تكوين دمج واجهة الإدارة والتشخيص في FMC

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لتكوين دمج واجهات الإدارة والتشخيص، الميزة التي تمت إضافتها في إصدار FTD 7.4.0.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الدفاع الآمن عن تهديد جدار الحماية (FTD) من Cisco
- مركز مدير جدار الحماية الآمن (FMC) من Cisco

معلومات أساسية

في الإصدار 7.3 والإصدارات السابقة، تتم مشاركة واجهة الإدارة المادية بين الواجهة المنطقية للتشخيص (LINA) والواجهة المنطقية للإدارة (Linux).

في الإصدار 7.4 والإصدارات الأحدث، يتم دمج واجهة التشخيص مع الإدارة لتبسيط تجربة المستخدم.
بالنسبة للأجهزة الجديدة التي تستخدم الإصدار 7.4 والإصدارات الأحدث، لا يمكنك إستخدام واجهة التشخيص القديمة. تتوفر واجهة الإدارة المدمجة فقط.

المكونات المستخدمة

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

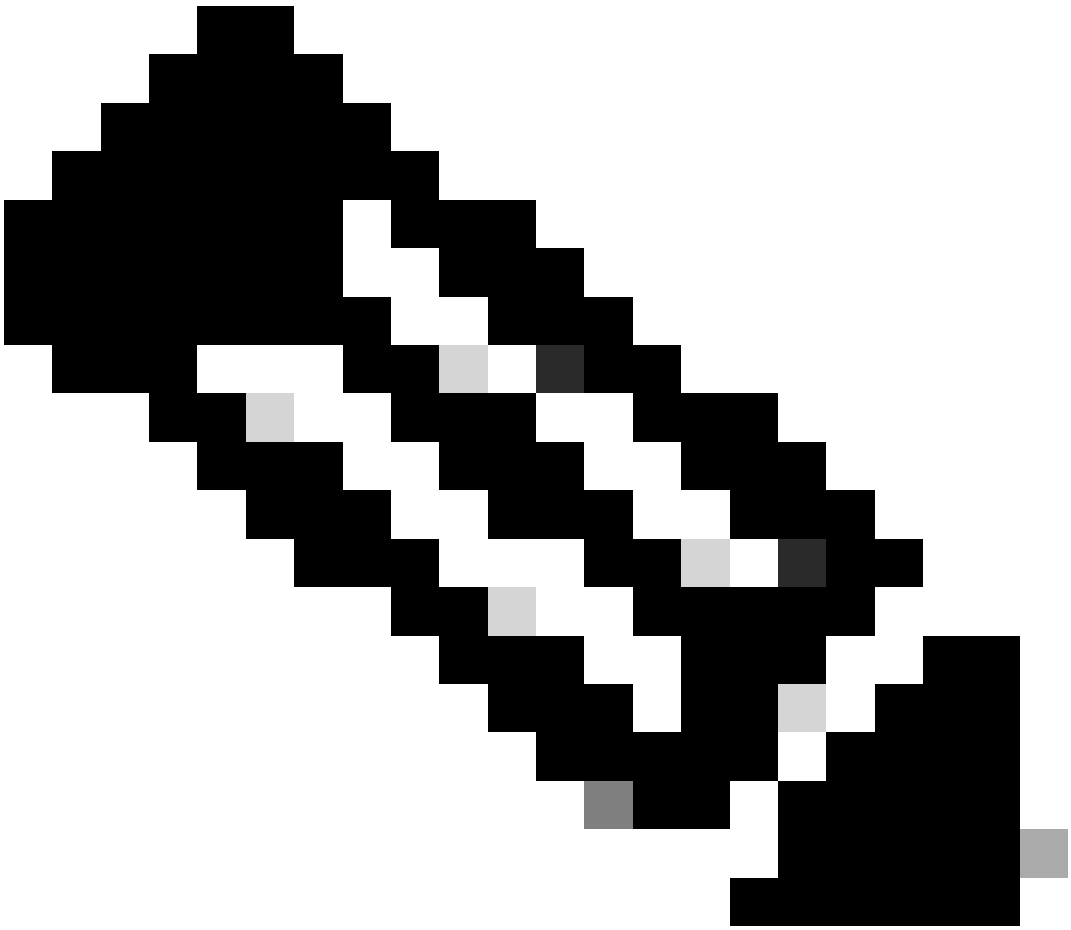
- Cisco Virtual Secure Firewall Threat Defense (FTD)، الإصدار 7.4.2
- مركز مدير جدار الحماية الآمن (FMC) الظاهري من Cisco، الإصدار 7.4.2

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.

التكوين

إذا قمت بالترقية إلى 7.4 أو إصدار أحدث، وكان لديك تكوين لواجهة التشخيص، فلديك الخيار لدمج الواجهات يدويا، أو يمكنك الاستمرار في إستخدام واجهة التشخيص المنفصلة.

في حالة عدم وجود أي تكوين لواجهة التشخيص، يتم دمج الواجهات تلقائيا.

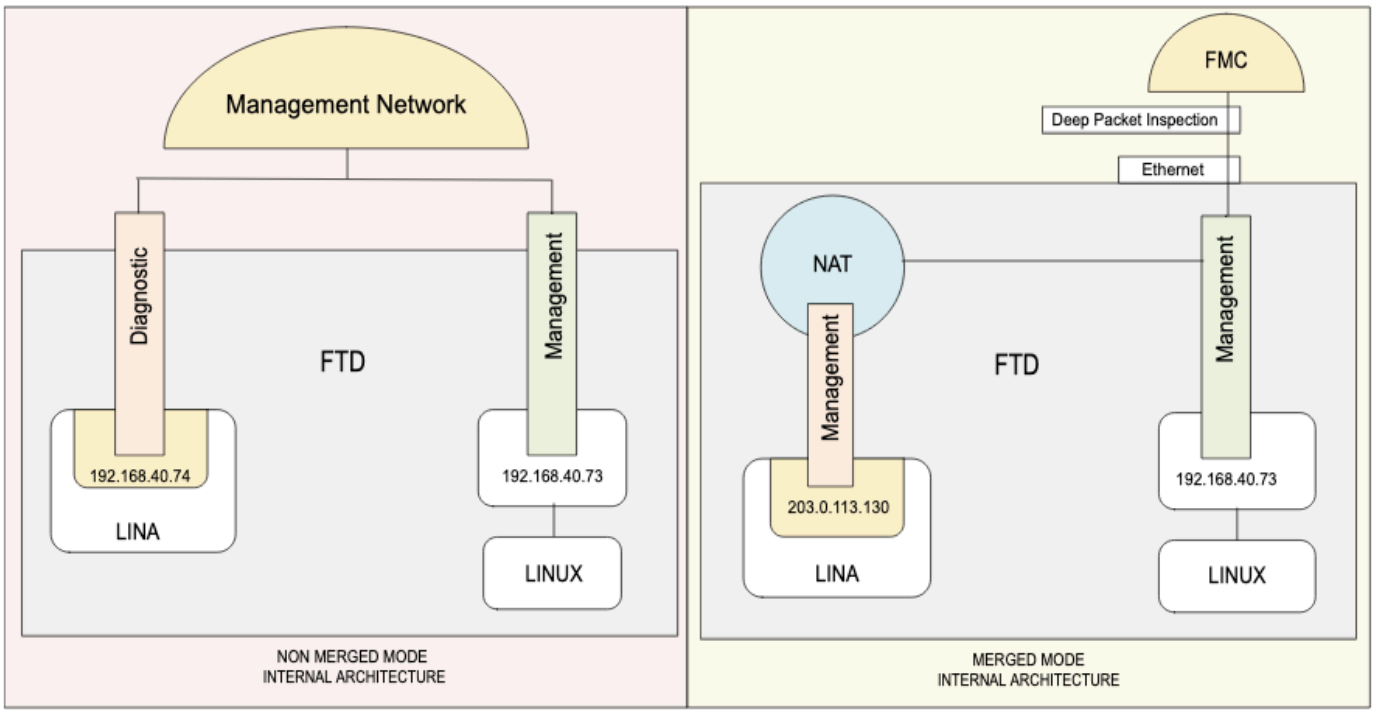


ملاحظة: ستتم إزالة دعم واجهة التشخيص في إصدار لاحق، لذلك، قم بالتخطيط

لدمج الواجهات في أقرب وقت ممكن.

الرسم التخطيطي لبنية FTD الداخلية

نظرة عامة على واجهة الإدارة المجمعة



نظرة عامة على البنية الداخلية قبل واجهة إدارة التقارب وبعدها

على اليسار، البنية الداخلية للواجهة المنطقية التشخيصية (Lina) والواجهة المنطقية للإدارة (Linux). الإصدار 7. 3 والإصدارات السابقة.

على اليمين، البنية الداخلية لواجهة إدارة واحدة. يستخدم وصول Lina إلى شبكة الإدارة خدمة NAT.

إجراء التقارب

في الحالة التي يوجد فيها التكوين في واجهة التشخيص، ال يتم دمج الواجهات تلقائيا بعد الترقية، ويجب عليك تنفيذ إجراء التقارب.

