FMCでの追加のSnort 3ルールアクションの設定

内容

はじめに

このドキュメントでは、7.1リリースで追加されたSnort 3ルールアクション機能に対するFirepower Management Center(FMC)のサポートについて説明します。

背景説明

Firepower Threat Defense(FTD)では、7.0で7つの侵入ポリシールールアクション(Alert/Disable/Block/Reject/Rewrite/Pass/Drop)がサポートされていますが、FMCでサポートされているのはSnort 3の3つのルールアクション(「Alert」、「Disable」、「Block」)だけです。

Firepower 7.1.0以降、FMCは新しいルールアクションの設定をサポートしています。

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Snortに関する知識
- Firepower Management Center(FMC)7.1.0以降
- Firepower Threat Defense(FTD)7.0.0+

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。
- このドキュメントは、Snort 3を実行するすべての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7.4.2を実行するCisco Firepower Threat Defense Virtual(FTD)
- ソフトウェアバージョン7.4.2を実行する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。

機能の詳細

追加された新しいSnort 3ルールアクションとその説明は次のとおりです。

Pass:イベントは生成されず、後続のSnortルールによる評価なしでパケットを通過させることができます。

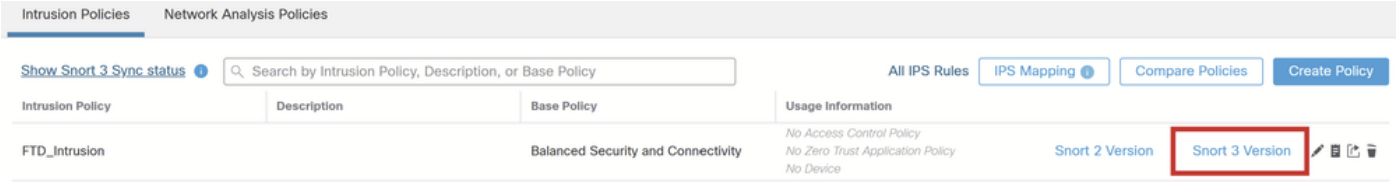
ドロップ：イベントを生成し、一致するパケットをドロップします。この接続ではこれ以上トラフィックをブロックしません。

Reject（拒否）：イベントを生成し、一致するパケットをドロップし、この接続でそれ以降のトラフィックをブロックして、TCP resetまたはICMP port unreachableを送信元ホストと宛先ホストに送信します。

