Firepower Threat Defense용 NAT(네트워크 주소 변환)

다음 주제에서는 NAT(네트워크 주소 변환)에 대한 내용 및 Firepower Threat Defense 디바이스에 NAT를 구성하는 방법을 설명합니다.

NAT를 사용해야 하는 이유

IP 네트워크 내의 각 컴퓨터와 디바이스에는 호스트를 식별하는 고유한 IP 주소가 할당됩니다. 공용 IPv4 주소의 부족 때문에 이러한 IP 주소는 대부분 사설이며, 사설 회사 네트워크 외부로 라우팅되지 않습니다. RFC 1918의 정의에 따르면 사설 IP 주소는 내부적으로 사용할 수 있지만 외부에 알려서는 안 되는 주소입니다.

- 10.0.0.0~10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0~192.168.255.255

NAT의 주요 기능 중 하나는 사설 IP 네트워크가 인터넷에 연결되도록 하는 것입니다. NAT는 사설 IP 주소를 공용 IP 주소로 교체하여, 내부 사설 네트워크의 사설 주소를 공용 인터넷에서 사용할 수 있는 합법적이고 라우팅 가능한 주소로 전환합니다. 이렇게 하여 NAT는 공용 주소를 절약합니다. 전체 네트워크에 대해 최소 하나의 공용 주소만 외부에 알리도록 구성할 수 있기 때문입니다.

NAT의 기타 기능은 다음과 같습니다.

- 보안 - 직접 공격을 피할 수 있도록 내부 IP 주소를 숨깁니다.
- IP 라우팅 솔루션 - NAT를 사용하는 경우 중첩 IP 주소 문제가 발생하지 않습니다.
- 유연성 - 외부적으로 사용 가능한 공용 주소에 영향을 주지 않고 내부 IP 주소 지정 방식을 변경할 수 있습니다. 예를 들어 인터넷에 액세스할 수 있는 서버의 경우, 인터넷용으로는 고정 IP 주소를 유지하고 내부적으로는 서버 주소를 변경할 수 있습니다.
- IPv4와 IPv6 간 변환(라우팅된 방식 전용) - IPv6 네트워크를 IPv4 네트워크에 연결하려는 경우 NAT를 이용하면 두 가지 주소 유형 간에 변환할 수 있습니다.

참고 NAT는 필수 항목이 아닙니다. 특정 트래픽에 대해 NAT를 구성하지 않으면 해당 트래픽은 변환되지 않지만, 모든 보안 정책은 정상적으로 적용됩니다.

NAT 기본 사항

다음 주제에서는 NAT의 기본 사항 일부를 설명합니다.

NAT 용어

이 설명서는 다음과 같은 용어를 사용합니다.

- 실제 주소/호스트/네트워크/인터페이스 - 실제 주소는 변환되기 전 호스트에서 정의된 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 내부 네트워크가 "실제" 네트워크일 수 있습니다. 내부 네트워크뿐 아니라 디바이스에 연결된 모든 네트워크를 변환할 수 있습니다. 따라서 외부 주소를 변환하도록 NAT를 구성하는 경우 "실제"는 내부 네트워크에 액세스하는 외부 네트워크를 지칭할 수 있습니다.
- 매핑된 주소/호스트/네트워크/인터페이스 - 매핑된 주소는 실제 주소가 변환되는 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 외부 네트워크가 "매핑된" 네트워크일 수 있습니다.

  참고 주소 변환 중에 디바이스 인터페이스용으로 구성된 IP 주소는 변환되지 않습니다.

- 양방향 시작 - 고정 NAT에서는 연결이 양방향으로 시작될 수 있습니다(호스트에서 나가기도 하고 호스트로 들어오기도 함).
- 소스 및 대상 NAT - 모든 패킷에 대해 소스 및 대상 IP 주소를 NAT 규칙과 비교하며, 하나 또는 둘 모두를 변환하거나 변환하지 않을 수 있습니다. 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "source(소스)"와 "destination(대상)"이 사용됩니다. 특정 연결이 "destination(대상)" 주소에서 시작되는 경우에도 마찬가지입니다.

NAT 유형

다음 방법을 사용하여 NAT를 구현할 수 있습니다.

- 동적 NAT - 실제 IP 주소의 그룹이 매핑된 IP 주소의 그룹(대개 더 작음)에 선착순으로 매핑됩니다. 실제 호스트만 트래픽을 시작할 수 있습니다. 동적 NAT, 21 페이지의 내용을 참조하십시오.
- 동적 PAT(동적 포트 주소 변환) - 실제 IP 주소의 그룹이 해당 IP 주소의 고유한 소스 포트를 사용하여 단일 IP 주소로 매핑됩니다. 동적 PAT, 27 페이지의 내용을 참조하십시오.
- 고정 NAT - 실제 IP 주소와 매핑된 IP 주소 간의 일관된 매핑입니다. 양방향 트래픽 시작이 허용됩니다. 고정 NAT, 38 페이지의 내용을 참조하십시오.
- ID NAT - 실제 주소가 기본적으로 NAT를 우회하여 자신에게 고정으로 변환됩니다. 대규모 주소 그룹을 변환하되 좀 더 작은 규모의 주소 하위 집합을 제외하고자 할 경우 이 방법으로 NAT를 구성할 수 있습니다. ID NAT, 47 페이지의 내용을 참조하십시오.

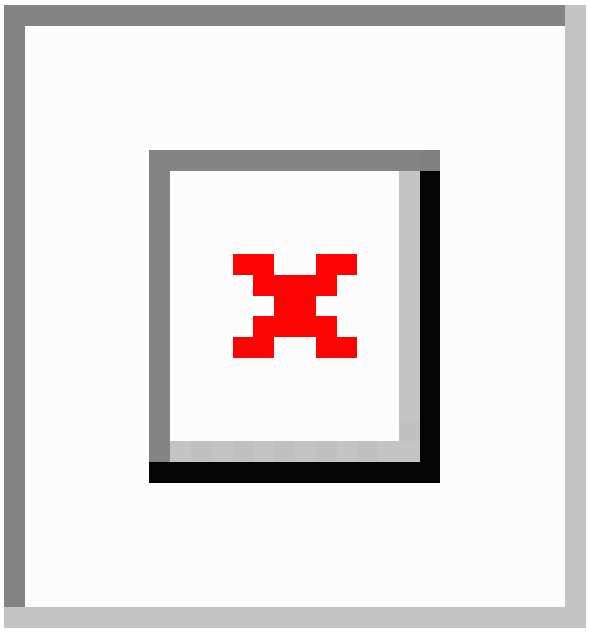
라우팅된 모드 및 투명 모드의 NAT

라우팅된 방화벽 모드와 투명 방화벽 모드에서 모두 NAT를 구성할 수 있습니다. 인라인, 인라인 탭 또는 수동 모드로 작동하는 인터페이스에 대해서는 NAT를 구성할 수 없습니다. 다음 섹션에서는 각 방화벽 모드의 일반적인 사용법에 대해 설명합니다.

라우팅 모드의 NAT

다음 그림은 내부에 사설 네트워크가 있는 라우팅된 모드의 일반적인 NAT 예를 보여줍니다.

그림 *1: NAT* 예: 라우팅된 모드



1. 10.1.2.27의 내부 호스트가 웹 서버로 패킷을 전송하면, 패킷의 실제 소스 주소 10.1.2.27이 매핑된 주소 209.165.201.10으로 변환됩니다.
2. 서버가 응답하면 해당 호스트는 응답을 매핑된 주소 209.165.201.10으로 전송하며 Firepower Threat Defense 디바이스에서 패킷을 수신합니다. 이는 Firepower Threat Defense 디바이스에서 프록시 ARP를 수행하여 패킷을 신청하기 때문입니다.
3. 그런 다음 Firepower Threat Defense 디바이스에서는 호스트로 전송하기 전에, 매핑된 주소 209.165.201.10에서 다시 실제 주소 10.1.2.27로의 변환을 변경합니다.

투명 모드 또는 브리지 그룹 내 NAT

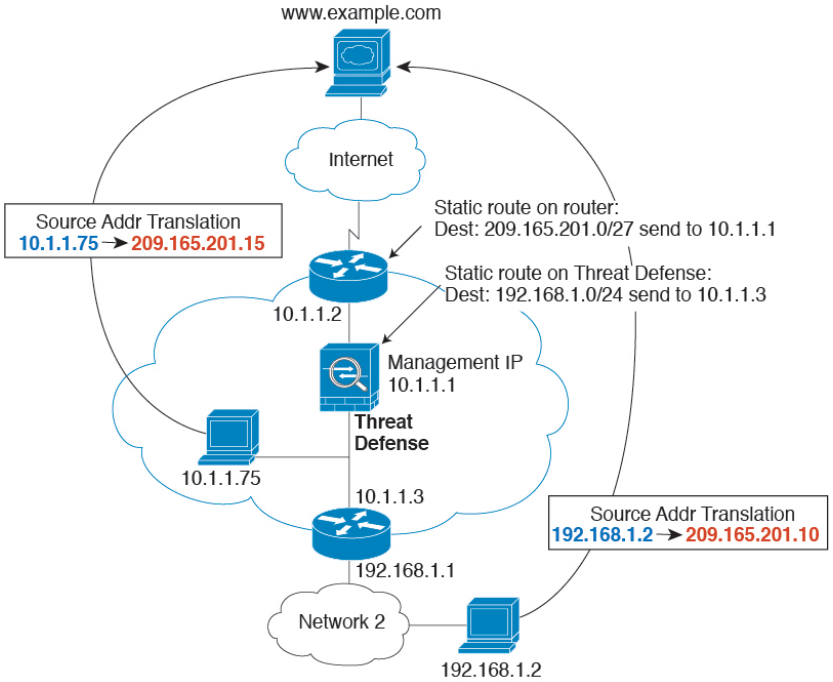
투명 모드에서 NAT를 사용하면 업스트림 또는 다운스트림 라우터가 네트워크에 대해 NAT를 수행할 필요가 없습니다. 라우팅 모드에서 브리지 그룹 내에 유사한 기능을 수행할 수 있습니다.

투명 모드의 NAT 또는 동일한 브리지 그룹의 멤버 간 라우팅 모드에서의 NAT에는 다음과 같은 요구사항과 제한 사항이 있습니다.

- 매핑된 주소가 브리지 그룹 멤버 인터페이스일 때는 인터페이스 PAT를 구성할 수 없습니다. 인터페이스에 연결된 IP 주소가 없기 때문입니다.
- ARP 검사는 지원되지 않습니다. 또한 Firepower Threat Defense 디바이스의 한 쪽에 있는 호스트가 어떤 이유로든 Firepower Threat Defense 디바이스의 다른 쪽에 있는 호스트로 ARP 요청을 전송하고, 시작한 호스트의 실제 주소가 동일한 서브넷의 다른 주소로 매핑되면, ARP 요청에 실제 주소가 가시적으로 남게 됩니다.
- IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 두 IPv6 네트워크 간 변환 또는 두 IPv4 네트워크 간 변환은 지원됩니다.

다음 그림은 내부 인터페이스와 외부 인터페이스의 네트워크가 동일한 투명 모드의 일반적인 NAT 시나리오를 보여줍니다. 이 시나리오의 투명 방화벽은 NAT 서비스를 수행하므로 업스트림 라우터가 NAT를 수행할 필요가 없습니다.

그림 *2: NAT* 예: 투명 모드



1. 10.1.1.75의 내부 호스트가 웹 서버로 패킷을 전송하면, 패킷의 실제 소스 주소 10.1.1.75가 매핑된 주소 209.165.201.15로 변경됩니다.
2. 서버가 응답하며 매핑된 주소 209.165.201.15로 응답을 전송하면, Firepower Threat Defense 디바이스에서 패킷을 수신합니다. 업스트림 라우터는 Firepower Threat Defense 디바이스 관리 IP 주소로 연결되는 고정 경로에 이 매핑된 주소를 포함하기 때문입니다.
3. 그런 다음 Firepower Threat Defense 디바이스에서는 매핑된 주소 209.165.201.15에서 다시 실제 주소 10.1.1.1.75로의 변환을 취소합니다. 실제 주소는 직접 연결되어 있으므로 Firepower Threat Defense 디바이스는 호스트로 주소를 직접 전송합니다.
4. 호스트 192.168.1.2에서도 반환 트래픽을 제외하고는 동일한 프로세스가 발생합니다. Firepower Threat Defense 디바이스는 라우팅 테이블에서 경로를 조회하고, 192.168.1.0/24에 대한 Firepower Threat Defense 디바이스 고정 경로를 기반으로 10.1.1.3의 다운스트림 라우터로 패킷을 전송합니다.

자동 NAT 및 수동 NAT

자동 *NAT* 및 수동 *NAT* 두 가지 방법으로 주소 변환을 구현할 수 있습니다.

수동 NAT에서 제공하는 추가 기능이 필요한 경우가 아니면 자동 NAT를 사용하는 것이 좋습니다. 자동 NAT가 컨피그레이션이 더 쉽고, VoIP(Voice over IP) 등의 애플리케이션에서 좀 더 안정적일 수 있습니다. VoIP의 경우 규칙에서 사용되는 개체 중 하나에 속하지 않는 간접 주소를 변환할 때 오류가 발생할 수 있습니다.

자동 NAT

네트워크 개체의 파라미터로 컨피그레이션되는 모든 NAT 규칙은 자동 *NAT* 규칙으로 간주됩니다. NAT 규칙을 사용하면 네트워크 개체에 대해 NAT를 빠르고 쉽게 구성할 수 있습니다. 그러나 그룹 개체에 대해서는 이러한 규칙을 생성할 수 없습니다.

이러한 규칙은 개체 자체의 일부분으로 구성되지만, 개체 관리자를 통해 개체 정의에서 NAT 컨피그레이션을 확인할 수는 없습니다.

패킷이 인터페이스로 들어가면 소스 및 대상 IP 주소 둘 다에서 자동 NAT 규칙을 확인합니다. 별도의 일치를 만든 경우 별도의 규칙을 통해 패킷의 소스 및 대상 주소를 변환할 수 있습니다. 이러한 규칙은 서로 연결되어 있지 않습니다. 트래픽에 따라 규칙의 서로 다른 조합을 사용할 수 있습니다.

규칙은 쌍을 이루지 않으므로 소스A/대상A가 소스A/대상B 이외의 다른 변환을 갖도록 지정할 수 없습니다. 이러한 종류의 기능이 필요한 경우 수동 NAT를 사용하십시오. 그러면 한 가지 규칙에서 소스 및 대상 주소를 식별할 수 있습니다.

수동 NAT

수동 NAT 한 가지 규칙에서 소스 및 대상 주소를 모두 식별할 수 있습니다. 소스 주소와 대상 주소를 모두 지정하면 소스A/대상A가 소스A/대상B 이외의 다른 변환을 갖도록 지정할 수 있습니다.

참고 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "source(소스)"와 "destination(대상)"이 사용됩니다. 특정 연결이 "destination(대상)" 주소에서 시작되는 경우에도 마찬가지입니다. 예를 들어 포트 주소 변환 고정 NAT를 구성하고, 소스 주소를 텔넷 서버로 지정하며, 텔넷 서버로 이동하는 모든 트래픽에 대해 포트를 2323에서 23으로 변환하려면 소스 포트가 변환되도록 지정해야 합니다(실제 포트: 23, 매핑된 포트: 2323). 텔넷 서버 주소를 소스 주소로 지정했기 때문에 소스 포트를 지정하는 것입니다.

대상 주소는 선택 사항입니다. 대상 주소를 지정하는 경우 이를 대상 주소 자신에게 매핑할 수도 있고(ID NAT) 다른 주소에 매핑할 수도 있습니다. 대상 주소 매핑은 항상 고정 매핑입니다.

자동 NAT와 수동 NAT 비교

이 두 NAT 유형의 주요 차이점은 다음과 같습니다.

- 실제 주소를 정의하는 방법
  - 자동 NAT - NAT 규칙은 네트워크 개체의 파라미터가 됩니다. 네트워크 개체 IP 주소는 원래(실제) 주소 역할을 합니다.
  - 수동 NAT- 실제 주소와 매핑된 주소 모두에서 네트워크 개체 또는 네트워크 개체 그룹을 식별합니다. 이 경우 NAT는 네트워크 개체의 매개변수가 아닙니다. 네트워크 개체 또는 그룹은 NAT 컨피그레이션의 매개변수입니다. 실제 주소에 네트워크 개체 그룹을 사용할 수 있으므로 수동 NAT의 확장성이 더 뛰어납니다.
- 소스 및 대상 NAT의 구현 방법

- 자동 NAT- 각 규칙을 패킷의 소스 또는 대상에 적용할 수 있습니다. 따라서 소스 IP 주소와 대상 IP 주소에 각각 하나씩 두 개의 규칙이 사용될 수 있습니다. 소스/대상조합에 특정 변환을 적용하기 위해 이러한 두 규칙을 결합할 수 없습니다.
- 수동 NAT단일 규칙에서 소스와 대상을 모두 변환합니다. 패킷은 하나의 규칙에서만 일치하며, 더 이상 규칙이 점검되지 않습니다. 선택적 대상 주소를 컨피그레이션하지 않더라도 일치하는 패킷은 여전히 하나의 수동 NAT 규칙과만 일치합니다. 소스와 대상이 결합되어 있으므로, 소스/대상조합에 따라 서로 다른 변환을 적용할 수 있습니다. 예를 들어 소스A/대상A의 변환은 소스A/대상B의 변환과 다를 수 있습니다.

• NAT 규칙의 순서
  - 자동 NAT- NAT 테이블에서 자동으로 순서가 지정됩니다.
  - 수동 NAT - NAT 테이블에서 수동으로 순서가 지정됩니다(자동 NAT 규칙 앞이나 뒤).

NAT 규칙 순서

자동 NAT 및 수동 NAT 규칙은 세 개의 섹션으로 구분되는 단일 테이블에 저장됩니다. 섹션 1 규칙이 먼저 적용된 다음, 일치가 발견될 때까지 섹션 2, 마지막으로 섹션 3이 적용됩니다. 예를 들어 섹션 1에서 일치가 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

표 ***1: NAT*** 규칙 테이블

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 1	수동 NAT	첫 번째 일치부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 첫 번째 일치가 적용되므로, 일반 규칙 앞에 특수 규칙이 오도록 해야 합니다. 그렇지 않으면 특수 규칙이 원하는 대로 적용되지 않을 수 있습니다. 기본적으로 수동 NAT 규칙은 섹션 1에 추가됩니다. "특정 규칙 우선"이라는 의미는 다음과 같습니다. • 정적 규칙이 동적 규칙 앞에 와야 합니다. • 대상 변환을 포함한 규칙은 소스 변환만을 포함한 규칙보다 앞에 와야 합니다. 소스 또는 대상 주소를 기반으로 둘 이상의 규칙이 적용될 수 있는 중복 규칙을 제거할 수 없는 경우에는 특히 주의하여 이러한 권장 사항을 따르십시오.

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 2	자동 NAT	섹션 1에서 일치하는 항목을 찾을 수 없으면 섹션 2 규칙이 다음 순서로 적용됩니다. **1.** 고정 규칙 **2.** 동적 규칙 각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다. **1.** 실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 개체가 주소가 10개인 개체보다 먼저 평가됩니다. **2.** 수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다. **3.** IP 주소가 동일한 경우 네트워크 개체의 이름이 알파벳순으로 사용됩니다. 예를 들면 abracadabra가 catwoman보다 먼저 평가됩니다.
섹션 3	수동 NAT	아직도 일치가 발견되지 않으면 섹션 3 규칙이 첫 번째부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 이 섹션에는 가장 일반적인 규칙을 포함해야 합니다. 또한 이 섹션에서는 특정 규칙이 일반 규칙보다 먼저 적용되도록 해야 합니다.

예를 들어 섹션 2 규칙의 경우 네트워크 개체 내에서 다음 IP 주소를 정의합니다.

- 192.168.1.0/24(고정)
- 192.168.1.0/24(동적)
- 10.1.1.0/24(고정)
- 192.168.1.1/32(고정)
- 172.16.1.0/24(동적)(개체 def)
- 172.16.1.0/24(동적)(개체 abc)

결과 순서는 다음과 같습니다.

- 192.168.1.1/32(고정)
- 10.1.1.0/24(고정)
- 192.168.1.0/24(고정)
- 172.16.1.0/24(동적)(개체 abc)
- 172.16.1.0/24(동적)(개체 def)

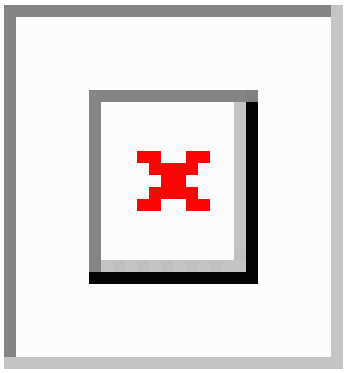
- 192.168.1.0/24(동적)

NAT 인터페이스

브리지 그룹 멤버 인터페이스를 제외한 임의의 인터페이스(즉, 모든 인터페이스)에 적용할 NAT 규칙을 구성할 수도 있고, 특정 실제 및 매핑된 인터페이스를 지정할 수도 있습니다. 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 특정 인터페이스를 지정하거나, 그 반대로 지정할 수도 있습니다.

예를 들어, 여러 인터페이스에서 동일한 사설 주소를 사용하며, 외부에 액세스할 때 이들을 모두 동일한 전역 풀로 변환하려는 경우 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 외부 인터페이스를 지정할 수 있습니다.

그림 *3:* 임의의 인터페이스 지정



그러나 브리지 그룹 멤버 인터페이스에는 "any" 인터페이스라는 개념이 적용되지 않습니다. "any" 인터페이스를 지정하면 모든 브리지 그룹 멤버 인터페이스는 제외됩니다. 따라서 브리지 그룹 멤버에 NAT를 적용하려면 멤버 인터페이스를 지정해야 합니다. 이렇게 하면 유사한 여러 규칙에서 인터페이스 하나만 다른 현상이 발생할 수 있습니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT를 구성할 수 없으며 멤버 인터페이스에 대해서만 NAT를 구성할 수 있습니다.

참고 인라인, 인라인 탭 또는 수동 모드로 작동하는 인터페이스에 대해서는 NAT를 구성할 수 없습니다. 인터페이스를 지정할 때는 인터페이스가 포함된 인터페이스 개체를 선택하여 간접적으로 지정합니다.

NAT 라우팅 구성

FTD 디바이스는 변환(매핑)된 주소로 전송되는 모든 패킷의 대상이어야 합니다.

패킷을 전송할 때 디바이스는 대상 인터페이스를 지정한 경우 해당 인터페이스를 사용하고, 그렇지 않으면 라우팅 테이블 조회를 사용하여 이그레스 인터페이스를 결정합니다. ID NAT의 경우에는 대상 인터페이스를 지정하더라도 경로 조회를 사용하는 옵션이 있습니다.

필요한 라우팅 컨피그레이션의 유형은 다음 항목에서 설명하는 것처럼 매핑된 주소의 유형에 따라 다릅니다.

매핑된 인터페이스와 동일한 네트워크의 주소

대상(매핑된) 인터페이스와 동일한 네트워크의 주소를 사용하는 경우, Firepower Threat Defense 디바이스에서는 매핑된 주소에 대한 ARP 요청에 응답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. Firepower Threat Defense 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 이 솔루션은 외부 네트워크에 적절한 수의 여유 주소가 있는 경우 이상적이며, 동적 NAT 또는 고정 NAT 등 1:1 변환을 사용하는 경우 고려해볼 수 있습니다. 동적 PAT는 소수의 주소로 사용 가능한 변환의 수를 크게 확장합니다. 따라서 외부 네트워크에 사용 가능한 주소가 적어도 이 방법을 사용할 수 있습니다. PAT의 경우 매핑된 인터페이스의 IP 주소를 사용할 수도 있습니다.

참고 매핑된 인터페이스를 임의의(any) 인터페이스로 구성하고 동일한 네트워크의 매핑된 주소를 매핑된 인터페이스 중 하나로 지정하면, 해당 매핑된 주소에 대한 ARP 요청이 다른 인터페이스에서 오는 경우 인그레스 인터페이스에서 해당 네트워크에 대한 ARP 항목을 수동으로 구성하여 해당 MAC 주소를 지정해야 합니다. 일반적으로 매핑된 인터페이스에 대해 임의의 인터페이스를 지정하면 매핑된 주소에 대해 고유한 네트워크를 사용하게 되므로 이러한 상황이 발생하지 않습니다. 인그레스 인터페이스의 **Advanced(**고급**)** 설정에서 ARP 테이블을 컨피그레이션합니다.

고유한 네트워크의 주소

대상(매핑된) 인터페이스 네트워크에서 사용할 수 있는 것보다 더 많은 주소가 필요한 경우 별도의 서브넷에서 주소를 지정할 수 있습니다. 업스트림 라우터에는 Firepower Threat Defense 디바이스를 가리키는, 매핑된 주소에 대한 고정 경로가 필요합니다.

라우팅된 모드에 대한 대안으로, 대상 네트워크의 IP 주소를 게이트웨이로 사용하여 Firepower Threat Defense 디바이스에서 매핑된 주소에 대해 고정 경로를 구성한 다음 라우팅 프로토콜을 사용하여 경로를 재배포할 수 있습니다. 예를 들어 내부 네트워크(10.1.1.0/24)에 대해 NAT를 사용하고 매핑된 IP 주소 209.165.201.5를 사용하는 경우 209.165.201.5 255.255.255.255(호스트 주소)에 대한 고정 경로를 재배포 가능한 10.1.1.99 게이트웨이로 구성할 수 있습니다.

투명 모드에서 실제 호스트가 직접 연결된 경우 8.3에서는 업스트림 라우터의 고정 경로가 Firepower Threat Defense 디바이스를 가리키도록 구성하고 합니다. 투명 모드의 원격 호스트에 대해서는 업스트림 라우터의 고정 경로에서 다운스트림 라우터 IP 주소를 대신 지정할 수 있습니다.

실제 주소와 동일한 주소**(ID NAT)**

ID NAT의 기본 동작은 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것입니다. 원하는 경우 프록시 ARP를 사용 해제할 수 있습니다. 원하는 경우 정기적인 고정 NAT에 대해 프록시 ARP를 사용 해제할 수도 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다.

일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다. 예를 들어 "any" IP 주소에 대해 광범위한 ID NAT 규칙을 구성하고 프록시 ARP를 사용하는 상태로 두면 매핑된 인터페이스에 직접 연결된 네트워크에서 호스트 문제가 발생할 수

있습니다. 이 경우 매핑된 네트워크의 호스트가 동일한 네트워크의 다른 호스트와 통신하려면 ARP 요청의 주소가 NAT 규칙과 일치해야 합니다("any" 주소와 일치). 패킷이 실제로 Firepower Threat Defense 디바이스로 이동하도록 지정되지 않아도 Firepower Threat Defense 디바이스에서는 주소에 대해 프록시 ARP를 수행합니다. (이 문제는 수동 NAT 규칙이 있는 경우에도 발생합니다. NAT 규칙은 소스 주소 및 대상 주소와 모두 일치해야 하지만 프록시 ARP 결정은 "소스" 주소에 대해서만 내려집니다.) 실제 호스트 ARP 응답 전에 Firepower Threat Defense 디바이스 ARP 응답을 수신하는 경우, 트래픽이 Firepower Threat Defense 디바이스로 잘못 전송됩니다.

NAT용 지침

다음 주제에서는 NAT 구현에 대한 자세한 지침을 제공합니다.

NAT용 방화벽 모드 지침

NAT는 라우팅된 모드 및 투명 방화벽 모드에서 지원됩니다.

그러나 브리지 그룹 멤버 인터페이스, 즉 BVI(브리지 그룹 가상 인터페이스)에 속하는 인터페이스에 대해 NAT를 구성할 때는 다음과 같은 제한이 있습니다.

- 브리지 그룹 멤버에 대해 NAT를 구성할 때는 멤버 인터페이스를 지정합니다. BVI(브리지 그룹 인터페이스) 자체에 대해서는 NAT를 구성할 수 없습니다.
- 브리지 그룹 멤버 인터페이스 간에 NAT를 수행할 때는 실제 및 매핑된 주소를 지정해야 합니다. 인터페이스로 "임의"를 지정할 수는 없습니다.
- 매핑된 주소가 브리지 그룹 멤버 인터페이스일 때는 인터페이스 PAT를 구성할 수 없습니다. 인터페이스에 연결된 IP 주소가 없기 때문입니다.
- 소스 및 대상 인터페이스가 동일한 브리지 그룹의 멤버이면 IPv4 및 IPv6 네트워크(NAT64/46) 간을 변환할 수 없습니다. 지원되는 방법은 고정 NAT/PAT 44/66, 동적 NAT44/66 및 동적 PAT44뿐이며 동적 PAT66은 지원되지 않습니다. 그러나 다른 브리지 그룹의 멤버나 브리지 그룹 멤버(소스)와 표준 라우팅 인터페이스(대상) 간에는 NAT64/46을 수행할 수 있습니다.

참고 인라인, 인라인 탭 또는 수동 모드로 작동하는 인터페이스에 대해서는 NAT를 구성할 수 없습니다.

IPv6 NAT 지침

NAT는 다음 지침 및 제약 사항과 함께 IPv6를 지원합니다.

- 표준 라우팅 모드 인터페이스에서는 IPv4와 IPv6 간을 변환할 수도 있습니다.
- 고정 NAT에서는 IPv6 서브넷을 최대 /64까지 지정할 수 있습니다. 더 큰 서브넷은 지원되지 않습니다.

- FTP with NAT46을 사용할 때, IPv4 FTP 클라이언트가 IPv6 FTP 서버에 연결될 때 클라이언트는 확장 패시브 모드(EPSV) 또는 확장 포트 모드(EPRT)를 사용해야 하며, PASV 및 PORT 명령은 IPv6에서 지원되지 않습니다.

IPv6 NAT 모범 사례

IPv6 네트워크 간 변환 및 IPv4와 IPv6 네트워크 간 변환(라우팅된 모드 전용)을 위해 NAT를 사용할 수 있습니다. 다음의 모범 사례를 권장합니다.

- NAT66(IPv6-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다. 반환 트래픽을 허용하지 않으려면 정적 NAT 규칙을 단방향으로 설정할 수 있습니다(수동 NAT에만 해당함).
- NAT46(IPv4-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. IPv6 주소 공간이 IPv4 주소 공간보다 훨씬 크기 때문에 고정 변환을 손쉽게 수용할 수 있습니다. 반환 트래픽을 허용하지 않으려면 정적 NAT 규칙을 단방향으로 설정할 수 있습니다(수동 NAT에만 해당함). IPv6 서브넷(/96 이하)으로 변환하면 결과로 나타나는 매핑된 주소는 기본적으로 IPv4가 포함된 IPv6 주소입니다. 이 경우 IPv6 접두사 뒤에 IPv4 주소의 32비트가 포함됩니다. 예를 들어 IPv6 접두사가 /96 접두사이면, 주소의 마지막 32비트에 IPv4 주소가 첨부됩니다. 예를 들어 192.168.1.0/24를 201b::0/96에 매핑하면 192.168.1.4는 201b::0.192.168.1.4(혼합된 표기로 표시됨)에 매핑됩니다. 접두사가 더 작으면(예: /64) IPv4 주소가 접두사 뒤에 첨부되고, 접미사 0이 IPv4 주소 뒤에 첨부됩니다. 선택적으로 주소를 net-to-net으로 변환할 수도 있습니다. 이 경우 첫 번째 IPv4 주소가 첫 번째 IPv6 주소로, 두 번째가 두 번째로 등과 같이 매핑됩니다.
- NAT64(IPv6-to-IPv4) - IPv6 주소의 수를 수용할 만큼 IPv4 주소가 충분하지 않을 수 있습니다. 대량의 IPv4 변환을 제공하려면 동적 PAT 풀을 사용하는 것이 좋습니다.

검사된 프로토콜에 대한 NAT 지원

보조 연결을 열거나 패킷에 IP 주소를 포함한 일부 애플리케이션 레이어 프로토콜을 검사하여 다음 서비스를 제공합니다.

- 핀홀 생성 - 일부 애플리케이션 프로토콜은 표준 포트 또는 협상된 포트에서 보조 TCP 또는 UDP 연결을 엽니다. 검사에서는 이러한 보조 포트를 허용하기 위한 액세스 제어 규칙을 생성할 필요가 없도록 해당 포트에 대해 핀홀을 엽니다.
- NAT 재작성 - FTP 등의 프로토콜은 프로토콜의 일부분으로 패킷 데이터에 보조 연결용 IP 주소 및 포트를 포함합니다. 엔드포인트 중 하나에서 NAT 변환이 수행되는 경우 검사 엔진은 포함된 주소와 포트의 NAT 변환을 반영하기 위해 패킷 데이터를 재작성합니다. NAT 재작성이 수행되지 않으면 보조 연결은 작동하지 않습니다.
- 프로토콜 적용 - 일부 검사에서는 검사된 프로토콜에 대해 특정 수준의 RFC 적합성을 적용합니다.

다음 표에는 NAT 재작성을 적용하는 검사된 프로토콜 및 이러한 프로토콜의 NAT 제한이 나와 있습니다. 이러한 프로토콜을 포함하는 NAT 규칙을 작성할 때는 이와 같은 제한에 주의해야 합니다. 여

기에 나와 있지 않은 검사된 프로토콜은 NAT 재작성을 적용하지 않습니다. 이러한 검사에는 GTP, HTTP, IMAP, POP, SMTP, SSH 및 SSL이 포함됩니다.

참고 NAT 재작성은 여기에 나와 있는 포트에서만 지원됩니다. 이러한 프로토콜 중 일부의 경우에는 네트워크 분석 정책을 사용하여 다른 포트로 검사를 확장할 수 있지만, NAT 재작성은 해당 포트로 확장되지 않습니다. 여기에는 DCERPC, DNS, FTP 및 Sun RPC 검사가 포함됩니다. 비표준 포트에서 이러한 프로토콜을 사용하는 경우에는 연결에 NAT를 사용하지 마십시오.

