在FMC中配置管理和诊断接口的合并

目录

简介

先决条件

背景信息

- 使用的组件

配置

- FTD内部架构图
- 收敛过程

验证

故障排除 — 研究案例

- 融合配置之前
- 融合配置后

简介

本文档介绍配置FTD 7.4.0版本中添加的管理接口和诊断接口合并功能的步骤。

先决条件

思科建议您了解以下主题：

- 思科安全防火墙威胁防御(FTD)
- 思科安全防火墙管理器中心(FMC)

背景信息

在7.3版及更早版本中，物理管理接口在诊断逻辑接口(Lina)和管理逻辑接口(Linux)之间共享。

在7.4版及更高版本中，诊断界面与管理相合并，从而简化用户体验。
对于使用7.4及更高版本的新设备，不能使用传统诊断界面。只有合并的管理界面可用。

使用的组件

本文档中的信息基于以下软件和硬件版本：

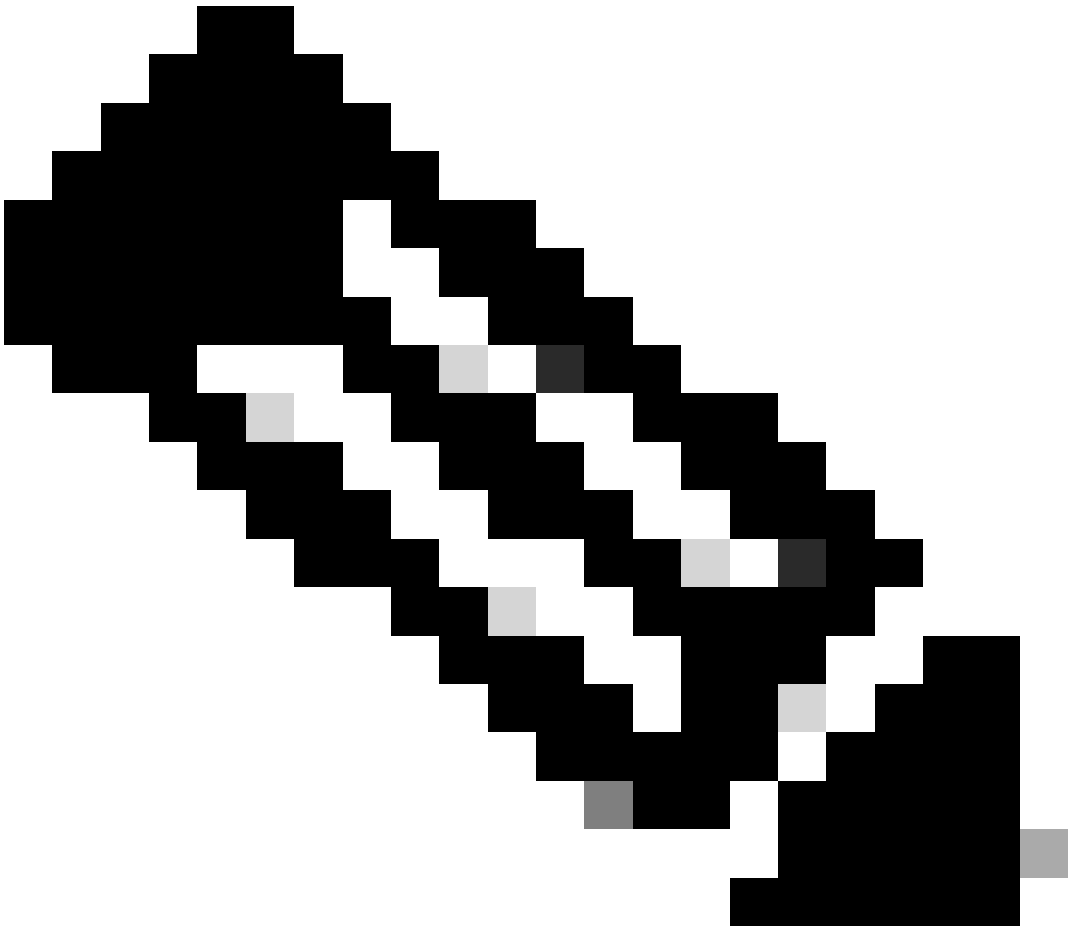
- 虚拟思科安全防火墙威胁防御(FTD)，版本7.4.2
- 虚拟思科安全防火墙管理器中心(FMC)，版本7.4.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

