네트워크 주소 변환 설정

목차

소개

이 문서에서는 Cisco 라우터에서 NAT(네트워크 주소 변환)를 설정하는 방법을 설명합니다.

사전 요구 사항

요구 사항

이 문서에는 NAT와 관련하여 사용되는 용어에 대한 기본 지식이 필요합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 2500 Series 라우터
- Cisco IOS® Software 릴리스 12.2(10b)

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

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

NAT 구성 및 구축을 위한 빠른 시작 단계

참고: 이 문서에서는 인터넷 또는 인터넷 장치를 언급할 때 외부 네트워크에 있는 장치를 의미합니다.

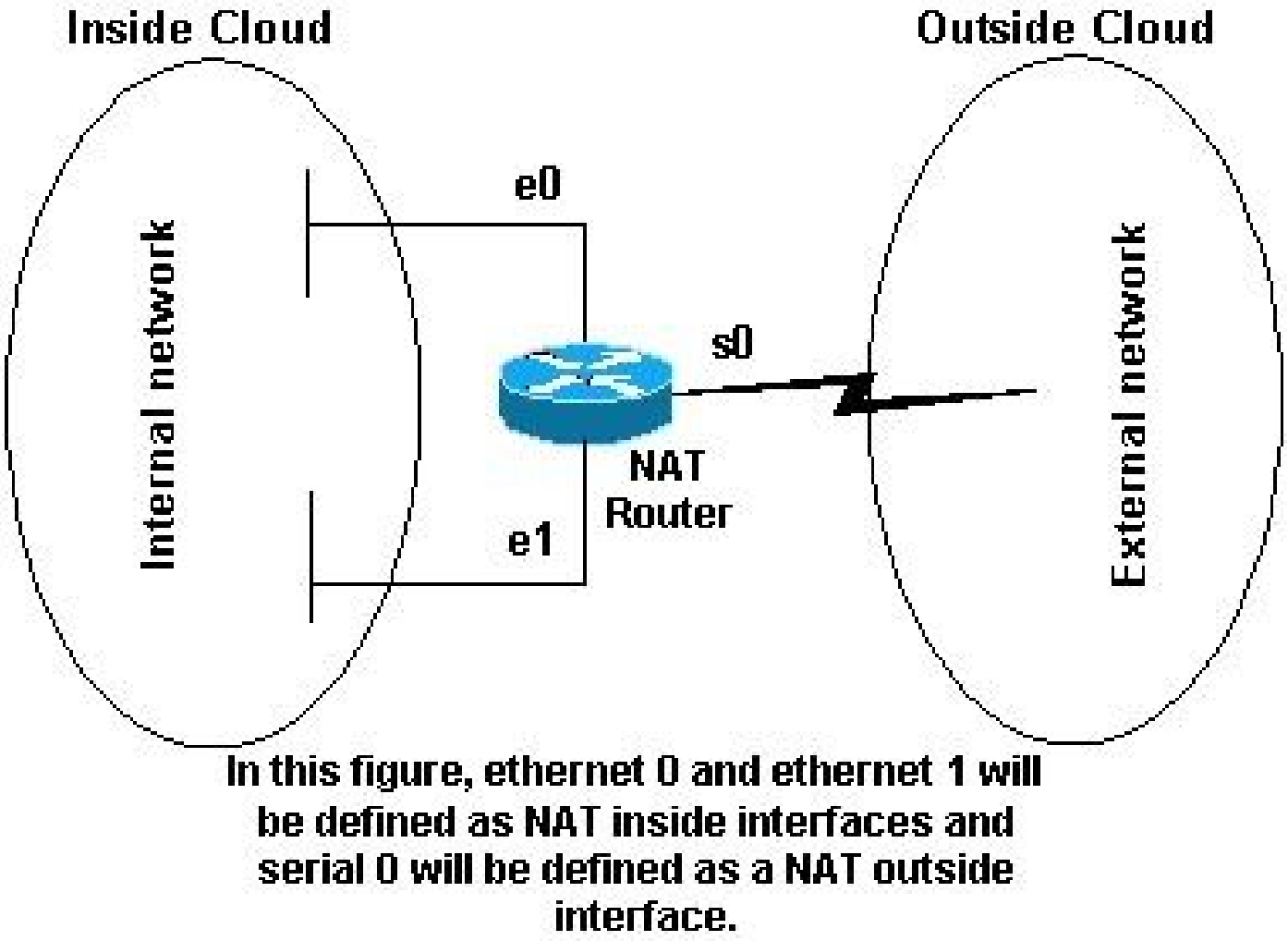
NAT를 구성할 때, 특히 NAT를 처음 사용하는 경우에는 어디서부터 시작해야 할지 아는 것이 어려울 수 있습니다. 다음 단계에서는 NAT가 수행할 작업 및 이를 구성하는 방법을 정의합니다.

