

# Fehlerbehebung bei Firepower Threat Defense (FTD)-Clustern

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Cluster-Grundlagen](#)

[NGFW-Architektur](#)

[Cluster erfasst](#)

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

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

[Cluster-Gesundheitscheck-Mechanismus](#)

[Cluster-HC-Fehlerszenarien](#)

[Verbindungsaufbau der Cluster-Datenebene](#)

[Fehlerbehebung](#)

[Cluster-Fehlerbehebung - Einführung](#)

[Probleme mit der Cluster-Datenebene](#)

[Häufige Probleme bei NAT/PAT](#)

[Fragment-Handling](#)

[ACI-Probleme](#)

[Probleme mit der Cluster-Kontrollebene](#)

[Einheit kann nicht am Cluster teilnehmen](#)

[MTU-Größe auf CCL](#)

[Schnittstellenkonflikt zwischen Cluster-Einheiten](#)

[Problem mit der Daten-/Port-Channel-Schnittstelle](#)

[Split-Brain aufgrund von Erreichbarkeitsproblemen über den CCL](#)

[Cluster wegen ausgesetzter Daten-Port-Channel-Schnittstellen deaktiviert](#)

[Probleme mit der Cluster-Stabilität](#)

[FXOS-Ablaufverfolgung](#)

[Festplatte voll](#)

[Überlaufschutz](#)

[Vereinfachter Modus](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird die Fehlerbehebung bei einer Cluster-Konfiguration auf der Firepower Next-Generation Firewall (NGFW) beschrieben.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesen Themen verfügen (Links finden Sie im Abschnitt "Verwandte Informationen"):

- FirePOWER Plattformarchitektur
- Konfiguration und Betrieb des FirePOWER Clusters
- Vertrautheit mit FTD und FirePOWER eXtensible Operating System (FXOS) CLI
- NGFW-/Datenebenenprotokolle
- NGFW/Datenebene - Paketverfolgung
- FXOS/Datenebenenenerfassung

## Verwendete Komponenten

- HW: FirePOWER 4125
- SW: 6.7.0 (Build 65) - Datenebene 9.15(1)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Die meisten der in diesem Dokument behandelten Aspekte gelten auch für die Fehlerbehebung in Clustern der Adaptive Security Appliance (ASA).

## Konfigurieren

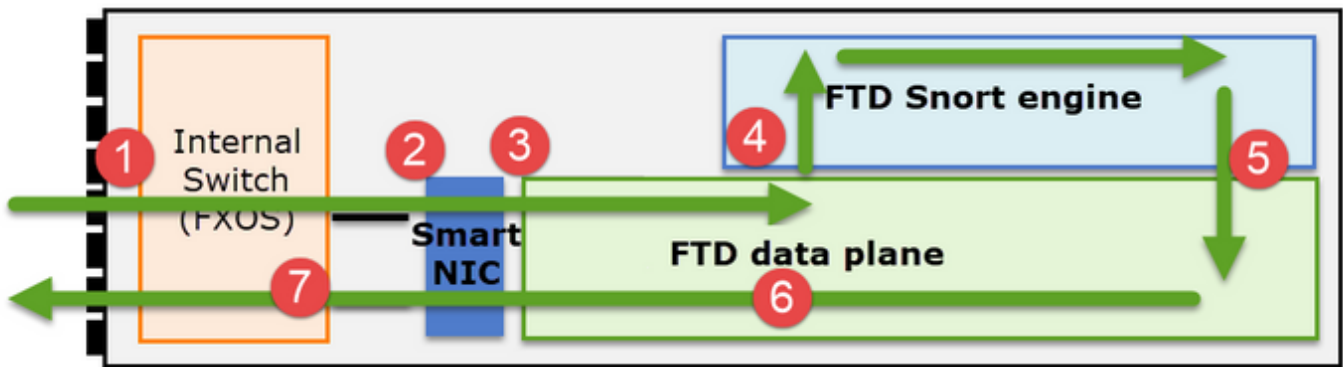
Der Konfigurationsteil einer Cluster-Bereitstellung wird in den FMC- und FXOS-Konfigurationsleitfäden behandelt:

- [Clustering für die FirePOWER Threat Defense](#)
- [Bereitstellung eines Clusters für FirePOWER Threat Defense für Skalierbarkeit und hohe Verfügbarkeit](#)

## Cluster-Grundlagen

### NGFW-Architektur

Es ist wichtig zu verstehen, wie eine FirePOWER 41xx- oder 93xx-Serie Transitpakete behandelt:



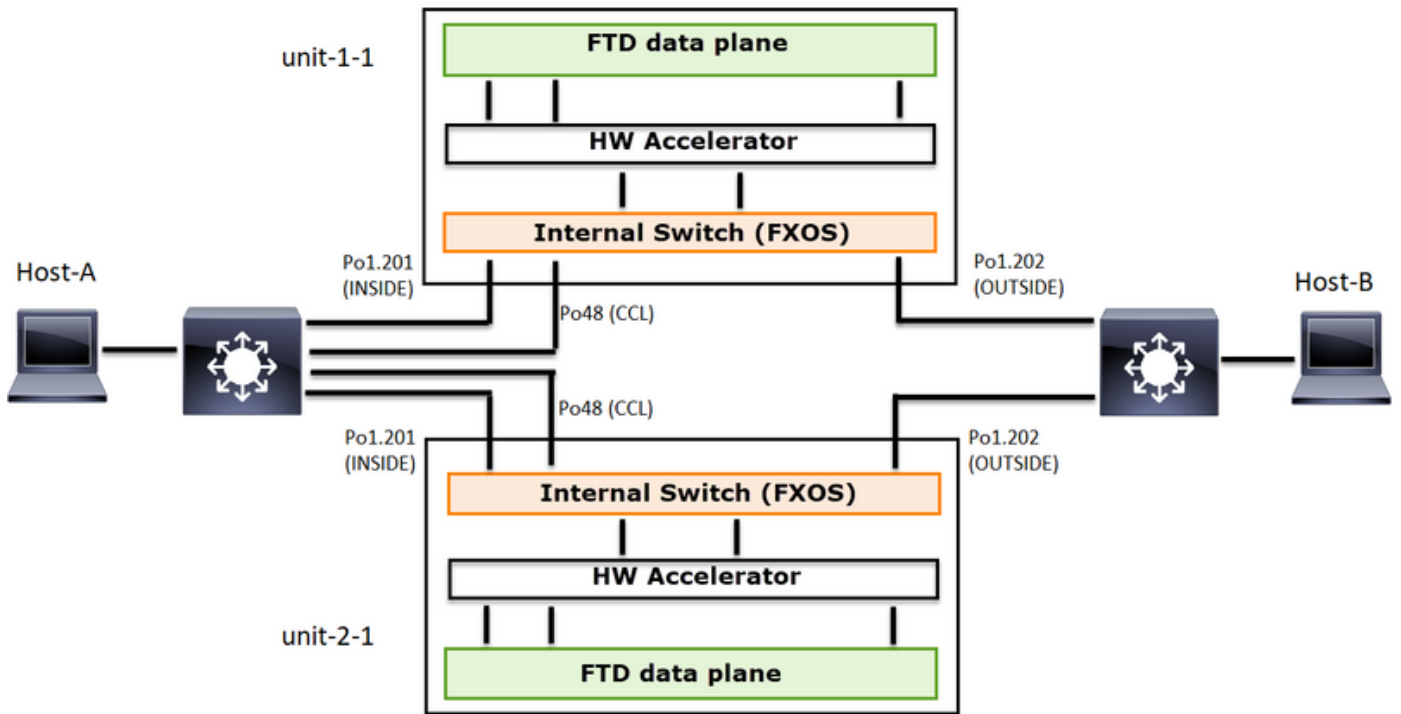
1. Ein Paket gelangt an die Eingangsschnittstelle, und es wird vom internen Chassis-Switch verarbeitet.
2. Das Paket durchläuft die Smart NIC. Wenn der Datenfluss ausgelagert wird (HW-Beschleunigung), wird das Paket nur von der Smart NIC verarbeitet und dann an das Netzwerk zurückgesendet.
3. Wenn das Paket nicht ausgelagert wird, gelangt es auf die FTD-Datenebene, die hauptsächlich L3-/L4-Prüfungen durchführt.
4. Wenn die Richtlinie dies erfordert, wird das Paket von der Snort-Engine geprüft (hauptsächlich L7-Inspektion).
5. Die Snort-Engine gibt ein Urteil für das Paket zurück (z. B. Zulassen oder Blockieren).
6. Die Datenebene verwirft oder leitet das Paket basierend auf dem Urteil von Snort weiter.
7. Das Paket gelangt über den internen Chassis-Switch aus dem Chassis.

## Cluster erfasst

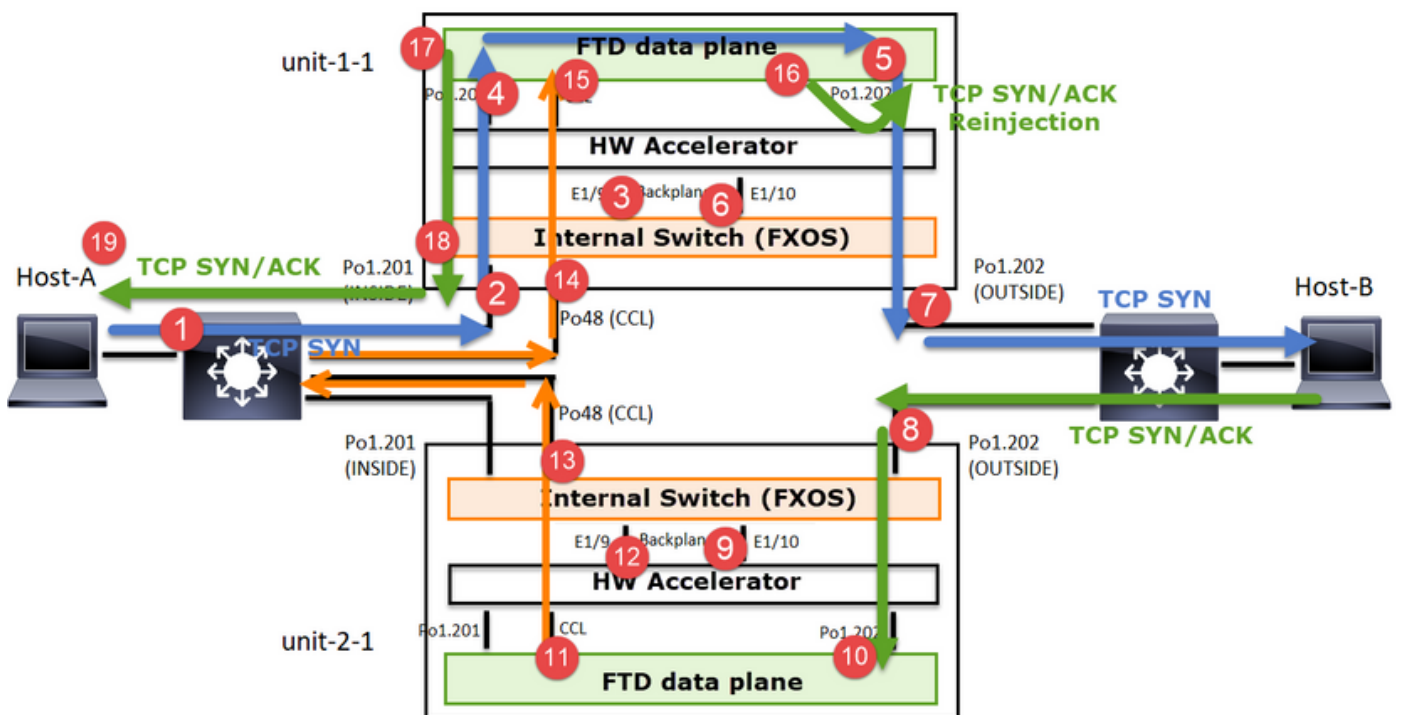
FirePOWER-Appliances stellen mehrere Erfassungspunkte bereit, die einen Überblick über die Datenverkehrsflüsse geben. Wenn Sie die Fehlerbehebung durchführen und Cluster-Erfassungen aktivieren, bestehen die folgenden Hauptprobleme:

- Die Anzahl der Aufnahmen steigt mit der Anzahl der Einheiten im Cluster.
- Sie müssen wissen, wie der Cluster einen bestimmten Fluss behandelt, um das Paket durch den Cluster verfolgen zu können.

Dieses Diagramm zeigt ein Cluster mit 2 Einheiten (z. B. FP941xx/FP9300):



Im Fall einer asymmetrischen TCP-Verbindung sieht ein TCP SYN-, SYN/ACK-Austausch wie folgt aus:



### Datenverkehr weiterleiten

1. TCP-SYN wird von Host-A an Host-B gesendet.
2. Das TCP-SYN erreicht das Chassis (eines der Elemente von Po1).
3. TCP-SYN wird über eine der Backplane-Schnittstellen des Chassis (z. B. E1/9, E1/10 usw.) an die Datenebene gesendet.
4. Das TCP-SYN kommt auf der Datenebene der Eingangsschnittstelle an (Po1.201/INSIDE). In diesem Beispiel übernimmt unit1-1 die Verantwortung für den Datenfluss, führt die

Zufallszuweisung für die Initial Sequence Number (ISN) durch und codiert die Besitzinformationen (Cookies) in der Sequenznummer.

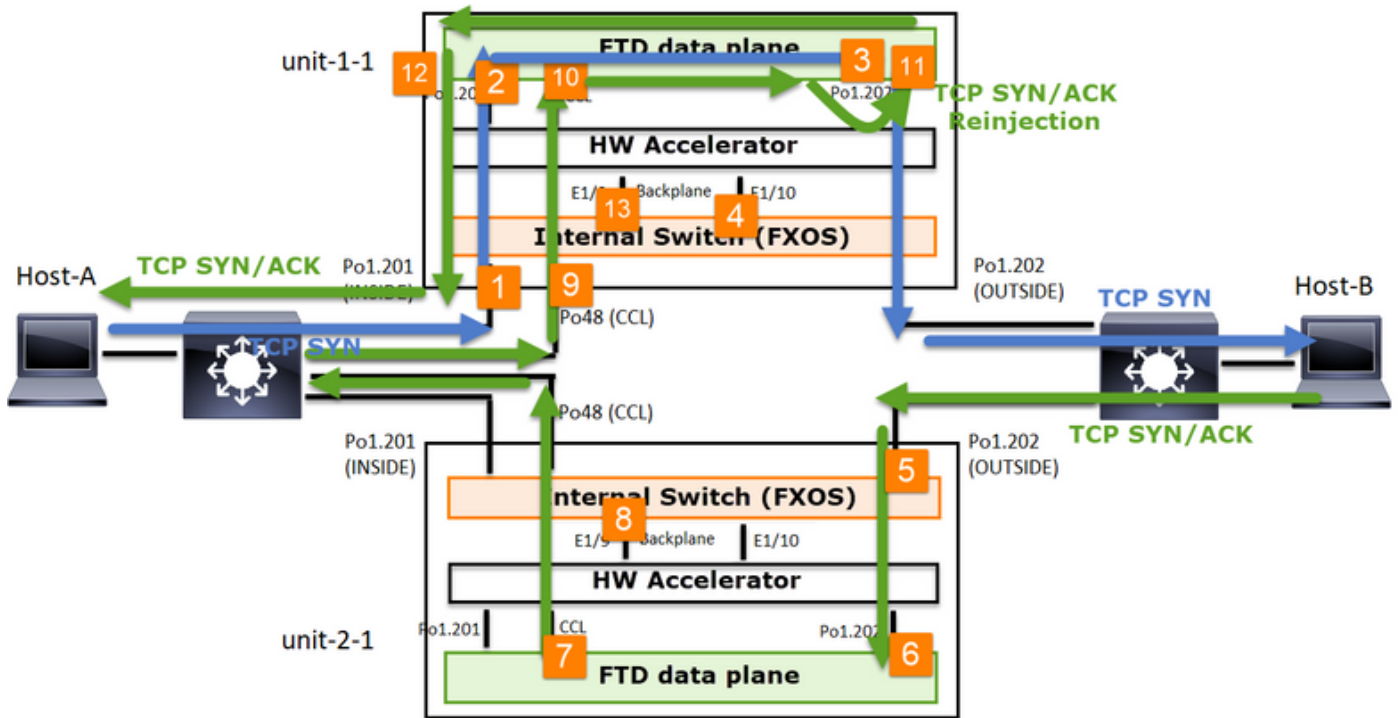
5. TCP SYN wird von Po1.202/OUTSIDE (Datenebenen-Ausgangsschnittstelle) gesendet.
6. Das TCP-SYN kommt an einer der Schnittstellen der Chassis-Backplane an (z. B. E1/9, E1/10 usw.).
7. Das TCP-SYN wird von der physischen Schnittstelle des Chassis (eines der Elemente von Po1) an Host B gesendet.

#### Rückverkehr

8. TCP SYN/ACK wird von Host B gesendet und kommt auf Einheit 2-1 an (einem der Elemente von Po1).
9. TCP SYN/ACK wird über eine der Backplane-Schnittstellen des Chassis (z. B. E1/9, E1/10 usw.) an die Datenebene gesendet.
10. TCP SYN/ACK kommt an der Datenebenen-Eingangsschnittstelle an (Po1.202/OUTSIDE).
11. TCP-SYN/ACK wird von der Cluster Control Link (CCL) an Unit-1-1 gesendet. ISN ist standardmäßig aktiviert. So findet der Forwarder die Eigentümer-Info für TCP SYN+ACKs ohne die Beteiligung des Direktors. Bei anderen Paketen oder wenn ISN deaktiviert ist, wird der Director abgefragt.
12. TCP SYN/ACK kommt an einer der Schnittstellen der Chassis-Backplane an (z. B. E1/9, E1/10 usw.).
13. TCP-SYN/ACK wird von der physischen Schnittstelle des Chassis (eines der Elemente von Po48) an Einheit 1-1 gesendet.
14. TCP SYN/ACK kommt an Einheit 1-1 an (einem der Mitglieder von Po48).
15. TCP SYN/ACK wird über eine der Backplane-Schnittstellen des Chassis an die CCL-Port-Channel-Schnittstelle der Datenebene (Namensfeld-Cluster) weitergeleitet.
16. Die Datenebene sendet das TCP SYN/ACK-Paket wieder an die Datenebenenschnittstelle Po1.202/OUTSIDE.
17. TCP SYN/ACK wird von Po1.201/INSIDE (Datenebenen-Ausgangsschnittstelle) an HOST-A gesendet.
18. Das TCP-SYN/ACK durchläuft eine der Backplane-Schnittstellen des Chassis (z. B. E1/9, E1/10 usw.) und geht aus einem der Elemente von Po1 aus.
19. TCP SYN/ACK erreicht Host A.

Weitere Einzelheiten zu diesem Szenario finden Sie im entsprechenden Abschnitt in den Anwenderberichten zu Cluster Connection Establishment.

Basierend auf diesem Paketaustausch sind alle möglichen Cluster-Erfassungspunkte:



Für den Weiterleitungsverkehr (z. B. TCP SYN) erfassen Sie Folgendes:

1. Die physische Schnittstelle des Chassis (z. B. Po1-Elemente). Diese Erfassung wird über die Benutzeroberfläche des Chassis Managers (CM) oder die CM-CLI konfiguriert.
2. Datenebene-Eingangsschnittstelle (z. B. Po1.201 INSIDE).
3. Ausgangsschnittstelle der Datenebene (z. B. Po1.202 OUTSIDE).
4. Schnittstellen für Chassis-Backplane Der FP4100 verfügt über 2 Backplane-Schnittstellen. Beim FP9300 sind es insgesamt 6 (2 pro Modul). Da Sie nicht wissen, an welcher Schnittstelle das Paket ankommt, müssen Sie die Erfassung an allen Schnittstellen aktivieren.


Erfassung des zurückfließenden Datenverkehrs (z. B. TCP SYN/ACK) auf:

5. Die physische Schnittstelle des Chassis (z. B. Po1-Elemente). Diese Erfassung wird über die Benutzeroberfläche des Chassis Managers (CM) oder die CM-CLI konfiguriert.
6. Datenebene-Eingangsschnittstelle (z. B. Po1.202 OUTSIDE).
7. Da das Paket umgeleitet wird, ist der nächste Erfassungspunkt die Datenebene CCL.
8. Schnittstellen für Chassis-Backplane Auch hier müssen Sie die Erfassung auf beiden Schnittstellen aktivieren.
9. Schnittstellen der CCL-Mitglieder im 1-HE-Chassis.
10. CCL-Schnittstelle auf Datenebene (name-if-Cluster).
11. Eingangsschnittstelle (Po1.202 OUTSIDE). Hierbei handelt es sich um das neu injizierte Paket von CCL zur Datenebene.
12. Ausgangsschnittstelle der Datenebene (z. B. Po1.201 INSIDE).
13. Schnittstellen für Chassis-Backplane

So aktivieren Sie die Clustererfassung

FXOS-Erfassungen

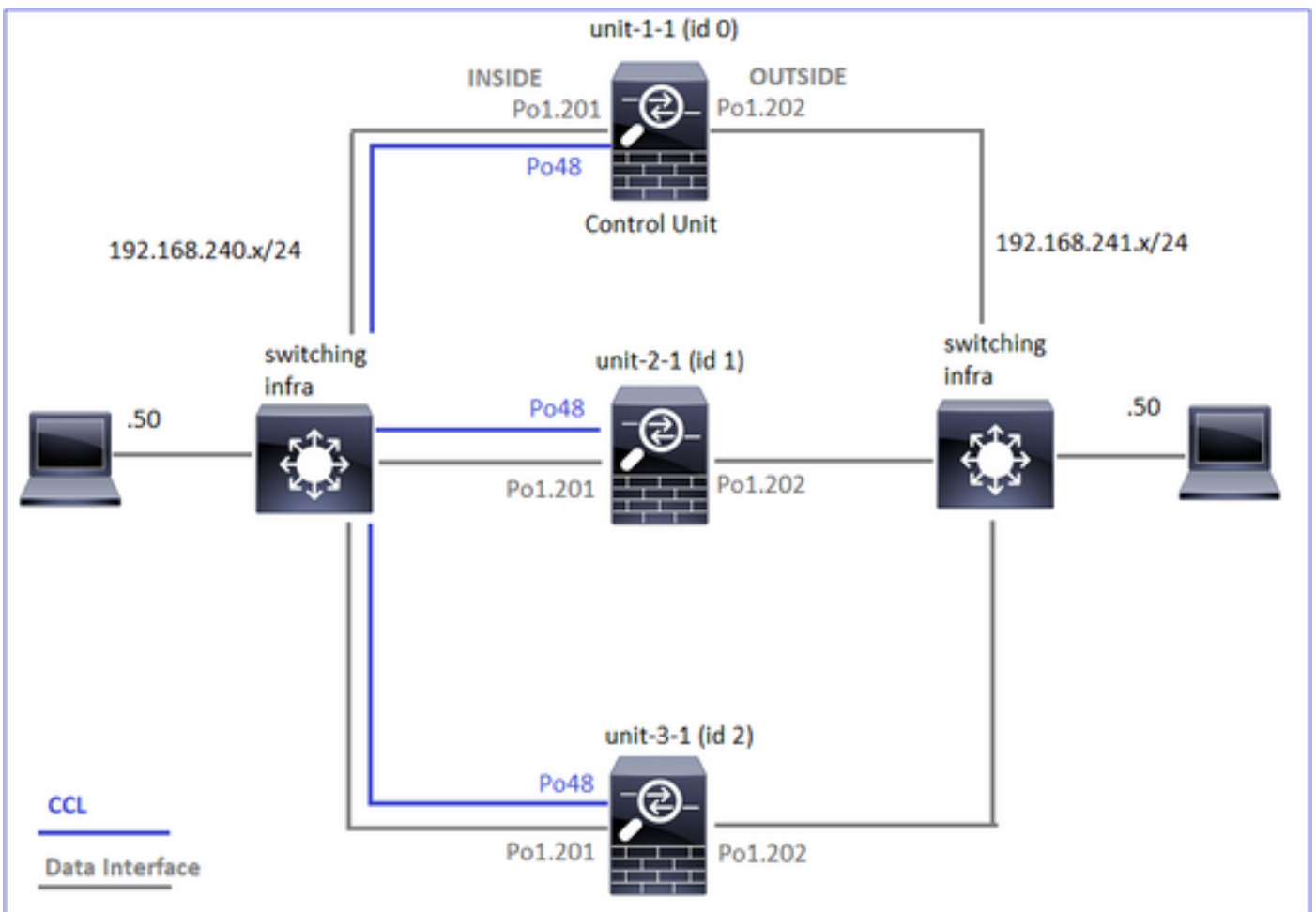
Der Vorgang wird in der FXOS-Konfigurationsanleitung beschrieben: [Paketfassung](#)

 Anmerkung: FXOS-Erfassungen können aus Sicht des internen Switches nur in Eingangsrichtung durchgeführt werden.

### Erfassung der Datenebene

Die empfohlene Methode zum Aktivieren der Erfassung für alle Cluster-Mitglieder ist der Befehl `cluster exec`.

Stellen Sie sich einen Cluster mit drei Einheiten vor:



Verwenden Sie den folgenden Befehl, um zu überprüfen, ob in allen Cluster-Einheiten aktive Erfassungen vorhanden sind:

```
<#root>
```

```
firepower#
```

```
cluster exec show capture
```

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

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

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

So aktivieren Sie die Erfassung der Datenebene für alle Geräte an Po1.201 (INSIDE):

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

Es wird dringend empfohlen, einen Erfassungsfiler anzugeben und den Erfassungspuffer zu erhöhen, falls ein hoher Datenverkehr erwartet wird:

```
<#root>  
firepower#  
cluster exec capture CAPI buffer 33554432 interface INSIDE match tcp host 192.168.240.50 host 192.168.241.50
```

Verifizierung

```
<#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
```

So zeigen Sie den Inhalt aller Aufnahmen an (diese Ausgabe kann sehr lang sein):

```
<#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 PO 192.168.240.50.45456 > 192.168.241.50.80: S 2225395909:2225395909  
2: 11:33:09.880401 802.1Q vlan#201 PO 192.168.241.50.80 > 192.168.240.50.45456: S 719653963:719653963(0  
3: 11:33:09.880691 802.1Q vlan#201 PO 192.168.240.50.45456 > 192.168.241.50.80: . ack 719653964 win 229  
4: 11:33:09.880783 802.1Q vlan#201 PO 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

## Traces erfassen

Wenn Sie sehen möchten, wie die eingehenden Pakete auf der Datenebene der einzelnen Einheiten behandelt werden, verwenden Sie das trace-Schlüsselwort. Dadurch werden die ersten 50 Eingangspakete nachverfolgt. Sie können bis zu 1000 eingehende Pakete verfolgen.



Anmerkung: Wenn auf eine Schnittstelle mehrere Erfassungen angewendet werden, können Sie ein einzelnes Paket nur einmal verfolgen.

---

So verfolgen Sie die ersten 1.000 Eingangspakete an der Schnittstelle OUTSIDE auf allen Cluster-Einheiten:

```
<#root>
```

```
firepower#
```

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

Sobald Sie den Fluss des Interesses erfassen, müssen Sie sicherstellen, dass Sie die Pakete des Interesses auf jeder Einheit verfolgen. Dabei ist zu beachten, dass ein bestimmtes Paket #1 in Einheit-1-1, #2 in einer anderen Einheit usw. sein kann.

In diesem Beispiel sehen Sie, dass SYN/ACK Paket #2 auf Einheit-2-1 ist, Paket #1 auf Einheit-3-1:

```
<#root>
```

```
firepower#
```

```
cluster exec show capture CAPO | include S.*ack
```

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

```
1: 12:58:31.117700 802.1Q vlan#202 PO 192.168.240.50.45468 > 192.168.241.50.80: S 441626016:441626016(0)
2: 12:58:31.118341 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45468:
```

```
s
```

```
301658077:301658077(0)
```

```
ack
```

```
441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
```

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

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

```
1: 12:58:31.111429 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45468:
```

```
s
```

```
301658077:301658077(0)
```

```
ack
```

```
441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
```

So verfolgen Sie das Paket #2 (SYN/ACK) auf der lokalen Einheit:

```
<#root>
```

```
firepower#
```

```
cluster exec show cap CAPO packet-number 2 trace
```

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

```
2: 12:58:31.118341 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45468:
```

```
s
```

```
301658077:301658077(0)
```

```
ack
```

```
441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

Additional Information:  
MAC Access list  
...

So verfolgen Sie dasselbe Paket (SYN/ACK) auf der Remote-Einheit:

<#root>

firepower#

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

1: 12:58:31.111429 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45468:

s

301658077:301658077(0)

ack

441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

...

