Firepower Data Path Problemen opsporen en verhelpen fase 1: PacketIngress

Inhoud

Inleiding

Dit artikel maakt deel uit van een reeks artikelen waarin wordt uitgelegd hoe u het gegevenspad op FirePOWER-systemen systematisch moet oplossen om te bepalen of onderdelen van Firepower invloed kunnen hebben op het verkeer. Raadpleeg het gedeelte Overzicht voor informatie over de architectuur van FirePOWER-platforms en de koppelingen naar de andere artikelen voor probleemoplossing in datacenters.

In dit artikel, zullen we de eerste fase van de het oplossen van het Vuurwerk van gegevenspad, het stadium van het Ingress van Packet bekijken.

Platform Guide

In de volgende tabel worden de onder dit artikel vallende platforms beschreven.

Naam van platform	Beschrijving	toepasbaar Hardware Platforms	Opmerkingen
SFR	ASA met FirePOWER Services (SFR) module geïnstalleerd.	ASA-5500-X Series Next-Generation	N.v.t.

FTD (niet-SSP en FPR-2100)	Firepower Threat Defense (FTD) afbeelding geïnstalleerd op een adaptieve security applicatie (ASA) of een virtueel platform	ASA-5500-X Series, virtuele NGFW-platforms	N.v.t.
FTD (SSP)	FTD geïnstalleerd als logisch apparaat op een op Firepower eXtensible Operative System (FXOS) gebaseerd chassis	FPR-9300, FPR-4100, FPR-2100	De 2100-serie gebruikt niet de FXOS Chassis Manager

Probleemoplossing voor de pakketinvoerfase

De eerste stap voor het opsporen van problemen bij het gegevenspad is om ervoor te zorgen dat er geen druppels voorkomen in het inloop- of voortgangsstadium van de pakketverwerking. Als een pakket knippert maar niet egaliseert, kunt u er zeker van zijn dat het pakket op een bepaalde plaats binnen het datapad door het apparaat wordt gedropt of dat het apparaat niet in staat is om het strips-pakket te maken (bijvoorbeeld een ontbrekende ARP-ingang).

Identificeer het betreffende verkeer

De eerste stap in het oplossen van het stadium van het pakketinvoeren is om de stroom en de interfaces betrokken bij het probleemverkeer te isoleren. Dit omvat:

Flow-informatie	Interfaceinformatie
Protocol IP-adres bron Bronpoort IP-bestemming Doelpoort	Ingress-interface Egypte-interface

Bijvoorbeeld:

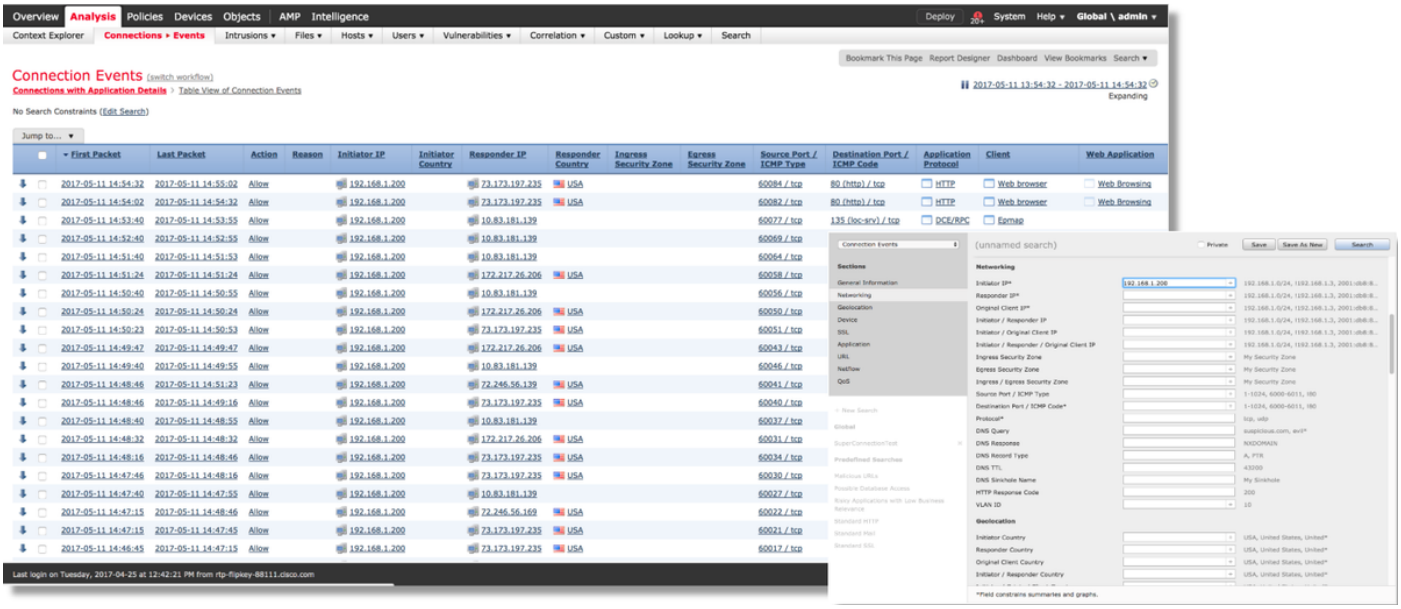
```
TCP inside 172.16.100.101:38974 outside 192.168.1.10:80
```

