

# Firepower資料路徑故障排除第2階段：DAQ層

## 目錄

[簡介](#)

[平台指南](#)

[排除Firepower DAQ階段的故障](#)

[在DAQ層捕獲流量](#)

[如何繞過Firepower](#)

[SFR — 將Firepower模組置於僅監控模式](#)

[FTD \(全部\) — 將內嵌集置於分流器模式](#)

[使用Packet Tracer對模擬流量進行故障排除](#)

[SFR — 在ASA CLI上運行Packet Tracer](#)

[FTD \(所有\) — 在FTD CLI上執行Packet Tracer](#)

[使用帶有跟蹤的捕獲功能對即時流量進行故障排除](#)

[FTD \(全部\) — 在FMC GUI上使用追蹤軌跡執行擷取](#)

[在FTD中建立PreFilter Fastpath規則](#)

[要提供給TAC的資料](#)

[下一步](#)

## 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二階段：daq (資料採集) 層。



## 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 (所有)	適用於所有Firepower威脅防禦(FTD)平台	ASA-5500-X系列、虛擬NGFW平台、FPR-2100、FPR-9300、FPR-4100	不適用
FTD (非SSP和FPR-2100)	FTD映像安裝在ASA或虛擬平台上	ASA-5500-X系列、虛擬NGFW平台、FPR-2100	不適用

FTD( SSP) 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 2100系列不使用FXOS機箱管理器

## 排除Firepower DAQ階段的故障

DAQ ( 資料獲取 ) 層是Firepower的一個元件，它將資料包轉換為snort可以理解的形式。最初在資料包傳送到snort時對其進行處理。因此，如果資料包正在進入，但未進入Firepower裝置，或者資料包進入故障排除沒有產生有用的結果，DAQ故障排除可能會很有用。

## 在DAQ層捕獲流量

若要顯示執行擷取所需的提示，您必須首先使用SSH連線至SFR或FTD IP位址。

**附註：**在FPR-9300和4100裝置上，輸入**connect ftd first**，以在第二個>提示時結束連線。您還可以使用SSH進入FXOS機箱管理器IP，然後輸入**connect module 1 console**，然後輸入**connect ftd**。

此[文章](#)說明如何在Firepower DAQ級別收集資料包捕獲。

請注意，語法與ASA上以及FTD平台的LINA端所用的**capture**命令不同。以下範例顯示從FTD裝置執行的DAQ封包擷取：

```
> system support capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - br1
```

```
1 - Router
```

```
2 - my-inline inline set
```

```
Selection? 2
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```


```
Options: -s 1518 -w ct.pcap
```

```
> expert
```

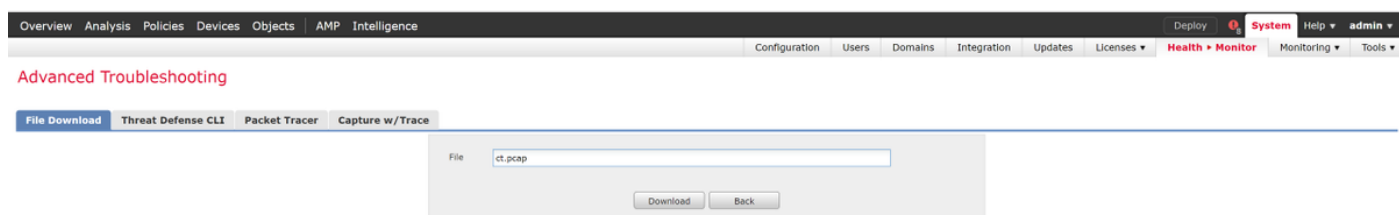
```
admin@ciscoasa:~$ ls /ngfw/var/common/
```