## CCL-Erfassung

So aktivieren Sie die Erfassung für den CCL-Link (für alle Einheiten):

<#root>

firepower#

cluster exec capture CCL interface cluster

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

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

unit-3-1:\*\*\*\*\*

Ausblenden erneut einwerfen

Eine auf einer Datenschnittstelle der Datenebene aktivierte Erfassung zeigt standardmäßig alle Pakete an:

- Diejenigen, die vom physischen Netzwerk eintreffen
- Diejenigen, die aus der CCL zurückgegeben werden

Wenn Sie die neu eingefügten Pakete nicht anzeigen möchten, verwenden Sie die Option reject-hide. Dies kann hilfreich sein, wenn Sie überprüfen möchten, ob ein Datenfluss asymmetrisch ist:

```
<#root>
```

```
firepower#
```

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

Diese Erfassung zeigt Ihnen nur, was die lokale Einheit auf der spezifischen Schnittstelle tatsächlich direkt vom physischen Netzwerk und nicht von den anderen Cluster-Einheiten erhält.

### ASP-Drops

Wenn Sie für einen bestimmten Datenfluss nach Softwareverwerfen suchen möchten, können Sie die asp-drop-Erfassung aktivieren. Wenn Sie nicht wissen, auf welchen Grund Sie sich konzentrieren sollten, verwenden Sie das Schlüsselwort all. Wenn Sie sich nicht für die Paketnutzlast interessieren, können Sie außerdem das Schlüsselwort header-only angeben. So können Sie 20- bis 30-mal mehr Pakete erfassen:

```
<#root>
```

```
firepower#
```

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

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

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

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

Darüber hinaus können Sie die für die ASP-Erfassung relevanten IPs angeben:

```
<#root>
```

```
firepower#
```

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

```
match ip host 192.0.2.100 any
```

## Erfassung löschen

Zum Löschen des Puffers von jeder Erfassung, die in allen Cluster-Einheiten ausgeführt wird. Dies stoppt die Aufnahmen nicht, sondern löscht nur die Puffer:

```
<#root>
firepower#
cluster exec clear capture /all

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

## Erfassen stoppen

Es gibt zwei Möglichkeiten, eine aktive Erfassung auf allen Cluster-Einheiten zu stoppen. Später können Sie fortfahren.

### Weg 1

```
<#root>
firepower#
cluster exec cap CAPI stop

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

### Fortsetzen

```
<#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:*****
```

## Fortsetzen

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

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

## Erfassen

Es gibt mehrere Möglichkeiten, eine Erfassung zu exportieren.

### Weg 1 - Zu einem Remote-Server

Auf diese Weise können Sie eine Aufzeichnung von der Datenebene auf einen Remote-Server (z. B. TFTP) hochladen. Die Erfassungsnamen werden automatisch entsprechend der Quelleinheit geändert:

```
<#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

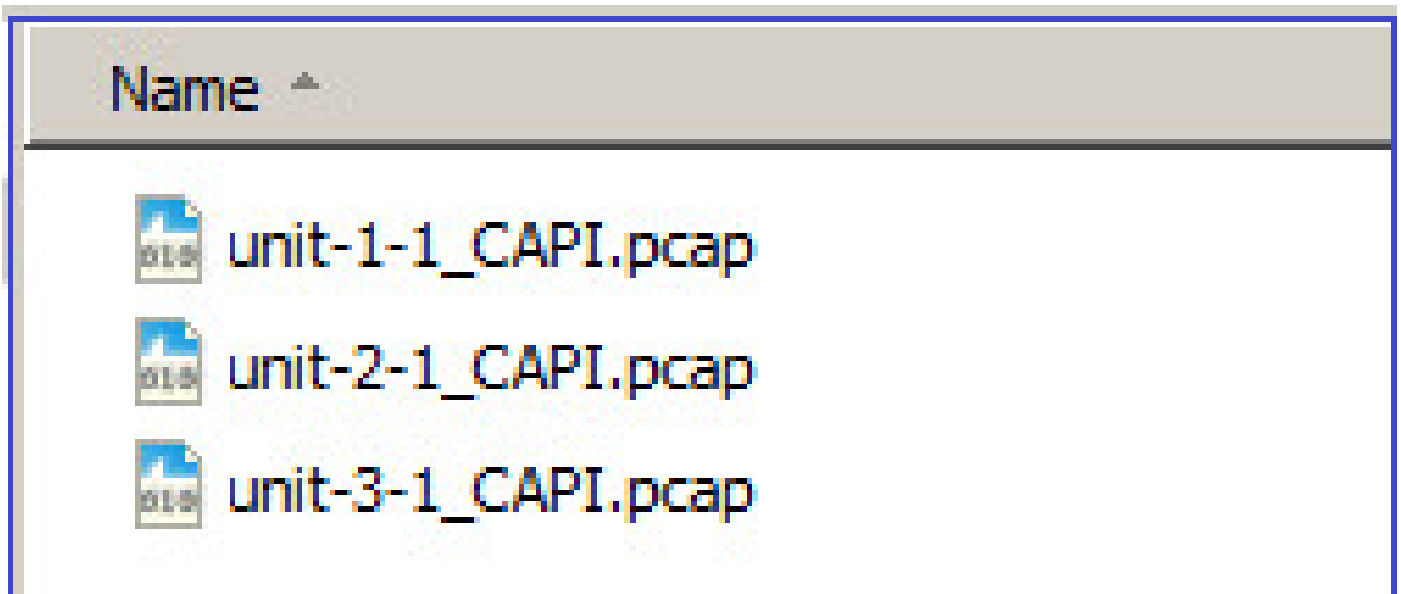
unit-2-1:\*\*\*\*\*

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 !

Die hochgeladenen pcap-Dateien:



Weg 2 - Holen Sie die Aufnahmen vom FMC

Diese Methode gilt nur für FTD. Zuerst kopieren Sie die Aufnahme auf die FTD-Diskette:

<#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

Kopieren Sie im Expertenmodus die Datei aus dem Verzeichnis /mnt/disk0/ in das Verzeichnis /ngfw/var/common/:

```
<#root>
```

```
>
```

```
expert
```

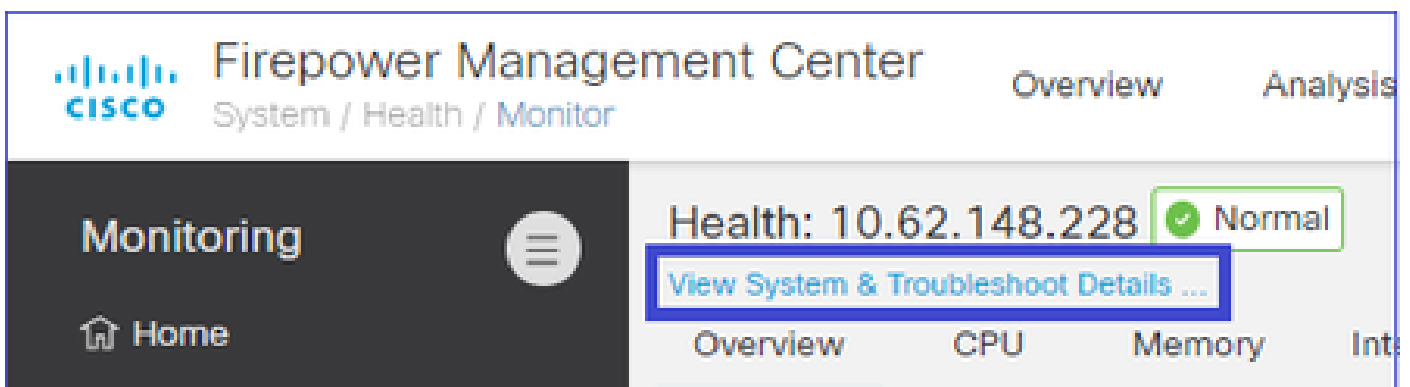
```
admin@firepower:~$
```

```
cd /mnt/disk0
```

```
admin@firepower:/mnt/disk0$
```

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

Navigieren Sie abschließend auf FMC zum Abschnitt System > Health > Monitor (System > Integrität > Monitor). Wählen Sie View System & Troubleshoot Details > Advanced Troubleshooting und holen Sie die Erfassungsdatei:



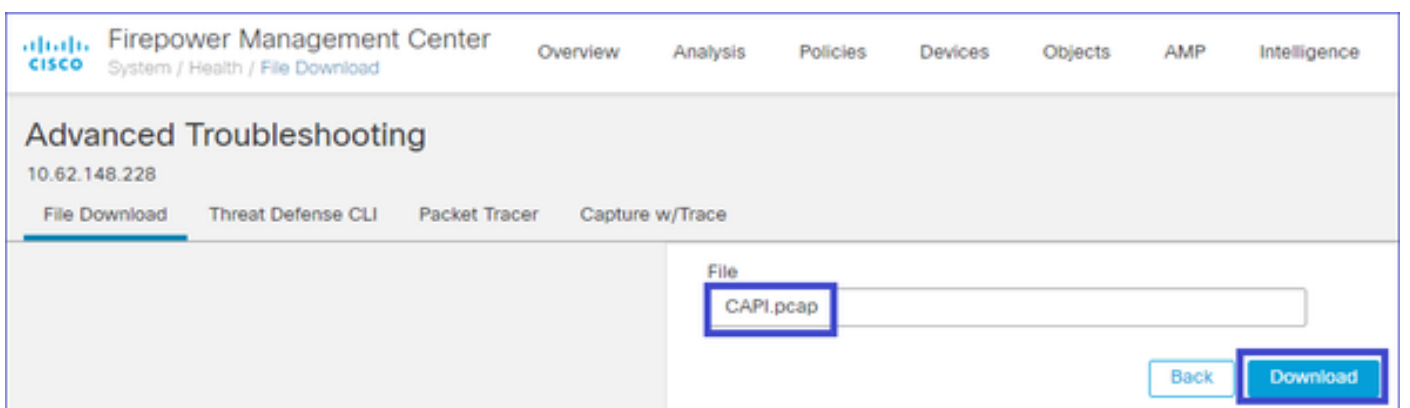
Firepower Management Center  
System / Health / Monitor

Monitoring

Health: 10.62.148.228 Normal

[View System & Troubleshoot Details ...](#)

Overview CPU Memory Int



Firepower Management Center  
System / Health / File Download

Advanced Troubleshooting

10.62.148.228

File Download Threat Defense CLI Packet Tracer Capture w/Trace

File

CAPI.pcap

Back Download

Erfassung löschen

Um eine Erfassung aus allen Cluster-Einheiten zu entfernen, verwenden Sie den folgenden Befehl:

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

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

### Ausgelagerte Ströme

Auf FP41xx/FP9300 können Flows entweder statisch (z. B. Fastpath-Regeln) oder dynamisch an HW Accelerator ausgelagert werden. Weitere Informationen zum Flow-Offload finden Sie in diesem Dokument:

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

Wird ein Datenfluss ausgelagert, passieren nur wenige Pakete die FTD-Datenebene. Der Rest übernimmt der Hardware-Beschleuniger (Smart NIC).

Aus Sicht der Erfassung bedeutet dies, dass Sie nicht alle Pakete sehen, die das Gerät durchlaufen, wenn Sie nur Aufzeichnungen auf FTD-Datenebene aktivieren. In diesem Fall müssen Sie auch FXOS-Erfassungen auf Chassis-Ebene aktivieren.

### Cluster Control Link (CCL)-Nachrichten

Wenn Sie eine Aufzeichnung auf der CCL durchführen, stellen Sie fest, dass die Cluster-Einheiten unterschiedliche Arten von Nachrichten austauschen. Interessant sind:

Protokolle	Beschreibung
UDP 49495	<p>Cluster-Heartbeats (Keepalives)</p> <ul style="list-style-type: none"><li>• L3-Broadcast (255.255.255.255)</li><li>• Diese Pakete werden von jeder Cluster-Einheit mit einem Drittel des Werts für die Zeit der Statusprüfung gesendet.</li><li>• Beachten Sie, dass nicht alle UDP 49495-Pakete, die in der Erfassung</li></ul>

	<p>erkannt werden, Heartbeats sind.</p> <ul style="list-style-type: none"> <li>Die Herzschläge enthalten eine Sequenznummer.</li> </ul>
UDP 4193	<p>Cluster Control Protocol - Datenpfadmeldungen</p> <ul style="list-style-type: none"> <li>Unicast</li> <li>Diese Pakete enthalten Informationen (Metadaten) über den Flow-Eigentümer, den Director, den Backup-Eigentümer usw. Beispiele: <ul style="list-style-type: none"> <li>Eine "Cluster-Add"-Nachricht wird vom Eigentümer an den Director gesendet, wenn ein neuer Fluss erstellt wird.</li> <li>Eine "Cluster-Löschnachricht" wird vom Besitzer an den Director gesendet, wenn ein Fluss beendet wird.</li> </ul> </li> </ul>
Datenpakete	<p>Datenpakete, die zu den verschiedenen Datenverkehrsflüssen gehören, die den Cluster durchlaufen</p>

### Cluster-Heartbeat

The image shows a network traffic capture analysis. At the top, there are four entries for UDP packets with the following details:

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

The detailed view for Frame 314 shows:

- Ethernet II, Src: Dell\_00:01:8f (00:15:c5:00:01:8f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.222.1.1, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 49495, Dst Port: 49495
- Data (163 bytes): 010100fe00a300000000000000000000000000000000001e008b0000000747524f5550310000...

The hex dump of the data shows the following sequence:

```

0000 ff ff ff ff ff 00 15 c5 00 01 8f 08 00 45 00 .....E.
0010 00 bf a8 1f 00 00 ff 11 51 2f c0 de 01 01 ff ff .....Q/.....
0020 ff ff c1 57 c1 57 00 ab 79 01 01 01 00 fe 00 a3 ...W.W. y.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e .....
0040 00 8b 00 00 00 07 47 52 4f 55 50 31 00 00 01 00 .....GR
0050 09 75 6e 69 74 2d 31 2d 31 00 00 02 00 09 75 6e ..unit-1-
0060 69 74 2d 31 2d 31 00 00 03 00 01 00 00 04 00 01 ..it-1-1-
0070 00 00 05 00 04 00 00 00 04 00 06 00 04 00 00 00 .....
0080 09 00 07 00 04 00 00 3a 98 00 08 00 0c 00 00 00 .....:
0090 00 c0 de 01 01 ff ff 00 00 00 09 00 02 01 1b 00 .....
00a0 0a 00 04 00 00 4e 9f 00 0b 00 0a 00 00 00 01 00 ....N.....
00b0 00 01 00 01 00 00 0c 00 08 00 00 00 00 00 00 00 .....
00c0 01 00 0d 00 08 00 00 00 00 00 00 00 00 00 00 00 .....

```

A red callout box points to the value '01 1b' in the hex dump at offset 0090, labeling it as the 'Heartbeat sequence number'.

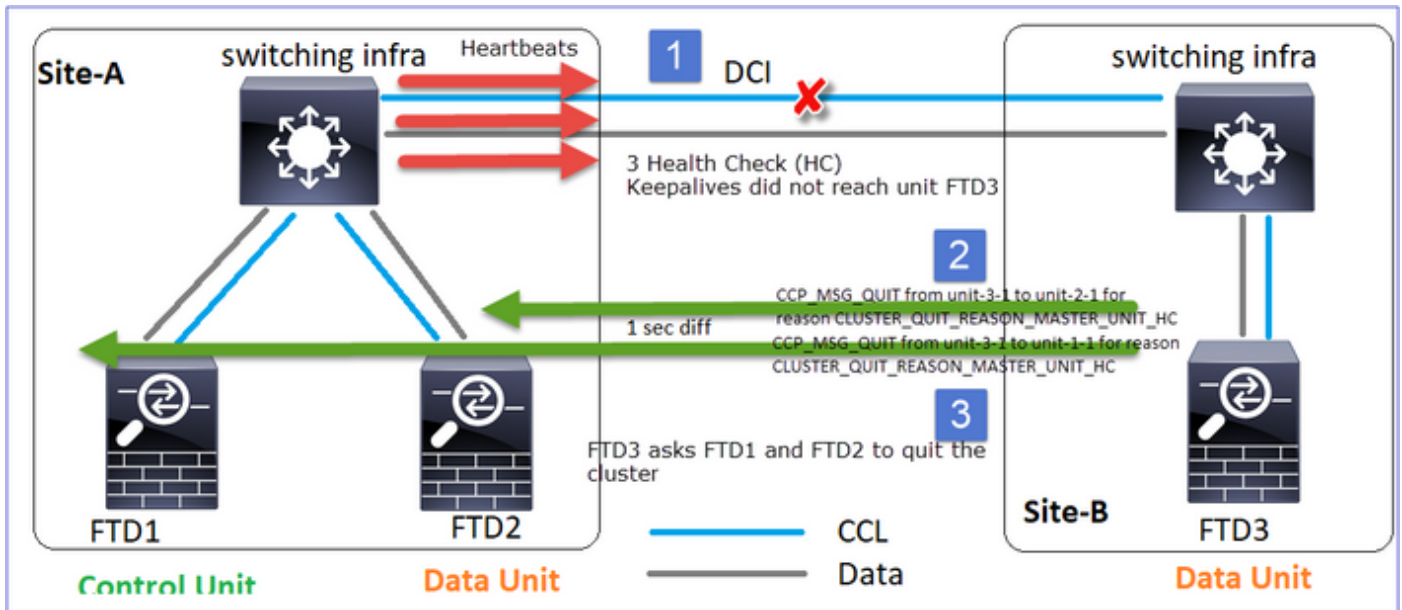
### Cluster Control Point (CCP)-Nachrichten

Zusätzlich zu den Heartbeat-Nachrichten gibt es eine Reihe von Cluster-Steuernachrichten, die in bestimmten Szenarien über die CCL ausgetauscht werden. Einige davon sind Unicast-Nachrichten, während andere Broadcasts sind.

## CLUSTER\_QUIT\_REASON\_PRIMARY\_UNIT\_HC

Wenn eine Einheit drei aufeinander folgende Heartbeat-Nachrichten vom Steuerungsknoten verliert, generiert sie eine CLUSTER\_QUIT\_REASON\_PRIMARY\_UNIT\_HC-Nachricht über die CCL. Diese Nachricht:

- Ist ein Unicast.
- Es wird in einem Intervall von 1 Sekunde an jede Einheit gesendet.
- Wenn ein Gerät diese Nachricht empfängt, beendet es den Cluster (DISABLED) und schließt sich erneut an.

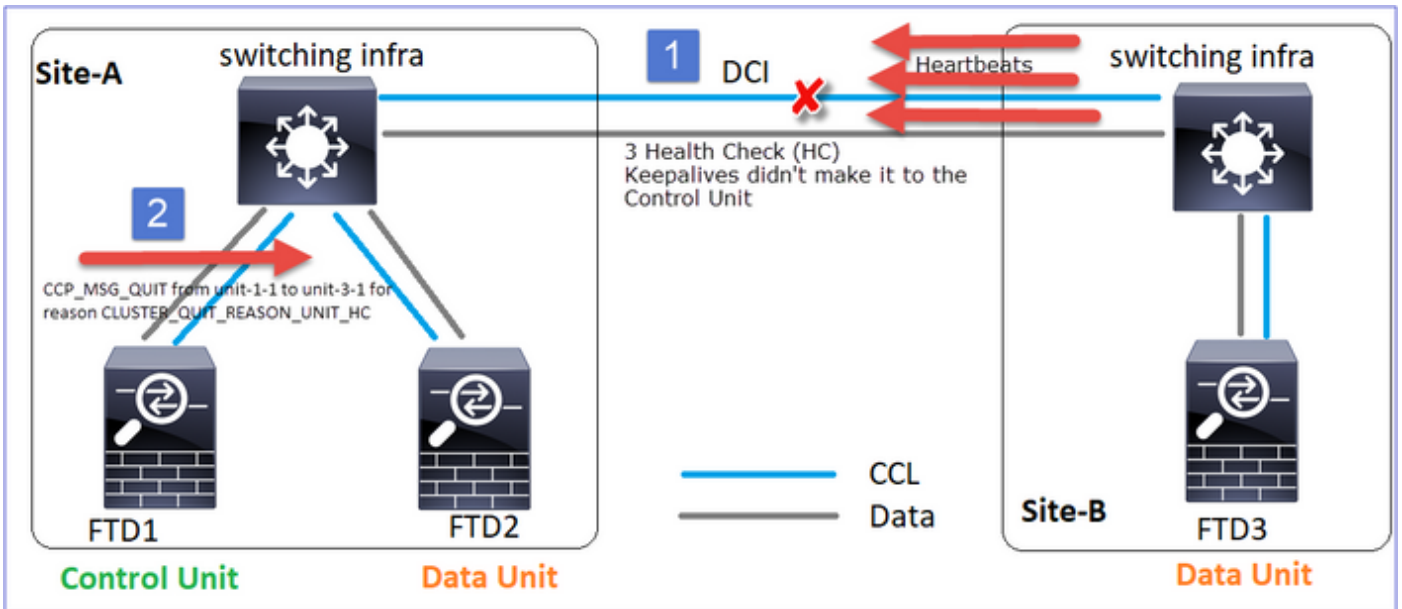


Frage: Wozu dient CLUSTER\_QUIT\_REASON\_PRIMARY\_UNIT\_HC?

A. Aus der Sicht von Einheit-3-1 (Standort-B) wird die Verbindung zu Einheit-1-1 und Einheit-2-1 von Standort A getrennt, sodass sie so schnell wie möglich aus der Mitgliederliste entfernt werden muss. Andernfalls kann es zu Paketverlusten kommen, wenn Einheit-2-1 noch in der Mitgliederliste enthalten ist und Einheit-2-1 zufällig Direktor einer Verbindung ist. Die Datenflussabfrage zu Einheit-2-1 schlägt fehl.

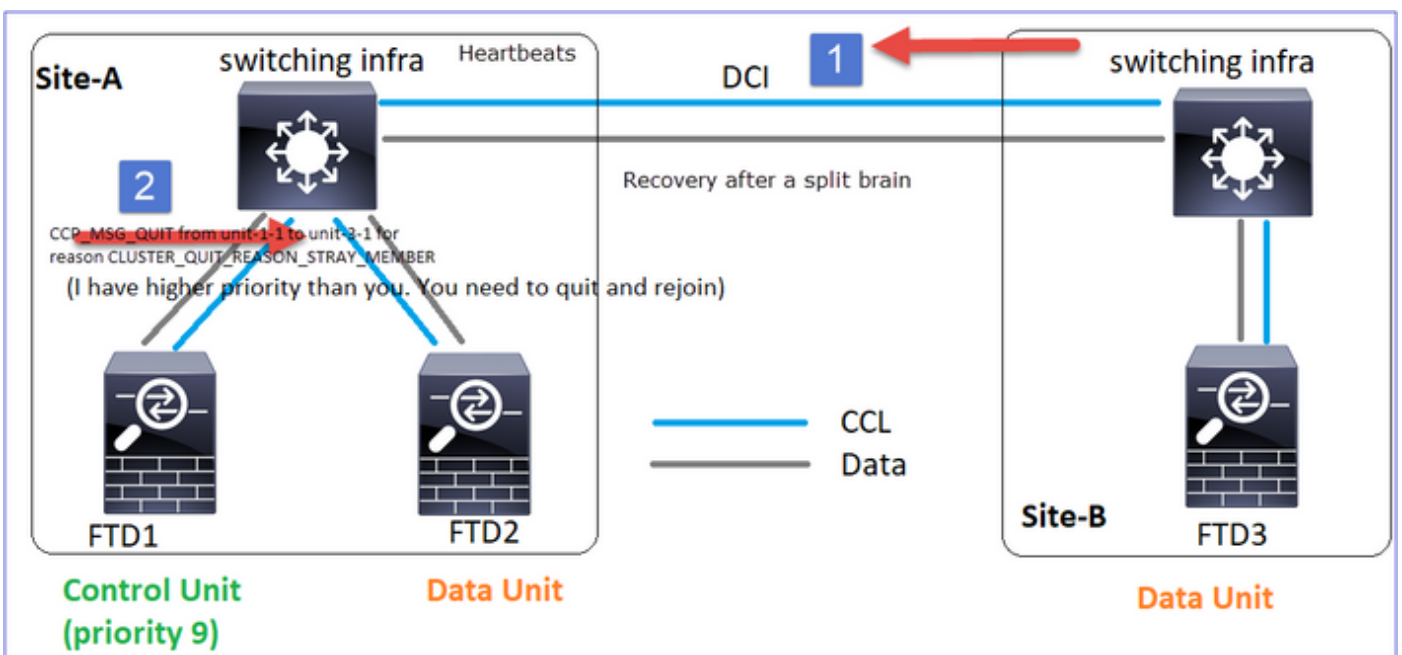
## CLUSTER\_QUIT\_REASON\_UNIT\_HC

Wenn der Steuerungsknoten drei aufeinander folgende Heartbeat-Nachrichten von einem Datenknoten verliert, sendet er die CLUSTER\_QUIT\_REASON\_UNIT\_HC-Nachricht über die CCL. Diese Nachricht ist Unicast.



### CLUSTER\_QUIT\_REASON\_STRAY\_MEMBER

Wenn eine Split-Partition wieder mit einer Peer-Partition verbunden wird, wird der neue Datenknoten von der dominanten Steuereinheit als Streuglied behandelt und erhält eine CCP-Abbruchmeldung mit dem Grund CLUSTER\_QUIT\_REASON\_STRAY\_MEMBER.



### CLUSTER\_QUIT\_MEMBER\_DROPOUT

Eine Broadcast-Nachricht, die von einem Datenknoten generiert und als Broadcast gesendet wird. Sobald ein Gerät diese Meldung erhält, wechselt es in den Status DISABLED (Deaktiviert). Darüber hinaus ist das automatische erneuten Beitreten kein Startpunkt:

<#root>

firepower#

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

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

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

Der Cluster-Verlauf zeigt Folgendes an:

```
<#root>
```

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

## Cluster-Gesundheitscheck-Mechanismus

### Wichtigste Punkte

- Jede Cluster-Einheit sendet alle 1/3 des Werts für die Haltezeit der Integritätsprüfung einen Heartbeat an alle anderen Einheiten (Broadcast 255.255.255.255) und verwendet den UDP-Port 49495 als Transport über den CCL.
- Jede Cluster-Einheit verfolgt unabhängig jede andere Einheit mit einem Abfragezeitgeber und einem Abfragezählerwert.
- Wenn eine Cluster-Einheit innerhalb eines Heartbeat-Intervalls kein Paket (Heartbeat- oder Datenpaket) von einer Cluster-Peer-Einheit empfängt, erhöht sie den Wert für die Anzahl der Abfragen.
- Wenn der Wert für die Abfrageanzahl für eine Cluster-Peer-Einheit auf 3 gesetzt wird, gilt der Peer als ausgefallen.
- Bei jedem Empfang eines Herzschlages wird dessen Sequenznummer überprüft, und bei einem Unterschied zum zuvor empfangenen Herzschlag von 1 erhöht sich der Herzschlagfallzähler entsprechend.
- Wenn der Zähler für die Abrufanzahl für einen Cluster-Peer nicht 0 ist und ein Paket vom Peer empfangen wird, wird der Zähler auf den Wert 0 zurückgesetzt.

Verwenden Sie diesen Befehl, um die Cluster-Zustandszähler zu überprüfen:

```
<#root>
```

```
firepower#
```

```
show cluster info health details
```

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

### Beschreibung der Hauptspalten

Spalte	Beschreibung
Einheit (ID)	Die ID des Remote-Cluster-Peers.
Herzschlag	Die Anzahl der Heartbeats, die vom Remote-Peer über den CCL empfangen wurden
Herzschlag sinkt	Die Anzahl der verpassten Heartbeats. Dieser Leistungsindikator wird auf der Grundlage der empfangenen Heartbeat-Sequenznummer berechnet.
durchschnittliche Lücke	Das durchschnittliche Zeitintervall der empfangenen Heartbeats.
Umfrageanzahl	Wenn dieser Zähler den Wert 3 annimmt, wird die Einheit aus dem Cluster entfernt. Das Intervall für die Abfrage der Abfrage entspricht dem Intervall für den Heartbeat, wird jedoch unabhängig ausgeführt.

Verwenden Sie den folgenden Befehl, um die Zähler zurückzusetzen:

```
<#root>
```

```
firepower#
```

```
clear cluster info health details
```

Frage: Wie kann ich die Herzschlagfrequenz überprüfen?

A. Durchschnittliche Lücke prüfen:

```
<#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|
```

Frage: Wie können Sie die Haltezeit des Clusters in FTD ändern?

A. FlexConfig verwenden

F. Wer wird der Kontrollknoten nach einem Split-Brain?

A. Die Einheit mit der höchsten Priorität (niedrigste Zahl):

