FMCでの管理インターフェイスと診断インターフェイスのマージの設定

内容

はじめに

このドキュメントでは、FTD 7.4.0バージョンリリースで追加された機能である管理インターフェイスと診断インターフェイスのマージを設定する手順について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

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

背景説明

バージョン7.3以前では、物理管理インターフェイスは診断論理インターフェイス(Lina)と管理論理インターフェイス(Linux)の間で共有されます。

バージョン7.4以降では、ユーザエクスペリエンスを簡素化するために、診断インターフェイスが管理と統合されています。
7.4以降を使用する新しいデバイスでは、レガシー診断インターフェイスを使用できません。マージされた管理インターフェイスだけが使用できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

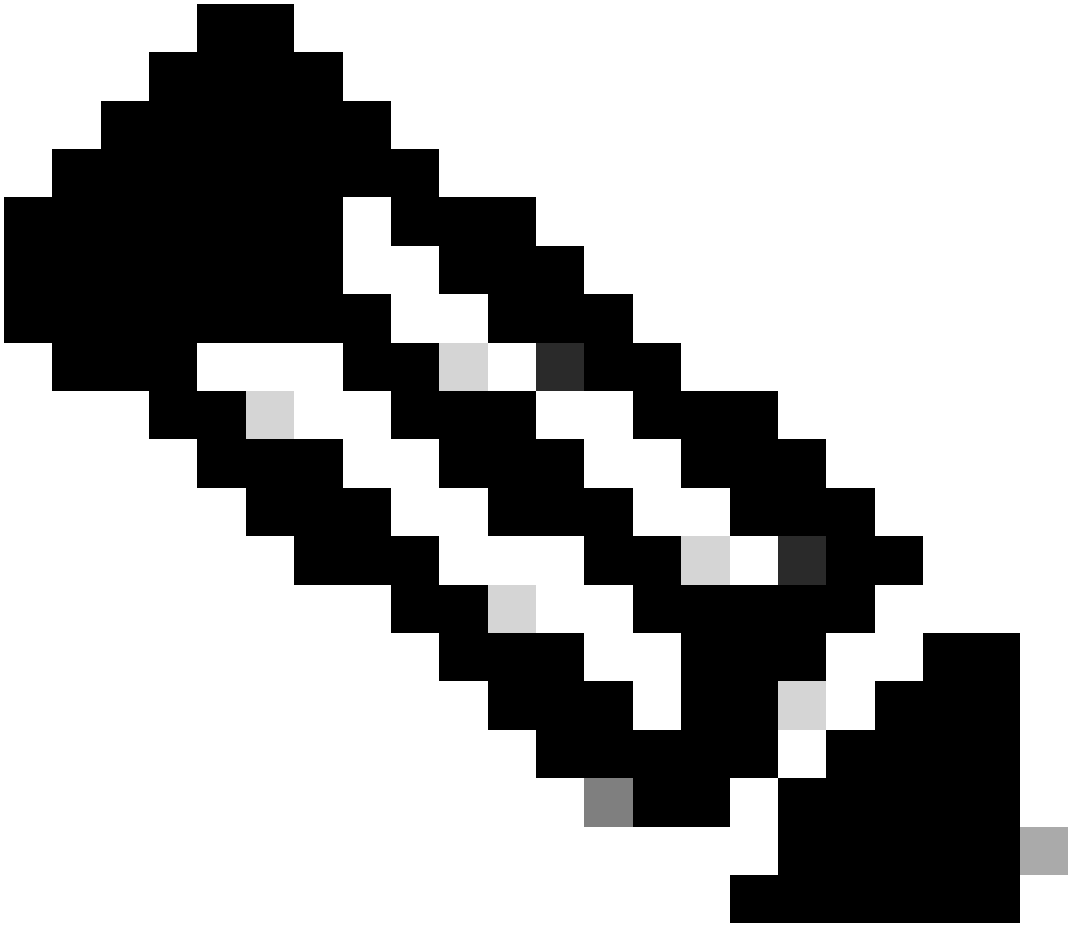
- Virtual Cisco Secure Firewall Threat Defense(FTD)、バージョン7.4.2
- Virtual Cisco Secure Firewall Manager Center(FMC)、バージョン7.4.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

7.4以降にアップグレードして、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージするか、または引き続き個別の診断インターフェイスを使用するかを選択できます。

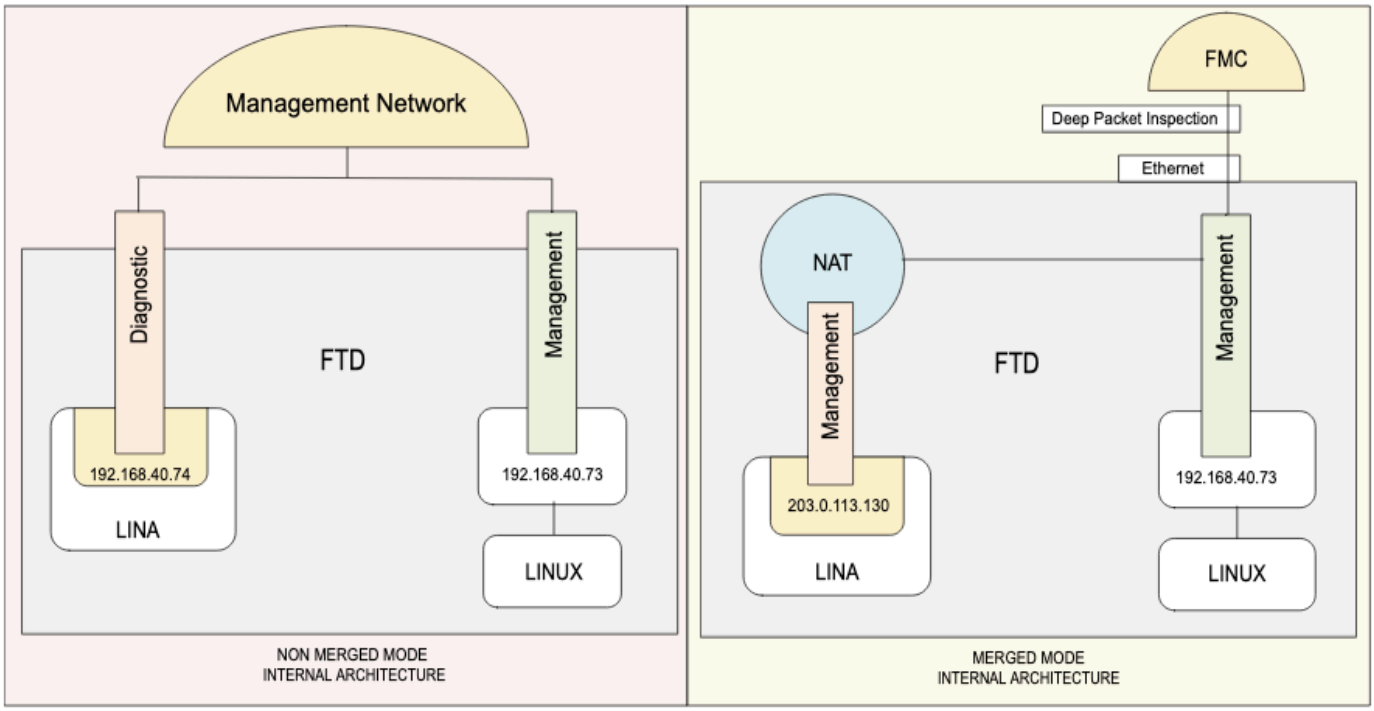
診断インターフェイスの設定がない場合、インターフェイスのマージは自動的に行われます。



