FMC를 통해 Snort 2에서 Snort 3으로 업그레이드

목차

소개

이 문서에서는 FMC(Firepower Manager Center)에서 Snort 2 및 Snort 3 버전에서 업그레이드하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 위협 방어
- Firepower 관리 센터
- Snort

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMC 7.0
- FTD 7.0

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.

배경 정보

Snort 3 기능은 Firepower Device Manager(FDM) 및 Cisco Defense Orchestrator(CDO)의 경우 6.7 릴리스에, Firepower Management Center(FMC)의 경우 7.0 릴리스에 추가되었습니다.

Snort 3.0은 다음과 같은 과제를 해결하도록 설계되었습니다.

1. 메모리 및 CPU 사용량 감소
2. HTTP 검사 효율성 향상
3. 더 빠른 컨피그레이션 로드 및 Snort 재시작
4. 프로그래밍 기능이 향상되어 기능을 더 빨리 추가할 수 있습니다.

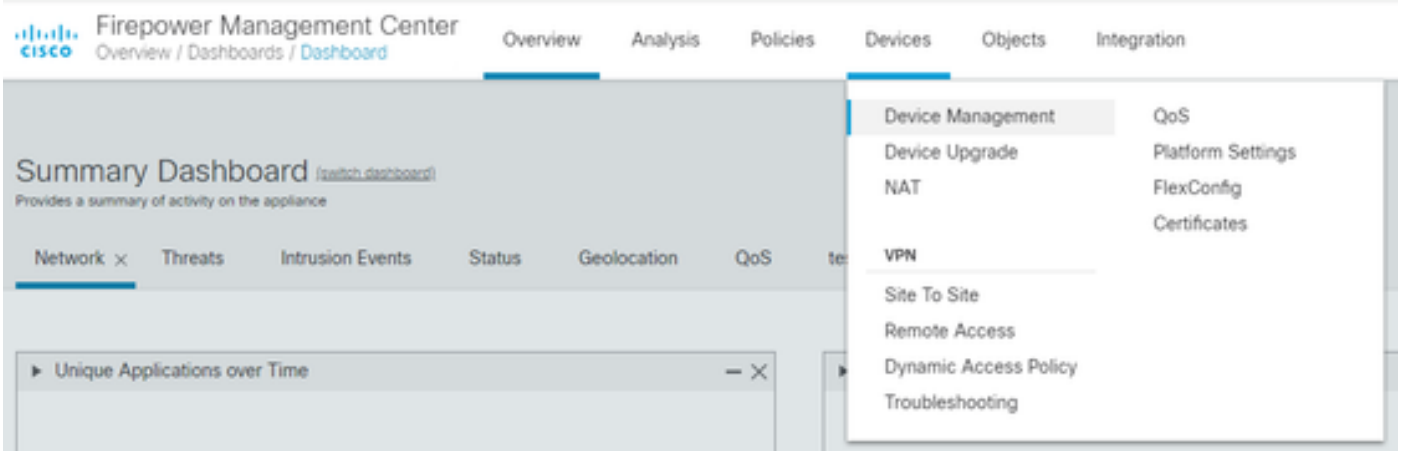
구성

Snort 버전 업그레이드

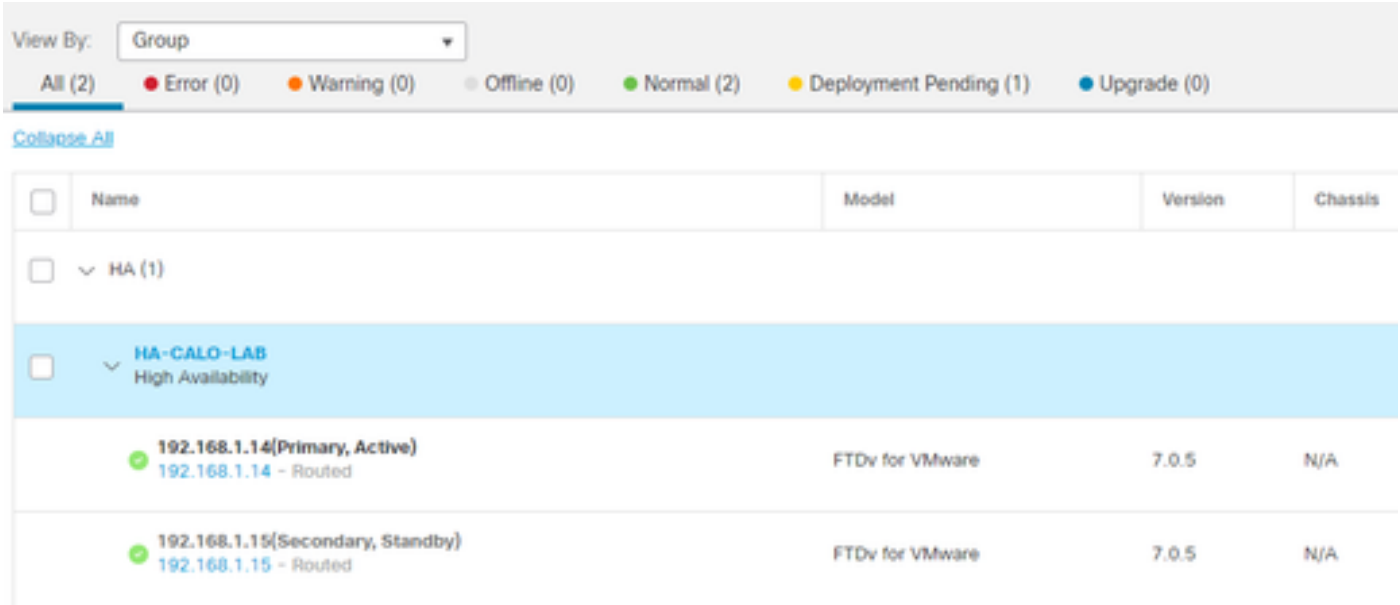
방법 1

1. firepower Management Center에 로그인합니다.

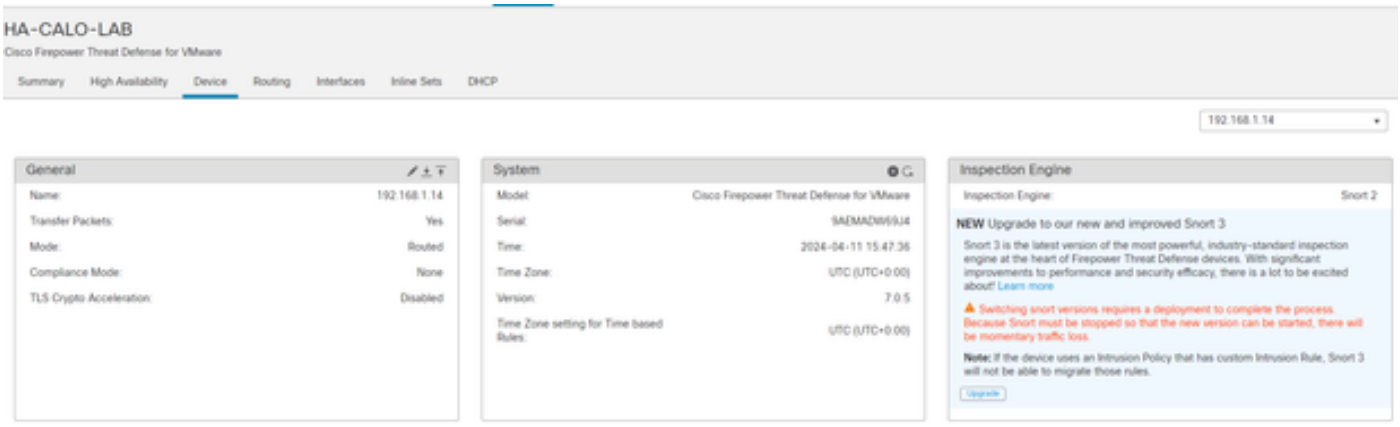
2. Device(디바이스) 탭에서 Devices(디바이스) > Device Manager(디바이스 관리자)로 이동합니다.