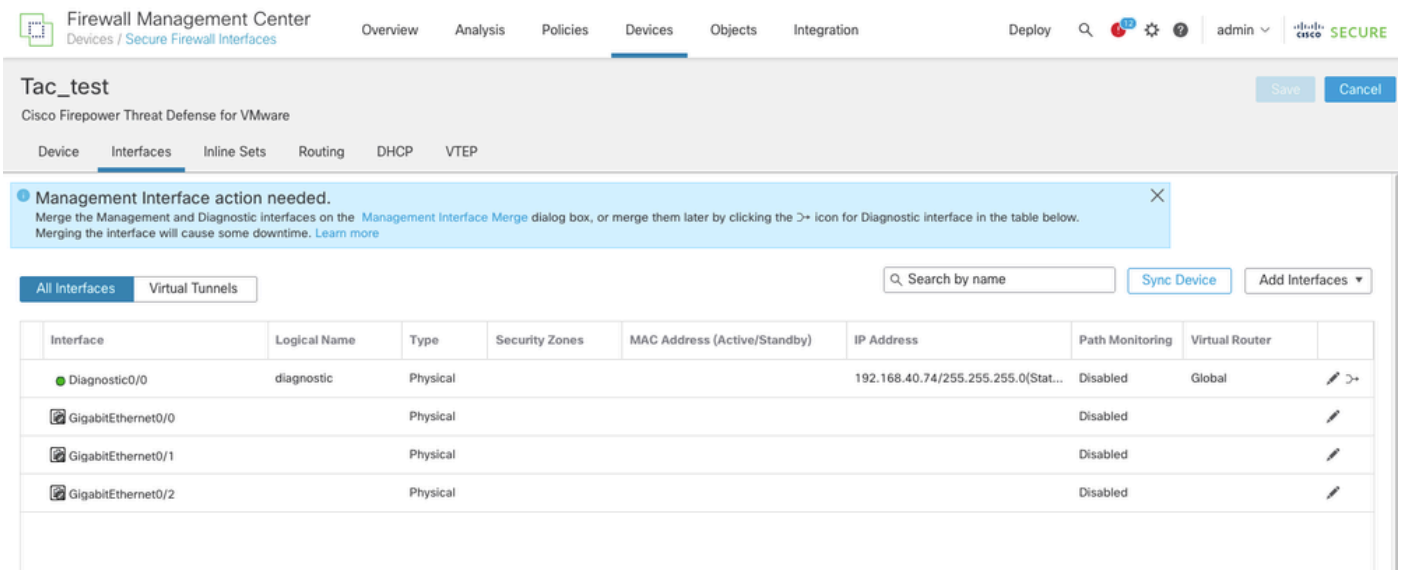
يتطلب هذا الإجراء منك الإقرار بتغييرات التكوين، وفي بعض الحالات، إصلاح التكوين يدويا.

لعرض الوضع الحالي للجهاز، أدخل الأمر show management-interface converge في واجهة سطر أوامر CLI (واجهة سطر الأوامر) ل FTD

```
> show management-interface convergence
no management-interface convergence
```

توضح هذه النتيجة أن واجهات الإدارة غير مدمجة.

الخطوة 1.
على واجهة مستخدم FMC، انتقل إلى الأجهزة > إدارة الأجهزة، وحدد FTD المراد تحريره. يتم فتحه مباشرة إلى علامة التبويب الواجهات.

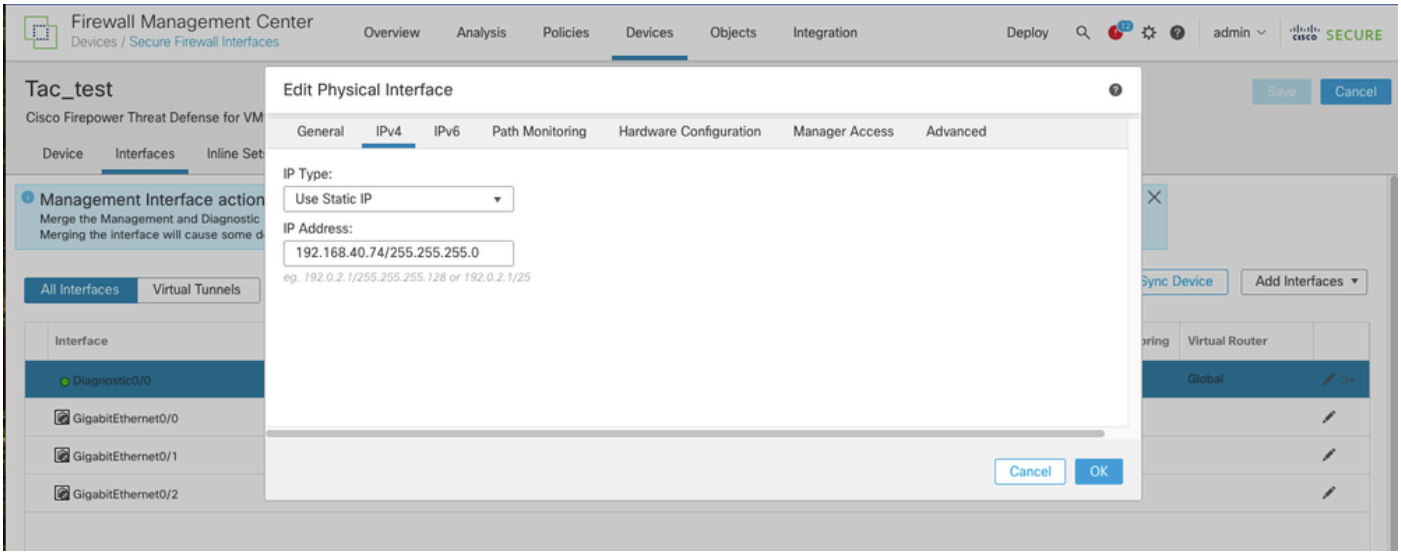


الإجراء المطلوب لدمج واجهة التشخيص والإدارة بعد ترقية الجهاز إلى إصدار البرنامج 7.4.2

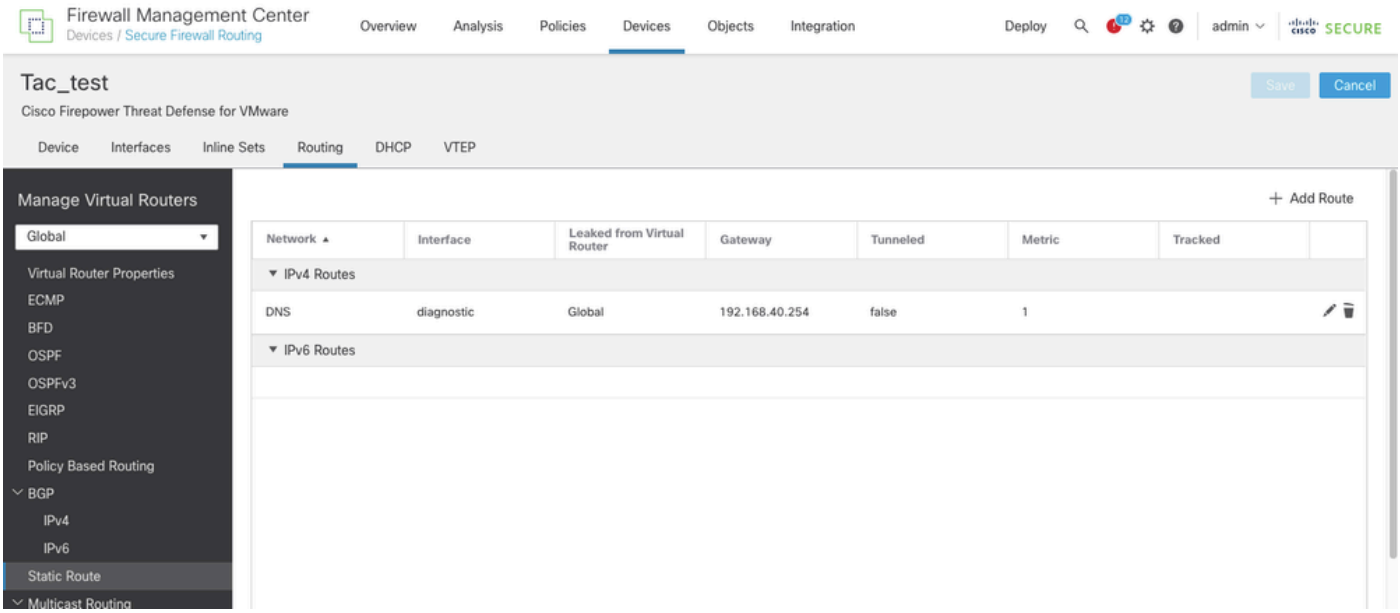
الخطوة 2.

قم بإزالة جميع التكوين على واجهة التشخيص. من الضروري ألا تحتوي واجهة التشخيص على أي تكوين لمتابعة الدمج.

على سبيل المثال، في واجهة التشخيص هذه، هناك: عنوان IP والموجه الثابت.



