Configurare l'unione dell'interfaccia di gestione e diagnostica in FMC

Sommario

Introduzione

In questo documento viene descritto come configurare l'unione delle interfacce di gestione e diagnostica, una funzione aggiunta nella versione FTD 7.4.0.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Premesse

Nella versione 7.3 e precedenti, l'interfaccia di gestione fisica è condivisa tra l'interfaccia logica di diagnostica (Lina) e l'interfaccia logica di gestione (Linux).

Nella versione 7.4 e successive, l'interfaccia di diagnostica viene unita a Management per semplificare l'esperienza utente.
Per i nuovi dispositivi che utilizzano la versione 7.4 e successive, non è possibile utilizzare l'interfaccia di diagnostica precedente. È disponibile solo l'interfaccia di gestione unita.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

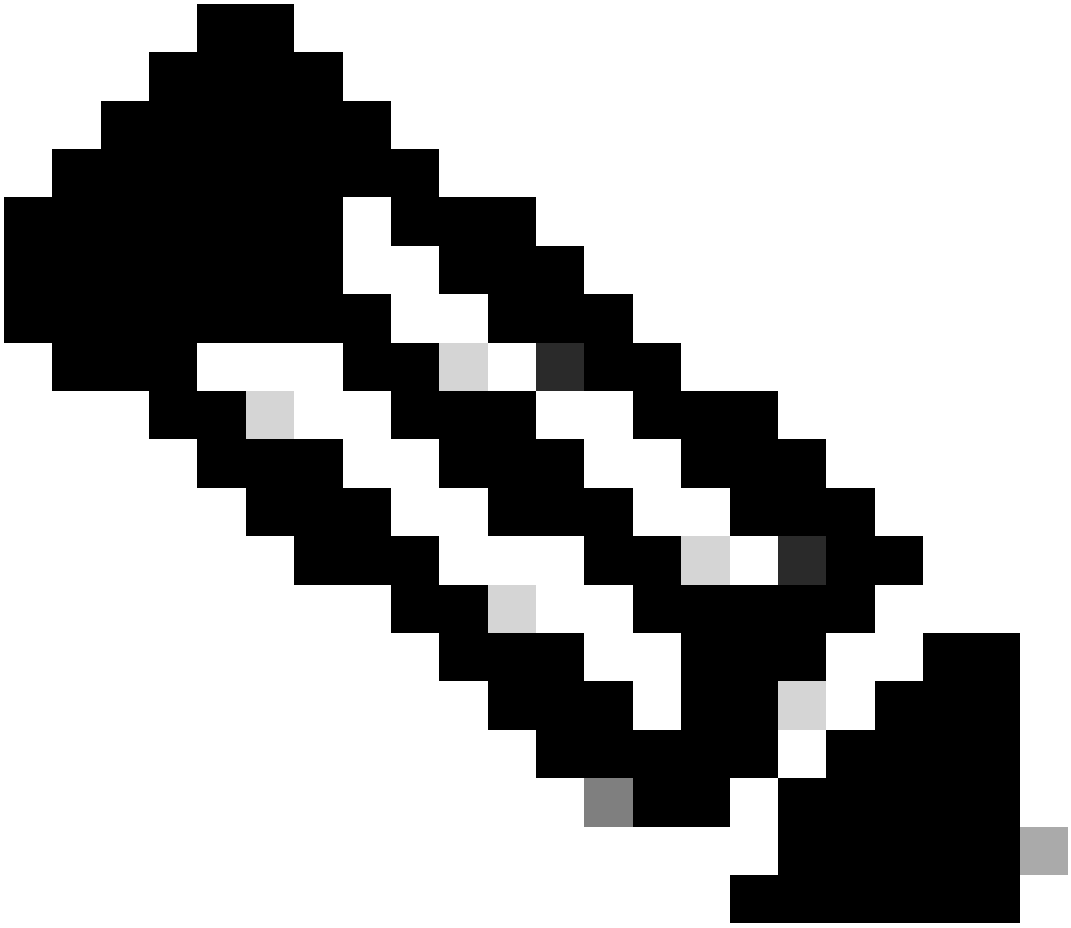
- Virtual Cisco Secure Firewall Threat Defense (FTD), versione 7.4.2
- Virtual Cisco Secure Firewall Manager Center (FMC), versione 7.4.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Se è stato eseguito l'aggiornamento alla versione 7.4 o successive e si dispone della configurazione per l'interfaccia di diagnostica, è possibile scegliere di unire le interfacce manualmente oppure continuare a utilizzare l'interfaccia di diagnostica separata.

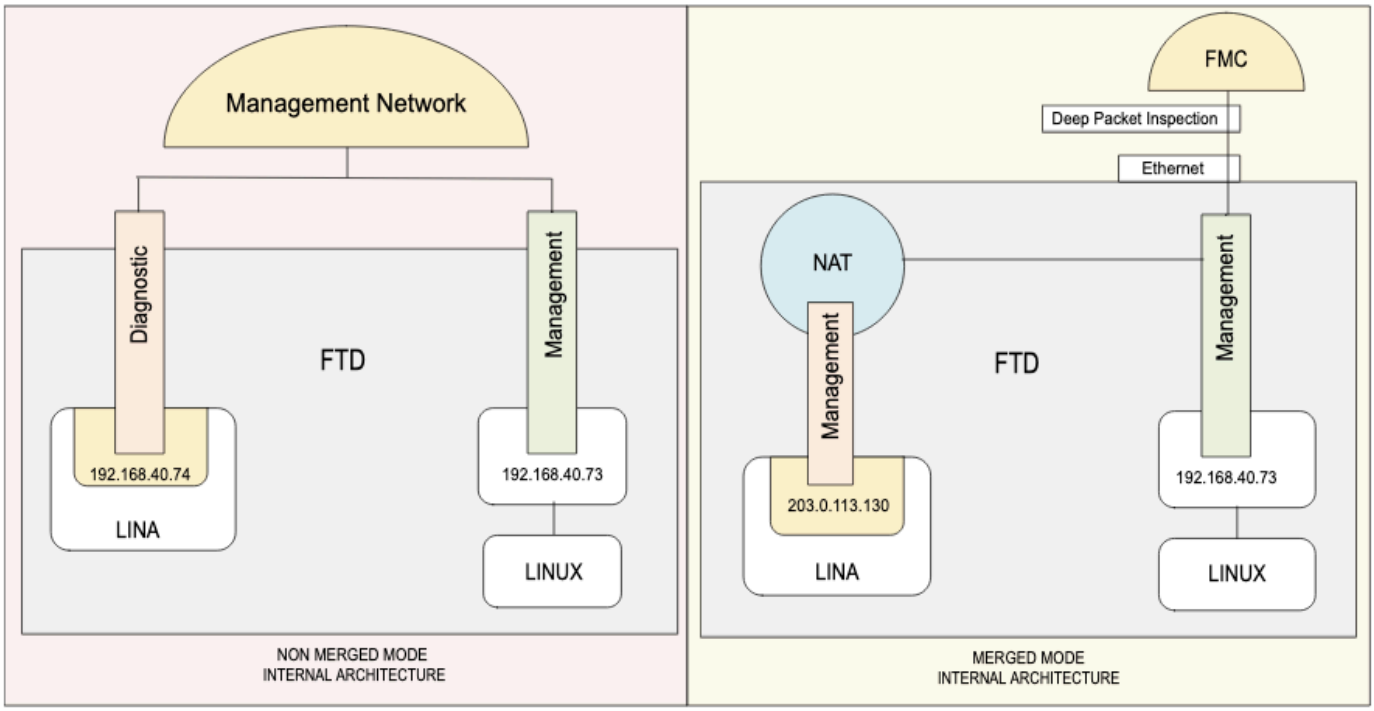
Se non si dispone di alcuna configurazione per l'interfaccia di diagnostica, l'unione delle interfacce viene eseguita automaticamente.



Nota: Il supporto per l'interfaccia diagnostica deve essere rimosso in una versione successiva, quindi si prevede di unire le interfacce il prima possibile.

Diagramma architettura interna FTD

Panoramica dell'interfaccia di gestione convergente



Panoramica dell'architettura interna prima e dopo l'interfaccia di gestione della convergenza

A sinistra, l'architettura interna per l'interfaccia logica di diagnostica (Lina) e l'interfaccia logica di gestione (Linux). Versione 7.3 e precedente.

Sulla destra, l'architettura interna per una singola interfaccia di gestione. L'accesso Lina alla rete di gestione utilizza il servizio NAT.

Procedura di convergenza

Se la configurazione è presente nell'interfaccia di diagnostica, le interfacce non vengono unite automaticamente dopo un aggiornamento ed è necessario eseguire la procedura di convergenza.

