Probleemoplossing voor FTD-cluster (Firepower Threat Defence)

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen bij een clusterinstelling in de Firepower Next-Generation Firewall (NGFW).

Voorwaarden

Vereisten

Cisco raadt u aan kennis van deze onderwerpen te hebben (zie Verwante informatie voor koppelingen):

- Firepower platform architectuur
- Configuratie en gebruik van Firepower Cluster
- Bekendheid met de FTD en Firepower eXtensible Operating System (FXOS) CLI
- Logbestanden van NGFW/dataplaat
- NGFW/dataplatform-pakkettracer
- FXOS/dataplaat vangt

Gebruikte componenten

- HW: FirePOWER-applicatie 4125
- SW: 6.7.0 (Bouw 65) - dataplaat 9.15(1)

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

Achtergrondinformatie

De meeste items die in dit document worden behandeld, zijn ook volledig van toepassing op probleemoplossing bij clusters van adaptieve security applicatie (ASA).

Configureren

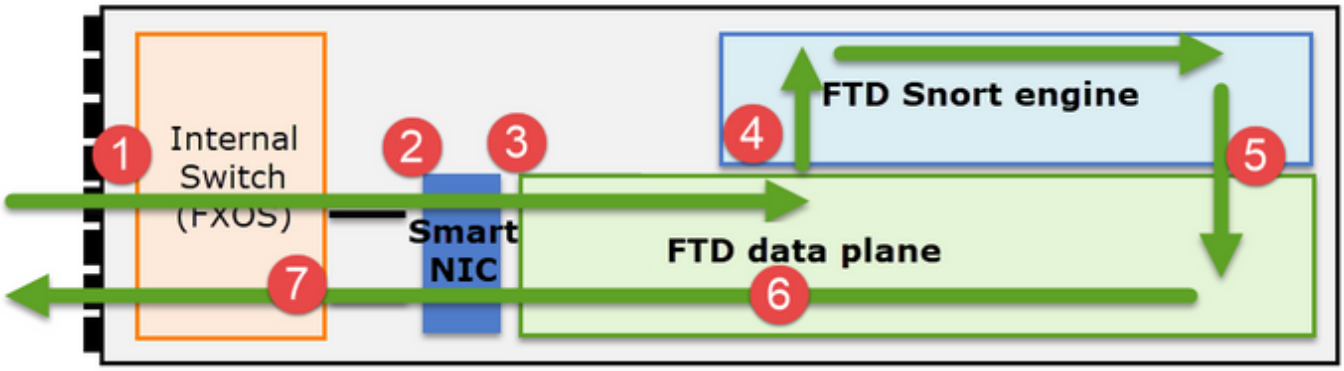
Het configuratiegedeelte van een clusterimplementatie wordt behandeld in de FMC- en FXOS-configuratiehandleidingen:

- Clustering voor de Firepower Threat Defence
- Een cluster implementeren voor Firepower Threat Defence voor schaalbaarheid en hoge beschikbaarheid

Cluster-basisgegevens

NGFW-architectuur

Het is belangrijk om te begrijpen hoe een Firepower 41xx- of 93xx-serie transitpakketten verwerkt:



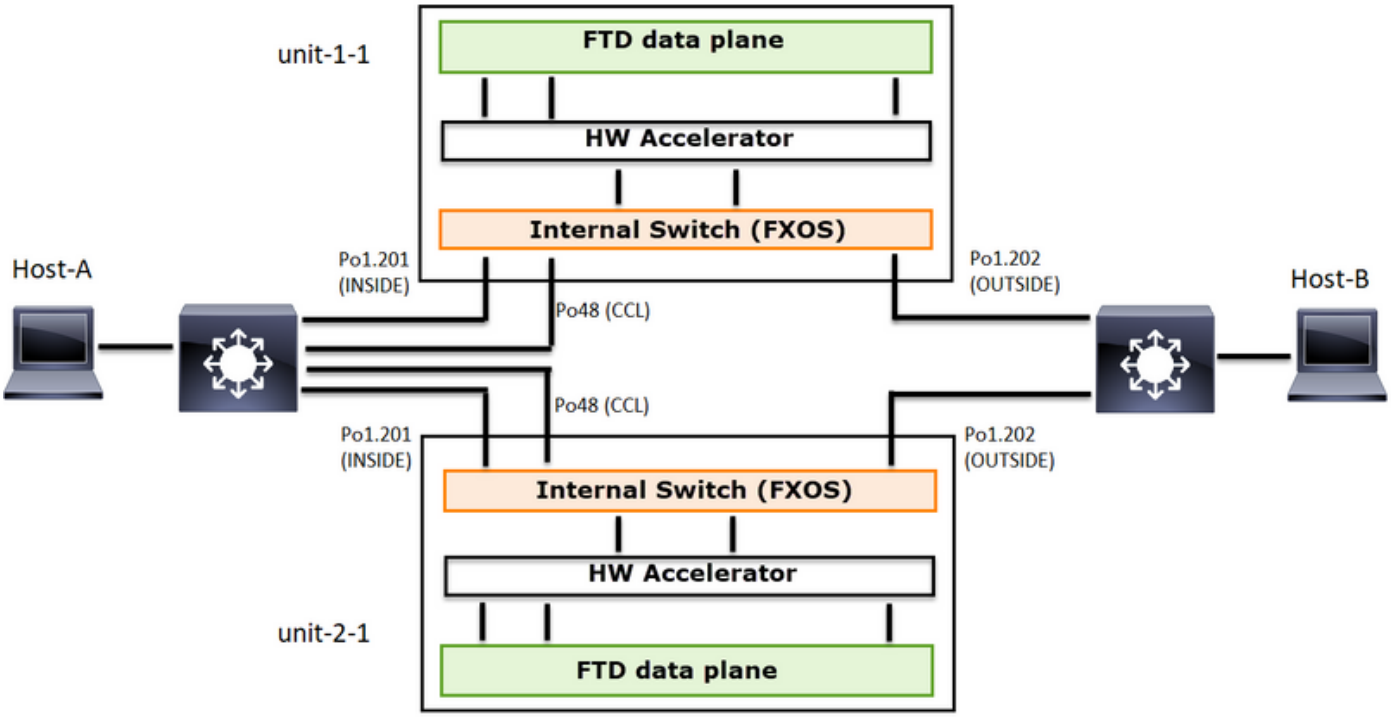
1. Een pakket gaat de toegangsinterface in en het wordt behandeld door de switch van de chassisbinnenkant.
2. Het pakket gaat door Slimme NIC. Als de stroom wordt geoffload (HW-versnelling), wordt het pakket alleen door de slimme NIC verwerkt en vervolgens naar het netwerk teruggestuurd.
3. Indien het pakket niet geoffload is, wordt het in het FTD-dataplatform ingevoerd dat voornamelijk L3/L4-controles uitvoert.
4. Als het beleid het vereist, wordt het pakket geïnspecteerd door de Snort-motor (voornamelijk L7-inspectie).
5. De snort-engine geeft een vonnis (bijvoorbeeld toestaan of blokkeren) voor het pakket terug.
6. Het gegevensvliegtuig laat vallen of door:sturen het pakket dat op de vonnis van Snort wordt gebaseerd.
7. Het pakket gaat met de switch van het chassis naar binnen.

Cluster-opnamen

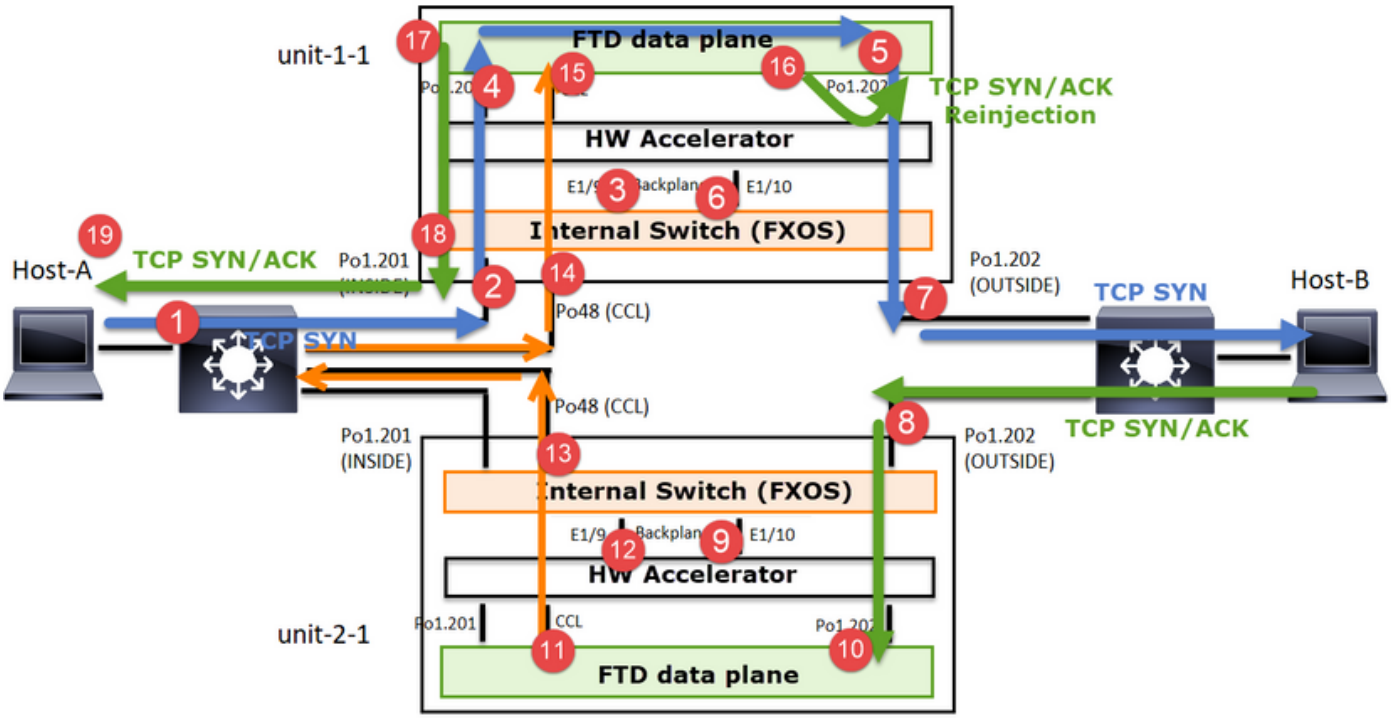
FirePOWER-apparaten bieden meerdere opnamepunten die zichtbaarheid geven in de transitstromen. Wanneer u problemen oplossen en cluster inschakelen de belangrijkste uitdagingen zijn:

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

In dit diagram wordt een cluster met 2 eenheden weergegeven (bijvoorbeeld FP941xx/FP9300):



In het geval van een asymmetrische TCP-verbindingsinstelling, ziet een TCP SYN, SYN/ACK-uitwisseling er als volgt uit:



Voorwaarts 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 via een van de backplane interfaces van het chassis (bijvoorbeeld E1/9, E1/10, enzovoort) naar het gegevensvlak verzonden.
4. TCP-SYN arriveert op de interface voor gegevensplane (Po1.201/INSIDE). In dit voorbeeld neemt unit1-1 de eigendom van de flow, doet Initial Sequence Number (ISDN)-randomisatie

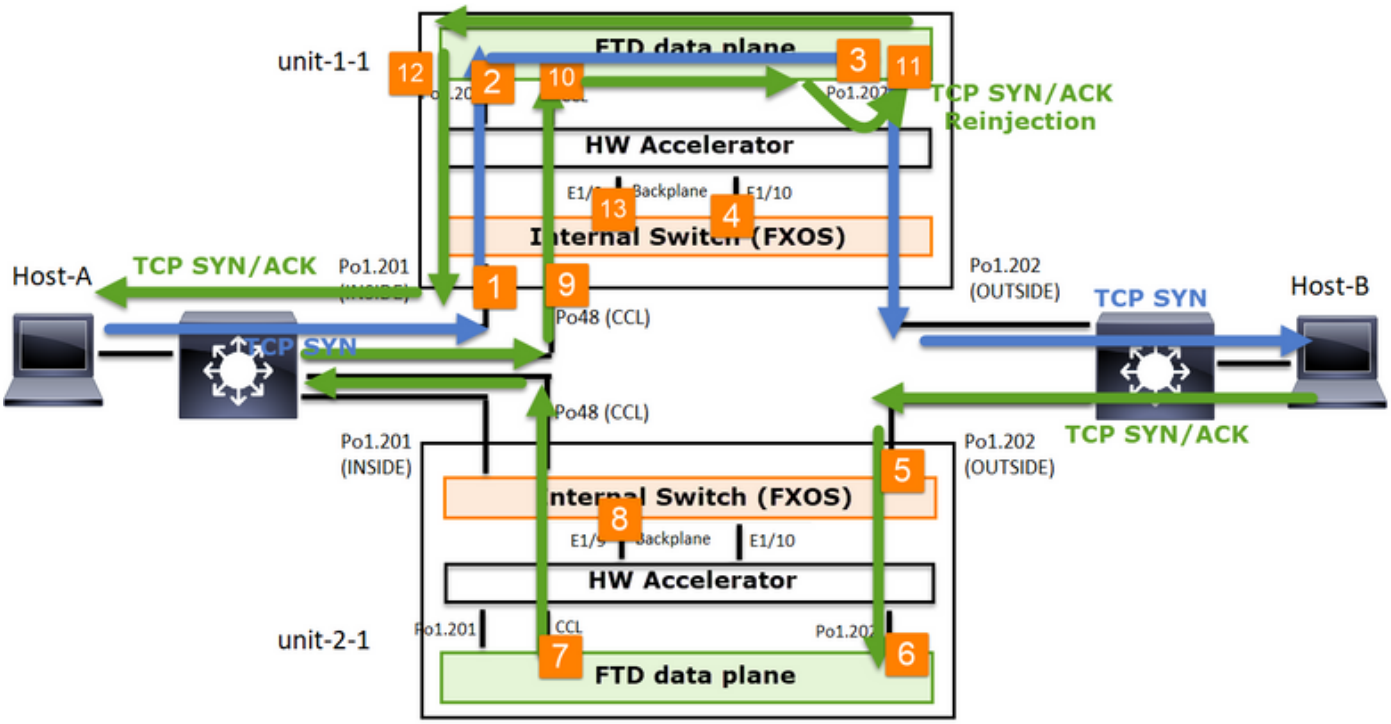
en codeert de eigendoms- (cookie) informatie in Seq-nummer.
5. TCP/SYN wordt verstuurd vanuit Po1.202/EXTERN (dataplatform egress interface).
6. TCP-SYN wordt geleverd op een van de backplane interfaces van het chassis (bijvoorbeeld E1/9, E1/10, enzovoort).
7. TCP SYN wordt verzonden uit de fysieke interface van het chassis (een van de leden van Po1) naar host-B.

Terugkeerverkeer

8. TCP/SYN/ACK wordt verzonden van host-B en komt aan op unit-2-1 (een van de leden van Po1).
9. TCP/SYN/ACK wordt via een van de backplane interfaces van het chassis (bijvoorbeeld E1/9, E1/10, enzovoort) naar het gegevensvlak verzonden.
10. TCP/SYN/ACK arriveert op de interface voor gegevensplatformtoegang (Po1.202/EXTERN).
11. TCP/SYN/ACK wordt vanuit Cluster Control Link (CCL) naar unit-1-1 verzonden. ISDN is standaard ingeschakeld. Aldus, vindt de expediteur de eigenaarinfo voor TCP SYN+ACKs zonder de betrokkenheid van de directeur. Voor andere pakketten of wanneer ISDN is uitgeschakeld, wordt de regisseur gevraagd.
12. TCP/SYN/ACK arriveert op een van de backplane interfaces van het chassis (bijvoorbeeld E1/9, E1/10, enzovoort).
13. TCP SYN/ACK wordt vanuit de fysieke interface van het chassis (een van de leden van Po48) naar unit-1-1 gestuurd.
14. TCP/SYN/ACK arriveert op unit-1-1 (een van de leden van Po48).
15. TCP/SYN/ACK wordt doorgestuurd via een van de chassis backplane interfaces naar het dataplatform CCL poort-kanaal interface (nameif cluster).
16. Het gegevensvliegtuig injecteert het TCP SYN/ACK pakket aan de interface Po1.202/EXTERN van het gegevensvliegtuig.
17. TCP/SYN/ACK wordt verzonden uit Po1.201/INSIDE (dataplatform egress interface) naar HOST-A.
18. TCP/SYN/ACK passeert een van de backplane interfaces van het chassis (bijvoorbeeld E1/9, E1/10, enzovoort) en verlaat een van de leden van Po1.
19. TCP/SYN/ACK arriveert op host-A.

Lees voor meer informatie over dit scenario het gerelateerde gedeelte in de casestudy’s van Cluster Connection Establishment.

Gebaseerd op deze pakketuitwisseling zijn alle mogelijke clusteropnamepunten:



Voor het voorwaartse verkeer (bijvoorbeeld TCP/SYN) moet u het volgende vastleggen:

1. De fysieke interface van het chassis (bijvoorbeeld Po1-leden). Deze opname wordt ingesteld vanuit de Chassis Manager (CM) UI of de CM CLI.
2. De interface van de gegevensplane (bijvoorbeeld, Po1.201 INSIDE).
3. Uitganginterface voor het gegevensvlak (bijvoorbeeld Po1.202 EXTERN).
4. Chassis backplane interfaces. Op FP4100 zijn er 2 backplane interfaces. Op 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 inschakelen.

Voor het retourverkeer (bijvoorbeeld TCP/SYN/ACK) moet u het volgende vastleggen:

5. De fysieke interface van het chassis (bijvoorbeeld Po1-leden). Deze opname wordt ingesteld vanuit de Chassis Manager (CM) UI of de CM CLI.
6. De interface van de gegevensplane (bijvoorbeeld, Po1.202 BUITEN).
7. Aangezien het pakket wordt omgeleid, is het volgende opnamepunt het gegevensvlak CCL.
8. Chassis backplane interfaces. Opnieuw, moet u opname op beide interfaces inschakelen.
9. Unit-1-1 chassis-CCL-ledeninterfaces.
10. Gegevensvlak CCL-interface (nameif-cluster).
11. Ingress-interface (Po1.202 EXTERN). Dit is het opnieuw ingevoerde pakket van CCL naar het gegevensvlak.
12. Uitganginterface voor het gegevensvlak (bijvoorbeeld Po1.201 INSIDE).
13. Chassis backplane interfaces.

Hoe u de Cluster-opnamen kunt inschakelen

FXOS-opnamen

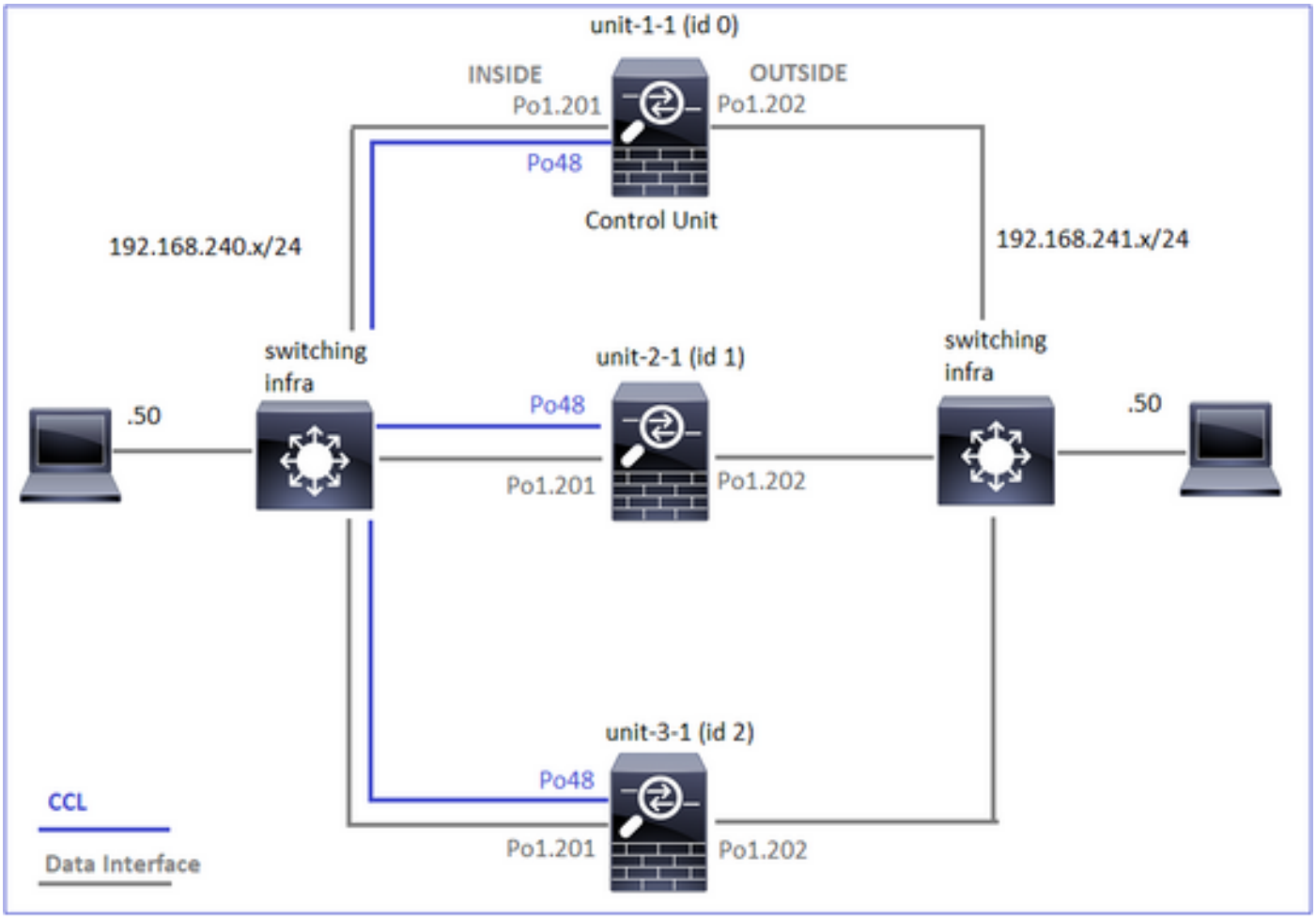
Het proces wordt beschreven in de FXOS Config Guide: PacketCapture

Opmerking: FXOS-opnamen kunnen alleen vanuit het oogpunt van de inwendige switch in de toegangsrichting worden genomen.

Opname van dataplane

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

Overweeg een cluster van 3 eenheden:



Gebruik deze opdracht om te controleren of er in alle clustereenheden actieve opnamen zijn:

<#root>

```
firepower#
```

```
cluster exec show capture
```

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

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

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

Om een gegevensvlak op alle eenheden op Po1.201 (INSIDE) in te schakelen:

<#root>

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

Het is sterk aanbevolen om een opnamefilter op te geven en om de opnamebuffer te verhogen als u veel verkeer verwacht:

<#root>

```
firepower#
cluster exec capture CAPI buffer 33554432 interface INSIDE match tcp host 192.168.240.50 host 192.168.24
```

Verificatie

<#root>

```
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
```

De inhoud van alle opnamen bekijken (deze uitvoer kan zeer lang zijn):

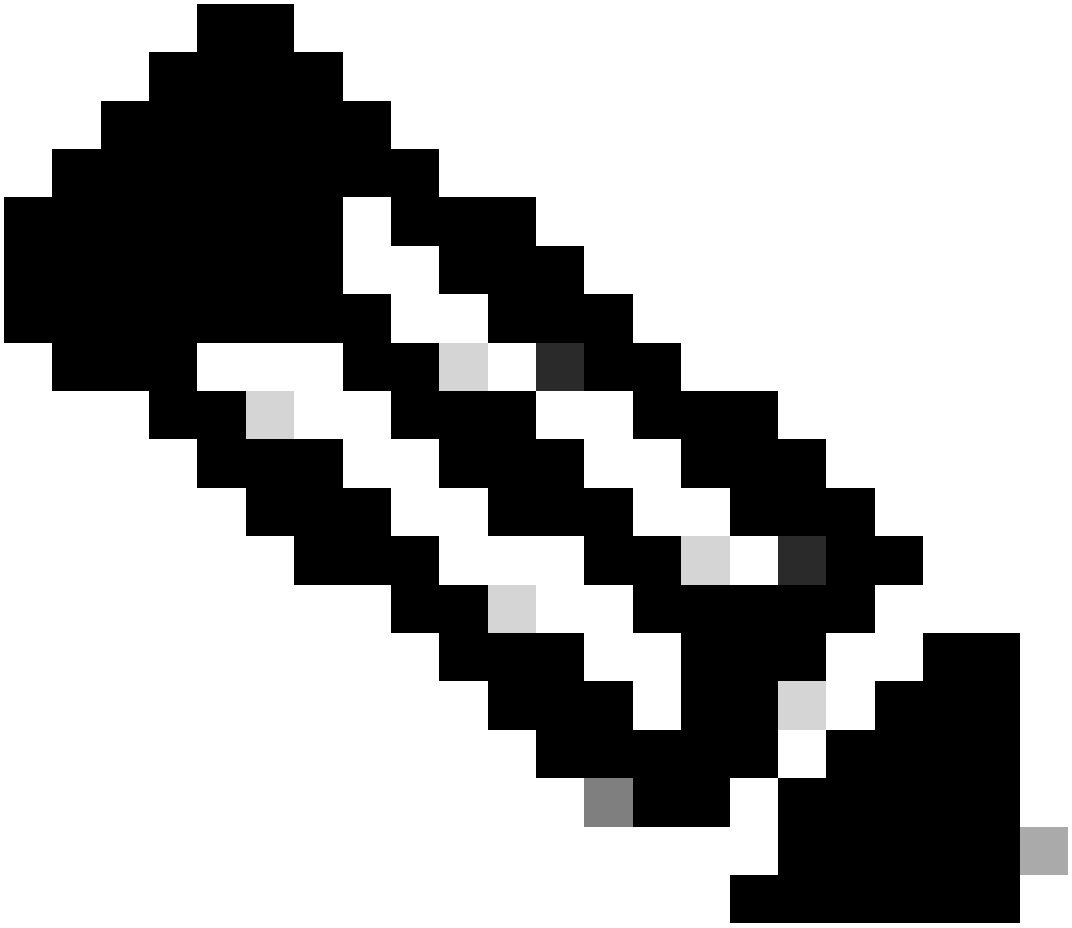
<#root>

```
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
2: 11:33:09.880401 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.45456: S 719653963:719653963(0
3: 11:33:09.880691 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: . ack 719653964 win 229
4: 11:33:09.880783 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: P 2225395910:2225396054

unit-2-1:*************************************************************
0 packet captured
0 packet shown

unit-3-1:*************************************************************
0 packet captured
0 packet shown
```

Opname-sporen

Als u wilt zien hoe de ingangspakketten door het gegevensvlak op elke eenheid worden behandeld, gebruik het spoor sleutelwoord. Dit traceert de eerste 50 ingangspakketten. U kunt tot 1000 ingangspakketten overtrekken.



Opmerking: Als u meerdere opnamen hebt toegepast op een interface, kunt u slechts één pakket één keer overtrekken.

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

<#root>

```
firepower#
```

```
cluster exec cap CAPO int OUTSIDE buff 33554432 trace trace-count 1000 match tcp host 192.168.240.50 hos
```

Zodra u de stroom van belang vangt, moet u ervoor zorgen dat u de pakketten van belang op elke eenheid vindt. Het belangrijkste om te onthouden is dat een specifiek pakket kan worden #1 op unit-1-1, maar #2 op een ander apparaat, enzovoort.

In dit voorbeeld kunt u zien dat SYN/ACK op unit-2-1 is #2, maar op unit-3-1 #1:

```
<#root>

firepower#

cluster exec show capture CAPO | include S.*ack


unit-1-1(LOCAL):*******************************************************
1: 12:58:31.117700 802.1Q vlan#202 P0 192.168.240.50.45468 > 192.168.241.50.80: S 441626016:441626016(0
2: 12:58:31.118341 802.1Q vlan#202 P0 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 P0 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>
```

U kunt als volgt #2 (SYN/ACK) op de lokale unit overtrekken:

```
<#root>

firepower#

cluster exec show cap CAPO packet-number 2 trace


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

2: 12:58:31.118341 802.1Q vlan#202 P0 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
...
```

U kunt als volgt hetzelfde pakket (SYN/ACK) op de afstandsbediening overtrekken:

<#root>

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


1: 12:58:31.111429 802.1Q vlan#202 P0 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-vastlegging

Opname via de CCL-link inschakelen (op alle eenheden):

<#root>

```
firepower#
cluster exec capture CCL interface cluster


unit-1-1(LOCAL):**********************************************************
unit-2-1:**********************************************************
unit-3-1:**********************************************************
```

Verberging opnieuw injecteren

Door gebrek, toont een opname die op een gegevensvlak wordt toegelaten gegevensinterface alle pakketten:

- Degenen die van het fysieke netwerk aankomen
- Degenen die van CCL worden opnieuw geïnjecteerd

Als u de opnieuw geïnjecteerde pakketten niet wilt zien, gebruikt u de optie opnieuw injecteren en verbergen. Dit kan handig zijn als u wilt controleren of een stroom asymmetrisch is:

```
<#root>

firepower#

cluster exec capture CAPI_RH reinject-hide interface INSIDE match tcp host 192.168.240.50 host 192.168.2
```

Deze opname laat alleen zien wat de lokale unit rechtstreeks van het fysieke netwerk ontvangt, en niet van de andere clustereenheden.

