# Firepower資料路徑故障排除第1階段：封包輸入

## 目錄



## 簡介

本文是一系列文章的一部分，這些文章介紹了如何對Firepower系統的資料路徑進行系統故障排除，以確定Firepower的元件是否影響流量。請參閱概述文章，瞭解有關Firepower平台架構的資訊，以及指向其他資料路徑故障排除文章的連結。

在本文中，我們將瞭解Firepower資料路徑故障排除的第一階段，即資料包輸入階段。


## 平台指南

下表介紹了本文涵蓋的平台。

| 平台代碼名稱 | 說明 | 適用 硬體 平台 | 備註 |
|---|---|---|---|
| SFR | 安裝了FirePOWER服務(SFR)模組的ASA。 | ASA-5500-X系列 | 不適用 |
| FTD（非SSP和FPR-2100） | 安裝在自適應安全裝置(ASA)或虛擬平台上的Firepower威脅防禦(FTD)映像 | ASA-5500-X系列、虛擬NGFW平台 | 不適用 |
| FTD(SSP) | FTD作為邏輯裝置安裝在Firepower可擴充作業系統(FXOS)型機箱上 | FPR-9300、FPR-4100、FPR-2100 | 2100系列不使用FXOS機箱管理器 |

# 資料包輸入階段故障排除

第一個資料路徑故障排除步驟是確保資料包處理的入口或出口階段不會發生丟包。如果資料包正在進入，但未進入，則您可以確定資料包已被裝置在資料路徑中的某個位置丟棄，或者裝置無法建立出口資料包（例如，缺少ARP條目）。

# 識別有問題的流量

排除資料包輸入階段故障的第一步是隔離問題流量中涉及的流量和介面。其中包括：

| 流資訊 | 介面資訊 |
| --- | --- |
| 通訊協定 | |
| 來源IP位址 | 輸入介面 |
| 來源連線埠 | 輸出介面 |
| 目的地 IP | |
| 目的地連線埠 | |

例如：

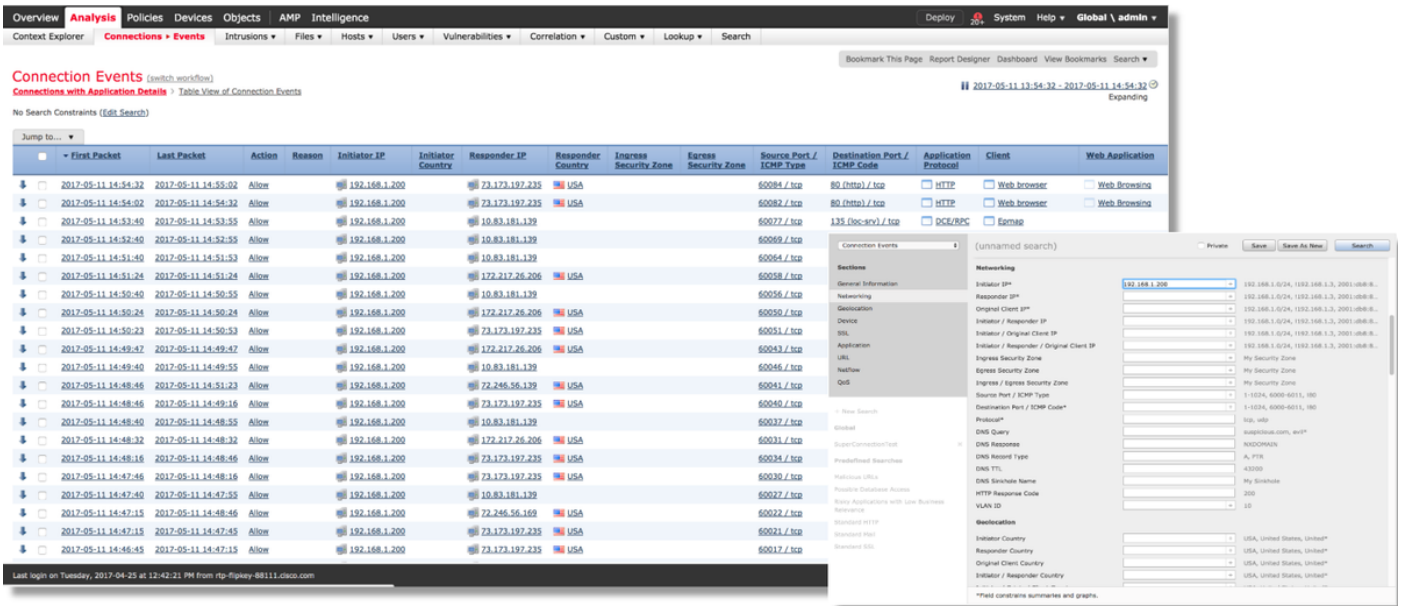
```
TCP inside 172.16.100.101:38974 outside 192.168.1.10:80
```

