Dépannage du chemin de données Firepower Phase 1 : Paquet entrant

Contenu

Introduction

Cet article fait partie d'une série d'articles qui expliquent comment dépanner systématiquement le chemin de données sur les systèmes Firepower pour déterminer si les composants de Firepower peuvent affecter le trafic. Reportez-vous à l'article Présentation pour obtenir des informations sur l'architecture des plates-formes Firepower et des liens vers les autres articles de dépannage du chemin de données.

Dans cet article, nous allons examiner la première étape du dépannage du chemin de données Firepower, l'étape d'entrée de paquets.

Guide de la plate-forme

Le tableau suivant décrit les plates-formes couvertes par cet article.

Nom du code de la plate-forme	Description	Applicable Matériel Plates-formes	Notes
SFR	Module ASA avec fonctionnalités FirePOWER (SFR) installé.	Gamme ASA-5500-X	S/O
FTD (non	Image Firepower Threat Defense (FTD)	Plates-formes de	S/O

SSP et FPR-2100)	installée sur un appareil de sécurité adaptatif (ASA) ou une plate-forme virtuelle	pare-feu de nouvelle génération virtuelles de la gamme ASA-5500-X	
FTD (SSP)	FTD installé en tant que périphérique logique sur un châssis basé sur Firepower eXtensible Operative System (FXOS)	FPR-9300, FPR-4100, FPR-2100	La gamme 2100 n'utilise pas le gestionnaire de châssis FXOS

Dépannage de la phase d'entrée des paquets

La première étape du dépannage du chemin de données consiste à s'assurer qu'aucune perte ne se produit au stade d'entrée ou de sortie du traitement des paquets. Si un paquet est en train d'entrer, mais pas de sortir, vous pouvez être sûr que le paquet est abandonné par le périphérique à un endroit quelconque du chemin de données ou que le périphérique ne peut pas créer le paquet de sortie (par exemple, une entrée ARP manquante).

Identifier le trafic en question

La première étape du dépannage de l'étape d'entrée de paquets consiste à isoler le flux et les interfaces impliquées dans le trafic problématique. Cela inclut :

Informations de flux	Informations d'interface
Protocol	
adresse IP source	Interface d'entrée
Port source	Interface de sortie
Adresse IP de destination	
Destination Port (port de destination)	

Exemple :

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

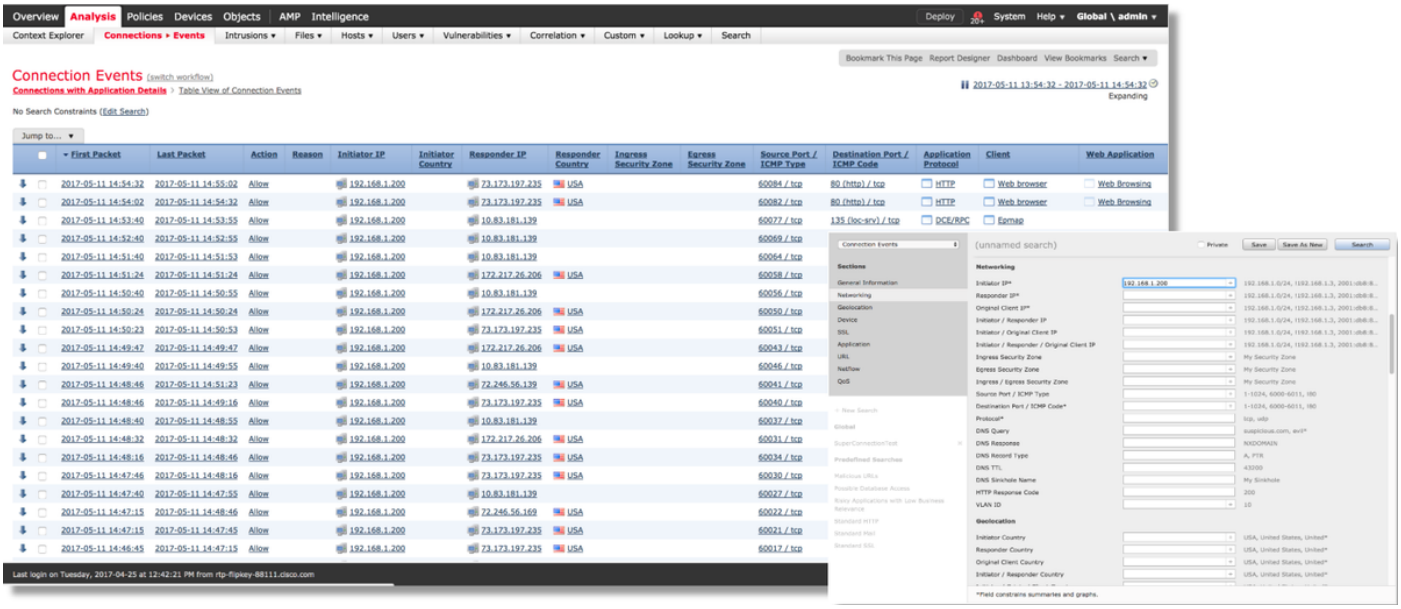
> **Astuce** : Il se peut que vous ne puissiez pas identifier le port source exact car il est souvent différent dans chaque flux, mais le port de destination (serveur) doit suffire.