표 ***2: NAT***가 지원되는 애플리케이션 검사

애플리케이션	검사된 프로토콜, 포트	**NAT** 제한	핀홀 생성 여부
DCERPC	TCP/135	NAT64 없음	예
DNS over UDP	UDP/53	WINS를 통한 이름 확인에 NAT 지원을 이용할 수 없음	아니요
ESMTP	TCP/25	NAT64 없음	아니요
FTP	TCP/21	제한 없음 (클러스터링) 고정 PAT 없음.	예
H.323 H.225(호출 신호) H.323 RAS	TCP/1720 UDP/1718 RAS의 경우 UDP/1718-1719	(클러스터링) 고정 PAT 없음 확장 PAT 없음 NAT64 없음	예
ICMP ICMP Error	ICMP (디바이스 인터페이스로 전달된 ICMP 트래픽은 검사되지 않음)	제한 없음	아니요
IP Options	RSVP	NAT64 없음	아니요
NetBIOS Name Server over IP	UDP/137, 138(소스 포트)	확장 PAT 없음 NAT64 없음	아니요
RSH	TCP/514	PAT 없음 NAT64 없음 (클러스터링) 고정 PAT 없음.	예

애플리케이션	검사된 프로토콜, 포트	NAT 제한	핀홀 생성 여부
RTSP	TCP/554 (HTTP 클로킹을 처리하지 않음)	확장 PAT 없음 NAT64 없음 (클러스터링) 고정 PAT 없음.	예
SIP	TCP/5060 UDP/5060	확장 PAT 없음 NAT64 또는 NAT46 없음 (클러스터링) 고정 PAT 없음.	예
Skinny(SCCP)	TCP/2000	확장 PAT 없음 NAT64, NAT46 또는 NAT66 없음 (클러스터링) 고정 PAT 없음.	예
SQL*Net (버전 1, 2)	TCP/1521	확장 PAT 없음 NAT64 없음 (클러스터링) 고정 PAT 없음.	예
Sun RPC	TCP/111 UDP/111	확장 PAT 없음 NAT64 없음	예
TFTP	UDP/69	NAT64 없음 (클러스터링) 고정 PAT 없음. 페이로드 IP 주소는 변환되지 않습니다.	예
XDMCP	UDP/177	확장 PAT 없음 NAT64 없음 (클러스터링) 고정 PAT 없음.	예

NAT 추가 지침

- 브리지 그룹 멤버인 인터페이스의 경우 멤버 인터페이스용 NAT 규칙을 작성합니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT 규칙을 작성할 수 없습니다.
- 사이트 대 사이트 VPN에서 사용되는 VTI(Virtual Tunnel Interface)에 대해서는 NAT 규칙을 작성할 수 없습니다. VTI의 소스 인터페이스에 대해 규칙을 작성하면 VPN 터널에 NAT가 적용되지 않습니다. VTI에서 터널링된 VPN 트래픽에 적용할 NAT 규칙을 작성하려면 "any"를 인터페이스로 사용해야 합니다. 인터페이스 이름을 명시적으로 지정할 수 없습니다.

- (자동 NAT에만 해당함.) 한 개체에는 단일 NAT 규칙만 정의할 수 있습니다. 한 개체에 대해 여러 NAT 규칙을 구성하려면 동일한 IP 주소를 지정하는 서로 다른 이름의 여러 개체를 생성해야 합니다.
- 인터페이스에 VPN이 정의되어 있으면 인터페이스의 인바운드 ESP 트래픽에는 NAT 규칙이 적용되지 않습니다. 시스템은 설정된 VPN 터널에 대해서만 ESP 트래픽을 허용하며 기존 터널과 연결되지 않은 트래픽은 삭제합니다. 이러한 제한은 ESP 및 UDP 포트 500과 4500에 적용됩니다.
- UDP 포트 500 및 4500이 실제로 사용되지 않도록 동적 PAT를 적용하는 디바이스 뒤에 있는 디바이스에서 사이트 대 사이트 VPN을 정의하는 경우에는 PAT 디바이스 뒤의 디바이스에서 연결을 시작해야 합니다. 응답자는 정확한 포트 번호를 모르므로 SA(보안 연결)를 시작할 수 없습니다.
- NAT 컨피그레이션을 변경할 때 새 NAT 컨피그레이션이 사용되기 전에 기존 변환이 시간 초과되기까지 기다리지 않으려면 디바이스 CLI에서 **clear xlate** 명령을 사용하여 변환 테이블을 지울 수 있습니다. 그러나 변환 테이블을 지우면 변환을 사용하는 현재의 모든 연결이 해제됩니다.

  참고 동적 NAT 또는 PAT 규칙을 제거한 후 제거된 규칙의 주소와 중복되는 매핑된 주소가 포함된 새 규칙을 추가하는 경우, 새 규칙을 사용하려면 제거된 규칙과 관련된 모든 연결이 시간 초과되기까지 기다리거나 **clear xlate** 명령으로 해당 연결을 지워야 합니다. 이러한 안전 조치는 동일한 주소가 여러 호스트에 할당되는 것을 방지합니다.

- IPv4 및 IPv6 주소를 모두 포함하는 개체 그룹은 사용할 수 없습니다. 개체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
- NAT에서 사용되는 네트워크 개체는 주소 범위 또는 서브넷에서 명시적으로 또는 묵시적으로 131,838개 이상의 IP 주소를 포함할 수 없습니다. 주소 공간을 더 작은 범위로 분할하고 더 작은 개체에 대해 별도의 규칙을 작성합니다.
- (수동 NAT에만 해당함.) NAT 규칙에서 **any**를 소스 주소로 사용하는 경우 "any" 트래픽의 정의(IPv4 대 IPv6)는 규칙에 따라 다릅니다. Firepower Threat Defense 디바이스가 패킷에 대해 NAT를 수행하기 전에 패킷은 IPv6-IPv6 또는 IPv4-IPv4여야 합니다. 이 전제 조건하에 Firepower Threat Defense 디바이스는 NAT 규칙에서 **any**의 값을 결정할 수 있습니다. 예를 들어 **any**에서 IPv6 서버로 규칙을 구성하며 해당 서버가 IPv4 주소에서 매핑된 것이면 any는 "모든 IPv6 트래픽"을 의미합니다. “any” 에서 “any”로 규칙을 구성하며 소스를 인터페이스 IPv4 주소로 매핑하면 **any**는 “모든 IPv4 트래픽”을 의미합니다. 매핑된 인터페이스 주소는 대상 주소도 IPv4임을 암시하기 때문입니다.
- 여러 NAT 규칙에서 동일한 매핑된 개체 또는 그룹을 사용할 수 있습니다.
- 매핑된 IP 주소 풀에는 다음을 포함할 수 없습니다.
  - 매핑된 인터페이스 IP 주소. 규칙에 대해 "any" 인터페이스를 지정하면 모든 인터페이스 IP 주소가 허용되지 않습니다. 인터페이스 PAT(라우팅 모드만 해당함)의 경우 인터페이스 주소 대신 인터페이스 이름을 사용합니다.
  - 페일오버 인터페이스 IP 주소

  - (투명 모드) 관리 IP 주소.
  - (동적 NAT) VPN이 활성화된 경우의 스탠바이 인터페이스 IP 주소

- 고정 및 동적 NAT 정책에서는 겹치는 주소 사용을 피해야 합니다. 예를 들어, PPTP의 보조 연결이 동적 xlate 대신 고정 상태인 경우 겹치는 주소를 사용하면 PPTP 연결 설정에 실패할 수 있습니다.
- NAT 규칙의 소스 주소와 원격 액세스 VPN 주소 풀에서는 겹치는 주소를 사용할 수 없습니다.
- 규칙에서 대상 인터페이스를 지정하는 경우에는 라우팅 테이블에서 경로를 조회하지 않고 해당 인터페이스를 이그레스 인터페이스로 사용합니다. 그러나 ID NAT의 경우에는 경로 조회를 대신 사용할 수 있는 옵션이 제공됩니다.
- NFS 서버에 연결하는 데 사용되는 Sun RPC 트래픽에서 PAT를 사용하는 경우, PAT'ed 포트가 1024 이상인 경우 NFS 서버가 연결을 거부할 수 있다는 점에 유의하십시오. NFS 서버의 기본 구성은 1024보다 상위 포트로부터의 연결을 거부하는 것입니다. 오류는 일반적으로 "권한 거부"입니다. PAT 풀의 포트 범위에 예약된 포트(1~1023)를 포함하는 옵션을 선택하지 않으면 1024 이상의 포트 매핑이 발생합니다. 모든 포트 번호를 허용하도록 NFS 서버 구성을 변경하여 이 문제를 방지할 수 있습니다.
- NAT는 통과 트래픽에만 적용됩니다. 시스템에서 생성된 트래픽에는 NAT가 적용되지 않습니다.
- 대문자 또는 소문자 조합을 사용하여 네트워크 개체 또는 그룹 pat-pool의 이름을 지정하지 마십시오.
- 단방향 옵션은 주로 테스트 용으로 유용하며 모든 프로토콜에서 작동하지 않을 수 있습니다. 예를 들어, NAT를 사용하여 SIP 헤더를 변환하려면 SIP에 프로토콜 검사가 필요하지만 변환을 단방향으로 설정하는 경우에는 이러한 검사가 수행되지 않습니다.

Threat Defense NAT 구성

네트워크 주소 변환은 매우 복잡해질 수 있습니다. 따라서 변환 문제와 까다로운 트러블슈팅 상황을 방지하기 위해 규칙을 최대한 단순하게 유지하는 것이 좋습니다. 그리고 NAT를 구현하기 전에 면밀한 계획을 세워야 합니다. 다음 절차에서는 기본적인 구성 방식에 대해 설명합니다.

NAT 정책은 공유 정책입니다. 디바이스에 NAT 규칙과 유사한 정책을 할당합니다.

할당된 디바이스에 정책의 규칙이 적용되는지 여부는 규칙에서 사용되는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)에 의해 결정됩니다. 인터페이스 개체가 디바이스에 하나 이상의 인터페이스를 포함하는 경우 규칙이 디바이스에 구축됩니다. 따라서 인터페이스 개체로 신중하게 구성된 단일 공유 정책 내에서 디바이스의 하위 집합에 적용되는 규칙을 구성할 수 있습니다. "Any" 인터페이스 개체에 적용되는 규칙은 모든 디바이스에 구축됩니다.

디바이스 그룹에 현저히 다른 규칙이 요구되는 경우 복수의 NAT 정책을 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**을 선택합니다.

- 새 정책을 생성하려면 **New Policy(**새 정책**)** > **Threat Defense NAT(**위협 방어 **NAT)**을 클릭합니다. 정책에 이름과 선택적으로 디바이스를 할당하고 **Save(**저장**)**을 클릭합니다.

  정책을 편집하고 정책 할당을 클릭하여 나중에 디바이스 할당을 변경할 수 있습니다.

- 수정( )을 클릭하여 기존 위협 방어 NAT 정책을 편집합니다. 해당 페이지는 FTD 디바이스에서 사용되지 않는 Firepower NAT 정책도 표시합니다.

단계 **2** 필요한 규칙의 종류를 결정합니다.

동적 NAT, 동적 PAT, 고정 NAT 및 ID NAT 규칙을 생성할 수 있습니다. 이와 관련된 개요는 NAT 유형, 3 페이지를 참조하십시오.

단계 **3** 수동 또는 자동 NAT로 구현할 규칙을 결정합니다.

이 두 가지 구현 옵션을 비교한 내용은 자동 NAT 및 수동 NAT, 5 페이지를 참조하십시오.

단계 **4** 디바이스에 따라 사용자 정의되어야 하는 규칙을 결정합니다.

여러 디바이스에 NAT 정책을 할당할 수 있으므로 여러 장치에 단일 규칙을 구성할 수 있습니다. 그러나 각 디바이스에 따라 다르게 해석되어야 하는 규칙 또는 디바이스의 하위 집합에만 적용되어야 하는 일부 규칙이 따로 있을 수 있습니다.

규칙이 구성될 디바이스를 제어할 때는 인터페이스 개체를 사용합니다. 디바이스당 주소를 사용자 정의하려면 네트워크 개체의 개체 오버라이드를 사용합니다.

자세한 내용은 여러 디바이스에 대한 NAT 규칙 맞춤 설정, 18 페이지를 참조하십시오.

단계 **5** 다음 섹션에서 설명하는 대로 규칙을 생성합니다.

- 동적 NAT, 21 페이지
- 동적 PAT, 27 페이지
- 고정 NAT, 38 페이지
- ID NAT, 47 페이지

단계 **6** NAT 정책 및 규칙을 관리합니다.

다음을 수행하여 정책과 해당 규칙을 관리할 수 있습니다.

- 정책 이름 또는 설명을 편집하려면 해당 필드를 클릭하고 변경 내용을 입력한 다음 필드 바깥쪽을 클릭합니다.
- 특정 디바이스에만 적용되는 규칙을 보려면 **Filter by Device(**디바이스별 필터**)**를 클릭하고 원하는 디바이스를 선택합니다. 디바이스의 인터페이스를 포함하는 인터페이스 개체를 사용하는 경우 규칙이 디바이스에 적용됩니다.

- 정책이 할당될 디바이스를 변경하려면 **Policy Assignment(**정책 할당**)** 링크를 클릭하고 선택한 디바이스 목록을 수정합니다.
- 규칙의 활성화 또는 비활성화 여부를 변경하려면 규칙을 오른쪽 클릭하고 **State(**상태**)** 명령에서 원하는 옵션을 선택합니다. 이런 제어를 사용해 규칙을 삭제하지 않고도 일시적으로 비활성화할 수 있습니다.
- 규칙을 수정하려면 해당 규칙의 수정( )을 클릭합니다.
- 규칙을 삭제하려면 해당 규칙의 삭제( )을 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

여러 디바이스에 대한 NAT 규칙 맞춤 설정

NAT 정책이 공유되기 때문에 두 개 이상의 디바이스에 특정 정책을 할당할 수 있습니다. 지정된 개체에 대해 최대 하나의 자동 NAT 규칙을 구성할 수 있습니다. 따라서 변환을 수행하는 특정 디바이스를 기반으로 개체에 대해 다른 변환을 구성하려는 경우 인터페이스 개체(보안 영역 또는 인터페이스 그룹)를 신중하게 구성하고 변환된 주소에 대한 네트워크 개체를 재정의해야 합니다.

인터페이스 개체는 규칙이 구성되는 디바이스를 결정합니다. 네트워크 개체 재정의는 해당 디바이스에서 해당 개체에 사용되는 IP 주소를 결정합니다.

다음 시나리오를 고려하십시오.

- FTD-A와 FTD-B에는 "inside"라는 인터페이스에 연결된 내부 네트워크 192.168.1.0/24가 있습니다.
- FTD-A에서는 "outside" 인터페이스로 이동할 때 모든 192.168.1.0/24 주소를 10.100.10.10 - 10.100.10.200 범위의 NAT 풀로 변환하려고 합니다.
- FTD-B에서는 "outside" 인터페이스로 이동할 때 모든 192.168.1.0/24 주소를 10.200.10.10 - 10.200.10.200 범위의 NAT 풀로 변환하려고 합니다.

위의 작업을 수행하려면 다음을 수행합니다. 이 예제 규칙은 동적 자동 NAT를 위한 것이지만 모든 유형의 NAT 규칙에 대한 기술을 일반화할 수 있습니다.

프로시저

단계 **1** 내부 및 외부 인터페이스용 보안 영역을 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Interface Objects(**인터페이스 개체**)**를 선택하고 **Add(**추가**)** > **Security Zone(**보안 영역**)**을 선택합니다. (영역 대신 인터페이스 그룹을 사용할 수 있습니다.)

c) 내부 영역 속성을 구성합니다.

- **Name(**이름**)** - 예를 들어 **inside-zone**이라는 이름을 입력합니다.
- **Type(**유형**)** - 라우팅된 모드 디바이스에 대해 **Routed(**라우팅됨**)**을 선택하고, 투명 모드로 전환합니다.
- **Selected Interfaces(**선택한 인터페이스**)** - 선택된 목록에 FTD-A/inside 및 FTD-B/inside 인터페이스를 추가합니다.

d) **Save(**저장**)**를 클릭합니다.

e) **Add(**추가**)** > **Security Zone(**보안 영역**)**을 클릭하고 외부 영역 속성을 정의합니다.

- **Name(**이름**)** - 예를 들어 **outside-zone**이라는 이름을 입력합니다.
- **Interface Type(**인터페이스 유형**)** - 라우팅된 모드 디바이스에 대해 **Routed(**라우팅됨**)**을 선택하고, 투명 모드로 전환합니다.
- **Selected Interfaces(**선택한 인터페이스**)** - 선택된 목록에 FTD-A/outside 및 FTD-B/outside 인터페이스를 추가합니다.

f) **Save(**저장**)**를 클릭합니다.

단계 **2** 개체 관리 페이지에서 원래의 내부 네트워크에 대한 네트워크 개체를 만듭니다.

a) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 내부 네트워크 속성을 구성합니다.

- **Name(**이름**)** - 예를 들어 **inside-network**라는 이름을 입력합니다.
- **Network(**네트워크**)** - 네트워크 주소를 입력합니다(예: **192.168.1.0/24**).

c) **Save(**저장**)**를 클릭합니다.

단계 **3** 변환된 NAT 풀에 대한 네트워크 개체를 만들고 재정의를 정의합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) FTD-A에 대한 NAT 풀 등록 정보를 구성합니다.

- **Name(**이름**)** - 예를 들어 **NAT-pool**이라는 이름을 입력합니다.
- **Network(**네트워크**)** - FTD-A용 풀에 포함할 주소 범위를 입력합니다(예: **10.100.10.10-10.100.10.200**).

c) **Allow Overrides(**재정의 허용**)**를 선택합니다.

d) **Overrides** 제목을 클릭하여 개체 재정의 목록을 엽니다.

e) **Add(**추가**)**를 클릭하여 Add Object Override(개체 재정의 추가) 대화 상자를 엽니다.

f) FTD-B를 선택하고 Selected Devices(선택한 디바이스) 목록에 추가합니다.

g) **Override(**재정의**)**를 클릭하고 **Network(**네트워크**)**를 **10.200.10.10-10.200.10.200**으로 변경합니다.

h) **Add(**추가**)**를 클릭하여 디바이스에 재정의를 추가합니다.

FTD-B에 대한 재정의를 정의하면 시스템이 FTD-B에서 이 개체를 구성할 때마다 원래 개체에 정의된 값 대신 대체 값을 사용합니다.

i) **Save(**저장**)**를 클릭합니다.

단계 **4** NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 동적

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside-zone.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside-zone.

참고 인터페이스 개체는 규칙이 구성되는 디바이스를 제어합니다. 이 예제에서는 영역에 FTD-A 및 FTD-B에 대한 인터페이스만 포함되어 있기 때문에 NAT 정책이 추가 디바이스에 할당된 경우에도 해당 규칙은 이 두 디바이스에만 배포됩니다.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = inside-network 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = NAT-pool 개체.

f) **Save(**저장**)**를 클릭합니다.

이제 FTD-A 및 FTD-B에 대해 다르게 해석될 단일 규칙이 있으며 각 방화벽으로 보호되는 내부 네트워크에 대한 고유한 변환을 제공합니다.

NAT 규칙 테이블 검색 및 필터링

NAT 규칙 테이블을 검색하고 필터링하여 수정하거나 확인해야 하는 규칙을 찾을 수 있습니다. 테이블을 필터링하면 일치하는 규칙만 표시됩니다. 규칙 번호는 1, 2 등으로 순차적으로 변경되지만 필터링에서는 숨겨진 규칙을 기준으로 실제 규칙 번호 또는 테이블의 규칙 위치가 변경되지 않습니다. 필터링은 사용자가 관심 있는 규칙을 찾는 데 도움이 될 수 있는 항목만 변경합니다.

NAT 정책을 수정할 때 테이블 위의 필드를 사용하여 다음 유형의 검색/필터를 수행할 수 있습니다.

- **Filter by Device(**디바이스로 필터링**)**-**Filter by Device(**디바이스로 필터링**)**를 클릭한 다음 규칙을 보려는 디바이스를 선택하고 **OK(**확인**)**를 클릭합니다. 규칙이 디바이스에 적용되는지 여부는 규칙의 인터페이스 제약 조건에 따라 결정됩니다. 소스 또는 대상 인터페이스에 대해 보안 영역 또는 인터페이스 그룹을 지정하는 경우 최소 하나의 디바이스 인터페이스가 해당 영역 또는 그

룹에 있어도 규칙이 디바이스에 적용됩니다. NAT 규칙이 모든 소스 및 대상 인터페이스에 적용되는 경우 모든 디바이스에 적용됩니다.

텍스트 또는 다중 속성 검색도 수행하는 경우 결과는 선택한 디바이스로 제한됩니다.

이 필터를 제거하려면 **Filter by Device(**디바이스 기준 필터링**)**를 클릭하고 디바이스를 선택 취소하거나 **All(**모두**)**을 선택하고 **OK(**확인**)**를 클릭합니다.

- **Simple Text Search(**단순 텍스트 검색**)-Filter(**필터**)** 상자에 문자열을 입력하고 Enter를 누릅니다. 문자열은 규칙의 모든 값과 비교됩니다. 예를 들어 네트워크 개체의 이름 인 "network-object-1"을 입력하면 소스, 대상 및 PAT 풀 속성에서 개체를 사용하는 규칙을 가져옵니다.

  네트워크 및 포트 개체의 경우 문자열은 규칙에 사용된 개체의 내용과도 비교됩니다. 예를 들어 PAT 풀 개체에 10.100.10.3-10.100.10.100 범위가 포함된 경우 10.100.10.3 또는 10.100.10.100(또는 부분 10.100.10)을 검색하면 해당 PAT 풀 개체를 사용하는 규칙이 포함됩니다. 그러나 정확히 일치해야 합니다. IP 주소가 개체의 IP 주소 범위 내에 있더라도 10.100.10.5를 검색하면 이 PAT 풀 개체와 일치하지 않습니다.

  필터를 제거하려면 Filter(필터) 상자의 오른쪽에 있는 **x**를 클릭합니다.

- **Multiple-Attribute Search(**다중 속성 검색**)**-단순 텍스트 검색에서 너무 많은 적중 횟수를 제공하는 경우 검색에 대해 여러 값을 구성할 수 있습니다. **Filter(**필터**)** 상자를 클릭하여 속성 목록을 연 다음 검색하려는 속성의 문자열을 선택하거나 입력하고 **Filter(**필터**)** 버튼을 클릭합니다. 이러한 속성은 NAT 규칙 내에서 구성하는 속성과 동일합니다. 속성에는 AND가 적용되므로 필터링된 결과에는 사용자가 구성한 모든 속성과 일치하는 규칙만 포함됩니다.

  - 규칙 상태(활성화됨/비활성화됨), 즉 PAT 풀의 구성 여부(활성화/비활성화), 규칙 방향(일방/쌍방) 또는 규칙 유형(고정/동적)과 같은 이진 속성의 경우 간단히 적절한 확인란을 선택 또는 선택 취소합니다. 속성 값이 중요하지 않은 경우 두 확인란을 모두 선택합니다. 두 확인란을 모두 선택 취소하면 필터와 일치하는 규칙이 없게 됩니다.
  - 문자열 속성의 경우 해당 속성과 관련된 전체 또는 부분 문자열을 입력합니다. 이는 보안 영역/인터페이스 그룹, 네트워크 개체 또는 포트 개체의 개체 이름입니다. 또한 간단한 텍스트 검색과 동일한 방식으로 일치하는 네트워크 또는 포트 개체 콘텐츠 일 수도 있습니다.

  필터를 제거하려면 Filter(필터) 상자 오른쪽의 **x**를 클릭하거나 Filter(필터) 상자를 클릭하여 드롭다운 목록을 열고 Clear(지우기) 버튼을 클릭합니다.

동적 **NAT**

다음 주제에서는 동적 NAT 및 동적 NAT를 구성하는 방법에 대해 설명합니다.

동적 **NAT** 정보

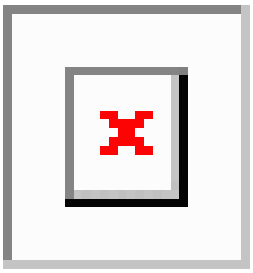
동적 NAT는 실제 주소의 그룹을 대상 네트워크에서 라우팅 가능한 매핑된 주소의 풀로 변환합니다. 매핑된 풀에는 일반적으로 실제 그룹보다 더 적은 수의 주소가 포함되어 있습니다. 변환하려는 호스트가 대상 네트워크에 액세스하면 NAT에서는 매핑된 풀의 IP 주소를 호스트에 할당합니다. 실제 호스트가 연결을 시작하는 경우에만 변환이 생성됩니다. 변환은 연결되어 있는 동안에만 이루어지며, 변환 시간이 초과된 후에는 사용자의 IP 주소가 동일하게 유지되지 않습니다. 따라서 액세스 규칙에

서 연결을 허용하더라도, 대상 네트워크의 사용자는 동적 NAT를 사용하는 호스트에 대해 안정적인 연결을 시작할 수 없습니다.

참고 액세스 규칙에서 허용하는 경우, 변환 기간 동안 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 주소는 예측할 수 없으므로 호스트로의 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

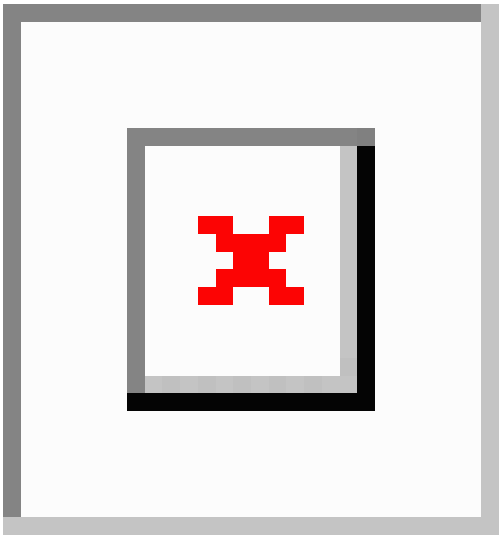
다음 그림은 일반적인 동적 NAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다.

그림 *4:* 동적 *NAT*



다음 그림은 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트를 보여줍니다. 이 주소는 현재 변환 테이블에 있지 않으므로 패킷이 삭제됩니다.

그림 *5:* 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트



동적 NAT의 단점 및 장점

동적 NAT의 단점은 다음과 같습니다.

- 매핑된 풀의 주소 수가 실제 그룹의 주소 수보다 적은 경우, 트래픽의 양이 예상보다 많아지면 주소가 부족해질 수 있습니다.

PAT는 단일 주소의 포트를 사용하여 64,000이 넘는 변환을 제공하므로, 이러한 상황이 발생하면 PAT 또는 PAT 대안을 사용하십시오.

- 매핑된 풀에서 대량의 라우팅 가능한 주소를 사용해야 하는데, 라우팅 가능한 주소는 대량으로 사용 가능하지 않을 수 있습니다.

동적 NAT의 장점은 일부 프로토콜이 PAT를 사용할 수 없다는 것입니다. PAT는 다음과 작동하지 않습니다.

- GRE 버전 0과 같이 오버로드할 포트가 없는 IP 프로토콜
- 한 포트에 데이터 스트림이 있고 다른 포트에 제어 경로가 있으며 개방형 표준이 아닌 일부 멀티미디어 애플리케이션

동적 자동 NAT 구성

동적 자동 NAT 규칙을 사용하여 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- **Translated Source(**변환된 소스**)** - 이는 네트워크 개체 또는 그룹일 수는 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- 유형 - 동적을 선택합니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** **Translation(**변환**)**에서 탭에서 다음 옵션을 구성합니다.

- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체입니다.
- **Translated Source(**변환된 소스**)** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다.

단계 **6** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 - DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 104 페이지을 참조하십시오.
- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **8** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

동적 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 동적 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 동적 NAT는 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.

- **Translated Source(**변환된 소스**)** - 이는 네트워크 개체 또는 그룹일 수는 있지만 서브넷을 포함할 수는 없습니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.

규칙에서 원본 대상 및 변환된 대상에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다.

동적 NAT의 경우 대상에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 대상 포트 및 변환된 대상 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. 소스 포트를 지정하면 무시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

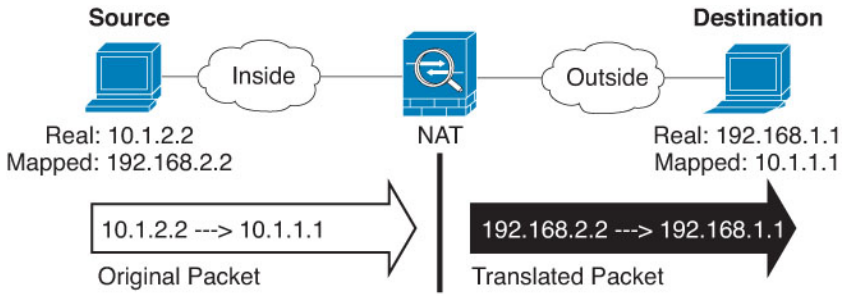
- **NAT Rule(NAT** 규칙**)** - **Manual NAT Rule(**수동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**)** - 동적을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.
- **Enable(**활성화**)**—규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다.
- **Insert(**삽입**)**—규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.
- 소스 인터페이스, 대상 인터페이스 - 이 NAT 규칙을 적용할 인터페이스입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**).

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** (변환 페이지에서) 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Source Interface IP(소스 인터페이스 **IP)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- **Translated Source(**변환된 소스**)** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다.
- **Translated Destination(**변환된 대상**)** - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환용 대상 서비스 포트(**Original Destination Port(**원본 대상 포트**)**, **Translated Destination Port(**변환된 대상 포트**)**)를 식별합니다.

동적 NAT는 포트 변환을 지원하지 않으므로 **Original Destination Port(**원본 대상 포트**)** 및 **Translated Destination Port(**변환된 대상 포트**)** 필드를 비워 둡니다. 그러나 대상 변환은 항상 고정이므로 대상 포트의 포트 변환을 수행할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

단계 **8** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- (소스 변환만 해당) 이 규칙과 일치하는 **DNS** 회신 변환 - DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 104 페이지을 참조하십시오.

- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

단계 **9** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **10** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

동적 **PAT**

다음 주제에서는 동적 PAT에 대해 설명합니다.

동적 **PAT** 정보

동적 PAT는 실제 주소 및 소스 포트를 매핑된 주소 및 고유한 포트로 변환함으로써 여러 실제 주소를 단일 매핑된 IP 주소로 변환합니다.

소스 포트는 각 연결에 대해 다르므로 연결마다 별도의 변환 세션이 필요합니다. 예를 들어 10.1.1.1:1025를 사용하려면 10.1.1.1:1026에서 별도로 변환해야 합니다.

다음 그림은 일반적인 동적 PAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다. 매핑된 주소는 각 변환에 대해 동일하지만 포트는 동적으로 할당됩니다.

그림 *6:* 동적 ***PAT***

액세스 규칙에서 허용하는 경우, 변환 기간 동안 대상 네트워크의 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 포트 주소(실제 및 매핑된 주소 모두)는 예측할 수 없으므로 호스트에 대한 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

연결이 만료되면 포트 변환도 만료됩니다.

참고 각 인터페이스에 각기 다른 PAT 풀을 사용하는 것이 좋습니다. 여러 인터페이스에 동일한 풀을 사용하는 경우, 특히 "any" 인터페이스에 동일한 풀을 사용하는 경우에 풀이 빠르게 소진될 수 있어 새 변환에 포트를 사용할 수 없게 됩니다.

동적 PAT의 단점 및 장점

동적 PAT에서는 단일 매핑된 주소를 사용하여 라우팅 가능한 주소를 아낄 수 있습니다. Firepower Threat Defense 디바이스 인터페이스 IP 주소를 PAT 주소로서 사용할 수도 있습니다.

데이터 스트림이 제어 경로와 다른 일부 멀티미디어 애플리케이션에서는 동적 PAT가 작동하지 않습니다. 자세한 내용은 검사된 프로토콜에 대한 NAT 지원, 12 페이지를 참조하십시오.

동적 PAT는 단일 IP 주소에서 오는 것처럼 보이는 대량의 연결을 생성할 수 있으며, 서버는 이 트래픽을 DoS 공격으로 해석할 수 있습니다. 주소의 PAT 풀을 구성하고 PAT 주소를 라운드 로빈 방식으로 할당하여 이 상황을 완화할 수 있습니다.

PAT 풀 개체 지침

PAT의 네트워크 개체를 만드는 경우 다음 지침을 따르십시오.

PAT 풀의 경우

- 포트는 1024~65535 범위의 사용 가능한 포트에 매핑됩니다. 경우에 따라 예약된 포트(1024 미만)를 포함하여 전체 포트 범위를 변환에 사용할 수 있습니다.

  클러스터에서 작동하는 경우, 주소당 512개 포트의 블록이 클러스터의 멤버에 할당되며 이러한 포트 블록 내에서 매핑이 이루어집니다. 블록 할당도 활성화할 경우, 포트는 블록 할당 크기에 따라 분산되며 기본값은 512입니다.

- PAT 풀에 대한 블록 할당을 활성화하면 포트 블록은 1024-65535 범위로만 할당됩니다. 따라서 애플리케이션에 낮은 포트 번호(1-1023)가 필요한 경우 작동하지 않을 수 있습니다. 예를 들어 포트 22(SSH)를 요청하는 애플리케이션은 1024-65535 범위 내에서 호스트에 할당된 블록 내에서 매핑된 포트를 가져옵니다.

- 별개의 두 규칙에서 동일한 PAT 풀 개체를 사용하는 경우 각 규칙에 대해 동일한 옵션을 지정해야 합니다. 예를 들어, 한 규칙에서 확장 PAT를 지정하는 경우, 다른 규칙에서도 확장 PAT를 지정해야 합니다.

PAT 풀용 확장 PAT의 경우

- 확장 PAT를 지원하지 않는 애플리케이션 검사가 많습니다.
- 동적 PAT 규칙에 대해 확장 PAT를 활성화하면, PAT 풀의 주소를 별도의 포트 변환 고정 NAT 규칙에서 PAT 주소로서 사용할 수 없습니다. 예를 들어 PAT 풀이 10.1.1.1을 포함하면, 10.1.1.1을 PAT 주소로 사용하는 포트 변환 고정 NAT 규칙을 만들 수 없습니다.
- PAT 풀을 사용하고 대안용 인터페이스를 지정하는 경우 확장 PAT를 지정할 수 없습니다.
- ICE 또는 TURN을 사용하는 VoIP 구축에는 확장 PAT를 사용할 수 없습니다. ICE 및 TURN은 모든 대상에 대해 PAT 바인딩이 동일할 것으로 신뢰합니다.
- 클러스터의 유닛에서는 확장 PAT를 사용할 수 없습니다.

PAT 풀용 라운드 로빈의 경우

- 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. 장애 조치 이후에는 "동질성"이 해제됩니다. 디바이스에서 장애 조치를 수행하면 호스트의 후속 연결에는 초기 IP 주소가 사용되지 않을 수 있습니다.
- 동일한 인터페이스에서 PAT 풀/라운드 로빈 규칙과 인터페이스 PAT 규칙을 혼합하면 IP 주소 "동질성"도 영향을 받습니다. 특정 인터페이스에 대해 PAT 풀 또는 인터페이스 PAT를 선택합니다. 경쟁적인 PAT 규칙을 만들지 마십시오.
- 라운드 로빈은 특히 확장 PAT와 함께 사용할 경우 대량의 메모리를 소모할 수 있습니다. NAT 풀은 모든 매핑된 프로토콜/IP 주소/포트 범위에 대해 생성되므로, 라운드 로빈에서 대량의 동시 NAT 풀이 생성되며 여기에서 메모리를 사용합니다. 확장 PAT를 사용하면 동시 NAT 풀의 수가 더 많아집니다.

