CLIおよびFMC GUIを使用して、Firepowerセンサーからカスタムsidリストを確認します

概要

このドキュメントでは、CLIおよびFMC GUIを使用して、Firepower Threat Defense(FTD)またはFirePOWERモジュールからカスタムSIDリストを取得する方法について説明します。SID情報は、FMC GUIで[Objects] > [*Intrusion Rules*]に移動する*と確認できます*。場合によっては、CLIから使用可能なSIDのリストを取得する必要があります。

前提条件

要件

次の項目について理解しておくことをお勧めします。

- Cisco Firepower Threat Defense（FTD）
- Cisco ASA with FirePOWER Services
- Cisco Firepower Management Center(FMC)
- Linuxの基礎知識

使用するコンポーネント

この文書の情報は、次のソフトウェアのバージョンに基づいています。

- Firepower Management Center 6.6.0
- Firepower Threat Defense 6.4.0.9
- FirePOWERモジュール6.2.3.2

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、初期（デフォルト）設定の状態から起動しています。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

侵入ルー*ル*は、ネットワークの脆弱性を悪用しようとする試みを検出するためにシステムが使用するキーワードと引数のセットです。システムがネットワークトラフィックを分析すると、パケットが各ルールで指定された条件と比較されます。パケットデータがルールで指定されたすべての条件に一致すると、ルールがトリガーされます。ルールがアラートルールの場合、侵入イベントが生成されます。パスルールの場合、トラフィックは無視されます。インライン展開の廃棄ルールでは、システムはパケットを廃棄し、イベントを生成します。Firepower Management Center(FMC)Webコンソールから侵入イベントを表示および評価できます。

Firepowerシステムには、次の2種類の侵入ルールがあります。*共有オブジェクト規則*と標準テ*キスト規則です*。Cisco Talos Security Intelligence and Research Group(Talos)は、共有オブジェクトルールを使用して、従来の標準テキストルールでは不可能だった脆弱性に対する攻撃を検出で

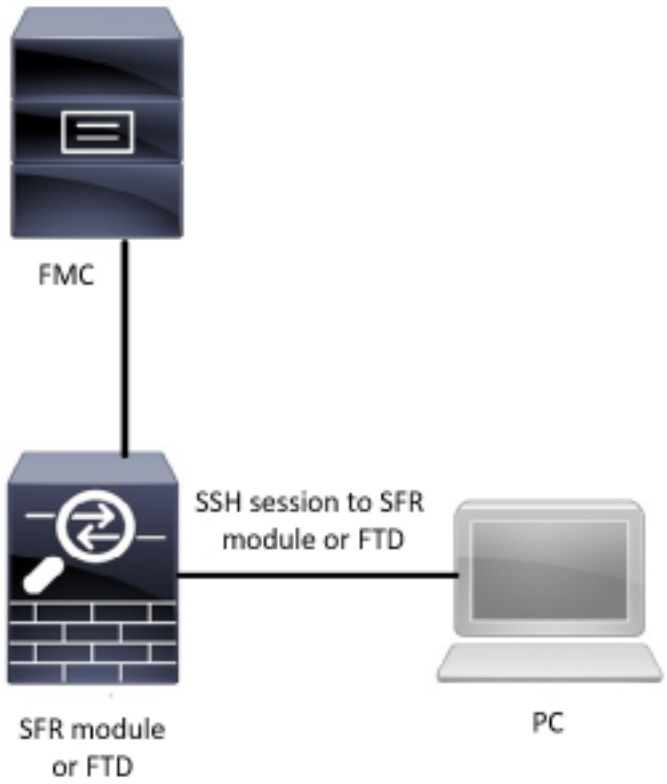
きます。共有オブジェクトルールを作成することはできません。侵入ルールを独自に作成する場合は、標準のテキストルールを作成する必要があります。表示される可能性のあるイベントの種類を調整するためのカスタム標準テキストルール。ルールを記述し、ルールのイベントメッセージを指定することで、攻撃とポリシーの回避を示すトラフィックをより簡単に特定できます。

カスタム侵入ポリシーでカスタム標準テキストルールを有効にする場合、ルールキーワードや引数によっては、トラフィックを最初に特定の方法でデコードまたは前処理する必要があることに注意してください。