如果升级到7.4或更高版本，并且已配置诊断接口，则可以选择手动合并接口，也可以继续使用单独的诊断接口。

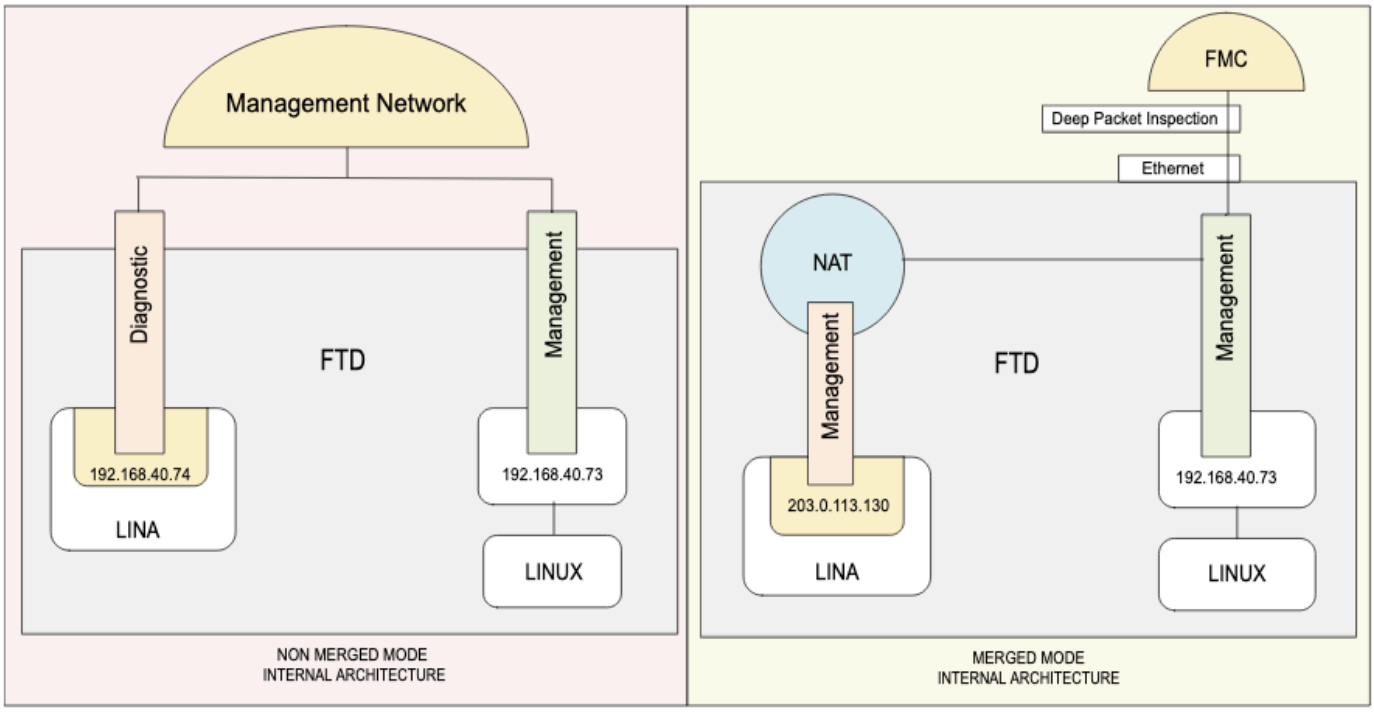
如果诊断接口没有任何配置，则接口合并会自动完成。



注意：将在后续版本中取消对诊断接口的支持，因此请尽快合并接口。

FTD内部架构图

融合管理接口概述



融合管理界面前后内部架构概述

在左侧，诊断逻辑接口(Lina)和管理逻辑接口(Linux)的内部架构。 7.3及更低版本。

在右侧，是单个管理接口的内部架构。Lina对管理网络的访问使用NAT服务。

收敛过程

如果诊断接口中存在配置，升级后不会自动合并接口，您需要执行收敛过程。

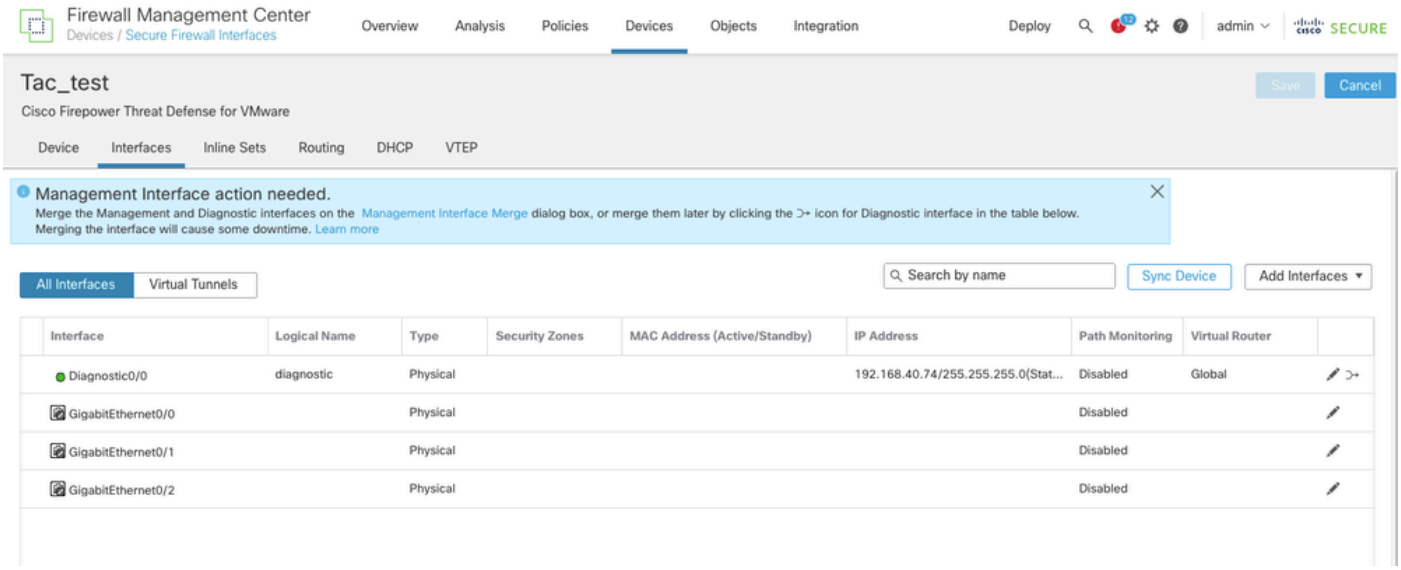
此过程要求您确认配置更改，在某些情况下，需要手动修复配置。

要查看设备的当前模式，请在FTD CLI屏幕中输入show management-interface converge命令

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

该结果显示管理接口未合并。

步骤1:
在FMC UI上，导航到Devices > Device Management，然后选择要编辑的FTD。它会直接打开到Interfaces选项卡。

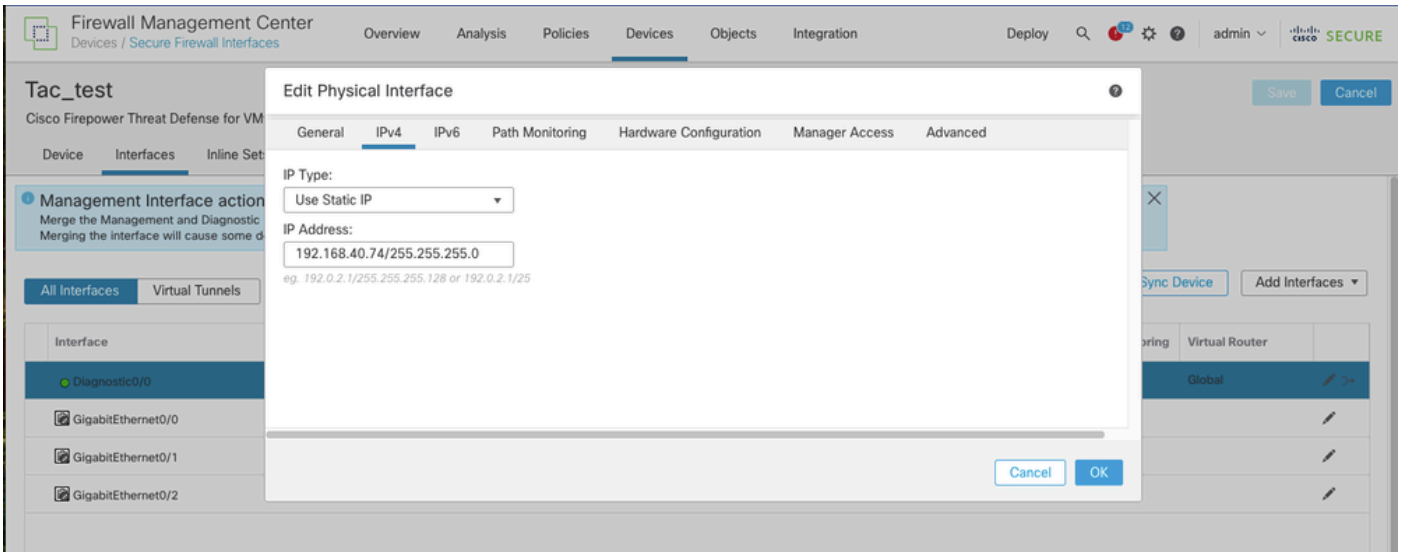


设备升级到软件版本7.4.2后合并诊断和管理接口所需的操作

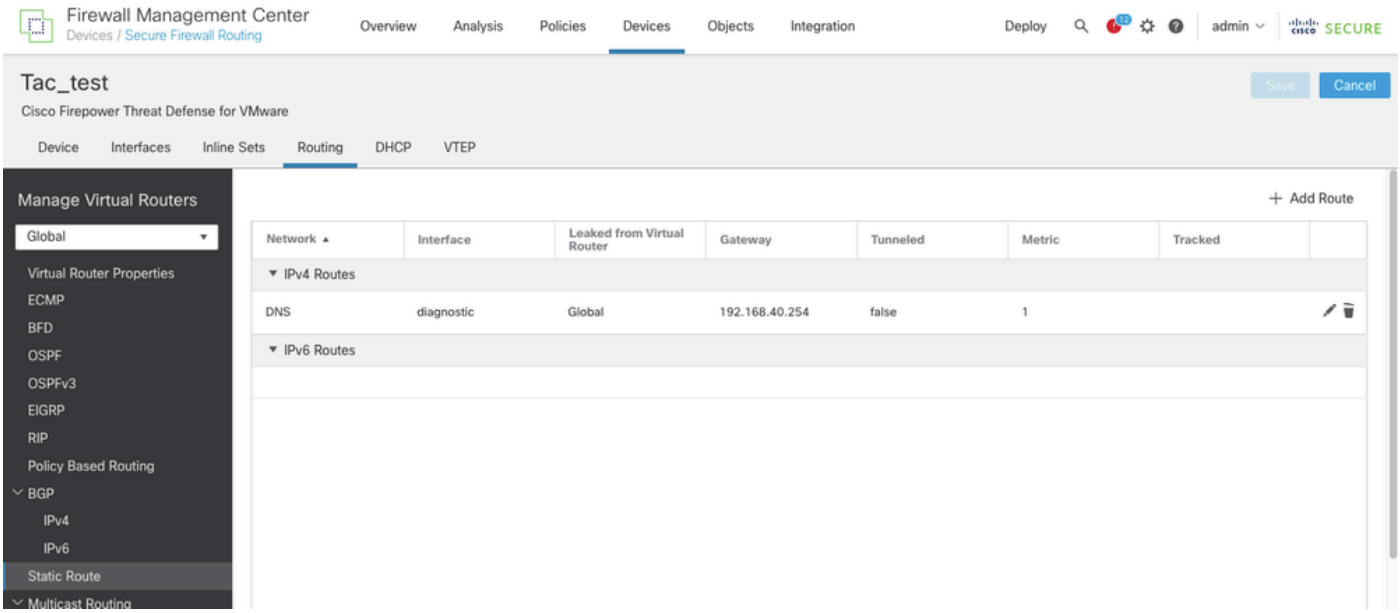
Step 2.

