Fase 1 de Troubleshooting de Trayectoria de Datos de Firepower: Entrada de paquetes

Contenido

Introducción

Este artículo forma parte de una serie de artículos que explican cómo resolver sistemáticamente los problemas de la ruta de datos en sistemas Firepower para determinar si los componentes de Firepower pueden estar afectando al tráfico. Consulte el artículo Descripción general para obtener información sobre la arquitectura de las plataformas Firepower y los enlaces a otros artículos de Troubleshooting de Trayectoria de Datos.

En este artículo, veremos la primera etapa de la solución de problemas de la ruta de datos de Firepower, la etapa de ingreso de paquetes.

Guía de la plataforma

En la tabla siguiente se describen las plataformas tratadas en este artículo.

Nombre de código de la plataforma	Descripción	Aplicable Hardware Plataformas	Notas
SFR	Módulo instalado de ASA con FirePOWER Services (SFR).	Serie ASA-5500-X	N/A

FTD (sin SSP y FPR-2100)	Imagen de Firepower Threat Defense (FTD) instalada en un dispositivo de seguridad adaptable (ASA) o una plataforma virtual	Plataformas de NGFW virtuales ASA-5500-X	N/A
FTD (SSP)	FTD instalado como dispositivo lógico en un chasis basado en Firepower eXtensible Operative System (FXOS)	FPR-9300, FPR-4100, FPR-2100	La serie 2100 no utiliza el administrador de chasis FXOS

Solución de problemas de la fase de ingreso de paquetes

El primer paso para la solución de problemas del trayecto de datos es asegurarse de que no se produzcan pérdidas en la etapa de ingreso o egreso del procesamiento de paquetes. Si un paquete ingresa pero no se arroja, puede estar seguro de que el dispositivo está descartando el paquete en algún lugar dentro de la ruta de datos o que el dispositivo no puede crear el paquete de salida (por ejemplo, una entrada ARP faltante).

Identificación del tráfico en cuestión

El primer paso en la solución de problemas de la etapa de ingreso del paquete es aislar el flujo y las interfaces involucradas en el tráfico problemático. Esto incluye:

Información de flujo	Información de interfaz
Protocolo	
Dirección IP de origen	Interfaz de ingreso
Puerto de Origen	Interfaz de salida
IP de destino	
Puerto de Destino	

Por ejemplo:

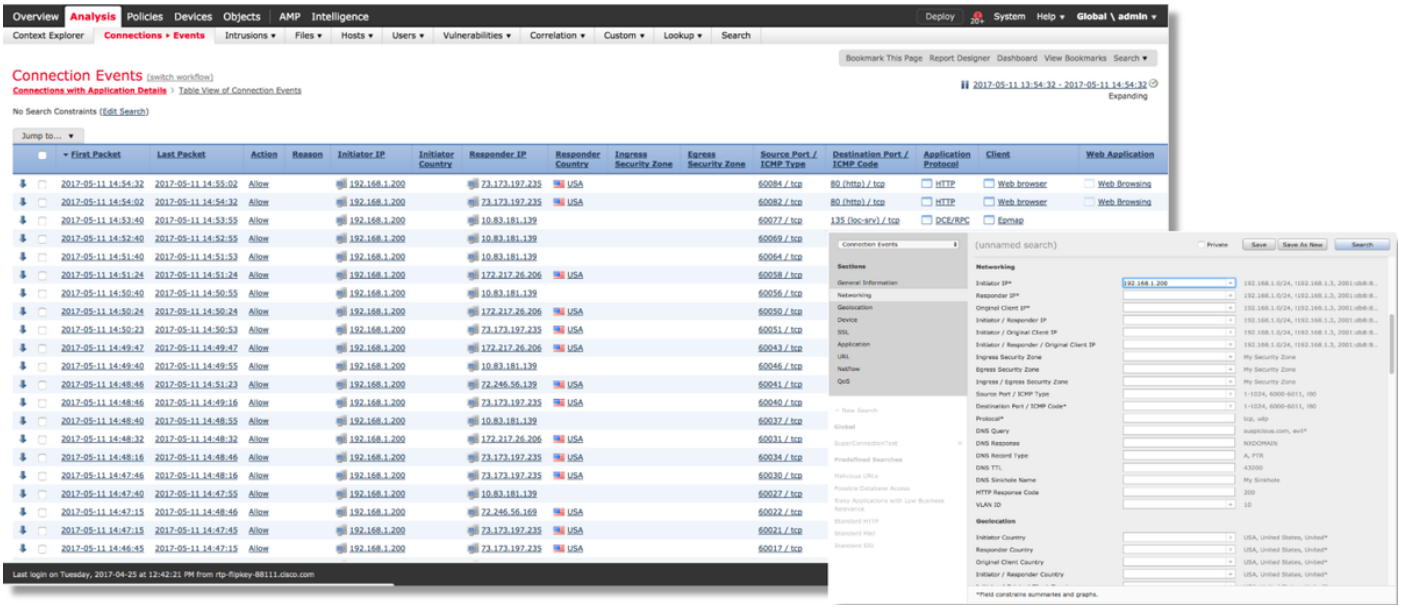
```
TCP inside 172.16.100.101:38974 outside 192.168.1.10:80
```