Firepower System***のカスタムロ***ーカルルールは、ローカルマシンからASCIIテキストファイル形式でインポートするカスタム標準Snortルールです。Firepowerシステムでは、Webインターフェイスを使用してローカルルールをインポートできます。ローカル ルールをインポートする手順は非常に簡単です。ただし、最適なローカルルールを作成するには、Snortおよびネットワークプロトコルに関する詳細な知識が必要です。

> **警告**：実稼働環境でルールを使用する前に、管理されたネットワーク環境を使用して、作成した侵入ルールをテストしてください。不適切な侵入ルールがシステムのパフォーマンスに重大な影響を与える可能性があります

ネットワーク図



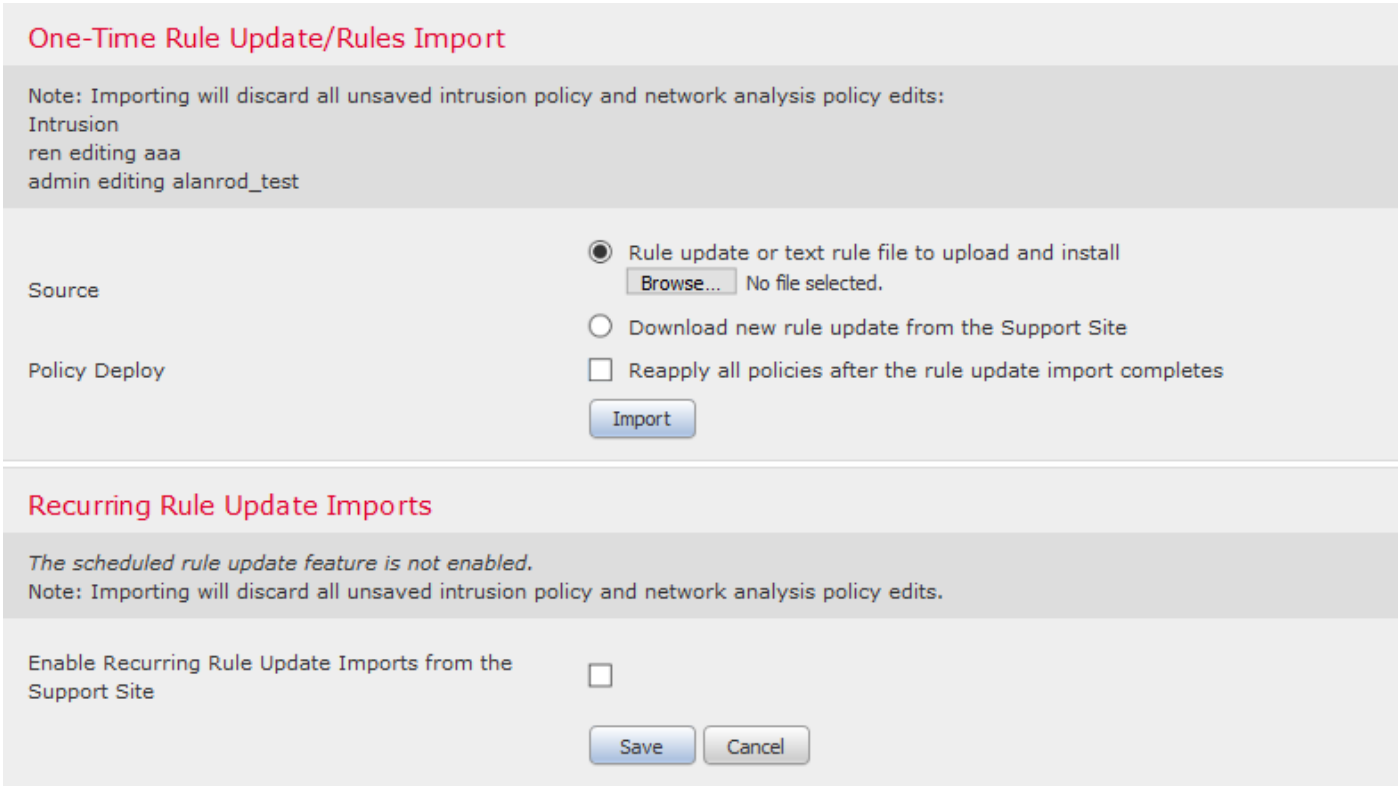
設定

ローカル ルールのインポート

作業を開始する前に、カスタムファイルに記載されているルールに特殊文字が含まれていないことを確認する必要があります。ルールをインポートする際は、すべてのカスタム ルールを ASCII または UTF-8 エンコーディングを使用してインポートする必要があります。次に示す手順では、

