Fase 2 della risoluzione dei problemi del percorso dei dati di Firepower: Livello DAQ

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 verrà esaminata la seconda fase della risoluzione dei problemi relativi al percorso dati di Firepower: il livello DAQ (Data Aquisition).

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-X	N/D

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

Risoluzione dei problemi relativi alla fase DAQ di Firepower

Il livello DAQ (Data Aquisition) è un componente di Firepower che converte i pacchetti in un formato che snort può comprendere. Gestisce inizialmente il pacchetto quando viene inviato allo snort. Pertanto, se i pacchetti in entrata ma non in uscita dall'appliance Firepower o la risoluzione dei problemi di entrata dei pacchetti non ha dato risultati utili, la risoluzione dei problemi tramite DAQ può essere utile.

Acquisizione del traffico sul layer DAQ

Per visualizzare la richiesta da cui eseguire l'acquisizione, è necessario prima connettersi con SSH all'indirizzo IP SFR o FTD.

> **Nota:** Sui dispositivi FPR-9300 e 4100, immettere prima **connect ftd**, per terminare al secondo **>** prompt. Inoltre, è possibile eseguire il protocollo SSH sull'indirizzo IP di FXOS Chassis Manager, quindi immettere la **console del modulo di connessione 1** e **infine connettere il dispositivo ftd**.

In questo articolo viene spiegato come raccogliere le acquisizioni dei pacchetti a livello DQ di Firepower.

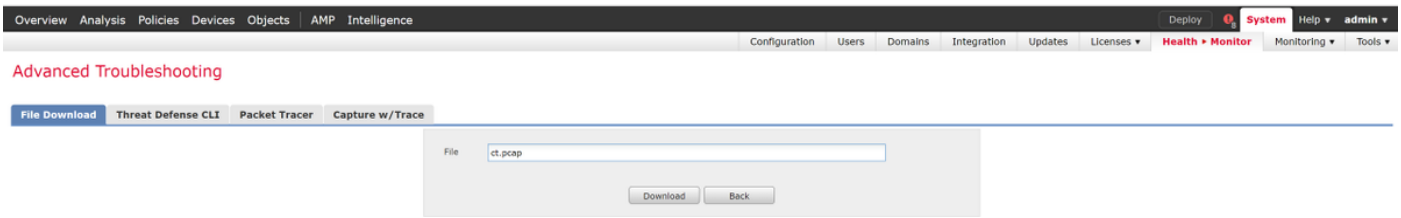
La sintassi è diversa da quella del comando **capture** usato sull'ASA e sul lato LINA della piattaforma FTD. Di seguito è riportato un esempio di acquisizione pacchetti DAQ eseguita da un dispositivo FTD:

```
> 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
```

Come mostrato nella schermata precedente, un'acquisizione sul formato PCAP chiamata ct.pcap è stata scritta nella directory **/ngfw/var/common** (**/var/common** sulla piattaforma SFR). Questi file di acquisizione possono essere copiati dal prompt **>** della periferica Firepower utilizzando le istruzioni riportate nell'articolo sopra.

In alternativa, nel Firepower Management Center (FMC) di Firepower versione 6.2.0 e successive, selezionare **Dispositivi > Gestione dispositivi**. Quindi, fare clic sul pulsante accanto al dispositivo in questione, quindi selezionare **Advanced Troubleshooting > File Download**.

Èquindi possibile immettere il nome del file di acquisizione e fare clic su Download.



Come ignorare Firepower

Se Firepower rileva il traffico, ma è stato determinato che i pacchetti non stanno uscendo dal dispositivo o che esiste un altro problema con il traffico, il passaggio successivo consiste nell'ignorare la fase di ispezione di Firepower per confermare che uno dei componenti Firepower sta eliminando il traffico. Di seguito è riportata una descrizione del modo più veloce per evitare che il traffico ignori Firepower sulle varie piattaforme.

