

FMC에서 관리하는 Firepower 디바이스의 SRU 및 LSP 버전을 기반으로 Snort 규칙 필터링

목차

- [소개](#)
 - [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
 - [배경 정보](#)
 - [Snort 규칙 필터링 절차](#)
-

소개

이 문서에서는 FMC(Firepower 관리 센터)에서 관리하는 firepower 디바이스의 Cisco SRU(Secure Rule Update) 및 LSP(Link State Packet) 버전을 기반으로 Snort 규칙을 필터링하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 오픈 소스 Snort 지식
- FMC(Firepower Management Center)
- FTD(Firepower Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 이 문서는 모든 Firepower 플랫폼에 적용됩니다.
- 소프트웨어 버전 7.0.0을 실행하는 Cisco FTD(Firepower 위협 방어)
- 소프트웨어 버전 7.0.0을 실행하는 FMC(firepower Management Center Virtual)

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

IDS(Intrusion Detection Systems) 및 IPS(Intrusion Prevention Systems)의 컨텍스트에서 "SID"는

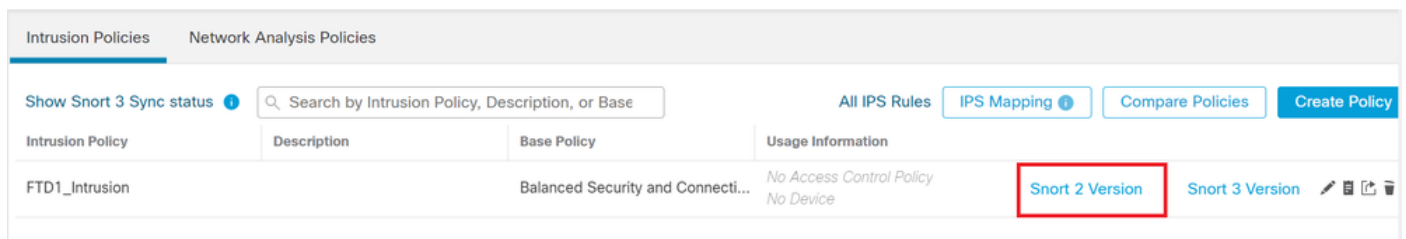
"Signature ID" 또는 "Snort Signature ID"를 나타냅니다.

SID(Snort Signature ID)는 각 규칙 또는 해당 규칙 집합 내의 시그니처에 할당되는 고유 식별자입니다. 이러한 규칙은 네트워크 트래픽에서 악의적인 활동이나 보안 위협을 나타낼 수 있는 특정 패턴이나 동작을 탐지하는 데 사용됩니다. 각 규칙은 SID와 연결되어 쉽게 참조하고 관리할 수 있도록 합니다.

오픈 소스 Snort에 대한 자세한 내용은 SNORT [웹 사이트](#)를 참조하십시오.