删除诊断接口上的所有配置。诊断接口必须没有任何配置才能继续合并。

例如，在此诊断界面中，有：IP地址和静态路由。



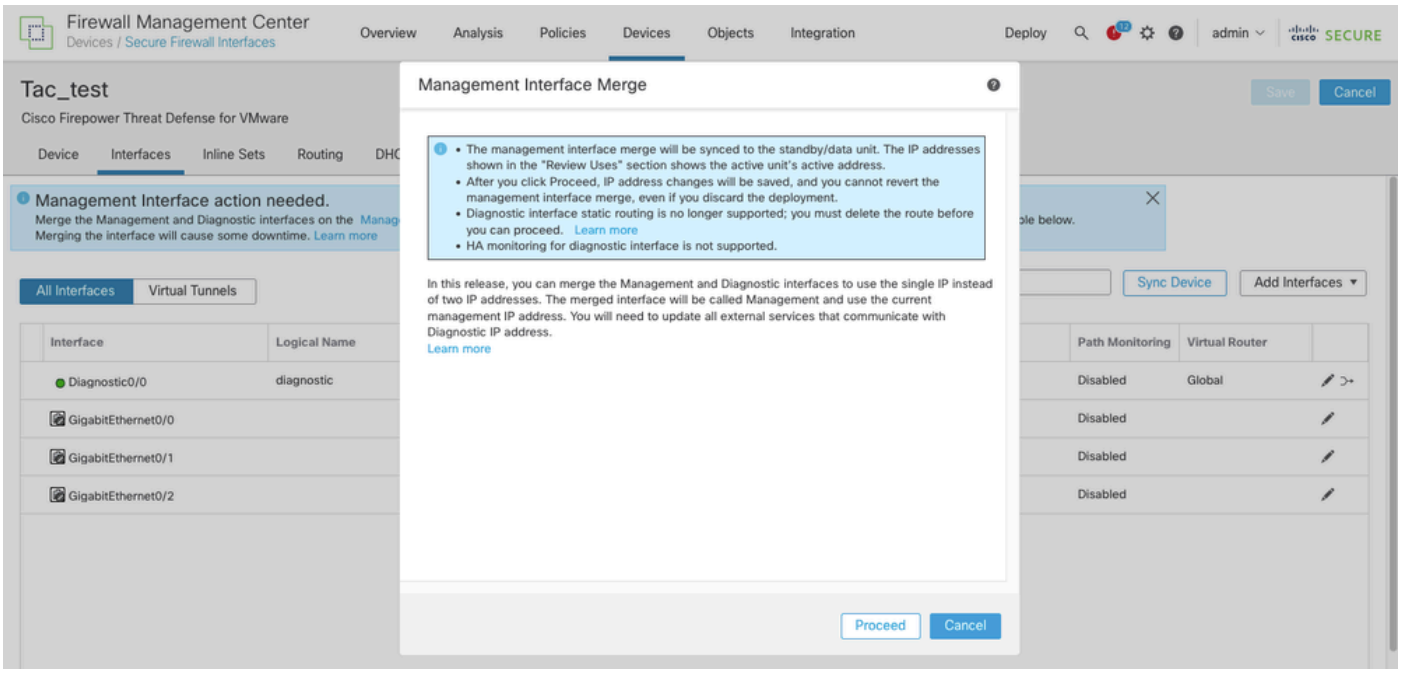
删除诊断接口IP地址



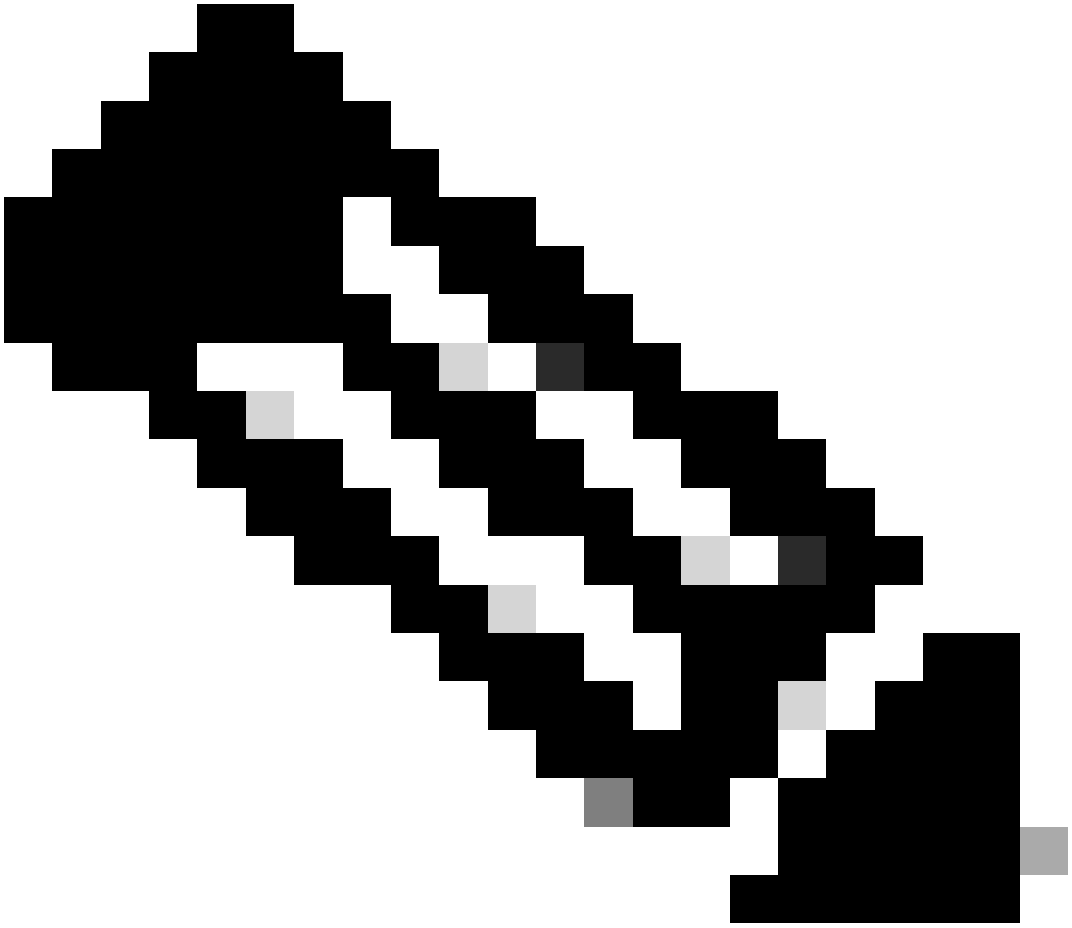
在诊断接口上配置静态路由

第 3 步：

单击Management Interface Merge action needed区域，或点击Diagnostic接口上Edit图标（铅笔）旁边的Merge图标。