```
<#root>
```

```
firepower#
```

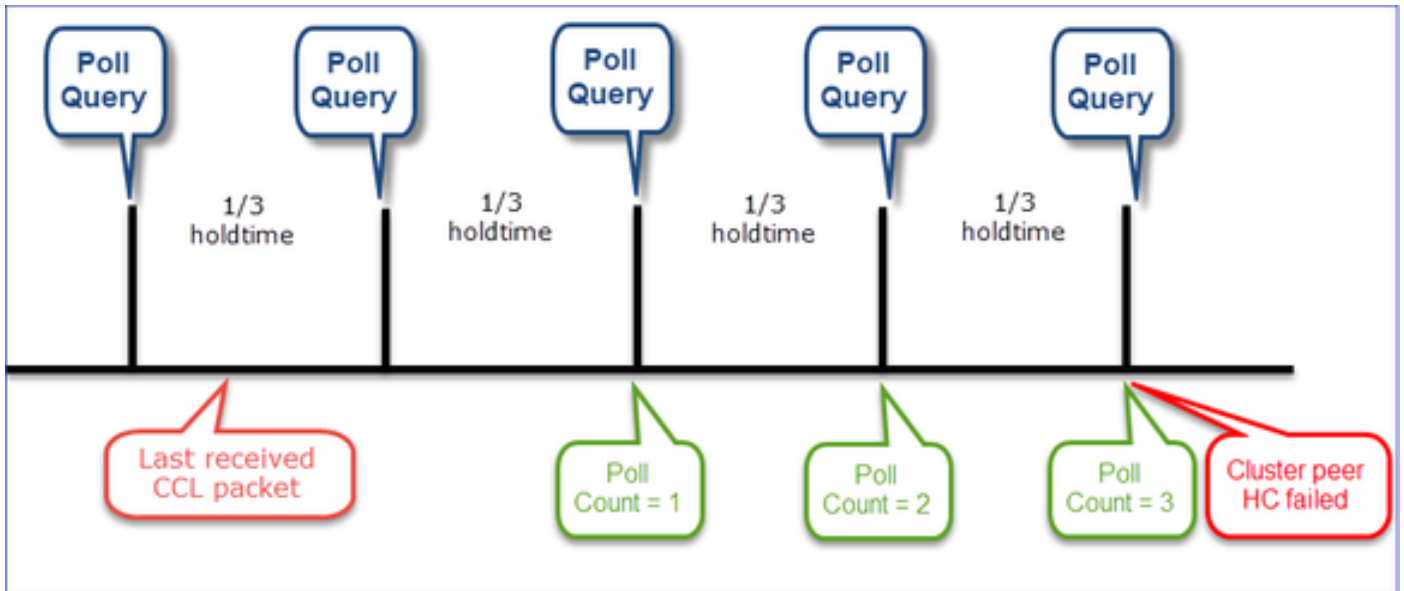
```
show run cluster | include priority
```

```
priority 9
```

Weitere Informationen finden Sie unter Szenario 1 des HC-Ausfalls.

Die Visualisierung des Cluster-HC-Mechanismus





Indikative Timer: Die Min- und Max-Werte hängen von der zuletzt empfangenen CCL-Paketeingabe ab.

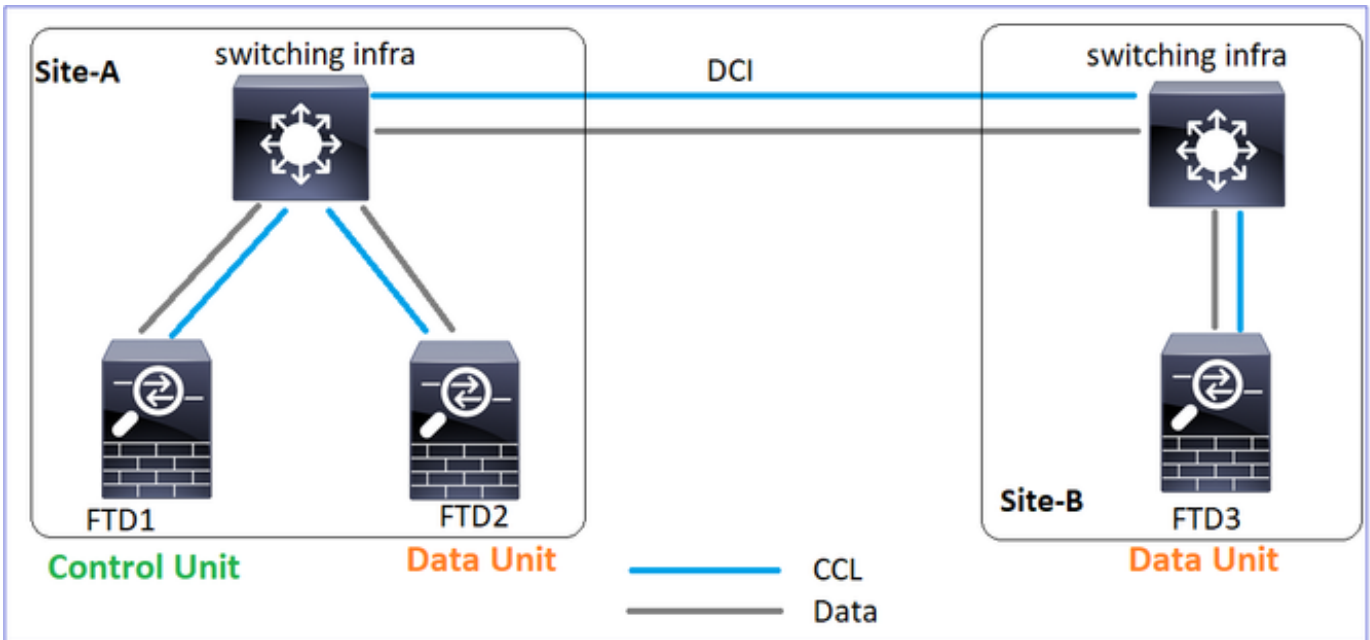
Haltezeit	Abfrageüberprüfung abfragen (Häufigkeit)	Min. Erkennungszeit	Max. Erkennungszeit
3 Sek. (Standard)	~ 1 Sekunde	~3,01 Sek.	~3,99 Sek.
4 Sekunden	~ 1,33 Sek.	~4,01 Sek.	~5,32 Sek.
5 s	~1,66 Sek.	~5,01 s	~6,65 s
6 Sekunden	~2 Sek.	~6,01 s	~7,99 Sek.
7 s	~2,33 Sek.	~7,01 s	~ 9,32 Sek.
8 Sekunden	~2,66 Sek.	~8,01 s	~10,65 Sek.

## Cluster-HC-Fehlerszenarien

In diesem Abschnitt werden folgende Ziele verfolgt:

- Verschiedene Cluster-HC-Ausfallszenarien.
- Wie die verschiedenen Protokolle und Befehlsausgaben korreliert werden können.

Topologie



Cluster-Konfiguration

Einheit-1-1	Einheit-2-1
<pre> cluster group GROUP1 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           </pre>	<pre> cluster group GROUP1 key ***** local-unit unit-2-1 cluster-interface Port-channel48 ip 10.17.1.1 255.255.0.0 priority 17 health-check holdtime 3 health-check data-interface auto-rejoin 3 5 2 health-check cluster-interface auto-rejoin unlimited 5 1 health-check system auto-rejoin 3 5 2 health-check monitor-interface debounce-time 500 site-id 1 enable           </pre>

Cluster-Status

Einheit-1-1	Einheit-2-1
<#root>	<#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

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

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.c500.028f  
Last join : 20:44:46 UTC Nov 1 2020  
Last leave: 20:44:38 UTC Nov 1 2020

Other members in the cluster:

Unit "unit-1-1" in state 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

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

Szenario 1

CCL-Kommunikationsverlust in beide Richtungen über ca. 4 Sekunden.

Vor dem Ausfall

FTD1	FTD2	FTD3
Standort A	Standort A	Standort B
Kontrollknoten	Datenknoten	Datenknoten

Nach der Wiederherstellung (keine Änderungen in den Rollen der Einheit)

FTD1	FTD2	FTD3
Standort A	Standort A	Standort B
Kontrollknoten	Datenknoten	Datenknoten

Analyse

Der Fehler (die CCL-Kommunikation ging verloren).

Konsolenmeldung auf Datenebene auf Einheit 3-1:

<#root>

firepower#

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

Cluster unit unit-3-1 transitioned from 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.

Cluster-Ablaufverfolgungsprotokolle von Einheit 1-1:

<#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

[DEBUG]Send CCP message to all: CCP\_MSG\_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER\_QUIT\_MEMBER\_DR

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

[DEBUG]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

Einheit-1-1	Einheit-2-1
<pre>&lt;#root&gt; 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</pre>	<pre>&lt;#root&gt; 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.c500.028f       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.c500.018f</pre>

Last join : 20:44:45 UTC Nov 1 2020  
 Last leave: 20:44:38 UTC Nov 1 2020

Last join : 20:25:36 UTC  
 Last leave: 20:25:28 UTC

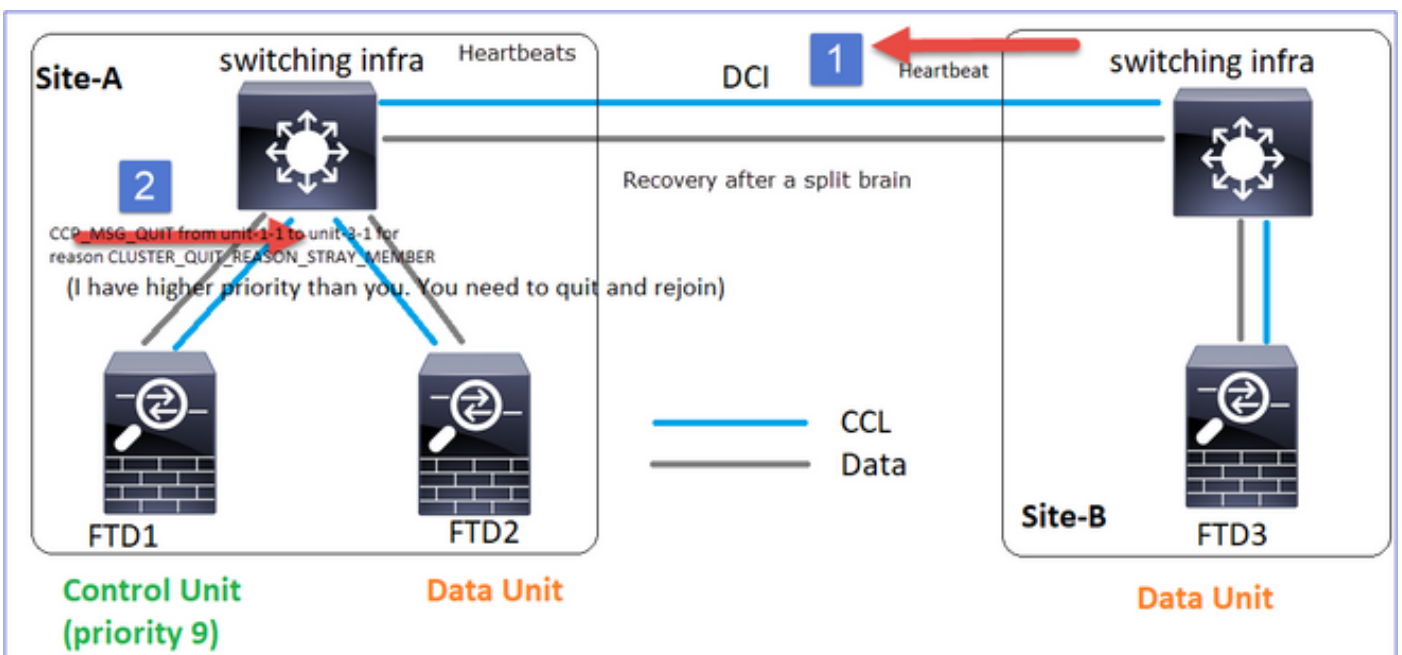
### Cluster-Verlauf

Einheit-1-1	Einheit-2-1	Einheit-3-1
Keine Veranstaltungen	Keine Veranstaltungen	<pre>&lt;#root&gt; 09:38:16 UTC Nov 2 2020 SECONDARY                                PRIMARY_POST_CONFIG  Pri 09:38:17 UTC Nov 2 2020 PRIMARY_POST_CONFIG  Primary              Primary</pre>

### Wiederherstellung der CCL-Kommunikation

Unit-1-1 erkennt den aktuellen Steuerungsknoten und sendet, da Unit-1-1 eine höhere Priorität hat, eine CLUSTER\_QUIT\_REASON\_STRAY\_MEMBER-Nachricht an Unit-3-1, um einen neuen Wahlvorgang auszulösen. Am Ende wird Einheit-3-1 wieder als Datenknoten verbunden.

Wenn eine Split-Partition erneut mit einer Peer-Partition verbunden wird, wird der Datenknoten vom dominanten Kontrollknoten als streunendes Mitglied behandelt und erhält eine CCP-Abbruchmeldung mit dem Grund CLUSTER\_QUIT\_REASON\_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 Einheiten (Einheit-1-1 und Einheit-3-1) zeigen in ihren Cluster-Protokollen:

```
<#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
```

Es werden auch Syslog-Meldungen für das Split-Brain generiert:

```
<#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 .
```

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

Cluster-Verlauf

Einheit-1-1	Einheit-2-1	Einheit-3-1
-------------	-------------	-------------

Keine Veranstaltungen	Keine Veranstaltungen	<pre> &lt;#root&gt; 09:47:33 UTC Nov 2 2020  Primary DISABLED          Detected a splitted cluster  09:47:38 UTC Nov 2 2020 DISABLED          ELECTION          Enabled from C 09:47:38 UTC Nov 2 2020 ELECTION          SECONDARY_COLD          Received o 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          SECON 09:48:29 UTC Nov 2 2020 SECONDARY_CONFIG          SECONDARY_FILESYS          Config 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 </pre>
--------------------------	--------------------------	--

## Szenario 2

CCL-Kommunikationsverlust für ca. 3-4 Sekunden in beide Richtungen.

Vor dem Ausfall

FTD1	FTD2	FTD3
Standort A	Standort A	Standort B
Kontrollknoten	Datenknoten	Datenknoten

Nach der Wiederherstellung (keine Änderungen in den Rollen der Einheit)

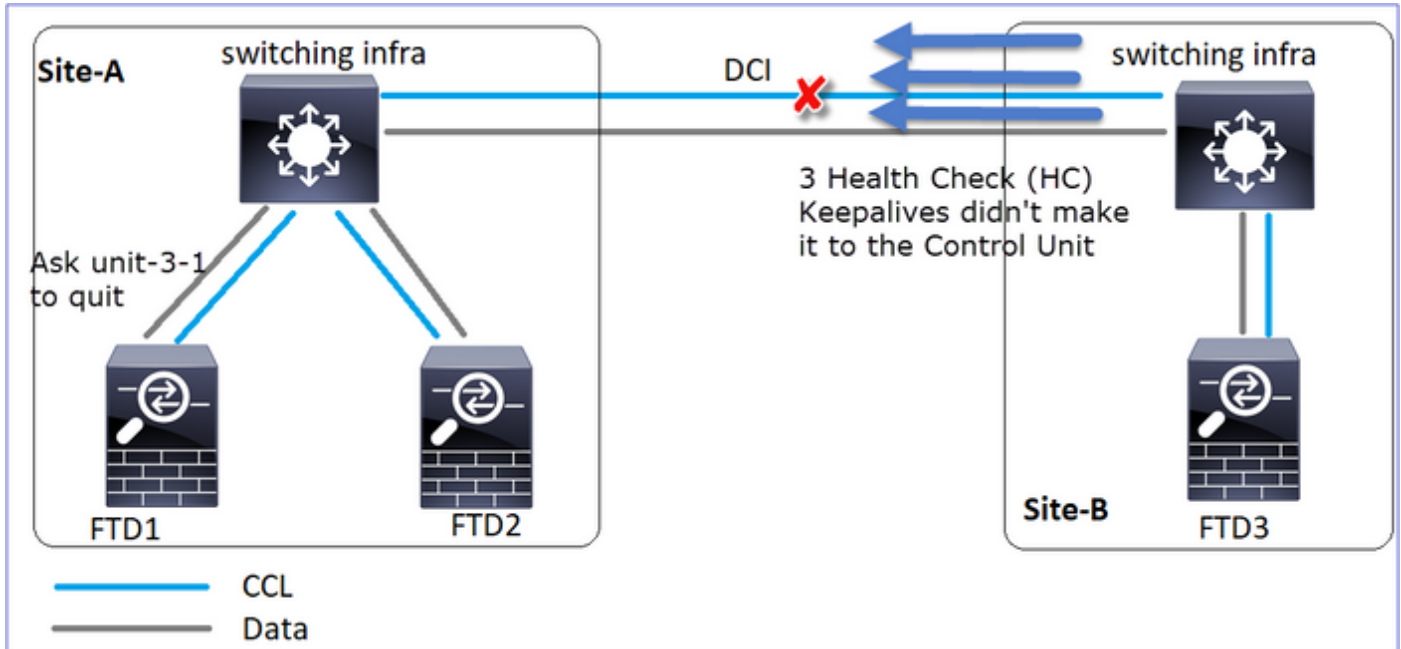
FTD1	FTD2	FTD3
Standort A	Standort A	Standort B



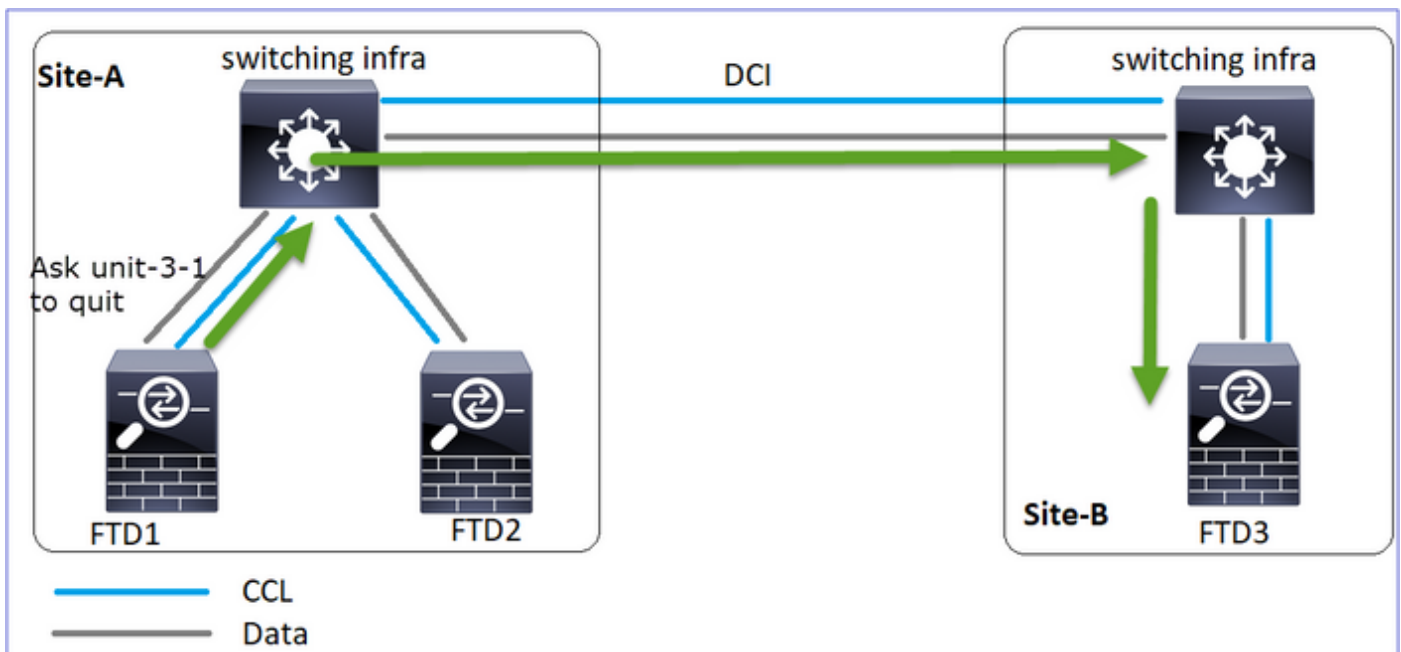
Kontrollknoten	Datenknoten	Datenknoten
----------------	-------------	-------------

### Analyse

Veranstaltung 1: Der Steuerknoten verliert 3 HCs von der Einheit 3-1 und sendet eine Nachricht an die Einheit 3-1, um den Cluster zu verlassen.



Veranstaltung 2: Die CCL wurde sehr schnell wiederhergestellt, und die CLUSTER\_QUIT\_REASON\_STRAY\_MEMBER-Nachricht vom Steuerungsknoten gelangte zur Remote-Seite. Unit-3-1 wechselt direkt in den DISABLED-Modus, es gibt kein Split-Brain



Auf Gerät-1-1 (Steuerung) sehen Sie:

```
<#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
```

Auf Einheit-3-1 (Datenknoten) wird Folgendes angezeigt:

```
<#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
```

Die Cluster-Einheit 3-1 wechselte in den Status DISABLED (Deaktiviert) und tritt nach der Wiederherstellung der CCL-Kommunikation wieder als Datenknoten bei:

```
<#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
```

### Szenario 3

CCL-Kommunikationsverlust für ca. 3-4 Sekunden in beide Richtungen.

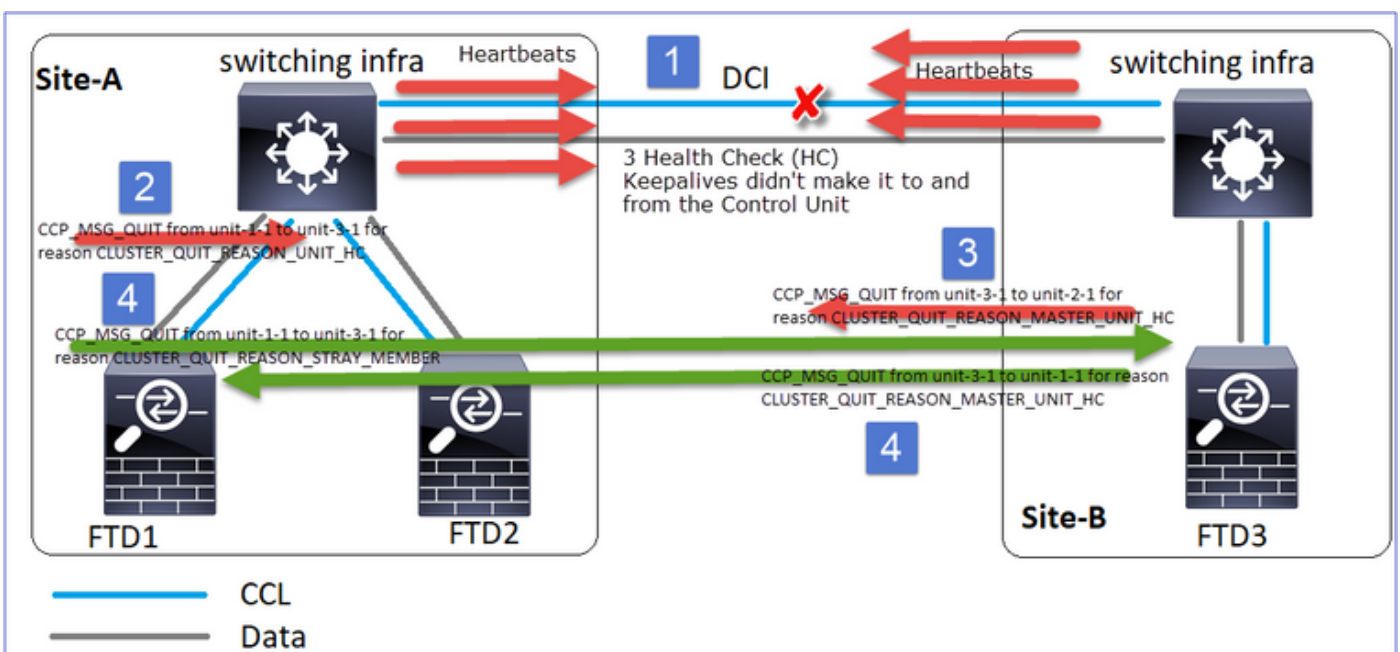
Vor dem Scheitern.

FTD1	FTD2	FTD3
Standort A	Standort A	Standort B
Kontrollknoten	Datenknoten	Datenknoten

Nach der Wiederherstellung (der Kontrollknoten wurde geändert).

FTD1	FTD2	FTD3
Standort A	Standort A	Standort B
Datenknoten	Kontrollknoten	Datenknoten

### Analyse



1. CCL erlischt.
2. Unit-1-1 erhält keine 3 HC-Nachrichten von Unit-3-1 und sendet eine QUIT-Nachricht an Unit-3-1. Diese Nachricht erreicht nie Unit-3-1.

3. Einheit-3-1 sendet eine QUIT-Nachricht an Einheit-2-1. Diese Nachricht erreicht Einheit-2-1 nie.

Wiederherstellung mit CCL.

4. Unit-1-1 erkennt, dass Unit-3-1 sich selbst als Kontrollknoten gemeldet hat und sendet die Nachricht QUIT\_REASON\_STRAY\_MEMBER an Unit-3-1. Sobald Unit-3-1 die Nachricht erhält, wechselt sie in den Status DISABLED. Gleichzeitig sendet Unit-3-1 eine QUIT\_REASON\_PRIMARY\_UNIT\_HC-Nachricht an Unit-1-1 und fordert sie zum Beenden auf. Sobald Gerät 1-1 diese Nachricht erhält, wechselt sie in den Status DISABLED (Deaktiviert).

Cluster-Verlauf

Einheit-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

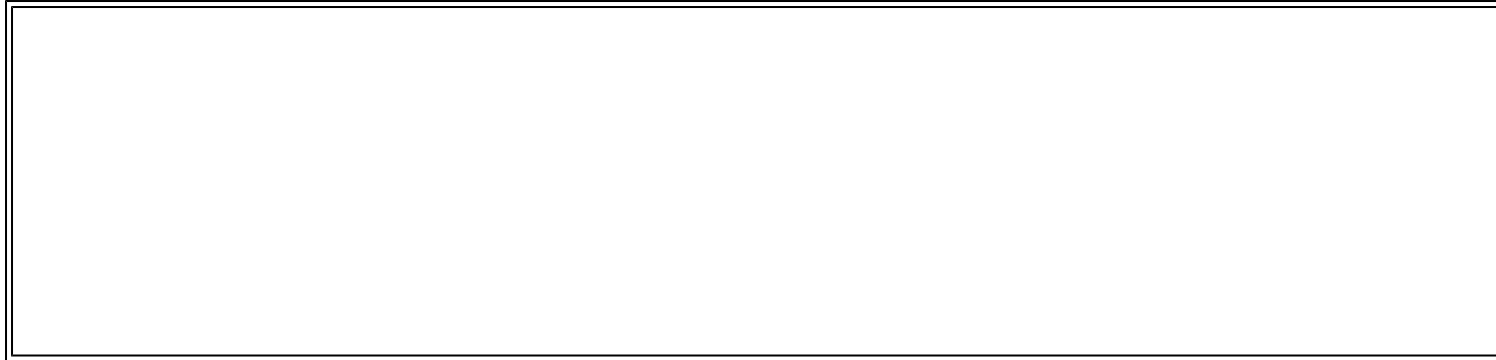
SECONDARY\_FILESYS SECONDARY\_BULK\_SYNC Client progression done

19:54:37 UTC Nov 2 2020

SECONDARY\_BULK\_SYNC

SECONDARY

Client progression done



### Szenario 4

CCL-Kommunikationsverlust für ~3-4 Sekunden

Vor dem Ausfall

FTD1	FTD2	FTD3
Standort A	Standort A	Standort B
Kontrollknoten	Datenknoten	Datenknoten

Nach der Wiederherstellung (der Kontrollknoten wechselte die Standorte)

FTD1	FTD2	FTD3
Standort A	Standort A	Standort B
Datenknoten	Datenknoten	Kontrollknoten

### Analyse

#### Der Fehler