> **Consejo:** Es posible que no pueda identificar el puerto de origen exacto, ya que a menudo es diferente en cada flujo, pero el puerto de destino (servidor) debe ser suficiente.

Comprobar eventos de conexión

Después de hacerse una idea de la interfaz de ingreso y egreso, el tráfico debe coincidir, así como la información de flujo, el primer paso para identificar si Firepower está bloqueando el flujo es verificar los eventos de conexión para el tráfico en cuestión. Estos se pueden ver en Firepower Management Center en **Análisis > Conexiones > Eventos**

> **Nota:** Antes de comprobar los eventos de conexión, asegúrese de que el registro esté habilitado en las reglas de la directiva de control de acceso. El registro se configura en la ficha "Registro" de cada regla de directiva de control de acceso, así como en la ficha Inteligencia de seguridad. Asegúrese de que las reglas sospechosas estén configuradas para enviar los registros al "Visor de eventos".



En el ejemplo anterior, se hace clic en "Editar búsqueda" y se agrega una IP de origen única (iniciador) como filtro para ver los flujos que estaba detectando Firepower. La columna Acción muestra "Permitir" para este tráfico de host.

Si Firepower bloquea el tráfico intencionalmente, la acción contiene la palabra "Block" (Bloquear). Al hacer clic en "Vista de tabla de eventos de conexión" se proporcionan más datos. Los campos siguientes de los eventos de conexión se pueden observar si la acción es "Bloquear":

-Motivo

- Regla de control de acceso

Esto, combinado con los otros campos del evento en cuestión, puede ayudar a reducir qué componente está bloqueando el tráfico.

Para obtener más información sobre la resolución de problemas de las Reglas de control de acceso, puede hacer clic aquí.

Captura de paquetes en las interfaces de entrada y salida

Si no hay eventos o se sospecha que Firepower está bloqueando a pesar de que los eventos de conexión muestran una acción de regla de "Permitir" o "Confiar", la solución de problemas de la ruta de datos continúa.

A continuación, se ofrecen instrucciones sobre cómo ejecutar una captura de paquetes de ingreso y egreso en las diversas plataformas mencionadas anteriormente:

SFR: captura en las interfaces ASA

Dado que el módulo SFR es simplemente un módulo que se ejecuta en el firewall ASA, es mejor capturar primero en las interfaces de ingreso y egreso del ASA para asegurarse de que los mismos paquetes que ingresan también se están dirigiendo.

Este artículo contiene instrucciones sobre cómo realizar las capturas en el ASA.

Si se ha determinado que los paquetes que ingresan al ASA no se están dirigiendo, continúe con la siguiente fase en la solución de problemas (la fase DAQ).

> **Nota:** Si se ven paquetes en la interfaz de ingreso de ASA, puede que valga la pena verificar los dispositivos conectados.

FTD (sin SSP y FPR-2100): captura en las interfaces de entrada y salida

La captura en un dispositivo FTD que no es SSP es similar a la captura en ASA. Sin embargo, puede ejecutar los comandos de captura directamente desde el mensaje inicial de CLI. Al resolver problemas de paquetes perdidos, se recomienda agregar la opción "trace" a la captura.