```
ct.pcap
```

如上面的螢幕截圖所示，PCAP格式中名為ct.pcap的捕獲已寫入/ngfw/var/common目錄(SFR平台上的/var/common)。可使用上述文章中的說明從>提示符處從Firepower裝置複製這些捕獲文件。

或者，在Firepower 6.2.0及更高版本中的Firepower管理中心(FMC)上，導航到**Devices > Device Management**。然後，按一下  圖示位於相關裝置旁，然後是**Advanced Troubleshooting > File Download**。

然後，可以輸入捕獲檔案的名稱，然後按一下「下載」。



## 如何繞過Firepower

如果Firepower看到流量，但已確定資料包未進入裝置或者流量存在其他問題，則下一步是繞過Firepower檢查階段，確認某個Firepower元件正在丟棄流量。下面是各種平台上讓流量繞過Firepower的最快方法的細分。

### SFR — 將Firepower模組置於僅監控模式

在託管SFR的ASA上，可以通過ASA命令列介面(CLI)或思科自適應安全裝置管理器(ASDM)將

SFR模組置於僅監控模式。這只會將活動資料包的副本傳送到SFR模組。

為了通過ASA CLI將SFR模組置於僅監控模式，必須首先通過運行**show service-policy sfr**命令來確定用於SFR重定向的類對映和策略對映。

```
# show service-policy sfr
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: sfr
```

```
SFR: card status Up, mode fail-open
```

```
packet input 10000, packet output 9900, drop 100, reset-drop 0
```

輸出顯示，global\_policy策略對映正在對「sfr」類對映實施sfr失效開放操作。

**附註：**「fail-close」也是一種可以運行SFR的模式，但它並不常用，因為它會在SFR模組關閉或無響應時阻止所有流量。

若要將SFR模組置於僅監控模式，可以發出以下命令以否定當前SFR配置並輸入僅監控配置：

```
# configure terminal
```

```
(config)# policy-map global_policy
```

```
(config-pmap)# class sfr
```

```
(config-pmap-c)# no sfr fail-open
```

```
(config-pmap-c)# sfr fail-open monitor-only
```

```
INFO: The monitor-only mode prevents SFR from denying or altering traffic.
```

```
(config-pmap-c)# write memory
```

```
Building configuration...
```

模組一旦進入僅監控模式，即可在**show service-policy sfr**輸出中對其進行驗證。

```
# sh service-policy sfr
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: sfr
```

