) Supplementary information about the route Enter up to 255 characters. Angle brackets (< or >) are not allowed.

7. Click **OK**.

2.4.7 Step 6: Add a Security Group Rule

Scenarios

Add an inbound security group rule to allow traffic to servers in the destination VPC.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Network**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control > Security Groups**. The security group list is displayed.
5. Locate the row that contains the target security group, and click **Manage Rule** in the **Operation** column. The page for configuring security group rules is displayed.
6. 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 2-12 Inbound rule parameter descriptions

Parameter	Description	Example Value
Protocol & Port	Protocol: network protocol The protocol can be All, TCP, UDP, ICMP, or GRE .	TCP

Parameter	Description	Example Value
	<p>Port: the port or port range over which the traffic can reach your ECS</p> <p>Supported range: 1 to 65535</p>	22 or 22-30
Type	<p>The IP address type. This parameter is available after the IPv6 function is enabled.</p> <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
Source	<p>The source of the security group rule</p> <p>The source can be an IP address or a security group to allow access from IP addresses or instances in another security group. For example:</p> <ul style="list-style-type: none"> • <i>xxx.xxx.xxx.xxx/32</i> (an IPv4 address) • <i>xxx.xxx.xxx.0/24</i> (a subnet) • 0.0.0.0/0 (all IP addresses) • sg-abc (a security group) 	0.0.0.0/0
Description	<p>(Optional) Supplementary information about the security group rule</p> <p>Enter up to 255 characters. Angle brackets (<>) are not allowed.</p>	N/A

7. Click **OK**.

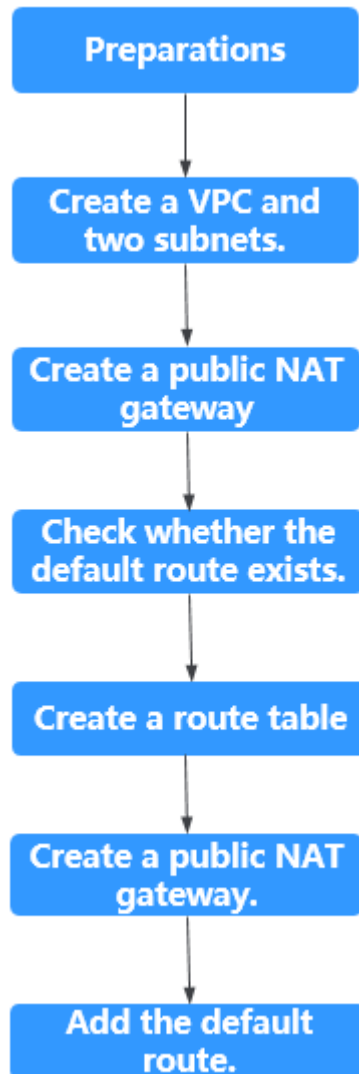
2.5 Using Multiple Public NAT Gateways Together in Performance-Demanding Scenarios

2.5.1 Overview

A single NAT gateway supports up to one million SNAT connections and 20 Gbit/s of bandwidth. If one NAT gateway cannot meet your requirements, you can use multiple NAT gateways.

This topic describes how to deploy multiple public NAT gateways.

Figure 2-12 Procedure



2.5.2 Step 1: Create a VPC and Two Subnets

Scenarios

Create one VPC and two subnets.

Procedure

For details, see section "Creating a VPC" in the *Virtual Private Cloud User Guide*.

2.5.3 Step 2: Create a Public NAT Gateway

Scenarios

Buy a public NAT gateway.

Prerequisites

A VPC is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create NAT Gateway**.
4. Configure required parameters. For details, see [Table 2-13](#).
Select the VPC and subnet you created in [Step 1: Create a VPC and Two Subnets](#) for **VPC** and **Subnet**.

Table 2-13 Descriptions of public NAT gateway parameters

Parameter	Description
Region	The region where the public NAT gateway is located
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) 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.
Subnet	The subnet of the VPC 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.
Specifications	The public NAT gateway specifications The value can be Small , Medium , Large , or Extra-large . To view more details about specifications, click Learn more on the page.
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** to create a public NAT gateway.
It takes 1 to 6 minutes to create a public NAT gateway.
7. In the list, view the status of the public NAT gateway.

2.5.4 Step 3: Check the Default Route

Scenarios

After the public NAT gateway is purchased, go to the route table list, locate the default route table of the VPC where you deploy the public NAT gateway, and check whether there is a default route with the next hop set to the public NAT gateway.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Network**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the route table list, click the name of the default route table of the VPC.
6. Go to the route table details page and check whether the default route pointing to the public NAT gateway.

NOTE

When the first public NAT gateway in a VPC is created, the default route (0.0.0.0/0) is automatically created in the default route table. If the default route already exists in the VPC, add a new route and set the next hop to the created public NAT gateway.

2.5.5 Step 4: Create a Route Table

Scenarios

Each public NAT gateway requires its unique route table. Create the second route table for the VPC.

NOTE

If the custom route table quota is insufficient, to increase the route table quota.

Prerequisites

A route table can be created in the VPC.

Procedure

1. Log in to the management console.

2. Click **Service List** in the upper left corner. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. In the upper right corner, click **Create Route Table**. On the displayed page, configure required parameters.

Table 2-14 Parameter descriptions

Parameter	Description	Example Value
Name	(Mandatory) The name of the route table Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. Spaces are not allowed.	rtb-001
VPC	(Mandatory) The VPC that the route table belongs to	vpc-001
Description	(Optional) Supplementary information about the route table Enter up to 255 characters. Angle brackets (<>) are not allowed.	N/A
Route Settings	Routes contained in the route table You can add a route when creating the route table or after the route table is created. You can click + to add more routes.	N/A

5. Click **OK**.
A message indicating that subnets can now be associated with the created route table is displayed. Perform the following steps to associate the other subnet of the VPC with the route table:
 - a. Click **Associate Subnet**.
The **Associated Subnets** tab is displayed.
 - b. Click **Associate Subnet** and select the second subnet created in [Step 1: Create a VPC and Two Subnets](#).
 - c. Click **OK**.