Este es un ejemplo de configuración de una captura de ingreso para el tráfico TCP en el puerto 22:

```
> capture ssh_traffic trace interface inside match tcp any any eq 22
> show capture ssh_traffic

7 packets captured

   1: 01:17:38.498906       192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 <mss
1460,sackOK,timestamp 1045829951 0,nop,wscale 7>
   2: 01:17:38.510898       10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win
17896 <mss 1380,sackOK,timestamp 513898266 1045829951,nop,wscale 7>
   3: 01:17:38.511402       192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop,nop,timestamp
1045829956 513898266>
   4: 01:17:38.511982       192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win
229 <nop,nop,timestamp 1045829957 513898266>
   5: 01:17:38.513294       10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop,nop,timestamp
513898268 1045829957>
   6: 01:17:38.528125       10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win
140 <nop,nop,timestamp 513898282 1045829957>
   7: 01:17:38.528613       192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop,nop,timestamp
1045829961 513898282>
```

Si agrega la opción "trace", puede seleccionar un paquete individual para rastrear a través del sistema para ver cómo llegó al veredicto final. También ayuda a asegurarse de que se realizan las modificaciones adecuadas en el paquete, como la modificación de IP de traducción de direcciones de red (NAT), y que se ha elegido la interfaz de salida adecuada.

```
> show capture ssh_traffic packet-number 4 trace

7 packets captured

   4: 01:17:38.511982       192.168.62.70.48560 > 10.83.180.173.22: P
4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 626406, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 4250994242, ack 903999423
AppID: service SSH (846), application unknown (0)
Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt
65535, user 2, icmpType 0, icmpCode 0
Firewall: trust/fastpath rule, id 268435458, allow
NAP id 1, IPS id 0, Verdict WHITELIST
Snort Verdict: (fast-forward) fast forward this flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
```

En el ejemplo anterior, vemos que el tráfico llega a la inspección de Snort y que finalmente llegó a un veredicto de permitir y en general se pasó a través del dispositivo. Dado que el tráfico se puede ver en ambas direcciones, puede estar seguro de que el tráfico fluye a través del dispositivo para esta sesión, por lo que puede que no sea necesaria una captura de salida, pero también puede tomar una captura allí para asegurarse de que el tráfico se esté dirigiendo correctamente como se muestra en el resultado del seguimiento.

> **Nota:** Si el dispositivo no puede crear el paquete de salida, la acción de seguimiento sigue siendo "permitir" pero el paquete no se crea ni se ve en la captura de la interfaz de salida. Este es un escenario muy común donde el FTD no tiene una entrada ARP para el salto siguiente o la IP de destino (si este último está conectado directamente).

FTD (SSP): captura en las interfaces lógicas FTD

Los mismos pasos para generar una captura de paquetes en FTD como se mencionó anteriormente pueden seguirse en una plataforma SSP. Puede conectarse mediante SSH a la dirección IP de la interfaz lógica FTD e ingresar el siguiente comando:

```
Firepower-module1> connect ftd
>
```

También puede navegar al shell del dispositivo lógico FTD desde el símbolo del sistema FXOS con los siguientes comandos:

```
# connect module 1 console
Firepower-module1> connect ftd
>
```

Si se utiliza Firepower 9300, el número de módulo puede variar según el módulo de seguridad que se esté utilizando. Estos módulos admiten hasta 3 dispositivos lógicos.

Si se utilizan varias instancias, el ID de instancia debe incluirse en el comando "connect". El comando Telnet se puede utilizar para conectarse a diferentes instancias al mismo tiempo.

```
# connect module 1 telnet
Firepower-module1>connect ftd ftd1
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>
```

Comprobar errores de interfaz

Los problemas de nivel de interfaz también se pueden verificar durante esta fase. Esto es especialmente útil si faltan paquetes en la captura de la interfaz de ingreso. Si se observan errores de interfaz, la verificación de los dispositivos conectados puede resultar útil.

SFR: verifique las interfaces ASA

Dado que el módulo FirePOWER (SFR) es básicamente una máquina virtual que se ejecuta en un ASA, se comprueban los errores de las interfaces ASA reales. Para obtener información detallada sobre la verificación de las estadísticas de la interfaz en el ASA, consulte esta sección de la Guía de Referencia de Comandos de la Serie ASA.