1. 내부 및 외부 인터페이스 NAT를 정의합니다.
    - 사용자가 여러 인터페이스에 존재합니까?
    - 인터넷에 사용할 수 있는 인터페이스가 여러 개입니까?
2. NAT로 수행할 작업을 정의합니다.
    - 내부 사용자의 인터넷 액세스를 허용하시겠습니까?
    - 인터넷이 메일 서버 또는 웹 서버와 같은 내부 장치에 액세스하도록 허용하시겠습니까?
    - TCP 트래픽을 다른 TCP 포트 또는 주소로 리디렉션하시겠습니까?
    - 네트워크 전환 중에 NAT를 사용하시겠습니까(예: 서버 IP 주소를 변경하고 모든 클라이언트를 업데이트할 수 있을 때까지 업데이트되지 않은 클라이언트가 원래 IP 주소로 서버에 액세스하고 업데이트된 클라이언트가 새 주소로 서버에 액세스할 수 있도록 허용하시겠습니까)?
    - 겹치는 네트워크가 통신할 수 있도록 사용하시겠습니까?
3. 이전에 정의한 사항을 달성하기 위해 NAT를 구성합니다. 2단계에서 정의한 내용에 따라 다음 기능 중 사용할 기능을 결정해야 합니다.
    - 고정 NAT
    - 동적 NAT
    - Overloading
    - 이러한 기능의 조합.
4. NAT 작업을 확인합니다.

이러한 각 NAT 예는 이전 이미지의 빠른 시작 단계 1~3단계를 안내합니다. 다음 예에서는 Cisco에서 NAT 구축을 권장하는 몇 가지 일반적인 시나리오를 설명합니다.

NAT 내부 및 외부 인터페이스 정의

NAT를 구축하는 첫 번째 단계는 인터페이스 내부 및 외부 NAT를 정의하는 것입니다. 내부 네트워크를 내부로, 외부 네트워크를 외부로 정의하는 것이 가장 쉽습니다. 다만, 내부 및 외부적 약관도 중재의 대상이 된다. 이 그림은 이에 대한 예를 보여 줍니다.