> **提示**：您可能無法識別確切的來源連線埠，因為每個流量中的來源連線埠通常不同，但目的地（伺服器）連線埠應能滿足需要。

# 檢查連線事件

瞭解了入口和出口介面後，流量應匹配以及流量資訊，確定Firepower是否阻止流量的第一步是檢查相關流量的連線事件。可在Firepower管理中心的**分析>連線>事件**下檢視這些資訊

> **附註**：檢查連線事件之前，請確保在訪問控制策略規則中啟用日誌記錄。日誌記錄在每個訪問控制策略規則中的「日誌記錄」頁籤以及安全情報頁籤中配置。確保將可疑規則配置為將日誌傳送到「事件檢視器」。



在上方示例中，按一下「編輯搜尋」，新增一個唯一的源（啟動器）IP作為過濾器，以檢視Firepower檢測到的流。Action列對此主機流量顯示Allow。

如果Firepower有意阻止流量，則操作包含「阻止」一詞。 按一下「連線事件的表檢視」可提供更多資料。如果操作為「Block」，則可以在「Connection Events」中記下以下欄位：

— 原因

— 訪問控制規則

結合相關事件中的其他欄位，有助於縮小阻塞流量的元件範圍。

有關對訪問控制規則進行故障排除的詳細資訊，可以按一下此處。

# 在輸入和輸出介面上捕獲資料包

如果沒有發生事件或儘管連線事件顯示規則操作「允許」或「信任」，仍懷疑Firepower存在阻塞，則資料路徑故障排除繼續進行。

以下說明如何在上述各種平台上執行輸入和輸出封包擷取：

## SFR - ASA介面上的捕獲

由於SFR模組只是在ASA防火牆上運行的模組，因此最好先在ASA的入口和出口介面上捕獲，以確保入口的相同資料包也正在出口。

本文包含有關如何在ASA上執行捕獲的說明。

如果確定進入ASA的資料包沒有進入，請繼續下一階段的故障排除（DAQ階段）。

> **附註**：如果在ASA輸入介面上看到資料包，則可能需要檢查連線的裝置。

## FTD（非SSP和FPR-2100）— 在輸入和輸出介面上擷取

在非SSP FTD裝置上捕獲與ASA上的捕獲類似。但是，可以直接從CLI初始提示符運行捕獲命令。對丟棄的資料包進行故障排除時，建議將「trace」選項新增到捕獲中。

以下是為連線埠22上的TCP流量設定輸入擷取的範例：

```
> 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>
```

如果新增「trace」選項，則可以選擇單個資料包在系統中進行跟蹤，以檢視它是如何做出最終裁決的。它還有助於確保正確修改資料包(如網路地址轉換(NAT)IP修改)並選擇正確的輸出介面。

```
> 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
```

在上方範例中，我們看到流量通過Snort檢查，且最終達到allow判定結果，且整體通過裝置。由於可以看到兩個方向的流量，因此可以確保此會話的流量流經裝置，因此可能不需要出口捕獲，但您也可以帶到此處以確保流量正確流出，如trace輸出所示。

