コンテンツ セキュリティ アプライアンスに関する FAQ： Cisco コンテンツ セキュリティ アプライアンスでパケット キャプチャを実行するにはどうしますか。

目次

概要

この資料に Cisco 内容セキュリティ アプライアンス モデルのパケットキャプチャを行う方法を記述されています。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco E メール セキュリティ アプライアンス（ESA）
- Cisco Web セキュリティ アプライアンス（WSA）
- Cisco セキュリティ管理アプライアンス（SMA）
- AsyncOS

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 AsyncOS のすべてのバージョンで基礎です。

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。

Cisco コンテンツ セキュリティ アプライアンスでパケット キャプチャを実行するにはどうしますか。

GUI によってパケットキャプチャ（**tcpdump コマンド**）を行うためにこれらのステップを完了して下さい:

1. **助けるべき**ナビゲート**およびサポート >** GUI の**パケットキャプチャ**。
2. パケットキャプチャ設定を要求に応じて編集して下さいネットワーク インターフェイスのようなパケットキャプチャが動作する。 あらかじめ定義されたフィルタの 1 つを使用できますまたは Unix tcpdump コマンドによってサポートされるあらゆる構文の使用でカスタム フィルタを作成できます。
3. キャプチャを始めるために**キャプチャを**『Start』 をクリック して下さい。
4. キャプチャを終了するために**キャプチャを**『Stop』 をクリック して下さい。
5. パケットキャプチャをダウンロードして下さい。

CLI とパケットキャプチャ（**tcpdump コマンド**）を行うためにこれらのステップを完了して下さい:

1. CLI にこのコマンドを入力して下さい:

```
wsa.run> packetcapture

Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     (tcp port 80 or tcp port 3128)
```

2. 行いたいと思うオペレーションを選択して下さい:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. キャプチャ ファイルのための最大許容サイズを入力して下さい（MB で）:

```
[200]> 200

Do you want to stop the capture when the file size is reached? (If not, a new
 file will be started and the older capture data will be discarded.)

[N]> n

The following interfaces are configured:

1. Management

2. T1

3. T2
```

4. カンマで分かれるパケットをキャプチャ するため 1つ以上のインターフェイスの名前か数に入って下さい:

```
[1]> 1
```

5. キャプチャのために使用したいと思うフィルタを入力して下さい。 フィルタをクリアし、選択したインターフェイスのパケットすべてをキャプチャ するためにワード **オフを**入力して下さい。

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80


Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```

6. キャプチャを始めるために**開始**オペレーションを選択して下さい:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> start


Status: Capture in progress (Duration: 0s)

File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)


Current Settings:

 Max file size:      200 MB
```

```
 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```

7. キャプチャを終了するために**停止**オペレーションを選択して下さい:

```
- STOP - Stop packet capture.

- STATUS - Display current capture status.

- SETUP - Change packet capture settings.

[]> stop


Status: No capture running (Capture stopped by user)


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     host 10.10.10.10 && port 80
```