

# Solución de problemas del clúster de Firepower Threat Defence (FTD)

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Fundamentos del clúster](#)

[Arquitectura de NGFW](#)

[Capturas de clúster](#)

[Mensajes del enlace de control de clústeres \(CCL\)](#)

[Mensajes del punto de control del clúster \(CCP\)](#)

[Mecanismo de comprobación del estado del clúster \(HC\)](#)

[Escenarios de falla de clúster HC](#)

[Establecimiento de conexión de plano de datos de clúster](#)

[Troubleshoot](#)

[Introducción a Troubleshooting de Cluster](#)

[Problemas del plano de datos del clúster](#)

[Problemas comunes de NAT/PAT](#)

[Manejo de fragmentos](#)

[Problemas de ACI](#)

[Problemas del plano de control del clúster](#)

[La unidad no puede unirse al clúster](#)

[Tamaño de MTU en CCL](#)

[Discordancia de interfaz entre unidades de clúster](#)

[Problema de interfaz de datos/canal de puerto](#)

[Cerebro partido debido a problemas de accesibilidad en el CCL](#)

[Clúster deshabilitado debido a interfaces de canal de puerto de datos suspendidos](#)

[Problemas de estabilidad del clúster](#)

[Seguimiento de FXOS](#)

[Disco lleno](#)

[Protección contra desbordamientos](#)

[Modo simplificado](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe la solución de problemas de una configuración de clúster en el firewall de última generación (NGFW) Firepower.

# Prerequisites

## Requirements

Cisco recomienda que conozca estos temas (consulte la sección Información Relacionada para ver los enlaces):

- Arquitectura de la plataforma Firepower
- Configuración y funcionamiento del clúster de Firepower
- Familiaridad con FTD y la CLI del sistema operativo extensible (FXOS) de Firepower
- Registros del plano de datos/NGFW
- Rastreador de paquetes de plano de datos/NGFW
- Capturas del plano de datos/FXOS

## Componentes Utilizados

- HW: Firepower 4125
- SW: 6.7.0 (Compilación 65): plano de datos 9.15(1)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

La mayoría de los elementos que se tratan en este documento también son totalmente aplicables a la resolución de problemas del clúster de Adaptive Security Appliance (ASA).

## Configurar

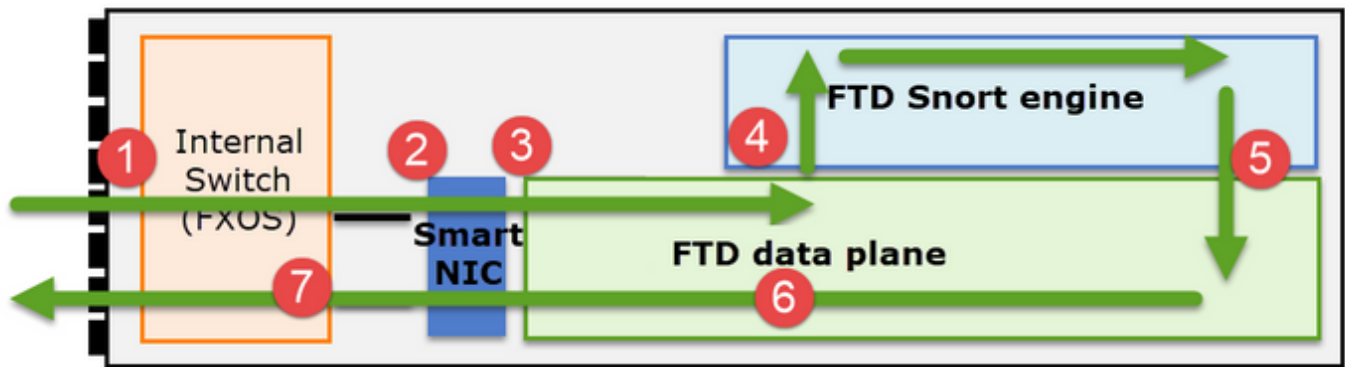
La parte de configuración de una implementación de clúster se trata en las guías de configuración de FMC y FXOS:

- [Agrupación en clústeres para Firepower Threat Defence](#)
- [Implementación de un clúster para Firepower Threat Defense para ofrecer escalabilidad y alta disponibilidad](#)

## Fundamentos del clúster

### Arquitectura de NGFW

Es importante comprender cómo un Firepower serie 41xx o 93xx gestiona los paquetes de tránsito:



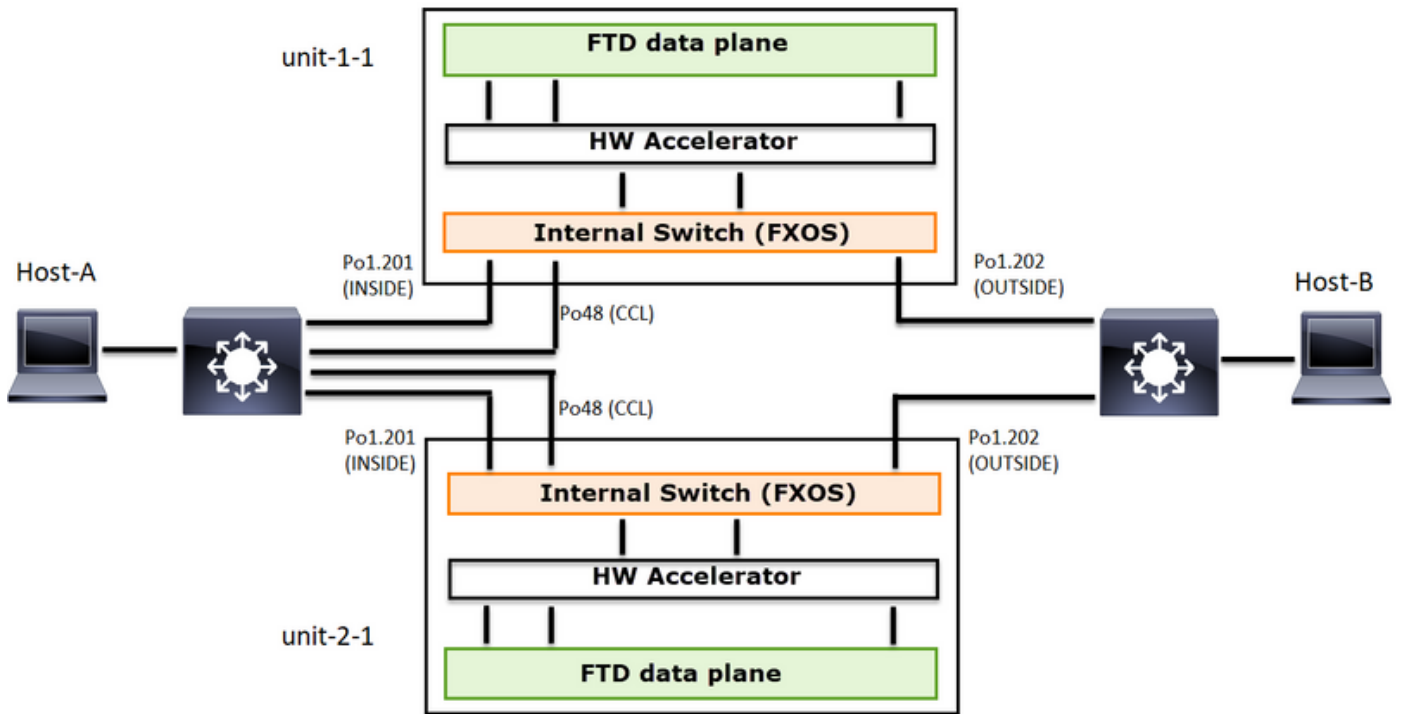
1. Un paquete ingresa a la interfaz de ingreso y es manejado por el switch interno del chasis.
2. El paquete pasa a través de la NIC inteligente. Si el flujo se descarga (aceleración de hardware), el paquete es manejado únicamente por la NIC inteligente y luego se envía de vuelta a la red.
3. Si el paquete no se descarga, entra en el plano de datos FTD que realiza principalmente comprobaciones L3/L4.
4. Si la política lo requiere, el motor Snort inspecciona el paquete (principalmente inspección L7).
5. El motor Snort devuelve un veredicto (por ejemplo, permitir o bloquear) para el paquete.
6. El plano de datos descarta o reenvía el paquete en función del veredicto de Snort.
7. El paquete sale del chasis a través del switch de chasis interno.

## Capturas de clúster

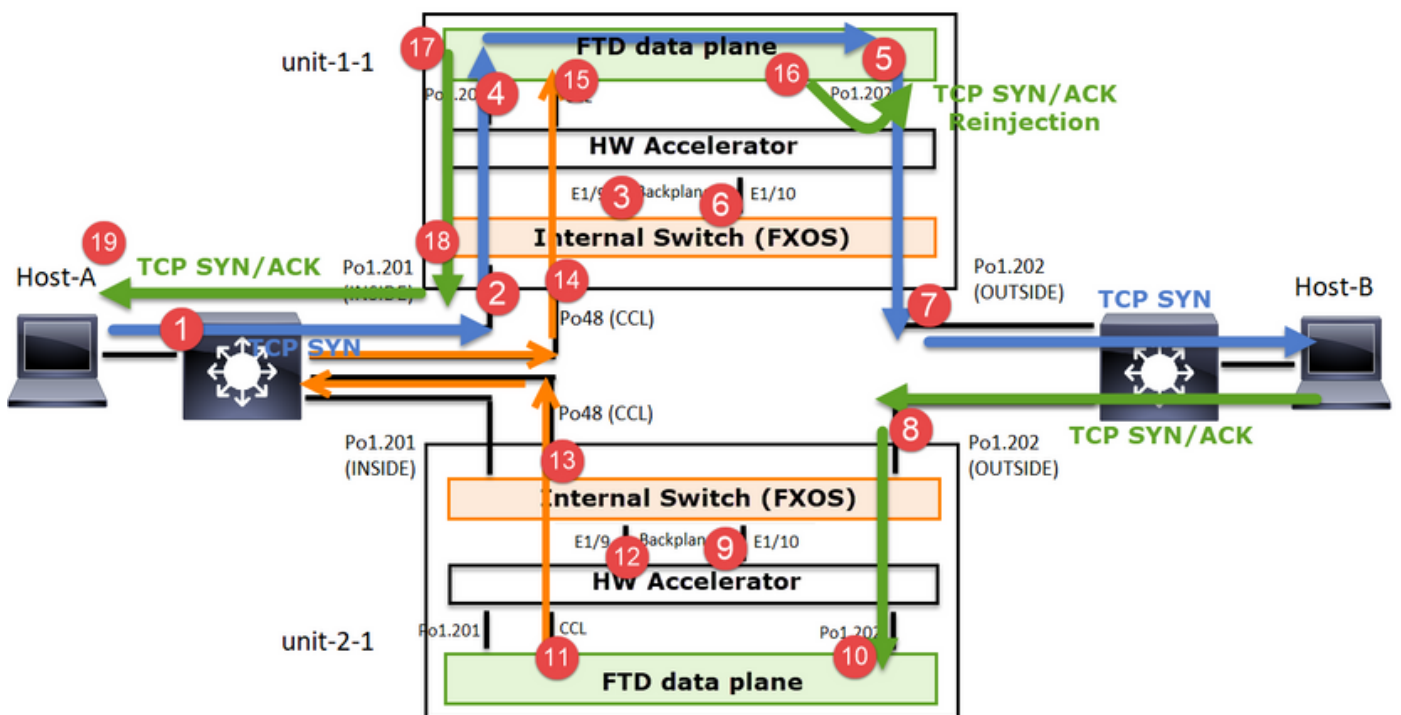
Los appliances Firepower proporcionan varios puntos de captura que proporcionan visibilidad de los flujos de tránsito. Al resolver problemas y habilitar las capturas de clúster, los principales desafíos son:

- El número de capturas aumenta a medida que aumenta el número de unidades del clúster.
- Debe ser consciente de la forma en que el clúster maneja un flujo específico para poder rastrear el paquete a través del clúster.

Este diagrama muestra un clúster de 2 unidades (por ejemplo, FP941xx/FP9300):



En el caso de un establecimiento de conexión TCP asimétrico, un intercambio SYN, SYN/ACK de TCP es similar a lo siguiente:



### Tráfico directo

1. TCP SYN se envía del Host A al Host B.
2. TCP SYN llega al chasis (uno de los miembros de Po1).
3. TCP SYN se envía a través de una de las interfaces de placa base del chasis (por ejemplo, E1/9, E1/10, etc.) al plano de datos.
4. TCP SYN llega a la interfaz de entrada del plano de datos (Po1.201/INSIDE). En este ejemplo, unit1-1 toma posesión del flujo, realiza la aleatorización del número de secuencia

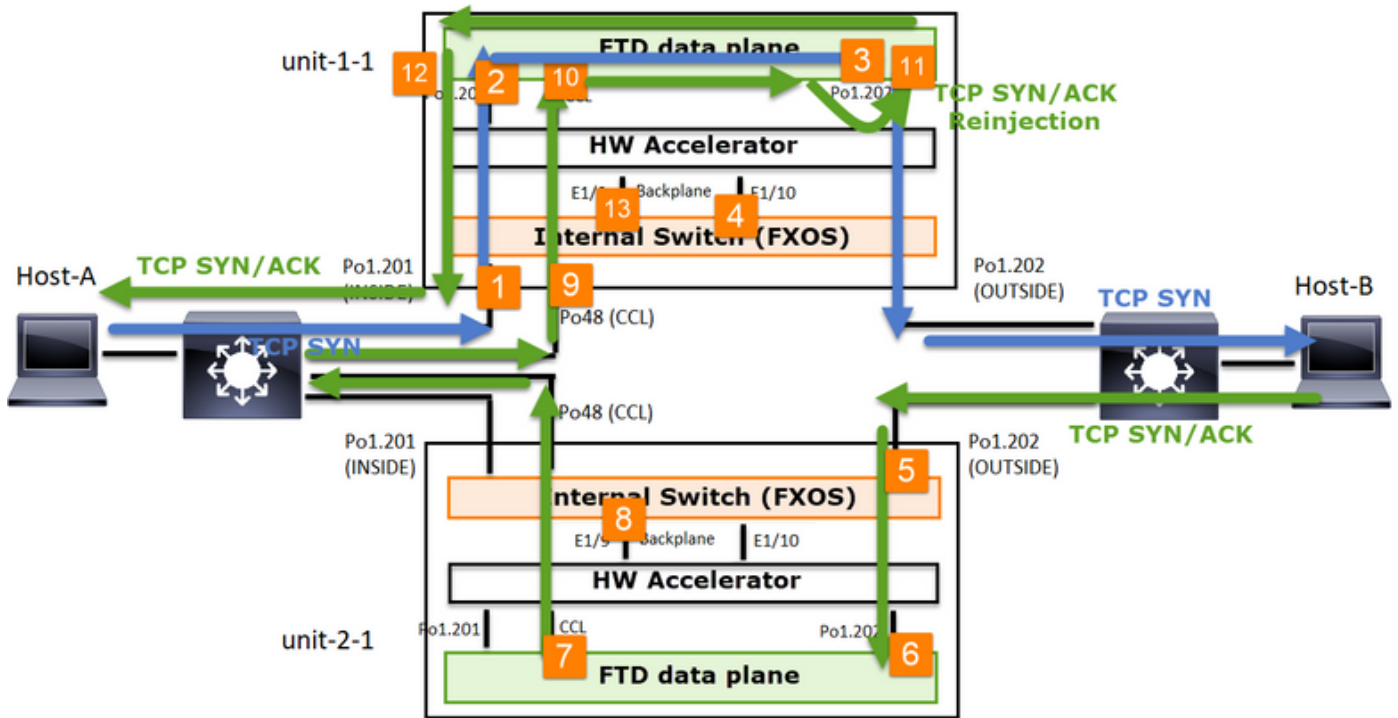
- inicial (ISN) y codifica la información de propiedad (cookie) en el número de secuencia.
5. TCP SYN se envía desde Po1.202/OUTSIDE (interfaz de salida del plano de datos).
  6. TCP SYN llega a una de las interfaces de placa base del chasis (por ejemplo, E1/9, E1/10, etc.).
  7. TCP SYN se envía desde la interfaz física del chasis (uno de los miembros de Po1) hacia el Host B.

#### Tráfico de retorno

8. TCP SYN/ACK se envía desde el Host B y llega a la unidad-2-1 (uno de los miembros de Po1).
9. TCP SYN/ACK se envía a través de una de las interfaces de placa base del chasis (por ejemplo, E1/9, E1/10, etc.) al plano de datos.
10. TCP SYN/ACK llega a la interfaz de ingreso del plano de datos (Po1.202/OUTSIDE).
11. TCP SYN/ACK se envía desde el enlace de control de clúster (CCL) hacia la unidad 1-1. De forma predeterminada, ISN está habilitado. Por lo tanto, el reenviador encuentra la información del propietario para TCP SYN+ACKs sin la participación del director. Para otros paquetes o cuando se inhabilita el ISN, se consulta al director.
12. TCP SYN/ACK llega a una de las interfaces de backplane del chasis (por ejemplo, E1/9, E1/10, etc.).
13. TCP SYN/ACK se envía fuera de la interfaz física del chasis (uno de los miembros de Po48) hacia la unidad-1-1.
14. TCP SYN/ACK llega a la unidad-1-1 (uno de los miembros de Po48).
15. TCP SYN/ACK se reenvía a través de una de las interfaces de placa base del chasis a la interfaz de canal de puerto CCL del plano de datos (nameif cluster).
16. El plano de datos reinyecta el paquete TCP SYN/ACK en la interfaz del plano de datos Po1.202/OUTSIDE.
17. TCP SYN/ACK se envía desde Po1.201/INSIDE (interfaz de salida del plano de datos) hacia HOST-A.
18. El TCP SYN/ACK atraviesa una de las interfaces de backplane del chasis (por ejemplo, E1/9, E1/10, etc.) y egresa uno de los miembros de Po1.
19. TCP SYN/ACK llega al Host-A.

Para obtener más detalles sobre esta situación, lea la sección relacionada en los casos prácticos de establecimiento de conexión a clústeres.

Según este intercambio de paquetes, todos los puntos de captura de clúster posibles son:



Para la captura de tráfico de reenvío (por ejemplo, TCP SYN) en:

1. La interfaz física del chasis (por ejemplo, miembros Po1). Esta captura se configura desde la interfaz de usuario del administrador de chasis (CM) o desde la CLI de CM.
2. Interfaz de entrada de plano de datos (por ejemplo, Po1.201 INSIDE).
3. Interfaz de salida del plano de datos (por ejemplo, Po1.202 OUTSIDE).
4. Interfaces de placa base del chasis. En FP4100 hay 2 interfaces de backplane. En FP9300 hay un total de 6 (2 por módulo). Dado que no sabe en qué interfaz llega el paquete, debe habilitar la captura en todas las interfaces.


Para la captura del tráfico de retorno (por ejemplo, TCP SYN/ACK) en:

5. La interfaz física del chasis (por ejemplo, miembros Po1). Esta captura se configura desde la interfaz de usuario del administrador de chasis (CM) o desde la CLI de CM.
6. Interfaz de entrada de plano de datos (por ejemplo, Po1.202 OUTSIDE).
7. Dado que el paquete se redirige, el siguiente punto de captura es el plano de datos CCL.
8. Interfaces de placa base del chasis. De nuevo, debe habilitar la captura en ambas interfaces.
9. Interfaces miembro CCL del chasis Unit-1-1.
10. Interfaz CCL del plano de datos (name if cluster).
11. Interfaz de entrada (Po1.202 OUTSIDE). Este es el paquete reinyectado desde CCL al plano de datos.
12. Interfaz de salida del plano de datos (por ejemplo, Po1.201 INSIDE).
13. Interfaces de placa base del chasis.

Cómo habilitar las capturas de clúster

Capturas de FXOS

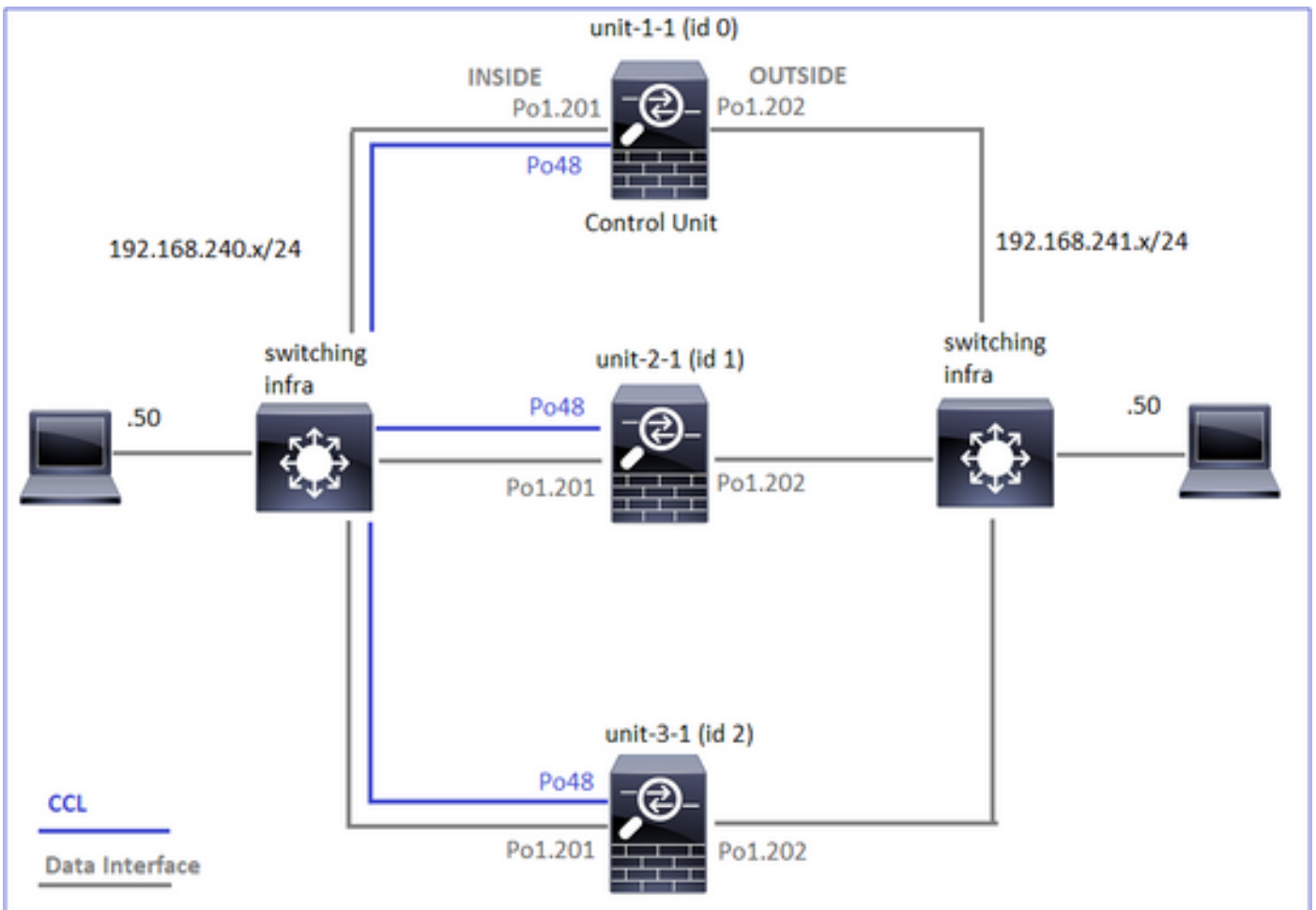
El proceso se describe en la Guía de configuración de FXOS: [Captura de paquete](#)

 Nota: Las capturas de FXOS solo se pueden realizar en la dirección de entrada desde el punto de vista del switch interno.

## Capturas del plano de datos

La manera recomendada de habilitar la captura en todos los miembros del clúster es con el comando cluster exec.