FTD (no SSP y FPR-2100): verifique si hay errores de interfaz

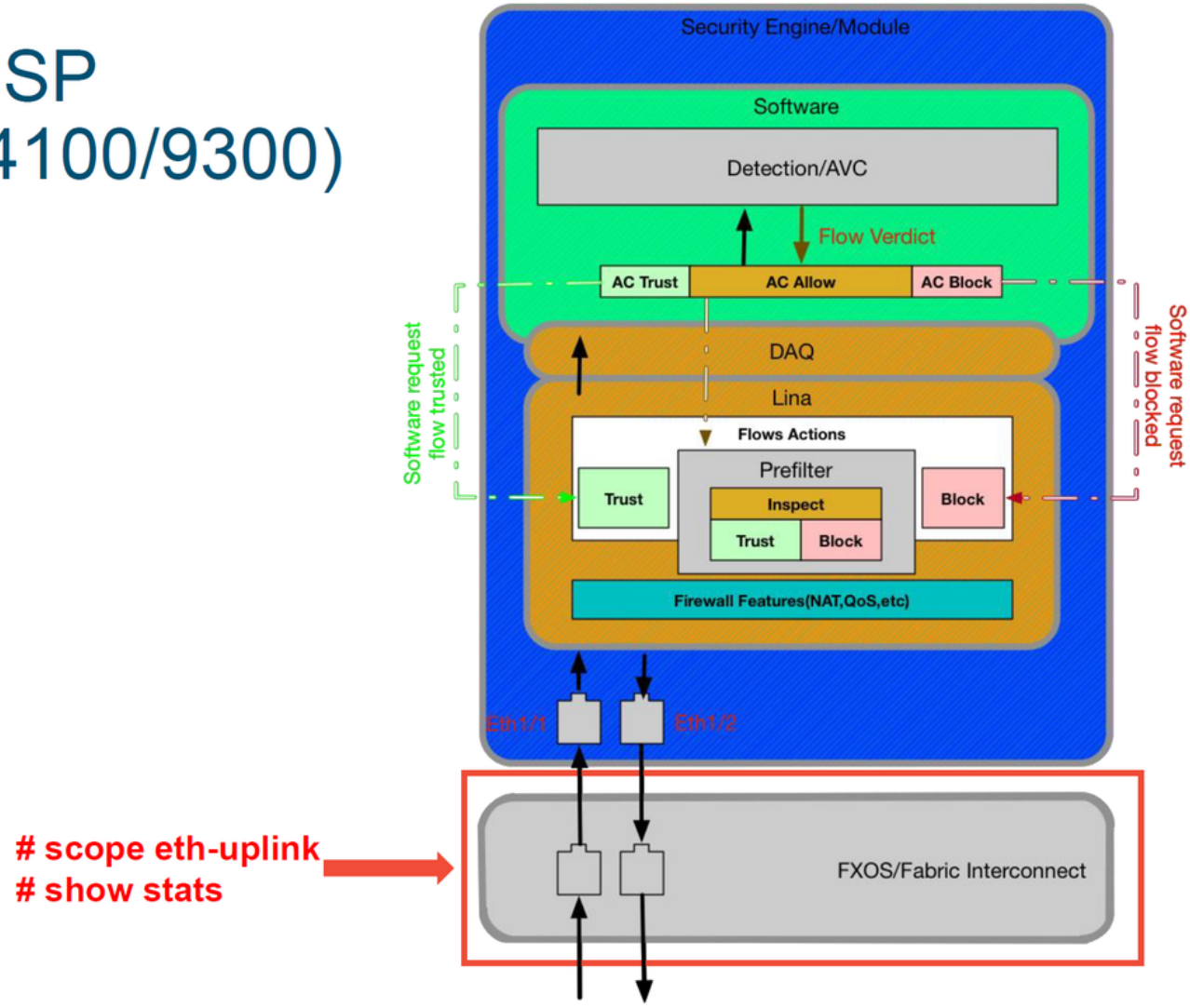
En los dispositivos FTD que no son SSP, el comando **> show interface** se puede ejecutar desde el símbolo del sistema inicial. El resultado interesante se resalta en rojo.

```
> show interface
InterfaceGigabitEthernet0/0 "outside", is up, line protocol is up
    Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
            Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
             Input flow control is unsupported, output flow control is off
             MAC address 000c.2961.f78b, MTU 1500
             IPS Interface-Mode: inline, Inline-Set: InlineSet
             IP address unassigned
             20686130 packets input, 8859847035 bytes, 0 no buffer
             Received 0 broadcasts, 0 runts, 0 giants
             2312 input errors, 0 CRC, 0 frame, 12313 overrun, 0 ignored, 0 abort
             0 pause input, 0 resume input
             0 L2 decode drops
             6485096 packets output, 1480276815 bytes, 0 underruns
             0 pause output, 0 resume output
             1341 output errors, 45635 collisions, 1 interface resets
             0 late collisions, 0 deferred
             0 input reset drops, 0 output reset drops
             input queue (blocks free curr/low): hardware (509/362)
             output queue (blocks free curr/low): hardware (511/415)
    Traffic Statistics for "outside":
             20686131 packets input, 8485139715 bytes
             6485096 packets output, 1375761699 bytes
             4702172 packets dropped
        1 minute input rate 2 pkts/sec,  999 bytes/sec
        1 minute output rate 0 pkts/sec,  78 bytes/sec
        1 minute drop rate, 0 pkts/sec
        5 minute input rate 3 pkts/sec,  1222 bytes/sec
        5 minute output rate 1 pkts/sec,  319 bytes/sec
        5 minute drop rate, 1 pkts/sec
```

