

Cluster Troubleshooter Firepower Threat Defense (FTD)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Cluster basiskennis](#)

[NGFW-architectuur](#)

[Cluster Capture](#)

[Cluster Control Link-berichten \(CCL\)](#)

[Cluster Control Point \(CCP\)-berichten](#)

[Mechanisme voor clustergezondheidscontrole \(HC\)](#)

[Cluster HC-storingsscenario's](#)

[Cluster-datacenterverbinding-instelling](#)

[Problemen oplossen](#)

[Cluster-problemen met datacenters](#)

[NAT/PAT gemeenschappelijke problemen](#)

[fragmentatieverwerking](#)

[ACI-problemen](#)

[Problemen met clusterbesturingsplane](#)

[Eenheid kan niet deelnemen aan het cluster](#)

[Data-poorts-kanaals interfacekaart](#)

[Cluster Stability Issues](#)

[Vereenvoudigde modus](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt het oplossen van een clusterinstelling beschreven in Firepower Next-generation firewall (NGFW). De meeste items die in dit document worden besproken, zijn ook volledig van toepassing op problemen met de adaptieve security applicatie (ASA).

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van deze onderwerpen (zie [Verwante informatie voor links](#)):

- Firepower platform architectuur

- Firepower Cluster configuratie en exploitatie
- Bekendheid met FTD en FXOS CLI
- NGFW/datalink
- NGFW/dataplaktracer
- Firepower eXtenable Operating System (FXOS)/datalevlak

Gebruikte componenten

- HW: Firepower 4125
- SW: 6.7.0 (Bouw 65) - gegevensvlak 9.15(1)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een gewalste (standaard) configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

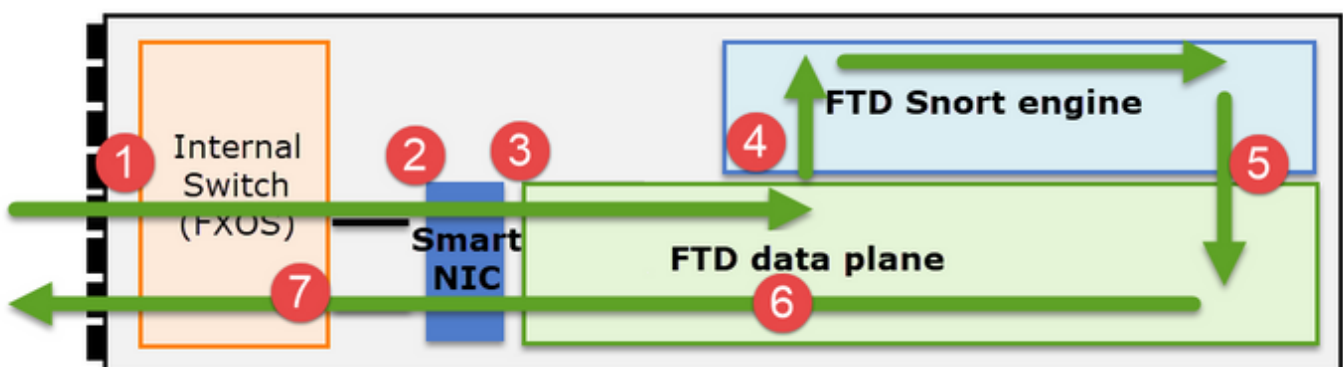
Het configuratie-gedeelte van een clustertoepassing wordt behandeld in de configuratiegids van FMC en FXOS:

- [Clustering voor de FireSIGHT Threat Defense](#)
- [Een cluster implementeren voor FirePOWER Threat Defense voor schaalbaarheid en hoge beschikbaarheid](#)

Cluster basiskennis

NGFW-architectuur

Het is belangrijk om te begrijpen hoe een Firepower 41xx of 93xx serie transitpakketten met handvatten toepast:



1. Een pakje gaat in op de ingangsiinterface en wordt behandeld door de switch van het chassis.
2. Het pakket gaat door de Smart NIC. Als de stroom is uitgeschakeld (HW acceleratie) dan wordt het pakket alleen afgehandeld door de Smart NIC en dan terug naar het netwerk gestuurd.
3. Als de verpakking niet wordt vrijgegeven, gaat het FTD-gegevensvliegtuig in, dat

voornamelijk L3/L4-controles verricht.

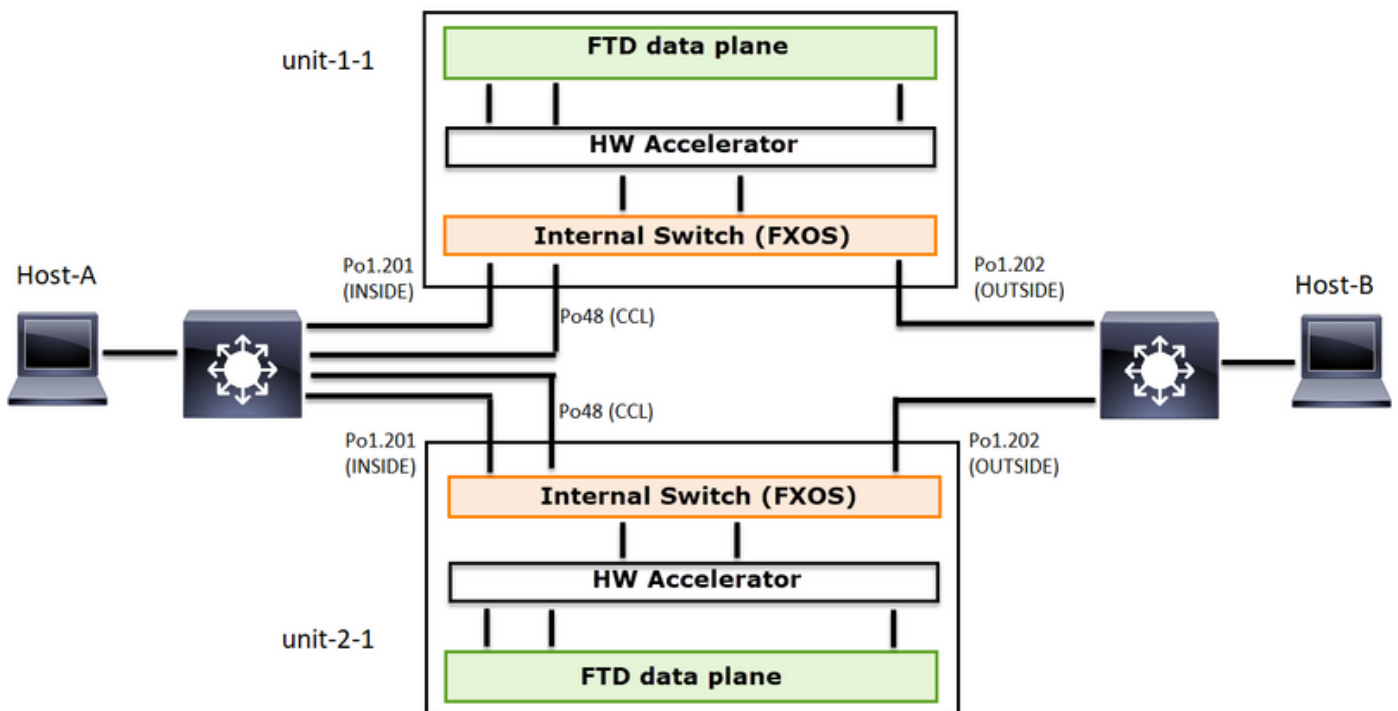
4. Indien het beleid vereist, wordt de verpakking gecontroleerd door de snortmotor (hoofdzakelijk L7-inspectie).
5. De motor van de SNA keert een vonnis (bijvoorbeeld, staat of blok) voor het pakje terug.
6. Het gegevensvlak daalt of voorwaarts het pakje op basis van de uitspraak van Snort.
7. Het pakket maakt gebruik van de switch van het onderstel.

Cluster Capture

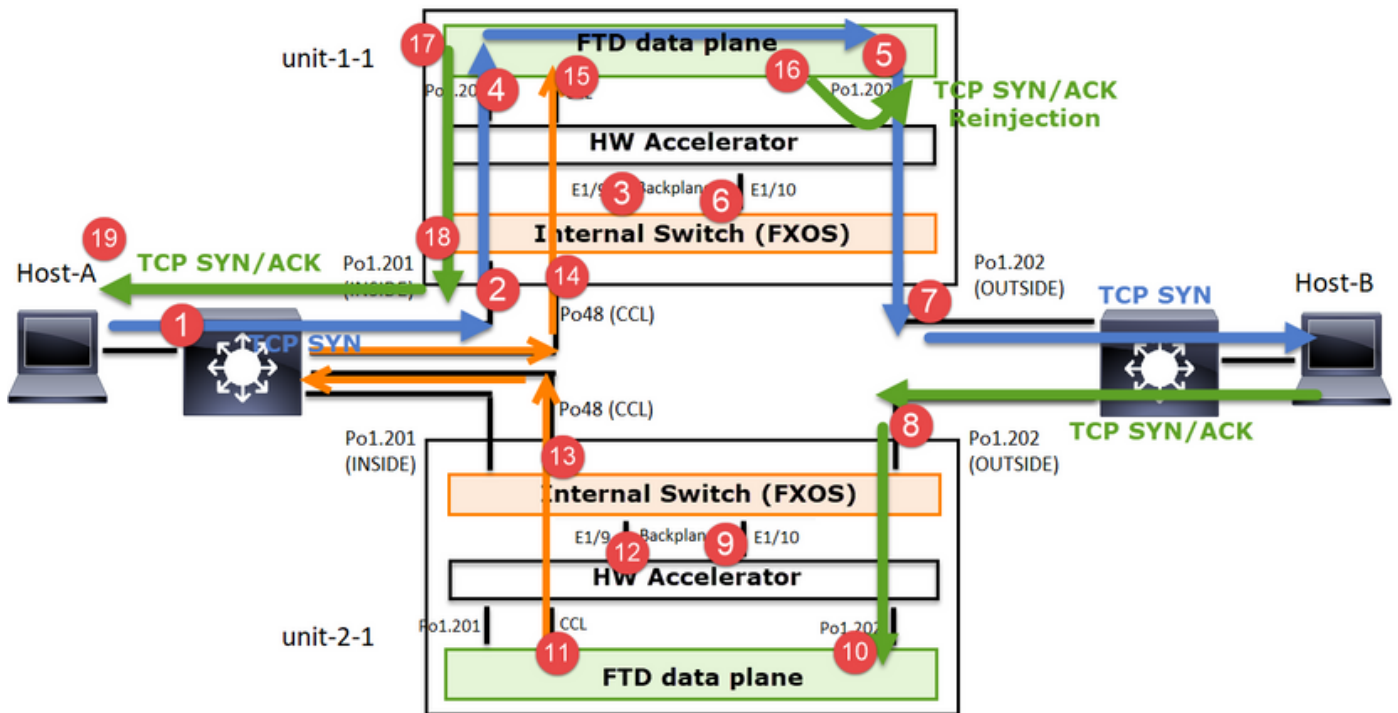
Vuurstroomapparaten voorzien in meerdere opnamepunten waarmee de doorvoerstromen zichtbaar kunnen worden. Wanneer u problemen oplossen en cluster inschakelen geeft u de belangrijkste uitdagingen aan:

- Het aantal opnames neemt toe naarmate het aantal eenheden in de cluster toeneemt
- U moet zich bewust zijn van de manier waarop het cluster een specifieke stroom verwerkt om het pakket door het cluster te kunnen volgen

In dit schema is een cluster met 2 eenheden te zien (bv. FP941xx/FP9300):



In het geval van een asymmetrische TCP verbinding vestiging ziet een TCP SYN/ACK-uitwisseling er zo uit:



Vooruitlopend verkeer

1. TCP SYN wordt verzonden van Host-A naar Host-B.
2. TCP SYN arriveert op het chassis (een van de leden van Po1).
3. TCP SYN wordt door een van de chassis backplane interfaces (bijv. E1/9, E1/10, enz.) naar het gegevensvlak verzonden.
4. TCP arriveert op de interface van het gegevensvliegtuig (Po1.201/INSIDE). In dit voorbeeld neemt unit 1-1 de eigendom van de stroom, doet de eerste sequentie Number (ISN) randomisatie en codeert de eigendom (koekje) informatie in Seq nummer
5. TCP SYN wordt verzonden vanuit Po1.202/OUTSIDE (interface met het gegevensvliegtuig).
6. TCP SYN arriveert op een van de chassis backplane interfaces (bijv. E1/9, E1/10, enz.).
7. TCP SYN wordt vanuit de fysieke interface van het chassis (een van de leden van Po1) naar Host-B verzonden.

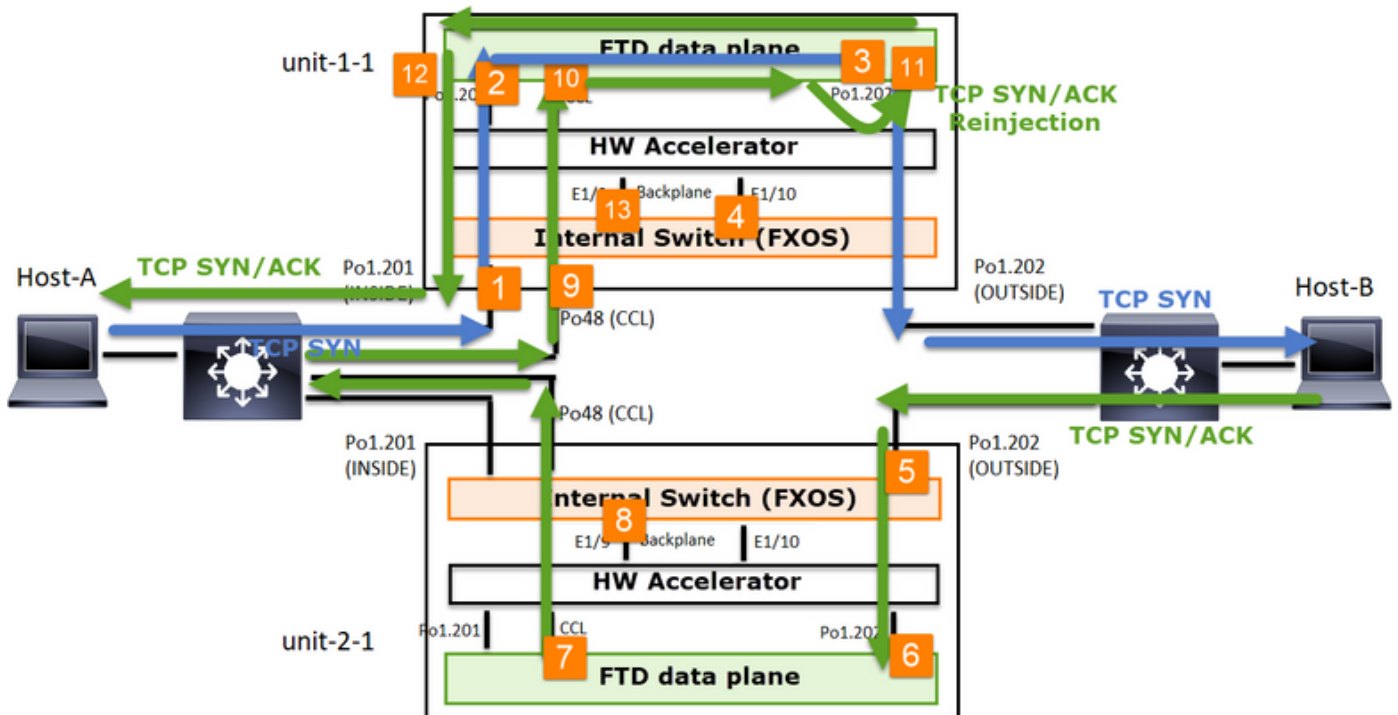
Terugkeerverkeer

8. TCP SYN/ACK wordt verzonden van Host-B en arriveert op unit-2-1 (een van de leden van Po1).
9. TCP SYN/ACK wordt door een van de chassis backplane interfaces (bijv. E1/9, E1/10, enz.) naar het gegevensvlak verzonden.
10. TCP SYN/ACK arriveert op de ingangsiinterface van het gegevensvliegtuig (Po1.202/OUTSIDE).
11. TCP SYN/ACK wordt vanuit Cluster Control Link (CCL) naar unit-1-1 verzonden. Standaard is ISN ingeschakeld. Dus vindt de expediteur de eigenaar info voor TCP SYN+ACKs zonder de betrokkenheid van de directeur. Voor andere pakketten of wanneer ISN wordt uitgeschakeld, wordt de regisseur gevraagd.
12. TCP SYN/ACK komt aan op een van de chassis backplane interfaces (bijv. E1/9, E1/10, enz.).
13. TCP SYN/ACK wordt vanuit de fysieke interface van het chassis (een van de leden van Po48) naar unit-1-1 verzonden.
14. TCP SYN/ACK arriveert op unit-1-1 (een van de leden van Po48).

15. TCP SYN/ACK wordt door één van de chassis backplane interfaces naar het gegevensvliegtuig CCL poort-kanaalinterface (name als cluster) doorgestuurd.
16. Het gegevensvliegtuig breekt het TCP SYN/ACK-pakket naar de dataverbinding Po1.202/BUITEN.
17. TCP SYN/ACK wordt verzonden vanuit Po1.201/INSIDE (data plane klokinterface) naar HOST-A.
18. TCP SYN/ACK overschrijdt een van de chassis backplane interfaces (bijv. E1/9, E1/10, enz.) en genereert een van de leden van Po1.
19. TCP SYN/ACK arriveert op Host-B.

Lees voor meer informatie over dit scenario de bijbehorende sectie in de **Cluster Connection Case Studies** van een vaste inrichting.

Gebaseerd op deze pakketuitwisseling, zijn alle mogelijke punten van de clustervangst:



Voor het voorwaartse verkeer (bijv. TCP SYN) neemt u de volgende informatie op:

1. De fysieke interface van het chassis (bv. Po1-leden). Deze opname is ingesteld in de Chassis Manager (CM) UI of de CM CLI.
2. Data plane ingress interface (bijv. Po1.201 INSIDE).
3. interface van het gegevensvlak (bv. Po1.202 BUITEN).
4. Chassis backplane interfaces. Op FP4100 zijn er 2 backplane interfaces. Voor FP9300 zijn er in totaal 6 (2 per module). Aangezien u niet weet in welke interface het pakket aankomt, moet u opname op alle interfaces mogelijk maken.

Voor het retourverkeer (bijvoorbeeld TCP/SYN/ACK) wordt de volgende informatie opgenomen:

5. De fysieke interface van het chassis (bv. Po1-leden). Deze opname is ingesteld in de Chassis Manager (CM) UI of de CM CLI.
6. Data plane ingress interface (bv. Po1.202 BUITEN).
7. Aangezien het pakket opnieuw wordt gericht, is het volgende opnamepunt het gegevensvliegtuig CCL.

8. Chassis backplane interfaces. Opnieuw moet u opname op beide interfaces inschakelen.
9. Eenheid-1-1 chassis CCL lid interfaces.
10. Data plane CCL-interface (naam als cluster).
11. Ingraving interface (Po1.202 BUITEN). Dit is het herinjecteerpakket van CCL naar gegevensvlak.
12. Data plane klokinterface (bv. Po1.201 INSIDE).
13. Chassis backplane interfaces.

Hoe de Cluster kan inschakelen

FXOS-opnamen

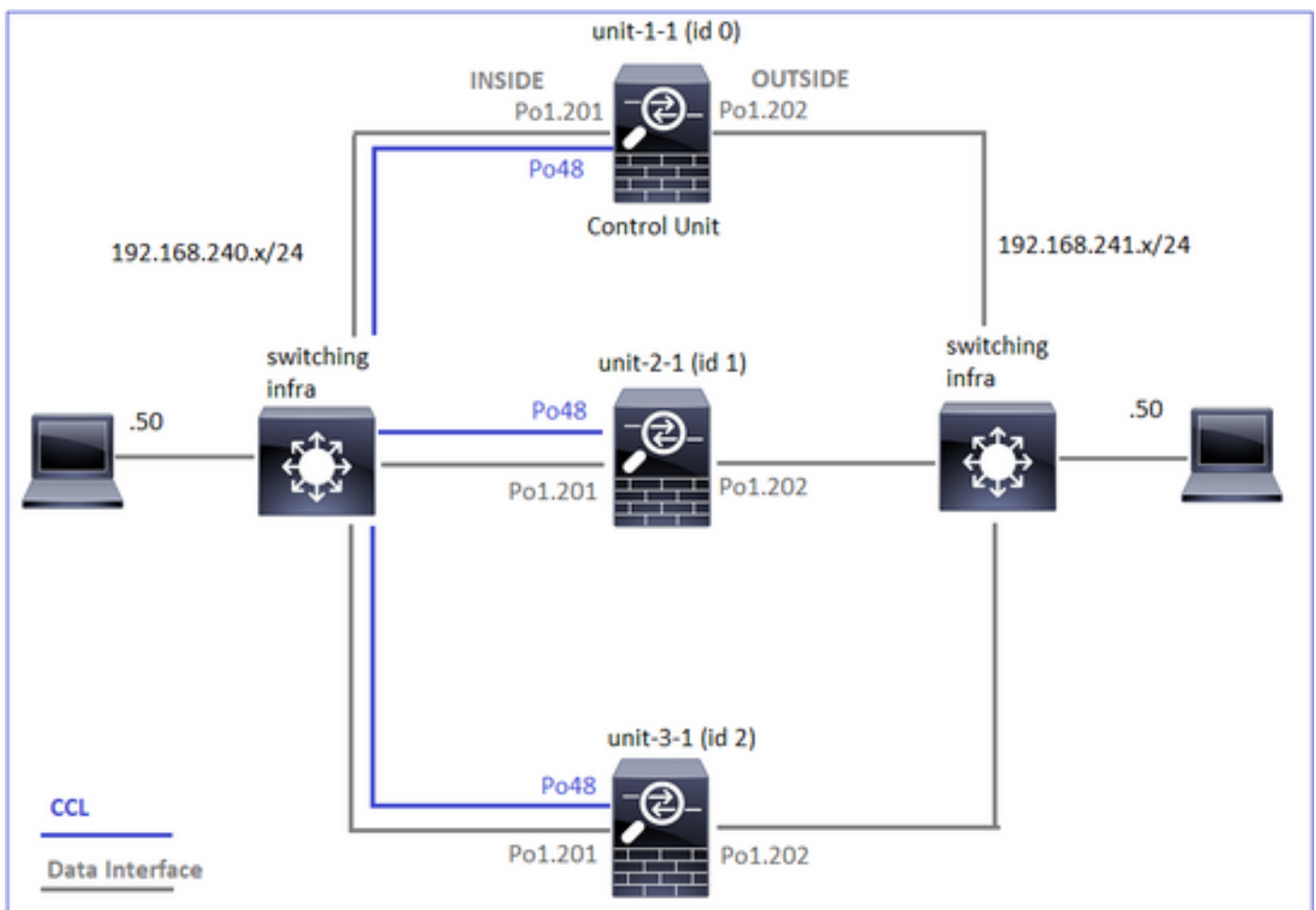
Dit proces wordt beschreven in de FXOS-configuratie: [Packet Capture](#)

Opmerking: FXOS-opnamen kunnen alleen vanuit het oogpunt van de interne switch in de richting van de ingang worden genomen.

Opname van datacenters

De aanbevolen manier om opname op alle clusterleden mogelijk te maken, is met de opdracht **clusterexpressie**.

Neem een 3-eenheid cluster:



Om te controleren of er actieve opnamen in alle clustereenheden zijn, gebruikt u deze opdracht:

```
firepower# cluster exec show capture
```

```
unit-1-1(LOCAL):*****
```

```
unit-2-1:*****
```

```
unit-3-1:*****
```

```
firepower#
```

Zo maakt u op Po1.201 (INSIDE) het mogelijk om een gegevensvliegtuig op alle eenheden op te nemen:

```
firepower# cluster exec capture CAPI interface INSIDE
```

Het is sterk aanbevolen om een opnamefilter te specificeren en voor het geval u veel verkeer verwacht om de opnamebuffer te verhogen:

```
firepower# cluster exec capture CAPI buffer 33554432 interface INSIDE match tcp host 192.168.240.50 host 192.168.241.50 eq 80
```

Verificatie

```
firepower# cluster exec show capture
```

```
unit-1-1(LOCAL):*****
```

```
capture CAPI type raw-data buffer 33554432 interface INSIDE [Capturing - 5140 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

```
unit-2-1:*****
```

```
capture CAPI type raw-data buffer 33554432 interface INSIDE [Capturing - 260 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

```
unit-3-1:*****
```

```
capture CAPI type raw-data buffer 33554432 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

U kunt als volgt de inhoud van alle opnamen bekijken (deze uitvoer kan erg lang zijn):

```
firepower# terminal pager 24
```

```
firepower# cluster exec show capture CAPI
```

```
unit-1-1(LOCAL):*****
```

```
21 packets captured
```

```
1: 11:33:09.879226 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: S
```

```
2225395909:2225395909(0) win 29200 <mss 1460,sackOK,timestamp 1110209649 0,nop,wscale 7>
```

```
2: 11:33:09.880401 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.45456: S
```

```
719653963:719653963(0) ack 2225395910 win 28960 <mss 1380,sackOK,timestamp 1120565119
```

```
1110209649,nop,wscale 7>
```

```
3: 11:33:09.880691 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: . ack 719653964
```

```
win 229 <nop,nop,timestamp 1110209650 1120565119>
```

```
4: 11:33:09.880783 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: P
```

```
2225395910:2225396054(144) ack 719653964 win 229 <nop,nop,timestamp 1110209650 1120565119>
```

```
unit-2-1:*****
```

```
0 packet captured
```

```
0 packet shown
```

```
unit-3-1:*****
```

```
0 packet captured
```

```
0 packet shown
```

Capture Traces

Als u wilt zien hoe de ingangspakketten door het gegevensvliegtuig op elke eenheid worden behandeld gebruik het **spoor** sleutelwoord. Dit volgt de eerste 50 ingangspakketten. U kunt maximaal 1000 ingangspakketten opvolgen. Merk op dat als u meerdere opnamen hebt die op een interface zijn toegepast, u slechts één pakket kunt overtrekken.

U kunt de eerste 1000 ingangspakketten op interface BUITEN op alle clustereenheden als volgt overtrekken:

```
firepower# cluster exec cap CAPO int OUTSIDE buff 33554432 trace trace-count 1000 match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

Wanneer u de rentestroom opneemt, moet u er zeker van zijn dat u de relevante pakketten op elke eenheid overtrekt. Het belangrijkste om niet te vergeten is dat een specifiek pakje #1 op unit-1-1 is, maar #2 op een andere eenheid, enz.

In dit voorbeeld kan u zien dat SYN/ACK pakje #2 op eenheid-2-1 is, maar pakje #1 op eenheid-3-1:

```
firepower# cluster exec show capture CAPO | include S.*ack
unit-1-1(LOCAL):*****
1: 12:58:31.117700 802.1Q vlan#202 PO 192.168.240.50.45468 > 192.168.241.50.80: S
441626016:441626016(0) win 29200 <mss 1380,sackOK,timestamp 1115330849 0,nop,wscale 7>
2: 12:58:31.118341 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45468: S
301658077:301658077(0) ack 441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319
1115330849,nop,wscale 7>

unit-2-1:*****

unit-3-1:*****
1: 12:58:31.111429 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45468: S
301658077:301658077(0) ack 441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319
1115330849,nop,wscale 7>
```

Zo slaat u pakje #2 (SYN/ACK) op de lokale eenheid op:

```
firepower# cluster exec show cap CAPO packet-number 2 trace
unit-1-1(LOCAL):*****

2: 12:58:31.118341 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45468: S
301658077:301658077(0) ack 441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319
1115330849,nop,wscale 7>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
...
```

Zo slaat u hetzelfde pakket (SYN/ACK) op de afstandsbediening op:

```
firepower# cluster exec unit unit-3-1 show cap CAPO packet-number 1 trace

1: 12:58:31.111429 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45468: S
301658077:301658077(0) ack 441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319
1115330849,nop,wscale 7>
Phase: 1
```


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

CCL-opname

U kunt opname op de CCL-link als volgt inschakelen (op alle eenheden):

```
firepower# cluster exec capture CCL interface cluster
unit-1-1(LOCAL):*****
unit-2-1:*****
unit-3-1:*****
```

Verbergen verbergen

Standaard wordt op een datalavigatie-interface een opname ingeschakeld die alle pakketten toont:

- Degenen die uit het fysieke netwerk komen
- Degenen die opnieuw van de CCL zijn verjaagd

Als u de herinjecteerde pakketten niet wilt zien, gebruikt u de optie **Verberg de huid opnieuw**. Dit kan handig zijn als u wilt controleren of een stroom asymmetrisch is:

```
firepower# cluster exec capture CAPI_RH reinject-hide interface INSIDE match tcp host
192.168.240.50 host 192.168.241.50 eq 80
```

Deze opname laat alleen zien wat de lokale eenheid daadwerkelijk ontvangt op de specifieke interface direct van het fysieke netwerk en niet van de andere clustereenheden.

ASP-druppels

Als u op een bepaalde stroom wilt controleren of er softwaredruppels bijkomen, kunt u de **asp-drop**-opname inschakelen. Als u niet weet op welke reden u zich moet concentreren, gebruik het sleutelwoord **allen**. Als u niet geïnteresseerd bent in de pakketlading, kunt u het trefwoord specificeren. Hiermee kunt u 20-30 keer meer pakketten opnemen:

```
firepower# cluster exec cap ASP type asp-drop all buffer 33554432 headers-only
unit-1-1(LOCAL):*****
unit-2-1:*****
unit-3-1:*****
```

Daarnaast kunt u de IP's specificeren die van belang zijn in de ASP-opname:

```
firepower# cluster exec cap ASP type asp-drop all buffer 33554432 headers-only match ip host
192.0.2.100 any
```

Een opname wissen

Om de buffer te verwijderen van elke opname die in alle clustereenheden draait. Dit stopt de opname niet, maar alleen de buffers:

```
firepower# cluster exec clear capture /all
unit-1-1(LOCAL):*****
unit-2-1:*****
unit-3-1:*****
```

Een opname stoppen

Er zijn 2 manieren om een actieve opname op alle clustereenheden te stoppen. Later kun je verder.

Way 1

```
firepower# cluster exec cap CAPI stop
unit-1-1(LOCAL):*****
unit-2-1:*****
unit-3-1:*****
```

Hervat

```
firepower# cluster exec no capture CAPI stop
unit-1-1(LOCAL):*****
unit-2-1:*****
unit-3-1:*****
```

Way 2

```
firepower# cluster exec no capture CAPI interface INSIDE
unit-1-1(LOCAL):*****
unit-2-1:*****
unit-3-1:*****
```

Hervat

```
firepower# cluster exec capture CAPI interface INSIDE
unit-1-1(LOCAL):*****
unit-2-1:*****
unit-3-1:*****
```

Verzamelen van een Capture

Er zijn meerdere manieren om een opname te exporteren.

Way 1 - Naar een externe server

Hiermee kunt u een opname van het gegevensvliegtuig naar een externe server uploaden (bijvoorbeeld TFTP). Merk op dat de opnamenamen automatisch worden gewijzigd om de broneenheid weer te geven:

```

firepower# cluster exec copy /pcap capture:CAPI tftp://192.168.240.55/CAPI.pcap
unit-1-1(LOCAL):*****
Source capture name [CAPI]?
Address or name of remote host [192.168.240.55]?
Destination filename [CAPI.pcap]?
INFO: Destination filename is changed to unit-1-1_CAPI.pcap !!!!!!!
81 packets copied in 0.40 secs

```

```

unit-2-1:*****
INFO: Destination filename is changed to unit-2-1_CAPI.pcap !

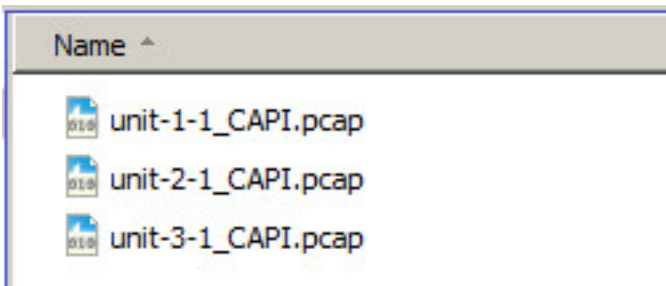
```

```

unit-3-1:*****
INFO: Destination filename is changed to unit-3-1_CAPI.pcap !

```

De geüploade pendop bestanden:



Way 2 - Opname van de VCC

Deze manier is alleen van toepassing op FTD. Eerst kopieert u de opname naar de FTD:

```

firepower# cluster exec copy /pcap capture:CAPI disk0:CAPI.pcap
unit-1-1(LOCAL):*****
Source capture name [CAPI]?
Destination filename [CAPI.pcap]?
!!!!!!
62 packets copied in 0.0 secs

```

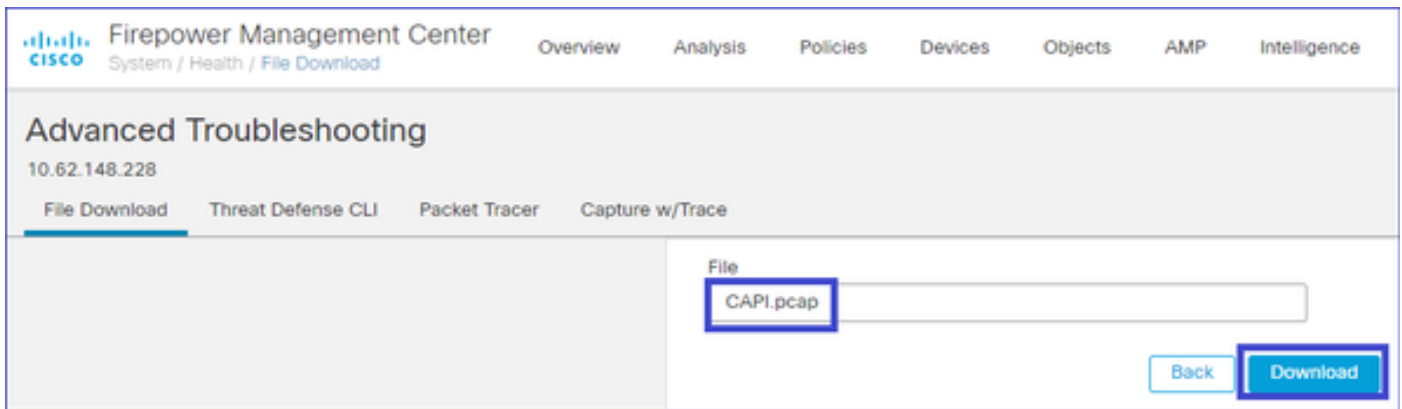
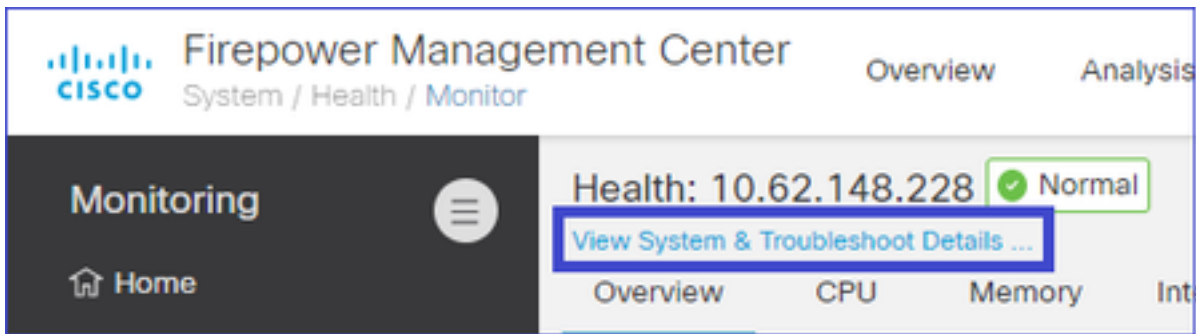
Van expert mode kopieert het bestand van /mnt/disk0/ naar /ngfw/var/common/ folder:

```

> expert
admin@firepower:~$ cd /mnt/disk0
admin@firepower:/mnt/disk0$ sudo cp CAPI.pcap /ngfw/var/common

```

Ten slotte navigeer op FMC naar **System > Health > Monitor** sectie. Selecteer **Details voor systeem- en probleemoplossing bekijken > Geavanceerde probleemoplossing** en haal het opnamebestand:



Een opname verwijderen

U verwijdert een opname uit alle clustereenheden door deze opdracht te gebruiken:

```
firepower# cluster exec no capture CAPI
unit-1-1(LOCAL):*****
unit-2-1:*****
unit-3-1:*****
```

Offset-stromen

Bij FP41xx/FP9300 kunnen stromen worden geofferd op HW-versneller, hetzij statisch (bv. Fastpath-regels) of dynamisch. Controleer dit document voor meer informatie over flow-offload:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212321-clarify-the-firepower-threat-defense-acc.html#anc22>

Als een stroom wordt uitgeladen, gaan slechts een paar pakketten door het FTD gegevensvliegtuig. De rest wordt verwerkt door de HW-versneller (Smart NIC).

