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

Contents

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

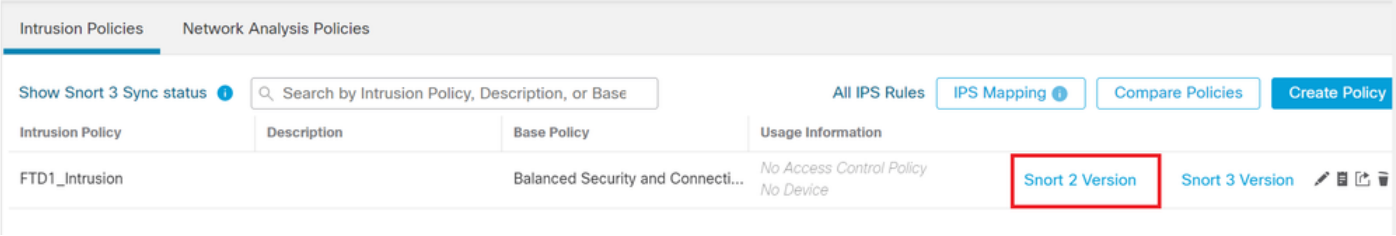
In the context of intrusion detection systems (IDS) and intrusion prevention systems (IPS), "SID" stands for "Signature ID" or "Snort Signature ID."

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

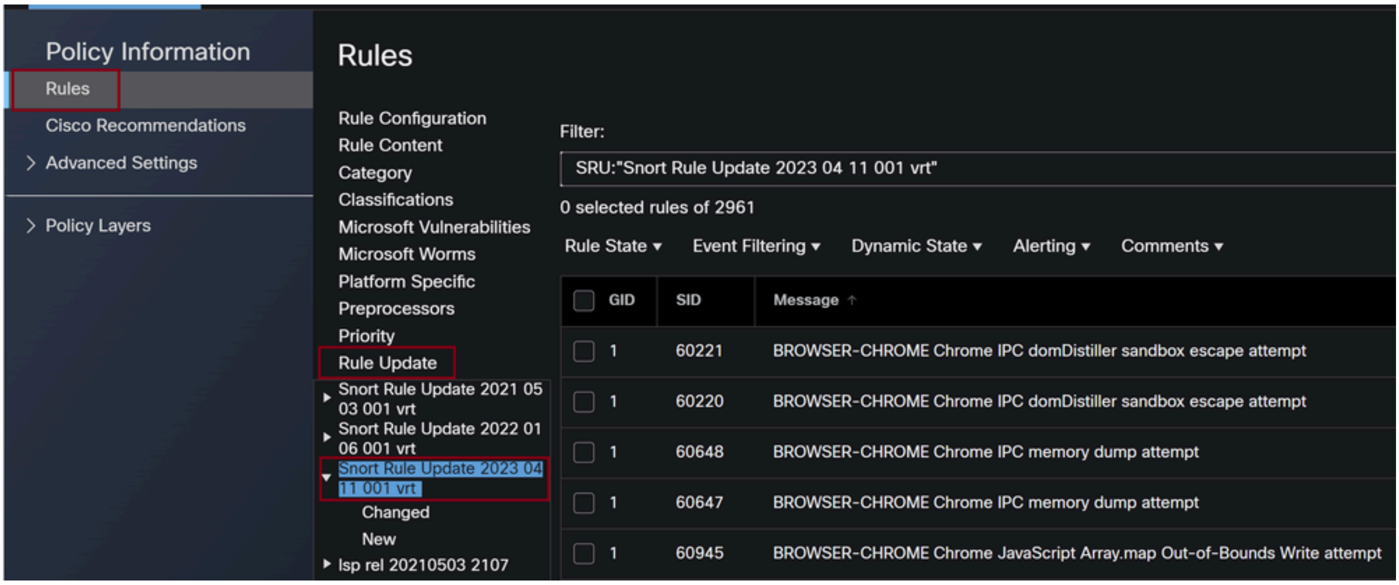
To view the Snort 2 rule SIDs, navigate to FMC Policies > Access Control > Intrusion, thereafter click the SNORT2 option in the top right corner, as shown in the image:



