

# Inzicht in acties door beleidsregels inzake toegangscntrole van Firepower Threat Defense

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Hoe ACP wordt geïmplementeerd](#)

[Configureren](#)

[Beschikbare ACP-acties](#)

[Hoe ACP en het voorfilterbeleid samenwerken](#)

[Block-actie van ACP](#)

[Scenario 1: Vroege afwijzing in LINA](#)

[Scenario 2: Afwijzing door Snort-oordeel](#)

[Block with reset-actie van ACP](#)

[Allow-actie van ACP](#)

[Scenario 1: Allow-actie van ACP \(L3/L4-voorwaarden\)](#)

[Scenario 2: Allow-actie van ACP \(L3-7-voorwaarden\)](#)

[Scenario 3: Snort fast-forward-oordeel met Allow](#)

[Trust-actie van ACP](#)

[Scenario 1: Trust-actie van ACP](#)

[Scenario 2. ACS-vertrouwensactie \(zonder SI, QoS en identiteitsbeleid\)](#)

[Block-actie van voorfilterbeleid](#)

[Fastpath-actie van voorfilterbeleid](#)

[Fastpath-actie van voorfilterbeleid \(inline-set\)](#)

[Fastpath-actie van voorfilterbeleid \(inline-set met tap-modus\)](#)

[Analyze-actie van voorfilterbeleid](#)

[Scenario 1: Voorfilter Analyze met Block-regel van ACP](#)

[Scenario 2: Voorfilter Analyze met Allow-regel van ACP](#)

[Scenario 3: Voorfilter Analyze met Trust-regel van ACP](#)

[Scenario 4: Voorfilter Analyze met Trust-regel van ACP](#)

[Monitor-actie van ACP](#)

[Interactive Block-actie van ACP](#)

[Interactive Block with reset-actie van ACP](#)

[Secundaire FTD-verbindingen en pinholes](#)

[Richtlijnen voor FTD-regels](#)

[Samenvatting](#)

[Gerelateerde informatie](#)

## Inleiding

In dit document worden de verschillende acties beschreven die beschikbaar zijn binnen het toegangscontrolebeleid (ACP) en het voorfilterbeleid van Firepower Threat Defense (FTD).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Flow-offload
- Packet-opnamen op FirePOWER Threat Defense-apparaten
- Packet Tracer en vastlegging met traceeroptie op FTD-applicaties

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firepower 4110 Threat Defense versie 6.4.0 (build 113) en 6.6.0 (build 90)
- Firepower Management Center (FMC) versie 6.4.0 (build 113) en 6.6.0 (build 90)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

### Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR1000, FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- Geïntegreerde services router (ISR) routermodule
- FTD softwareversie 6.1.x en hoger

**Opmerking:** Flow Offload wordt alleen ondersteund op native exemplaren van de ASA en FTD-toepassingen en op FPR4100 en FPR9300 platforms. FTD container cases ondersteunen flow offload niet.

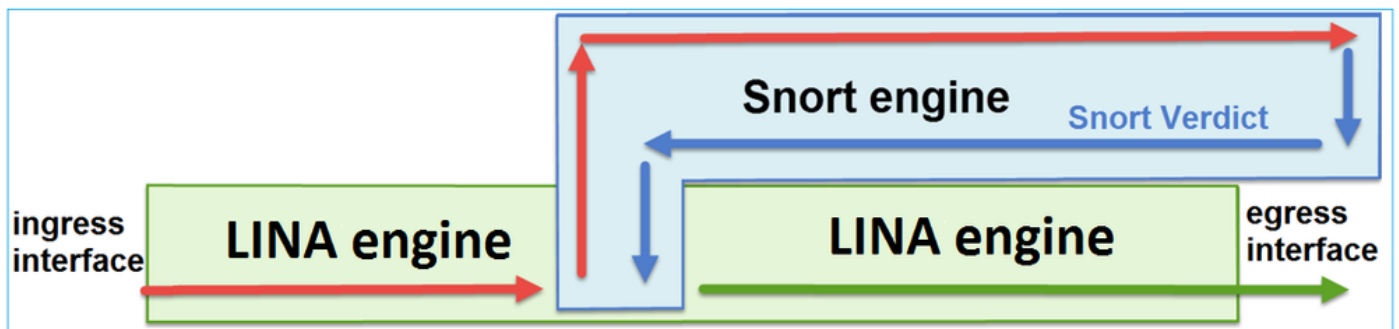
## Achtergrondinformatie

De achtergrondwerking van elke actie wordt onderzocht samen met de interactie ervan met andere functies zoals Flow Offload en protocollen die secundaire verbindingen openen.

FTD is een unified software-image die bestaat uit twee hoofd-engines:

- LINA-engine
- Snort-engine

Deze afbeelding toont de interactie tussen de twee engines:



- Een pakket komt binnen via de inkomende interface en wordt verwerkt door de LINA-engine
- Wanneer het FTD-beleid dit vereist, wordt het pakket geïnspecteerd door de Snort-engine
- De snort engine geeft een vonnis (lijst met vergunningen of lijst met blokken) voor het pakket terug
- De LINA-engine wijst het pakket af of stuurt het door op basis van het Snort-oordeel

## Hoe ACP wordt geïmplementeerd

Het FTD-beleid wordt geconfigureerd op FMC wanneer extern beheer (buiten het apparaat) wordt gebruikt of Firepower Device Manager (FDM) wanneer lokaal beheer wordt gebruikt. In beide scenario's wordt het ACP geïmplementeerd als:

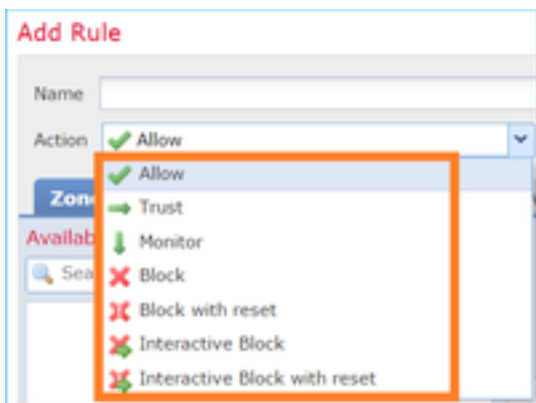
- Een algemene toegangscontrolelijst (ACL) met de naam CSM\_FW\_ACL\_ voor de FTD LINA-engine
- Toegangscontroleregels (AC) in het /ngfw/var/sf/detection\_engines/<UUID>/ngfw.rules-bestand voor de FTD Snort-engine

## Configureren

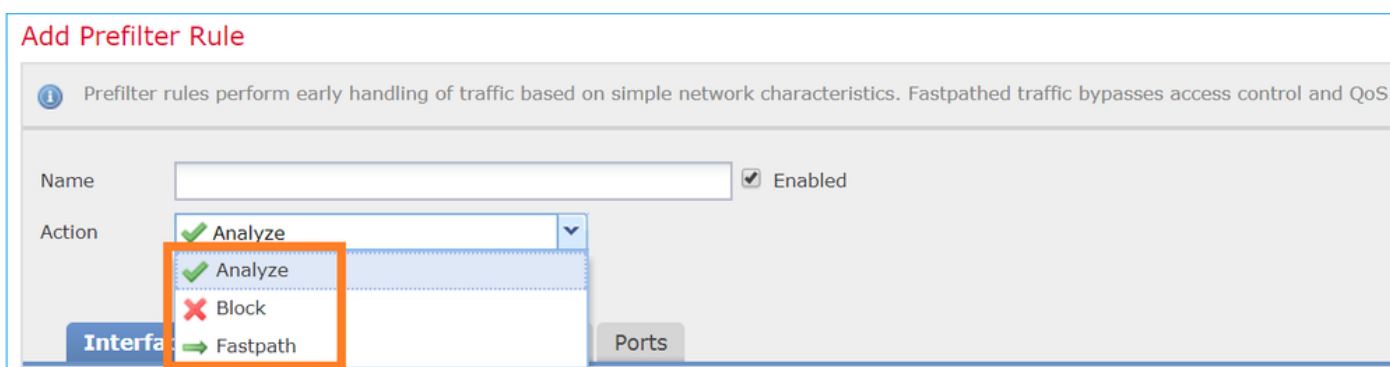
### Beschikbare ACP-acties

Het FTD ACP bevat een of meer regels en elke regel kan een van deze acties hebben, zoals weergegeven in de afbeelding:

- Allow
- Trust
- Monitor
- Block
- Block with reset
- Interactive Block
- Interactive Block with reset



Op dezelfde manier kan een voorfilterbeleid een of meer regels bevatten. De mogelijke acties worden weergegeven in de volgende afbeelding:



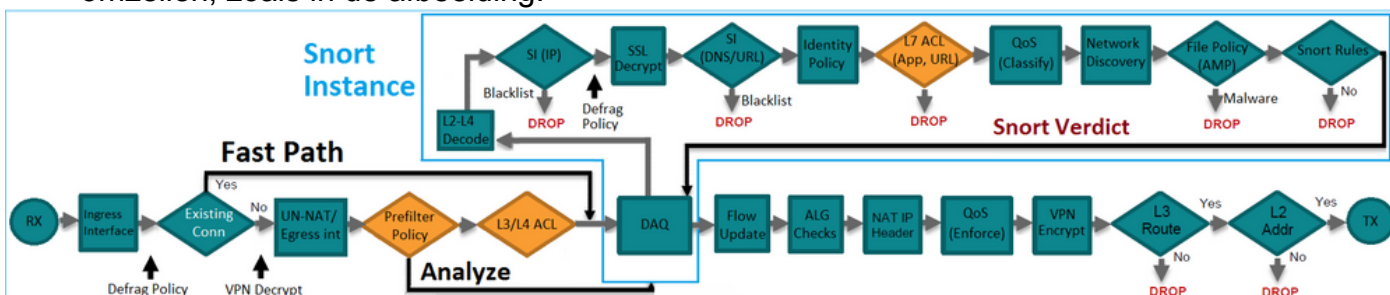
## Hoe ACP en het voorfilterbeleid samenwerken

Het Prefilterbeleid werd geïntroduceerd in versie 6.1 en dient 2 hoofddoelen:

1. Het inspecteren van getunnelde verkeer waarbij de FTD LINA-engine de buitenste IP-header controleert terwijl de Snort-engine de binnenste IP-header controleert. Meer specifiek, in het geval van tunnelverkeer (bijvoorbeeld GRE) zijn de regels in het Prefilterbeleid altijd gericht op de **outer headers**, terwijl de regels in de ACS-staten altijd van toepassing zijn op de interne zittingen (**inner headers**). Het getunnelde verkeer verwijst naar deze protocollen:

- GRE
- IP-in-IP
- IPv6-in-IP
- Teredo-poort 3544

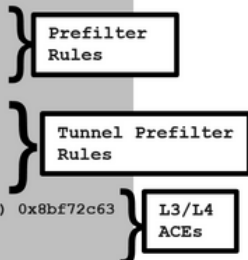
2. Het voorziet in Early Access Control (EAC) waarmee de stroom de Snort-motor volledig kan omzeilen, zoals in de afbeelding.



De Prefilterregels worden op FTD geïmplementeerd als L3/L4 Access Control Elements (ACE's)

en gaan de geconfigureerde L3/L4 ACE's vooraf zoals in de afbeelding:

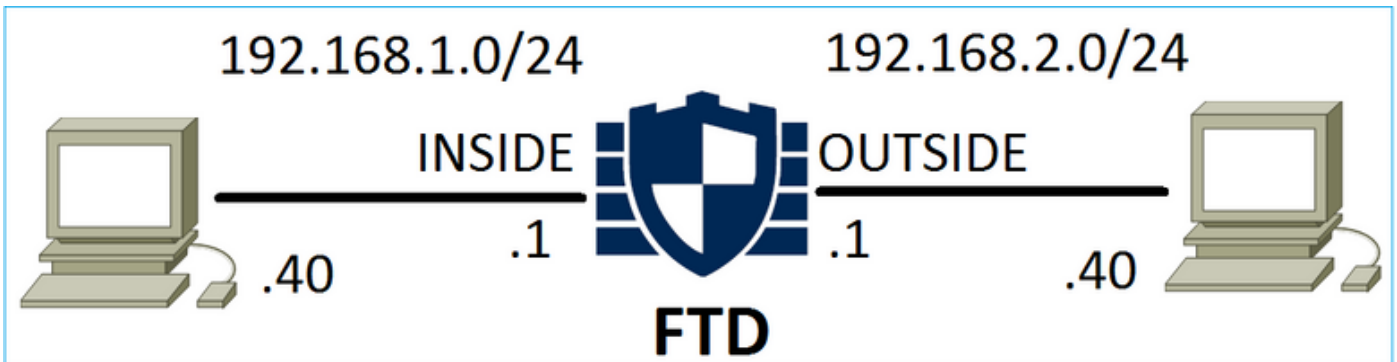
```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xald3780e
```



Opmerking: Voorfilter vs. ACP-regels = de eerste match wordt toegepast.

