Cisco Secure IPS - 誤検出アラームの除外

目次

概要

このドキュメントでは、Cisco Secure Intrusion Prevention System（IPS）の false positive アラームの除外について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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基づいた on Cisco セキュア侵入防御システム（IPS）バージョン 7.0 および Cisco IPS Manager Express 7.0 です。

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

False Positive アラームと False Negative アラーム

パケットのある特定のパケットかシーケンスが Cisco Secure IPS シグニチャで定義される既知の攻撃プロファイルの特性と一致するとき Cisco Secure IPS はアラームを引き起こします。 重要な IPS シグニチャ 設計基準は false positive および誤った ネガティブ アラームの発生回数を最小限に抑えることです。

IPS が悪意のあるようにある特定の良性 アクティビティを報告すると False positive（正常動作でのトリガー）は行われます。 これは人間の介入がイベントを診断するように要求します。 多数の false positive はかなりリソースを流出できそれらを分析するために必要となる専門にされたスキルは高価、見つけにくいです。

偽陰性は IPS が実際の悪意のあるアクティビティを検出するし、報告すると発生します。 これの結果は破局的である場合もあり、新しいエクスプロイトおよび切り刻む手法が検出されると同時にシグニチャは絶えずアップデートする必要があります。 false negative を最小限にすることは非常に優先順位が高い項目であり、時には false positive の発生が高くなることを承知した上で行う必要があります。

IPS が悪意のあるアクティビティを検出するのに使用するシグニチャの性質が原因で完全に IPS の効果を大幅に低下させるか、またはひどく組織のコンピューティング インフラストラクチャを破壊しないで false positive および負を除去することはほとんど不可能です（ホストおよびネットワークのような）。 IPS が展開されるときカスタマイズされた調整は false positive を最小に します。 コンピュータ環境が変更されたときなどは（新しいシステムやアプリケーションの導入など）、定期的な再調整も必要です。 Cisco Secure IPS は定常オペレーションの間に false positive を最小に することができる適用範囲が広い調整機能を提供します。