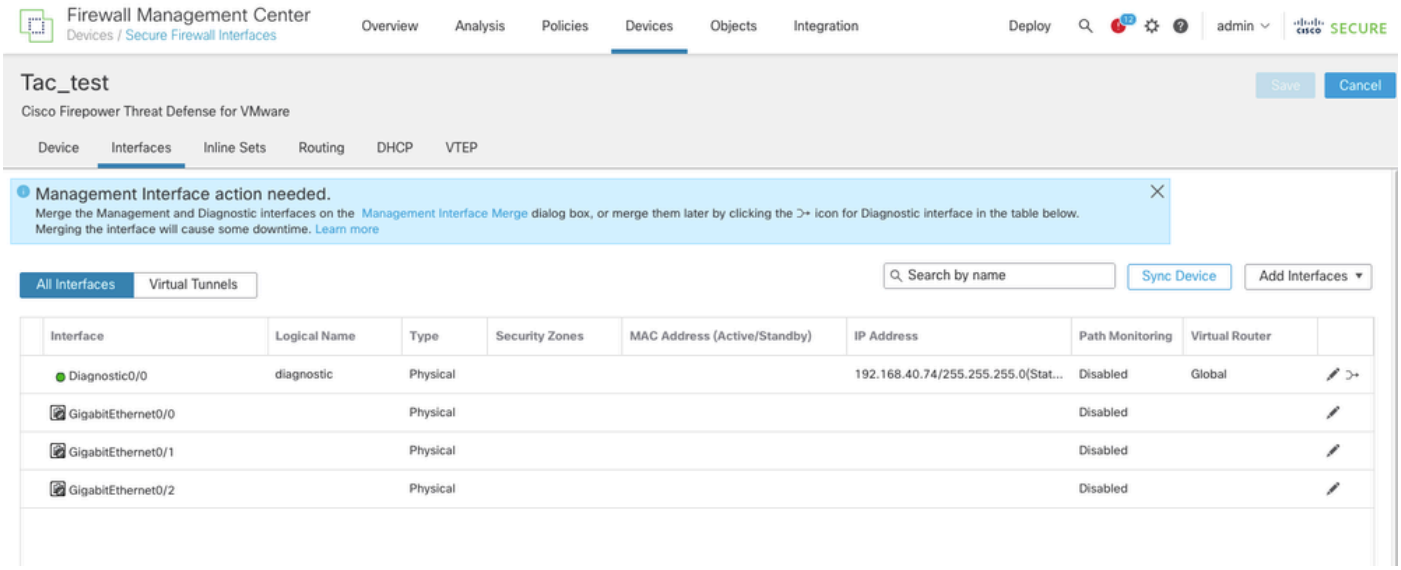
Questa procedura richiede la conferma delle modifiche apportate alla configurazione e, in alcuni casi, la correzione manuale della configurazione.

Per visualizzare la modalità corrente del dispositivo, immettere il comando show management-interface converge nella CLI Client FTD

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

Questo risultato indica che le interfacce di gestione non sono unite.

Passaggio 1.
Nell'interfaccia utente di FMC, selezionare Devices > Device Management, quindi selezionare l'FTD da modificare. Viene visualizzata direttamente la scheda Interfacce.

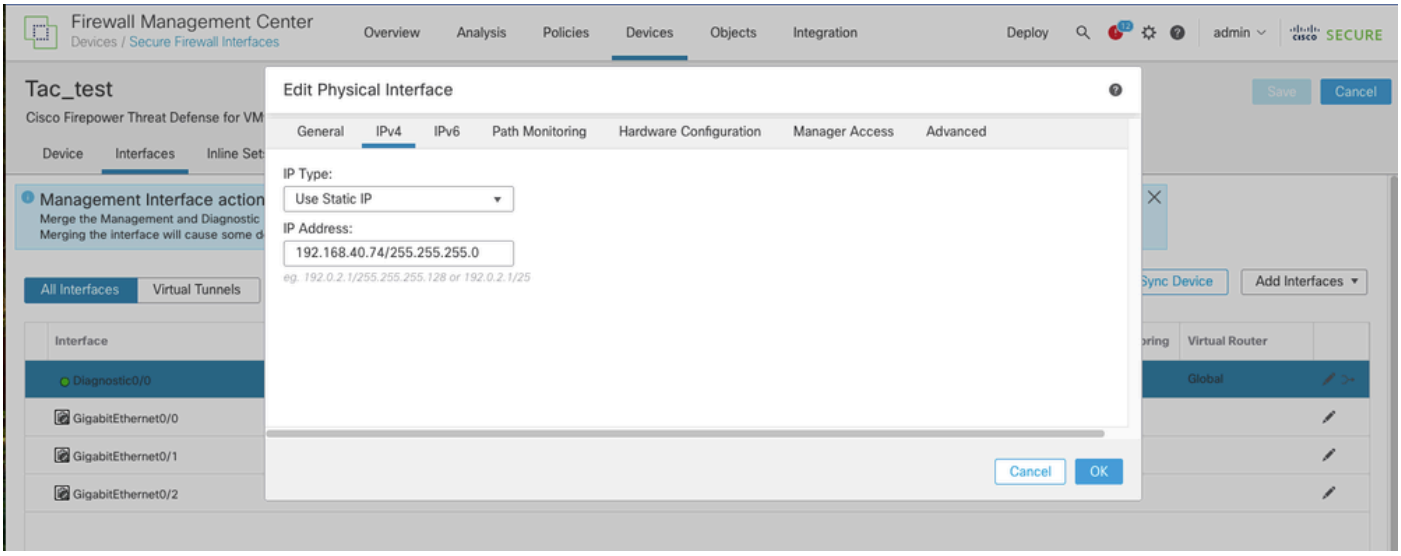


Azione necessaria per unire l'interfaccia di diagnostica e gestione dopo l'aggiornamento del dispositivo alla versione software 7.4.2

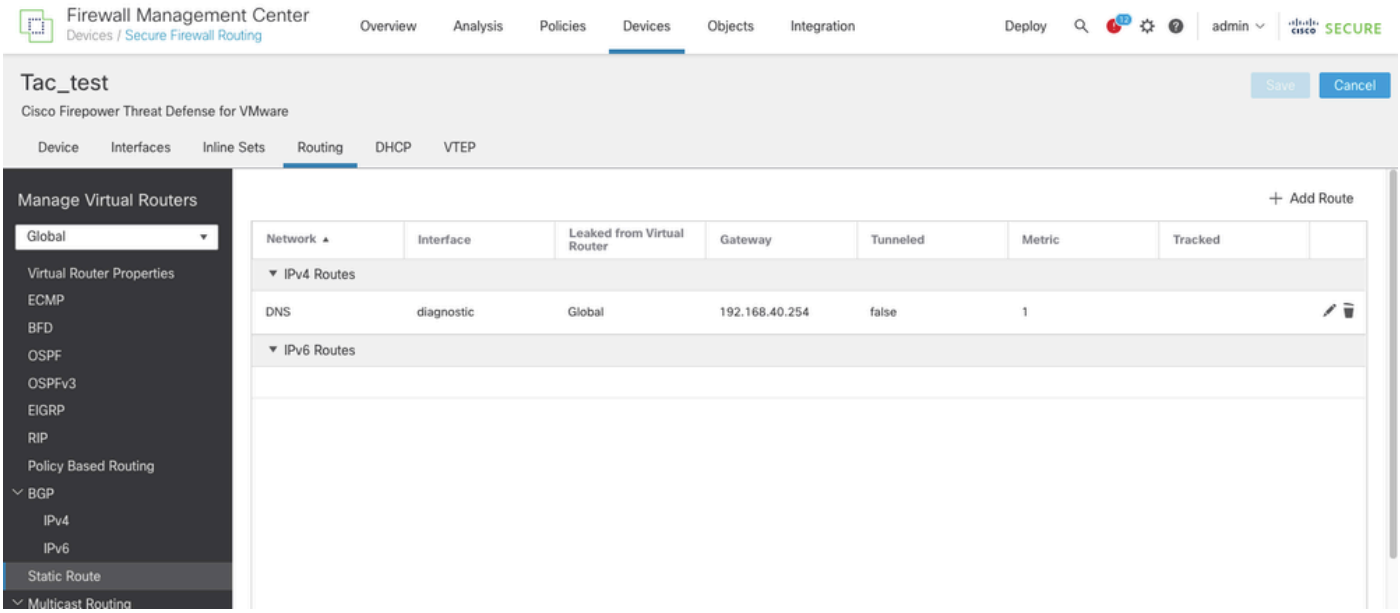
Passaggio 2.

Rimuovere tutte le configurazioni dall'interfaccia di diagnostica. È necessario che l'interfaccia di diagnostica non disponga di alcuna configurazione per continuare l'unione.

In questa interfaccia di diagnostica, ad esempio, sono disponibili le opzioni seguenti: Indirizzo IP e route statica.