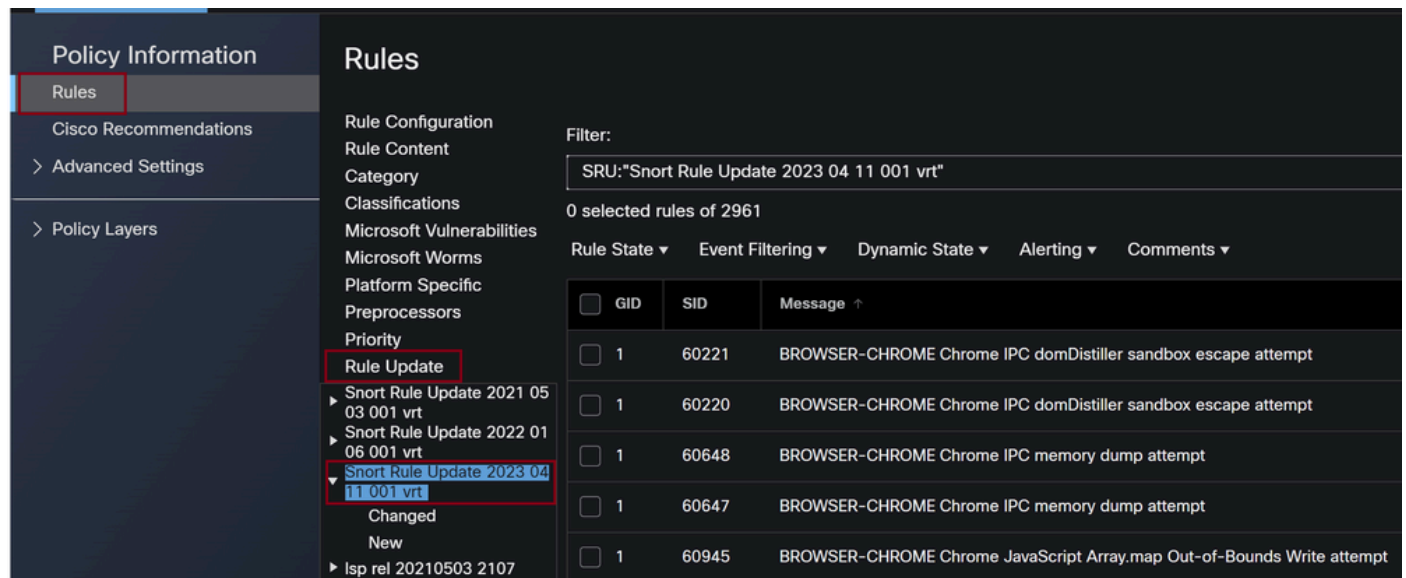
Snort 규칙 필터링 절차

Snort 2 규칙 SID를 보려면 FMC Policies > Access Control > Intrusion, 그런 다음 그림과 같이 오른쪽 상단 모서리에서 SNORT2 옵션을 클릭합니다.

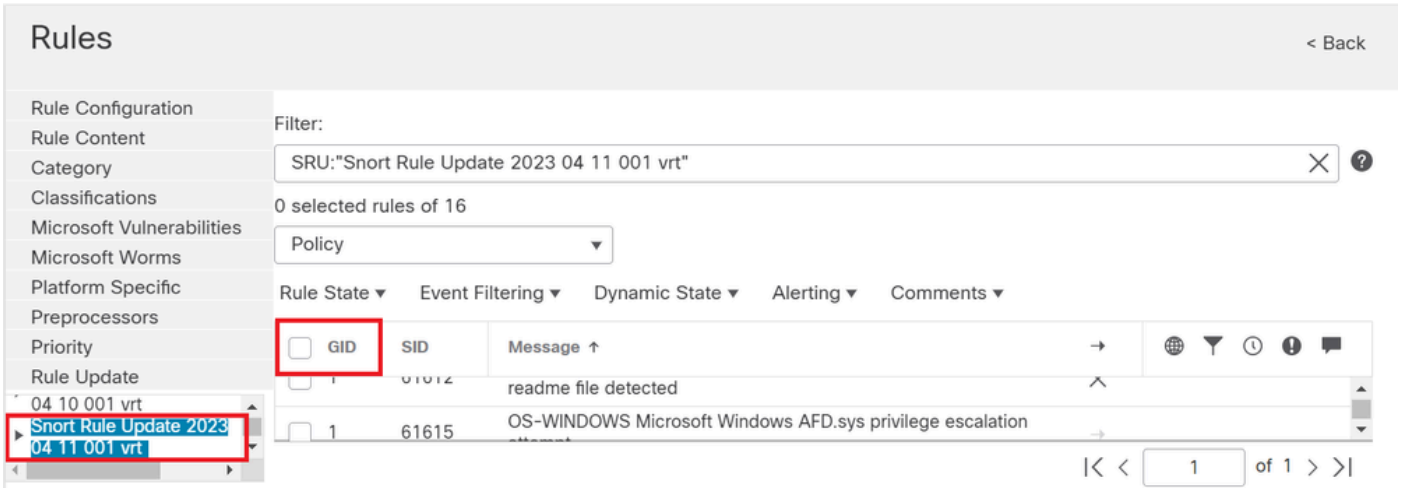


Snort 2

탐색 Rules > Rule Update 최신 날짜를 선택하여 SID를 필터링합니다.