Vanuit een oogpunt van opname betekent dit dat als u alleen het FTD-gegevensniveau activeert, u niet alle pakketten ziet die door het apparaat gaan. In dit geval moet u ook FXOS chassis-niveau opnamen inschakelen.

Cluster Control Link-berichten (CCL)

Als je een opname op de CCL neemt, merk je dat de clustereenheden verschillende soorten berichten uitwisselen. De belangrijkste zijn:

Protocol	Beschrijving
UDP 49495	Cluster hartslagen (keepalives)

- L3-uitzending (255.255.255.255)
- Deze pakketten worden door elke clustereenheid verzonden bij 1/3 van de waarde van de Hold Time Time (Glasertijd) voor de gezondheidscontrole.
- Merk op dat niet alle UDP 49495-pakketten die in de opname worden gezien, hartslagen zijn

UDP 4193

Cluster Control Protocol-datacenter-berichten

- Unicast
- Deze pakketten bevatten informatie (metagegevens) over de stroomeigenaar, regisseur, back-upeigenaar, enz. Voorbeelden zijn:
 - Er wordt een 'cluster add'-bericht van de eigenaar naar de regisseur gestuurd wanneer er een nieuwe stroom wordt aangemaakt
 - Er wordt een "clusterwissel"-bericht van de eigenaar naar de regisseur verstuurd wanneer een stroom wordt beëindigd

Gegevenspakketten

Gegevenspakketten die tot de verschillende verkeersstromen behoren die de cluster doorkruisen

Cluster hartslag

314	23.954349	192.222.1.1	255.255.255.255	UDP	205 49495 → 49495 Len=163
315	23.954364	192.222.1.1	255.255.255.255	UDP	205 49495 → 49495 Len=163
368	28.950976	192.222.1.1	255.255.255.255	UDP	205 49495 → 49495 Len=163
369	28.950992	192.222.1.1	255.255.255.255	UDP	205 49495 → 49495 Len=163

```

> Frame 314: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Ethernet II, Src: Dell_00:01:8f (00:15:c5:00:01:8f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.222.1.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 49495, Dst Port: 49495
# Data (163 bytes)
Data: 010100fe00a30000000000000000000000000000000000000001e008b0000000747524f5550310000...
0000 ff ff ff ff ff ff 00 15 c5 00 01 8f 08 00 45 00 .....E.
0010 00 bf a8 1f 00 00 ff 11 51 2f c0 de 01 01 ff ff .....Q/.....
0020 ff ff c1 57 c1 57 00 ab 79 01 01 01 00 fe 00 a3 ...-W-W- y.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e .....
0040 00 8b 00 00 00 07 47 52 4f 55 50 31 00 00 01 00 .....GR
0050 09 75 6e 69 74 2d 31 2d 31 00 00 02 00 09 75 6e unit-1-
0060 69 74 2d 31 2d 31 00 00 03 00 01 00 00 04 00 01 it-1-1-
0070 00 00 05 00 04 00 00 00 04 00 06 00 04 00 00 00 ...:
0080 09 00 07 00 04 00 00 3a 98 00 08 00 0c 00 00 00 .....
0090 00 c0 de 01 01 ff ff 00 00 00 09 00 02 01 1b 00 .....
00a0 0a 00 04 00 00 4e 9f 00 0b 00 0a 00 00 00 01 00 .....N.....
00b0 00 01 00 01 00 00 0c 00 08 00 00 00 00 00 00 00 .....
00c0 01 00 0d 00 08 00 00 00 00 00 00 00 00 00 .....

```

Heartbeat
sequence number

Cluster Control Point (CCP)-berichten

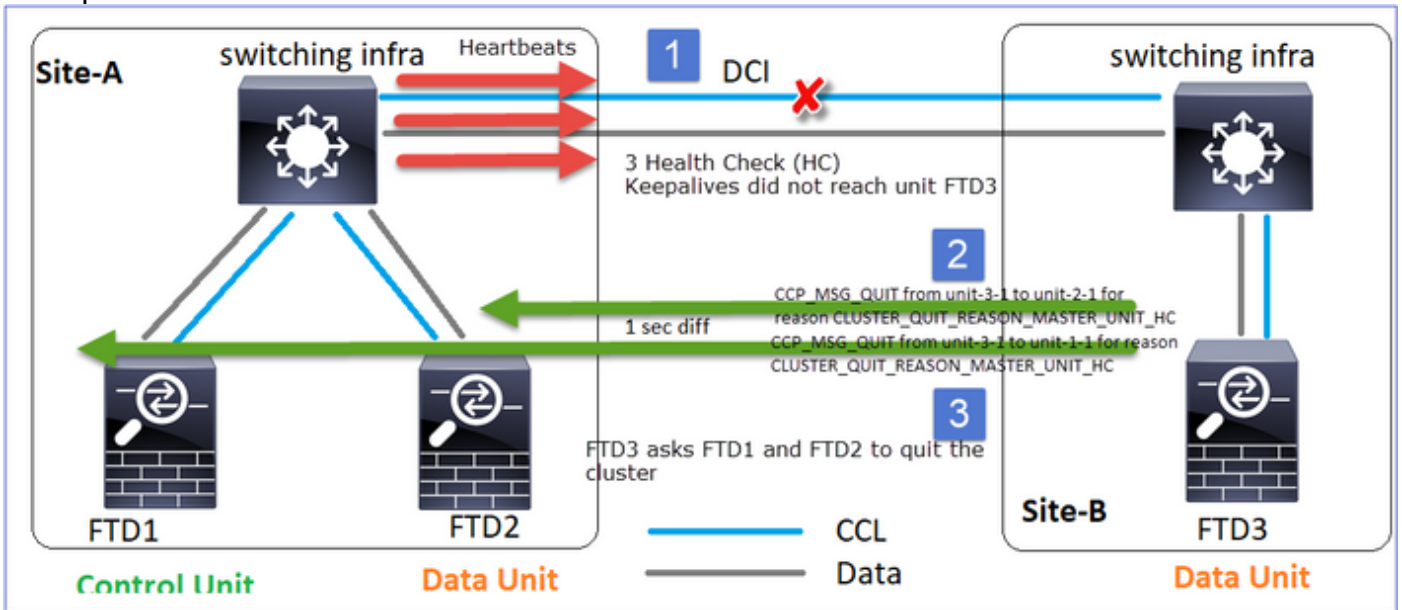
Naast de hartslaan-berichten is er een aantal clusterbeheerboodschappen die in specifieke scenario's via de CCL worden uitgewisseld. Sommige van deze programma's zijn éénmails, andere uitzendingen.

CLUSTER_QUIT_REASON_MASTER_UNIT_HC

Wanneer een unit 3 opeenvolgende hartslaan-berichten uit het controleknop verliest, genereert het een CLUSTER_QUIT_REASON_MASTER_UNIT_HC-bericht via de CCL. Dit bericht:

- Is een eenling
- Het wordt naar elk apparaat verzonden met een interval van 1 seconden
- Wanneer een eenheid dit bericht ontvangt, stopt het cluster (UITGESCHAKELD) en voegt het

opnieuw toe

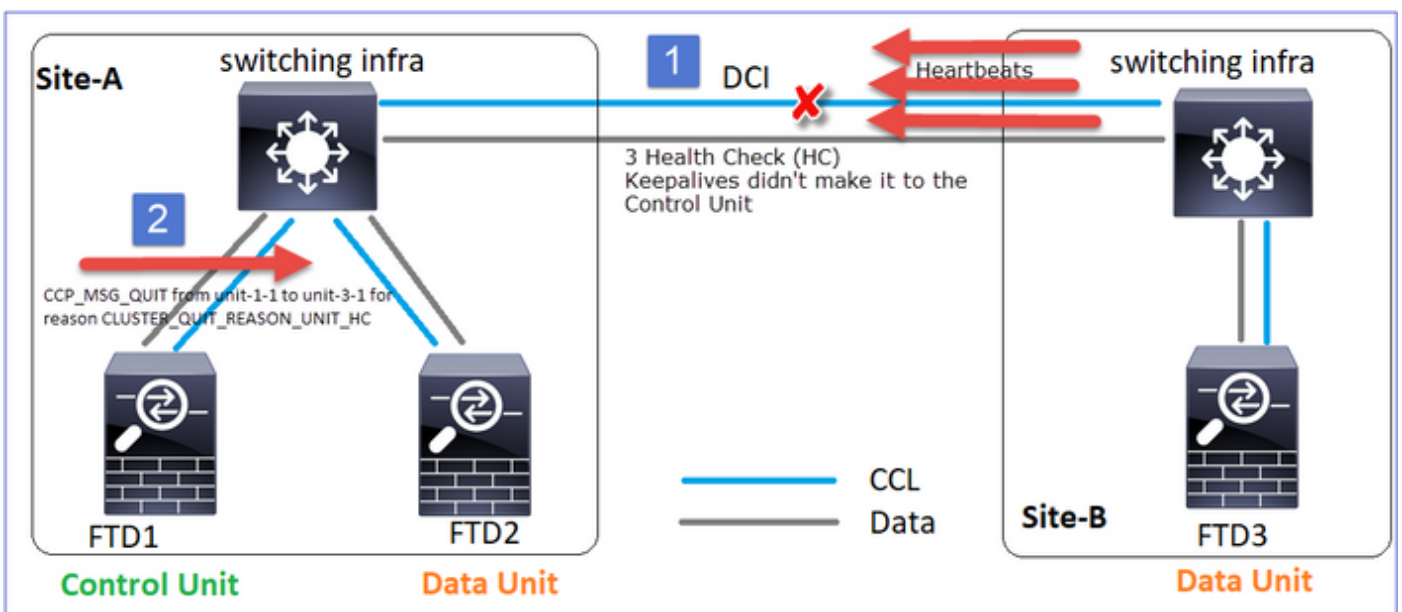


V. Wat is het doel van CLUSTER_QUIT_REASON_MASTER_UNIT_HC?

A. Vanuit het gezichtspunt van eenheid-3-1 (Site-B) verliest het de verbinding met zowel eenheid-1-1 als eenheid-2-1 van site A, zodat het deze zo snel mogelijk anders uit zijn lijst van leden moet verwijderen, kan het pakketverlies ontstaan als eenheid-2-1 nog in zijn lijst van leden staat en eenheid-2-1 een directeur van een verbinding is, en er wordt een query naar unit-2-1 uitgevoerd.

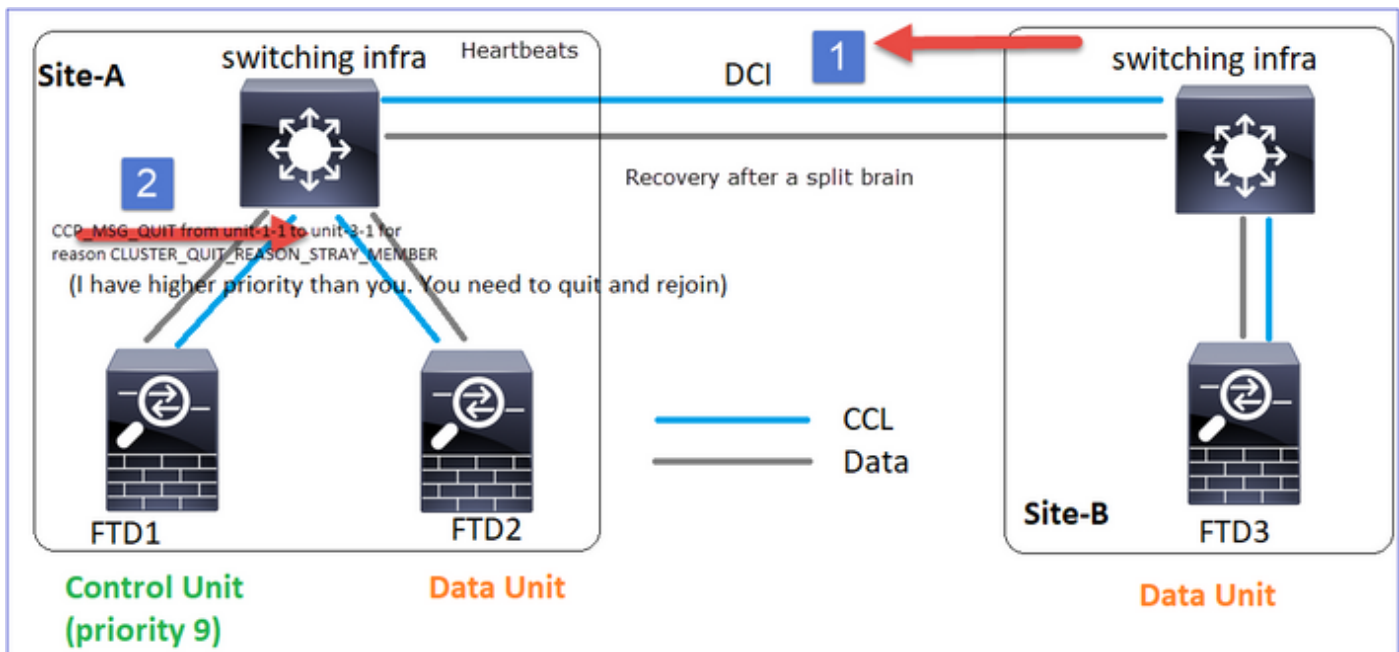
CLUSTER_QUIT_REASON_UNIT_HC

Wanneer het controleknooppunt 3 opeenvolgende hartslagen uit een gegevensknooppunt verliest, stuurt het CLUSTER_QUIT_REASON_UNIT_HC-bericht via de CCL. Deze boodschap is eenrichtig.



CLUSTER_QUIT_REASON_STRAY_LID

Wanneer een split-partitie zich herverbint met een peer partitie, wordt het nieuwe gegevensknooppunt door de dominante controle-eenheid behandeld als een gewoon lid en ontvangt het een CCP-melding met de reden van CLUSTER_QUIT_REASON_STRAY_LID.



CLUSTER_QUIT_LID_DROPOUT

Een uitzendbericht dat door een gegevensknooppunt gegenereerd wordt en als uitzending verzonden wordt. Zodra een eenheid dit bericht ontvangt, gaat deze naar de UITGESCHAKELDE status. Bovendien gaat automatisch opnieuw samenvoegen niet van start:

```
firepower# show cluster info trace | include DROPOUT
```

```
Nov 04 00:22:54.699 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-1-1 for reason CLUSTER_QUIT_MEMBER_DROPOUT
```

```
Nov 04 00:22:53.699 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-2-1 for reason CLUSTER_QUIT_MEMBER_DROPOUT
```

De clustergeschiedenis toont:

```
MASTER      DISABLED      Received control message DISABLE (member dropout announcement)
```

Mechanisme voor clustergezondheidscontrole (HC)

Hoofdpunten

- Elke clustereenheid stuurt een hartslag elke 1/3 van de waarde van de wachttijd voor de gezondheidscontrole naar alle andere eenheden (uitzending 255.255.255.255) en gebruikt UDP-poort 49495 als transport over de CCL.
- Elke clustereenheid volgt onafhankelijk elke andere eenheid met een pols-timer en een pols-telling.
- Als een clustereenheid geen pakje (hartslag of gegevenspakje) ontvangt van een cluster peer-eenheid binnen een hartslaginterval, verhoogt dit de waarde van de poll.
- Wanneer de pols-telwaarde voor een cluster peer-unit 3 wordt, wordt de peer afgezwakt.
- Wanneer een hartslag wordt ontvangen, wordt het sequentienummer gecontroleerd en als het diff met de eerder ontvangen hartslag anders is dan 1, wordt de hartdruppelteller dienovereenkomstig verhoogd.
- Als de pols teller voor een cluster peer anders is dan 0 en een pakket door de peer wordt ontvangen wordt de teller teruggezet op 0 waarde.

Gebruik deze opdracht om de gezondheidscentra van het cluster te controleren:

```
firepower# show cluster info health details
```

Unit (ID)	Heartbeat count	Heartbeat drops	Average gap (ms)	Maximum slip (ms)	Poll count
unit-2-1 (1)	650	0	4999	1	0
unit-3-1 (2)	650	0	4999	1	0

Beschrijving van de hoofdkolommen

kolom	Beschrijving
Eenheid (ID)	De ID van de externe clusterpeer
hartslag	Het aantal hartslagen dat van de afstandsbediening via de CCL wordt ontvangen
druppels in de hartslag	Het aantal gemiste hartslagen. Deze teller wordt berekend op basis van het ontvangen aantal hartslagen
Gemiddelde kloof	Het gemiddelde tijdsinterval van de ontvangen hartslagen
stembiljet	Wanneer deze teller 3 wordt, wordt de eenheid uit het cluster verwijderd. Het poll query interval is hetzelfde als het hartslag interval maar werkt onafhankelijk

Gebruik deze opdracht om de tellers terug te stellen:

```
firepower# clear cluster info health details
```

Q. Hoe de hartslaan-frequentie wordt geverifieerd

A. Controleer de gemiddelde leemwaarde:

```
firepower# show cluster info health details
```

Unit (ID)	Heartbeat count	Heartbeat drops	Average gap (ms)	Maximum slip (ms)	Poll count
unit-2-1 (1)	3036	0	999	1	0

Q. Hoe kunt u de wachttijd van het cluster op FTD wijzigen?

A. Gebruik FlexConfig

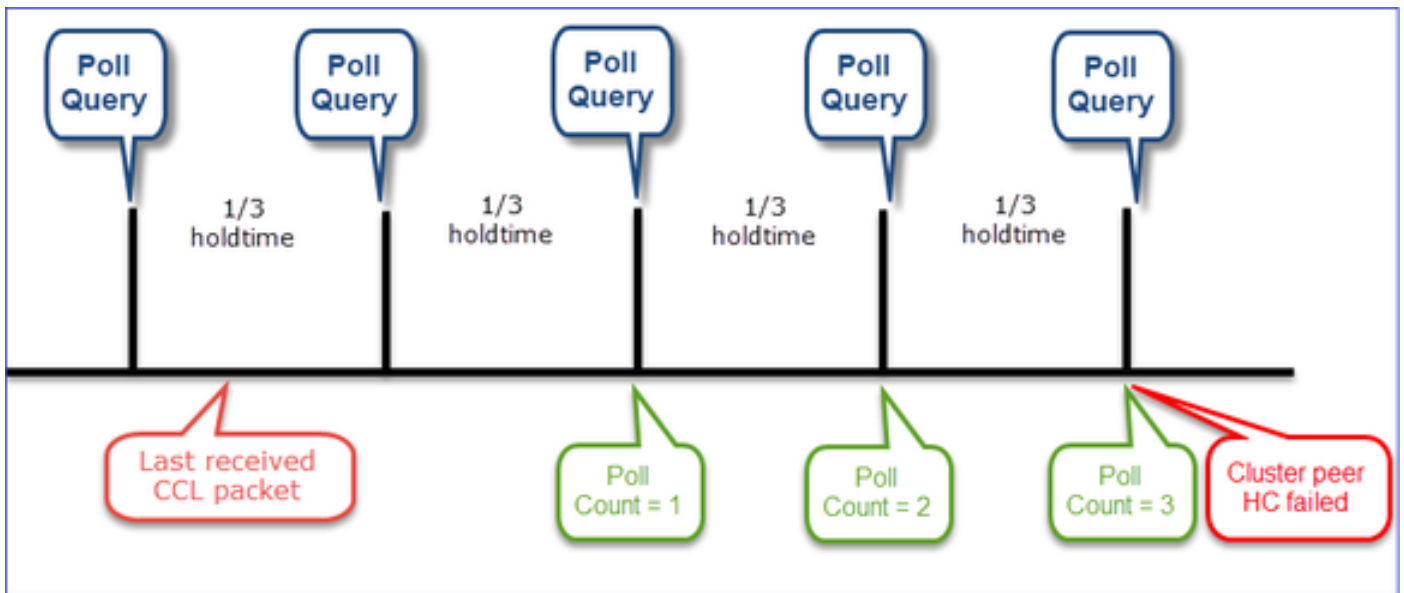
Wie wordt de controleknoop na een gespleten brein?

A. De eenheid met de hoogste prioriteit (laagste aantal):

```
firepower# show run cluster | include priority  
priority 9
```

Controleer HC-storingsscenario 1 voor meer details.

Visualisatie van het cluster HC-mechanisme



Indicatieve timers: De min en max zijn afhankelijk van de laatst ontvangen CCL-pakketaankomst

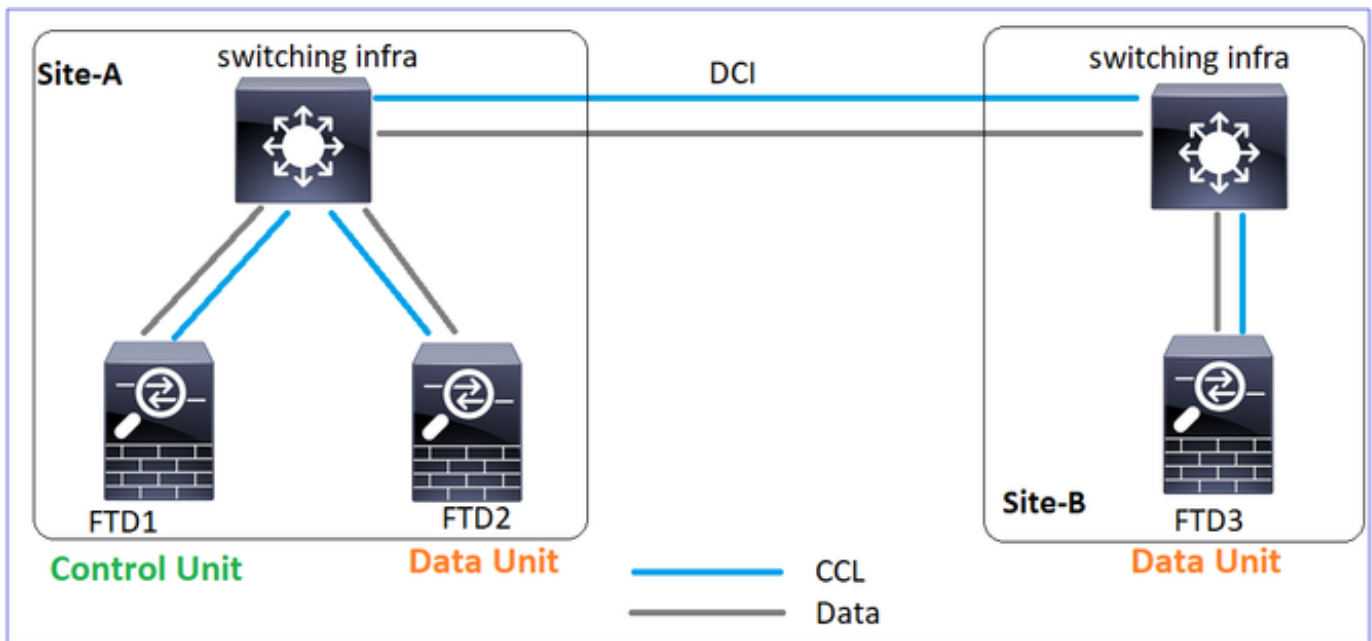
Tijd vasthouden	Poll query check (frequentie)	Min. detectietijd	Max. detectietijd
3 seconden (standaard)	~1 sec	~3,01 sec	~3,99 seconden
4 seconden	~1,33 seconden	~4,01 sec	~5,32 seconden
5 seconden	~1,66 seconden	~5,01 sec	~6,65 seconden
6 seconden	~2 seconden	~6,01 sec	~7,99 sec
7 seconden	~2,33 seconden	~7,01 sec	~9,32 seconden
8 seconden	~2,66 seconden	~8,01 sec	~10,65 seconden

Cluster HC-storingsscenario's

De doelstellingen van deze paragraaf zijn het aantonen van:

- Verschillende scenario's voor HC-falen
- Hoe de verschillende logbestanden en opdrachtuitgangen gecorreleerd kunnen worden

Topologie



Cluster-configuratie

Eenheid-1-1

```
cluster group GROUP1
key *****
local-unit unit-1-1
cluster-interface Port-channel48
ip 192.222.1.1 255.255.0.0
priority 9
health-check holdtime 3
health-check data-interface
auto-rejoin 3 5 2
health-check cluster-interface
auto-rejoin unlimited 5 1
health-check system auto-rejoin
3 5 2
health-check monitor-interface
debounce-time 500
site-id 1
enable
```

Eenheid-2-1

```
cluster group GROUP1
key *****
local-unit unit-2-1
cluster-interface Port-channel48
ip 192.222.2.1 255.255.0.0
priority 17
health-check holdtime 3
health-check data-interface
auto-rejoin 3 5 2
health-check cluster-interface
auto-rejoin unlimited 5 1
health-check system auto-rejoin
3 5 2
health-check monitor-interface
debounce-time 500
site-id 1
enable
```

Eenheid-3-1

```
cluster group GROUP1
key *****
local-unit unit-3-1
cluster-interface Port-channel48
ip 192.222.3.1 255.255.0.0
priority 25
health-check holdtime 3
health-check data-interface
auto-rejoin 3 5 2
health-check cluster-interface
auto-rejoin unlimited 5 1
health-check system auto-rejoin
3 5 2
health-check monitor-interface
debounce-time 500
site-id 2
enable
```

Cluster status

Eenheid-1-1

```
firepower# show cluster info
Cluster GROUP1: On
Interface mode: spanned
This is "unit-1-1" in state
MASTER
ID          : 0
Site ID     : 1
Version     : 9.12(2)33
Serial No.: FCH22247LNK
CCL IP      : 192.222.1.1
CCL MAC     : 0015.c500.018f
Last join   : 20:25:36 UTC
Nov 1 2020
Last leave: 20:25:28 UTC
```

Eenheid-2-1

```
firepower# show cluster info
Cluster GROUP1: On
Interface mode: spanned
This is "unit-2-1" in state
SLAVE
ID          : 2
Site ID     : 1
Version     : 9.12(2)33
Serial No.: FCH23157Y9N
CCL IP      : 192.222.2.1
CCL MAC     : 0015.c500.028f
Last join   : 20:44:46 UTC
Nov 1 2020
Last leave: 20:44:38 UTC
```

Eenheid-3-1

```
firepower# show cluster info
Cluster GROUP1: On
Interface mode: spanned
This is "unit-3-1" in state
SLAVE
ID          : 1
Site ID     : 2
Version     : 9.12(2)33
Serial No.: FCH22247MK
CCL IP      : 192.222.3.1
CCL MAC     : 0015.c500.018f
Last join   : 20:58:45 UTC
Nov 1 2020
Last leave: 20:58:37 UTC
```

Nov 1 2020

Other members in the cluster:

Unit "unit-3-1" in state SLAVE

ID : 1
Site ID : 2
Version : 9.12(2)33
Serial No.: FCH22247MKJ
CCL IP : 192.222.3.1
CCL MAC : 0015.c500.038f
Last join : 20:58:45 UTC

Nov 1 2020

Last leave: 20:58:37 UTC

Nov 1 2020

Unit "unit-2-1" in state SLAVE

ID : 2
Site ID : 1
Version : 9.12(2)33
Serial No.: FCH23157Y9N
CCL IP : 192.222.2.1
CCL MAC : 0015.c500.028f
Last join : 20:44:45 UTC

Nov 1 2020

Last leave: 20:44:38 UTC

Nov 1 2020

Nov 1 2020

Other members in the cluster:

Unit "unit-1-1" in state MASTER

ID : 0
Site ID : 1
Version : 9.12(2)33
Serial No.: FCH22247LNK
CCL IP : 192.222.1.1
CCL MAC : 0015.c500.018f
Last join : 20:25:36 UTC

Nov 1 2020

Last leave: 20:25:28 UTC

Nov 1 2020

Unit "unit-3-1" in state SLAVE

ID : 1
Site ID : 2
Version : 9.12(2)33
Serial No.: FCH22247MKJ
CCL IP : 192.222.3.1
CCL MAC : 0015.c500.038f
Last join : 20:58:45 UTC

Nov 1 2020

Last leave: 20:58:37 UTC

Nov 1 2020

Nov 1 2020

Other members in the cluster:

Unit "unit-1-1" in state MASTER

ID : 0
Site ID : 1
Version : 9.12(2)33
Serial No.: FCH22247LNK
CCL IP : 192.222.1.1
CCL MAC : 0015.c500.018f
Last join : 20:25:36 UTC

Nov 1 2020

Last leave: 20:25:28 UTC

Nov 1 2020

Unit "unit-2-1" in state SLAVE

ID : 2
Site ID : 1
Version : 9.12(2)33
Serial No.: FCH23157Y9N
CCL IP : 192.222.2.1
CCL MAC : 0015.c500.028f
Last join : 20:44:45 UTC

Nov 1 2020

Last leave: 20:44:38 UTC

Nov 1 2020

Scenario 1

CCL-communicatieverlies voor ~4+ sec in beide richtingen

Voor de storing

FTD1
Site-A
Control-knooppunt

Ftd2
Site-A
Gegevensknooppunt

FTD3
Site-B
Gegevensknooppunt

Na herstel (geen wijzigingen in de eenheidsrollen)

FTD1
Site-A
Control-knooppunt

Ftd2
Site-A
Gegevensknooppunt

FTD3
Site-B
Gegevensknooppunt

Analyse

De storing (CCL-communicatie is verloren)

The image shows three terminal screenshots from a Firepower device. The first screenshot shows 'unit-1-1 Control Unit' with commands: 'clear cluster info trace' and 'clear cap /'. The second screenshot shows 'unit-2-1 Data Unit' with a command: 'Asking slave unit unit-3-1 to quit because it failed unit health-check.'. The third screenshot shows 'unit-3-1 Data Unit' with a message: 'Cluster unit unit-3-1 transitioned from SLAVE to MASTER'.

