Filtern von Snort-Regeln basierend auf der SRUund LSP-Version von FirePOWER-Geräten, die von FMC verwaltet werden

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Verfahren zum Filtern von Snort-Regeln

Einleitung

In diesem Dokument wird beschrieben, wie Snort-Regeln basierend auf der Cisco Secure Rule Update (SRU)- und Link State Packet (LSP)-Version von Firepower-Geräten gefiltert werden, die vom FirePOWER Management Center (FMC) verwaltet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse von Open-Source Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Dieser Artikel gilt für alle Firepower-Plattformen.
- Cisco Firepower Threat Defense (FTD) mit der Softwareversion 7.0.0
- FirePOWER Management Center Virtual (FMC) mit der Softwareversion 7.0.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Im Kontext von Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) steht "SID" für "Signature ID" oder "Snort Signature ID".

Eine Snort Signature ID (SID) ist eine eindeutige ID, die jeder Regel oder Signatur innerhalb ihres Regelsatzes zugewiesen wird. Diese Regeln werden verwendet, um bestimmte Muster oder Verhaltensweisen im Netzwerkverkehr zu erkennen, die auf schädliche Aktivitäten oder Sicherheitsbedrohungen hinweisen können. Jede Regel ist mit einer SID verknüpft, um den Zugriff und die Verwaltung zu vereinfachen.

Weitere Informationen zu Open-Source Snort finden Sie auf der <u>SNORT-</u>Website.

Verfahren zum Filtern von Snort-Regeln

Um die Snort 2-Regel-SIDs anzuzeigen, navigieren Sie zu FMC Policies > Access Control > Intrusion, Klicken Sie anschließend auf die SNORT2-Option in der rechten oberen Ecke, wie im Bild gezeigt:

Intrusion Policies Network	Analysis Policies				
Show Snort 3 Sync status ① Intrusion Policy	Q Search by Intrusion Policy, De Description	scription, or Base Base Policy	All IPS Rules IPS Usage Information	Mapping O 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

Navigieren Sie zu Rules > Rule Update und wählen Sie das späteste Datum aus, um die SID zu filtern.

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 Policy Layers Policy Layers Microsoft Vulnerabilities Microsoft Worms Platform Specific Preprocessors Priority Rule Update	0 selected ru Rule State ▼	lles 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	1	60220	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt
> Snort R 06 001 Snort R 11 001 Char	Short Rule Update 2022 01 06 001 vrt	1	60648	BROWSER-CHROME Chrome IPC memory dump attempt
	Changed	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

Regelaktualisierung

Rules					< Back
Rule Configuration	Filter				
Rule Content	Filter:				
Category	SRU:"Snort Rule Update 2023 04 11 001 vrt"				\times
Classifications	0 selected rules of 16				
Microsoft Vulnerabilities					
Microsoft Worms	Policy				
Platform Specific	Rule State Very Event Filtering Very Dynamic State Alerting Comments Very				
Preprocessors					
Priority	GID SID Message ↑	\rightarrow	• •	Ū 🛛	, 💻
Rule Update	UIUIZ readme file detected	~			
04 10 001 vrt					î
Snort Rule Update 2023	1 61615 OS-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow			•
04 11 001 vrt ▼		< <	1	of 1	> >

Verfügbare Sids gemäß Snort-Regeln

Wählen Sie die gewünschte Option unter Rule State wie im Bild dargestellt.

Rules					r	< Back
Rule Configuration Rule Content Category	Filter: SRU:"Snort Rule Update 20	023 04 11 001 vrt"				× 0
Classifications Microsoft Vulnerabilities Microsoft Worms	16 selected rules of 16 Policy	¥				
Platform Specific Preprocessors Priority	Rule State Event Filterin Generate Events	ng ▼ Dynamic State ▼ Alerting ▼ Comments ▼ ssage ↑	→	• •	0	-
Rule Update 04 10 001 vrt Snort Rule Update 2023 04 11 001 vrt	Drop and Generate Events Disable	dme file detected -WINDOWS Microsoft Windows AFD.sys privilege escalation	→ < <	1	of 1	>>

Auswählen von Regelzuständen

Um die Snort 3-Regel-SIDs anzuzeigen, navigieren Sie zu FMC Policies > Access Control > Intrusion, klicken Sie anschließend auf die SNORT3-Option in der rechten oberen Ecke, wie in der Abbildung dargestellt:

Intrusion Policies Network	Analysis Policies					
Show Snort 3 Sync status 🌒	C Search by Intrusion Policy, De Description	scription, or Base Base Policy	All IPS Rules Usage Information	IPS Mapping Compa	re Policies C	reate Policy
FTD1_Intrusion		Balanced Security and Connecti	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version	/ 🛙 🖒 🗑

Snort 3

Navigieren Sie zu Advanced Filters und wählen Sie das späteste Datum aus, um die SID wie im Bild dargestellt zu filtern.

< Intrusion Policy Policy Name FTD1_Intrusion	Used by: No Access Control Polic	y No Device	
Mode Prevention Base Policy Base Disabled 39249 Alert 470 Block 91	alanced 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	All Rules All rules assigned to current intrusion policy irrespective of rule group		
Overridden	Rule Action V Q Search by CVE, SID, Reference Info, or Rule Message		
All Rules Reco	48,870 rules Preset 470 Alert rules 9,151 Block rules 39,249 Disabled rules 0 Overridden rules Filters: Advanced Filters	I	
> Browser (6 groups)	GID:SID Info Rule Action O Assigned Groups		
> Server (8 groups)	> 1:28496 🖸 BROWSER-IE Microsoft Internet Explore ▲ Alert (Default) ∨ Browser/Internet Explo		

Snort 3-Filter

r

Advanced Filters

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

0

LSP mit erweitertem Filter

Advanced Fil	ters	?
LSP	Isp rel 20230420 1056 ✓ Show Only * ✓ New ✓ Changed	
Classifications	Select v	
Microsoft Vulnerabilities	Select V	
_SP-Version	Cancel OK	
All Rules All rules assigned to current intrusion	policy irrespective of rule group	
Rule Action 22 T 48,870 rules GID:SID Info	Isp:Isp rel 20230420 1056 × reset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advanced F Rule Action Assigned Groups	×

Voreingestellter Filter für Sid's

>

Wählen Sie die gewünschte Option unter Rule state wie im Bild dargestellt.

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

	All Rules All rules assigned to current intrusion policy irrespective of rule group Rule Action Isp:lsp rel 20230420 1056 × 22 2 1 22 1 48,870 rules Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advanced Filters	×)
	GID:SID Info Rule Action I Assigned Groups		
	> 🗹 1:300509 🖸 MALWARE-BACKDOOR Win.Backdoor 😑 Block (Default) ∨ Malware/Backdoor 🖥 💻	l	
I			-

Malware/Backdoor

 \sim

Regelaktion

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.