ASP-druppels

Als u wilt controleren op softwaredruppels voor een specifieke stroom, kunt u asp-drop-opname inschakelen. Als u niet weet op welke reden u zich moet richten, gebruikt u het trefwoord all. Bovendien, als u niet geinteresseerd bent in de pakketlading, kunt u het kopballen-enige sleutelwoord specificeren. Hierdoor kunt u 20 tot 30 keer meer pakketten vastleggen:

```
<#root>

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 voor de ASP-opname:

```
<#root>

firepower#

cluster exec cap ASP type asp-drop all buffer 33554432 headers-only


match ip host 192.0.2.100 any
```

Opname wissen

Om de buffer van elke opname die in alle clustereenheden loopt, te wissen. Dit stopt de opnamen niet, maar maakt alleen de buffers schoon:

```
<#root>

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 kunt u verder gaan.

Weg 1

```
<#root>

firepower#

cluster exec cap CAPI stop


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

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

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

Hervatten

```
<#root>

firepower#

cluster exec no capture CAPI stop


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

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

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

Weg 2

```
<#root>
firepower#
cluster exec no capture CAPI interface INSIDE

unit-1-1(LOCAL):*********************************************************
unit-2-1:*********************************************************
unit-3-1:*********************************************************
```

Hervatten

```
<#root>
firepower#
cluster exec capture CAPI interface INSIDE

unit-1-1(LOCAL):*********************************************************
unit-2-1:*********************************************************
unit-3-1:*********************************************************
```

Een opname verzamelen

Er zijn meerdere manieren om een opname te exporteren.

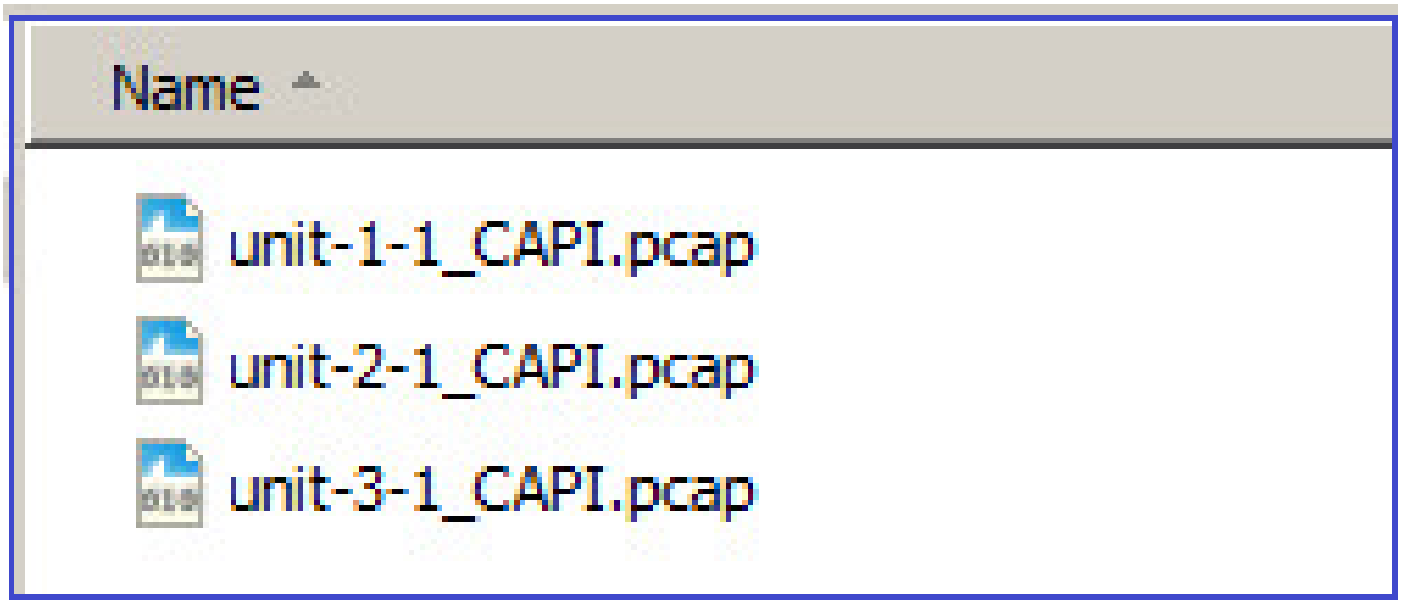
Weg 1 - Naar een externe server

Dit staat u toe om een opname van het gegevensvliegtuig aan een verre server (bijvoorbeeld, TFTP) te uploaden. De opnamenamen worden automatisch gewijzigd om de broneenheid weer te geven:

```
<#root>
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 cap bestanden:



Weg 2 - Vang de opnamen van het VCC

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

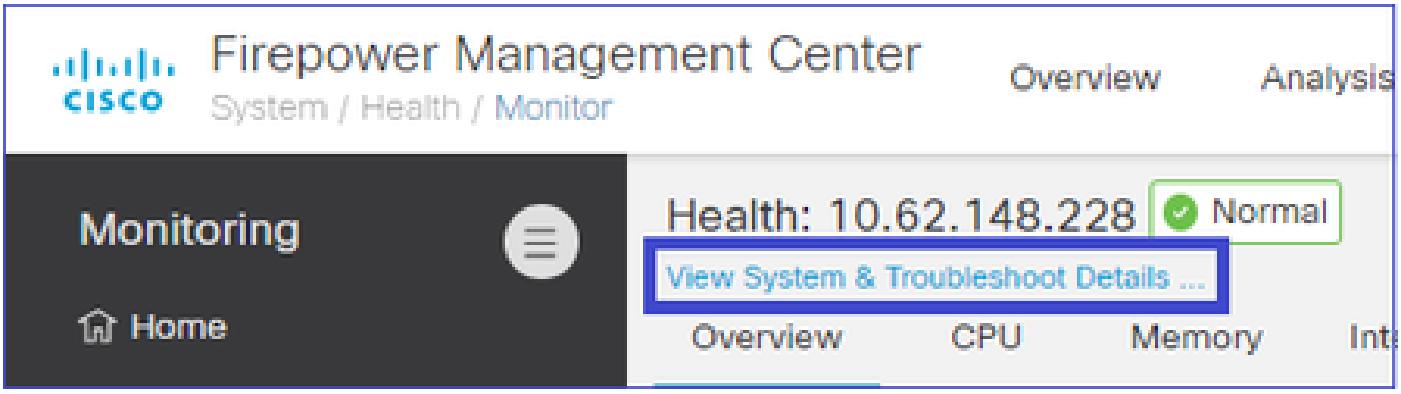
```
<#root>

firepower#

cluster exec copy /pcap capture:CAPI disk0:CAPI.pcap

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

Source capture name [CAPI]?

Destination filename [CAPI.pcap]?
!!!!!
```

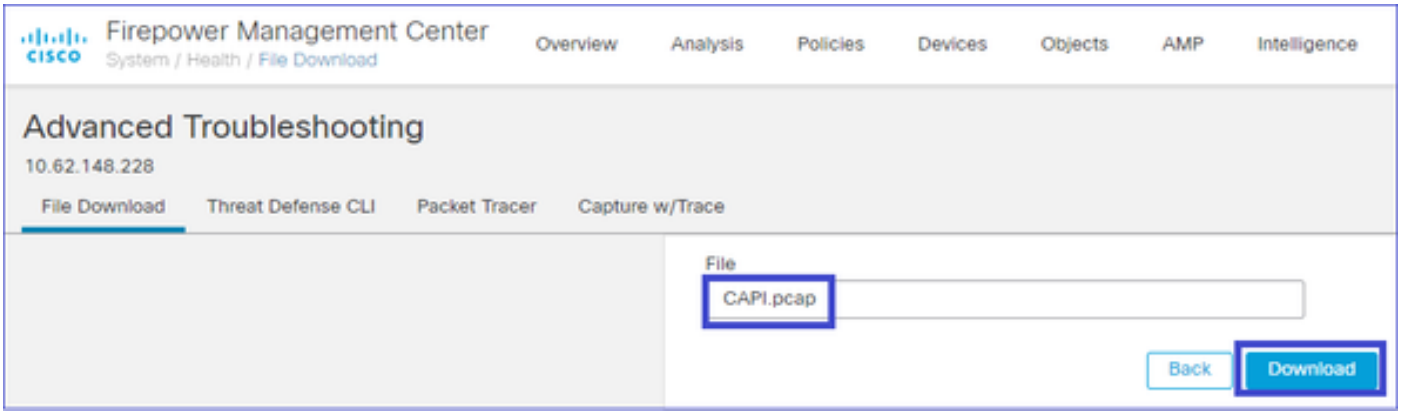
```
62 packets copied in 0.0 secs
```

Kopieer in de expertmodus het bestand van /mnt/disk0/ naar /ngfw/var/common/ directory:

```
<#root>

>

expert

admin@firepower:~$

cd /mnt/disk0

admin@firepower:/mnt/disk0$

sudo cp CAPI.pcap /ngfw/var/common
```

Uiteindelijk, op FMC navigeren naar Systeem > Gezondheid > Monitor sectie. Kies Systeem bekijken en problemen oplossen > Geavanceerde probleemoplossing en haal het opnamebestand:





Een opname verwijderen

Gebruik deze opdracht om een opname uit alle clustereenheden te verwijderen:

<#root>

```
firepower#

cluster exec no capture CAPI


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

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

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

Geoffload-stromen

Op FP41xx/FP9300 kunnen stromen statisch (bijvoorbeeld FastPath-regels) of dynamisch worden geoffload naar HW Accelerator. 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 geoffload, gaan slechts een paar pakketten door het FTD-dataplatform. De rest wordt verwerkt door de HW-versneller (Smart NIC).

Vanuit een opnamepunt betekent dit dat als u alleen FTD-dataplatform inschakelt, u niet alle pakketten ziet die door het apparaat gaan. In dit geval moet u ook FXOS-opnamen op chassisniveau inschakelen.

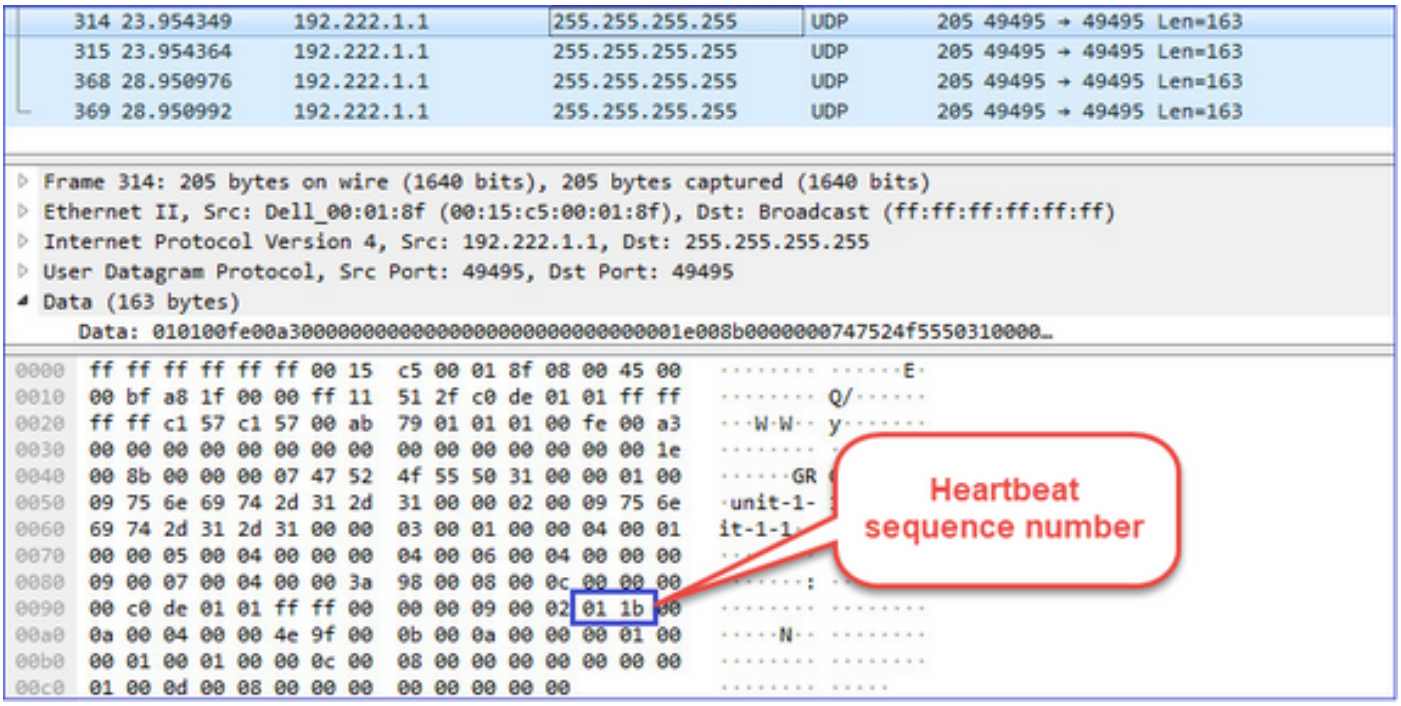
Cluster Control Link (CCL)-berichten

Als u een opname neemt op de CCL, merkt u op 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 clusterunit verzonden op 1/3 van de waarde van de wachttijd voor de gezondheidscontrole. · Merk op dat niet alle UDP 49495-pakketten die in de opname worden gezien, hartslagen zijn · De hartslagen bevatten een volgnummer.
UDP 4193	Cluster Control Protocol-berichten over gegevenspad

	Unicast · Deze pakketten bevatten informatie (metagegevens) over de flow-eigenaar, regisseur, back-up-eigenaar, enzovoort. Voorbeelden hiervan zijn: · Een ‘cluster add’-bericht wordt door de eigenaar naar de directeur gestuurd wanneer een nieuwe flow wordt gecreëerd · Er wordt een ‘cluster delete’-bericht van de eigenaar naar de directeur gestuurd wanneer een stroom wordt afgesloten
Gegevenspakketten	Datapakketten die behoren tot de verschillende verkeersstromen die de cluster passeren

Cluster hartslag



Cluster Control Point (CCP)-berichten

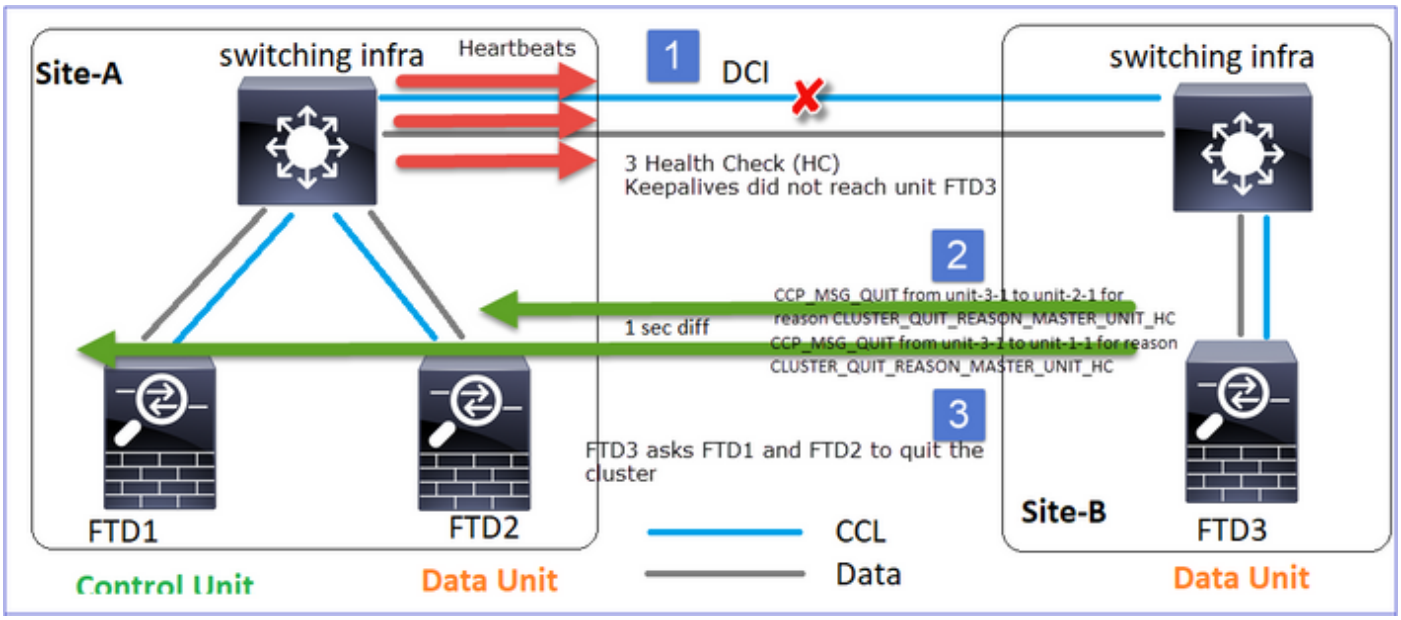
Naast de hartslagberichten zijn er een aantal clustercontroleberichten die in specifieke scenario's via de CCL worden uitgewisseld. Sommige zijn unicastberichten, andere zijn uitzendingen.

CLUSTER_QUIT_REDEN_PRIMAIRE_UNIT_HC

Wanneer een eenheid 3 opeenvolgende hartslagberichten van de controleknoop verliest, genereert zij een CLUSTER_QUIT_REDEN_PRIMAIR_UNIT_HC-bericht via de CLS. Dit bericht:

- Is een unicast.
- Het wordt met een interval van 1 seconden naar elk van de eenheden verzonden.

- Wanneer een eenheid dit bericht ontvangt, wordt het cluster gesloten (UITGESCHAKELD) en wordt het opnieuw aangemeld.

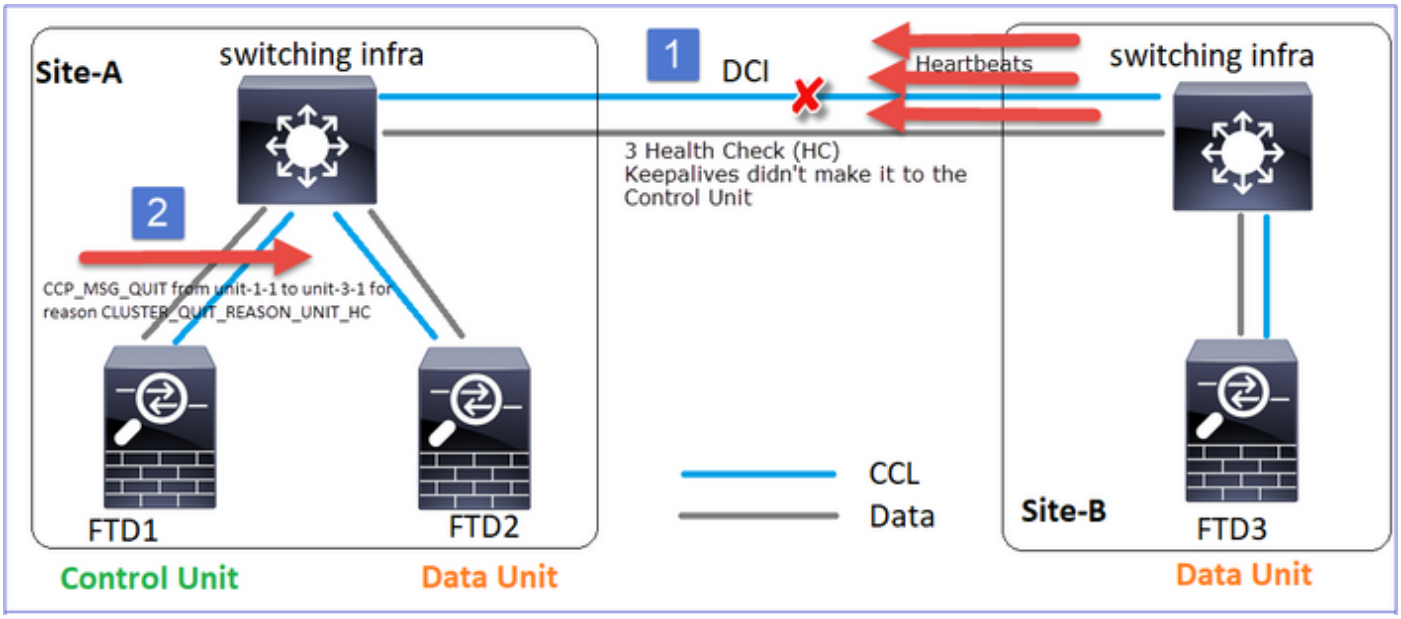


V. Wat is het doel van de CLUSTER_QUIT_REDEN_PRIMAIRE_UNIT_HC?

A. Vanuit het oogpunt van eenheid-3-1 (Site-B) verliest unit-1-1 en unit-2-1 van site A, zodat het deze zo snel mogelijk uit de ledenlijst moet verwijderen, anders kan unit-2-1 pakketverlies hebben als unit-2-1 nog steeds in de ledenlijst staat en unit-2-1 toevallig een verbindingsdirecteur is, en kan flow query naar unit-2-1 mislukken.

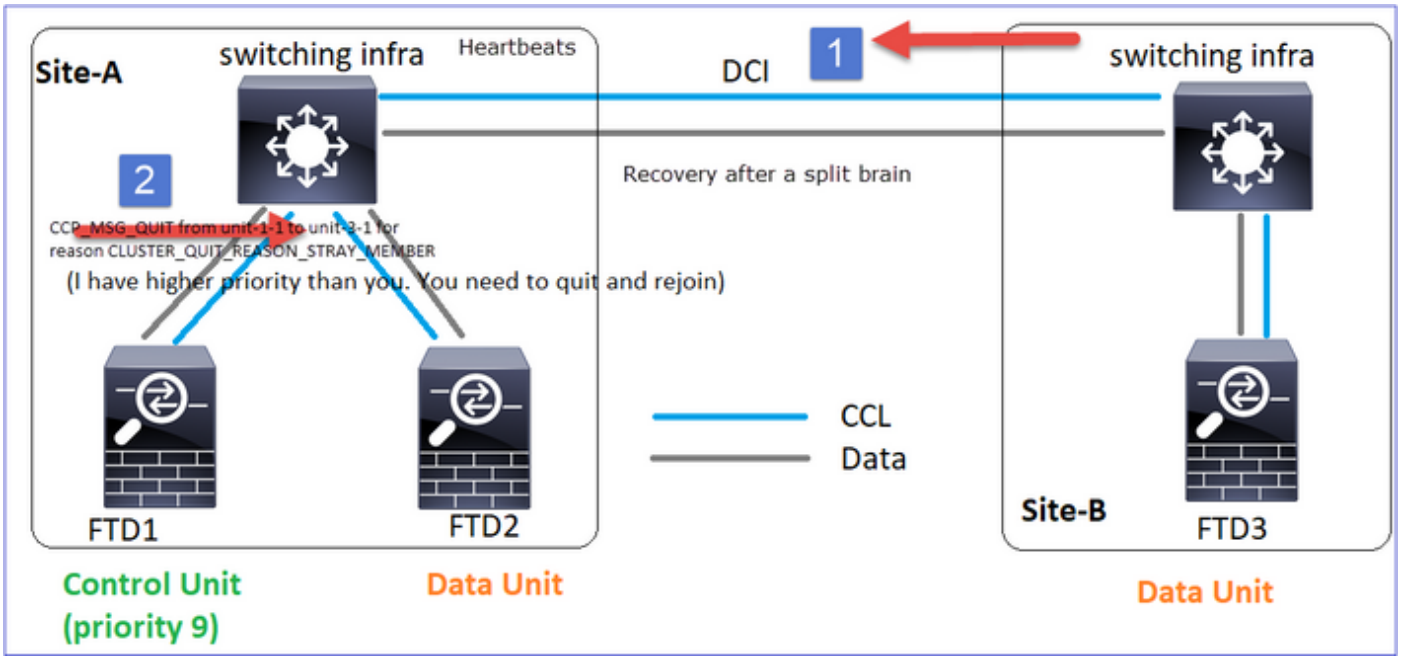
CLUSTER_QUIT_REDEN_UNIT_HC

Wanneer de controleknooppunt 3 opeenvolgende hartslagberichten van een gegevensknooppunt verliest, verstuurt het CLUSTER_QUIT_REDEN_UNIT_HC-bericht via de CCL. Dit bericht is unicast.



CLUSTER_QUIT_REDEN_STRAY_LID

Wanneer een split-partitie opnieuw verbonden is met een peer-partitie, wordt de nieuwe data-node door de dominante control-unit behandeld als een zwerflid en ontvangt een CCP-stopbericht met de reden van CLUSTER_QUIT_REDENSTRAY_STRAY_Member.



CLUSTER_QUIT_LID_UITVAL

Een uitzendingsbericht dat door een gegevensknooppunt wordt gegenereerd en als uitzending wordt verzonden. Zodra een eenheid dit bericht heeft ontvangen, verplaatst het zich naar de status UITGESCHAKELD. Bovendien start automatisch opnieuw toetreden niet op:

<#root>

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

Nov 04 00:22:54.699 [DBUG]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 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-2-1 for reason
CLUSTER_QUIT_MEMBER_DROPOUT
```

De clustergeschiedenis laat zien:

<#root>

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

Mechanisme voor Cluster Health Check (HC)

Hoofdpunten

- Elke clustereenheid stuurt een hartslag om de 1/3 van de waarde van de wachttijd voor de gezondheidscontrole naar alle andere eenheden (uitzending 255.255.255.255) en gebruikt UDP-49495 als transport over de CCL.
- Elke clustereenheid volgt onafhankelijk elke andere eenheid met een Poll timer en een Poll count waarde.
- Als een clustereenheid binnen een hartslaginterval geen pakket (hartslag of gegevenspakket) ontvangt van een cluster per eenheid, verhoogt het de waarde van de Poll Count.
- Wanneer de waarde voor het aantal polls voor een cluster peer unit 3 wordt, wordt de peer neergezet.
- Telkens wanneer een hartslag wordt ontvangen, wordt het volgnummer gecontroleerd en in het geval dat het verschil met de eerder ontvangen hartslag anders is dan 1, neemt het teller van de hartslagdruppel dienovereenkomstig toe.
- Als de teller van de opiniepeiling voor een clusterpeer verschillend is dan 0, en een pakket door de peer wordt ontvangen, wordt de teller teruggesteld aan waarde 0.

Gebruik deze opdracht om de clustergezondheidstellers te controleren:

<#root>

```
firepower#
```

show cluster info health details

```
-------------------------------------------------------------------------------
|                Unit (ID)| Heartbeat| Heartbeat|   Average|   Maximum|      Poll|
|                         |     count|     drops|  gap (ms)| slip (ms)|     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 telling	Het aantal hartslagen die van de verre peer over CCL worden ontvangen.

Hartaandoeningen	Het aantal gemiste hartslagen. Deze teller wordt berekend op basis van het ontvangen hartslag volgnummer.
Gemiddelde kloof	Het gemiddelde tijdsinterval van de ontvangen hartslagen.
Poll count	Wanneer deze teller 3 wordt wordt het apparaat verwijderd uit het cluster. Het poll query interval is hetzelfde als het hartslag interval, maar werkt onafhankelijk.