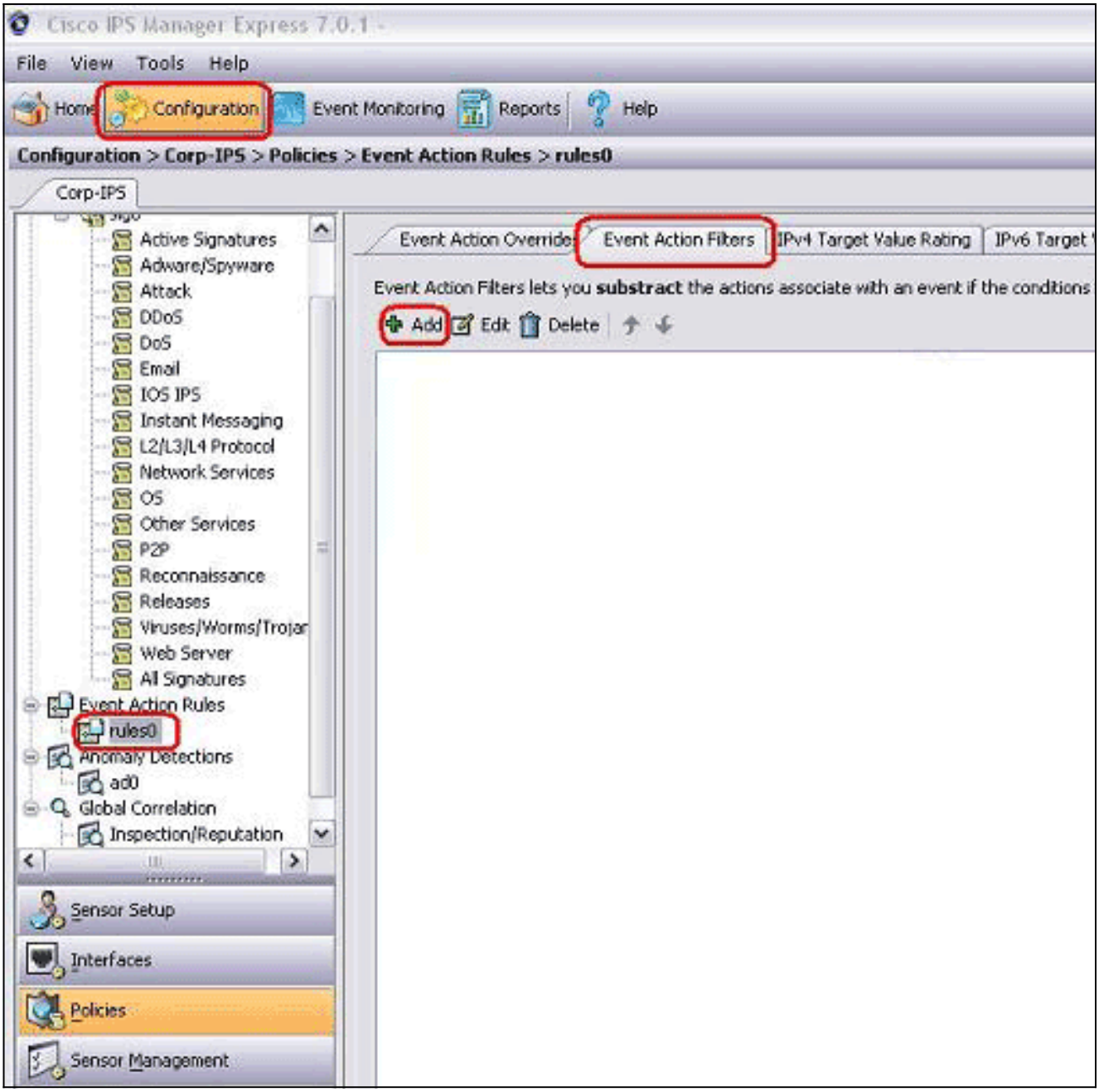
Cisco Secure IPS はメカニズムを除きます

Cisco Secure IPS は特定のホストかネットワーク アドレスからまたはに特定のシグニチャを除くために機能を提供します。 除外されたシグニチャは、このメカニズムによって明確に除外されたホストやネットワークからトリガされた場合にはアラーム アイコンやログ レコードを生成しません。 たとえば、ネットワーク管理ステーションはエコー シグニチャ（2100）シグニチャ ID が付いている ICMP ネットワーク スイープを引き起こす ping スイープの実行によってネットワーク開発を行うかもしれません。 シグニチャを除く場合、ネットワーク開発プロセスが動作する度にアラームを分析し、それを削除する必要がありません。