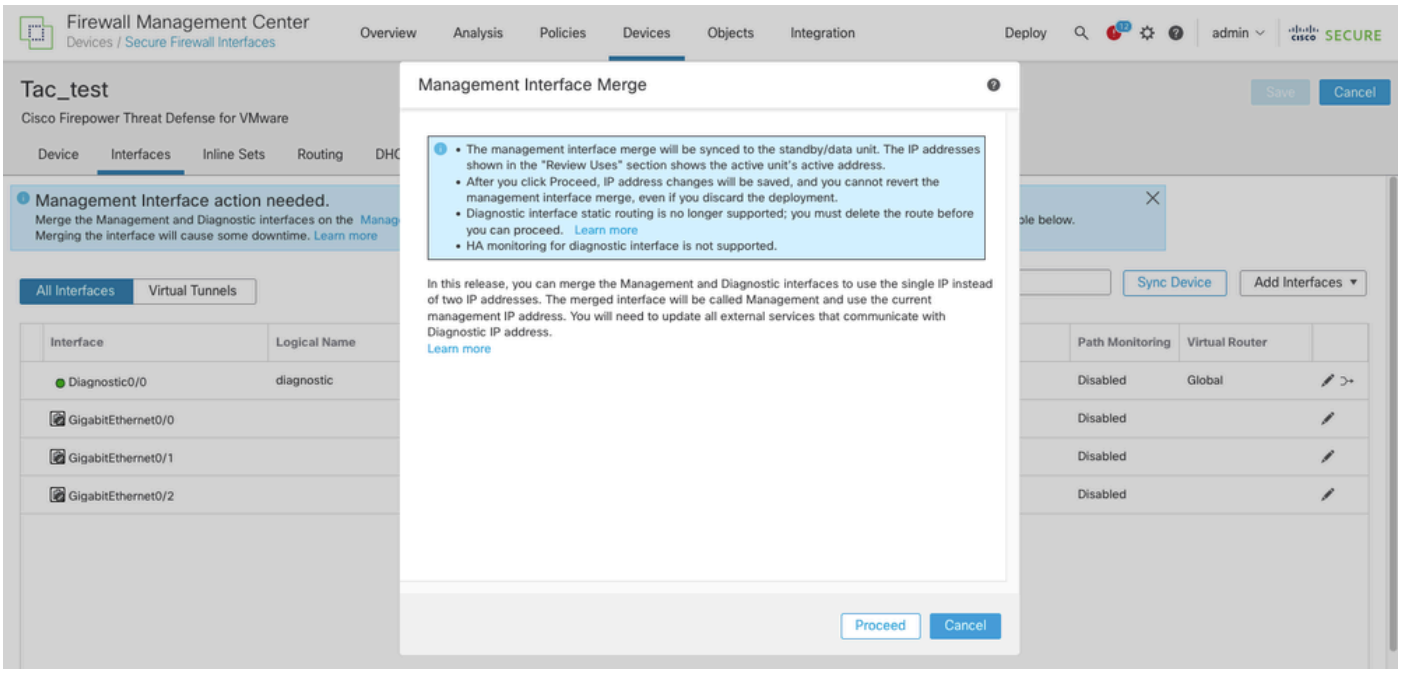
إزالة عنوان IP للواجهة التشخيصية



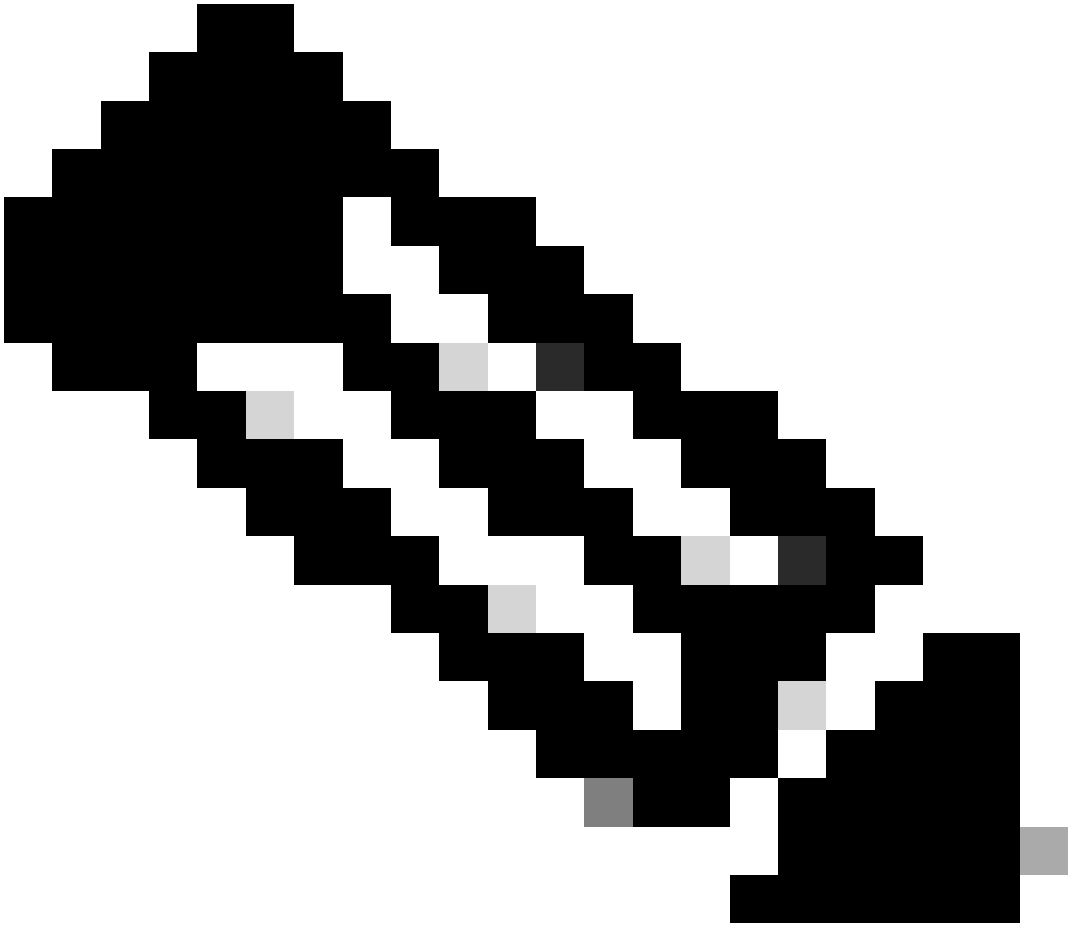
تكوين المسار الثابت على واجهة التشخيص

الخطوة 3.

انقر فوق منطقة إجراء دمج واجهة الإدارة المطلوبة أو أيقونة الدمج المجاورة لأيقونة التحرير (القلم الرصاص) على واجهة التشخيص.

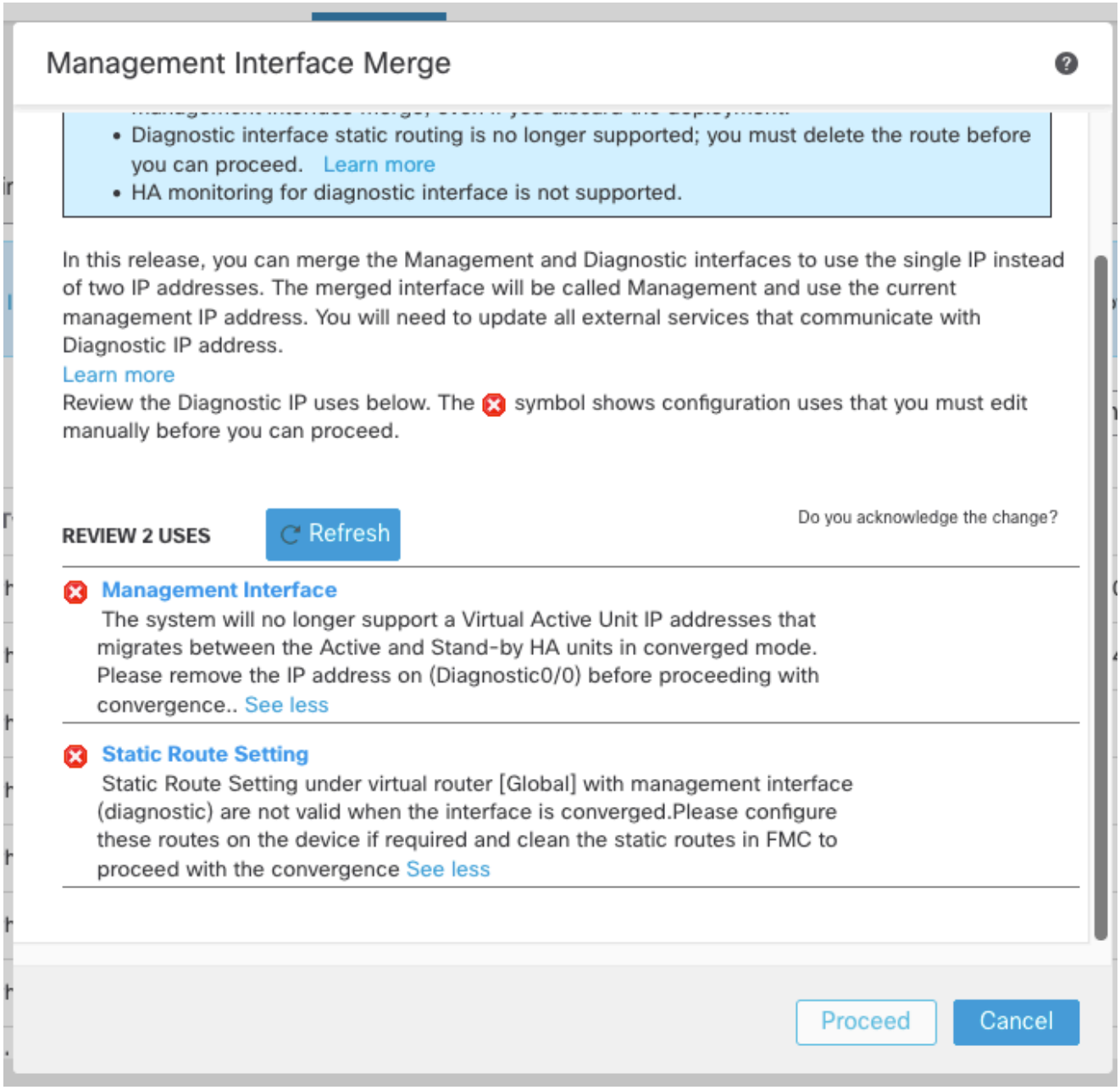


معلومات دمج واجهة الإدارة قبل المتابعة



ملاحظة: بالنسبة للأزواج والمجموعات عالية التوفر، قم بتنفيذ هذه المهمة على الوحدة النشطة/وحدة التحكم. يتم نسخ التكوين المدمج نسخا متماثلا تلقائيا إلى وحدات الاستعداد/البيانات.

