# 根据FMC管理的Firepower设备的SRU和LSP版本 过滤Snort规则

### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u>

<u>过滤Snort规则的过程</u>

## 简介

本文档介绍如何根据Firepower管理中心(FMC)管理的firepower设备的思科安全规则更新(SRU)和链路状态数据包(LSP)版本过滤snort规则。

### 先决条件

#### 要求

Cisco 建议您了解以下主题:

- 开源Snort知识
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

#### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- 本文适用于所有Firepower平台
- 运行软件版本7.0.0的思科Firepower威胁防御(FTD)
- 运行软件版本7.0.0的Firepower管理中心虚拟(FMC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

### 背景信息

在入侵检测系统(IDS)和入侵防御系统(IPS)环境中,"SID"表示"签名ID"或"Snort签名ID"。

Snort签名ID(SID)是分配给规则集内每个规则或签名的唯一标识符。这些规则用于检测网络流量中

可能表示恶意活动或安全威胁的特定模式或行为。每个规则都与SID关联,以便于参考和管理。

有关开源Snort的信息,请访问<u>SNORT网</u>站。

### 过滤Snort规则的过程

要查看Snort 2规则SID,请导航至 FMC Policies > Access Control > Intrusion, 然后,点击右上角的SNORT2选项,如图所示:

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 📝 🛱 🖆 🗑

Snort 2

导航至 Rules > Rule Update 并选择过滤SID的最新日期。

Policy Information Rules Cisco Recommendations > Advanced Settings	Rules Rule Configuration Rule Content	Filter:	t Dule I Indat	e 2023.04.11.001.vrt*
	Category Classifications			
> Policy Layers	Microsoft Vulnerabilities		les of 2961	
	Microsoft Worms	Rule State ▼	Event Fil	tering
Pi Pr Pr Ru	Platform Specific Preprocessors Priority Rule Update	GID	SID	Message 🕆
		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 Opdate 2022 01 06 001 vrt Snort Rule Update 2023 04	1	60648	BROWSER-CHROME Chrome IPC memory dump attempt
	Changed	1	60647	BROWSER-CHROME Chrome IPC memory dump attempt
3 373	New ▶ Isp rel 20210503 2107	1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt



Rules					< B	ack
Rule Configuration Rule Content	Filter:					
Category	SRU:"Snort Rule Update 2023 04 11 001 vrt"				X	U
Classifications	0 selected rules of 16					e
Microsoft Vulnerabilities						
Microsoft Worms	Policy					
Platform Specific	Rule State   Event Filtering   Dynamic State  Alerting  Comments					
Preprocessors						
Priority	GID SID Message ↑	$\rightarrow$	● ▼	0	9 🖛	
Rule Update	1 UTUTZ reading file detected	~				
04 10 001 vrt	readme lie detected					-
Snort Rule Update 2023	OS-WINDOWS Microsoft Windows AFD.sys privilege escalation					-
<u>04 11 001 vrt</u> ✓ ►		< > > ۱	1	of 1	> 3	>1

#### 在下面选择所需的选项 Rule State 如图所示.

Rules					< Bac	ck
Rule Configuration Rule Content	Filter:				×	•
Category	SRU:"Snort Rule Update	2023 04 11 001 vrt"			X	U
Classifications	16 selected rules of 16					
Microsoft Vulnerabilities	Deliev					
Microsoft Worms	Policy	•				
Platform Specific	Rule State V Event Filte	ring      Dynamic State      Alerting      Comments				
Preprocessors	Conorato Evonto					
Priority	Generale Events	ssage ↑	$\rightarrow$	● ▼	0 🖗 🗭	
Rule Update	Drop and Generate Even	Is the file detected	~			
04 10 001 vrt 🔺		ane me detected				
Snort Rule Update 2023	Disable	-WINDOWS Microsoft Windows AFD.sys privilege escalation	$\rightarrow$			Ŧ
04 11 001 vrt	1		< <	1	of 1 > >	I

选择规则状态

要查看Snort 3规则SID,请导航至 FMC Policies > Access Control > Intrusion ,然后点击右上角的SNORT3选 项,如图所示:

Intrusion Policies Network Analysis Policies						
Show Snort 3 Sync status ①	Q Search by Intrusion Policy, De	scription, or Base	All IPS Rules	IPS Mapping  Co	mpare Policies	Create Policy
Intrusion Policy	Description	Base Policy	Usage Information			
FTD1_Intrusion		Balanced Security and Connecti	No Access Control Policy No Device	Snort 2 Versior	Snort 3 Ver	rsion 🗡 🗎 🖆 🗑

Snort 3

### 导航至 Advanced Filters 并选择最新日期以过滤SID,如图所示。

< Intrusion Policy Policy Name FTD1_Intrusion	Used by: No Access Control Policy	No Device
Mode     Prevention     V     Base Policy B       Disabled     39249     Alert     470     Block     91	alanced Security and Connectivity       151     Overridden 0     Rewrite 0     Pass 0     Drop 0     Reject 0	
Rule Groups	E	Back To Top
50 items + Q Search Rule Group Excluded   Included	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   Advanced Filters	
> Browser (6 groups)	GID:SID Info Rule Action • Assigned Groups	
> Server (8 groups)	→ 1:28496 🖸 BROWSER-IE Microsoft Internet Explore 🔺 Alert (Default) 🗸 Browser/Internet Explo	∎ <b>#</b> _

Snort 3过滤器

# Advanced Filters

LSP	Select	~
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select	$\sim$
Microsoft	Select	$\sim$
vunerabilities		
	Cancel	ОК
高级过滤器下的LSP		
Advanced Filt	ers	0
LSP	lsp rel 20230420 1056	~
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select	~
Microsoft	Select	$\sim$
vuiterabilities		
	Cancel	К

0

All Rules All rules assigned to current intru	ision policy irrespective of rule group	
Rule Action	lsp:lsp rel 20230420 1056 🗙	×
22 🝸   48,870 rules	Preset Filters: 0 Alert rules   11 Block rules   11 Disabled r	ules 0 Overridden rules   Advanced Filters
GID:SID Info	Rule Action 💿	Assigned Groups
> 🗌 1:300509 🖬 MALWAR	E-BACKDOOR Win.Backdoor GBlock (Default)	Malware/Backdoor 🐴 🗭 💼
		<b>.</b> •

Sid的预设置过滤器

### 在下面选择所需的选项 Rule state 如图所示.

	All Rules		
	Rule Action     V     Isp:Isp rel 20230420 1056 ×	×	
I.	22 🔽   22 🍸   48,870 rules Preset Filters: 0 Alert rules   11 Block rules   11 Disabled rules   0 Overridden rules   Advanced Filters		
	GID:SID Info Rule Action () Assigned Groups		
	> 🔽 1:300509 🖸 MALWARE-BACKDOOR Win.Backdoor 🕒 Block (Default) 🗸 Malware/Backdoor		Î
ľ			Ŧ

规则操作

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。