

同时配置静态与动态 NAT

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置 NAT](#)

[相关信息](#)

[相关的思科支持社区讨论](#)

简介

在一些情况下，您可能会发现有必要在Cisco路由器上配置静态和动态网络地址转换 (NAT)命令。本文档介绍如何执行此操作，并提供示例情景。

先决条件

要求

基本的 NAT 概念和操作知识会有所帮助。

- [NAT 如何工作](#)
- [NAT 运行顺序](#)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 3600 系列路由器
- Cisco IOS® 软件版本 12.3(3)

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

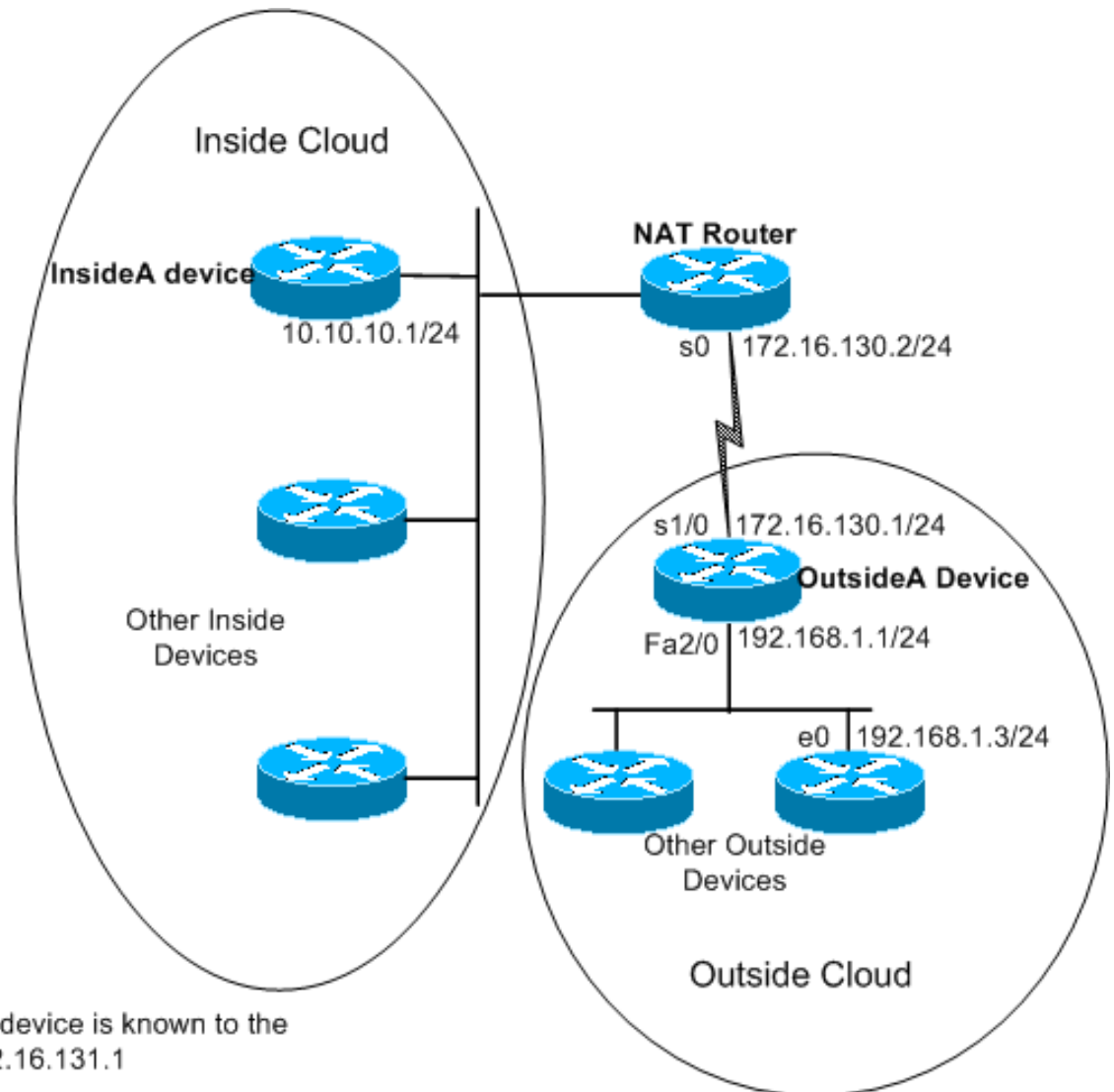
有关文件规则的更多信息请参见“Cisco技术提示规则”。

配置 NAT

具备动态NAT后，除非路由器接收要求转换的数据流，否则NAT表不存在转换。动态转换有一个超时周期，在这个周期之后它们会从转换表中清除。

使用静态NAT时，只要配置静态NAT命令，转换就存在于NAT转换表中，并且这些转换将保留在转换表中，直到删除静态NAT命令。

以下是一个网络图示例：



这些命令在上面所示的 NAT 路由器上配置：

NAT 路由器

```
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
```

OutsideA 设备上的配置为：

```
OutsideA 路由器

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
```

InsideA 设备上的配置为：

```
InsideA 路由器

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
!
!
```

使用 `show ip nat translations` 命令，您可以看到转换表中的内容：

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

请注意，转换表中仅列出了静态转换。此条目将内部全局地址转换到内部本地地址，这意味着外部网云设备可以将信息包发送到全局地址172.16.131.1，并且到达本地地址为10.10.10.1的内部网云设备。

同样如下所示：

```
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]
```

直到路由器在内部接口收到信息包之前，没有其他转换生成或输入转换表。此时内部接口带访问控制表(ACL)允许的源地址。

