ESA - Opname van pakketten en netwerkonderzoek

Inhoud

Inleiding

Dit document beschrijft hoe u pakketvastlegging kunt configureren en verzamelen op de Cisco e-mail security applicatie (ESA), en extra netwerkonderzoek en probleemoplossing kunt uitvoeren.

Achtergrondinformatie

Wanneer u contact opneemt met Cisco Technical Support met een probleem, kan u worden gevraagd om inzicht te geven in de uitgaande en inkomende netwerkactiviteit van het ESA. Het apparaat biedt de mogelijkheid om TCP-, IP- en andere pakketten die worden verzonden of ontvangen via het netwerk waaraan het apparaat is gekoppeld, te onderscheppen en weer te geven. Mogelijk wilt u een pakketvastlegging uitvoeren om de netwerkinstellingen te debug of om het netwerkverkeer te controleren dat het apparaat bereikt of verlaat.

> **Opmerking:** Dit document verwijst naar software die niet wordt onderhouden of ondersteund door Cisco. Deze informatie wordt ter beschikking gesteld als hoffelijkheid voor uw gemak. Neem voor verdere assistentie contact op met de verkoper van de software.

Het is belangrijk op te merken dat de eerder gebruikte tcpdump CLI-opdracht wordt vervangen door de nieuwe packetcapture Opdracht in AsyncOS versies 7.0 en hoger. Deze opdracht biedt functionaliteit vergelijkbaar met tcpdump Deze is ook beschikbaar voor gebruik op de GUI.

Als u AsyncOS versie 6.x of eerder gebruikt, raadpleegt u de instructies hoe u het tcpdump opdracht in het *Packet Captures op AsyncOS versies 6.x en eerder* gedeelte van dit document. Ook de

filteropties die in het gedeelte *Packet Capture Filters* worden beschreven, zijn geldig voor de nieuwe opdracht pakketvastlegging.

Packet Capture op AsyncOS versies 7.x en later

In dit gedeelte wordt het proces beschreven van de pakketvastlegging met AsyncOS-versies 7.x en hoger.

Een pakketvastlegging starten of stoppen

Als u een pakketvastlegging vanuit de GUI wilt starten, navigeer dan naar het menu **Help en Ondersteuning** rechtsboven, kies **Packet Capture** en klik vervolgens op **Start**. Klik op **Opname stoppen** om het proces van pakketvastlegging te stoppen.

> **Opmerking:** Een opname die begint in de GUI wordt bewaard tussen sessies.

Voer de **packetcapture > start** uit. Voer het volgende in om het pakketopnameproces te stoppen **packetcapture > stop** De pakketvastlegging wordt gestopt wanneer de sessie eindigt.

Functionaliteit voor pakketvastlegging

Hier is een lijst met behulpzame informatie die u kunt gebruiken om de pakketvastlegging te manipuleren:

- Het ESA slaat de opgenomen pakketactiviteit op in een bestand en slaat deze lokaal op. U kunt de maximale grootte van een pakketvastlegging, de tijdsduur waarvoor het pakketvastlegging draait en de interface van het netwerk waarop de opname draait, configureren. U kunt ook een filter gebruiken om de pakketvastlegging te beperken tot verkeer door een specifieke poort of verkeer vanaf een bepaalde client of server-IP-adres.
- Navigeren in **om Help en Ondersteuning > Packet Capture** van de GUI om een volledige lijst te bekijken van de opgeslagen pakketvastlegging bestanden. Wanneer een pakketvastlegging draait, geeft de Packet Capture pagina de status van de opname weer die momenteel wordt uitgevoerd met de huidige statistieken, zoals de bestandsgrootte en de verlopen tijd.
- Kies een opname en klik op **Downloadbestand** om een opgeslagen pakketvastlegging te downloaden.
- Kies een of meer bestanden en klik op **Geselecteerde bestanden verwijderen** om een pakketopnambestand te verwijderen.
- Om de instellingen voor de pakketvastlegging met de GUI te bewerken, kiest u **Packet Capture** van het menu Help en Support en klikt u op **Instellingen bewerken**.
- Om de instellingen voor de pakketvastlegging met de CLI te bewerken, voert u het **packetcapture > setup** uit.

Opmerking: De GUI geeft alleen pakketvastlegging weer die in de GUI begint, niet de opnamen die met de CLI beginnen. Op dezelfde manier geeft CLI alleen de status weer van een huidige pakketvastlegging die in CLI is begonnen. Slechts één opname kan tegelijkertijd lopen.