2.5.6 Step 5: Create Another Public NAT Gateway

Scenarios

Create another public NAT gateway in the service VPC.

Prerequisites

The second route table has been created for the VPC and has been associated with the second subnet of the VPC.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create NAT Gateway**.
4. Configure required parameters. For details, see [Table 2-15](#).
Select the VPC and the other subnet you created in [Step 1: Create a VPC and Two Subnets](#) for **VPC** and **Subnet**.

Table 2-15 Descriptions of public NAT gateway parameters

Parameter	Description
Region	The region where the public NAT gateway is located
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) 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.
Subnet	The subnet of the VPC 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.
Specifications	The public NAT gateway specifications The value can be Small , Medium , Large , or Extra-large . To view more details about specifications, click Learn more on the page.
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** to create a public NAT gateway.
It takes 1 to 6 minutes to create a public NAT gateway.
7. In the list, view the status of the public NAT gateway.

2.5.7 Step 6: Add the Default Route

Scenarios

If the VPC already has one or more NAT gateways configured, a route table must be created for the second public NAT gateway. You need to add the default route (0.0.0.0/0) with the next hop set to the second public NAT gateway in the new route table you have created.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Network**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the route table list, click the name of the route table to which you want to add a route.
6. Click **Add Route** and configure required parameters.


You can click  to add more routes.

Table 2-16 Parameter descriptions

Parameter	Description	Example Value
Destination	The destination CIDR block The destination of each route must be unique. The destination cannot overlap with any subnet in the VPC.	0.0.0.0/0
Next Hop Type	Type of the next hop	NAT gateway
Next Hop	Set the next hop. The resources in the drop-down list box are displayed based on the selected next hop type.	N/A
Description	(Optional) Supplementary information about the route Enter up to 255 characters. Angle brackets (< or >) are not allowed.	N/A

7. Click **OK**.

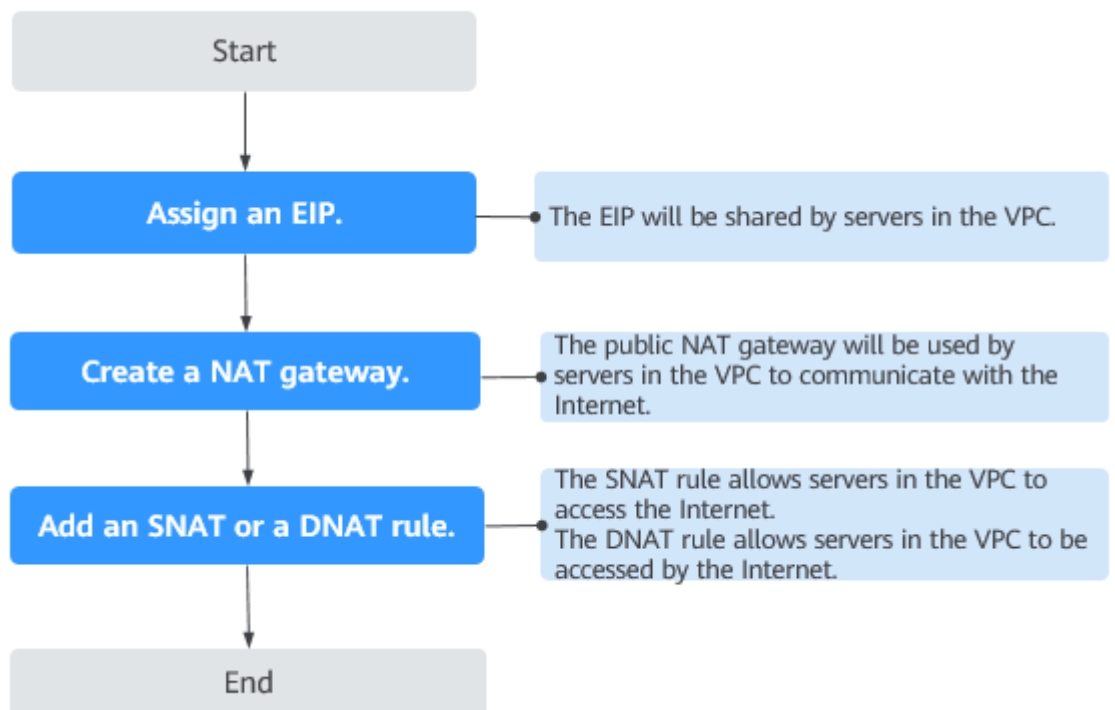
3 Public NAT Gateways

3.1 Public NAT Gateway Overview

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

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

Figure 3-1 Process of using a public NAT gateway



 NOTE

An SNAT rule and a DNAT rule cannot share the same EIP. If you need to create an SNAT rule and a DNAT rule, assign two EIPs.

3.2 Managing Public NAT Gateways

3.2.1 Creating a Public NAT Gateway

Scenarios

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

Constraints and Limitations

- Rules on one public NAT gateway can use the same EIP, but rules on different NAT gateways must use different EIPs.
- Each VPC can have only one NAT gateway.
- Each VPC can be associated with multiple public NAT gateways.
- SNAT and DNAT rules cannot use the same EIP.
- If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.
- 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

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. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create 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
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed.
VPC	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.
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 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.
Specifications	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.

Parameter	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** to create a public NAT gateway.
It takes 1 to 6 minutes to create a public NAT gateway.
7. In the list, view the status of the public NAT gateway.

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. The following describes how to add a route to a custom route table.

Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the **Route Tables** page, click **Create Route Table** in the upper right corner.
VPC: Select the VPC to which the public NAT gateway belongs.
5. After the custom route table is created, click its name.
The **Summary** page is displayed.
6. 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.
7. Click **OK**.

3.2.2 Viewing a Public NAT Gateway

Scenarios

View information about a public NAT gateway.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. View information about the public NAT gateway.