> **Tip**: U kunt de exacte bronpoort niet vinden omdat deze vaak verschillend is in elke flow, maar de bestemming (server) poort moet voldoende zijn.

Op aansluitingen controleren

Na het krijgen van een idee van de ingang en de spanning interface zou het verkeer zowel als de stroominformatie bij elkaar moeten passen, is de eerste stap om te identificeren of Firepower de stroom blokkeert het controleren van de verbindingsgebeurtenissen voor het betreffende verkeer. U kunt deze informatie in het FireSIGHT Management Center bekijken onder **Analyse > Connections > Evenementen**

> Opmerking: Voordat u verbindingsgebeurtenissen controleert, moet u ervoor zorgen dat logging mogelijk is in de regels van het toegangsbeleid. Vastlegging is ingesteld in het tabblad "Vastlegging" binnen elke regel van het toegangsbeleid en in het tabblad Security Intelligence. Zorg ervoor dat de verdachte regels zijn ingesteld om de logbestanden naar het "Event Viewer" te sturen.



In het bovenstaande voorbeeld wordt op "Zoeken bewerken" gedrukt en wordt een IP-telefoon met een unieke bron (initiator) toegevoegd als een filter om de stromen te zien die met FirePOWER zijn gedetecteerd. De kolom Actie toont "toestaan" voor dit host verkeer.

Als Firepower bedoeld verkeer blokkeert, bevat de Action het woord "Blok". Wanneer u op "Tabelweergave van verbindingsgebeurtenissen" klikt, worden er meer gegevens gegenereerd. De volgende velden in de verbindingsgebeurtenissen kunnen worden opgemerkt als de actie "Blok" is:

- Reden

- Toegangscontroleregels

Dit kan, in combinatie met de andere velden in het geval in kwestie, helpen om te verkleinen welke component het verkeer blokkeert.

U kunt hier voor meer informatie over de toegangscontroleregels voor probleemoplossing klikken.

Packets op de inlaat- en bovenloopinterfaces opnemen

Als er geen gebeurtenissen zijn of het Firepower nog steeds wordt vermoed te blokkeren ondanks de Connection-gebeurtenissen die een regelactie van "Allow" of "Trust" weergeven, gaat de probleemoplossing in het datapad door.

Hieronder vindt u instructies voor het uitvoeren van een instap- en noodpakketvastlegging op de verschillende hierboven genoemde platforms:

SFR - Opname op de ASA-interfaces

Aangezien de SFR-module slechts een module is die op de ASA Firewall draait, is het het beste om eerst op de invoer- en spanningsinterfaces van de ASA te klikken om ervoor te zorgen dat dezelfde pakketten die ook in de lucht komen, worden opgenomen.

Dit artikel bevat instructies over hoe de opnamen op de ASA moeten worden uitgevoerd.

Als is vastgesteld dat de pakketten die de ASA niet tegenkomen, doorgaan naar de volgende fase in het oplossen van problemen (de DAQ fase).

> Opmerking: Als pakketten op de ASA INGress interface worden gezien, is het mogelijk de moeite waard om de aangesloten apparaten te controleren.

FTD (niet-SSP en FPR-2100) - Capture on the Ingress and Egress Interfaces

Het opnemen op een niet-SSP FTD apparaat is vergelijkbaar met het opnemen op de ASA. U kunt de Opname-opdrachten echter rechtstreeks vanuit de CLI-initiële melding uitvoeren. Wanneer u problemen oplossen met gedropte pakketten, is het raadzaam de optie "overtrekken" aan de opname toe te voegen.

