

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

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[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。](#)

概要

このドキュメントでは、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方法について説明します。

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 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. 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ください:

[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クリアを入力して下さい。

[(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**開始する** 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