Tip: Raadpleeg het gedeelte **Packet Capture Filters** van dit document voor meer informatie over opties en filterinstellingen. Om toegang te hebben tot de AsyncOS online Help van de GUI, navigeer naar **Help en ondersteuning > Online Help >** zoeken naar **pakketvastlegging >** kies **het uitvoeren van een pakketvastlegging.**

Packet Capture op AsyncOS versies 6.x en eerder

In dit gedeelte wordt het proces beschreven van de pakketvastlegging op AsyncOS versies 6.x en eerder.

Een pakketvastlegging starten of stoppen

U kunt de tcpdump opdracht om TCP/IP en andere pakketten op te nemen die worden verzonden of ontvangen via een netwerk waaraan het ESA is verbonden.

Voltooi deze stappen om een pakketvastlegging te starten of te stoppen:

1. Voer het **diagnostic > network > tcpdump** commando in de CLI van de ESA. Hier wordt een voorbeeld uitgevoerd:

```
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. Stel de interface (Data 1, Data 2 of Management) en het filter in.

Opmerking: Het filter gebruikt hetzelfde formaat als Unix tcpdump uit.

3. Kies **START** om de opname te starten en **op te houden** om het te beëindigen.

> **Opmerking:** Sluit het TCP-menu niet af terwijl de opname is gestart. U moet een tweede CLI-venster gebruiken om andere opdrachten te kunnen uitvoeren. Nadat het opnameproces is voltooid, moet u beveiligde kopie (SCP) of File Transfer Protocol (FTP) van uw lokale bureaublad gebruiken om de bestanden te downloaden van de map die diagnostiek heet (raadpleeg de sectie *Packet Capture Filters* voor meer informatie). De bestanden gebruiken Packet Capture (PCAP)-indeling en kunnen worden herzien met een programma zoals EtherSwitch of Wireshark.

Packet Capture Filters

Het **Diagnostic > NET** CLI-opdracht gebruikt de syntaxis van het standaardfilter van de pomp. Dit deel bevat informatie over de vangfilters van de pomp en geeft enkele voorbeelden.

Dit zijn de standaardfilters die worden gebruikt:

- **ip** - filters voor al het IP-protocolverkeer
- **TCP** - filters voor al het TCP-protocolverkeer
- **ip host** - filters voor een specifieke IP-adresbron of -bestemming

Hier zijn een paar voorbeelden van de filters die in gebruik zijn:

- **ip-host 10.1.1**.1 - Met dit filter wordt elk verkeer dat 10.1.1.1 als bron of bestemming bevat, opgenomen.
- **ip-host 10.1.1.1 of ip-host 10.1.1.2** - met dit filter wordt verkeer opgenomen dat 10.1.1.1 of 10.1.1.2 als bron of bestemming bevat.

Voor het ophalen van het opgenomen bestand, navigeer naar **var > log > diagnostiek** of **data > pub > diagnostiek** om de diagnostische directory te bereiken.

> **Opmerking:** Wanneer deze opdracht wordt gebruikt, kan de schijfruimte in de ESA-schijf gevuld zijn en kan deze ook verslechtering van de prestaties veroorzaken. Cisco raadt u aan deze opdracht alleen te gebruiken met de hulp van een Cisco TAC Engineer.

Aanvullende netwerkdetectie en -onderzoek

> **Opmerking:** De onderstaande methoden kunnen alleen van de CLI worden gebruikt.

TUSSENS

Het tcpservices Deze opdracht geeft TCP/IP-informatie weer voor de huidige functie- en systeemprocessen.

```
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

Dit hulpprogramma toont netwerkverbindingen voor het Protocol van de Transmission Control (zowel inkomend als uitgaand), het routingstabellen en een aantal statistieken van de netwerkinterface en het netwerkprotocol.

```
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
```

NETWERK

De netwerk sub-opdracht onder diagnostiek geeft toegang tot extra opties. U kunt dit gebruiken om alle netwerk-gerelateerde caches te spoelen, de inhoud van het ARP cache te tonen, de inhoud van het NDP cache (indien van toepassing) te tonen en u in staat te stellen om externe TCP-connectiviteit te testen met behulp van SMTPPING.

```
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

Het etherconfig Met deze opdracht kunt u bepaalde instellingen bekijken en configureren die betrekking hebben op duplex- en MAC-informatie voor interfaces, VLAN's, loopback-interfaces, grootte van MTU's en acceptatie of afwijzing van ARP-antwoorden met een multicast adres.

```
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

Toont de netwerkroute naar een externe host. U kunt ook de traceroute6 opdracht als u een IPv6-adres hebt dat op ten minste één interface is ingesteld.

```
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 staat u toe om de bereikbaarheid van een host te testen met het IP-adres of hostname en geeft statistieken met betrekking tot mogelijke vertraging en/of druppels in de communicatie.

```
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
```