

使用 ip nat outside source list 命令的示例配置

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[摘要](#)

[相关信息](#)

简介

本文档提供了使用 ip nat outside source list 命令的配置示例，并简要介绍了 NAT 过程中 IP 数据包所发生的情况。您可以使用此命令，转换从网络外部向网络内部传输的 IP 数据包的源地址。此操作可以转换以相反方向（从网络内部向网络外部）传输的 IP 数据包的目标地址。此命令在重叠网络等情况下非常有用，因为此时网络内部地址与网络外部地址相互重叠。让我们考虑以[网络图为例](#)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。但是，本文档中的信息基于以下软件和硬件版本：

- Cisco 2500 系列路由器
- 在所有路由器上运行的 Cisco IOS® 软件版本 12.2(24a)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

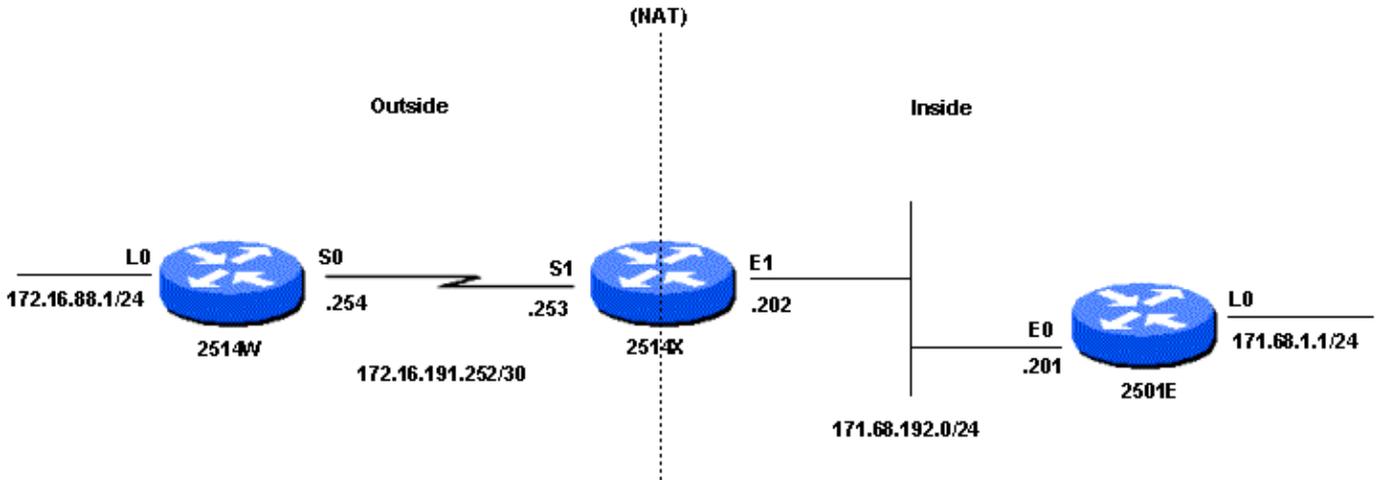
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用[命令查找工具](#)(仅注册客户)。

网络图

本文档使用以下网络设置：



当 ping 从路由器 2514W Loopback0 接口 (172.16.88.1) 发往路由器 2501E Loopback0 接口 (171.68.1.1) 时，会发生以下情况：

因为配置了默认路由，路由器 2514W 会将数据包转发给路由器 2514X。在路由器 2514X 的外部接口上，数据包的源地址(SA)为 172.16.88.1，目的地址(DA)为 171.68.1.1。因为 SA 允许在访问列表 1 中，而 `ip nat outside source list` 则使用命令，它转换为 NAT 池 Net171 的地址。请注意，`ip nat outside source list` 命令引用 NAT 池“Net171”。在这种情况下，地址被转换为 NAT 池中的第一个可用地址 171.68.16.10。转换后，路由器 2514X 在路由表中查找目的地并路由数据包。路由器 2501E 在其传入接口上看到数据包的 SA 为 171.68.16.10，DA 为 171.68.1.1。它通过向 171.68.16.10 发送 Internet 控制消息协议(ICMP)应答来作出响应。如果它没有路由，它会丢弃数据包。在这种情况下，它有 (默认) 路由，因此它使用 SA 171.68.1.1 和 DA 171.68.16.10 向路由器 2514X 发送数据包。路由器 2514X 在其内部接口上看到数据包，并检查通往 171.68.16.10 的路由。如果该路由器没有这样一个路由，就会发送一个 ICMP 不可达的应答作为响应。在本例中，由于 `ip nat outside source` 命令的 `add-route` 选项会根据外部全局地址和外部本地地址之间的转换添加一个主机路由，该路由器具备一个指向 171.68.16.10 的路由，因此它会将该数据包转换回 172.16.88.1 地址，然后将该数据包路由出其外部接口。

