Fase 1 della risoluzione dei problemi relativi al percorso dei dati di Firepower: Pacchetto in ingresso

Sommario

Introduzione

Questo articolo fa parte di una serie di articoli che spiegano come risolvere in modo sistematico i problemi relativi al percorso dei dati nei sistemi Firepower per determinare se i componenti di Firepower possono influire sul traffico. Per informazioni sull'architettura delle piattaforme Firepower e per i collegamenti agli altri articoli sulla risoluzione dei problemi relativi ai percorsi di dati, consultare l'articolo di panoramica.

In questo articolo, esamineremo la prima fase della risoluzione dei problemi del percorso dati di Firepower, la fase Packet Ingress.

Guida alla piattaforma

Nella tabella seguente vengono descritte le piattaforme descritte in questo articolo.

Nome codice piattaforma	Descrizione	Applicabile Hardware Piattaforme	Note
SFR	ASA con modulo FirePOWER Services	Serie ASA-5500-	N/D

	(SFR) installato.	X	
FTD (non SSP e FPR-2100)	Immagine Firepower Threat Defense (FTD) installata su un'appliance ASA (Adaptive Security Appliance) o una piattaforma virtuale	ASA serie 5500-X, piattaforme NGFW virtuali	N/D
FTD (SSP)	FTD installato come dispositivo logico su uno chassis basato su Firepower eXtensible Operative System (FXOS)	FPR-9300, FPR-4100, FPR-2100	La serie 2100 non utilizza FXOS Chassis Manager

Risoluzione dei problemi della fase di ingresso dei pacchetti

Il primo passaggio per la risoluzione dei problemi relativi al percorso dei dati consiste nell'assicurarsi che non si verifichino perdite in entrata o in uscita durante l'elaborazione dei pacchetti. Se un pacchetto è in entrata ma non in uscita, è possibile verificare che il pacchetto sia stato scartato dal dispositivo in un punto qualsiasi del percorso dati o che il dispositivo non sia in grado di creare il pacchetto in uscita (ad esempio, una voce ARP mancante).

Identificare il traffico in questione

Il primo passo per risolvere i problemi nella fase di ingresso del pacchetto è isolare il flusso e le interfacce coinvolte nel traffico che causa il problema. Ciò include:

Informazioni sul flusso	Informazioni interfaccia
Protocollo Source IP Address Porta di origine IP di destinazione Porta di destinazione	Interfaccia in ingresso Interfaccia in uscita

Ad esempio:

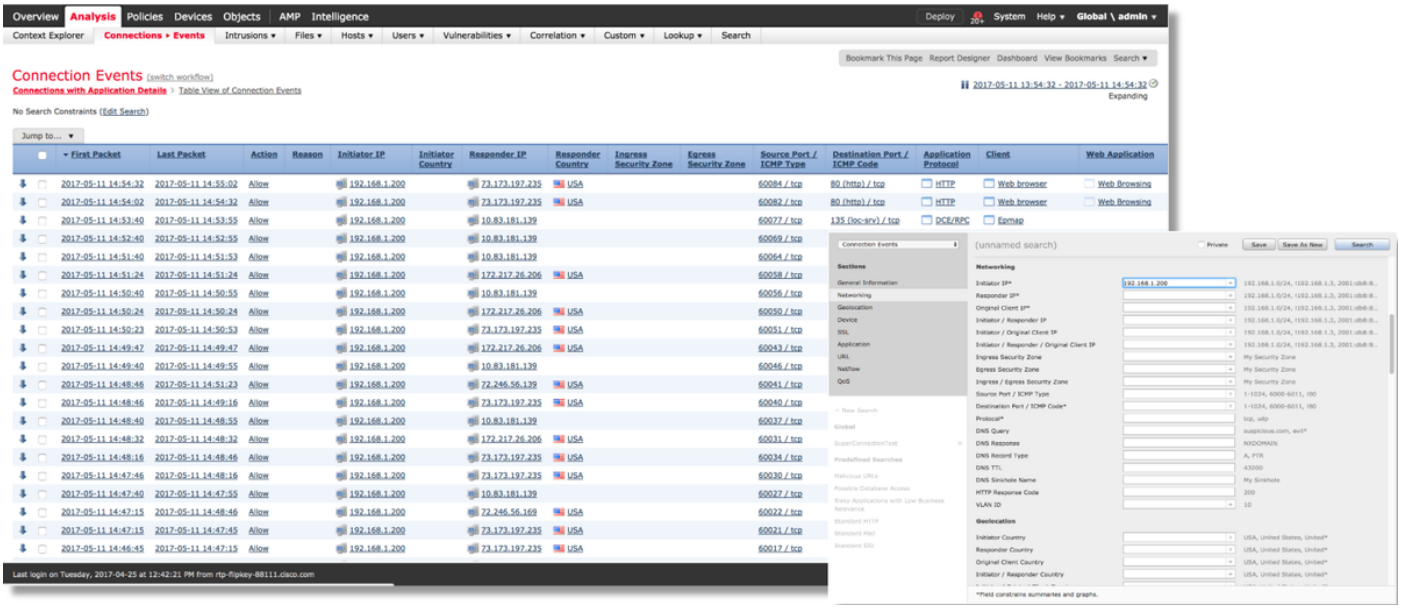
```
TCP inside 172.16.100.101:38974 outside 192.168.1.10:80
```