ローカルマシンからローカル標準テキストルールをインポートする方法について説明します。

ステップ1:[Import Rules]タブにアクセスするには、[Objects] > [Intrusion Rules] > [Import Rules]に移動します。[ルールの更新]ページが次の図のように表示されます。



ステップ2：アップロードしてインストールするルール更新ファイルまたはテキストルールファイルを選択し、[参照]をクリックして、カスタムルールファイルを選択します

> **注**：アップロードされたすべてのルールは、ローカルルールカテゴリ**に保存されます**

ステップ 3：[Import] をクリックします。ルールファイルがインポートされます

> **注**:Firepowerシステムでは、検査に新しいルールセットは使用しません。ローカル ルールをアクティブにするには、侵入ポリシーでローカル ルールを有効にしてから、そのポリシーを適用します。

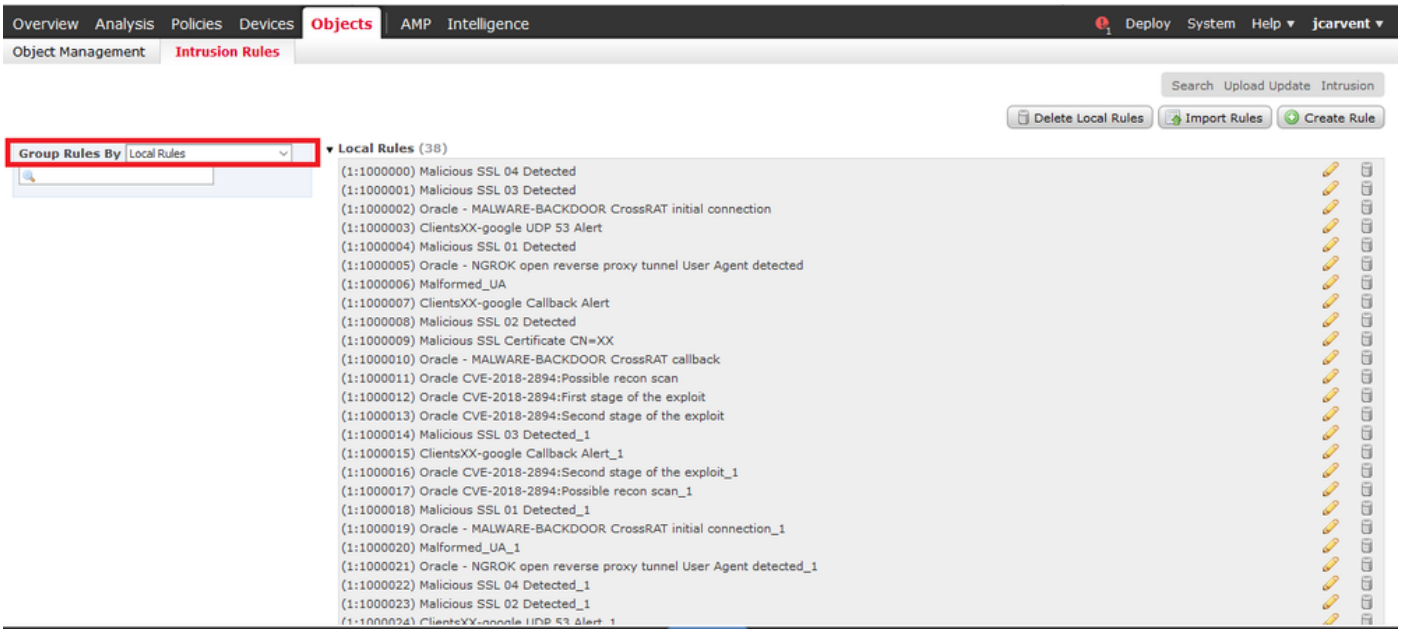
確認

FMC GUIから

1. FMC GUIからインポートされたローカルルールの表示

ステップ1:[Objects] > [**Intrusion Rules]に移動します。**

ステップ2：グループのルールから**ローカルルを選択します。**



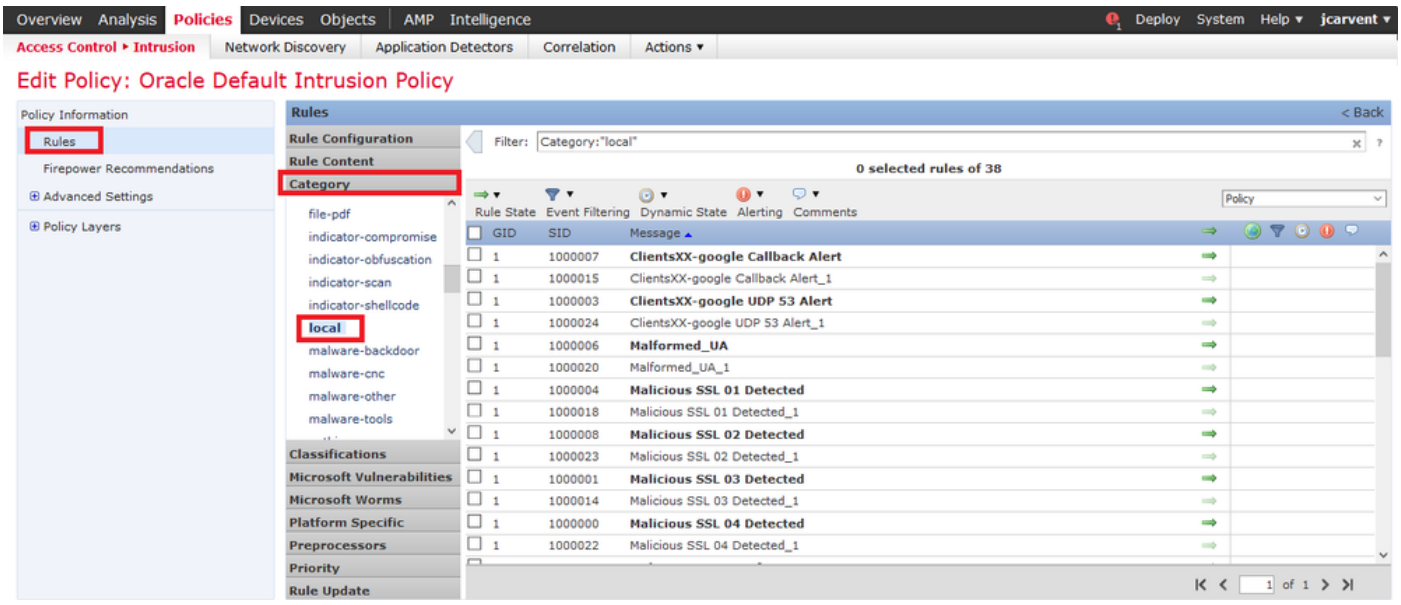
デフォルトでは、Firepowerシステムはローカルルールをディセーブル状態に設定します。これらのローカルルールを侵入ポリシーで使用するには、ローカルルールの状態を手動で設定する必要があります。

