FMC에서 Packet Tracer Tool을 사용하여 패킷 재생

목차

소개

이 문서에서는 FMC GUI Packet Tracer 툴을 사용하여 FTD 디바이스에서 패킷을 재생하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- firepower 기술에 대한 지식
- 방화벽을 통과하는 패킷 흐름에 대한 지식

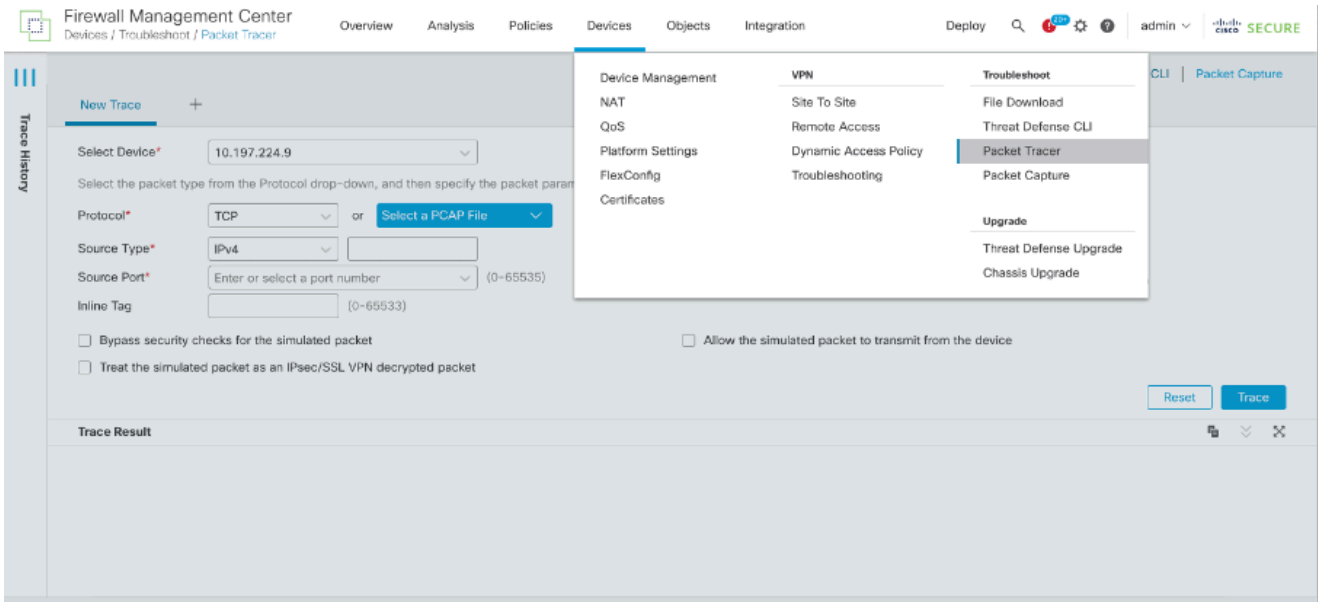
사용되는 구성 요소

- Cisco FMC(Secure Firewall Management Center) 및 Cisco FTD(Firewall Threat Defense) 버전 7.1 이상
- pcap 형식의 패킷 캡처 파일

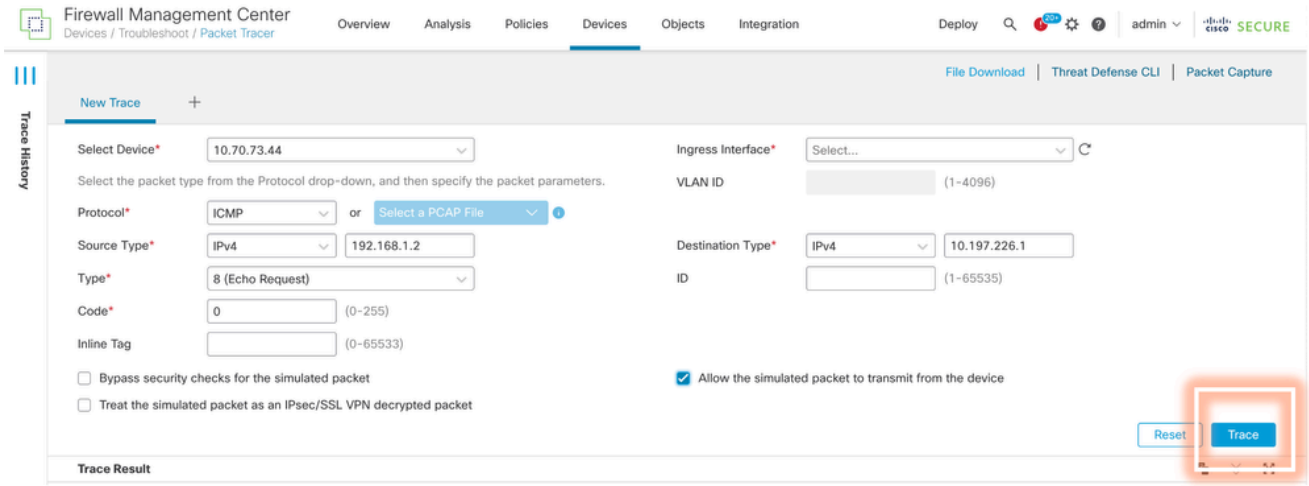
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