3.2.3 Modifying a Public NAT Gateway

Scenarios

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

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.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** 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.

3.2.4 Deleting a Public NAT Gateway

Scenarios

Delete public NAT gateways that are no longer required to release resources and reduce costs.

Prerequisites

- All SNAT and DNAT rules created on the public 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](#).

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.

The **Public NAT Gateway** 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, click **Yes**.

3.3 Managing SNAT Rules

3.3.1 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.

Constraints and Limitations

- 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.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** 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.
EIP	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.
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.

3.3.2 Viewing an SNAT Rule

Scenarios

View details about an SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.

3. Click the name of the public NAT gateway.
4. In the SNAT rule list, view details about the SNAT rule.

3.3.3 Modifying an SNAT Rule

Scenarios

Modify an SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the **SNAT Rules** tab, locate the row that contains the SNAT rule you want to modify.
5. Click **Modify** in the **Operation** column.
6. In the displayed dialog box, modify parameters as needed.
7. Click **OK**.

3.3.4 Deleting an SNAT Rule

Scenarios

Delete an SNAT rule that you no longer need.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **Yes**.

3.4 Managing DNAT Rules

3.4.1 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

- DNAT rules cannot map virtual IP addresses to EIPs.
- 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.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** 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.

Parameter	Description
Port Type	<p>The port type</p> <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	<p>The protocol can be TCP or UDP.</p> <p>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.</p>
EIP	<p>The EIP that will be used by the server to provide services accessible from the Internet</p> <p>You can select an EIP that either 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>
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>
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.

3.4.2 Viewing a DNAT Rule

Scenarios

View details about a DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, view details about the DNAT rule.

3.4.3 Modifying a DNAT Rule

Scenarios

Modify a DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.
6. In the displayed dialog box, modify parameters as needed.
7. Click **OK**.

3.4.4 Deleting a DNAT Rule

Scenarios

Delete a DNAT rule that you no longer need.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.
6. In the displayed dialog box, click **Yes**.

3.4.5 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 **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, select DNAT rules that you no longer need and click **Delete DNAT Rule**.
6. In the displayed dialog box, click **Yes**.

3.4.6 Importing and Exporting DNAT Rules Using Templates

Scenarios

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

One DNAT rule is configured for one server. If there are multiple servers, add multiple DNAT rules.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click the name of the public NAT gateway to which you want to import DNAT rules.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. On the displayed page, click **Import Rule** and then **Download Template**.
6. Fill in DNAT rule parameters based on the table heading in the template. For details, see [Table 3-4](#).

Table 3-4 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	The following two scenarios are available: <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	The EIP that will be used by the server to provide publicly accessible services Only EIPs that have not been bound or that have been bound to a DNAT rule in the current VPC are available for selection.
Outside Port	The EIP port This parameter is only available if you select Specific port for Port Type . You can enter a specific port number or a port range, for example, 80 or 80-100.

Parameter	Description
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 you set Protocol 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 you select Specific port for Port Type. <p>The number of inside and outside ports must match.</p>
Description	<p>Provides supplementary information about the DNAT rule. Enter up to 255 characters. Open angle brackets (<), close angel brackets (>), and angle brackets (<>) are not allowed.</p>

7. After filling in the template, click **Import Rule**, select the template, and click **Import**.
8. View details in the DNAT rule list.
If **Status** is **Running**, the rules have been added.
9. In the displayed dialog box, click **Yes**.

4 Private NAT Gateways

4.1 Private NAT Gateway Overview

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 across AZs in a VPC to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers across AZs in a VPC to share a transit IP address to provide services accessible from on-premises data centers or other VPCs.

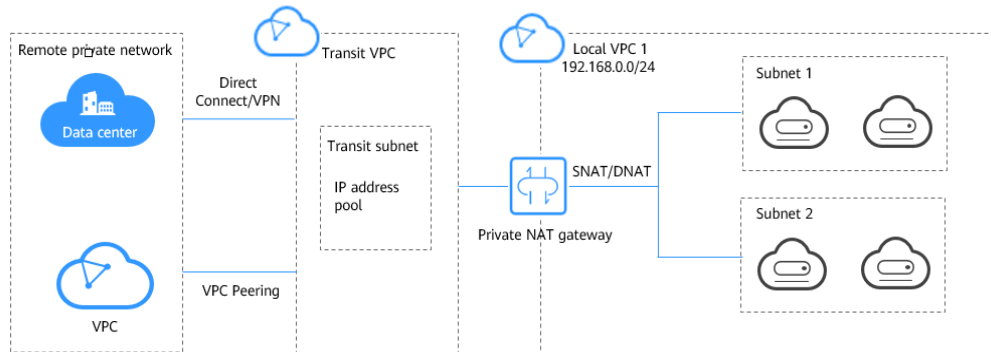
Transit Subnet

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



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

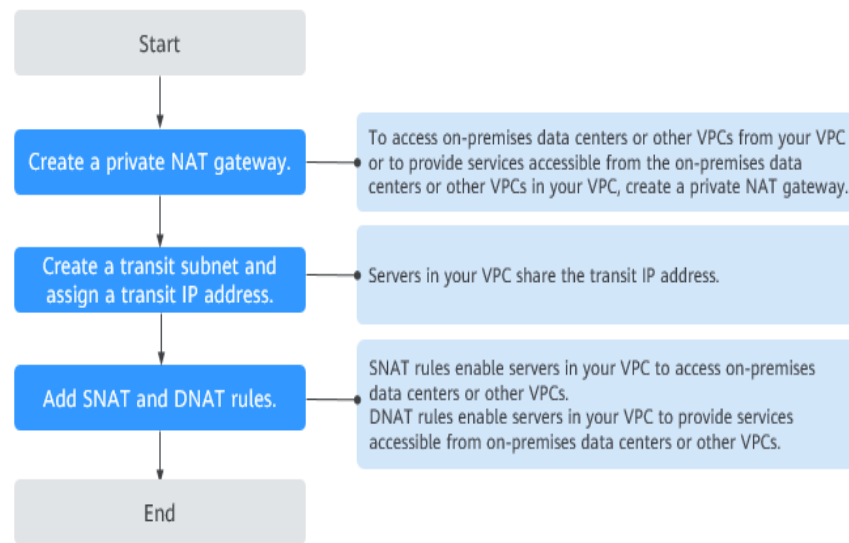
Item	Public NAT Gateway	Private NAT Gateway
Function	Connects a private network to the Internet	Connects private networks
SNAT	Enables access to the Internet	Enables access to on-premises data centers or other VPCs
DNAT	Allows servers to provide services accessible from the Internet	Allows servers to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

4.2 Creating a Private NAT Gateway

4.2.1 Overview

This section describes how to deploy a private NAT gateway.

