FTD-interfaces configureren in inline-modus

Inhoud

Inleiding

In dit document worden de configuratie, verificatie en achtergrondbediening van een inline-interface op een FirePOWER-apparaat (FTD) beschreven.

Voorwaarden

Vereisten

Er zijn geen specifieke eisen voor dit document.

Gebruikte componenten

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

- Firepower 4150 FTD (code 6.1.0.x en 6.3.x)
- Firepower Management Center (FMC) (code 6.1.0.x en 6.3.x)

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Verwante producten

Dit document kan ook met deze hardware- en softwareversies worden gebruikt:

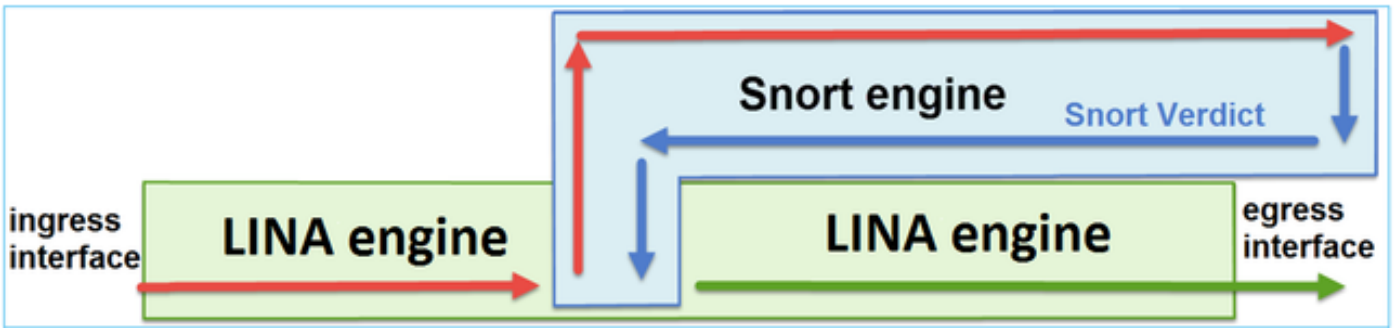
- ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X
- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), op Kernel gebaseerde virtuele machine (KVM)
- FTD-softwarecode 6.2.x en later

Achtergrondinformatie

FTD is een uniform softwarebeeld dat bestaat uit twee hoofdmotoren:

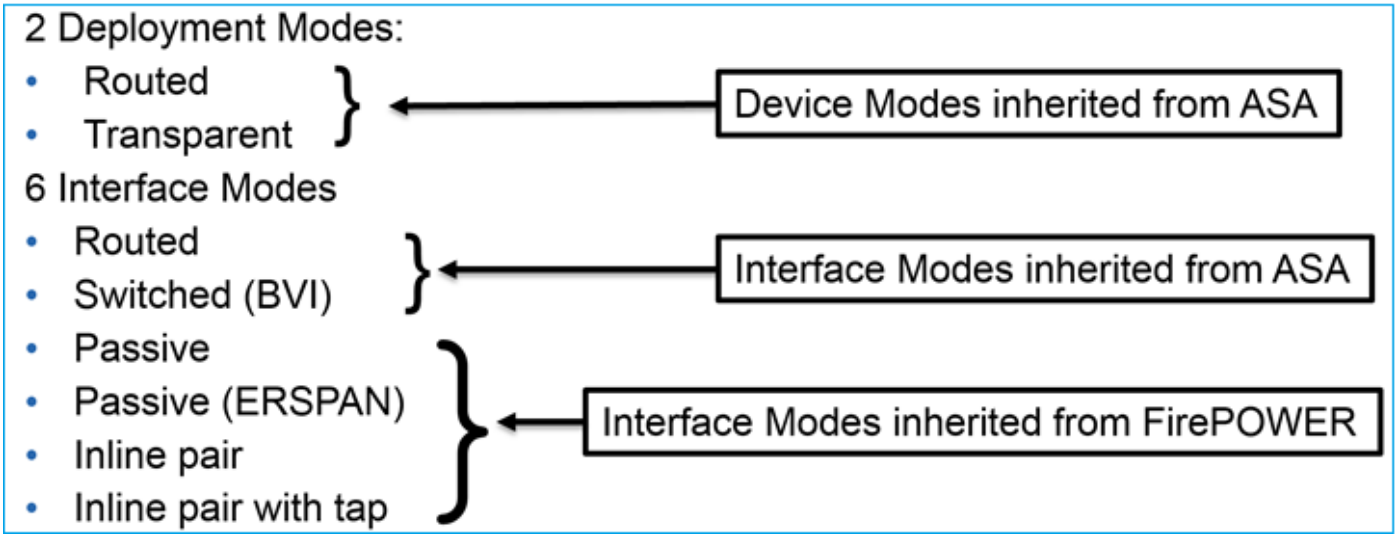
- LINA-motor
- sorteermachine

Dit getal laat zien hoe de twee motoren reageren:



- Een pakje gaat in de toegangsinterface en wordt behandeld door de LINA-motor
- Indien dit door het FTD-beleid vereist is, wordt het pakket door de snortmotor geïnspecteerd
- De Snort-machine geeft een oordeel voor het pakje terug
- De LINA-motor daalt of verstuurt het pakket op basis van de uitspraak van de Snort

FTD biedt twee implementatiemodi en zes interfacemodi zoals in afbeelding:



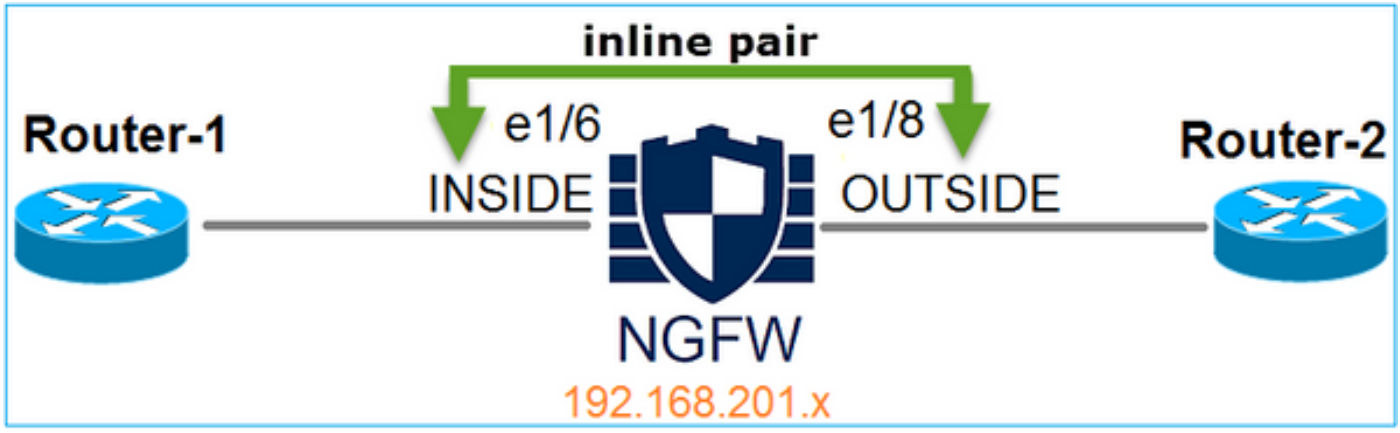
Opmerking: U kunt de interfacemodi op één FTD-apparaat combineren.

Hier volgt een overzicht van de verschillende FTD-implementaties en interfacemodi:

FTD-interfacemodus	FTD-implementatiemodus	Beschrijving	Verkeer kan worden verlaagd
Routed	Routed	Controle van de volledige LINA-motor en de snijmotor	Ja
switched	Doorzichtig	Controle van de volledige LINA-motor en de snijmotor	Ja
Inline paar	Routed of Transparent	Gedeeltelijke LINA-motor- en volledige motorcontroles	Ja
Inline paar met tap	Routed of Transparent	Gedeeltelijke LINA-motor- en volledige motorcontroles	Nee
passief	Routed of Transparent	Gedeeltelijke LINA-motor- en volledige motorcontroles	Nee
Passief (ERSPAN)	Routed	Gedeeltelijke LINA-motor- en volledige motorcontroles	Nee