Considere un clúster de 3 unidades:



Para verificar si hay capturas activas en todas las unidades del clúster, utilice este comando:

```
<#root>
```

```
firepower#
```

```
cluster exec show capture
```

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

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

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

```
firepower#
```

Para habilitar una captura de plano de datos en todas las unidades en Po1.201 (INSIDE):

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

Se recomienda especificar un filtro de captura y, en caso de que espere mucho tráfico, aumentar el búfer de captura:

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

Verificación

```
<#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
```

Para ver el contenido de todas las capturas (este resultado puede ser muy largo):

```
<#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

## Capturar seguimientos

Si desea ver cómo el plano de datos de cada unidad maneja los paquetes de ingreso, utilice la palabra clave trace. Esto rastrea los primeros 50 paquetes de ingreso. Puede rastrear hasta 1000 paquetes de ingreso.



Nota: En caso de que tenga varias capturas aplicadas en una interfaz, puede rastrear un solo paquete una sola vez.

---

Para rastrear los primeros 1000 paquetes de ingreso en la interfaz OUTSIDE en todas las unidades del clúster:

```
<#root>
```

```
firepower#
```

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

Una vez que capture el flujo de interés, es necesario asegurarse de que rastrea los paquetes de interés en cada unidad. Lo importante a recordar es que un paquete específico puede ser #1 en la unidad-1-1, pero #2 en otra unidad, y así sucesivamente.

En este ejemplo, puede ver que el SYN/ACK es el paquete #2 en la unidad-2-1, pero el paquete #1 en la unidad-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>
```

Para rastrear el paquete #2 (SYN/ACK) en la unidad local:

```
<#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  
...

Para rastrear el mismo paquete (SYN/ACK) en la unidad remota:

<#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

...

## Captura de CCL

Para activar la captura en el enlace CCL (en todas las unidades):

<#root>

firepower#

```
cluster exec capture CCL interface cluster
```

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

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

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

## Rechazar ocultar

De forma predeterminada, una captura habilitada en una interfaz de datos del plano de datos muestra todos los paquetes:

- Los que llegan de la red física
- Los que se reinyectan desde la CCL

Si no desea ver los paquetes reinyectados, utilice la opción `reinject-hide`. Esto puede ser útil si desea verificar si un flujo es asimétrico:

```
<#root>
```

```
firepower#
```

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

Esta captura sólo muestra lo que la unidad local recibe realmente en la interfaz específica directamente de la red física, y no de las otras unidades del clúster.

### caídas ASP

Si desea verificar si hay caídas de software para un flujo específico, puede habilitar la captura `asp-drop`. Si no sabe en qué motivo de caída debe centrarse, utilice la palabra clave `all`. Además, si no está interesado en la carga útil del paquete, puede especificar la palabra clave `header-only`. Esto le permite capturar de 20 a 30 veces más paquetes:

```
<#root>
```

```
firepower#
```

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

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

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

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

Además, puede especificar las IP de interés en la captura ASP:

```
<#root>
```

```
firepower#
```

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

```
match ip host 192.0.2.100 any
```

### Borrar una captura

Para borrar el buffer de cualquier captura que se ejecute en todas las unidades del cluster. Esto no detiene las capturas, pero solo borra las memorias intermedias:

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

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

### Detener una captura

Hay 2 maneras de detener una captura activa en todas las unidades de clúster. Más adelante podrá continuar.

#### Vía 1

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

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

### Para reanudar

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

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

## Vía 2

```
<#root>
```

```
firepower#
```

```
cluster exec no capture CAPI interface INSIDE
```

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

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

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

## Para reanudar

```
<#root>
```

```
firepower#
```

```
cluster exec capture CAPI interface INSIDE
```

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

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

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

## Recopilar una captura

Hay varias formas de exportar una captura.

Modo 1: a un servidor remoto

Esto le permite cargar una captura desde el plano de datos a un servidor remoto (por ejemplo, TFTP). Los nombres de captura se cambian automáticamente para reflejar la unidad de origen:

```
<#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

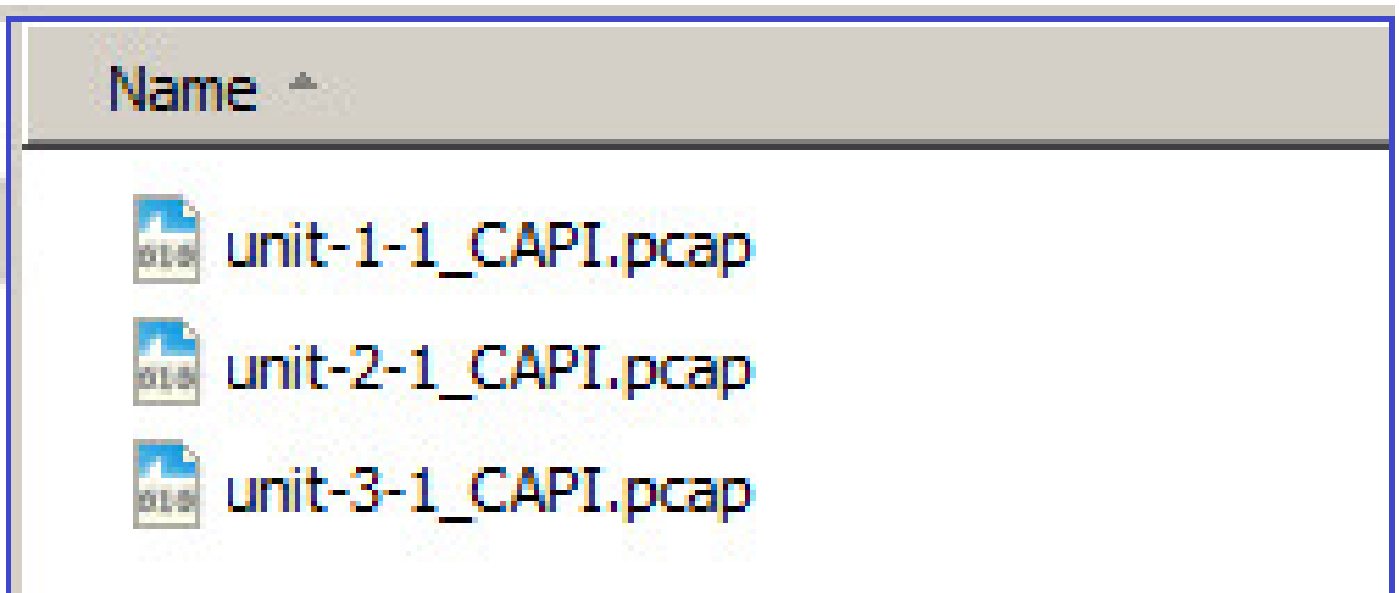
unit-2-1:\*\*\*\*\*

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 !

Los archivos pcap cargados:



Camino 2 - Obtener las capturas de la FMC

Esta forma solo es aplicable al FTD. En primer lugar, copie la captura en el disco FTD:

<#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



En el modo experto, copie el archivo de /mnt/disk0/ al directorio /ngfw/var/common/:

```
<#root>
```

```
>
```

```
expert
```

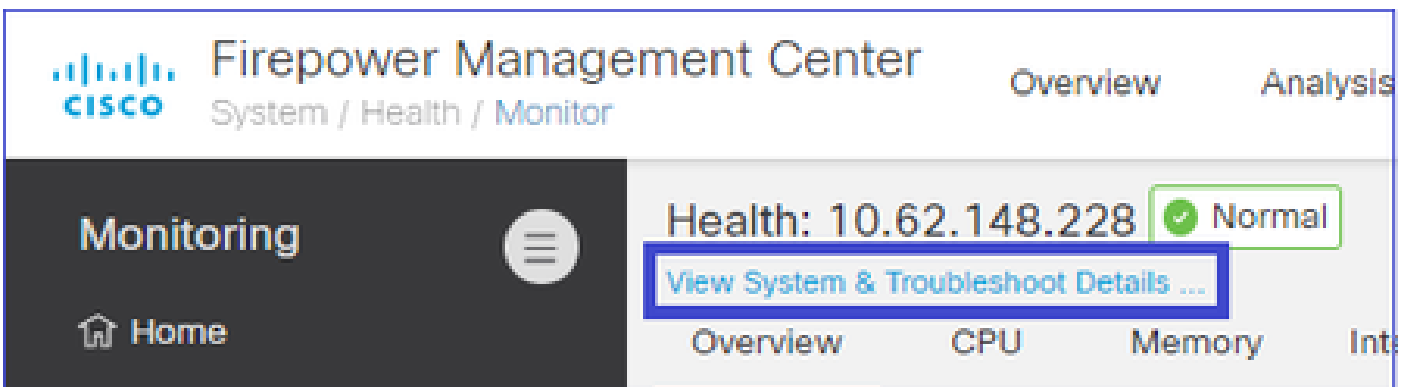
```
admin@firepower:~$
```

```
cd /mnt/disk0
```

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

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

Por último, en FMC, vaya a la sección System > Health > Monitor. Elija View System & Troubleshoot Details > Advanced Troubleshooting y obtenga el archivo de captura:



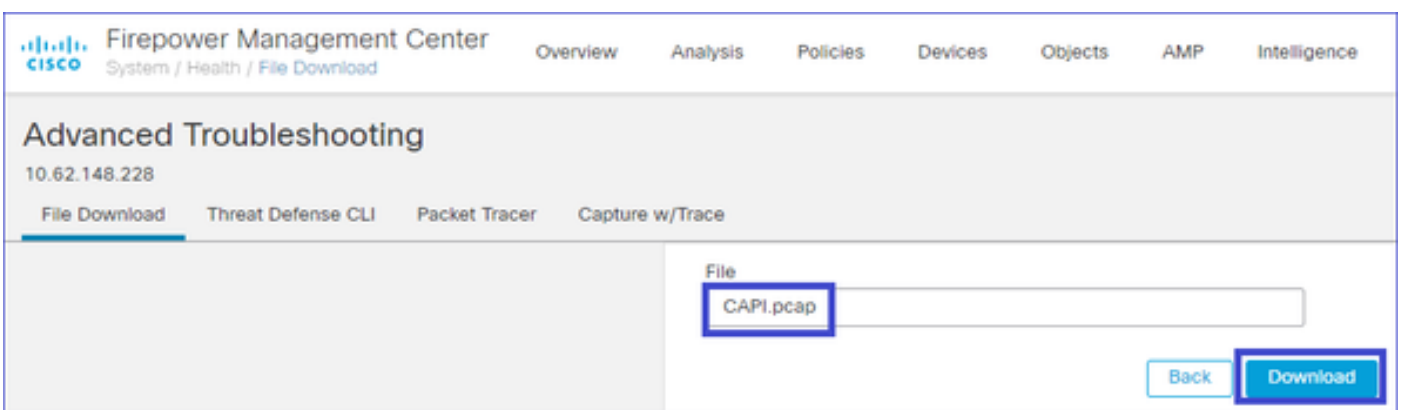
Firepower Management Center  
System / Health / Monitor

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

Eliminar una captura

Para eliminar una captura de todas las unidades de clúster, utilice este comando:

```
<#root>
```

```
firepower#
```

cluster exec no capture CAPI

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

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

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

## Flujos descargados

En FP41xx/FP9300, los flujos se pueden descargar en el acelerador de hardware de forma estática (por ejemplo, reglas de ruta rápida) o dinámica. Para obtener más detalles sobre la descarga de flujo, consulte este documento:

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

Si se descarga un flujo, solo unos pocos paquetes pasan por el plano de datos FTD. El resto lo gestiona el acelerador de hardware (Smart NIC).

Desde el punto de vista de la captura, esto significa que si solo habilita las capturas de nivel de plano de datos FTD, no verá todos los paquetes que pasan a través del dispositivo. En este caso, también debe habilitar las capturas a nivel de chasis FXOS.

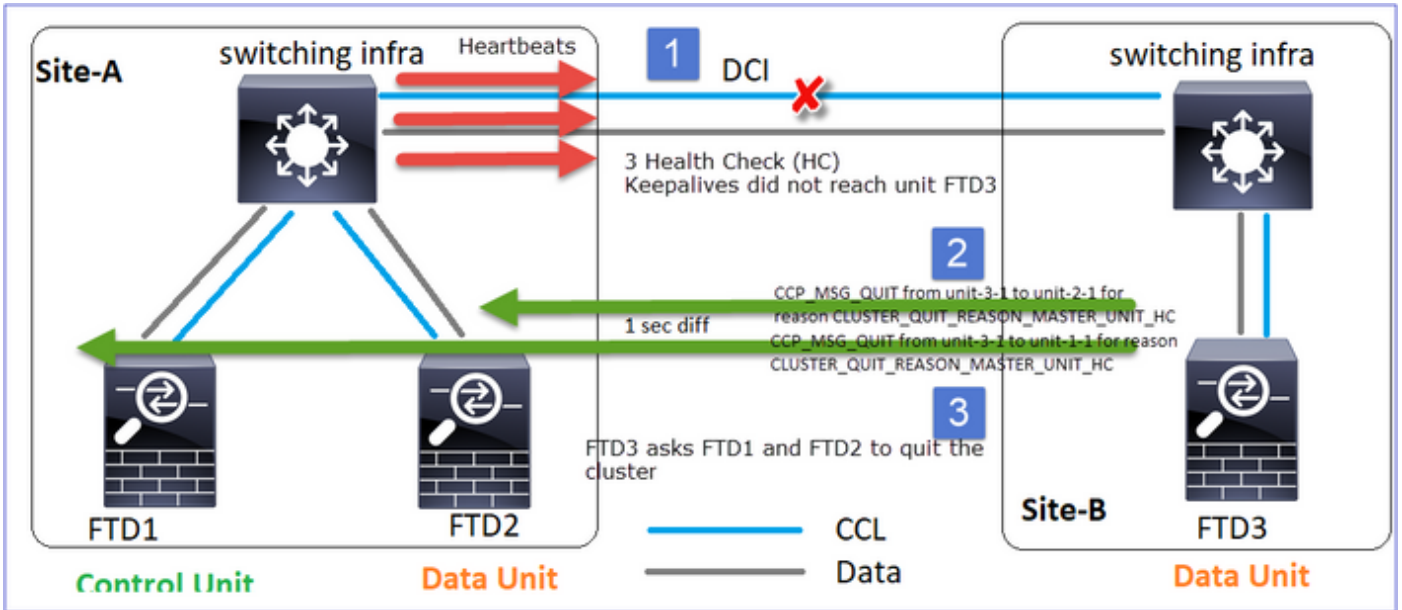
## Mensajes del enlace de control de clústeres (CCL)

Si realiza una captura en CCL, observará que las unidades del clúster intercambian diferentes tipos de mensajes. Los de interés son:

Protocolo	Descripción
UDP 49495	<p>Latidos del clúster (keepalives)</p> <ul style="list-style-type: none"><li>· Transmisión de L3 (255.255.255.255)</li><li>· Cada unidad de clúster envía estos paquetes a la mitad del valor de tiempo de espera de comprobación de estado.</li><li>· Tenga en cuenta que no todos los paquetes UDP 49495 que se ven en la captura son latidos</li><li>· Los latidos contienen un número de secuencia.</li></ul>
UDP 4193	<p>Mensajes de ruta de datos de Cluster Control Protocol</p> <ul style="list-style-type: none"><li>· Unidifusión</li></ul>



- Cuando una unidad recibe este mensaje, sale del clúster (DISABLED) y vuelve a unirse.

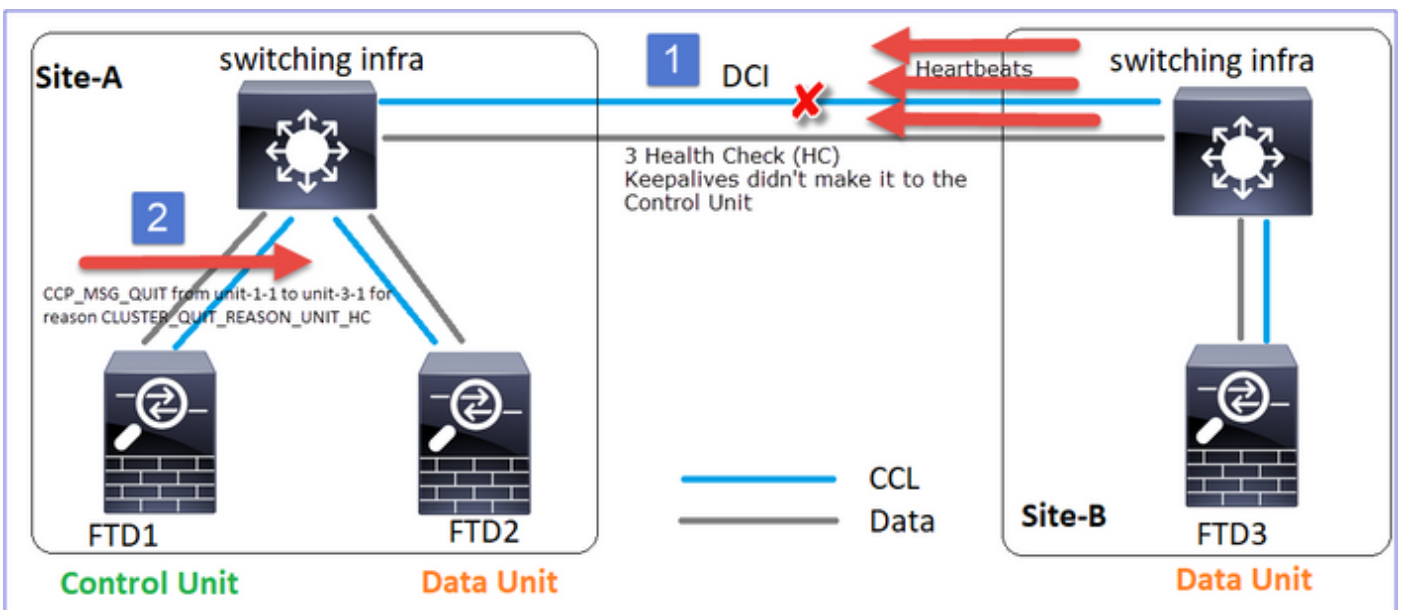


P. ¿Cuál es el propósito de CLUSTER\_QUIT\_REASON\_PRIMARY\_UNIT\_HC?

A. Desde el punto de vista de la unidad-3-1 (Sitio-B), pierde la conexión tanto con la unidad-1-1 como con la unidad-2-1 del sitio A, por lo que necesita eliminarlas de su lista de miembros tan pronto como sea posible; de lo contrario, puede perder paquetes si la unidad-2-1 sigue en su lista de miembros y la unidad-2-1 resulta ser un director de una conexión, y la consulta de flujo a la unidad-2-1 falla.

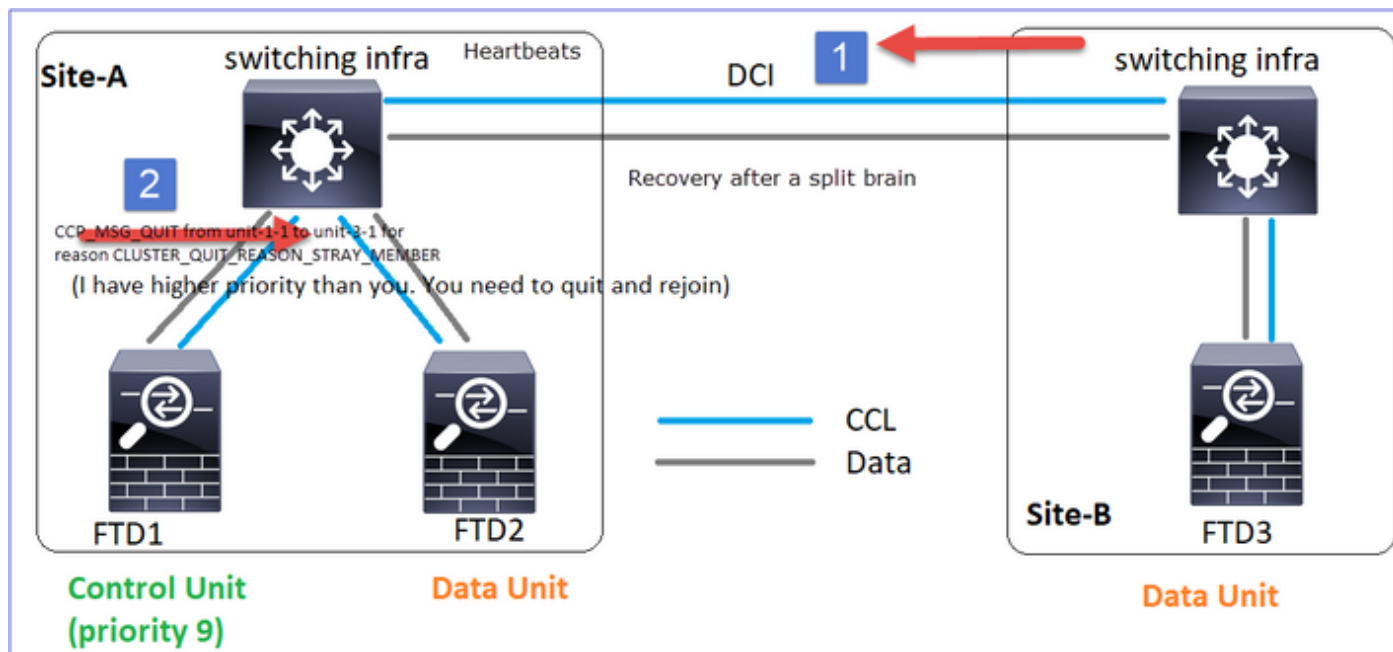
CLUSTER\_QUIT\_REASON\_UNIT\_HC

Siempre que el nodo de control pierde 3 mensajes de latido consecutivos de un nodo de datos, envía el mensaje CLUSTER\_QUIT\_REASON\_UNIT\_HC a través de la CCL. Este mensaje es unicast.



CLUSTER\_QUIT\_REASON\_STRAY\_MEMBER

Cuando una partición dividida se vuelve a conectar con una partición par, la unidad de control dominante trata el nuevo nodo de datos como un miembro perdido y recibe un mensaje de salida de CCP con la razón de CLUSTER\_QUIT\_REASON\_STRAY\_MEMBER.



## CLUSTER\_QUIT\_MEMBER\_DROPOUT

Mensaje de difusión generado por un nodo de datos y que se envía como difusión. Una vez que una unidad recibe este mensaje, pasa al estado DISABLED (DESACTIVADO). Además, la reincorporación automática no se inicia:

```
<#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
```

El historial del clúster muestra:

```
<#root>
```

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

## Mecanismo de comprobación del estado del clúster (HC)

### Puntos principales

- Cada unidad de clúster envía un latido cada 1/3 del valor de tiempo de espera de comprobación de estado a todas las demás unidades (difusión 255.255.255.255) y utiliza el puerto UDP 49495 como transporte a través de CCL.
- Cada unidad de clúster realiza un seguimiento independiente de cada otra unidad con un temporizador de sondeo y un valor de recuento de sondeo.
- Si una unidad de clúster no recibe ningún paquete (latido o paquete de datos) de una unidad de clúster par dentro de un intervalo de latido, aumenta el valor de recuento de sondeo.
- Cuando el valor de conteo de sondeo para una unidad de peer de clúster se convierte en 3, el peer se considera inactivo.
- Siempre que se recibe un latido, se verifica su número de secuencia y, en caso de que la diferencia con el latido recibido anteriormente sea diferente a 1, el contador de caídas de latido aumenta en consecuencia.
- Si el contador de conteo de sondeos para un par de clúster es diferente de 0 y el par recibe un paquete, el contador se restablece a un valor 0.

Utilice este comando para verificar los contadores de estado del clúster:

```
<#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

### Descripción de las columnas principales

Columna	Descripción
Unidad (ID)	El ID del peer del cluster remoto.
Conteo de latidos	El número de latidos recibidos del peer remoto a través de CCL.

Heartbeat drops	El número de latidos perdidos. Este contador se calcula en función del número de secuencia de latido recibido.
Brecha media	El intervalo de tiempo promedio de los latidos recibidos.
Recuento de sondeos	Cuando este contador se convierte en 3, la unidad se elimina del clúster. El intervalo de consulta de sondeo es el mismo que el intervalo de latido, pero se ejecuta de forma independiente.

Para restablecer los contadores utilice este comando:

```
<#root>
```

```
firepower#
```

```
clear cluster info health details
```

P. ¿Cómo verificar la frecuencia de los latidos del corazón?

A. Compruebe el valor de la diferencia media:

```
<#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|
-----
```

P. ¿Cómo puede cambiar el tiempo de espera del clúster en FTD?

A. Uso de FlexConfig

P. ¿Quién se convierte en el nodo de control después de un cerebro partido?

A. La unidad con la prioridad más alta (el número más bajo):

```
<#root>
```

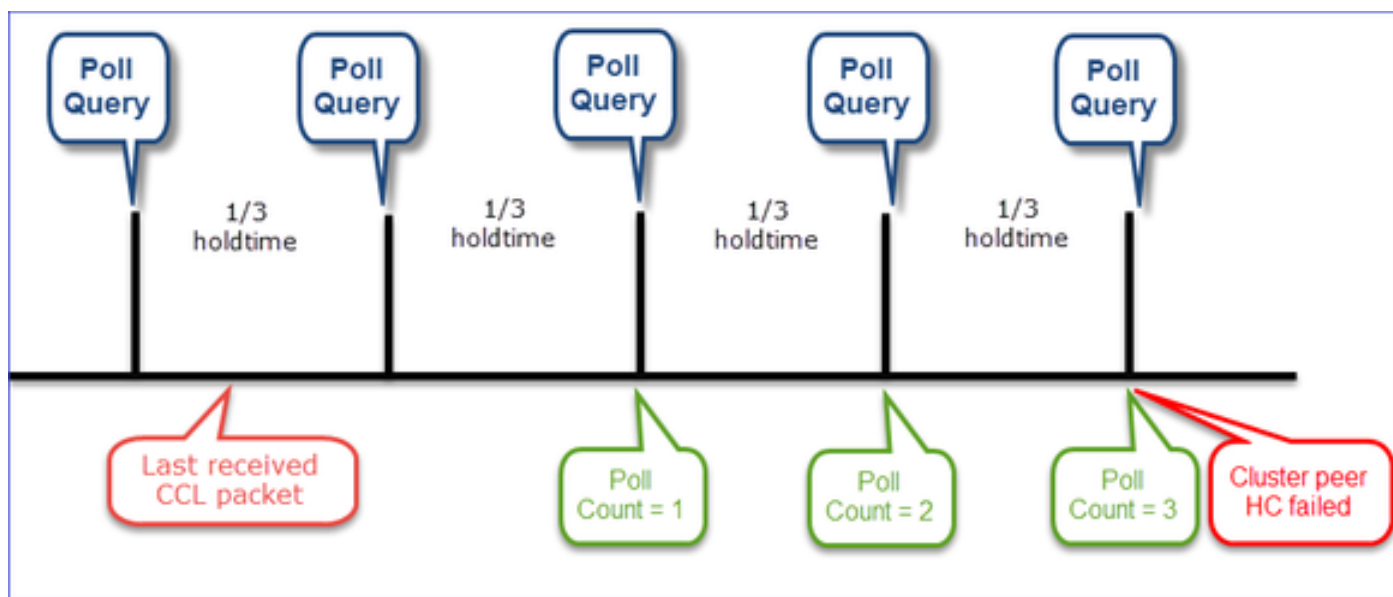
```
firepower#
```

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

