Cisco SireSIGHT システムのカスタム ローカル Snort ルール

目次

概要

FireSIGHT システムでのカスタム ローカル ルールとは、ユーザが標準 Snort ルールをカスタマイズしてローカル マシンから ASCII テキスト ファイル形式でインポートするルールのことです。 FireSIGHT 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るようになっています。 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 とネットワーク プロトコルに精通している必要があります。

このドキュメントの目的は、カスタム ローカル ルールを作成するためのヒントとサポートを提供することです。 ローカル ルールの作成手順については、『*Snort Users Manual*』を参照してください。このマニュアルは、snort.org から入手できます。 カスタム ローカル ルールを作成する前に、このユーザ マニュアルをダウンロードして読むことを推奨します。

> **注:** Sourcefire Rule Update（SRU）パッケージで提供されているルールは、Cisco Talos セキュリティ インテリジェンス & リサーチ グループによって作成およびテストされ、Cisco Technical Assistance Center（TAC）でサポートされています。 Cisco TAC ではカスタム ローカル ルールの作成または調整に対するサポートを提供していませんが、FireSIGHT システムのルール インポート機能で問題が発生した場合は、Cisco TAC に連絡してください。

> **警告**： 不適切に作成されたカスタム ローカル ルールが FireSIGHT システムのパフォーマンスに影響し、結果としてネットワーク全体のパフォーマンスが劣化する可能性があります。 ネットワークでパフォーマンス問題が発生したときに、FireSIGHT システムで有効にされているカスタム ローカル Snort ルールがある場合、それらのローカル ルールを無効にすることを推奨します。

前提条件

要件

Snort ルールおよび FireSIGHT システムに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- FireSIGHT Management Center（別名 Defense Center）
- ソフトウェア バージョン 5.2 以降

