أستكشاف أخطاء مجموعة الدفاع عن تهديد FirePOWER (FTD) وإصلاحها

المحتويات

المقدمة

يصف هذا المستند أستكشاف أخطاء إعداد نظام مجموعة وإصلاحها على جدار حماية الجيل التالي (NGFW) من FirePOWER.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية (راجع قسم المعلومات ذات الصلة للروابط):

- بنية النظام الأساسي Firepower
- تكوين مجموعة Firepower وتشغيلها
- التعرف على واجهة سطر الأوامر (CLI) الخاصة ب FTD و FirePOWER
- سجلات مستوى البيانات/NGFW
- NGFW/مستوى البيانات Packet-tracer
- التقاط مستوى البيانات/FXOS

المكونات المستخدمة

- هيغ دبليو: Firepower 4125
- ستيفاني: 6.7.0 (بنية 65) - مستوى البيانات 9.15(1)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

كما أن معظم العناصر التي يغطيها هذا المستند تنطبق بالكامل على أستكشاف أخطاء مجموعة أجهزة الأمان المعدلة (ASA) وإصلاحها.

التكوين

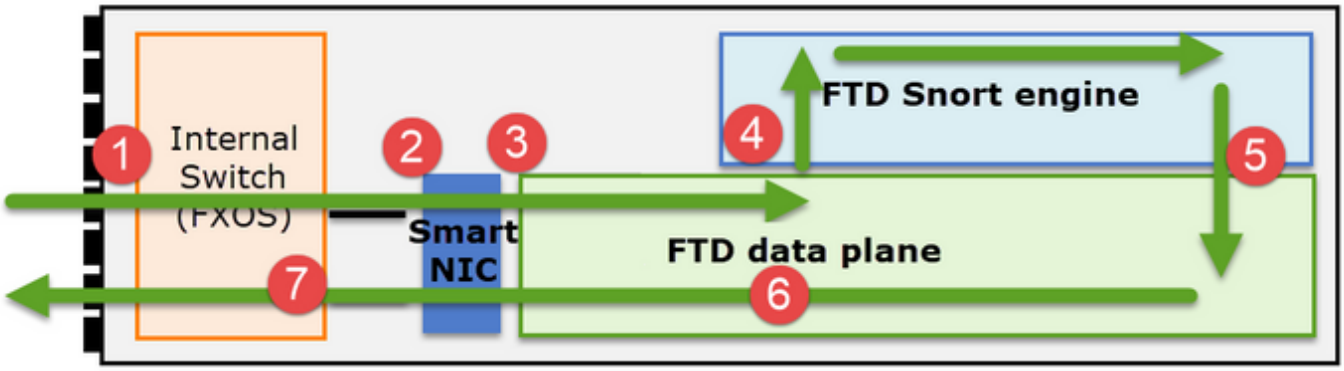
تتم تغطية جزء التكوين من نشر نظام المجموعة في أدلة تكوين FMC و FXOS:

- التجميع الخاص بالدفاع ضد تهديد قوة النيران
- نشر مجموعة للدفاع عن تهديد الطاقة النارية لضمان قابلية التطوير والتوفر العالي

أساسيات المجموعة

بنية NGFW

من المهم فهم كيفية معالجة FirePOWER 41xx أو 93xx series لحزم النقل:



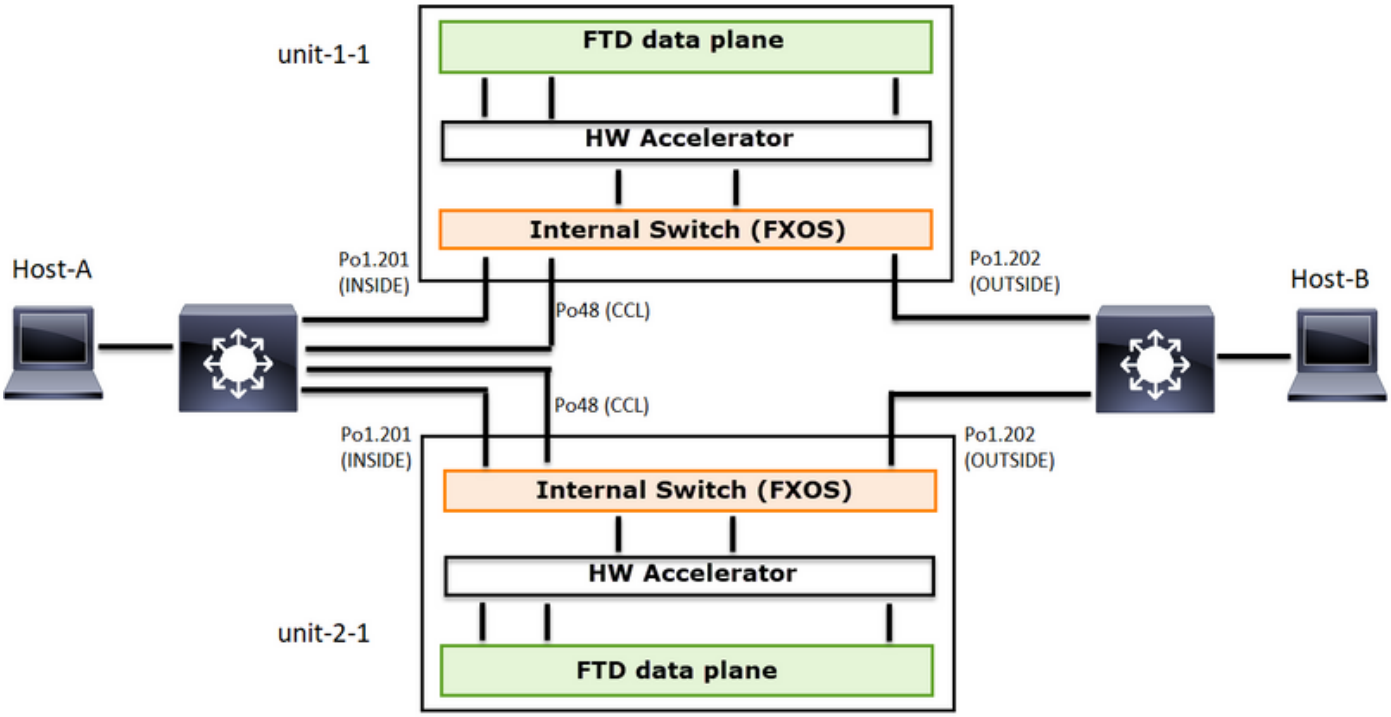
1. تدخل الحزمة واجهة الدخول، ويعالج بالمحول الداخلي للهيكل.
2. تمر الحزمة عبر الـ NIC ذكي. إذا تم إلغاء تحميل التدفق (تسريع HW)، حينئذ تتم معالجة الحزمة فقط من قبل NIC الذكي، ثم يتم إرسالها مرة أخرى إلى الشبكة.
3. إذا لم يتم إلغاء تحميل الحزمة، فإنها تدخل مستوى بيانات FTD الذي يقوم أساسا بفحص L3/L4.
4. إذا كانت السياسة تتطلب ذلك، يتم فحص الحزمة بواسطة محرك الشخير (فحص L7 بشكل أساسي).
5. يرجع محرك الشخير حكما (على سبيل المثال، السماح أو الحظر) للحزمة.
6. يقوم مستوى البيانات بإسقاط الحزمة أو إعادة توجيهها بناء على قرار الشخر.
7. تعمل الحزمة على تركيب الهيكل من خلال محول الهيكل الداخلي.

التقاط نظام المجموعة

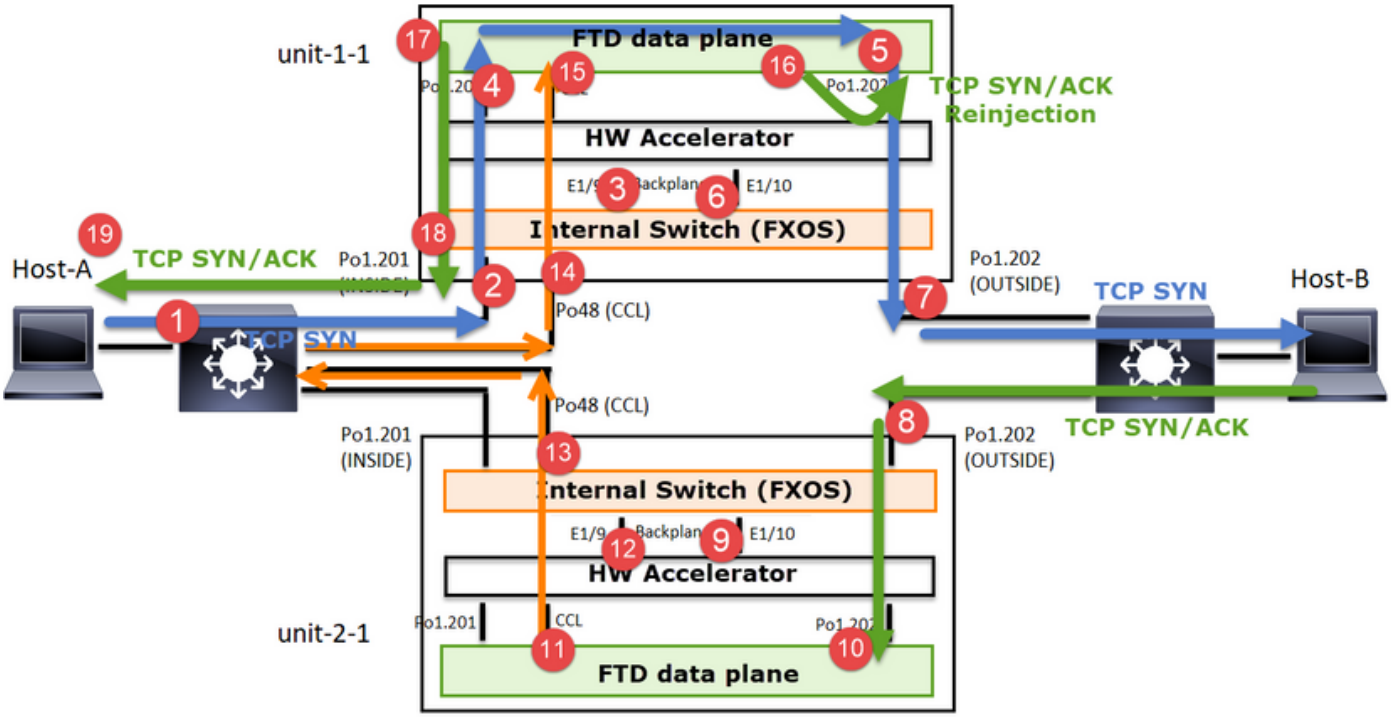
توفر أجهزة FirePOWER نقاط التقاط متعددة توفر إمكانية رؤية في تدفقات النقل. عند أستكشاف أخطاء نظام المجموعة وإصلاحها وتمكينها، تكون التحديات الرئيسية هي:

- يزداد عدد عمليات الالتقاط كلما زاد عدد الوحدات في نظام المجموعة.
- يجب أن تكون على دراية بالطريقة التي يتعامل بها نظام المجموعة مع تدفق معين لتتمكن من تعقب الحزمة عبر نظام المجموعة.

يوضح هذا المخطط مجموعة مكونة من وحدتين (على سبيل المثال، FP941xx/FP9300):



في حالة إنشاء اتصال TCP غير متماثل، يبدو نظام TCP، تبادل SYN/ACK كما يلي:



إعادة توجيه حركة المرور

1. يتم إرسال TCP SYN من المضيف-A إلى المضيف-B.
2. يصل TCP SYN إلى الهيكل (أحد أعضاء Po1).
3. يتم إرسال TCP SYN من خلال إحدى واجهات اللوحة الخلفية للهيكل (على سبيل المثال، E1/9، E1/10، وما إلى ذلك) إلى مستوى البيانات.
4. يصل TCP SYN إلى واجهة مدخل مستوى البيانات (Po1.201/Inside). في هذا المثال، تقوم الوحدة 1-1 بملكية التدفق، وتقوم بالترتيب العشوائي للرقم التسلسلي الأولي (IS)، وتقوم بترميز معلومات الملكية (ملف تعريف الارتباط) في الرقم الفريد.

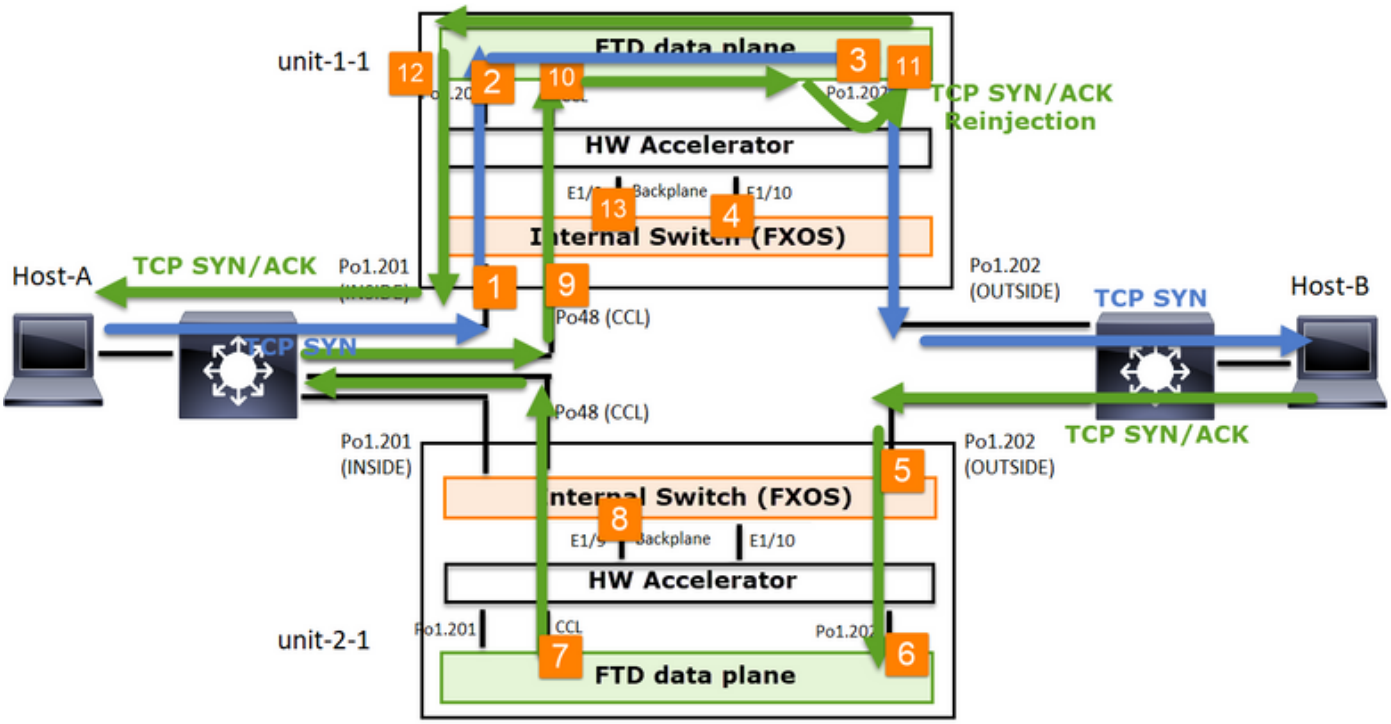
5. يتم إرسال TCP SYN من Po1.202/Outdoor (واجهة مخرج مستوى البيانات).
6. يصل TCP SYN إلى إحدى واجهات اللوحة الخلفية للهيكل (على سبيل المثال، E1/9 و E1/10، وما إلى ذلك).
7. يتم إرسال TCP SYN من الواجهة المادية للهيكل (أحد أعضاء Po1) باتجاه Host-B.

إرجاع حركة المرور

8. يتم إرسال TCP SYN/ACK من المضيف-B ويصل إلى الوحدة-2-1 (أحد أعضاء Po1).
9. يتم إرسال TCP SYN/ACK عبر إحدى واجهات اللوحة الخلفية للهيكل (على سبيل المثال، E1/9، E1/10، وما إلى ذلك) إلى مستوى البيانات.
10. يصل TCP SYN/ACK على واجهة مدخل مستوى البيانات (Po1.202/Outdoor).
11. يتم إرسال TCP SYN/ACK من إرتباط التحكم في النظام الأساسي (CCL) إلى الوحدة 1-1. يتم تمكين IS بشكل افتراضي. وبالتالي، يجد مقدم العرض معلومات المالك الخاصة ب TCP SYN+ACK دون تدخل من المدير. بالنسبة للحزم الأخرى أو عندما يتم تعطيل IS، يتم الاستعلام عن المدير.
12. يصل TCP SYN/ACK إلى إحدى واجهات اللوحة الخلفية للهيكل (على سبيل المثال، E1/9 و E1/10 وما إلى ذلك).
13. يتم إرسال TCP SYN/ACK من الواجهة المادية للهيكل (أحد أعضاء Po48) تجاه الوحدة 1-1.
14. يصل TCP SYN/ACK على الوحدة 1-1 (أحد أعضاء Po48).
15. تتم إعادة توجيه TCP SYN/ACK من خالل واحدة من واجهات اللوحة الخلفية للهيكل إلى واجهة قناة CCL لمستوى البيانات (نظام المجموعة Namelf).
16. يعمل مستوى البيانات على إعادة إدخال حزمة TCP SYN/ACK إلى واجهة مستوى البيانات Po1.202/Outdoor.
17. يتم إرسال TCP SYN/ACK من Po1.201/Inside (واجهة مخرج مستوى البيانات) نحو Host-A.
18. يجتاز TCP SYN/ACK إحدى واجهات اللوحة الخلفية للهيكل (على سبيل المثال، E1/9، E1/10، وما إلى ذلك) ويصنف أحد أعضاء Po1.
19. يصل TCP SYN/ACK على المضيف-A.

لمزيد من التفاصيل حول هذه السيناريو، أقرأ القسم ذي الصلة في دراسات الحالة الخاصة بإنشاء اتصال نظام المجموعة.

استنادا إلى تدابير الحزم هذه، فإن جميع نقاط التقاط نظام المجموعة المحتملة هي:



لحركة مرور البيانات التي يتم توجيهها (على سبيل المثال، TCP SYN) على:

1. الواجهة المادية للهيكل (على سبيل المثال، أعضاء Po1). يتم تكوين هذا الالتقاط من واجهة مستخدم "مدير الهيكل" (CM) أو واجهة سطر الأوامر (CLI) الخاصة ب CM.
2. واجهة مدخل مستوى البيانات (على سبيل المثال، Po1.201 INSIDE).
3. واجهة مخرج مستوى البيانات (على سبيل المثال، Po1.202 خارج).
4. واجهات اللوحة الخلفية للهيكل. على FP4100 هناك 2 قارن لوحة خلفية. في FP9300 هناك ما مجموعه 6 (2 لكل وحدة نمطية). بما أن أنت لا تعرف في أي قارن تصل الربط، أنت ينبغي مكنت قبض على كل قارن.

بالنسبة لحركة مرور الإرجاع (على سبيل المثال، TCP SYN/ACK) التي تم التقاطها على:

5. الواجهة المادية للهيكل (على سبيل المثال، أعضاء Po1). يتم تكوين هذا الالتقاط من واجهة مستخدم "مدير الهيكل" (CM) أو واجهة سطر الأوامر (CLI) الخاصة ب CM.
6. واجهة مدخل مستوى البيانات (على سبيل المثال، Po1.202 OUTDOOR).
7. بما أن الربط يكون أعدت وجهت التالي التقاط نقطة وه ال CCL مستوى البيانات.
8. واجهات اللوحة الخلفية للهيكل. ثانية، أنت ينبغي مكنت على كل قارن.
9. واجهات أعضاء قائمة التحكم في الوصول (CCL) للوحدة-1-1 للهيكل.
10. واجهة CCL لمستوى البيانات (نظام المجموعة Namelf).
11. واجهة الدخول (Po1.202 خارج). هذه هي الحزمة التي تم إعادتها من CCL إلى مستوى البيانات.
12. واجهة مخرج مستوى البيانات (على سبيل المثال، Po1.201 INSIDE).
13. واجهات اللوحة الخلفية للهيكل.

كيفية تمكين التقاط نظام المجموعة

التقاط FXOS

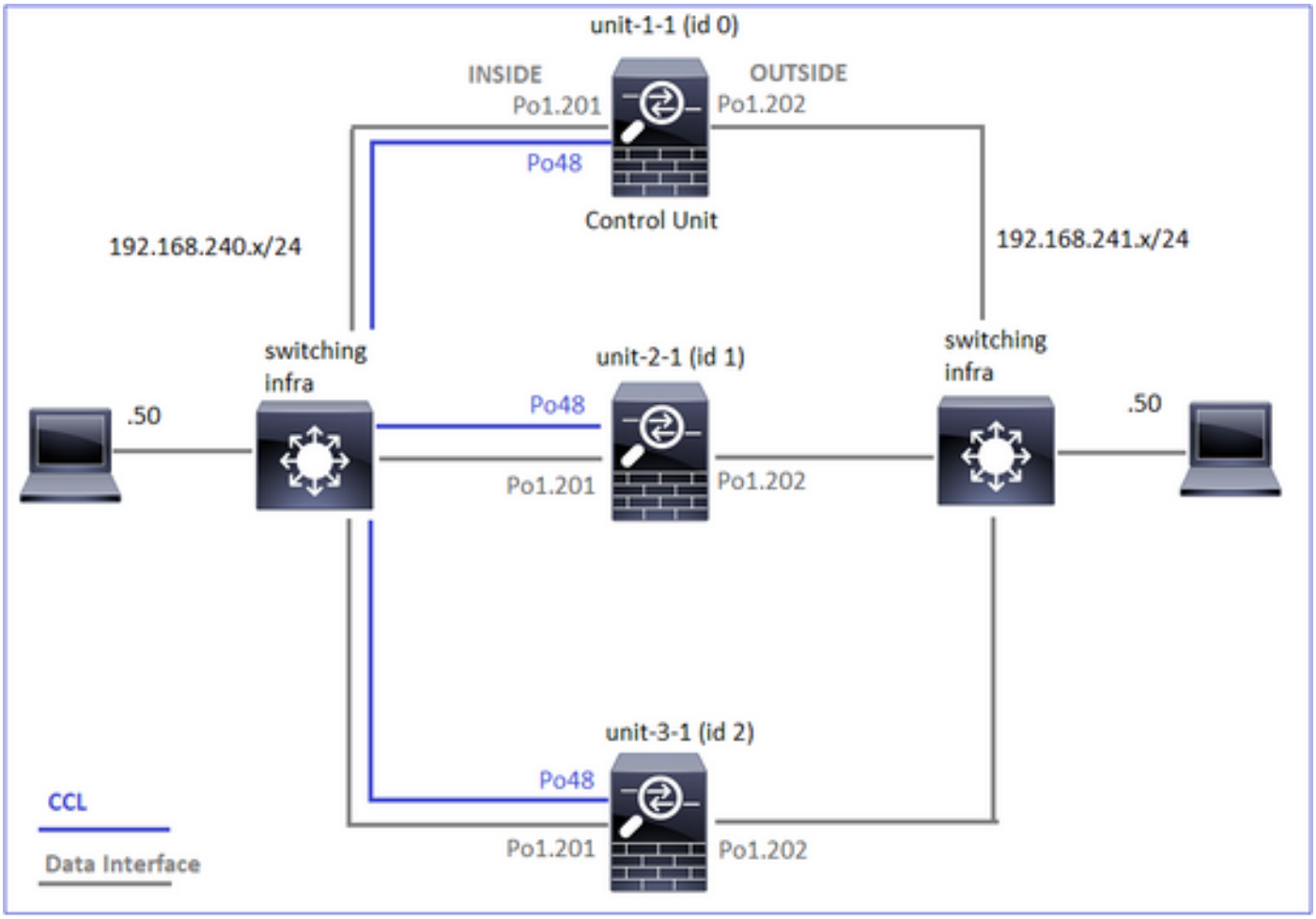
يتم وصف العملية في دليل تكوين FXOS: التقاط الحزم

ملاحظة: يمكن التقاط FXOS فقط في إتجاه المدخل من وجهة نظر المحول الداخلي.

التقاط مستوى البيانات

الطريقة الموصى بها لتمكين الالتقاط على جميع أعضاء المجموعة هي باستخدام أمر cluster exec.

ولنتأمل هنا مجموعة تتألف من ثلاث وحدات:



للتحقق من وجود التقاط نشط في كل وحدات نظام المجموعة، أستخدم هذا الأمر:

```
<#root>

firepower#

cluster exec show capture


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

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

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

لتمكين التقاط مستوى بيانات على جميع الوحدات على Po1.201 (INSIDE):

```
<#root>

firepower#

cluster exec capture CAPI interface INSIDE
```

يوصى بشدة بتحديد مرشح الالتقاط، وفي حالة توقع الكثير من حركة المرور، لزيادة مخزن الالتقاط المؤقت:

```
<#root>

firepower#

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

التحقق

```
<#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
```

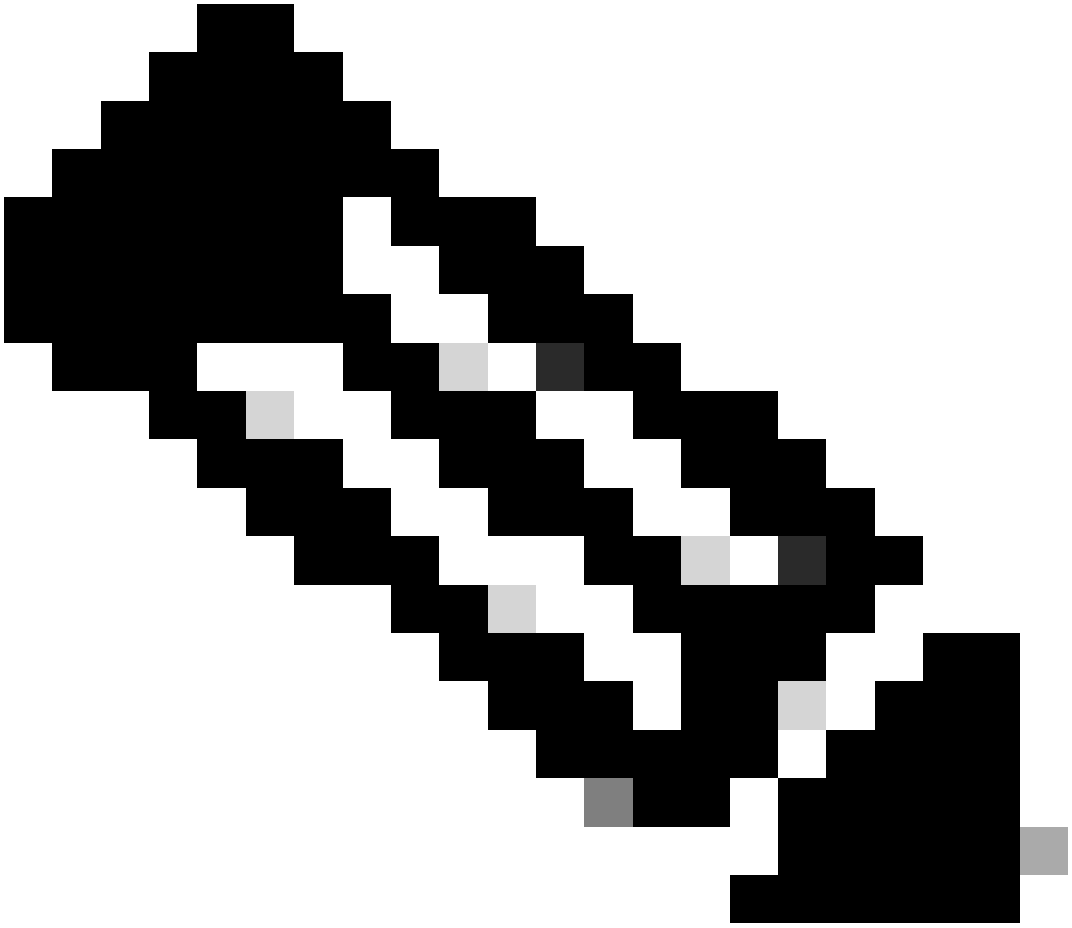
لرؤية محتويات كل الالتقاط (يمكن أن يكون هذا الإخراج طويل جدا):

```
<#root>

firepower#

terminal pager 24


firepower#

cluster exec show capture CAPI
```

```
unit-1-1(LOCAL):******************************************************
21 packets captured

1: 11:33:09.879226 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: S 2225395909:2225395909
2: 11:33:09.880401 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.45456: S 719653963:719653963(0
3: 11:33:09.880691 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: . ack 719653964 win 229
4: 11:33:09.880783 802.1Q vlan#201 P0 192.168.240.50.45456 > 192.168.241.50.80: P 2225395910:2225396054

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

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

مسارات الالتقاط

إذا كنت ترغب في رؤية كيفية معالجة حزم الدخول بواسطة مستوى البيانات على كل وحدة، فاستخدم الكلمة الأساسية trace. هذا يتتبع أول 50 رطب مدخل. يمكنك تتبع حتى 1000 حزمة مدخل.



ملاحظة: في حالة تطبيق عدة التقاط على واجهة، يمكنك تتبع حزمة واحدة مرة واحدة فقط.

لتتبع أول 1000 حزمة مدخل على قارن خارجي على كل وحدات نظام المجموعة:

<#root>

firepower#

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

بمجرد التقاط تدفق الفائدة هناك حاجة إلى التأكد من أنك تتبعت حزم الفائدة على كل وحدة. الشيء المهم الذي يجب تذكره هو أن الحزمة المحددة يمكن أن تكون #1 على الوحدة-1-1، لكن #2 على وحدة أخرى، وهكذا.

في هذا المثال، أنت يستطيع رأيت أن ال syn/ACK ربط #2 على وحدة-2-1، غير أن ربط #1 على

وحدة-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 P0 192.168.240.50.45468 > 192.168.241.50.80: S 441626016:441626016(0)
2: 12:58:31.118341 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45468:

S

 301658077:301658077(0)

ack

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

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

unit-3-1:*******************************************************************
1: 12:58:31.111429 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45468:

S

 301658077:301658077(0)

ack

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

لتتبع الحزمة رقم 2 (SYN/ACK) على الوحدة المحلية:

```
<#root>

firepower#

cluster exec show cap CAPO packet-number 2 trace


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

2: 12:58:31.118341 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45468:

S

 301658077:301658077(0)

ack

 441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
MAC Access list
...
```

لتتبع الحزمة نفسها (SYN/ACK) على الوحدة البعيدة:

<#root>

```
firepower#
```

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

```
1: 12:58:31.111429 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45468:
```

S

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

ack

```
 441626017 win 28960 <mss 1460,sackOK,timestamp 1125686319 1115330849,nop,wscale 7>
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
...
```

التقاط CCL

لتمكين الالتقاط على إرتباط CCL (على جميع الوحدات):

<#root>

```
firepower#
```

cluster exec capture CCL interface cluster

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

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

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

إعادة إدخال إخفاء

بشكل افتراضي، يعرض الالتقاط الذي تم تمكينه على واجهة بيانات مستوى البيانات جميع الحزم:

- التي تصل من الشبكة المادية
- التي تم إعادتها من CCL

إذا كنت ال تريد أن ترى الحزم التي تم إعادة حقنها، أستخدم الخيار reinject-hide. يمكن أن يكون هذا مفيدا إذا كنت تريد التحقق من أن التدفق غير متماثل:

```
<#root>

firepower#

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

يظهر لك هذا االلتقاط فقط ما تتلقاه الوحدة المحلية بالفعل على الواجهة المحددة مباشرة من الشبكة المادية، وليس من وحدات المجموعة الأخرى.

