ACNS ソフトウェアの tcpdump コマンドの使用

目次

はじめに

tcpdump コマンドは、Cisco Application and Content Networking Software (ACNS) 4.2.1 で導入されたものです。 このコマンドにより、Cisco テクニカル サポートからデータを収集するように依頼された場合、トラブルシューティング用に Content Engine、コンテンツ ルータ、または Content Distribution Manager のスニファ トレースを収集できます。 このユーティリティは、Linux や Unix の tcpdump コマンドに類似しています。

前提条件

要件

このドキュメントの読者は次のトピックについて理解している必要があります。

- FTP
- ACNS
- ACNS のコマンドライン インターフェイス (CLI)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ACNS 4.2.1 ソフトウェアおよびそれ以降
- ACNS 4.2.X 以降が稼働するすべてのプラットフォーム

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。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

パケットのキャプチャ

ACNS の CLI では、管理者（ユーザ admin）によるイーサネットからのパケットのキャプチャが可能になっています。 Content Engine 500 シリーズでは、インターフェイス名は eth0 と eth1 です。 すべての ACNS プラットフォームで、local1 ディレクトリでのパスまたはファイル名の指定を推奨します。

CLI で **tcpdump** コマンドを発行すると、パケット ヘッダー ダンプを画面に直接出力できます。ダンプを停止するには、**Ctrl-C** キーを押します。

オプション

tcpdump コマンドには、次のオプションがあります。

- **--w** *filename*：未加工のパケット キャプチャ出力をファイルに書きこみます。
- **--s** *count*：各パケットの最初の <count> バイトをキャプチャします。
- **--i** *interface*：パケットのキャプチャに使用する特定のインターフェイスを指定できます。
- **--c** *count*：キャプチャを *count* 個のパケットに制限します。

コマンドの例を次に示します。

tcpdump -w /local1/dump.pcap -i eth0 -s 1500 -c 10000

このコマンドにより、interface ethernet 0 において続く 10,000 パケットの先頭から 1,500 バイト分のデータをキャプチャし、Content Engine の local1 ディレクトリに **dump.pcap** というファイル名で出力が保存されます。

注: パケットの snaplength を設定するために、**-s** オプションを指定していることを確認してください。 デフォルト値では 64 バイトだけがキャプチャされ、キャプチャ ファイルにはパケット ヘッダーのみが保存されます。 リダイレクトされたパケット、またはより高レベルのトラフィック（HTTP、認証など）のトラブルシューティングを行うには、パケット一式のコピーが必要です。

次のように **tcpdump** コマンドを実行することにより、特定の IP アドレスでのフィルタリングも可能です。

- **tcpdump** 行の最後に **host 10.255.1.34** を追加します。 **注: 10.255.1.34** を、クライアントが使用している IP アドレスに置き換えてください。
- また、1500 バイトより大きい可能性がある不良パケットを取得するために、サイズ 1600 を使用してください。

次に例を示します。

```
tcpdump -w /local/mydump -s 1600 -c10000 host 10.255.2.34
```

FTP

TCP ダンプが収集された後、スニファ デコーダで表示できるように、Content Engine から PC へファイルを移動する必要があります。

```
ftp <ip address of the CE>
 !--- Log in with the admin username and password. cd local1 bin hash get <name of the file> !--
- Using the previous example, it is dump.pcap.

     bye
```

Ethereal

機能の豊富さや WCCP リダイレクションに用いられる GRE トンネルでカプセル化されたパケットをデコードする機能など、コンテントネット ワーキングでの使い勝手から TCP ダンプを読み取るためのソフトウェア アプリケーションとして、Ethereal が推奨されます。 詳細については、Wireshark の Web サイトを参照してください。

注: ほとんどの場合、ACNS CLI で利用可能な **tcpdump** ファシリティでキャプチャされたリダイレクト済みのパケットは、インターフェイスで受信したデータと異なります。 リダイレクトされたパケットの内部実装および処理によって、デバイス IP アドレスとポート番号 8999 を反映するために、宛先 IP アドレスと TCP ポート番号が修正されます。

関連情報

- Cisco Application and Content Networking Software (ACNS) ソフトウェア サポート
- テクニカル サポートとドキュメント – Cisco Systems