firepower Management Center로 헤어핀 구성

목차

소개

이 문서에서는 FMC(Firepower Management Center)를 사용하여 FTD(Firepower Threat Defense)에서 헤어핀을 성공적으로 구성하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(Firepower Management Center)
- FTD(Firepower Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower Management Center Virtual 7.2.4
- Firepower Threat Defense Virtual 7.2.4.

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

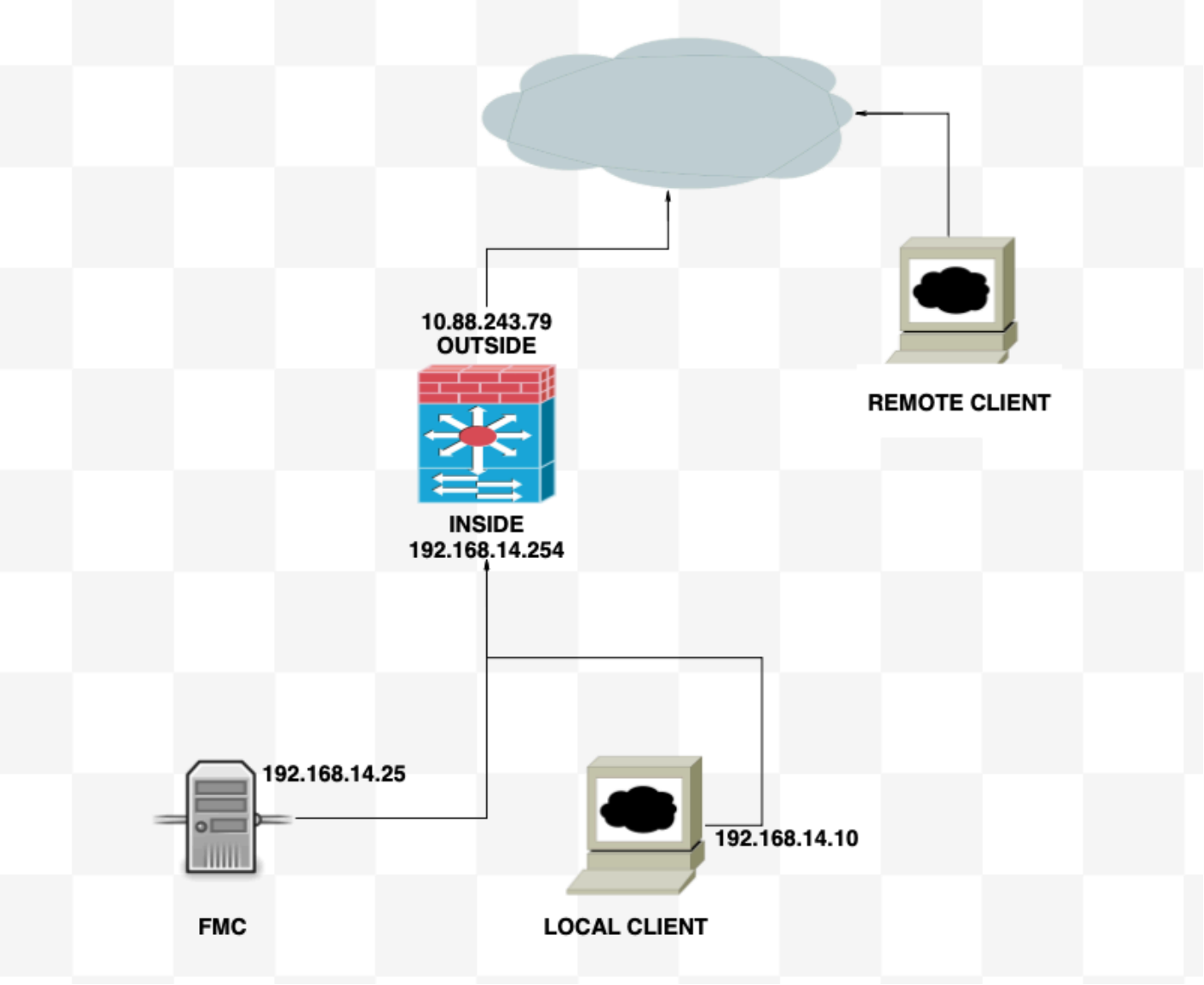
구성

클라이언트의 트래픽이 라우터(또는 NAT를 구현하는 방화벽)로 이동한 다음 서버의 사설 IP 주소에 액세스하기 위해 변환 후 내부 네트워크로 헤어핀처럼 돌아가기 때문에 헤어핀이라는 용어가 사용됩니다.