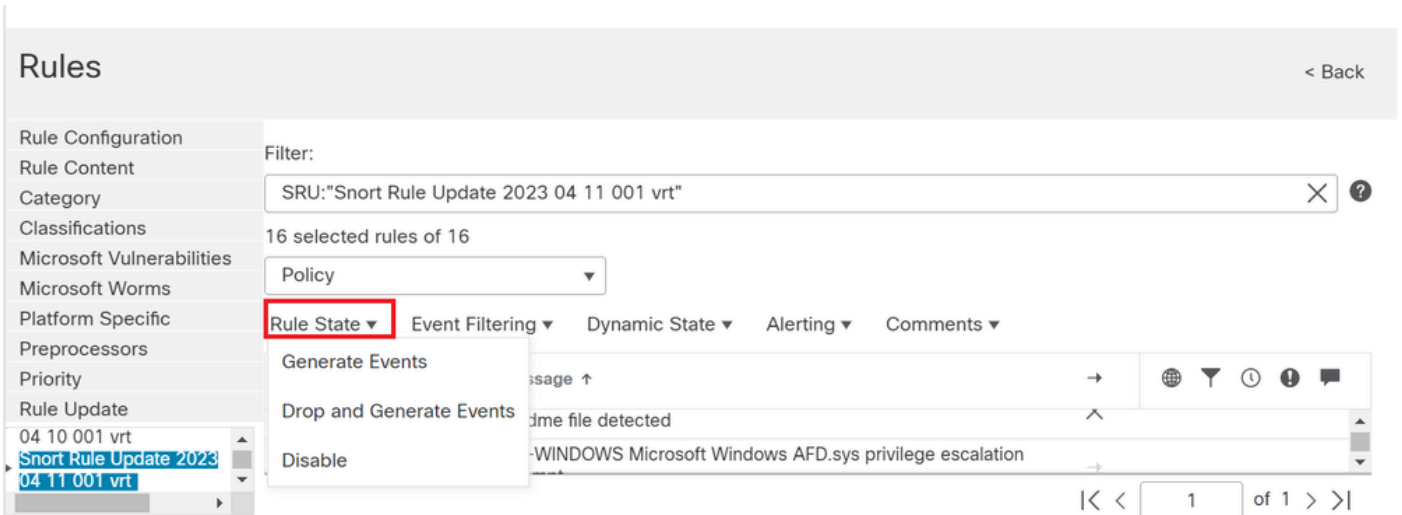


규칙 업데이트



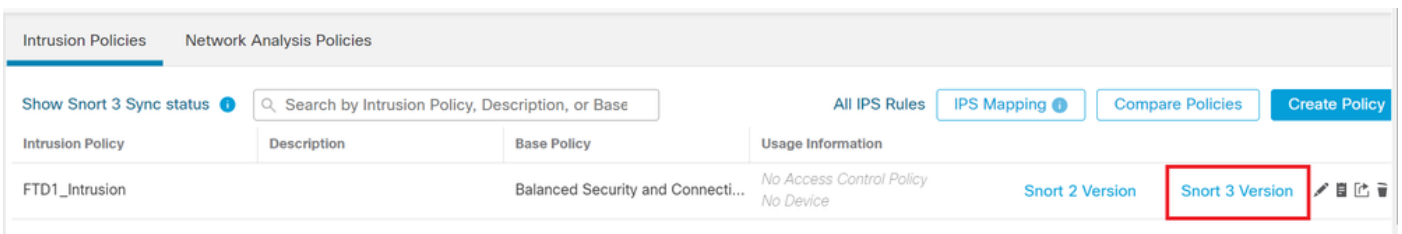
Snort 규칙에 따라 사용 가능한 Sid

아래에서 필요한 옵션을 선택합니다. Rule State 그림에 표시된 것과 같습니다.



규칙 상태 선택

Snort 3 규칙 SID를 보려면 FMC Policies > Access Control > Intrusion 그런 다음 그림과 같이 오른쪽 상단 모서리에서 SNORT3 옵션을 클릭합니다.



Snort 3

탐색 Advanced Filters 이미지에 표시된 대로 SID를 필터링할 최신 날짜를 선택합니다.

< Intrusion Policy

Policy Name Used by: No Access Control Policy | No Device

Mode Base Policy Balanced Security and Connectivity

Disabled 39249 | Alert 470 | Block 9151 | Overridden 0 | Rewrite 0 | Pass 0 | Drop 0 | Reject 0

Rule Groups Back To Top

50 items Excluded | Included | Overridden

All Rules Reco

> Browser (6 groups)

> Server (8 groups)

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

48,870 rules Preset Filters: Advanced Filters | 470 Alert rules | 9,151 Block rules | 39,249 Disabled rules | 0 Overridden rules

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
>	1:28496	BROWSER-IE Microsoft Internet Explore...	Alert (Default)	Browser/Internet Explo...

Snort 3 필터

Advanced Filters ?

LSP

Select...

Show Only * New Changed

Classifications

Select...

Microsoft

Vulnerabilities

Select...

Cancel

OK

고급 필터의 LSP

Advanced Filters ?

LSP

Show Only * New Changed

Classifications

Microsoft Vulnerabilities

Cancel

LSP 버전

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22 ▾ | 48,870 rules Preset Filters: 0 Alert rules | **11 Block rules** | 11 Disabled rules | 0 Overridden rules | Advanced Filters

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

Sid에 대한 사전 설정 필터

아래에서 필요한 옵션을 선택합니다. Rule state 그림에 표시된 것과 같습니다.

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22 | 22 ▾ | 48,870 rules Preset Filters: 0 Alert rules | 11 Block rules | 11 Disabled rules | 0 Overridden rules | Advanced Filters

<input checked="" type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input checked="" type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

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.