

Firepower Data Path Problemen opsporen en verhelpen fase 2: DAQ-laag

Inhoud

[Inleiding](#)

[Platform Guide](#)

[Problemen oplossen in de DAQ-fase van Firepower](#)

[Opname van verkeer op de DAQ-laag](#)

[Firepower omzeilen](#)

[SFR - Plaats de FirePOWER-module in de alleen-monitor](#)

[FTD \(alle\) - Plaats inline sets in TAP-modus](#)

[Packet Tracer gebruiken om problemen op te lossen met gesimuleerd verkeer](#)

[SFR - Run Packet Tracer op ASA CLI](#)

[FTD \(alle\) - Draai pakkettracer op de FTD CLI](#)

[Opname met sporen gebruiken voor probleemoplossing in levend verkeer](#)

[FTD \(alle\) - Doorlopende opname met sporen op FMC GUI](#)

[Een voorfilter snellen in een FTD maken](#)

[Gegevens om te leveren aan TAC](#)

[Volgende stap](#)

Inleiding

Dit artikel maakt deel uit van een reeks artikelen waarin wordt uitgelegd hoe u het gegevenspad op FirePOWER-systemen systematisch moet oplossen om te bepalen of onderdelen van Firepower invloed kunnen hebben op het verkeer. Raadpleeg het [gedeelte Overzicht](#) voor informatie over de architectuur van FirePOWER-platforms en de koppelingen naar de andere artikelen voor probleemoplossing in datacenters.

In dit artikel kijken we naar de tweede fase van de probleemoplossing bij het FirePOWER-gegevenspad: de DAQ-laag (gegevensverzameling).



Platform Guide

In de volgende tabel worden de onder dit artikel vallende platforms beschreven.

Naam van platform	Beschrijving	toepasbaar Hardware Platforms	Opmerkingen
SFR	ASA met FirePOWER Services (SFR) module	ASA-5500-X Series Next-Generation	N.v.t.

geïnstalleerd.

FTD (alle)	Is van toepassing op alle FTD-platforms (Firepower Threat Defense)	ASA-5500-X Series, virtuele NGFW-platforms, FPR-2100, FPR-9300, FPR-4100	N.v.t.
FTD (niet-SSP en FPR-2100)	FTD-afbeelding geïnstalleerd op een ASA of een virtueel platform	ASA-5500-X Series, virtuele NGFW-platforms, FPR-2100	N.v.t.
FTD (SSP)	FTD geïnstalleerd als logisch apparaat op een op Firepower eXtensible Operative System (FXOS) gebaseerd chassis	FPR-9300, FPR-4100	De 2100-serie gebruikt niet de FXOS Chassis Manager

Problemen oplossen in de DAQ-fase van Firepower

De DAQ (Data Acquisition) Layer is een component van Firepower die pakketten vertaalt naar een formulier dat snort kan begrijpen. Eerst moet het pakje worden verwerkt wanneer het naar de snelmodus wordt gestuurd. Als de pakketten daarom handmatig worden ingesteld maar het FirePOWER-apparaat niet verwijderen of als de probleemoplossing bij de pakketvastlegging geen nuttige resultaten oplevert, kan het oplossen van DAQ nuttig zijn.

Opname van verkeer op de DAQ-laag

Om snel te kunnen vragen van wie om de opname te starten, moet u eerst het gebruik van SSH verbinden met het SFR of FTD IP adres.

Opmerking: Ga eerst op de FPR-9300 en 4100 apparaten **verbinding met fdd** in om bij de tweede >melding te eindigen. U kunt ook SSH in de FXOS Chassis Manager IP invoeren en dan **module 1 console** invoeren, gevolgd door **ftd aansluiten**.

Dit [artikel](#) legt uit hoe u pakketvastlegging op het niveau van Firepower DAQ kunt verzamelen.

