FMC에서 추가 Snort 3 규칙 작업 구성

목차

소개

이 문서에서는 7.1 릴리스에 추가된 추가 Snort 3 규칙 작업 기능에 대한 FMC(Firepower Management Center) 지원에 대해 설명합니다.

배경 정보

FTD(Firepower Threat Defense)는 7.0에서 7개의 침입 정책 규칙 작업 Alert/Disable/Block/Reject/Rewrite/Pass/Drop을 지원하지만, FMC는 3개의 Snort 3 규칙 작업만 지원합니다. 'Alert', 'Disable' 및 'Block'입니다.

firepower 7.1.0에서 FMC는 새 규칙 작업을 구성할 수 있도록 지원합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.
· 오픈 소스 Snort 지식
· FMC(Firepower 관리 센터) 7.1.0+
· FTD(Firepower 위협 방어) 7.0.0 이상

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
· 이 문서는 Snort 3을 실행하는 모든 Firepower 플랫폼에 적용됩니다.
· 소프트웨어 버전 7.4.2를 실행하는 Cisco FTD(Firepower Threat Defense Virtual)
· 소프트웨어 버전 7.4.2를 실행하는 FMC(Firepower 관리 센터 가상)

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.

기능 세부사항

새로 추가된 Snort 3 규칙 작업 및 설명은 다음과 같습니다.

통과: 이벤트가 생성되지 않으므로 후속 Snort 규칙에 의한 추가 평가 없이 패킷이 통과할 수 있습니다.

삭제: 이벤트를 생성하고, 일치하는 패킷을 삭제하며, 이 연결에서 추가 트래픽을 차단하지 않습니다.

거부: 이벤트를 생성하고, 일치하는 패킷을 삭제하고, 이 연결에서 추가 트래픽을 차단하고, 소스 및 목적지 호스트에 연결할 수 없는 TCP 재설정 또는 ICMP 포트를 전송합니다.

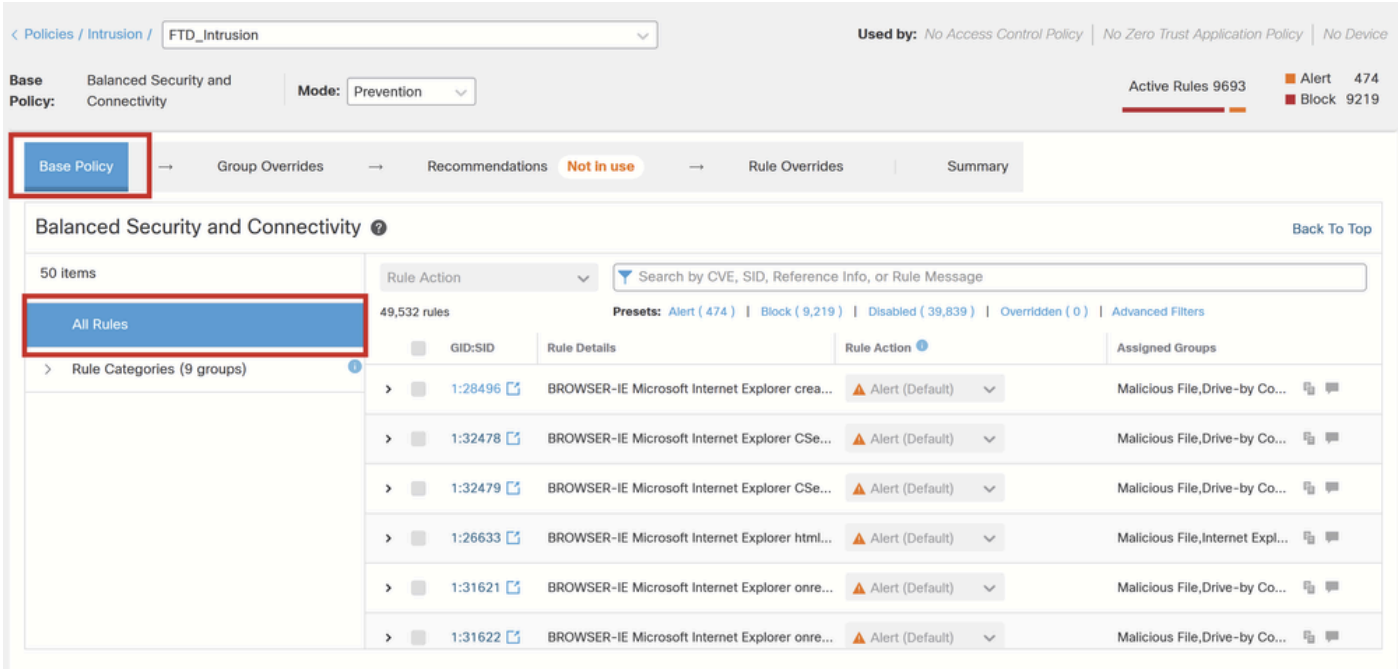
다시 쓰기: 이벤트를 생성하고 규칙의 replace 옵션을 기반으로 패킷 내용을 덮어씁니다.