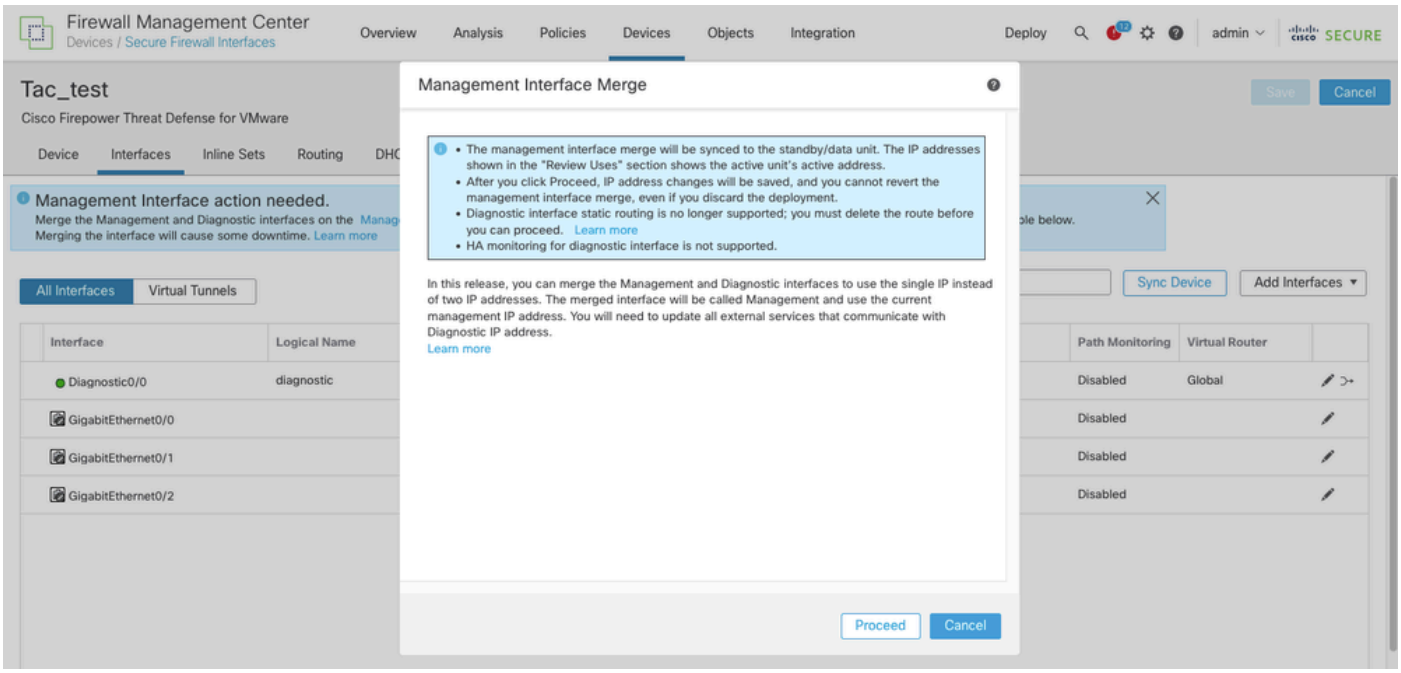
Rimuovi indirizzo IP dell'interfaccia di diagnostica



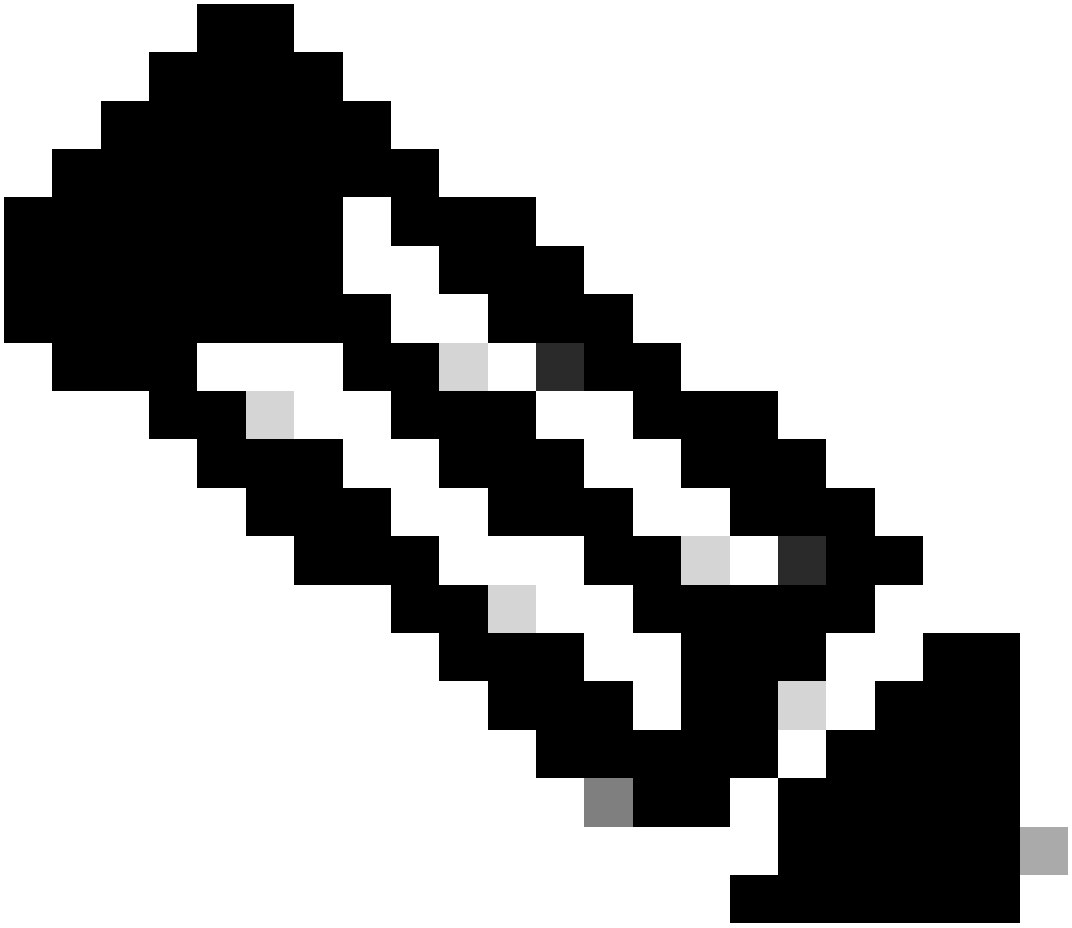
Route statica configurata sull'interfaccia di diagnostica

Passaggio 3.

Fare clic sull'area Azione unione interfaccia di gestione necessaria o sull'icona Unisci accanto all'icona Modifica (matita) nell'interfaccia di diagnostica.

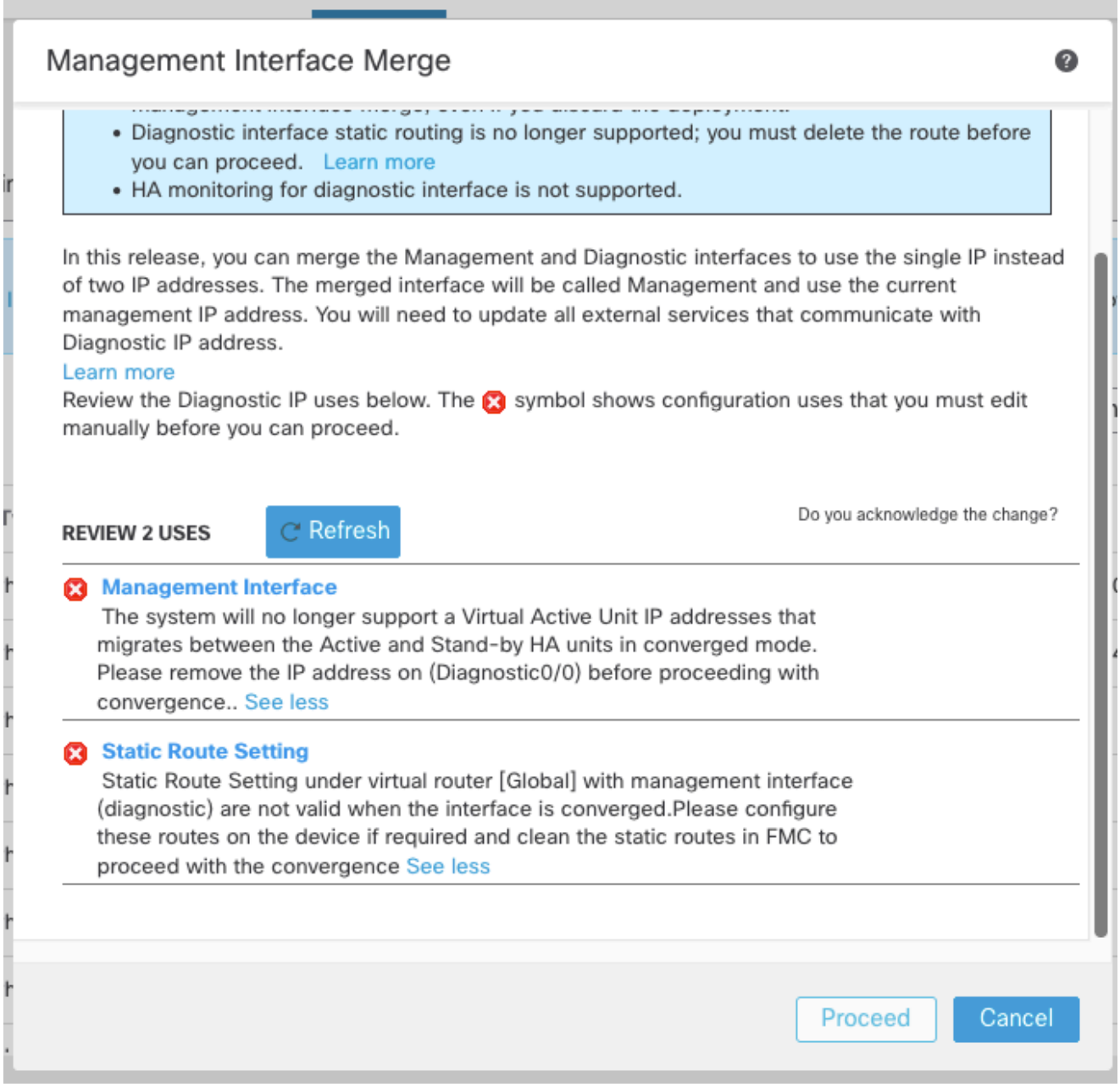


Informazioni unione interfaccia di gestione prima di procedere



Nota: Per le coppie e i cluster ad alta disponibilità, eseguire questa operazione sull'unità di controllo/attiva. La configurazione unita viene replicata automaticamente nelle unità di standby/dati.

