

同時配置靜態和動態NAT

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[配置NAT](#)

[相關資訊](#)

[相關思科支援社群討論](#)

簡介

在某些情況下，您可能會發現有必要在Cisco路由器上配置靜態和動態網路地址轉換(NAT)命令。本檔案將說明如何執行此作業，並提供範例情境。

必要條件

需求

瞭解基本NAT概念和操作很有幫助。

- [NAT的工作原理](#)
- [NAT操作順序](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 3600系列路由器
- Cisco IOS[®]軟體版本12.3(3)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

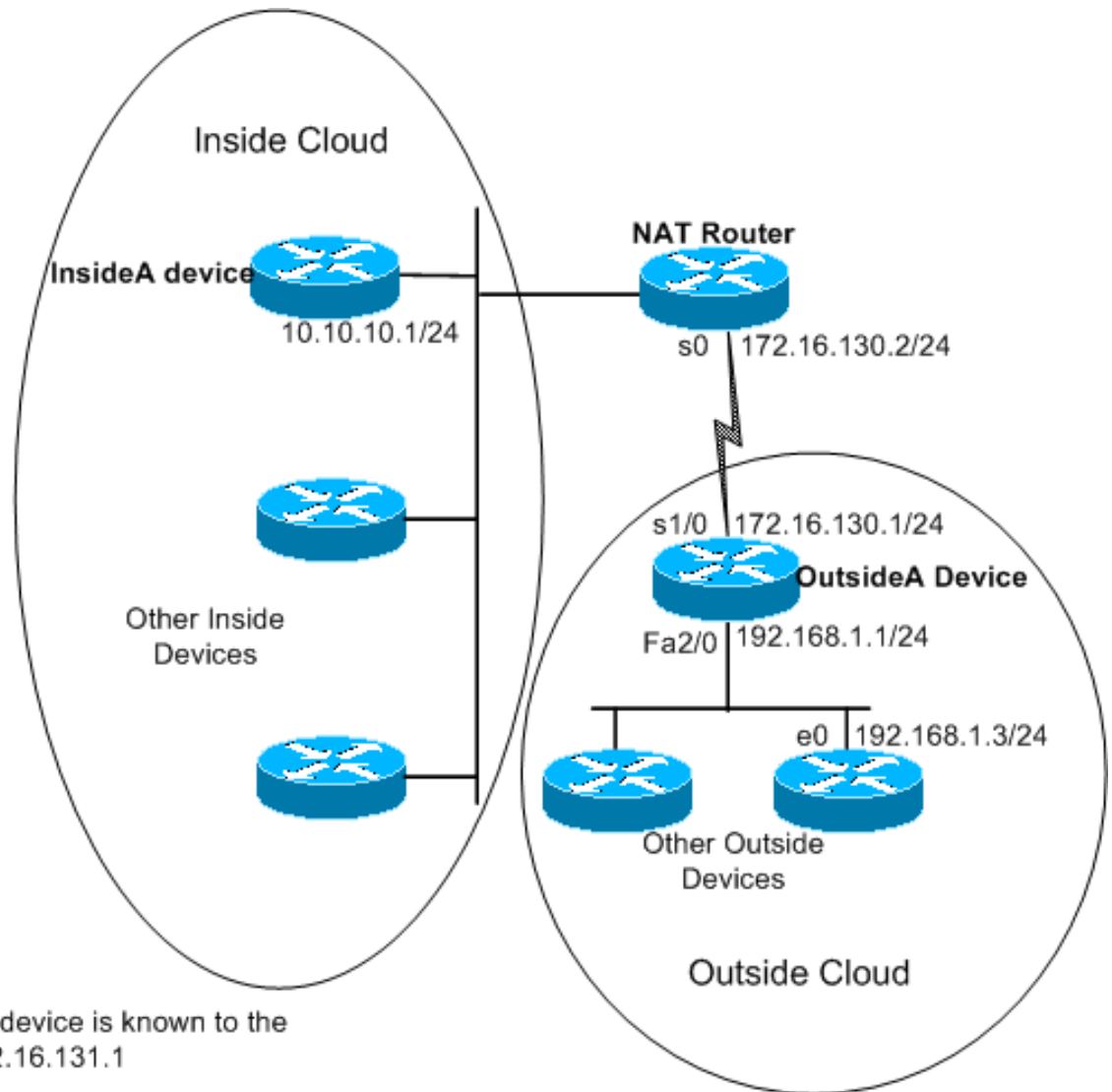
如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