Merk op dat de syntaxis niet hetzelfde is als de opdracht **opname** die wordt gebruikt in ASA en ook de LINA-kant van het FTD-platform. Hier is een voorbeeld van een DAQ pakketvastlegging die vanuit een FTD-apparaat wordt uitgevoerd:

```
> 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
```

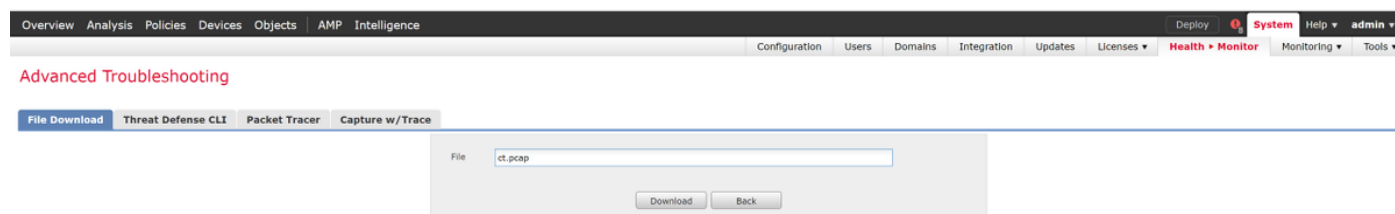
```
admin@ciscoasa:~$ ls /ngfw/var/common/
```

```
ct.pcap
```

Zoals te zien is in het bovenstaande screenshot, is een opname in het PCAP-formaat, ct.pcap, geschreven naar de `/ngfw/var/common` folder (`/var/common` op het SFR-platform). Deze opnamebestanden kunnen van het FirePOWER-apparaat uit de `>`-prompt worden gekopieerd met behulp van de aanwijzingen in het bovengenoemde [artikel](#).

U kunt ook in Firepower Management Center (FMC) in Firepower versie 6.2.0 en hoger navigeren naar **Apparaten > Apparaatbeheer**. Klik vervolgens op de  pictogram naast het apparaat in kwestie, gevolgd door **Advanced Problemen opsporen en verhelpen > Bestand downloaden**.

U kunt vervolgens de naam van het opnamebestand invoeren en op Downloaden klikken.



Firepower omzeilen

Als Firepower het verkeer ziet, maar het is vastgesteld dat de pakketten het apparaat niet uitgraven of dat er een ander probleem is met het verkeer, dan zou de volgende stap zijn om de inspectie van de vuurkracht te omzeilen om te bevestigen dat een van de onderdelen van de vuurkracht het verkeer laat vallen. Hierna volgt een uitsplitsing van de snelste manier om verkeersbypass Firepower op de verschillende platforms te hebben.

SFR - Plaats de FirePOWER-module in de alleen-monitor

Op ASA die de SFR gastheer is, kunt u de SFR module in monitor-only modus via de ASA Opdracht Line Interface (CLI) of de Cisco Adaptieve Security ApparaatManager (ASDM) plaatsen. Hierdoor wordt slechts een kopie van de levende pakketten naar de SFR-module verzonden.

Om de SFR-module in monitor-only modus via de ASA CLI te plaatsen, moeten de class-map en de beleidskaart die gebruikt worden voor SFR-omleiding eerst worden bepaald door de opdracht van de **showservice-beleidssfr uit te voeren**.

```
# 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
```

De output laat zien dat de global_policy map het aanwenden van de sfr fail-open action op de "sfr" class-map afdwingt.

Opmerking: "fail-close" is ook een modus waarin de SFR kan lopen, maar het wordt niet zo vaak gebruikt omdat het al verkeer blokkeert als de SFR module is neergeslagen of niet reageert.

Om de SFR-module in monitor-only modus te plaatsen, kunt u deze opdrachten uitvoeren om de huidige SFR-configuratie te negeren en de monitor-only configuratie in te voeren:

```
# 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...
```

Nadat de module in monitor-only modus is geplaatst, kan deze in de **show service-beleid**-output worden geverifieerd.

```
# 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
```

Opmerking: Om de SFR module terug te plaatsen in inline mode, geef de **geen veiligheids-open monitor-only** opdracht uit van de (configuratie-kaart-c)# hierboven getoond, gevolgd door de **sfr {faalopen | fail-close}** opdracht die er oorspronkelijk was.