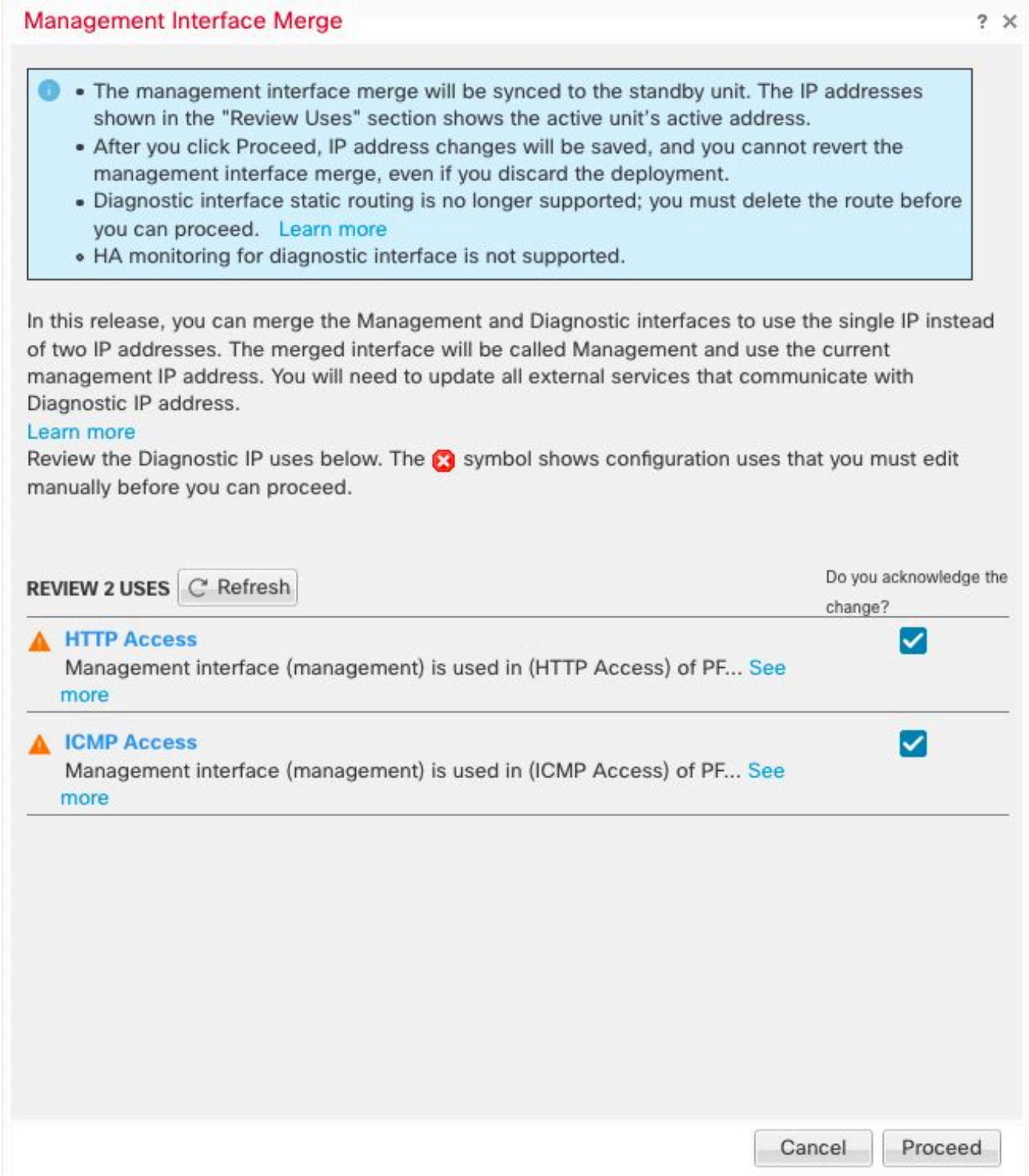
- Per qualsiasi occorrenza che richiede una modifica o rimozione manuale, è possibile che venga visualizzata un'icona di avviso.



Esempio di avviso relativo alle configurazioni da rimuovere prima dell'unione

In caso affermativo: annullare la finestra di dialogo, procedere con la rimozione della configurazione o riconfigurazione, quindi riaprire la finestra di dialogo Unione interfaccia di gestione.

- Le impostazioni della piattaforma che funzioneranno sul dispositivo sono contrassegnate da un'icona di attenzione e richiedono conferma.



Esempio di avviso relativo alle configurazioni di Impostazioni piattaforma che devono essere modificate

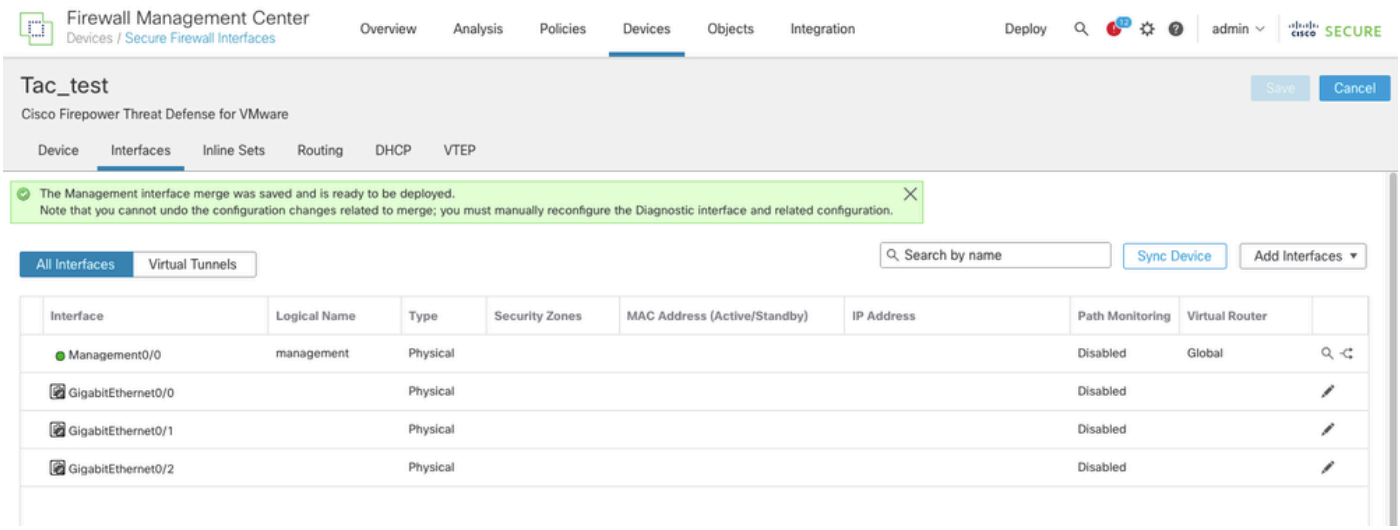
- Fare clic sulla casella in Confermare la modifica? e quindi fare clic su Continua.

Passaggio 4.

Dopo l'unione della configurazione, viene visualizzata un'intestazione di operazione riuscita: "L'unione dell'interfaccia di gestione è stata salvata ed è pronta per la distribuzione.
Non è possibile annullare le modifiche di configurazione correlate all'unione; è necessario

riconfigurare manualmente l'interfaccia di diagnostica e la configurazione correlata."

Distribuire la nuova configurazione unita.



Unione dell'interfaccia di gestione salvata e pronta per la distribuzione

L'interfaccia di gestione è visualizzata nella pagina Interfacce, sebbene sia di sola lettura.

Al termine della distribuzione, la procedura di convergenza sull'interfaccia di gestione è completata.

Passaggio 5. Facoltativo

Se erano presenti servizi esterni che comunicavano con l'interfaccia di diagnostica, è necessario modificarne la configurazione per utilizzare l'indirizzo IP dell'interfaccia di gestione, poiché il fallback della route di gestione è stato rimosso in modalità di convergenza.

