ESA パケット キャプチャ手順

目次

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス（ESA）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

Cisco ESA について十分に理解しておくことをお勧めします。

使用するコンポーネント

この文書に記載する情報は、あらゆるバージョンの AsyncOS を実行する Cisco ESA に基づいています。

背景説明

IronPort カスタマー サポートに問題について問い合わせると、ESA の発信と着信のネットワーク状況について尋ねられることがあります。 アプライアンスは、アプライアンスが接続されているネットワーク上で送受信される TCP、IP、およびその他のパケットを傍受および表示できます。 パケット キャプチャを実行すると、ネットワーク設定をデバッグしたり、アプライアンスで送受

信されるネットワーク トラフィックを検証したりすることができます。

> **注:** このドキュメントでは、IronPort で保守やサポートが行われていないソフトウェアに言及します。 情報は、利便性のために無償で提供されています。 さらにサポートが必要な場合は、ソフトウェア ベンダーに連絡してください。

以前使用されていた **tcpdump** CLI コマンドは、AsyncOS バージョン 7.0 以降では新しい **packetcapture** コマンドに置き換えられたことに注意してください。 このコマンドは、**tcpdump コマンド**と同様の機能を提供し、GUI でも使用できます。

AsyncOS バージョン 6.x 以前を実行する場合は、このドキュメントの「**AsyncOS バージョン 6.x 以前でのパケット キャプチャ**」セクションで **tcpdump コマンド**を使用する手順を参照してください。 また、「**パケット キャプチャ フィルタ**」セクションで説明しているフィルタ オプションは、新しい **packetcapture** コマンドでも有効です。

AsyncOS バージョン 7.x 以降でのパケット キャプチャ

このセクションでは、AsyncOS バージョン 7.x 以降でのパケット キャプチャ プロセスについて説明します。

パケット キャプチャの開始または停止

GUI を使用してパケット キャプチャを開始するには、[Support and Help] メニューに移動し、[Packet Capture] を選択し、[Start Capture] をクリックします。 パケット キャプチャ プロセスを停止するには、[Stop Capture] をクリックします。

> **注:** GUI で開始されるキャプチャは次のセッションまで保持されます。

CLI を使用してパケット キャプチャを開始するには、**packetcapture > start** コマンドを入力します。 パケット キャプチャ プロセスを停止するには、**packetcapture > stop** コマンドを入力します。これにより ESA が、セッション終了時にパケット キャプチャを停止します。

パケット キャプチャの機能性

次に、パケット キャプチャを操作するために使用できる有用な情報をリストします。

- ESA は、キャプチャされたパケット アクティビティをファイルに保存し、そのファイルをローカルで保管します。 パケット キャプチャの最大ファイル サイズ、パケット キャプチャの実行時間、およびキャプチャを実行するネットワーク インターフェイスを設定できます。 また、フィルタを使用して、特定のポートからのトラフィックや特定のクライアントまたはサーバの IP アドレスからのトラフィックにパケット キャプチャを制限することもできます。

- GUI で [Support and Help] > [Packet Capture] を選択すると、ハード ドライブに保存されているパケット キャプチャ ファイルの完全なリストが表示されます。 パケット キャプチャを実行すると、[Packet Capture] ページが表示され、実行中のキャプチャのステータス (ファ

イル サイズや経過時間などの現在の統計情報）が表示されます。

- [Download File] ボタンをクリックすると、パケット キャプチャ ファイルをダウンロードできます。 問題のデバッグおよびトラブルシューティングを依頼するために、このファイルを IronPort カスタマー サポートに電子メールで転送できます。
- パケット キャプチャ ファイルを削除するには、1 つ以上のファイルを選択し、[Delete Selected Files] をクリックします。
- GUI を使用してパケット キャプチャ設定を編集するには、[Support and Help] メニューの [Packet Capture] を選択し、[Edit Settings] をクリックします。
- CLI を使用してパケット キャプチャ設定を編集するには、**packetcapture > setup** コマンドを入力します。

注: GUI では、GUI で開始されるパケット キャプチャのみが表示され、CLI で開始されるパケット キャプチャは表示されません。 同様に、CLI では、CLI で開始される現在のパケット キャプチャのステータスのみが表示されます。 同時に 1 つのキャプチャしか実行できません。

ヒント： パケット キャプチャのオプションやフィルタの設定の詳細については、このドキュメントの「**パケット キャプチャ フィルタ**」セクションを参照してください。 GUI から AsyncOS オンライン ヘルプにアクセスするには、[Help and Support] > [Online Help] > [Index] > [P] > [Packet Capture] を選択します。

AsyncOS バージョン 6.x 以前でのパケット キャプチャ

このセクションでは、AsyncOS バージョン 6.x 以前でのパケット キャプチャ プロセスについて説明します。

パケット キャプチャの開始または停止

tcpdump コマンドを使用すると、ESA が接続されているネットワーク上で送受信される TCP/IP およびその他のパケットをキャプチャできます。

パケット キャプチャを開始または停止するには、次の手順を実行してください:

1. ESA の CLI で **diagnostic > network > tcpdump** コマンドを入力します。 次に出力例を示します。

```
example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
```

```
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> tcpdump

- START - Start packet capture
- STOP - Stop packet capture
- STATUS - Status capture
- FILTER - Set packet capture filter
- INTERFACE - Set packet capture interface
- CLEAR - Remove previous packet captures
[]>
```

2. インターフェイス (Data 1、Data 2、または Management) とフィルタを設定します。

   注: フィルタは Unix tcpdump コマンドと同じ形式を使用します。
3. キャプチャを開始するには **START** を選択し、終了するには **STOP** を選択します。

   注: キャプチャの進行中には、tcpdump メニューを終了しないでください。 2 つ目の CLI ウィンドウを使用すると、他のコマンドを実行できます。 キャプチャ プロセスが完了したら、ローカル デスクトップからセキュア コピー (SCP) またはファイル転送プロトコル (FTP) を使用して、Diagnostic という名前のディレクトリからファイルをダウンロードする必要があります (詳細については、「**パケット キャプチャ フィルタ**」セクションを参照してください)。 ファイルはパケット キャプチャ (PCAP) の形式を使用します。これは、Ethereal や Wireshark などのプログラムで確認できます。

パケットキャプチャフィルタ

CLI コマンド **Diagnostic > NET** では、標準 tcpdump フィルタ構文を使用します。 このセクションでは、tcpdump キャプチャ ファイルについて説明するとともに、例をいくつか紹介します。

使用される標準フィルタは次のとおりです。

- **ip -** すべての IP プロトコル トラフィックのフィルタ
- **tcp -** すべての TCP プロトコル トラフィックのフィルタ
- **ip host** - 特定の IP アドレス送信元または宛先のフィルタ

次に、実際に使用するフィルタの例を示します。

- **ip host 10.1.1.1** - このフィルタは、送信元または宛先として 10.1.1.1 を含むトラフィックをキャプチャします。
- **ip host 10.1.1.1 または ip host 10.1.1.2** - このフィルタは、送信元または宛先として 10.1.1.1 または 10.1.1.2 を含むトラフィックをキャプチャします。

キャプチャ ファイルを取得するには、**var > log > diagnostic** または **data > pub > diagnostic** を選択し、診断ディレクトリに移動します。

注: このコマンドを使用すると、ESA のディスク スペースがいっぱいになることがあり、パフォーマンス低下を引き起こす可能性があります。 このコマンドは、Cisco IronPort カスタマー サポート エンジニアのサポート下で使用することをお勧めします。