```
priority 9
```

Verifique el escenario 1 de falla de HC para obtener más detalles.

Visualización del mecanismo de HC del clúster



Temporizadores indicativos: El mínimo y el máximo dependen de la última llegada de paquetes CCL recibida.

Tiempo de espera	Comprobación de consulta de sondeo (frecuencia)	Tiempo mínimo de detección	Tiempo máximo de detección
3 s (predeterminado)	~1 s	~3,01 s	~3,99 s



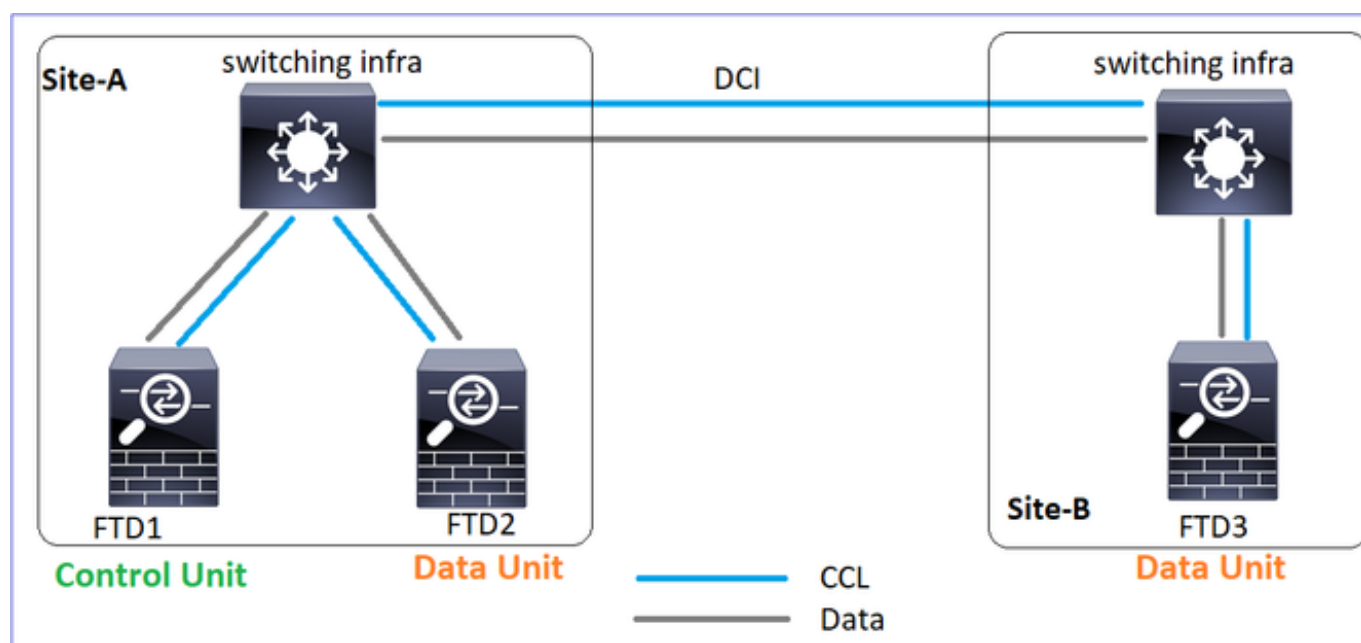
4 seg.	~1,33 s	~4,01 s	~5,32 s
5 seg.	~1,66 s	~5,01 s	~6,65 s
6 seg.	~2 s	~6,01 s	~7,99 s
7 seg.	~2,33 s	~7,01 s	~9,32 s
8 seg.	~2,66 s	~8,01 s	~10,65 s

## Escenarios de falla de clúster HC

Los objetivos de esta sección son demostrar:

- Diferentes escenarios de falla de HC de clúster.
- Cómo se pueden correlacionar los diferentes registros y salidas de comandos.

## Topología



## Configuración de agrupamiento

Unidad-1-1	Unidad-2-1
cluster group GROUP1	cluster group GROUP

```

key *****
local-unit unit-1-1
cluster-interface Port-channel48 ip 10.17.1.1 255.255.0.0
priority 9
health-check holdtime 3
health-check data-interface auto-rejoin 3 5 2
health-check cluster-interface auto-rejoin unlimited 5 1
health-check system auto-rejoin 3 5 2
health-check monitor-interface debounce-time 500
site-id 1
enable

```

```

key *****
local-unit unit-2-1
cluster-interface
priority 17
health-check hold
health-check data
health-check clus
health-check syst
health-check moni
site-id 1
enable

```

Estado del clúster

Unidad-1-1	Unidad-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-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 </pre>	<pre> &lt;#root&gt; 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 </pre>

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

### Escenario 1

Pérdida de comunicación de CCL durante más de 4 segundos en ambas direcciones.

Antes del fracaso

FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B
Nodo de control	Nodo de datos	Nodo de datos

Después de la recuperación (sin cambios en las funciones de unidad)

FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B
Nodo de control	Nodo de datos	Nodo de datos

### Análisis

Error (se perdió la comunicación de CCL).



El mensaje de la consola del plano de datos en la unidad-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.
```

Registros de seguimiento de clúster de Unit-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 0x000055a8918307fb
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_DISCONNECTED
```

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

```
Nov 02 09:38:14.239 [CRIT]Received heartbeat event 'SECONDARY heartbeat failure' for member unit-3-1 (IP: 10.10.10.10)
```

Cerebro partido



```

<#root>
firepower#
show cluster info

Cluster GROUP1: On
  Interface mode: spanned

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

      ID      : 0
      Site ID  : 1
      Version  : 9.12(2)33
      Serial No.: FCH22247LNK
      CCL IP   : 10.17.1.1
      CCL MAC  : 0015.c500.018f
      Last join : 20:25:36 UTC Nov 1 2020
      Last leave: 20:25:28 UTC Nov 1 2020
Other members in the cluster:
  Unit "unit-2-1" in state SECONDARY
      ID      : 2
      Site ID  : 1
      Version  : 9.12(2)33
      Serial No.: FCH23157Y9N
      CCL IP   : 10.17.2.1
      CCL MAC  : 0015.c500.028f
      Last join : 20:44:45 UTC Nov 1 2020
      Last leave: 20:44:38 UTC Nov 1 2020

```

```

<#root>
firepower#
show cluster info

Cluster GROUP1: On
  Interface mode: spanned
  This is "unit-2-1" in state S
      ID      : 2
      Site ID  : 1
      Version  : 9.12(2)33
      Serial No.: FCH23157Y9N
      CCL IP   : 10.17.2.1
      CCL MAC  : 0015.c500.028f
      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
      Last join : 20:25:36 UTC
      Last leave: 20:25:28 UTC

```

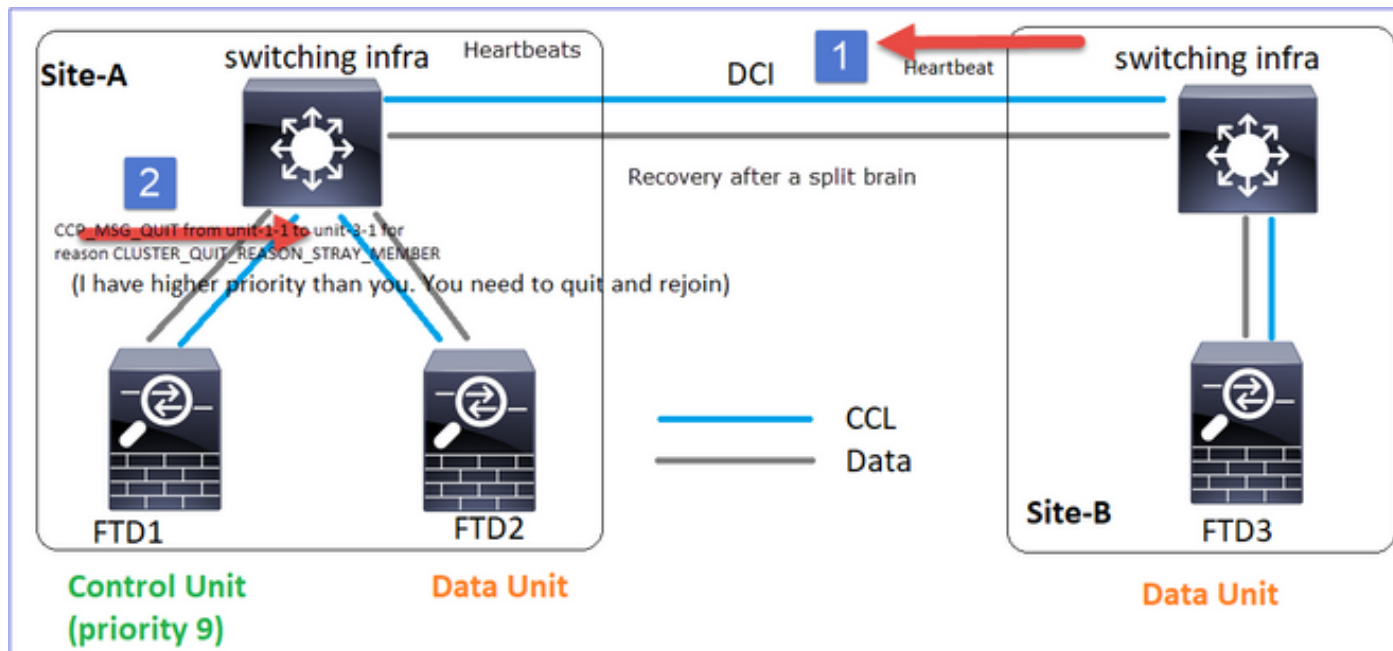
### Historial de clústeres

Unidad-1-1	Unidad-2-1	Unidad-3-1
No hay eventos	No hay eventos	<pre> &lt;#root&gt; 09:38:16 UTC Nov 2 2020 SECONDARY PRIMARY_POST_CONFIG Primary relinqua 09:38:17 UTC Nov 2 2020 PRIMARY_POST_CONFIG Primary Primary post config </pre>

restauración de comunicación CCL

La unidad-1-1 detecta el nodo de control actual y, dado que la unidad-1-1 tiene mayor prioridad, envía a la unidad-3-1 un mensaje CLUSTER\_QUIT\_REASON\_STRAY\_MEMBER para activar un nuevo proceso de elección. Al final, la unidad-3-1 se vuelve a unir como un nodo de datos.

Cuando una partición dividida se vuelve a conectar con una partición par, el nodo de datos es tratado como un miembro perdido por el nodo de control dominante y recibe un mensaje de salida de CCP con una razón de 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
```

Ambas unidades (unit-1-1 y unit-3-1) muestran en sus registros de clúster:

<#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

También hay mensajes syslog generados para el cerebro partido:

<#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

### Historial de clústeres

Unidad-1-1	Unidad-2-1	Unidad-3-1
No hay eventos	No hay eventos	<#root> 09:47:33 UTC Nov 2 2020  <b>Primary DISABLED</b> <b>Detected a splitted cluster</b>  09:47:38 UTC Nov 2 2020 DISABLED                      ELECTION                      Enabled from CLI 09:47:38 UTC Nov 2 2020 ELECTION                      SECONDARY_COLD                      Received cluster contr 09:47:38 UTC Nov 2 2020 SECONDARY_COLD                      SECONDARY_APP_SYNC                      Client progression 09:48:18 UTC Nov 2 2020 SECONDARY_APP_SYNC                      SECONDARY_CONFIG                      SECONDARY applicat 09:48:29 UTC Nov 2 2020 SECONDARY_CONFIG                      SECONDARY_FILESYS                      Configuration repl 09:48:30 UTC Nov 2 2020 SECONDARY_FILESYS                      SECONDARY_BULK_SYNC                      Client progression 09:48:54 UTC Nov 2 2020 SECONDARY_BULK_SYNC  SECONDARY  Client progression done

## Escenario 2

Pérdida de comunicación de CCL durante aproximadamente 3-4 segundos en ambas direcciones.

Antes del fracaso

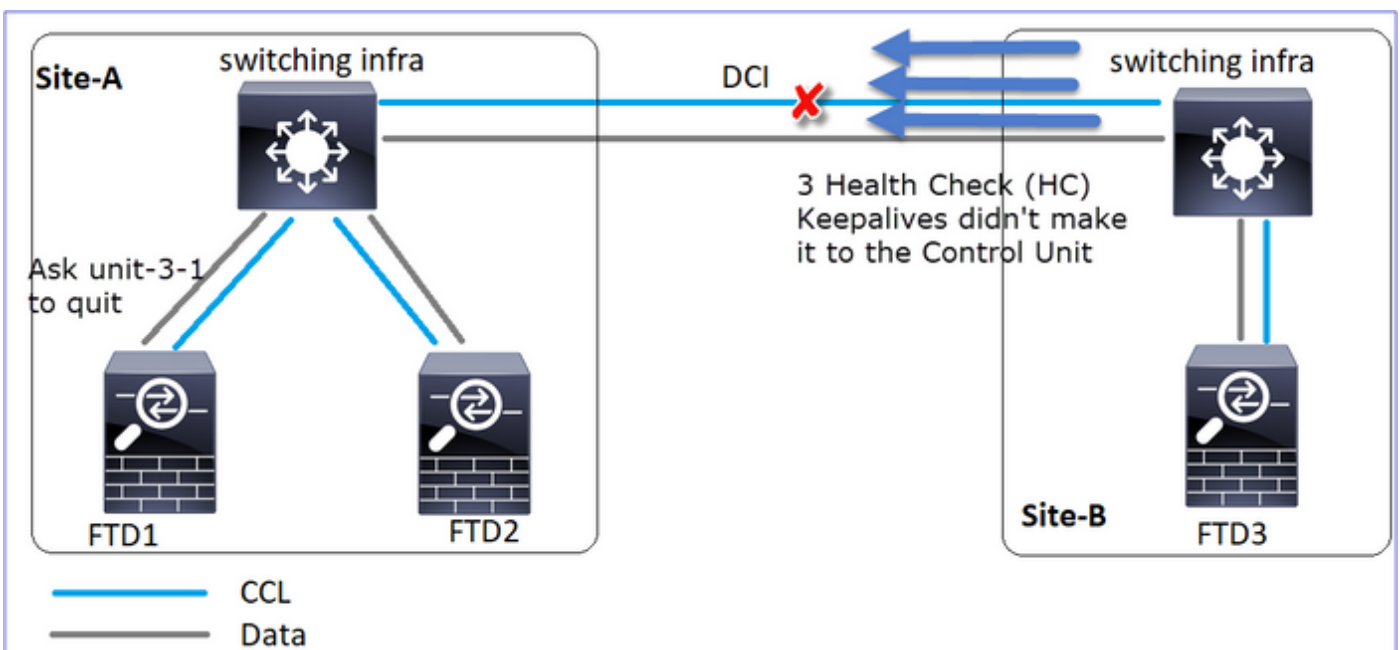
FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B
Nodo de control	Nodo de datos	Nodo de datos

Después de la recuperación (sin cambios en las funciones de unidad)

FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B
Nodo de control	Nodo de datos	Nodo de datos

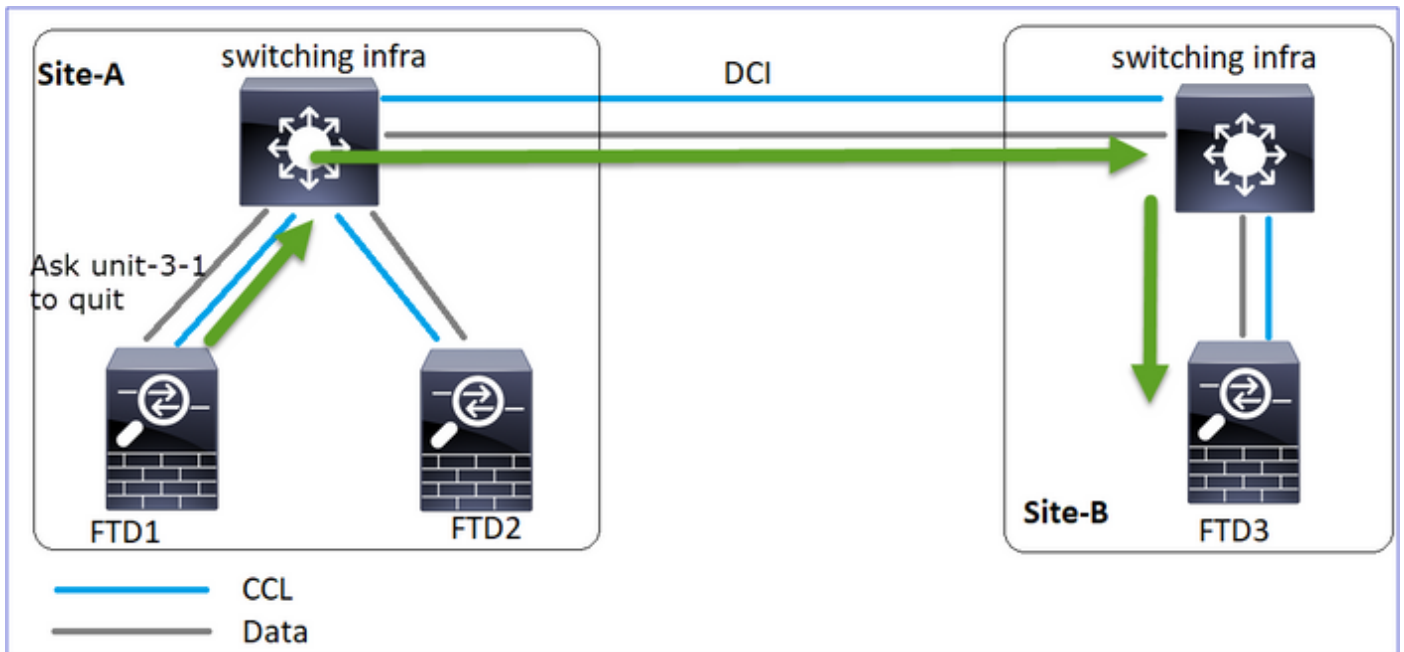
## Análisis

Evento 1: El nodo de control pierde 3 HCs de la unidad-3-1 y envía un mensaje a la unidad-3-1 para salir del clúster.





Evento 2: El CCL se recuperó muy rápido y el mensaje CLUSTER\_QUIT\_REASON\_STRAY\_MEMBER del nodo de control llegó al lado remoto. La Unidad-3-1 va directamente al modo DISABLED y no hay cerebro partido



En la unidad-1-1 (control) verá:

```
<#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
```

En unit-3-1 (nodo de datos) verá:

```
<#root>
```

```
firepower#
```

```
Cluster disable
```

```
is performing cleanup..done.
```

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

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

La unidad de clúster 3-1 pasó a un estado DISABLED y, una vez restaurada la comunicación CCL, se vuelve a unir como un nodo de datos:

<#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
```

### Escenario 3

Pérdida de comunicación de CCL durante aproximadamente 3-4 segundos en ambas direcciones.

Antes del fracaso.

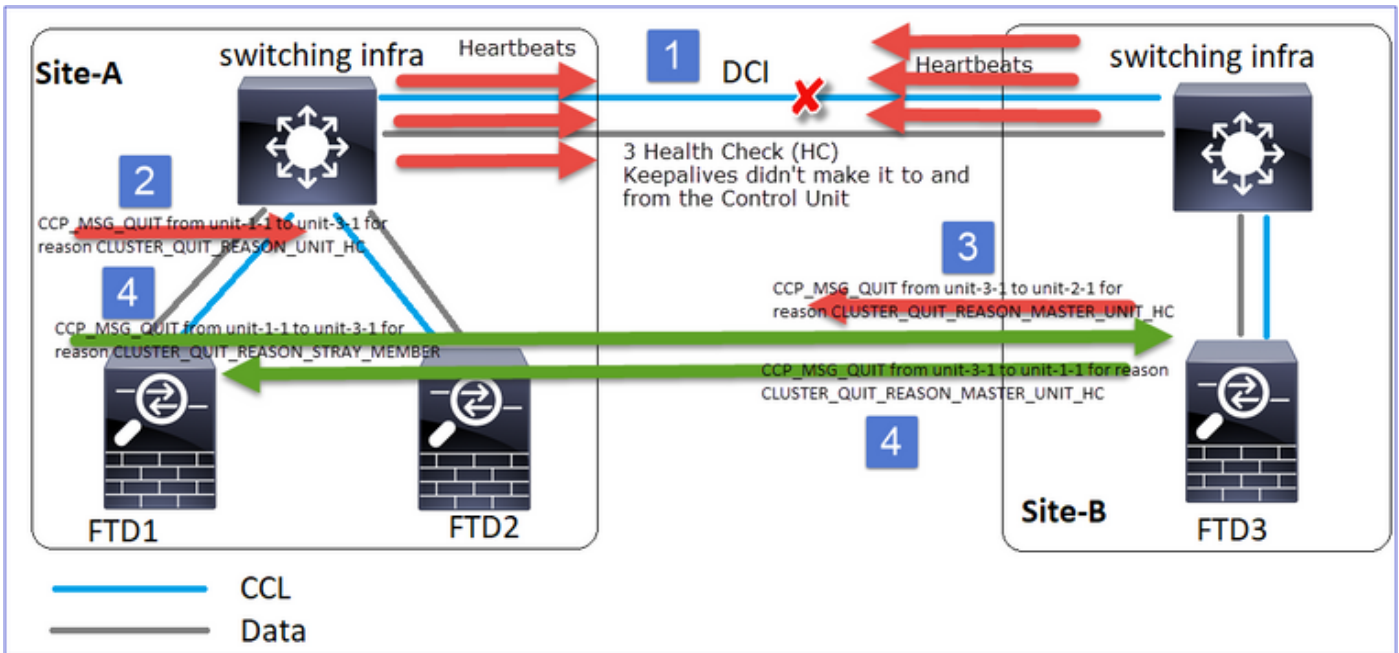
FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B
Nodo de control	Nodo de datos	Nodo de datos

Después de la recuperación (se cambió el nodo de control).

FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B

Nodo de datos	Nodo de control	Nodo de datos
---------------	-----------------	---------------

## Análisis



1. CCL se desactiva.
2. La Unidad-1-1 no obtiene 3 mensajes HC de la unidad-3-1 y envía un mensaje QUIT a la unidad-3-1. Este mensaje nunca llega a la unidad-3-1.
3. La unidad-3-1 envía un mensaje QUIT a la unidad-2-1. Este mensaje nunca llega a la unidad-2-1.

CCL se recupera.

4. La Unidad-1-1 ve que la unidad-3-1 se anuncia a sí misma como un nodo de control y envía el mensaje QUIT\_REASON\_STRAY\_MEMBER a la unidad-3-1. Una vez que la unidad-3-1 obtiene este mensaje, pasa al estado DISABLED. Al mismo tiempo, la unidad-3-1 envía un mensaje QUIT\_REASON\_PRIMARY\_UNIT\_HC a la unidad-1-1 y le pide que salga. Una vez que la unidad-1-1 recibe este mensaje pasa al estado DISABLED.

## Historial de clústeres

Unidad-1-1
<pre>&lt;#root&gt; 19:53:09 UTC Nov 2 2020 PRIMARY DISABLED     Received control message DISABLE         (primary unit health check failure)</pre>

```

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

#### Situación 4

Pérdida de comunicación de CCL durante aproximadamente 3-4 s

Antes del fracaso

FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B
Nodo de control	Nodo de datos	Nodo de datos

Después de la recuperación (el nodo de control cambió de sitio)

FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B
Nodo de datos	Nodo de datos	Nodo de control

### Análisis

### El fracaso

```

firepower#
firepower#
firepower#
firepower#
firepower#
firepower# Cluster disable is performing cleanup..done.
firepower# Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.
Cluster unit unit-1-1 transitioned from [redacted] to DISABLED
firepower#

firepower#
firepower#
firepower#
firepower#
firepower# Cluster disable is performing cleanup..done.
firepower# Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.
Cluster unit unit-2-1 transitioned from [redacted] to DISABLED
The 3DES/AES algorithms require a Encryption-3DES-AES activation key.
firepower#

firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower# WARNING: dynamic routing is not supported on management interface when cluster interface-mode is 'spanned'. If dynamic routing is configured on any management interface, please remove it.
Cluster unit unit-3-1 transitioned from [redacted]
    
```