> **Suggerimento**: Potrebbe non essere possibile identificare la porta di origine esatta perché è spesso diversa in ogni flusso, ma la porta di destinazione (server) dovrebbe essere sufficiente.

Verifica eventi connessione

Dopo aver avuto un'idea dell'interfaccia in entrata e in uscita, il traffico deve corrispondere, così come le informazioni sul flusso, il primo passo per stabilire se Firepower sta bloccando il flusso è controllare gli eventi di connessione per il traffico in questione. È possibile visualizzarle in Firepower Management Center in **Analisi > Connessioni > Eventi**

> **Nota:** Prima di controllare gli eventi di connessione, verificare che la registrazione sia attivata nelle regole dei criteri di controllo di accesso. La registrazione è configurata nella scheda "Registrazione" all'interno di ciascuna regola dei criteri di controllo di accesso e nella scheda Security Intelligence. Verificare che le regole sospette siano configurate per l'invio dei registri al "Visualizzatore eventi".



Nell'esempio precedente, si fa clic su "Edit Search" (Modifica ricerca) e si aggiunge un indirizzo IP di origine univoco (Iniziatore) come filtro per visualizzare i flussi rilevati da Firepower. Nella colonna Azione viene visualizzato "Consenti" per il traffico host.

Se Firepower blocca intenzionalmente il traffico, l'azione conterrà la parola "Blocca". Facendo clic su "Table View of Connection Events" vengono forniti ulteriori dati. Se l'azione è "Blocca", è possibile annotare i campi seguenti negli eventi di connessione:

- Motivo

- Regola di controllo di accesso

Questa funzionalità, combinata con gli altri campi dell'evento, consente di individuare il componente che blocca il traffico.

Per ulteriori informazioni sulla risoluzione dei problemi relativi alle regole di controllo di accesso, fare clic qui.

Cattura di pacchetti sulle interfacce in entrata e in uscita

Se non sono presenti eventi o si sospetta che Firepower sia ancora bloccato nonostante in Eventi connessione sia visualizzata un'azione regola "Consenti" o "Attendibilità", la risoluzione dei problemi relativi al percorso dati continua.

Di seguito sono riportate le istruzioni su come eseguire l'acquisizione dei pacchetti in entrata ed in uscita sulle varie piattaforme sopra menzionate:

SFR - Acquisizione sulle interfacce ASA

Poiché il modulo SFR è semplicemente un modulo in esecuzione sul firewall ASA, la soluzione migliore è catturare le informazioni sulle interfacce in entrata e in uscita dell'appliance ASA per essere certi che anche i pacchetti in entrata escano.

In questo documento viene spiegato come eseguire le acquisizioni sull'appliance ASA.

Se è stato stabilito che i pacchetti in entrata sull'appliance ASA non stanno andando verso l'alto, procedere alla fase successiva della risoluzione dei problemi (la fase DAQ).

> **Nota:** Se si rilevano pacchetti sull'interfaccia in entrata dell'ASA, potrebbe essere utile controllare i dispositivi collegati.

FTD (non SSP e FPR-2100) - Acquisizione sulle interfacce in entrata e in uscita

La cattura su un dispositivo FTD non SSP è simile alla cattura sull'appliance ASA. Tuttavia, è possibile eseguire i comandi di acquisizione direttamente dal prompt iniziale della CLI. Quando si risolvono i problemi relativi ai pacchetti scartati, si consiglia di aggiungere l'opzione "trace" all'acquisizione.

