根據FMC管理的Firepower裝置的SRU和LSP版本篩選Snort規則

目錄

簡介

本檔案介紹如何根據Firepower管理中心(FMC)管理的firepower裝置的思科安全規則更新(SRU)和鏈路狀態資料包(LSP)版本過濾snort規則。

必要條件

需求

思科建議您瞭解以下主題：

- 開源Snort知識
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 本文適用於所有Firepower平台
- 執行7.0.0版軟體的Cisco Firepower威脅防禦(FTD)
- Firepower管理中心虛擬(FMC)，運行軟體版本7.0.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

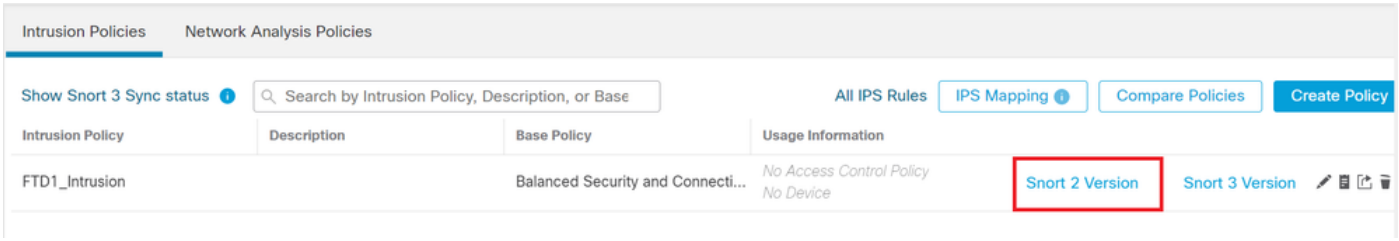
在入侵檢測系統(IDS)和入侵防禦系統(IPS)環境中，「SID」表示「特徵碼ID」或「Snort特徵碼ID」。

Snort特徵碼ID(SID)是分配給規則集內每個規則或特徵碼的唯一識別符號。這些規則用於檢測網路流量中可能表示惡意活動或安全威脅的特定模式或行為。每個規則都與SID關聯，以便易於參考和管理。