FTD (SSP): Navegación por la ruta de datos para buscar errores de interfaz

Las plataformas SSP 9300 y 4100 tienen una fabric interconectada interna que primero maneja los paquetes.

SSP (4100/9300)



Vale la pena verificar si hay algún problema de interfaz en el ingreso inicial del paquete. Estos son los comandos que se ejecutarán en la CLI del sistema FXOS para obtener esta información.

```
ssp# scope eth-uplink
ssp /et-uplink # show stats
```

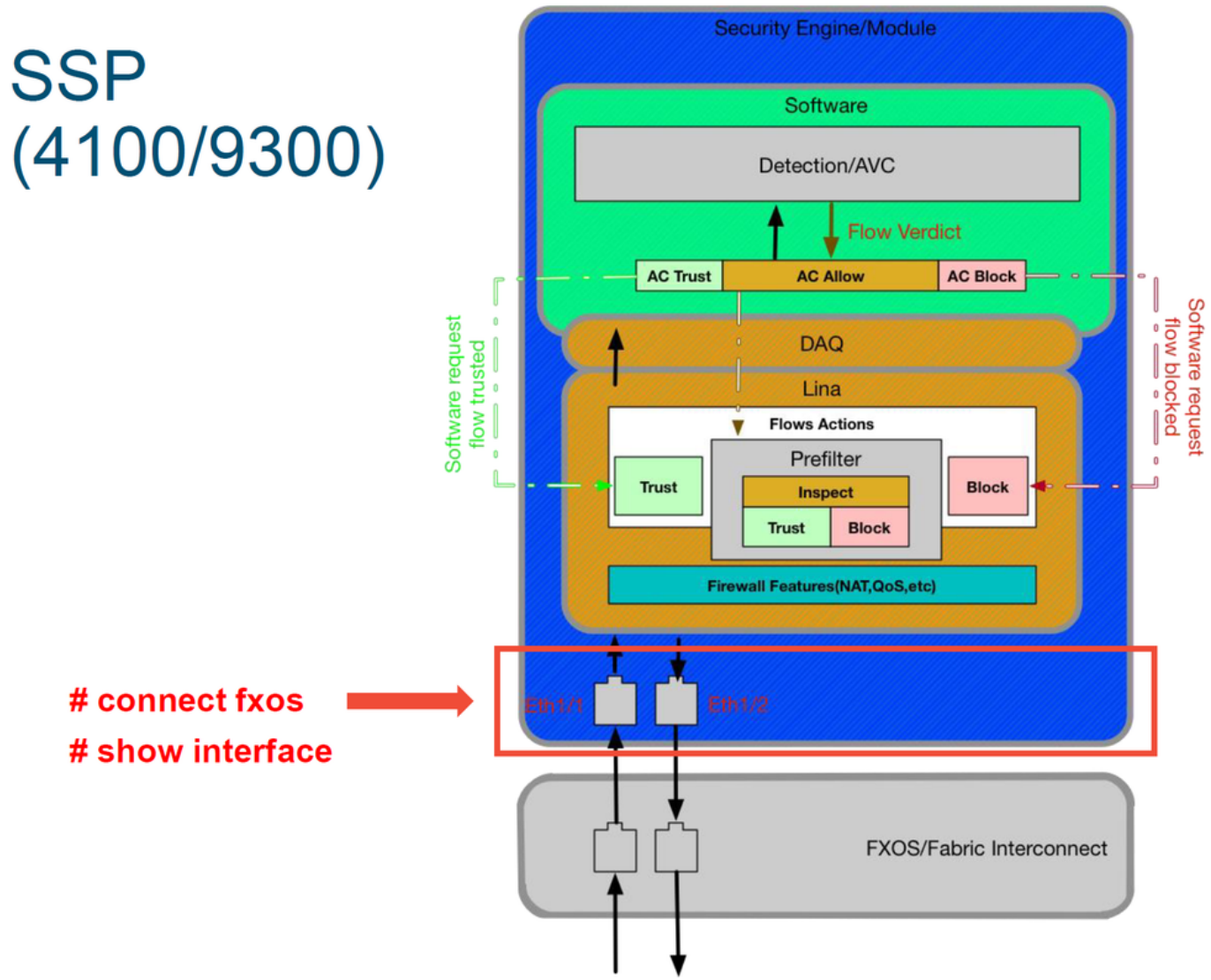
Éste es un ejemplo de salida.

```
ssp# scope eth-uplink

ssp /eth-uplink # show stats

Ether Error Stats:
    Time Collected: 2017-05-15T14:13:46.032
    Monitored Object: fabric/lan/A/pc-44/err-stats
    Suspect: No
    Rcv (errors): 0
    Align (errors): 0
    Fcs (errors): 0
    Xmit (errors): 0
    Under Size (errors): 0
    Out Discard (errors): 0
    Int Mac Tx (errors): 0
    Int Mac Rx (errors): 0
    Deferred Tx (errors): 0
    Thresholded: Xmit Delta Min

Time Collected: 2017-05-15T14:13:46.032
    Monitored Object: fabric/lan/A/pc-48/err-stats
    Suspect: No
    Rcv (errors): 0
    Align (errors): 0
