Konfigurieren der Schnittstelle für die Zusammenführung von Management und Diagnose in FMC

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren der Zusammenführung der Verwaltungs- und Diagnoseschnittstellen beschrieben, die in der FTD 7.4.0-Version hinzugefügt wurden.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesen Themen verfügen:

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

Hintergrundinformationen

In Version 7.3 und früheren Versionen wird die physische Verwaltungsschnittstelle von der logischen Diagnoseschnittstelle (Lina) und der logischen Verwaltungsschnittstelle (Linux) gemeinsam verwendet.

In Version 7.4 und höher wird die Diagnoseschnittstelle mit Management zusammengeführt, um die Benutzererfahrung zu vereinfachen.

Bei neuen Geräten, die Version 7.4 oder höher verwenden, können Sie die ältere Diagnoseschnittstelle nicht verwenden. Nur die zusammengeführte Management-Schnittstelle ist verfügbar.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

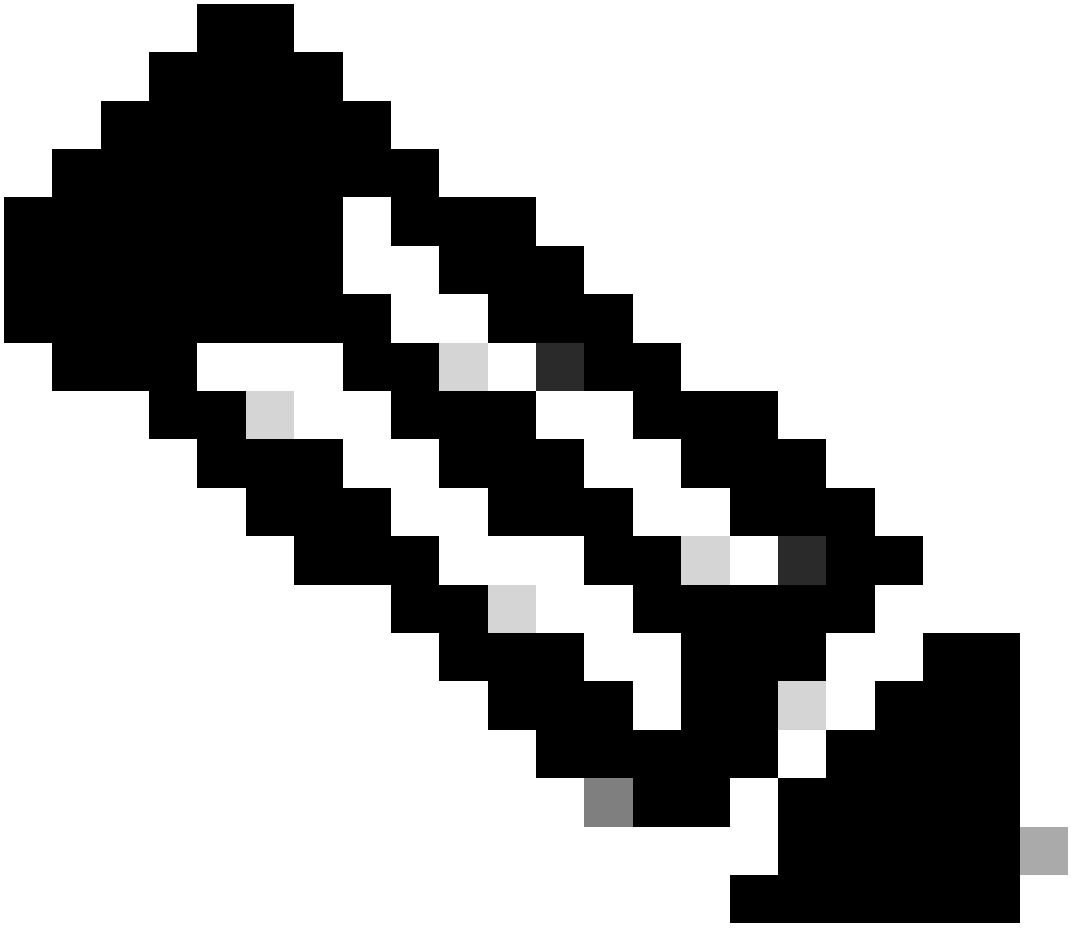
- Virtual Cisco Secure Firewall Threat Defense (FTD), Version 7.4.2
- Virtual Cisco Secure Firewall Manager Center (FMC), Version 7.4.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Wenn Sie ein Upgrade auf Version 7.4 oder höher durchgeführt haben und über eine Konfiguration für die Diagnoseschnittstelle verfügen, können Sie die Schnittstellen manuell zusammenführen, oder Sie können die separate Diagnoseschnittstelle weiter verwenden.

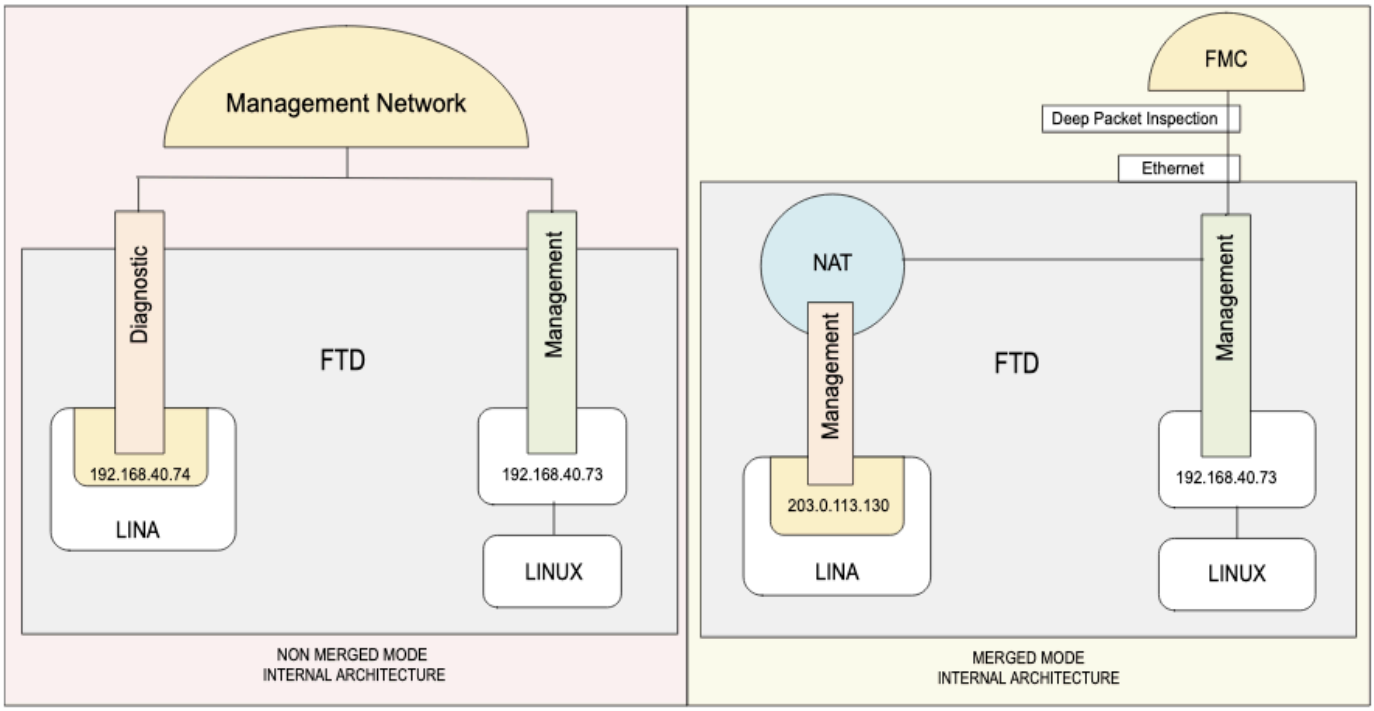
Falls Sie keine Konfiguration für die Diagnoseschnittstelle haben, wird die Schnittstellenzusammenführung automatisch durchgeführt.



Anmerkung: Die Unterstützung für die Diagnoseschnittstelle soll in einem späteren Release entfernt werden, daher planen Sie, die Schnittstellen so schnell wie möglich zusammenzuführen.

FTD - Diagramm der internen Architektur

Überblick über die konvergente Management-Schnittstelle



Überblick über die interne Architektur vor und nach der Konvergenzmanagement-Schnittstelle

Links die interne Architektur für die logische Diagnoseschnittstelle (Lina) und die logische Verwaltungsschnittstelle (Linux). Version 7.3 und früher.

Auf der rechten Seite sehen Sie die interne Architektur für eine einzige Management-Schnittstelle. Der Lina-Zugriff auf das Managementnetzwerk nutzt den NAT-Dienst.

Konvergenzverfahren

Wenn die Konfiguration auf der Diagnoseschnittstelle vorhanden ist, werden die Schnittstellen nach einem Upgrade nicht automatisch zusammengeführt, und Sie müssen das Konvergenzverfahren durchführen.

Bei diesem Verfahren müssen Konfigurationsänderungen bestätigt und in einigen Fällen manuell behoben werden.