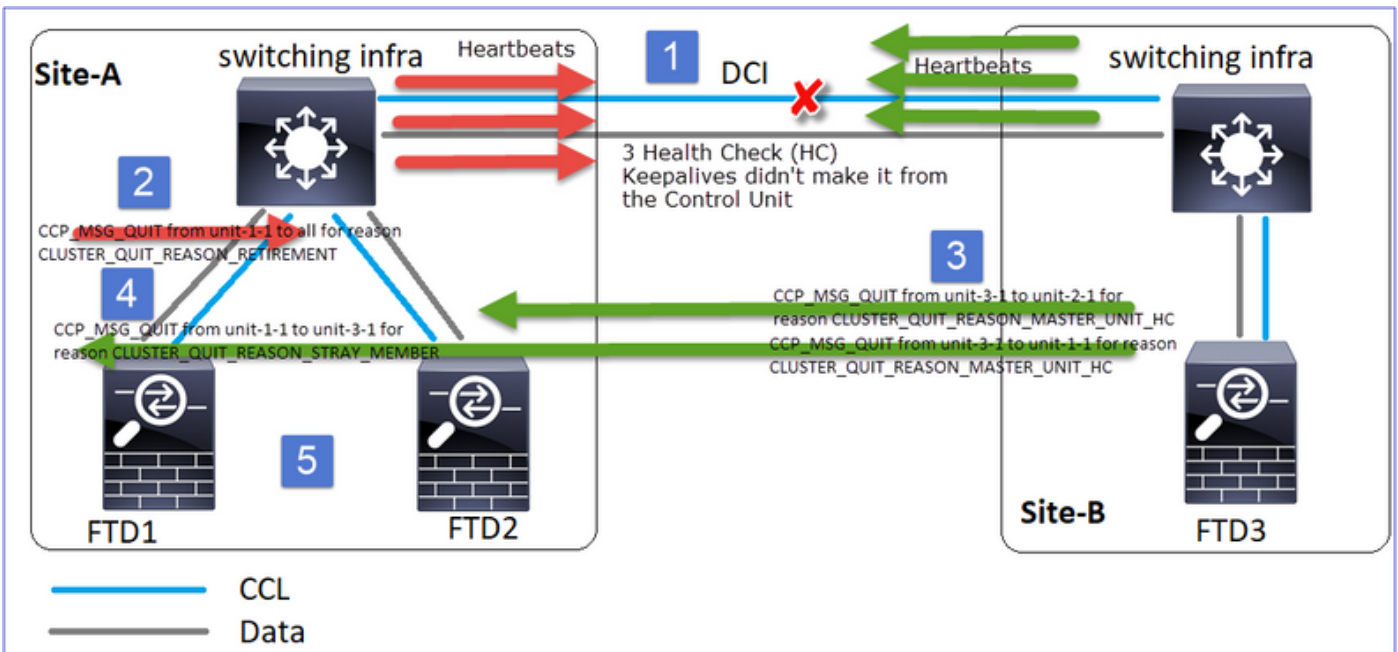
Un sabor diferente de la misma falla. En este caso, la unidad-1-1 tampoco recibió 3 mensajes de HC de la unidad-3-1, y una vez que recibió un nuevo keepalive, trató de expulsar la unidad-3-1 con el uso de un mensaje STRAY, pero el mensaje nunca llegó a la unidad-3-1:

```

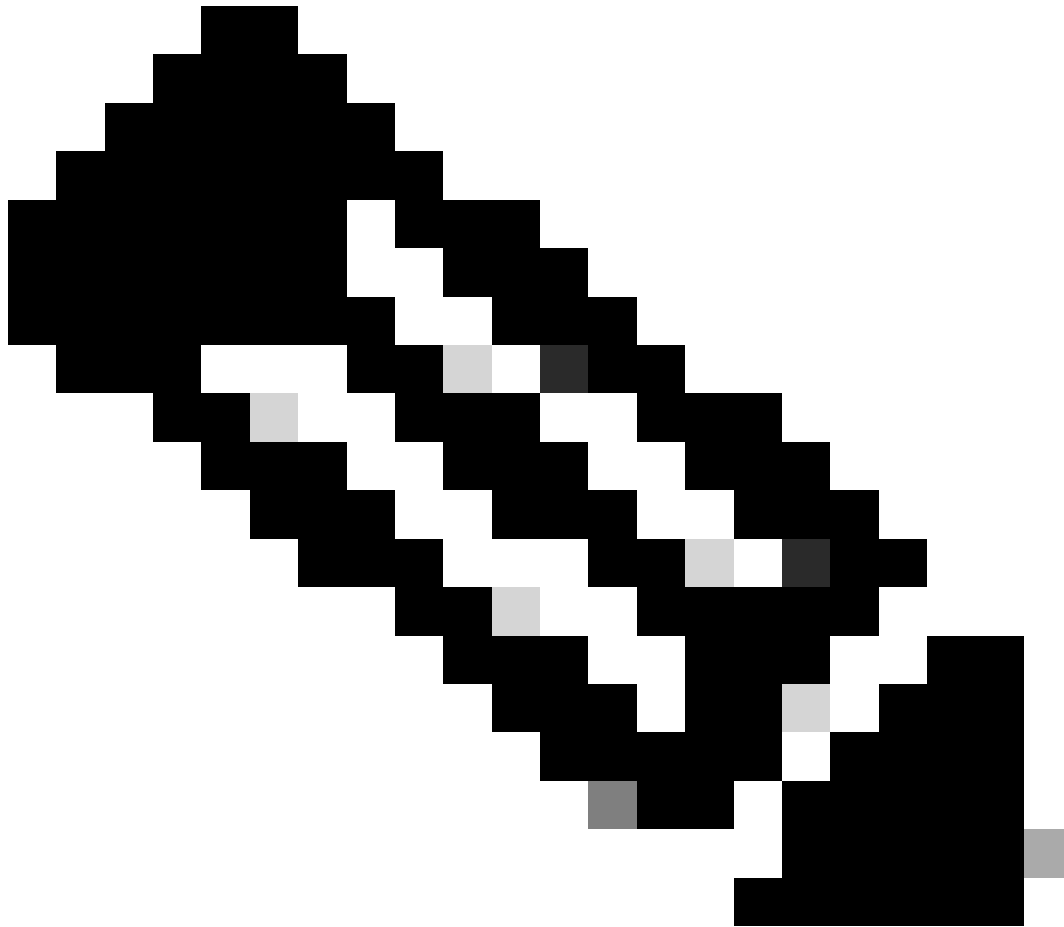
firepower#
firepower#
firepower#
firepower#
firepower# Asking slave unit unit-3-1 to quit because it failed unit health-check.
firepower# Forcing stray member unit-3-1 to leave the cluster
firepower# Forcing stray member unit-3-1 to leave the cluster
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.
Cluster unit unit-1-1 transitioned from [redacted] to DISABLED
firepower#

firepower#
firepower#
firepower#
firepower#
firepower# Cluster disable is performing cleanup..done.
firepower# Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.
Cluster unit unit-2-1 transitioned from [redacted] to DISABLED
The 3DES/AES algorithms require a Encryption-3DES-AES activation key.
firepower#

firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower#
firepower# WARNING: dynamic routing is not supported on management interface when cluster interface-mode is 'spanned'. If dynamic routing is configured on any management interface, please remove it.
Cluster unit unit-3-1 transitioned from [redacted]
    
```



1. CCL pasa a ser unidireccional durante unos segundos. La Unidad-3-1 no recibe 3 mensajes HC de la unidad-1-1 y se convierte en un nodo de control.
  2. La Unidad-2-1 envía un mensaje CLUSTER\_QUIT\_REASON\_RETIREMENT (difusión).
  3. La Unidad-3-1 envía un mensaje QUIT\_REASON\_PRIMARY\_UNIT\_HC a la unidad-2-1. La Unidad-2-1 lo recibe y sale del agrupamiento.
  4. La Unidad-3-1 envía un mensaje QUIT\_REASON\_PRIMARY\_UNIT\_HC a la unidad-1-1. La Unidad-1-1 lo recibe y sale del agrupamiento. CCL se recupera.
  5. Las unidades 1-1 y 2-1 se vuelven a unir al clúster como nodos de datos.
- 



Nota: Si en el paso 5 CCL no se recupera, en el sitio A el FTD1 se convierte en el nuevo nodo de control y, tras la recuperación de CCL, gana la nueva elección.

---

Mensajes de Syslog en la unidad-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
```

## Registros de seguimiento de clúster en la unidad-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
```

## Mensajes de Syslog en la unidad-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 to  
Nov 03 2020 23:13:10: %FTD-7-747006: Clustering:

State machine is at state PRIMARY

## Historial de clústeres

Unidad-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	

## Situación 5

### Antes del fracaso

FTD1	FTD2	FTD3
------	------	------



Sitio-A	Sitio-A	Sitio-B
Nodo de control	Nodo de datos	Nodo de datos

Después de la recuperación (sin cambios)

FTD1	FTD2	FTD3
Sitio-A	Sitio-A	Sitio-B
Nodo de control	Nodo de datos	Nodo de datos

El fracaso

The image shows three screenshots of Cisco Firepower CLI logs. The first screenshot shows a cluster unit transitioning to a disabled state. The second screenshot shows a warning about dynamic routing not being supported on a management interface. The third screenshot shows a cluster unit transitioning to a disabled state and a warning about local user database being empty.

La Unidad-3-1 envió mensajes QUIT tanto a la unidad-1-1 como a la unidad-2-1, pero debido a problemas de conectividad sólo la unidad-2-1 recibió el mensaje QUIT.

Registros de seguimiento de clúster de Unit-1-1:

```
<#root>
```

```
firepower#
```

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

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

Registros de seguimiento de clúster de Unit-2-1:

<#root>

firepower#

show cluster info trace | include QUIT

Nov 04 00:52:10.389 [DEBUG]Receive CCP message: CCP\_MSG\_QUIT from unit-3-1 for reason CLUSTER\_QUIT\_REASON  
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

### Historial de clústeres

Unidad-1-1	Unidad-2-1
No hay eventos	<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 message 00:51:54 UTC Nov 4 2020 SECONDARY_COLD          SECONDARY_APP_SYNC          Client progression done 00:52:42 UTC Nov 4 2020 SECONDARY_APP_SYNC          SECONDARY_CONFIG          SECONDARY application configu sync done 00:52:54 UTC Nov 4 2020 SECONDARY_CONFIG          SECONDARY_FILESYS          Configuration replication fir 00:52:55 UTC Nov 4 2020 SECONDARY_FILESYS          SECONDARY_BULK_SYNC          Client progression done 00:53:19 UTC Nov 4 2020 SECONDARY_BULK_SYNC  SECONDARY  Client progression done</pre>

--	--

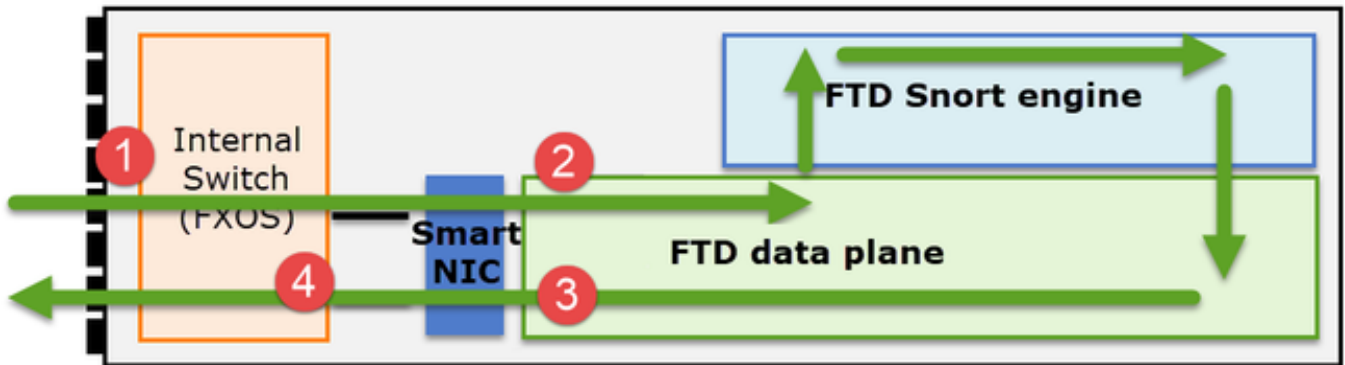
## Establecimiento de conexión de plano de datos de clúster

### Puntos de captura de NGFW

El NGFW ofrece funciones de captura en los siguientes puntos:

- Switch interno del chasis (FXOS)
- motor de plano de datos FTD
- Motor FTD Snort

Cuando resuelve problemas de trayectoria de datos en un clúster, los puntos de captura utilizados en la mayoría de los casos son las capturas del motor de plano de datos FXOS y FTD.



1. Captura de ingreso de FXOS en la interfaz física
2. Captura de ingreso de FTD en el motor del plano de datos
3. Captura de salida de FTD en el motor del plano de datos
4. Captura de ingreso de FXOS en la interfaz de backplane

Para obtener más información sobre las capturas de NGFW, consulte este documento:

### Fundamentos de roles de flujo de unidades de clúster

Las conexiones se pueden establecer a través de un clúster de varias maneras que dependen de factores como:

- Tipo de tráfico (TCP, UDP, etc.)
- Algoritmo de equilibrio de carga configurado en el switch adyacente
- Funciones configuradas en el firewall
- Condiciones de red (por ejemplo, fragmentación de IP, retrasos de red, etc.)

Función de flujo	Descripción	Indicador(es)
------------------	-------------	---------------

OWNER	Normalmente, la unidad que recibe inicialmente la conexión	UIO
Director	Unidad que gestiona las solicitudes de búsqueda de propietarios de los reenviadores.	S
Propietario de backup	Mientras el director no sea la misma unidad que el propietario, el director también será el propietario de la copia de seguridad. Si el propietario se elige a sí mismo como director, se elige un propietario de copia de seguridad independiente.	Y (si el director es también el propietario de la copia de seguridad) y (si el director no es el propietario de la copia de seguridad)
Reenviador	Unidad que reenvía paquetes al propietario	Z
Propietario del fragmento	La unidad que maneja el tráfico fragmentado	-
Respaldo del chasis	En un clúster entre chasis, cuando los flujos director/respaldo y propietario son propiedad de las unidades del mismo chasis, una unidad en uno de los otros chasis se convierte en un respaldo/director secundario.  Esta función es específica para los clústeres entre chasis de Firepower serie 9300 con más de un blade.	W

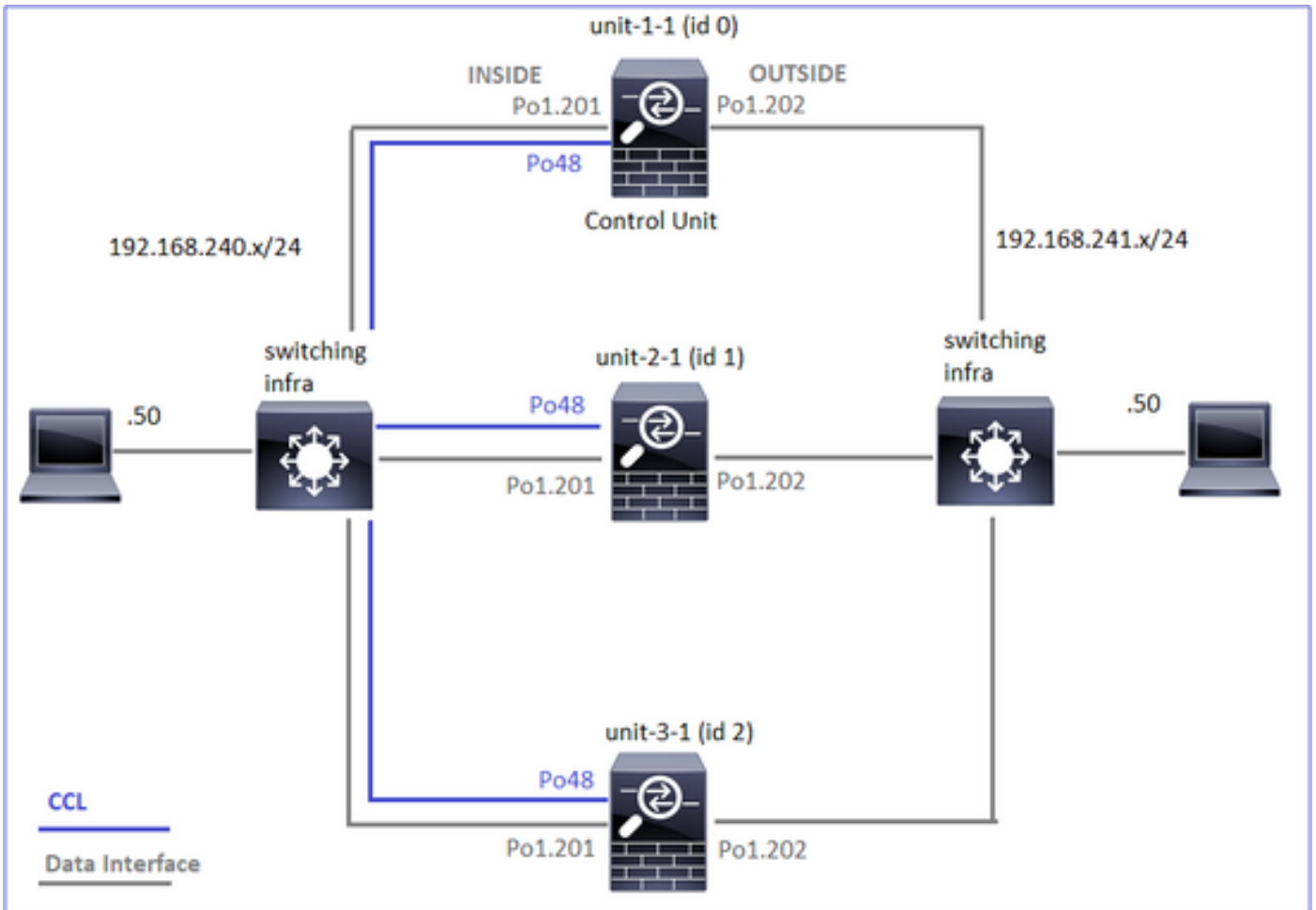
- Para obtener más información, consulte la sección relacionada de la Guía de configuración (consulte los enlaces de la Información relacionada)
- En escenarios específicos (consulte la sección de casos prácticos), algunos indicadores no siempre se muestran.

#### Casos prácticos de establecimiento de conexión a clústeres

En la siguiente sección se describen varios casos prácticos que muestran algunas de las formas en que se puede establecer una conexión a través de un clúster. Los objetivos son:

- Familiarícese con los distintos roles de las unidades.
- Demuestre cómo se pueden correlacionar los distintos resultados de comandos.

Topología



Unidades de clúster e ID:


Unidad-1-1	Unidad-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 </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 </pre>

```
CCL IP      : 10.17.1.1
CCL MAC     : 0015.c500.018f
Last join   : 02:24:43 UTC Nov 27 2020
Last leave  : N/A
```

Last Leave: N/A

### Capturas de clúster habilitadas:

```
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
```

 Nota: Estas pruebas se ejecutaron en un entorno de laboratorio con un tráfico mínimo a través del clúster. En la producción, intente utilizar los filtros de captura más específicos posibles (por ejemplo, el puerto de destino y, siempre que sea posible, el puerto de origen) para minimizar el "ruido" en las capturas.

### Caso práctico 1. Tráfico simétrico (el propietario es también el director)

Observación 1. Las capturas de reinyección-ocultación muestran paquetes solamente en la unidad-1-1. Esto significa que el flujo en ambas direcciones pasó por la unidad-1-1 (tráfico simétrico):

<#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
```

Observación 2. Análisis del indicador de conexión para el flujo con el puerto de origen 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

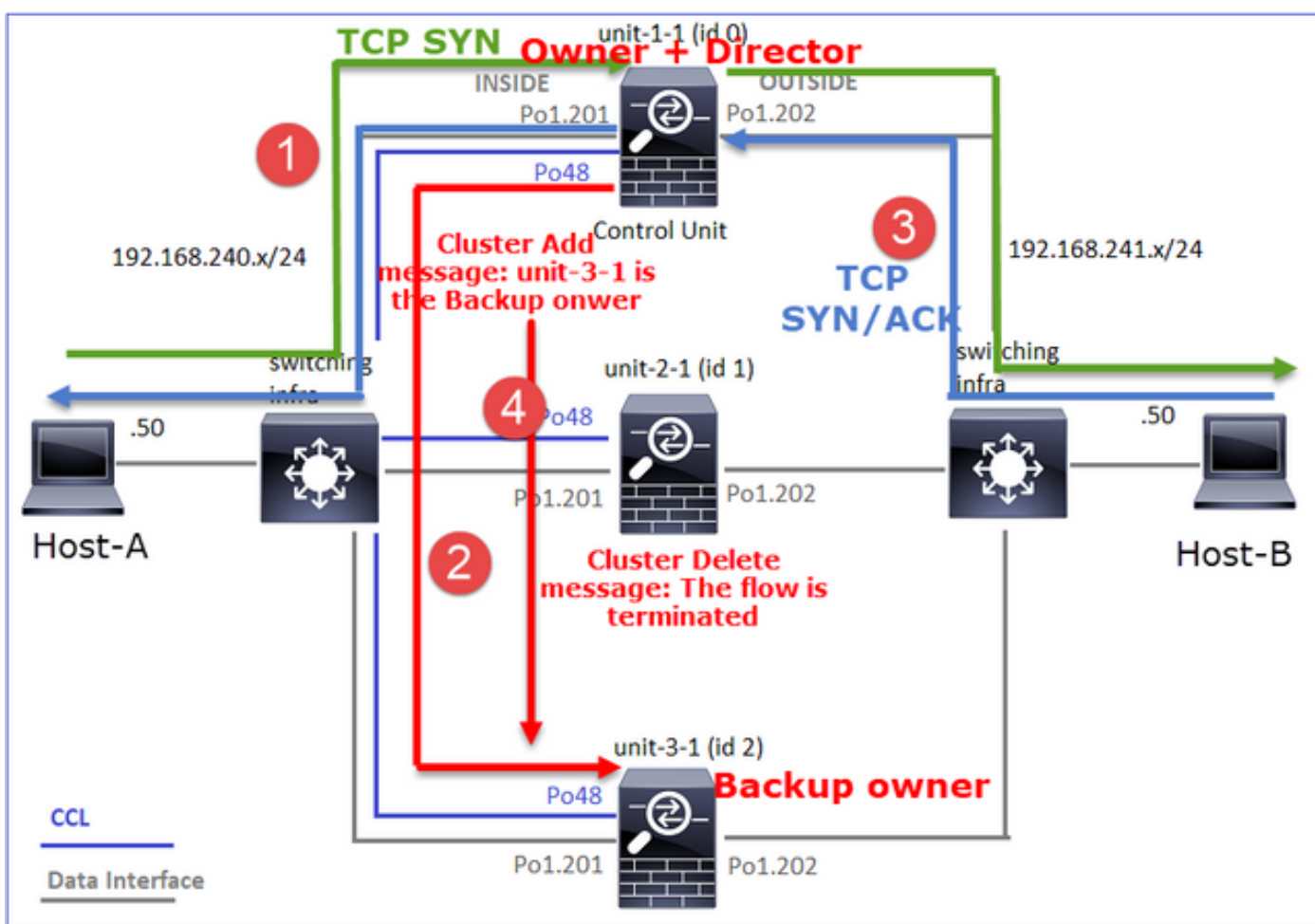
```

Unidad	Indicador	Nota
Unidad-1-1	UIO	<ul style="list-style-type: none"> <li>· Propietario de flujo: la unidad maneja el flujo</li> <li>· Director: dado que la unidad-3-1 tiene "y" y no "Y", esto implica que</li> </ul>



		la unidad-1-1 fue elegida como el director para este flujo. Por lo tanto, dado que también es el propietario, se eligió otra unidad (unit-3-1 en este caso) como propietario de la copia de seguridad
Unidad-2-1	-	-
Unidad-3-1	s	La unidad es un propietario de respaldo

Esto se puede visualizar como:



1. El paquete TCP SYN llega del Host-A a la unidad-1-1. La unidad-1-1 se convierte en el propietario del flujo.
2. La Unidad-1-1 también es elegida directora de flujo. Por lo tanto, también elige la unidad-3-1 como el propietario de la copia de seguridad (mensaje de adición de clúster).
3. El paquete TCP SYN/ACK llega del Host B a la unidad 3-1. El flujo es simétrico.
4. Una vez finalizada la conexión, el propietario envía un mensaje de eliminación de clúster para quitar la información de flujo del propietario de la copia de seguridad.

Observación 3. Capturar con traza muestra que ambas direcciones van solo a través de la unidad-1-1.

Paso 1. Identifique el flujo y los paquetes de interés en todas las unidades de agrupamiento basadas en el puerto de origen:

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

Paso 2. Dado que se trata de un flujo TCP, realice un seguimiento de los paquetes de entrada en contacto de 3 vías. Como se puede ver en esta salida, la unidad-1-1 es el propietario. Para simplificar, se omiten las fases de seguimiento no relevantes:

```
<#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

...

El tráfico de retorno (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
```

Observación 4. Los syslogs del plano de datos FTD muestran la creación y terminación de la conexión en todas las unidades:

```
<#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
```

Caso práctico 2. Tráfico simétrico (el propietario es distinto del director)

- Igual que en el caso práctico #1, pero en este caso práctico, el propietario de un flujo es una unidad diferente a la del director.
- Todos los resultados son similares al caso práctico #1. La diferencia principal en comparación con el caso práctico #1 es el indicador "Y" que sustituye al indicador "y" del escenario 1.

Observación 1. El propietario es diferente del director.