注：診断インターフェイスのサポートは今後のリリースで削除される予定です。このため、できるだけ早くインターフェイスをマージすることを計画してください。

FTD内部アーキテクチャ図

統合管理インターフェイスの概要



コンバージェンス管理インターフェイスの前後の内部アーキテクチャの概要

左側は、診断論理インターフェイス(Lina)と管理論理インターフェイス(Linux)の内部アーキテクチャです。 バージョン7.3以前。

右側は、単一の管理インターフェイス用の内部アーキテクチャです。管理ネットワークへの回線アクセスには、NATサービスが使用されます。

コンバージェンス手順

診断インターフェイスに設定が存在する場合は、アップグレード後にインターフェイスが自動的にマージされないため、コンバージェンス手順を実行する必要があります。

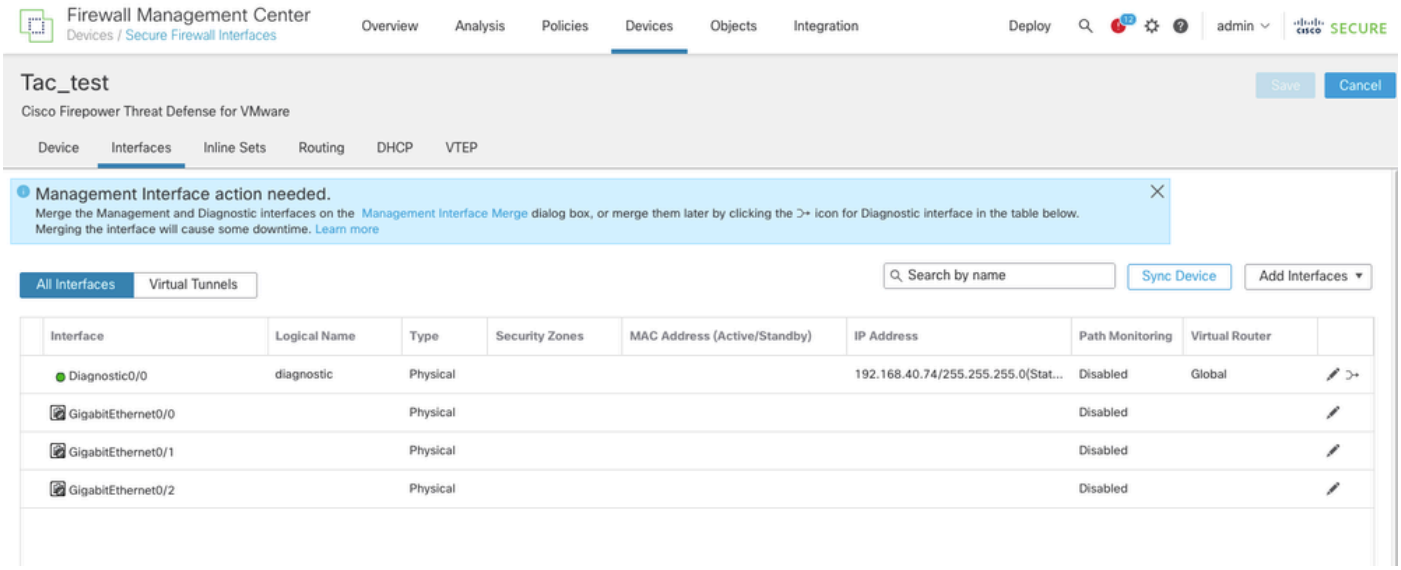
この手順では、設定変更を確認し、場合によっては設定を手動で修正する必要があります。

デバイスの現在のモードを表示するには、FTD CLIクリックでshow management-interface convergeコマンドを入力します

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

この結果は、管理インターフェイスがマージされていないことを示しています。

ステップ 1：
FMCのUIで、Devices > Device Managementの順に移動し、編集するFTDを選択します。
Interfacesタブが直接開きます。