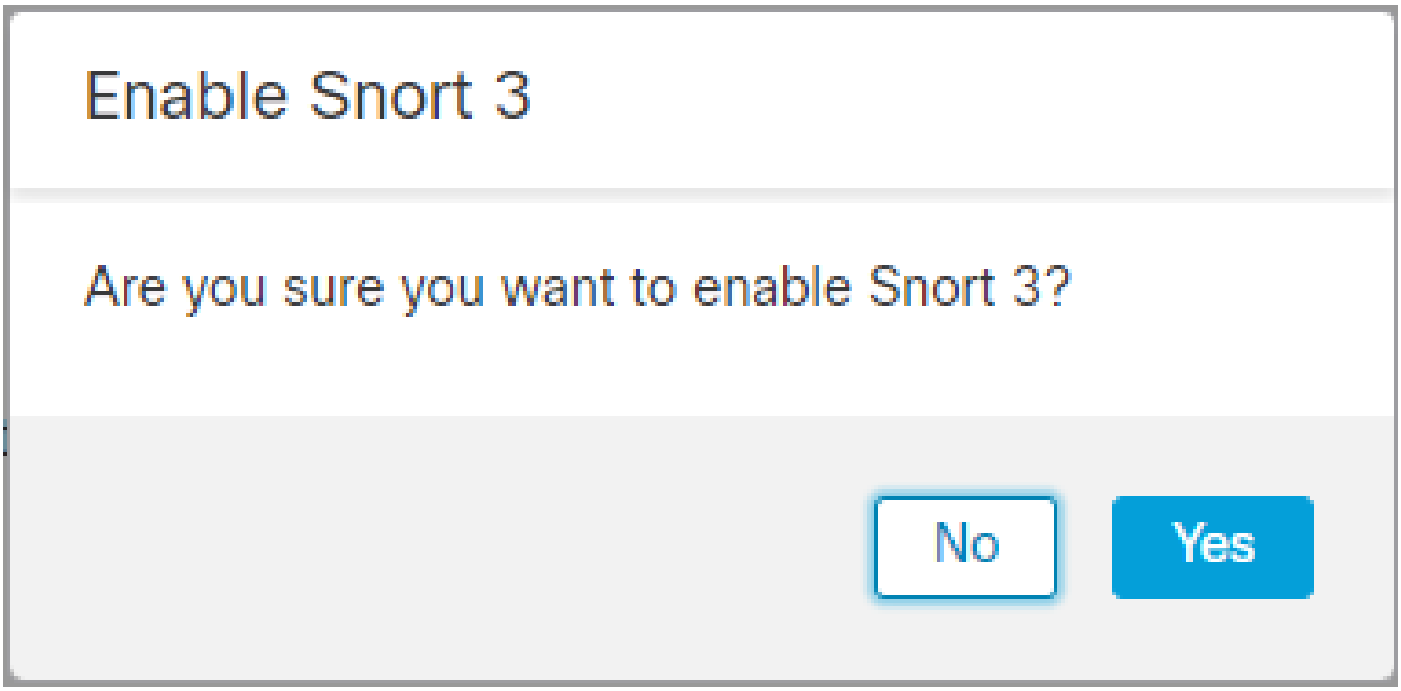
3. Snort 버전을 변경할 디바이스를 선택합니다.



4. 장치 탭을 클릭하고 검사 엔진 섹션에서 업그레이드 버튼을 클릭합니다.



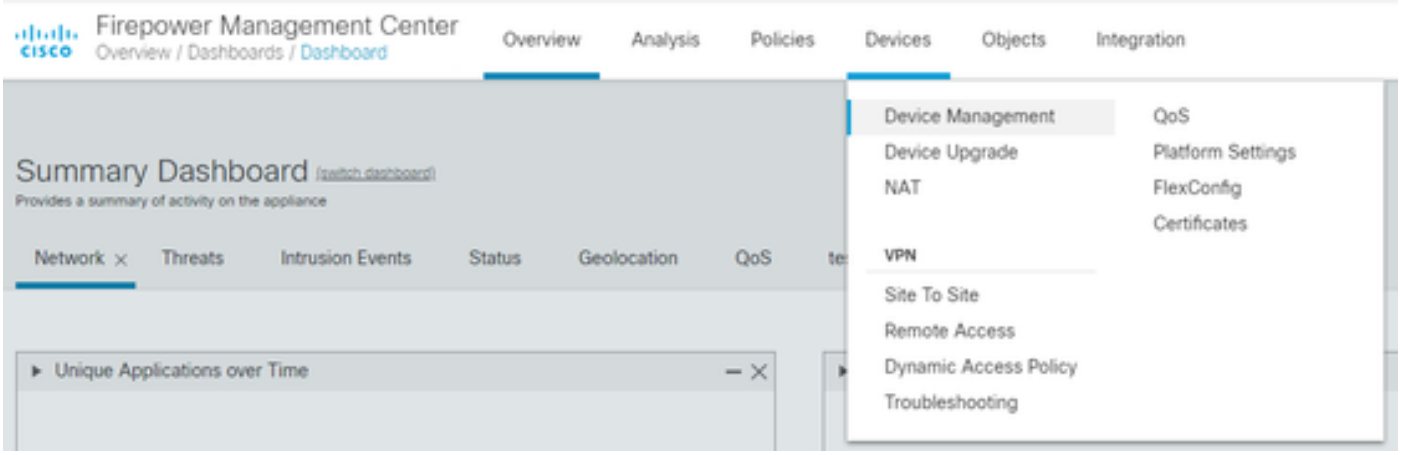
5. 선택을 확인합니다.



