Configuring Static and Dynamic NAT Simultaneously

Document ID: 13778

Contents

Introduction

In some situations, you may find it necessary to configure both static and dynamic Network Address Translation (NAT) commands on a Cisco router. This document explains how you can do this, and gives a sample scenario.

Prerequisites

Requirements

Knowledge of basic NAT concepts and operations is helpful.

- How NAT Works
- NAT Order of Operation

For additional information, please see the Related Information section of this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 3600 Series routers
- Cisco IOS® Software Release 12.3(3)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

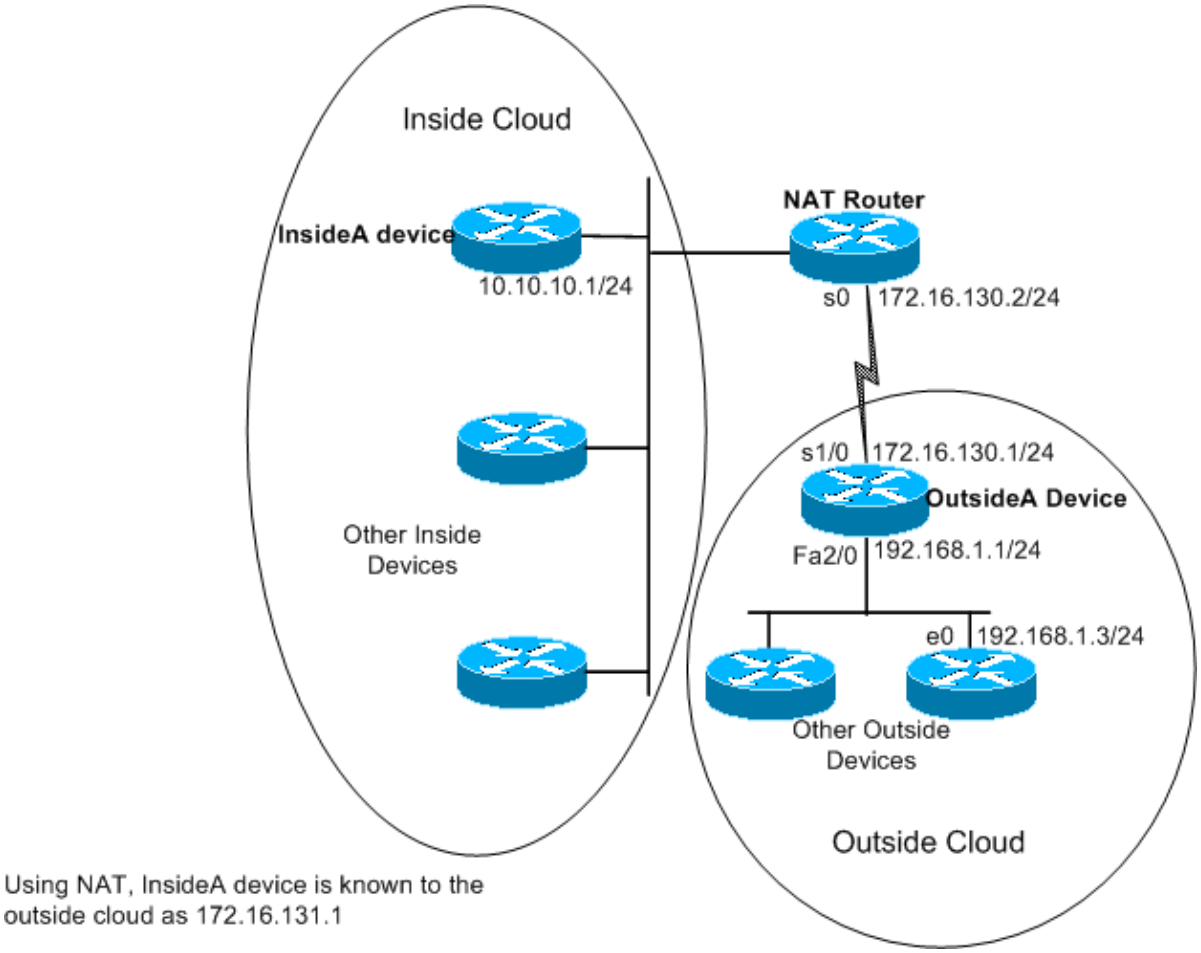
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configuring NAT

With dynamic NAT, translations do not exist in the NAT table until the router receives traffic that requires translation. Dynamic translations have a timeout period after which they are purged from the translation table.

With static NAT, translations exist in the NAT translation table as soon as you configure static NAT command(s), and they remain in the translation table until you delete the static NAT command(s).