동적 자동 PAT 구성

동적 자동 PAT 규칙을 사용하여 주소를 여러 IP 주소만으로 변환하는 대신 고유한 IP 주소/포트 조합으로 변환합니다. 단일 주소(대상 인터페이스의 주소 또는 다른 주소)로 변환하거나 PAT 주소 풀을 사용하여 가능한 많은 수의 변환을 제공할 수 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- 변환된 소스 - 다음 옵션을 사용하여 PAT 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다.
  - 단일 **PAT** 주소 - 단일 호스트를 포함하는 네트워크 개체를 생성합니다.
  - **PAT** 풀 - 범위가 포함된 네트워크 개체를 만들거나 호스트, 범위 또는 둘 다를 포함하는 네트워크 개체 그룹을 만듭니다. 서브넷을 포함할 수 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- 유형 - 동적을 선택합니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** **Translation(**변환**)**에서 탭에서 다음 옵션을 구성합니다.

- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 소스**(Translated Source)** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. PAT 풀 구성 단계를 건너뜁니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다. PAT 풀 구성 단계를 건너뜁니다.
  - PAT 풀을 사용하려면 변환된 소스**(Translated Source)** 를 비워 둡니다.

단계 **6** PAT 풀을 사용하는 경우 **PAT Pool(PAT** 풀**)** 페이지를 선택하고 다음을 수행합니다.

a) **Enable PAT pool(PAT** 풀 활성화**)**을 선택합니다.

b) **PAT** > **Address(**주소**)** 필드에서 풀의 주소를 포함하는 네트워크 개체 그룹을 선택합니다.

Destination Interface IP(대상 인터페이스 **IP)**를 선택하여 인터페이스 PAT를 구현할 수도 있습니다.

c) (선택 사항) 필요한 경우 다음 옵션을 선택합니다.

- **Use Round Robin Allocation(**라운드 로빈 할당 사용**)** - 라운드 로빈 방식으로 주소/포트를 할당하려는 경우 선택합니다. 기본적으로, 라운드 로빈이 아니면 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다.
- **Extended PAT Table(**확장 **PAT** 테이블**)** - 확장 PAT를 사용하려는 경우 선택합니다. 확장 PAT는 변환 정보의 대상 주소 및 포트를 포함하여 서비스당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 대상 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이

동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다. 이 옵션은 인터페이스 PAT 또는 인터페이스 PAT 대체와 함께 사용할 수 없습니다.

- **Flat Port Range(**균일 포트 범위**)**, **Include Reserved Ports(**예약된 포트 포함**)** - TCP/UDP 포트를 할당할 때 단일 균일 범위로 1024~65535 포트 범위를 사용하려는 경우 선택합니다. (6.7 버전 이전) 변환할 매핑된 포트 번호를 선택하면 PAT에서는 실제 소스 포트 번호(사용 가능한 경우)를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 없는 경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **Include Reserved Ports(**예약된 포트 포함**)** 옵션도 선택합니다. 버전 6.7 이상을 실행하는 FTD 디바이스의 경우 옵션 선택 여부에 관계없이 플랫 포트 범위가 항상 구성됩니다. 이러한 시스템에 대해 **Include Reserved Ports(**예약 포트 포함**)** 옵션을 여전히 선택할 수 있으며 해당 설정이 적용됩니다.
- **Block Allocation(**블록 할당**)**- 포트 블록 할당을 활성화하려는 경우 선택합니다. 캐리어급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다. 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한 활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 포트 블록은 1024~65535 범위에서만 할당됩니다. 포트 블록 할당은 라운드 로빈과는 호환되지만 확장 PAT 또는 플랫 포트 범위 옵션과 함께 사용할 수는 없습니다. 또한 인터페이스 PAT 대체를 사용할 수 없습니다.

단계 **7** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- **Fallthrough to Interface PAT (Destination Interface)(**인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**)** - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다. 인터페이스 PAT를 변환된 주소 또는 PAT 풀로 이미 구성한 경우에는 이 옵션을 선택할 수 없습니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **9** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

동적 수동 **PAT** 구성

자동 PAT가 요구를 충족하지 않을 때는 동적 수동 PAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 동적 PAT는 주소를 여러 IP 주소만으로 변환하는 대신 고유한 IP 주소/포트 조합으로 변환합니다. 단일 주소(대상 인터페이스의 주소 또는 다른 주소)로 변환하거나 PAT 주소 풀을 사용하여 가능한 많은 수의 변환을 제공할 수 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- 변환된 소스 - 다음 옵션을 사용하여 PAT 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다.
  - 단일 **PAT** 주소 - 단일 호스트를 포함하는 네트워크 개체를 생성합니다.
  - **PAT** 풀 - 범위가 포함된 네트워크 개체를 만들거나 호스트, 범위 또는 둘 다를 포함하는 네트워크 개체 그룹을 만듭니다. 서브넷을 포함할 수 없습니다.

규칙에서 원본 대상 및 변환된 대상에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다.

동적 NAT의 경우 대상에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 대상 포트 및 변환된 대상 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. 소스 포트를 지정하면 무시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

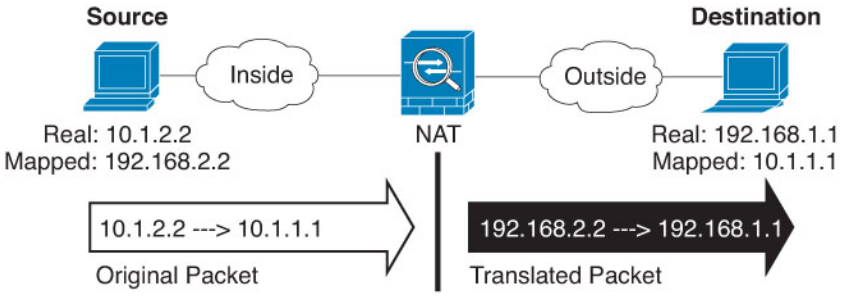
- **NAT Rule(NAT** 규칙**)** - **Manual NAT Rule(**수동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**)** - 동적을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.
- **Enable(**활성화**)**—규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다.
- **Insert(**삽입**)**—규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** (변환 페이지에서) 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Source Interface IP(소스 인터페이스 **IP)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스**(Translated Source)** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. PAT 풀 구성 단계를 건너뜁니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다. PAT 풀 구성 단계를 건너뜁니다.
  - PAT 풀을 사용하려면 변환된 소스**(Translated Source)** 를 비워 둡니다.
- **Translated Destination(**변환된 대상**)** - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환용 대상 서비스 포트(**Original Destination Port(**원본 대상 포트**)**, **Translated Destination Port(**변환된 대상 포트**)**)를 식별합니다.

동적 NAT는 포트 변환을 지원하지 않으므로 **Original Destination Port(**원본 대상 포트**)** 및 **Translated Destination Port(**변환된 대상 포트**)** 필드를 비워 둡니다. 그러나 대상 변환은 항상 고정이므로 대상 포트의 포트 변환을 수행할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

단계 **8** PAT 풀을 사용하는 경우 **PAT Pool(PAT** 풀**)** 페이지를 선택하고 다음을 수행합니다.

a) **Enable PAT pool(PAT** 풀 활성화**)**을 선택합니다.

b) **PAT** > **Address(**주소**)** 필드에서 풀의 주소를 포함하는 네트워크 개체 그룹을 선택합니다.

Destination Interface IP(대상 인터페이스 **IP)**를 선택하여 인터페이스 PAT를 구현할 수도 있습니다.

c) (선택 사항) 필요한 경우 다음 옵션을 선택합니다.

- **Use Round Robin Allocation(**라운드 로빈 할당 사용**)** - 라운드 로빈 방식으로 주소/포트를 할당하려는 경우 선택합니다. 기본적으로, 라운드 로빈이 아니면 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다.
- **Extended PAT Table(**확장 **PAT** 테이블**)** - 확장 PAT를 사용하려는 경우 선택합니다. 확장 PAT는 변환 정보의 대상 주소 및 포트를 포함하여 서비스당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 대상 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다. 이 옵션은 인터페이스 PAT 또는 인터페이스 PAT 대체와 함께 사용할 수 없습니다.
- **Flat Port Range(**균일 포트 범위**)**, **Include Reserved Ports(**예약된 포트 포함**)** - TCP/UDP 포트를 할당할 때 단일 균일 범위로 1024~65535 포트 범위를 사용하려는 경우 선택합니다. (6.7 버전 이전) 변환할 매핑된 포트 번호를 선택하면 PAT에서는 실제 소스 포트 번호(사용 가능한 경우)를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 없는 경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **Include Reserved Ports(**예약된 포트 포함**)** 옵션도 선택합니다. 버전 6.7 이상을 실행하는 FTD 디바이스의 경우 옵션 선택 여부에 관계없이 플랫 포트 범위가 항상 구성됩니다. 이러한 시스템에 대해 **Include Reserved Ports(**예약 포트 포함**)** 옵션을 여전히 선택할 수 있으며 해당 설정이 적용됩니다.
- **Block Allocation(**블록 할당**)**- 포트 블록 할당을 활성화하려는 경우 선택합니다. 캐리어급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다. 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한

활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 포트 블록은 1024~65535 범위에서만 할당됩니다. 포트 블록 할당은 라운드 로빈과는 호환되지만 확장 PAT 또는 플랫 포트 범위 옵션과 함께 사용할 수는 없습니다. 또한 인터페이스 PAT 대체를 사용할 수 없습니다.

단계 **9** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 인터페이스 **PAT(**대상 인터페이스**)**로 폴스루 - 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

단계 **10** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **11** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

포트 블록 할당으로 **PAT** 설정

통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한 활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 블록에서 포트를 사용하는 마지막 xlate가 제거되면 블록이 해제됩니다.

포트 블록을 할당하는 주된 이유는 로깅을 줄이는 것입니다. 포트 블록 할당이 기록되고 연결은 기록되지만 포트 블록 내에서 생성된 xlate는 기록되지 않습니다. 반면에, 이렇게 하면 로그 분석이 더 어려워집니다.

포트 블록은 1024~65535 범위에서만 할당됩니다. 따라서 애플리케이션에 낮은 포트 번호(1-1023)가 필요한 경우 작동하지 않을 수 있습니다. 예를 들어 포트 22(SSH)를 요청하는 애플리케이션은 1024-65535 범위 내에서 호스트에 할당된 블록 내에서 매핑된 포트를 가져옵니다. 낮은 포트 번호를 사용하는 애플리케이션에 대해 블록 할당을 사용하지 않는 별도의 NAT 규칙을 만들 수 있습니다. 2회 NAT를 사용하려면 규칙이 블록 할당 규칙보다 먼저 적용되는지 확인하십시오.

시작하기 전에

NAT 규칙에 대한 사용 참고 사항:

- **Use Round Robin Allocation(**라운드 로빈 할당 사용**)** 옵션을 포함할 수 있지만 PAT 고유성 확장, 플랫 범위 사용, 예비 포트 포함, 또는 PAT 인터페이스로 폴스루할 수 있는 옵션은 포함할 수 없습니다. 다른 소스/대상 주소 및 포트 정보도 허용됩니다.
- 모든 NAT 변경 사항과 마찬가지로 기존 규칙을 바꿀 경우 교체된 규칙과 관련된 xlate를 지워야 새 규칙이 적용됩니다. 명시적으로 지우거나 시간 초과될 때까지 기다릴 수 있습니다. 클러스터에서 작업할 때는 클러스터 전체에서 xlate를 전역적으로 지워야 합니다.

참고 개체 NAT에 대해 일반 PAT와 블록 할당 PAT 규칙 간에 전환하는 경우 먼저 규칙을 삭제한 다음 xlate를 지워야 합니다. 그런 다음 새 개체 NAT 규칙을 생성할 수 있습니다. 그렇지 않으면, **show asp drop** 출력에서 pat-port-block-state-mismatch 삭제가 발생합니다.

- 지정된 PAT 풀의 경우 풀을 사용하는 모든 규칙에 대해 블록 할당을 지정하거나 지정하지 않아야 합니다. 하나의 규칙에는 블록을 할당할 수 없고 다른 규칙에는 블록을 할당할 수 있습니다. 중복되는 PAT 풀도 블록 할당 설정을 혼합할 수 없습니다. 또한 정적 NAT는 풀의 포트 변환 규칙과 중복될 수 없습니다.

프로시저

단계 **1** (선택 사항). 전역 PAT 포트 블록 할당 설정을 구성합니다.

포트 블록 할당을 제어하는 몇 가지 전역 설정이 있습니다. 이 옵션의 기본값을 변경하려면 FlexConfig 개체를 구성하여 FlexConfig 정책에 추가해야 합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)** > **FlexConfig** > **FlexConfig Object(FlexConfig** 개체**)**를 선택하고 새 개체를 만듭니다.

b) 각 블록의 포트 수인 블록 할당 크기를 구성합니다.

xlate block-allocation size 값

범위는 32~4096입니다. 기본값은 512입니다. 기본값으로 되돌리려면 "no" 양식을 사용합니다.

기본값을 사용하지 않는 경우 선택한 크기가 64,512(1024-65535 범위의 포트 수)로 균등하게 나뉘어 있는지 확인합니다. 그렇지 않으면 사용할 수 없는 포트가 있게 됩니다. 예를 들어 100을 지정하는 경우 사용되지 않는 포트가 12개 있습니다.

c) 호스트당 할당할 수 있는 최대 블록을 구성합니다.

xlate block-allocation maximum-per-host *number*

제한은 프로토콜에 따라 다르기 때문에 4개의 제한은 호스트당 최대 4개의 UDP 블록, 4개의 TCP 블록 및 4개의 ICMP 블록을 의미합니다. 범위는 1-8이며, 기본값은 4입니다. 기본값으로 되돌리려면 "no" 양식을 사용합니다.

d) (선택 사항). 임시 syslog 생성을 활성화합니다.

xlate block-allocation pba-interim-logging *seconds*

기본적으로 시스템이 포트 블록 생성 및 삭제를 수행하는 동안 syslog 메시지를 생성합니다. 중간 로깅을 활성화하면 시스템은 지정하는 간격으로 다음 메시지를 생성합니다. 메시지는 이때 프로토콜(ICMP, TCP, UDP), 소스 및 대상 인터페이스, IP 주소, 포트 블록을 포함하여 할당된 모든 활성 포트 블록을 보고합니다. 21600-604800초(6시간~7일) 사이의 간격을 지정할 수 있습니다.

%ASA-6-305017: Pba-interim-logging: *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*의 변환에 대한 활성 포트 프로토콜 블록

예제:

다음 예제는 블록 할당 크기를 64로 설정하고 호스트당 최대 값을 8로 설정하고 6시간마다 임시 로깅을 활성화합니다.

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

e) FlexConfig 개체에서 다음 옵션을 선택합니다.

- **Deployment(**구축**)** = **Everytime(**항상**)**
- **Type(**유형**)** = **Append(**뒤에 추가**)**

f) **Save(**저장**)**를 클릭하여 FlexConfig 개체를 생성합니다.

g) **Devices(**디바이스**)** > **FlexConfig**를 선택하고 이러한 설정을 조정해야 하는 디바이스에 할당된 FlexConfig 정책을 만들거나 편집합니다.

h) 사용 가능한 개체 목록에서 개체를 선택하고 >를 클릭하여 선택한 개체 목록으로 이동합니다.

i) **Save(**저장**)**를 클릭합니다.

Preview Config(구성 미리보기**)**를 클릭하고 대상 디바이스 중 하나를 선택한 다음 xlate 명령이 올바르게 나타나는지 확인할 수 있습니다.

단계 **2** PAT 풀 포트 블록 할당을 사용하는 NAT 규칙을 추가합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 Threat Defense NAT 정책을 생성하거나 편집합니다.

b) NAT 규칙을 추가 또는 편집하고 다음 옵션을 구성합니다.

- **Type(**유형**)** = **Dynamic(**동적**)**.
- **Translation(**변환**)** > **Original Source(**원본 소스**)**에서 원본 주소를 정의하는 개체를 선택합니다.
- **PAT** 풀에서 다음 옵션을 구성합니다.
  - **Enable PAT Pool(PAT** 풀 활성화**)**을 선택합니다.
  - **PAT** > **Address(**주소**)**에서 pat 풀을 정의하는 네트워크 개체를 선택합니다.
  - **Block Allocation(**블록 할당**)** 옵션을 선택합니다.

c) 변경 사항을 규칙 및 NAT 정책에 저장합니다.

고정 NAT

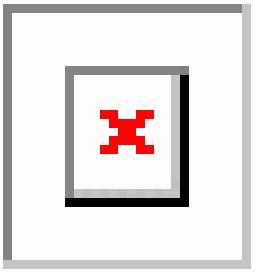
다음 주제에서는 고정 NAT 및 고정 NAT를 구현하는 방법에 대해 설명합니다.

고정 NAT 정보

고정 NAT는 실제 주소에서 매핑된 주소로의 고정된 변환을 생성합니다. 매핑된 주소는 각각의 연속 연결에 대해 동일하므로 NAT는 양방향 연결 시작을 허용합니다. 이를 허용하는 액세스 규칙이 있는 경우 호스트에서 나가기도 하고 호스트로 들어오기도 합니다. 반면 동적 NAT 및 PAT의 경우, 각 호스트는 각 후속 변환에 대해 서로 다른 주소 또는 포트를 사용하므로 양방향 시작이 지원되지 않습니다.

다음 그림은 일반적인 고정 NAT 시나리오를 보여줍니다. 변환이 항상 활성 상태이므로 실제 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 *7:* 고정 *NAT*



참고 원하는 경우 양방향을 비활성화할 수 있습니다.

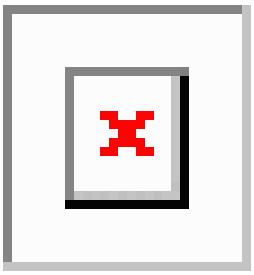
포트 변환 고정 NAT

포트 변환 고정 NAT를 사용하면 실제 및 매핑된 프로토콜과 포트를 지정할 수 있습니다.

고정 NAT로 포트를 지정하는 경우 포트 및/또는 IP 주소를 동일한 값으로 매핑할지 아니면 다른 값으로 매핑할지를 선택할 수 있습니다.

다음 그림은 자신에게 매핑되는 포트와 다른 값으로 매핑되는 포트 모두를 보여주는 포트 변환 시나리오의 일반적인 고정 NAT를 보여줍니다. 두 경우 모두 IP 주소는 다른 값으로 매핑됩니다. 변환이 항상 활성 상태이므로 변환된 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 *8:* 일반적인 포트 변환 고정 *NAT* 시나리오



포트 변환 고정 NAT 규칙은 지정된 포트에 대해서만 대상 IP 주소 액세스를 제한합니다. NAT 규칙이 적용되지 않는 다른 포트에서 대상 IP 주소에 액세스를 시도하면 연결은 차단됩니다. 또한 수동 NAT의 경우 NAT 규칙의 소스 IP 주소와 일치하지 않는 트래픽은 대상 포트와 관계없이 대상 IP 주소와 일치하는 경우 삭제됩니다. 그러므로 대상 IP 주소에 대해 허용되는 기타 모든 트래픽을 위한 규칙을 더 추가해야 합니다. 예를 들어 포트 사양 없이 IP 주소용 고정 NAT 규칙을 구성하여 포트 변환 규칙 뒤에 배치할 수 있습니다.

참고 보조 채널(예: FTP 및 VoIP)에 대해 애플리케이션 검사를 요구하는 애플리케이션의 경우 NAT에서는 자동으로 보조 포트를 변환합니다.

포트 변환 고정 NAT의 몇 가지 다른 사용 방식은 다음과 같습니다.

ID 포트 변환 고정 **NAT**

내부 리소스에 대한 외부 액세스를 간소화할 수 있습니다. 예를 들어, FTP, HTTP, SMTP 등 각기 다른 포트에서 서비스를 제공하는 개별 서버 3개가 있는 경우 외부 사용자에게 해당 서비스 액세스를 위한 단일 IP 주소를 제공할 수 있습니다. 그런 후에 외부 사용자들이 액세스하려는 포트를 기준으로 하여 실제 서버의 올바른 IP 주소에 단일 외부 IP 주소를 매핑하도록 ID 포트 변환 고정 NAT를 구성할 수 있습니다. 이러한 서버는 표준 포트(각각 21, 80, 25)를 사용하므로 포트를 변경할 필요는 없습니다.

비표준 포트에 대한 포트 변환 고정 **NAT**

잘 알려진 포트를 비표준 포트로 또는 그 반대로 변환하려는 경우에도 포트 변환 고정 NAT를 사용할 수 있습니다. 예를 들어 내부 웹 서버가 포트 8080을 사용하는 경우 외부 사용자가 포트 80에 연결하도록 허용한 다음 원본 포트 8080으로의 변환을 취소할 수 있습니다. 마찬가지로, 보안을 강화하려면 웹 사용자에게 비표준 포트 6785로 연결하도록 안내한 다음 포트 80으로의 변환을 취소할 수 있습니다.

포트 변환 고정 인터페이스 **NAT**

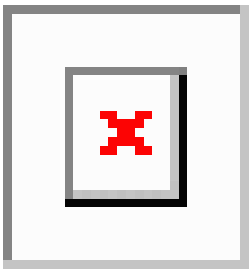
실제 주소를 인터페이스 주소/포트 조합으로 매핑하도록 고정 NAT를 구성할 수 있습니다. 예를 들어 디바이스의 외부 인터페이스에 대한 텔넷 액세스를 내부 호스트로 리디렉션하려는 경우 내부 호스트 IP 주소/포트 23을 외부 인터페이스 주소/포트 23에 매핑할 수 있습니다.

일대다 고정 **NAT**

일반적으로 NAT는 일대일 매핑으로 구성합니다. 그러나 경우에 따라 여러 매핑된 주소에 대해 단일 실제 주소를 구성해야 할 수도 있습니다(일대다). 일대다 고정 NAT를 구성할 경우, 실제 호스트가 트래픽을 시작하면 항상 첫 번째 매핑된 주소를 사용합니다. 그러나 호스트에 대해 시작된 트래픽의 경우, 매핑된 주소 중 하나에 대해 트래픽을 시작할 수 있습니다. 이러한 주소는 단일 실제 주소로 변환되지 않습니다.

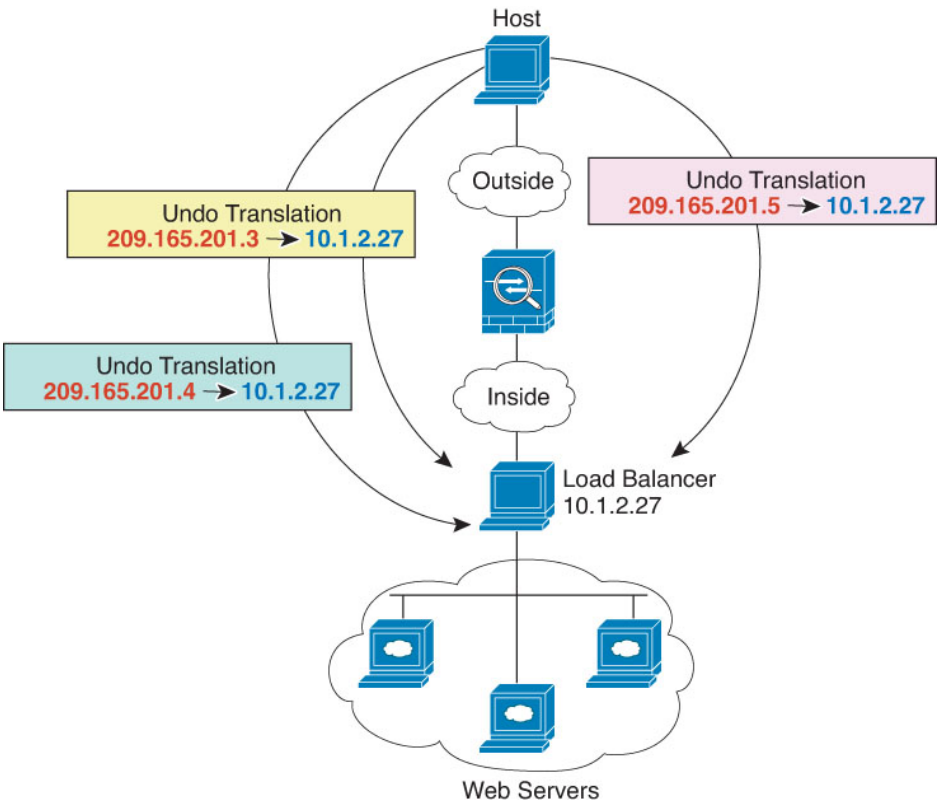
다음 그림은 일반적인 일대다 고정 NAT 시나리오를 보여줍니다. 실제 호스트에 의한 시작은 항상 첫 번째 매핑된 주소를 사용하므로, 실제 호스트 IP/첫 번째 매핑된 IP의 변환이 기술적으로 유일한 양방향 변환입니다.

그림 *9:* 일대다 고정 *NAT*



예를 들어 10.1.2.27에 로드 밸런서가 있으면, 요청된 URL에 따라 트래픽이 올바른 웹 서버로 리디렉션됩니다.

그림 *10:* 일대다 고정 *NAT* 예



기타 매핑 시나리오(권장되지 않음)

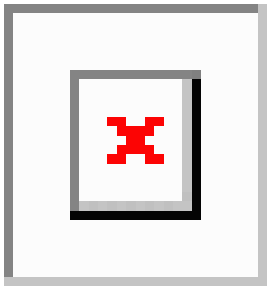
NAT에서는 일대일, 일대다, 소수대다수, 다수대소수, 다대일 등 모든 종류의 고정 매핑 시나리오를 유연하게 허용합니다. 그러나 일대일 또는 일대다 매핑만 사용하는 것이 좋습니다. 다른 매핑 옵션을 사용할 경우 예기치 않은 결과가 발생할 수 있습니다.

소수대다수는 기능상 일대다와 같지만, 구성이 좀 더 복잡하고 실제 매핑이 한눈에 명확히 파악되지 않을 수 있으므로 필요한 경우 각 실제 주소에 대해 일대다 구성을 만드는 것이 좋습니다. 소수대다수 시나리오에서는 소수의 실제 주소가 다수의 매핑된 주소로 순서대로 매핑됩니다(A-1, B-2, C-3).

모든 실제 주소가 매핑되면 다음의 매핑된 주소는 첫 번째 실제 주소로 매핑되며, 모든 매핑된 주소가 매핑될 때까지 같은 방식이 반복됩니다(A-4, B-5, C-6). 그 결과 각 실제 주소에 다수의 매핑된 주소가 연결됩니다. 일대다 구성의 경우와 마찬가지로 첫 번째 매핑만 양방향이고 이후 매핑에서는 실제 호스트로만 트래픽이 시작되고, 실제 호스트로부터의 모든 트래픽은 소스에 대해 첫 번째 매핑된 주소만 사용합니다.

다음 그림은 일반적인 소수대다수 고정 NAT 시나리오를 보여줍니다.

그림 ***11:*** 소수대다수 고정 ***NAT***

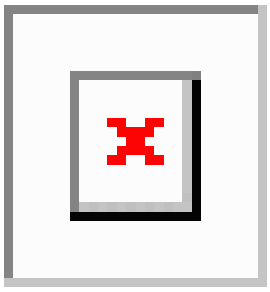


매핑된 주소보다 실제 주소가 더 많은 다수대소수 또는 다대일 컨피그레이션의 경우, 실제 주소가 소진되기 전에 매핑된 주소가 소진됩니다. 가장 낮은 실제 IP 주소와 매핑된 풀 간의 매핑만 양방향 시작이 가능합니다. 나머지 더 높은 실제 주소는 트래픽을 시작할 수 있지만 이러한 주소로 트래픽이 시작될 수는 없습니다. 연결에 대한 고유한 5튜플(소스/대상 IP 주소, 소스/대상 포트 및 프로토콜) 때문에 연결에 대한 반환 트래픽은 정확한 실제 주소로 전달됩니다.

참고 다수대소수 또는 다대일 NAT는 PAT가 아닙니다. 두 개의 실제 호스트가 동일한 소스 포트 번호를 사용하고 동일한 외부 서버 및 동일한 TCP 대상 포트로 이동하며 두 호스트가 동일한 IP 주소로 변환되면, 주소 충돌 때문에(5튜플이 고유하지 않음) 두 연결이 재설정됩니다.

다음 그림은 일반적인 다수대소수 고정 NAT 시나리오를 보여줍니다.

그림 ***12:*** 다수대소수 고정 ***NAT***



고정 규칙을 이 방식으로 사용하는 대신, 양방향 시작이 필요한 트래픽에 대해 일대일 규칙을 만든 다음 나머지 주소에 대해 동적 규칙을 만드는 방식을 권장합니다.

고정 자동 NAT 구성

고정 자동 NAT 규칙을 사용하여 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다. 또한 고정 NAT 규칙을 사용하여 포트 변환을 수행할 수도 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- **Translated Source(**변환된 소스**)** - 다음 옵션을 사용하여 변환된 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
  - 주소 - 호스트, 범위 또는 서브넷이 포함된 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**)** - **Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- 유형 - 고정을 선택합니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** **Translation(**변환**)**에서 탭에서 다음 옵션을 구성합니다.

- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 소스**(Translated Source)** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 **Address(**주소**)**를 선택하고 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
- (선택 사항). **Original Port(**원래 포트**)**, Translated Port(변환된 포트) - TCP 또는 UDP 포트를 변환해야 하는 경우 **Original Port(**원래 포트**)**에서 프로토콜을 선택하고 원래 및 변환된 포트 번호를 입력합니다. 예를 들어, 필요에 따라 TCP/80을 8080으로 변환할 수 있습니다.

단계 **6** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 -DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 104 페이지을 참조하십시오. 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.
- **Net to Net Mapping(**네트워크 대 네트워크 매핑**)**—NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째 IPv4 주소를 두 번째 IPv6 주소로 변환하는 방식을 사용하려면 이 옵션을 선택합니다. 이 옵션이 없으면 IPv4 포함 메서드가 사용됩니다. 일대일 변환에는 이 옵션을 사용해야 합니다.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **8** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

고정 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 고정 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 고정 NAT는 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다. 또한 고정 NAT 규칙을 사용하여 포트 변환을 수행할 수도 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- **Translated Source(**변환된 소스**)** - 다음 옵션을 사용하여 변환된 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
  - 주소 - 호스트, 범위 또는 서브넷이 포함된 네트워크 개체 또는 그룹을 생성합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.

규칙에서 원본 대상 및 변환된 대상에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다. 포트 변환 대상 고정 인터페이스 NAT만 구성하려면 대상 매핑된 주소에 대한 개체 추가를 건너뛰고 규칙에서 인터페이스를 지정할 수 있습니다.

소스나 대상 또는 둘 다에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 및 변환된 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**)** - **Manual NAT Rule(**수동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**)** - 고정을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.

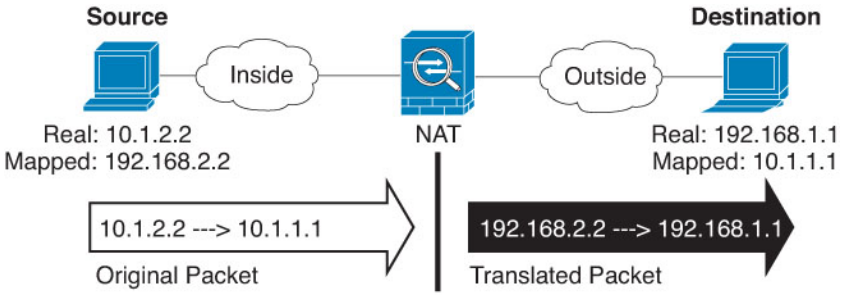
- **Enable(활성화)**—규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다.
- **Insert(삽입)**—규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.

단계 **4** **Interface Objects(인터페이스 개체)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(소스 인터페이스 개체)**, **Destination Interface Objects(대상 인터페이스 개체)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(소스)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(대상)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(모두)**)에 적용됩니다.

단계 **5** (변환 페이지에서) 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(원본 소스** - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Source Interface IP(소스 인터페이스 IP)를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스**(Translated Source)** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 **Address(주소)**를 선택하고 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(대상 인터페이스 IP)**를 선택합니다. 또한 특정 대상 interface object(인

터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.

- **Translated Destination(**변환된 대상**)** - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환의 원본 또는 대상 서비스 포트를 식별합니다.

포트 변환 고정 NAT를 구성하는 경우 소스나 대상 또는 둘 다에 대해 포트를 변환할 수 있습니다. 예를 들어 TCP/80과 TCP/8080 간에 변환할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

- 원본 소스 포트, 변환된 소스 포트 - 소스 주소에 대한 포트 변환을 정의합니다.
- 원본 대상 포트, 변환된 대상 포트 - 대상 주소에 대한 포트 변환을 정의합니다.

단계 **8** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 회신 변환 -DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 104 페이지을 참조하십시오. 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.
- **Net to Net Mapping(**네트워크 대 네트워크 매핑**)**—NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째 IPv4 주소를 두 번째 IPv6 주소로 변환하는 방식을 사용하려면 이 옵션을 선택합니다. 이 옵션이 없으면 IPv4 포함 메서드가 사용됩니다. 일대일 변환에는 이 옵션을 사용해야 합니다.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.
- **Unidirectional(**단방향**)**—대상 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 이 옵션을 선택합니다. 단방향 옵션은 주로 테스트 용으로 유용하며 모든 프로토콜에서 작동하지 않을 수 있습니다. 예를 들어, NAT를 사용하여 SIP 헤더를 변환하려면 SIP에 프로토콜 검사가 필요하지만 변환을 단방향으로 설정하는 경우에는 이러한 검사가 수행되지 않습니다.

단계 **9** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

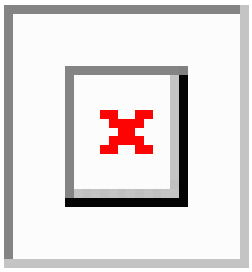
단계 **10** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

ID NAT

IP 주소를 자신으로 변환해야 하는 NAT 구성이 있을 수 있습니다. 예를 들어 NAT를 모든 네트워크에 적용하는 광범위한 규칙을 만들되 NAT에서 하나의 네트워크만 제외하고 싶은 경우, 주소를 자신으로 변환하는 고정 NAT 규칙을 만들 수 있습니다.

다음 그림은 일반적인 ID NAT 시나리오를 보여줍니다.

그림 ***13: ID NAT***



다음 주제에서는 ID NAT를 구성하는 방법을 설명합니다.

ID 자동 NAT 구성

주소 변환을 방지하려면 고정 ID 자동 NAT 규칙을 사용합니다. 이 경우 주소가 자체로 변환됩니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이는 그룹이 아닌 네트워크 개체여야 하며 호스트, 범위 또는 서브넷일 수 있습니다.
- **Translated Source(**변환된 소스**)** - 원본 소스 개체와 내용이 정확히 동일한 네트워크 개체 또는 그룹입니다. 동일한 개체를 사용할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- 유형 - 고정을 선택합니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** **Translation(**변환**)**에서 탭에서 다음 옵션을 구성합니다.

- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체입니다.
- **Translated Source(**변환된 소스**)** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

ID NAT의 경우에는 원본 포트 및 변환된 포트 옵션을 구성하지 마십시오.

단계 **6** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 응답 변환 - ID NAT의 경우에는 이 옵션을 구성하지 마십시오.
- **IPv6** - ID NAT에 이 옵션을 구성하지 마십시오.
- **Net to Net Mapping(**네트워크 대 네트워크 매핑**)** - ID NAT에 이 옵션을 구성하지 마십시오.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.
- 대상 인터페이스에 대해 경로 조회 수행 - 원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **8** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

ID 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 고정 ID 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 주소 변환을 방지하려면 고정 ID NAT 규칙을 사용합니다. 이 경우 주소가 자체로 변환됩니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- **Original Source(**원본 소스**)** - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 **Any(**모두**)**를 지정하면 됩니다.
- **Translated Source(**변환된 소스**)** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

규칙에서 원본 대상 및 변환된 대상에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다. 포트 변환 대상 고정 인터페이스 NAT만 구성하려면 대상 매핑된 주소에 대한 개체 추가를 건너뛰고 규칙에서 인터페이스를 지정할 수 있습니다.

소스나 대상 또는 둘 다에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 및 변환된 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. ID NAT에 대해 동일한 개체를 사용할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)** 버튼을 클릭하여 새 규칙을 생성합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

오른쪽 클릭 메뉴에는 규칙 잘라내기, 복사, 붙여넣기, 삽입, 삭제 옵션도 있습니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

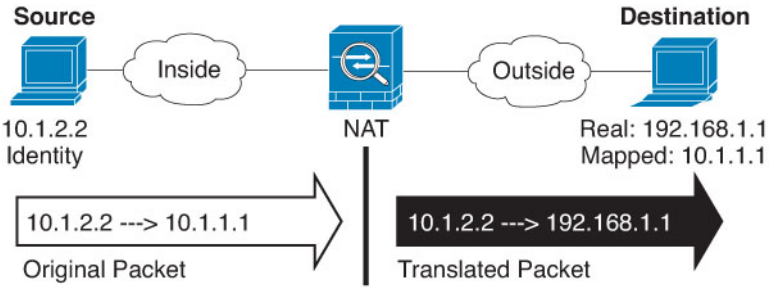
- **NAT Rule(NAT** 규칙**)** - **Manual NAT Rule(**수동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**)** - 고정을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대해 변환을 정의하는 경우 변환은 항상 고정입니다.
- **Enable(**활성화**)**—규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다.
- **Insert(**삽입**)**—규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.

단계 **4** **Interface Objects(**인터페이스 개체**)**에서 다음 옵션을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)**, **Destination Interface Objects(**대상 인터페이스 개체**)**—(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다.

원래 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오. 여기서 내부 호스트에 대해서는 ID NAT를 수행하지만 외부 호스트는 변환합니다.



- **Original Source(**원본 소스**)** - 변환하는 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination(**원본 대상**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Interface Object(인터페이스 개체**)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- **Translated Source(**변환된 소스**)** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.
- **Translated Destination(**변환된 대상**)** - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환의 원본 또는 대상 서비스 포트를 식별합니다.

포트 변환 고정 NAT를 구성하는 경우 소스나 대상 또는 둘 다에 대해 포트를 변환할 수 있습니다. 예를 들어 TCP/80과 TCP/8080 간에 변환할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

- 원본 소스 포트, 변환된 소스 포트 - 소스 주소에 대한 포트 변환을 정의합니다.
- 원본 대상 포트, 변환된 대상 포트 - 대상 주소에 대한 포트 변환을 정의합니다.

단계 **8** (선택 사항). **Advanced(**고급**)**에서 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 응답 변환 - ID NAT의 경우에는 이 옵션을 구성하지 마십시오.
- **IPv6**—인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.
- 대상 인터페이스에서 **ARP** 프록시 설정 안 함 - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.
- 대상 인터페이스에 대해 경로 조회 수행 - 원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.
- **Unidirectional(**단방향**)**—대상 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 이 옵션을 선택합니다. 단방향 옵션은 주로 테스트 용으로 유용하며 모든 프로토콜에서 작동하지 않을 수 있습니다. 예를 들어, NAT를 사용하여 SIP 헤더를 변환하려면 SIP에 프로토콜 검사가 필요하지만 변환을 단방향으로 설정하는 경우에는 이러한 검사가 수행되지 않습니다.

단계 **9** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **10** 변경 사항을 저장하려면 NAT 페이지에서 **Save(**저장**)**를 클릭합니다.

Firepower Threat Defense의 NAT 규칙 속성

NAT(네트워크 주소 변환) 규칙을 사용하여 IP 주소를 다른 IP 주소로 변환합니다. 일반적으로는 NAT 규칙을 사용하여 전용 어드레스를 공개적으로 라우팅 가능한 주소로 변환합니다. 변환을 주소 간에 수행할 수도 있고, PAT(포트 주소 변환)를 사용해 여러 주소를 하나 또는 소수의 주소로 변환하고 포트 번호를 사용해 각 소스 주소를 구분할 수도 있습니다.

NAT 규칙은 다음 기본 속성을 포함합니다. 이러한 속성은 별도로 명시된 경우를 제외하면 자동 NAT 및 수동 NAT 규칙에 대해 동일합니다.

NAT 유형

수동 **NAT** 규칙 또는 자동 **NAT** 규칙을 구성할 것인지 여부입니다. 자동 NAT는 원본 주소만 변환하므로 대상 주소를 기반으로 다른 번환을 수행할 수 없습니다. 자동 NAT는 구성하기가 더 쉽기 때문에 수동 NAT의 추가 기능이 필요하지 않는 한 자동 NAT를 사용하십시오. 차이점에 대한 자세한 내용은 자동 NAT 및 수동 NAT, 5 페이지 섹션을 참고하십시오.

유형

변환 규칙이 동적인지 아니면 정적인지를 나타냅니다. 동적 변환에서는 주소 풀에서 매핑된 주소를 자동으로 선택하며, PAT를 구현할 때는 주소/포트 조합을 선택합니다. 매핑된 주소/포트를 정확하게 정의하려면 정적 변환을 사용하십시오.

Enable(활성화**)(**수동 **NAT**만 해당**)**

규칙을 활성화할지 여부를 선택합니다. 규칙 페이지에서 오른쪽 클릭 메뉴를 사용하여 나중에 규칙을 활성화하거나 비활성화할 수 있습니다. 자동 NAT 규칙을 비활성화할 수 없습니다.

Insert(삽입**)(**수동 **NAT**만 해당**)**

규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 지정한 규칙 번호 위나 아래에 삽입할 수도 있습니다.

Description(설명**)(**선택 사항**,** 수동 **NAT**만 해당**)**

규칙의 목적에 대한 설명입니다.

다음 주제에서는 나머지 NAT 규칙 속성 탭에 대해 설명합니다.

인터페이스 개체 **NAT** 속성

NAT 규칙이 적용되는 인터페이스를 정의하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. 라우팅된 모드에서는 소스와 대상 모두에 대해 기본 "임의" 개념을 사용하여 할당된 모든 디바이스의 모든 인터페이스에 적용할 수 있습니다. 하지만 일반적으로 특정 소스 및 대상 인터페이스를 선택하고자 합니다.

참고 브리지 그룹 멤버 인터페이스에는 "임의" 인터페이스라는 개념이 적용되지 않습니다. "any" 인터페이스를 지정하면 모든 브리지 그룹 멤버 인터페이스는 제외됩니다. 따라서 브리지 그룹 멤버에 NAT를 적용하려면 멤버 인터페이스를 지정해야 합니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT를 구성할 수 없으며 멤버 인터페이스에 대해서만 NAT를 구성할 수 있습니다.

인터페이스 개체를 선택한 경우 디바이스에 선택한 모든 개체에 인터페이스가 있는 경우에만 할당된 디바이스에 NAT 규칙이 구성됩니다. 예를 들어 원본 및 대상 보안 영역을 모두 선택하면 두 영역 모두 특정 디바이스에 대한 하나 이상의 인터페이스를 포함해야 합니다.

Source Interface Objects(소스 인터페이스 개체**), Destination Interface Objects(**대상 인터페이스 개체**)**

(브리지 그룹 멤버 인터페이스의 경우 필수) 이 NAT 규칙이 적용되는 인터페이스를 식별하는 인터페이스 개체(보안 영역 또는 인터페이스 그룹)입니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스가 포함된 개체입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스가 포함된 개체입니다. 기본적으로 규칙은 브리지 그룹 멤버 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

자동 NAT에 대한 Translation 속성

Translation(변환**)**의 옵션을 사용하여 소스 주소와 매핑된 변환 주소를 정의합니다. 다음 속성은 자동 NAT에만 적용됩니다.

원본 소스**(**항상 필수**)**

변환 중인 주소를 포함하는 네트워크 개체입니다. 그룹이 아닌 네트워크 개체여야 하며, 호스트, 범위 또는 서브넷일 수 있습니다.

시스템 정의 any-ipv4 또는 any-ipv6 개체에 대해서는 자동 NAT 규칙을 생성할 수 없습니다.

변환된 소스**(**대개 필수**)**

원본 주소를 변환하는 매핑된 주소입니다. 여기서 선택하는 항목에 따라 정의하는 변환 규칙의 유형이 달라집니다.

- 동적 **NAT** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.
- 동적 **PAT** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. PAT 풀을 구성하지 마십시오.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다. PAT 풀을 구성하지 마십시오.
  - PAT 풀을 사용하려면 변환된 소스**(Translated Source)** 를 비워 둡니다. **PAT Pool(PAT** 풀**)**에서 PAT 풀 개체를 선택합니다.
- 고정 **NAT** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 **Address(**주소**)**를 선택하고 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 개체 또는 그룹은 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)** 탭에서 **IPv6** 옵션을 선택해야 합니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
- **ID NAT** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

원본 포트, 변환된 포트(고정 NAT에만 해당됨)

TCP 또는 UDP 포트를 변환해야 하는 경우 **Original Port(**원래 포트**)**에서 프로토콜을 선택하고 원래 및 변환된 포트 번호를 입력합니다. 예를 들어, 필요에 따라 TCP/80을 8080으로 변환할 수 있습니다. ID NAT에 이 옵션을 구성하지 마십시오.

수동 NAT에 대한 Translation 속성

Translation(변환**)**의 옵션을 사용하여 소스 주소와 매핑된 변환 주소를 정의합니다. 다음 속성은 수동 NAT에만 적용됩니다. 별도로 표시된 항목을 제외한 모든 항목은 선택 사항입니다.

원본 소스(항상 필수)

변환 중인 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있으며, 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 규칙에서 임의를 지정하면 됩니다.

변환된 소스(대개 필수)

원본 주소를 변환하는 매핑된 주소입니다. 여기서 선택하는 항목에 따라 정의하는 변환 규칙의 유형이 달라집니다.

- 동적 **NAT** - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 그룹에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안으로 사용됩니다.
- 동적 **PAT** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)**에서 **IPv6** 옵션을 선택해야 합니다. PAT 풀을 구성하지 마십시오.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다. PAT 풀을 구성하지 마십시오.
  - PAT 풀을 사용하려면 변환된 소스**(Translated Source)** 를 비워 둡니다. **PAT Pool(PAT** 풀**)**에서 PAT 풀 개체를 선택합니다.
- 고정 **NAT** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 **Address(**주소**)**를 선택하고 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 개체 또는 그룹은 호스트, 범위 또는 서브넷을 포함할 수 있습니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 **Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다. 또한 특정 대상 interface object(인터페이스 개체)를 선택해야 합니다. 인터페이스의 IPv6 주소를 사용하려면 **Advanced(**고급**)** 탭에서 **IPv6** 옵션을 선택해야 합니다. 이 경우 포트 변환 고정 인터페

이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.

- **ID NAT** - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

Original Destination(원본 대상**)**

대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

Source Interface IP(소스 인터페이스 **IP)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

Translated Destination(변환된 대상**)**

변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

원본 소스 포트, 변환된 소스 포트, 원본 대상 포트, 변환된 대상 포트

원본 및 변환된 패킷의 소스 및 대상 서비스를 정의하는 포트 개체입니다. 포트를 변환할 수도 있고, 동일한 개체를 선택하여 포트를 변환하지 않고 규칙이 서비스에 따라 달라지도록 설정할 수도 있습니다. 서비스를 구성할 때는 다음 규칙에 유의하십시오.

- (동적 NAT 또는 PAT) 원본 소스 포트 및 변환된 소스 포트에 대해서는 변환을 수행할 수 없습니다. 대상 포트에 대해서만 변환을 수행할 수 있습니다.
- NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

PAT 풀 NAT 속성

동적 NAT를 구성할 때 **PAT Pool(PAT** 풀**)** 탭의 등록 정보를 사용하여 포트 주소 변환에 사용할 주소 풀을 정의할 수 있습니다.

Enable PAT Pool(PAT 풀 활성화**)**

Pat 풀의 주소를 구성하려면 이 옵션을 선택합니다.

PAT

PAT 풀에 사용할 주소이며 다음 중 하나입니다.

- **Address(**주소**)** - 범위를 포함하는 네트워크 개체 또는 호스트, 범위 또는 둘 다를 포함하는 네트워크 개체 그룹 중 하나인 PAT 풀 주소를 정의하는 개체입니다 서브넷을 포함할 수 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.

- **Destination Interface IP(**대상 인터페이스 **IP)** - 대상 인터페이스를 PAT 주소로 사용하려고 하는 것을 나타냅니다. 이 옵션의 경우 특정 **Destination Interface Object(**대상 인터페이스 개체**)** 인터페이스 개체를 선택해야 합니다. 대상 인터페이스로 **Any**를 사용할 수 없습니다. 이는 인터페이스 PAT를 구현하는 또 다른 방법입니다.

라운드 로빈

라운드 로빈 방식으로 주소/포트를 할당하려는 경우 선택합니다. 기본적으로, 라운드 로빈이 아니면 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다.

확장된 **PAT** 테이블

확장 PAT를 사용하려는 경우 선택합니다. 확장 PAT는 변환 정보의 대상 주소 및 포트를 포함하여 서비스당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 대상 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다. 이 옵션은 인터페이스 PAT 또는 인터페이스 PAT 대체와 함께 사용할 수 없습니다.

Flat Port Range, Include Reserved Ports

TCP/UDP 포트를 할당할 때 단일 균일 범위로 1024~65535 포트 범위를 사용하려는 경우 선택합니다. (6.7 버전 이전) 변환할 매핑된 포트 번호를 선택하면 PAT에서는 실제 소스 포트 번호(사용 가능한 경우)를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 없는 경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **Include Reserved Ports(**예약된 포트 포함**)** 옵션도 선택합니다. 버전 6.7 이상을 실행하는 FTD 디바이스의 경우 옵션 선택 여부에 관계없이 플랫 포트 범위가 항상 구성됩니다. 이러한 시스템에 대해 **Include Reserved Ports(**예약 포트 포함**)** 옵션을 여전히 선택할 수 있으며 해당 설정이 적용됩니다.

할당 차단

포트 블록 할당을 활성화하려는 경우 선택합니다. 캐리어급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다. 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한 활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 포트 블록은 1024~65535 범위에서만 할당됩니다. 포트 블록 할당은 라운드 로빈과는 호환되지만 확장 PAT 또는 플랫 포트 범위 옵션과 함께 사용할 수는 없습니다. 또한 인터페이스 PAT 대체를 사용할 수 없습니다.

고급 **NAT** 속성

NAT를 구성할 때는 고급 옵션에서 특수 서비스를 제공하는 속성을 구성할 수 있습니다. 이러한 모든 속성은 선택 사항이므로 서비스가 필요할 때만 구성하면 됩니다.

이 규칙과 일치하는 **DNS** 응답 변환

DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 104 페이지을 참조하십시오. 정적 NAT 규칙에서 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.

인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**(**동적 **NAT**만 해당됨**)**

다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스의 IPv6 주소를 사용하려면 **IPv6** 옵션도 선택합니다. 인터페이스 PAT를 변환된 주소로 이미 컨피그레이션한 경우에는 이 옵션을 선택할 수 없습니다. 또한, PAT 풀을 구성하는 경우 이 옵션을 선택할 수 없습니다.

IPv6

인터페이스 PAT에 대해 대상 인터페이스의 IPv6 주소를 사용할지 여부를 선택합니다.

네트워크 대 네트워크 매핑**(**고정 **NAT**만 해당됨**)**

NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째 IPv4 주소를 두 번째 IPv6 주소로 변환하는 방식을 사용하려면 이 옵션을 선택합니다. 이 옵션이 없으면 IPv4 포함 메서드가 사용됩니다. 일대일 변환에는 이 옵션을 사용해야 합니다.

대상 인터페이스에서 **ARP** 프록시 설정 안 함**(**고정 **NAT**만 해당됨**)**

매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

대상 인터페이스에 대해 경로 조회 수행**(**고정 **ID NAT** 및 라우팅 모드만 해당됨**)**

원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

단방향**(**수동 **NAT** 및 고정 **NAT**만 해당됨**)**

대상 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 이 옵션을 선택합니다. 단방향 옵션은 주로 테스트 용으로 유용하며 모든 프로토콜에서 작동하지 않을 수 있습니다. 예를 들어, NAT를 사용하여 SIP 헤더를 변환하려면 SIP에 프로토콜 검사가 필요하지만 변환을 단방향으로 설정하는 경우에는 이러한 검사가 수행되지 않습니다.

IPv6 네트워크 변환

IPv6 전용 및 IPv4 전용 네트워크 간에 트래픽을 전달해야 하는 경우에는 NAT를 사용해 주소 유형을 변환해야 합니다. 두 IPv6 네트워크 간에 트래픽을 전달할 때도 외부 네트워크에서 내부 네트워크를 숨기려는 경우가 있습니다.

IPv6 네트워크에서는 다음 변환 유형을 사용할 수 있습니다.

- NAT64, NAT46 - IPv6 패킷에서 IPv4 패킷으로, 또는 그 반대로 변환합니다. 이 경우 두 개의 정책(IPv6에서 IPv4로의 변환 정책과 IPv4에서 IPv6으로의 변환 정책)을 정의해야 합니다. 단일 수동 NAT 규칙을 사용하여 정책 2개를 정의할 수는 있지만, DNS 서버가 외부 네트워크에 있는 경우에는 DNS 응답을 재작성해야 할 수도 있습니다. 대상을 지정할 때는 수동 NAT 규칙에 대해 DNS 재작성을 활성화할 수 없으므로 자동 NAT 규칙 2개를 생성하는 것이 더 나은 해결책입니다.

  참고 NAT46은 정적 매핑만 지원합니다.

- NAT66 - IPv6 패킷을 다른 IPv6 주소로 변환합니다. 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다.

참고 NAT64 및 NAT 46은 표준 라우팅 인터페이스에서만 사용할 수 있습니다. NAT66은 라우팅 인터페이스 및 브리지 그룹 멤버 인터페이스에서 모두 사용 가능합니다.

NAT64/46: IPv6 주소를 IPv4로 변환

트래픽이 IPv6 네트워크에서 IPv4 전용 네트워크로 이동하는 경우에는 IPv6 주소를 IPv4로 변환해야 하며, 반환 트래픽은 IPv4에서 IPv6으로 변환해야 합니다. 따라서 주소 풀 2개(IPv4 네트워크에서 IPv6 주소를 바인딩하기 위한 IPv4 주소 풀과 IPv6 네트워크에서 IPv4 주소를 바인딩하기 위한 IPv6 주소 풀)를 정의해야 합니다.

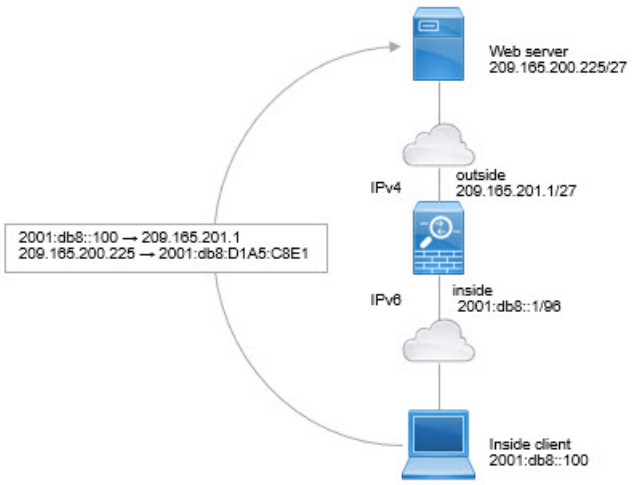
- NAT64 규칙용 IPv4 주소 풀은 일반적으로 크기가 작으므로 대개 IPv6 클라이언트 주소와 일대일로 매핑할 주소를 충분히 포함하지 않을 수 있습니다. 동적 PAT의 경우 동적 또는 고정 NAT에 비해 더 쉽게 많은 IPv6 클라이언트 주소를 포함할 수 있습니다.
- NAT46 규칙용 IPv6 주소 풀은 매핑할 IPv4 주소보다 많은 수의 주소를 포함할 수 있습니다. 따라서 각 IPv4 주소를 서로 다른 IPv6 주소에 매핑할 수 있습니다. NAT46은 고정 매핑만 지원하므로 동적 PAT는 사용할 수 없습니다.

소스 IPv6 네트워크와 대상 IPv4 네트워크 중에 하나씩 2개의 정책을 정의해야 합니다. 단일 수동 NAT 규칙을 사용하여 정책 2개를 정의할 수는 있지만, DNS 서버가 외부 네트워크에 있는 경우에는 DNS

응답을 재작성해야 할 수도 있습니다. 대상을 지정할 때는 수동 NAT 규칙에 대해 DNS 재작성을 활성화할 수 없으므로 자동 NAT 규칙 2개를 생성하는 것이 더 나은 해결책입니다.

NAT64/46 예: 내부 IPv6 네트워크 및 외부 IPv4 인터넷

다음은 내부 IPv6 전용 네트워크를 보유하고 있으며 인터넷으로 전송된 트래픽에 대해 IPv4로 변환하려는 경우의 간단한 예입니다. 이 예에서는 DNS 변환이 필요하지 않다고 가정하므로 단일 수동 NAT 규칙에서 NAT64 및 NAT46 변환을 모두 수행할 수 있습니다.



이 예에서는 외부 인터페이스의 IP 주소가 포함된 동적 인터페이스 PAT를 사용하여 내부 IPv6 네트워크를 IPv4로 변환합니다. 외부 IPv4 트래픽은 2001:db8::/96 네트워크의 주소로 정적 변환되어 내부 네트워크에서 전송을 허용합니다.

프로시저

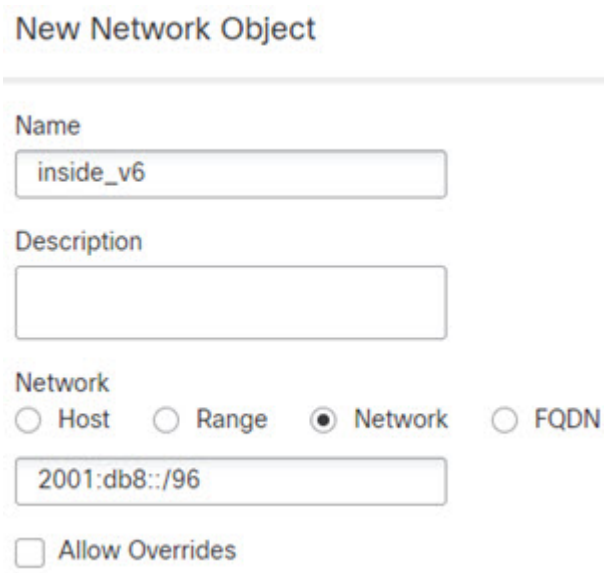
단계 **1** 내부 IPv6 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.

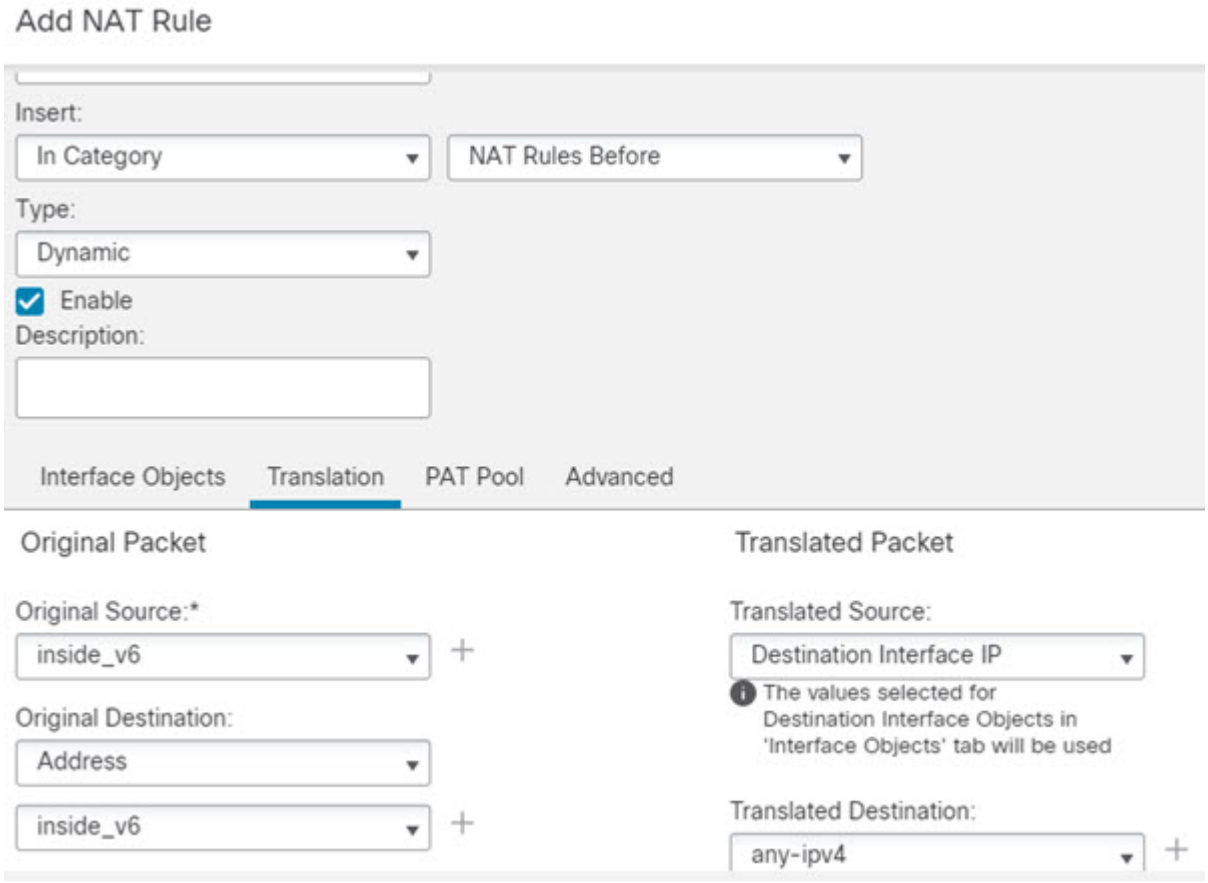
네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:db8::/96을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

단계 **2** 수동 NAT 규칙을 생성하여 IPv6 네트워크를 IPv4로 변환한 후 다시 되돌립니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.
b) **Add Rule(**규칙 추가**)**을 클릭합니다.
c) 다음 속성을 구성합니다.
   - **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
   - 유형 = 동적
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.
   - **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
   - **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.
e) **Translation(**변환**)**에서 다음을 구성합니다.
   - **Original Source(**원본 소스**)** = inside_v6 네트워크 개체.
   - **Translated Source(**변환된 소스**)** = **Destination Interface IP(**대상 인터페이스 **IP)**
   - **Original Destination(**원본 대상**)** = inside_v6 네트워크 개체
   - **Translated Destination(**변환된 대상**)** = any-ipv4 네트워크 개체



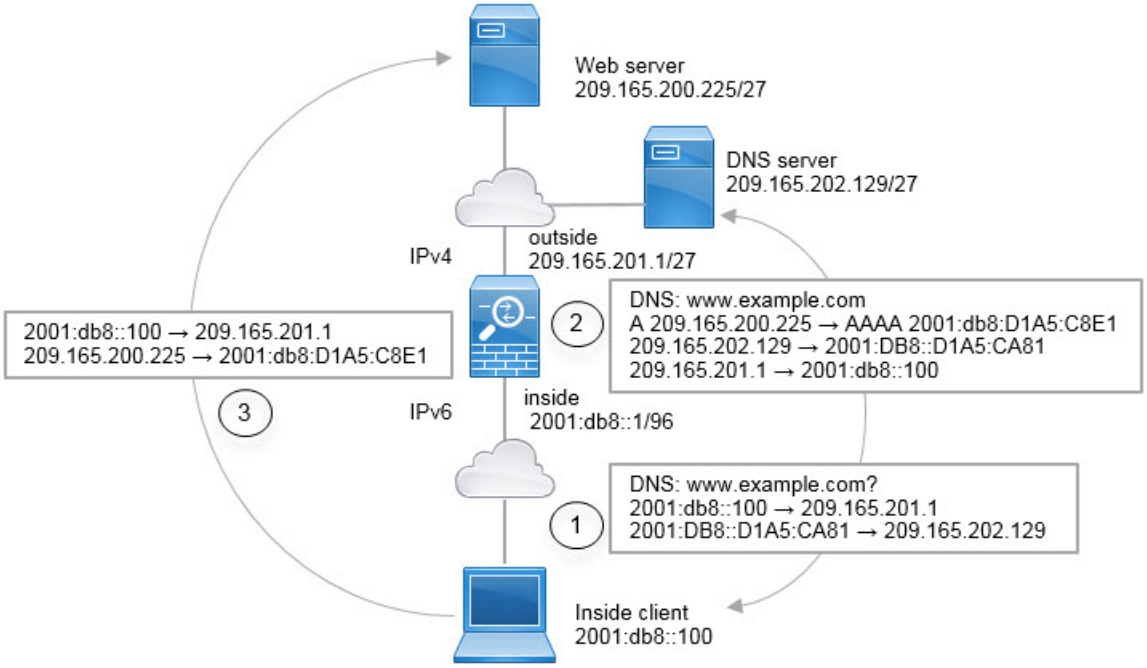
f) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 외부 인터페이스의 IPv4 주소를 사용하여 NAT64 PAT로 변환됩니다. 반대로 외부 네트워크에서 내부 인터페이스로 들어오는 모든 IPv4 주소는 임베디드 IPv4 주소 메서드를 사용하여 2001:db8::/96 네트워크의 주소로 변환됩니다.

g) NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

NAT64/46 예: 내부 IPv6 네트워크와 외부 IPv4 인터넷 및 DNS 변환

아래에는 내부 IPv6 전용 네트워크가 있는데 내부 사용자에게 필요한 일부 IPv4 전용 서비스는 외부 인터넷에 있는 일반적인 예가 나와 있습니다.



이 예에서는 외부 인터페이스의 IP 주소가 포함된 동적 인터페이스 PAT를 사용하여 내부 IPv6 네트워크를 IPv4로 변환합니다. 외부 IPv4 트래픽은 2001:db8::/96 네트워크의 주소로 정적 변환되어 내부 네트워크에서 전송을 허용합니다. 외부 DNS 서버의 회신을 A(IPv4) 레코드에서 AAAA(IPv6) 레코드로 변환하고 주소를 IPv4에서 IPv6으로 변환할 수 있도록 NAT46 규칙에 대해 DNS 재작성을 활성화합니다.

내부 IPv6 네트워크의 2001:DB8::100에 있는 클라이언트가 www.example.com을 열려고 하는 웹 요청의 일반적인 순서는 다음과 같습니다.

1. 클라이언트의 컴퓨터가 2001:DB8::D1A5:CA81에 있는 DNS 서버에 DNS 요청을 보냅니다. NAT 규칙이 DNS 요청에서 소스 및 대상을 다음과 같이 변환합니다.
   - 2001:DB8::100을 209.165.201.1의 고유 포트로 변환합니다(NAT64 인터페이스 PAT 규칙).
   - 2001:DB8::D1A5:CA81을 209.165.202.129로 변환합니다(NAT46 규칙. D1A5:CA81은 209.165.202.129에 해당하는 IPv6 주소입니다.).
2. DNS 서버가 www.example.com이 209.165.200.225에 있음을 나타내는 A 레코드로 응답합니다. DNS 재작성이 활성화된 NAT46 규칙이 A 레코드를 IPv6의 동일 AAAA 레코드로 변환하고 AAAA 레코드의 209.165.200.225를 2001:db8:D1A5:C8E1로 변환합니다. 또한 DNS 응답의 소스 및 대상 주소는 변환되지 않은 상태입니다.
   - 209.165.202.129 -> 2001:DB8::D1A5:CA81
   - 209.165.201.1 -> 2001:db8::100
3. 이제 IPv6 클라이언트는 웹 서버의 IP 주소를 포함하며 2001:db8:D1A5:C8E1의 www.example.com에 대한 HTTP 요청을 수행합니다. D1A5:C8E1은 209.165.200.225에 해당하는 IPv6 주소입니다. 그리고 HTTP 요청의 소스 및 대상이 변환됩니다.

- 2001:DB8::100을 209.156.101.54의 고유 포트로 변환합니다(NAT64 인터페이스 PAT 규칙).
- 2001:db8:D1A5:C8E1을 209.165.200.225로 변환합니다(NAT46 규칙).

다음 절차에서는 이 예를 구성하는 방법을 설명합니다.

시작하기 전에

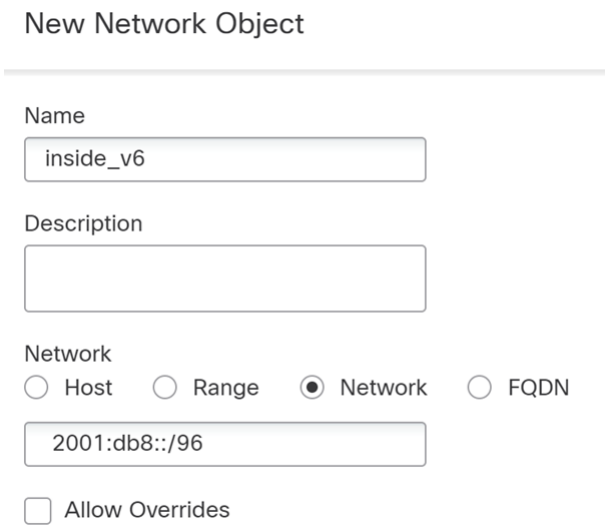
디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 내부 IPv6 및 외부 IPv4 네트워크를 정의하는 네트워크 개체를 생성합니다.