Intrusion 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

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



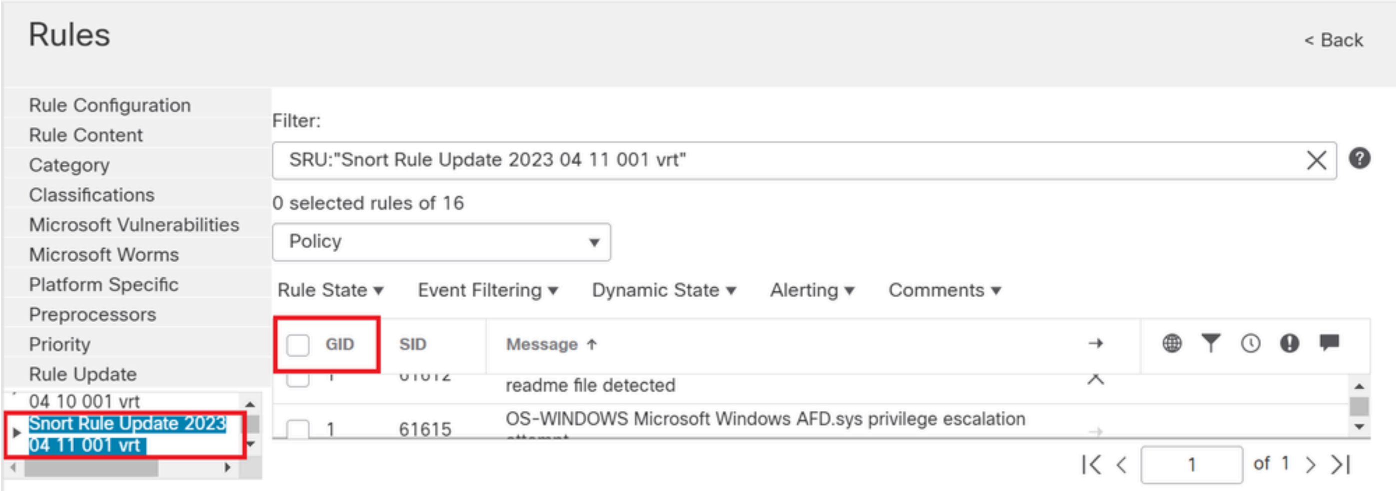
Filter:

SRU:"Snort Rule Update 2023 04 11 001 vrt"

0 selected rules of 2961

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
1	60945	BROWSER-CHROME Chrome JavaScript Array.map Out-of-Bounds Write attempt

Rule update



Filter:

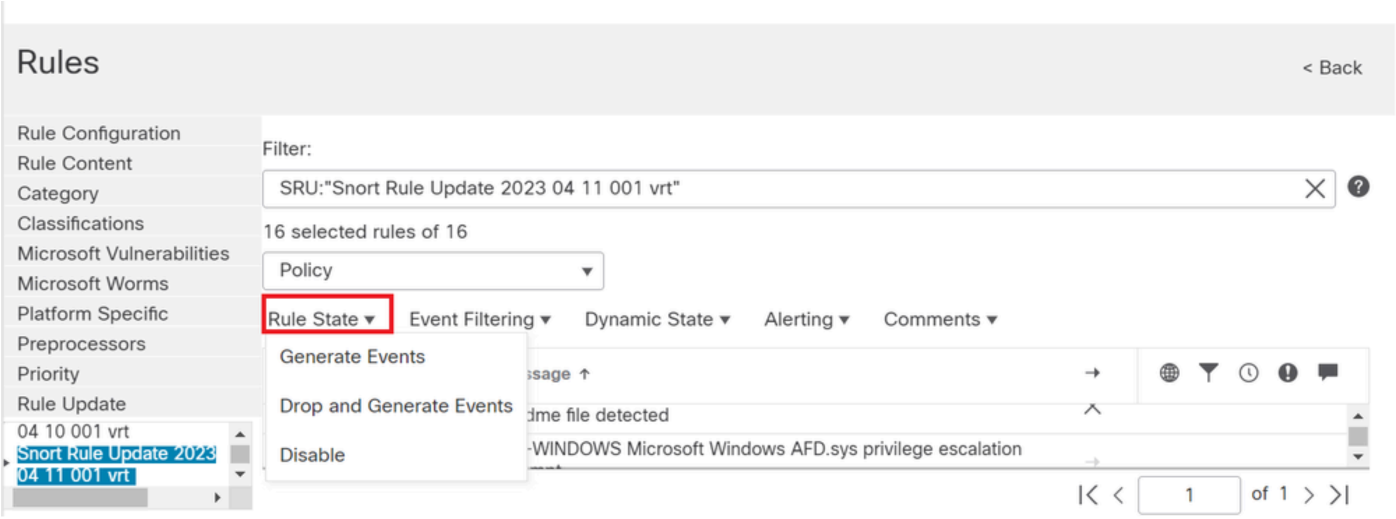
SRU:"Snort Rule Update 2023 04 11 001 vrt"