然而，由于此处没有任何动态转换输入，外部设备不能到达任何内部设备(10.10.10.1除外)，即使它们将数据包发送到全局地址(172.16.131.2至172.16.131.10)时也如此。当路由器接收为这些全局地址之一指定的信息包时，它检查现有转换的转换表。如果没有现有转换，它会尝试路由数据包。[在使用 ip nat outside source list 命令的示例配置和使用 ip nat outside source static 命令的示例配置中进一步讨论NAT的工作情况。](#)

在上述拓扑图里，如果内部和外部网络设备之间的通信之是由内部设备产生，那么动态转换工作正常。但是如果电子邮件服务器被添加到需要接收外部发起的信息包的内部网络时怎么办？现在您必须配置一个静态NAT条目，以便外部的电子邮件服务器能与内部的电子邮件服务器进行通信。如果在上述例子中，电子邮件服务器是带本地地址10.10.10.1的设备，那么您已经拥有一个静态转换。

然而，在您不需要许多全局地址作为备用，或需要为NAT静态配置单个设备时，您可以使用如下配置：

NAT 路由器
<pre>ip nat inside source list 7 interface serial 0 overload ip nat inside source static tcp 10.10.10.1 25</pre>

```

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

```

在上述示例中，NAT 被配置为在 Serial 0 的 IP 地址上过载。这意味着可以将多个内部本地地址动态转换为同一全局地址，在本例中为分配给 Serial 0 的地址。此外，NAT 是静态配置的，因此从本地地址 10.10.10.1（带 TCP 端口 25）的数据包转换为 Serial 0 的 IP 地址 TCP 端口 25。静态 NAT 条目，外部的电子邮件服务器可以发送 SMTP（TCP 端口 25）数据包到全局地址 172.16.131.254。

注意：虽然对动态 NAT 和静态 NAT 可以使用相同的全局地址，但最好尽可能使用不同的全局地址。

NAT 转换表包含以下项：

```
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    ---            ---

```

debug ip nat 输出显示当 outsideA 设备访问 InsideA 时的 NAT 转换：

```

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]
```

总之，动态NAT需要信息包通过NAT路由器转换，以便在转换表中生成NAT转换。如果使用 `ip nat inside` 命令，这些数据包必须源自内部。如果使用 `ip nat outside` 命令，这些数据包必须源自外部。

静态NAT不要求数据包通过路由器被转换，并且静态地转换进入转换表。

[相关信息](#)

- [NAT 常见问题](#)
- [技术支持 - Cisco Systems](#)