FMCによって管理されるFirepowerデバイスのSRUおよびLSPバージョンに基づくSnortルールのフィルタリング

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

[Snortルールをフィルタリングする手順](#)

はじめに

このドキュメントでは、Firepower Management Center(FMC)で管理されるfirepowerデバイスのCisco Secure Rule Update(SRU)およびLink State Packet(LSP)バージョンに基づいてSnortルールをフィルタリングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- オープンソースのSnortに関する知識
- Firepower Management Center（FMC）
- Firepower Threat Defense（FTD）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- この記事は、すべてのFirepowerプラットフォームに適用されます
- ソフトウェアバージョン7.0.0が稼働するシスコFirepower脅威対策(FTD)
- ソフトウェアバージョン7.0.0が稼働するFirepower Management Center Virtual(FMC)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

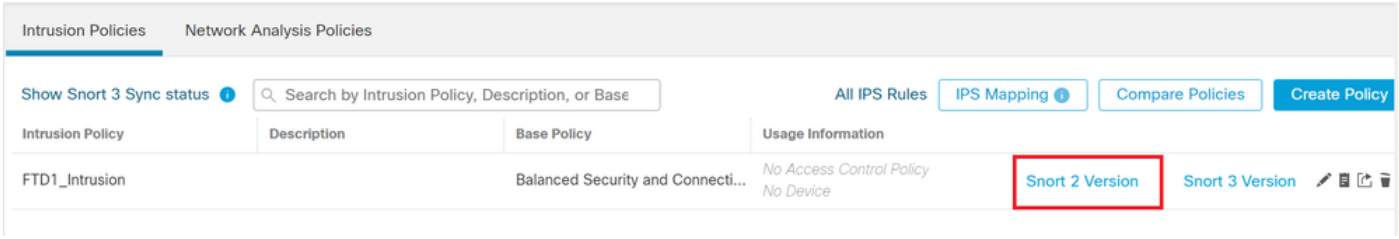
侵入検知システム(IDS)と侵入防御システム(IPS)のコンテキストでは、「SID」は「Signature ID」または「Snort Signature ID」を意味します。

Snortシグニチャ ID(SID)は、そのルールセット内の各ルールまたはシグニチャに割り当てられる一意のIDです。これらのルールは、悪意のあるアクティビティやセキュリティの脅威を示す可能性があるネットワークトラフィックの特定のパターンや動作を検出するために使用されます。各ルールはSIDに関連付けられ、参照と管理が容易になります。