> **附註**：如果裝置無法建立出口資料包，跟蹤操作仍為「允許」，但在出口介面捕獲中不會建立或看到資料包。這是非常常見的情況，其中FTD沒有下一個躍點或目的地IP的ARP專案（如果最後一個躍點是直接連線的）。

### FTD(SSP) — 在邏輯FTD介面上擷取

在SSP平台上，可遵循上述在FTD上產生封包擷取的相同步驟。您可以使用SSH連線到FTD邏輯介面的IP位址，並輸入以下命令：

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

您還可以使用以下命令從FXOS命令提示符導航到FTD邏輯裝置shell:

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

如果使用Firepower 9300，則模組編號可能因所使用的安全模組而異。這些模組最多可支援3個邏輯裝置。

如果使用多個例項，則例項ID必須包含在「connect」命令中。Telnet命令可用於同時連線到不同的例項。

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

## 檢查介面錯誤

在此階段也可以檢查介面級別問題。如果輸入介面擷取中遺失封包，此功能尤其有用。如果出現介面錯誤，檢查連線的裝置可能會很有幫助。

### SFR — 檢查ASA介面

由於FirePOWER(SFR)模組基本上是在ASA上運行的虛擬機器，因此會檢查實際ASA介面是否有錯誤。有關檢查ASA上的介面統計資訊的詳細資訊，請參閱此ASA系列命令參考指南部分。