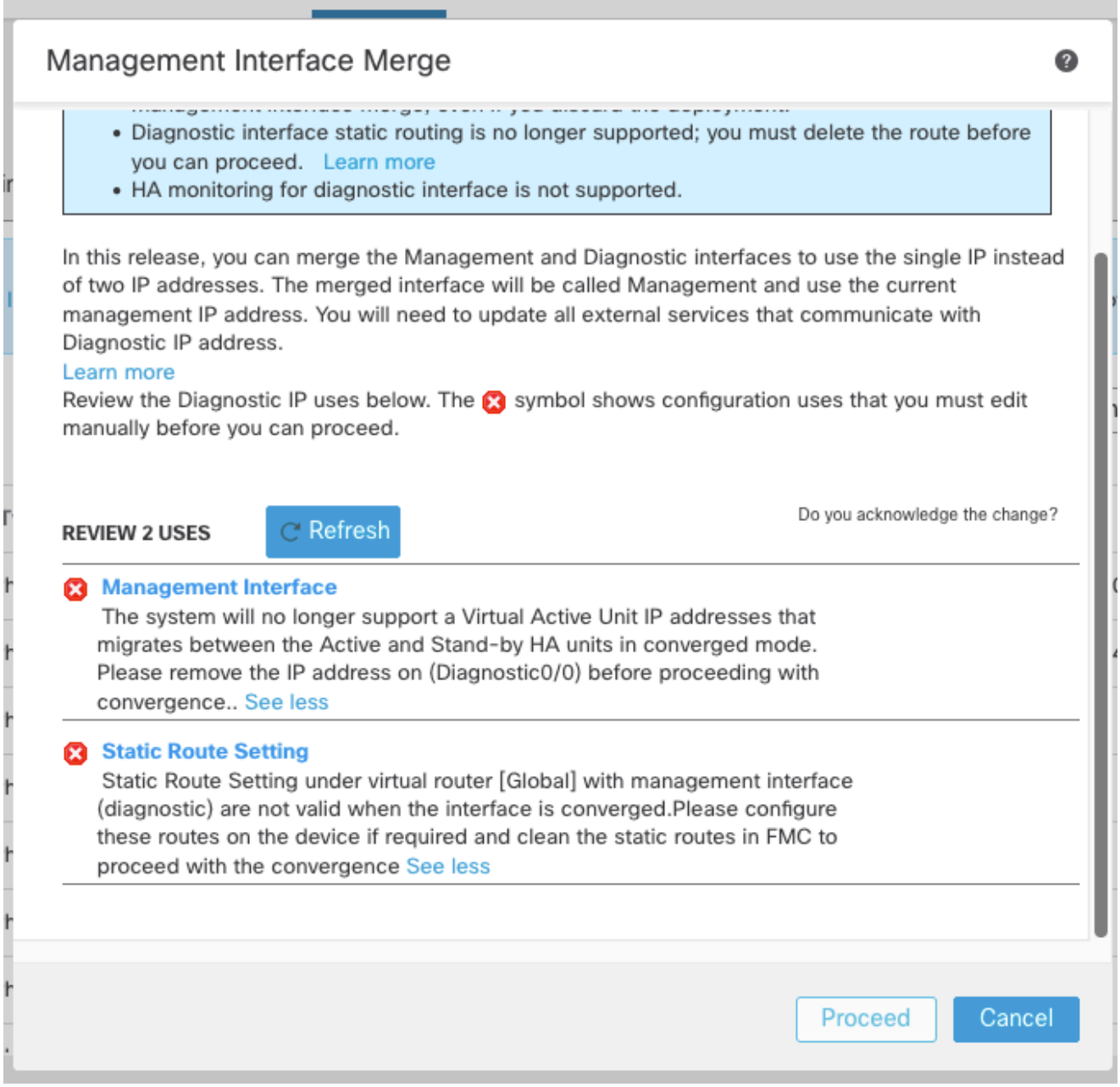


管理接口合并信息，然后继续



注意：对于高可用性对和集群，请在主用/控制单元上执行此任务。合并的配置会自动复制到备用/数据单元。

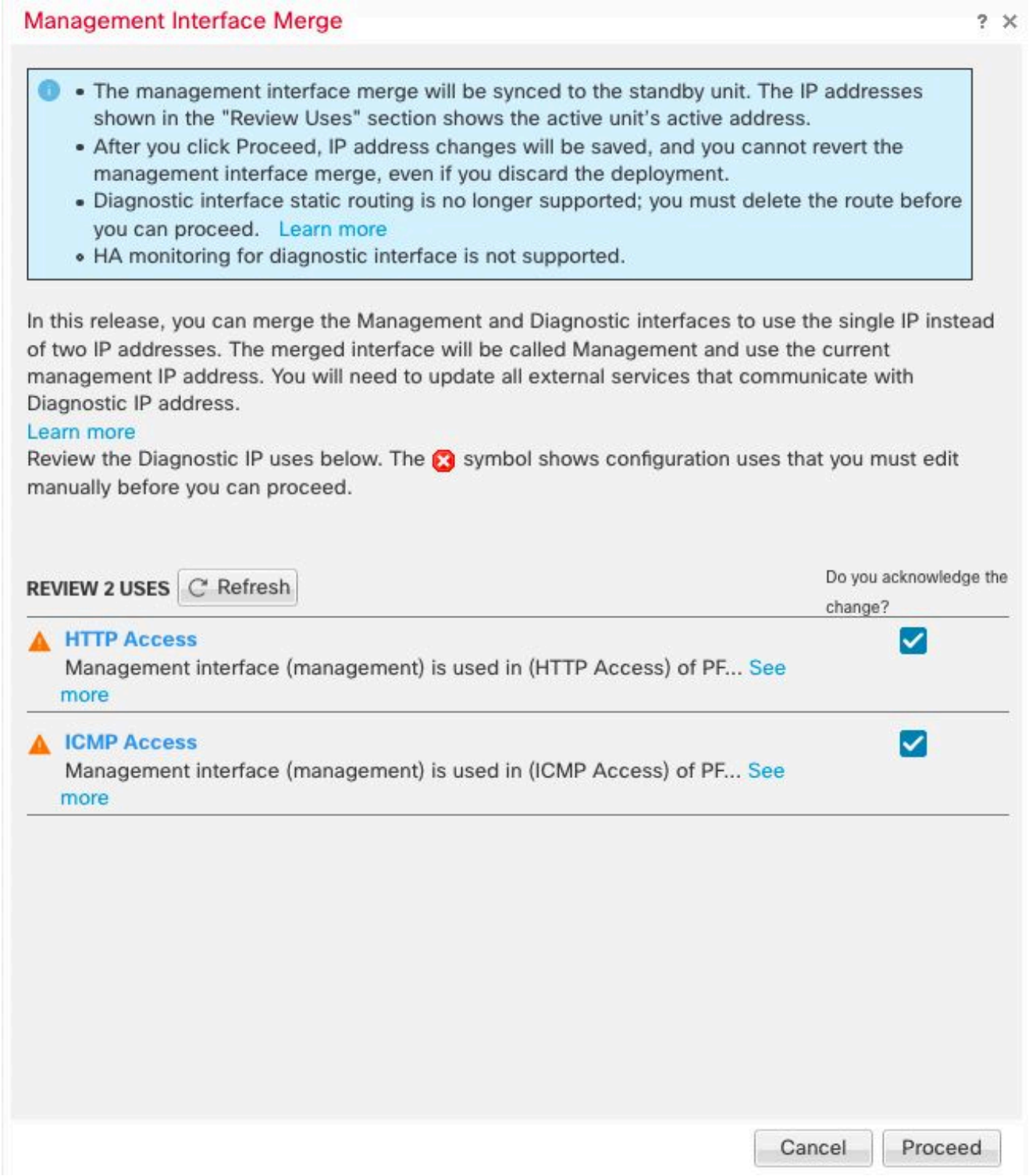
- 对于需要手动更改或移除的任何事件，都可能会出现警告图标。



合并前需要删除的配置警告示例

如果情况如此：取消对话框，继续删除配置或重新配置，然后重新打开Management Interface Merge对话框。

- 将在设备上运行的平台设置标有警告图标并要求确认。



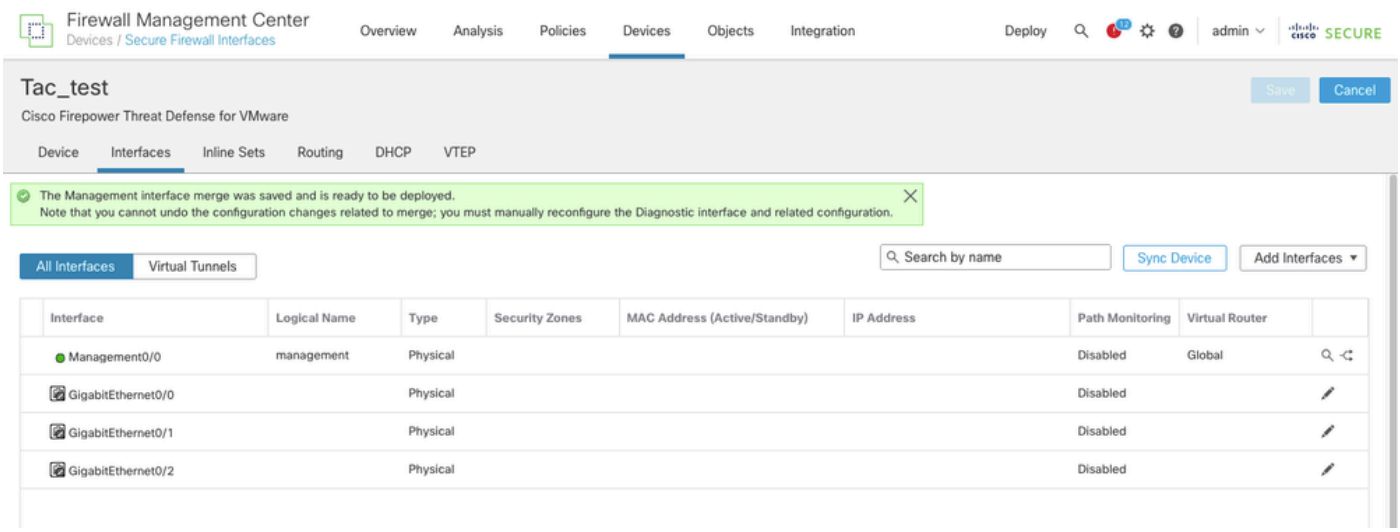
必须编辑的平台设置配置警告示例

- 单击Do you acknowledge the change中的框。列，然后单击继续。

第 4 步：

合并配置后，将显示成功标语：
“管理接口合并已保存并准备部署。
请注意，无法撤消与合并相关的配置更改；您必须手动重新配置诊断接口和相关配置。"

