

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

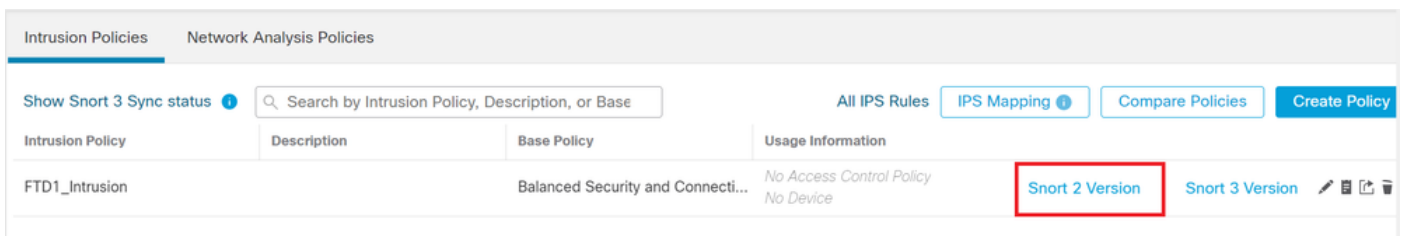
侵入検知システム(IDS)と侵入防御システム(IPS)のコンテキストでは、「SID」は「Signature ID」または「Snort Signature ID」を意味します。

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。

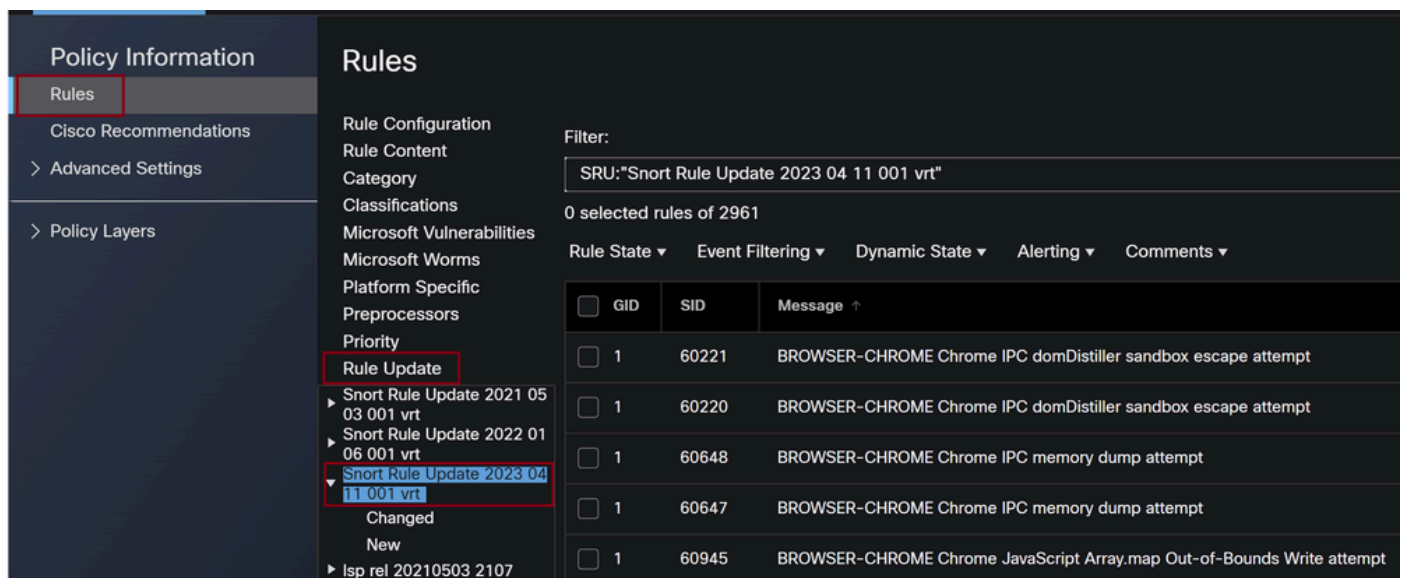
Snortルールをフィルタリングする手順

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

Rules

Rule Configuration

Rule Content

Category: SRU:"Snort Rule Update 2023 04 11 001 vrt"

Classifications: 0 selected rules of 16

Microsoft Vulnerabilities: Policy

Microsoft Worms

Platform Specific: Rule State, Event Filtering, Dynamic State, Alerting, Comments

Preprocessors

Priority: GID

Rule Update

04 10 001 vrt

Snort Rule Update 2023 04 11 001 vrt

Rule State	SID	Message
<input type="checkbox"/>	61614	readme file detected
<input type="checkbox"/>	61615	OS-WINDOWS Microsoft Windows AFD.sys privilege escalation

1 of 1

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。

Rules

Rule Configuration

Rule Content

Category: SRU:"Snort Rule Update 2023 04 11 001 vrt"

Classifications: 16 selected rules of 16

Microsoft Vulnerabilities: Policy

Microsoft Worms

Platform Specific: Rule State, Event Filtering, Dynamic State, Alerting, Comments

Preprocessors

Priority

Rule Update

04 10 001 vrt

Snort Rule Update 2023 04 11 001 vrt

Rule State

- Generate Events
- Drop and Generate Events
- Disable

Rule State	SID	Message
<input type="checkbox"/>	61614	readme file detected
<input type="checkbox"/>	61615	OS-WINDOWS Microsoft Windows AFD.sys privilege escalation

1 of 1

ルールの状態の選択

Snort 3ルールを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。

Intrusion Policies Network Analysis Policies

Show Snort 3 Sync status

Search by Intrusion Policy, Description, or Base

All IPS Rules IPS Mapping Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information
FTD1_Intrusion	Balanced Security and Connecti...	No Access Control Policy No Device	Snort 2 Version Snort 3 Version

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。

< Intrusion Policy

Policy Name Used by: No Access Control Policy | No Device

Mode Base Policy Balanced Security and Connectivity

Disabled 39249 | Alert 470 | Block 9151 | Overridden 0 | Rewrite 0 | Pass 0 | Drop 0 | Reject 0

Rule Groups Back To Top

50 items Excluded | Included | Overridden

All Rules Reco

All Rules assigned to current intrusion policy irrespective of rule group

Rule Action

48,870 rules Preset Filters: Advanced Filters | 470 Alert rules | 9,151 Block rules | 39,249 Disabled rules | 0 Overridden rules

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input type="checkbox"/>	1:28496	BROWSER-IE Microsoft Internet Explore...	<input type="text" value="Alert (Default)"/>	Browser/Internet Explo...

Snort 3フィルタ

Advanced Filters ?

LSP

Select...

Show Only * New Changed

Classifications

Select...

Microsoft
Vulnerabilities

Select...

Cancel

OK

高度なフィルタの下のLSP

Advanced Filters ?

LSP

Show Only * New Changed

Classifications

Microsoft Vulnerabilities

Cancel

LSPバージョン

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22 ▾ | 48,870 rules Preset Filters: 0 Alert rules | **11 Block rules** | 11 Disabled rules | 0 Overridden rules | Advanced Filters

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

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。

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22 | 22 ▾ | 48,870 rules Preset Filters: 0 Alert rules | 11 Block rules | 11 Disabled rules | 0 Overridden rules | Advanced Filters

<input checked="" type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input checked="" type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

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。