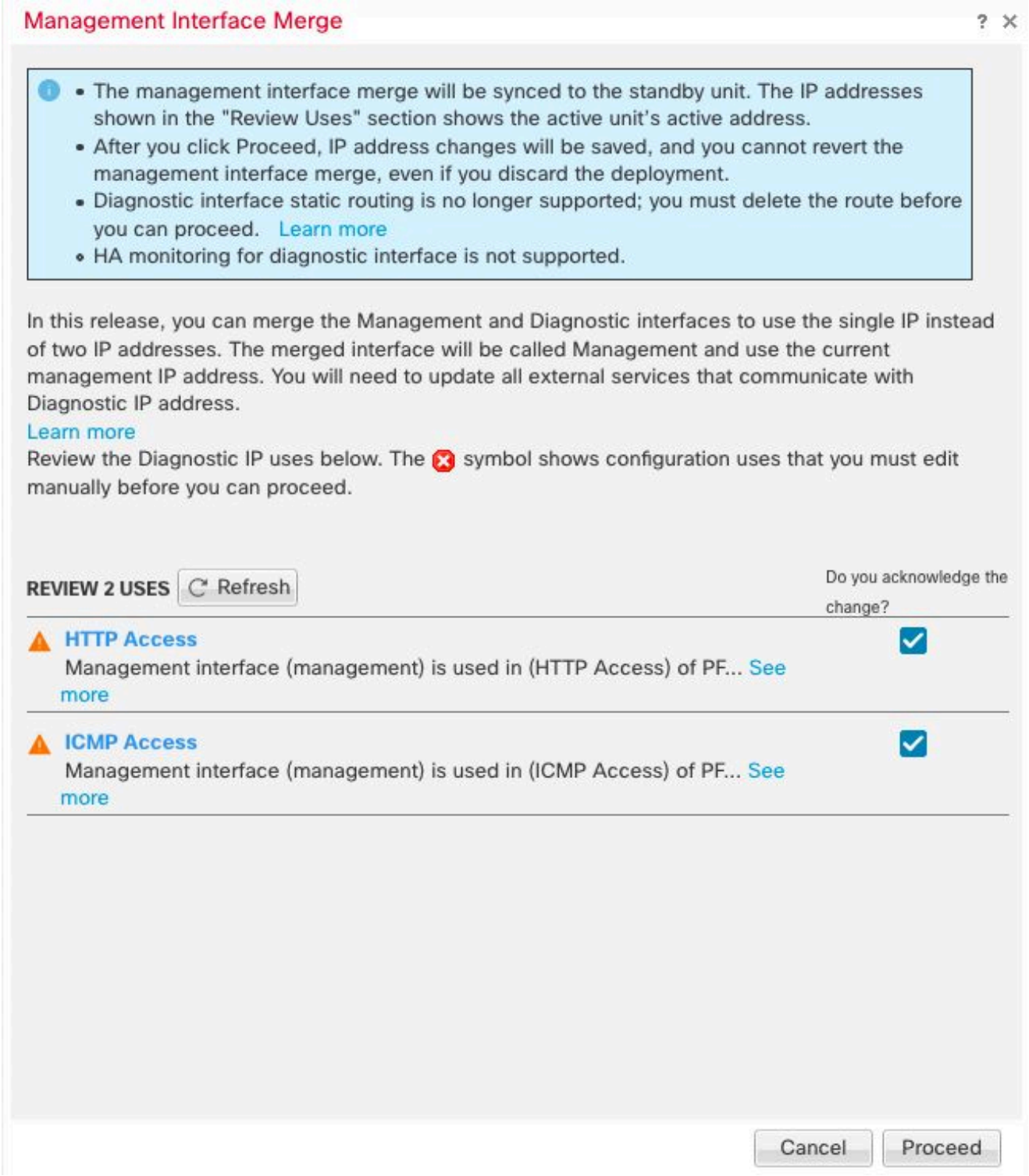
- لأي تكرار يتطلب أن يكون تغيير أو إزالة يدوية، يمكن أن تظهر أيقونة تحذير.



مثال التحذير حول التكوينات المطلوب إزالتها قبل الدمج

إذا كان هذا هو الحال: قم بإلغاء مربع الحوار، ثم تابع إزالة التكوين أو إعادة التكوين، ثم أعد فتح مربع الحوار "دمج واجهة الإدارة".

- يتم وضع علامة على إعدادات النظام الأساسي التي تعمل على الجهاز برمز تحذير وتتطلب إشعارا.



مثال على التحذير من تكوينات إعدادات النظام الأساسي التي يجب تحريرها

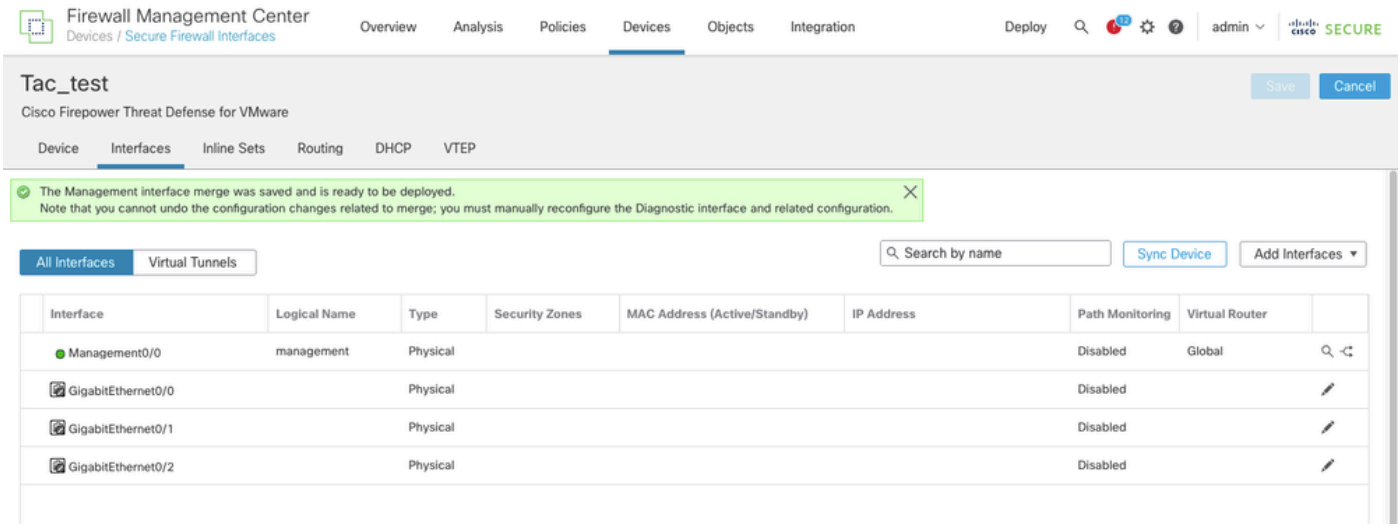
- انقر المربع في هل تعترف بالتغيير؟ عمود، ثم انقر فوق متابعة.

الخطوة 4.

بعد دمج التكوين، يتم عرض شعار نجاح:
"تم حفظ دمج واجهة الإدارة وهو جاهز للنشر.
لاحظ أنه لا يمكنك التراجع عن تغييرات التكوين المتعلقة بالدمج؛ يجب إعادة تكوين واجهة

التشخيص والتكوين ذي الصلة يدويا.

قم بنشر التكوين المدمج الجديد.



تم حفظ دمج واجهة الإدارة وأصبح جاهزا للنشر

تظهر واجهة الإدارة على صفحة الواجهات، بالرغم من أنها للقراءة فقط.

بعد النشر، يكون إجراء التقارب على واجهة الإدارة قد اكتمل.

الخطوة 5. إختياري

إذا كان لديك أي خدمات خارجية اتصلت بواجهة التشخيص، فأنت بحاجة إلى تغيير التكوين الخاص بها لاستخدام عنوان IP لواجهة الإدارة، حيث تمت إزالة إدارة المسار الاحتياطي على الوضع المجمع.

على سبيل المثال:

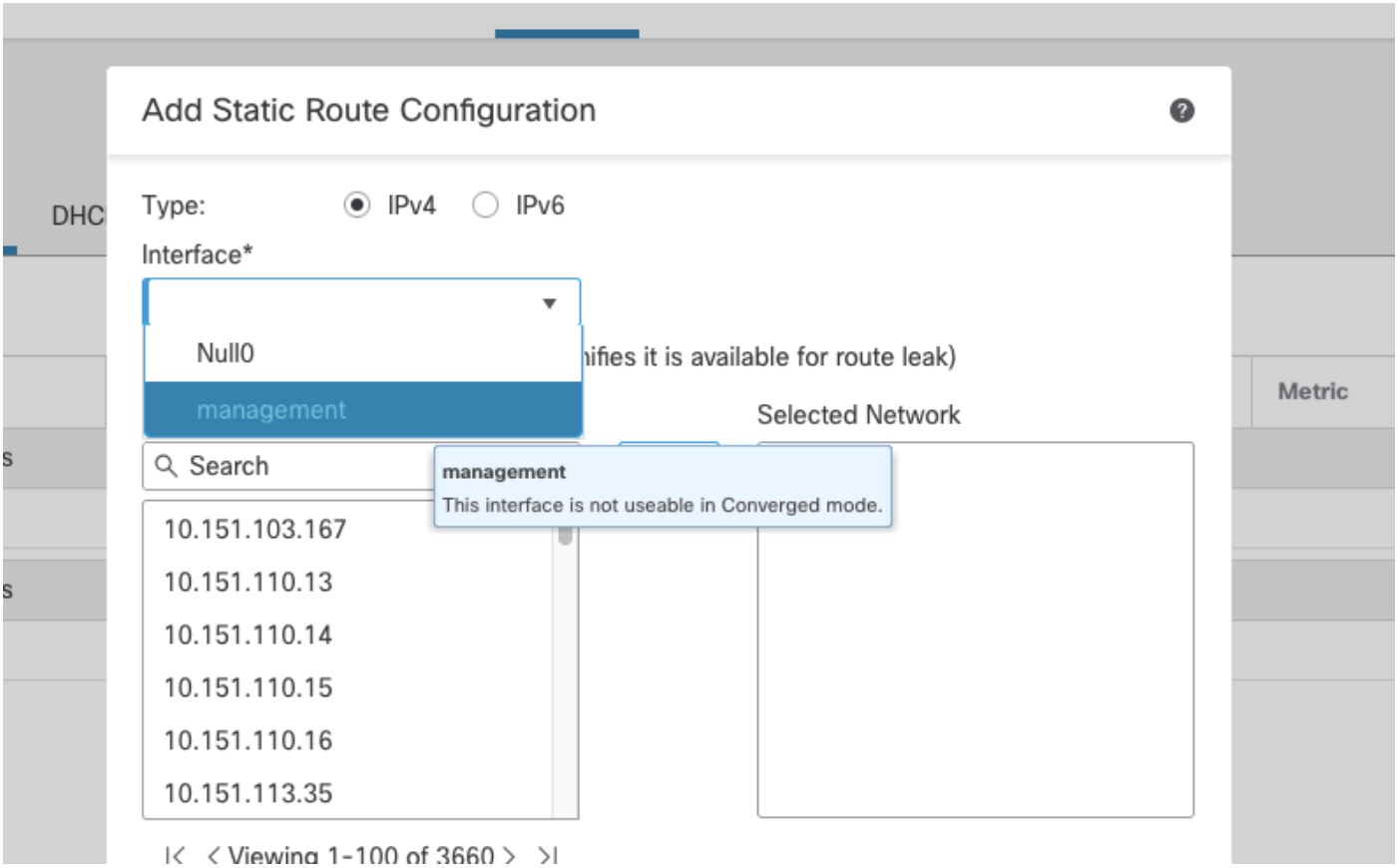
- عميل SNMP
- خادم RADIUS
- خادم DNS الذي يمكن الوصول إليه عبر شبكة الإدارة، يجب على المستخدم تحديد تمكين بحث DNS بشكل صريح عبر واجهة التشخيص/الإدارة أيضا." في إعدادات النظام الأساسي > تكوين DNS كاستثناء يتم تعيينه لعمليات البحث في DNS و ICMP (إختبار الاتصال و traceroute): وفي هذه الحالات، يستخدم الدفاع عن التهديد البيانات ثم يعود إلى الإدارة بشكل تلقائي في حالة عدم العثور على مسار.

