

NAT Gateway

FAQs

Issue	01
Date	2025-10-31



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Public NAT Gateways.....	1
1.1 What Is the Relationship Between a VPC, Public NAT Gateway, EIP Bandwidth, and ECS?.....	1
1.2 How Does a Public NAT Gateway Offer High Availability?.....	1
1.3 Which Ports Cannot Be Accessed?.....	1
1.4 What Are the Differences Between Using a Public NAT Gateway and Using an EIP for an ECS?.....	2
1.5 What Should I Do If I Fail to Access the Internet Through a Public NAT Gateway?.....	2
1.6 Can I Change the VPC for a Public NAT Gateway?.....	2
1.7 Does Public NAT Gateway Support IPv6 Addresses?.....	2
1.8 What Security Policies Can I Configure to Implement Access Control If I Use a Public NAT Gateway?.....	3
1.9 What Can I Do If Connection Between My Servers and the Internet Fails After I Add SNAT and DNAT Rules?.....	3
1.10 What Can I Do If the Number of Lost Packets of a Public NAT Gateway Exceeds the Threshold (or EIP Port Allocation Exceeds the Threshold)?.....	11
2 Private NAT Gateways.....	12
2.1 How Do I Troubleshoot a Network Failure After a Private NAT Gateway Is Configured?.....	12
2.2 How Many Private NAT Gateways Can I Create in a VPC?.....	13
2.3 Can I Increase the Numbers of SNAT and DNAT Rules Supported by a Private NAT Gateway?.....	13
2.4 Can Private NAT Gateways Translate On-premises IP Addresses Connected to the Cloud Through Direct Connect?.....	13
2.5 What Are the Differences Between Private NAT Gateways and Public NAT Gateways?.....	13
2.6 Can a Private NAT Gateway Be Used Across Accounts?.....	14
3 SNAT Rules.....	15
3.1 Why Do I Need SNAT?.....	15
3.2 What Are SNAT Connections?.....	15
3.3 What Is the Bandwidth of a Public NAT Gateway That Is Used by Servers to Access the Internet? How Do I Configure the Bandwidth?.....	16
3.4 How Do I Resolve Packet Loss or Connection Failure Issues When Using a NAT Gateway?.....	16
3.5 What Should I Do If My ECS Fails to Access a Server on the Public Network Through a Public NAT Gateway?.....	16
3.6 What Are the Relationships and Differences Between the CIDR Blocks in a NAT Gateway and in an SNAT Rule?.....	17
4 DNAT Rules.....	18
4.1 Why Do I Need DNAT?.....	18

4.2 Can I Modify DNAT Rules?.....	18
4.3 What Can I Do If a DNAT Rule Is Not Working?.....	18

1 Public NAT Gateways

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.

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 and works with Cloud Eye to report alarms, thereby reducing risks and improving availability.

1.3 Which Ports Cannot Be Accessed?

Table 1-1 lists some high-risk ports that are blocked by default. Even if you have added a security group rule to allow access over these ports, traffic over these ports in restricted regions is still denied. In this case, do not use these high-risk ports for your services.

Table 1-1 High-risk ports

Protocol	Port
TCP	42 135 137 138 139 444 445 593 1025 1068 1433 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 8998 9995 9996

Protocol	Port
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9995 9996

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

Public NAT gateways support both SNAT and DNAT and allow multiple ECSs to share EIPs.

An EIP bound to an ECS cannot be used by any other ECSs.

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, inbound traffic will be forwarded by the EIP configured for the DNAT rule or the EIP directly bound to the ECS, which is determined by the client user. The outbound traffic will be forwarded by the EIP bound to the ECS preferentially. If the EIPs used for forwarding inbound and outbound traffic are different, the traffic will fail to be forwarded.

Associating an ECS with both an EIP and a public NAT gateway is not recommended.

1.5 What Should I Do If I Fail to Access the Internet Through a Public 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.

1.6 Can I Change the VPC for a Public NAT Gateway?

No.

The VPC you selected when you buy a public NAT gateway cannot be changed.