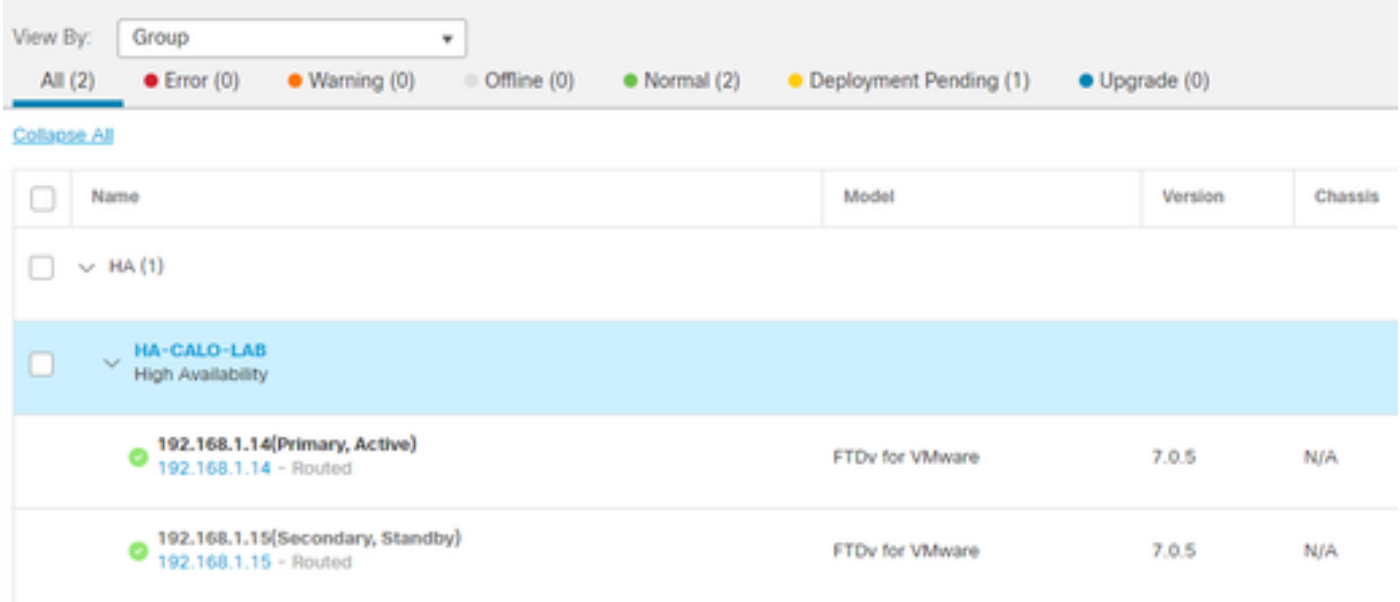
방법 2

1. firepower Management Center에 로그인합니다.

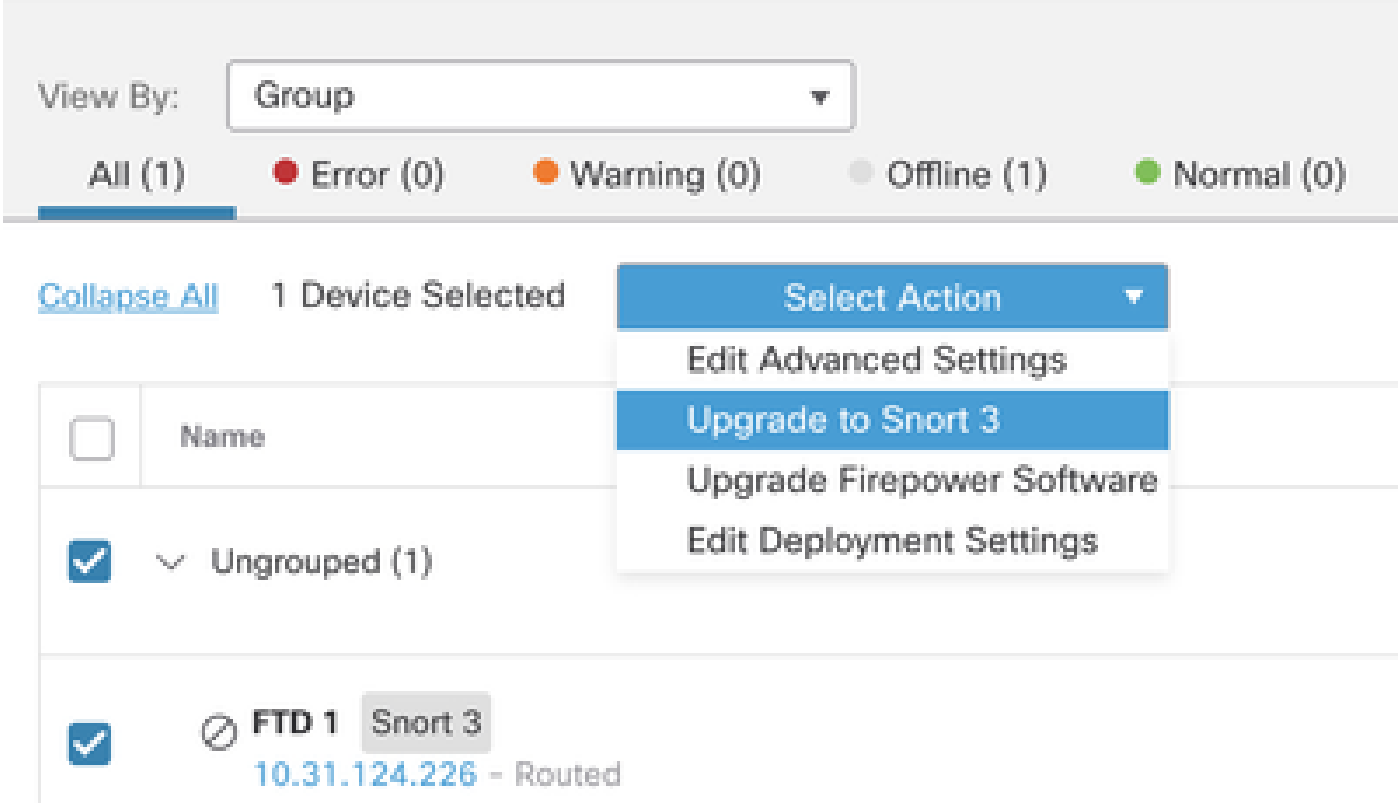
2. Device(디바이스) 탭에서 Devices(디바이스) > Device Manager(디바이스 관리자)로 이동합니다.