```
firepower#  
firepower#  
firepower#  
firepower#  
firepower#  
firepower#  
firepower# Cluster disable is performing cleanup..done.  
All data interfaces have been shutdown due to clustering b  
ing disabled. To recover either enable clustering or remo  
ve cluster group configuration.  
Cluster unit unit-1-1 transitioned from [redacted] to DISABLE  
d  
firepower#  
firepower#  
firepower#  
firepower#  
firepower#  
firepower#  
firepower# Cluster disable is performing cleanup..done.  
All data interfaces have been shutdown due to clustering b  
ing disabled. To recover either enable clustering or remo  
ve cluster group configuration.  
Cluster unit unit-2-1 transitioned from [redacted] to DISABLE  
d  
The 3DES/AES algorithms require a Encryption 3DES/AES sec  
uration key.  
firepower#  
firepower#  
firepower#  
firepower#  
firepower#  
firepower#  
firepower# WARNING: dynamic routing is not supported on management interface wh  
a cluster interface-mode is 'spanned'. If dynamic routing is config  
red on any management interface, please remove it.  
Cluster unit unit-3-1 transitioned from [redacted]
```

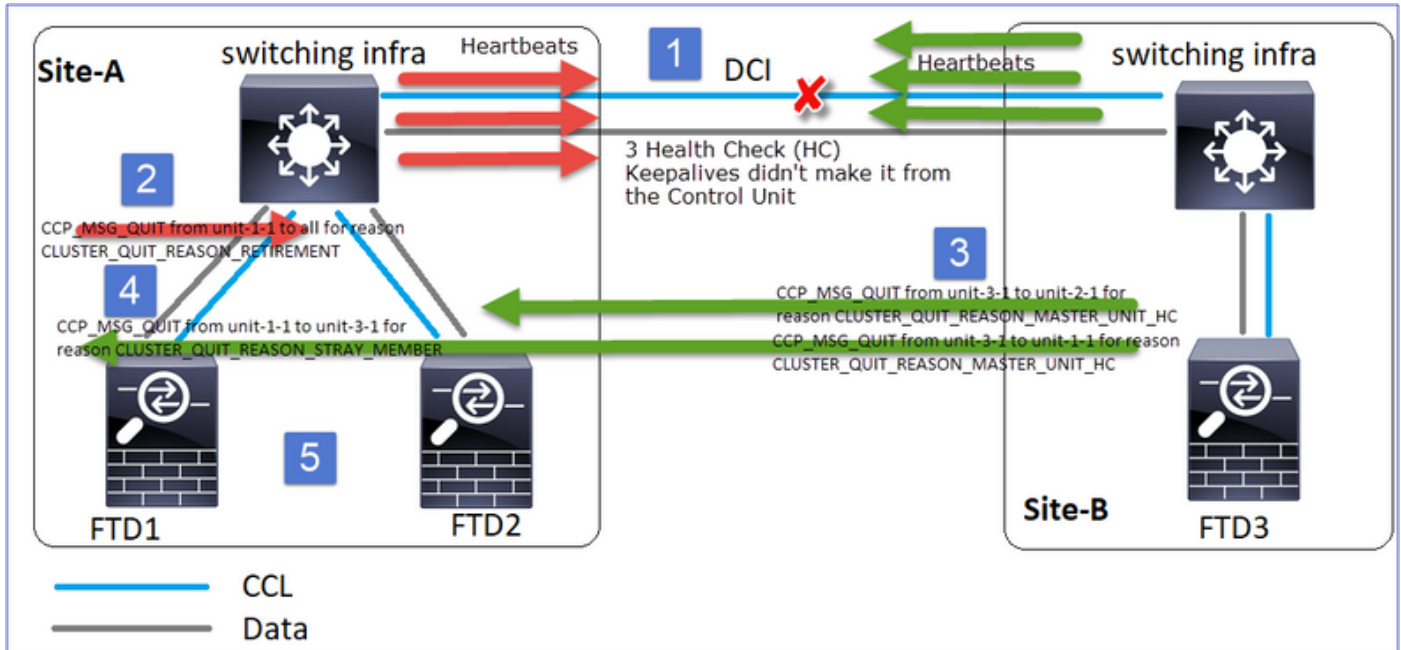
Ein anderer Geschmack desselben Versagens. In diesem Fall erhielt die Einheit-1-1 auch keine 3 HC-Nachrichten von der Einheit-3-1, und nachdem sie einen neuen Keepalive erhalten hatte, versuchte sie, die Einheit-3-1 mithilfe einer STRAY-Nachricht auszustoßen, aber die Nachricht

schaffe es nie an die Einheit-3-1:

```

firepower#
firepower#
firepower#
firepower#
firepower# Asking slave unit unit-3-1 to quit because it
failed unit health-check.
Forcing stray member unit-3-1 to leave the cluster
Forcing stray member unit-3-1 to leave the cluster
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering
being disabled. To recover either enable clustering or re
move cluster group configuration.
Cluster unit unit-1-1 transitioned from [redacted]
to DISABLED
firepower#
firepower#
firepower#
firepower#
firepower# Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering b
eing disabled. To recover either enable clustering or remo
ve cluster group configuration.
Cluster unit unit-2-1 transitioned from [redacted]
to DISABLED
The 3DES/AES algorithms require a Encryption-3DES-AES acti
vation key.
firepower#
firepower#
firepower#
firepower#
firepower# WARNING: dynamic routing is not supported on management interface
on cluster interface-mode is 'spanned'. If dynamic routing is conf
red on any management interface, please remove it.
Cluster unit unit-3-1 transitioned from [redacted]

```



1. Die CCL-Funktion bleibt einige Sekunden unidirektional. Unit-3-1 empfängt keine 3 HC-Nachrichten von Unit-1-1 und wird zu einem Kontrollknoten.
2. Unit-2-1 sendet eine CLUSTER\_QUIT\_REASON\_RETIREMENT-Nachricht (Broadcast).
3. Unit-3-1 sendet eine QUIT\_REASON\_PRIMARY\_UNIT\_HC-Nachricht an Unit-2-1. Unit-2-1 empfängt sie und beendet den Cluster.
4. Unit-3-1 sendet eine QUIT\_REASON\_PRIMARY\_UNIT\_HC-Nachricht an Unit-1-1. Unit-1-1 empfängt sie und beendet den Cluster. Wiederherstellung mit CCL.
5. Die Einheiten 1-1 und 2-1 treten dem Cluster wieder als Datenknoten bei.



Anmerkung: Wenn sich die CCL in Schritt 5 nicht erholt, wird am Standort A der FTD1 zum neuen Kontrollknoten, und nach der CCL-Wiederherstellung gewinnt sie die neue Wahl.

---

#### Syslog-Meldungen auf Gerät 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-Ablaufverfolgungsprotokolle auf Gerät 1-1:

```
<#root>
```

```
firepower#
```

```
show cluster info trace | include QUIT
```

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

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

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

## Syslog-Meldungen auf Gerät-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
```

## Cluster-Verlauf



Einheit-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

## Szenario 5

Vor dem Ausfall

FTD1	FTD2	FTD3
Standort A	Standort A	Standort B
Kontrollknoten	Datenknoten	Datenknoten



Nov 04 00:52:10.389 [DEBUG]Receive CCP message: CCP\_MSG\_QUIT from unit-3-1 for reason CLUSTER\_QUIT\_REASON  
 Nov 04 00:51:47.019 [DEBUG]Send CCP message to all: CCP\_MSG\_QUIT from unit-2-1 for reason CLUSTER\_QUIT\_REASON  
 Nov 04 00:51:46.999 [DEBUG]

Receive CCP message: CCP\_MSG\_QUIT from unit-3-1 to unit-2-1 for reason CLUSTER\_QUIT\_REASON\_PRIMARY\_UNIT

Nov 04 00:51:45.389 [DEBUG]Receive CCP message: CCP\_MSG\_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER\_QUIT\_REASON\_SECONDARY\_UNIT

### Cluster-Verlauf

Einheit-1-1	Einheit-2-1
Keine Veranstaltungen	<pre> &lt;#root&gt; 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 m 00:51:54 UTC Nov 4 2020 SECONDARY_COLD          SECONDARY_APP_SYNC          Client progression don 00:52:42 UTC Nov 4 2020 SECONDARY_APP_SYNC          SECONDARY_CONFIG          SECONDARY application sync done 00:52:54 UTC Nov 4 2020 SECONDARY_CONFIG          SECONDARY_FILESYS          Configuration replicat 00:52:55 UTC Nov 4 2020 SECONDARY_FILESYS          SECONDARY_BULK_SYNC          Client progression don 00:53:19 UTC Nov 4 2020 SECONDARY_BULK_SYNC  SECONDARY Client progression done           </pre>

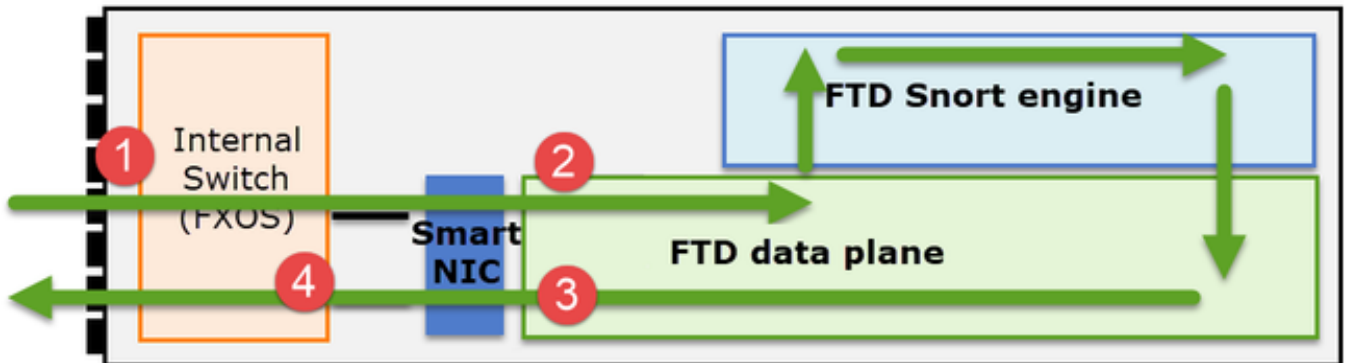
### Verbindungsaufbau der Cluster-Datenebene

## NGFW-Erfassungspunkte

Die NGFW bietet Erfassungsfunktionen in folgenden Punkten:

- Gehäuseinterner Switch (FXOS)
- FTD-Datenebenen-Engine
- FTD Snort-Engine

Bei der Fehlerbehebung von Datenpfad-Problemen in einem Cluster werden in den meisten Fällen die FXOS- und FTD-Datenebenen-Engine-Erfassungspunkte verwendet.



1. FXOS-Eingangserfassung an der physischen Schnittstelle
2. FTD-Eingangserfassung in Datenebenen-Engine
3. FTD-Ausgangserfassung in Datenebenen-Engine
4. FXOS-Eingangserfassung an Backplane-Schnittstelle

Weitere Informationen zu NGFW-Aufzeichnungen finden Sie in diesem Dokument:

### Grundlagen der Cluster Unit Flow-Rollen

Verbindungen können auf verschiedene Weise über einen Cluster hergestellt werden, wobei Faktoren wie die folgenden ausschlaggebend sind:

- Art des Datenverkehrs (TCP, UDP usw.)
- Auf dem benachbarten Switch konfigurierter Lastenausgleichsalgorithmus
- Auf der Firewall konfigurierte Funktionen
- Netzwerkbedingungen (z. B. IP-Fragmentierung, Netzwerkverzögerungen usw.)

Flow-Rolle	Beschreibung	Flag(s)
Besitzer	In der Regel wird das Gerät, das die Verbindung ursprünglich erhält,	UIO
Direktor	Die Einheit, die Ownerlookup-Anfragen von Weiterleitungen	Y

	verarbeitet.	
Sicherungseigentümer	Solange der Director nicht dieselbe Einheit wie der Eigentümer ist, ist er auch der Backup-Eigentümer. Wenn sich der Besitzer selbst als Director entscheidet, wird ein separater Backup-Besitzer ausgewählt.	Y (wenn der Director auch Sicherungseigentümer ist) y (wenn der Director nicht der Sicherungseigentümer ist)
Weiterleitung	Eine Einheit, die Pakete an den Besitzer weiterleitet.	z
Fragment-Besitzer	Die Einheit, die den fragmentierten Datenverkehr verarbeitet	-
Chassis-Backup	Wenn in einem Interchassis-Cluster die Director/Backup- und Owner-Flows den Einheiten desselben Chassis gehören, wird eine Einheit in einem der anderen Chassis zu einem sekundären Backup/Director.  Diese Rolle ist spezifisch für Interchassis-Cluster der FirePOWER Serie 9300 mit mehr als einem Blade.	w

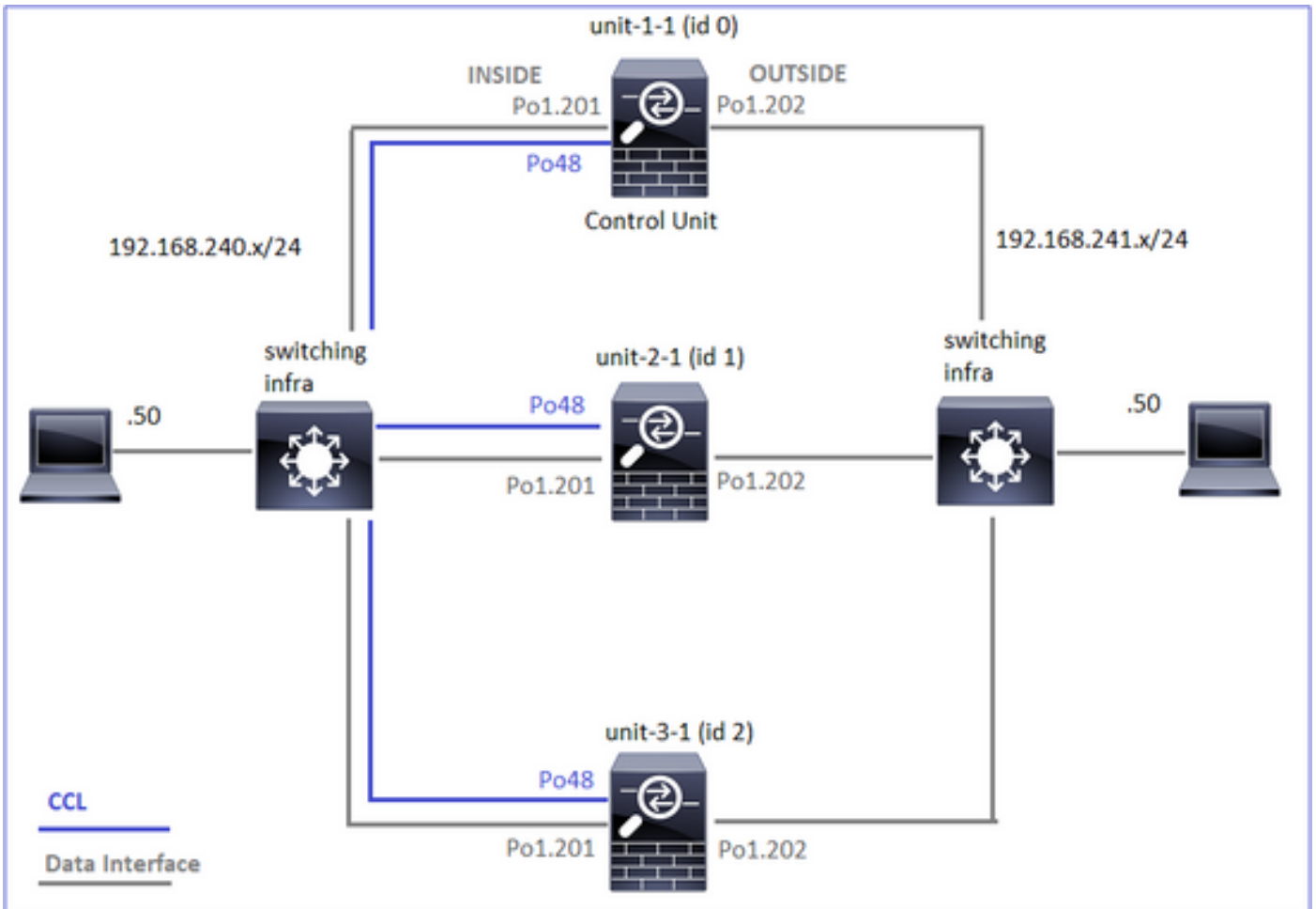
- Weitere Informationen finden Sie im entsprechenden Abschnitt im Konfigurationshandbuch (siehe Links im Abschnitt "Weitere Informationen").
- In bestimmten Szenarien (siehe Abschnitt mit Fallstudien) werden einige Kennzeichen nicht immer angezeigt.

## Erstellung von Cluster-Verbindungen - Anwenderberichte

Im nächsten Abschnitt werden verschiedene Fallstudien behandelt, die einige Möglichkeiten aufzeigen, wie eine Verbindung über einen Cluster hergestellt werden kann. Die Ziele sind:

- Machen Sie sich mit den verschiedenen Rollen der Einheiten vertraut.
- Demonstrieren Sie, wie die verschiedenen Befehlsausgaben korreliert werden können.

## Topologie



Cluster-Einheiten und -IDs:

Einheit-1-1	Einheit-2-1
<pre> &lt;#root&gt; 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   CCL MAC     : 0015.c500.018f   Last join   : 02:24:43 UTC Nov 27 2020   Last leave  : N/A           </pre>	<pre> &lt;#root&gt;    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           </pre>

## Cluster-Erfassung aktiviert:

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



Anmerkung: Diese Tests wurden in einer Laborumgebung mit minimalem Datenverkehr durch den Cluster ausgeführt. Versuchen Sie, in der Produktion möglichst spezifische Erfassungsfiler (z. B. Zielport und wenn möglich Quellport) zu verwenden, um das "Rauschen" in den Erfassungen zu minimieren.

## Fallstudie 1. Symmetrischer Datenverkehr (Eigentümer ist auch der Leiter)

Beobachtung 1. Die Erfassung von "reinject-hide" zeigt Pakete nur an Einheit 1-1. Das bedeutet, dass der Fluss in beide Richtungen durch Einheit 1-1 ging (symmetrischer Verkehr):

<#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

```

## Beobachtung 2. Analyse des Verbindungsflags für den Datenfluss mit Quellport 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

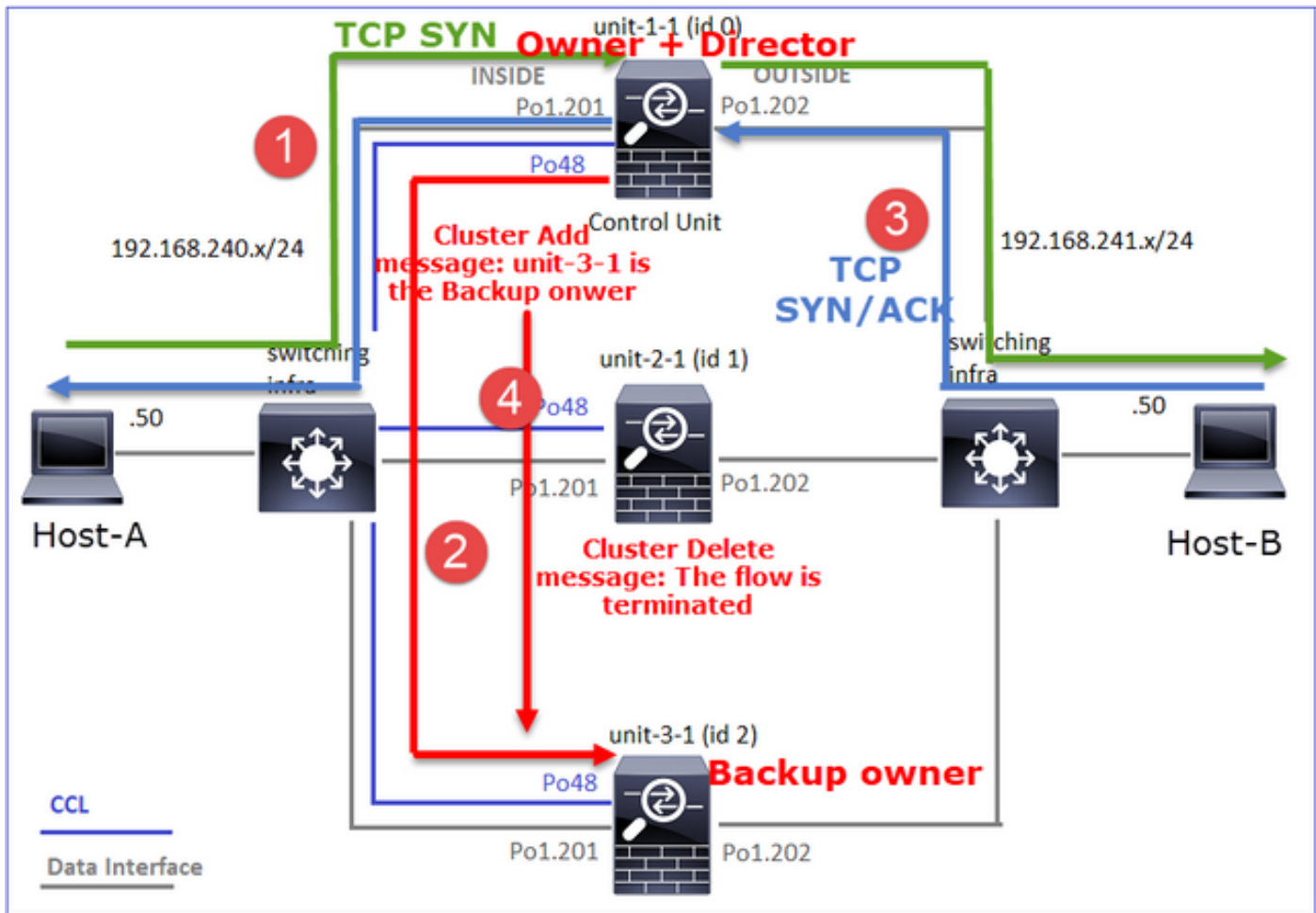
, idle 0:00:06, bytes 0,

flags y

Einheit	Flag	Hinweis
Einheit-1-1	UIO	<ul style="list-style-type: none"> <li>• Flow Owner - Die Einheit übernimmt den Flow</li> <li>• Director - Da Unit-3-1 über "y" und nicht "Y" verfügt, impliziert dies, dass Unit-1-1 als Director für diesen Fluss ausgewählt wurde. Da es sich also auch um den Eigentümer handelt, wurde eine weitere Einheit (in diesem Fall Einheit-3-1) als Sicherungseigentümer ausgewählt</li> </ul>
Einheit-2-1	-	-

Einheit-3-1	y	Das Gerät ist Sicherungseigentümer.
-------------	---	-------------------------------------

Dies kann wie folgt visualisiert werden:



1. Das TCP-SYN-Paket kommt von Host-A an Einheit-1-1. Einheit-1-1 wird zum Eigentümer des Datenflusses.
2. Unit-1-1 wird ebenfalls zum Flow Director gewählt. Daher wird auch Unit-3-1 als Backup-Eigentümer (Cluster-Add-Message) ausgewählt.
3. Das TCP-SYN/ACK-Paket kommt von Host-B zu Einheit-3-1. Der Fluss ist symmetrisch.
4. Sobald die Verbindung beendet ist, sendet der Besitzer eine Cluster-Löschmeldung, um die Flow-Informationen vom Backup-Besitzer zu entfernen.

Beobachtung 3. Erfassung mit Spur zeigt, dass beide Richtungen nur durch Einheit-1-1 gehen.

Schritt 1: Identifizieren Sie den Fluss und die Pakete, die für alle Cluster-Einheiten von Interesse sind, basierend auf dem Quell-Port:

```
<#root>
```

```
firepower#
```

```
cluster exec show capture CAPI | i 45954
```

```
unit-1-1(LOCAL):*****
1: 08:42:09.362697 802.1Q vlan#201 PO 192.168.240.50.45954 > 192.168.241.50.80: S 992089269:992089269(0
2: 08:42:09.363521 802.1Q vlan#201 PO 192.168.241.50.80 > 192.168.240.50.45954: S 4042762409:4042762409
3: 08:42:09.363827 802.1Q vlan#201 PO 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 PO 192.168.240.50.45954 > 192.168.241.50.80: S 2732339016:2732339016
2: 08:42:09.363415 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.45954: S 3603655982:3603655982
3: 08:42:09.363903 802.1Q vlan#202 PO 192.168.240.50.45954 > 192.168.241.50.80: . ack 3603655983 win 22
...
unit-2-1:*****
unit-3-1:*****
```

Schritt 2: Da es sich um einen TCP-Flow handelt, werden die 3-Wege-Handshake-Pakete verfolgt. Wie in dieser Ausgabe zu sehen ist, ist "unit-1-1" der Eigentümer. Der Einfachheit halber werden die nicht relevanten Spurenphasen weggelassen:

<#root>

firepower#

show cap CAPI packet-number 1 trace

```
25985 packets captured
1: 08:42:09.362697 802.1Q vlan#201 PO 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

...

Rückverkehr (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

Beobachtung 4. FTD-Datenebenen-Syslogs zeigen die Verbindungsherstellung und -terminierung auf allen Einheiten an:

```
<#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
```

Anwenderbericht 2. Symmetrischer Datenverkehr (anderer Eigentümer als der Director)

- Wie Fallstudie #1, aber in diesem Fall ist ein Flow Owner eine andere Einheit als der Director.
- Alle Ergebnisse sind ähnlich wie in der Fallstudie #1. Der Hauptunterschied zur Fallstudie #1 ist die "Y"-Markierung, die die "y"-Markierung von Szenario 1 ersetzt.

Beobachtung 1. Der Besitzer ist anders als der Direktor.

# Analyse des Verbindungs-Flags für den Datenfluss mit Quellport 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:

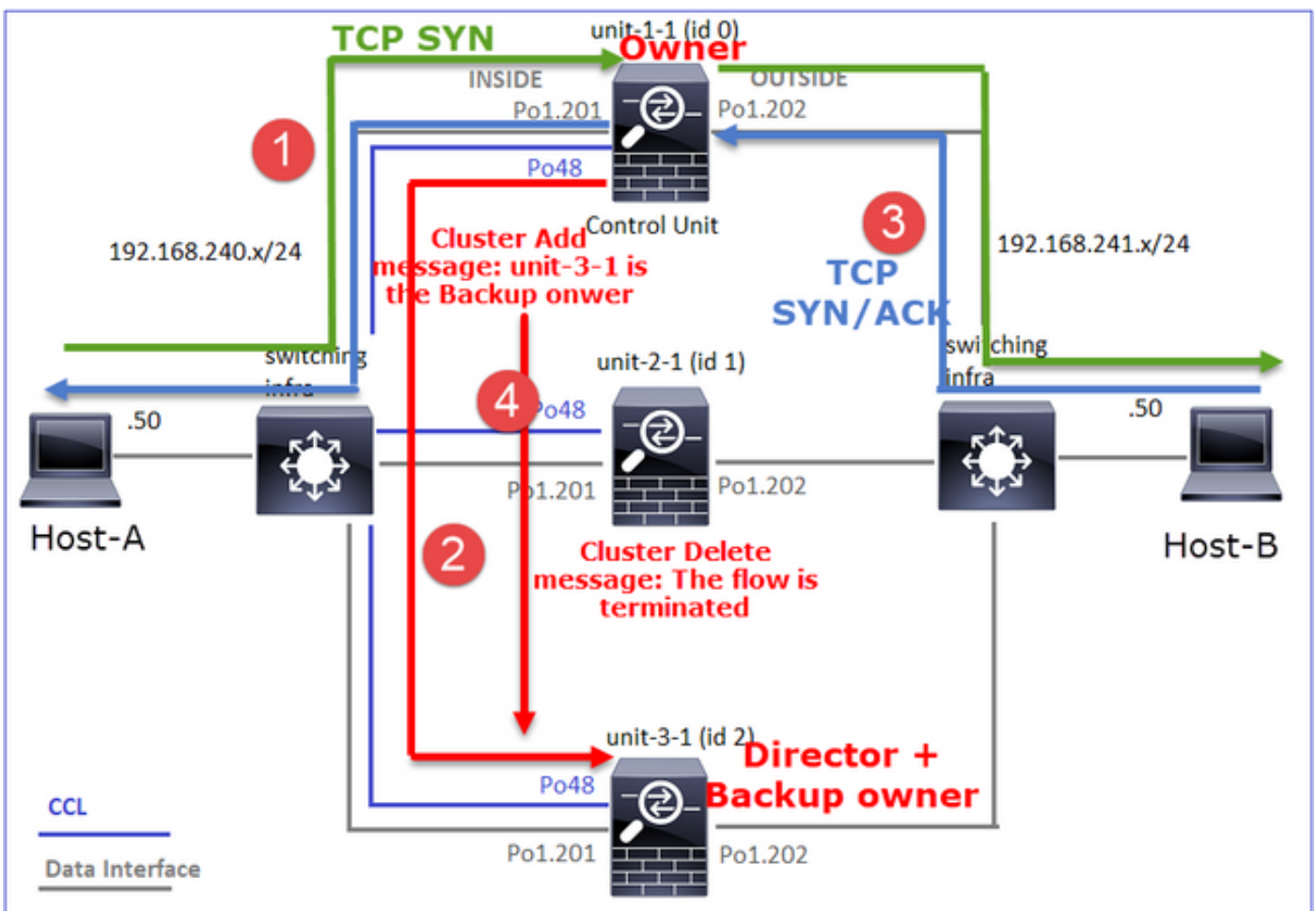
46278

, idle 0:00:06, bytes 0,

flags Y

Einheit	Flag	Hinweis
Einheit-1-1	UIO	· Flow Owner - Die Einheit übernimmt den Flow
Einheit-2-1	-	-
Einheit-3-1	Y	· Director und Backup Owner - Unit 3-1 hat die Markierung Y (Director).