Rewrite:ルールのreplaceオプションに基づいて、イベントを生成してパケットの内容を上書きします。

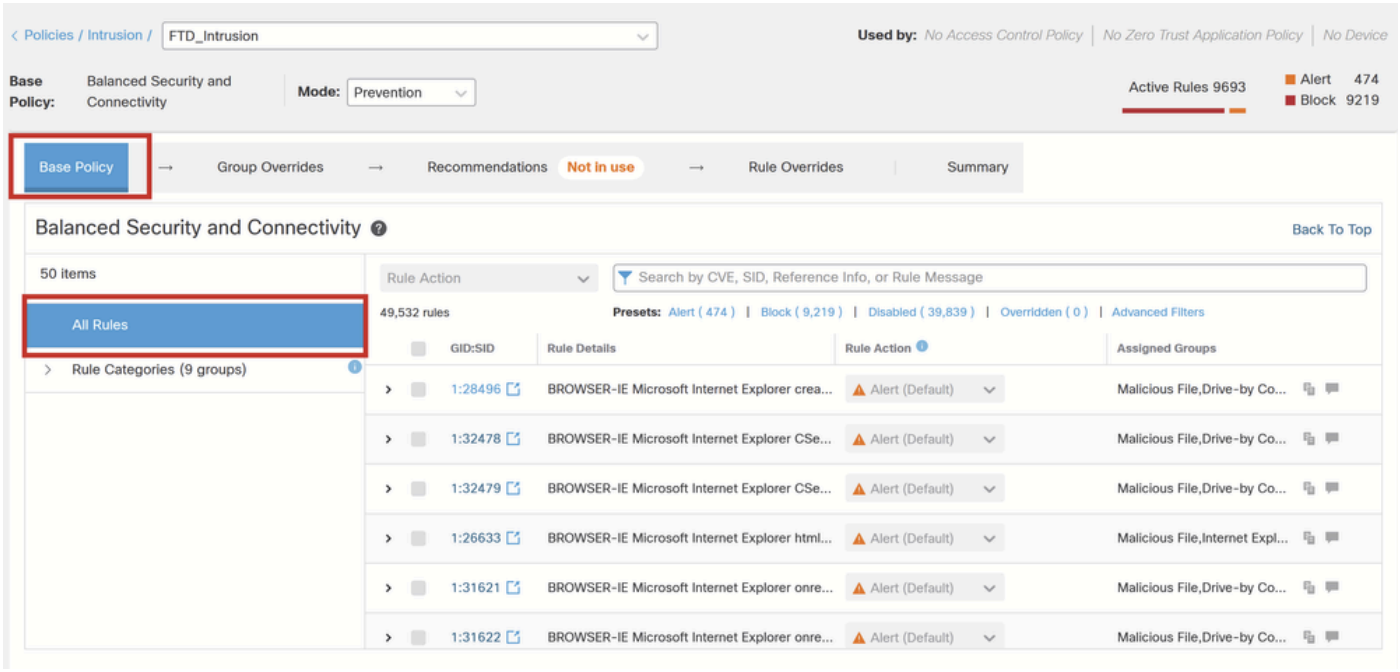
FMCウォークスルー

侵入ポリシーのSnort 3ルールを表示するには、FMC Policies > Access Control > Intrusion,その後に移動し、図に示すように、ポリシーの右上隅にあるSnort 3バージョンオプションをクリックします。



