Cisco - Одновременная настройка статического и динамического NAT

Содержание

Введение

В некоторых ситуациях, возможно, окажется необходимой одновременная настройка команд статического и динамического преобразования сетевых адресов (NAT) в маршрутизаторе Cisco. Этот документ объясняет, как можно это сделать, и дает эталонный сценарий.

Предварительные условия

Требования

Знание основных концепций и процедур NAT может оказаться полезным.

- Работа NAT
- Порядок работы NAT

Дополнительные сведения представлены в разделе Дополнительные сведения данного документа.

Используемые компоненты

Сведения, содержащиеся в данном документе, относятся к следующим версиям программного и аппаратного обеспечения:

- Маршрутизаторы Cisco серии 3600
- ПО Cisco Cisco IOS® версия 12.3 (3)

Сведения, представленные в данном документе, были получены на тестовом оборудовании в специально созданных лабораторных условиях. При написании данного документа использовались только данные, полученные от устройств с конфигурацией по умолчанию.

При работе с реально функционирующей сетью необходимо полностью осознавать возможные последствия выполнения команд до их применения.

Условные обозначения

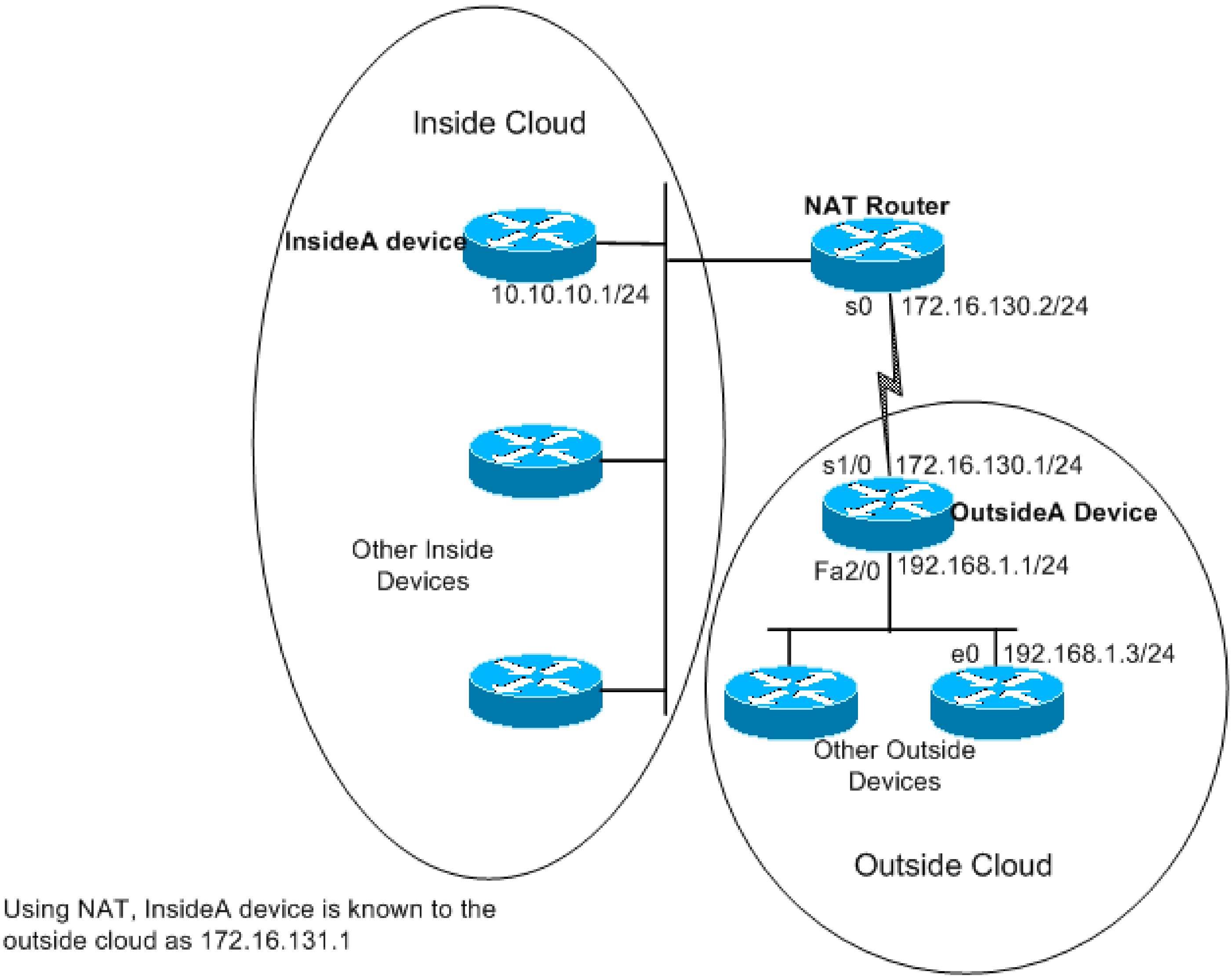
Дополнительные сведения об условных обозначениях см. в разделе Технические советы Cisco. Условные обозначения.