In plaats hiervan kunt u de module ook via de ASDM in monitor-only plaatsen door in te navigeren op **Configuration > Firewall > Service Policy Regels**. Klik vervolgens op de betreffende regel. Ga vervolgens naar de pagina **Handelingen** in de **regel** en klik op het tabblad **ASA FirePOWER Inspection**. Wanneer er eenmaal een **monitor** is geïnstalleerd, kan **alleen** de monitor worden geselecteerd.

Als het verkeersprobleem blijft bestaan, zelfs nadat is bevestigd dat de SFR-module in de monitor-only modus staat, veroorzaakt de Firepower module niet de kwestie. Packet tracer kan dan worden gebruikt om kwesties op ASA-niveau verder te diagnosticeren.



Als de kwestie niet langer overblijft, zou de volgende stap zijn om de componenten van de software van het Vuurwerk op te lossen.

FTD (alle) - Plaats inline sets in TAP-modus

Als het verkeer door interfacekaarten gaat die in inline sets zijn geconfigureerd, kan de inline set in TAP-modus worden geplaatst. Dit zorgt er in wezen voor dat Firepower geen actie onderneemt op het live pakket. Het is niet van toepassing op router of transparante modus zonder inline sets omdat het apparaat de pakketten moet wijzigen voordat u ze naar de volgende hop stuurt en niet in een bypass-modus kan worden geplaatst zonder verkeer te laten vallen. Ga voor routekaarten en transparante modus zonder inline sets verder met de stap van de pakkettracer.

Om TAP-modus te configureren vanuit de FMC User Interface (UI), navigeer naar **Apparaten > Apparaatbeheer** en bewerken vervolgens het apparaat in kwestie. Schakel de optie voor de **TAP-modus** uit op het tabblad **Inline Series**.

The screenshot displays the FMC User Interface for configuring an inline set. The top navigation bar includes tabs for **Devices**, **Routing**, **Interfaces**, **Inline Sets** (selected), and **DHCP**. Below the navigation bar is a table with the following content:

Name	Interface Pairs	
my_inline	inline1<->inline2	 

A callout box titled **Edit Inline Set** is shown, with the **Advanced** tab selected. The **Tap Mode:** checkbox is highlighted with a red box and is currently unchecked. Other options shown include **Propagate Link State:** and **Strict TCP Enforcement:**, both of which are also unchecked.

Als de TAP-modus het probleem oplost, is de volgende stap het oplossen van de FirePOWER-softwarecomponenten.

Als de TAP-modus het probleem niet oplost, ligt het probleem buiten de FirePOWER-software. Packet tracer kan dan worden gebruikt om het probleem verder te diagnosticeren.

Packet Tracer gebruiken om problemen op te lossen met gesimuleerd verkeer

Packet Tracer is een hulpprogramma dat kan helpen de locatie van een pakketdaling te identificeren. Het is een simulator, dus hij voert een spoor van een kunstpakje uit.

SFR - Run Packet Tracer op ASA CLI

Hier is een voorbeeld van hoe te om pakkettracer op de ASA CLI voor het verkeer van SSH te lopen. Raadpleeg voor meer informatie over de syntaxis van het commando van de pakkettracer deze [sectie](#) in de ASA Series Opdrachtgids.

```
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
```

In het bovenstaande voorbeeld zien we zowel de ASA als SFR module die de pakketten toestaat evenals nuttige informatie over hoe de ASA pakketstroom zou omgaan.

FTD (alle) - Draai pakkettracer op de FTD CLI

Op alle FTD-platforms kan de opdracht van de pakkettracer worden uitgevoerd vanaf de FTD CLI.

```
> 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
```

In dit voorbeeld, toont de pakkettracer de reden voor de daling. In dit geval is het de zwarte lijst van IP in de veiligheidscontrole-functie in Firepower die het pakket blokkeert. De volgende stap is het oplossen van de individuele component van de software van het Vuurwerk die de daling veroorzaakt.