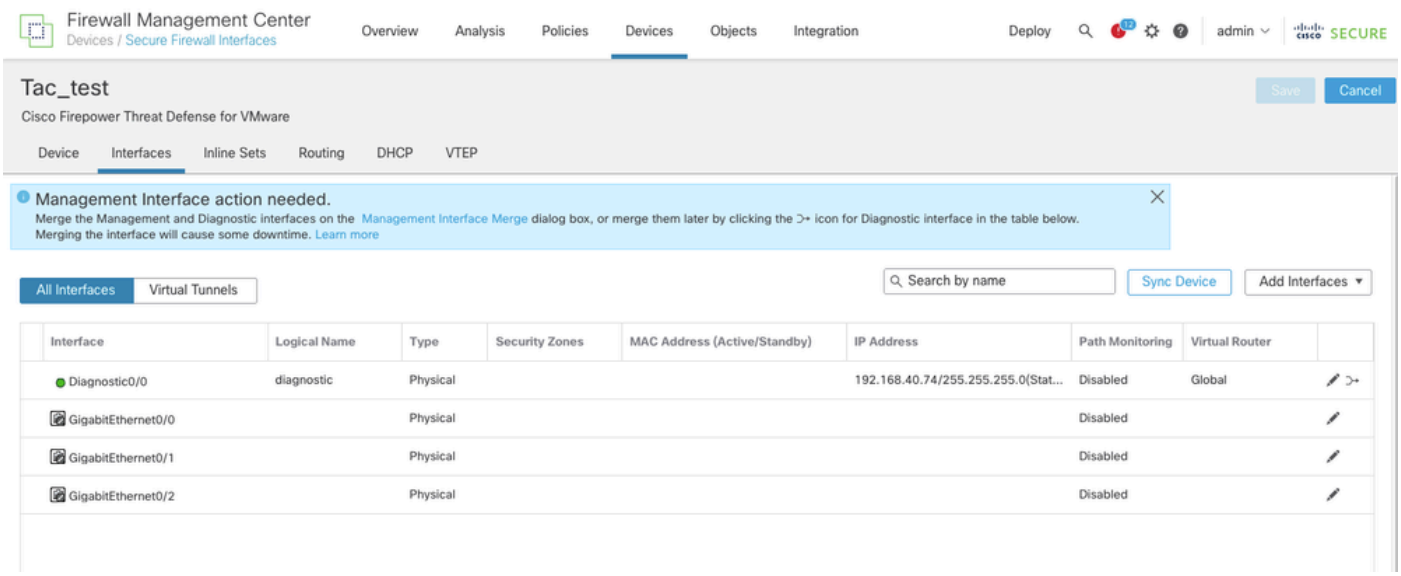
Um den aktuellen Modus des Geräts anzuzeigen, geben Sie den Befehl show management-interface converge in der FTD-CLI ein.

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

Dieses Ergebnis zeigt, dass die Verwaltungsschnittstellen nicht zusammengeführt wurden.

Schritt 1:
Navigieren Sie auf der FMC-Benutzeroberfläche zu Devices > Device Management (Geräte > Gerätemanagement), und wählen Sie das FTD aus, das bearbeitet werden soll. Es wird direkt zur

Registerkarte Schnittstellen geöffnet.

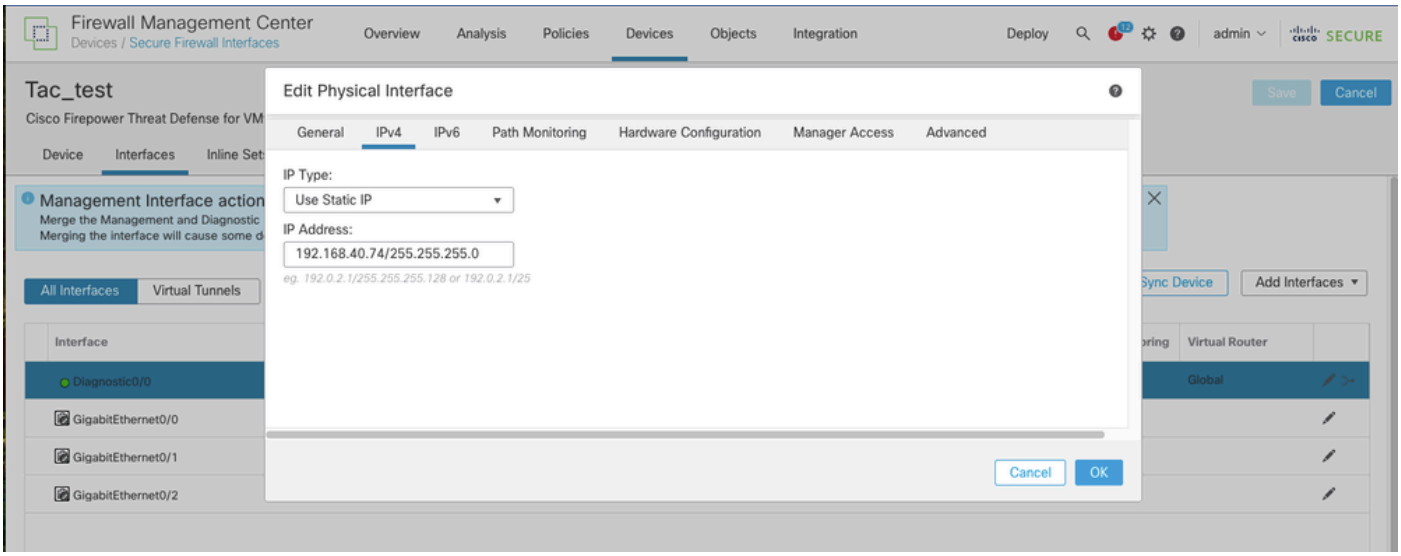


Aktion erforderlich, um Diagnose- und Verwaltungsschnittstelle nach dem Geräte-Upgrade auf Softwareversion 7.4.2 zusammenzuführen

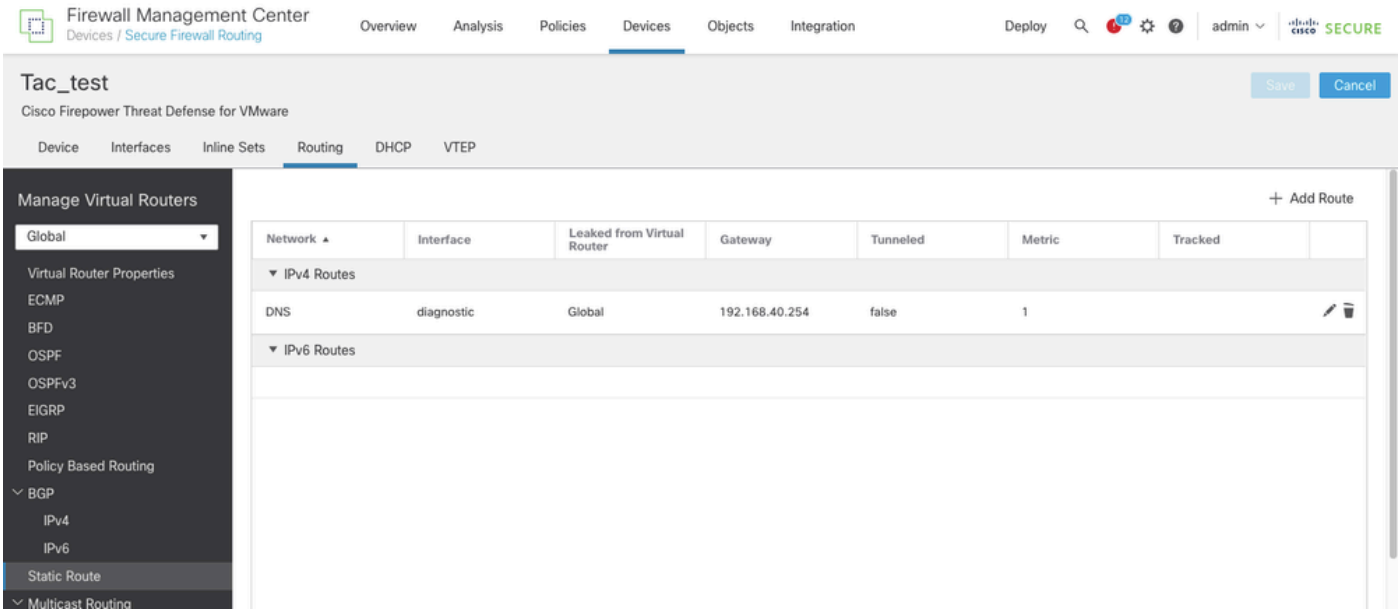
Schritt 2:

Entfernen Sie alle Konfigurationen der Diagnoseschnittstelle. Es ist zwingend erforderlich, dass die Diagnoseschnittstelle nicht konfiguriert ist, um mit dem Zusammenführen fortzufahren.

In dieser Diagnoseschnittstelle gibt es z. B.: IP-Adresse und statische Route.