## Block-actie van ACP

Overweeg de topologie die in dit beeld wordt getoond:



## Scenario 1: Vroege afwijzing in LINA

Het ACP bevat een Block-regel die een L4-voorwaarde (bestemmingspoort TCP 80) gebruikt, zoals is weergegeven in de afbeelding:

Access Control													
ACP1													
Enter Description													
Prefilter Policy: Default Prefilter Policy													
SSL Policy: None													
Identity Policy: None													
Inheritance Set													
Rules													
Filter by Device													
Show Rule Conflicts													
Add Category													
Add Rule													
Search Rule													
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	Block

Het geïmplementeerde beleid in Snort:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

Het geïmplementeerde beleid in LINA. Merk op dat de regel als volgt wordt gedrukt deny actie:

```
firepower# show access-list
```

...

```
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 event-log flow-start (hitcnt=0) 0x6149c43c
```

## Gedrag controleren:

Wanneer host-A (192.168.1.40) probeert om een HTTP-sessie te openen voor host-B (192.168.2.40), synchroniseren TCP-pakketten (SYN) door de FTD LINA-engine en bereiken ze de Snort Engine of de bestemming:

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
430 bytes]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
0 bytes]
  match ip host 192.168.1.40 any
```

```
firepower# show capture CAPI
1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
2: 11:08:12.672435 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4063517 0>
3: 11:08:18.672847 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4069517 0>
4: 11:08:30.673610 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4081517 0>
```

```
firepower# show capture CAPI packet-number 1 trace
1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
...
```

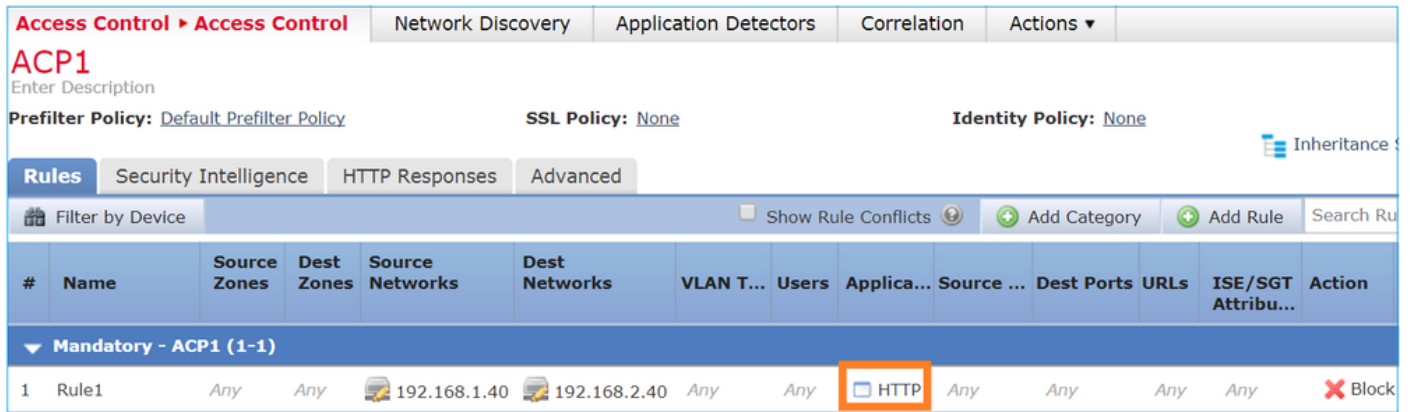
```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id
268435461 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L4 RULE: Rule1
Additional Information:
```

**<- No Additional Information = No Snort Inspection**

```
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

## Scenario 2: Afwijzing door Snort-oordeel

Het ACP bevat een Block-regel die een L7-voorwaarde (HTTP-toepassing) gebruikt, zoals is weergegeven in de afbeelding:



#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	HTTP	Any	Any	Any	Any	Block

Het geïmplementeerde beleid in Snort:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any (appid 676:1)
```

Appid 676:1 = HTTP

Het geïmplementeerde beleid in LINA.

**Opmerking:** De regel wordt als een **permit** actie omdat LINA niet kan bepalen dat de sessie HTTP gebruikt. Op de FTD bevindt het toepassingsdetectiemechanisme zich in de Snortengine.

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 (hitcnt=0) 0xb788b786
```

Voor een blokregel die gebruik maakt van **Application** als voorwaarde, toont het spoor van een echt pakket aan dat de zitting door LINA wegens het vonnis van de Snortmotor wordt gelaten vallen.

**Opmerking:** Om ervoor te zorgen dat de Snort-engine de toepassing kan bepalen, moeten er een aantal pakketten worden geïnspecteerd (meestal 3-10, afhankelijk van de toepassingsdecoder). Op deze manier worden enkele pakketten toegelaten door de FTD en deze bereiken de bestemming. De toegestane pakketten zijn nog steeds onderworpen aan de controle van het inbraakbeleid op basis van de **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** optie.

**Gedrag controleren:**

Wanneer host-A (192.168.1.40) probeert een HTTP-sessie op te zetten met host-B (192.168.2.40), dan toont de inkomende LINA-vastlegging:

```
firepower# show capture CAPI
```

## 8 packets captured

```
1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
2: 11:31:19.826403 192.168.2.40.80 > 192.168.1.40.32790: S 1283931030:1283931030(0) ack
357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579>
3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>
4: 11:31:20.026899 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450781 5449236>
5: 11:31:20.428887 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5451183 5449236>
...
```

## De uitgaande vastlegging:

```
firepower# show capture CAPO
```

## 5 packets captured

```
1: 11:31:19.825869 192.168.1.40.32790 > 192.168.2.40.80: S 1163713179:1163713179(0) win 2920
<mss 1380,sackOK,timestamp 5450579 0>
2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
3: 11:31:23.426049 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5452836 5450579>
4: 11:31:29.426430 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5458836 5450579>
5: 11:31:41.427208 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5470836 5450579>
```

Het spoor toont aan dat het eerste pakket (TCP SYN) door de Snort wordt toegestaan aangezien de uitspraak van de Opsporing van de Toepassing nog niet is bereikt:

```
firepower# show capture CAPI packet-number 1 trace
```

```
1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
...
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM\_FW\_ACL\_ global

access-list CSM\_FW\_ACL\_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461

access-list CSM\_FW\_ACL\_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory

access-list CSM\_FW\_ACL\_ remark rule-id 268435461: L7 RULE: Rule1

### Additional Information:

**This packet will be sent to snort for additional processing where a verdict will be reached**

...

Phase: 10

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

**New flow created with id 23194**, packet dispatched to next module

...



Phase: 12  
Type: SNORT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Snort Trace:  
Packet: TCP, SYN, seq 357753151  
AppID: service unknown (0), application unknown (0)  
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,  
icmpType 0, icmpCode 0  
Firewall: **pending rule-matching, id 268435461, pending AppID**  
NAP id 1, IPS id 0, **Verdict PASS**  
**Snort Verdict: (pass-packet) allow this packet**

Result:  
input-interface: OUTSIDE  
input-status: up  
input-line-status: up  
output-interface: OUTSIDE  
output-status: up  
output-line-status: up  
**Action: allow**

Hetzelfde geldt voor het TCP SYN/ACK-pakket:

```
firepower# show capture CAPO packet-number 2 trace
  2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
```

...

Phase: 3  
Type: FLOW-LOOKUP  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
**Found flow with id 23194, using existing flow**

...

Phase: 5  
Type: SNORT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Snort Trace:  
Packet: TCP, SYN, ACK, seq 1283931030, ack 357753152  
AppID: service unknown (0), application unknown (0)  
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,  
icmpType 0, icmpCode 0  
Firewall: **pending rule-matching, id 268435461, pending AppID**  
NAP id 1, IPS id 0, **Verdict PASS**  
**Snort Verdict: (pass-packet) allow this packet**

Result:  
input-interface: INSIDE  
input-status: up  
input-line-status: up  
output-interface: INSIDE  
output-status: up  
output-line-status: up

Action: allow

Snort geeft een DROP-uitspraak terug als een inspectie van het derde pakket voltooid is:

```
firepower# show capture CAPI packet-number 3 trace
  3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow

Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 357753152, ack 1283931031
AppID: service HTTP (676), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 65535, user 9999997,
url http://192.168.2.40/128k.html
Firewall: block rule, id 268435461, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

U kunt de opdracht ook uitvoeren `system support trace` uit de FTD CLISH-modus. Deze tool heeft twee functies:

- Toont de korte uitspraak voor elk pakket zoals het wordt verzonden naar de bibliotheek van de Verwerving van Gegevens (DAQ) en in LINA gezien. DAQ is een component die zich tussen de FTD LINA-engine en de Snort-engine bevindt
- hiermee kan `system support firewall-engine-debug` tegelijkertijd om te zien wat er gebeurt binnen de Snort-motor zelf

Dit is de output:

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
```

## Monitoring packet tracer debug messages

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, seq 2620409313
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 New session
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', 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
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS
```

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, ACK, seq 3700371680, ack 2620409314
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', 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
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS
```

Tracing enabled by Lina

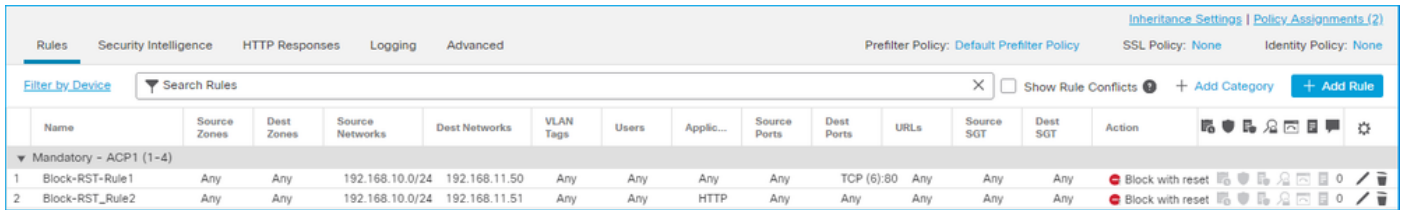
```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, ACK, seq 2620409314, ack 3700371681
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc
676, payload 0, client 686, misc 0, user 9999997, url http://192.168.2.40/128k.html, xff
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0)
-> 0, vlan 0, sgt 65535, user 9999997, url http://192.168.2.40/128k.html
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 match rule order 2, 'Rule1', action Block
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: block rule, 'Rule1', drop
192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict BLOCKLIST
192.168.1.40-32791 > 192.168.2.40-80 6 ==> Blocked by Firewall
```

## Samenvatting

- De Block-actie van het ACP wordt geïmplementeerd als permit- of deny-regel in LINA en is afhankelijk van de regelvoorwaarden
- Als de voorwaarden L3/L4 zijn dan blokkeert de LINA het pakket. In het geval van TCP wordt het eerste pakket (TCP/SYN) geblokkeerd
- Als de voorwaarden L7 zijn, wordt het pakket doorgestuurd naar de Snort-engine voor verdere inspectie. In het geval van TCP, worden enkele pakketten toegelaten door de FTD totdat Snort een oordeel heeft. De toegestane pakketten zijn nog steeds onderworpen aan de controle van het inbraakbeleid op basis van de **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** optie.

## Block with reset-actie van ACP

## Een Block with reset-regel geconfigureerd in de FMC UI:



Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
▼ Mandatory - ACP1 (1-4)													
1 Block-RST_Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Block with reset
2 Block-RST_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Block with reset

Het blok met reset regel wordt ingezet op FTD LINA engine als een **permit** en op Snortmotor als een **reset** Regel:

```
firepower# show access-list
```

```
...
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=0) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Block-RST_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Snort-engine:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438864 reset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 reset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Wanneer een pakket overeenkomt met Block met reset rule stuurt FTD een **TCP Reset** pakket of een **ICMP Type 3 Code 13** Bericht bestemming onbereikbaar (administratief gefilterd):

```
root@kali:~/tests# wget 192.168.11.50/file1.zip
--2020-06-20 22:48:10-- http://192.168.11.50/file1.zip
Connecting to 192.168.11.50:80... failed: Connection refused.
```

Hier ziet u een vastlegging van de inkomende FTD-interface:

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 P0 192.168.10.50.41986 > 192.168.11.50.80: S
3120295488:3120295488(0) win 29200 <mss 1460,sackOK,timestamp 3740873275 0,nop,wscale 7>
2: 21:01:00.978114 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack
3120295489 win 0 2 packets shown
```

**System support trace** de output, in dit geval, toont aan dat het pakket wegens het korte vonnis wordt gelaten vallen:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
```

Please specify an IP protocol: tcp  
Please specify a client IP address: 192.168.10.50  
Please specify a client port:  
Please specify a server IP address: 192.168.11.50  
Please specify a server port:  
Monitoring packet tracer and firewall debug messages

```
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3387496622
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 new firewall session
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 using HW or preset rule order 2, 'Block-RST-
Rule1', action Reset and prefilter rule 0
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 HitCount data sent for rule id: 268438864,
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 reset action
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0,
fwFlags = 0x0
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: block w/ reset rule, 'Block-RST-
Rule1', drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 9, NAP id 1, IPS id 0, Verdict
BLOCKLIST
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

## Use cases

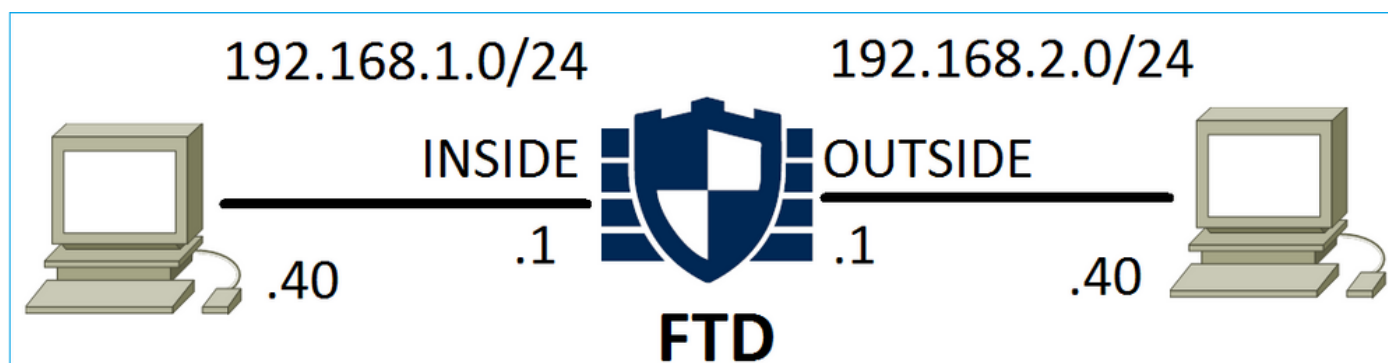
Hetzelfde als **Block** actie, maar beëindigt onmiddellijk de verbinding.

## Allow-actie van ACP

### Scenario 1: Allow-actie van ACP (L3/L4-voorwaarden)

Normaliter zou u een Allow-regel configureren om extra inspecties op te geven, zoals een Intrusion Policy (inbraakbeleid) en/of een File Policy (bestandsbeleid). Dit eerste scenario toont de werking van een Allow regel aan wanneer een L3/L4 voorwaarde wordt toegepast.

Bekijk de topologie die in de afbeelding is weergegeven:



Dit beleid wordt toegepast zoals in de afbeelding is weergegeven:

Access Control > Access Control												
Network Discovery			Application Detectors			Correlation			Actions			
<b>ACP1</b>												
Enter Description												
Prefilter Policy: <a href="#">Default Prefilter Policy</a>				SSL Policy: <a href="#">None</a>				Identity Policy: <a href="#">None</a>				
<a href="#">Inheritance Settings</a>												
<b>Rules</b>   Security Intelligence   HTTP Responses   Advanced												
Filter by Device <input type="checkbox"/> Show Rule Conflicts <input type="checkbox"/> Add Category <input type="button" value="+"/> Add Rule <input type="text" value="Search Rules"/>												
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Action Attribu...
▼ Mandatory - ACP1 (1-1)												
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Allow

Het geïmplementeerde beleid in Snort. Merk op dat de regel als een **allow** actie:

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

Het beleid in LINA.

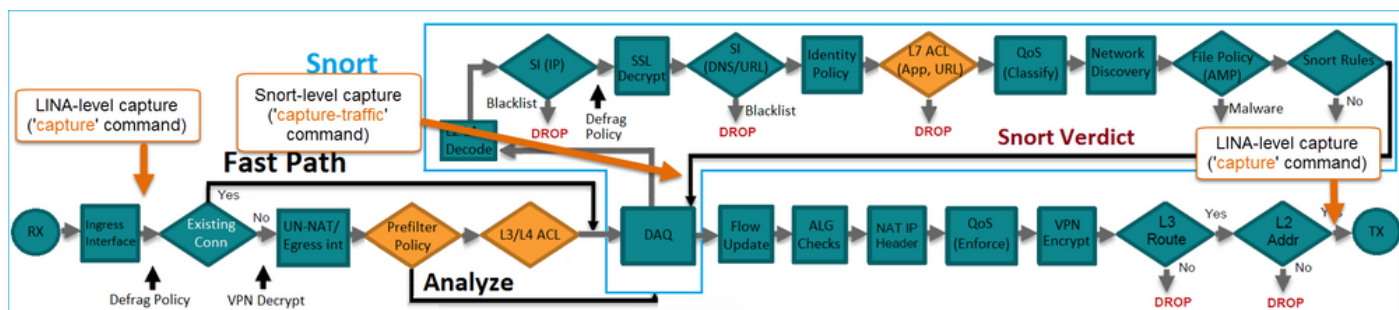
**Opmerking:** De regel wordt als een **permit** maatregelen die in wezen neerkomen op een omleiding naar Snort voor verdere inspectie.

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 (hitcnt=1) 0x641a20c3
```

Om te zien hoe FTD een stroom verwerkt die aanpast en regel toestaat zijn er een paar manieren:

- Snort-statistieken verifiëren
- Met behulp van de systeemtracering van de CLISH-tool
- Met behulp van vastlegging met de traceeroptie in LINA en optioneel met verkeer vastleggen in de Snort-engine

LINA-vastlegging vs. verkeer vastleggen in Snort:



Gedrag controleren:

Schakel de snelstatistieken in **system support trace** from CLISH, and initiate an HTTP flow from host-A (192.168.1.40) to host-B (192.168.2.40). All the packets are forwarded to the Snort engine and get the PASS verdict by the Snort:

```
firepower# clear snort statistics
```

```
> system support trace
```

Please specify an IP protocol:

Please specify a client IP address: **192.168.1.40**

Please specify a client port:

Please specify a server IP address: **192.168.2.40**

Please specify a server port:

Enable firewall-engine-debug too? [n]:

Monitoring packet tracer debug messages

Tracing enabled by Lina

192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, seq 361134402

192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)

192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow

192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, **Verdict PASS**

Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina

192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, ACK, seq 1591434735, ack 361134403

192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)

192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow

192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, **Verdict PASS**

Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina

192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, ACK, seq 361134403, ack 1591434736

192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service HTTP (676), application unknown (0)

192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow

192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, **Verdict PASS**

De tellers voor passerpakketten stijgen:

```
> show snort statistics
```

Packet Counters:

<b>Passed Packets</b>	<b>54</b>
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

Flow Counters:

Fast-Forwarded Flows	0
Blocklisted Flows	0

...

Doorgegeven pakketten = geïnspecteerd door de Snort-engine

## Scenario 2: Allow-actie van ACP (L3-7-voorwaarden)

Vergelijkbaar gedrag treedt op wanneer de Allow-regel als volgt wordt geïmplementeerd.

Alleen een L3/L4-toestand zoals in het beeld:

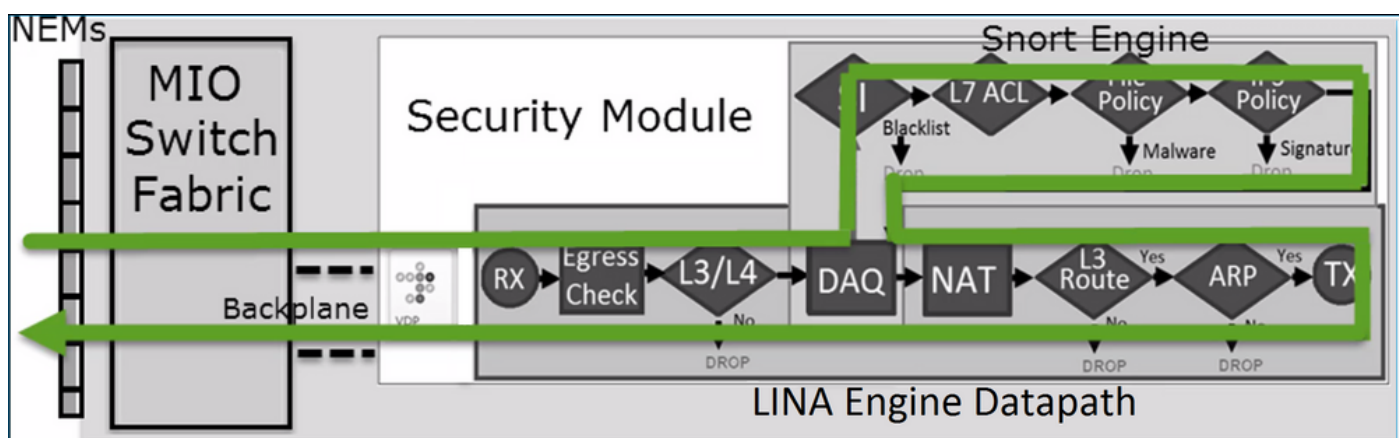
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

Een L7 voorwaarde (bijvoorbeeld Inbraakbeleid, Bestandsbeleid, Toepassing, etc.) wordt in de afbeelding weergegeven:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

## Samenvatting

Samenvattend is dit hoe een flow wordt verwerkt door een FTD die is geïmplementeerd op een FP4100/9300 wanneer er een Allow-regel is, zoals is weergegeven in de afbeelding:



**Opmerking:** Management Input Output (MIO) is de supervisor-engine van het Firepower-chassis.

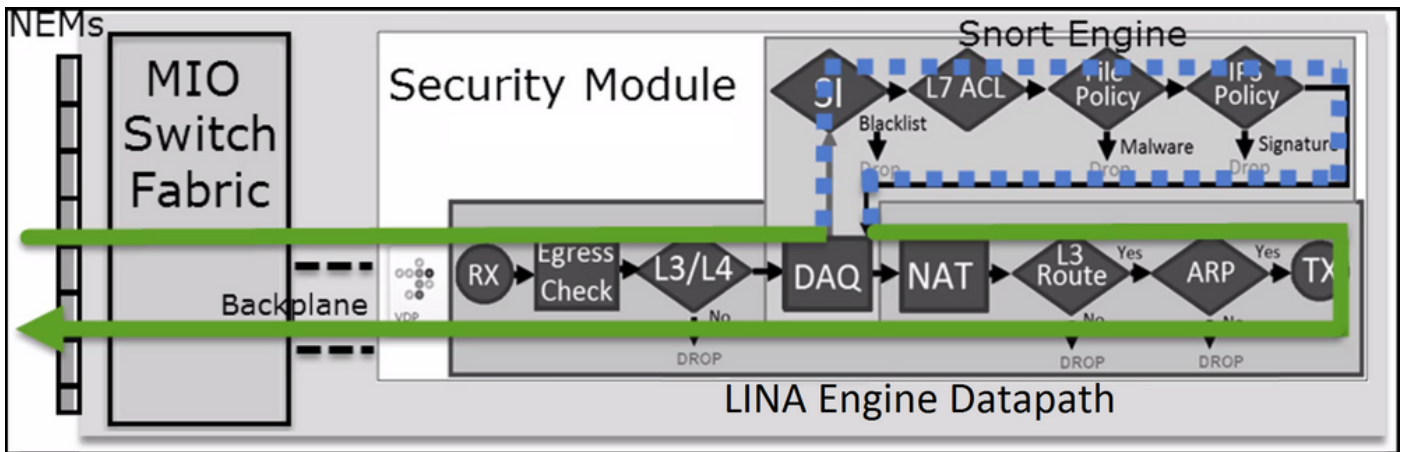
## Scenario 3: Snort fast-forward-ordeel met Allow

Er zijn specifieke scenario's waarbij de FTD Snort-motor een PERMITLIST-uitspraak geeft (vooruitspoelen) en de rest van de stroom wordt overgeladen naar de LINA-motor (in sommige gevallen wordt dan overgeladen naar de HW Accelerator - SmartNIC). Deze zijn:

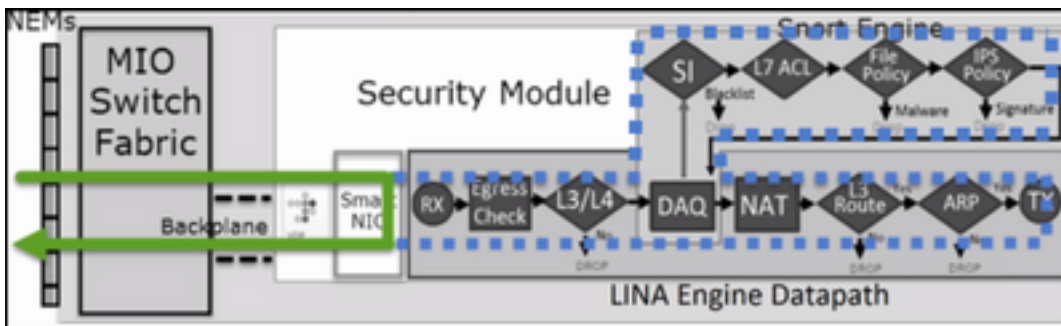
1. SSL-verkeer zonder een geconfigureerd SSL-beleid
2. Intelligent Application Bypass (IAB)

Dit is de visuele weergave van het pakketpad:





Of in sommige gevallen:



## Hoofdpunten

- De regel Toestaan wordt ingesteld als **allow** in de vorm van snurken en **permit** In LINA
- In de meeste gevallen worden alle pakketten van een sessie doorgestuurd naar de Snort-engine voor extra inspectie

## Use cases

Configureer een Allow-regel wanneer de Snort-engine een L7-inspectie moet uitvoeren, zoals:

- Intrusion Policy (inbraakbeleid)
- File Policy (bestandsbeleid)

## Trust-actie van ACP

### Scenario 1: Trust-actie van ACP

Als u geen geavanceerde L7-inspectie op snorniveau wilt toepassen (bijvoorbeeld inbraakbeleid, bestandsbeleid, netwerkdetectie), maar u nog steeds functies wilt gebruiken zoals Security Intelligence (SI), Identity Policy, QoS, enz., dan is het aan te raden om de Trust-actie in uw regel te gebruiken.

Topologie:



Het geconfigureerde beleid:

ACP1															Analyze Hit Counts	Save	Cancel	
Enter Description															Inheritance Settings   Policy Assignments (1)			
Rules	Security Intelligence	HTTP Responses	Logging	Advanced	Prefilter Policy: Prefilter1					SSL Policy: None		Identity Policy: None						
Filter by Device															Search Rules	Show Rule Conflicts	Add Category	Add Rule
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action	Icons				
Mandatory - ACP1 (1-4)																		
1	trust_L3-L4	Any	Any	192.168.10.50 192.168.10.51	192.168.11.50 192.168.11.51	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Trust				

De Trust-regel zoals deze in de FTD Snort-engine is geïmplementeerd:

```
# Start of AC rule.
268438858 fastpath any 192.168.10.50 31 any any 192.168.11.50 31 80 any 6 (log dcforward
flowend)
```

**Opmerking:** Het cijfer 6 is het protocol (TCP).

De regel in FTD LINA:

```
firepower# show access-list | i 268438858
access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 18 remark rule-id 268438858: L7 RULE: trust_L3-L4
access-list CSM_FW_ACL_ line 19 advanced permit tcp object-group FMC_INLINE_src_rule_268438858
object-group FMC_INLINE_dst_rule_268438858 eq www rule-id 268438858 (hitcnt=19) 0x29588b4f
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=19) 0x9d442895
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0xd026252b
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=0) 0x0d785cc4
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

**Verificatie:**

Inschakelen `system support trace` en start een HTTP-sessie van host-A (192.168.10.50) naar host-B (192.168.11.50). Er zijn drie pakketten doorgestuurd naar de Snort-engine. Snort-motor stuurt naar LINA het oordeel PERMITLIST dat in wezen de rest van de stroom naar de LINA-motor

ontlaadt:

> **system support trace**

Enable firewall-engine-debug too? [n]: **y**

Please specify an IP protocol: **tcp**

**Please** specify a client IP address: **192.168.10.50**

Please specify a client port:

Please specify a server IP address: **192.168.11.50**

Please specify a server port: **80**

Monitoring packet tracer and firewall debug messages

```
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 453426648
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 new firewall session
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 using HW or preset rule order 5, 'trust_L3-
L4', action Trust and prefilter rule 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 HitCount data sent for rule id: 268438858,
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2820426532, ack
453426649
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 453426649, ack
2820426533
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PERMITLIST
```

Zodra de verbinding is beëindigd, krijgt de Snort-engine de metagegevens van de LINA-engine en wordt de sessie verwijderd:

```
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 3
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Logging EOF for event from hardware with
rule_id = 268438858 ruleAction = 3 ruleReason = 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 : Received EOF, deleting the snort session.

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleting snort session, reason:
timeout
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 deleting firewall session flags = 0x10003,
fwFlags = 0x1115
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0
bytes; protocol id:(-1) : LWstate 0xf LWFlags 0x6007
```

Snelopname toont de 3 pakketten die naar de Snortmotor gaan:

```
> capture-traffic
```

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

- 0 - management0
- 1 - management1
- 2 - Global

```
Selection? 2
```

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

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

```
Options: -n vlan and (host 192.168.10.50 and host 192.168.11.50)
```

```
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [S], seq 3065553465, win 29200, options [mss 1380,sackOK,TS val 3789188468 ecr 0,nop,wscale 7], length 0
```

```
10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack 3065553466, win 8192, options [mss 1380,nop,wscale 8,sackOK,TS val 57650410 ecr 3789188468], length 0
```

```
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options [nop,nop,TS val 3789188470 ecr 57650410], length 0
```

LINA-vastlegging toont de flow die hierdoor gaat:

```
firepower# show capture CAPI
```

```
437 packets captured
```

```
1: 09:51:19.431007 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: S
2459891187:2459891187(0) win 29200 <mss 1460,sackOK,timestamp 3787091387 0,nop,wscale 7>
2: 09:51:19.431648 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S
2860907367:2860907367(0) ack 2459891188 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
57440579 3787091387>
3: 09:51:19.431847 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack
2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
4: 09:51:19.431953 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P
2459891188:2459891337(149) ack 2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
5: 09:51:19.444816 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860907368:2860908736(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
6: 09:51:19.444831 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860908736:2860910104(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
```

```
...
```

Tracering van de pakketten van LINA is een andere manier om de Snort-oordelen te zien. Het eerste pakket heeft het oordeel PASS gekregen:

```
firepower# show capture CAPI packet-number 1 trace | i Type|Verdict
```

```
Type: CAPTURE
```

```
Type: ACCESS-LIST
```

```
Type: ROUTE-LOOKUP
```

```
Type: ACCESS-LIST
```

```
Type: CONN-SETTINGS
```

```
Type: NAT
```

```
Type: NAT
```

```
Type: IP-OPTIONS
```

```
Type: CAPTURE
```

```
Type: CAPTURE
```

```
Type: NAT
```

```
Type: CAPTURE
```

Type: NAT  
Type: IP-OPTIONS  
Type: CAPTURE  
Type: FLOW-CREATION  
Type: EXTERNAL-INSPECT

**Type: SNORT**

**Snort id 22, NAP id 2, IPS id 0, Verdict PASS**

**Snort Verdict: (pass-packet) allow this packet**

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP

Type: ADJACENCY-LOOKUP

Type: CAPTURE

Sporen van het TCP SYN/ACK-pakket op de buiteninterface:

```
firepower# show capture CAPO packet-number 2 trace | i Type|Verdict
```

Type: CAPTURE

Type: ACCESS-LIST

Type: FLOW-LOOKUP

Type: EXTERNAL-INSPECT

Type: SNORT

**Snort id 22, NAP id 2, IPS id 0, Verdict PASS**

**Snort Verdict: (pass-packet) allow this packet**

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP

Type: ADJACENCY-LOOKUP

Type: CAPTURE

TCP ACK krijgt de PERMITLIST uitspraak:

```
firepower# show capture CAPI packet-number 3 trace | i Type|Verdict
```

Type: CAPTURE

Type: ACCESS-LIST

Type: FLOW-LOOKUP

Type: EXTERNAL-INSPECT

Type: SNORT

**Snort id 22, NAP id 2, IPS id 0, Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow

Type: CAPTURE

Dit is de volledige output van het Snort-oordeel (pakket nr. 3)

