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

目录

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”。

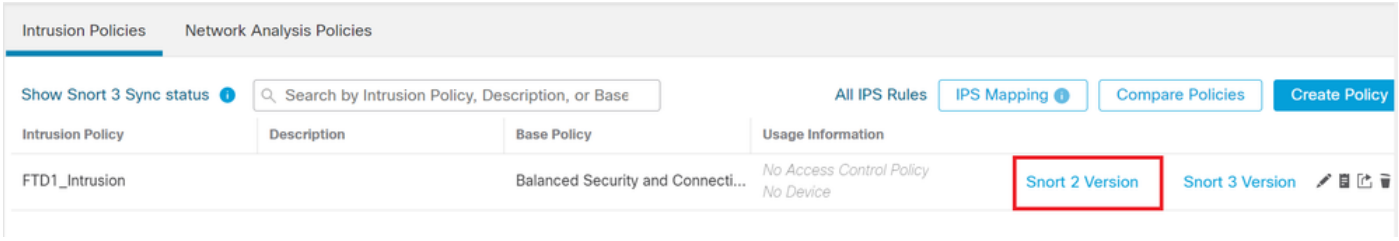
Snort签名ID(SID)是分配给规则集内每个规则或签名的唯一标识符。这些规则用于检测网络流量中

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SNORT网站。

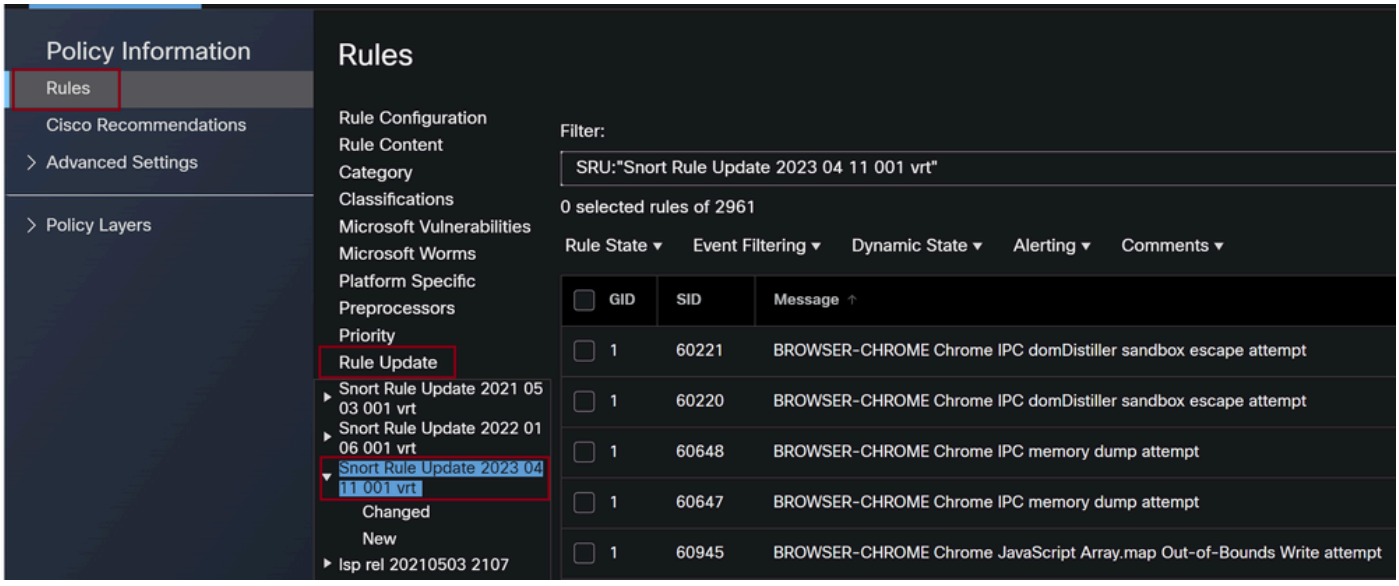