Vérifier les événements de connexion

Après avoir obtenu une idée de l'interface d'entrée et de sortie, le trafic doit correspondre ainsi que les informations de flux, la première étape pour identifier si Firepower bloque le flux est de vérifier les événements de connexion pour le trafic en question. Ils peuvent être affichés dans Firepower Management Center sous **Analysis > Connections > Events**

> **Note**: Avant de vérifier les événements de connexion, assurez-vous que la journalisation est activée dans vos règles de stratégie de contrôle d'accès. La journalisation est configurée dans l'onglet « Journalisation » de chaque règle de stratégie de contrôle d'accès ainsi que dans l'onglet Security Intelligence. Assurez-vous que les règles suspectes sont configurées

pour envoyer les journaux à l'« Observateur d'événements ».



Dans l'exemple ci-dessus, « Edit Search » est cliqué et une adresse IP source unique (Initiator) est ajoutée comme filtre pour voir les flux détectés par Firepower. La colonne Action indique « Autoriser » pour ce trafic hôte.

Si Firepower bloque intentionnellement le trafic, l'action contient le mot « Bloquer ». Cliquer sur « Affichage table des événements de connexion » fournit plus de données. Les champs suivants des événements de connexion peuvent être notés si l'action est « Bloquer » :

- Motif

- Règle de contrôle d'accès

Ceci, combiné aux autres champs de l'événement en question, peut aider à réduire le composant qui bloque le trafic.

Pour plus d'informations sur le dépannage des règles de contrôle d'accès, cliquez ici.

Capture de paquets sur les interfaces d'entrée et de sortie

S'il n'y a aucun événement ou si Firepower est toujours suspecté de blocage malgré les événements de connexion affichant une action de règle « Autoriser » ou « Approuver », le dépannage du chemin de données se poursuit.

Voici des instructions sur l'exécution d'une capture de paquets d'entrée et de sortie sur les différentes plates-formes mentionnées ci-dessus :

SFR - Capture sur les interfaces ASA

Puisque le module SFR est simplement un module exécuté sur le pare-feu ASA, il est préférable de d'abord capturer sur les interfaces d'entrée et de sortie de l'ASA pour s'assurer que les mêmes paquets qui entrent sont également en sortie.

Cet article contient des instructions sur l'exécution des captures sur l'ASA.

S'il a été déterminé que les paquets qui entrent dans l'ASA ne sortent pas, passez à la phase suivante du dépannage (la phase DAQ).

> **Note**: Si des paquets sont vus sur l'interface d'entrée ASA, il peut être utile de vérifier les périphériques connectés.

FTD (non-SSP et FPR-2100) - Capture sur les interfaces d'entrée et de sortie

La capture sur un périphérique FTD non SSP est similaire à la capture sur l'ASA. Cependant, vous pouvez exécuter les commandes de capture directement à partir de l'invite initiale de l'interface de ligne de commande. Lors du dépannage des paquets abandonnés, il est conseillé d'ajouter l'option « trace » à la capture.