Opname met sporen gebruiken voor probleemoplossing in levend verkeer

Het bewegende verkeer kan ook worden getraceerd via de opname met behulp van een spoorfunctie, die op alle platforms via de CLI beschikbaar is. Hieronder staat een voorbeeld van het uitvoeren van een opname met sporen tegen SSH-verkeer.

```
> 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
```

In dit voorbeeld werd het vierde pakket in de opname getraceerd, omdat dit het eerste pakket is met toepassingsgegevens gedefinieerd. Zoals aangegeven wordt de verpakking uiteindelijk gefloten door een snort, wat betekent dat er geen verdere inspectie van de snort nodig is voor de stroom en dat alles is toegestaan.

Raadpleeg deze [sectie](#) in de ASA Series Opdrachtgids voor meer informatie over de opname met de syntaxis van sporen.

FTD (alle) - Doorlopende opname met sporen op FMC GUI

Op de FTD-platforms kan opname met sporen worden uitgevoerd op de FMC UI. Om toegang tot het hulpprogramma te krijgen, navigeer naar **Apparaten > Apparaatbeheer**.

Klik vervolgens op de  pictogram naast het apparaat in kwestie, gevolgd door **Advanced Troubleshooter > Capture met Trace**.

Hieronder zie je een voorbeeld van hoe je een opname met overtrekken kunt uitvoeren via de GUI.

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

Name	Interface	Type	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status
Test	Inside	raw-data	✓	524288	1518	Capturing	TCP	192.168.1.200	any	Running	

View of all current captures

```

Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
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: EXTERNAL-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-interfaces: Inside
input-status: up
  
```

Example output shows the packet was blocked by Snort

Als de opname met overtrekken de oorzaak van de pakketdaling toont, zou de volgende stap de individuele softwarecomponenten probleemoplossing zijn.

Als dit niet duidelijk de oorzaak van het probleem laat zien zou de volgende stap het versnellen van het verkeer zijn.

Een voorfilter snellen in een FTD maken

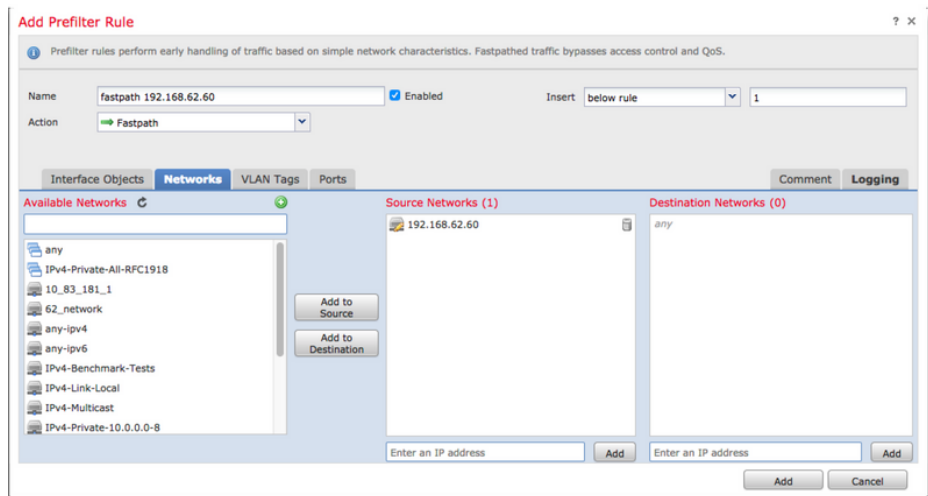
Op alle FTD-platforms is er een Pre-Filter beleid, dat kan worden gebruikt om verkeer af te leiden van FirePOWER-inspectie (snort).