```
SFR: card status Up, mode fail-open monitor-only
```

```
packet input 0, packet output 100, drop 0, reset-drop 0
```

**附註：**若要將SFR模組重新置於內聯模式，請從上面顯示的(config-pmap-c)# 提示符處發出**no sfr fail-open monitor-only**命令，然後發出**sfr {fail-open | fail-close}**命令時，該命令才處於初始狀態。

或者，您可以通過導航到**配置 > 防火牆 > 服務策略規則**，通過ASDM將模組置於僅監控狀態。然後，按一下相關規則。接下來，轉到**Rule Actions**頁面，然後按一下**ASA FirePOWER Inspection**頁籤。一旦到達此位置，就可以選擇**Monitor-only**。

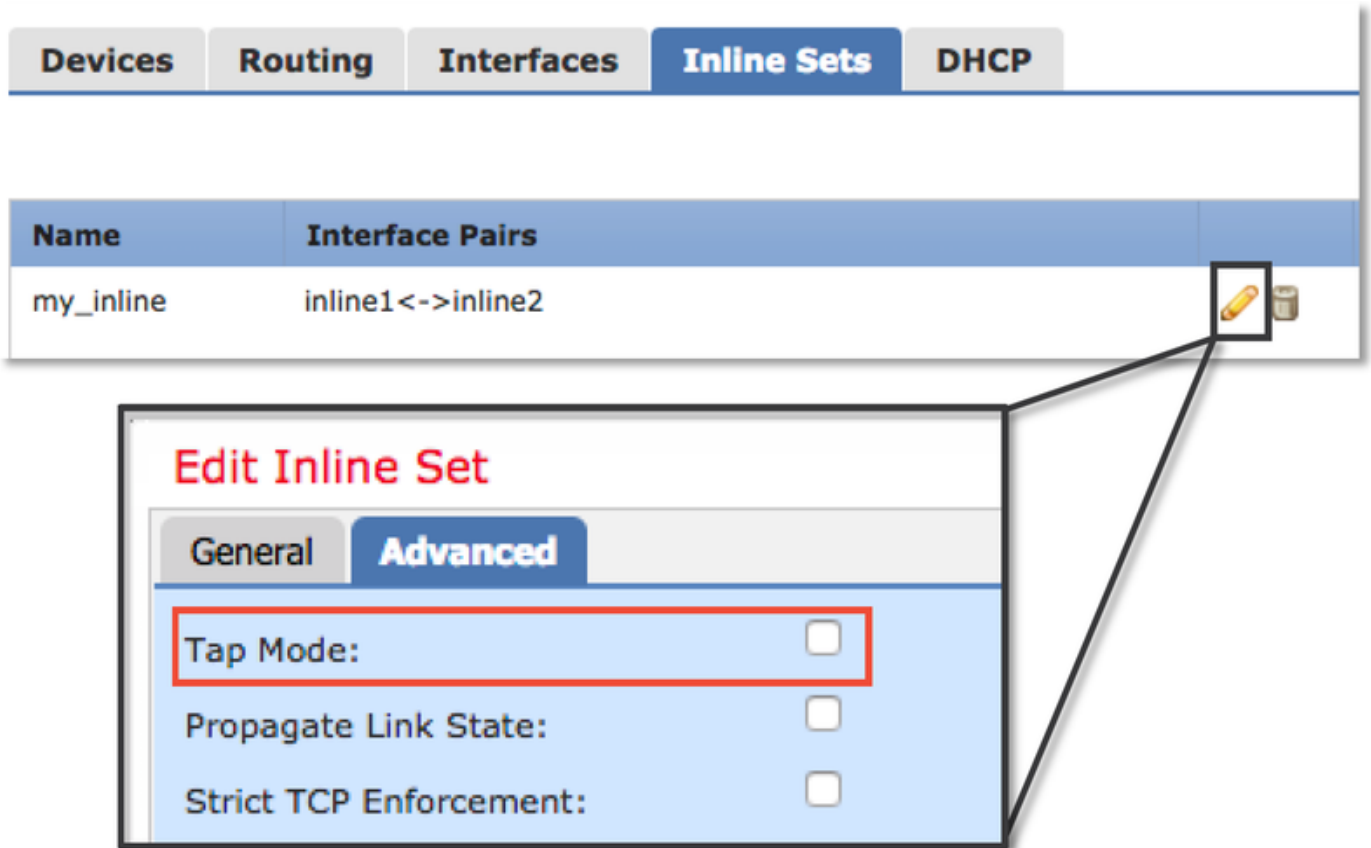
如果流量問題在SFR模組被確認處於僅監控模式後仍然存在，則Firepower模組不會導致此問題。然後，可以運行Packet tracer來進一步診斷ASA級別的問題。

如果問題不再存在，下一步是對Firepower軟體元件進行故障排除。

## FTD (全部) — 將內嵌集置於分流器模式

如果流量通過內嵌集內配置的介面對，則內嵌集可以置於TAP模式。這基本上會導致Firepower不對活動資料包執行操作。它不適用於沒有內嵌集的路由器或透明模式，因為裝置必須在將資料包傳送到下一跳之前修改資料包，並且不能在不丟棄流量的情況下將其置於旁路模式。對於沒有內聯集的路由和透明模式，請繼續Packet Tracer步驟。

要從FMC使用者介面(UI)配置TAP模式，請導航到**Devices > Device Management**，然後編輯相關裝置。在**Inline Sets**索引標籤下，勾選**TAP Mode**的選項。



如果TAP模式解決了問題，下一步是對Firepower軟體元件進行故障排除。

如果TAP模式不能解決問題，則問題在Firepower軟體之外。然後可使用Packet tracer進一步診斷問題。

## 使用Packet Tracer對模擬流量進行故障排除

Packet Tracer是一種實用程式，可幫助確定丟包的位置。它是模擬器，因此它執行人工資料包的跟蹤。

## SFR — 在ASA CLI上運行Packet Tracer

以下示例說明如何在ASA CLI上為SSH流量運行Packet Tracer。有關Packet Tracer命令語法的更多詳細資訊，請參閱ASA系列命令參考指南中的[部分](#)。

