Snort3ルールについて

内容

[概要](#)
[前提条件](#)
[要件](#)
[ライセンス](#)
[使用するコンポーネント](#)
[背景説明](#)
[Snort3ルール](#)
[ルールアクション](#)
[ルールの分析](#)
[ルール機能](#)
[例](#)
[httpサービスヘッダーとスティッキバッファhttp_uriの例](#)
[ファイルサービスヘッダーの例](#)
[関連するリンク](#)

概要

このドキュメントでは、 **Snort3** シスコのエンジン **Secure Firewall Threat Defense (FTD).**

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 『シスコ **Secure Firewall Threat Defense (FTD)**
- **Intrusion Prevention System (IPS)**
- **Snort2** 構文

ライセンス

特定のライセンス要件はありません。基本ライセンスで十分であり、ここに示す機能はFTD内のSnortエンジンとSnort3オープンソースバージョンに含まれています。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 『シスコ **Secure Firewall Threat Defense (FTD),**シスコ **Secure Firewall Management Center (FMC)** バージョン 7.0以降 **Snort3.**

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Snort Cisco IPSエンジンは、リアルタイムトラフィック分析とパケットロギングに対応しています。

Snort プロトコル分析、コンテンツ検索、および攻撃の検出を実行できます。

Snort3 は、Snort2 IPSの更新バージョンで、パフォーマンス、検出、スケーラビリティ、および使いやすさを向上させる新しいソフトウェアアーキテクチャを備えています。

Snort3ルール

このLUA形式を使用して、 Snort3 読み取り、書き込み、検証が容易なルール。

ルールアクション

この新しいバージョンでは、ルールのアクションが変更されます。新しい定義は次のとおりです。

- Pass：パケットに対する後続のルールの評価を停止します。
- Alert：イベントのみを生成
- Block：パケットをドロップし、残りのセッションをブロックします。
- Drop：パケットのみをドロップする
- Rewrite:replacesオプションを使用する場合は必須です。
- React: HTMLブロック応答ページを送信します。
- Reject:TCP RSTまたはICMP到達不能を挿入します。

ルールの分析

解剖学的構造は以下の通りである：

ルールヘッダーには、アクション、プロトコル、送信元と宛先のネットワーク、およびポートが含まれます。

イン Snort3ルールヘッダーは次のいずれかのオプションになります。

- サービスルールヘッダー

```
<iline" lang="lua">alert http ( msg:"Alert HTTP rule"; flow:to_client,established;
content:"evil", nocase; sid:1000001; )
```

- ファイルルールヘッダー

```
alert file ( msg: “Alert File example”; file_data; content:”malicious_stuff”; sid:1000006; )
```

- 従来のルールヘッダー

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"Alert HTTP rule";
flow:to_client,established; content:"evil", nocase; sid:1000001; )
```

ルール機能

新機能の一部を次に示します。

- 任意の空白（各オプションが独自の行に表示される）

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"Alert TCP rule";
flow:to_client,established; content:"evil", nocase; sid:1000000; )
```

- および の一貫した使用

```
content:"evil", offset 5, depth 4, nocase;
```

- ネットワークとポートはオプション

```
alert http ( Rule body )
```

- スティッキバッファを追加します（完全なリストではありません）。

```
http_uri http_raw_uri http_header http_raw_header http_trailer http_raw_trailer http_cookie
http_raw_cookie http_true_ip http_client_body http_raw_body http_method http_stat_code
http_stat_msg http_version http2_frama_header script_data raw_data
```

- Cスタイルのコメント

```
alert http ( msg:"Alert HTTP rule"; /* I can write a comment here */ ... )
```

- Remark(rem)キーワード

```
alert http ( msg:"Alert HTTP rule"; flow:to_client,established; rem:"Put comments in the rule
anywhere"; content:"evil", nocase; sid:1000001; )
```

- APPIDSキーワード

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any ( msg:"Alert on apps"; appids:"Google, Google
Drive"; content:"evil", nocase; sid:1000000; )
```

- sd_pattern：機密データのフィルタリング用
- Hyperflexテクノロジーを使用したRegexキーワード
- メタデータを置き換えるサービスキーワード

例

httpサービスヘッダーとスティッキバッファhttp_uriの例

タスク：単語を検出するルールを作成する malicious HTTP URI内に含まれます。

ソリューション：

```
alert http ( msg:"Snort 3 http_uri sticky buffer"; flow:to_server,established; http_uri;
content:"malicious", within 20; sid:1000010; )
```

ファイルサービスヘッダーの例

作業：PDFファイルを検出するルールを作成します。

ソリューション：

```
alert file ( msg:"PDF File Detected"; file_type: "PDF"; sid:1000008; )
```

関連するリンク

[SnortルールおよびIDSソフトウェアのダウンロード]

[Github]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。