Dies kann wie folgt visualisiert werden:



1. Das TCP-SYN-Paket kommt von Host-A an Einheit-1-1. Einheit-1-1 wird zum Eigentümer des Datenflusses.
2. Unit-3-1 wird zum Flow Director gewählt. Unit-3-1 ist auch der Sicherungseigentümer (Cluster-Add-Meldung auf UDP 4193 über CCL).
3. Das TCP-SYN/ACK-Paket kommt von Host-B zu Einheit-3-1. Der Fluss ist symmetrisch.
4. Sobald die Verbindung beendet ist, sendet der Besitzer über den CCL eine "Cluster Delete"-Nachricht auf UDP 4193, um die Flow-Informationen vom Backup-Besitzer zu entfernen.

Beobachtung 2. Erfassung mit Spur zeigt, dass beide Richtungen nur durch Einheit-1-1 gehen

Schritt 1: Verwenden Sie den gleichen Ansatz wie in Fallstudie 1, um den Datenfluss und die relevanten Pakete in allen Cluster-Einheiten basierend auf dem Quell-Port zu identifizieren:

```
<#root>
```

```
firepower#
```

```
cluster exec show cap CAPI | include 46278
```

```
unit-1-1
```

```
(LOCAL):*****
```

```
3: 11:01:44.841631 802.1Q vlan#201 PO 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 PO 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 PO 192.168.240.50.46278 > 192.168.241.50.80: . ack 3524167696 win 22
```

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

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

```
firepower#
```

Erfassung an der OUTSIDE-Schnittstelle:

```
<#root>
```

```
firepower#
```

```
cluster exec show cap CAPO | include 46278
```

```
unit-1-1
```

```
(LOCAL):*****
```

```
3: 11:01:44.841921 802.1Q vlan#202 PO 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 PO 192.168.241.50.80 > 192.168.240.50.46278:
```

```
s
```

```
3382481337:3382481337(0)
```



ack

2153055700 win 28960 <mss 1460,sackOK,timestamp 513884542 503529072,nop,wscale 7>  
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#

## Schritt 2: Fokus auf Eingangspaketen (TCP SYN und 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

Verfolgen Sie SYN/ACK auf Einheit 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 PO 192.168.241.50.80 > 192.168.240.50.

46278

:

S

3382481337:3382481337(0)

ack

2153055700 win 28960 <mss 1460,sackOK,timestamp 513884542 503529072,nop,wscale 7>

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Config:

Additional Information:

Found flow with id 9583, using existing flow

Beobachtung 3. Die FTD-Syslogs auf Datenebene zeigen die Verbindungserstellung und -beendigung beim Eigentümer und Sicherungseigentümer:

<#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 (192.168.241.50/80)

Dec 01 2020 11:01:53: %FTD-6-302014:

Teardown TCP connection

9583 for INSIDE:192.168.240.50/46278 to OUTSIDE:192.168.241.50/80 duration 0:00:08 bytes 1024001808 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

Fallstudie 3. Asymmetrischer Datenverkehr (Director leitet den Datenverkehr weiter).

Beobachtung 1. Die Erfassung zum Ausblenden der Wiedereinfuhr zeigt Pakete in Einheit 1-1 und Einheit 2-1 (asymmetrischer Fluss) an:

<#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

```

Beobachtung 2. Analyse des Verbindungsflags für den Datenfluss mit Quellport 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

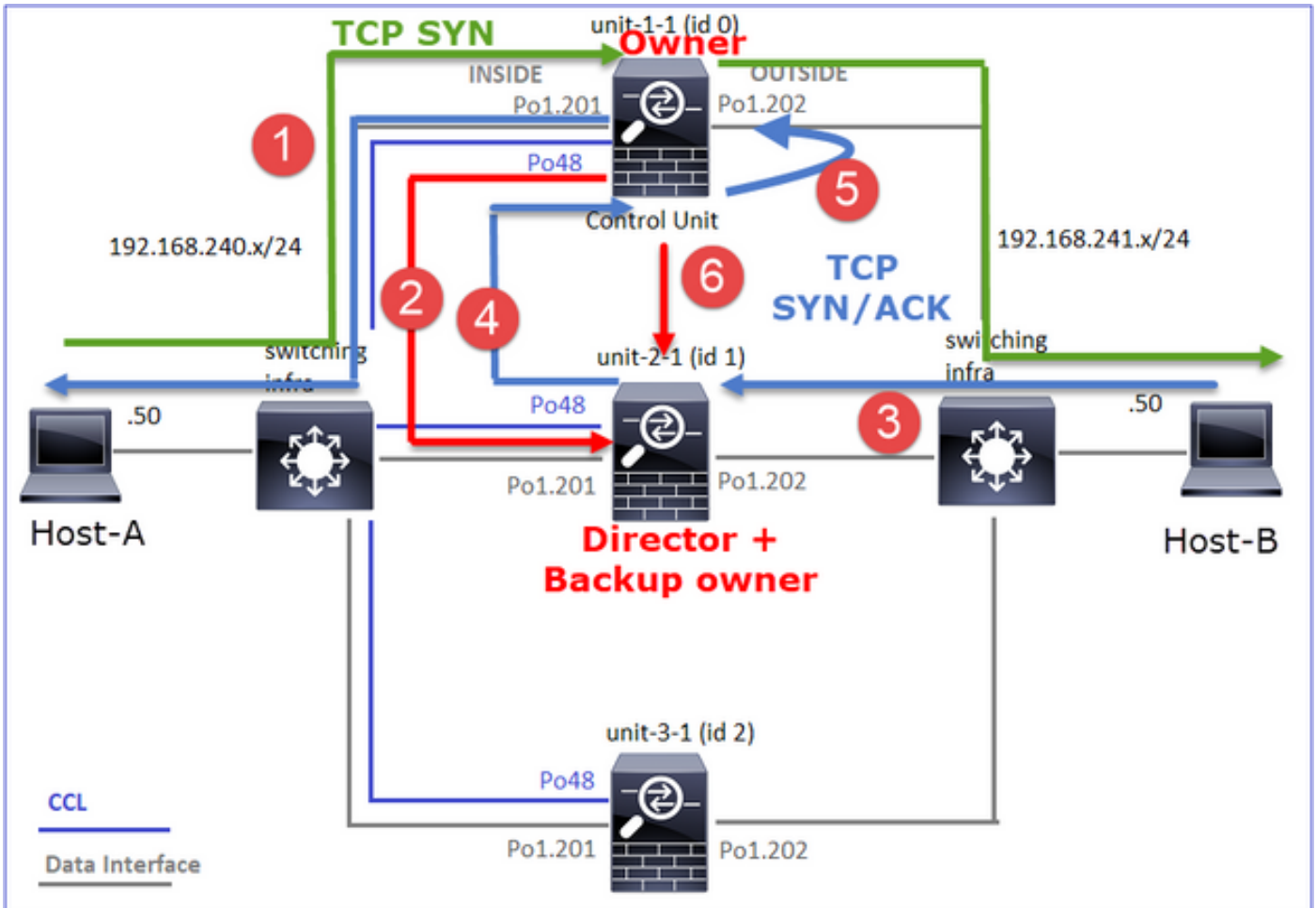
Inspect Snort:

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

Einheit	Flag	Hinweis
Einheit-1-1	UIO	<ul style="list-style-type: none"><li>• Flow Owner - Die Einheit übernimmt den Flow.</li></ul>
Einheit-2-1	Y	<ul style="list-style-type: none"><li>• Director - Da Unit-2-1 die Markierung "Y" trägt, bedeutet dies, dass Unit-2-1 als Director für diesen Fluss ausgewählt wurde.</li><li>• Backup Owner</li><li>• Schließlich, obwohl es aus dieser Ausgabe nicht offensichtlich ist, aus der Ausgabe von show capture und show log, ist es offensichtlich, dass unit-2-1 diesen Fluss an den Eigentümer weiterleitet (obwohl es technisch in diesem Szenario nicht als Forwarder angesehen wird).</li></ul> <p>Anmerkung: Eine Einheit kann nicht gleichzeitig Director (Y-Fluss) und Forwarder (z-Fluss) sein. Diese beiden Rollen schließen sich gegenseitig aus. Directors (Y-Fluss) können weiterhin Datenverkehr weiterleiten. Siehe die Ausgabe von show log weiter unten in diesem</p>

		Anwenderbericht.
Einheit-3-1	-	-

Dies kann wie folgt visualisiert werden:



1. Das TCP-SYN-Paket kommt von Host-A an Einheit-1-1. Einheit-1-1 wird zum Eigentümer des Datenflusses.
2. Unit-2-1 wird zum Flow Director und zum Backup-Eigentümer gewählt. Der Flow Owner sendet eine Unicast-Meldung zum Hinzufügen eines Clusters zum UDP 4193, um den Backup Owner über den Flow zu informieren.
3. Das TCP-SYN/ACK-Paket kommt von Host-B an Einheit-2-1 an. Der Datenfluss ist asymmetrisch.
4. Unit-2-1 leitet das Paket (aufgrund des TCP-SYN-Cookies) über die CCL an den Eigentümer weiter.
5. Der Eigentümer sendet das Paket neu in die EXTERNE Schnittstelle und leitet es dann an Host A weiter.
6. Sobald die Verbindung beendet ist, sendet der Besitzer eine Cluster-Löschmeldung, um die Flow-Informationen vom Backup-Besitzer zu entfernen.

Beobachtung 3: Die Erfassung mit Spur zeigt den asymmetrischen Datenverkehr und die

Umleitung von Einheit-2-1 zu Einheit-1-1.

Schritt 1: Identifizieren Sie die Pakete, die zu dem gewünschten Fluss gehören (Port 46502):

```
<#root>
```

```
firepower#
```

```
cluster exec show capture CAPI | include 46502
```

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

```
3: 12:58:33.356121 802.1Q vlan#201 PO 192.168.240.50.46502 > 192.168.241.50.80: S 4124514680:4124514680
```

```
4: 12:58:33.357037 802.1Q vlan#201 PO 192.168.241.50.80 > 192.168.240.50.46502: S 883000451:883000451(0
```

```
5: 12:58:33.357357 802.1Q vlan#201 PO 192.168.240.50.46502 > 192.168.241.50.80: . ack 883000452 win 229
```

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

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

Die Rückwärtsrichtung:

```
<#root>
```

```
firepower#
```

```
cluster exec show capture CAPO | include 46502
```

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

```
3: 12:58:33.356426 802.1Q vlan#202 PO 192.168.240.50.46502 > 192.168.241.50.80: S 1434968587:1434968587
```

```
4: 12:58:33.356915 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.46502: S 4257314722:4257314722
```

```
5: 12:58:33.357403 802.1Q vlan#202 PO 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 PO 192.168.241.50.80 > 192.168.240.50.46502: S 4257314722:4257314722
```

```
2: 12:58:33.360302 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.46502: . ack 1434968736 win 23
```

```
3: 12:58:33.361004 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.46502: . 4257314723:4257316091
```

```
...
```

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

Schritt 2: Verfolgen Sie die Pakete. Standardmäßig werden nur die ersten 50 eingehenden Pakete verfolgt. Der Einfachheit halber werden die nicht relevanten Spurenphasen weggelassen.

Unit-1-1 (Eigentümer):

```
<#root>
```

```
firepower#
```

```
cluster exec show capture CAPI packet-number 3 trace
```

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

3: 12:58:33.356121 802.1Q v1an#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

## Einheit-2-1 (Weiterleitung)

Der zurückgegebene Datenverkehr (TCP SYN/ACK). Die interessierende Einheit ist Einheit 2-1, die dem Direktor/Sicherungseigentümer gehört und den Datenverkehr an den Eigentümer weiterleitet:

<#root>

firepower#

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

1: 12:58:33.359249 802.1Q v1an#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).

Beobachtung 4. FTD-Datenebenen-Syslogs zeigen die Verbindungsherstellung und -terminierung auf allen Einheiten an:

<#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 (192.168.241.50/80)  
Dec 01 2020 12:59:02: %FTD-6-302014:

Teardown TCP connection

9742 for INSIDE:192.168.240.50/46502 to OUTSIDE:192.168.241.50/80 duration 0:00:28 bytes 2048000440 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 (192.168.240.50/46502)  
Dec 01 2020 12:58:33: %FTD-6-302023:

Teardown forwarder TCP connection

for OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46502 duration 0:00:00 forwarded bytes 0 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#

#### Fallstudie 4. Asymmetrischer Datenverkehr (der Besitzer ist der Leiter)

Beobachtung 1. Die Erfassung zum Ausblenden der Wiedereinfuhr zeigt Pakete in Einheit 1-1 und Einheit 2-1 (asymmetrischer Fluss) an:

<#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

```

## Beobachtung 2. Analyse des Verbindungsflags für den Datenfluss mit Quellport 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:

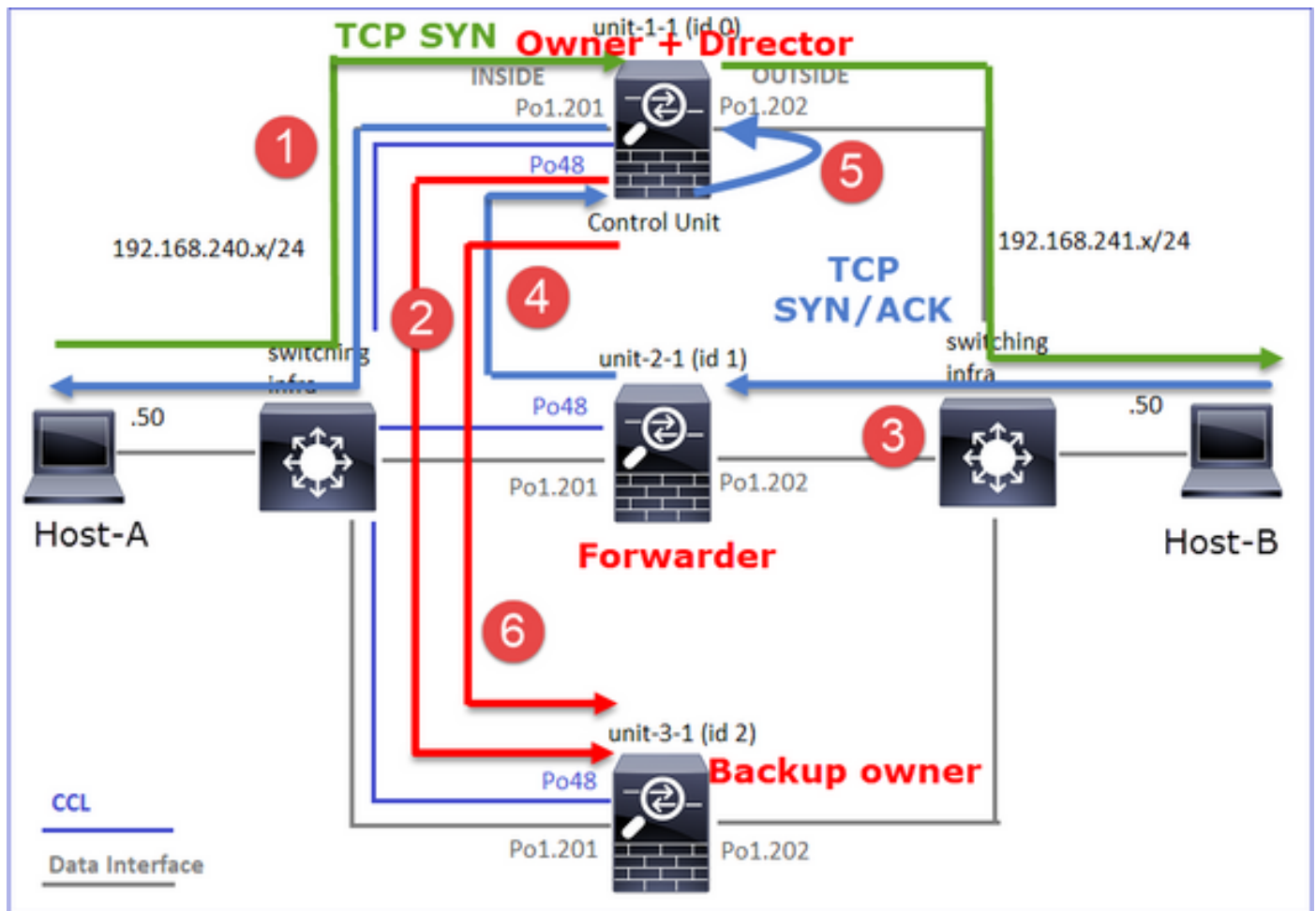
46916

, idle 0:00:04, bytes 0,

flags y

Einheit	Flag	Hinweis
Einheit-1-1	UIO	<ul style="list-style-type: none"><li>• Flow Owner - Die Einheit übernimmt den Flow</li><li>• Director - Da Unit-3-1 über "y" und nicht "Y" verfügt, impliziert dies, dass Unit-1-1 als Director für diesen Fluss ausgewählt wurde. Da es sich also auch um den Eigentümer handelt, wurde eine weitere Einheit (in diesem Fall Einheit-3-1) als Sicherungseigentümer ausgewählt</li></ul>
Einheit-2-1	z	<ul style="list-style-type: none"><li>• Weiterleitung</li></ul>
Einheit-3-1	y	- Sicherungseigentümer

Dies kann wie folgt visualisiert werden:



1. Das TCP-SYN-Paket kommt von Host-A an Einheit-1-1. Einheit-1-1 wird zum Flow-Eigentümer und wird als Director ausgewählt.
2. Unit-3-1 wird als Sicherungseigentümer ausgewählt. Der Flow Owner sendet eine Unicast-"Cluster Add"-Nachricht an UDP 4193, um den Backup Owner über den Flow zu informieren.
3. Das TCP-SYN/ACK-Paket kommt von Host-B an Einheit-2-1 an. Der Datenfluss ist asymmetrisch.
4. Unit-2-1 leitet das Paket (aufgrund des TCP-SYN-Cookies) über die CCL an den Eigentümer weiter.
5. Der Eigentümer sendet das Paket neu in die EXTERNE Schnittstelle und leitet es dann an Host A weiter.
6. Sobald die Verbindung beendet ist, sendet der Besitzer eine Cluster-Löschmeldung, um die Flow-Informationen vom Backup-Besitzer zu entfernen.

Beobachtung 3: Die Erfassung mit Spur zeigt den asymmetrischen Datenverkehr und die Umleitung von Einheit-2-1 zu Einheit-1-1.

Einheit-2-1 (Weiterleitung)

```
<#root>
```

```
firepower#
```

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

```
1: 16:11:33.653164 802.1Q vlan#202 PO 192.168.241.50.80 > 192.168.240.50.
```

```
46916
```

```
:
```

```
S
```

```
1331019196:1331019196(0)
```

```
ack
```

```
3089755618 win 28960 <mss 1460,sackOK,timestamp 532473211 522117741,nop,wscale 7>
```

```
...
```

```
Phase: 4
```

```
Type: CLUSTER-EVENT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

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

```
Flow type: NO FLOW
```

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

```
Phase: 5
```

```
Type: CLUSTER-EVENT
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

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

```
Flow type: NO FLOW
```

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

Beobachtung 4. FTD-Datenebenen-Syslogs zeigen die Verbindungsherstellung und -terminierung auf allen Einheiten an:

- Einheit-1-1 (Eigentümer)
- Einheit-2-1 (Weiterleitung)
- Unit-3-1 (Sicherungseigentümer)

```
<#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 (192.168.241.50/80) duration 0:00:09 bytes 1024010016 T  
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 (192.168.240.50/46916) duration 0:00:09 forwarded bytes 1024009

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) duration 0:00:09 forwarded bytes 0 Cluste

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

Fallstudie 5. Asymmetrischer Datenverkehr (Eigentümer ist nicht der Director).

Beobachtung 1. Die Erfassung zum Ausblenden der Wiedereinfuhr zeigt Pakete in Einheit 1-1 und Einheit 2-1 (asymmetrischer Fluss) an:

<#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
```

Beobachtung 2. Analyse des Verbindungs-Flags für den Datenfluss mit Quellport 4694:

<#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:

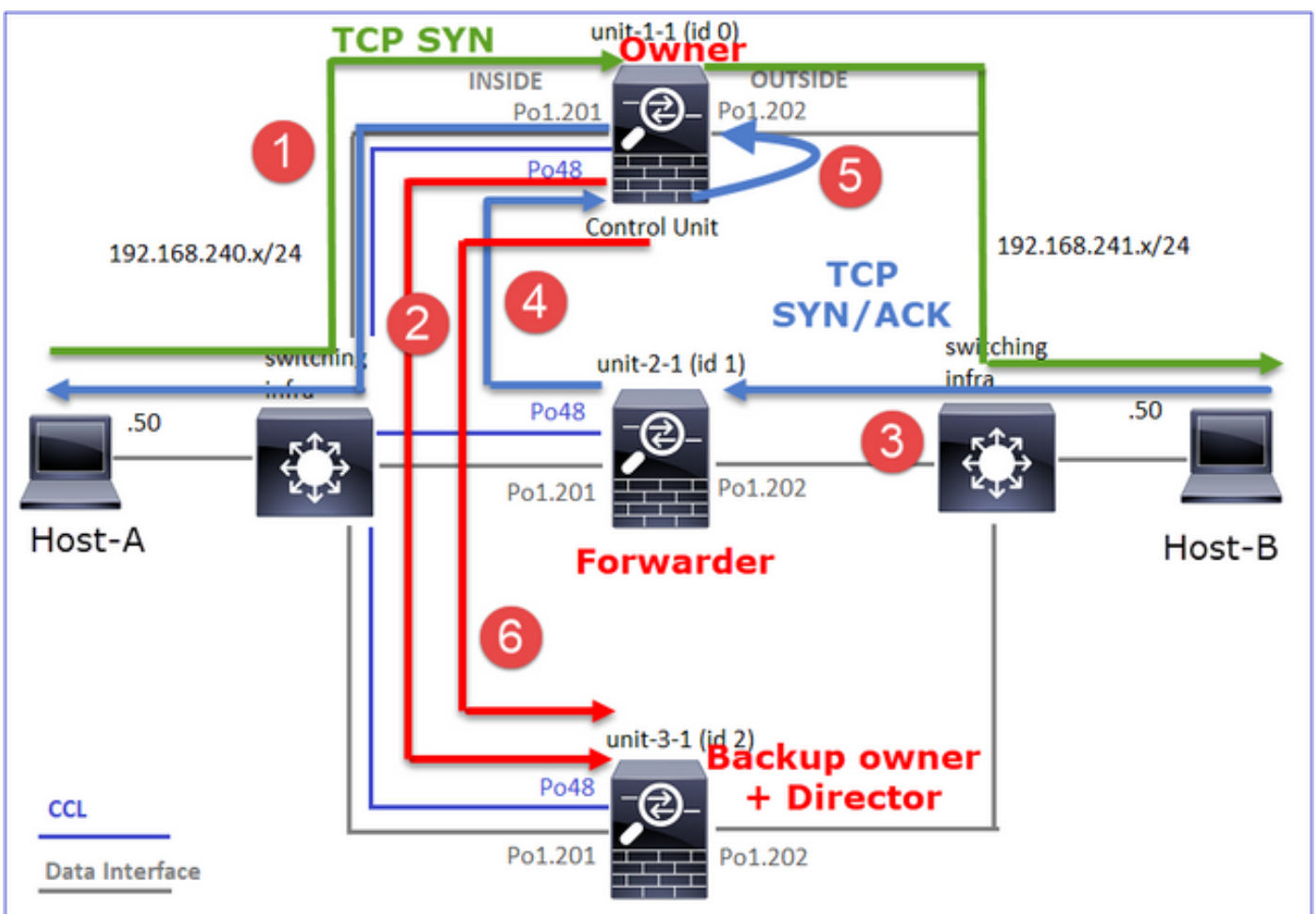
46994

, idle 0:00:05, bytes 0,

flags Y

Einheit	Flag	Hinweis
Einheit-1-1	UIO	· Flow Owner - Die Einheit übernimmt den Flow
Einheit-2-1	z	· Weiterleitung
Einheit-3-1	Y	· Backup Owner · Direktor

Dies kann wie folgt visualisiert werden:



1. Das TCP-SYN-Paket kommt von Host-A an Einheit-1-1. Einheit-1-1 wird zum Eigentümer des Datenflusses.

2. Unit-3-1 wird als Director und Backup Owner ausgewählt. Der Flow Owner sendet eine Unicast-Meldung zum Hinzufügen eines Clusters zum UDP 4193, um den Backup Owner über den Flow zu informieren.
3. Das TCP-SYN/ACK-Paket kommt von Host-B an Einheit-2-1 an. Der Datenfluss ist asymmetrisch.
4. Unit-2-1 leitet das Paket (aufgrund des TCP-SYN-Cookies) über die CCL an den Eigentümer weiter.
5. Der Eigentümer sendet das Paket neu in die EXTERNE Schnittstelle und leitet es dann an Host A weiter.
6. Sobald die Verbindung beendet ist, sendet der Besitzer eine Cluster-Löschmeldung, um die Flow-Informationen vom Backup-Besitzer zu entfernen.

Beobachtung 3: Die Erfassung mit Spur zeigt den asymmetrischen Datenverkehr und die Umleitung von Einheit-2-1 zu Einheit-1-1.

### Einheit-1-1 (Eigentümer)

```
<#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
```

### Einheit-2-1 (Weiterleitung)

<#root>

firepower#

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

1: 16:46:44.232074 802.1Q vlan#202 PO 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).