عمليات إسقاط ASP

إذا كنت ترغب في التحقق من عمليات إسقاط البرامج لتدفق معين، فيمكنك تمكين التقاط ASP-DROP. إذا لم تكن تعرف سبب الإسقاط الذي يجب التركيز عليه، فاستخدم الكلمة الأساسية all. بالإضافة إلى ذلك، إذا لم تكن متأكدا بالحمولة في الحزمة، يمكنك تحديد الكلمة الأساسية الرؤوس فقط. وهذا يتيح لك التقاط حزم أكثر ب 20 إلى 30 مرة:

```
<#root>

firepower#

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


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

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

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

وبالإضافة إلى ذلك، يمكنك تحديد عناوين IP موضع الاهتمام في التقاط ASP:

```
<#root>

firepower#

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


match ip host 192.0.2.100 any
```

مسح التقاط

لمسح المخزن المؤقت من أي التقاط يتم تشغيله في جميع وحدات نظام المجموعة. الي يؤدي هذا إلى إيقاف عمليات االلتقاط، ولكنه يعمل فقط على مسح المخازن المؤقتة:

```
<#root>

firepower#

cluster exec clear capture /all

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

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

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

إيقاف التقاط

هناك طريقتان لإيقاف التقاط نشط لكل وحدات نظام المجموعة. الحاقي يمكنك إستئناف.

الطريقة 1

```
<#root>

firepower#

cluster exec cap CAPI stop

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

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

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

فنأتسي

```
<#root>

firepower#

cluster exec no capture CAPI stop

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

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

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

الطريقة الثانية

```
<#root>

firepower#

cluster exec no capture CAPI interface INSIDE

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

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

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

فيتأنس

```
<#root>

firepower#

cluster exec capture CAPI interface INSIDE

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

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

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

تجميع التقاط

هناك طرق متعددة لتصدير التقاط.

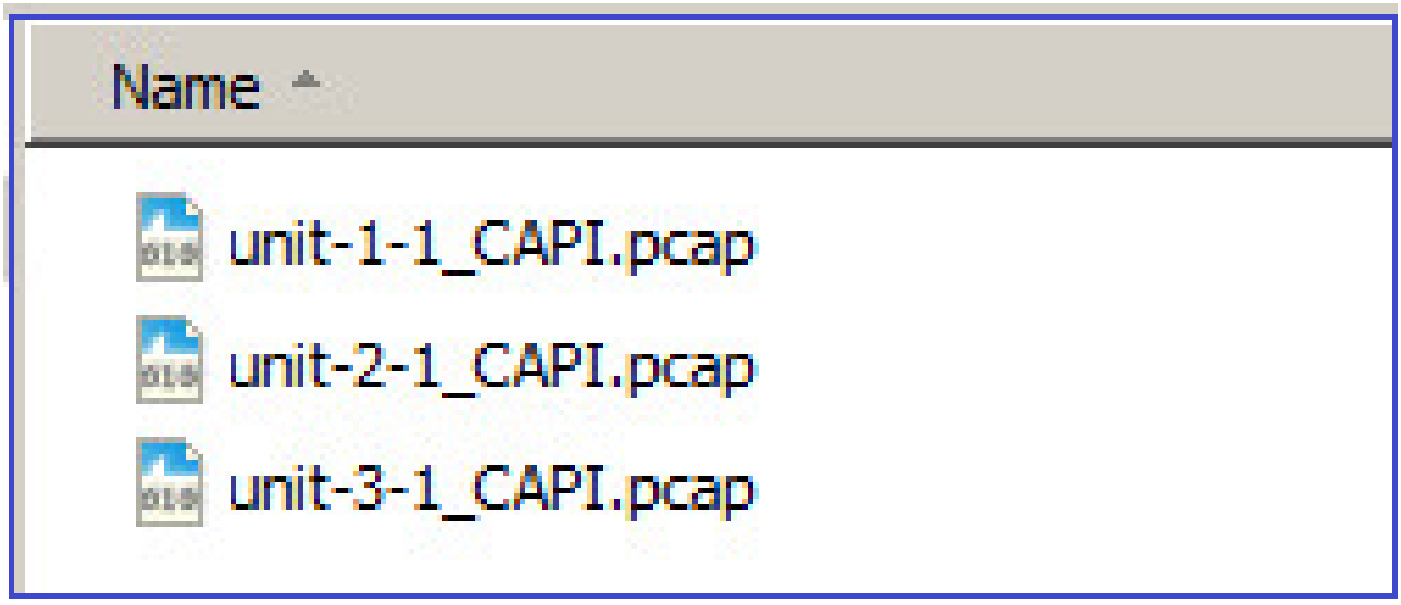
الطريقة 1 - إلى خادم بعيد

وهذا يتيح لك تحميل التقاط من مستوى البيانات إلى خادم بعيد (على سبيل المثال، TFTP). تتغير أسماء الالتقاط تلقائيا لتعكس الوحدة المصدر:

```
<#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 !
```

ملفات PCAP التي تم تحميلها:



الطريقة 2 - إحضار التقاط من FMC

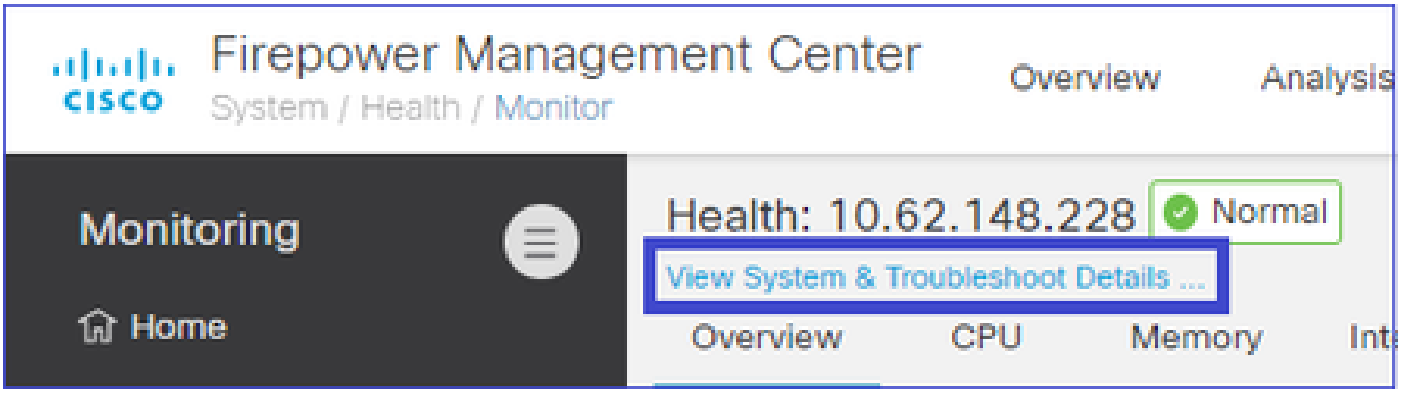
لا تنطبق هذه الطريقة إلا على FTD. أولا، قم بنسخ الالتقاط إلى قرص FTD:

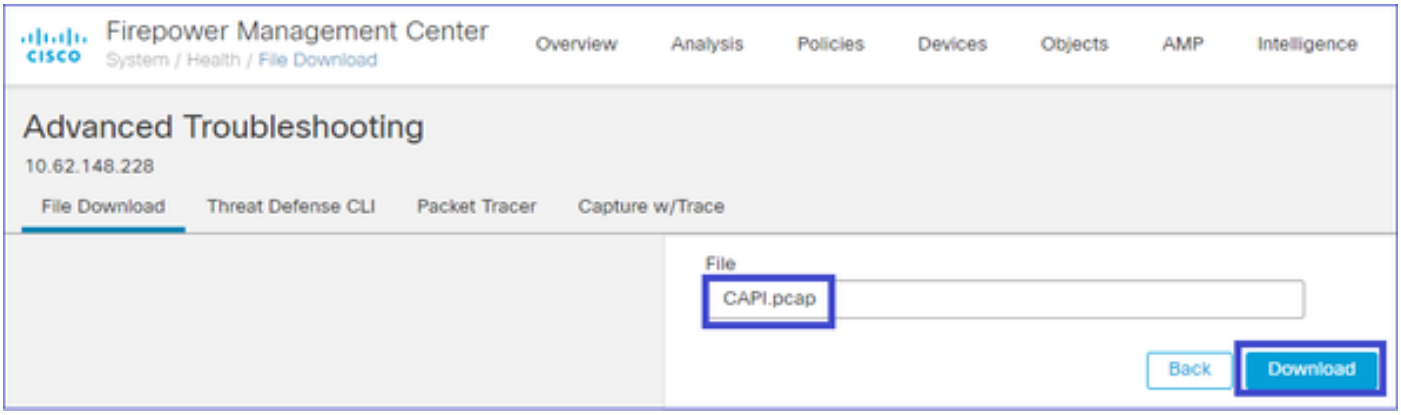
```
<#root>

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
```

من وضع الخبير، انسخ الملف من /mnt/disk0/ إلى /ngfw/var/common/ directory:

```
<#root>

>

expert


admin@firepower:~$

cd /mnt/disk0


admin@firepower:/mnt/disk0$

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

وأخيرا، على FMC، انتقل إلى قسم النظام > الصحة > الشاشة. أختر عرض النظام وتفاصيل أستكشاف الأخطاء وإصلاحها > أستكشاف الأخطاء وإصلاحها المتقدم وجلب ملف الالتقاط:





حذف التقاط

لإزالة التقاط من كل وحدات نظام المجموعة، أستخدم هذا الأمر:

```
<#root>

firepower#
```

```
cluster exec no capture CAPI

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

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

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

تدفقات تم إلغاء تحميلها

في تدفقات FP41xx/FP9300 يمكن تفريغها إلى مسرع الأجهزة إما بشكل ثابت (على سبيل المثال، قواعد FastPath) أو بشكل ديناميكي. لمزيد من التفاصيل حول إلغاء تحميل التدفق، تحقق من هذا المستند:

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

إذا تم إلغاء تحميل تدفق، فعندئذ تنتقل حزم قليلة فقط من خلال مستوى بيانات FTD. ويتم التعامل مع الباقي بواسطة مسرع الأجهزة (بطاقة واجهة الشبكة الذكية).

من نقطة التقاط عرض، هذا يعني أنه إذا قمت بتمكين التقاط مستوى بيانات FTD فقط، فلن ترى جميع الحزم التي تمر عبر الجهاز. في هذه الحالة، يلزمك أيضا تمكين التقاط مستوى هيكل FXOS.

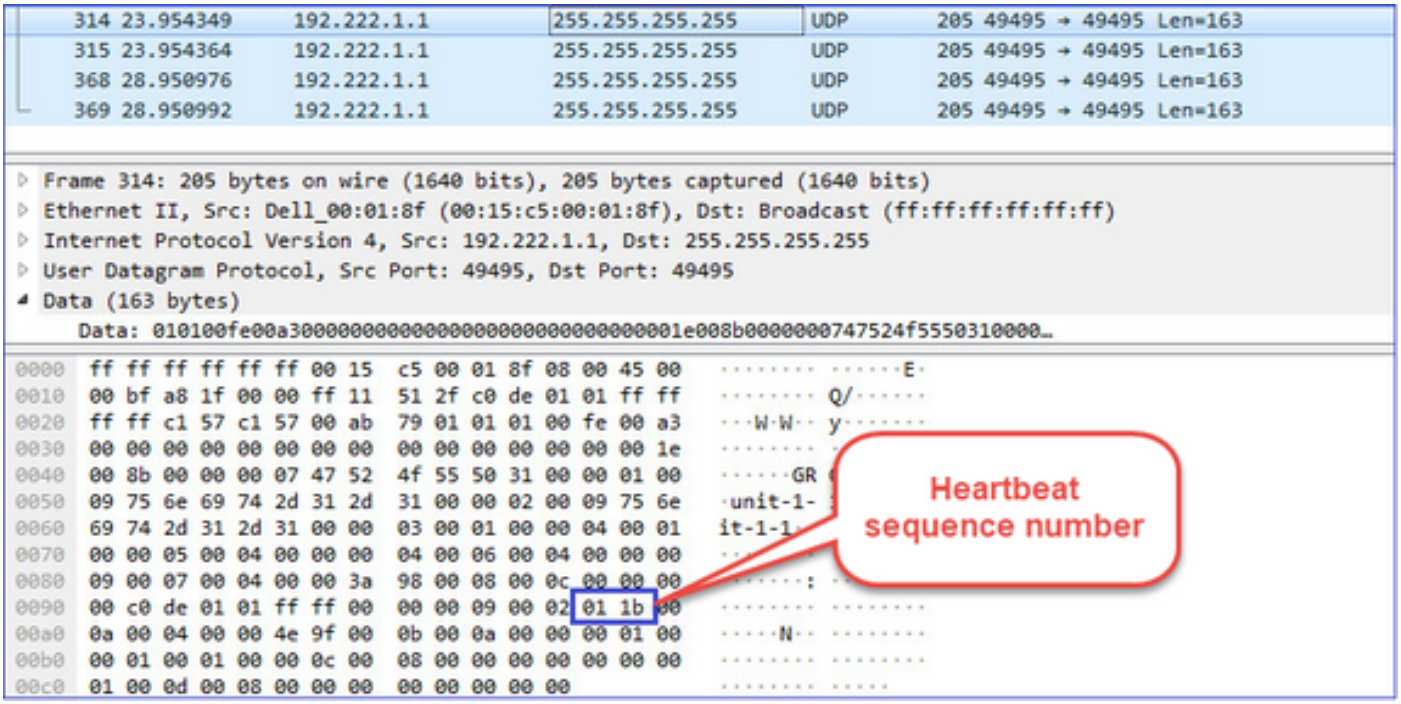
رسائل إرتباط التحكم في نظام المجموعة (CCL)

إذا قمت بالتقاط التقاط على CCL، تلاحظ أن وحدات نظام المجموعة تتبادل أنواع مختلفة من الرسائل. والاهتمامات هي:

البروتوكول	الوصف
UDP 49495	نبضات القلب العنقودية (رسائل تنشيط الاتصال) بث · L3 (255.255.255.255) · يتم إرسال هذه الحزم بواسطة كل وحدة نظام مجموعة في 1/3 من قيمة وقت الانتظار لفحص السلامة. · لاحظ أن حزم UDP 49495 التي تشاهد في الالتقاط ليست كلها نبضات قلب · تحتوي دقات القلب على رقم تسلسلي.
UDP 4193	رسائل مسار بيانات بروتوكول التحكم في نظام المجموعة البث الأحادي ·

	· تحتوي هذه الحزم على معلومات (بيانات تعريف) حول مالك التدفق والمدير ومالك النسخ الاحتياطي وما إلى ذلك. الأمثلة هي: · يتم إرسال رسالة "إضافة نظام المجموعة" من المالك إلى المدير عند إنشاء تدفق جديد · يتم إرسال رسالة "حذف نظام المجموعة" من المالك إلى المدير عند إنهاء التدفق
حزم البيانات	حزم البيانات التي تنتمي إلى تدفقات حركة المرور المختلفة التي تجتاز نظام المجموعة

نبضات القلب العنقودي



رسائل نقطة تحكم نظام المجموعة (CCP)

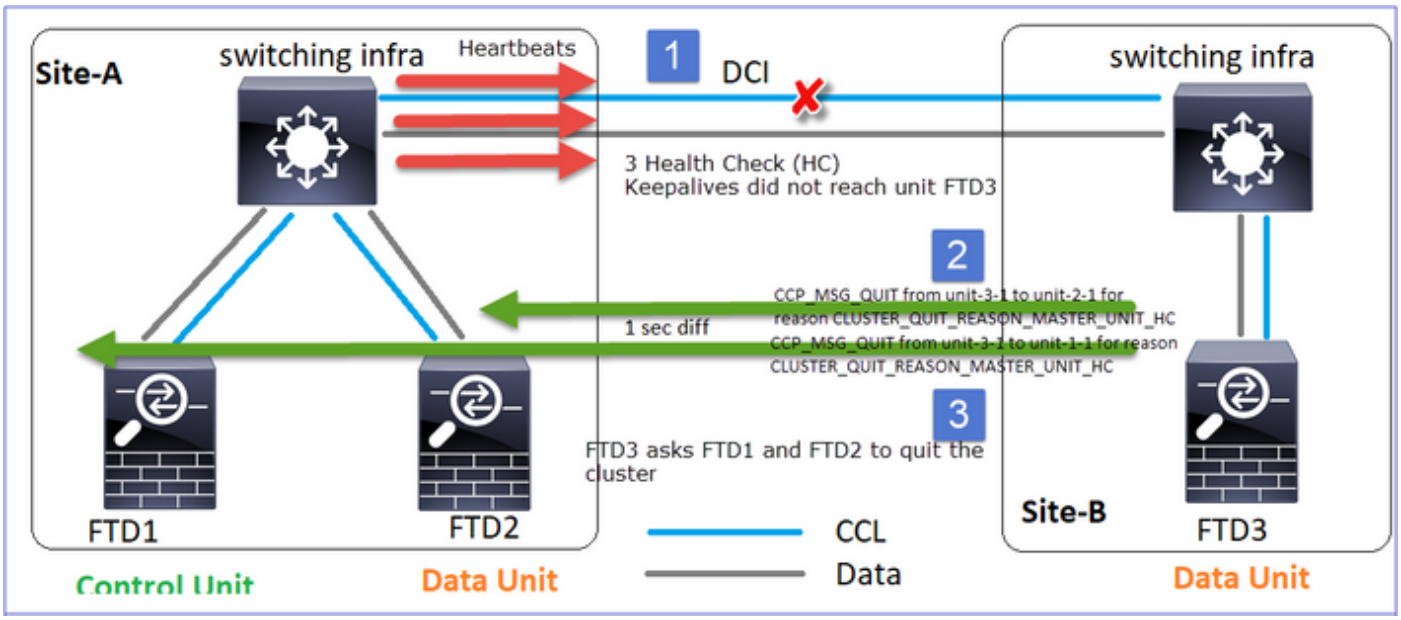
بالإضافة إلى رسائل النبضات، يوجد عدد من رسائل التحكم في نظام المجموعة يتم تبادلها عبر قائمة التحكم في الوصول (CCL) في سيناريوهات محددة. بعضها رسائل للبث الأحادي بينما البعض الآخر يتم إذاعته.

CLUSTER_QUIT_REASON_PRIMARY_UNIT_HC

كلما فقدت وحدة 3 رسائل متتالية لنبضات القلب من عقدة التحكم، تولد رسالة CLUSTER_QUIT_REASON_PRIMARY_UNIT_HC عبر قائمة التحكم في الوصول (CCL). هذه الرسالة:

- هو unicast.
- يتم إرسالها إلى كل وحدة بفاصل زمني 1 ثانية.

- عندما تتلقى إحدى الوحدات هذه الرسالة، قم بإنهاء نظام المجموعة (معطل) ثم قم بإعادة الربط.

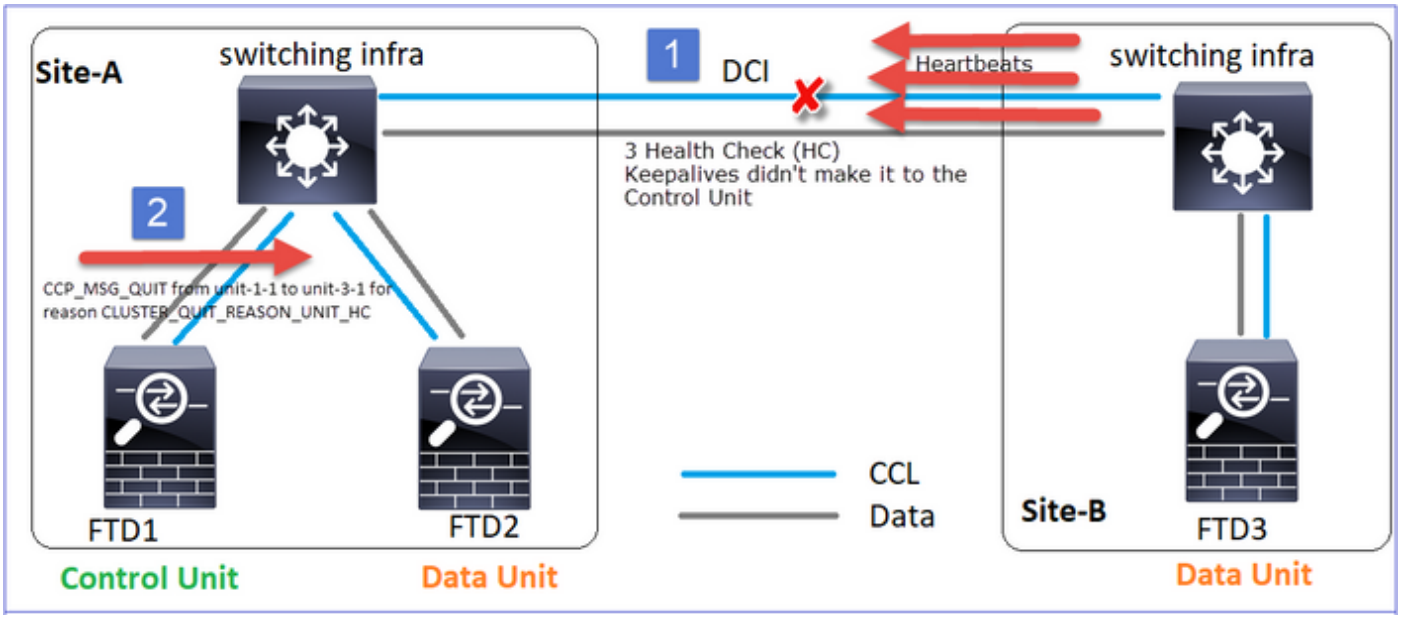


س. ما هو الغرض من نظام المجموعة_QUIT_REASON_PRIMARY_UNIT_HC؟

أ. من وجهة نظر الوحدة-3-1 (الموقع-ب)، تفقد الاتصال بكل من الوحدة-1 والوحدة-2-1 من الموقع أ، وبالتالي فإنها تحتاج إلى إزالتهم من قائمة أعضائها بأسرع ما يمكن، وإلا، فقد تكون الحزمة مفقودة إذا كانت الوحدة-2-1 لا تزال في قائمة أعضائها وصادف أن الوحدة-2-1 تكون مدير اتصال، ويفشل الاستعلام المتدفق إلى الوحدة-2-1.

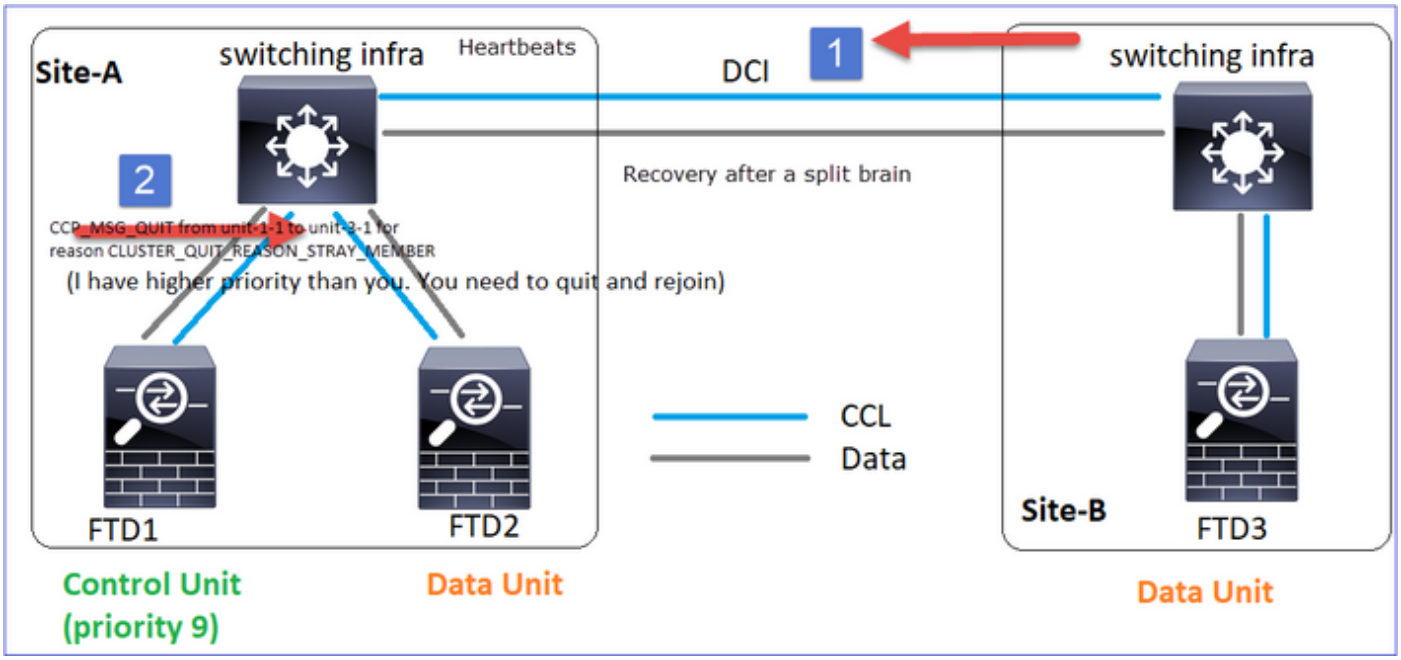
cluster_quit_reason_unit_hc

كلما فقدت عقدة التحكم 3 رسائل متتالية لنبضات القلب من عقدة بيانات، فإنها ترسل رسالة CLUSTER_QUIT_REASON_UNIT_HC عبر CCL. هذه الرسالة هي unicast.



CLUSTER_QUIT_REASON_STRAY_MEMBER

عندما تتم إعادة اتصال قسم مقسم بتقسيم نظير، تتم معالجة عقدة البيانات الجديدة كعضو سطحي بواسطة وحدة التحكم المسيطرة ويستلم رسالة CCP Quit مع سبب CLUSTER_QUIT_REASON_STRAY_MEMBER.



CLUSTER_QUIT_MEMBER_DROP

رسالة بث يتم إنشاؤها بواسطة عقدة بيانات، ويتم إرسالها كبث. بمجرد أن تستلم وحدة هذه الرسالة، تنتقل إلى حالة "معطل". بالإضافة إلى ذلك، لا تبدأ إعادة الربط التلقائي:

```
<#root>

firepower#

show cluster info trace | include DROPOUT

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

CLUSTER_QUIT_MEMBER_DROPOUT

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

CLUSTER_QUIT_MEMBER_DROPOUT
```

يظهر سجل نظام المجموعة:

```
<#root>

PRIMARY       DISABLED      Received control message DISABLE (

member dropout announcement

)
```

آلية التحقق من صحة المجموعات

النقاط الأساسية

- تقوم كل وحدة من وحدات نظام المجموعة بإرسال ضربات القلب كل 1/3 من قيمة وقت تعليق الفحص الصحي إلى جميع الوحدات الأخرى (بث 255.255.255.255) وتستخدم منفذ UDP 49495 عبر CCL.
- تقوم كل وحدة نظام مجموعة بتعقب كل وحدة أخرى بشكل مستقل باستخدام وحدة توقيت الاستطلاع وقيمة تعداد الاستقصاء.
- إذا لم تستلم وحدة نظام المجموعة أي حزمة (نبض القلب أو حزمة البيانات) من وحدة نظير نظام المجموعة ضمن فاصل زمني لنبضات القلب، فإنها تزيد من قيمة عدد الاستقصاء.
- عندما تصبح قيمة عدد الاستقصاء لوحدة نظير نظام المجموعة هي 3 يتم إعتبار النظير معطل.
- كلما تم تلقي نبضة قلب، يتم التحقق من رقم تسلسلها وفي حالة أختلاف ذلك، فإن عداد النبضات يزداد وقوائم النبضات التي تم استقبالها سابقا عن 1.
- إذا كان عداد عدد الاستقصاء الخاص بنظر نظام المجموعة مختلفا عن 0، وتم تلقي الحزمة بواسطة النظير، تتم إعادة تعيين العداد إلى قيمة 0.

أستخدم هذا الأمر للتحقق من عدادات حماية نظام المجموعة:

<#root>

```
firepower#
```

show cluster info health details

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

وصف الأعمدة الرئيسية

العمود	الوصف
الوحدة (المعرف)	معرف نظير نظام المجموعة البعيد.
عدد نبضات القلب	عدد نبضات القلب التي تم تلقيها من النظير البعيد عبر CCL.

انحدارات نبضات القلب	عدد نبضات القلب التي تفتقد. يتم حساب هذا العداد استنادا إلى رقم تسلسل نبض القلب الذي تم تلقيه.
متوسط الفجوة	متوسط الفترة الزمنية للنبضات التي تم تلقيها.
عدد الاستقصاءات	عندما يصبح هذا العداد 3، تتم إزالة الوحدة من نظام المجموعة. الفاصل الزمني لاستعلام الاستقصاء هو نفس الفاصل الزمني لنبضات الفواصل الزمنية ولكن يتم تشغيله بشكل مستقل.

إعادة ضبط العدادات أستخدم هذا الأمر:

```
<#root>

firepower#

clear cluster info health details
```

س. كيف نتحقق من تكرار نبضات القلب؟

أ - التحقق من متوسط قيمة الفجوة:

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

س. كيف يمكنك تغيير وقت تعليق نظام المجموعة في FTD؟

أ. إستخدام FlexConfig

س. من يصبح عقدة التحكم بعد انقسام الدماغ؟

ألف - الوحدة ذات الأولوية العليا (أقل عدد):

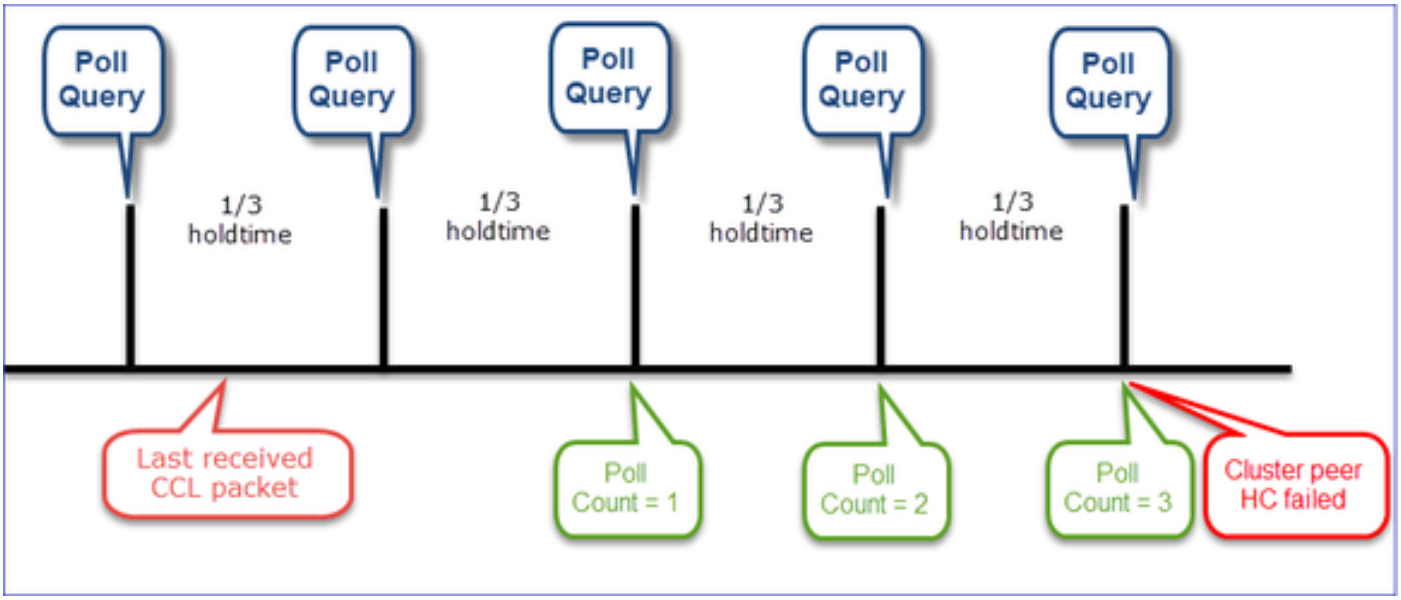
<#root>

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

```
priority 9
```

راجع سيناريو فشل HC 1 للحصول على مزيد من التفاصيل.