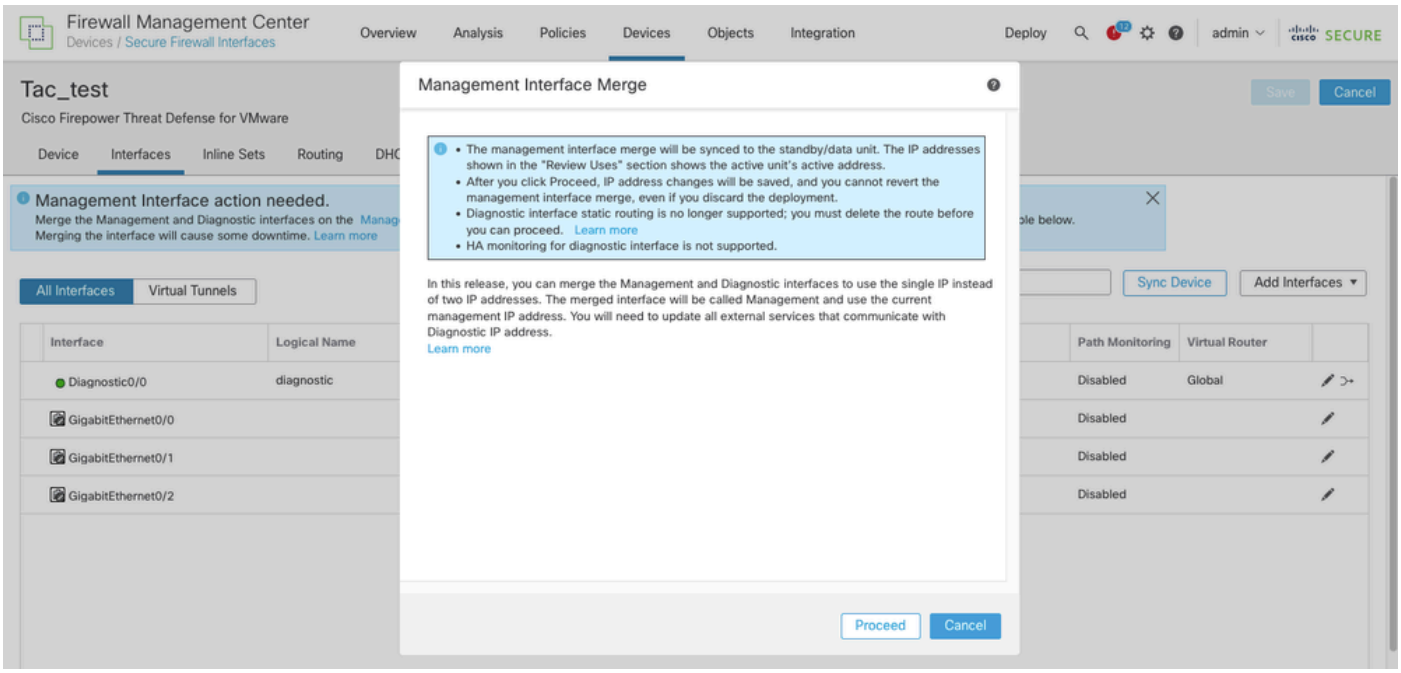
IP-Adresse der Diagnoseschnittstelle entfernen



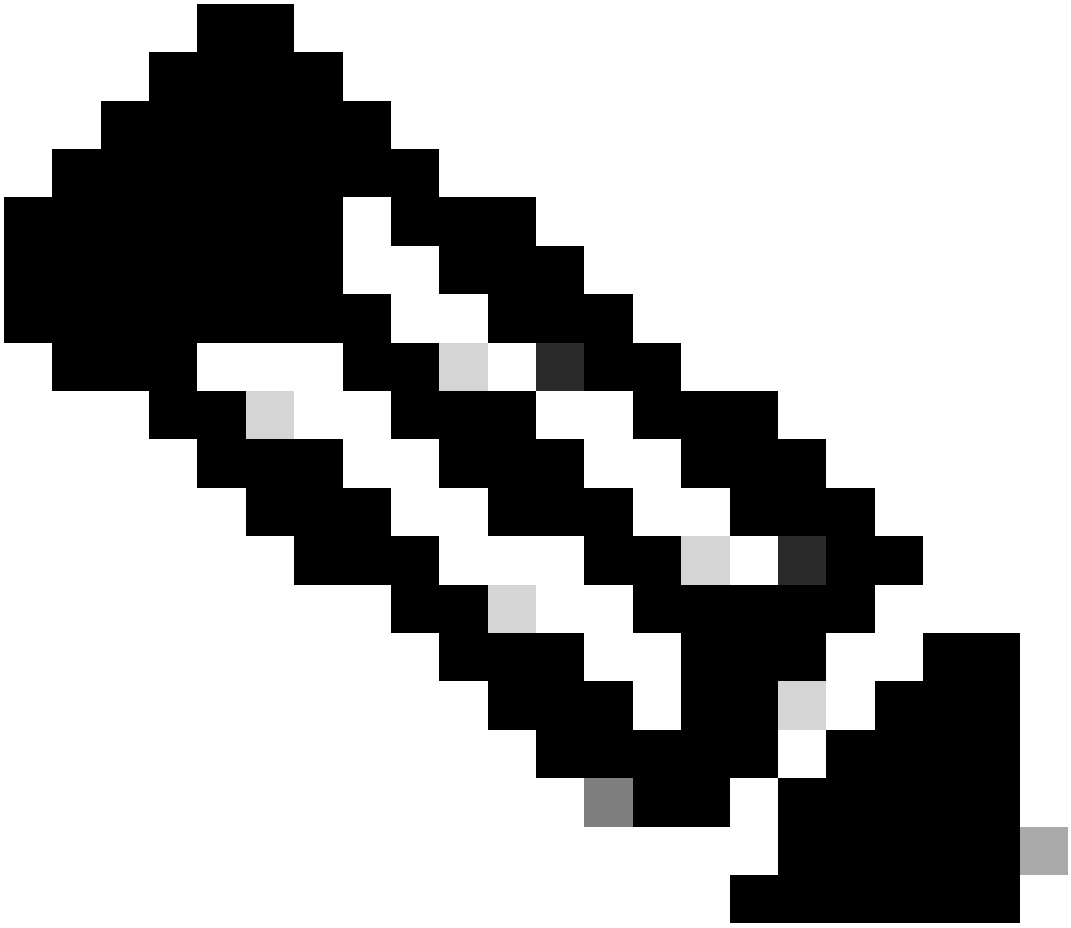
Statische Routenkonfiguration auf Diagnoseschnittstelle

Schritt 3:

Klicken Sie auf den Bereich Management Interface Merge (Aktion erforderlich) oder auf das Symbol Merge neben dem Symbol Edit (Bearbeiten) auf der Diagnoseschnittstelle.

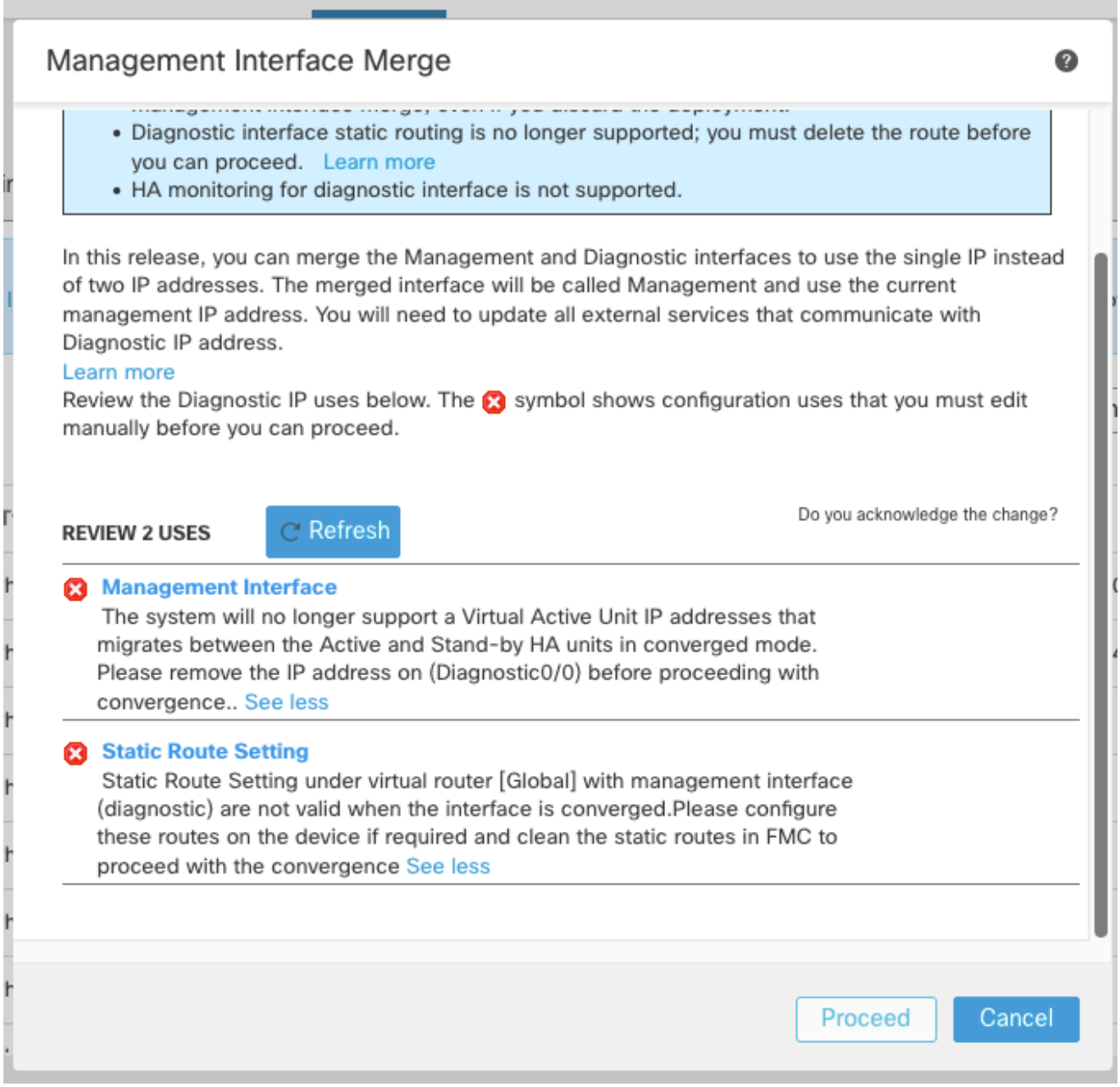


Zusammenführungsinformationen der Verwaltungsschnittstelle vor dem Fortfahren



Anmerkung: Bei Hochverfügbarkeitspaaren und -clustern führen Sie diese Aufgabe an der Aktiv-/Steuereinheit aus. Die zusammengeführte Konfiguration wird automatisch auf die Standby-/Dateneinheiten repliziert.