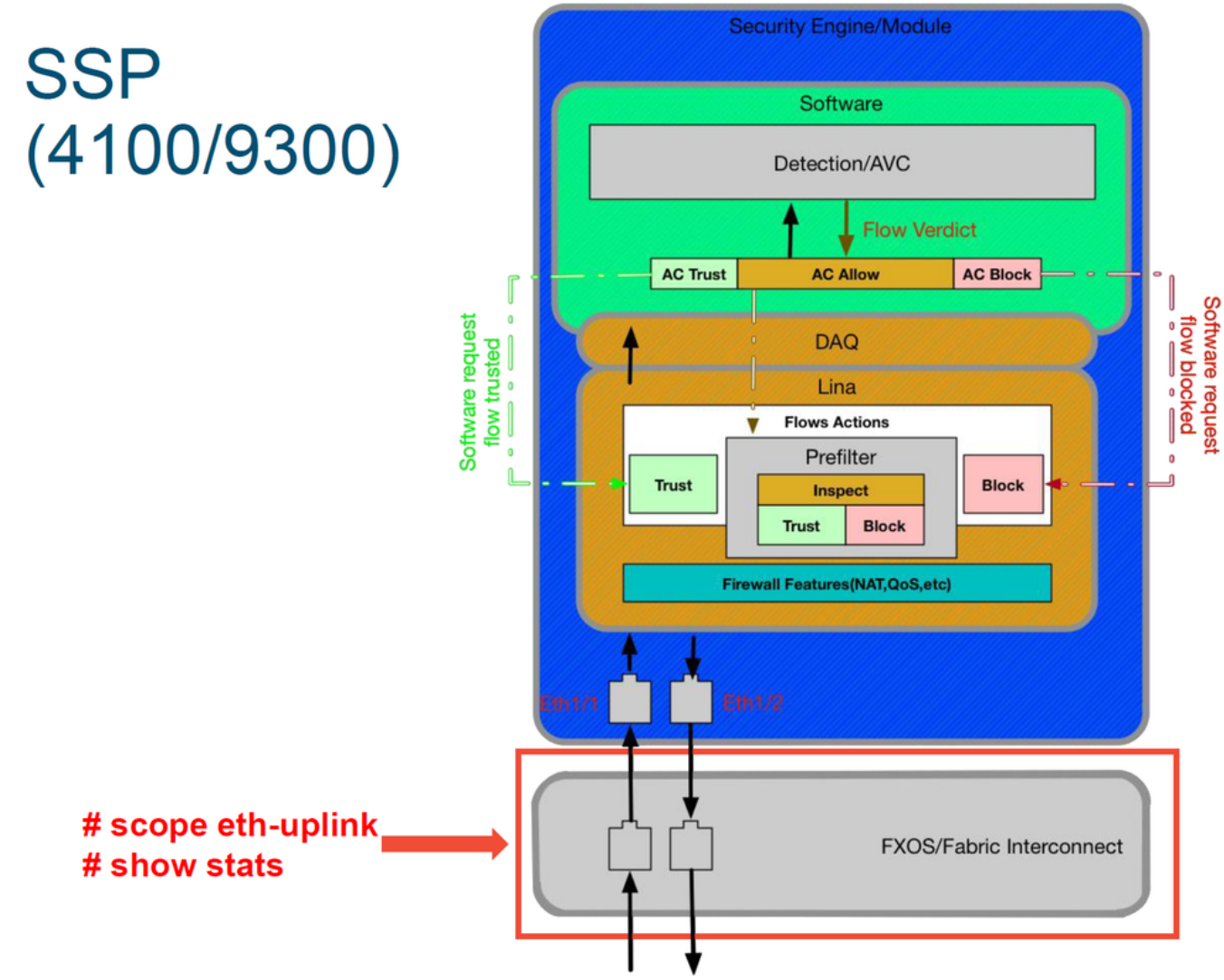
### FTD（非SSP和FPR-2100）— 檢查介面錯誤

在非SSP FTD裝置上，可以從初始命令提示符運行**> show interface**命令。有趣的輸出以紅色突出顯示。

```
> 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) — 導航資料路徑以查詢介面錯誤

9300和4100 SSP平台具有內部交換矩陣互聯，該互聯首先處理資料包。




檢查初始封包輸入是否有任何介面問題。以下是在FXOS系統CLI上運行的命令以獲取此資訊。

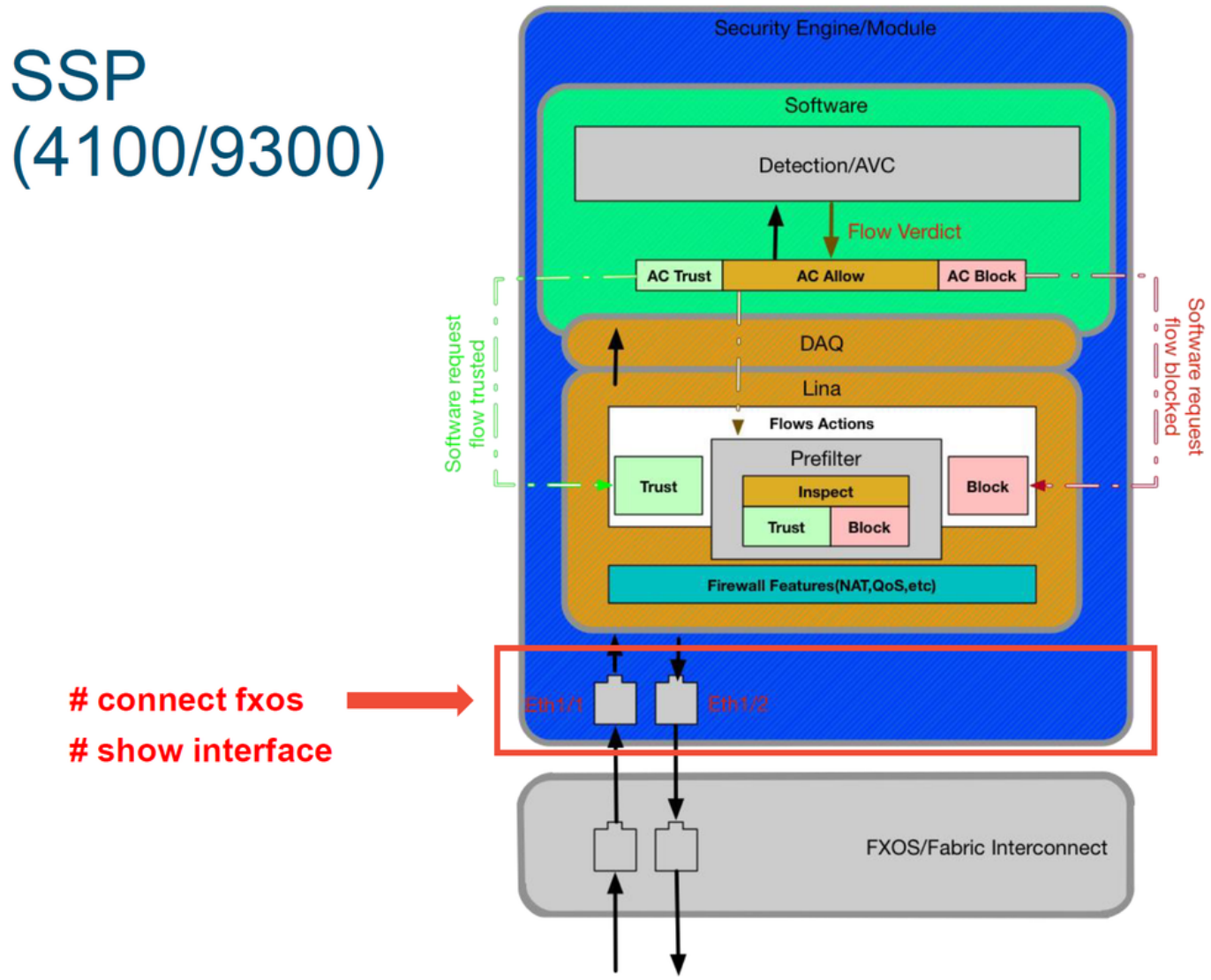
```
ssp# scope eth-uplink
ssp /et-uplink # show stats
```

以下是輸出示例。