3. Snort 버전을 변경할 디바이스를 선택합니다.



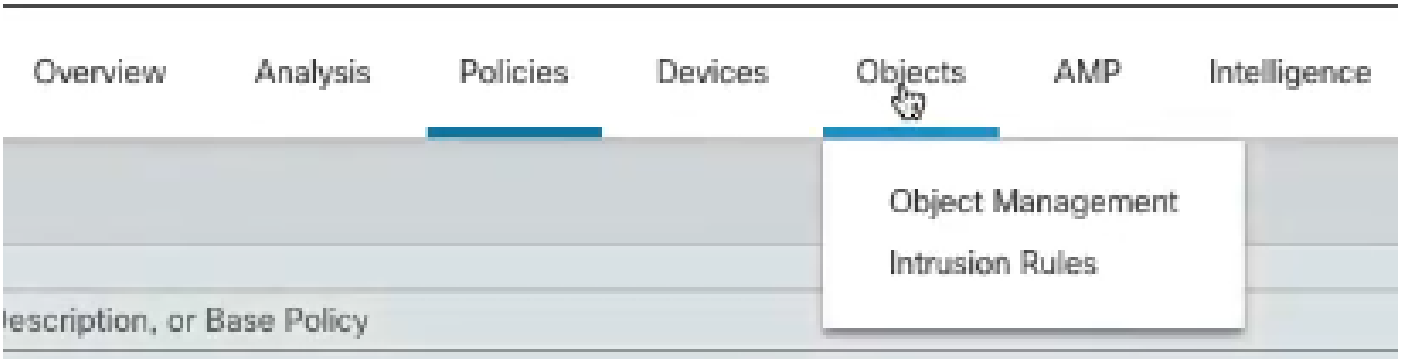
4. 조치 선택 버튼을 클릭하고 Upgrade to Snort 3을 선택합니다.