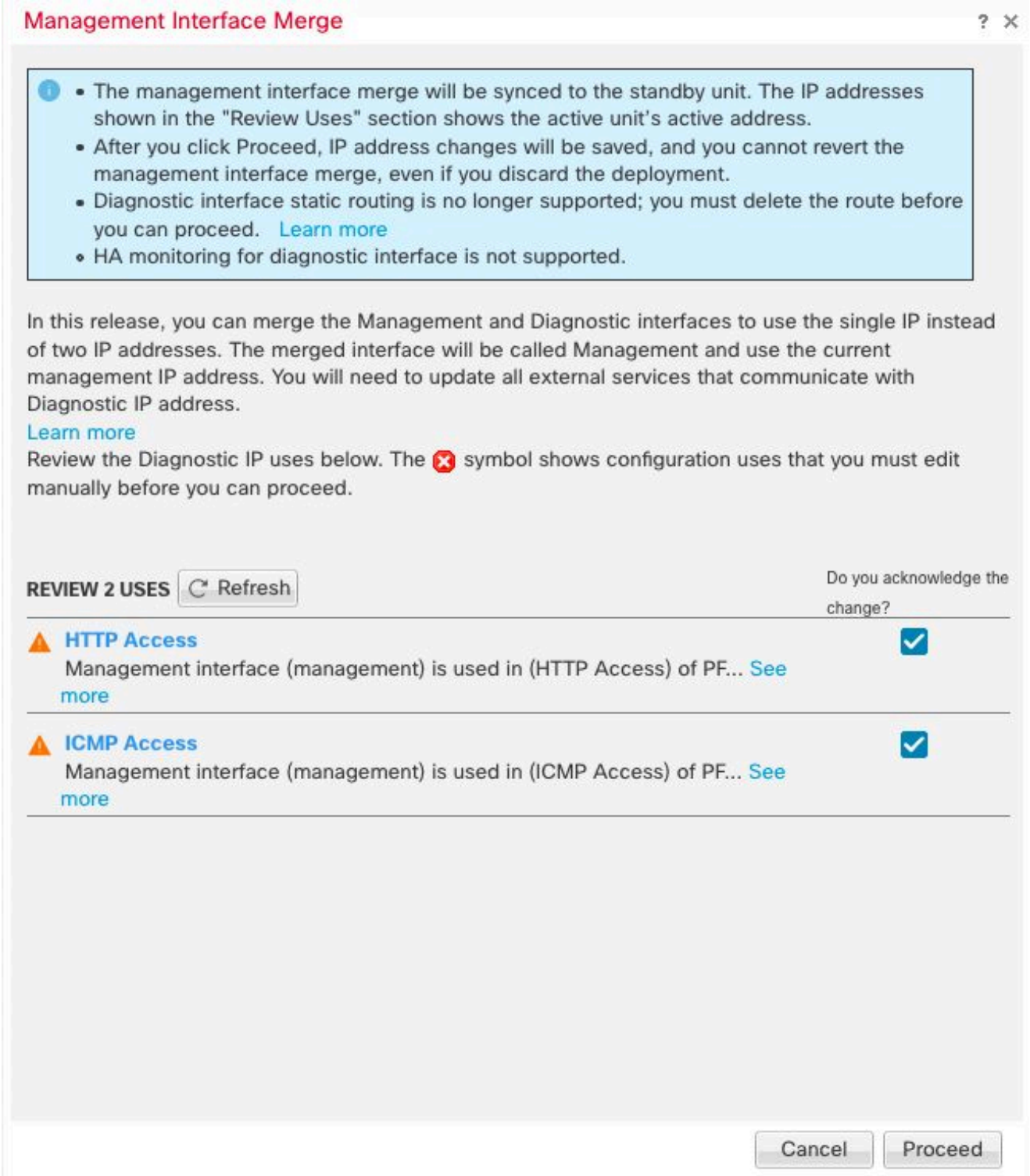
- Bei allen Ereignissen, die manuell geändert oder entfernt werden müssen, kann ein Warnsymbol angezeigt werden.



Beispiel für eine Warnung, dass Konfigurationen vor dem Zusammenführen entfernt werden müssen

Wenn dies der Fall ist: das Dialogfeld abbrechen, mit dem Entfernen der Konfiguration oder der Neukonfiguration fortfahren und dann das Dialogfeld "Management Interface Merge" erneut öffnen.

- Plattformeinstellungen, die auf dem Gerät funktionieren, sind mit einem Warnsymbol gekennzeichnet und erfordern eine Bestätigung.



Beispiel für eine Warnung bei Plattformeinstellungskonfigurationen, die bearbeitet werden müssen

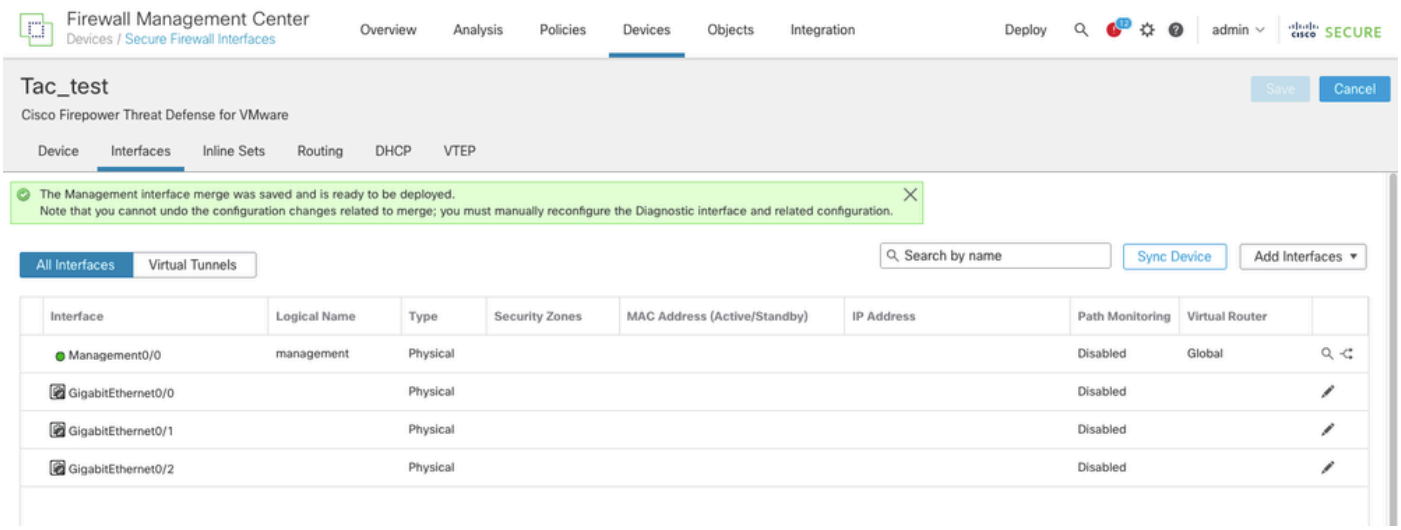
- Klicken Sie auf das Feld Bestätigen Sie die Änderung? , und klicken Sie dann auf Proceed (Fortfahren).

Schritt 4:

Nach dem Zusammenführen der Konfiguration wird ein Banner mit Erfolgsgeschichten angezeigt: "Die Zusammenführung der Management-Schnittstelle wurde gespeichert und kann jetzt

bereitgestellt werden.
Beachten Sie, dass Sie die beim Zusammenführen vorgenommenen Konfigurationsänderungen nicht rückgängig machen können. Sie müssen die Diagnoseschnittstelle und die zugehörige Konfiguration manuell neu konfigurieren."

Bereitstellen der neuen zusammengeführten Konfiguration



Die Zusammenführung der Management-Schnittstelle wird gespeichert und ist einsatzbereit.

Die Management-Schnittstelle wird auf der Seite Interfaces (Schnittstellen) angezeigt, obwohl sie schreibgeschützt ist.

Nach der Bereitstellung ist das Konvergenzverfahren auf der Verwaltungsschnittstelle abgeschlossen.

Schritt 5. Optional

Wenn externe Dienste mit der Diagnoseschnittstelle kommuniziert haben, müssen Sie deren Konfiguration ändern, um die IP-Adresse der Verwaltungsschnittstelle zu verwenden, da der Fallback "Management Route" im konvergenten Modus entfernt wurde.