部署新的合并配置。



管理接口合并已保存并准备部署

管理接口显示在Interfaces页面上，但它是只读的。

部署后，管理接口上的收敛过程完成。

步骤5.可选

如果您有任何外部服务与诊断接口通信，则需要更改其配置以使用管理接口IP地址，因为在融合模式下已删除管理路由回退。

例如：

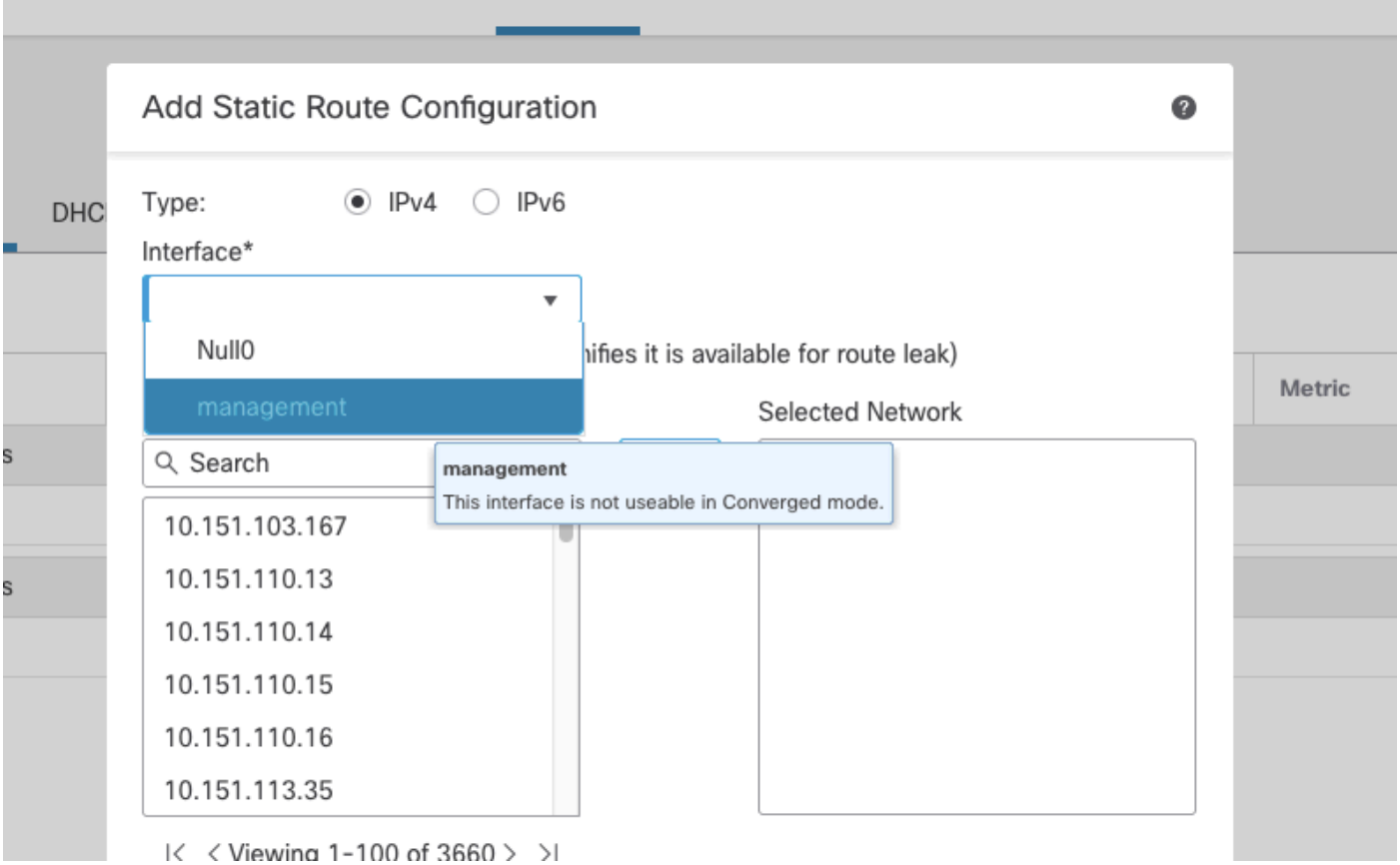
- SNMP客户端
- RADIUS 服务器
- 要通过管理网络访问DNS服务器，用户必须明确选择“Enable DNS Lookup via diagnostic/Management Interface also”。 在Platform Settings > DNS configuration上，DNS查找和ICMP（ping和traceroute）设置为例外：在这些情况下，threat defense使用数据，如果没有找到路由，则自动回退到管理层。

管理接口使用静态路由只能通过FTD CLI类(Linux)配置

Lina管理端口默认路由将所有帧发送到Linux模块。

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

在FMC UI上，管理界面灰显以供选择。



合并完成后，管理接口不可用于静态路由选择。

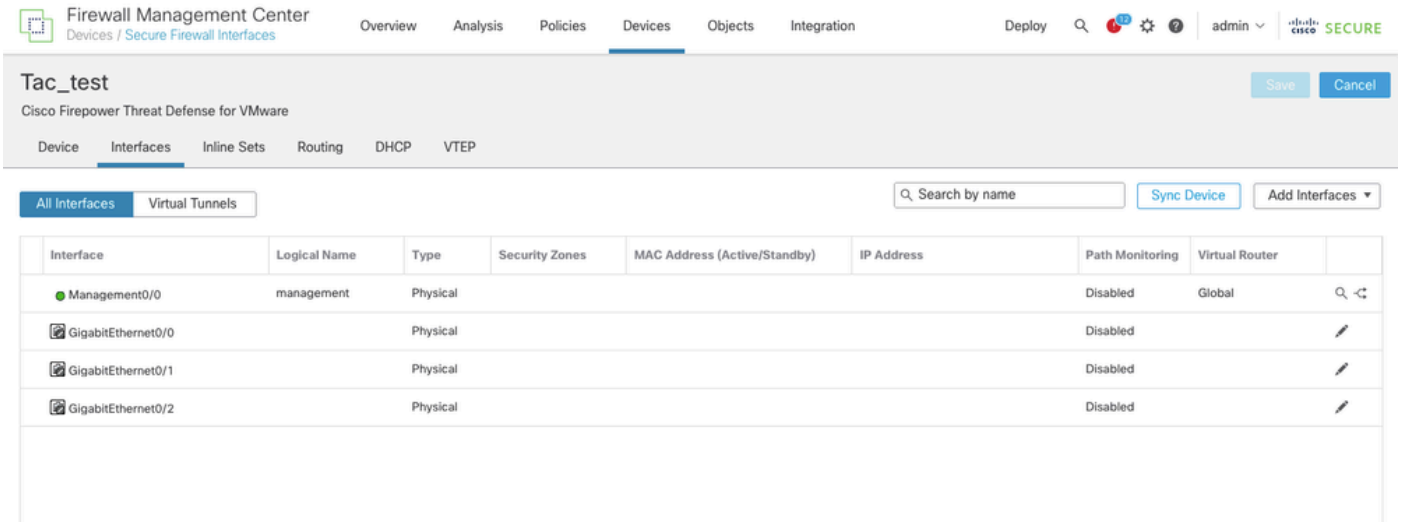
验证

在管理接口上合并后预期的更改

- 通过执行命令检验FTD CLI的收敛模式关闭

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

- 在FMC UI上，接口名称更改为Management0/0 ，逻辑名称更改为management。



管理接口名称和逻辑名称合并确认

- 在FTD CLI Clish中，新的IP地址在Lina上自动配置用于管理接口。
  NAT用作内部实施：分配的内部私有IPv4地址203.0.113.130和IPv6地址fd00:0:1:1::2是内部私有IPv4地址（两者可能更改）。
  这些IP通过NAT转换到公共Linux内核FTD IPv4和IPv6地址，因此不再需要Lina上的公共IP。

  在专家模式下，“ifconfig”显示Linux的内部IPv4(203.0.113.129)和IPv6(fd00:0:1:1::1)地址。

```
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
```

故障排除 — 研究案例

在本研究案例中，在升级到7.4.2之前，虚拟FTD上的诊断接口已配置一个单独的IP地址，用于连接到DNS查找的外部服务。

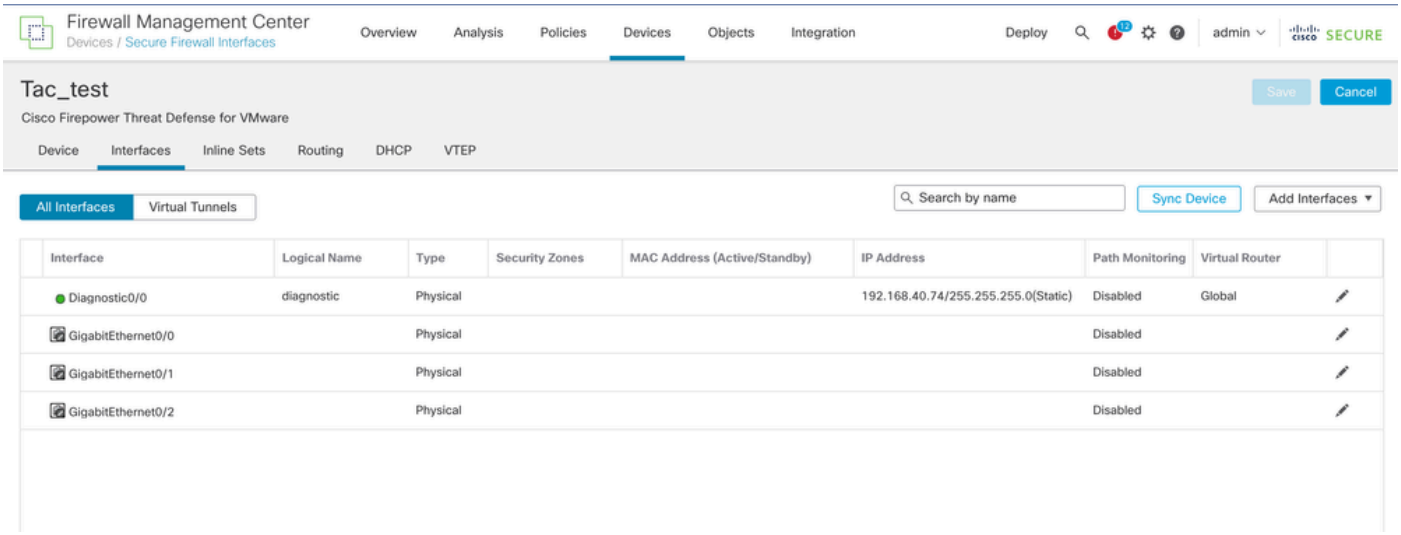
升级到7.4.2后，需要进行融合，这就是合并前后FMC UI、FTD CLI Lina和Linux中的配置方式。