SFR - Attivare la modalità solo monitor per il modulo Firepower

Sull'appliance ASA che ospita l'SFR, è possibile configurare il modulo SFR in modalità di solo monitoraggio tramite l'interfaccia della riga di comando ASA (CLI) o Cisco Adaptive Security Device Manager (ASDM). In questo modo, solo una copia dei pacchetti live viene inviata al modulo SFR.

Per porre il modulo SFR in modalità di solo monitoraggio tramite la CLI di ASA, la mappa delle classi e la mappa dei criteri utilizzate per il reindirizzamento SFR devono essere determinate prima tramite il comando **show service-policy sfr**.

```
# 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
```

L'output mostra che la mappa dei criteri global_policy sta applicando l'azione di apertura degli errori della sfr sulla mappa delle classi "sfr".

> **Nota:** "fail-close" è anche una modalità in cui può essere eseguito l'SFR, ma non è così comunemente utilizzato in quanto blocca tutto il traffico se il modulo SFR è inattivo o non risponde.

Per impostare il modulo SFR in modalità di solo monitoraggio, è possibile utilizzare questi comandi per negare la configurazione SFR corrente e accedere alla configurazione di solo monitoraggio:

```
# 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...
```

Una volta che il modulo è stato messo in modalità solo monitor, è possibile verificarlo nell'output del comando **show service-policy sfr**.

```
# 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
```

> **Nota:** Per ripristinare la modalità in linea del modulo SFR, usare il comando **no sfr fail-open monitor-only** dal prompt **(config-pmap-c)#** mostrato sopra, seguito dal comando **sfr {fail-open | fail-close}**, comando originariamente presente.

In alternativa, è possibile configurare il modulo in modo che sia disponibile solo per il monitoraggio tramite ASDM selezionando **Configurazione > Firewall > Regole dei criteri di servizio**. Quindi, fare clic sulla regola in questione. Quindi, andare alla pagina **Azioni regola** e fare clic sulla scheda **ASA FirePOWER Inspection**. In questo modo, è possibile selezionare **solo monitor**.