Figure 4-2 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](#).

4.2.2 Creating a Private NAT Gateway

Scenarios

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

Constraints and Limitations

- 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. Click **Service List** in the upper left corner. Under **Network**, select **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 (_), and hyphens (-) 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 section "NAT Gateway Specifications" in the <i>NAT Gateway Service Overview</i> .
Description	Supplementary information about the private NAT gateway Enter up to 255 characters. Angle brackets (<>) are not allowed.

Table 4-3 Tag requirements

Parameter	Requirement
Key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each NAT gateway. • Can contain a maximum of 36 characters.
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters.

6. Click **Create Now**.

Helpful Links

[Managing Private NAT Gateways](#)

4.2.3 Assigning a Transit IP Address

Scenarios

After a private NAT gateway is created, assign a transit IP address, so that servers in your VPC can share the transit IP address to communicate with on-premises data centers or other VPCs.

Prerequisites

- There are transit VPCs available.
- A Direct Connect connection has been created with the VPC CIDR block set to **0.0.0.0/0**. For detailed configurations, see the *Direct Connect User Guide*.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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 **Transit IP Addresses**.

Figure 4-3 Assign Transit IP Address

✕

Assign Transit IP Address

Transit VPC:

Transit Subnets:

Transit IP Address: Automatic Manual

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)

Tag key: Tag value:

You can add 10 more tags.

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

Table 4-4 Parameter descriptions of a transit IP address

Parameter	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	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 .

6. Click **OK**.

4.2.4 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.

Constraints and Limitations

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

Prerequisites

- A private NAT gateway is available.
- Transit IP addresses are available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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 the name of the private NAT gateway on which you need to add an SNAT rule.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.
6. Configure required parameters. For details, see .

Figure 4-4 Add SNAT Rule

Table 4-5 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.

Parameter	Description
Monitoring	You can create alarm rules to watch the number of SNAT connections.
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.

- Click **OK**.

 **NOTE**

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

Helpful Links

[Managing SNAT Rules](#)

4.2.5 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.

Constraints and Limitations

- 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.
- Transit IP addresses are available.

Procedure

- Log in to the management console.
- Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The NAT gateway console is displayed.
- In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.

4. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add a DNAT rule.
5. On the private NAT gateway details page, click the **DNAT Rules** tab.
6. 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.

7. Configure required parameters. For details, see [Table 4-6](#).

Figure 4-5 Add DNAT Rule

Table 4-6 Descriptions of DNAT rule parameters

Parameter	Description
Local Network	
Port Type	<p>The port type</p> <p>The type can be:</p> <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 a 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.

8. Click **OK**.

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

Helpful Links

[Managing DNAT Rules](#)

4.3 Managing Private NAT Gateways

4.3.1 Viewing a Private NAT Gateway

Scenarios

View information about a private NAT gateway.

Prerequisites

A private NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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 the name of the private NAT gateway.
5. On the displayed page, view information about the private NAT gateway.

4.3.2 Modifying a Private NAT Gateway

Scenarios

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

Prerequisites

A private NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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, locate the row that contains the private NAT gateway you want to modify and click **Modify** in the **Operation** column.
5. Modify the name, specifications, or description of the private NAT gateway.
6. Confirm your modification and click **OK**.

You can view information about the modified NAT gateway in the private NAT gateway list.

4.3.3 Deleting a Private NAT Gateway

Scenarios

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

Prerequisites

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](#).

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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, locate the private NAT gateway that you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **Yes**.

4.4 Managing SNAT Rules

4.4.1 Viewing an SNAT Rule

Scenarios

View details about an SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click **Service List** in the upper left corner. Under **Network**, select **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 the name of the private NAT gateway.
5. In the SNAT rule list, view details about the SNAT rule.

4.4.2 Modifying an SNAT Rule

Scenarios

Modify an SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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 the name of the private NAT gateway.
5. On the **SNAT Rules** tab, locate the row that contains the SNAT rule you want to modify.
6. Click **Modify** in the **Operation** column.
7. In the displayed dialog box, modify parameters as needed.
8. Click **OK**.

4.4.3 Deleting an SNAT Rule

Scenarios

Delete SNAT rules that you no longer need.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click **Service List** in the upper left corner. Under **Network**, select **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 the name of the private NAT gateway.
5. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.
6. In the displayed dialog box, click **Yes**.

4.5 Managing DNAT Rules

4.5.1 Viewing a DNAT Rule

Scenarios

View details about a DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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 the name of the private NAT gateway.
5. On the private NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, view details about the DNAT rule.

4.5.2 Modifying a DNAT Rule

Scenarios

Modify a DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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 the name of the private NAT gateway.
5. On the private NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.
7. In the displayed dialog box, modify parameters as needed.
8. Click **OK**.

4.5.3 Deleting a DNAT Rule

Scenarios

Delete a DNAT rule that you no longer need.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **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 the name of the private NAT gateway.
5. On the private NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.
7. In the displayed dialog box, click **Yes**.

4.6 Managing Transit IP Addresses

4.6.1 Assigning a Transit IP Address

Scenarios

Servers in a VPC all 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. Click **Service List** in the upper left corner. Under **Network**, select **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 **Transit IP Addresses**.