Análisis del indicador de conexión para el flujo con el puerto de origen 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:
```

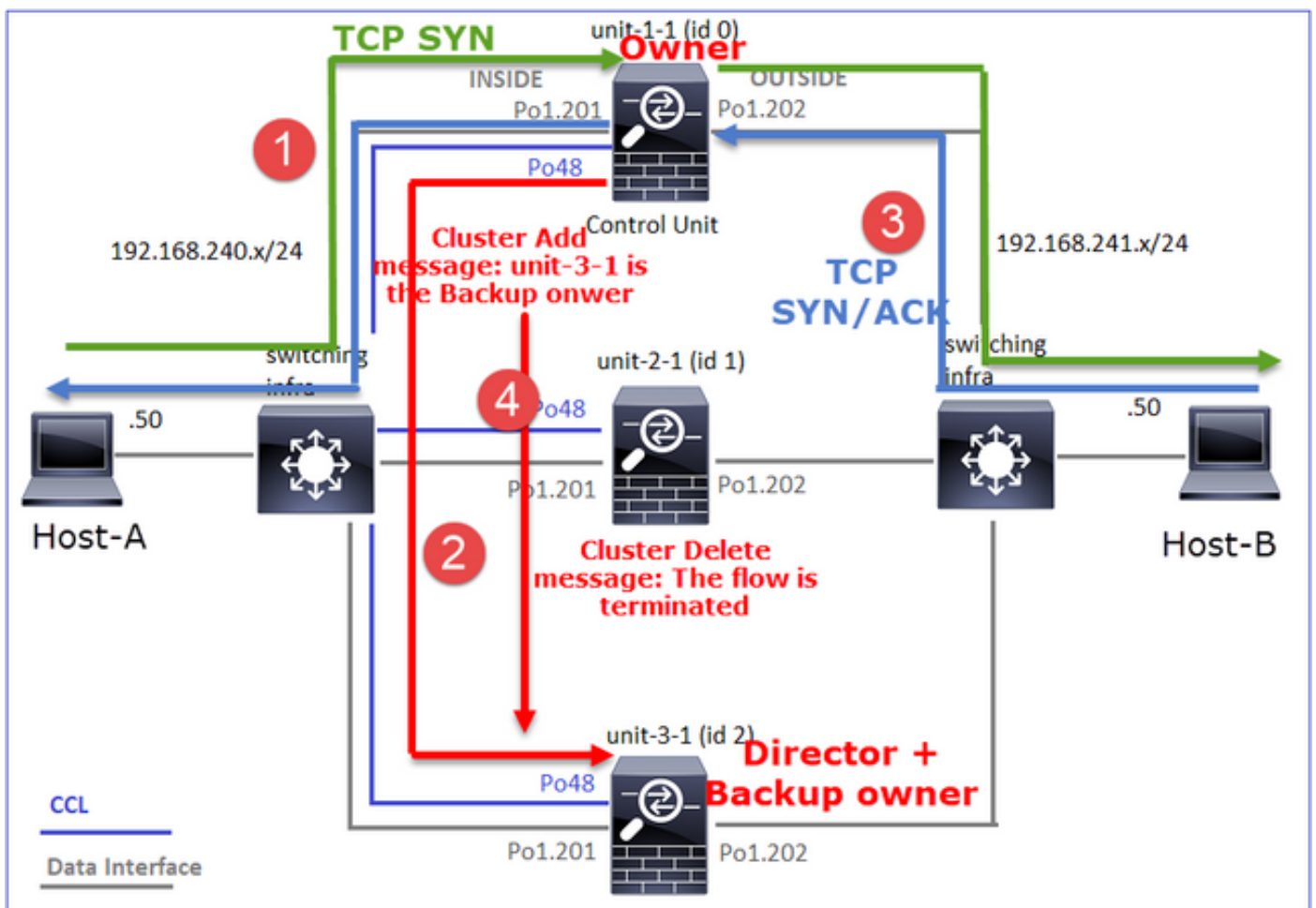
46278

, idle 0:00:06, bytes 0,

flags Y

Unidad	Indicador	Nota
Unidad-1-1	UIO	· Propietario de flujo: la unidad maneja el flujo
Unidad-2-1	-	-
Unidad-3-1	S	· Director y Propietario de Respaldo - La Unidad 3-1 tiene el indicador Y (Director).

Esto se puede visualizar como:



1. El paquete TCP SYN llega del Host-A a la unidad-1-1. La unidad-1-1 se convierte en el propietario del flujo.
2. La Unidad 3-1 es elegida como el director de flujo. Unit-3-1 también es el propietario de la

- copia de seguridad (mensaje 'cluster add' en UDP 4193 sobre CCL).
- 3. El paquete TCP SYN/ACK llega del Host B a la unidad 3-1. El flujo es simétrico.
- 4. Una vez que se termina la conexión, el propietario envía a través de CCL un mensaje de 'eliminación de clúster' en UDP 4193 para eliminar la información de flujo del propietario de la copia de seguridad.

Observación 2. La captura con traza muestra que ambas direcciones pasan solamente por la unidad-1-1

Paso 1. Utilice el mismo enfoque que en el caso práctico 1 para identificar el flujo y los paquetes de interés en todas las unidades de clúster basadas en el puerto de origen:

```
<#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#
```

Captura en la interfaz EXTERNA:

```
<#root>
```

```
firepower#
```

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

```
unit-1-1
```

(LOCAL):\*\*\*\*\*

3: 11:01:44.841921 802.1Q v1an#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 v1an#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 v1an#202 PO 192.168.240.50.46278 > 192.168.241.50.80: . ack 3382481338 win 22

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

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

firepower#

## Paso 2. Enfoque en los paquetes de ingreso (TCP SYN y 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 v1an#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>

...

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
```

Rastree el SYN/ACK en la unidad-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
```

Observación 3. Los syslogs del plano de datos FTD muestran la creación y terminación de la conexión en propietario y propietario de respaldo:

```
<#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

### Caso práctico 3. Tráfico asimétrico (director reenvía el tráfico).

Observación 1. Las capturas de reinyección-ocultación muestran paquetes en la unidad-1-1 y la unidad-2-1 (flujo asimétrico):

```
<#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

Observación 2. Análisis del indicador de conexión para el flujo con el puerto de origen 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

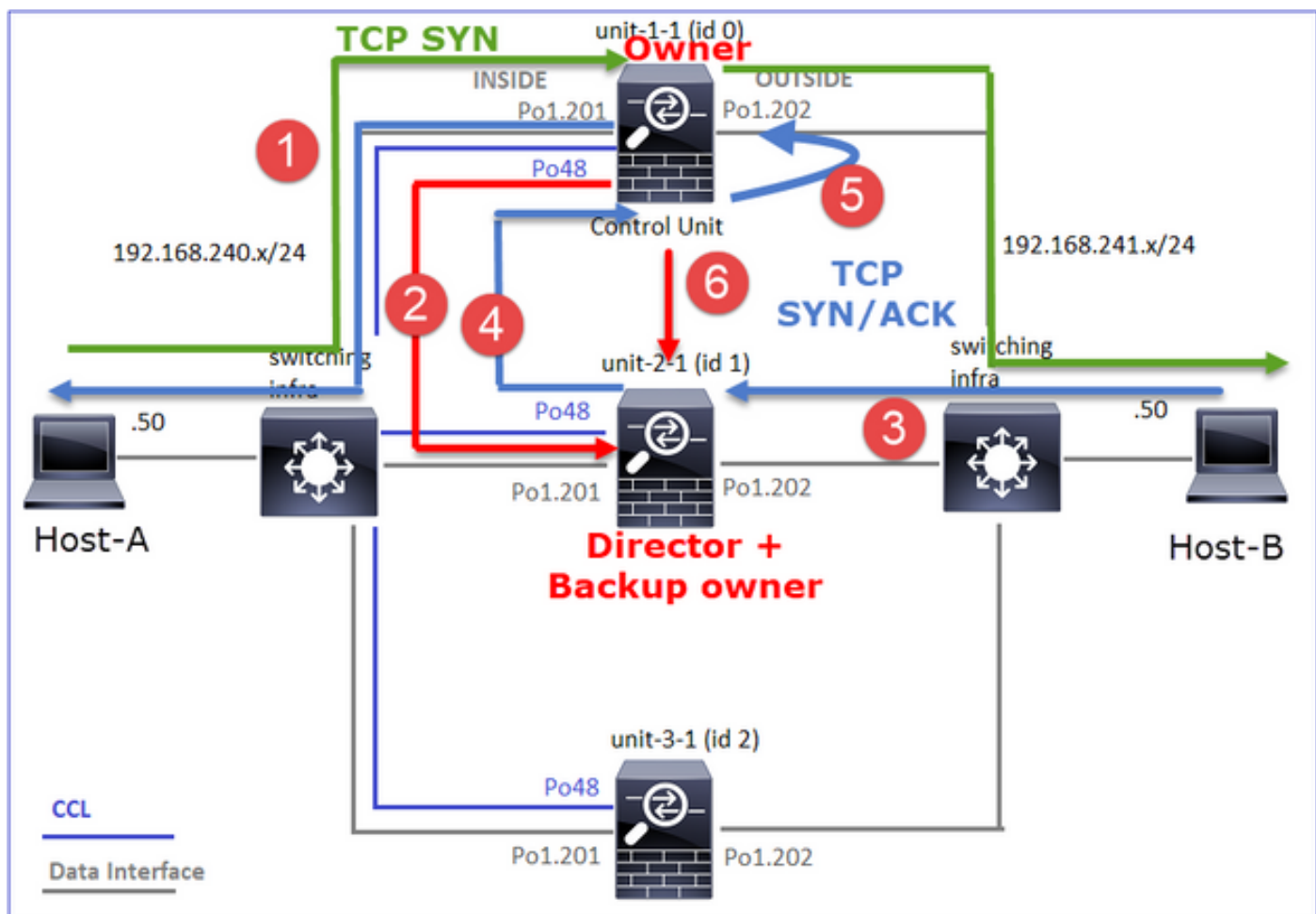
TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:  
 46502  
 , idle 0:00:00, bytes 0,  
 flags Y

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

Unidad	Indicador	Nota
Unidad-1-1	UIO	· Propietario de flujo: la unidad maneja el flujo.
Unidad-2-1	S	· Director: dado que la unidad-2-1 tiene el indicador "Y", esto implica que la unidad-2-1 fue elegida como el director para este flujo. · Propietario de respaldo

		<p>· Finalmente, aunque no es obvio a partir de esta salida, a partir de las salidas show capture y show log es evidente que la unidad-2-1 reenvía este flujo al propietario (aunque técnicamente no se considera un reenviador en este escenario).</p> <p>Nota: Una unidad no puede ser tanto director (flujo Y) como reenviador (flujo z), estas dos funciones se excluyen mutuamente. Los directores (flujo Y) aún pueden reenviar tráfico. Vea el resultado de show log más adelante en este caso práctico.</p>
Unidad-3-1	-	-

Esto se puede visualizar como:



1. El paquete TCP SYN llega del Host-A a la unidad-1-1. La unidad-1-1 se convierte en el propietario del flujo.
2. La Unidad 2-1 se elige como director de flujo y propietario de la copia de seguridad. El propietario del flujo envía un mensaje de unidifusión 'cluster add' en UDP 4193 para informar al propietario de la copia de seguridad sobre el flujo.
3. El paquete TCP SYN/ACK llega del Host B a la unidad 2-1. El flujo es asimétrico.
4. Unit-2-1 reenvía el paquete a través de CCL al propietario (debido a TCP SYN Cookie).

5. El propietario reinyecta el paquete en la interfaz OUTSIDE y luego reenvía el paquete hacia el Host-A.
6. Una vez finalizada la conexión, el propietario envía un mensaje de eliminación de clúster para quitar la información de flujo del propietario de la copia de seguridad.

Observación 3. La captura con traza muestra el tráfico asimétrico y la redirección de la unidad-2-1 a la unidad-1-1.

Paso 1. Identifique los paquetes que pertenecen al flujo de interés (puerto 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:*****
```

Dirección de retorno:

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

Paso 2. Seguimiento de los paquetes. De forma predeterminada, sólo se realiza un seguimiento de los primeros 50 paquetes de ingreso. Para simplificar, se omiten las fases de seguimiento no relevantes.

Unidad-1-1 (propietario):

<#root>

firepower#

cluster exec show capture CAPI packet-number 3 trace

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

3: 12:58:33.356121 802.1Q vlan#201 P0 192.168.240.50.

46502

> 192.168.241.50.80:

S

4124514680:4124514680(0) win 29200 <mss 1460,sackOK,timestamp 510537534 0,nop,wscale 7>

...

Phase: 4

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'INSIDE'

Flow type: NO FLOW

I (0) got initial, attempting ownership.

Phase: 5

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'INSIDE'

Flow type: NO FLOW

I (0) am becoming owner

Unidad 2-1 (reenviador)

El tráfico de retorno (TCP SYN/ACK). La unidad de interés es la unidad-2-1, que es el director/propietario de la copia de seguridad y reenvía el tráfico al propietario:

<#root>

firepower#

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

1: 12:58:33.359249 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.

46502

```
: S 4257314722:4257314722(0) ack 1434968588 win 28960 <mss 1460,sackOK,timestamp 520893004 510537534,no
...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
```

I (1) got initial, attempting ownership.

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

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

Observación 4. Los syslogs del plano de datos FTD muestran la creación y terminación de la conexión en todas las unidades:

```
<#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#
```

#### Caso práctico 4. Tráfico asimétrico (el propietario es el director)

Observación 1. Las capturas de reinyección-ocultación muestran paquetes en la unidad-1-1 y la unidad-2-1 (flujo asimétrico):

```
<#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

```

Observación 2. Análisis del indicador de conexión para el flujo con el puerto de origen 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
```

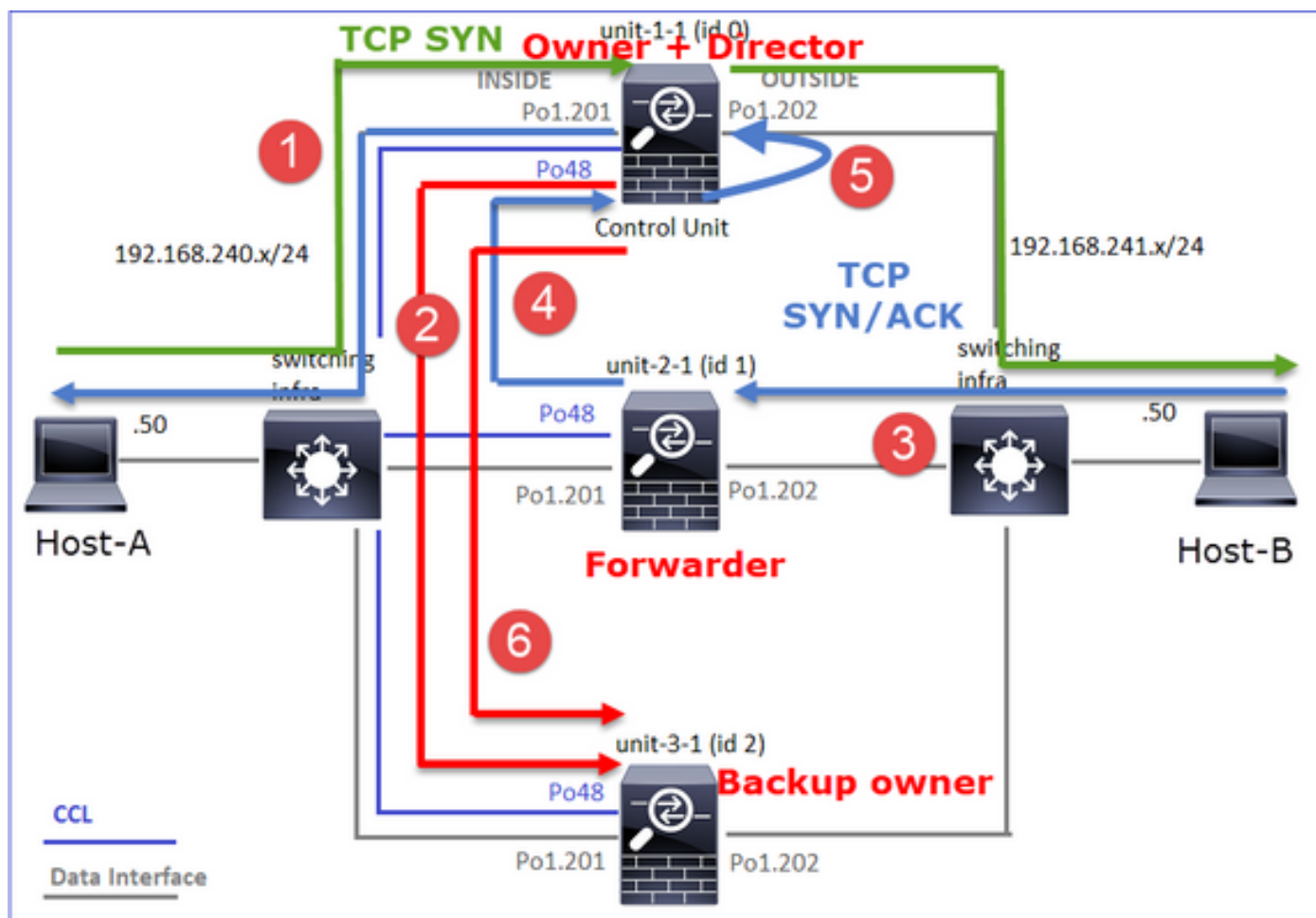
unit-3-1

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

Unidad	Indicador	Nota
Unidad-1-1	UIO	<ul style="list-style-type: none"><li>· Propietario de flujo: la unidad maneja el flujo</li><li>· Director: dado que la unidad-3-1 tiene "y" y no "Y", esto implica que la unidad-1-1 fue elegida como el director para este flujo. Por lo tanto, dado que también es el propietario, se eligió otra unidad (unit-3-1 en este caso) como propietario de la copia de seguridad</li></ul>

Unidad-2-1	z	· Reenviador
Unidad-3-1	s	- Propietario de respaldo

Esto se puede visualizar como:



1. El paquete TCP SYN llega del Host-A a la unidad-1-1. La unidad-1-1 se convierte en el propietario del flujo y se elige como director.
2. La Unidad 3-1 se elige como propietario de respaldo. El propietario del flujo envía un mensaje 'cluster add' de unidifusión en UDP 4193 para informar al propietario de la copia de seguridad sobre el flujo.
3. El paquete TCP SYN/ACK llega del Host B a la unidad 2-1. El flujo es asimétrico.
4. Unit-2-1 reenvía el paquete a través de CCL al propietario (debido a TCP SYN Cookie).
5. El propietario reinyecta el paquete en la interfaz OUTSIDE y luego reenvía el paquete hacia el Host-A.
6. Una vez finalizada la conexión, el propietario envía un mensaje de eliminación de clúster para quitar la información de flujo del propietario de la copia de seguridad.

Observación 3. La captura con traza muestra el tráfico asimétrico y la redirección de la unidad-2-1 a la unidad-1-1.

## Unidad 2-1 (reenviador)

<#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).
```

Observación 4. Los syslogs del plano de datos FTD muestran la creación y terminación de la conexión en todas las unidades:

- Unidad-1-1 (propietario)
- Unidad 2-1 (reenviador)
- Unidad-3-1 (propietario de la copia de seguridad)

<#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)  
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)  
Dec 01 2020 16:11:42: %FTD-6-302023:
```

```
Teardown forwarder TCP connection
```

```
for OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46916 duration 0:00:09 forwarded bytes 1024009
```

```
unit-3-1:*****  
Dec 01 2020 16:11:33: %FTD-6-302022:
```

```
Built backup stub TCP connection
```

```
for INSIDE:192.168.240.50/46916 (192.168.240.50/46916) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80)  
Dec 01 2020 16:11:42: %FTD-6-302023:
```

```
Teardown backup TCP connection
```

```
for INSIDE:192.168.240.50/46916 to OUTSIDE:192.168.241.50/80 duration 0:00:09 forwarded bytes 0 Cluste
```

Caso práctico 5. Tráfico asimétrico (el propietario es diferente del director).

Observación 1. Las capturas de reinyección-ocultación muestran paquetes en la unidad-1-1 y la unidad-2-1 (flujo asimétrico):

```
<#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
```

Observación 2. Análisis del indicador de conexión para el flujo con el puerto de origen 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:

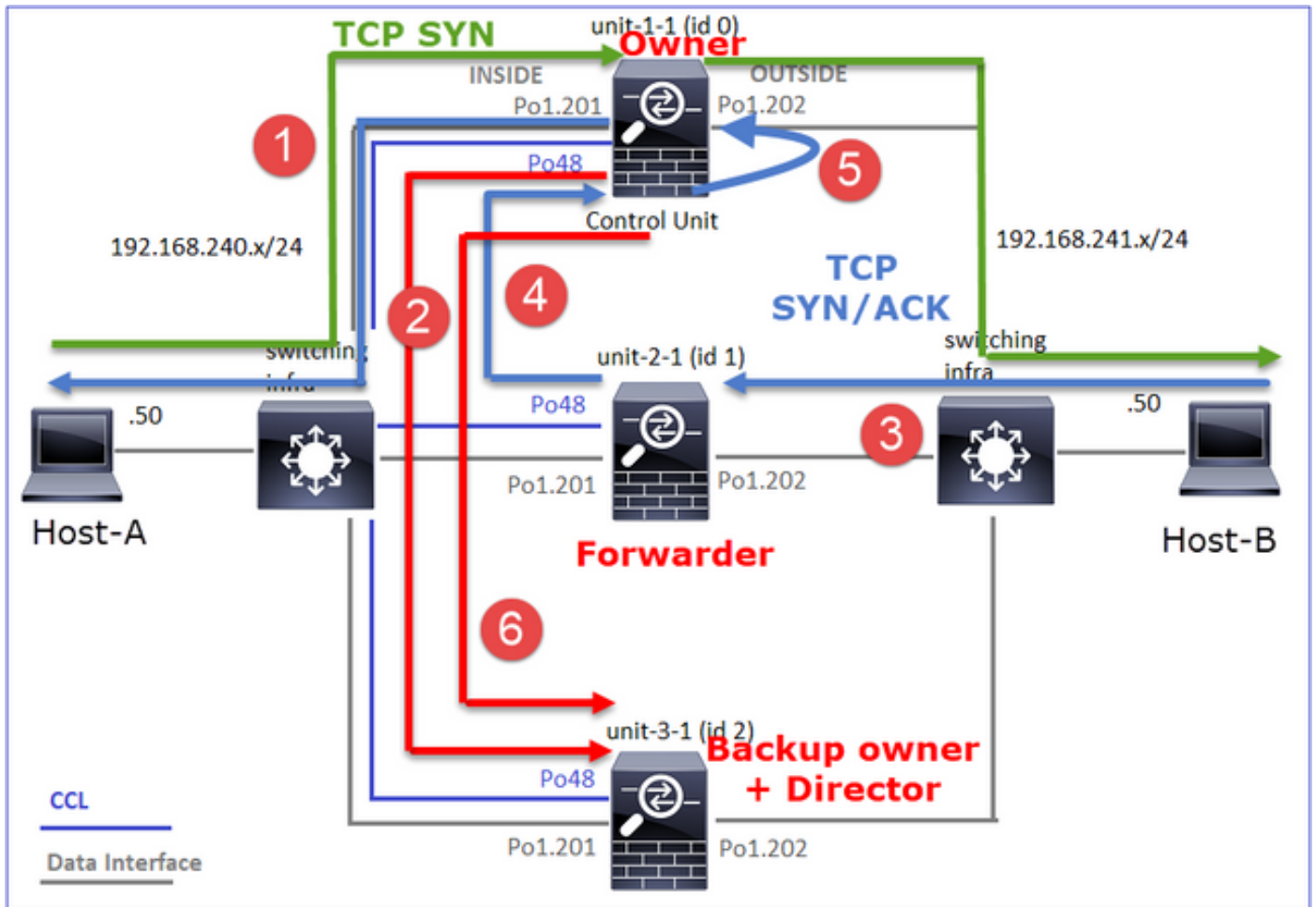
46994

, idle 0:00:05, bytes 0,

flags Y

Unidad	Indicador	Nota
Unidad-1-1	UIO	· Propietario de flujo: la unidad maneja el flujo
Unidad-2-1	z	· Reenviador
Unidad-3-1	S	· Propietario de respaldo · Director

Esto se puede visualizar como:



1. El paquete TCP SYN llega del Host-A a la unidad-1-1. La unidad-1-1 se convierte en el propietario del flujo.
2. La Unidad 3-1 es elegida como directora y propietaria de respaldo. El propietario del flujo envía un mensaje de unidifusión 'cluster add' en UDP 4193 para informar al propietario de la copia de seguridad sobre el flujo.
3. El paquete TCP SYN/ACK llega del Host B a la unidad 2-1. El flujo es asimétrico
4. Unit-2-1 reenvía el paquete a través de CCL al propietario (debido a TCP SYN Cookie).
5. El propietario reinyecta el paquete en la interfaz OUTSIDE y luego reenvía el paquete hacia el Host-A.
6. Una vez finalizada la conexión, el propietario envía un mensaje de eliminación de clúster para quitar la información de flujo del propietario de la copia de seguridad.

Observación 3. La captura con traza muestra el tráfico asimétrico y la redirección de la unidad-2-1 a la unidad-1-1.

Unidad-1-1 (propietario)

```
<#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

Unidad 2-1 (reenviador)

<#root>

firepower#

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

1: 16:46:44.232074 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.

46994

: S 2863659376:2863659376(0) ack 2879616990 win 28960 <mss 1460,sackOK,timestamp 534583774 524228304,no

...  
Phase: 4  
Type: CLUSTER-EVENT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Input interface: 'OUTSIDE'  
Flow type: NO FLOW

I (1) got initial, attempting ownership.