Beispiele:

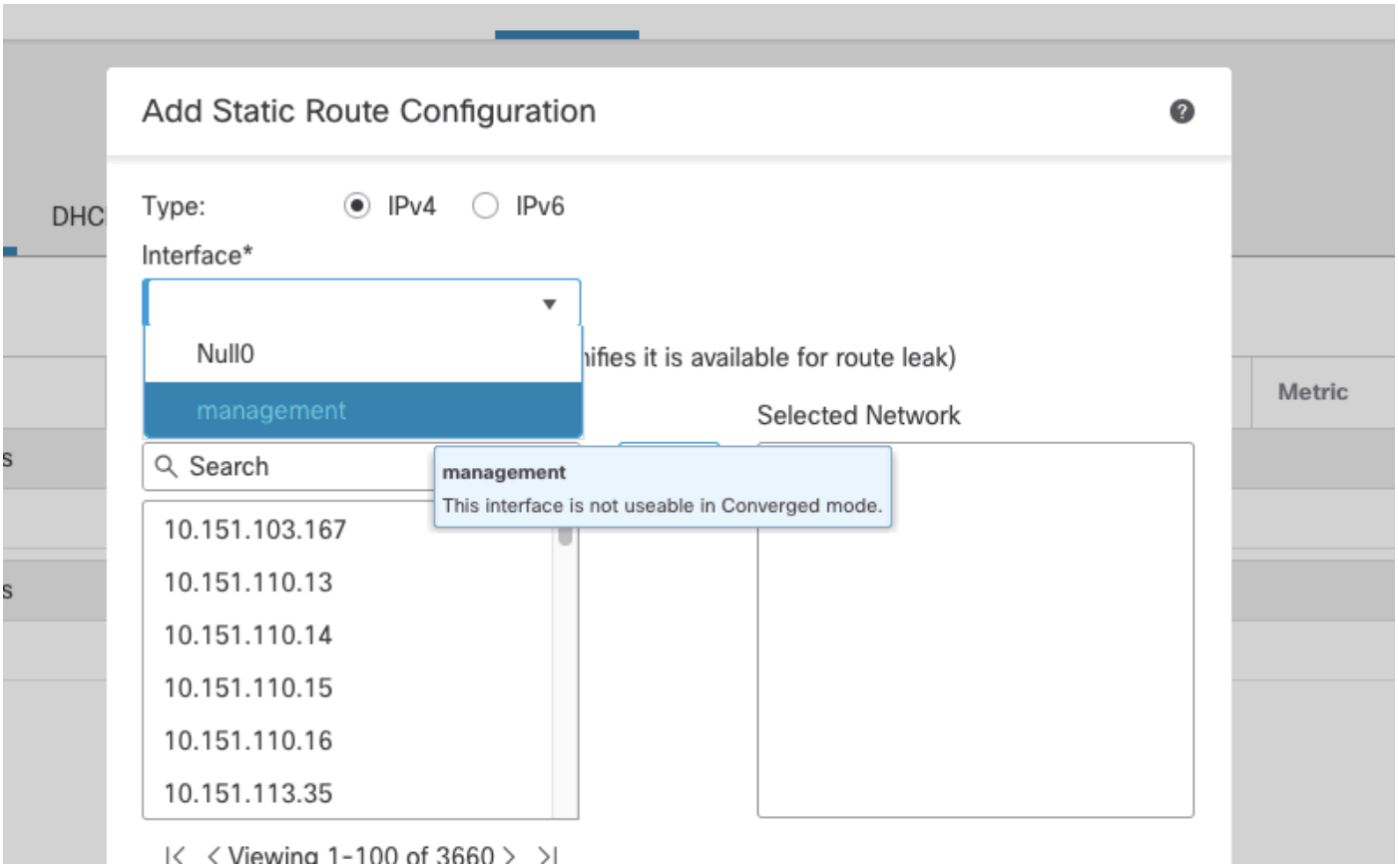
- SNMP-Client
- RADIUS-Server
- Um über das Managementnetzwerk auf den DNS-Server zugreifen zu können, muss der Benutzer explizit "DNS-Lookup über Diagnose-/Verwaltungsschnittstelle aktivieren" auswählen. unter Plattformeinstellungen > DNS-Konfiguration als Ausnahme für DNS-Lookups und ICMP (Ping und Traceroute): In diesen Fällen verwendet die Bedrohungsabwehr Daten und greift dann automatisch auf das Management zurück, wenn keine Route gefunden wird.

Die Verwendung statischer Routen für die Management-Schnittstelle kann nur über die FTD CLI Clish (Linux) konfiguriert werden.

Die Standardroute des Lina-Management-Ports sendet alle Frames an das Linux-Modul.

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

Auf der FMC-Benutzeroberfläche ist die Management-Oberfläche zur Auswahl abgeblendet.



Die Verwaltungsschnittstelle ist nach Abschluss des Zusammenführens für statische Routen nicht verfügbar.

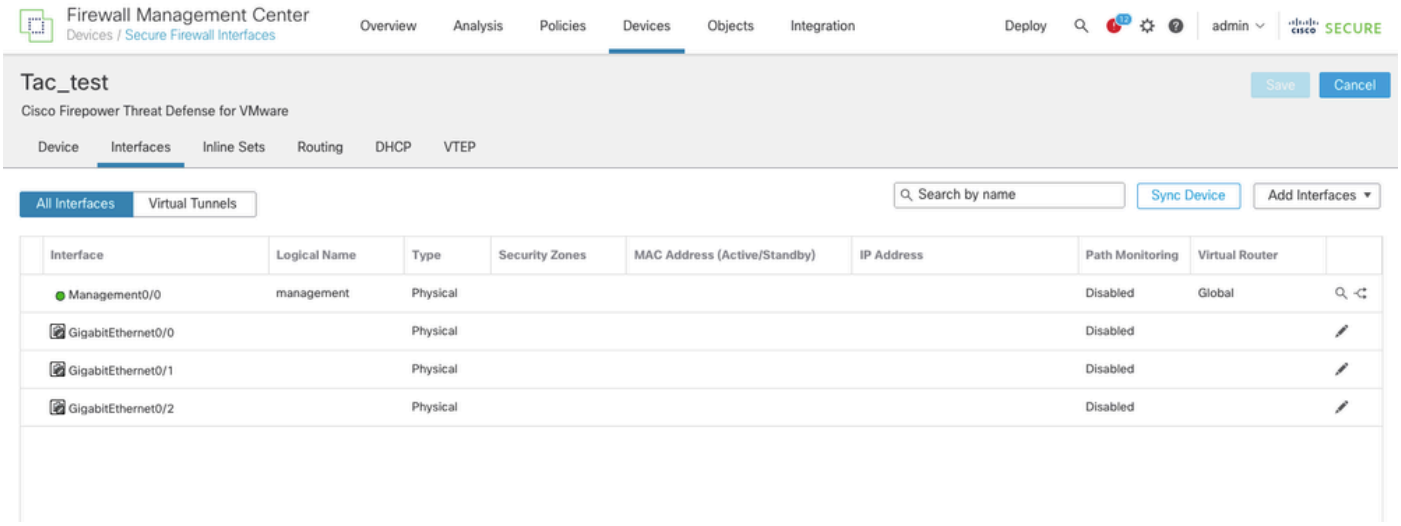
Überprüfung

Erwartete Änderungen nach dem Zusammenführen auf der Verwaltungsschnittstelle

- Überprüfen Sie den Konvergenzmodus bei einem FTD CLI-Mausklick, indem Sie den Befehl

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

- Auf der FMC-Benutzeroberfläche wird der Schnittstellenname in Management0/0, der logische Name in Management geändert.



Zusammenführungsbestätigung für den Management-Schnittstellennamen und den logischen Namen

- Bei FTD CLI Clish werden die neuen IP-Adressen automatisch auf der Lina for Management-Schnittstelle konfiguriert.
  NAT wird als interne Implementierung verwendet: Die interne private IPv4-Adresse 203.0.113.130 und die IPv6-Adresse fd00:0:1:1::2 sind zugewiesen (Änderungen vorbehalten).
  Diese IPs sind NATed zu den öffentlichen Linux Kernel FTD IPv4 und IPv6 Adressen, daher gibt es keinen Bedarf für öffentliche IPs auf Lina mehr.

  Im Expertenmodus zeigt "ifconfig" die interne IPv4- (203.0.113.129) und IPv6-Adresse (fd00:0:1:1::1) für Linux an.

```
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
```

Fehlerbehebung - Fallstudie

In diesem Fall hat die Diagnoseschnittstelle auf einem virtuellen FTD eine separate IP-Adresse für die Verbindung zu externen Diensten der DNS-Suche konfiguriert, bevor ein Upgrade auf 7.4.2 durchgeführt wird.