Figure 4-6 Assign Transit IP Address

Assign Transit IP Address ×

Transit VPC C

Transit Subnets C

Transit IP Address Automatic Manual

Tag
It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) C

You can add 10 more tags.

5. Click **OK**.

4.6.2 Viewing a Transit IP Address

Scenarios

View details about transit IP addresses assigned to you.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The NAT gateway console is displayed.

3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. Click the **Transit IP Addresses** tab and then click the transit IP address.
5. On the page displayed, view details about the assigned transit IP addresses.

4.6.3 Releasing a Transit IP Address

Scenarios

Release a transit IP address that you no longer need.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. In the **Transit IP Addresses** area, locate the transit IP address you want to release, and click **Release** in the **Operation** column.
5. Click **Yes**.

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 the *Direct Connect User Guide*.

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

Accessing Other VPCs

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

For details, see the *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 cloud service to perform efficient O&M on your NAT Gateway resources.

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

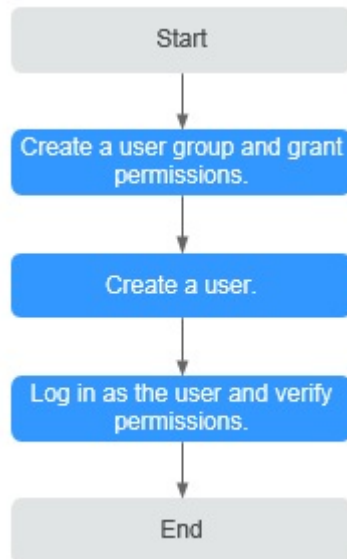
This section describes the procedure for granting permissions (see [Figure 5-1](#)).

Prerequisites

Learn about the permissions supported by NAT Gateway and choose policies or roles according to your requirements. For details, see [Permissions](#). For the permissions of other services, see System Permissions.

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 **ReadOnlyAccess** policy to the group.
2. Create an IAM user and add it to a user group.
Create a user on the IAM console and add the user to the group created in **1**.
3. Log in and verify permissions.
Log in to the management console as the created user. Switch to the authorized region and verify the permissions.
 - Choose **Service List > NAT Gateway**. Then click **Create NAT Gateway**. If a message appears indicating that you have insufficient permissions to perform the operation, the **ReadOnlyAccess** policy has already taken effect.
 - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **ReadOnlyAccess** policy has already taken effect.

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 the *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. You do not need to have knowledge of the policy syntax.
- JSON: Create a JSON policy or edit an existing one.

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

Example Policies

- Example 1: 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 permission 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 x 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 x 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 ID
vpc_nat_gateway_id	Private NAT gateway ID

6.2 Creating Alarm Rules

Scenarios

You can set NAT gateway alarm rules to customize the monitored objects and notification policies. Then, you can learn NAT gateway running status in a timely manner.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the left navigation pane, choose **Alarm Management > Alarm Rules**.
4. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters to create an alarm rule, or modify an existing alarm rule.
5. On the **Create Alarm Rule** page, follow the prompts to configure the parameters.


- a. Set the alarm rule name and description.

Table 6-3 Configuring the alarm rule name and description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: alarm-b6a1
Description	(Optional) Provides supplementary information about the alarm rule.

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

Table 6-4 Parameters

Parameter	Description	Example Value
Resource Type	Specifies the type of the resource the alarm rule is created for.	NAT Gateway
Dimension	Specifies the metric dimension of the selected resource type.	Public NAT Gateway
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select Resource groups or Specific resources . NOTE <ul style="list-style-type: none"> • If Resource groups is selected and any resource in the group meets the alarm policy, an alarm is triggered. • If you select Specific resources, select one or more resources and click  to add them to the box on the right. 	Specific resources
Method	There are two options: Use template or Create manually .	Create manually
Template	Specifies the template to be used. You can select a default alarm template or customize a template.	N/A

Parameter	Description	Example Value
Alarm Policy	Specifies the policy for triggering an alarm. If you set Resource Type to Website Monitoring, Log Monitoring, Custom Monitoring , or a specific cloud service, whether to trigger an alarm depends on whether the metric data in consecutive periods reaches the threshold. For example, Cloud Eye triggers an alarm if the raw data of the SNAT connections of the monitored object is 8000 or more for three consecutive 1-minute periods.	N/A
Alarm Severity	Specifies the alarm severity, which can be Critical, Major, Minor, or Informational .	Major

- c. Configure the alarm notification.

Table 6-5 Alarm notification parameters

Parameter	Description
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Object	Specifies the object that receives alarm notifications. You can select the account contact or a topic. <ul style="list-style-type: none"> • Account contact is the mobile phone number and email address of the registered account. • A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it. For details, see the <i>Creating Alarm Notification Topics</i>.
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If Validity Period is set to 08:00-20:00 , Cloud Eye sends notifications only within 08:00-20:00.
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select Generated alarm (when an alarm is generated), Cleared alarm (when an alarm is cleared), or both.

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

 NOTE

For more information about how to configure alarm rules, 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.

6.4 Viewing Metrics of Resources Using a NAT Gateway

Scenarios

You can view metrics details of resources using a specific NAT gateway. The resources can be ECSs or BMSs.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
The NAT gateway console is displayed.
3. Click the name of the NAT gateway whose metrics you want to view.
4. On the displayed page, choose the **Monitoring** tab and click **View Details**.
On the Cloud Eye console, view metrics of the NAT Gateway.
5. Configure a time range for metrics to be viewed.
6. Click  in the upper right corner of the page to switch the display mode.

7. Select a metric to be viewed and click a specific time point in the displayed graph.

In the lower part of the page, you can view the metric details of resources at the time point.

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.

7.1.3 Which Ports Cannot Be Accessed?

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

Protocol	Port
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 to 139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

7.1.4 What Are the Differences Between Using a NAT Gateway and Using an EIP for an ECS?

A public NAT gateway provides SNAT and DNAT, so multiple ECSs can share an EIP.