عرض آلية التنسيق بين المجموعات



المؤقتات الإرشادية: يعتمد الحد الأدنى والحد الأقصى على آخر وصول لحزم CCL تم إستلامه.

وقت الانتظار	فحص استعلام الاستقصاء (تردد)	الحد الأدنى لوقت الكشف	الحد الأقصى لوقت الكشف
3 ثواني (الافتراضي)	~1 ثانية	~3.01 ثانية	~3.99 ثانية

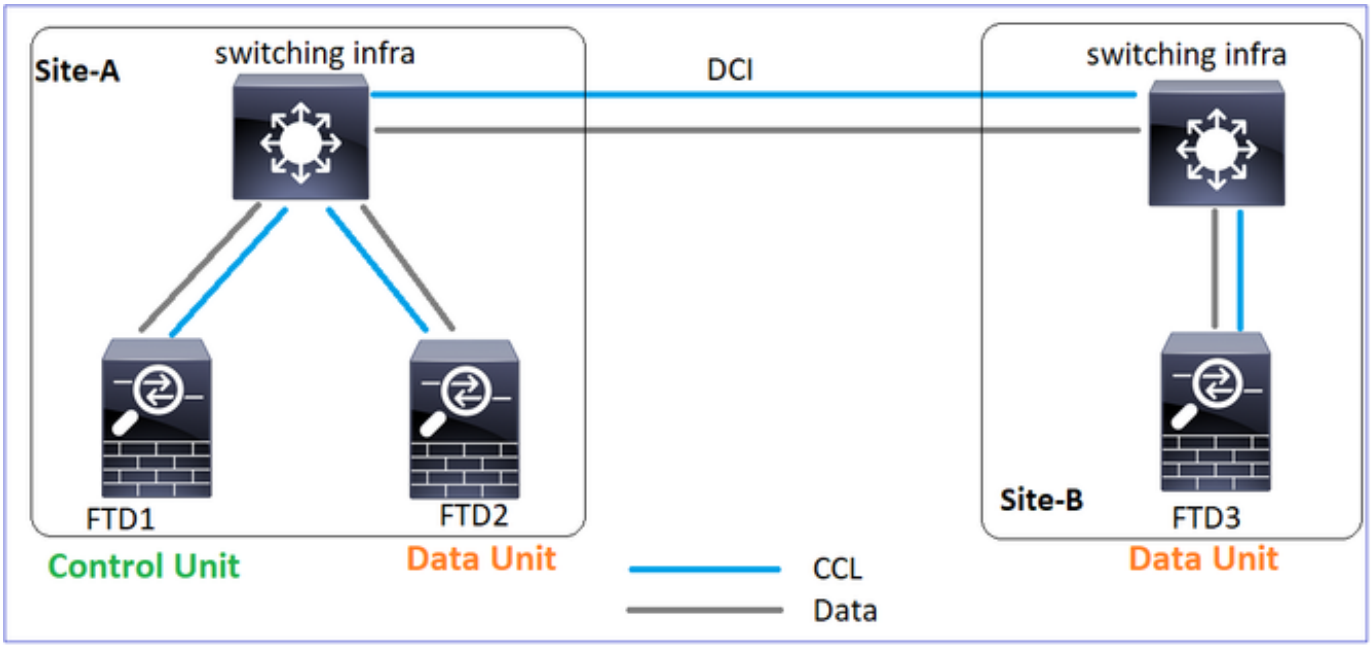
4 ثواني	~1.33 ثانية	~4.01 ثانية	~5.32 ثانية
5 ثواني	~1.66 ثانية	~5.01 ثانية	~6.65 ثانية
6 ثواني	~2 ثانية	~6.01 ثانية	~7.99 ثانية
7 ثواني	~2.33 ثانية	~7.01 ثانية	~9.32 ثانية
8 ثواني	~2.66 ثانية	~8.01 ثانية	~10.65 ثانية

سيناريوهات فشل HC لنظام المجموعة

أهداف هذا القسم هي توضيح:

- سيناريوهات مختلفة لفشل نظام المجموعة.
- كيف يمكن ربط السجلات المختلفة ومخرجات الأوامر.

المخطط



تكوين نظام المجموعة

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

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

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

حالة نظام المجموعة

الوحدة 1-1

```
<#root>

firepower#

show cluster info


Cluster GROUP1: On
    Interface mode: spanned


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


        ID        : 0
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH22247LNK
        CCL IP    : 10.17.1.1
        CCL MAC   : 0015.c500.018f
        Last join : 20:25:36 UTC Nov 1 2020
        Last leave: 20:25:28 UTC Nov 1 2020
Other members in the cluster:


Unit "unit-3-1" in state secondary


        ID        : 1
        Site ID   : 2
        Version   : 9.12(2)33
        Serial No.: FCH22247MKJ
        CCL IP    : 10.17.3.1
        CCL MAC   : 0015.c500.038f
        Last join : 20:58:45 UTC Nov 1 2020
        Last leave: 20:58:37 UTC Nov 1 2020
```

الوحدة 2-1

```
<#root>

firepower#

show cluster info


Cluster GROUP1: On
    Interface mode: spanned


This is "unit-2-1" in state SECONDARY


        ID        : 2
        Site ID   : 1
        Version   : 9.12(2)33
        Serial No.: FCH23157Y9N
        CCL IP    : 10.17.2.1
        CCL MAC   : 0015.c500.028
        Last join : 20:44:46 UTC
        Last leave: 20:44:38 UTC
Other members in the cluster:


 Unit "unit-1-1" in state PRIMARY


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

Unit "unit-2-1" in state SECONDARY	Unit "unit-3-1" 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	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

السيناريو 1

فقدان الاتصال CCL لمدة 4+ ثانية تقريبا في كل الاتجاهين.

قبل الفشل

FTD1	FTD2	FTD3
سايت-أ	سايت-أ	سايت ب
عقدة التحكم	عقدة البيانات	عقدة البيانات

بعد الاستدراد (لا توجد تغييرات في أدوار الوحدات)

FTD1	FTD2	FTD3
سايت-أ	سايت-أ	سايت ب
عقدة التحكم	عقدة البيانات	عقدة البيانات

تحليل

الفشل (تم فقد اتصال CCL).

رسالة وحدة تحكم مستوى البيانات على الوحدة-3-1:

<#root>

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


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

Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled.
To recover either enable clustering or remove cluster group configuration.
```

سجلات تتبع نظام المجموعة للوحدة 1-1:

<#root>

```
firepower#
show cluster info trace | include unit-3-1

Nov 02 09:38:14.239 [INFO]Notify chassis de-bundle port for blade unit-3-1, stack 0x000055a8918307fb 0x
Nov 02 09:38:14.239 [INFO]FTD - CD proxy received state notification (DISABLED) from unit unit-3-1
Nov 02 09:38:14.239
[DBUG]Send CCP message to all: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_MEMBER_DRO

Nov 02 09:38:14.239 [INFO]Notify chassis de-bundle port for blade unit-3-1, stack 0x000055a8917eb596 0x
Nov 02 09:38:14.239
[DBUG]Send CCP message to id 1: CCP_MSG_QUIT from unit-1-1 to unit-3-1 for reason CLUSTER_QUIT_REASON_UN

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

انقسام الدماغ

الوحدة 1-1	الوحدة 2-1

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

Cluster GROUP1: On
    Interface mode: spanned

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

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

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

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

Unit "unit-1-1" in state PRIMARY

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

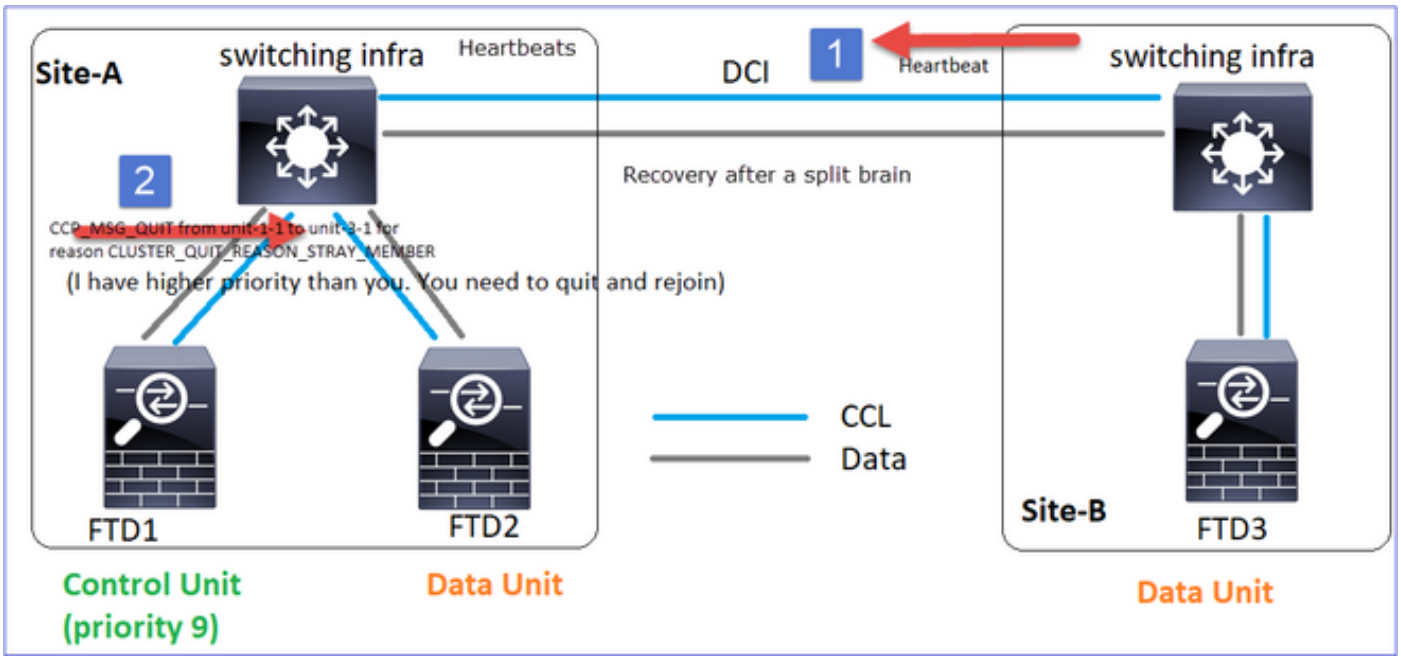
محفوظات نظام المجموعة

الوحدة 1-1	الوحدة 2-1	الوحدة 3-1
الدور الحالي	الدور الحالي	<#root> 09:38:16 UTC Nov 2 2020 **SECONDARY PRIMARY_POST_CONFIG Primary relinquis** 09:38:17 UTC Nov 2 2020 PRIMARY_POST_CONFIG Primary Primary post config d

إعادة اتصال CCL

تقوم الوحدة 1-1 باكتشاف عقدة التحكم الحالية، وبما أن الوحدة 1-1 لها أولوية أعلى ترسل إلى الوحدة 3-1 رسالة CLUSTER_QUIT_REASON_STRAY_MEMBER لتشغيل عملية انتخابية جديدة. وفي النهاية، تعود الوحدة 3-1 للربط كعقدة بيانات.

عند إعادة اتصال قسم مقسم بتقسيم نظير، تتم معالجة عقدة البيانات كعضو متداخل بواسطة عقدة التحكم المميزة ويستلم CCP QUIT msg مع سبب 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
```

تظهر كلتا الوحدتين (وحدة-1-1 ووحدة-3-1) في سجلات نظام المجموعة الخاصة بهما:

<#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
```

هناك أيضا syslog رسالة ولدت ل ال split-brain:

```
<#root>
firepower#
show log | include 747016

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

محفوظات نظام المجموعة

الوحدة 1-1	الوحدة 2-1	الوحدة 3-1
الوجود أحدث	الوجود أحدث	<#root> 09:47:33 UTC Nov 2 2020 **Primary DISABLED Detected a splitted cluster** 09:47:38 UTC Nov 2 2020 DISABLED ELECTION Enabled from CLI 09:47:38 UTC Nov 2 2020 ELECTION SECONDARY_COLD Received cluster control 09:47:38 UTC Nov 2 2020 SECONDARY_COLD SECONDARY_APP_SYNC Client progression d 09:48:18 UTC Nov 2 2020 SECONDARY_APP_SYNC SECONDARY_CONFIG SECONDARY applicatio 09:48:29 UTC Nov 2 2020 SECONDARY_CONFIG SECONDARY_FILESYS Configuration replic 09:48:30 UTC Nov 2 2020 SECONDARY_FILESYS SECONDARY_BULK_SYNC Client progression d 09:48:54 UTC Nov 2 2020 SECONDARY_BULK_SYNC **SECONDARY** Client progression done

السيناريو 2

فقدان الاتصال لمدة 3-4 ثانية تقريبا في كل الاتجاهين. CCL

قبل الفشل

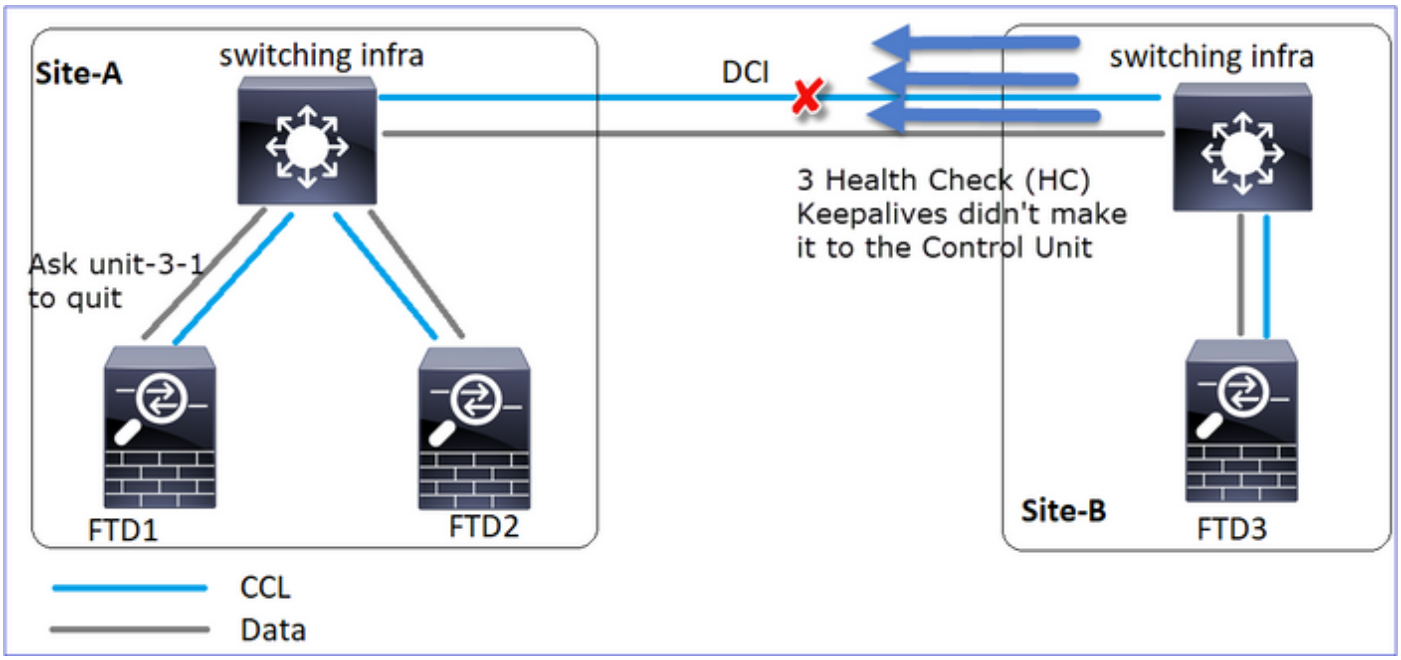
FTD1	FTD2	FTD3
سايت-أ	سايت-أ	سايت ب
عقدة التحكم	عقدة البيانات	عقدة البيانات

بعد الاستدراد (لا توجد تغييرات في أدوار الوحدات)

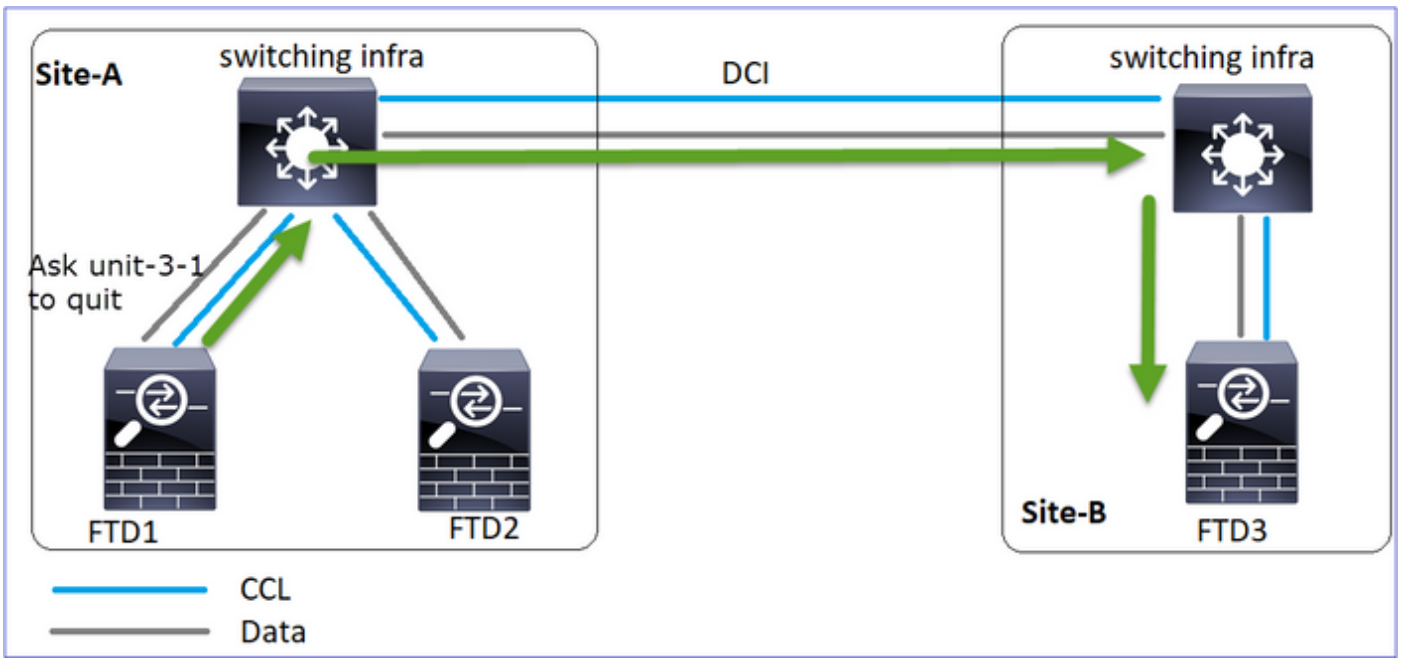
FTD1	FTD2	FTD3
سايت-أ	سايت-أ	سايت ب
عقدة التحكم	عقدة البيانات	عقدة البيانات

تحليل

الحدث الأول: تفقد عقدة التحكم 3 وحدات HC من الوحدة-3-1 وترسل رسالة إلى الوحدة-3-1 لمغادرة نظام المجموعة.



الحدث الثاني: تم إستردادقائمة التحكم في الوصول (CCL) بسرعة كبيرة، كما أن رسالة CLUSTER_QUIT_REASON_STRAY_MEMBER من عقدة التحكم قد وصلت إلى الجانب البعيد. الوحدة 3-1 تذهب مباشرة إلى الوضع المعطل والا يوجد انقسام الدماغ



على الوحدة 1-1 (المراقبة) ترون:

<#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

على الوحدة 3-1 (عقدة البيانات) ترى:

<#root>

```
firepower#
```

Cluster disable

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

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

يتم نقل وحدة نظام المجموعة -3-1 إلى حالة "معطل" وبمجرد إستعادة اتصال CCL، يتم إعادة ربطها كعقدة بيانات:

```
<#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
```

السيناريو 3

فقدان الاتصال لمدة 3-4 ثانية تقريبا في كل الاتجاهين. CCL

قبل الفشل.

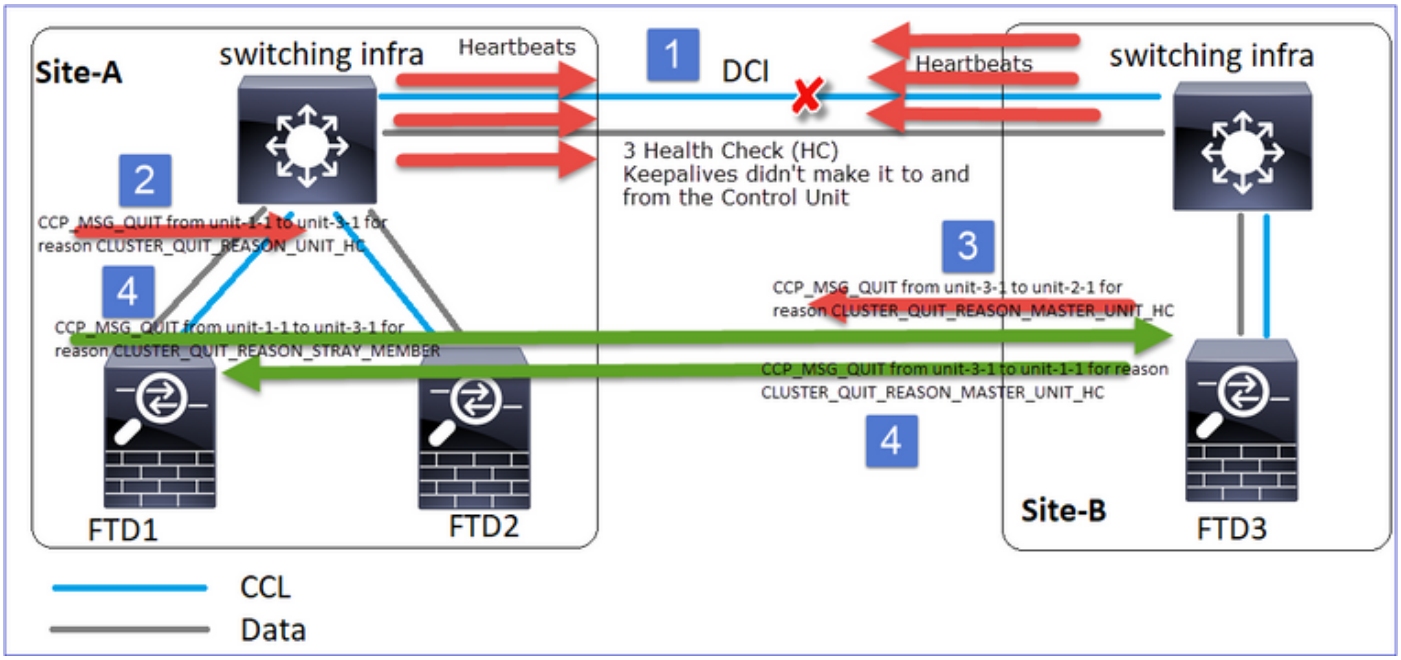
FTD1	FTD2	FTD3
سايت-أ	سايت-أ	سايت ب
عقدة التحكم	عقدة البيانات	عقدة البيانات

بعد الاستدراد (تم تغيير عقدة التحكم).

FTD1	FTD2	FTD3
سايت-أ	سايت-أ	سايت ب

عقدة البيانات	عقدة التحكم	عقدة البيانات

تحليل



1. قائمة التحكم في الوصول تنخفض.
2. لا تحصل الوحدة 1-1 على 3 رسائل HC من الوحدة-3-1 وترسل رسالة QUIT إلى الوحدة-3-1. لا تصل هذه الرسالة إلى الوحدة-3-1 أبدا.
3. ترسل الوحدة 3-1 رسالة QUIT إلى الوحدة 2-1. لا تصل هذه الرسالة أبدا إلى الوحدة 2-1.

أجهزة إسترداد قائمة التحكم في الوصول (CCL).

4. ترى Unit-1-1 أن Unit-3-1 أعلنت عن نفسها كعقدة تحكم وترسل رسالة QUIT_REASON_STRAY_MEMBER إلى Unit-3-1. بمجرد أن تحصل الوحدة-3-1 على هذه الرسالة تنتقل إلى دولة معطلة. وفي الوقت نفسه، ترسل الوحدة 3-1 رسالة QUIT_REASON_PRIMARY_UNIT_HC إلى الوحدة-1-1 وتطلب منها إنهاء العمل. ما إن يحصل وحدة-1-1 على هذا رسالة يذهب إلى دولة معأق.

محفوظات نظام المجموعة

الوحدة 1-1
<#root> 19:53:09 UTC Nov 2 2020 **PRIMARY DISABLED** Received control message DISABLE (primary unit health check failure) 19:53:13 UTC Nov 2 2020

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

      SECONDARY

           Client progression done
```

السيناريو 4

فقدان الاتصال لمدة تتراوح من 3 إلى 4 ثانية تقريبا CCL

قبل الفشل

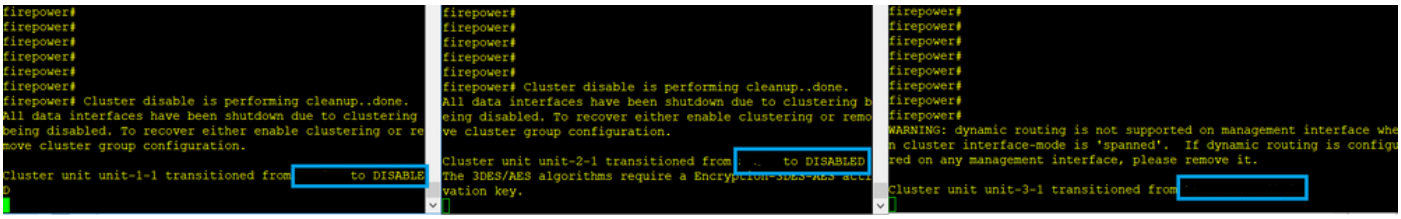
FTD1	FTD2	FTD3
أ-ساي	أ-ساي	ساي ب
عقدة التحكم	عقدة البيانات	عقدة البيانات

بعد الاسترداد (قام عقدة التحكم بتغيير المواقع)

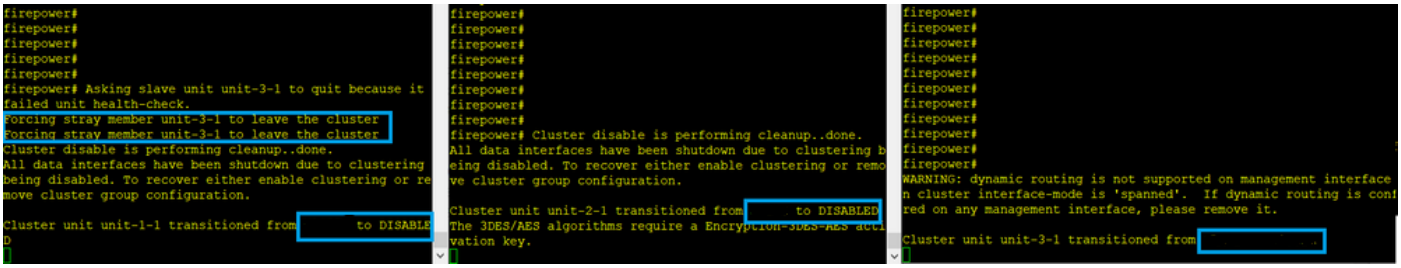
FTD1	FTD2	FTD3
سايت-أ	سايت-أ	سايت ب
عقدة البيانات	عقدة البيانات	عقدة التحكم

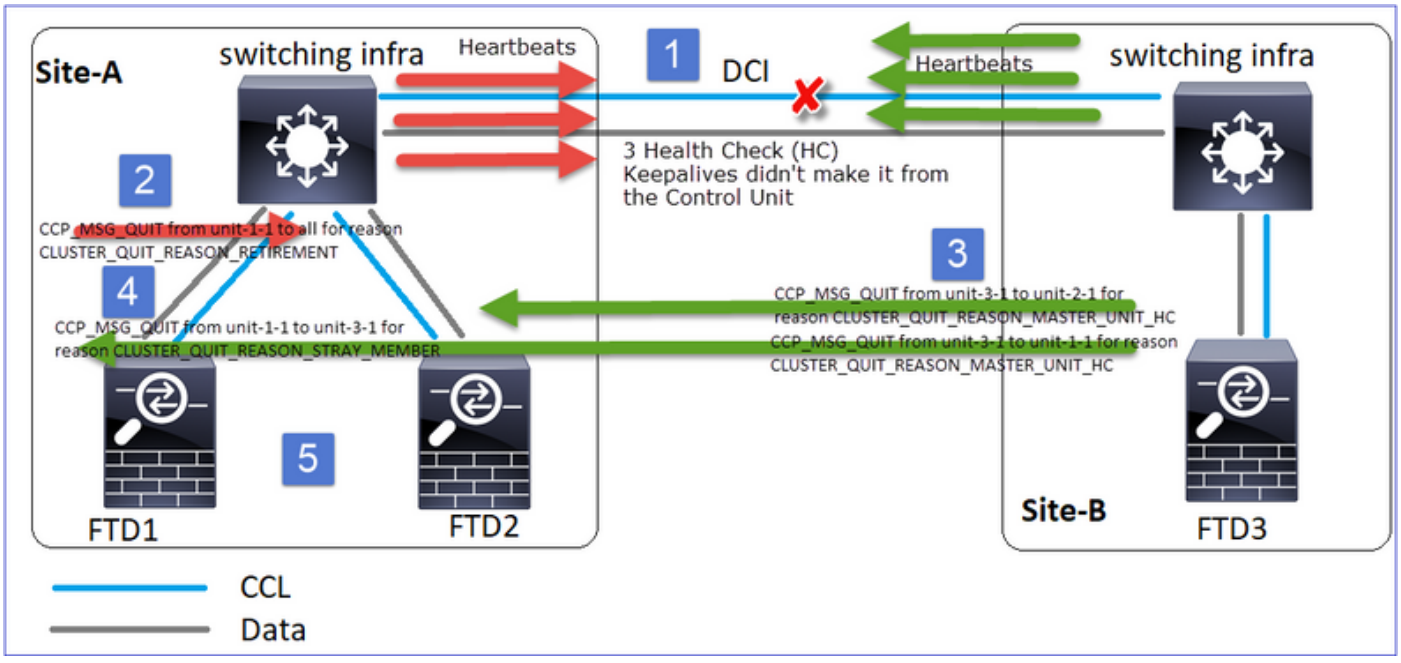
تحليل

الفشل



نكهة مختلفة لنفس الفشل. في هذه الحالة، الوحدة-1-1 أيضا لم تحصل على 3 رسائل HC من الوحدة-3-1، وبمجرد أن حصلت على منصة جديدة، حاولت طرد الوحدة-3-1 باستخدام رسالة مضللة، ولكن الرسالة لم تصل إلى الوحدة-3-1:

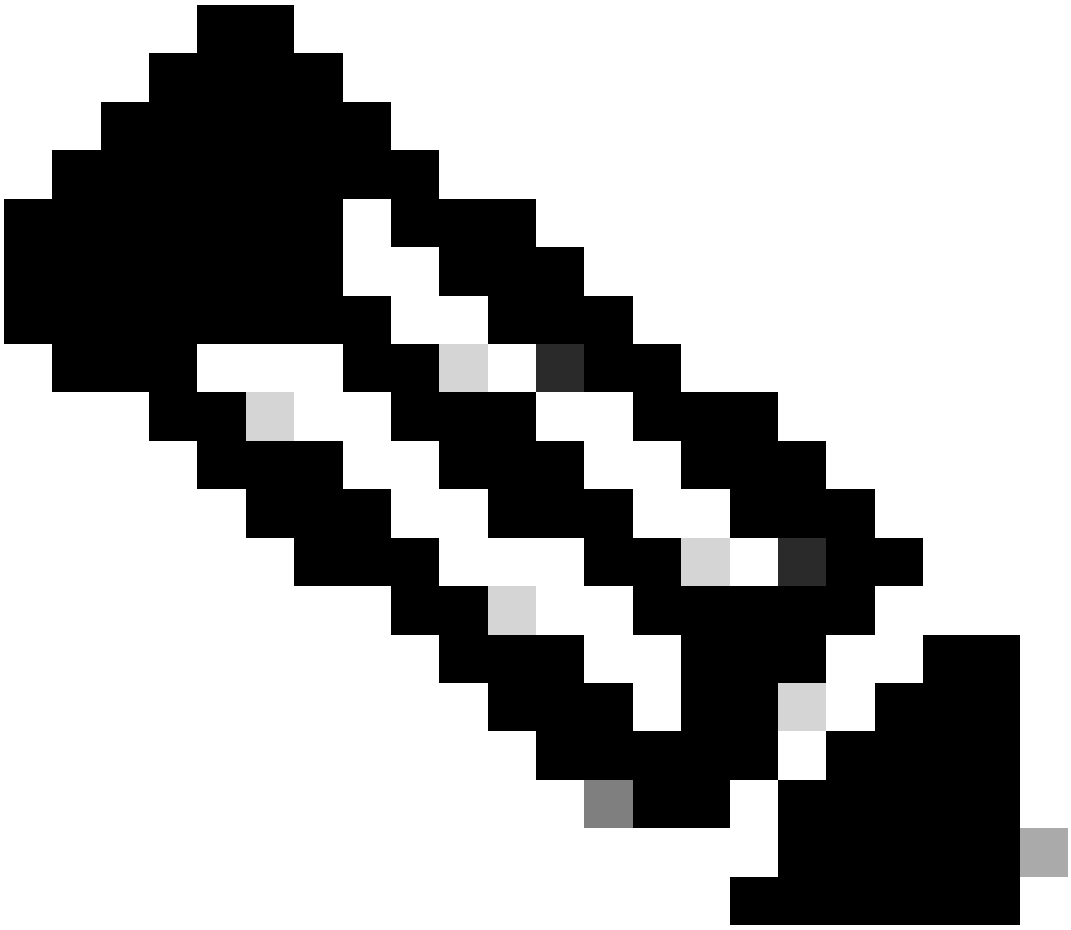




1. يصبح CCL أحادي الإتجاه لبضع ثوان. لا تتلقى الوحدة 3-1 3 رسائل HC من الوحدة-1-1

وتصبح عقدة تحكم.

2. تقوم Unit-2-1 بإرسال رسالة CLUSTER_QUIT_REASON_RETIREMENT (ثابت).
3. ترسل UNIT-3-1 رسالة QUIT_REASON_PRIMARY_UNIT_HC إلى UNIT-2-1. تستلمها Unit-2-1 وتغادر المجموعة.
4. ترسل UNIT-3-1 رسالة QUIT_REASON_PRIMARY_UNIT_HC إلى UNIT-1-1. تستلمها Unit-1-1 وتغادر المجموعة. أجهزة إستردادقائمة التحكم في الوصول (CCL).
5. تقوم الوحدات 1-1 و 2-1 بإعادة مضاهاة المجموعة كعقد بيانات.



ملاحظة: إن السيترد الـ CCL في خطوة 5، بعد ذلك في موقع a الـ FTD1 يصبح الجديد تحكم عقدة، وبعد الـ CCL إستعادة، هو يفوز الـ انتخاب جديد.

رسائل Syslog على الوحدة-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
```

