パケットキャプチャ手順 on Cisco Firepower デバイス

目次

概要

この文書に Firepower デバイスのネットワーク インターフェイスによって見られるパケットをキャプチャするために **tcpdump コマンドを**使用する方法を記述されています。 それはバークレーパケットフィルタ（BPF）構文を使用します。

前提条件

要件

Cisco は Cisco Firepower デバイスおよび仮想デバイス モデルのナレッジがあることを推奨します。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

> **警告**： 生産システムの **tcpdump** 実行する場合、ネットワークパフォーマンスに影響を与えることができます。

パケットをキャプチャ するステップ

Firepower デバイスの CLI へのログイン。

バージョン 6.1 および それ 以降では、キャプチャ **トラフィックを**入力して下さい。 次に例を示します。

```
> capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```
バージョン 6.0.x.x および それ 以前では、**システム 支援キャプチャ トラフィックを**入力して下さい。 次に例を示します。

```
> system support capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```
選択をした後、オプションのためにプロンプト表示されます:

```
> system support capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```
パケットからの十分なデータをキャプチャ するために、snaplength を正しく設定するために- s オプションを使用することは必要です。 snaplength は 1518 にデフォルトで設定される、インターフェイス一定設定の設定された最大伝送ユニット （MTU）値と一致する値に設定する必要があります。

> **警告**： 画面へのトラフィックをキャプチャすることがシステムおよびネットワークのパフォーマンスを低下できるので Cisco は使用すること- tcpdump で w <filename> オプションを推奨します。 それはファイルにパケットをキャプチャ します。 なしでコマンドを実行すれば- w オプションは終了するために、**Ctrl-C キー** 組み合せを押します。

- w <filename> オプションの例:

```
-w capture.pcap -s 1518
```

> **注意**： パケットキャプチャ（pcap）ファイル名を指定するときパス要素を使用しないで下さい。 アプライアンスで作成されるべき pcap ファイル名だけ指定して下さい。

パケットの限られた数をキャプチャ すればことは好ましい場合キャプチャ するためにパケットの数を規定 するために- c <packets> フラグを使用できます。 たとえば、5000 のパケットを丁度キャプチャ するため:

```
-w capture.pcap -s 1518 -c 5000
```
さらに、BPF フィルタはコマンドの終わりにどのパケットがキャプチャされるか制限するために追加することができます。 たとえば、パケットキャプチャを 192.0.2.1 のソースまたは宛先 IP アドレスの 5000 のパケットに制限するために、これらのオプションを使用する可能性があります:

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```
タグ付けされるバーチャルLAN （VLAN）であるトラフィックをキャプチャ するとき BPF 構文

の VLAN を規定 して下さい。 さもなければ、pcap は VLAN タグ付きパケットがのうちのどれも含まれていません。 たとえば、この例は 192.0.2.1 からタグ付けされる VLAN であるトラフィックにキャプチャを制限したものです:

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

トラフィックがタグ付けされる VLAN である場合不確実ならタグ付けされる VLAN あり、ない 192.0.2.1 からのトラフィックをキャプチャ するためにこの構文は使用できます:

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

> **注:** 前例では、かっこは「」だけでなく、「VLAN に」適用するように必要です。 単一 引用符はシェルによってそれからかっこの可能性のある誤解を防ぐために必要とされます。

VLAN タグの仕様は BPF の他と一致するすべての VLANトラフィックをキャプチャ します。 ただし、仕様 VLAN タグをキャプチャ したいと思えば VLAN タグがそうのようにキャプチャ することを望む規定できます:

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

望ましいオプションを規定 した、『Enter』 を押す後、tcpdump はトラフィックをキャプチャ し始めます。

> **ヒント**： - c オプションは使用されませんでしたり、キャプチャを停止するために **Ctrl-C キー** 組み合せを押します。

キャプチャを停止すれば、確認を受け取ります。 次に、例を示します。

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -w capture.pcap -s 1518 -c 5000 host 192.0.2.1
Cleaning up.
Done.
```

Pcap ファイルをコピーして下さい

pcap ファイルを FirePOWER アプライアンスから受信 SSH 接続を許可する別のシステムにコピーするために、このコマンドを使用して下さい:

```
> system file secure-copy hostname username destination_directory pcap_file
```

『Enter』 を押した後、リモート システムへのパスワードのためにプロンプト表示されます。 ファイルはネットワークを渡ってコピーされます。

> **注:** この例では、**ホスト名は**ターゲット リモートホストの名前か IP アドレスを示します、**ユーザ名は**リモートホストのユーザの名前を規定 します、**destination_directory** リモートホストの宛先パスを規定 し、**pcap_file** 転送のためのローカル pcap ファイルを規定 します。