Gebruik deze opdracht om de tellers opnieuw in te stellen:

<#root>

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

V. Hoe de hartslagfrequentie te verifiëren?

A. Controleer de gemiddelde waarde van de tussenruimte:

<#root>

```
firepower#
show cluster info health details

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

V. Hoe kunt u de clusterhoudtijd op FTD wijzigen?

A. Gebruik FlexConfig

Q. Wie wordt de controleknoop na een spleet-brein?

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

<#root>

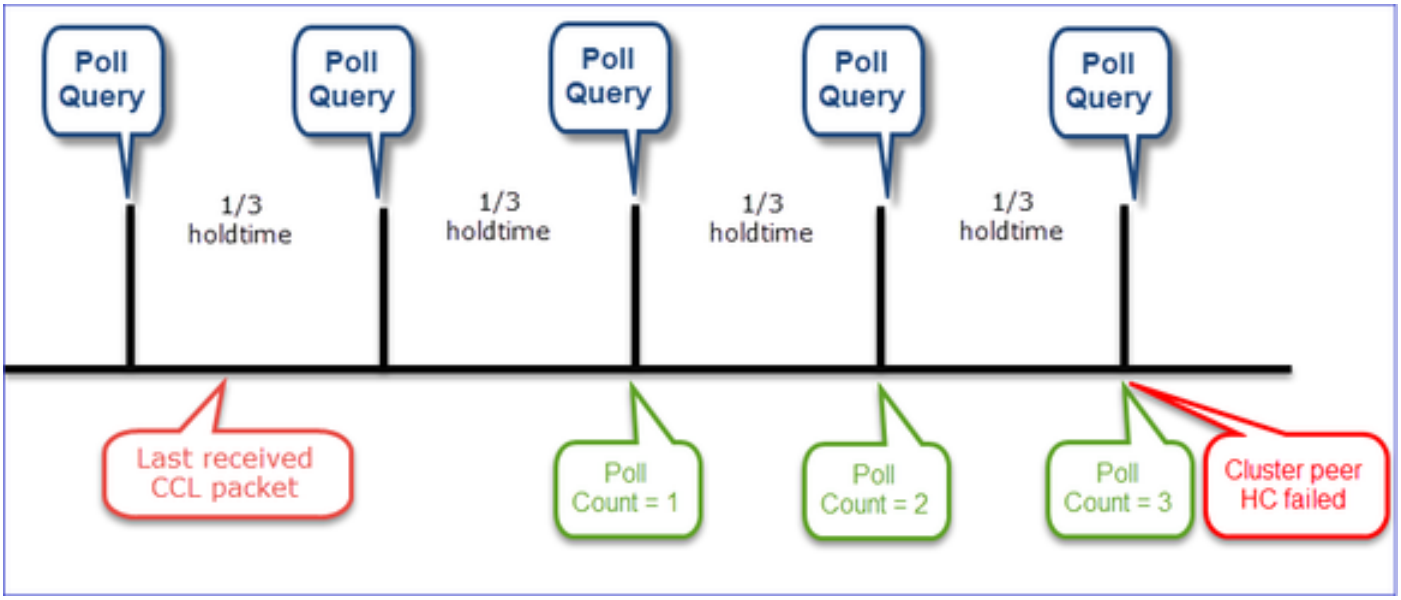
```
firepower#
```

show run cluster | include priority

priority 9

Controleer HC-storing scenario 1 voor meer details.

De visualisatie van het cluster-HC-mechanisme



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

Wachtstandtijd	Vrachtcontrole peiling (frequentie)	Min. detectietijd	Max. detectietijd
3 seconden (standaard)	~1 sec	~3,01 sec	~3,99 sec

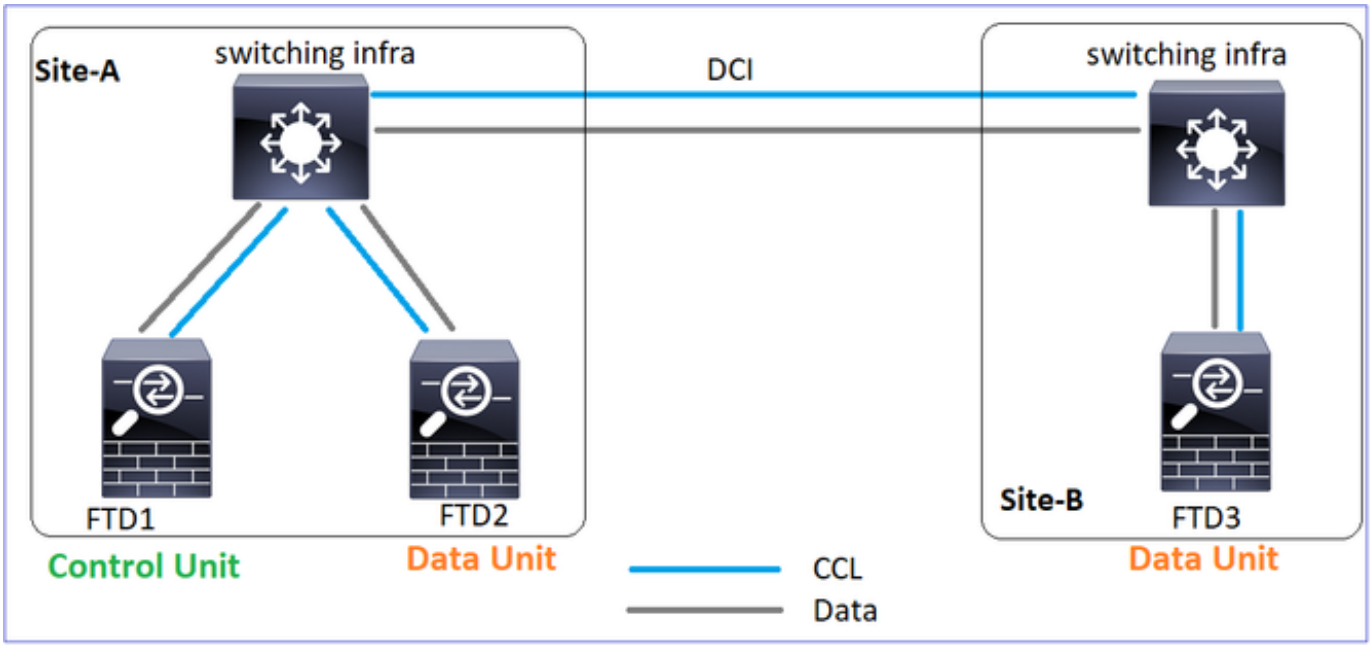
4 sec.	~1,33 sec	~4,01 sec	~5,32 sec
5 sec.	~1,66 sec	~5,01 sec	~6,65 sec
6 sec.	~2 seconden	~6,01 sec	~7,99 sec
7 sec.	~2,33 sec	~7,01 sec	~9,32 sec
8 sec.	~2,66 sec	~8,01 sec	~10,65 sec

Cluster-scenario's voor HC-mislukking

De doelstellingen van dit deel moeten aantonen:

- Verschillende cluster HC-storingsscenario's.
- Hoe de verschillende logbestanden en opdrachtoutput kunnen worden gecorreleerd.

Topologie



Clusterconfiguratie

Eenheid-1-1	Eenheid-2-1
`cluster group GROUP1`	`cluster group GROU`

```
key *****
local-unit unit-1-1
cluster-interface Port-channel48 ip 10.17.1.1 255.255.0.0
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
```

```
key *****
local-unit unit-2-
cluster-interface
priority 17
health-check holdt
health-check data-
health-check clust
health-check syste
health-check monit
site-id 1
enable
```

Clusterstatus

Eenheid-1-1	Eenheid-2-1
<#root> firepower# **show cluster info** Cluster GROUP1: On Interface mode: spanned **This is "unit-1-1" in state PRIMARY** ID : 0 Site ID : 1 Version : 9.12(2)33 Serial No.: FCH22247LNK CCL IP : 10.17.1.1 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-3-1" in state secondary** ID : 1 Site ID : 2 Version : 9.12(2)33 Serial No.: FCH22247MKJ CCL IP : 10.17.3.1 CCL MAC : 0015.c500.038f Last join : 20:58:45 UTC Nov 1 2020 Last leave: 20:58:37 UTC Nov 1 2020	<#root> firepower# **show cluster info** Cluster GROUP1: On Interface mode: spanned **This is "unit-2-1" in state SECONDARY** ID : 2 Site ID : 1 Version : 9.12(2)33 Serial No.: FCH23157Y9N CCL IP : 10.17.2.1 CCL MAC : 0015.c500.028 Last join : 20:44:46 UTC Last leave: 20:44:38 UTC Other members in the cluster: **Unit "unit-1-1" in state PRIMARY** ID : 0 Site ID : 1 Version : 9.12(2)33 Serial No.: FCH22247LNK CCL IP : 10.17.1.1 CCL MAC : 0015.c500.018 Last join : 20:25:36 UTC Last leave: 20:25:28 UTC

Unit "unit-2-1" in state SECONDARY ID : 2 Site ID : 1 Version : 9.12(2)33 Serial No.: FCH23157Y9N CCL IP : 10.17.2.1 CCL MAC : 0015.c500.028f Last join : 20:44:45 UTC Nov 1 2020 Last leave: 20:44:38 UTC Nov 1 2020	**Unit "unit-3-1" in state SECONDARY** ID : 1 Site ID : 2 Version : 9.12(2)33 Serial No.: FCH22247MKJ CCL IP : 10.17.3.1 CCL MAC : 0015.c500.038 Last join : 20:58:45 UTC Last leave: 20:58:37 UTC

Scenario 1

CCL-communicatieverlies voor ~4+ sec in beide richtingen.

Voor de storing

FTD1	FTD2	FTD3
Site-A	Site-A	Site-B
Control-knooppunt	Gegevensknooppunt	Gegevensknooppunt

Na het herstel (geen wijzigingen in de eenheidsrollen)

FTD1	FTD2	FTD3
Site-A	Site-A	Site-B
Control-knooppunt	Gegevensknooppunt	Gegevensknooppunt

Analyse

De fout (CCL-communicatie is verloren gegaan).

Het gegevensvlak console-bericht op unit-3-1:

<#root>

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


Cluster unit unit-3-1 transitioned from SECONDARY to PRIMARY


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.
```

Eenheid-1-1 clustertraceerlogboeken:

<#root>

```
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 0x
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

[DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_MEMBER_DRO


Nov 02 09:38:14.239 [INFO]Notify chassis de-bundle port for blade unit-3-1, stack 0x000055a8917eb596 0x
Nov 02 09:38:14.239

[DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_REASON_UN


Nov 02 09:38:14.239 [CRIT]Received heartbeat event 'SECONDARY heartbeat failure' for member unit-3-1 (I
```

Split-brain

Eenheid-1-1	Eenheid-2-1

```
<#root>
firepower#
show cluster info

Cluster GROUP1: On
    Interface mode: spanned

This is "unit-1-1" in state PRIMARY

        ID        : 0
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH22247LNK
        CCL IP    : 10.17.1.1
        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 SECONDARY
        ID        : 2
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH23157Y9N
        CCL IP    : 10.17.2.1
        CCL MAC   : 0015.c500.028f
        Last join : 20:44:45 UTC Nov 1 2020
        Last leave: 20:44:38 UTC Nov 1 2020
```

```
<#root>
firepower#
show cluster info

Cluster GROUP1: On
    Interface mode: spanned
    This is "unit-2-1" in state S
        ID        : 2
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH23157Y9N
        CCL IP    : 10.17.2.1
        CCL MAC   : 0015.c500.028
        Last join : 20:44:46 UTC
        Last leave: 20:44:38 UTC
Other members in the cluster:

Unit "unit-1-1" in state PRIMARY

        ID        : 0
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH22247LNK
        CCL IP    : 10.17.1.1
        CCL MAC   : 0015.c500.018
        Last join : 20:25:36 UTC
        Last leave: 20:25:28 UTC
```

Clustergeschiedenis

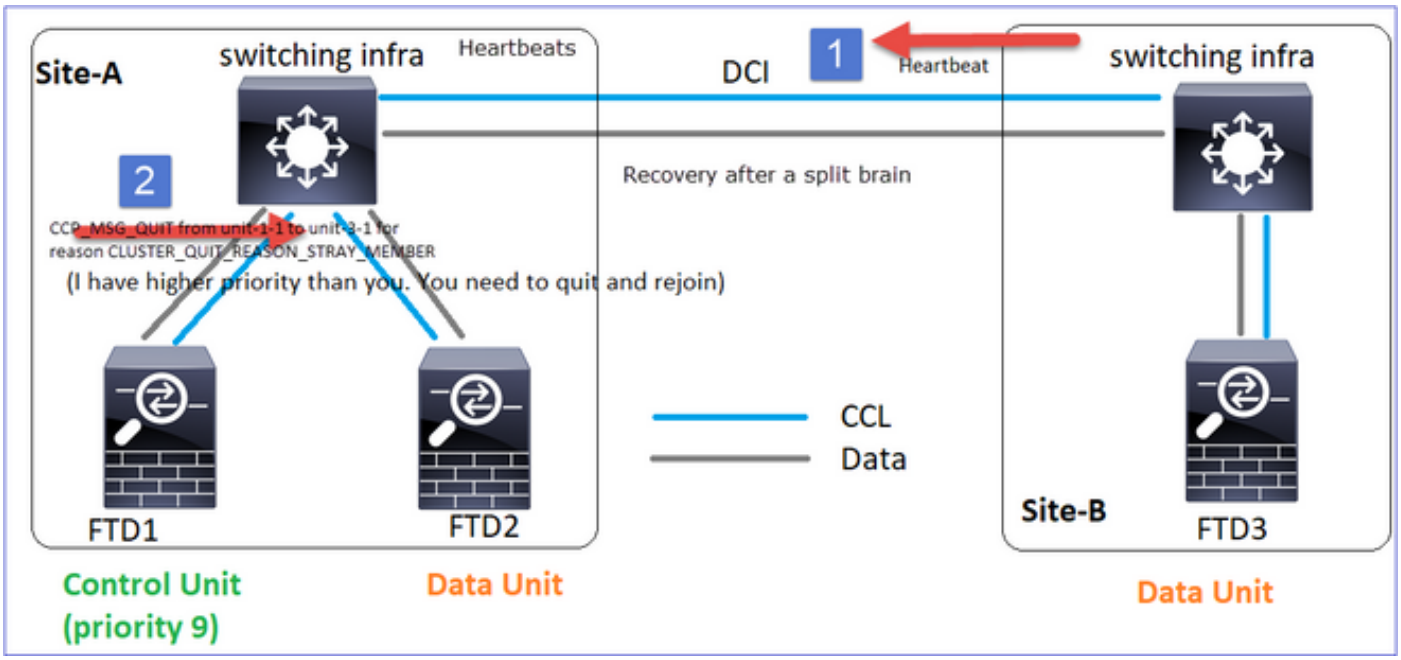
Eenheid-1-1	Eenheid-2-1	Eenheid-3-1
Geen gebeurtenissen	Geen gebeurtenissen	<#root> 09:38:16 UTC Nov 2 2020 **SECONDARY PRIMARY_POST_CONFIG Prim** 09:38:17 UTC Nov 2 2020 PRIMARY_POST_CONFIG Primary Primary

Terugzetten van CCL-communicatie

Unit-1-1 detecteert het huidige controleknooppunt en aangezien unit-1-1 een hogere prioriteit

heeft, stuurt hij een Cluster_QUIT_REDEN_STRAY_Member bericht naar unit-3-1 om een nieuw verkiezingsproces te starten. Uiteindelijk wordt unit-3-1 opnieuw toegevoegd als gegevensknooppunt.

Wanneer een split-partitie opnieuw verbonden is met een peer-partitie, wordt de data-node door de dominante control-node behandeld als een zwerflid en ontvangt een CCP-stop msg met een reden van CLUSTER_QUIT_REDENSTRAY_STRAY_Member.



<#root>

```
Unit-3-1 console logs show:
```

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

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

Detected Cluster Primart.

```
Beginning configuration replication from Primary.
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
..
Cryptochecksum (changed): a9ed686f 8e2e689c 2553a104 7a2bd33a
End configuration replication from Primary.
```

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

Beide eenheden (unit-1-1 en unit-3-1) tonen in hun clusterlogboeken:

<#root>

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

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

<#root>

```
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 a
Nov 03 2020 21:20:23: %FTD-4-747016: Clustering: Found a split cluster with both unit-1-1 and unit-3-1 a
```

Clustergeschiedenis

Eenheid-1-1	Eenheid-2-1	Eenheid-3-1
Geen gebeurtenissen	Geen gebeurtenissen	<#root> 09:47:33 UTC Nov 2 2020 **Primary DISABLED Detected a splitted cluster** 09:47:38 UTC Nov 2 2020 DISABLED ELECTION Enabled from CL 09:47:38 UTC Nov 2 2020 ELECTION SECONDARY_COLD Received cl 09:47:38 UTC Nov 2 2020 SECONDARY_COLD SECONDARY_APP_SYNC Client 09:48:18 UTC Nov 2 2020 SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDA 09:48:29 UTC Nov 2 2020 SECONDARY_CONFIG SECONDARY_FILESYS Configu 09:48:30 UTC Nov 2 2020 SECONDARY_FILESYS SECONDARY_BULK_SYNC Client 09:48:54 UTC Nov 2 2020 SECONDARY_BULK_SYNC **SECONDARY** Client progression done

Scenario 2

CCL-communicatieverlies gedurende ~3-4 seconden in beide richtingen.

Voor de storing

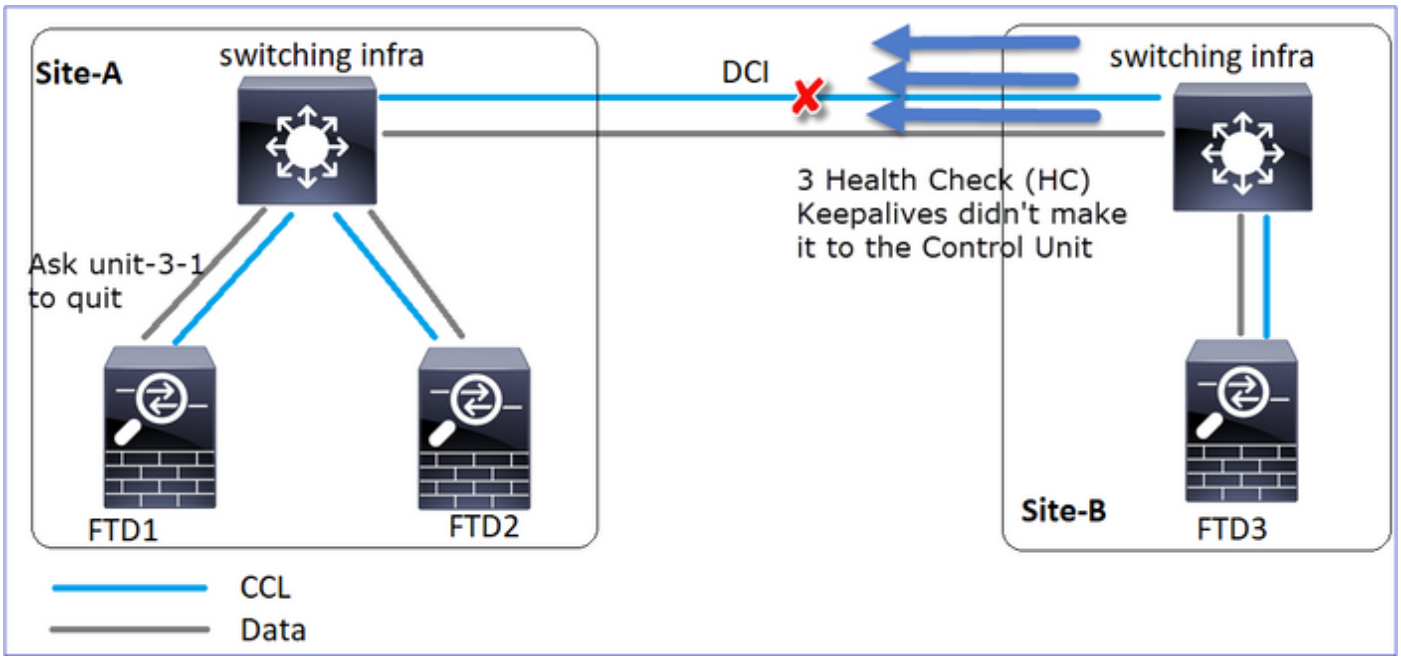
FTD1	FTD2	FTD3
Site-A	Site-A	Site-B
Control-knooppunt	Gegevensknooppunt	Gegevensknooppunt

Na het herstel (geen wijzigingen in de eenheidsrollen)

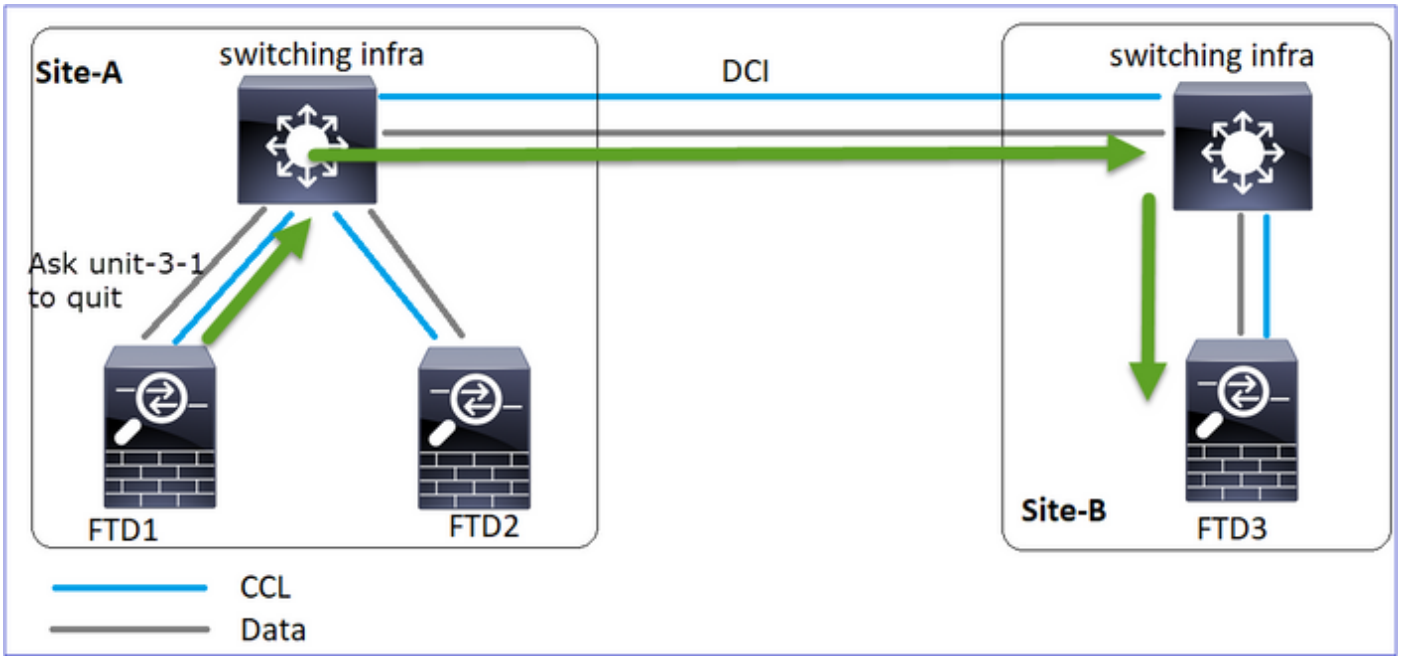
FTD1	FTD2	FTD3
Site-A	Site-A	Site-B
Control-knooppunt	Gegevensknooppunt	Gegevensknooppunt

Analyse

Fase 1: Het controleknooppunt verliest 3 HC's uit eenheid-3-1 en verstuurt een bericht naar eenheid-3-1 om het cluster te verlaten.



Fase 2: De CCL herstelde heel snel en het Cluster_QUIT_REDEN_STRAY_Member bericht van de controleknooppunt kwam aan de kant van de afstandsbediening. Unit-3-1 gaat rechtstreeks naar de DISABLED-modus en er is geen split-brain



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

<#root>

```
firepower#
Asking SECONDARY 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:

<#root>

```
firepower#
```

Cluster disable

```
 is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clust
```

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

Cluster unit-3-1 is overgegaan naar een UITGESCHAKELD toestand en zodra de CCL-communicatie is hersteld, wordt het opnieuw als gegevensknooppunt aangesloten:

```
<#root>

firepower#

show cluster history


20:58:40 UTC Nov 1 2020

SECONDARY                  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              SECONDARY_COLD            Received cluster control message
20:58:45 UTC Nov 1 2020
SECONDARY_COLD            SECONDARY_APP_SYNC        Client progression done
20:59:33 UTC Nov 1 2020
SECONDARY_APP_SYNC        SECONDARY_CONFIG          SECONDARY application configuration sync done
20:59:44 UTC Nov 1 2020
SECONDARY_CONFIG          SECONDARY_FILESYS         Configuration replication finished
20:59:45 UTC Nov 1 2020
SECONDARY_FILESYS         SECONDARY_BULK_SYNC       Client progression done
21:00:09 UTC Nov 1 2020

SECONDARY_BULK_SYNC       SECONDARY

                Client progression done
```

Scenario 3

CCL-communicatieverlies gedurende ~3-4 seconden in beide richtingen.

Voor de mislukking.

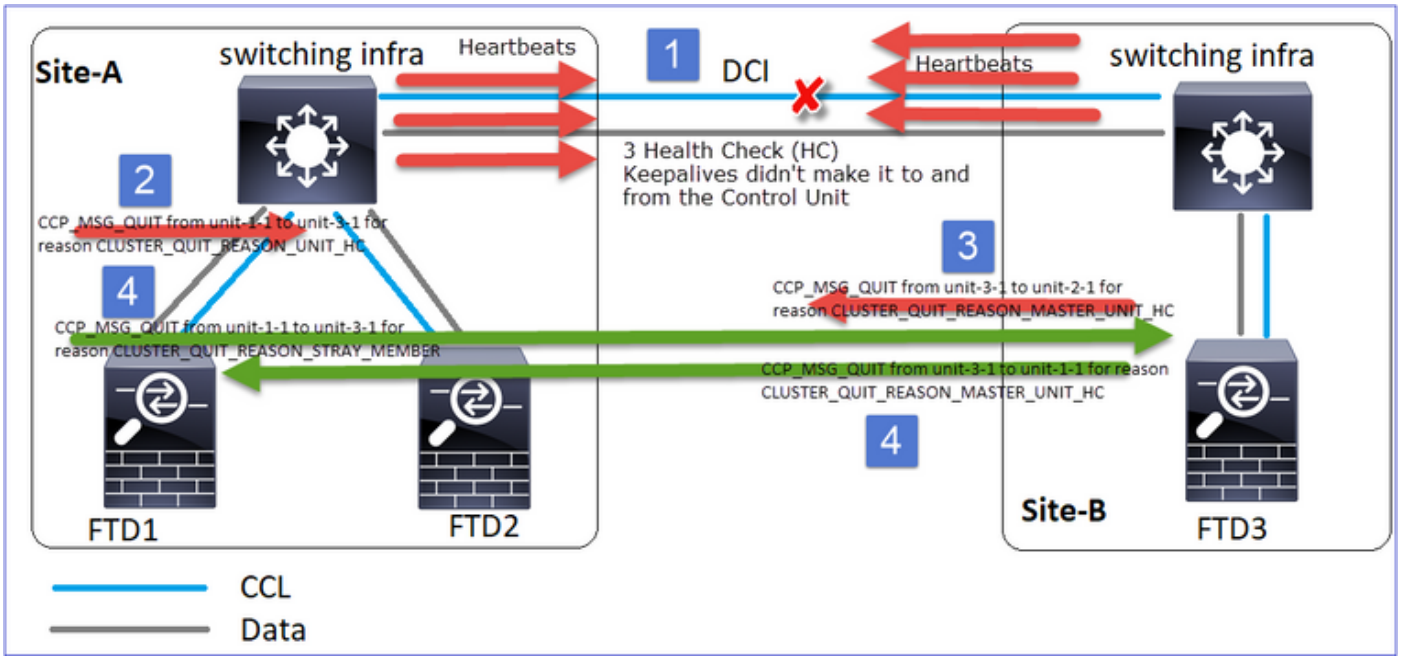
FTD1	FTD2	FTD3
Site-A	Site-A	Site-B
Control-knooppunt	Gegevensknooppunt	Gegevensknooppunt

Na het herstel (het controleknooppunt is gewijzigd).

FTD1	FTD2	FTD3
Site-A	Site-A	Site-B

Gegevensknooppunt	Control-knooppunt	Gegevensknooppunt

Analyse



1. CCL gaat omlaag.
2. Eenheid-1-1 krijgt geen 3 HC-berichten van eenheid-3-1 en verstuurt een QUIT-bericht naar eenheid-3-1. Dit bericht bereikt nooit eenheid-3-1.
3. Eenheid-3-1 verstuurt een QUIT-bericht naar eenheid-2-1. Dit bericht bereikt eenheid-2-1 nooit.

CCL herstelt.

4. Unit-1-1 ziet dat unit-3-1 zichzelf adverteerde als een control node en verstuurt QUIT_REDEN_STRAY_Member bericht naar unit-3-1. Zodra unit-3-1 dit bericht krijgt, gaat het naar een DISABLED state. Tegelijkertijd verstuurt unit-3-1 een QUIT_REDEN_PRIMAIR_UNIT_HC bericht naar unit-1-1 en vraagt het om te stoppen. Zodra unit-1-1 dit bericht krijgt, gaat het naar een UITGESCHAKELD toestand.

Clustergeschiedenis

Eenheid-1-1
<#root> 19:53:09 UTC Nov 2 2020 **PRIMARY DISABLED** Received control message DISABLE (primary unit health check failure)