FMC에서 사용 가능한 패킷 추적기 툴을 사용하여 패킷 재생

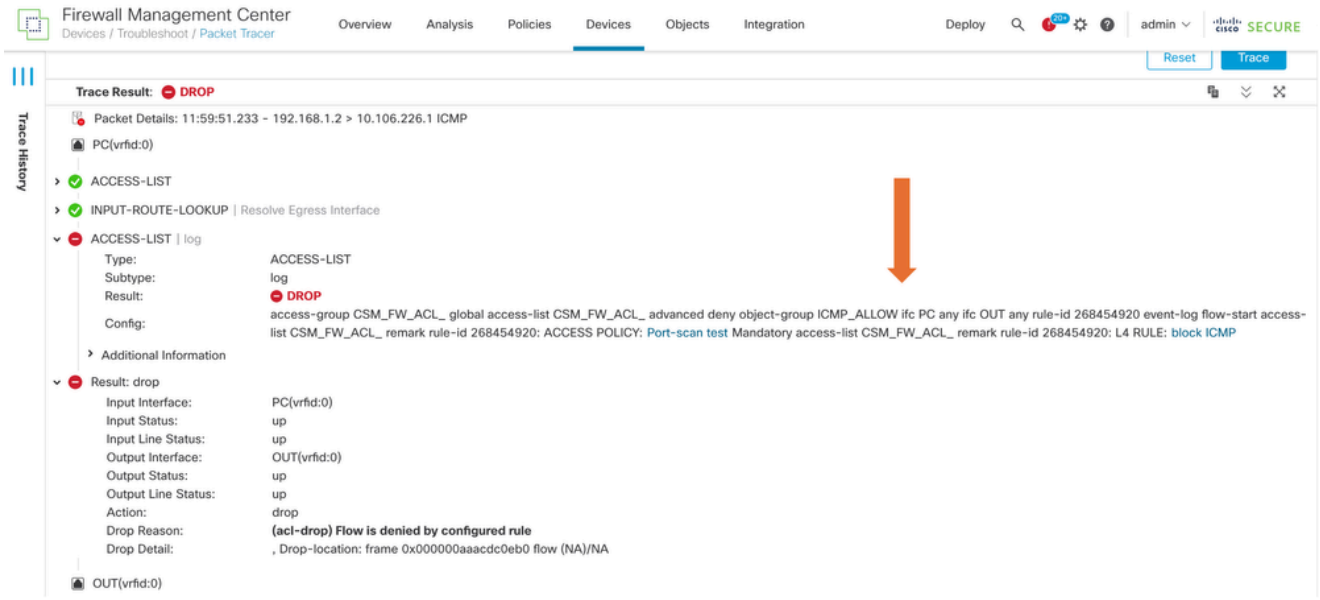
1. FMC GUI에 로그인합니다. Devices > Troubleshoot > Packet Tracer로 이동합니다.