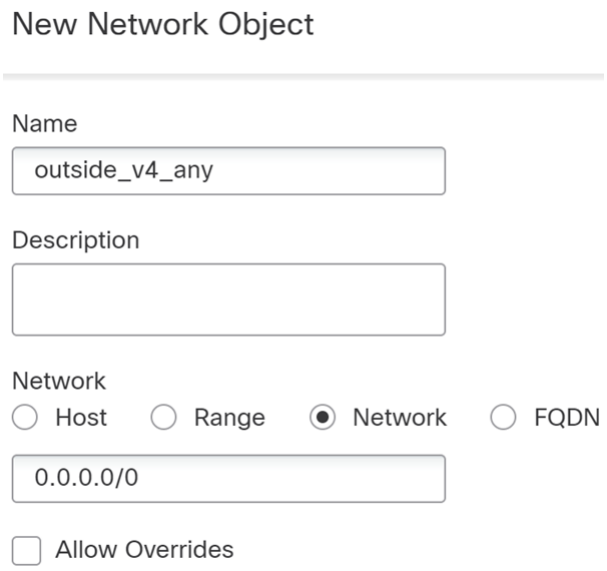
a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 내부 IPv6 네트워크를 정의합니다.

네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:db8::/96을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.
e) **Add Network(**추가 네트워크**)** > **Add Object(**개체 추가**)**를 클릭하고 외부 IPv4 네트워크를 정의합니다.

네트워크 개체의 이름을 outside_v4_any와 같이 지정하고 네트워크 주소 0.0.0.0/0을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 IPv6 네트워크용 NAT64 동적 PAT 규칙을 구성합니다.

단계 **3** 외부 IPv4 네트워크용 고정 NAT46 규칙을 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

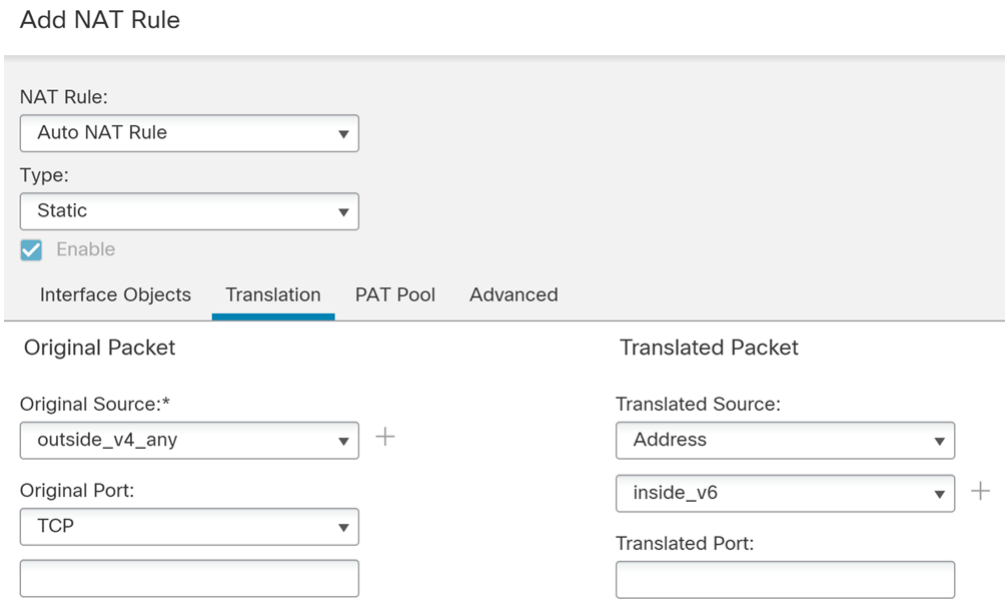
c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = outside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = outside_v4_any 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = inside_v6 네트워크 개체.

e) **Advanced(**고급**)**에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



f) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 외부 네트워크에서 내부 인터페이스로 들어오는 모든 IPv4 주소는 임베디드 IPv4 주소 방법을 사용하여 2001:db8::/96 네트워크의 주소로 변환됩니다. 또한 DNS 응답은 A(IPv4) 레코드에서 AAAA(IPv6) 레코드로 변환되며 주소는 IPv4에서 IPv6으로 변환됩니다.

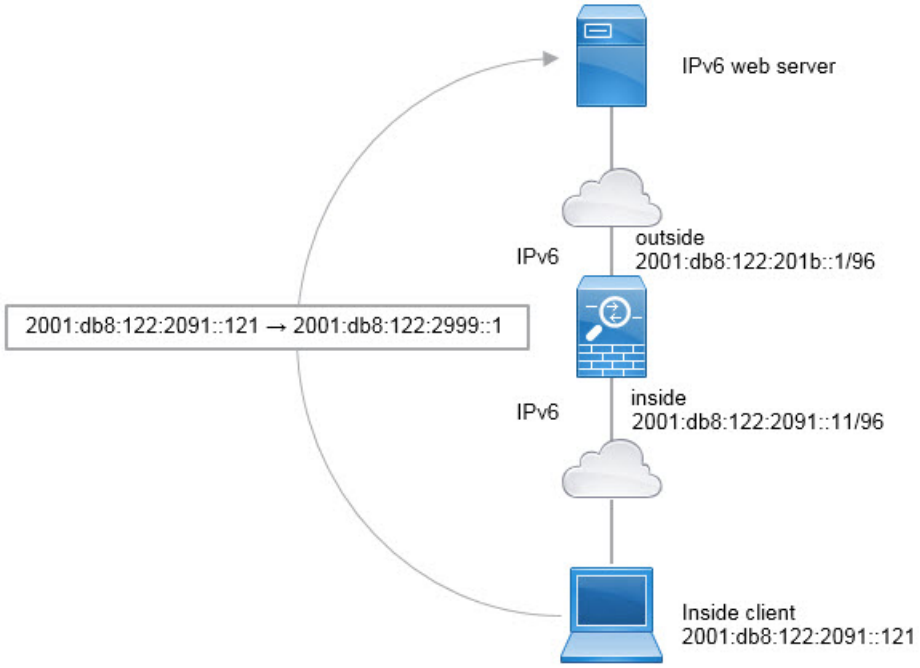
NAT66: IPv6 주소를 다른 IPv6 주소로 변환

IPv6 네트워크 간을 이동할 때는 주소를 외부 네트워크의 다른 IPv6 주소로 변환할 수 있습니다. 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다.

서로 다른 주소 유형 간을 변환하는 것이 아니므로 NAT66 변환을 위한 규칙 하나만 있으면 됩니다. 자동 NAT를 사용하면 이러한 규칙을 쉽게 모델링할 수 있습니다. 그러나 반환 트래픽을 허용하지 않으려면 수동 NAT만 사용해 정적 NAT 규칙을 단방향으로 설정할 수 있습니다.

NAT66 예, 네트워크 간의 고정 변환

자동 NAT를 사용하여 IPv6 주소 풀 간의 고정 변환을 컨피그레이션할 수 있습니다. 다음 예에서는 2001:db8:122:2091::/96 네트워크의 내부 주소를 2001:db8:122:2999::/96 네트워크의 외부 주소로 변환하는 방법을 설명합니다.



시작하기 전에

디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

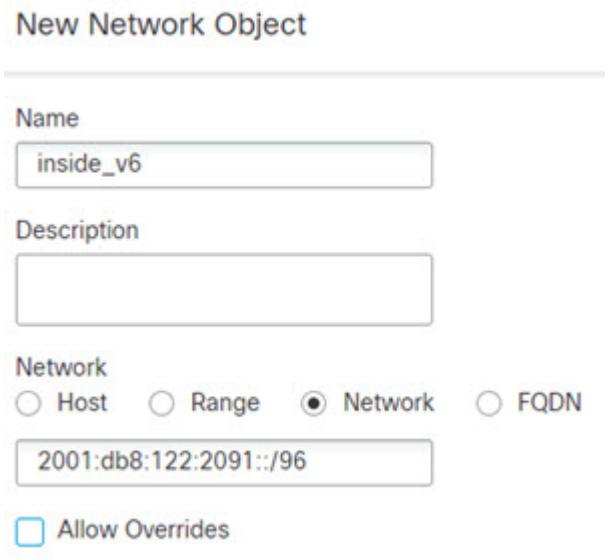
단계 **1** 내부 IPv6 및 외부 IPv6 NAT 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.

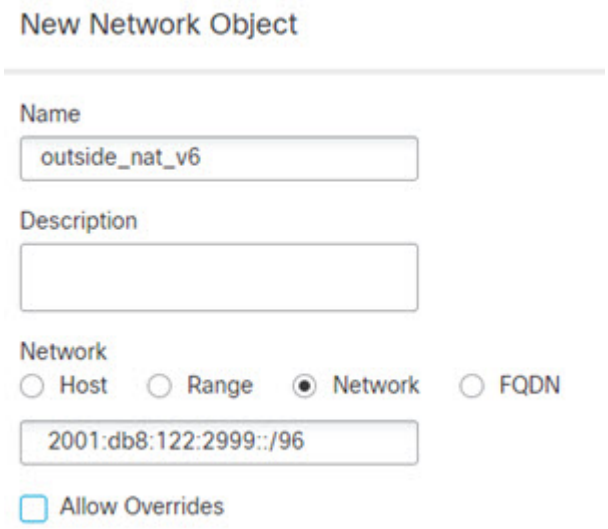
네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:db8:122:2091::/96을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 외부 IPv6 NAT 네트워크를 정의합니다.

네트워크 개체의 이름을 outside_nat_v6과 같이 지정하고 네트워크 주소 2001:db8:122:2999::/96을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 IPv6 네트워크용 고정 NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.

- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = inside_v6 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = outside_nat_v6 네트워크 개체.

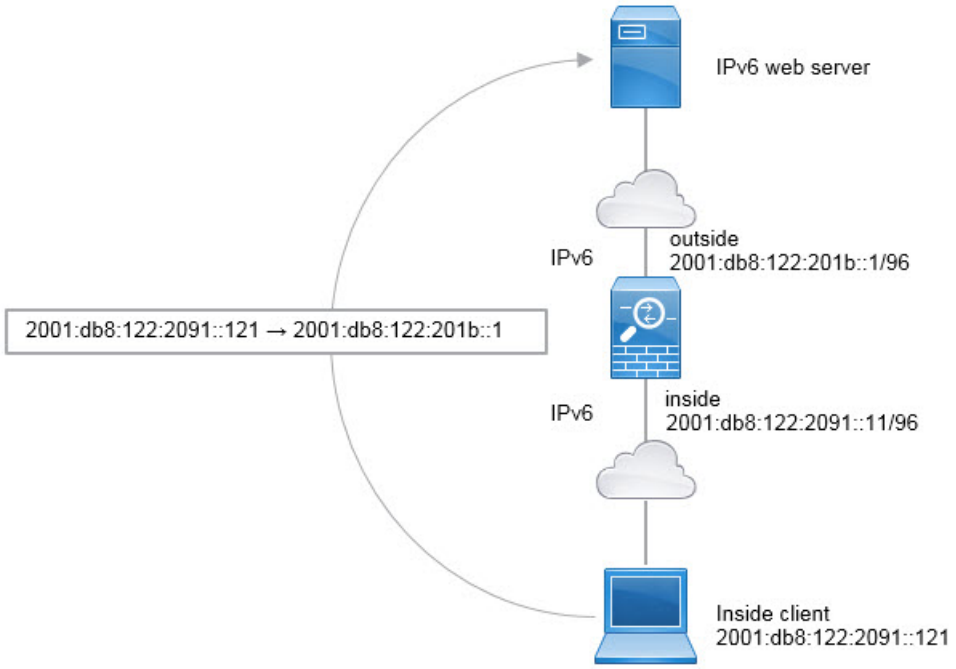
f) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8:122:2091::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 2001:db8:122:2999::/96 네트워크의 주소로 고정 NAT66 변환됩니다.

NAT66 예, 간단한 IPv6 인터페이스 PAT

NAT66을 구현하는 단순한 방식은 내부 주소를 외부 인터페이스 IPv6 주소의 각기 다른 포트에 동적으로 할당하는 것입니다.

NAT66용 인터페이스 PAT 규칙을 구성할 때는 해당 인터페이스에 구성되어 있는 모든 글로벌 주소가 PAT 매핑에 사용됩니다. 인터페이스에 대한 링크-로컬 또는 사이트-로컬 주소는 PAT에 사용되지 않습니다.



시작하기 전에

디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

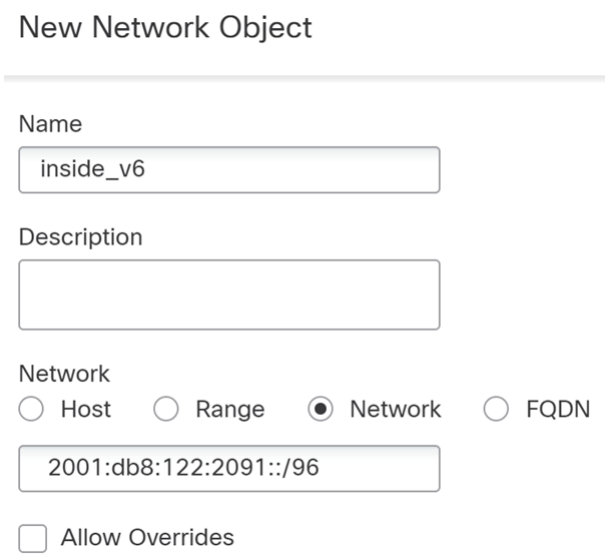
단계 **1** 내부 IPv6 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.

네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:db8:122:2091::/96을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 IPv6 네트워크용 동적 PAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 동적

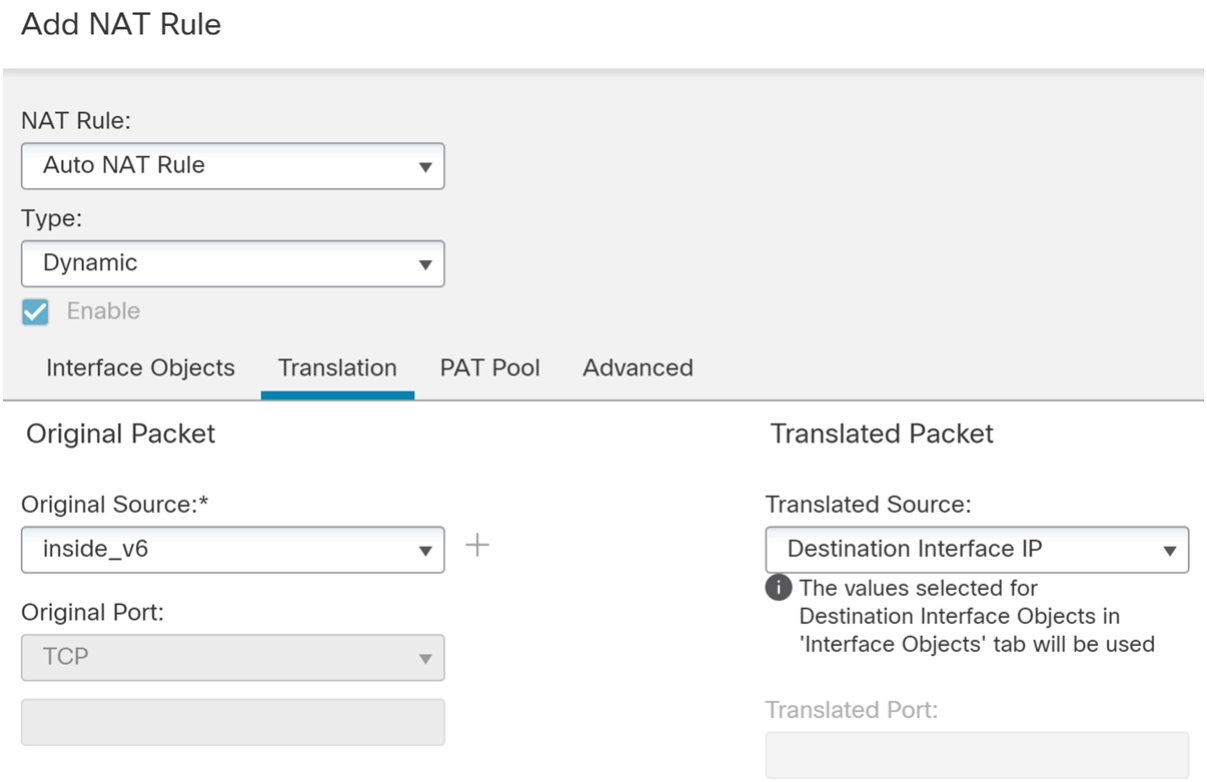
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = inside_v6 네트워크 개체.
- **Translated Source(**변환된 소스**)** = **Destination Interface IP(**대상 인터페이스 **IP)**

f) **Advanced(**고급**)**에서 대상 인터페이스의 IPv6 주소가 사용되어야 함을 나타내는 **IPv6**를 선택합니다.



g) **OK(**확인**)**를 클릭합니다.

이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8:122:2091::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 외부 인터페이스에 대해 구성된 IPv6 전역 주소를 사용하여 NAT66 PAT로 변환됩니다.

NAT 모니터링

NAT 연결을 모니터링하고 트러블슈팅하려면 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show nat** NAT 규칙 및 규칙별 적중 횟수를 표시합니다. NAT의 다른 측면을 표시하는 추가 키워드도 있습니다.
- **show xlate** 현재 활성 상태인 활성 NAT 변환을 표시합니다.
- **clear xlate** 활성 NAT 변환을 제거할 수 있습니다. NAT 규칙을 변경하는 경우에는 활성 변환을 제거해야 할 수 있습니다. 기존 연결은 종료될 때까지 이전 변환 슬롯을 계속 사용하기 때문입니다. 변환을 지우면 시스템에서 새 규칙을 기반으로 하여 클라이언트의 다음 연결 시도 시 클라이언트에 대한 새 변환을 작성할 수 있습니다.

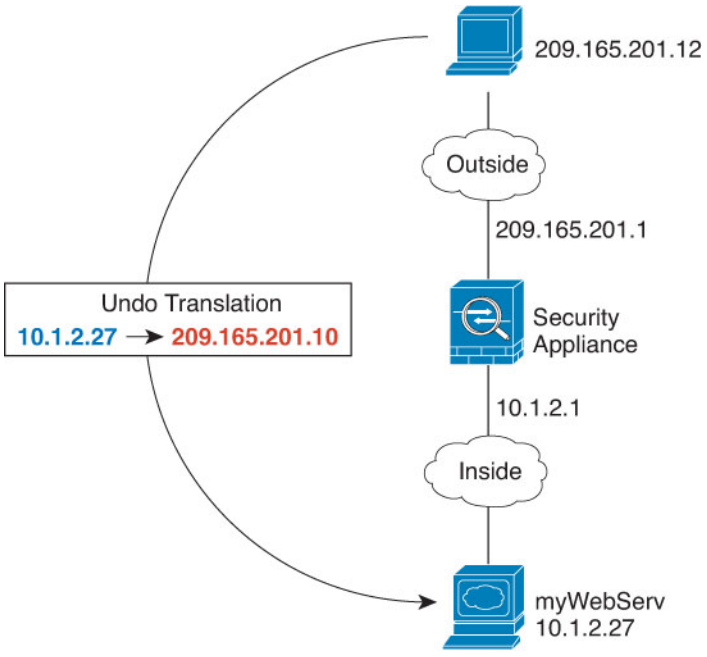
NAT의 예

다음 항목에서는 Threat Defense 디바이스에서 NAT를 구성하는 예를 제공합니다.

내부 웹 서버에 대한 액세스 제공(고정 자동 NAT)

다음 예는 내부 웹 서버에 대해 고정 NAT를 수행합니다. 실제 주소는 사설 네트워크에 있으므로 공용 주소가 필요합니다. 호스트가 고정된 주소에서 웹 서버에 대한 트래픽을 시작할 수 있으려면 고정 NAT가 필요합니다.

그림 ***14:*** 내부 웹 서버에 대한 고정 ***NAT***



시작하기 전에

웹 서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보

안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

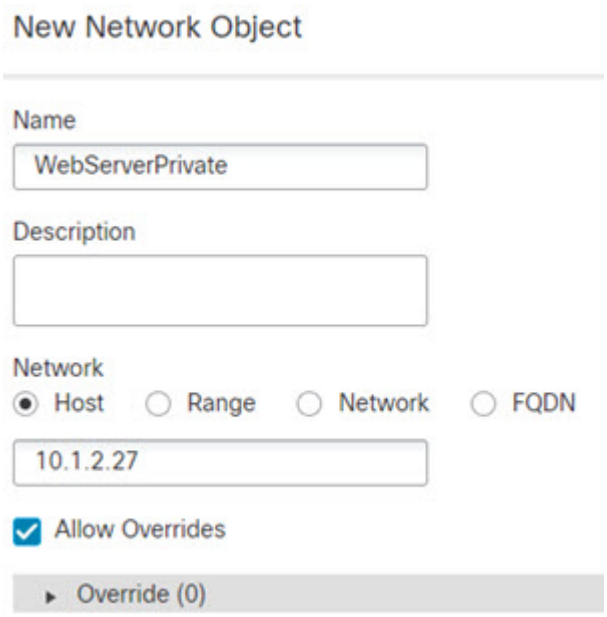
단계 **1** 서버의 전용 및 공용 호스트 주소를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 웹 서버의 전용 어드레스를 정의합니다.

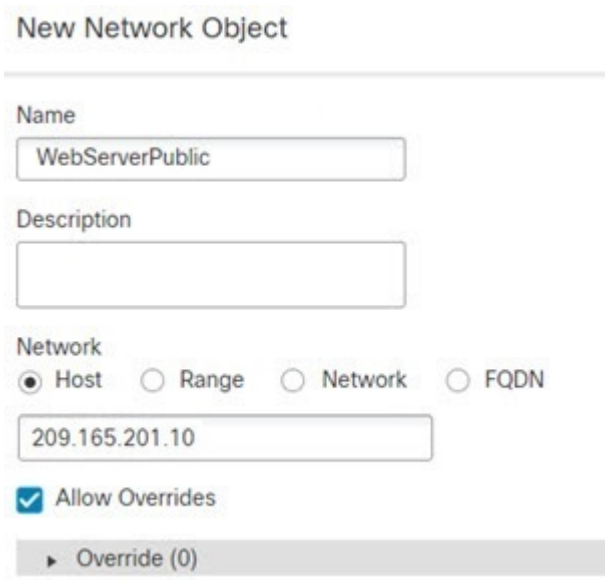
네트워크 개체의 이름을 WebServerPrivate과 같이 지정하고 실제 호스트 IP 주소 10.1.2.27을 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 공용 주소를 정의합니다.

네트워크 개체의 이름을 WebServerPublic과 같이 지정하고 호스트 주소 209.165.201.10을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** 개체용 고정 NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

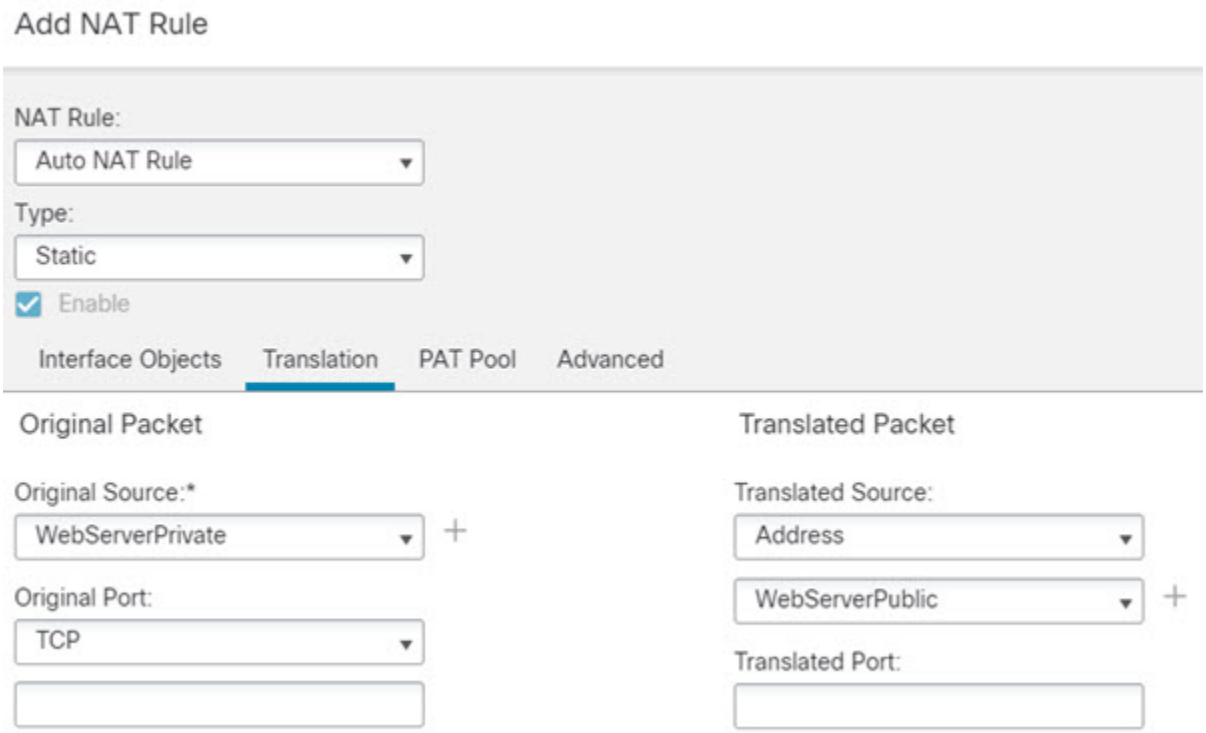
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- 원본 소스 = WebServerPrivate 네트워크 개체
- 변환된 소스 > 주소 = WebServerPublic 네트워크 개체



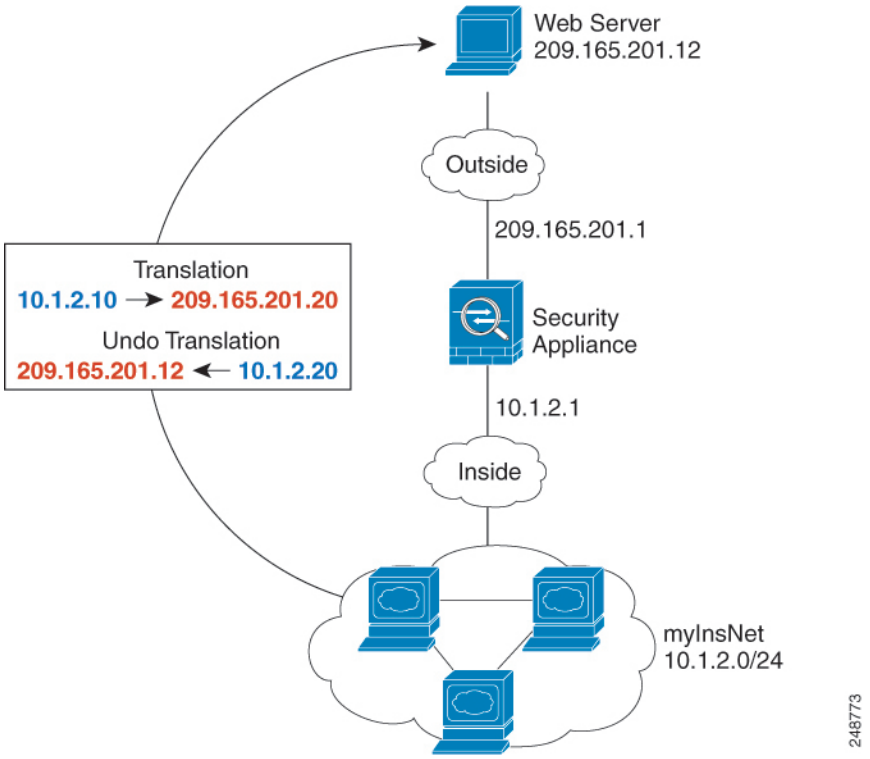
f) **Save(**저장**)**를 클릭합니다.

단계 **3** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

외부 웹 서버의 내부 호스트 및 고정 **NAT**에 대한 동적 자동 **NAT**

다음 예는 사설 네트워크의 내부 사용자가 외부에서 액세스하는 경우를 위한 동적 NAT를 구성합니다. 내부 사용자가 외부 웹 서버에 연결하는 경우도 포함됩니다. 이 경우 웹 서버 주소가 내부 네트워크에 있는 것처럼 보이는 주소로 변환됩니다.

그림 15: 내부용 동적 NAT, 외부 웹 서버용 고정 NAT



시작하기 전에

웹 서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

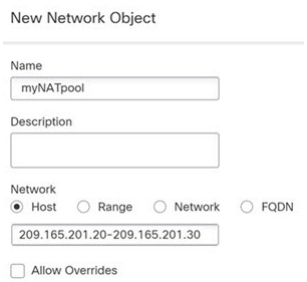
단계 **1** 내부 주소를 변환할 동적 NAT 풀용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 동적 NAT 풀을 정의합니다.

네트워크 개체의 이름을 지정하고(예: myNATpool) 네트워크 범위 209.165.201.20-209.165.201.30을 입력합니다.

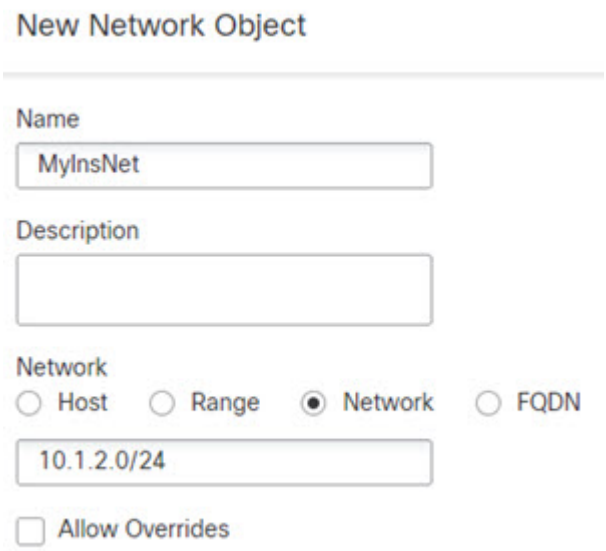


d) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 MyInsNet과 같이 지정하고 네트워크 주소 10.1.2.0/24를 입력합니다.

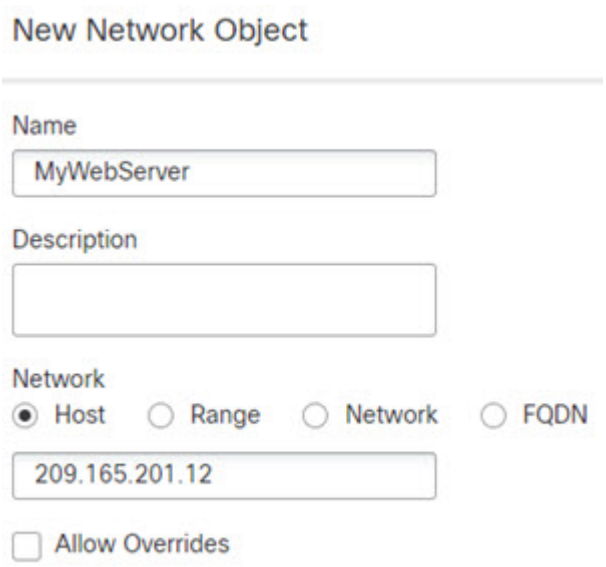


c) **Save(**저장**)**를 클릭합니다.

단계 **3** 외부 웹 서버용 네트워크 개체를 만듭니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 MyWebServer와 같이 지정하고 호스트 주소 209.165.201.12를 입력합니다.

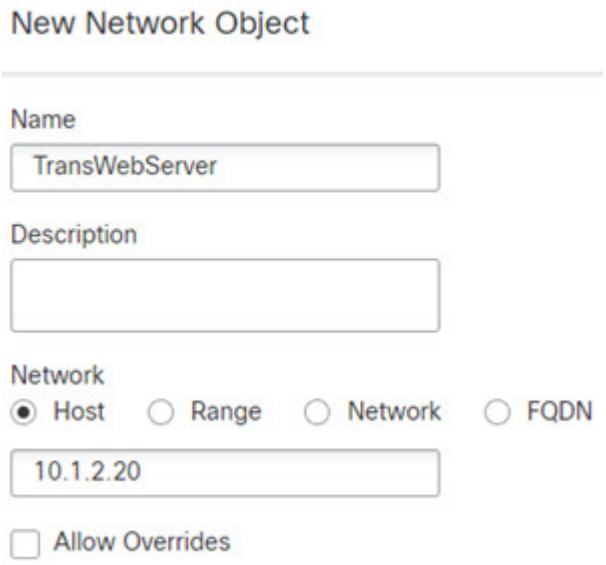


c) **Save(**저장**)**를 클릭합니다.