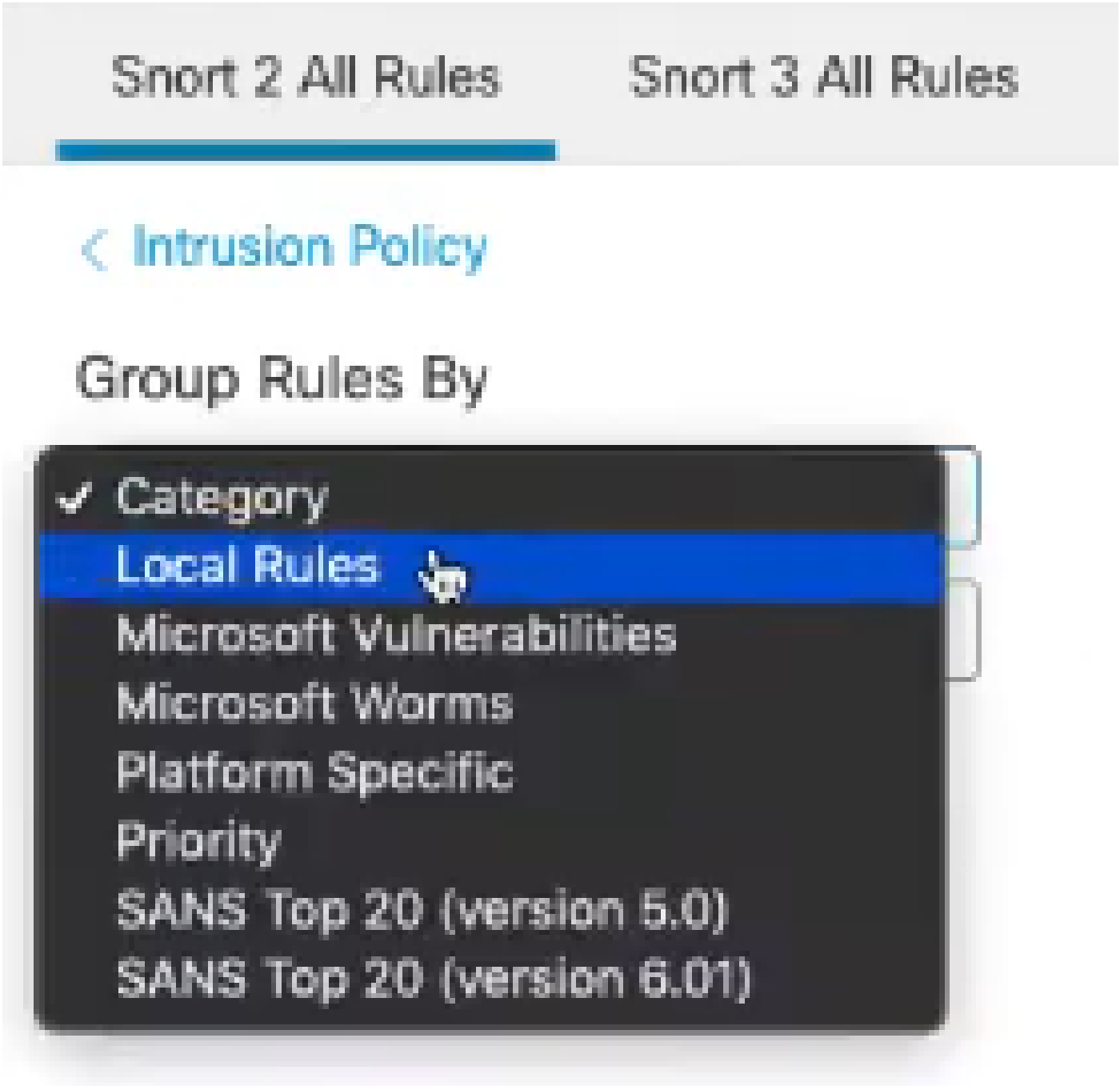
침입 규칙 업그레이드

또한 Snort 2 규칙을 Snort 3 규칙으로 변환해야 합니다.

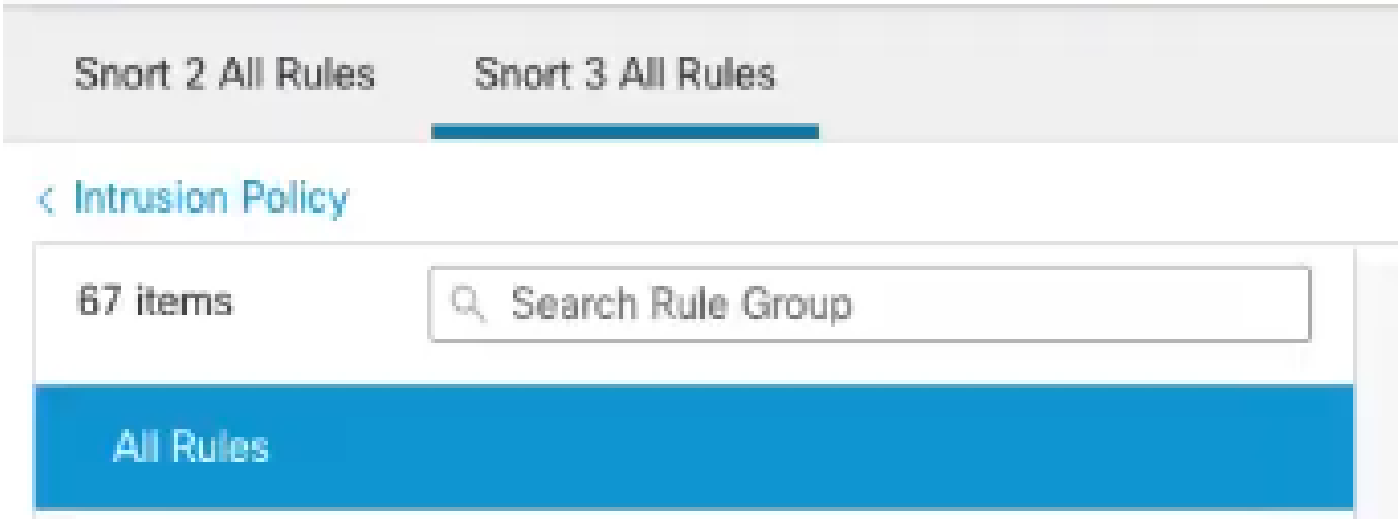
1. 메뉴에서 Objects(개체) > Intrusion Rules(침입 규칙)를 선택합니다.



