

# Firepower Data Path Problemen opsporen en verhelpen fase 8: Beleid voor netwerkanalyse

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Problemen oplossen met de beleidsfunctie voor netwerkanalyse](#)

[Het "overtrekken"-gereedschap gebruiken om pré-druppels te zoeken \(alleen FTD\)](#)

[Controleer NAP-configuratie](#)

[NAP-instellingen weergeven](#)

[NAP-instellingen die slapende druppels kunnen veroorzaken](#)

[Controleer de configuratie van de achterzijde](#)

[Een doelgerichte NAP maken](#)

[Onjuist positieve analyse](#)

[Beperkingsstappen](#)

[Gegevens om te leveren aan TAC](#)

## 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 [Overzicht artikel](#) voor informatie over de architectuur van FirePOWER-platforms en de koppelingen naar de andere artikelen voor probleemoplossing in datacenters.

Dit artikel bestrijkt de achtste fase van de probleemoplossing bij het gebruik van FirePOWER-gegevens, de beleidsfunctie voor netwerkanalyse.



## Voorwaarden

- Dit artikel is van toepassing op alle FirePOWER-platforms  
De spoorfunctie is alleen beschikbaar in softwareversie 6.2.0 en hoger voor het Firepower Threat Defense (FTD) platform.
- Kennis van opensource is behulpzaam, maar niet nodig Kijk op <https://www.snort.org/> voor meer informatie over open source snort.

## Problemen oplossen met de beleidsfunctie voor netwerkanalyse

Het Network Analysis Policy (NAP) bevat hyperprocessorinstellingen die inspecties uitvoeren op

verkeer, gebaseerd op de geïdentificeerde toepassing. De preprocessoren hebben de mogelijkheid om verkeer te beperken op basis van de configuratie. Dit artikel beschrijft hoe de NAP-configuratie moet worden geverifieerd en hoe op de druppels van de voorprocessor moet worden gecontroleerd.

Opmerking: Voorbeweringsregels hebben een generator-ID (GID) anders dan '1' of '3' (d.w.z. 129, 119, 124). Meer informatie over de GID naar de voorverwerker-indeling is te vinden in de FMC [Configuration Guides](#).

## Het "overtrekken"-gereedschap gebruiken om pré-druppels te zoeken (alleen FTD)

Het **systeem** ter ondersteuning van het spoor kan worden gebruikt om vallen op te sporen die op het niveau van de voorprocessor zijn uitgevoerd.

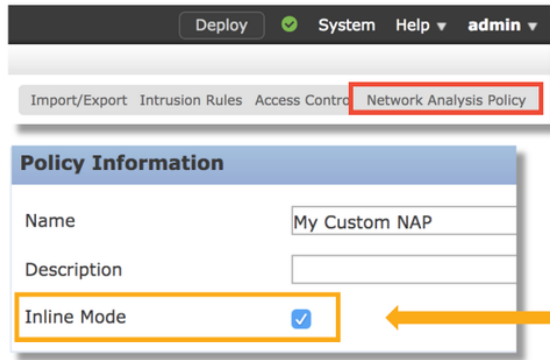
In het onderstaande voorbeeld, ontdekte de TCP-normalisatie voorprocessor een anomalie. Als resultaat hiervan wordt het verkeer gedropt door regel **129:14**, die op ontbrekende tijden binnen een TCP-stream zoekt.

```
> system support trace
[omitted for brevity...]
172.16.111.226-51174 - 50.19.123.95-443 6 Packet: TCP, ACK, seq 3849839667, ack 1666843207
172.16.111.226-51174 - 50.19.123.95-443 6 Stream: TCP normalization error in timestamp, window, seq, ack, fin, flags, or
unexpected data, drop
172.16.111.226-51174 - 50.19.123.95-443 6 AppID: service unknown (0), application unknown (0)
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 | 0 Starting with minimum 3, 'block urls', and SrcZone first with zones -1 -> -1, geo 0 ->
0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 | 0 pending rule order 3, 'block urls', URL
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: pending rule-matching, 'block urls', pending URL
172.16.111.226-51174 > 50.19.123.95-443 6 Snort: processed decoder alerts or actions queue, drop
172.16.111.226-51174 > 50.19.123.95-443 6 IPS Event: gid 129, sid 14, drop
172.16.111.226-51174 > 50.19.123.95-443 6 NAP id 1, IPS id 0, Verdict BLOCK
172.16.111.226-51174 > 50.19.123.95-443 6 ==>> Blocked by Stream
```