Voici un exemple de configuration d'une capture d'entrée pour le trafic TCP sur le port 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 vous ajoutez l'option « trace », vous pouvez ensuite sélectionner un paquet individuel à suivre dans le système pour voir comment il en est arrivé au verdict final. Il permet également de s'assurer que les modifications appropriées sont apportées au paquet, telles que la modification de l'adresse IP NAT (Network Address Translation) et que l'interface de sortie appropriée a été choisie.

```
> 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
```

Dans l'exemple ci-dessus, nous voyons que le trafic arrive à l'inspection Snort et qu'il a finalement atteint un verdict d'autorisation et que l'ensemble a été passé par le périphérique. Puisque le trafic peut être vu dans les deux directions, vous pouvez être sûr que le trafic traverse le périphérique pour cette session, de sorte qu'une capture de sortie peut ne pas être nécessaire, mais vous pouvez également en prendre une là pour vous assurer que le trafic est en train de passer correctement comme indiqué dans la sortie de trace.

> **Note**: Si le périphérique ne peut pas créer le paquet de sortie, l'action de suivi est toujours « autoriser » mais le paquet n'est pas créé ou visible sur la capture d'interface de sortie. Il s'agit d'un scénario très courant où le FTD ne dispose pas d'entrée ARP pour le prochain saut ou l'adresse IP de destination (si ce dernier est directement connecté).

FTD (SSP) : capture sur les interfaces FTD logiques

Les mêmes étapes pour générer une capture de paquets sur FTD que celles mentionnées ci-dessus peuvent être suivies sur une plate-forme SSP. Vous pouvez vous connecter à l'aide de SSH à l'adresse IP de l'interface logique FTD et entrer la commande suivante :

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

Vous pouvez également accéder au shell de périphérique logique FTD à partir de l'invite de commandes FXOS à l'aide des commandes suivantes :

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

Si un Firepower 9300 est utilisé, le numéro du module peut varier en fonction du module de sécurité utilisé. Ces modules peuvent prendre en charge jusqu'à 3 périphériques logiques.

Si plusieurs instances sont utilisées, l'ID d'instance doit être inclus dans la commande « connect ». La commande Telnet peut être utilisée pour se connecter simultanément à différentes instances.

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

Rechercher les erreurs d'interface

Les problèmes de niveau interface peuvent également être vérifiés au cours de cette phase. Ceci est particulièrement utile si des paquets sont manquants dans la capture d'interface d'entrée. Si des erreurs d'interface sont détectées, la vérification des périphériques connectés peut s'avérer utile.

SFR - Vérifier les interfaces ASA

Puisque le module FirePOWER (SFR) est essentiellement une machine virtuelle exécutée sur un ASA, les interfaces ASA réelles sont vérifiées pour détecter les erreurs. Pour obtenir des

informations détaillées sur la vérification des statistiques d'interface sur l'ASA, reportez-vous à la section du guide de référence des commandes de la gamme ASA.