Beobachtung 4. FTD-Datenebenen-Syslogs zeigen die Verbindungsherstellung und -terminierung auf allen Einheiten an:

- Einheit-1-1 (Eigentümer)
- Einheit-2-1 (Weiterleitung)
- Unit-3-1 (Backup-Eigentümer/-Leiter)

<#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 (192.168.240.50/46994)  
Dec 01 2020 16:46:53: %FTD-6-302023:

**Teardown forwarder TCP connection**

for OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46994 duration 0:00:09 forwarded bytes 1024000

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

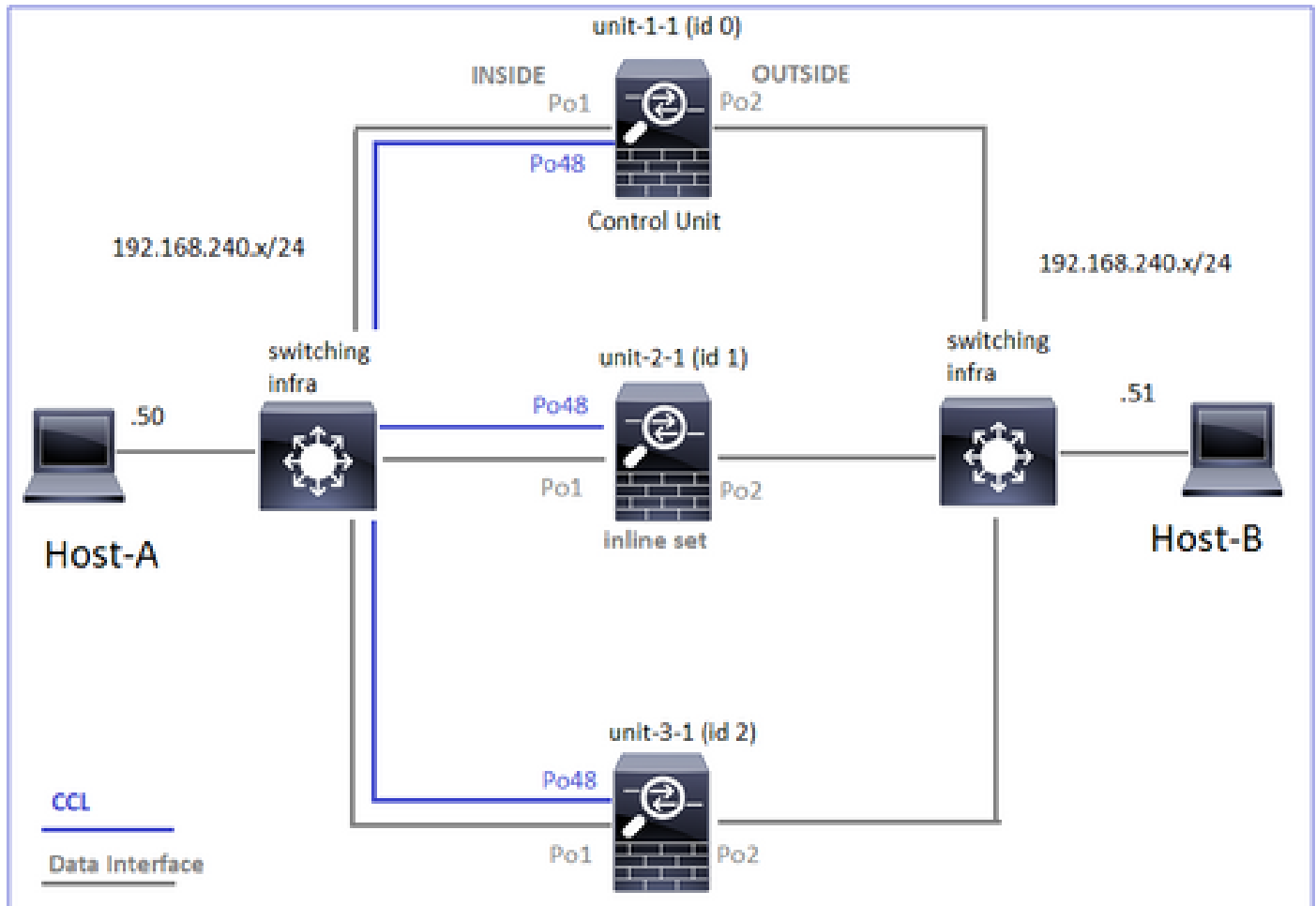
**Built director stub TCP connection**

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

Für die nächsten Fallstudien basiert die verwendete Topologie auf einem Cluster mit Inline-Sätzen:



## Fallstudie 6. Asymmetrischer Datenverkehr (Inline-Set, der Besitzer ist der Leiter)

Beobachtung 1: Die Erfassung von "reject-hide" zeigt Pakete in den Einheiten 1-1 und 2-1 (asymmetrischer Fluss). Darüber hinaus ist der Besitzer Einheit-2-1 (es gibt Pakete auf beiden, INSIDE und OUTSIDE Schnittstellen für die reject-hide Captures, während Einheit-1-1 nur auf OUTSIDE existiert):

```
<#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

```

Beobachtung 2. Analyse des Verbindungsflags für den Datenfluss mit Quellport 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
```

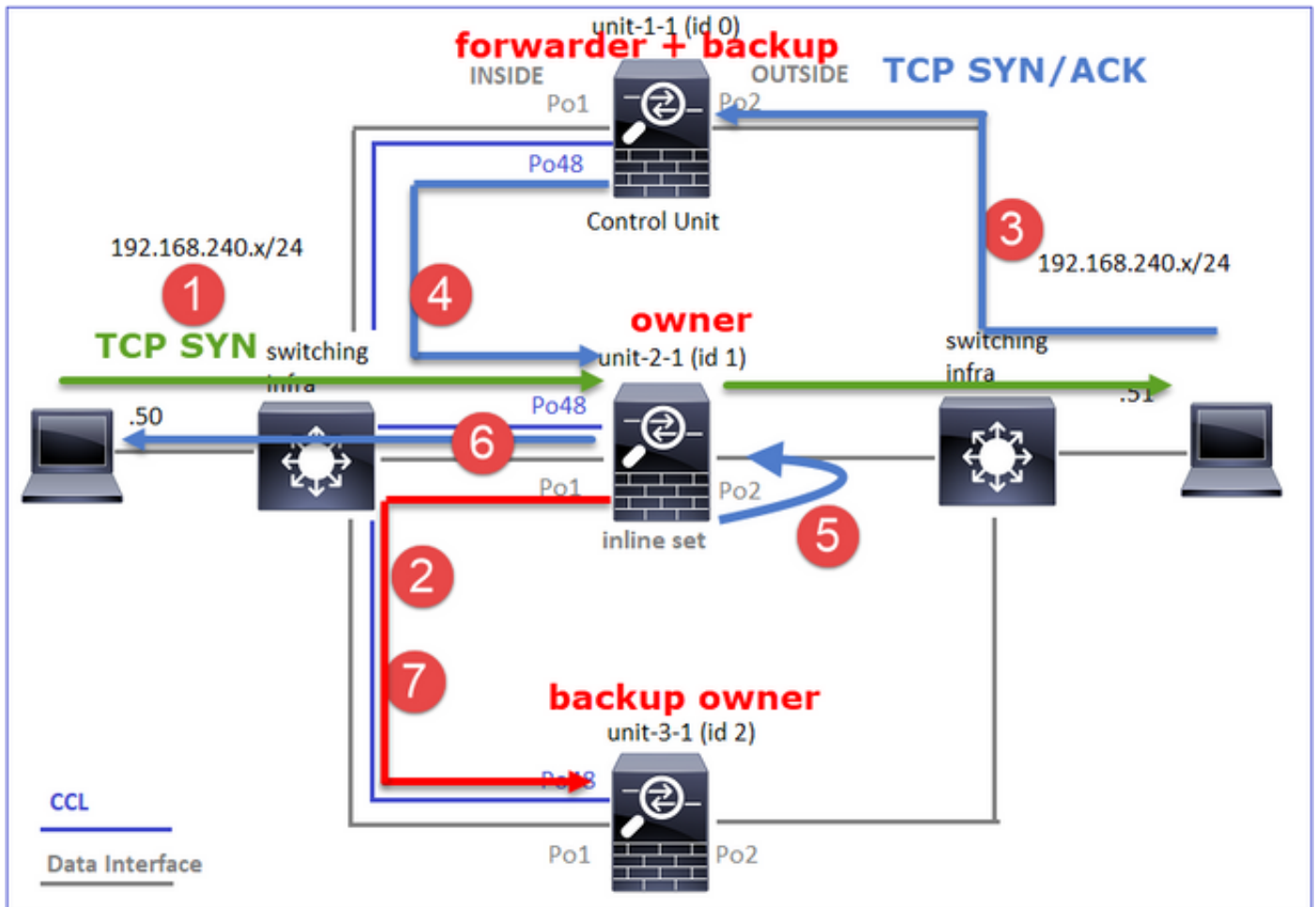
unit-3-1

```
:*****  
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
```

Einheit	Flag	Hinweis
Einheit-1-1	z	· Weiterleitung
Einheit-2-1	b N	· Flow Owner - Die Einheit übernimmt den Flow
Einheit-3-1	y	· Backup Owner

Dies kann wie folgt visualisiert werden:





1. Das TCP-SYN-Paket kommt von Host-A an Einheit-2-1. Einheit-2-1 wird zum Flow-Eigentümer und wird als Director ausgewählt.
2. Unit-3-1 wird zum Sicherungseigentümer gewählt. Der Flow Owner sendet eine Unicast-Meldung zum Hinzufügen eines Clusters zum UDP 4193, um den Backup Owner über den Flow zu informieren.
3. Das TCP-SYN/ACK-Paket kommt von Host-B an Einheit-1-1 an. Der Datenfluss ist asymmetrisch.
4. Unit-1-1 leitet das Paket über die CCL an den Director weiter (Unit-2-1).
5. Unit-2-1 ist ebenfalls der Eigentümer und leitet das Paket an der Schnittstelle OUTSIDE neu ein.
6. Einheit 2-1 leitet das Paket an Host A weiter.
7. Sobald die Verbindung beendet ist, sendet der Besitzer eine Cluster-Löschmeldung, um die Flow-Informationen vom Backup-Besitzer zu entfernen.

Beobachtung 3: Die Erfassung mit Spur zeigt den asymmetrischen Datenverkehr und die Umleitung von Einheit-1-1 zu Einheit-2-1.

Unit-2-1 (Eigentümer/Leiter)

```
<#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

Einheit-1-1 (Weiterleitung)

<#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

Phase: 1

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'OUTSIDE'

Flow type: NO FLOW

I (0) am asking director (1).

Rückverkehr (TCP SYN/ACK)

## Unit-2-1 (Eigentümer/Leiter)

<#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 v
```

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
```

Beobachtung 4. FTD-Datenebenen-Syslogs zeigen die Verbindungsherstellung und -terminierung auf allen Einheiten an:

- Einheit-1-1 (Eigentümer)
- Einheit-2-1 (Weiterleitung)
- Unit-3-1 (Backup-Eigentümer/-Leiter)

<#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 (192.168.240.50/51844)
```

```
Dec 02 2020 18:10:22: %FTD-6-302023:
```

```
Teardown forwarder TCP connection
```

for OUTSIDE:192.168.240.51/80 to unknown:192.168.240.50/51844 duration 0:00:09 forwarded bytes 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 (192.168.240.51/80)

Dec 02 2020 18:10:22: %FTD-6-302304:

Teardown TCP state-bypass connection

7109 from INSIDE:192.168.240.50/51844 to OUTSIDE:192.168.240.51/80 duration 0:00:09 bytes 1024001888 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

## Fallstudie 7. Asymmetrischer Datenverkehr (Inline-Set, der Besitzer ist anders als der Director)

Eigentümer ist Unit-2-1 (es gibt Pakete an beiden Schnittstellen, INSIDE und OUTSIDE für die Erfassung von "reject-hide", während Unit-3-1 nur über OUTSIDE verfügt):

<#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

```

Beobachtung 2. Analyse des Verbindungsflags für den Datenfluss mit Quellport 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:

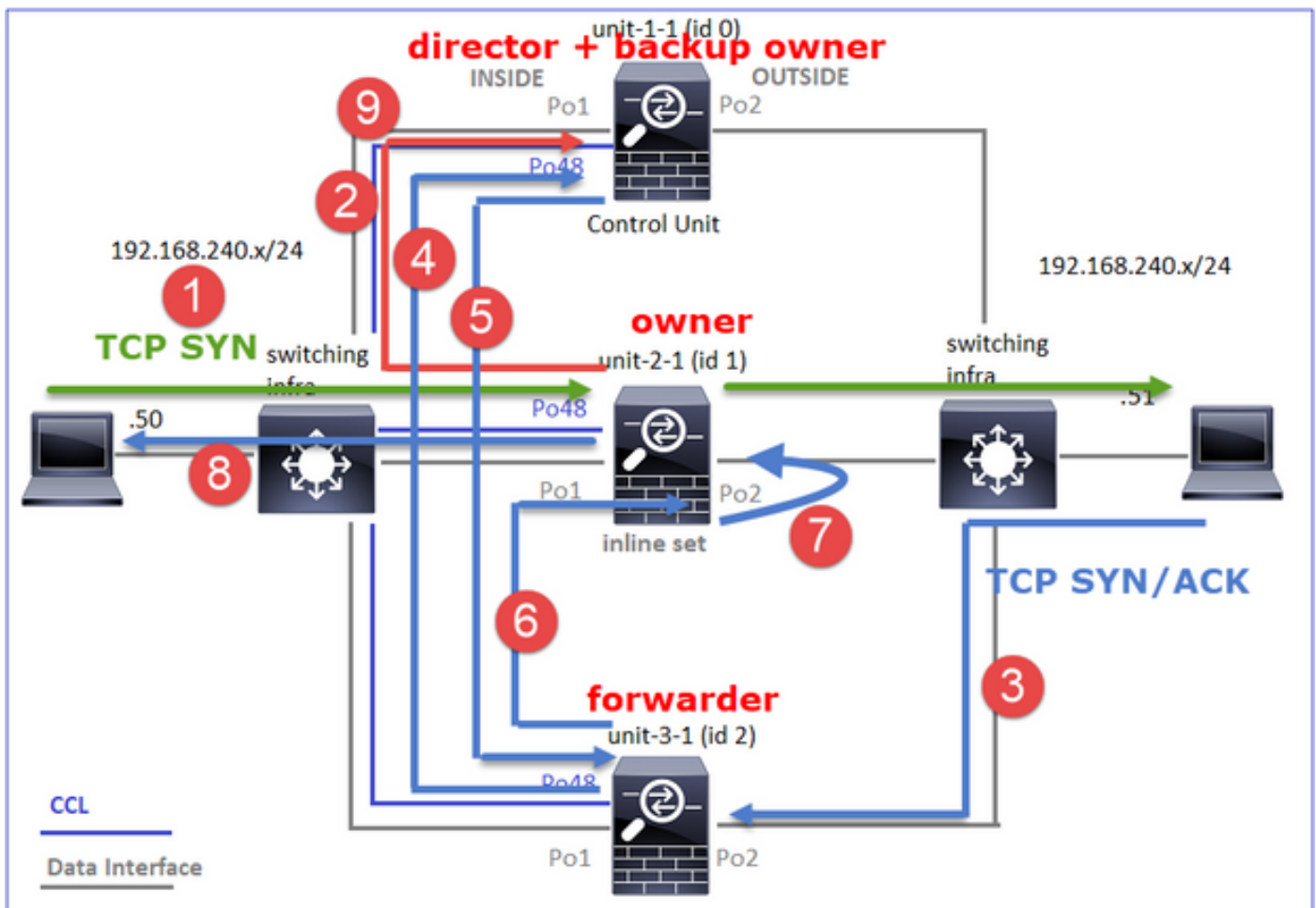
59210

, idle 0:00:00, bytes 0,

flags z


Einheit	Flag	Hinweis
Einheit-1-1	Y	· Director/Backup Owner
Einheit-2-1	b N	· Flow Owner - Die Einheit übernimmt den Flow
Einheit-3-1	z	· Weiterleitung

Dies kann wie folgt visualisiert werden:



1. Das TCP-SYN-Paket kommt von Host-A zu Einheit-2-1. Einheit-2-1 wird zum Datenflusseigentümer, und Einheit-1-1 wird zum Director gewählt
2. Unit-1-1 wird zum Backup-Eigentümer gewählt (da es sich um den Director handelt). Der Flow Owner sendet eine Unicast-Meldung zum Hinzufügen eines Clusters für UDP 4193 an den Sicherungsinhaber über den Datenfluss informieren.

3. Das TCP-SYN/ACK-Paket kommt von Host-B an Einheit-3-1 an. Der Datenfluss ist asymmetrisch.
4. Unit-3-1 leitet das Paket über die CCL an den Director weiter (Unit-1-1).
5. Unit-1-1 (Director) weiß, dass der Besitzer Unit-2-1 ist, sendet das Paket zurück an die Weiterleitung (Unit-3-1) und benachrichtigt ihn, dass der Besitzer Unit-2-1 ist.
6. Unit-3-1 sendet das Paket an Unit-2-1 (Eigentümer).
7. Unit-2-1 startet das Paket an der Schnittstelle OUTSIDE neu.
8. Einheit 2-1 leitet das Paket an Host A weiter.
9. Sobald die Verbindung beendet ist, sendet der Besitzer eine Cluster-Löschmeldung, um die Flow-Informationen vom Backup-Besitzer zu entfernen.

 Anmerkung: Es ist wichtig, dass Schritt 2 (Paket über die CCL) vor Schritt 4 (Datenverkehr) ausgeführt wird. In einem anderen Fall (z. B. bei einem Wettrennen) ist dem Regisseur der Fluss nicht bekannt. Da es sich also um ein Inline-Set handelt, wird das Paket an das Ziel weitergeleitet. Wenn sich die Schnittstellen nicht in einem Inline-Set befinden, wird das Datenpaket verworfen.

Beobachtung 3. Die Erfassung mit Trace zeigt den asymmetrischen Datenverkehr und den Austausch über das CCL:

Weitergeleiteter Datenverkehr (TCP SYN)

Unit-2-1 (Eigentümer)

<#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

Rückverkehr (TCP SYN/ACK)

Unit-3-1 (ID 2 - Forwarder) sendet das Paket über die CCL an 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) weiß, dass es sich bei dem Datenflusseigentümer um Unit-2-1 (ID 1) handelt, und sendet das Paket über die CCL zurück an Unit-3-1 (ID 2 - Forwarder).

<#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) ruft das Paket über die CCL ab und sendet es an Unit-2-1 (ID 1 - Owner).

```
<#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).
```

Der Eigentümer wirft das Paket neu ein und leitet es an das Ziel weiter:

```
<#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).

Beobachtung 4. FTD-Datenebenen-Syslogs zeigen die Verbindungsherstellung und -terminierung auf allen Einheiten an:

- Unit-1-1 (Director/Backup Owner)
- Unit-2-1 (Eigentümer)
- Einheit-3-1 (Weiterleitung)

<#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 (192.168.240.51/80)

Dec 03 2020 09:19:59: %FTD-6-302304:

Teardown TCP state-bypass connection

14483 from INSIDE:192.168.240.50/59210 to OUTSIDE:192.168.240.51/80 duration 0:00:09 bytes 1024003336

unit-3-1:\*\*\*\*\*

Dec 03 2020 09:19:49: %FTD-6-302022:

Built forwarder stub TCP connection

for OUTSIDE:192.168.240.51/80 (192.168.240.51/80) to unknown:192.168.240.50/59210 (192.168.240.50/59210)

Dec 03 2020 09:19:59: %FTD-6-302023:

Teardown forwarder TCP connection

for OUTSIDE:192.168.240.51/80 to unknown:192.168.240.50/59210 duration 0:00:09 forwarded bytes 1024003

## Fehlerbehebung

### Cluster-Fehlerbehebung - Einführung

Die Cluster-Probleme lassen sich wie folgt kategorisieren:

- Probleme mit der Kontrollebene (mit der Stabilität des Clusters zusammenhängende Probleme)
- Probleme mit der Datenebene (im Zusammenhang mit dem Transitverkehr)

### Probleme mit der Cluster-Datenebene

Häufige Probleme bei NAT/PAT

Wichtige Überlegungen zur Konfiguration

- Port Address Translation (PAT)-Pools müssen mindestens so viele IPs verfügbar sein wie Einheiten im Cluster, vorzugsweise mehr IPs als Cluster-Knoten.
- Die standardmäßigen Xlate-Befehle pro Sitzung müssen beibehalten werden, es sei denn, es gibt einen bestimmten Grund, sie zu deaktivieren. Jede PAT-Erweiterung für eine Verbindung, bei der "xlate per session" deaktiviert ist, wird immer von der Kontrollknoteneinheit im Cluster verarbeitet, was zu Leistungseinbußen führen kann.

Hohe Nutzung des PAT-Poolbereichs aufgrund von Datenverkehr von niedrigen Ports, der ein Cluster-IP-Ungleichgewicht verursacht

Die FTD teilt eine PAT-IP in Bereiche auf und versucht, die Übersetzung im gleichen Quellbereich zu halten. Diese Tabelle zeigt, wie ein Quell-Port in einen globalen Port innerhalb desselben Quell-Bereichs umgewandelt wird.

Ursprünglicher SRC-Port	Übersetzter src-Port
1-511	1-511
512-1023	512-1023
1024-65535	1024-65535

Wenn ein Quellportbereich voll ist und ein neuer PAT-Ausdruck aus diesem Bereich zugewiesen werden muss, wechselt FTD zur nächsten IP-Adresse, um neue Übersetzungen für diesen Quellportbereich zuzuweisen.

## Symptome

Verbindungsprobleme bei NAT-Datenverkehr, der den Cluster durchquert

## Verifizierung

```
<#root>
```

```
#
```

```
show nat pool
```

FTD-Datenebenenprotokolle zeigen Erschöpfung des PAT-Pools:

```
<#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
```

## Eindämmung

Konfigurieren Sie den Bereich der flachen NAT-Ports, und schließen Sie Reserveports ein.

Darüber hinaus können Sie in Post-6.7/9.15.1 nur dann mit einer unausgewogenen Port-Block-Verteilung enden, wenn Knoten den Cluster mit großem Hintergrunddatenverkehr verlassen bzw. diesem beitreten, der PAT unterliegt. Die einzige Möglichkeit zur Wiederherstellung besteht darin, Port-Blöcke freizugeben und über mehrere Knoten neu zu verteilen.

Mit Port-Block-basierter Verteilung, wenn ein Knoten mit z. B. 10 Port-Blöcken wie pb-1, pb-2 ... pb-10 zugewiesen wird. Der Knoten beginnt immer mit dem ersten verfügbaren Port-Block und weist ihm einen zufälligen Port zu, bis er erschöpft ist. Die Zuweisung wird nur dann zum nächsten Port-Block verschoben, wenn alle Port-Blöcke bis zu diesem Punkt aufgebraucht sind.

Wenn ein Host beispielsweise 512 Verbindungen herstellt, weist die Einheit allen diesen 512 Verbindungen von pb-1 zugeordnete Ports zufällig zu. Wenn nun all diese 512 Verbindungen aktiv sind, wenn der Host die 513. Verbindung seit der Ausschöpfung von pb-1 herstellt, wechselt er zu pb-2 und weist ihm einen zufälligen Port zu. Nehmen Sie erneut an, dass von 513 Verbindungen

die 10. Verbindung beendet ist, und löschen Sie einen in pb-1 verfügbaren Port. Wenn der Host jetzt die 514. Verbindung herstellt, weist die Cluster-Einheit einen zugeordneten Port von pb-1 und nicht von pb-2 zu, da pb-1 jetzt einen freien Port hat (der im Rahmen der 10. Verbindungsentfernung freigegeben wurde).

Dabei ist zu beachten, dass die Zuweisung vom ersten verfügbaren Portblock mit freien Ports erfolgt, sodass die letzten Portblöcke in einem normal geladenen System immer zur Neuverteilung zur Verfügung stehen. Darüber hinaus wird PAT in der Regel für kurzlebige Verbindungen verwendet. Die Wahrscheinlichkeit, dass ein Port-Block in kürzerer Zeit verfügbar wird, ist sehr hoch. Der Zeitaufwand für die Poolverteilung kann sich mit der Port-Block-basierten Poolverteilung verbessern.

Falls jedoch alle Port-Blöcke, von pb-1 bis pb-10, erschöpft sind oder jeder Port-Block einen Port für eine langlebige Verbindung enthält, werden die Port-Blöcke nie schnell freigegeben und werden neu verteilt. In diesem Fall ist der am wenigsten disruptive Ansatz der:

1. Identifizieren Sie Knoten mit übermäßig großen Port-Blöcken (zeigen Sie eine Zusammenfassung des NAT-Pool-Clusters an).
2. Identifizieren Sie die am wenigsten genutzten Port-Blöcke auf diesem Knoten (zeigen Sie Details zu `nat pool ip <addr>` an).
3. Löschen Sie die `xlates` für solche Port-Blöcke (`clear xlate global <addr> gport 'start-end'`), um sie für die Neuverteilung zur Verfügung zu stellen.

---

 **Warnung:** Dadurch werden die relevanten Verbindungen unterbrochen.

---

Es kann nicht zu Dual-Channel-Websites (wie Webmail, Banking usw.) oder SSO-Websites navigiert werden, wenn die Umleitung an ein anderes Ziel erfolgt.

### Symptome

Es kann nicht zu Dual-Channel-Websites (wie Webmail, Bank-Websites usw.) gewechselt werden. Wenn ein Benutzer eine Verbindung zu einer Website herstellt, für die der Client einen zweiten Socket/eine zweite Verbindung öffnen muss, und die zweite Verbindung zu einem anderen Clustermittglied gehasht wird als der, für den die erste Verbindung gehasht wurde, und der Datenverkehr einen IP-PAT-Pool verwendet, wird der Datenverkehr vom Server zurückgesetzt, da er die Verbindung von einer anderen öffentlichen IP-Adresse empfängt.

### Verifizierung

Erfassen Sie die Cluster-Daten auf Datenebene, um zu sehen, wie der betroffene Transitfluss gehandhabt wird. In diesem Fall kommt ein TCP-Reset von der Ziel-Website.

### Risikominderung (vor 6.7/9.15.1)

- Prüfen Sie, ob Anwendungen mit mehreren Sitzungen mehrere zugeordnete IP-Adressen verwenden.
- Verwenden Sie den Befehl `show nat pool cluster summary`, um zu überprüfen, ob der Pool gleichmäßig verteilt ist.

- Verwenden Sie den Befehl `cluster exec show conn`, um zu überprüfen, ob ein angemessenes Load Balancing des Datenverkehrs vorliegt.
- Verwenden Sie den Befehl `show nat pool cluster ip <address> detail`, um die Pool-Nutzung von Sticky IP zu überprüfen.
- Aktivieren Sie Syslog 305021 (6.7/9.15), um festzustellen, für welche Verbindungen kein Sticky IP verwendet werden konnte.
- Fügen Sie dem PAT-Pool weitere IPs hinzu, oder passen Sie den Load Balancing-Algorithmus auf den verbundenen Switches an.

Informationen zum Etherchannel-Lastenausgleichsalgorithmus:

- Für Nicht-FP9300 und wenn die Authentifizierung über einen Server erfolgt: Passen Sie den Etherchannel-Lastenausgleichsalgorithmus am benachbarten Switch von Quell-IP/Port und Ziel-IP/Port zu Quell-IP und Ziel-IP an.
- Für Nicht-FP9300 und wenn die Authentifizierung über mehrere Server erfolgt: Passen Sie den Etherchannel-Lastenausgleichsalgorithmus am benachbarten Switch von Quell-IP/Port und Ziel-IP/Port zu Quell-IP an.
- Für FP9300: Auf dem FP9300-Chassis wurde der Lastenausgleichsalgorithmus als "source-dest-port source-dest-ip source-dest-mac" festgelegt und kann nicht geändert werden. Die Problemumgehung besteht in diesem Fall darin, FlexConfig zu verwenden, um der FTD-Konfiguration `xlate-per-session deny`-Befehle hinzuzufügen, um zu erzwingen, dass der Datenverkehr für bestimmte Ziel-IP-Adressen (für die problematischen/inkompatiblen Anwendungen) nur vom Steuerungsknoten im Chassis-internen Cluster verarbeitet wird. Die Problemumgehung hat folgende Nebenwirkungen:
  - Kein Load Balancing des anders übersetzten Datenverkehrs (alles wird an den Steuerungsknoten übertragen).
  - Die Möglichkeit, dass die Erweiterungssteckplätze bald erschöpft sein werden (und sich nachteilig auf die NAT-Übersetzung für anderen Datenverkehr auf dem Steuerungsknoten auswirken).
  - Reduzierte Skalierbarkeit des Chassis-internen Clusters.

Geringe Cluster-Leistung aufgrund des gesamten Datenverkehrs, der an den Steuerungsknoten gesendet wird, da nicht genügend PAT-IPs in den Pools vorhanden sind.

### Symptome

Es gibt nicht genügend PAT-IPs im Cluster, um den Datenknoten eine freie IP zuzuordnen. Daher wird der gesamte Datenverkehr, der der PAT-Konfiguration unterliegt, zur Verarbeitung an den Steuerungsknoten weitergeleitet.

### Verifizierung

Verwenden Sie den Befehl `show nat pool cluster`, um die Zuweisungen für jede Einheit anzuzeigen und zu bestätigen, dass alle Einheiten mindestens eine IP im Pool besitzen.

### Eindämmung

Für die Versionen vor 6.7/9.15.1 muss ein PAT-Pool mit einer Größe vorhanden sein, die

mindestens der Anzahl der Knoten im Cluster entspricht. In einem PAT-Pool nach 6.7/9.15.1 weisen Sie Port-Blöcke von allen PAT-Pool-IPs zu. Wenn die PAT-Poolnutzung sehr hoch ist, was zu einer häufigen Erschöpfung des Pools führt, müssen Sie die PAT-Poolgröße erhöhen (siehe Abschnitt FAQ).

Die Leistung ist gering, da der gesamte Datenverkehr an den Steuerungsknoten gesendet wird, da XLATE nicht pro Sitzung aktiviert ist.

## Symptome

Über den Cluster-Kontrollknoten werden viele Hochgeschwindigkeits-UDP-Backup-Datenströme verarbeitet, was sich auf die Leistung auswirken kann.

## Hintergrund

Nur Verbindungen mit aktivierten XLATE pro Sitzung können von einem Datenknoten verarbeitet werden, der PAT verwendet. Verwenden Sie den Befehl `show run all xlate`, um die xlate-Konfiguration pro Sitzung anzuzeigen.

Bei Aktivierung pro Sitzung wird der Xlate sofort beendet, wenn die zugehörige Verbindung beendet wird. Dadurch wird die Leistung der Verbindung pro Sekunde verbessert, wenn die Verbindungen einer PAT unterzogen werden. Nicht-pro-Sitzung läuft weitere 30 Sekunden, nachdem die zugehörige Verbindung getrennt wurde. Wenn die Verbindungsrate hoch genug ist, können die 65.000 TCP/UDP-Ports auf jeder globalen IP-Adresse in kurzer Zeit belegt werden.

Standardmäßig ist der gesamte TCP-Datenverkehr per Xlate aktiviert, und nur UDP DNS-Datenverkehr pro Sitzung ist aktiviert. Dies bedeutet, dass der gesamte UDP-Datenverkehr, der nicht DNS ist, zur Verarbeitung an den Steuerungsknoten weitergeleitet wird.

## Verifizierung

Verwenden Sie diesen Befehl, um die Verbindung und die Paketverteilung zwischen den Cluster-Einheiten zu überprüfen:

```
<#root>
```

```
firepower#
```

```
show cluster info conn-distribution
```

```
firepower#
```

```
show cluster info packet-distribution
```

```
firepower#
```

```
show cluster info load-monitor
```

Verwenden Sie den Befehl `cluster exec show conn`, um zu sehen, welche Cluster-Knoten



Eigentümer der UDP-Verbindungen sind.