オープンソースのSnortについては、SNORTのWebサイトを参照してください。

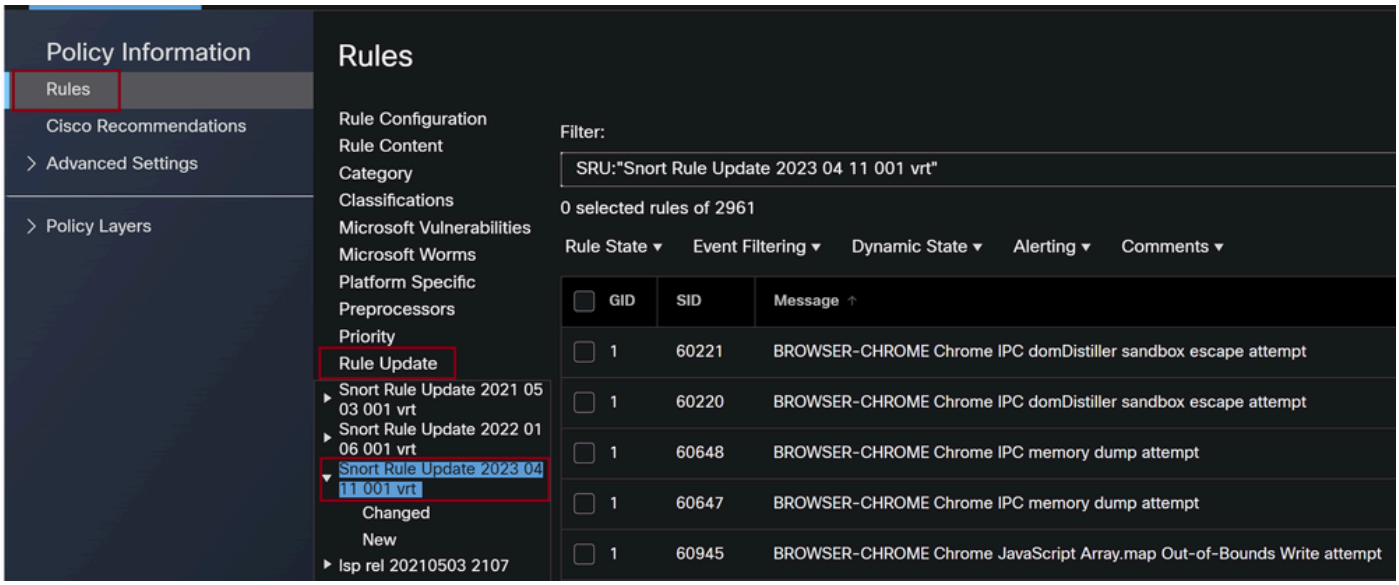
Snortルールをフィルタリングする手順

Snort 2ルールのSIDを表示するには、 FMC Policies > Access Control > Intrusion, 次の図に示すように、右上隅のSNORT2オプションをクリックします。

