ترحيل FTD HA (تجاوز الفشل) إلى FMC أخرى

المحتويات

المقدمة

يوضح هذا المستند إجراء ترحيل FTD HA من وحدة تحكم في الإدارة الأساسية (FMC) موجودة إلى وحدة تحكم في الإدارة الأساسية (FMC) أخرى.

للحصول على ترحيل مستقل لجدار الحماية إلى فحص FMC جديد
https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense/222480-migrate-an-ftd-from-one-fmc-to-another-f.html

الاختصارات

ACP = سياسة التحكم في الوصول

ARP = بروتوكول تحليل العنوان

CLI = واجهة سطر الأوامر

FMC = مركز إدارة جدار الحماية الآمن

FTD = الدفاع الآمن ضد تهديد جدار الحماية

GARP = ARP مجاني

HA = الإتاحة العالية

MW = إطار الصيانة

UI = واجهة المستخدم

المتطلبات الأساسية

قبل بدء عملية الترحيل، تأكد من توفر المتطلبات الأساسية التالية:

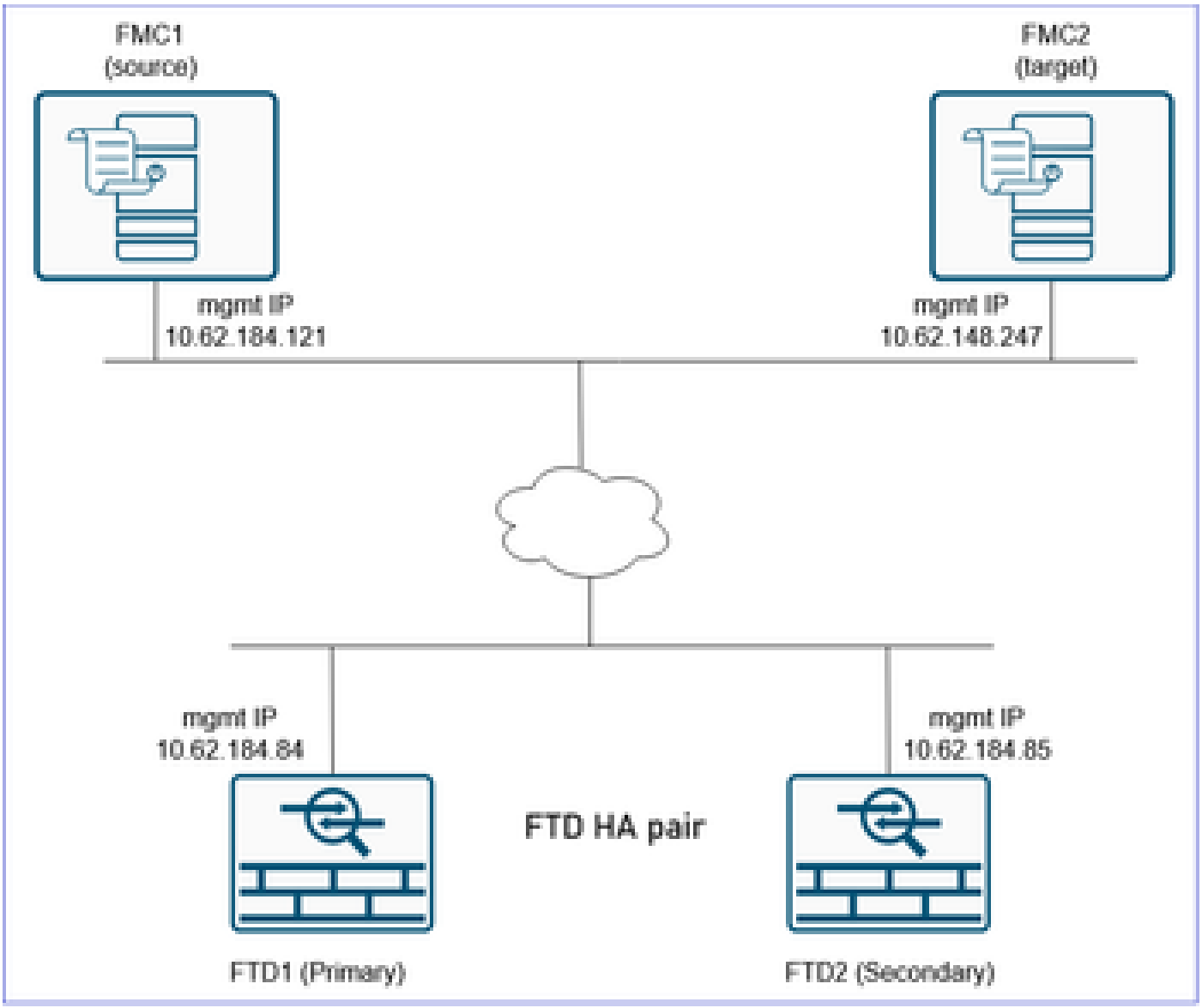
- وصول UI و CLI إلى كل من المصدر والوجهة FMCs.
- المسوغات الإدارية لكل من FMCs وجدران الحماية.
- وصول وحدة التحكم إلى كل من جدران الحماية.
- الوصول إلى أجهزة تدفق البيانات من الخادم إلى الخادم من المستوى الثالث (في حالة الحاجة إلى مسح ذاكرة تخزين ARP المؤقت).
- تأكد من أن الغاية/الهدف FMC له نفس إصدار المصدر/القديم FMC.
- تأكد من أن الغاية/الهدف FMC له نفس التراخيص الخاصة بالمصدر/FMC القديم.
- تأكد من ترتيب MW لتنفيذ عملية الترحيل لأنها ستؤثر على حركة المرور العابرة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Secure Firewall 31xx، الإصدار 7.4.2.2.
- Secure Firewall Management Center، الإصدار 7.4.2.2.
- 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.

المخطط



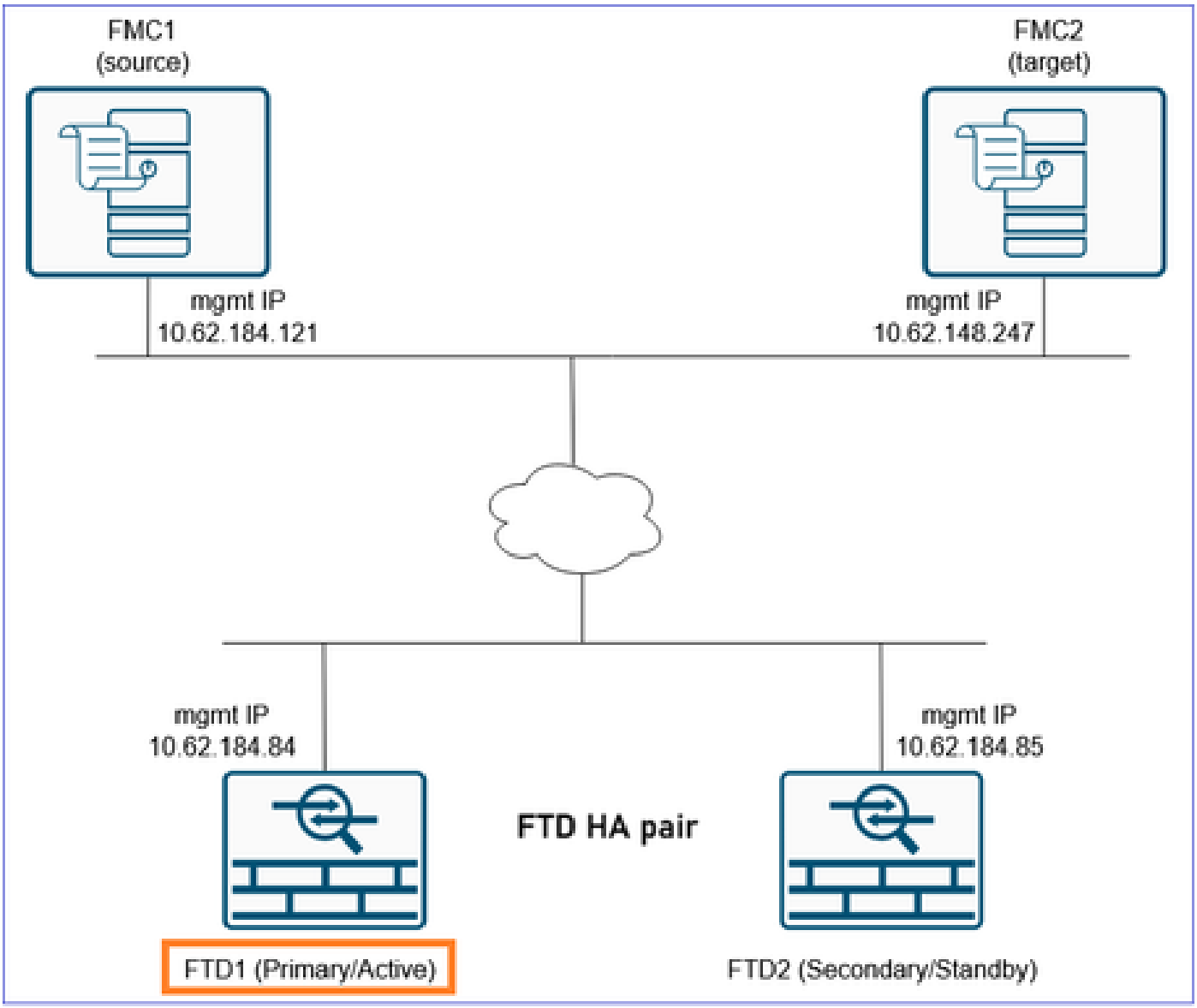
التكوين

خطوات الترحيل

بالنسبة لهذا السيناريو، فإننا نعتبر هذه الحالات:

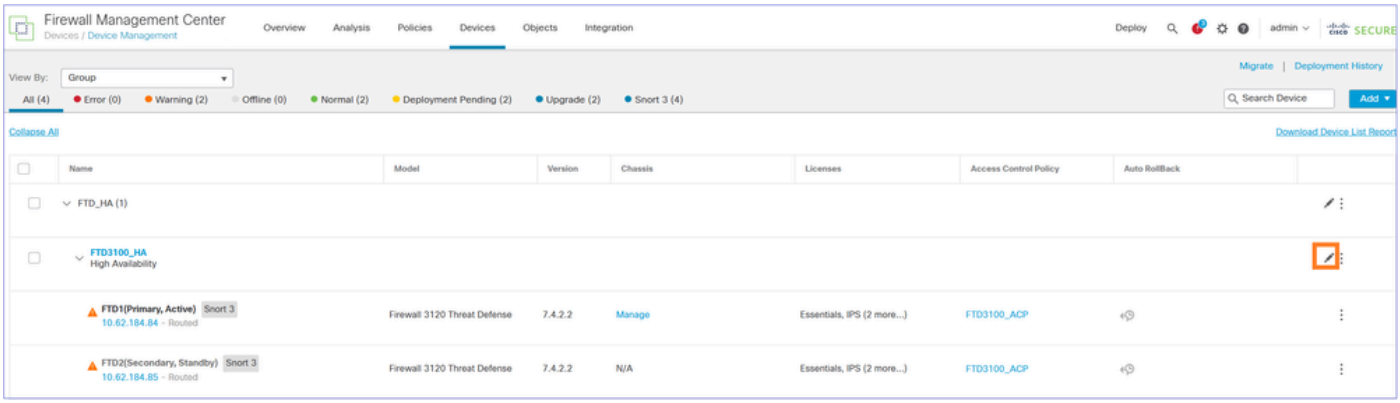
بروتوكول FTD1: أساسي/نشط

بروتوكول FTD2: ثانوي/وضع الاستعداد

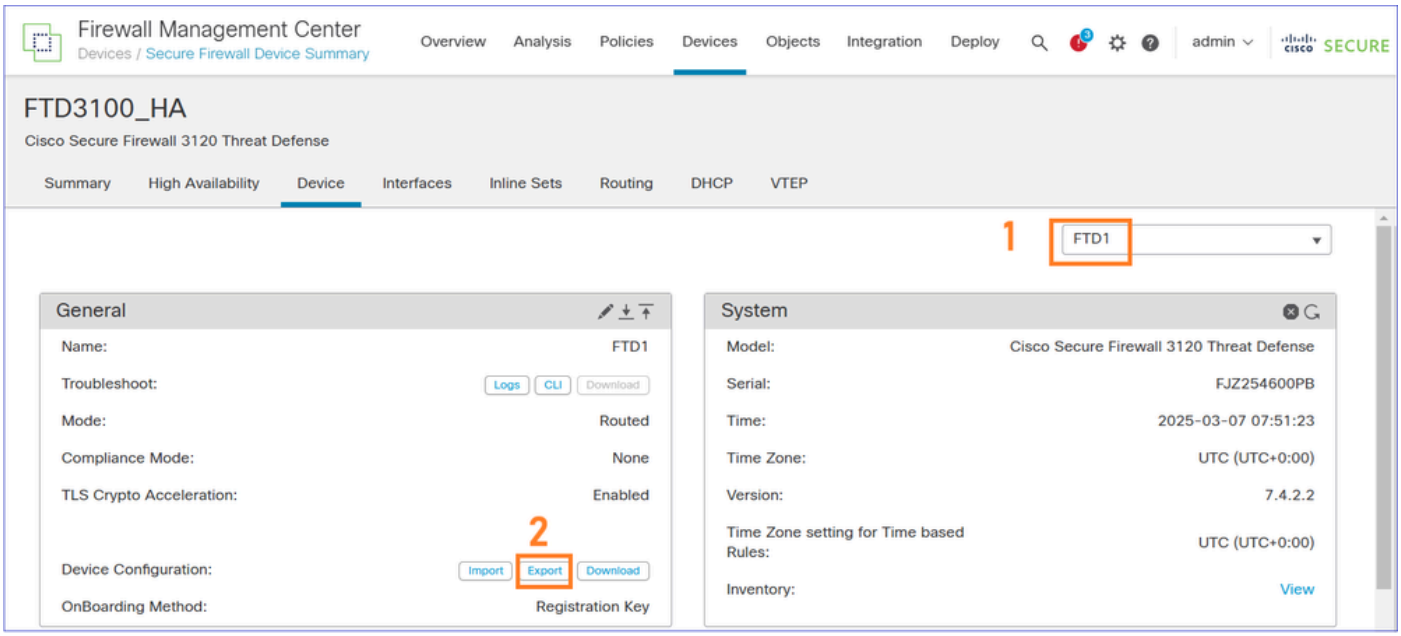


الخطوة 1. تصدير تكوين الجهاز من جدار الحماية الأساسي

على FMC1 (مصدر FMC)، انتقل إلى الأجهزة > إدارة الأجهزة. حدد زوج FTD HA وحدد تحرير:

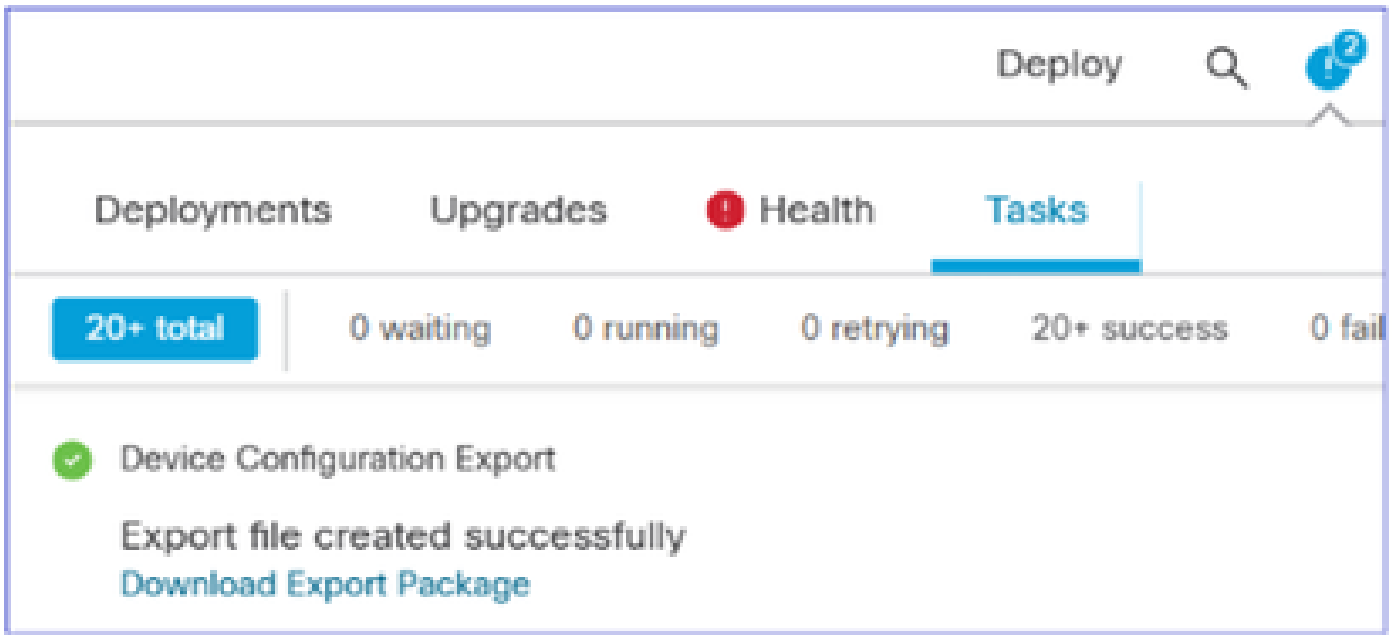


انتقل إلى علامة التبويب الجهاز. تأكد من تحديد FTD الأساسي/النشط (FTD1 في هذه الحالة) وحدد تصدير لتصدير تكوين الجهاز:



ملاحظة: يتوفر خيار التصدير اعتبارا من إصدار البرنامج 7.1 والإصدارات الأحدث.