```
<#root>
```

```
firepower#
```

```
cluster exec show conn
```

Verwenden Sie diesen Befehl, um die Pool-Nutzung über Cluster-Knoten hinweg zu verstehen.

```
<#root>
```

```
firepower#
```

```
cluster exec show nat pool ip
```

```
| in UDP
```

## Eindämmung

Konfigurieren Sie sitzungsbasierte PAT (Befehl pro Sitzung `permit udp`) für den relevanten Datenverkehr (z. B. UDP). Für ICMP können Sie die standardmäßige Multi-Session-PAT nicht ändern. ICMP-Datenverkehr wird daher immer vom Steuerungsknoten verarbeitet, wenn PAT konfiguriert ist.

Die Verteilung des PAT-Pools ist unausgewogen, wenn Knoten den Cluster verlassen oder ihm beitreten.

## Symptome

- Verbindungsprobleme, da die PAT-IP-Zuweisung im Laufe der Zeit aufgrund von Einheiten, die den Cluster verlassen und ihm beitreten, zu einem Ungleichgewicht werden kann.
- Nach 6.7/9.15.1 kann es Fälle geben, in denen der neu verbundene Knoten nicht genügend Portblöcke erhält. Ein Knoten ohne Port-Block leitet den Datenverkehr zum Steuerungsknoten um. Ein Knoten mit mindestens einem Port-Block verarbeitet den Datenverkehr und verwirft ihn, sobald der Pool aufgebraucht ist.

## Verifizierung

- Die Syslogs der Datenebene enthalten Meldungen wie:

<#root>

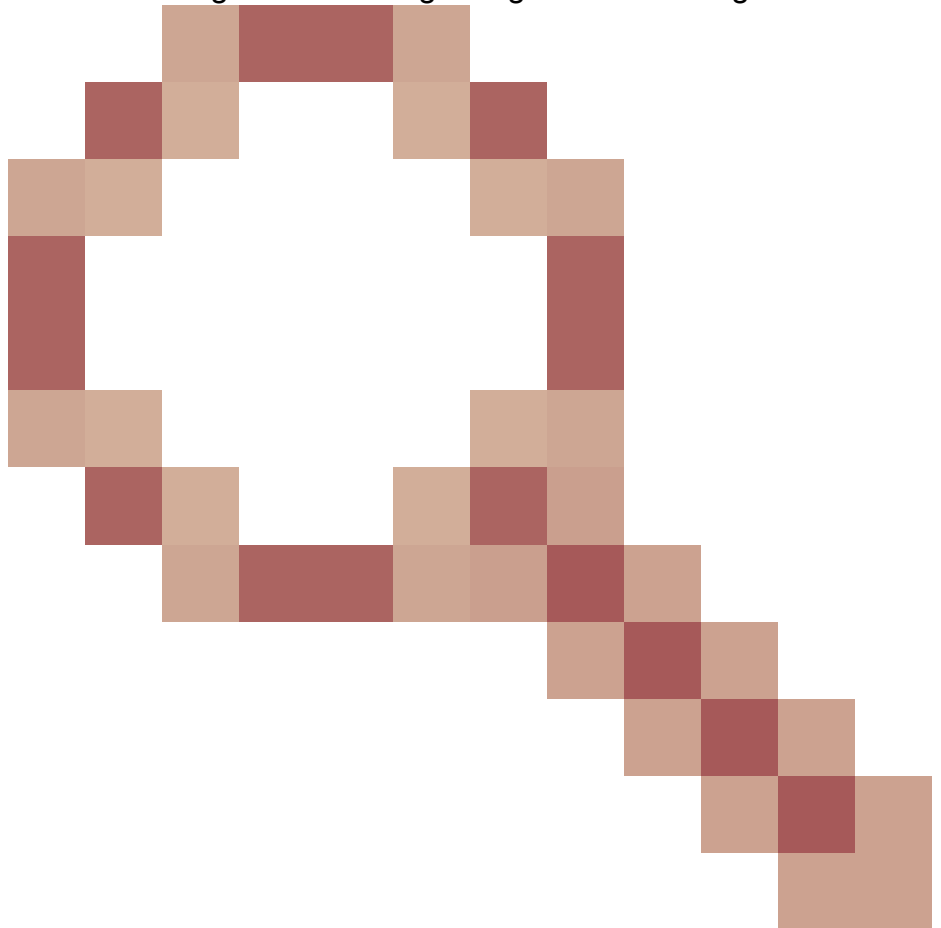
%ASA-3-202010:

```
NAT pool exhausted. Unable to create TCP connection
from inside:192.0.2.1/2239 to outside:192.0.2.150/80
```

- Verwenden Sie den Befehl `show nat pool cluster summary`, um die Poolverteilung zu identifizieren.
- Verwenden Sie den Befehl `cluster exec show nat pool ip <addr> detail`, um die Pool-Nutzung über Cluster-Knoten hinweg zu verstehen.

### Eindämmung

- Für die Version vor 6.7/9.15.1 werden einige Problemumgehungen in Cisco Bug-ID



[CSCvd10530](#) beschrieben.

- In post-6.7/9.15.1 verwenden Sie den Befehl `clear xlate global <ip> gport <start-end>`, um einige der Port-Blöcke auf anderen Knoten manuell zu löschen und sie an die erforderlichen Knoten weiterzuverteilen.

### Symptome

Wichtigste Verbindungsprobleme für den vom Cluster per PAT weitergeleiteten Datenverkehr Der Grund hierfür ist, dass die FTD-Datenebene gemäß Design kein GARP für globale NAT-Adressen sendet.

## Verifizierung

Die ARP-Tabelle der direkt verbundenen Geräte zeigt nach einem Wechsel des Kontrollknotens eine andere MAC-Adresse der Cluster-Datenschnittstelle:

```
<#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
```

## Eindämmung

Konfigurieren Sie statische (virtuelle) MACs auf Cluster-Datenschnittstellen.

## PAT-ausgefallene Verbindungen

## Symptome

Verbindungsprobleme für Datenverkehr, der vom Cluster per PAT geleitet wird

## Überprüfung/Problembehebung

- Stellen Sie sicher, dass die Konfiguration ordnungsgemäß repliziert wird.
- Stellen Sie sicher, dass der Pool gleichmäßig verteilt ist.
- Stellen Sie sicher, dass Pooleigentum gültig ist.
- Keine Inkremente des Fehlerzählers in der Anzeige des ASP-Clusterzählers.
- Stellen Sie sicher, dass Director-/Forwarder-Flows mit den richtigen Informationen erstellt werden.
- Validieren Sie, ob Backup-Xlate wie erwartet erstellt, aktualisiert und bereinigt werden.
- Validieren Sie, ob XLATE gemäß dem Verhalten "pro Sitzung" erstellt und beendet werden.
- Aktivieren Sie "debug nat 2", um auf Fehler hinzuweisen. Beachten Sie, dass diese Ausgabe

sehr laut sein kann, zum Beispiel:

```
<#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
```

So beenden Sie das Debuggen:

```
<#root>
firepower#
un all
```

- Aktivieren Sie verbindungsbezogene und NAT-bezogene Syslogs, um die Informationen mit einer fehlerhaften Verbindung in Beziehung zu setzen.

Verbesserungen bei ASA- und FTD-Clustering-PAT (nach 9.15 und 6.7)

Was hat sich geändert?

Der PAT-Betrieb wurde neu konzipiert. Die einzelnen IPs werden nicht mehr auf die einzelnen Cluster-Mitglieder verteilt. Stattdessen werden die PAT-IP(s) in Port-Blöcke aufgeteilt und diese Port-Blöcke gleichmäßig (so weit wie möglich) zwischen den Cluster-Elementen in Kombination mit dem IP-Stickiness-Betrieb verteilt.

Das neue Design geht diese Einschränkungen an (siehe vorigen Abschnitt):

- Anwendungen mit mehreren Sitzungen sind betroffen, da keine clusterweite IP-Stickiness vorliegt.
- Es ist ein PAT-Pool erforderlich, dessen Größe mindestens der Anzahl der Knoten im Cluster entspricht.
- Die Verteilung des PAT-Pools ist unausgewogen, wenn Knoten den Cluster verlassen oder ihm beitreten.
- Keine Syslogs zur Anzeige eines PAT-Pool-Ungleichgewichts

Technisch gesehen gibt es anstelle der Standardportbereiche 1-511, 512-1023 und 1024-65535 jetzt 1024-65535 als Standardportbereich für PAT. Dieser Standardbereich kann erweitert werden, um den privilegierten Port-Bereich 1-1023 für reguläre PAT einzubeziehen (Option "include-reserve").

Dies ist ein Beispiel für eine PAT-Pool-Konfiguration in FTD 6.7. Weitere Details finden Sie im entsprechenden Abschnitt im Konfigurationsleitfaden:

**NAT Rule:**  
Manual NAT Rule

**Insert:**  
In Category NAT Rules Before

**Type:**  
Dynamic

Enable

Description:

Interface Objects Translation PAT Pool Advanced

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

Interface Objects Translation **PAT Pool** Advanced

Enable PAT Pool

PAT:

Address  +

Use Round Robin Allocation

Extended PAT Table

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

Include Reserve Ports

Block Allocation

## Zusätzliche Informationen zur Fehlerbehebung in Bezug auf PAT

### FTD-Syslogs auf Datenebene (nach 6.7/9.15.1)

Ein Syslog für die Stickiness-Ungültigerklärung wird generiert, wenn alle Ports in der Sticky IP auf einem Clusterknoten aufgebraucht sind und die Zuweisung zur nächsten verfügbaren IP mit freien Ports verschoben wird. Beispiel:

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

Ein Pool-Ungleichgewicht-Syslog wird auf einem Knoten generiert, wenn dieser dem Cluster beitrifft, und erhält keinen oder einen ungleichen Anteil an Portblöcken. Beispiel:

```
%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 have
```

## Show-Befehle

### Poolverteilungsstatus

In der Ausgabe von `show nat pool cluster summary` darf es für jede PAT-IP-Adresse in einem Verteilungsszenario mit ausgewogener Verteilung keinen Unterschied von mehr als einem Port-Block über die Knoten geben. Beispiele für eine ausgewogene und unausgewogene Portblockverteilung.

```
<#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)
```

Unausgewogene Verteilung:

```
<#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 /
```

```
22 / 38
```

```
/ 36)
```

Pooleigentumsstatus

In der Ausgabe von show nat pool cluster darf es keinen einzigen Port-Block geben, dessen Besitzer oder Backup UNBEKANNT ist. Wenn ein Problem auftritt, weist es auf ein Problem mit der Pooleigentumskommunikation hin. Beispiel:

```
<#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>
```

## Verbuchung von Hafenzuweisungen in Hafenblöcken

Der Befehl `show nat pool` wurde um zusätzliche Optionen zur Anzeige detaillierter Informationen sowie gefilterter Ausgaben erweitert. Beispiel:

```
<#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 *
```

"\*" bedeutet, dass es sich um einen gesicherten Port-Baustein handelt.

Verwenden Sie den Befehl `clear xlate global <ip> gport <start-end>`, um einige der Port-Blöcke auf anderen Knoten manuell zu löschen und sie an die erforderlichen Knoten weiterzuverteilen.

## Manuell ausgelöste Neuverteilung von Port-Blöcken

- In einem Produktionsnetzwerk mit konstantem Datenverkehr kann es vorkommen, dass ein Knoten beim Verlassen des Clusters und bei einem erneuten Verbinden mit dem Cluster (möglicherweise aufgrund eines Tracebacks) nicht den gleichen Anteil am Pool erhält oder im schlimmsten Fall keinen Port-Block erhält.
- Verwenden Sie den Befehl `show nat pool cluster summary`, um zu ermitteln, welcher Knoten mehr Port-Blöcke besitzt als erforderlich.
- Verwenden Sie für Knoten mit mehr Port-Blöcken den Befehl `show nat pool ip <addr> detail`, um die Port-Blöcke mit der geringsten Anzahl an Zuweisungen zu ermitteln.
- Mit dem Befehl `clear xlate global <address> gport <start-end>` können Sie Übersetzungen löschen, die aus diesen Portblöcken erstellt wurden, sodass sie für die Neuverteilung an die erforderlichen Knoten zur Verfügung stehen. Beispiel:

```
<#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
```

## Häufig gestellte Fragen (FAQs) zur PAT nach 6.7/9.15.1

Frage: Falls Sie über die Anzahl der verfügbaren IPs für die Anzahl der verfügbaren Einheiten im Cluster verfügen, können Sie weiterhin eine IP pro Einheit als Option verwenden?

Antwort: Dies ist nicht mehr der Fall, und es gibt keinen Umschalter zwischen IP-Adressen- und Port-Block-basierten Poolverteilungsschemata.

Das ältere Schema der IP-Adressen-basierten Poolverteilung führte zu Anwendungsfehlern bei mehreren Sitzungen, bei denen mehrere Verbindungen (die Teil einer einzelnen Anwendungstransaktion sind) von einem Host auf verschiedene Knoten des Clusters ausbalanciert und so durch verschiedene zugeordnete IP-Adressen übersetzt werden, was dazu führt, dass der Zielservice sie als von verschiedenen Einheiten bezogen ansieht.

Und mit dem neuen Port-Block-basierten Verteilungsschema wird es immer empfohlen, genügend PAT-IP-Adressen zu haben, basierend auf der Anzahl der Verbindungen, die mit PAT verbunden werden müssen, auch wenn Sie jetzt mit nur einer einzigen PAT-IP-Adresse arbeiten können.

Frage: Können Sie weiterhin über einen Pool von IP-Adressen für den PAT-Pool für den Cluster verfügen?

A. Ja, das können Sie. Port-Blöcke aller PAT-Pool-IPs werden über die Cluster-Knoten verteilt.

Frage: Wenn Sie eine Anzahl von IP-Adressen für den PAT-Pool verwenden, wird dann der gleiche Port-Block für jedes Mitglied pro IP-Adresse angegeben?

A. Nein, jede IP wird unabhängig voneinander verteilt.

Frage: Alle Cluster-Knoten haben alle öffentlichen IPs, aber nur eine Teilmenge der Ports? Wenn dies der Fall ist, wird dann sichergestellt, dass jedes Mal, wenn die Quell-IP dieselbe öffentliche IP verwendet?

A. Das ist richtig. Jede PAT-IP gehört teilweise jedem Knoten. Wenn eine ausgewählte öffentliche IP-Adresse auf einem Knoten erschöpft ist, wird ein Syslog generiert, das anzeigt, dass die statische IP-Adresse nicht beibehalten werden kann, und die Zuweisung wird zur nächsten verfügbaren öffentlichen IP-Adresse verschoben. Ob Standalone-, HA- oder Cluster-

Bereitstellung, IP-Stickiness wird immer nach bestem Wissen und Gewissen bereitgestellt, je nach Verfügbarkeit des Pools.

Frage: Basiert alles auf einer einzigen IP-Adresse im PAT-Pool, gilt jedoch nicht, wenn mehr als eine IP-Adresse im PAT-Pool verwendet wird?

Antwort: Sie gilt auch für mehrere IP-Adressen im PAT-Pool. Port-Blöcke von jeder IP im PAT-Pool werden über Cluster-Knoten verteilt. Jede IP-Adresse im PAT-Pool wird auf alle Mitglieder im Cluster aufgeteilt. Wenn Sie also eine Klasse C von Adressen im PAT-Pool haben, hat jedes Cluster-Mitglied Port-Pools von jeder der PAT-Pool-Adressen.

Frage: Funktioniert die Lösung mit CGNAT?

Antwort: Ja, CGNAT wird ebenfalls unterstützt. CGNAT, auch als Block-Allocation-PAT bezeichnet, hat eine Standardblockgröße von '512', die über die CLI der Xlate-Blockallokationsgröße geändert werden kann. Bei regulärer dynamischer PAT (nicht CGNAT) ist die Blockgröße immer '512', was fest und nicht konfigurierbar ist.

F. Weist der Steuerungsknoten den Port-Blockbereich anderen Einheiten zu oder behält er ihn bei, wenn das Gerät den Cluster verlässt?

Antwort: Jeder Port-Baustein verfügt über einen Eigentümer und ein Backup. Jedes Mal, wenn ein Xlate aus einem Port-Block erstellt wird, wird er auch auf den Backup-Knoten des Port-Blocks repliziert. Wenn ein Knoten den Cluster verlässt, besitzt der Backup-Knoten alle Port-Blöcke und alle aktuellen Verbindungen. Da der Backup-Knoten zum Eigentümer dieser zusätzlichen Port-Blöcke geworden ist, wählt er ein neues Backup für diese Blöcke aus und repliziert alle aktuellen Xlate auf diesen Knoten, um Ausfallszenarien zu bewältigen.

F. Welche Maßnahmen können auf der Grundlage dieser Warnung ergriffen werden, um die Einhaltung der Vorschriften durchzusetzen?

A. Es gibt zwei mögliche Gründe, warum Klebrigkeit nicht erhalten werden kann.

Grund 1: Der Datenverkehr ist nicht korrekt ausgeglichen, wodurch einer der Knoten eine höhere Anzahl von Verbindungen sieht als andere, was zu der jeweiligen klebrigen IP-Erschöpfung führt. Dies kann erreicht werden, wenn sichergestellt ist, dass der Datenverkehr gleichmäßig auf die Cluster-Knoten verteilt wird. Optimieren Sie beispielsweise auf einem FPR41xx-Cluster den Lastenausgleichsalgorithmus auf verbundenen Switches. Stellen Sie in einem FPR9300-Cluster sicher, dass die Anzahl der Blades im Chassis gleich ist.

Grund 2: Die Nutzung des PAT-Pools ist sehr hoch, was zu einer häufigen Erschöpfung des Pools führt. Um diesem Problem zu begegnen, muss die Größe des PAT-Pools erhöht werden.

Frage: Wie wird die Unterstützung für das erweiterte Schlüsselwort gehandhabt? Zeigt es einen Fehler an und verhindert, dass der gesamte NAT-Befehl während des Upgrades hinzugefügt wird, oder entfernt es das erweiterte Schlüsselwort und zeigt eine Warnung an?

A. Die erweiterte PAT-Option wird im Cluster ab ASA 9.15.1/FP 6.7 nicht unterstützt. Die Konfigurationsoption wird nicht aus der CLI/ASDM/CSM/FMC entfernt. Bei einer Konfiguration

(direkt oder indirekt über ein Upgrade) erhalten Sie eine Warnmeldung, und die Konfiguration wird akzeptiert, aber die erweiterte Funktionalität von PAT ist nicht aktiv.

Frage: Entspricht die Anzahl der Übersetzungen der Anzahl der gleichzeitigen Verbindungen?

A. In der Zeit vor 6.7/9.15.1, obwohl es 1-65535 war, da die Quellports nie viel im Bereich 1-1024 verwendet werden, macht es effektiv 1024-65535 (64512 Verbindungen). In der Implementierung nach 6.7/9.15.1 mit 'flat' als Standardverhalten ist es 1024-65535. Wenn Sie jedoch die 1-1024 verwenden möchten, können Sie die Option "include-reserve" verwenden.

F. Wenn der Knoten wieder dem Cluster beitrifft, hat er den alten Backup-Knoten als Backup und dieser Backup-Knoten gibt ihm seinen alten Port-Block?

Antwort: Das hängt von der Verfügbarkeit der jeweiligen Port-Blöcke ab. Wenn ein Knoten den Cluster verlässt, werden alle seine Port-Blöcke auf den Backup-Knoten verschoben. Es ist dann der Kontrollknoten, der freie Port-Blöcke ansammelt und sie an die erforderlichen Knoten verteilt.

F. Wird bei einer Zustandsänderung des Kontrollknotens ein neuer Kontrollknoten ausgewählt, die PAT-Blockzuweisung beibehalten oder werden die Portblöcke basierend auf dem neuen Kontrollknoten neu zugewiesen?

A. Der neue Steuerknoten versteht, welche Blöcke zugewiesen wurden und welche frei sind und beginnt von dort.

Frage: Entspricht die maximale Anzahl von Xlates der maximalen Anzahl gleichzeitiger Verbindungen mit diesem neuen Verhalten?

A: Ja. Die maximale Anzahl von Xlate hängt von der Verfügbarkeit der PAT-Ports ab. Es hat nichts mit der maximalen Anzahl gleichzeitiger Verbindungen zu tun. Wenn Sie nur eine Adresse zulassen, haben Sie 65535 mögliche Verbindungen. Wenn Sie mehr benötigen, müssen Sie mehr IP-Adressen zuweisen. Wenn genügend Adressen/Ports vorhanden sind, können Sie die maximale Anzahl gleichzeitiger Verbindungen erreichen.

Frage: Wie erfolgt die Portblockzuweisung, wenn ein neues Clustermitglied hinzugefügt wird? Was passiert, wenn ein Clustermitglied nach einem Neustart hinzugefügt wird?

A. Portblöcke werden immer vom Kontrollknoten verteilt. Portblöcke werden einem neuen Knoten nur dann zugewiesen, wenn freie Portblöcke vorhanden sind. Freie Port-Blöcke bedeuten, dass keine Verbindung über einen zugeordneten Port innerhalb des Port-Blocks bereitgestellt wird.

Außerdem berechnet jeder Knoten beim erneuten Verbinden die Anzahl der Blöcke neu, die er besitzen kann. Hält ein Knoten mehr Blöcke, als er eigentlich sollte, gibt er diese zusätzlichen Portblöcke an den Kontrollknoten frei, sobald sie verfügbar sind. Der Steuerknoten weist sie dann dem neu verknüpften Datenknoten zu.

Frage: Wird es nur von TCP- und UDP-Protokollen oder auch von SCTP unterstützt?

A. SCTP wurde von dynamischer PAT nie unterstützt. Für SCTP-Datenverkehr wird empfohlen, nur ein statisches Netzwerkobjekt (NAT) zu verwenden.

F. Wenn einem Knoten die Blockports ausgehen, werden Pakete verworfen und der nächste verfügbare IP-Block nicht verwendet?

A. Nein, es fällt nicht sofort. Dabei werden die verfügbaren Port-Blöcke der nächsten PAT-IP verwendet. Wenn alle Port-Blöcke über alle PAT-IPs ausgeschöpft werden, wird der Datenverkehr verworfen.

F. Wäre es besser, eine neue Steuerung früher manuell auszuwählen (z. B. nach der Hälfte eines 4-Einheiten-Cluster-Upgrades), anstatt darauf zu warten, dass alle Verbindungen auf dem Steuerknoten verarbeitet werden, um die Überlastung des Steuerknotens in einem Cluster-Upgrade-Fenster zu vermeiden?

A. Das Steuerelement muss zuletzt aktualisiert werden. Dies liegt daran, dass der Kontrollknoten, wenn er die neuere Version ausführt, die Poolverteilung nur initiiert, wenn alle Knoten die neuere Version ausführen. Wenn ein Upgrade ausgeführt wird, ignorieren darüber hinaus alle Datenknoten mit einer neueren Version Poolverteilungsnachrichten von einem Steuerknoten, wenn dieser eine ältere Version ausführt.

Um dies im Detail zu erläutern, sollten Sie eine Cluster-Bereitstellung mit vier Knoten A, B, C und D mit A als Steuerung in Betracht ziehen. Nachfolgend sind die typischen Upgrade-Schritte bei laufendem Betrieb aufgeführt:

1. Laden Sie eine neue Version auf jeden Knoten herunter.
2. Einheit "D" neu laden. Alle Verbindungen, xlates werden in den Backup-Knoten verschoben.
3. Einheit "D" erscheint und:

antwort: Verarbeitung der PAT-Konfiguration

b. Unterteilt jede PAT-IP in Port-Blöcke

c. Hat alle Port-Blöcke in nicht zugewiesenem Zustand

d. Ignoriert ältere Version der Cluster-PAT-Nachrichten, die von der Steuerung empfangen wurden

e. Leitet alle PAT-Verbindungen zu Primary um.

4. Ähnlich, bringen Sie andere Knoten mit der neuen Version.

5. Regelung der Einheit "A" neu laden. Da kein Backup für die Steuerung vorhanden ist, werden alle vorhandenen Verbindungen getrennt

6. Das neue Steuerelement startet die Verteilung von Port-Blöcken im neueren Format.

7. Einheit "A" schließt sich erneut an und kann Verteilungsnachrichten für Port-Blöcke annehmen und darauf reagieren.

Fragment-Handling

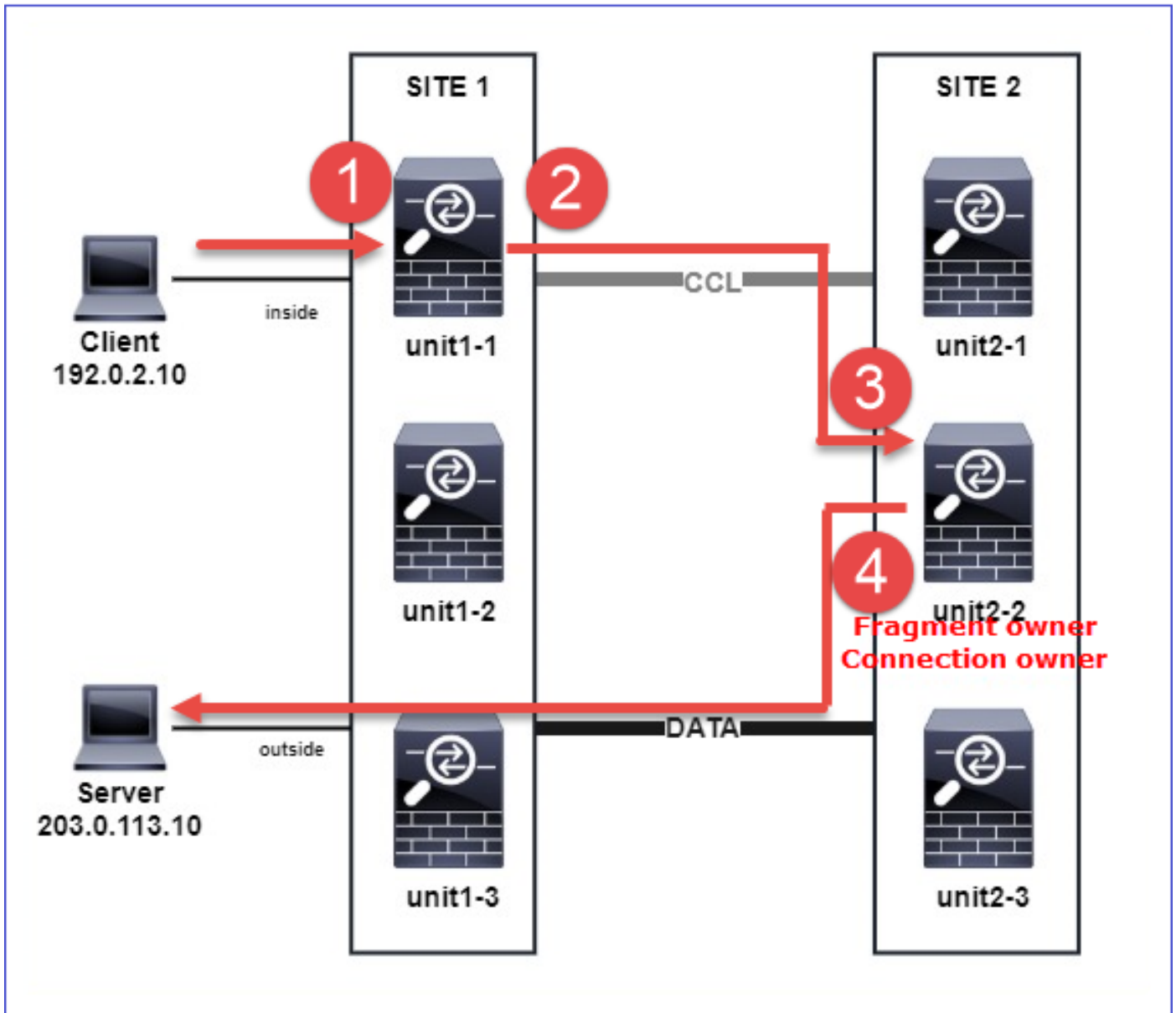
Symptom

In standortübergreifenden Cluster-Bereitstellungen können fragmentierte Pakete, die an einem bestimmten Standort (standortlokaler Datenverkehr) verarbeitet werden müssen, weiterhin an die Einheiten an anderen Standorten gesendet werden, da einer dieser Standorte über den Besitzer des Fragments verfügen kann.

In der Clusterlogik wird eine zusätzliche Rolle für Verbindungen mit fragmentierten Paketen definiert: Fragmenteigentümer.

Bei fragmentierten Paketen bestimmen Clustereinheiten, die ein Fragment empfangen, einen Fragmenteigentümer auf der Grundlage eines Hashs der Quell-IP-Adresse des Fragments, der Ziel-IP-Adresse und der Paket-ID. Alle Fragmente werden dann über die Cluster-Steuerungsverbindung an den Fragmentbesitzer weitergeleitet. Fragmente können mit Lastausgleich auf verschiedene Cluster-Einheiten verteilt werden, da nur das erste Fragment das 5-Tupel enthält, das im Lastausgleich-Hash des Switches verwendet wird. Andere Fragmente enthalten keine Quell- und Ziel-Ports und können auf andere Cluster-Einheiten mit Lastausgleich verteilt werden. Der Fragmenteigentümer reassembliert das Paket vorübergehend, sodass er den Director anhand eines Hashs der Quell-/Ziel-IP-Adresse und der Ports bestimmen kann. Wenn es sich um eine neue Verbindung handelt, wird der Fragmenteigentümer zum Verbindungseigentümer. Wenn es sich um eine bestehende Verbindung handelt, leitet der Fragmentbesitzer alle Fragmente über die Clustersteuerungsverbindung an den Verbindungsbesitzer weiter. Der Verbindungseigentümer reassembliert dann alle Fragmente.

Betrachten Sie diese Topologie mit dem Fluss einer fragmentierten ICMP-Echoanfrage vom Client zum Server:



Um die Reihenfolge der Vorgänge zu verstehen, gibt es clusterweite Paketerfassungen auf der Innen- und Außenseite und Cluster Control Link-Schnittstellen, die mit der Trace-Option konfiguriert sind. Außerdem wird auf der Innen-Schnittstelle eine Paketerfassung mit der Option reject-hide konfiguriert.