Inline air-interface op FTD configureren

Netwerkdiagram



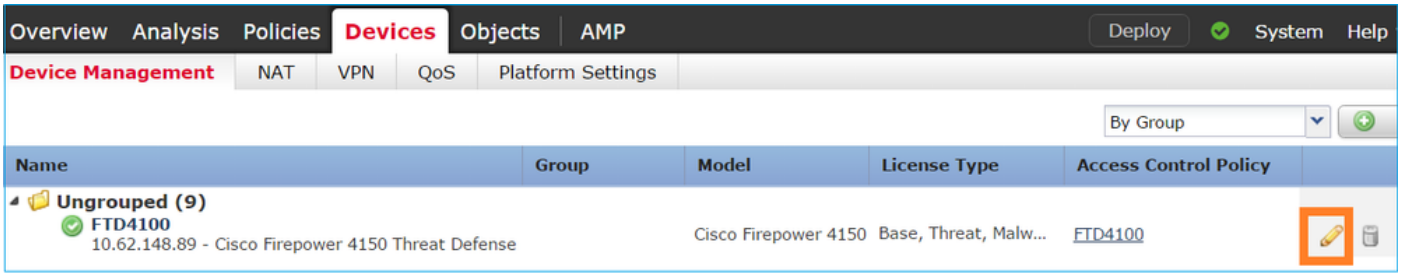
Vereisten

Configureer fysieke interfaces e1/6 en e1/8 in de modus Inline paar overeenkomstig deze eisen:

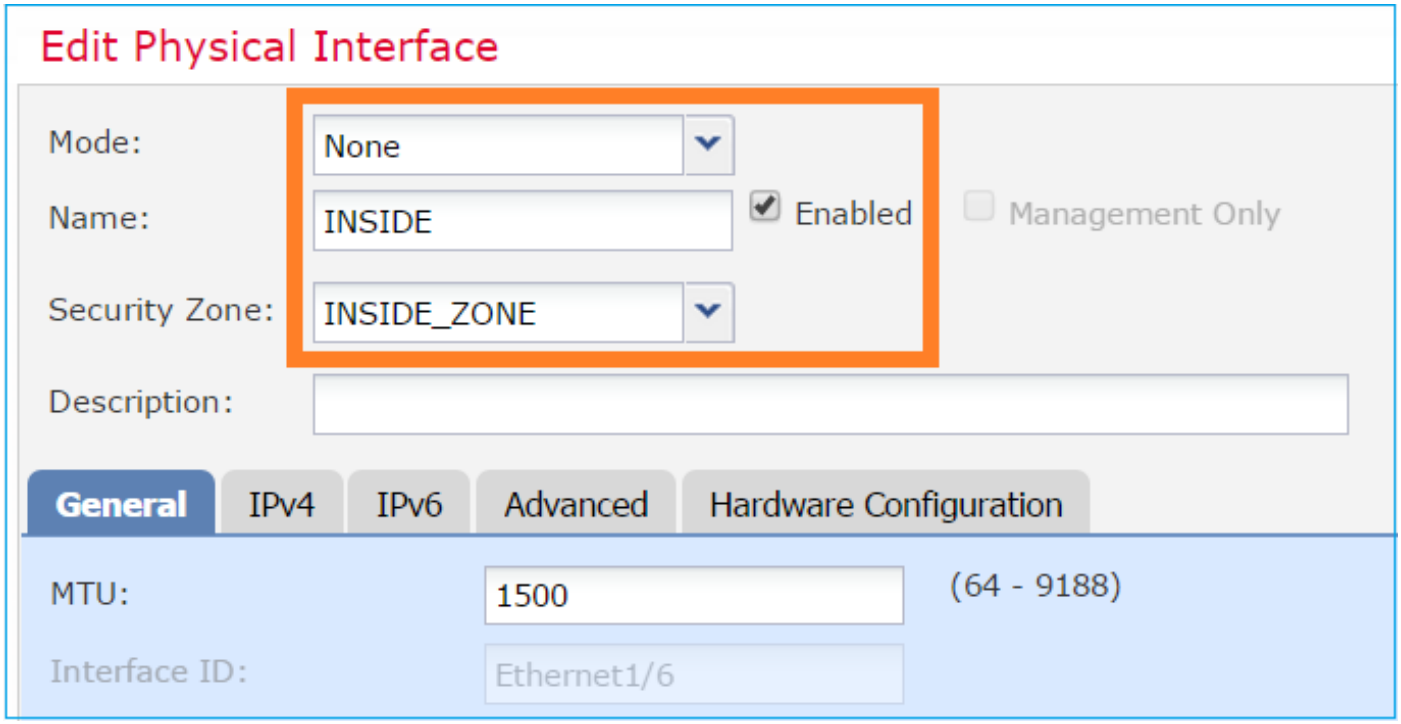
Interface	e1/6	E1/8
Name	BINNENKANT	BUITENKANT
Security zone	BINNENKANT_ZONE	BUITENKANT_ZONE
Naam inline instellen	Inline-air-1	
Inline stellen MTU	1500	
FailSafe	Ingeschakeld	
Verlengen linkstaat	Ingeschakeld	

Oplossing

Stap 1. Om aan de individuele interfaces te configureren selecteert u naar **Apparaatbeheer**, het juiste apparaat en selecteert u **Bewerken** zoals in de afbeelding.

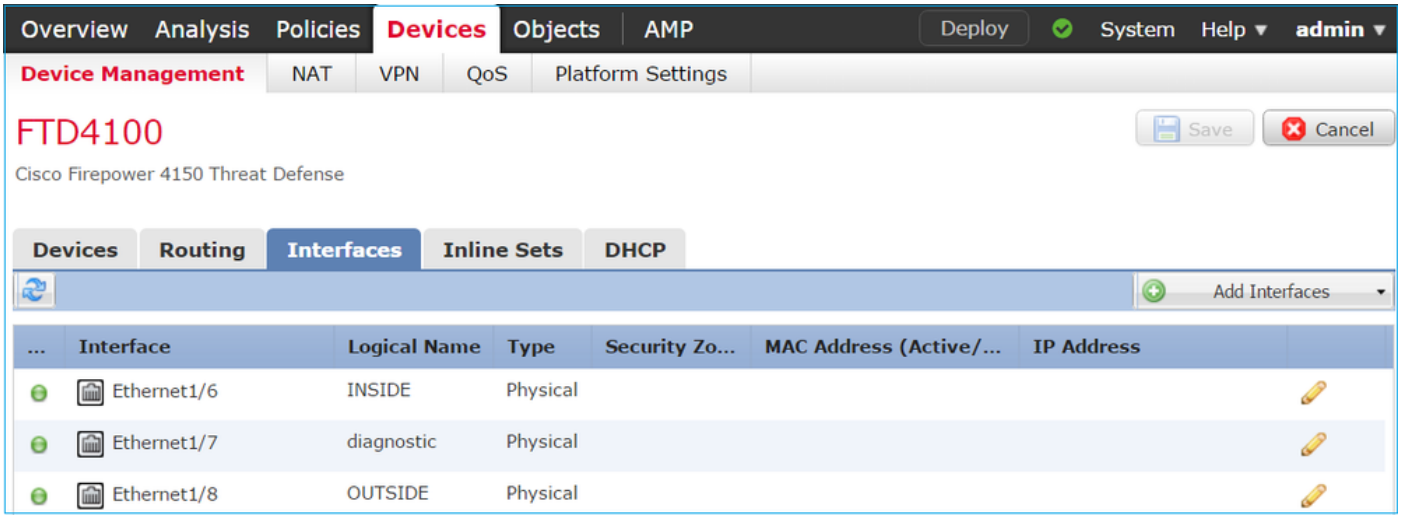


Specificeer vervolgens **Naam** en Tik **ingeschakeld** voor de interface zoals in de afbeelding.



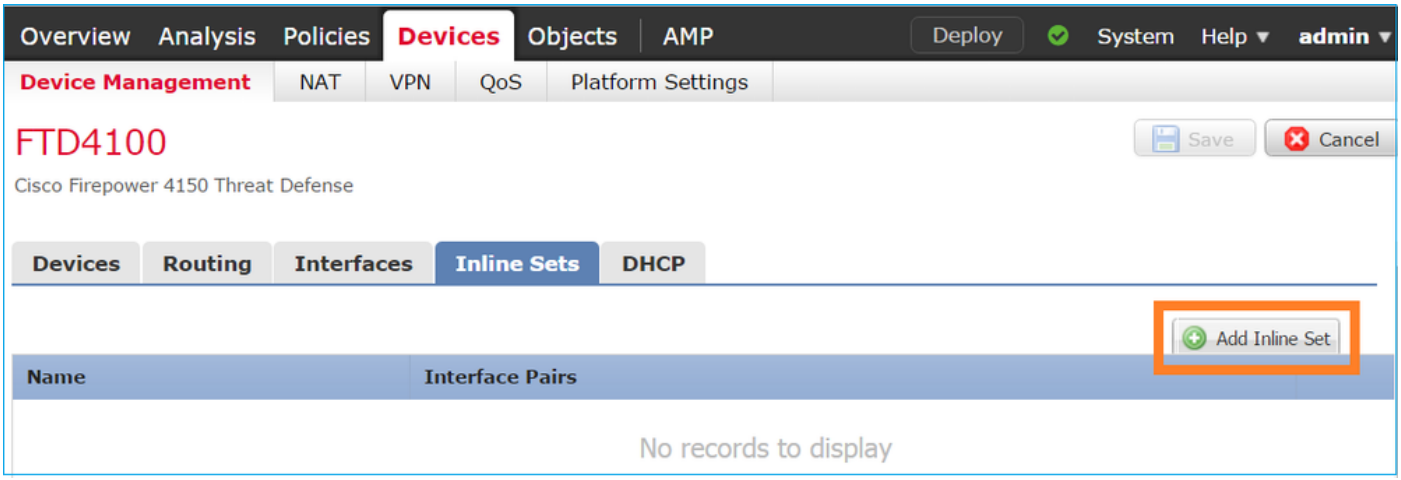
Opmerking: De naam is de naam van de interface.