سجلات تتبع نظام المجموعة على الوحدة 1-1:

<#root>

firepower#

show cluster info trace | include QUIT

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

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

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

رسائل Syslog على الوحدة-3-1:

<#root>

firepower#

show log | include 747

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

State machine changed from state SECONDARY to PRIMARY

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

State machine is at state PRIMARY

محفوظات نظام المجموعة

الوحدة 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

السيناريو 5

قبل الفشل

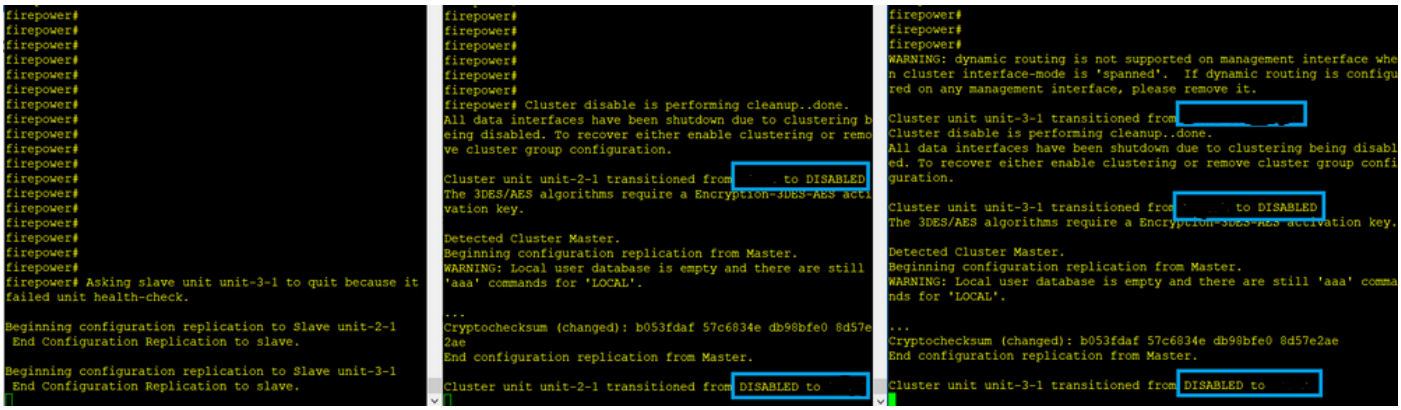
FTD1	FTD2	FTD3

سايت ب	سايت-أ	سايت-أ
عقدة البيانات	عقدة البيانات	عقدة التحكم

بعد الاستيراد (لا تغييرات)

FTD3	FTD2	FTD1
سايت ب	سايت-أ	سايت-أ
عقدة البيانات	عقدة البيانات	عقدة التحكم

الفشل



أرسلت الوحدة-3-1 رسائل QUIT إلى كل من الوحدة-1-1 والوحدة-2-1، لكن بسبب مشكل الاتصال لم يستلم رسالة QUIT إلا الوحدة-2-1.

سجلات تتبع نظام المجموعة للوحدة 1-1:

<#root>

firepower#

show cluster info trace | include QUIT

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

سجلات تتبع نظام المجموعة للوحدة 2-1:

<#root>

firepower#

show cluster info trace | include QUIT

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

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

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

محفوظات نظام المجموعة

الوحدة 1-1	الوحدة 2-1
الوجود الأخير	<#root> 00:51:50 UTC Nov 4 2020 **SECONDARY DISABLED Received control message DISABLE (primary unit health check failure)** 00:51:54 UTC Nov 4 2020 DISABLED ELECTION Enabled from CLI 00:51:54 UTC Nov 4 2020 ELECTION SECONDARY_COLD Received cluster control 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 configur sync done 00:52:54 UTC Nov 4 2020 SECONDARY_CONFIG SECONDARY_FILESYS Configuration replication fini 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

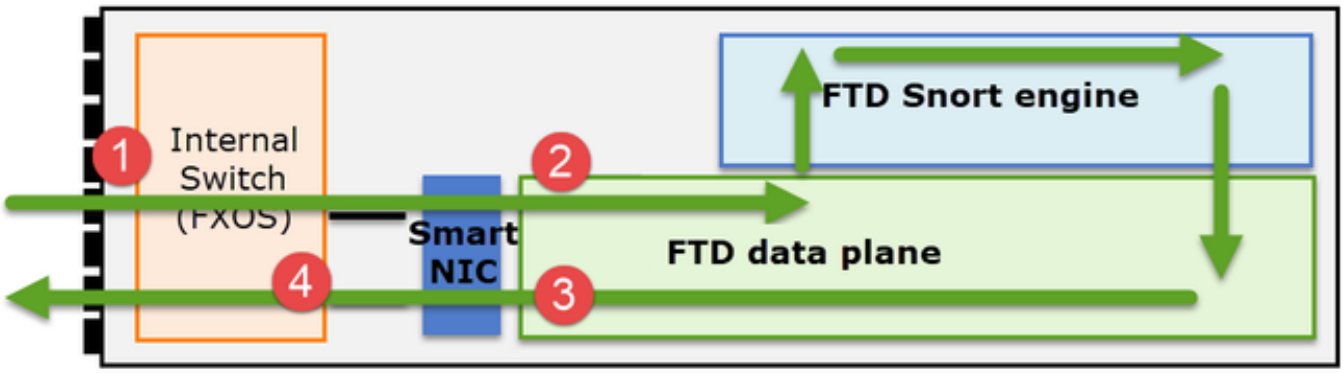
إنشاء اتصال مستوى بيانات المجموعة

نقاط التقاط NGFW

يوفر جدار الحماية من الجيل التالي إمكانيات التقاط على هذه النقاط:

- المحول الداخلي للهيكل (FXOS)
- محرك مستوى البيانات FTD
- محرك شخير FTD

عندما تقوم باستكشاف أخطاء مسار البيانات وإصلاحها على نظام مجموعة، فإن نقاط الالتقاط المستخدمة في معظم الحالات هي FXOS ومحرك مستوى البيانات FTD.



1. التقاط مدخل FXOS على الواجهة المادية
2. التقاط مدخل FTD في محرك مستوى البيانات
3. التقاط مخرج FTD في محرك مستوى البيانات
4. التقاط مدخل FXOS على واجهة اللوحة الخلفية

للحصول على تفاصيل إضافية حول التقاط NGFW، تحقق من هذا المستند:

أساسيات أدوار تدفق وحدة نظام المجموعة

يمكن إنشاء الاتصالات من خلال نظام المجموعة بطرق متعددة تعتمد على عوامل مثل:

- نوع حركة المرور (TCP، UDP، وما إلى ذلك)
- خوارزمية موازنة التحميل التي تم تكوينها على المحول المجاور
- المميزات التي تم تكوينها على جدار الحماية
- شروط الشبكة (على سبيل المثال، تجزئة IP، تأخيرات الشبكة، وما إلى ذلك)

دور التدفق	الوصف	عالمة (عالمات)

مالك	عادة، الوحدة التي تتلقى الاتصال في البداية	وأو
مخرج	الوحدة التي تتعامل مع طلبات البحث عن المالك من العملاء.	Y
مالك النسخة الاحتياطية	وطالما أن المدير ليس نفس الوحدة التي يستخدمها المالك، فإن المدير هو أيضا مالك النسخة الاحتياطية. إذا اختار المالك نفسه كمدير، فسيتم إختيار مالك منفصل للنسخ الاحتياطي.	Y (إذا كان المدير هو مالك النسخة الاحتياطية أيضا) y (إذا لم يكن المدير مالك النسخة الاحتياطية)
مرسل	وحدة تقوم بإعادة توجيه الحزم إلى المالك	z
مالك الجزء	الوحدة التي تتعامل مع حركة المرور المجزأة	-
النسخ الاحتياطي للهيكل	في نظام مجموعة مشترك بين الهياكل عندما يتم تملك تدفقات كل من المدير/النسخ الاحتياطي ومالك الهيكل بوحدات تابعة للهيكل نفسه، تصبح الوحدة الموجودة في أحد الهياكل الأخرى وحدة نسخ إحتياطي/إخراج ثانوية. هذا الدور خاص بالمجموعات بين الهياكل لسلسلة Firepower 9300 التي تحتوي على أكثر من خادم نصلي واحد.	w

- لمزيد من التفاصيل، راجع القسم المرتبط في دليل التكوين (راجع الروابط في الموضوعات ذات الصلة)
- في سيناريوهات محددة (راجع قسم دراسات الحالات) التي يتم عرض بعض العلامات دائما..

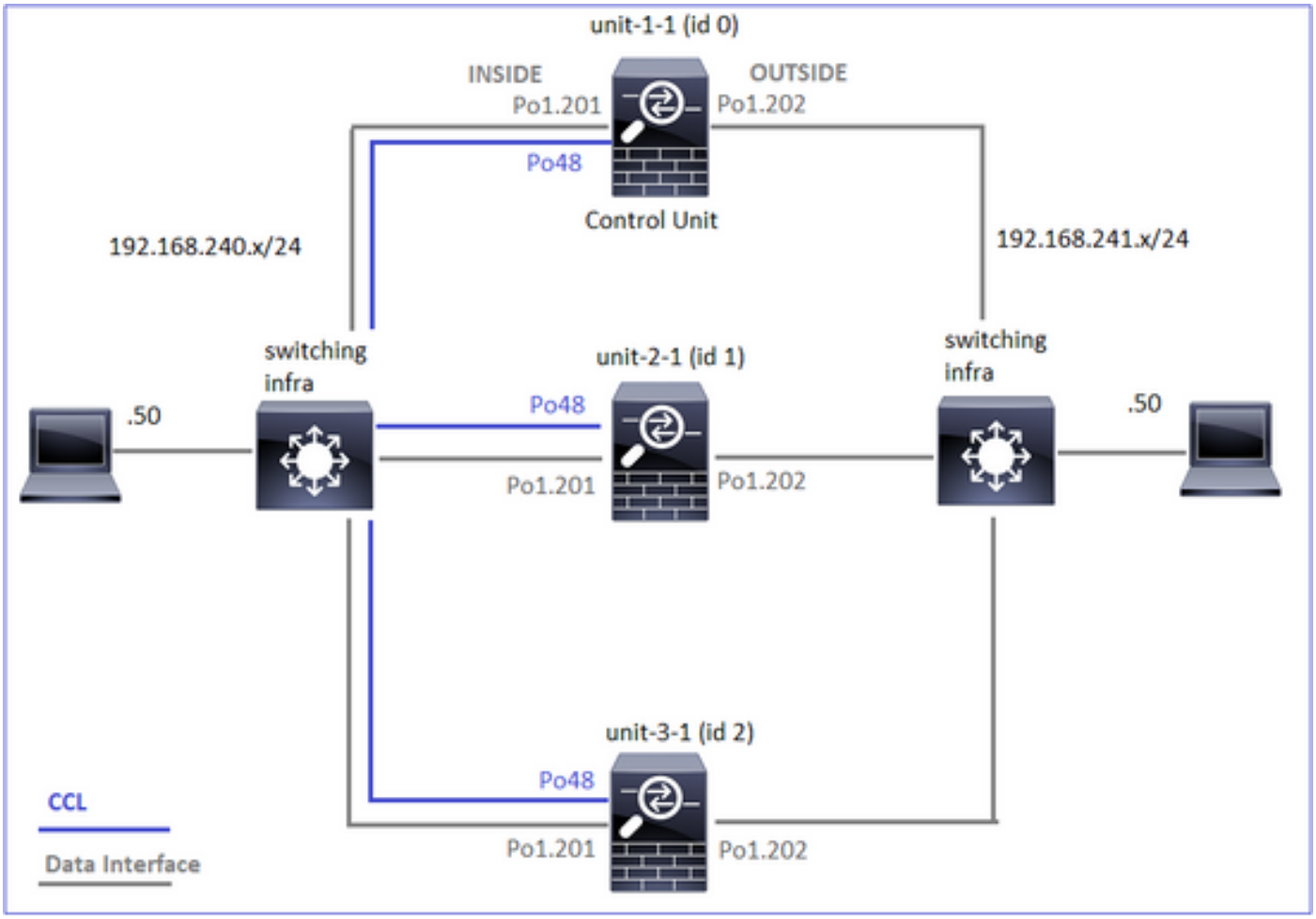
دراسات حالات مؤسسة اتصال المجموعة

ويغطي الفرع التالي دراسات حالات مختلفة تبين بعض الطرق التي يمكن بها إقامة اتصال من خلال مجموعة. وتتمثل الأهداف فيما يلي:

- إطلاع على أدوار الوحدات المختلفة.

- إستعرض كيف يمكن ربط مخرجات الأوامر المختلفة.

المخطط



وحدات نظام المجموعة والمعرفات:

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

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

تم تمكين التقاط نظام المجموعة:

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

ملاحظة: تم إجراء هذه الاختبارات في بيئة معملية مع الحد الأدنى من حركة المرور عبر نظام المجموعة. في الإنتاج، حاول أن يستعمل كمرشح التقاط خاص بقدر الإمكان (على سبيل المثال، غاية ميناء وكلما أمكن مصدر ميناء) أن يقلل "التشويش" في التقاطات.

دراسة الحالة 1. حركة المرور المتماثلة (المالك وه أيضا المدير)

الملاحظة 1. يظهر التقاط الداخلي حزم فقط على وحدة-1-1. هذا يعني أن التدفق في كل الاتجاهين مر عبر وحدة-1-1 (حركة مرور متماثلة):

<#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
```

الملاحظة 2 - تحليل عالمة الوصلة للتدفق بمنفذ المصدر 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

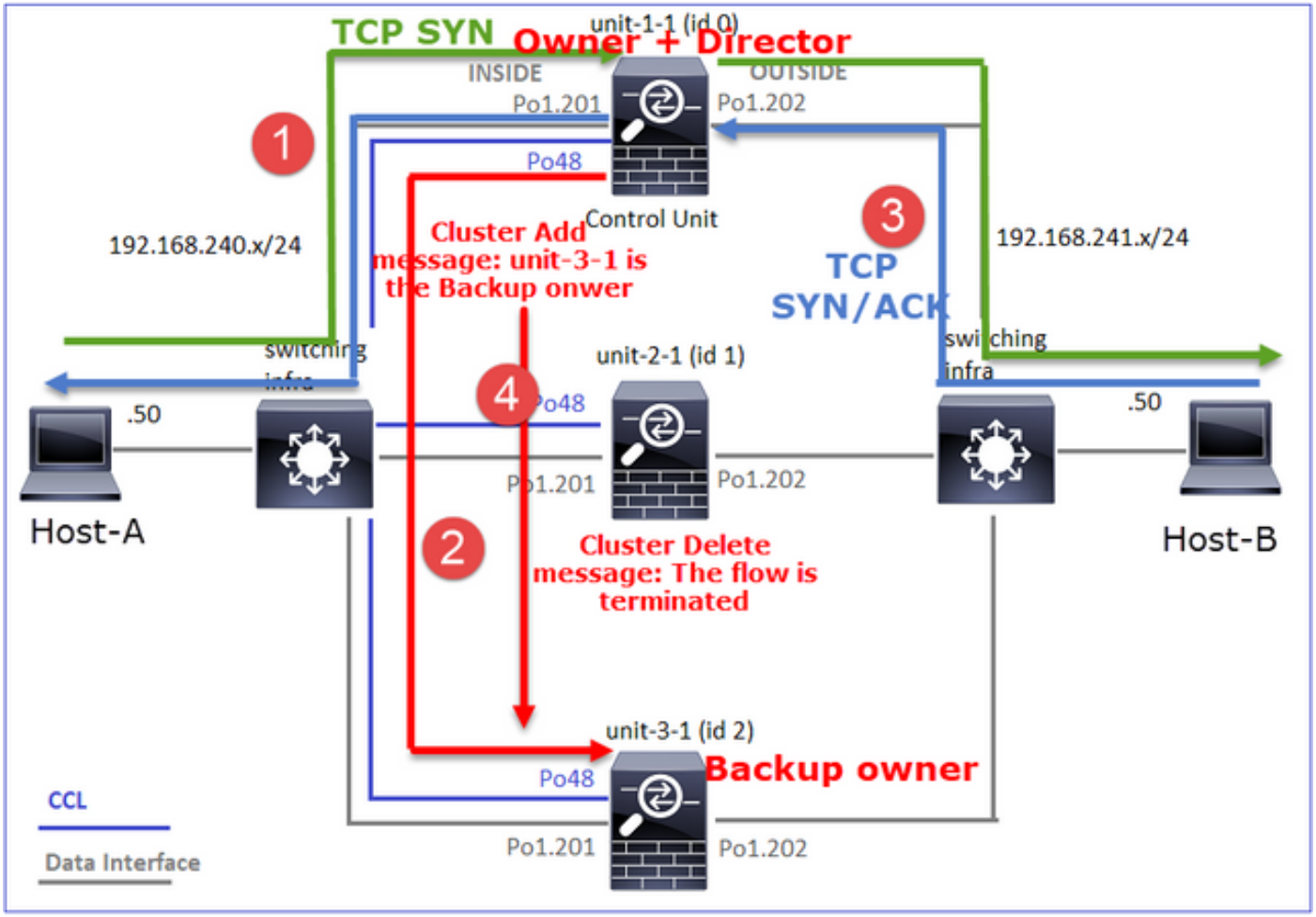
```
, idle 0:00:06, bytes 0,
```

flags y

وحدة	راية	ةظحالم
الوحدة 1-1	ويوأ	· مالك التدفق - تتولى الوحدة التدفق · المدير - نظرا لأن الوحدة 3-1 لها "ص" وليس "ص" فإن هذا يعني أن الوحدة 1-1 قد تم إختياراها كمدير لهذا التدفق. وهكذا، بما انه

		المالك أيضا، انتخبت وحدة أخرى (الوحدة 3-1 في هذه الحالة) كمالك إحتياطي
الوحدة 2-1	-	-
الوحدة 3-1	Y	الوحدة هي مالك للنسخ الاحتياطي

ويمكن تمثيل ذلك على النحو التالي:



1. تصل حزمة نظام TCP من المضيف-A إلى الوحدة-1-1. تصبح الوحدة-1-1 مالك التدفق.
2. كما يتم انتخاب الوحدة 1-1 كمدير للتدفق. ومن ثم، فإنه ينتخب أيضا الوحدة 3-1 كمالك للنسخ الاحتياطي (رسالة إضافة نظام المجموعة).
3. تصل حزمة TCP SYN/ACK من المضيف-B إلى الوحدة-3-1. التدفق متماثل.
4. بمجرد إنهاء الاتصال، يرسل المالك رسالة حذف نظام مجموعة لإزالة معلومات التدفق من مالك النسخة الاحتياطية.

الملاحظة 3 - الالتقاط تتبع يبين أن الاتجاهين لا يتجاوزان إلا من خلال الوحدة 1-1.

الخطوة 1. تحديد التدفق والحزم ذات الأهمية في جميع وحدات نظام المجموعة استنادا إلى منفذ المصدر:

```
<#root>

firepower#

cluster exec show capture CAPI | i 45954


unit-1-1(LOCAL):*******************************************************
1: 08:42:09.362697 802.1Q vlan#201 P0 192.168.240.50.45954 > 192.168.241.50.80: S 992089269:992089269(0)
2: 08:42:09.363521 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.45954: S 4042762409:4042762409
3: 08:42:09.363827 802.1Q vlan#201 P0 192.168.240.50.45954 > 192.168.241.50.80: . ack 4042762410 win 22
…
unit-2-1:*******************************************************

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

```
<#root>

firepower#

cluster exec show capture CAPO | i 45954


unit-1-1(LOCAL):*******************************************************
1: 08:42:09.362987 802.1Q vlan#202 P0 192.168.240.50.45954 > 192.168.241.50.80: S 2732339016:2732339016
2: 08:42:09.363415 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.45954: S 3603655982:3603655982
3: 08:42:09.363903 802.1Q vlan#202 P0 192.168.240.50.45954 > 192.168.241.50.80: . ack 3603655983 win 22
…
unit-2-1:*******************************************************

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

الخطوة 2. نظرا لأن هذا هو تدفق TCP، فإنها تتبع حزم المصافحة ثلاثية الإتجاه. وكما يمكننا أن نرى في هذا المخرج، فإن الوحدة 1-1 هي المالك. من أجل التبسيط، يتم حذف مراحل التتبع غير ذات الصلة:

```
<#root>

firepower#

show cap CAPI packet-number 1 trace


25985 packets captured
1: 08:42:09.362697 802.1Q vlan#201 P0 192.168.240.50.

45954

 > 192.168.241.50.80:

S

 992089269:992089269(0) win 29200 <mss 1460,sackOK,timestamp 495153655 0,nop,wscale 7>
...
Phase: 4
```

Type: CLUSTER-EVENT

Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'

Flow type: NO FLOW

I (0) got initial, attempting ownership.

Phase: 5

Type: CLUSTER-EVENT

Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW

I (0) am becoming owner

...

حركة مرور الإرجاع (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

الملاحظة 4. توضح نظم مستوى بيانات FTD إنشاء الاتصال وإنهائه على جميع الوحدات:

<#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

دراسة الحالة 2. حركة المرور المتماثلة (المالك مختلف عن المدير)

- مثل دراسة الحالة رقم 1، لكن في دراسة الحالة هذه، مالك التدفق هو وحدة مختلفة عن المدير.
- جميع المخرجات مشابهة لدراسة الحالة رقم 1. الفرق الرئيسي بالمقارنة مع دراسة

الحالة رقم 1 هو علم "Y" الذي يستبدل علم "Y" في السيناريو 1.

الملاحظة 1 - المالك مختلف عن المدير.

تحليل عالمة الاتصال للتدفق باستخدام منفذ المصدر 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:

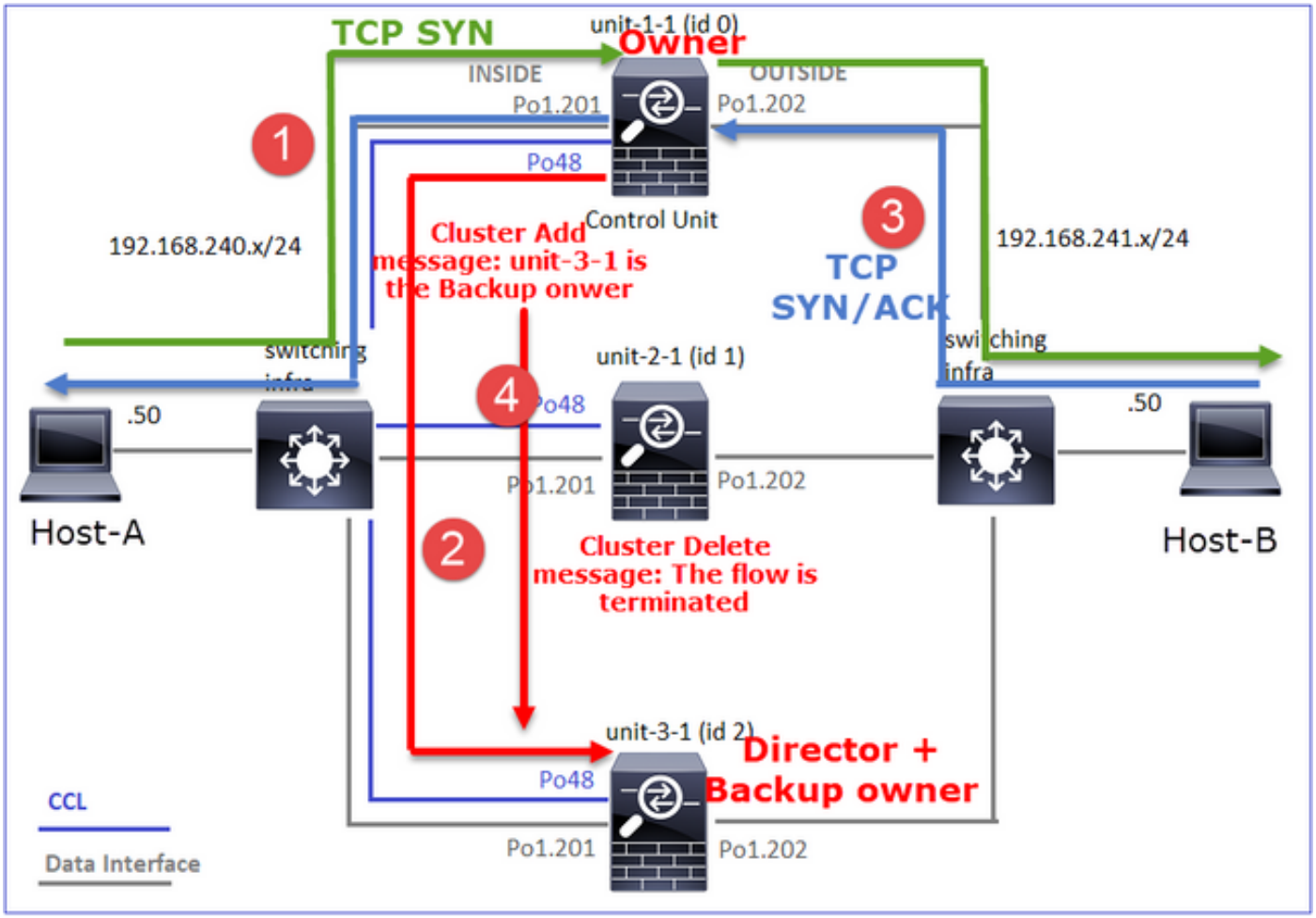
46278

, idle 0:00:06, bytes 0,

flags Y

وحدة	راية	ملاحظة
الوحدة 1-1	أوي	· مالك التدفق - تتولى الوحدة التدفق
الوحدة 2-1	-	-
الوحدة 3-1	Y	· مدير ومالك وحدة النسخ الاحتياطي - تحمل الوحدة 3-1 العلامة ص (مدير).

ويمكن تمثيل ذلك على النحو التالي:



1. تصل حزمة نظام TCP من المضيف-A إلى الوحدة-1-1. تصبح الوحدة-1-1 مالك التدفق.
2. يتم إختيار الوحدة 3-1 كمدير التدفق. Unit-3-1 أيضا مالك النسخة الاحتياطية ('رسالة إضافة نظام المجموعة على UDP 4193 عبر CCL).
3. تصل حزمة TCP SYN/ACK من المضيف-B إلى الوحدة-3-1. التدفق متماثل.
4. بمجرد إنهاء الاتصال، يرسل المالك عبر قناة التحكم في الوصول (CCL) رسالة "حذف نظام المجموعة" على UDP 4193 لإزالة معلومات التدفق من مالك النسخة الاحتياطية.

الملاحظة 2 - الالتقاط بالتتبع يظهر أن الاتجاهين لا يتجهان إلا من خلال الوحدة 1-1

الخطوة 1. أستخدم النهج نفسه كما في دراسة الحالة 1 لتحديد التدفق والحزم ذات الاهتمام في جميع وحدات المجموعة استنادا إلى منفذ المصدر:

<#root>

firepower#

cluster exec show cap CAPI | include 46278

unit-1-1

(LOCAL):**********
3: 11:01:44.841631 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80:

S

 1972783998:1972783998(0) win 29200 <mss 1460,sackOK,timestamp 503529072 0,nop,wscale 7>
4: 11:01:44.842317 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.46278:

S

 3524167695:3524167695(0)

ack

 1972783999 win 28960 <mss 1380,sackOK,timestamp 513884542 503529072,nop,wscale 7>
5: 11:01:44.842592 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80: . ack 3524167696 win 22
…
unit-2-1:**********

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

التقاط على الواجهة الخارجية:

<#root>

firepower#

cluster exec show cap CAPO | include 46278

unit-1-1

(LOCAL):**********
3: 11:01:44.841921 802.1Q vlan#202 P0 192.168.240.50.46278 > 192.168.241.50.80:

S

 2153055699:2153055699(0) win 29200 <mss 1380,sackOK,timestamp 503529072 0,nop,wscale 7>
4: 11:01:44.842226 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46278:

S

 3382481337:3382481337(0)

ack

```
 2153055700 win 28960 <mss 1460,sackOK,timestamp 513884542 503529072,nop,wscale 7>
5: 11:01:44.842638 802.1Q vlan#202 P0 192.168.240.50.46278 > 192.168.241.50.80: . ack 3382481338 win 22
```

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

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

الخطوة 2. ركز على حزم الدخول (TCP SYN و TCP syn/ACK):

<#root>

```
firepower#
```

cluster exec show cap CAPI packet-number 3 trace

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

```
824 packets captured
```

```
3: 11:01:44.841631 802.1Q vlan#201 P0 192.168.240.50.46278 > 192.168.241.50.80:
```

S

```
 1972783998:1972783998(0) win 29200 <mss 1460,sackOK,timestamp 503529072 0,nop,wscale 7>
…
```

```
Phase: 4
```

Type: CLUSTER-EVENT

```
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: NO FLOW
```

I (0) got initial, attempting ownership.

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

I (0) am becoming owner

تتبع SYN/ACK على الوحدة 1-1:

```
<#root>

firepower#

cluster exec show cap CAPO packet-number 4 trace


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

4: 11:01:44.842226 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.

