Fehlerbehebung für FirePOWER-Datenpfade Phase 1: Paketeingang

Inhalt

Einführung

Dieser Artikel ist Teil einer Reihe von Artikeln, in denen erläutert wird, wie der Datenpfad auf FirePOWER-Systemen systematisch behoben wird, um festzustellen, ob Komponenten von FirePOWER den Datenverkehr beeinträchtigen können. Weitere Informationen zur Architektur von FirePOWER-Plattformen und Links zu anderen Artikeln zur Fehlerbehebung für Datenpfade finden Sie im Übersichtsartikel.

In diesem Artikel wird die erste Phase der Fehlerbehebung für den FirePOWER-Datenpfad, die Phase des Paketeingangs beschrieben.

Plattform-Leitfaden

Die folgende Tabelle beschreibt die in diesem Artikel behandelten Plattformen.

Plattformcode-Name	Beschreibung	Anwendbar Hardware Plattformen	Hinweise
SFR	Installiertes ASA mit FirePOWER Services (SFR)-Modul.	Serie ASA-5500-X	K/A
FTD (nicht	FirePOWER Threat Defense (FTD)-Image	ASA-5500-X-	K/A

SSP und FPR-2100)	auf einer Adaptive Security Appliance (ASA) oder einer virtuellen Plattform installiert	Serie, virtuelle NGFW-Plattformen	
FTD (SSP)	FTD als logisches Gerät auf einem FXOS-basierten Chassis (FirePOWER eXtensible Operative System) installiert	FPR-9300, FPR-4100, FPR-2100	Die Serie 2100 verwendet den FXOS Chassis Manager nicht.

Fehlerbehebung in der Phase des Paketeingangs

Der erste Schritt zur Fehlerbehebung bei Datenpfaden besteht darin, sicherzustellen, dass es bei der Ein- oder Ausgangs-Paketverarbeitung keine Paketverluste gibt. Wenn ein Paket eingeht, aber nicht ausgeht, können Sie sicher sein, dass das Paket vom Gerät an einer Stelle im Datenpfad verworfen wird oder dass das Gerät das Ausgangspaket nicht erstellen kann (z. B. ein fehlender ARP-Eintrag).

Identifizieren des betreffenden Datenverkehrs

Der erste Schritt bei der Fehlerbehebung für die Phase des Paketeingangs besteht in der Isolierung des Datenflusses und der Schnittstellen, die am problematischen Datenverkehr beteiligt sind. Dazu gehören:

Flow-Informationen	Schnittstelleninformationen
Protokoll Quell-IP-Adresse Quell-Port Ziel-IP Zielport	Eingangsschnittstelle Ausgangsschnittstelle

Beispiel:

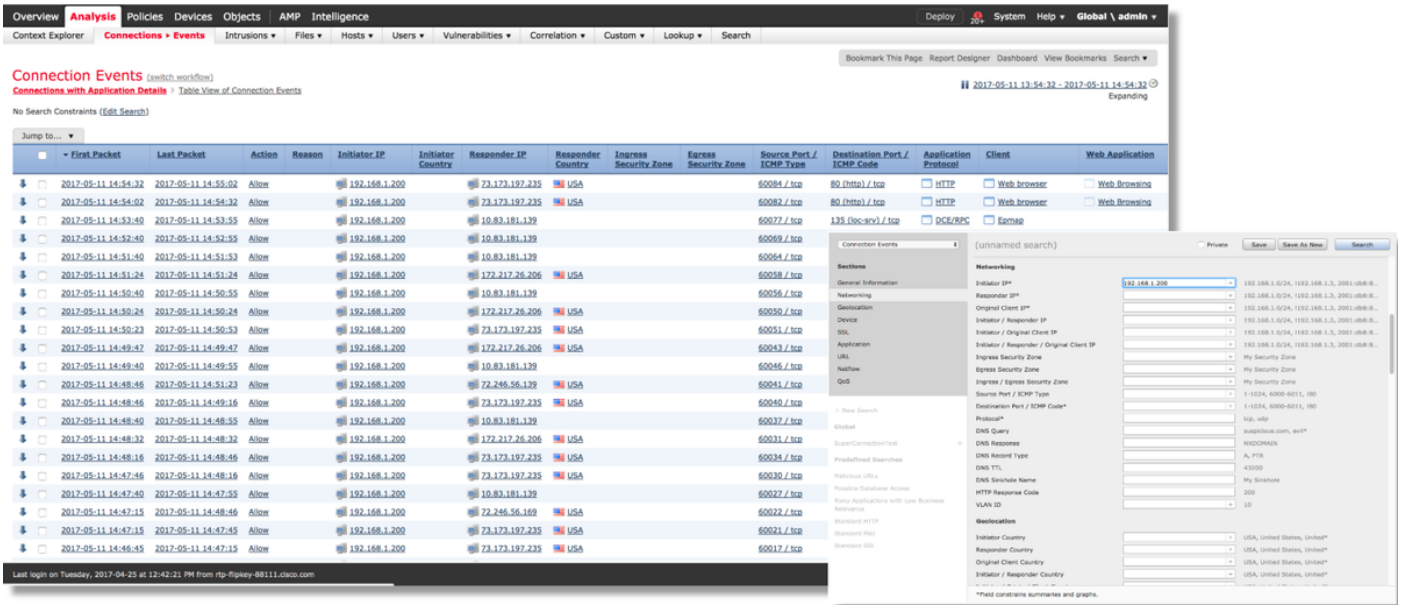
```
TCP inside 172.16.100.101:38974 outside 192.168.1.10:80
```

> **Tipp**: Möglicherweise können Sie den genauen Quell-Port nicht identifizieren, da er in jedem Fluss oft unterschiedlich ist, aber der Ziel-Port (Server) sollte ausreichen.

Auf Verbindungsvereignisse prüfen

Nachdem Sie eine Vorstellung von der Eingangs- und Ausgangsschnittstelle erhalten haben, sollten der Datenverkehr und die Flussinformationen übereinstimmen. Der erste Schritt zu ermitteln, ob FirePOWER den Datenfluss blockiert, besteht darin, die Verbindungsereignisse für den betreffenden Datenverkehr zu überprüfen. Diese können im FirePOWER Management Center unter **Analysis > Connections > Events** angezeigt werden.

> **Hinweis**: Stellen Sie vor der Überprüfung von Connection Events sicher, dass die Protokollierung in den Zugriffskontrollrichtlinien aktiviert ist. Die Protokollierung wird in jeder Zugriffskontrollrichtlinie auf der Registerkarte "Protokollierung" sowie auf der Registerkarte "Sicherheitsinformationen" konfiguriert. Stellen Sie sicher, dass die fehlerverdächtigen Regeln so konfiguriert sind, dass sie die Protokolle an die Ereignisanzeige senden.



Im obigen Beispiel wird auf "Suche bearbeiten" geklickt, und eine eindeutige Quelle (Initiator)-IP wird als Filter hinzugefügt, um die von FirePOWER erkannten Flows anzuzeigen. In der Spalte Aktion wird für diesen Hostverkehr "Zulassen" angezeigt.

Wenn FirePOWER Datenverkehr absichtlich blockiert, enthält die Aktion das Wort "Blockieren". Wenn Sie auf "Table View of Connection Events" (Tabellenansicht von Verbindungsereignissen) klicken, werden weitere Daten angezeigt. Die folgenden Felder in den Connection Events (Verbindungsereignisse) können bei Aktion "Block" (Blockieren) angezeigt werden:

- Grund

- Zugriffskontrollregel

Zusammen mit den anderen Feldern im betreffenden Fall kann dies dazu beitragen, die Komponente einzugrenzen, die den Datenverkehr blockiert.

Weitere Informationen zur Fehlerbehebung bei Zugriffskontrollregeln finden Sie hier.

Erfassen von Paketen auf den Eingangs- und Ausgangsschnittstellen

Wenn keine Ereignisse vorliegen oder die FirePOWER-Firewall trotz der Verbindungsereignisse, die eine Regelaktion mit "Zulassen" oder "Vertrauen" anzeigen, weiterhin blockiert wird, wird die Fehlerbehebung für den Datenpfad fortgesetzt.