有關開源Snort的資訊，請訪問SNORT網站。

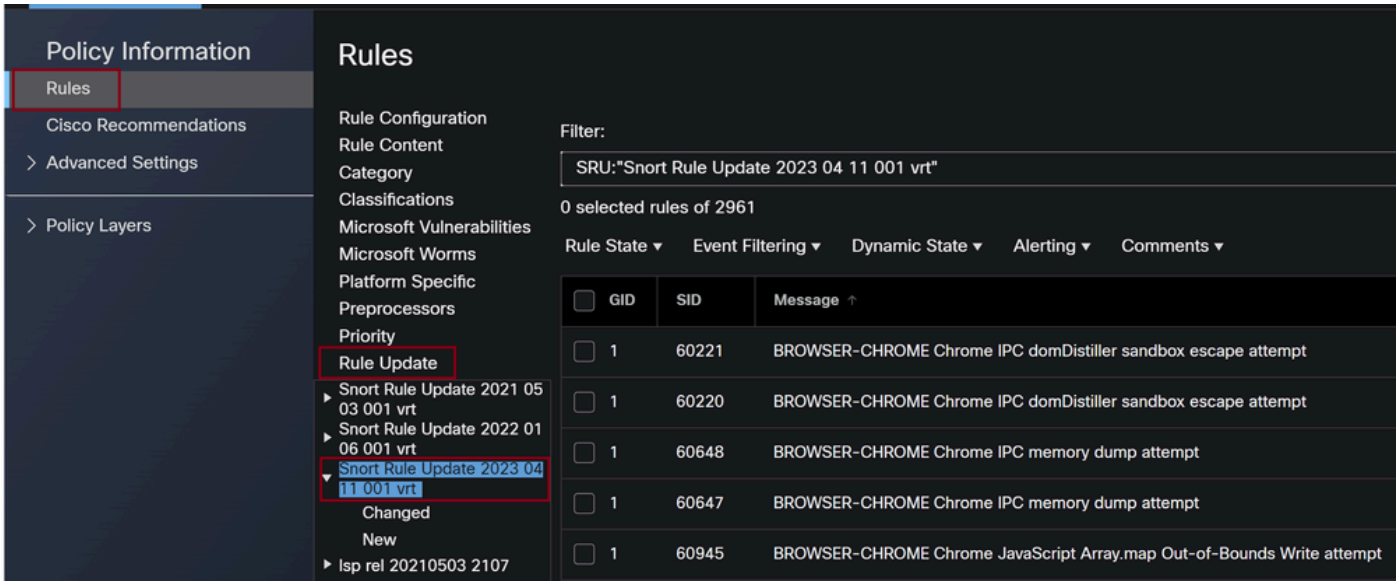
過濾Snort規則的過程

要檢視Snort 2規則SID，請導航至 FMC Policies > Access Control > Intrusion, 然後點選右上角的SNORT2選項，如下圖所示：