Phase: 5  
Type: CLUSTER-EVENT  
Subtype:  
Result: ALLOW  
Config:

Additional Information:  
Input interface: 'OUTSIDE'  
Flow type: NO FLOW

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

Observación 4. Los syslogs del plano de datos FTD muestran la creación y terminación de la conexión en todas las unidades:

- Unidad-1-1 (propietario)
- Unidad 2-1 (reenviador)
- Unit-3-1 (backup owner/director)

<#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 (192.168.241.50/80)

Dec 01 2020 16:46:53: %FTD-6-302014:

Teardown TCP connection

10080 for INSIDE:192.168.240.50/46994 to OUTSIDE:192.168.241.50/80 duration 0:00:09 bytes 1024000440 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)

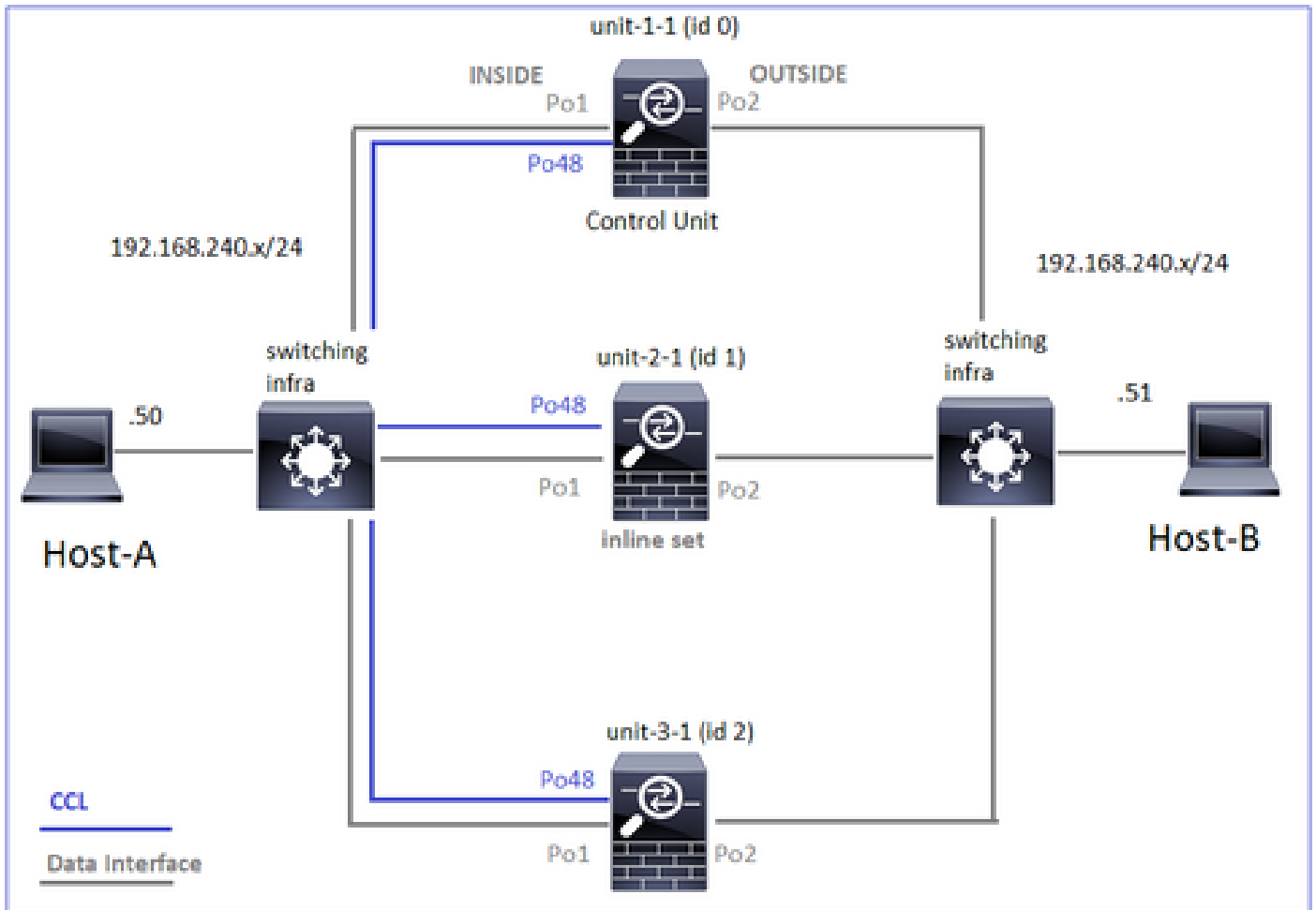
Dec 01 2020 16:46:53: %FTD-6-302023:

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

Para los siguientes casos prácticos, la topología utilizada se basa en un clúster con conjuntos en

línea:



### Caso práctico 6. Tráfico asimétrico (conjunto en línea, el propietario es el director)

Observación 1. Las capturas de reinyección-ocultación muestran paquetes en la unidad-1-1 y la unidad-2-1 (flujo asimétrico). Además, el propietario es la unidad-2-1 (hay paquetes en las interfaces INSIDE y OUTSIDE para las capturas de reinyección y ocultación, mientras que la unidad-1-1 sólo tiene en OUTSIDE):

```
<#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

Observación 2. Análisis del indicador de conexión para el flujo con el puerto de origen 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:

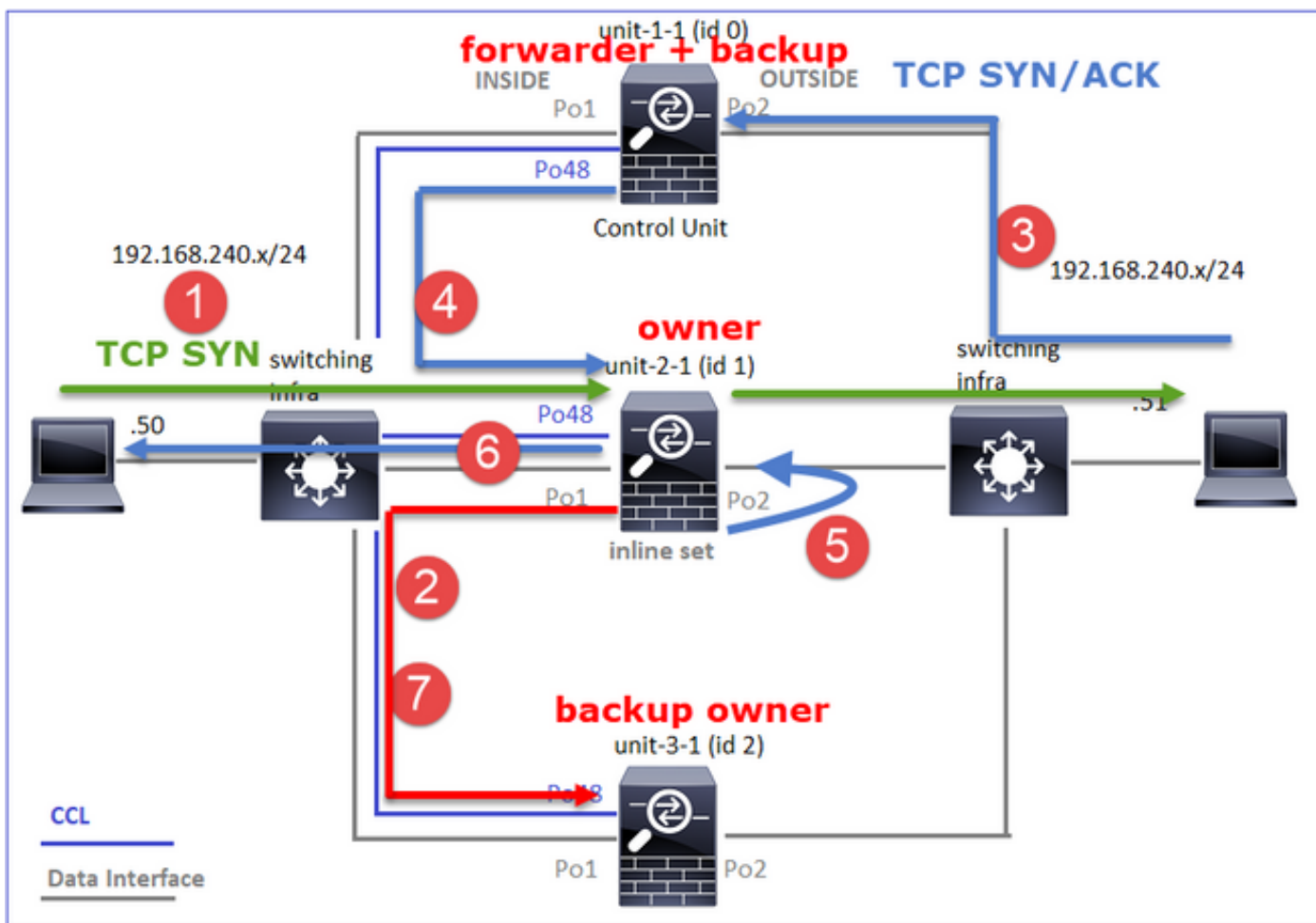
fwd connections: 0 in use, 5 most used

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

Unidad	Indicador	Nota
Unidad-1-1	z	· Reenviador
Unidad-2-1	b N	· Propietario de flujo: la unidad maneja el flujo
Unidad-3-1	s	· Propietario de respaldo

Esto se puede visualizar como:



1. El paquete TCP SYN llega del Host-A a la unidad-2-1. La unidad-2-1 se convierte en el



propietario del flujo y se elige como el director.

2. La Unidad 3-1 es elegida como propietario de la copia de seguridad. El propietario del flujo envía un mensaje de unidifusión 'cluster add' en UDP 4193 para informar al propietario de la copia de seguridad sobre el flujo.
3. El paquete TCP SYN/ACK llega del Host B a la unidad 1-1. El flujo es asimétrico.
4. La unidad 1-1 reenvía el paquete a través de la CCL al director (unidad 2-1).
5. La Unidad 2-1 también es el propietario y reinyecta el paquete en la interfaz OUTSIDE.
6. La Unidad 2-1 reenvía el paquete hacia el Host A.
7. Una vez finalizada la conexión, el propietario envía un mensaje de eliminación de clúster para quitar la información de flujo del propietario de la copia de seguridad.

Observación 3. La captura con traza muestra el tráfico asimétrico y la redirección de la unidad-1-1 a la unidad-2-1.

Unidad 2-1 (propietario/director)

<#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
```

Unidad-1-1 (reenviador)

<#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).

Tráfico de retorno (TCP SYN/ACK)

Unidad 2-1 (propietario/director)

<#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  
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

Observación 4. Los syslogs del plano de datos FTD muestran la creación y terminación de la conexión en todas las unidades:

- Unidad-1-1 (propietario)
- Unidad 2-1 (reenviador)
- Unit-3-1 (backup owner/director)

```
<#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
```

Caso práctico 7. Tráfico asimétrico (conjunto en línea, el propietario es diferente del director)

El propietario es la unidad-2-1 (hay paquetes en las interfaces INSIDE y OUTSIDE para las capturas de reinyección y ocultación, mientras que la unidad-3-1 sólo tiene en OUTSIDE):

```
<#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
```

Observación 2. Análisis del indicador de conexión para el flujo con el puerto de origen 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:

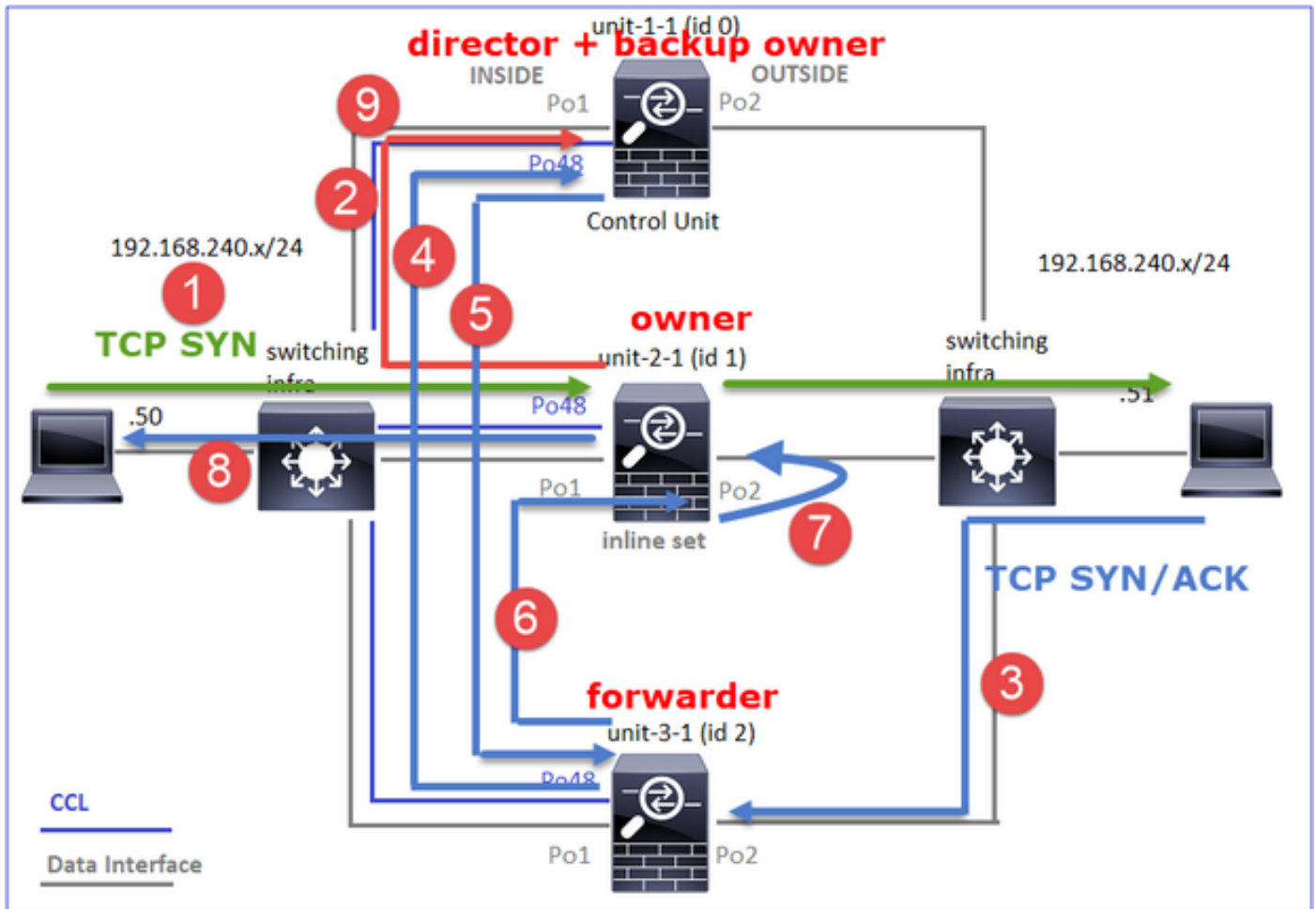
59210

, idle 0:00:00, bytes 0,

flags z

Unidad	Indicador	Nota
Unidad-1-1	S	· Director/Propietario de copia de seguridad
Unidad-2-1	b N	· Propietario de flujo: la unidad maneja el flujo
Unidad-3-1	z	· Reenviador

Esto se puede visualizar como:



1. El paquete TCP SYN llega del Host-A a la unidad-2-1. La unidad-2-1 se convierte en el propietario del flujo y la unidad-1-1 se elige como el director
2. La unidad 1-1 se elige como propietario de la copia de seguridad (ya que es el director). El propietario del flujo envía un mensaje de unidifusión 'cluster add' en UDP 4193 a. informe al propietario de la copia de seguridad sobre el flujo.
3. El paquete TCP SYN/ACK llega del Host B a la unidad 3-1. El flujo es asimétrico.
4. La Unidad-3-1 reenvía el paquete a través del CCL al director (unidad-1-1).
5. La Unidad-1-1 (director) sabe que el propietario es la unidad-2-1, envía el paquete al reenviador (unidad-3-1) y le notifica que el propietario es la unidad-2-1.
6. La unidad-3-1 envía el paquete a la unidad-2-1 (propietario).
7. La Unidad 2-1 reinyecta el paquete en la interfaz OUTSIDE.
8. La Unidad 2-1 reenvía el paquete hacia el Host A.
9. Una vez finalizada la conexión, el propietario envía un mensaje de eliminación de clúster para quitar la información de flujo del propietario de la copia de seguridad.

✍ Nota: Es importante que el paso 2 (paquete a través de CCL) se produzca antes del paso 4 (tráfico de datos). En otro caso (por ejemplo, la condición de carrera), el director no es consciente del flujo. Por lo tanto, dado que es un conjunto en línea, reenvía el paquete hacia el destino. Si las interfaces no están en un conjunto en línea, el paquete de datos se descarta.

Observación 3. La captura con traza muestra el tráfico asimétrico y los intercambios a través de la

CCL:

Tráfico de reenvío (TCP SYN)

Unidad-2-1 (propietario)

<#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
```

Tráfico de retorno (TCP SYN/ACK)

La unidad 3-1 (ID 2 - reenviador) envía el paquete a través de CCL a la unidad 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) sabe que el propietario del flujo es unit-2-1 (ID 1) y envía el paquete a través de CCL de vuelta a unit-3-1 (ID 2 - reenviador).

<#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).

La Unidad-3-1 (ID 2 - reenviador) obtiene el paquete a través de la CCL y lo envía a la unidad-2-1 (ID 1 - propietario).

<#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).
```

El propietario reinyecta y reenvía el paquete hacia el destino:

```
<#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).
```

Observación 4. Los syslogs del plano de datos FTD muestran la creación y terminación de la conexión en todas las unidades:

- Unit-1-1 (director/propietario de la copia de seguridad)
- Unidad-2-1 (propietario)

- Unidad-3-1 (reenviador)

<#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

## Troubleshoot

### Introducción a Troubleshooting de Cluster

Los problemas de clúster se pueden clasificar en:

- Problemas del plano de control (problemas relacionados con la estabilidad del clúster)
- Problemas del plano de datos (problemas relacionados con el tráfico de tránsito)

### Problemas del plano de datos del clúster

## Problemas comunes de NAT/PAT

### Consideraciones de configuración importantes

- Los agrupamientos de traducción de direcciones de puerto (PAT) deben tener al menos tantas IP disponibles como el número de unidades del agrupamiento, preferiblemente más IP que nodos del agrupamiento.
- Los comandos predeterminados `xlate per-session` se deben dejar en su lugar a menos que haya una razón específica para desactivarlos. Cualquier `xlate PAT` generado para una conexión que tiene `xlate` por sesión inhabilitado siempre es manejado por la unidad de nodo de control en el clúster, lo que puede causar una degradación del rendimiento.

Uso de alto rango de grupos PAT debido al tráfico originado en puertos de baja capacidad que causa desequilibrio de IP de clúster

El FTD divide una IP PAT en rangos e intenta mantener la `xlate` en el mismo rango de origen. Esta tabla muestra cómo un puerto de origen se traduce a un puerto global dentro del mismo rango de origen.

Puerto Src Original	Puerto Src Traducido
1-511	1-511
512-1023	512-1023
1024-65535	1024-65535

Cuando un intervalo de puertos de origen está lleno y es necesario asignar una nueva `xlate PAT` desde ese intervalo, FTD se desplaza a la siguiente IP para asignar nuevas traducciones para ese intervalo de puertos de origen.

### Síntomas

Problemas de conectividad para el tráfico NATed que atraviesa el clúster

### Verificación

```
<#root>
```

```
#
```

```
show nat pool
```

Los registros del plano de datos de FTD muestran el agotamiento del conjunto PAT:

<#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
```

## Mitigación

Configure el rango de puertos planos NAT e incluya los puertos de reserva.

Además, en post-6.7/9.15.1 puede terminar con una distribución de bloques de puertos desequilibrada solamente cuando los nodos salen/se unen al clúster con un enorme tráfico de fondo que está sujeto a PAT. La única forma de recuperarse por sí misma es cuando los bloques de puertos se liberan para ser redistribuidos a través de los nodos.

Con la distribución basada en bloques de puertos, cuando se asigna un nodo con, por ejemplo, 10 bloques de puertos como pb-1, pb-2 ... pb-10. El nodo siempre comienza con el primer bloque de puertos disponible y asigna un puerto aleatorio desde él hasta que se agota. La asignación se traslada al siguiente bloque de puerto solamente cuando se agotan todos los bloques de puerto hasta ese punto.

Por ejemplo, si un host establece 512 conexiones, la unidad asigna puertos asignados aleatoriamente para todas esas 512 conexiones de pb-1. Ahora, con todas estas 512 conexiones activas, cuando el host establece la conexión 513 desde que se agota pb-1, se mueve a pb-2 y le asigna un puerto aleatorio. De nuevo, de 513 conexiones, suponga que la 10ª conexión finalizó y borró un puerto disponible en pb-1. En este punto, si el host establece la 514ª conexión, la unidad de clúster asigna un puerto asignado desde pb-1 y no desde pb-2 porque pb-1 ahora tiene un puerto libre (que se liberó como parte de la eliminación de la 10ª conexión).

La parte importante a tener en cuenta es que la asignación ocurre desde el primer bloque de puerto disponible con puertos libres para que los últimos bloques de puerto estén siempre disponibles para la redistribución en un sistema cargado normalmente. Además, la PAT se utiliza normalmente para conexiones de corta duración. La probabilidad de que un bloque de puertos esté disponible en un tiempo más corto es muy alta. Por lo tanto, el tiempo necesario para equilibrar la distribución de grupos puede mejorar con la distribución de grupos basada en bloques de puertos.

Sin embargo, en caso de que se agoten todos los bloques de puerto, desde pb-1 hasta pb-10, o de que cada bloque de puerto contenga un puerto para una conexión de larga duración, los bloques de puerto nunca se liberan rápidamente y se redistribuyen. En tal caso, el enfoque menos

perjudicial es el siguiente:

1. Identifique los nodos con bloques de puertos excesivos (show nat pool cluster summary).
2. Identifique los bloques de puerto menos utilizados en ese nodo (show nat pool ip <addr> detail).
3. Borre las xlates para dichos bloques de puertos (clear xlate global <addr> gport 'start-end') para que estén disponibles para su redistribución.



Advertencia: Esto interrumpe las conexiones relevantes.

---

No se puede navegar a sitios web de doble canal (como Webmail, banca, etc.) o a sitios web de SSO cuando se produce la redirección a un destino diferente.

### Síntomas

No se puede navegar a sitios web de canal dual (como el correo web, sitios web bancarios, etc.). Cuando un usuario se conecta a un sitio web que requiere que el cliente abra un segundo socket/conexión y la segunda conexión se trocea con un miembro del clúster diferente del que obtuvo la primera conexión con troceo, y el tráfico utiliza un conjunto PAT IP, el tráfico es restablecido por el servidor cuando recibe la conexión desde una dirección IP pública diferente.

### Verificación

Realice capturas de clúster de plano de datos para ver cómo se gestiona el flujo de tránsito afectado. En este caso, un reinicio de TCP proviene del sitio web de destino.

### Mitigación (anterior a 6.7/9.15.1)

- Observe si alguna aplicación multisesión utiliza varias direcciones IP asignadas.
- Utilice el comando show nat pool cluster summary para verificar si el conjunto se distribuye uniformemente.
- Utilice el comando cluster exec show conn para verificar si el tráfico está balanceado correctamente.
- Utilice el comando show nat pool cluster ip <address> detail para verificar el uso del conjunto de IP fija.
- Habilite syslog 305021 (6.7/9.15) para ver qué conexiones no han podido utilizar IP fija.
- Para resolver, agregue más IP al conjunto PAT o ajuste el algoritmo de equilibrio de carga en los switches conectados.

### Acerca del algoritmo de balanceo de carga de canal éter:

- Para los dispositivos que no sean FP9300 y si la autenticación se produce a través de un servidor: Ajuste el algoritmo de balanceo de carga de canal Ethernet en el switch adyacente de IP/puerto de origen e IP/puerto de destino a IP de origen e IP de destino.
- Para servidores que no sean FP9300 y si la autenticación se produce a través de varios servidores: Ajuste el algoritmo de balanceo de carga de canal Ethernet en el switch adyacente de IP/puerto de origen e IP/puerto de destino a IP de origen.
- Para FP9300: En el chasis FP9300, el algoritmo de balanceo de carga se fija como source-

dest-port source-dest-ip source-dest-mac y no se puede cambiar. La solución alternativa, en este caso, es utilizar FlexConfig para agregar comandos xlate per-session deny a la configuración de FTD para forzar que el tráfico para ciertas direcciones IP de destino (para las aplicaciones problemáticas o incompatibles) sea manejado solamente por el nodo de control en el clúster dentro del chasis. La solución alternativa viene con estos efectos secundarios:

- Sin equilibrio de carga del tráfico traducido de forma diferente (todo va al nodo de control).
- Posibilidad de que las ranuras xlate se agoten (y afecten negativamente a la traducción NAT para otro tráfico en el nodo de control).
- Escalabilidad reducida del clúster dentro del chasis.

Bajo rendimiento del clúster debido a todo el tráfico enviado al nodo de control debido a que no hay suficientes IP PAT en los grupos.

### Síntomas

No hay suficientes IP PAT en el clúster para asignar una IP libre a los nodos de datos y, por lo tanto, todo el tráfico sujeto a la configuración PAT se reenvía al nodo de control para su procesamiento.

### Verificación

Utilice el comando `show nat pool cluster` para ver las asignaciones para cada unidad y confirmar que todos poseen al menos una IP en el conjunto.

### Mitigación

Para pre-6.7/9.15.1 asegúrese de tener un conjunto PAT de tamaño al menos igual al número de nodos en el clúster. En post-6.7/9.15.1 con el conjunto PAT, se asignan bloques de puertos de todas las IP del conjunto PAT. Si el uso del conjunto PAT es realmente alto, lo que provoca un agotamiento frecuente del conjunto, debe aumentar el tamaño del conjunto PAT (consulte la sección de preguntas frecuentes).

Bajo rendimiento debido a todo el tráfico enviado al nodo de control porque las xlates no están habilitadas por sesión.

### Síntomas

Muchos flujos de respaldo UDP de alta velocidad se procesan a través del nodo de control del clúster, lo que puede afectar el rendimiento.

### Background

Un nodo de datos que utiliza PAT sólo puede procesar las conexiones que utilizan xlates habilitados por sesión. Utilice el comando `show run all xlate` para ver la configuración xlate por sesión.

Por sesión habilitada significa que la xlate se desactiva inmediatamente cuando se desactiva la

conexión asociada. Esto ayuda a mejorar el rendimiento de la conexión por segundo cuando las conexiones están sujetas a PAT. Las xlates que no son por sesión permanecen activas durante otros 30 segundos después de que se interrumpa la conexión asociada y, si la velocidad de conexión es lo suficientemente alta, los 65 000 puertos TCP/UDP disponibles en cada IP global se pueden utilizar en un breve período de tiempo.

De forma predeterminada, todo el tráfico TCP se habilita por xlate y sólo el tráfico DNS UDP se habilita por sesión. Esto significa que todo el tráfico UDP no DNS se reenvía al nodo de control para su procesamiento.

## Verificación

Utilice este comando para verificar la conexión y la distribución de paquetes entre las unidades del clúster:

```
<#root>
```

```
firepower#
```

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

```
firepower#
```

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

```
firepower#
```

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

Utilice el comando `cluster exec show conn` para ver qué nodos del clúster poseen las conexiones UDP.

```
<#root>
```

```
firepower#
```

```
cluster exec show conn
```

Utilice este comando para comprender el uso del conjunto en los nodos del clúster.