カスタム ローカル ルールの使用

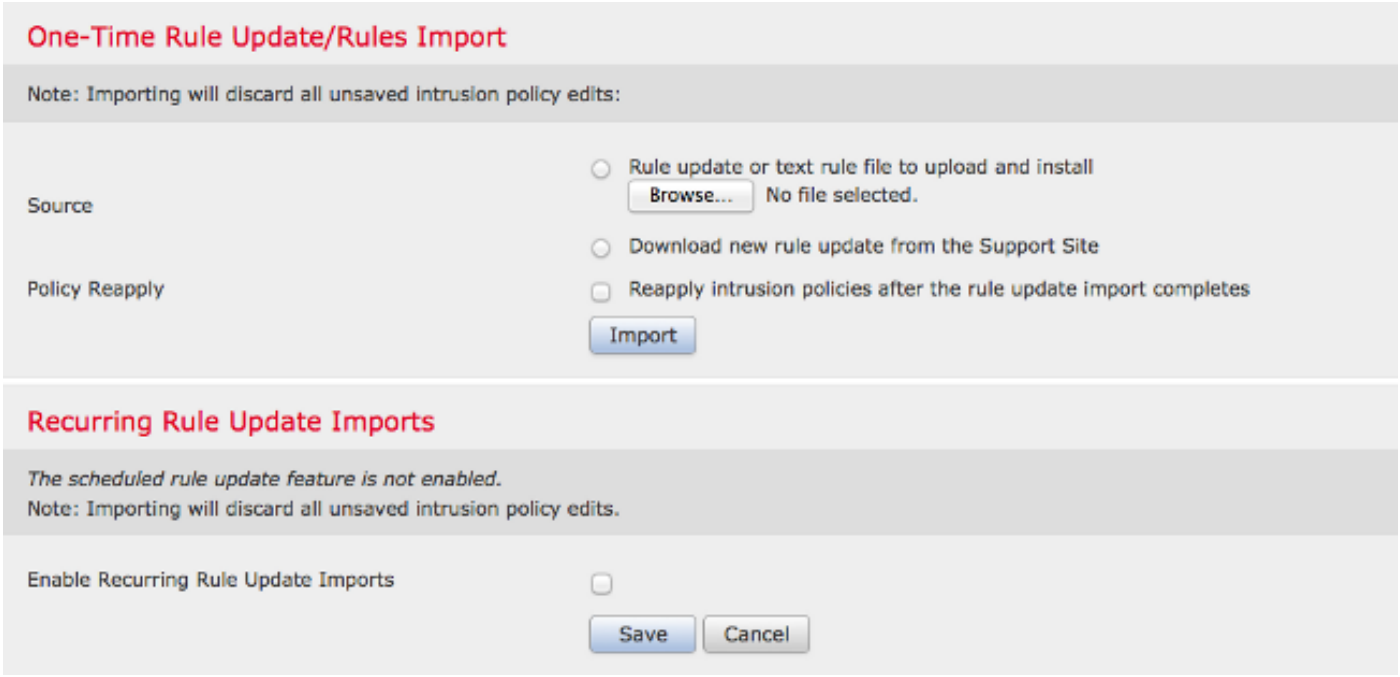
ローカル ルールのインポート

手順を開始する前に、ファイル内のルールにエスケープ文字が一切含まれていないことを確認してください。 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。

次の手順では、標準テキスト形式のローカル ルールをローカル マシンからインポートする方法を説明します。

1. [Policies] > [Intrusion] > [Rule Editor] に移動してルール エディタにアクセスします。

2. [Import Rules] をクリックします。 [Rule Updates] ページが表示されます。



図： [Rule Updates] ページのスクリーンショット

3. [Rule update or text rule file to upload and install] を選択してから [Browse] をクリックし、ルール ファイルを選択します。

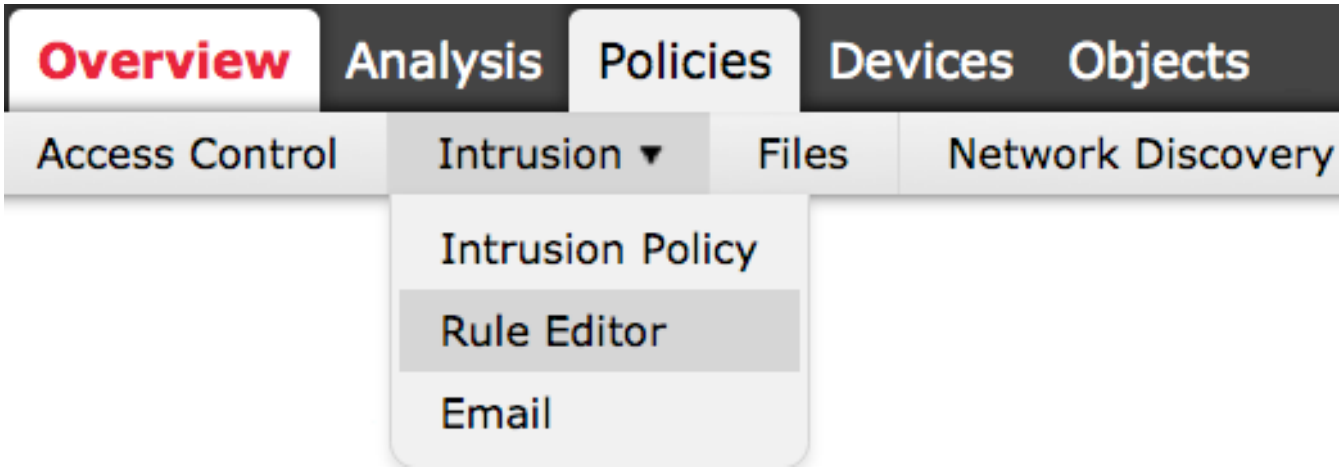
> **注:** アップロードされたすべてのルールは、[local rule] カテゴリに保存されます。

4. [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。

> **注意**： FireSIGHT システムでは、インスペクションに新規ルール セットを使用しません。 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。