Ad esempio:

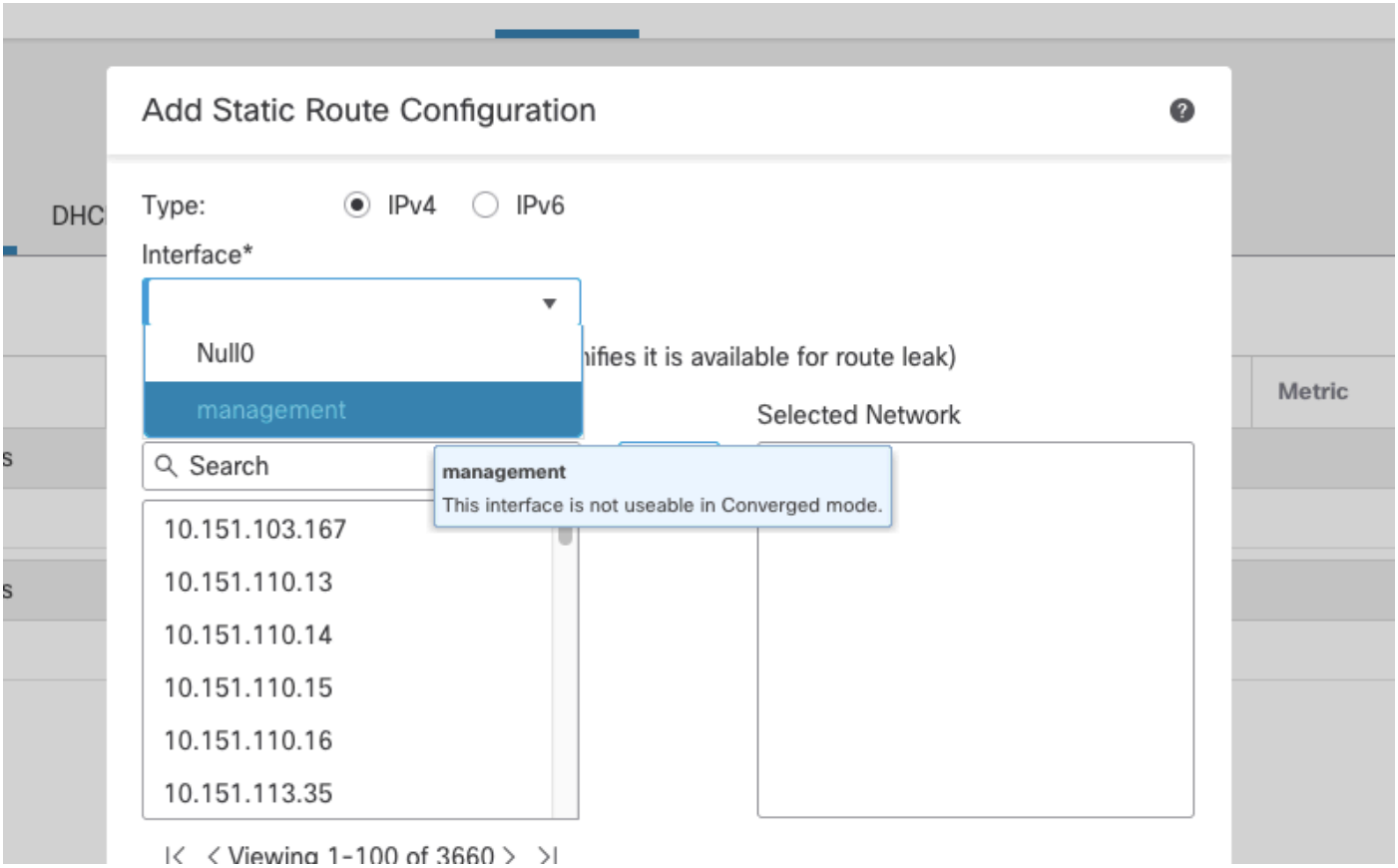
- client SNMP
- server RADIUS
- Server DNS raggiungibile tramite la rete di gestione, l'utente deve selezionare in modo esplicito "Abilita ricerca DNS anche tramite interfaccia di diagnostica/gestione". in Impostazioni piattaforma > Configurazione DNS come eccezione impostata per le ricerche DNS e ICMP (ping e traceroute): in questi casi, la difesa dalle minacce utilizza i dati per poi eseguire automaticamente il fallback alla gestione se non viene individuata una route.

L'uso di route statiche per l'interfaccia di gestione può essere configurato solo tramite la CLI FTD (Linux)

Il percorso predefinito della porta di gestione Lina invia tutti i frame al modulo 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
```

Nell'interfaccia utente di FMC, l'interfaccia di gestione è disattivata per la selezione.



L'interfaccia di gestione non è disponibile per la selezione sulle route statiche dopo il completamento dell'unione.

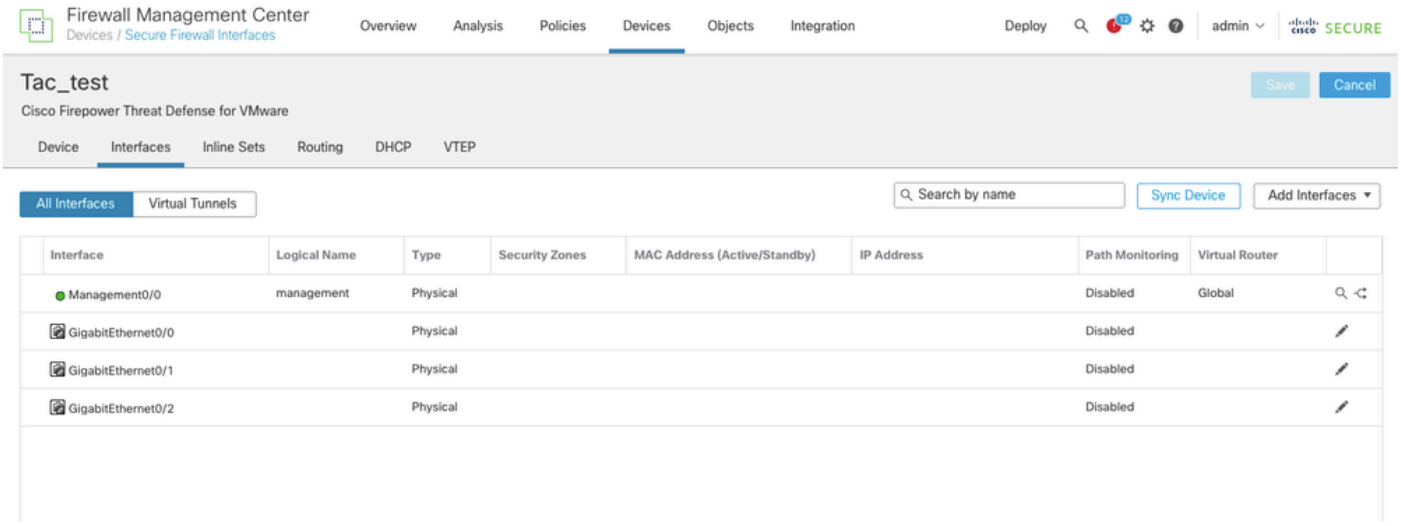
Verifica

Modifiche previste dopo l'unione nell'interfaccia di gestione

- Verificare la modalità di convergenza sulla CLI FTD eseguendo il comando

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

- Nell'interfaccia utente di FMC, il nome dell'interfaccia viene modificato in Management0/0 , il nome logico in management.



Conferma dell'unione per il nome dell'interfaccia di gestione e il nome logico

- Nella CLI FTD, i nuovi indirizzi IP vengono configurati automaticamente su Lina per l'interfaccia di gestione.
  NAT viene utilizzato come implementazione interna: Vengono assegnati l'indirizzo IPv4 privato interno 203.0.113.130 e l'indirizzo IPv6 fd00:0:1:1:2 (entrambi soggetti a modifica). Questi IP sono NAT per gli indirizzi IPv4 e IPv6 FTD del kernel Linux pubblico, quindi non è più necessario avere IP pubblici su Lina.

  In modalità Expert, "ifconfig" visualizza l'indirizzo IPv4 (203.0.113.129) e IPv6 (fd00:0:1:1::1) interno per 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
```

Risoluzione dei problemi - Caso di studio

In questo caso di studio, l'interfaccia di diagnostica su un FTD virtuale ha configurato un indirizzo IP separato per la connettività ai servizi esterni di Ricerca DNS, prima dell'aggiornamento alla versione 7.4.2.

