ESA - Acquisizione dei pacchetti e indagine di rete

Sommario

Introduzione

In questo documento viene descritto come configurare e raccogliere le acquisizioni di pacchetti su Cisco Email Security Appliance (ESA) ed eseguire ulteriori indagini sulla rete e la risoluzione dei problemi.

Premesse

Quando si contatta il supporto tecnico Cisco per un problema, potrebbe essere necessario fornire informazioni dettagliate sull'attività di rete in entrata e in uscita dell'ESA. L'accessorio consente di intercettare e visualizzare i pacchetti TCP, IP e altri pacchetti trasmessi o ricevuti tramite la rete a cui è collegato. È possibile eseguire un'acquisizione di pacchetti per eseguire il debug dell'installazione di rete o per verificare il traffico di rete che raggiunge o esce dall'accessorio.

> **Nota:** Il presente documento fa riferimento a software non gestito o supportato da Cisco. Le informazioni sono fornite a titolo di cortesia. Per ulteriore assistenza, contattare il fornitore del software.

Èimportante notare che le tcpdump il comando CLI è sostituito dal nuovo packetcapture in AsyncOS versione 7.0 e successive. Questo comando offre una funzionalità simile a tcpdump ed è disponibile per l'uso sulla GUI.

Se si esegue AsyncOS versione 6.x o precedente, consultare le istruzioni sull'utilizzo del tcpdump nella sezione *Packet Capture su AsyncOS versioni 6.x e precedenti* di questo documento. Inoltre,

le opzioni di filtro descritte nella sezione *Filtri di acquisizione pacchetti* sono valide anche per il nuovo comando packetcapture.

Acquisizioni di pacchetti su AsyncOS versione 7.x e successive

In questa sezione viene descritto il processo di acquisizione dei pacchetti in AsyncOS versione 7.x e successive.

Avviare o interrompere un'acquisizione pacchetto

Per avviare l'acquisizione di un pacchetto dalla GUI, accedere al menu **Guida e supporto tecnico** in alto a destra, selezionare **Packet Capture** (Acquisizione pacchetto), quindi fare clic su **Start Capture** (Avvia acquisizione). Per interrompere il processo di acquisizione del pacchetto, fare clic su **Stop Capture** (Interrompi acquisizione).

> **Nota:** Un'acquisizione che inizia nella GUI viene mantenuta tra una sessione e l'altra.

Per avviare l'acquisizione di un pacchetto dalla CLI, immettere il comando **packetcapture > start** Per interrompere il processo di acquisizione dei pacchetti, immettere il **packetcapture > stop** e l'ESA interrompe l'acquisizione del pacchetto al termine della sessione.

Funzionalità di acquisizione pacchetti

Di seguito è riportato un elenco di informazioni utili che è possibile utilizzare per modificare le acquisizioni dei pacchetti:

- L'ESA salva l'attività del pacchetto catturato in un file e lo memorizza localmente. È possibile configurare le dimensioni massime dei file di acquisizione dei pacchetti, la durata dell'esecuzione dell'acquisizione e l'interfaccia di rete su cui viene eseguita l'acquisizione. È possibile anche utilizzare un filtro per limitare l'acquisizione del pacchetto al traffico attraverso una porta specifica o al traffico proveniente da un indirizzo IP specifico di client o server.

- Selezionare **Guida e supporto tecnico > Acquisizione pacchetti** dalla GUI per visualizzare un elenco completo dei file di acquisizione pacchetti archiviati. Quando viene eseguita l'acquisizione di un pacchetto, nella pagina Acquisizione pacchetto viene visualizzato lo stato dell'acquisizione in corso con le statistiche correnti, ad esempio le dimensioni del file e il tempo trascorso.

- Scegliere un'acquisizione e fare clic su **Download File** per scaricare un'acquisizione pacchetto archiviata.

- Per eliminare un file di acquisizione dei pacchetti, scegliere uno o più file e fare clic su **Elimina file selezionati**.

- Per modificare le impostazioni di acquisizione dei pacchetti con la GUI, scegliere **Packet Capture** dal menu Help and Support (Guida e supporto) e fare clic su **Edit Settings** (Modifica impostazioni).

- Per modificare le impostazioni di acquisizione dei pacchetti con la CLI, immettere il comando **packetcapture > setup**

Nota: La GUI visualizza solo le acquisizioni dei pacchetti che iniziano dalla GUI, non quelle che iniziano con la CLI. Analogamente, la CLI visualizza solo lo stato di un'acquisizione di pacchetto corrente iniziata nella CLI. È possibile eseguire una sola acquisizione alla volta.

