ESA - Paketerfassung und Netzwerkanalyse

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Paketerfassung auf der Cisco E-Mail Security Appliance (ESA) konfigurieren und erfassen und zusätzliche Netzwerkanalysen und Fehlerbehebungen durchführen.

Hintergrundinformationen

Wenn Sie sich bei einem Problem an den technischen Support von Cisco wenden, werden Sie möglicherweise gebeten, einen Einblick in die Aktivitäten des ausgehenden und eingehenden Netzwerks der ESA zu geben. Die Appliance ermöglicht das Abfangen und Anzeigen von TCP-, IP- und anderen Paketen, die über das Netzwerk übertragen oder empfangen werden, an das die Appliance angeschlossen ist. Sie können eine Paketerfassung ausführen, um die Netzwerkeinrichtung zu debuggen oder den Netzwerkverkehr zu überprüfen, der die Appliance erreicht oder verlässt.

> **Hinweis:** Dieses Dokument bezieht sich auf Software, die nicht von Cisco verwaltet oder unterstützt wird. Die Informationen werden Ihnen zu Ihrer Zufriedenheit zur Verfügung gestellt. Weitere Unterstützung erhalten Sie vom Softwareanbieter.

Beachten Sie, dass die zuvor tcpdump Der CLI-Befehl wird durch den neuen Befehl ersetzt. packetcapture in AsyncOS 7.0 und höher ausgeführt werden. Dieser Befehl bietet Funktionen, die denen der tcpdump -Befehl ein, und es ist auch für die Verwendung in der GUI verfügbar.

Wenn Sie AsyncOS 6.x oder eine frühere Version ausführen, lesen Sie die Anweisungen zur Verwendung des tcpdump im Abschnitt *Packet Captures on AsyncOS Version 6.x and Ältere*

Abschnitte dieses Dokuments. Die Filteroptionen, die im Abschnitt *Packet Capture Filters* beschrieben werden, gelten auch für den neuen Paketerfassungsbefehl.

Paketerfassungen auf AsyncOS 7.x und höher

In diesem Abschnitt wird der Paketerfassungsprozess für AsyncOS 7.x und höher beschrieben.

Starten oder Beenden einer Paketerfassung

Um eine Paketerfassung über die Benutzeroberfläche zu starten, navigieren Sie oben rechts zum Menü **Hilfe und Unterstützung**, wählen Sie **Paketerfassung aus**, und klicken Sie dann auf **Erfassung starten**. Um den Paketerfassungsprozess zu beenden, klicken Sie auf **Erfassung beenden**.

Hinweis: Eine Erfassung, die in der GUI beginnt, wird zwischen Sitzungen beibehalten.

Um eine Paketerfassung über die CLI zu starten, geben Sie die **packetcapture > start** aus. Um den Paketerfassungsprozess zu stoppen, geben Sie die **packetcapture > stop** und die ESA beendet die Paketerfassung, wenn die Sitzung beendet ist.

Funktion zur Paketerfassung

Im Folgenden finden Sie eine Liste hilfreicher Informationen, mit denen Sie die Paketerfassung bearbeiten können:

- Die ESA speichert die erfasste Paketaktivität in einer Datei und speichert sie lokal. Sie können die Dateigröße für die maximale Paketerfassung, die Zeitdauer, für die die Paketerfassung ausgeführt wird, und die Netzwerkschnittstelle, für die die Erfassung ausgeführt wird, konfigurieren. Sie können auch einen Filter verwenden, um die Paketerfassung auf Datenverkehr über einen bestimmten Port oder Datenverkehr von einer bestimmten Client- oder Server-IP-Adresse zu beschränken.

- Navigieren Sie in der Benutzeroberfläche zu **Hilfe und Unterstützung > Paketerfassung**, um eine vollständige Liste der gespeicherten Paketerfassungsdateien anzuzeigen. Wenn eine Paketerfassung ausgeführt wird, zeigt die Seite Paketerfassung den Status der Erfassung an, die mit den aktuellen Statistiken ausgeführt wird, z. B. die Dateigröße und die verstrichene Zeit.

- Wählen Sie eine Erfassung aus, und klicken Sie auf **Datei herunterladen**, um eine gespeicherte Paketerfassung herunterzuladen.

- Um eine Paketerfassungsdatei zu löschen, wählen Sie eine oder mehrere Dateien aus, und klicken Sie auf **Ausgewählte Dateien löschen**.

- Um die Paketerfassungseinstellungen über die Benutzeroberfläche zu bearbeiten, wählen Sie im Menü Hilfe und Support die Option **Paketerfassung** aus, und klicken Sie auf **Einstellungen bearbeiten**.

- Um die Paketerfassungseinstellungen mit der CLI zu bearbeiten, geben Sie die **packetcapture > setup** aus.

Hinweis: Die GUI zeigt nur die Paketerfassungen an, die in der GUI beginnen, nicht die, die mit der CLI beginnen. Ebenso zeigt die CLI nur den Status einer aktuellen Paketerfassung an, die in der CLI begann. Es kann jeweils nur eine Erfassung ausgeführt werden.