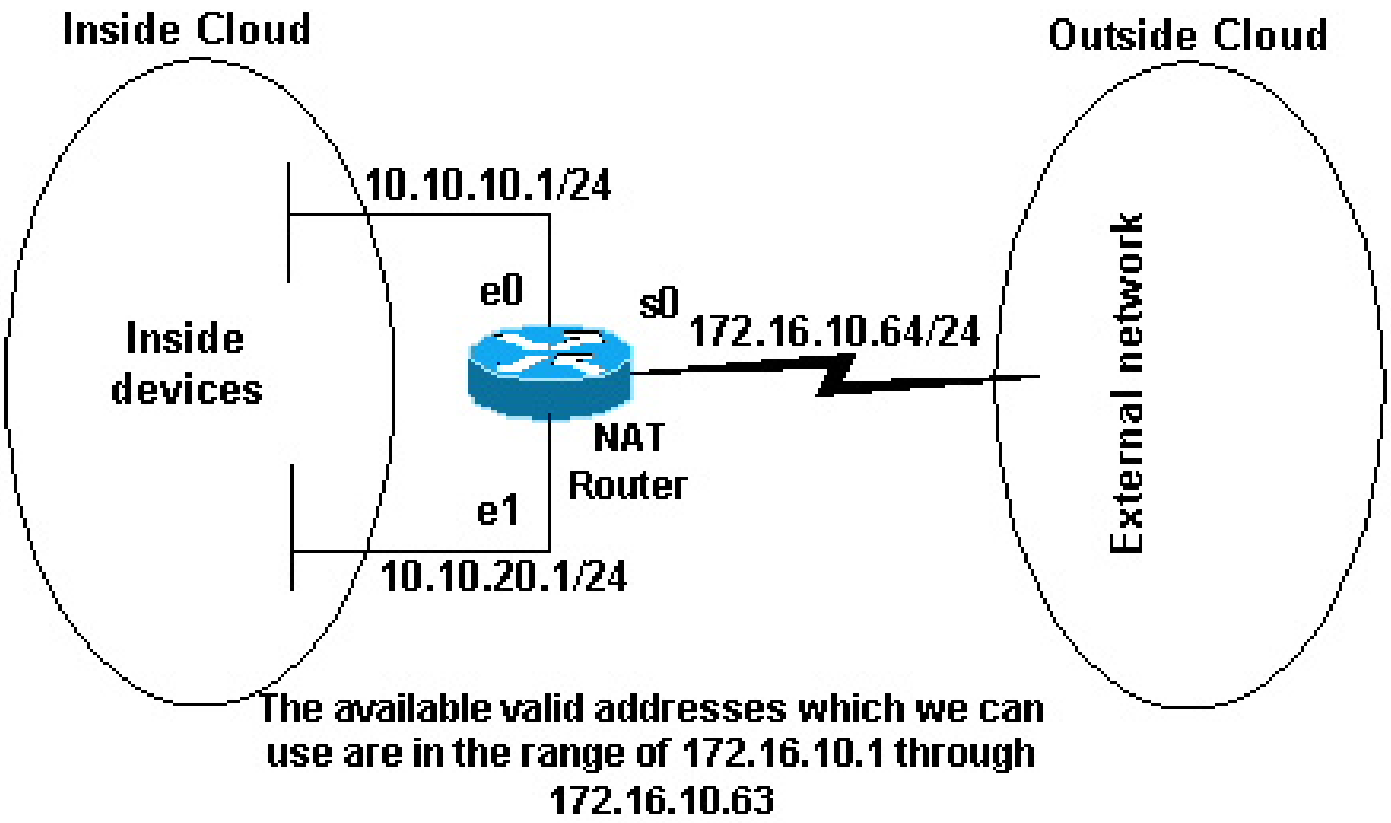
NAT 토폴로지

예

1. 내부 사용자의 인터넷 액세스 허용

내부 사용자의 인터넷 액세스를 허용할 수 있지만 모든 사용자를 수용할 수 있는 유효한 주소가 충분하지 않은 경우. 인터넷의 모든 장치와 통신이 내부 장치에서 발생하는 경우 유효한 단일 주소 또는 유효한 주소 풀이 필요합니다.

이 그림에서는 라우터 인터페이스가 내부 및 외부로 정의된 간단한 네트워크 다이어그램을 보여줍니다.



사용 가능한 유효한 주소

이 예에서는 NAT가 내부의 특정 디바이스(각 서브넷의 처음 31개)가 외부의 디바이스와의 통신을 시작하고 잘못된 주소를 유효한 주소 또는 주소 풀로 변환하도록 허용할 수 있습니다. 풀은 172.16.10.1에서 172.16.10.63까지의 주소 범위로 정의되었습니다.

이제 NAT를 구성할 수 있습니다. 이전 이미지에 정의된 사항을 달성하려면 동적 NAT를 사용합니다. 동적 NAT의 경우, 라우터의 변환 테이블은 처음에 비어 있으며 변환해야 하는 트래픽이 라우터를 통과하면 채워집니다. 고정 NAT와 달리, 변환은 정적으로 구성되며 트래픽이 필요 없이 변환 테이블에 배치됩니다.

이 예에서는 각 내부 디바이스를 고유한 유효 주소로 변환하거나 각 내부 디바이스를 동일한 유효 주소로 변환하도록 NAT를 구성할 수 있습니다. 이 두 번째 방법은 overloading 입니다. 각 방법을 구성하는 방법의 예는 여기에 나와 있습니다.

내부 사용자가 인터넷에 액세스할 수 있도록 NAT 구성

NAT 라우터
interface ethernet 0 ip address 10.10.10.1 255.255.255.0 ip nat inside

```
!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.


interface ethernet 1
 ip address 10.10.20.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.


ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24


!--- Defines a NAT pool named no-overload with a range of addresses
!--- 172.16.10.1 - 172.16.10.63.


ip nat inside source list 7 pool no-overload


!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has
!--- the source address translated to an address out of the
!--- NAT pool "no-overload".


access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

참고: Cisco에서는 permit any로 NAT 명령에서 참조하는 액세스 목록을 구성하지 않는 것을 권장합니다. NAT에서 permit any를 사용하면 너무 많은 라우터 리소스가 소모되어 네트워크 문제가 발생할 수 있습니다.

이전 컨피그레이션에서는 액세스 목록 7에서 서브넷 10.10.10.0의 첫 32개 주소와 서브넷 10.10.20.0의 첫 32개 주소만 허용됩니다. 따라서 이러한 소스 주소만 변환됩니다. 내부 네트워크에 다른 주소가 있는 다른 디바이스가 있을 수 있지만 이러한 디바이스는 변환되지 않습니다.

마지막 단계는 NAT가 의도한 대로 작동하는지 확인하는 것입니다.

내부 사용자가 오버로드로 인터넷에 액세스할 수 있도록 NAT 구성

NAT 라우터

```
interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.


interface ethernet 1
 ip address 10.10.20.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.


ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24


!--- Defines a NAT pool named ovrld with a range of a single IP
!--- address, 172.16.10.1.


ip nat inside source list 7 pool ovrld overload


!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has the source address
!--- translated to an address out of the NAT pool named ovrld.
!--- Translations are overloaded, which allows multiple inside
!--- devices to be translated to the same valid IP address.

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

이전의 두 번째 컨피그레이션에서는 NAT 풀의 ovrld 주소 범위가 1개뿐입니다. ip nat inside source list 7 pool overload 명령에서 사용되는 키워드 오버로드를 사용하면 NAT에서 여러 내부 디바이스를 풀의 단일 주소로 변환할 수 있습니다.

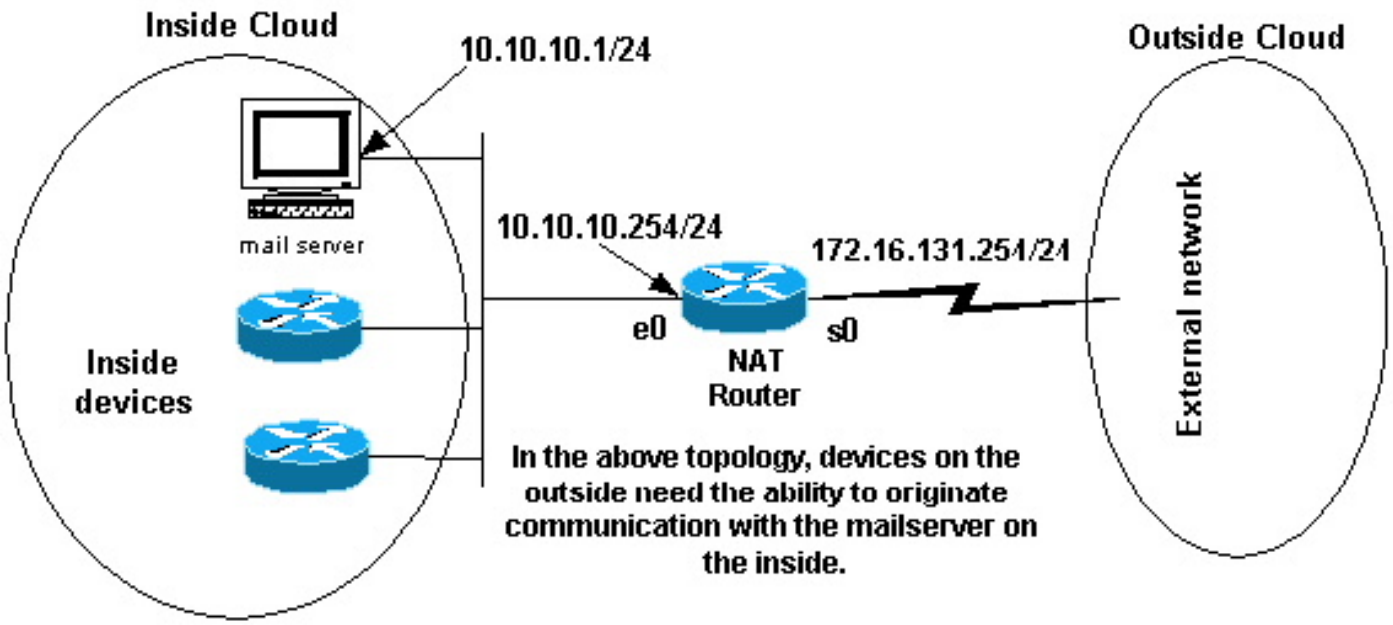
이 명령의 또 다른 변형인 isip nat inside source list 7 interface serial 0 overload는 serial 0 인터페이스에 할당된 주소에 오버로드하도록 NAT를 구성합니다.