```
asa# packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh
```

```
Phase: 1  
Type: ACCESS-LIST  
Subtype:  
Result: ALLOW  
Config:  
Implicit Rule  
Additional Information:  
MAC Access list
```

```
Phase: 2  
Type: ROUTE-LOOKUP  
Subtype: Resolve Egress Interface  
Result: ALLOW  
Config:  
Additional Information:  
found next-hop 10.151.37.1 using egress ifc outside
```

```
Phase: 3  
Type: NAT  
Subtype: per-session  
Result: ALLOW  
Config:  
Additional Information:
```

```
Phase: 4  
Type: IP-OPTIONS  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:
```

```
Phase: 5  
Type: SFR  
Subtype:  
Result: ALLOW  
Config:  
class-map inspection_default  
match any  
policy-map global_policy  
class inspection_default  
sfr fail-open  
service-policy global_policy global  
Additional Information:
```

```
Phase: 6  
Type: INSPECT  
Subtype: np-inspect  
Result: ALLOW  
Config:  
class-map inspection_default  
match any  
policy-map global_policy  
class inspection_default  
inspect icmp  
service-policy global_policy global  
Additional Information:
```

```
Phase: 7  
Type: NAT  
Subtype: per-session  
Result: ALLOW  
Config:  
Additional Information:
```

```
Phase: 8  
Type: IP-OPTIONS  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:
```

```
Phase: 9  
Type: FLOW-CREATION  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
New flow created with id 756, packet dispatched to next module
```

```
Result:  
input-interface: inside  
input-status: up  
input-line-status: up  
output-interface: outside  
output-status: up  
output-line-status: up  
Action: allow
```

在上方示例中，我們看到ASA和SFR模組都允許資料包以及ASA如何處理資料包流的有用資訊。

## FTD ( 所有 ) — 在FTD CLI上執行Packet Tracer

在所有FTD平台上，均可從FTD CLI執行Packet Tracer命令。

```
> packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh
```

```
Phase: 1  
Type: ACCESS-LIST  
Subtype:  
Result: ALLOW  
Config:  
Implicit Rule  
Additional Information:  
MAC Access list
```

```
Phase: 2  
Type: ROUTE-LOOKUP  
Subtype: Resolve Egress Interface  
Result: ALLOW  
Config:  
Additional Information:  
found next-hop 192.168.100.1 using egress ifc outside
```

```
Phase: 3  
Type: ACCESS-LIST  
Subtype: log  
Result: ALLOW  
Config:  
access-group CSM_FW_ACL_global  
access-list CSM_FW_ACL_advanced permit ip any any rule-id 268434433  
access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY:  
My_AC_Policy - Mandatory  
access-list CSM_FW_ACL_remark rule-id 268434433: L7 RULE: Block urls  
Additional Information:  
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
Phase: 4  
Type: CONN-SETTINGS  
Subtype:  
Result: ALLOW  
Config:  
class-map class-default  
match any  
policy-map global_policy  
class class-default  
set connection advanced-options UM_STATIC_TCP_MAP  
service-policy global_policy global  
Additional Information:
```

```
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 62_network
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.62.60/10000 to 192.168.100.51/10000
```

```
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 9
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 612016, packet dispatched to next module
```

```
Phase: 11
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 12
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 1821549761
Reputation: packet blacklisted, drop
Snort: processed decoder alerts or actions queue, drop
IPS Event: gid 136, sid 1, drop
Snort detect_drop: gid 136, sid 1, drop
NAP id 1, IPS id 0, Verdict BLACKLIST, Blocked by Reputation
Snort Verdict: (black-list) black list this flow
```

在本例中，Packet Tracer顯示了丟棄的原因。在這種情況下，它是Firepower中安全情報功能內的IP黑名單阻止資料包。下一步是排除導致丟包的個別Firepower軟體元件的故障。

## 使用帶有跟蹤的捕獲功能對即時流量進行故障排除

也可通過capture with trace功能跟蹤即時流量，此功能可通過CLI在所有平台上可用。以下是針對SSH流量運行帶有跟蹤的捕獲的示例。