    Fcs (errors): 0
    Xmit (errors): 0
    Under Size (errors): 0
    Out Discard (errors): 0
    Int Mac Tx (errors): 0
    Int Mac Rx (errors): 0
    Deferred Tx (errors): 0
    Thresholded: Xmit Delta Min
```

```
Ether Loss Stats:
    Time Collected: 2017-05-15T14:13:46.032
    Monitored Object: fabric/lan/A/pc-44/loss-stats
    Suspect: No    Single Collision (errors): 0
    Multi Collision (errors): 0
    Late Collision (errors): 0
    Carrier Sense (errors): 0
    Giants (errors): 0
    Symbol (errors): 0
    SQE Test (errors): 0
    Excess Collision (errors): 0
    Thresholded: 0

    Time Collected: 2017-05-15T14:13:46.032
    Monitored Object: fabric/lan/A/pc-48/loss-stats
    Suspect: No    Single Collision (errors): 0
    Multi Collision (errors): 0
    Late Collision (errors): 0
    Carrier Sense (errors): 0
    Giants (errors): 0
    Symbol (errors): 0
    SQE Test (errors): 0
    Excess Collision (errors): 0
    Thresholded: 0
```

Después de que la fabric interconectada maneja el paquete al ingreso, se envía a las interfaces que se asignan al dispositivo lógico que aloja el dispositivo FTD.

