Configure IP NAT Outside Source List Command

Contents

Introduction

This document describes how to configure the ip nat outside source list command and describes what happens to the IP packet during the NAT process.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Routers running Cisco IOS® Software Release.

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, ensure that you understand the potential impact of any command.

Background Information

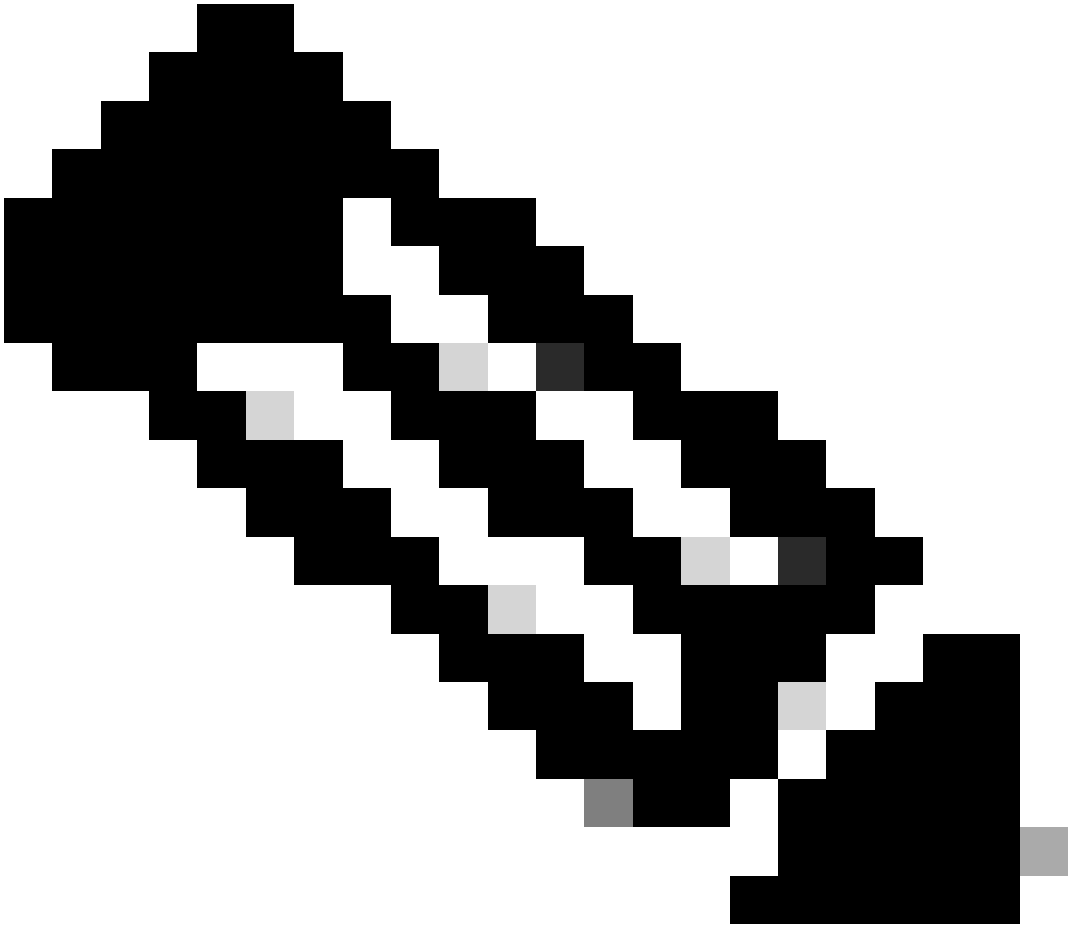
You can use this command to translate the source address of the IP packets that travel from outside of the network to inside the network. This action translates the destination address of the IP packets that travel in the opposite direction—from inside to outside of the network. This command is useful 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.