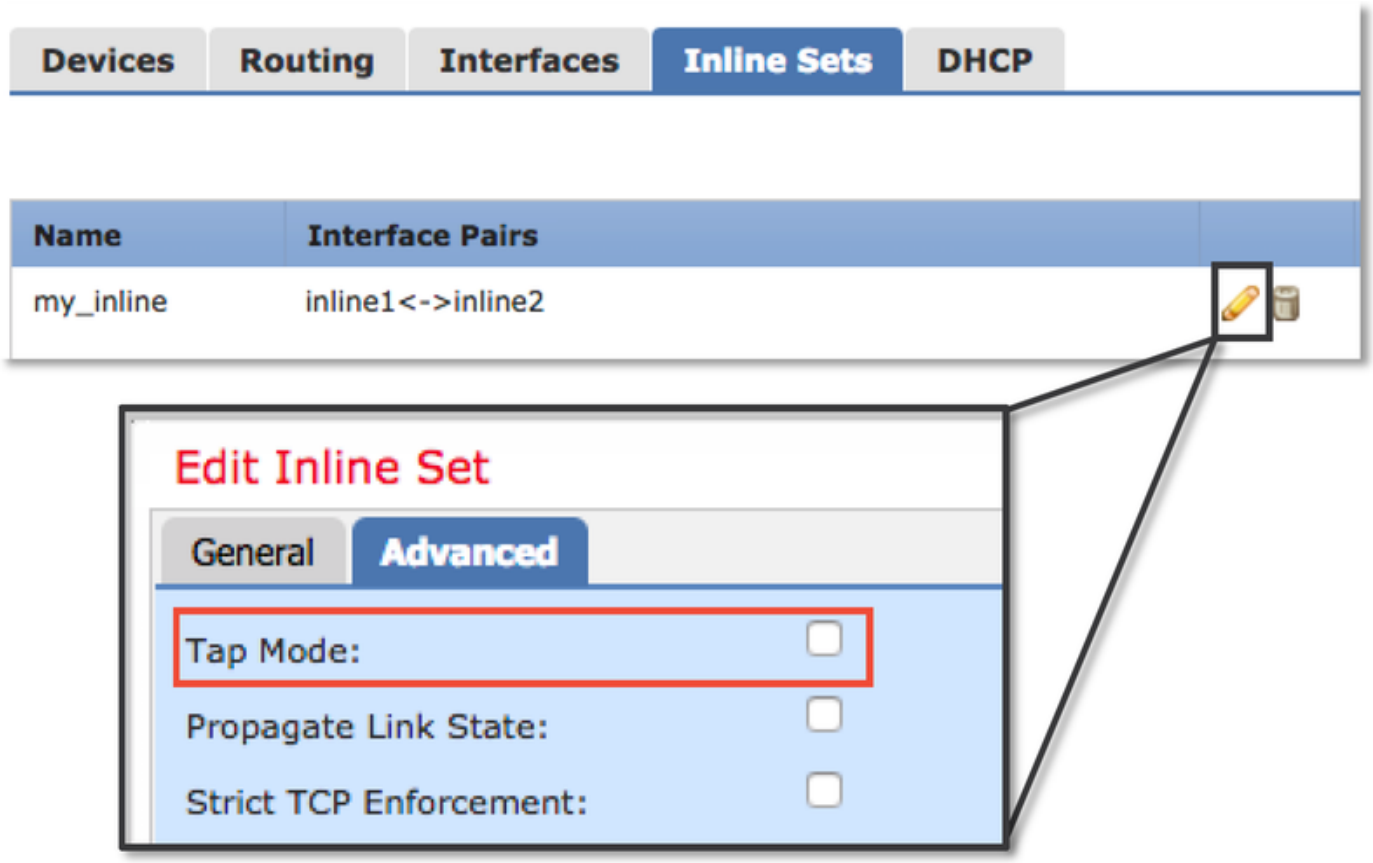
Se il problema persiste anche dopo che è stato confermato che il modulo SFR è in modalità solo monitor, il modulo Firepower non lo causa. È quindi possibile eseguire Packet Tracer per diagnosticare ulteriormente i problemi a livello di ASA.

Se il problema persiste, il passaggio successivo consiste nella risoluzione dei problemi dei componenti software di Firepower.

FTD (all) - Imposta set inline in modalità TAP

Se il traffico passa attraverso coppie di interfacce configurate in set inline, il set inline può essere messo in modalità TAP. In questo modo, Firepower non interviene sul pacchetto live. Non si applica al router o alla modalità trasparente senza set in linea, in quanto il dispositivo deve modificare i pacchetti prima di inviarli all'hop successivo e non può essere impostato su una modalità bypass senza interrompere il traffico. Per la modalità instradata e trasparente senza set inline, procedere con il passaggio packet tracer.

Per configurare la modalità TAP dall'interfaccia utente di FMC, selezionare **Dispositivi > Gestione dispositivi**, quindi modificare il dispositivo in questione. Nella scheda **Insiemi in linea**, selezionate l'opzione **Modalità MASCHIO**.



Se la modalità TAP risolve il problema, il passaggio successivo consiste nella risoluzione dei problemi dei componenti software Firepower.

Se la modalità TAP non risolve il problema, il problema è esterno al software Firepower. È quindi

possibile utilizzare Packet Tracer per diagnosticare ulteriormente il problema.

Uso di Packet Tracer per risolvere i problemi relativi al traffico simulato

Packet Tracer è un'utilità che può aiutare a identificare la posizione in cui un pacchetto viene scartato. È un simulatore, quindi esegue una traccia di un pacchetto artificiale.

SFR - Esegui Packet Tracer sulla CLI ASA

Di seguito è riportato un esempio di come eseguire packet-tracer sulla CLI di ASA per il traffico SSH. Per informazioni più dettagliate sulla sintassi del comando packet tracer, consultare questa sezione della guida di riferimento dei comandi della serie ASA.

```
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
```

Nell'esempio precedente, vengono mostrati sia il modulo ASA che il modulo SFR che permette l'uso dei pacchetti, oltre a informazioni utili su come l'ASA gestirebbe il flusso dei pacchetti.

