Configuración de la combinación de la interfaz de administración y diagnóstico en FMC

Contenido

Introducción

Este documento describe los pasos para configurar la fusión de las interfaces de administración y diagnóstico, función agregada en la versión FTD 7.4.0.

Prerequisites

Cisco le recomendó que tuviera conocimientos sobre los siguientes temas:

- Cisco Secure Firewall Threat Defence (FTD)
- Cisco Secure Firewall Manager Center (FMC)

Antecedentes

En la versión 7.3 y anteriores, la interfaz de administración física se comparte entre la interfaz lógica de diagnóstico (Lina) y la interfaz lógica de administración (Linux).

En la versión 7.4 y posteriores, la interfaz de diagnóstico se fusiona con la de gestión para simplificar la experiencia del usuario.
En el caso de dispositivos nuevos que utilicen la versión 7.4 y posteriores, no puede utilizar la interfaz de diagnóstico heredada. Sólo está disponible la interfaz de administración fusionada.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

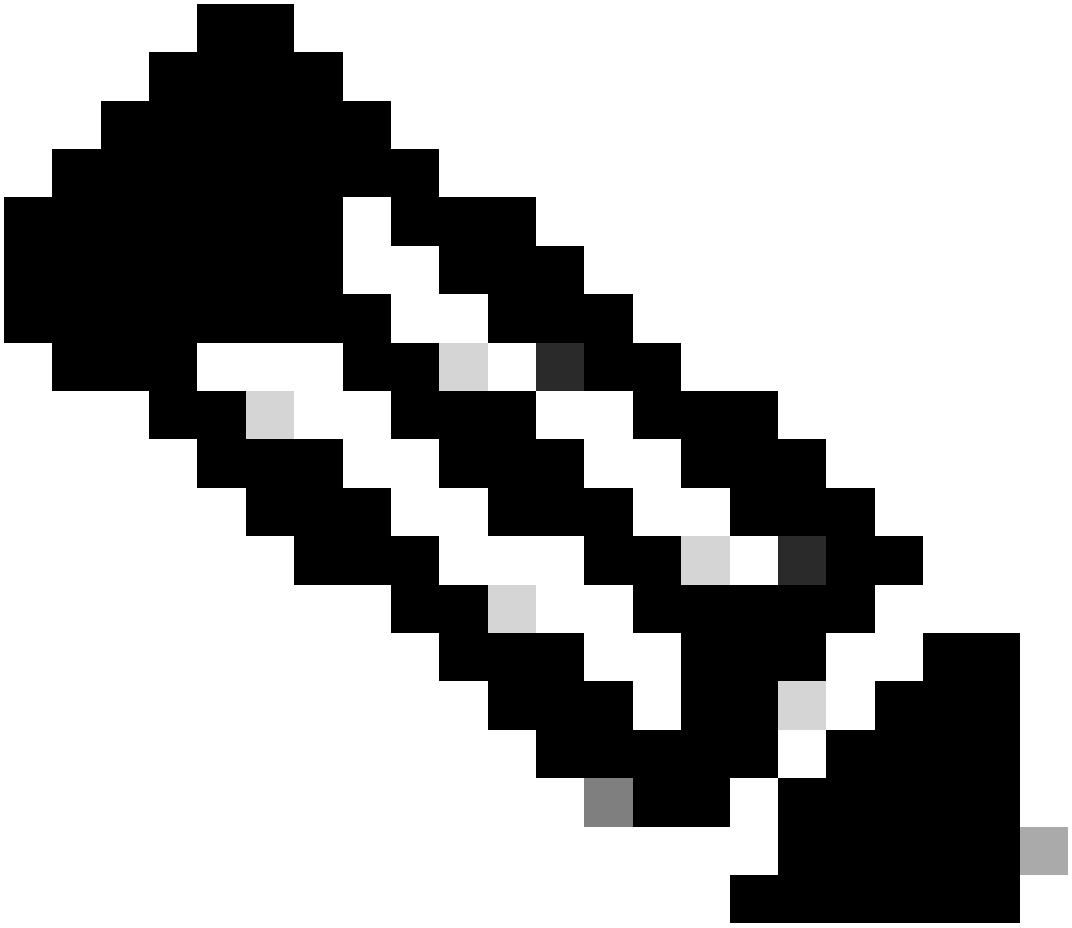
- Virtual Cisco Secure Firewall Threat Defence (FTD), versión 7.4.2
- Virtual Cisco Secure Firewall Manager Center (FMC), versión 7.4.2

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

Configurar

Si ha actualizado a la versión 7.4 o posterior y dispone de configuración para la interfaz de diagnóstico, tiene la opción de fusionar las interfaces manualmente o puede seguir utilizando la interfaz de diagnóstico independiente.

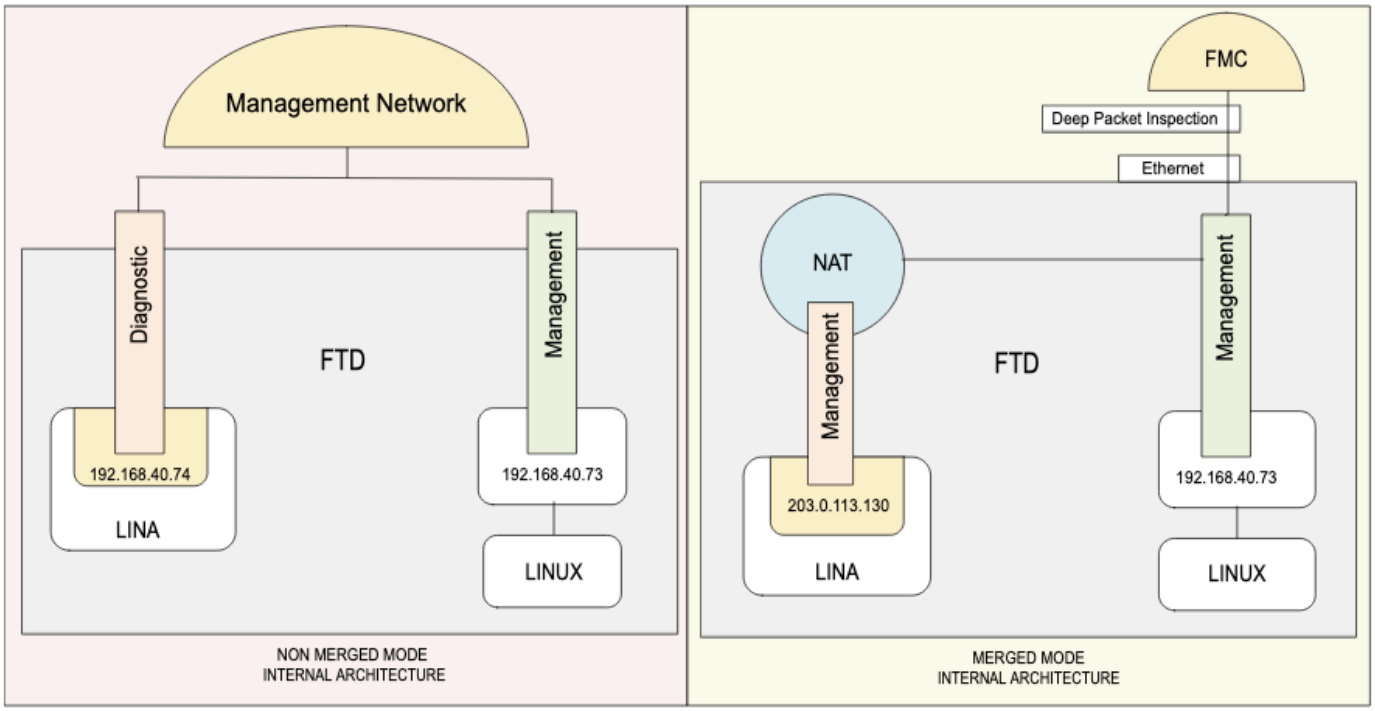
En caso de que no tuviera ninguna configuración para la interfaz de diagnóstico, la combinación de interfaces se realiza automáticamente.



Nota: El soporte para la interfaz de diagnóstico se eliminará en una versión posterior, por lo tanto, planifique fusionar las interfaces lo antes posible.

Diagrama de arquitectura interna de FTD

Descripción General de Converged Management Interface



Descripción general de la arquitectura interna antes y después de la interfaz de gestión de convergencia

A la izquierda, la arquitectura interna para la interfaz lógica de diagnóstico (Lina) y la interfaz lógica de gestión (Linux). Versión 7.3 y anteriores.

A la derecha, la arquitectura interna para una única interfaz de gestión. El acceso de línea a la red de administración utiliza el servicio NAT.

Procedimiento de convergencia

En el caso de que exista una configuración en la interfaz de diagnóstico, las interfaces no se fusionan automáticamente después de una actualización y debe realizar el procedimiento de convergencia.