An ECS can also have an EIP bound to it. The EIP does not have to be shared.

If both SNAT and EIP are configured for an ECS, data will be forwarded through the EIP.

If both DNAT and EIP are configured for an ECS, the ECS will have two EIPs, one that is directly bound to the ECS and one that is associated with the DNAT rule. Incoming data will be forwarded by one of the two EIPs, which is determined by the client user. Outgoing data will be forwarded by the EIP directly bound to the ECS in priority. If the two EIPs are different, data forwarding will fail.

Configuring both a public NAT gateway and an EIP for an ECS is not recommended.

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

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

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

7.1.6 Can I Change the VPC for a NAT Gateway?

No.

The VPC you selected when you create a public NAT gateway cannot be changed after the public NAT gateway is created.


7.1.7 What Is the Quota of the NAT Gateway?

What Is the Quota?

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

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

How Do I View My Quotas?

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

How Do I Apply for a Higher Quota?

The system does not support online quota adjustment.

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

7.1.8 Can I Update NAT Gateways and SNAT Rules?

Public NAT gateways can be updated. SNAT rules cannot be updated.

7.1.9 Does NAT Gateway Support IPv6 Addresses?

No.

7.1.10 What Security Policies Can I Configure to Implement Access Control If I Use a NAT Gateway?

There are two types of security policies you can configure: security groups and Access Control Lists (ACLs):

- A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted. After a security group is created, you can create various access rules for the security group, and these rules will apply to all ECSs added to this security group.
- A network ACL is an optional layer of security for your subnets. You can associate one or more subnets with a network ACL to control traffic in and out of the subnets.

Security groups operate at the ECS level, whereas network ACLs operate at the subnet level. You can use network ACLs together with security groups to implement access control that is both comprehensive and fine-grained.

For details about security groups and network ACLs, see section "Security" in the .

7.1.11 What Can I Do If Connection Between My Servers and the Internet Fails After I Add SNAT and DNAT Rules?

Symptom

You have bought a public NAT gateway and added SNAT and DNAT rules, but your servers cannot access the Internet or provide services accessible from the Internet. Whether the network configured with a public NAT gateway can connect

to the Internet depends on the route table configuration, security group configuration, and network ACL configuration. If any configuration problem occurs, the network connection will fail. This section describes the fault locating process after a public NAT gateway is configured.

Fault Locating

The following fault causes are listed in descending order of occurrence probability.

If the fault persists after one possible cause is ruled out, move down the list to the other possible causes.

Figure 7-1 Network disconnection troubleshooting

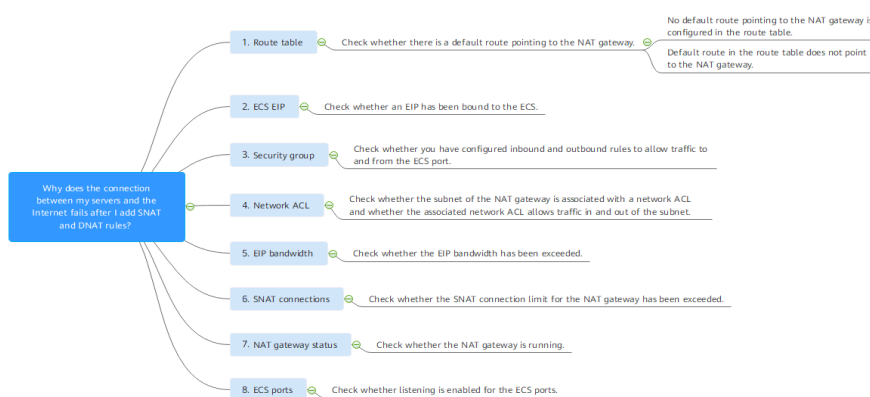


Table 7-1 Network disconnection troubleshooting

Possible Cause	Solution
The route table is incorrectly configured.	Add the default route or a route pointing to the public NAT gateway to the route table. For details, see Checking Whether Default Route Pointing to the Public NAT Gateway Is Configured in the Route Table .
The ECS has an EIP bound.	Unbind the EIP from the ECS. For details, see Checking Whether the ECS Has an EIP Bound .
The security group rules are incorrectly configured.	Configure ECS security group rules to allow traffic to and from the ECS. For details, see Checking Whether Security Group Rules Allow Traffic to and from the ECS Port .
The network ACL is incorrectly configured.	Add network ACL rules to allow traffic in and out of the subnet. For details, see Checking Whether Network ACL Rules Allow Traffic in and out of the Subnet .
The EIP bandwidth exceeds the threshold.	Increase the EIP bandwidth by referring to Checking Whether the EIP Bandwidth Limit Has Been Exceeded .

Possible Cause	Solution
The service volume of the Public NAT gateway exceeds the upper limit.	Increase the public NAT gateway specifications. For details, see Checking Whether the SNAT Connection Limit for the Public NAT Gateway Has Been Exceeded .
The assign status is abnormal.	Ensure that the public NAT gateway is running. For details, see Check Whether the Public NAT Gateway Status is Normal .
The ECS port is not listened on.	Enable the ECS port again. For details, see Checking ECS Ports .

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


1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Network**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Route Tables**.
5. In the route table list, click the name of the route table associated with the VPC to which the public NAT gateway belongs.
6. Check whether default route (0.0.0.0/0) pointing to the public NAT gateway is in the route list.
 - If no, add the default route pointing to the public NAT gateway to the route table.
 - i. Click **Add Route** and configure required parameters.

Table 7-2 Descriptions of route parameters

Parameter	Description
Destination	The destination CIDR block Set it to 0.0.0.0/0 .
Next Hop Type	Set it to NAT gateway .
Next Hop	Set it to the ID of the public NAT gateway you purchased.
Description	(Optional) Supplementary information about the route Enter up to 255 characters. Angle brackets (<>) are not allowed.

- ii. Click **OK**.