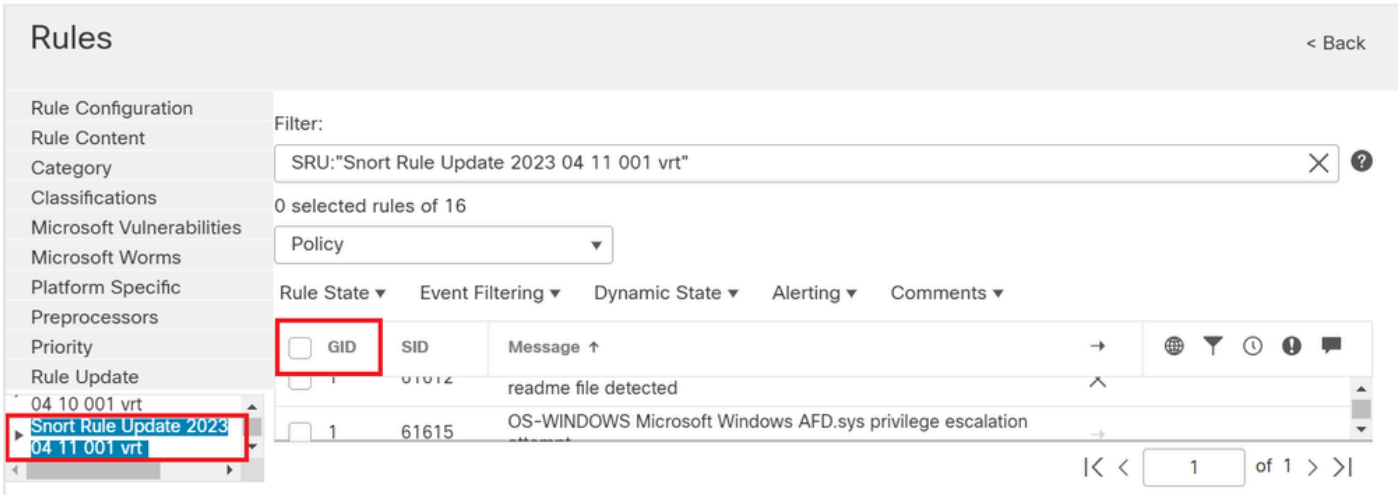


Snort 2

導航至 Rules > Rule Update 並選擇最新日期以篩選SID。

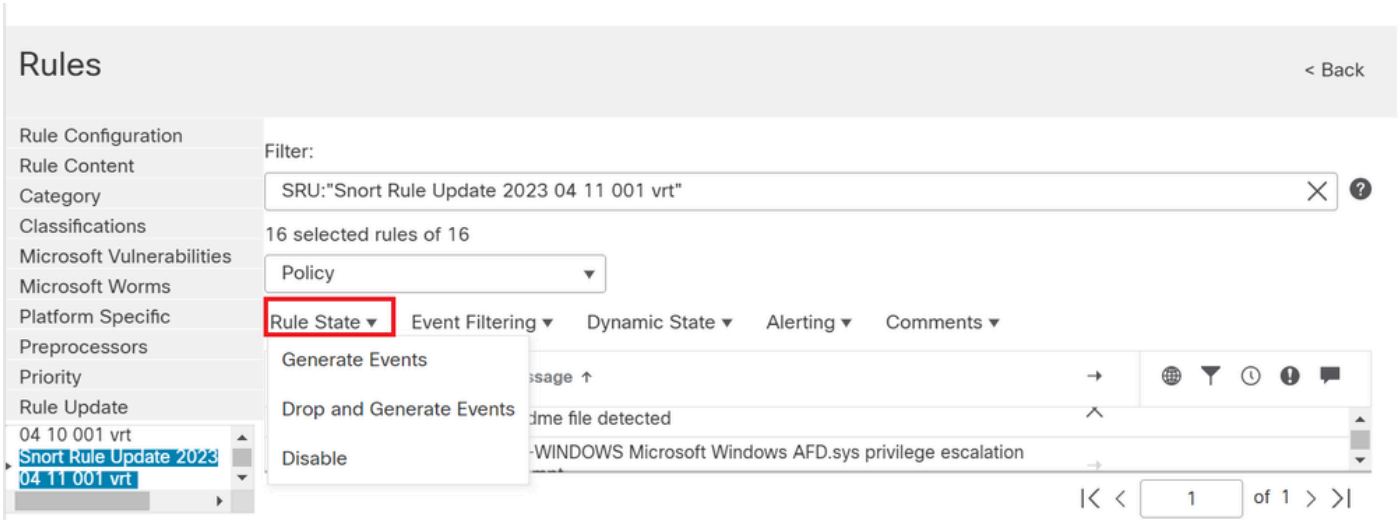


規則更新



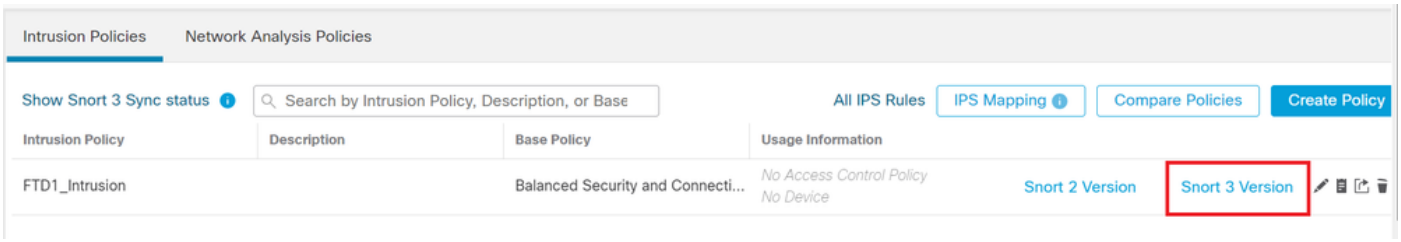