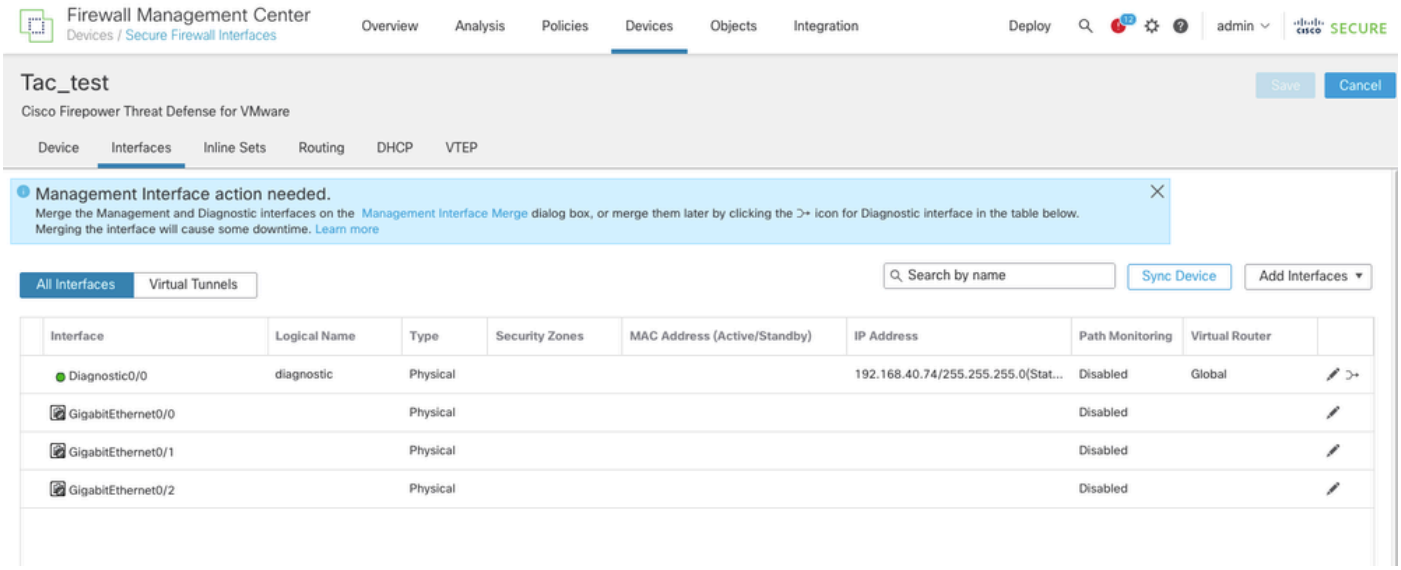
Este procedimiento requiere que acepte los cambios de configuración y, en algunos casos, que corrija manualmente la configuración.

Para ver el modo actual del dispositivo, ingrese el comando show management-interface converge en la CLI de FTD

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

Ese resultado muestra que las interfaces de administración no se fusionan.

Paso 1.
En la interfaz de usuario de FMC, navegue hasta Devices > Device Management, y seleccione el FTD que desea editar. Se abre directamente en la pestaña Interfaces.

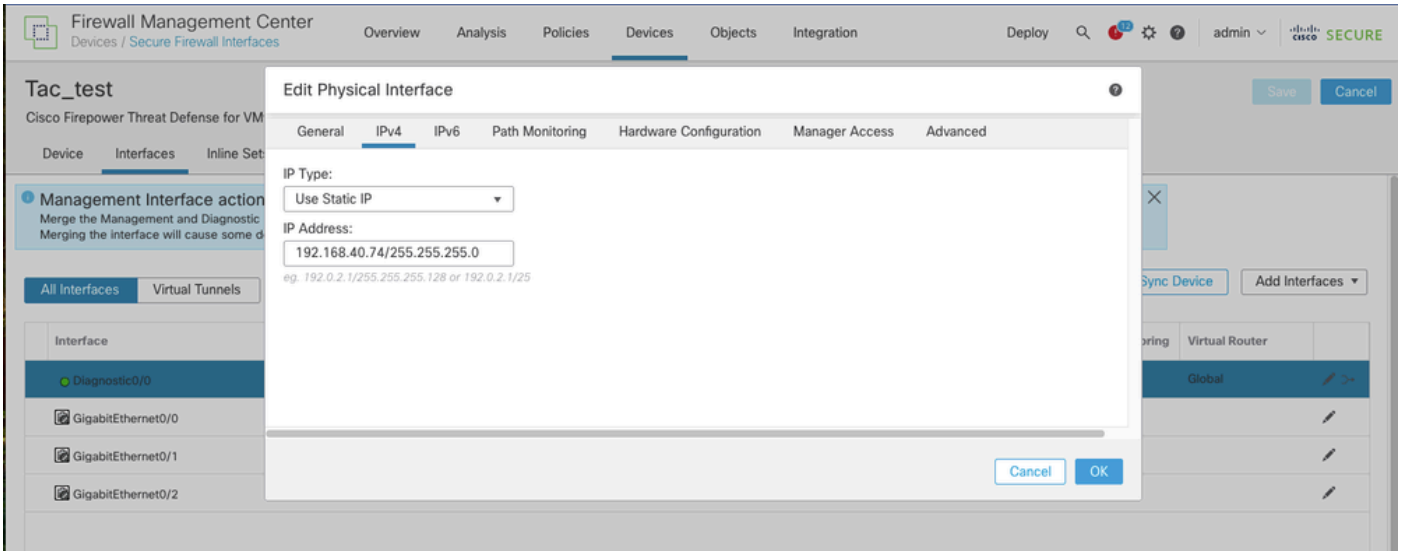


Acción necesaria para fusionar la interfaz de diagnóstico y administración después de actualizar el dispositivo a la versión de software 7.4.2

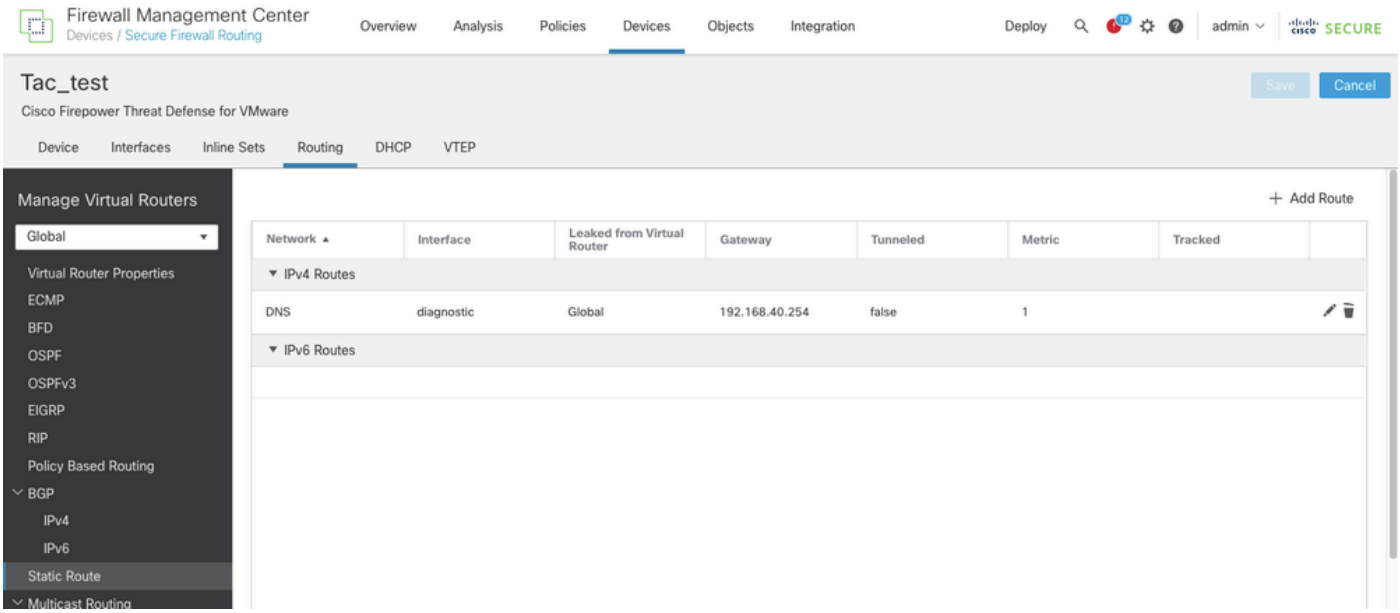
Paso 2.

Elimine toda la configuración de la interfaz de diagnóstico. Es obligatorio que la interfaz de diagnóstico no tenga ninguna configuración para continuar con la combinación.

Por ejemplo, en esta interfaz de diagnóstico, hay: Dirección IP y ruta estática.