단계 **4** 변환된 웹 서버 주소용 네트워크 개체를 만듭니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 TransWebServer와 같이 지정하고 호스트 주소 10.1.2.20을 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **5** 동적 NAT 풀 개체를 사용하여 내부 네트워크용 동적 NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

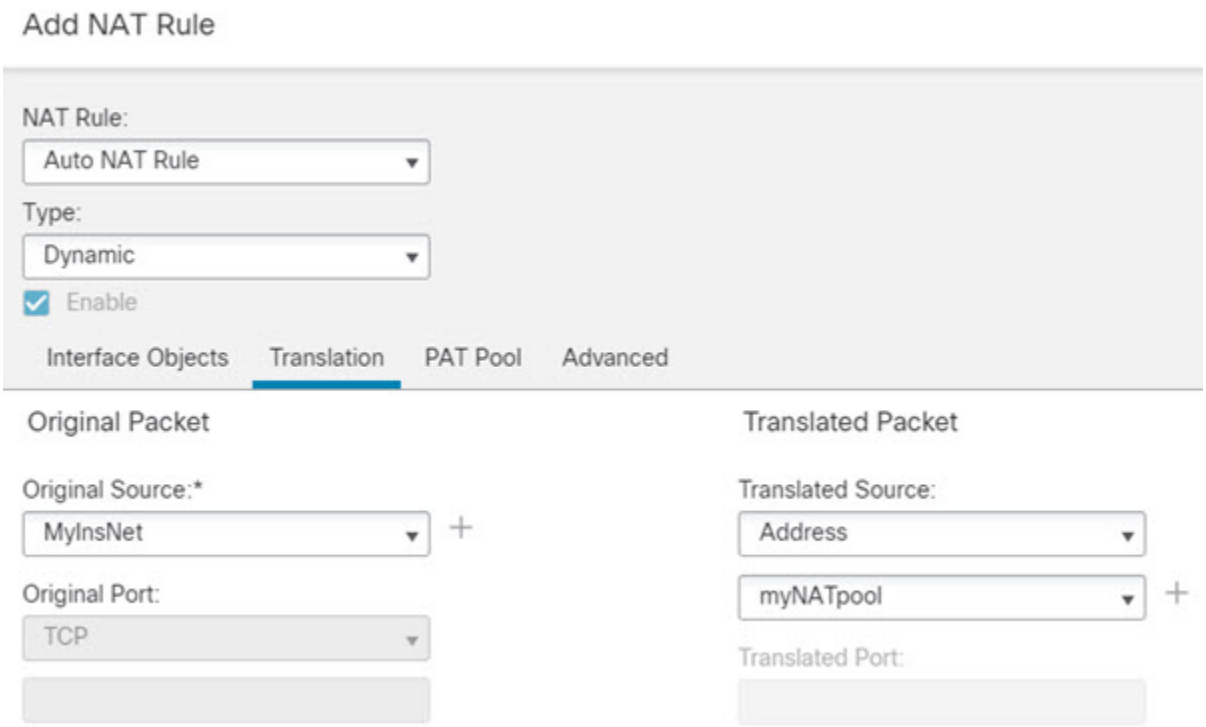
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 동적

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsNet 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = myNATpool 네트워크 그룹입니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **6** 웹 서버용 고정 NAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

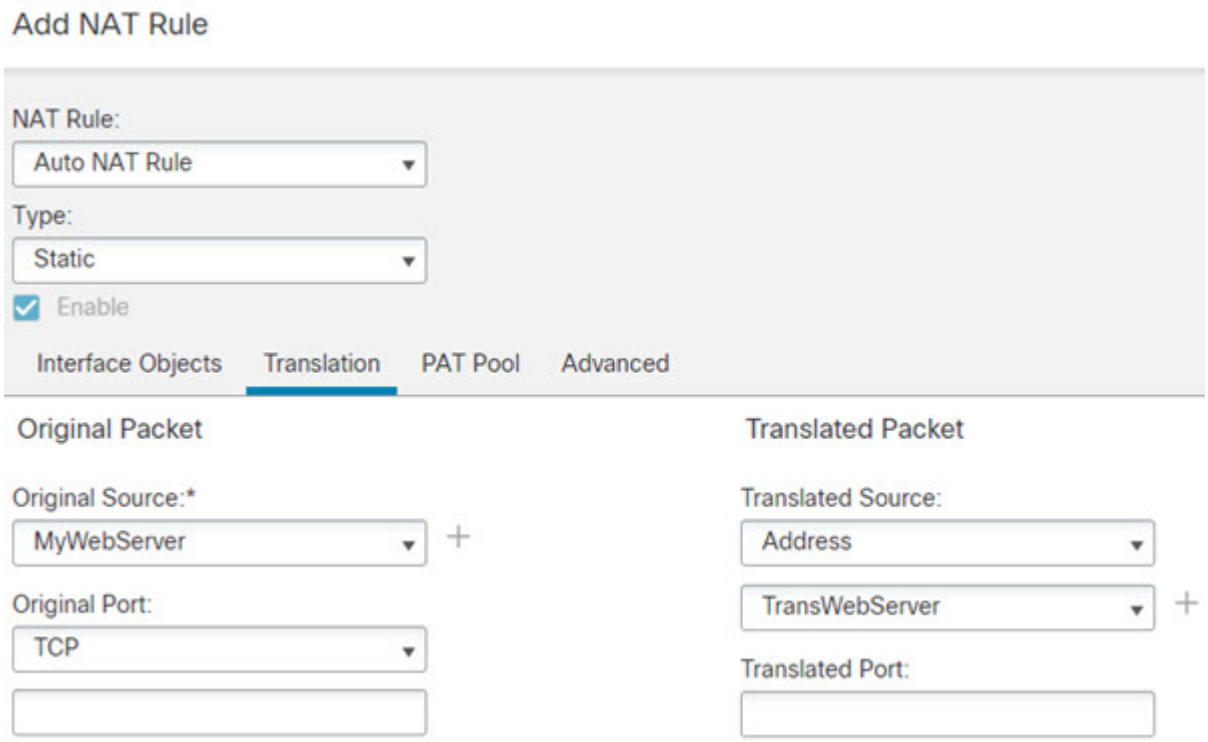
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = outside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myWebServer 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = TransWebServer 네트워크 개체.



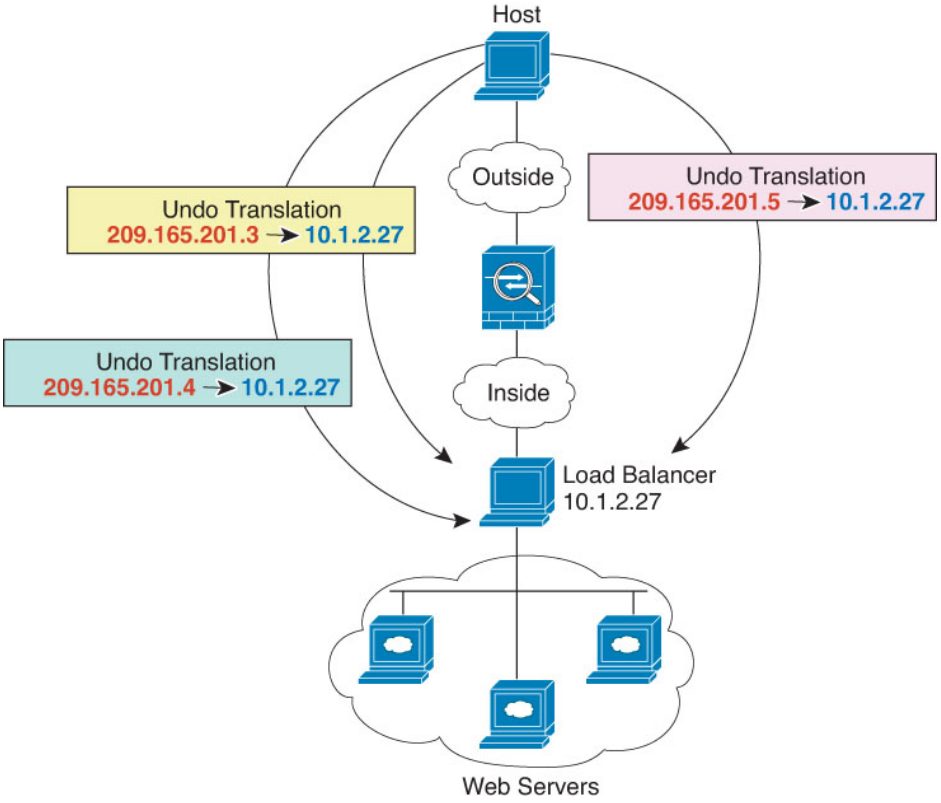
e) **Save(**저장**)**를 클릭합니다.

단계 **7** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

여러 매핑된 주소가 있는 내부 로드 밸런서(고정 자동 NAT, 일대다)

다음 예는 여러 IP 주소로 변환되는 내부 로드 밸런서를 보여줍니다. 외부 호스트가 매핑된 IP 주소 중 하나에 액세스하는 경우 단일 로드 밸런서 주소로 변환되지 않습니다. 요청된 URL에 따라 트래픽이 올바른 웹 서버로 리디렉션됩니다.

그림 *16:* 내부 로드 밸런서용 일대다 고정 ***NAT***



시작하기 전에

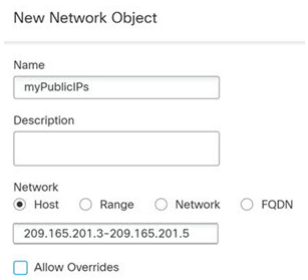
웹 서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 로드 밸런서를 매핑하려는 주소용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) Define the addresses.

네트워크 개체의 이름을 지정하고(예: myPublicIPs) 네트워크 범위 209.165.201.3-209.165.201.5를 입력합니다.

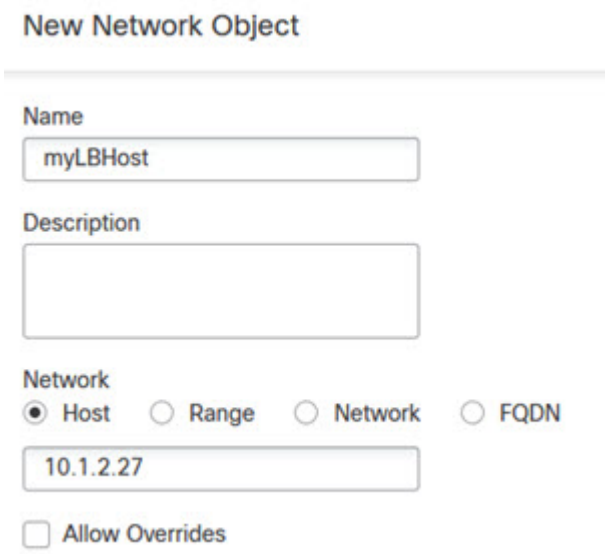


d) **Save(**저장**)**를 클릭합니다.

단계 **2** 로드 밸런서용 네트워크 개체를 만듭니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 myLBHost와 같이 지정하고 호스트 주소 10.1.2.27을 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **3** 로드 밸런서용 고정(static) NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

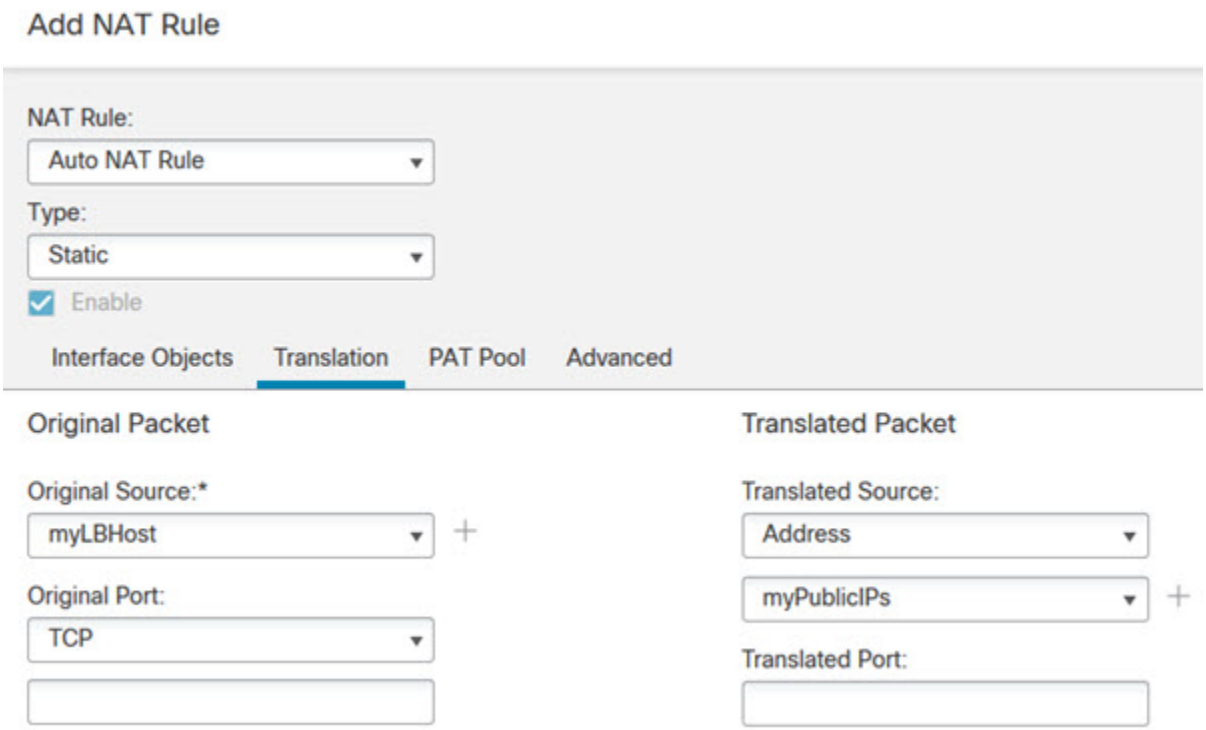
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myLBHost 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = myPublicIPs 네트워크 그룹.



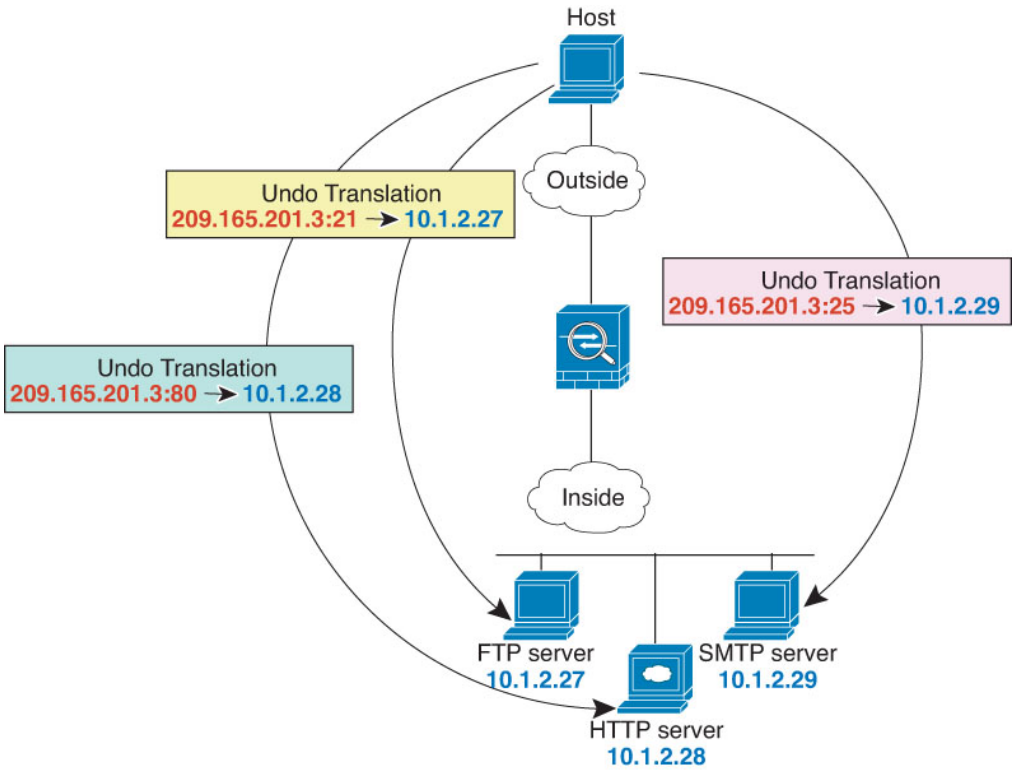
f) **Save(**저장**)**를 클릭합니다.

단계 **4** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

FTP, HTTP 및 SMTP용 단일 주소(포트 변환 고정 자동 NAT)

다음과 같은 포트 변환 고정 NAT의 예는 원격 사용자가 FTP, HTTP 및 SMTP에 액세스하기 위해 사용할 단일 주소를 제공합니다. 이러한 서버는 실제 네트워크에서 실제로 서로 다른 디바이스이지만, 각 서버에 대해 동일하게 매핑된 IP 주소를 사용하되 포트는 다른 포트 변환 고정 NAT 규칙을 지정할 수 있습니다.

그림 *17:* 포트 변환 고정 ***NAT***



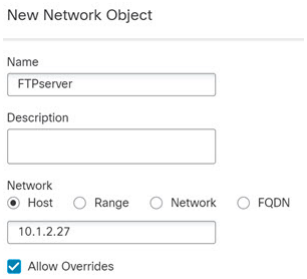
시작하기 전에

서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** FTP 서버용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 네트워크 개체의 이름을 FTPserver와 같이 지정하고 FTP 서버의 실제 IP 주소 10.1.2.27을 입력합니다.

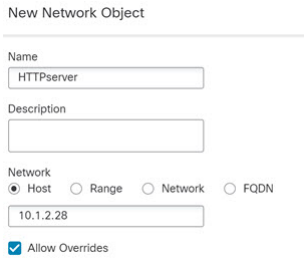


d) **Save(**저장**)**를 클릭합니다.

단계 **2** HTTP 서버용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 HTTPserver와 같이 지정하고 호스트 주소 10.1.2.28을 입력합니다.

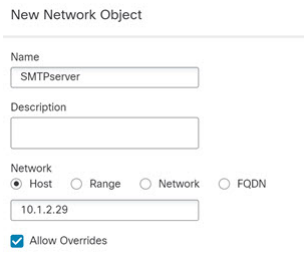


c) **Save(**저장**)**를 클릭합니다.

단계 **3** SMTP 서버용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 SMTPserver와 같이 지정하고 호스트 주소 10.1.2.29를 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **4** 서버 3대에 사용되는 공용 IP 주소용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 ServerPublicIP와 같이 지정하고 호스트 주소 209.165.201.3을 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **5** FTP 포트를 자기 자신에 매핑하는 FTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

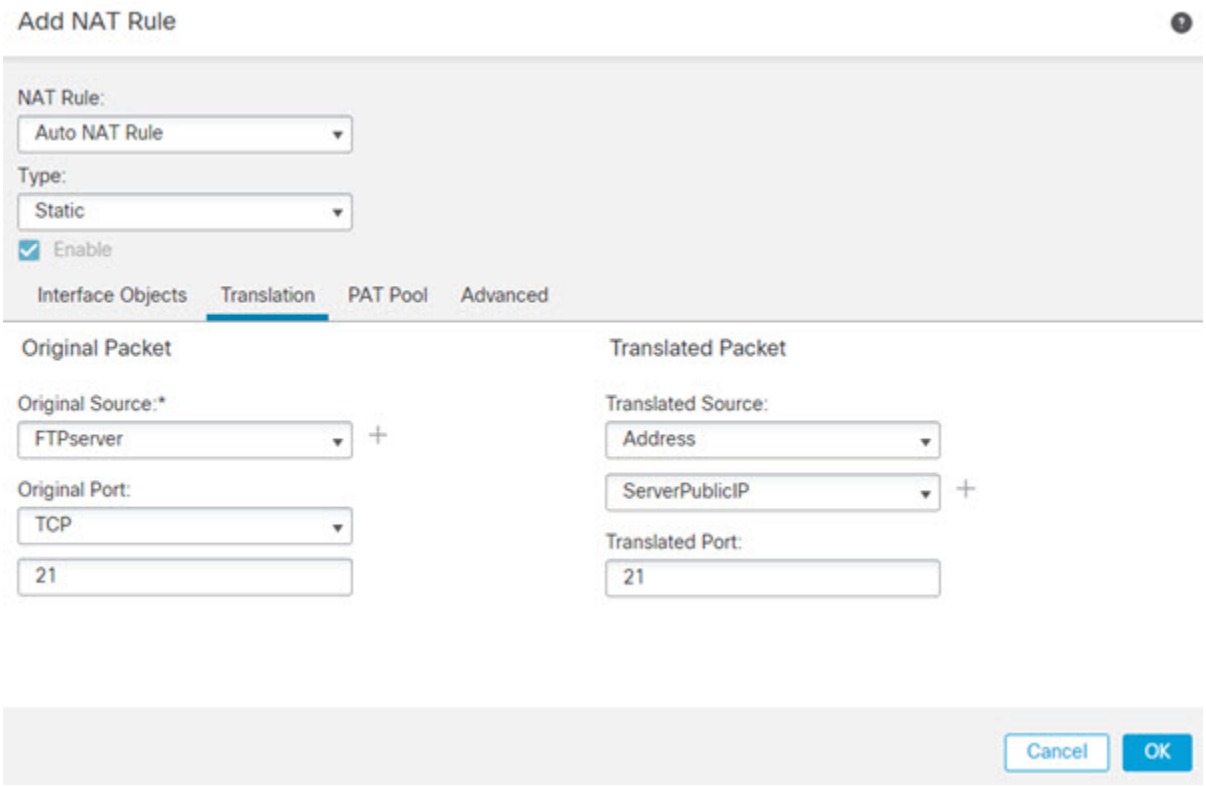
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = FTPserver 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ServerPublicIP 네트워크 개체.
- **Original Port(**원본 포트**)** > **TCP** = 21.
- **Translated Port(**변환된 포트**)** = 21.



f) **Save(**저장**)**를 클릭합니다.

단계 **6** HTTP 포트를 자기 자신에 매핑하는 HTTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

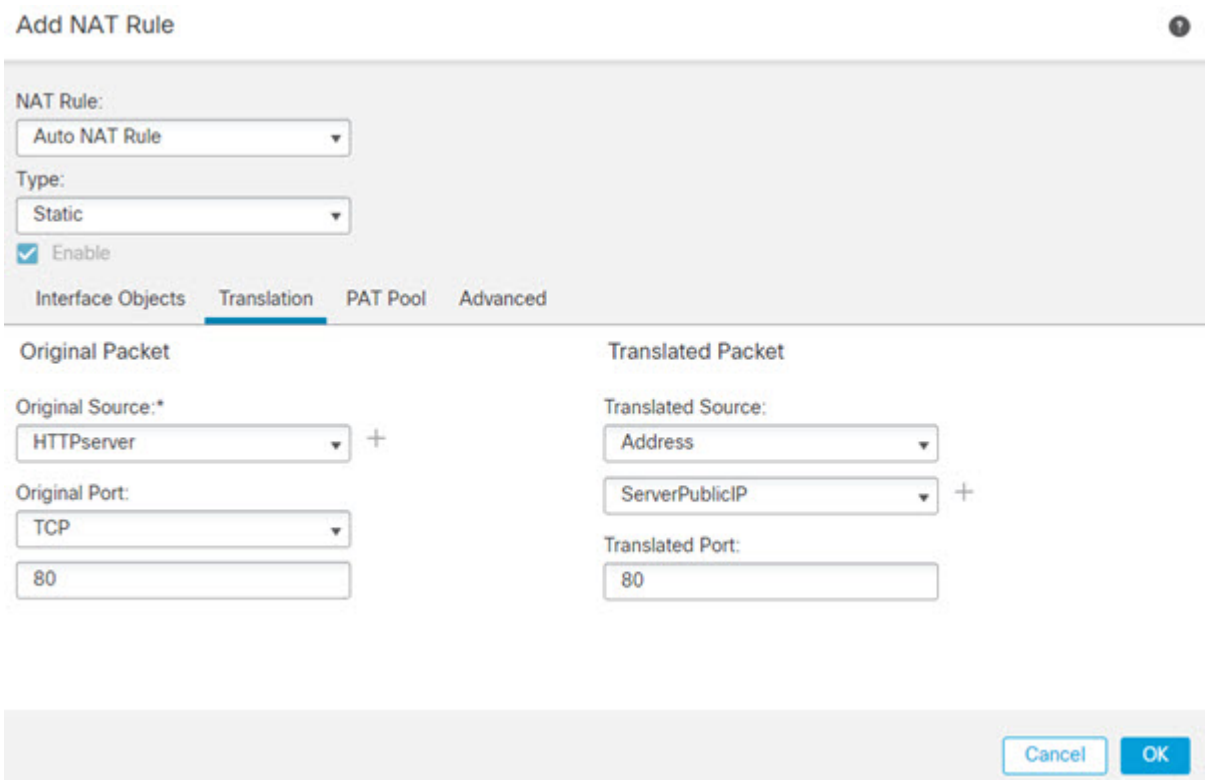
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = HTTPserver 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ServerPublicIP 네트워크 개체.
- **Original Port(**원본 포트**)** > **TCP** = 80.
- **Translated Port(**변환된 포트**)** = 80.



e) **Save(**저장**)**를 클릭합니다.

단계 **7** SMTP 포트를 자기 자신에 매핑하는 SMTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

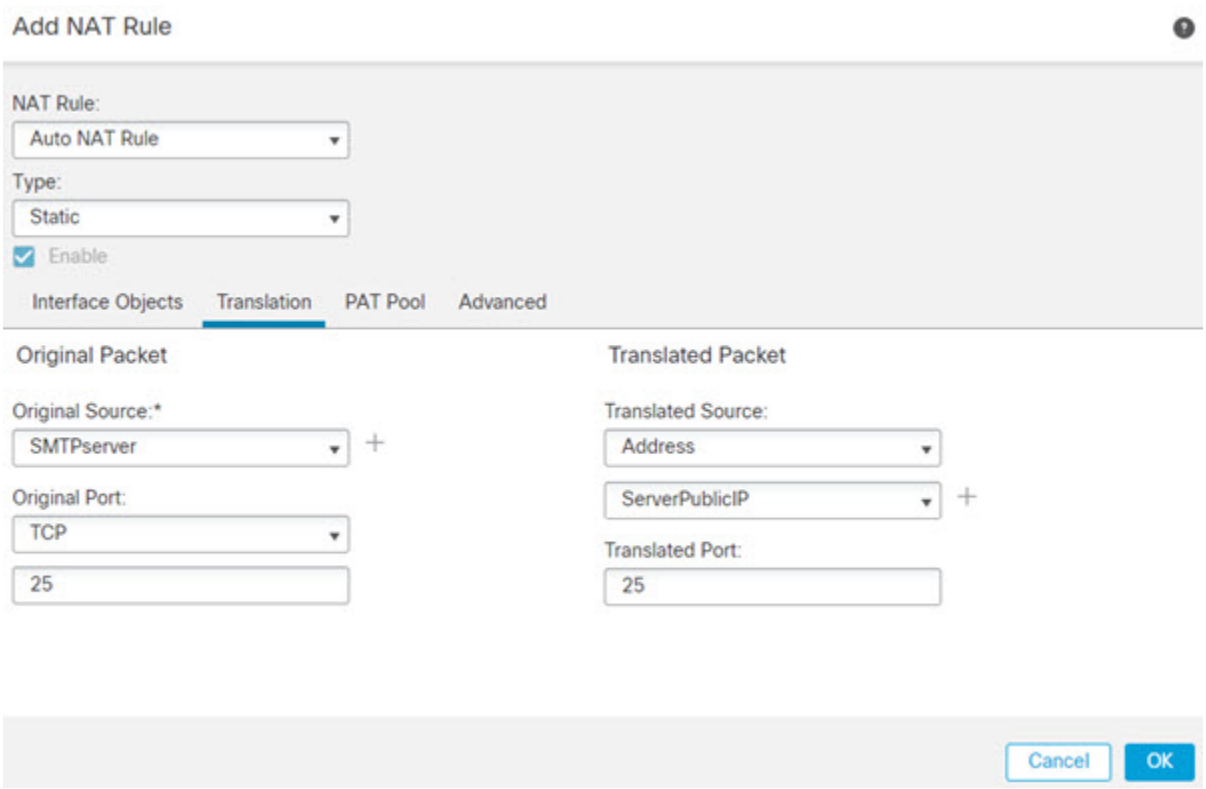
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = SMTPserver 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ServerPublicIP 네트워크 개체.
- **Original Port(**원본 포트**)** > **TCP** = 25.
- **Translated Port(**변환된 포트**)** = 25.



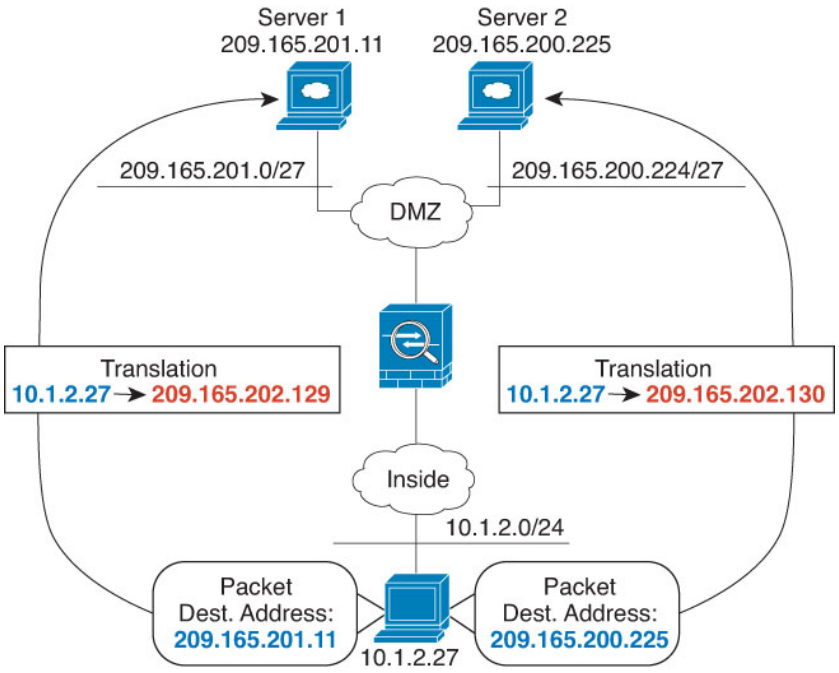
e) **Save(**저장**)**를 클릭합니다.

단계 **8** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

대상에 따라 다른 변환(동적 수동 **PAT)**

다음 그림은 두 개의 서로 다른 서버에 액세스하는 10.1.2.0/24 네트워크의 호스트를 보여줍니다. 호스트가 209.165.201.11의 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 209.165.200.225의 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

그림 *18:* 서로 다른 대상 주소를 사용하는 수동 *NAT*



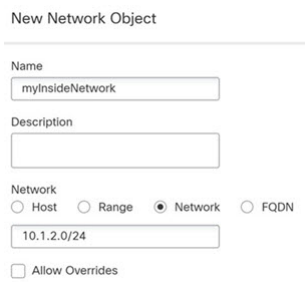
시작하기 전에

서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **dmz**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 네트워크 개체의 이름을 myInsideNetwork와 같이 지정하고 실제 네트워크 주소 10.1.2.0/24를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

단계 **2** DMZ 네트워크 1용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

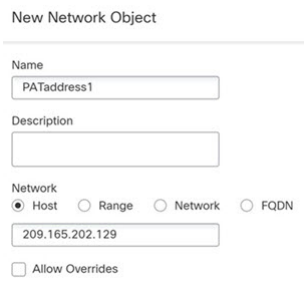
b) 네트워크 개체의 이름을 DMZnetwork1과 같이 지정하고 네트워크 주소 209.165.201.0/27(서브넷 마스크 255.255.255.224)을 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **3** DMZ 네트워크 1용 PAT 주소의 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress1과 같이 지정하고 호스트 주소 209.165.202.129를 입력합니다.

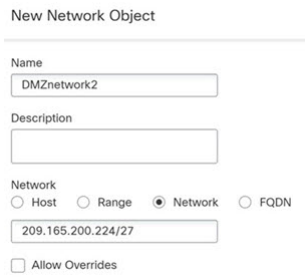


c) **Save(**저장**)**를 클릭합니다.

단계 **4** DMZ 네트워크 2용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 DMZnetwork2와 같이 지정하고 네트워크 주소 209.165.200.224/27(서브넷 마스크 255.255.255.224)을 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **5** DMZ 네트워크 2용 PAT 주소의 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress2와 같이 지정하고 호스트 주소 209.165.202.130을 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **6** DMZ 네트워크 1용 동적 수동 PAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적

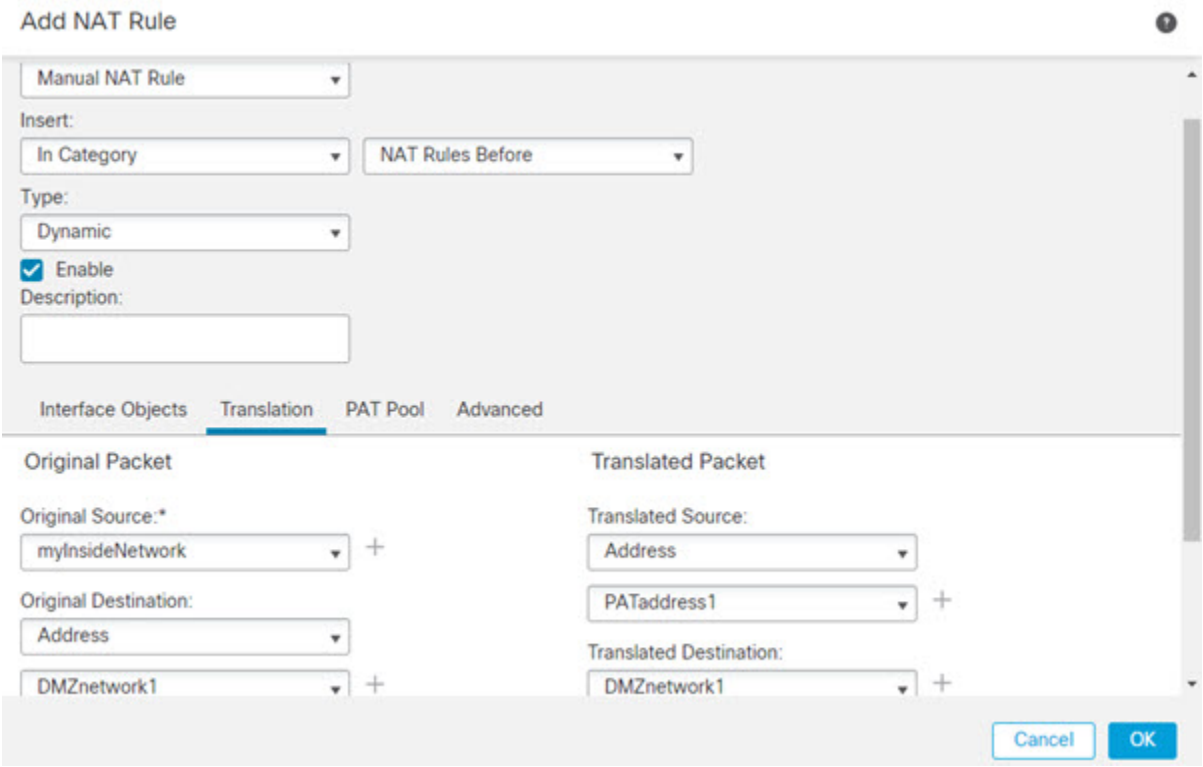
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = dmz.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsideNetwork 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = PATaddress1 네트워크 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = DMZnetwork1 네트워크 개체.
- **Translated Destination(**변환된 대상**)** = DMZnetwork1 네트워크 개체.

참고 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **7** DMZ 네트워크 2용 동적 수동 PAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적

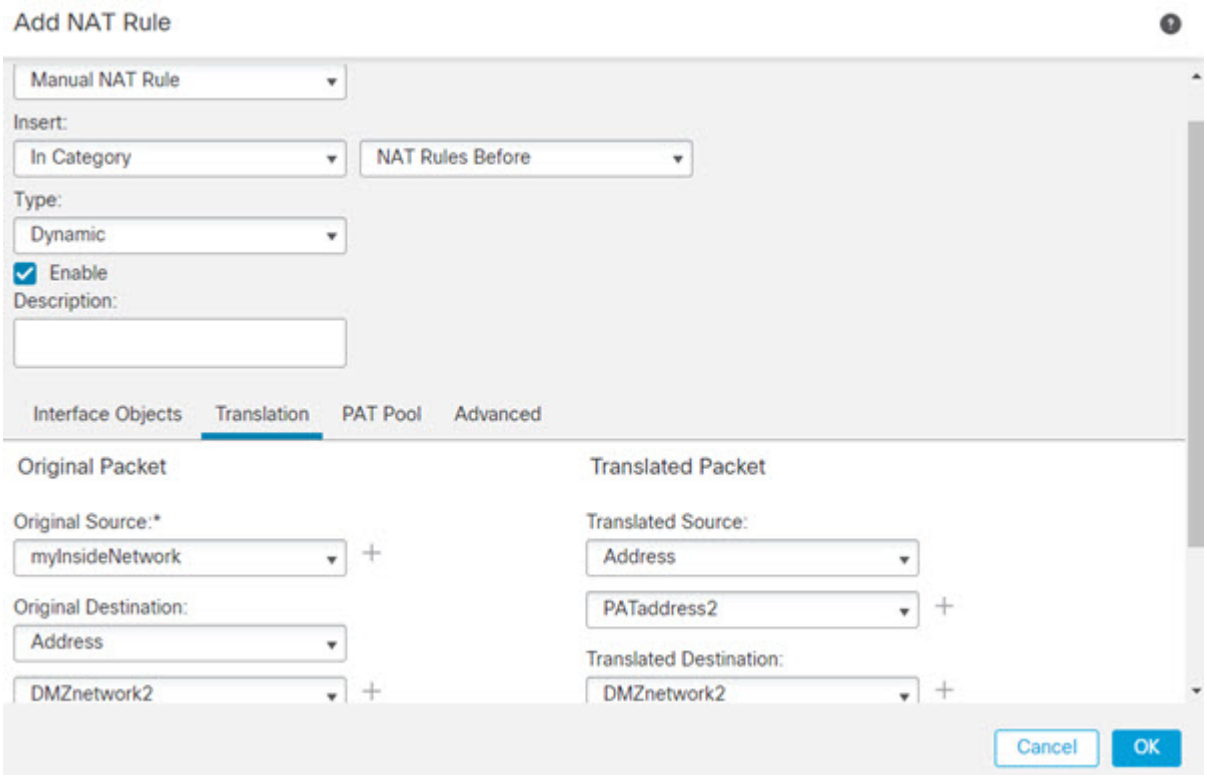
c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = dmz.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsideNetwork 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = PATaddress2 네트워크 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = DMZnetwork2 네트워크 개체.