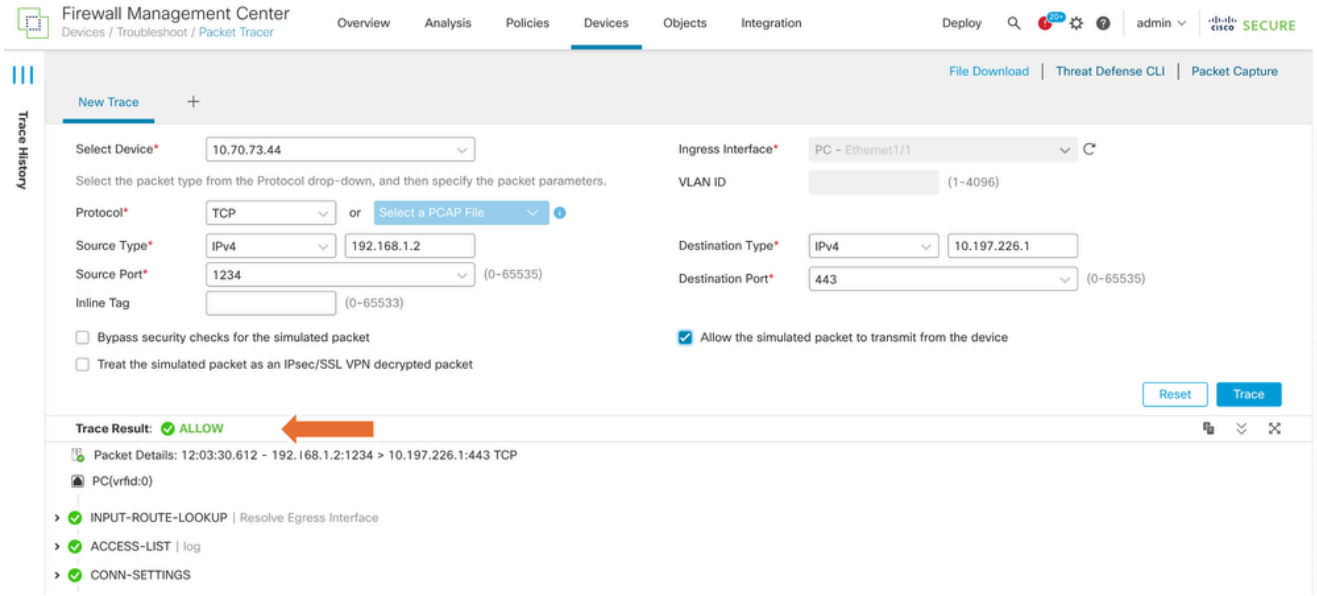
2. 소스, 목적지, 프로토콜, 인그레스 인터페이스에 대한 세부사항을 제공합니다. Trace(추적)를 클릭합니다.



3. 시뮬레이션된 패킷이 디바이스에서 전송되도록 허용 옵션을 사용하여 디바이스에서 이 패킷을 재생합니다.
4. ICMP 패킷을 삭제하도록 액세스 제어 정책에 구성된 규칙이 있으므로 패킷이 삭제되었는지 확인합니다.

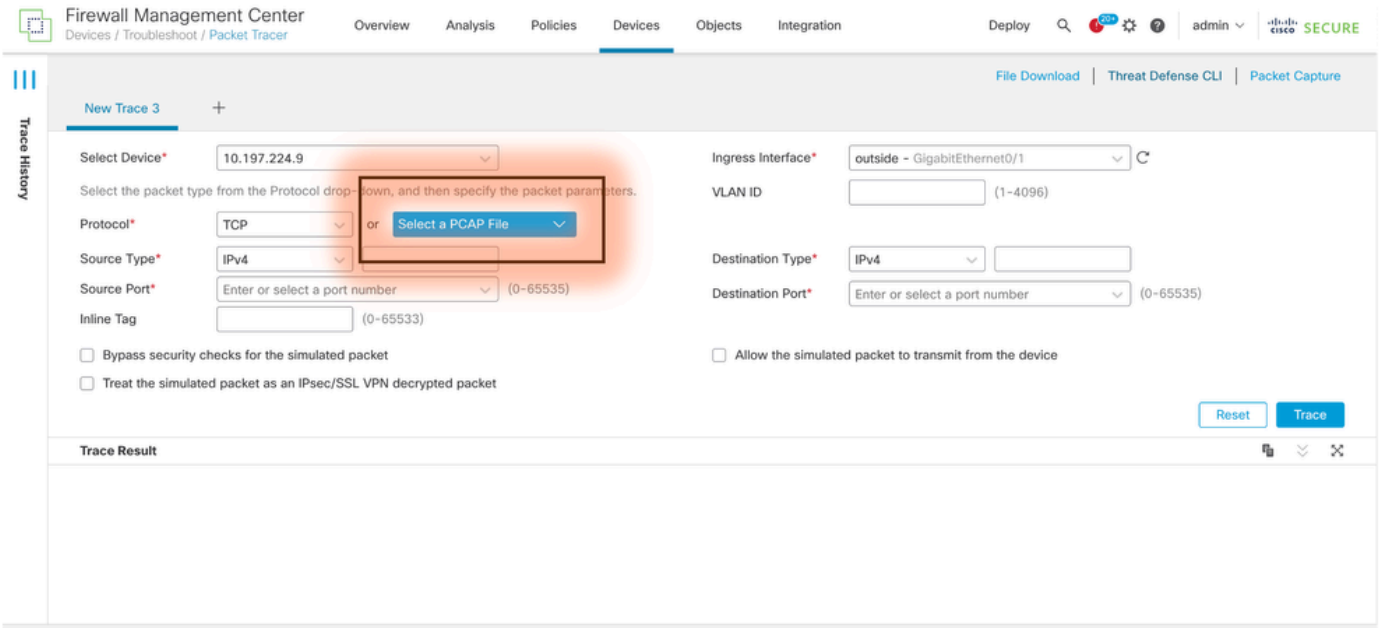


5. 이 패킷 추적기는 TCP 패킷과 함께 추적의 최종 결과입니다(표시된 대로).