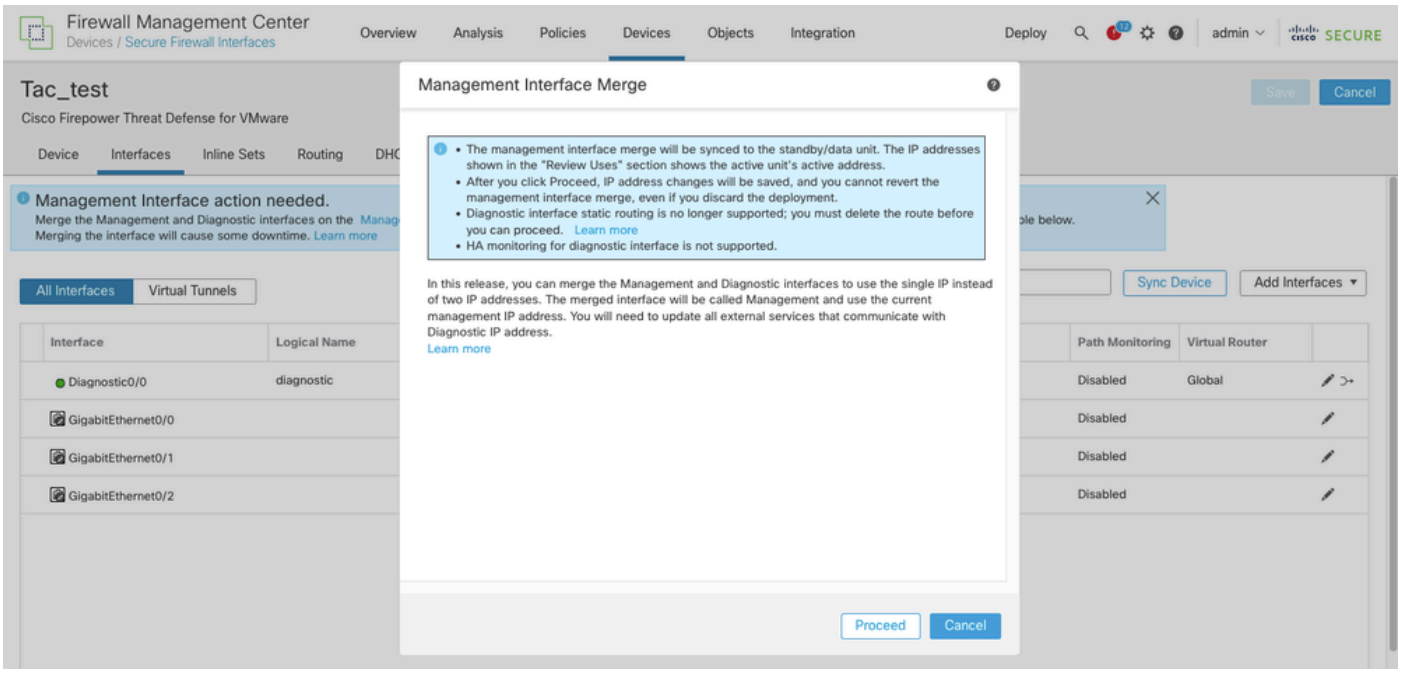
Quitar dirección IP de interfaz de diagnóstico



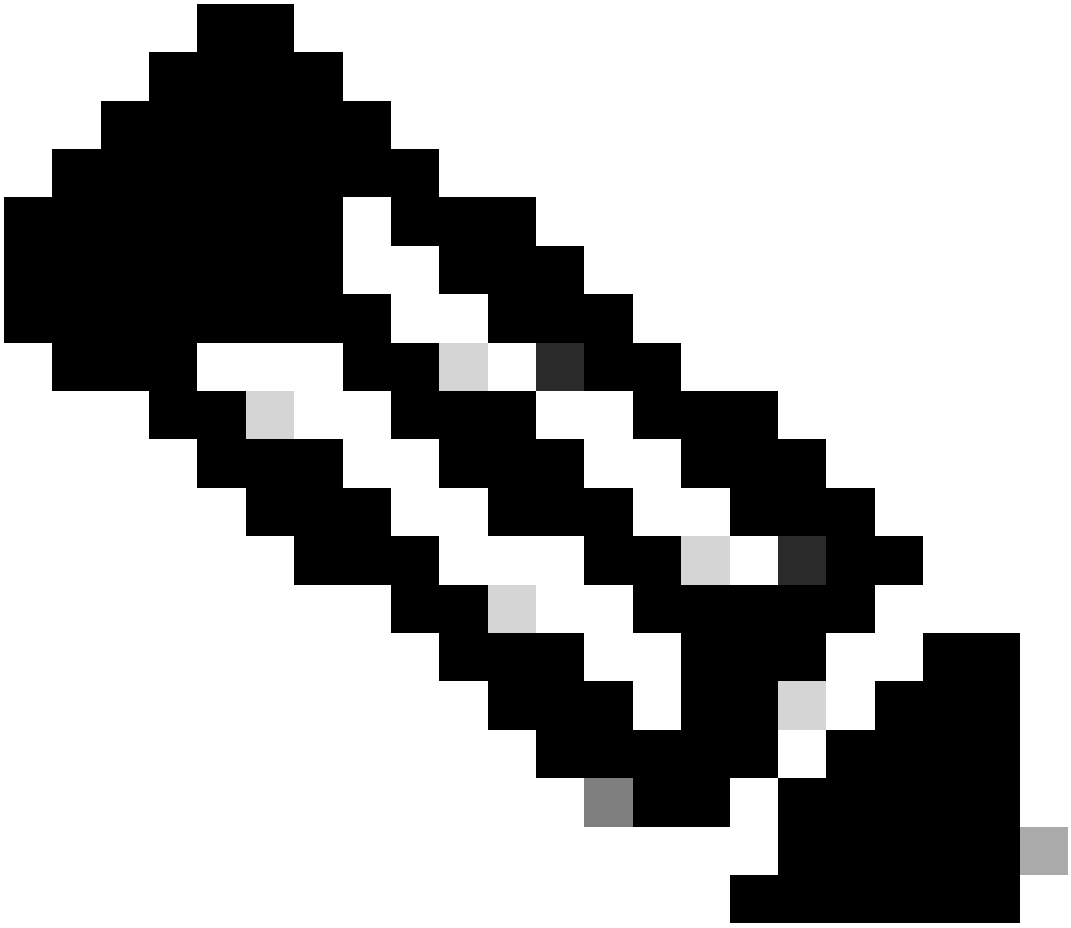
Configuración de la ruta estática en la interfaz de diagnóstico

Paso 3.

Haga clic en el área Management Interface Merge action needed o en el icono Merge situado junto al icono Edit (lápiz) en la interfaz de diagnóstico.

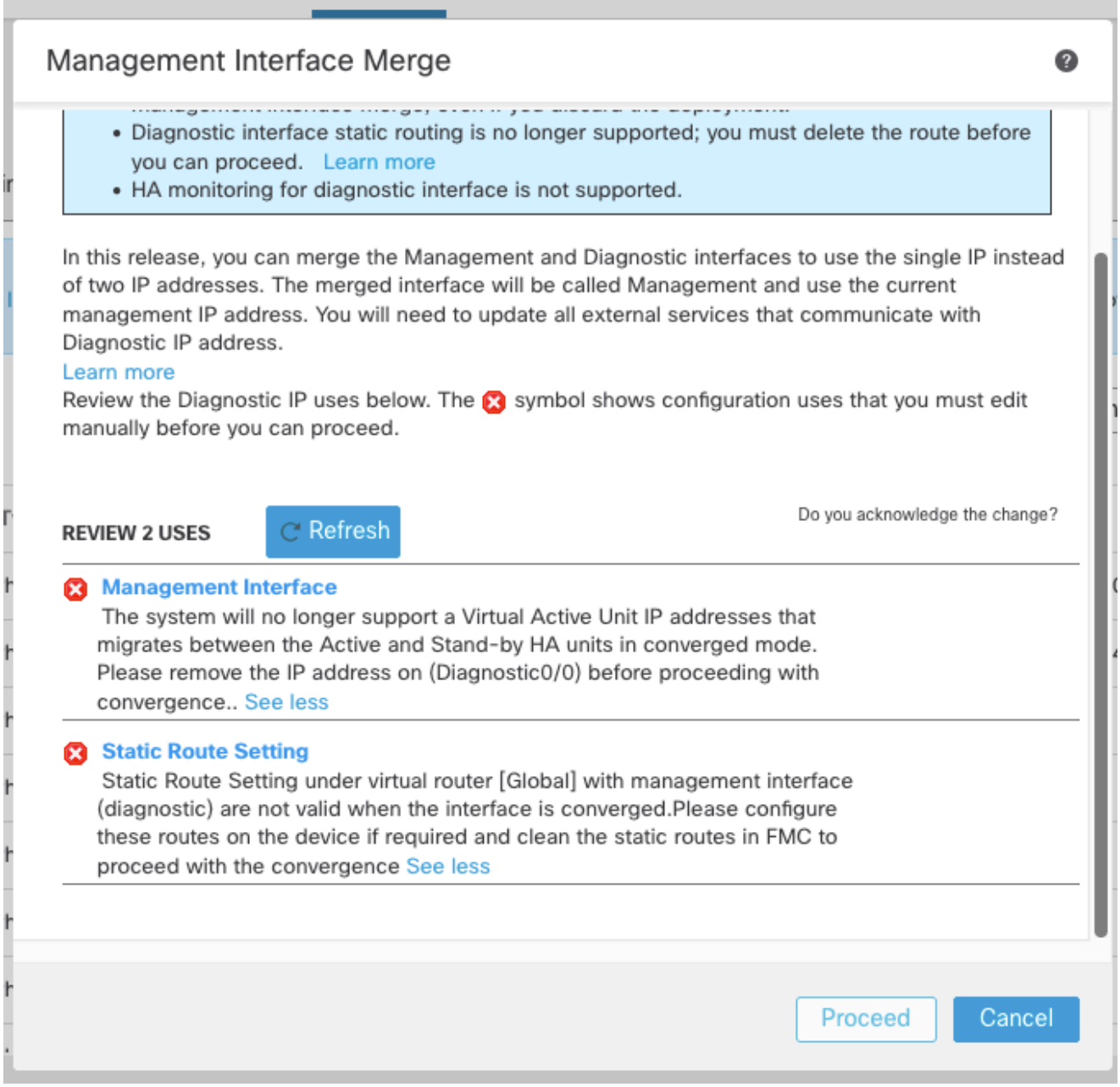


Información de Management Interface Merge antes de continuar



Nota: Para pares y clústeres de alta disponibilidad, realice esta tarea en la unidad de control/activa. La configuración fusionada se replica automáticamente en las unidades de datos/en espera.