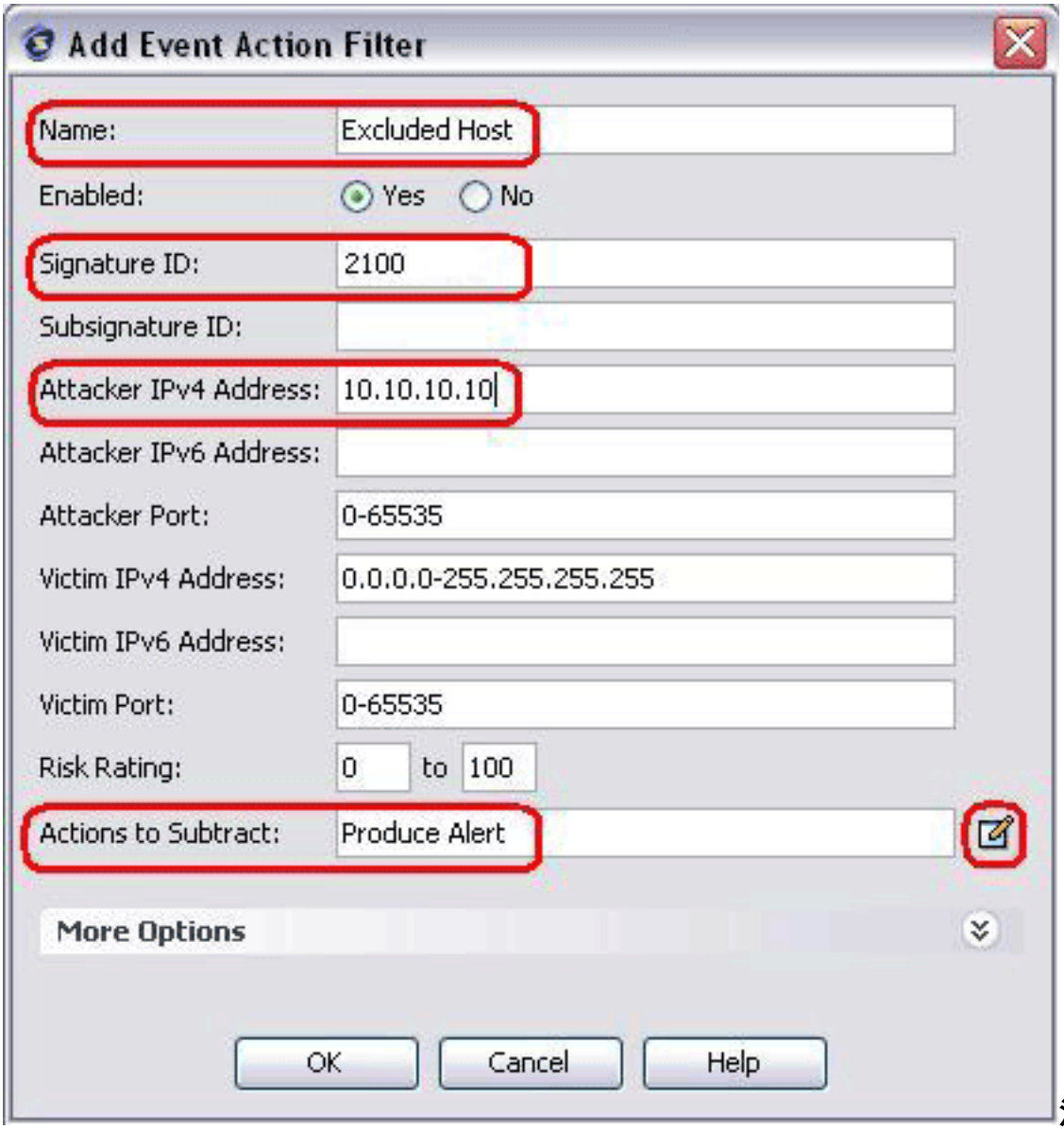
ホストの除外

特定のシグニチャ アラームの生成から特定のホスト（ソース IP アドレス）を除外するためにこれらのステップを完了して下さい:

1. **> Corp IPS > ポリシー > 検知時のアクション支配し > rules0**、クリックします**検知時のアクション Filters タブを**『Configuration』 を選択 して下さい。



2. [Add] をクリックします。
3. 適切なフィールドで引くフィルタ名前、シグニチャ ID、攻撃者の IPv4 アドレスおよび操作を入力し次に『OK』 をクリック して下さい。