0 selected rules of 16

GID	SID	Message
1	01012	readme file detected
1	61615	OS-WINDOWS Microsoft Windows AFD.sys privilege escalation attempt

Available Sid's under snort rules

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



Rules

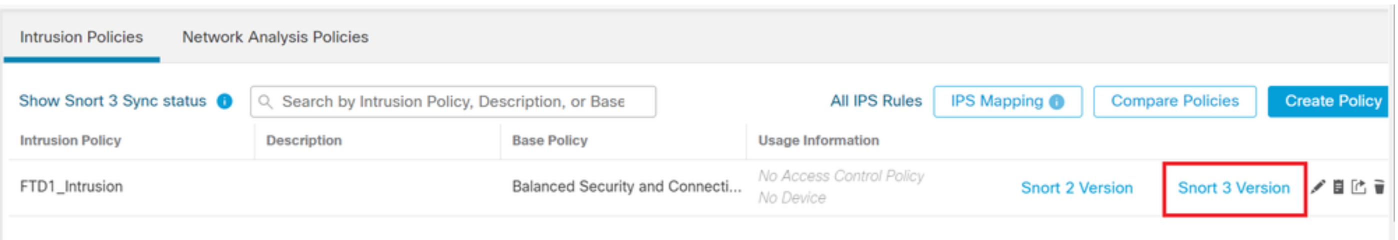
Filter: SRU:"Snort Rule Update 2023 04 11 001 vrt"

16 selected rules of 16

Policy

Selecting Rule states

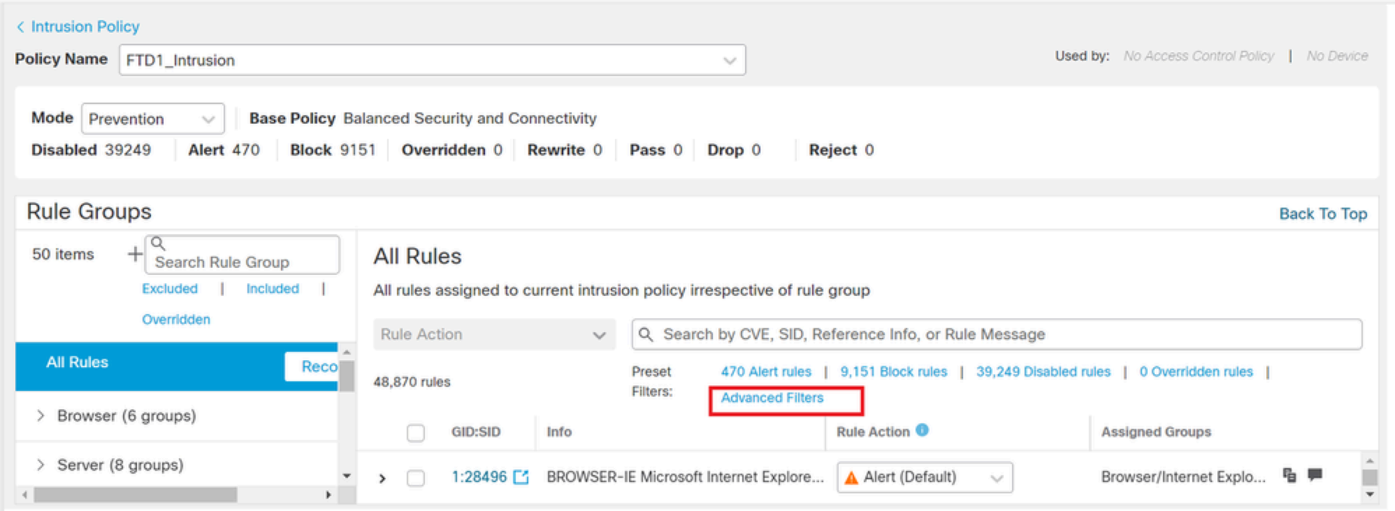
To view the Snort 3 rule SIDs, navigate to FMC Policies > Access Control > Intrusion , thereafter click the SNORT3 option in the top right corner, as shown in the image:



Intrusion Policy	Description	Base Policy	Usage Information
FTD1_Intrusion		Balanced Security and Connecti...	No Access Control Policy No Device

Snort 3

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



Policy Name FTD1_Intrusion

Used by: No Access Control Policy | No Device

Mode Prevention Base Policy Balanced Security and Connectivity

Disabled 39249 Alert 470 Block 9151 Overridden 0 Rewrite 0 Pass 0 Drop 0 Reject 0

All Rules

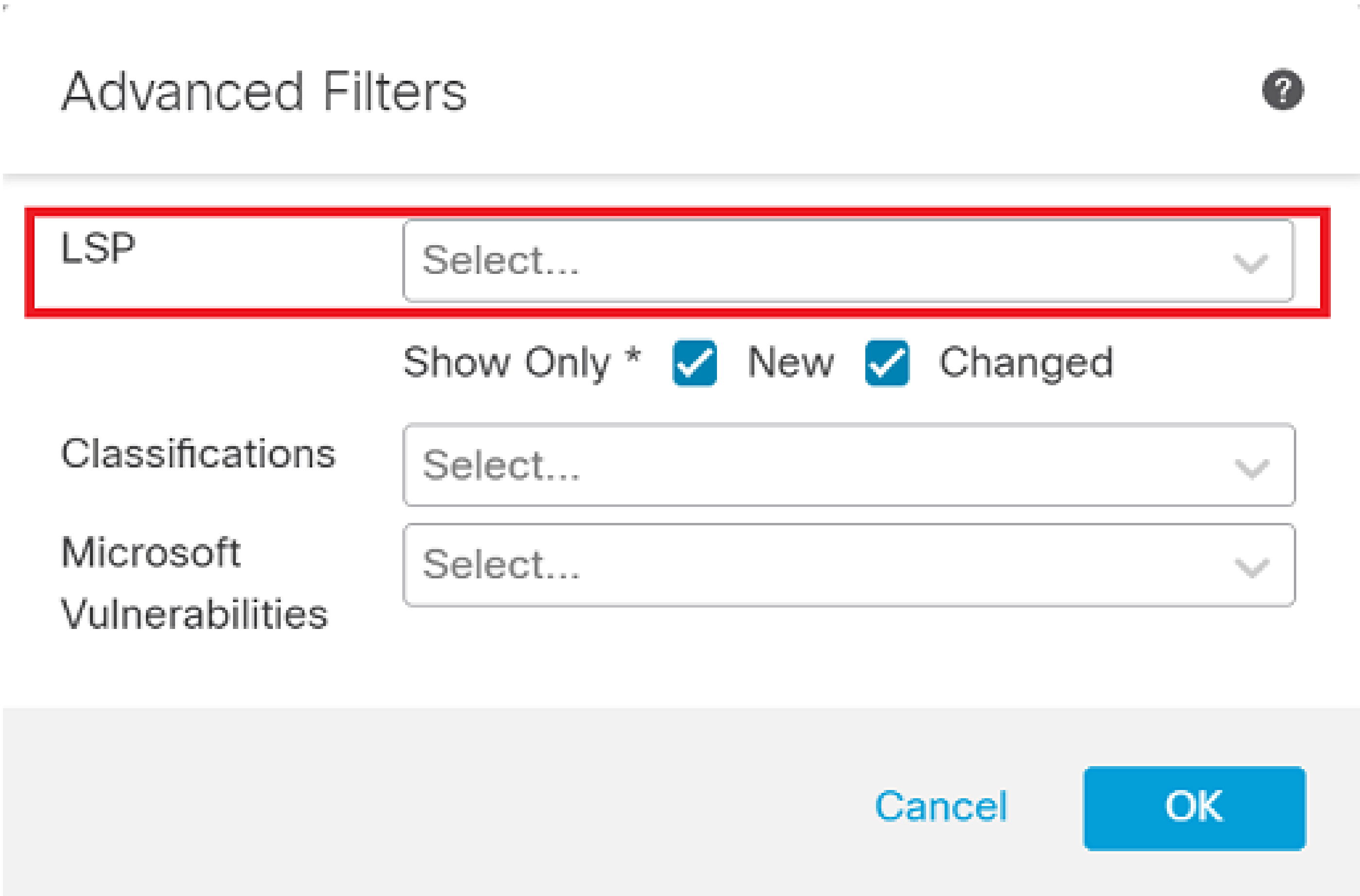
All rules assigned to current intrusion policy irrespective of rule group

48,870 rules

Preset Filters: 470 Alert rules | 9,151 Block rules | 39,249 Disabled rules | 0 Overridden rules | Advanced Filters

GID:SID	Info	Rule Action	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet Explore...	Alert (Default)	Browser/Internet Explo...

