配置IP NAT外部源列表命令

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)
- [背景信息](#)
- [规则](#)

[配置](#)

- [网络图](#)
- [配置](#)

[验证](#)

[故障排除](#)

[摘要](#)

[相关信息](#)

简介

本文档介绍如何配置命令ip nat outside source list，并介绍在NAT过程中IP数据包会发生什么情况。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于运行Cisco IOS®软件版本的Cisco路由器。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

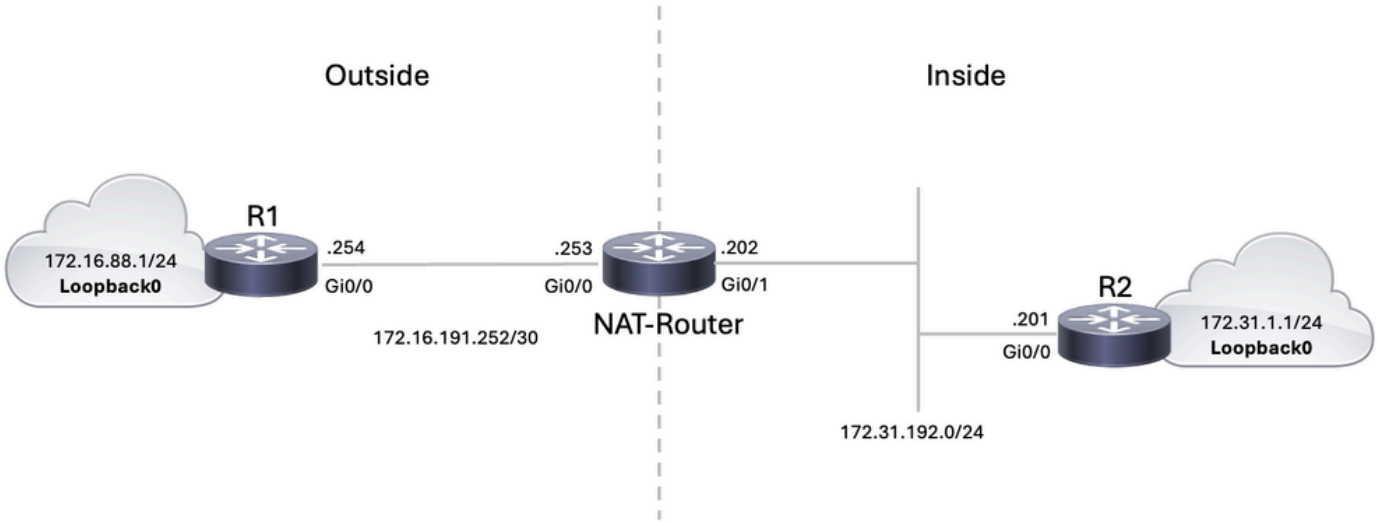
配置

本部分提供有关如何配置本文档所述功能的信息。

> 注意：要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：



网络图

当从路由器R1的环回接口0接口(172.16.88.1)向路由器R2的环回接口0接口(172.31.1.1)发出ping命令时，将会发生以下下一系列事件：

1. 数据包转发:路由器R1将数据包转发到NAT路由器，因为它配置了默认路由。在NAT路由器的外部接口上，数据包的源地址(SA)为172.16.88.1，目的地址(DA)为172.31.1.1。
2. NAT转换：由于ip nat outside source list命令使用的access-list 1允许SA，因此将其转换为NAT池“NET”中的地址。 在这种情况下，地址将转换为172.31.16.10，这是NAT池中的第一个可用地址。
3. 路由至目标：转换后，NAT路由器在其路由表中查找目标并路由数据包。路由器R2在其传入接口上接收该数据包，其SA为172.31.16.10,DA为172.31.1.1。路由器R2通过向172.31.16.10发送Internet控制消息协议(ICMP)回应应答进行响应。如果路由器R2没有通往172.31.16.10的路由，则会丢弃该数据包。
4. 回复处理：在这种情况下，路由器R2具有默认路由，因此它使用SA 172.31.1.1和DA 172.31.16.10将应答数据包发送到NAT路由器。NAT路由器在其内部接口上接收数据包，并检查通向172.31.16.10地址的路由。如果它没有路由，则会使用ICMP不可达应答进行响应。
5. 转换和传回：在这种情况下，由于ip nat outside source命令的add-route选项，NAT-Router具有通往172.31.16.10的路由，该选项根据外部全局地址和外部本地地址之间的转换添加主机路

由。NAT路由器将数据包转换回原始源地址(172.16.88.1)，并将数据包从其外部接口路由回路由器R1。

配置

路由器 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.
```

路由器NAT — 路由器

```
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.
```

路由器 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.
```

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。

Output Interpreter Tool（仅限注册用户）支持某些show命令，使用此工具可以查看命令输出的**show**分析。

show ip nat translations命令可用于检查转换条目，如以下输出所示：

```
<#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#
```

输出显示，外部全局地址172.16.88.1（路由器R1的Loopback0接口上的地址）被转换为外部本地地址172.31.16.10。

如下所示，您可以使用 show ip route 命令检查路由表项：

```
<#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#
```

输出显示了外部本地地址 172.31.16.10 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。

以下输出是在路由器NAT-Router上运行debug ip packet和debug ip nat命令的结果，同时从路由器R1的loopback0接口地址(172.16.88.1)对路由器R2的loopback0接口地址(172.31.1.1)执行ping操作：

```
<#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 the ins

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

*Oct  4 20:26:48.839: IP: s=172.31.16.10 (GigabitEthernet0/0), d=172.31.1.1 (GigabitEthernet0/1), g=172.

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

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

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

!--- 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 outside int

*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10
*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10

*Oct  4 20:26:48.841: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), g=172.1

*Oct  4 20:26:48.843: IP: s=172.31.1.1 (GigabitEthernet0/1), d=172.16.88.1 (GigabitEthernet0/0), len 10


*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]
```

对外部接口上接收的每个数据包重复上述过程。

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。在上一个示例中，SA为172.16.88.1的数据包（进入NAT-Router的外部接口）满足access-list 1，即ip nat outside source list命令所使用的标准。因此，数据包必须来自外部网络，内部网络的数据包才能与路由器R1的loopback0接口通信。

此示例中需要注意两个重要事项：

1.当数据包从外部传输到内部时，首先进行转换，然后检查路由表以查找目的地。当数据包从内部传输到外部时，首先检查路由表以查找目的地，然后进行转换。

2.必须注意的是，使用前面所述的每个命令时，IP数据包的哪一部分会被转换。下表提供了指南：

命令	操作
ip nat outside source list	• 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	• 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

这些指导原则表明，转换数据包的方式不止一种。根据您的特定需求，您可以确定如何定义NAT接口（内部或外部），以及路由表在转换前后包含哪些路由。请记住，数据包的转换部分取决于数据包的传输方向以及您配置NAT的方式。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。