```
firepower# show capture CAPI packet-number 3 trace | b Type: SNORT
```

**Type: SNORT**

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Trace:

Packet: TCP, ACK, seq 687485179, ack 1029625865

AppID: service unknown (0), application unknown (0)

Firewall: trust/fastpath rule, id 268438858, allow

Snort id 31, NAP id 2, IPS id 0, **Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow

Het 4de pakket wordt niet doorgestuurd naar de Snort engine, omdat het oordeel wordt gecached door de LINA engine:

firepower# **show capture CAPI packet-number 4 trace**

441 packets captured

4: 10:34:02.741523 802.1Q vlan#202 PO 192.168.10.50.42158 > 192.168.11.50.80: P  
164375589:164375738(149) ack 3008397532 win 229 <nop,nop,timestamp 3789654678 57697031>

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 1254, using existing flow**

**Phase: 4**

**Type: SNORT**

**Subtype:**

**Result: ALLOW**

**Config:**

**Additional Information:**

**Snort Verdict: (fast-forward) fast forward this flow**

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

Action: allow

1 packet shown

Snort-statistieken bevestigen dit:

firepower# **show snort statistics**

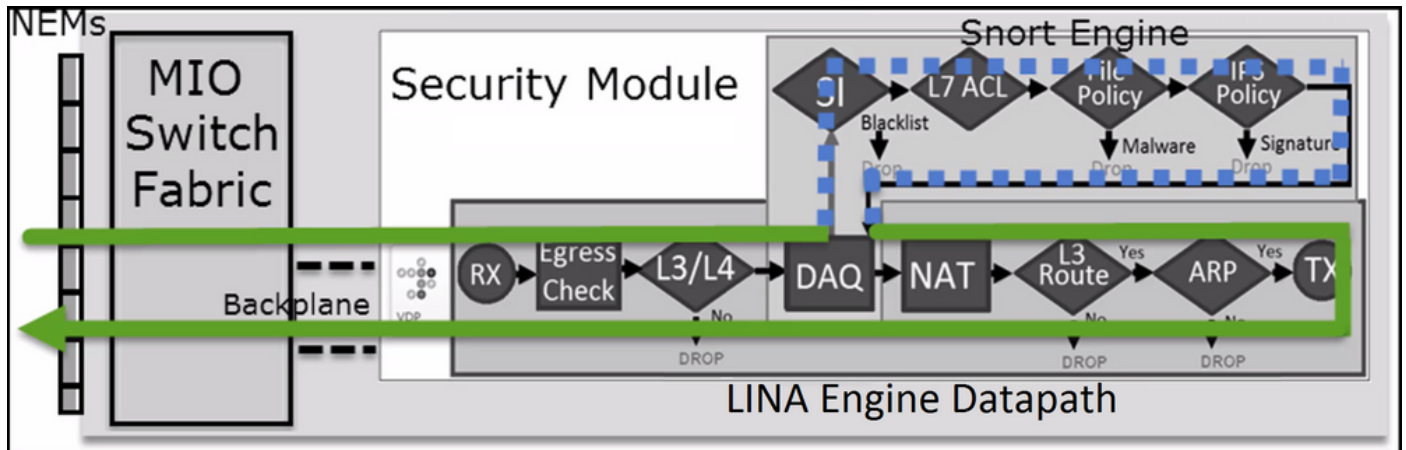
Packet Counters:

<b>Passed Packets</b>	<b>2</b>
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

Flow Counters:

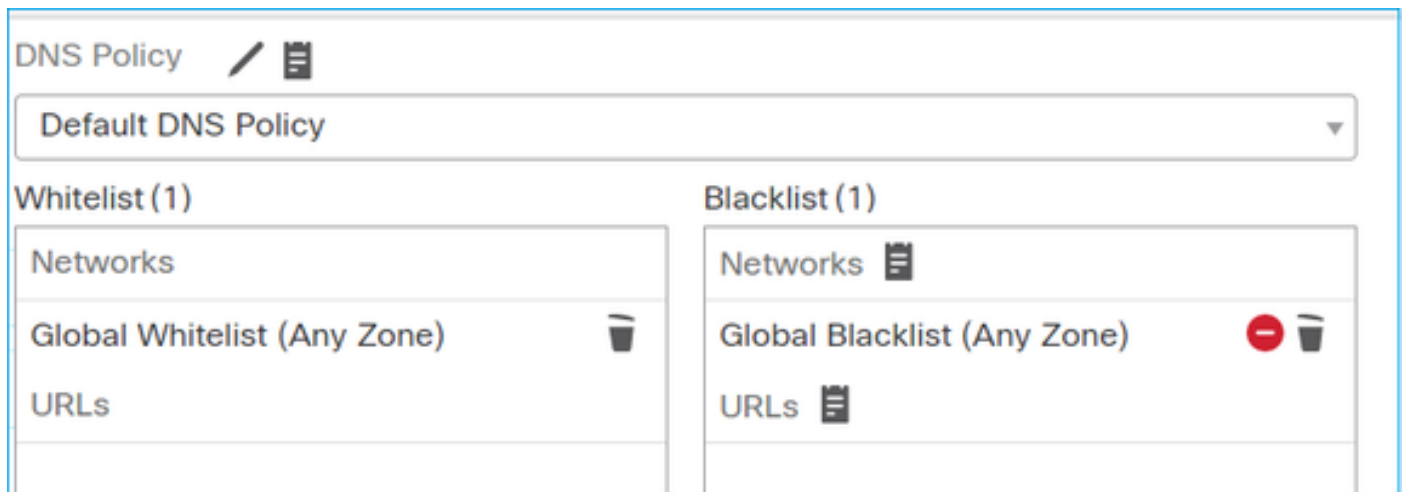
<b>Fast-Forwarded Flows</b>	<b>1</b>
Blacklisted Flows	0
Miscellaneous Counters:	
Start-of-Flow events	0
End-of-Flow events	1
Denied flow events	0
Frames forwarded to Snort before drop	0
Inject packets dropped	0

Pakketstroom met Trust-regel. Enkele pakketten worden door Snort geïnspecteerd en de rest wordt door LINA geïnspecteerd:



## Scenario 2. ACS-vertrouwensactie (zonder SI, QoS en identiteitsbeleid)

Indien u wilt dat de FTD veiligheidsintelligentie (SI)-controles toepast op alle stromen, is SI al ingeschakeld op ACS-niveau en kunt u de SI-bronnen (TALOS, feeds, lijsten, enz.) specificeren. Wanneer u dit echter wilt uitschakelen, schakel SI voor netwerken dan globaal uit via ACP, SI voor URL en SI voor DNS. De SI voor netwerken en URL is uitgeschakeld, zoals in de afbeelding is weergegeven:



In dit geval wordt de Trust-regel voor LINA geïmplementeerd als trust:

```
> show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
```

**Opmerking:** Vanaf 6.2.2 ondersteunt FTD TID. TID werkt op een vergelijkbare manier als SI, maar als SI is uitgeschakeld worden pakketten niet 'gedwongen' omgeleid naar de Snort-engine voor TID-inspectie.

## Controleer het gedrag

Start een HTTP-sessie vanaf host-A (192.168.1.40) naar host-B (192.168.2.40). Aangezien dit een FP4100 is en Flow Offload in hardware ondersteunt, gebeuren deze dingen:

- Een paar pakketten worden doorgestuurd via de FTD LINA-engine en de rest van de flow wordt overgedragen naar SmartNIC (HW-accelerator)
- Geen pakketten worden doorgestuurd naar de Snort engine

De FTD LINA-verbindingstabel toont de vlag "o", dat wil zeggen dat de stroom naar HW is overgeslagen. Let ook op het ontbreken van de vlag. Dit betekent feitelijk 'geen Snort-omleiding':

```
firepower# show conn
1 in use, 15 most used
```

```
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:32809, idle 0:00:00, bytes 949584, flags UIOo
```

Snort-statistieken tonen alleen logboekregistraties aan het begin en einde van de sessie:

```
firepower# show snort statistics
```

### Packet Counters:

Passed Packets	0
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

### Flow Counters:

Fast-Forwarded Flows	0
Blacklisted Flows	0

### Miscellaneous Counters:

<b>Start-of-Flow events</b>	<b>1</b>
<b>End-of-Flow events</b>	<b>1</b>

FTD LINA-logbestanden laten zien dat er voor elke sessie twee flows (één per richting) zijn overgedragen naar HW:

```
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384 for
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
```

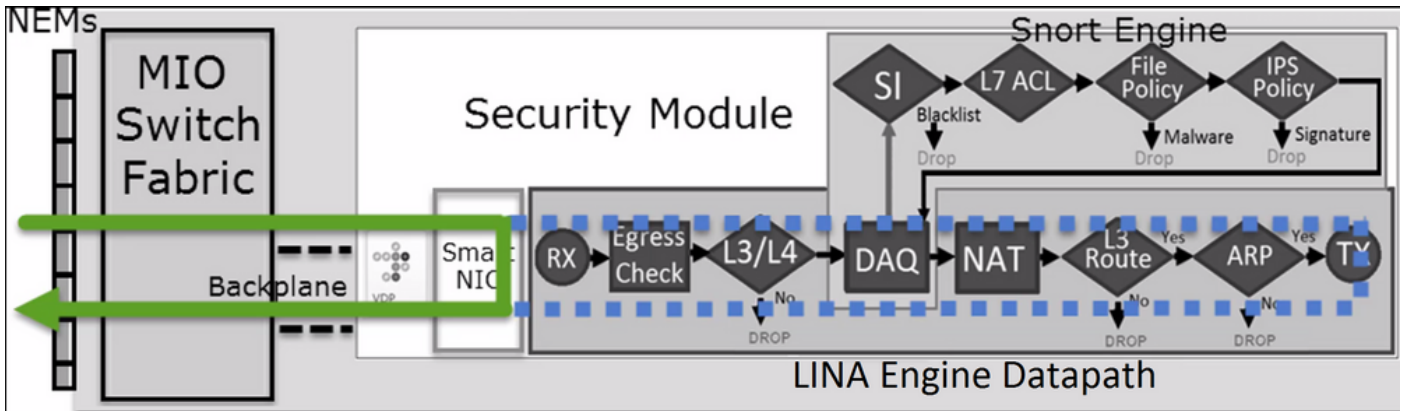


```

Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809
to OUTSIDE:192.168.2.40/80 duration 0:00:00 bytes 1055048 TCP FINs
Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00

```

Packet flow met vertrouwensregel geïmplementeerd als **trust** actie in LINA. Enkele pakketten worden geïnspecteerd door LINA en de rest wordt overgedragen naar SmartNIC (FP4100/FP9300):

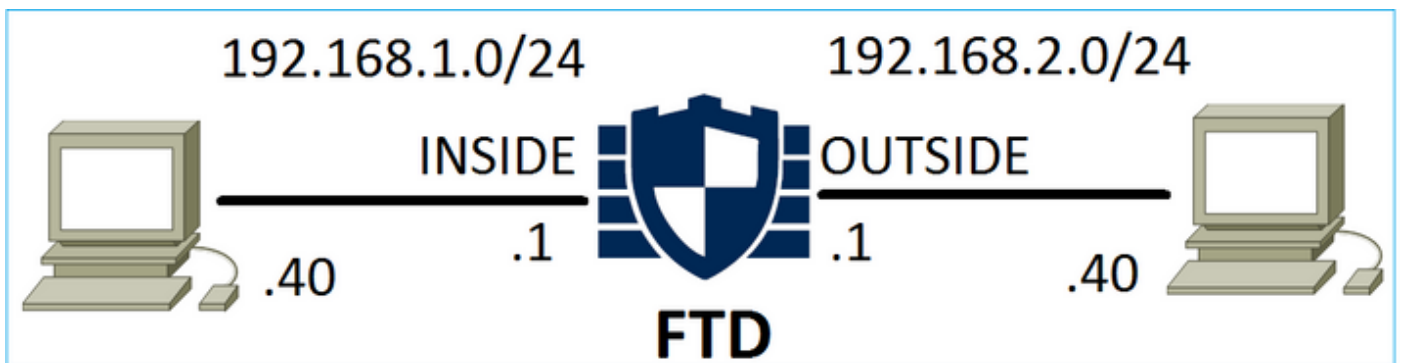


### Use cases

- U moet Trust actie wanneer u wilt dat slechts een paar pakketten worden gecontroleerd door de Snort-motor (bijvoorbeeld Application Detection, SI check) en de rest van de stroom worden geoffload naar de LINA-motor
- Als u FTD gebruikt op FP4100/9300 en wilt dat de stroom de inspectie van de snort volledig omzeilt, overweeg dan de Prefilterregel met Fastpath actie (zie de desbetreffende paragraaf in dit document)

### Block-actie van voorfilterbeleid

Bekijk de topologie in de afbeelding:



Bekijk ook het beleid zoals is weergegeven in de afbeelding:

Access Control ▶ Prefilter		Network Discovery	Application Detectors	Correlation	Actions ▼				
FTD_Prefilter									
Enter Description									
Rules									
<span>➕ Add Tunnel Rule</span> <span>➕ Add Prefilter Rule</span> <span>Search Rules</span>									
#	Name	Rule T...	...	De Source In Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter1	Prefilter	any any	192.168.1.40	192.168.2.40	any	any	any	✖ Block

Dit is het geïmplementeerde beleid in de FTD Snort engine (ngfw.rules bestand):

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268437506 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1
```

In LINA:

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id
268437506 event-log flow-start (hitcnt=0) 0x76476240
```

Wanneer u een virtueel pakket traceert, wordt aangegeven dat het pakket door LINA is afgewezen en nooit is doorgestuurd naar Snort:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ remark rule-id 268437506: RULE: Prefilter1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Snort-statistieken tonen:

```
firepower# show snort statistics
```

```

Packet Counters:
  Passed Packets                0
  Blocked Packets               0
  Injected Packets              0
  Packets bypassed (Snort Down) 0
  Packets bypassed (Snort Busy) 0