Hier is een voorbeeld van het configureren van een inbraakopname voor TCP-verkeer op poort 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>
```

Als u de optie "overtrekken" toevoegt, kunt u vervolgens een afzonderlijk pakket selecteren om door het systeem te overtrekken om te zien hoe het tot de uiteindelijke beslissing is gekomen. Het helpt ook om ervoor te zorgen dat de juiste wijzigingen worden aangebracht in het pakket, zoals NAT-aanpassing (Network adresomzetting) IP en dat de juiste IP-interface is geselecteerd.

```
> 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
```

In het bovenstaande voorbeeld zien we dat het verkeer tot snorinspectie leidt en dat het uiteindelijk tot een oordeel kwam en over het geheel genomen door het apparaat werd gepasseerd. Aangezien het verkeer in beide richtingen kan worden gezien, kunt u er zeker van zijn dat het verkeer door het apparaat voor deze sessie stroomt, zodat een drukopname misschien niet nodig is, maar u kunt er ook een nemen om er zeker van te zijn dat het verkeer correct werkt zoals in de sporenuitvoer wordt getoond.

> Opmerking: Als het apparaat niet in staat is om het strips-pakket te maken, staat de overtrek-handeling nog steeds "toe", maar het pakket wordt niet aangemaakt of gezien op de video-opname. Dit is een veel voorkomend scenario waarin de FTD geen ARP ingang voor de volgende hop of bestemming IP heeft (als deze laatste direct verbonden is).

FTD (SSP) - Capture on the Logical FTD Interfaces

Dezelfde stappen om een pakketvastlegging op de FTD te genereren zoals hierboven vermeld, kunnen op een SSP-platform worden gevolgd. U kunt met behulp van SSH verbinding maken met het IP-adres van de FTD logische interface en de volgende opdracht invoeren:

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

U kunt ook met de volgende opdrachten naar het FTD logische apparaatshell navigeren vanuit de FXOS-opdrachtmelding:

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

Als een Firepower 9300 wordt gebruikt, kan het modulenummer variëren afhankelijk van welke Security Module gebruikt wordt. Deze modules kunnen tot 3 logische hulpmiddelen ondersteunen.

Als er meerdere exemplaren worden gebruikt, moet de instantie-ID in de "connect" opdracht worden opgenomen. De opdracht Telnet kan worden gebruikt om tegelijkertijd met verschillende instanties te verbinden.

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

Op interfacekaarten controleren

Ook tijdens deze fase kunnen problemen op het interfaceniveau worden gecontroleerd. Dit is vooral handig als er pakketten ontbreken in de interface-opname. Als er interfacefouten worden gezien, kan het controleren van de aangesloten apparaten behulpzaam zijn.

SFR - Controleer ASA-interfaces

Aangezien de FirePOWER-module (SFR) in wezen een virtuele machine is die op een ASA draait, worden de feitelijke ASA-interfaces op fouten gecontroleerd. Zie dit ASA Series Opdrachtgids sectie voor uitgebreide informatie over het controleren van de interfacestatistieken op de ASA

Series Opdrachtgids.

FTD (niet-SSP en FPR-2100) - Controleer op interfaceresultaten

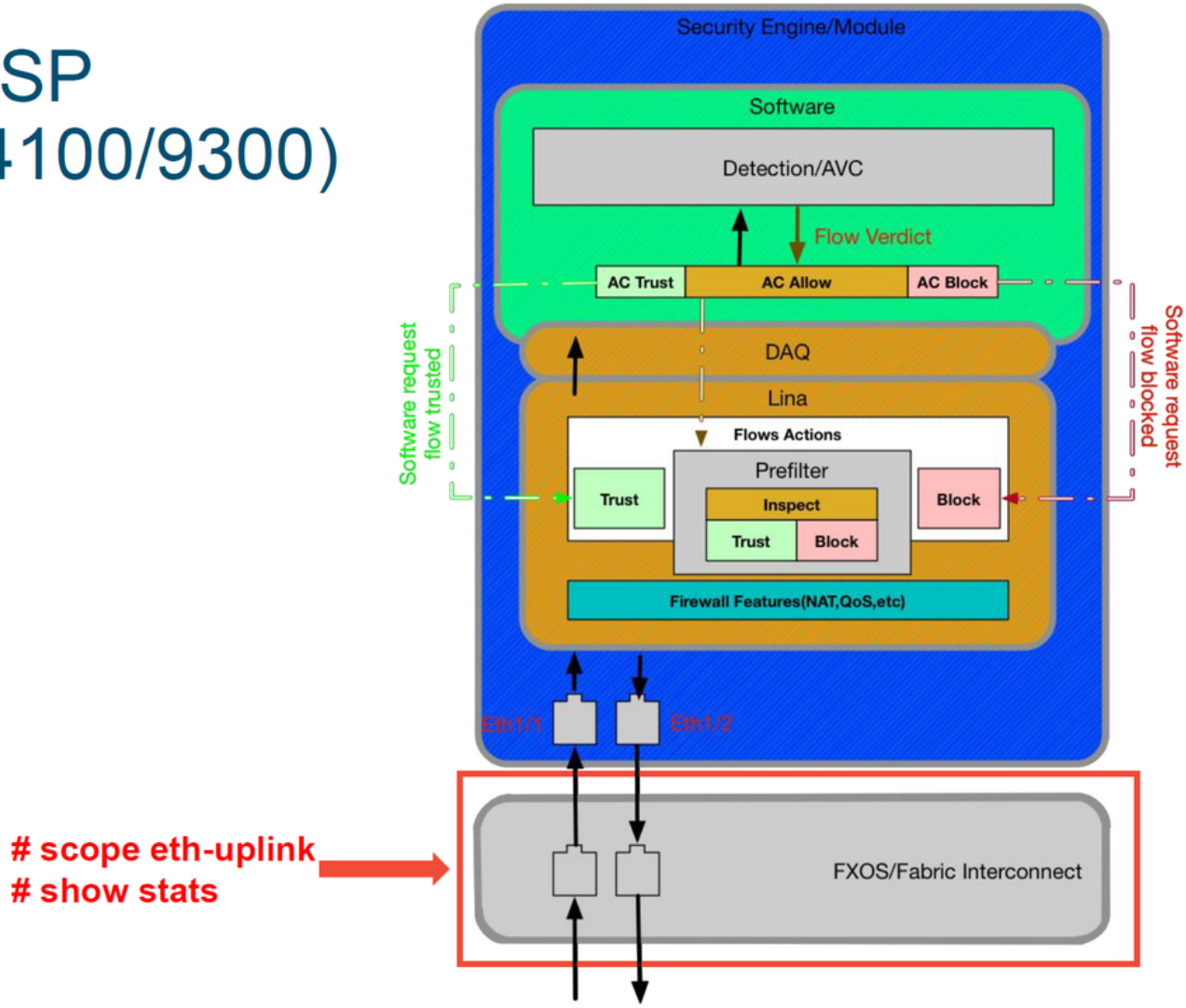
Op niet-SSP FTD-apparaten kan de **> show interface**-opdracht worden uitgevoerd vanaf de eerste opdrachtmelding. De interessante uitvoer wordt in rood gemarkeerd.