Opmerking: Hoewel de voorprocessor van de **TCP-stream** het verkeer verlaagt, kan dit ook omdat de voorprocessor van de **inline normalisatie** ook is ingeschakeld. Voor meer over inline normalisatie kunt u dit [artikel](#) lezen.

## Controleer NAP-configuratie

Op Firepower Management Center (FMC) UI kan de NAP worden bekeken onder **beleid > Toegangsbeheer > Inbraaklijden**. Klik vervolgens op de optie **Network Analysis Policy** in de rechtsboven, waarna u de NAP's kunt bekijken, nieuwe kunt maken en bestaande opties kunt bewerken.



Edit or create a Network Analysis Policy

Uncheck this box to disable Inline Mode

Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
	172.16.111.226	50.19.123.95	51177 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)

Inline Mode disabled = No Inline Result

Inline Mode enabled = "Dropped" Inline Result

Zoals in de afbeelding hierboven wordt getoond, bevatten de NAP's een optie "Inline mode", die gelijk is aan de optie "Drop Wanneer Inline" in het Inbraakbeleid. Een snelle matigingsstap om te voorkomen dat de NAP het verkeer laat vallen zou zijn om de **inline-modus** uit te schakelen. De inbraakgebeurtenissen die door het NAP zijn gegenereerd geven niets weer in het tabblad **Inline Resultaat** met inline modus uitgeschakeld.

## NAP-instellingen weergeven

Binnen het NAP kunt u de huidige instellingen bekijken. Hieronder vallen de totale toegestane preprocessoren, gevolgd door de

preprocessoren die worden ingeschakeld met niet-standaardinstellingen (die handmatig worden getweekt) en instellingen die worden ingeschakeld met standaardinstellingen, zoals in de onderstaande afbeelding wordt weergegeven.

Edit Policy: My Custom NAP

**View preprocessors** →

**Currently Enabled**

**Enabled with non-default settings**

**Enabled with default settings**

## NAP-instellingen die slapende druppels kunnen veroorzaken

In het voorbeeld dat in het springsgedeelte wordt genoemd, laat de regel TCP-streamconfiguratieregel **129:14** verkeer vallen. Dit wordt bepaald door te kijken naar de uitvoer **van de sporen die het systeem ondersteunt**. Indien de genoemde regel echter niet is ingeschakeld in het betreffende inbraakbeleid, worden geen inbraakgebeurtenissen naar het VCC gestuurd.

De reden waarom dit gebeurt is te wijten aan een instelling binnen de voorprocessor **Inline Normalization, Blok Onoplosbare TCP-headeranaloge** genaamd. Met deze optie kan Snort een blokactie uitvoeren wanneer bepaalde GID 129-regels anomalieën in de TCP-stroom detecteren.

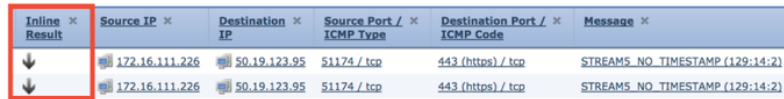
Als de **Anomalies van de Kop TCP onoplosbaar blokkeren** zijn ingeschakeld, wordt aanbevolen de GID 129-regels in te schakelen, zoals aangegeven in de onderstaande afbeelding.

The screenshot displays the 'Intrusion Policy' configuration window. At the top, a filter is set to 'GID:"129"'. Below the filter, there are tabs for 'Rule State', 'Event Filtering', 'Dynamic State', 'Alerting', and 'Comments'. A table lists 19 rules, all with GID 129, and all are checked. A context menu is open over rule 129:14, showing options: 'Generate Events', 'Drop and Generate Events', and 'Disable'. To the right, the 'Policy Information' panel is open, showing various settings. The 'Inline Normalization' section is expanded, and the 'Block Unresolvable TCP Header Anomalies' option is checked and highlighted with a red box.