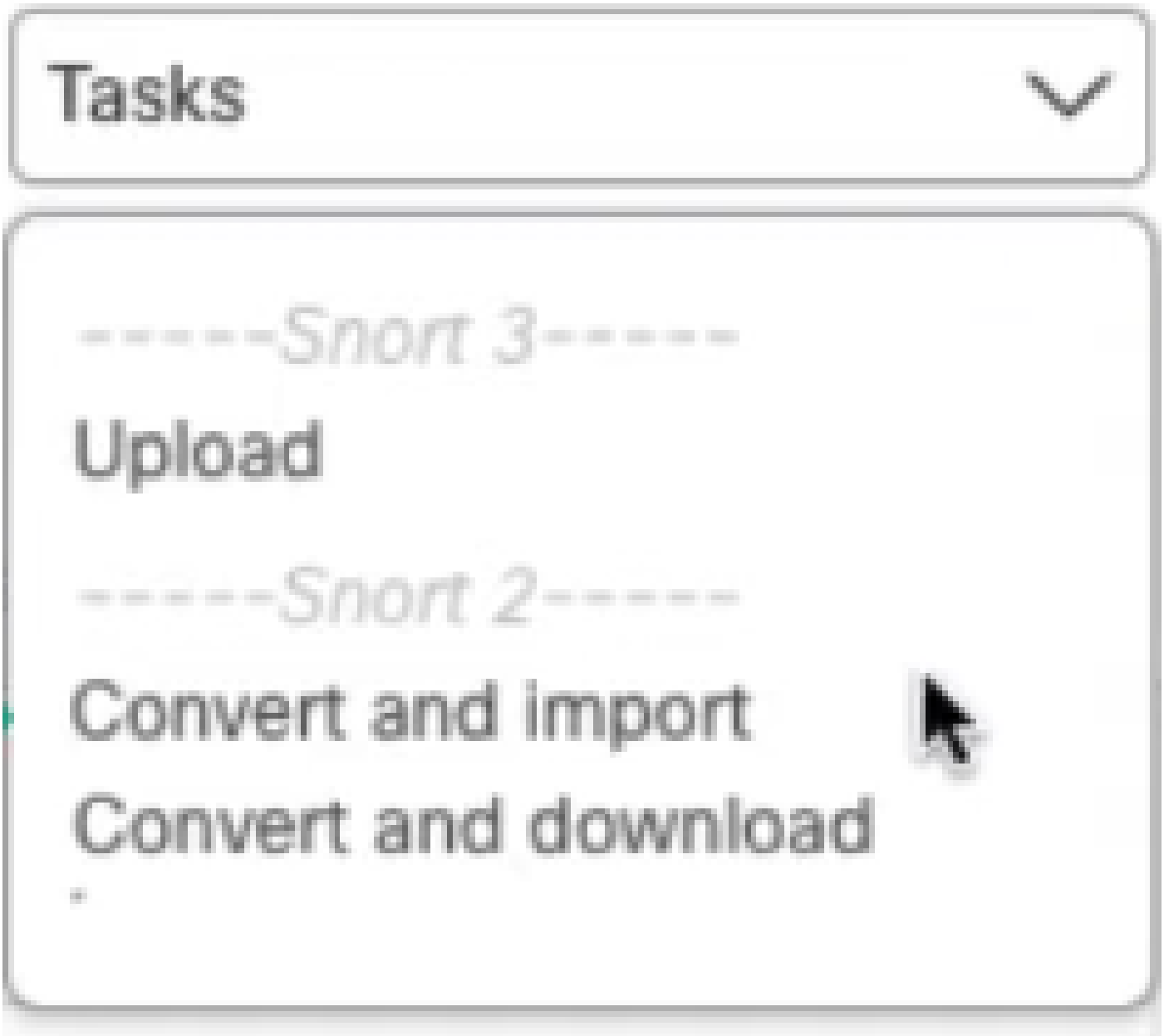
2. 메뉴에서 Snort 2 All Rules 탭 > Group Rules By > Local Rules를 선택합니다.



