

고정 및 동적 NAT를 동시에 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[NAT 구성](#)

[관련 정보](#)

[관련 Cisco 지원 커뮤니티 토론](#)

소개

경우에 따라 Cisco 라우터에서 정적 및 동적 NAT(Network Address Translation) 명령을 모두 구성해야 할 수도 있습니다. 이 문서에서는 이 작업을 수행하는 방법에 대해 설명하고 샘플 시나리오를 제공합니다.

사전 요구 사항

요구 사항

기본 NAT 개념 및 운영에 대한 지식이 도움이 됩니다.

- [NAT 작동 방식](#)
- [NAT 작업 순서](#)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 3600 Series 라우터
- Cisco IOS[®] Software 릴리스 12.3(3)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

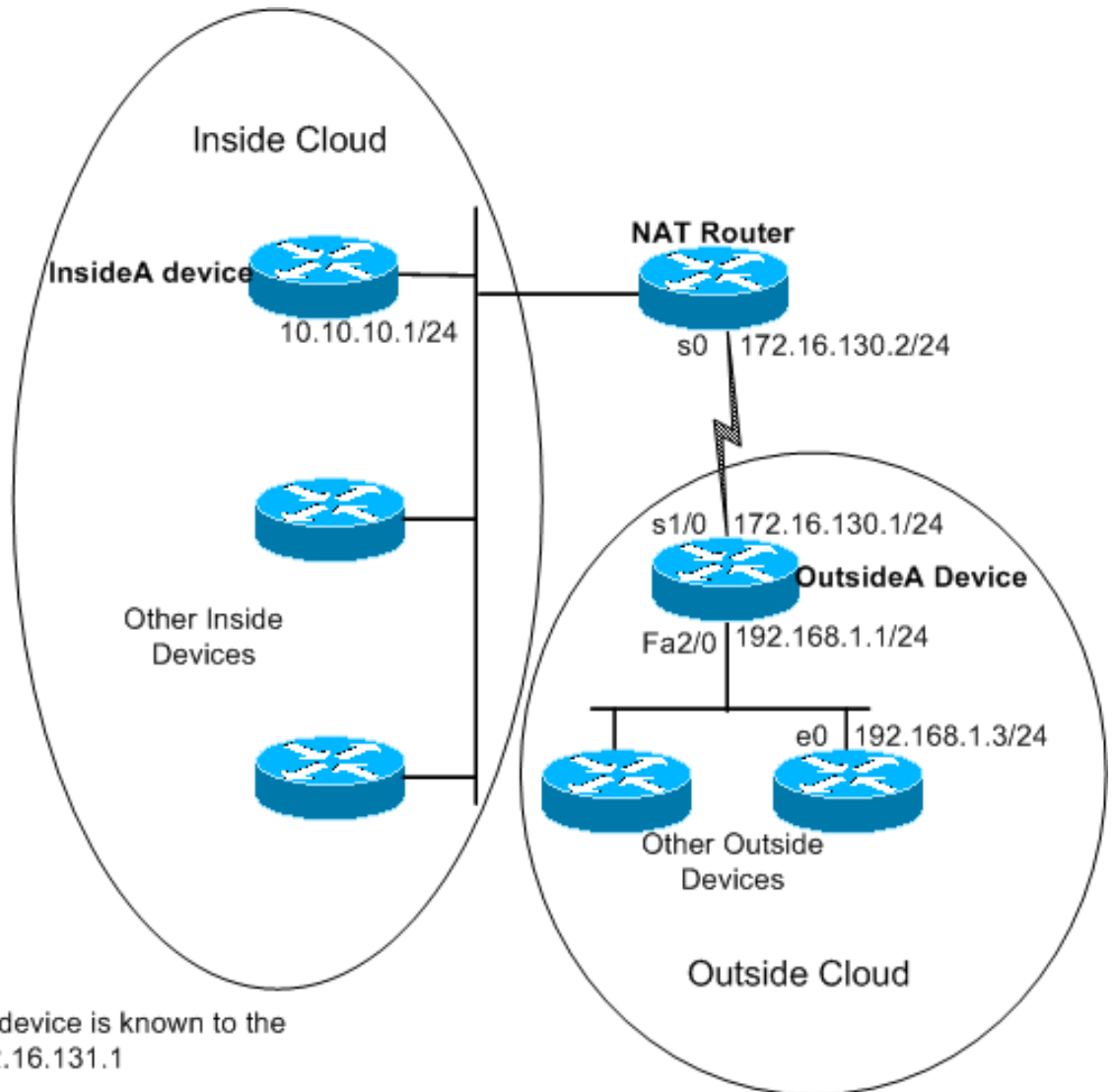
NAT 구성

동적 NAT를 사용하면 라우터가 변환이 필요한 트래픽을 수신할 때까지 변환이 NAT 테이블에 존재

하지 않습니다. 동적 변환의 시간 초과 기간이 지나면 변환 테이블에서 제거됩니다.