يمكن تكوين إستخدام المسارات الثابتة لواجهة الإدارة فقط من خلال واجهة سطر أوامر (CLI) ل FTD (Linux)

يرسل المسار الافتراضي لمنفذ إدارة Lina جميع الإطارات إلى وحدة Linux.

```
> configure network static-routes ipv4 add management ?
  IP address AAA.BBB.CCC.DDD where each part is in the range 0-255  destination address
```

على واجهة مستخدم FMC، يتم تصنيف واجهة الإدارة للتحديد.



لا تتوفر واجهة الإدارة للتحديد على المسارات الثابتة بعد اكتمال الدمج.

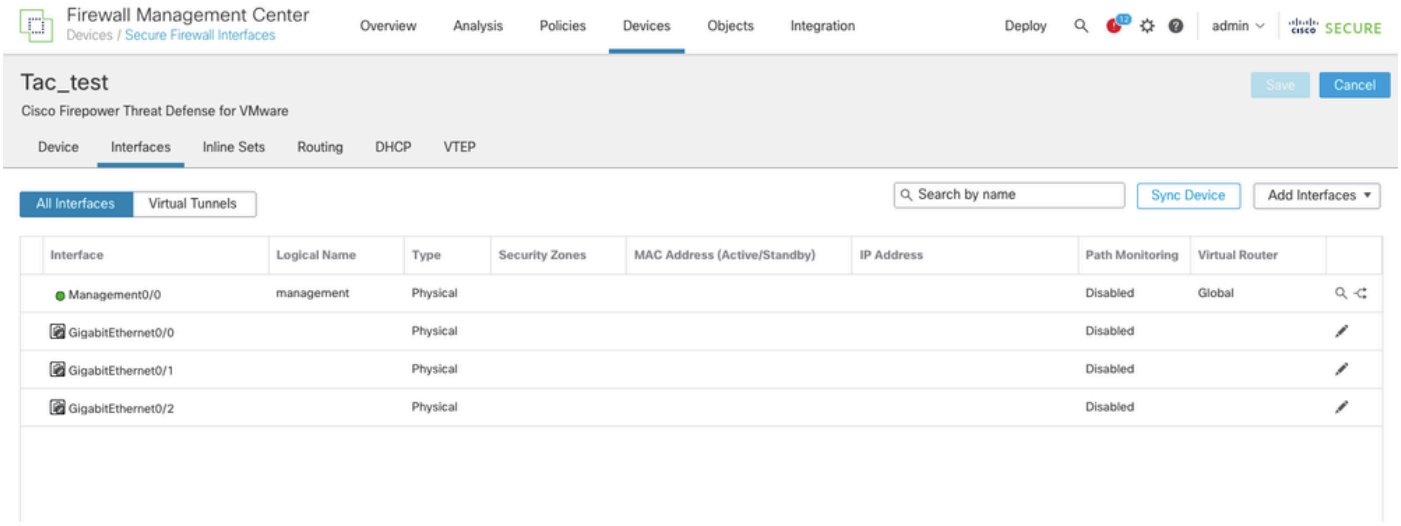
التحقق من الصحة

التغييرات المتوقعة بعد الدمج على واجهة الإدارة

- التحقق من وضع التقارب على واجهة سطر الأوامر (CLI) ل FTD من خلال تنفيذ الأمر

```
> show management-interface convergence
management-interface convergence
```

- على واجهة مستخدم FMC، يتم تغيير اسم الواجهة إلى Management0/0 ، الاسم المنطقي إلى الإدارة.



تأكيد الدمج على اسم واجهة الإدارة والاسم المنطقي

- على واجهة سطر واجهة سطر أوامر (CLI) لـ FTD، يتم تكوين عناوين IP الجديدة تلقائيا على Lina لواجهة الإدارة.
  يتم إستخدام NAT كتنفيذ داخلي: إن عنوان IPv4 الخاص الداخلي 203.0.113.130 وعنوان IPv6 fd00:0:1:1::2 هي تلك المعينة (وكلاهما يخضع للتغيير).
  إن عناوين IPs هذه هي NATed إلى عناوين IPv4 و IPv6 الخاصة بنواة ليونكس العامة، لذلك لم تعد هناك حاجة إلى عناوين IP العامة على Lina.

  في وضع الخبراء، يعرض "ifconfig" عنوان IPv4 داخلي (203.0.113.129) وعنوان IPv6 (fd00:0:1:1::1) لنظام التشغيل Linux.

```
FTD CLI Clish:
> show interface management
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, DLY 10 usec
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0050.56b3.f75d, MTU 1500
        IP address 203.0.113.130, subnet mask 255.255.255.248

Expert mode on Linux:
root@ftd01:/home/admin# ifconfig
...
tap5: flags=4419


         mtu 1500
        inet 203.0.113.129  netmask 255.255.255.248  broadcast 203.0.113.135
        inet6 fe80::8403:9ff:fefb:6d16  prefixlen 64  scopeid 0x20


        inet6 fd00:0:1:1::1  prefixlen 123  scopeid 0x0
```

أستكشاف الأخطاء وإصلاحها - حالة الدراسة

في حالة الدراسة هذه، قامت واجهة التشخيص على FTD ظاهري بتكوين عناوين IP منفصلة للاتصال بالخدمات الخارجية الخاصة بالبحث عن DNS، قبل الترقية إلى 7.4.2.

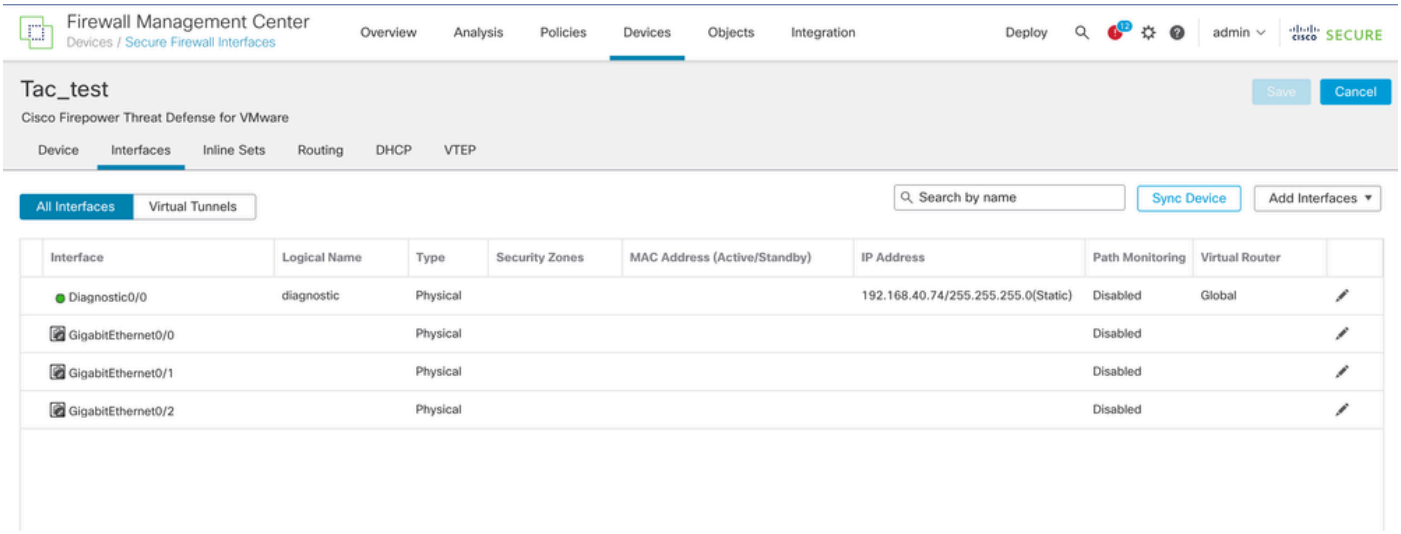
بعد الترقية إلى 7.4.2، يلزم توفر التقارب، وهذه هي الطريقة التي يتم بها التكوين في واجهة مستخدم FMC و FTD CLI Lina و Linux قبل الدمج وبعده.

هناك أيضا التقاط حركة مرور على FTD CLI Lina و Linux لعرض حركة المرور باستخدام حركة واجهة التشخيص المنطقية لاستخدام واجهة الإدارة.