Het datacommunicatiebericht op unit-3-1:

```
firepower#
WARNING: dynamic routing is not supported on management interface when cluster interface-mode is 'spanned'.
If dynamic routing is configured on any management interface, please remove it.
```

```
Cluster unit unit-3-1 transitioned from SLAVE to MASTER
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled.
To recover either enable clustering or remove cluster group configuration.
```

Enheid-1-1 clustersporenstammen:

```
firepower# show cluster info trace | include unit-3-1
Nov 02 09:38:14.239 [INFO]Notify chassis de-bundle port for blade unit-3-1, stack
0x000055a8918307fb 0x000055a8917fc6e8 0x000055a8917f79b5
Nov 02 09:38:14.239 [INFO]FTD - CD proxy received state notification (DISABLED) from unit unit-
3-1
Nov 02 09:38:14.239 [DEBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for
reason CLUSTER_QUIT_MEMBER_DROPOUT
Nov 02 09:38:14.239 [INFO]Notify chassis de-bundle port for blade unit-3-1, stack
0x000055a8917eb596 0x000055a8917f4838 0x000055a891abef9d
Nov 02 09:38:14.239 [DEBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for
reason CLUSTER_QUIT_REASON_UNIT_HC
Nov 02 09:38:14.239 [CRIT]Received heartbeat event 'slave heartbeat failure' for member unit-3-1
(ID: 1).
```

brein splitsen

Enheid-1-1

Enheid-2-1

Enheid-3-1

```
firepower# show cluster info
Cluster GROUP1: On
Interface mode: spanned
This is "unit-1-1" in state
```

```
firepower# show cluster info
Cluster GROUP1: On
Interface mode: spanned
This is "unit-2-1" in state
```

```
firepower# show cluster info
Cluster GROUP1: On
Interface mode: spanned
This is "unit-3-1" in state
```

MASTER

```

ID          : 0
Site ID     : 1
Version     : 9.12(2)33
Serial No.: FCH22247LNK
CCL IP      : 192.222.1.1
CCL MAC     :
0015.c500.018f
  Last join : 20:25:36 UTC
Nov 1 2020
  Last leave: 20:25:28 UTC
Nov 1 2020
Other members in the cluster:
  Unit "unit-2-1" in state

```

SLAVE

```

ID          : 2
Site ID     : 1
Version     : 9.12(2)33
Serial No.: FCH23157Y9N
CCL IP      : 192.222.2.1
CCL MAC     :
0015.c500.028f
  Last join : 20:44:45 UTC
Nov 1 2020
  Last leave: 20:44:38 UTC
Nov 1 2020

```

SLAVE

```

ID          : 2
Site ID     : 1
Version     : 9.12(2)33
Serial No.: FCH23157Y9N
CCL IP      : 192.222.2.1
CCL MAC     :
0015.c500.028f
  Last join : 20:44:46 UTC
Nov 1 2020
  Last leave: 20:44:38 UTC
Nov 1 2020
Other members in the cluster:
  Unit "unit-1-1" in state

```

MASTER

```

ID          : 0
Site ID     : 1
Version     : 9.12(2)33
Serial No.: FCH22247LNK
CCL IP      : 192.222.1.1
CCL MAC     :
0015.c500.018f
  Last join : 20:25:36 UTC
Nov 1 2020
  Last leave: 20:25:28 UTC
Nov 1 2020

```

MASTER

```

ID          : 1
Site ID     : 2
Version     : 9.12(2)33
Serial No.: FCH22247MKJ
CCL IP      : 192.222.3.1
CCL MAC     :
0015.c500.038f
  Last join : 09:34:02 UTC
Nov 2 2020
  Last leave: 09:33:54 UTC
Nov 2 2020
Other members in the cluster:
  There is no other unit in the
cluster

```

Cluster historie**Eenheid-1-1**

Geen gebeurtenissen

Eenheid-2-1

Geen gebeurtenissen

Eenheid-3-1

09:38:16 UTC Nov 2 2020

SLAVE

```

MASTER_POST_CONFIG      Master
relinquished role

```

09:38:17 UTC Nov 2 2020

MASTER_POST_CONFIG

```

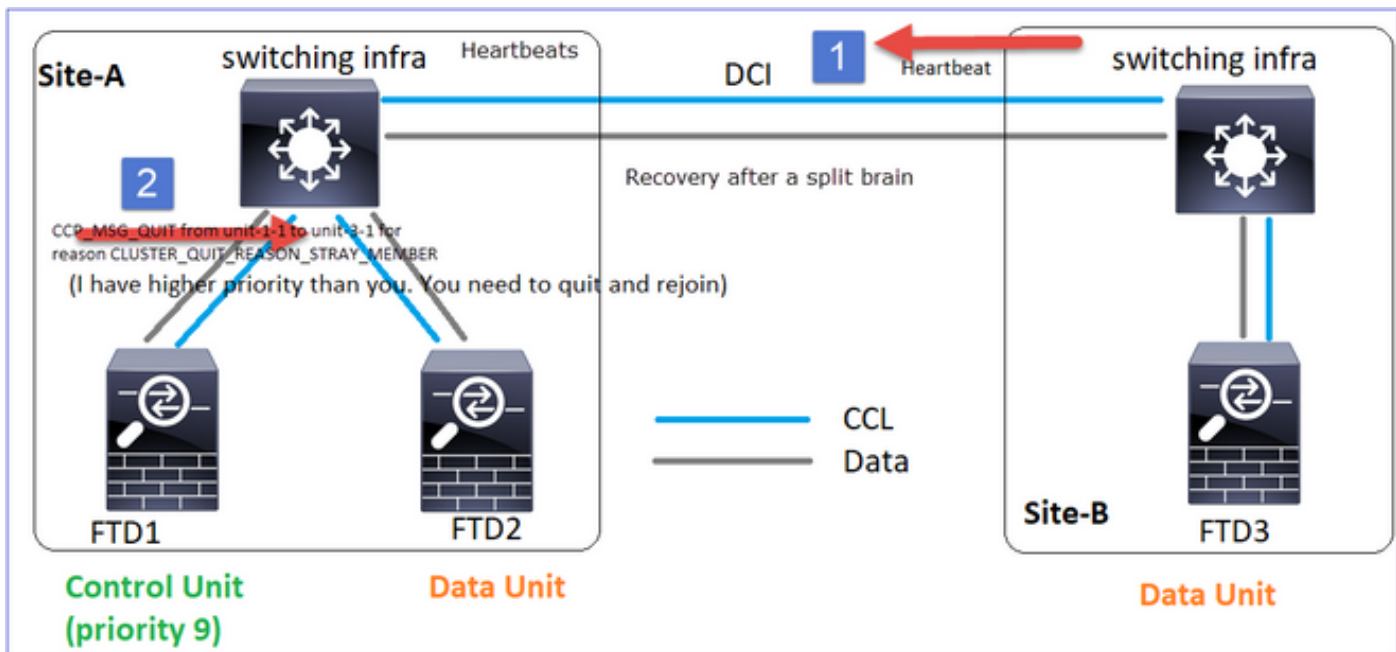
MASTER                      Master post
config done and waiting for ntfy

```

Herstel van CCL-communicatie

Unit-1-1 detecteert het huidige controleknooppunt en aangezien unit-1-1 hogere prioriteit heeft wordt verzonden naar unit-3-1 a CLUSTER_QUIT_REASON_STRAY_LID om een nieuw verkiezingsproces te starten. Aan het eind, unit-3-1 sluit zich opnieuw aan als een gegevensknooppunt.

Wanneer een split-partitie zich herverbint met een peer partitie, wordt het gegevensknooppunt door het dominante controleknooppunt behandeld als een stroomlid en krijgt u een CCP die stopt met msg met een reden voor CLUSTER_QUIT_REASON_STRAY_LID.



Unit-3-1 console logs show:

Cluster unit unit-3-1 transitioned from MASTER to DISABLED

The 3DES/AES algorithms require a Encryption-3DES-AES activation key.

Detected Cluster Master.

Beginning configuration replication from Master.

WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.

..

Cryptochecksum (changed): a9ed686f 8e2e689c 2553a104 7a2bd33a

End configuration replication from Master.

Cluster unit unit-3-1 transitioned from DISABLED to SLAVE

Beide eenheden (eenheid-1-1 en eenheid-3-1) geven in hun clusterstammen aan:

```
firepower# show cluster info trace | include retain
```

```
Nov 03 21:20:23.019 [CRIT]Found a split cluster with both unit-1-1 and unit-3-1 as master units.
```

```
Master role retained by unit-1-1, unit-3-1 will leave then join as a slave
```

```
Nov 03 21:20:23.019 [CRIT]Found a split cluster with both unit-1-1 and unit-3-1 as master units.
```

```
Master role retained by unit-1-1, unit-3-1 will leave then join as a slave
```

Er zijn ook syslog-berichten gegenereerd voor de split-brain:

```
firepower# show log | include 747016
```

```
Nov 03 2020 21:20:23: %FTD-4-747016: Clustering: Found a split cluster with both unit-1-1 and unit-3-1 as master units. Master role retained by unit-1-1, unit-3-1 will leave then join as a slave
```

```
Nov 03 2020 21:20:23: %FTD-4-747016: Clustering: Found a split cluster with both unit-1-1 and unit-3-1 as master units. Master role retained by unit-1-1, unit-3-1 will leave then join as a slave
```

Cluster historie

Eenheid-1-1

Eenheid-2-1

Eenheid-3-1

Geen gebeurtenissen

Geen gebeurtenissen

09:47:33 UTC Nov 2 2020

MASTER

DISABLED Detected a splitted cluster

09:47:38 UTC Nov 2 2020

DISABLED

ELECTION

Enabled

```
from CLI
09:47:38 UTC Nov 2 2020
ELECTION
SLAVE_COLD      Received cluster
control message
09:47:38 UTC Nov 2 2020
SLAVE_COLD
SLAVE_APP_SYNC  Client
progression done
09:48:18 UTC Nov 2 2020
SLAVE_APP_SYNC
SLAVE_CONFIG    Slave application
configuration sync done
09:48:29 UTC Nov 2 2020
SLAVE_CONFIG
SLAVE_FILESYS   Configuration
replication finished
09:48:30 UTC Nov 2 2020
SLAVE_FILESYS
SLAVE_BULK_SYNC Client
progression done
09:48:54 UTC Nov 2 2020
SLAVE_BULK_SYNC
SLAVE         Client
progression done
```

Scenario 2

CCL-communicatieverlies voor ~3-4 sec in beide richtingen

Voor de storing

FTD1
Site-A
Control-knooppunt

Ftd2
Site-A
Gegevensknooppunt

FTD3
Site-B
Gegevensknooppunt

Na herstel (geen wijzigingen in de eenheidsrollen)

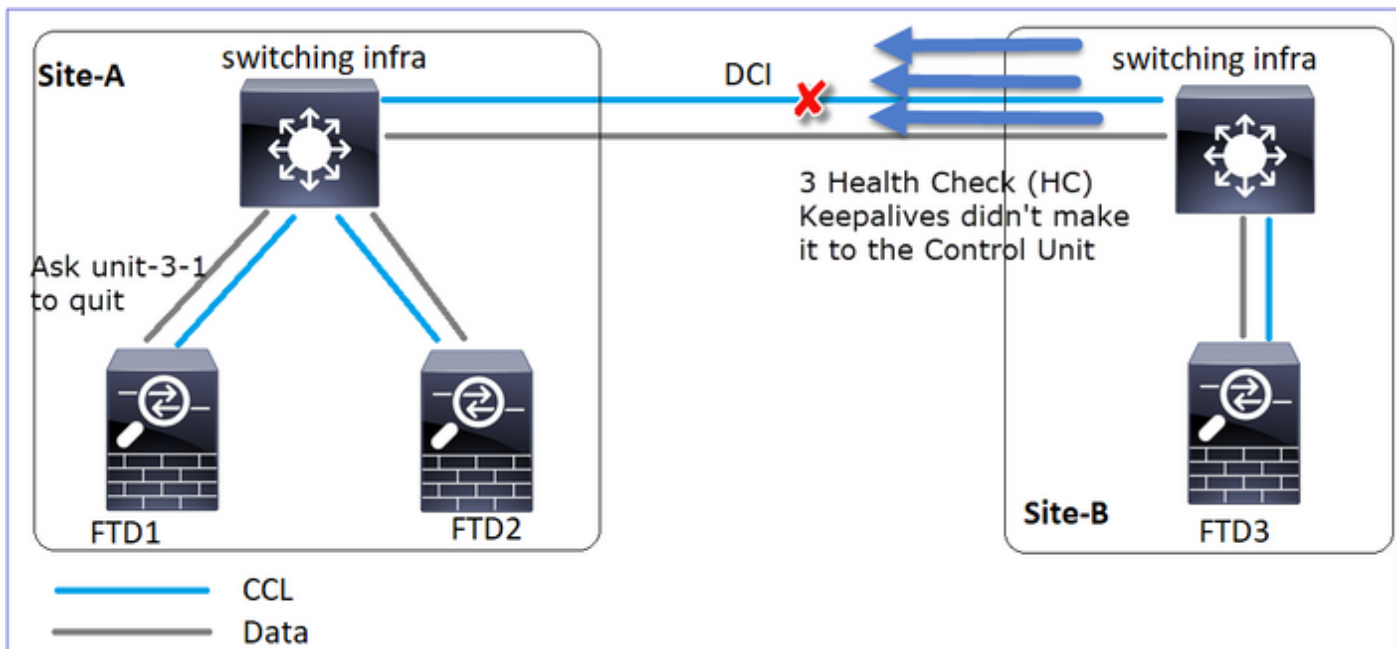
FTD1
Site-A
Control-knooppunt

Ftd2
Site-A
Gegevensknooppunt

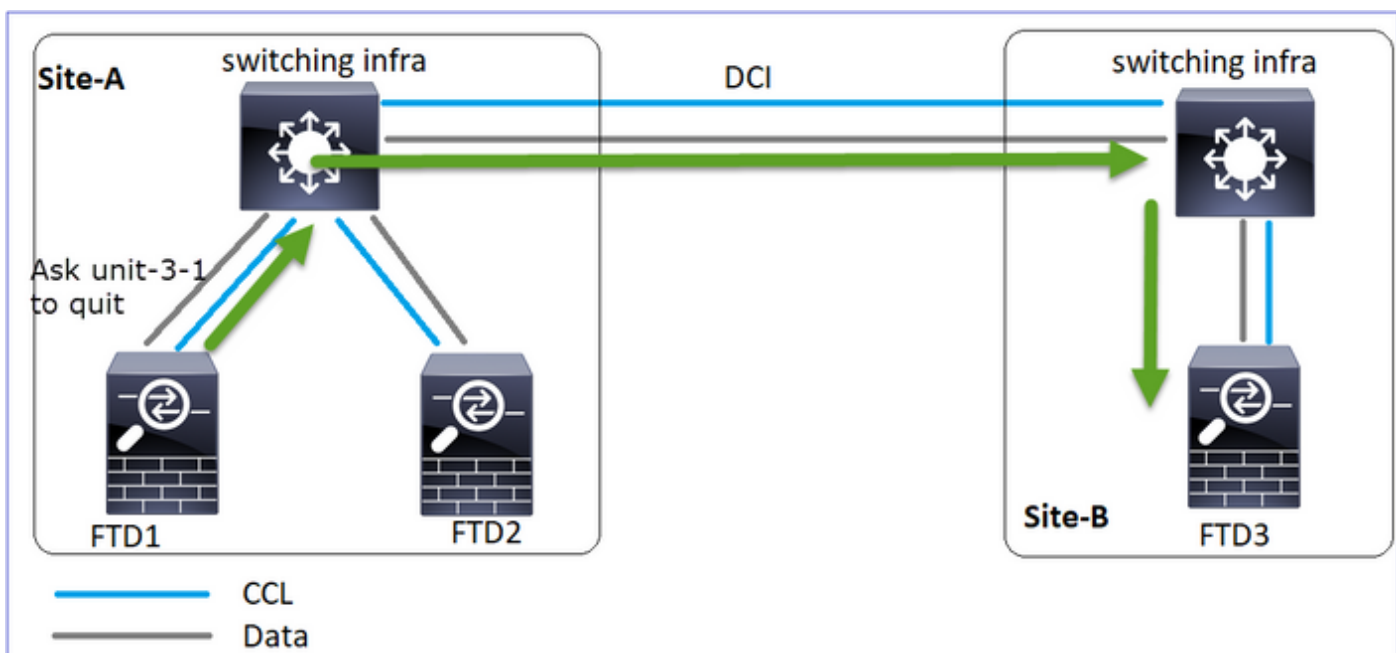
FTD3
Site-B
Gegevensknooppunt

Analyse

Event 1: Het controleknooppunt verliest 3 HCs uit unit-3-1 en stuurt een bericht naar unit-3-1 om het cluster te verlaten.



Event 2: De CCL herstelde zeer snel en het CLUSTER_QUIT_REASON_STRAY_LID bericht van het bedieningspaneel maakte het naar de afgelegen kant. Unit-3-1 gaat direct naar de uitGESCHAKELDE modus en er is geen gesplitste hersenen



Op unit-1-1 (controle) ziet u:

```
firepower#
Asking slave unit unit-3-1 to quit because it failed unit health-check.
Forcing stray member unit-3-1 to leave the cluster
```

Op unit-3-1 (gegevensknooppunt) ziet u:

```
firepower#
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.
Cluster unit unit-3-1 transitioned from SLAVE to DISABLED
Cluster-unit-3-1, overgeschakeld naar een UITGESCHAKELDE status en zodra de CCL-
```


communicatie is hersteld, wordt het opnieuw als een gegevensknooppunt toegevoegd:

```
firepower# show cluster history
20:58:40 UTC Nov 1 2020
SLAVE                DISABLED                Received control message DISABLE (stray member)
20:58:45 UTC Nov 1 2020
DISABLED                ELECTION                Enabled from CLI
20:58:45 UTC Nov 1 2020
ELECTION                SLAVE_COLD              Received cluster control message
20:58:45 UTC Nov 1 2020
SLAVE_COLD              SLAVE_APP_SYNC          Client progression done
20:59:33 UTC Nov 1 2020
SLAVE_APP_SYNC          SLAVE_CONFIG            Slave application configuration sync done
20:59:44 UTC Nov 1 2020
SLAVE_CONFIG            SLAVE_FILESYS           Configuration replication finished
20:59:45 UTC Nov 1 2020
SLAVE_FILESYS           SLAVE_BULK_SYNC         Client progression done
21:00:09 UTC Nov 1 2020
SLAVE_BULK_SYNC      SLAVE                Client progression done
```

Scenario 3

CCL-communicatieverlies voor ~3-4 sec in beide richtingen

Voor de storing

FTD1
Site-A
Control-knooppunt

Ftd2
Site-A
Gegevensknooppunt

FTD3
Site-B
Gegevensknooppunt

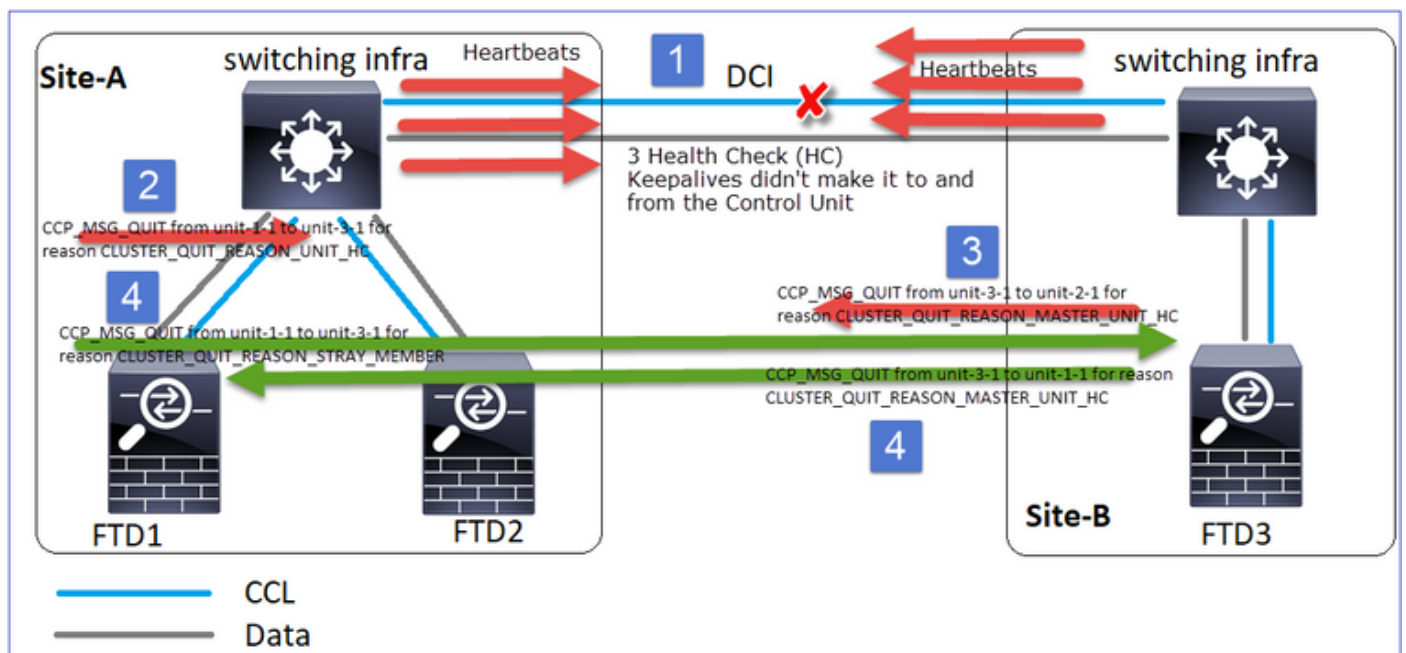
Na herstel (het controleknop is gewijzigd)

FTD1
Site-A
Gegevensknooppunt

Ftd2
Site-A
Control-knooppunt

FTD3
Site-B
Gegevensknooppunt

Analyse



1. CCL daalt.
 2. Eenheid-1-1 krijgt geen 3 HC-berichten van unit-3-1 en stuurt een QUIT-bericht naar unit-3-1.
Dit bericht bereikt nooit unit-3-1
 3. Eenheid-3-1 stuurt een QUIT-bericht naar eenheid-2-1. Dit bericht bereikt nooit eenheid-2-1.
- CCL-herstellen

4. Eenheid-1-1 ziet dat unit-3-1 zichzelf geadverteerd heeft als een controleknop en stuurt het bericht QUIT_REASON_STRAY_LID naar unit-3-1. Zodra unit-3-1 dit bericht krijgt gaat het naar een UITGESCHAKELDE toestand. Tegelijkertijd verstuurt unit-3-1 een QUIT_REASON_MASTER_UNIT_HC-bericht naar unit-1-1 en vraagt deze om te stoppen. Als unit-1-1 dit bericht krijgt naar een UITGESCHAKELDE status

Cluster historie

Eenheid-1-1

```

19:53:09 UTC Nov 2 2020
MASTER
DISABLED          Received control
message DISABLE
(master unit health check
failure)
19:53:13 UTC Nov 2 2020
DISABLED
      ELECTION          Enabled
from CLI
19:53:13 UTC Nov 2 2020
ELECTION
SLAVE_COLD          Received cluster
control message
19:53:13 UTC Nov 2 2020
SLAVE_COLD
SLAVE_APP_SYNC      Client
progression done
19:54:01 UTC Nov 2 2020
SLAVE_APP_SYNC
SLAVE_CONFIG        Slave
application configuration sync
done
19:54:12 UTC Nov 2 2020
SLAVE_CONFIG
SLAVE_FILESYS        Configuration
replication finished
19:54:13 UTC Nov 2 2020
SLAVE_FILESYS
SLAVE_BULK_SYNC      Client
progression done
19:54:37 UTC Nov 2 2020
SLAVE_BULK_SYNC
SLAVE          Client
progression done

```

Eenheid-2-1

```

19:53:06 UTC Nov 2 2020
SLAVE          MASTER_POST_CONFIG
Master relinquished role
19:53:07 UTC Nov 2 2020
MASTER_POST_CONFIG MASTER
      Master post config done
and waiting for ntfy
19:53:07 UTC Nov 2 2020
MASTER_POST_CONFIG MASTER
      Master post config done
and waiting for ntfy

```

Eenheid-3-1

```

19:53:06 UTC Nov 2 2020
SLAVE          MASTER_POST_CONFIG
Master relinquished role
19:53:07 UTC Nov 2 2020
MASTER_POST_CONFIG MASTER
      Master post config done
and waiting for ntfy
19:53:09 UTC Nov 2 2020
MASTER
DISABLED          Detected a
splitting cluster
19:53:15 UTC Nov 2 2020
DISABLED
      ELECTION          Enabled
from CLI
...
19:53:20 UTC Nov 2 2020
ELECTION
      ONCALL
Received cluster control message
19:54:44 UTC Nov 2 2020
ONCALL
SLAVE_COLD          Received cluster
control message
19:54:44 UTC Nov 2 2020
SLAVE_COLD
SLAVE_APP_SYNC      Client
progression done
19:55:32 UTC Nov 2 2020
SLAVE_APP_SYNC
SLAVE_CONFIG        Slave
application
configuration sync done
19:55:43 UTC Nov 2 2020
SLAVE_CONFIG
SLAVE_FILESYS        Configuration
replication finished
19:55:44 UTC Nov 2 2020
SLAVE_FILESYS
SLAVE_BULK_SYNC      Client
progression done
19:56:08 Nov 2 2020
SLAVE_BULK_SYNC
SLAVE          Client

```

progression done

Scenario 4

CCL-communicatieverlies voor ~3-4 sec

Voor de storing

FTD1
Site-A
Control-knooppunt

Ftd2
Site-A
Gegevensknooppunt

FTD3
Site-B
Gegevensknooppunt

Na herstel (het controlknooppunt veranderde locaties)

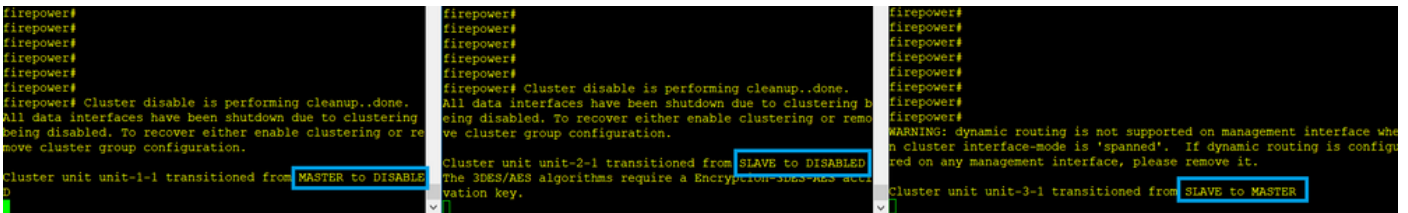
FTD1
Site-A
Gegevensknooppunt

Ftd2
Site-A
Gegevensknooppunt

FTD3
Site-B
Control-knooppunt

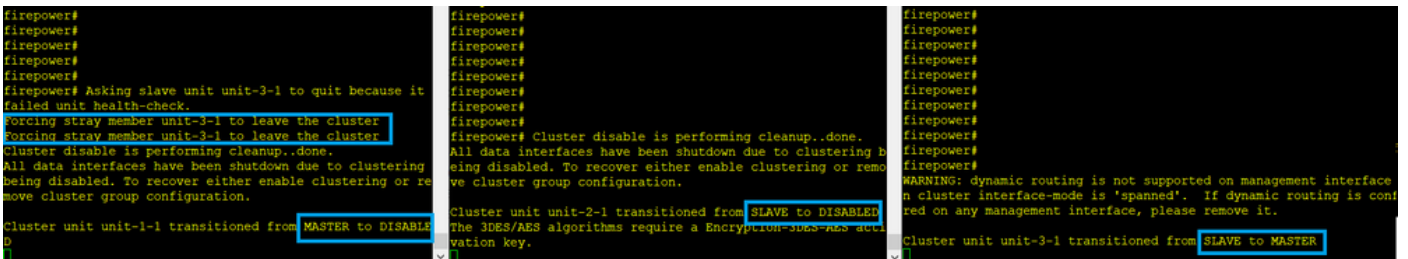
Analyse

De mislukking

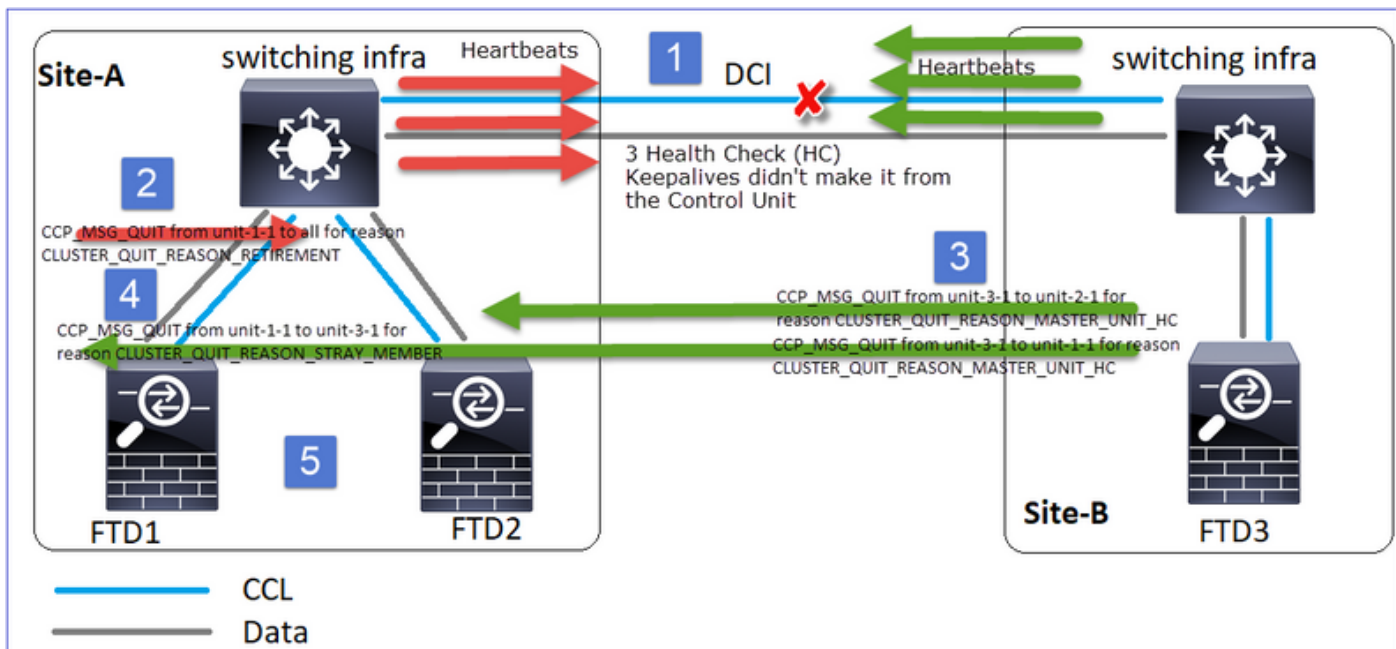


The image shows three terminal screenshots side-by-side. The left screenshot shows the transition of unit-1-1 from MASTER to DISABLED. The middle screenshot shows the transition of unit-2-1 from SLAVE to DISABLED. The right screenshot shows the transition of unit-3-1 from SLAVE to MASTER. All screenshots include the message 'Cluster disable is performing cleanup..done.' and a warning about dynamic routing on management interfaces.

Een andere gewaarwording van dezelfde mislukking. In dit geval kreeg unit-1-1 ook geen 3 HC-berichten van de unit-3-1 en toen er een nieuwe keeplevout was, trachtte de unit-3-1 uit te schoppen met behulp van een STRAY-bericht, maar het bericht haalde deze nooit naar unit-3-1:



The image shows three terminal screenshots side-by-side. The left screenshot shows the transition of unit-1-1 from MASTER to DISABLED and the message 'Forcing stray member unit-3-1 to leave the cluster'. The middle screenshot shows the transition of unit-2-1 from SLAVE to DISABLED. The right screenshot shows the transition of unit-3-1 from SLAVE to MASTER. All screenshots include the message 'Cluster disable is performing cleanup..done.' and a warning about dynamic routing on management interfaces.



1. CCL wordt enkele seconden in één richting gericht. Eenheid-3-1 ontvangt geen 3 HC-berichten van unit-1-1 en wordt een controleknooppunt
2. Eenheid-2-1 verstuurt een CLUSTER_QUIT_REASON_RETIREMENT bericht (uitzending)
3. Eenheid-3-1 verstuurt een QUIT_REASON_MASTER_UNIT_HC-bericht naar unit-2-1. Eenheid-2-1 ontvangt het en stopt het cluster.
4. Eenheid-3-1 verstuurt een QUIT_REASON_MASTER_UNIT_HC-bericht naar unit-1-1. Eenheid-1-1 ontvangt het en stopt het cluster. CCL herstelt.
5. Eenheden-1-1 en 2-1 voegen zich opnieuw bij de cluster als gegevensknooppunten aan

Opmerking

Als in stap 5 de CCL niet terugkrijgt, dan wordt op site-A de FTD1 het nieuwe controleknooppunt en na het CCL-herstel, het de nieuwe verkiezing.

Syslog-berichten op unit-1-1:

```
firepower# show log | include 747
Nov 03 2020 23:13:08: %FTD-7-747005: Clustering: State machine notify event
CLUSTER_EVENT_MEMBER_STATE (unit-3-1,DISABLED,0x0000000000000000)
Nov 03 2020 23:13:09: %FTD-4-747015: Clustering: Forcing stray member unit-3-1 to leave the
cluster
Nov 03 2020 23:13:09: %FTD-7-747005: Clustering: State machine notify event
CLUSTER_EVENT_MEMBER_STATE (unit-2-1,DISABLED,0x0000000000000000)
Nov 03 2020 23:13:10: %FTD-4-747015: Clustering: Forcing stray member unit-3-1 to leave the
cluster
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state MASTER to
DISABLED
Nov 03 2020 23:13:12: %FTD-7-747006: Clustering: State machine is at state DISABLED
Nov 03 2020 23:13:12: %FTD-7-747005: Clustering: State machine notify event
CLUSTER_EVENT_MY_STATE (state DISABLED,0x0000000000000000,0x0000000000000000)
Nov 03 2020 23:13:18: %FTD-6-747004: Clustering: State machine changed from state ELECTION to
ONCALL
```

Cluster-boomstammen op unit-1-1:

```
firepower# show cluster info trace | include QUIT
Nov 03 23:13:10.789 [DEBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 for reason
```

CLUSTER_QUIT_REASON_RETIREMENT

Nov 03 23:13:10.769 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-1-1 for reason CLUSTER_QUIT_REASON_MASTER_UNIT_HC

Nov 03 23:13:10.769 [DEBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_REASON_STRAY_MEMBER

Nov 03 23:13:09.789 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-2-1 for reason CLUSTER_QUIT_REASON_RETIREMENT

Nov 03 23:13:09.769 [DEBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_REASON_STRAY_MEMBER

Nov 03 23:13:08.559 [DEBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_MEMBER_DROPOUT

Nov 03 23:13:08.559 [DEBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_REASON_UNIT_HC

Syslog-berichten op unit-3-1:

firepower# show log | include 747

Nov 03 2020 23:13:09: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE (unit-2-1,DISABLED,0x0000000000000000)

Nov 03 2020 23:13:10: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE (unit-1-1,DISABLED,0x0000000000000000)

Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: **State machine changed from state SLAVE to MASTER**

Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state MASTER_FAST to MASTER_DRAIN

Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state MASTER_DRAIN to MASTER_CONFIG

Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state MASTER_CONFIG to MASTER_POST_CONFIG

Nov 03 2020 23:13:10: %FTD-7-747006: Clustering: State machine is at state MASTER_POST_CONFIG

Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state MASTER_POST_CONFIG to MASTER

Nov 03 2020 23:13:10: %FTD-7-747006: Clustering: **State machine is at state MASTER**

Cluster historie

Eenheid-1-1

23:13:13 UTC Nov 3 2020
MASTER DISABLED
Received control message DISABLE (master unit health check failure)
23:13:18 UTC Nov 3 2020
DISABLED ELECTION
Enabled from CLI
23:13:18 UTC Nov 3 2020
ELECTION ONCALL
Received cluster control message
23:13:23 UTC Nov 3 2020
ONCALL ELECTION
Received cluster control message
...
23:14:48 UTC Nov 3 2020
ONCALL ELECTION
Received cluster control message
23:14:48 UTC Nov 3 2020
ELECTION SLAVE_COLD
Received cluster control message
23:14:48 UTC Nov 3 2020
SLAVE_COLD SLAVE_APP_SYNC
Client progression done
23:15:36 UTC Nov 3 2020

Eenheid-2-1

23:13:12 UTC Nov 3 2020
R SLAVE DISABLED
Received control message DISABLE (master unit health check failure)
23:13:17 UTC Nov 3 2020
E DISABLED ELECTION
Enabled from CLI
23:13:17 UTC Nov 3 2020
R ELECTION SLAVE_COLD
Received cluster control message
23:13:17 UTC Nov 3 2020
R SLAVE_COLD SLAVE_APP_SYNC
Client progression done
23:14:05 UTC Nov 3 2020
SLAVE_APP_SYNC SLAVE_CONFIG
R Slave application configuration sync done
23:14:16 UTC Nov 3 2020
R SLAVE_CONFIG
SLAVE_FILESYS Configuration replication finished
23:14:17 UTC Nov 3 2020
C SLAVE_FILESYS SLAVE_BULK_SYNC
Client progression done

Eenheid-3-1

23:13:10 UTC Nov 3 2020
SLAVE MASTER_POST_CONFIG
Master relinquished role
23:13:11 UTC Nov 3 2020
MASTER_POST_CONFIG MASTER
Master post config done and waiting for ntfy

```

SLAVE_APP_SYNC SLAVE_CONFIG S
lave application configuration
sync done
23:15:48 UTC Nov 3 2020 SLAVE_BULK_SYNC SLAVE
Client progression done
SLAVE_CONFIG SLAVE_FILESYS C
onfiguration replication finished
23:15:49 UTC Nov 3 2020
SLAVE_FILESYS SLAVE_BULK_SYNC C
lient progression done
23:16:13 UTC Nov 3 2020
SLAVE_BULK_SYNC SLAVE C
lient progression done

```

Scenario 5

Voor de storing

FTD1
Site-A
Control-knooppunt

Ftd2
Site-A
Gegevensknooppunt

FTD3
Site-B
Gegevensknooppunt

Na herstel (geen wijzigingen)

FTD1
Site-A
Control-knooppunt

Ftd2
Site-A
Gegevensknooppunt

FTD3
Site-B
Gegevensknooppunt

De mislukking

```

firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower# Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.
firepower#
firepower# Cluster unit unit-2-1 transitioned from SLAVE to DISABLED
The 3DES/AES algorithms require a Encryption-3DES-AES activation key.
firepower#
firepower# Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
...
Cryptochecksum (changed): b053fdaf 57c6834e db98bfe0 8d57e2ae
End configuration replication from Master.
firepower#
firepower# Cluster unit unit-2-1 transitioned from DISABLED to SLAVE
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower# WARNING: dynamic routing is not supported on management interface when cluster interface-mode is 'spanned'. If dynamic routing is configured on any management interface, please remove it.
firepower#
firepower# Cluster unit unit-3-1 transitioned from SLAVE to MASTER
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.
firepower#
firepower# Cluster unit unit-3-1 transitioned from MASTER to DISABLED
The 3DES/AES algorithms require a Encryption-3DES-AES activation key.
firepower#
firepower# Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
...
Cryptochecksum (changed): b053fdaf 57c6834e db98bfe0 8d57e2ae
End configuration replication from Master.
firepower#
firepower# Cluster unit unit-3-1 transitioned from DISABLED to SLAVE

```

Enheid-3-1 stuurde QUIT-berichten naar zowel unit-1-1 als unit-2-1, maar vanwege aansluitingsproblemen heeft slechts unit-2-1 het QUIT-bericht ontvangen.