1.7 Does Public NAT Gateway Support IPv6 Addresses?

No.

1.8 What Security Policies Can I Configure to Implement Access Control If I Use a Public 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 [Virtual Private Cloud User Guide](#).

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

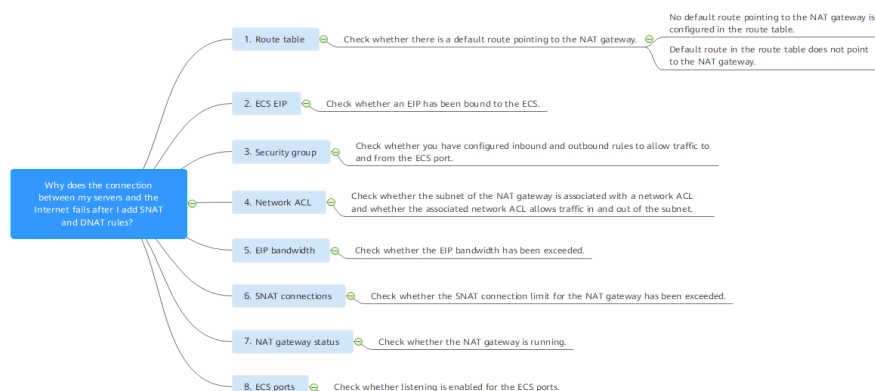
Symptom

You have created a 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 configurations of route tables, security groups, and network ACLs. If any configuration problem occurs, the network connection will fail. This section describes how to troubleshoot network disconnection after a public NAT gateway is created.

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 1-1 Network disconnection troubleshooting**Table 1-2** 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 .
The SNAT connection limit for the public NAT gateway has been exceeded.	Increase the public NAT gateway specifications. For details, see Checking Whether the SNAT Connection Limit for the Public NAT Gateway Has Been Exceeded .
The public NAT gateway 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 **Networking**, 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 1-3 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 1-4 Descriptions of route parameters

Parameter	Description
Destination	The destination CIDR block
Next Hop Type	Set it to NAT gateway .

Parameter	Description
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 1-5 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
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 user of the client. 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 [Unbinding an EIP](#).

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 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 [Adding a Security Group Rule](#).

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 **Networking**, 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 [Adding a Network ACL Rule](#) and [Disassociating a Subnet from a Network ACL](#).

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.

For details, see [How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?](#)

For instructions about how to increase the bandwidth, see [Changing an EIP Bandwidth](#).

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 [Modifying a Public NAT Gateway](#).

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 **Networking**, 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 1-6](#) 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 1-2 Checking port listening status (Linux)

```
[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:
 - a. Run **cmd.exe**.
 - b. Run the **netstat -ano | findstr "PID"** command to obtain the PID used by the process.
For example, run **netstat -ano | findstr "80"**.

Figure 1-3 Checking port listening status (Windows)