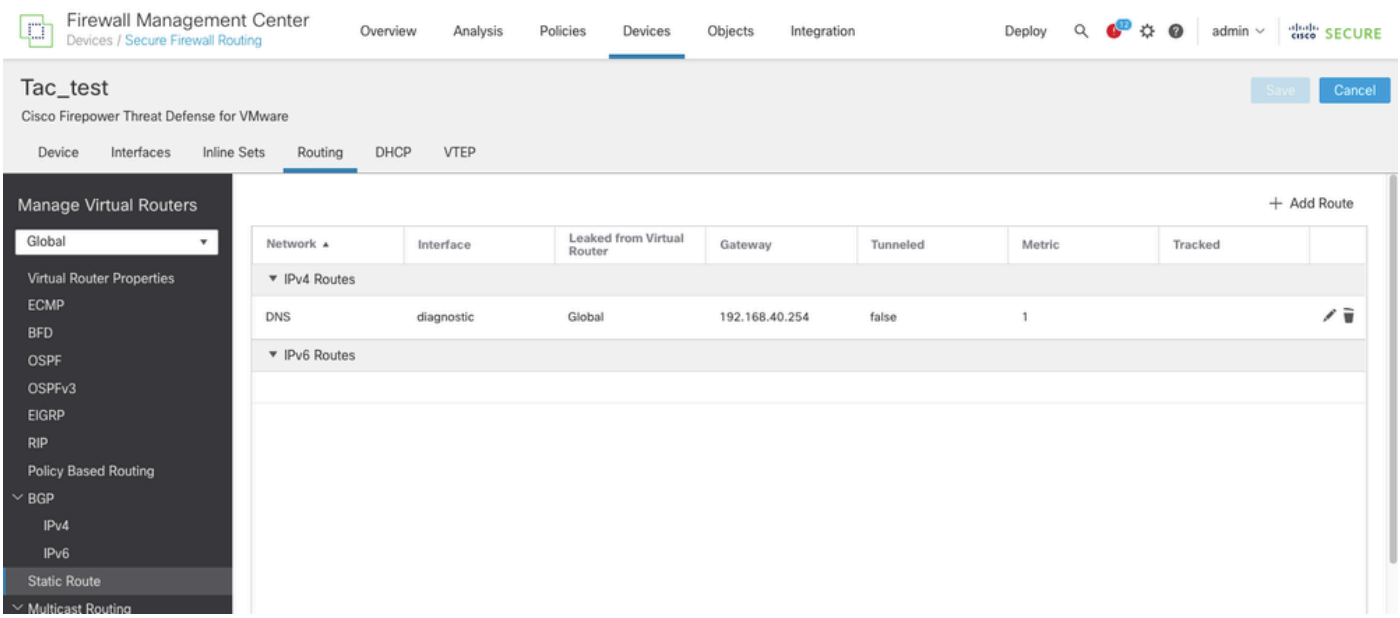
قبل تكوين تقارب

تحتوي واجهة التشخيص على IP منفصل ومسار ثابت للبحث عن DNS، بهذه الطريقة تعمل باستخدام كل الواجهات المنطقية من Lina إلى Linux في FTD.

تكوين واجهة مستخدم FMC



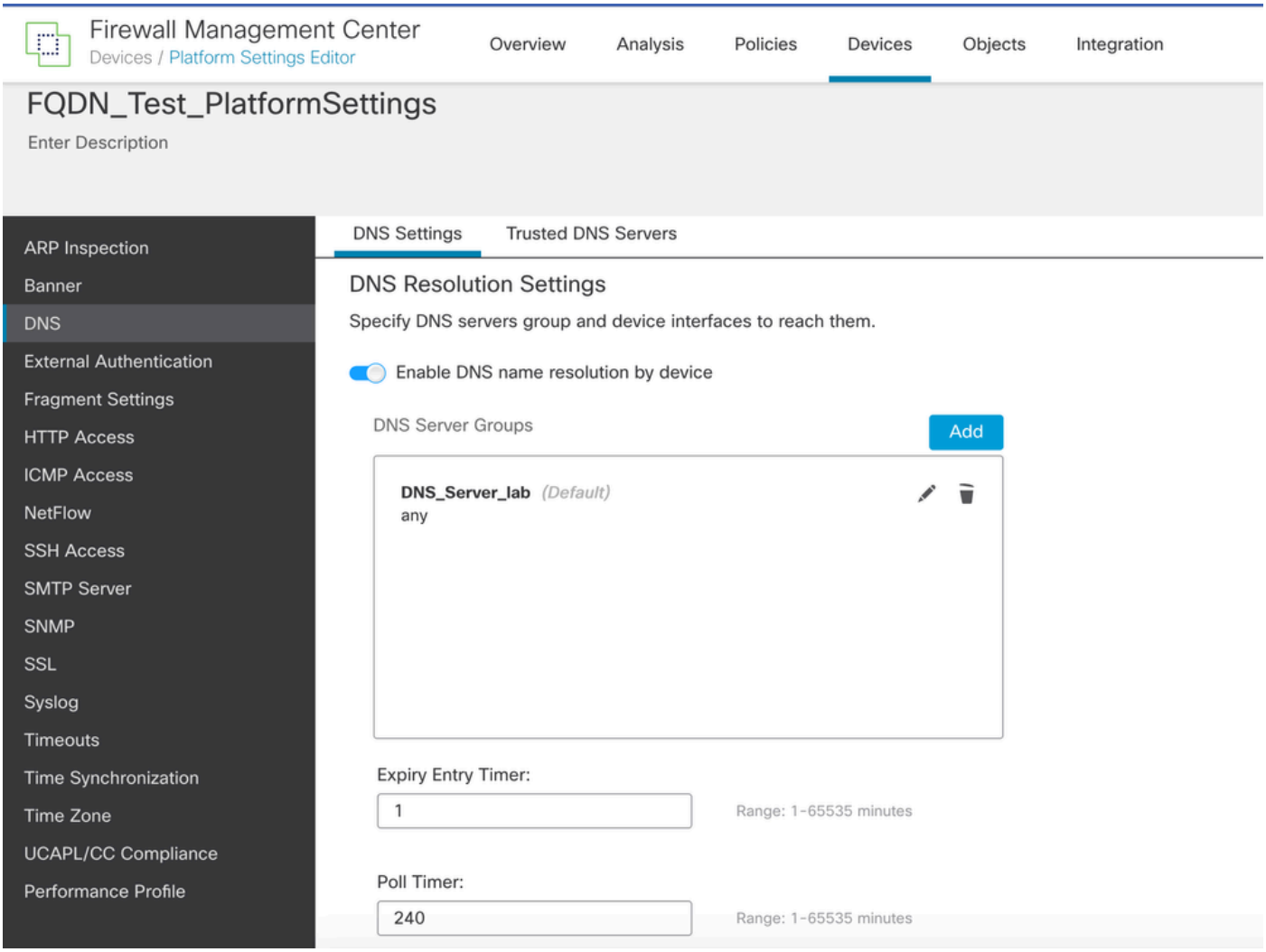
تكوين الواجهة التشخيصية قبل الدمج



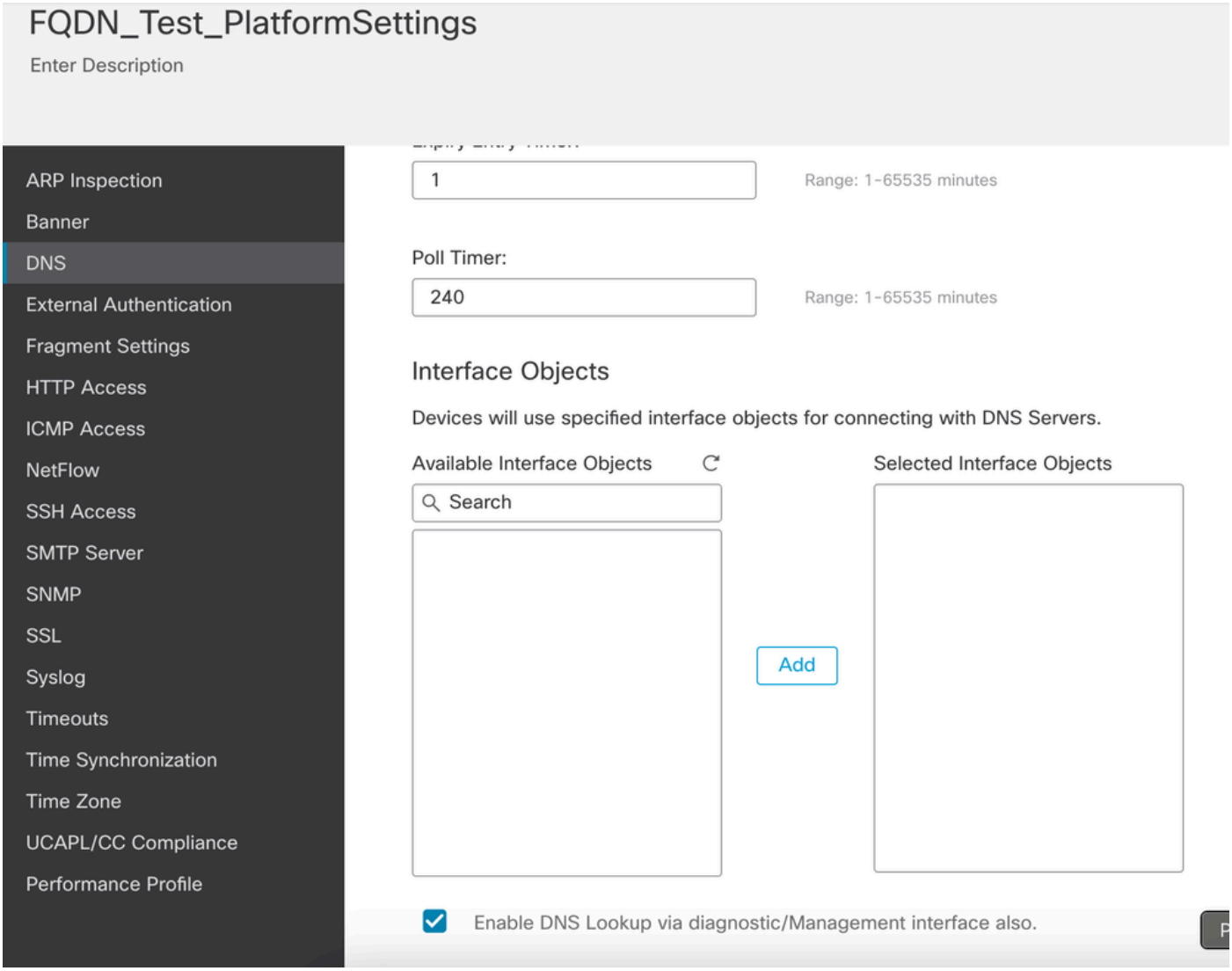
المسار الثابت الذي تم تكوينه على الواجهة التشخيصية

تجاوز تكوين DNS

أجهزة > إعدادات النظام الأساسي، حدد السياسة، ثم علامة تبويب DNS.



