Filtrar regras de Snort com base nas versões SRU e LSP de dispositivos Firepower gerenciados pelo FMC

Contents Introdução Pré-requisitos Requisitos Componentes Utilizados

Informações de Apoio Procedimento para filtrar regras do Snort

Introdução

Este documento descreve como filtrar regras de snort com base na versão Cisco Secure Rule Update (SRU) e Link State Packet (LSP) de dispositivos firepower gerenciados pelo Firepower Management Center (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Snort de código aberto
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Este artigo se aplica a todas as plataformas Firepower
- O Cisco Firepower Threat Defense (FTD), que executa a versão 7.0.0 do software
- Firepower Management Center Virtual (FMC) que executa a versão de software 7.0.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

No contexto dos sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS), "SID" significa "ID de assinatura" ou "ID de assinatura Snort".

Um Snort Signature ID (SID) é um identificador exclusivo atribuído a cada regra ou assinatura dentro de seu conjunto de regras. Essas regras são usadas para detectar padrões ou comportamentos específicos no tráfego de rede que podem indicar atividade mal-intencionada ou ameaças à segurança. Cada regra é associada a um SID para permitir fácil referência e gerenciamento.

Para obter informações sobre o Snort de código aberto, visite o site do SNORT.

Procedimento para filtrar regras do Snort

Para exibir os SIDs de regra do Snort 2, navegue até FMC Policies > Access Control > Intrusion, em seguida, clique na opção SNORT2 no canto superior direito, conforme mostrado na imagem:

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 Usage Information	IPS Map	ping 🕕	Com	pare Policies	Create Policy
FTD1_Intrusion		Balanced Security and	Connecti	No Access Control Policy No Device		Snort 2	Version	Snort 3 Vers	ion 🗡 🖥 🖆 🗑

Snort 2

Navegue até Rules > Rule Update e selecione a data mais recente para filtrar o SID.

Policy Information Rules Cisco Recommendations	Rules Rule Configuration Rule Content	Filter:					
> Advanced Settings	Category	SRU:"Snort	t Rule Updat	te 2023 04 11 001 vrt"			
Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific Preprocessors Priority Rule Update Snort Rule Update 2021 Snort Rule Update 2021 Snort Rule Update 2021 Snort Rule Update 2022 O6 001 vrt Snort Rule Update 2028 If 1001 vrt Changed	Classifications Microsoft Vulnerabilities Microsoft Worms	0 selected ru Rule State ▼	selected rules of 2961 Rule State ▼ Event Filtering ▼ Dynamic State ▼ Alerting ▼ Commer				
	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 2028 02 11 001 vrt Changed	GID	SID	Message 🕆			
		1	60221	BROWSER-CHROME Chrome IPC domDistiller sandbox escape attempt			
		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			
- 7 - 77 3	New ▶ Isp rel 20210503 2107	1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt			

Atualização de regra

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	Ø	-
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 >	>>

Sids disponíveis sob regras de snort

Selecione uma opção necessária em Rule State conforme mostrado na imagem.

Rules						< [Back
Rule Configuration Rule Content	Filter:						
Category	SRU:"Snort Rule Update	2023 04 11 001 vrt"				\times	0
Classifications	16 selected rules of 16						
Microsoft Vulnerabilities							
Microsoft Worms	Policy	•					
Platform Specific	Rule State V Event Filte	ering Dynamic State Alerting Comments					
Preprocessors	Generate Events						
Priority	Generate Events	sage ↑	\rightarrow	⊕ ▼	(U	0	
Rule Update	Drop and Generate Ever	ts dme file detected	~				
04 10 001 vrt							- 1
Snort Rule Update 2023	Disable	-WINDOWS Microsoft Windows AFD.sys privilege escalation	\rightarrow				*
			< <	1	of	1 >	>

Seleção de estados de Regra

Para exibir os SIDs de regra do Snort 3, navegue até FMC Policies > Access Control > Intrusion e, em seguida, clique na opção SNORT3 no canto superior direito, conforme mostrado na imagem:

Intrusion Policies Network	Analysis Policies						
Show Snort 3 Sync status	C Search by Intrusion Policy, De	escription, or Base		All IPS Rules	IPS Mapping Cor	pare Policies	Create Policy
Intrusion Policy	Description	Base Policy		Usage Information			
FTD1_Intrusion		Balanced Security and Co	Connecti	No Access Control Policy No Device	Snort 2 Version	Snort 3 Vers	ion 🖊 🖥 🖆 🗑

Snort 3

Navegue até Advanced Filters e selecione a data mais recente para filtrar o SID como mostrado na imagem.

< Intrusion Policy Policy Name FTD1_Intrusion			~		Used by: No Access C	Control Policy No Device	
Mode Prevention V Base Policy Base Policy Disabled 39249 Alert 470 Block 91	alanced Security and Conr 51 Overridden 0 Re	ectivity	Pass 0 Drop 0 Re	eject 0			
Rule Groups						Back To Top	
50 items + Q Search Rule Group Excluded Included	All Rules All rules assigned to cur	rrent intrusio	on policy irrespective of rule	group			
Overridden	Rule Action	\sim	Q Search by CVE, SID, Reference Info, or Rule Message				
All Rules Reco	48,870 rules		Preset 470 Alert rules Filters: Advanced Filters	9,151 Block rules 39,249 D	lisabled rules 0 Overrido	den rules	
> Browser (6 groups)	GID:SID	Info		Rule Action	Assigned Group	os	
> Server (8 groups)	> 🗌 1:28496 Ґ	BROWSER-I	IE Microsoft Internet Explore	Alert (Default)	Browser/Intern	et Explo 🖻 🗭	

3 filtros Snort

r

Advanced Filters

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

0

LSP no filtro avançado

Advanced Fil	ters	
LSP	Isp rel 20230420 1056 ✓ Show Only * ✓ New ✓]
Classifications	Select V	
Microsoft Vulnerabilities	Select v	Ĵ
	Cancel OK	
versão de LSP		
All Rules All rules assigned to current intrusion Rule Action 22 48,870 rules GID:SID Info	Isp:Isp rel 20230420 1056 X Preset Filters: 0 Alert rules 11 Block rules 11 Disabled rules 0 Overridden rules Advanced Fil Rule Action 1 Assigned Groups	×
> 🗌 1:300509 🗂 MALWARE-B	ACKDOOR Win.Backdoor 😑 Block (Default) 🗸 Malware/Backdoor 🖥	-

Filtro predefinido para Sid's

Selecione uma opção necessária em Rule state conforme mostrado na imagem.

	All Rules Il rules assigned to current intrusion policy irrespective of rule group	
	Rule Action Isp:lsp rel 20230420 1056 × × 2 2 7 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 🖥 💻	^
E		-

Ação da regra

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.