Di seguito è riportato un esempio di configurazione di un'acquisizione in entrata per il traffico TCP sulla porta 2:

```
> 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>
```

Aggiungendo l'opzione "trace", è possibile selezionare un singolo pacchetto da tracciare nel sistema per verificare come è giunto al verdetto finale. Inoltre, aiuta a verificare che vengano apportate le modifiche appropriate al pacchetto, ad esempio la modifica IP NAT (Network Address Translation), e che sia stata scelta l'interfaccia di uscita appropriata.

```
> 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
```

Nell'esempio di cui sopra, vediamo che il traffico lo fa a Snort ispezione e che ha finalmente raggiunto un verdetto permesso e complessivamente è stato passato attraverso il dispositivo. Poiché il traffico può essere visualizzato in entrambe le direzioni, è possibile verificare che scorra attraverso il dispositivo per questa sessione, quindi potrebbe non essere necessaria un'acquisizione in uscita, ma è possibile acquisirne una in questa posizione per verificare che il traffico stia avanzando correttamente, come mostrato nell'output della traccia.

> **Nota:** Se il dispositivo non è in grado di creare il pacchetto in uscita, l'azione tracerestituisce ancora "consenti" ma il pacchetto non viene creato né visualizzato sull'acquisizione dell'interfaccia di uscita. Si tratta di uno scenario molto comune in cui l'FTD non ha una voce ARP per l'hop successivo o per l'IP di destinazione (se l'ultimo è connesso direttamente).

FTD (SSP) - Acquisizione sulle interfacce FTD logiche

Su una piattaforma SSP è possibile seguire la stessa procedura descritta sopra per generare un'acquisizione di pacchetto su FTD. È possibile connettersi utilizzando SSH all'indirizzo IP dell'interfaccia logica FTD e immettere il comando seguente:

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

Èinoltre possibile passare alla shell del dispositivo logico FTD dal prompt dei comandi FXOS con i comandi seguenti:

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

Se si utilizza Firepower 9300, il numero del modulo può variare a seconda del modulo di sicurezza in uso. Questi moduli possono supportare fino a 3 dispositivi logici.

Se si utilizzano più istanze, l'ID istanza deve essere incluso nel comando "connect". Il comando Telnet può essere utilizzato per connettersi a istanze diverse contemporaneamente.

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

Verifica errori interfaccia

In questa fase è possibile anche controllare i problemi a livello di interfaccia. Questa opzione è utile soprattutto se mancano dei pacchetti nell'acquisizione dell'interfaccia in entrata. Se vengono rilevati errori dell'interfaccia, può essere utile controllare i dispositivi collegati.

SFR - Controllo interfacce ASA

Poiché il modulo FirePOWER (SFR) è fondamentalmente una macchina virtuale in esecuzione su un'ASA, le interfacce ASA effettive vengono controllate per rilevare eventuali errori. Per informazioni dettagliate sul controllo delle statistiche dell'interfaccia sull'appliance ASA, vedere questa sezione della guida di riferimento dei comandi della serie ASA.