ローカル ルールの確認

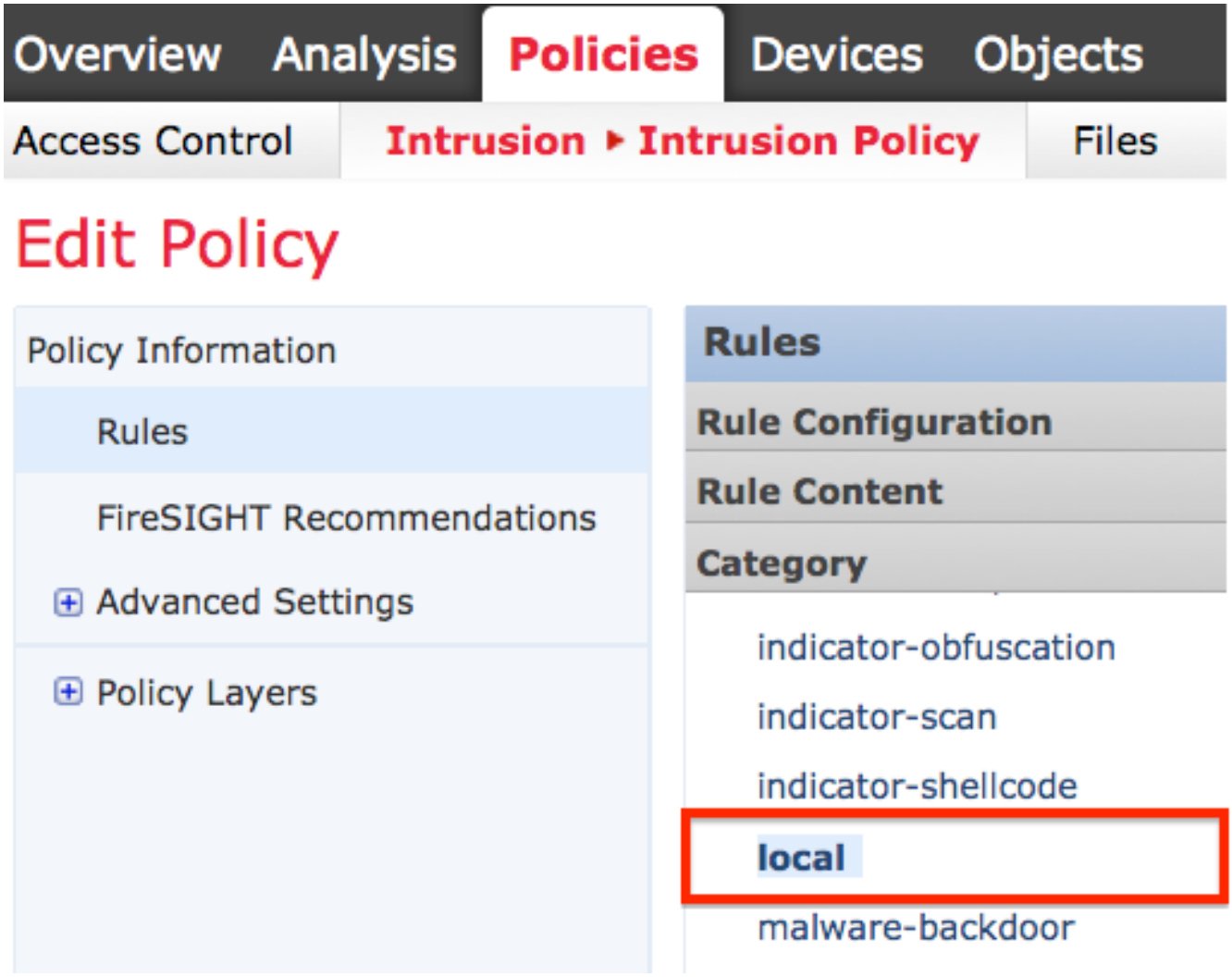
- 現在のローカル ルールのリビジョン番号を確認するには、[Rule Editor] ページに移動します（ [Policies] > [Intrusion] > [Rule Editor] ）。



