인바운드 및 아웃바운드 트래픽 필터링을 위해 FTD에서 지오로케이션 기반 트래픽 차단 구성

목차

문제

- Cisco FTD(Secure Firewall Threat Defense)에서 지리적 위치를 기반으로 트래픽을 차단하는 가장 좋은 방법은 무엇인지 설명하십시오. 이는 특정 지역에서 시작된 트래픽과 해당 지역으로 향하는 트래픽에 모두 해당됩니다.
- 인바운드 및 아웃바운드 트래픽 필터링에 별도의 액세스 제어 규칙이 필요한지 여부와, 액세스 제어 규칙 Networks(네트워크) 탭 아래의 Geolocations(지오로케이션) 탭에서 지오로케이션 엔트리를 이미 사용할 수 있는 경우 추가 지오로케이션 객체를 생성해야 하는지 여부에 대한 질문이 제기됩니다.

환경

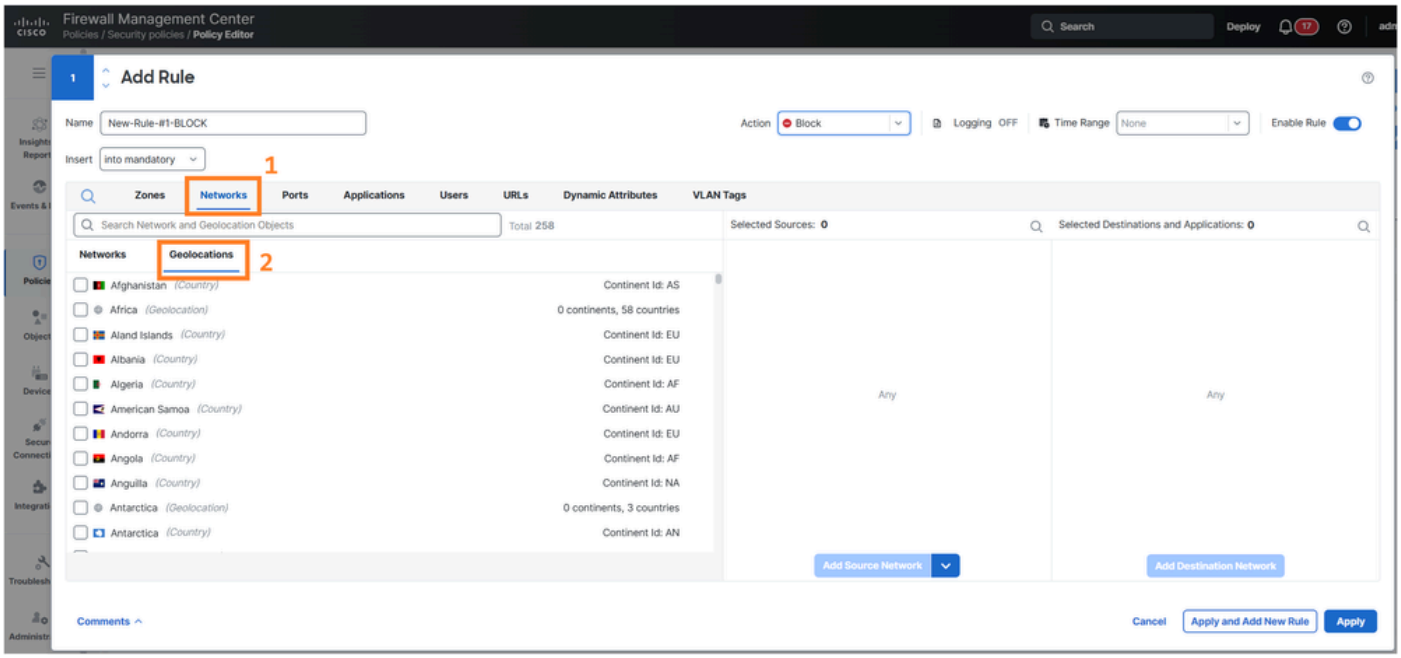
- FTD 소프트웨어 버전 7.1. 다른 소프트웨어 버전도 영향을 받습니다.
- Cisco FMC(Secure Firewall Management Center) 소프트웨어 버전 7.1. 다른 소프트웨어 버전도 영향을 받습니다.

해결

Cisco FTD의 지오로케이션 기반 트래픽 필터링은 FMC UI(사용자 인터페이스)의 Networks(네트워크) 탭, Access Control Policy Rule(액세스 제어 정책 규칙) 섹션에서 사용할 수 있는 기존 Geolocations(지오로케이션) 기능을 사용하여 효과적으로 관리할 수 있습니다. 컨피그레이션 접근 방식은 특정 트래픽 방향 및 정책 요구 사항에 따라 달라집니다.

지오로케이션 컨피그레이션 액세스

Policies(정책) > Security policies(보안 정책) > Policy Editor(정책 편집기)로 이동하여 규칙을 편집하고 FMC UI에서 Networks(네트워크) > Geolocations(위치) 탭을 선택합니다. 이 섹션에서 사용할 수 있는 기존 지오로케이션 항목은 별도의 지오로케이션 객체가 없어도 액세스 제어 정책을 생성하는 데 직접 활용할 수 있습니다.



규칙 생성 전략

규칙 생성 접근 방식은 트래픽 방향성 및 정책 목표에 따라 달라집니다.

특정 지리로부터의 인바운드 트래픽 차단

특정 지리적 지역에서 발생하는 소스 트래픽을 식별하고 차단 조치를 적용하는 액세스 제어 규칙을 생성합니다. 적절한 정책 시행을 위해 이러한 규칙을 규칙에서 적절하게 배치해야 합니다.

특정 위치에 대한 아웃바운드 트래픽 제어

특정 지역으로 향하는 목적지 트래픽을 식별하는 액세스 제어 규칙을 구성합니다. 보안 정책에 따라 이러한 대상에 대한 트래픽을 허용하거나 차단하도록 구성할 수 있습니다.

별도의 규칙 요구 사항

양방향 지오로케이션 필터링을 구현할 때는 다음과 같은 이유로 별도의 액세스 제어 규칙이 필요합니다.

- 인바운드 필터링에는 소스 지오로케이션 특성을 평가하는 규칙이 필요합니다.
- 아웃바운드 필터링에는 대상 지오로케이션 특성을 평가하는 규칙이 필요합니다.
- 트래픽 방향성은 액세스 제어 엔진에서 평가되는 지오로케이션 필드(소스 또는 목적지)를 결정합니다.

특정 규칙 컨피그레이션은 네트워크 토폴로지, 보안 요구 사항, 각 지리적 영역에 대해 원하는 트래픽 흐름 제어 목표에 따라 달라집니다.

원인

명확화의 필요성은 지리적 위치 기반 액세스 제어 구현의 복잡성에서 비롯되며, 여기서 트래픽 방향에 따라 서로 다른 규칙 유형 및 컨피그레이션이 필요합니다. 보안 정책 액세스 제어 규칙의 Networks(네트워크) 탭에서 기존 지오로케이션 엔트리를 사용할 수 있으면 정책 구현에 추가 객체 생성이 필요한지 여부에 대한 혼란이 발생할 수 있습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.