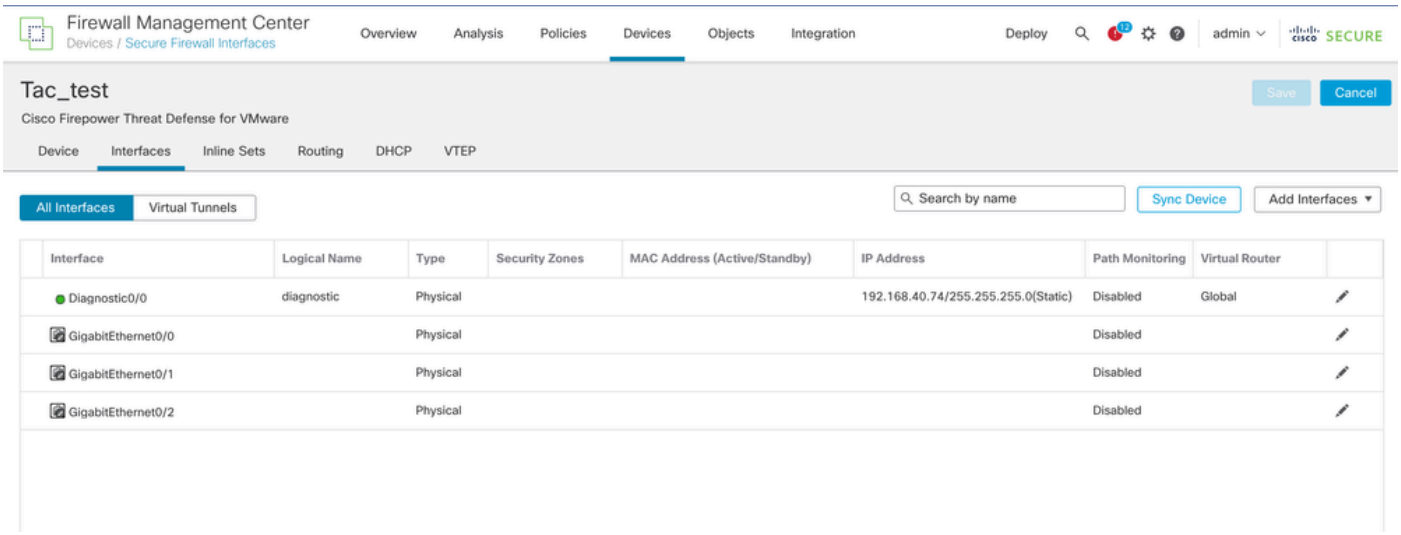
Dopo l'aggiornamento alla versione 7.4.2, è necessaria la convergenza, così è la configurazione nell'interfaccia utente FMC, nella CLI FTD e in Linux, prima e dopo l'unione.

Ci sono anche acquisizioni del traffico su FTD CLI Lina e Linux per mostrare il traffico usando lo spostamento dell'interfaccia diagnostica logica per usare l'interfaccia di gestione.

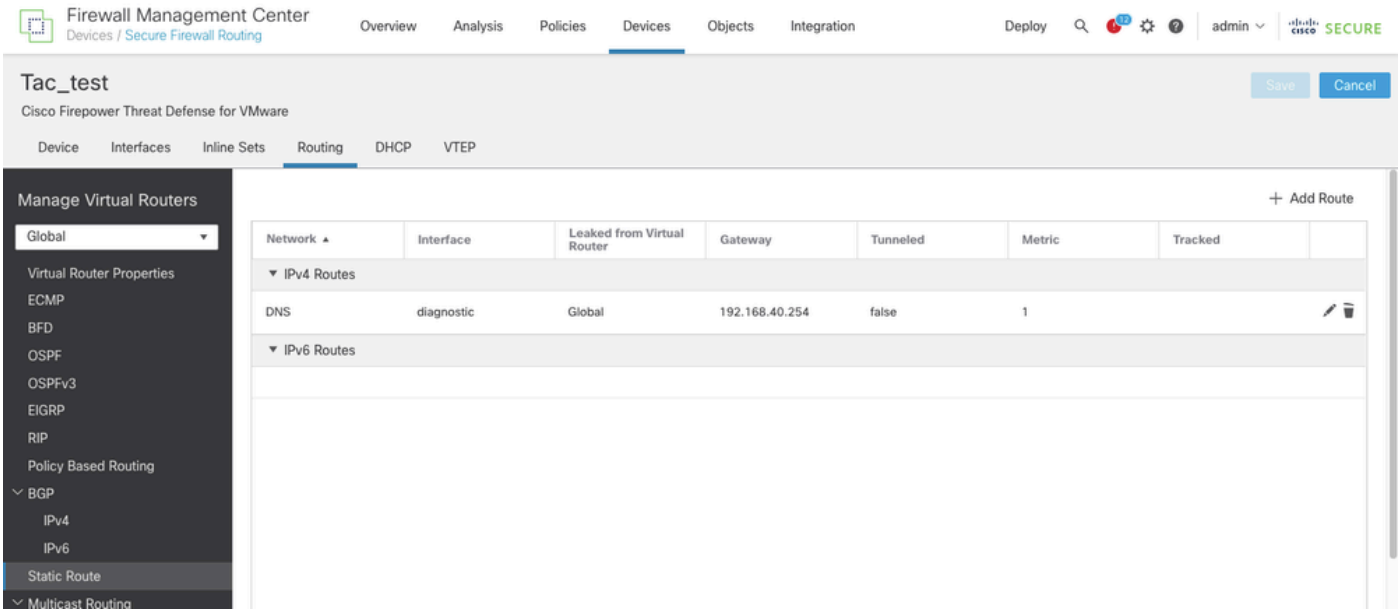
Prima della configurazione di convergenza

L'interfaccia diagnostica ha un IP separato e una route statica per la ricerca DNS, in questo modo funziona usando entrambe le interfacce logiche da Lina a Linux nell'FTD.

Configurazione interfaccia utente FMC



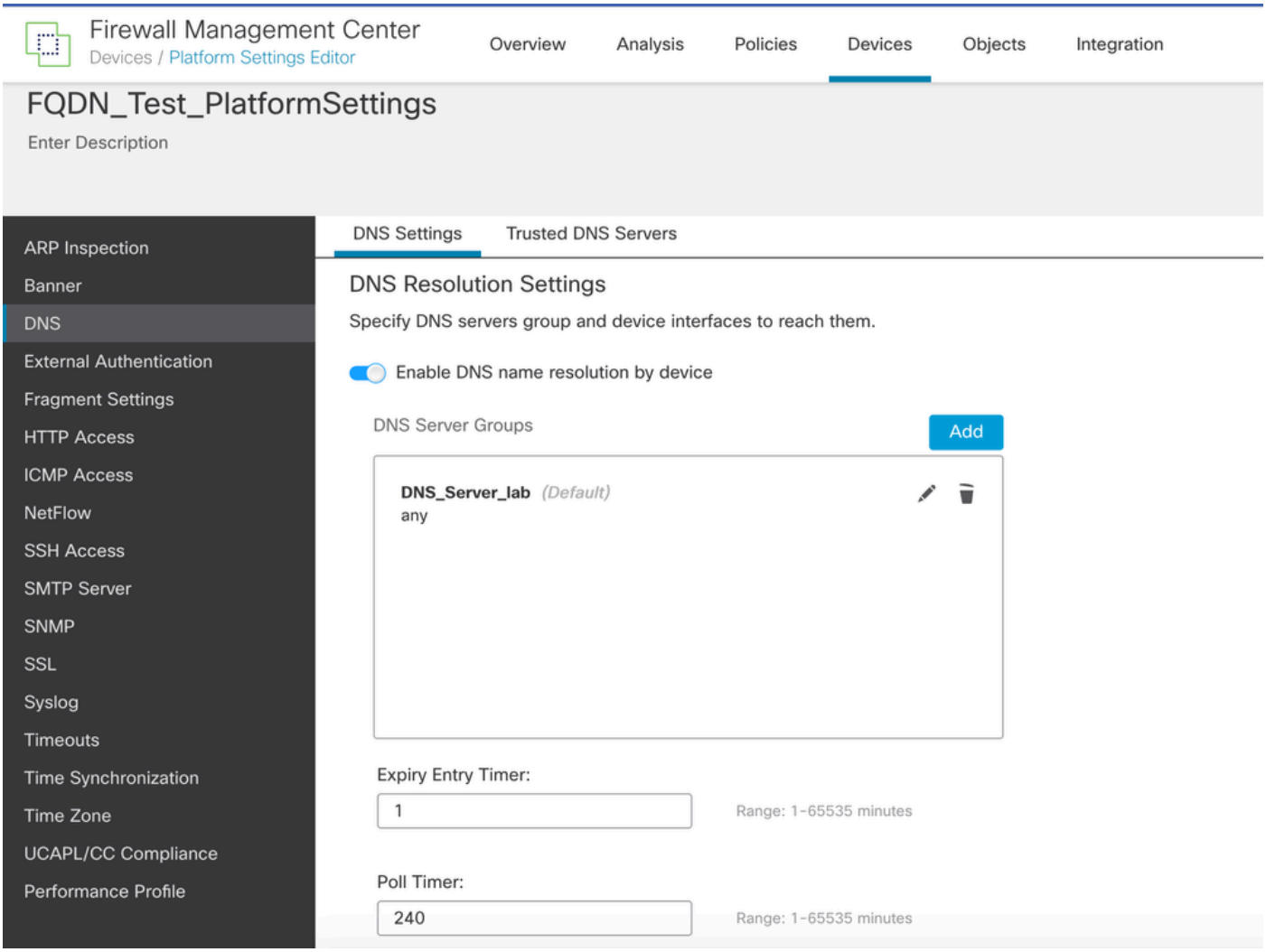
Configurazione dell'interfaccia di diagnostica prima dell'unione