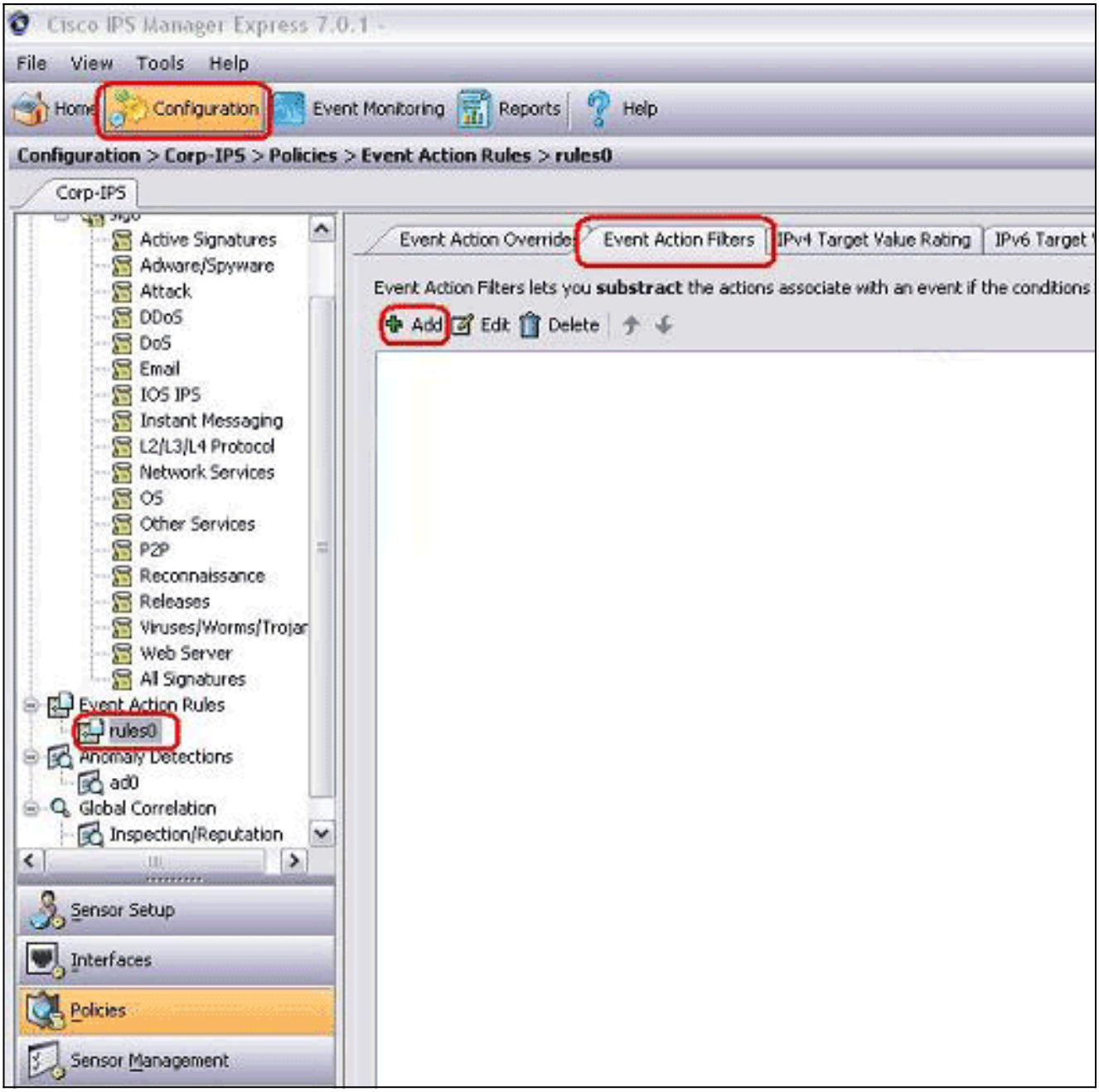
注: 異なるネットワークから複数の IP アドレスを除外する必要がある場合デリミタとしてカンマを使用できます。 ただしカンマを使用したら、カンマの後で後ろ の スペースを避けて下さい; さもなければ、エラーを受け取るかもしれません。**注:** さらに、事象変数タブで定義される変数を使用できます。 これらの変数は同じ値が複数のイベント アクション フィルターで繰り返す必要があるとき役立ちます。 変数にプレフィクスとしてドル記号 ($) を使用して下さい。 変数はこれらの形式の 1 つである場合もあります:完全な IP アドレス; たとえば、10.77.23.23。IP アドレスの範囲; たとえば、10.9.2.10-10.9.2.155。IP アドレスの範囲のセット; たとえば、172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.11。