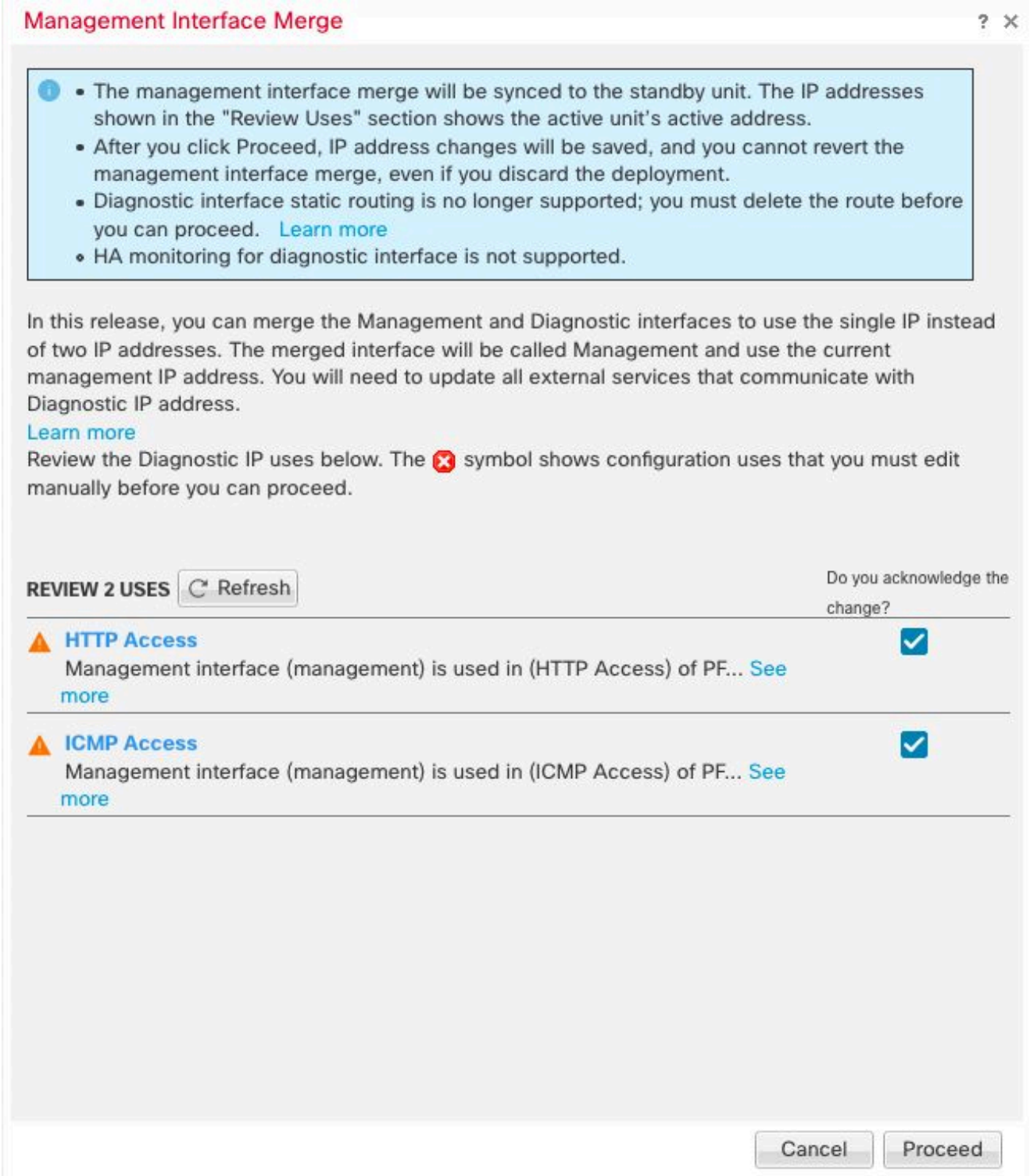
- En el caso de cualquier incidencia que deba cambiarse o eliminarse manualmente, puede aparecer un icono de advertencia.



Ejemplo de advertencia sobre las configuraciones que se deben quitar antes de la combinación

En tal caso: cancele el cuadro de diálogo, continúe con la eliminación de la configuración o la reconfiguración y, a continuación, vuelva a abrir el cuadro de diálogo Combinación de interfaz de administración.

- La configuración de la plataforma que va a funcionar en el dispositivo se marca con un icono de precaución y requiere confirmación.



Ejemplo de advertencia de las configuraciones de configuración de la plataforma que se deben editar

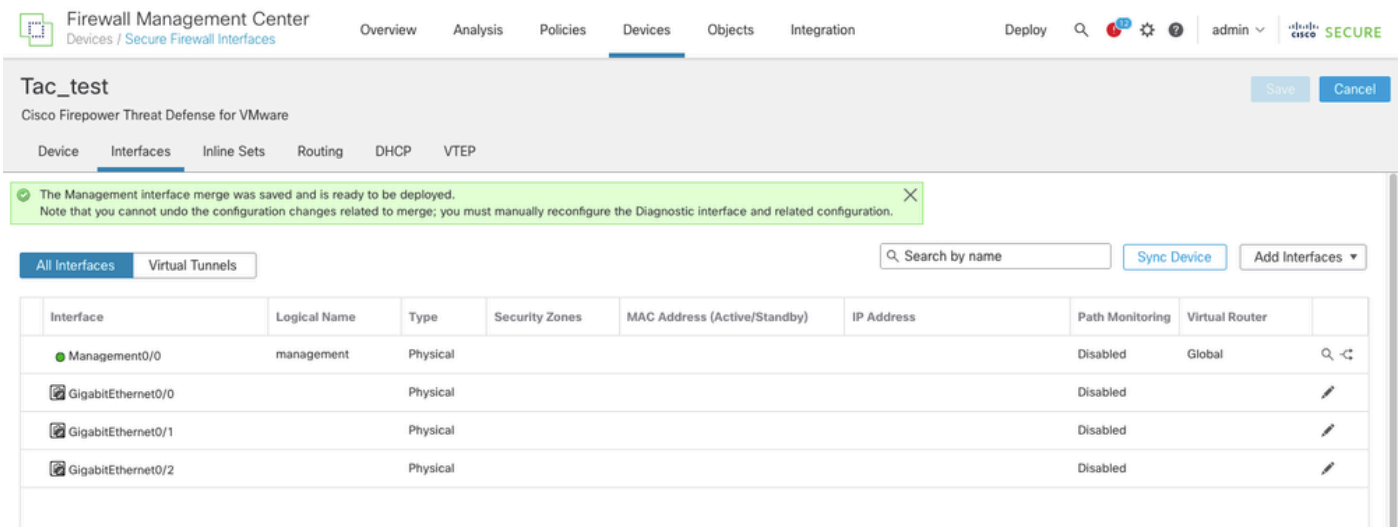
- Haga clic en el cuadro de ¿Reconoce el cambio? y, a continuación, haga clic en Continuar.

Paso 4.

Después de fusionar la configuración, se muestra un anuncio de éxito:
"La combinación de interfaz de administración se guardó y está lista para implementarse.
Tenga en cuenta que no puede deshacer los cambios de configuración relacionados con la

combinación; debe volver a configurar manualmente la interfaz de diagnóstico y la configuración relacionada."

Implemente la nueva configuración combinada.



La combinación de interfaz de administración se guarda y está lista para implementarse

La interfaz de administración se muestra en la página Interfaces, aunque es de sólo lectura.

Después del despliegue, el procedimiento de convergencia en la interfaz de gestión ha finalizado.

Paso 5. Opcional

Si tenía algún servicio externo que se comunicara con la interfaz de diagnóstico, debe cambiar su configuración para utilizar la dirección IP de la interfaz de administración, ya que el repliegue de la ruta de administración se ha eliminado en el modo convergente.

Por ejemplo:

- cliente SNMP
- servidor RADIUS
- Para que el servidor DNS sea accesible a través de la red de administración, el usuario debe seleccionar explícitamente "Habilitar búsqueda de DNS también a través de la interfaz de diagnóstico/administración". en Platform Settings > DNS configuration as an exception is set for DNS lookup and ICMP (ping and traceroute): en estos casos, threat defense utiliza los datos y, a continuación, recurre a la gestión automáticamente si no se encuentra una ruta.

