Reglas de filtrado de snort basadas en la versión de SRU y LSP de los dispositivos Firepower administrados por FMC

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Procedimiento para filtrar reglas Snort

Introducción

Este documento describe cómo filtrar reglas de snort basadas en la versión de actualización de reglas seguras (SRU) y paquete de estado de enlace (LSP) de Cisco de los dispositivos firepower administrados por Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Snort de código abierto
- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- · Este artículo es aplicable a todas las plataformas Firepower
- Cisco Firepower Threat Defense (FTD), que ejecuta la versión de software 7.0.0
- Firepower Management Center Virtual (FMC), que ejecuta la versión de software 7.0.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En el contexto de los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS), "SID" significa "ID de firma" o "ID de firma de Snort".

Un identificador de firma de Snort (SID) es un identificador único asignado a cada regla o firma dentro de su conjunto de reglas. Estas reglas se utilizan para detectar patrones o comportamientos específicos en el tráfico de red que pueden indicar actividad maliciosa o amenazas de seguridad. Cada regla se asocia a un SID para facilitar la referencia y la administración.

Para obtener información sobre Snort de código abierto, visite el sitio web de SNORT.

Procedimiento para filtrar reglas Snort

Para ver los SID de la regla de Snort 2, vaya a FMC Policies > Access Control > Intrusion, a continuación, haga clic en la opción SNORT2 en la esquina superior derecha, como se muestra en la imagen:

Intrusion Policies Network	Analysis Policies						
Show Snort 3 Sync status ①	 Search by Intrusion Policy, De Description 	scription, or Base		All IPS Rules	IPS Mapping	Compare Policies	Create Policy
FTD1_Intrusion		Balanced Security and Co	onnecti	No Access Control Policy No Device	Snort 2 Ver	rsion Snort 3 Ve	rsion 📝 🛱 🖆 🗑

Snort 2

Desplácese hasta Rules > Rule Update y seleccione la fecha límite para filtrar el SID.

Policy Information Rules Cisco Recommendations	Rules Rule Configuration Rule Content	Filter:		
> Advanced Settings	Category	SRU:"Snort	t Rule Upda	te 2023 04 11 001 vrt"
> Policy Layers	Classifications Microsoft Vulnerabilities Microsoft Worms	0 selected ru Rule State ▼	lles of 2961 Event Fi	Itering ▼ Dynamic State ▼ Alerting ▼ Comments ▼
	Platform Specific Preprocessors	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	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
	Changed	1	60647	BROWSER-CHROME Chrome IPC memory dump attempt
- 2 - 3 2 2	New ▶ Isp rel 20210503 2107	1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt

Actualización de reglas

Rules					< Ba	ck
Rule Configuration	Filter					
Rule Content	Filter.					
Category	SRU:"Snort Rule Update 2023 04 11 001 vrt"				\times	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	Ļ	
Rule Update	readme file detected	~				
04 10 001 vrt						
Snort Rule Update 2023	1 61615 OS-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow				Ŧ
		< <	1	of 1	> >	

Sid disponibles bajo reglas de snort

Seleccione una opción necesaria en Rule State como se muestra en la imagen.

Rules						< Ba	ıck
Rule Configuration	Filter						
Rule Content							
Category	SRU:"Snort Rule Update	2023 04 11 001 vrt"				\times	?
Classifications	16 selected rules of 16						
Microsoft Vulnerabilities							
Microsoft Worms	Policy	¥					
Platform Specific	Rule State Event Filte	ring Dynamic State Alerting Comments					
Preprocessors	Concrete Evente						
Priority	Generate Events	ssage ↑	\rightarrow	T	0	, 💻	
Rule Update	Drop and Generate Event	S the file detected	~				
04 10 001 vrt							-
Snort Rule Update 2023	Disable	-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow				*
04 11 001 vrt ▼	1		< <	1	of 1	> >	1

Selección de estados de regla

Para ver los SID de la regla Snort 3, vaya a FMC Policies > Access Control > Intrusion A continuación, haga clic en la opción SNORT3 de la esquina superior derecha, como se muestra en la imagen:

Intrusion Policies Network	Analysis Policies							
Show Snort 3 Sync status 1	C Search by Intrusion Policy, De	escription, or Base		All IPS Rules	IPS Mapping	Compa	re Policies	Create Policy
FTD1_Intrusion	beachpilon	Balanced Security and	Connecti	No Access Control Policy No Device	Snort 2 \	/ersion	Snort 3 Versior	n 🖊 🗄 🖒 🗑

Snort 3

Desplácese hasta Advanced Filters y seleccione la fecha límite para filtrar el SID como se muestra en la imagen.

< Intrusion Policy Policy Name FTD1_Intrusion		V	Used by: No Access Control Policy No Device
Mode Prevention V Base Policy Base Disabled 39249 Alert 470 Block 91	Inced Security and Connectivity	0 Drop 0 Reject 0	
Rule Groups			Back To Top
50 items + Search Rule Group Excluded Included	All Rules All rules assigned to current intrusion po	licy irrespective of rule group	
Overridden	Rule Action 🗸 🔍	Search by CVE, SID, Reference Info, or Rule Mess	age
All Rules Reco	48,870 rules Pres	et 470 Alert rules 9,151 Block rules 39,249 S: Advanced Filters	Disabled rules 0 Overridden rules
> Browser (6 groups)	GID:SID Info	Rule Action 1	Assigned Groups
> Server (8 groups)	> 1:28496 🖸 BROWSER-IE Mic	rosoft Internet Explore 🔺 Alert (Default) 🗸	Browser/Internet Explo 🖷 💻 🖡

Filtros Snort 3

r

Advanced Filters

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

0

LSP bajo filtro avanzado

Advanced Fil	ters 0
LSP	Isp rel 20230420 1056
Classifications	Select
Microsoft Vulnerabilities	Select v
	Cancel
versión de LSP	
All Rules All rules assigned to current intrusio	n policy irrespective of rule group
22 T 48,870 rules	Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advanced Filters Rule Action Assigned Groups
> 🗌 1:300509 🕻 MALWARE-E	BACKDOOR Win.Backdoor 🕒 Block (Default) 🗸 Malware/Backdoor 🔹 💻

Filtro predefinido para Sid's

Seleccione una opción necesaria en Rule state como se muestra en la imagen.

All Rule	ES issigned 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	×	
	GID:SID	Info	Rule Action ⁽¹⁾	Assigned Groups		
› 🗹	1:300509 Ґ	MALWARE-BACKDOOR Win.Backdoor	Block (Default)	Malware/Backdoor 🛛 🖥 🗭		-
						Ŧ

Acción de regla

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).