تكوين DNS في إعدادات النظام الأساسي



تم تحديد خانة الاختيار لتمكين بحث DNS عبر واجهة التشخيص/الإدارة أيضا

تكوين الواجهة التشخيصية عبر FTD LINA

```
interface Management0/0
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.40.74 255.255.255.0

ftd01# sh ip
System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Management0/0            diagnostic          192.168.40.74   255.255.255.0   manual
Current IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Management0/0            diagnostic          192.168.40.74   255.255.255.0   manual

ftd01# sh route management-only
Routing Table: mgmt-only
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

S        10.10.10.10 255.255.255.255 [1/0] via 192.168.40.254, diagnostic
C        192.168.40.0 255.255.255.0 is directly connected, diagnostic
L        192.168.40.74 255.255.255.255 is directly connected, diagnostic
```

تكوين DNS على FTD CLI Lina

```
ftd01# sh run dns
dns domain-lookup diagnostic
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 diagnostic
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
```

التقاط على الواجهة التشخيصية لحركة مرور DNS المتجهة إلى خادم DNS 10.10.10.10

```
ftd01# sh cap
capture diag type raw-data trace detail interface diagnostic [Capturing - 340 bytes]
  match udp any host 10.10.10.10 eq domain

ftd01# sh cap diag

5 packets captured

   1: 00:15:39.660442       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
   2: 00:15:54.661953       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
   3: 00:16:09.661739       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
   4: 00:16:24.667674       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
   5: 00:16:39.684946       192.168.40.74.59939 > 10.10.10.10.53:  udp 27
5 packets shown
ftd01#
```

التقاط على وضع خبير Linux، لتأكيد التدفق الصحيح لحركة مرور بحث DNS على واجهة الإدارة من الواجهة التشخيصية

```
root@ftd01:/home/admin# tcpdump -i br1 port 53
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
04:58:14.648941 IP 192.168.40.74.49171 > 10.10.10.10.domain: 5655+ AAAA? cisco.com. (27)
04:58:29.656317 IP 192.168.40.74.11606 > 10.10.10.10.domain: 26905+ A? cisco.com. (27)
04:58:44.686568 IP 192.168.40.74.11606 > 10.10.10.10.domain: 24324+ A? cisco.com. (27)
04:58:59.704586 IP 192.168.40.74.11606 > 10.10.10.10.domain: 35592+ A? cisco.com. (27)
04:59:14.742685 IP 192.168.40.74.11606 > 10.10.10.10.domain: 40993+ A? cisco.com. (27)
04:59:29.763690 IP 192.168.40.74.11606 > 10.10.10.10.domain: 62225+ A? cisco.com. (27)
04:59:44.796484 IP 192.168.40.74.11606 > 10.10.10.10.domain: 25350+ A? cisco.com. (27)
```

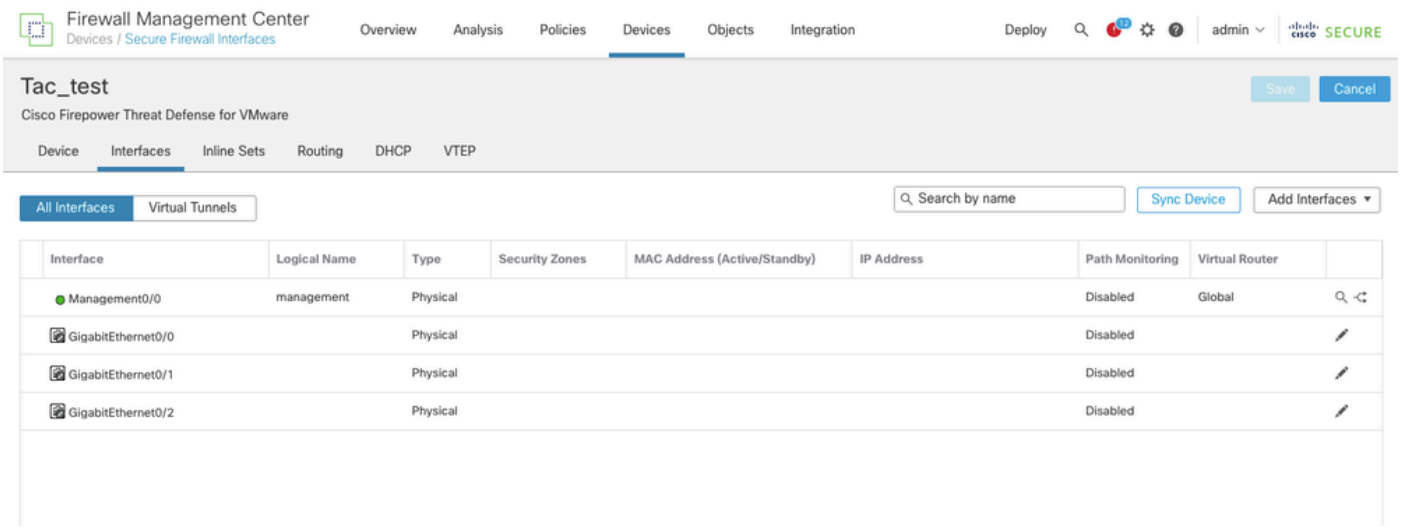
بعد تكوين تقارب

وكما هو موضح في إجراء التقارب، فمن أجل إجراء الدمج، يجب إزالة جميع التكوينات الموجودة على واجهة التشخيص.

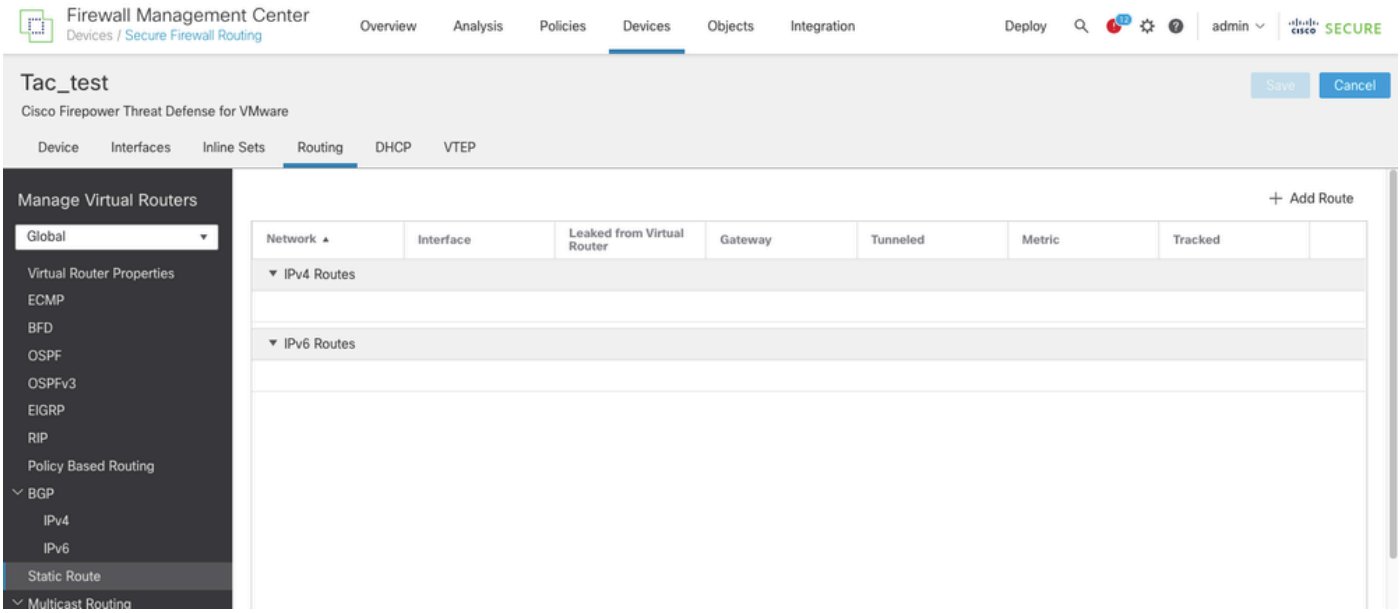
هذه هي المعلومات الخاصة ب FMC و FTD CLI بمجرد اكتمال الدمج.

تكوين واجهة الإدارة عبر واجهة مستخدم FMC

أجهزة > إدارة الأجهزة، حدد FTD. يتم فتح مباشرة إلى علامة التبويب الواجهات.