```
<#root>
```

```
firepower#
```

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



| in UDP

## Mitigación

Configure PAT por sesión (comando `per-session permit udp`) para el tráfico de interés (por ejemplo, UDP). Para el ICMP, no puede cambiar de la PAT multisesión predeterminada, por lo tanto, el tráfico ICMP es manejado siempre por el nodo de control cuando hay PAT configurado.

La distribución del conjunto PAT se desequilibra a medida que los nodos abandonan el clúster o se unen a él.

## Síntomas

- Los problemas de conectividad desde la asignación de IP PAT pueden desequilibrar con el tiempo debido a las unidades que salen y se unen al clúster.
- En post-6.7/9.15.1, puede haber casos en los que el nodo recién unido no pueda obtener suficientes bloques de puerto. Un nodo que no tiene ningún bloque de puerto redirige el tráfico al nodo de control. Un nodo que tiene al menos un bloque de puerto maneja el tráfico y lo descarta una vez que se agota el conjunto.

## Verificación

- Los syslogs del plano de datos muestran mensajes como:

```
<#root>
```

```
%ASA-3-202010:
```

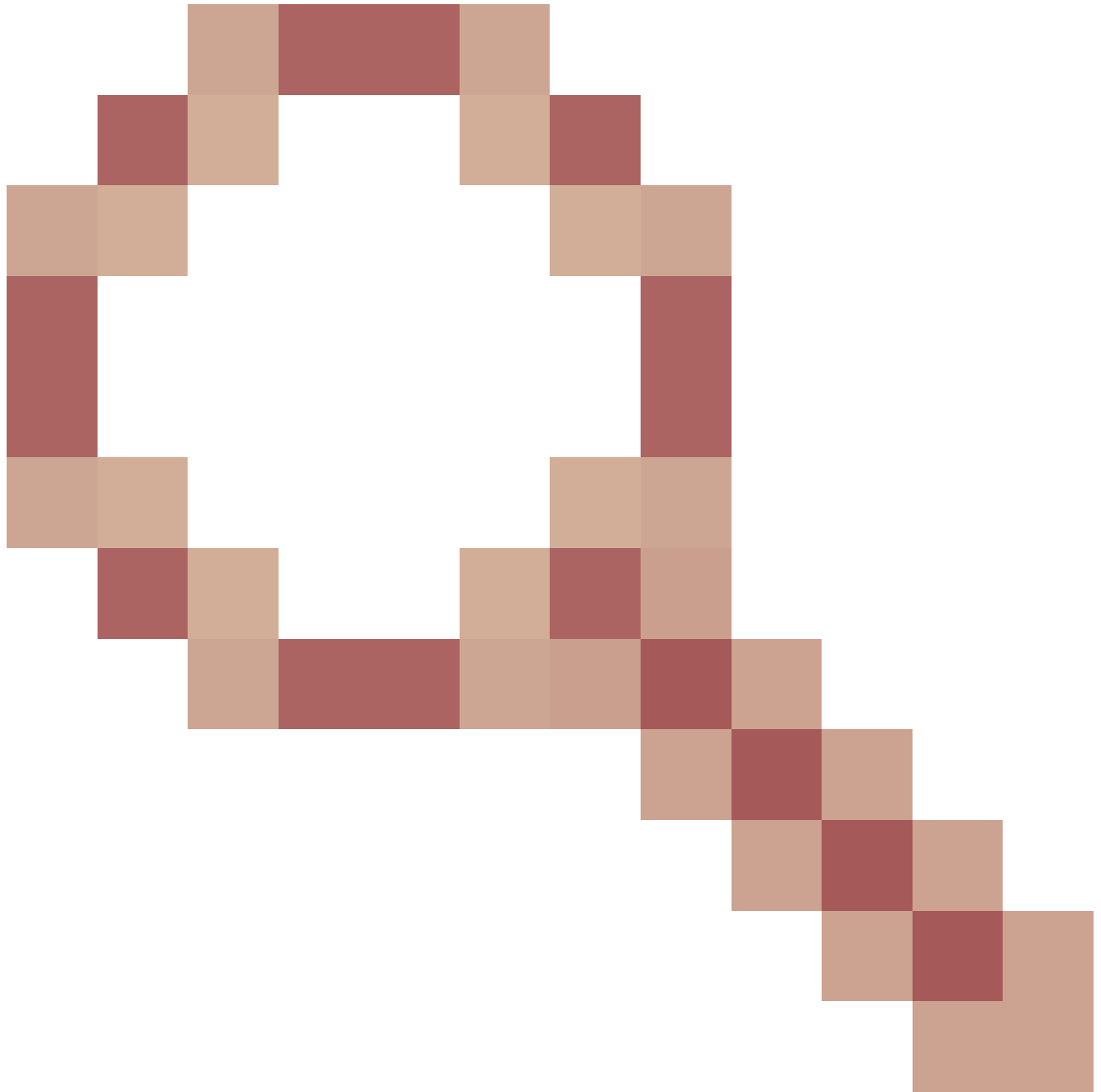
```
NAT pool exhausted. Unable to create TCP connection
```

```
from inside:192.0.2.1/2239 to outside:192.0.2.150/80
```

- Utilice el comando `show nat pool cluster summary` para identificar la distribución del grupo.
- Utilice el comando `cluster exec show nat pool ip <addr>detail` para comprender el uso del conjunto en los nodos del clúster.

## Mitigación

- Para pre-6.7/9.15.1, se describen algunas soluciones alternativas en Cisco bug ID [CSCvd10530](#)



- En post-6.7/9.15.1, utilice el comando `clear xlate global <ip> gport <start-end>` para borrar manualmente algunos de los bloques de puerto en otros nodos para la redistribución a los nodos requeridos.

## Síntomas

Problemas de conectividad importantes para el tráfico que es PATed por el clúster. Esto se debe a que el plano de datos FTD, por diseño, no envía GARP para direcciones NAT globales.

## Verificación

La tabla ARP de los dispositivos conectados directamente muestra diferentes direcciones MAC de la interfaz de datos del clúster después de un cambio del nodo de control:

<#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
```

## Mitigación

Configure MAC estático (virtual) en las interfaces de datos del clúster.

Conexiones sometidas a fallo de PAT

## Síntomas

Problemas de conectividad para el tráfico que es PATed por el clúster.

## Verificación/Mitigación

- Asegúrese de que la configuración se replica correctamente.
- Asegúrese de que el conjunto se distribuye de manera uniforme.
- Asegúrese de que la propiedad del conjunto sea válida.
- No se incrementa ningún contador de errores en `show asp cluster counter`.
- Asegúrese de que los flujos de director/reenviador se crean con la información adecuada.
- Valide si las xlates de copia de seguridad se crean, actualizan y limpian según lo esperado.
- Valide si las xlates se crean y terminan según el comportamiento "por sesión".
- Habilite "debug nat 2" para una indicación de cualquier error. Tenga en cuenta que esta salida puede ser muy ruidosa, por ejemplo:

```
<#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
```

Para detener la depuración:

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

- Habilite los syslogs relacionados con la conexión y NAT para correlacionar la información con una conexión fallida.

Mejoras de PAT de agrupación de ASA y FTD (posteriores a las versiones 9.15 y 6.7)

¿Qué cambió?

Se ha rediseñado la operación PAT. Las IP individuales ya no se distribuyen a cada uno de los miembros del clúster. En su lugar, las IP de PAT se dividen en bloques de puertos y se distribuyen esos bloques de puertos de manera uniforme (en la medida de lo posible) entre los miembros del clúster, en combinación con el funcionamiento de conservación de IP.

El nuevo diseño aborda estas limitaciones (consulte la sección anterior):

- Las aplicaciones multisesión se ven afectadas por la falta de conservación de IP en todo el clúster.
- El requisito es tener un conjunto PAT de tamaño al menos igual al número de nodos del clúster.
- La distribución del conjunto PAT se desequilibra a medida que los nodos abandonan el clúster o se unen a él.
- No hay registros del sistema para indicar el desequilibrio del conjunto PAT.

Técnicamente, en lugar de los intervalos de puertos predeterminados 1-511, 512-1023 y 1024-65535, ahora hay 1024-65535 como intervalo de puertos predeterminado para PAT. Este intervalo predeterminado se puede ampliar para incluir el intervalo de puertos privilegiados 1-1023 para PAT normal (opción "incluir reserva").

Este es un ejemplo de una configuración de conjunto PAT en FTD 6.7. Para obtener más detalles, consulte la sección relacionada en la Guía de configuración:

**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	
Original Source Port:	Translated Source Port:
Original Destination Port:	Translated Destination Port:

Interface Objects Translation PAT Pool Advanced

Enable PAT Pool

**PAT:**  
Address ip\_192.168.241.57-59

Use Round Robin Allocation

Extended PAT Table

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

Include Reserve Ports

Block Allocation

Información adicional sobre resolución de problemas de PAT

Registros del sistema del plano de datos de FTD (posteriores a 6.7/9.15.1)

Se genera un syslog de invalidación de adhesividad cuando se agotan todos los puertos en la IP

fija de un nodo de clúster y la asignación se traslada a la siguiente IP disponible con puertos libres, por ejemplo:

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

Un syslog de desequilibrio de agrupamiento se genera en un nodo cuando se une al agrupamiento y no obtiene ninguna o desigual porción de bloques de puerto, por ejemplo:

```
%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
```

## Comandos show

### Estado de distribución del grupo

En el resultado del resumen del clúster de `show nat pool`, para cada dirección IP de PAT, no debe haber una diferencia de más de 1 bloque de puertos a través de los nodos en un escenario de distribución balanceada. Ejemplos de una distribución de bloques de puertos equilibrada y desequilibrada.

```
<#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)
```

### Distribución desequilibrada:

```
<#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 /
```

## Estado de propiedad del grupo

En el resultado de `show nat pool cluster`, no debe haber un solo bloque de puerto con propietario o respaldo como DESCONOCIDO. Si hay uno, indica un problema con la comunicación de propiedad del conjunto. Ejemplo:

```
<#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>
```

## Contabilidad de las asignaciones de puertos en los bloques de puertos

El comando `show nat pool` se mejora con opciones adicionales para mostrar información detallada así como resultados filtrados. Ejemplo:

```
<#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 *
```

"" indica que se trata de un bloque de puertos de reserva

Para resolver esto, utilice el comando `clear xlate global <ip> gport <start-end>` para borrar manualmente algunos de los bloques de puerto en otros nodos para la redistribución a los nodos requeridos.

Redistribución de bloques de puertos activada manualmente

- En una red de producción con tráfico constante, cuando un nodo sale del clúster y vuelve a unirse a él (probablemente debido a un seguimiento), puede haber casos en los que no pueda obtener una cuota igual del conjunto o, en el peor de los casos, no pueda obtener ningún bloque de puerto.
- Utilice el comando `show nat pool cluster summary` para identificar qué nodo posee más bloques de puertos de los requeridos.
- En los nodos que poseen más bloques de puerto, utilice el comando `show nat pool ip <addr>detail` para calcular los bloques de puerto con el menor número de asignaciones.
- Utilice el comando `clear xlate global <address> gport <start-end>` para borrar las traducciones creadas a partir de esos bloques de puerto de modo que estén disponibles para la redistribución a los nodos requeridos, por ejemplo:

```
<#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
```

Preguntas más frecuentes (FAQ) sobre PAT posterior a 6.7/9.15.1

P. En caso de que tenga el número de IP disponibles para el número de unidades disponibles en el clúster, ¿puede utilizar 1 IP por unidad como opción?

R. Ya no, y no hay alternancia para cambiar entre esquemas de distribución de agrupamiento



basados en direcciones IP versus esquemas de distribución de agrupamiento basados en bloques de puertos.

El esquema más antiguo de distribución de grupos basada en direcciones IP dio lugar a errores de aplicaciones de sesiones múltiples en las que varias conexiones (que forman parte de una transacción de aplicación única) de un host se equilibran con la carga en diferentes nodos del clúster y, por tanto, se traducen mediante diferentes direcciones IP asignadas, lo que lleva al servidor de destino a verlas como originadas en diferentes entidades.

Además, con el nuevo esquema de distribución basado en bloques de puertos, aunque ahora puede trabajar con tan solo una dirección IP PAT, siempre se recomienda tener suficientes direcciones IP PAT en función del número de conexiones que se requieren para PATed.

P. ¿Aún puede tener un conjunto de direcciones IP para el conjunto PAT para el clúster?

R: Sí, puede. Los bloques de puertos de todas las IP del grupo PAT se distribuyen a través de los nodos del clúster.

P. Si utiliza un número de direcciones IP para el conjunto PAT, ¿se asigna el mismo bloque de puertos a cada miembro por cada dirección IP?

R. No, cada IP se distribuye de forma independiente.

P. ¿Todos los nodos del clúster tienen todas las IP públicas, pero solo un subconjunto de puertos? Si este es el caso, ¿se garantiza entonces que cada vez que la IP de origen utilice la misma IP pública?

R. Es correcto, cada IP PAT es propiedad parcial de cada nodo. Si se agota una IP pública elegida en un nodo, se genera un syslog que indica que la IP fija no se puede conservar y la asignación se desplaza a la siguiente IP pública disponible. Ya se trate de una implementación independiente, de alta disponibilidad o de clúster, la conservación de IP siempre se realiza con el máximo esfuerzo, en función de la disponibilidad del grupo.

P. ¿Todo se basa en una sola dirección IP en el conjunto PAT, pero no se aplica si se utiliza más de una dirección IP en el conjunto PAT?

R. También se aplica a múltiples direcciones IP en el conjunto PAT. Los bloques de puertos de cada IP del conjunto PAT se distribuyen a través de los nodos del clúster. Cada dirección IP del grupo PAT se divide en todos los miembros del clúster. Por lo tanto, si tiene una clase C de direcciones en el agrupamiento PAT, cada miembro del agrupamiento tiene agrupamientos de puertos de cada una de las direcciones del agrupamiento PAT.

P. ¿Funciona con CGNAT?

R. Sí, CGNAT también es compatible. CGNAT, también conocido como PAT de asignación de bloques tiene un tamaño de bloque predeterminado de '512' que se puede modificar a través de la CLI de tamaño de asignación de bloques de xlate. En el caso de PAT dinámica regular (no CGNAT), el tamaño del bloque es siempre '512', que es fijo y no configurable.

P. Si la unidad abandona el clúster, ¿el nodo de control asigna el rango de bloques de puertos a otras unidades o lo guarda para sí mismo?

R. Cada bloque de puertos tiene un propietario y una copia de seguridad. Cada vez que se crea una xlate a partir de un bloque de puerto, también se replica en el nodo de respaldo del bloque de puerto. Cuando un nodo abandona el clúster, el nodo de copia de seguridad posee todos los bloques de puertos y todas las conexiones actuales. El nodo de respaldo, ya que se ha convertido en el propietario de estos bloques de puerto adicionales, elige una nueva copia de respaldo para ellos y replica todas las xlates actuales a ese nodo para manejar escenarios de falla.

P. ¿Qué medidas se pueden tomar sobre la base de esa alerta para hacer cumplir la conservación?

R. Hay dos posibles razones por las que no se puede preservar la adherencia.

Motivo 1: El tráfico está equilibrado de carga incorrectamente debido a que uno de los nodos ve un mayor número de conexiones que otros, lo que lleva al agotamiento de IP persistente en particular. Esto se puede solucionar si se asegura de que el tráfico se distribuya uniformemente a través de los nodos del clúster. Por ejemplo, en un clúster FPR41xx, ajuste el algoritmo de equilibrio de carga en los switches conectados. En un clúster FPR9300, asegúrese de que haya el mismo número de servidores blade en el chasis.

Motivo 2: El uso del conjunto PAT es realmente alto, lo que provoca un agotamiento frecuente del conjunto. Para hacer frente a este problema, aumente el tamaño del conjunto PAT.

P. ¿Cómo se maneja el soporte para la palabra clave extendida? ¿Muestra un error e impide que se agregue el comando NAT completo durante la actualización o elimina la palabra clave extended y muestra una advertencia?

R. La opción ampliada PAT no se admite en el clúster desde ASA 9.15.1/FP 6.7 en adelante. La opción de configuración no se elimina de ninguna de las CLI/ASDM/CSM/FMC. Cuando se configura (directa o indirectamente a través de una actualización), se le notifica con un mensaje de advertencia y se acepta la configuración, pero no se ve la funcionalidad ampliada de PAT en acción.

P. ¿Es el mismo número de traducciones que las conexiones simultáneas?

R. En pre-6.7/9.15.1, aunque era 1-65535, como los puertos de origen nunca se utilizan mucho en el rango 1-1024, lo convierte efectivamente en 1024-65535 (64512 conns). En la implementación posterior a 6.7/9.15.1 con 'flat' como comportamiento predeterminado, es 1024-65535. Pero si desea utilizar el 1-1024, puede hacerlo con la opción "include-reserve".

P. Si el nodo se une de nuevo al clúster, ¿tiene el nodo de copia de seguridad antiguo como copia de seguridad y ese nodo de copia de seguridad le da su bloque de puerto antiguo?

R. Depende de la disponibilidad de los bloques de puertos en ese momento. Cuando un nodo abandona el clúster, todos sus bloques de puertos se mueven al nodo de copia de seguridad. Es entonces el nodo de control que acumula los bloques de puerto libre y los distribuye a los nodos requeridos.

P. Si se produce un cambio en el estado del nodo de control, se selecciona un nuevo nodo de control, ¿se mantiene la asignación de bloques PAT o se reasignan los bloques de puerto en función del nuevo nodo de control?

R. El nuevo nodo de control tiene un entendimiento de qué bloques han sido asignados y cuáles son libres y comienza desde allí.

P. ¿Es el número máximo de xlates el mismo que el número máximo de conexiones simultáneas con este nuevo comportamiento?

R. Sí. El número máximo de xlates depende de la disponibilidad de los puertos PAT. No tiene nada que ver con el número máximo de conexiones simultáneas. Si sólo permite 1 dirección, tiene 65535 conexiones posibles. Si necesita más, debe asignar más direcciones IP. Si hay suficientes direcciones/puertos, puede alcanzar el número máximo de conexiones simultáneas.

P. ¿Cuál es el proceso de asignación del bloque de puerto cuando se agrega un nuevo miembro del agrupamiento? ¿Qué sucede si se agrega un miembro del clúster debido al reinicio?

R. Los bloques de puerto siempre son distribuidos por el nodo de control. Los bloques de puerto se asignan a un nuevo nodo sólo cuando hay bloques de puerto libres. Los bloques de puertos libres significan que no se sirve ninguna conexión a través de ningún puerto asignado dentro del bloque de puertos.

Además, al volver a unirse, cada nodo vuelve a calcular el número de bloques que puede poseer. Si un nodo contiene más bloques de lo que se supone que debe, libera dichos bloques de puerto adicionales al nodo de control cuando estén disponibles. A continuación, el nodo de control los asigna al nodo de datos recién unido.

P. ¿Se soporta solamente los protocolos TCP y UDP o SCTP también?

R. SCTP nunca fue compatible con PAT dinámico. Para el tráfico SCTP, se recomienda utilizar solamente un objeto de red estático NAT.

P. Si un nodo se queda sin puertos de bloque, ¿descarta paquetes y no utiliza el siguiente bloque IP disponible?

R: No, no se cae inmediatamente. Utiliza los bloques de puertos disponibles de la siguiente IP PAT. Si se agotan todos los bloques de puertos a través de todas las IP PAT, entonces descarta el tráfico.

P. Para evitar la sobrecarga del nodo de control en una ventana de actualización de clúster, ¿es mejor seleccionar un nuevo control manualmente antes (por ejemplo, a mitad de camino de una actualización de clúster de 4 unidades), en lugar de esperar a que se controlen todas las conexiones en el nodo de control?

R. El control debe actualizarse en último lugar. Esto se debe a que, cuando el nodo de control ejecuta la versión más reciente, no inicia la distribución de grupos a menos que todos los nodos ejecuten la versión más reciente. Además, cuando se ejecuta una actualización, todos los nodos de datos con una versión más reciente omiten los mensajes de distribución de grupos de un nodo

de control si ejecuta una versión anterior.

Para explicar esto en detalle, considere una implementación de clúster con 4 nodos A, B, C y D con A como control. A continuación se indican los pasos de actualización habituales sin impacto:

1. Descargue una nueva versión en cada uno de los nodos.
2. Vuelva a cargar la unidad "D". Todas las conexiones, xlates se mueven al nodo de copia de seguridad.
3. Aparece la unidad "D" y:
  - a. Procesa la configuración de PAT
  - b. Divide cada IP PAT en bloques de puertos
  - c. Tiene todos los bloques de puerto en estado no asignado
  - d. Omite la versión anterior de los mensajes PAT del clúster recibidos del control
  - e. Redirige todas las conexiones PAT a Primario.
4. Del mismo modo, traer a otros nodos con la nueva versión.
5. Vuelva a cargar el mando de la unidad "A". Dado que no hay respaldo para el control, se descartan todas las conexiones existentes
6. El nuevo control inicia la distribución de bloques de puertos en el formato más nuevo
7. La unidad "A" vuelve a unirse y es capaz de aceptar y actuar en los mensajes de distribución de bloque de puerto

## Manejo de fragmentos

### Síntoma

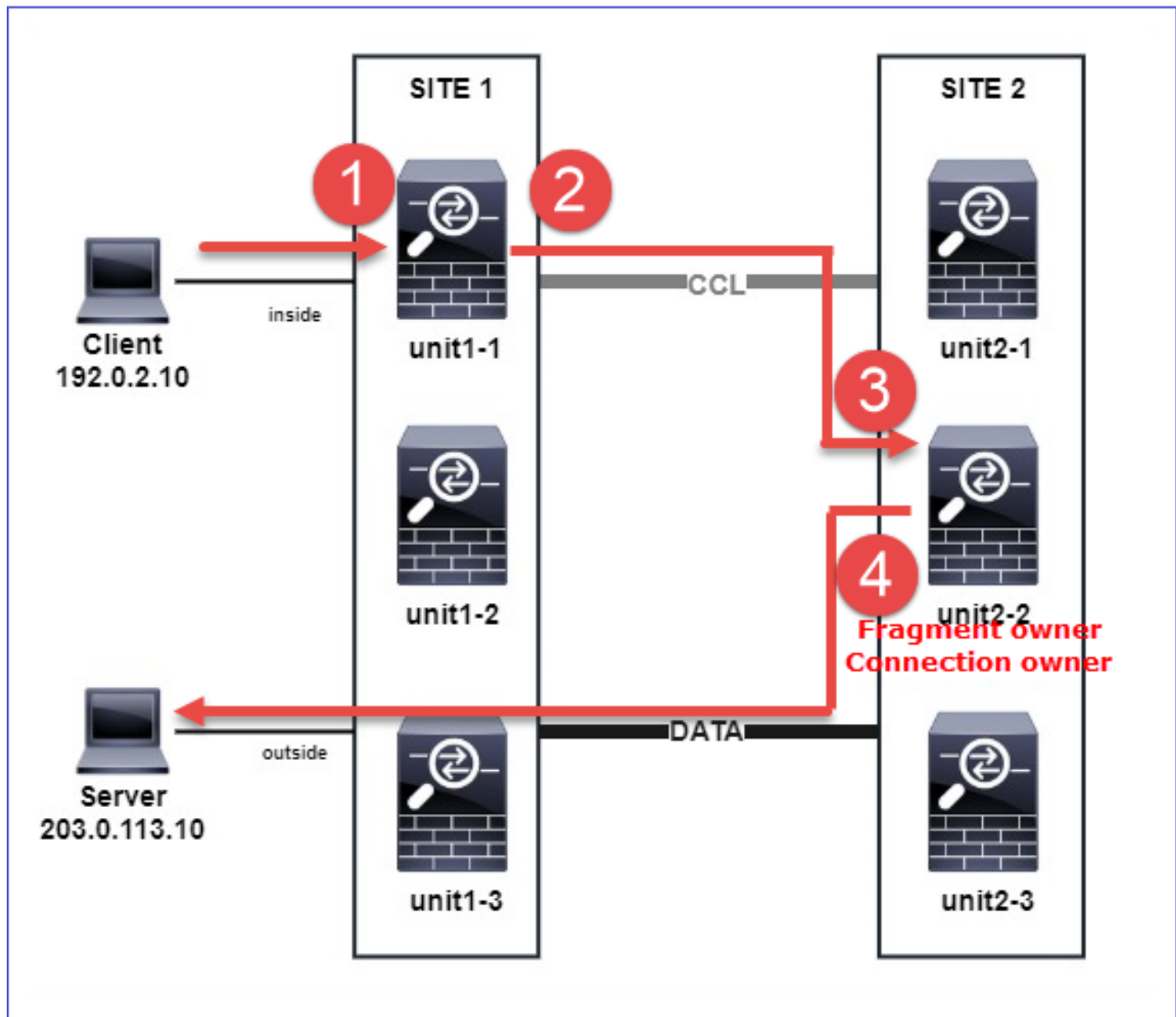
En las implementaciones de clúster entre sitios, los paquetes fragmentados que deben gestionarse en un sitio específico (tráfico local del sitio) se pueden enviar a las unidades de otros sitios, ya que uno de estos sitios puede tener el propietario del fragmento.

En la lógica de clúster, hay una función adicional definida para las conexiones con paquetes fragmentados: propietario del fragmento.

En el caso de los paquetes fragmentados, las unidades de clúster que reciben un fragmento determinan el propietario del fragmento basándose en un hash de la dirección IP de origen del fragmento, la dirección IP de destino y el ID del paquete. A continuación, todos los fragmentos se reenvían al propietario del fragmento a través del vínculo de control de clúster. Los fragmentos se pueden balancear en función de la carga en diferentes unidades de clúster porque sólo el primer fragmento incluye la 5 tupla utilizada en el hash de balanceo de carga del switch. Otros fragmentos no contienen los puertos de origen y destino y se pueden equilibrar la carga en otras unidades de clúster. El propietario del fragmento reensambla temporalmente el paquete para que pueda determinar el director basándose en un hash de la dirección IP de origen/destino y los

puertos. Si se trata de una nueva conexión, el propietario del fragmento se convierte en el propietario de la conexión. Si se trata de una conexión existente, el propietario del fragmento reenvía todos los fragmentos al propietario de la conexión a través del vínculo de control de clúster. El propietario de la conexión reensambla todos los fragmentos.