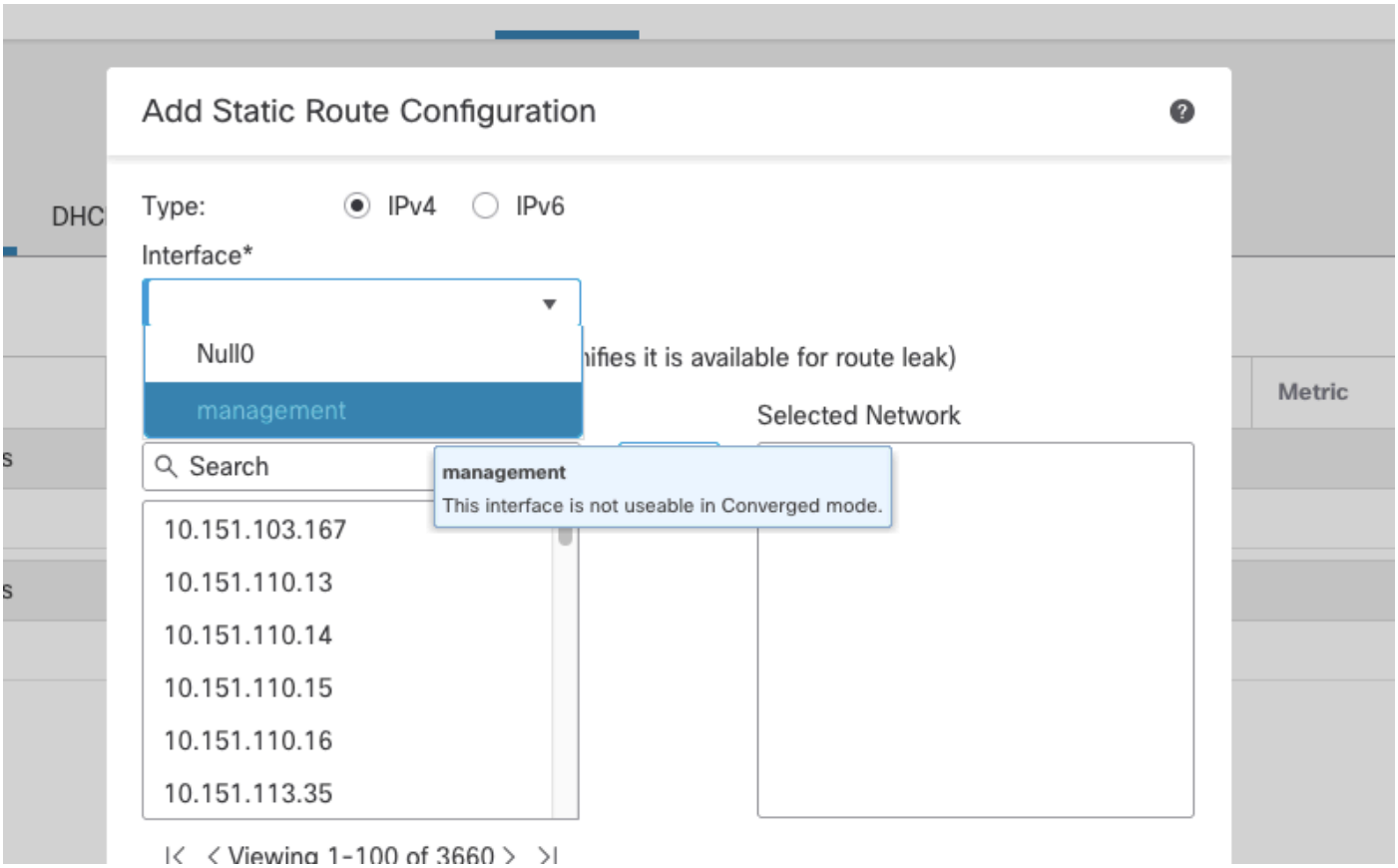
El uso de rutas estáticas para la interfaz de administración solo se puede configurar a través de la CLI de FTD en la nube (Linux)

La ruta predeterminada del puerto de administración de línea envía todas las tramas al módulo 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
```

En la interfaz de usuario de FMC, la interfaz de administración aparece atenuada para la selección.



La interfaz de administración no está disponible para la selección en rutas estáticas después de completar la combinación.

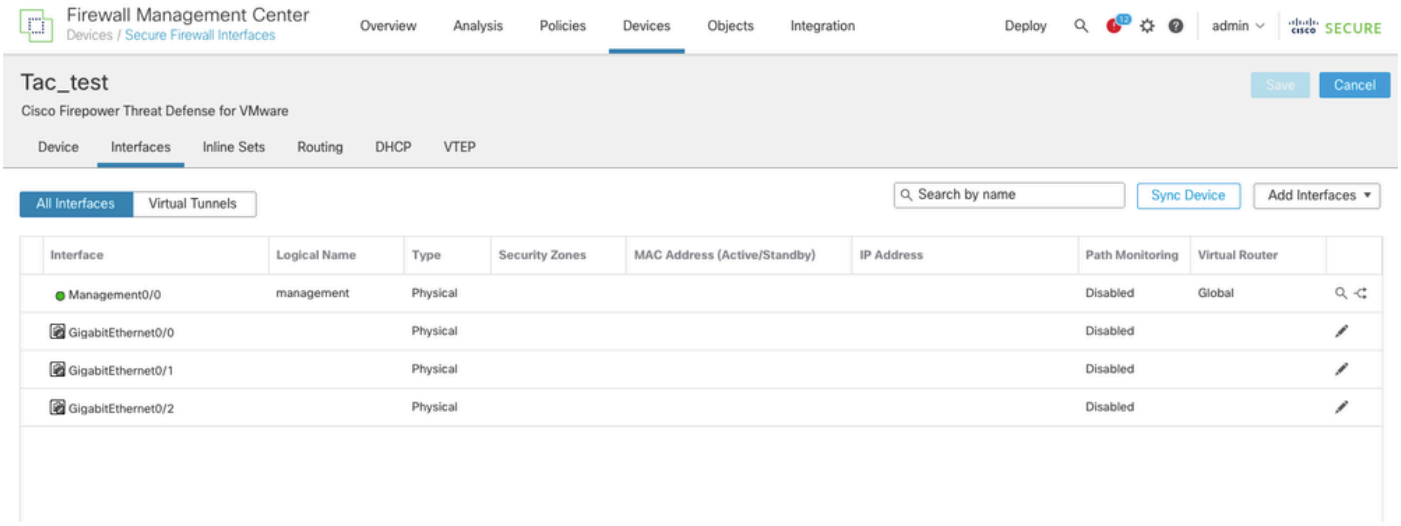
Verificación

Cambios esperados después de la fusión en la interfaz de administración

- Verifique el modo de convergencia en FTD CLI Clish mediante la ejecución del comando

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

- En la interfaz de usuario de FMC, el nombre de la interfaz se cambia a Management0/0 , el nombre lógico a management.



Combinar confirmación en el nombre de la interfaz de gestión y el nombre lógico

- En FTD CLI Clish, las nuevas direcciones IP se configuran automáticamente en la interfaz Line for Management.
  NAT se utiliza como implementación interna: Las direcciones IPv4 privadas internas 203.0.113.130 e IPv6 fd00:0:1:1::2 son las asignadas (ambas sujetas a cambios).
  Esas IPs están NATed a las direcciones IPv4 e IPv6 del FTD del núcleo Linux público, por lo tanto ya no hay necesidad de IPs públicas en Lina.

  En el modo experto, "ifconfig" muestra la dirección IPv4 (203.0.113.129) e IPv6 (fd00:0:1:1::1) interna para 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
```

Solución de problemas: caso práctico

En este caso práctico, la interfaz de diagnóstico en un FTD virtual ha configurado direcciones IP independientes para la conectividad con servicios externos de búsqueda de DNS, antes de actualizar a 7.4.2.