고정 NAT를 사용하면 static NAT 명령을 구성하자마자 NAT 변환 테이블에 변환이 존재하며, 고정 NAT 명령을 삭제할 때까지 변환 테이블에 그대로 유지됩니다.

다음 네트워크 다이어그램이 그 예입니다.



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

이러한 명령은 위에 표시된 NAT 라우터에서 구성됩니다.

```
NAT 라우터

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 디바이스의 컨피그레이션은 다음과 같습니다.

OutsideA 라우터

```
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 디바이스의 컨피그레이션은 다음과 같습니다.

InsideA 라우터

```
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
!  
!
```

show ip nat translations 명령을 사용하면 변환 테이블의 내용을 확인할 수 있습니다.

```
NATrouter#show ip nat translations
```

```
Pro Inside global    Inside local    Outside local    Outside global  
--- 172.16.131.1      10.10.10.1      ---            ---
```

변환 테이블에는 고정 변환만 나열됩니다. 이 항목은 내부 전역 주소를 내부 로컬 주소로 다시 변환합니다. 즉, 외부 클라우드의 디바이스는 패킷을 전역 주소 172.16.131.1으로 보내고 내부 클라우드의 디바이스에 연결할 수 있으며, 이는 로컬 주소가 10.10.10.1입니다.

아래와 같은 내용이 표시됩니다.

```
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]
```

라우터가 내부 인터페이스에서 ACL(Access Control List) 7에서 허용하는 소스 주소로 패킷을 수신할 때까지 다른 번역이 생성되거나 변환 테이블에 입력되지 않습니다.

그러나 아직 동적 변환이 입력되지 않았으므로 외부 디바이스는 전역 주소 (172.16.131.2~172.16.131.10)으로 패킷을 전송하더라도 내부 디바이스(10.10.10.1 제외)에 도달할 수 없습니다. 라우터는 이러한 전역 주소 중 하나로 향하는 패킷을 수신하면 변환 테이블에서 기존 변환을 확인합니다. 없는 경우 패킷을 라우팅하려고 시도합니다. 이 NAT 동작에 대해서는 샘플 컨피그레이션 [샘플 nat outside source list 명령](#) 및 샘플 컨피그레이션 [에서 ip nat outside source static 명령을 사용하여](#) 자세히 [설명합니다](#).

위 토폴로지에서 내부 및 외부 네트워크 디바이스 간의 통신이 내부 디바이스에서만 시작된 경우 동적 변환이 정상적으로 작동합니다. 그러나 외부에서 시작된 패킷을 수신해야 하는 내부 네트워크에 이메일 서버를 추가하는 경우 어떻게 해야 합니까? 이제 외부 이메일 서버가 내부의 이메일 서버와 통신을 시작할 수 있도록 고정 NAT 항목을 구성해야 합니다. 위의 예에서 로컬 주소가 10.10.10.1인 디바이스가 이메일 서버인 경우 이미 고정 변환이 있습니다.

그러나 예비 글로벌 주소가 많지 않고 NAT에 대해 단일 디바이스를 정적으로 구성해야 하는 경우 아래 컨피그레이션과 같은 컨피그레이션을 사용할 수 있습니다.

NAT 라우터

```
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
```

위의 예에서 NAT는 Serial 0의 IP 주소에 오버로드하도록 구성됩니다. 즉, 둘 이상의 내부 로컬 주소가 동일한 전역 주소로 동적으로 변환될 수 있습니다. 이 경우 Serial 0에 할당된 주소입니다. 또한 TCP 포트 25(SMTP)를 사용하여 로컬 주소 10.10.10.1에서 제공된 패킷이 Serial 0의 IP 주소 TCP 포트 25로 변환되도록 NAT가 정적으로 구성됩니다. 이 항목이 고정 NAT 항목이므로 외부의 전자 메일 서버는 전역 주소에 대한 SMTP(TCP 포트 25) 패킷을 172.16.131.254.

참고: 동적 NAT와 고정 NAT에 동일한 전역 주소를 사용할 수 있지만 가능하면 다른 전역 주소를 사용하는 것이 좋습니다.

NAT 변환 테이블에는 다음 항목이 있습니다.

```
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 출력은 outsideA 디바이스가 InsideA에 액세스할 때 NAT 변환을 표시합니다.

```
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]
```

요약하자면, 동적 NAT는 변환 테이블에서 NAT 변환을 생성하려면 NAT 라우터를 통해 패킷을 전환해야 합니다. **ip nat inside** 명령을 사용하는 경우 이러한 패킷은 내부에서 시작해야 합니다. **ip nat outside** 명령을 사용하는 경우 이러한 패킷은 외부에서 시작되어야 합니다.

고정 NAT는 라우터를 통해 패킷을 스위칭할 필요가 없으며 변환 테이블에 정적으로 입력됩니다.

[관련 정보](#)

- [NAT FAQ](#)
- [Technical Support - Cisco Systems](#)