구성된 경우 라우터overloading는 전역 주소를 올바른 로컬 주소로 다시 변환하기에 충분한 정보를 상위 레벨 프로토콜(예: TCP 또는 UDP 포트 번호)에서 유지 관리합니다. 전역 및 로컬 주소의 정의는 NAT: 전역 및 로컬 정의를 참조하십시오.

마지막 단계는 NAT가 의도한 대로 작동하는지 확인하는 것입니다.

2. 인터넷이 내부 장치에 액세스하도록 허용

내부 디바이스가 있어야 인터넷 디바이스(예: 이메일)에서 통신이 시작되는 인터넷 상의 디바이스와 정보를 교환할 수 있습니다. 일반적으로 인터넷의 디바이스는 내부 네트워크에 상주하는 메일 서버로 이메일을 전송합니다.



커뮤니케이션 시작

인터넷이 내부 장치에 액세스할 수 있도록 NAT 구성

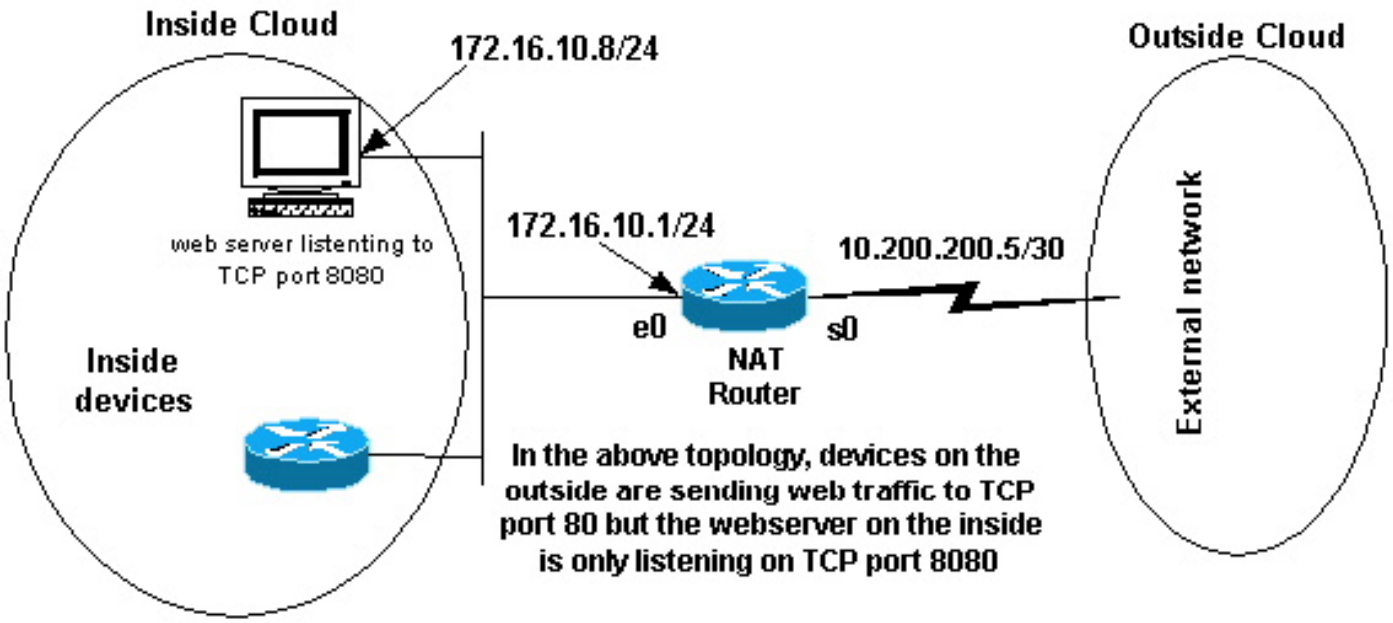
이 예에서는 먼저 이전 네트워크 다이어그램에 표시된 대로 내부 및 외부 인터페이스의 NAT를 정의합니다.

둘째, 내부의 사용자가 외부와의 통신을 시작할 수 있도록 정의합니다. 외부에 있는 장치는 내부에 있는 메일 서버와만 통신을 시작할 수 있어야 합니다.

세 번째 단계는 NAT를 구성하는 것입니다. 정의한 사항을 달성하기 위해 고정 및 동적 NAT를 함께 구성할 수 있습니다. 이 예제를 구성하는 방법에 대한 자세한 내용은 고정 및 동적 NAT 동시 구성을 참조하십시오. 마지막 단계는 NAT가 의도한 대로 작동하는지 확인하는 것입니다.