FTD CLI Lina和Linux上也有流量捕获，用于显示使用逻辑诊断接口移动以使用管理接口的流量。

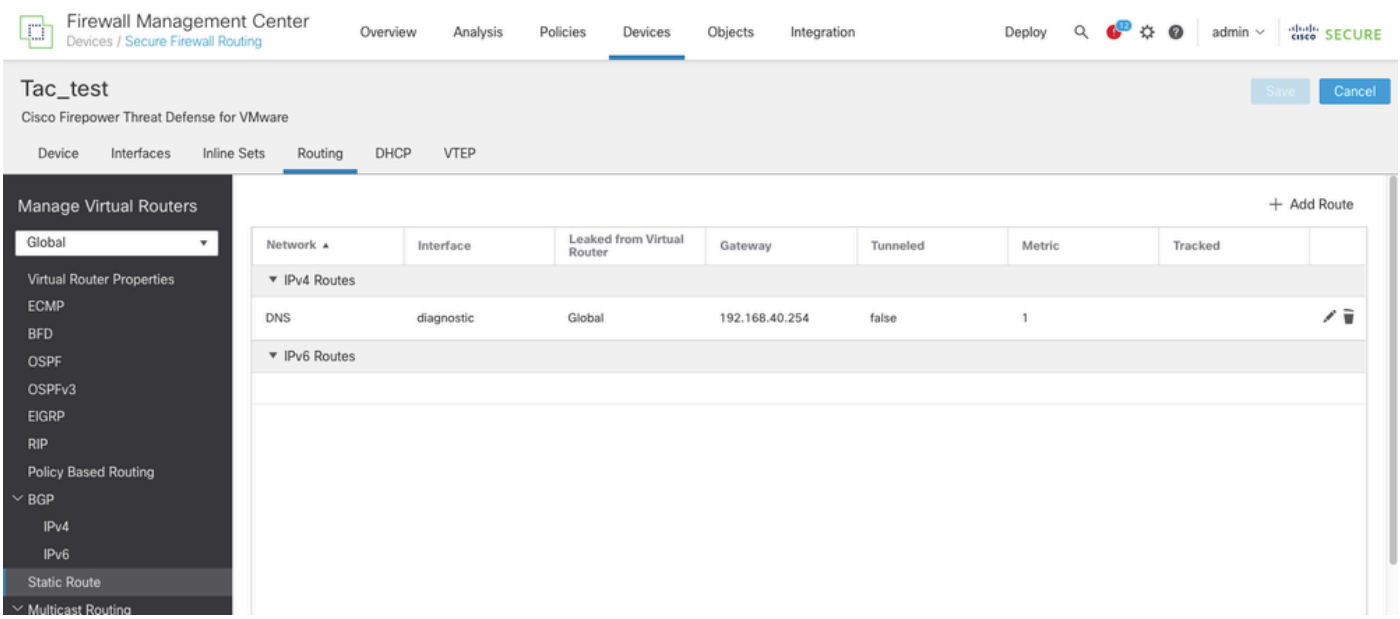
融合配置之前

诊断接口具有用于DNS查找的单独IP路由和静态路由，这样在FTD中可以使用从Lina到Linux的两个逻辑接口。

FMC UI配置



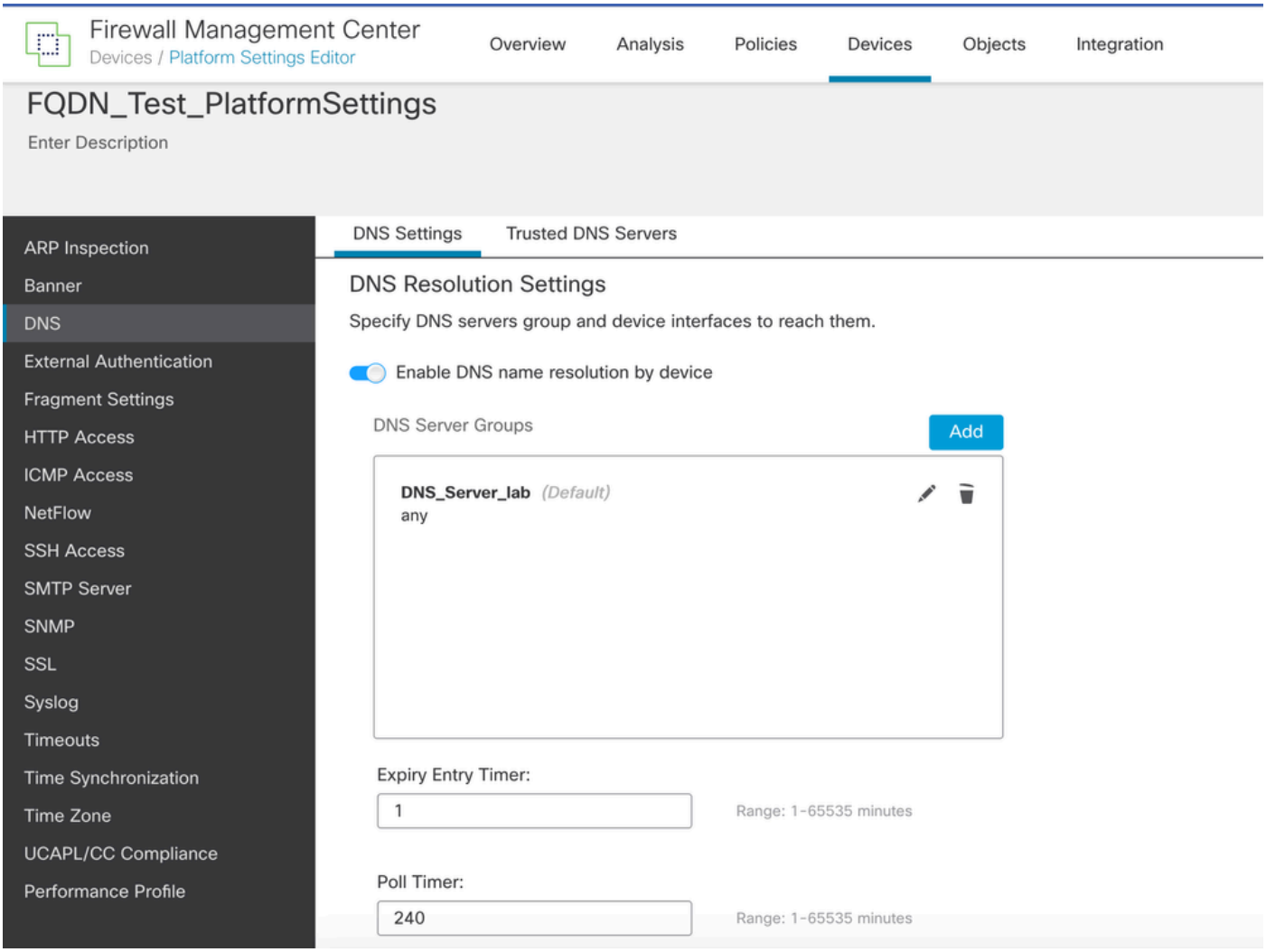
合并前的诊断接口配置



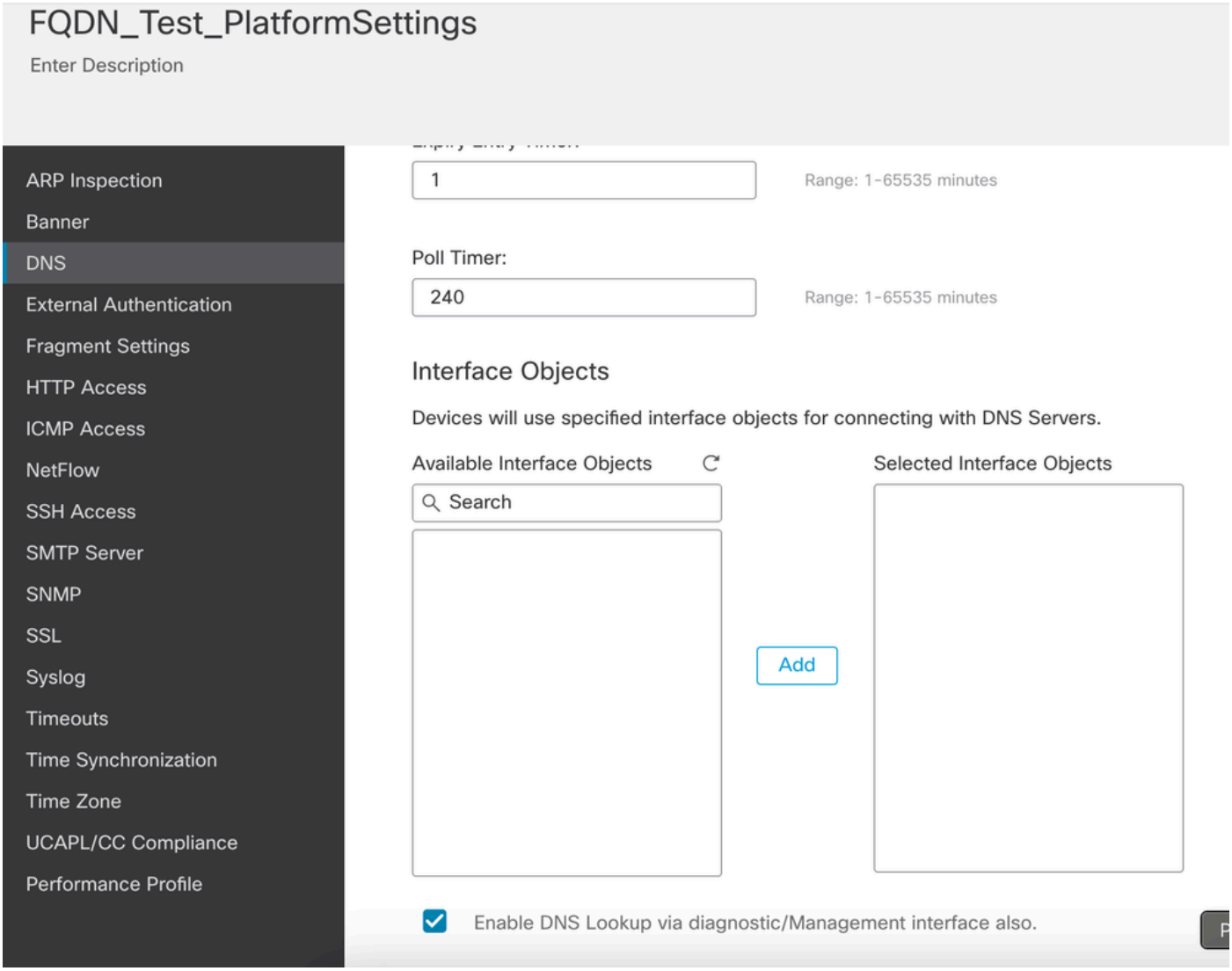
在诊断接口上配置的静态路由

DNS配置通过

Devices > Platform Settings，选择策略，然后选择DNS选项卡。



平台设置中的DNS配置



选中“通过诊断/管理界面启用DNS查找”复选框

FTD Lina上的诊断接口的配置

```
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
```

FTD CLI链路上的DNS配置

```
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
```

在诊断接口上捕获流向DNS服务器10.10.10.10的DNS流量

```
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#
```

在Linux expert模式下捕获，以确认管理接口上来自诊断接口的DNS查找流量的正确流

```
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)
```