46278

:

S

 3382481337:3382481337(0)

ack

 2153055700 win 28960 <mss 1460,sackOK,timestamp 513884542 503529072,nop,wscale 7>
Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:


Found flow with id 9583, using existing flow
```

الملاحظة 3. تظهر مخططات مستوى بيانات FTD إنشاء الاتصال وإنهائه على المالك ومالك النسخة الاحتياطية:

```
<#root>

firepower#

cluster exec show log | include 46278


unit-1-1(LOCAL):*******************************************************
Dec 01 2020 11:01:44: %FTD-6-302013:

Built inbound TCP connection

 9583 for INSIDE:192.168.240.50/46278 (192.168.240.50/46278) to OUTSIDE:192.168.241.50/80 (192.168.241.
Dec 01 2020 11:01:53: %FTD-6-302014:

Teardown TCP connection

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

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

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

```
Dec 01 2020 11:01:44: %FTD-6-302022:

Built director stub TCP connection

 for INSIDE:192.168.240.50/46278 (192.168.240.50/46278) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80)
Dec 01 2020 11:01:53: %FTD-6-302023:

Teardown director TCP connection

 for INSIDE:192.168.240.50/46278 to OUTSIDE:192.168.241.50/80 duration 0:00:08 forwarded bytes 0 Cluste
```

دراسة الحالة الإفرادية 3 - حركة المرور غير المتماثلة (يقوم المدير بإعادة توجيه حركة المرور).

الملاحظة 1. يظهر إلتقاط إخفاء حقن حزم على الوحدة 1-1 و الوحدة 2-1 (التدفق غير المتماثل):

```
<#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
```

الملاحظة 2. تحليل عالمة الوصلة للتدفق بمنفذ المصدر 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,
```

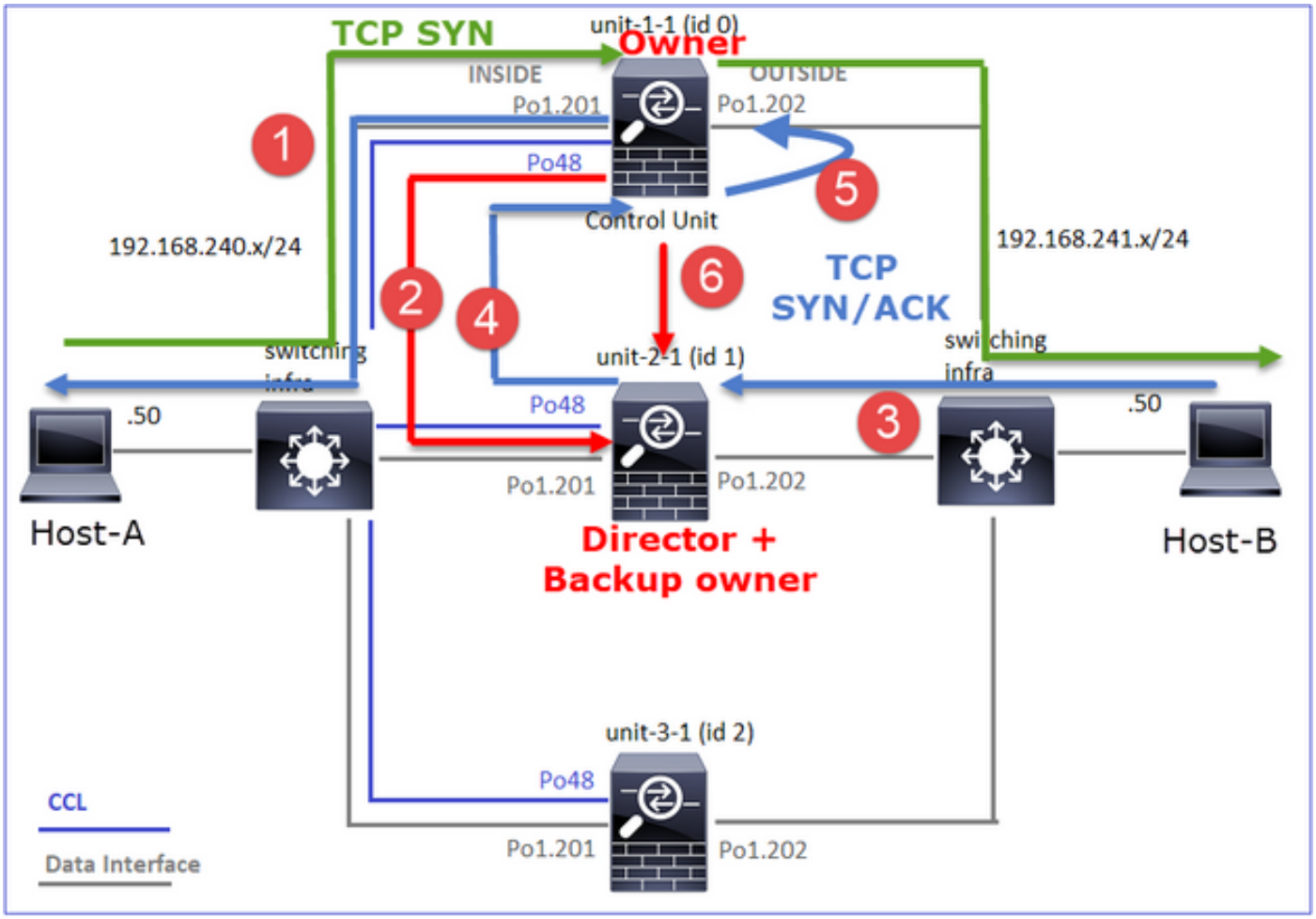
flags Y

```
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
```

وحدة	راية	ةظحالم
الوحدة 1-1	وياً	· مالك التدفق - تتولى الوحدة التدفق.
الوحدة 2-1	Y	· المدير - بما أن الوحدة 2-1 تحمل علامة "Y" فإن ذلك يعني أن الوحدة 2-1 قد تم إختياراها كمدير لهذا التدفق. · مالك النسخ الاحتياطي · أخيراً، وعلى الرغم من أنه ليس واضحاً من هذا الناتج، فمن الخلل الإظهار وإظهار السجل، من الواضح أن الوحدة 2 - 1 تعيد توجيه هذه التدفق إلى المالك (على الرغم من أنه لا يعتبر من الناحية الفنية مصدر شحن في هذا السيناريو). ملاحظة: لا يمكن أن تكون الوحدة الكل من المدير (Y flow) والمرسل (z flow)، وهذان الدوران لا يجتمعان. لا يزال بإمكان المدراء (التدفق Y) إعادة توجيه حركة المرور. راجع إخراج show log لاحقا في دراسة هذه الحالة.

الوحدة 3-1	-	-

ويمكن تمثيل ذلك على النحو التالي:



1. تصل حزمة نظام TCP من المضيف-A إلى الوحدة-1-1. تصبح الوحدة-1-1 مالك التدفق.
2. يتم إختيار الوحدة 2-1 كمدير للتدفق ومالك للنسخ الاحتياطي. يرسل مالك التدفق رسالة "إضافة نظام المجموعة" للبث الأحادي على UDP 4193 لإعلام مالك النسخ الاحتياطي بالتدفق.
3. تصل حزمة TCP SYN/ACK من المضيف-B إلى الوحدة-2-1. التدفق غير المتماثل.
4. تقوم الوحدة 2-1 بإعادة توجيه الحزمة من خلال CCL إلى المالك (بسبب ملف تعريف إرتباط TCP SYN).
5. يقوم المالك بإعادة إدخال الحزمة على الواجهة الخارجية ثم إعادة توجيه الحزمة نحو المضيف-A.
6. بمجرد إنهاء الاتصال، يرسل المالك رسالة حذف نظام مجموعة لإزالة معلومات التدفق من مالك النسخة الاحتياطية.

الملاحظة 3 - يظهر التسجيل بالتتبع حركة المرور غير المتماثلة وإعادة التوجيه من الوحدة 2-1 إلى الوحدة 1-1.

الخطوة 1. حدد الحزم التي تنتمي إلى تدفق الفائدة (المنفذ 46502):

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


unit-1-1(LOCAL):*******************************************************
3: 12:58:33.356121 802.1Q vlan#201 P0 192.168.240.50.46502 > 192.168.241.50.80: S 4124514680:4124514680
4: 12:58:33.357037 802.1Q vlan#201 P0 192.168.241.50.80 > 192.168.240.50.46502: S 883000451:883000451(0)
5: 12:58:33.357357 802.1Q vlan#201 P0 192.168.240.50.46502 > 192.168.241.50.80: . ack 883000452 win 229
unit-2-1:*************************************************************

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

إتجاه الإرجاع:

```
<#root>
firepower#
cluster exec show capture CAPO | include 46502


unit-1-1(LOCAL):*******************************************************
3: 12:58:33.356426 802.1Q vlan#202 P0 192.168.240.50.46502 > 192.168.241.50.80: S 1434968587:1434968587
4: 12:58:33.356915 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: S 4257314722:4257314722
5: 12:58:33.357403 802.1Q vlan#202 P0 192.168.240.50.46502 > 192.168.241.50.80: . ack 4257314723 win 22

unit-2-1:*************************************************************
1: 12:58:33.359249 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: S 4257314722:4257314722
2: 12:58:33.360302 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: . ack 1434968736 win 23
3: 12:58:33.361004 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.46502: . 4257314723:4257316091
…

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

الخطوة 2. تتبع الحزم. بشكل افتراضي، يتم تتبع أول 50 حزمة مدخل فقط. وللتبسيط، يتم حذف حزم التتبع غير ذات الصلة.

الوحدة 1-1 (المالك):

```
<#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
```

الوحدة 2-1 (مرسل)

حركة مرور الإرجاع (TCP syn/ACK). وحدة الفائدة هي UNIT-2-1 والتي هي المدير/مالك النسخة الاحتياطية وتوقوم بإعادة توجيه حركة المرور إلى المالك:

<#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).
```

الملاحظة 4. توضح نظم مستوى بيانات FTD إنشاء الاتصال وإنهائه على جميع الوحدات:

```
<#root>

firepower#

cluster exec show log | i 46502


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

B

uilt inbound TCP connection

 9742 for INSIDE:192.168.240.50/46502 (192.168.240.50/46502) to OUTSIDE:192.168.241.50/80 (192.168.241.
Dec 01 2020 12:59:02: %FTD-6-302014:

Teardown TCP connection

 9742 for INSIDE:192.168.240.50/46502 to OUTSIDE:192.168.241.50/80 duration 0:00:28 bytes 2048000440 TC

unit-2-1:*******************************************************************
Dec 01 2020 12:58:33: %FTD-6-302022:

Built forwarder stub TCP connection

 for OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46502 (192.168.240.50/4650
Dec 01 2020 12:58:33: %FTD-6-302023:

Teardown forwarder TCP connection

 for OUTSIDE:192.168.241.50/80 to unknown:192.168.240.50/46502 duration 0:00:00 forwarded bytes 0 Forwa
Dec 01 2020 12:58:33: %FTD-6-302022:

Built director stub TCP connection

 for INSIDE:192.168.240.50/46502 (192.168.240.50/46502) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80
Dec 01 2020 12:59:02: %FTD-6-302023:

Teardown director TCP connection

 for INSIDE:192.168.240.50/46502 to OUTSIDE:192.168.241.50/80 duration 0:00:28 forwarded bytes 20483163

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

دراسة الحالة الإفرادية 4 - حركة المرور غير المتماثلة (المالك وه المدير)

الملاحظة 1. يظهر إلتقاط إخفاء حقن حزم على الوحدة 1-1 و الوحدة 2-1 (التدفق غير المتماثل):

<#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
```

الملاحظة 2- تحليل عالمة الوصلة للتدفق بمنفذ المصدر 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:

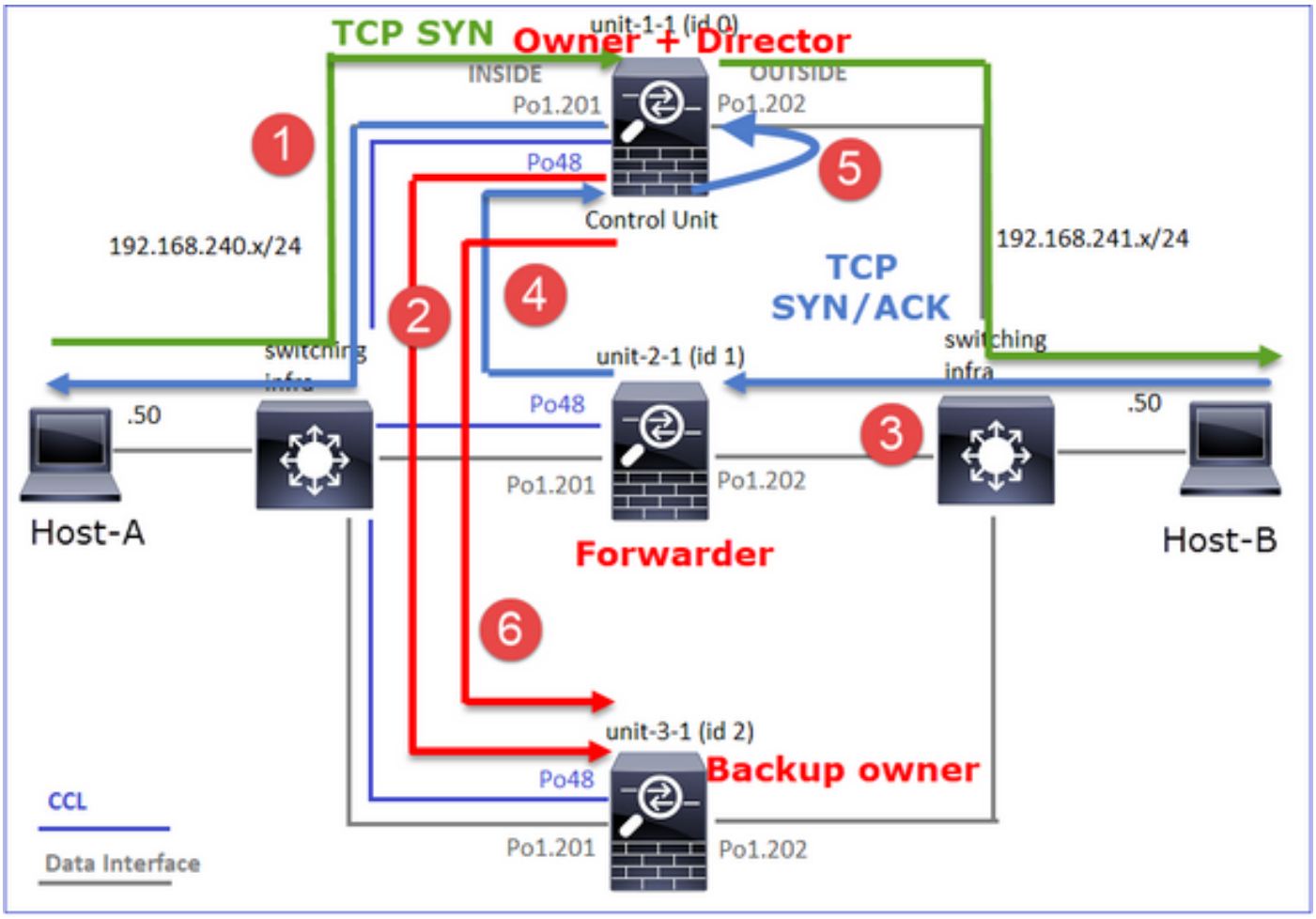
46916

, idle 0:00:04, bytes 0,

flags y

وحدة	راية	ةظحالم
الوحدة 1-1	وأوي	· مالك التدفق - تتولى الوحدة التدفق · المدير - نظر لأن الوحدة 3-1 لها "ص" ولي س "ص" فإن هذا يعني أن الوحدة 1-1 قد تم إختياره كمدير لهذا التدفق. وهكذا، بما أن المالك الأصلي، انتخبت وحدة أخرى (الوحدة 3-1 في هذه الحالة) كمالك إحتياطي
الوحدة 2-1	z	· مرسل
الوحدة 3-1	Y	- مالك النسخ الاحتياطي

ويمكن تمثيل ذلك على النحو التالي:



1. تصل حزمة TCP SYN من المضيف-A إلى الوحدة-1-1. تصبح الوحدة-1-1 هي مالك التدفق ويتم إختيارها كمدير.
2. يتم إختيار الوحدة 3-1 كمالك للنسخ الاحتياطي. يرسل مالك التدفق رسالة "إضافة نظام مجموعة" للبث الأحادي على UDP 4193 لإعلام مالك النسخ الاحتياطي بالتدفق.
3. تصل حزمة TCP SYN/ACK من المضيف-B إلى الوحدة-2-1. التدفق غير المتماثل.
4. تقوم الوحدة 2-1 بإعادة توجيه الحزمة من خلال CCL إلى المالك (بسبب ملف تعريف إرتباط TCP SYN).
5. يقوم المالك بإعادة إدخال الحزمة على الواجهة الخارجية ثم إعادة توجيه الحزمة نحو المضيف-A.
6. بمجرد إنهاء الاتصال، يرسل المالك رسالة حذف نظام مجموعة لإزالة معلومات التدفق من مالك النسخة الاحتياطية.

الملاحظة 3 - يظهر التسجيل بالتتبع حركة المرور غير المتماثلة وإعادة التوجيه من الوحدة 2-1 إلى الوحدة 1-1.

الوحدة 2-1 (مرسل)

```
<#root>

firepower#

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

1: 16:11:33.653164 802.1Q vlan#202 P0 192.168.241.50.80 > 192.168.240.50.
```

46916

:

S

 1331019196:1331019196(0)

ack

 3089755618 win 28960 <mss 1460,sackOK,timestamp 532473211 522117741,nop,wscale 7>
...
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW

I (1) got initial, attempting ownership.

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

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

الملاحظة 4. توضح نظم مستوى بيانات FTD إنشاء الاتصال وإنهائه على جميع الوحدات:

- الوحدة 1-1 (المالك)
- الوحدة 2-1 (مرسل)
- الوحدة 3-1 (مالك النسخة الاحتياطية)

<#root>

firepower#

cluster exec show log | i 46916

unit-1-1(LOCAL):***
Dec 01 2020 16:11:33: %FTD-6-302013:

Built inbound TCP connection

 10023 for INSIDE:192.168.240.50/46916 (192.168.240.50/46916) to OUTSIDE:192.168.241.50/80 (192.168.241
Dec 01 2020 16:11:42: %FTD-6-302014:

Teardown TCP connection

```
 10023 for INSIDE:192.168.240.50/46916 to OUTSIDE:192.168.241.50/80 duration 0:00:09 bytes 1024010016 T

unit-2-1:************************************************************
Dec 01 2020 16:11:33: %FTD-6-302022:

Built forwarder stub TCP connection

 for OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46916 (192.168.240.50/4691
Dec 01 2020 16:11:42: %FTD-6-302023:

Teardown forwarder TCP connection

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

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

Built backup stub TCP connection

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

Teardown backup TCP connection

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

دراسة الحالة 5 - حركة المرور غير المتماثلة (المالك مختلف عن المدير).

الملاحظة 1. يظهر إلتقاط إخفاء حقن حزم على الوحدة 1-1 و الوحدة 2-1 (التدفق غير المتماثل):

<#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

الملاحظة 2. تحليل علم الاتصال للتدفق بمنفذ المصدر 46994:

<#root>

firepower#

cluster exec show conn

unit-1-1

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

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

46994

, idle 0:00:00, bytes 406028640,

flags UIO N1

unit-2-1

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

TCP OUTSIDE 192.168.241.50:80 NP Identity Ifc 192.168.240.50:

46994

, idle 0:00:00, bytes 0,

flags z

unit-3-1

:**********
17 in use, 20 most used
Cluster:
fwd connections: 2 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 0 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

TCP OUTSIDE 192.168.241.50:80 INSIDE 192.168.240.50:

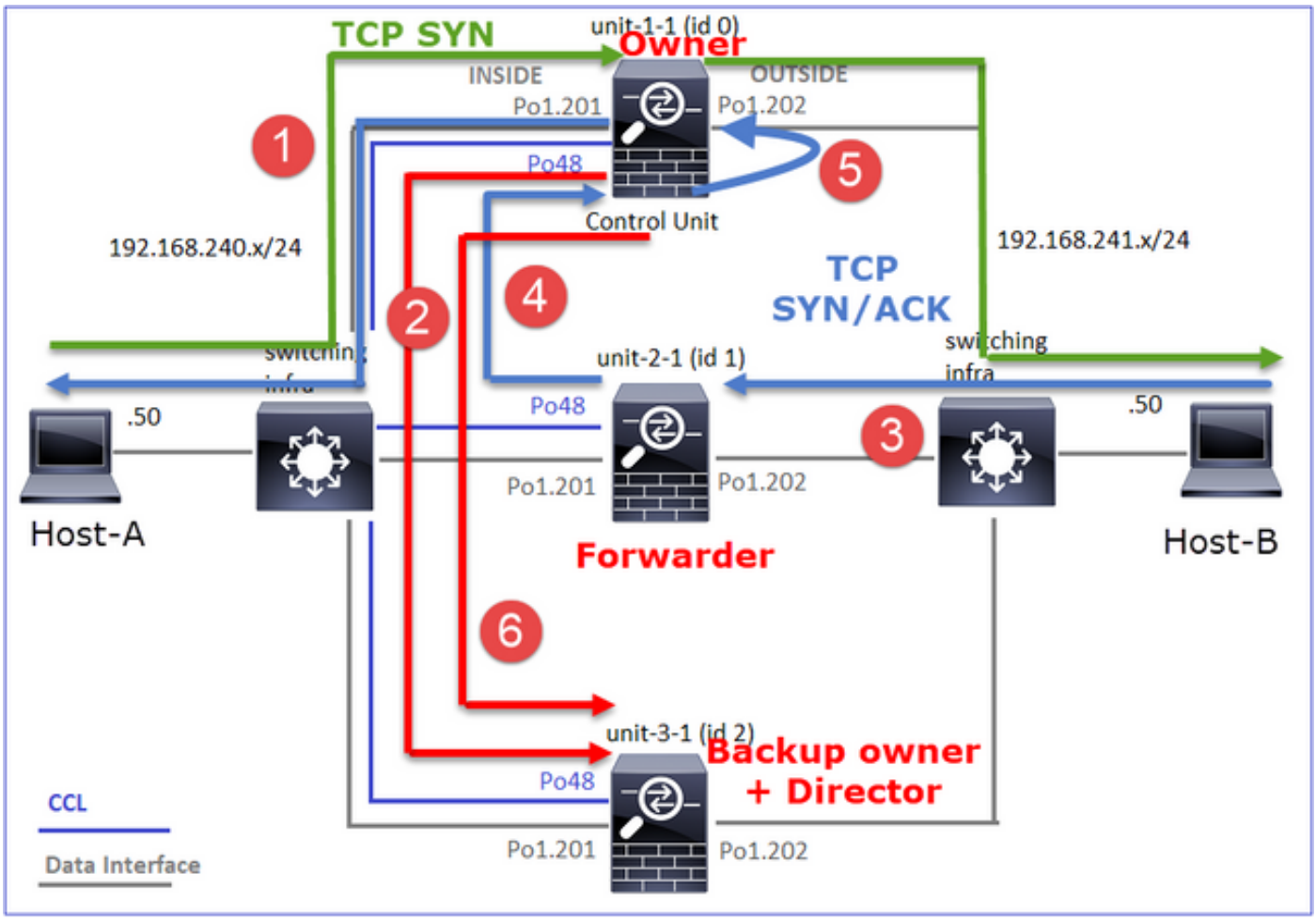
46994

, idle 0:00:05, bytes 0,

flags Y

وحدة	راية	ملاحظة
الوحدة 1-1	أويو	· مالك التدفق - تتولى الوحدة التدفق
الوحدة 2-1	z	· مرسل
الوحدة 3-1	Y	مالك النسخ الاحتياطي · مدير ·

ويمكن تمثيل ذلك على النحو التالي:



1. تصل حزمة نظام TCP من المضيف-A إلى الوحدة-1-1. تصبح الوحدة-1-1 مالك التدفق.
2. يتم إختيار الوحدة 3-1 كمدير ومالك للنسخ الاحتياطي. يرسل مالك التدفق رسالة "إضافة نظام المجموعة" للبث الأحادي على UDP 4193 لإعلام مالك النسخ الاحتياطي بالتدفق.
3. تصل حزمة TCP SYN/ACK من المضيف-B إلى الوحدة-2-1. التدفق غير المتماثل
4. تقوم الوحدة 2-1 بإعادة توجيه الحزمة من خلال CCL إلى المالك (بسبب ملف تعريف إرتباط TCP SYN).
5. يقوم المالك بإعادة إدخال الحزمة على الواجهة الخارجية ثم إعادة توجيه الحزمة نحو

المضيف-A.

6. بمجرد إنهاء الاتصال، يرسل المالك رسالة حذف نظام مجموعة لإزالة معلومات التدفق من مالك النسخة الاحتياطية.

الملاحظة 3 - يظهر التسجيل بالتتبع حركة المرور غير المتماثلة وإعادة التوجيه من الوحدة 1-1 إلى الوحدة 2-1.