FTD (all) - Esegui packet tracer sulla CLI FTD

Su tutte le piattaforme FTD, il comando packet tracer può essere eseguito dalla CLI FTD.

```
> 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
```

Nell'esempio, il tracer del pacchetto mostra il motivo della perdita. In questo caso, è la blacklist IP all'interno della funzionalità Security Intelligence di Firepower a bloccare il pacchetto. Il passaggio successivo consiste nella risoluzione dei problemi relativi al singolo componente software Firepower che causa la caduta.

Uso di Acquisisci con traccia per risolvere i problemi relativi al traffico in tempo reale

Il traffico in tempo reale può essere tracciato anche tramite la funzione di acquisizione con traccia, disponibile su tutte le piattaforme dalla CLI. Di seguito è riportato un esempio di esecuzione di un'acquisizione con traccia sul traffico SSH.

```
> 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
```

Nell'esempio riportato sotto, è stato tracciato il quarto pacchetto nell'acquisizione, poiché è il primo pacchetto con dati dell'applicazione definiti. Come mostrato nella figura, il pacchetto viene quindi reso bianco da uno snort, il che significa che non è necessaria un'ulteriore ispezione dello snort per il flusso, ed è consentito in generale.

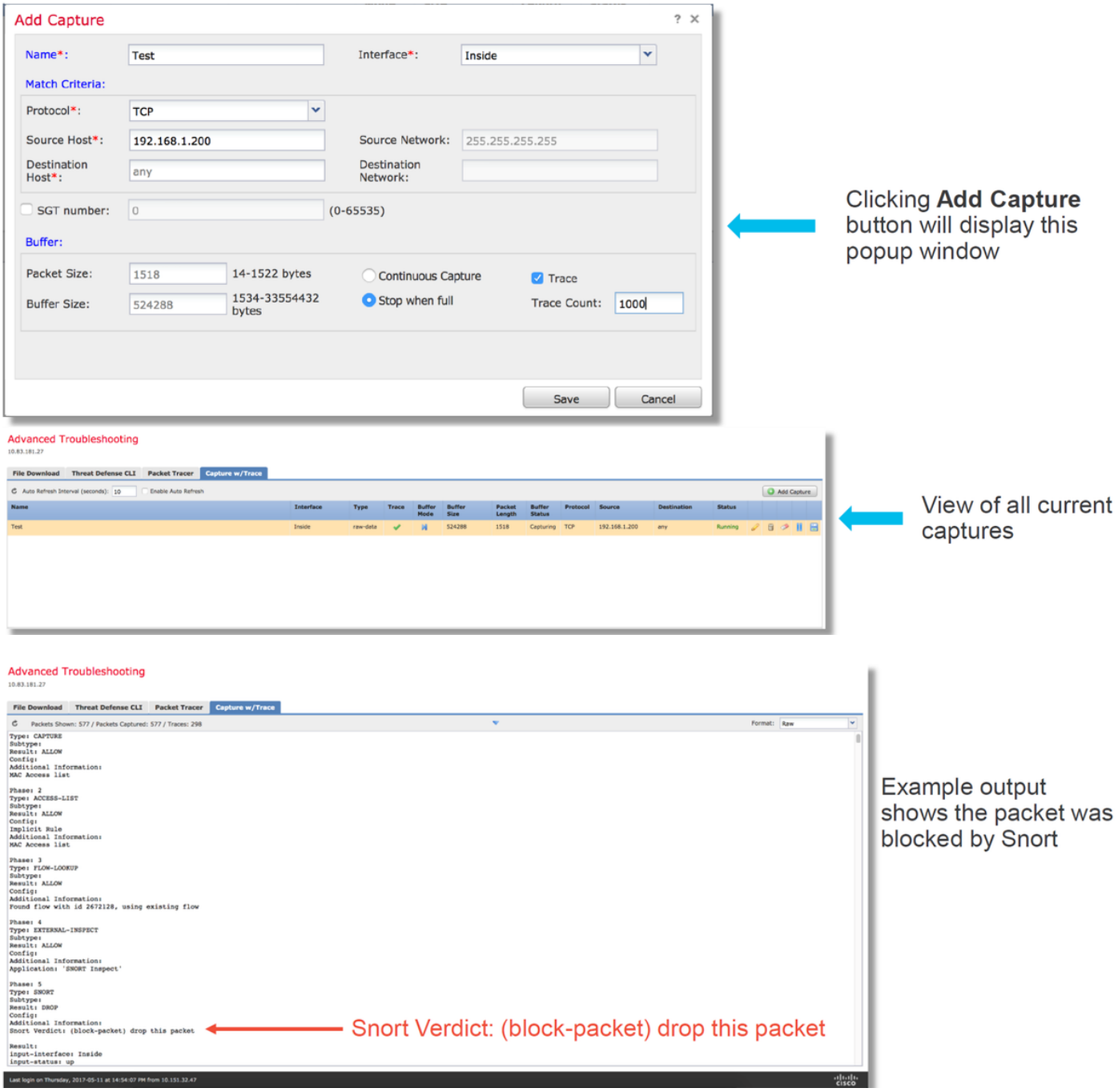
Per ulteriori informazioni sulla sintassi di acquisizione con trace, consultare questa sezione della guida di riferimento dei comandi della serie ASA.