Enheid-1-1 clustersporenstammen:

```

firepower# show cluster info trace | include QUIT
Nov 04 00:52:10.429 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 for reason CLUSTER_QUIT_REASON_RETIREMENT
Nov 04 00:51:47.059 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-2-1 for reason CLUSTER_QUIT_REASON_RETIREMENT
Nov 04 00:51:45.429 [DEBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_MEMBER_DROPOUT
Nov 04 00:51:45.429 [DEBUG]Send CCP message to unit-3-1(1): CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_REASON_UNIT_HC

```

Enheid-2-1 clustersporenstammen:

firepower# show cluster info trace | include QUIT

```
Nov 04 00:52:10.389 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 for reason
CLUSTER_QUIT_REASON_RETIREMENT
Nov 04 00:51:47.019 [DEBUG]Send CCP message to all: CCP_MSG_QUIT from unit-2-1 for reason
CLUSTER_QUIT_REASON_RETIREMENT
Nov 04 00:51:46.999 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-2-1 for reason
CLUSTER_QUIT_REASON_MASTER_UNIT_HC
Nov 04 00:51:45.389 [DEBUG]Receive CCP message: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason
CLUSTER_QUIT_MEMBER_DROPOUT
```

Cluster historie

Eenheid-1-1

Eenheid-2-1

Eenheid-3-1

```
00:51:47 UTC Nov 4 2020
SLAVE MASTER_POST_CONFIG
Master relinquished role
00:51:48 UTC Nov 4 2020
MASTER_POST_CONFIG
MASTER Master post config
done and
waiting for ntfy
00:52:12 UTC Nov 4 2020
MASTER DISABLED
Detected a splitted cluster
00:52:17 UTC Nov 4 2020
DISABLED ELECTION
Enabled from CLI
00:52:17 UTC Nov 4 2020
ELECTION ONCALL
Received cluster control message
00:53:25 UTC Nov 4 2020
ONCALL SLAVE_COLD
Received cluster control message
00:53:25 UTC Nov 4 2020
SLAVE_COLD SLAVE_APP_SYNC
Client progression done
00:54:12 UTC Nov 4 2020
SLAVE_APP_SYNC SLAVE_CONFIG
Slave application configuration
sync done
00:54:24 UTC Nov 4 2020
SLAVE_CONFIG SLAVE_FILESYS
Configuration replication
finished
00:54:25 UTC Nov 4 2020
SLAVE_FILESYS SLAVE_BULK_SYNC
Client progression done
00:54:49 UTC Nov 4 2020
SLAVE_BULK_SYNC SLAVE
Client progression done
```

Geen gebeurtenissen

```
00:51:50 UTC Nov 4 2020
SLAVE DISABLED
Received control message
DISABLE
(master unit health check
failure)
00:51:54 UTC Nov 4 2020
DISABLED ELECTION
Enabled from CLI
00:51:54 UTC Nov 4 2020
ELECTION SLAVE_COLD
Received cluster control message
00:51:54 UTC Nov 4 2020
SLAVE_COLD SLAVE_APP_SYNC
Client progression done
00:52:42 UTC Nov 4 2020
SLAVE_APP_SYNC SLAVE_CONFIG
Slave application configuration
sync done
00:52:54 UTC Nov 4 2020
SLAVE_CONFIG SLAVE_FILESYS
Configuration replication
finished
00:52:55 UTC Nov 4 2020
SLAVE_FILESYS SLAVE_BULK_SYNC
Client progression done
00:53:19 UTC Nov 4 2020
SLAVE_BULK_SYNC SLAVE
Client progression done
```

Cluster-datacenterverbinding-instelling

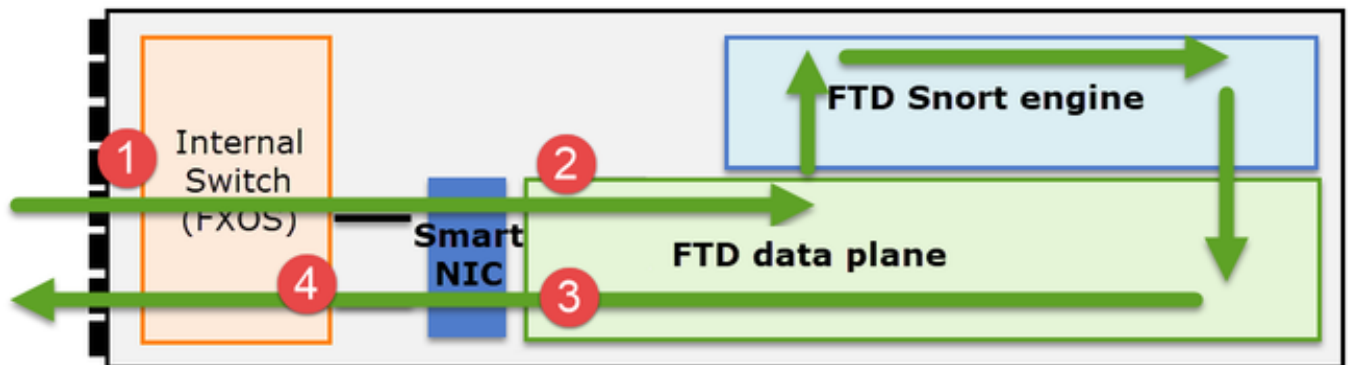
NGFW-Capture points

NGFW biedt opnamemogelijkheden op deze punten:

- Chassis interne switch (FXOS)
- FTD-gegevensvliegtuigmotor

- FTD Snortmachine

Wanneer u problemen met de datapad-oplossing op een cluster signaleert, zijn de opnamepunten die in de meeste gevallen worden gebruikt de FXOS en FTD gegevensvliegtuigmotor opnamen.



1. FXOS-ingangsoptname op de fysieke interface
2. FTD-ingangsoptname in de gegevensvliegtuigmotor
3. FTD-uitzetting in datatevlakmotor
4. FXOS-ingangssignaal op backplane interface

Kijk in dit document voor meer informatie over NGFW-opnamen:

Cluster Unity Flow Rolls-basisproducten

Aansluitingen kunnen op verschillende manieren door een cluster worden vastgesteld die afhankelijk zijn van factoren als:

- Type verkeer (TCP, UDP, enz.)
- Taakalgoritme ingesteld op de aangrenzende switch
- Functies ingesteld in de firewall
- Netwerkomstandigheden (bijvoorbeeld IP-fragmentatie, netwerkvertragingen, enz.)

Flow rol	Beschrijving	Vlag(en)
Eigenaar	Het apparaat dat de aansluiting aanvankelijk ontvangt	UIO
Directeur	De eenheid die de eigenaren verzorgt zoekt verzoeken van expediteurs.	Y
Reserve-eigenaar	Zolang de regisseur niet dezelfde eenheid is als de eigenaar, is de regisseur ook de back-ueigenaar. Als de eigenaar zichzelf kiest als regisseur, dan wordt er een aparte back-ueigenaar gekozen.	Y (als de regisseur ook de back-ueigenaar is) y (als de regisseur niet de back-ueigenaar is)
doorsturen	Een eenheid die pakketten naar de eigenaar stuurt	z
Eigenaar van fragmentatie	De eenheid die het gefragmenteerde verkeer verwerkt	-
Back-uplijn	In een interChassis-cluster waarin zowel de regisseur-/back-up- als de eigenaarstromen eigendom zijn van de eenheden van hetzelfde chassis, wordt een eenheid in een van de andere chassis een secundaire back-	weien

up/registreur.

Deze rol is specifiek voor clusters tussen chassis van FirePOWER 9300-serie met meer dan één kant.

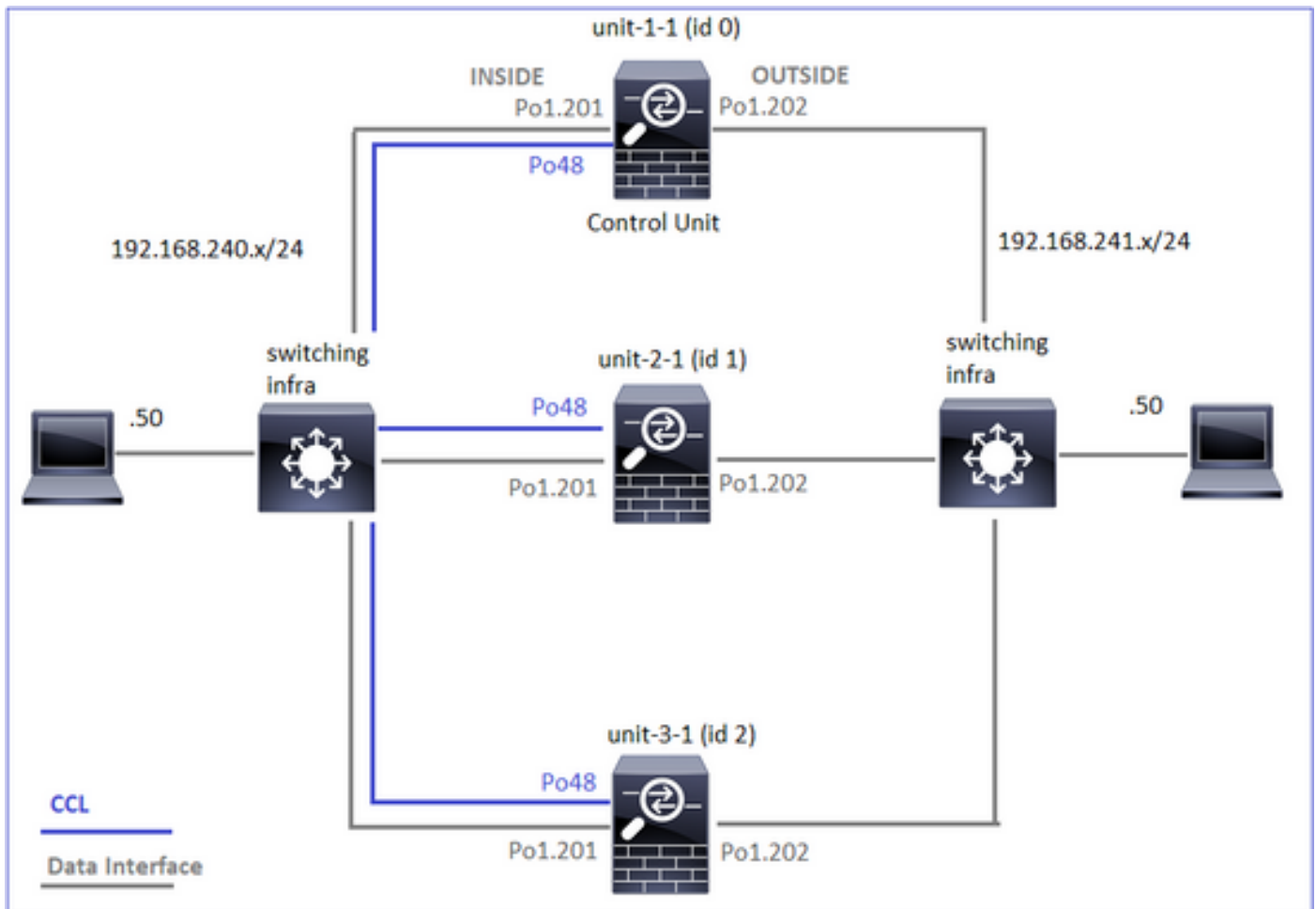
- Kijk voor meer informatie in het gedeelte dat betrekking heeft op de Configuration Guide (zie koppelingen in de verwante informatie)
- In specifieke scenario's (zie onderdeel casestudy's) kunnen sommige vlaggen niet worden getoond

Cluster Connection-casestudy's

De volgende paragraaf betreft verschillende casestudies die een aantal manieren aantonen waarop een verbinding via een cluster tot stand kan worden gebracht. De doelstellingen zijn:

- Zorg ervoor dat u de verschillende eenheidrollen beheerst
- demonstreren hoe de verschillende opdrachtoutput gecorreleerd kan worden

Topologie



Cluster-eenheden en ID's:

Eenheid-1-1

```
Cluster GROUP1: On
Interface mode: spanned
This is "unit-1-1" in state
MASTER
  ID      : 0
  Site ID : 1
```

Eenheid-2-1

```
Unit "unit-2-1" in state
SLAVE
  ID      : 1
  Site ID : 1
  Version : 9.15(1)
  Serial No.: FCH23157Y9N
```

Eenheid-3-1

```
Unit "unit-3-1" in state
SLAVE
  ID      : 2
  Site ID : 2
  Version : 9.15(1)
  Serial No.: FCH22247MKJ
```

Version	: 9.15(1)	CCL IP	: 192.222.2.1	CCL IP	: 192.222.3.1
Serial No.:	FCH22247LNK	CCL IP	: 192.222.2.1	CCL MAC	:
CCL IP	: 192.222.1.1	CCL MAC	:	0015.c500.038f	
CCL MAC	:	0015.c500.028f		Last join	: 01:42:59 UTC
0015.c500.018f		Last join	: 02:04:19 UTC	Nov 27 2020	
Last join	: 02:24:43 UTC	Nov 27 2020		Last leave:	: 01:29:18 UTC
Nov 27 2020		Last leave:	: N/A	Nov 27 2020	
Last leave:	: N/A				

Cluster is ingeschakeld:

```
cluster exec cap CAPI int INSIDE buffer 33554432 match tcp host 192.168.240.50 host
192.168.241.50 eq 80
cluster exec cap CAPO int OUTSIDE buffer 33554432 match tcp host 192.168.240.50 host
192.168.241.50 eq 80
cluster exec cap CAPI_RH reinject-hide int INSIDE buffer 33554432 match tcp host 192.168.240.50
host 192.168.241.50 eq 80
cluster exec cap CAPO_RH reinject-hide int OUTSIDE buffer 33554432 match tcp host 192.168.240.50
host 192.168.241.50 eq 80
cluster exec cap CCL int cluster buffer 33554432
```

Opmerking: Deze testen werden uitgevoerd in een labomgeving met minimaal verkeer door het cluster. Probeer bij de productie zoveel mogelijk specifieke opnamefilters te gebruiken (bv. bestemmingspoorten en indien mogelijk de bronpoort) om het "lawaai" in de opnamen te minimaliseren.

Case Studie 1. Symmetrisch verkeer (eigenaar is ook de regisseur)

Waarneming 1. De heruitspuiten-verstopperschepping tonen alleen pakketten op unit-1-1. Dit betekent dat de stroom in beide richtingen door unit-1-1 (symmetrisch verkeer) ging:

```
firepower# cluster exec show cap
unit-1-1(LOCAL):*****
capture CCL type raw-data interface cluster [Capturing - 33513 bytes]
capture CAPI type raw-data buffer 33554432 trace interface INSIDE [Buffer Full - 33553914 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO type raw-data buffer 33554432 trace interface OUTSIDE [Buffer Full - 33553914
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPI_RH type raw-data reinject-hide buffer 33554432 interface INSIDE [Buffer Full -
33553914 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO_RH type raw-data reinject-hide buffer 33554432 interface OUTSIDE [Buffer Full -
33553914 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80

unit-2-1:*****
capture CCL type raw-data interface cluster [Capturing - 23245 bytes]
capture CAPI type raw-data buffer 33554432 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO type raw-data buffer 33554432 trace interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPI_RH type raw-data reinject-hide buffer 33554432 interface INSIDE [Capturing - 0
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
capture CAPO_RH type raw-data reinject-hide buffer 33554432 interface OUTSIDE [Capturing - 0
bytes]
```

```
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
```

```
unit-3-1:*****
```

```
capture CCL type raw-data interface cluster [Capturing - 24815 bytes]
```

```
capture CAPI type raw-data buffer 33554432 trace interface INSIDE [Capturing - 0 bytes]
```

```
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
```

```
capture CAPO type raw-data buffer 33554432 trace interface OUTSIDE [Capturing - 0 bytes]
```

```
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
```

```
capture CAPI_RH type raw-data reinject-hide buffer 33554432 interface INSIDE [Capturing - 0 bytes]
```

```
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
```

```
capture CAPO_RH type raw-data reinject-hide buffer 33554432 interface OUTSIDE [Capturing - 0 bytes]
```

```
match tcp host 192.168.240.50 host 192.168.241.50 eq 80
```

Observatie 2. Connection flag analysis for flow with source port 45954

```
firepower# cluster exec show conn
```

```
unit-1-1(LOCAL):*****
```

```
22 in use, 25 most used
```

```
Cluster:
```

```
fwd connections: 0 in use, 1 most used
```

```
dir connections: 0 in use, 122 most used
```

```
centralized connections: 0 in use, 0 most used
```

```
VPN redirect connections: 0 in use, 0 most used
```

```
Inspect Snort:
```

```
preserve-connection: 1 enabled, 0 in effect, 2 most enabled, 1 most in effect
```

```
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:45954, idle 0:00:00, bytes 487413076, flags UIO N1
```

```
unit-2-1:*****
```

```
22 in use, 271 most used
```

```
Cluster:
```

```
fwd connections: 0 in use, 2 most used
```

```
dir connections: 0 in use, 2 most used
```

```
centralized connections: 0 in use, 0 most used
```

```
VPN redirect connections: 0 in use, 0 most used
```

```
Inspect Snort:
```

```
preserve-connection: 1 enabled, 0 in effect, 249 most enabled, 0 most in effect
```

```
unit-3-1:*****
```

```
17 in use, 20 most used
```

```
Cluster:
```

```
fwd connections: 1 in use, 2 most used
```

```
dir connections: 1 in use, 127 most used
```

```
centralized connections: 0 in use, 0 most used
```

```
VPN redirect connections: 0 in use, 0 most used
```

```
Inspect Snort:
```

```
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect
```

```
TCP OUTSIDE 192.168.241.50:443 NP Identity Ifc 192.168.240.50:39698, idle 0:00:23, bytes 0, flags z
```

```
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:45954, idle 0:00:06, bytes 0, flags y
```

Eenheid

Vlag

Opmerking

Eenheid-1-1

UIO

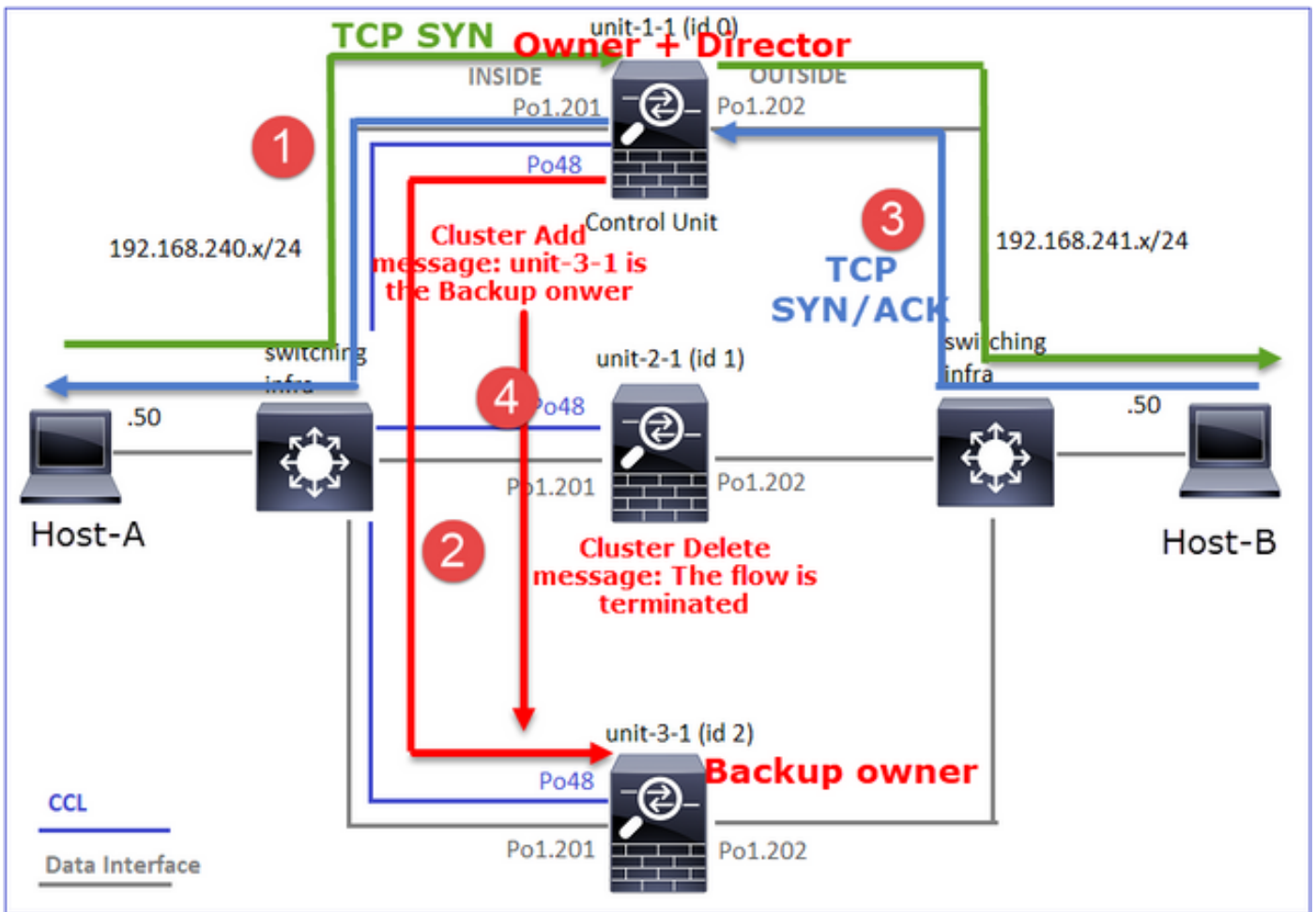
- **Flow Owner** - De eenheid regelt de stroom
- **Directeur** - Aangezien eenheid 3-1 "y" en niet "Y" heeft, betekent dit dat eenheid-1-1 werd gekozen als directeur voor deze stroom. Aangezien het dus ook de eigenaar is, werd een andere eenheid (in dit geval eenheid 3-1) gekozen als de back-up eigenaar

Eenheid-2-1

-

-

Dit kan als volgt worden gevisualiseerd:



1. TCP SYN-pakket arriveert vanaf Host-A naar unit-1. Unit-1-1 wordt de stroomeigenaar
2. Eenheid-1-1 wordt ook tot stroomdirecteur gekozen. Zodoende selecteert het ook unit-3-1 als back-opeigenaar (**cluster add** bericht)
3. TCP SYN/ACK-pakket arriveert van Host-B naar unit-3-1. De stroom is symmetrisch
4. Zodra de verbinding wordt beëindigd, stuurt de eigenaar een bericht om de stroominformatie te verwijderen van de back-opeigenaar

Waarneming 3. Opname met sporen toont aan dat beide richtingen alleen door eenheid-1-1 gaan

Stap 1. Identificeer de stroom en de pakketten van belangen in alle clustereenheden op basis van de bronpoort:

```
firepower# cluster exec show capture CAPI | i 45954
unit-1-1(LOCAL):*****
1: 08:42:09.362697 802.1Q vlan#201 P0 192.168.240.50.45954 > 192.168.241.50.80: S
992089269:992089269(0) win 29200 <mss 1460,sackOK,timestamp 495153655 0,nop,wscale 7>
2: 08:42:09.363521 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.45954: S
4042762409:4042762409(0) ack 992089270 win 28960 <mss 1380,sackOK,timestamp 505509125
495153655,nop,wscale 7>
3: 08:42:09.363827 802.1Q vlan#201 P0 192.168.240.50.45954 > 192.168.241.50.80: . ack 4042762410
win 229 <nop,nop,timestamp 495153657 505509125>
...
unit-2-1:*****
```

unit-3-1:*****

firepower# **cluster exec show capture CAPO | i 45954**

unit-1-1(LOCAL):*****

1: 08:42:09.362987 802.1Q vlan#202 P0 192.168.240.50.45954 > 192.168.241.50.80: S
2732339016:2732339016(0) win 29200 <mss 1380,sackOK,timestamp 495153655 0,nop,wscale 7>
2: 08:42:09.363415 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45954: S
3603655982:3603655982(0) ack 2732339017 win 28960 <mss 1460,sackOK,timestamp 505509125
495153655,nop,wscale 7>
3: 08:42:09.363903 802.1Q vlan#202 P0 192.168.240.50.45954 > 192.168.241.50.80: . ack 3603655983
win 229 <nop,nop,timestamp 495153657 505509125>

...
unit-2-1:*****

unit-3-1:*****

Stap 2. Aangezien dit een TCP-stroming is, worden de 3-weg handshake-pakketten overgetrokken. Zoals het in deze uitvoer zichtbaar is, is unit-1-1 de eigenaar. Voor de eenvoud worden de niet-relevante fasen weggelaten:

firepower# **show cap CAPI packet-number 1 trace**

25985 packets captured
1: 08:42:09.362697 802.1Q vlan#201 P0 192.168.240.50.45954 > 192.168.241.50.80: S
992089269:992089269(0) win 29200 <mss 1460,sackOK,timestamp 495153655 0,nop,wscale 7>

...

Phase: 4

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'INSIDE'

Flow type: NO FLOW

I (0) got initial, attempting ownership.

Phase: 5

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'INSIDE'

Flow type: NO FLOW

I (0) am becoming owner

...

Het retourverkeer (TCP SYN/ACK):

firepower# **show capture CAPO packet-number 2 trace**

25985 packets captured
2: 08:42:09.363415 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45954: S
3603655982:3603655982(0) **ack** 2732339017 win 28960 <mss 1460,sackOK,timestamp 505509125
495153655,nop,wscale 7>

...

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Config:

Additional Information:

Found flow with id 9364, using existing flow

Waarneming 4. Op FTD-gegevensvliegtuigsystemen worden de verbinding creatie en -beëindiging op alle eenheden getoond:

```
firepower# cluster exec show log | include 45954
unit-1-1(LOCAL):*****
Dec 01 2020 08:42:09: %FTD-6-302013: Built inbound TCP connection 9364 for
INSIDE:192.168.240.50/45954 (192.168.240.50/45954) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 08:42:18: %FTD-6-302014: Teardown TCP connection 9364 for
INSIDE:192.168.240.50/45954 to OUTSIDE:192.168.241.50/80 duration 0:00:08 bytes 1024000440 TCP
FINs from INSIDE

unit-2-1:*****

unit-3-1:*****
Dec 01 2020 08:42:09: %FTD-6-302022: Built backup stub TCP connection for
INSIDE:192.168.240.50/45954 (192.168.240.50/45954) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 08:42:18: %FTD-6-302023: Teardown backup TCP connection for
INSIDE:192.168.240.50/45954 to OUTSIDE:192.168.241.50/80 duration 0:00:08 forwarded bytes 0
Cluster flow with CLU closed on owner
```

Case Studie 2. Symmetrisch verkeer (eigenaar anders dan de regisseur)

- Dit is hetzelfde als studie nr. 1, maar in dit geval is de stroomeigenaar een andere eenheid dan de regisseur.
- Alle uitgangen lijken op casestudy nr. 1. Het belangrijkste verschil ten opzichte van casestudy nr. 1 is de Y-vlag die de y-vlag van scenario 1 vervangt.

Waarneming 1. De eigenaar is anders dan de directeur

Connection flag-analyse voor flow met bronpoort 46278

```
firepower# cluster exec show conn
unit-1-1(LOCAL):*****
23 in use, 25 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 0 in use, 122 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46278, idle 0:00:00, bytes 508848268, flags
UIO N1
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46276, idle 0:00:03, bytes 0, flags aA N1

unit-2-1:*****
21 in use, 271 most used
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 0 in use, 2 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect
```

```

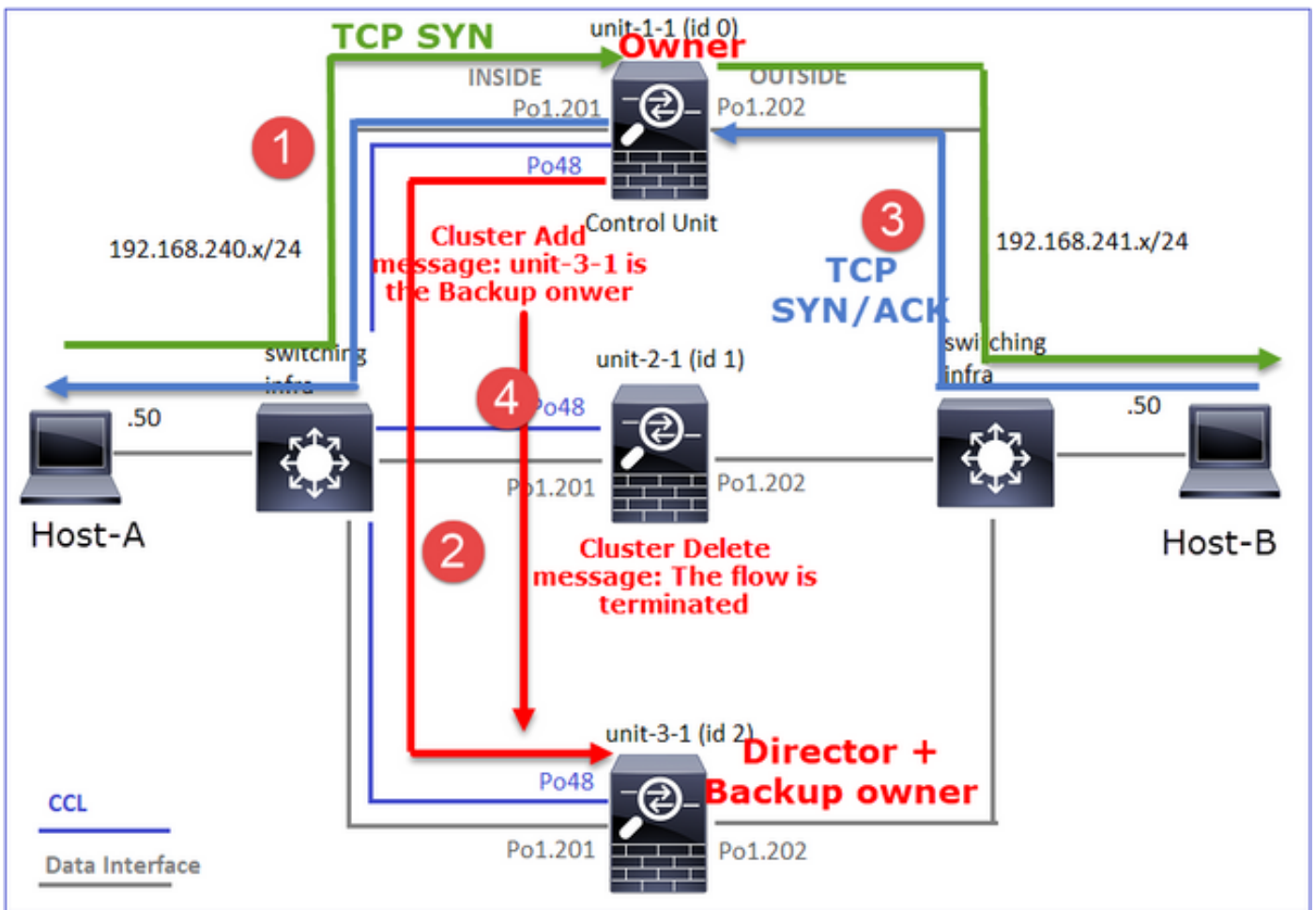
unit-3-1:*****
17 in use, 20 most used
Cluster:
fwd connections: 1 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 NP Identity Ifc 192.168.240.50:46276, idle 0:00:02, bytes 0, flags
z
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46278, idle 0:00:06, bytes 0, flags Y

```

Eenheid	Vlag	Opmerking
Eenheid-1-1	UIO	• Flow Owner - De eenheid regelt de stroom
Eenheid-2-1	-	-
Eenheid-3-1	Y	• Director en back-up eigenaar - unit 3-1 heeft vlag Y (Director).