الوحدة 1-1 (المالك)

<#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

الوحدة 2-1 (مرسل)

<#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).
```

الملاحظة 4. توضح نظم مستوى بيانات FTD إنشاء الاتصال وإنهائه على جميع الوحدات:

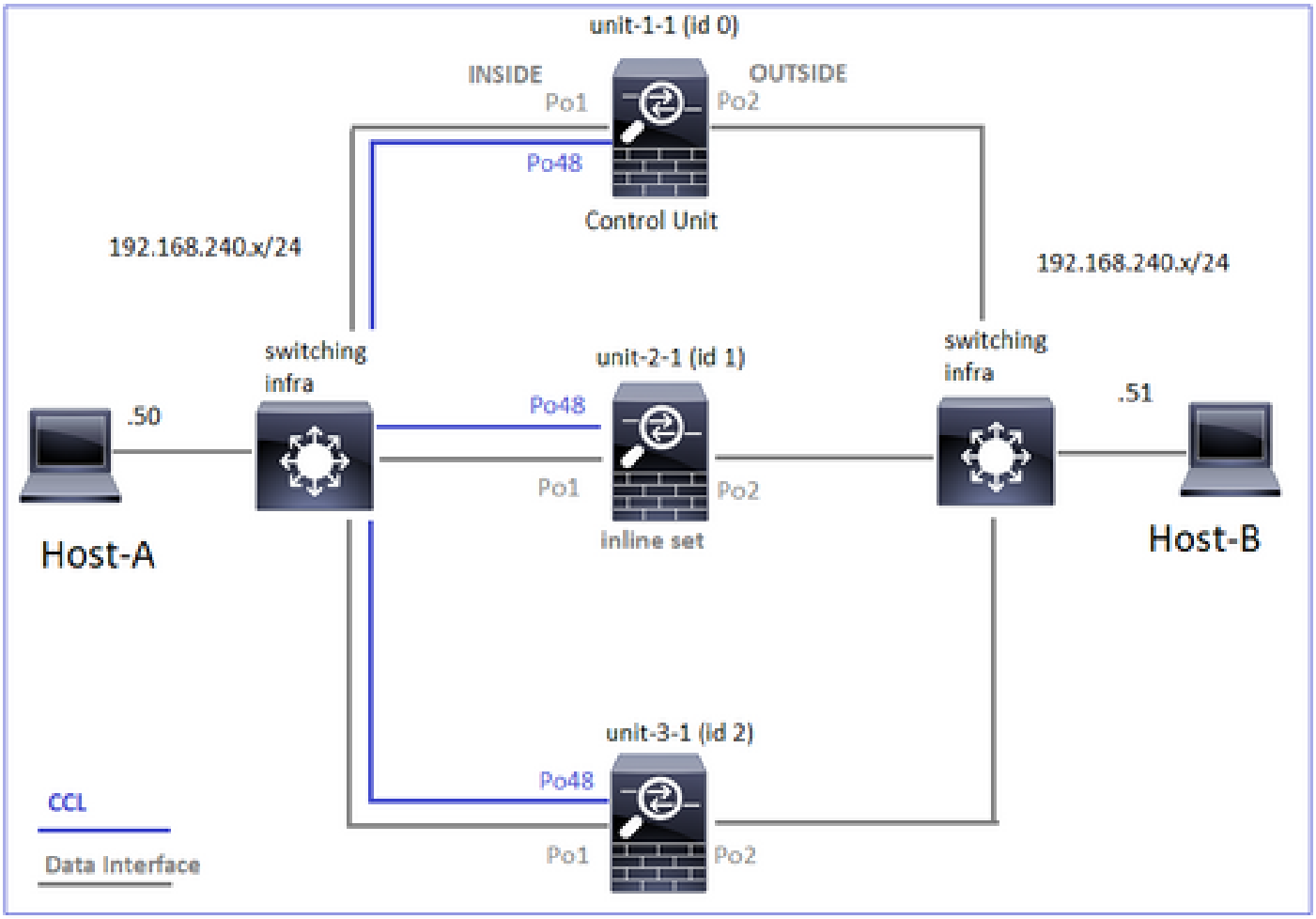
- الوحدة 1-1 (المالك)
- الوحدة 2-1 (مرسل)
- الوحدة 3-1 (مالك/مدير النسخة الاحتياطية)

<#root>

```
firepower#

cluster exec show log | i 46994


unit-1-1(LOCAL):*******************************************************
Dec 01 2020 16:46:44: %FTD-6-302013:

Built inbound TCP connection

 10080 for INSIDE:192.168.240.50/46994 (192.168.240.50/46994) to OUTSIDE:192.168.241.50/80 (192.168.241
Dec 01 2020 16:46:53: %FTD-6-302014:

Teardown TCP connection

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

unit-2-1:*************************************************************
Dec 01 2020 16:46:44: %FTD-6-302022:

Built forwarder stub TCP connection

 for OUTSIDE:192.168.241.50/80 (192.168.241.50/80) to unknown:192.168.240.50/46994 (192.168.240.50/4699
Dec 01 2020 16:46:53: %FTD-6-302023:
```

```
Teardown forwarder TCP connection

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

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

Built director stub TCP connection

 for INSIDE:192.168.240.50/46994 (192.168.240.50/46994) to OUTSIDE:192.168.241.50/80 (192.168.241.50/80
Dec 01 2020 16:46:53: %FTD-6-302023:

Teardown director TCP connection

 for INSIDE:192.168.240.50/46994 to OUTSIDE:192.168.241.50/80 duration 0:00:09 forwarded bytes 0 Cluste
```

لدراسات الحالة التالية، تستند الطبوغرافيا المستخدمة إلى نظام مجموعة بمجموعات داخلية:



دراسة الحالة 6 - حركة المرور غير المتماثلة (مجموعة داخلية، المالك وه المدير)

الملاحظة 1 - تظهر صور أعياني الأعناق حزم على الوحدة 1-1 والوحدة 2-1 (التدفق غير المتماثل). بالإضافة إلى ذلك، يكون المالك وه الوحدة 2-1 (هناك حزم على كل الواجهات الداخلية والخارجية لبطاقات الإدخال/الإخفاء، بينما الوحدة 1-1 تحتوي على الواجهات الخارجية فقط):

<#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
```

الملاحظة 2. تحليل عالمة الوصلة للتدفق بمنفذ المصدر 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

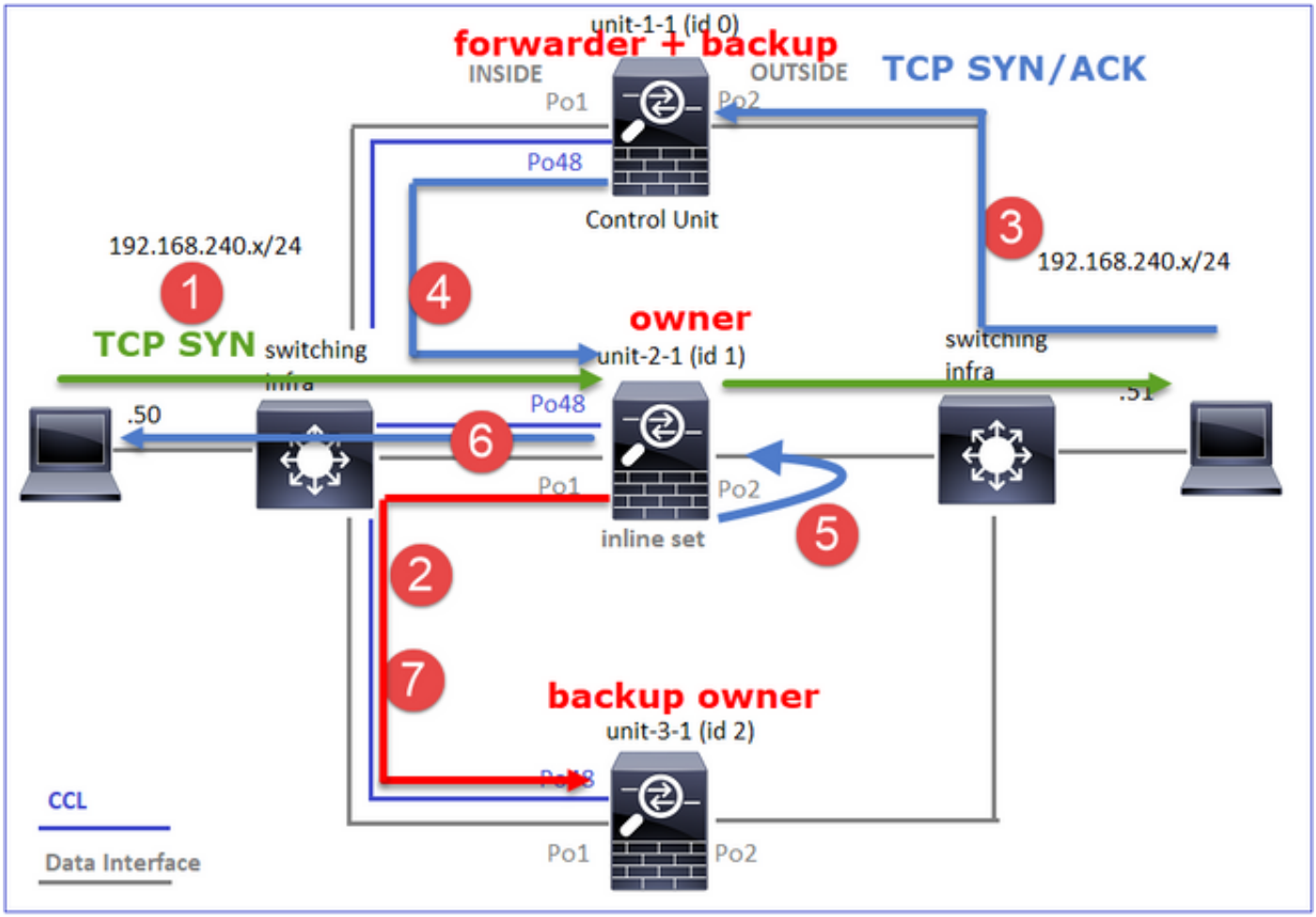
:**********
20 in use, 55 most used
Cluster:
fwd connections: 0 in use, 5 most used
dir connections: 1 in use, 127 most used
centralized connections: 0 in use, 24 most used
VPN redirect connections: 0 in use, 0 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect

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

flags y

وحدة	راية	ملاحظة
الوحدة 1-1	z	· مرسل
الوحدة 2-1	ب ن	· مالك التدفق - تتولى الوحدة التدفق
الوحدة 3-1	Y	مالك النسخ الاحتياطي ·

ويمكن تمثيل ذلك على النحو التالي:



1. تصل حزمة TCP SYN من المضيف-A إلى الوحدة-2-1. تصبح الوحدة-2-1 هي مالك التدفق ويتم إختياراها كمدير.
2. تم إختيار الوحدة 3-1 كمالك للنسخ الاحتياطي. يرسل مالك التدفق رسالة "إضافة نظام المجموعة" للبث الأحادي على UDP 4193 لإعلام مالك النسخ الاحتياطي بالتدفق.
3. تصل حزمة TCP SYN/ACK من المضيف-B إلى الوحدة-1-1. التدفق غير المتماثل.
4. تقوم الوحدة 1-1 بإعادة الحزمة من خلال قائمة التحكم في الوصول (CCL) إلى المدير (الوحدة 2-1).
5. كما أن UNIT-2-1 هو المالك ويقوم بإعادة إدخال الحزمة على الواجهة الخارجية.
6. تقوم الوحدة 2-1 بإعادة توجيه الحزمة باتجاه المضيف-A.
7. بمجرد إنهاء الاتصال، يرسل المالك رسالة حذف نظام مجموعة لإزالة معلومات التدفق من مالك النسخة الاحتياطية.

الملاحظة 3 - يظهر التسجيل بالتتبع حركة المرور غير المتماثلة وإعادة التوجيه من الوحدة 1-1 إلى الوحدة 2-1.

الوحدة 2-1 (المالك/المدير)

```
<#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

الوحدة 1-1 (مرسل)

<#root>

```
firepower#
```

cluster exec show cap CAPO packet-number 1 trace

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

1: 18:10:12.842317 192.168.240.51.80 > 192.168.240.50.51844: S 2339579109:2339579109(0) ack 4082593464 w
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: NO FLOW
```

I (0) am asking director (1).

حركة مرور الإرجاع (TCP SYN/ACK)

الوحدة 2-1 (المالك/المدير)

```
<#root>

firepower#

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



2: 18:10:12.843660 192.168.240.51.80 > 192.168.240.50.51844: S 2339579109:2339579109(0) ack 4082593464 w
Phase: 1
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'OUTSIDE'
Flow type: FULL


I (1) am owner, update sender (0).



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


Found flow with id 7109, using existing flow
```

الملاحظة 4. توضح نظم مستوى بيانات FTD إنشاء الاتصال وإنهائه على جميع الوحدات:

- الوحدة 1-1 (المالك)
- الوحدة 2-1 (مرسل)
- الوحدة 3-1 (مالك/مدير النسخة الاحتياطية)

```
<#root>

firepower#

cluster exec show log | include 51844


unit-1-1(LOCAL):*******************************************************
Dec 02 2020 18:10:12: %FTD-6-302022:

Built forwarder stub TCP connection

 for OUTSIDE:192.168.240.51/80 (192.168.240.51/80) to unknown:192.168.240.50/51844 (192.168.240.50/5184
Dec 02 2020 18:10:22: %FTD-6-302023:

Teardown forwarder TCP connection

 for OUTSIDE:192.168.240.51/80 to unknown:192.168.240.50/51844 duration 0:00:09 forwarded bytes 1024001

unit-2-1:*************************************************************
Dec 02 2020 18:10:12: %FTD-6-302303:
```

Built TCP state-bypass connection

```
 7109 from INSIDE:192.168.240.50/51844 (192.168.240.50/51844) to OUTSIDE:192.168.240.51/80 (192.168.240
Dec 02 2020 18:10:22: %FTD-6-302304:
```

Teardown TCP state-bypass connection

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

```
unit-3-1:************************************************************
Dec 02 2020 18:10:12: %FTD-6-302022:
```

Built backup stub TCP connection

```
 for INSIDE:192.168.240.50/51844 (192.168.240.50/51844) to OUTSIDE:192.168.240.51/80 (192.168.240.51/80)
Dec 02 2020 18:10:22: %FTD-6-302023:
```

Teardown backup TCP connection

```
 for INSIDE:192.168.240.50/51844 to OUTSIDE:192.168.240.51/80 duration 0:00:09 forwarded bytes 0 Cluste
```

دراسة الحالة 7 - حركة المرور غير المتماثلة (مجموعة داخلية، المالك مختلف عن المدير)

المالك هو u-2-1 (هناك حزم على كل الواجهات الداخلية والخارجية لالتقاط Reinject-hide، بينما الوحدة-3-1 لديها فقط على الخارج):

<#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

الملاحظة 2. تحليل عالمة الوصلة للتدفق بمنفذ المصدر 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:

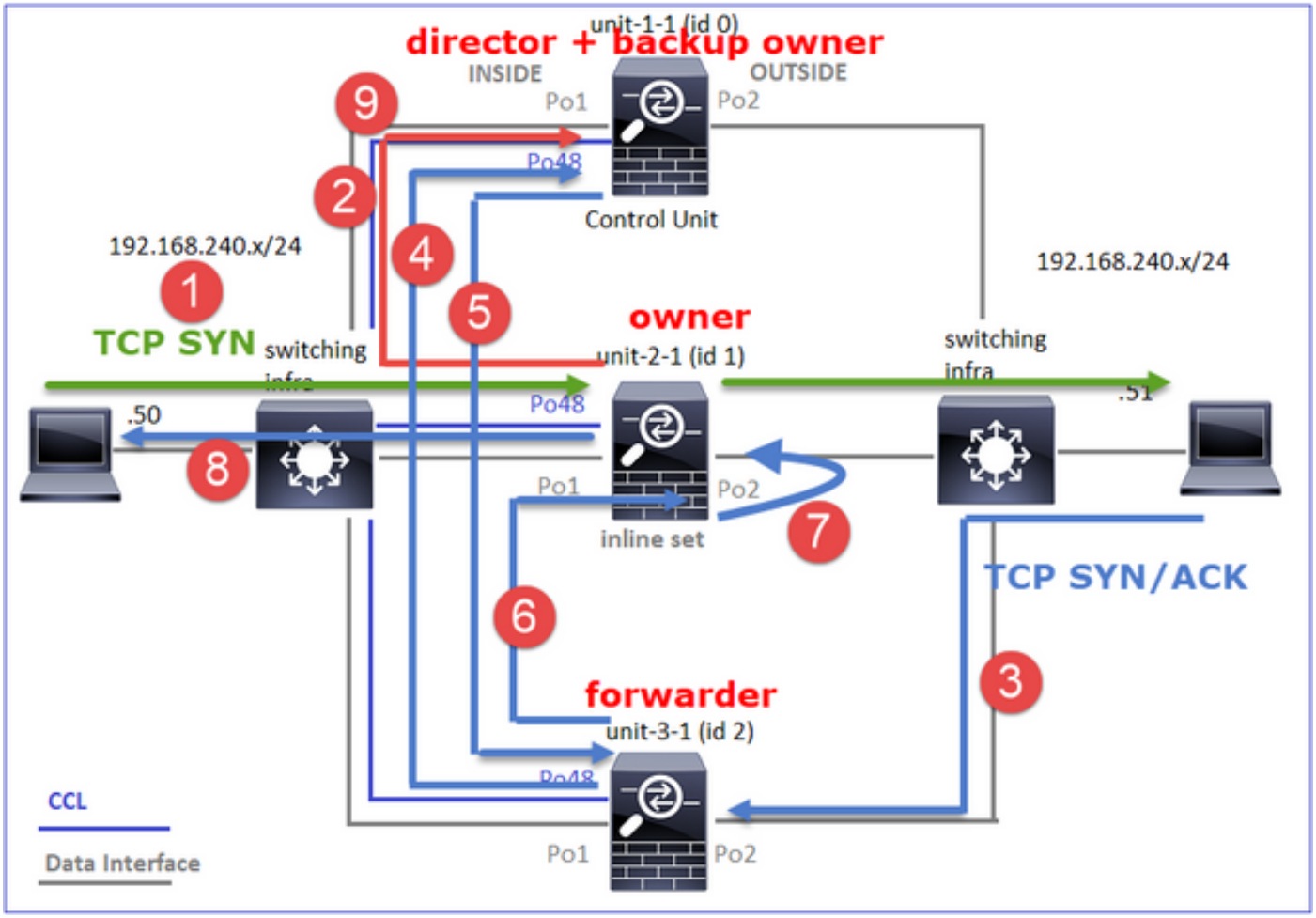
59210

, idle 0:00:00, bytes 0,

flags z

وحدة	رايه	ملاحظة
الوحدة 1-1	Y	مدير ·/مالك النسخة الاحتياطية
الوحدة 2-1	ب ن	· مالك التدفق - تتولى الوحدة التدفق
الوحدة 3-1	z	· مرسل

ويمكن تمثيل ذلك على النحو التالي:



1. تصل حزمة TCP SYN من المضيف-A إلى الوحدة-2-1. تصبح الوحدة-2-1 هي مالك التدفق ويتم إختيار الوحدة-1-1 كمدير
2. الوحدة-1-1 ينتخب مالك النسخة الاحتياطية (بما أنه المدير). يرسل مالك التدفق رسالة "إضافة نظام مجموعة" أحادية البث على UDP 4193 إلى. إعلام مالك النسخة الاحتياطية بالتدفق.
3. تصل حزمة TCP SYN/ACK من المضيف-B إلى الوحدة-3-1. التدفق غير المتماثل.
4. تقوم الوحدة 3-1 بإعادة الحزمة من خلال قائمة التحكم في الوصول (CCL) إلى المدير (الوحدة 1-1).
5. الوحدة 1-1 (مدير) يعرف أن المالك هو الوحدة 2-1، ويرسل الحزمة مرة أخرى إلى المرسل

(وحدة-3-1)، ويبلغه أن المالك هو الوحدة-2-1.
6. ترسل الوحدة-3-1 الحزمة إلى الوحدة-2-1 (المالك).
7. تضخ الوحدة 2-1 الحزمة على الواجهة الخارجية.
8. توقوم الوحدة 2-1 بإعادة توجيه الحزمة باتجاه المضيف-A.
9. بمجرد إنهاء الاتصال، يرسل المالك رسالة خذف نظام مجموعة لإزالة معلومات التدفق من مالك النسخة الاحتياطية.

ملاحظة: من المهم أن تحدث الخطوة 2 (الحزمة من خلال CCL) قبل الخطوة 4 (حركة مرور البيانات). وفي حالة أخرى (مثل حالة العرق)، الا يكون المدير على علم بالتدفق. لذلك، بما أنه مجموعة في السطر، فأعد توجيه الحزمة نحو الوجهة. إذا لم تكن الواجهات في مجموعة أسطر، يتم إسقاط حزمة البيانات.

الملاحظة 3 - يظهر التسجيل بالتتبع حركة المرور غير المتماثلة وعمليات التبادل عبر CCL:

حركة مرور البيانات للأمام (TCP SYN)

الوحدة 2-1 (المالك)

<#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

حزمة مرور الإرجاع (TCP SYN/ACK)

ترسل الوحدة-3-1 (المعرف 2 - المومج) الحزمة عبر قناة التحكم في الوصول (CCL) إلى الوحدة-1-1 (المعرف 0 - المدير).

```
<#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).
```

الوحدة-1-1 (المدير) - تعرف الوحدة-1-1 (المعرف 0) أن مالك التدفق هو الوحدة-2-1 (المعرف 1) الوحدة-1-1 (المدير) ويرسل الحزمة عبر قناة التحكم في الوصول (CCL) مرة أخرى إلى الوحدة-3-1 (المعرف 2 - المومج).

```
<#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).

تحصل الوحدة-3-1 (المعرف 2 - الموجه) على الحزمة من خلال CCL وترسلها إلى الوحدة-2-1 (المعرف 1 - المالك).

<#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).

يقوم المالك بإعادة إدخال الحزمة وإعادة توجيهها نحو الوجهة:

<#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).
```

الملاحظة 4. توضح نظم مستوى بيانات FTD إنشاء الاتصال وإنهائه على جميع الوحدات:

- الوحدة 1-1 (المدير/مالك النسخة الاحتياطية)
- الوحدة 2-1 (المالك)
- الوحدة 3-1 (مرسل)

```
<#root>

firepower#

 cluster exec show log | i 59210


unit-1-1(LOCAL):*********************************************************
Dec 03 2020 09:19:49: %FTD-6-302022:

Built director stub TCP connection

 for INSIDE:192.168.240.50/59210 (192.168.240.50/59210) to OUTSIDE:192.168.240.51/80 (192.168.240.51/80)
Dec 03 2020 09:19:59: %FTD-6-302023:

Teardown director TCP connection

 for INSIDE:192.168.240.50/59210 to OUTSIDE:192.168.240.51/80 duration 0:00:09 forwarded bytes 0 Cluste

unit-2-1:*********************************************************
Dec 03 2020 09:19:49: %FTD-6-302303:

Built TCP state-bypass connection

 14483 from INSIDE:192.168.240.50/59210 (192.168.240.50/59210) to OUTSIDE:192.168.240.51/80 (192.168.240
Dec 03 2020 09:19:59: %FTD-6-302304:

Teardown TCP state-bypass connection

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

unit-3-1:*********************************************************
Dec 03 2020 09:19:49: %FTD-6-302022:

Built forwarder stub TCP connection

 for OUTSIDE:192.168.240.51/80 (192.168.240.51/80) to unknown:192.168.240.50/59210 (192.168.240.50/5921
Dec 03 2020 09:19:59: %FTD-6-302023:

Teardown forwarder TCP connection

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

استكشاف الأخطاء وإصلاحها

مقدمة حول أستكشاف أخطاء المجموعة وإصلاحها

يمكن تصنيف مشاكل نظام المجموعة في:

- مشاكل مستوى التحكم (مشاكل متعلقة باستقرار نظام المجموعة)
- مشاكل مستوى البيانات (مشاكل متعلقة بحركة مرور النقل)

مشاكل مستوى بيانات نظام المجموعة

القضايا المشتركة بين NAT/PAT

اعتبارات التكوين الهامة

- يجب أن تحتوي تجمعات ترجمة عنوان المنفذ (PAT) على عدد IPs متوفر على الأقل مثل عدد الوحدات في نظام المجموعة، ويفضل أن يكون عدد وحدات IP أكثر من عقد نظام المجموعة.
- يجب ترك أوامر xlate الافتراضية لكل جلسة عمل في مكانها ما لم يكن هناك سبب محدد لتعطيلها. يتم إنشاؤه لتعطيل التقاط تم إنشاء أي PAT Xlate متحدة لكل جلسة عمل بواسطة وحدة عقدة التحكم في نظام المجموعة، والتي يمكن أن تتسبب في انخفاض الأداء.

إستخدام نطاق تجمع PAT العالي بسبب حركة المرور التي يتم الحصول عليها من المنافذ المنخفضة والتي تتسبب في عدم توازن IP للمجموعة

يقوم FTD بتقسيم IP برض إلى نطاقات ويحاول الحفاظ على xlate في نطاق المصدر نفسه. يبدي هذا الجدول كيف يتم ترجمة منفذ مصدر إلى منفذ مصدر ضمن نطاق المصدر نفسه.

منفذ SRC الأصلي	منفذ SRC المترجم
1-511	1-511
512-1023	512-1023
1024-65535	1024-65535

عندما يكون منفذ المصدر أعلى من أن يكون في النطاق وهناك حاجة إلى كمال رسمي أي أعلى، FTD ينتقل إلى التالي ip أن يتخصص ترجمة جديد ل أن مصدر ميناء مدى.

الأعراض

مشكلات الاتصال لحركة مرور NATed التي تجتاز المجموعة

التحقق

<#root>

```
#
show nat pool
```

تظهر سجلات مستوى بيانات FTD إستهلاك تجمع 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
```

تخفيف

قم بتكوين قاطن المنفذ الثابت NAT وتضمين المنافذ الاحتياطية.

بالإضافة إلى ذلك، في مرحلة ما بعد 6.7/9.15.1 يمكنك أن ينتهي بك الأمر مع توزيع لتلك المنافذ غير المتوازن فقط عندما تنضم/تغادر العقد إلى نظام المجموعة مع حركة مرور بيانات خلفية ضخمة تخضع لتعليمات ربط. الطريقة الوحيدة التي تتعافى بها بنفسها هي عندما يتم تحرير تلك المنافذ لإعادة توزيعها عبر العقد.

باستخدام التوزيع القائم على حظر المنافذ، عند تخصيص عقدة مع 10 على منافذ لتلك الحالات مثل PB-1 و PB-2 ... PB-10. تبدأ العقدة دائما بأول تلك المنافذ المتوفرة وتخصص منفذا عشوائيا منها حتى تستنفذ. ينتقل التخصيص إلى تلك المنافذ التالية فقط عندما يتم استنفاد جميع تلك المنافذ حتى تلك النقطة.

على سبيل المثال، إذا قام المضيف بإنشاء 512 اتصالا، فإن الوحدة تقوم بتخصيص المنافذ المعينة لكل هذه الاتصالات الـ 512 من PB-1 بشكل عشوائي. الآن، مع كل هذه الاتصالات الـ 512 نشطة، عندما يؤسس المضيف الـ 513 اتصالا بما أن PB-1 مستنفذ، ينتقل إلى PB-2 ويخصص منفذا عشوائيا منه. الآن مرة أخرى، من بين 513 وصلة، افترض أن الاتصال العاشر انتهى وحسم منفذا واحدا متوفرا في PB-1. في هذه النقطة، إذا كان المضيف يؤسس الاتصال 514، فإن وحدة نظام المجموعة تخصص منفذا معينا من PB-1 وليس PB-2 لأن PB-1 لديه الآن منفذ حر (والذي تم إطلاقه كجزء من إزالة الاتصال العاشر).

الجزء المهم الذي يجب وضعه في الاعتبار هو أن التخصيص يحدث من أول تلك المنافذ متاحة

بمنافذ حرة بحيث تكون كتل المنفذ الأخيرة متاحة دائما لإعادة التوزيع في نظام محمل عادة. وبالإضافة إلى ذلك، يستخدم ضرب عادة للاتصالات القصيرة العمر. والاحتمال أن تصبح كتلة المنفذ متوفرة في وقت أقصر كبير جدا. لذلك، يمكن أن يتحسن الوقت المطلوب لكي يصبح توزيع التجمع متوازنا مع توزيع التجمع القائم على كتل المنافذ.

ومع ذلك، في حالة استنفاد جميع كتل المنافذ، من PB-1 إلى PB-10، أو أن كل كتلة منافذ تحتوي على منفذ لاتصال طويل الأجل، فلا يتم تحرير كتل المنافذ أبدا بسرعة ويتم إعادة توزيعها. وفي مثل هذه الحالة، فإن النهج الأقل تعطيلا هو:

1. التعرف على العقد ذات كتل المنافذ الزائدة (إظهار ملخص مجموعة التجمع nat).
2. حدد كتل المنافذ الأقل إستخداما على تلك العقدة (إظهار تفاصيل <addr> الخاصة بالتجمع غير المستعمل).
3. امسح الحدود لكتل المنافذ هذه (امسح الحدود العمومية <addr> gport 'start-end') لتوفيرها لإعادة التوزيع.

تحذير: يؤدي ذلك إلى مقاطعة الاتصالات ذات الصلة.

غير قادر على الاستعراض إلى مواقع ويب مزدوجة القنوات (مثل البريد الإلكتروني أو الأعمال المصرفية، إلخ) أو إلى مواقع SSO على الويب عند حدوث إعادة التوجيه إلى وجهة مختلفة.

الأعراض

غير قادر على الاستعراض إلى مواقع ويب مزدوجة القنوات (مثل البريد الإلكتروني ومواقع البنك وما إلى ذلك). عندما يتصل مستخدم بموقع ويب يتطلب من العميل فتح اتصال ثان ويتم تجزئة الاتصال الثاني إلى عضو نظام مجموعة مختلف عن العضو الذي تم قطع الاتصال الأول إليه، كما تستخدم حركة مرور البيانات تجمع IP PAT، تتم إعادة تعيين حركة مرور البيانات بواسطة الخادم حيث إنها تتلقى الاتصال من عنوان IP عام مختلف.

التحقق

قم بأخذ مجموعات مستوى البيانات لترى كيفية التعامل مع تدفق النقل المتأثر. في هذه الحالة، تأتي إعادة تعيين TCP من موقع الوجهة على الويب.

التخفيف (ما قبل 6.7/9.15.1)

- لاحظ ما إذا كانت أي تطبيقات متعددة الجلسات تستخدم عناوين IP متعددة تم تعيينها.
- أستخدم الأمر show nat pool cluster summary للتحقق من توزيع التجمع بالتساوي.
- أستخدم أمر show conn الخاص ببروتوكول نظام المجموعة لفحص ما إذا كانت حركة مرور البيانات متوازنة بشكل صحيح.
- أستخدم الأمر show nat pool cluster ip <address> detail للتحقق من إستخدام التجمع ل IP اللاصق.
- قم بتمكين syslog 305021 (6.7/9.15) من معرفة الاتصالات التي فشلت في إستخدام IP اللاصق.
- لحل هذه المشكلة قم بإضافة المزيد من عناوين IP إلى تجمع PAT أو قم بضبط خوارزمية موازنة التحميل على المحولات المتصلة.

حول خوارزمية موازنة حمل Ether-channel:

- بالنسبة لغير FP9300 وإذا حدث تشتت الاتصال عبر خادم واحد: قم بضبط خوارزمية موازنة التحميل من Ether-Channel على المحول المجاور من المصدر IP/Port والوجهة IP/Port إلى مصدر IP والوجهة.
- بالنسبة لغير FP9300 وإذا حدث تشتت الاتصال عبر خوادم متعددة: قم بضبط خوارزمية موازنة التحميل من Ether-Channel على المحول المجاور من المصدر IP/Port والوجهة IP/Port إلى المصدر IP.
- بالنسبة للمحولات FP9300: على هيكل FP9300، يتم تثبيت خوارزمية موازنة الأحمال باعتبارها مصدر-top-port source-dest-ip source-mac ولا يمكن تغييرها. الـ workaround، في هذه الحالة، أن يستعمل FlexConfig أن يضيف xlate فتحة لكل ضرر أمر إلى الـ FTD تشكيل أن يجبر حركة مرور خاص غاية معين غاية عناوين (إشكالية/غير متوافقة للغاية) أن يكون موجه ب فقط الـ تحكم عقدة في الهيكل الداخلي للمجموعة. الحل يأتي مع هذه الآثار الجانبية:
  - لا يوجد موازنة حمل لحركة المرور التي تمت ترجمتها بشكل مختلف (كل بهذي شيء إلى عقدة التحكم).
  - احتمال نفاد فتحات xlate (والتأثير سلبا على ترجمة NAT لحركة المرور الأخرى على عقدة التحكم).
  - إمكانية توسع أقل لمجموعة الهيكل الداخلي.

أداء نظام مجموعة منخفض بسبب حركة مرور البيانات التي يتم إرسالها إلى عقدة التحكم بسبب عدم وجود ما يكفي من عناوين IP الخاصة بالمجموعات.

الأعراض

لا يوجد ما يكفي من عناوين IP الخاصة بالدراسة المؤقتة (PAT) في المجموعة لتخصيص عنوان IP حر إلى عقد البيانات، وبالتالي، تتم إعادة توجيه جميع حركات المرور الخاضعة لتكوين PAT إلى عقدة التحكم لمعالجتها.

التحقق

أستخدم الأمر show nat pool cluster لعرض عمليات التخصيص لكل وحدة والتأكد من أنها تمتلك IP واحد على الأقل في المجموعة.

تخفيف

بالنسبة لما قبل 6.7/9.15.1، تأكد من أن لديك تجمع PAT بحجم واسع على الأقل لعدد العقد في المجموعة. في ما بعد 6.7/9.15.1 مع كتلة PAT، تخصص أنت كتلة من كل الـ PAT كتلة. إذا كان استخدام تجمع PAT مرتفع حقا مما يؤدي إلى استنفاد متكرر للتجمع، فإنك بحاجة إلى زيادة حجم تجمع PAT (راجع قسم الأسئلة المتداولة).

أداء منخفض بسبب كل حركات المرور المرسلة إلى عقدة التحكم لأن قوائم التحكم ليست ممكنة لكل جلسة عمل.

الأعراض

تتم معالجة الكثير من تدفقات النسخ الاحتياطي لـ UDP عالية السرعة من خلال عقدة التحكم في نظام المجموعة، والتي يمكن أن تؤثر على الأداء.

الخلفية

يمكن طقف نكمي ةجلاعم الاتصالات التي تستخدم xlates لكل جلسة ممكنة بواسطة عقدة بيانات تستخدم PAT. أستخدم الأمر show run all allLate لعرض تكوين xlate لكل جلسة.