يمكنك الانتقال إلى صفحة الإعلامات > المهام لضمان اكتمال التصدير. ثم حدد حزمة تنزيل التصدير:



بدلا من ذلك، يمكنك النقر فوق الزر تنزيل في منطقة عام. يمكنك الحصول على ملف sfo، على سبيل المثال DeviceExport-cc3fdc40-f9d7-11ef-bf7f-6c8e2fc106f6.sfo

يحتوي الملف على تكوين مرتبط بالجهاز مثل:

- الواجهات المهيأة
- مجموعات في السطر
- توجيه
- DHCP
- VTEP

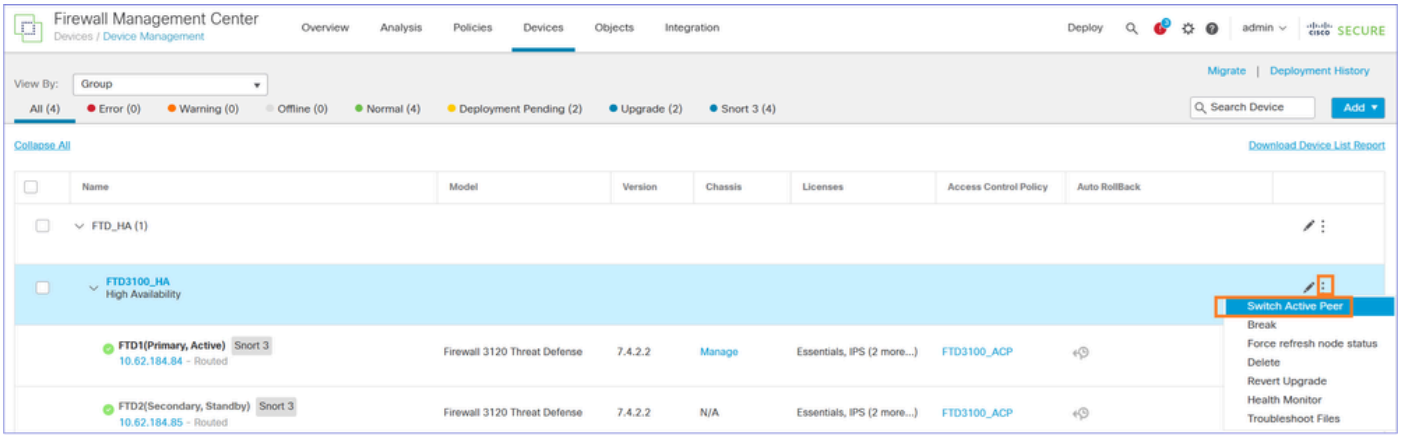
- الكائنات المرتبطة

ملاحظة: يمكن إستيراد ملف التكوين المصدر مرة أخرى إلى FTD نفسه فقط. يجب أن يتطابق UUID الخاص ب FTD مع محتوى ملف sfo المستورد. نفس FTD يستطيع كنت استوردت. مبرد يستطيع كنت sfo و FMC آخر على سجلت

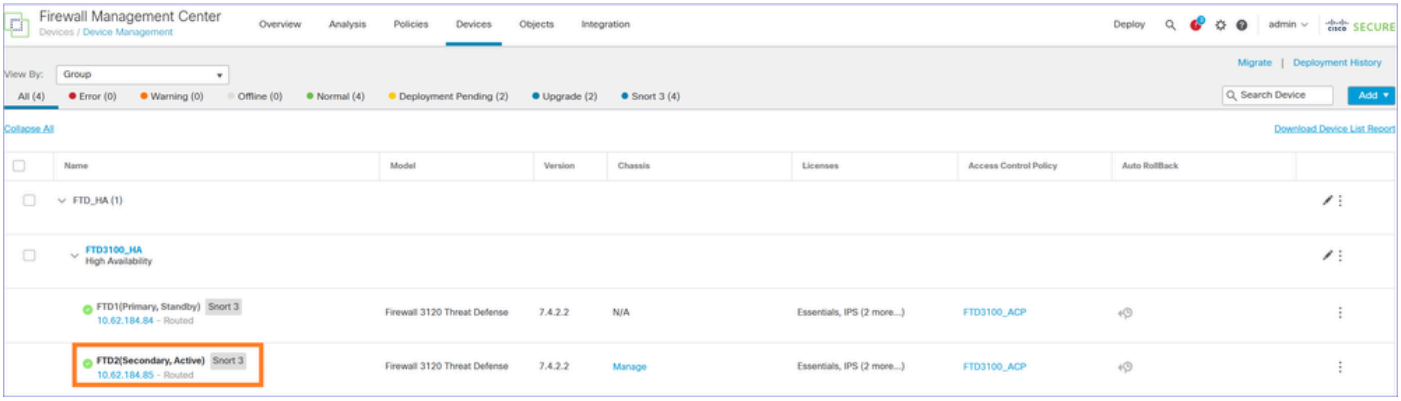
المرجع: 'تصدير واستيراد تكوين الجهاز' https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/get-started-device-settings.html#Cisco_Task.dita_7ccc8e87-6522-4ba9-bb00-eccc8b72b7c8

الخطوة 2. جعل FTD الثانوي نشط

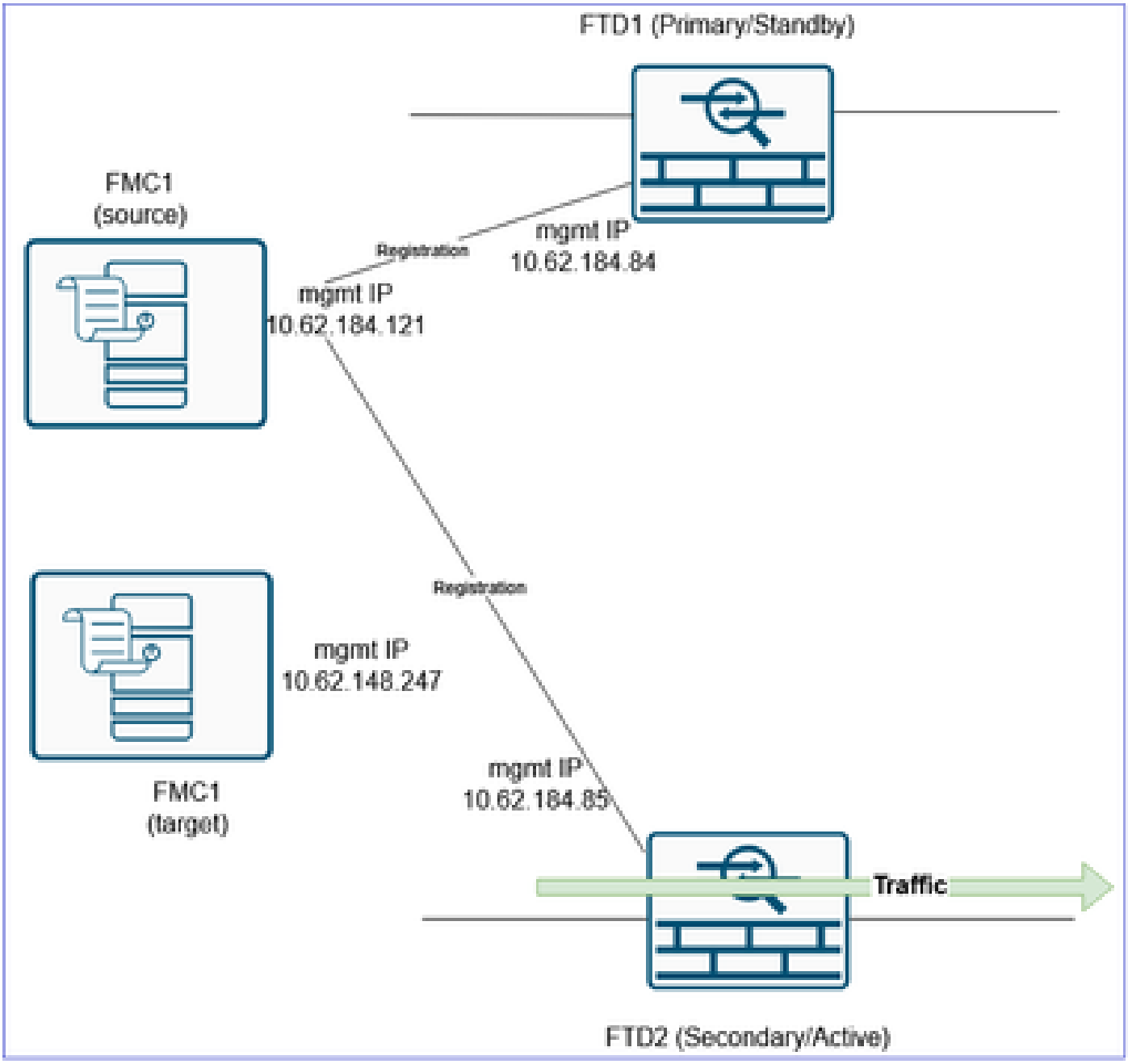
انتقل إلى الأجهزة > إدارة الأجهزة، وحدد زوج FTD HA، وحدد الوزوج النشط للمحول:



تتمثل النتيجة في FTD1 (أساسي/إحتياطي) و FTD (ثانوي/نشط):

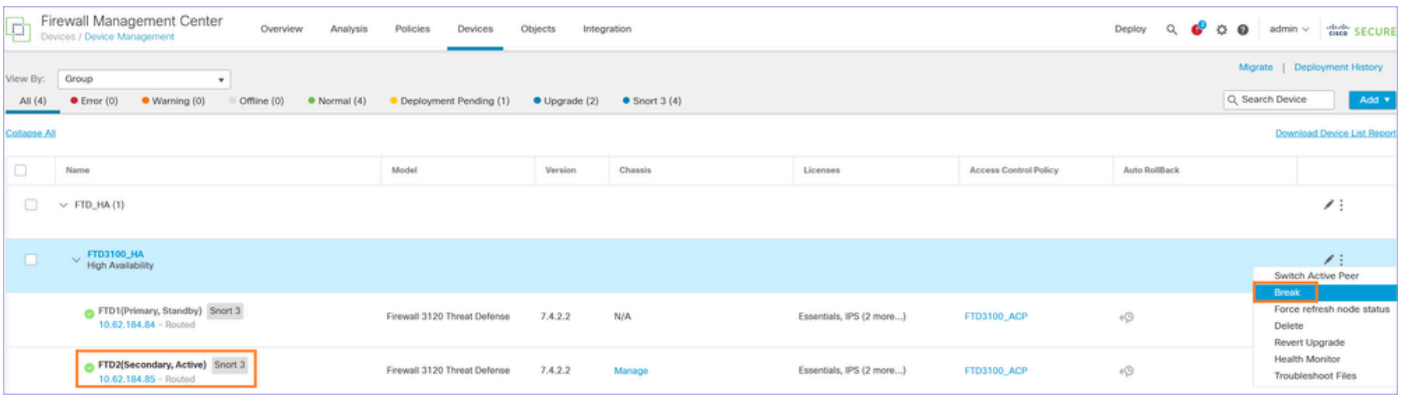


تتم الآن معالجة حركة المرور بواسطة FTD الثانوي/النشط:

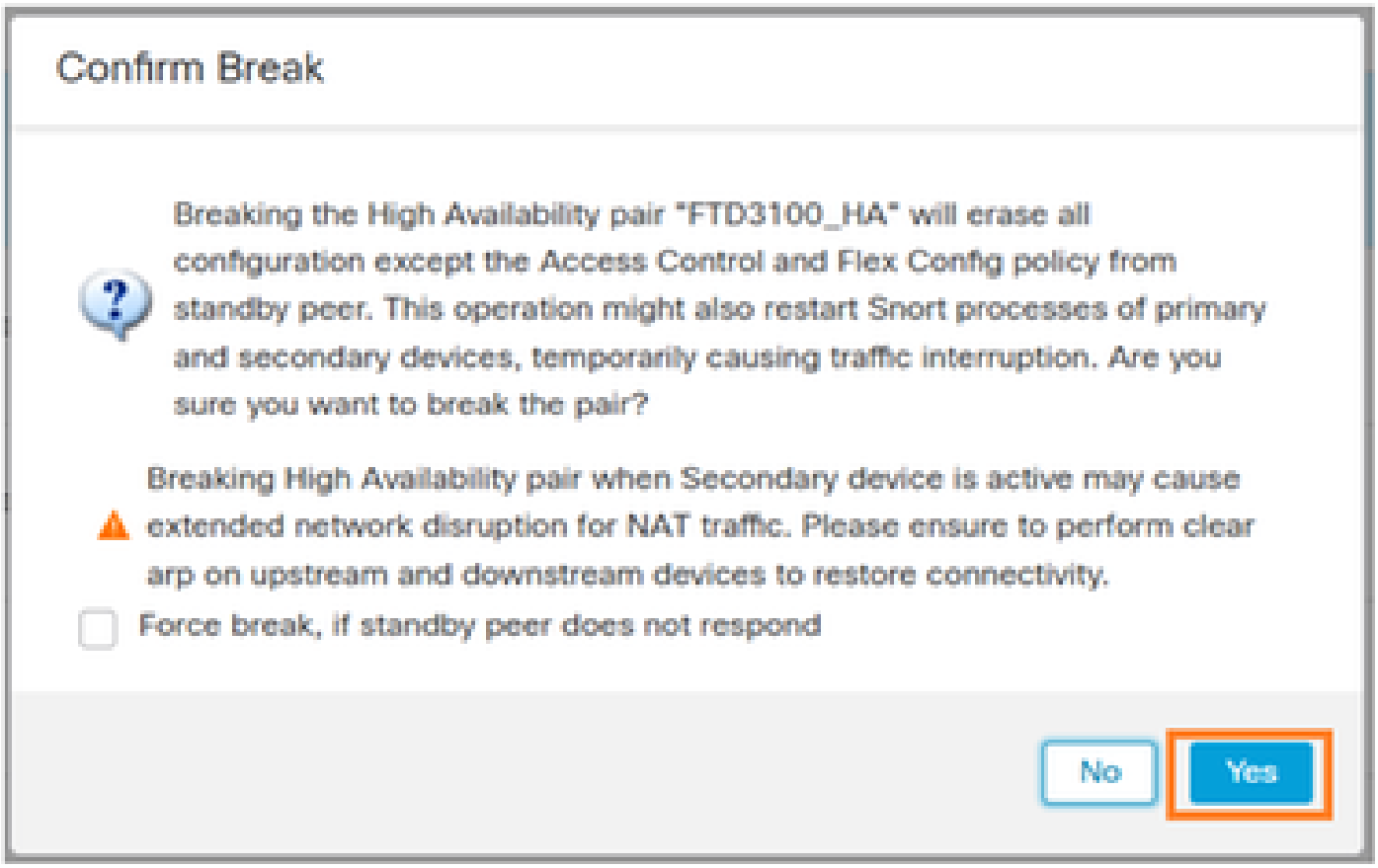


الخطوة 3، كسر FTD HA

انتقل إلى الأجهزة > إدارة الأجهزة وكسر FTD HA:



يظهر هذه النافذة. حدد نعم



ملاحظة: عند هذه النقطة، يمكنك تجربة بعض مقاطعة حركة المرور لثواني قليلة منذ إعادة تشغيل محرك الشيخ أثناء إستراحة HA. أيضا، كما تذكر الرسالة، إذا كنت تستخدم NAT وتعاني من انقطاع حركة المرور لفترة طويلة، فاستخدم مسح ذاكرة تخزين ARP المؤقت على أجهزة تدفق البيانات من الخادم والنهاية.

بعد كسر FTD HA، لديك إثنان FTD مستقلان على FMC.

من وجهة نظر التكوين، ال يزال FTD2 (نشط مسبقا) يحتوي على التكوين الموجود باستثناء التكوين المرتبط بتجاوز الفشل ويعالج حركة مرور البيانات:

```
<#root>

FTD3100-4#

show failover


Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1288 maximum
MAC Address Move Notification Interval not set
```

```
<#root>

FTD3100-4#

show interface ip brief


Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Data0/1           unassigned      YES           unset  up          up
Port-channel1              unassigned      YES           unset  up          up
Port-channel1.200          10.0.200.70     YES           manual up          up
Port-channel1.201          10.0.201.70     YES           manual up          up
```

يحتوي FTD1 (وضع الاستعداد السابق) على إزالة جميع التكوين:

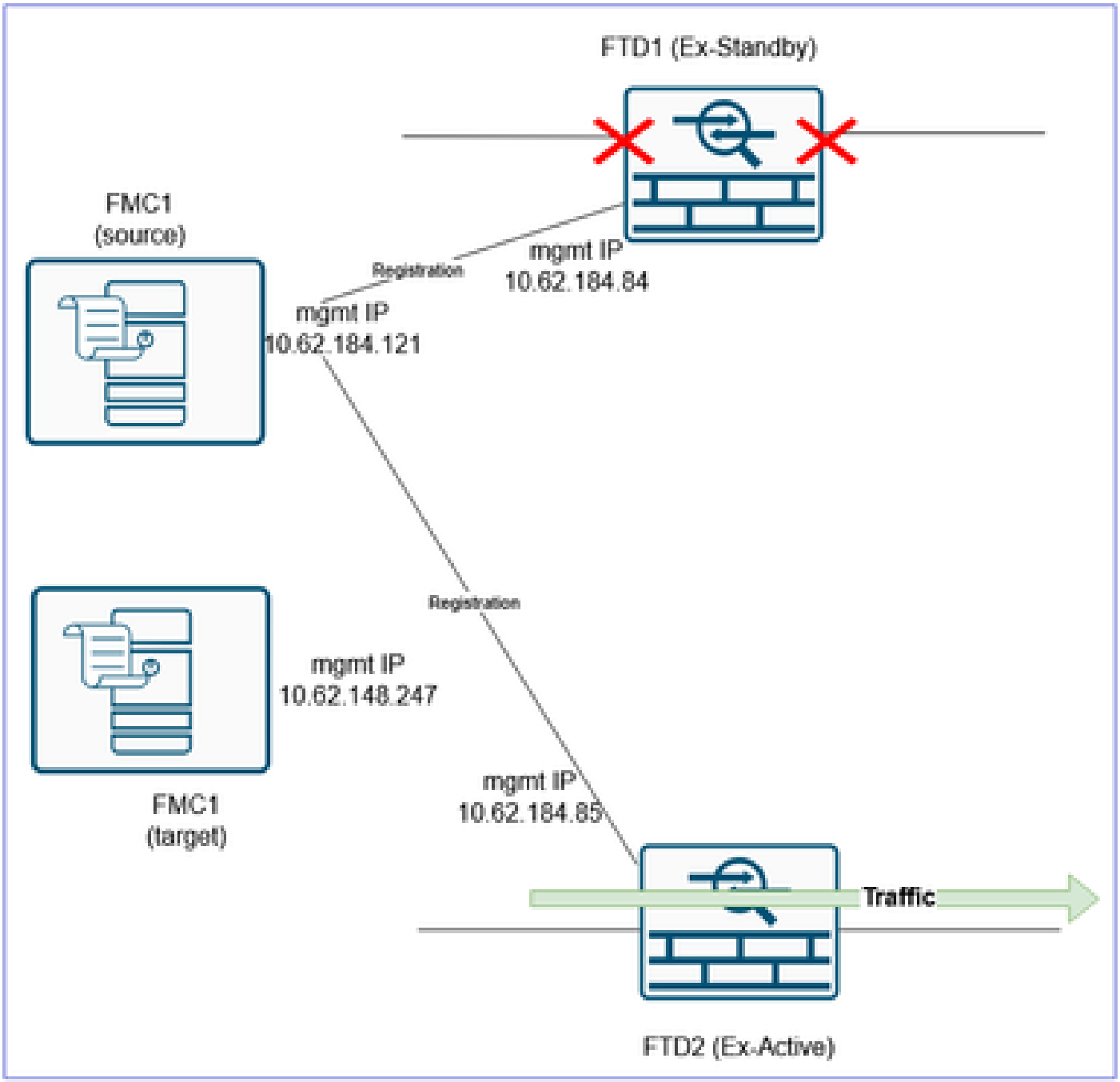
```
<#root>

FTD3100-3#

show failover


Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1288 maximum
MAC Address Move Notification Interval not set
```

```
<#root>

FTD3100-3#

show interface ip brief


Interface                  IP-Address      OK?           Method Status      Protocol
Internal-Data0/1           unassigned      YES           unset  up          up
Ethernet1/1                unassigned      YES           unset  admin down  down
Ethernet1/2                unassigned      YES           unset  admin down  down
Ethernet1/3                unassigned      YES           unset  admin down  down
Ethernet1/4                unassigned      YES           unset  admin down  down
Ethernet1/5                unassigned      YES           unset  admin down  down
Ethernet1/6                unassigned      YES           unset  admin down  down
Ethernet1/7                unassigned      YES           unset  admin down  down
Ethernet1/8                unassigned      YES           unset  admin down  down
Ethernet1/9                unassigned      YES           unset  admin down  down
Ethernet1/10               unassigned      YES           unset  admin down  down
Ethernet1/11               unassigned      YES           unset  admin down  down
Ethernet1/12               unassigned      YES           unset  admin down  down
Ethernet1/13               unassigned      YES           unset  admin down  down
```

```
Ethernet1/14               unassigned      YES           unset  admin down  down
Ethernet1/15               unassigned      YES           unset  admin down  down
Ethernet1/16               unassigned      YES           unset  admin down  down
```