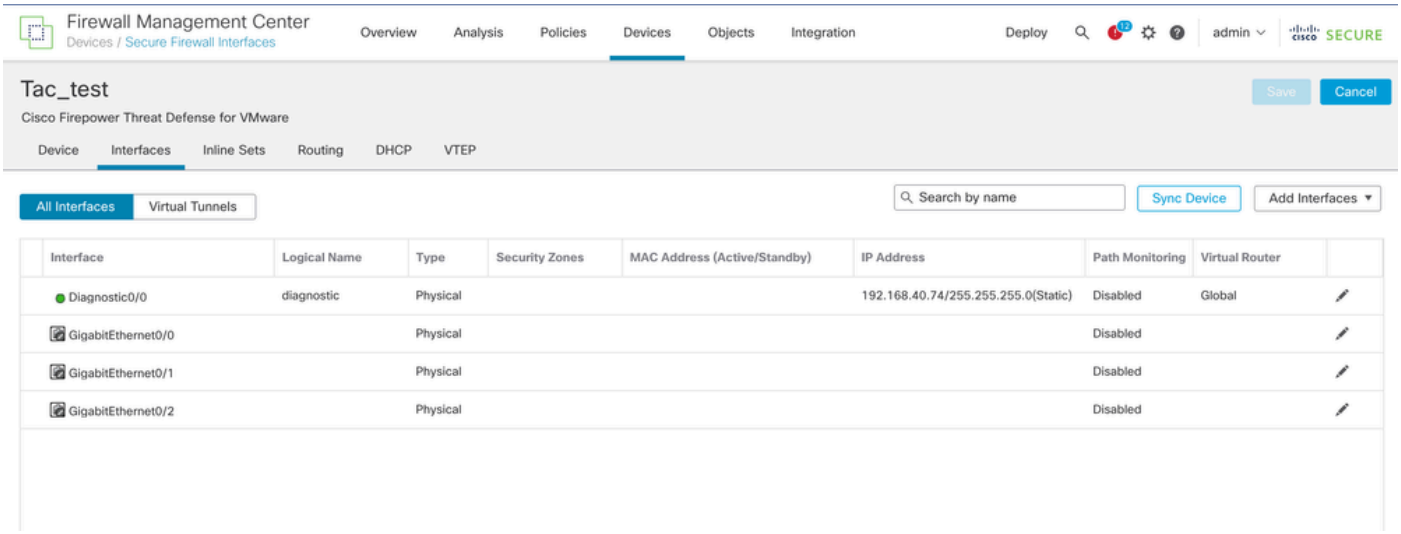
Después de la actualización a 7.4.2, la convergencia es necesaria, así es como es la configuración en la interfaz de usuario de FMC, la línea CLI de FTD y Linux, antes y después de la fusión.

También hay capturas de tráfico en la línea CLI de FTD y Linux para mostrar el tráfico mediante el traslado de la interfaz de diagnóstico lógica para utilizar la interfaz de administración.

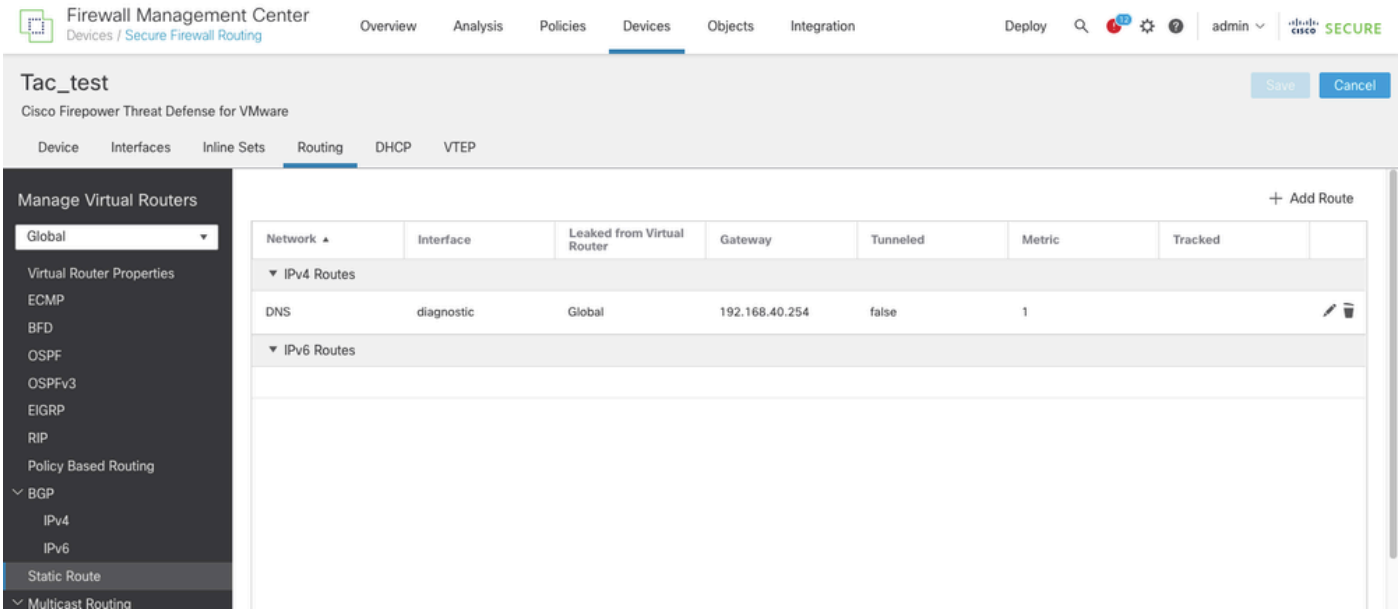
Antes de la configuración de convergencia

La interfaz de diagnóstico tiene una IP independiente y una ruta estática para la búsqueda de DNS, de esta manera funciona utilizando ambas interfaces lógicas de Lina a Linux en el FTD.

Configuración de IU de FMC



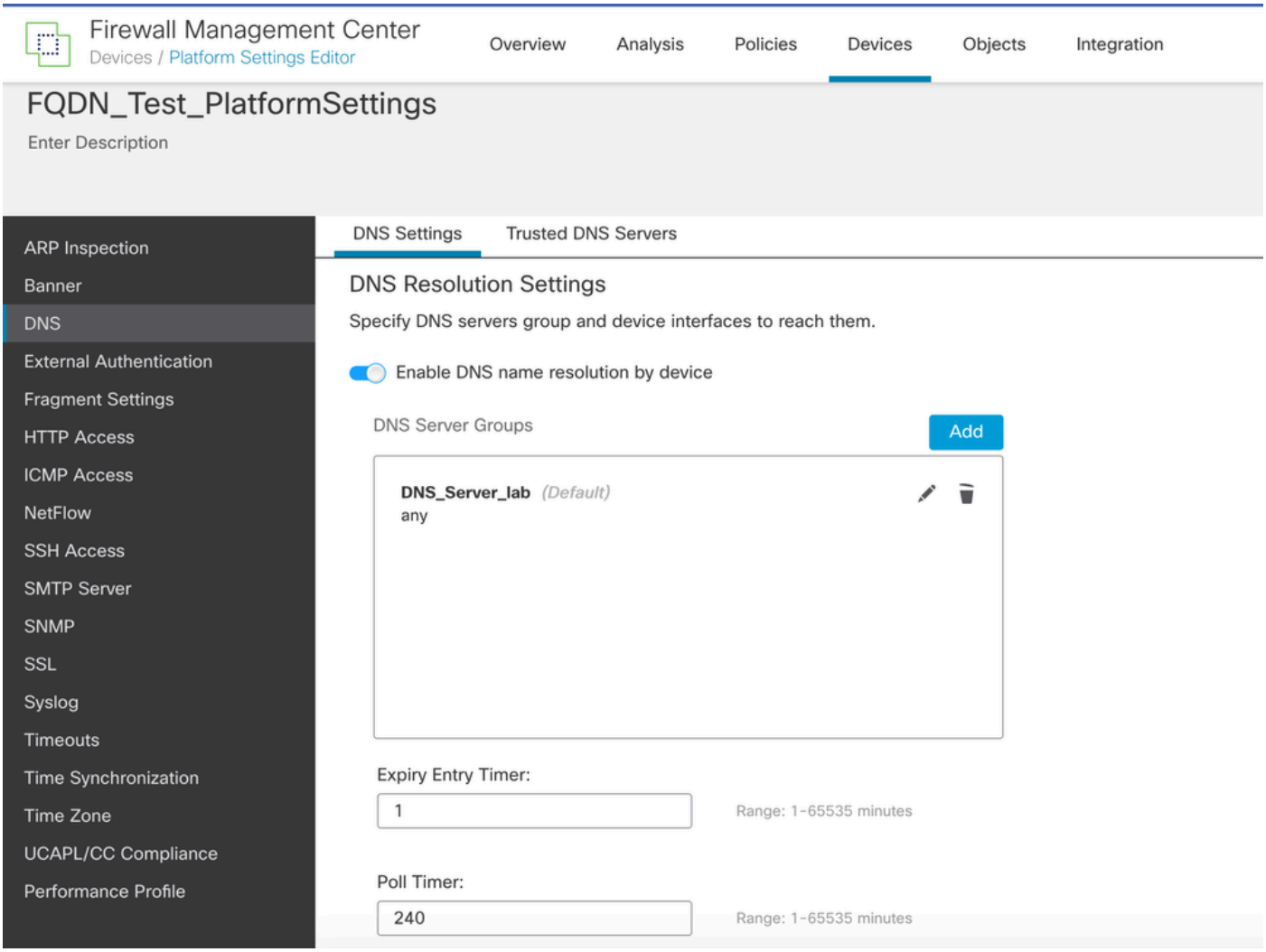
Configuración de interfaz de diagnóstico antes de la fusión