Op dezelfde manier voor interface Ethernet1/8. Het eindresultaat is zoals in de afbeelding weergegeven.

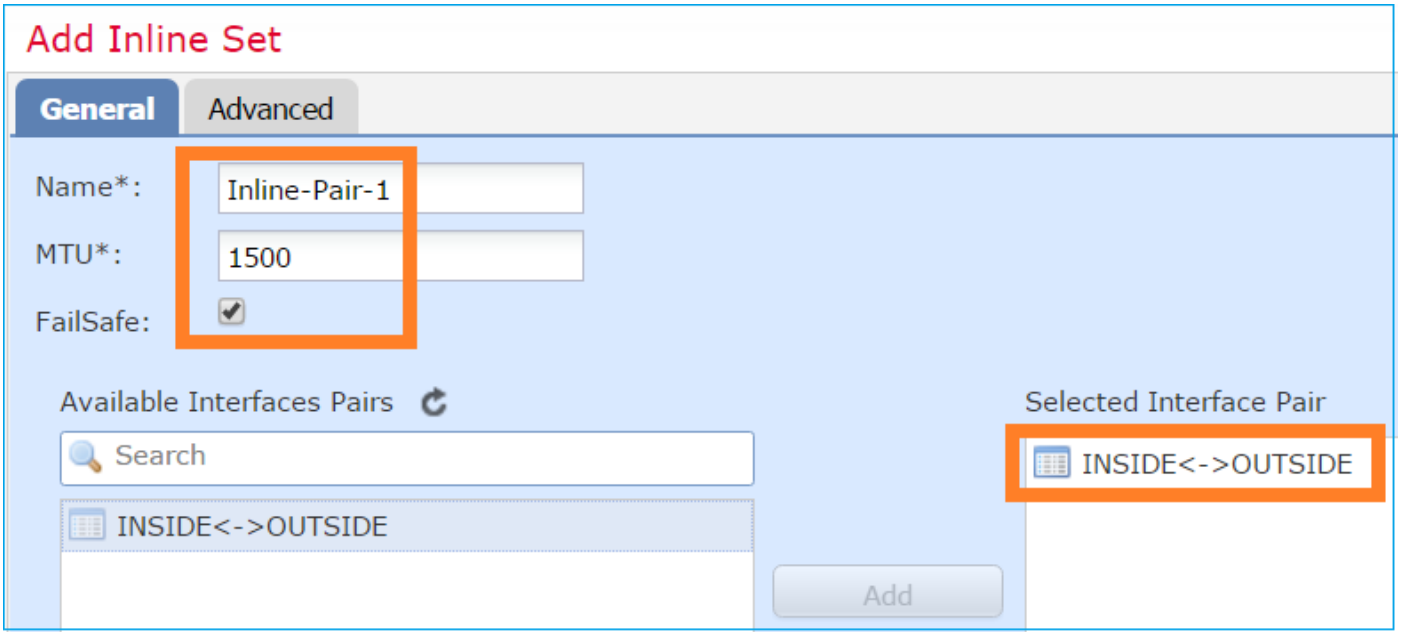


Stap 2. Configureer het inline paar.

Navigeren in op **inline sets > Inline set toevoegen** zoals in de afbeelding.

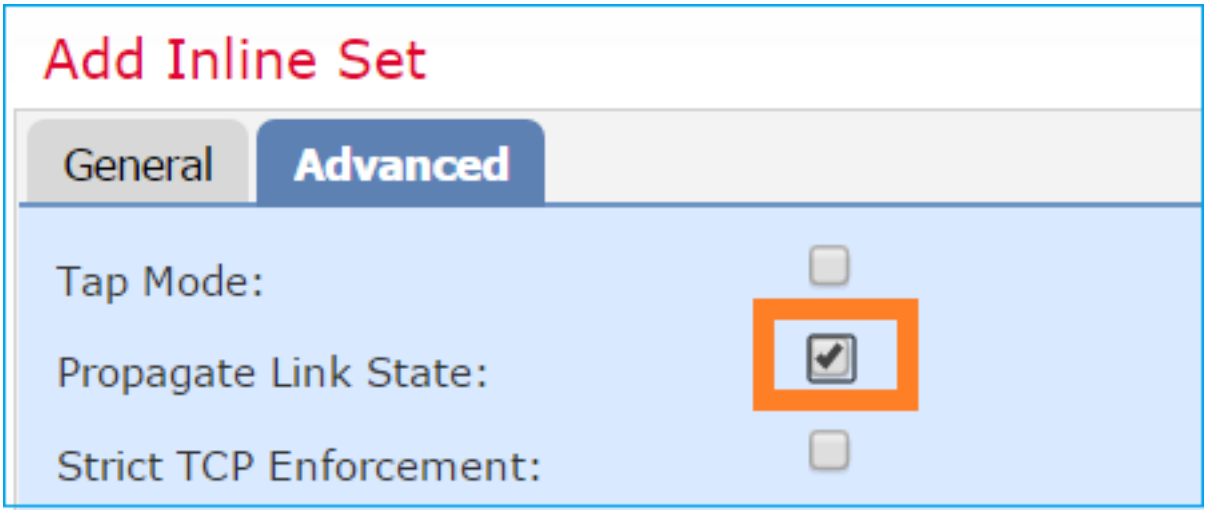


Stap 3. Het configureren van de algemene instellingen volgens de vereisten zoals in de afbeelding.



Opmerking: Met een defect kan het verkeer door het inline paar ongeïnspecteerd passeren voor het geval de interfacebuffers vol zijn (meestal gezien wanneer het apparaat overbelast is of de Snort-motor overbelast is). De grootte van de interfacebuffer wordt dynamisch toegewezen.

Stap 4. Schakel de optie **Link-status** uit in de geavanceerde instellingen zoals in de afbeelding.



De propagatie van de verbindingsstaat brengt automatisch de tweede interface in het inline interfacepaar neer wanneer één van de interfaces in de inline set daalt.

Stap 5. **Bewaar** de wijzigingen en **implementeer**.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Controleer de configuratie van het inline paar van de FTD CLI.

Oplossing

Meld u aan bij FTD CLI en controleer de configuratie van het inline paar:

```
> show inline-set

Inline-set Inline-Pair-1
 Mtu is 1500 bytes
 Failsafe mode is on/activated
 Failsecure mode is off
 Tap mode is off
 Propagate-link-state option is on
 hardware-bypass mode is disabled
 Interface-Pair[1]:
   Interface: Ethernet1/6 "INSIDE"
     Current-Status: UP
   Interface: Ethernet1/8 "OUTSIDE"
     Current-Status: UP
   Bridge Group ID: 509
>
```

Opmerking: De ID van de Bridge Group is een waarde die afwijkt van 0. Als de Tap-modus is ingeschakeld, is deze 0

Interface- en naaminformatie:

```
> show nameif
Interface                Name                    Security
Ethernet1/6              INSIDE                    0
Ethernet1/7              diagnostic                0
Ethernet1/8              OUTSIDE                   0
>
```

Controleer de interfacestatus:

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           169.254.1.1     YES unset  up                    up
Ethernet1/6                unassigned      YES unset  up                    up
Ethernet1/7                unassigned      YES unset  up                    up
Ethernet1/8                unassigned      YES unset  up                    up
```

Controleer de fysieke interfaceinformatie:

```
> show interface e1/6
Interface Ethernet1/6 "INSIDE", is up, line protocol is up
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
       MAC address 5897.bdb9.770e, MTU 1500
       IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
       IP address unassigned
 Traffic Statistics for "INSIDE":
       468 packets input, 47627 bytes
```