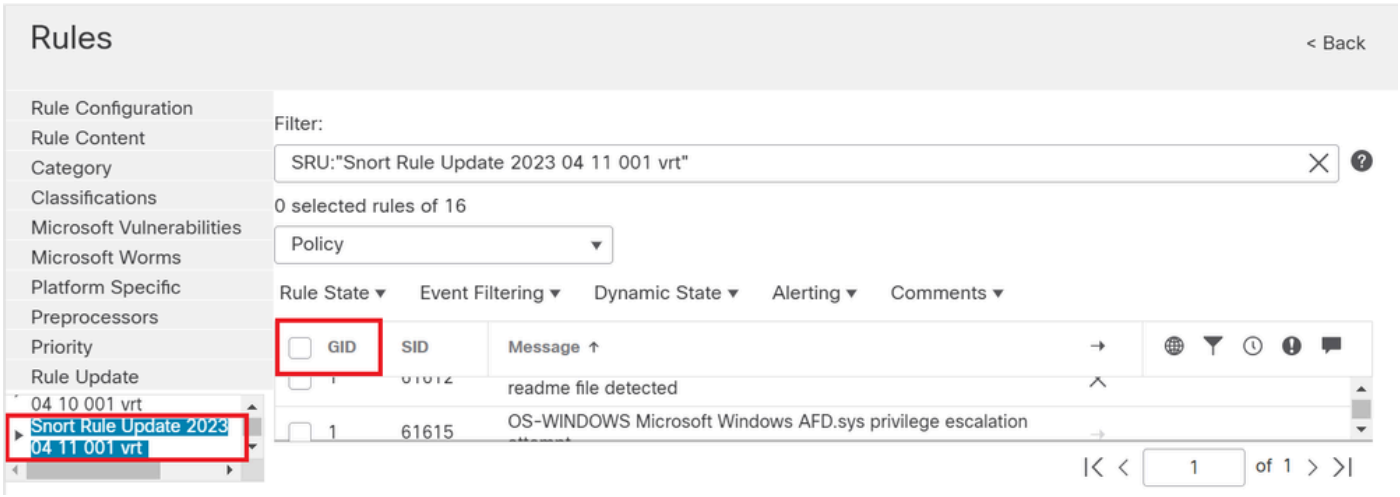


Snort 2

移動先 Rules > Rule Update SIDをフィルタリングする最新の日付を選択します。

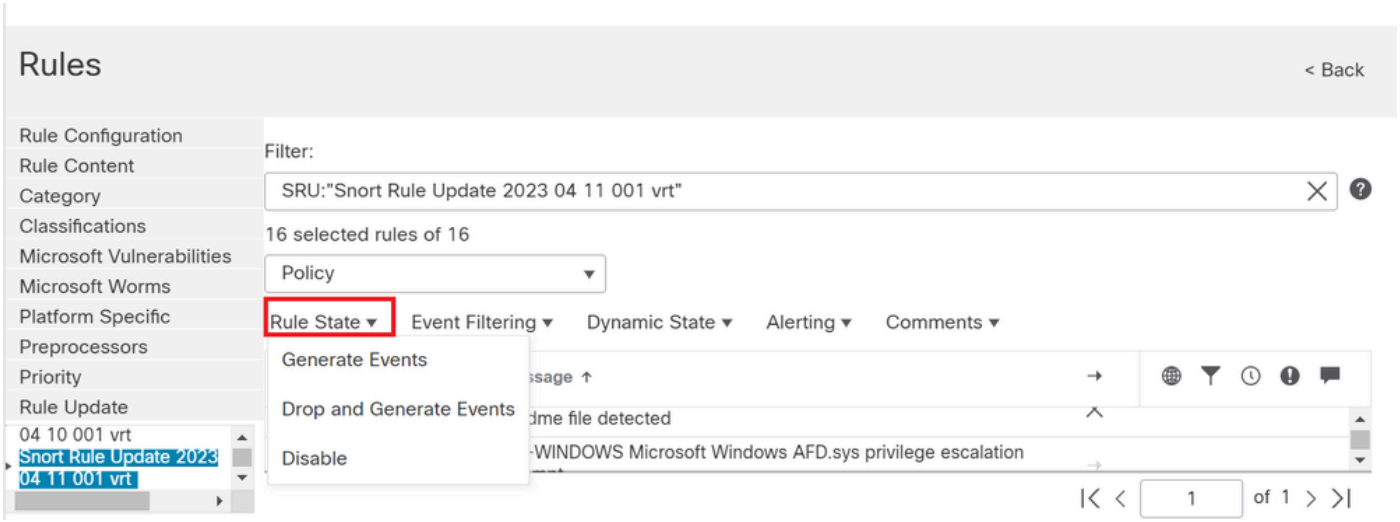


ルールの更新



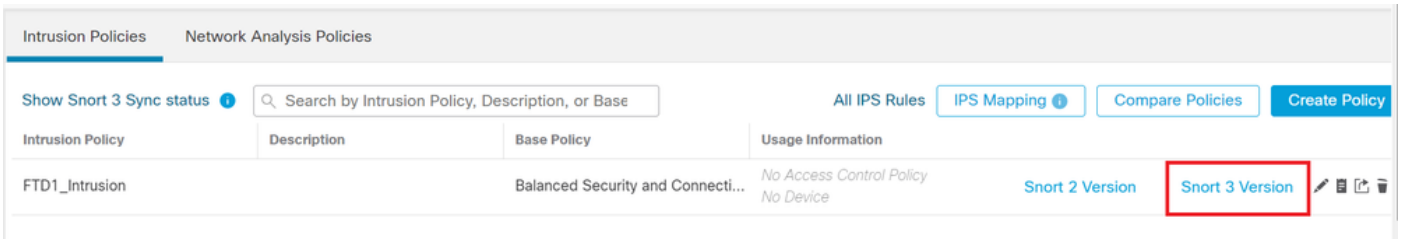
Snortルールで使用可能なSID