Conventions

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

Configure

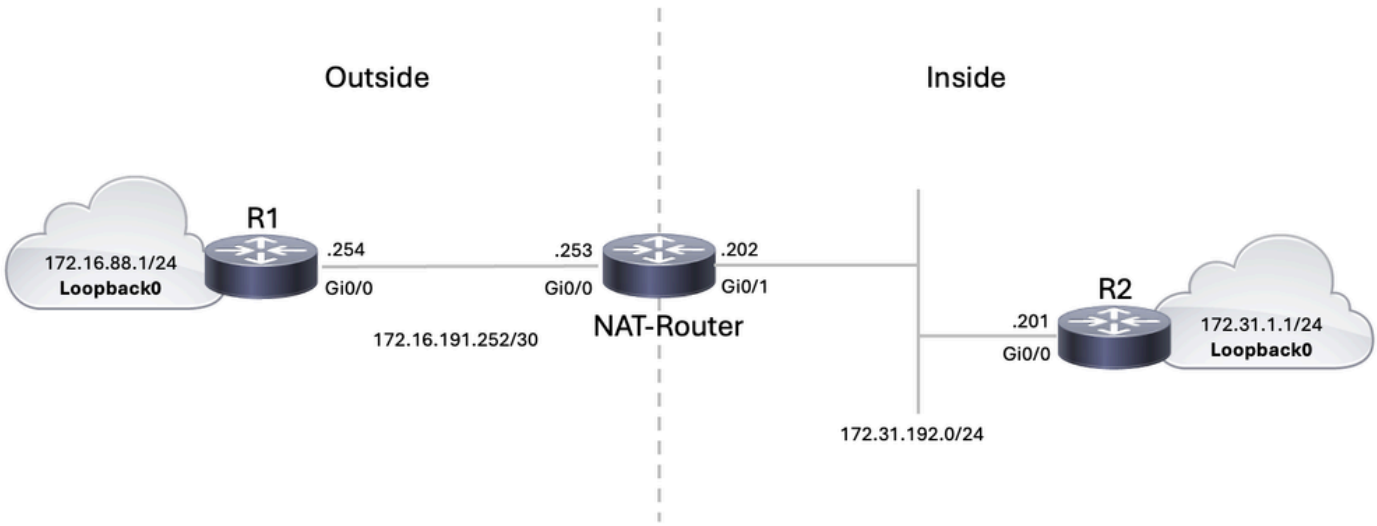
In this section, you are presented with the information to configure the features described in this document.



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:



Network Diagram

When a ping is sourced from the Router R1 Loopback0 interface (172.16.88.1) to the Router R2 Loopback0 interface (172.31.1.1), the next sequence of events occurs:

1. **Packet Forwarding:** Router R1 forwards the packets to the NAT-Router because it is configured with a default route. On the outside interface of the NAT-Router, the packet has a source address (SA) of 172.16.88.1 and a destination address (DA) of 172.31.1.1.
2. **NAT Translation:** Since the SA is permitted by access-list 1, which is used by the **ip nat outside source list** command, it is translated to an address from the NAT pool "NET". In this case, the address is translated to 172.31.16.10, which is the first available address in the NAT pool.
3. **Routing to Destination:** After translation, the NAT-Router looks for the destination in its routing table and routes the packet. Router R2 receives the packet on its incoming interface with an SA of 172.31.16.10 and a DA of 172.31.1.1. Router R2 responds by sending an Internet Control Message Protocol (ICMP) echo reply to 172.31.16.10. If Router R2 does not have a route to 172.31.16.10, it drops the packet.
4. **Reply Handling:** In this case, Router R2 has a default route, so it sends the reply packet to the NAT-Router, using an SA of 172.31.1.1 and a DA of 172.31.16.10. The NAT-Router receives the packet on its inside interface and checks for a route to the 172.31.16.10 address. If it does not have a route, it responds with an ICMP unreachable reply.
5. **Translation and Routing Back:** In this case, the NAT-Router has a route to 172.31.16.10 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. The NAT-Router translates the packet back to the original source address (172.16.88.1) and routes the packet out its outside interface back to Router R1.

Configurations

Router R1

```
hostname R1
!

!--- Output suppressed.

!
interface Loopback0
 ip address 172.16.88.1 255.255.255.0
```

```
!

!--- Output suppressed.

!
interface GigabitEthernet0/0
 ip address 172.16.191.254 255.255.255.252
 duplex auto
 speed auto
!

!--- Output suppressed.

ip route 0.0.0.0 0.0.0.0 172.16.191.253

!--- Default route to forward packets to NAT-Router.
!--- Output suppressed.
```

Router NAT-Router

```
hostname NAT-Router
!

!--- Output suppressed.

!
interface GigabitEthernet0/0
 ip address 172.16.191.253 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.31.192.202 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
ip nat pool NET 172.31.16.10 172.31.16.254 netmask 255.255.255.0

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

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

!--- Configures translation for Outside Global addresses !--- with the NAT pool.

!
ip route 172.16.88.0 255.255.255.0 172.16.191.254
ip route 172.31.1.0 255.255.255.0 172.31.192.201
!

!--- Static routes for reaching the loopback interfaces on R1 and R2.
```

```
!
access-list 1 permit 172.16.88.0 0.0.0.255
!

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

Router R2

```
hostname R2
!