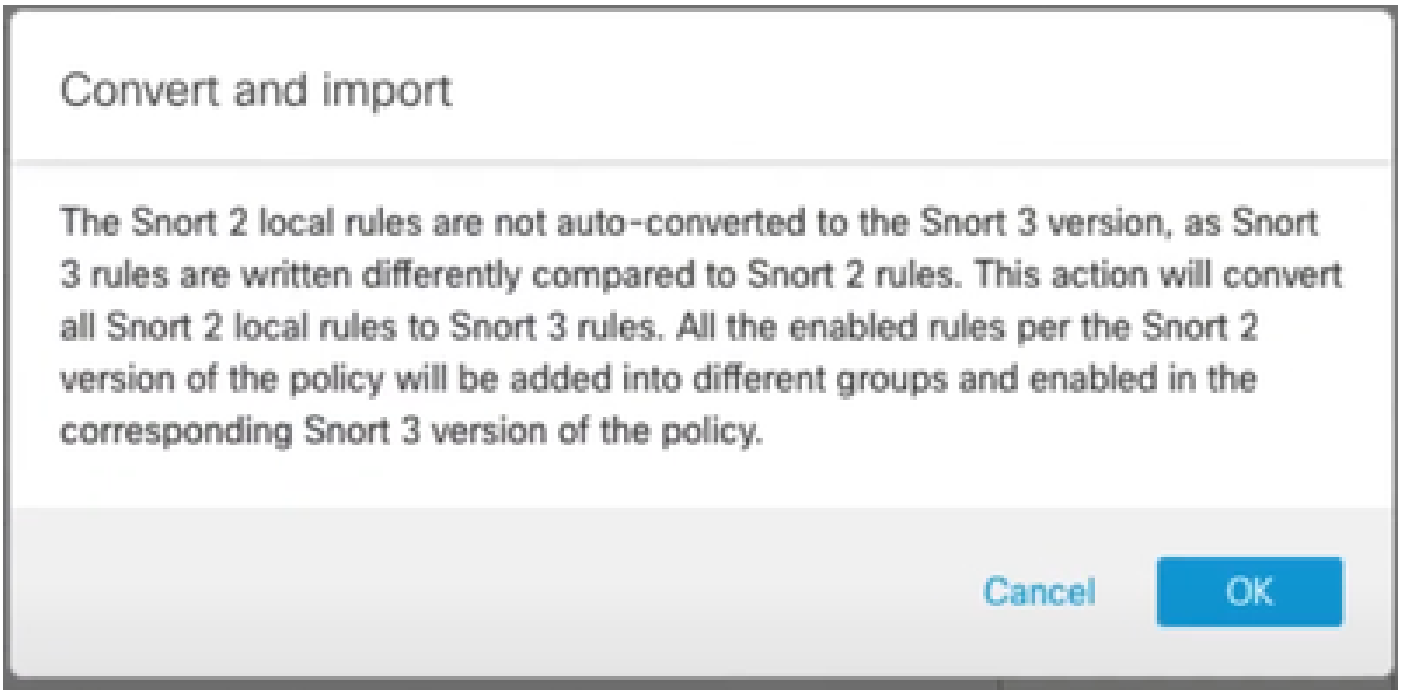
3. Snort 3 All Rules(Snort 3 모든 규칙) 탭을 클릭하고 All Rules(모든 규칙)가 선택되었는지 확인합니다.



4.작업 드롭다운 메뉴에서 변환 및 가져오기를 선택합니다.



5. 경고 메시지에서 확인을 클릭합니다.

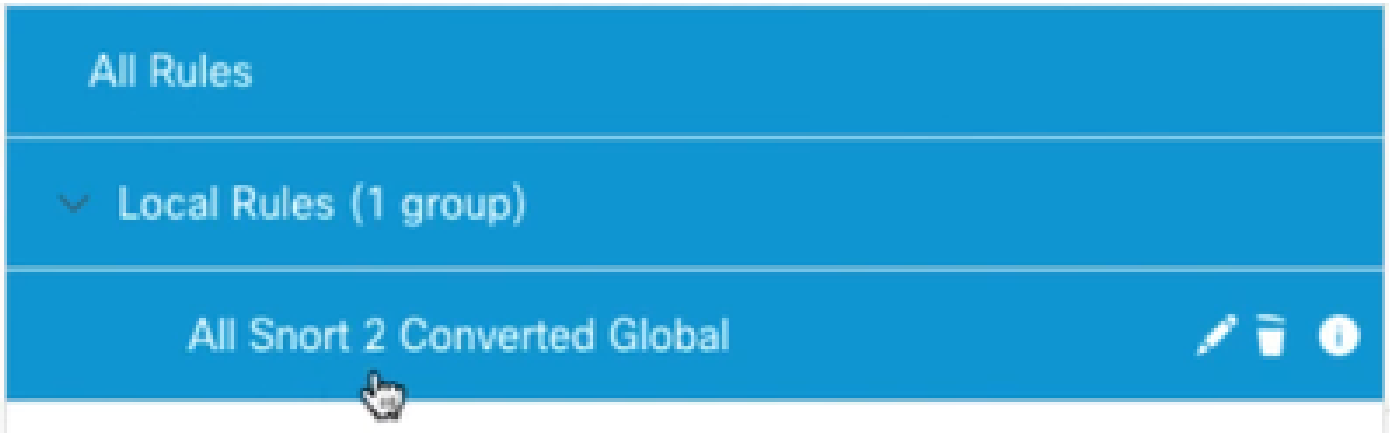


다음을 확인합니다.

Inspection Engine(검사 엔진) 섹션에는 현재 버전의 Snort 3이 표시됩니다.

다음 메시지가 표시되면 규칙 변환에 성공했습니다.

마지막으로 Local Rules(로컬 규칙) 그룹에서 All Snort 2 Converted Global(Snort 2에서 Snort 3으로 변환된 모든 규칙이 포함된 All Snort 2 Converted Global) 섹션을 찾아야 합니다.



문제 해결

마이그레이션이 실패하거나 충돌하는 경우 Snort 2로 롤백하고 다시 시도하십시오.

관련 정보

- Snort 2에서 Snort 3으로 마이그레이션하는 방법
- Cisco Secure - Snort 3 디바이스 업그레이드(외부 YouTube 비디오)

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.