目次

概要

この資料に Cisco E メール セキュリティ アプライアンス (ESA) 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

Cisco は Cisco ESA 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

AsyncOS のバージョンを実行するこの文書に記載されている情報は Cisco ESA に基づいています。

背景説明

問題が付いている IronPort カスタマー サポートに連絡するとき、ESA の送信および受信 ネットワークアクティビティに把握を提供するように頼まれるかもしれません。 アプライアンス TCP を、IP 代行受信し、表示する機能をおよびアプライアンスが接続されるネットワークに送信されるか、または受信される他のパケットは提供します。 アプライアンスに達するか、または出て行くネットワークトラフィックを確認するためにネットワーク セットアップをデバッグするためにパケットキャプチャを実行したいと思い。

注 この資料はソフトウェアを参照します IronPort によって維持されないし、サポートされ

ない。 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。

以前に使用された **tcpdump** CLI コマンドが AsyncOS バージョン 7.0 および それ 以降の新しい **packetcapture** コマンドで取り替えられることに注意することは重要です。 このコマンドは **tcpdump コマンド**と同じような機能性を提供したもので GUI のまた利用可能です。

AsyncOS バージョン 6.x または それ以前を実行する場合、この資料の **AsyncOS バージョン 6.x および それ 以前** セクション**のパケットキャプチャ**で **tcpdump コマンドを**使用する方法に関する指示を参照して下さい。 また、**パケットキャプチャ フィルター** セクションに説明があるフィルタオプションは新しい **packetcapture** コマンドのために同様に有効です。

AsyncOS バージョン 7.x および それ 以降のパケットキャプチャ

このセクションは AsyncOS バージョン 7.x および それ 以降のパケットキャプチャ プロセスを説明します。

パケットキャプチャを開始するか、または停止して下さい

GUI のパケットキャプチャを、ナビゲート サポートに開始するためにおよび Help メニューは、**パケットキャプチャを**選択し、次に**キャプチャを**『Start』 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ために、**キャプチャを**『Stop』 をクリック して下さい。

注 GUI で始めるキャプチャはセッションの間で維持されます。

CLI のパケットキャプチャを開始するために、**packetcapture > start コマンドを**入力して下さい。 パケットキャプチャ プロセスを停止するために、**packetcapture > 停止**コマンドを入力すれば、セッションが終了するとき ESA はパケットキャプチャを停止します。

パケットキャプチャ 機能性

パケットキャプチャを処理するために使用できる有用 な 情報のリストはここにあります:

- ESA はファイルにキャプチャされるパケット アクティビティを保存し、ファイルをローカルで保存します。 最大 パケット キャプチャ ファイル サイズを設定できますどののためのネットワーク インターフェイスをでキャプチャが実行するか時間いっぱいがパケットキャプチャ動作し。 またか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特定のポートを通してトラフィックにパケットキャプチャを制限するためにフィルタを使用できます。
- **ヘルプ >** GUI からの**パケットキャプチャはサポートするために**ハード ドライブで保存されるパケットキャプチャ ファイルの完全なリストを表示するためにナビゲート し。 パケットキャプチャが動作するとき、パケットキャプチャ ページはファイルサイズのような現在の統計情報と、進行中のキャプチャのステータスを表示する、時間は経過しました。

- パケットキャプチャ ファイルをダウンロードするために**ダウンロード File ボタンを**クリックして下さい。 IronPort カスタマー サポートに電子メールで問題をデバッグしてトラブルシューティングを行うためにそれを転送できます。

- パケットキャプチャ ファイルを削除するために、1つ以上のファイルを選択し、**選択されたファイルを**『Delete』 をクリック して下さい。

- GUI のパケットキャプチャ設定を編集するために、**パケットキャプチャを**サポートおよび Help メニューから選択し、『Edit Settings』 をクリック して下さい。

- CLI のパケットキャプチャ設定を編集するために、**packetcapture > setup コマンドを**入力して下さい。

  注 GUI は GUI で始めるパケットキャプチャだけを、CLI から始めるそれら表示する。 同様に、CLI は CLI で始めた現在のパケットキャプチャのステータスだけを表示する。 1 人のキャプチャだけ一度に動作できます。

  ヒント： パケットキャプチャ オプションおよびフィルターの設定についてのその他の情報に関しては、この資料の**パケットキャプチャ フィルター** セクションを参照して下さい。 AsyncOS オンライン ヘルプに GUI からアクセスするために、**>Online ヘルプ > インデックス > P > パケットキャプチャを助け、サポートするために**ナビゲート して下さい。

AsyncOS バージョン 6.x および それ 以前のパケットキャプチャ

このセクションは AsyncOS バージョン 6.x および それ 以前のパケットキャプチャ プロセスを説明します。

パケットキャプチャを開始するか、または停止して下さい

ESA が接続するネットワークに送信されるか、または受信される他のパケットおよび TCP/IP をキャプチャ するために **tcpdump コマンドを**使用できます。

パケットキャプチャを開始するか、または停止するためにこれらのステップを完了して下さい:

1. ESA の CLI に**診断を > ネットワーク > tcpdump コマンド**入力して下さい。 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（データ 1、データ 2、または管理）およびフィルタを設定 して下さい。

   注 フィルタは Unix tcpdump コマンドと同じ形式を使用します。
3. キャプチャおよび**停止を**それを終了し始めるために『Start』 を選択 して下さい。

   注 キャプチャが進行中の間、tcpdump メニューを終了しないで下さい。 他のどのコマンドも実行するために第 2 CLI ウィンドウを使用して下さい。 キャプチャ プロセスが完了した、Diagnostic と指名されるディレクトリからファイルをダウンロードするためにローカル デスクトップからの Secure Copy（SCP）か File Transfer Protocol （FTP）を使用して下さい（詳細については**パケットキャプチャ フィルター** セクションを参照して下さい）。 ファイル使用 パケットキャプチャ（PCAP）形式は Ethereal または Wireshark のようなプログラムと検討され。

パケットキャプチャ フィルター

診断 > NET CLI コマンド使用標準 tcpdump フィルタ構文。 このセクションは tcpdump キャプチャに関して情報をフィルタリングし、提供しますいくつかの例を提供します。

これらは使用する標準フィルターです:

- **IP -**すべての IP プロトコル トラフィックのためのフィルター
- **TCP -**すべての TCP プロトコル トラフィックのためのフィルター
- **IPホスト**-特定の IP アドレス ソースまたは宛先のためのフィルター

使用中のフィルターのいくつかの例はここにあります:

- **IPホスト 10.1.1.1** -このフィルタはトラフィックをキャプチャ します ソースか宛先として 10.1.1.1 が含まれている。
- **IPホスト 10.1.1.1 か IPホスト 10.1.1.2** -このフィルタはトラフィックをキャプチャ します ソースとして 10.1.1.1 か 10.1.1.2 または宛先が含まれている。

キャプチャされるファイルの検索、ナビゲートへの **var > ログ > 診断**または**データ > パブ > 診断**に関しては診断ディレクトリに達するため。

注 このコマンドが使用されるとき、により ESA ディスクスペースはいっぱいになりますまたパフォーマンス低下を引き起こす場合があります。 Cisco は Cisco IronPort カスタマーサポートエンジニアの支援とだけこのコマンドを使用することを推奨します。