# Filter Snort Rules Based on SRU and LSP Version of Firepower Devices Managed by FMC

### Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Procedure to filter Snort rules

## Introduction

This document describes how to filter snort rules based on the Cisco Secure Rule Update (SRU) and Link State Packet (LSP) version of firepower devices managed by the Firepower Management Centre (FMC).

## Prerequisites

#### Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of open-source Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

#### **Components Used**

The information in this document is based on these software and hardware versions:

- This article is applicable to all Firepower platforms
- Cisco Firepower Threat Defense (FTD) which runs software version 7.0.0
- Firepower Management Center Virtual (FMC) which runs software version 7.0.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

### **Background Information**

In the context of intrusion detection systems (IDS) and intrusion prevention systems (IPS), "SID" stands for "Signature ID" or "Snort Signature ID."

A Snort Signature ID (SID) is a unique identifier assigned to each rule or signature within its rule set. These rules are used to detect specific patterns or behaviors in network traffic that can indicate malicious activity or security threats. Each rule is associated with a SID to allow for easy reference and management.

For information on open-source Snort, please visit the **SNORT** website.

### **Procedure to filter Snort rules**

To view the Snort 2 rule SIDs, navigate to FMC Policies > Access Control > Intrusion, thereafter click the SNORT2 option in the top right corner, as shown in the image:

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 O Comp	are Policies Create Pol	olicy
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 📝 🖥 🗹	21

Snort 2

Navigate to Rules > Rule Update and select the latest date to filter the SID.

Policy Information Rules Cisco Recommendations	Rules Rule Configuration Rule Content	Filter:		
> Advanced Settings	Category Classifications	SRU:"Snort	t Rule Upda	te 2023 04 11 001 vrt"
> Policy Layers	Microsoft Vulnerabilities Microsoft Worms	Rule State •	Event Fi	Itering ▼ Dynamic State ▼ Alerting ▼ Comments ▼
	Platform Specific Preprocessors Priority Rule Update Snort Rule Update 2021 05 03 001 vrt Snort Rule Update 2022 01 06 001 vrt	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
	11 001 vrt Changed	1	60647	BROWSER-CHROME Chrome IPC memory dump attempt
3 333	New ▶ Isp rel 20210503 2107	1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt

Rule update

ack
0
1
- 11
*

Available Sid's under snort rules

Select a required option under Rule State as shown in the image.

Rules									~	< Ba	ck
Rule Configuration	Ciltary.										
Rule Content	Filter:										
Category	SRU:"Snort F	Rule Update 20	023 04	11 001 vrt"					2	$\times$	0
Classifications	16 selected ru	les of 16									
Microsoft Vulnerabilities											
Microsoft Worms	Policy	-		<b>~</b>							
Platform Specific	Rule State 🔻	Event Filterir	ng 🔻	Dynamic State  Alerting  Comments							
Preprocessors	Conorata Eu	anto	1								
Priority	Generate Eve	ents	sage	<b>↑</b>	$\rightarrow$	۲	T	0	0		
Rule Update	Drop and Ge	nerate Events	dme fi	le detected	~						
04 10 001 vrt			amen								
Snort Rule Update 2023	Disable		-WIND	DOWS Microsoft Windows AFD.sys privilege escalation							Ŧ
04 11 001 vrt ►					< <		1	of	1 )	> >	I

Selecting Rule states

To view the Snort 3 rule SIDs, navigate to FMC Policies > Access Control > Intrusion, thereafter click the SNORT3 option in the top right corner, as shown in the image:

Intrusion Policies Network	Analysis Policies					
Show Snort 3 Sync status 0	Q Search by Intrusion Policy, De	escription, or Base	All IPS Rules	IPS Mapping  Compa	are Policies Crea	ate 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	/ 8 🖒 🕯

Snort 3

#### Navigate to Advanced Filters and select the latest date to filter the SID as shown in the image.

< Intrusion Policy Policy Name FTD1_Intrusion	Used by: No Access Control Policy	No Device
Mode Prevention V 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   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 filters

# Advanced Filters

LSP	Select	~
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select	$\sim$
Microsoft Vulnerabilities	Select	~
	Cancel	OK
SP under advanced filter		
Advanced Fil	ters	0
LSP	lsp rel 20230420 1056	~
	Show Only * 🗹 New 🗹 Changed	
Classifications	Select	~
Microsoft Vulnerabilities	Select	~
	Cancel	K

0

All Rules All rules assigned to current intrusion	a policy irrespective of rule group	
Rule Action 🗸	lsp:lsp rel 20230420 1056 $\times$	×
22 🝸   48,870 rules P	Preset Filters: 0 Alert rules   11 Block rules   11 Disabled rules	s 0 Overridden rules   Advanced Filters
GID:SID Info	Rule Action 💶	Assigned Groups
> 🗋 1:300509 🖬 MALWARE-B/	ACKDOOR Win.Backdoor	Malware/Backdoor 🛯 📮 💼
		· ·

Pre-set filter for Sid's

Select a required option under Rule state as shown in the image.

	All Rules	
	All rules assigned to current intrusion policy irrespective of rule group	
	Rule Action	×
Ĺ	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 I Assigned Groups	
	> 🗹 1:300509 🗹 MALWARE-BACKDOOR Win.Backdoor 😑 Block (Default) 🗸 Malware/Backdoor 🔹 💻	-
ł		-

Rule action