以下のオプションから必要なものを選択します。 Rule State 図に示すように。



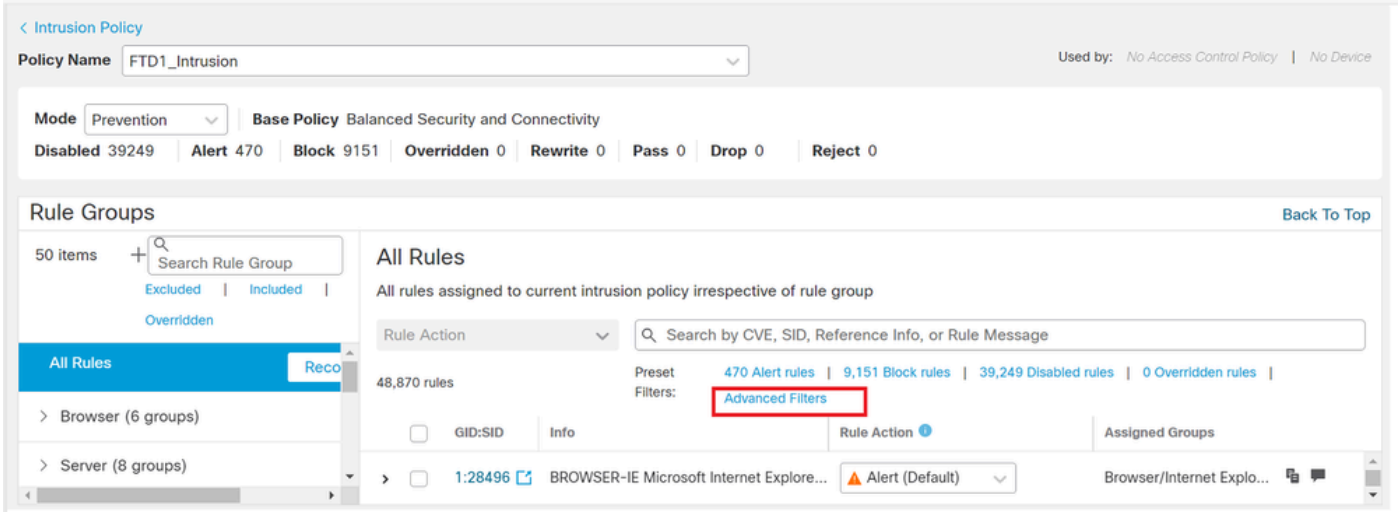
ルールの状態の選択

Snort 3ルールのSIDを表示するには、 FMC Policies > Access Control > Intrusion 次の図に示すように、右上隅のSNORT3オプションをクリックします。

