

# 目次

[概要](#)

[はじめに](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[EAFs の概要](#)

[設定](#)

[関連情報](#)

## 概要

この資料が IPS デバイスマネージャ (IDM) または Express (IME) IPS マネージャを使用して False positive 防止のための侵入防御システム (IPS) を調整するために必要なステップを提供したものです。IPS で調整する False positive は検知時のアクション フィルタ (EAF) と呼ばれる機能によって実現します。

## [はじめに](#)

### [要件](#)

このドキュメントを読む人は Cisco IPS のナレッジがあるはずです。

### [使用するコンポーネント](#)

この文書に記載されている情報は特定のハードウェア および ソフトウェア バージョンに基づいていません。

### [表記法](#)

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## [EAFs の概要](#)

EAFs は false positive 調整のために主に設定されます。EAF は特定のシグニチャをトラフィックのサブセットのための望ましい アクションを奪取しなくてももらう機能を提供します。

EAFs は複数の条件を満たすことを必要とする状況で役立ちます (以下を参照) :

- シグニチャ X はトラフィックの望ましいサブネットのための処置 y をとりません。
- シグニチャ X は他のすべてのトラフィックのための処置 y をとります。

EAFs はシグニチャの良性に引き起こすことをあつかう上で役立ちます。

# 設定

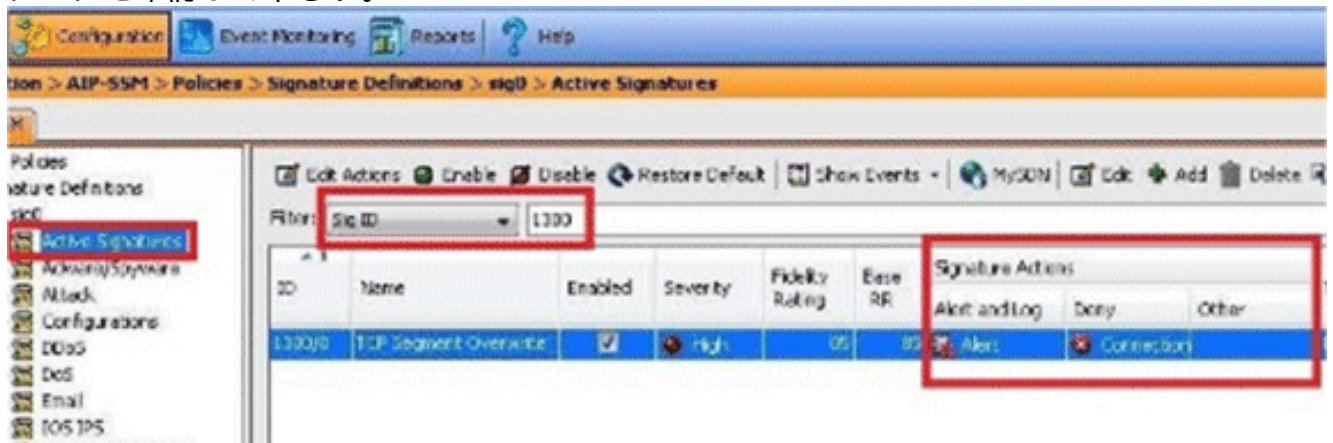
例： False positive イベント: 既知 信頼できるホストからおよびに来るトラフィックのためのシグニチャ 1300 トリガー。

注これはデモンストレーション目的でのみちょうど例です。 シグニチャトリガーによる特定のイベントは良性であるかどうか不確実、更なる分析に関しては Cisco テクニカル サポートに連絡して下さい。

注IPS シグニチャに関するその他の情報に関しては [Cisco 侵入防御システム シグニチャ](#)を参照して下さい。

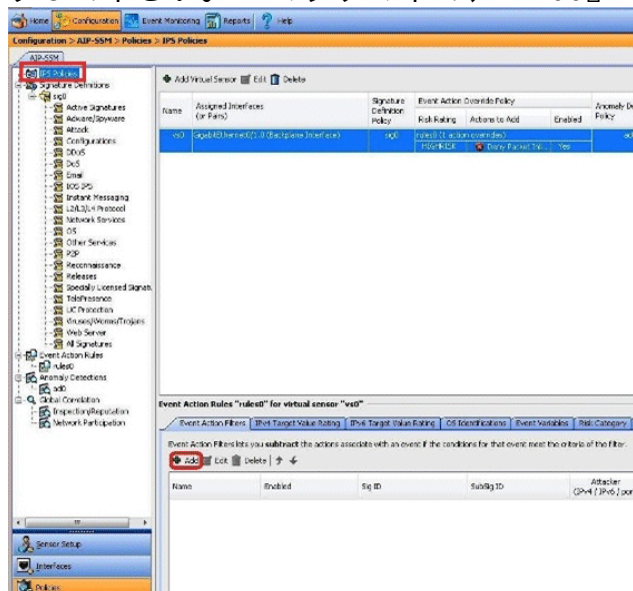
次の手順を実行します。

1. EAF が設定される必要があるシグニチャ ( この例の 1300、 ) があるようにデフォルト アクションを確認して下さい。



シグニチャ 1300 のデフォルト アクションは生成し、アラートをインラインに否定します 接続を含んでいます。

2. このシグニチャが起動 するべきではないホストを識別して下さい。たとえば、シグニチャに 10.1.1.1-10.1.1.254 のような信頼されたサブネットから、来るトラフィックで起動してほしくないです。
3. ステップ 2 に説明がある基準のための EAF を作成して下さい:IDM/IME から、> IPS ポリシー Configuration > Policies の順に進んで下さい。 検知時のアクション Filters タブをクリックして下さい。このタブの下で、『Add』 をクリックして下さい。



