Sample Configuration Using the ip nat outside source list Command

Document ID: 13770

Contents

Introduction

This document provides a sample configuration with the **ip nat outside source list** command, and includes a brief description of what happens to the IP packet during the NAT process. You can use this command to translate the source address of the IP packets that travel from outside of the network to inside the network. This action translates the destination address of the IP packets that travel in the opposite direction from inside to outside of the network. This command is useful in situations such as overlapping networks, where the inside network addresses overlap addresses that are outside the network. Let us consider the network diagram as an example.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions. However, the information in this document is based on these software and hardware versions:

- Cisco 2500 series routers
- Cisco IOS® Software Release 12.2(24a) running on all the routers

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 Cisco Technical Tips Conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:
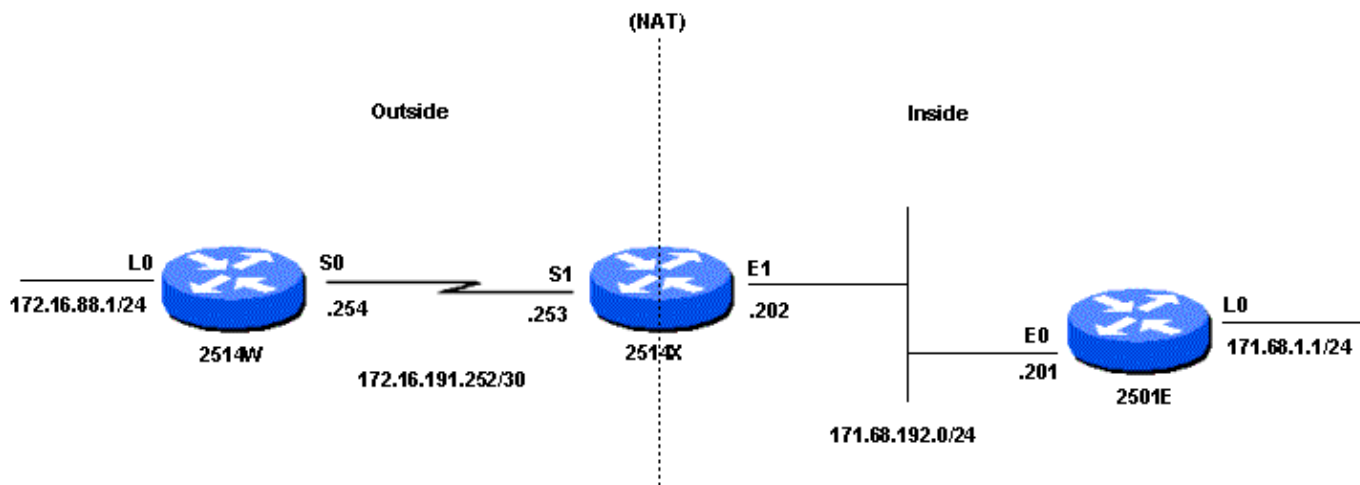
When ping is sourced from the Router 2514W Loopback0 interface (172.16.88.1) to the Router 2501E Loopback0 interface (171.68.1.1), this occurs:

The Router 2514W forwards the packets to Router 2514X because it is configured with a default route. On the outside interface of Router 2514X, the packet has a source address (SA) of 172.16.88.1 and a Destination Address (DA) of 171.68.1.1. Because the SA is permitted in access−list 1, which is used by the **ip nat outside source list** command, it is translated to an address from the NAT pool Net171. Notice that the **ip nat outside source list** command references the NAT pool "Net171". In this case, the address is translated to 171.68.16.10 which is the first available address in the NAT pool. After translation, Router 2514X looks for the destination in the routing table, and routes the packet. Router 2501E sees the packet on its incoming interface with a SA of 171.68.16.10 and a DA of 171.68.1.1. It responds by sending an Internet Control Message Protocol (ICMP) echo reply to 171.68.16.10. If it doesn't have a route, it drops the packet. In this case, it has a (default) route, so it sends a packet to Router 2514X, using an SA of 171.68.1.1 and a DA of 171.68.16.10. Router 2514X sees the packet on its inside interface and checks for a route to the 171.68.16.10 address. If it does not have one, it responds with an ICMP unreachable reply. In this case, it has a route to 171.68.16.10, due to the **add−route** option of the **ip nat outside source** command which adds a host route based on the translation between the outside global and outside local address, so it translates the packet back to the 172.16.88.1 address, and routes the packet out its outside interface.

Configurations

Router 2514W

```
hostname 2514W
!

!--- Output suppressed.

interface Loopback0
 ip address 172.16.88.1 255.255.255.0
!

!--- Output suppressed.

interface Serial0
 ip address 172.16.191.254 255.255.255.252
 no ip mroute-cache
!

!--- Output suppressed.

ip classless
ip route 0.0.0.0 0.0.0.0 172.16.191.253

!--- Default route to forward packets to 2514X.


!

!--- Output suppressed.
```

Router 2514X

```
hostname 2514X
!

!--- Output suppressed.

!
interface Ethernet1
 ip address 171.68.192.202 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
!

!--- Output suppressed.

interface Serial1
 ip address 172.16.191.253 255.255.255.252
 ip nat outside
 no ip mroute-cache
 no ip route-cache
 clockrate 2000000
!
ip nat pool Net171 171.68.16.10 171.68.16.254 netmask 255.255.255.0

!--- NAT pool defining Outside Local addresses to be used for translation.


!
ip nat outside source list 1 pool Net171 add-route

!--- Configures translation for Outside Global addresses
```

```
!--- with the NAT pool.


ip classless
ip route 172.16.88.0 255.255.255.0 172.16.191.254
ip route 171.68.1.0 255.255.255.0 171.68.192.201

!--- Static routes for reaching the loopback interfaces
!--- on 2514W and 2501E.


access-list 1 permit 172.16.88.0 0.0.0.255

!--- Access-list defining Outside Global addresses to be translated.



!

!--- Output suppressed.

!
```