PCAP 파일을 사용하여 패킷 재생

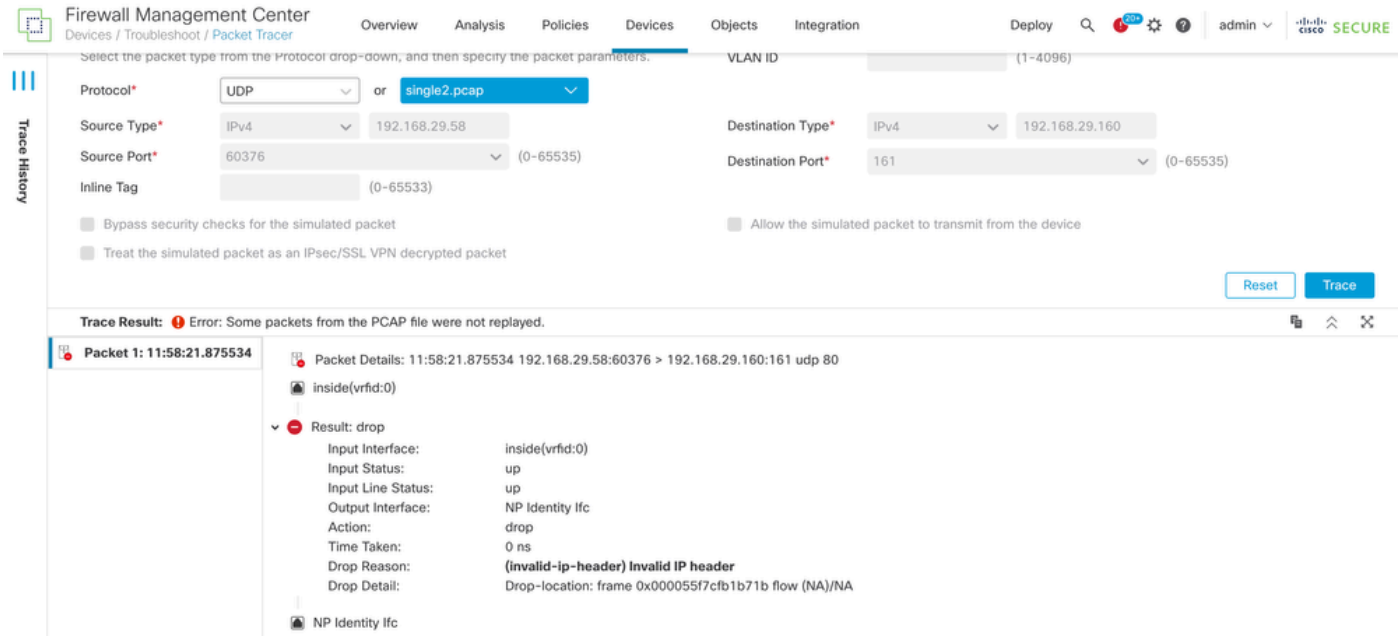
Select a PCAP File(PCAP 파일 선택) 버튼을 사용하여 pcap 파일을 업로드할 수 있습니다. 그런 다음 Ingress 인터페이스를 선택하고 Trace(추적)를 클릭합니다.



이 옵션 사용의 제한 사항

1. TCP/UDP 패킷만 시뮬레이션할 수 있습니다.
2. PCAP 파일에서 지원되는 최대 패킷 수는 100입니다.
3. Pcap 파일 크기는 1MB 미만이어야 합니다.
4. PCAP 파일 이름은 64자(확장자 포함)를 초과할 수 없으며 영숫자, 특수 문자(".", "-", "_") 또는 둘 다만 포함해야 합니다.
5. 현재 단일 플로우 패킷만 지원됩니다.

추적 3에서 삭제 이유를 잘못된 ip 헤더로 표시하고 있습니다.



관련 문서

패킷 캡처 및 추적기에 대한 자세한 내용은 Cisco Live Document를 참조하십시오.

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.