NAT Order of Operation

Document ID: 6209

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
NAT Overview
NAT Configuration and Output
Related Information

Introduction

This document illustrates that the order in which transactions are processed using Network Address Translation (NAT) is based on whether a packet goes from the inside network to the outside network, or from the outside network to the inside network.

Prerequisites

Requirements

Readers of this document should have knowledge of this topic:

- Network Address Translation (NAT). For more information on NAT, see How NAT Works.

Components Used

This document is not restricted to specific software and hardware versions.

Note: The information in this document is based on the Software Version, Cisco IOS® Software Release 12.2(27)

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

NAT Overview

In this table, when NAT performs the global to local, or local to global, translation is different in each flow.

<table>
<thead>
<tr>
<th>Inside—to—Outside</th>
<th>Outside—to—Inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If IPSec then check input access list</td>
<td></td>
</tr>
<tr>
<td>• decryption – for CET (Cisco Encryption)</td>
<td></td>
</tr>
<tr>
<td>• If IPSec then check input access list</td>
<td></td>
</tr>
<tr>
<td>• decryption – for CET or IPSec</td>
<td></td>
</tr>
</tbody>
</table>
NAT Configuration and Output

This example demonstrates how the order of operations can effect NAT. In this case, only NAT and routing are shown.

In the previous example, Router–A is configured to translate the inside local address 171.68.200.48 to 172.16.47.150, as shown in this configuration.

```plaintext
! version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
enable password ww
!
ip nat inside source static 171.68.200.48 172.16.47.150

!--- This command creates a static NAT translation
!--- between 171.68.200.48 and 172.16.47.150

ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Ethernet0
no ip address
shutdown
```
interface Serial0
  ip address 172.16.47.161 255.255.255.240
  ip nat inside

  no ip mroute-cache
  no ip route-cache

  interface Serial1
  ip address 172.16.47.146 255.255.255.240
  ip nat outside

  no ip mroute-cache
  no ip route-cache

  no ip classless

  ip route 0.0.0.0 0.0.0.0 172.16.47.145

  !--- Configures a default route to 172.16.47.145

  ip route 171.68.200.0 255.255.255.0 172.16.47.162

  !

  line con 0
    exec-timeout 0 0

  line aux 0

  line vty 0 4
    password ww

  login

  end

The translation table indicates that the intended translation exists.

Router-A#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      171.68.200.48      ---                ---

This output is taken from Router–A with debug ip packet detail and debug ip nat enabled, and a ping issued from device 171.68.200.48 destined for 172.16.47.142.

Note: Debug commands generate a significant amount of output. Use them only when traffic on the IP network is low, so other activity on the system is not adversely affected. Before you issue debug commands, refer to Important Information on Debug Commands.

IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
  ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
  ICMP type=3, code=1
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
  ICMP type=8, code=0
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
  ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
  ICMP type=3, code=1
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
  ICMP type=8, code=0
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
ICMP type=3, code=1

Since there are no NAT debug messages in the previous output, you know that the existing static translation is not used and that the router does not have a route for the destination address (172.16.47.142) in its routing table. The result of the non-routable packet is an ICMP Unreachable message, which is sent to the inside device.

But, Router–A has a default route of 172.16.47.145, so why is the route considered non-routable?

Router–A has no ip classless configured, which means if a packet destined for a "major" network address (in this case, 172.16.0.0) for which subnets exist in the routing table, the router does not rely on the default route. In other words, if you issue the no ip classless command, this turns off the ability of the router to look for the route with the longest bit match. In order to change this behavior, you have to configure ip classless on Router–A. The ip classless command is enabled by default on Cisco routers with Cisco IOS Software Releases 11.3 and later.

```
Router−A#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
Router−A(config)#ip classless
Router−A(config)#end
```

When you repeat the same ping test as previously done, you see that the packet gets translated and the ping is successful.

```
Ping Response on device 171.68.200.48
D:\>ping 172.16.47.142
Pinging 172.16.47.142 with 32 bytes of data:

Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.47.142:
   Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli−seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

Debug messages on Router A indicating that the packets generated by device 171.68.200.48 are getting translated by NAT.
```

```
Router−A#
*Mar 28 03:34:28: IP: tableid=0, s=171.68.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [160]
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1),
g=172.16.47.145, len 100, forward
*Mar 28 03:34:28: ICMP type=8, code=0
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial0), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
```
The previous example shows that when a packet traverses inside to outside, a NAT router checks its routing table for a route to the outside address before it continues to translate the packet. Therefore, it is important that the NAT router has a valid route for the outside network. The route to the destination network must be known through an interface that is defined as NAT outside in the router configuration.

It is important to note that the return packets are translated before they are routed. Therefore, the NAT router must also have a valid route for the Inside local address in its routing table.

Related Information

- Configuring Network Address Translation: Getting Started
- Verifying NAT Operation and Basic NAT Troubleshooting
- NAT: Local and Global Definitions
- How Does Multicast NAT Work on Cisco Routers?
- NAT Support Page
- Technical Support & Documentation – Cisco Systems