```
       12 packets output, 4750 bytes
       1 packets dropped
     1 minute input rate 0 pkts/sec,  200 bytes/sec
     1 minute output rate 0 pkts/sec,  7 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec,  96 bytes/sec
     5 minute output rate 0 pkts/sec,  8 bytes/sec
     5 minute drop rate, 0 pkts/sec
>show interface e1/8
Interface Ethernet1/8 "OUTSIDE", is up, line protocol is up
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
       MAC address 5897.bdb9.774d, MTU 1500
       IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
       IP address unassigned
 Traffic Statistics for "OUTSIDE":
       12 packets input, 4486 bytes
       470 packets output, 54089 bytes
       0 packets dropped
     1 minute input rate 0 pkts/sec,  7 bytes/sec
     1 minute output rate 0 pkts/sec,  212 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec,  7 bytes/sec
     5 minute output rate 0 pkts/sec,  106 bytes/sec
     5 minute drop rate, 0 pkts/sec
>
```

Controleer de werking van FTD inline-interface

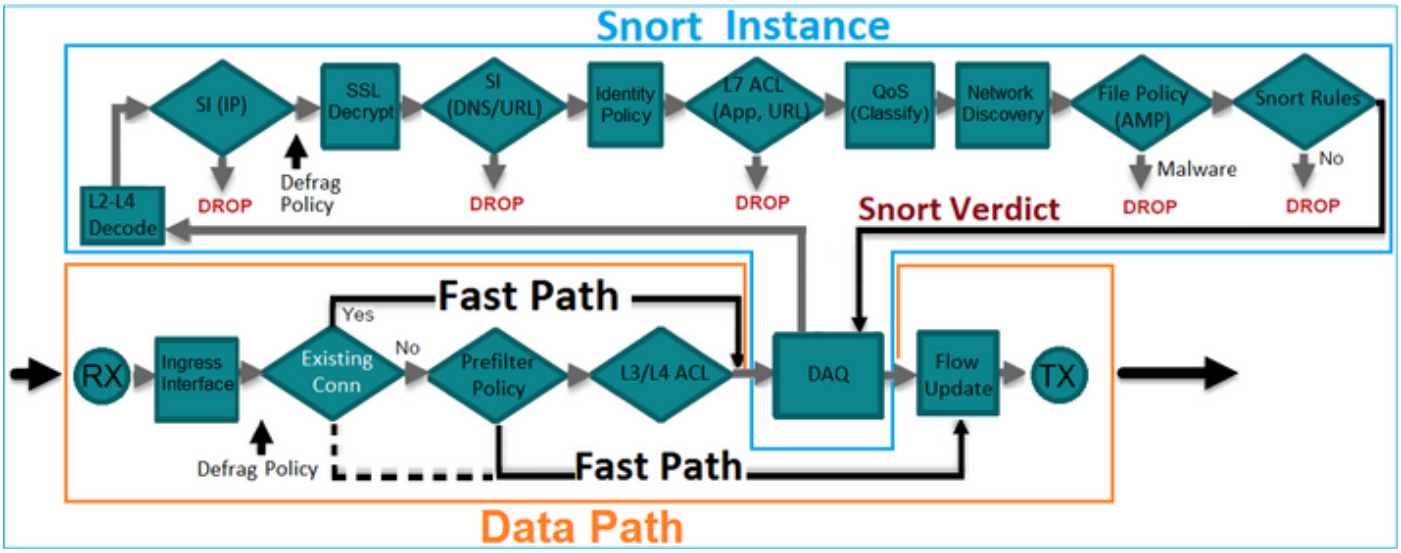
In dit deel worden deze verificatiecontroles behandeld om de inline-air-werking te verifiëren:

- Verificatie 1. Met behulp van pakkettracer
- Verificatie 2. Schakel opname met overtrekken in en verstuur een TCP-synchroniseer/erkende (SYN/ACK) pakket via het inline paar
- Verificatie 3. Controleer FTD-verkeer met het gebruik van een firewall-motor
- Verificatie 4. Controleer de doorgifte-functie van de koppelingsstaat
- Verificatie 5. Statische netwerkadresomzetting (NAT) configureren

Oplossing

Overzicht van architecturen

Wanneer 2 FTD interfaces in de modus Inline-paar werken, wordt een pakje verwerkt zoals in de afbeelding.

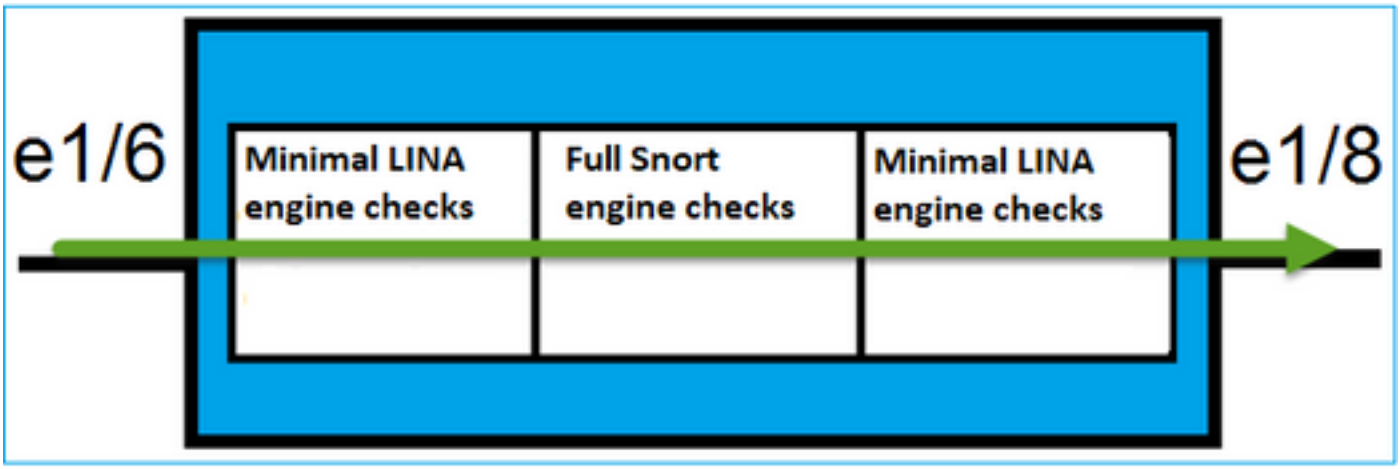


Opmerking: Alleen fysieke interfaces kunnen lid zijn van een inline-paar

Basistheorie

- Wanneer u een inline-paar 2 fysieke interfaces intern omgeven vormt
- Zeer vergelijkbaar met klassiek inline inbraakpreventiesysteem (IPS)
- Beschikbaar in Routed of Transparent Deployment-modi
- De meeste eigenschappen van de LINA-motor (NAT, routing enz.) zijn niet beschikbaar voor stromen die door een inline-paar gaan
- Doorvoerverkeer kan worden verbroken
- Enkele LINA-motorcontroles worden uitgevoerd samen met controles van de volledige motoren van de snijmotor

Het laatste punt kan zoals in de afbeelding worden weergegeven:



Verificatie 1. Met het gebruik van Packet-Tracer

De uitvoer van de pakkettracer die een pakje emuleert dat het inline-paar met de gemarkeerde belangrijke punten overbrengt:

```
> packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80
```

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

Phase: 2
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

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 4
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: 5
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 106, packet dispatched to next module

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

>
```

Verificatie 2. Verzend TCP SYN/ACK-pakketten via inline paar

U kunt TCP SYN/ACK-pakketten genereren met het gebruik van een pakket dat een hulpprogramma zoals Scapy maakt. Deze syntaxis genereert 3 pakketten met SYN/ACK-vlaggen die zijn ingeschakeld:

```
root@KALI:~# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>> conf.iface='eth0'
>>> packet = IP(dst="192.168.201.60")/TCP(flags="SA",dport=80)
>>> syn_ack=[]
>>> for i in range(0,3): # Send 3 packets
...  syn_ack.extend(packet)
...
>>> send(syn_ack)
```

Schakel deze opname in op FTD CLI en stuur een paar TCP/ACK-pakketten:

```
> capture CAPI interface INSIDE trace match ip host 192.168.201.60 any
>capture CAPO interface OUTSIDE match ip host 192.168.201.60 any
>
```

Nadat u de pakketten door de FTD hebt verzonden, kunt u een verbinding zien die werd gemaakt:

```
> show conn detail
1 in use, 34 most used
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       b - TCP state-bypass or nailed,
      C - CTIQBE media, c - cluster centralized,
      D - DNS, d - dump, E - outside back connection, e - semi-distributed,
      F - initiator FIN, f - responder FIN,
      G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
      i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
      k - Skinny media, M - SMTP data, m - SIP media, N - inspected by Snort, n - GUP
      O - responder data, P - inside back connection,
      q - SQL*Net data, R - initiator acknowledged FIN,
      R - UDP SUNRPC, r - responder acknowledged FIN,
      T - SIP, t - SIP transient, U - up,
      V - VPN orphan, v - M3UA W - WAAS,
      w - secondary domain backup,
      X - inspected by service module,
      x - per session, Y - director stub flow, y - backup stub flow,
      Z - Scansafe redirection, z - forwarding stub flow

TCP Inline-Pair-1:OUTSIDE(OUTSIDE): 192.168.201.60/80 Inline-Pair-1:INSIDE(INSIDE):
192.168.201.50/20,
   flags b N, idle 13s, uptime 13s, timeout 1h0m, bytes 0

>
```

Opmerking: b vlag - Een klassieke ASA zou een ongevraagd SYN/ACK-pakket laten vallen tenzij TCP state-bypass werd geactiveerd. Een FTD interface in de modus Inline Pair verwerkt een TCP-verbinding in een stand-bypass-modus en laat TCP-pakketten niet vallen die niet behoren tot de reeds bestaande verbindingen.