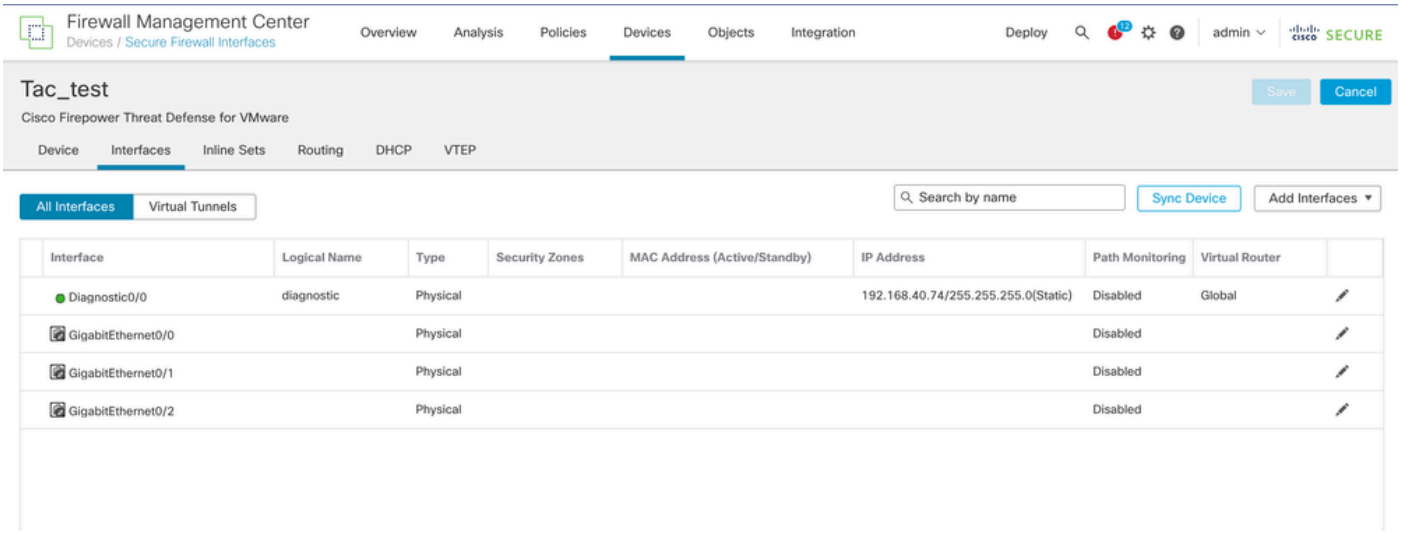
Nach dem Upgrade auf 7.4.2 ist die Konvergenz erforderlich, so ist die Konfiguration in der FMC UI, FTD CLI Lina und Linux, vor und nach dem Merge.

Außerdem gibt es Datenerfassungen auf FTD CLI Lina und Linux, um den Datenverkehr mithilfe der logischen Diagnoseschnittstelle zur Verwendung der Management-Schnittstelle anzuzeigen.

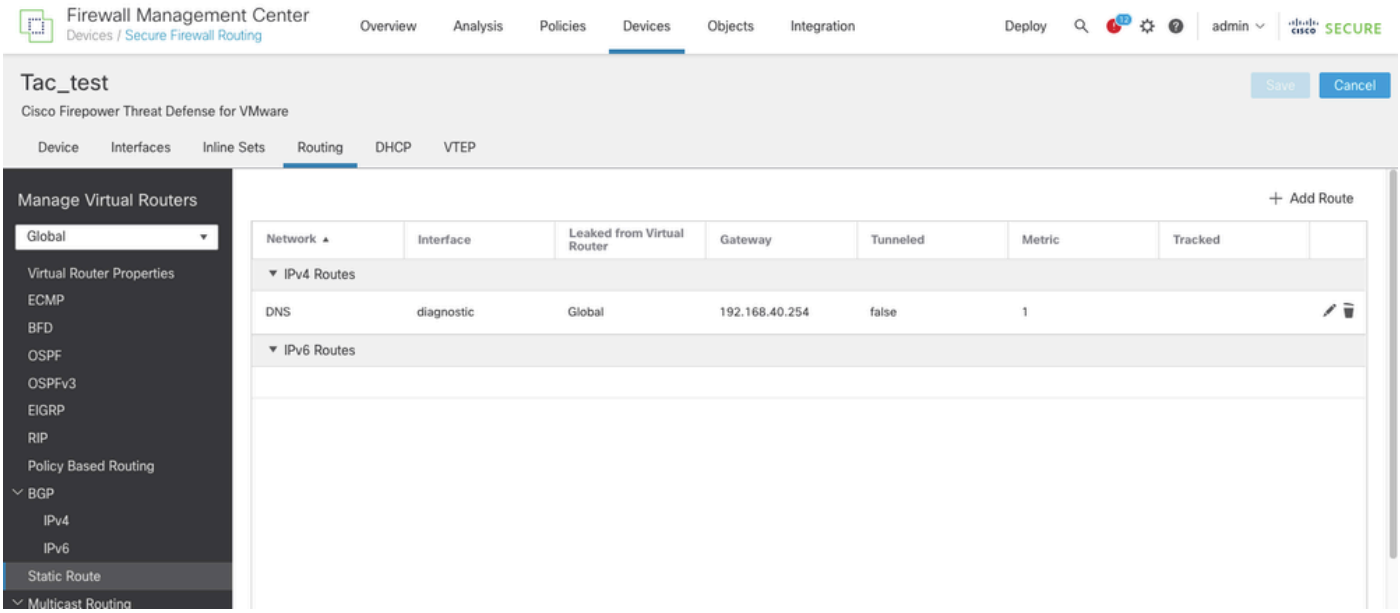
Vor der Konvergenzkonfiguration

Die Diagnoseschnittstelle verfügt über eine separate IP und eine statische Route für die DNS-Suche. Auf diese Weise werden beide logischen Schnittstellen von Lina zu Linux in der FTD verwendet.

Konfiguration der FMC-Benutzeroberfläche



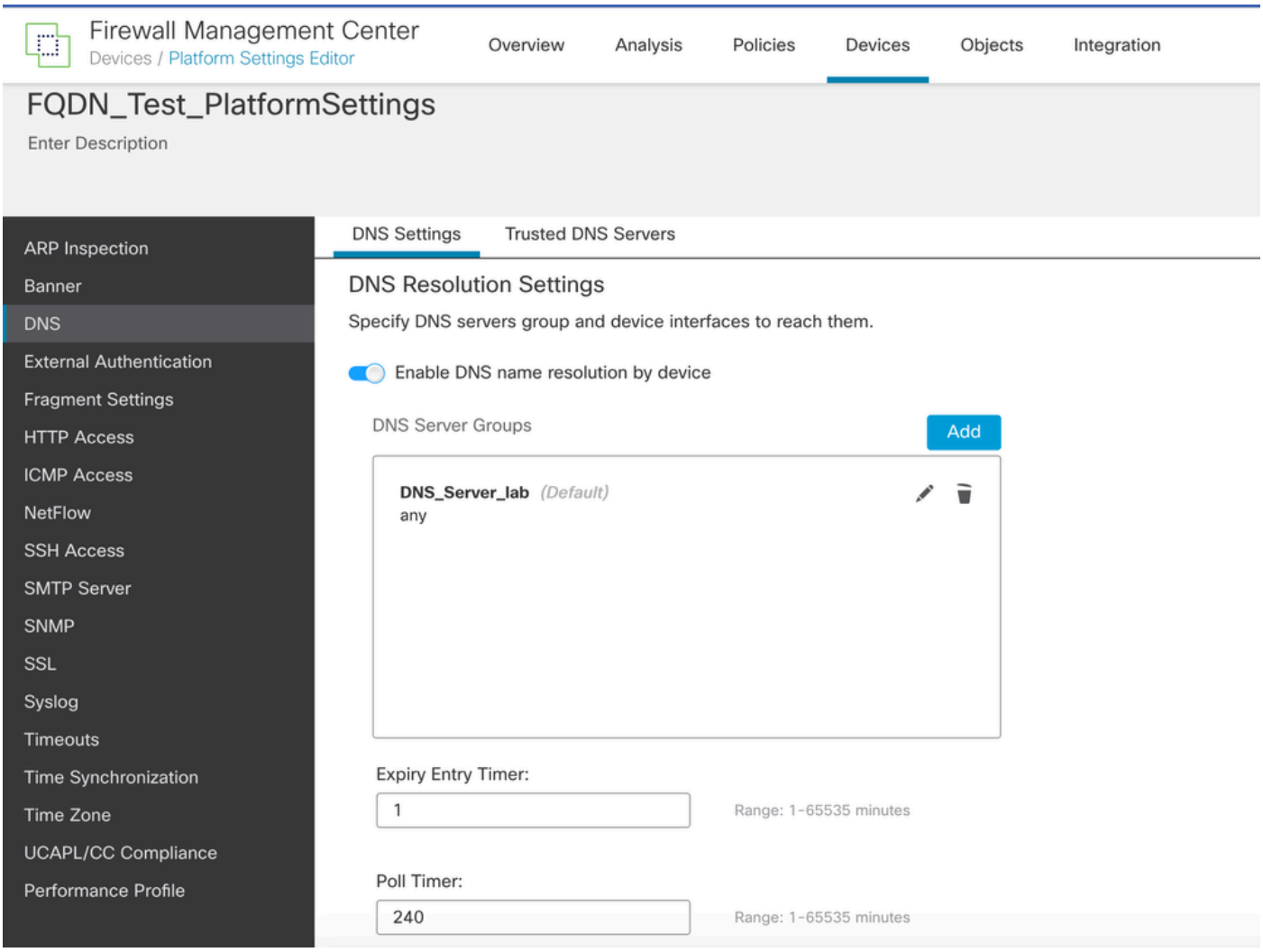
Konfiguration der Diagnoseschnittstelle vor dem Zusammenführen