FTD (non SSP e FPR-2100) - Controllo errori interfaccia

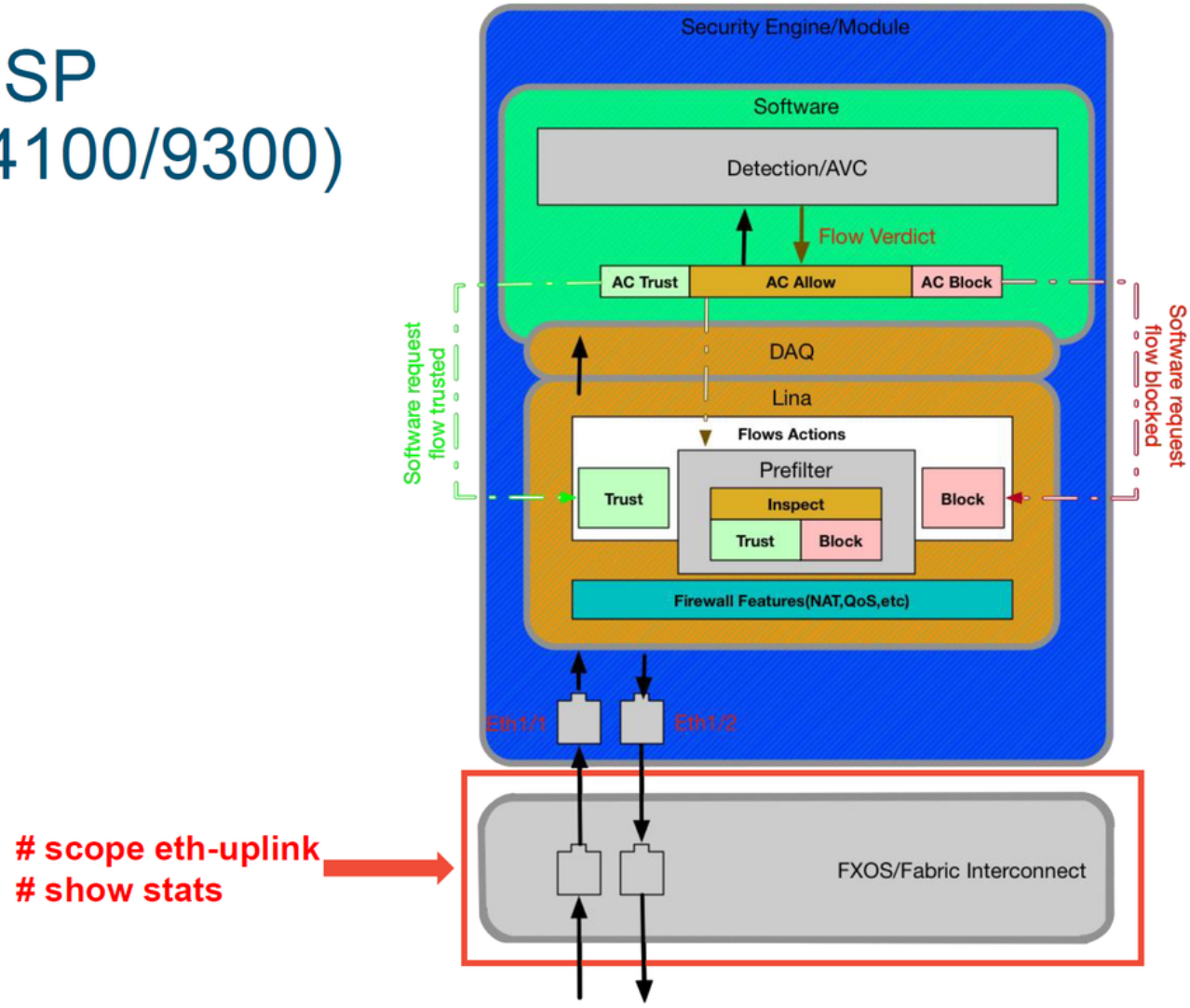
Sui dispositivi FTD non SSP, il comando **> show interface** può essere eseguito dal prompt dei comandi iniziale. L'output interessante viene evidenziato in rosso.

```
> 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) - Esplorazione del percorso dati per la ricerca di errori di interfaccia

Le piattaforme SSP 9300 e 4100 dispongono di un'interconnessione fabric interna che gestisce per prima cosa i pacchetti.

SSP (4100/9300)



Èopportuno verificare la presenza di problemi di interfaccia all'ingresso del pacchetto iniziale. Questi sono i comandi da eseguire sulla CLI del sistema FXOS per ottenere queste informazioni.

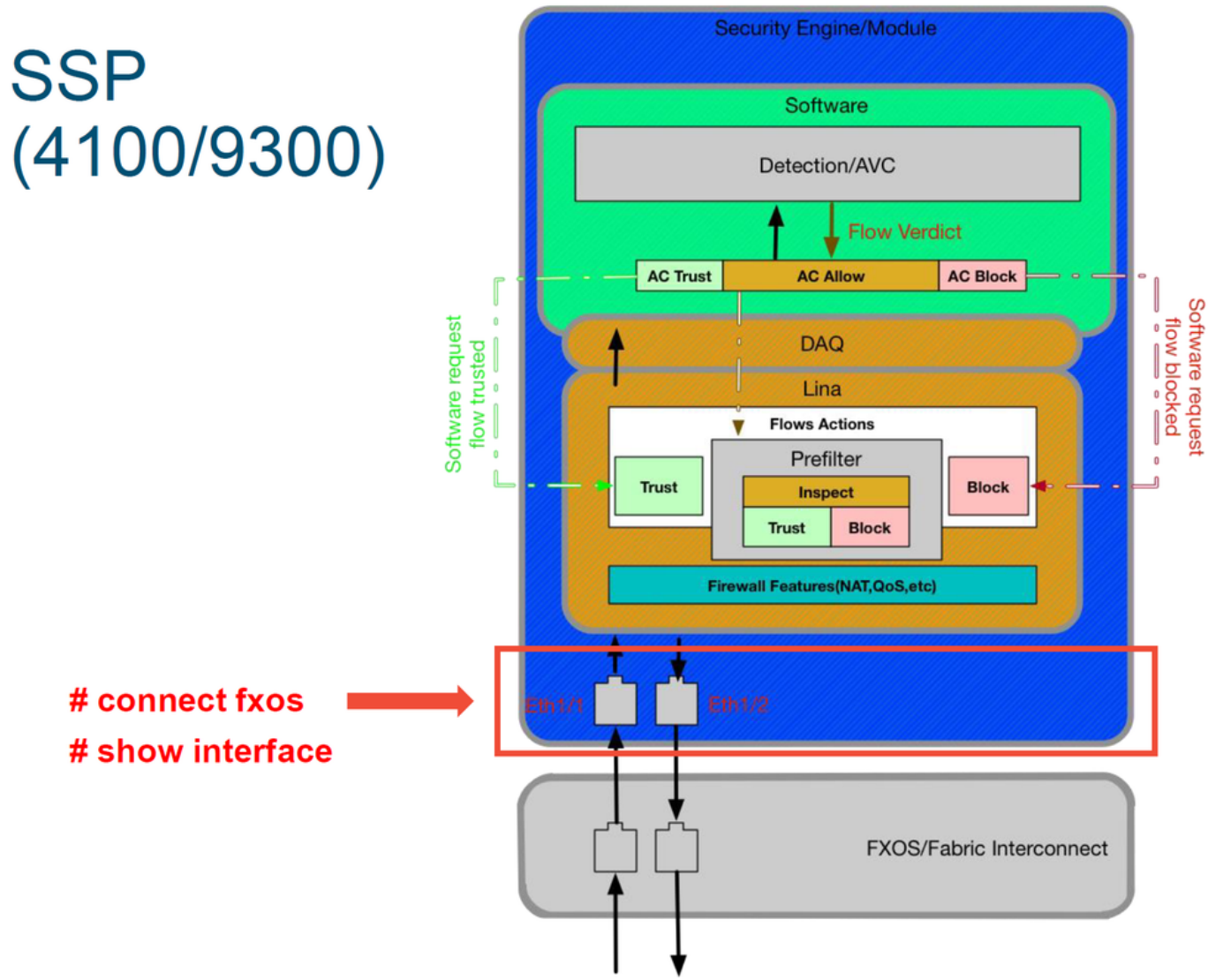
```
ssp# scope eth-uplink
ssp /et-uplink # show stats
```

Questo è un output di esempio.