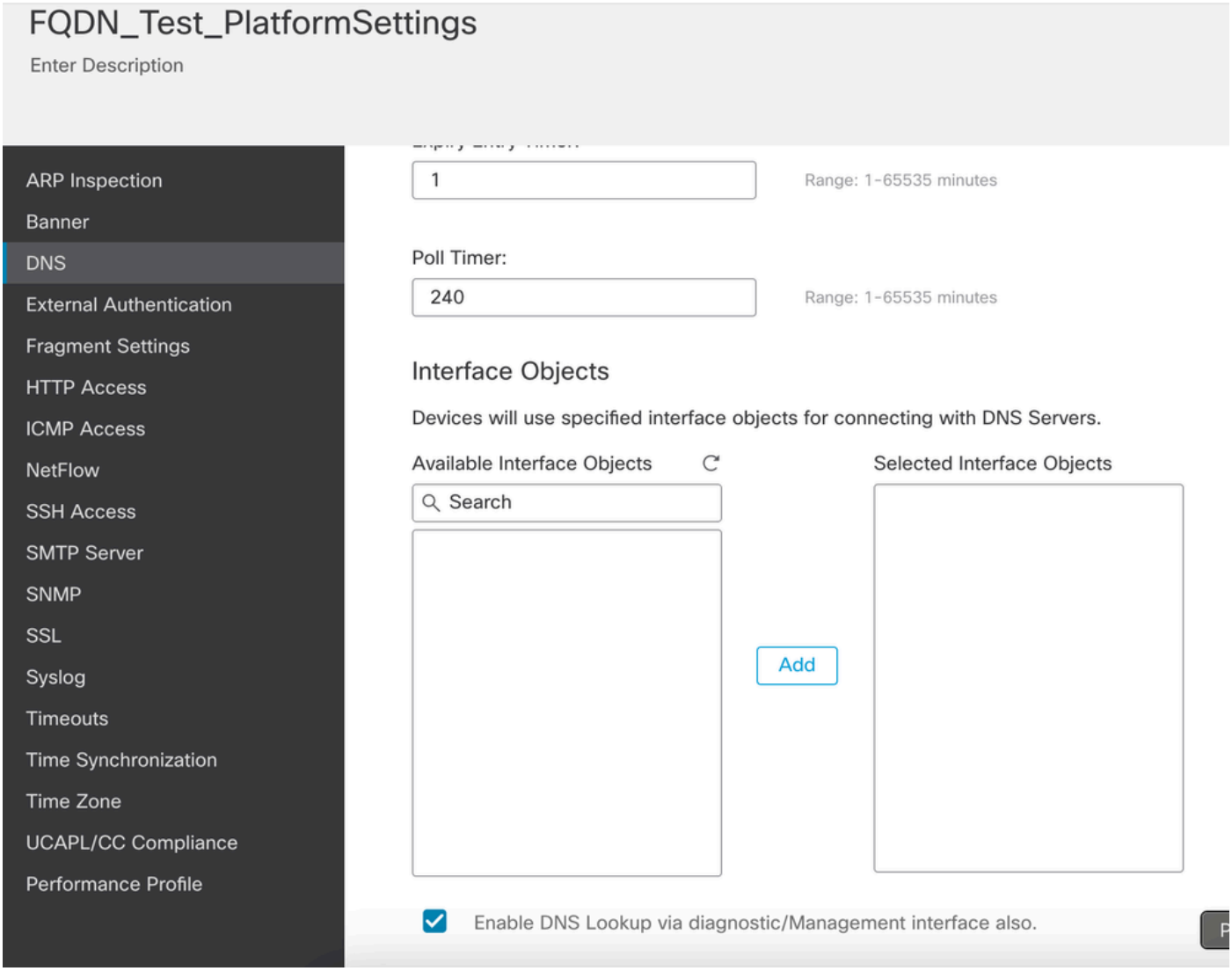
Ruta estática configurada en la interfaz de diagnóstico

Configuración de DNS sobre

Devices > Platform Settings, seleccione la política y, a continuación, la ficha DNS.



Configuración de DNS en Configuración de la plataforma



Casilla de verificación activada para Habilitar búsqueda de DNS también a través de la interfaz de diagnóstico/gestión

Configuración de la interfaz de diagnóstico sobre la línea FTD

```
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
```

Configuración de DNS en la línea CLI de FTD

```
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
```

Captura en la interfaz de diagnóstico para el tráfico DNS que va al servidor 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#
```

Capture en el modo experto de Linux para confirmar el flujo correcto del tráfico de búsqueda de DNS en la interfaz de administración desde la interfaz de diagnóstico