Opmerking: N vlag - Het pakket wordt geïnspecteerd door de FTD Sortmotor.

Dit blijkt uit de opnames, omdat je de 3 pakketten ziet die door de FTD worden verzonden:

```
> show capture CAPI
```

```
3 packets captured

  1: 15:27:54.327146       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
  2: 15:27:54.330000       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
  3: 15:27:54.332517       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
>
```

3 pakketten bestaat uit het FTD-apparaat:

```
> show capture CAPO

3 packets captured

  1: 15:27:54.327299       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
  2: 15:27:54.330030       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
  3: 15:27:54.332548       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
>
```

Met het gedeelte Trace van het eerste opnamepakket onthult u aanvullende informatie zoals het vonnis van de Snort-motor:

```
> show capture CAPI packet-number 1 trace

3 packets captured

   1: 15:27:54.327146       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
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: 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

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
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: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 282, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 8
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

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


1 packet shown
>
```

Met het spoor van het tweede opgenomen pakket toont dat het pakket met een bestaande verbinding overeenkomt zodat het de ACL-controle omzeilt, maar nog steeds wordt geïnspecteerd door de Snort-motor:

> **show capture CAPI packet-number 2 trace**

3 packets captured

   2: 15:27:54.330000   192.168.201.50.20 > 192.168.201.60.80: **S** 0:0(0) **ack** 0 win 8192
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:ing
Result: ALLOW
Config:
Additional Information:
Found flow with id 282, using existing flow

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

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

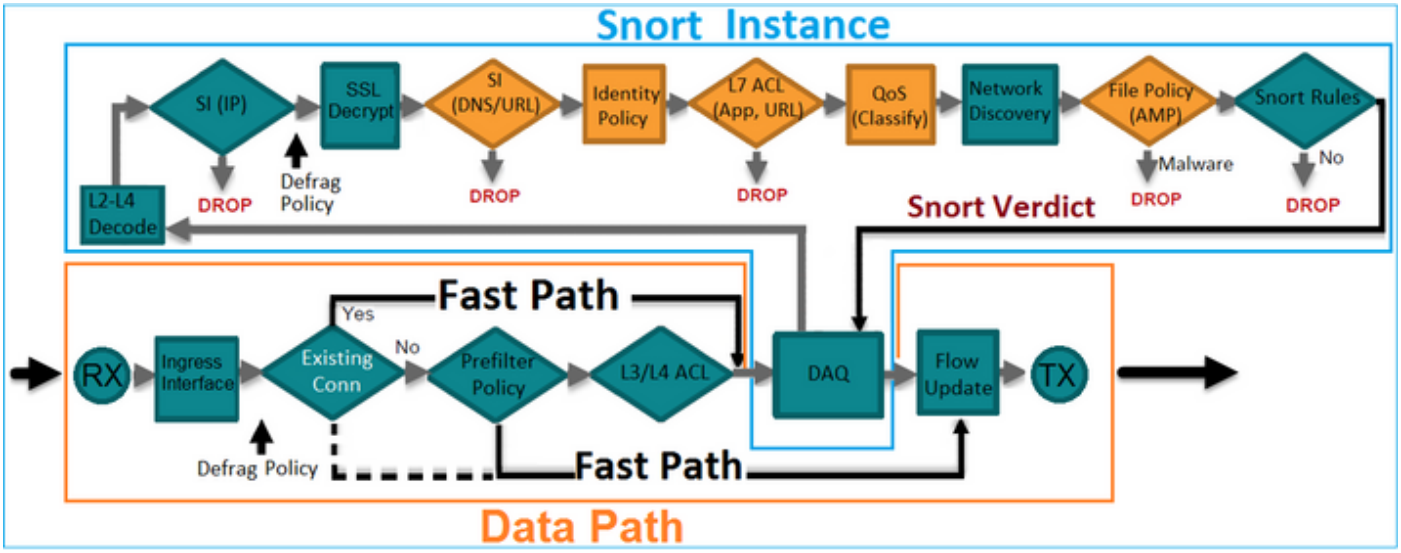
Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
Action: allow

1 packet shown

>

Verificatie 3. Firewallmotor defect voor toegestaan verkeer

Firewallmotor debug werkt tegen specifieke onderdelen van de FTD Snort Engine zoals in het toegangscontrolebeleid wordt weergegeven in de afbeelding:



Wanneer u de TCP SYN/ACK-pakketten via inline paar verzenden, kunt u in de debug-uitvoer zien:

```
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address: 192.168.201.60
Please specify a server port: 80
Monitoring firewall engine debug messages

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 New session
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 using HW or preset rule order 3, id 268438528
action Allow and prefilter rule 0
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 allow action
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 Deleting session
```

Verificatie 4. Controleer de doorgifte van de verbindingsstaat

Schakel de buffer logging op de FTD in en sluit de verbindingspoort die werd aangesloten op de e1/6 interface. Op FTD CLI moet je zien dat beide interfaces omlaag gingen:

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           169.254.1.1     YES unset  up                    up
Ethernet1/6                unassigned      YES unset  down                  down
Ethernet1/7                unassigned      YES unset  up                    up
Ethernet1/8                unassigned      YES unset  administratively down up
>
```

De FTD-logboeken tonen:

```
> show logging

Jan 03 2017 15:53:19: %ASA-4-411002: Line protocol on Interface Ethernet1/6, changed state to
down
Jan 03 2017 15:53:19: %ASA-4-411004: Interface OUTSIDE, changed state to administratively down
Jan 03 2017 15:53:19: %ASA-4-411004: Interface Ethernet1/8, changed state to administratively
down
Jan 03 2017 15:53:19: %ASA-4-812005: Link-State-Propagation activated on inline-pair due to
failure of interface Ethernet1/6(INSIDE) bringing down pair interface Ethernet1/8(OUTSIDE)
>
```

De inline-status toont de status van de 2 interfaceleden:

```
> show inline-set

Inline-set Inline-Pair-1
 Mtu is 1500 bytes
 Failsafe mode is on/activated
 Failsecure mode is off
 Tap mode is off
 Propagate-link-state option is on
 hardware-bypass mode is disabled
 Interface-Pair[1]:
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: Down(Propagate-Link-State-Activated)
    Interface: Ethernet1/8 "OUTSIDE"
      Current-Status: Down(Down-By-Propagate-Link-State)
   Bridge Group ID: 509
>
```

Let op het verschil in de status van de 2 interfaces:

```
> show interface e1/6
Interface Ethernet1/6 "INSIDE", is down, line protocol is down
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
       MAC address 5897.bdb9.770e, MTU 1500
       IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
        Propagate-Link-State-Activated
       IP address unassigned
 Traffic Statistics for "INSIDE":
       3393 packets input, 234923 bytes
       120 packets output, 49174 bytes
       1 packets dropped
     1 minute input rate 0 pkts/sec,  0 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec,  6 bytes/sec
     5 minute output rate 0 pkts/sec,  3 bytes/sec
     5 minute drop rate, 0 pkts/sec
>
```

En voor de Ethernet1/8 interface:

```
> show interface e1/8
Interface Ethernet1/8 "OUTSIDE", is administratively down, line protocol is up
```

```
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
       MAC address 5897.bdb9.774d, MTU 1500
       IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
       Down-By-Propagate-Link-State
       IP address unassigned
 Traffic Statistics for "OUTSIDE":
       120 packets input, 46664 bytes
       3391 packets output, 298455 bytes
       0 packets dropped
     1 minute input rate 0 pkts/sec,  0 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec,  3 bytes/sec
     5 minute output rate 0 pkts/sec,  8 bytes/sec
     5 minute drop rate, 0 pkts/sec
>
```

Nadat u de schakelaar opnieuw hebt ingeschakeld, tonen de FTD-logboeken:

```
> show logging
...
Jan 03 2017 15:59:35: %ASA-4-411001: Line protocol on Interface Ethernet1/6, changed state to up
Jan 03 2017 15:59:35: %ASA-4-411003: Interface Ethernet1/8, changed state to administratively up
Jan 03 2017 15:59:35: %ASA-4-411003: Interface OUTSIDE, changed state to administratively up
Jan 03 2017 15:59:35: %ASA-4-812006: Link-State-Propagation de-activated on inline-pair due to
recovery of interface Ethernet1/6(INSIDE) bringing up pair interface Ethernet1/8(OUTSIDE)
>
```

Verificatie 5. Statische NAT configureren

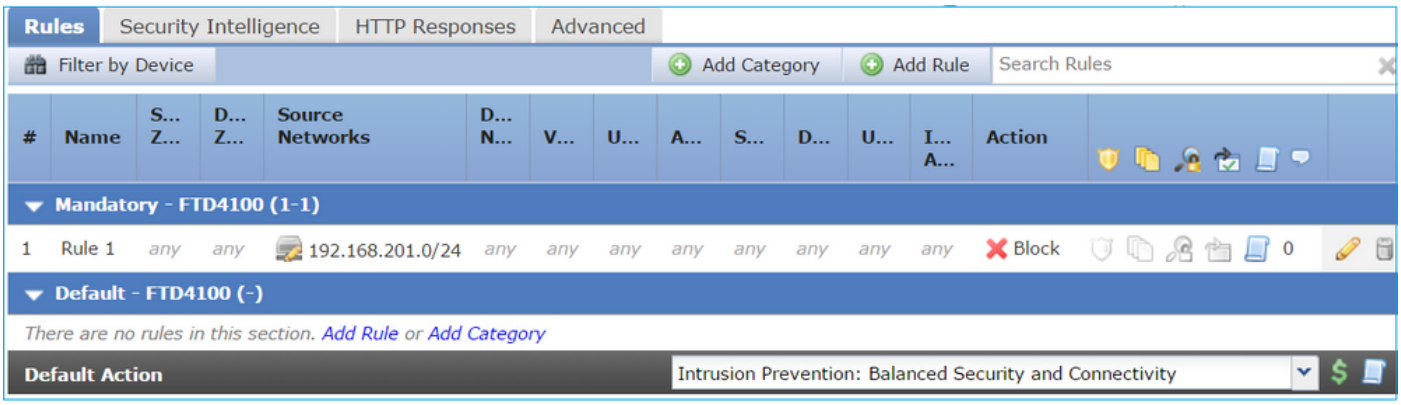
Oplossing

NAT wordt niet ondersteund voor interfaces die actief zijn in inline, inline kraan of passieve modi:

http://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Network_Address_Translation__NAT__for_Threat_Defense.html

Packet over inline paar interfacemodule blokkeren

Maak een blokregel, verstuur verkeer door het FTD Inline paar en observeer het gedrag zoals in de afbeelding.



Oplossing

Schakel opname met overtrekken in en verstuur de SYN/ACK-pakketten door het FTD Inline paar.

Het verkeer is geblokkeerd:

```
> show capture
capture CAPI type raw-data trace interface INSIDE [Capturing - 210 bytes]
  match ip host 192.168.201.60 any
capture CAPO type raw-data interface OUTSIDE [Capturing - 0 bytes]
  match ip host 192.168.201.60 any
```

Met de overtrek onthult een pakje:

```
> show capture CAPI packet-number 1 trace

3 packets captured

  1: 16:12:55.785085       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
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: 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

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1
Additional Information:

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

```
1 packet shown
```

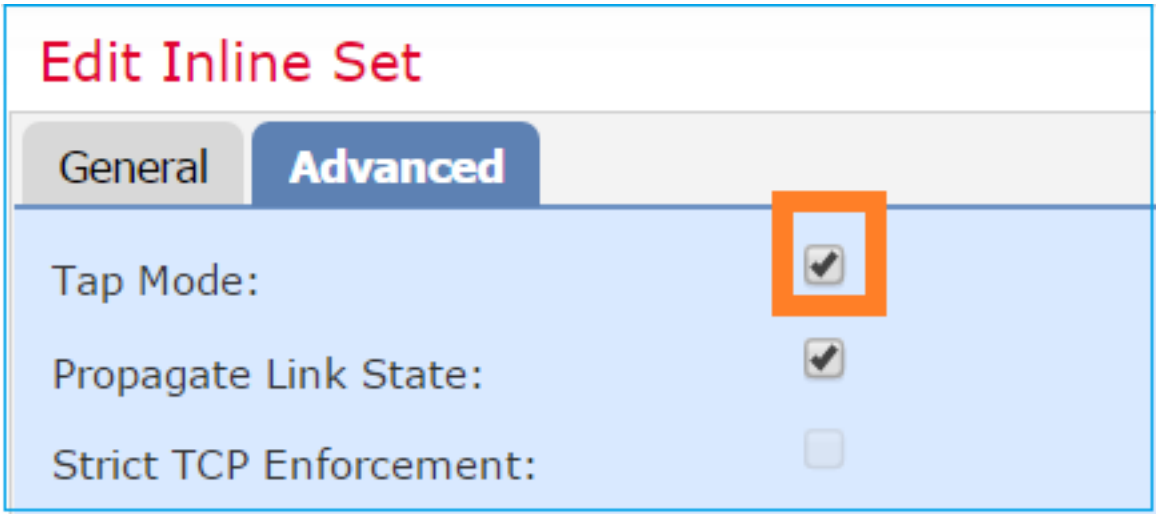
In dit spoor kan worden gezien dat het pakket door de FTD LINA-motor is gevallen en niet naar de FTD Snort-motor is doorgestuurd.

Inline pofmodus instellen met tap

Schakel de Tap-modus in op het inline paar.

Oplossing

Navigeren in op **Apparaten > Apparaatbeheer > Inline sets > Inline set bewerken > Geavanceerd** en **Tap Mode** inschakelen zoals in het beeld wordt getoond.



Verificatie

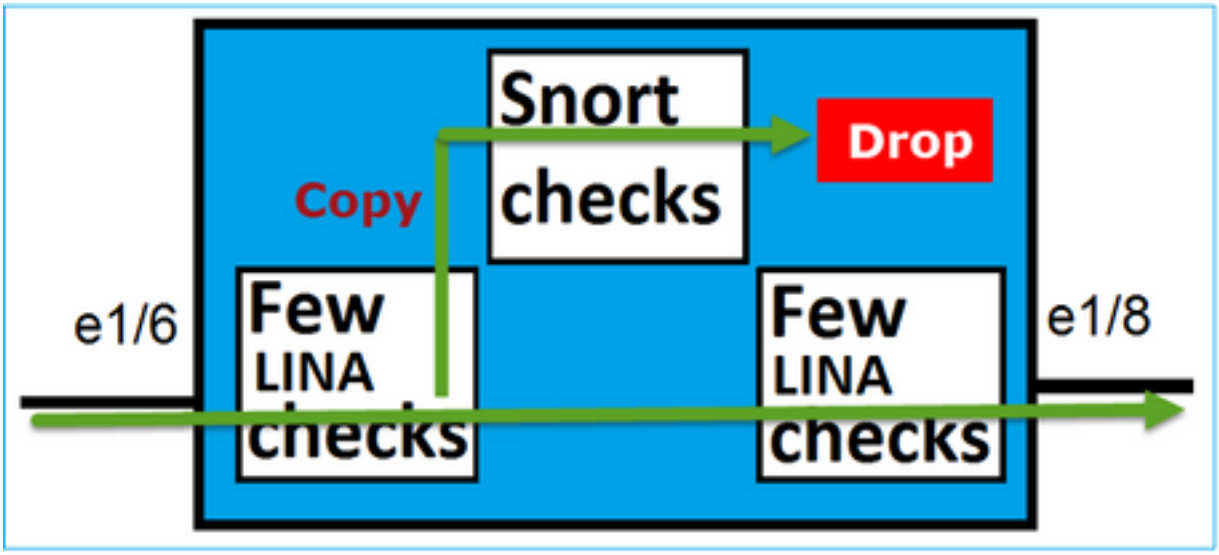
```
> show inline-set

Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
  Tap mode is on
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/8 "OUTSIDE"
      Current-Status: UP
    Bridge Group ID: 0
>
```

Controleer FTD Inline paar met tap-interfacewerking

Basistheorie

- Wanneer u een inline paar met tap 2 vormt, worden de fysieke interfaces intern overbrugd
- Het is beschikbaar in Routed of Transparent Deployment-modi
- De meeste motorfuncties van de LINA (NAT, routing enz.) zijn niet beschikbaar voor stromen die door het inline paar gaan
- Feitelijk verkeer kan niet worden laten vallen
- Enkele LINA-motorcontroles worden samen met volledige controles van de snijmachine op een kopie van het werkelijke verkeer uitgevoerd

