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

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배경 정보</u> 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 디바 이스는 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 식별자입 니다. 이러한 규칙은 네트워크 트래픽에서 악의적인 활동이나 보안 위협을 나타낼 수 있는 특정 패 턴이나 동작을 탐지하는 데 사용됩니다. 각 규칙은 SID와 연결되어 쉽게 참조하고 관리할 수 있도록 합니다.

오픈 소스 Snort에 대한 자세한 내용은 SNORT 웹 사이트를 참조하십시오.

Snort 규칙 필터링 절차

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

Intrusion Policies Network	Analysis Policies				
Show Snort 3 Sync status 0	 Search by Intrusion Policy, Department Description 	scription, or Base	All IPS Rules	IPS Mapping Compa	are Policies Create Policy
FTD1_Intrusion		Balanced Security and Connecti	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version 📝 🖥 🖆 🗑

Snort 2

탐색 Rules > Rule Update 최신 날짜를 선택하여 SID를 필터링합니다.

Policy Information Rules Cisco Recommendations	Rules Rule Configuration Rule Content	Filter:				
Policy Layers	Advanced Settings Category Classifications Policy Layers Microsoft Vulnerabilities	SRU:"Snort Rule Update 2023 04 11 001 vrt" 0 selected rules of 2961 Pule State x Event Eiltering x Dynamic State x Alerting x Comments x				
Microsoft Worms Platform Specific Preprocessors Priority Rule Update Snort Rule Update 2021 05 03 001 vrt Snort Rule Update 2022 01 06 001 vrt Snort Rule Update 2023 02 11 001 vrt Changed New Isp rel 20210503 2107	GID	SID	Message \uparrow			
	Rule Update Snort Rule Update 2021 05 03 001 vrt	□ 1 □ 1	60221 60220	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt		
	Snort Rule Update 2022 01 06 001 vrt Snort Rule Update 2023 04	1	60648	BROWSER-CHROME Chrome IPC memory dump attempt		
	□ 1 □ 1	60647 60945	BROWSER-CHROME Chrome IPC memory dump attempt BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt			

규칙 업데이트

Rules					< Back
Rule Configuration	Filter				
Rule Content	Filter:				
Category	SRU:"Snort Rule Update 2023 04 11 001 vrt"				× 0
Classifications	0 selected rules of 16				
Microsoft Vulnerabilities					
Microsoft Worms	Policy				
Platform Specific	Rule State Event Filtering Dynamic State Alerting Comments				
Preprocessors					
Priority	☐ GID SID Message ↑	\rightarrow	T	00	-
Rule Update	1 VIVI2 readme file detected	~			
04 10 001 vrt					- 1
Snort Rule Update 2023	1 61615 OS-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow			*
04 11 001 vrt ▼ →		< <	1	of 1	> >

Snort 규칙에 따라 사용 가능한 Sid

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

Rules						< Back
Rule Configuration	Filtor					
Rule Content	Filter.					
Category	SRU:"Snort Rule Update 2	023 04 11 001 vrt"				× 0
Classifications	16 selected rules of 16					
Microsoft Vulnerabilities						
Microsoft Worms	Policy	¥				
Platform Specific	Rule State • Event Filteri	ng Dynamic State Alerting Comments				
Preprocessors	Generate Events					
Priority	Generate Events	sage ↑	\rightarrow	⊕ ▼	0	.
Rule Update	Drop and Generate Events	time file detected	~			
04 10 001 vrt 🔺						
Snort Rule Update 2023	Disable	-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow			*
04 11 001 vrt ▼	1		< > > ا	1	of 1	> >

규칙 상태 선택

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

Intrusion Policies Network	Analysis Policies				
Show Snort 3 Sync status 1	Q Search by Intrusion Policy, De Description	escription, or Base Base Policy	All IPS Rules Usage Information	IPS Mapping () Compa	re Policies Create Policy
FTD1_Intrusion		Balanced Security and Connecti	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version 🖌 🖥 🖆 🗑

Snort 3

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

< Intrusion Policy Policy Name FTD1_Intrusion		v	Used by: No Access Control Policy No Device
Mode Prevention Sase Policy Base Disabled 39249 Alert 470 Block 91	nced Security and Connectivity Overridden 0 Rewrite 0 Pass 0 1	Drop 0 Reject 0	
Rule Groups			Back To Top
50 items + Q Search Rule Group Excluded Included Overridden	All Rules All rules assigned to current intrusion policy irre	spective of rule group	
All Rules Reco	Rule Action Q Search Preset Filters:	by CVE, SID, Reference Info, or Rule Message 470 Alert rules 9,151 Block rules 39,249 Disat Advanced Filters	bled rules 0 Overridden rules
Server (6 groups) Server (8 groups)	GID:SID Info IL:28496 T BROWSER-IE Microsoft I	Rule Action Rule Action	Assigned Groups Browser/Internet Explo 🔒 🗭 🛔

Snort 3 필터

r

Advanced Filters

LSP	Select	~
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select	\sim
Microsoft Vulnerabilities	Select	~
	Cancel	OK

0

고급 필터의 LSP

Advanced Fil	lters 0	
LSP	lsp rel 20230420 1056 🗸 🗸	
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select v	
Microsoft Vulnerabilities	Select v	
	Cancel OK	
iP 버전		
All Rules All rules assigned to current intrusio	n policy irrespective of rule group	
Rule Action ✓ 22 ▼ 48,870 rules	Isp:lsp rel 20230420 1056 × Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advanced Filters	;
GID:SID Info	Rule Action Assigned Groups	
> 1:300509 🗂 MALWARE-E	BACKDOOR Win.Backdoor 😑 Block (Default) 🗸 Malware/Backdoor 🔹 🖛	ı

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 Isp:lsp rel 20230420 1056 × 22 V 48,870 rules Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advanced Filters	×	
GID:SID Info Rule Action () Assigned Groups		
> 🗹 1:300509 🖸 MALWARE-BACKDOOR Win.Backdoor 🕒 Block (Default) 🗸 Malware/Backdoor 🗳 💻		
	-	Ŧ

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 번 역 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.