ネットワークの除外

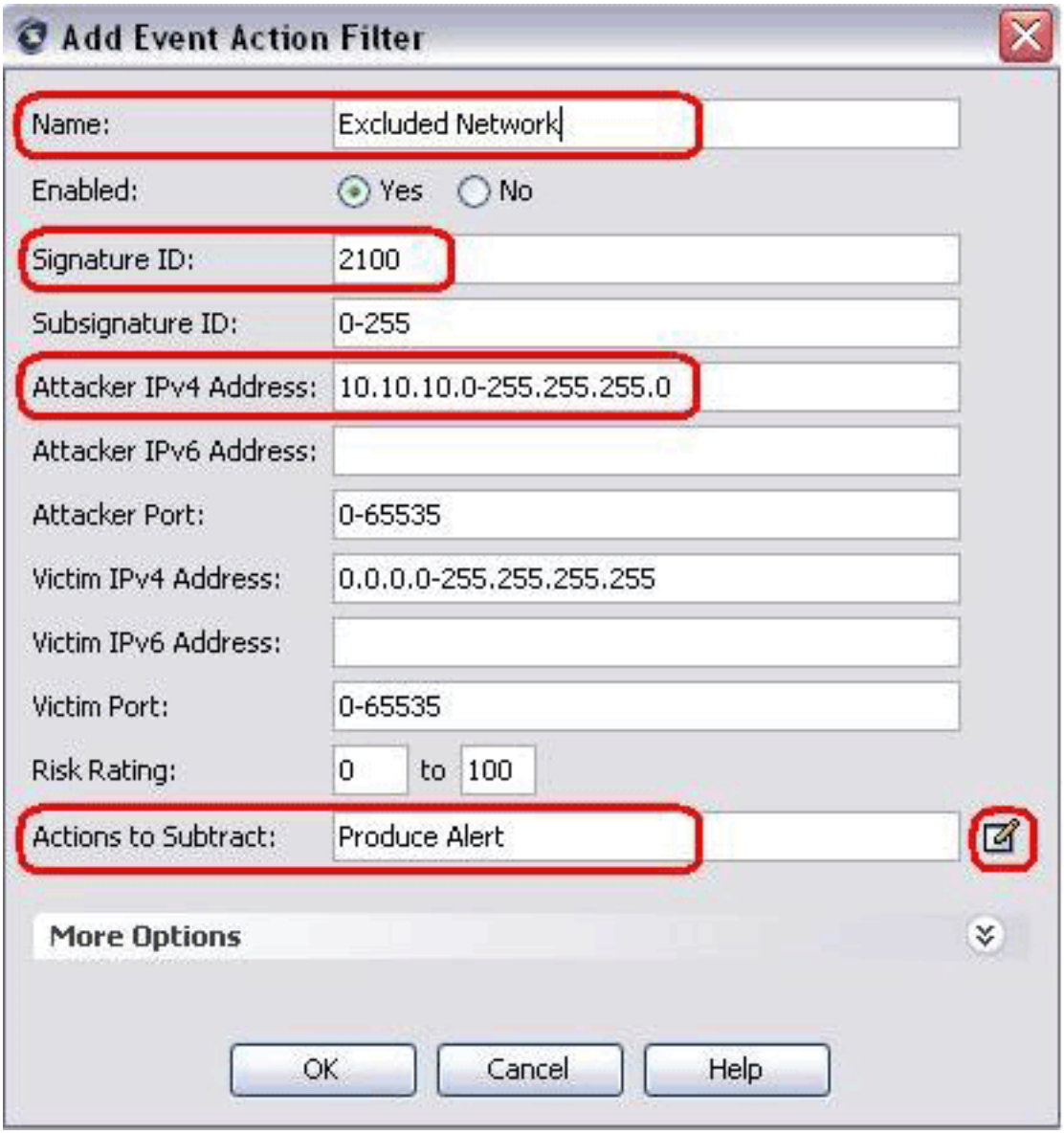
検知時のアクション フィルタはまた送信元/宛先 ネットワーク アドレスに基づいてアラームを始動させるために特定のシグニチャを除きます。

特定のシグニチャ アラームの生成からネットワークを除外するためにこれらのステップを完了して下さい:

1. **検知時のアクション Filters タブを**クリックして下さい。



2. [Add] をクリックします。
3. 適切なフィールドで引くフィルタ名前、シグニチャ ID、サブネット マスクのネットワーク アドレス、および操作を入力し次に『OK』 をクリック して下さい。