配置NAT

使用動態NAT時，在路由器收到需要轉換的流量之前，NAT表中不會存在轉換。動態轉換具有超時時間，超過此時間後，將從轉換表中清除動態轉換。

使用靜態NAT時，只要配置靜態NAT命令，轉換就會存在於NAT轉換表中，並且它們會保留在轉換表中，直到刪除靜態NAT命令。

以下網路圖是一個示例：



Using NAT, InsideA device is known to the outside cloud as 172.16.131.1

這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裝置上的配置為：

路由器外部

```
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裝置上的配置為：

路由器內部

```
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，您可以看到轉換表的內容：

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

請注意，轉換表中只列出了靜態轉換。此條目將內部全域性地址轉換回內部本地地址，這意味著外部雲上的裝置可以將資料包傳送到全域性地址172.16.131.1並到達本地地址為10.10.10.1的內部雲上的裝置。

同樣情況如下所示：

```
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]
```

除非路由器在其內部介面上收到帶有訪問控制清單(ACL)7允許的源地址的資料包，否則不會生成其他轉換或輸入到轉換表中。

但是，由於尚未輸入任何動態轉換，因此外部裝置無法到達任何內部裝置（10.10.10.1除外），即使它們將資料包傳送到全域性地址（172.16.131.2到172.16.131.10）也無法到達。當路由器收到發往這些全域性地址之一的資料包時，它會檢查轉換表是否有現有的轉換。如果沒有路由，它會嘗試路由資料包。[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](#)中將進一步討論此NAT行為。

在上述拓撲中，如果內部和外部網路裝置之間的通訊僅由內部裝置發起，則動態轉換工作正常。但是，如果在內部網路中新增了電子郵件伺服器，而該伺服器需要接收源自外部的資料包，該怎麼辦？現在，您必須配置靜態NAT條目，以便外部的電子郵件伺服器可以發起與內部電子郵件伺服器的通訊。如果在上述示例中，電子郵件伺服器是本地地址為10.10.10.1的裝置，則您已具有靜態轉換。

但是，如果您沒有多個全域性地址可供使用，並且需要為NAT靜態配置單個裝置，則可以使用如下配置：

NAT路由器

```
ip nat inside source list 7 interface serial 0 overload
```

```

ip nat inside source static tcp 10.10.10.1 25
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

```

在上方示例中，NAT配置為對串列0的IP地址進行過載。這意味著可以將多個內部本地地址動態轉換為同一個全域性地址，在本例中是分配給串列0的地址。此外，NAT是靜態配置的，因此源自TCP埠25(SMTP)的本地地址10.10.10.1的資料包會轉換為串列0的IP地址TCP埠25。由於這是一個靜態NAT條目，因此外部的電子郵件伺服器可以將SMTP (TCP埠25) 資料包傳送到全域性地址172.16.131.254。

注意：儘管可以對動態和靜態NAT使用相同的全域性地址，但儘可能最好使用不同的全域性地址。

NAT轉換表包含以下條目：

```
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輸出顯示了當outsideA裝置訪問InsideA時的NAT轉換：

```

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]

總之，動態NAT要求通過NAT路由器交換資料包，以便在轉換表中生成NAT轉換。如果使用`ip nat inside`命令，則這些資料包必須源自內部。如果使用`ip nat outside`命令，則這些資料包必須源自外部。

靜態NAT不需要通過路由器交換資料包，轉換會靜態輸入到轉換表中。

[相關資訊](#)

- [NAT常見問題](#)
- [技術支援 - Cisco Systems](#)