Flow Counters:
  Fast-Forwarded Flows         0
  Blacklisted Flows            0

Miscellaneous Counters:
  Start-of-Flow events         0
  End-of-Flow events           0
  Denied flow events         1

```

### LINA ASP-afwijzingen tonen:

```
firepower# show asp drop
```

```

Frame drop:
  Flow is denied by configured rule (acl-drop)          1

```

### Use cases

U kunt een Prefilter Block regel gebruiken als u verkeer wilt blokkeren op basis van L3/L4 voorwaarden en zonder dat u een Snort-inspectie van het verkeer hoeft te doen.

### Fastpath-actie van voorfilterbeleid

Bekijk de regel van het voorfilterbeleid in de volgende afbeelding:

#	Name	Rule T...	Sot Int	De Int	Source Networks	Destination Networks	Source Port	Destinati...	VLAN Tag	Action
1	Prefilter1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	TCP (6):80	any	→ Fastpath

Dit is het beleid in de FTD Snort engine:

```
268437506 fastpath any any any any any any any (log dcfoward flowend) (tunnel -1)
```

In FTD LINA:

```

access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced trust tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410b6f

```

## Gedrag controleren

Wanneer host-A (192.168.1.40) probeert een HTTP-sessie te openen naar host-B (192.168.2.40), dan doorlopen enkele pakketten LINA en wordt de rest overgedragen naar SmartNIC. In dit geval **system support trace** met **firewall-engine-debug** ingeschakeld toont:

```
> system support trace
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages
```

```
192.168.1.40-32840 > 192.168.2.40-80 6 AS 1 I 8 Got end of flow event from hardware with flags
04000000
```

LINA-logboeken bevatten de overgedragen flow:

```
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Oct 01 2017 14:36:51: %ASA-6-302013: Built inbound TCP connection 966 for
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32840 (192.168.1.40/32840)
```

LINA vangt tonen 8 pakketten gaan door:

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
```

```
firepower# show capture CAPI
```

```
8 packets captured
```

```
1: 14:45:32.700021 192.168.1.40.32842 > 192.168.2.40.80: S 3195173118:3195173118(0) win 2920
<mss 1460,sackOK,timestamp 332569060 0>
2: 14:45:32.700372 192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack
3195173119 win 2896 <mss 1380,sackOK,timestamp 332567732 332569060>
3: 14:45:32.700540 192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack
184794125 win 2920 <nop,nop,timestamp 332569060 332567732>
4: 14:45:32.700876 192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
5: 14:45:32.700922 192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack
```

```

3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
 6: 14:45:32.701425 192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569061>
 7: 14:45:32.701532 192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack
184810852 win 2736 <nop,nop,timestamp 332569061 332567733>
 8: 14:45:32.701639 192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697
<nop,nop,timestamp 332567734 332569061>

```

Flow-offload-statistieken van FTD geven aan dat er 22 pakketten zijn overgedragen aan HW:

```

firepower# show flow-offload statistics
Packet stats of port : 0
  Tx Packet count      :                22
  Rx Packet count      :                22
  Dropped Packet count :                0
  VNIC transmitted packet :                22
  VNIC transmitted bytes :              15308
  VNIC Dropped packets  :                0
  VNIC erroneous received :                0
  VNIC CRC errors       :                0
  VNIC transmit failed  :                0
  VNIC multicast received :                0

```

U kunt ook de **show flow-offload flow** bevel om extra informatie met betrekking tot de geoffload stromen te zien. Hierna volgt een voorbeeld:

```

firepower# show flow-offload flow
Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intf0 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets
33240, bytes 2326800
TCP intf0 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets
249140, bytes 358263320
firepower# show conn
5 in use, 5 most used
Inspect Snort:
  preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 0 most in effect

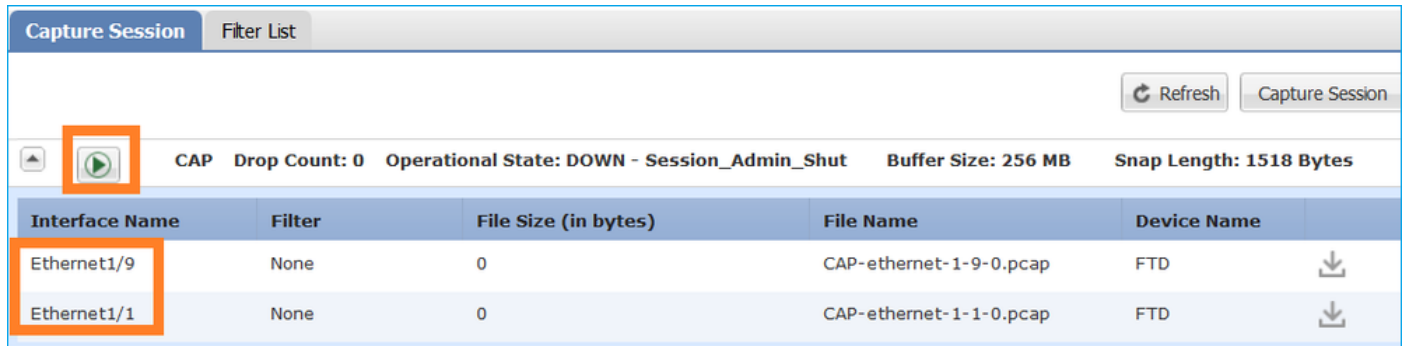
TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO
TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO
N1
TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags Uo
<- offloaded flow
TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags
UFRIO

```

- Het percentage is gebaseerd op de **show conn** uitvoer. Bijvoorbeeld, als 5 conns in totaal gaan door de FTD LINA motor en 1 van hen wordt geoffload dan wordt 20% gemeld als geoffload
- De maximumgrens van geoffload sessies hangt af van de softwareversie (bijvoorbeeld ASA 9.8.3 en FTD 6.2.3 ondersteunen 4 miljoen bidirectionele (of 8 miljoen unidirectionele) geoffload flows)
- Als het aantal offload-stromen de limiet bereikt (bijvoorbeeld 4 miljoen bi-directionele stromen), worden er geen nieuwe verbindingen geoffload totdat de huidige verbindingen uit de offload-tabel worden verwijderd

Om alle pakketten op FP4100/9300 te zien die FTD doorlopen (overgedragen + LINA), moet

vastlegging op chassisniveau worden ingeschakeld, zoals in de afbeelding is weergegeven:



The screenshot shows a network capture configuration window. At the top, there are tabs for 'Capture Session' and 'Filter List'. Below the tabs, there are buttons for 'Refresh' and 'Capture Session'. The main configuration area shows 'CAP' as the capture type, 'Drop Count: 0', 'Operational State: DOWN - Session\_Admin\_Shut', 'Buffer Size: 256 MB', and 'Snap Length: 1518 Bytes'. Below this is a table with columns for 'Interface Name', 'Filter', 'File Size (in bytes)', 'File Name', and 'Device Name'. Two interfaces are listed: 'Ethernet1/9' and 'Ethernet1/1', both with 'None' as the filter, '0' as the file size, and 'CAP-ethernet-1-9-0.pcap' and 'CAP-ethernet-1-1-0.pcap' as the file names, respectively. The device name for both is 'FTD'. There are download icons for each interface.

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/9	None	0	CAP-ethernet-1-9-0.pcap	FTD
Ethernet1/1	None	0	CAP-ethernet-1-1-0.pcap	FTD

De vastlegging van de backplane van het chassis toont beide richtingen. Door de architectuur van de FXOS-vastlegging (twee vastleggingspunten per richting) wordt elk pakket **twee** keer weergegeven zoals in de afbeelding is te zien:

Packet statistiek:

- Totaal aantal pakketten via FTD: 30
- Pakketten via FTD LINA: 8
- Pakketten overgedragen naar SmartNIC HW-accelerator: 22

In het geval van een ander platform dan FP4100/FP9300 worden alle pakketten door de LINA-motor verwerkt, aangezien flow-offload niet wordt ondersteund (let op het ontbreken van de markering **of** vlag):

```
FP2100-6# show conn addr 192.168.1.40
33 in use, 123 most used
Inspect Snort:
    preserve-connection: 0 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:50890, idle 0:00:09, bytes 175, flags UxIO
```

De LINA-syslogs tonen alleen de gebeurtenissen voor het instellen en verbreken van de verbinding:

```
FP2100-6# show log | i 192.168.2.40
Jun 21 2020 14:29:44: %FTD-6-302013: Built inbound TCP connection 6914 for
INSIDE:192.168.1.40/50900 (192.168.11.101/50900) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Jun 21 2020 14:30:30: %FTD-6-302014: Teardown TCP connection 6914 for INSIDE:192.168.1.40/50900
to OUTSIDE:192.168.2.40/80 duration 0:00:46 bytes 565 TCP FINs from OUTSIDE
```

## Use cases

- Gebruik **Prefilter Fastpath** actie wanneer u de inspectie van de snort volledig wilt omzeilen. Dit is over het algemeen wenselijk voor zeer grote flows die u vertrouwt, zoals back-ups en databaseoverdrachten
- Op FP4100/9300-apparaten **Fastpath** actie triggers flow-offload en slechts een paar pakketten gaan door de FTD LINA motor. De rest wordt verwerkt door SmartNIC, waardoor de latentie afneemt

## Fastpath-actie van voorfilterbeleid (inline-set)

Als een Prefilter Policy FastPath-actie wordt toegepast op verkeer dat door een inline-set (NGIPS-interfaces) gaat, moet met deze punten rekening worden gehouden:

- De regel wordt toegepast op de LINA-motor als een trust actie
- De flow wordt niet geïnspecteerd door de Snort-engine
- Flow-offload (hardwareversnelling) treedt niet op aangezien flow-offload niet van toepassing is op NGIPS-interfaces

Hier is een voorbeeld van een pakketspoor in het geval van Prefilter FastPath actie die op een inline-set wordt toegepast:

```
firepower# packet-tracer input inside tcp 192.168.1.40 12345 192.168.1.50 80 detailed
```

Phase: 1

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW

Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Forward Flow based lookup yields rule:

```
in id=0x2ad7ac48b330, priority=501, domain=ips-mode, deny=false
hits=2, user_data=0x2ad80d54abd0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any
```

Phase: 2

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced trust ip object 192.168.1.0 object 192.168.1.0 rule-id
268438531 event-log flow-end
```

```
access-list CSM_FW_ACL_ remark rule-id 268438531: PREFILTER POLICY: PF1
```

```
access-list CSM_FW_ACL_ remark rule-id 268438531: RULE: 1
```

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x2ad9f9f8a7f0, priority=12, domain=permit, trust
hits=1, user_data=0x2ad9b23c5d40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any
dst ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any
```

Phase: 3

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface inside is in NGIPS inline mode.