Dit kan als volgt worden gevisualiseerd:



1. TCP SYN-pakket arriveert vanaf Host-A naar unit-1. Unit-1-1 wordt de stroomeigenaar
2. Unit-3-1 wordt gekozen tot de stroomdirecteur. Eenheid-3-1 is ook de back-ubeigenaar ('cluster add'-bericht op UDP 4193 via de CCL)
3. TCP SYN/ACK-pakket arriveert van Host-B naar unit-3-1. De stroom is symmetrisch
4. Zodra de verbinding wordt beëindigd, stuurt de eigenaar via de CCL een 'cluster Delete'-bericht op UDP 4193 om de stroominformatie van de back-ubeigenaar te verwijderen

Waarneming 2. Opname met sporen toont aan dat beide richtingen alleen door eenheid-1-1 gaan

Stap 1. Volg dezelfde benadering als in casestudy 1 om de stroom en pakketten van belang in alle clustereenheden aan te duiden die op de bronpoort zijn gebaseerd:

```
firepower# cluster exec show cap CAPI | include 46278
unit-1-1(LOCAL):*****
3: 11:01:44.841631 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80: S
1972783998:1972783998(0) win 29200 <mss 1460,sackOK,timestamp 503529072 0,nop,wscale 7>
4: 11:01:44.842317 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.46278: S
3524167695:3524167695(0) ack 1972783999 win 28960 <mss 1380,sackOK,timestamp 513884542
503529072,nop,wscale 7>
5: 11:01:44.842592 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80: . ack 3524167696
win 229 <nop,nop,timestamp 503529073 513884542>
...
unit-2-1:*****
unit-3-1:*****
firepower#
```

Opnemen op de BUITENinterface:

```
firepower# cluster exec show cap CAPO | include 46278
unit-1-1(LOCAL):*****
3: 11:01:44.841921 802.1Q vlan#202 P0 192.168.240.50.46278 > 192.168.241.50.80: S
2153055699:2153055699(0) win 29200 <mss 1380,sackOK,timestamp 503529072 0,nop,wscale 7>
4: 11:01:44.842226 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46278: S
3382481337:3382481337(0) ack 2153055700 win 28960 <mss 1460,sackOK,timestamp 513884542
503529072,nop,wscale 7>
5: 11:01:44.842638 802.1Q vlan#202 P0 192.168.240.50.46278 > 192.168.241.50.80: . ack 3382481338
win 229 <nop,nop,timestamp 503529073 513884542>
unit-2-1:*****
unit-3-1:*****
firepower#
```

Stap 2. Stel scherp op de IP-pakketten (TCP SYN en TCP SYN/ACK):

```
firepower# cluster exec show cap CAPI packet-number 3 trace
unit-1-1(LOCAL):*****

824 packets captured

3: 11:01:44.841631 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80: S
1972783998:1972783998(0) win 29200 <mss 1460,sackOK,timestamp 503529072 0,nop,wscale 7>
...

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
```


Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW

I (0) am becoming owner

Overtrek de SYN/ACK op unit-1-1:

```
firepower# cluster exec show cap CAPO packet-number 4 trace
unit-1-1(LOCAL):*****
```

```
4: 11:01:44.842226 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.46278: S
3382481337:3382481337(0) ack 2153055700 win 28960 <mss 1460,sackOK,timestamp 513884542
503529072,nop,wscale 7>
```

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:

Found flow with id 9583, using existing flow

Waarneming 3. Op dataplausystemen van FTD zijn de verbindingscreeatie en -beëindiging van de eigenaar en de back-ueigenaar te zien:

```
firepower# cluster exec show log | include 46278
unit-1-1(LOCAL):*****
```

```
Dec 01 2020 11:01:44: %FTD-6-302013: Built inbound TCP connection 9583 for
INSIDE:192.168.240.50/46278 (192.168.240.50/46278) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 11:01:53: %FTD-6-302014: Teardown TCP connection 9583 for
INSIDE:192.168.240.50/46278 to OUTSIDE:192.168.241.50/80 duration 0:00:08 bytes 1024001808 TCP
FINs from INSIDE
```

```
unit-2-1:*****
```

```
unit-3-1:*****
```

```
Dec 01 2020 11:01:44: %FTD-6-302022: Built director stub TCP connection for
INSIDE:192.168.240.50/46278 (192.168.240.50/46278) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 11:01:53: %FTD-6-302023: Teardown director TCP connection for
INSIDE:192.168.240.50/46278 to OUTSIDE:192.168.241.50/80 duration 0:00:08 forwarded bytes 0
Cluster flow with CLU closed on owner
```

Case Studie 3. Asymmetric Traffic Engineering (regisseur voor het verkeer)

Waarneming 1. De heruitspuiten vangen toont pakketten op unit-1-1 en unit-2-1 (asymmetrische stroom):

```
firepower# cluster exec show cap
unit-1-1(LOCAL):*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33554320 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Buffer Full - 98552 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 98552 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Buffer Full - 98552
```

```

bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Buffer Full - 99932
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-2-1:*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553268 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 99052 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Buffer Full - 99052
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-3-1:*****
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 53815 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Capturing - 658 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Capturing - 658
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

```

Observatie 2. Connection flag analysis for flow with source port 46502

```

firepower# cluster exec show conn
unit-1-1(LOCAL):*****
23 in use, 25 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 0 in use, 122 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46502, idle 0:00:00, bytes 448760236, flags
UIO N1
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46500, idle 0:00:06, bytes 0, flags aA N1

unit-2-1:*****
21 in use, 271 most used
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 1 in use, 2 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46502, idle 0:00:00, bytes 0, flags Y

unit-3-1:*****
17 in use, 20 most used
Cluster:
fwd connections: 1 in use, 5 most used

```

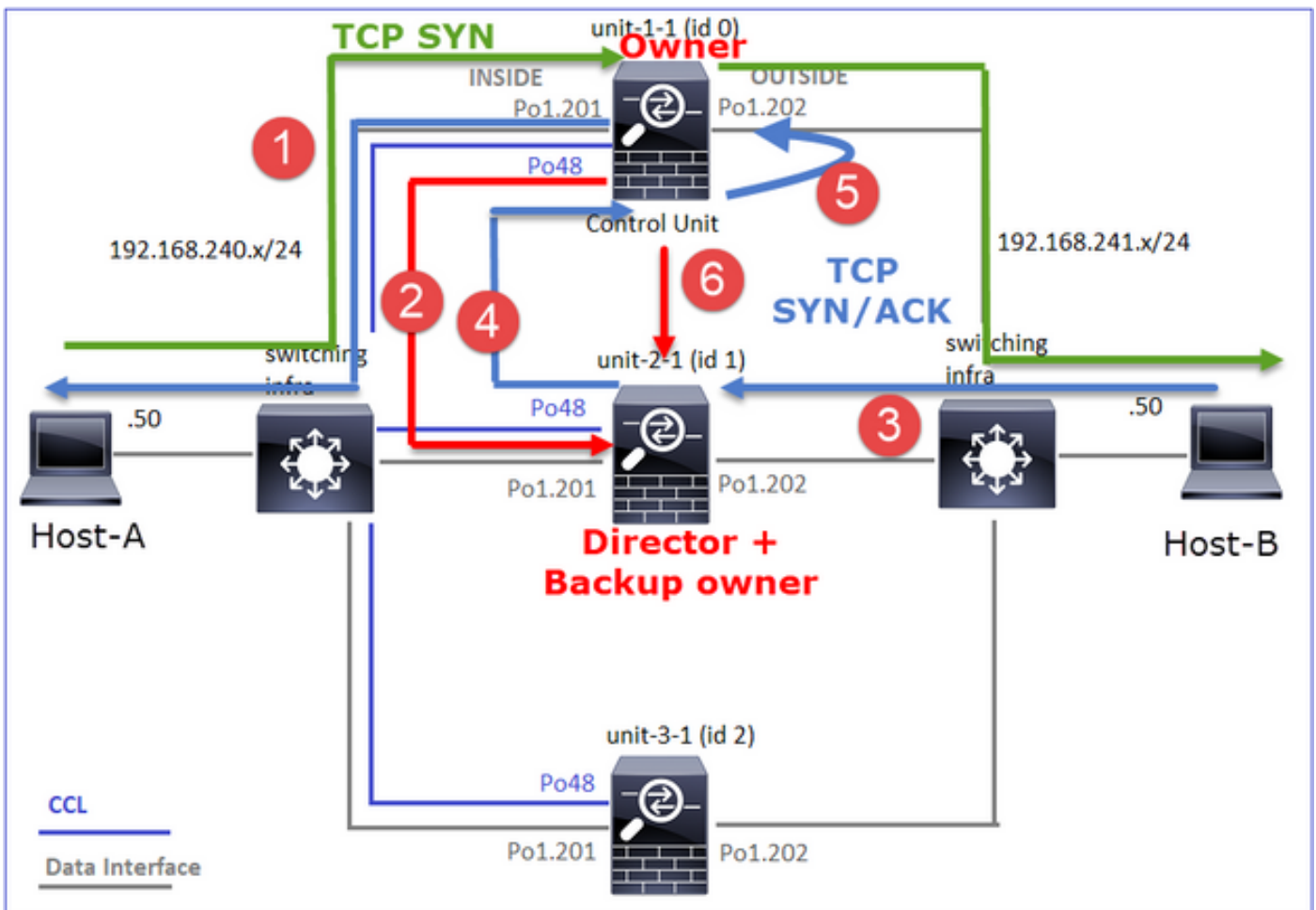
```

dir connections: 0 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

```

Eenheid	Vlag	Opmerking
Eenheid-1-1	UIO	<ul style="list-style-type: none"> • Flow Owner - De eenheid regelt de stroom • Director - Aangezien unit-2-1 de markering 'Y' heeft, betekent dit dat eenheid-2-1 is gekozen als directeur voor deze stroom. • Reserve-eigenaar • Ten slotte is het, hoewel het niet duidelijk is uit deze productie, maar uit de show-opname en de show-loguitgangen blijkt dat unit-2-1 deze stroom naar de eigenaar doorstuurt (hoewel dit scenario technisch niet als expediteur wordt beschouwd)
Eenheid-2-1	Y	<p>Opmerking: Een eenheid kan niet zowel regisseur (Y flow) als expediteur (z flow) zijn, deze 2 rollen sluiten elkaar uit. Merk op dat de regisseurs (Y flow) nog steeds voorwaarts verkeer kunnen doorsturen. Zie de Uitvoer van het logboek later in deze casestudy.</p>
Eenheid-3-1	-	-

Dit kan als volgt worden gevisualiseerd:



1. TCP SYN-pakket arriveert vanaf Host-A naar unit-1. Unit-1-1 wordt de stroomeigenaar
2. Unit 2-1 wordt gekozen als stroomregisseur en back-ueigenaar. De stroomeigenaar stuurt een 'cluster add' eenastbericht op UDP 4193 om de back-ueigenaar te informeren over de stroom
3. TCP SYN/ACK-pakket arriveert van Host-B naar unit-2-1. De stroom is asymmetrisch

4. Unit-2-1 zendt het pakket door de CCL naar de eigenaar (door TCP SYN Cookie)
5. De eigenaar steekt het pakje op interface BUITEN en stuurt het pakje naar host-A door
6. Zodra de verbinding wordt beëindigd, stuurt de eigenaar een bericht om de stroominformatie te verwijderen van de back-up-eigenaar

Waarneming 3. Opname met sporen toont het asymmetrische verkeer en de omleiding van eenheid-2-1 naar eenheid-1-1

Stap 1. Identificeer de pakketten die aan de stroom van belang (haven 46502) behoren:

```
firepower# cluster exec show capture CAPI | include 46502
unit-1-1(LOCAL):*****
3: 12:58:33.356121 802.1Q vlan#201 P0 192.168.240.50.46502 > 192.168.241.50.80: S
4124514680:4124514680(0) win 29200 <mss 1460,sackOK,timestamp 510537534 0,nop,wscale 7>
4: 12:58:33.357037 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.46502: S
883000451:883000451(0) ack 4124514681 win 28960 <mss 1380,sackOK,timestamp 520893004
510537534,nop,wscale 7>
5: 12:58:33.357357 802.1Q vlan#201 P0 192.168.240.50.46502 > 192.168.241.50.80: . ack 883000452
win 229 <nop,nop,timestamp 510537536 520893004>
unit-2-1:*****
unit-3-1:*****
```

De terugkeerrichting:

```
firepower# cluster exec show capture CAPO | include 46502
unit-1-1(LOCAL):*****
3: 12:58:33.356426 802.1Q vlan#202 P0 192.168.240.50.46502 > 192.168.241.50.80: S
1434968587:1434968587(0) win 29200 <mss 1380,sackOK,timestamp 510537534 0,nop,wscale 7>
4: 12:58:33.356915 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: S
4257314722:4257314722(0) ack 1434968588 win 28960 <mss 1460,sackOK,timestamp 520893004
510537534,nop,wscale 7>
5: 12:58:33.357403 802.1Q vlan#202 P0 192.168.240.50.46502 > 192.168.241.50.80: . ack 4257314723
win 229 <nop,nop,timestamp 510537536 520893004>
unit-2-1:*****
1: 12:58:33.359249 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: S
4257314722:4257314722(0) ack 1434968588 win 28960 <mss 1460,sackOK,timestamp 520893004
510537534,nop,wscale 7>
2: 12:58:33.360302 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: . ack 1434968736
win 235 <nop,nop,timestamp 520893005 510537536>
3: 12:58:33.361004 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: .
4257314723:4257316091(1368) ack 1434968736 win 235 <nop,nop,timestamp 520893006 510537536>
...
unit-3-1:*****
```

Stap 2. Controleer de pakketten. Merk op dat standaard alleen de eerste 50 ingangspakketten worden overgetrokken. Voor de eenvoud worden de niet-relevante spoorfasen weggelaten.

Eenheid-1-1 (eigenaar):

```
firepower# cluster exec show capture CAPI packet-number 3 trace
unit-1-1(LOCAL):*****
3: 12:58:33.356121 802.1Q vlan#201 P0 192.168.240.50.46502 > 192.168.241.50.80: S
4124514680:4124514680(0) win 29200 <mss 1460,sackOK,timestamp 510537534 0,nop,wscale 7>
...
Phase: 4
Type: CLUSTER-EVENT
```

Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
I (0) got initial, attempting ownership.

Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
I (0) am becoming owner
Eenheid-2-1 (expediteur)

Het retourverkeer (TCP SYN/ACK). De belangeneenheid is eenheid-2-1 die de regisseur/back-up-eigenaar is en het verkeer doorgeeft aan de eigenaar:

```
firepower# cluster exec unit unit-2-1 show capture CAPO packet-number 1 trace
1: 12:58:33.359249 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: S
4257314722:4257314722(0) ack 1434968588 win 28960 <mss 1460,sackOK,timestamp 520893004
510537534,nop,wscale 7>
```

...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
I (1) got initial, attempting ownership.

Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
I (1) am early redirecting to (0) due to matching action (-1).

Waarneming 4. Op FTD-gegevensvliegtuigsystemen worden de verbindingscreeatie en -beëindiging op alle eenheden getoond:

```
firepower# cluster exec show log | i 46502
unit-1-1(LOCAL):*****
Dec 01 2020 12:58:33: %FTD-6-302013: Built inbound TCP connection 9742 for
INSIDE:192.168.240.50/46502 (192.168.240.50/46502) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 12:59:02: %FTD-6-302014: Teardown TCP connection 9742 for
INSIDE:192.168.240.50/46502 to OUTSIDE:192.168.241.50/80 duration 0:00:28 bytes 2048000440 TCP
FINs from INSIDE
unit-2-1:*****
```

```
Dec 01 2020 12:58:33: %FTD-6-302022: Built forwarder stub TCP connection for
OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46502
(192.168.240.50/46502)
Dec 01 2020 12:58:33: %FTD-6-302023: Teardown forwarder TCP connection for
OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46502 duration 0:00:00 forwarded bytes 0
Forwarding or redirect flow removed to create director or backup flow
Dec 01 2020 12:58:33: %FTD-6-302022: Built director stub TCP connection for
INSIDE:192.168.240.50/46502 (192.168.240.50/46502) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 12:59:02: %FTD-6-302023: Teardown director TCP connection for
INSIDE:192.168.240.50/46502 to OUTSIDE:192.168.241.50/80 duration 0:00:28 forwarded bytes
2048316300 Cluster flow with CLU closed on owner
```

```
unit-3-1:*****
firepower#
```

Case Studie 4. Asymmetric Traffic Engineering (eigenaar is de regisseur)

Waarneming 1. De heruitspuiten vangen toont pakketten op unit-1-1 en unit-2-1 (asymmetrische stroom):

```
firepower# cluster exec show cap
unit-1-1(LOCAL):*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33554229 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Buffer Full - 98974 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 98974 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Buffer Full - 98974
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Buffer Full - 99924
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-2-1:*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33552925 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 99052 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Buffer Full - 99052
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-3-1:*****
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 227690 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Capturing - 4754 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Capturing - 0
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
```

Observatie 2. Connection flag analysis for flow with source port 46916

```
firepower# cluster exec show conn
```

```

unit-1-1(LOCAL):*****
23 in use, 25 most used
Cluster:
fwd connections: 0 in use, 1 most used
dir connections: 0 in use, 122 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46916, idle 0:00:00, bytes 414682616, flags
UIO N1

```

```

unit-2-1:*****
21 in use, 271 most used
Cluster:
fwd connections: 1 in use, 2 most used
dir connections: 0 in use, 2 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 NP Identity Ifc 192.168.240.50:46916, idle 0:00:00, bytes 0, flags
z

```

```

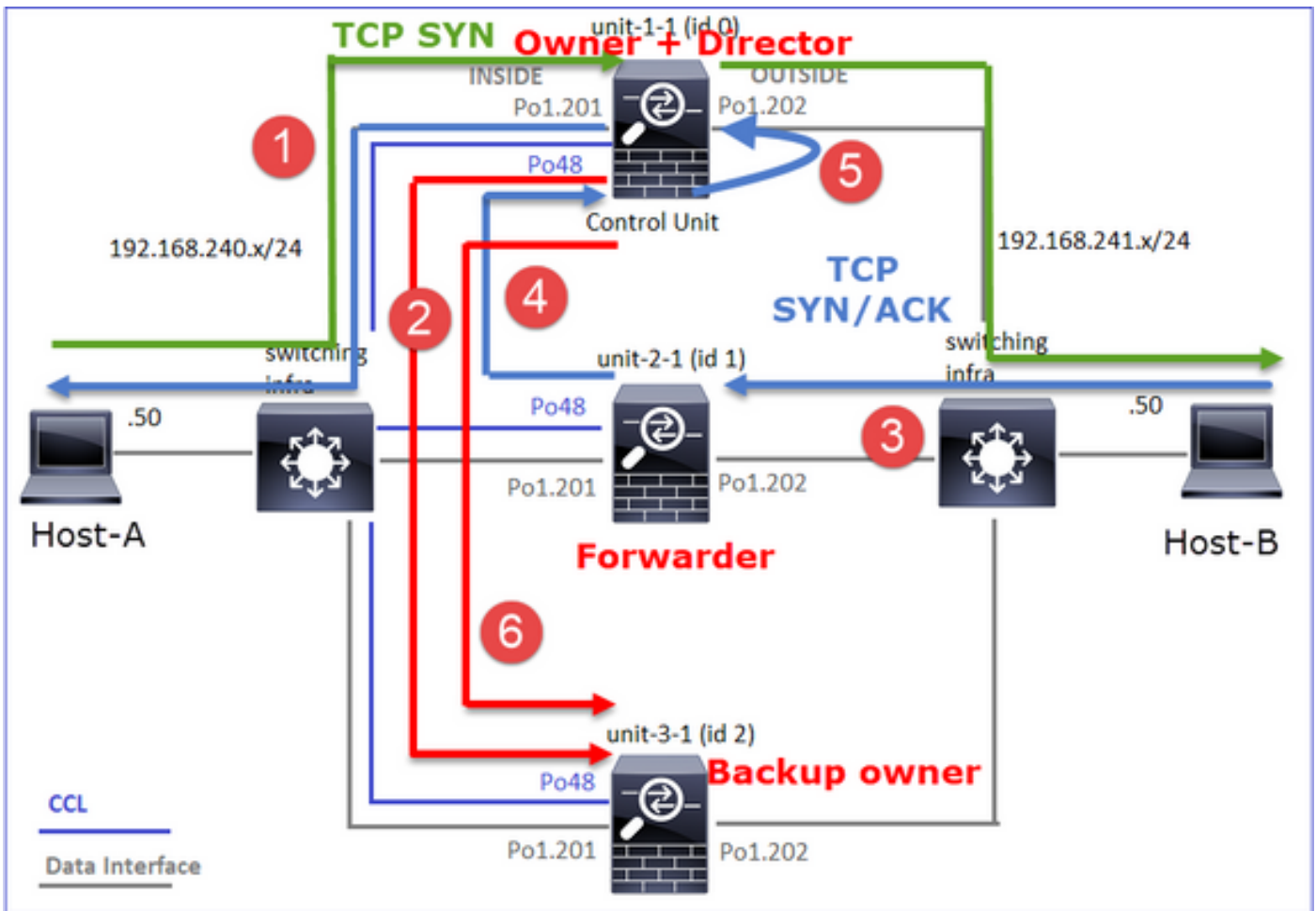
unit-3-1:*****
17 in use, 20 most used
Cluster:
fwd connections: 0 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46916, idle 0:00:04, bytes 0, flags y

```

Eenheid	Vlag	Opmerking
Eenheid-1-1	UIO	<ul style="list-style-type: none"> · Flow Owner - De eenheid regelt de stroom · Directeur - Aangezien eenheid 3-1 "y" en niet "Y" heeft, betekent dit dat eenheid-1-1 werd gekozen als directeur voor deze stroom. Aangezien het dus ook de eigenaar is, werd een andere eenheid (in dit geval eenheid 3-1) gekozen als de back-upeigenaar
Eenheid-2-1	z	<ul style="list-style-type: none"> · Doorsturen
Eenheid-3-1	Y	<ul style="list-style-type: none"> - Reserve-eigenaar

Dit kan als volgt worden gevisualiseerd:



1. TCP SYN-pakket arriveert vanaf Host-A naar eenheid-1. Unit-1-1 wordt de stroomeigenaar en wordt geselecteerd als regisseur
2. Eenheid-3-1 wordt gekozen als back-up-eigenaar. De stroomeigenaar stuurt een cluster voegt bericht toe op UDP 4193 om de back-ueigenaar te informeren over de stroom
3. TCP SYN/ACK-pakket arriveert van Host-B naar unit-2-1. De stroom is asymmetrisch
4. Unit-2-1 zendt het pakket door de CCL naar de eigenaar (door TCP SYN Cookie)
5. De eigenaar steekt het pakje op interface BUITEN en stuurt het pakje naar host-A door
6. Zodra de verbinding wordt beëindigd, stuurt de eigenaar een bericht om de stroominformatie te verwijderen van de back-ueigenaar

Waarneming 3. Opname met sporen toont het asymmetrische verkeer en de omleiding van eenheid-2-1 naar eenheid-1-1

Eenheid-2-1 (expediteur)

```
firepower# cluster exec unit unit-2-1 show capture CAPO packet-number 1 trace
1: 16:11:33.653164 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.46916: S
1331019196:1331019196(0) ack 3089755618 win 28960 <mss 1460,sackOK,timestamp 532473211
522117741,nop,wscale 7>
...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
```


I (1) got initial, attempting ownership.

Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW

I (1) am early redirecting to (0) due to matching action (-1).

Waarneming 4. Op FTD-gegevensvliegtuigsystemen worden de verbinding creatie en -beëindiging op alle eenheden getoond:

- Eenheid-1-1 (eigenaar)
- Eenheid-2-1 (expediteur)
- Eenheid-3-1 (back-upeigenaar)

```
firepower# cluster exec show log | i 46916
unit-1-1(LOCAL):*****
Dec 01 2020 16:11:33: %FTD-6-302013: Built inbound TCP connection 10023 for
INSIDE:192.168.240.50/46916 (192.168.240.50/46916) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 16:11:42: %FTD-6-302014: Teardown TCP connection 10023 for
INSIDE:192.168.240.50/46916 to OUTSIDE:192.168.241.50/80 duration 0:00:09 bytes 1024010016 TCP
FINs from INSIDE

unit-2-1:*****
Dec 01 2020 16:11:33: %FTD-6-302022: Built forwarder stub TCP connection for
OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46916
(192.168.240.50/46916)
Dec 01 2020 16:11:42: %FTD-6-302023: Teardown forwarder TCP connection for
OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46916 duration 0:00:09 forwarded bytes
1024009868 Cluster flow with CLU closed on owner

unit-3-1:*****
Dec 01 2020 16:11:33: %FTD-6-302022: Built backup stub TCP connection for
INSIDE:192.168.240.50/46916 (192.168.240.50/46916) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 16:11:42: %FTD-6-302023: Teardown backup TCP connection for
INSIDE:192.168.240.50/46916 to OUTSIDE:192.168.241.50/80 duration 0:00:09 forwarded bytes 0
Cluster flow with CLU closed on owner
```

Case Studie 5. Asymmetric Traffic Engineering (eigenaar is anders dan de regisseur)

Waarneming 1. De heruitspuiten vangen toont pakketten op unit-1-1 en unit-2-1 (asymmetrische stroom):

```
firepower# cluster exec show cap
unit-1-1(LOCAL):*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553207 bytes]
capture CAPI type raw-data buffer 100000 trace interface INSIDE [Buffer Full - 99396 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 99224 bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Buffer Full - 99396
bytes]
match tcp host 192.168.240.50 host 192.168.241.50 eq www
capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Buffer Full - 99928
```

bytes]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-2-1:*****

capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33554251 bytes]

capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Buffer Full - 99052 bytes]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

capture CAPO_RH type raw-data **reinject-hide** buffer 100000 interface **OUTSIDE** [Buffer Full - **99052 bytes**]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

unit-3-1:*****

capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 131925 bytes]

capture CAPI type raw-data buffer 100000 trace interface INSIDE [Capturing - 0 bytes]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

capture CAPO type raw-data buffer 100000 trace interface OUTSIDE [Capturing - 2592 bytes]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

capture CAPI_RH type raw-data reinject-hide buffer 100000 interface INSIDE [Capturing - 0 bytes]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

capture CAPO_RH type raw-data reinject-hide buffer 100000 interface OUTSIDE [Capturing - 0 bytes]

match tcp host 192.168.240.50 host 192.168.241.50 eq www

Waarneming 2. Condensatie van de vlag voor stroom met bronpoort 46994

firepower# **cluster exec show conn**

unit-1-1(LOCAL):*****

23 in use, 25 most used

Cluster:

fwd connections: 0 in use, 1 most used

dir connections: 0 in use, 122 most used

centralized connections: 0 in use, 0 most used

VPN redirect connections: 0 in use, 0 most used

Inspect Snort:

preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 1 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:**46994**, idle 0:00:00, bytes 406028640, **flags UIO N1**

unit-2-1:*****

22 in use, 271 most used

Cluster:

fwd connections: 1 in use, 2 most used

dir connections: 0 in use, 2 most used

centralized connections: 0 in use, 0 most used

VPN redirect connections: 0 in use, 0 most used

Inspect Snort:

preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 NP Identity Ifc 192.168.240.50:**46994**, idle 0:00:00, bytes 0, **flags z**

unit-3-1:*****

17 in use, 20 most used

Cluster:

fwd connections: 2 in use, 5 most used

dir connections: 1 in use, 127 most used

centralized connections: 0 in use, 0 most used

VPN redirect connections: 0 in use, 0 most used

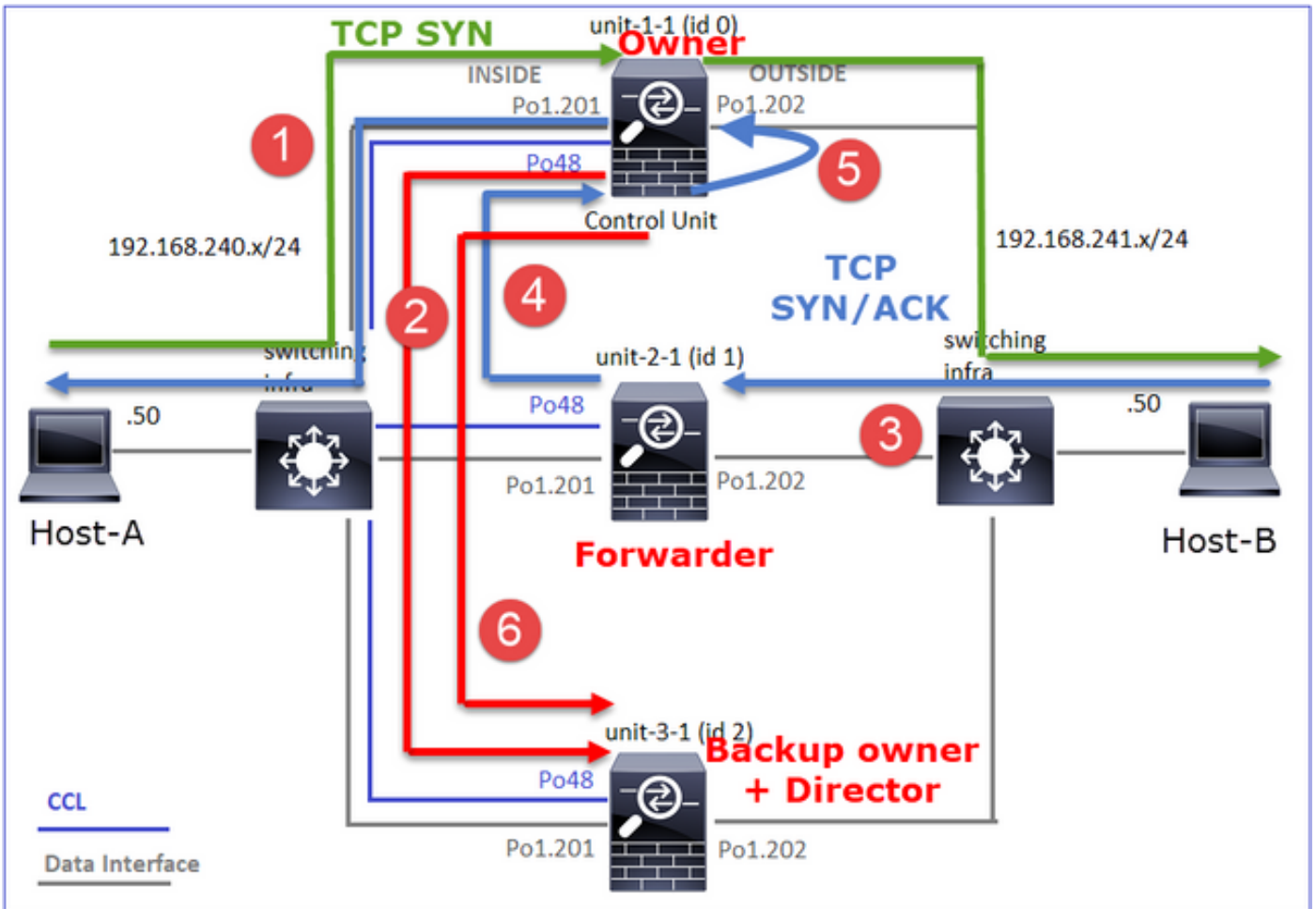
Inspect Snort:

preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:46994, idle 0:00:05, bytes 0, flags Y

Eenheid	Vlag	Opmerking
Eenheid-1-1	UIO	• Flow Owner - De eenheid regelt de stroom
Eenheid-2-1	z	• Doorsturen
Eenheid-3-1	Y	• Reserve-eigenaar • Directeur

Dit kan als volgt worden gevisualiseerd:



1. TCP SYN-pakket arriveert vanaf Host-A naar unit-1. Unit-1-1 wordt de stroomeigenaar
2. Eenheid-3-1 wordt gekozen als regisseur en back-opeigenaar. De stroomeigenaar stuurt een 'cluster add' eenastbericht op UDP 4193 om de back-opeigenaar te informeren over de stroom
3. TCP SYN/ACK-pakket arriveert van Host-B naar unit-2-1. De stroom is asymmetrisch
4. Unit-2-1 zendt het pakket door de CCL naar de eigenaar (door TCP SYN Cookie)
5. De eigenaar steekt het pakje op interface BUITEN en stuurt het pakje naar host-A door
6. Zodra de verbinding wordt beëindigd, stuurt de eigenaar een bericht om de stroominformatie te verwijderen van de back-opeigenaar

Waarneming 3. Opname met sporen toont het asymmetrische verkeer en de omleiding van eenheid-2-1 naar eenheid-1-1

Eenheid-1-1 (eigenaar)

```
firepower# cluster exec show cap CAPI packet-number 1 trace
unit-1-1(LOCAL):*****
...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
```

```
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
I (0) am becoming owner
Eenheid-2-1 (expediteur)
```

```
firepower# cluster exec unit unit-2-1 show cap CAPO packet-number 1 trace
1: 16:46:44.232074 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46994: S
2863659376:2863659376(0) ack 2879616990 win 28960 <mss 1460,sackOK,timestamp 534583774
524228304,nop,wscale 7>
```

```
...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
I (1) got initial, attempting ownership.
```

```
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
I (1) am early redirecting to (0) due to matching action (-1).
```

Waarneming 4. Op FTD-gegevensvliegtuigsystemen worden de verbinding creatie en - beëindiging op alle eenheden getoond:

- Eenheid-1-1 (eigenaar)
- Eenheid-2-1 (expediteur)
- Eenheid-3-1 (back-ueigenaar/regisseur)

```
firepower# cluster exec show log | i 46994
unit-1-1(LOCAL):*****
Dec 01 2020 16:46:44: %FTD-6-302013: Built inbound TCP connection 10080 for
```

```

INSIDE:192.168.240.50/46994 (192.168.240.50/46994) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 16:46:53: %FTD-6-302014: Teardown TCP connection 10080 for
INSIDE:192.168.240.50/46994 to OUTSIDE:192.168.241.50/80 duration 0:00:09 bytes 1024000440 TCP
FINs from INSIDE

```

```

unit-2-1:*****
Dec 01 2020 16:46:44: %FTD-6-302022: Built forwarder stub TCP connection for
OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46994
(192.168.240.50/46994)
Dec 01 2020 16:46:53: %FTD-6-302023: Teardown forwarder TCP connection for
OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46994 duration 0:00:09 forwarded bytes
1024000292 Cluster flow with CLU closed on owner

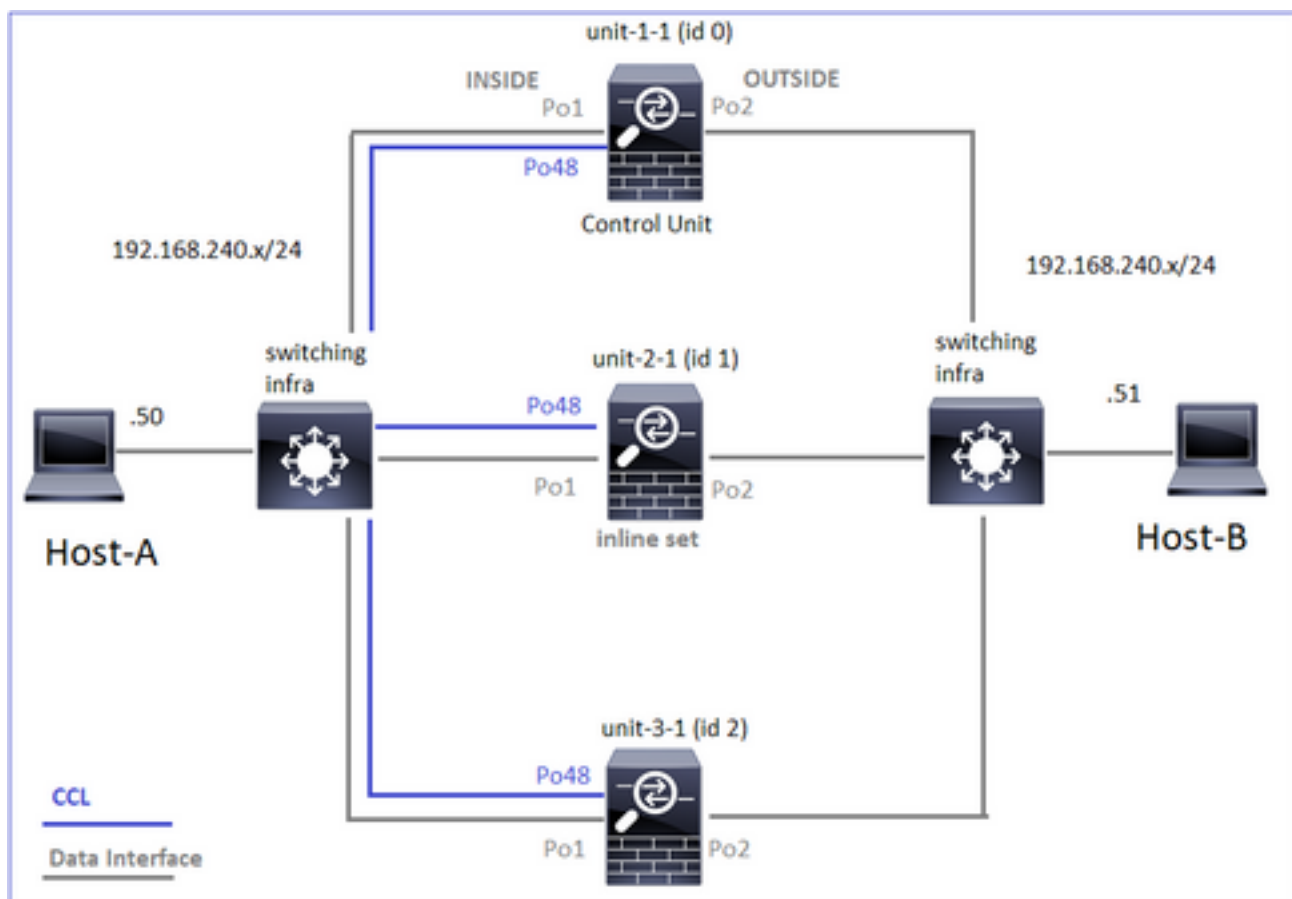
```

```

unit-3-1:*****
Dec 01 2020 16:46:44: %FTD-6-302022: Built director stub TCP connection for
INSIDE:192.168.240.50/46994 (192.168.240.50/46994) to OUTSIDE:192.168.241.50/80
(192.168.241.50/80)
Dec 01 2020 16:46:53: %FTD-6-302023: Teardown director TCP connection for
INSIDE:192.168.240.50/46994 to OUTSIDE:192.168.241.50/80 duration 0:00:09 forwarded bytes 0
Cluster flow with CLU closed on owner