Rule ID	Action	Rule Name
129 4	<input checked="" type="checkbox"/>	STREAM5_BAD_TIMESTAMP
129 5	<input type="checkbox"/>	STREAM5_BAD_SEGMENT
129 6	<input checked="" type="checkbox"/>	STREAM5_WINDOW_TOO_LARGE
129 7	<input type="checkbox"/>	STREAM5_EXCESSIVE_TCP_OVERLAPS
129 8	<input checked="" type="checkbox"/>	STREAM5_DATA_AFTER_RESET
129 9	<input type="checkbox"/>	STREAM5_SESSION_HIJACKED_CLIENT
129 10	<input type="checkbox"/>	STREAM5_SESSION_HIJACKED_SERVER
129 11	<input checked="" type="checkbox"/>	STREAM5_DATA_WITHOUT_FLAGS
129 12	<input type="checkbox"/>	STREAM5_SMALL_SEGMENT
129 13	<input type="checkbox"/>	STREAM5_4WAY_HANDSHAKE
129 14	<input checked="" type="checkbox"/>	STREAM5_NO_TIMESTAMP
129 15	<input checked="" type="checkbox"/>	STREAM5_BAD_RST
129 16	<input checked="" type="checkbox"/>	STREAM5_BAD_FIN
129 17	<input checked="" type="checkbox"/>	STREAM5_BAD_ACK
129 18	<input checked="" type="checkbox"/>	STREAM5_DATA_AFTER_RST_RCVD
129 19	<input checked="" type="checkbox"/>	STREAM5_WINDOW_SLAM

Door de GID 129-regels in te voeren worden inbraakgebeurtenissen naar het VCC gestuurd wanneer zij actie ondernemen op het verkeer. Maar zolang de **blokonoplosbare TCP-headeranaloge** is ingeschakeld, kan deze nog steeds verkeer laten vallen zelfs als de **regelstatus** in het inbraakbeleid alleen **gebeurtenissen** zal **genereren**. Dit gedrag wordt uitgelegd in de Configuratiehandleidingen van FMC.

Still drops after setting to generate



Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)

## Check configuration guide for relative protocols/preprocessors:

### Block Unresolvable TCP Header Anomalies

When you enable this option, the system blocks anomalous TCP packets that, if normalized, would be invalid and likely would be blocked by the receiving host. For example, the system blocks any SYN packet transmitted subsequent to an established session.

The system also drops any packet that matches any of the following TCP stream preprocessor rules, regardless of whether the rules are enabled:

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 through 129:19

The Total Blocked Packets performance graph tracks the number of packets blocked in inline deployments and, in passive deployments and inline deployments in tap mode, the number that would have been blocked in an inline deployment.

Bovenstaande documentatie is te vinden in dit [artikel](#) (voor versie 6.4, de meest recente versie ten tijde van de publicatie van dit artikel).

## Controleer de configuratie van de achterzijde

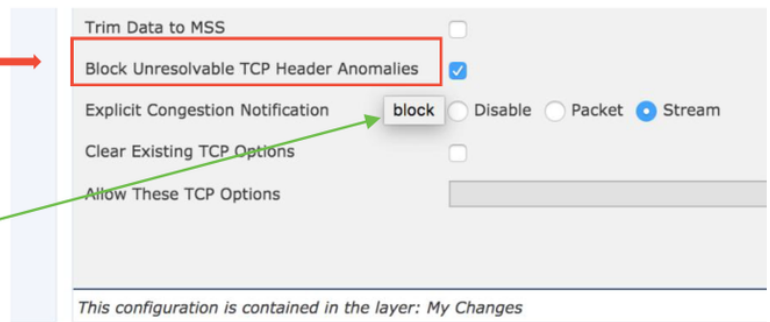
Een andere laag van complexiteit wordt toegevoegd aan het gedrag van de preprocessor in die zin dat bepaalde instellingen op de backend kunnen worden ingeschakeld zonder dat dit in het FMC wordt weerspiegeld. Dit zijn een paar mogelijke redenen.