이 기능은 로컬 네트워크 내에서 웹 호스팅과 같은 네트워크 서비스에 유용합니다. 로컬 네트워크의 사용자는 외부 사용자와 동일한 URL 또는 IP 주소를 사용하여 내부 서버에 액세스해야 합니다. 요청이 로컬 네트워크 내부에서 시작되는지 아니면 외부에서 시작되는지에 관계없이 리소스에 대한 균일한 액세스를 보장합니다.

이 예에서는 FTD의 외부 인터페이스의 IP를 통해 FMC에 액세스해야 합니다

다이어그램



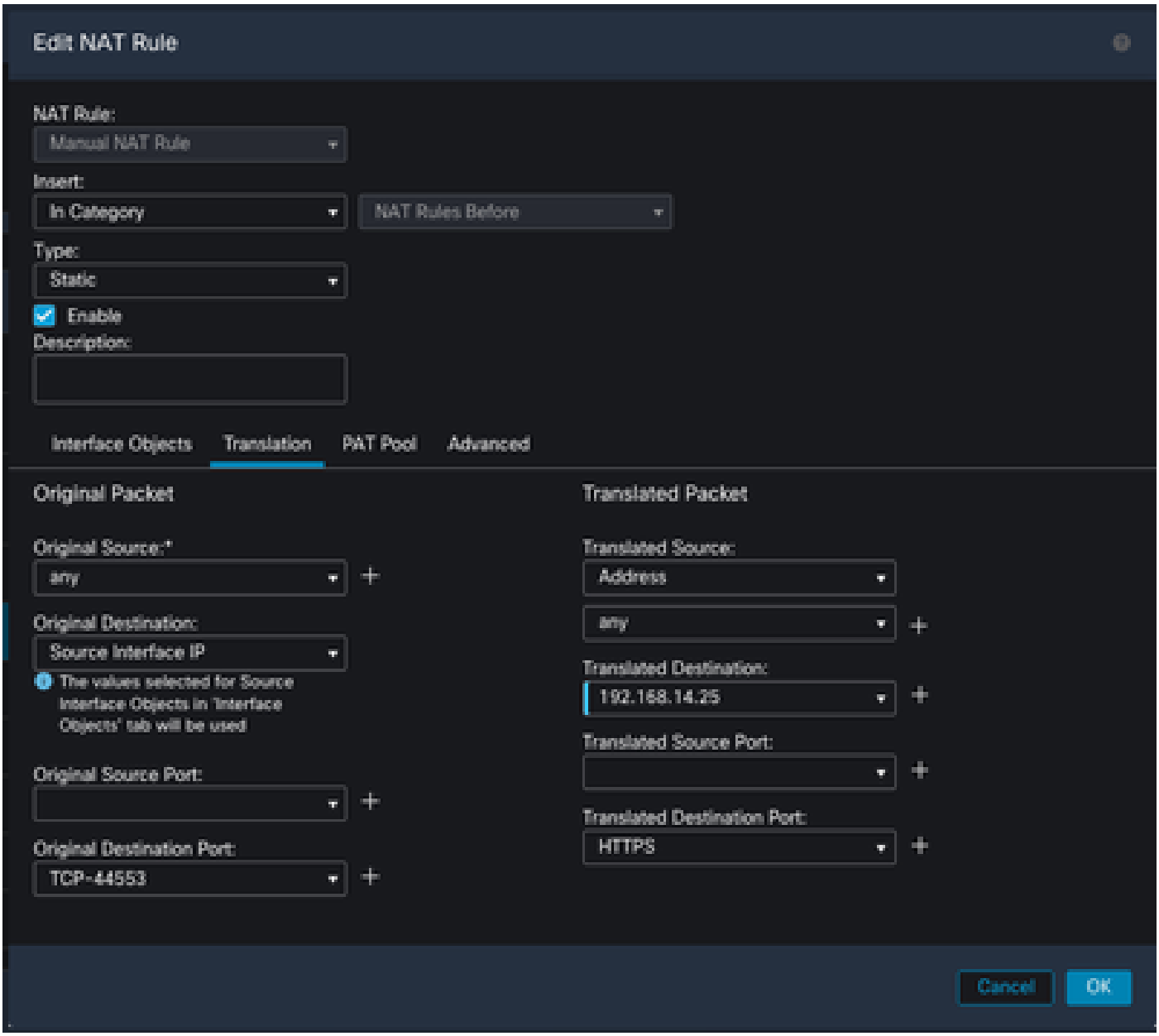
1단계. Outside-Inside Nat 구성

첫 번째 단계로 고정 NAT를 구성해야 합니다. 이 예에서 대상 IP 및 대상 포트는 외부 인터페이스의

IP를 사용하여 변환되며 포트 대상은 44553.