配置

路由器 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.
```

路由器 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. !
```

路由器 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.
```

验证

您可以使用本部分提供的信息来确认您的配置运行正常。

[命令输出解释程序工具（仅限注册用户）支持某些 show 命令](#)，使用此工具可以查看对 show 命令输出的分析。

如下面的输出所示，[show ip nat translations 命令可用于检查转换项。](#)

```
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#
```

上面的输出显示，路由器 2514W 的 Loopback0 接口上的地址，外部全局地址 172.16.88.1，被转换为外部本地地址 171.68.16.10。

如下所示，您可以使用 [show ip route 命令检查路由表项](#)：

```
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#
```

输出显示了外部本地地址 171.68.16.10 的一个 /32 路由，该路由是通过 `ip nat outside source` 命令的 `add-route` 选项创建的。此路由用于路由和转换从网络内部传输到网络外部的数据包。

故障排除

本部分提供的信息可用于对配置进行故障排除。

此输出是在路由器2514X上运行`debug ip packet`和`debug ip nat`命令，同时从路由器2514W loopback0接口地址(172.16.88.1)ping路由器2501E loopback0接口地址(171)的结果。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), routed via
RIB
*Mar 1 00:02:48.087: IP: s=171.68.16.10 (Serial1), d=171.68.1.1 (Ethernet1), g=171.68.192.201,
len
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), routed via
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]
!--- The destination address in the packet is then translated. *Mar 1 00:02:48.103: IP:
s=171.68.1.1 (Ethernet1), d=172.16.88.1 (Serial1), g=172.16.191.254, len 1
00, forward
!--- The ICMP echo reply packet with the translated destination !--- address is forwarded on the
outside interface.
```

上述过程会对在外部接口上收到的每个数据包都重复一次。

摘要

使用 `ip nat outside source list` 命令 (动态 NAT) 而不是 `ip nat outside source static` 命令 (静态 NAT) 的主要区别在于，在 (为 NAT 配置的) 路由器检验数据包的转换标准之前，在转换表中没有

条目。在上述示例中，SA 为 172.16.88.1 的数据包（进入路由器 2514x 的外部接口）符合访问列表 1，即 **ip nat outside source list 命令使用的标准**。因此，在内部网络数据包可以与路由器 2514w 的 loopback0 接口通信之前，必须先从外部网络始发数据包。

本例中需要注意两点：

当信息包从外向里移动时，首先进行转换，然后通过路由表检查目的地。当数据包从内部传输到外部时，先检查目的地的路由表，然后进行转换。

第二，使用上述每条命令时，记录IP数据包的哪个部分被转换很重要。下表给出了一个纲要：

命令	操作
ip nat outside source list	<ul style="list-style-type: none">• 转换IP包的源，这些IP包正在从外部传输到内部• 转换IP包的目的地，这些IP包正在从内部传输到外部
ip nat inside source list	<ul style="list-style-type: none">• 转换IP包的源，这些IP包正在从内部传输到外部• 转换IP包的目的地，这些IP包正在从外部传输到内部

上述指导显示：转换信息包的方法不止一种。根据您的特定需要，您需要确定如何定义NAT接口(内部或外部)以及转换前后由什么来路由路由表。记住被转换的信息包部分取决于信息包移动的方向以及您如何配置NAT的。

[相关信息](#)

- [单接口网络地址转换](#)
- [NAT 技术支持页](#)
- [技术支持 - Cisco Systems](#)