- Andere enabled-functies hebben de mogelijkheid om preprocessor instellingen (de belangrijkste is File Policy) te forceren
- Sommige inbraakbeleidsregels vereisen bepaalde voorprocessoropties om detectie uit te voeren
- Een defect kan het gedrag veroorzaken We hebben één voorbeeld hiervan gezien: [CSCuz50295](#) - "Het bestandsbeleid met Malware-blok maakt TCP-normalisatie mogelijk met blokvlag"

Voordat u de configuratie van de achterzijde bekijkt, moet u bedenken dat de trefwoorden van de snort, die gebruikt worden in de configuratiebestanden van de backend-snort, kunnen worden gezien door de instelling van een specifieke instelling binnen de NAP. Raadpleeg de onderstaande illustratie.

Hover over option to see backend snort configuration keyword

Snort config keyword is "block"



De optie **Onoplosbare TCP-headeranaloge** blokkering in het tabblad NAP vertaalt zich naar het **blokkwoord** op de achterkant. Met die informatie in gedachten, kan de backend configuratie worden gecontroleerd van het shell van de experts.

```
root@ciscoasa:~# de_info.pl
-----
DE Name      : Primary Detection Engine (c9ef19d6-e187-11e6-ba76-99617d53da68)
DE Type      : ids
DE Description : Primary detection engine for device c9ef19d6-e187-11e6-ba76-99617d53da68
DE Resources  : 1
DE UUID      : 0d82120c-e188-11e6-8606-a4827d53da68
-----

root@ciscoasa:~# cd /var/sf/detection_engines/0d82120c-e188-11e6-8606-a4827d53da68/network_analysis/
root@ciscoasa: network_analysis# ls
b50f27b0-e31a-11e6-b866-dd9e65c01d56 object_b50f27b0-e31a-11e6-b866-dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-
dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-dd9e65c01d56.default
root@ciscoasa: network_analysis# cat b50f27b0-e31a-11e6-b866-dd9e65c01d56/normalize.conf
#
# generated from My Changes
#
preprocessor normalize_tcp: ips, rsv, pad, req_urg, req_pay, req_urp, block
```

