FMCによって管理されるFirepowerデバイスの SRUおよびLSPバージョンに基づくSnortルール のフィルタリング

内容	
<u>はじめに</u>	
<u>前提条件</u>	
<u>要件</u>	
<u>使用するコンポーネント</u>	
<u>背景説明</u>	
<u>Snortルールをフィルタリングする手順</u>	

はじめに

このドキュメントでは、Firepower Management Center(FMC)で管理されるfirepowerデバイスの Cisco Secure Rule Update(SRU)およびLink State Packet(LSP)バージョンに基づいてSnortルール をフィルタリングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- オープンソースのSnortに関する知識
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- この記事は、すべてのFirepowerプラットフォームに適用されます
- ・ソフトウェアバージョン7.0.0が稼働するシスコFirepower脅威対策(FTD)
- ・ ソフトウェアバージョン7.0.0が稼働するFirepower Management Center Virtual(FMC)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

侵入検知システム(IDS)と侵入防御システム(IPS)のコンテキストでは、「SID」は「Signature ID」または「Snort Signature ID」を意味します。

SnortシグニチャID(SID)は、そのルールセット内の各ルールまたはシグニチャに割り当てられる 一意のIDです。これらのルールは、悪意のあるアクティビティやセキュリティの脅威を示す可能 性があるネットワークトラフィックの特定のパターンや動作を検出するために使用されます。各 ルールはSIDに関連付けられ、参照と管理が容易になります。

オープンソースのSnortについては、<u>SNORT</u>のWebサイトを参照してください。

Snortルールをフィルタリングする手順

Snort 2ルールのSIDを表示するには、 FMC Policies > Access Control > Intrusion, 次の図に示すように、右上隅のSNORT2オプションをクリックします。

Intrusion Policies Network	Analysis Policies				
Show Snort 3 Sync status 0	Q Search by Intrusion Policy, De	scription, or Base	All IPS Rules	IPS Mapping 🚯 Comp	are Policies Create Policy
Intrusion Policy	Description	Base Policy	Usage Information		
FTD1_Intrusion		Balanced Security and Connecti.	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version 📝 🖥 🖆 👕

Snort 2

移動先 Rules > Rule Update SIDをフィルタリングする最新の日付を選択します。

Policy Information Rules Cisco Recommendations	Rules Rule Configuration Rule Content	Filter:		
> Advanced Settings	Category	SRU:"Snort	Rule Updat	ate 2023 04 11 001 vrt"
Classifications Microsoft Vulnerabilities Microsoft Vulnerabilities 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 04 11 001 vrt Changed	Classifications	0 selected ru	les of 2961	1
	Rule State •	Event Fil	Filtering	
	GID	SID	Message 1	
	Priority Rule Update	1	60221	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
	 Snort Rule Update 2021 05 03 001 vrt Snort Rule Update 2022 01 06 001 vrt Snort Rule Update 2023 04 11 001 vrt Changed 	1	60220	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
		1	60648	BROWSER-CHROME Chrome IPC memory dump attempt
		1	60647	BROWSER-CHROME Chrome IPC memory dump attempt
	New ▶ Isp rel 20210503 2107	1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt

Rules					< Back
Rule Configuration	Ciltor:				
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 Very Event Filtering Very Dynamic State Alerting Comments				
Preprocessors					
Priority	GID SID Message ↑	\rightarrow	● ▼	0	
Rule Update	1 UTUTZ readmo file deteated	~			
04 10 001 vrt					î
Snort Rule Update 2023	1 61615 OS-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow			•
		< <	1	of 1	> >

Snortルールで使用可能なSID

以下のオプションから必要なものを選択します。 Rule State 図に示すように。

Rules								< Bac	k
Rule Configuration Rule Content Category	Filter: SRU:"Snort F	Rule Update 20	23 04 11 001 vrt"					×	?
Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific	16 selected rul Policy Rule State ▼	les of 16 Event Filterin	▼ g ▼ Dynamic State ▼ Alerting ▼ Comments ▼						
Preprocessors Priority Rule Update	Generate Eve	ents	ssage ↑	→ ^)	-	
04 10 001 vrt Snort Rule Update 2023 04 11 001 vrt	Disable		-WINDOWS Microsoft Windows AFD.sys privilege escalation	→ < <	1	(of 1	> >	Y

ルールの状態の選択

Snort 3ルールのSIDを表示するには、 FMC Policies > Access Control > Intrusion 次の図に示すように、右上 隅のSNORT3オプションをクリックします。

Intrusion Policies Network	Analysis Policies				
Show Snort 3 Sync status ①	C Search by Intrusion Policy, De	scription, or Base	All IPS Rules	IPS Mapping Compa	Create Policy
FTD1_Intrusion	Description	Base Policy Balanced Security and Connecti	No Access Control Policy	Snort 2 Version	Snort 3 Version 💉 🖥 🖆
			NO Device		

Snort 3

移動先 Advanced Filters をクリックし、図に示すようにSIDをフィルタリングする最新の日付を選択 します。

< Intrusion Policy Policy Name FTD1_Intrusion	Used by: No Access Control Policy	No Device
Mode Prevention Sase Policy Base Policy B	slanced Security and Connectivity 51 Overridden 0 Rewrite 0 Pass 0 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 irrespective of rule group	
All Rules Reco	Rule Action C Search by CVE, SID, Reference info, or Rule Message 48,870 rules Preset Filters: 470 Alert rules 9,151 Block rules 39,249 Disabled rules 0 Overridden rules Advanced Filters	
Server (8 groups) Server (8 groups)	GID:SID Info Rule Action Assigned Groups I:28496 [] BROWSER-IE Microsoft Internet Explore Alert (Default) Browser/Internet Explo	°a ≠

Snort 3フィルタ

r

Advanced Filters

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

0

高度なフィルタの下のLSP

Advanced Fil	ters 🕜	
LSP	lsp rel 20230420 1056 V	٦
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select v	
Microsoft Vulnerabilities	Select v	
	Cancel OK	
GPバージョン		
All Rules All rules assigned to current intrusion	n policy irrespective of rule group	
Rule Action 🗸	lsp:lsp rel 20230420 1056 X	>
22 🝸 48,870 rules	Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advanced Filter Rule Action Assigned Groups	S
> 1:300509 🗂 MALWARE-B	ACKDOOR Win.Backdoor 🕒 Block (Default) 🗸 Malware/Backdoor 🔒 🎙	

Sidの事前設定フィルタ

以下のオプションから必要なものを選択します。 Rule state 図に示すように。

All Rule	es ssigned to cu	urrent intrusion policy irrespective of rule	group			
Rule Acti	ion 2 🍸 48,870	rules Preset Filters: 0 Alert rules	X 11 Block rules 11 Disabled rules 0	Overridden rules Advanced Filters	×	ļ
	GID:SID	Info	Rule Action ¹	Assigned Groups		
› 🗹	1:300509 Ґ	MALWARE-BACKDOOR Win.Backdoor	Block (Default)	Malware/Backdoor 🛛 🖥 🗭		^
						-

ルールアクション

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。