Considere esta topología con el flujo de una solicitud de eco ICMP fragmentada del cliente al servidor:



Para comprender el orden de las operaciones, hay capturas de paquetes en todo el clúster en las interfaces de link de control de agrupamiento, internas y externas configuradas con la opción de rastreo. Además, en la interfaz interna se configura una captura de paquetes con la opción reinyectar y ocultar.

```
<#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
```

Orden de las operaciones dentro del clúster:

1. unit-1-1 en el sitio 1 recibe los paquetes fragmentados de solicitud de eco ICMP.

```
<#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 selecciona la unidad-2-2 en el sitio 2 como propietario del fragmento y le envía paquetes fragmentados.

La dirección MAC de destino de los paquetes enviados desde la unidad-1-1 a la unidad-2-2 es la dirección MAC del link CCL en la unidad-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 capcc1 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 recibe, reensambla los paquetes fragmentados y se convierte en el propietario del flujo.

<#root>

firepower#

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

11 packets captured

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

Phase: 1

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'inside'

Flow type: NO FLOW

I (2) received a FWD\_FRAG\_TO\_FRAG\_OWNER from (0).

Phase: 2

Type: CLUSTER-EVENT

Subtype:

Result: ALLOW

Config:

Additional Information:

Input interface: 'inside'

Flow type: NO FLOW

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

Phase: 3

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 4

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list



Phase: 5  
Type: ROUTE-LOOKUP  
Subtype: No ECMP load balancing  
Result: ALLOW  
Config:  
Additional Information:  
Destination is locally connected. No ECMP load balancing.  
Found next-hop 203.0.113.10 using egress ifc outside(vrfid:0)

Phase: 6  
Type: CLUSTER-EVENT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Input interface: 'inside'

Flow type: NO FLOW

I (2) am becoming owner

Phase: 7  
Type: ACCESS-LIST  
Subtype: log  
Result: ALLOW  
Config:  
access-group CSM\_FW\_ACL\_ global  
access-list CSM\_FW\_ACL\_ advanced trust ip any any rule-id 268435460 event-log flow-end  
access-list CSM\_FW\_ACL\_ remark rule-id 268435460: PREFILTER POLICY: igasimov\_prefilter1  
access-list CSM\_FW\_ACL\_ remark rule-id 268435460: RULE: r1  
Additional Information:

...

Phase: 19  
Type: FLOW-CREATION  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
New flow created with id 1719, packet dispatched to next module

...

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

Action: allow

1 packet shown  
firepower#

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

11 packets captured

2: 20:13:58.231875  
Phase: 1  
Type: CLUSTER-EVENT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Input interface: 'inside'

Flow type: NO FLOW

I (2) received a FWD\_FRAG\_TO\_FRAG\_OWNER from (0).

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

1 packet shown

4. unit-2-2 permite los paquetes basados en la política de seguridad y los envía, a través de la interfaz externa, desde el sitio 2 al sitio 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

## Observaciones/Advertencias

- A diferencia del rol de director, el propietario del fragmento no se puede localizar dentro de un sitio determinado. El propietario del fragmento viene determinado por la unidad que recibe originalmente los paquetes fragmentados de una nueva conexión y se puede ubicar en cualquier sitio.
- Dado que el propietario de un fragmento también puede convertirse en el propietario de la conexión, para reenviar los paquetes al host de destino, debe poder resolver la interfaz de salida y buscar las direcciones IP y MAC del host de destino o el salto siguiente. Esto presupone que los saltos siguientes también deben tener el alcance al host de destino.
- Para reensamblar los paquetes fragmentados, ASA/FTD mantiene un módulo de reensamblado de fragmentos IP para cada interfaz nombrada. Para mostrar los datos operativos del módulo de reensamblado de fragmentos IP, utilice el comando 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
```

En las implementaciones de clúster, el propietario del fragmento o el propietario de la conexión coloca los paquetes fragmentados en la cola de fragmentos. El tamaño de la cola de fragmentos está limitado por el valor del contador Tamaño (de forma predeterminada 200) que se configura con el comando fragment size <size> <nameif>. Cuando el tamaño de la cola de fragmentos alcanza 2/3 del tamaño, se considera que se ha superado el umbral de la cola de fragmentos y se descartan los fragmentos nuevos que no forman parte de la cadena de fragmentos actual. En este caso, se incrementa el umbral de cola de fragmentos excedido y se genera el mensaje de syslog FTD-3-209006.

```
<#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

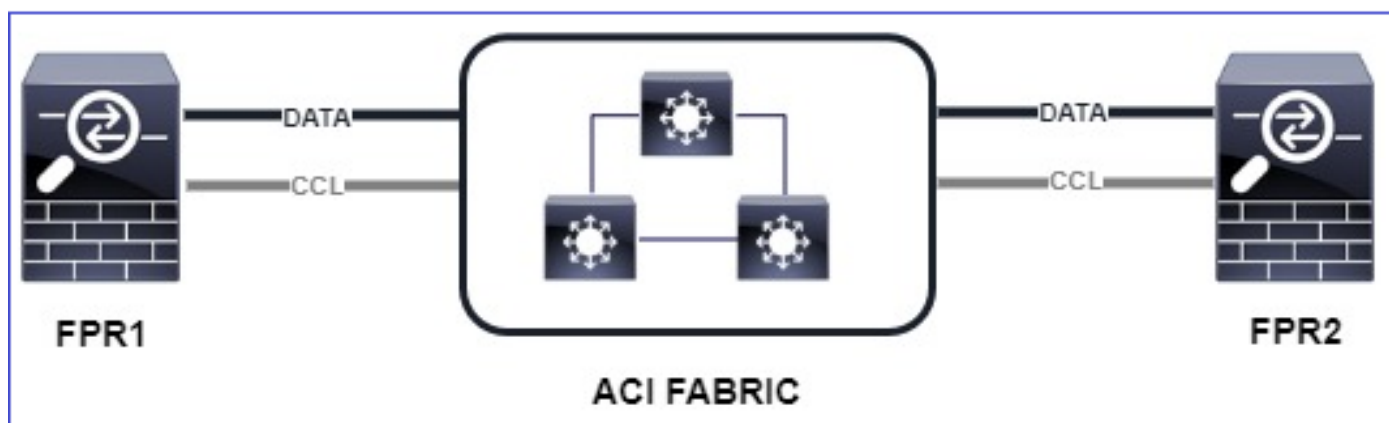
Como solución alternativa, aumente el tamaño en Firepower Management Center > Devices > Device Management > [Edit Device] > Interfaces > [Interface] > Advanced > Security Configuration > Override Default Fragment Setting, guarde la configuración e implemente las políticas. Luego monitoree el contador de cola en el resultado del comando show fragment y la aparición del mensaje de syslog FTD-3-209006.

## Problemas de ACI

Problemas de conectividad intermitente a través del clúster debido a la verificación de suma de comprobación L4 activa en el grupo de dispositivos ACI

### Síntoma

- Problemas de conectividad intermitentes a través del clúster ASA/FTD implementado en un grupo de dispositivos ACI.
- Si sólo hay una unidad en el clúster, no se observan los problemas de conectividad.
- Los paquetes enviados desde una unidad de clúster a una o más unidades del clúster no son visibles en el FXOS ni en las capturas del plano de datos de las unidades de destino.



### Mitigación

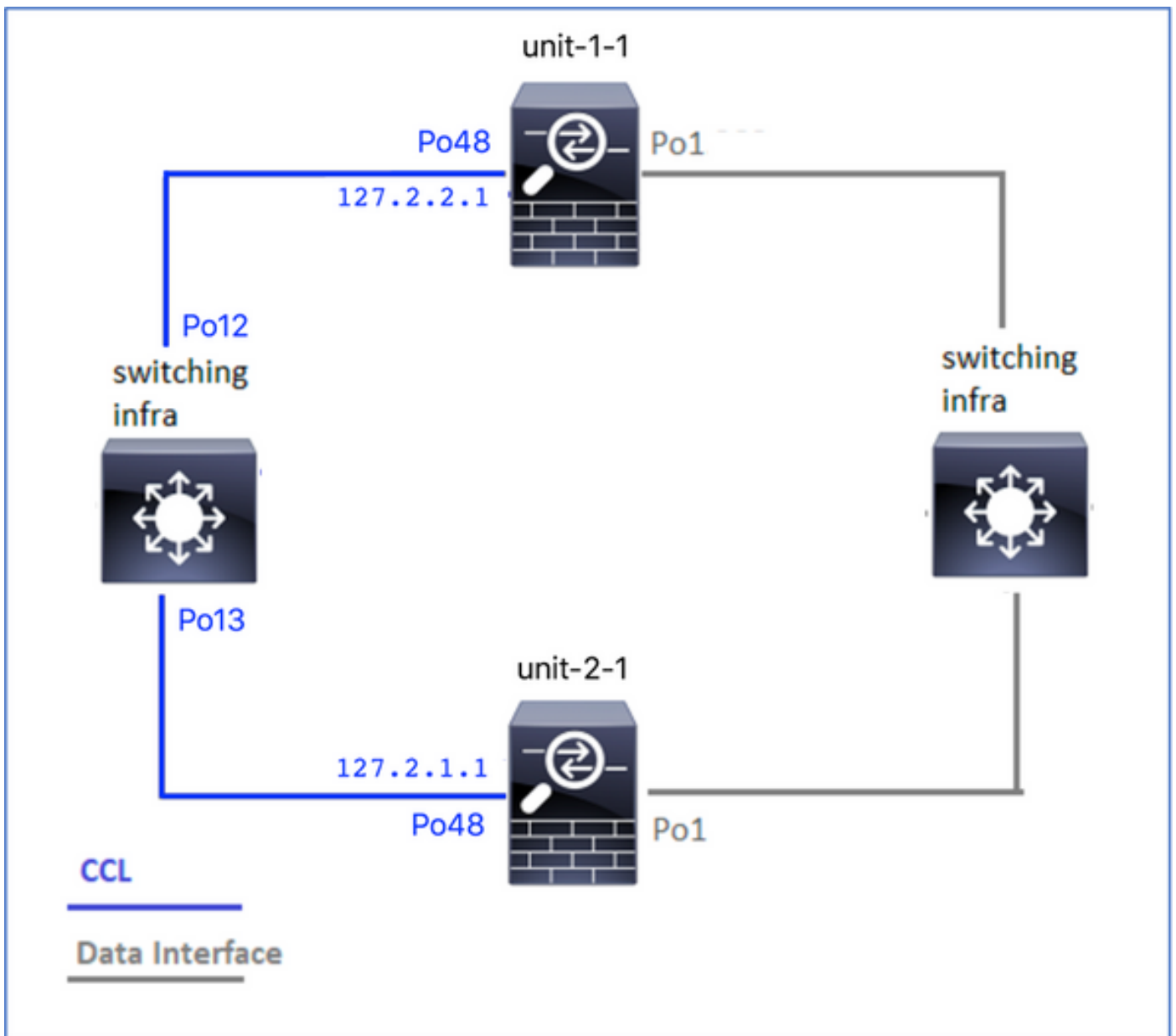
- El tráfico redirigido a través del link de control del clúster no tiene una suma de

comprobación L4 correcta y se espera este comportamiento. Los switches en la trayectoria del link de control del clúster no deben verificar la suma de comprobación L4. Los switches que verifican la suma de comprobación L4 pueden hacer que se descarte el tráfico. Verifique la configuración del switch de fabric ACI y asegúrese de que no se realice ninguna suma de comprobación L4 en los paquetes recibidos o enviados a través del link de control del clúster.

## Problemas del plano de control del clúster

La unidad no puede unirse al clúster

Tamaño de MTU en CCL



Síntomas

La unidad no puede unirse al clúster y se muestra este mensaje:

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

## Verificación/Mitigación

- Utilice el comando show interface en el FTD, para verificar que la MTU en la interfaz de link de control de agrupamiento es por lo menos 100 bytes más alta que la MTU de la interfaz de datos:

```
<#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.
```

- Haga un ping a través de CCL, con la opción size, para verificar si la MTU de CCL está configurada correctamente en todos los dispositivos de la trayectoria.

```
<#root>
```

```
firepower#
```

```
ping 127.2.1.1 size 9184
```

- Utilice el comando `show interface` en el switch para verificar la configuración de MTU

```
<#root>
```

```
Switch#
```

```
show interface
```

```
port-channel12
```

```
is up  
admin state is up,  
Hardware: Port-Channel, address: 7069.5a3a.7976 (bia 7069.5a3a.7976)
```

```
MTU 9084
```

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

```
port-channel13
```

```
is up  
admin state is up,  
Hardware: Port-Channel, address: 7069.5a3a.7967 (bia 7069.5a3a.7967)
```

```
MTU 9084
```

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

## Discordancia de interfaz entre unidades de clúster

### Síntomas

La unidad no puede unirse al clúster y se muestra este mensaje:

```
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
```

### Verificación/Mitigación

Inicie sesión en la GUI de FCM en cada chasis, navegue hasta la pestaña Interfaces y verifique si

todos los miembros del clúster tienen la misma configuración de interfaz:

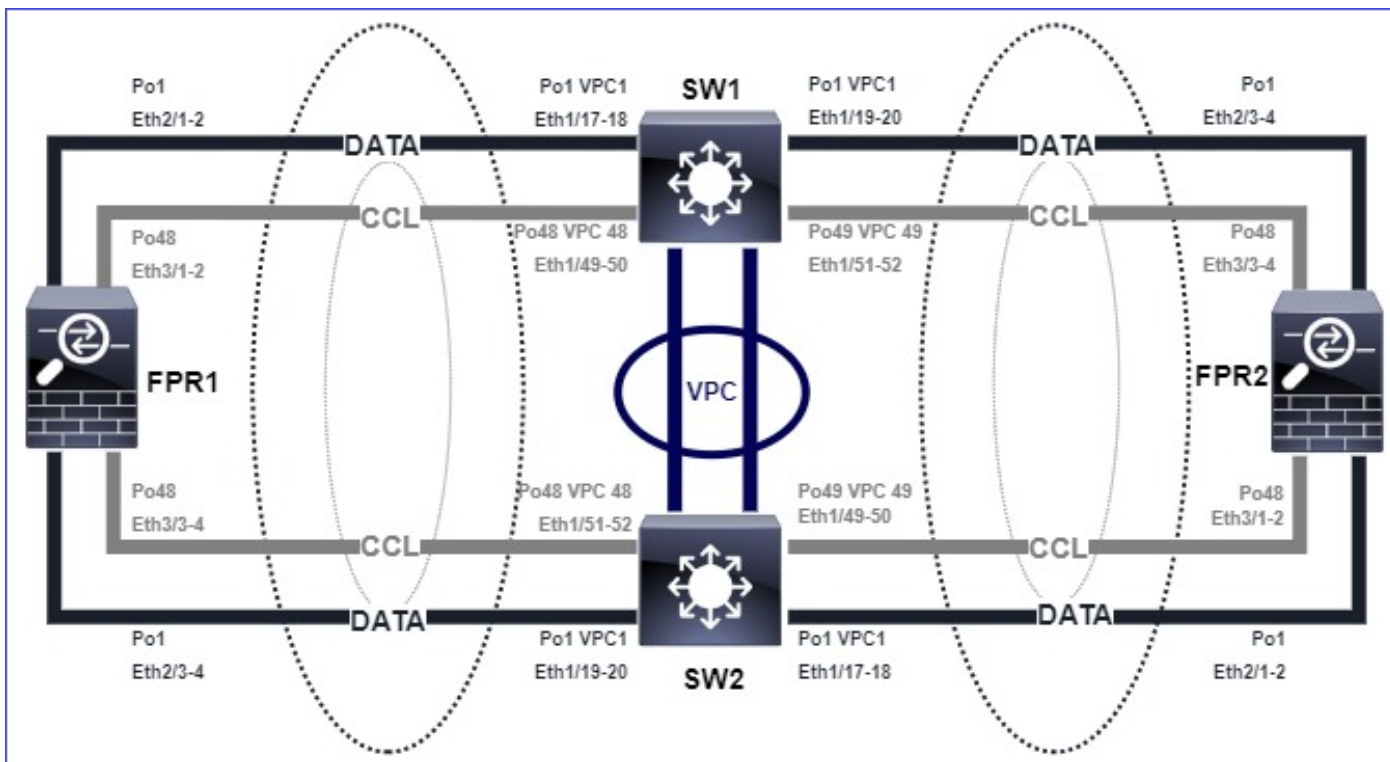
- Interfaces asignadas al dispositivo lógico
- Velocidad de administración de las interfaces
- Dúplex de administración de las interfaces
- Estado de interfaz

Problema de interfaz de datos/canal de puerto

Cerebro partido debido a problemas de accesibilidad en el CCL

Síntoma

Hay varias unidades de control en el clúster. Tenga en cuenta esta topología:



Chasis 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

## Chasis 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

## Verificación

- Utilice el comando ping para verificar la conectividad entre las direcciones IP del link de control de agrupamiento (CCL) de las unidades de control:

<#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)

- Verifique la tabla ARP:

<#root>

```
firepower# show arp
```

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

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

- En las unidades de control, configure y verifique las capturas en las interfaces CCL:

<#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
```

## Mitigación

- Asegúrese de que las interfaces de canal de puerto CCL estén conectadas a interfaces de canal de puerto independientes en el switch.
- Cuando se utilizan canales de puerto virtuales (vPC) en switches Nexus, asegúrese de que las interfaces de canal de puerto CCL están conectadas a vPC diferentes y de que la configuración de vPC no tiene un estado de coherencia fallido.
- Asegúrese de que las interfaces de canal de puerto de CCL estén en el mismo dominio de broadcast y que la VLAN de CCL se cree y se permita en las interfaces.

Este es un ejemplo de configuración del switch:

```
<#root>
```

```
Nexus#
```

```
show run int po48-49
```

```
interface port-channel48  
description FPR1
```

```
switchport access vlan 48
```

```
vpc 48
```

```
interface port-channel49  
description FPR2
```

```
switchport access vlan 48
```

```
vpc 49
```

```
Nexus#
```

```
show vlan id 48
```

```
VLAN Name Status Ports  
-----
```

48 CCL active Po48, Po49, Po100, Eth1/53, Eth1/54

VLAN Type Vlan-mode

-----

48 enet CE

1 Po1 up success success 10,20

48 Po48 up success success 48

49 Po49 up success success 48

<#root>

Nexus1#

show vpc brief

Legend:

(\*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 1

Peer status : peer adjacency formed ok

vPC keep-alive status : peer is alive

Configuration consistency status : success

Per-vlan consistency status : success

Type-2 consistency status : success

vPC role : primary

Number of vPCs configured : 3

Peer Gateway : Disabled

Dual-active excluded VLANs : -

Graceful Consistency Check : Enabled

Auto-recovery status : Disabled

Delay-restore status : Timer is off.(timeout = 30s)

Delay-restore SVI status : Timer is off.(timeout = 10s)

vPC Peer-link status

-----  
id Port Status Active vlans

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

vPC status

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

-----  
1 Po1 up success success 10,20

48 Po48 up success success 48

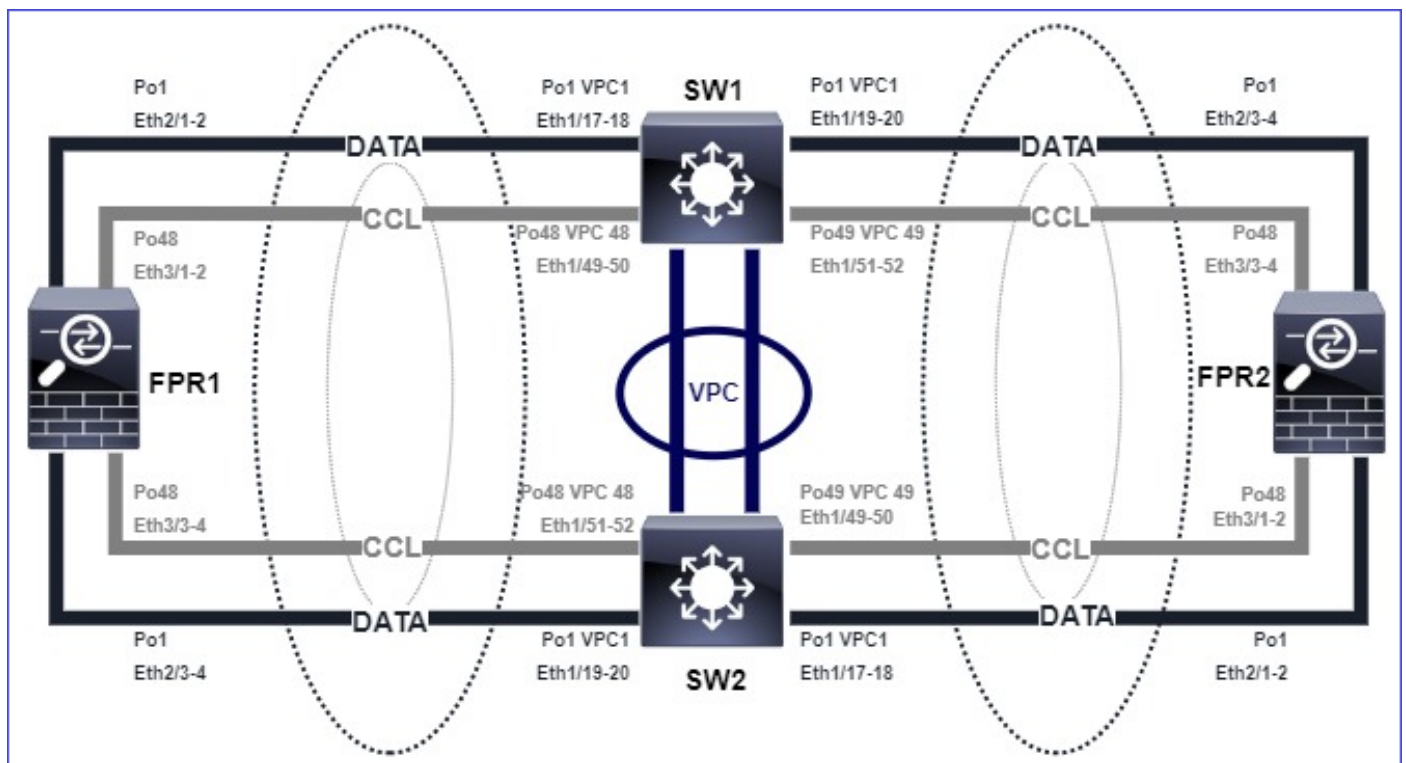
49 Po49 up success success 48

Clúster deshabilitado debido a interfaces de canal de puerto de datos suspendidos

### Síntoma

Una o más interfaces de canal de puerto de datos están suspendidas. Cuando se suspende una interfaz de datos habilitada administrativamente, todas las unidades de clúster del mismo chasis se expulsan del clúster debido a un error en la comprobación de estado de la interfaz.

Tenga en cuenta esta topología:



### Verificación

- Compruebe la consola de la unidad de control:

```
<#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.

- Verifique el resultado de los comandos show cluster history y show cluster info trace module hc en las unidades afectadas:

<#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
```

- Verifique el resultado del comando `show port-channel summary` en el shell de comandos `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)
```

## Mitigación

- Asegúrese de que todos los chasis tengan el mismo nombre de grupo de clúster y la misma contraseña.
- Asegúrese de que las interfaces de canal de puerto tengan administrativamente habilitadas interfaces miembro físicas con la misma configuración dúplex/velocidad en todos los chasis y switches.
- En los clústeres dentro del sitio, asegúrese de que la misma interfaz de canal de puerto de datos de todos los chasis esté conectada a la misma interfaz de canal de puerto del switch.
- Cuando se utilizan canales de puerto virtuales (vPC) en switches Nexus, asegúrese de que la configuración de vPC no tiene un estado de coherencia fallido.
- En los clústeres dentro del sitio, asegúrese de que la misma interfaz de canal de puerto de datos de todos los chasis esté conectada al mismo vPC.

## Problemas de estabilidad del clúster

### Seguimiento de FXOS

#### Síntoma

La unidad sale del clúster.

#### Verificación/Mitigación

- Utilice el comando `show cluster history` para ver cuándo la unidad abandonó el clúster

```
<#root>
```

```
firepower#
```

```
show cluster history
```

- Utilice estos comandos para verificar si el FXOS tenía una señal de seguimiento

```
<#root>
```

```
FPR4150#
```

```
connect local-mgmt
```

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

```
dir cores
```

- Recopile el archivo de núcleo generado alrededor del momento en que la unidad dejó el clúster y proporciónelo al TAC.

## Disco lleno

En caso de que la utilización del disco en la partición `/ngfw` de una unidad de clúster alcance el 94%, la unidad sale del clúster. La comprobación del uso del disco se realiza cada 3 segundos:

```
<#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
```

En este caso, el resultado de show cluster history muestra:

```
<#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
```

or

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

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

Otra forma de verificar la falla es:

```
<#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
```

Además, si el disco es de ~100%, la unidad puede tener dificultades para volver a unirse al clúster hasta que se libere espacio en disco.

## Protección contra desbordamientos

Cada 5 minutos, cada unidad de clúster comprueba la utilización de la CPU y la memoria local y de la unidad par. Si la utilización es superior a los umbrales del sistema (LINA CPU 50% o LINA memory 59%), se muestra un mensaje informativo en:

- Registros del sistema (FTD-6-748008)
- Archivo log/cluster\_trace.log, por ejemplo:

```
<#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
```

El mensaje indica que en caso de fallo de una unidad, se pueden sobresuscribir los otros recursos de la unidad.

## Modo simplificado

### Comportamiento en versiones anteriores a la 6.3 de FMC


- Cada nodo de clúster se registra individualmente en FMC.
- Luego se forma un clúster lógico en FMC.
- Para cada nueva adición de nodo de clúster, debe registrar manualmente el nodo.

### FMC posterior a la versión 6.3

- La función de modo simplificado le permite registrar todo el clúster en FMC en un solo paso

(simplemente registre cualquier nodo del clúster).

Administrador mínimo admitido	Dispositivos gestionados	Versión mínima de dispositivos administrados admitidos requerida	Notas
CSP 6.3	Clústeres FTD solo en FP9300 y FP4100	6.2.0	Se trata solo de una función de FMC

 Advertencia: Una vez que se ha formado el clúster en FTD, debe esperar a que se inicie el registro automático. No debe intentar registrar los nodos del clúster manualmente (Agregar dispositivo), sino que debe utilizar la opción Reconciliar.

## Síntoma

### Fallos de registro del nodo

- Si el registro del nodo de control falla por cualquier motivo, el clúster se elimina de FMC.

### Mitigación

Si el registro del nodo de datos falla por cualquier motivo, hay 2 opciones:

1. Con cada implementación en el clúster, FMC comprueba si hay nodos del clúster que deban registrarse y, a continuación, inicia el registro automático para estos nodos.
2. Hay una opción Reconciliar disponible en la ficha de resumen del clúster (enlace Dispositivos > Administración de dispositivos > ficha Clúster > Ver estado del clúster). Una vez que se activa la acción de reconciliación, FMC inicia el registro automático de los nodos que deben registrarse.

## Información Relacionada

- [Agrupación en clústeres para Firepower Threat Defence](#)
- [Clúster ASA para el chasis Firepower 4100/9300](#)
- [Acerca de la agrupación en clústeres en el chasis Firepower 4100/9300](#)
- [Perspectiva en profundidad de la agrupación en clústeres de Firepower NGFW - BRKSEC-3032](#)
- [Análisis de las capturas de firewall de Firepower para solucionar problemas de red de manera eficaz](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).