```
C:\Users\Administrator>netstat -ano |findstr "80"
TCP    0.0.0.0:80          0.0.0.0:*          LISTENING        4
TCP    0.0.0.0:49155      0.0.0.0:*          LISTENING        880
TCP    [::]:80           [::]:*             LISTENING        4
TCP    [::]:49155        [::]:*             LISTENING        880
UDP    0.0.0.0:123       *:.*               808
UDP    [::]:123          [::]:*             808
```

If no, enable the ECS port.

Table 1-6 Common TCP statuses

TCP Status	Description	Scenario
LISTEN	Listens for network connection requests from a remote TCP port.	The TCP server is running properly.
ESTABLISHED	Indicates that 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.	An application program fault leads to 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 termination request from a remote TCP server.	The network has been disconnected and requires 12 minutes to automatically recover.
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.

1.10 What Can I Do If the Number of Lost Packets of a Public NAT Gateway Exceeds the Threshold (or EIP Port Allocation Exceeds the Threshold)?

If the number of lost packets exceeds the upper limit (that is, the number of allocated EIP ports exceeds the upper limit) when the public NAT gateway is in use, the EIP ports bound to the SNAT rule have been used up. You are advised to increase the number of EIPs bound to the SNAT rule.

2 Private NAT Gateways

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

Checking Security Group Rules

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

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select the desired region and project.

Step 3 Choose **Compute** > **Elastic Cloud Server**.

Step 4 In the ECS list, click the name of the ECS for which you will check the security group rules.

Step 5 Click the **Security Groups** tab and view security group rules.

Step 6 Check whether you have configured inbound and outbound rules to allow traffic to and from the ECS port.

- If yes, go to [Checking Whether Default Route Pointing to the Private NAT Gateway Is Configured in the Route Table](#).
- If no, go to [Step 7](#).

Step 7 Click **Manage Rule**. On the displayed page, click **Inbound Rules** or **Outbound Rules** to add an inbound rule and outbound rule that allow traffic to and from the ECS port.

----End

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

Step 1 Log in to the management console.

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

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.

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

You can to address this issue.

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

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

2.5 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.

2.6 Can a Private NAT Gateway Be Used Across Accounts?

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

3 SNAT Rules

3.1 Why Do I Need SNAT?

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

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

3.2 What Are SNAT Connections?

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

SNAT supports three protocols: TCP, UDP, and ICMP. A NAT gateway supports up to 55,000 concurrent connections to each destination IP address and port. If any of the destination IP address, port number, and protocol (TCP, UDP, or ICMP) changes, you can create another 55,000 connections. You can run the **netstat** command on an ECS to obtain the number of connections in the **ESTABLISHED** state, but this number reflects only the number of connections established to this ECS, and due to the impact of connection timeout, connection reuse, and other issues, this number may be different from the number of SNAT connections

maintained by the NAT gateway. Assume that an ECS creates 100 connections to a fixed destination every second and there are no interrupted TCP connections, 55,000 connections will be used up in about 10 minutes. As a result, new connections cannot be established.

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

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

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

For details about how to adjust a bandwidth, see [Modifying an EIP Bandwidth](#).

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.

3.5 What Should I Do If My ECS Fails to Access a Server on the Public Network Through a Public 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.

Modifying the Kernel Parameters 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!**, save the file, and exit.
 - c. Run the following command to make the modification take effect:
sysctl -p

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/Cloud 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.

4 DNAT Rules

4.1 Why Do I Need DNAT?

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

In a private NAT gateway, DNAT enables servers, regardless of if they are in the same AZ, to share the same transit IP address to provide services accessible from on-premises data centers or other VPCs. For details, see [Adding a DNAT Rule](#).

4.2 Can I Modify DNAT Rules?

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

4.3 What Can I Do If a DNAT Rule Is Not Working?

Checking Whether There Is a Route Pointing to the Current NAT Gateway

Check whether there is a route pointing to the public NAT gateway in the route table associated with the VPC where the public NAT gateway is located. If there is no such a route, configure one destined for the CIDR block of the public NAT gateway or 0.0.0.0/0. Otherwise, the public NAT gateway cannot receive traffic.

Checking Whether the DNAT Rule Is Correctly Configured

Check whether the DNAT rule status is **normal** on the DNAT rule list page. If the status is not normal, access will fail.

Checking the Inbound Rules of the Security Group and Network ACL of the ECS

After traffic passes through the NAT gateway, it is filtered by the security group and network ACL rules of the ECS. Check whether the security group and network ACL rules allow access from the client IP address.

Checking Whether the Service Port of the ECS Is Enabled

Check whether the service port of the ECS configured for the DNAT rule is enabled. If the service port is not enabled, the access will fail.

Run the following command on the ECS to check whether the service port is enabled:

```
netstat -tuln | grep port
```

Checking Whether the EIP Configured for the DNAT Rule Has a Bandwidth Bound

To route traffic, the EIP configured for the DNAT rule must have a bandwidth.

Checking the Domain Name Resolution and ICP Filing

If the domain name cannot be directly accessed but can be accessed through the EIP bound to it, the DNAT rule is normal. In this case, you need to check the domain name resolution and ICP filing.