2.侵入ポリシーからローカルルールを有効にする

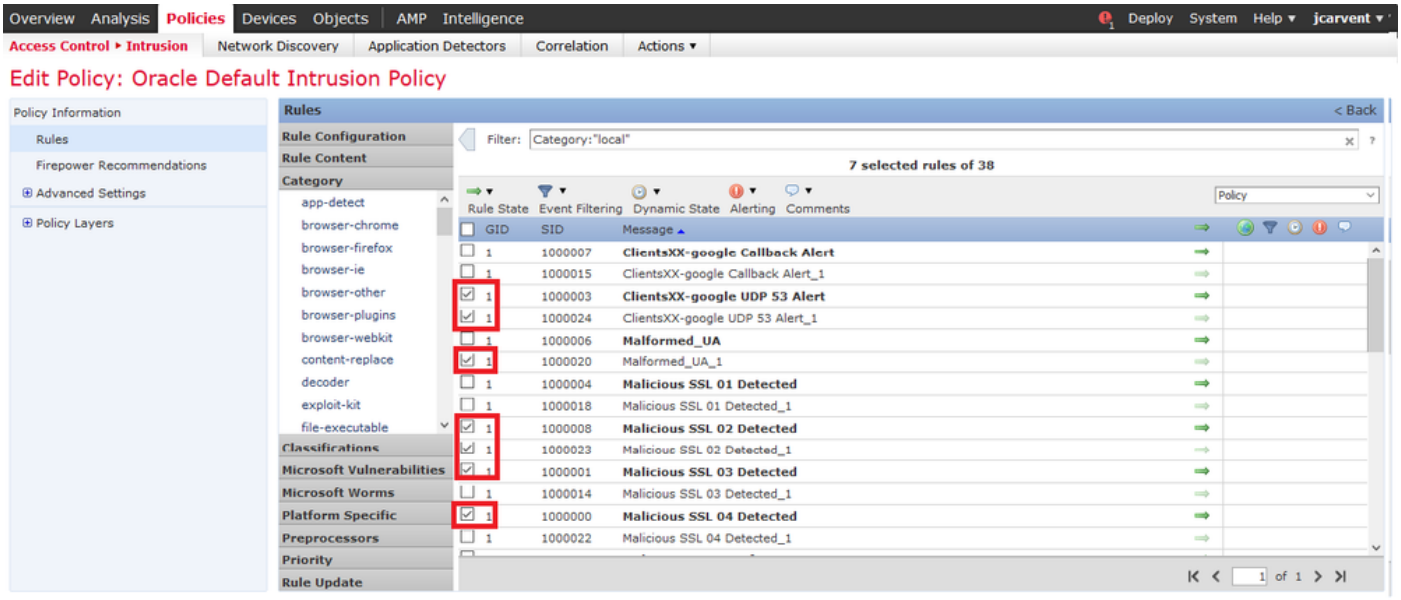
ステップ1:[Policies] > [Intrusion] > [Intrusion Policy]の下の[Policy Editor] ページに移動します。

ステップ2：左側のパネルで[ルール]を選択します。

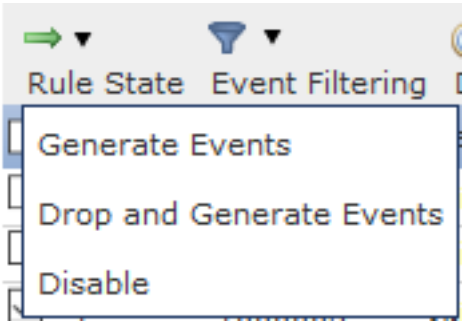
ステップ3:[カテゴリ]で[local]を選択します。すべてのローカルルールが使用可能な場合は表示されます。