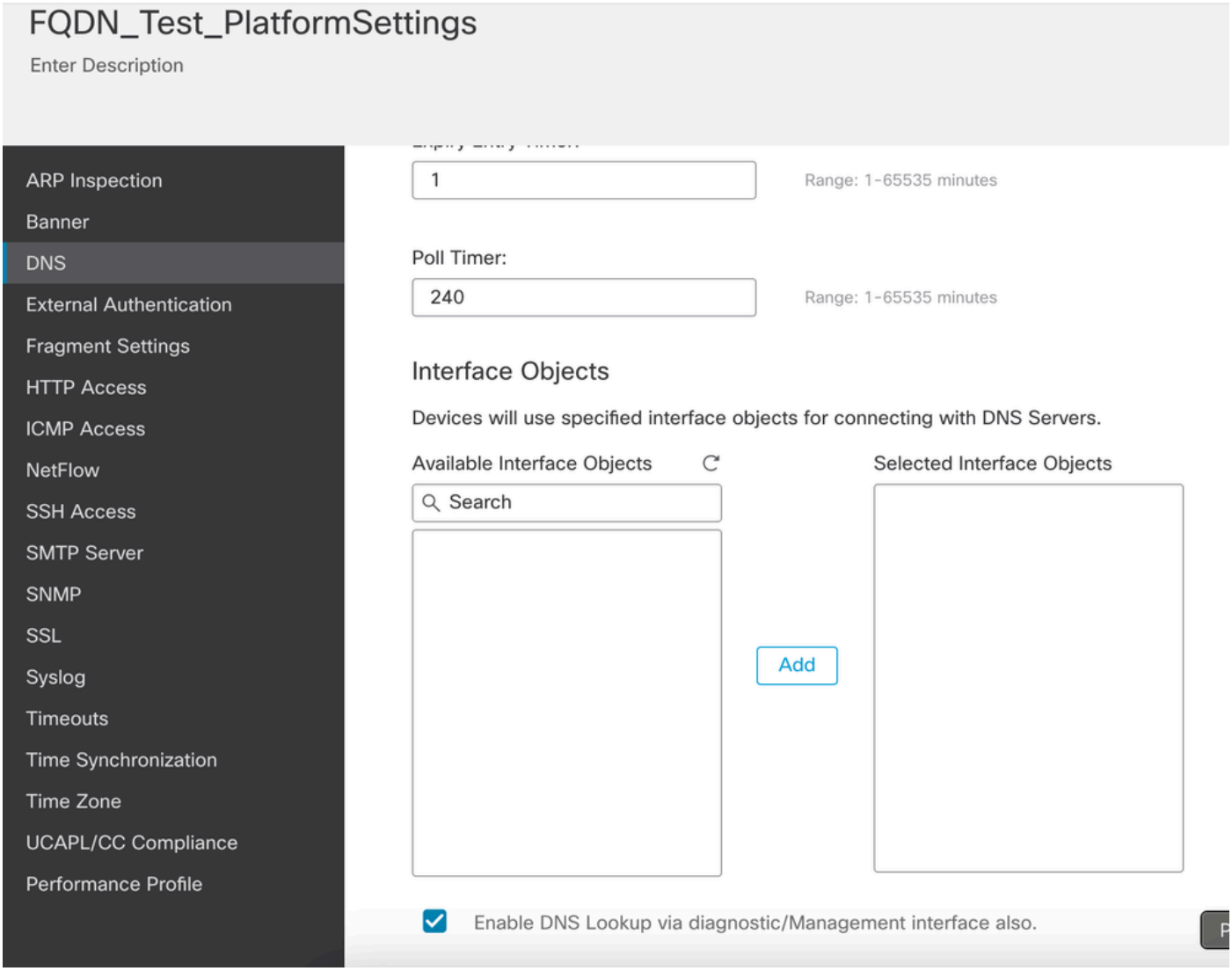
Route statica configurata sull'interfaccia di diagnostica

Configurazione DNS su

Dispositivi > Impostazioni piattaforma, selezionare il criterio, quindi scheda DNS.



Configurazione DNS in Impostazioni piattaforma



Casella di controllo selezionata per Abilita ricerca DNS anche tramite interfaccia di diagnostica/gestione

Configurazione per l'interfaccia diagnostica su Lina 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
```

Configurazione DNS su Lina CLI 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
```

Acquisizione sull'interfaccia diagnostica per il traffico DNS diretto al server 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#
```

Acquisire in modalità esperto Linux per verificare il corretto flusso del traffico di ricerca DNS sull'interfaccia di gestione dall'interfaccia di diagnostica