- If a default route is there but does not point to the public NAT gateway, add a route pointing to the public NAT gateway to the existing route table. Alternatively, create a route table and add a default route pointing to the public NAT gateway to the new route table.
- To add a route pointing to the public NAT gateway to the existing route table, perform the following steps:
 - 1) Click **Add Route** and configure required parameters.

Table 7-3 Descriptions of route parameters

Parameter	Description
Destination	The destination CIDR block
Next Hop Type	Set it to NAT gateway .
Next Hop	Set it to the ID of the public NAT gateway you purchased.
Description	(Optional) Supplementary information about the route Enter up to 255 characters. Angle brackets (<>) are not allowed.

- 2) Click **OK**.

- Create a route table and add a default route pointing to the public NAT gateway.
 - 1) In the upper right corner of the **Route Tables** page, click **Create Route Table** and configure required parameters.

Table 7-4 Descriptions of route table parameters

Parameter	Description	Example Value
Name	(Mandatory) The name of the route table Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. Spaces are not allowed.	rtb-001
VPC	(Mandatory) The VPC that the route table belongs to	vpc-001
Description	(Optional) Supplementary information about the route table Enter up to 255 characters. Angle brackets (<>) are not allowed.	N/A

Parameter	Description	Example Value
Route Settings	Information about routes You can click Add Route to add more routes. Set Destination to 0.0.0.0/0 , Next Hop Type to NAT gateway , and Next Hop to the public NAT gateway you purchased.	N/A


- 2) Click **OK**.
An **Information** dialog box is displayed, indicating that you can associate the route table with a subnet now or later.
- 3) Click **Associate Subnet**.
The **Associated Subnets** tab is displayed.
- 4) Click **Associate Subnet** and select the subnet to be associated.
- 5) Click **OK**.

Checking Whether the ECS Has an EIP Bound

If both SNAT and EIP are configured for an ECS, the EIP is preferentially used for data forwarding.

If both DNAT and EIP are configured for an ECS, the ECS will have two EIPs, one that is bound to the ECS and one that is associated with the DNAT rule. Incoming data will be forwarded by one of the two EIPs, which is determined by the client user. Outgoing data will be forwarded by the EIP bound to the ECS in priority. If the two EIPs are different, data forwarding will fail.


If the ECS has an EIP bound, perform the following steps to unbind the EIP.

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. In the list, locate the ECS. In the **IP Address** column, check whether the ECS has an EIP bound.
 - If no, check the next item.
 - If yes, unbind it.

For details about how to unbind an EIP from an ECS, see section "Unbinding an EIP from an ECS and Releasing the EIP" in the *Elastic IP User Guide*.

Checking Whether Security Group Rules Allow Traffic to and from the ECS Port


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.

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, click the name of the ECS.
5. Click the **Security Groups** tab and view security group rules.
6. Check whether you have configured inbound and outbound rules to allow traffic to and from the ECS port.
 - If yes, check the next item.
 - If no, click **Manage Rule**.

On the **Summary** tab page of the security group, click **Inbound Rules** or **Outbound Rules** to add an inbound rule and outbound rule that allow traffic to and from the ECS port. For details about inbound and outbound rule parameters, see section "Adding a Security Group Rule" in the *Virtual Private Cloud User Guide*.

Checking Whether Network ACL Rules Allow Traffic in and out of the Subnet

Check whether the VPC subnet is associated with network ACL rules. If yes, check the network ACL rules.

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Network**, select **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Subnets**.
5. Check whether the NAT gateway subnet is associated with a network ACL. The specific network ACL name indicates that the association is successful.
6. Click the network ACL name to view the details.
7. Check whether the inbound and outbound rules that allow traffic in and out of the subnet have been added.

If no, add such inbound and outbound rules, or disassociate the network ACL from the subnet.

For details, see section "Adding a Network ACL Rule" in the *Virtual Private Cloud User Guide* and section "Disassociating a Subnet from a Network ACL" in the *Virtual Private Cloud User Guide*.

NOTE


The default network ACL rules deny all incoming and outgoing packets. After the network ACL is disabled, the default rules still take effect.

Checking Whether the EIP Bandwidth Limit Has Been Exceeded

If an EIP is bound to the public NAT gateway, the bandwidth is used to provide access traffic between the public network and the public NAT gateway.


If the network is disconnected, check whether the EIP bandwidth exceeds the limit.

Checking Whether the SNAT Connection Limit for the Public NAT Gateway Has Been Exceeded

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Management & Governance**, choose **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring > NAT Gateway**.
5. Locate the row that contains the public NAT gateway you purchased and click **View Metric** in the **Operation** column to check detailed monitoring.
6. Check whether the SNAT connection limit for the public NAT gateway has been exceeded.
 - If no, check the next item.
 - If the number of SNAT connections exceeds the upper limit of the public NAT gateway specifications, increase the specifications.

For details about how to increase the public NAT gateway specifications, see section "Modifying a Public NAT Gateway" in the *NAT Gateway User Guide*.

Check Whether the Public NAT Gateway Status is Normal

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
4. In the public NAT gateway list, locate the NAT gateway and check whether its status is **Running**.
 - If yes, check the next item.
 - If no, the possible causes are as follows:
 - Your account or resources are frozen because you violated related security requirements or laws and regulations when using the cloud platform. If you complete the rectification within the required period and meet related security and legal requirements, your account and resources can be unfrozen. If you do not complete the rectification within the required period, your resources will be deleted.

Checking ECS Ports

Ensure that ECS ports are in the **LISTEN** state. [Table 7-5](#) lists the common TCP statuses.

- Linux
Run the **netstat -antp** command to check whether the ECS port is in the **LISTEN** state.
For example, run **netstat -ntulp |grep 80**.

Figure 7-2 Checking port listening status

```
[root@elb-mq02 ~]# netstat -antpu | grep sshd
tcp        0      0 0.0.0.0:22          0.0.0.0:*        LISTEN    7178/sshd
```

If no, enable the ECS port.

- Windows

Perform the following operations to check port communication:

- Run **cmd.exe**.
- Run the **netstat -ano | findstr "PID"** command to obtain the PID used by the process.