```

Voor de volgende case studies is de gebruikte topologie gebaseerd op een cluster met inline sets:



Case Studie 6. Asymmetric Traffic Engineering (inline), is de eigenaar de regisseur

Waarneming 1. De heruiteinde-verstopt opnames tonen pakketten op unit-1-1 en unit-2-1 (asymmetrische stroom). Bovendien is de eigenaar unit-2-1 (er zijn pakketten op zowel INSIDE als BUITEN interfaces voor de heruitprojectieverstopping, terwijl unit-1-1 alleen op BUITEN heeft):

```

firepower# cluster exec show cap
unit-1-1(LOCAL):*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553253 bytes]

```

```
capture CAPO type raw-data trace interface OUTSIDE [Buffer Full - 523432 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data reinject-hide interface OUTSIDE [Buffer Full - 523432 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
```

```
unit-2-1:*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33554312 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Buffer Full - 523782 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Buffer Full - 523782 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data reinject-hide interface OUTSIDE [Buffer Full - 524218 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Buffer Full - 523782 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
```

```
unit-3-1:*****
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 53118 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data reinject-hide interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
```

Observatie 2. Connection flag analysis for flow with source port 51844

```
firepower# cluster exec show conn addr 192.168.240.51
```

```
unit-1-1(LOCAL):*****
```

```
30 in use, 102 most used
```

```
Cluster:
```

```
fwd connections: 1 in use, 1 most used
```

```
dir connections: 2 in use, 122 most used
```

```
centralized connections: 3 in use, 39 most used
```

```
VPN redirect connections: 0 in use, 0 most used
```

```
Inspect Snort:
```

```
preserve-connection: 0 enabled, 0 in effect, 4 most enabled, 1 most in effect
```

```
TCP OUTSIDE 192.168.240.51:80 NP Identity Ifc 192.168.240.50:51844, idle 0:00:00, bytes 0, flags
```

```
z
```

```
unit-2-1:*****
```

```
23 in use, 271 most used
```

```
Cluster:
```

```
fwd connections: 0 in use, 2 most used
```

```
dir connections: 4 in use, 26 most used
```

```
centralized connections: 0 in use, 14 most used
```

```
VPN redirect connections: 0 in use, 0 most used
```

```
Inspect Snort:
```

```
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect
```

```
TCP OUTSIDE 192.168.240.51:80 INSIDE 192.168.240.50:51844, idle 0:00:00, bytes 231214400, flags
```

```
b N
```

```
unit-3-1:*****
```

```
20 in use, 55 most used
```

```
Cluster:
```

```

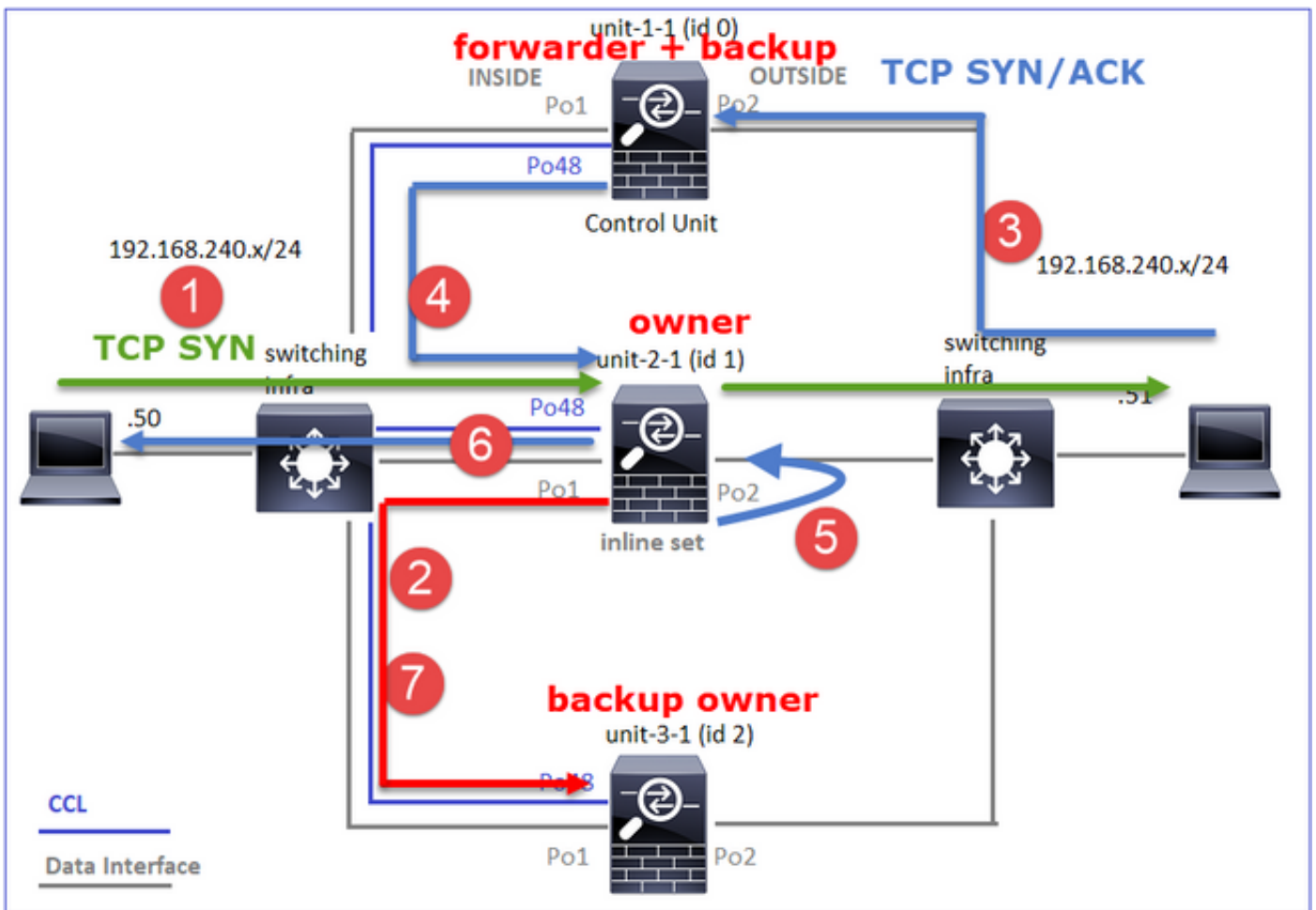
fwd connections: 0 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 24 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

```

```
TCP OUTSIDE 192.168.240.51:80 INSIDE 192.168.240.50:51844, idle 0:00:01, bytes 0, flags y
```

Eenheid	Vlag	Opmerking
Eenheid-1-1	z	• Doorsturen
Eenheid-2-1	b N	• Flow Owner - De eenheid regelt de stroom
Eenheid-3-1	Y	• Reserve-eigenaar

Dit kan als volgt worden gevisualiseerd:



1. TCP SYN-pakket arriveert vanaf Host-A naar unit-2-1. Unit-2-1 wordt de stroomeigenaar en wordt geselecteerd als regisseur
2. Eenheid-3-1 wordt gekozen tot de back-ueigenaar. De stroomeigenaar stuurt een 'cluster add' eenastbericht op UDP 4193 om de back-ueigenaar te informeren over de stroom
3. TCP SYN/ACK-pakket arriveert van Host-B naar unit-1-1. De stroom is asymmetrisch
4. Unit-1-1 zendt het pakket via de CCL naar de regisseur (eenheid-2-1)
5. Unit-2-1 is ook de eigenaar en breekt het pakje op de interface BUITEN
6. Unit-2-1 zendt het pakket naar host-A
7. Zodra de verbinding wordt beëindigd, stuurt de eigenaar een bericht om de stroominformatie te verwijderen van de back-ueigenaar

Waarneming 3. Opname met sporen toont het asymmetrische verkeer en de omleiding van eenheid-1-1 naar eenheid-2-1

Eenheid-2-1 (eigenaar/directeur)

```
firepower# cluster exec unit unit-2-1 show cap CAPI packet-number 1 trace
1: 18:10:12.842912 192.168.240.50.51844 > 192.168.240.51.80: S 4082593463:4082593463(0) win
29200 <mss 1460,sackOK,timestamp 76258053 0,nop,wscale 7>
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
I (1) got initial, attempting ownership.
```

```
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
I (1) am becoming owner
Eenheid-1-1 (expediteur)
```

```
firepower# cluster exec show cap CAPO packet-number 1 trace
unit-1-1(LOCAL):*****

1: 18:10:12.842317 192.168.240.51.80 > 192.168.240.50.51844: S 2339579109:2339579109(0) ack
4082593464 win 28960 <mss 1460,sackOK,timestamp 513139467 76258053,nop,wscale 7>
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
I (0) am asking director (1).
Terugkeerverkeer (TCP SYN/ACK)
```

Eenheid-2-1 (eigenaar/directeur)

```
firepower# cluster exec unit unit-2-1 show cap CAPO packet-number 2 trace

2: 18:10:12.843660 192.168.240.51.80 > 192.168.240.50.51844: S 2339579109:2339579109(0) ack
4082593464 win 28960 <mss 1460,sackOK,timestamp 513139467 76258053,nop,wscale 7>
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: FULL
I (1) am owner, update sender (0).
```


Phase: 2
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:

Found flow with id 7109, using existing flow

Waarneming 4. Op FTD-gegevensvliegtuigsystemen worden de verbinding creatie en -beëindiging op alle eenheden getoond:

- Eenheid-1-1 (eigenaar)
- Eenheid-2-1 (expediteur)
- Eenheid-3-1 (back-opeigenaar/regisseur)

```
firepower# cluster exec show log | include 51844
unit-1-1(LOCAL):*****
Dec 02 2020 18:10:12: %FTD-6-302022: Built forwarder stub TCP connection for
OUTSIDE:192.168.240.51/80 (192.168.240.51/80) to unknown:192.168.240.50/51844
(192.168.240.50/51844)
Dec 02 2020 18:10:22: %FTD-6-302023: Teardown forwarder TCP connection for
OUTSIDE:192.168.240.51/80 to unknown:192.168.240.50/51844 duration 0:00:09 forwarded bytes
1024001740 Cluster flow with CLU closed on owner

unit-2-1:*****
Dec 02 2020 18:10:12: %FTD-6-302303: Built TCP state-bypass connection 7109 from
INSIDE:192.168.240.50/51844 (192.168.240.50/51844) to OUTSIDE:192.168.240.51/80
(192.168.240.51/80)
Dec 02 2020 18:10:22: %FTD-6-302304: Teardown TCP state-bypass connection 7109 from
INSIDE:192.168.240.50/51844 to OUTSIDE:192.168.240.51/80 duration 0:00:09 bytes 1024001888 TCP
FINs

unit-3-1:*****
Dec 02 2020 18:10:12: %FTD-6-302022: Built backup stub TCP connection for
INSIDE:192.168.240.50/51844 (192.168.240.50/51844) to OUTSIDE:192.168.240.51/80
(192.168.240.51/80)
Dec 02 2020 18:10:22: %FTD-6-302023: Teardown backup TCP connection for
INSIDE:192.168.240.50/51844 to OUTSIDE:192.168.240.51/80 duration 0:00:09 forwarded bytes 0
Cluster flow with CLU closed on owner
```

Case Studie 7. Asymmetric Traffic Engineering (inline), is de eigenaar anders dan de regisseur

De eigenaar is unit-2-1 (er zijn pakketten op zowel binnen- als BUITENinterfaces voor de heruitprojectieverstopping, terwijl unit-3-1 alleen op BUITEN heeft):

```
firepower# cluster exec show cap
unit-1-1(LOCAL):*****
capture CCL type raw-data buffer 33554432 interface cluster [Capturing - 13902 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Capturing - 90 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data reinject-hide interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www

unit-2-1:*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553936 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Buffer Full - 523126 bytes]
```

```
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Buffer Full - 523126 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data reinject-hide interface OUTSIDE [Buffer Full - 524230 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Buffer Full - 523126 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
```

```
unit-3-1:*****
capture CCL type raw-data buffer 33554432 interface cluster [Buffer Full - 33553566 bytes]
capture CAPO type raw-data trace interface OUTSIDE [Buffer Full - 523522 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPO_RH type raw-data reinject-hide interface OUTSIDE [Buffer Full - 523432 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
capture CAPI_RH type raw-data reinject-hide interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.240.50 host 192.168.240.51 eq www
```

Observatie 2. Connection flag analysis for flow with source port 59210

```
firepower# cluster exec show conn addr 192.168.240.51
```

```
unit-1-1(LOCAL):*****
```

```
25 in use, 102 most used
```

```
Cluster:
```

```
fwd connections: 0 in use, 1 most used
```

```
dir connections: 2 in use, 122 most used
```

```
centralized connections: 0 in use, 39 most used
```

```
VPN redirect connections: 0 in use, 0 most used
```

```
Inspect Snort:
```

```
preserve-connection: 0 enabled, 0 in effect, 4 most enabled, 1 most in effect
```

```
TCP OUTSIDE 192.168.240.51:80 INSIDE 192.168.240.50:59210, idle 0:00:03, bytes 0, flags Y
```

```
unit-2-1:*****
```

```
21 in use, 271 most used
```

```
Cluster:
```

```
fwd connections: 0 in use, 2 most used
```

```
dir connections: 0 in use, 28 most used
```

```
centralized connections: 0 in use, 14 most used
```

```
VPN redirect connections: 0 in use, 0 most used
```

```
Inspect Snort:
```

```
preserve-connection: 0 enabled, 0 in effect, 249 most enabled, 0 most in effect
```

```
TCP OUTSIDE 192.168.240.51:80 INSIDE 192.168.240.50:59210, idle 0:00:00, bytes 610132872, flags b N
```

```
unit-3-1:*****
```

```
19 in use, 55 most used
```

```
Cluster:
```

```
fwd connections: 1 in use, 5 most used
```

```
dir connections: 0 in use, 127 most used
```

```
centralized connections: 0 in use, 24 most used
```

```
VPN redirect connections: 0 in use, 0 most used
```

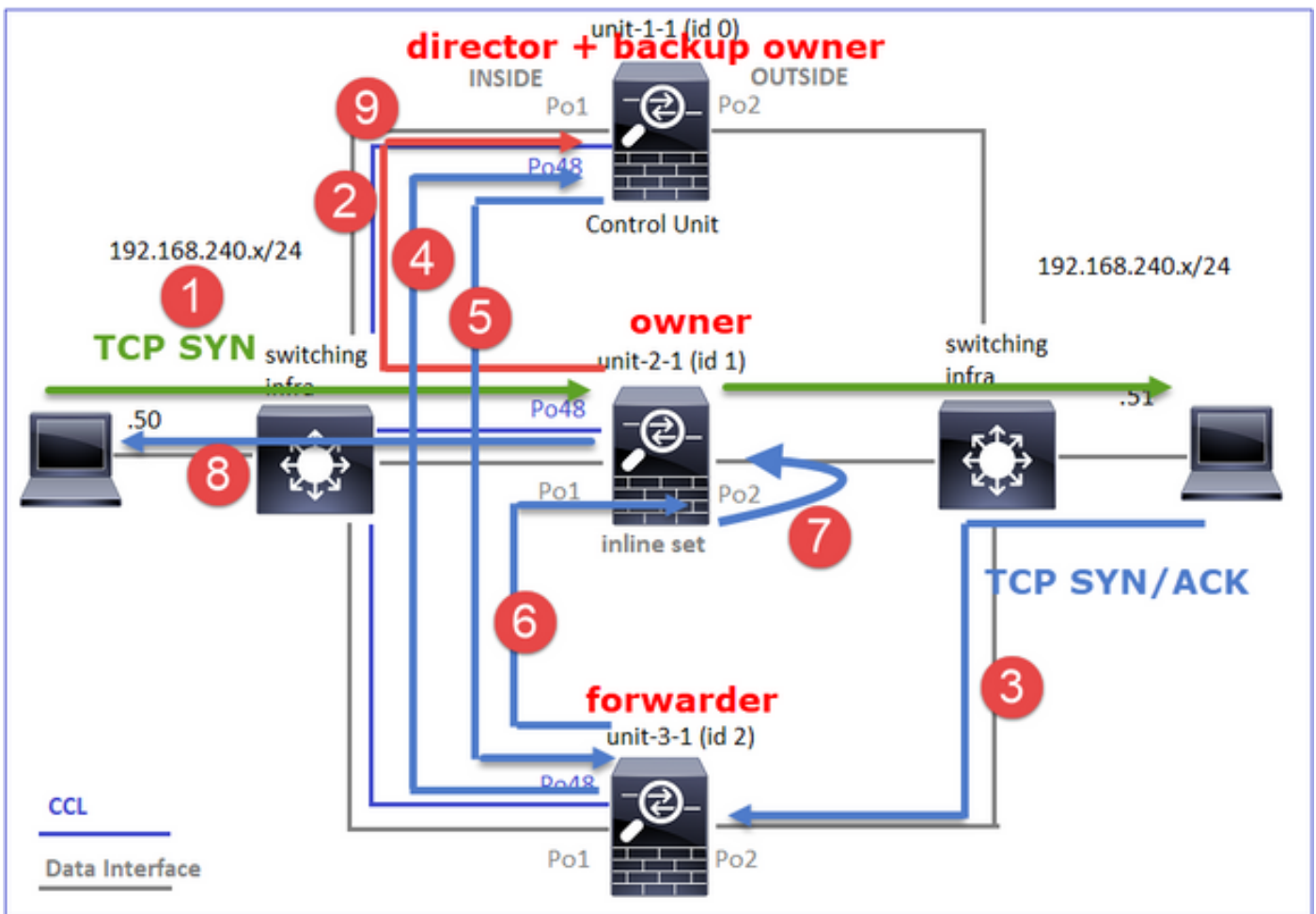
```
Inspect Snort:
```

```
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect
```

```
TCP OUTSIDE 192.168.240.51:80 NP Identity Ifc 192.168.240.50:59210, idle 0:00:00, bytes 0, flags z
```

Eenheid	Vlag	Opmerking
Eenheid-1-1	Y	• Director/back-up-eigenaar
Eenheid-2-1	b N	• Flow Owner - De eenheid regelt de stroom

Dit kan als volgt worden gevisualiseerd:



1. TCP SYN-pakket arriveert vanaf Host-A naar unit-2-1. Unit-2-1 wordt de stroomeigenaar en unit-1-1 wordt geselecteerd als regisseur
2. Unit-1-1 wordt gekozen als de back-opeigenaar (omdat het de regisseur is). De stroomeigenaar stuurt een 'cluster add' eenastbericht op UDP 4193 om de back-opeigenaar te informeren over de stroom
3. TCP SYN/ACK-pakket arriveert van Host-B naar unit-3-1. De stroom is asymmetrisch
4. Unit-3-1 zendt het pakket via de CCL naar de regisseur (eenheid-1-1)
5. Unit-1-1 (regisseur) weet dat de eigenaar unit-2-1 is, het pakket terugstuurt naar de expediteur (eenheid-3-1) en deelt hem mee dat de eigenaar unit-2-1 is
6. Eenheid-3-1 stuurt het pakje naar eenheid-2-1 (eigenaar)
7. Unit-2-1 bevestigt het pakket op interface BUITEN
8. Unit-2-1 zendt het pakket naar host-A
9. Zodra de verbinding wordt beëindigd, stuurt de eigenaar een bericht om de stroominformatie te verwijderen van de back-opeigenaar

Opmerking: Het is belangrijk voor stap 2 (pakket door de CCL) komt voor stap 4 (gegevensverkeer). In een ander geval (bv. de staat van het ras) is de directeur niet op de hoogte van de stroom. Aangezien deze inline is, stuurt u het pakket naar de bestemming door. Als de interfaces niet in een inline set zijn geplaatst, wordt het gegevenspakket verbroken.

Waarneming 3. Opname met sporen toont het asymmetrische verkeer en de uitwisselingen via de CCL:

Voorwaarts verkeer (TCP SYN)

Eenheid-2-1 (eigenaar)

```
firepower# cluster exec unit unit-2-1 show cap CAPI packet-number 1 trace
```

```
1: 09:19:49.760702 192.168.240.50.59210 > 192.168.240.51.80: S 4110299695:4110299695(0) win 29200 <mss 1460,sackOK,timestamp 130834570 0,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CLUSTER-EVENT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Input interface: 'INSIDE'
```

```
Flow type: NO FLOW
```

```
I (1) got initial, attempting ownership.
```

```
Phase: 2
```

```
Type: CLUSTER-EVENT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Input interface: 'INSIDE'
```

```
Flow type: NO FLOW
```

```
I (1) am becoming owner
```

Terugkeerverkeer (TCP SYN/ACK)

Eenheid-3-1 (ID 2 - expediteur) stuurt de verpakking door de CCL naar unit-1-1 (ID 0 - regisseur)

```
firepower# cluster exec unit unit-3-1 show cap CAPO packet-number 1 trace
```

```
1: 09:19:49.760336 192.168.240.51.80 > 192.168.240.50.59210: S 4209225081:4209225081(0) ack 4110299696 win 28960 <mss 1460,sackOK,timestamp 567715984 130834570,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CLUSTER-EVENT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Input interface: 'OUTSIDE'
```

```
Flow type: NO FLOW
```

```
I (2) am asking director (0).
```

Unit-1-1 (regisseur) - Unit-1-1 (ID 0) weet dat de stroomeigenaar unit-2-1 (ID 1) is en stuurt het pakket terug naar unit-3-1 (ID 2 - expediteur)

```
firepower# cluster exec show cap CAPO packet-number 1 trace
```

```
unit-1-1(LOCAL):*****
```

```
1: 09:19:49.761038 192.168.240.51.80 > 192.168.240.50.59210: S 4209225081:4209225081(0) ack 4110299696 win 28960 <mss 1460,sackOK,timestamp 567715984 130834570,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CLUSTER-EVENT
```

Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: STUB

I (0) am director, valid owner (1), update sender (2).

Unit-3-1 (ID 2 - expediteur) krijgt de verpakking door de CCL en stuurt deze naar unit-2-1 (ID 1 - eigenaar)

```
firepower# cluster exec unit unit-3-1 show cap CAPO packet-number 2 trace
```

```
...  
2: 09:19:49.761008 192.168.240.51.80 > 192.168.240.50.59210: S 4209225081:4209225081(0) ack  
4110299696 win 28960 <mss 1460,sackOK,timestamp 567715984 130834570,nop,wscale 7>  
Phase: 1  
Type: CLUSTER-EVENT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Input interface: 'OUTSIDE'  
Flow type: STUB
```

I (2) am becoming forwarder to (1), sender (0).

De eigenaar trekt het pakje in en stuurt het naar de bestemming:

```
firepower# cluster exec unit unit-2-1 show cap CAPO packet-number 2 trace
```

```
2: 09:19:49.775701 192.168.240.51.80 > 192.168.240.50.59210: S 4209225081:4209225081(0) ack  
4110299696 win 28960 <mss 1460,sackOK,timestamp 567715984 130834570,nop,wscale 7>  
Phase: 1  
Type: CLUSTER-EVENT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Input interface: 'OUTSIDE'  
Flow type: FULL
```

I (1) am owner, sender (2).

Waarneming 4. Op FTD-gegevensvliegtuigsystemen worden de verbinding creatie en -beëindiging op alle eenheden getoond:

- Eenheid-1-1 (regisseur/back-upeigenaar)
- Eenheid-2-1 (eigenaar)
- Eenheid-3-1 (expediteur)

```
firepower# cluster exec show log | i 59210
```

```
unit-1-1(LOCAL):*****  
Dec 03 2020 09:19:49: %FTD-6-302022: Built director stub TCP connection for  
INSIDE:192.168.240.50/59210 (192.168.240.50/59210) to OUTSIDE:192.168.240.51/80  
(192.168.240.51/80)  
Dec 03 2020 09:19:59: %FTD-6-302023: Teardown director TCP connection for  
INSIDE:192.168.240.50/59210 to OUTSIDE:192.168.240.51/80 duration 0:00:09 forwarded bytes 0  
Cluster flow with CLU closed on owner
```

```
unit-2-1:*****  
Dec 03 2020 09:19:49: %FTD-6-302303: Built TCP state-bypass connection 14483 from  
INSIDE:192.168.240.50/59210 (192.168.240.50/59210) to OUTSIDE:192.168.240.51/80
```

(192.168.240.51/80)

Dec 03 2020 09:19:59: %FTD-6-302304: **Teardown TCP state-bypass connection** 14483 from INSIDE:192.168.240.50/59210 to OUTSIDE:192.168.240.51/80 duration 0:00:09 bytes 1024003336 TCP FINs

unit-3-1:*****

Dec 03 2020 09:19:49: %FTD-6-302022: **Built forwarder stub TCP connection** for OUTSIDE:192.168.240.51/80 (192.168.240.51/80) to unknown:192.168.240.50/59210 (192.168.240.50/59210)

Dec 03 2020 09:19:59: %FTD-6-302023: **Teardown forwarder TCP connection** for OUTSIDE:192.168.240.51/80 to unknown:192.168.240.50/59210 duration 0:00:09 forwarded bytes 1024003188 Cluster flow with CLU closed on owner

Problemen oplossen

Inleiding Cluster probleemoplossing

De clusterproblemen kunnen worden gecategoriseerd in:

- Problemen met besturingsplane (kwesties in verband met de clusterstabiliteit)
- problemen van het datacentrum (kwesties in verband met het transitovervoer)

Cluster-problemen met datacenters

NAT/PAT gemeenschappelijke problemen

Belangrijke configuratieoverwegingen

- PAT-pools (Port Address Translation) moeten ten minste evenveel IP's beschikbaar zijn als het aantal eenheden in het cluster, bij voorkeur meer IP's dan clusterknooppunten.
- De standaardinstelling is **dat de opdrachten per sessie** moeten worden ingeschakeld, tenzij er een specifieke reden is om ze uit te schakelen. Elk PAT-verlengstuk dat is gebouwd voor een verbinding die **per sessie** uitgeschakeld is, wordt altijd verwerkt door de control-knoopeenheid in het cluster, wat verslechtering van de prestaties kan veroorzaken.

Gebruik van een hoog PAT-poolbereik vanwege verkeer dat afkomstig is van lage poorten en dat leidt tot een onevenwichtigheid in cluster IP

De FTD verdeelt een PAT IP in "bereik" en probeert de extensie in hetzelfde bronbereik te behouden. Deze tabel laat zien hoe een bronpoort wordt vertaald naar een wereldwijde poort binnen hetzelfde bronbereik.

Originele SRC-poort	Vertaalde SRC-poort
1-511	1-511
512-1023	512-1023
1024-65535	1024-65535

Wanneer een bronpoortbereik volledig is en een nieuw PAT-bereik van dat bereik moet worden toegewezen, gaat FTD naar de volgende IP om nieuwe vertalingen voor dat bronpoortbereik toe te wijzen.

Symptomen

Connectiviteitsproblemen voor NAT-verkeer dat de cluster overbrengt

Verificatie

```
# show nat pool
```

VHBK-gegevensbestanden tonen PAT-polaire uitputting:

```
Dec 9 09:00:00 192.0.2.10 FTD-FW %ASA-3-202010: PAT pool exhausted. Unable to create TCP connection from Inside:192.0.2.150/49464 to Outside:192.0.2.250/20015
```

```
Dec 9 09:00:00 192.0.2.10 FTD-FW %ASA-3-202010: PAT pool exhausted. Unable to create TCP connection from Inside:192.0.2.148/54141 to Outside:192.0.2.251/443
```

Beperken

Configureer het NAT platte poortbereik en neem reservepoorten op.

Daarnaast kan je in post-6.7/9.15.1 alleen eindigen met een ongebalanceerde poortblokdistributie wanneer knooppunten de cluster verlaten/aansluiten met een groot achtergrondverkeer dat aan PAT onderhevig is. De enige manier waarop het zich herstelt is wanneer havenblokken worden vrijgemaakt om over knooppunten te worden herverdeeld.

Bij distributie op basis van poortblokken, wanneer een knooppunt wordt toegewezen met bijvoorbeeld 10 poortblokken zoals pb-1, pb-2 ... pb-10. Het knooppunt begint altijd met het eerste beschikbare poortblok en wijst er een willekeurige poort toe totdat het uitblaast. De toewijzing gaat alleen naar het volgende havenblok als alle havenblokken tot dat punt zijn uitgeput.

Bijvoorbeeld, als een host 512 verbindingen aanlegt, wijst de unit in kaart gebrachte poorten toe voor al die 512 verbindingen van pb-1 willekeurig. Nu, met al deze 512 verbindingen actief, wanneer de host de 513e verbinding vestigt aangezien pb-1 is uitgeput, beweegt hij naar pb-2 en wijst er een willekeurige poort van toe. Ga er opnieuw van uit dat 513 verbindingen de 10e verbinding is voltooid en klaarde één poort beschikbaar in pb-1. Als de host de 514e verbinding aanlegt, wijst de cluster unit een toegewezen poort toe vanaf pb-1 en niet pb-2, omdat pb-1 nu een vrije haven heeft (die werd vrijgegeven als onderdeel van de 10e verbindingverwijdering).

Het belangrijkste om in gedachten te houden is dat de toewijzing plaatsvindt uit het eerste beschikbare havenblok met vrije havens zodat de laatste havenblokken altijd beschikbaar zijn voor herverdeling in een normaal geladen systeem. Daarnaast wordt PAT doorgaans gebruikt voor kortdurende verbindingen. De kans dat een havenblok in een kortere tijd beschikbaar komt is zeer hoog. Dus de tijd die nodig is om de pooldistributie in evenwicht te brengen kan verbeteren met poortop blok gebaseerde pooldistributie.

Indien echter alle havenblokken, van pb-1 tot pb-10, uitgeput zijn of ieder havenblok een haven heeft voor een lange-termijnverbinding, worden de havenblokken nooit snel bevrijd en herverdeeld. In een dergelijk geval is de minst versturende benadering:

1. Identificeer knooppunten met excessieve poortblokken (**toon NAT pool clustersamenvatting**).
2. Identificeer de minst gebruikte poortblokken op dat knooppunt (**toon nat pool ip <addr> details**).
3. Heldere limieten voor dergelijke poortblokken (**duidelijk uitvouwen mondiaal <addr>-logbestand'start-end'**) om deze beschikbaar te maken voor herdistributie.

Waarschuwing: Dit verstoort de relevante verbindingen.

Kan niet bladeren naar dual-kanaals websites (zoals webmail, bankieren, enzovoort) of naar SSO-

websites als er sprake is van een omleiding naar een andere bestemming

Symptomen

Kan niet naar dual-kanaals websites bladeren (zoals webmail, bankwebsites, enz.) Wanneer een gebruiker verbinding maakt met een website waarop de client een tweede socket/verbinding moet openen en de tweede verbinding wordt gehashed naar een clusterlid dat afwijkt van de eerste verbinding naar wie de eerste verbinding is gehashed en het verkeer gebruikt een IP PAT-pool, wordt het verkeer teruggezet door de server omdat het de verbinding ontvangt van een ander openbaar IP-adres.

Verificatie

Neem datatoolcluster-opnamen om te zien hoe de getroffen doorvoerstroam wordt behandeld. In dit geval, komt een TCP reset uit de doelwebsite.

Beperking (pre-6.7/9.15.1)

- Let op als toepassingen met meerdere sessies meerdere in kaart gebrachte IP-adressen gebruiken.
- Gebruik de opdracht **Inat poolcluster summiere** opdracht tonen om te controleren of de pool gelijkmatig wordt verdeeld.
- Gebruik de **cluster exec show conn** opdracht om te controleren of het verkeer goed gelijkmatig verdeeld is.
- Gebruik de opdracht **Inat pool cluster ip <adres> detail** om het poolgebruik van kleverige IP te controleren.
- Schakel syslog 305021 (6.7/9.15) in om te zien welke verbindingen geen kleverige IP hebben gebruikt.
- U kunt meer IP's aan de PAT-pool toevoegen of het algoritme voor de laadbalans op aangesloten switches fijnafstemmen.

Over het taakverdeling voor andere kanalen:

- Voor niet-FP9300 en als verificatie via één server plaatsvindt: Stel het taakverdeling-algoritme van het ether-kanaal op de aangrenzende switch van Bron IP/Port en Destination IP/Port in op Bron IP en Bestemming IP.
- Voor niet-FP9300 en indien verificatie plaatsvindt via meerdere servers: Stel het taakverdeling-algoritme voor andere kanalen op de aangrenzende switch van Bron IP/Port en Destination IP/Port in op Bron IP.
- Voor FP9300: Op het FP9300-chassis is het belastingsbalanceringsalgoritme vastgelegd als **bron-dest-ip bron-dest-mac** en kan niet worden gewijzigd. In dit geval moet u FlexConfig gebruiken om **xlate per sessie ontkende** opdrachten aan de configuratie van het FTD toe te voegen om verkeer voor bepaalde IP-adressen van de bestemming (voor de problematische/oncompatibele toepassingen) te dwingen die alleen door het controleknooppunt in het intra-chassis cluster moeten worden verwerkt. Het werkspoor heeft deze bijwerkingen: Geen taakverdeling voor het anders vertaalde verkeer (alles gaat naar het controleknooppunt). Potentieel voor verlenging van slots om af te lopen (en heeft een negatieve invloed op NAT-vertaling voor ander verkeer op het controleknoop). Verminderde schaalbaarheid van het intra-chassis cluster.