FTD (non-SSP et FPR-2100) - Rechercher les erreurs d'interface

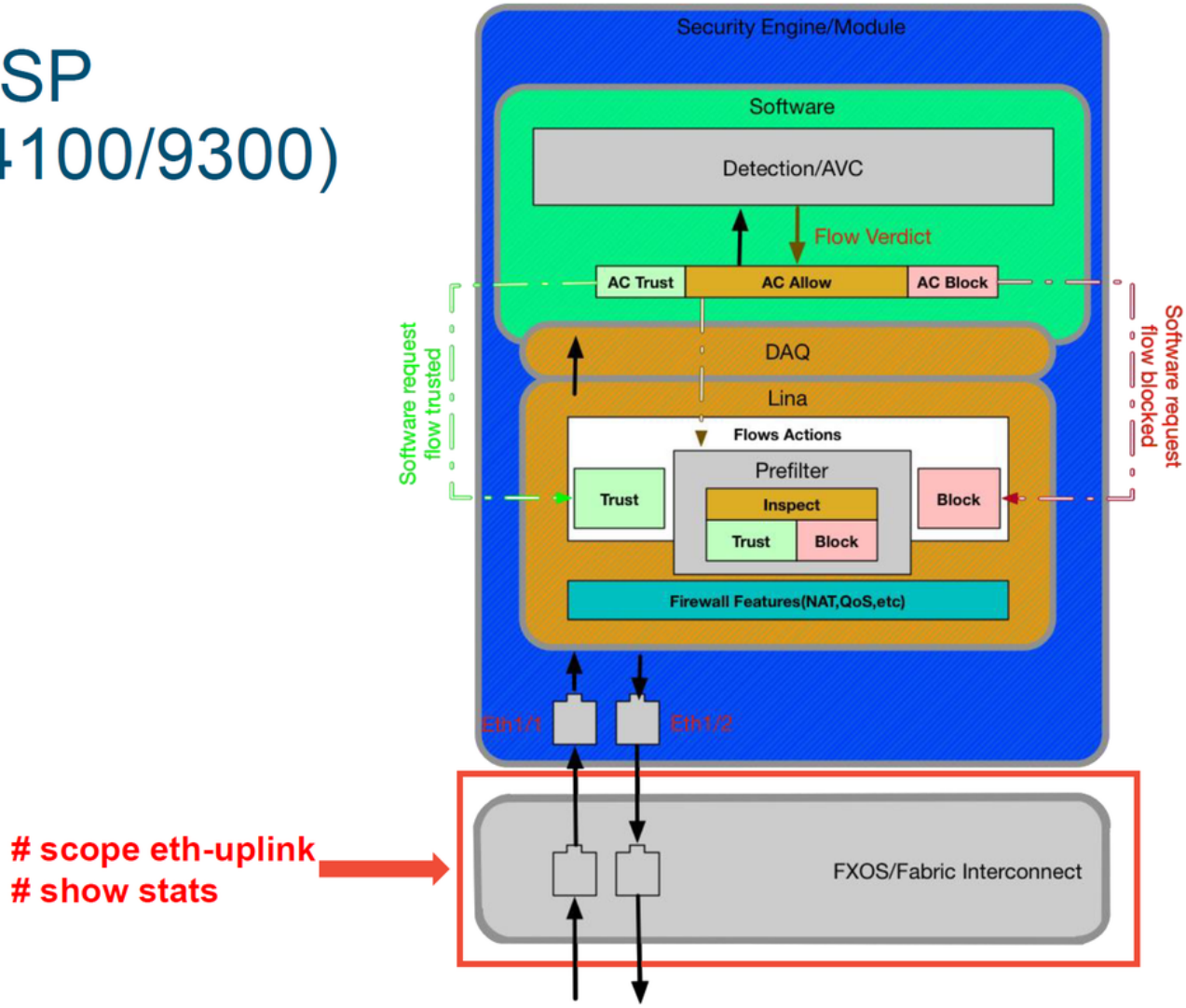
Sur les périphériques FTD non SSP, la commande **> show interface** peut être exécutée à partir de l'invite de commandes initiale. La sortie intéressante est surlignée en rouge.

```
> 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) - Navigation dans le chemin des données pour rechercher les erreurs d'interface

Les plates-formes SSP 9300 et 4100 disposent d'une interconnexion de fabric interne qui gère d'abord les paquets.

SSP (4100/9300)



Il est utile de vérifier s'il y a des problèmes d'interface lors de l'entrée initiale du paquet. Il s'agit des commandes à exécuter sur l'interface de ligne de commande du système FXOS afin d'obtenir ces informations.

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

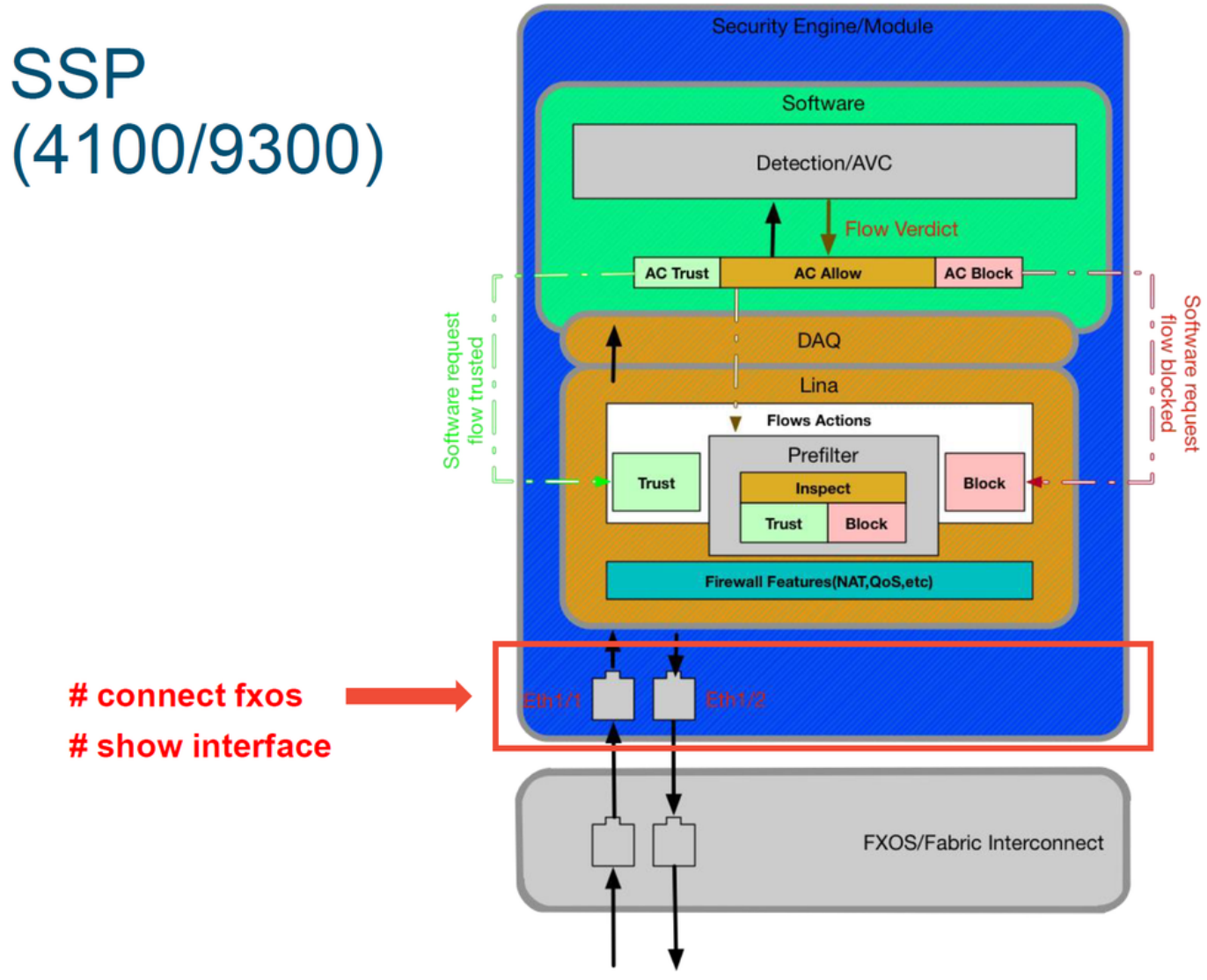
Voici est un exemple de sortie .