يعني تمكين لك جلسة لمع أنه يتم تقسيم xlate على الفور عندما يتم قطع الاتصال المرتبط. ويساعد هذا على تحسين الاتصال في الثانية عند تعرض الاتصالات إلى عملية تحديد الأداء (PAT). في حالة عدم وجود جلسة لمع مباشرة لمدة 30 ثانية أخرى بعد أن يتم تقسيم الاتصال المقترن إلى أسفل، وإذا كان معدل الاتصال مرتفعا بدرجة كافية، فيمكن إستخدام منافذ TCP/UDP المتاحة بسرعة 65 كيلو على كل عنوان IP عام في وقت قصير.

بشكل افتراضي، تكون جميع حركة مرور TCP ممكنة لكل xlate وتكون حركة مرور DNS ل UDP فقط ممكنة لكل جلسة لمع. وهذا يعني إعادة توجيه جميع حركة مرور بيانات UDP غير الخاصة ب DNS إلى عقدة التحكم لمعالجتها.

التحقق

أستخدم هذا الأمر للتحقق من الاتصال وتوزيع الحزم بين وحدات نظام المجموعة:

<#root>

```
firepower#

show cluster info conn-distribution

firepower#

show cluster info packet-distribution

firepower#

show cluster info load-monitor
```

أستخدم أمر show conn Jcluster" لمعرفة عقد نظام المجموعة التي تمتلك إتصالات UDP.

<#root>

```
firepower#

cluster exec show conn
```

أستخدم هذا الأمر لفهم إستخدام التجمع عبر عقد نظام المجموعة.

<#root>

```
firepower#

cluster exec show nat pool ip
```

```
| in UDP
```

تخفيف

شكلت لكل جلسة ضرب (لكل جلسة يسمح udp أمر) لحركة مرور المصلحة (مثال، UDP). ل ICMP، أنت يستطيع ال يغير من التقصير multi-session ضرب، لذلك ICMP معالجة حركة مرور دائما ب التحكم عقدة عندما هناك ضرب يشكل.

توزيع تجمع PAT يصبح غير متوازن حيث أن العقد تغادر/تنضم إلى نظام المجموعة.

الأعراض

- مشكلات الاتصال نظرا لأن تخصيص IP للضرب يمكن أن يصبح غير متوازن مع مرور الوقت بسبب الوحدات التي تغادر المجموعة وتنضم إليها.
- في ام بعد 6.7/9.15.1، يمكن أن يكون هناك حالات ال يمكن فيها للعقدة المتصلة حديثا الحصول على كتل منافذ كافية. تقوم العقدة التي ال تحتوي على أي كتلة منافذ بإعادة توجيه حركة مرور البيانات إلى عقدة التحكم. تقوم العقدة التي تحتوي على كتلة منفذ واحدة على الأقل بمعالجة حركة المرور وإسقاطها بمجرد استنفاد التجمع.

التحقق

- تظهر مخططات مستوى البيانات رسائل مثل:

```
<#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
```

- أستخدم الأمر show nat pool cluster summary لتحديد توزيع التجمع.
- أستخدم الأمر cluster exec show nat pool ip <addr> detail لفهم إستخدام التجمع عبر عقد نظام المجموعة.

تخفيف

- بالنسبة لما قبل 6.7/9.15.1 يتم وصف بعض الحلول البديلة في معرف تصحيح الأخطاء من Cisco CSCvd10530
.
- في مرحلة ما بعد 6.7/9.15.1، أستخدم الأمر clear xlate global <ip> gport <start-end>لمسح بعض كتل المنافذ على العقد الأخرى يدويا لإعادة التوزيع على العقد المطلوبة.

الأعراض

مشكلات الاتصال الرئيسية لحركة المرور التي تتم معالجتها بواسطة نظام المجموعة. وذلك لأن مستوى بيانات FTD، لكل تصميم، لا يرسل GARP لعناوين NAT العالمية.

التحقق

يظهر جدول ARP الخاص بالأجهزة المتصلة مباشرة عنوان MAC الخاص بواجهة بيانات نظام المجموعة بشكل مختلف بعد تغيير عقدة التحكم:

```
<#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
```

تخفيف

تكوين MAC ثابت (ظاهري) على واجهات بيانات نظام المجموعة.

فشل الاتصالات الخاضعة لجهاز "بات"

الأعراض

مشاكل الاتصال لحركة المرور التي يتم نقلها بواسطة نظام المجموعة.

التحقق/التخفيف

- تأكد من نسخ التكوين نسخا متماثلا بشكل صحيح.
- تأكد من توزيع التجمع بالتساوي.
- تأكد من صحة ملكية التجمع.
- تأكد من إنشاء تدفقات الموجه/الموجه باستخدام المعلومات المنسوبة.
- التحقق من صحة ما إذا تم إنشاء وحدات النسخ الاحتياطي وتحديثها وتنظيفها كما هو متوقع.
- التحقق من صحة ما إذا تم إنشاء وحدات xlates وإنهاؤها وفقا لسلوك "لكل جلسة عمل".
- قم بتمكين "debug nat 2" للإشارة إلى أي أخطاء. ملاحظة، هذا المخرج يمكن أن يكون خاصا جدا، على سبيل المثال:

```
<#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
```

إلى تصحيح الأخطاء فاق:

```
<#root>
firepower#
```

```
un all
```

- قم بتمكين الاتصال وقوائم التحكم المرتبطة ب NAT لربط المعلومات باتصال فاشل.

تحسينات ASA و FTD لمجموعات PAT (ما بعد 9. 15 و 6. 7)

ما الذي تغير؟

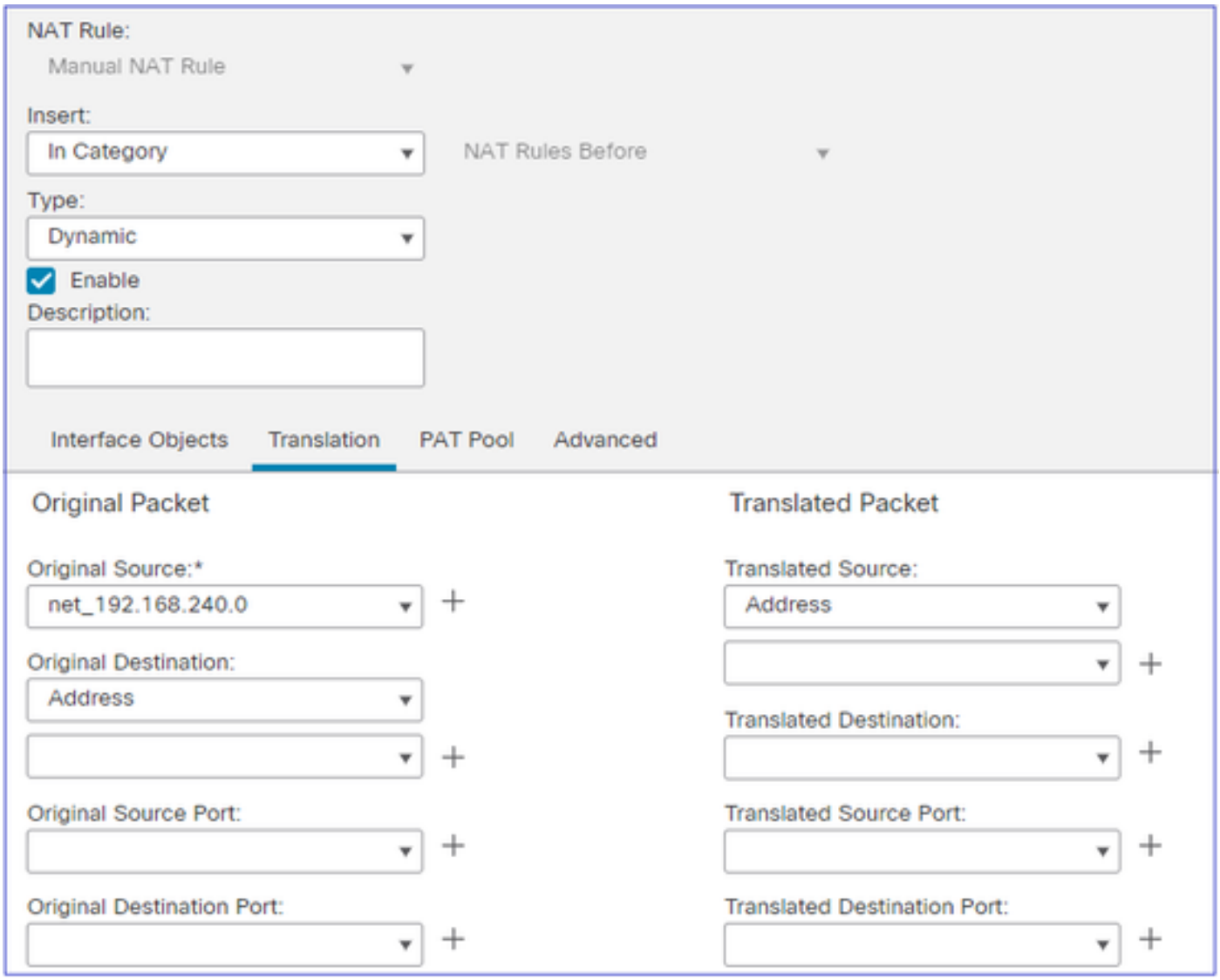
تم إعادة تصميم عملية PAT. لم تعد عناوين IP الفردية موزعة على كل عضو من أعضاء المجموعة. بدلاً من ذلك، يتم تقسيم IP (آت) ضرب إلى كتل أيسر وتوزيع تلك كتل أيسر بالتساوي (قدر الإمكان) بين أعضاء المجموعة، مع عملية لصق IP.

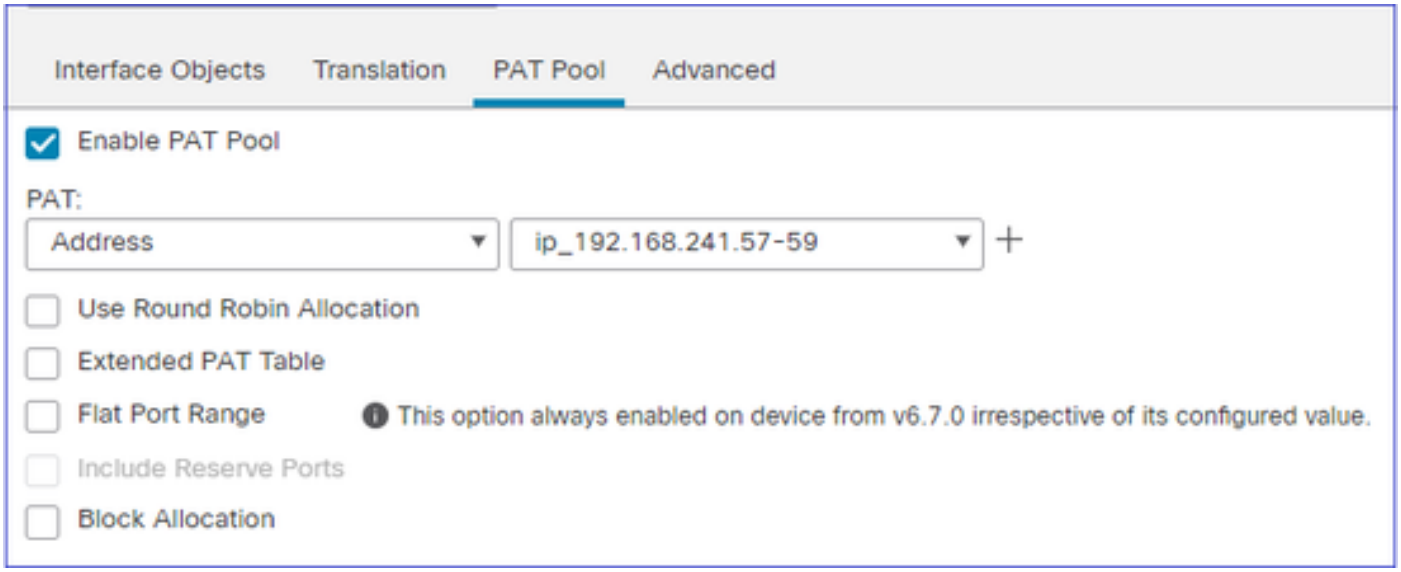
يعالج التصميم الجديد هذه القيود (راجع القسم السابق):

- تتأثر التطبيقات متعددة الجلسات بسبب عدم وجود لصاقة IP على مستوى المجموعة.
- يتطلب الأمر وجود تجمع PAT بالحجم يساوي على الأقل عدد العقد في نظام المجموعة.
- توزيع تجمع PAT يصبح غير متوازن حيث أن العقد تغادر/تنضم إلى نظام المجموعة.
- ال syslogs أن يشير إلى عدم توازن تجمع PAT.

من الناحية الفنية، بدلا من نطاقات المنافذ الافتراضية 1-511 و 512-1023 و 1024-65535، هناك الآن 1024-65535 نطاق المنفذ الافتراضي ل PAT. يمكن توسيع هذا النطاق ل PAT العادي (خيار "include-reserve") ليشمل نطاق المنفذ المميز 1-1023 الافتراضي.

هذا مثال على تكوين تجمع PAT على FTD 6.7. للحصول على تفاصيل إضافية، راجع القسم المرتبط في دليل التكوين:





معلومات إضافية حول أستكشاف الأخطاء وإصلاحها حول PAT

أنظمة مستوى بيانات FTD (POST-6.7/9.15.1)

يتم إنشاء syslog لإبطال صلاحية الملصق عندما يتم استنفاد جميع المنافذ في IP

الللاصق على عقدة نظام مجموعة، وينقل التوزيع إلى IP التالي المتاح مع المنافذ الحرة، على سبيل المثال:

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

يتم إنشاء syslog لعدم توازن التجمع على عقدة عند انضمامه إلى نظام المجموعة والا يحصل على أي من كتل المنافذ أو حصة غير متساوية منها، على سبيل المثال:

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

إظهار الأوامر

حالة توزيع التجمع

في إخراج ملخص تجميع الشبكة (NAT)، لكل عنوان IP للضرب، يجب أن يكون هناك فرق يزيد عن كتلة منفذ واحد عبر العقد في سيناريو توزيع متوازن. أمثلة على توزيع كتل المنافذ المتوازن وغير المتوازن.

```
<#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)
```

توزيع غير متوازن:

```
<#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 /
```

حالة ملكية التجمع

وأ كل امإ دحاو ذفنم ةلتك هنكان نوكي الأ بجي، ضرعلا عمجتل NAT ةعومجملا مظان جراخإ في ل UNKNOWN. إذا كان هنك واحد، فإنه يشير إلى مشكلة في الاتصال نسخ إحتياطي بملكية التجمع. مثال:

<#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>

محاسبة عمليات تخصيص المنفذ في كتل المنفذ

يتم تحسين الأمر show nat pool مع خيارات إضافية لعرض المعلومات التفصيلية وكذلك الإخراج الذي تمت تصفيته. مثال:

<#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 *
```

‘*’ يشير إلى أن هذه كتلة منفذ نسخ إحتياطي

لحل هذه المشكلة، أستخدم الأمر clear xlate global <ip> gport <start-end>لمسح بعض كتل المنافذ على العقد الأخرى يدويا إلى إعادة التوزيع إلى العقد المطلوبة.

إعادة توزيع كتل المنافذ يدويا

- في شبكة إنتاج ذات حركة مرور مستمرة، عندما تغادر عقدة النظام وتعيد وصله (ربما بسبب traceback)، قد تكون هناك حالات الى يمكنها فيها الحصول على حصة متساوية من التجمع، وأ في أسوأ الحالات، الى يمكنها الحصول على أي كتلة منفذ.
- أستخدم الأمر show nat pool cluster summary لتحديد العقدة التي تمتلك كتل منافذ أكثر من المطلوب.
- على العقد التي تمتلك المزيد من كتل المنافذ، أستخدم الأمر show nat pool ip <addr> detail للبحث عن كتل المنافذ التي تحتوي على أقل عدد من عمليات التخصيص.
- أستخدم الأمر clear xlate global <address> gport <start-end>لمسح الترجمات التي تم إنشاؤها من كتل المنافذ هذه بحيث تصبح متوفرة لإعادة التوزيع على العقد المطلوبة، على سبيل المثال:

<#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
```

الأسئلة المتداولة (FAQ) لما بعد 6.7/9.15.1 PAT

س. في حالة وجود عدد من عناوين IP المتاحة لعدد الوحدات المتاحة في المجموعة، هل يمكنني إستخدام عنوان IP واحد لكل وحدة كخيار؟

a. لم يعد، والا يوجد تبديل للتبديل بين مخططات توزيع التجمع المستندة إلى عناوين IP مقابل كتل المنافذ.

نتج عن النظام الأقدم لتوزيع تجمع IP المستند إلى عنوان حالات فشل تطبيقات متعددة الجلسات حيث يتم موازنة حمل الاتصالات المتعددة (التي تعد جزءا من معاملة تطبيق واحدة) من المضيف إلى وقع مخلفة من المجموعة، وبالتالي تتم ترجمتها بواسطة عنوان IP مع مخطط التوزيع الجديد القائم على حظر المنفذ، حتى وإن كنت تستطيع الآن العمل باستخدام عنوان IP ضرب واحد فقط، يوصى دائما بأن يكون لديك عناوين IP كافية ضرب استنادا إلى عدد الاتصالات المطلوبة لـ PATed.

س. هل لا يزال لديك مجموعة من عناوين IP لتجمع PAT الخاص بالمجموعة؟

أ. نعم، يمكنك. يتم توزيع كتل المنفذ من جميع عناوين IP الخاصة بتجمع PAT عبر وقع نظام المجموعة.

q. إذا كنت تستخدم عدد من عناوين IP لتجمع PAT، فهل يتم توفير نفس كتلة المنافذ لكل وضع لكل عنوان IP؟

أ. لا، يتم توزيع كل IP بشكل مستقل.

س. تحتوي جميع وقع نظام المجموعة على جميع عناوين IP العامة، ولكن تحتوي فقط على مجموعة فرعية من المنافذ؟ إذا كان هذا هو الحال، هل من المؤكد بعد ذلك أن المصدر IP يستخدم نفس IP العام؟

أ. ذلك صحيح، كل PAT IP مملوكة جزئيا لكل وقع. في حال استنفاد عنوان IP عام مختار على وقع، يتم إنشاء syslog الذي يشير إلى عدم إمكانية الاحتفاظ بعنوان IP الأصلي، ويتم توزيع إلى عنوان IP العام التالي المتاح. سواء كان نشر بروتوكول IP مستقر أو HA أو مجموعة، فإنه يتم دائما الحصول على أفضل الجهود وقف تواقر المجموعة.

q. هل لك شيء يستند إلى عنوان وحيد في المجموعة ضرب، غير أن الأطباق إن أكثر من واحد عنوان في المجموعة استعملت؟

a. يطبق وه إلى يتعدد عنوان في ضرب بركة أيضا. يتم توزيع كتل المنفذ من كل IP في تجمع PAT عبر جميع وقع نظام المجموعة. يتم تقسيم كل عنوان IP في تجمع PAT عبر الأعضاء في نظام المجموعة. لذلك، إذا كان لديك، فئة C من العناوين في تجمع PAT، فسيكون لكل عضو نظام مجموعة تجمعات منافذ من كل عنوان من عناوين تجمع PAT.

س. هل يعمل مع CGNAT؟

ألف - نعم، إن CGNAT مدعوم أيضا. يحتوي CGNAT، المعروف أيضا باسم PAT تخصيص الكتلة xlate. في حالة ضرب ديناميكي منظم (غير CGNAT)، يكون حجم الكتلة دائما '512' وهو ثابت وغير قابل للتكوين.

س. إذا غادرت الوحدة المجموعة، هل تقوم وقع التحكم بتخصيص نطاق كتلة المنفذ للوحدات الأخرى أو الاحتفاظ به لنفسها؟

أ. تحتوي كل كتلة منفذ على مالك ونسخة إحتياطية. في كل مرة يتم إنشاء xlate من كتلة منفذ، فإنه يتم أيضا نسخ نسخ متماثل إلى وقع النسخ الاحتياطي لكتلة المنفذ. عندما تترك وقع نظام المجموعة، تمتلك وقع النسخ الاحتياطي جميع كتل المنافذ وجميع

الاتصالات الحالية. تقوق عقدة النسخ الاحتياطي، منذ أن أصبحت مالك الكتلة للمنافذ الإضافية هذه، باختيار نسخ إحتياطية جديدة لها ونسخ كافة العناصر الحالية لتلك العقدة لمعالجة سيناريوهات الفشل.

س - أي إجراء يمكن إتخاذه على أساس هذا التنبيه لفرض اللصق؟

ألف - هناك سببان محتملان لعدم الحفاظ على اللصق.

السبب-1: تتم موازنة حركة المرور بشكل غير صحيح للتحميل نظرا لأن إحدى العقد ترى عدد أكبر من الاتصالات من العقد الأخرى، مما يؤدي إلى إستهلاك IP اللصق المعين. يمكن معالجة هذا الأمر إذا قمت بضمان توزيع حركة المرور بالتساوي عبر عقد نظام المجموعة. على سبيل المثال، في مجموعة FPR41xx، قم بتعديل خوارزمية موازنة الأحمال على المحولات المتصلة. في أي مجموعة FPR9300، تأكد من توفر عدد متساو من الخوادم النصلية عبر الهيكل.

السبب-2: إستخدام مجمع PAT منخفض جدا مما يؤدي إلى الإرهاق المتكرر للمسبح. لمعالجة هذا، قم بزيادة حجم تجمع PAT.

س. كيف يتم التعامل مع عدم الكلمة الأساسية الموسعة؟ هو يبدي خطأ، ويمنع الأمر كاملا nat أن يكون أضيفت أثناء التحسين، أو هو لا يزيل الكلمة موسع المفتاح، ويبدي تحذير؟

أ. خيار PAT الموسع غير مدعوم في نظام المجموعة من ASA 9.15.1/FP 6.7 وما بعده. لا تتم إزالة خيار التكوين من أي من CLI/ASDM/CSM/FMC. عند تكوينها (بشكل مباشر أو غير مباشر من خلال الترقية)، يتم إعلامك برسالة تحذير، ويتم قبول التكوين ولكن لا ترى الوظيفة الموسعة ل PAT في الإجراء.

س. هل هو نفس عدد الترجمات لكل الاتصالات المتزامنة؟

أ. في الفترة ما قبل 6.7/9.15.1، على الرغم من أنها كانت 1-65535، حيث أن منافذ المصدر لا يتم إستخدامها كثيرا في النطاق 1-1024، فإنها تجعل ذلك فعليا 1024-65535 (64512 conns). في التطبيق بعد 6.7/9.15.1 مع "ثابت" كسلوك افتراضي، هو 1024-65535. ولكن إذا كنت تريد إستخدام 1-1024، يمكنك مع خيار "include-reserve".

س. إذا كانت العقدة تنضم إلى نظام المجموعة مرة أخرى، فلديها عقدة النسخ الاحتياطي القديمة كنسخة إحتياطية وتعطي عقدة النسخ الاحتياطي تلك المنفذ القديمة الخاصة بها؟

أ. يعتمد على توفر تلك المنافذ في ذلك الوقت. عندما تترك عقدة نظام المجموعة، يتم نقل جميع تلك المنافذ الخاصة بها إلى عقدة النسخ الاحتياطي. ومن ثم تكون عقدة التحكم هي التي تجمع تلك المنافذ الحرة وتوزعها على العقد المطلوبة.

Q. إذا كان هناك تغيير في حالة عقدة التحكم، يتم إختيار عقدة تحكم جديدة، هل يتم الحفاظ على تخصيص كتلة PAT، أو يتم إعادة توزيع تلك المنافذ استنادا إلى عقدة التحكم الجديدة؟

ألف - تعرف عقدة المراقبة الجديدة أنواع الكتل التي تم تخصيصها وتلك التي هي حرة ومن أين تبدأ هناك.

س. هل الحد الأقصى لعدد الاتصالات المتزامنة مع هذا هو نفس الحد الأقصى لعدد مرات

السلوك الجديد؟

ج. نعم. يعتمد أقصى عدد من xlate على توفر منافذ ضرب. العلاقة له بالعدد الأقصى للاتصالات المتزامنة. إذا كنت تسمح بعنوان واحد فقط، فلديك 65535 اتصال ممكن. إذا كنت بحاجة إلى المزيد، فعليك تخصيص المزيد من عناوين IP. إذا كان هناك عدد كاف من العناوين/المنافذ، فيمكن الوصول إلى الحد الأقصى من الاتصالات المتزامنة.

س. ما هي عملية تخصيص كتلة المنفذ عند إضافة عضو مجموعة جديد؟ ماذا يحدث في حالة إضافة عضو المجموعة بسبب إعادة التشغيل؟

أ. يتم توزيع كتل المنفذ دائما بواسطة عقدة التحكم. يتم تخصيص كتل المنافذ لعقدة جديدة فقط عندما تكون هناك كتل منافذ حرة. تعني كتل المنافذ الحرة أنه لا يتم خدمة أي اتصال من خلال أي منفذ معين داخل كتلة المنفذ.

وعلاوة على ذلك، تقوم كل عقدة عند إعادة الانضمام بإعادة حساب عدد الكتل التي يمكنها امتلاكها. إذا كانت العقدة تحتوي على كتل أكثر مما يفترض بها، فإنها تطلق كتل منافذ إضافية إلى عقدة التحكم حتى وأين تصبح متوفرة. ثم تقوم عقدة التحكم بتخصيصها لعقدة البيانات المتصلة حديثا.

س. هل وهو مدعوم فقط بروتوكولات TCP و UDP وأ SCTP كذلك؟

أ. لم يتم دعم SCTP مطلقا بميزة PAT الديناميكية. لحركة مرور SCTP، التوصية هي إستخدام كائن شبكة ساكن إستاتيكي NAT فقط.

س. إذا نفذت عقدة من منافذ الحظر، هل تقوم بإسقاط الحزم والا تستخدم كتلة IP التالية المتاحة؟

أ. لا، لا يسقط فورا. وهي يستعمل يتوفر ميناء قالب من التالي ضرب ip. إن يكون all the ضرب IPs إستنفدت، بعد ذلك هو يسقط حركة مرور. ميناء قالب عبر all the

س. لتجنب الحمل الزائد لعقدة التحكم في نافذة ترقية نظام المجموعة، هل من الأفضل إختيار عنصر تحكم جديد يدوي في وقت سابق (على سبيل المثال، في منتصف الطريق من خلال ترقية نظام المجموعة المكونة من 4 وحدات)، بدلا من الانتظار حتى تتم معالجة كافة الاتصالات على عقدة التحكم؟

أ. يجب تحديث عنصر التحكم آخر مرة. وذلك لأنه، عندما تقوم عقدة التحكم بتشغيل الإصدار الأحدث، فإنها تقوم بدء توزيع التجمع إلا إذا تمت كافة العقد بتشغيل الإصدار الأحدث. بالإضافة إلى ذلك، عند تشغيل عملية ترقية، تتجاهل جميع عقد البيانات ذات الإصدار الأقدم. الأحدث رسائل توزيع التجمع من عقدة تحكم إذا كانت تقوم بتشغيل إصدار

ولتوضيح هذا الأمر بالتفصيل، يمكن النظر في نشر نظام مجموعة يحتوي على أربع عقد هي A و B و C و D مع إمكانية التحكم A. فيما يلي خطوات الترقية النموذجية المستمرة:

1. قم بتنزيل إصدار جديد على كل عقدة.
2. إعادة تحميل الوحدة "D". كافة الاتصالات، يتم نقل xlates إلى عقدة النسخ الاحتياطي.
3. تظهر وحدة "D" و:

أ. يعالج تشكيل PAT

ب. يقسم كل ضرب IP إلى كتل أيسر

ج. تحتوي على كافة كتل المنافذ في حالة غير معينة

د. تجاهل الإصدار الأقدم من رسائل PAT لنظام المجموعة المتلقاة من عنصر التحكم

هـ. يعيد توجيه كل إتصالات PAT إلى أساسي.

4. بالمثل، قم بإحضار عقد أخرى مع الإصدار الجديد.

5. إعادة تحميل عنصر تحكم الوحدة "A". انظر لعدم وجود نسخة إحتياطية للتحكم، يتم إسقاط جميع الاتصالات الموجودة

6. يبدأ عنصر التحكم الجديد في توزيع كتل المنافذ بالتنسيق الأحدث

7. تعود الوحدة "A" للربط وتكون قادرة على قبول رسائل توزيع كتلة المنفذ والعمل عليها

معالجة الأجزاء

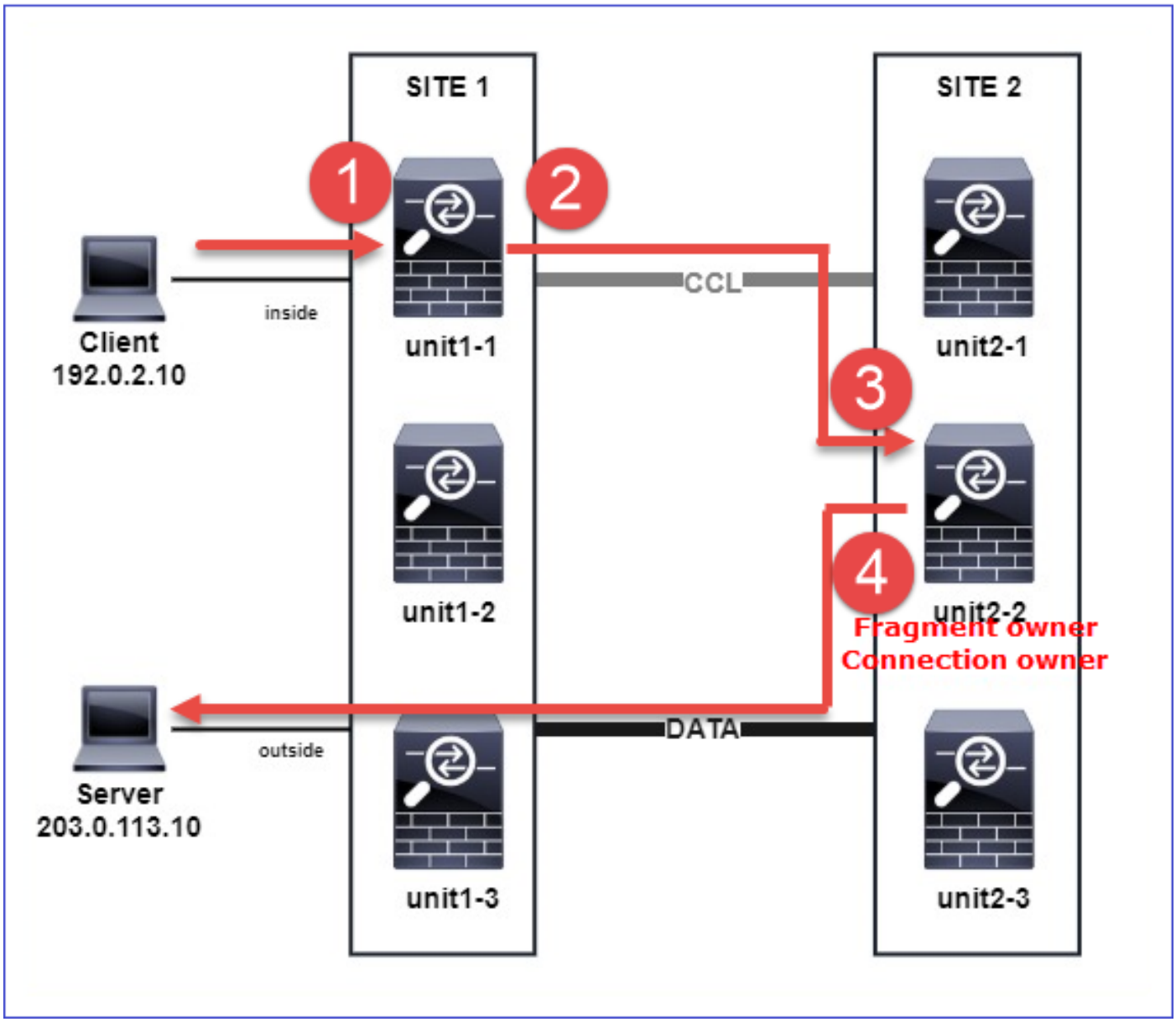
العرض

في عمليات نشر مجموعات المواقع المشتركة المجزأة التي يجب معالجتها في موقع واحد محدد (حركة مرور البيانات المحلية للموقع)، لا يزال من الممكن إرسالها إلى الوحدات في مواقع أخرى، حيث يمكن أن يكون لدى أحد هذه المواقع مالك الجزء.