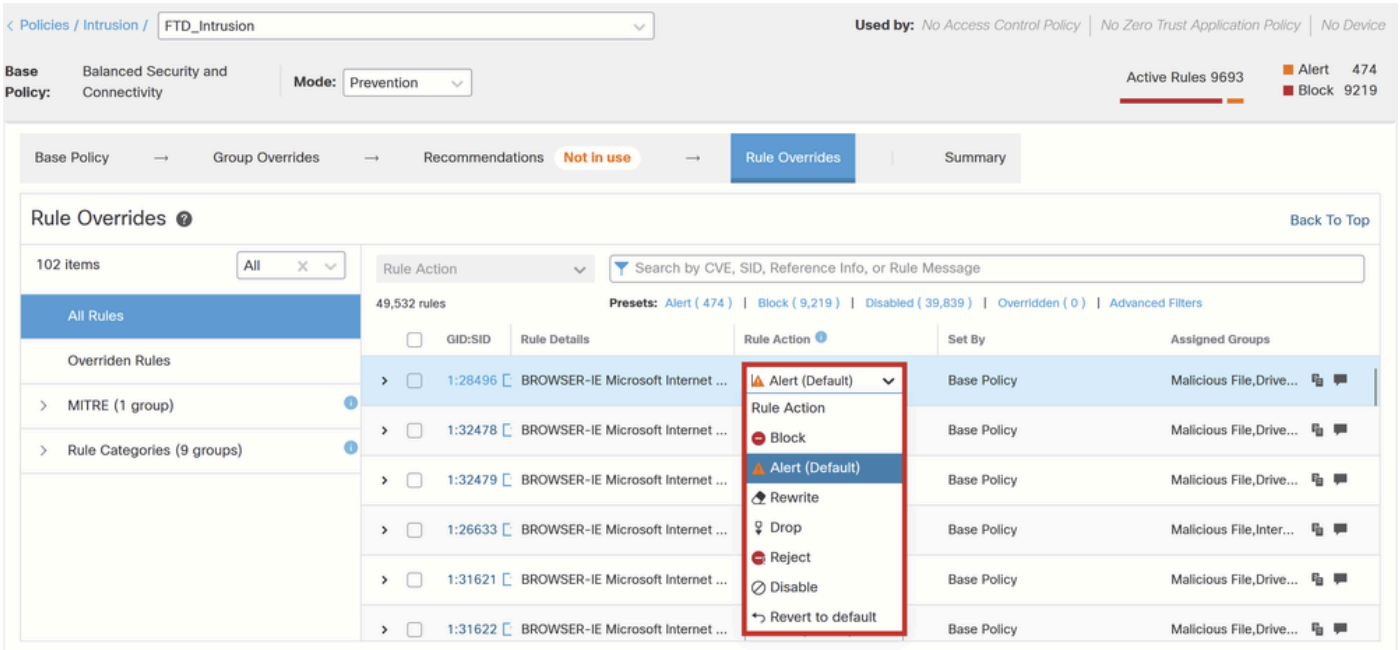
Snort 3のバージョン

Base Policy > All Rulesの順にクリックすると、システム定義のすべてのSnort 3ルールのデフォルトアクションを確認できます。

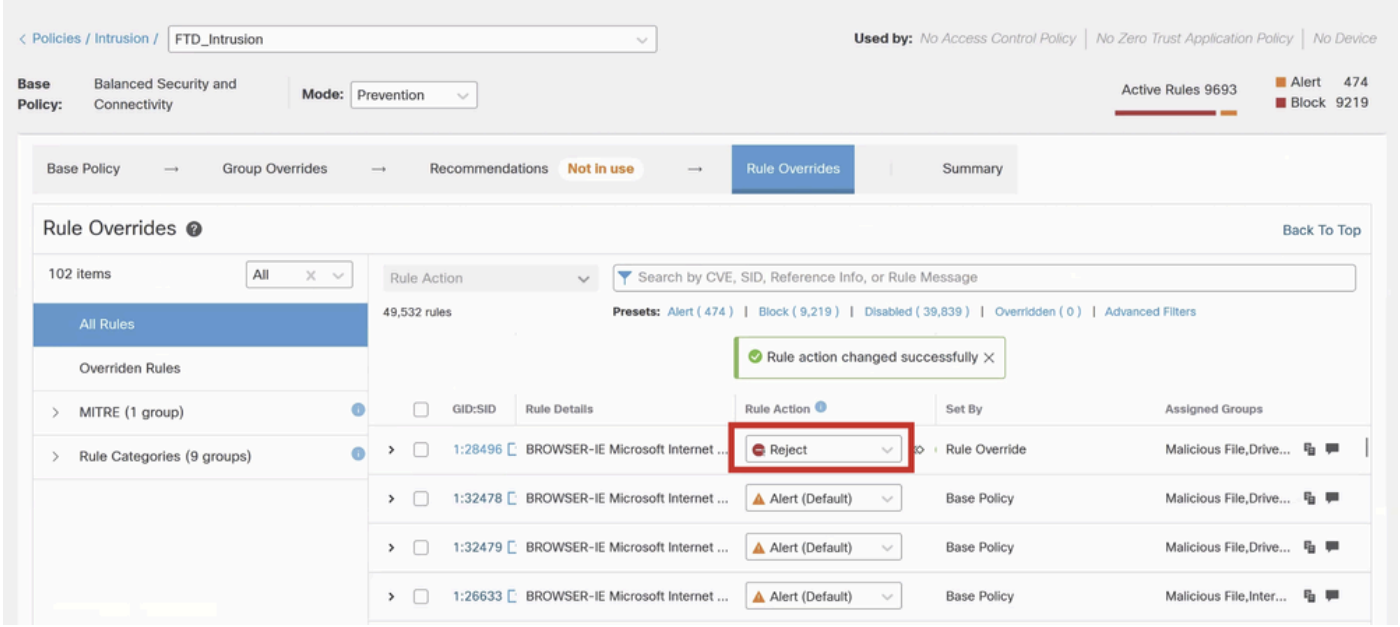


基本ポリシー

ルールの処理をこれらの新しいルールの処理のいずれかに変更するには、Rule Overrides > All Rulesの順に移動し、選択したルールのドロップダウンからルールの処理を選択します。

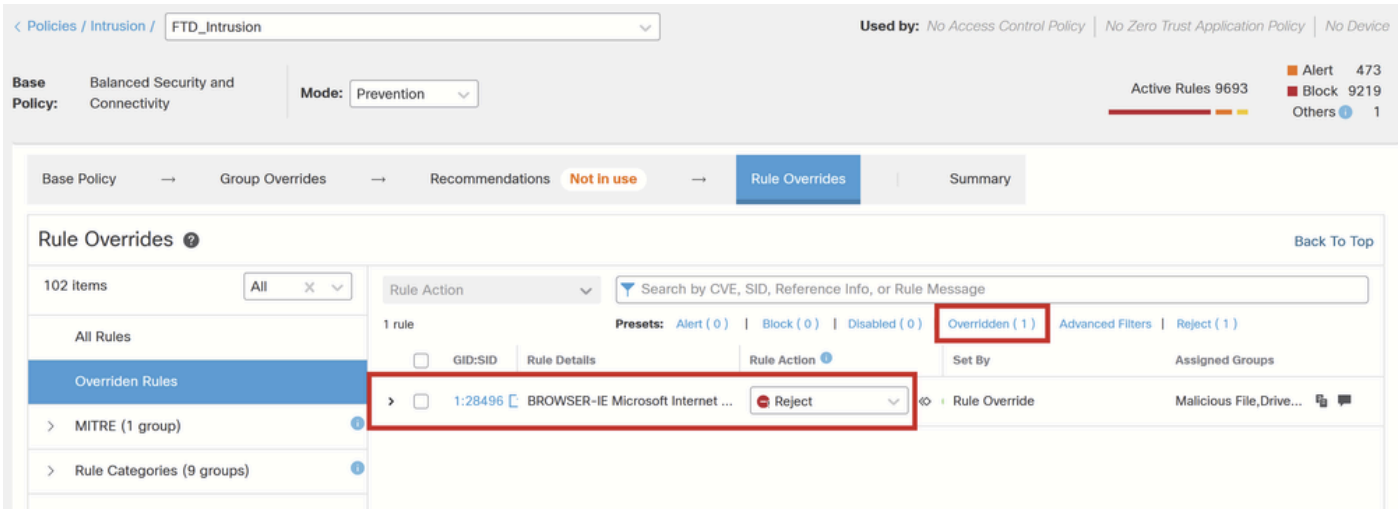


その他の規則の処理



ルール処理の変更

オーバーライドされたルールは、Rule Overrides > Override Rulesの下にあります。



オーバーライドされた規則

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。