

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](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[機能の詳細](#)

[FMCウォークスルー](#)

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。



The screenshot shows the FMC interface for managing intrusion policies. At the top, there are tabs for 'Intrusion Policies' and 'Network Analysis Policies'. Below the tabs is a search bar and several action buttons: 'All IPS Rules', 'IPS Mapping', 'Compare Policies', and 'Create Policy'. A table lists intrusion policies. The first row shows 'FTD_Intrusion' with a description of 'Balanced Security and Connectivity'. Under the 'Usage Information' column, it lists 'No Access Control Policy', 'No Zero Trust Application Policy', and 'No Device'. At the bottom right of this row, there are two buttons: 'Snort 2 Version' and 'Snort 3 Version'. The 'Snort 3 Version' button is highlighted with a red box.

Intrusion Policy	Description	Base Policy	Usage Information
FTD_Intrusion	Balanced Security and Connectivity		No Access Control Policy No Zero Trust Application Policy No Device

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。

< Policies / Intrusion / FTD_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 ■ Alert 474 ■ Block 9219

Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides | Summary

Balanced Security and Connectivity Back To Top

50 items Rule Action ▼ Search by CVE, SID, Reference Info, or Rule Message

All Rules 49,532 rules Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

	GID:SID	Rule Details	Rule Action	Assigned Groups
>	1:28496	BROWSER-IE Microsoft Internet Explorer crea...	Alert (Default)	Malicious File, Drive-by Co...
>	1:32478	BROWSER-IE Microsoft Internet Explorer CSe...	Alert (Default)	Malicious File, Drive-by Co...
>	1:32479	BROWSER-IE Microsoft Internet Explorer CSe...	Alert (Default)	Malicious File, Drive-by Co...
>	1:26633	BROWSER-IE Microsoft Internet Explorer html...	Alert (Default)	Malicious File, Internet Expl...
>	1:31621	BROWSER-IE Microsoft Internet Explorer onre...	Alert (Default)	Malicious File, Drive-by Co...
>	1:31622	BROWSER-IE Microsoft Internet Explorer onre...	Alert (Default)	Malicious File, Drive-by Co...

基本ポリシー

ルール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処理を選択します。

< Policies / Intrusion / FTD_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 ■ Alert 474 ■ Block 9219

Base Policy → Group Overrides → Recommendations Not in use → **Rule Overrides** | Summary

Rule Overrides Back To Top

102 items Rule Action ▼ Search by CVE, SID, Reference Info, or Rule Message

All Rules 49,532 rules Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
>	1:28496	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
>	1:32478	BROWSER-IE Microsoft Internet ...	Block	Base Policy	Malicious File, Drive...
>	1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
>	1:26633	BROWSER-IE Microsoft Internet ...	Rewrite	Base Policy	Malicious File, Inter...
>	1:31621	BROWSER-IE Microsoft Internet ...	Drop	Base Policy	Malicious File, Drive...
>	1:31622	BROWSER-IE Microsoft Internet ...	Reject	Base Policy	Malicious File, Drive...
>	1:31622	BROWSER-IE Microsoft Internet ...	Disable	Base Policy	Malicious File, Drive...
>	1:31622	BROWSER-IE Microsoft Internet ...	Revert to default	Base Policy	Malicious File, Drive...

その他の規則の処理

< Policies / Intrusion / FTD_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 Alert 474 Block 9219

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

Rule Overrides Back To Top

102 items All x v Rule Action v Search by CVE, SID, Reference Info, or Rule Message

49,532 rules Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

✔ Rule action changed successfully ✕

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
<input type="checkbox"/>	1:28496	BROWSER-IE Microsoft Internet ...	Reject	Rule Override	Malicious File, Drive...
<input type="checkbox"/>	1:32478	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
<input type="checkbox"/>	1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
<input type="checkbox"/>	1:26633	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Inter...

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。

< Policies / Intrusion / FTD_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 Alert 473 Block 9219 Others 1

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

Rule Overrides Back To Top

102 items All x v Rule Action v Search by CVE, SID, Reference Info, or Rule Message

1 rule Presets: Alert (0) | Block (0) | Disabled (0) | **Overridden (1)** | Advanced Filters | Reject (1)

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
<input type="checkbox"/>	1:28496	BROWSER-IE Microsoft Internet ...	Reject	Rule Override	Malicious File, Drive...

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。