Router 2501E

```
hostname 2501E
!

!--- Output suppressed.

interface Loopback0
 ip address 171.68.1.1 255.255.255.0
!
interface Ethernet0
 ip address 171.68.192.201 255.255.255.0
!

!--- Output suppressed.

ip classless
ip route 0.0.0.0 0.0.0.0 171.68.192.202

!--- Default route to forward packets to 2514X.



!

!--- Output suppressed.
```

Verify

This section provides information you can use to confirm that your configuration is works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

The **show ip nat translations** command can be used to check the translation entries, as shown in the output below.

```
2514X# show ip nat translations
Pro Inside global    Inside local      Outside local      Outside global
--- 171.68.1.1        171.68.1.1        171.68.16.10       172.16.88.1
```

```
--- ---                    ---                    171.68.16.10        172.16.88.1

2514X#
```

The above output shows that the Outside Global address 172.16.88.1, which is the address on Loopback0 interface of router 2514W, gets translated to the Outside Local address 171.68.16.10.

You can use the **show ip route** command to check the routing table entries, as shown:

```
2514X# show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP
       D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
       N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2
       E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
       i – IS-IS, su – IS-IS summary, L1 – IS-IS level-1, L2 – IS-IS level-2
       ia – IS-IS inter area, * – candidate default, U – per-user static route
       o – ODR, P – periodic downloaded static route

Gateway of last resort is not set

     171.68.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       171.68.192.0/24 is directly connected, Ethernet1
S       171.68.1.0/24 [1/0] via 171.68.192.201
S       171.68.16.10/32 [1/0] via 172.16.88.1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S       172.16.88.0/24 [1/0] via 172.16.191.254
C       172.16.191.252/30 is directly connected, Serial1
2514X#
```

The output shows a /32 route for the Outside Local address 171.68.16.10, which is created due to the **add−route** option of the **ip nat outside source** command. This route is used for routing and translating packets that travel from the inside to the outside of the network.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

This output is the result of running the **debug ip packet** and **debug ip nat** commands on Router 2514X, while pinging from the Router 2514W loopback0 interface address (172.16.88.1) to the Router 2501E loopback0 interface address (171.68.1.1):

```
*Mar  1 00:02:48.079: NAT*: s=172.16.88.1–>171.68.16.10, d=171.68.1.1 [95]

!--- The source address in the first packet arriving on
!--- the outside interface is first translated.


*Mar  1 00:02:48.119: IP: tableid=0, s=171.68.16.10 (Serial1), d=171.68.1.1 (Ethernet1), r
RIB
*Mar  1 00:02:48.087: IP: s=171.68.16.10 (Serial1), d=171.68.1.1 (Ethernet1), g=171.68.192
100, forward

!--- The ICMP echo request packet with the translated source address
!--- is routed and forwarded on the inside interface.


*Mar  1 00:02:48.095: IP: tableid=0, s=171.68.1.1 (Ethernet1), d=171.68.16.10 (Serial1), r
RIB

!--- The ICMP echo reply packet arriving on the inside interface
!--- is first routed based on the destination address.
```

```
*Mar  1 00:02:48.099: NAT: s=171.68.1.1, d=171.68.16.10->172.16.88.1 [95]
```

```
*Mar  1 00:02:48.103: IP: s=171.68.1.1 (Ethernet1), d=172.16.88.1 (Serial1), g=172.16.191.
00, forward
```

The above procedure is repeated for every packet received on the outside interface.

Summary

The major difference between using the **ip nat outside source list** command (dynamic NAT) instead of the **ip nat outside source static** command (static NAT) is that there are no entries in the translation table until the router (configured for NAT) verifies the translation criteria of the packet. In the example above, the packet with the SA 172.16.88.1 (which comes into the outside interface of Router 2514X) satisfies access–list 1, the criteria used by the **ip nat outside source list** command. For this reason, packets must originate from the outside network before packets from the inside network can communicate with the Router 2514W loopback0 interface.

There are two important things to note in this example.

First, when the packet travels from outside to inside, translation occurs first, and then the routing table is checked for the destination. When the packet is travels from inside to outside, the routing table is checked for the destination first, and then translation occurs.

Second, it's important to note which part of the IP packet gets translated when using each of the commands above. The following table contains a guideline:

Command	Action
ip nat outside source list	• translates the source of the IP packets that are traveling outside to inside • translates the destination of the IP packets that are traveling inside to outside
ip nat inside source list	• translates the source of IP packets that are traveling inside to outside • translates the destination of the IP packets that are traveling outside to inside

What the above guidelines indicate is that there is more than one way to translate a packet. Depending on your specific needs, you should determine how to define the NAT interfaces (inside or outside) and what routes the routing table should contain before or after translation. Keep in mind that the portion of the packet that will be

translated depends upon the direction the packet is traveling, and how you configured NAT.

Related Information

- **How NAT works**
- **NAT: Local and Global Definitions**
- **Sample Configuration Using the ip nat outside source static Command**
- **NAT Order of Operation**
- **Using NAT in Overlapping Networks**
- **Network Address Translation on a Stick**
- **NAT Technology Support Page**
- **Technical Support – Cisco Systems**

Updated: Jan 24, 2006   Document ID: 13770