3. TCP 트래픽을 다른 TCP 포트 또는 주소로 리디렉션

내부 네트워크의 웹 서버는 인터넷의 장치가 내부 장치와 통신을 시작하는 데 필요할 수 있는 경우에 대한 또 다른 예입니다. 경우에 따라 내부 웹 서버가 포트 80이 아닌 TCP 포트에서 웹 트래픽을 수신하도록 구성할 수 있습니다. 예를 들어, 내부 웹 서버는 TCP 포트 8080을 수신하도록 구성할 수 있습니다. 이 경우 NAT를 사용하여 TCP 포트 80으로 향하는 트래픽을 TCP 포트 8080으로 리디렉션할 수 있습니다.



웹 트래픽 TCP 포트

이전 네트워크 다이어그램에 표시된 대로 인터페이스를 정의한 후 NAT가 172.16.10.8:80을 목적지로 하는 외부 패킷을 172.16.10.8:8080으로 리디렉션하도록 결정할 수 있습니다. 이를 위해 TCP 포트 번호를 변환하려면 static nat 명령을 사용할 수 있습니다. 샘플 컨피그레이션이 여기에 표시됩니다.

TCP 트래픽을 다른 TCP 포트 또는 주소로 리디렉션하도록 NAT 구성

NAT 라우터
interface ethernet 0 ip address 172.16.10.1 255.255.255.0 ip nat inside *!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.* interface serial 0 ip address 10.200.200.5 255.255.255.252 ip nat outside *!--- Defines serial 0 with an IP address and as a NAT outside interface.* ip nat inside source static tcp 172.16.10.8 8080 172.16.10.8 80 *!--- Static NAT command that states any packet received in the inside* *!--- interface with a source IP address of 172.16.10.8:8080 is* *!--- translated to 172.16.10.8:80.*

참고: static NAT 명령에 대한 컨피그레이션 설명은 소스 주소가 172.16.10.8:8080인 내부 인

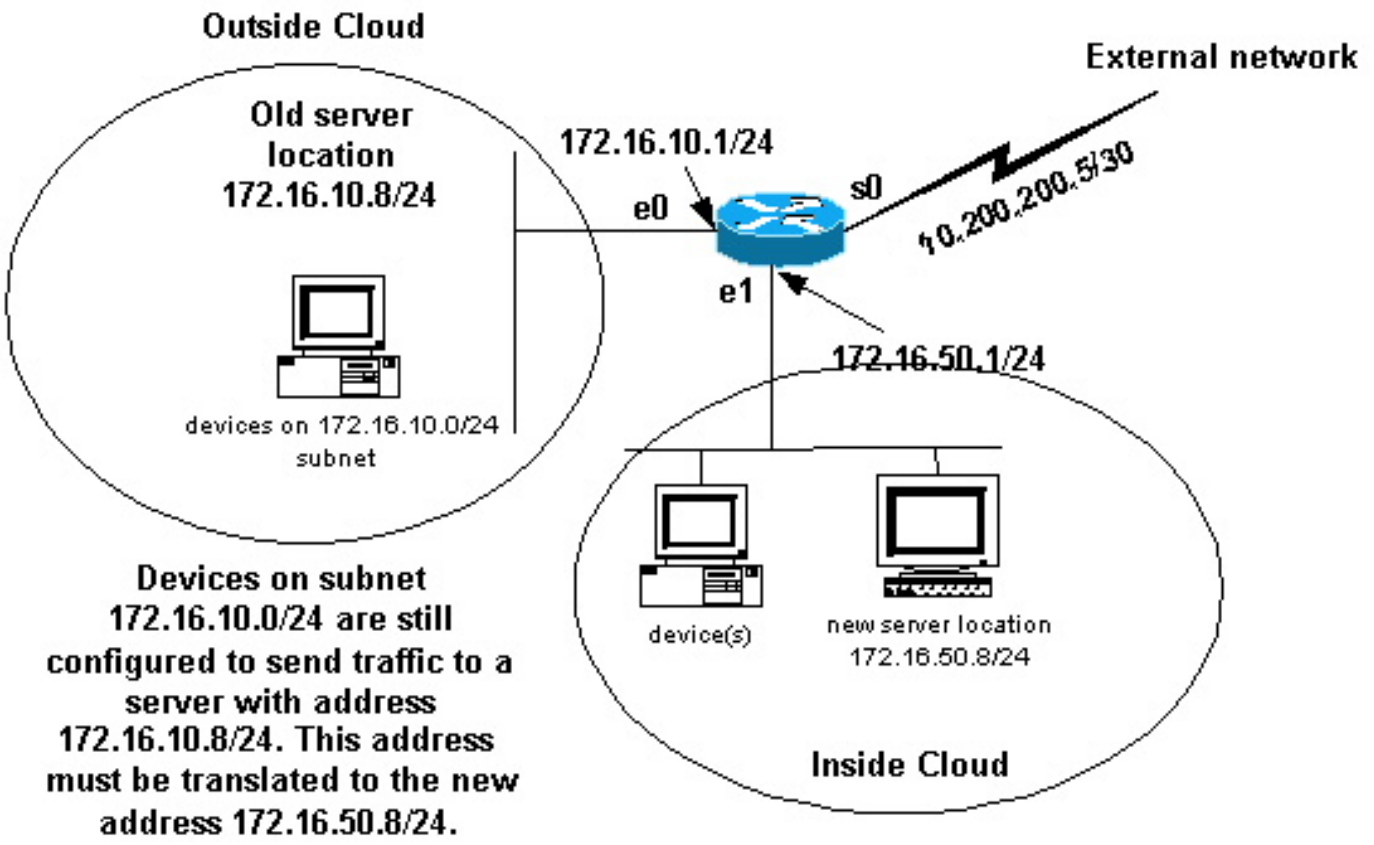
터페이스에서 수신된 패킷이 172.16.10.8:80으로 변환됨을 나타냅니다. 이는 또한 대상 주소가 172.16.10.8:80인 외부 인터페이스에서 수신된 모든 패킷에 대상이 172.16.10.8:8080으로 변환되었음을 의미합니다.