```
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)
```

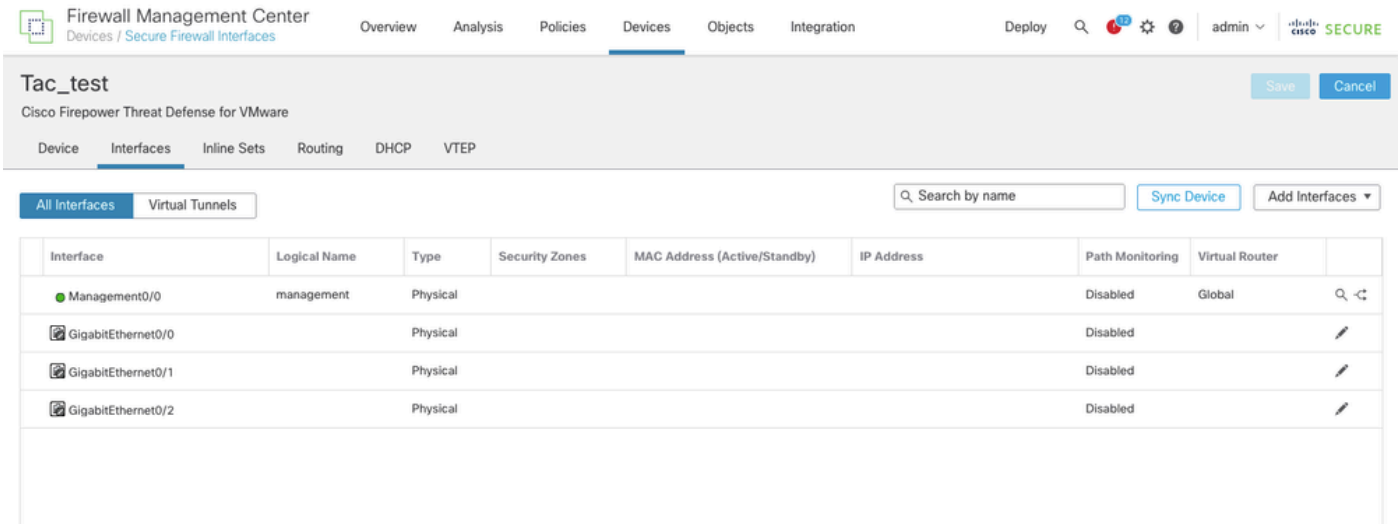
Después de la configuración de convergencia

Como se menciona en el procedimiento de convergencia, para realizar la fusión, se deben eliminar todas las configuraciones de la interfaz de diagnóstico.

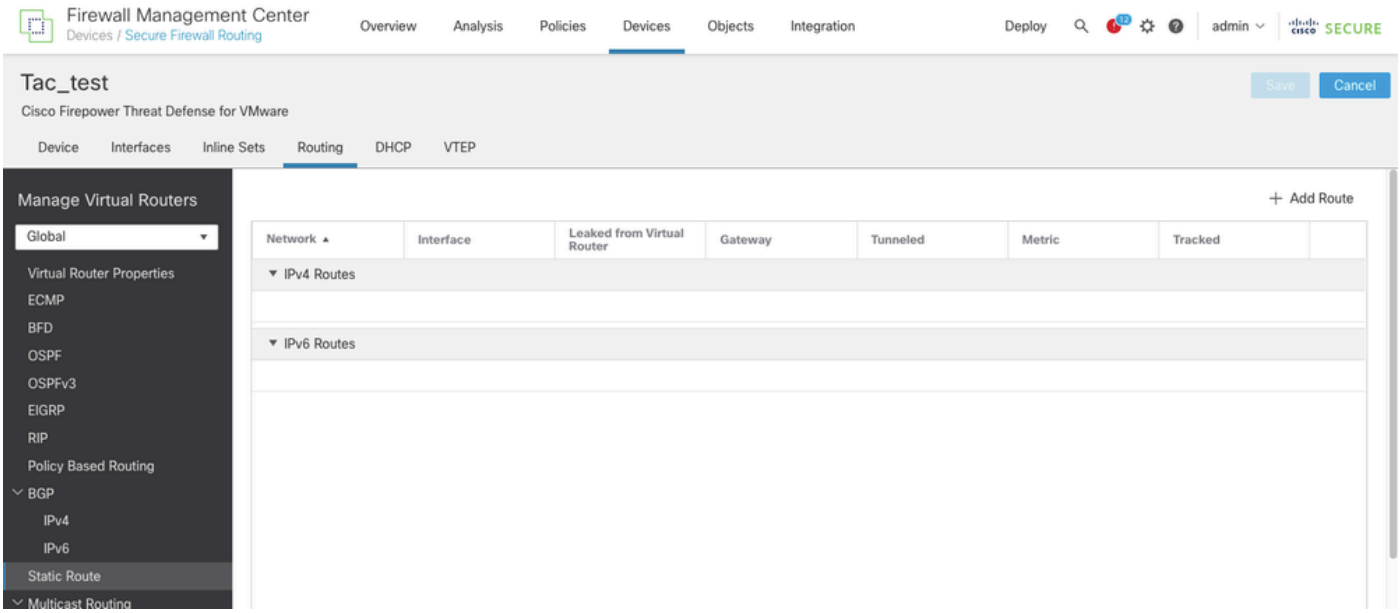
Esta es la información sobre FMC y FTD CLI una vez que se ha completado la combinación.

Configuración de la interfaz de administración sobre FMC UI

Devices > Device Management, seleccione el FTD. Se abre directamente en la pestaña Interfaces.



Interfaz de administración después de la combinación

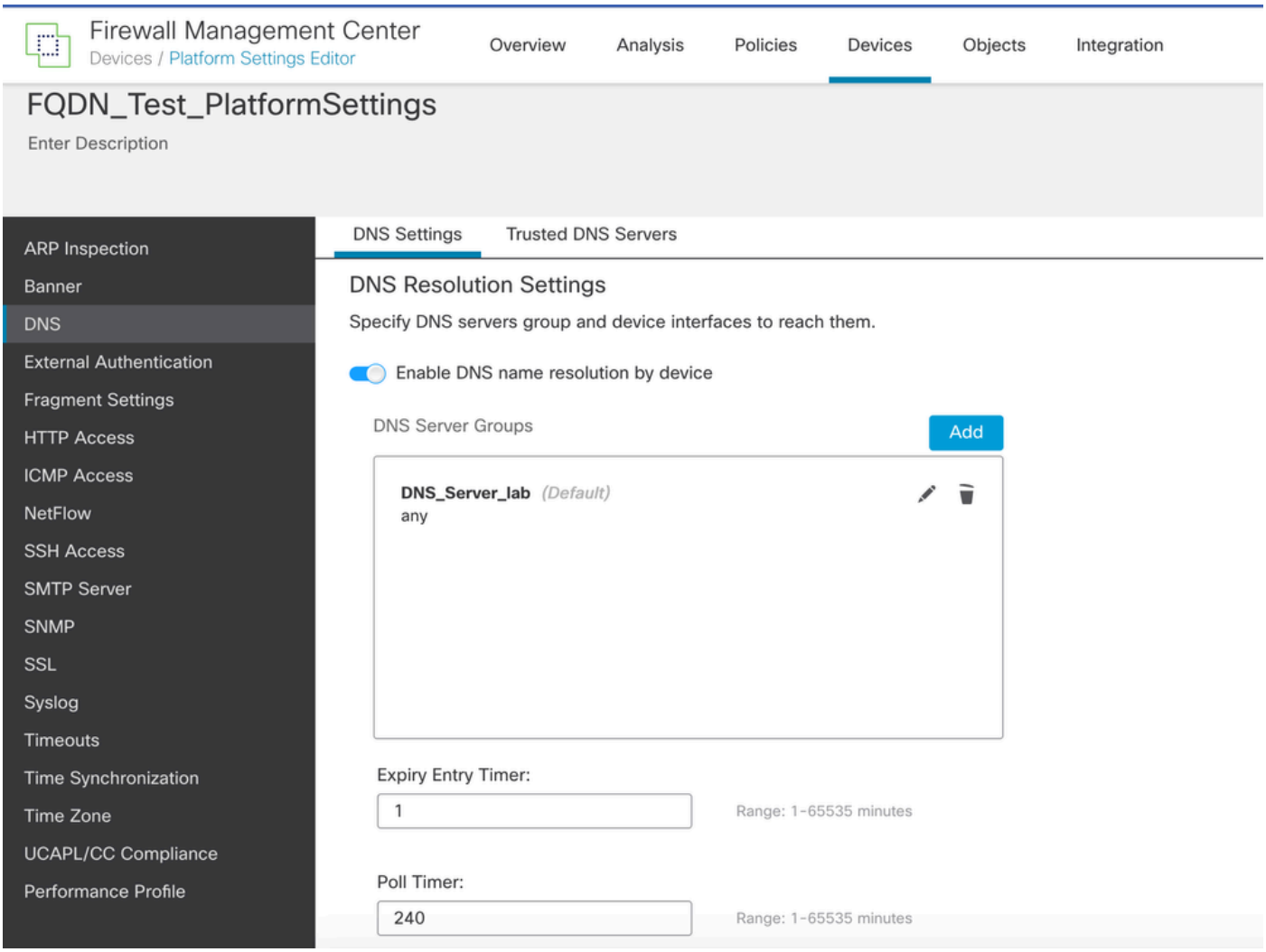


No se agregan rutas estáticas al servidor DNS

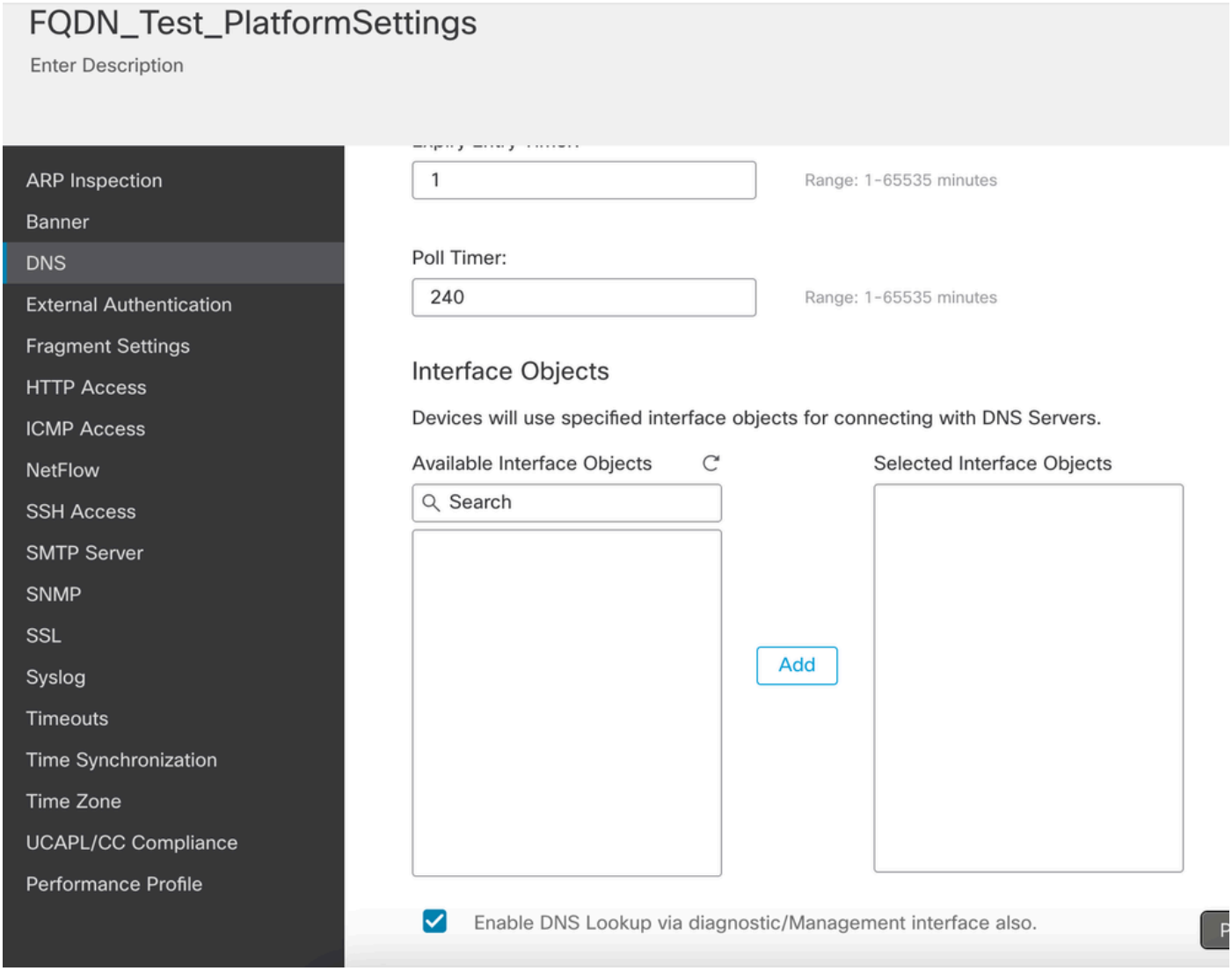
La configuración de DNS debe ser la misma en Configuración de la plataforma.

Devices > Platform Settings, seleccione la política y, a continuación, la ficha DNS.

Para que la búsqueda de DNS se siga enviando a la interfaz de administración sin necesidad de agregar una ruta estática, la opción "Habilitar búsqueda de DNS a través de la interfaz de diagnóstico/administración también". debe permanecer seleccionado.



Configuración de DNS en la configuración de la plataforma



La opción Enable DNS Lookup via diagnostic/Management interface también debe permanecer igual

Configuración en la CLI de 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
```

Configuración de DNS en la CLI de FTD en el lado 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
```

Capture en el modo experto de Linux, para confirmar el flujo correcto del tráfico de búsqueda de DNS en la interfaz de administración.

```
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)
```

Con esta evidencia, se puede confirmar que la búsqueda de DNS continúa funcionando incluso si no se agrega una ruta estática en la interfaz de administración a través de Linux.

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

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

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