```
> 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>
```

```
> 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
```

在本例中，捕獲中的第四個資料包被跟蹤，因為這是定義有應用程式資料的第一個資料包。如圖所示，資料包最終被snort列入白名單，這意味著流無需進行進一步的snort檢查，並且允許進行總體檢查。

有關使用跟蹤語法的捕獲的詳細資訊，請參閱《ASA系列命令參考指南》中的[此部分](#)。

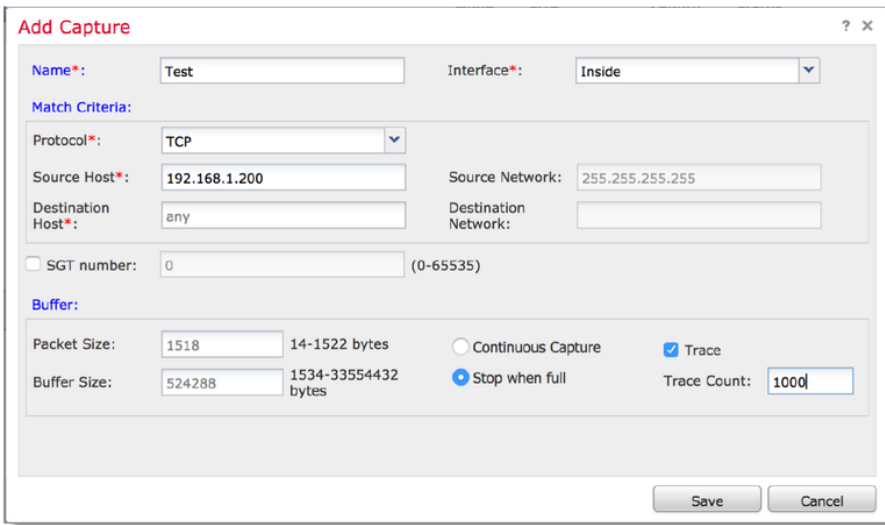
## FTD (全部) — 在FMC GUI上使用追蹤軌跡執行擷取

在FTD平台上，可在FMC UI上執行包含追蹤軌跡的擷取。要訪問該實用程式，請導航至Devices > Device Management。

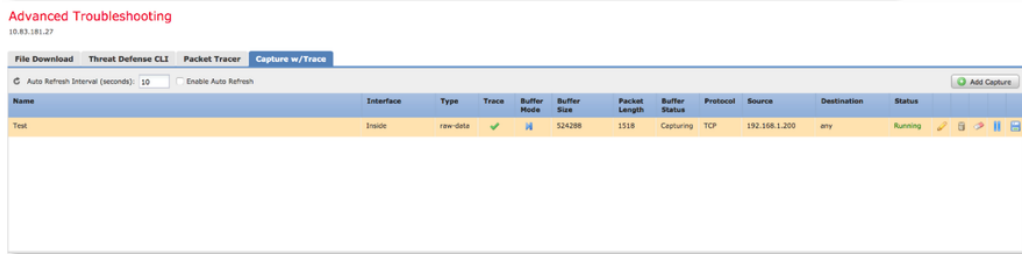


然後，按一下  圖示位於相關裝置旁，然後是Advanced Troubleshooting > Capture w/Trace。

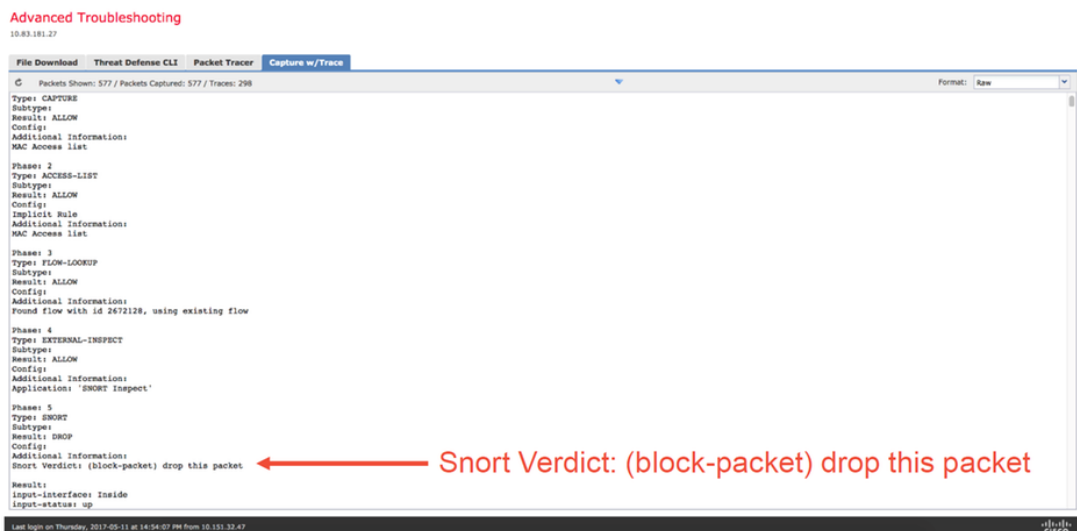
以下是如何透過GUI使用追蹤軌跡執行擷取的範例。



Clicking **Add Capture** button will display this popup window



View of all current captures