마지막 단계는 NAT가 의도한 대로 작동하는지 확인하는 것입니다.

```
show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.10.8:80     172.16.10.8:8080   ---                ---
```

4. 네트워크 전환에 NAT 사용

NAT는 네트워크에서 디바이스를 다시 준비해야 할 때 또는 디바이스를 다른 디바이스로 교체할 때 유용합니다. 예를 들어, 네트워크의 모든 디바이스가 특정 서버를 사용하고 이 서버를 새 IP 주소가 있는 새 디바이스로 교체해야 하는 경우, 새 서버 주소를 사용하도록 모든 네트워크 디바이스를 재구성하는 데 시간이 걸립니다. 그 동안 NAT를 사용하여 이전 주소로 디바이스를 구성하여 새 서버와 통신하도록 패킷을 변환할 수 있습니다.



NAT 네트워크 전환

이전 이미지에서 설명한 대로 NAT 인터페이스를 정의했으면, NAT에서 이전 서버 주소(172.16.10.8)로 보낼 외부 패킷을 새 서버 주소로 변환 및 전송하도록 허용할 것인지를 결정할 수 있습니다. 새 서버가 다른 LAN에 있고, 이 LAN의 장치 또는 이 LAN을 통해 연결할 수 있는 모든 장

치(네트워크 내부의 장치)는 가능한 경우 새 서버 IP 주소를 사용하도록 구성해야 합니다.

고정 NAT를 사용하여 필요한 작업을 수행할 수 있습니다. 샘플 컨피그레이션입니다.

네트워크 전환을 통해 사용할 NAT 구성

NAT 라우터

```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat outside

!--- Defines Ethernet 0 with an IP address and as a NAT outside interface.


interface ethernet 1
 ip address 172.16.50.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 10.200.200.5 255.255.255.252

!--- Defines serial 0 with an IP address. This interface is not
!--- participating in NAT.


ip nat inside source static 172.16.50.8 172.16.10.8

!--- States that any packet received on the inside interface with a
!--- source IP address of 172.16.50.8 is translated to 172.16.10.8.
```

참고: 이 예에서 inside source NAT 명령은 또한 목적지 주소가 172.16.10.8인 외부 인터페이스에서 수신된 패킷에 목적지 주소가 172.16.50.8로 변환되었음을 의미합니다.

마지막 단계는 NAT가 의도한 대로 작동하는지 확인하는 것입니다.

5. 겹치는 네트워크에 NAT 사용

겹치는 네트워크는 인터넷 내의 다른 디바이스에서 이미 사용 중인 내부 디바이스에 IP 주소를 할당하면 발생합니다. 이러한 네트워크는 두 회사 모두 네트워크에서 RFC 1918 IP 주소를 사용하는 회사가 병합될 때도 발생합니다. 이 두 네트워크는 통신해야 하며, 바람직하게는 모든 디바이스를 재배치하지 않고 통신해야 합니다.

