ESA：パケットキャプチャとネットワーク調査

内容

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設定および収集し、追加のネットワーク調査とトラブルシューティングを実行する方法について説明します。

背景説明

問題が発生した状態でシスコテクニカルサポートに連絡すると、ESAの発信および着信ネットワークアクティビティに関する情報を提供するように求められる場合があります。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して、ネットワーク設定をデバッグしたり、アプライアンスに到達またはアプライアンスから発信するネットワークトラフィックを確認したりできます。

> **注**：このドキュメントでは、Cisco が管理およびサポートしていないソフトウェアを参照します。この情報は、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。

以前に使用した tcpdump CLIコマンドが新しい packetcapture コマンドを使用します。このコマンドは、 tcpdump コマンドを発行します。GUIでも使用できます。

AsyncOSバージョン6.x以前を実行している場合は、 tcpdump このドキュメントの「*AsyncOSバージョン6.x以前のパケットキャプチャ」セクション*のコマンドを使用します。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からパケットキャプチャを開始するには、右上の[Help and Support]メニューに移動し、[Packet Capture]を選択して、[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からパケットキャプチャを開始するには、 **packetcapture > start** コマンドが表示されない場合もあります。パケットキャプチャプロセスを停止するには、 **packetcapture > stop** コマンドを発行して、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、ローカルに保存します。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から[Help and Support] > [Packet Capture]に移動し、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を表示します。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。

- キャプチャを選択し、[Download File]をクリックして、保存されたパケットキャプチャをダウンロードします。

- パケットキャプチャファイルを削除するには、1つまたは複数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の設定を編集するには、Help and Supportメニューから 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** コマンドが表示されない場合もあります。

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] > [**search for **Packet Capture] > [**Running a 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

コントローラ GUI または CLI を使用して tcpdump コマンドを使用して、ESAが接続されているネットワークで送受信されるTCP/IPおよびその他のパケットをキャプチャします。

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. Enter the **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と同じ形式を使用しますす tcpdump コマンドが表示されない場合もあります。
3. キャプチャ**を開始**するにはSTARTを選択し、キャプチャを終了するには**STOP**を選択します。

注：キャプチャの進行中は、tcpdumpメニューを終了しないでください。他のコマンドを実行するには、2番目のCLIウィンドウを使用する必要があります。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

「 **Diagnostic > NET** CLIコマンドでは、標準の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を含むすべての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 TACエンジニアの支援を受けたときにのみ使用することを推奨します。

追加のネットワーク検出と調査

注：次の方法は、CLIからのみ使用できます。

TCPSERVICES

「 tcpservices コマンドは、現在の機能およびシステムプロセスのTCP/IP情報を表示します。

```
example.com> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main     - The FTP daemon
  ginetd        - The INET daemon
```

```
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon

Feature Processes
  euq_webui    - GUI for ISQ
  gui          - GUI process
  hermes       - MGA mail server
  postgres     - Process for storing and querying quarantine data
  splunkd      - Processes for storing and querying Email Tracking data

COMMAND      USER         TYPE NODE   NAME
postgres     pgsql        IPv4 TCP    127.0.0.1:5432
interface    root         IPv4 TCP    127.0.0.1:53
ftpd.main    root         IPv4 TCP    10.0.202.7:21
gui          root         IPv4 TCP    10.0.202.7:80
gui          root         IPv4 TCP    10.0.202.7:443
ginetd       root         IPv4 TCP    10.0.202.7:22
java         root         IPv6 TCP    [::127.0.0.1]:18081
hermes       root         IPv4 TCP    10.0.202.7:25
hermes       root         IPv4 TCP    10.0.202.7:7025
api_serve    root         IPv4 TCP    10.0.202.7:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    10.0.202.7:6443
nginx        root         IPv4 TCP    *:4431
nginx        nobody       IPv4 TCP    *:4431
nginx        nobody       IPv4 TCP    *:4431
java         root         IPv4 TCP    127.0.0.1:9999
```

NETSTAT

このユーティリティは、Transmission Control Protocol（TCP；伝送制御プロトコル）（着信と発信の両方）、ルーティングテーブル、およびネットワークインターフェイスとネットワークプロトコルの統計情報のネットワーク接続を表示します。

```
example.com> netstat

Choose the information you want to display:
1. List of active sockets.
2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
```

Example of Option 1 (List of active sockets)

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 10.0.202.7.10275      10.0.201.4.6025        ESTABLISHED
tcp4       0      0 10.0.202.7.22         10.0.201.4.57759       ESTABLISHED
tcp4       0      0 10.0.202.7.10273      a96-17-177-18.deploy.static.akamaitechnologies.com.80
TIME_WAIT
tcp4       0      0 10.0.202.7.10260      10.0.201.5.443     ESTABLISHED
tcp4       0      0 10.0.202.7.10256      10.0.201.5.443     ESTABLISHED
```

Example of Option 2 (State of network interfaces)

