ESA - Capturas de paquetes e investigación de red

Contenido

Introducción

Este documento describe cómo configurar y recopilar capturas de paquetes en Cisco Email Security Appliance (ESA), y realizar investigaciones y resolución de problemas de red adicionales.

Antecedentes

Cuando se ponga en contacto con el Soporte Técnico de Cisco para tratar un problema, se le puede pedir que proporcione información sobre la actividad de red saliente e entrante del ESA. El dispositivo proporciona la capacidad de interceptar y mostrar TCP, IP y otros paquetes que se transmiten o reciben a través de la red a la que se conecta el dispositivo. Es posible que desee ejecutar una captura de paquetes para depurar la configuración de red o para verificar el tráfico de red que llega o sale del dispositivo.

> **Nota:** Este documento hace referencia al software que Cisco no mantiene ni soporta. La información se proporciona como cortesía para su conveniencia. Para obtener más ayuda, póngase en contacto con el proveedor de software.

Es importante tener en cuenta que el tcpdump El comando CLI se reemplaza por el nuevo packetcapture en las versiones 7.0 y posteriores de AsyncOS. Este comando ofrece una funcionalidad similar a la tcpdump y también está disponible para su uso en la GUI.

Si ejecuta AsyncOS versión 6.x o anterior, consulte las instrucciones sobre cómo utilizar el tcpdump en la sección *Capturas de Paquetes en AsyncOS Versiones 6.x y Anteriores* de este documento.

Además, las opciones de filtro que se describen en la sección *Filtros de captura de paquetes* también son válidas para el nuevo comando packetcapture.

Capturas de paquetes en versiones 7.x y posteriores de AsyncOS

Esta sección describe el proceso de captura de paquetes en las versiones 7.x y posteriores de AsyncOS.

Iniciar o detener una captura de paquetes

Para iniciar una captura de paquetes desde la GUI, navegue al menú **Ayuda y soporte** en la parte superior derecha, elija **Captura de paquetes** y luego haga clic en **Iniciar captura**. Para detener el proceso de captura de paquetes, haga clic en **Detener captura**.

> **Nota:** Una captura que comienza en la GUI se conserva entre las sesiones.

Para iniciar una captura de paquetes desde la CLI, ingrese el **packetcapture > start** comando. Para detener el proceso de captura de paquetes, ingrese el **packetcapture > stop** y el ESA detiene la captura de paquetes cuando finaliza la sesión.

Funcionalidad de captura de paquetes

Esta es una lista de información útil que puede utilizar para manipular las capturas de paquetes:

- El ESA guarda la actividad del paquete capturado en un archivo y lo almacena localmente. Puede configurar el tamaño máximo del archivo de captura de paquetes, el tiempo durante el cual se ejecuta la captura de paquetes y en qué interfaz de red se ejecuta la captura. También puede utilizar un filtro para limitar la captura de paquetes al tráfico a través de un puerto específico o al tráfico de una dirección IP de cliente o servidor específica.

- Navegue hasta **Ayuda y soporte > Captura de paquetes** desde la GUI para ver una lista completa de los archivos de captura de paquetes almacenados. Cuando se ejecuta una captura de paquetes, la página Captura de paquetes muestra el estado de la captura en curso con las estadísticas actuales, como el tamaño del archivo y el tiempo transcurrido.

- Elija una captura y haga clic en **Descargar archivo** para descargar una captura de paquetes almacenada.

- Para eliminar un archivo de captura de paquetes, elija uno o más archivos y haga clic en **Eliminar archivos seleccionados**.

- Para editar la configuración de captura de paquetes con la GUI, elija **Captura de paquetes** en el menú Ayuda y soporte y haga clic en **Editar configuración**.

- Para editar la configuración de captura de paquetes con la CLI, ingrese el **packetcapture > setup** comando.

Nota: La GUI sólo muestra las capturas de paquetes que comienzan en la GUI, no las que comienzan con la CLI. De manera similar, la CLI sólo muestra el estado de una captura de paquetes actual que comenzó en la CLI. Sólo se puede ejecutar una captura a la vez.