Het laatste punt is zoals in de afbeelding weergegeven:



Het inline paar met de Tap-modus laat het transitoverkeer niet vallen. Met het spoor van een pakje bevestigt dit:

```
> show capture CAPI packet-number 2 trace

3 packets captured

   2: 13:34:30.685084       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
```

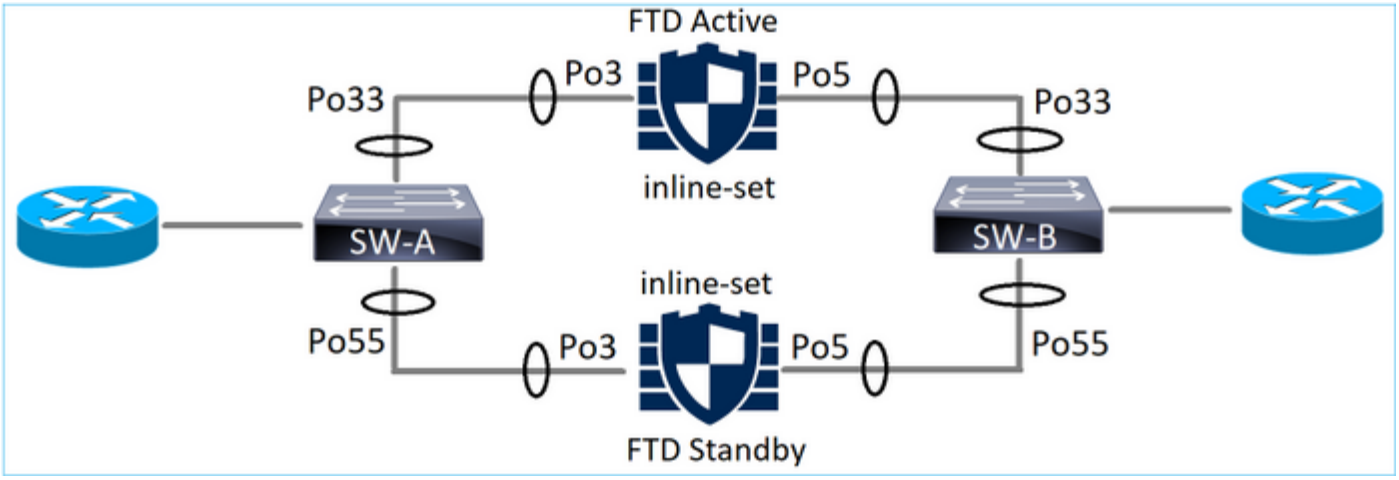
```
Additional Information:
MAC Access list

Phase: 3
Type: 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

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: WOULD HAVE DROPPED
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: Access-list would have dropped, but packet forwarded due to inline-tap


1 packet shown
>
```

Inline paar en Ethernet

U kunt online paar op twee manieren met etherchannel configureren:

1. EtherChannel beëindigd op FTD
2. EtherChannel die door de FTD gaat (hiervoor is FXOS-code 2.3.1.3 en hoger nodig)

EtherChannel beëindigd op FTD



Ethernet op SW-A:

```
SW-A# show etherchannel summary | i Po33|Po55
33     Po33(SU)         LACP      Gi3/11(P)
35     Po35(SU)         LACP      Gi2/33(P)
```

Ethernet op SW-B:

```
SW-B# show etherchannel summary | i Po33|Po55
33     Po33(SU)         LACP        Gi1/0/3(P)
55     Po55(SU)         LACP        Gi1/0/4(P)
```

Het verkeer wordt doorgestuurd door de actieve FTD op basis van het leren van MAC-adres:

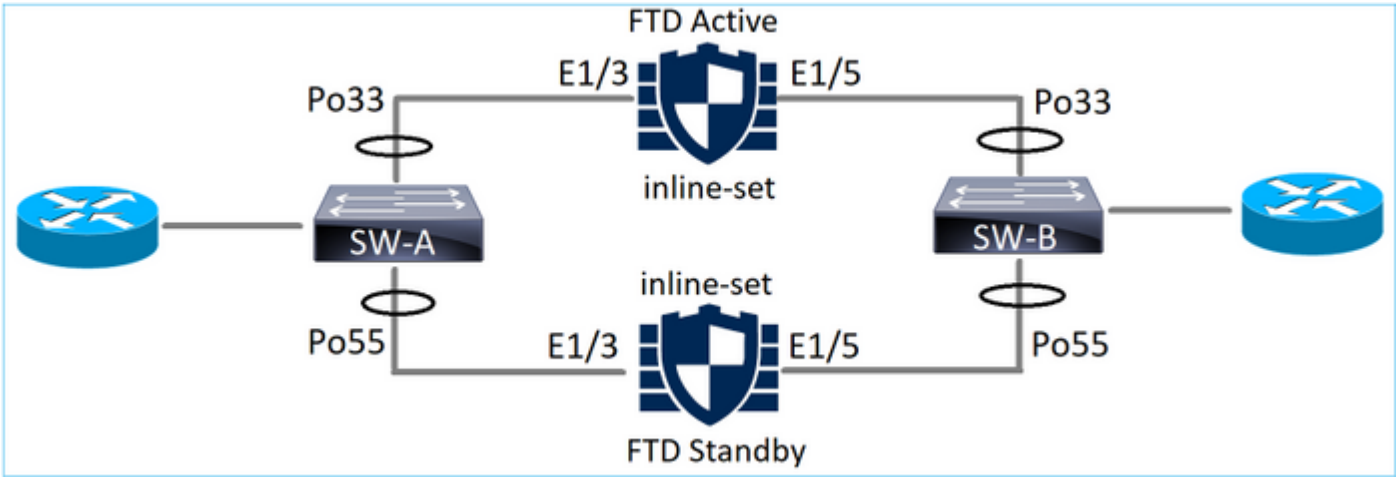
```
SW-B# show mac address-table address 0017.dfd6.ec00
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC     Po33
Total Mac Addresses for this criterion: 1
```

De inline-set op FTD:

```
FTD# show inline-set

Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Port-channel3 "INSIDE"
      Current-Status: UP
    Interface: Port-channel5 "OUTSIDE"
      Current-Status: UP
    Bridge Group ID: 775
```

Opmerking: In het geval van een FTD failover-gebeurtenis is de verkeersuitval voornamelijk afhankelijk van de tijd die het op de switches vergt om het MAC-adres van de externe peer te leren.

Ethernet door de FTD



Ethernet op SW-A:

```
SW-A# show etherchannel summary | i Po33|Po55
33     Po33(SU)         LACP      Gi3/11(P)
55     Po55(SD)         LACP      Gi3/7(I)
```

De LACP-pakketten die door de Standby FTD gaan worden geblokkeerd:

```
FTD# capture ASP type asp-drop fo-standby
FTD# show capture ASP | i 0180.c200.0002
  29: 15:28:32.658123       a0f8.4991.ba03 0180.c200.0002 0x8809 Length: 124
  70: 15:28:47.248262       f0f7.556a.11e2 0180.c200.0002 0x8809 Length: 124
```

Ethernet op SW-B:

```
SW-B# show etherchannel summary | i Po33|Po55
33     Po33(SU)         LACP        Gi1/0/3(P)
55     Po55(SD)         LACP        Gi1/0/4(s)
```

Het verkeer wordt doorgestuurd door de actieve FTD op basis van het leren van MAC-adres:

```
SW-B# show mac address-table address 0017.dfd6.ec00
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC     Po33
Total Mac Addresses for this criterion: 1
```

De inline-set op FTD:

```
FTD# show inline-set

Inline-set SET1
 Mtu is 1500 bytes
 Fail-open for snort down is on
 Fail-open for snort busy is off
 Tap mode is off
 Propagate-link-state option is off
 hardware-bypass mode is disabled
 Interface-Pair[1]:
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/5 "OUTSIDE"
      Current-Status: UP
   Bridge Group ID: 519
```

> **Voorzichtig:** In dit scenario hangt de convergentietijd in het geval van een FTD-uitvalgebeurtenis hoofdzakelijk af van de Ethernet LACP-onderhandeling en kan, afhankelijk van de tijd die de uitval vergt, veel langer zijn. Indien de EtherChannel-modus ON (geen LACP) is, hangt de convergentietijd af van het MAC-adresleren.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Vergelijking: Inline paar vs inline paar met tap