FTD (all) - Acquisizione con traccia in esecuzione sull'interfaccia utente di FMC

Nelle piattaforme FTD è possibile eseguire l'acquisizione con traccia nell'interfaccia utente di FMC. Per accedere all'utility, selezionare **Dispositivi > Gestione dispositivi**.

Quindi, fare clic sul pulsante  accanto al dispositivo in questione, quindi selezionare **Advanced Troubleshooting > Capture w/Trace.**

Di seguito è riportato un esempio di come eseguire un'acquisizione con trace tramite la GUI.



Se l'acquisizione con traccia indica la causa del rilascio del pacchetto, il passaggio successivo consiste nella risoluzione dei problemi dei singoli componenti software.

Se la causa del problema non è indicata chiaramente, procedere come segue per velocizzare il traffico.

Creazione di una regola Fastpath del prefiltro in FTD

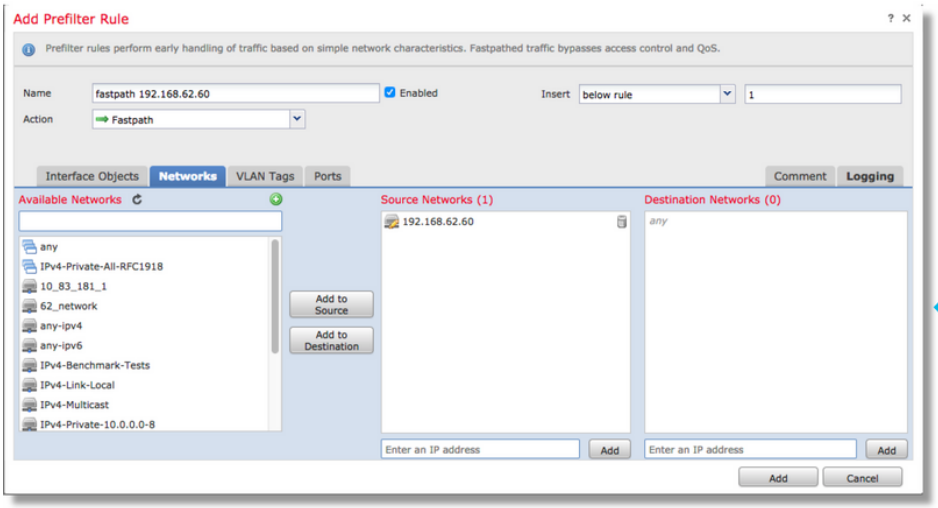
Su tutte le piattaforme FTD è presente una Policy Pre-Filter, che può essere utilizzata per deviare il traffico dall'ispezione Firepower (snort).