```
<#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
```

Reihenfolge der Vorgänge im Cluster:

1. Unit-1-1 an Standort 1 empfängt die fragmentierten ICMP-Echoanforderungspakete.

```
<#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 wählt unit-2-2 an Standort 2 als Fragmenteigentümer aus und sendet fragmentierte Pakete an diesen.

Die Ziel-MAC-Adresse der von Gerät 1-1 an Gerät 2-2 gesendeten Pakete ist die MAC-Adresse der CCL-Verbindung in Gerät 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 empfängt die fragmentierten Pakete, setzt sie wieder zusammen und wird zum Eigentümer des Datenflusses.

```
<#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 capcc1 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 lässt die Pakete gemäß der Sicherheitsrichtlinie zu und sendet sie über die externe Schnittstelle von Standort 2 an Standort 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

## Beobachtungen/Hinweise

- Anders als die Direktorenrolle kann der Fragmentbesitzer nicht innerhalb einer bestimmten Site lokalisiert werden. Der Fragmenteigentümer wird durch die Einheit bestimmt, die ursprünglich die fragmentierten Pakete einer neuen Verbindung empfängt und sich an einem beliebigen Standort befinden kann.
- Da ein Fragmenteigentümer auch zum Verbindungseigentümer werden kann, muss er, um die Pakete an den Zielhost weiterzuleiten, in der Lage sein, die Ausgangsschnittstelle

aufzulösen und die IP- und MAC-Adressen des Zielhosts oder des nächsten Hop zu finden. Dies setzt voraus, dass der/die nächste(n) Hop(s) auch für den Ziel-Host erreichbar sein muss/müssen.

- Um die fragmentierten Pakete wieder zusammenzufassen, unterhält die ASA/FTD für jede benannte Schnittstelle ein Modul zur Reassemblierung von IP-Fragmenten. Um die Betriebsdaten des Reassemblierungsmoduls für IP-Fragment anzuzeigen, verwenden Sie den Befehl `show fragment`:

```
<#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 Clusterbereitstellungen werden die fragmentierten Pakete vom Fragmenteigentümer oder Verbindungsbesitzer in die Fragmentwarteschlange gestellt. Die Größe der Fragmentwarteschlange wird durch den Wert des Größenzählers (standardmäßig 200) begrenzt, der mit dem Befehl `fragmentgröße <size> <nameif>` konfiguriert wird. Wenn die Größe der Fragmentwarteschlange 2/3 der Größe erreicht, wird angenommen, dass der Schwellenwert für Fragmentwarteschlangen überschritten wird, und alle neuen Fragmente, die nicht Teil der aktuellen Fragmentkette sind, werden verworfen. In diesem Fall wird der Grenzwert für die Fragmentwarteschlange überschritten, und die Syslog-Meldung FTD-3-209006 wird generiert.

```
<#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 203.0.113.1

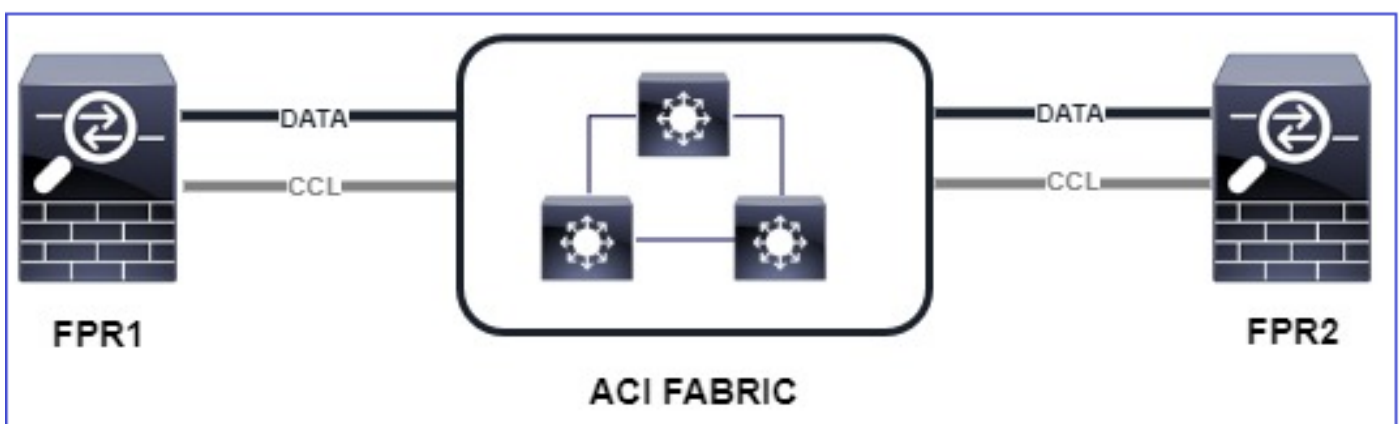
Erhöhen Sie zur Problemumgehung die Größe in FirePOWER Management Center > Devices > Device Management > [Edit Device] > Interfaces > [Interface] > Advanced > Security Configuration > Override Default Fragment Setting, speichern Sie die Konfiguration, und stellen Sie Richtlinien bereit. Überwachen Sie dann den Queue-Zähler in der Befehlsausgabe show fragment (Fragment anzeigen) und das Auftreten der Syslog-Meldung FTD-3-209006.

## ACI-Probleme

Intermittierende Verbindungsprobleme im Cluster aufgrund der aktiven L4-Prüfsummenüberprüfung im ACI-POD

### Symptom

- Intermittierende Verbindungsprobleme durch den ASA-/FTD-Cluster, der in einem ACI-POD bereitgestellt wird.
- Wenn sich nur eine Einheit im Cluster befindet, werden die Verbindungsprobleme nicht beobachtet.
- Pakete, die von einer Cluster-Einheit an eine oder mehrere andere Einheiten im Cluster gesendet werden, sind in den FXOS- und Datenebenenerfassungen der Zieleinheiten nicht sichtbar.



### Eindämmung

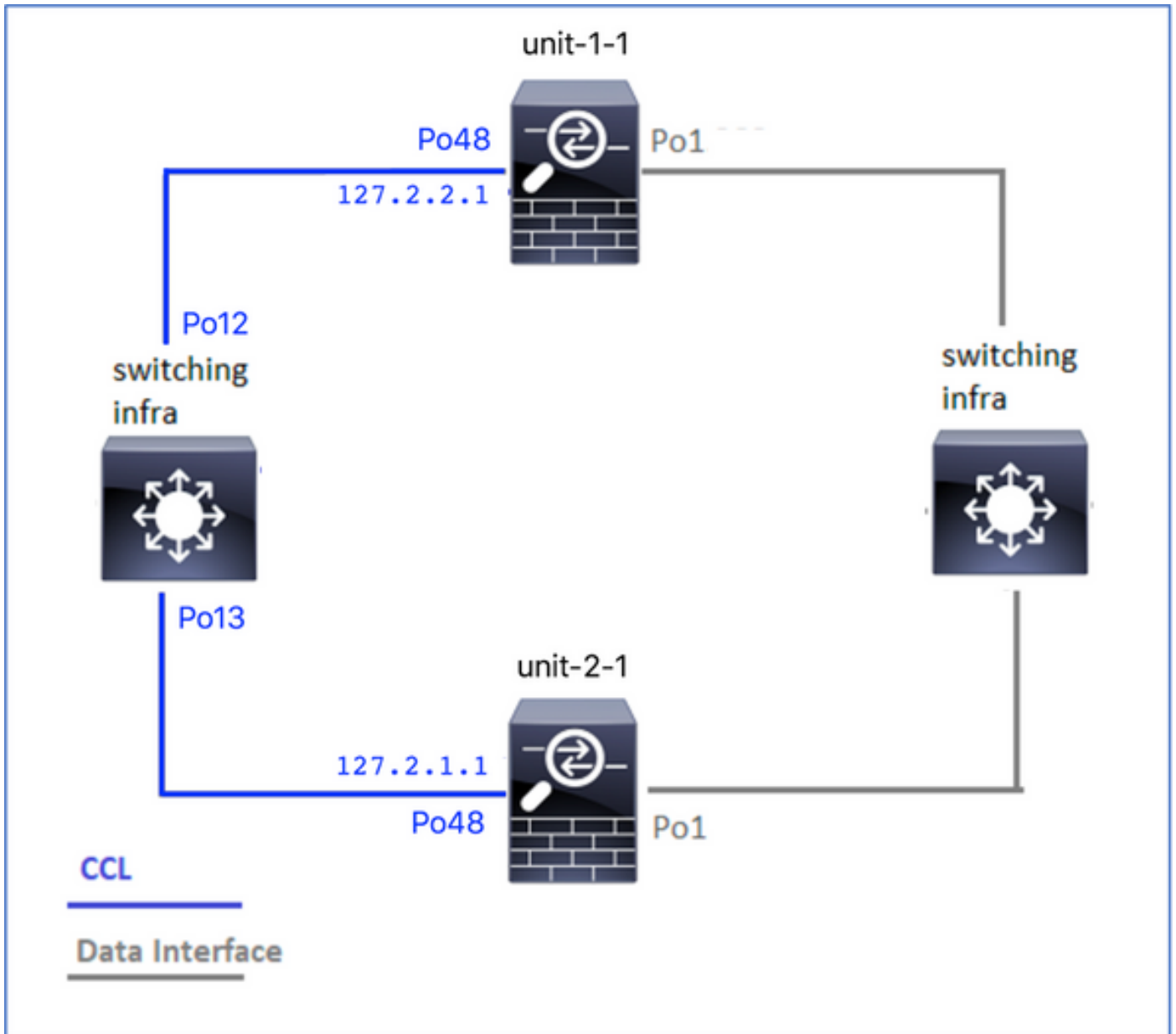
- Der umgeleitete Datenverkehr über die Cluster-Steuerungsverbindung hat keine richtige L4-Prüfsumme, und dieses Verhalten wird erwartet. Switches auf dem Verbindungspfad für die Cluster-Steuerung dürfen die L4-Prüfsumme nicht überprüfen. Switches, die die L4-Prüfsumme überprüfen, können dazu führen, dass Datenverkehr verworfen wird. Überprüfen Sie die ACI Fabric Switch-Konfiguration, und stellen Sie sicher, dass keine L4-Prüfsumme

für empfangene oder gesendete Pakete über die Cluster Control Link ausgeführt wird.

## Probleme mit der Cluster-Kontrollebene

Einheit kann nicht am Cluster teilnehmen

MTU-Größe auf CCL



## Symptome

Die Einheit kann dem Cluster nicht beitreten. Es wird folgende Meldung angezeigt:

```
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
```

## Überprüfung/Problembehebung

- Verwenden Sie den Befehl `show interface` auf dem FTD, um sicherzustellen, dass die MTU auf der Cluster Control Link-Schnittstelle mindestens 100 Byte höher ist als die MTU der Datenschnittstelle:

```
<#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.
```

- Führen Sie einen Ping über den CCL mit der Größenoption aus, um zu überprüfen, ob die Konfiguration für die CCL-MTU auf allen Geräten im Pfad korrekt ist.

```
<#root>
firepower#
ping 127.2.1.1 size 9184
```

- Überprüfen der MTU-Konfiguration mit dem Befehl show interface auf dem Switch

```
<#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
```

## Schnittstellenkonflikt zwischen Cluster-Einheiten

### Symptome

Die Einheit kann dem Cluster nicht beitreten. Es wird folgende Meldung angezeigt:

```
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 error)  
All data interfaces have been shutdown due to clustering being disabled. To recover either enable cluster
```

### Überprüfung/Problembehebung

Melden Sie sich an der FCM-GUI jedes Chassis an, navigieren Sie zur Registerkarte Interfaces (Schnittstellen), und überprüfen Sie, ob alle Cluster-Mitglieder über dieselbe Schnittstellenkonfiguration verfügen:

- Schnittstellen, die dem logischen Gerät zugewiesen sind



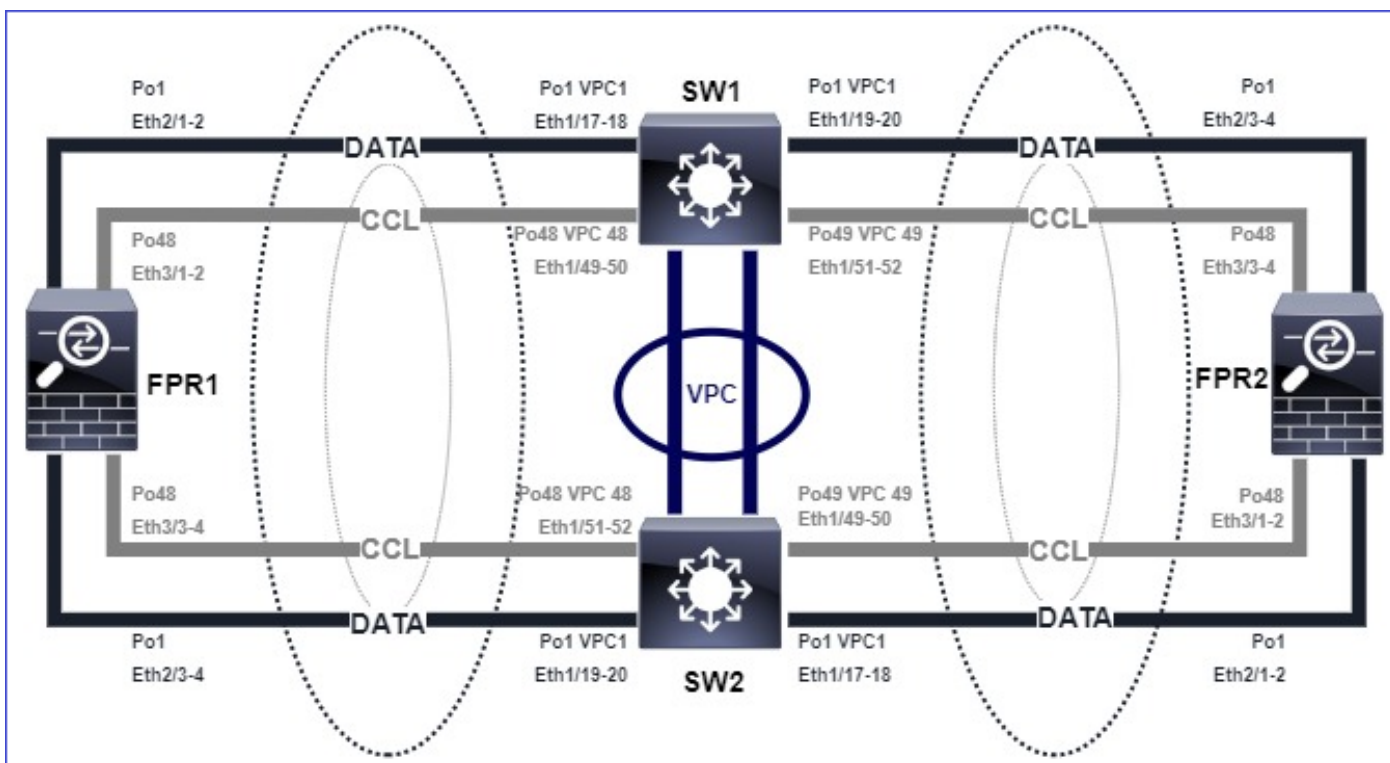
- Admin-Geschwindigkeit der Schnittstellen
- Admin-Duplex der Schnittstellen
- Schnittstellenstatus

Problem mit der Daten-/Port-Channel-Schnittstelle

Split-Brain aufgrund von Erreichbarkeitsproblemen über den CCL

Symptom

Es gibt mehrere Steuereinheiten im Cluster. Betrachten Sie diese 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

## Verifizierung

- Verwenden Sie den Befehl ping, um die Verbindung zwischen den IP-Adressen der Steuereinheit für die Cluster Control Link (CCL) zu überprüfen:

<#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)

- Prüfen Sie die ARP-Tabelle:

<#root>

```
firepower# show arp
```

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

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

- Konfigurieren und überprüfen Sie in den Steuergeräten die Erfassungen an den CCL-Schnittstellen:

<#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
```

## Eindämmung

- Stellen Sie sicher, dass die CCL-Port-Channel-Schnittstellen mit separaten Port-Channel-Schnittstellen am Switch verbunden sind.
- Wenn virtuelle Port-Channels (vPC) auf Nexus-Switches verwendet werden, stellen Sie sicher, dass CCL-Port-Channel-Schnittstellen mit verschiedenen vPCs verbunden sind und dass der vPC-Konfigurationsstatus nicht fehlerhaft ist.
- Stellen Sie sicher, dass sich die CCL-Port-Channel-Schnittstellen in derselben Broadcast-Domäne befinden und dass das CCL-VLAN erstellt und für die Schnittstellen zugelassen wird.

Dies ist eine Switch-Beispielkonfiguration:

```
<#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

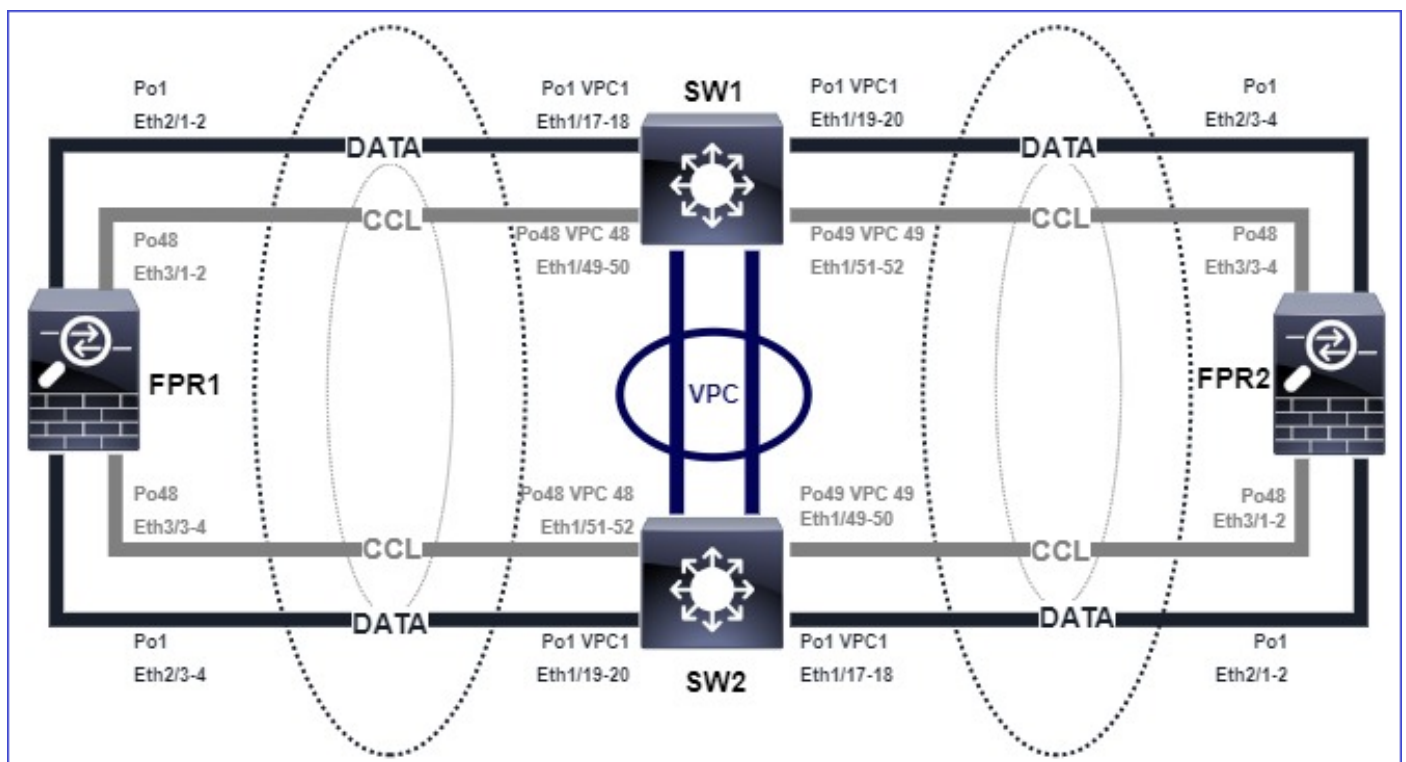
49 Po49 up success success 48

Cluster wegen ausgesetzter Daten-Port-Channel-Schnittstellen deaktiviert

### Symptom

Eine oder mehrere Datenport-Channel-Schnittstellen wurden ausgesetzt. Wenn eine für den Administrator aktivierte Datenschnittstelle außer Kraft gesetzt wird, werden alle Cluster-Einheiten im gleichen Chassis aufgrund eines Fehlers bei der Überprüfung der Schnittstellenintegrität aus dem Cluster entfernt.

Betrachten Sie diese Topologie:



### Verifizierung

- Regelungskonsole prüfen:

```
<#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.

- Überprüfen Sie die Ausgabe der Befehle show cluster history und show cluster info trace module hc in den betroffenen Einheiten:

<#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
```

- Überprüfen Sie die Ausgabe des Befehls `show port-channel summary` in der Befehlszeile `fxos`:

<#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)
```

## Eindämmung

- Stellen Sie sicher, dass alle Chassis den gleichen Clustergruppennamen und das gleiche Kennwort aufweisen.
- Stellen Sie sicher, dass für die Port-Channel-Schnittstellen vom Administrator aktivierte physische Mitgliederschnittstellen mit derselben Duplex-/Geschwindigkeitskonfiguration in allen Chassis und Switches vorhanden sind.
- In Intra-Site-Clustern stellen Sie sicher, dass die gleiche Daten-Port-Channel-Schnittstelle in allen Chassis mit der gleichen Port-Channel-Schnittstelle am Switch verbunden ist.
- Wenn virtuelle Port-Channels (vPC) in Nexus-Switches verwendet werden, stellen Sie sicher, dass der Status der vPC-Konfiguration nicht fehlerhaft ist.
- In Intra-Site-Clustern stellen Sie sicher, dass die gleiche Daten-Port-Channel-Schnittstelle in allen Chassis mit dem gleichen vPC verbunden ist.



## Probleme mit der Cluster-Stabilität

### FXOS-Ablaufverfolgung

#### Symptom

Einheit verlässt den Cluster.

#### Überprüfung/Problembehebung

- Verwenden Sie den Befehl `show cluster history` (Clusterverlauf anzeigen), um zu sehen, wann die Einheit den Cluster verlassen hat.

```
<#root>
```

```
firepower#
```

```
show cluster history
```

- Verwenden Sie diese Befehle, um zu überprüfen, ob der FXOS über ein Traceback verfügt.

```
<#root>
```

```
FPR4150#
```

```
connect local-mgmt
```

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

```
dir cores
```

- Sammeln Sie die Core-Datei, die zu dem Zeitpunkt generiert wurde, als die Einheit den Cluster verließ, und stellen Sie sie dem TAC zur Verfügung.

#### Festplatte voll

Falls die Festplattenauslastung in der /ngfw-Partition einer Clustereinheit 94 % erreicht, beendet die Einheit den Cluster. Die Festplattenauslastungsprüfung findet alle 3 Sekunden statt:

```
<#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 diesem Fall zeigt die Ausgabe zum Anzeigen des Clusterverlaufs Folgendes an:

```
<#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
```

Oder

```
14:07:26 CEST May 18 2021
```

```
SECONDARY DISABLED Received control message DISABLE (application health check failure)
```

Eine weitere Möglichkeit, den Fehler zu überprüfen, ist:

```
<#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
```

Wenn die Festplatte ~100 % beträgt, kann die Einheit außerdem Schwierigkeiten haben, dem Cluster beizutreten, bis etwas Speicherplatz freigegeben wird.

## Überlaufschutz

Alle 5 Minuten überprüft jede Cluster-Einheit die lokale und die Peer-Einheit auf CPU- und Speichernutzung. Liegt die Auslastung über den Systemschwellenwerten (LINA CPU 50% oder LINA Memory 59%), wird eine Informationsmeldung angezeigt in:

- Syslogs (FTD-6-748008)
- Datei log/cluster\_trace.log, zum Beispiel:

```
<#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
```

Die Nachricht weist darauf hin, dass bei einem Ausfall der Einheit die anderen Ressourcen überbelegt werden können.

## Vereinfachter Modus

### Verhalten bei FMC-Versionen vor 6.3


- Sie registrieren jeden Cluster-Knoten einzeln auf dem FMC.
- Dann bilden Sie einen logischen Cluster in FMC.
- Für jede neue Cluster-Knoten-Hinzufügung müssen Sie den Knoten manuell registrieren.

### Nach 6.3 FMC

- Der vereinfachte Modus ermöglicht es Ihnen, den gesamten Cluster in einem Schritt auf

FMC zu registrieren (nur einen Knoten des Clusters zu registrieren).

Minimaler unterstützter Manager	Verwaltete Geräte	Min. unterstützte Version des verwalteten Geräts erforderlich	Hinweise
FMC 6.3	FTD-Cluster nur für FP9300 und FP4100	6.2.0	Dies ist nur eine FMC-Funktion.

 **Warnung:** Sobald der Cluster auf FTD gebildet ist, müssen Sie warten, bis die automatische Registrierung gestartet wird. Sie dürfen die Clusterknoten nicht manuell registrieren (Gerät hinzufügen), sondern müssen die Option "Abstimmen" verwenden.

## Symptom

### Fehler bei der Knotenregistrierung

- Wenn die Registrierung des Kontrollknotens aus irgendeinem Grund fehlschlägt, wird der Cluster aus dem FMC gelöscht.

## Eindämmung

Wenn die Datenknotenregistrierung aus irgendeinem Grund fehlschlägt, gibt es zwei Optionen:

1. Bei jeder Bereitstellung im Cluster prüft das FMC, ob Clusterknoten vorhanden sind, die registriert werden müssen, und startet dann die automatische Registrierung für diese Knoten.
2. Auf der Registerkarte "Cluster-Übersicht" steht eine Option zum Abgleich zur Verfügung (Geräte > Gerätemanagement > Registerkarte "Cluster" > Cluster-Status anzeigen). Sobald die Aktion "Abstimmen" ausgelöst wird, beginnt das FMC mit der automatischen Registrierung der zu registrierenden Knoten.

## Zugehörige Informationen

- [Clustering für die FirePOWER Threat Defense](#)
- [ASA-Cluster für das Firepower 4100/9300-Chassis](#)
- [Informationen zum Clustering auf dem FirePOWER 4100/9300-Chassis](#)
- [FirePOWER NGFW-Clustering im Detail - BRKSEC-3032](#)
- [Analysieren von Firepower-Firewall-Erfassungen zur effektiven Behebung von Netzwerkproblemen](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.