```
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
```

Dopo che l'interconnessione fabric gestisce il pacchetto all'ingresso, viene inviato alle interfacce assegnate al dispositivo logico che ospita il dispositivo FTD.

Di seguito è riportato un diagramma di riferimento:



Per verificare la presenza di eventuali problemi a livello di interfaccia, immettere i seguenti comandi:

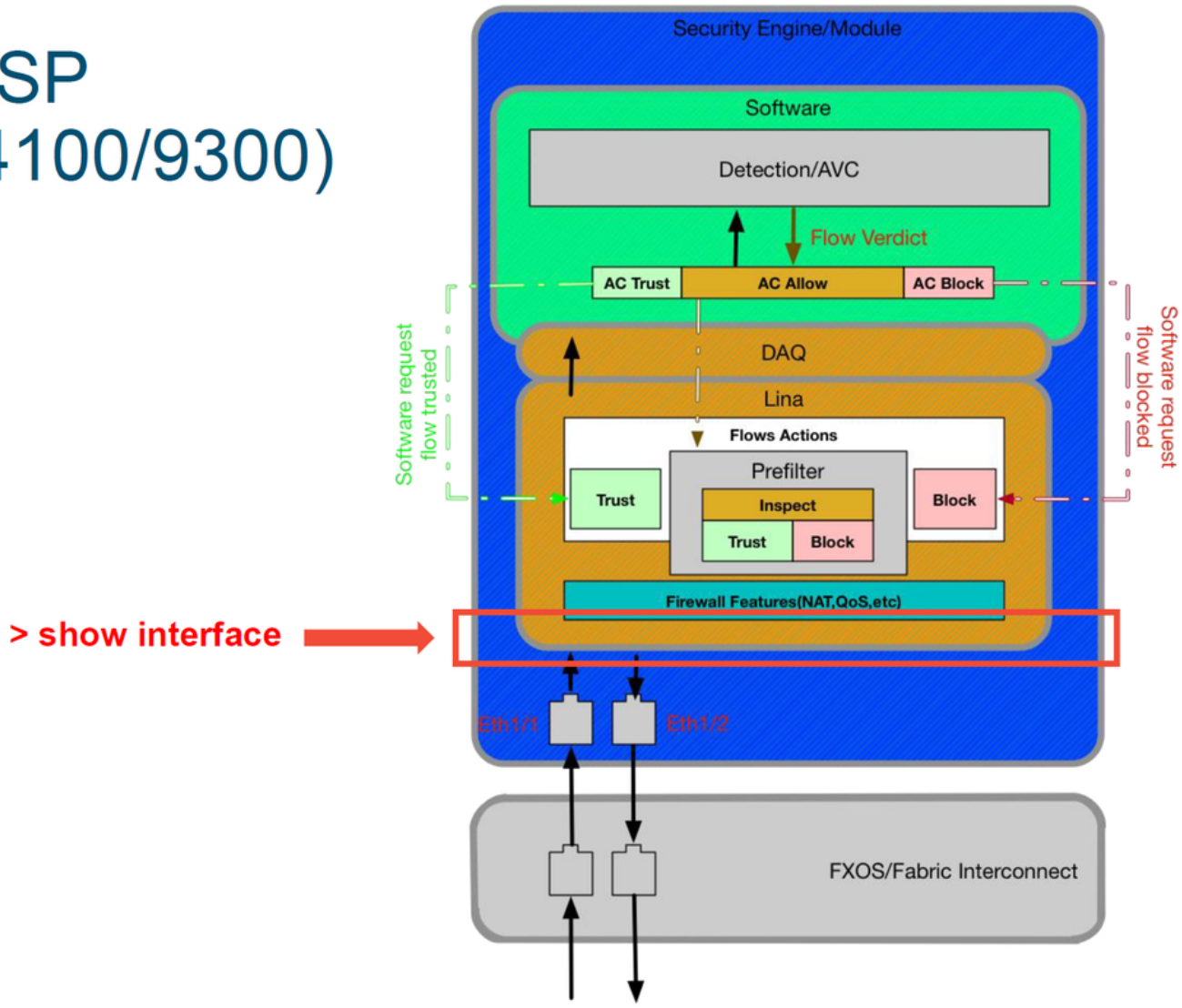
```
ssp# connect fxos
ssp(fxos)# show interface Ethernet 1/7
```

Questo è un esempio di output (i possibili problemi sono evidenziati in rosso):