过滤Snort规则的过程

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：

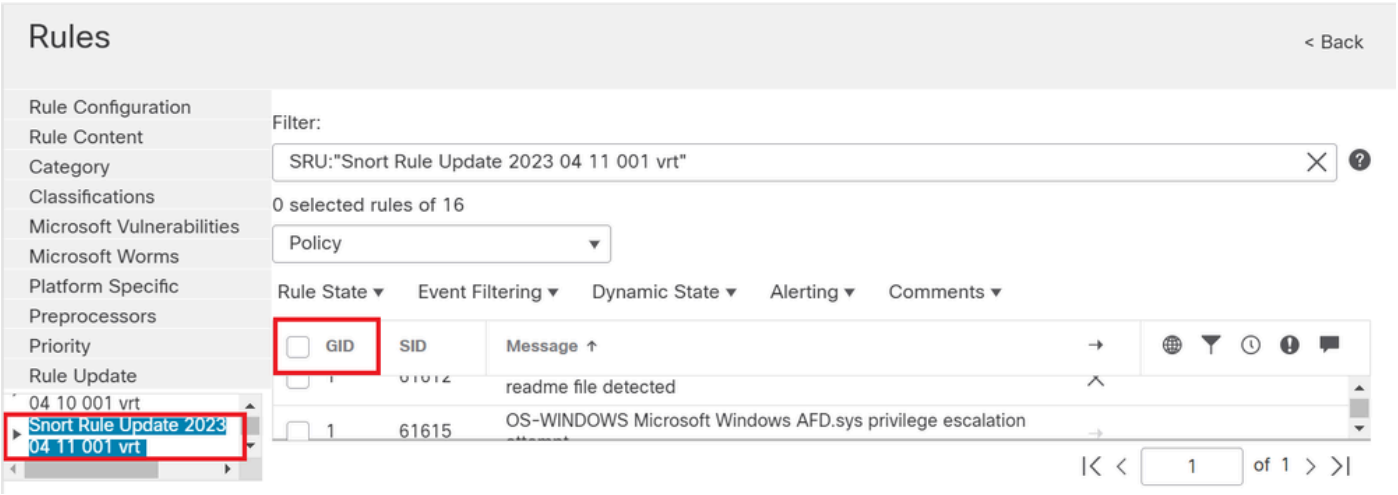


Snort 2

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

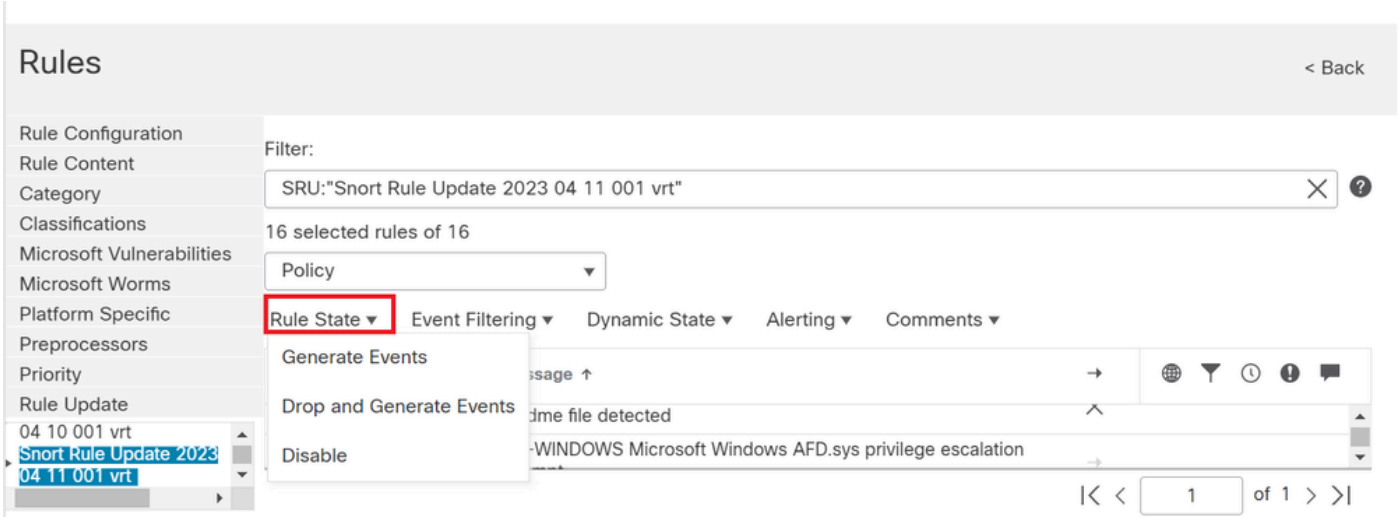


规则更新



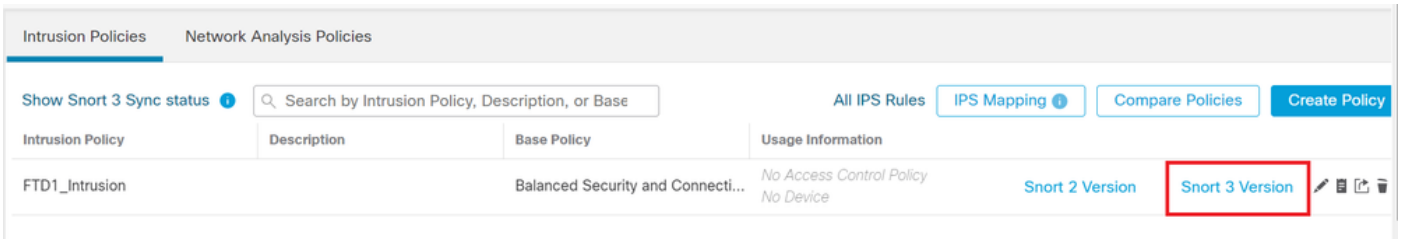
可用SID在Snort规则下

在下面选择所需的选项 Rule State 如图所示.