The following network diagram is an example:



These commands are configured on the NAT router shown above:

NAT Router

`version 12.3`
 	
`ip nat pool test 172.16.131.2 172.16.131.10 netmask 255.255.255.0`
 	
`!--- Refer to`
`ip nat pool`
`for more details on the command.`
`.`
 	
`ip nat inside source list 7 pool test`
 	
`!--- Refer to`
`ip nat inside source`
`for more details on the command.`

```
ip nat inside source static 10.10.10.1 172.16.131.1

 interface e 0

 ip address 10.10.10.254 255.255.255.0

 ip nat inside

 interface s 0

 ip address 172.16.130.2 255.255.255.0

 ip nat outside

ip route 192.168.1.0 255.255.255.0 172.16.130.1

 access-list 7 permit 10.10.10.0 0.0.0.255
```

The configuration on the OutsideA device is:

OutsideA Router

```
version 12.3
hostname outsideA

!
!
!
interface Serial1/0

ip address 172.16.130.1 255.255.255.0

serial restart-delay 0

clockrate 64000

!

interface FastEthernet2/0

ip address 192.168.1.1 255.255.255.0

speed auto

half-duplex

ip route 172.16.131.0 255.255.255.0 172.16.130.2
```

The configuration on the InsideA device is:

InsideA Router

```
version 12.3

!
interface Ethernet1/0
 ip address 10.10.10.1 255.255.255.0
 half-duplex
!
ip route 0.0.0.0 0.0.0.0 10.10.10.254
!
!
```

Using the **show ip nat translations** command, you can see the contents of the translation table:

```
NATrouter#show ip nat translations
Pro Inside global    Inside local    Outside local    Outside global
--- 172.16.131.1     10.10.10.1      ---              ---
```

Notice that only the static translation is listed in the translation table. This entry translates the inside global address back to the inside local address, which means that devices on the outside cloud can send packets to the global address 172.16.131.1 and reach the device on the inside cloud, which has the local address 10.10.10.1.

The same is shown below:

```
outsideA#ping 172.16.131.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.131.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms



NATrouter#debug ip nat

18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1005]
18:12:06: NAT: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1005]
18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1006]
18:12:06: NAT*: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1006]
18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1007]
18:12:06: NAT*: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1007]
18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1008]
18:12:06: NAT*: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1008]
18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1009]
18:12:06: NAT*: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1009]
```

No other translations are generated or entered into the translation table until the router receives a packet on its inside interface with a source address permitted by access control list (ACL) 7.

However, since there are not any dynamic translations entered yet, outside devices cannot reach any of the inside devices (other than 10.10.10.1), not even if they send packets to a global address (172.16.131.2 through 172.16.131.10). When the router receives a packet destined for one of these global addresses, it checks the translation table for an existing translation. If there is none, it tries to route the packet. This NAT behavior is discussed further in Sample Configuration Using the **ip nat outside source list** Command and Sample Configuration Using the **ip nat outside source static** Command.

In the above topology, if communication between inside and outside network devices is only originated by the inside devices, dynamic translation works fine. But what if an email server is added on the inside network that needs to receive packets originated by the outside? Now you have to configure a static NAT entry so that email servers on the outside can originate communication with the email server on the inside. If in the example above the email server is the device with the local address of 10.10.10.1, you already have a static translation.

However, in cases where you do not have many global addresses to spare and you need to statically configure a single device for NAT, you can use a configuration such as the one below:

NAT Router
`ip nat inside source list 7 interface serial 0 overload`

```
ip nat inside source static tcp 10.10.10.1 25 172.16.130.2 25

!--- Refer to
ip nat inside source
 for more details on the command.


 interface e 0

 ip address 10.10.10.254 255.255.255.0

 ip nat inside

!--- For more details the ip nat inside|outside command,
!--- please refer to
ip nat inside
.


 interface s 0

ip address 172.16.130.2 255.255.255.0

ip nat outside

 access-list 7 permit 10.10.10.0 0.0.0.255

 ip route 0.0.0.0 0.0.0.0 172.16.130.1
```

In the above example, NAT is configured to overload on Serial 0's IP address. This means that more than one inside local address can be dynamically translated to the same global address, in this case, the address assigned to Serial 0. In addition, NAT is statically configured so that packets sourced from local address 10.10.10.1 with TCP port 25 (SMTP) are translated to Serial 0's IP address TCP port 25. Since this is a static NAT entry, email servers on the outside can originate SMTP (TCP port 25) packets to the global address of 172.16.131.254.

Note: Although it is possible to use the same global address for both the Dynamic and Static NAT, whenever possible it is better to use different global addresses.

The NAT translation table has the following entry:

```
NATRouter#show ip nat translations

   Pro Inside global    Inside local   Outside local Outside global

   tcp 172.16.130.2:25  10.10.10.1:25      ---           ---
```

The **debug ip nat** output shows the NAT translation when the outsideA device accesses InsideA:

```
04:21:16: NAT: s=192.168.1.3, d=172.16.130.2->10.10.10.1    [9919]

   04:21:16: NAT: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [0]

   04:21:16: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9922]

   04:21:16: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9923]

   04:21:16: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [1]

   04:21:16: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [2]

   04:21:16: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [3]
```

```
04:21:16: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9927]

04:21:16: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [4]

04:21:16: NAT: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [5]

04:21:16: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9931]

04:21:17: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9934]

04:21:17: NAT: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9935]

04:21:17: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [6]
```

In summary, dynamic NAT requires packets to be switched through the NAT router in order to generate NAT translations in the translation table. If you use the **ip nat inside** command, these packets must originate from the inside. If you use the **ip nat outside** command, these packets must originate on the outside.

Static NAT does not require packets to be switched through the router, and translations are statically entered into the translation table.

Related Information

- **NAT Frequently Asked Questions**
- **NAT Technical Support Page**
- **Technical Support − Cisco Systems**

Updated: Jan 24, 2006 Document ID: 13778