Настройка NAT

При динамическом преобразовании NAT данные в таблице NAT отсутствуют, пока маршрутизатор не получит трафик, требующий преобразования. Динамическим преобразованиям свойственен период ожидания, после которого они удаляются из таблицы преобразований.

При статическом NAT преобразования существуют в таблице NAT при условии, что настроены команды статического NAT, и они остаются в таблице преобразований, пока пользователь не удалит команды статического NAT.

Следующая схема сети служит примером:



Эти команды настроены на маршрутизаторе NAT показанном выше:

Маршрутизатор NAT

```
 12.3

ip nat pool test 172.16.131.2 172.16.131.10 netmask
255.255.255.0

!---     ip nat pool     .
.

ip nat inside source list 7 pool test

!---     ip nat inside source     .


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
```

Конфигурация устройства OutsideA:

Маршрутизатор OutsideA

```
 12.3

ip nat pool test 172.16.131.2 172.16.131.10 netmask
255.255.255.0

!---     ip nat pool     .
.

ip nat inside source list 7 pool test

!---     ip nat inside source     .


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
```

Конфигурация устройства InsideA:

Маршрутизатор InsideA
12.3 ip nat pool test 172.16.131.2 172.16.131.10 netmask 255.255.255.0 !--- **ip nat pool** . . ip nat inside source list 7 pool test !--- **ip nat inside source** .   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

С помощью **команды** show ip nat translations можно увидеть содержимое таблицы трансляции:

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

Обратите внимание, что в таблице представлена только статическая трансляция. Эта запись преобразовывает внутренний глобальный адрес обратно во внутренний локальный адрес; это означает, что устройства внешнего облака могут передавать пакеты по глобальному адресу 172.16.131.1 и связываться с устройством во внутреннем облаке с локальным адресом 10.10.10.1.

См. пример ниже:

```
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]
```

В таблицу трансляции больше не вносятся и не создаются другие преобразования, пока маршрутизатор не получит пакет на внутренний интерфейс с адресом источника, разрешенным списком управления доступом (ACL) 7.

Однако поскольку пока не введено ни одного динамического преобразования, внешние устройства не могут связаться с внутренними (за исключением 10.10.10.1), даже если отправляют пакеты на глобальные адреса (от 172.16.131.2 до 172.16.131.10). Когда маршрутизатор получает пакет, предназначенный одному из этих глобальных адресов, он проверяет таблицу преобразования адресов на наличие существующего преобразования. Если его нет, он пытается маршрутизировать пакет. Это поведение NAT описано далее в разделах "Пример настройки с помощью команды **ip nat outside source list**" и "Пример настройки с помощью команды **ip nat outside source static**".

В топологии, представленной выше, динамическое преобразование функционирует нормально, если связь между устройствами внутренней и внешней сети образована только внутренними устройствами. Но что, если почтовый сервер добавлен к внутренней сети, которая должна получить пакеты, созданные снаружи? Теперь следует настроить статическое правило NAT, чтобы внешние почтовые серверы могли устанавливать соединение с внутренним почтовым сервером. Если в приведенном выше примере почтовый сервер является устройством с локальным адресом 10.10.10.1, то уже имеется статическое преобразование.

Однако в тех случаях, когда в резерве нет большого количества глобальных адресов и нужно статически настроить одно устройство для NAT, можно использовать конфигурацию, подобную приведенной ниже:

Маршрутизатор NAT

```
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
!---     ip nat inside source     .


 interface e 0

 ip address 10.10.10.254 255.255.255.0

 ip nat inside
```

```
!---      ip nat inside|outside !---   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
```

В примере выше преобразование NAT настроено для перегрузки IP-адреса на последовательном порте 0. Это означает, что можно динамически преобразовать несколько внутренних локальных адресов на те же глобальные адреса; в данном случае - это адрес, назначенный Serial 0. Кроме того, преобразование NAT настроено статически и пакеты, исходящие из локального адреса 10.10.10.1 с портом TCP 25 (SMTP) транслируются в IP-адрес TCP порта 25 Serial 0. Поскольку это запись статического NAT, почтовые серверы извне могут создавать пакеты SMTP (TCP порт 25) для глобального адреса 172.16.131.254.

Примечание. Хотя можно использовать один и тот же глобальный адрес как для динамического, так и статического NAT, лучше все же использовать разные глобальные адреса.

В таблице преобразования NAT присутствует следующая запись:

```
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      ---          ---
```

Выходные данные **debug ip nat** иллюстрируют преобразование NAT при доступе устройства outsideA к InsideA:

```
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]
```

Таким образом, при динамическом преобразовании сетевых адресов (NAT) необходима коммутация пакетов через маршрутизатор NAT, чтобы генерировать преобразования NAT в таблице преобразований. Если используется команда **ip nat inside** , эти пакеты должны создаваться внутри. Если используется команда **ip nat outside**, эти пакеты должны создаваться снаружи.

Статическое преобразование NAT не требует коммутации пакетов через маршрутизатор, а все преобразования вводятся в таблицу преобразования статически.

Дополнительные сведения

- Настройка трансляции сетевых адресов: Начало работы
- Работа NAT
- Часто задаваемые вопросы NAT
- Как изменить динамическую конфигурацию NAT
- Страница технической поддержки NAT
- Техническая поддержка - Cisco Systems