• **Translated Destination(**변환된 대상**)** = DMZnetwork2 네트워크 개체.



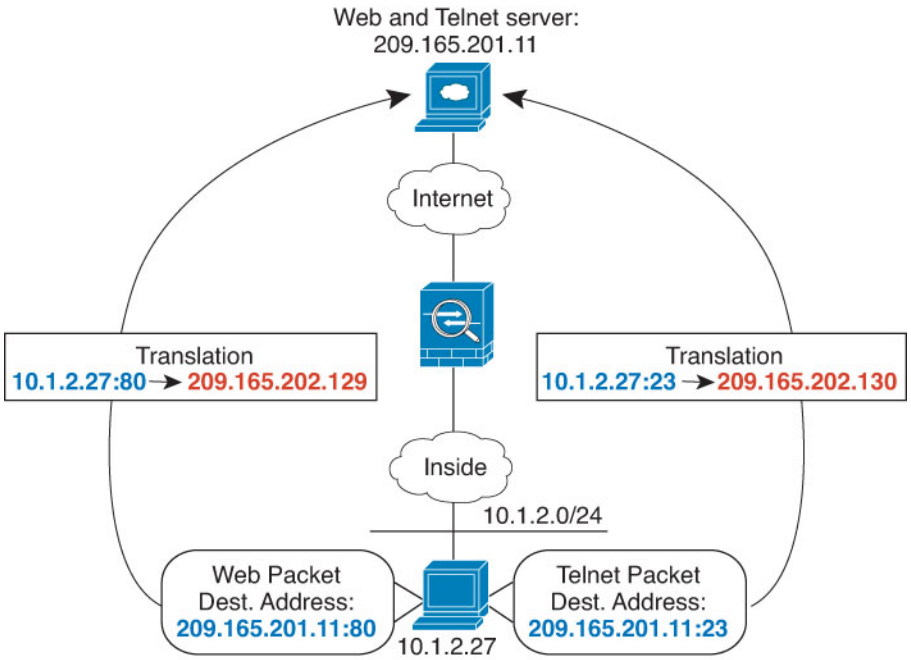
e) **Save(**저장**)**를 클릭합니다.

단계 **8** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

대상 주소 및 포트에 따라 다른 변환(동적 수동 **PAT)**

다음 그림은 소스 포트와 대상 포트의 사용법을 보여줍니다. 10.1.2.0/24 네트워크의 호스트가 웹 서비스와 텔넷 서비스를 모두 제공하는 단일 호스트에 액세스합니다. 호스트가 텔넷 서비스용 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 동일한 웹 서비스용 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

그림 *19:* 서로 다른 대상 포트를 사용하는 수동 *NAT*



시작하기 전에

서버를 보호하는 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **dmz**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

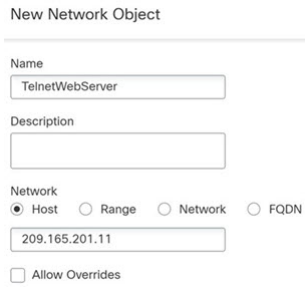
c) 네트워크 개체의 이름을 myInsideNetwork와 같이 지정하고 실제 네트워크 주소 10.1.2.0/24를 입력합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** 텔넷/웹 서버용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 TelnetWebServer와 같이 지정하고 호스트 주소 209.165.201.11을 입력합니다.

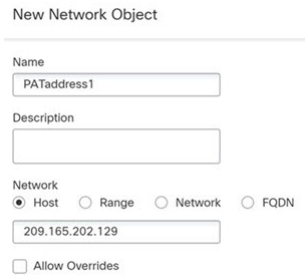


c) **Save(**저장**)**를 클릭합니다.

단계 **3** 텔넷 사용 시의 PAT 주소용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress1과 같이 지정하고 호스트 주소 209.165.202.129를 입력합니다.



c) **Save(**저장**)**를 클릭합니다.

단계 **4** HTTP 사용 시의 PAT 주소용 네트워크 개체를 생성합니다.

a) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress2와 같이 지정하고 호스트 주소 209.165.202.130을 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **5** 텔넷 액세스용 동적 수동 PAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적

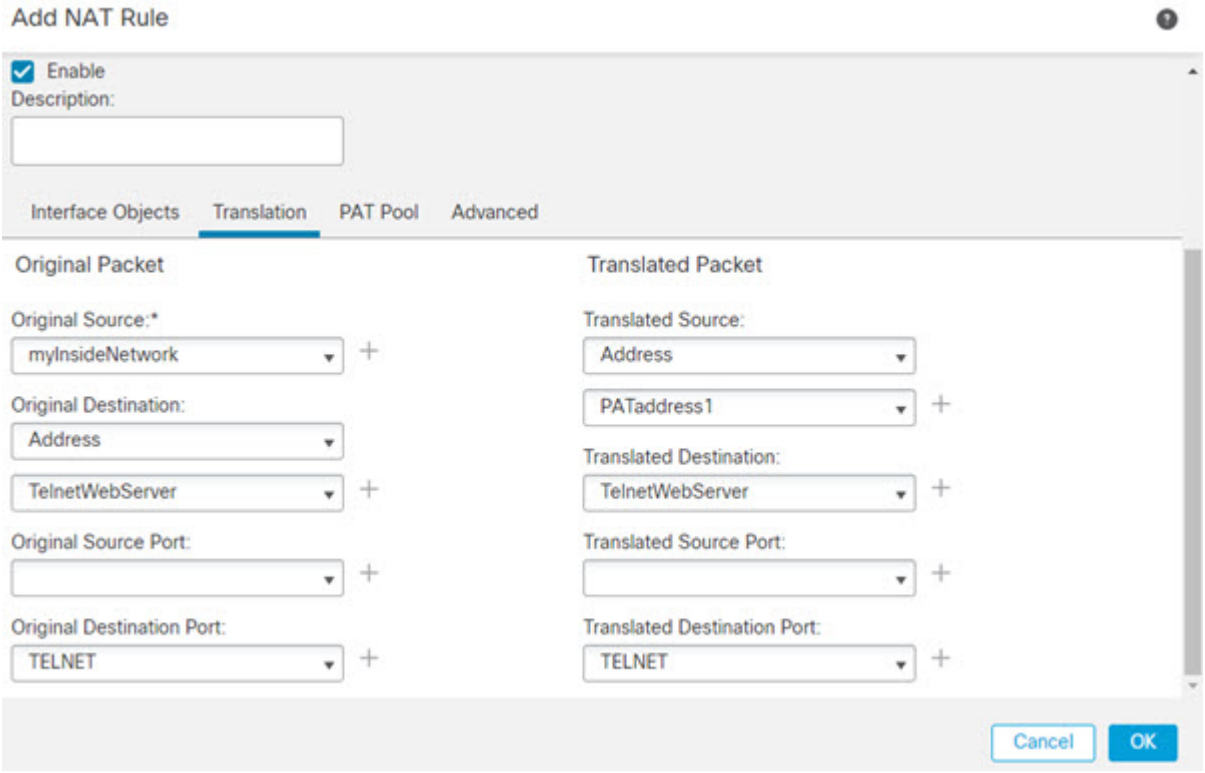
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = dmz.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsideNetwork 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = PATaddress1 네트워크 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = TelnetWebServer 네트워크 개체.
- **Translated Destination(**변환된 대상**)** = TelnetWebServer 네트워크 개체.
- **Original Destination Port(**원본 대상 포트**)** = TELNET 포트 개체(시스템 정의)
- **Translated Destination Port(**변환된 대상 포트**)** = TELNET 포트 개체(시스템 정의)

참고 대상 주소 또는 포트를 변환하지 않을 것이기 때문에 원본 및 변환된 대상 주소에 대해 동일한 주소를 지정하고 원본 및 변환된 포트에 대해 동일한 포트를 지정하여, 대상 주소 또는 포트에 대한 ID NAT를 구성해야 합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **6** 웹 액세스용 동적 수동 PAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적

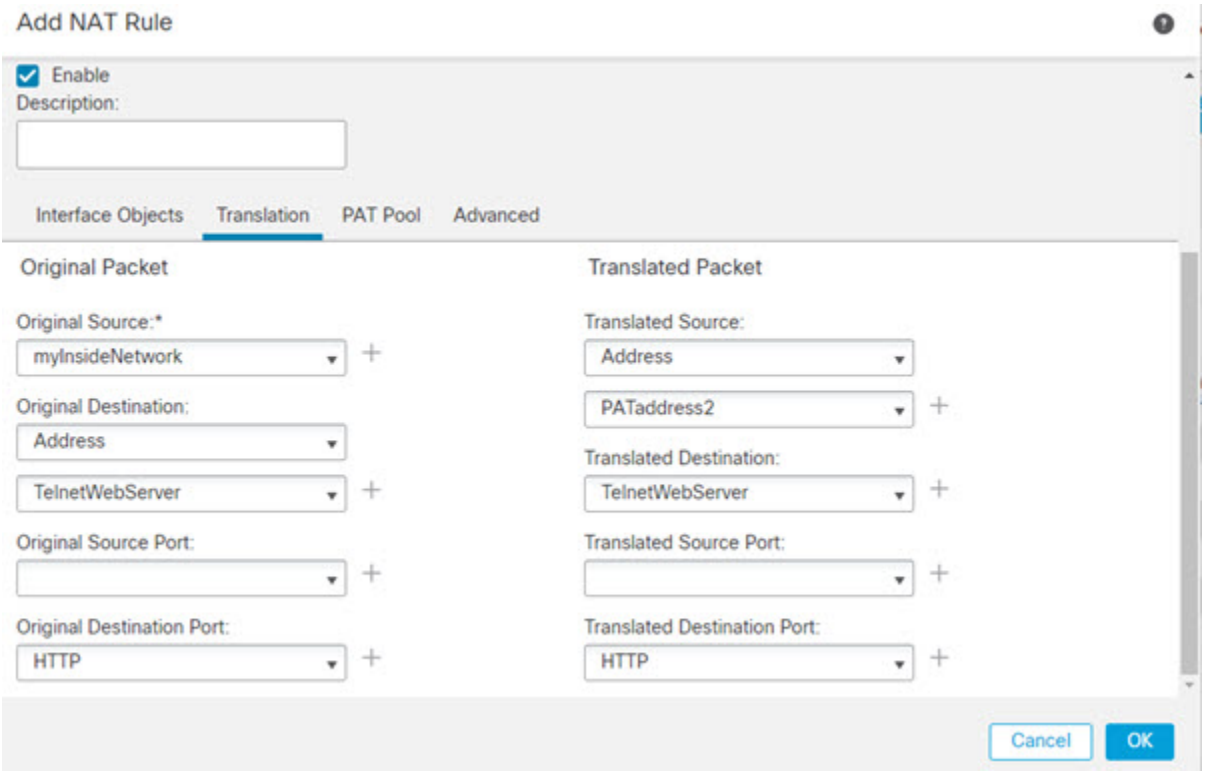
c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = dmz.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = myInsideNetwork 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = PATaddress2 네트워크 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = TelnetWebServer 네트워크 개체.
- **Translated Destination(**변환된 대상**)** = TelnetWebServer 네트워크 개체.
- **Original Destination Port(**원본 대상 포트**)** = HTTP 포트 개체(시스템 정의)

- **Translated Destination Port(**변환된 대상 포트**)** = HTTP 포트 개체(시스템 정의)



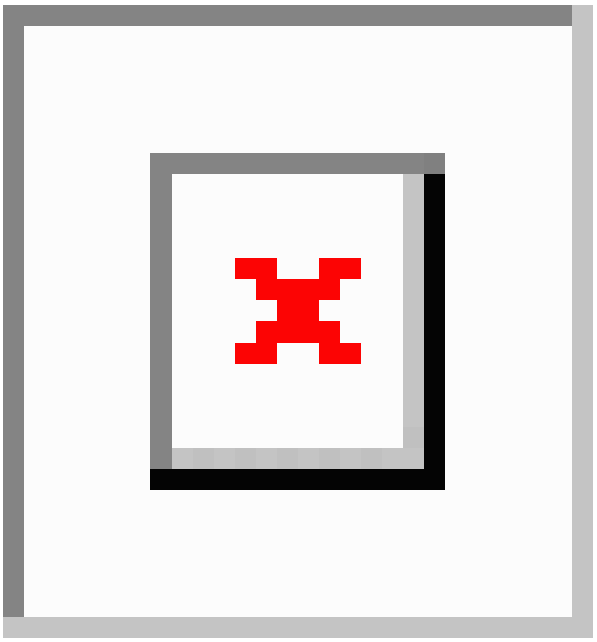
e) **Save(**저장**)**를 클릭합니다.

단계 **7** NAT 규칙 페이지에서 **Save(**저장**)**를 클릭합니다.

NAT 및 사이트 대 사이트 VPN

다음 그림은 볼더 사무실과 산호세 사무실을 연결하는 사이트 대 사이트 터널을 보여줍니다. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래의 예에서는 인터페이스 PAT 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 단순히 주소를 동일한 주소로 변환합니다.

그림 *20:* 사이트 대 사이트 *VPN*을 위한 인터페이스 *PAT* 및 *ID NAT*



다음 예에서는 방화벽1(볼더)의 구성에 대해 설명합니다.

시작하기 전에

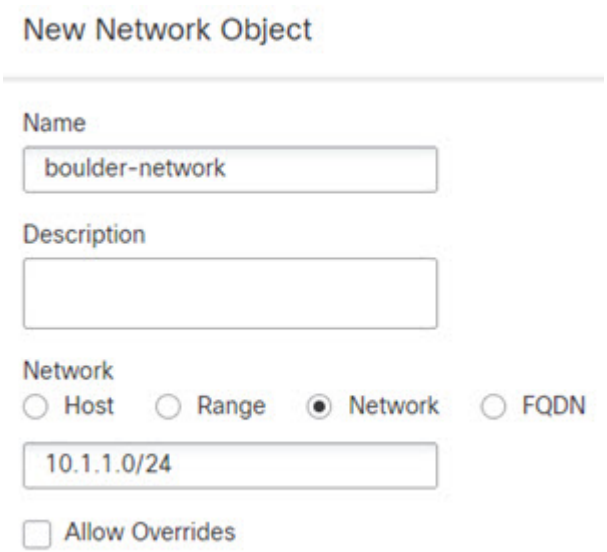
VPN의 디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 Firewall1(Boulder) 인터페이스에 대한 **inside-boulder** 및 **outside-boulder**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interfaces(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** 여러 네트워크를 정의하기 위한 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 볼더 내부 네트워크를 확인합니다.

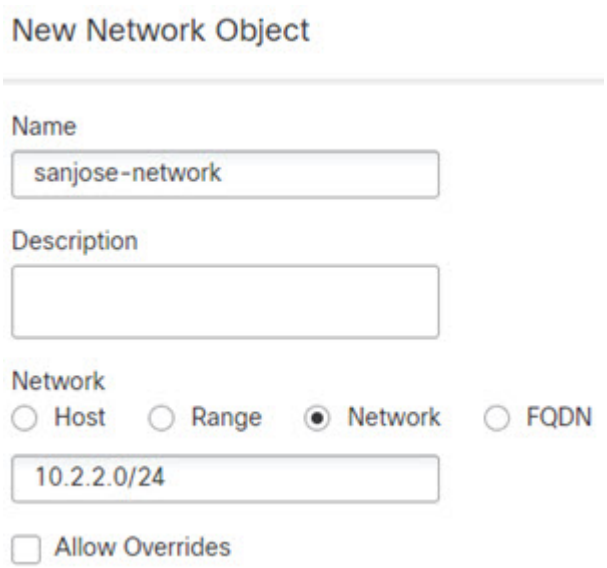
네트워크 개체의 이름을 boulder-network와 같이 지정하고 네트워크 주소 10.1.1.0/24를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 내부 San Jose 네트워크를 정의합니다.

네트워크 개체의 이름을 sanjose-network와 같이 지정하고 네트워크 주소 10.2.2.0/24를 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 고정

d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

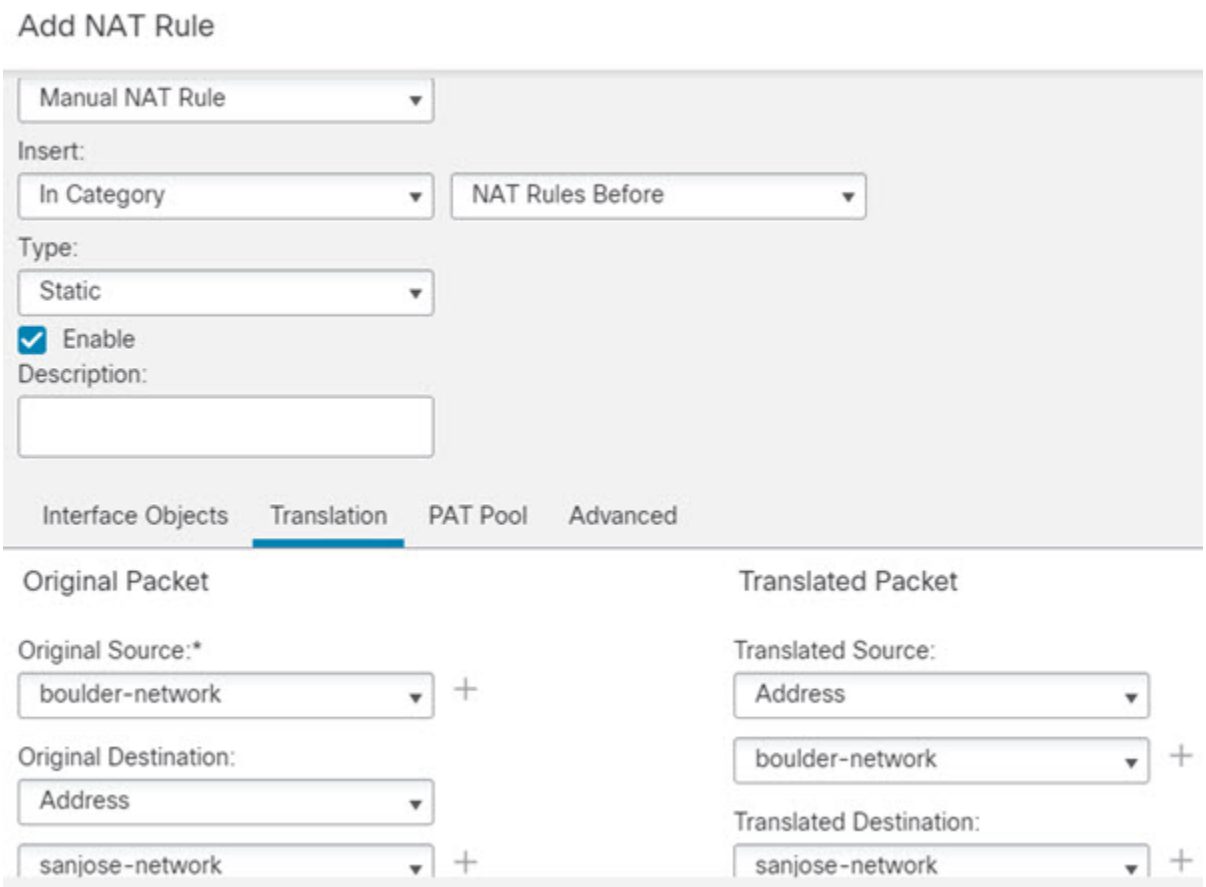
- **Source Interface Objects(**소스 인터페이스 개체**)** = inside-boulder.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside-boulder.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = boulder-network 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = boulder-network 개체.
- **Original Destination(**원본 대상**)** > **Address(**주소**)** = sanjose-network 개체.
- **Translated Destination(**변환된 대상**)** = sanjose-network 개체.

  참고 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘 다에 대해 ID NAT를 구성합니다.

f) **Advanced(**고급**)**에서 **Do not proxy ARP on Destination interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)**를 선택합니다.



g) **Save(**저장**)**를 클릭합니다.

단계 **3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

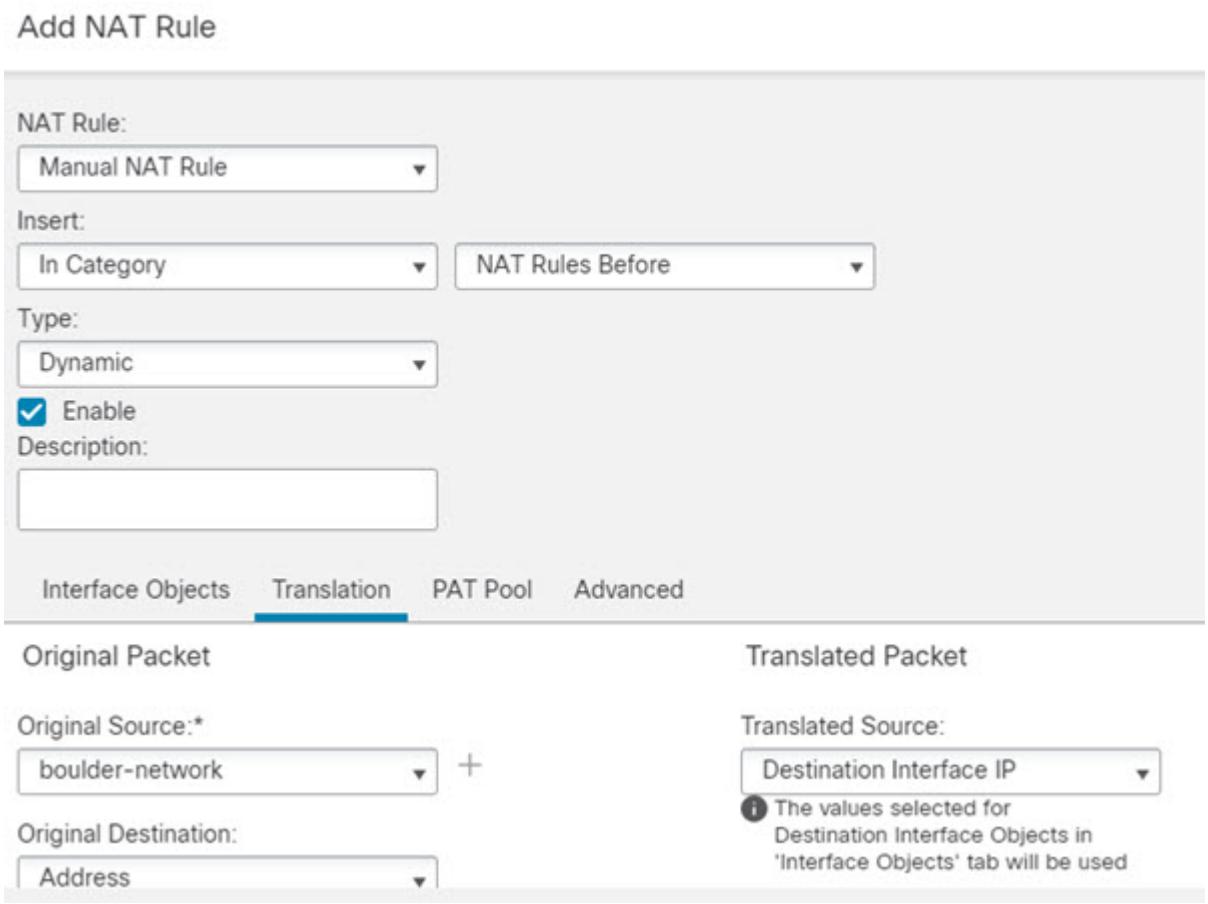
- **Nat Rule(NAT** 규칙**)** - Manual NAT Rule(수동 NAT 규칙).
- 유형 = 동적
- **Insert Rule(**규칙 삽입**)** = 첫 번째 규칙 뒤의 모든 위치. 이 규칙은 모든 대상 주소에 적용되므로 sanjose-network를 대상으로 사용하는 규칙이 이 규칙 앞에 와야 합니다. 그렇지 않으면 sanjose-network 규칙은 어떤 주소와도 일치하지 않게 됩니다. 기본적으로는 "자동 NAT 앞의 NAT 규칙" 섹션 끝에 새 수동 NAT 규칙을 배치합니다.

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside-boulder.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside-boulder.

d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = boulder-network 개체.
- **Translated Source(**변환된 소스**)** = **Destination Interface IP(**대상 인터페이스 **IP)** 이 옵션은 대상 인터페이스 개체에 포함된 인터페이스를 사용하여 인터페이스 PAT를 구성합니다.
- **Original Destination(**원본 대상**)** > **Address** = 임의(빈 상태로 유지).
- **Translated Destination(**변환된 대상**)** = 임의(빈 상태로 유지).



e) **Save(**저장**)**를 클릭합니다.

단계 **4** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

NAT를 사용하여 DNS 쿼리 및 응답 재작성

회신의 주소를 NAT 구성과 일치하는 주소로 교체하여 DNS 회신을 수정하도록 Firepower Threat Defense 디바이스를 구성해야 할 수 있습니다. 각 변환 규칙을 구성할 때 DNS 수정을 구성할 수 있습니다. DNS 수정은 DNS Doctoring이라고도 합니다.

이 기능은 NAT 규칙과 일치하는 DNS 쿼리 및 회신의 주소를 재작성합니다(예: IPv4의 A 레코드, IPv6의 AAAA 레코드 또는 역방향 DNS 쿼리의 PTR 레코드). 매핑된 인터페이스에서 다른 임의의 인터페이스로 이동하는 DNS 회신의 경우 매핑된 값에서 실제 값으로 레코드가 재작성됩니다. 반대로, 임의의 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 회신의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 기능은 NAT44, NAT 66, NAT46 및 NAT64에서 작동합니다.

다음은 NAT 규칙에 DNS 재작성을 구성해야 하는 몇 가지 주요 상황입니다.

- 규칙이 NAT64 또는 NAT46이며 DNS 서버가 외부 네트워크에 있는 경우. DNS A 레코드(IPv4의 경우)를 AAAA 레코드(IPv6의 경우)로 변환하려면 DNS 재작성이 필요합니다.
- DNS 서버가 외부에 있고 클라이언트는 내부에 있으며 클라이언트가 사용하는 일부 FQDN(Fully Qualified Domain Name)이 다른 내부 호스트로 확인되는 경우.
- DNS 서버가 내부에 있고 프라이빗 IP 어드레스로 응답하며, 클라이언트는 외부에 있고 내부에서 호스팅되는 서버를 가리키는 FQDN(Fully Qualified Domain Name)에 액세스하는 경우.

DNS 재작성 제한

다음은 DNS 재작성의 몇 가지 제한 사항입니다.

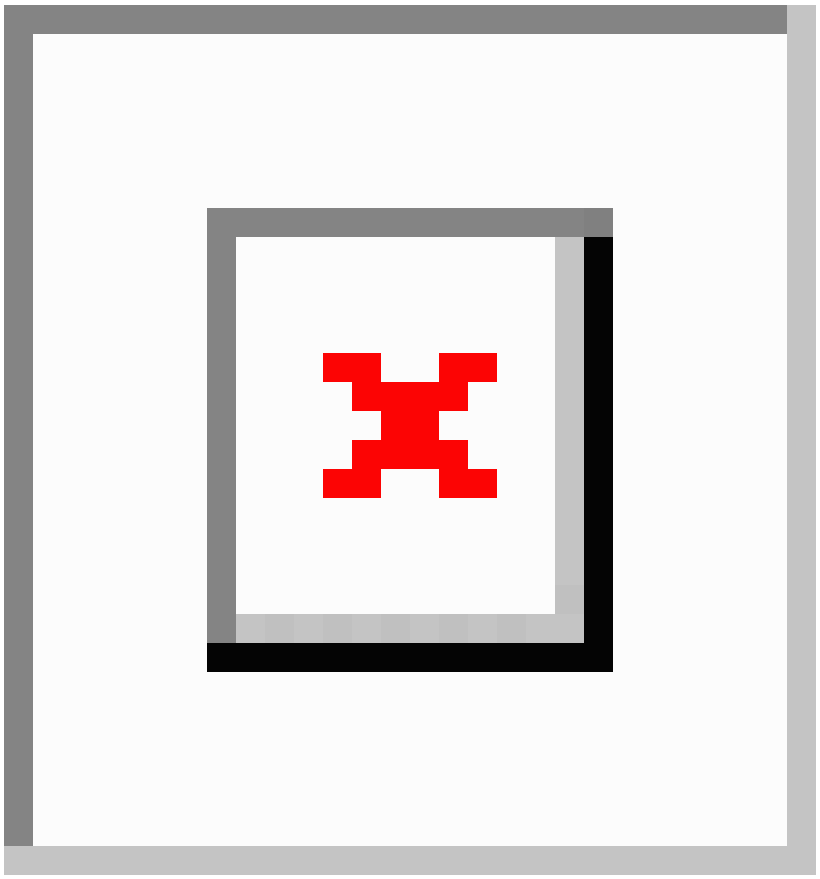
- 각 A 또는 AAAA 레코드에 여러 PAT 규칙을 적용할 수 있으며 사용할 PAT 규칙이 모호하므로 PAT에는 DNS 재작성이 적용되지 않습니다.
- 수동 NAT 규칙을 구성할 때 소스 주소와 대상 주소를 모두 지정하는 경우에는 DNS 수정을 구성할 수 없습니다. A와 B를 비교하여 전송하는 경우 이러한 종류의 규칙에는 잠재적으로 단일 주소에 다른 변환이 있을 수 있습니다. 따라서 이는 DNS 회신 내부의 IP 주소를 정확한 2회 NAT 규칙에 대해 올바르게 확인할 수 없습니다. DNS 회신에는 DNS 요청을 표시한 패킷에 어떤 source/destination 주소 조합이 있었는지에 대한 정보가 포함되어 있지 않습니다.
- DNS 쿼리 및 응답을 재작성하려면 NAT 규칙에 대해 DNS NAT 재작성을 활성화하여 DNS 애플리케이션 검사를 활성화해야 합니다. 기본적으로 DNS NAT 재작성이 활성화된 DNS 검사는 글로벌로 적용되므로 검사 구성을 변경하지 않아도 됩니다.
- DNS 재작성은 실제로 NAT 규칙이 아니라 xlate 항목에서 수행됩니다. 따라서 동적 규칙에 대한 xlate가 없으면 재작성을 정확히 수행할 수 없습니다. 고정 NAT에 대해서는 동일한 문제가 발생하지 않습니다.
- DNS 재작성에서는 DNS 동적 업데이트 메시지(opcode 5)를 재작성하지 않습니다.

다음 항목에서는 NAT 규칙의 DNS 재작성 예를 제공합니다.

DNS64 회신 수정

다음 그림은 외부 IPv4 네트워크의 FTP 서버 및 DNS 서버를 보여줍니다. 시스템은 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 IPv6 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.200.225로 응답합니다.

내부 사용자가 ftp.cisco.com(2001:DB8::D1A5:C8E1, 여기서 D1A5:C8E1은 209.165.200.225에 해당하는 IPv6 주소)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다. 이 예에는 DNS 서버용 고정 NAT 변환 및 내부 IPv6 호스트용 PAT 규칙도 포함되어 있습니다.



시작하기 전에

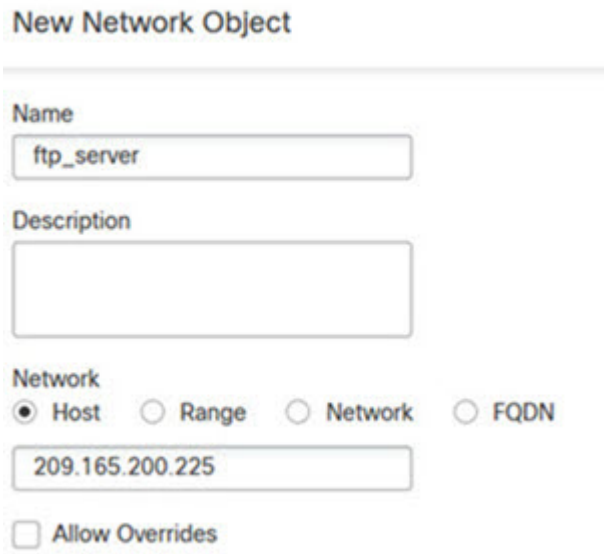
디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** FTP 서버, DNS 서버, 내부 네트워크 및 PAT 풀용 네트워크 개체를 생성합니다.

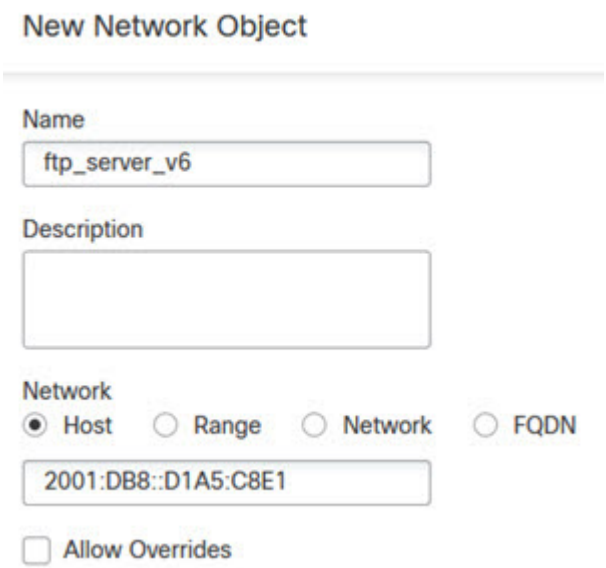
a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 실제 FTP 서버 주소를 정의합니다.

네트워크 개체의 이름을 ftp_server와 같이 지정하고 호스트 주소 209.165.200.225를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.
e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 FTP 서버의 변환된 IPv6 주소를 정의합니다.