Nel FMC, è disponibile in **Policy > Controllo di accesso > Prefiltro**. Impossibile modificare il criterio di prefiltro predefinito. È quindi necessario creare un criterio personalizzato.

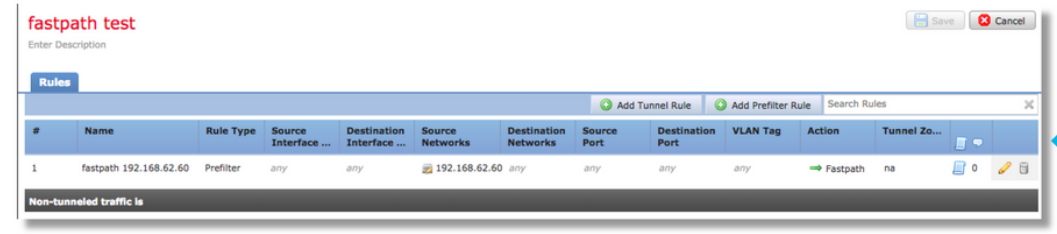
In seguito, è necessario associare il nuovo criterio di filtro al criterio di controllo dell'accesso. Questa impostazione è configurata nella scheda Avanzate di Criteri di controllo di accesso della

sezione **Impostazioni criteri filtro preliminare**.

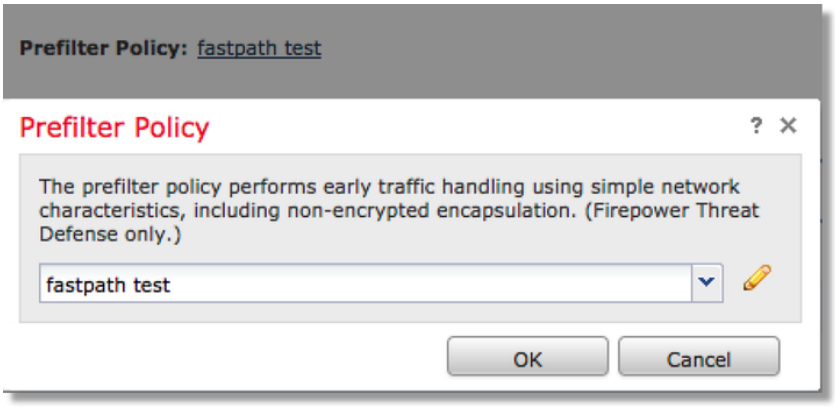
Di seguito è riportato un esempio di come creare una regola Fastpath in un criterio di prefiltro e verificare il numero di accessi.



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

[Fare clic qui](#) per ulteriori dettagli sul funzionamento e la configurazione dei criteri di prefiltro.

Se l'aggiunta di un criterio PreFilter risolve il problema di traffico, è possibile lasciare la regola attiva. Tuttavia, non viene effettuata alcuna ulteriore ispezione di tale flusso. Sarà necessario eseguire ulteriori operazioni di risoluzione dei problemi del software Firepower.

Se l'aggiunta del criterio di prefiltro non risolve il problema, è possibile eseguire nuovamente il pacchetto con la fase di traccia per tracciare il nuovo percorso del pacchetto.

Dati da fornire a TAC

Dati	Istruzioni
Output dei comandi	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-asa-00.html Per Firepower: http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-sourcefire-00.html
Output ASA 'show tech'	Accedere alla CLI di ASA e salvare la sessione terminale in un log. Immettere **il comando sh** 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 traffico	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techno

Passaggio successivo

Se è stato determinato che il problema è causato da un componente software Firepower, il passaggio successivo consiste nell'escludere sistematicamente ogni componente, a partire da Security Intelligence.

Fare clic qui per procedere con la guida successiva.