!--- Output suppressed.

interface Loopback0
 ip address 172.31.1.1 255.255.255.0
!
!
interface GigabitEthernet0/0
 ip address 172.31.192.201 255.255.255.0
 duplex auto
 speed auto
!

!--- Output suppressed.

ip route 0.0.0.0 0.0.0.0 172.31.192.202

!--- Default route to forward packets to NAT-Router.
!--- 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 this output:

```
<#root>

NAT-Router#

show ip nat translations


Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                172.31.16.10       172.16.88.1
icmp 172.31.1.1:0      172.31.1.1:0       172.31.16.10:0     172.16.88.1:0
NAT-Router#
```

The output shows that the Outside Global address 172.16.88.1, which is the address on Loopback0 interface of router R1, gets translated to the Outside Local address 172.31.16.10.

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

```
<#root>

NAT-Router#

show ip route

Codes: L - local, C - connected, S - static, 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
       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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
S        172.16.88.0/24 [1/0] via 172.16.191.254
C        172.16.191.252/30 is directly connected, GigabitEthernet0/0
L        172.16.191.253/32 is directly connected, GigabitEthernet0/0
      172.31.0.0/16 is variably subnetted, 4 subnets, 2 masks
S        172.31.1.0/24 [1/0] via 172.31.192.201

S        172.31.16.10/32 [1/0] via 172.16.88.1

C        172.31.192.0/24 is directly connected, GigabitEthernet0/1
L        172.31.192.202/32 is directly connected, GigabitEthernet0/1
NAT-Router#
```

The output shows a /32 route for the Outside Local address 172.31.16.10, 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 NAT-Router, while pinging from the Router R1 loopback0 interface address (172.16.88.1) to the Router R2 loopback0 interface address (172.31.1.1):

```
<#root>

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

*Oct  4 20:26:48.839: NAT: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [0]
```

```
!--- The ICMP echo request packet with the translated source address is routed and forwarded on th

*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1),
*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1),
*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1),
*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1),

*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1),

*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1),

!--- The ICMP echo reply packet arriving on the inside interface, is first routed based on the des

Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input feature
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input featur
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input featur
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input featur
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.31.16.10, len 100, input featur

!--- The destination address in the packet is then translated.


*Oct 4 20:26:48.841: NAT: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [0]


!--- The ICMP echo reply packet with the translated destination address is forwarded on the outsid

*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), l
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), l
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), l
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), l

*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), g

*Oct  4 20:26:48.843: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), l


*Oct  4 20:26:48.845: NAT*: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [1]
*Oct  4 20:26:48.846: NAT*: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [1]
*Oct  4 20:26:48.848: NAT*: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [2]
*Oct  4 20:26:48.849: NAT*: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [2]
*Oct  4 20:26:48.851: NAT*: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [3]
*Oct  4 20:26:48.852: NAT*: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [3]
*Oct  4 20:26:48.854: NAT*: s=172.16.88.1->172.31.16.10, d=172.31.1.1 [4]
*Oct  4 20:26:48.855: NAT*: s=172.31.1.1, d=172.31.16.10->172.16.88.1 [4]
```

The previous 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 previous example, the packet with the SA 172.16.88.1 (which comes into the outside interface of NAT-Router) 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 Router R1 loopback0 interface.

There are two important things to note in this example:

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

2. It is important to note which part of the IP packet gets translated when using each of the previous commands. This next table provides 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 these guidelines indicate is that there is more than one way to translate a packet. Depending on your specific needs, you can determine how to define the NAT interfaces (inside or outside) and what routes the routing table contains before or after translation. Keep in mind that the portion of the packet that is translated depends upon the direction the packet is traveling, and how you configured NAT.

Related Information

- **Network Address Translation on a Stick**
- **NAT Technology Support Page**
- **Technical Support - Cisco Systems**