FMC에서 Device(디바이스) > NAT로 이동하여 기존 정책을 생성하거나 수정한 다음 Add Rule(규칙 추가) 상자를 클릭합니다.

- NAT 규칙: 수동 Nat 규칙
- 원래 소스: 모두
- Original Destination(원래 대상): Source Interface IP
- 원래 대상 포트: 44553
- 변환된 대상: 192.168.14.25
- 변환된 목적지 포트: 443



정책을 구성합니다. Policies(정책) > Access Control(액세스 제어)로 이동하여 기존 정책을 생성하거나 수정한 다음 Add Rule(규칙 추가) 상자를 클릭합니다.

소스 영역: 외부

대상 영역: 내부

소스 네트워크: 모두

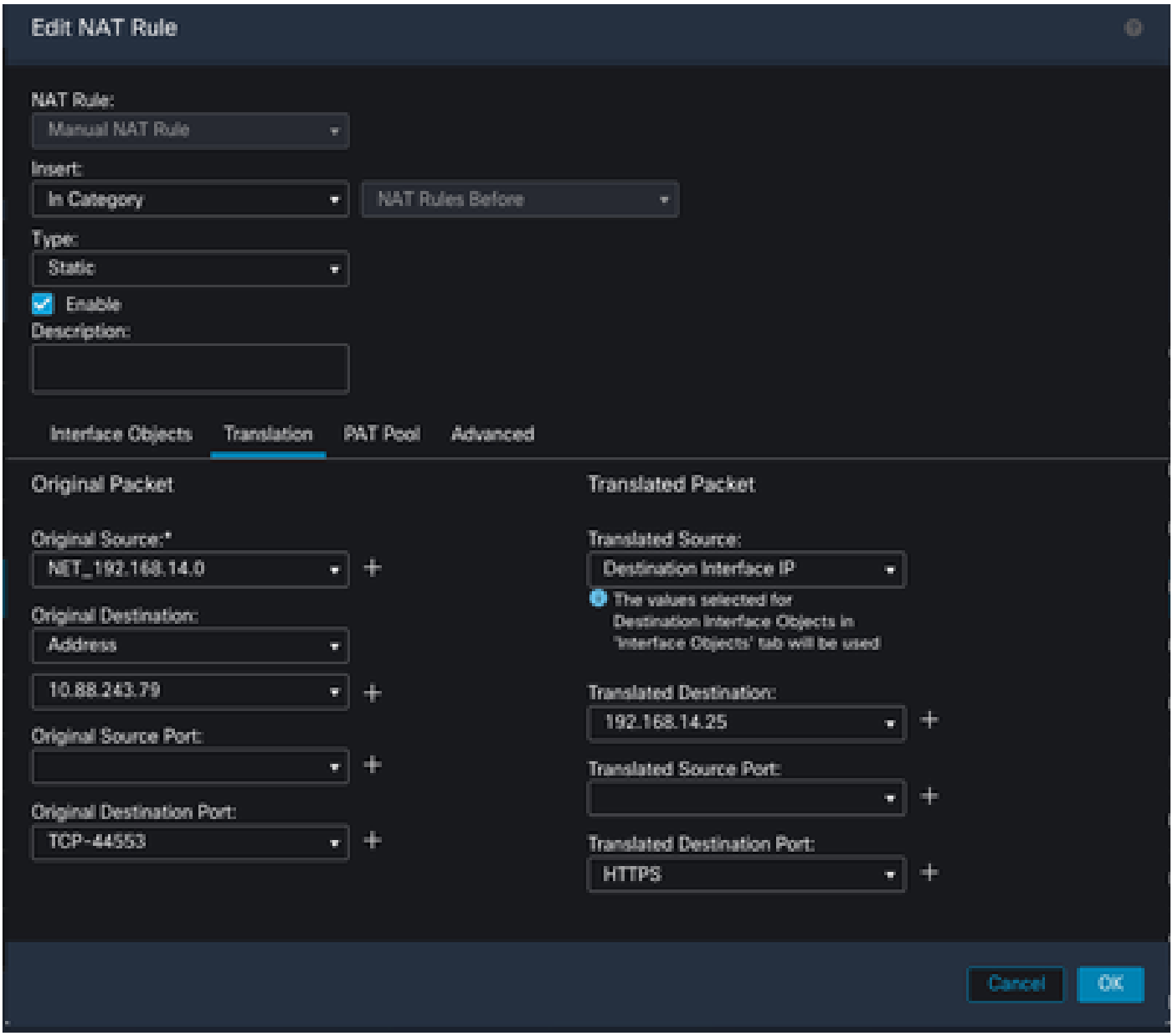
대상 네트워크: 10.88.243.79

2단계. Inside-Inside Nat(헤어핀) 구성

두 번째 단계로 고정 NAT를 내부에서 내부로 구성해야 합니다. 이 예에서는 대상 IP 및 대상 포트가 외부 인터페이스의 IP가 있는 객체를 사용하여 변환되고 대상 포트가 44553.