FMC 연습

침입 정책에서 Snort 3 규칙을 보려면 다음 이미지에 표시된 것처럼 정책의 오른쪽 상단 모서리에서 Snort 3 Version 옵션을FMC Policies > Access Control > Intrusion,클릭합니다.

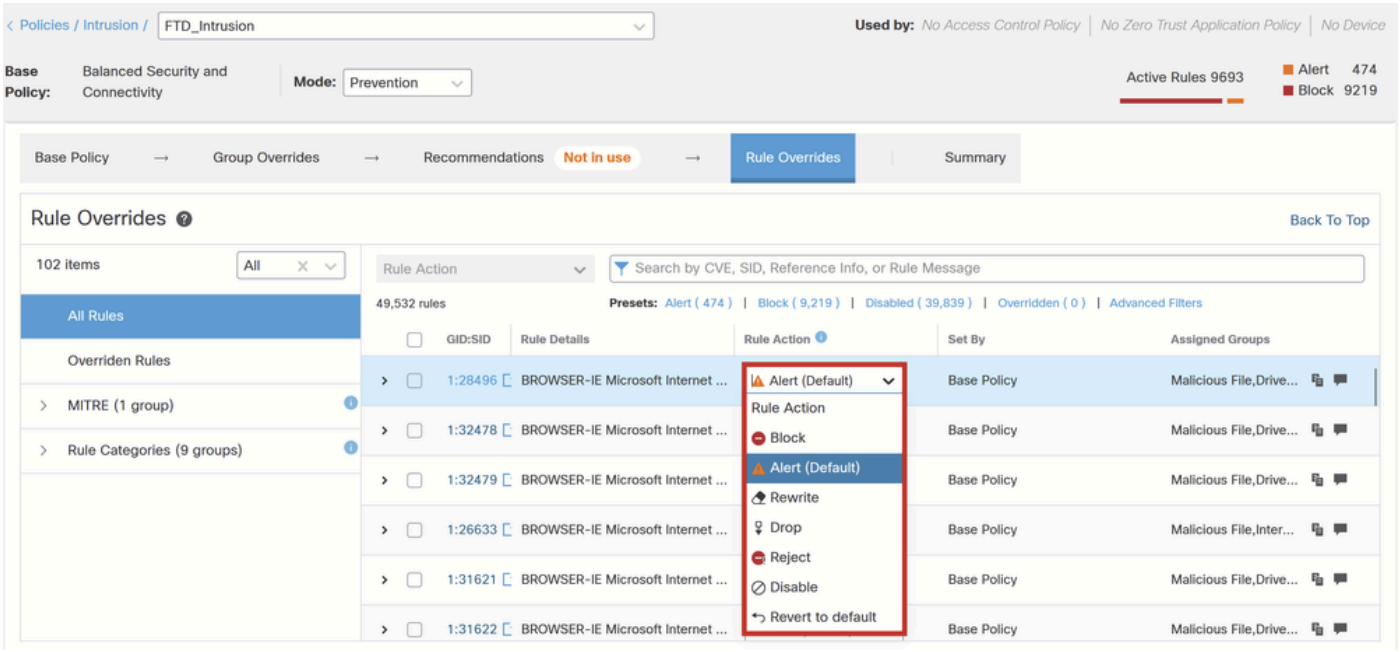
Snort 3 버전

Base Policy(기반 정책) > All Rules(모든 규칙)를 클릭하면 시스템에서 정의한 모든 Snort 3 규칙의 기본 작업을 볼 수 있습니다.