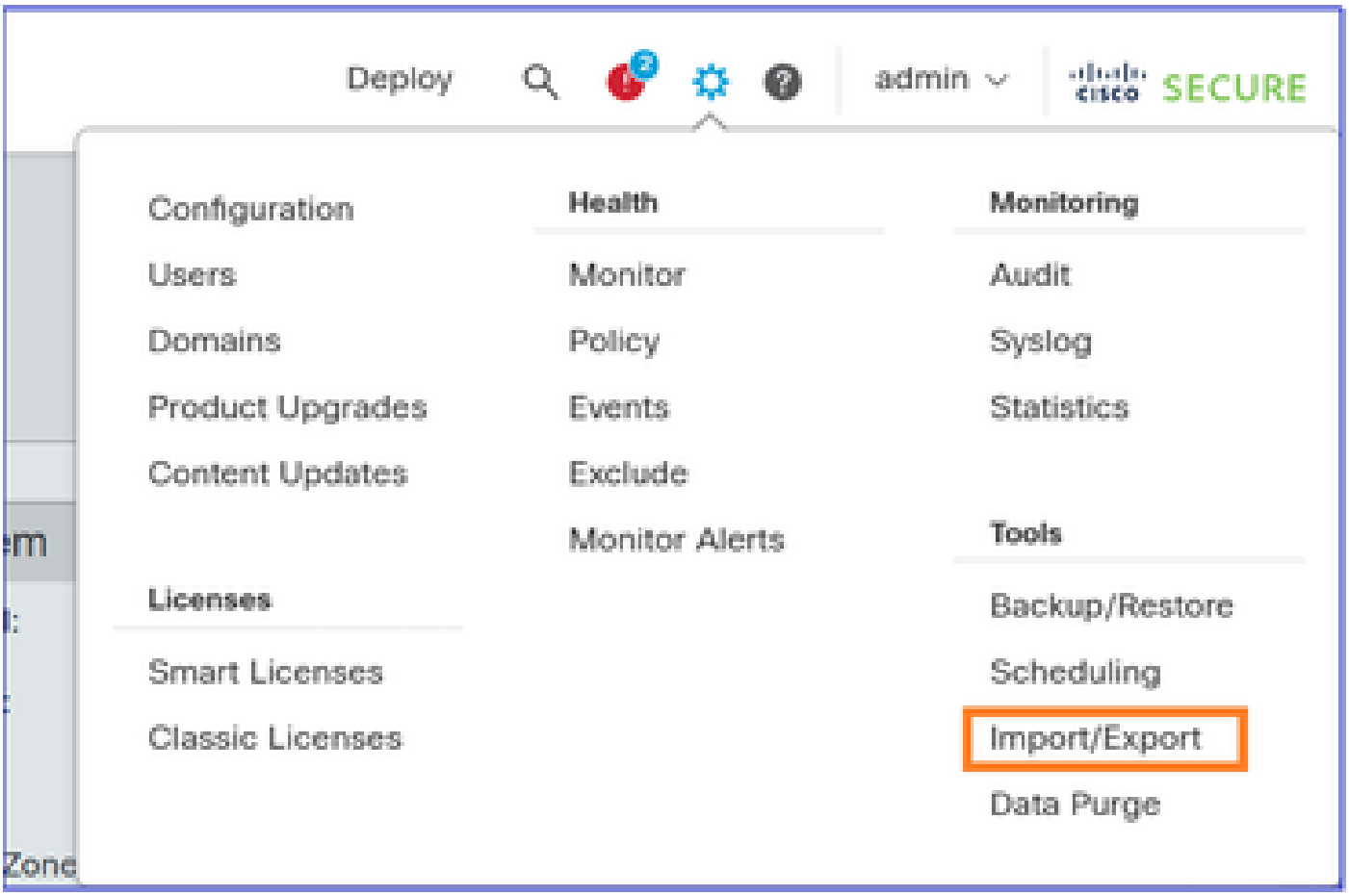
الخطوة 4. عزل واجهات البيانات FTD1 (سابقة أساسية)

قم بفصل كبلات البيانات من FTD1 (أساسي سابق). أترك فقط منفذ إدارة FTD المتصل.



الخطوة 5. تصدير سياسات FTD المشتركة

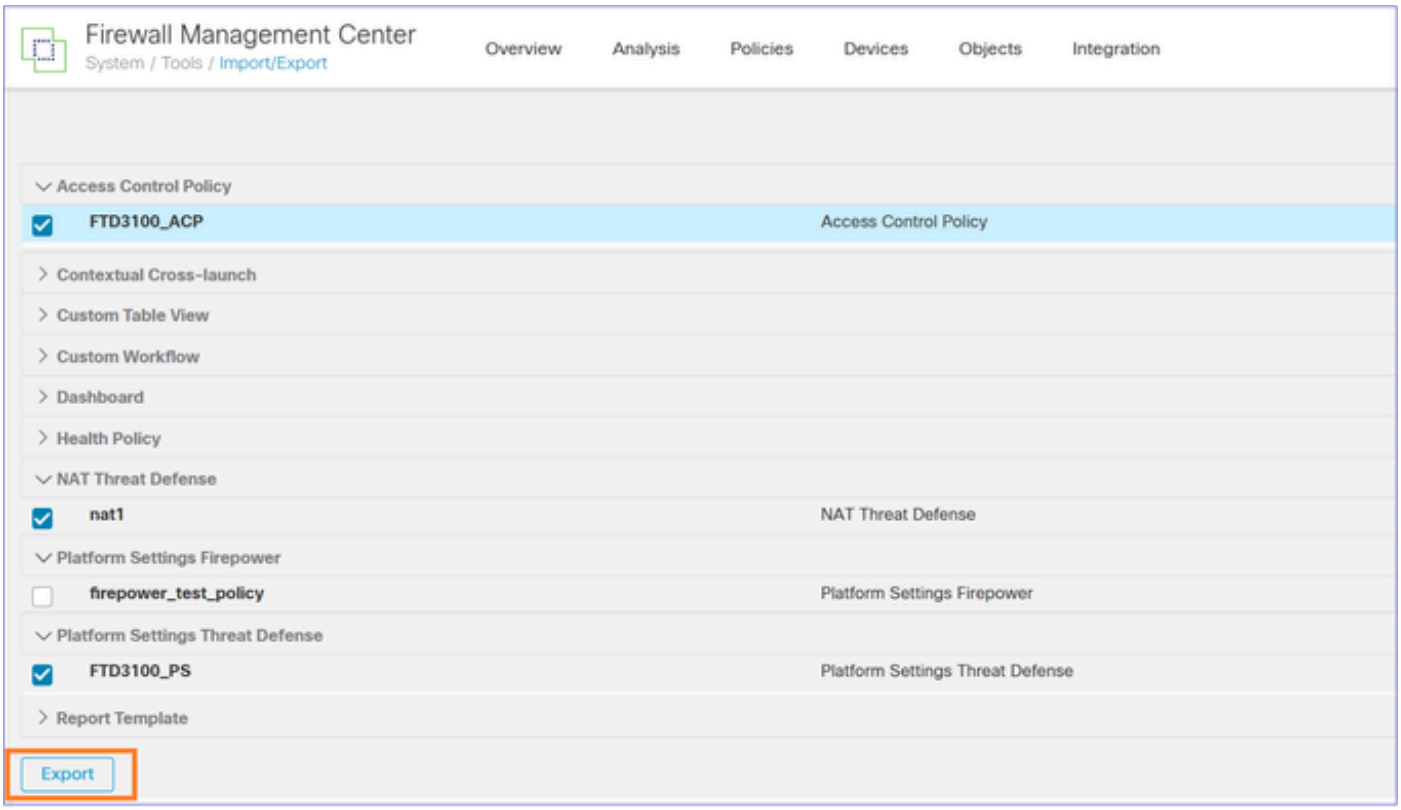
انتقل إلى نظام > أدوات وحدد إستيراد/تصدير:



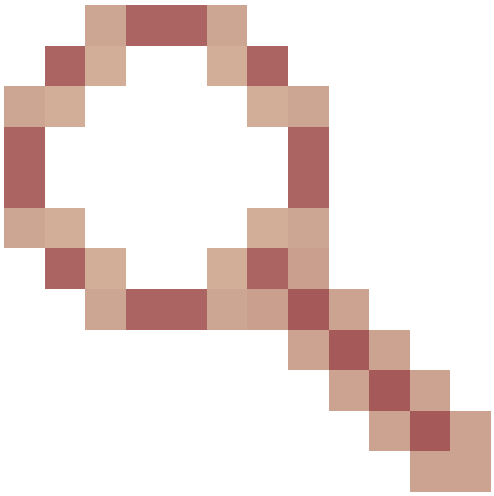
تصدير السياسات المختلفة المرفقة بالجهاز. تأكد من تصدير جميع السياسات المرفقة ب FTD مثل:

- سياسة التحكم في الوصول (ACP)
- سياسة ترجمة عنوان الشبكة (NAT)
- نهج الحماية (إذا كان مخصصا)
- إعدادات النظام الأساسي ل FTD

وهكذا.



ملاحظة: في وقت كتابة هذا التقرير، لا يتم دعم تصدير التكوين المرتبط بشبكة VPN. أنت تحتاج أن يعيد شكلت ال VPN يدويا على ال FMC2 (هدف FMC) بعد الأداة تسجيل.

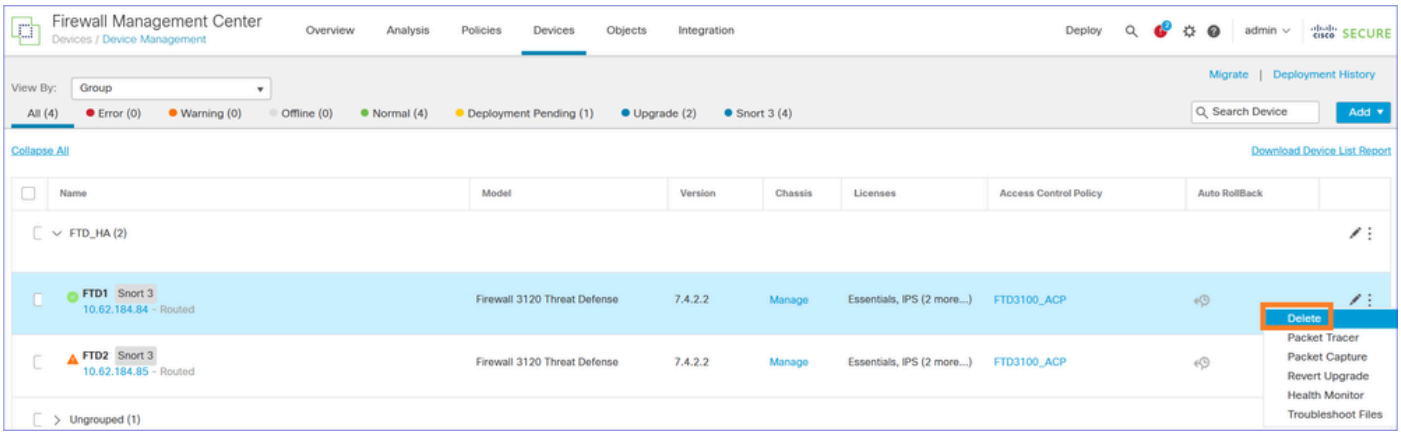


معرف تصحيح الأخطاء من Cisco CSCwf05294 ذو الصلة.

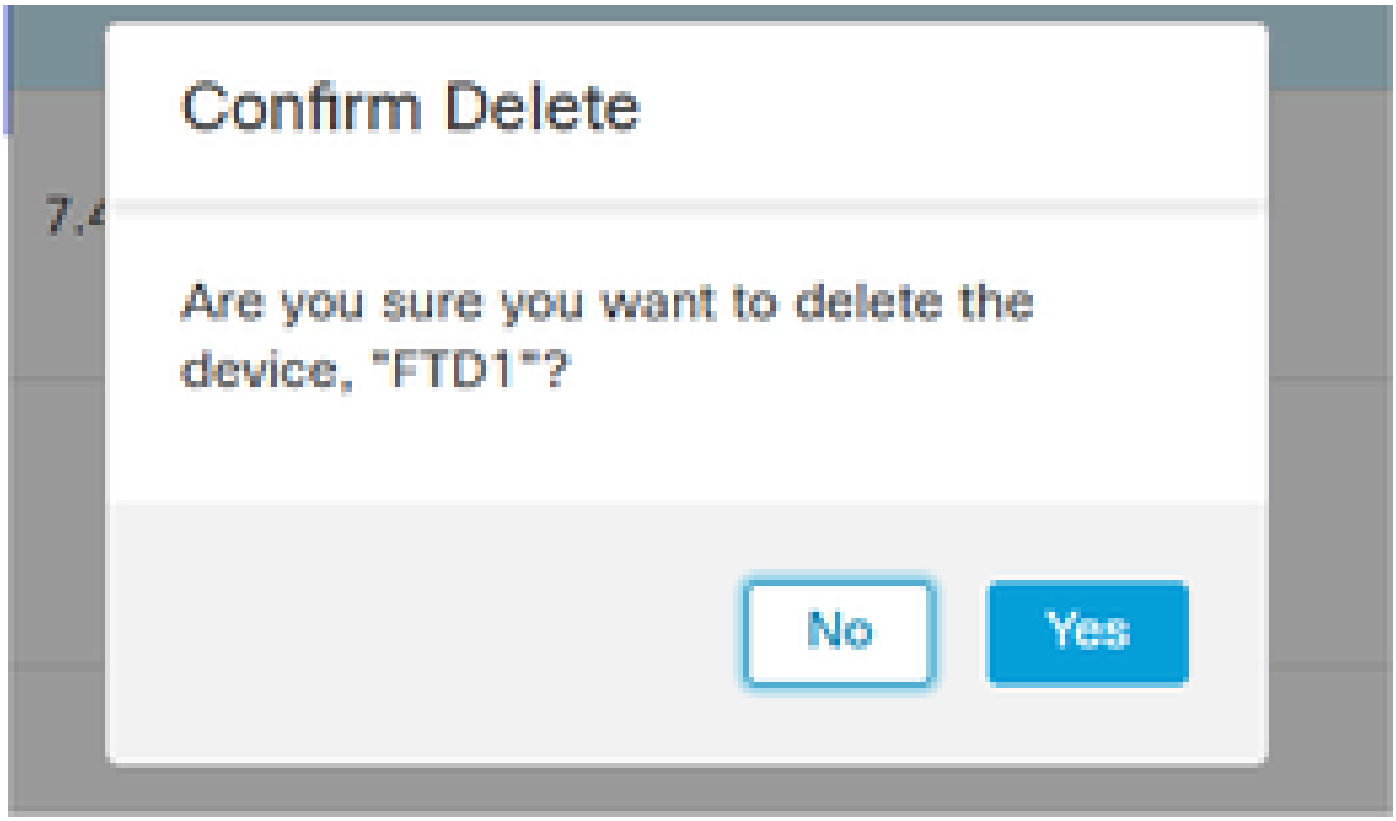
.

النتيجة هو ملف .sfo، على سبيل المثال ObjectExport_20250306082738.sfo

الخطوة 6. حذف/إلغاء تسجيل FTD1 (أساسي سابق) من FMC القديم/المصدر



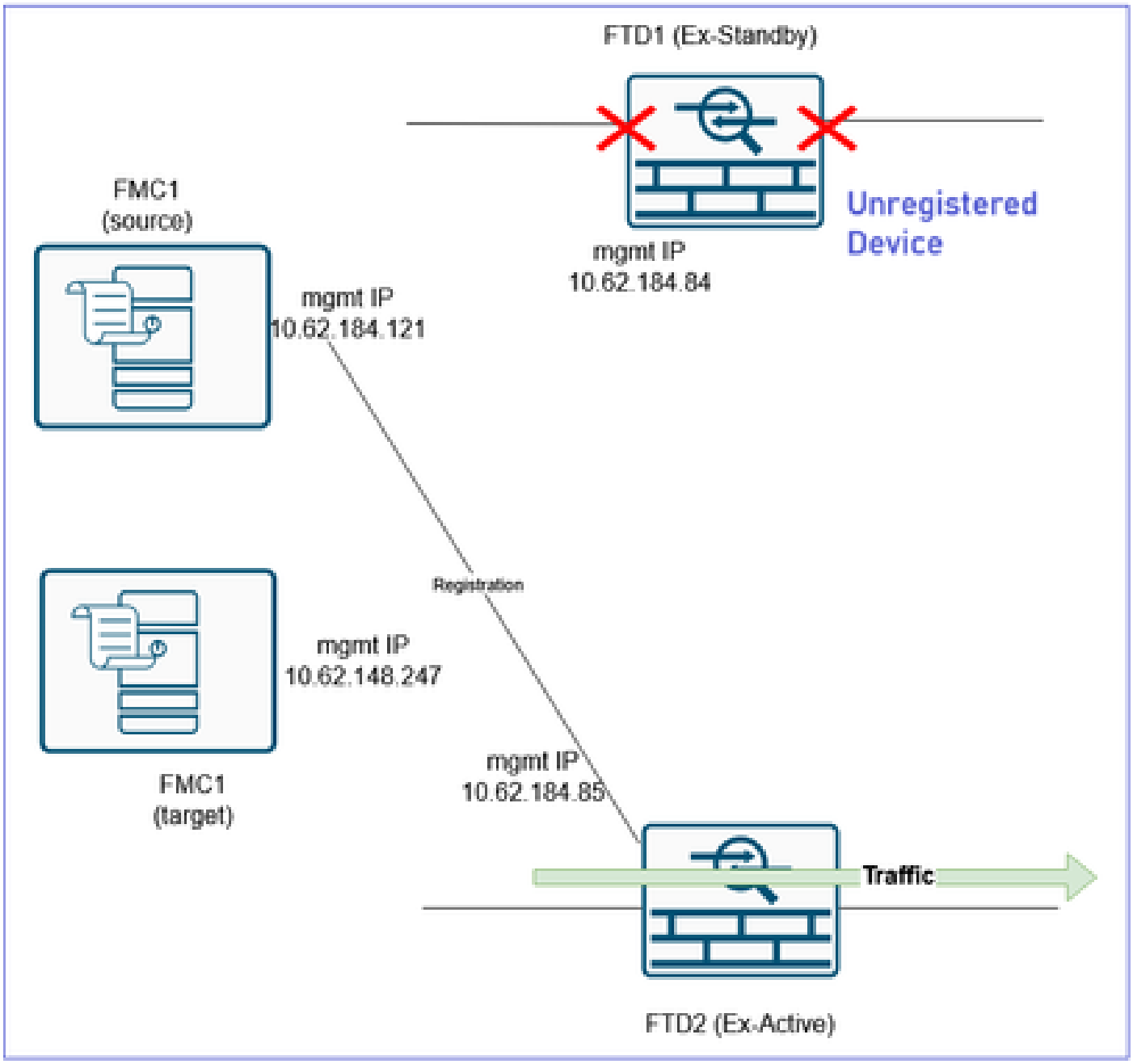
تأكيد حذف الجهاز:



التحقق من واجهة سطر الأوامر (CLI) لـ FTD1:

```
<#root>

>

show managers

No managers configured.

>
```

الحالة الحالية بعد حذف جهاز FTD1:



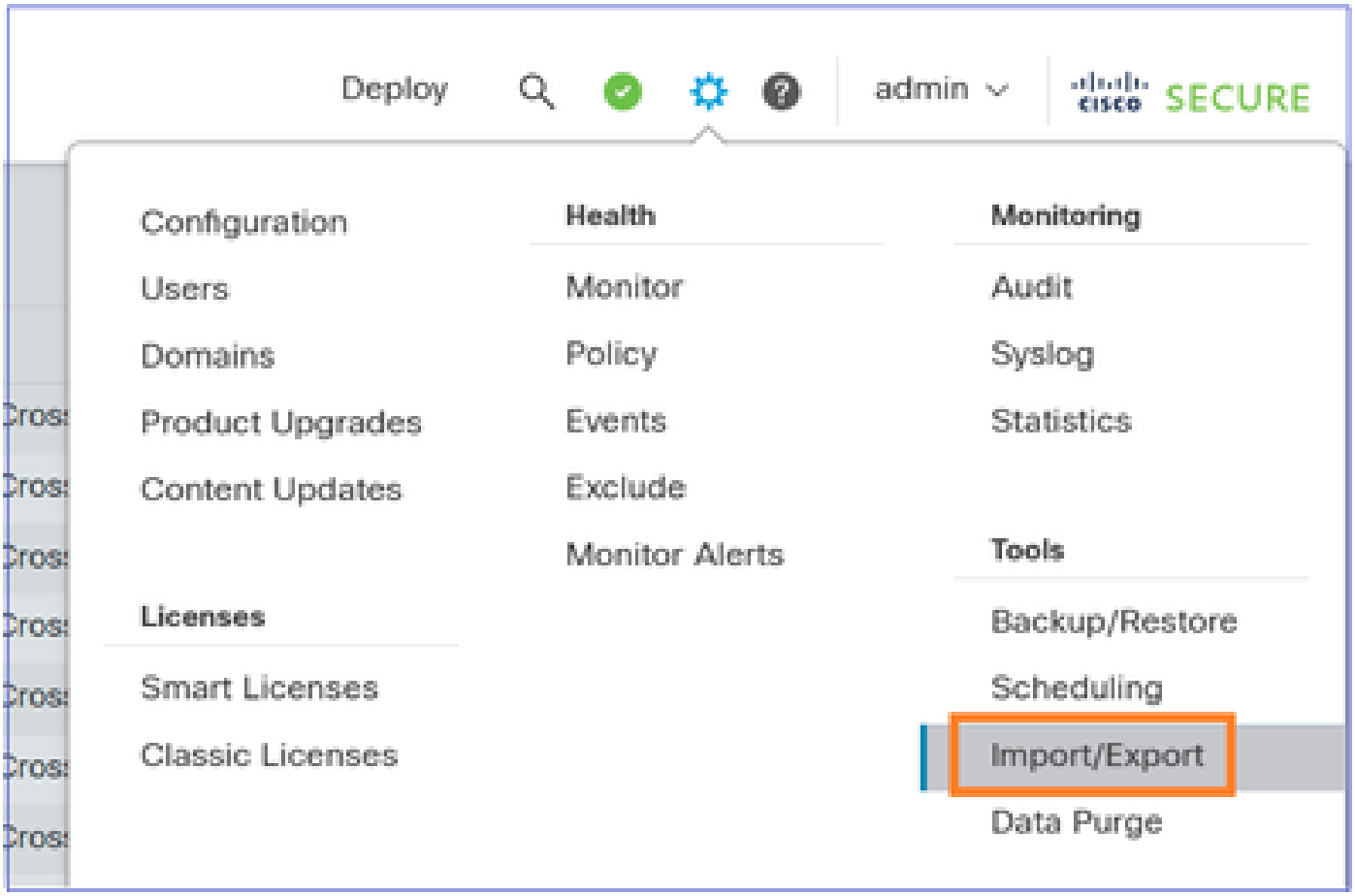
الخطوة 7. إستيراد كائن تكوين نهج FTD إلى FMC2 (FMC الهدف)

ملاحظة: يركز المستند على ترحيل زوج FTD HA واحد إلى وحدة تحكم في الإدارة المالية (FMC) جديدة. من ناحية أخرى، إذا كنت تخطط لترحيل العديد من جدران الحماية التي تشترك في نفس السياسات (على سبيل المثال، ACP و NAT) والكائنات وتريد أن تقوم بذلك على مراحل تحتاج إلى مراعاة هذه النقاط.
- إذا كان لديك نهج موجود على FMC الهدف بنفس الاسم، فيرجى منك:
أ. تريد إستبدال النهج أو
ب. قم بإنشاء اسم جديد باسم مختلف. يؤدي ذلك إلى إنشاء كائنات مضاعفة بأسماء مختلفة (لاحق _1).

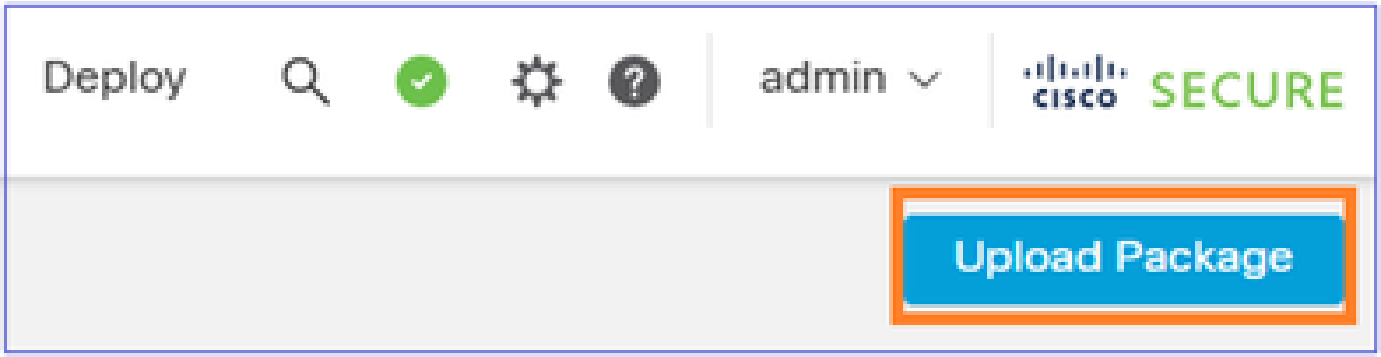
- إذا ذهبت مع الخيار 'b'، في الخطوة 9 تأكد من إعادة تكوين الكائنات التي تم إنشاؤها حديثا إلى السياسات التي تم ترحيلها (مناطق أمان ACP، مناطق أمان NAT، التوجيه،

إعدادات النظام الأساسي، وما إلى ذلك).

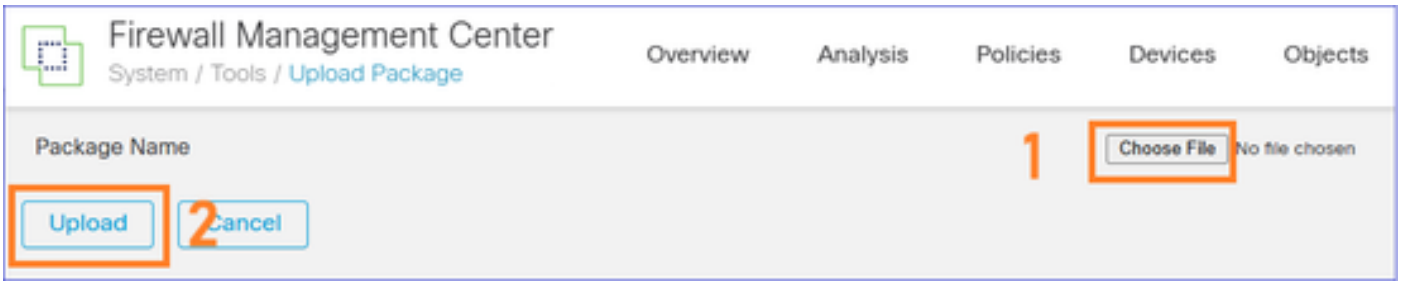
قم بتسجيل الدخول إلى FMC2 (FMC الهدف) واستورد كائن SFO الخاص بنهج FTD الذي قمت بتصديره في الخطوة 5:



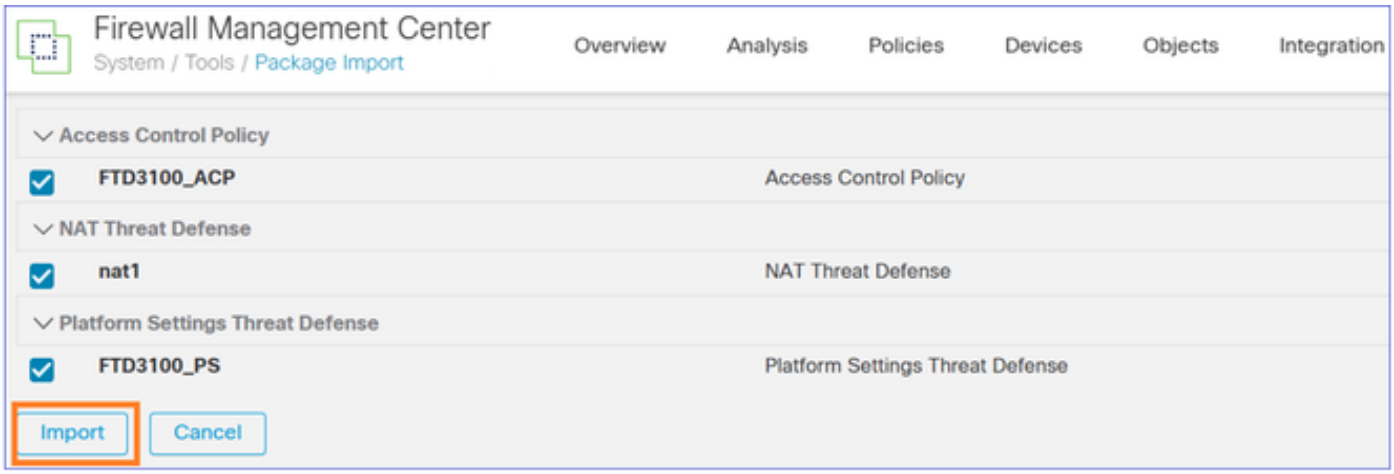
حدد تحميل الحزمة:



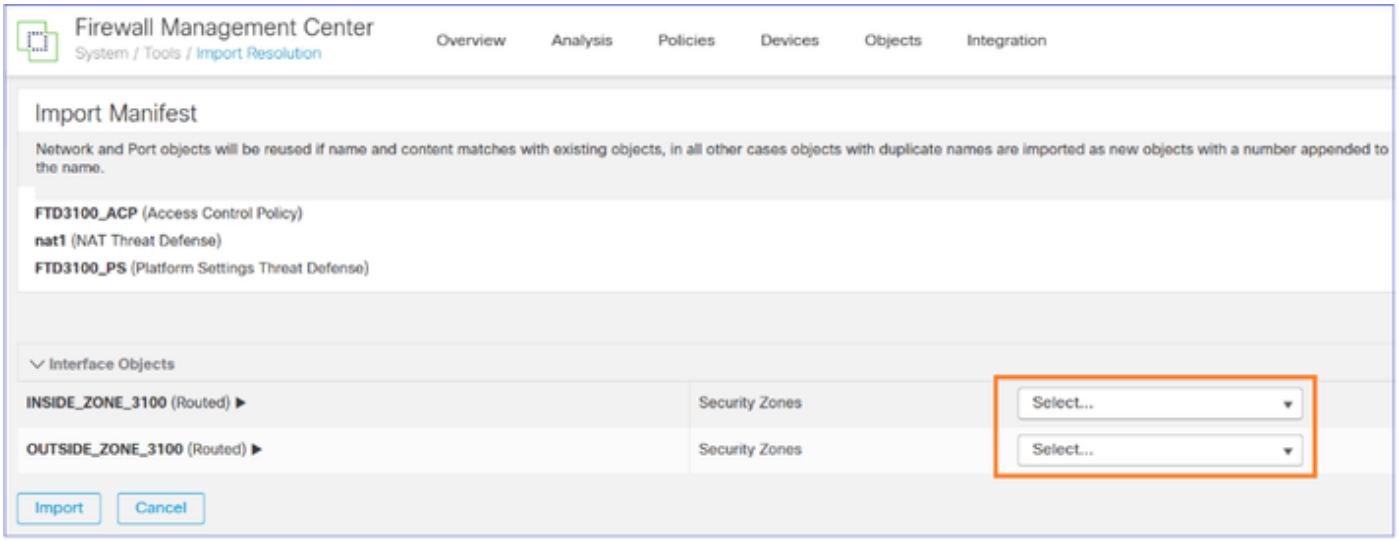
تحميل الملف:



إستيراد السياسات:



قم بإنشاء كائنات الواجهة/مناطق الأمان على FMC2 (FMC الهدف):



يمكنك إعطاء نفس الأسماء التي كانت لديهم على FMC1 (مصدر FMC):

بمجرد تحديد الاستيراد، تبدأ مهمة في إستيراد السياسات ذات الصلة إلى FMC2 (FMC الهدف):

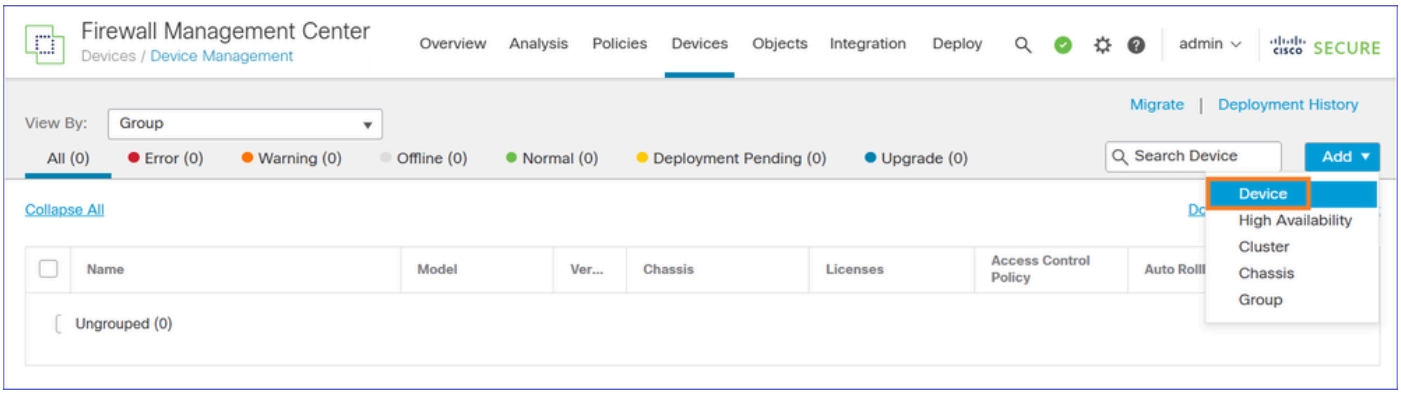
تم إنجاز المهمة:

الخطوة 8. سجل FTD1 (أساسي سابق) في FMC2

انتقل إلى واجهة سطر الأوامر (CLI) لـ FTD1 (أساسي سابق) وقم بتكوين المدير الجديد:

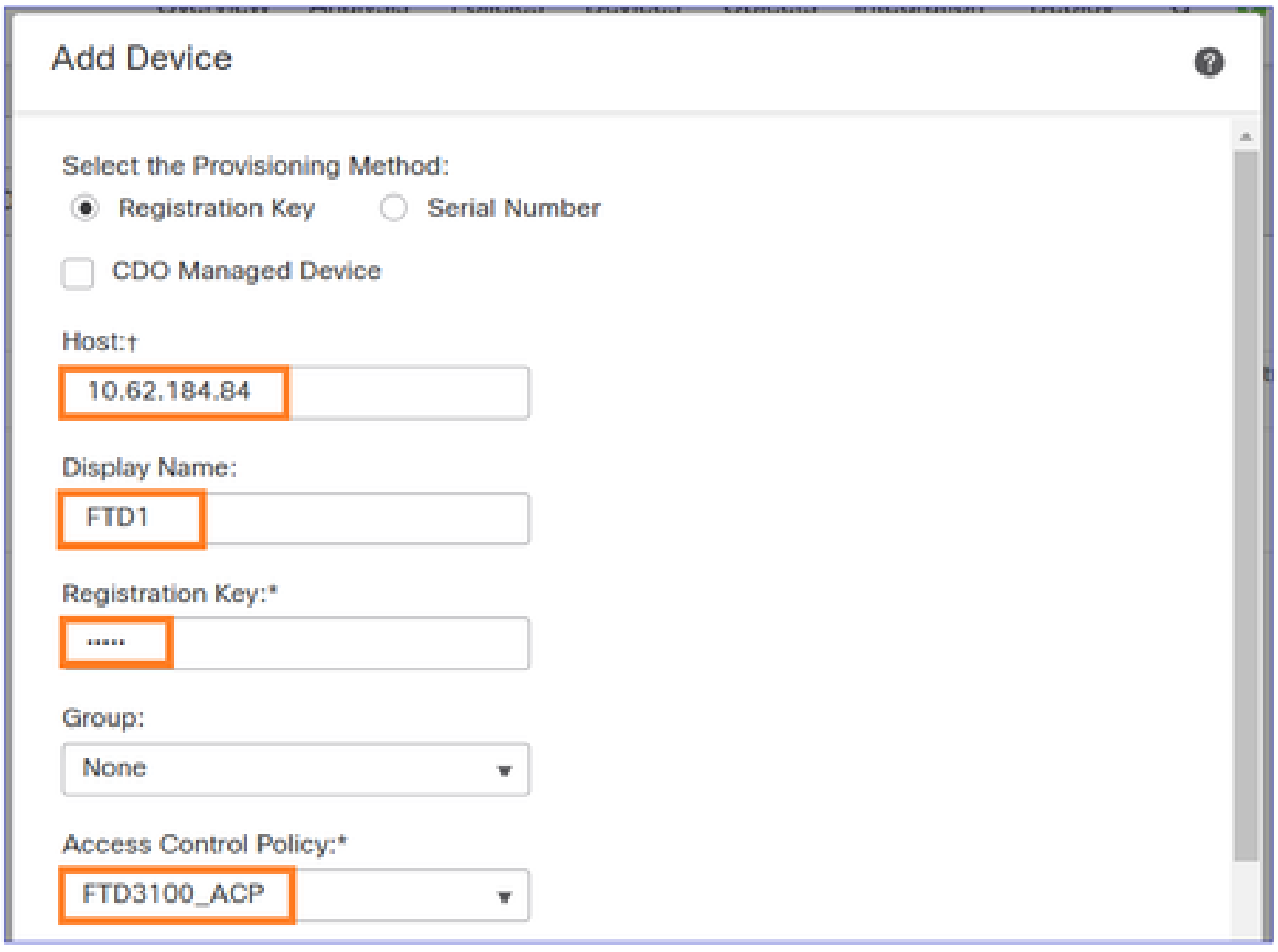
```
<#root>

>

configure manager add 10.62.148.247 cisco


Manager 10.62.148.247 successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

انتقل إلى أجهزة واجهة المستخدم (FMC2) (الهدف FMC) > إدارة الأجهزة وأضف جهاز FTD:

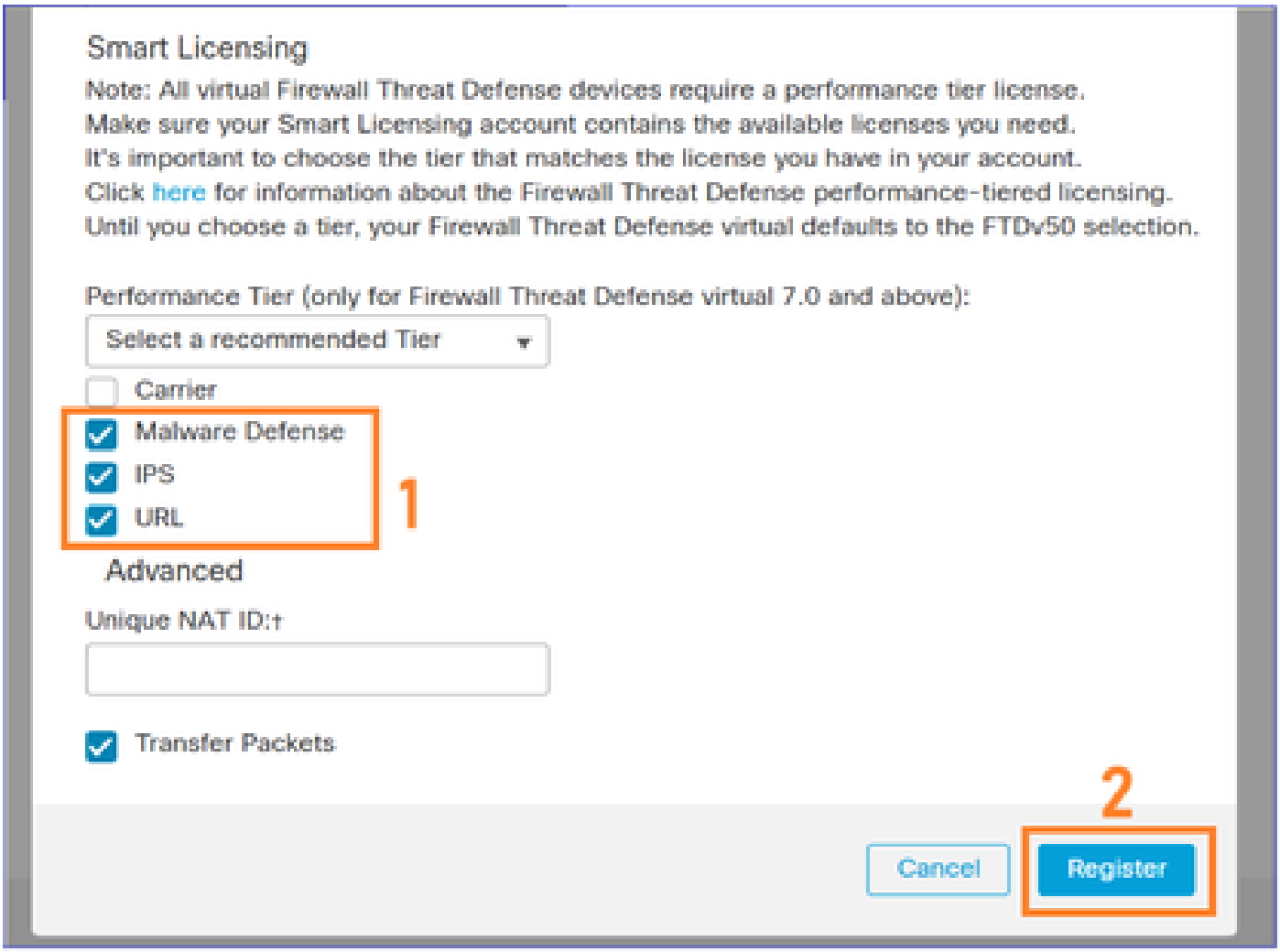


إذا فشل تسجيل الجهاز، ارجع إلى هذا المستند لاستكشاف المشكلة وإصلاحها: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

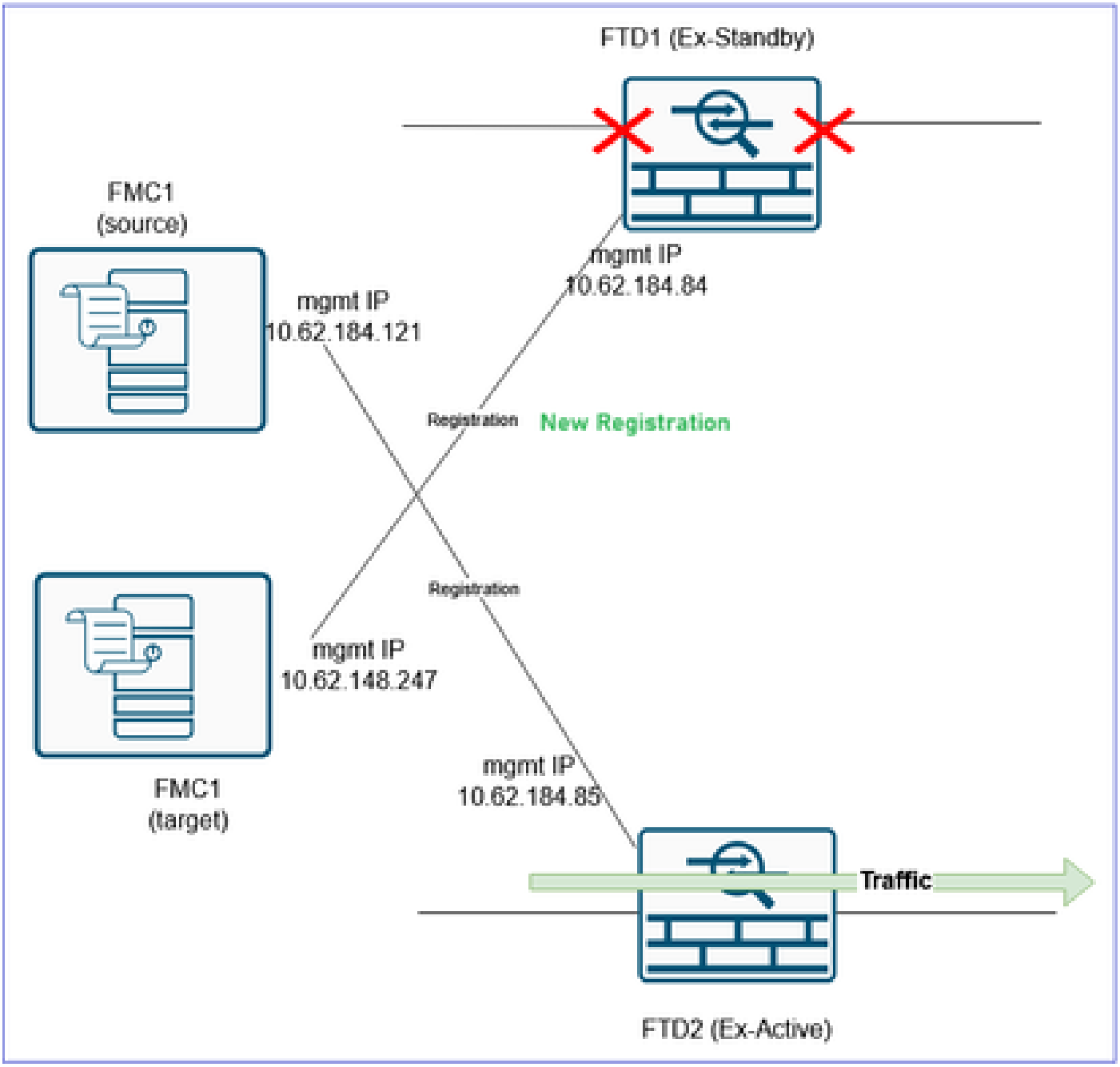
تعيين نهج التحكم بالوصول الذي قمت باستيراده في الخطوة السابقة:



تطبيق الترخيص المطلوب وتسجيل الجهاز:


Smart Licensing
Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.
Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):
Select a recommended Tier
Carrier
Malware Defense
IPS
URL
1
Advanced
Unique NAT ID:†
Transfer Packets
2
Cancel
Register

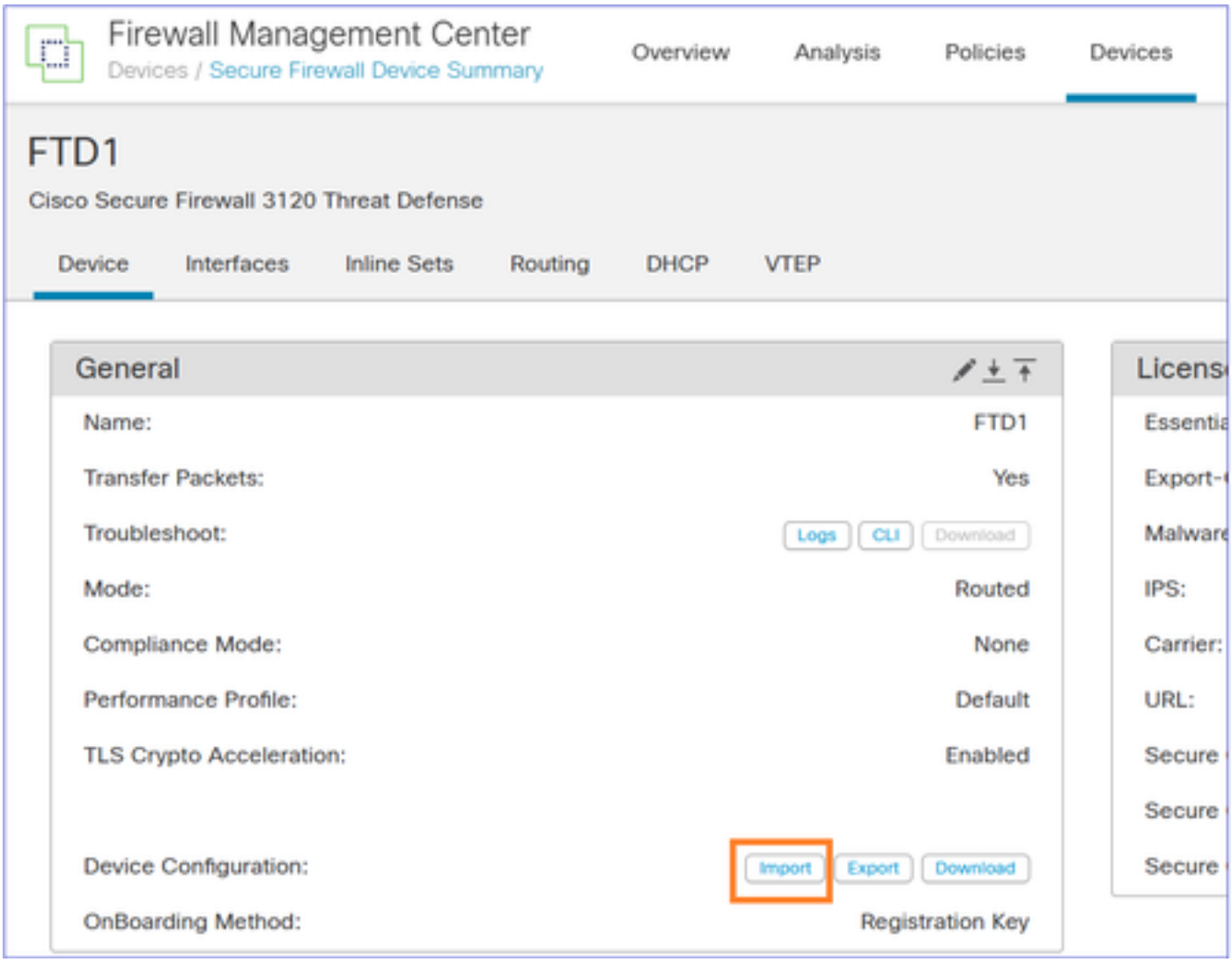
النتيجة:



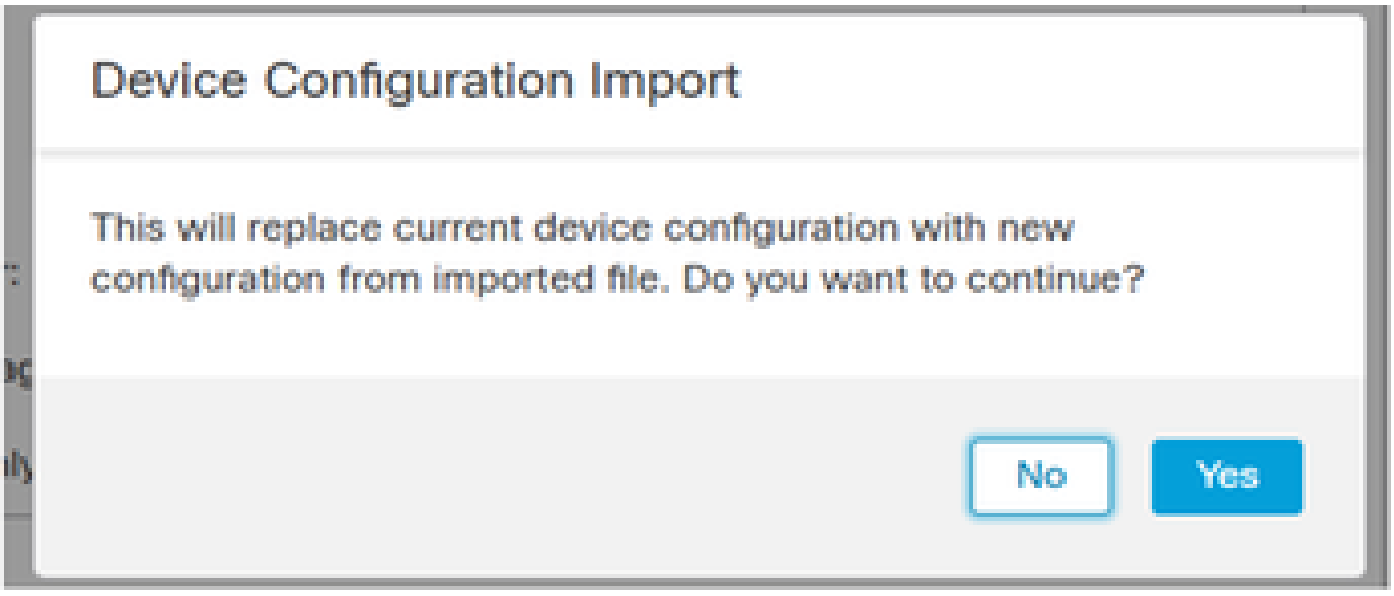
الخطوة 9. إستيراد كائن تكوين جهاز FTD إلى FMC2 (وحدة التحكم FMC الهدف)

قم بتسجيل الدخول إلى FMC2 (وحدة التحكم FMC الهدف)، وتصفح إلى الأجهزة > إدارة الأجهزة وتحرير جهاز FTD الذي قمت بتسجيله في الخطوة السابقة.

انتقل إلى علامة التبويب الجهاز وإستيراد كائن FTD Policy الذي قمت بتصديره في الخطوة 2:

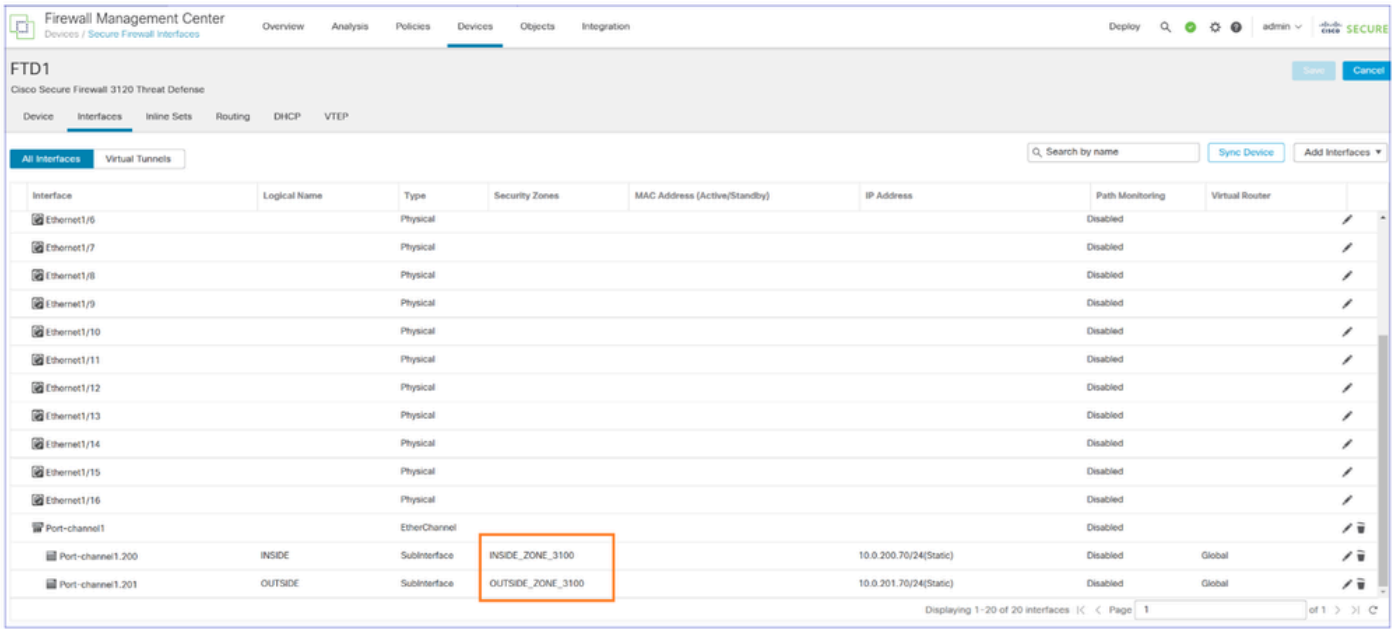


ملاحظة: في حالة ما إذا كنت قد ذهبت في الخطوة 7 مع الخيار 'b' (إنشاء سياسة جديدة)، تأكد من إعادة تجميع الكائنات التي تم إنشاؤها حديثا إلى السياسات التي تم ترحيلها (مناطق أمان ACP، مناطق أمان NAT، التوجيه، إعدادات النظام الأساسي، وهكذا).



تم بدء مهمة FMC.

يتم تطبيق تكوين الجهاز على FTD1، على سبيل المثال، مناطق الأمان و ACP و NAT وما إلى ذلك:



تحذير: إذا كان لديك قائمة تحكم في الوصول (ACP) تتسع إلى العديد من عناصر التحكم في الوصول، فإن عملية التحويل البرمجي ل ACP (تطابق التحويل البرمجي) يمكن أن تستغرق عدة دقائق للاكتمال. يمكنك إستخدام هذا الأمر للتحقق من حالة التحويل البرمجي ل ACP:

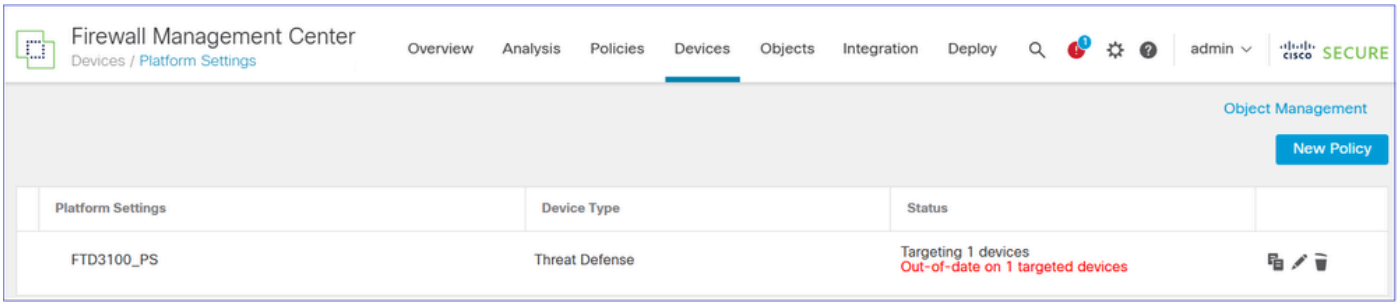
```
<#root>