Im Folgenden finden Sie Anweisungen zum Ausführen einer Paketerfassung für Ein- und Ausgang auf den oben genannten Plattformen:

SFR - Erfassung auf den ASA-Schnittstellen

Da es sich beim SFR-Modul lediglich um ein Modul handelt, das auf der ASA-Firewall ausgeführt wird, ist es am besten, zunächst die Eingangs- und Ausgangsschnittstellen der ASA zu erfassen, um sicherzustellen, dass dieselben eingehenden Pakete auch aussteigen.

Dieser Artikel enthält Anweisungen zur Durchführung der Erfassung auf der ASA.

Wenn festgestellt wurde, dass die Pakete, die die ASA empfangen, nicht abnehmen, fahren Sie mit der nächsten Phase der Fehlerbehebung fort (der DAQ-Phase).

> **Hinweis**: Wenn Pakete auf der ASA-Eingangsschnittstelle angezeigt werden, lohnt es sich, die angeschlossenen Geräte zu überprüfen.

FTD (Nicht-SSP und FPR-2100) - Erfassung auf den Eingangs- und Ausgangsschnittstellen

Die Erfassung auf einem FTD-Gerät ohne SSP ähnelt der Erfassung auf der ASA. Sie können die Erfassungsbefehle jedoch direkt über die CLI-Eingabeaufforderung ausführen. Bei der Fehlerbehebung verworfener Pakete wird empfohlen, die Option "trace" zur Erfassung hinzuzufügen.

Im folgenden Beispiel wird eine Eingangserfassung für TCP-Datenverkehr an Port 22 konfiguriert:

```
> 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>
```

Wenn Sie die Option "trace" (Nachverfolgung) hinzufügen, können Sie dann ein einzelnes Paket auswählen, das durch das System verfolgt werden soll, um zu sehen, wie es zum endgültigen Urteil gekommen ist. Außerdem wird sichergestellt, dass die richtigen Änderungen am Paket vorgenommen werden, z. B. die Änderung der Network Address Translation (NAT)-IP-Adresse, und dass die richtige Ausgangsschnittstelle gewählt wurde.

```
> 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
```

Im obigen Beispiel sehen wir, dass der Datenverkehr zu Snort Inspection führt und schließlich ein Zulassungsurteil erreicht hat und das Gerät insgesamt durchlaufen wurde. Da der Datenverkehr in beide Richtungen sichtbar ist, können Sie sicherstellen, dass der Datenverkehr für diese Sitzung durch das Gerät fließt. Eine Erfassung des Dateneingangs ist daher nicht erforderlich. Sie können jedoch auch einen Datenverkehr dorthin nehmen, um sicherzustellen, dass der Datenverkehr ordnungsgemäß ansteigt, wie in der Ablaufverfolgungsausgabe gezeigt.

> **Hinweis**: Wenn das Gerät das Ausgangspaket nicht erstellen kann, ist die Ablaufverfolgungsaktion weiterhin "zugelassen", aber das Paket wird nicht in der Erfassung der Ausgangsschnittstelle erstellt oder angezeigt. Dies ist ein sehr verbreitetes Szenario, bei dem die FTD keinen ARP-Eintrag für die nächste Hop- oder Ziel-IP-Adresse hat (wenn diese letzte direkt verbunden ist).

FTD (SSP) - Erfassung auf den logischen FTD-Schnittstellen

Auf einer SSP-Plattform können die gleichen Schritte zur Erstellung einer Paketerfassung in FTD wie oben erwähnt ausgeführt werden. Sie können über SSH eine Verbindung mit der IP-Adresse der logischen FTD-Schnittstelle herstellen und den folgenden Befehl eingeben:

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

Mithilfe der folgenden Befehle können Sie auch über die FXOS-Eingabeaufforderung zur Shell für logische FTD-Geräte navigieren:

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

Wenn eine FirePOWER 9300 verwendet wird, kann die Modulnummer variieren, je nachdem, welches Sicherheitsmodul verwendet wird. Diese Module können bis zu drei logische Geräte unterstützen.