Op het VCC, wordt dit gevonden onder **Beleid > Toegangsbeheer > Prefilter**. Het standaard Pre-Filter beleid kan niet worden bewerkt, dus moet er een aangepast beleid worden gemaakt.

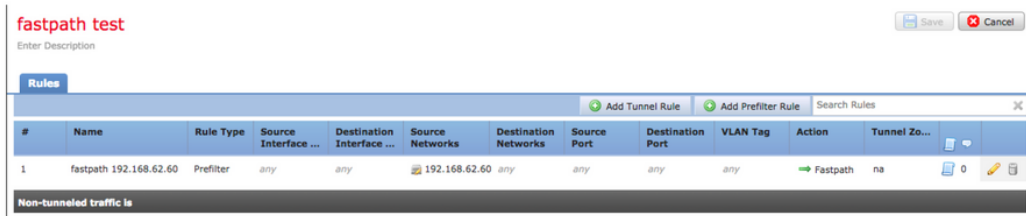
Daarna moet het nieuw gecreëerde prefilterbeleid worden gekoppeld aan het toegangscontrolebeleid. Dit wordt ingesteld in het tabblad Geavanceerd van het beleid voor

toegangscontrole in het gedeelte **Prefilter Policy Settings**.

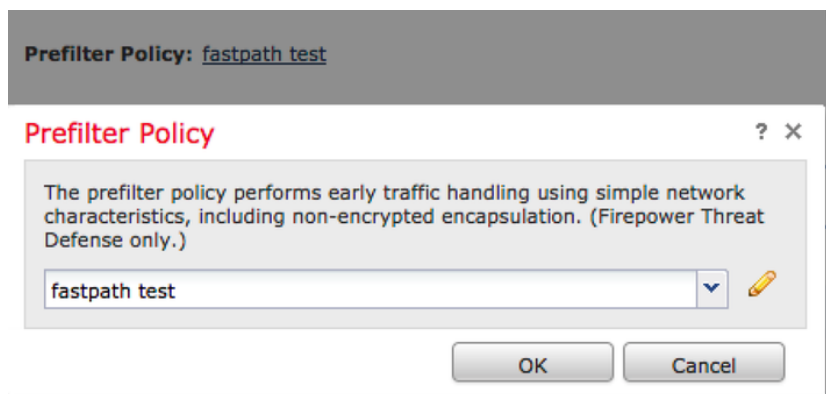
Hieronder zie je hoe je een Fastpath-regel kunt maken in een prefilterbeleid en de hit-teller kunt controleren.



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

[Klik hier](#) voor meer informatie over de werking en configuratie van het prefilterbeleid.

Als het toevoegen van een PreFilter beleid het verkeersprobleem oplost, kan de regel op zijn plaats worden verlaten indien gewenst. Er wordt echter geen verdere inspectie van deze stroom verricht. Er moet meer worden gedaan voor het opsporen en verhelpen van problemen bij de FirePOWER-software.

Als het toevoegen van het Prefilter Policy de kwestie niet oplost, kan het pakket met stappen overtrekken opnieuw worden uitgevoerd om het nieuwe pad van het pakket te overtrekken.

Gegevens om te leveren aan TAC

Gegevens

Opdracht-uitgangen

Instructies

Zie dit artikel voor instructies

Voor ASA/LINA: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-5/asa-00.html>

Packet Capture

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

ASA 'show tech'-
uitvoer

Log in op ASA CLI en de eindsessie wordt opgeslagen op een logbestand. Typ de naam van de eindsessie aan TAC op.

Dit bestand kan met deze opdracht op schijf of een extern opslagsysteem worden opgeslagen:
show tech | redirect disk0:/show_tech.log

Probleemoplossing
bestand via het

FirePOWER-apparaat dat het verkeer controleert
<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117777.html>

Volgende stap

Als is vastgesteld dat een component van de Firepower software de oorzaak is van de zaak, zou de volgende stap zijn om systematisch elke component uit te sluiten, om te beginnen met Security Intelligence.

Klik [hier](#) om verder te gaan met de volgende handleiding.