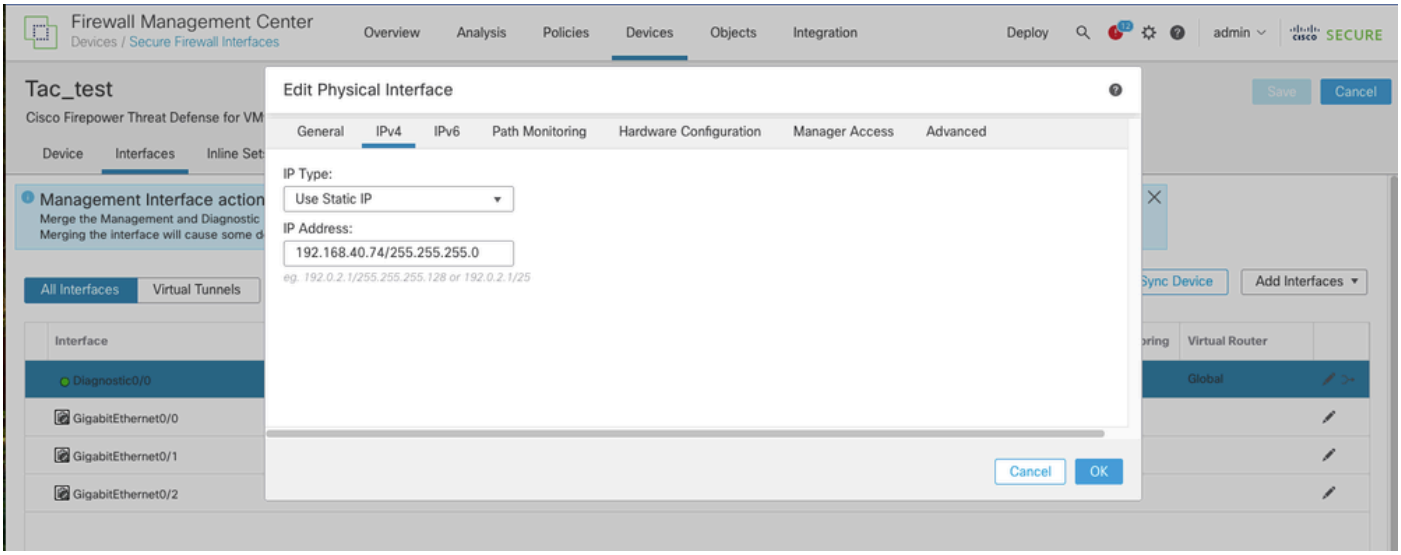


ソフトウェアバージョン7.4.2にデバイスをアップグレードした後、診断および管理インターフェイスをマージするために必要なアクション

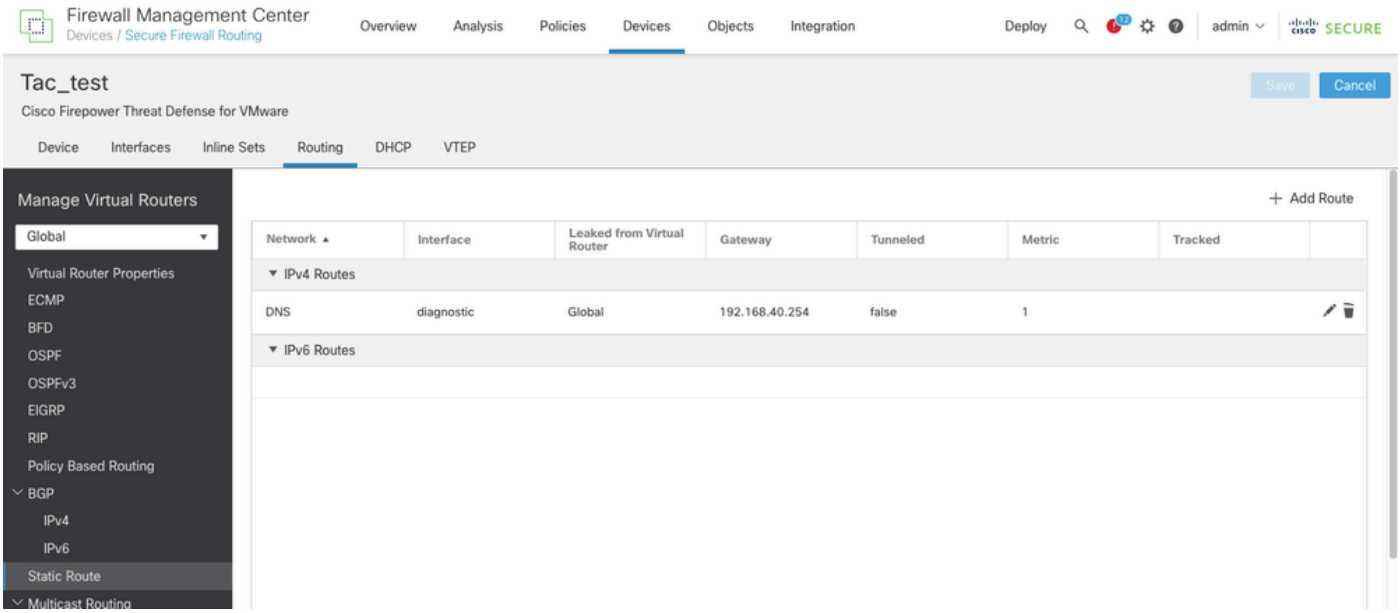
ステップ 2：

診断インターフェイスの設定をすべて削除します。診断インターフェイスには、マージを続行するための設定がないことが必須です。

たとえば、この診断インターフェイスには、IPアドレスとスタティックルートがあります。



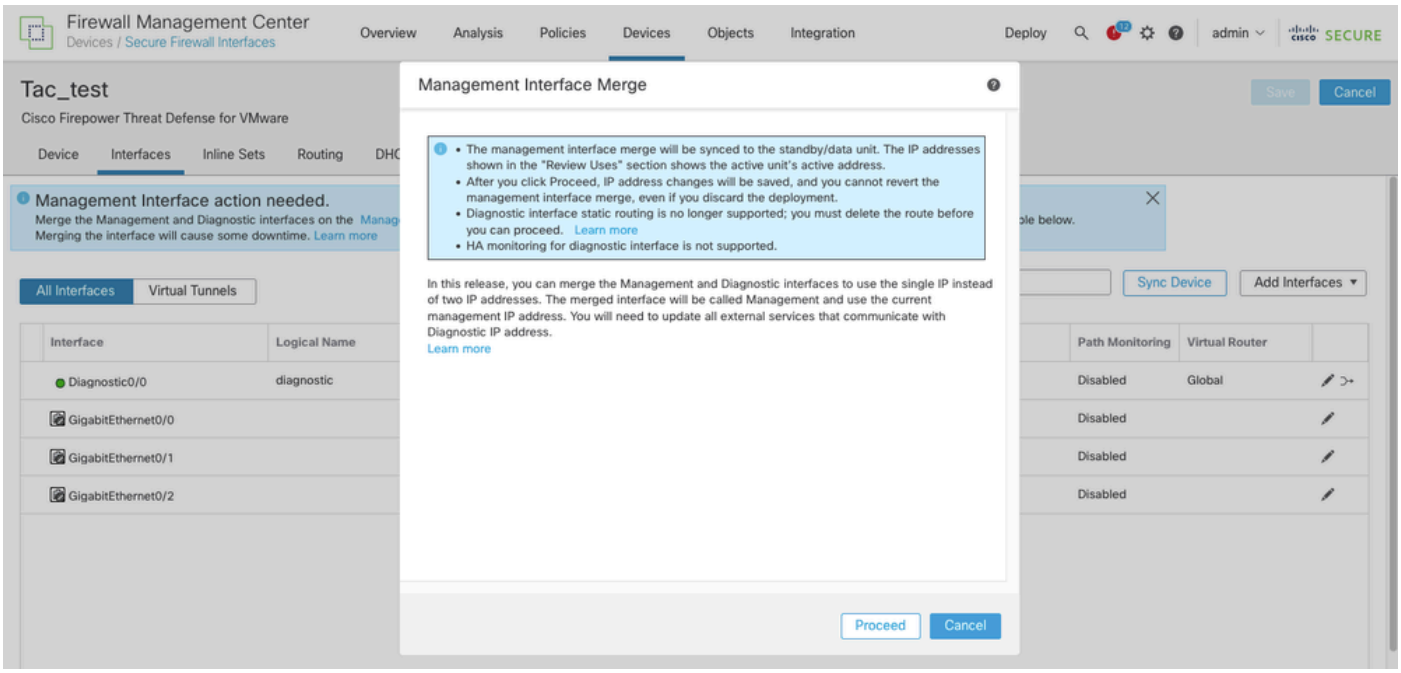
診断インターフェイスのIPアドレスの削除



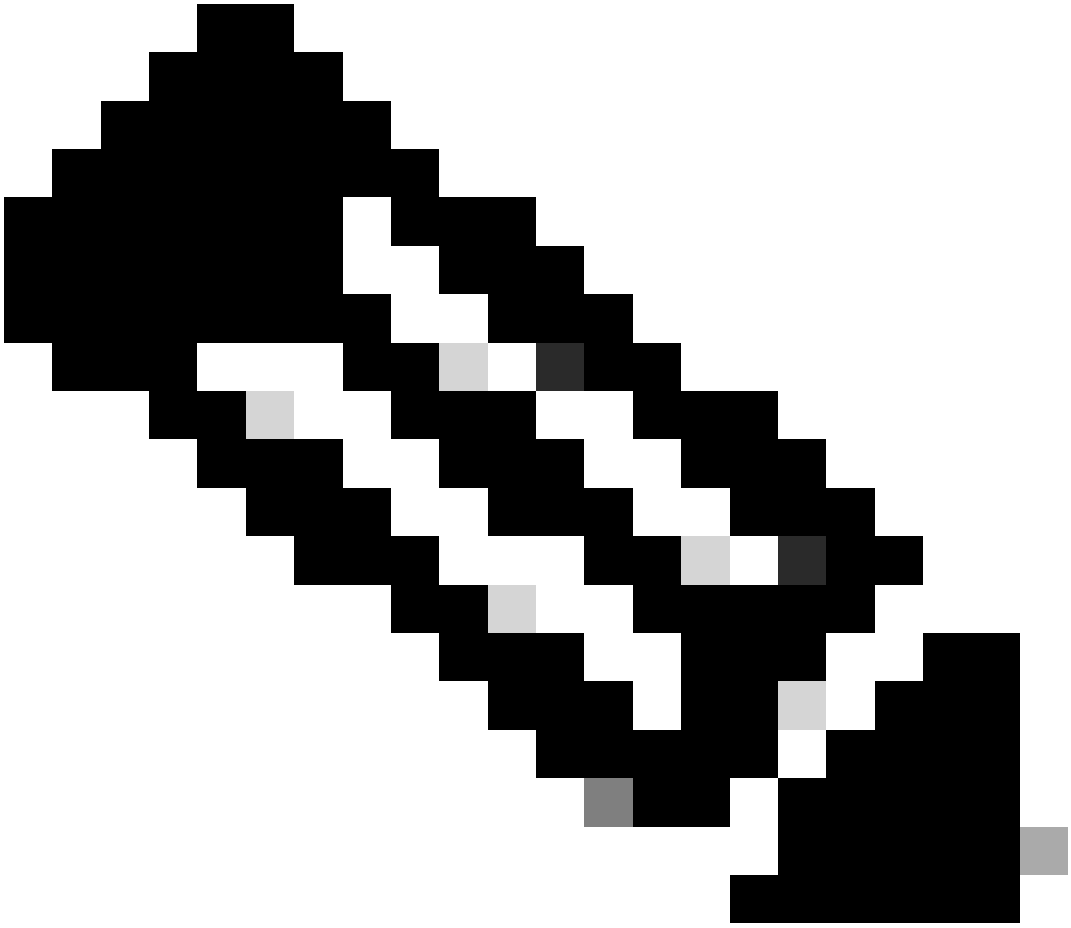
診断インターフェイスでのスタティックルートの設定

ステップ 3：

Diagnosticインターフェイスで、Management Interface Merge action needed領域、またはEditアイコン（鉛筆）の横にあるMerge iconをクリックします。

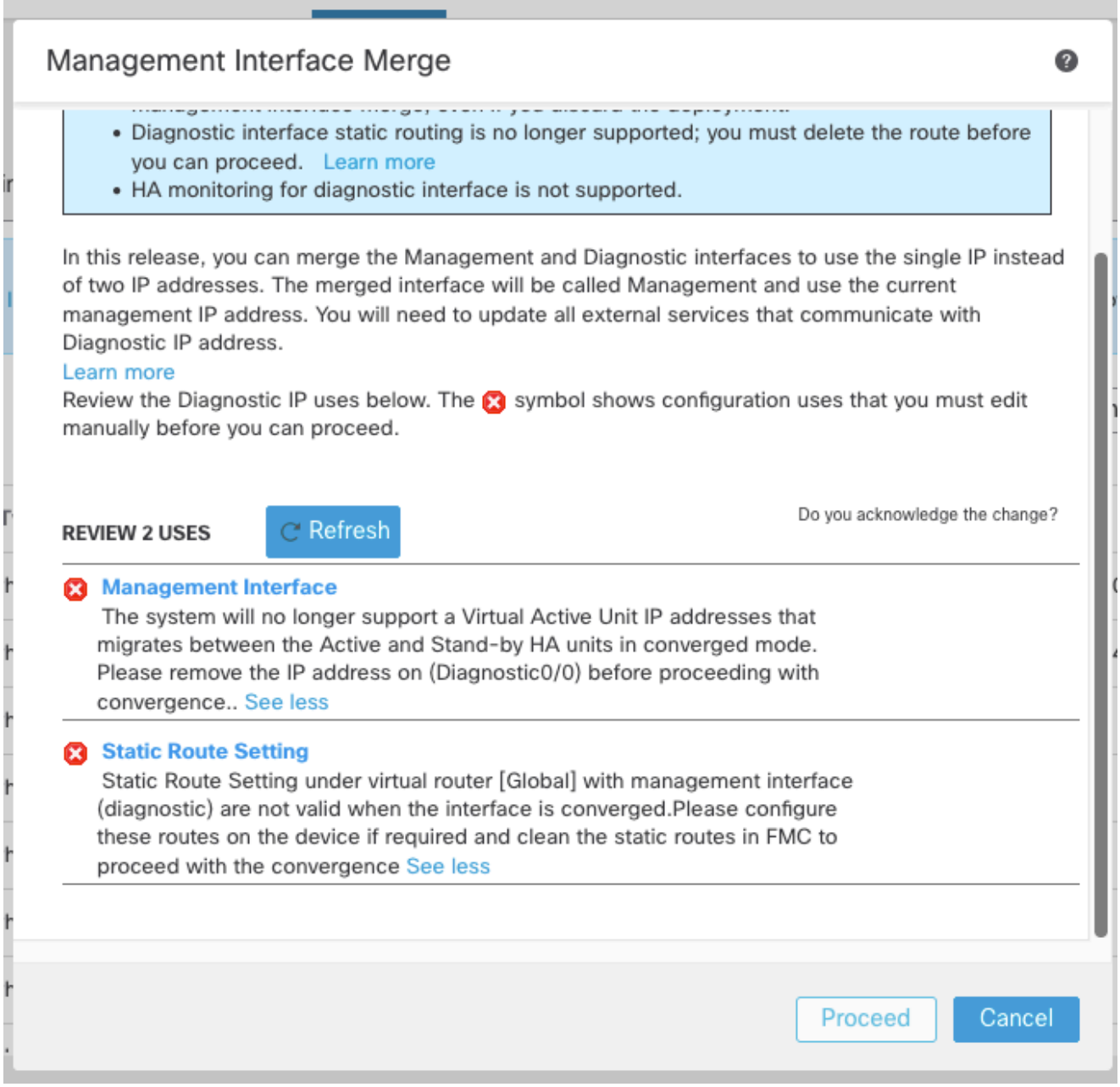


続行する前の管理インターフェイスマージ情報



注：ハイアベイラビリティペアおよびクラスタの場合は、このタスクをアクティブ/コントロールユニットで実行します。マージされたコンフィギュレーションは、スタンバイ/データユニットに自動的に複製されます。