FTD3100-3#

show asp rule-engine

Rule compilation Status:

Completed
```

الخطوة 10. إنهاء تكوين FTD

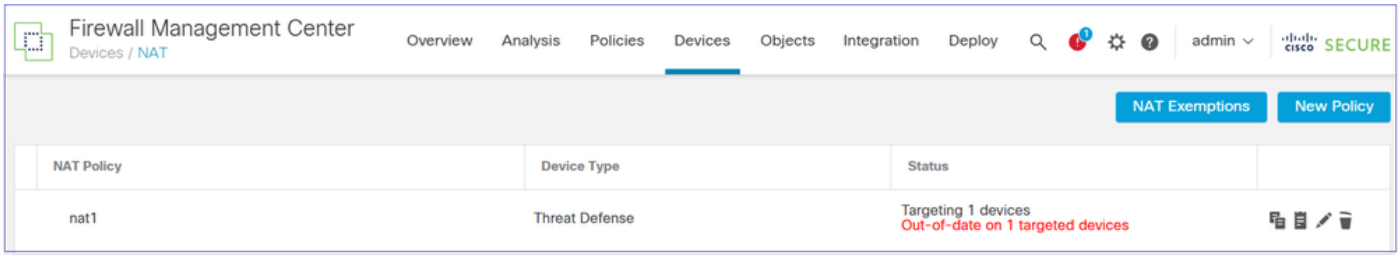
عند هذه النقطة، يكون الهدف هو تكوين جميع المميزات التي لا تزال مفقودة من FTD1 بعد التسجيل في FMC2 (FMC الهدف) واستيراد نهج الجهاز.

تأكد من أن السياسات مثل NAT، إعدادات النظام الأساسي، جودة الخدمة، وهكذا. تم تعيينها إلى FTD. ترى أن النهج معينة ولكن في انتظار النشر.

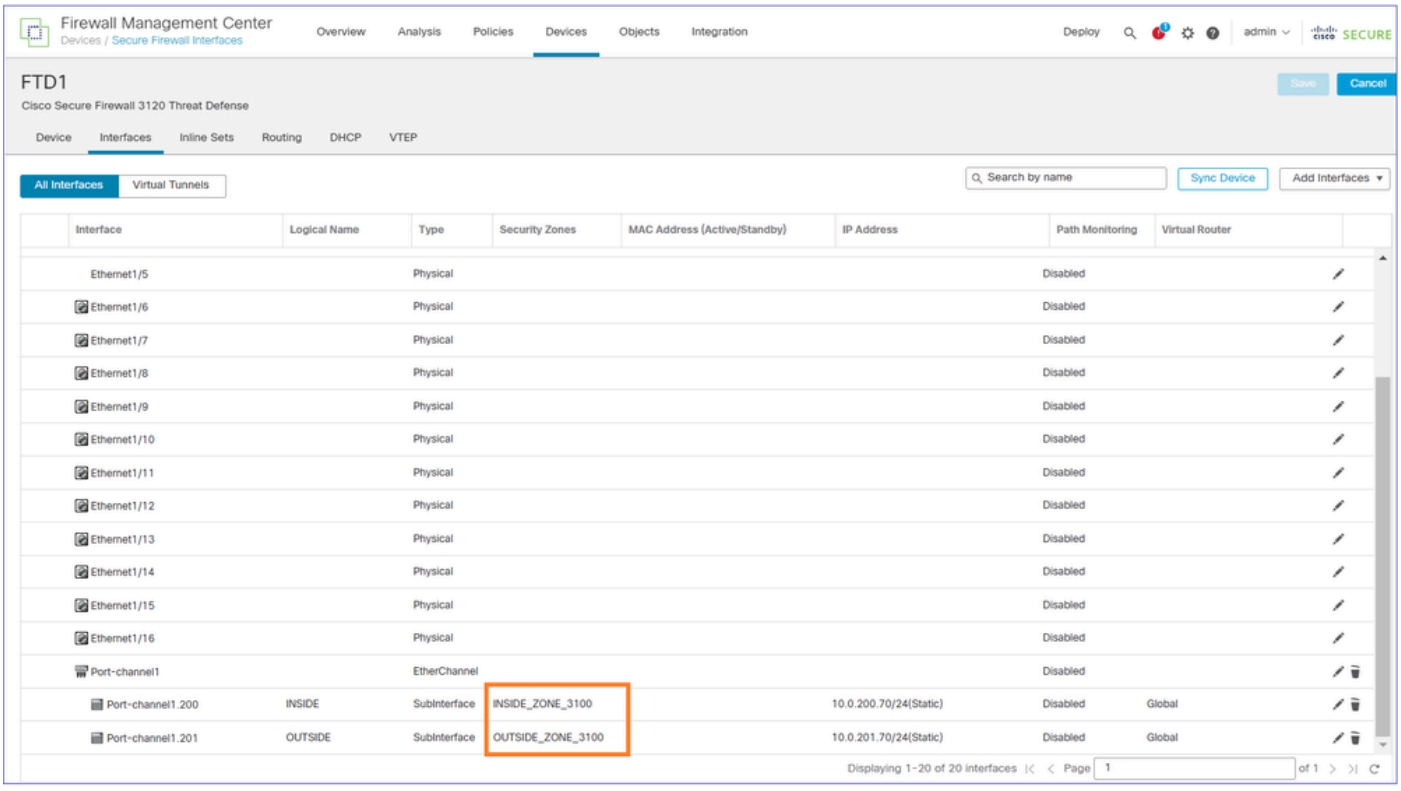
على سبيل المثال، يتم إستيراد إعدادات النظام الأساسي وتخصيصها للجهاز، ولكن في انتظار النشر:



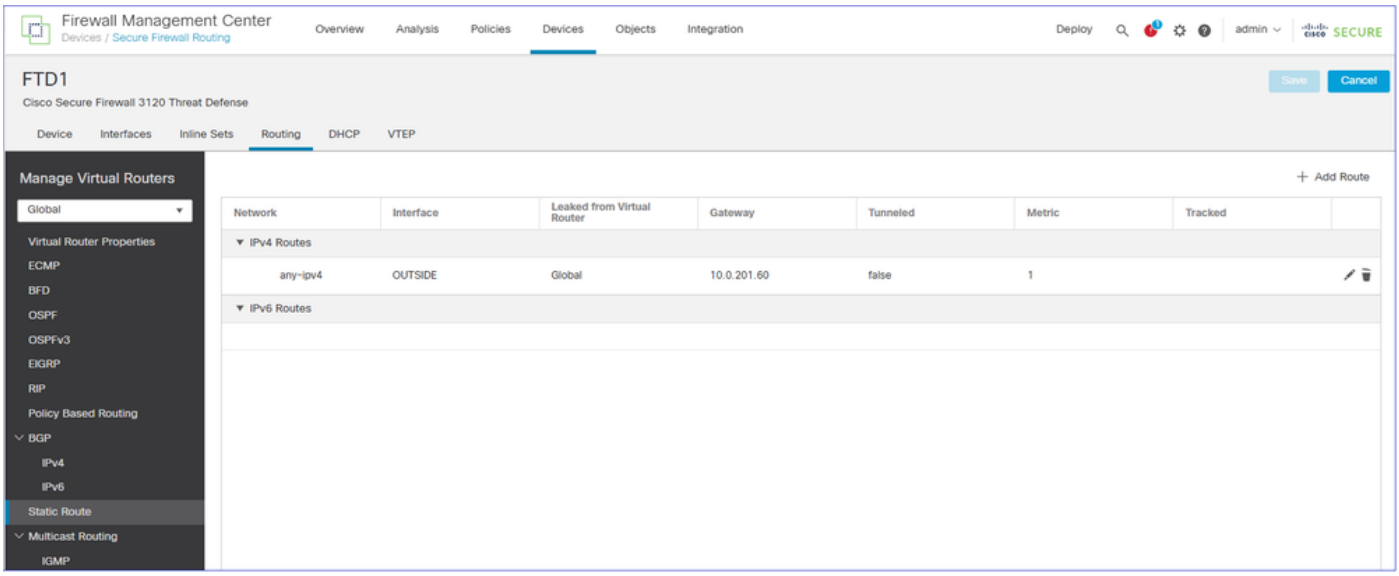
في حالة تكوين NAT، يتم إستيراد نهج NAT وتخصيصه للجهاز، ولكن في انتظار النشر:



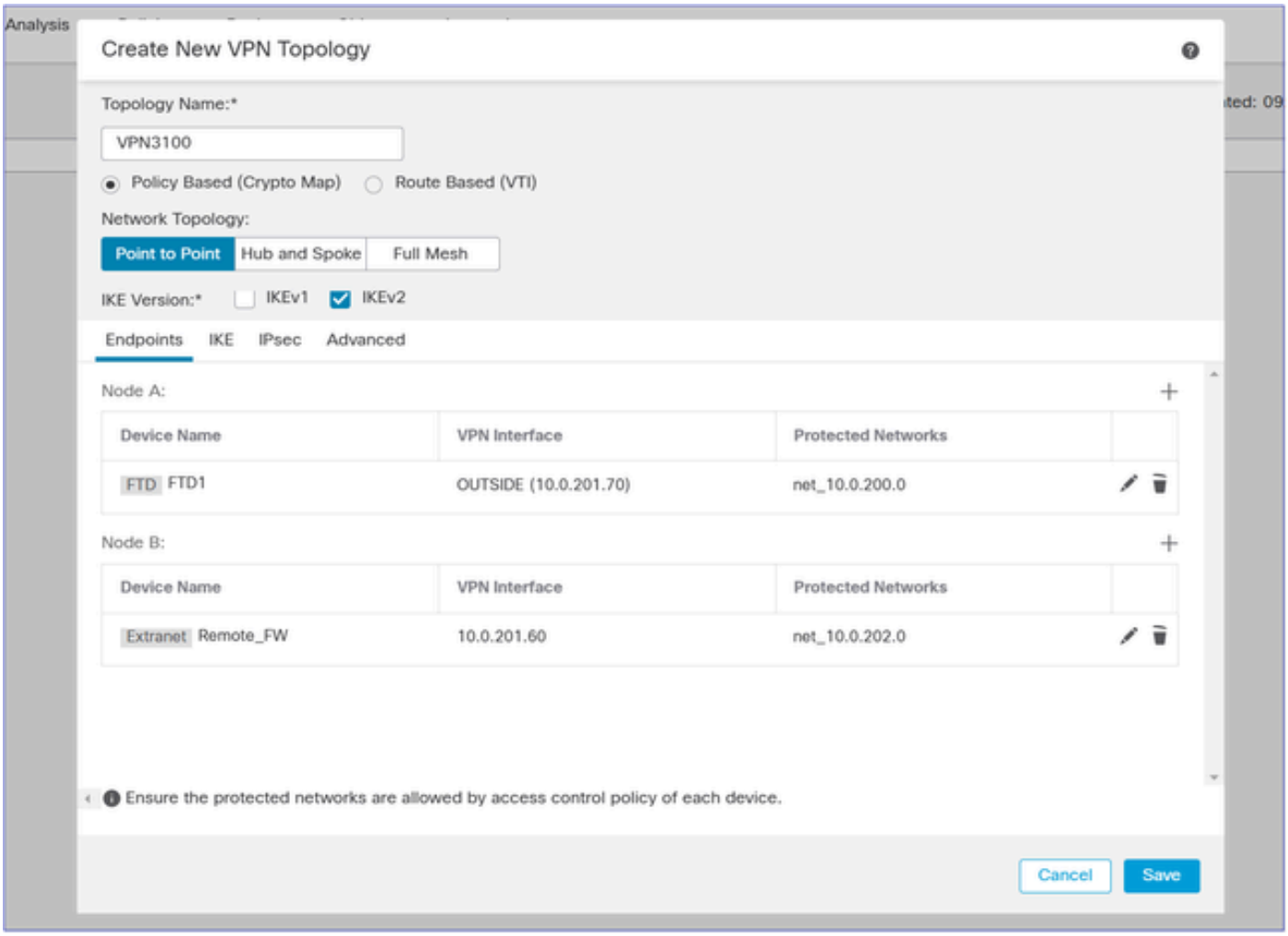
يتم تطبيق مناطق الأمان على الواجهات:



يتم تطبيق تكوين التوجيه على جهاز FTD:



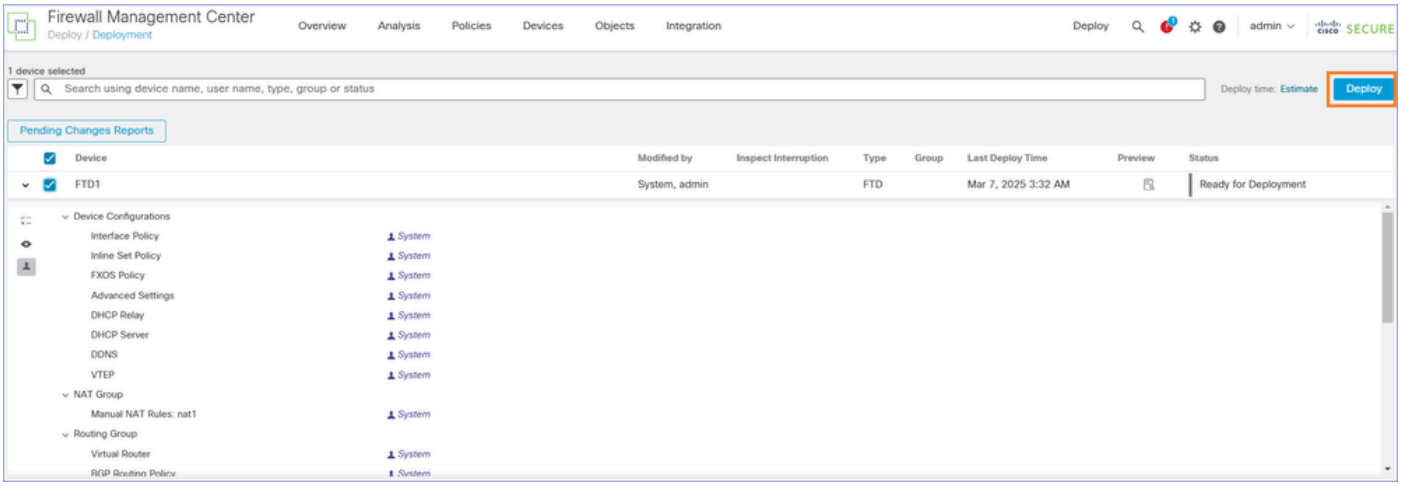
ملاحظة: الآن هو الوقت لتكوين السياسات التي تعذر ترحيلها تلقائيا (على سبيل المثال، VPNs).



ملاحظة: إذا كان ل FTD الذي يتم ترحيله نظائر S2S VPN التي يتم ترحيلها أيضا إلى

FMC الهدف، فعليك تكوين VPN بعد نقل جميع FTDs إلى FMC الهدف.

نشر التغييرات المعلقة:



الخطوة 11. تحقق من تكوين FTD الذي تم نشره

عند هذه النقطة، يكون الهدف هو التحقق من واجهة سطر الأوامر (CLI) الخاصة ب FTD أن جميع التكوين في موضعه.

الاقتراح هو مقارنة إخراج "show running-config" من كل من FTDs. يمكنك إستخدام أدوات مثل WinMerge أو Diff للمقارنة.

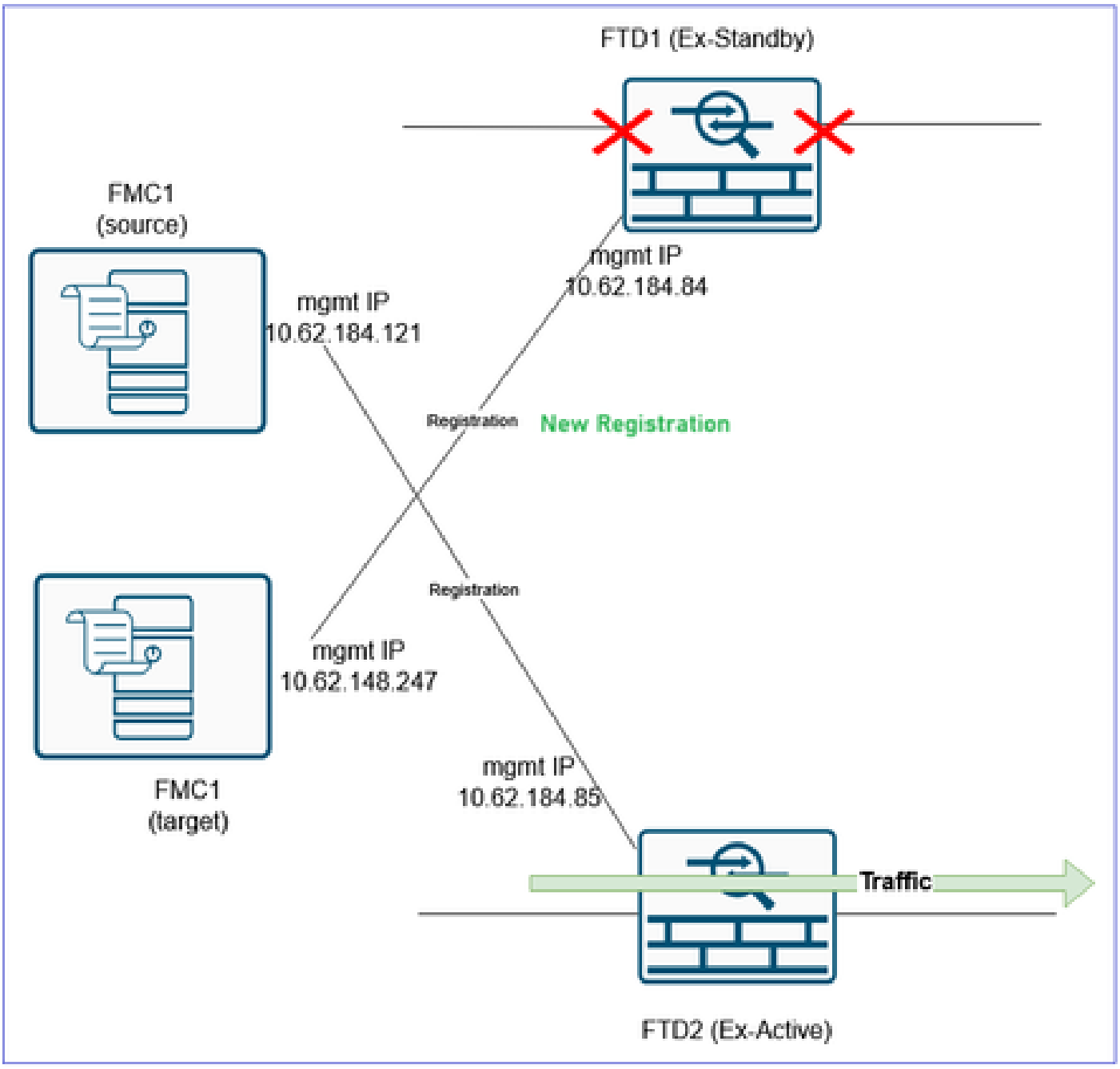
الفروق التي تراها وتكون عادية هي:

- الرقم التسلسلي للجهاز
- أوصاف الواجهة
- معرفات قواعد ACL
- المجموع الاختباري للتشفير للتكوين

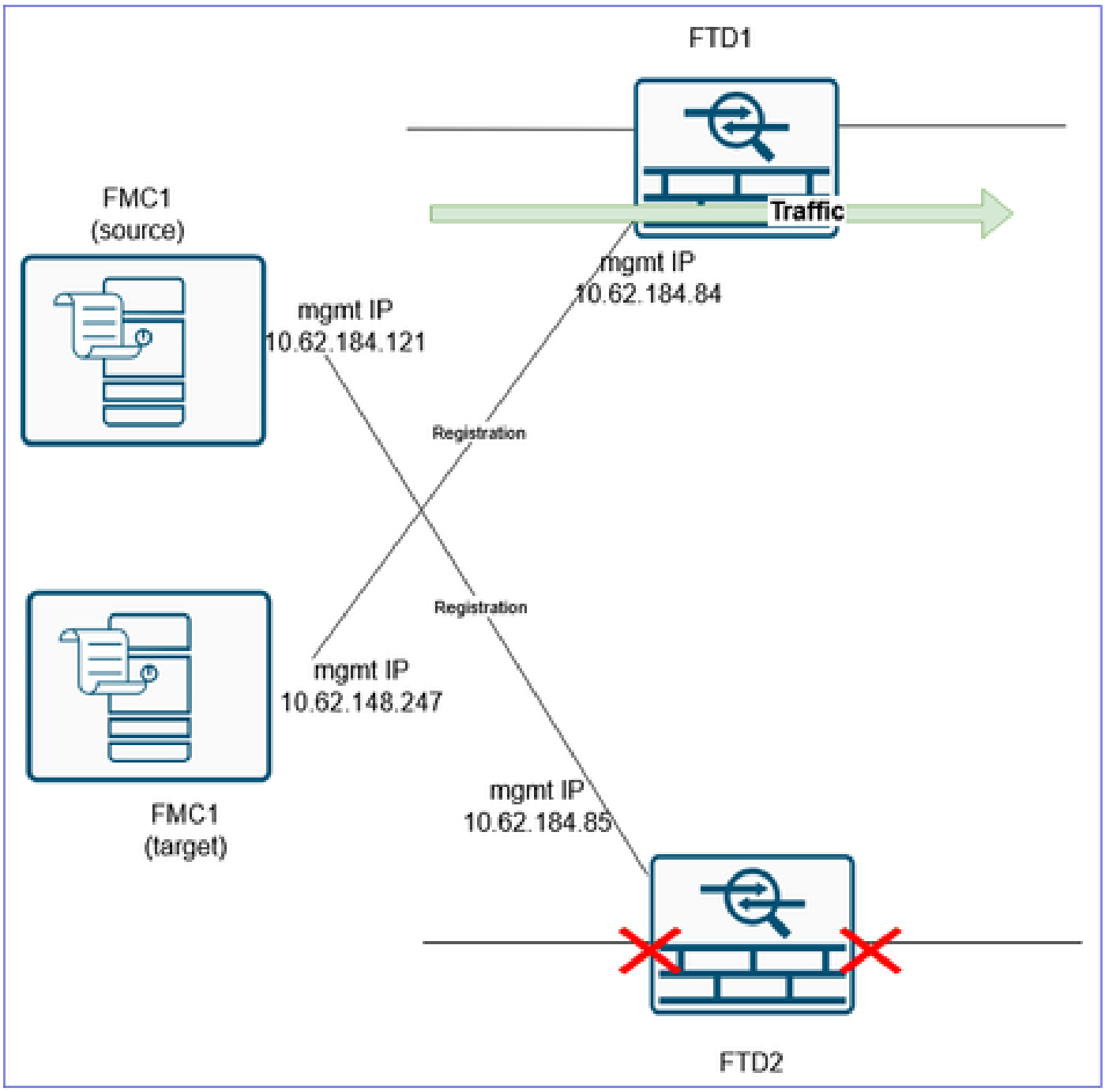
الخطوة 12. قم بالتقطيع

في هذه الخطوة، الهدف هو تحويل حركة المرور من FTD2 الذي يعالج حركة المرور حاليا والى يزال مسجلا إلى FMC القديم/المصدر، إلى FTD1 الذي تم تسجيله إلى FMC الهدف.

قبل:


FTD1 (Ex-Standby)
FMC1
(source)
mgmt IP
10.62.184.84
mgmt IP
10.62.184.121
Registration
New Registration
Registration
mgmt IP
10.62.148.247
FMC1
(target)
mgmt IP
10.62.184.85
Traffic
FTD2 (Ex-Active)

بعد:



⚠ تحذير: رتبوا سيارة ميكرو واتا للقيام بالقطع. أثناء عملية القطع، ستحدث لك بعض مقاطعة حركة المرور حتى يتم تحويل حركة المرور بالكامل إلى FTD1، كما ستتم إعادة إنشاء شبكات VPN، وما إلى ذلك.

⚠ تحذير: لا تقم بدء عملية القطع ما لم يتم إكمال تجميع ACP (انظر الخطوة 10 أعلاه).

⚠ تحذير: تأكد من قطع اتصال كبلات البيانات من FTD2 أو إيقاف تشغيل منافذ المحولات ذات الصلة. وإلا، يمكنك الانتباه باستخدام كل الجهازين اللذين يعالجان حركة المرور!

⚠ تحذير: ونظرا لأن كل الجهازين يستخدم تكوين IP نفسه، يلزم تحديث ذاكرة التخزين

⚠ المؤقت ل ARP الخاصة بأجهزة L3 المجاورة. فكر في مسح ذاكرة تخزين ARP المؤقت للأجهزة المجاورة يدويا لتسريع قطع حركة المرور.

تلميح: يمكنك أيضا إرسال حزمة GARP وتحديث ذاكرة تخزين ARP المؤقت للأجهزة المجاورة باستخدام أمر CLI ل FTD:

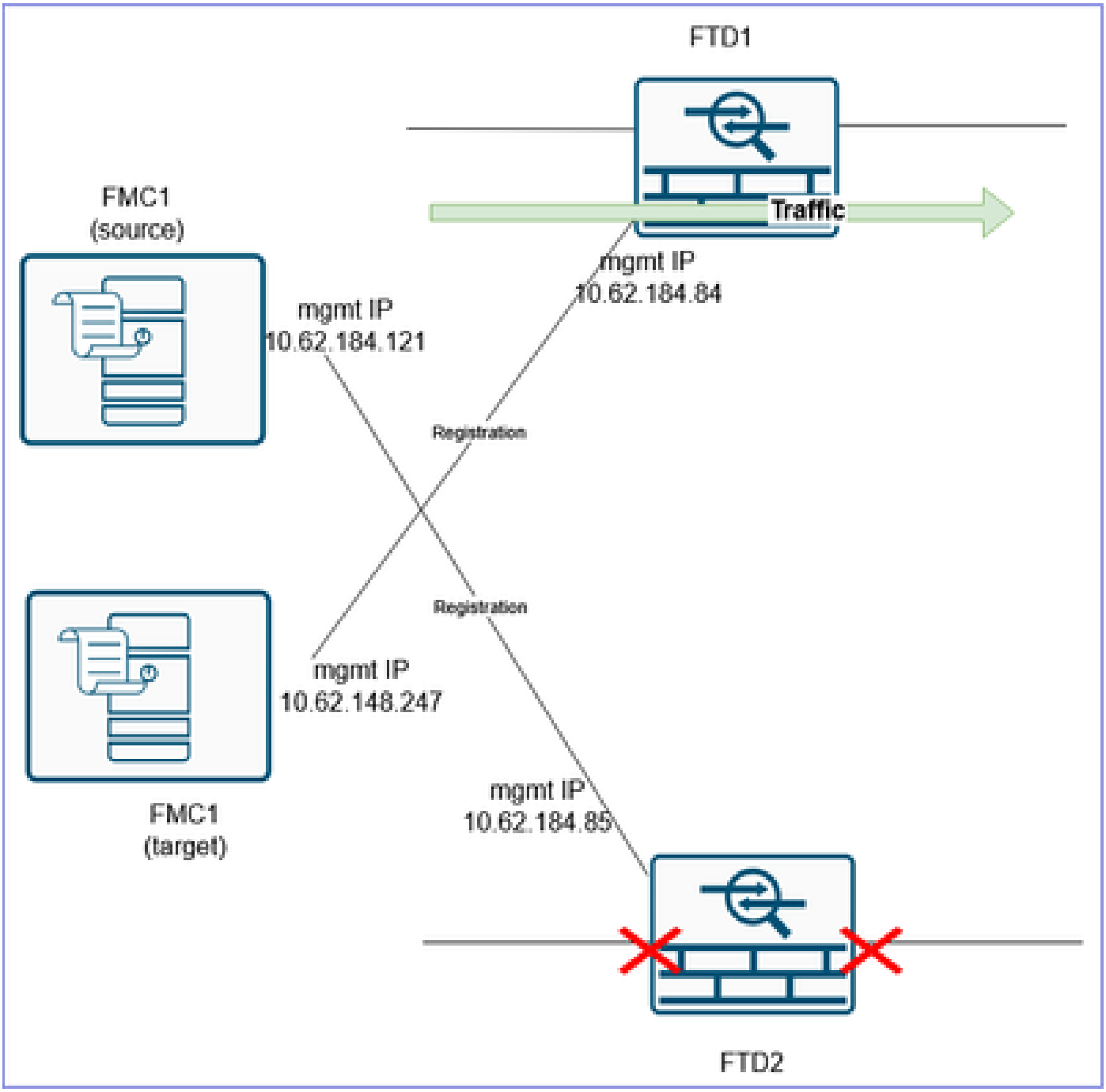
```
<#root>