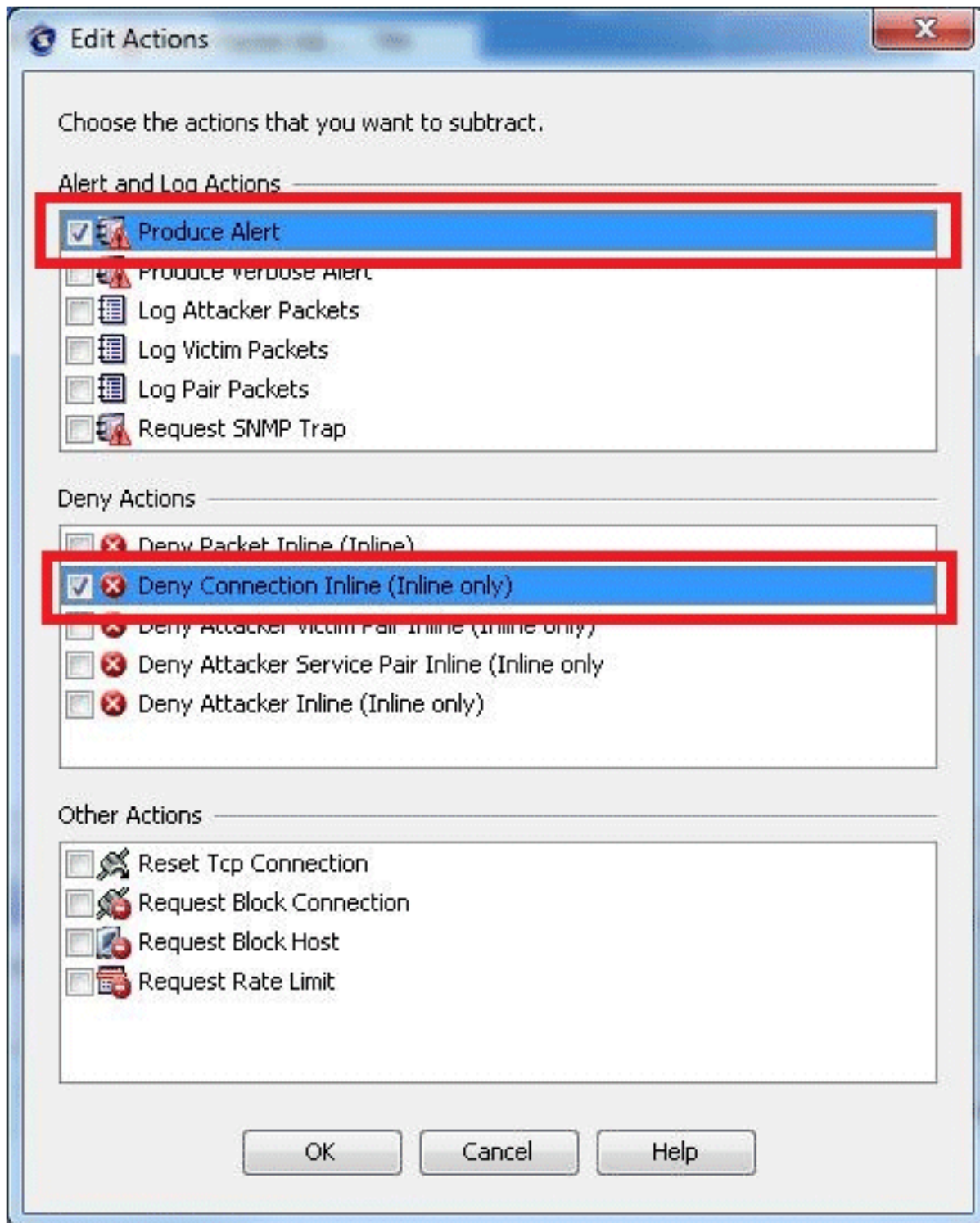
このウィンドウは表示する

名前、シグニチャ ID、攻撃者 IP、先祖などのようなさまざまなフィールドを設定して下さい

フィールドを編集操作ダイアログボックスを開くために引く操作の右へアイコンをクリックして下さい

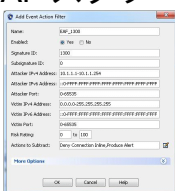
このウィンドウで、IPS に実行してほ

しくないシグニチャ操作を規定できます。注正しくシグニチャを引きたいと思う操作は選択するためにステップ 1.に記述されているようにデフォルト シグニチャ操作を理解する必要があります。この例では、生成し、アラートをインラインに否定します接続を選択しました。



IPS はこれらの処置を 10.1.1.1-10.1.1.254 から来るトラフィックのための 1300 のシグニチャトリガーと見ません。他のすべてのトラフィックに関しては、インラインに Produce アラートおよび拒否接続のデフォルト シグニチャ操作はまだ適用します。選択した後アラートを生成し、パケットを、見ます EAF スクリーンの一番下でこれらの操作にデータを入力する

をインラインに拒否して下さい:



『OK』 をクリックし、次に変更を保存するた

めに適用して下さい。

CLI を使用して検知時のアクション フィルタの設定には、[コンフィギュレーション ガイド ページ](#)の IPS Command Line Interface セクションを参照して下さい。適切なコンフィギュレーション ガイドから、[検知時のアクション ルールを設定することをクリックし](#)、「検知時のアクションの設定をフィルタリングします」捜して下さい。

## [関連情報](#)

- [テクニカルサポートとドキュメント - Cisco Systems](#)