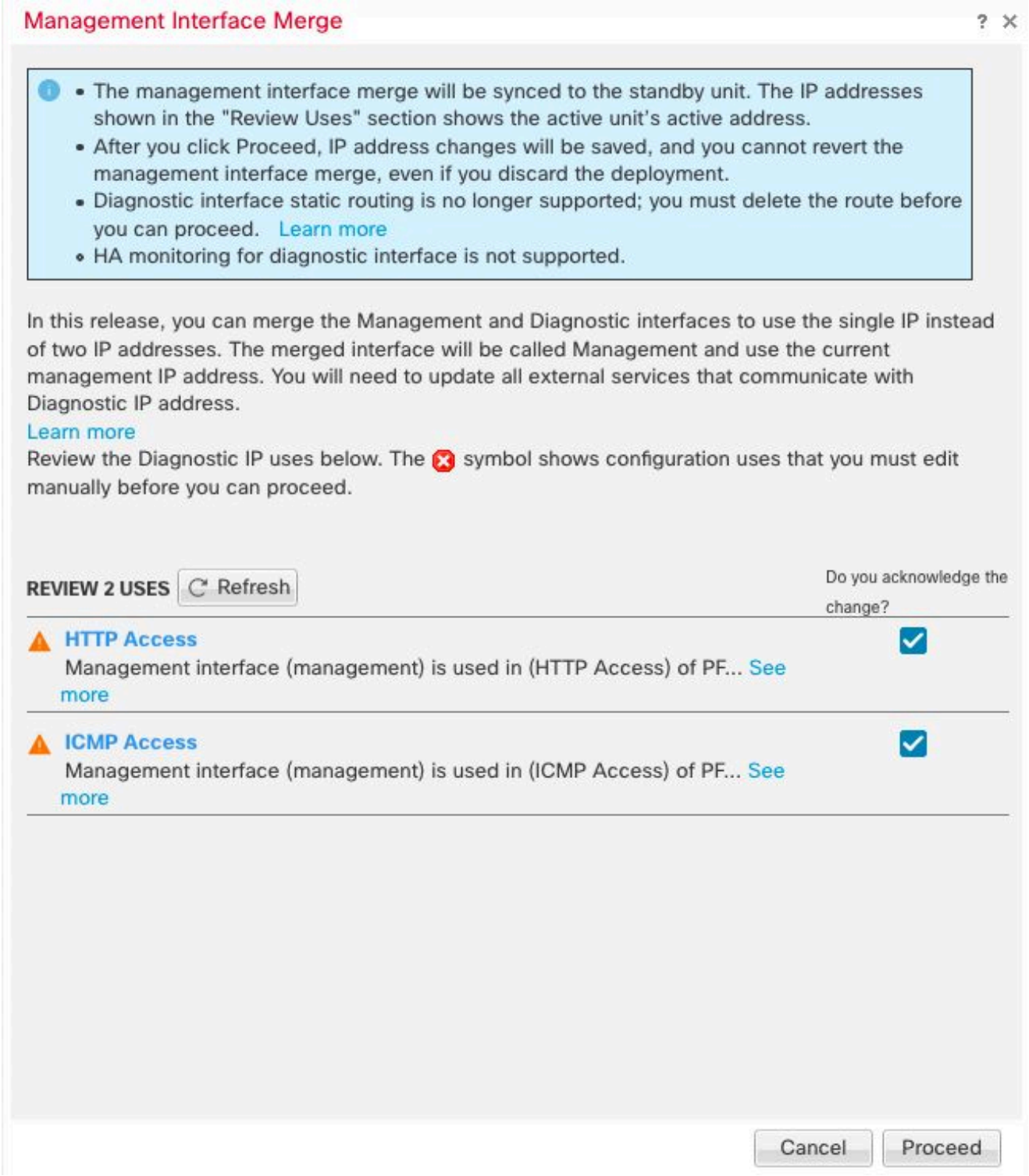
- 手動で変更または削除する必要がある場合は、警告アイコンが表示されます。



マージの前に削除する必要がある構成に関する警告例

その場合は、ダイアログボックスをキャンセルし、設定または再設定の削除に進み、[管理インターフェイスのマージ]ダイアログボックスを再度開きます。

- デバイス上で動作する予定のプラットフォーム設定には警告アイコンが表示され、確認が必要です。



編集が必要なプラットフォーム設定の警告例

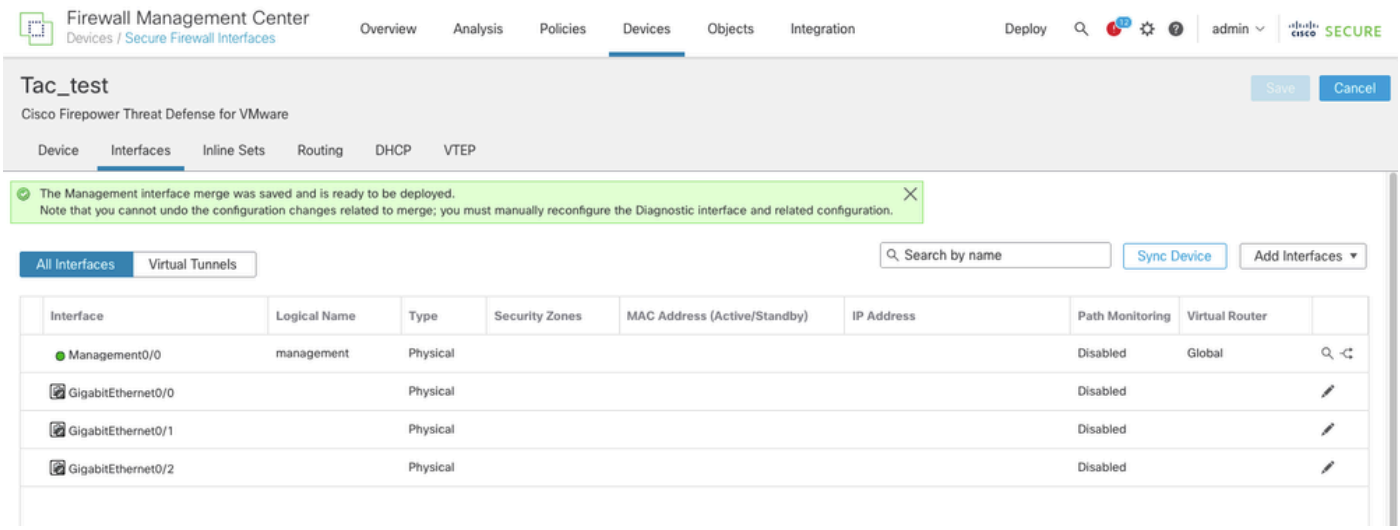
- Do you acknowledge the change?列のボックスをクリックし、Proceedをクリックします。

ステップ 4：

設定がマージされると、成功のバナーが表示されます。
“管理インターフェイスのマージは保存され、展開の準備ができました。
マージに関連する設定変更を元に戻すことはできません。診断インターフェイスと関連する設定

を手動で再設定する必要があります。

新しいマージされた設定を展開します。



管理インターフェイスのマージが保存され、展開できる状態になりました

管理インターフェイスは読み取り専用ですが、Interfacesページに表示されます。

展開後、管理インターフェイスでのコンバージェンス手順は完了します。

ステップ 5：Optional

診断インターフェイスと通信する外部サービスがある場合、管理ルートフォールバックはコンバージドモードでは削除されているため、管理インターフェイスのIPアドレスを使用するように設定を変更する必要があります。