```
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
```

Une fois que l'interconnexion de fabric gère le paquet en entrée, il est envoyé aux interfaces qui sont affectées au périphérique logique hébergeant le périphérique FTD.

Voici un schéma de référence :



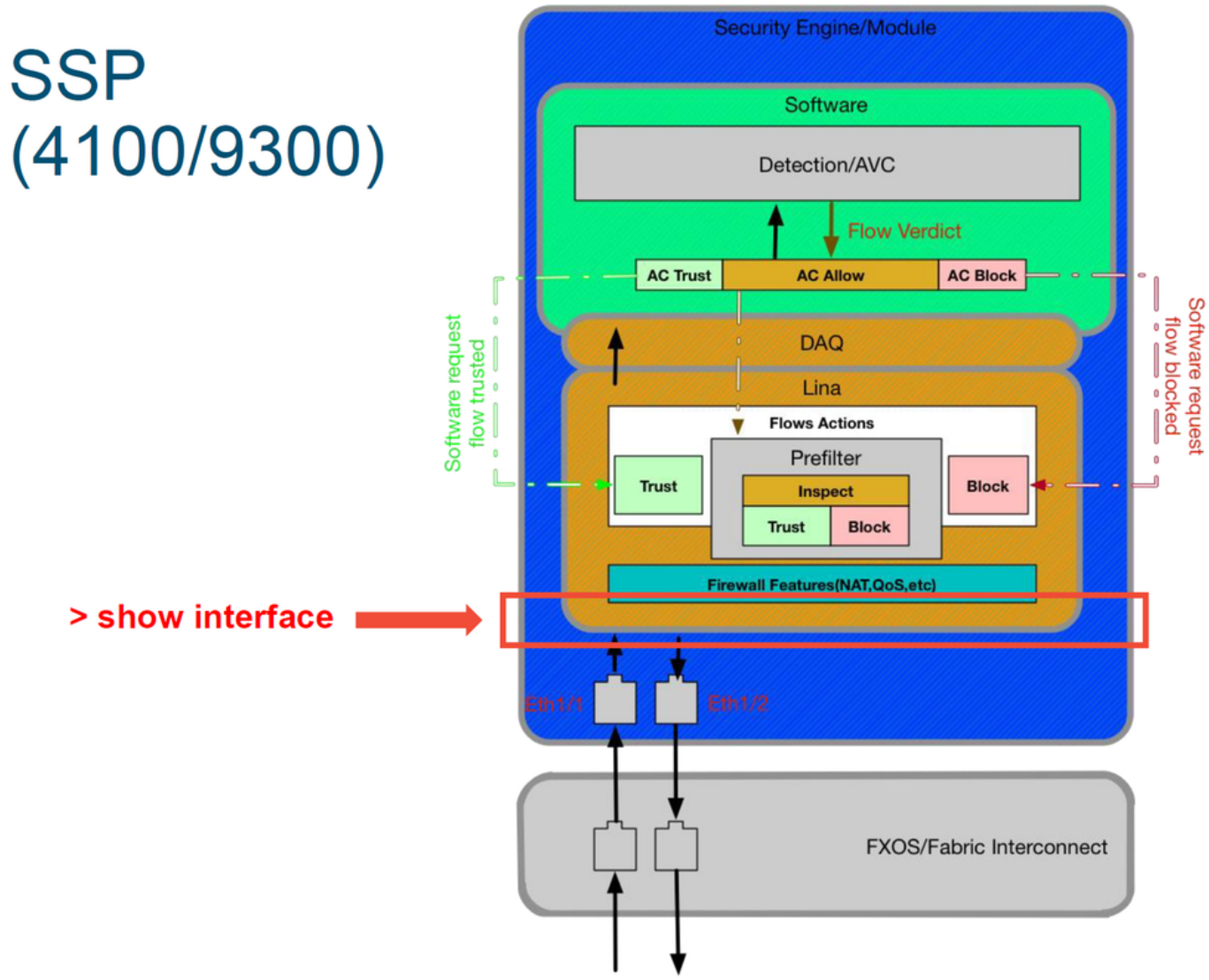
Afin de rechercher des problèmes au niveau de l'interface, entrez les commandes suivantes :

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

Voici un exemple de sortie (problèmes possibles surlignés en rouge) :