ステップ 4： 必要なローカルルールを選択します。



ステップ 5：必要なローカル· ルールを選択した後、「ルールの状態」から状態**を選択します**



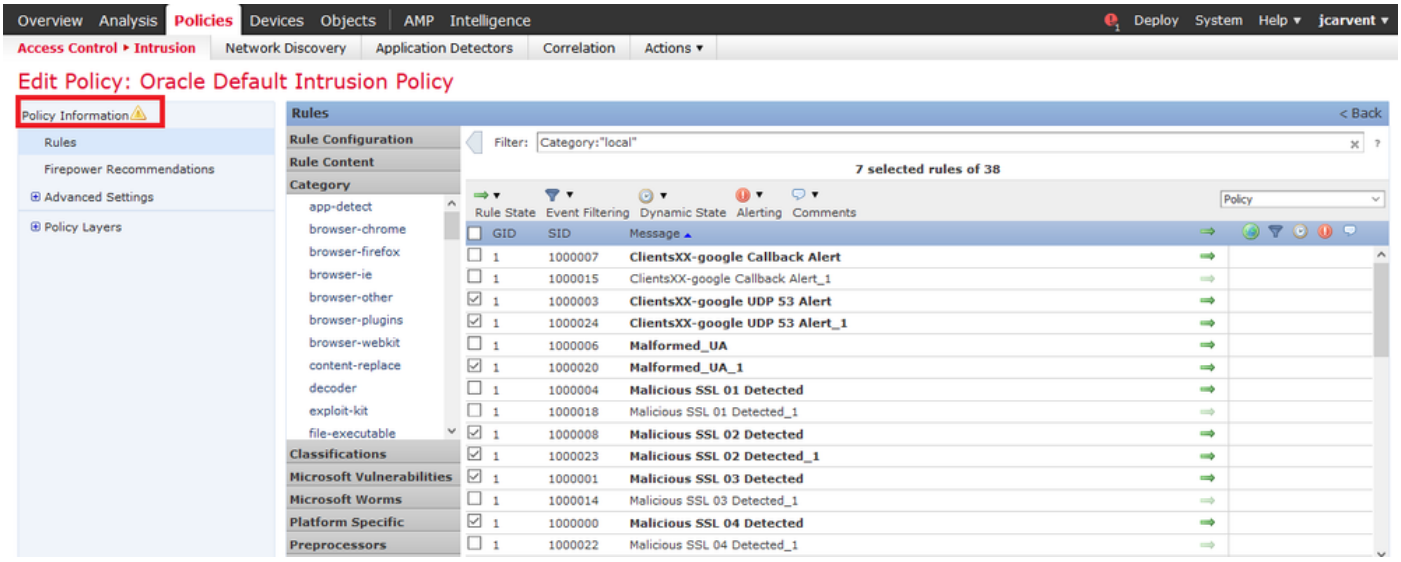
次のオプションを使用できます。

– イベントの生成：ルールを有効にし、イベントを生成します

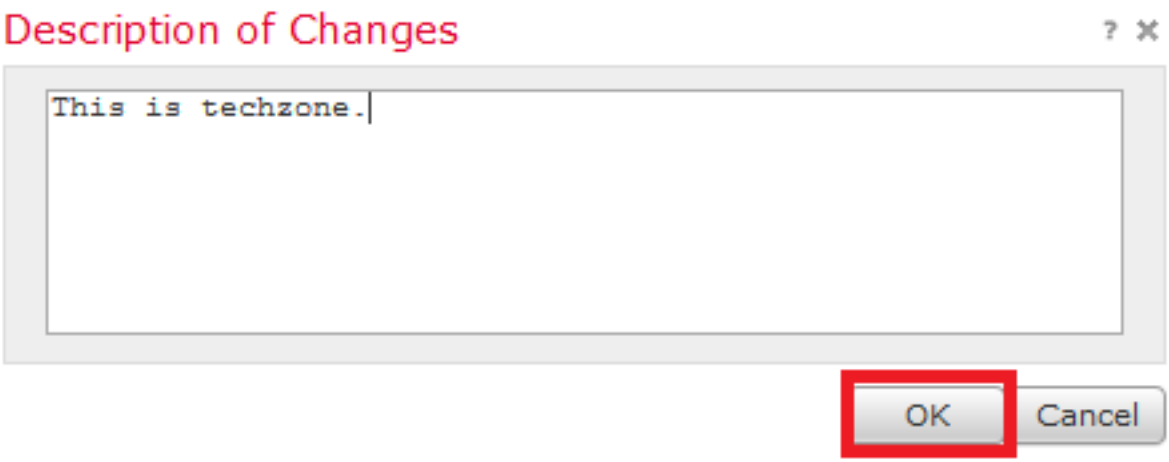
– イベントのドロップと生成：ルールの有効化、トラフィックのドロップ、イベントの生成

-無効化:ルールを有効にしない、イベントを無効にする

手順 6： ルールの状態を選択したら、 **左側のパネルの[Policy Information]オプション**



ステップ7:[Commit **Changes**]ボタンを選択し、変更の簡単な説明を入力します。後で[OK]をクリックします。侵入ポリシーが検証されます。



注：侵入ポリシーの侵入イベントしきい値機能と組み合わせて非推奨のしきい値キーワードを使用するインポートされたローカルルールを有効にすると、ポリシー検証は失敗します。

ステップ8：変更の展開

FTDまたはSFRモジュールのCLIから

1. FTDまたはSFRモジュールのCLIからインポートされたローカルルールを表示する

ステップ1:SFRモジュールまたはFTDからSSHまたはCLIセッションを確立します

ステップ2：エキスパートモードに移動します。

```
> expert
admin@firepower:~$
```

ステップ3：管理者権限の取得

```
admin@firepower:~$ sudo su -
```

ステップ4：パスワードを入力します

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

ステップ5:/ngfw/**var/sf/detection_engines/UUID/intrusion/に移動します。**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