例：

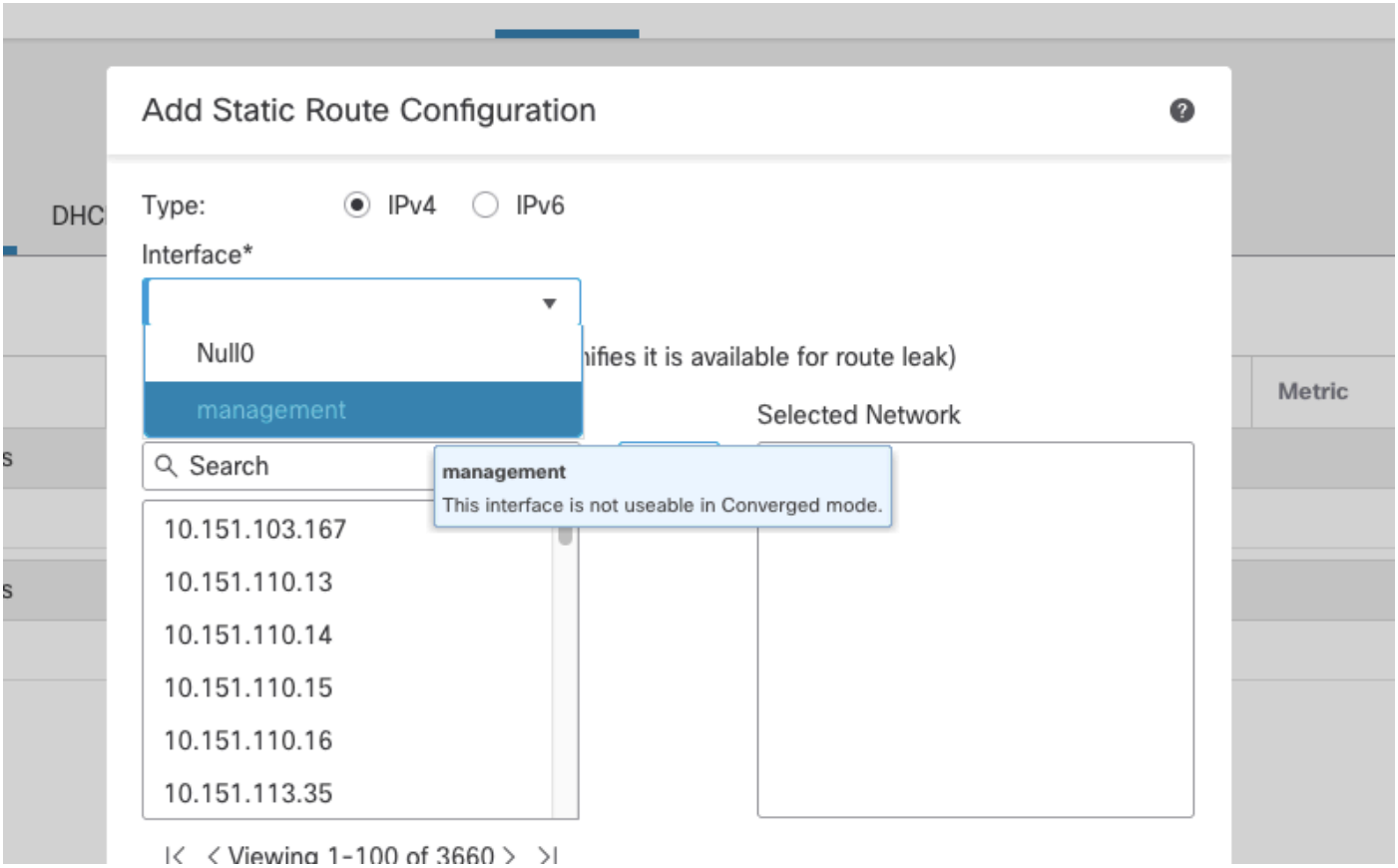
- SNMPクライアント
- RADIUS サーバ
- 管理ネットワークを介してDNSサーバに到達できるようにするには、DNSルックアップとICMP（pingおよびtraceroute）に例外が設定されているため、ユーザは明示的に[Enable DNS Lookup via diagnostic/Management Interface also]を選択する必要があります。この場合、threat defenseはデータを使用し、ルートが見つからない場合は自動的に管理にフォールバックします。

管理インターフェイスのスタティックルートの使用は、FTD CLIクリック(Linux)でのみ設定できます

Lina管理ポートのデフォルトルートは、すべてのフレームをLinuxモジュールに送信します。

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

FMCのUIでは、管理インターフェイスがグレー表示され、選択できます。



マージが完了した後のスタティックルートでは、管理インターフェイスを選択できません。

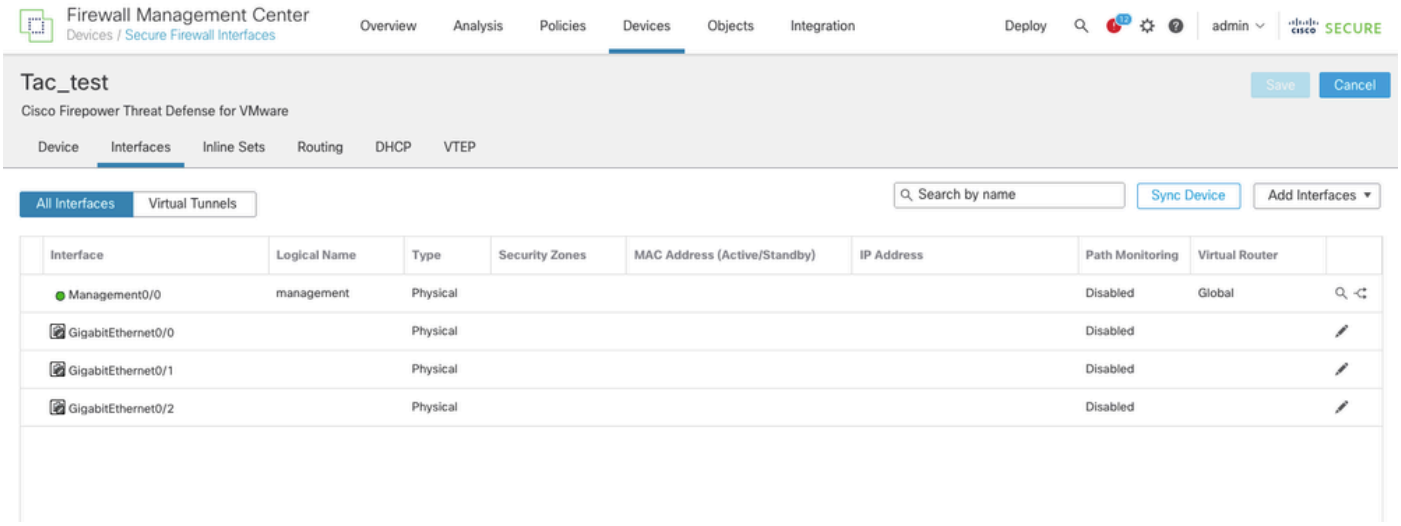
確認

管理インターフェイスでのマージ後の予期される変更

- FTD CLIクリックでコマンドを実行して、コンバージェンスモードを確認します。

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

- FMCのUIで、インターフェイス名がManagement0/0、論理名がmanagementに変更されます。



管理インターフェイス名と論理名のマージ確認

- FTD CLIクリックで、新しいIPアドレスが管理インターフェイスのLinaに自動的に設定されます。
  NATは内部実装として使用されます。内部プライベートIPv4アドレス203.0.113.130およびIPv6アドレスfd00:0:1:1::2は、割り当てられているものです（どちらも変更される可能性があります）。
  これらのIPはパブリックLinuxカーネルのFTDのIPv4アドレスとIPv6アドレスにNAT変換されるため、Lina上でパブリックIPは不要になります。

  エキスパートモードでは、「ifconfig」はLinuxの内部IPv4 (203.0.113.129)とIPv6 (fd00:0:1:1::1)アドレスを表示します。

```
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
```

トラブルシューティング：テストケース

このテストケースでは、7.4.2にアップグレードする前に、仮想FTDの診断インターフェイスで、DNSルックアップの外部サービスへの接続用に個別のIPアドレスが設定されています。

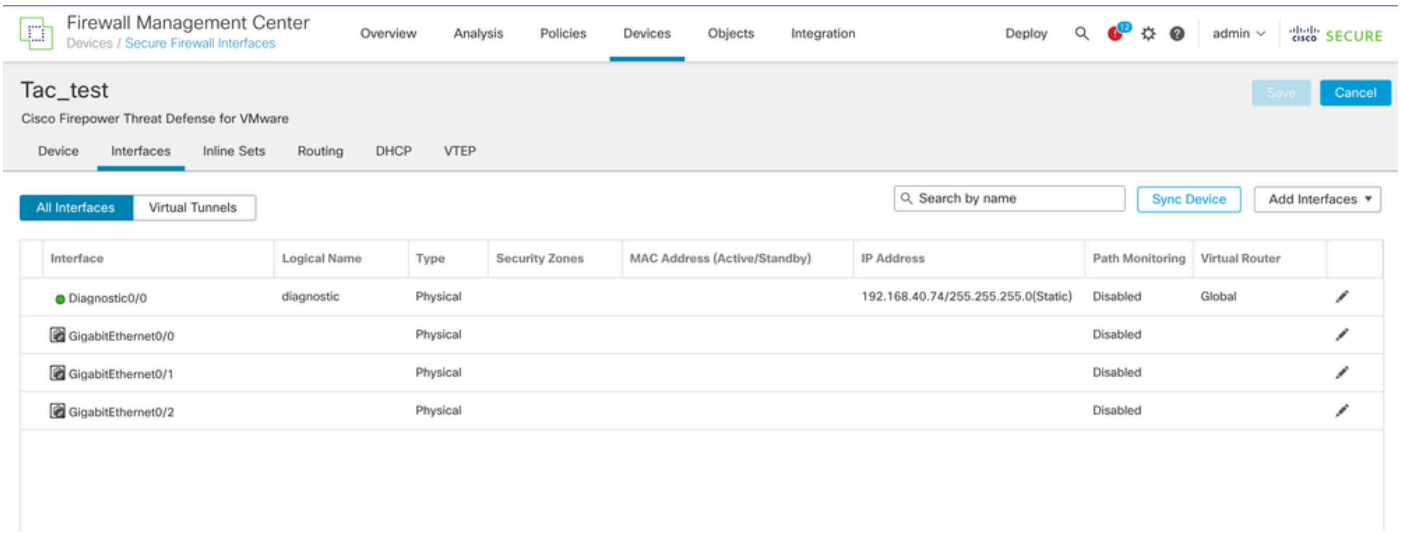
7.4.2へのアップグレード後、コンバージェンスが必要になります。マージの前後には、FMC UI、FTD CLI Lina、およびLinuxの設定はこのようになっています。