```
19:53:13 UTC Nov 2 2020
DISABLED              ELECTION         Enabled from CLI
19:53:13 UTC Nov 2 2020
ELECTION              SECONDARY_COLD       Received cluster control message
19:53:13 UTC Nov 2 2020
SECONDARY_COLD            SECONDARY_APP_SYNC   Client progression done
19:54:01 UTC Nov 2 2020
SECONDARY_APP_SYNC        SECONDARY_CONFIG     SECONDARY application configur
19:54:12 UTC Nov 2 2020
SECONDARY_CONFIG          SECONDARY_FILESYS    Configuration replication fini
19:54:13 UTC Nov 2 2020
SECONDARY_FILESYS         SECONDARY_BULK_SYNC  Client progression done
19:54:37 UTC Nov 2 2020
SECONDARY_BULK_SYNC

      SECONDARY

           Client progression done
```

Scenario 4

CCL-communicatieverlies voor ~3-4 seconden

Voor de storing

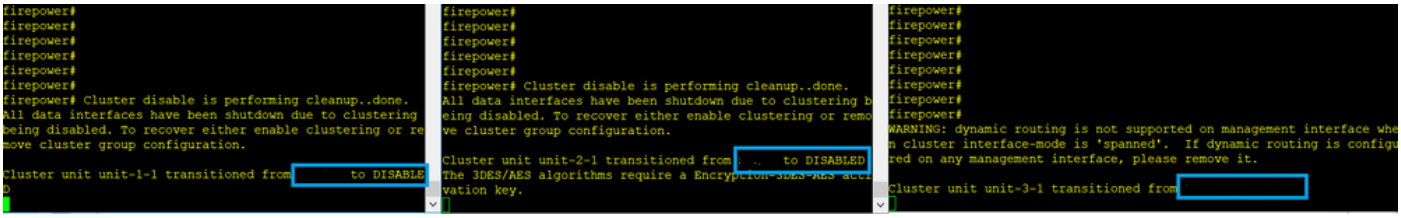
FTD1	FTD2	FTD3
Site-A	Site-A	Site-B
Control-knooppunt	Gegevensknooppunt	Gegevensknooppunt

Na het herstel (het controleknooppunt is van locatie veranderd)

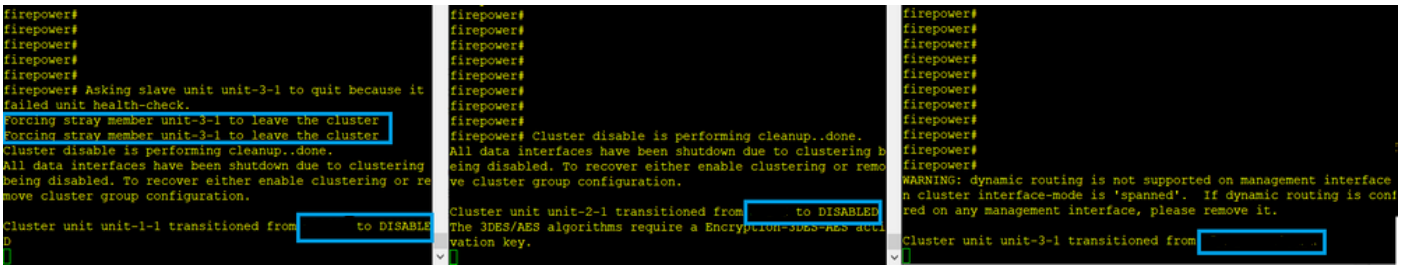
FTD1	FTD2	FTD3
Site-A	Site-A	Site-B
Gegevensknooppunt	Gegevensknooppunt	Control-knooppunt

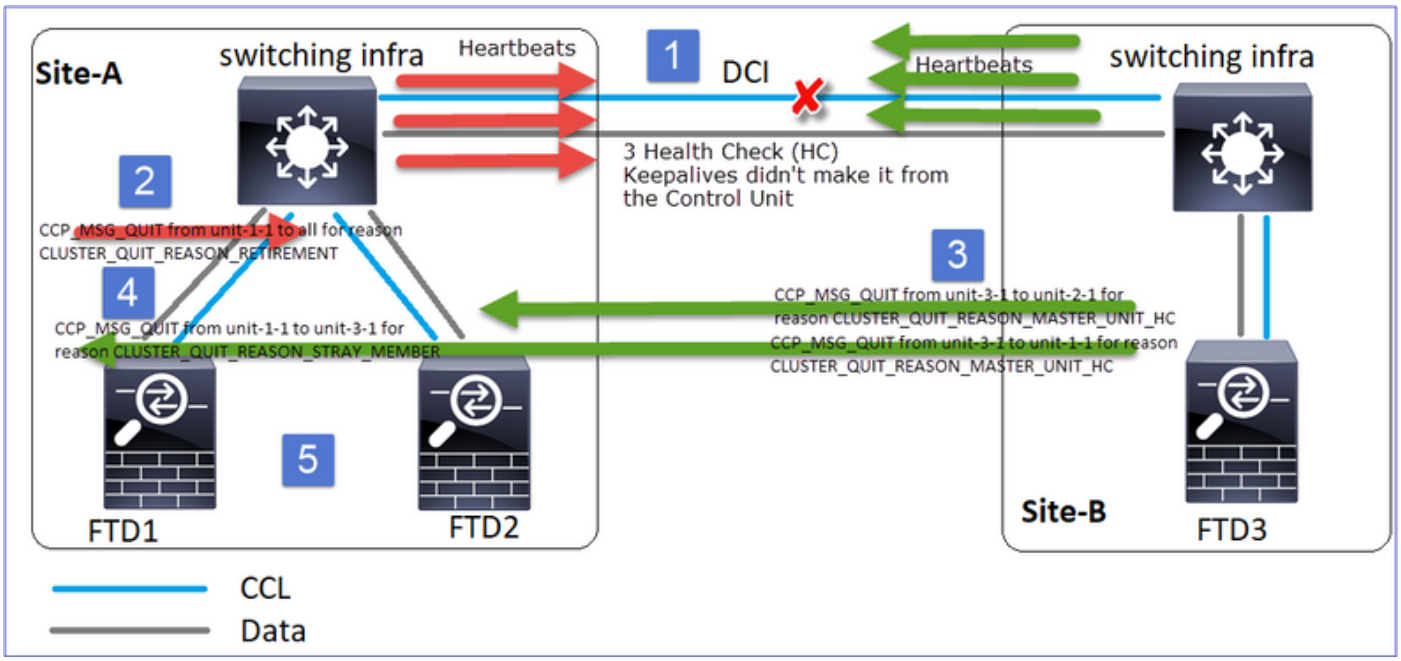
Analyse

De mislukking

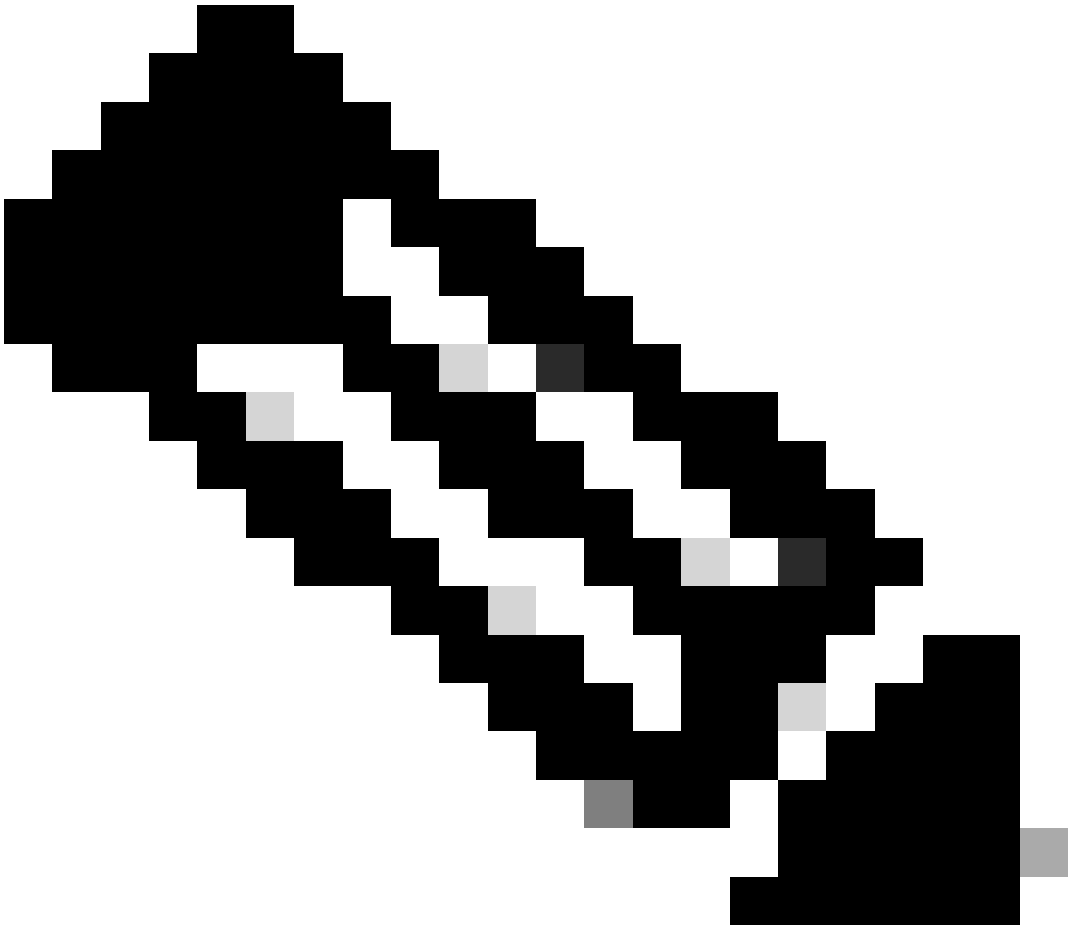


Een andere smaak van dezelfde mislukking. In dit geval kreeg de unit-1-1 ook geen 3 HC-berichten van de unit-3-1 en toen er een nieuwe keepalive kwam, probeerde de unit-3-1 eruit te schoppen met behulp van een STRAY-bericht, maar dat bericht haalde het nooit naar de unit-3-1:





1. CCL wordt een paar seconden eenrichtingsvrij. Unit-3-1 ontvangt geen 3 HC-berichten van unit-1-1 en wordt een controleknooppunt.
2. Unit-2-1 verstuurt een CLUSTER_QUIT_REDEN_RETIrement bericht (broadcast).
3. Eenheid-3-1 stuurt een QUIT_REDEN_PRIMAIR_UNIT_HC-bericht naar eenheid-2-1. Eenheid-2-1 ontvangt het bericht en beëindigt het cluster.
4. Eenheid-3-1 stuurt een QUIT_REDEN_PRIMAIR_UNIT_HC-bericht naar eenheid-1-1. Eenheid-1-1 ontvangt het bericht en beëindigt het cluster. CCL herstelt.
5. Eenheden-1-1 en 2-1 voegen het cluster opnieuw toe als gegevensknooppunten.



> Opmerking: Als in stap 5 de CCL niet herstelt, dan wordt in site-A de FTD1 de nieuwe controleknooppunt, en na het herstel van de CCL wint het de nieuwe verkiezing.

Syslogberichten op unit-1-1:

<#root>

```
firepower#
```

show log | include 747

```
Nov 03 2020 23:13:08: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE
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
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 PRIMARY 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 (sta
Nov 03 2020 23:13:18: %FTD-6-747004: Clustering: State machine changed from state ELECTION to ONCALL
```

Cluster sporenlogboeken op unit-1-1:

<#root>

firepower#

show cluster info trace | include QUIT

```
Nov 03 23:13:10.789 [DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 for reason CLUSTER_QUIT_R
Nov 03 23:13:10.769 [DBUG]
```

Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-1-1 for reason CLUSTER_QUIT_REASON_PRIMARY_UNIT_

```
Nov 03 23:13:10.769 [DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason C
Nov 03 23:13:09.789 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-2-1 for reason CLUSTER_QUIT_REASO
Nov 03 23:13:09.769 [DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason C
Nov 03 23:13:08.559 [DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CL
Nov 03 23:13:08.559 [DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason C
```

Syslog-berichten op unit-3-1:

<#root>

firepower#

show log | include 747

```
Nov 03 2020 23:13:09: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE
Nov 03 2020 23:13:10: %FTD-7-747005: Clustering: State machine notify event CLUSTER_EVENT_MEMBER_STATE
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering:
```

State machine changed from state SECONDARY to PRIMARY

```
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state PRIMARY_FAST to PRIMA
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state PRIMARY_DRAIN to PRIM
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state PRIMARY_CONFIG to PRI
Nov 03 2020 23:13:10: %FTD-7-747006: Clustering: State machine is at state PRIMARY_POST_CONFIG
```

```
Nov 03 2020 23:13:10: %FTD-6-747004: Clustering: State machine changed from state PRIMARY_POST_CONFIG t
Nov 03 2020 23:13:10: %FTD-7-747006: Clustering:
```

State machine is at state PRIMARY

Clustergeschiedenis

Eenheid-1-1
<#root> 23:13:13 UTC Nov 3 2020 **PRIMARY DISABLED Received control message DISABLE** **(primary 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 SECONDARY_COLD Received cluster control message 23:14:48 UTC Nov 3 2020 SECONDARY_COLD SECONDARY_APP_SYNC Client progression done 23:15:36 UTC Nov 3 2020 SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDARY application configuration sync done 23:15:48 UTC Nov 3 2020 SECONDARY_CONFIG SECONDARY_FILESYS Configuration replication finished 23:15:49 UTC Nov 3 2020 SECONDARY_FILESYS SECONDARY_BULK_SYNC Client progression done 23:16:13 UTC Nov 3 2020 SECONDARY_BULK_SYNC **SECONDARY** Client progression done

Scenario 5

Voor de storing

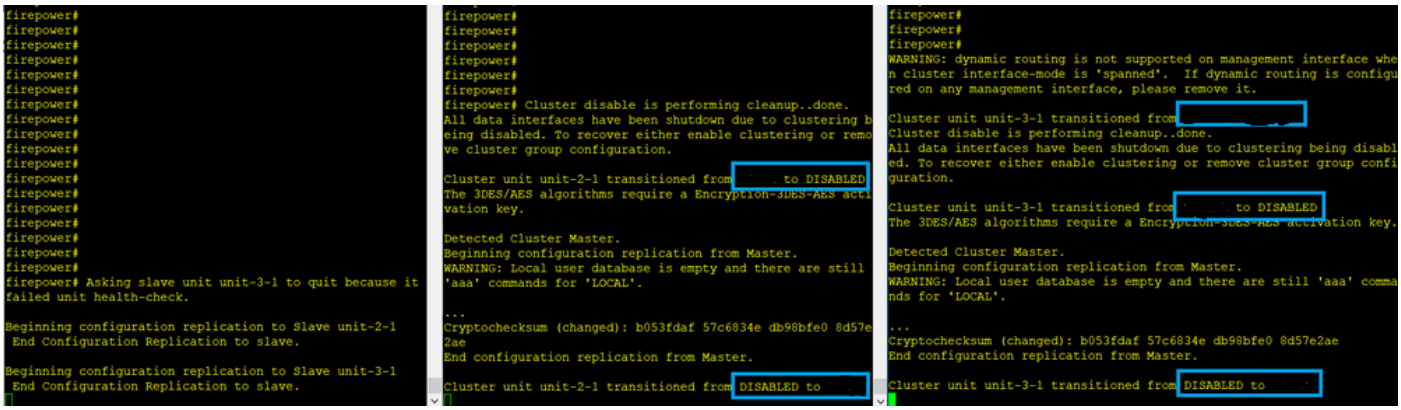
FTD1	FTD2	FTD3

Site-A	Site-A	Site-B
Control-knooppunt	Gegevensknooppunt	Gegevensknooppunt

Na het herstel (geen wijzigingen)

FTD1	FTD2	FTD3
Site-A	Site-A	Site-B
Control-knooppunt	Gegevensknooppunt	Gegevensknooppunt

De mislukking



Unit-3-1 stuurde QUIT-berichten naar zowel unit-1-1 als unit-2-1, maar vanwege problemen met de connectiviteit ontving unit-2-1 alleen het QUIT-bericht.

Eenheid-1-1 clustertraceerlogboeken:

<#root>

```
firepower#
```

show cluster info trace | include QUIT

```
Nov 04 00:52:10.429 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 for reason CLUSTER_QUIT_REASO
Nov 04 00:51:47.059 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-2-1 for reason CLUSTER_QUIT_REASO
Nov 04 00:51:45.429 [DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CL
Nov 04 00:51:45.429 [DBUG]Send CCP message to unit-3-1(1): CCP_MSG_QUIT from unit-1-1 to unit-3-1 for r
```

Eenheid-2-1 clustertraceerlogboeken:

<#root>

firepower#

show cluster info trace | include QUIT

Nov 04 00:52:10.389 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-3-1 for reason CLUSTER_QUIT_REASO
Nov 04 00:51:47.019 [DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-2-1 for reason CLUSTER_QUIT_R
Nov 04 00:51:46.999 [DBUG]

Receive CCP message: CCP_MSG_QUIT from unit-3-1 to unit-2-1 for reason CLUSTER_QUIT_REASON_PRIMARY_UNIT_

Nov 04 00:51:45.389 [DBUG]Receive CCP message: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTE

Clustergeschiedenis

Eenheid-1-1	Eenheid-2-1
Geen gebeurtenissen	<#root> 00:51:50 UTC Nov 4 2020 **SECONDARY DISABLED Received control message DISABLE** **(primary unit health check failure)** 00:51:54 UTC Nov 4 2020 DISABLED ELECTION Enabled from CLI 00:51:54 UTC Nov 4 2020 ELECTION SECONDARY_COLD Received cluster control me 00:51:54 UTC Nov 4 2020 SECONDARY_COLD SECONDARY_APP_SYNC Client progression done 00:52:42 UTC Nov 4 2020 SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDARY application c sync done 00:52:54 UTC Nov 4 2020 SECONDARY_CONFIG SECONDARY_FILESYS Configuration replicati 00:52:55 UTC Nov 4 2020 SECONDARY_FILESYS SECONDARY_BULK_SYNC Client progression done 00:53:19 UTC Nov 4 2020 SECONDARY_BULK_SYNC **SECONDARY** Client progression done

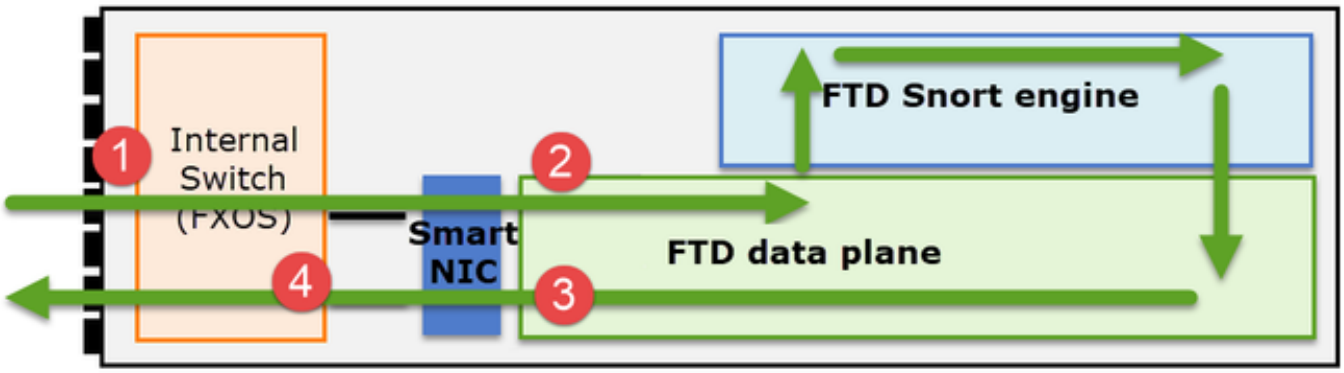
Connectie met Cluster-dataplane

NGFW opnamepunten

De NGFW biedt opnamemogelijkheden op deze punten:

- Interne switch chassis (FXOS)
- FTD-dataplatformmotor
- FTD Snort-engine

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



1. FXOS-toegangsopname op de fysieke interface
2. FTD-ingangsopname in dataplatformmotor
3. FTD uitgaande vastlegging in dataplatformmotor
4. FXOS-toegangsopname op backplane interface

Controleer dit document voor meer informatie over NGFW-opnamen:

Cluster Unit Flow Roles Basics

Verbindingen kunnen op meerdere manieren via een cluster tot stand worden gebracht, afhankelijk van factoren zoals:

- Type verkeer (TCP, UDP, enzovoort)
- Algoritme voor taakverdeling geconfigureerd op de aangrenzende switch
- Functies die zijn geconfigureerd op de firewall
- Netwerkvoorwaarden (bijvoorbeeld IP-fragmentatie, netwerkvertragingen enzovoort)

Stroomrol	Beschrijving	Vlag(en)
Eigenaar	Meestal de eenheid die de aansluiting	UIO

	aanvankelijk ontvangt	
Directeur	De eenheid die eigenaarsopzoekverzoeken van doorgevers verwerkt.	Y
Reserve-eigenaar	Zolang de regisseur niet dezelfde eenheid is als de eigenaar, dan is de regisseur ook de backup-eigenaar. Als de eigenaar zichzelf kiest als regisseur, dan wordt een aparte back-up eigenaar gekozen.	Y (als de director ook de backup-eigenaar is) y (als de director niet de backup-eigenaar is)
doorgeefster	Een eenheid die pakketten doorstuurt naar de eigenaar	z
Eigenaar van fragment	De eenheid die het gefragmenteerde verkeer verwerkt	-
Back-uplijn chassis	In een interchassiscluster waarin zowel regisseur/back-up als eigenaarsstromen eigendom zijn van de eenheden van hetzelfde chassis, wordt een eenheid in een van de andere chassis een secundaire back-up/directeur. Deze rol is specifiek voor interchassisclusters van de Firepower 9300-serie met meer dan 1 blade.	w

- Voor meer informatie, raadpleeg de betreffende sectie in de Configuratiehandleiding (zie koppelingen in de bijbehorende informatie)
- In specifieke scenario's (zie het gedeelte over casestudy's) worden sommige vlaggen niet altijd getoond.

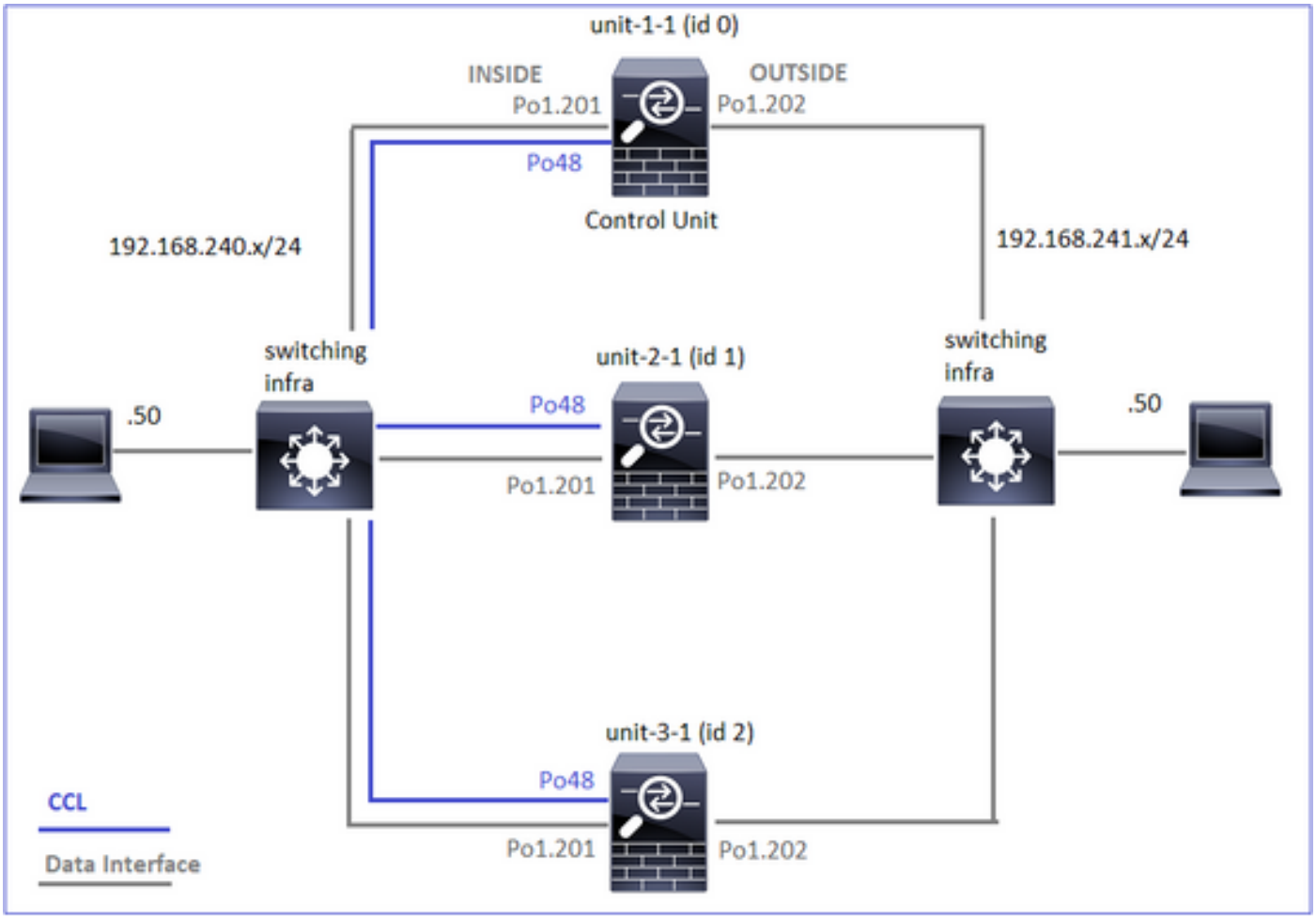
Casestudy’s voor clusterverbinding

De volgende sectie behandelt diverse gevallenstudies die sommige manieren aantonen een verbinding door een cluster kan worden gevestigd. De doelstellingen zijn:

- Maak je vertrouwd met de verschillende eenheidsrollen.

- Toon aan hoe de verschillende opdrachtoutput gecorreleerd kan worden.

Topologie



Clustereenheden en ID's:

Eenheid-1-1	Eenheid-2-1
<#root> Cluster GROUP1: On Interface mode: spanned **This is "unit-1-1" in state PRIMARY** **ID : 0** Site ID : 1 Version : 9.15(1) Serial No.: FCH22247LNK CCL IP : 10.17.1.1	<#root> **Unit "unit-2-1" in state SECO** **ID : 1** Site ID : 1 Version : 9.15(1) Serial No.: FCH23157Y9N CCL IP : 10.17.2.1 CCL MAC : 0015.c500.02 Last join : 02:04:19 UTC Last leave: N/A

```
        CCL MAC   : 0015.c500.018f
        Last join : 02:24:43 UTC Nov 27 2020
        Last leave: N/A
```

Cluster neemt het volgende op:

```
cluster exec cap CAPI int INSIDE buffer 33554432 match tcp host 192.168.240.50 host 192.168.241.50 eq 8
cluster exec cap CAPO int OUTSIDE buffer 33554432 match tcp host 192.168.240.50 host 192.168.241.50 eq
cluster exec cap CAPI_RH reinject-hide int INSIDE buffer 33554432 match tcp host 192.168.240.50 host 19
cluster exec cap CAPO_RH reinject-hide int OUTSIDE buffer 33554432 match tcp host 192.168.240.50 host 1
cluster exec cap CCL int cluster buffer 33554432
```

Opmerking: Deze tests werden uitgevoerd in een laboratoriumomgeving met minimaal verkeer door het cluster. Probeer in productie zo specifiek mogelijke opnamefilters te gebruiken (bijvoorbeeld de bestemmingshaven en indien mogelijk de bronpoort) om het "ruis" in de opnamen te minimaliseren.

Case Study 1. Symmetric Traffic (eigenaar is ook de directeur)

Waarneming 1. De renjecthuid vangt uitsluitend op eenheid-1-1 pakketten op. Dit betekent dat de stroom in beide richtingen door eenheid-1-1 ging (symmetrisch verkeer):

<#root>

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
```