```
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)
```

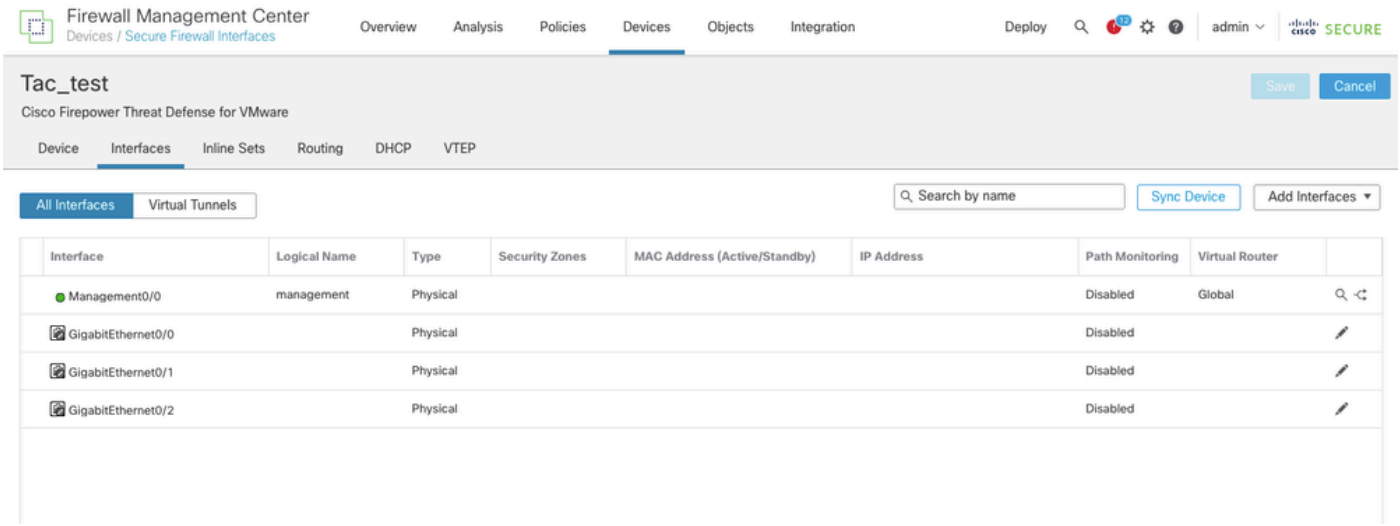
Dopo la configurazione della convergenza

Come indicato nella procedura di convergenza, per eseguire l'unione è necessario rimuovere tutte le configurazioni dell'interfaccia diagnostica.

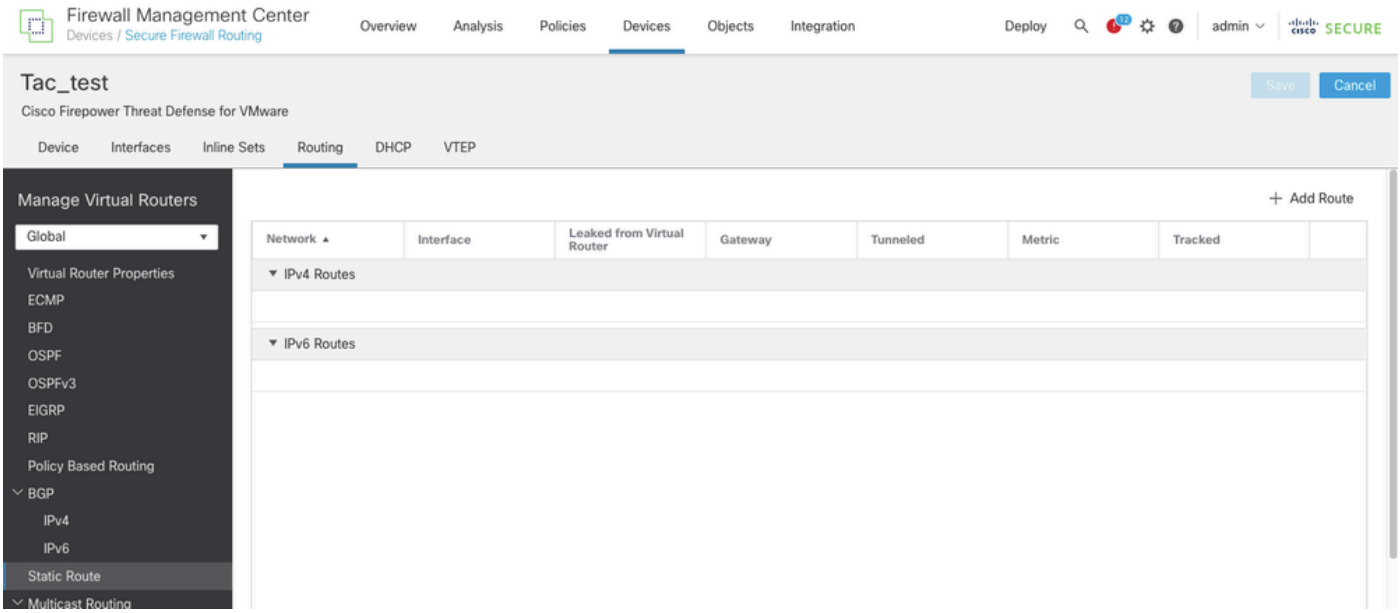
Queste sono le informazioni su FMC e FTD CLI una volta completata l'unione.

Configurazione dell'interfaccia di gestione sull'interfaccia utente di FMC

Dispositivi > Gestione dispositivi, selezionare FTD. Viene visualizzata direttamente la scheda Interfacce.



Interfaccia di gestione dopo l'unione

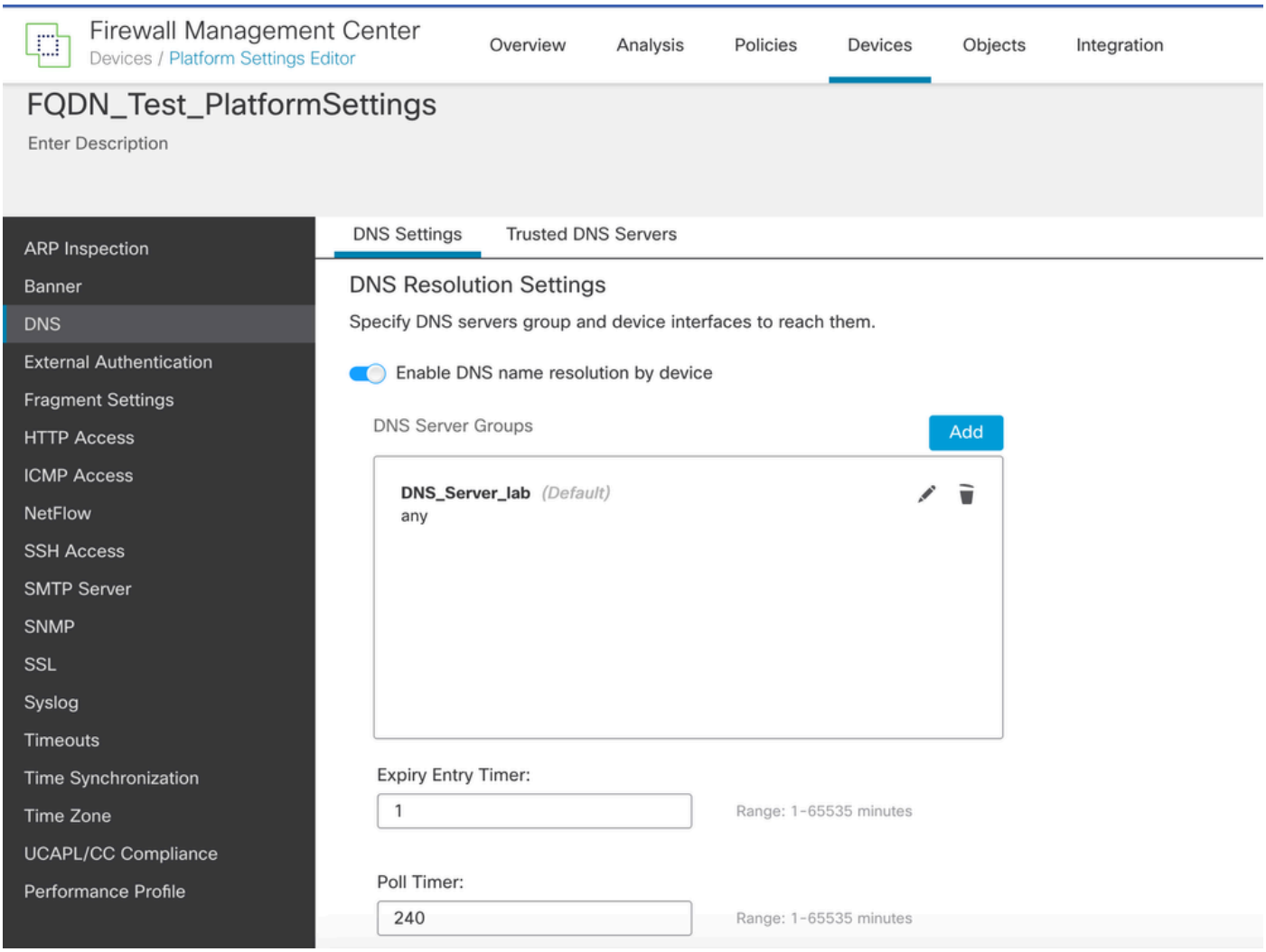


Nessuna route statica aggiunta al server DNS

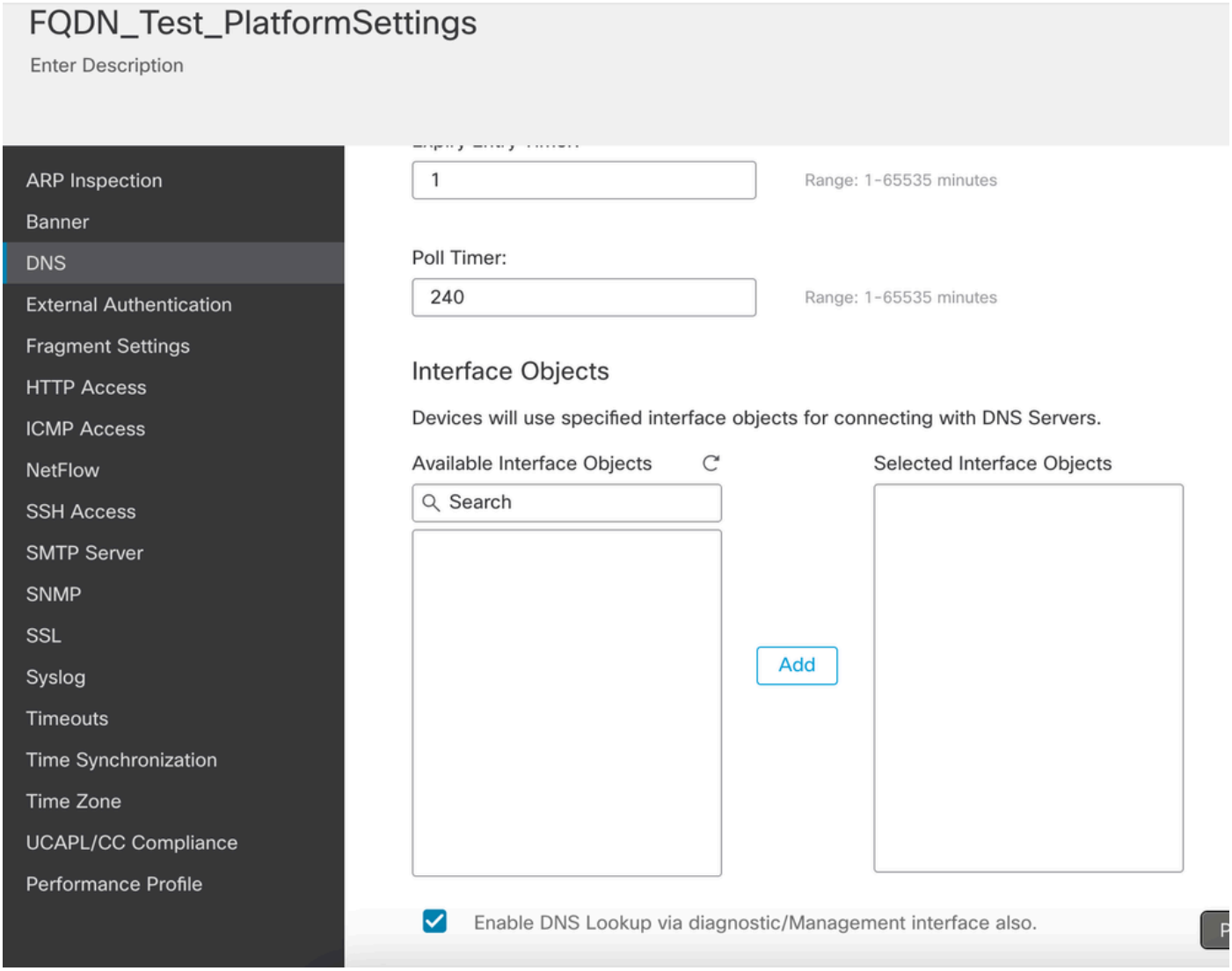
La configurazione DNS deve rimanere la stessa in Impostazioni piattaforma.

Dispositivi > Impostazioni piattaforma, selezionare il criterio, quindi scheda DNS.

Affinché la ricerca DNS possa continuare a essere inviata all'interfaccia di gestione senza dover aggiungere una route statica, è necessario attivare la funzionalità "Abilita ricerca DNS anche tramite l'interfaccia di diagnostica/gestione". deve rimanere selezionato.



Configurazione DNS in Impostazioni piattaforma



Anche l'opzione per l'abilitazione della ricerca DNS tramite l'interfaccia di diagnostica/gestione deve rimanere invariata

Configurazione sulla CLI 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
```

Configurazione DNS su CLI FTD su 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
```

Acquisire in modalità esperto Linux per confermare il flusso corretto del traffico di ricerca DNS sull'interfaccia di gestione.

```
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 questa evidenza, è possibile confermare che la ricerca DNS continua a funzionare anche se non viene aggiunta alcuna route statica all'interfaccia di gestione tramite Linux.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).