```
Show the number of dropped packets? [N]> y

Name    Mtu Network       Address              Ipkts Ierrs Idrop     Ibytes    Opkts Oerrs
Obytes  Coll  Drop
Data 1    - 10.0.202.0    10.0.202.7        110624529     -     - 117062552515 122028093     -
30126949890     -     -
```

Example of Option 3 (Contents of routing tables)

```
Routing tables

Internet:
Destination        Gateway            Flags      Netif Expire
default            10.0.202.1         UGS         Data 1
10.0.202.0         link#2             U           Data 1
10.0.202.7         link#2             UHS         lo0
localhost.example. link#4             UH          lo0
```

Example of Option 4 (Size of the listen queues)

```
Current listen queue sizes (qlen/incqlen/maxqlen)
Proto Listen         Local Address
tcp4  0/0/50         localhost.exampl.9999
tcp4  0/0/50         10.0.202.7.7025
tcp4  0/0/50         10.0.202.7.25
tcp4  0/0/15         10.0.202.7.6443
tcp4  0/0/15         localhost.exampl.60001
tcp4  0/0/15         10.0.202.7.6080
tcp4  0/0/20         localhost.exampl.18081
tcp4  0/0/20         10.0.202.7.443
tcp4  0/0/20         10.0.202.7.80
tcp4  0/0/10         10.0.202.7.21
tcp4  0/0/10         10.0.202.7.22
tcp4  0/0/10         localhost.exampl.53
tcp4  0/0/208        localhost.exampl.5432
```

Example of Option 5 (Packet traffic information)

```
            input           nic1           output
   packets  errs idrops      bytes    packets  errs      bytes colls drops
        49     0     0       8116         55     0       7496     0     0
```

ネットワーク

diagnosticの下のnetworkサブコマンドは、追加オプションへのアクセスを提供します。これを使用すると、すべてのネットワーク関連キャッシュのフラッシュ、ARPキャッシュの内容の表示、NDPキャッシュの内容の表示（該当する場合）、SMTPPINGを使用してリモートSMTP接続をテストできます。

```
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.
- RELOAD - Reset configuration to the initial manufacturer values.
```

```
- SERVICES - Service Utilities.
[]> network


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

ETHERCONFIG

「 etherconfig コマンドを使用すると、インターフェイス、VLAN、ループバックインターフェイス、MTUサイズ、マルチキャストアドレスによるARP応答の受け入れまたは拒否に関するデュプレックスおよびMAC情報の一部を表示して設定できます。

```
example.com> etherconfig


Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]>
```

TRACEROUTE

リモートホストへのネットワークルートを表示します。または、 traceroute6 コマンドを発行します。

```
example.com> traceroute google.com

Press Ctrl-C to stop.
traceroute to google.com (216.58.194.206), 64 hops max, 40 byte packets
1 68.232.129.2 (68.232.129.2) 0.902 ms
68.232.129.3 (68.232.129.3) 0.786 ms 0.605 ms
2 139.138.24.10 (139.138.24.10) 0.888 ms 0.926 ms 1.092 ms
3 68.232.128.2 (68.232.128.2) 1.116 ms 0.780 ms 0.737 ms
4 139.138.24.42 (139.138.24.42) 0.703 ms
208.90.63.209 (208.90.63.209) 1.413 ms
139.138.24.42 (139.138.24.42) 1.219 ms
5 svl-edge-25.inet.qwest.net (63.150.59.25) 1.436 ms 1.223 ms 1.177 ms
6 snj-edge-04.inet.qwest.net (67.14.34.82) 1.838 ms 2.086 ms 1.740 ms
7 108.170.242.225 (108.170.242.225) 1.986 ms 1.992 ms
108.170.243.1 (108.170.243.1) 2.852 ms
8 108.170.242.225 (108.170.242.225) 2.097 ms
108.170.243.1 (108.170.243.1) 2.967 ms 2.812 ms
9 108.170.237.105 (108.170.237.105) 1.974 ms
sfo03s01-in-f14.1e100.net (216.58.194.206) 2.042 ms 1.882 ms
```

ping

pingを使用すると、IPアドレスまたはホスト名を使用してホストの到達可能性をテストし、通信の遅延やドロップに関する統計情報を提供できます。

```
example.com> ping google.com

Press Ctrl-C to stop.
PING google.com (216.58.194.206): 56 data bytes
64 bytes from 216.58.194.206: icmp_seq=0 ttl=56 time=2.095 ms
64 bytes from 216.58.194.206: icmp_seq=1 ttl=56 time=1.824 ms
64 bytes from 216.58.194.206: icmp_seq=2 ttl=56 time=2.005 ms
64 bytes from 216.58.194.206: icmp_seq=3 ttl=56 time=1.939 ms
64 bytes from 216.58.194.206: icmp_seq=4 ttl=56 time=1.868 ms
64 bytes from 216.58.194.206: icmp_seq=5 ttl=56 time=1.963 ms

--- google.com ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.824/1.949/2.095/0.088 ms
```