IPS 6.X： IDM を使用した特定イベントのサマリーのイネーブル化またはディセーブル化

目次

概要

このドキュメントでは、IPS Device Manager（IDM）を使用して、侵入防御システム（IPS）ソフトウェア バージョン 6.x の特定のイベントのサマリーをイネーブル/ディセーブルにする方法を説明します。

注: アクセス リストは、IDM などの管理ソフトウェアと IEV（IDS イベント ビューア）がインストールされ、正常に動作しているホストやネットワークからのアクセスを許可するために、IPS アプライアンス内に設定する必要があります。 詳細については、『コマンドライン インターフェイス 5.0 を使用したシスコ侵入防御システム センサーの設定』の「アクセス リストの変更」の項を参照してください。

前提条件

要件

このドキュメントは、IPS 6.x がインストールされ、正常に機能していることを前提としています。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 6.0(2)E1 が稼働する Cisco 4200 シリーズ IPS センサーに基づくものです。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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。

IDM を使用した特定イベントのサマリーのイネーブルまたはディセーブル

明確な理解が得られるよう、この項では次のサマリのイネーブルとディセーブルの例を示します。**Signature ID： 5748**。

IDM の設定

次の手順を実行します。

1. IDM を起動します。
2. [Home] をクリックして、IDM のホームページを表示します。 このページには、デバイス情報が表示されます。
3. [Configuration] > [Policies] > [Signature Definitions] > [sig0] > [Signature Configuration] > [Select By: Sig ID] の順に選択して、センサー内で使用できるすべての署名を表示します。
4. [Select By] ドロップダウン メニューから [Sig ID] を選択し、Sig ID に「5748」を入力すると、特定の署名が検索されます。
5. 署名を編集するには、[Edit] をクリックします。
6. [Edit Signature] ウィンドウで、[Signature Definition] > [Alert Frequency] > [Summary Mode] の順に選択し、[Summary Mode] ドロップダウン メニューで、アクションを [Summarize] から [Fire all] に変更します。
7. [Specify Global Summary Threshold] が [No] に設定されていることを確認します。

関連情報

- Cisco Intrusion Prevention System に関するサポート ページ
- Cisco IPS Device Manager に関するサポート ページ
- IOS IPS の概要
- テクニカル サポートとドキュメント – Cisco Systems