"block" option is enabled in normalize.conf

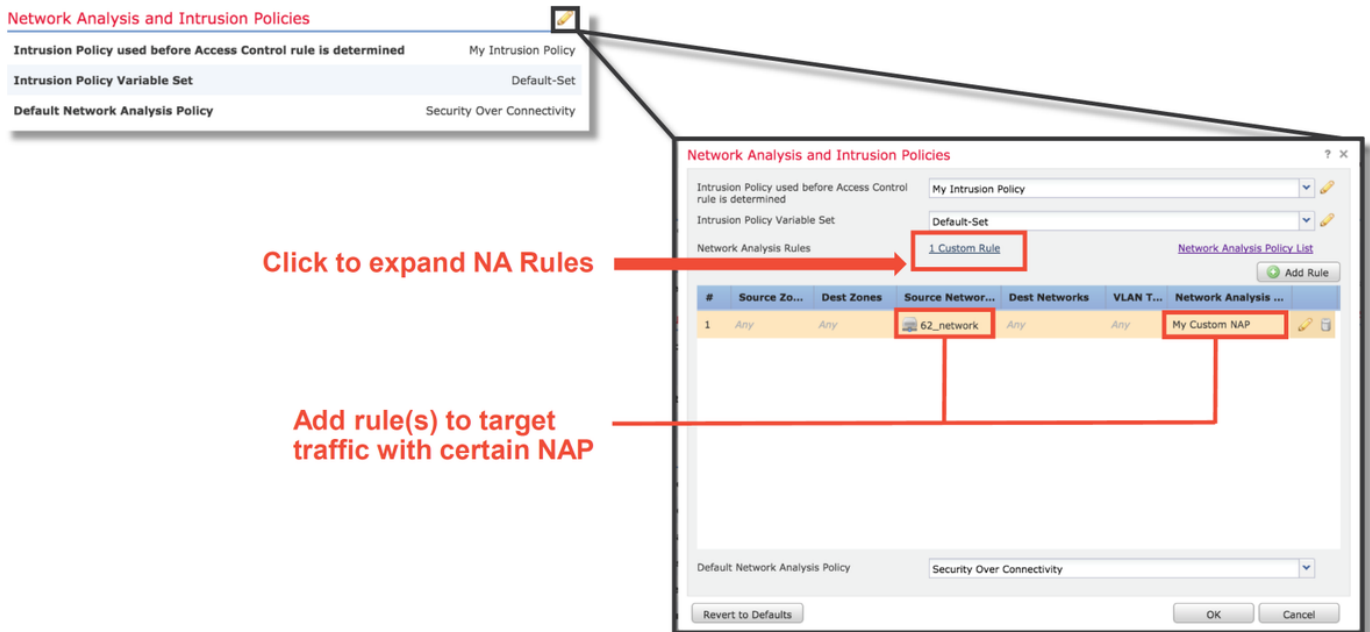
## Een doelgerichte NAP maken

Als bepaalde hosts pre-processor gebeurtenissen in werking stellen, kan een aangepaste NAP worden gebruikt om verkeer naar of van genoemde hosts te inspecteren. Binnen de aangepaste NAP kunnen de instellingen die problemen veroorzaken worden uitgeschakeld.

Dit zijn de stappen voor de implementatie van een doelgericht NAP.

1. Maak het NAP volgens de instructies die in de verify-configuratie van dit artikel worden vermeld.
2. In het **tabblad Geavanceerd** van het beleid voor toegangscontrole kunt u navigeren naar het gedeelte **Netwerkanalyse en inbraakbeleid**. Klik op **Regel toevoegen** en maak een regel, met behulp van de gerichte hosts en kies de nieuwe NAP in de sectie **Netwerkanalyse**.





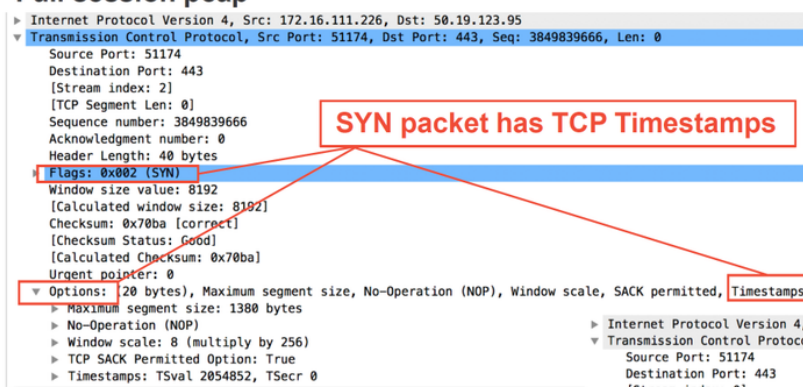
## Onjuist positieve analyse

Het controleren op valse positieven in inbraakgebeurtenissen is voor de regels van de preprocessor heel anders dan die van de regels van de Snort die voor de regevaluatie worden gebruikt (die een GID van 1 en 3 bevatten).

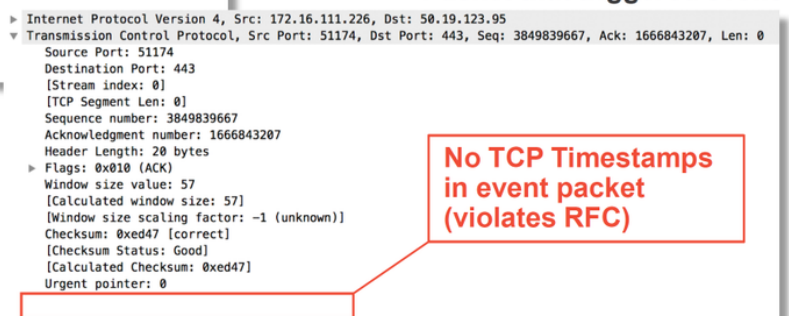
Om een valse positieve analyse voor preprocessor regelgebeurtenissen uit te voeren is een volledige sessieopname nodig om anomalieën in de TCP stream te zoeken.