Waarneming 2. Aansluitvlaganalyse voor stroom met bronpoort 45954

```
<#root>

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

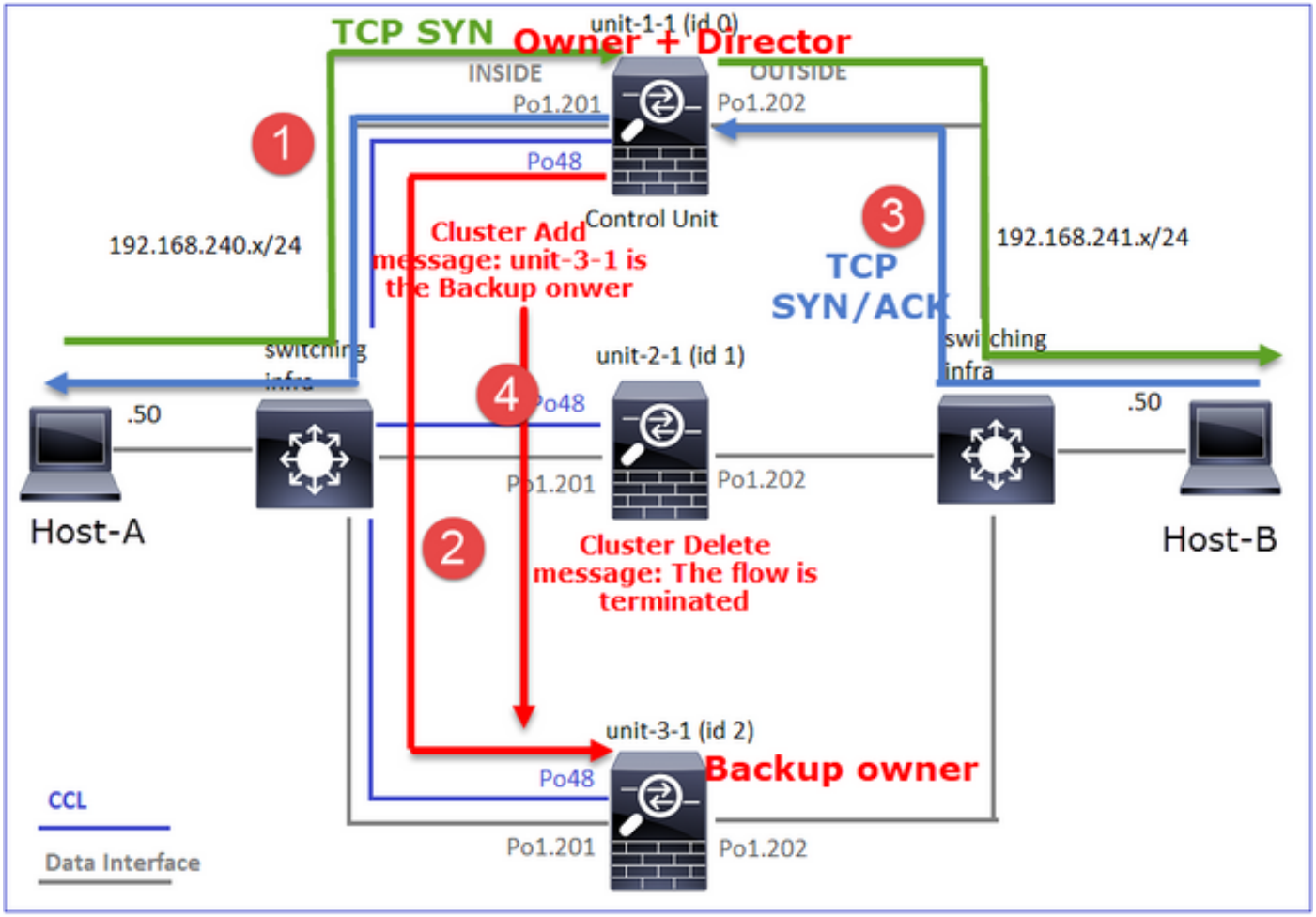
```
, idle 0:00:06, bytes 0,
```

flags y

Eenheid	Vlag	Opmerking
Eenheid-1-1	UIO	· Flow Owner - het apparaat verwerkt de stroom · Directeur - Aangezien eenheid-3-1 "y" heeft en niet "Y", betekent dit dat eenheid-1-1 werd gekozen als de directeur voor deze stroom.

		Omdat het ook de eigenaar is, werd een andere eenheid (in dit geval eenheid 3-1) gekozen als de back-up-eigenaar
Eenheid-2-1	-	-
Eenheid-3-1	y	De eenheid is een backup-eigenaar

Dit kan als volgt worden weergegeven:



1. TCP-SYN-pakket wordt geleverd van host-A naar unit-1-1. Unit-1-1 wordt de flow-eigenaar.
2. Unit-1-1 wordt ook gekozen als flow director. Daarom kiest het ook unit-3-1 als back-up eigenaar (cluster add bericht).
3. TCP/SYN/ACK-pakket komt van host-B aan op unit-3-1. De stroom is symmetrisch.
4. Zodra de verbinding is beëindigd, stuurt de eigenaar een clusterverwijderingsbericht om de stroominformatie van de back-upeigenaar te verwijderen.

Observatie 3. Capture with trace laat zien dat beide richtingen alleen door eenheid-1-1 gaan.

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

<#root>

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)
2: 08:42:09.363521 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.45954: S 4042762409:4042762409
3: 08:42:09.363827 802.1Q vlan#201 P0 192.168.240.50.45954 > 192.168.241.50.80: . ack 4042762410 win 22
…
unit-2-1:*******************************************************************

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

<#root>

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
2: 08:42:09.363415 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45954: S 3603655982:3603655982
3: 08:42:09.363903 802.1Q vlan#202 P0 192.168.240.50.45954 > 192.168.241.50.80: . ack 3603655983 win 22
…
unit-2-1:*******************************************************************

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

Stap 2. Aangezien dit een TCP flow-spoor is, worden de 3-weg handshake-pakketten overgetrokken. Zoals je kan zien in deze output, is unit-1-1 de eigenaar. Voor de eenvoud worden de niet-relevante spoorfasen weggelaten:

<#root>

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):

<#root>

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. FTD-dataplatformsystemen tonen het tot stand brengen en beëindigen van de verbinding op alle eenheden:

<#root>

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 FIN

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 Cluste

Case Study 2. symmetrisch verkeer (eigenaar anders dan de regisseur)

- Hetzelfde als het geval studie #1, maar in dit geval studie, een flow-eigenaar is een andere eenheid dan de director.

- Alle uitkomsten zijn vergelijkbaar met de #1 van casestudy's. Het belangrijkste verschil met casestudy's #1 is de Y-vlag die de y-vlag van scenario 1 vervangt.

Waarneming 1. De eigenaar is anders dan de directeur.

Aansluitingsvlaganalyse voor stroom met bronpoort 46278.

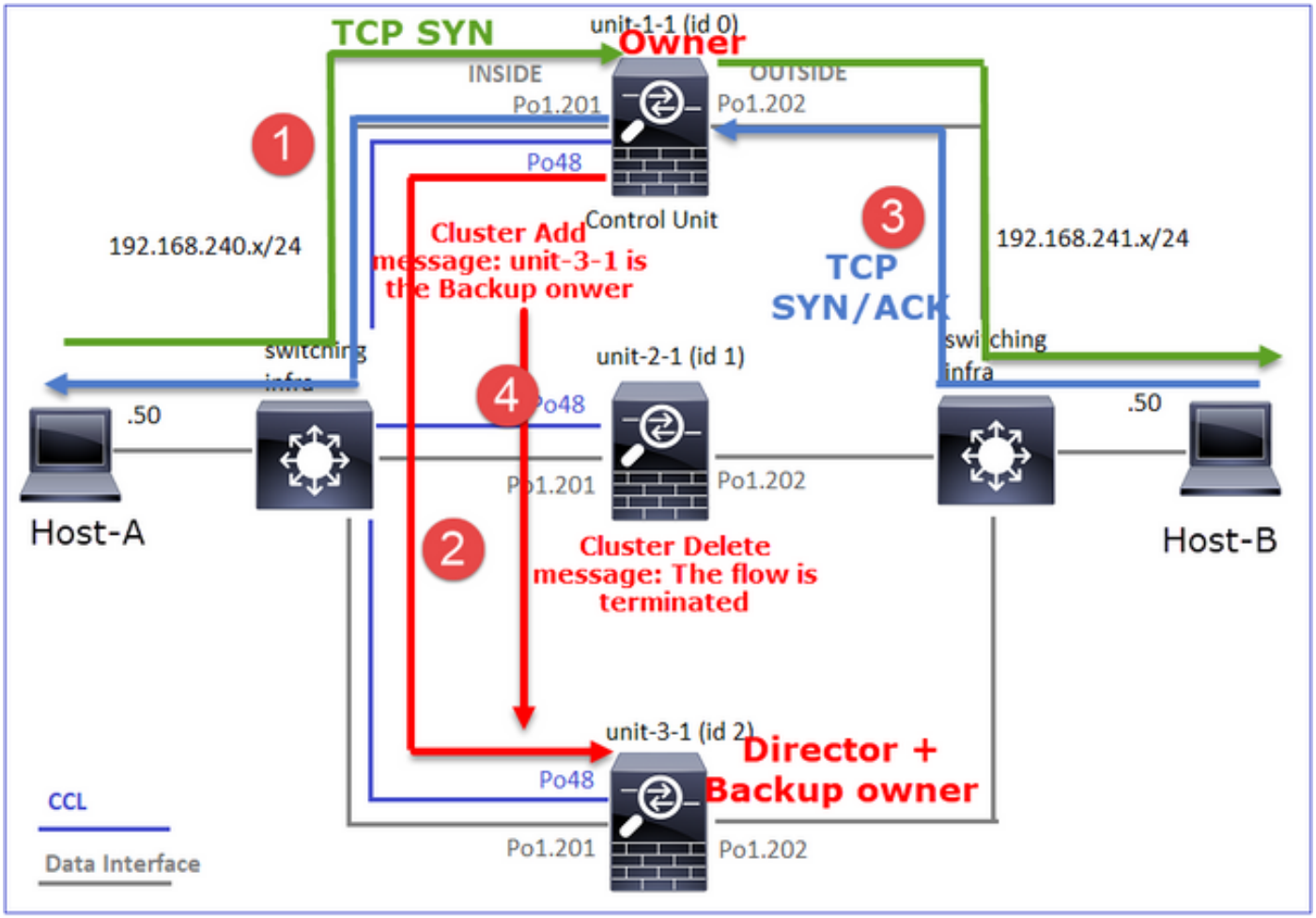
<#root>

```
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 - het apparaat verwerkt de stroom
Eenheid-2-1	-	-
Eenheid-3-1	Y	· Directeur en back-upeigenaar - Eenheid 3-1 heeft de vlag Y (Director).

Dit kan als volgt worden weergegeven:



1. TCP-SYN-pakket wordt geleverd van host-A naar unit-1-1. Unit-1-1 wordt de flow-eigenaar.
2. Unit-3-1 wordt gekozen als flow director. Unit-3-1 is ook de back-upeigenaar (clusteradd-bericht op UDP 4193 via de CCL).
3. TCP/SYN/ACK-pakket komt van host-B aan op unit-3-1. De stroom is symmetrisch.
4. Zodra de verbinding is beëindigd, stuurt de eigenaar via de CCL een 'cluster delete' bericht

op UDP 4193 om de stroominformatie van de back-upeigenaar te verwijderen.

Observatie 2. Capture with trace laat zien dat beide richtingen alleen door eenheid 1-1 gaan

Stap 1. Gebruik dezelfde aanpak als in casestudy 1 om de relevante stroom en pakketten in alle clustereenheden op basis van de bronpoort te identificeren:

```
<#root>

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 22
…
unit-2-1:*************************************************************

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

Leg het volgende vast op de BUITENinterface:

```
<#root>


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 22

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

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

Stap 2. Focus op de ingangspakketten (TCP SYN en TCP SYN/ACK):

<#root>

```
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:

<#root>

```
firepower#
```

cluster exec show cap CAPO packet-number 4 trace

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

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

Found flow with id 9583, using existing flow

Waarneming 3. FTD dataplatformsyslogs tonen het tot stand brengen en beëindigen van de verbinding op eigenaar en backup-eigenaar:

<#root>

```
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.
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 TC

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 Cluste

Case Study 3. Asymmetrisch verkeer (Director forwards the traffic).

Observatie 1. De renjecthuid vangt pakketten op eenheid 1-1 en eenheid 2-1 (asymmetrische stroom) op:

<#root>

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
```

Waarneming 2. Aansluitvlaganalyse voor stroom met bronpoort 46502.

<#root>

```
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,

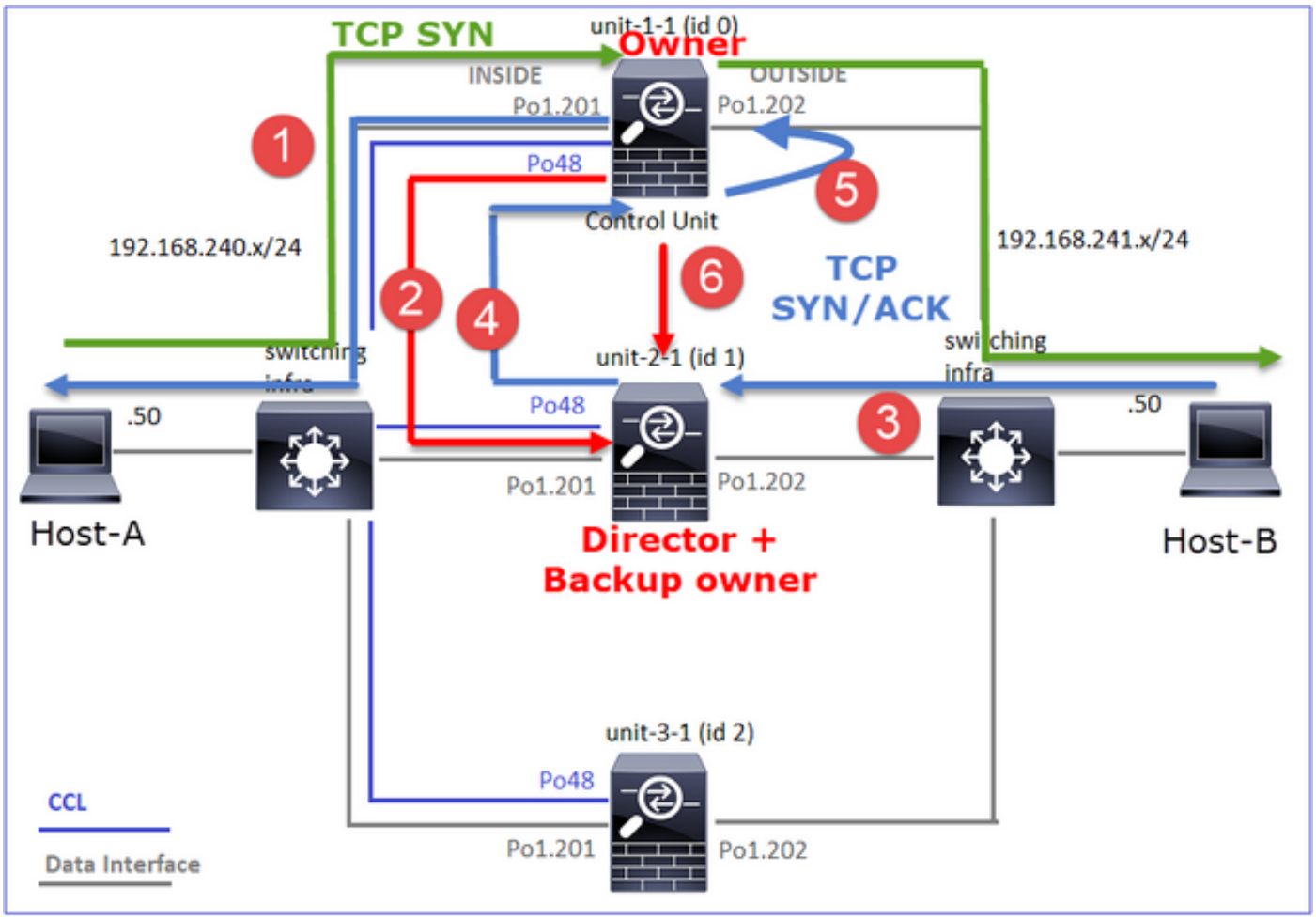
flags Y

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	· Flow Owner - het apparaat verwerkt de stroom.
Eenheid-2-1	Y	· Directeur - Aangezien eenheid-2-1 de vlag "Y" heeft, betekent dit dat eenheid-2-1 werd gekozen als de directeur voor deze stroom. · Reserve-eigenaar · Tot slot, hoewel het niet duidelijk is uit deze output, van de show opname en toon logoutput is het duidelijk dat eenheid-2-1 deze stroom naar de eigenaar doorstuurt (hoewel het technisch niet wordt beschouwd als een doorvoerder in dit scenario).

		Opmerking: Een eenheid kan niet zowel regisseur (Y flow) als doorvoerder (z flow) zijn, deze 2 rollen sluiten elkaar wederzijds uit. Directors (Y-stroom) kunnen nog steeds verkeer doorsturen. Zie de output van het showlogboek later in deze casestudy.
Eenheid-3-1	-	-

Dit kan als volgt worden weergegeven:



1. TCP-SYN-pakket wordt geleverd van host-A naar unit-1-1. Unit-1-1 wordt de flow-eigenaar.
2. Eenheid-2-1 wordt gekozen als flow director en backup-eigenaar. De flow-eigenaar stuurt een 'cluster add'-unicastbericht op UDP 4193 om de back-up-eigenaar over de stroom te informeren.
3. TCP/SYN/ACK-pakket komt van host-B aan op unit-2-1. De stroom is asymmetrisch.
4. Unit-2-1 stuurt het pakket door de CCL naar de eigenaar (vanwege TCP SYN Cookie).
5. De eigenaar injecteert het pakket op de interface BUITEN en door:sturen dan het pakket naar host-A.
6. Zodra de verbinding is beëindigd, stuurt de eigenaar een clusterverwijderingsbericht om de stroominformatie van de back-upeigenaar te verwijderen.

Observatie 3. Capture with trace toont het asymmetrische verkeer en de omleiding van eenheid-2-

1 naar eenheid-1-1.

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

<#root>

```
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
4: 12:58:33.357037 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.46502: S 883000451:883000451(0)
5: 12:58:33.357357 802.1Q vlan#201 P0 192.168.240.50.46502 > 192.168.241.50.80: . ack 883000452 win 229
unit-2-1:*************************************************************

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

De retourrichting:

<#root>

```
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
4: 12:58:33.356915 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: S 4257314722:4257314722
5: 12:58:33.357403 802.1Q vlan#202 P0 192.168.240.50.46502 > 192.168.241.50.80: . ack 4257314723 win 22

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
2: 12:58:33.360302 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: . ack 1434968736 win 23
3: 12:58:33.361004 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: . 4257314723:4257316091
…

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

Stap 2. Traceer de pakketten. Standaard worden alleen de eerste 50 ingangspakketten overgetrokken. Voor de eenvoud worden de niet-relevante spoorfasen weggelaten.

Eenheid-1-1 (eigenaar):

<#root>

```
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 (expeditor)

Het retourverkeer (TCP/SYN/ACK). De eenheid van belang is eenheid-2-1 die de directeur/back-up-eigenaar is en het verkeer doorstuurt naar de eigenaar:

<#root>

```
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,no
...
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. FTD-dataplatformsystemen tonen het tot stand brengen en beëindigen van de verbinding op alle eenheden:

<#root>

```
firepower#
```

cluster exec show log | i 46502

```
unit-1-1(LOCAL):*******************************************************
Dec 01 2020 12:58:33: %FTD-6-302013:
```

B

uilt 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.
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 TC

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 (192.168.240.50/4650
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 Forwa
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 20483163

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

Case Study 4. Asymmetrisch verkeer (eigenaar is de directeur)

Observatie 1. De renjecthuid vangt pakketten op eenheid 1-1 en eenheid 2-1 (asymmetrische stroom) op:

<#root>

```
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

Waarneming 2. Aansluitvlaganalyse voor stroom met bronpoort 46916.

<#root>

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:
```

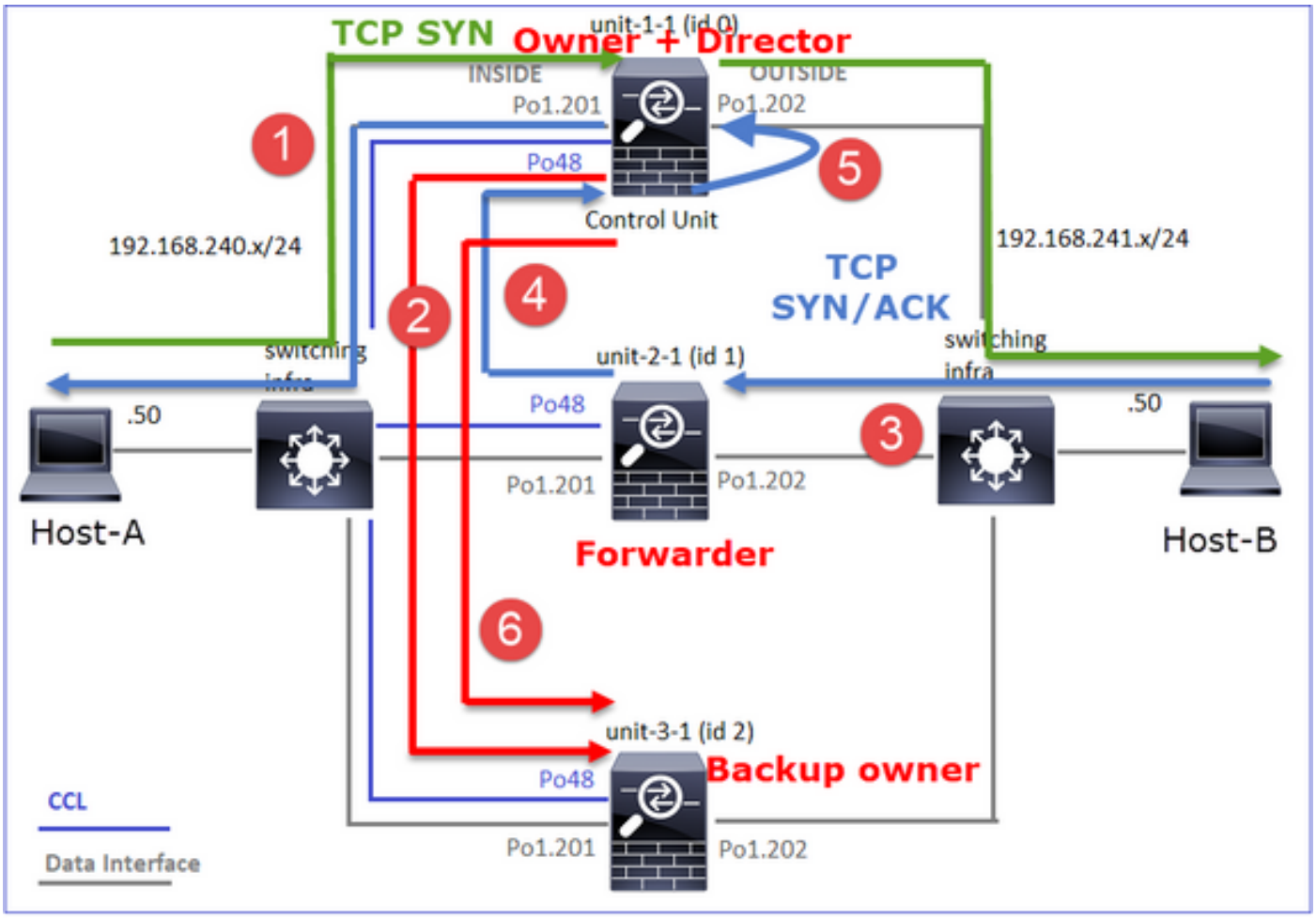
46916

```
, idle 0:00:04, bytes 0,
```

flags y

Eenheid	Vlag	Opmerking
Eenheid-1-1	UIO	· Flow Owner - het apparaat verwerkt de stroom · Directeur - Aangezien eenheid-3-1 "y" heeft en niet "Y", betekent dit dat eenheid-1-1 werd gekozen als de directeur voor deze stroom. Omdat het ook de eigenaar is, werd een andere eenheid (in dit geval eenheid 3-1) gekozen als de back-up-eigenaar
Eenheid-2-1	z	· Forwarder
Eenheid-3-1	y	- Reserve-eigenaar

Dit kan als volgt worden weergegeven:



1. TCP/SYN-pakket komt van host-A aan op unit-1-1. Unit-1-1 wordt de flow-eigenaar en wordt gekozen als Director.
2. Eenheid-3-1 wordt gekozen als back-upeigenaar. De flow-eigenaar stuurt een unicast 'cluster add' bericht op UDP 4193 om de back-up-eigenaar te informeren over de flow.
3. TCP/SYN/ACK-pakket komt van host-B aan op unit-2-1. De stroom is asymmetrisch.
4. Unit-2-1 stuurt het pakket door de CCL naar de eigenaar (vanwege TCP SYN Cookie).
5. De eigenaar injecteert het pakket op de interface BUITEN en door:sturen dan het pakket naar host-A.
6. Zodra de verbinding is beëindigd, stuurt de eigenaar een clusterverwijderingsbericht om de stroominformatie van de back-upeigenaar te verwijderen.

Observatie 3. Capture with trace toont het asymmetrische verkeer en de omleiding van eenheid-2-1 naar eenheid-1-1.

Eenheid-2-1 (expeditor)

```
<#root>

firepower#

cluster exec unit unit-2-1 show capture CAPO packet-number 1 trace

1: 16:11:33.653164 802.1Q vlan#202 P0 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. FTD-dataplatformsystemen tonen het tot stand brengen en beëindigen van de verbinding op alle eenheden:

- Eenheid-1-1 (eigenaar)
- Eenheid-2-1 (expeditor)
- Eenheid-3-1 (back-up-eigenaar)

<#root>

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
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 T

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 (192.168.240.50/4691
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 1024009

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 Cluste
```

Case Study 5. Asymmetrisch verkeer (eigenaar is anders dan de regisseur).

Observatie 1. De renjecthuid vangt pakketten op eenheid 1-1 en eenheid 2-1 (asymmetrische stroom) op:

<#root>

```
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-hid

e 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. Aansluitvlaganalyse voor stroom met bronpoort 46994:

```
<#root>

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

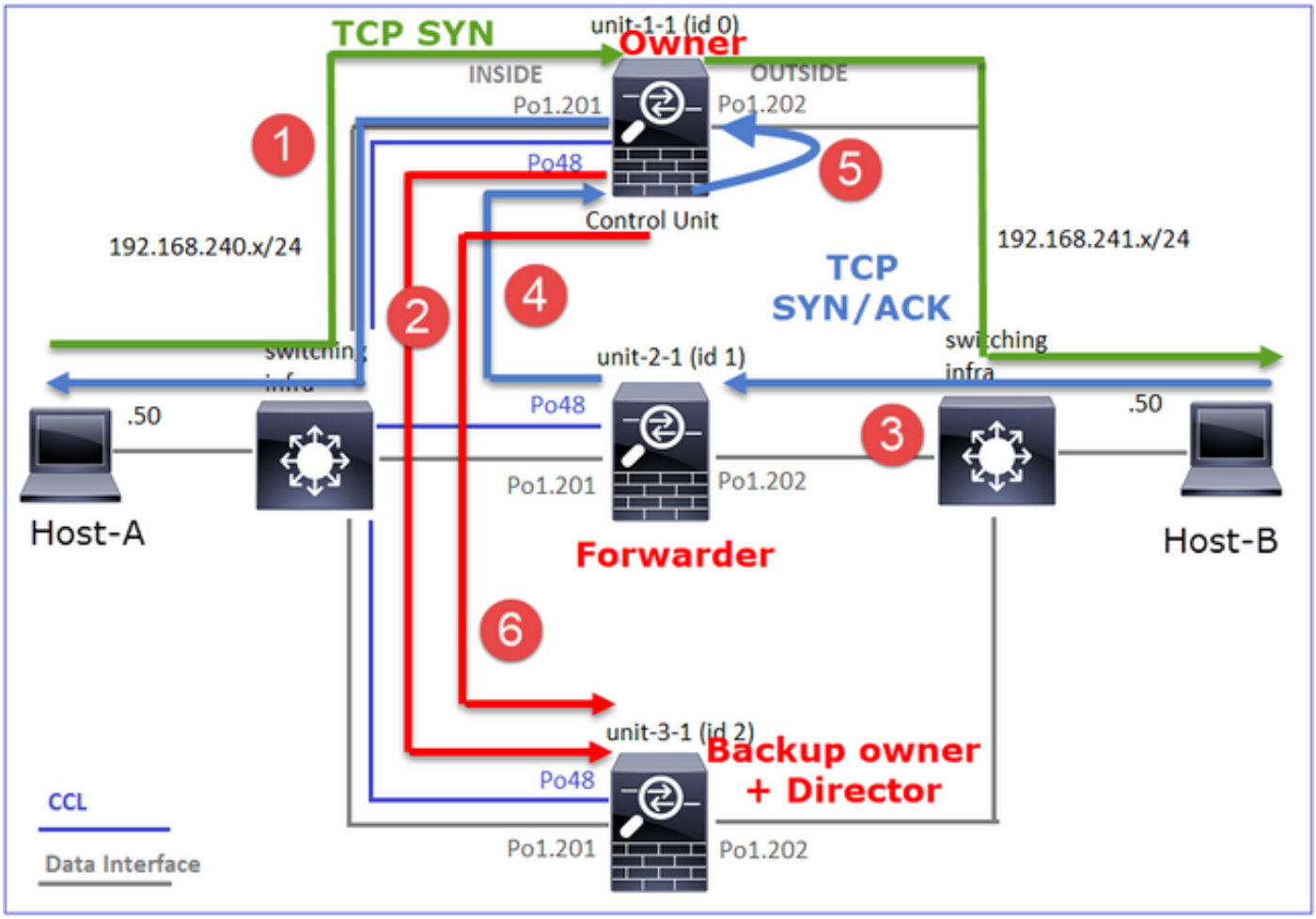
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

46994

```
, idle 0:00:05, bytes 0,
flags Y
```

Eenheid	Vlag	Opmerking
Eenheid-1-1	UIO	· Flow Owner - het apparaat verwerkt de stroom
Eenheid-2-1	z	· Forwarder
Eenheid-3-1	Y	· Reserve-eigenaar Director

Dit kan als volgt worden weergegeven:



1. TCP-SYN-pakket wordt geleverd van host-A naar unit-1-1. Unit-1-1 wordt de flow-eigenaar.
2. Unit-3-1 wordt gekozen als regisseur en backup-eigenaar. De flow-eigenaar stuurt een 'cluster add'-unicastbericht op UDP 4193 om de back-up-eigenaar over de stroom te

informeren.
3. TCP/SYN/ACK-pakket wordt geleverd van host-B naar unit-2-1. De stroom is asymmetrisch
4. Unit-2-1 stuurt het pakket door de CCL naar de eigenaar (vanwege TCP SYN Cookie).
5. De eigenaar injecteert het pakket op de interface BUITEN en door:sturen dan het pakket naar host-A.
6. Zodra de verbinding is beëindigd, stuurt de eigenaar een clusterverwijderingsbericht om de stroominformatie van de back-upeigenaar te verwijderen.