Snort 3 filters



Advanced Filters

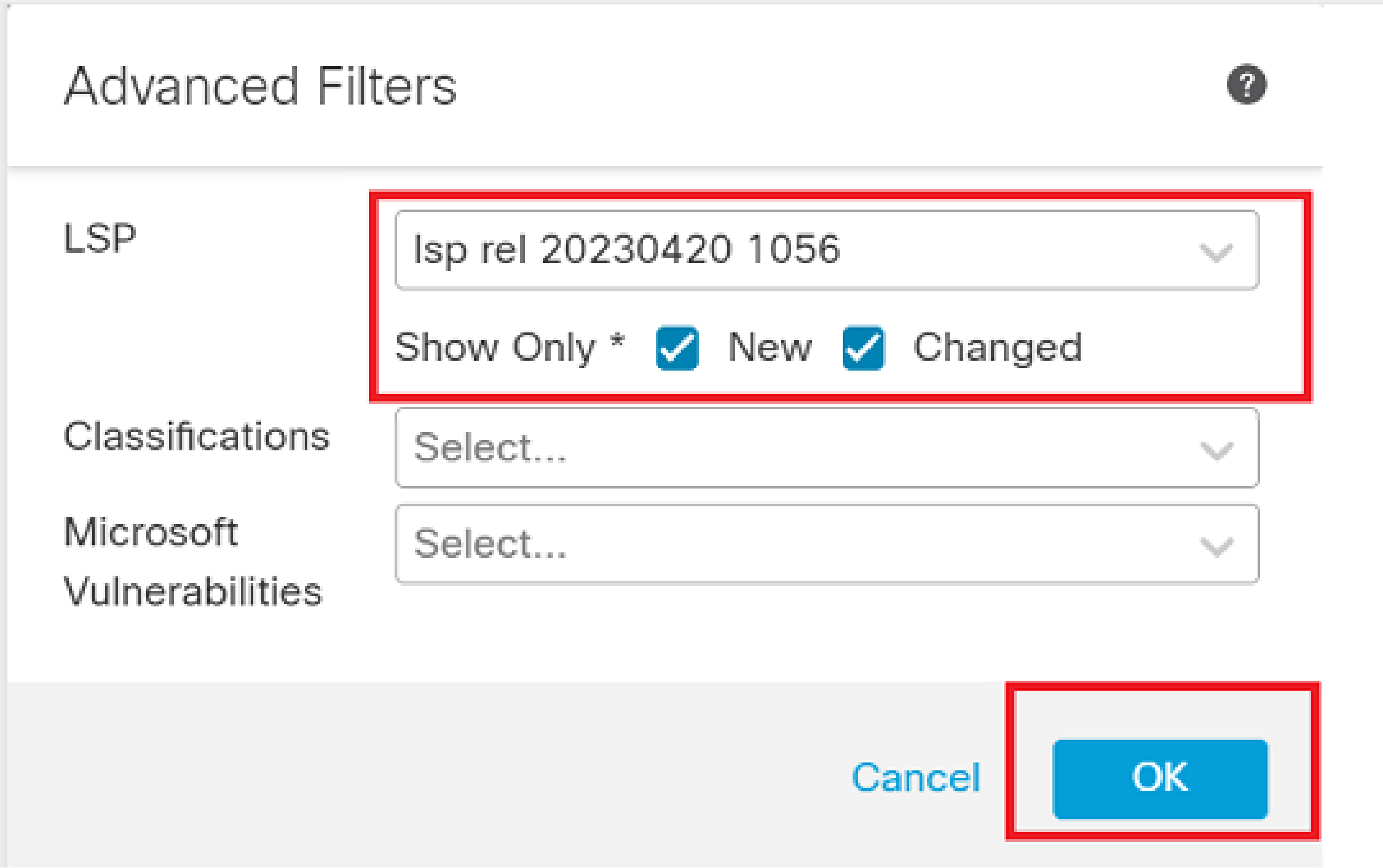
LSP: Select...