また、FTD CLI LinaおよびLinuxでは、論理診断インターフェイスを使用するトラフィックが管理インターフェイスを使用するトラフィックに移行したことを示すトラフィックキャプチャも表示されます。

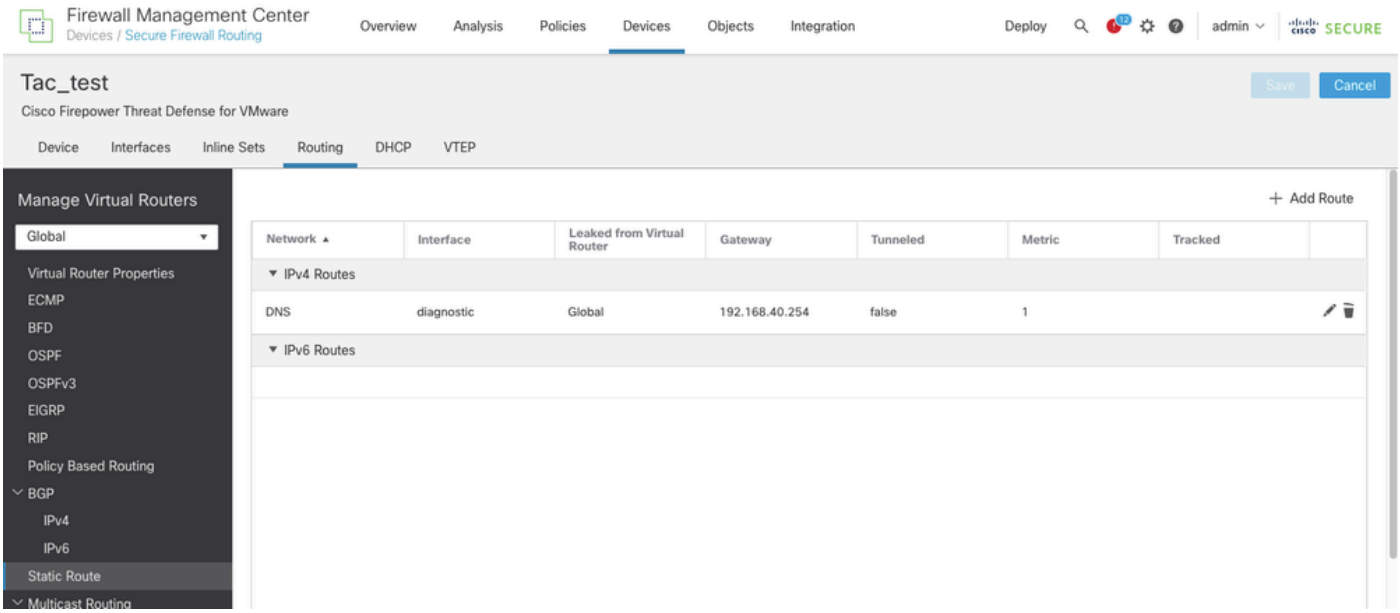
コンバージェンス設定前

診断インターフェイスには、DNSルックアップ用に別個のIPとスタティックルートがあります。この方法では、FTDでLinaからLinuxへの両方の論理インターフェイスを使用して動作します。