```
Advanced Troubleshooting
10.83.181.27

File Download Threat Defense CLI Packet Tracer Capture w/Trace
Packets Shown: 577 / Packets Captured: 577 / Traces: 298
Format: raw

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 2672128, using existing flow

Phase: 4
Type: INTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Verdict: (block-packet) drop this packet
Result:
input-interface: Inside
input-status: up

Last login on Thursday, 2017-05-11 at 14:54:07 PM from 10.151.32.47
```

Example output shows the packet was blocked by Snort

如果包含追蹤軌跡的擷取顯示封包捨棄的原因，則下一步是排解個別軟體元件的疑難問題。

如果它沒有明確顯示問題的原因，下一步是快速引導流量。

## 在FTD中建立PreFilter Fastpath規則

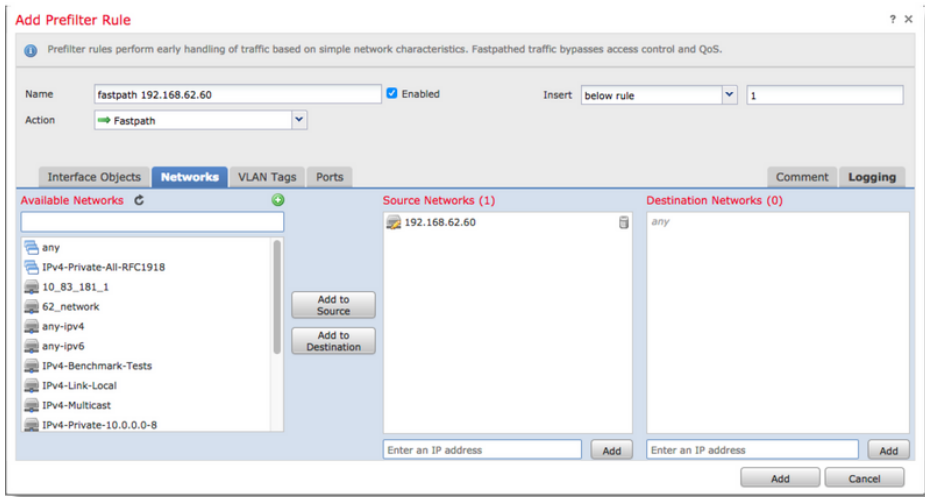
在所有FTD平台上，都有一個預先篩選原則，可用於轉移來自Firepower(snort)檢查的流量。

在FMC上，可在Policies > Access Control > Prefilter下找到此項。無法編輯預設預過濾器策略，因此需要建立自定義策略。

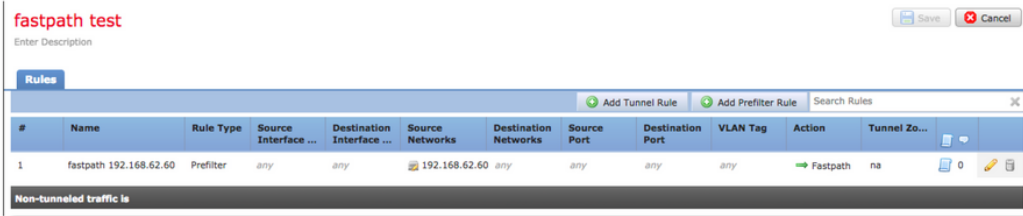
之後，新建立的預過濾器策略需要與訪問控制策略相關聯。這是在預過濾器策略設定部分中的訪問

控制策略的「高級」頁籤中配置的。

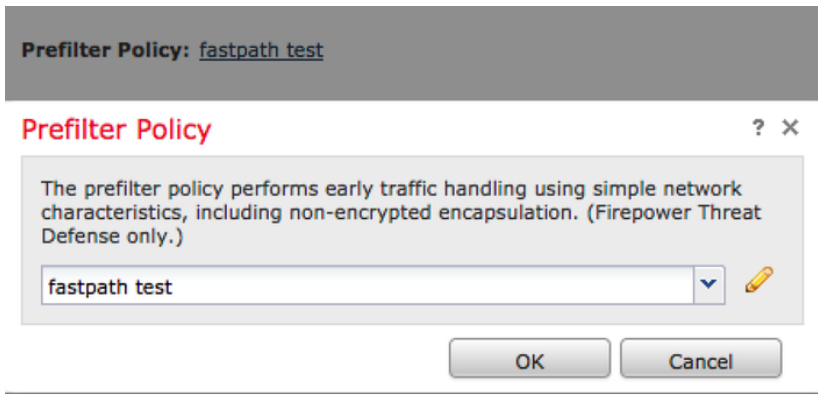
以下示例說明如何在Prefilter Policy中建立快速路徑規則並驗證命中計數。



Clicking **Add Prefilter Rule** button will display this popup window.