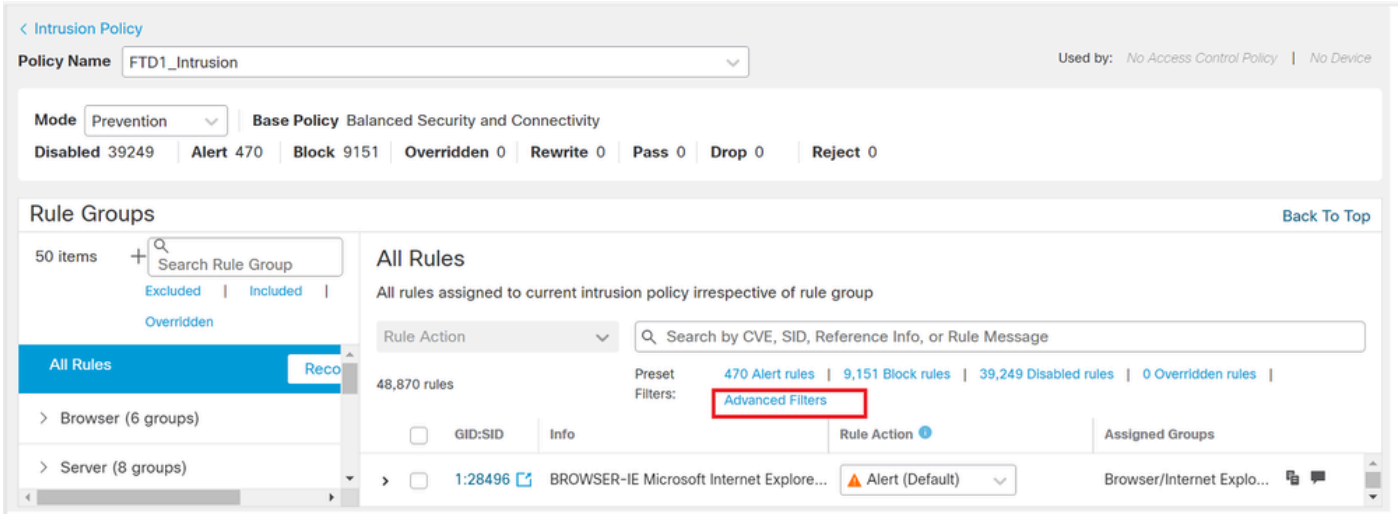
选择规则状态

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：

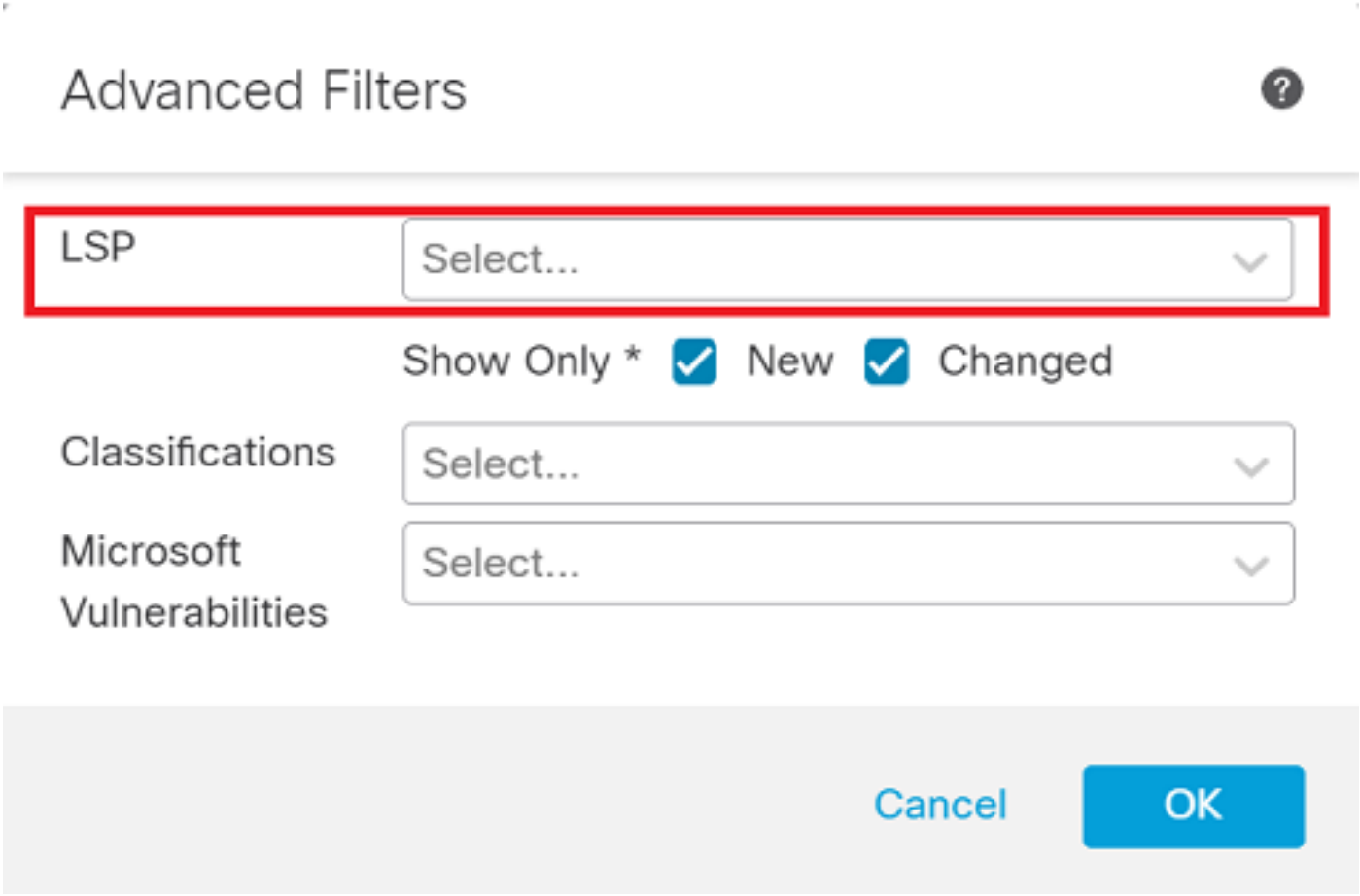


Snort 3

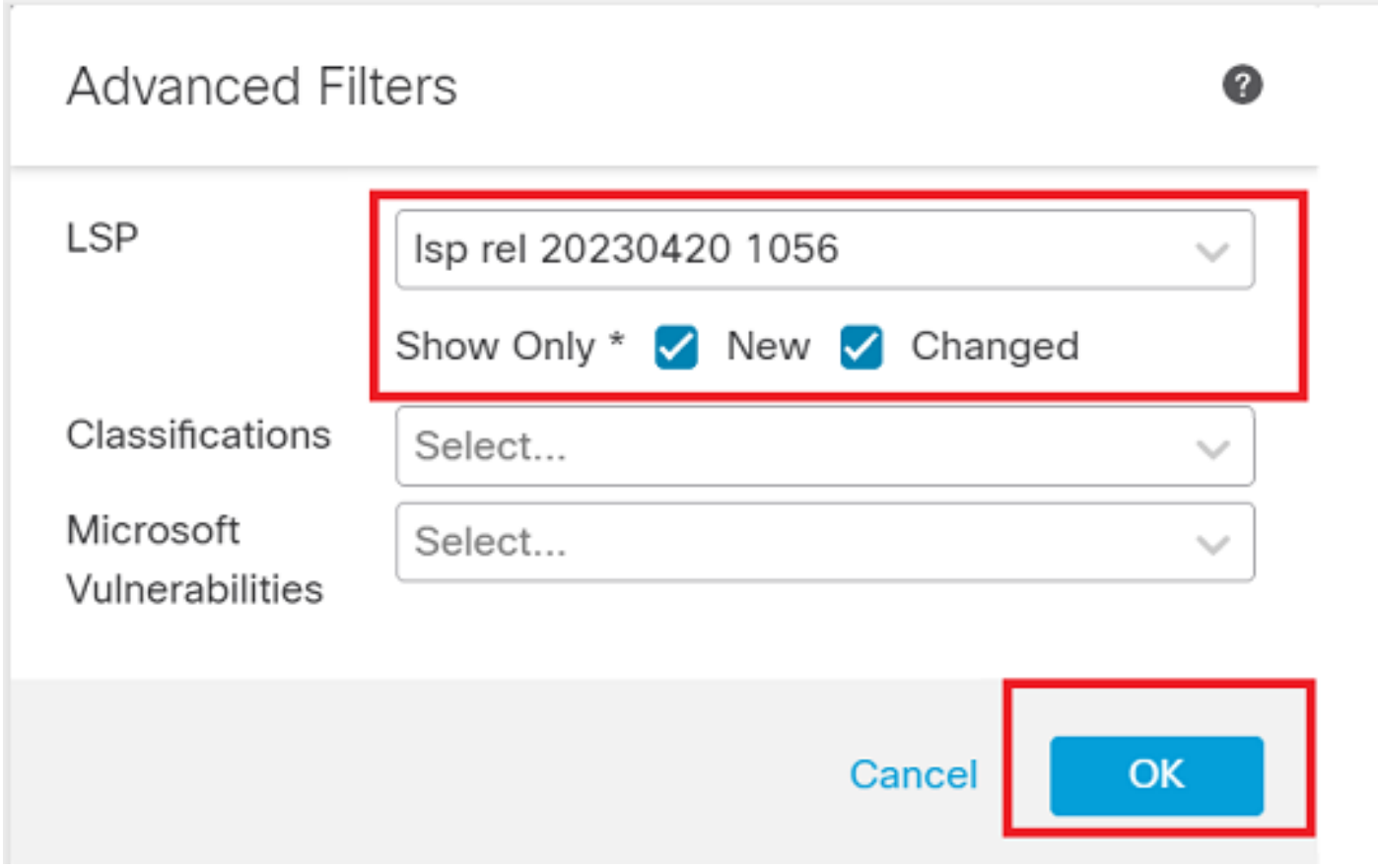
导航至 Advanced Filters 并选择最新日期以过滤SID，如图所示。



Snort 3过滤器


Advanced Filters
LSP
Select...
Show Only *
New
Changed
Classifications
Select...
Microsoft Vulnerabilities
Select...
Cancel
OK

高级过滤器下的LSP


Advanced Filters
LSP
lsp rel 20230420 1056
Show Only *
New
Changed
Classifications
Select...
Microsoft Vulnerabilities
Select...
Cancel
OK

LSP版本

Sid的预设置过滤器

在下面选择所需的选项 Rule state 如图所示.

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）。