FMC UIの設定



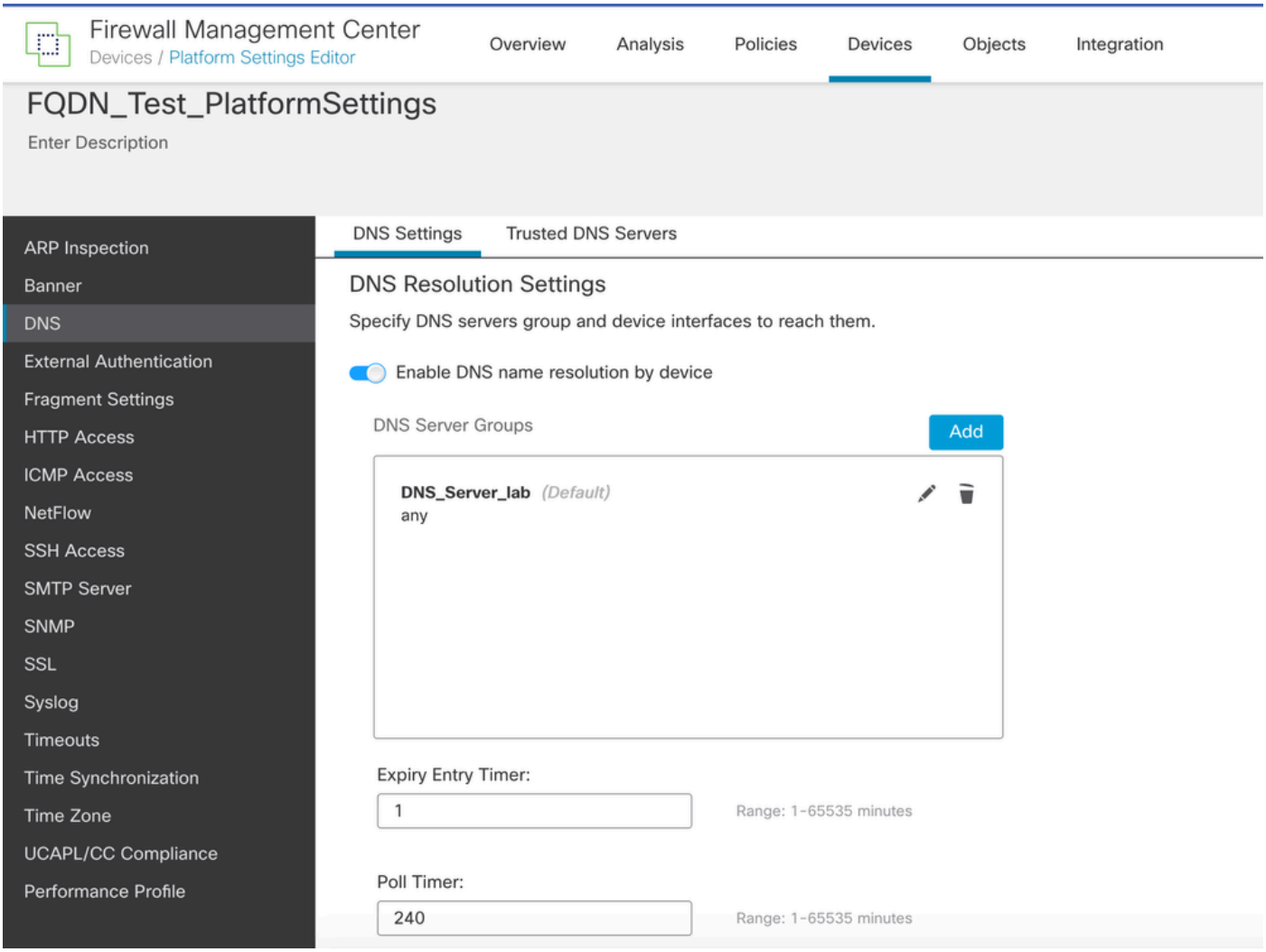
マージ前の診断インターフェイスの設定



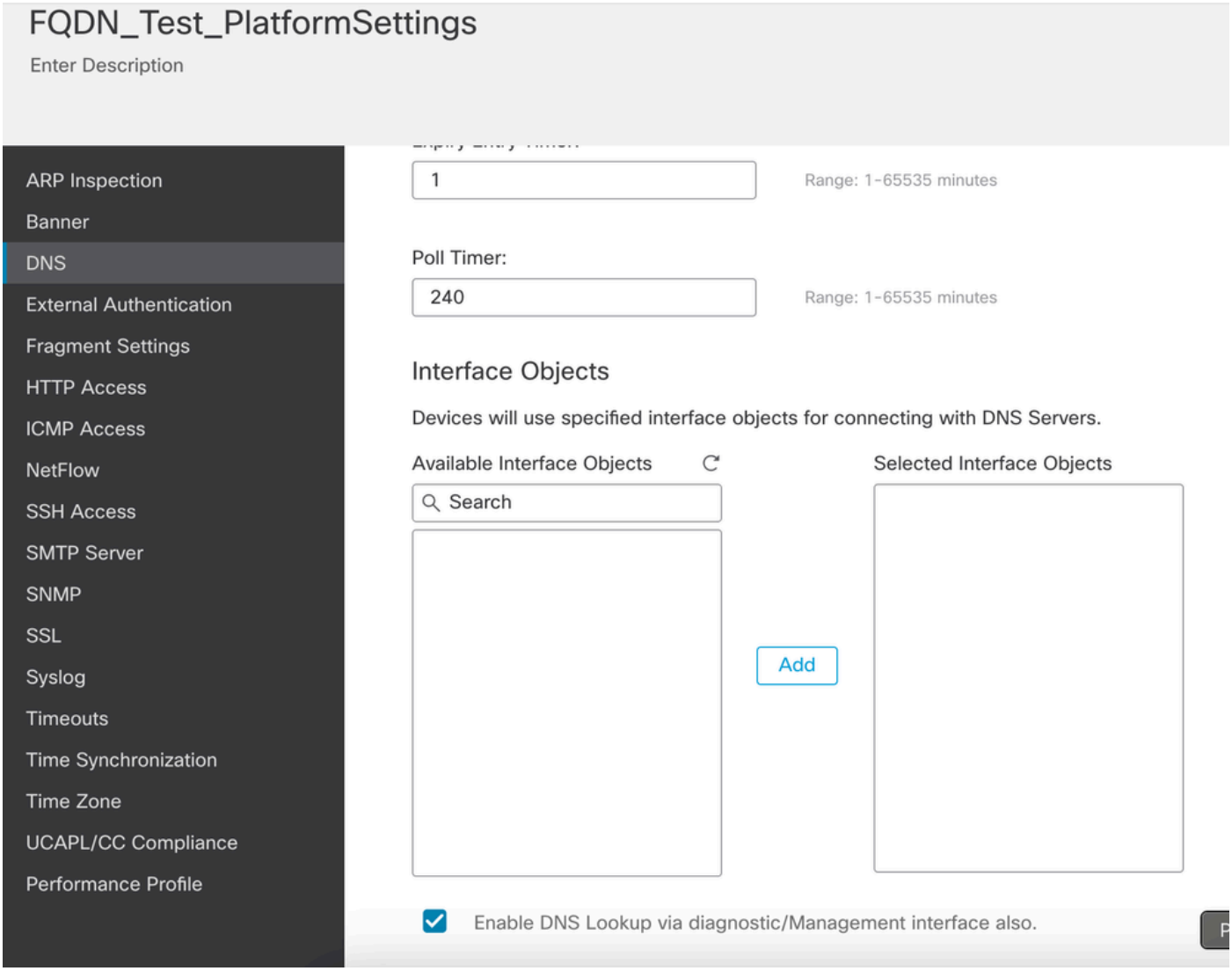
診断インターフェイスに設定されたスタティックルート

DNS設定

Devices > Platform Settingsの順に選択し、ポリシー、DNSタブの順に選択します。



プラットフォーム設定でのDNS設定



Enable DNS Lookup via diagnostic/Management interface alsoチェックボックスがオンになっている

FTD Lina上の診断インターフェイスの設定

```
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回線でのDNS設定

```
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
```

DNSサーバ10.10.10.10に送信されるDNSトラフィックの診断インターフェイスでのキャプチャ

```
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#
```

Linuxエキスパートモードでキャプチャし、診断インターフェイスから管理インターフェイス上のDNSルックアップトラフィックの正しいフローを確認します。

