firepowerデバイスでのパケットキャプチャ手順の使用

内容

はじめに

このドキュメントでは、Firepower デバイスのネットワーク インターフェイスで確認さ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について説明します。

前提条件

要件

シスコのFirepowerデバイスと仮想デバイスの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内容は、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。 Berkeley Packet Filter(BPF)構文を使用します。

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、クリアな（デフォルト）設定で作業を開始しています。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。

警告：実稼働システムでtcpdump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を与える可能性があります。

パケットをキャプチャする手順

firepowerデバイスのCLIにログインします。

バージョン6.1以降では、capture-trafficと入力します。たとえば、

<#root>

```
> 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以前では、system support capture-trafficと入力します。たとえば、

<#root>

```
> system support capture-traffic
```

```
Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set  (Interfaces s2p1, s2p2)
```

選択を行うと、オプションの入力を求めるプロンプトが表示されます。

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

パケットから十分なデータをキャプチャするには、-sオプションを使用してsnaplengthを正しく設定する必要があります。snaplengthは、インターフェイスセット設定の設定済みの最大伝送ユニット(MTU)値と一致する値に設定できます。デフォルトは1518です。

⚠ 警告：画面に表示されるトラフィックをキャプチャすると、システムおよびネットワークのパフォーマンスが低下する可能性があります。-w <filename>オプションとtcpdumpコマンドを使用することを推奨します。パケットをファイルにキャプチャする-wオプションを付けずにコマンドを実行する場合は、Ctrl+Cキーを押して終了します。

-w <filename>オプションの例：

<#root>

```
-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には、パス要素を使用しないで

⚠ ください。アプライアンスで作成するpcapファイル名だけを指定する必要があります。

キャプチャするパケットの数を制限したい場合は、-c <packets>フラグを使用してキャプチャするパケットの数を指定できます。たとえば、5000パケットを正確にキャプチャするには、次のようにします。

<#root>

```
-w capture.pcap -s 1518 -c 5000
```

また、キャプチャされるパケットを制限するために、コマンドの最後にBPFフィルタを追加できます。たとえば、送信元IPアドレスまたは宛先IPアドレスが192.0.2.1のパケットを5000個に制限するには、次のオプションを使用できます。

<#root>

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

仮想LAN(VLAN)タグ付きのトラフィックをキャプチャする場合は、BPF構文でVLANを指定する必要があります。それ以外の場合、pcapにはVLANタグ付きパケットは含まれません。たとえば、次の例では、キャプチャを192.0.2.1からVLANタグ付けされたトラフィックに制限しています。

<#root>

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

トラフィックにVLANタグが付いているかどうかわからない場合は、次の構文を使用して192.0.2.1からのトラフィックをキャプチャできます。このトラフィックはVLANタグが付いていますが、付いていません。

<#root>

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

✎ 注：前述の例では、「or」が「vlan」のみに適用されないよう、カッコが必要です。シェルによって括弧が誤って解釈されることを防ぐために、一重引用符が必要になります。

VLANタグの指定は、BPFの他の部分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、特定のVLANタグをキャプチャする場合は、キャプチャするVLANタグを次のように指

定できます。

<#root>

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

目的のオプションを指定してEnterキーを押すと、tcpdumpはトラフィックのキャプチャを開始します。


ヒント:-cオプションが使用されていない場合は、キャプチャを停止するためにCtrl-Cキーの組み合わせを押します。

キャプチャを停止すると、確認メッセージが表示されます。例：

<#root>

```
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ファイルのコピー

pcapファイルをFirepowerアプライアンスから、インバウンドSSH接続を受け入れる別のシステムにコピーするには、次のコマンドを使用します。

<#root>

> system file secure-copy hostname username destination_directory pcap_file

Enterキーを押すと、リモートシステムへのパスワードの入力を求められます。ファイルはネットワーク経由でコピーできます。


注意：この例では、hostnameはターゲット・リモート・ホストの名前またはIPアドレスを参照し、usernameはリモート・ホスト上のユーザー名を指定し、destination_directoryはリモート・ホスト上の宛先パスを指定し、pcap_fileは転送用のローカルpcapファイルを指定します。

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。