Lage clusterprestaties als gevolg van al het verkeer dat naar de controleknoop wordt gestuurd

omdat er niet genoeg PAT-IP's in de pools zijn

Symptomen

Er zijn niet genoeg PAT IP's in de cluster om een vrije IP aan de gegevensknooppunten toe te wijzen en daarom wordt al het verkeer dat onderworpen is aan de PAT-configuratie doorgestuurd naar het controleknooppunt voor verwerking.

Verificatie

Gebruik de opdracht **Show nat pool** cluster om de toewijzingen voor elke eenheid te zien en bevestig dat zij allemaal minstens één IP in de pool bezitten.

Beperken

Zorg er bij pre-6.7/9.15.1 voor dat u een PAT-pool van grootte hebt die ten minste gelijk is aan het aantal knooppunten in het cluster. In post-6.7/9.15.1 met PAT pool, wijst u poortblokken van alle PAT pool IPs toe. Als het PAT-poolgebruik echt hoog is, wat leidt tot frequente uitputting van de pool, moet u de PAT-pooladoptie vergroten (zie de FAQ-sectie)

Lage prestaties door al het verkeer dat naar het bedieningspaneel wordt verzonden omdat de wachtwoorden niet per sessie zijn ingeschakeld

Symptomen

Een groot aantal snelle UDP-back-upstromen wordt verwerkt door het knooppunt voor clusterbeheer, dat invloed kan hebben op de prestaties.

Achtergrond

Alleen verbindingen die limieten gebruiken die per sessie aan kunnen worden gekoppeld, kunnen worden verwerkt door een gegevensknooppunt dat PAT gebruikt. Gebruik de opdracht **show run all xlate** om de uitloop per sessie te zien

Als deze optie is ingeschakeld, wordt de verlooptdatum onmiddellijk afgebroken wanneer de aangesloten verbinding wordt afgebroken. Hierdoor wordt de verbinding per seconde verbeterd wanneer de verbindingen aan PAT worden onderworpen. Niet per sessie loopt nog 30 seconden nadat de bijbehorende verbinding is afgebroken, en als het verbindingstarief hoog genoeg is, kunnen de beschikbare 65k TCP/UDP-poorten op elke wereldwijde IP in een korte tijd worden gebruikt.

Standaard is al het TCP-verkeer per-expate ingeschakeld en is alleen het UDP DNS-verkeer per sessie ingeschakeld. Dit betekent dat al het niet-DNS UDP-verkeer naar het controleknooppunt wordt verzonden voor verwerking.

Verificatie

Gebruik deze opdracht om de verbinding en pakketdistributie tussen de clustereenheden te controleren:

```
firepower# show cluster info conn-distribution
firepower# show cluster info packet-distribution
```

```
firepower# show cluster info load-monitor
```

Gebruik het **cluster exec tonen conn** opdracht om te zien welke clusterknooppunten de UDP verbindingen bezitten.

```
firepower# cluster exec show conn
```

Gebruik deze opdracht om het poolgebruik over clusterknooppunten te begrijpen.

```
firepower# cluster exec show nat pool ip
```

Beperken

Configureer de PAT per sessie (**licentie udp** opdracht) voor het relevante verkeer (bijvoorbeeld UDP). Voor ICMP, kunt u niet van de standaard multi-sessie PAT veranderen en daarom wordt het ICMP-verkeer altijd door het besturingsknooppunt verwerkt wanneer er PAT is ingesteld.

PAT-pool distributie wordt onevenwichtig als er knooppunten weggaan/zich bij het cluster aansluiten.

Symptomen

- Connectiviteitsproblemen sinds PAT IP-toewijzing kunnen in de loop der tijd onevenwichtig worden als gevolg van eenheden die het cluster verlaten en er zich bij aansluiten.
- In post-6.7/9.15.1 kunnen er gevallen zijn waarin het pas aangesloten knooppunt niet genoeg poortblokken kan krijgen. Een knooppunt dat geen poortblok heeft, wijst verkeer terug naar het controleknooppunt. Een knooppunt met ten minste één poortblok verwerkt het verkeer en laat het vallen zodra de pool is uitgeput.

Verificatie

- De data plane syslogs tonen berichten als:

```
%ASA-3-202010: NAT pool exhausted. Unable to create TCP connection from inside:192.0.2.1/2239 to outside:192.0.2.150/80
```

- Gebruik de opdracht van de **show nat pool cluster summary** om de pooldistributie te identificeren.
- Gebruik de **clusterexec toont nat pool ip <addr> detail** opdracht om het poolgebruik tussen clusterknooppunten te begrijpen.

Beperken

- Voor de pre-6.7/9.15.1 worden een aantal omwentelingen beschreven in <https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvd10530>
- Los dit gebruik in post-6.7/9.15.1 op de **heldere** verbinding van **<ip>begin-end** opdracht om sommige van de havenblokken op andere knopen voor herdistributie aan de vereiste knooppunten handmatig te ontruimen.

Symptomen

Belangrijke aansluitingsproblemen voor verkeer dat PATed door de cluster is. Dit komt doordat het FTD-datalevlak, per ontwerp, GARP niet verstuurt voor wereldwijde NAT-adressen.

Verificatie

De ARP-tabel van de direct aangesloten apparaten toont het MAC-adres van de clustergegevensinterface na een wijziging van het controleknooppunt:

```
root@kali2:~/tests# arp -a
? (192.168.240.1) at f4:db:e6:33:44:2e [ether] on eth0
root@kali2:~/tests# arp -a
? (192.168.240.1) at f4:db:e6:9e:3d:0e [ether] on eth0
```

Beperken

Configuratie van statische (virtuele) MAC op clustergegevensinterfaces.

Aansluitingen waarvoor PAT is defect

Symptomen

Connectiviteitsproblemen voor verkeer dat PATed door het cluster is.

Verificatie/beperking

- Zorg ervoor dat de configuratie goed is gerepliceerd.
- Zorg ervoor dat de pool gelijkmatig verdeeld is.
- Zorg ervoor dat het eigenaarschap van de pool geldig is.
- Geen toename van mislukkingteller in **show asp clusterteller**.
- Zorg ervoor dat er stromen tussen regisseur en expediteur met de juiste informatie worden gecreëerd.
- Bevestig als reservekopieën gecreëerd, bijgewerkt en zoals verwacht worden schoongemaakt.
- Bevestig als er datums worden gemaakt en beëindigd volgens het gedrag per sessie.
- Schakel "debug nat 2" in voor een indicatie van fouten. Deze uitvoer kan bijvoorbeeld zeer veel lawaai veroorzaken.

```
firepower# debug nat 2
nat: no free blocks available to reserve for 192.168.241.59, proto 17
nat: no free blocks available to reserve for 192.168.241.59, proto 17
nat: no free blocks available to reserve for 192.168.241.58, proto 17
nat: no free blocks available to reserve for 192.168.241.58, proto 17
nat: no free blocks available to reserve for 192.168.241.57, proto 17
```

U stopt het debug:

```
firepower# un all
```

- Schakel verbinding en NAT-gerelateerde systemen in om de informatie te correleren met een defecte verbinding.

ASA and FTD Clusters PAT-verbeteringen (na 9.15 en 6.7)

Wat is er veranderd?

De PAT-bewerking is opnieuw ontworpen. Individuele IP's worden niet meer verdeeld onder elk van de clusterleden. In plaats daarvan worden de PAT IP(s) in poortblokken verdeeld en deze poortblokken gelijkmatig (zoveel mogelijk) verdeeld tussen de clusterleden, in combinatie met IP-kleverigheid.

Het nieuwe ontwerp gaat in op deze beperkingen (zie het vorige hoofdstuk):

- Toepassingen voor meerdere sessies worden beïnvloed door een gebrek aan clusterbrede IP-kleverheid.
- De vereiste om een PAT-pool van grootte te hebben die ten minste gelijk is aan het aantal knooppunten in de cluster.
- PAT-pooldistributie wordt onevenwichtig als er knooppunten weggaan/zich bij het cluster aansluiten.
- Geen symbolen die duiden op een onbalans in het PAT-podium.

Technisch gezien is er in plaats van de standaard poortbereiken 1-511, 512-1023 en 1024-65535 nu 1024-65535 als het standaard poortbereik voor PAT. Dit standaardbereik kan worden uitgebreid tot geprivilegieerd poortbereik 1-1023 voor regelmatig PAT (inclusief-reserve optie).

Dit is een voorbeeld van een PAT-poolconfiguratie op FTD 6.7. Kijk voor meer details in de configuratiegids:

NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

Type:
Dynamic

Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* net_192.168.240.0 +	Translated Source: Address +
Original Destination: Address +	Translated Destination: + +
Original Source Port: + +	Translated Source Port: + +
Original Destination Port: + +	Translated Destination Port: + +

Interface Objects Translation **PAT Pool** Advanced

Enable PAT Pool

PAT:

Address +

Use Round Robin Allocation

Extended PAT Table

Flat Port Range ⓘ This option always enabled on device from v6.7.0 irrespective of its configured value.

Include Reserve Ports

Block Allocation

Aanvullende informatie over probleemoplossing voor PAT

FTD-gegevensvliegtuigsyslogs (post-6.7/9.15.1)

Er wordt een systeem voor het ongeldig maken van de kleverigheid gegenereerd wanneer alle poorten zijn uitgeput in de kleverige IP op een clusterknooppunt en de toewijzing verplaatst naar de volgende beschikbare IP met gratis poorten. bijvoorbeeld

```
%ASA-4-305021: Ports exhausted in pre-allocated PAT pool IP 192.0.2.100 for host 198.51.100.100
Allocating from new PAT pool IP 203.0.113.100.
```

Er wordt een systeem met een onevenwichtigheid gegenereerd op een knooppunt wanneer het zich in het cluster voegt en er wordt geen of ongelijk aandeel in poortblokken gevonden, bijvoorbeeld.

```
%ASA-4-305022: Cluster unit ASA-4 has been allocated 0 port blocks for PAT usage. All units
should have at least 32 port blocks.
```

```
%ASA-4-305022: Cluster unit ASA-4 has been allocated 12 port blocks for PAT usage. All units
should have at least 32 port blocks.
```

Opdrachten tonen

Toestatus van pool

In de **show nat pool cluster summie** output, voor elk PAT IP adres, moet er geen verschil van meer dan 1 havenblok over de knopen in een evenwichtig distributiescenario zijn. Voorbeelden van een evenwichtige en onevenwichtige poortverdeling.

```
firepower# show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1, unit-3-1
IP OUTSIDE:ip_192.168.241.57-59 192.168.241.57 (126 - 42 / 42 / 42)
IP OUTSIDE:ip_192.168.241.57-59 192.168.241.58 (126 - 42 / 42 / 42)
IP OUTSIDE:ip_192.168.241.57-59 192.168.241.59 (126 - 42 / 42 / 42)
```

Onevenwichtige verdeling:

```
firepower# show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-4-1, unit-2-1, unit-3-1
```

IP outside:src_map 192.0.2.100 (128 - 32 / 22 / 38 / 36)

Beursstatus

In de **show nat pool cluster** uitvoer moet er geen enkel havenblok zijn met of eigenaar of reserve als "ONBEKEND". Als er een is, duidt dat op een probleem met de communicatie van het pooleigendom. Voorbeeld:

```
firepower# show nat pool cluster | in
```

```
[3072-3583], owner unit-4-1, backup <UNKNOWN>  
[56832-57343], owner <UNKNOWN>, backup <UNKNOWN>  
[10240-10751], owner unit-2-1, backup <UNKNOWN>
```

Boekhouding van de toewijzing van havens in havenblokken

De opdracht **Inat pool weergeven** wordt uitgebreid met extra opties om gedetailleerde informatie evenals gefilterde uitvoer weer te geven. Voorbeeld:

```
firepower# show nat pool detail  
TCP PAT pool INSIDE, address 192.168.240.1, range 1-1023, allocated 0  
TCP PAT pool INSIDE, address 192.168.240.1, range 1024-65535, allocated 18  
UDP PAT pool INSIDE, address 192.168.240.1, range 1-1023, allocated 0  
UDP PAT pool INSIDE, address 192.168.240.1, range 1024-65535, allocated 20  
TCP PAT pool OUTSIDE, address 192.168.241.1, range 1-1023, allocated 0  
TCP PAT pool OUTSIDE, address 192.168.241.1, range 1024-65535, allocated 18  
UDP PAT pool OUTSIDE, address 192.168.241.1, range 1-1023, allocated 0  
UDP PAT pool OUTSIDE, address 192.168.241.1, range 1024-65535, allocated 20  
UDP PAT pool OUTSIDE, address 192.168.241.58  
range 1024-1535, allocated 512  
range 1536-2047, allocated 512  
range 2048-2559, allocated 512  
range 2560-3071, allocated 512  
...  
unit-2-1:*****  
UDP PAT pool OUTSIDE, address 192.168.241.57  
range 1024-1535, allocated 512 *  
range 1536-2047, allocated 512 *  
range 2048-2559, allocated 512 *
```

Opmerking: "*" geeft aan dat het een door back-up beschermd poortblok is

Om dit op te lossen moet u de **heldere globale <ip> poort <start-end>** opdracht gebruiken om bepaalde poortblokken op andere knooppunten voor herdistributie naar de vereiste knooppunten handmatig te verwijderen.

Handmatig geactiveerd herdistributie van poortblokken

- In een productienetwerk met constant verkeer, wanneer een knooppunt vertrekt en zich bij het cluster voegt (waarschijnlijk door een traceback), kunnen er gevallen zijn waarin het geen gelijk deel van de pool kan krijgen of, in het ergste geval, het geen poortblok kan krijgen.
- Gebruik het bevel van de **show nat pool** om te identificeren welke knoop meer havenblokken dan vereist heeft.
- Op de knooppunten die meer poortblokken bezitten, gebruik de opdracht van de **show nat**

pool ip <addr> details om de poortblokken met het minste aantal toewijzingen te ontdekken.

- Gebruik de **duidelijke** globale **<adres>**-pagina-opdracht **<start-end>** om vertalingen te verwijderen die gemaakt zijn uit die poortblokken, zodat ze beschikbaar komen voor herdistributie naar de vereiste knooppunten, bijvoorbeeld.

```
firepower# show nat pool detail | i 19968
    range 19968-20479, allocated 512
    range 19968-20479, allocated 512
    range 19968-20479, allocated 512
```

```
firepower# clear xlate global 192.168.241.57 gport 19968-20479
INFO: 1074 xlates deleted
```

Vaak gestelde vragen (FAQ) voor post-6.7/9.15.1 PAT

Q. Als u het aantal IP's beschikbaar hebt voor het aantal beschikbare eenheden in het cluster, kunt u 1 IP per eenheid nog steeds als optie gebruiken

A. Niet meer en er is geen toggle om te switches tussen op IP-adressen gebaseerde vs op haven block gebaseerde pooldistributiesystemen.

Het oudere schema van IP-adresgebaseerde pooldistributie resulteerde in toepassingsfouten van meerdere sessies, waarbij meerdere verbindingen (die deel uitmaken van één toepassingstransactie) van een host worden gebalanceerd op verschillende knooppunten van het cluster en dus vertaald worden door verschillende in kaart gebrachte IP-adressen die naar de doelservers leiden om ze te zien als bron van verschillende entiteiten.

En met het nieuwe op poortblokken gebaseerde distributieschema, ook al kunt u nu met zo weinig werken als één PAT IP-adres, wordt het altijd aanbevolen om voldoende PAT IP-adressen te hebben gebaseerd op het aantal verbindingen dat vereist is om PATed te hebben.

Q. Kan u nog een pool van IP adressen voor de PAT pool voor de cluster hebben?

A. Ja, dat kan. Poortblokken van alle PAT pool IP's worden verdeeld over de clusterknooppunten.

Q. Als u een aantal IP-adressen voor de PAT-pool gebruikt, is hetzelfde blok poorten dat per IP-adres aan elk lid wordt opgegeven?

A. Nee, elke IP wordt onafhankelijk verdeeld.

Q. Alle clusterknooppunten hebben alle openbare IP's, maar slechts een subset van poorten? Als dit het geval is, is het dan gegarandeerd dat elke keer dat de bron-IP dezelfde openbare IP gebruikt?

A. Klopt, elk PAT IP is gedeeltelijk eigendom van elk knooppunt. Als een gekozen openbare IP op een knooppunt is uitgeput, wordt er een syslog gegenereerd om aan te geven dat kleverige IP niet kan worden bewaard, en wordt de toewijzing verplaatst naar de volgende beschikbare openbare IP. Of het nu een standalone, HA of clustertoepassing is, IP-kleverigheid is altijd op een best-inspanningsbasis afhankelijk van de beschikbaarheid van de pool.

Q. is alles gebaseerd op één enkel IP-adres in het PAT-bestand maar is niet van toepassing als u meer dan één IP-adres in het PAT-bestand gebruikt?

A. Het is ook van toepassing op meerdere IP-adressen in PAT Pool. Poortblokken van elk IP in de PAT Pool worden verdeeld over clusterknooppunten. Elk IP-adres in de PAT-pool wordt over alle leden in het cluster verdeeld. Dus, als je een klasse C van adressen in de PAT pool hebt, heeft elk clusterlid poortpools van elk van de PAT pool adressen.

Werk het met CGNAT?

A. Ja, CGNAT wordt ook ondersteund. CGNAT, ook bekend als "bloktoewijzing" PAT heeft een standaardblok grootte van '512' die kan worden gewijzigd door **het** vergroten van de **bloktoewijzing grootte** CLI. In het geval van een regelmatig dynamisch PAT (niet-CGNAT) is de blok grootte altijd '512', dat vast en niet-aanpasbaar is.

Q. Als de eenheid het cluster verlaat, verdeelt de controleknoop het poortblok aan andere eenheden of houdt het zich aan zichzelf?

A. Elk havenblok heeft een eigenaar en back-up. Telkens wanneer een expate van een havenblok wordt gemaakt, wordt het ook herhaald aan de reserveknoop van het havenblok. Wanneer een knooppunt het cluster verlaat, heeft het reserveknooppunt alle poortblokken en alle huidige verbindingen. Het reserveknooppunt, aangezien het de eigenaar van deze extra poortblokken is geworden, selecteert een nieuwe reserve voor hen en herhaalt alle huidige verwijzingen naar dat knooppunt om mislukkingsscenario's te behandelen.

Welke maatregelen kunnen op basis van die waarschuwing worden genomen om de kleverigheid te handhaven?

A. Er zijn twee mogelijke redenen waarom kleverigheid niet behouden kan worden.

Reden-1: Het verkeer is niet juist geladen, waardoor een van de knooppunten een hoger aantal verbindingen ziet dan anderen, wat tot de specifieke kleverige IP-uitputting leidt. Dit kan worden aangepakt als u ervoor zorgt dat het verkeer gelijkmatig over clusterknooppunten wordt verdeeld. Bijvoorbeeld op een FPR41xx-cluster, tweet het taakverdeling-algoritme op verbonden switches. Zorg er op een FPR9300-cluster voor dat er evenveel blades zijn in het chassis.

Reden-2: Het gebruik van PAT-pool is zeer hoog, hetgeen leidt tot frequente uitputting van de pool. Om dit aan te pakken moet u het PAT-poolformaat vergroten.

Hoe wordt de ondersteuning van het uitgebreide sleutelwoord verwerkt? Toont het een fout en voorkomt het gehele NAT bevel om tijdens upgrade toegevoegd te worden of het verwijdert het uitgebreide sleutelwoord en toont een waarschuwing?

A. De "uitgebreide" optie PAT wordt niet ondersteund in Cluster vanaf ASA 9.15.1/FP 6.7. De configuratieoptie is niet uit een van CLI/ASDM/CSM/FMC verwijderd. Indien geconfigureerd (direct of indirect via een upgrade) wordt u gecommuniceerd met een waarschuwingsbericht en de configuratie is geaccepteerd, maar u ziet de uitgebreide functionaliteit van PAT in actie niet.

Q. Is het hetzelfde aantal vertalingen als gelijktijdige verbindingen?

A. In pre-6.7/9.15.1 was het 1-65535, omdat de bronhavens nooit veel worden gebruikt in de periode 1-1024, maar in feite 1024-65535 (64512 verbindingen). In de post6.7/9.15.1 implementatie met 'plat' als standaardgedrag, is het 1024-65535. Maar als je de 1-1024 wilt gebruiken, kan je de "inclusieve reserve" optie gebruiken.

Q. Als het knooppunt zich bij het cluster terugsluit, heeft het de oude reserveknoop als "back-up"

en geeft dat reserveknooppunt het oude poortblok aan?

A. Het hangt af van de beschikbaarheid van havenblokken op dat moment. Wanneer een knooppunt het cluster verlaat, worden alle poortblokken verplaatst naar de reserveknoop. Het is dan het controleknoop dat gratis poortblokken accumuleert en het naar de vereiste knooppunten distribueert.

Q. Als de staat van de controleknoop verandert, wordt een nieuw gekozen controleknooppunt gehandhaafd, wordt de PAT-bloktoewijzing gehandhaafd of worden de poortblokken opnieuw toegewezen op basis van het nieuwe controleknooppunt?

A. Het nieuwe controleknooppunt heeft inzicht in welke blokken zijn toegewezen en welke gratis zijn en vanaf dat moment beginnen.

Q. Is het maximum aantal uitgangen hetzelfde als het maximum aantal gelijktijdige verbindingen met dit nieuwe gedrag?

A. Ja. Het maximum aantal uittreksels is afhankelijk van de beschikbaarheid van PAT-poorten. Het heeft niets te maken met het max aantal gelijktijdige verbindingen. Als u slechts 1 adres toestaat, hebt u 65535 mogelijke verbindingen. Als u meer nodig hebt, moet u meer IP adressen toewijzen. Als er genoeg adressen/poorten zijn, kunt u maximaal gelijktijdige verbindingen bereiken.

Q. Wat is het proces van de toewijzing van havenblokken wanneer een nieuw clusterlid wordt toegevoegd? Wat gebeurt er als een clusterlid wordt toegevoegd door de herstart?

A. Poortblokken worden altijd verdeeld door het bedieningspaneel. Poortblokken worden alleen aan een nieuw knooppunt toegewezen als er vrije poortblokken zijn. Vrije havenblokken betekenen dat er geen verbinding wordt onderhouden door een in kaart gebrachte haven binnen het havenblok.

Verder berekent elk knooppunt na opnieuw toetreden het aantal blokken dat het kan aanleggen. Als een knooppunt meer blokken bevat dan het zou moeten, geeft het deze extra poortblokken op aan het controleknoop zodra en wanneer deze beschikbaar komen. Het controleknooppunt wijst ze vervolgens toe aan het nieuw aangesloten dataknooppunt.

Q. wordt het ook alleen TCP- en UDP-protocollen of SCTP ondersteund?

A. SCTP werd nooit ondersteund met dynamisch PAT. Voor SCTP-verkeer is de aanbeveling alleen om een statisch netwerkobject NAT te gebruiken.

Q. Als een knooppunt uit blokpoorten loopt, zet het dan pakketten neer en gebruikt u niet het volgende beschikbare IP-blok?

A. Nee, het valt niet meteen. Het gebruikt beschikbare poortblokken van het volgende PAT IP. Als alle poortblokken over alle PAT IP's zijn uitgeput, vermindert het verkeer.

Q. Om de overbelasting van het controleknooppunt in een clusterupgradevenster te voorkomen, is het beter om eerder een nieuwe controle handmatig te selecteren (bijvoorbeeld halverwege een 4-unit-clusterupgrade) in plaats van te wachten tot alle verbindingen op de controleknoop worden verwerkt?

A. De controle moet het laatst worden bijgewerkt. Dit komt doordat, wanneer het controleknooppunt de nieuwere versie draait, dit geen pooldistributie initieert tenzij alle

knooppunten de nieuwere versie uitvoeren. Bovendien, wanneer een upgrade wordt uitgevoerd, negeren alle gegevensknooppunten met een nieuwere versie pooldistributieberichten van een controleknoop als er een oudere versie wordt uitgevoerd.

Om dit in detail te verklaren, overweeg een clusterimplementatie met 4 knopen A, B, C, en D met A als controle. Hier zijn de typische hitless upgradestappen:

1. Download een nieuwe versie op elk van de knooppunten.
2. Opnieuw laden van eenheid "D". Alle verbindingen, limieten worden verplaatst naar de reserveknoop.
3. Eenheid "D" verschijnt en:
 - a. Verwerkt PAT-configuratie
 - b. Breekt elke PAT IP in poortblokken
 - c. Heeft alle poortblokken in niet-toegewezen staat
 - d. Hiermee wordt de oudere versie van PAT-clusterberichten die van de controle zijn ontvangen, genegeerd
 - e. Richt alle PAT-verbindingen op Master
4. Neem op dezelfde manier andere knooppunten met de nieuwe versie op.
5. Opnieuw laden van de eenheid A. Aangezien er geen back-up is voor de bediening, worden alle bestaande verbindingen verbroken
6. De nieuwe controle start de distributie van havenblokken in een nieuwere indeling
7. Eenheid "A" valt samen met de distributieboodschappen van havenblokken en kan deze accepteren en handelen

fragmentatieverwerking

Symptoom

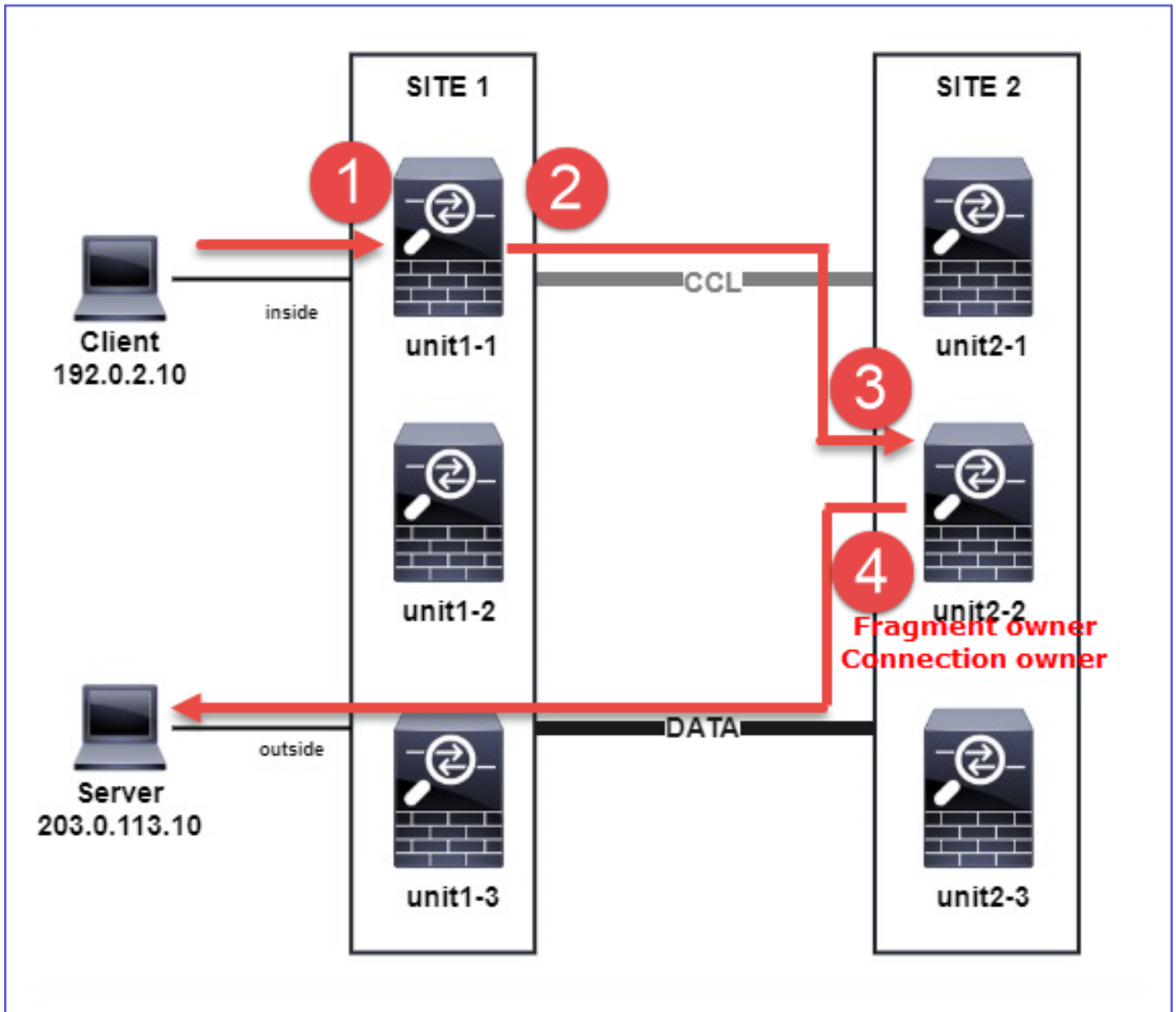
In intersite clusterimplementaties kunnen gefragmenteerde pakketten die moeten worden verwerkt in 1 specifieke locatie (site-local traffic shaping), nog steeds worden verzonden naar de eenheden op andere locaties, omdat een van deze locaties de eigenaar van het fragment kan hebben.

In clusterlogica is een extra rol gedefinieerd voor verbindingen met gefragmenteerde pakketten: **eigenaar van fragment**.

Voor gefragmenteerde pakketten bepalen clustereenheden die een fragment ontvangen een fragment-eigenaar op basis van een hash van het IP-adres van de fragmentatiebron, het IP-adres van de bestemming en de pakket-ID. Alle fragmenten worden vervolgens doorgestuurd naar de eigenaar van het fragment over de cluster control link. Fragmenten kunnen worden geladen in verschillende clustereenheden omdat alleen het eerste fragment de 5-tuple bevat die wordt gebruikt in de taakverdeling van de switch. Andere fragmenten bevatten niet de bron- en doelpoorten en kunnen worden geladen in een ander cluster. De eigenaar van het fragment assembleert het pakket tijdelijk opnieuw, zodat het de regisseur kan bepalen op basis van een hash van het bron/bestemming IP-adres en de poorten. Als het om een nieuwe verbinding gaat,

wordt de eigenaar van het fragment de verbindingseigenaar. Als het een bestaande verbinding is, stuurt de fragmenteigenaar alle fragmenten door naar de verbindingseigenaar over de clustercontrol link. De verbindingseigenaar monteert vervolgens alle fragmenten.

Overweeg deze topologie met de stroom van een gefragmenteerd ICecho verzoek van de cliënt aan de server:



Om de volgorde van bewerkingen te begrijpen, zijn er pakketvastlegging voor meerdere groepen binnen, buiten, achter en achter de clustercontrole-interfaces ingesteld met de sporenoptie. Bovendien wordt een pakketvastlegging met de optie voor de herprojectie-verstoppers ingesteld op de interne interface.

```
firepower# cluster exec capture capi interface inside trace match icmp any any
firepower# cluster exec capture capir interface inside reinject-hide trace match icmp any any
firepower# cluster exec capture capo interface outside trace match icmp any any
firepower# cluster exec capture capccl interface cluster trace match icmp any any
```

Opstellen van activiteiten binnen het cluster:

1. unit-1-1 op site 1 ontvangt de gefragmenteerde ICMP-echo-aanvraagpakketten.

```
firepower# cluster exec show cap capir
unit-1-1(LOCAL):*****
```

2 packets captured

```
1: 20:13:58.227801 802.1Q vlan#10 P0 192.0.2.10 > 203.0.113.10 icmp: echo request
```

```
2: 20:13:58.227832 802.1Q vlan#10 P0
```

2 packets shown

2. unit-1-1 selecteert eenheid-2-2 in site 2 als de fragmentatieeigenaar en stuurt gefragmenteerde pakketten naar de eenheid.

Het bestemmings MAC-adres van de pakketten die van eenheid-1-1 naar eenheid-2-2 worden verzonden is het MAC-adres van de CCL verbinding in eenheid-2-2.

```
firepower# show cap capccl packet-number 1 detail
```

7 packets captured

```
1: 20:13:58.227817 0015.c500.018f 0015.c500.029f 0x0800 Length: 1509
```

```
192.0.2.10 > 203.0.113.10 icmp: echo request (wrong icmp csum) (frag 46772:1475@0+) (ttl 3)
```

1 packet shown

```
firepower# show cap capccl packet-number 2 detail
```

7 packets captured

```
2: 20:13:58.227832 0015.c500.018f 0015.c500.029f 0x0800 Length: 637
```

```
192.0.2.10 > 203.0.113.10 (frag 46772:603@1480) (ttl 3)
```

1 packet shown

```
firepower# cluster exec show interface po48 | i MAC
```

```
unit-1-1(LOCAL):*****
```

```
MAC address 0015.c500.018f, MTU 1500
```

```
unit-1-2:*****
```

```
MAC address 0015.c500.019f, MTU 1500
```

```
unit-2-2:*****
```

```
MAC address 0015.c500.029f, MTU 1500
```

```
unit-1-3:*****
```

```
MAC address 0015.c500.016f, MTU 1500
```

```
unit-2-1:*****
```

```
MAC address 0015.c500.028f, MTU 1500
```

```
unit-2-3:*****
```

```
MAC address 0015.c500.026f, MTU 1500
```

3. unit-2-2 ontvangt, monteert de gefragmenteerde pakketten opnieuw en wordt de eigenaar van de stroom.

```
firepower# cluster exec unit unit-2-2 show capture capccl packet-number 1 trace
```

11 packets captured

```
1: 20:13:58.231845 192.0.2.10 > 203.0.113.10 icmp: echo request
```

```
Phase: 1
```

```
Type: CLUSTER-EVENT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Input interface: 'inside'
```

Flow type: NO FLOW

I (2) received a FWD_FRAG_TO_FRAG_OWNER from (0).

Phase: 2

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'inside'

Flow type: NO FLOW

I (2) have reassembled a packet and am processing it.

Phase: 3

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 4

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 5

Type: ROUTE-LOOKUP

Subtype: No ECMP load balancing

Result: ALLOW

Config:

Additional Information:

Destination is locally connected. No ECMP load balancing.

Found next-hop 203.0.113.10 using egress ifc outside(vrfid:0)

Phase: 6

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'inside'

Flow type: NO FLOW

I (2) am becoming owner

Phase: 7

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip any any rule-id 268435460 event-log flow-end

access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: igasimov_prefilter1

access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: r1

Additional Information:

...

Phase: 19

Type: FLOW-CREATION

```
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1719, packet dispatched to next module
```

...

```
Result:
input-interface: cluster(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

1 packet shown

```
firepower# cluster exec unit unit-2-2 show capture capccl packet-number 2 trace
```

11 packets captured

2: 20:13:58.231875

Phase: 1

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'inside'

Flow type: NO FLOW

I (2) received a FWD_FRAG_TO_FRAG_OWNER from (0).

Result:

input-interface: cluster(vrfid:0)

input-status: up

input-line-status: up

Action: allow

1 packet shown

4. unit-2-2 staat de pakketten toe op basis van het veiligheidsbeleid en stuurt ze via de externe interface van plaats 2 naar plaats 1.