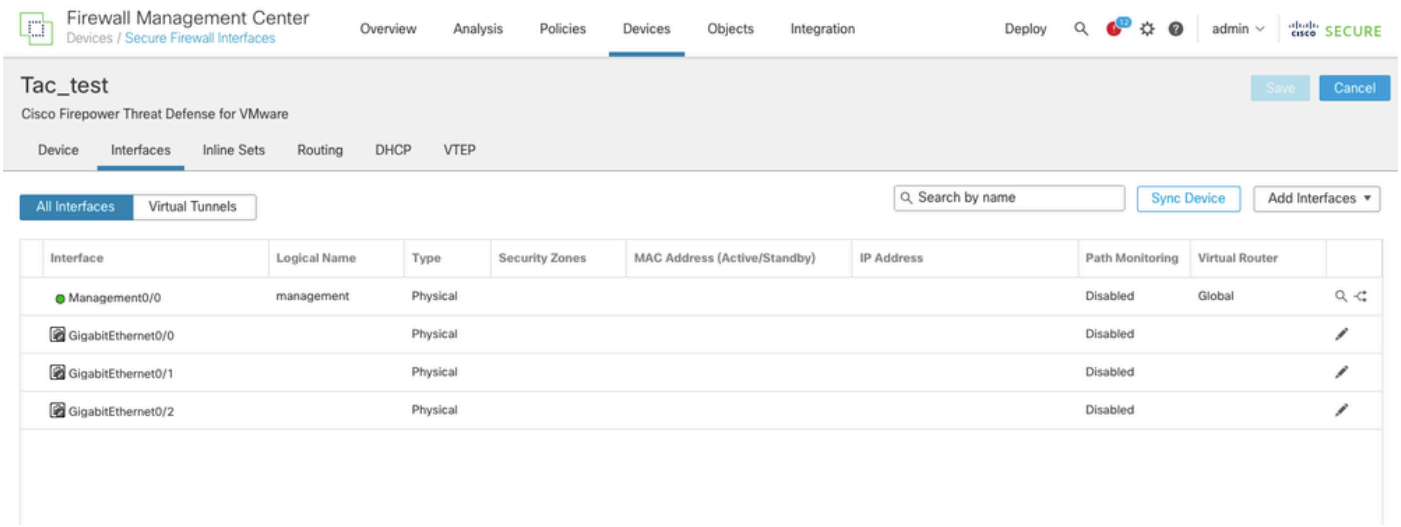
融合配置后

如融合过程所述，为了进行合并，必须删除诊断接口上的所有配置。

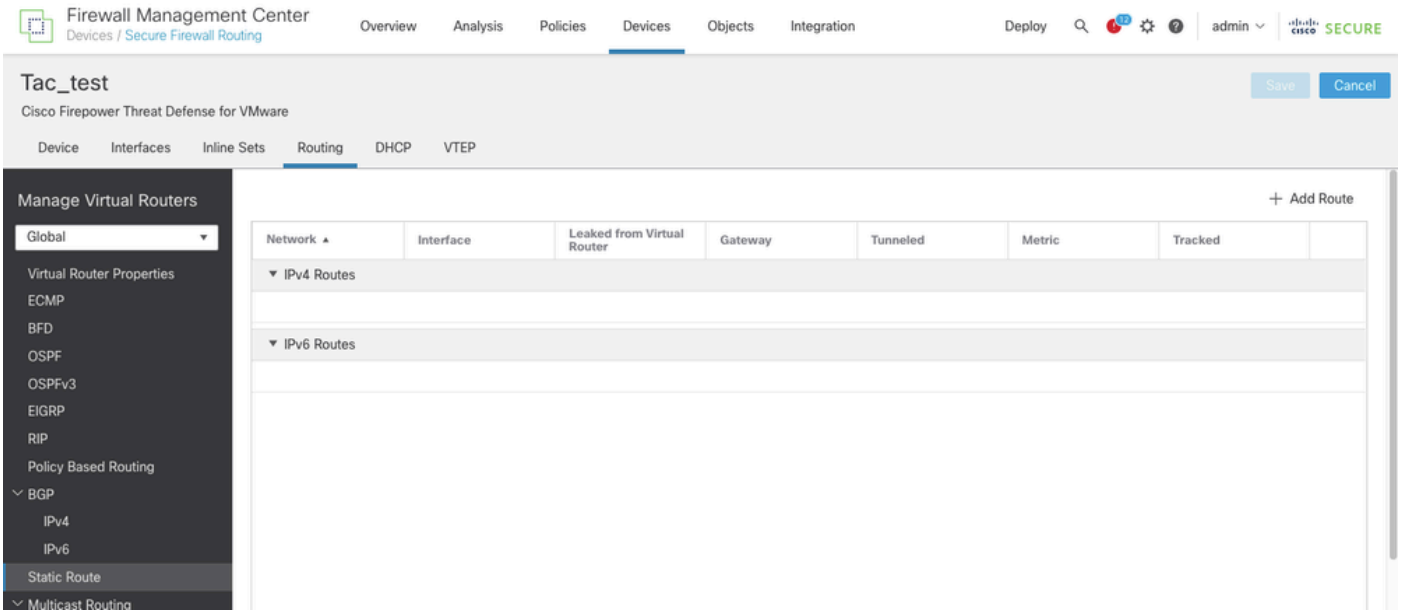
以下是合并完成后FMC和FTD CLI上的信息。

FMC UI上的管理接口配置

Devices > Device Management，选择FTD。它会直接打开到Interfaces选项卡。



合并后的管理接口

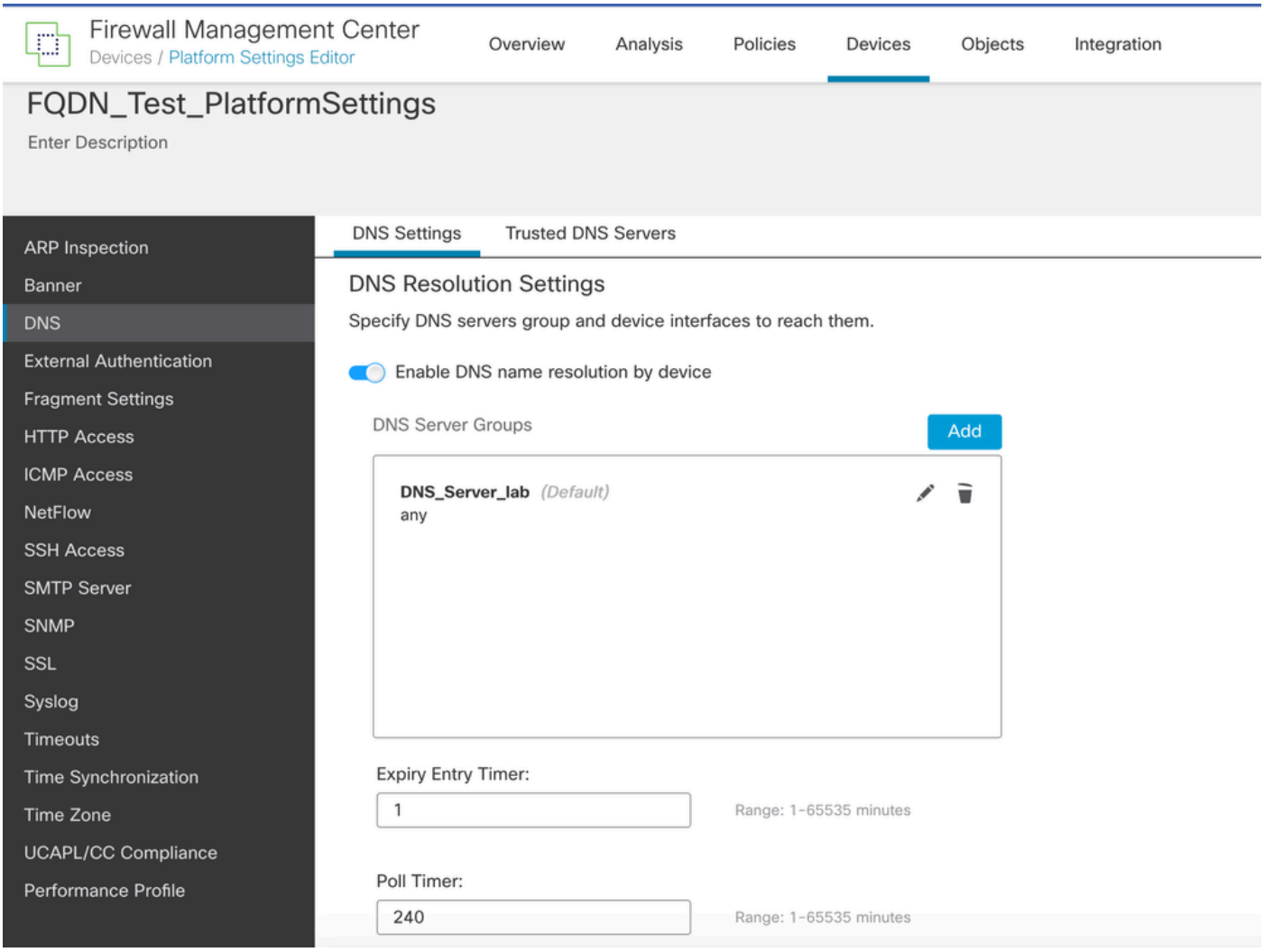


没有添加到DNS服务器的静态路由

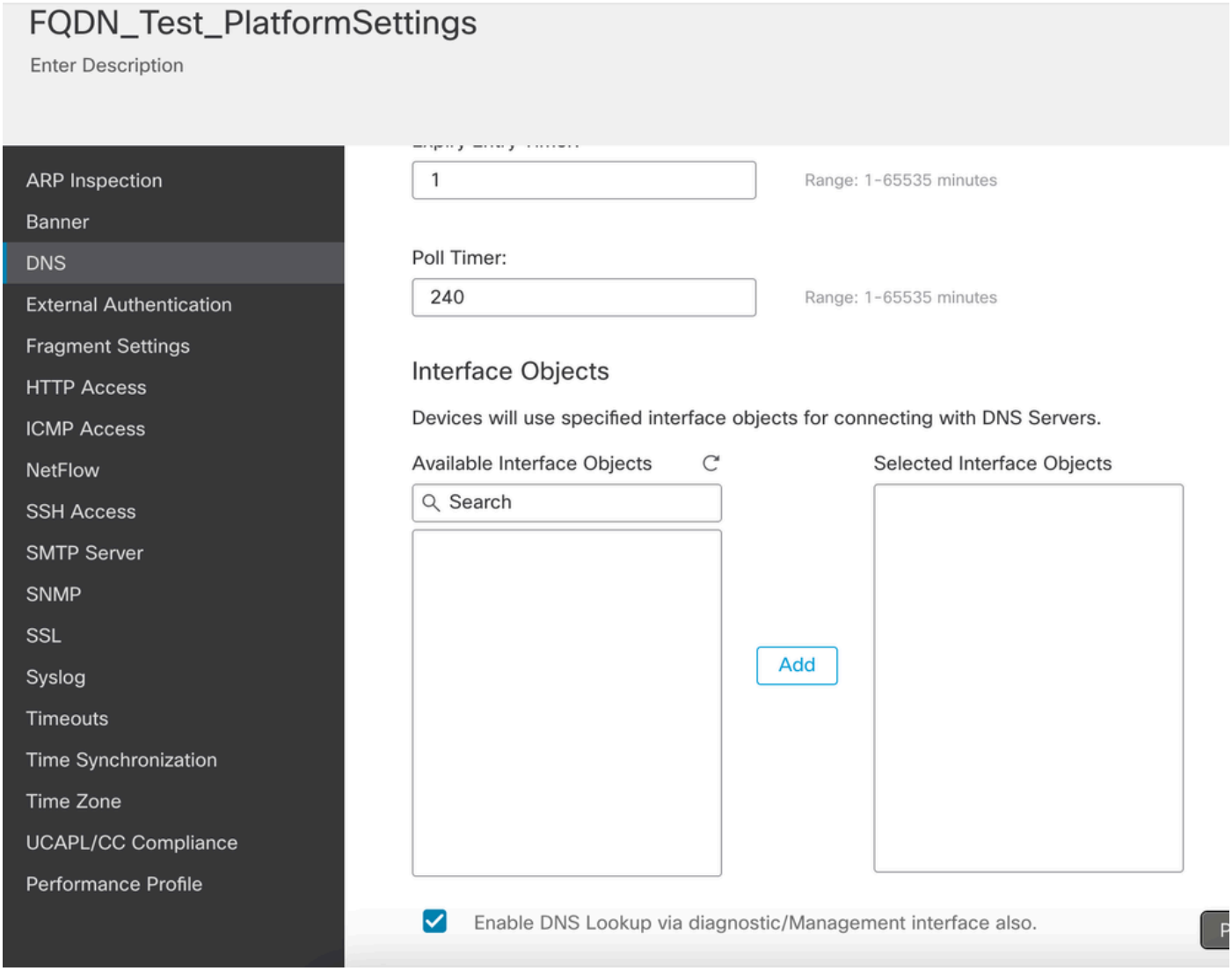
平台设置上的DNS配置必须保持不变。

Devices > Platform Settings，选择策略，然后选择DNS选项卡。

为了使DNS查找继续发送到管理接口，而无需添加静态路由，请输入“Enable DNS Lookup via diagnostic/Management interface also”。 必须保持选定状态。



平台设置上的DNS配置



通过诊断/管理接口启用DNS查找的选项也必须保持相同

FTD CLI上的配置

```
> 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
```

LINA端的FTD CLI上的DNS配置

```
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
```

在Linux expert模式下捕获，以确认DNS查找流量在管理接口上的正确流动。

```
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)
```

通过此证据，可以确认DNS查找继续工作，即使通过Linux在管理接口上未添加静态路由也是如此。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。