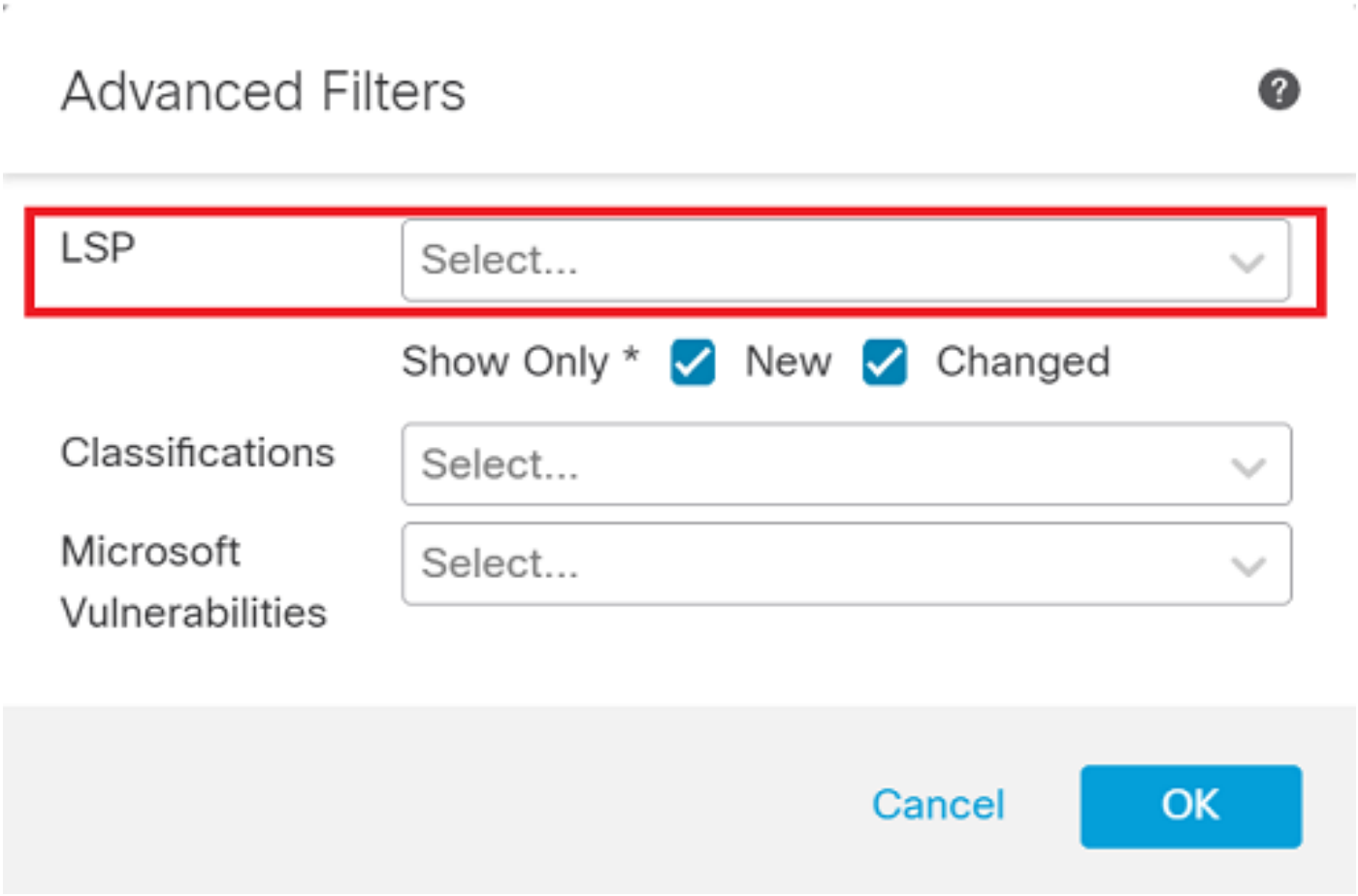


Snort 3

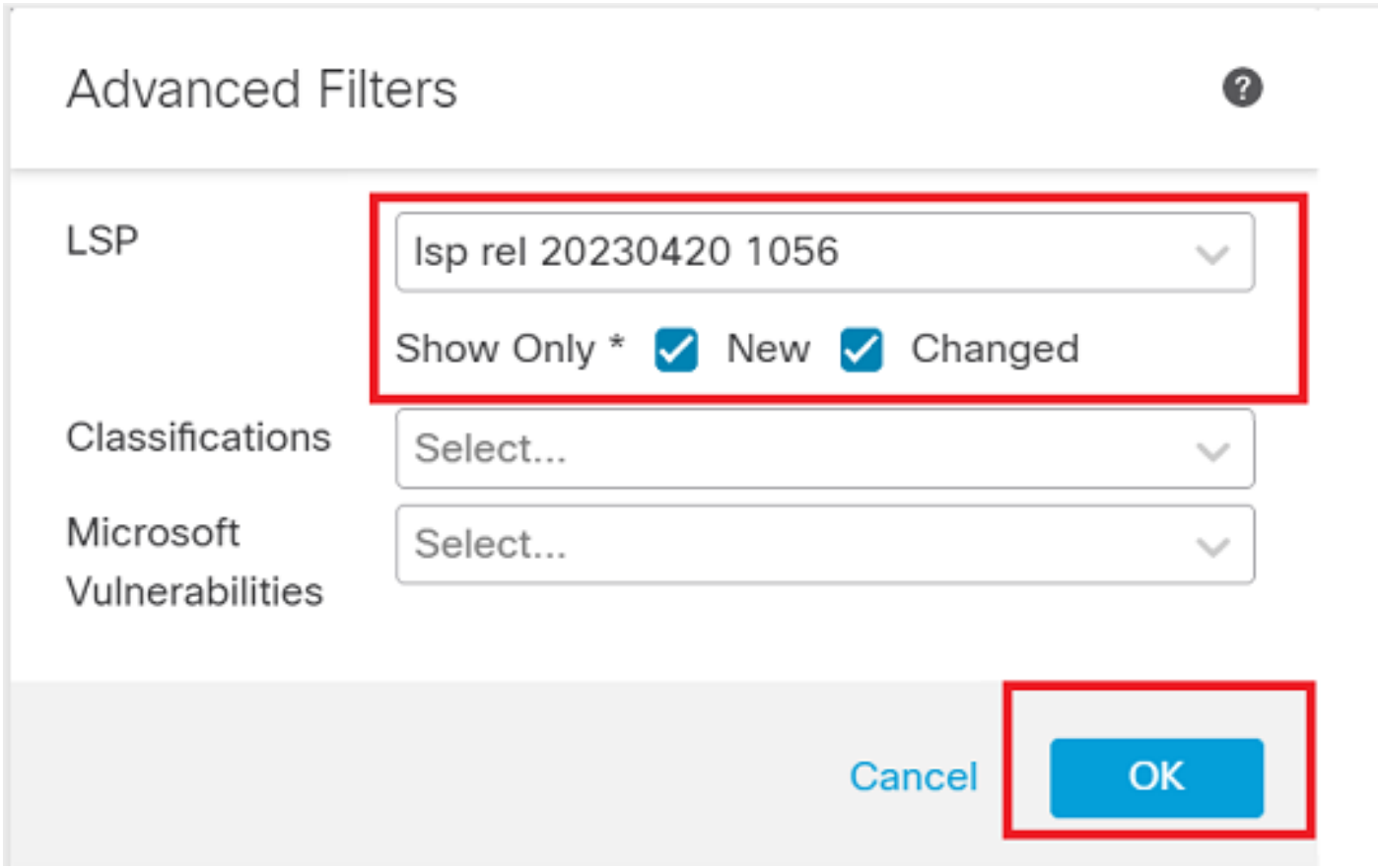
移動先 Advanced Filters をクリックし、図に示すようにSIDをフィルタリングする最新の日付を選択します。



Snort 3フィルタ