Egress interface outside is determined by inline-set configuration

Phase: 4

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 7, packet dispatched to next module

```

Module information for forward flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

```

```

Module information for reverse flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

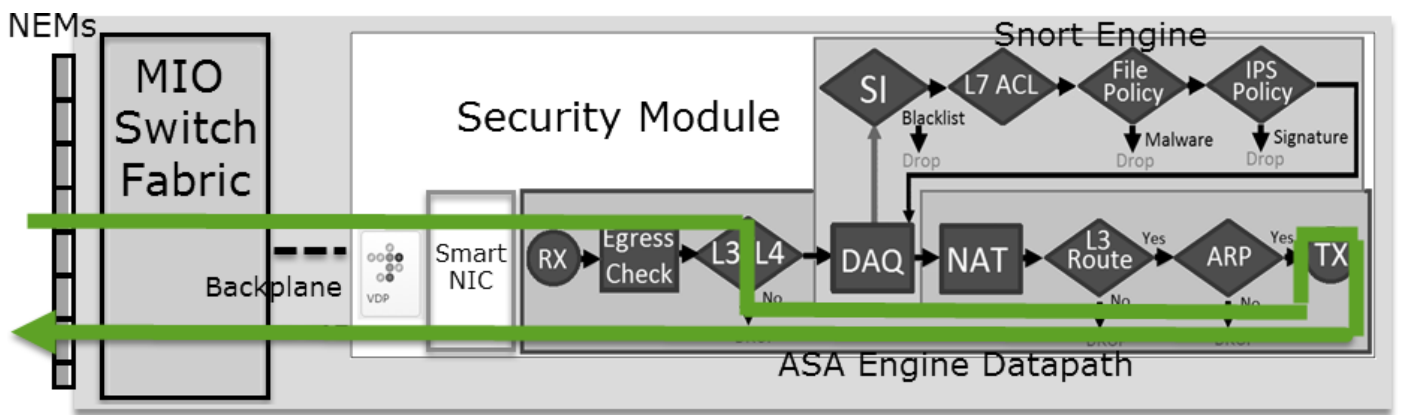
```

```

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow

```

Dit is de visuele weergave van het pakketpad:



### Fastpath-actie van voorfilterbeleid (inline-set met tap-modus)

Hetzelfde als bij een inline-set

### Analyze-actie van voorfilterbeleid

### Scenario 1: Voorfilter Analyze met Block-regel van ACP

Bekijk het voorfilterbeleid dat een Analyze-regel bevat, zoals in de afbeelding is weergegeven:

Access Control ► Prefilter										
		Network Discovery		Application Detectors		Correlation		Actions ▼		
Prefilter_Policy1										
Enter Description										
Rules										
<div style="text-align: right;"> <span>+</span> Add Tunnel Rule    <span>+</span> Add Prefilter Rule    Search R </div>										
#	Name	Rule T...	Source Interfac...	Destinat... Interfac...	Source Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter_Rule1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	any	any	Analyze

De ACS bevat alleen de standaardregel die is ingesteld op **Block All Traffic** zoals aangegeven op de afbeelding:



Access Control ▶ Access Control    Network Discovery    Application Detectors    Correlation    Actions ▼

**ACP1**  
Enter Description

Prefilter Policy: **Prefilter\_Policy1**    SSL Policy: None

Rules    Security Intelligence    HTTP Responses    Advanced

Show Rule Conflicts

#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Action
▼ Mandatory - ACP1 (-)													
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>													
▼ Default - ACP1 (-)													
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>													
Default Action												Access Control: Block All Traffic	

Dit is het geïmplementeerde beleid in de FTD Snort engine (ngfw.rules bestand):

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268435460 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1)
268435459 allow any any 1025-65535 any any 3544 any 17 (tunnel -1)
268435459 allow any any 3544 any any 1025-65535 any 17 (tunnel -1)
268435459 allow any any any any any any any any 47 (tunnel -1)
268435459 allow any any any any any any any any 41 (tunnel -1)
268435459 allow any any any any any any any any 4 (tunnel -1)
# End of tunnel and priority rules.
# Start of AC rule.
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

Dit is het geïmplementeerde beleid in de FTD LINA-engine:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=0) 0xb788b786
```

Gedrag controleren

Packet-tracer toont dat het pakket is toegestaan door LINA, wordt doorgestuurd naar Snort engine (vanwege permit actie) en Snort Engine geeft een Block vonnis omdat de standaardactie van AC wordt aangepast.

**Opmerking:** Snort evalueert geen verkeer op basis van tunnelregels

Wanneer u een pakket traceert, resulteert dit in hetzelfde:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
```

```

access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

```

```

...
Phase: 14
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: block rule, id 268435458, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

```

```

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor

```

## Scenario 2: Voorfilter Analyze met Allow-regel van ACP

Als het doel is het pakket toe te staan de FTD te passeren, dan moet er een regel worden toegevoegd in het ACP. De Actie kan zijn Toestaan of Vertrouwen dat afhankelijk is van het doel (bijvoorbeeld als u een L7-inspectie wilt toepassen moet u gebruiken Allow actie) zoals getoond in het beeld:

The screenshot shows the Fortinet ACP configuration page for 'ACP1'. The 'Rules' tab is selected, displaying a table of rules. Rule 1 is highlighted with an orange border, indicating it is the selected rule. The rule is named 'Rule1' and has an 'Allow' action. The 'Default Action' is set to 'Access Control: Block All Traffic'.

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow
Default - ACP1 (-)													
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>													
Default Action												Access Control: Block All Traffic	

Het geïmplementeerde beleid in de FTD Snort-engine:

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

## In de LINA-engine

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=1) 0xb788b786
```

## Gedrag controleren

Packet-tracer toont dat het pakket voldoet aan de regel 268435460 in LINA en 268435461 in snortmotor:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
  This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: allow rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
...
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

## Scenario 3: Voorfilter Analyze met Trust-regel van ACP

Als het ACP een Trust-regel bevat, dan is de situatie als volgt:

Access Control ▸ Access Control    Network Discovery    Application Detectors    Correlation    Actions ▾

## ACP1

Enter Description

Prefilter Policy: [Prefilter\\_Policy1](#)      SSL Policy: [None](#)      Identif...

Inheritance Se...

Rules    Security Intelligence    HTTP Responses    Advanced

Filter by Device    Show Rule Conflicts    Add Category    Add Rule    Search Rule

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
▼ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	→ Trust
▼ Default - ACP1 (-)													
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>													
Default Action											Access Control: Block All Traffic		

## Snort:

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

## LINA:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=2) 0xb788b786
```

Vergeet niet dat aangezien de SI standaard is ingeschakeld, de vertrouwensregel wordt toegepast als permit actie op LINA zodat ten minste een paar pakketten worden omgeleid naar de Snort-motor voor inspectie.

## Gedrag controleren

Packet-tracer toont aan dat de Snort engine Permitlist het pakket en offloads van de rest stroom naar LINA:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
  This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
```

Additional Information:

Snort Trace:

Packet: ICMP

AppID: service ICMP (3501), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 8, icmpCode 0

Firewall: **trust/fastpath rule, id 268435461, allow**

NAP id 1, IPS id 0, **Verdict PERMITLIST**

**Snort Verdict: (fast-forward) fast forward this flow**

...

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

**Action: allow**

## Scenario 4: Voorfilter Analyze met Trust-regel van ACP

In dit scenario is de SI handmatig uitgeschakeld.

De regel is als volgt in Snort geïmplementeerd:

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

In LINA is de regel als Trust geïmplementeerd. Een pakket hoewel past de vergunningsregel (zie de ACE klaptellingen) aan die wegens Analyze Prefilterregel wordt opgesteld en het pakket wordt geïnspecteerd door de Snelmotor:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=3) 0xb788b786
...
access-list CSM_FW_ACL_ line 13 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
...
access-list CSM_FW_ACL_ line 16 advanced deny ip any any rule-id 268435458 event-log flow-start
(hitcnt=0) 0x97aa021a
```

## Gedrag controleren

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
```

Additional Information:

**This packet will be sent to snort for additional processing where a verdict will be reached**

...

Phase: 14

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Trace:

Packet: ICMP

AppID: service ICMP (3501), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 8, icmpCode 0

Firewall: **trust/fastpath rule, id 268435461, allow**

NAP id 1, IPS id 0, **Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow

...

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

**Action: allow**

## Hoofdpunten

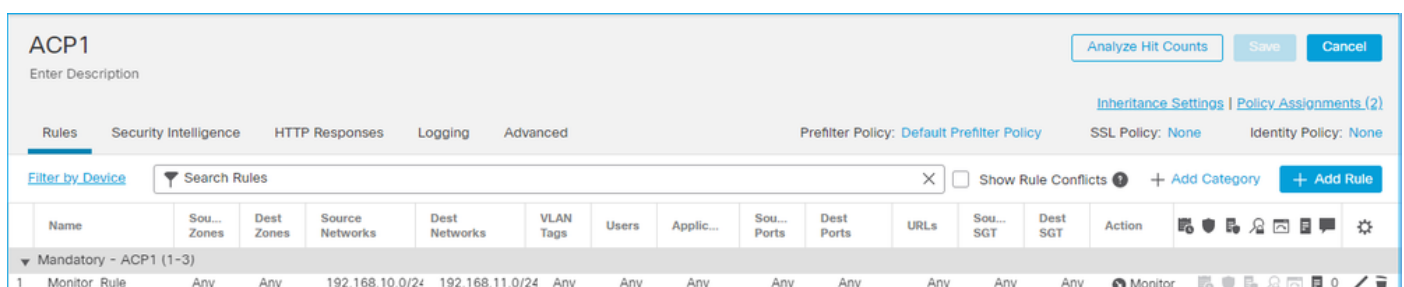
- Het **Analyze** De actie wordt als vergunningsregel in de motor van LINA ingezet. Dit heeft een effect op het pakket dat voor inspectie naar de Snort-engine wordt doorgestuurd
- Het **Analyze** Actie implementeert geen regel in de Snort-engine, zodat u ervoor moet zorgen dat u een regel in ACS configureert die in Snort wordt afgestemd
- Dit is afhankelijk van de ACS-regel die wordt toegepast in de Snort-motor (**block vs allow vs fastpath**) geen of alle of een paar pakketten zijn toegestaan door Snort

## Use cases

- Een gebruiksgeval van **Analyze** Actie is wanneer u een brede FastPath-regel in het Prefilter-beleid hebt en u wilt enkele uitzonderingen voor specifieke stromen, zodat ze worden geïnspecteerd door Snort

## Monitor-actie van ACP

Een monitorregel geconfigureerd in de FMC UI:



The screenshot shows the configuration page for ACP1 in the FMC UI. The 'Rules' tab is active, displaying a table of rules. A rule named 'Monitor\_Rule' is highlighted, with a 'Monitor' action. The rule is configured with 'Any' for source and destination zones, and specific source and destination networks (192.168.10.0/24 and 192.168.11.0/24). The action is set to 'Monitor'.

Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Sou... Ports	Dest Ports	URLs	Sou... SGT	Dest SGT	Action	Icons
Mandatory - ACP1 (1-3)														
1 Monitor_Rule	Any	Any	192.168.10.0/24	192.168.11.0/24	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	🔍 🛡️ 📄 🗑️

De monitorregel wordt op de FTD LINA-motor als **permit** en de Snort-motor als een **audit** actie.

```
firepower# show access-list
```

```
...  
access-list CSM_FW_ACL_line 10 advanced permit ip 192.168.10.0 255.255.255.0 192.168.11.0  
255.255.255.0 rule-id 268438863 (hitcnt=0) 0x61bbaf0c
```

## De Snort-regel:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules  
...  
# Start of AC rule.  
268438863 audit any 192.168.10.0 24 any any 192.168.11.0 24 any any any (log dcfoward flowend)  
# End rule 268438863
```

## Hoofdpunten

- De Regel van de monitor laat geen verkeer vallen of toestaat maar produceert een Gebeurtenis van de Verbinding. Het pakket wordt gecontroleerd op basis van verdere regels en wordt toegestaan of afgewezen
- FMC Connection-gebeurtenissen tonen aan dat het pakket aan 2 regels voldoet:

Connection Events <small>(switch workflow)</small>									
No Search Constraints <small>(Edit Search)</small>									
Connections with Application Details					Table View of Connection Events				
Jump to...									
<input type="checkbox"/>	First Packet ×	Last Packet ×	Action ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Access Control Policy ×	Access Control Rule ×
▼ <input type="checkbox"/>	2020-06-20 22:17:40	2020-06-20 22:17:43	Trust	192.168.10.50	192.168.11.50	41920 / tcp	80 (http) / tcp	ACP1	trust_L3-L4, Monitor_Rule

System support trace de output toont aan dat de pakketten beide regels aanpassen:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y  
Please specify an IP protocol: tcp  
Please specify a client IP address: 192.168.10.50  
Please specify a client port:  
Please specify a server IP address: 192.168.11.50  
Please specify a server port:  
Monitoring packet tracer and firewall debug messages
```