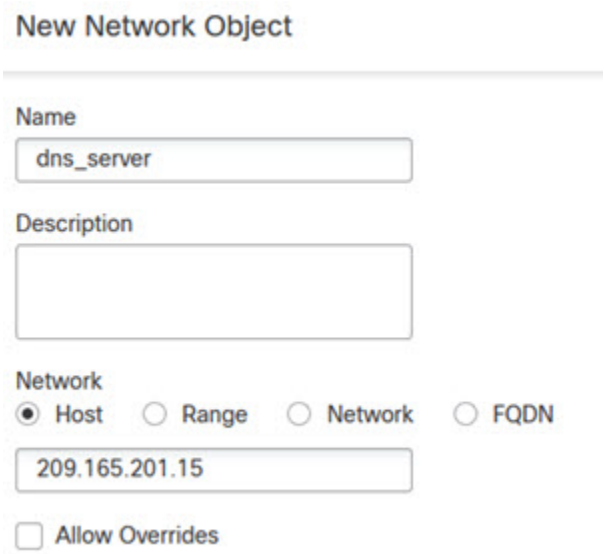
네트워크 개체의 이름을 ftp_server_v6와 같이 지정하고 호스트 주소 2001:DB8::D1A5:C8E1을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

g) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 DNS 서버의 실제 주소를 정의합니다.

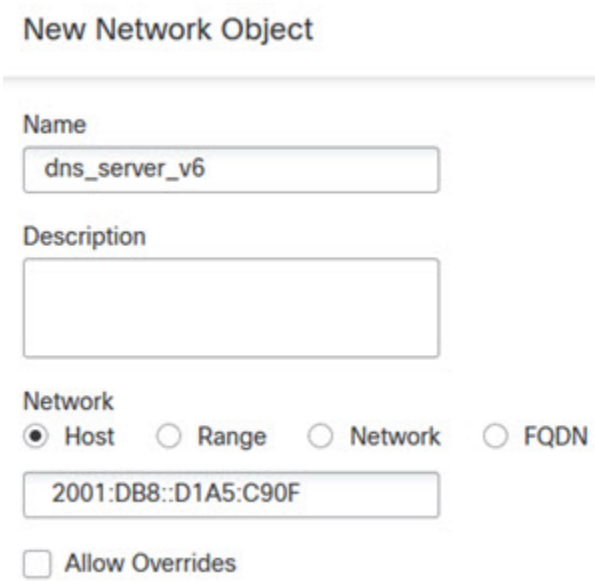
네트워크 개체의 이름을 dns_server와 같이 지정하고 호스트 주소 209.165.201.15를 입력합니다.



h) **Save(**저장**)**를 클릭합니다.

i) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 DNS 서버의 변환된 IPv6 주소를 정의합니다.

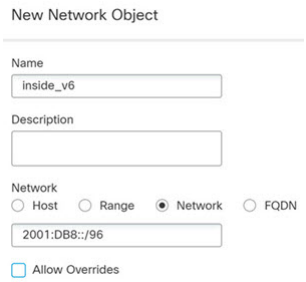
네트워크 개체의 이름을 dns_server_v6와 같이 지정하고 호스트 주소 2001:DB8::D1A5:C90F(D1A5:C90F는 209.165.201.15에 해당하는 IPv6)를 입력합니다.



j) **Save(**저장**)**를 클릭합니다.

k) **Add Network(**추가 네트워크**)** > **Add Object(**개체 추가**)**를 클릭하고 내부 IPv6 네트워크를 정의합니다.

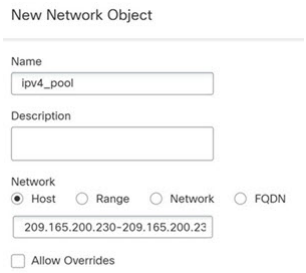
네트워크 개체의 이름을 inside_v6과 같이 지정하고 네트워크 주소 2001:DB8::/96을 입력합니다.



l) **Save(**저장**)**를 클릭합니다.

m) **Add Network(**추가 네트워크**)** > **Add Object(**개체 추가**)**를 클릭하고 내부 IPv6 네트워크에 대한 IPv4 PAT 풀을 정의합니다.

네트워크 개체의 이름을 지정하고(예: ipv4_pool) 네트워크 범위 209.165.200.230-209.165.200.235를 입력합니다.



n) **Save(**저장**)**를 클릭합니다.

단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

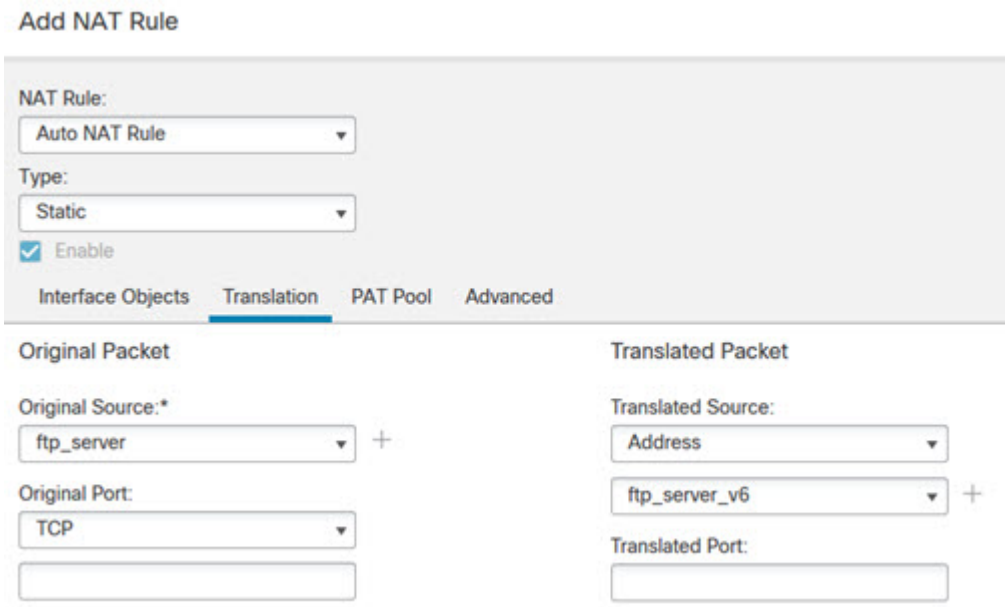
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = outside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = ftp_server 네트워크 개체.

• 번역 된 원본 > 주소 = ftp_server_v6 네트워크 개체.



f) **Advanced(**고급**)**에서 다음 옵션을 선택합니다.

• **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 회신 변환**)**.

• **Net to Net Mapping(**네트워크 대 네트워크 매핑**)**(일대일 NAT46 변환이므로).

g) **OK(**확인**)**를 클릭합니다.

단계 **3** DNS 서버용 고정 NAT 규칙을 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

• **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.

• 유형 = 고정

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

• **Source Interface Objects(**소스 인터페이스 개체**)** = outside.

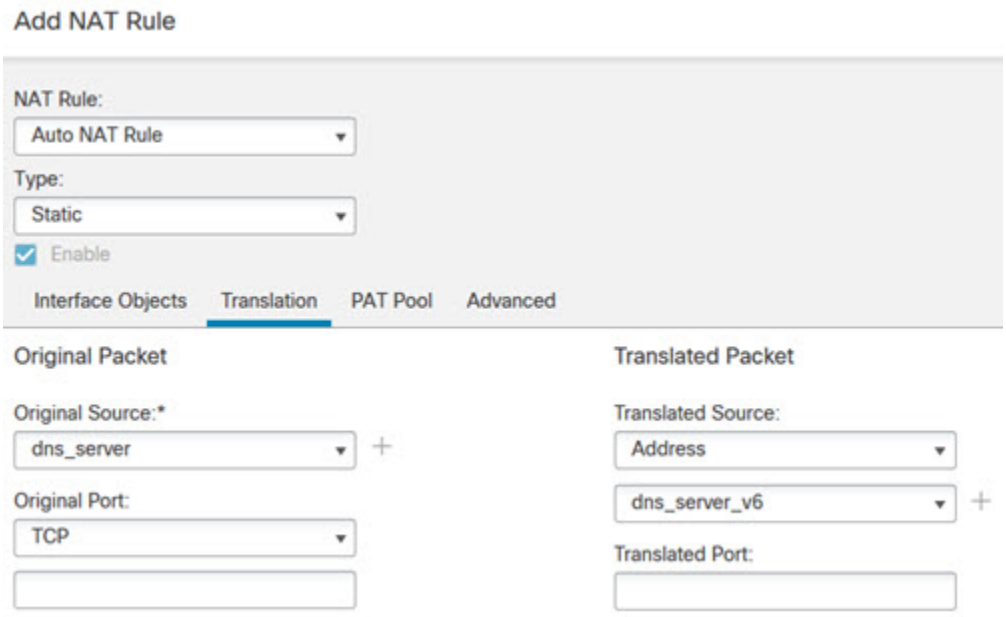
• **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

d) **Translation(**변환**)**에서 다음을 구성합니다.

• 원본 소스 = dns_server 네트워크 개체.

• **Translated Source(**변환된 소스**)** > **Address(**주소**)** = dns_server_v6 네트워크 개체.

e) **Advanced(**고급**)**에서 **Net to Net Mapping(**네트워크 대 네트워크 매핑**)**을 선택합니다. 일대일 NAT46 변환이기 때문입니다.



f) **OK(**확인**)**를 클릭합니다.

단계 **4** 내부 IPv6 네트워크용 PAT 풀 규칙을 통해 동적 NAT를 구성합니다.

a) **Add Rule(**규칙 추가**)**을 클릭합니다.

b) 다음 속성을 구성합니다.

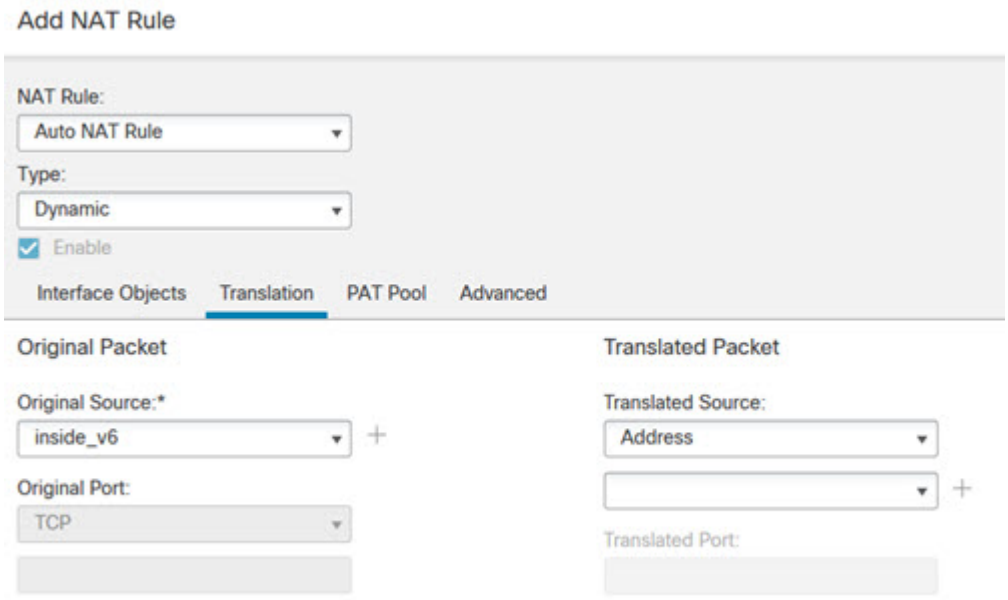
- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 동적

c) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

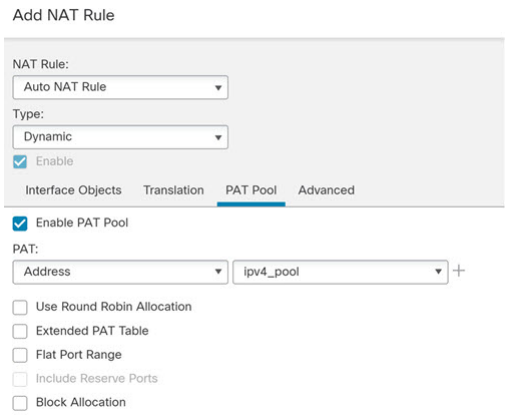
d) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = inside_v6 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = 이 필드를 비워 둡니다.



e) **PAT Pool(PAT** 풀**)**에서 다음을 구성합니다.

- **Enable PAT Pool(PAT** 풀 활성화**)** = 이 옵션을 선택합니다.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ipv4_pool 네트워크 개체.



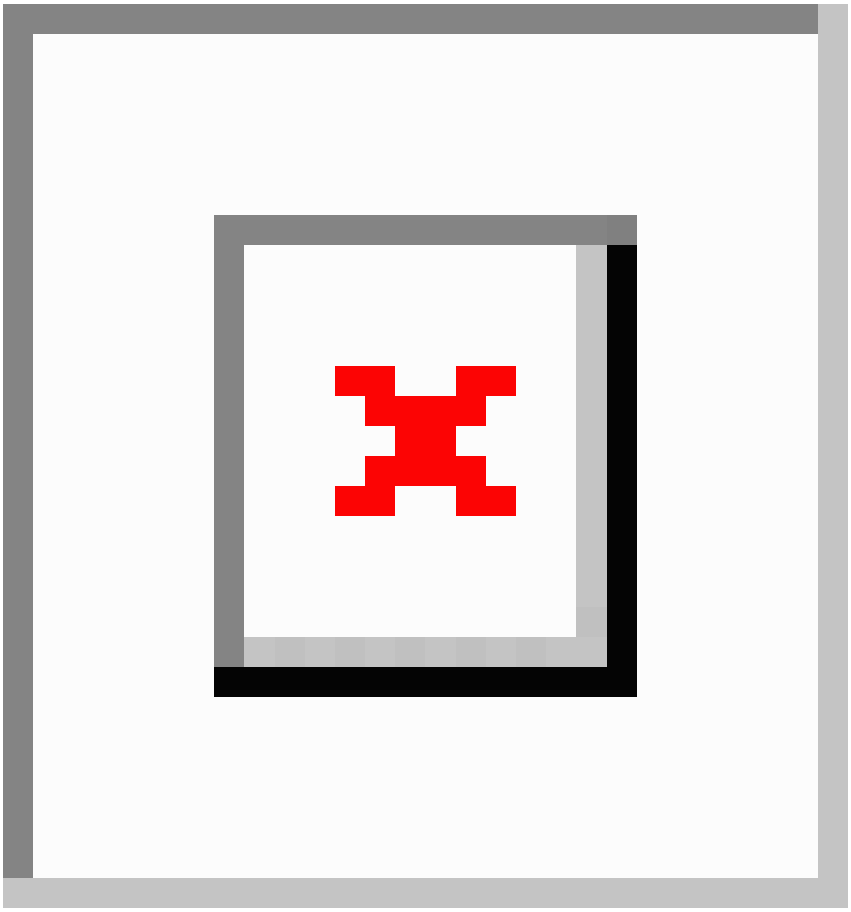
f) **OK(**확인**)**를 클릭합니다.

DNS 회신 수정, 외부의 DNS 서버

다음 그림은 인터페이스 외부에서 액세스할 수 있는 DNS 서버를 보여줍니다. ftp.cisco.com 서버는 내부 인터페이스에 있습니다. ftp.cisco.com 실제 주소(10.1.3.14)를 외부 네트워크에서 보이는 매핑된 주소(209.165.201.10)로 고정 변환하도록 NAT를 구성하십시오.

이 경우, 실제 주소를 사용하여 ftp.cisco.com에 액세스할 수 있는 내부 사용자가 DNS 서버에서 실제 주소(매핑된 주소가 아님)를 받을 수 있도록 고정 규칙에 대한 DNS 회신 수정을 사용할 수 있습니다.

내부 호스트가 ftp.cisco.com 주소에 DNS 요청을 전송하면, DNS 서버는 매핑된 주소(209.165.201.10)로 회신합니다. 시스템은 내부 서버에 대한 고정 규칙을 참조하여 DNS 회신에 있는 주소를 10.1.3.14로 변환합니다. DNS 회신 수정을 활성화하지 않으면 내부 호스트는 ftp.cisco.com에 직접 액세스하는 대신 트래픽을 209.165.201.10으로 전송하려고 시도하게 됩니다.



시작하기 전에

디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

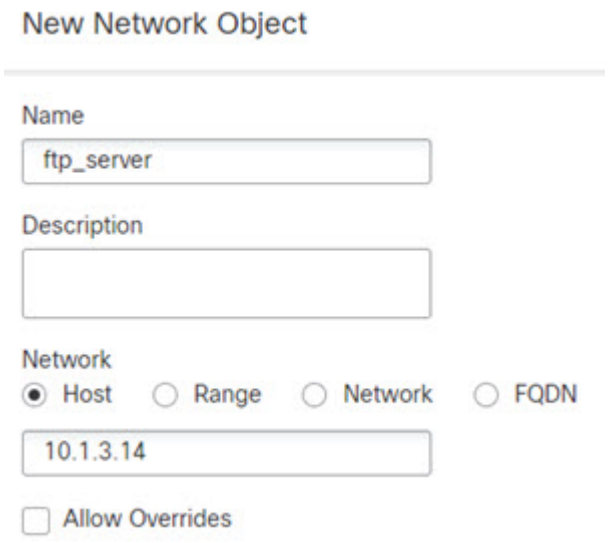
단계 **1** FTP 서버용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.

c) 실제 FTP 서버 주소를 정의합니다.

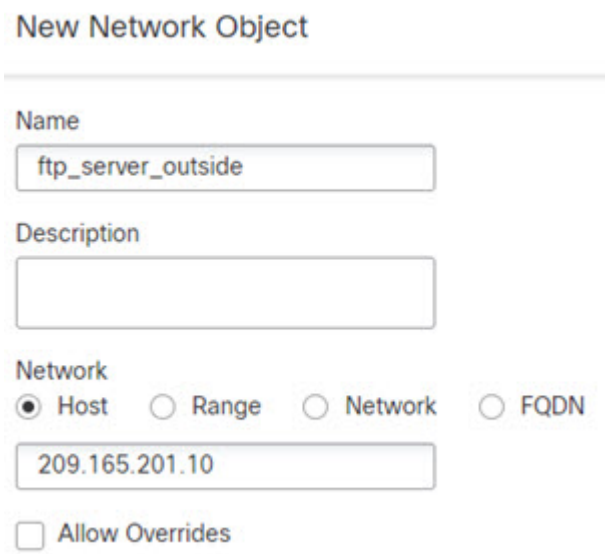
네트워크 개체의 이름을 ftp_server와 같이 지정하고 호스트 주소 10.1.3.14를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 FTP 서버의 변환된 주소를 정의합니다.

네트워크 개체의 이름을 ftp_server_outside와 같이 지정하고 호스트 주소 209.165.201.10을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT** 규칙**)** = Auto NAT Rule.
- 유형 = 고정

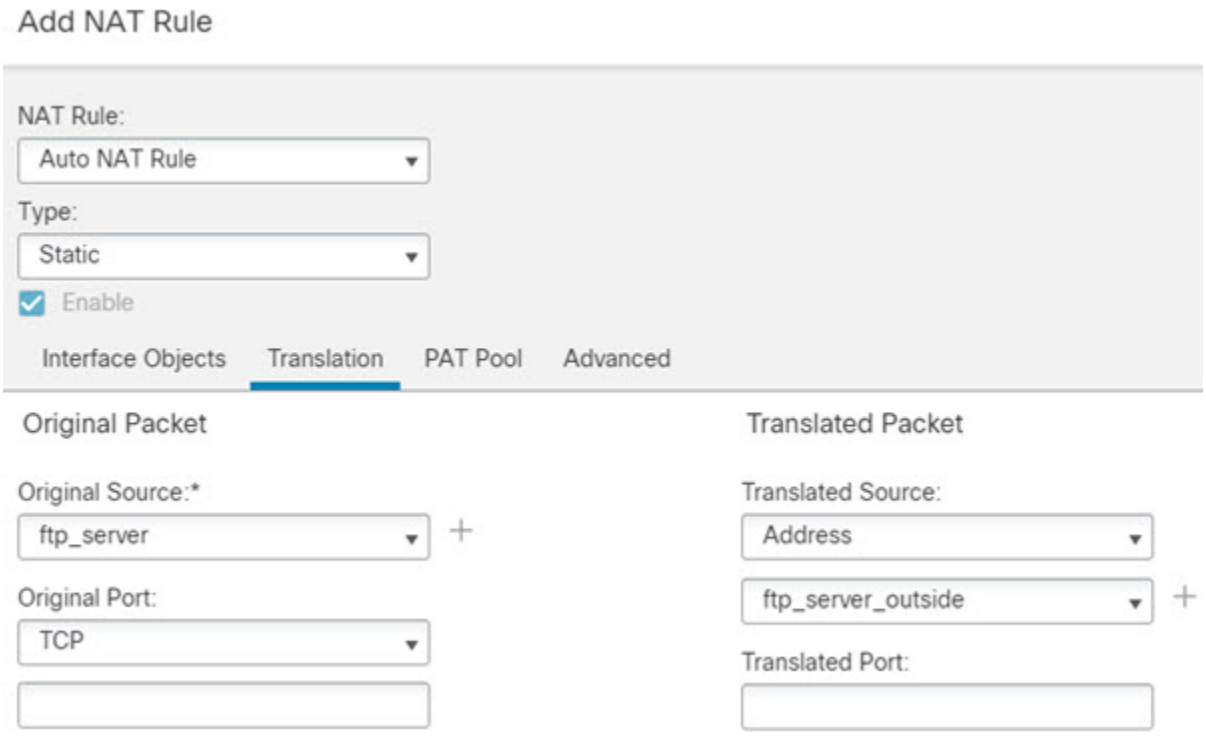
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = inside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = outside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = ftp_server 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ftp_server_outside 네트워크 개체.

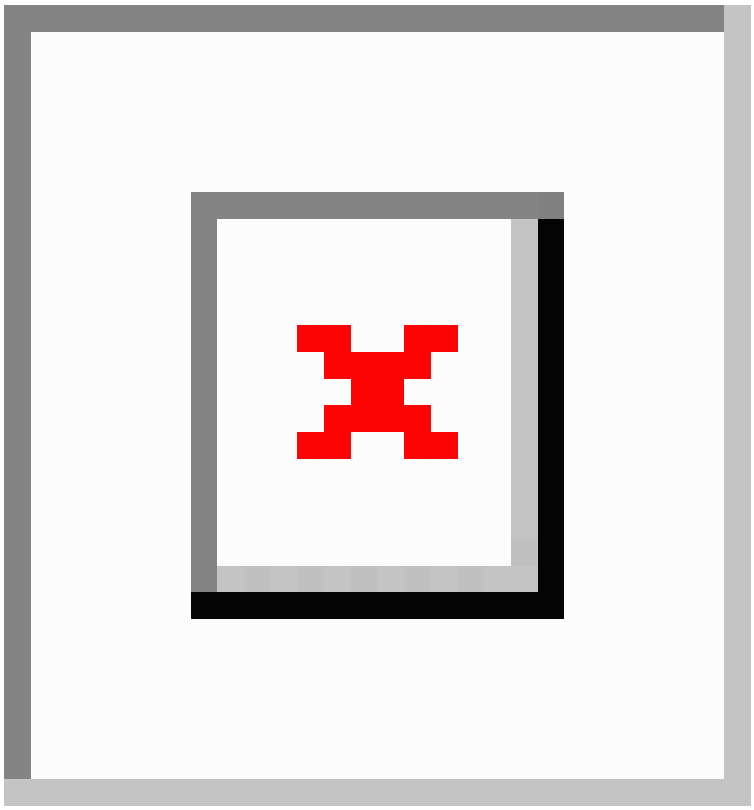
f) **Advanced(**고급**)**에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



g) **OK(**확인**)**를 클릭합니다.

DNS 회신 수정, 호스트 네트워크의 DNS 서버

다음 그림은 외부의 FTP 서버 및 DNS 서버를 보여줍니다. 시스템은 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.20.10으로 응답합니다. 내부 사용자가 ftp.cisco.com(10.1.2.56)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다.



시작하기 전에

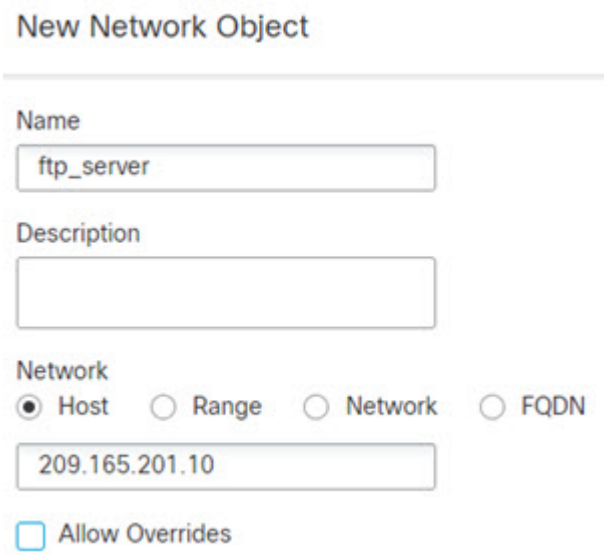
디바이스에 대한 인터페이스가 포함된 인터페이스 개체(보안 영역 또는 인터페이스 그룹)가 있는지 확인합니다. 이 예제에서는 인터페이스 개체가 **inside** 및 **outside**라는 이름의 보안 영역이라고 가정합니다. 인터페이스 개체를 구성하려면 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택한 다음 **Interface(**인터페이스**)**를 선택합니다.

프로시저

단계 **1** FTP 서버용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭합니다.
c) 실제 FTP 서버 주소를 정의합니다.

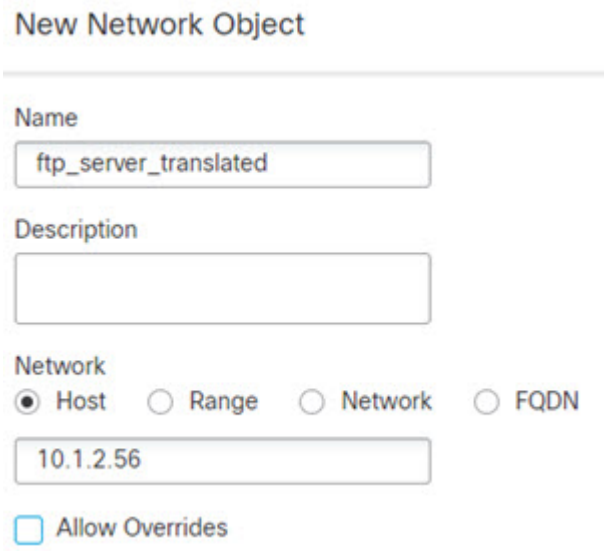
네트워크 개체의 이름을 ftp_server와 같이 지정하고 호스트 주소 209.165.201.10를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

e) **Add Network(**네트워크 추가**)** > **Add Object(**개체 추가**)**를 클릭하고 FTP 서버의 변환된 주소를 정의합니다.

네트워크 개체의 이름을 ftp_server_translated와 같이 지정하고 호스트 주소 10.1.2.56을 입력합니다.



f) **Save(**저장**)**를 클릭합니다.

단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Devices(**디바이스**)** > **NAT**를 선택하고 FTD NAT 정책을 생성하거나 수정합니다.

b) **Add Rule(**규칙 추가**)**을 클릭합니다.

c) 다음 속성을 구성합니다.

- **NAT Rule(NAT 규칙)** = Auto NAT Rule.
- 유형 = 고정

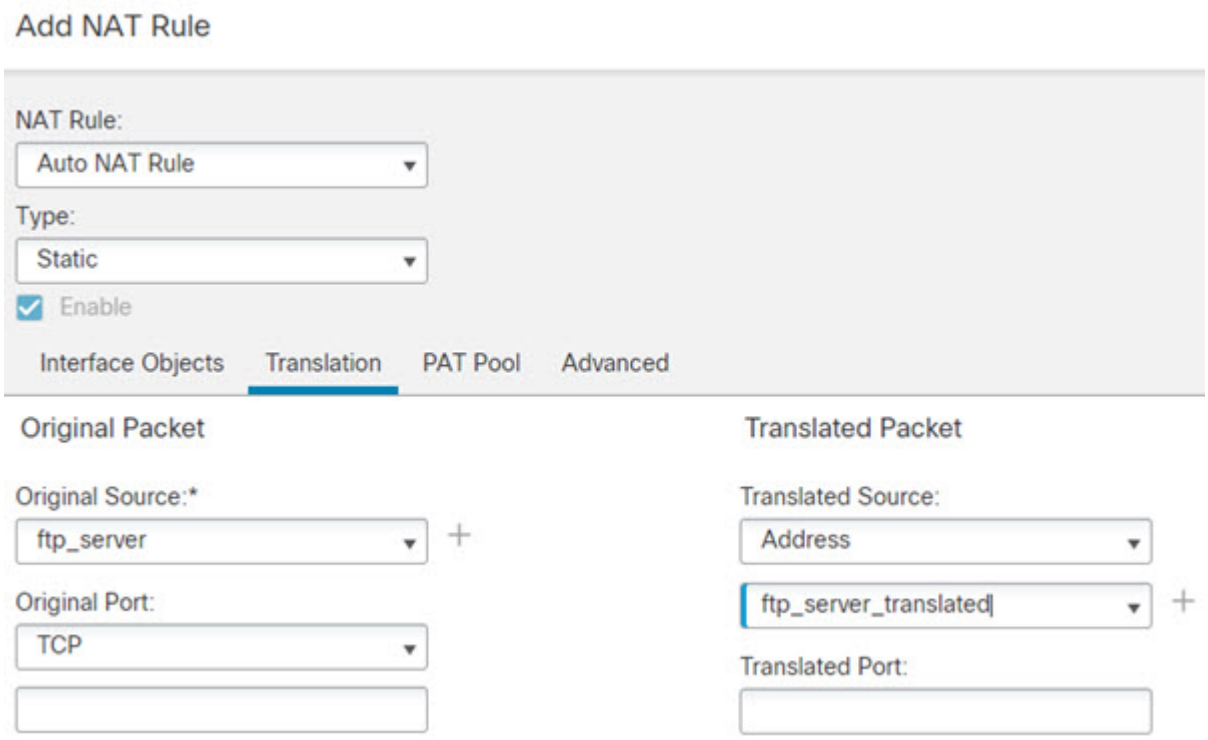
d) **Interface Objects(**인터페이스 개체**)**에서 다음을 구성합니다.

- **Source Interface Objects(**소스 인터페이스 개체**)** = outside.
- **Destination Interface Objects(**대상 인터페이스 개체**)** = inside.

e) **Translation(**변환**)**에서 다음을 구성합니다.

- **Original Source(**원본 소스**)** = ftp_server 네트워크 개체.
- **Translated Source(**변환된 소스**)** > **Address(**주소**)** = ftp_server_translated 네트워크 개체.

f) **Advanced(**고급**)**에서 **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)**을 선택합니다.



g) **OK(**확인**)**를 클릭합니다.

FTD NAT 기록

기능	버전	세부 사항
Firepower Threat Defense에 대한 NAT(Network Address Translation).	6.0.1	Firepower Threat Defense에 대한 NAT 정책이 추가되었습니다. 신규/수정된 화면: Threat Defense가 **Devices(**디바이스**)** > **NAT** 페이지에 NAT 정책 유형으로 추가되었습니다. 지원되는 플랫폼: Firepower Threat Defense
Firepower Threat Defense용 NAT에서 네트워크 범위 개체에 대해 지원합니다.	6.1.0	해당되는 경우 Firepower Threat Defense NAT 규칙에서 네트워크 범위 개체를 사용할 수 있습니다.
통신 사업자급 NAT 개선 사항	6.5	통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 신규/수정된 화면: Firepower Threat Defense NAT 규칙의 NAT PAT Pool 탭에 **Block Allocation(**블록 할당**)** 옵션을 추가했습니다. 지원되는 플랫폼: Firepower Threat Defense
FTD NAT 규칙 테이블을 검색하고 필터링하는 기능.	6.7	이제 FTD NAT 정책에서 규칙을 검색하여 IP 주소, 포트, 개체 이름 등을 기준으로 규칙을 찾을 수 있습니다. 검색 결과에는 부분 일치 항목이 포함됩니다. 기준을 검색하면 규칙 테이블이 필터링되므로 일치하는 규칙만 표시됩니다. FTD NAT 정책을 편집할 때 규칙 테이블 위에 검색 필드를 추가했습니다.

기능	버전	세부 사항
클러스터링에서 PAT 주소 할당을 변경합니다. PAT 풀 **Flat Port Range(**플랫 포트 범위**)** 옵션은 이제 기본적으로 활성화되어 있으며 구성할 수 없습니다.	6.7	PAT 주소가 클러스터 멤버에 배포되는 방식이 변경되었습니다. 이전에는 주소가 클러스터의 멤버에 분산되었으므로 PAT 풀에는 클러스터 멤버당 최소 1개의 주소가 필요했습니다. 이제 제어 유닛은 각 PAT 풀 주소를 동일한 크기의 포트 블록으로 분할하여 클러스터 멤버에 분산시킵니다. 각 멤버에는 동일한 PAT 주소에 대한 포트 블록이 있습니다. 따라서 일반적으로 PAT에 필요한 연결의 양에 따라 PAT 풀의 크기를 하나의 IP 주소로 줄일 수 있습니다. 포트 블록은 1024~65535 범위에서 512 포트 블록에 할당됩니다. PAT 풀 규칙을 구성할 때 이 블록 할당에 예약된 포트 1 ~ 1023을 선택적으로 포함할 수 있습니다. 예를 들어, 4 노드 클러스터에서 각 노드는 PAT 풀 IP 주소당 16,384 개의 연결을 처리할 수 있는 32개 블록을 가져오며, PAT 풀 IP 주소당 모든 65535 연결을 처리하는 단일 노드와 비교됩니다. 이러한 변경의 일환으로, 독립형이든 클러스터에서 작동 중인지에 관계 없이 모든 시스템의 PAT 풀은 이제 1023 ~ 65535의 플랫 포트 범위를 사용합니다. 이전에는 PAT 풀 규칙에 **Flat Port Range(**플랫 포트 범위**)** 옵션을 포함하여 플랫 범위를 선택적으로 사용할 수 있었습니다. 이제 **Flat Port Range(**플랫 포트 범위**)** 옵션이 무시됩니다. PAT 풀이 항상 플랫 상태입니다. 선택적으로 **Include Reserved Ports(**예약된 포트 포함**)** 옵션을 선택하여 PAT 풀에 1 ~ 1023 포트 범위를 포함할 수 있습니다. 포트 블록 할당(**Block Allocation(**블록 할당**)** PAT 풀 옵션)을 구성하면 기본 512 포트 블록이 아닌 블록 할당 크기가 사용됩니다. 또한 클러스터의 시스템에 대한 PAT 풀에 대해 확장 PAT를 구성할 수 없습니다.