View of all rules in the **fastpath test** Prefilter policy



From AC policy make sure the Prefilter Policy is set to the custom Prefilter Policy

View of connection events matching prefilter rule

	First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Prefilter Policy	Tunnel/Prefilter Rule
	2017-05-15 16:05:14	2017-05-15 16:05:14	Fastpath		192.168.62.60	10.83.180.173	48480 / tcp	22 (ssh) / tcp	fastpath test	fastpath 192.168.62.60

[按一下此處](#)瞭解有關預過濾器策略的操作和配置的詳細資訊。

如果新增PreFilter策略解決了流量問題，則根據需要可以保留規則。然而，沒有對該流量進行進一步檢查。需要對Firepower軟體執行進一步的故障排除。

如果新增預過濾器策略不能解決此問題，則可以再次運行帶有跟蹤步驟的資料包，以跟蹤資料包的新路徑。

## 要提供給TAC的資料

## 資料

命令輸出

封包擷取

ASA 「show tech」輸出

檢查流量的Firepower裝置的故障排除檔案

## 說明

有關說明，請參閱本文

對於ASA/LINA:<https://www.cisco.com/c/en/us/support/docs/sec/asa-00.html>

對於Firepower:<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-00.html>

登入ASA CLI並將終端會話儲存到日誌。輸入show技術命令，然後使用此命令可以將此檔案儲存到磁碟或外部儲存系統中。

show tech |重定向磁碟0:/show\_tech.log

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-00.html>

## 下一步

如果確定Firepower軟體元件是問題的原因，下一步將是系統地排除每個元件，從安全情報開始。

按一下[此處](#)繼續下一指南。