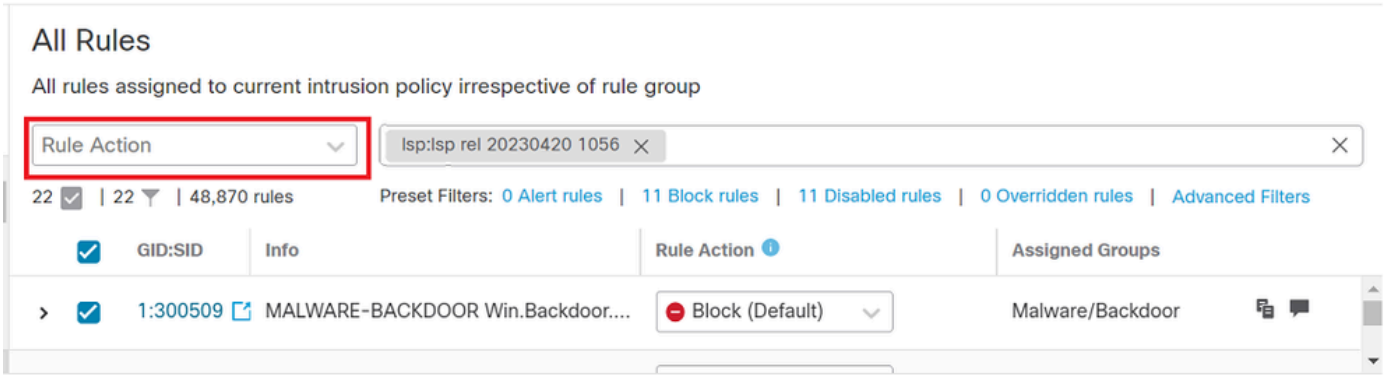
高度なフィルタの下のLSP



LSPバージョン

Sidの事前設定フィルタ

以下のオプションから必要なものを選択します。 Rule state 図に示すように。



ルールアクション

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。