	Inline paar	Lijnen met tap
inline tonen	> inline-set tonen Inline-set inline-air-1 Mtu is 1500 bytes De failover-veilige modus is ingeschakeld/geactiveerd De failover-modus is uit **De Tap-modus is uit** De optie Verspreiding-link-staat is ingeschakeld hardware-bypass-modus is uitgeschakeld Interfacepair[1]: Interface: Ethernet1/6 "INSIDE" Huidige status: OMHOOG Interface: Ethernet1/8 "BUITEN" Huidige status: OMHOOG **Bridge Group-ID: 509**	**> inline tonen** Inline-set inline-air-1 Mtu is 1500 bytes De failover-veilige modus is ingeschakeld/geactiveerd De failover-modus is uit **De Tap-modus is ingeschakeld** De optie Verspreiding-link-staat is ingeschakeld hardware-bypass-modus is uitgeschakeld Interfacepair[1]: Interface: Ethernet1/6 "INSIDE" Huidige status: OMHOOG Interface: Ethernet1/8 "BUITEN" Huidige status: OMHOOG **Bridge Group-ID: 0**
raakvlak tonen	> **> Interface e1/6 tonen** Interface Ethernet1/6 "INSIDE", is omhoog, het lijnprotocol is omhoog Hardware is EtherSwitch, BW 1000 Mbps, DLY 1000 usec MAC-adres 5897.bdb9.770e, MTU 1500 IPS-interfacemodule: **inline**, inline-set: Inline-air-1 IP-adres niet toegewezen Verkeersstatistieken voor "INSIDE": 3957 ingevoerde pakketten, 264913 bytes 144 Packet-uitvoer, 5864 bytes 4 gevallen pakketten 1 minuut ingangssnelheid 0 pkts/sec, 26 bytes/sec 1 minuut uitvoersnelheid 0 pkts/sec, 7 bytes/sec 1 minuut druppelsnelheid, 0 pkts/sec 5 minuten ingangssnelheid, 0 pkts/sec, 28 bytes/sec 5 minuten uitvoersnelheid, 0 pkts/sec, 9 bytes/sec 5 minuten druppelsnelheid, 0 pkts/sec **>Interface e1/8 tonen** Interface Ethernet1/8 "BUITENKANT", omhoog, is het lijnprotocol omhoog Hardware is EtherSwitch, BW 1000 Mbps, DLY 1000 usec MAC-adres 5897.bdb9.774d, MTU 1500 IPS-interfacemodule: **inline**, inline-set: Inline-air-1 IP-adres niet toegewezen	> **> Interface e1/6 tonen** Interface Ethernet1/6 "INSIDE", is omhoog, het lijnprotocol is omhoog Hardware is EtherSwitch, BW 1000 Mbps, DLY 1000 usec MAC-adres 5897.bdb9.770e, MTU 1500 IPS-interfacemodule: **inline kraan**, inline-set: Inline-air-1 IP-adres niet toegewezen Verkeersstatistieken voor "INSIDE": 24 pakketten die worden ingevoerd, 1378 bytes 0 pakketten, uitvoer, 0 bytes 24 dode pakketten 1 minuut ingangssnelheid 0 pkts/sec, 0 bytes/sec 1 minuut uitvoersnelheid 0 pkts/sec, 0 bytes/sec 1 minuut druppelsnelheid, 0 pkts/sec 5 minuten ingangssnelheid, 0 pkts/sec, 0 bytes/sec 5 minuten uitvoersnelheid, 0 pkts/sec, 0 bytes/sec 5 minuten druppelsnelheid, 0 pkts/sec **>Interface e1/8 tonen** Interface Ethernet1/8 "BUITENKANT", omhoog, is het lijnprotocol omhoog Hardware is EtherSwitch, BW 1000 Mbps, DLY 1000 usec MAC-adres 5897.bdb9.774d, MTU 1500 IPS-interfacemodule: **inline kraan**, inline-set: Inline-air-1 IP-adres niet toegewezen

Packet met blokregel omgaan	Verkeersstatistieken voor "BUITEN": 144 pakketten die worden ingevoerd, 5634 bytes 3954-pakketten, 39987 bytes 0 zakken 1 minuut ingangssnelheid 0 pkts/sec, 7 bytes/sec 1 minuut uitvoer, 0 pkts/sec, 37 bytes/sec 1 minuut druppelsnelheid, 0 pkts/sec 5 minuten ingangssnelheid, 0 pkts/sec, 8 bytes/sec 5 minuten uitvoer, 0 pkts/sec, 39 bytes/sec 5 minuten druppelsnelheid, 0 pkts/sec > **> Opname CAPI-pakketnummer 1-spoor tonen** 3 opgenomen pakketten 1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 wint 8192 Fase: 1 Type: OPVANGEN Subtype: Resultaat: TOESTAAN Config: Aanvullende informatie: MAC-toegangslijst Fase: 2 Type: TOEGANGSLIJST Subtype: Resultaat: TOESTAAN Config: impliciete regel Aanvullende informatie: MAC-toegangslijst **Fase: 3** **Type: NGIPS-MODE** **Subtype: NGIPS-modus** **Resultaat: TOESTAAN** **Config:** **Aanvullende informatie:** **De stroom wordt ingedrukt en er wordt een interface ingesteld voor NGIPS-modus en NGIPS-services** **Fase: 4** **Type: TOEGANGSLIJST** **Subtype: logboek** **Resultaat: DROP** Config: toegangsgroep CSM_FW_ACL_ global toegangslijst CSM_FW_ACL_ Advanced ontkennen ip 192.168.201.0 255.255.255.0 elk regelnummer-id 268441600-log flow-start toegangslijst CSM_FW_ACL_ remark regel-id 26841600: TOEGANGSBELEID: FTD4100 - Verplicht/1 toegangslijst CSM_FW_ACL_ remark regel-id 26841600: L4 REGEL: Artikel 1 Aanvullende informatie: Resultaat: input-interface: BINNENKANT invoerstatus: omhoog invoerregel-status: omhoog Actie: vallen **Drop-rede: (acl-drop) Flow wordt ontkend door geconfigureerde regel** 1 pakket getoond >	Verkeersstatistieken voor "BUITEN": 1 Packet-invoer, 441 bytes 0 pakketten, uitvoer, 0 bytes 1 postpakketten 1 minuut ingangssnelheid 0 pkts/sec, 0 bytes/sec 1 minuut uitvoersnelheid 0 pkts/sec, 0 bytes/sec 1 minuut druppelsnelheid, 0 pkts/sec 5 minuten ingangssnelheid, 0 pkts/sec, 0 bytes/sec 5 minuten uitvoersnelheid, 0 pkts/sec, 0 bytes/sec 5 minuten druppelsnelheid, 0 pkts/sec > **> Opname CAPI-pakketnummer 1-spoor tonen** 3 opgenomen pakketten 1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win Fase: 1 Type: OPVANGEN Subtype: Resultaat: TOESTAAN Config: Aanvullende informatie: MAC-toegangslijst Fase: 2 Type: TOEGANGSLIJST Subtype: Resultaat: TOESTAAN Config: impliciete regel Aanvullende informatie: MAC-toegangslijst **Fase: 3** **Type: NGIPS-MODE** **Subtype: NGIPS-modus** **Resultaat: TOESTAAN** **Config:** **Aanvullende informatie:** **De stroom wordt ingedrukt en er wordt een interface ingesteld voor NGIPS-NGIPS-services** **Fase: 4** **Type: TOEGANGSLIJST** Subtype: logboek **Resultaat: ZOU ZIJN VERDROOGD** Config: toegangsgroep CSM_FW_ACL_ global toegangslijst CSM_FW_ACL_ Advanced ontkennen ip 192.168.201.0 255.2 elk regelnummer-id 268441600-log flow-start toegangslijst CSM_FW_ACL_ remark regel-id 26841600: TOEGANGSBEL FTD4100 - Verplicht/1 toegangslijst CSM_FW_ACL_ remark regel-id 26841600: L4 REGEL: Artike Aanvullende informatie: Resultaat: input-interface: BINNENKANT invoerstatus: omhoog invoerregel-status: omhoog **Actie: De toegangslijst zou zijn gevallen, maar pakje zou zijn doorgestuurd inline tap** 1 pakket getoond >

Samenvatting

- Wanneer u de modus Inline paar gebruikt, gaat het pakje voornamelijk door de FTD Snort-motor
- TCP-verbindingen worden verwerkt in een TCP-state-bypass-modus
- Vanuit het motorstandpunt van de FTD LINA wordt een ACL-beleid toegepast
- Wanneer de modus Inline paar in gebruik is, kunnen er pakketten worden geblokkeerd omdat ze online zijn verwerkt
- Als de Tap Mode is ingeschakeld, wordt een kopie van het pakket intern geïnspecteerd en gedemonteerd terwijl het echte verkeer via FTD ongewijzigd verloopt

Gerelateerde informatie

- Cisco Firepower NGFW
- Technische ondersteuning en documentatie – Cisco Systems