Tipp: Weitere Informationen zu Paketerfassungsoptionen und Filtereinstellungen finden Sie im Abschnitt **Packet Capture Filters** dieses Dokuments. Um über die Benutzeroberfläche auf die AsyncOS-Onlinehilfe zuzugreifen, wählen Sie **Hilfe und Support > Online Help >** Suchen Sie nach **Paketerfassung >** wählen **Eine Paketerfassung ausführen aus.**

Paketerfassungen auf AsyncOS 6.x und früheren Versionen

In diesem Abschnitt wird der Paketerfassungsprozess für AsyncOS 6.x und frühere Versionen beschrieben.

Starten oder Beenden einer Paketerfassung

Sie können tcpdump um TCP/IP und andere Pakete zu erfassen, die über ein Netzwerk übertragen oder empfangen werden, an das die ESA angeschlossen ist.

Gehen Sie wie folgt vor, um eine Paketerfassung zu starten oder zu beenden:

1. Geben Sie **diagnostic > network > tcpdump** in die CLI der ESA ein. Hier ein Beispiel für die Ausgabe:

```
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. Legen Sie die Schnittstelle (Data 1, Data 2 oder Management) und den Filter fest.

   Hinweis: Der Filter verwendet das gleiche Format wie der Unix tcpdump aus.
3. Wählen Sie **START** aus, um die Erfassung zu beginnen und zu beenden.

   Hinweis: Beenden Sie während der Erfassung nicht das tcpdump-Menü. Sie müssen ein zweites CLI-Fenster verwenden, um andere Befehle auszuführen. Nachdem der Erfassungsprozess abgeschlossen ist, müssen Sie Secure Copy (SCP) oder File Transfer Protocol (FTP) von Ihrem lokalen Desktop aus verwenden, um die Dateien aus dem Verzeichnis Diagnostic herunterzuladen (weitere Einzelheiten finden Sie im Abschnitt *Packet Capture Filters*). Die Dateien verwenden das Packet Capture (PCAP)-Format und können mit einem Programm wie Ethereal oder Wireshark überprüft werden.

Paketerfassungsfilter

Die **Diagnostic > NET** Der CLI-Befehl verwendet die standardmäßige tcpdump-Filtersyntax. Dieser Abschnitt enthält Informationen zu tcpdump-Erfassungsfiltern und enthält einige Beispiele.

Die folgenden Standardfilter werden verwendet:

- **ip** - Filter für den gesamten IP-Protokollverkehr
- **tcp** - Filter für den gesamten TCP-Protokollverkehr
- **ip host** - Filter für eine bestimmte IP-Adressquelle oder ein bestimmtes Ziel

Hier einige Beispiele der verwendeten Filter:

- **ip host 10.1.1.1** - Dieser Filter erfasst jeglichen Datenverkehr, der 10.1.1.1 als Quelle oder Ziel enthält.
- **ip host 10.1.1.1 oder ip host 10.1.1.2** - Dieser Filter erfasst Datenverkehr, der entweder 10.1.1.1 oder 10.1.1.2 als Quelle oder Ziel enthält.

Um die erfasste Datei abzurufen, navigieren Sie zu **var > log > diagnostic** or **data > pub > diagnostics (var > log > diagnose > diagnose > diagnostic),** um zum Diagnostic directory zu gelangen.

Hinweis: Wenn dieser Befehl verwendet wird, kann dies dazu führen, dass Ihr ESA-Festplattenspeicher belegt wird, und es kann auch zu Leistungseinbußen kommen. Cisco empfiehlt, diesen Befehl nur mit Unterstützung eines Cisco TAC-Technikers zu verwenden.

Zusätzliche Netzwerkanalyse und -untersuchung

Hinweis: Die folgenden Methoden können nur über die CLI verwendet werden.

TCPSERVICES

Die tcpservices zeigt TCP/IP-Informationen für aktuelle Funktionen und Systemprozesse an.

```
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

Dieses Dienstprogramm zeigt Netzwerkverbindungen für das Transmission Control Protocol (sowohl ein- als auch ausgehend), Routing-Tabellen sowie eine Reihe von Netzwerkschnittstellen- und Netzwerkprotokollstatistiken an.

```
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
```

NETZWERK

Der Netzwerkunterbefehl unter "Diagnostic" bietet Zugriff auf zusätzliche Optionen. Mit dieser Methode können Sie alle netzwerkbezogenen Caches leeren, den Inhalt des ARP-Cache anzeigen, den Inhalt des NDP-Cache anzeigen (falls zutreffend) und die Remote-SMTP-Verbindung mit SMTPPING testen.

```
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

Die etherconfig Mit diesem Befehl können Sie einige Einstellungen für Duplex- und MAC-Informationen für Schnittstellen, VLANs, Loopback-Schnittstellen, MTU-Größen und die Annahme oder Ablehnung von ARP-Antworten mit einer Multicast-Adresse anzeigen und konfigurieren.

```
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

Zeigt die Netzwerkroute zu einem Remotehost an. Alternativ können Sie die traceroute6 , wenn Sie eine IPv6-Adresse auf mindestens einer Schnittstelle konfiguriert haben.

```
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

Mit Ping können Sie die Erreichbarkeit eines Hosts entweder mithilfe der IP-Adresse oder des Hostnamens testen und Statistiken zu möglichen Latenzzeiten und/oder Kommunikationsverlusten bereitstellen.

```
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
```