NAT Gateway

FAQs

Issue	01
Date	2020-06-24



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

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

Trademarks and Permissions


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

Notice

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

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

Contents

1 NAT Gateway 1
1.1 What Is the Relationship Between a VPC, NAT Gateway, EIP Bandwidth, and ECS? 1
1.2 How Does A NAT Gateway Offer High Availability? 1
1.3 Which Ports Cannot Be Accessed? 1
1.4 What Are the Differences Between Using a NAT Gateway and Using an EIP for an ECS? 2
1.5 What Should I Do If I Fail to Access the Internet Through the NAT Gateway? 2
1.6 Can I Change the VPC for a NAT Gateway After It Is Created? 2
1.7 Does NAT Gateway Support IPv6 Addresses? 2
2 SNAT 3
2.1 Why Is SNAT Used? 3
2.2 What Are SNAT Connections? 3
2.3 What Is the Bandwidth of the NAT Gateway When a Server Accesses the Internet Through the NAT Gateway? Where Can I Configure the Bandwidth? 4
2.4 How Do I Resolve Packet Loss or Connection Failure Issues When Using a NAT Gateway? 4
2.5 What Should I Do If the Remote Server Fails to Be Accessed Through the NAT Gateway? 4
2.6 What Are the Relationships and Differences Between the CIDR Blocks in a NAT Gateway and in an SNAT Rule? 5
3 DNAT 6
3.1 Why Is DNAT Used? 6
3.2 Can I Modify DNAT Rules? 6
3.3 What Should I Do If NAT Gateway Rules Become Invalid After ECS Specifications Are Changed? 6

 Copyright © Huawei Technologies Co., Ltd.

1 NAT Gateway

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

- A VPC is a secure, isolated, logical network environment.
- A NAT gateway enables ECSs in the VPC to access the Internet.
- EIP is a service that provides valid static IP addresses on the Internet. The throughput of a VPC is determined by the EIP bandwidth.
- An ECS is a running instance in the VPC and uses the NAT gateway to access the Internet.

1.2 How Does A NAT Gateway Offer High Availability?

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

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

Copyright © Huawei Technologies Co., Ltd.

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

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

An ECS can also be directly bound to an EIP. 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 NAT gateway and an EIP for an ECS is not recommended.

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

If your server cannot access the Internet through the NAT gateway, you may 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 NAT Gateway After It Is Created?

No.

You can select a VPC when creating a NAT gateway and cannot change the VPC for the NAT gateway after it is created.

1.7 Does NAT Gateway Support IPv6 Addresses?

No.

Copyright © Huawei Technologies Co., Ltd.

2 SNAT

2.1 Why Is SNAT Used?

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

2.2 What Are SNAT Connections?

An SNAT connection consists of the source IP address, source port, destination IP address, destination port, and transmission-layer protocol. These five elements identify a connection as a unique session. The source IP address refers to the EIP, and the source port refers to the EIP port. They will be used to access the destination IP address and port of the Internet.

SNAT supports three protocols: TCP, UDP, and ICMP. A NAT gateway supports up to 55,000 concurrent connections for each destination IP address and port. If any of the destination IP address, port number, and protocol (TCP/UDP/ICMP) changes, you can create another 55,000 connections. The number of connections you query on an ECS may be different from the actual number of SNAT connections. (You can run the **netstat** command to query the number of connections.) Assume that an ECS creates 100 connections to a fixed destination every second. 55,000 connections will be used up in about 10 minutes without considering the dropped idle connections. As a result, 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. Therefore, to prevent connection interruption, you need to initiate more data packets or use TCP to maintain connections. In addition, to prevent service interruption caused by insufficient connections, you are advised to use Cloud Eye to monitor the number of SNAT connections and set proper alarms.

 Copyright © Huawei Technologies Co., Ltd.

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

NAT Gateway SNAT translates a private IP address to a public IP address by binding EIPs to servers in a VPC. When a server accesses the Internet through the NAT gateway, the bandwidth is related to the EIP bandwidth you purchased.

For details about how to change the bandwidth size, see **Modifying the Bandwidth Size**.

2.4 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 type supports, there will be packet loss or connection failures. Check whether the number of SNAT connections exceeds that the NAT gateway type supports by referring to **Querying Metrics**. If the number of connections exceeds the upper limit, change the NAT gateway type.

2.5 What Should I Do If the Remote Server Fails to Be Accessed Through the NAT Gateway?

When an ECS accesses a server on the public network through an SNAT rule, TCP connection fails. To rectify the fault, perform the following steps:

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

   sysctl -a|grep tcp_tw_recycle

   If the value of **tcp_tw_recycle** is **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 the value of **ListenDrops** is not **0**, packet loss occurs, that is, the network is faulty.

Troubleshooting

This problem can be solved by 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

 Copyright © Huawei Technologies Co., Ltd.

- 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

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

When creating an SNAT rule with **Scenario** set to **Direct Connect/Cloud Connect**, you need to configure the CIDR block of a local data center or another VPC so that ECSs in the CIDR block can access the Internet through the SNAT rule.

 Copyright © Huawei Technologies Co., Ltd.

3 DNAT

3.1 Why Is DNAT Used?

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

3.2 Can I Modify DNAT Rules?

You can modify DNAT rules.

3.3 What Should I Do If NAT Gateway Rules Become Invalid After ECS Specifications Are Changed?

If the ECS specifications are changed, the configured rules will become invalid. You will need to delete the rules and recreate them.

 Copyright © Huawei Technologies Co., Ltd.