Intrusion Prevention System Device Manager 5.1 - トーン シグニチャ

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[背景説明](#)
[調整シグニチャ](#)
[ステップバイステップ手順](#)
[関連情報](#)

概要

侵入防御システム（IPS）5.1 には 1000 を超える組み込みのデフォルト シグニチャが含まれています。 組み込みのシグニチャ リストにあるシグニチャの名前を変更したり、削除したりはできませんが、センシング エンジンから削除するためにシグニチャをリタイアすることができます。 リタイアしたシグニチャは後でアクティブにできます。 ただし、このプロセスでは、センシング エンジンがそれらの設定を再構築する必要があります。これには時間がかかり、トラフィックの処理が遅延することがあります。 複数のシグニチャ パラメータを調整すると、組み込みのシグニチャを調整できます。 変更された組み込みのシグニチャは、調整されたシグニチャと呼ばれます。

この資料は使用するようにステップを IPS Device Manager （IDM）を使用してシグニチャを調整するために説明したものです。 IDM は Webベース、センサーを設定･管理することを可能にする Javaアプリケーションです。 IDM のための Webサーバはセンサーに常駐します。 Internet Explorer、Netscape、または Mozilla Webブラウザによってそれにアクセスできます。

注: *カスタム シグニチャ*と呼ばれるシグニチャを作成できます。 カスタム シグニチャ ID は 60000 で始まります。 UDP 接続のストリングの一致し、ネットワーク フラッドのトラッキングし、スキャンのような複数の事柄のためにそれらを、設定できます。 各シグニチャは特別に監視されるトラフィック の 種類のために設計されているシグニチャ エンジンを使用して作成されます。

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 Cisco 侵入防御システム デバイスマネージャ 5.x に基づいています。

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。

背景説明

特定のシグニチャのためのネットワークトラフィックをモニタするためにセンサーを設定するためにシグニチャを有効に して下さい。 デフォルトで、最も重要なシグニチャはシグニチャアップデートをインストールするとき有効に なります。 攻撃が検出するときイネーブルになったシグニチャと一致する、センサーのイベント ストアで保存されるセンサーはアラートを生成します。 アラート、また他のイベントは Webベース クライアントによってイベント ストアから、取得することができます。 デフォルトで、センサーはすべての情報アラートをまたはより高く記録 します。

いくつかのシグニチャにサブ シグニチャがあります。 すなわち、シグニチャは下位範疇に分けられます。 サブ シグニチャを設定するとき、行う 1 つのサブ シグニチャのパラメータへの変更をそのサブ シグニチャにだけ適用します。 たとえば、シグニチャ 3050 サブ シグニチャ 1 を編集し、重大度を変更すれば、重大度変更はサブ シグニチャ 1 だけとない 3050 2、3050 に 3、および 3050 4.適用します。

調整シグニチャ

+ アイコンはより多くのオプションがこのパラメータに利用できることを示します。 セクションを拡張し、残りのパラメータを表示するために **+ アイコンを**クリックして下さい。

グリーン アイコンはパラメータが現在 デフォルト値を使用することを示します。 パラメータ フィールドをアクティブにする従って値を編集できるレッドにそれを変更するためにグリーン アイコンをクリックして下さい。

ステップバイステップ手順

シグニチャを調整する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 IDM へのログイン。
2. **> シグニチャ 定義 > シグニチャ 設定** 『Configuration』 を選択 して下さい。シグニチャ 設定 ペインは現われます。
3. シグニチャを見つけるために、リスト**によって選り抜き**からソート オプションを選択して下さい。次にたとえば UDP フラッド シグニチャを捜したら、**L2/L3/L4 プロトコル**および **UDP フラッドを**選択して下さい。シグニチャ 設定 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調整するために、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:編集シグニチャ ダイアログボックスを開くために『Edit』 をクリック して下さい。パラメータ値を検討し、調整したいと思うあらゆるパラメータの値を変更して下さい。**注:** 1 つの検知時のアクションより『More』 を選択 するために、**Ctrl** キーを維持して下さい。ステータスの下で、シグニチャを有効に するために『Yes』 を選択 して下さい。**注:** シグニチャはセンサーがシグニチャによってアクティブに 規定 された 攻撃を検出することができるように有効に する必要があります。ステータスの下で、このシグニチャが終了させまされる場合規定 して下さい。 シグニチャをアクティブにするために『No』 をクリック して下さい。 これはエンジンにシグニチャを置きます。**注:** シグニチャはセンサーがシグニチャによってアクティブに 規定 された 攻撃を検出することができるようにアクティブにする必要があります。**注:** 変更を取消し、編集シグニチャ ダイアログボックスを閉じるために『Cancel』 をクリック して下さい。[OK] をクリックします。編集されたシグニチャは調整されるに型セットのリストに今現われます。**注:** 変更を取消したいと思う場合『Reset』 をクリック して下さい。

5. 変更を加え、修正された設定を保存するために『Apply』 をクリック して下さい。

関連情報

- Cisco Intrusion Prevention System
- テクニカルサポートとドキュメント - Cisco Systems