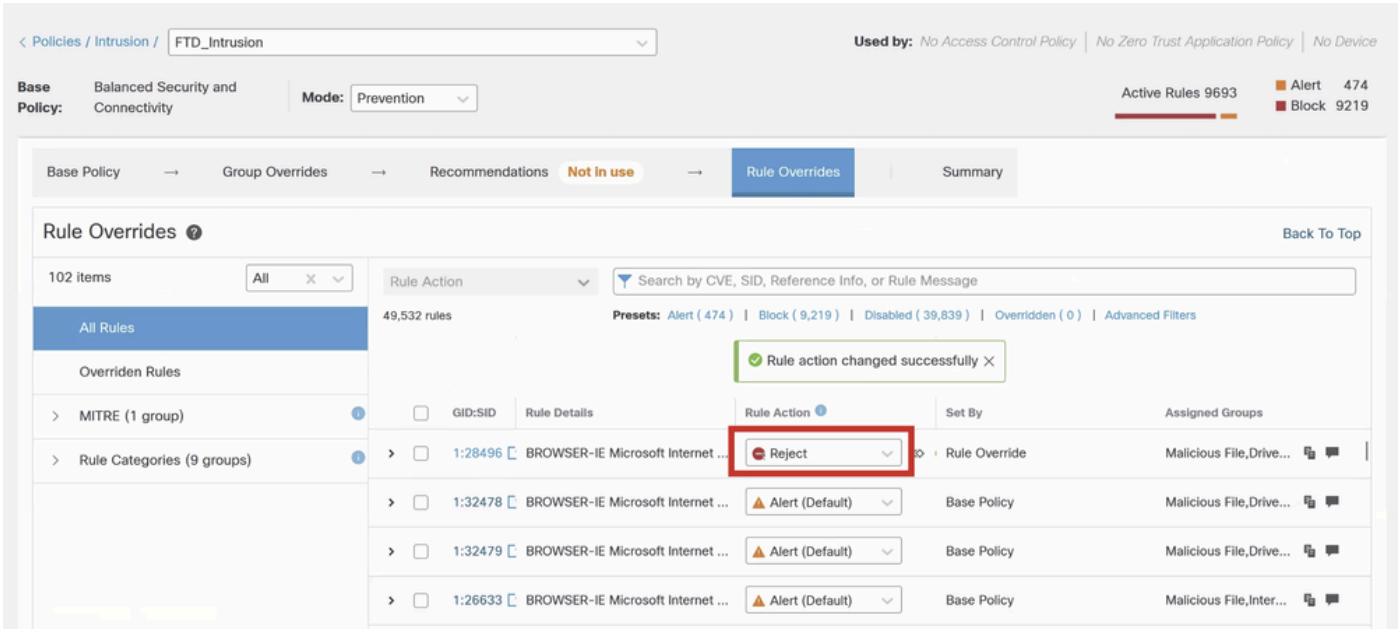


기반 정책

규칙 작업을 이러한 새 규칙 작업으로 변경하려면 Rule Overrides > All Rules로 이동하여 선택한 규칙의 드롭다운에서 규칙 작업을 선택합니다.

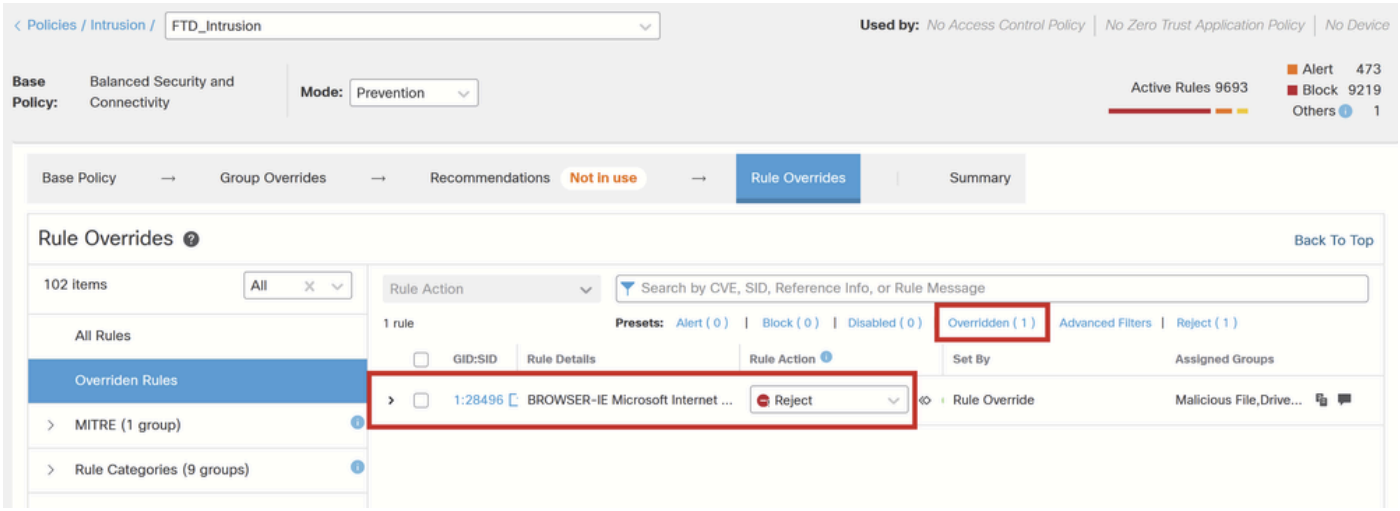


추가 규칙 작업



규칙 작업 변경

재정의된 규칙은 Rule Overrides(규칙 재정의) > Overrided Rules(재정의된 규칙)에서 찾을 수 있습니다.


Policies / Intrusion /
FTD_Intrusion
Used by: No Access Control Policy | No Zero Trust Application Policy | No Device
Base Policy: Balanced Security and Connectivity
Mode: Prevention
Active Rules 9693
Alert 473
Block 9219
Others 1
Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides | Summary
Rule Overrides
Back To Top
102 items
All
All Rules
Overriden Rules
MITRE (1 group)
Rule Categories (9 groups)
Rule Action
Search by CVE, SID, Reference Info, or Rule Message
1 rule
Presets: Alert (0) | Block (0) | Disabled (0) | Overridden (1) | Advanced Filters | Reject (1)
GID:SID
Rule Details
Rule Action
Set By
Assigned Groups
1:28496
BROWSER-IE Microsoft Internet ...
Reject
Rule Override
Malicious File,Drive...

재정의된 규칙

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.