Consejo: Para obtener información adicional sobre las opciones de captura de paquetes y la configuración de filtros, consulte la sección **Filtros de captura de paquetes** de este documento. Para acceder a la ayuda en línea de AsyncOS desde la GUI, navegue hasta **Ayuda y soporte > Ayuda en línea >** buscar **captura de paquetes >** elija **Ejecutar una captura de paquetes.**

Capturas de paquetes en las versiones 6.x y anteriores de AsyncOS

Esta sección describe el proceso de captura de paquetes en las versiones 6.x y anteriores de AsyncOS.

Iniciar o detener una captura de paquetes

Puede utilizar el tcpdump para capturar TCP/IP y otros paquetes que se transmiten o reciben a través de una red a la que se conecta el ESA.

Complete estos pasos para iniciar o detener una captura de paquetes:

1. Escriba el **diagnostic > network > tcpdump** en la CLI del ESA. A continuación se presenta un ejemplo de salida:

```
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. Establezca la interfaz (Data 1, Data 2 o Management) y el filtro.

   Nota: El filtro utiliza el mismo formato que Unix tcpdump comando.
3. Elija **START** para comenzar la captura y **STOP** para terminarla.

   Nota: No salga del menú tcpdump mientras la captura está en curso. Debe utilizar una segunda ventana CLI para ejecutar cualquier otro comando. Una vez completado el proceso de captura, debe utilizar copia segura (SCP) o protocolo de transferencia de archivos (FTP) desde su escritorio local para descargar los archivos del directorio denominado Diagnostic (consulte la sección *Filtros de captura de paquetes* para obtener más detalles). Los archivos utilizan el formato de captura de paquetes (PCAP) y se pueden revisar con un programa como Ethereal o Wireshark.

Filtros de captura de paquetes

Diagnostic > NET El comando CLI utiliza la sintaxis estándar del filtro tcpdump. Esta sección proporciona información con respecto a los filtros de captura tcpdump y proporciona algunos ejemplos.

Estos son los filtros estándar que se utilizan:

- **ip**: Filtros para todo el tráfico del protocolo IP
- **tcp**: Filtra todo el tráfico del protocolo TCP
- **ip host**: filtra un origen o destino de dirección IP específico

A continuación se muestran algunos ejemplos de los filtros en uso:

- **ip host 10.1.1.1** - Este filtro captura cualquier tráfico que incluya 10.1.1.1 como origen o destino.
- **ip host 10.1.1.1 o ip host 10.1.1.2** - Este filtro captura el tráfico que contiene 10.1.1.1 o 10.1.1.2 como origen o destino.

Para recuperar el archivo capturado, navegue hasta **var > log > diagnostic** o **data > pub > diagnostic** para alcanzar el directorio de diagnóstico.

Nota: Cuando se utiliza este comando, puede provocar que el espacio en disco de ESA se llene y también puede causar una degradación del rendimiento. Cisco recomienda utilizar este comando únicamente con la ayuda de un ingeniero del TAC de Cisco.

Detección e investigación de redes adicionales

Nota: Los siguientes métodos sólo se pueden utilizar desde la CLI.

TCPSERVICES

tcpservices mostrará información de TCP/IP para los procesos actuales de la función y del sistema.

```
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

Esta utilidad muestra las conexiones de red para el protocolo de control de transmisión (tanto entrantes como salientes), las tablas de ruteo y una serie de estadísticas de interfaz de red y protocolo de red.

```
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
```

RED

El subcomando network bajo diagnóstico proporciona acceso a opciones adicionales. Puede utilizar esto para vaciar todas las memorias caché relacionadas con la red, mostrar el contenido de la memoria caché ARP, mostrar el contenido de la memoria caché NDP (si corresponde) y le permite probar la conectividad SMTP remota usando 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

etherconfig permite ver y configurar algunos de los ajustes relacionados con la información de dúplex y MAC para interfaces, VLAN, interfaces de loopback, tamaños de MTU y aceptación o rechazo de las respuestas ARP con una dirección 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

Muestra la ruta de red a un host remoto. También puede utilizar el traceroute6 si tiene una dirección IPv6 configurada en al menos una interfaz.

```
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 le permite probar el alcance de un host usando la dirección IP o el nombre de host y proporciona estadísticas relacionadas con la latencia posible y/o caídas en la comunicación.

```
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
```