FireSIGHT システムでの規則のプロファイリング手順

内容

概要

Firepower アプライアンスまたは NGIPS 仮想アプライアンスがオーバーサブスクライブになっている場合は、システムの速度を低下させているデバイスのコンポーネントを特定するために、いくつかの追加データを収集する必要があります。規則のプロファイリングにより、FireSIGHT システムは、最も CPU サイクルを使用している検出エンジンの規則とサブシステムに関する詳細なデータを生成できるようになります。この記事では、FireSIGHT アプライアンスおよび NGIPS 仮想アプライアンスで規則のプロファイリングを実行する方法の手順を示します。

前提条件

要件

FirePOWERアプライアンスと仮想アプライアンスモデル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いています。

- FirePOWER 7000シリーズアプライアンス、8000シリーズアプライアンス、およびNGIPS仮想アプライアンス
- ソフトウェア バージョン 5.2 以降

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ました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

警告：ルール・プロファイリング・コマンドを実行すると、ネットワークのパフォーマンスに影響が及ぶ場合があります。したがって、このコマンドは、シスコテクニカルサポートがルールプロファイルデータを要求した場合にのみ実行してください。

ルール・プロファイリングの実行手順

ステップ 1：管理対象デバイスのCLIにアクセスします。

ステップ 2：次のルールプロファイルコマンドを一定時間実行します。時間は15 ~ 120分の間である必要があります。次の例では、スクリプトは15分間実行されます。

```
> system support run-rule-profiling 15
```

ステップ 3：コマンドの実行を確認します。**y**と入力し、Enterキーを押します。

警告： rule profilingコマンドは、検出機能に影響を与える可能性のある検出エンジンを再起動し、CPU使用率を高めます。

```
> system support run-rule-profiling 15

You are about to profile
 DE    Primary Detection Engine (94854a60-cb17-11e3-a2f5-8de07680f9f3)
 Time  15 minutes

WARNING!!  Detection Engine will be restarted.
Intrusion Detection / Prevention will be affected

Please confirm by entering 'y': y
```

実行を確認した後、ルールプロファイリングが開始されます。プロファイリングを完了する時間は0分までカウントされます。

```
Restarting DE for profiling...done
Profiling for 15 more minutes...
```

完了すると、シェルプロンプトが戻ります。

```
Restarting DE for profiling...done
Profiling...done
Restarting DE with original configuration...in progress
>
```

ステップ 4：rule profilingコマンドは、.tgzファイルを生成します。このファイルは、シェルで次のコマンドを実行することで検索できます。

```
> system file list
May 12 15:53 99364308 profiling.94854a60-cb17-11e3-a2f5-8de07680f9f3.1399909945.tgz
```

ステップ 5：詳細な分析のために、シスコテクニカルサポートにこのファイルを提供してください。