Show Only * ☑ New ☑ Changed

Classifications: Select...

Microsoft Vulnerabilities: Select...

LSP under advanced filter



Advanced Filters

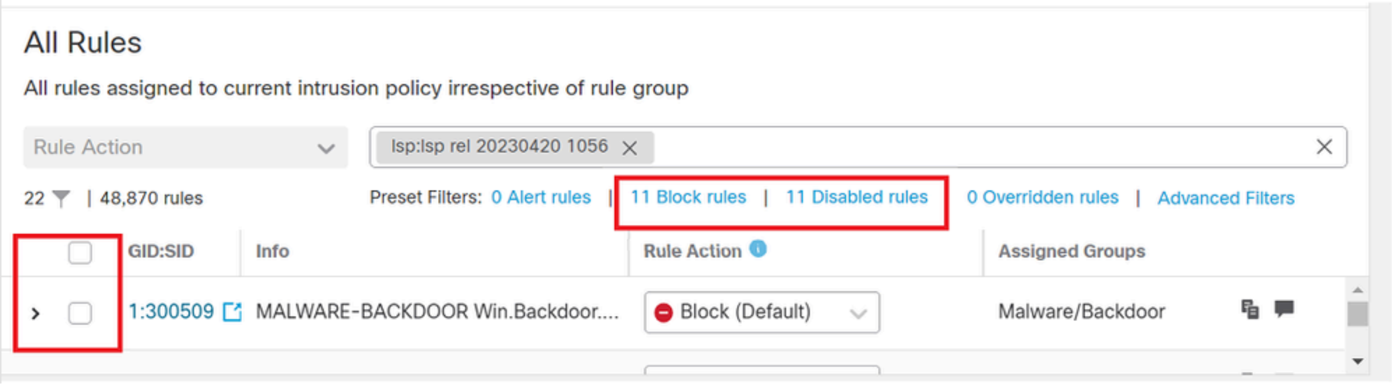
LSP: lsp rel 20230420 1056

Show Only * ☑ New ☑ Changed

Classifications: Select...

Microsoft Vulnerabilities: Select...

LSP version



All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action ⌄ | lsp:lsp rel 20230420 1056 ✕ | ✕

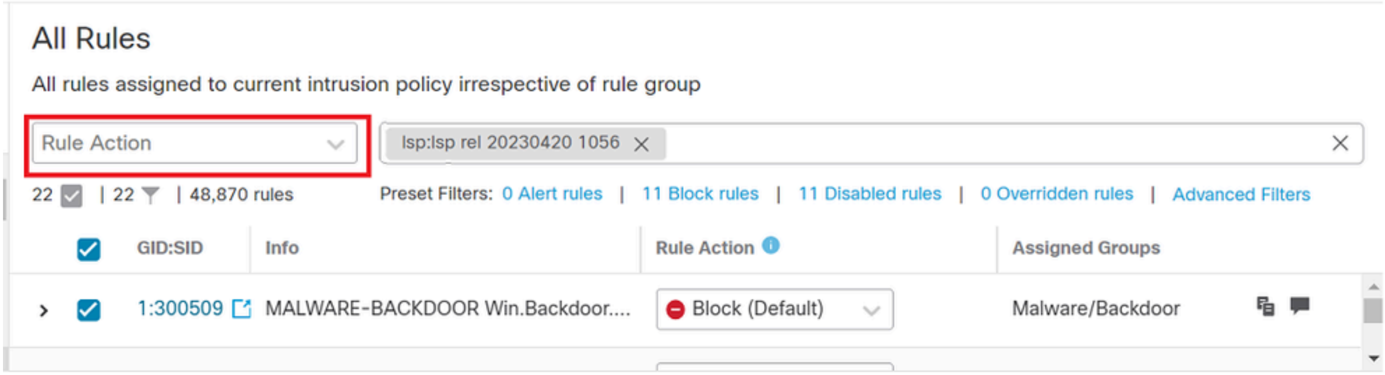
22 | 48,870 rules

Preset Filters: 0 Alert rules | 11 Block rules | 11 Disabled rules | 0 Overridden rules | Advanced Filters

	□	GID:SID	Info	Rule Action	Assigned Groups
›	□	1:300509	MALWARE-BACKDOOR Win.Backdoor....	Block (Default)	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 ⌄ | lsp:lsp rel 20230420 1056 ✕ | ✕

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

Rule action