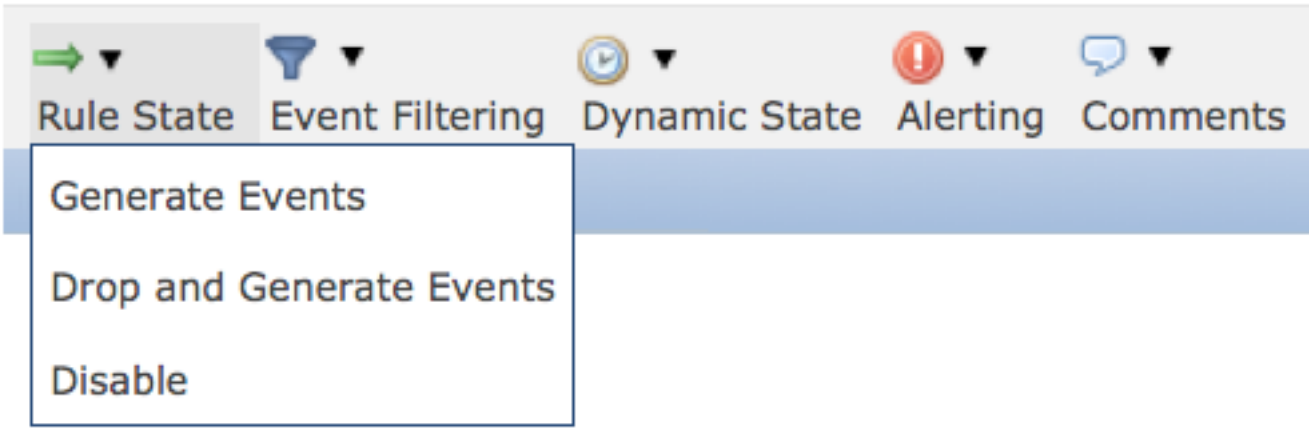
- [Rule Editor] ページで、[Local Rule] カテゴリをクリックしてフォルダを展開し、対象のルールの横にある [Edit] をクリックします。
- インポートされたすべてのローカル ルールは、[local rule] カテゴリに自動的に保存されます。

ローカル ルールの有効化

- デフォルトでは、FireSIGHT システムはローカル ルールを無効の状態に設定します。 ローカル ルールの状態を手動で設定してからでないと、侵入ポリシーでローカル ルールを使用できません。
- ローカル ルールを有効にするには、[Policy Editor] ページに移動します（ [Policies] > [Intrusion] > [Intrusion Policy] ）。 左側のパネルで [Rules] を選択します。 [Category] で [local] を選択します。 使用可能なローカル ルールがすべて表示されます。



- 目的のローカル ルールを選択してから、ルールの状態を選択します。



- ルールの状態を選択したら、左側のパネルで [Policy Information] オプションをクリックします。 [Commit Changes] ボタンをクリックします。 侵入ポリシーが検証されます。

  注: 侵入ポリシーで、侵入イベントのしきい値機能と組み合わせて非推奨の threshold キーワードを使用しているローカル ルールをインポートして有効にすると、ポリシーの検証は失敗します。

削除されたローカル ルールの確認

- 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。
- 削除されたローカル ルールのリビジョン番号を確認するには、[Rule Editor] ページに移動し、[deleted] カテゴリをクリックしてフォルダを展開した後、鉛筆アイコンをクリックします。これにより、[Rule Editor] ページにルールの詳細が表示されます。

ローカル ルールの番号指定

- ジェネレータ ID（GID）を指定する必要はありません。 GID を指定する場合は、標準テキスト ルールに対しては GID 1 のみ、機密データ ルールに対しては 138 のみを指定できます。
- 初めてルールをインポートするときには、Snort ID（SID）またはリビジョン番号を指定しないでください。 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。
- FireSIGHT Management Center はルールに対し、次に使用できる 1000000 以降のカスタム ルール SID と、リビジョン番号 1 を自動的に割り当てます。
- 2147483647 よりも大きい SID が割り当てられた侵入ルールをインポートしようとすると、検証エラーが発生します。
- 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には、IPS 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後のリビジョン番号を含める必要があります。
- IPS 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後のリビジョン番号を使用してルールをインポートすることにより、削除したローカル ルールを復元することができます。 ローカル ルールを削除すると、FireSIGHT Management Center は自動的にリビジョン番号を増やすことに注意してください。 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。