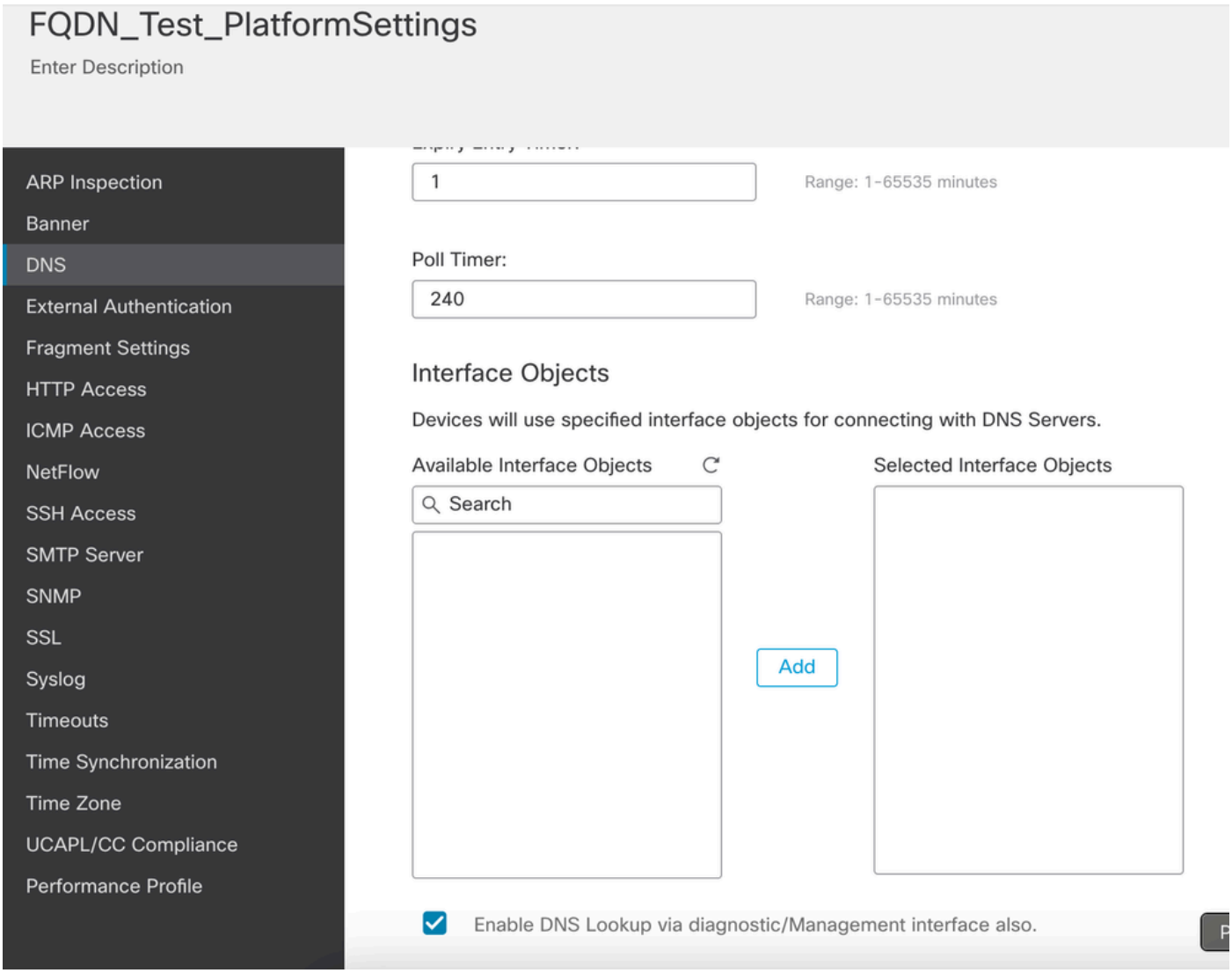
Statische Route auf Diagnoseschnittstelle konfiguriert

DNS-Konfiguration über

Devices (Geräte) > Platform Settings (Plattformeinstellungen): Wählen Sie die Richtlinie und anschließend die Registerkarte DNS aus.



DNS-Konfiguration in Plattformeinstellungen



Kontrollkästchen aktiviert für DNS-Suche über Diagnose-/Management-Schnittstelle aktivieren

Konfiguration der Diagnoseschnittstelle über 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
```

DNS-Konfiguration auf 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
```

Erfassung des DNS-Datenverkehrs zum DNS-Server über die Diagnoseschnittstelle 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#
```

Erfassung im Expertenmodus von Linux, um den korrekten Fluss des DNS-Lookup-Verkehrs von der Diagnoseschnittstelle über die Management-Schnittstelle zu bestätigen