A continuación se muestra un diagrama de referencia:



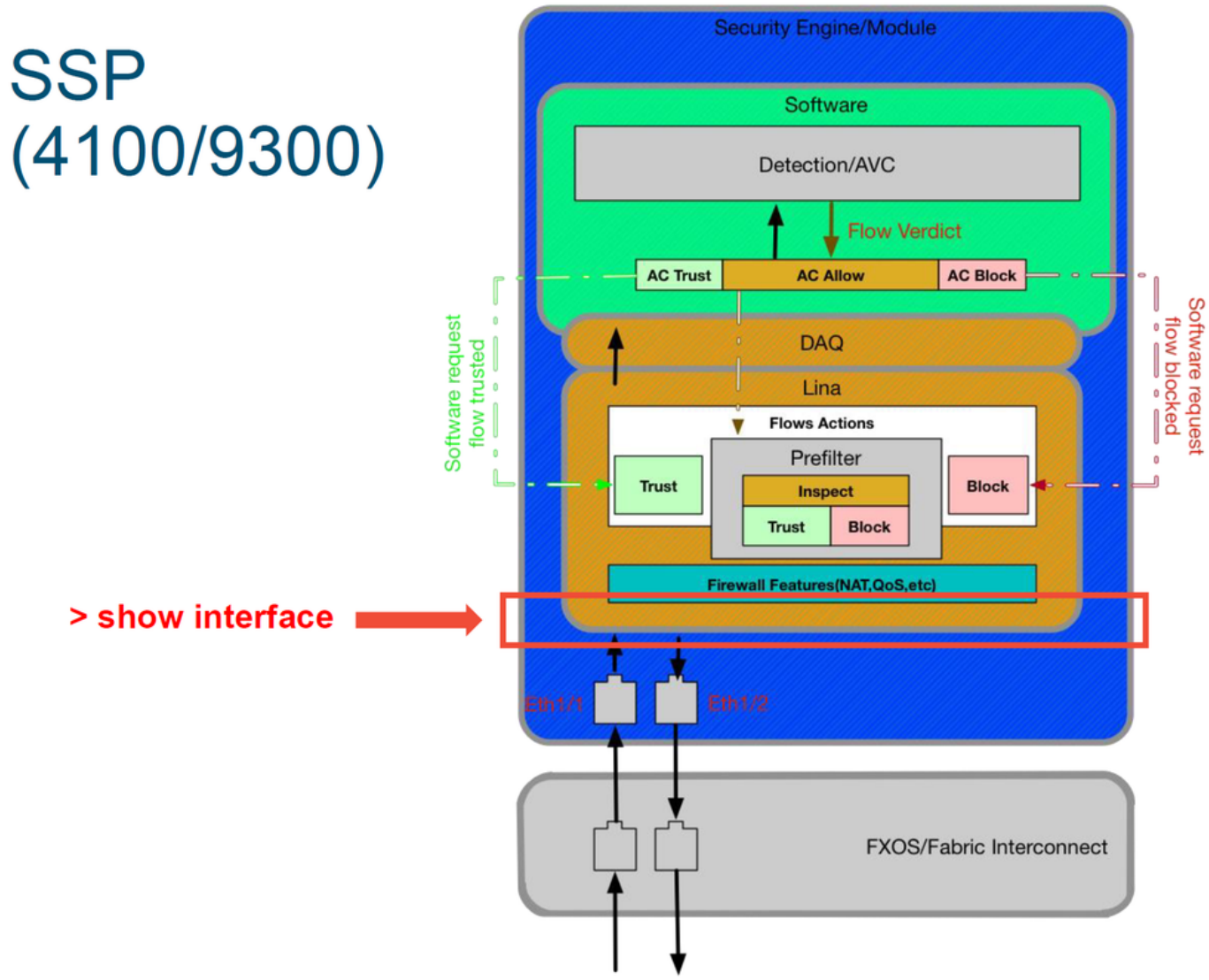
Para verificar cualquier problema de nivel de interfaz, ingrese los siguientes comandos:

```
ssp# connect fxos
ssp(fxos)# show interface Ethernet 1/7
```