```
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
```

交換矩陣互聯在入口處理資料包後，將其傳送到介面，這些介面分配給承載FTD裝置的邏輯裝置。

以下是供參考的圖表：




要檢查任何介面級別問題，請輸入以下命令：

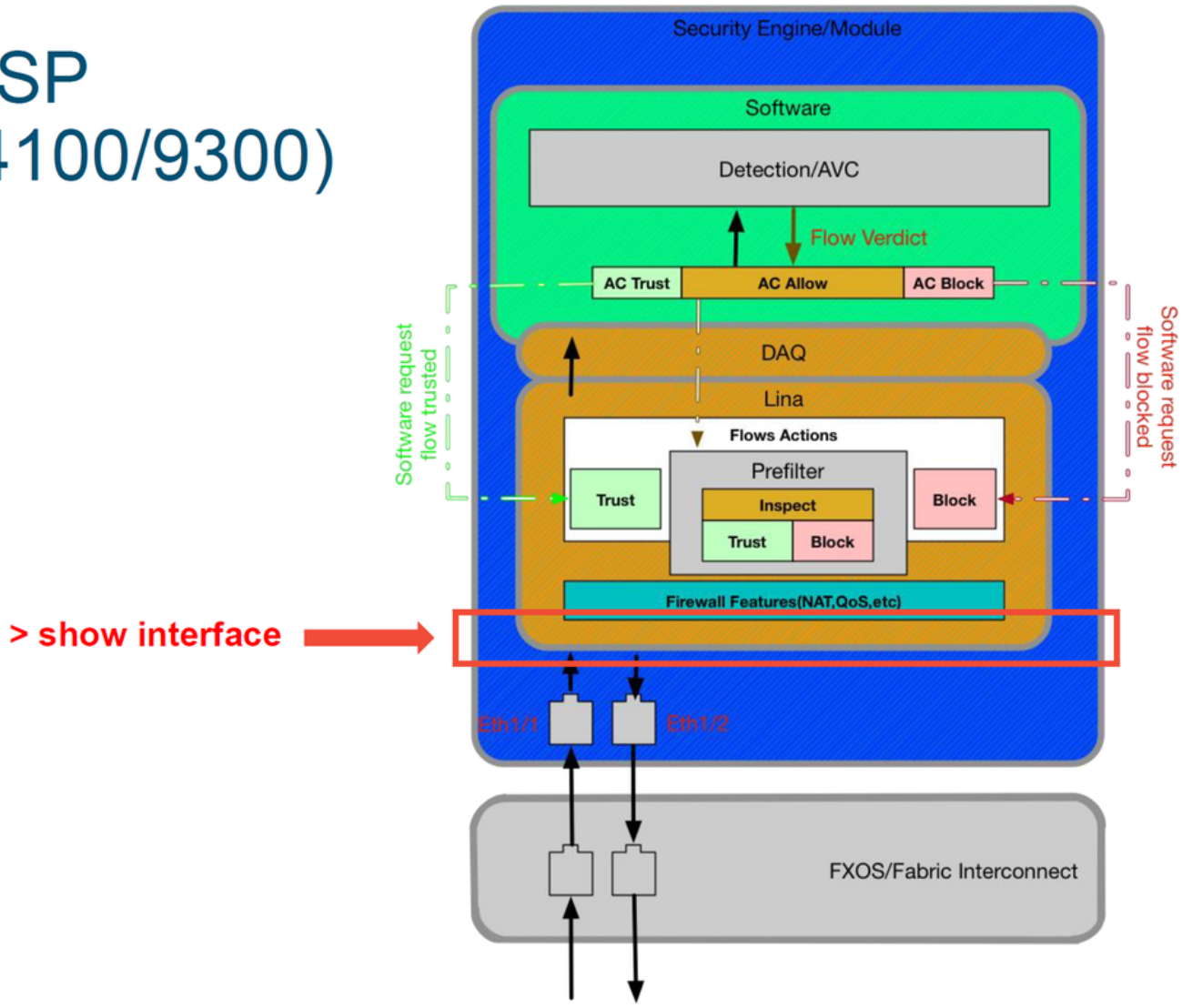
```
ssp# connect fxos
ssp(fxos)# show interface Ethernet 1/7
```

以下是輸出範例（可能的問題以紅色突出顯示）：

