Filter snortregels op basis van SRU en LSP versie van Firepower Devices die door FMC worden beheerd

Inhoud	
Inleiding	
Voorwaarden	
Vereisten	
Gebruikte componenten	
Achtergrondinformatie	
Procedure om gesorteerde regels te filteren	

Inleiding

Dit document beschrijft hoe u snurkregels kunt filteren op basis van de versie Cisco Secure Rule Update (SRU) en Link State Packet (LSP) van vuurkrachtapparaten die worden beheerd door het Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van opensource Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Dit artikel is van toepassing op alle Firepower platforms
- Cisco Firepower Threat Defence (FTD), waarop softwareversie 7.0.0 wordt uitgevoerd
- Firepower Management Center Virtual (FMC) waarop softwareversie 7.0.0 wordt uitgevoerd

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

In de context van inbraakdetectiesystemen (IDS) en inbraakpreventiesystemen (IPS) staat "SID" voor "Signature ID" of "Snort Signature ID".

Een Sort Signature ID (SID) is een unieke identificator die aan elke regel of handtekening binnen de regelset is toegewezen. Deze regels worden gebruikt om specifieke patronen of gedragingen in netwerkverkeer te detecteren die kunnen duiden op kwaadaardige activiteit of beveiligingsbedreigingen. Elke regel is gekoppeld aan een SID om gemakkelijk referentie en beheer mogelijk te maken.

Bezoek de <u>SNORT</u>-website voor informatie over opensource Snort.

Procedure om gesorteerde regels te filteren

Als u de SID's van de regel Sneltoets 2 wilt bekijken, navigeert u naar FMC Policies > Access Control > Intrusion, klik vervolgens op de SNORT2-optie in de rechterbovenhoek, zoals in de afbeelding:

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

Sorteren 2

Naar navigeren Rules > Rule Update en selecteer de meest recente datum om de SID te filteren.

Policy Information Rules Cisco Recommendations	Rules	Filter:		
> Advanced Settings	Category	SRU:"Snort	Rule Upda	te 2023 04 11 001 vrt"
> Policy Layers	Classifications Microsoft Vulnerabilities Microsoft Worms	0 selected ru Rule State ▼	les of 2961 Event Fi	Itering ▼ Dynamic State ▼ Alerting ▼ Comments ▼
	Platform Specific Preprocessors	GID	SID	Message 🔿
	Priority Rule Update	1	60221	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
	 Snort Rule Update 2021 05 03 001 vrt Snort Rule Update 2020 01 	1	60220	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
	Short Rule Update 2022 01 06 001 vrt Short Rule Update 2023 04	1	60648	BROWSER-CHROME Chrome IPC memory dump attempt
	11 001 vrt Changed	1	60647	BROWSER-CHROME Chrome IPC memory dump attempt
1.11.1	New ▶ lsp rel 20210503 2107	1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt

Regelupdate

Rules					<	Back
Rule Configuration	Filterer					
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		0	Ð	-
Rule Update	viviz readme file detected	~				
04 10 001 vrt	reddine nie deleted					- 1
Snort Rule Update 2023	1 61615 OS-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow				Ψ.
		< <	1	of	1 >	>>

Beschikbare Sid's volgens snelregels

Selecteer een gewenste optie onder Rule State zoals in de afbeelding.

Rules								<	Back
Rule Configuration Rule Content	Filter:								
Category	SRU: Short F	Rule Update 20	23 04 11 001 vrt*					X	
Classifications	16 selected ru	les of 16							
Microsoft Vulnerabilities	Dellau		_						
Microsoft Worms	Policy	_	•						
Platform Specific	Rule State 🔻	Event Filterin	g Dynamic State Alerting Comments						
Preprocessors	Conorata Eu	anto							
Priority	Generate Eve	ents	sage ↑	\rightarrow		T (0	Ð	.
Rule Update	Drop and Ge	enerate Events	tme file detected	~					
04 10 001 vrt	4 10 001 vrt Disable								
Snort Rule Update 2023			-WINDOWS Microsoft Windows AFD.sys privilege escalation						Ŧ
				< <	1		of 1	>	\geq

Regelstaten selecteren

Als u de SID's van de snort 3-regel wilt weergeven, navigeert u naar FMC Policies > Access Control > Intrusion Klik vervolgens op de SNORT3-optie in de rechterbovenhoek, zoals in de afbeelding:

Intrusion Policies Network Analysis Policies							
Show Snort 3 Sync status	Q Search by Intrusion Policy, De	scription, or Base		All IPS Rules	IPS Mapping Compa	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	n / 8 C T

Sorteren 3

Naar navigeren Advanced Filters en selecteer de meest recente datum om de SID te filteren zoals in de afbeelding.

< Intrusion Policy Policy Name FTD1_Intrusion		~	Use	ad by: No Access Control Policy No Device
Mode Prevention Sase Policy Base Policy B	anced Security and Connectin	ivity te 0 Pass 0 Drop 0 F	teject 0	
Rule Groups				Back To Top
50 items + Q Search Rule Group Excluded Included	All Rules All rules assigned to current	t intrusion policy irrespective of rul	e group	
Overridden	Rule Action	✓ Q Search by CVE, SID, I	Reference Info, or Rule Message	
All Rules Reco	48,870 rules	Preset 470 Alert rules Filters: Advanced Filter	9,151 Block rules 39,249 Disabled	I rules 0 Overridden rules
> Browser (6 groups)	GID:SID Info		Rule Action 0	Assigned Groups
> Server (8 groups)	> □ 1:28496 🗹 BRO	WSER-IE Microsoft Internet Explore.	🔺 Alert (Default) 🗸	Browser/Internet Explo 📭 🗭 🖡

Sorteren op 3 filters

r

Advanced Filters

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

0

LSP onder geavanceerd filter

Advanced Fil	ters @)
LSP	Isp rel 20230420 1056 ✓ Show Only * ✓ New ✓]
Classifications	Select v	
Microsoft Vulnerabilities	Select V	
	Cancel OK	
_SP-versie		
All Rules All rules assigned to current intrusion	policy irrespective of rule group	
Rule Action 🗸	lsp:lsp rel 20230420 1056 X	×
22 🝸 48,870 rules F	Image: Second state of the second s	ers

Vooraf ingestelde filter voor Sid's

>

Selecteer een gewenste optie onder Rule state zoals in de afbeelding.

1:300509 🖸 MALWARE-BACKDOOR Win.Backdoor.... 🕒 Block (Default)

	All Rule	Ssigned to cu	urrent intrusion policy irrespective	of rule group			
	Rule Actio	on ? 🍸 48,870	rules Preset Filters: 0 Alert ru	ules 11 Block rules 11 Disabled rules	0 Overridden rules Advanced Filter	×	
		GID:SID	Info	Rule Action ⁽⁾	Assigned Groups		
	> 🗹	1:300509 [MALWARE-BACKDOOR Win.Backd	door 🖨 Block (Default) 🗸	Malware/Backdoor 🛛 🖥 📕		•
Г							Ŧ

Malware/Backdoor

 \sim

Regelgeving

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.