FTD3100-3#

debug menu ipaddrutl 5 10.0.200.70

Gratuitous ARP sent for 10.0.200.70
```

يجب تكرار هذا الأمر لكل IP يمتلكه FW. وبالتالي، يمكن أن تكون عملية مسح ذاكرة تخزين المؤقت للأجهزة المجاورة أسرع من إرسال حزم GARP لكل IP الذي يملكه جدار الحماية.

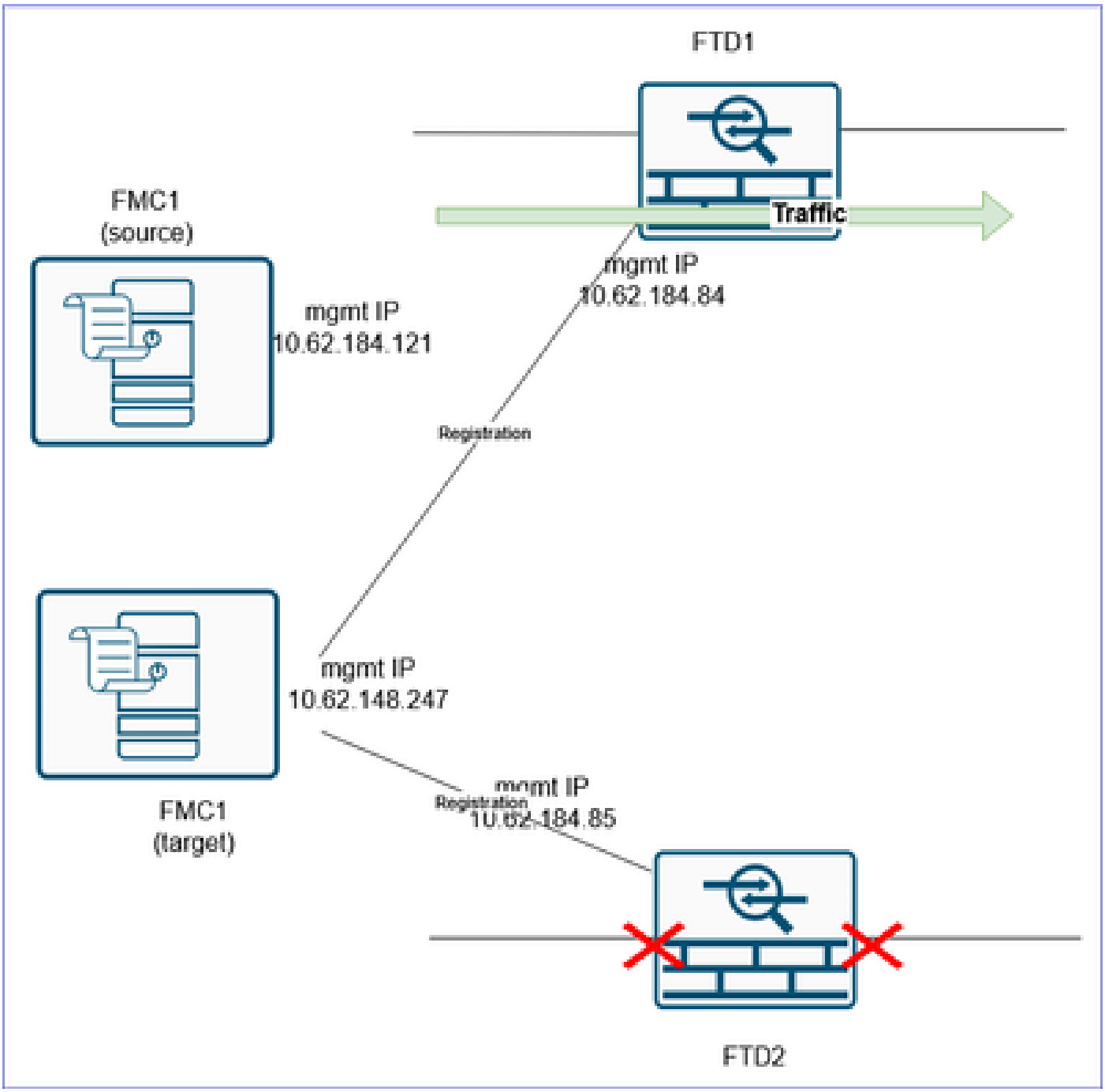
الخطوة 13. قم بترحيل "برنامج الإرسال فائق السرعة (FTD)" الثاني إلى FMC2 (الموجه FMC)

العنصر الأخير هو إصلاح زوج HA. للقيام بذلك، يلزمك أولا حذف FTD2 من FMC1 (مصدر FMC) وتسجيله إلى FMC2 (هدف FMC).

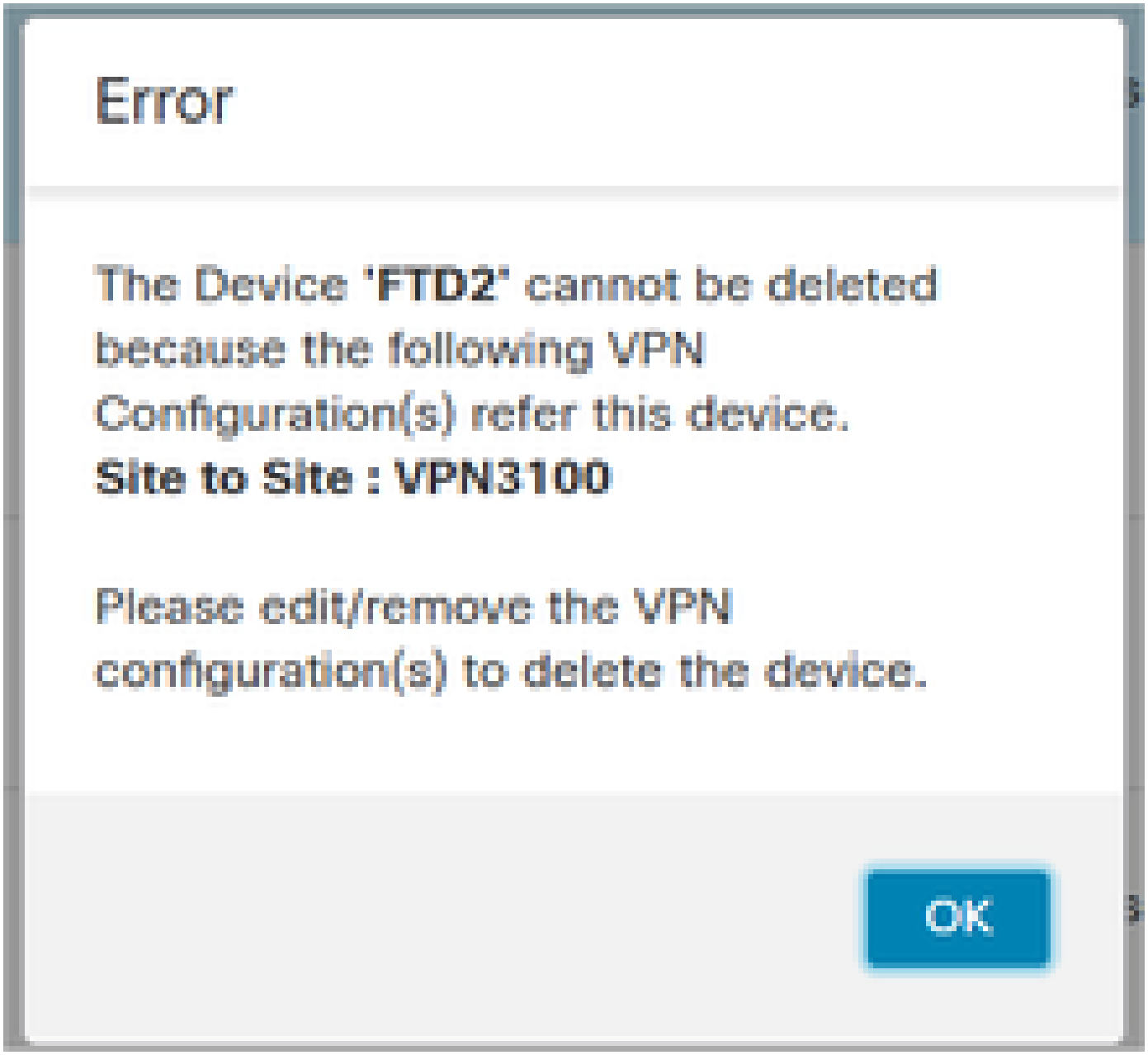
قبل:


FTD1
Traffic
mgmt IP
10.62.184.84
FMC1
(source)
mgmt IP
10.62.184.121
Registration
Registration
mgmt IP
10.62.148.247
FMC1
(target)
mgmt IP
10.62.184.85
FTD2

بعد:



إذا كان لديك تكوين شبكة VPN مرتبط ب FTD2، فيجب عليك إزالته أولا قبل حذف FTD. في حالة مختلفة، يتم عرض رسالة مماثلة لهذه:



التحقق من واجهة سطر الأوامر:

```
<#root>

>

show managers


No managers configured.
```

من الممارسات الجيدة القضاء على تكوين FTD بالكامل قبل تسجيله إلى FMC الهدف.
هناك طريقة سريعة للقيام بذلك وهي التبديل بين أوضاع جدار الحماية.

على سبيل المثال، إذا كان لديك وضع موجه، قم بالتبديل إلى الشفافية ثم عد إلى

الموجه:

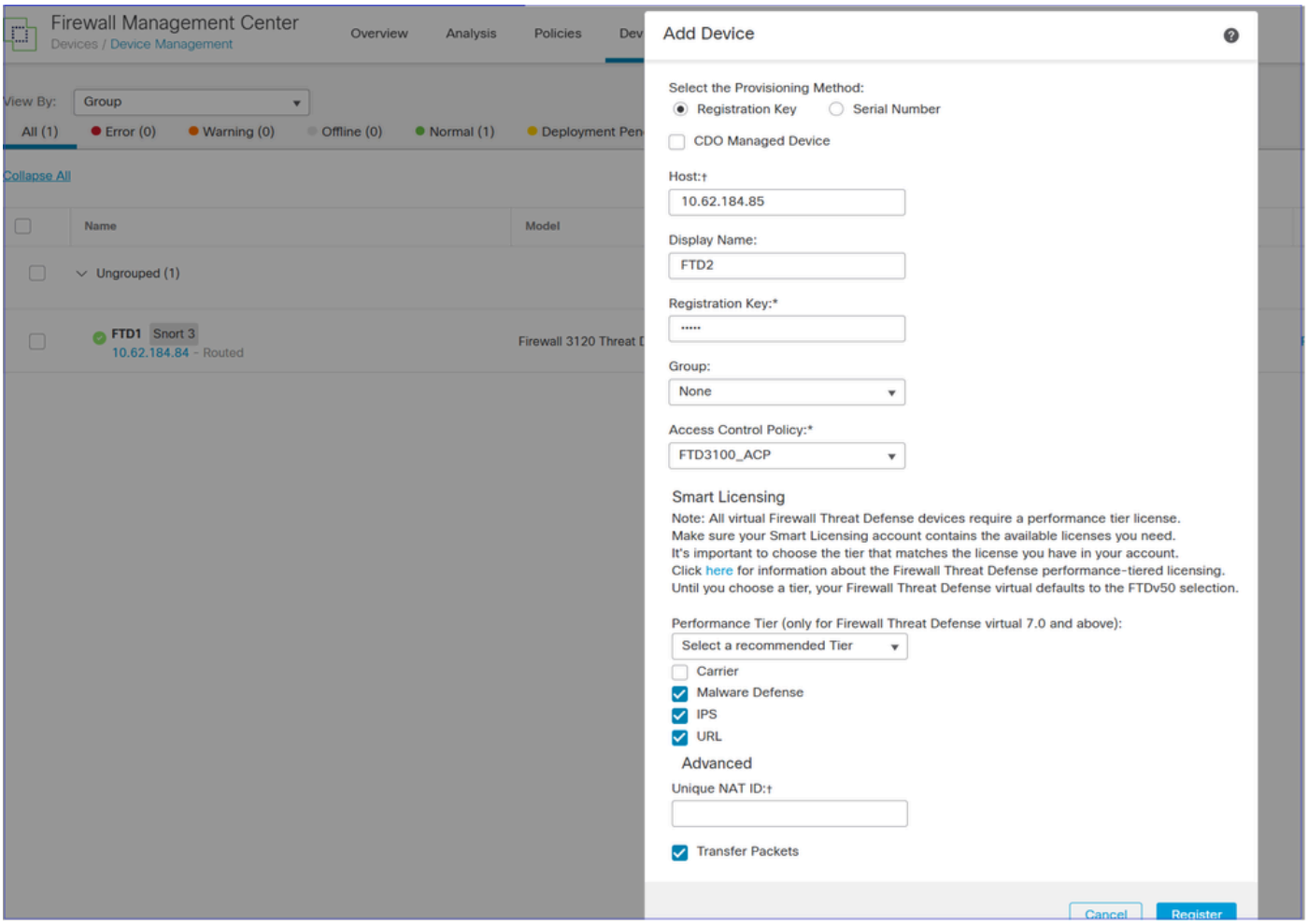
```
<#root>

>

configure firewall transparent
```

ثم:

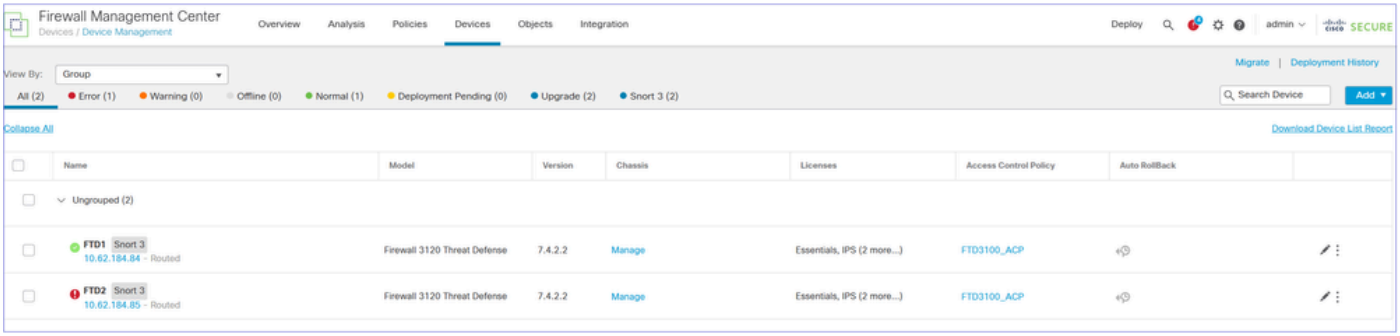
```
<#root>

>

configure firewall routed
```

ثم قم بتسجيله في FMC2 (هدف FMC):

```
<#root>

>

configure manager add 10.62.148.247 cisco


Manager 10.62.148.247 successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```



النتيجة:

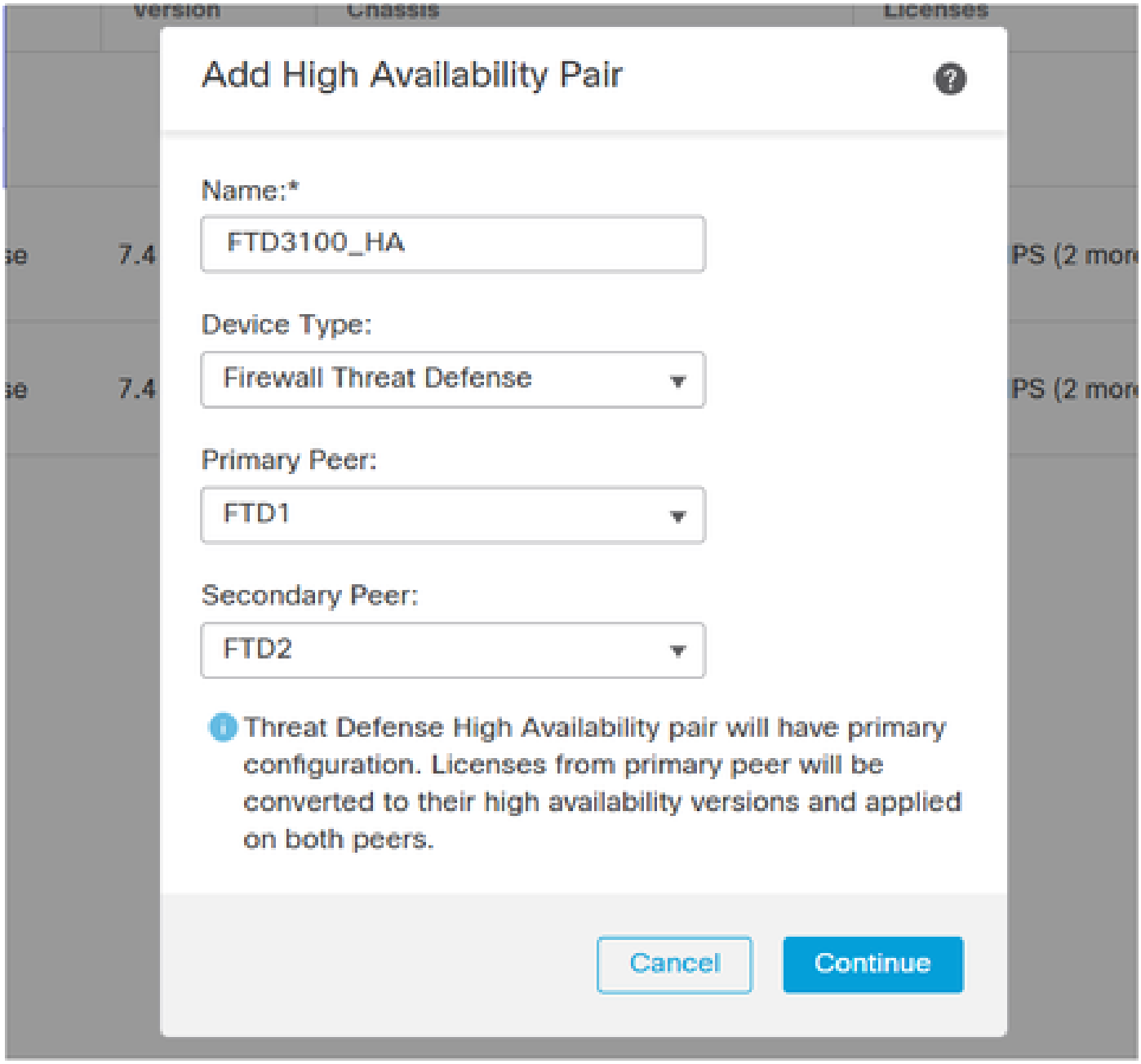


الخطوة 14. إعادة تشكيل FTD HA

ملاحظة: ويجب أيضا القيام بهذه المهمة (كأي مهمة متعلقة بالمجال الإنساني) خلال إستخدام بطاقة MW. خلال مفاوضات HA سيكون هناك انقطاع حركة مرور لمدة دقيقة واحدة تقريبا منذ أن إنخفضت واجهات البيانات.

في FMC الهدف، انتقل إلى الأجهزة > إدارة الأجهزة وإضافة > الإتاحة العالية.

تحذير: تأكد من تحديد FTD الذي يعالج حركة مرور البيانات (FTD1 في هذا السيناريو) كنظير أساسي:



أعد تكوين إعدادات HA بما في ذلك الواجهات المراقبة و IPs الاحتياطية وعناوين MAC الظاهرية وما إلى ذلك.

التحقق من خلال FTD1 CLI:

```
<#root>

FTD3100-3#

show failover | include host

        This host: Primary - Active
        Other host: Secondary - Standby Ready
```

التحقق من خلال FTD2 CLI:

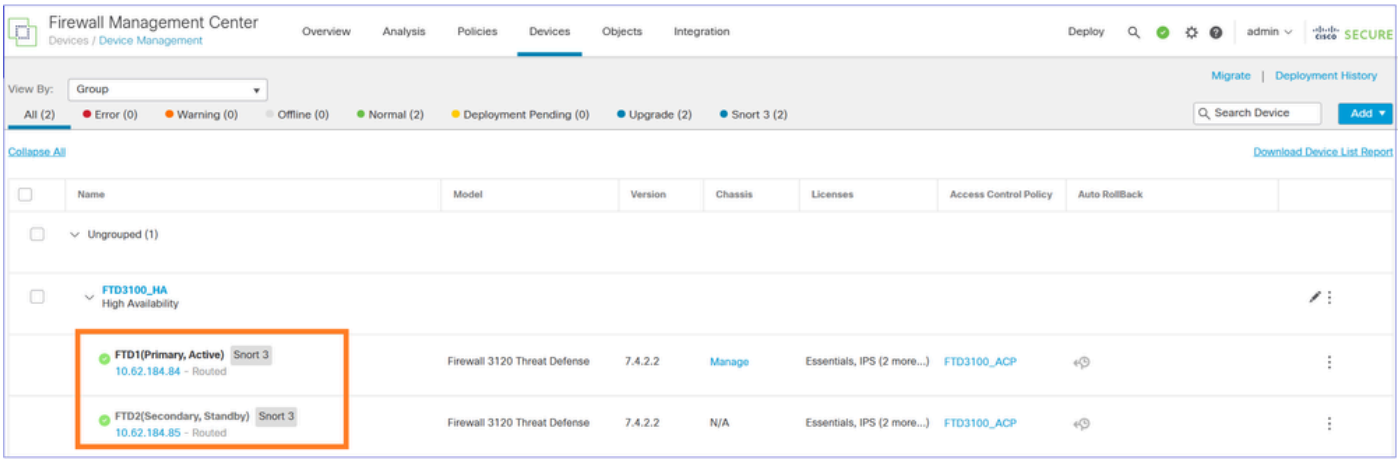
<#root>

FTD3100-3#

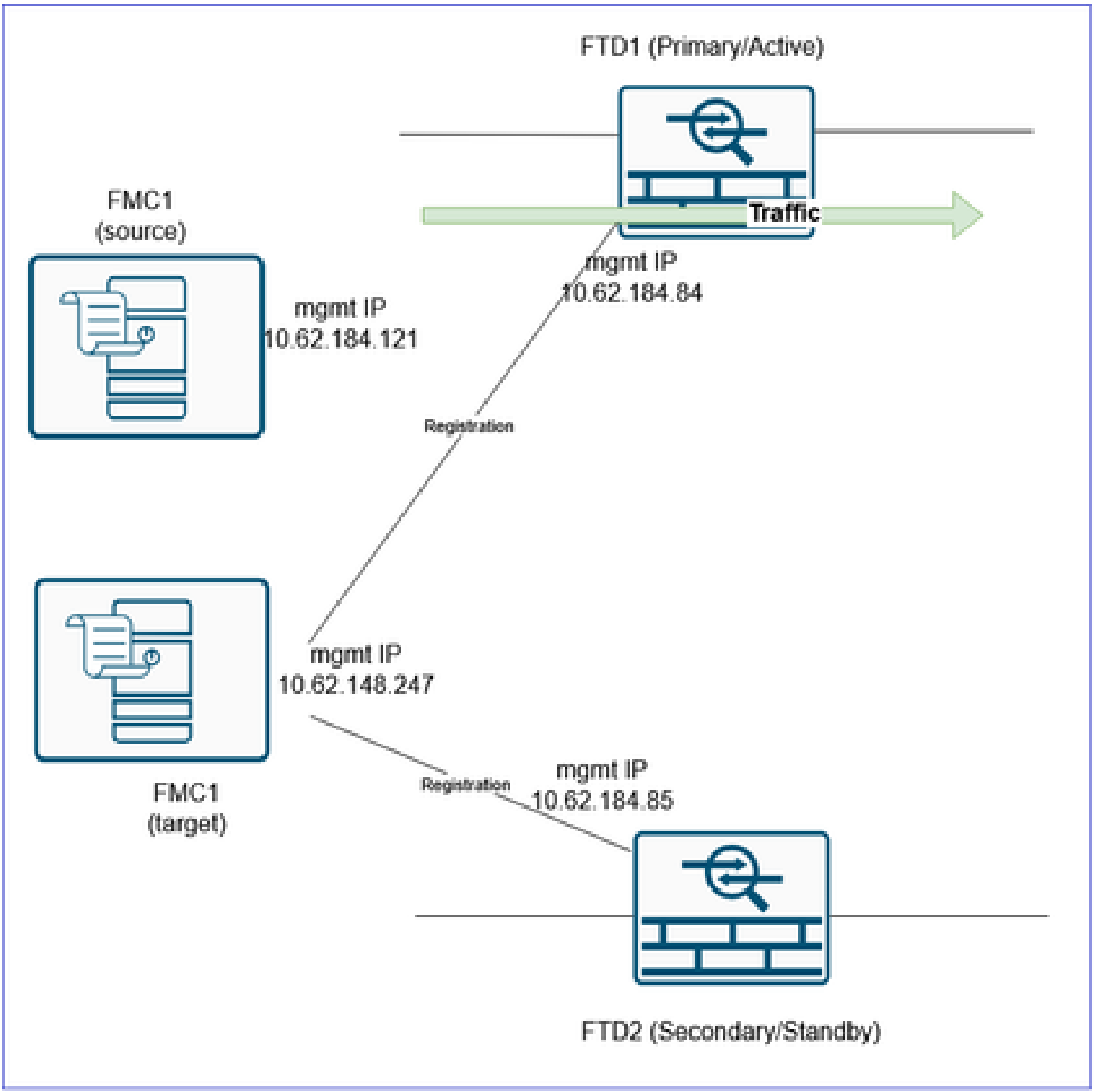
show failover | include host

```
        This host: Secondary - Standby Ready
        Other host: Primary - Active
```

التحقق من واجهة مستخدم FMC:



أخيرا، قم بإحضار/إعادة توصيل واجهات البيانات لجهاز FTD2.



المراجع

- تصدير تكوين الجهاز واستيراده
- اضافة زوج عالي التوفر
- ترحيل FTD من FMC إلى FMC آخر

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).