```
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)
```

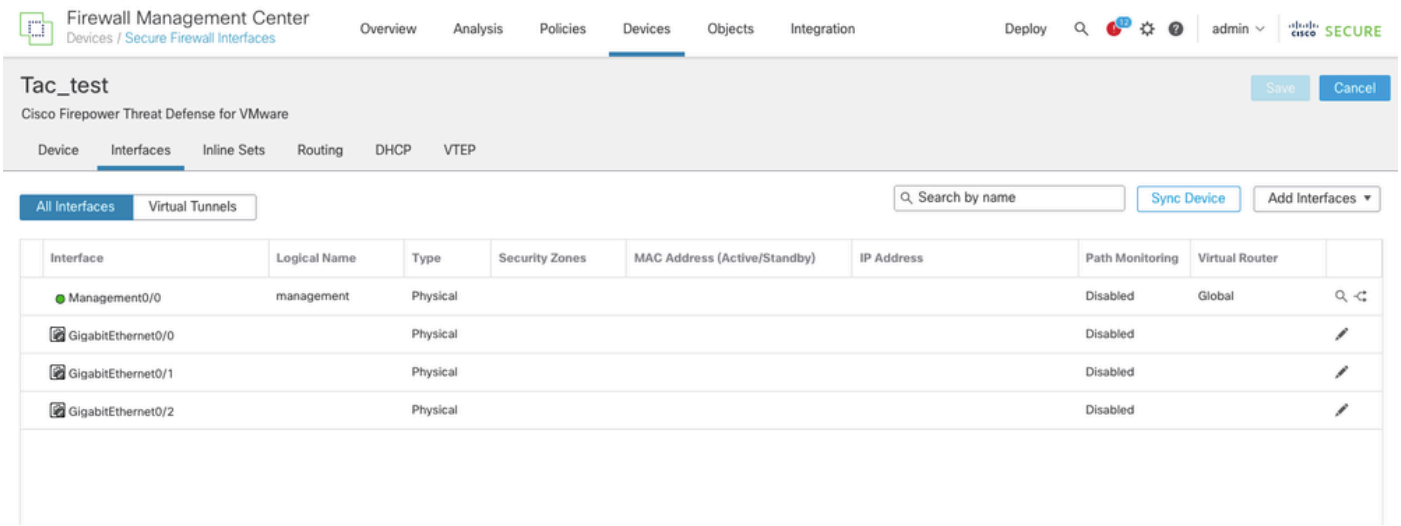
Nach Konfiguration der Konvergenz

Wie beim Konvergenzverfahren erwähnt, müssen zum Zusammenführen alle Konfigurationen auf der Diagnoseschnittstelle entfernt werden.

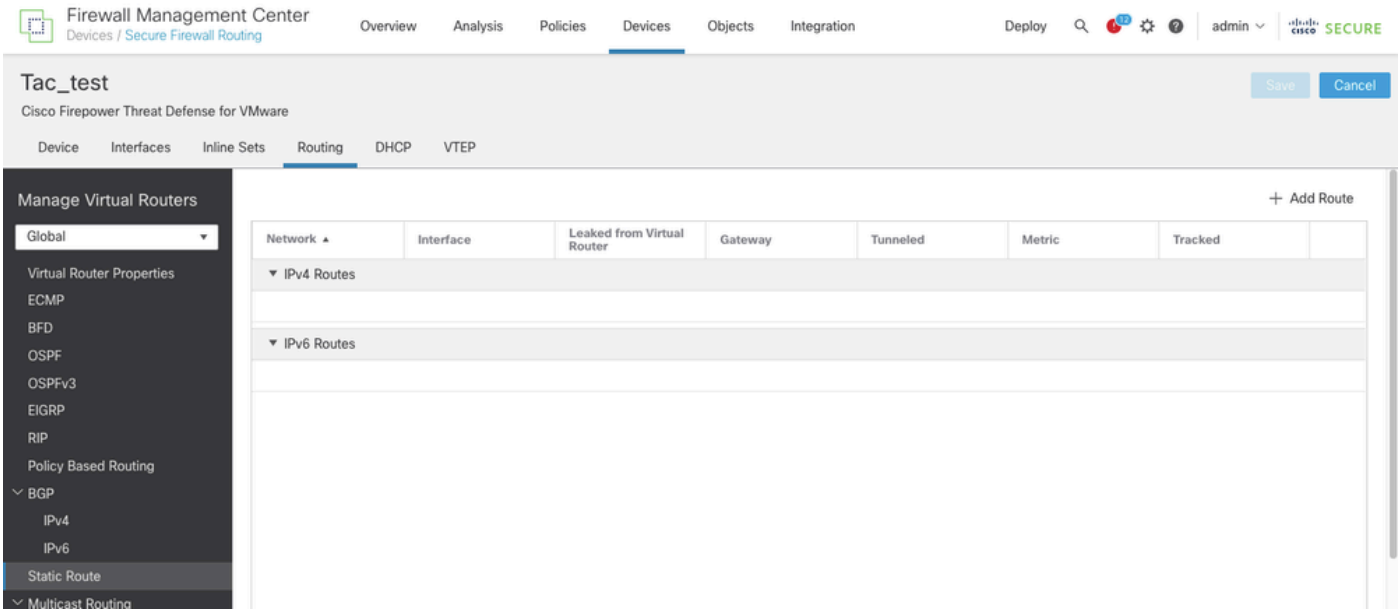
Dies sind die Informationen über FMC und FTD CLI nach Abschluss der Zusammenführung.

Konfiguration der Management-Schnittstelle über die FMC-Benutzeroberfläche

Geräte > Gerätemanagement, wählen Sie das FTD aus. Es wird direkt zur Registerkarte Schnittstellen geöffnet.



Verwaltungsschnittstelle nach dem Zusammenführen

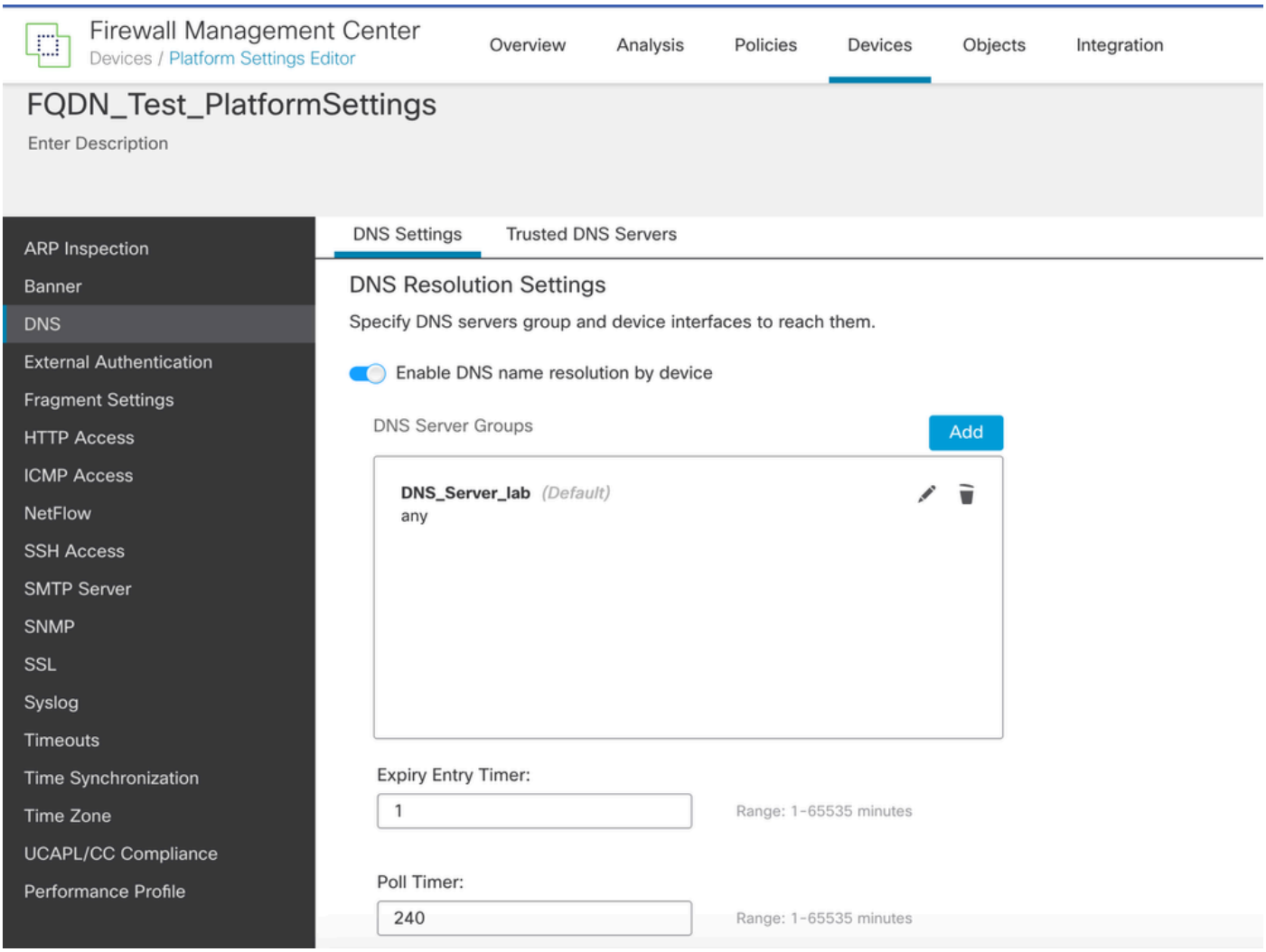


Es werden keine statischen Routen zum DNS-Server hinzugefügt.

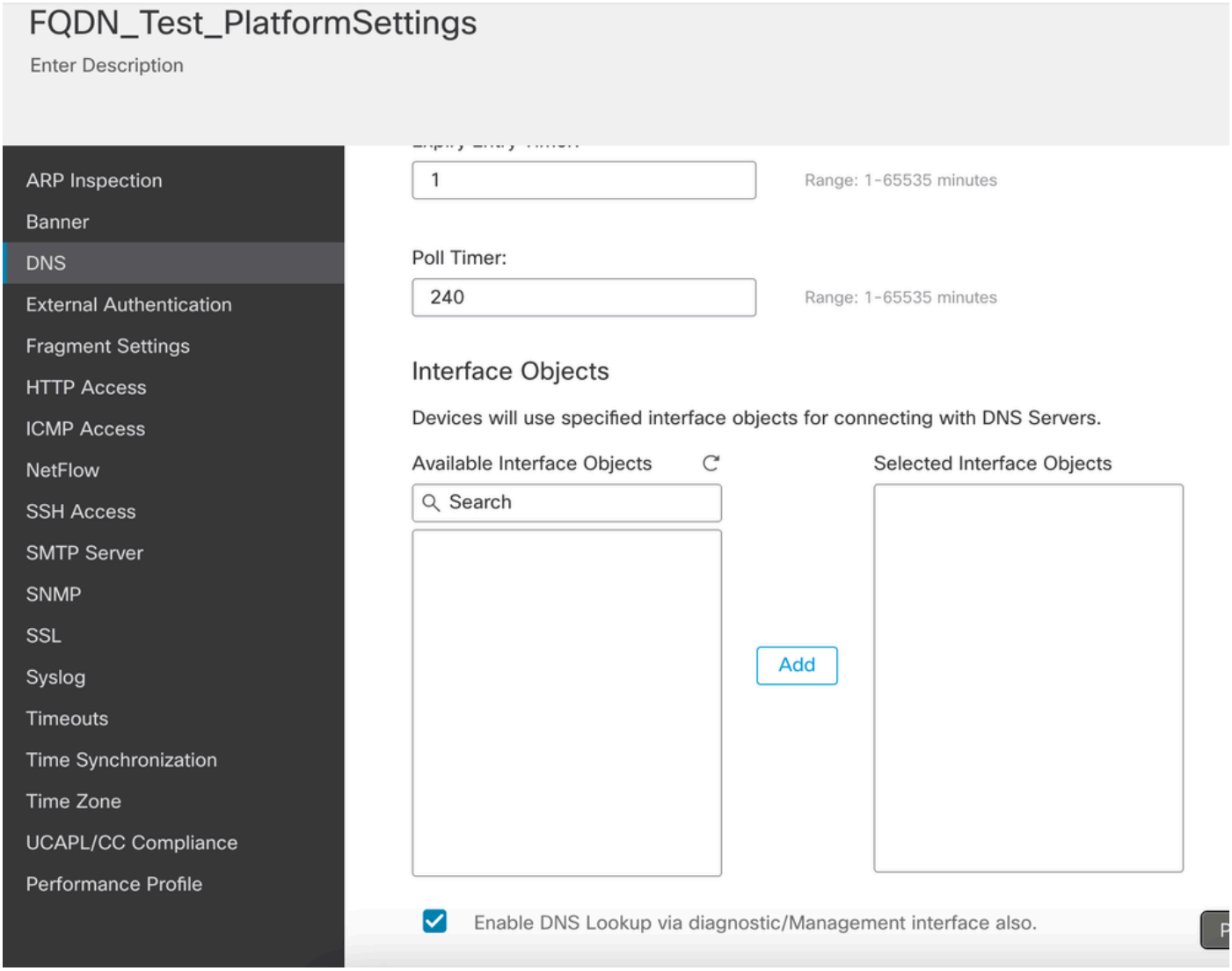
Die DNS-Konfiguration muss in den Plattformeinstellungen unverändert bleiben.

Devices (Geräte) > Platform Settings (Plattformeinstellungen): Wählen Sie die Richtlinie und anschließend die Registerkarte DNS aus.

Damit die DNS-Suche weiterhin an die Verwaltungsschnittstelle gesendet wird, ohne dass eine statische Route hinzugefügt werden muss, muss "DNS-Suche über die Diagnose-/Verwaltungsschnittstelle aktivieren" angegeben werden. muss ausgewählt bleiben.



DNS-Konfiguration auf Plattformeinstellungen



Die Option zum Aktivieren der DNS-Suche über die Diagnose-/Management-Schnittstelle muss ebenfalls unverändert bleiben.

Konfiguration auf der FTD-CLI

```
> 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
```

DNS-Konfiguration auf FTD CLI auf LINA-Seite

```
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
```

Erfassung im Linux Expertenmodus, um den korrekten Fluss des DNS-Lookup-Verkehrs auf der Management-Schnittstelle zu bestätigen.

```
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)
```

Mit diesem Nachweis kann bestätigt werden, dass die DNS-Suche auch dann weiter funktioniert, wenn der Management-Schnittstelle unter Linux keine statische Route hinzugefügt wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.