```
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 419031630  
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session  
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application  
unknown (0)  
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 new firewall session  
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 Starting AC with minimum 2, 'Monitor_Rule',  
and IPProto first with zone s -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source  
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0,  
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0  
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 2, 'Monitor_Rule', action  
Audit  
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 3, 'trust_L3-L4', action
```

## Trust

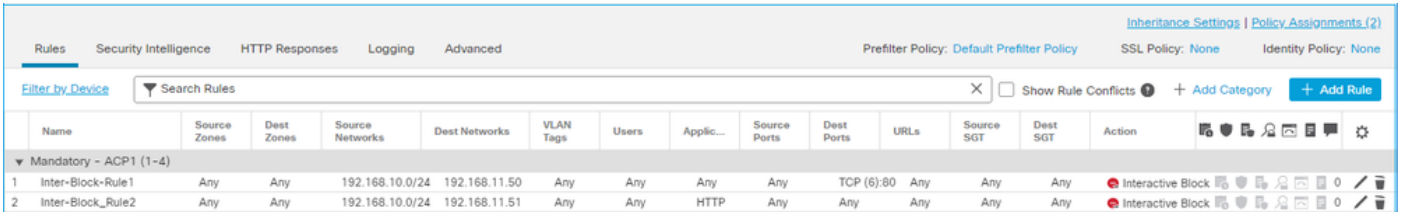
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id: 268438858,rule\_action:3, rev id:1078 02206, rule\_match flag:0x2

## Use cases

Gebruikt om netwerkactiviteit te controleren en een verbingsgebeurtenis te genereren

## Interactive Block-actie van ACP

Een Interactive Block-regel geconfigureerd in de FMC UI:



Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Mandatory - ACP1 (1-4)													
1 Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block
2 Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Interactive Block

De interactieve blokregel wordt op de FTD LINA-motor als een permit en de Snort-motor als omzeilingsregel:

```
firepower# show access-list
```

```
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Snort-engine:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438864 bypass any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 bypass any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

De Interactive Block-regel laat de gebruiker weten dat de bestemming verboden is



# Access Denied

**You are attempting to access a forbidden site.**

You may continue to the site by clicking on the button below.  
*Note:* You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

Continue

Standaard staat de firewall toe dat de blokkering 600 seconden wordt omzeild:

Rules	Security Intelligence	HTTP Responses	Logging	Advanced
<b>General Settings</b> 				
Maximum URL characters to store in connection events				1024
Allow an Interactive Block to bypass blocking for (seconds)				600
Retry URL cache miss lookup				Yes
Enable Threat Intelligence Director				Yes
Inspect traffic during policy apply				Yes

In het **system support trace** u kunt zien dat de firewall in eerste instantie het verkeer blokkeert en de blokpagina toont:

```
> system support trace
```

```
...
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 983273680, ack
2014879580
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 22, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

Zodra de gebruiker selecteert **Continue** (of vernieuwt de browser pagina) de debug toont aan dat de pakketten worden toegestaan door dezelfde regel die imiteert en **Allow** actie:

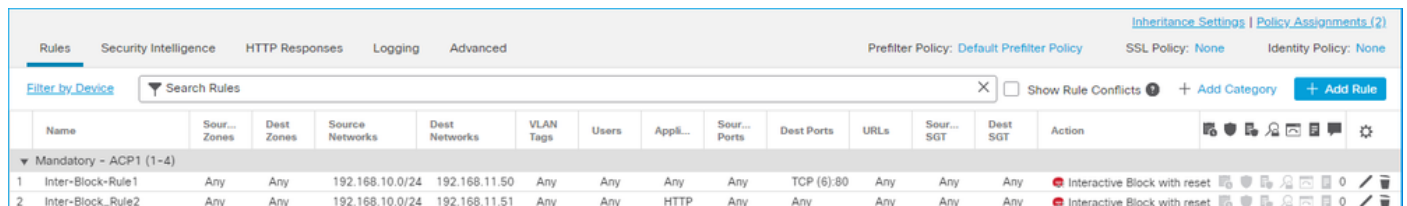
```
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack 2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0)
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589, misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 bypass action interactive bypass
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 allow action
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 8, NAP id 1, IPS id 0, Verdict PASS
```

## Use cases

Laat webgebruikers een waarschuwingspagina zien en geef hen de optie om door te gaan.

## Interactive Block with reset-actie van ACP

Een Interactive Block with reset-regel geconfigureerd in de FMC UI:



Name	Sour... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Appli...	Sour... Ports	Dest Ports	URLs	Sour... SGT	Dest SGT	Action
▼ Mandatory - ACP1 (1-4)													
1	Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block with reset
2	Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Interactive Block with reset

Het Interactive Block met reset rule wordt op FTD LINA engine als een **permit** actie en op Snortmotor als interreset regel:

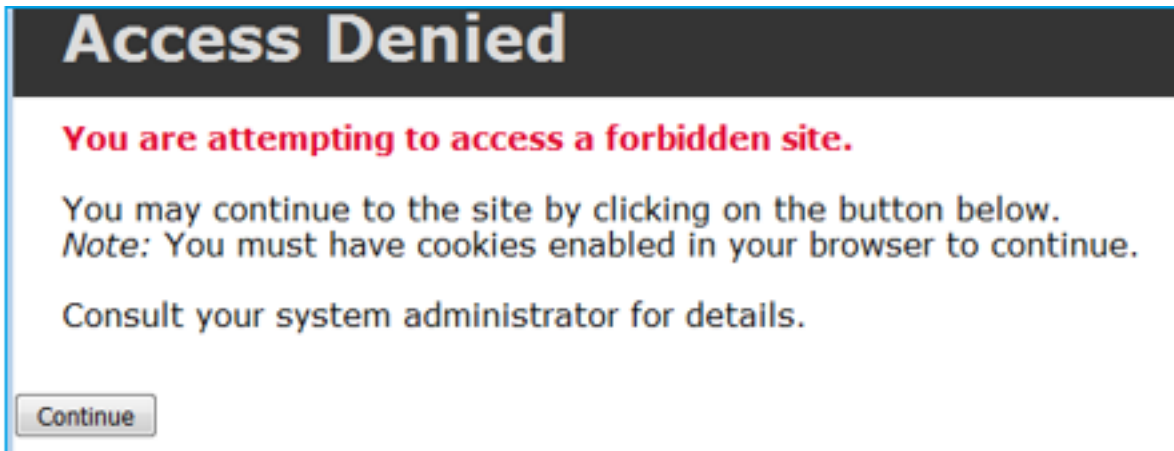
```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Snort-engine:

```
# Start of AC rule.
268438864 intreset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
```

```
# End rule 268438864
268438865 intreset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Net als bij het Blok met Reset kan de gebruiker het **Continue** optie:



In de Snort-debug wordt de actie Interactive Reset weergegeven:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.52
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3232128039
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 new firewall session
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0, client 0,
misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id:
268438864,rule_action:8, rev id:1099034206, rule_match flag:0x0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 HitCount data sent for rule id: 268438864,
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2228213518, ack
3232128040
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
```

```
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

Op dit punt wordt de blokpagina weergegeven aan de eindgebruiker. Als de gebruiker **Continue** (of vernieuwt de webpagina) dezelfde regel komt overeen die dit keer het verkeer door:

```
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1593478294, ack
3135589307
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 bypass action interactive bypass
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 allow action
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3135589307, ack
1593478786
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
```

## De Interactive Block with reset-regel stuurt een TCP RST naar niet-webverkeer:

```
firepower# show cap CAPI | i 11.50
 2: 22:13:33.112954      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: S
3109534920:3109534920(0) win 29200 <mss 1460,sackOK,timestamp 3745225378 0,nop,wscale 7>
 3: 22:13:33.113626      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S
3422362500:3422362500(0) ack 3109534921 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
53252448 3745225378>
 4: 22:13:33.113824      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362501 win 229 <nop,nop,timestamp 3745225379 53252448>
 5: 22:13:33.114953      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362501:3422362543(42) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 6: 22:13:33.114984      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362543:3422362549(6) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 7: 22:13:33.114984      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362549:3422362570(21) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 8: 22:13:33.115182      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362543 win 229 <nop,nop,timestamp 3745225381 53252448>
 9: 22:13:33.115411      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362549 win 229 <nop,nop,timestamp 3745225381 53252448>
10: 22:13:33.115426      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362570 win 229 <nop,nop,timestamp 3745225381 53252448>
12: 22:13:34.803699      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P
3109534921:3109534931(10) ack 3422362570 win 229 <nop,nop,timestamp 3745227069 53252448>
13: 22:13:34.804523      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: R
3422362570:3422362570(0) ack 3109534931 win 0
```

## FTD secundaire verbindingen en Pinholes

In oudere versies (bijvoorbeeld 6.2.2, 6.2.3, etc) opent de Snort-motor geen pinholes voor secundaire verbindingen (bijvoorbeeld FTD Data) als u de Trust actie. In recente releases wordt dit gedrag gewijzigd en opent de Snort-motor pinholes zelfs met de Trust actie.

## Richtlijnen voor FTD-regels

- Gebruik Fastpath-regels van het voorfilterbeleid voor zeer grote flows en om de latentie door het apparaat heen te verminderen
- Gebruik Block-regels in het voorfilter voor verkeer dat moet worden geblokkeerd op basis van L3/L4-voorwaarden
- Gebruik Trust-regels van het ACP als u een groot deel van de Snort-controles wilt omzeilen, maar nog wel gebruik wilt maken van functies zoals Identity Policy (identiteitsbeleid), QoS, SI, toepassingsdetectie, URL-filtering
- Plaats regels die een minder grote invloed hebben op de prestaties van de firewall boven aan het toegangscontrolebeleid met behulp van de volgende richtlijnen:
  1. Block-regels (lagen 1-4) - Block in voorfilter
  2. Allow-regels (lagen 1-4) - Fastpath in voorfilter
  3. Block-regels van ACP (lagen 1-4)
  4. Trust-regels (lagen 1-4)
  5. Block-regels (lagen 5-7 - toepassingsdetectie, URL-filtering)
  6. Allow-regels (lagen 1-7 - toepassingsdetectie, URL-filtering, Intrusion Policy/File Policy)
  7. Block-regel (standaardregel)

- Vermijd overmatige logboekregistraties (maak een logbestand bij de start of aan het einde en niet beide tegelijk)
- Houd rekening met de uitbreiding regels, om het aantal regels in LINA te controleren

```
firepower# show access-list | include elements
access-list CSM_FW_ACL; 7 elements; name hash: 0x4a69e3f3
```

## Samenvatting

### Voorfilteracties

Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). <b>No packets</b> are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. <b>Few or all packets</b> are sent to Snort engine for inspection. Traffic is allowed or dropped based on Snort engine verdict
Block (Prefilter)	Deny	-	Early drop by FTD LINA <b>No packets</b> are sent to Snort engine

### ACP-acties

Rule Action (FMC UI)	Additional Conditions	LINA Action	Snort Action	Notes
Block	The rule matches L3/L4 conditions	Deny	Deny	
Block	The rule has L7 conditions	Permit	Deny	
Allow		Permit	Allow	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, or ID) enabled	Permit	Fastpath	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, and ID) disabled	Trust	Fastpath	Static Flow Offload (4100/9300)
Monitor		Permit	Audit	Monitor Rule doesn't drop or permit traffic, but it generates a Connection Event. The packet is checked against subsequent rules and it is either allowed or dropped
Block with reset		Permit	Reset	When a packet matches Block with reset rule FTD sends a TCP Reset packet or an ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) message
Interactive Block		Permit	Bypass	Interactive Block Rule prompts the user that the destination is forbidden If bypassed, by default, the firewall allows to bypass the block for 600 seconds
Interactive Block with reset		Permit	Intreset	Same as Interactive Block with the addition of a TCP RST in case of non-web traffic

**Opmerking:** Vanaf 6.3 FTD-softwarecode Dynamic flow offload kan verbindingen offload die voldoen aan aanvullende criteria, bijvoorbeeld vertrouwde pakketten die een snelle inspectie vereisen. Controleer de sectie 'Offload Large Connections (Flows)' in de configuratiehandleiding van het Firepower Management Center voor meer informatie

## Gerelateerde informatie

- [FTD-toegangscontroleregels](#)
- [FTD-voorfilter en voorfilterbeleid](#)
- [Vastleggingen van de Firepower-firewall analyseren om netwerkproblemen effectief te troubleshooten](#)
- [Werken met vastleggingen van Firepower Threat Defense \(FTD\) en Packet Tracer](#)
- [Logboekregistratie configureren op FTD via FMC](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)
- [Grote verbindingen overdragen](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.