Observatie 3. Capture with trace toont het asymmetrische verkeer en de omleiding van eenheid-2-1 naar eenheid-1-1.

Eenheid-1-1 (eigenaar)

<#root>

```
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 (expeditor)

<#root>

```
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,no
…
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. FTD-dataplatformsystemen tonen het tot stand brengen en beëindigen van de verbinding op alle eenheden:

- Eenheid-1-1 (eigenaar)
- Eenheid-2-1 (expeditor)
- Eenheid-3-1 (back-upeigenaar/directeur)

<#root>

```
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
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 T

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 (192.168.240.50/4699
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 1024000

unit-3-1:************************************************************
Dec 01 2020 16:46:44: %FTD-6-302022:
```

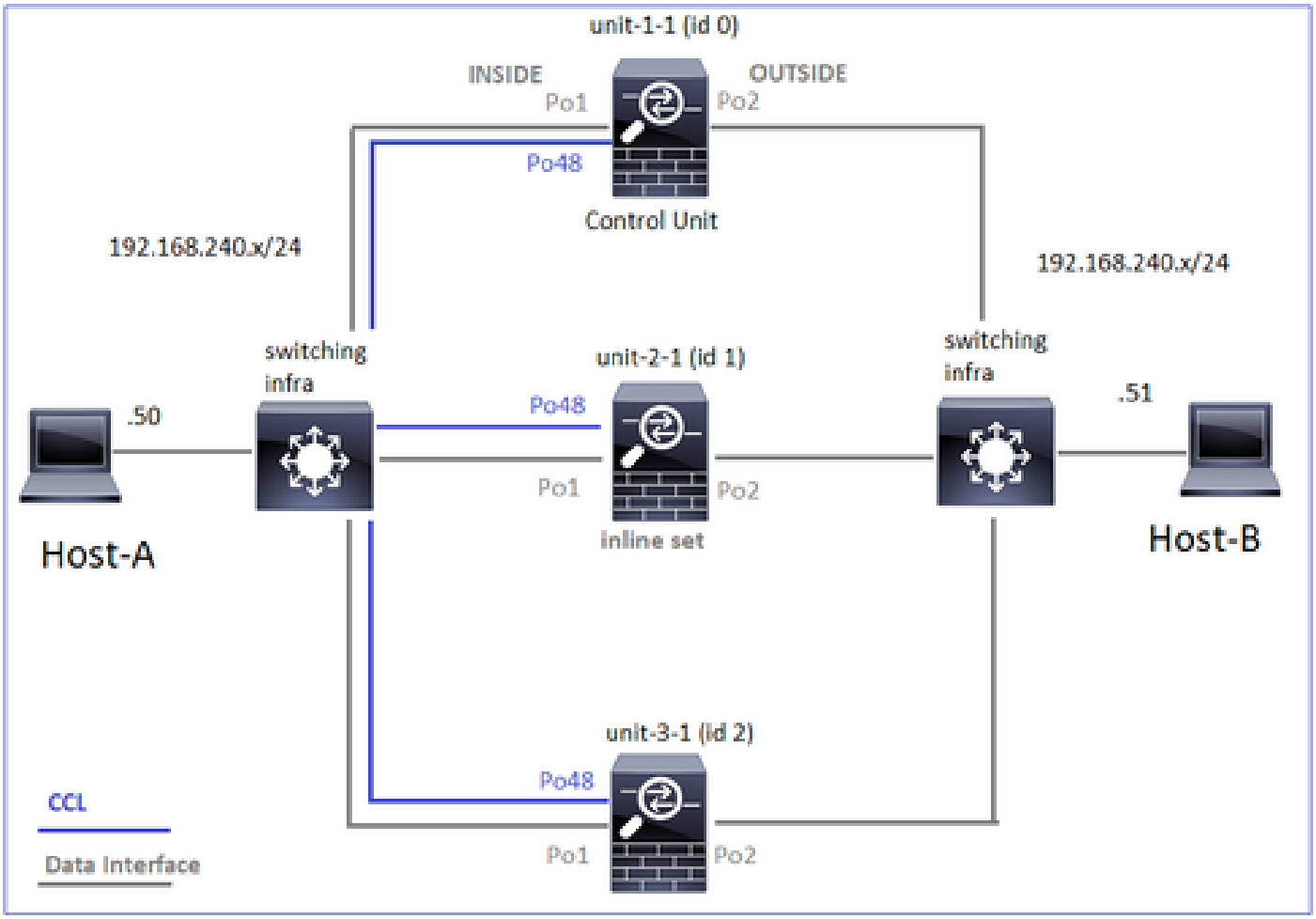
Built director stub TCP connection

```
 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 Cluste
```

Voor de volgende casestudy's is de gebruikte topologie gebaseerd op een cluster met inline sets:



Case Study 6. Asymmetrisch verkeer (Inline-set, de eigenaar is de regisseur)

Waarneming 1. De renjecthuid vangt pakketten op eenheid-1-1 en eenheid-2-1 (asymmetrische stroom) op. Bovendien is de eigenaar unit-2-1 (er zitten pakketten op zowel binnen- als buitenkant

interfaces voor de opnamen van de herinjectiescherm, terwijl unit-1-1 alleen op buitenkant staat):

<#root>

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

Waarneming 2. Aansluitvlaganalyse voor stroom met bronpoort 51844.

<#root>

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

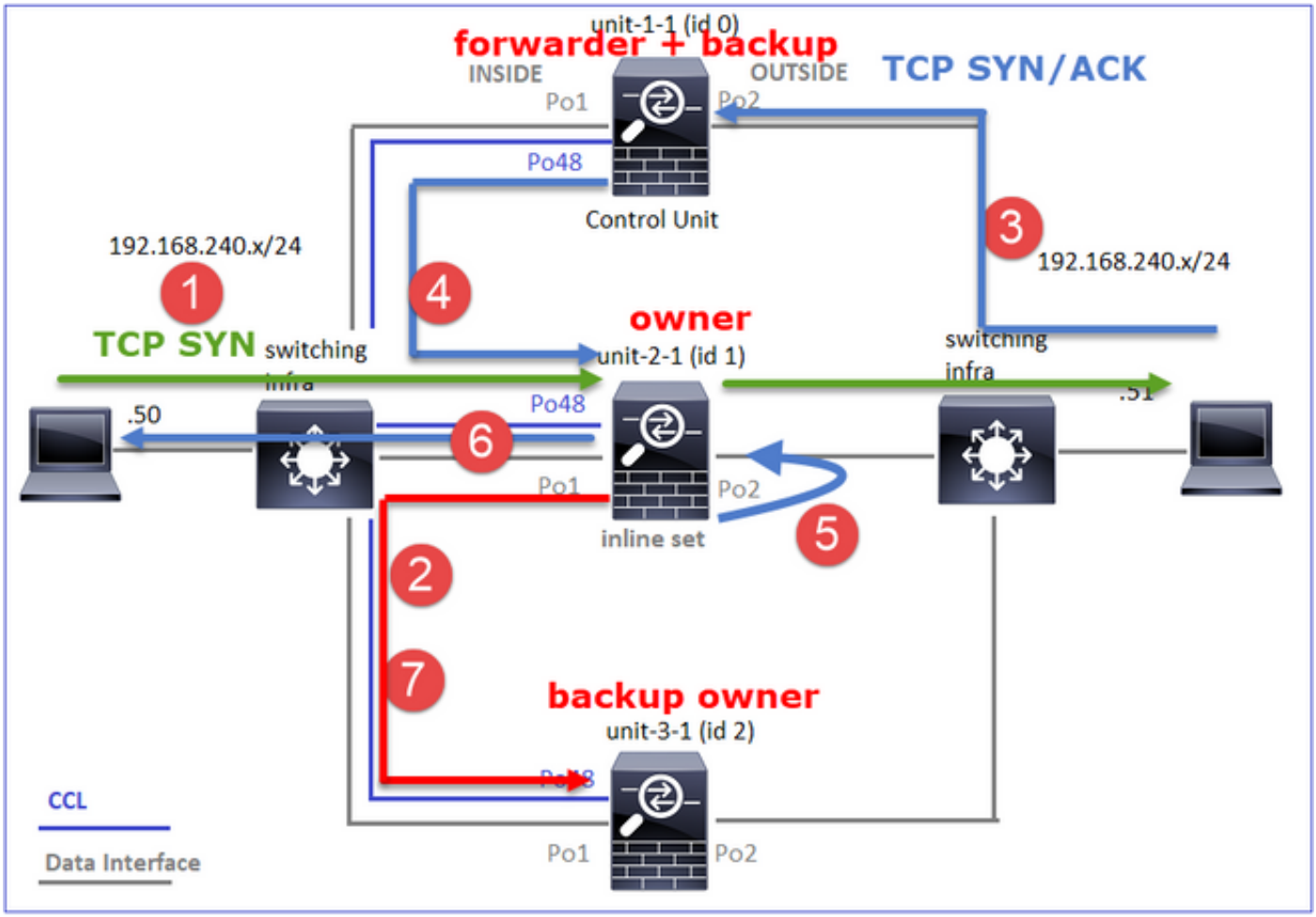
unit-3-1

```
:************************************************************
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	· Forwarder
Eenheid-2-1	b N	· Flow Owner - het apparaat verwerkt de stroom
Eenheid-3-1	y	· Reserve-eigenaar

Dit kan als volgt worden weergegeven:



1. TCP/SYN-pakket komt van host-A aan op unit-2-1. Unit-2-1 wordt de flow-eigenaar en wordt gekozen als de Director.
2. Eenheid-3-1 wordt gekozen als de back-upeigenaar. De flow-eigenaar stuurt een 'cluster add'-unicastbericht op UDP 4193 om de back-up-eigenaar over de stroom te informeren.
3. TCP/SYN/ACK-pakket komt van host-B aan op unit-1-1. De stroom is asymmetrisch.
4. Unit-1-1 stuurt het pakket door de CLS naar de Director (unit-2-1).
5. Unit-2-1 is ook de eigenaar en injecteert het pakket op de interface BUITEN.
6. Unit-2-1 stuurt het pakket door naar host-A.
7. Zodra de verbinding is beëindigd, stuurt de eigenaar een clusterverwijderingsbericht om de stroominformatie van de back-upeigenaar te verwijderen.

Observatie 3. Capture with trace toont het asymmetrische verkeer en de omleiding van eenheid 1-1 naar eenheid 2-1.

Eenheid-2-1 (eigenaar/directeur)

<#root>

```
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 (expeditor)

<#root>

```
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 w
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)

<#root>

```
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 w
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. FTD-dataplatformsystemen tonen het tot stand brengen en beëindigen van de verbinding op alle eenheden:

- Eenheid-1-1 (eigenaar)
- Eenheid-2-1 (expeditor)
- Eenheid-3-1 (back-upeigenaar/directeur)

<#root>

```
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 (192.168.240.50/5184
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 1024001

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
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 T

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 Cluste

Case Study 7. Asymmetrisch verkeer (Inline-set, de eigenaar is anders dan de regisseur)

De eigenaar is unit-2-1 (er zijn pakketten op zowel binnen- als buitenkant interfaces voor de herinjecteren-huid opnamen, terwijl unit-3-1 alleen op buitenkant heeft):

<#root>

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-hid

e

 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

Waarneming 2. Aansluitvlaganalyse voor stroom met bronpoort 59210.

<#root>

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:

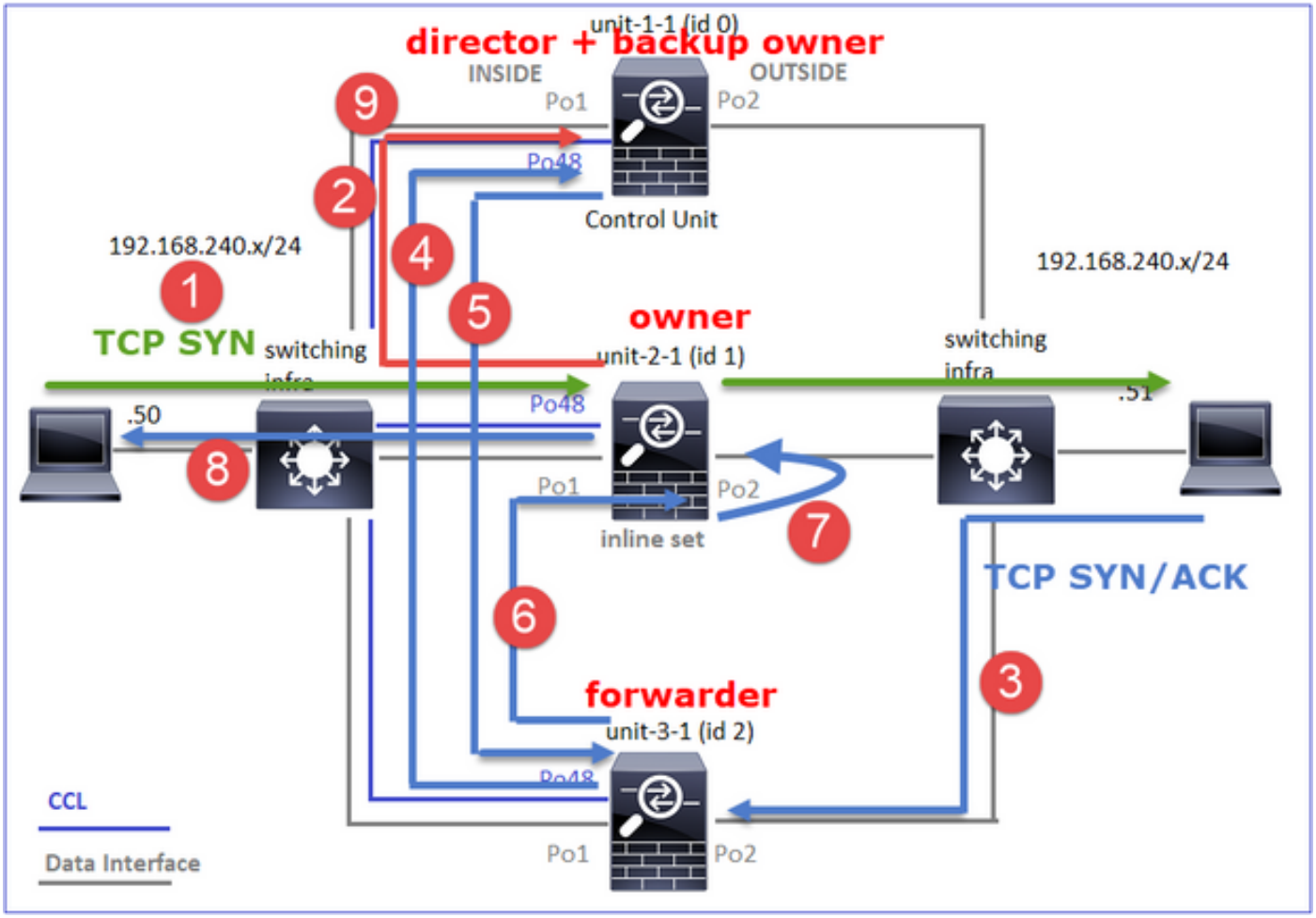
59210

, 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 - het apparaat verwerkt de stroom
Eenheid-3-1	z	· Forwarder

Dit kan als volgt worden weergegeven:



1. TCP-SYN-pakket wordt geleverd van host-A naar unit-2-1. Unit-2-1 wordt de flow-eigenaar en unit-1-1 wordt gekozen als de Director
2. Eenheid-1-1 wordt gekozen als de backup-eigenaar (omdat het de Director is). De flow-eigenaar stuurt een 'cluster add'-unicastbericht op UDP 4193 naar. de back-upeigenaar op de hoogte stellen van de stroom.
3. TCP/SYN/ACK-pakket komt aan van host-B op unit-3-1. De stroom is asymmetrisch.
4. Unit-3-1 stuurt het pakket door de CLS naar de Director (unit-1-1).
5. Unit-1-1 (Director) weet dat de eigenaar unit-2-1 is, stuurt het pakket terug naar de expediteur (unit-3-1) en deelt hem mee dat de eigenaar unit-2-1 is.

6. Unit-3-1 verstuurt het pakket naar unit-2-1 (eigenaar).
7. Eenheid-2-1 injecteert het pakket op de interface BUITEN.
8. Unit-2-1 stuurt het pakket door naar host-A.
9. Zodra de verbinding is beëindigd, stuurt de eigenaar een clusterverwijderingsbericht om de stroominformatie van de back-upeigenaar te verwijderen.

Opmerking: Het is belangrijk dat stap 2 (pakket door de CCL) wordt uitgevoerd vóór stap 4 (gegevensverkeer). In een ander geval (bijvoorbeeld, ras conditie), is de regisseur niet op de hoogte van de stroom. Aldus, aangezien het een gealigneerde reeks is, door:sturen het pakket naar de bestemming. Als de interfaces niet in een inline set staan, wordt het gegevenspakket verbroken.

Observatie 3. Capture with trace toont het asymmetrische verkeer en de uitwisseling via de CCL:

Doorsturen van verkeer (TCP/SYN)

Eenheid-2-1 (eigenaar)

<#root>

```
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
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)

Unit-3-1 (ID 2 - Forwarder) verstuurt het pakket via de CCL naar unit-1-1 (ID 0 - Director).

<#root>

```
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 (Director) - Unit-1-1 (ID 0) weet dat de flow-eigenaar unit-2-1 (ID 1) is en stuurt het pakket via de CCL terug naar unit-3-1 (ID 2 - forward).

<#root>

```
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 - Forwarder) krijgt het pakket door de CCL en verstuurt het naar unit-2-1 (ID 1 - eigenaar).

<#root>

```
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,w
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 injecteert en stuurt het pakket naar de bestemming:

<#root>

```
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. FTD-dataplatformsystemen tonen het tot stand brengen en beëindigen van de verbinding op alle eenheden:

- Unit-1-1 (Director/backup-eigenaar)
- Eenheid-2-1 (eigenaar)
- Eenheid-3-1 (expeditor)

<#root>

```
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 Cluste

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
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 T

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 (192.168.240.50/5921
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 1024003
```

Problemen oplossen

Inleiding Cluster Probleemoplossing

De clusterproblemen kunnen worden gecategoriseerd in:

- Problemen met besturingsplane (kwesties die verband houden met de clusterstabiliteit)
- Problemen met het gegevensplane (kwesties in verband met het transitoverkeer)

Problemen met Cluster-dataplane

NAT/PAT gemeenschappelijke problemen

Belangrijke configuratieoverwegingen

- PAT-pools (Port Address Translation) moeten ten minste evenveel IP's beschikbaar hebben als het aantal eenheden in het cluster, bij voorkeur meer IP's dan clusterknooppunten.
- De standaard opdrachten per sessie moeten op hun plaats blijven, tenzij er een specifieke reden is om ze uit te schakelen. Elke PAT-xlate die is gebouwd voor een verbinding die per sessie is uitgeschakeld, wordt altijd verwerkt door de eenheid van de controleknooppunt in het cluster, wat prestatievermindering kan veroorzaken.

Gebruik van het bereik van de hoge PAT-pool vanwege verkeer afkomstig van lage poorten dat de onbalans van het cluster veroorzaakt

De FTD verdeelt een PAT IP in reeksen en probeert de xlate in hetzelfde bronbereik te houden. 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 vol is en er een nieuwe PAT-xlate uit dat bereik moet worden toegewezen, gaat FTD naar het volgende IP om nieuwe vertalingen toe te wijzen voor dat bronpoortbereik.

Symptomen

Connectiviteitsproblemen voor NATed-verkeer dat het cluster passeert

Verificatie

<#root>

#

show nat pool

Logboeken van het FTD-dataplatform tonen de uitputting van de PAT-pool:

<#root>

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 NAT vlak poortbereik en neem reservepoorten op.

Bovendien, in post-6.7/9.15.1 kunt u met ongebalanceerde havenblokdistributie slechts eindigen wanneer de knooppunten verlaten/zich bij de cluster met groot achtergrondverkeer aansluiten dat aan PAT onderworpen is. De enige manier waarop het zich herstelt, is wanneer havenblokken worden vrijgemaakt om opnieuw over knooppunten te worden verdeeld.

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

Als een host bijvoorbeeld 512 verbindingen maakt, wijst de unit toegewezen poorten toe voor al die 512 verbindingen van pb-1 willekeurig. Nu, met al deze 512 verbindingen actief, wanneer de gastheer de 513ste verbinding aangezien pb-1 wordt uitgeput vestigt, beweegt het zich aan pb-2 en wijst een willekeurige haven van het toe. Nogmaals, van de 513 verbindingen gaat men ervan uit dat de 10e verbinding voltooid is en een poort vrij is in pb-1. Op dit punt, als de host de 514e verbinding tot stand brengt, wijst de cluster unit een in kaart gebrachte poort toe aan pb-1 en niet aan pb-2, omdat pb-1 nu een vrije poort heeft (die werd vrijgegeven als onderdeel van de 10e verbindingsverwijdering).

Het belangrijkste is dat de toewijzing gebeurt vanaf het eerste beschikbare havenblok met vrije havens, zodat de laatste havenblokken altijd beschikbaar zijn voor herverdeling in een normaal geladen systeem. Bovendien wordt PAT meestal gebruikt voor kortstondige verbindingen. De kans dat een havenblok in een kortere tijd beschikbaar komt, is zeer groot. Zo kan de tijd die nodig is om de verdeling van het zwembad in evenwicht te brengen, verbeteren met poortblok-gebaseerde verdeling van het zwembad.

Indien echter alle havenblokken, van pb-1 tot pb-10, uitgeput zijn of elk havenblok een haven voor een langdurige verbinding houdt, worden de havenblokken nooit snel vrijgemaakt en worden opnieuw verdeeld. In een dergelijk geval is de minst verstorende aanpak:

1. Identificeer knooppunten met excessieve poortblokken (toon NAT pool cluster samenvatting).
2. Identificeer de minst gebruikte poortblokken op dat knooppunt (toon NAT-poolip <addr>-details).
3. Duidelijke verklaringen voor dergelijke poortblokken (duidelijk xlate global <addr> gport 'start-end') om ze beschikbaar te maken voor herdistributie.

⚠ Waarschuwing: Dit verstoort de relevante verbindingen.

Kan niet bladeren naar tweekanaals websites (zoals webmail, bankieren, etc), of naar SSO-websites wanneer omleiding naar een andere bestemming gebeurt.

Symptomen

Kan niet bladeren naar tweekanaals websites (zoals webmail, bankwebsites, enzovoort). Wanneer een gebruiker verbinding maakt met een website waarvoor de client een tweede aansluiting/verbinding moet openen en de tweede verbinding wordt gehakt op een ander clusterlid dan dat waar de eerste verbinding is gehakt, en het verkeer een IP PAT-pool gebruikt, wordt het verkeer door de server opnieuw ingesteld als het de verbinding ontvangt van een ander publiek IP-adres.

Verificatie

Neem dataplatformcluster op om te zien hoe de beïnvloede doorvoerstroom wordt afgehandeld. In dit geval komt een TCP reset van de doelwebsite.

Beperking (pre-6.7/9.15.1)

- Let op als er meerdere toepassingen voor meerdere sessies zijn die meerdere in kaart gebrachte IP-adressen gebruiken.
- Gebruik de opdracht show nat pool cluster om te controleren of de pool gelijkmatig is verdeeld.
- Gebruik de cluster exec show conn opdracht om te controleren of het verkeer goed is gebalanceerd met de lading.
- Gebruik de opdracht show nat 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 aansluitingen geen gebruik hebben gemaakt van de plakkerige IP.
- Voeg meer IP's toe aan de PAT-pool of verfijn het algoritme voor de taakverdeling op verbonden switches.

Informatie over het ether-kanaal taakverdelingsalgoritme:

- Voor non-FP9300 en indien verificatie via één server plaatsvindt: Pas het ether-kanaal taakverdelingsalgoritme aan op de aangrenzende switch van bron IP/poort en bestemming IP/poort naar bron IP en bestemming IP.
- Voor non-FP9300 en als verificatie via meerdere servers plaatsvindt: Pas het ether-kanaal lastverdelingsalgoritme op de aangrenzende switch van Bron IP/Port en Bestemming IP/Port aan BronIP aan.
- Voor FP9300: Op het FP9300 chassis is het load balancing algoritme vast als source-dest-poorts source-dest-ip source-dest-mac en kan niet worden gewijzigd. De tijdelijke oplossing is in dit geval FlexConfig te gebruiken om opdrachten per sessie toe te voegen om opdrachten aan de FTD-configuratie te ontkennen om verkeer af te dwingen voor bepaalde IP-adressen op de bestemming (voor problematische/incompatibele toepassingen) die alleen door de controleknooppunt in het intra-chassis cluster moeten worden verwerkt. De tijdelijke oplossing wordt geleverd met de volgende bijwerkingen:
    - Geen taakverdeling van het verkeer met verschillende vertalingen (alles gaat naar het controleknooppunt).
    - Potentieel voor explosiegroeven om uit te lopen (en ongunstig NAT vertaling voor ander verkeer op de controleknoop beïnvloeden).
    - Verminderde schaalbaarheid van het intra-chassis cluster.

Lage clusterprestaties als gevolg van al het verkeer dat naar het controleknooppunt wordt verzonden omdat er niet genoeg PAT IP's in de pools zijn.

Symptomen

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

Verificatie

Gebruik de opdracht show nat pool cluster om de toewijzingen voor elke eenheid te zien en te bevestigen dat zij allemaal ten minste één IP in de pool bezitten.

Beperken

Voor pre-6.7/9.15.1 zorg ervoor dat u een PAT-pool van grootte hebt die minstens gelijk is aan het aantal knooppunten in het cluster. In post-6.7/9.15.1 met PAT-pool, wijst u poortblokken toe van alle PAT-pool IP's. Als het PAT zwembad gebruik is echt hoog, wat leidt tot frequente uitputting van het zwembad moet u de PAT pool grootte (zie de FAQ sectie) te vergroten.

Lage prestaties als gevolg van al het verkeer dat naar het controleknooppunt wordt verzonden

omdat sjablonen niet per sessie zijn ingeschakeld.

Symptomen

Veel snelle UDP-back-upstromen worden verwerkt door de clustercontroleknooppunt, wat de prestaties kan beïnvloeden.

Achtergrond

Alleen verbindingen die gebruikmaken van variabelen die per sessie zijn ingeschakeld, kunnen worden verwerkt door een gegevensknooppunt dat PAT gebruikt. Gebruik het commando show run all xlate om de xlate per-sessie configuratie te zien.

Per sessie ingeschakeld betekent dat de xlate onmiddellijk wordt afgebroken als de bijbehorende verbinding wordt afgebroken. Dit helpt de verbinding per seconde te verbeteren wanneer de verbindingen worden blootgesteld aan PAT. Niet-per-sessie verkent nog eens 30 seconden live nadat de verbinding is verbroken, en als de verbindingssnelheid hoog genoeg is, kunnen de beschikbare 65k TCP/UDP-poorten op elk wereldwijd IP in een korte tijd worden opgebruikt.

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

Verificatie

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

```
<#root>

firepower#

show cluster info conn-distribution


firepower#

show cluster info packet-distribution


firepower#

show cluster info load-monitor
```

Gebruik de cluster exec show conn commando om te zien welke cluster knooppunten de UDP verbindingen bezitten.

```
<#root>

firepower#

cluster exec show conn
```

Gebruik deze opdracht om inzicht te krijgen in het gebruik van de pool bij clusterknooppunten.