Este es un ejemplo de salida (posibles problemas resaltados en rojo):

```
ssp# connect fxos

ssp(fxos)# show interface Ethernet 1/7
Ethernet1/7 is up
 Dedicated Interface
  Hardware: 1000/10000 Ethernet, address: 5897.bdb9.4080 (bia 5897.bdb9.4080)
  Description: U: Uplink
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec
  reliability 254/255, txload 1/255, rxload 1/255
  […Omitted for brevity]
  Last link flapped 14week(s) 4day(s)
  Last clearing of "show interface" counters never
  2 interface resets
  30 seconds input rate 1352 bits/sec, 1 packets/sec
  30 seconds output rate 776 bits/sec, 1 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 728 bps, 0 pps; output rate 608 bps, 0 pps
  RX
    3178795 unicast packets  490503 multicast packets  1142652 broadcast packets
    4811950 input packets  3354211696 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    44288 input error  0 short frame  44288 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  306404 input discard
    0 Rx pause
  TX
    1974109 unicast packets  296078 multicast packets  818 broadcast packets
    2271005 output packets  696237525 bytes
    0 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble 0 output discard
    0 Tx pause
```

Si se observa algún error, el software FTD real también se puede comprobar en busca de errores de interfaz.



Para llegar a la indicación FTD, primero es necesario navegar a la indicación FTD CLI.

```
# connect module 1 console
Firepower-module1> connect ftd
>show interface
```

Para instancias múltiples:

```
# connect module 1 telnet
Firepower-module1>connect ftd ftd1
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>
```

Este es un ejemplo de salida.

```
# connect module 1 console

Firepower-module1> connect ftd

> show interface
InterfaceGigabitEthernet0/0 "outside", is up, line protocol is up
     Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
                Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
                 Input flow control is unsupported, output flow control is off
                 MAC address 000c.2961.f78b, MTU 1500
                 IPS Interface-Mode: inline, Inline-Set: InlineSet
                 IP address unassigned
                 20686130 packets input, 8859847035 bytes, 0 no buffer
                 Received 0 broadcasts, 0 runts, 0 giants
                 2312 input errors, 0 CRC, 0 frame, 12313 overrun, 0 ignored, 0 abort
                 0 pause input, 0 resume input
                 0 L2 decode drops
                 6485096 packets output, 1480276815 bytes, 0 underruns
                 0 pause output, 0 resume output
                 1341 output errors, 45635 collisions, 1 interface resets
                 0 late collisions, 0 deferred
                 0 input reset drops, 0 output reset drops
                 input queue (blocks free curr/low): hardware (509/362)
                 output queue (blocks free curr/low): hardware (511/415)
    Traffic Statistics for "outside":
                 20686131 packets input, 8485139715 bytes
                 6485096 packets output, 1375761699 bytes
                 4702172 packets dropped
           1 minute input rate 2 pkts/sec,  999 bytes/sec
           1 minute output rate 0 pkts/sec,  78 bytes/sec
           1 minute drop rate, 0 pkts/sec
           5 minute input rate 3 pkts/sec,  1222 bytes/sec
           5 minute output rate 1 pkts/sec,  319 bytes/sec
           5 minute drop rate, 1 pkts/sec
```

Datos para proporcionar al Cisco Technical Assistance Center (TAC)

Datos	Instrucciones
Capturas de pantalla de un evento de conexión resultado	Consulte este artículo para obtener instrucciones
'show interface'	Consulte este artículo para obtener instrucciones
Capturas de paquetes	Para ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next firewalls/1180... Para Firepower: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-800 appliances/11777...
Salida 'show tech' de ASA	Inicie sesión en ASA CLI y guarde la sesión de terminal en un registro. Ingrese el comando s proporcione el archivo de salida de la sesión terminal al TAC. Este archivo se puede guardar en disco o en un sistema de almacenamiento externo con est show tech | redirect disk0:/show_tech.log
Solución de problemas de archivo del dispositivo	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techno

Firepower que inspecciona el tráfico

Siguiente paso: Solución de problemas de la capa de Firepower DAQ

Si no está claro si el dispositivo Firepower está descartando paquetes, se puede omitir el dispositivo Firepower para descartar todos los componentes Firepower a la vez. Esto es especialmente útil para mitigar un problema si el tráfico en cuestión ingresa al dispositivo Firepower pero no se arroja.

Para continuar, revise la siguiente fase de la solución de problemas de la ruta de datos de Firepower; El DAQ de Firepower. Haga clic aquí para continuar.