```
> 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) - Navigatie in het pad van de Gegevens om interfacekaarten te zoeken

De 9300 en 4100 SSP-platforms hebben een interne fabric interconnect die eerst de pakketten verwerkt.

SSP (4100/9300)



Het is de moeite waard om te controleren of er interfacekaarten zijn bij de eerste pakketingang. Dit zijn de opdrachten die u op de FXOS-systeemCLI moet uitvoeren om deze informatie te verkrijgen.

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

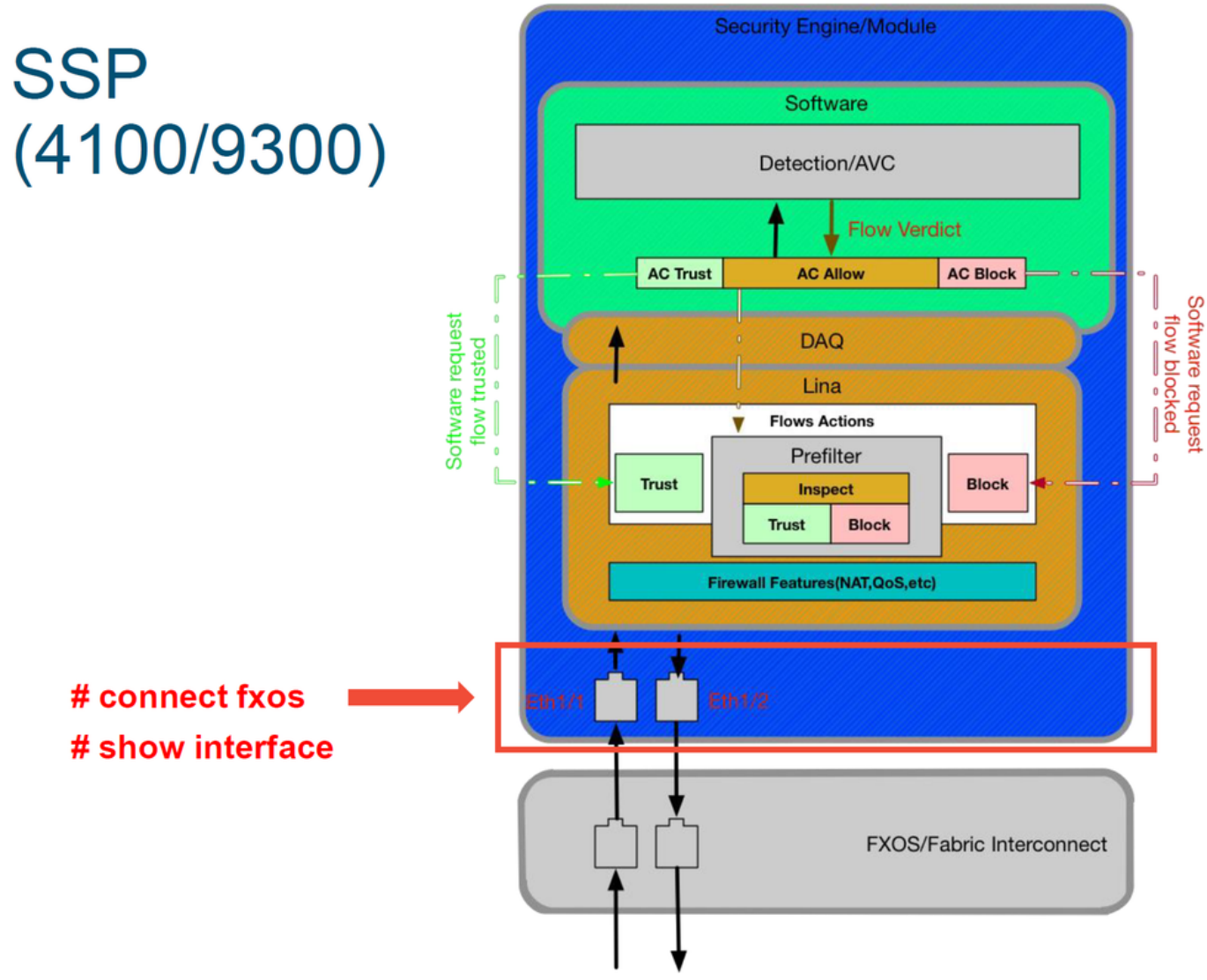
Dit is een voorbeelduitvoer.

```
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
```

Nadat de fabric interconnect het pakje bij invoer verwerkt, wordt deze vervolgens verzonden naar de interfaces die zijn toegewezen aan het logische apparaat dat het FTD-apparaat gastheer ontvangt.

Hier is een diagram ter referentie:



Ga als volgt te controleren op problemen met het interfaceniveau:

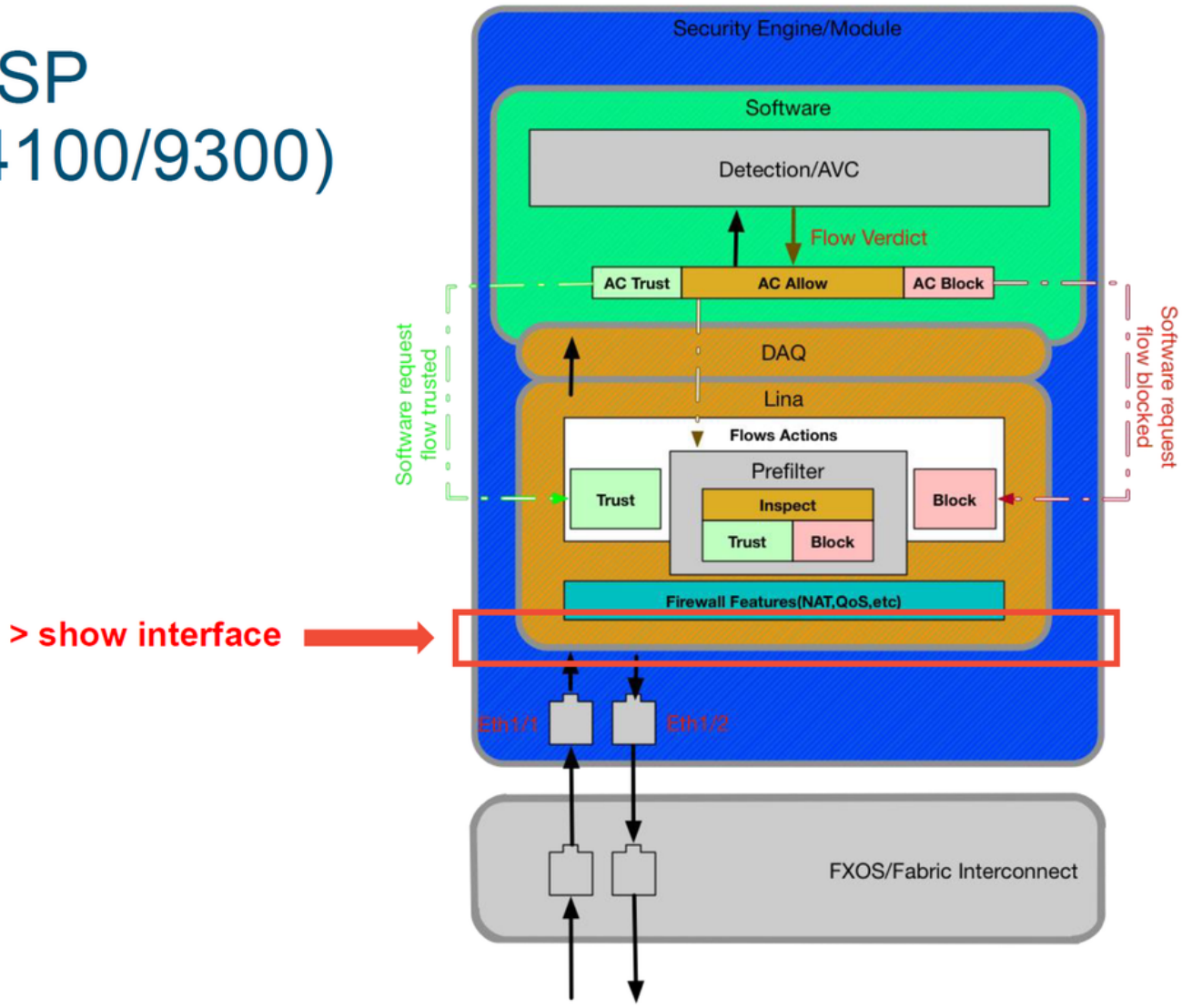
```
ssp# connect fxos
ssp(fxos)# show interface Ethernet 1/7
```

Dit is een uitvoervoorbeeld (mogelijke problemen worden in rood gemarkeerd):

```
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
```

Als er fouten worden gezien, kan de eigenlijke FTD-software ook worden gecontroleerd op interfacefouten.

SSP (4100/9300)



Om de FTD-prompt te bereiken, moet eerst naar de FTD CLI-prompt worden gevlogen.

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

Voor meerdere gevallen:

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

Dit is een uitvoervoorbeeld.

```
# 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
```

Gegevens om aan Cisco Technical Assistance Center (TAC) te leveren

Gegevens	Instructies
Screenshots van verbindingsgebeurtenissen	Zie dit artikel voor instructies
uitvoer 'interface tonen'	Zie dit artikel voor instructies
Packet Capture	Voor ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-550 firewalls/1180... Voor vuurkracht: http://www.cisco.com/c/en/us/support/docs/security/sourcefir appliances/11777...
ASA 'show tech'-uitvoer	Log in op ASA CLI en de eindsessie wordt opgeslagen op een logbestand. Ty het uitvoerbestand van de eindsessie aan TAC op. Dit bestand kan met deze opdracht op schijf of een extern opslagsysteem wor toontechniek | redirect disk0:/show_tech.log
Probleemoplossing bestand via het FirePOWER-apparaat dat het verkeer controleert	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center

Volgende stap: Probleemoplossing in de FirePOWER DAQ-laag

Als niet duidelijk is of het FirePOWER-apparaat pakketten laat vallen, kan het Firepower-apparaat

zelf worden omzeild om alle FirePOWER-onderdelen tegelijk uit te sluiten. Dit is met name nuttig voor het verzachten van een probleem als het betreffende verkeer het Firepower device probeert te verhullen maar niet verbazingwekkend.

Raadpleeg de volgende fase van probleemoplossing bij FirePOWER-gegevens als volgt: De Firepower DAQ. Klik hier om verder te gaan