FMC에서 Device(디바이스) > NAT로 이동하여 기존 정책을 수정한 다음 Add Rule(규칙 추가) 상자를 클릭합니다.

- NAT 규칙: 수동 Nat 규칙
- 원본: 192.168.14.0/24
- Original Destination(원래 대상): 주소 10.88.243.79
- 원래 대상 포트: 44553
- 변환된 소스: 대상 인터페이스 IP
- 변환된 대상: 192.168.14.25
- 변환된 목적지 포트: 443



정책을 구성합니다. Policies > Access Control로 이동하여 기존 정책을 수정한 다음 Add Rule 상자를 클릭합니다.

소스 영역: 모두

Destination Zone(대상 영역): 모두

소스 네트워크: 192.168.14.0/24

대상 네트워크: 10.88.243.79

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - la primera (1-4)					
1	nat-fmc	OUTSIDE	INSIDE	any	*Any*
2	Hairpin	*Any*	*Any*	NET_192.168.14	10.88.243.79

다음을 확인합니다.

로컬 클라이언트에서 대상 IP 및 대상 포트로 텔넷을 수행합니다.

이 오류 메시지 "telnet unable to connect to remote host: Connection timed out(텔넷에서 원격 호스트에 연결할 수 없음: 연결 시간 초과)" 프롬프트가 표시되면 컨피그레이션 중 특정 지점에서 오류가 발생한 것입니다.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

하지만 Connected(연결됨)라고 표시되어 있으면 컨피그레이션이 성공했습니다.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

문제 해결

NAT(Network Address Translation)에 문제가 있는 경우 이 단계별 가이드를 사용하여 일반적인 문제를 해결하고 해결하십시오.

1단계: NAT 규칙 컨피그레이션 확인

- NAT 규칙 검토: 모든 NAT 규칙이 FMC에서 올바르게 구성되었는지 확인합니다. 소스 및 목적지 IP 주소와 포트가 정확한지 확인합니다.
- Interface Assignment(인터페이스 할당): 소스 인터페이스와 목적지 인터페이스가 모두 NAT 규칙에서 올바르게 할당되었는지 확인합니다. 매핑이 잘못되면 트래픽이 제대로 변환되거나 라우팅되지 않을 수 있습니다.
- NAT 규칙 우선순위: NAT 규칙이 동일한 트래픽과 일치할 수 있는 다른 규칙의 맨 위에 있는지 확인합니다. FMC의 규칙은 순서대로 처리되므로, 위에 있는 규칙이 우선권을 갖습니다.

2단계: ACL(액세스 제어 규칙) 확인

- ACL 검토: ACL이 NAT 트래픽 허용에 적합한지 확인하려면 ACL을 선택합니다. 변환된 IP 주

소를 인식하도록 ACL을 구성해야 합니다.
- 규칙 순서: 액세스 제어 목록이 올바른 순서인지 확인하십시오. NAT 규칙과 마찬가지로 ACL은 위에서 아래로 처리되며 트래픽과 일치하는 첫 번째 규칙이 적용됩니다.
- Traffic Permissions(트래픽 권한): 내부 네트워크에서 변환된 목적지로의 트래픽을 허용하기 위한 적절한 액세스 제어 목록이 있는지 확인합니다. 규칙이 누락되거나 잘못 구성된 경우 원하는 트래픽을 차단할 수 있습니다.

3단계: 추가 진단

- Use Diagnostic Tools(진단 도구 사용): FMC에서 제공되는 진단 도구를 활용하여 디바이스를 통과하는 트래픽을 모니터링하고 디버깅합니다. 여기에는 실시간 로그 및 연결 이벤트 보기가 포함됩니다.
- Restart Connections(연결 재시작): 경우에 따라 기존 연결은 재시작될 때까지 NAT 규칙 또는 ACL에 대한 변경 사항을 인식할 수 없습니다. 새 규칙을 강제로 적용하려면 기존 연결을 지우는 것이 좋습니다.

LINA에서:

```
<#root>

firepower#

 clear xlate
```

- Verify Translation(변환 확인): FTD 디바이스로 작업하는 경우 명령줄에서 show xlate 및 show nat와 같은 명령을 사용하여 NAT 변환이 예상대로 수행되고 있는지 확인합니다.

LINA에서:

```
<#root>

firepower#

 show nat
```

```
<#root>

firepower#

 show xlate
```

이 번역에 관하여

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