可用Sid在snort規則下

選擇下面的必需選項 Rule State 如下圖所示。



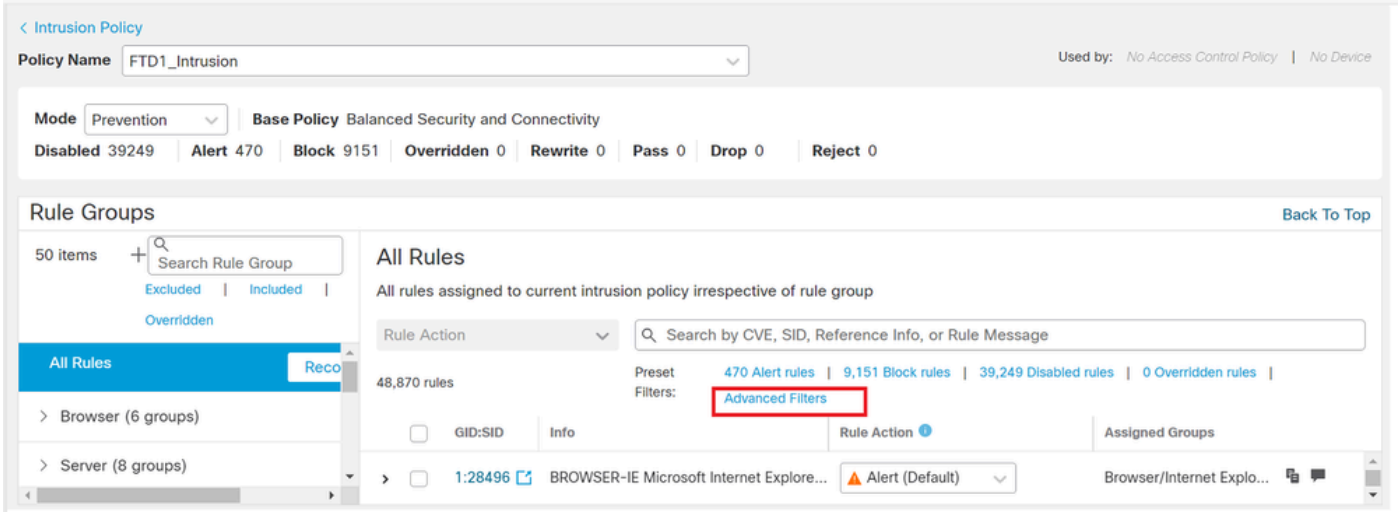
選擇規則狀態

要檢視Snort 3規則SID，請導航至 FMC Policies > Access Control > Intrusion ，然後點選右上角的SNORT3選項，如下圖所示：