في منطق المجموعة، يوجد دور إضافي محدد للاتصالات مع الحزم المجزأة: مالك الجزء.

بالنسبة للحزم المجزأة، تحدد وحدات نظام المجموعة التي تتلقى جزءا منها مالك الجزء استنادا إلى تجزئة عنوان IP لمصدر الجزء وعنوان IP للوجهة ومعرف الحزمة. ثم تتم إعادة توجيه جميع الأجزاء إلى مالك الجزء عبر إرتباط التحكم في نظام المجموعة. يمكن أن تكون الأجزاء متوازنة الأحمال لوحدات نظام المجموعة المختلفة لأن الجزء الأول فقط يتضمن الحزمة 5 المستخدمة في تجزئة موازنة حمل المحول. لا تحتوي الأجزاء الأخرى على منافذ المصدر والوجهة ويمكن أن تكون متوازنة الحمل لوحدات نظام المجموعة الأخرى. يقوم مالك الجزء بإعادة تجميع الحزمة مؤقتا حتى تتمكن من تحديد الموجه استنادا إلى تجزئة عنوان IP للمصدر/الوجهة والمنافذ. إذا كان اتصالا جديدا، يصبح مالك الجزء مالك الاتصال. إذا كان اتصالا موجودا، يقوم مالك الجزء بإعادة توجيه كافة الأجزاء إلى مالك الاتصال عبر إرتباط التحكم في نظام المجموعة. ثم يقوم مالك الاتصال بإعادة تجميع كافة الأجزاء.

ضع في الاعتبار هذا المخطط مع تدفق طلب صدى ICMP المجزأ من العميل إلى الخادم:



لفهم ترتيب العمليات، هناك التقاط حزم على مستوى المجموعة على الواجهات الداخلية والخارجية وواجهات إرتباط التحكم في المجموعة التي تم تكوينها باستخدام خيار التتبع. بالإضافة إلى ذلك، تم تكوين التقاط حزمة باستخدام خيار reinject-hide على الواجهة الداخلية.

<#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
```

ترتيب العمليات داخل المجموعة:

1. تتلقى الوحدة-1-1 في الموقع 1 حزم طلبات صدى ICMP المجأزة.

<#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. تختار الوحدة 1-1 الوحدة 2-2 في الموقع 2 كمالك للجزء وترسل إليه الحزم المجأزة.
الغاية {upper}mac address من الرطب يرسل من وحدة-1-1 إلى وحدة-2-2 ال MAC عنوان من ال CCL خطوة في وحدة-2-2.

<#root>

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


7 packets captured
1: 20:13:58.227817
0015.c500.018f 0015.c500.029f
 0x0800 Length: 1509

192.0.2.10 > 203.0.113.10
```

```
 icmp: echo request (wrong icmp csum) (frag 46772:1475@0+) (ttl 3)
1 packet shown

firepower#

show cap capccl packet-number 2 detail



7 packets captured

2: 20:13:58.227832

0015.c500.018f 0015.c500.029f

 0x0800 Length: 637


192.0.2.10 > 203.0.113.10

 (

frag 46772

:603@1480) (ttl 3)
1 packet shown


firepower#

cluster exec show interface po48 | i MAC


unit-1-1(LOCAL):*******************************************************
MAC address 0015.c500.018f, MTU 1500
unit-1-2:*******************************************************
MAC address 0015.c500.019f, MTU 1500


unit-2-2

:*******************************************************


MAC address 0015.c500.029f, MTU 1500


unit-1-3:*******************************************************
MAC address 0015.c500.016f, MTU 1500
unit-2-1:*******************************************************
MAC address 0015.c500.028f, MTU 1500
unit-2-3:*******************************************************
MAC address 0015.c500.026f, MTU 1500
```

3. حيث تستقبل الوحدة 2-2، وتعيد تجميع الحزم المجزأة، وتصبح مالكة التدفق.

```
<#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. تسمح الوحدة 2-2 بالحزم استنادا إلى سياسة الأمان وترسلها، عبر الواجهة الخارجية، من الموقع 2 إلى الموقع 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
```

الملاحظات/التحذيرات

- خلاف دور المدير، لا يمكن ترجمة مالك الجزء ضمن موقع معين. يتم تحديد مالك الجزء بواسطة الوحدة التي تتلقى في الأصل الحزمة المجزأة لاتصال جديد ويمكن تحديد موقعها في أي موقع.
- وبما أن مالك الجزء يمكن أن يصبح أيضا مالك الاتصال، بعد ذلك in order to أرسلت الرد إلى المضيف الوجهة، وهو ينبغي كنت يمكن أن يحل المخرج قارن، والعثور على عناوين IP و MAC من الغاية مضيف أو الخطوة التالية. يفترض هذا أنه يجب أن تحتوي

الخطوة (الخطوات) التالية أيضا على إمكانية الوصول إلى مضيف الوجهة.

- لإعادة تجميع الحزم المجزأة يحتفظ ASA/FTD بوحدة إعادة تجميع جزء IP لكل واجهة مسماة. لعرض البيانات التشغيلية لوحدة إعادة تجميع جزء IP، أستخدم الأمر 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
```

في عمليات نشر نظام المجموعة، يقوم مالك الجزء أو مالك الاتصال بوضع الحزم في المجزأة في قائمة انتظار الأجزاء. حجم قائمة انتظار الجزء محدود بقيمة عداد الحجم <nameif> <size> الذي تم تكوينه باستخدام الأمر حجم الجزء (200 بشكل افتراضي). عندما يصل حجم قائمة انتظار الأجزاء إلى 2/3 من الحجم، يتم إعتبار حد قائمة انتظار الأجزاء متجاوزا، ويتم إسقاط أي أجزاء جديدة ليست جزءا من سلسلة الأجزاء الحالية. في هذه الحالة، يتم زيادة حد قائمة انتظار التجزئة، ويتم إنشاء رسالة 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 203.0.11
```

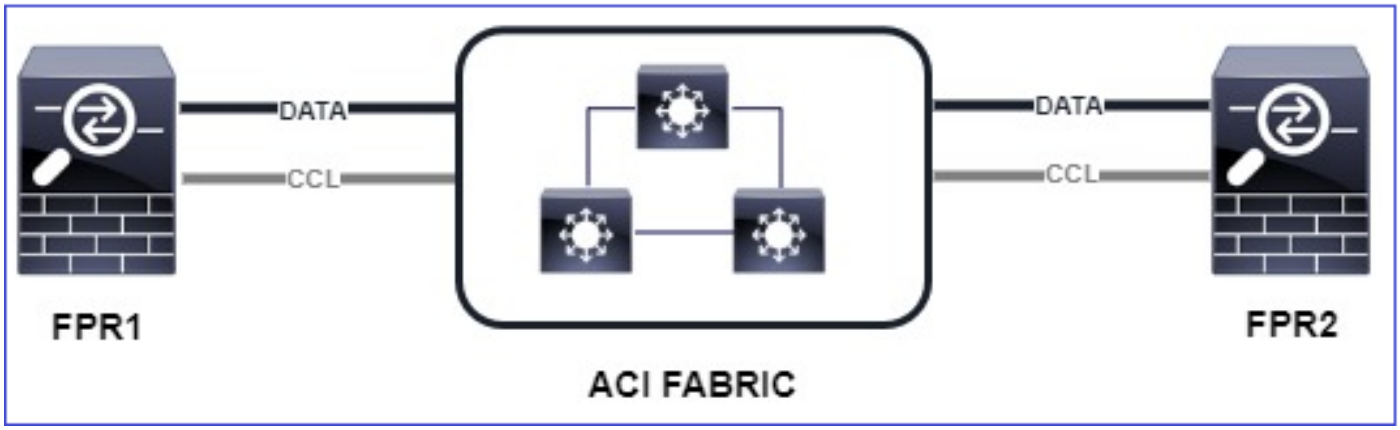
كحل بديل، قم بزيادة الحجم في مركز إدارة FirePOWER > الأجهزة > إدارة الأجهزة > [تحرير الجهاز] > [تحرير الجهاز] > الواجهات > [الواجهة] > خيارات متقدمة > تكوين الأمان > تجاوز الإعداد الافتراضي للجزء، واحفظ سياسات التكوين والنشر. ثم قم بمراقبة عداد قائمة الانتظار في إخراج الأمر show fragment وتكرار ظهور رسالة syslog FTD-3-209006.

مشاكل ACI

مشكلات التوصيل المتقطع من خلال المجموعة بسبب التحقق النشط من المجموع الاختباري من المستوى الرابع في ACI Pod

العرض

- مشكلات التوصيل المتقطع من خلال مجموعة ASA/FTD التي تم نشرها في نقطة وصول (ACI) خاصة بالبنية الأساسية المركزة على التطبيقات.
- في حالة وجود وحدة واحدة فقط في المجموعة، لا تتم ملاحظة مشكلات الاتصال.
- لا تظهر الحزم المرسلة من وحدة نظام مجموعة واحدة إلى وحدة أو أكثر من الوحدات الأخرى في نظام المجموعة في FXOS والتقاط مستوى البيانات للوحدات المستهدفة.



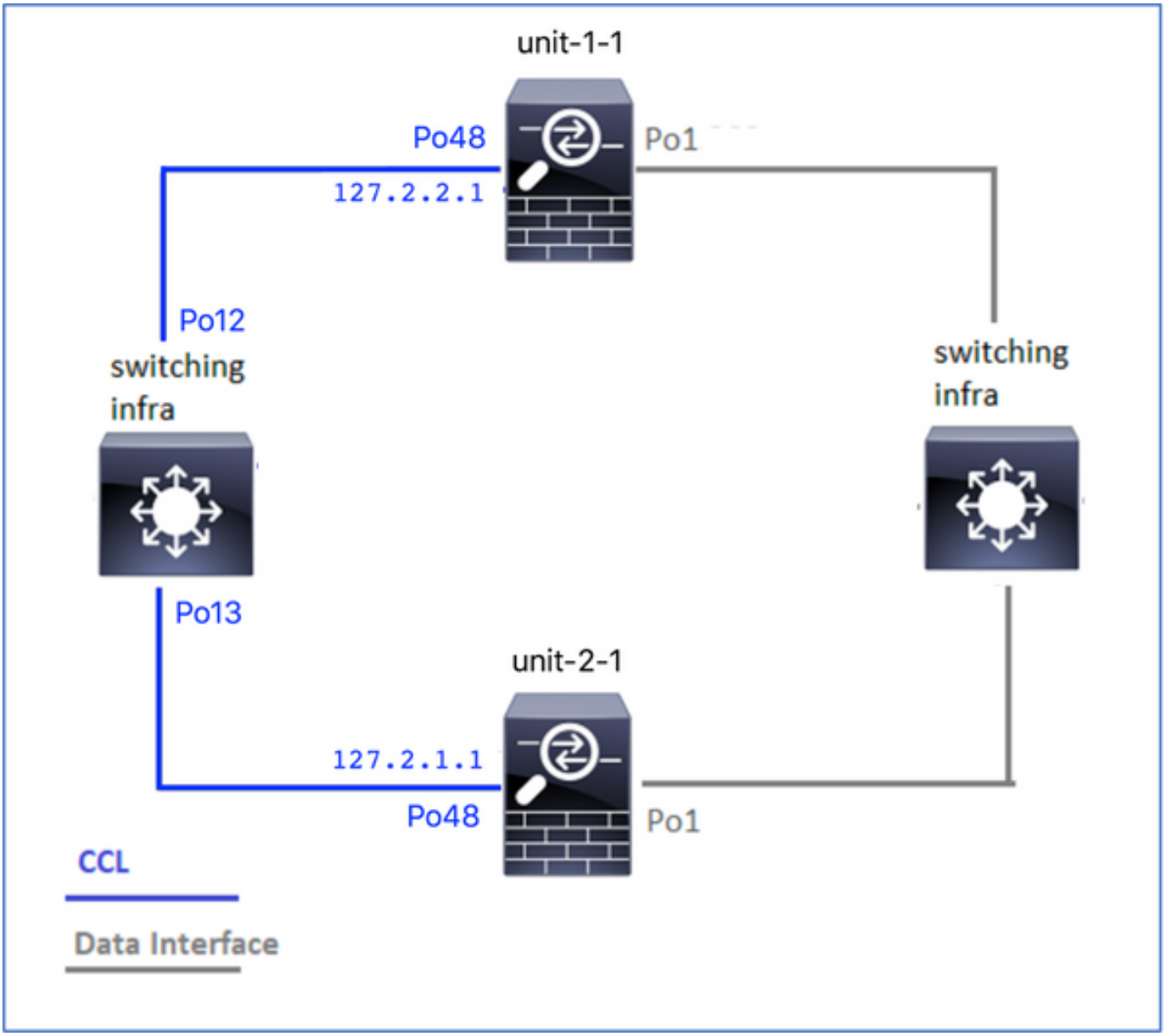
تخفيف

- لا تحتوي حركة المرور التي تمت إعادة توجيهها عبر إرتباط التحكم في نظام المجموعة على المجموع الاختباري الصحيح للمستوى 4 وهذا السلوك المتوقع. يجب ألا تتحقق المحولات الموجودة على مسار إرتباط التحكم في نظام المجموعة من المجموع الاختباري L4. يمكن أن تتسبب المحولات التي تتحقق من المجموع الاختباري L4 في إسقاط حركة المرور. تحقق من تكوين محول بنية قائمة التحكم في الوصول (ACI) وتأكد من عدم تنفيذ المجموع الاختباري L4 على الحزم المستلمة أو المرسلة عبر إرتباط التحكم في نظام المجموعة.

مشاكل مستوى التحكم في نظام المجموعة

يتعذر على الوحدة الانضمام إلى نظام المجموعة

حجم MTU على CCL



الأعراض

يتعذر على الوحدة الانضمام إلى نظام المجموعة ويتم عرض هذه الرسالة:

```
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
```

التحقق/التخفيف

- أستخدم الأمر show interface على FTD، للتحقق من أن وحدة الحد الأقصى للنقل (MTU) على واجهة إرتباط التحكم في نظام المجموعة أعلى بمقدار 100 بايت على الأقل من وحدة

الحد الأقصى للنقل (MTU) الخاصة بواجهة البيانات:

```
<#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.
```

- قم بإجراء إختبار اتصال من خلال CCL، باستخدام خيار الحجم، للتحقق من أنه تم تكوين MTU CCL على جميع الأجهزة الموجودة في المسار بشكل صحيح على جميع الأجهزة الموجودة في المسار.

```
<#root>

firepower#

ping 127.2.1.1 size 9184
```

- أستخدم الأمر show interface على المحول للتحقق من تكوين MTU

```
<#root>
```

```
Switch#
```

show interface

port-channel12

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

MTU 9084

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

port-channel13

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

MTU 9084

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

عدم تطابق الواجهة بين وحدات نظام المجموعة

الأعراض

يتعذر على الوحدة الانضمام إلى نظام المجموعة ويتم عرض هذه الرسالة:

```
Interface mismatch between cluster primary and joining unit unit-2-1. unit-2-1 aborting cluster join.
Cluster disable is performing cleanup..done.
Unit unit-2-1 is quitting due to system failure for 1 time(s) (last failure is Internal clustering erro
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clust
```

التحقق/التخفيف

قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) الخاصة ب FCM على كل هيكل، وتصفح إلى علامة التبويب الواجهات، والتحقق من أن جميع أعضاء نظام المجموعة لديهم تكوين الواجهة نفسه:

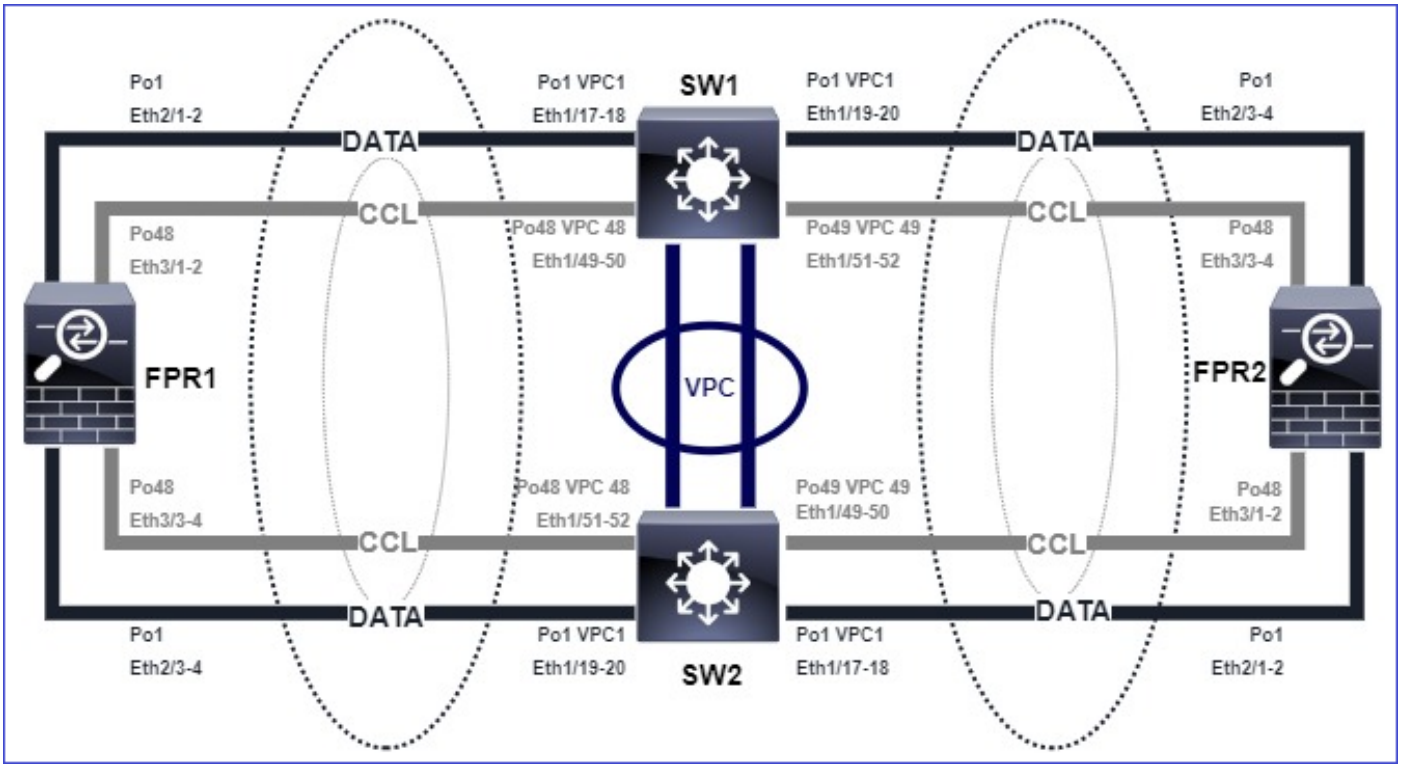
- الواجهات التي تم تعيينها للجهاز المنطقي
- سرعة المؤول للواجهات
- إدارة الوجهات
- حالة الواجهة

مشكلة واجهة قناة البيانات/Port

انقسام الدماغ بسبب مشاكل إمكانية الوصول عبر CCL

العرض

توجد وحدات تحكم متعددة في المجموعة. خذ بعين الاعتبار هذا الهيكل:



الهيكل 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
```

الهيكل رقم 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
```

التحقق

- أستخدم الأمر ping للتحقق من الاتصال بين عناوين IP الخاصة باتباط التحكم في المجموعة (CCL) الخاصة بوحدات التحكم:

```
<#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)
```

- تحقق من جدول ARP:

```
<#root>

firepower# show arp


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

- في وحدات التحكم، قم بتكوين عمليات الالتقاط والتحقق منها على واجهات 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
```

تخفيف

- ضمنت أن ال CCL ميناء قارن ربطت إلى منفصل قناة قارن على المفاتيح.
- عند إستخدام قنوات المنفذ الظاهرية (vPC) على محولات Nexus، فتأكد من اتصال واجهات قناة منفذ CCL ب vPC مختلف ومن عدم فشل تكوين vPC في حالة التناسق.

- ضمنت أن ال CCL ميناء قارن في ال نفسه بث مجال وأن ال CCL VLAN خلقت وسمحت عل ى القارن.

هذا نموذج لتكوين المحول:

```
<#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

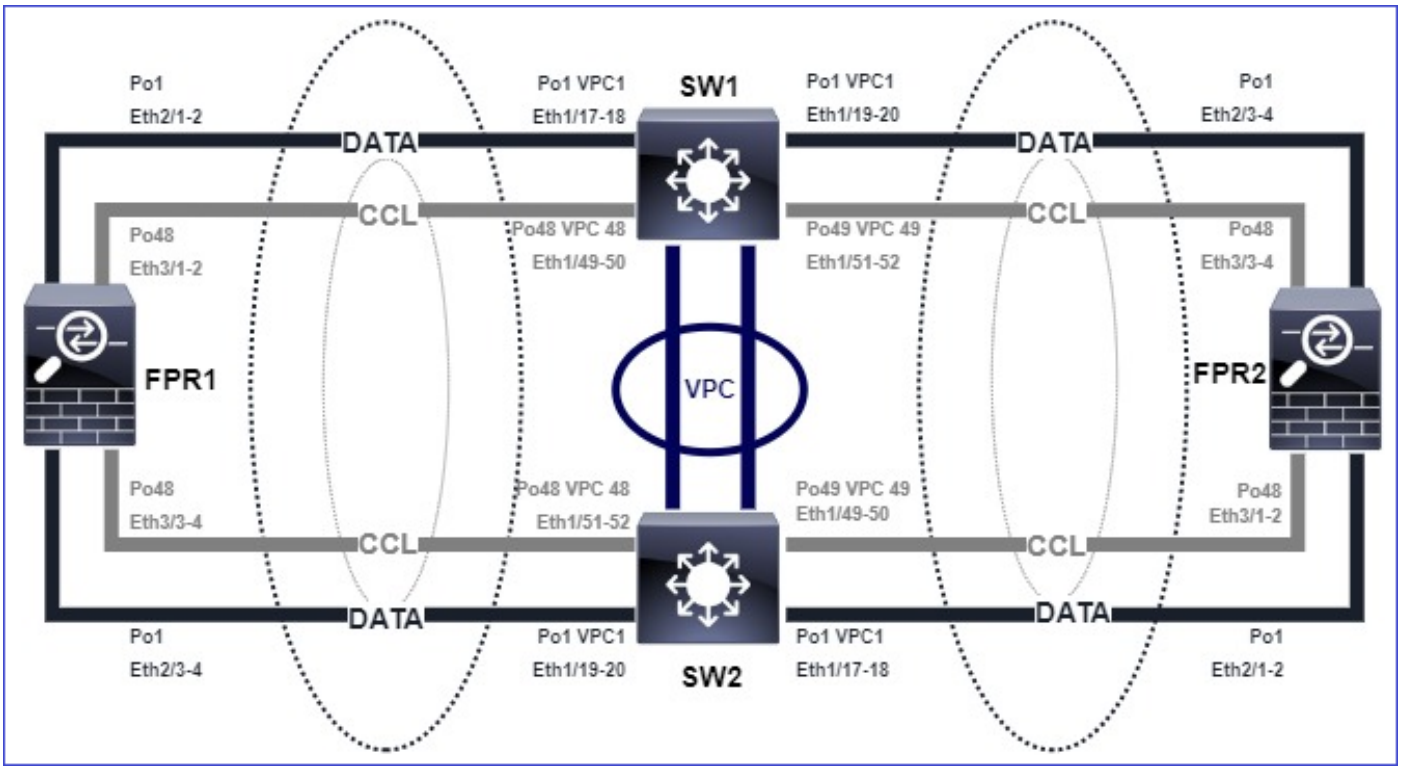
49 Po49 up success success 48

نظام مجموعة معطل بسبب واجهات قناة منفذ البيانات المعلقة

العرض

يتم إيقاف واجهة واحدة أو أكثر من واجهات قناة منفذ البيانات مؤقتا. عند إيقاف تشغيل واجهة بيانات تم تمكينها إداريا، يتم إستبعاد جميع وحدات نظام المجموعة الموجودة في نفس الهيكل من نظام المجموعة بسبب فشل التحقق من صحة الواجهة.

خذ بعين الاعتبار هذا الهيكل:



التحقق

- تحقق من وحدة تحكم وحدة التحكم:

<#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.
```

- تحقق من مخرجات محفوظات نظام المجموعة وأوامر show cluster info trace module hc في الوحدة (الوحدات) المتأثرة:

<#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 cluste

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

- فحصت الإنتاج من العرض ميناء-channel الخاصة أمر في ال fxos أمر shell:

<#root>

FPR2(fxos)#

show port-channel summary

Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
S - Switched R - Routed
U - Up (port-channel)
M - Not in use. Min-links not met

Group Port-Channel Type Protocol Member Ports

---

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

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

تخفيف

- تأكد من أن جميع الهياكل لها نفس اسم مجموعة نظام المجموعة وكلمة المرور.
- تأكد من أن واجهات قناة المنفذ تحتوي على واجهات عضو مادية مكنة إداريا مع تكوين السرعة/الإرسال ثنائي الإتجاه نفسه في جميع الهياكل والمحولات.
- في المجموعات داخل الموقع، تضمن أن نفس البيانات ميناء-channel قارن في كل هيكل يكون ربطت إلى ال نفسه قناة قارن على المفاتح.
- عند إستخدام قنوات المنفذ الظاهرية (vPC) في محولات Nexus، فتأكد من أن تكوين vPC ال يحتوي على حالة التناسق الفاشلة.
- في المجموعات داخل الموقع، تأكد من أن نفس واجهة قناة منفذ البيانات في كل الهيكل متصلة بنفس vPC.

مشاكل إستقرار نظام المجموعة

نظام التشغيل FXOS Traceback

العرض

الوحدة تترك المجموعة.

التحقق/التخفيف

- أستخدم الأمر show cluster history" لمعرفة متى غادرت الوحدة نظام المجموعة

<#root>

```
firepower#
show cluster history
```

- أستخدم هذه الأوامر للتحقق مما إذا كان لـ FXOS traceback

```
<#root>
FPR4150#
connect local-mgmt

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

- تجميع الملف الأساسي الذي تم إنشاؤه حول الوقت الذي غادرت فيه الوحدة نظام المجموعة وتوفيره إلى TAC.

القرص ممتلئ

في حالة وصول إستخدام القرص في قسم /ngfw الخاص بوحدة نظام المجموعة إلى 94٪ تقوم الوحدة بالإخلاء من نظام المجموعة. يتم التحقق من إستخدام القرص كل 3 ثوان:

```
<#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
```

في هذه الحالة، يظهر إخراج محفوظات نظام المجموعة show:

```
<#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
```

وأ

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

هناك طريقة أخرى للتحقق من الفشل وهي:

<#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
```

بالإضافة إلى ذلك، إذا كان القرص حوالي 100٪، فقد تواجه الوحدة صعوبات في إسترجاع نظام المجموعة حتى يتم تحرير بعض مساحة القرص.

الحماية ضد التدفق

كل 5 دقائق تقوم كل وحدة مجموعة بالتحقق من وحدة المعالجة المركزية (CPU) ووحدة النظير المحلية للتحقق من إستخدام وحدة المعالجة المركزية (CPU) والذاكرة. إذا كان الاستخدام

أعلى من حدود النظام (LINA CPU 50٪ وأ LINA ذاكرة 59٪) يتم عرض رسالة إعلامية في:

- Syslogs (FTD-6-748008)
- ملف log/cluster_trace.log، على سبيل المثال:

```
<#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
```

تشير الرسالة إلى أنه في حالة فشل وحدة ما، يمكن زيادة الاشتراك في موارد الوحدة (الوحدات) الأخرى.

الوضع المبسط

السلوك في إصدارات ما قبل 6.3 FMC

- يمكنك تسجيل كل عقدة نظام مجموعة بشكل فردي على FMC.
- ثم تقوم بتكوين مجموعة منطقية في FMC.
- لكل إضافة جديدة لعقدة نظام المجموعة، يجب عليك تسجيل العقدة يدويا.

بعد 6.3 FMC

- تتيح لك ميزة الوضع المبسط إمكانية تسجيل نظام المجموعة بالكامل على وحدة (قم فقط بتسجيل أي عقدة واحدة من مجموعة نظام) في خطوة واحدة في إدارة الهيكل (FMC) التحكم.

الحد الأدنى للمدير المدعوم	الأجهزة المدارة	الحد الأدنى لإصدار الجهاز المدار المدعوم المطلوب	ملاحظات
FMC 6.3	مجموعات FTD في FP4100 و FP9300 فقط	6.2.0	هذه ميزة في وحدة التحكم في إدارة الهيكل (FMC) فقط

تحذير: بمجرد تكوين نظام المجموعة في FTD، يجب الانتظار حتى يبدأ التسجيل التلقائي. يجب عدم محاولة تسجيل عقد نظام المجموعة يدويا (إضافة جهاز) ولكن إستخدام خيار التسوية.

العرض

حالات فشل تسجيل العقد

- إذا فشل تسجيل عقدة التحكم لأي سبب، فسيتم حذف نظام المجموعة من FMC.

تخفيف

إذا فشل تسجيل عقدة البيانات لأي سبب، فهناك خياران:

1. مع كل عملية نشر يتم إجراؤها على نظام المجموعة، تتحقق FMC مما إذا كانت هناك عقد نظام مجموعة تحتاج إلى التسجيل، ومن ثم تبدأ في التسجيل التلقائي لهذه العقد.
2. هناك خيار تسوية متوفر ضمن عالمة التبويب ملخص نظام المجموعة (الأجهزة > إدارة الأجهزة > عالمة التبويب نظام المجموعة > عرض إرتباط حالة نظام المجموعة). بمجرد تشغيل إجراء التسوية، تبدأ FMC التسجيل التلقائي للعقد التي يلزم تسجيلها.

معلومات ذات صلة

- التجميع الخاص بالدفاع ضد تهديد قوة النيران
- مجموعة ASA لهيكل Firepower 4100/9300
- حول التجميع على هيكل Firepower 4100/9300
- الغطس العميق لميزة التجميع في جدار الحماية من الجيل التالي Firepower - BRKSEC-3032
- تحليل لقطات Firepower Firewall (جدار حماية Firepower) لاستكشاف مشكلات الشبكة وإصلاحها بشكل فعّال

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).