Wenn mehrere Instanzen verwendet werden, muss die Instanz-ID im Befehl "connect" (Verbinden) enthalten sein. Der Telnet-Befehl kann verwendet werden, um gleichzeitig eine Verbindung zu verschiedenen Instanzen herzustellen.

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

Auf Schnittstellenfehler prüfen

Probleme auf Schnittstellenebene können während dieser Phase ebenfalls überprüft werden. Dies ist besonders dann hilfreich, wenn bei der Erfassung der Eingangsschnittstellen Pakete fehlen. Wenn Schnittstellenfehler auftreten, kann es hilfreich sein, die angeschlossenen Geräte zu überprüfen.

SFR - ASA-Schnittstellen prüfen

Da das FirePOWER (SFR)-Modul im Grunde ein virtuelles System ist, das auf einer ASA ausgeführt wird, werden die ASA-Schnittstellen tatsächlich auf Fehler überprüft. Ausführliche Informationen zum Überprüfen der Schnittstellenstatistiken auf der ASA finden Sie in diesem Abschnitt der ASA-Serien-Befehlsreferenz.

FTD (Nicht-SSP und FPR-2100) - Auf Schnittstellenfehler prüfen

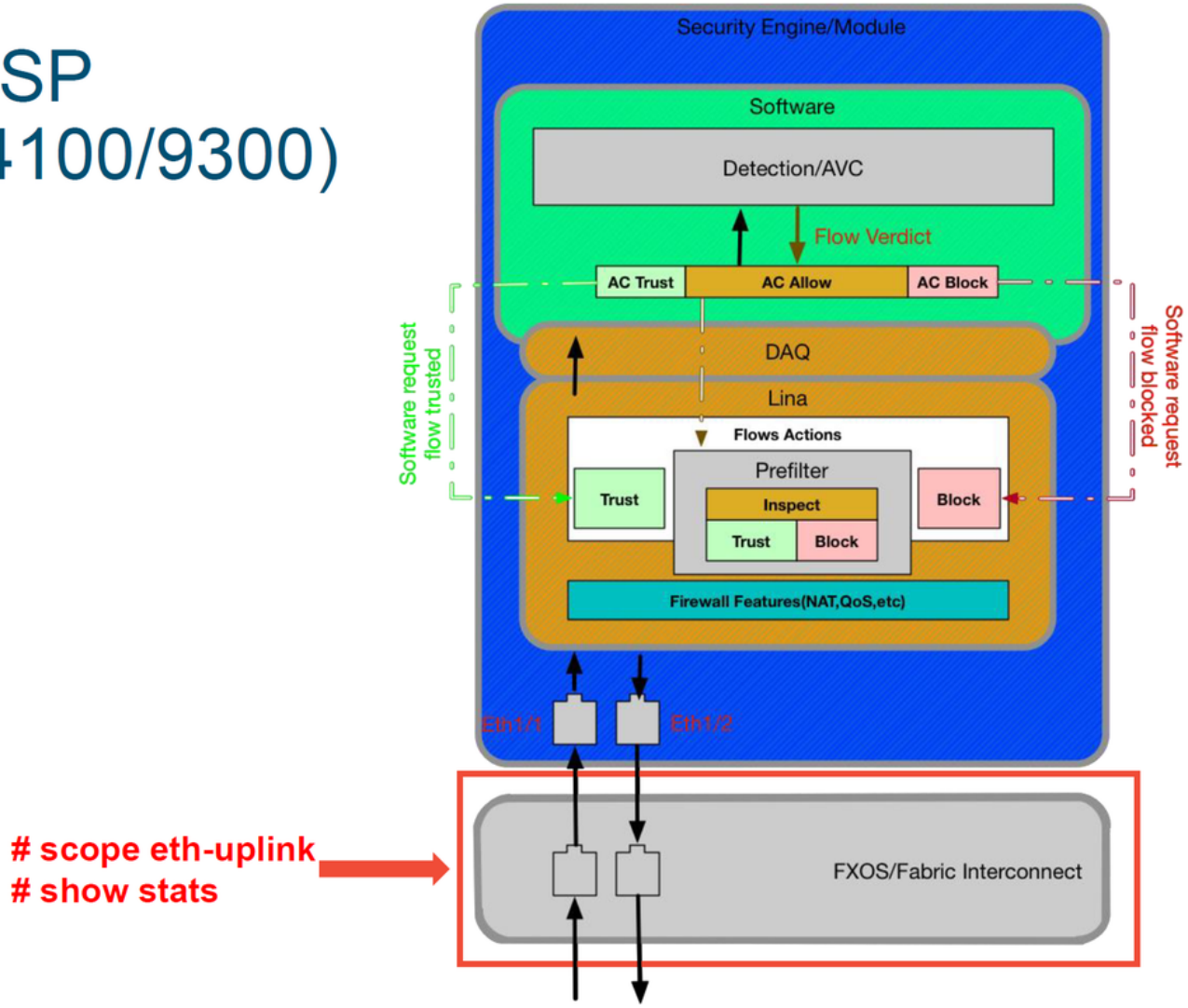
Auf FTD-Geräten ohne SSP kann der Befehl **> show interface** über die erste Eingabeaufforderung ausgeführt werden. Die interessante Ausgabe wird rot hervorgehoben.

```
> 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) - Navigieren im Datenpfad zur Suche nach Schnittstellenfehlern

Die SSP-Plattformen 9300 und 4100 verfügen über ein internes Fabric Interconnect, das die Pakete zuerst behandelt.

SSP (4100/9300)



Es lohnt sich zu überprüfen, ob beim ersten Paketeingang Schnittstellenprobleme auftreten. Dies sind die Befehle, die in der FXOS-System-CLI ausgeführt werden müssen, um diese Informationen abzurufen.

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

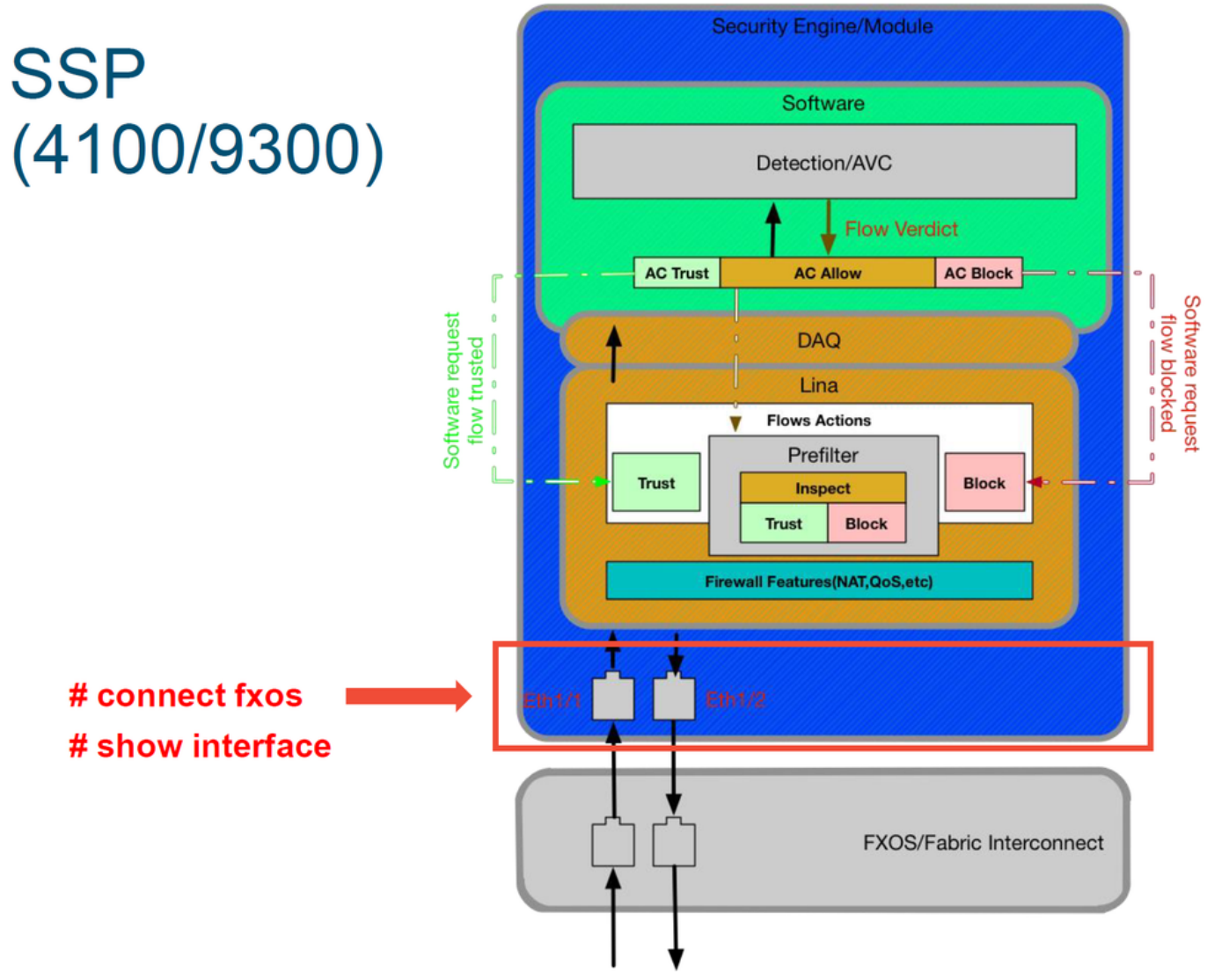
Dies ist eine Beispielausgabe.