일대일 매핑과 다대다 매핑의 차이

고정 NAT 컨피그레이션은 일대일 매핑을 생성하고 특정 주소를 다른 주소로 변환합니다. 이 컨피

그레이션 유형은 컨피그레이션이 있는 한 NAT 테이블에 영구 엔트리를 생성하고 내부 및 외부 호스트 모두 연결을 시작할 수 있도록 합니다. 이는 메일, 웹, FTP 등의 애플리케이션 서비스를 제공하는 호스트에 주로 유용합니다. 예를 들면 다음과 같습니다.

```
<#root>

Router(config)#

ip nat inside source static 10.3.2.11 10.41.10.12

Router(config)#

ip nat inside source static 10.3.2.12 10.41.10.13
```

동적 NAT는 변환할 실제 호스트 수보다 사용 가능한 주소가 적을 때 유용합니다. 호스트가 연결을 시작하고 주소 간에 일대일 매핑을 설정하면 NAT 테이블에 항목이 생성됩니다. 그러나 매핑은 다를 수 있으며, 통신 시 풀에서 사용 가능한 등록된 주소에 따라 다릅니다. 동적 NAT는 구성된 내부 또는 외부 네트워크에서만 세션을 시작할 수 있도록 허용합니다. 동적 NAT 항목은 호스트가 구성 가능한 특정 기간 동안 통신하지 않는 경우 변환 테이블에서 제거됩니다. 그런 다음 다른 호스트에서 사용할 수 있도록 주소가 풀로 반환됩니다.

예를 들어, 세부 구성의 다음 단계를 완료합니다.

1. 주소 풀을 생성합니다.

```
<#root>

Router(config)#

ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

2. 매핑해야 하는 내부 네트워크에 대한 액세스 목록을 만듭니다.

```
<#root>

Router(config)#

access-list 100 permit ip 10.3.2.0 0.0.0.255 any
```

3. 풀 MYPOOLEXAMPLE에 들어갈 내부 네트워크 10.3.2.0 0.0.0.255를 선택한 다음 주소를 오버로드하는 액세스 목록 100을 연결합니다.

```
<#root>

Router(config)#

ip nat inside source list 100 pool MYPOOLEXAMPLE overload
```

NAT 작업 확인

NAT를 구성한 후에는 NAT가 예상대로 작동하는지 확인합니다. 네트워크 분석기, show 명령 또는 debug 명령을 사용하여 여러 가지 방법으로 이 작업을 수행할 수 있습니다. NAT 확인의 자세한 예는 Verify NAT Operation and Basic NAT를 참조하십시오.

결론

이 문서의 예는 NAT를 구성하고 구축하는 데 도움이 될 수 있는 빠른 시작 단계를 보여줍니다.

이러한 빠른 시작 단계는 다음과 같습니다.

1. 인터페이스 내부 및 외부 NAT를 정의합니다.
2. NAT를 통해 달성하고자 하는 것은 무엇입니까?
3. 2단계에서 정의한 사항을 달성하기 위해 NAT를 구성합니다.
4. NAT 작업을 확인합니다.

앞의 각 예에서는 다양한 형태의 ip nat insidecode가 사용되었습니다. 또한 동일한 목표를 달성하기 위해 ip nat outsidecommand를 사용할 수 있지만 NAT 작업 순서를 염두에 두어야 합니다. ip nat outsidecommands를 사용하는 컨피그레이션 예는 IP NAT Outside Source List Command를 사용하는 샘플 컨피그레이션을 참조하십시오.

앞의 예에서는 다음 작업도 수행했습니다.

명령을 사용합니다	작업
ip nat 내부 소스	• 내부에서 외부로 이동하는 IP 패킷의 소스를 변환합니다. • 외부로 이동하는 IP 패킷의 목적지를 변환합니다.
ip nat 외부 소스	• 외부로 이동하는 IP 패킷의 소스를 변환합니다. • 내부에서 외부로 이동하는 IP 패킷의 목적지를 변환합니다.

관련 정보

- NAT: 로컬 및 글로벌 정의.
- NAT 지원 페이지
- IP 라우팅 프로토콜 지원 페이지
- IP 라우팅 지원 페이지
- IP 주소 지정 서비스
- NAT 작동 순서

- Cisco IOS NAT에 대한 FAQ(자주 묻는 질문)
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.