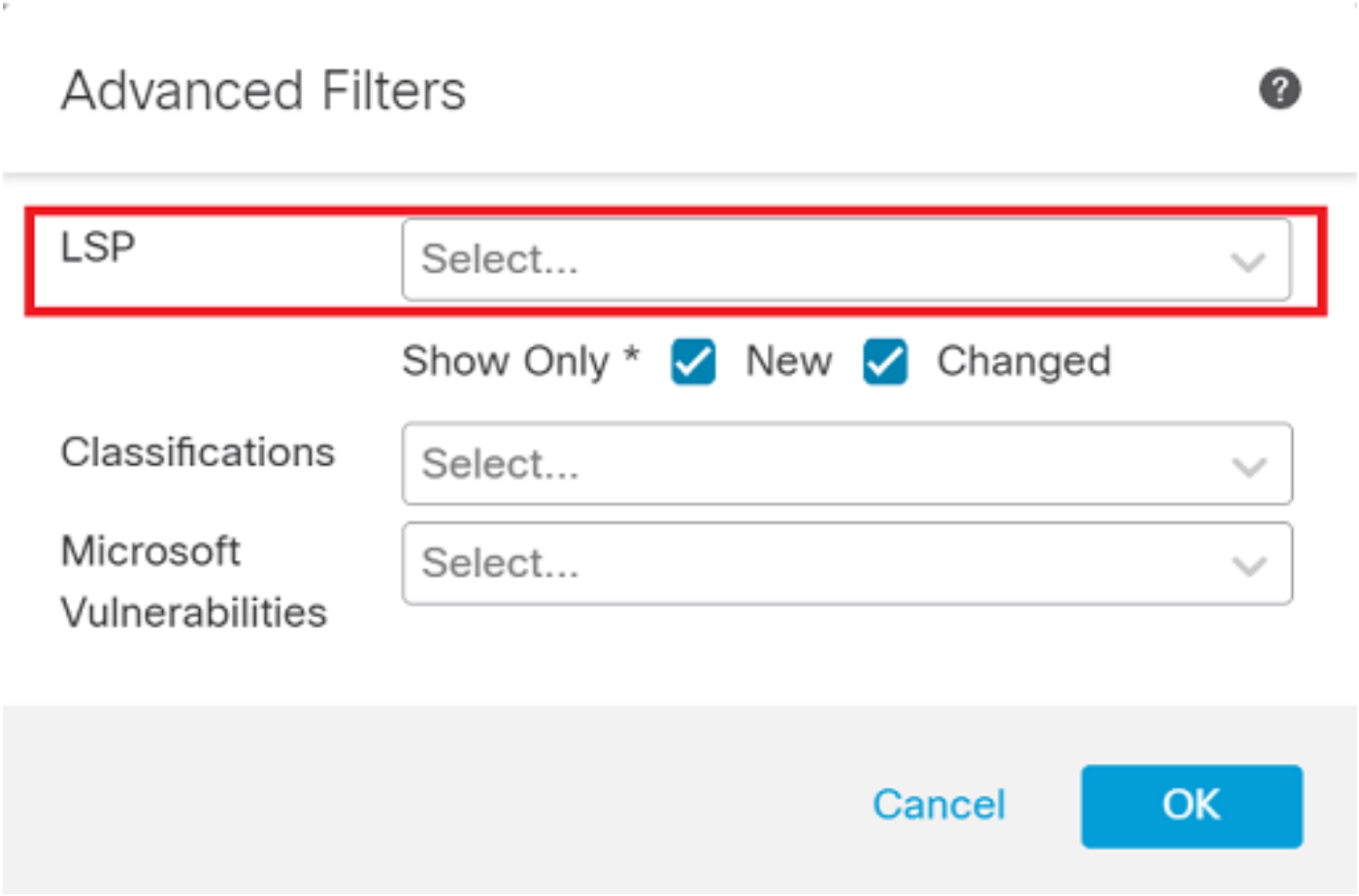


Snort 3

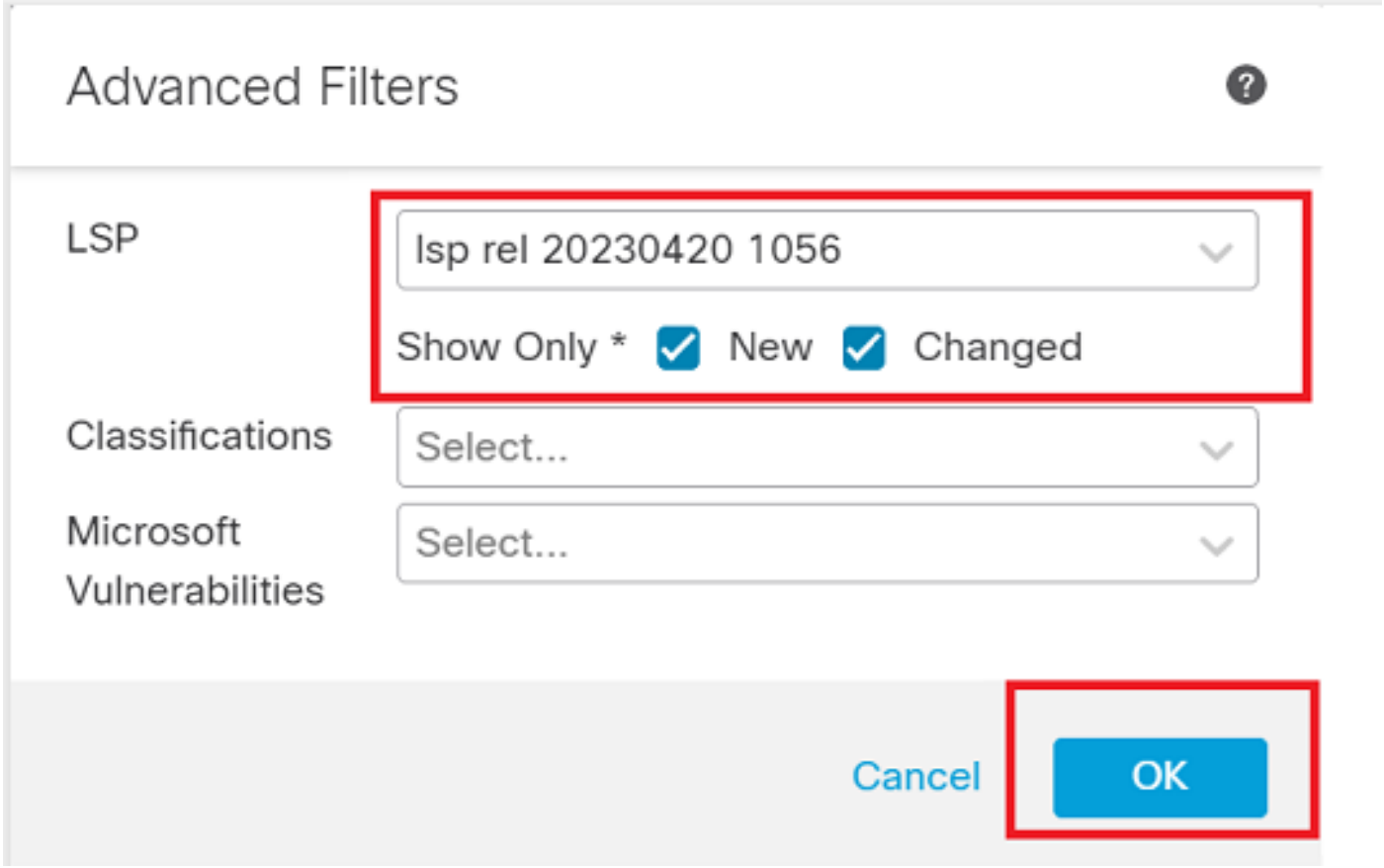
導航至 Advanced Filters 並選擇最新日期以過濾SID，如下圖所示。