```
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
```

Nachdem das Fabric Interconnect das Paket beim Eingang behandelt, wird es an die Schnittstellen gesendet, die dem logischen Gerät zugewiesen sind, das das FTD-Gerät hostet.

Nachstehend finden Sie ein Referenzdiagramm:



Geben Sie die folgenden Befehle ein, um nach Problemen auf Schnittstellenebene zu suchen:

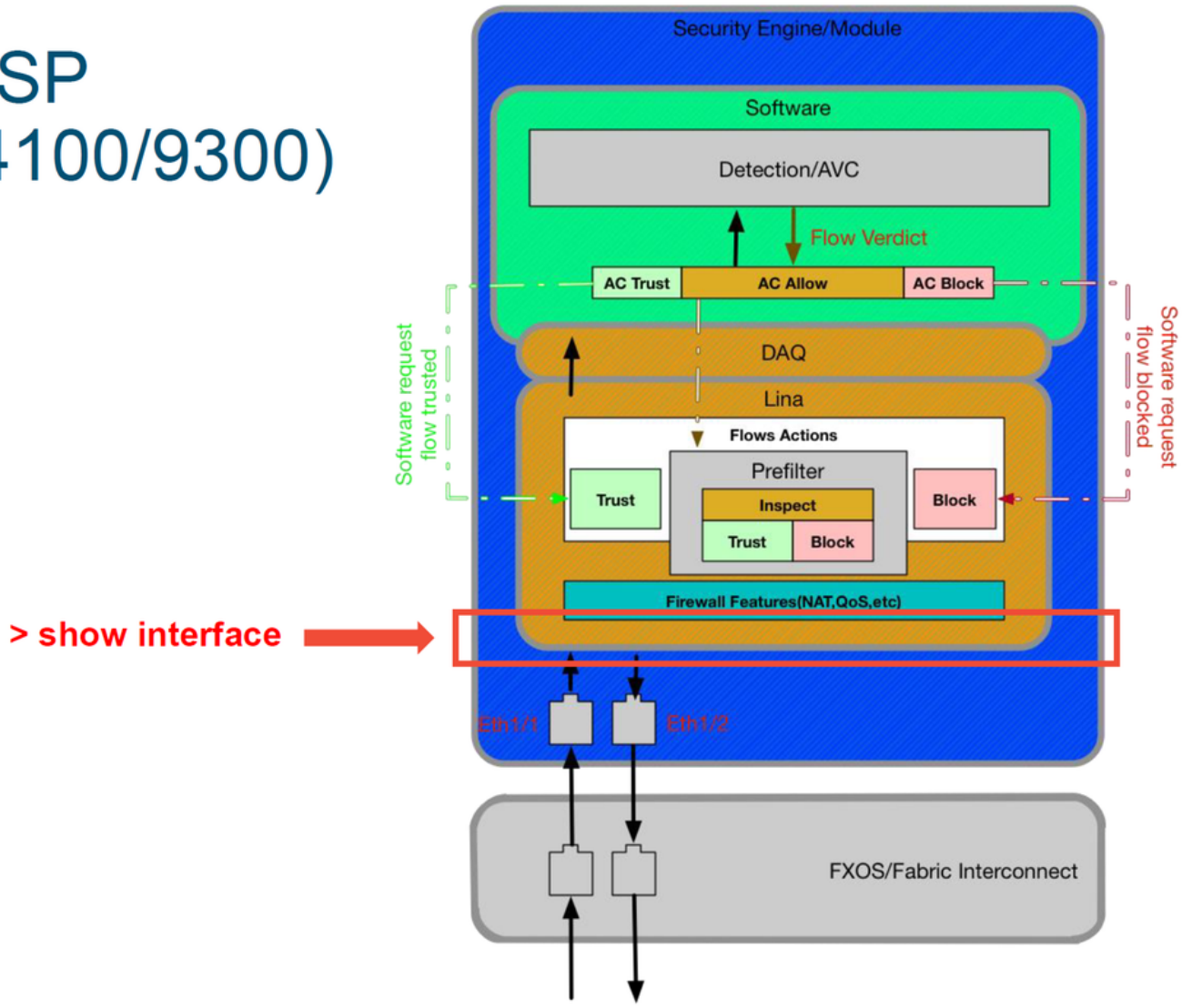
```
ssp# connect fxos
ssp(fxos)# show interface Ethernet 1/7
```

Dies ist ein Ausgabebeispiel (mögliche Probleme sind rot markiert):