<#root>

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

```
      | in UDP
```

Beperken

Configureer per sessie PAT (per sessie permissie udp-opdracht) voor het interessant verkeer (bijvoorbeeld UDP). Voor ICMP, kunt u niet van het standaard multi-sessie PAT veranderen, zodat wordt het verkeer ICMP altijd behandeld door de controleknoop wanneer er gevormd PAT is.

PAT-poortverdeling wordt onevenwichtig wanneer knooppunten het cluster verlaten of zich bij het cluster aansluiten.

Symptomen

- Connectiviteitsproblemen sinds PAT IP-toewijzing kunnen in de loop van de tijd onevenwichtig worden doordat eenheden het cluster verlaten en er zich bij aansluiten.
- In post-6.7/9.15.1 kunnen er gevallen zijn waarin het nieuw aangesloten knooppunt niet genoeg poortblokken kan krijgen. Een knooppunt zonder poortblok leidt verkeer om naar het controleknooppunt. Een knooppunt met ten minste één poortblok behandelt het verkeer en laat het vallen zodra het zwembad is uitgeput.

Verificatie

- De gegevensvlak syslogs tonen berichten zoals:

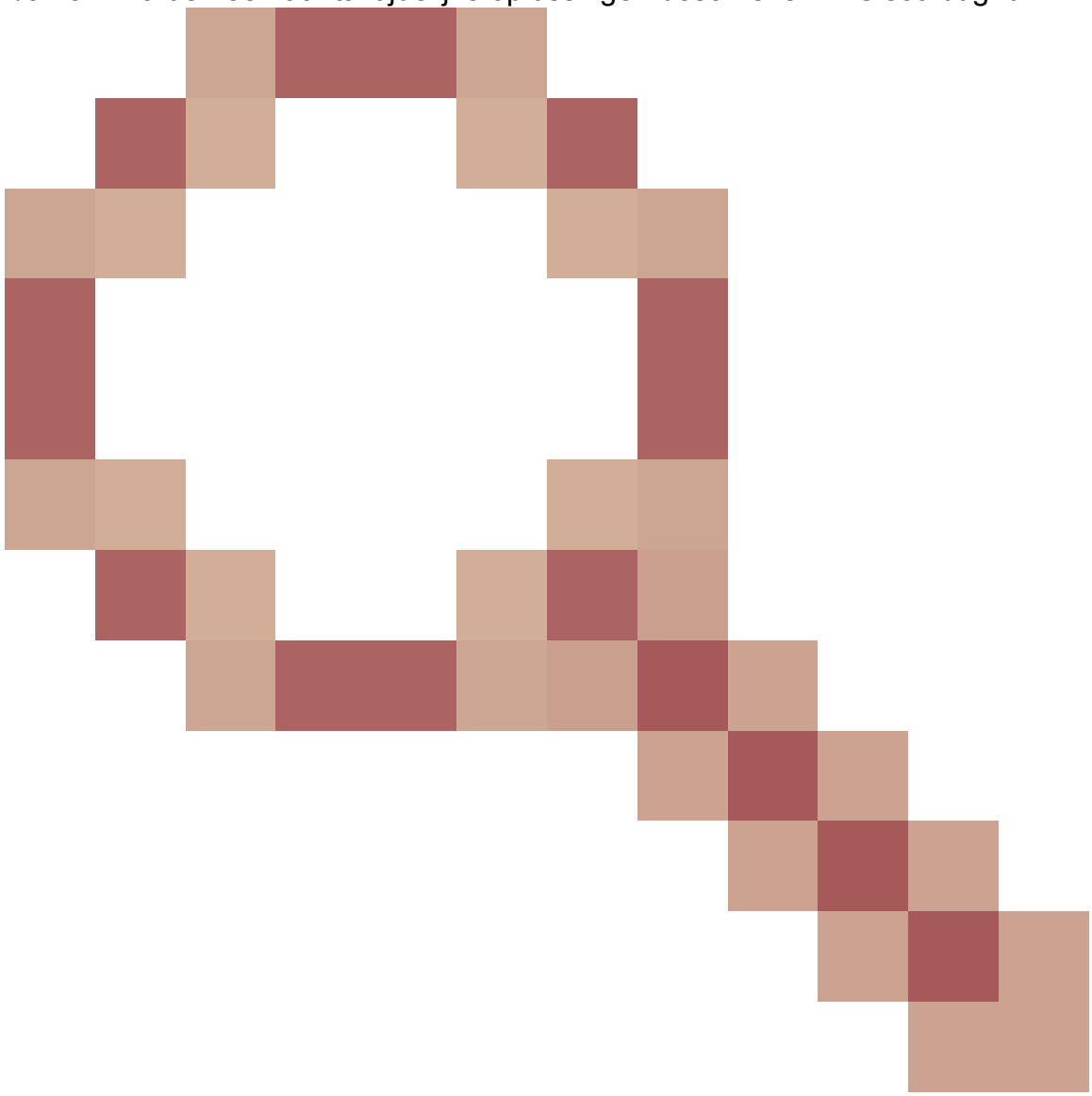
<#root>

```
%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 show nat pool cluster om de pooldistributie te identificeren.
- Gebruik de opdracht NAT-poolip <addr> voor het tonen van details van het cluster om het poolgebruik over clusterknooppunten te begrijpen.

Beperken

- Voor pre-6.7/9.15.1 worden een aantal tijdelijke oplossingen beschreven in Cisco bug-id



CSC10530

.
- In post-6.7/9.15.1, gebruik de duidelijke globale <ip> gport <start-end>opdracht om sommige van de poortblokken op andere knooppunten handmatig te verwijderen voor herdistributie naar de vereiste knooppunten.

Symptomen

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

Verificatie

De ARP-tabel van de direct verbonden apparaten toont het MAC-adres van de interface van

clustergegevens na een wijziging van de controleknooppunt:

<#root>

```
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

Configureer statische (virtuele) MAC op clustergegevensinterfaces.

Aansluitingen onderworpen aan PAT-storing

Symptomen

Connectiviteitsproblemen voor verkeer dat door het cluster is gekoppeld.

Verificatie/beperking

- Zorg ervoor dat de configuratie correct wordt herhaald.
- Zorg ervoor dat het zwembad gelijkmatig is verdeeld.
- Zorg ervoor dat het eigendom van de pool geldig is.
- Geen storingsteller stappen in tonen asp cluster teller.
- Zorg ervoor dat de directeuren-/expeditiestromen met de juiste informatie worden gecreëerd.
- Valideren als back-upxates worden gemaakt, bijgewerkt en opgeruimd zoals verwacht.
- Valideren als xates worden aangemaakt en beëindigd per "per-sessie"-gedrag.
- Schakel "debug nat 2" in voor een indicatie van fouten. Deze uitvoer kan bijvoorbeeld zeer ruis veroorzaken:

<#root>

```
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 de debug als volgt:

<#root>

```
firepower#
un all
```

- Schakel verbinding en NAT-gerelateerde syslogs in om de informatie te correleren aan een mislukte verbinding.

ASA en FTD Clustering PAT Verbeteringen (na 9.15 en 6.7)

Wat is er veranderd?

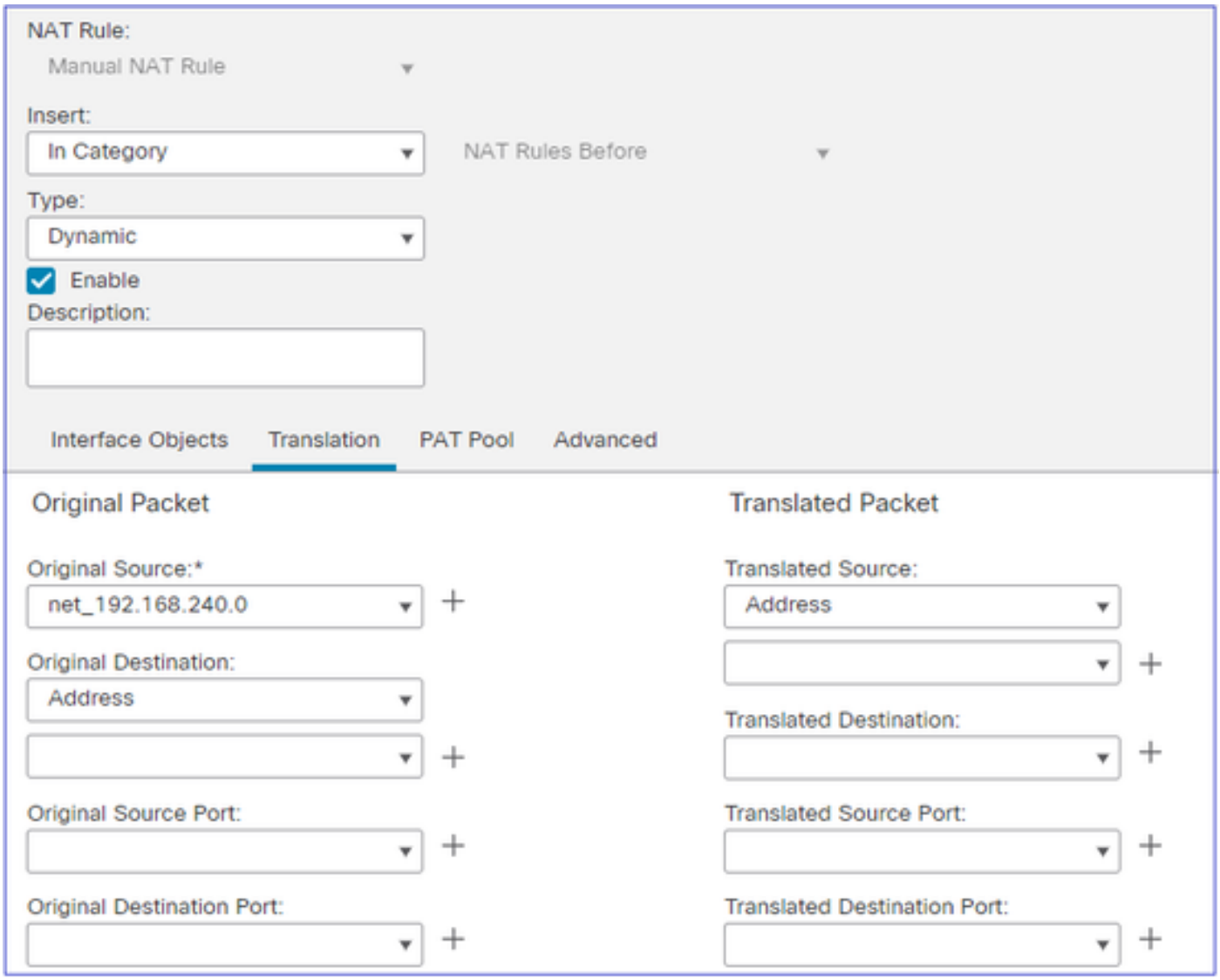
De operatie PAT werd herontworpen. Individuele IP's worden niet meer verdeeld onder elk van de clusterleden. In plaats daarvan worden de PAT IP's in poortblokken opgesplitst en worden die poortblokken gelijkmatig (zoveel mogelijk) verdeeld over de clusterleden, in combinatie met de werking van de IP-stickiness.

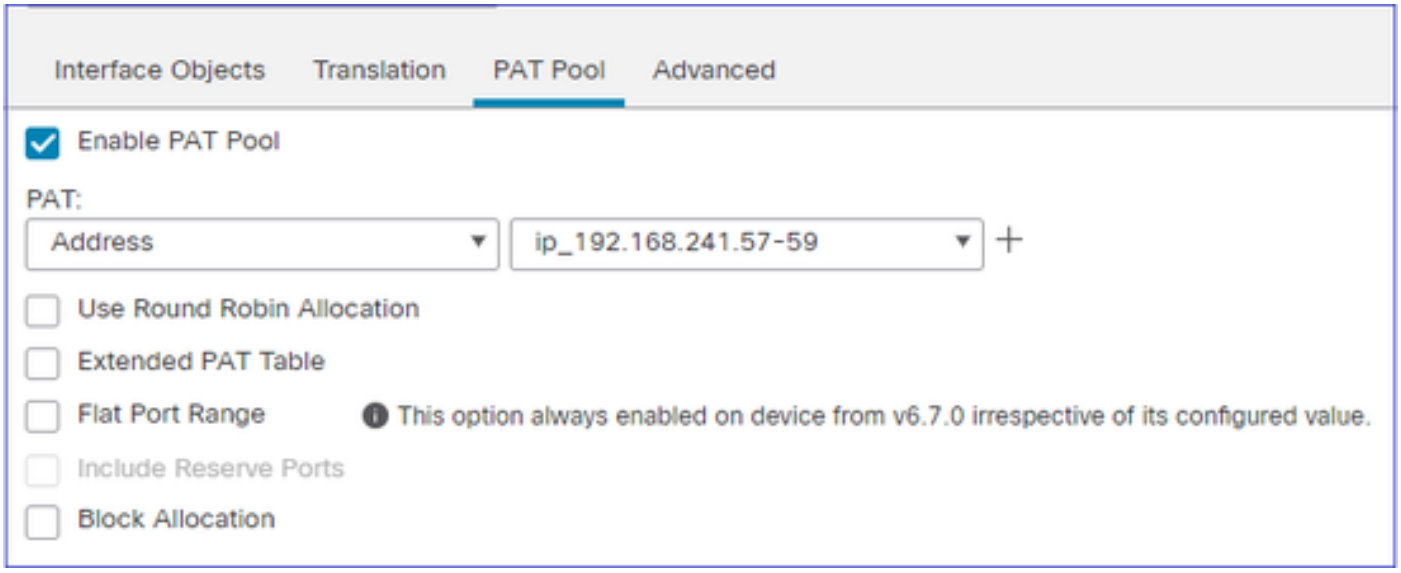
Het nieuwe ontwerp gaat in op deze beperkingen (zie de vorige paragraaf):

- Multisessietoepassingen worden beïnvloed door een gebrek aan clusterbrede IP-kleverigheid.
- De eis is dat er een PAT-pool van grootte is die ten minste gelijk is aan het aantal knooppunten in het cluster.
- PAT-poortverdeling wordt onevenwichtig wanneer knooppunten het cluster verlaten of zich bij het cluster aansluiten.
- Geen syslogs om PAT pool onbalans aan te geven.

Technisch, in plaats van standaard 1-511, 512-1023, en 1024-65535 poortbereiken, is er nu 1024-65535 als standaardpoortbereik voor PAT. Dit standaardbereik kan worden uitgebreid met een geprivilegieerde poortbereik 1-1023 voor reguliere PAT ("include-reserve"-optie).

Dit is een voorbeeld van een configuratie van een PAT-pool op FTD 6.7. Voor extra details, raadpleeg de betreffende sectie in de Configuration Guide:





Aanvullende informatie over probleemoplossing voor PAT

FTD dataplatformsystemen (post-6.7/9.15.1)

Een stickiness-invaliditeitssyslog wordt gegenereerd wanneer alle poorten uitgeput zijn in de

kleverige IP op een clusterknooppunt, en allocatiebewegingen naar de volgende beschikbare IP met vrije poorten, bijvoorbeeld:

```
%ASA-4-305021: Ports exhausted in pre-allocated PAT pool IP 192.0.2.100 for host 198.51.100.100 Allocat
```

Een Pool onbalans-syslog wordt gegenereerd op een knooppunt wanneer het zich aansluit bij het cluster en krijgt geen of ongelijk aandeel van poortblokken, bijvoorbeeld:

```
%ASA-4-305022: Cluster unit ASA-4 has been allocated 0 port blocks for PAT usage. All units should have
%ASA-4-305022: Cluster unit ASA-4 has been allocated 12 port blocks for PAT usage. All units should hav
```

Opdrachten weergeven

Distributiestatus van de groep

In de samenvattende output van het show-nat-poolcluster mag er voor elk IP-adres van het PAT geen verschil zijn van meer dan 1 poortblok over de knooppunten in een evenwichtig distributiescenario. Voorbeelden van een evenwichtige en onevenwichtige verdeling van de havenblokken.

<#root>

```
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:

<#root>

```
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 /
```

Eigendomsstatus van pool

In de show Nat pool cluster uitvoer, mag er geen enkele poortblok met ofwel eigenaar of back-up als ONBEKEND zijn. Als er een is, wijst het op een probleem met de communicatie van het poolbezit. Voorbeeld:

<#root>

```
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 haventoewijzingen in havenblokken

De opdracht NAT-pool tonen wordt uitgebreid met extra opties voor het weergeven van gedetailleerde informatie en gefilterde uitvoer. Voorbeeld:

<#root>

```
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 *
```

"*" geeft aan dat het een back-uppoortblok is

Om dit op te lossen, gebruikt u de opdracht clear xate global <ip> gport <start-end> om sommige poortblokken op andere knooppunten handmatig te verwijderen en ze opnieuw te distribueren naar de vereiste knooppunten.

Handmatig geactiveerde herverdeling van havenblokken

- In een productienetwerk met constant verkeer, wanneer een knooppunt het cluster verlaat en weer betreedt (waarschijnlijk als gevolg van een traceback), kunnen er gevallen zijn waarin het geen gelijk deel van het zwembad kan krijgen of, in het ergste geval, kan het geen poortblok krijgen.
- Gebruik de opdracht show nat pool cluster samenvatting om te identificeren welke knooppunt meer poortblokken bezit dan vereist is.
- Op de knooppunten die meer poortblokken bezitten, gebruik de opdracht show nat pool ip <addr> detail om de poortblokken met het minste aantal toewijzingen te ontdekken.
- Gebruik de opdracht clear xate global <adres> gport <start-end> om de vertalingen te verwijderen die uit die poortblokken zijn gemaakt, zodat ze beschikbaar worden voor herdistributie naar de vereiste knooppunten, bijvoorbeeld:

<#root>

```
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
```

Veelgestelde vragen (FAQ) voor post-6.7/9.15.1 PAT

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

A. Niet meer, en er is geen knevel aan switch tussen IP op adressen-gebaseerde versus op

poortblok-gebaseerde pooldistributieregelingen.

De oudere regeling van de op IP-adres gebaseerde pooldistributie resulteerde in multi-sessie applicatiefouten waarbij meerdere verbindingen (die deel uitmaken van één enkele toepassingstransactie) van een host worden gebalanceerd op verschillende knooppunten van het cluster en dus worden vertaald door verschillende in kaart gebrachte IP-adressen, wat ertoe leidt dat de doelserver ze ziet als afkomstig van verschillende entiteiten.

En met de nieuwe op poortblokken gebaseerde distributieregeling, zelfs als u nu kunt werken met zo laag als één PAT IP-adres, wordt het altijd aanbevolen om genoeg PAT IP-adressen te hebben op basis van het aantal verbindingen dat nodig is om PATed te zijn.

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

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

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

A. Nee, elk IP wordt onafhankelijk verdeeld.

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

A. Dat klopt, elke PAT IP is gedeeltelijk eigendom van elk knooppunt. Als een gekozen openbare IP op een knooppunt is uitgeput, wordt een syslog gegenereerd die aangeeft dat kleverige IP niet kan worden behouden en wordt de toewijzing verplaatst naar het volgende openbare IP. Of het nu een standalone, HA, of Cluster-implementatie is, IP-stickiness is altijd op een best-inspanningsbasis afhankelijk van de beschikbaarheid van de pool.

Q. Is alles gebaseerd op één enkel IP-adres in de PAT-pool, maar is niet van toepassing als meer dan één IP-adres in de PAT-pool wordt 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 verdeeld over alle leden in het cluster. Dus, als je een klasse C van adressen in de PAT-pool hebt, heeft elk clusterlid poortpools van elk van de PAT-pooladressen.

V. Werkt het met CGNAT?

A. Ja, CGNAT wordt eveneens ondersteund. CGNAT, ook bekend als block-allocation PAT, heeft een standaard blokgrootte van '512', die kan worden gewijzigd via xlate bloktoewijzingsgrootte CLI. In het geval van reguliere dynamische PAT (non-CGNAT) is de blokgrootte altijd '512', die vast en niet configureerbaar is.

Q. Als de eenheid het cluster verlaat, wijst de controleknoop de waaier van het havenblok aan andere eenheden toe of houdt het aan zich?

A. Elk poortblok heeft een eigenaar en back-up. Elke keer dat een xlate wordt gemaakt van een poortblok, wordt deze ook gerepliceerd naar de back-upknooppunt van het poortblok. Wanneer een knooppunt het cluster verlaat, bezit het back-upknooppunt alle poortblokken en alle huidige verbindingen. De back-upknooppunt, omdat het de eigenaar is geworden van deze extra poortblokken, kiest een nieuwe back-up voor deze knooppunten en repliceert alle huidige uitzettingen naar dat knooppunt om storingsscenario's te verwerken.

V. Welke maatregelen kunnen op basis van die signalering worden genomen om de kleverigheid te handhaven?

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

Reden 1: Het verkeer is niet correct in balans door welke een van de knooppunten een hoger aantal verbindingen ziet dan anderen wat leidt tot de bijzondere kleverige IP-uitputting. Dit kan worden aangepakt als u ervoor zorgt dat het verkeer gelijkmatig over clusterknooppunten is verdeeld. Bijvoorbeeld, op een FPR41xx-cluster, pas het algoritme voor taakverdeling aan op verbonden switches. Zorg er op een FPR9300-cluster voor dat het chassis een gelijk aantal blades bevat.

Reden 2: PAT zwembad gebruik is echt hoog, wat leidt tot frequente uitputting van het zwembad. Om deze verhoging aan te pakken, vergroot de PAT-poolgrootte.

V. Hoe wordt de ondersteuning voor het uitgebreide trefwoord verwerkt? Toont het een fout, en verhindert het gehele NAT bevel om tijdens de verbetering worden toegevoegd, of verwijdert het het uitgebreide sleutelwoord, en toont een waarschuwing?

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

V. Is het hetzelfde aantal vertalingen als gelijktijdige verbindingen?

A. In pre-6.7/9.15.1, hoewel het 1-65535 was, omdat de bronpoorten nooit veel in de range 1-1024 worden gebruikt, maakt het effectief het 1024-65535 (64512 conns). In de post-6.7/9.15.1 implementatie met 'plat' als standaardgedrag, is het 1024-65535. Maar als u de 1-1024 wilt gebruiken, kunt u met de optie "Inclusief-reserve".

Q. Als de knoop zich bij de cluster terug aansluit, heeft het de oude reserveknoop als steun en die reserveknoop geeft zijn oude havenblok aan het?

A. Het hangt af van de beschikbaarheid van havenblokken op dat moment. Wanneer een knooppunt het cluster verlaat, worden alle poortblokken naar het back-upknooppunt verplaatst. Het is dan de controleknoop die vrije havenblokken ophoopt en hen aan de vereiste knooppunten verdeelt.

Q. Als er een verandering in de staat van het controleknooppunt is, wordt een nieuw controleknooppunt geselecteerd, wordt de PAT-bloktoewijzing gehandhaafd of worden de

poortblokken opnieuw toegewezen op basis van het nieuwe controleknooppunt?

A. Het nieuwe controleknooppunt begrijpt welke blokken toegewezen zijn en welke vrij zijn en begint vanaf daar.

Q. Is het maximumaantal uitsplitsingen hetzelfde als het maximumaantal gelijktijdige verbindingen met dit nieuwe gedrag?

A. Ja. Het maximum aantal xlates is afhankelijk van de beschikbaarheid van PAT-poorten. Het heeft niets te maken met het maximum 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 max. gelijktijdige verbindingen bereiken.

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

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

Verder, na opnieuw toetreden, herberekent elk knooppunt het aantal blokken dat het kan bezitten. Als een knooppunt meer blokken bevat dan het zou moeten, geeft het dergelijke extra poortblokken vrij aan het controleknooppunt zodra deze beschikbaar komen. Het controleknooppunt wijst ze vervolgens toe aan het nieuw aangesloten gegevensknooppunt.

Q. Wordt het slechts TCP en UDP protocollen of SCTP eveneens gesteund?

A. SCTP werd nooit ondersteund met dynamisch PAT. Voor SCTP-verkeer wordt aanbevolen alleen een statisch netwerkobject NAT te gebruiken.

V. Als een knooppunt geen blokpoorten heeft, laat het dan pakketten vallen en gebruikt het niet het volgende beschikbare IP-blok?

A. Nee, het valt niet onmiddellijk. Het maakt gebruik van beschikbare poortblokken van het volgende PAT IP. Als alle poortblokken in alle PAT IP's zijn uitgeput, wordt het verkeer verlaagd.

Q. Om de overbelasting van de controleknoop in een venster van de clusterverbetering te vermijden, is het beter om een nieuwe controle eerder (bijvoorbeeld, halverwege een 4-eenheid clusterverbetering) te verkiezen, eerder dan te wachten op alle verbindingen die op de controleknoop worden behandeld?

A. De controle moet als laatste worden bijgewerkt. Dit komt doordat, wanneer de control node de nieuwere versie uitvoert, het geen pooloverdeling initieert tenzij alle knooppunten de nieuwere versie uitvoeren. Bovendien, wanneer een upgrade wordt uitgevoerd, negeren alle gegevensknooppunten met een nieuwere versie pooldistributieberichten van een controleknooppunt als het een oudere versie uitvoert.

Om dit in detail te verklaren, overweeg een clusterplaatsing met 4 knooppunten A, B, C, en D met

A als controle. Hier zijn de typische hitless upgrade stappen:

1. Download een nieuwe versie op elk van de knooppunten.
2. Opnieuw laden eenheid "D". Alle verbindingen, versies worden verplaatst naar het back-upknooppunt.
3. Eenheid "D" komt naar voren en:

a. Processen PAT-configuratie

b. Verdeelt elk IP-pakketsnelheid in poortblokken

c. Heeft alle havenblokken in niet-toegewezen staat

d. Negeert oudere versie van cluster PAT-berichten die van controle zijn ontvangen

e. Richt alle PAT-verbindingen op Primair.

4. Op dezelfde manier brengt u andere knooppunten naar voren met de nieuwe versie.

5. Besturing van herlaadeenheid A. Aangezien er geen back-up voor de besturing is, worden alle bestaande verbindingen verbroken

6. Met de nieuwe controle wordt begonnen met de distributie van havenblokken in het nieuwere formaat

7. Eenheid "A" treedt weer toe en is in staat berichten over de distributie van havenblokken te accepteren en erop te reageren

Gefragmenteerde verwerking

Symptoom

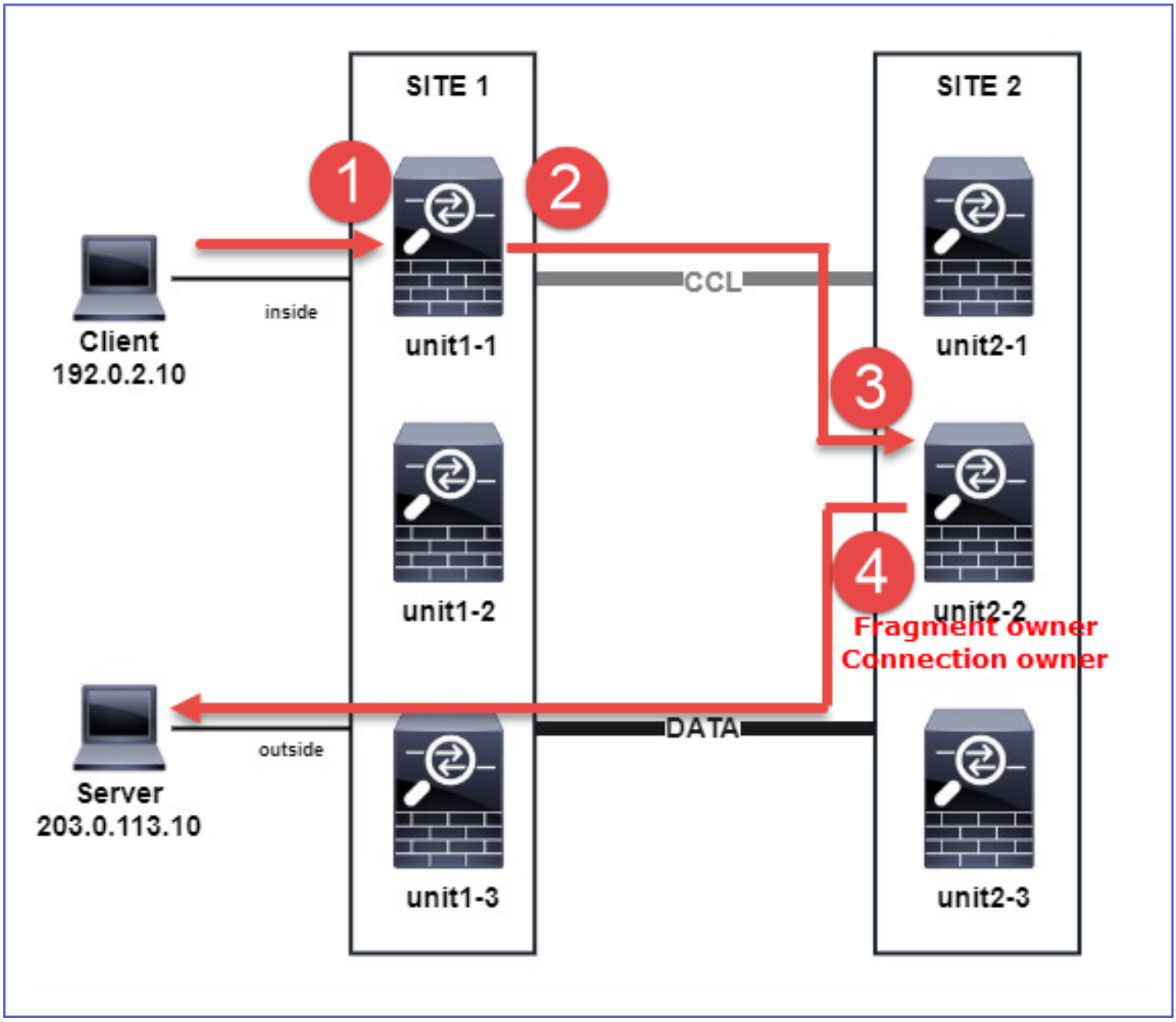
In intersite cluster implementaties gefragmenteerde pakketten die moeten worden verwerkt in 1 specifieke site (site-local traffic), kan nog steeds worden verzonden naar de eenheden in andere sites, omdat een van deze sites de fragment-eigenaar kan hebben.

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

Voor gefragmenteerde pakketten bepalen clustereenheden die een fragment ontvangen, een fragmenteigenaar op basis van een hash van het IP-adres van de fragmentbron, het IP-adres van de bestemming en de pakketid. Alle fragmenten worden vervolgens doorgestuurd naar de fragmenteigenaar via de koppeling voor clustercontrole. De fragmenten kunnen aan verschillende clustereenheden worden in evenwicht gebracht omdat slechts het eerste fragment de 5-tuple omvat die in de switch de lading-saldo hash wordt gebruikt. Andere fragmenten bevatten niet de bron- en bestemmingshavens en kunnen met andere clustereenheden worden gebalanceerd. De fragmenteigenaar brengt het pakket tijdelijk weer samen zodat het de regisseur kan bepalen op basis van een hash van het IP-adres van de bron/bestemming en de poorten. Als het om een nieuwe verbinding gaat, wordt de eigenaar van het fragment de eigenaar van de verbinding. Als

het om een bestaande verbinding gaat, stuurt de fragmenteigenaar alle fragmenten door naar de verbindingseigenaar via de clusterbesturingsverbinding. De verbindingseigenaar assembleert vervolgens alle fragmenten.

Overweeg deze topologie met de stroom van een gefragmenteerd ICMP echoverzoek van de cliënt aan de server:



Om de volgorde van de bewerkingen te begrijpen, zijn er clusterbrede pakketopnamen op de binnen-, buitenkant- en clusterbesturingskoppelingsinterfaces geconfigureerd met de traceeroptie. Bovendien is een pakketopname met de optie reject-hide geconfigureerd op de binnenkant van de interface.

<#root>

```
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
```

Orde van de activiteiten binnen het cluster:

1. unit-1-1 in site 1 ontvangt de gefragmenteerde ICMP-echopakketten.

<#root>

```
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 unit-2-2 in site 2 als de fragmenteigenaar en stuurt er gefragmenteerde pakketten naar.
Het MAC-adres van de bestemming van de pakketten die van unit-1-1 naar unit-2-2 worden verzonden, is het MAC-adres van de CCL-link in unit-2-2.