Snort 3過濾器



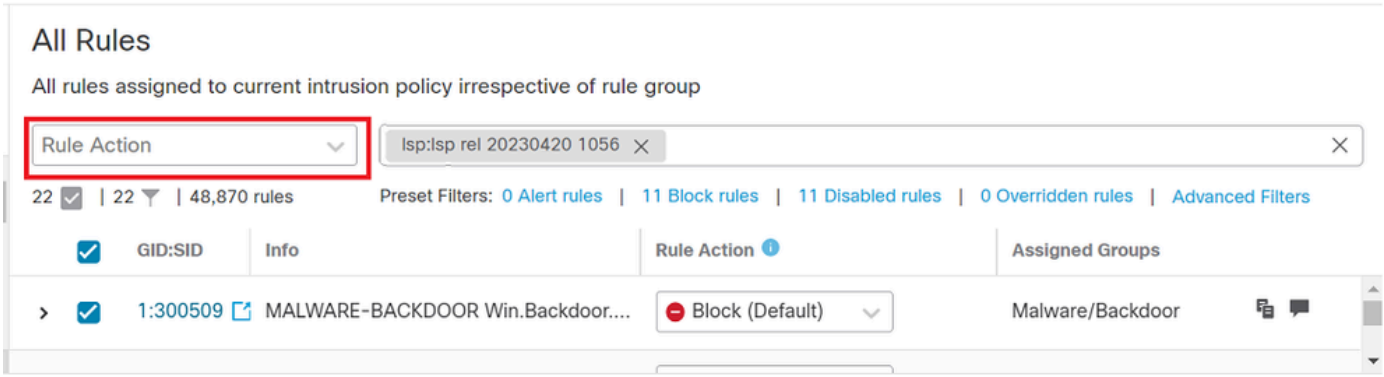
高級過濾器下的LSP



LSP版本

Sid的預設定篩選器

選擇下面的必需選項 Rule state 如下圖所示。



規則操作

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。