```
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 des erreurs sont détectées, le logiciel FTD réel peut également être vérifié pour détecter les erreurs d'interface.



Pour accéder à l'invite FTD, il est d'abord nécessaire d'accéder à l'invite CLI FTD.

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

Pour les instances multiples :

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

Voici un exemple de sortie.

```
# 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
```

Données à fournir au centre d'assistance technique Cisco (TAC)

Données	Instructions
Captures d'écran d'événement de connexion	Reportez-vous à cet article pour obtenir des instructions.
sortie 'show interface'	Reportez-vous à cet article pour obtenir des instructions.
Captures de paquets	Pour ASA/LINA : https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-ne firewalls/1180... Pour Firepower : http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8(appliances/11777...
Sortie ASA 'show tech'	Connectez-vous à l'interface de ligne de commande ASA et faites enregistrer la session de journal. Entrez la commande **show tech**, puis fournissez le fichier de sortie de session de te Ce fichier peut être enregistré sur disque ou sur un système de stockage externe à l'aide de show tech | redirection disk0:/show_tech.log
Dépannage du fichier à partir du périphérique Firepower inspectant le trafic	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techr

Étape suivante : Dépannage de la couche DAQ Firepower

S'il n'est pas clair si le périphérique Firepower abandonne des paquets, le périphérique Firepower lui-même peut être contourné pour exclure tous les composants Firepower en même temps. Ceci est particulièrement utile pour atténuer un problème si le trafic en question touche le périphérique Firepower, mais pas en sortie.

Pour continuer, passez en revue la phase suivante du dépannage du chemin de données Firepower ; Le DAQ Firepower. Cliquez ici pour continuer.