For example, run **netstat -ano | findstr "80"**.

Figure 7-3 Checking port listening status

```
C:\Users\Administrator>netstat -ano |findstr "80"
TCP        0.0.0.0:80          0.0.0.0:0        LISTENING    4
TCP        0.0.0.0:49155      0.0.0.0:0        LISTENING    888
TCP        [::]:80           [::]:0           LISTENING    4
TCP        [::]:49155        [::]:0           LISTENING    888
UDP        0.0.0.0:123       *:               808
UDP        [::]:123          *:               808
```

If no, enable the ECS port.

Table 7-5 Common TCP statuses

TCP Status	Description	Scenario
LISTEN	Listens for network connection requests from a remote TCP port.	The TCP server is running.
ESTABLISHED	A connection has been set up.	A TCP connection is properly set up.
TIME-WAIT	Waits until the remote TCP server receives the acknowledgement of the connection termination request.	The TCP connection is terminated, and the session is closed in 1 minute.
CLOSE-WAIT	Waits for a connection termination request sent by a local user.	A program fault resulted in an open socket. This state is displayed after the network is disconnected, indicating that a process is in an infinite loop or waiting for certain requirements to be met. To resolve this issue, restart the affected process.
FIN-WAIT-2	Waits for the network disconnection request from a remote TCP server.	The network has been disconnected and requires 12 minutes to automatically recover.


TCP Status	Description	Scenario
SYN-SENT	Waits for the matched network connection request after a network connection request is sent.	The TCP connection request failed, which is generally caused by the delayed handling of high CPU usage on the server or by a DDoS attack.
FIN-WAIT-1	Waits for the remote TCP disconnection request, or the acknowledgement for a previous disconnection request.	If the network has been disconnected, this state may not automatically recover after 15 minutes. If the port remains occupied for a long period of time, restart the OS to resolve the issue.

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** Under **Compute**, select .
- 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 I Increase the Numbers of SNAT and DNAT Rules Supported by a Private NAT Gateway?

You can to address this issue.

7.2.4 Can an SNAT Rule and a DNAT Rule of a Private NAT Gateway Share the Same Transit IP Address?

No.

7.2.5 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-premise IP address.

7.2.6 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.

7.2.7 Can a Private NAT Gateway Be Used Across ?

Private NAT gateways cannot be used across . However, you can use a to connect transit VPCs of the 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 ECS 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.

7.3.2 What Are SNAT Connections?

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 source port refer to the IP address and port after NAT.

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. The number of connections you query on an ECS may be different from the actual number of SNAT connections. (You can run the **netstat** command to query the number of connections.) Assume that an ECS creates 100 connections to a fixed destination every second. 55,000 connections will be used up in about 10 minutes without considering the dropped idle connections. As a result, new connections cannot be established.

If there is no data packet passing through the SNAT connection for a long time, the connection will be timed out.

7.3.3 What Is the Bandwidth of a NAT Gateway That Is Used by Servers to Access the Internet? How Do I Configure the Bandwidth?

NAT Gateway SNAT translates private IP addresses of servers to EIPs. The bandwidth of a NAT gateway depends on that of the EIP you purchased.

For details about how to adjust a bandwidth, see .

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

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

7.3.5 What Should I Do If My ECS Fails to Access a Server on the Public Network Through a NAT Gateway?

TCP connection may fail when an ECS accesses a server on the public network through an SNAT rule. Perform the following steps to locate the fault cause:

1. Run the following command to check whether **tcp_tw_recycle** is enabled on the remote server:

```
sysctl -a|grep tcp_tw_recycle
```

If **tcp_tw_recycle** is set to **1**, **tcp_tw_recycle** is enabled.

2. Run the following command to check the number of lost packets of the remote server:

```
cat /proc/net/netstat | awk '/TcpExt/ { print $21,$22 }'
```

If **ListenDrops** is not set to **0**, packet loss occurs, that is, the network is faulty.

Troubleshooting

Method 1: Modifying the kernel parameter of the remote server

- Run the following command to temporarily modify the parameters (the modification becomes invalid after the server is restarted):

```
sysctl -w net.ipv4.tcp_tw_recycle=0
```
- Perform the following operations to permanently modify the parameters:

- a. Modify the **/etc/sysctl.conf** file:

```
vi /etc/sysctl.conf
```

Add the following content to the file:

```
net.ipv4.tcp_tw_recycle=0
```

- b. Press **Esc**, enter **:wq!**, and save the file and exit.
- c. Run the following command to make the modification take effect:

```
sysctl -p
```

Method 2: Modifying the kernel parameter of the local client

- To temporarily modify parameters (the settings become invalid after the local client is restarted), configure the parameter as follows:

```
sysctl -w net.ipv4.tcp_timestamps=0
```

- Perform the following operations to permanently modify the parameters:

- a. Modify the `/etc/sysctl.conf` file:
`vi /etc/sysctl.conf`
Add the following content to the file:
`net.ipv4.tcp_timestamps=0`
- b. Press **Esc**, enter `:wq!`, and save the file and exit.
- c. Run the following command to make the modification take effect:
`sysctl -p`

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

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

When you are creating an SNAT rule and set **Scenario** to **VPC**, select a subnet in the target VPC. This way, servers in the subnet can access the Internet through the SNAT rule.

When you are creating an SNAT rule and set **Scenario** to **Direct Connect**, enter a CIDR block of an on-premises data center or another VPC. With this, on-premises servers or cloud servers in the CIDR block can access the Internet through the SNAT rule.

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. 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. For details, see [Adding a DNAT Rule](#).

7.4.2 Can I Modify DNAT Rules?

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

A Change History

Released On	Description
2020-01-02	This issue is the second official release, which incorporates the following changes: <ul style="list-style-type: none">• Added description about the DNAT function.• Added Allowing Internet Users to Access a Service in a Private Network Using DNAT and Allowing On-Premises Servers to Communicate with the Internet.
2018-08-15	This issue is the first official release.