In het onderstaande voorbeeld wordt op regel 129:14 een fout-positieve analyse uitgevoerd, waarbij in de bovenstaande voorbeelden is aangetoond dat het verkeer afneemt. Sinds 129:14 op zoek is naar TCP-stromen waarin tijdstempels ontbreken, kunt u duidelijk zien waarom de regel is geactiveerd per de pakketvastlegging analyse die hieronder wordt geïllustreerd.

### Full session pcap



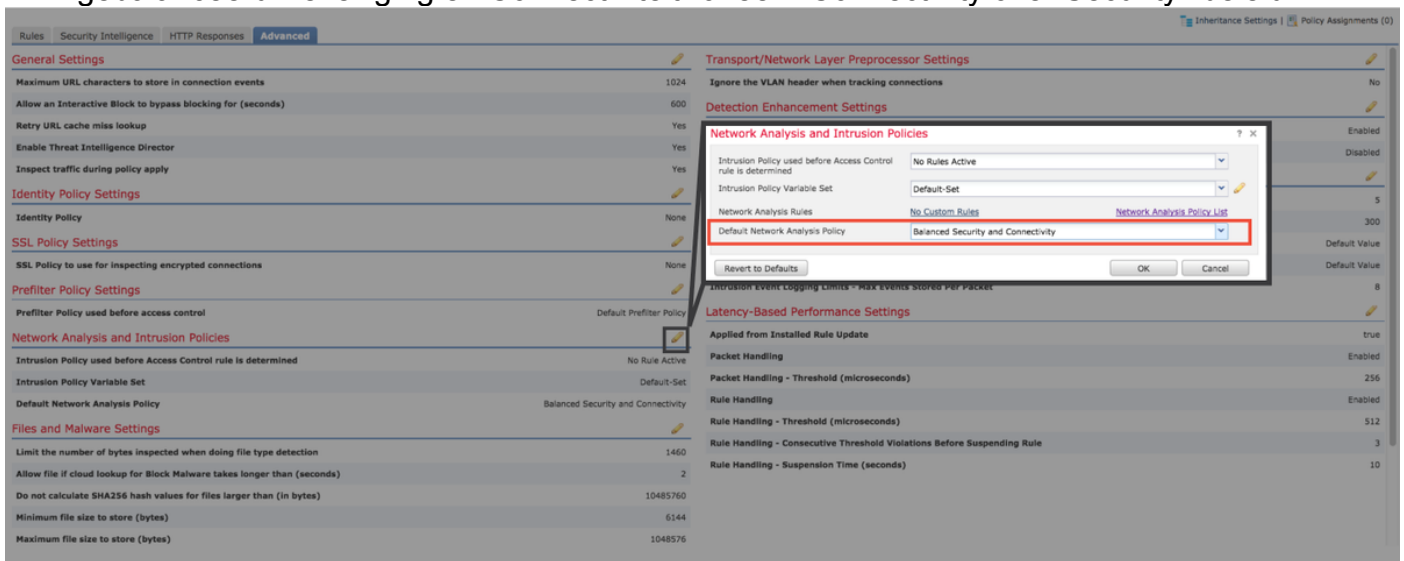
### Packet that triggered event



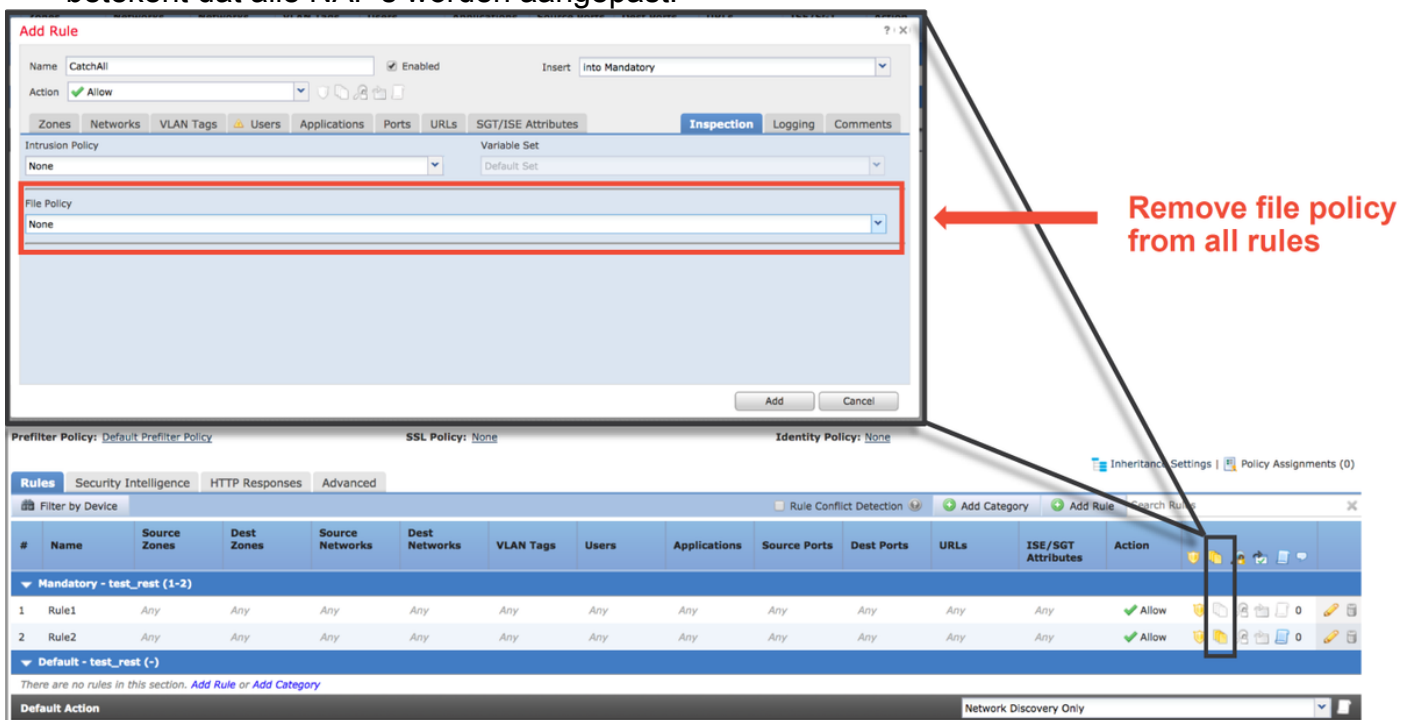
## Beperkingsstappen

Om mogelijke problemen met de NAP snel te verhelpen, kunnen de volgende stappen worden uitgevoerd.

- Als een aangepaste NAP wordt gebruikt en u weet niet of een NAP-instelling verkeer laat vallen maar u vermoedt dat dit het geval is, kunt u proberen het te vervangen door een "gebalanceerd Beveiliging en Connectiviteit" of een "Connectivity over Security"-beleid.



- Als er "Aangepaste regels" worden gebruikt, zorg er dan voor dat u de NAP op een van de bovengenoemde standaardinstellingen instelt
- Als een toegangscontroleregeling een bestandsbeleid gebruikt, moet u misschien tijdelijk proberen het te verwijderen omdat een bestandsbeleid instellingen op de backend mogelijk maakt die niet in het FMC worden weergegeven. Dit gebeurt op een 'mondiaal' niveau, wat betekent dat alle NAP's worden aangepast.



Elk protocol heeft een andere preprocessor en het oplossen ervan kan zeer specifiek zijn voor de preprocessor. Dit artikel heeft geen betrekking op alle instellingen van de voorprocessor en de methoden voor het opsporen en verhelpen van fouten voor elk van deze producten.

U kunt de documentatie voor elke preprocessor controleren om een beter idee te krijgen van wat



elke optie doet, wat behulpzaam is bij het oplossen van een specifieke preprocessor.

## Gegevens om te leveren aan TAC

### Gegevens

Bestand van  
probleemoplossing  
via het FirePOWER-  
apparaat

Full Session Packet

Capture van het  
FirePOWER-apparaat

### Instructies

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1170>

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series>