```
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
```

如果發現任何錯誤，實際上也可檢查介面錯誤。

# SSP (4100/9300)




若要進入FTD提示，首先必須導覽至FTD CLI提示。

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

對於多例項：

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

以下是輸出範例。

```
# 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
```

## 要提供給思科技術援助中心(TAC)的資料

| 資料 | 說明 |
| --- | --- |
| 連線事件螢幕截圖 | 有關說明，請參閱本文 |
| 'show interface'輸出 | 有關說明，請參閱本文 |
| 封包擷取 | 對於ASA/LINA:https://www.cisco.com/c/en/us/support/docs/sec firewalls/1180..。<br>對於Firepower:http://www.cisco.com/c/en/us/support/docs/secu appliances/11777..。 |
| ASA「show tech」輸出 | 登入ASA CLI並將終端會話儲存到日誌。輸入**show tech**命令，然<br>使用此命令可以將此檔案儲存到磁碟或外部儲存系統中。<br>show tech |重定向磁碟0:/show_tech.log |
| 檢查流量的Firepower裝置的故障排除檔案 | http://www.cisco.com/c/en/us/support/docs/security/sourcefire- |

## 下一步：排除Firepower資料層故障

如果不清楚Firepower裝置是否正在丟棄資料包，則可以繞過Firepower裝置本身來同時排除所有Firepower元件。如果相關流量正在進入Firepower裝置但並未進入，這對於緩解問題特別有用。

要繼續，請檢視Firepower資料路徑故障排除的下一階段；Firepower DAQ。按一下此處繼續。