واجهة الإدارة بعد الدمج

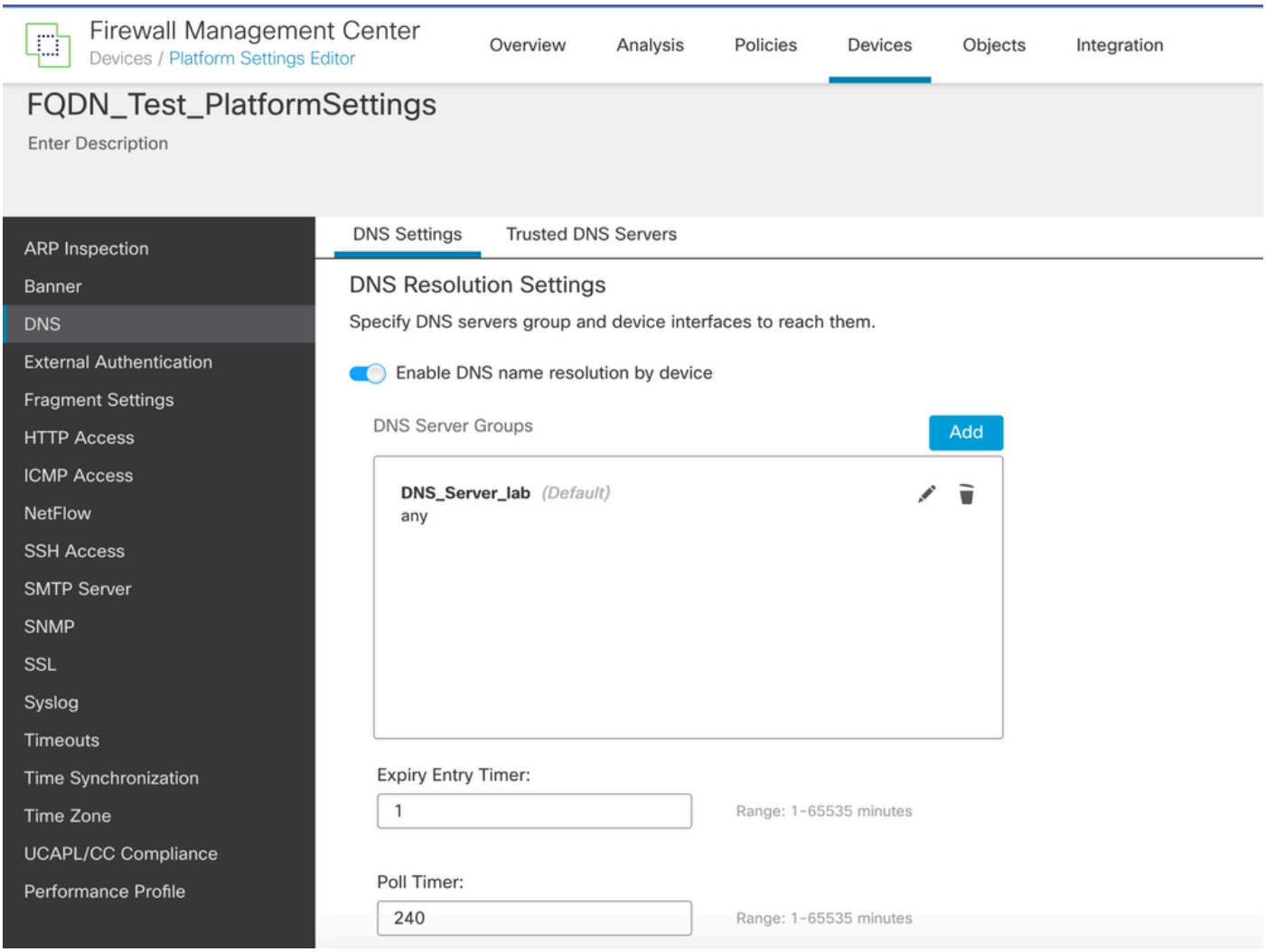


لم تتم إضافة أي مسارات ثابتة إلى خادم DNS

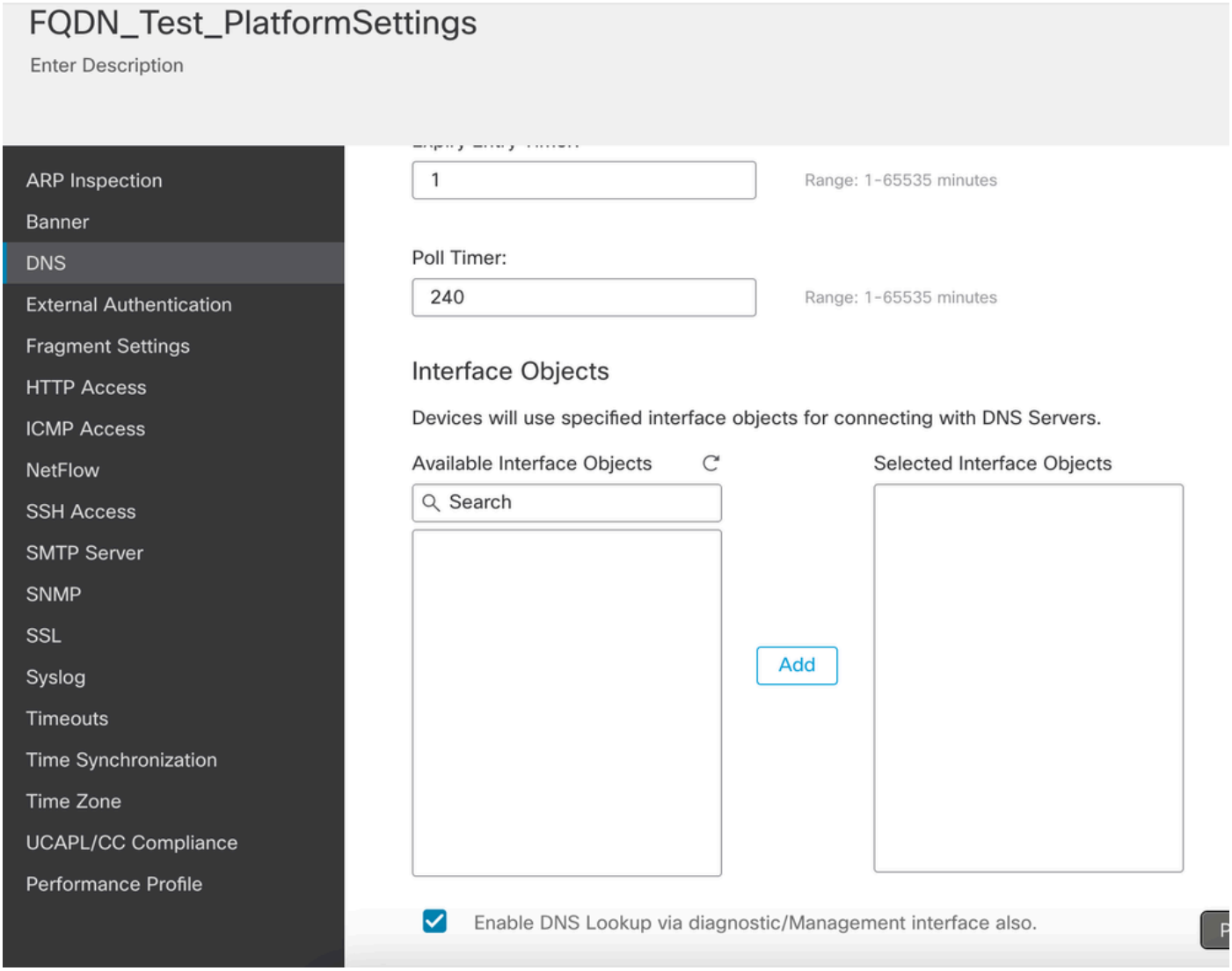
يجب أن يبقى تكوين DNS كما هو على إعدادات النظام الأساسي.

أجهزة > إعدادات النظام الأساسي، حدد السياسة، ثم علامة تبويب DNS.

لمتابعة إرسال بحث DNS إلى واجهة الإدارة دون الحاجة إلى إضافة مسار ثابت، "تمكين بحث DNS عبر واجهة التشخيص/الإدارة أيضا." يجب أن يبقى محددا.



تكوين DNS على إعدادات النظام الأساسي



كما يجب أن يظل خيار تمكين بحث DNS عبر واجهة التشخيص/الإدارة هو نفسه

التكوين على واجهة سطر الأوامر (CLI) لـ FTD

```
> show interface management
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, DLY 10 usec
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0050.56b3.f75d, MTU 1500
        IP address 203.0.113.130, subnet mask 255.255.255.248

> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  administratively down up
GigabitEthernet0/1         unassigned      YES unset  administratively down up
GigabitEthernet0/2         unassigned      YES unset  administratively down up
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Control0/1        unassigned      YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  down                  up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           169.254.1.1     YES unset  up                    up
Internal-Data0/2           unassigned      YES unset  up                    up
Management0/0              203.0.113.130   YES unset  up                    up
```

```
ftd01# sh route management-only


Routing Table: mgmt-only
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set
```

تكوين DNS على CLI لـ FTD على جانب LINA

```
ftd01# sh run dns
dns domain-lookup management
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 management
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
```

التقط على وضع خبير Linux، لتأكيد التدفق الصحيح لحركة مرور بحث DNS على واجهة الإدارة.

```
root@ftd01:/home/admin# tcpdump -i br1 port 53
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:20:33.623146 IP ftd01.60310 > 10.10.10.10.domain: 61954+ A? cisco.com. (27)
20:20:33.623533 IP ftd01.33417 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)
20:20:48.660172 IP ftd01.60310 > 10.10.10.10.domain: 41252+ A? cisco.com. (27)
20:20:52.638426 IP ftd01.39304 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)
20:21:09.669133 IP ftd01.47150 > umbrella.domain: 39343+ AAAA? ftd01. (23)
20:21:09.669305 IP ftd01.50173 > umbrella.domain: 57694+ AAAA? ftd01. (23)
20:21:11.659352 IP ftd01.48092 > umbrella.domain: 46478+ PTR? opendns.in-addr.arpa. (45)
20:21:14.673992 IP ftd01.58547 > umbrella.domain: 57694+ AAAA? ftd01. (23)
20:21:18.673371 IP ftd01.47607 > umbrella.domain: 39343+ AAAA? ftd01. (23)
20:21:18.695507 IP ftd01.60310 > 10.10.10.10.domain: 29973+ A? cisco.com. (27)
```

مع هذا الدليل، يمكن التأكد من أن بحث DNS يستمر في العمل حتى إذا لم تتم إضافة مسار ثابت على واجهة الإدارة عبر Linux.

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).