```
firepower# cluster exec unit unit-2-2 show cap capo
```

2 packets captured

1: 20:13:58.232058 802.1Q vlan#20 P0 192.0.2.10 > 203.0.113.10 icmp: echo request

2: 20:13:58.232058 802.1Q vlan#20 P0

Opmerkingen/opmerkingen

- In tegenstelling tot de regisseur, kan de fragmentaareigenaar niet gelokaliseerd worden binnen een bepaalde site. De eigenaar van het fragment wordt bepaald door de eenheid die oorspronkelijk de gefragmenteerde pakketten van een nieuwe verbinding ontvangt en op elke locatie kan worden geplaatst.
- Aangezien een fragmentaareigenaar ook de verbindingseigenaar kan worden, dan moet om de pakketten naar de doelhost door te sturen het in staat zijn om de noodoplossing op te lossen, de IP- en MAC-adressen van de doelhost of de volgende hop. Dit veronderstelt dat de

volgende hop(en) ook de bereikbaarheid aan de bestemmingsgastheer moet(en) hebben.

- Om de gefragmenteerde pakketten opnieuw te assembleren handhaaft de ASA/FTD een IP van de fragmentatie module voor elke genoemde interface. Om de operationele gegevens van de module van de hermontage van het IP-fragment weer te geven, gebruikt u de opdracht **showfragment**:

```
Interface: inside
Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
Run-time stats: Queue: 0, Full assembly: 0
Drops: Size overflow: 0, Timeout: 0,
Chain overflow: 0, Fragment queue threshold exceeded: 0,
Small fragments: 0, Invalid IP len: 0,
Reassembly overlap: 0, Fraghead alloc failed: 0,
SGT mismatch: 0, Block alloc failed: 0,
Invalid IPV6 header: 0, Passenger flow assembly failed: 0
```

In clusterimplementaties plaatst de fragmentatieeigenaar of de verbindingseigenaar de gefragmenteerde pakketten in de fragmentwachtrij. De grootte van de fragmentwachtrij is beperkt door de waarde van de teller van het formaat (standaard 200) die is ingesteld met de opdracht **<size> <name indien>**. Wanneer de grootte van de fragmentwachtrij 2/3 van de grootte bereikt, wordt de drempelwaarde voor de fragmentwachtrij als overschreden beschouwd, worden alle nieuwe fragmenten die geen deel uitmaken van de huidige fragmentatieketen laten vallen. In dit geval wordt de **overschreden drempel voor de wachtrij voor fragmentatie** verhoogd en wordt **FTD-3-209006** gegenereerd.

```
firepower# show fragment inside
Interface: inside
```

```
Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
Run-time stats: Queue: 133, Full assembly: 0
Drops: Size overflow: 0, Timeout: 8178,
Chain overflow: 0, Fragment queue threshold exceeded: 40802,
Small fragments: 0, Invalid IP len: 0,
Reassembly overlap: 9673, Fraghead alloc failed: 0,
SGT mismatch: 0, Block alloc failed: 0,
Invalid IPV6 header: 0, Passenger flow assembly failed: 0
```

```
%FTD-3-209006: Fragment queue threshold exceeded, dropped TCP fragment from 192.0.2.10/21456 to 203.0.113.10/443 on inside interface.
```

Als een tijdelijke oplossing kunt u het formaat **vergroten** in **FireSIGHT Management Center > Apparaatbeheer > [Apparatuur bewerken] > Interfaces > [Interface] > Geavanceerd > Security Configuration > Default Fragment-instelling negeren**, configuratie opslaan en beleid implementeren. Controleer vervolgens de teller van de wachtrij in de opdrachtoutput van het **showfragment** en het optreden van het syslogbericht **FTD-3-209006**.

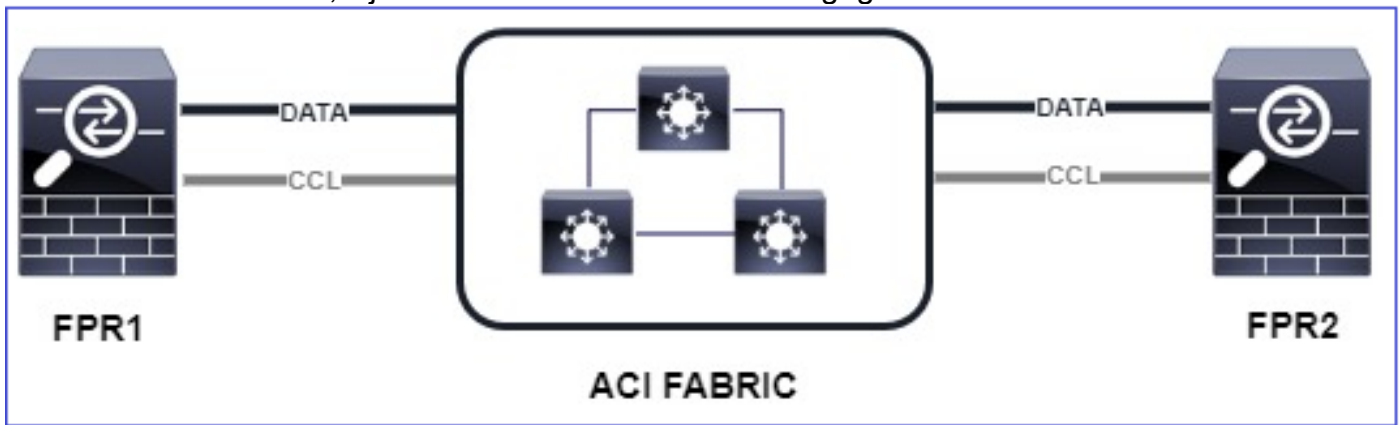
ACI-problemen

Intermitterende aansluitingsproblemen door het cluster door actieve L4-checksum verificatie in ACI Pod

Symptoom

- Intermitterende aansluitingsproblemen door de ASA/FTD-cluster in een ACI-podd.
- Als er slechts 1 eenheid in de cluster is, worden de aansluitingsproblemen niet waargenomen.
- Pakketten die van één clustereenheid naar één of meer andere eenheden in de cluster

worden verzonden, zijn niet zichtbaar in de FXOS en gegevensvlakken van de doeleenheden.



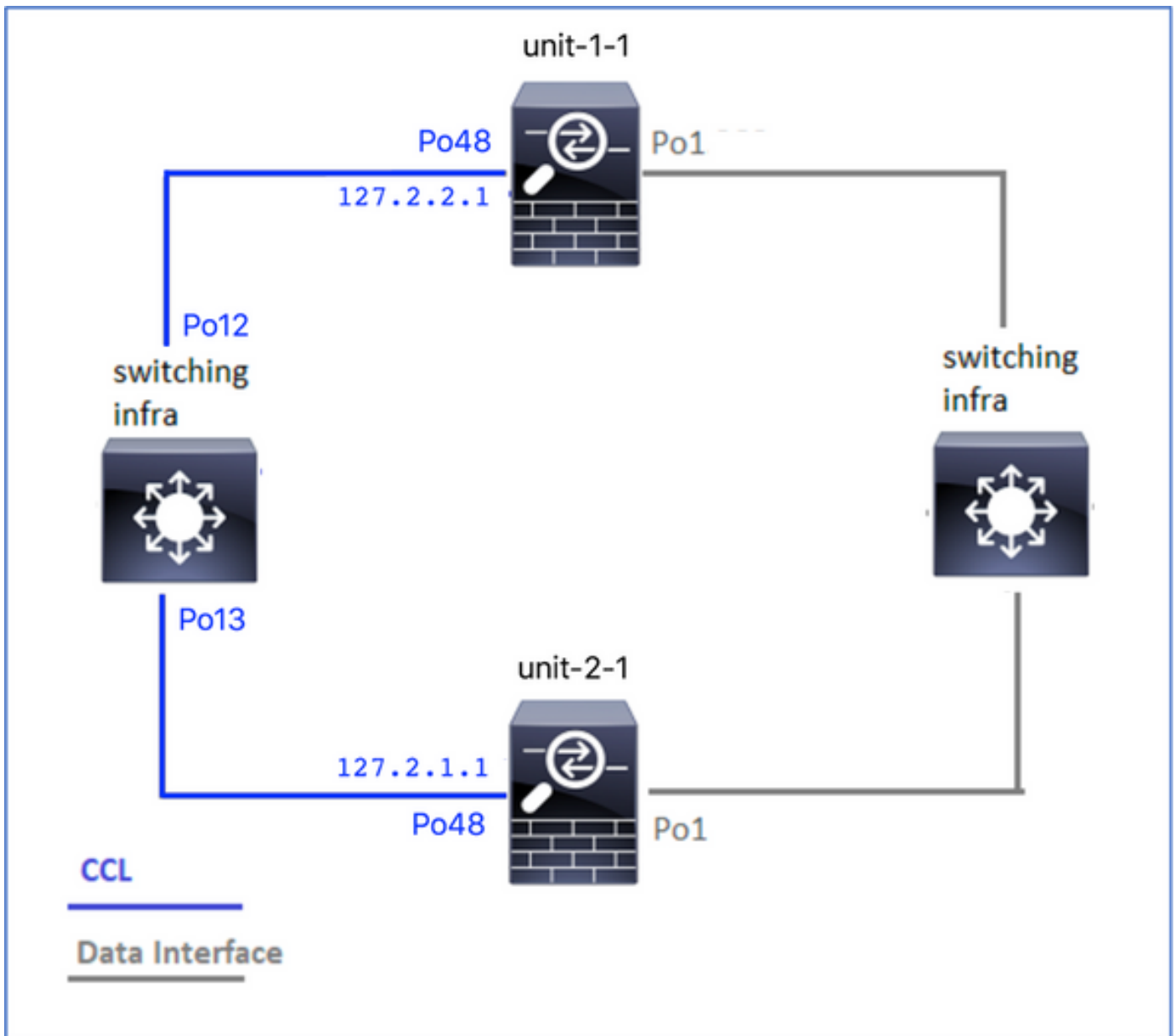
Beperken

- Omgeleid verkeer via de clusterbesturingskoppeling heeft geen correcte L4-checksum en dit wordt verwacht gedrag. Switches op het traject van de clustercontrole mogen de L4-checksum niet verifiëren. Switches die de L4 checksum controleren, kunnen verkeer doen vallen. Controleer de configuratie van de ACI-switch en controleer of er geen L4-checksum wordt uitgevoerd op de ontvangen of verzonden pakketten via de clustercontrol-link.

Problemen met clusterbesturingsplane

Eenheid kan niet deelnemen aan het cluster

MTU-grootte op CCL



Symptomen

De eenheid kan zich niet aansluiten bij het cluster en dit bericht wordt weergegeven:

```
The slave has left the cluster because application configuration sync is timed out on this unit.
Disabling cluster now!
Cluster disable is performing cleanup..done.
Unit unit-2-1 is quitting due to system failure for 1 time(s) (last failure is Slave application
configuration sync timeout). Rejoin will be attempted after 5 minutes.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.
```

Verificatie/bepanking

- Gebruik de opdracht **Show interface** op de FTD om te controleren of de MTU op de interface van de clustercontrole minstens 100 bytes hoger is dan de interface van de gegevensinterface MTU:

```
firepower# show interface
Interface Port-channel1 "Inside", is up, line protocol is up
```

Hardware is EtherSVI, BW 40000 Mbps, DLY 10 usec

MAC address 3890.a5f1.aa5e, **MTU 9084**

Interface **Port-channel148 "cluster"**, is up, line protocol is up

Hardware is EtherSVI, BW 40000 Mbps, DLY 10 usec

Description: Clustering Interface

MAC address 0015.c500.028f, **MTU 9184**

IP address 127.2.2.1, subnet mask 255.255.0.

- Voer een **ping** door de CCL uit met de optie **grootte** om te controleren of deze op de CCL MTU is ingesteld op alle apparaten in het pad.

```
firepower# ping 127.2.1.1 size 9184
```

- Gebruik de opdracht interface-unit op de switch om de configuratie van de MTU te controleren

```
Switch# show interface
```

```
port-channel12 is up
```

```
admin state is up,
```

```
Hardware: Port-Channel, address: 7069.5a3a.7976 (bia 7069.5a3a.7976)
```

```
MTU 9084 bytes, BW 40000000 Kbit , DLY 10 usec
```

```
port-channel13 is up
```

```
admin state is up,
```

```
Hardware: Port-Channel, address: 7069.5a3a.7967 (bia 7069.5a3a.7967)
```

```
MTU 9084 bytes, BW 40000000 Kbit , DLY 10 use
```

Interfacemoorden tussen clustereenheden

Symptomen

De eenheid kan zich niet aansluiten bij het cluster en dit bericht wordt weergegeven:

```
Interface mismatch between cluster master and joining unit unit-2-1. unit-2-1 aborting cluster join.
```

```
Cluster disable is performing cleanup..done.
```

```
Unit unit-2-1 is quitting due to system failure for 1 time(s) (last failure is Internal clustering error). Rejoin will be attempted after 5 minutes.
```

```
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.
```

Verificatie/beperking

Meld u aan bij de FCM GUI op elk chassis, navigeer naar het tabblad **Interfaces** en controleer of alle clusterleden dezelfde interfacemodules hebben:

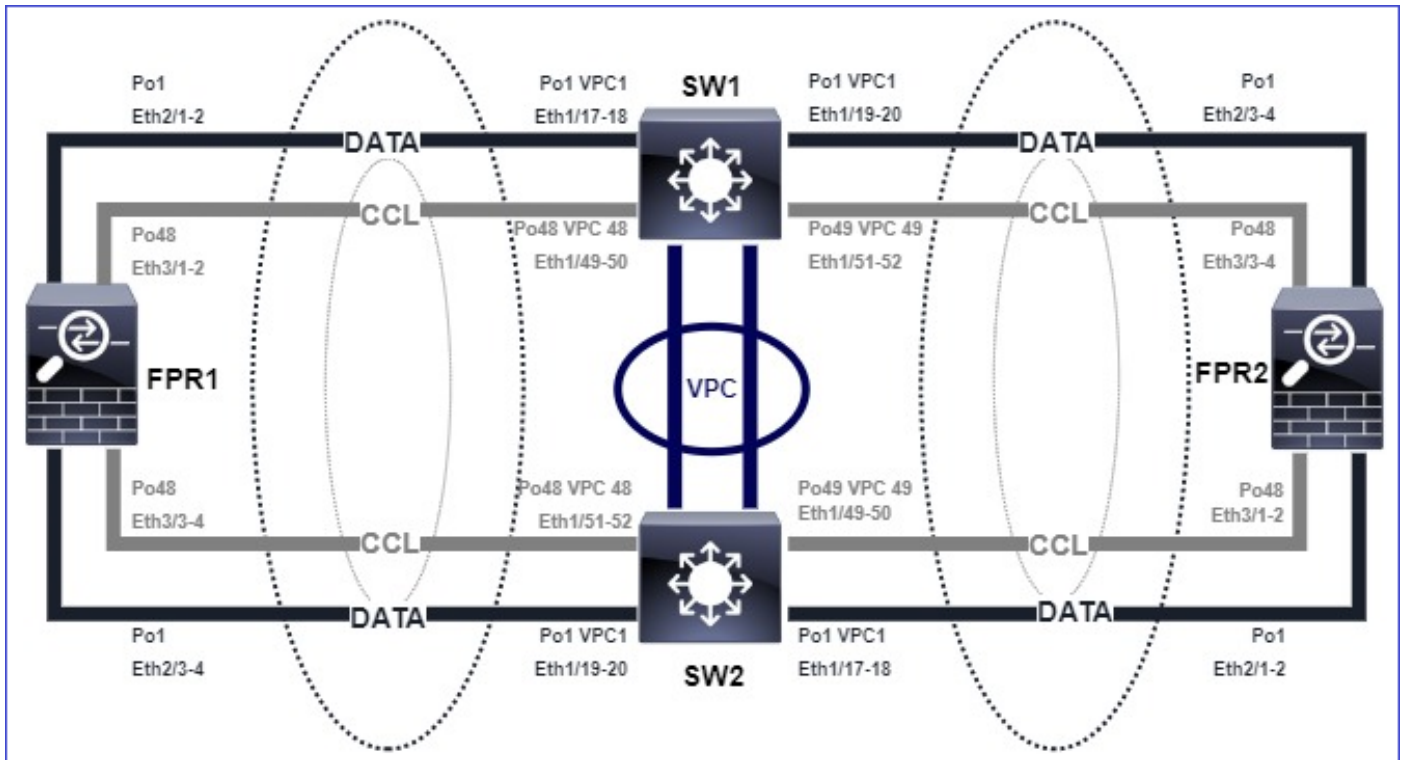
- Interfaces die aan het logische apparaat zijn toegewezen
- Admin-snelheid van de interfaces
- Admin duplex van de interfaces
- Interfacestatus

Data-poorts-kanaals interfacekaart

Splitsen-brein vanwege bereikbaarheidsproblemen via de CCL

Symptoom

Er zijn meerdere besturingseenheden in het cluster. Neem deze topologie in overweging:



Chassis 1:

```
firepower# show cluster info
```

```
Cluster ftd_cluster1: On
Interface mode: spanned
This is "unit-1-1" in state MASTER
ID : 0
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2103TU5H
CCL IP : 127.2.1.1
CCL MAC : 0015.c500.018f
Last join : 07:30:25 UTC Dec 14 2020
Last leave: N/A
Other members in the cluster:
Unit "unit-1-2" in state SLAVE
ID : 1
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2103TU4D
CCL IP : 127.2.1.2
CCL MAC : 0015.c500.019f
Last join : 07:30:26 UTC Dec 14 2020
Last leave: N/A
Unit "unit-1-3" in state SLAVE
ID : 3
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2102THJT
CCL IP : 127.2.1.3
CCL MAC : 0015.c500.016f
Last join : 07:31:49 UTC Dec 14 2020
Last leave: N/A
```

Chassis 2:

firepower# show cluster info

```
Cluster ftd_cluster1: On
Interface mode: spanned
This is "unit-2-1" in state MASTER
ID : 4
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2103TUN1
CCL IP : 127.2.2.1
CCL MAC : 0015.c500.028f
Last join : 11:21:56 UTC Dec 23 2020
Last leave: 11:18:51 UTC Dec 23 2020
Other members in the cluster:
Unit "unit-2-2" in state SLAVE
ID : 2
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2102THR9
CCL IP : 127.2.2.2
CCL MAC : 0015.c500.029f
Last join : 11:18:58 UTC Dec 23 2020
Last leave: 22:28:01 UTC Dec 22 2020
Unit "unit-2-3" in state SLAVE
ID : 5
Site ID : 1
Version : 9.15(1)
Serial No.: FLM2103TUML
CCL IP : 127.2.2.3
CCL MAC : 0015.c500.026f
Last join : 11:20:26 UTC Dec 23 2020
Last leave: 22:28:00 UTC Dec 22 2020
```

Verificatie

- Gebruik de **ping** opdracht om connectiviteit tussen de IP-adressen van de clustercontrole (CCL) van de besturingseenheden te verifiëren:

```
firepower# ping 127.2.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 127.2.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

- Controleer de ARP-tabel:

```
firepower# show arp
cluster 127.2.2.3 0015.c500.026f 1
cluster 127.2.2.2 0015.c500.029f 1
```

- In de eenheden van de controle, vorm en controleer opnamen op de interfaces van de CCL:

```
firepower# capture capccl interface cluster
firepower# show capture capccl | i 127.2.1.1
2: 12:10:57.652310 arp who-has 127.2.1.1 tell 127.2.2.1
41: 12:11:02.652859 arp who-has 127.2.1.1 tell 127.2.2.1
74: 12:11:07.653439 arp who-has 127.2.1.1 tell 127.2.2.1
97: 12:11:12.654018 arp who-has 127.2.1.1 tell 127.2.2.1
```

```
126: 12:11:17.654568 arp who-has 127.2.1.1 tell 127.2.2.1
151: 12:11:22.655148 arp who-has 127.2.1.1 tell 127.2.2.1
174: 12:11:27.655697 arp who-has 127.2.1.1 tell 127.2.2.1
```

Beperken

- Zorg ervoor dat de CCL poort-kanaalinterfaces zijn aangesloten op afzonderlijke poort-kanaalinterfaces op de switch.
- Wanneer virtuele poortkanalen (vPC) worden gebruikt op Nexus-switches, zorg er dan voor dat de CCL poort-kanaalinterfaces zijn aangesloten op verschillende vPC en dat de vPC-configuratie geen mislukte consistentiestatus heeft.
- Zorg ervoor dat de CCL poort-kanaalinterfaces in hetzelfde uitzending-domein zijn en CCL VLAN wordt gecreëerd en toegestaan op de interfaces.

Dit is een voorbeeldconfiguratie van de switch:

```
Nexus# show run int po48-49
```

```
interface port-channel48
description FPR1
switchport access vlan 48
vpc 48
```

```
interface port-channel49
description FPR2
switchport access vlan 48
vpc 49
```

```
Nexus# show vlan id 48
```

```
VLAN Name Status Ports
-----
48 CCL active Po48, Po49, Po100, Eth1/53, Eth1/54

VLAN Type Vlan-mode
----
48 enet CE
```

```
1 Po1 up success success 10,20
48 Po48 up success success 48
49 Po49 up success success 48
```

```
Nexus1# show vpc brief
```

```
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 3
Peer Gateway : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
```

```
vPC Peer-link status
```

```
-----  
id Port Status Active vlans  
-----
```

```
1 Po100 up 1,10,20,48-49,148
```

```
vPC status
```

```
-----  
id Port Status Consistency Reason Active vlans  
-----
```

```
1 Po1 up success success 10,20
```

```
48 Po48 up success success 48
```

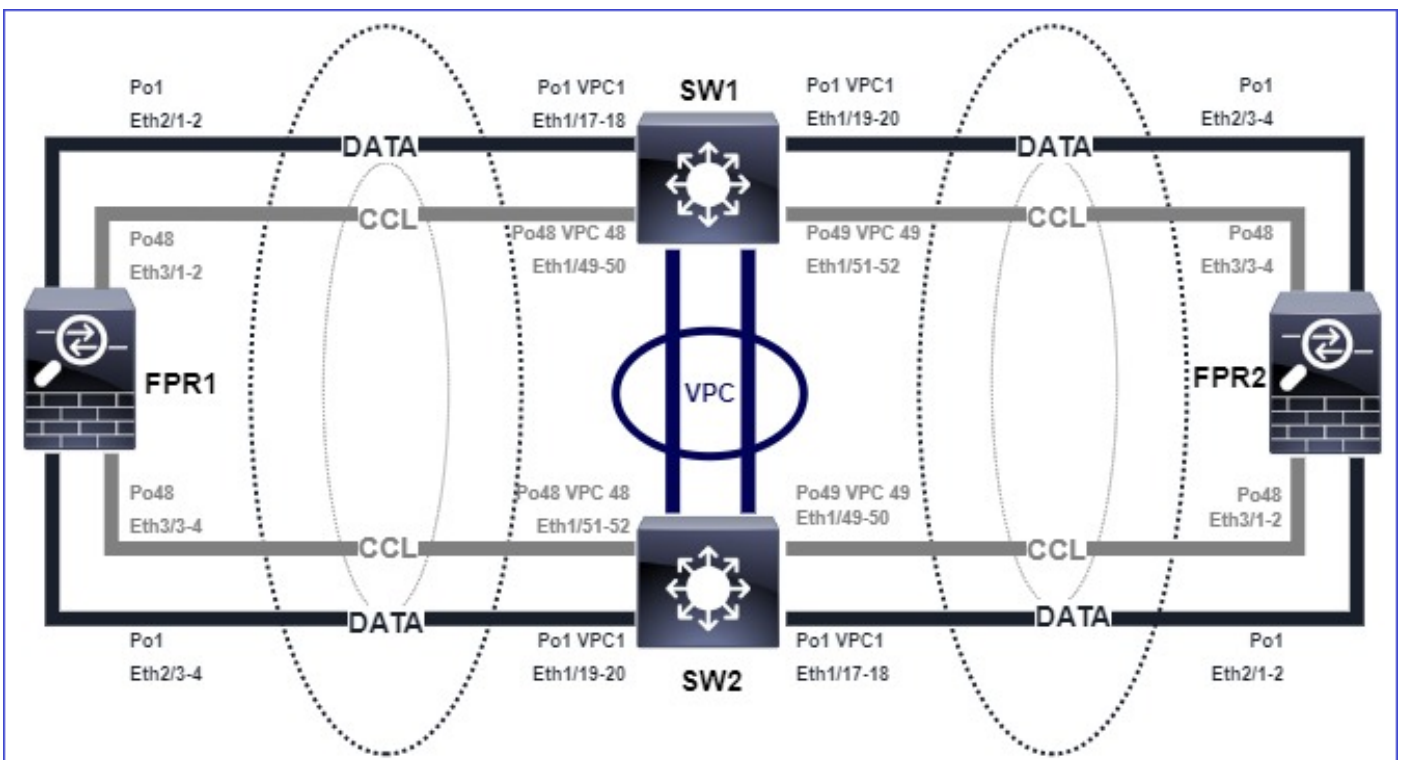
```
49 Po49 up success success 48
```

Uitgeschakelde Cluster vanwege uitgestelde data-kanaalinterfaces

Symptoom

Een of meer gegevenspoort-kanaalinterfaces worden opgeschort. Wanneer een administratief enabled-gegevensinterface wordt opgeschort, worden alle clustereenheden in hetzelfde chassis uit het cluster gebrand omdat de interface-gezondheidscontrole defect is.

Neem deze topologie in overweging:



Verificatie

- Controleer de bedieningspaneel:

```
firepower#
```

```
Beginning configuration replication to Slave unit-2-2
```

```
End Configuration Replication to slave.
```

```
Asking slave unit unit-2-2 to quit because it failed interface health check 4 times (last failure on Port-channel1). Clustering must be manually enabled on the unit to rejoin.
```

- Controleer de uitvoer van de **show cluster history** en de **show cluster info trace module hc-**

opdrachten in de betrokken unit(s):

```
firepower# Unit is kicked out from cluster because of interface health check failure.
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.
```

```
Cluster unit unit-2-1 transitioned from SLAVE to DISABLED
```

```
firepower# show cluster history
```

```
=====
From State To State Reason
=====
```

```
12:59:37 UTC Dec 23 2020
ONCALL SLAVE_COLD Received cluster control message
```

```
12:59:37 UTC Dec 23 2020
SLAVE_COLD SLAVE_APP_SYNC Client progression done
```

```
13:00:23 UTC Dec 23 2020
SLAVE_APP_SYNC SLAVE_CONFIG Slave application configuration sync done
```

```
13:00:35 UTC Dec 23 2020
SLAVE_CONFIG SLAVE_FILESYS Configuration replication finished
```

```
13:00:36 UTC Dec 23 2020
SLAVE_FILESYS SLAVE_BULK_SYNC Client progression done
```

```
13:01:35 UTC Dec 23 2020
SLAVE_BULK_SYNC DISABLED Received control message DISABLE (interface health check failure)
```

```
firepower# show cluster info trace module hc
```

```
Dec 23 13:01:36.636 [INFO]cluster_fsm_clear_np_flows: The clustering re-enable timer is started
to expire in 598000 ms.
```

```
Dec 23 13:01:32.115 [INFO]cluster_fsm_disable: The clustering re-enable timer is stopped.
```

```
Dec 23 13:01:32.115 [INFO]Interface Port-channel1 is down
```

- Controleer de uitvoer van de **show port-channel summary** opdracht in de **fxos** opdrachtschaal:

```
FPR2(fxos)# show port-channel summary
```

```
Flags: D - Down P - Up in port-channel (members)
```

```
I - Individual H - Hot-standby (LACP only)
```

```
s - Suspended r - Module-removed
```

```
S - Switched R - Routed
```

```
U - Up (port-channel)
```

```
M - Not in use. Min-links not met
```

```
-----
Group Port-Channel Type Protocol Member Ports
```

```
-----
1 Po1(SD) Eth LACP Eth2/1(s) Eth2/2(s) Eth2/3(s) Eth2/4(s)
```

```
48 Po48(SU) Eth LACP Eth3/1(P) Eth3/2(P) Eth3/3(P) Eth3/4(P)
```

Beperken

- Zorg ervoor dat alle chassis dezelfde clustergroepnaam en hetzelfde wachtwoord hebben.
- Zorg ervoor dat de poort-kanaalinterfaces administratief fysieke lidinterfaces met dezelfde duplex/snelheidsconfiguratie in alle chassis en switches hebben ingeschakeld.

- In intersite clusters dient u ervoor te zorgen dat dezelfde gegevenspoort-kanaalinterface in alle chassis is aangesloten op dezelfde poort-kanaalinterface in de switch.
- Wanneer virtuele poortkanalen (vPC) worden gebruikt in Nexus-switches, zorg er dan voor dat de vPC-configuratie geen mislukte consistentiestatus heeft.
- In intersite clusters dient dezelfde gegevenspoort-kanaalinterface in alle chassis te worden aangesloten op dezelfde vPC.

Cluster Stability Issues

FXOS-tracering

Symptoom

Eenheid verlaat het cluster.

Verificatie/beperking

- Gebruik de opdracht **show clustergeschiedenis** om te zien wanneer de eenheid het cluster heeft verlaten

```
firepower# show cluster history
```

- Gebruik deze opdrachten om te controleren of de FXOS een traceback-up had

```
FPR4150# connect local-mgmt
```

```
FPR4150 (local-mgmt)# dir cores
```

- Verzamel het basisbestand dat gegenereerd is rond het tijdstip waarop de eenheid het cluster heeft verlaten en geef het aan TAC.

Schijf vol

Indien het gebruik van de schijf in de /ngfw-verdeling van een clustereenheid **94%** bereikt, wordt de eenheid het cluster stopgezet. De controle van het gebruik van de schijf vindt elke 3 seconden plaats:

```
> show disk
```

```
Filesystem Size Used Avail Use% Mounted on
rootfs 81G 421M 80G 1% /
devtmpfs 81G 1.9G 79G 3% /dev
tmpfs 94G 1.8M 94G 1% /run
tmpfs 94G 2.2M 94G 1% /var/volatile
/dev/sda1 1.5G 156M 1.4G 11% /mnt/boot
/dev/sda2 978M 28M 900M 3% /opt/cisco/config
/dev/sda3 4.6G 88M 4.2G 3% /opt/cisco/platform/logs
/dev/sda5 50G 52M 47G 1% /var/data/cores
/dev/sda6 191G 191G 13M 100% /ngfw
cgroup_root 94G 0 94G 0% /dev/cgroups
```

In dit geval, toont de uitvoer van de **show clustergeschiedenis**:

```
15:36:10 UTC May 19 2021
```

```
MASTER MASTER Event: Master unit unit-1-1 is quitting
```


due to **diskstatus** Application health check failure, and master's application state is down

of

14:07:26 CEST May 18 2021

SLAVE DISABLED Received control message DISABLE (application health check failure)

Een andere manier om de fout te verifiëren is:

```
firepower# show cluster info health
```

```
Member ID to name mapping:
```

```
0 - unit-1-1(myself) 1 - unit-2-1
```

```
0 1
```

```
Port-channel48 up up
```

```
Ethernet1/1 up up
```

```
Port-channel12 up up
```

```
Port-channel13 up up
```

```
Unit overall healthy healthy
```

```
Service health status:
```

```
0 1
```

```
diskstatus (monitor on) down down
```

```
snort (monitor on) up up
```

```
Cluster overall healthy
```

Als de schijf ~100% is, kan het bovendien moeilijk zijn om de cluster terug te koppelen naar de groep totdat er enige schijfruimte is vrijgekomen.

Overflow-bescherming

Iedere 5 minuten controleert elke clustereenheid de lokale en de peer-unit voor CPU- en geheugengebruik. Als het gebruik boven de systeemdrempels gaat (LINA CPU 50% of LINA geheugen 59%) wordt er een informatief bericht weergegeven in:

- Syslogs (FTD-6-74808)
- Bestand log/cluster_trace.log, bijvoorbeeld

```
firepower# more log/cluster_trace.log | i CPU
```

```
May 20 16:18:06.614 [INFO][CPU load 87% | memory load 37%] of module 1 in chassis 1 (unit-1-1) exceeds overflow protection threshold [CPU 50% | Memory 59%]. System may be oversubscribed on member failure.
```

```
May 20 16:18:06.614 [INFO][CPU load 87% | memory load 37%] of chassis 1 exceeds overflow protection threshold [CPU 50% | Memory 59%]. System may be oversubscribed on chassis failure.
```

```
May 20 16:23:06.644 [INFO][CPU load 84% | memory load 35%] of module 1 in chassis 1 (unit-1-1) exceeds overflow protection threshold [CPU 50% | Memory 59%]. System may be oversubscribed on member failure.
```

Het bericht duidt erop dat bij een storing van de eenheid de resterende eenheden kunnen worden overschreden.

Vereenvoudigde modus

Gedrag op pre-6.3 FMC-releases

- U registreert elk clusterknooppunt afzonderlijk op FMC.

- Dan vormt u een logisch cluster in FMC.
- Bij elke nieuwe toevoeging van clusterknooppunten moet u het knooppunt handmatig registreren.

Post-6.3 FMC

- Met de functie voor vereenvoudigde modus kunt u het hele cluster in één stap registreren (alleen één knooppunt van het cluster registreren).

Minimale ondersteunde Manager	Beheerde apparaten	Min. ondersteunde beheerde apparaatversie vereist	Opmerkingen
VMC 6,3	Alleen FTD-clusters op FP9300 en FP4100	6.2.0	Dit is alleen een FMC-functie

Waarschuwing: Als het cluster op FTD is gevormd, moet u wachten tot de auto-registratie start. U moet niet proberen de clusterknooppunten handmatig te registreren (apparaat toevoegen), maar de optie Gereedschap gebruiken.

Symptoom

Registratiefouten voor knooppunt

- Als de registratie van de besturingsknooppunten om wat dan ook faalt, wordt de cluster verwijderd van het VCC.

Beperken

Als de registratie van gegevensknooppunten om welke reden dan ook mislukt, zijn er 2 opties:

1. Met elke toepassing in cluster controleert FMC of er clusterknooppunten zijn die moeten worden geregistreerd en start vervolgens de automatische registratie voor deze knooppunten.
2. Er is een optie **Reconcile** beschikbaar onder het tabblad clustersamenvatting (**Apparaten > Apparaatbeheer > Cluster tabblad > Cluster Status weergeven**). Zodra de Reconcile-actie is geactiveerd, start FMC de automatische registratie van de knooppunten die moeten worden geregistreerd.

Gerelateerde informatie

- [Clustering voor de FireSIGHT Threat Defense](#)
- [ASA-cluster voor FirePOWER 4100/9300-chassis](#)
- [Informatie over clusters op het FirePOWER 4100/9300-chassis](#)
- [Firepower NGFW Clustering Deep Dive - BRKSEC-3032](#)
- [Firepower Firewall Captures analyseren om netwerkproblemen effectief op te lossen](#)