```
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
```

Falls Fehler auftreten, kann die FTD-Software auch auf Schnittstellenfehler überprüft werden.

SSP (4100/9300)



Um zur FTD-Eingabeaufforderung zu gelangen, muss zuerst die CLI-Eingabeaufforderung FTD aufgerufen werden.

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

Für mehrere Instanzen:

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

Dies ist ein Ausgabebeispiel.

```
# 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
```

Daten für das Cisco Technical Assistance Center (TAC)

Daten	Anweisungen
Screenshots für Verbindungsereignisse	Anweisungen hierzu finden Sie in diesem Artikel
Ausgabe von 'show interface'	Anweisungen hierzu finden Sie in diesem Artikel
Paketerfassung	Für ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-s firewalls/1180 Für FirePOWER: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-fi appliances/11777
ASA-Ausgabe "show tech"	Melden Sie sich bei der ASA CLI an, und lassen Sie die Terminalsitzung in einem den Befehl **show tech** ein, und stellen Sie dann die Ausgabedatei der Terminalsitz Diese Datei kann mit diesem Befehl auf der Festplatte oder einem externen Speic Showtechnik | Redirect disk0:/show_tech.log
Fehlerbehebungsdatei vom FirePOWER-Gerät, die den Datenverkehr prüft	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117

Nächster Schritt: Fehlerbehebung für die FirePOWER-DAQ-Ebene

Wenn unklar ist, ob das FirePOWER-Gerät Pakete verwirft, kann das FirePOWER-Gerät selbst umgangen werden, um alle FirePOWER-Komponenten gleichzeitig auszuschließen. Dies ist besonders hilfreich, um ein Problem zu beheben, wenn der betreffende Datenverkehr das FirePOWER-Gerät empfängt, aber nicht absteigt.

Lesen Sie zum Fortfahren die nächste Phase der Fehlerbehebung für den FirePOWER-Datenpfad. Die FirePOWER-DAQ. Klicken Sie hier, um fortzufahren.