注：SFRモジュールを使用している場合は、/ngfw/var/sf/detection_engines/*/intrusion pathを使用しないでください。insted use **/var/sf/detection_engines/*/intrusion**

ステップ6：次のコマンドを導入します

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```

次の図を例として参照してください。

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```

これにより、FTDまたはSFRモジュールで有効になっているカスタマーSIDリストが表示されます。

トラブルシュート

ステップ1: FMC detection_enginesからSFRモジュールまたはFTDへのSSHセッションが確立されていないことを確認します

ステップ2:コマンドgrep -Eo "sid:*([0-9]{1,8})" */*local.rulesは侵入ディレクトリでのみ動作します。このコマンドは別のディレクトリからは使用できません

ステップ3: grep -Eo "sid:*([0-9]{1,8})" */*.rulesコマンドを使用して、すべてのカテゴリから完全なSIDリストを取得します

ローカル侵入ルールをインポートするためのベストプラクティス

ローカル規則ファイルをインポートする場合は、次のガイドラインに従ってください。

- ルールのインポートでは、すべてのカスタムルールをプレーンテキストファイルにインポートし、ASCIIまたはUTF-8でエンコードする必要があります
- テキストファイル名には、英数字、スペース、およびアンダースコア(_)、ピリオド(.)、ダッシュ(-)以外の特殊文字を使用できません
- ローカルルールの先頭にポンド文字(#)が1つ付いてインポートされますが、削除のフラグが付けられます
- システムは、1つのシャープ文字(#)で始まるローカルルールをインポートし、2つのシャープ文字(##)で始まるローカルルールはインポートしません
- ルールにエスケープ文字を含めることはできません
- ローカルルールをインポートするときに、ジェネレータID(GID)を指定する必要はありません。この場合、標準のテキストルールに対してGID 1のみを指定します
- ルールを初めてインポートする場合は、次の手順を実行します *not* を指定 Snort ID (SID)またはリビジョン番号。これにより、削除されたルールを含む、他のルールの SID との競合が回避されます。システムは、次に使用可能なカスタムルールSID 1000000以上、リビジョン番号1を自動的にルールに割り当てます
- SIDを持つルールをインポートする必要がある場合、SIDは1,000,000 ~ 9,999,999の一意の

番号である必要があります
- マルチドメイン展開では、システムは、WLC上のすべてのドメインで使用される共有プールからインポートされたルールにSIDを割り当てます Firepower Management Center.複数の管理者が同時にローカルルールをインポートしている場合、システムが別のドメインにシーケンスの間に番号を割り当てているため、個々のドメイン内のSIDが連続していないように見える場合があります
- 以前にインポートしたローカルルールの更新バージョンをインポートする場合、または削除したローカルルールを復元する場合は、システムによって割り当てられたSIDと現在のリビジョン番号より大きいリビジョン番号を含める必要があります。ルールを編集することで、現在または削除されているルールのリビジョン番号を確認できます

  注：ローカルルールを削除すると、システムによってリビジョン番号が自動的に増分されます。これは、ローカル ルールを復元できるようにするための方法です。削除されたすべてのローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動されます。

- SIDの番号付けの問題を回避するために、プライマリFirepower Management Center(FMC)でハイアベイラビリティペアのローカルルールをインポートします
- ルールに次のいずれかが含まれている場合、インポートは失敗します。SIDが2147483647より大きい64文字を超える送信元ポートまたは宛先ポートのリスト
- 侵入ポリシーの侵入イベントしきい値機能と組み合わせて非推奨のしきい値キーワードを使用するインポートされたローカルルールを有効にすると、ポリシーの検証が失敗します
- インポートされたすべてのローカルルールは、ローカルルールカテゴリに自動的に保存されます
- インポートするローカルルールは、常に無効なルール状態に設定されます。ローカルルールを侵入ポリシーで使用するには、ローカルルールの状態を手動で設定する必要があります

関連情報

Snort SIDに関連する参照用のドキュメントを次に示します。

侵入ルールの更新

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

侵入ルールエディタ

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html