```
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)
```

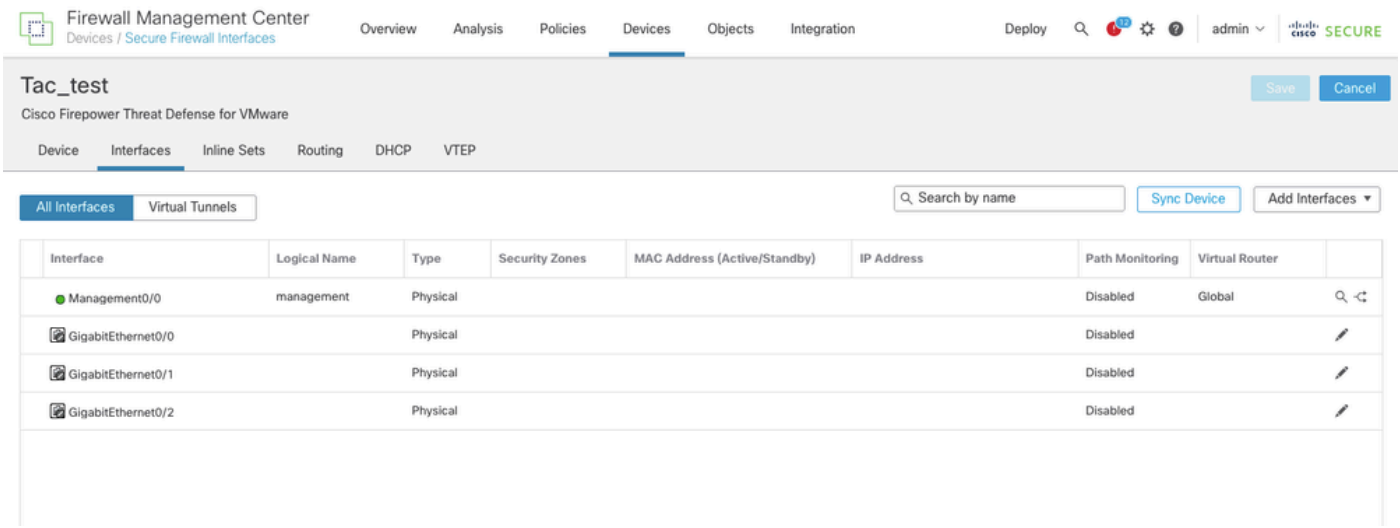
コンバージェンス設定後

コンバージェンス手順で説明したように、マージを実行するには、診断インターフェイスのすべての設定を削除する必要があります。

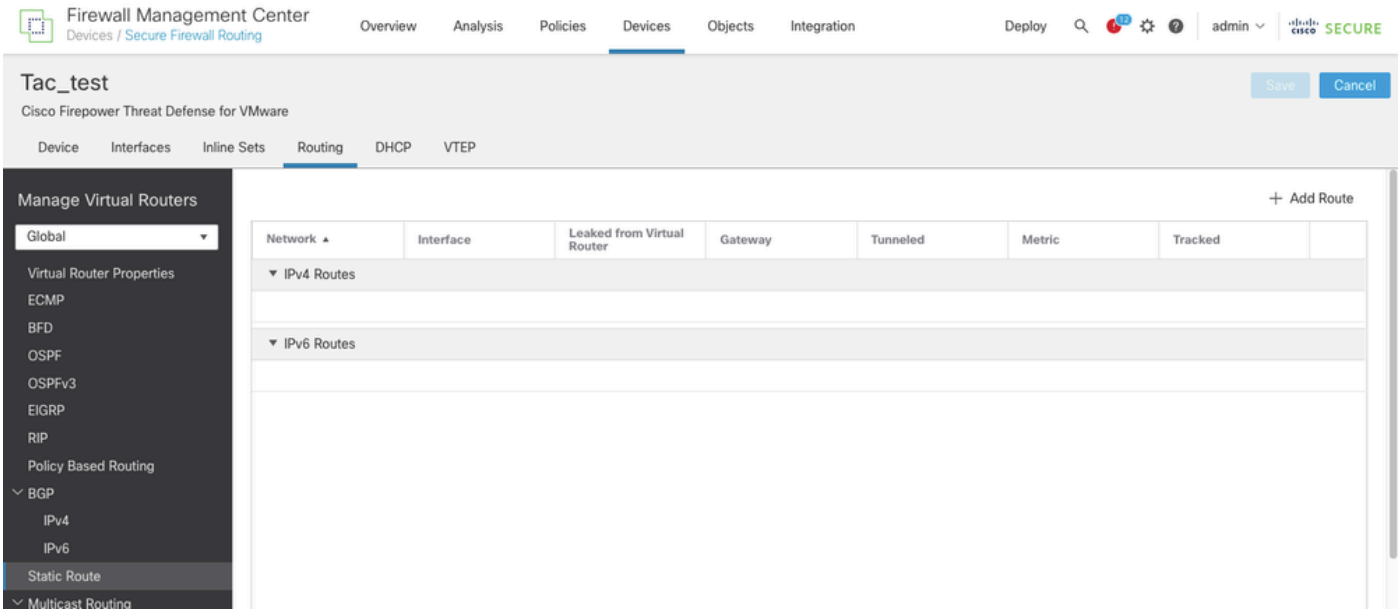
マージが完了した後のFMCとFTD CLIの情報を次に示します。

FMC UIでの管理インターフェイスの設定

Devices > Device Managementの順に選択し、FTDを選択します。Interfacesタブが直接開きます。



マージ後の管理インターフェイス

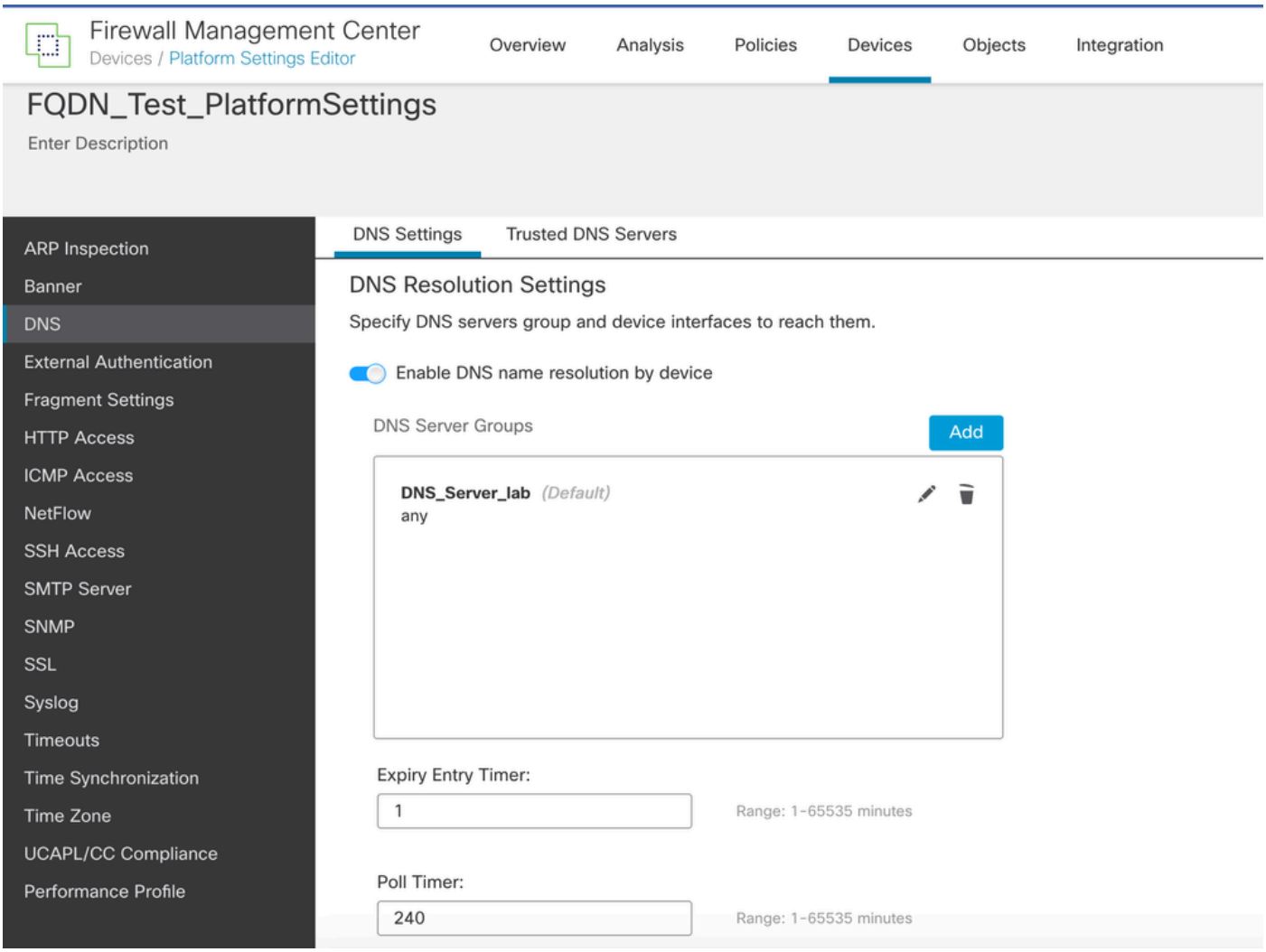


DNSサーバへのスタティックルートは追加されない

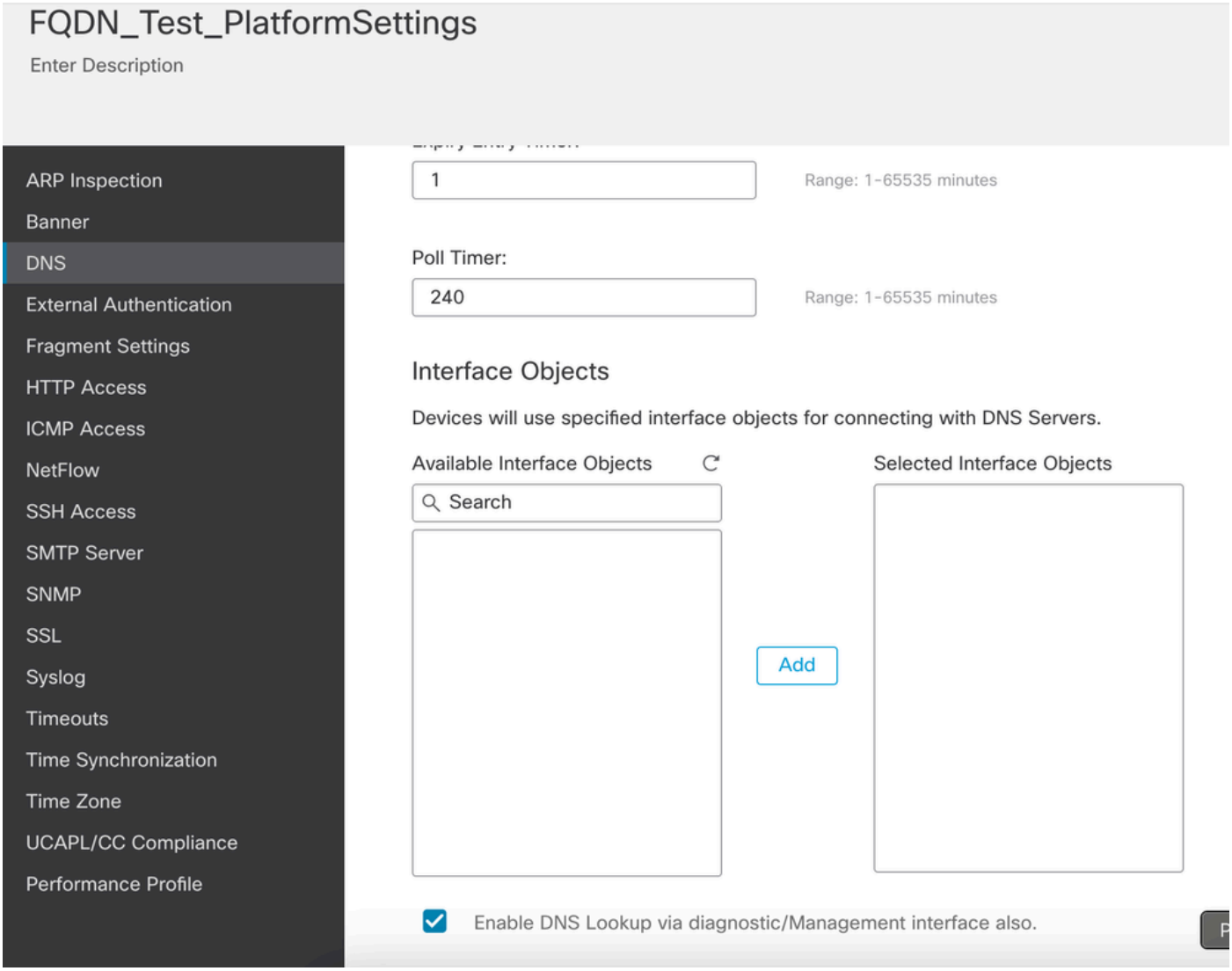
DNSの設定は、プラットフォームの設定と同じにする必要があります。

Devices > Platform Settingsの順に選択し、ポリシー、DNSタブの順に選択します。

スタティックルートを追加せずにDNSルックアップを管理インターフェイスに送信し続けるには、「Enable DNS Lookup via diagnostic/Management interface also.」を選択したままにする必要があります。



プラットフォーム設定でのDNS設定



診断/管理インターフェイス経由のDNSルックアップを有効にするオプションも同じままにする必要があります

FTD CLIでの設定

```
> 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側のFTD CLIでのDNS設定

```
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
```

Linuxエキスパートモードでキャプチャし、管理インターフェイス上のDNSルックアップトラフィックの正しいフローを確認します。

```
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)
```

この証拠から、Linux経由で管理インターフェイスにスタティックルートが追加されていなくても、DNSルックアップが引き続き機能することが確認できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。