Suggerimento: Per ulteriori informazioni sulle opzioni di acquisizione dei pacchetti e le impostazioni dei filtri, consultare la sezione **Filtri acquisizione pacchetti** in questo documento. Per accedere alla Guida in linea di AsyncOS dalla GUI, selezionare **Guida e supporto tecnico > Guida in linea >** cerca **acquisizione pacchetti >** scegliere **Esecuzione di acquisizione pacchetti.**

Acquisizioni di pacchetti su AsyncOS versione 6.x e precedenti

In questa sezione viene descritto il processo di acquisizione dei pacchetti in AsyncOS versione 6.x e precedenti.

Avviare o interrompere un'acquisizione pacchetto

Èpossibile utilizzare tcpdump per acquisire pacchetti TCP/IP e altri pacchetti trasmessi o ricevuti su una rete a cui l'ESA è collegata.

Per avviare o interrompere l'acquisizione di un pacchetto, completare i seguenti passaggi:

1. Immettere il **diagnostic > network > tcpdump** nella CLI dell'ESA. Di seguito è riportato un esempio di output:

```
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. Impostare l'interfaccia (Dati 1, Dati 2 o Gestione) e il filtro.

   Nota: Il filtro utilizza lo stesso formato di Unix tcpdump
3. Scegliere **START** per avviare la cattura e **STOP** per terminarla.

   Nota: Non uscire dal menu tcpdump mentre l'acquisizione è in corso. Per eseguire qualsiasi altro comando è necessario utilizzare una seconda finestra CLI. Al termine del processo di acquisizione, è necessario utilizzare SCP (Secure Copy) o FTP (File Transfer Protocol) dal desktop locale per scaricare i file dalla directory denominata Diagnostic (per ulteriori informazioni, vedere la sezione *Filtri di acquisizione pacchetti*). I file utilizzano il formato Packet Capture (PCAP) e possono essere rivisti con un programma come Etheral o Wireshark.

Filtri di acquisizione pacchetti

OSPF (Open Shortest Path First) **Diagnostic > NET** Il comando CLI utilizza la sintassi standard del filtro tcpdump. Questa sezione fornisce informazioni relative ai filtri di acquisizione tcpdump e alcuni esempi.

Di seguito sono riportati i filtri standard utilizzati:

- **ip** - Filtri per tutto il traffico del protocollo IP
- **tcp** - Filtri per tutto il traffico del protocollo TCP
- **ip host** - Filtri per un'origine o una destinazione specifica dell'indirizzo IP

Di seguito sono riportati alcuni esempi dei filtri in uso:

- **ip host 10.1.1.1** - Questo filtro acquisisce qualsiasi traffico che include 10.1.1.1 come origine o destinazione.
- **ip host 10.1.1.1 o ip host 10.1.1.2** - Questo filtro acquisisce il traffico che contiene 10.1.1.1 o 10.1.1.2 come origine o destinazione.

Per recuperare il file acquisito, selezionare **var > log > diagnostic** o **data > pub > diagnostic** per raggiungere la directory Diagnostic.

Nota: Quando si usa questo comando, lo spazio su disco dell'ESA potrebbe riempirsi e le prestazioni peggiorare. Cisco consiglia di utilizzare questo comando solo con l'assistenza di un tecnico TAC Cisco.

Individuazione e analisi aggiuntive della rete

Nota: i metodi seguenti possono essere utilizzati solo dalla CLI.

SERVIZI TCP

OSPF (Open Shortest Path First) tcpservices Il comando visualizza le informazioni TCP/IP per i processi di sistema e le funzionalità correnti.

```
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

Questa utilità visualizza le connessioni di rete per il protocollo di controllo della trasmissione (in entrata e in uscita), le tabelle di routing e una serie di statistiche relative all'interfaccia di rete e al protocollo di rete.

```
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
```

RETE

Il sottocomando network in diagnostic consente di accedere a opzioni aggiuntive. È possibile utilizzare questo comando per scaricare tutte le cache di rete, visualizzare il contenuto della cache ARP, visualizzare il contenuto della cache NDP (se applicabile) e consentire di verificare la connettività SMTP remota utilizzando 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

OSPF (Open Shortest Path First) etherconfig Questo comando consente di visualizzare e configurare alcune delle impostazioni relative alle informazioni duplex e MAC per interfacce, VLAN, interfacce di loopback, dimensioni MTU e accettazione o rifiuto di risposte ARP con un indirizzo multicast.

```
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

Visualizza il percorso di rete verso un host remoto. In alternativa, è possibile utilizzare traceroute6 se è stato configurato un indirizzo IPv6 su almeno un'interfaccia.

```
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

Il ping consente di verificare la raggiungibilità di un host utilizzando l'indirizzo IP o il nome host e fornisce le statistiche relative a possibili latenze e/o interruzioni nella comunicazione.

```
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
```