<#root>

```
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 de gefragmenteerde pakketten, herschikt deze en wordt de eigenaar van de stroom.

<#root>

```
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 beveiligingsbeleid en verstuurt ze, via de buiteninterface, van site 2 naar site 1.

<#root>

```
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/voorbehouden

- Anders dan de rol van regisseur kan de fragmenteigenaar niet binnen een bepaalde site worden gelokaliseerd. De fragmenteigenaar wordt bepaald door de eenheid die oorspronkelijk de gefragmenteerde pakketten van een nieuwe verbinding ontvangt en op om het even welke plaats kan worden gevestigd.
- Aangezien een fragmenteigenaar ook de verbindingseigenaar kan worden, dan om de pakketten aan de bestemmingsgastheer door te sturen, moet het de uitgangsinterface kunnen oplossen, en de IP en MAC adressen van de bestemmingsgastheer of de volgende hop vinden. Dit veronderstelt dat de volgende hop(en) ook de bereikbaarheid naar de doelhost moet(en) hebben.
- Om de gefragmenteerde pakketten opnieuw samen te stellen, onderhoudt ASA/FTD een module voor de herassemblage van IP-fragmenten voor elke genoemde interface. Om de operationele gegevens van de IP module van de fragmentherassemblage te tonen, gebruik het bevel van het showfragment:
  <#root>

  ```
  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 fragmenteigenaar of de verbindingseigenaar de gefragmenteerde pakketten in de fragmentwachtrij. De grootte van de fragmentwachtrij wordt beperkt door de waarde van de teller Grootte (standaard 200) die met de opdracht fragmentgrootte <grootte> <naam> is geconfigureerd. Wanneer de grootte van de fragmentwachtrij 2/3 van de grootte bereikt, wordt de drempel van de fragmentwachtrij geacht te zijn overschreden en worden alle nieuwe fragmenten die geen deel uitmaken van de huidige fragmentketen, verwijderd. In dit geval wordt de overschreden Fragment-wachtrij verhoogd en wordt syslog-bericht FTD-3-209006 gegenereerd.

<#root>

```
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 203.0.11

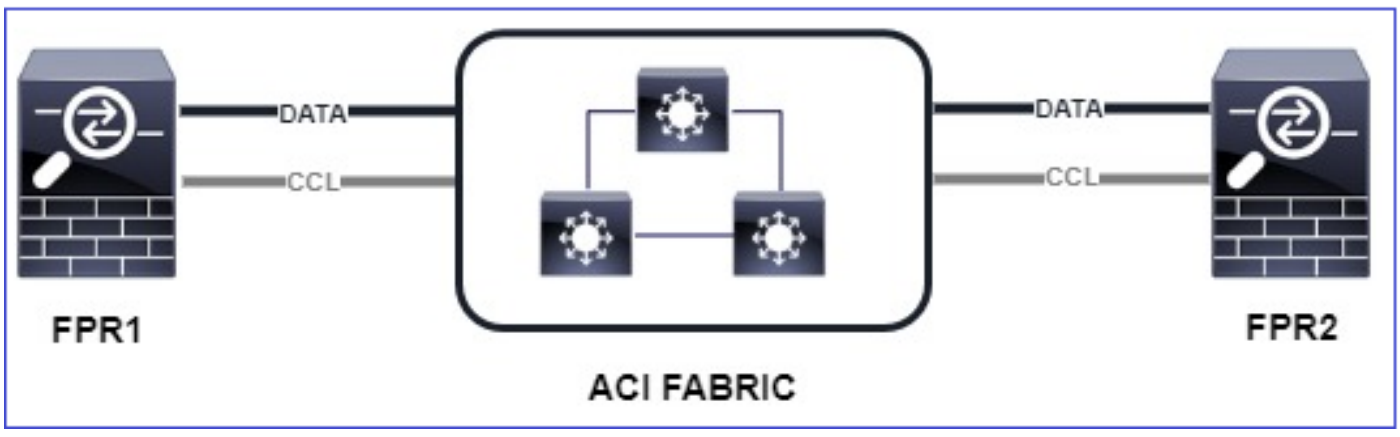
Als tijdelijke oplossing kunt u de grootte van Firepower Management Center > Apparaten > Apparaatbeheer > [Apparaat bewerken] > Interfaces > [Interface] > Geavanceerd > Beveiligingsconfiguratie > Standaardinstelling voor fragmenten negeren, de configuratie opslaan en beleid implementeren. Controleer vervolgens de wachtrijteller in de opdrachtoutput van het showfragment en het optreden van het syslogbericht FTD-3-209006.

ACI-problemen

Intermitterende connectiviteitsproblemen door de cluster door actieve L4 checksum verificatie in ACI Pod

Symptoom

- Intermitterende connectiviteitsproblemen door de ASA/FTD-cluster, geïmplementeerd in een ACI Pod.
- Als er slechts 1 eenheid in het cluster zit, worden de connectiviteitsproblemen niet waargenomen.
- Pakketten die van een clustereenheid naar een of meer andere eenheden in het cluster worden verzonden, zijn niet zichtbaar in de FXOS en dataplaat vangt de doeleenheden op.



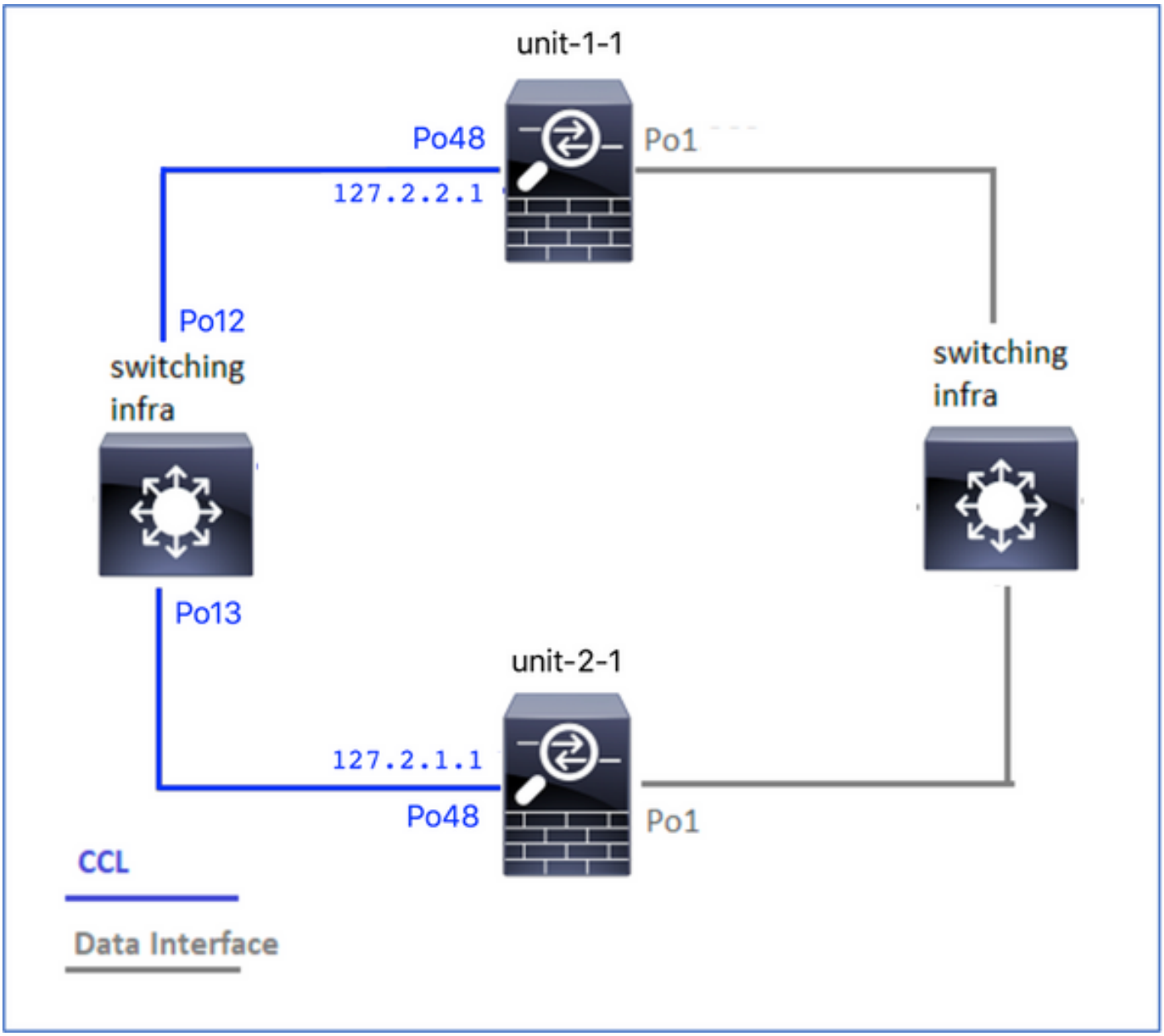
Beperken

- Omgeleid verkeer over de clusterbesturingslink heeft geen correcte L4-checksum en dit wordt verwacht. Switches op het clusterbesturingslinkpad mogen de L4-checksum niet verifiëren. Switches die de L4-checksum verifiëren kunnen ervoor zorgen dat het verkeer wordt gedropt. Controleer de configuratie van de ACI-fabric-switch en controleer of er geen L4-checksum op de ontvangen of verzonden pakketten wordt uitgevoerd via de clusterbesturingslink.

Problemen met Cluster Control Plane

Eenheid kan zich niet bij het cluster aansluiten

MTU-grootte op CCL



Symptomen

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

```
The SECONDARY has left the cluster because application configuration sync is timed out on this unit. Di
Cluster disable is performing cleanup..done.
Unit unit-2-1 is quitting due to system failure for 1 time(s) (last failure is SECONDARY application co
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clust
```

Verificatie/beperking

- Gebruik de opdracht interface show op de FTD om te verifiëren dat de MTU op de interface van de link van de clusterbesturing ten minste 100 bytes hoger is dan de gegevensinterface MTU:

<#root>

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-channel48

"

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 uit door de CCL, met de grootteoptie, om te controleren of deze is geconfigureerd op de CCL MTU, die correct is geconfigureerd op alle apparaten in het pad.

<#root>

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

- Gebruik het bevel van de showinterface op de switch om de configuratie te verifiëren MTU

```
<#root>
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
```

Interfacemismatch tussen clustereenheden

Symptomen

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

```
Interface mismatch between cluster primary 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 erro
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clust
```

Verificatie/beperking

Log in op de FCM GUI op elk chassis, navigeer naar het tabblad Interfaces en controleer of alle

clusterleden dezelfde interfaceconfiguratie hebben:

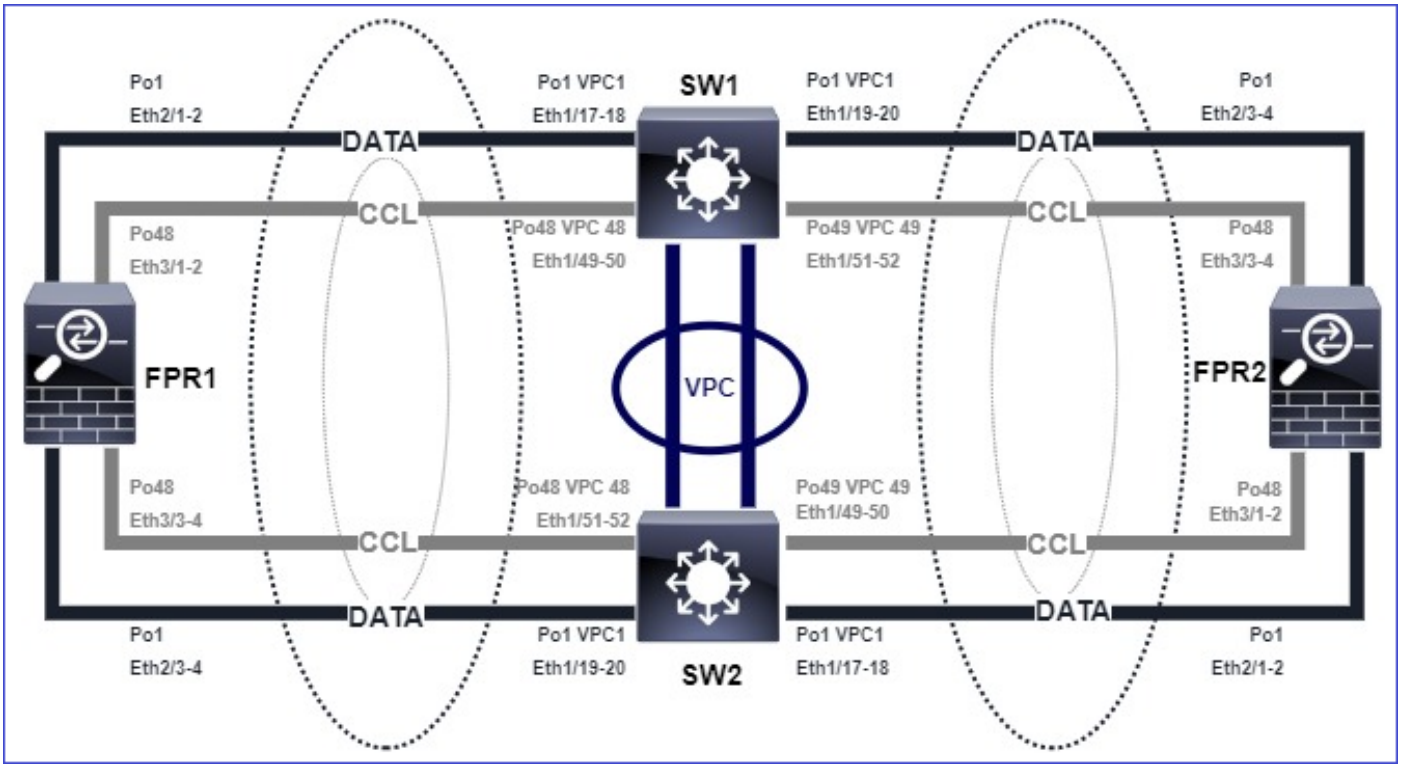
- Interfaces toegewezen aan het logische apparaat
- Beheersnelheid van de interfaces
- Admin-duplex van de interfaces
- Interfacestatus

Probleem met data-/poortinterface

Split-brain vanwege problemen met de bereikbaarheid via de CCL

Symptoom

Er zijn meerdere controle-eenheden in het cluster. Bekijk de volgende topologie:



Chassis 1:

<#root>

```
firepower# show cluster info
```

```
Cluster ftd_cluster1: On
Interface mode: spanned
```

```
This is "unit-1-1" in state PRIMARY
```

```
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 SECONDARY
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 SECONDARY
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:

<#root>

```
firepower# show cluster info
```

```
Cluster ftd_cluster1: On
Interface mode: spanned
```

```
This is "unit-2-1" in state PRIMARY
```

```
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 SECONDARY
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 SECONDARY
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 de connectiviteit tussen de IP-adressen van de clusterbesturingseenheden (CCL) te verifiëren:

<#root>

```
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:

<#root>

```
firepower# show arp
```

```
cluster 127.2.2.3 0015.c500.026f 1
cluster 127.2.2.2 0015.c500.029f 1
```

- In besturingseenheden kunt u opnamen op de CCL-interfaces configureren en controleren:

<#root>

```
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-kanaal interfaces zijn aangesloten op aparte poort-kanaal interfaces op de switch.
- Als Virtual Port-Channel (vPC) op Nexus-switches worden gebruikt, zorg er dan voor dat CCL poort-kanaal interfaces zijn aangesloten op verschillende vPC en dat de vPC-configuratie geen mislukte consistentiestatus heeft.
- Zorg ervoor dat de CCL poort-kanaal interfaces zich in hetzelfde uitzenddomein bevinden en dat het CCL VLAN is gemaakt en toegestaan op de interfaces.

Dit is een voorbeeld van een switch:

<#root>

```
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

<#root>

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
```

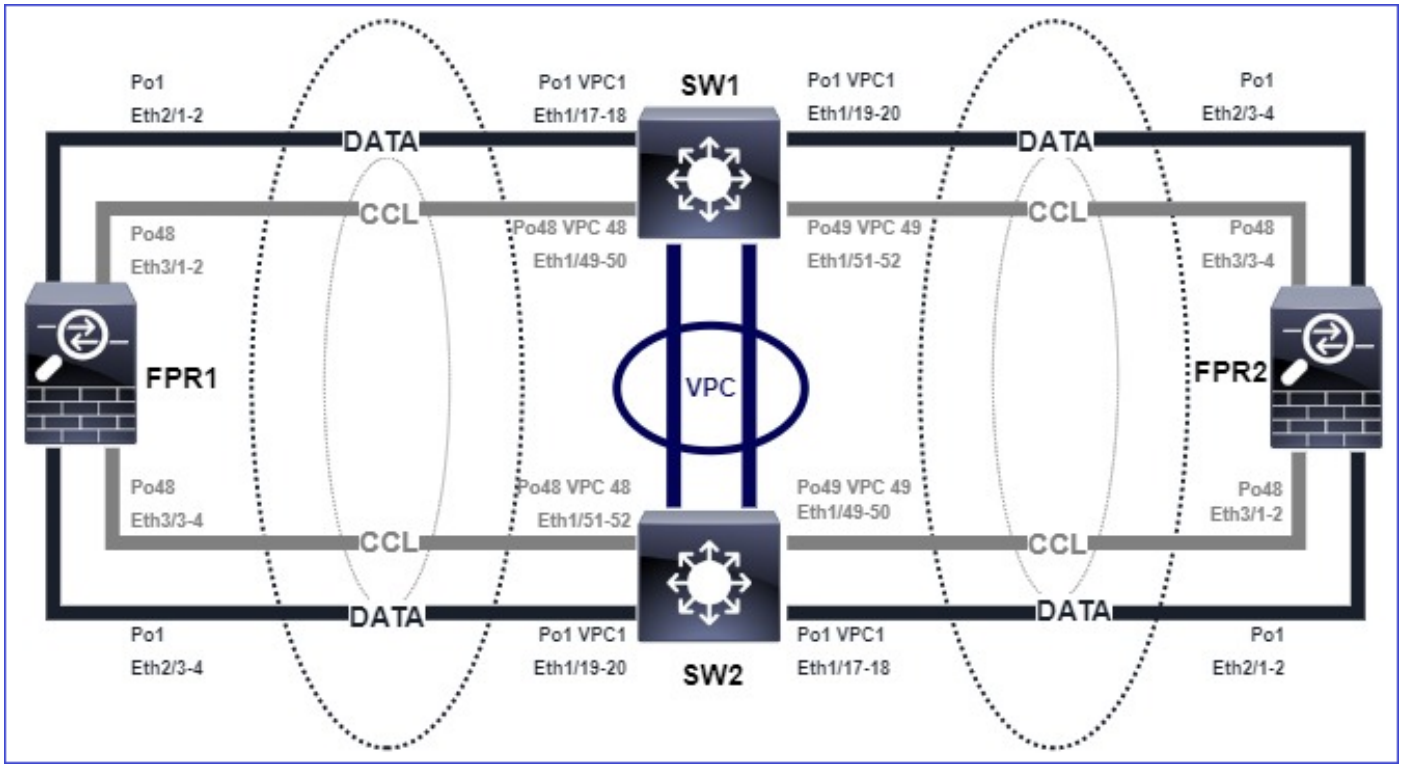
```
49 Po49 up success success 48
```

Uitgeschakelde cluster vanwege opgeschorte datapoortkanaals interfaces

Symptoom

Een of meer data poort-kanaal interfaces zijn opgeschort. Wanneer een administratief ingeschakelde data-interface is opgeschort, worden alle clustereenheden in hetzelfde chassis uit het cluster geschopt vanwege een fout in de interfacestatus.

Bekijk de volgende topologie:



Verificatie

- Controleer de console van de regeleenheid:

<#root>

```
firepower#
Beginning configuration replication to
```

SECONDARY unit-2-2

```
End Configuration Replication to SECONDARY.
```

```
Asking SECONDARY 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 output van de show cluster geschiedenis en de show cluster info spoor module hc opdrachten in de getroffen eenheid (eenheden):

<#root>

```
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 clust

Cluster unit unit-2-1 transitioned from SECONDARY to DISABLED


firepower#
 show cluster history


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

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

12:59:37 UTC Dec 23 2020
SECONDARY_COLD SECONDARY_APP_SYNC Client progression done

13:00:23 UTC Dec 23 2020
SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDARY application configuration sync done

13:00:35 UTC Dec 23 2020
SECONDARY_CONFIG SECONDARY_FILESYS Configuration replication finished

13:00:36 UTC Dec 23 2020
SECONDARY_FILESYS SECONDARY_BULK_SYNC Client progression done


13:01:35 UTC Dec 23 2020


SECONDARY_BULK_SYNC DISABLED Received control message DISABLE (interface health check failure)
```

<#root>

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 expi
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 output van de show port-channel summiere opdracht in de fxos commando shell:

<#root>

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-kanaal interfaces administratief zijn ingeschakeld voor fysieke lidinterfaces met dezelfde duplex/speed-configuratie in alle switches.
- Zorg er in intra-site clusters voor dat dezelfde data poort-kanaalinterface in alle behuizing is aangesloten op dezelfde poort-kanaalinterface op de switch.
- Zorg er bij gebruik van virtuele poortkanalen (vPC) in Nexus-switches voor dat de vPC-configuratie geen mislukte consistentiestatus heeft.
- Zorg er in intra-site clusters voor dat dezelfde datapoortkanaalinterface in alle chassis is aangesloten op dezelfde vPC.

Problemen met clusterstabiliteit

FXOS-tracering

Symptoom

Eenheid verlaat het cluster.

Verificatie/beperking

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

<#root>

```
firepower#
show cluster history
```

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

<#root>

```
FPR4150#
connect local-mgmt

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

- Verzamel het kernbestand dat is gegenereerd rond de tijd dat de eenheid het cluster heeft verlaten en geef het door aan TAC.

Schijf vol

Als het schijfgebruik in de /ngfw-partitie van een cluster-eenheid 94% bereikt, stopt de unit het cluster. De controle van het schijfgebruik gebeurt om de 3 seconden:

<#root>

```
> 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 output van de showclustergeschiedenis:

<#root>

```
15:36:10 UTC May 19 2021
PRIMARY Event: Primary unit unit-1-1 is quitting
                    due to
```

diskstatus

```
 Application health check failure, and
                    primary's application state is down
```

of

```
14:07:26 CEST May 18 2021
SECONDARY DISABLED Received control message DISABLE (application health check failure)
```

Een andere manier om de fout te verifiëren is:

<#root>

```
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
```

Bovendien, als de schijf ~100% is kan de eenheid problemen hebben om zich terug aan te sluiten bij het cluster tot er wat schijfruimte is vrijgegeven.

Overflow-bescherming

Elke 5 minuten controleert elke clustereenheid de lokale en de peer-eenheid op CPU- en geheugengebruik. Als het gebruik hoger is dan de systeemdrempels (LINA CPU 50% of LINA geheugen 59%) wordt een informatieve boodschap weergegeven in:

- Syslogs (FTD-6-748008)
- Bestand log/cluster_trace.log, bijvoorbeeld:

<#root>

```
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 thr
May 20 16:23:06.644 [INFO][CPU load 84% | memory load 35%] of module 1 in chassis 1 (unit-1-1) exceeds
```

Het bericht geeft aan dat bij een storing van de unit de andere middelen van de unit(s) kunnen worden overschreven.

Vereenvoudigde modus

Gedrag bij de vrijgave van VCC vóór 6.3

- U registreert elk clusterknooppunt afzonderlijk op VCC.
- Dan vormt u een logische cluster in FMC.
- Voor elke toevoeging van nieuwe clusterknooppunten moet u de knooppunten handmatig registreren.

VCC na 6.3

- Met de functie voor vereenvoudigde modus kunt u het hele cluster in één stap registreren op

het VCC (registreer slechts één knooppunt van het cluster).

Minimale ondersteunde beheerder	Beheerde apparaten	Min. ondersteunde versie van beheerde apparaat vereist	Opmerkingen
VCC 6.3	FTD-clusters, alleen op FP9300 en FP4100	6.2.0	Dit is alleen een FMC-functie

Waarschuwing: Zodra het cluster op FTD is gevormd, moet u wachten tot de automatische registratie om af te schoppen. U moet niet proberen om de clusterknooppunten handmatig te registreren (Apparaat toevoegen), maar gebruik de optie Reconcile.

Symptoom

Registratiefouten voor knooppunten

- Indien de registratie van de controleknooppunten om welke reden dan ook mislukt, wordt het cluster uit het VCC verwijderd.

Beperken

Als de registratie van de gegevensknooppunten om welke reden dan ook mislukt, zijn er 2 opties:

1. Bij elke inzet in het cluster controleert het VCC of er clusterknooppunten zijn die moeten worden geregistreerd en start het automatisch registreren van deze knooppunten.
2. Er is een Reconcile-optie beschikbaar onder het tabblad Cluster Samenvatting (Apparaten > Apparaatbeheer > tabblad Cluster > link Cluster bekijken). Zodra de Reconcile-actie is gestart, start FMC de automatische registratie van de knooppunten die moeten worden geregistreerd.

Gerelateerde informatie

- Clustering voor de Firepower Threat Defence
- ASA-cluster voor het FirePOWER 4100/9300-chassis
- Over clustering op het FirePOWER 4100/9300-chassis
- Firepower NGFW die Deep Dive groepeert - BRKSEC-3032
- Vastleggingen van de Firepower-firewall analyseren om netwerkproblemen effectief te troubleshooten

Over deze vertaling

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