```
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
```

Se si rilevano errori, è possibile verificare la presenza di errori di interfaccia anche nel software FTD.

SSP (4100/9300)



Per arrivare al prompt FTD, è prima necessario passare al prompt CLI FTD.

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

Per le istanze multiple:

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

Questo è un esempio di output.

```
# 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
```

Dati da fornire al Cisco Technical Assistance Center (TAC)

Dati	Istruzioni
Schermate degli eventi di connessione	Per istruzioni, vedere questo articolo
output 'show interface'	Per istruzioni, vedere questo articolo
Acquisizioni pacchetti	Per ASA/LINA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-firewalls/1180... Per Firepower: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-800-appliances/11777...
Output ASA 'show tech'	Accedere alla CLI di ASA e salvare la sessione terminale in un log. Immettere il comando **sh** di output della sessione terminale a TAC. Questo comando consente di salvare il file su disco o su un sistema di storage esterno. show tech | reindirizzare il disco0:/show_tech.log
Risoluzione dei problemi relativi al file dal dispositivo Firepower per il controllo del	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn

traffico

Passaggio successivo: Risoluzione dei problemi relativi al livello DAQ di Firepower

Se non è chiaro se il dispositivo Firepower sta perdendo pacchetti, può essere ignorato per escludere tutti i componenti Firepower contemporaneamente. Ciò è particolarmente utile per mitigare un problema se il traffico in questione sta entrando nel dispositivo Firepower ma non sta uscendo.

Per continuare, rivedere la fase successiva della risoluzione dei problemi relativi al percorso dati di Firepower; Il DAQ Firepower. Fare clic qui per continuare.