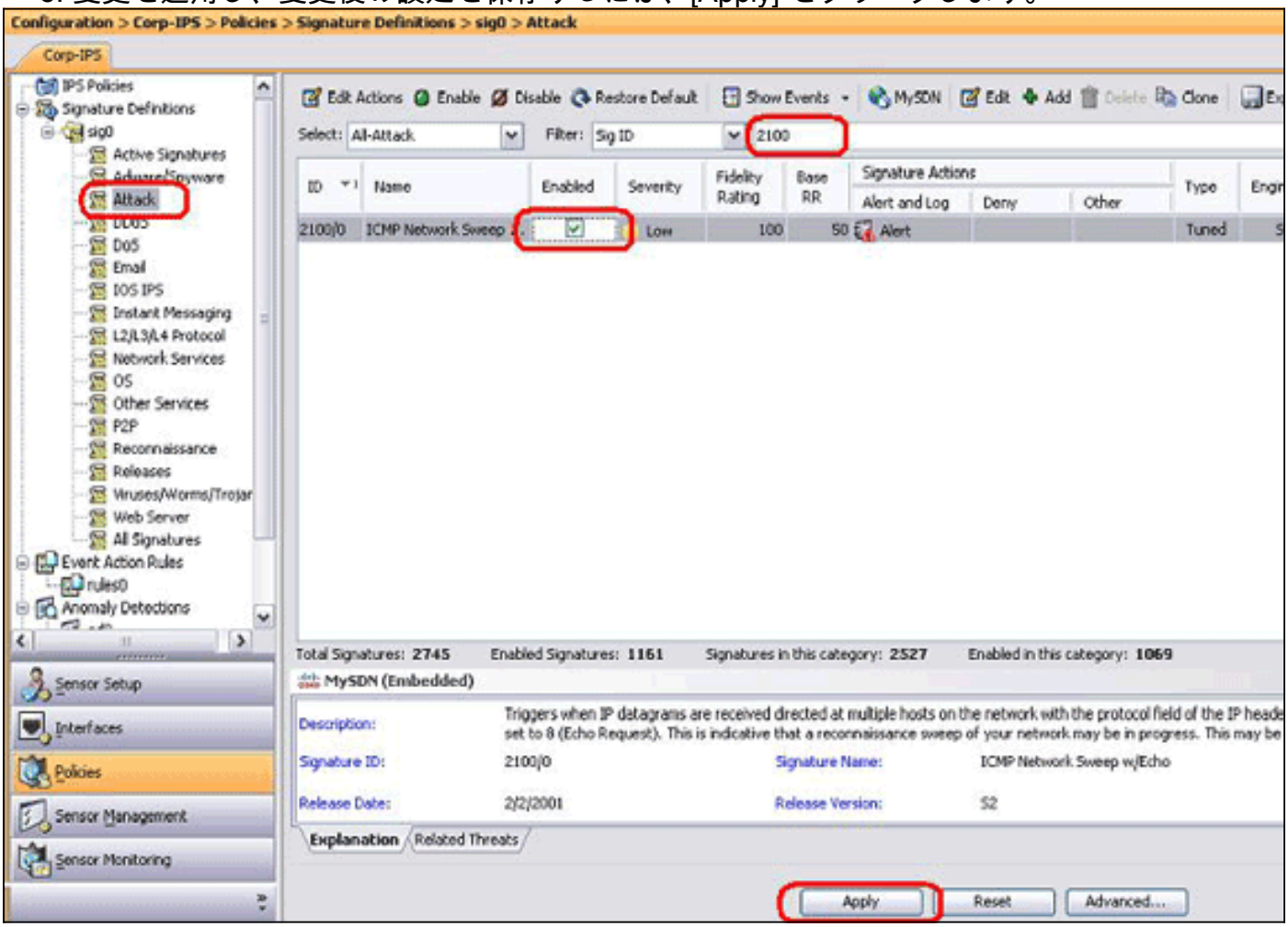
グローバルに シグニチャをディセーブルにして下さい

いつでも警告からのシグニチャをディセーブルにしたいと思うかもしれません。 、有効に なるためにディセーブルにし、シグニチャを終了させますために、これらのステップを完了して下さい:

1. 管理者またはオペレータ特権のアカウントを使用して IME へのログイン。
2. **>sensor_name > ポリシー > シグニチャ 定義 > sig0 > すべてのシグニチャ** 『Configuration』 を選択 して下さい。
3. シグニチャを見つけるために、フィルタ ドロップダウン リストからソート オプションを選択して下さい。 たとえば ICMP ネットワーク スイープ シグニチャを捜したら、sig0 の下で『All Signatures』 を選択 しか、そしてシグニチャ ID によって検索するか、または指名して下さい。 sig0 ペインは分類規準を満たしたそれらのシグニチャだけリフレッシュし、表示する。
4. 既存のシグニチャをディセーブルにするために有効に するか、または、シグニチャを選択し、これらのステップを完了して下さい:シグニチャのステータスを判別するために Enabled カラムを表示して下さい。 有効に なる シグニチャにチェックされるチェックボックスがあります。無効であるシグニチャを有効に するために、**Enabled チェックボックスを**チェックして下さい。有効に なる シグニチャをディセーブルにするために、**Enabled チェックボックスの**チェックを外して下さい。1つ以上のシグニチャを終了させますために、シグニチャ

を選択し、右クリックし、それから**ステータスをに > 終了させまされる** 『Change』 をクリック して下さい。

5. 変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。



関連情報

- Cisco Secure IDS ディレクターのための販売の終わり
- Cisco Secure Intrusion Detection のサポートページ
- テクニカルサポートとドキュメント - Cisco Systems