Configurar a mesclagem da interface de gerenciamento e diagnóstico no FMC

Contents

Introdução

Este documento descreve as etapas para configurar a mesclagem das interfaces de gerenciamento e diagnóstico, recurso adicionado no FTD versão 7.4.0.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Defesa contra ameaças (FTD) do Cisco Secure Firewall
- Cisco Secure Firewall Manager Center (FMC)

Informações de Apoio

Na versão 7.3 e anteriores, a interface de gerenciamento físico é compartilhada entre a interface lógica de diagnóstico (Lina) e a interface lógica de gerenciamento (Linux).

Na versão 7.4 e posterior, a interface de diagnóstico é mesclada com o gerenciamento para uma experiência de usuário simplificada.
Para novos dispositivos que usam a versão 7.4 ou posterior, você não pode usar a interface de diagnóstico herdada. Somente a interface de Gerenciamento mesclada está disponível.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

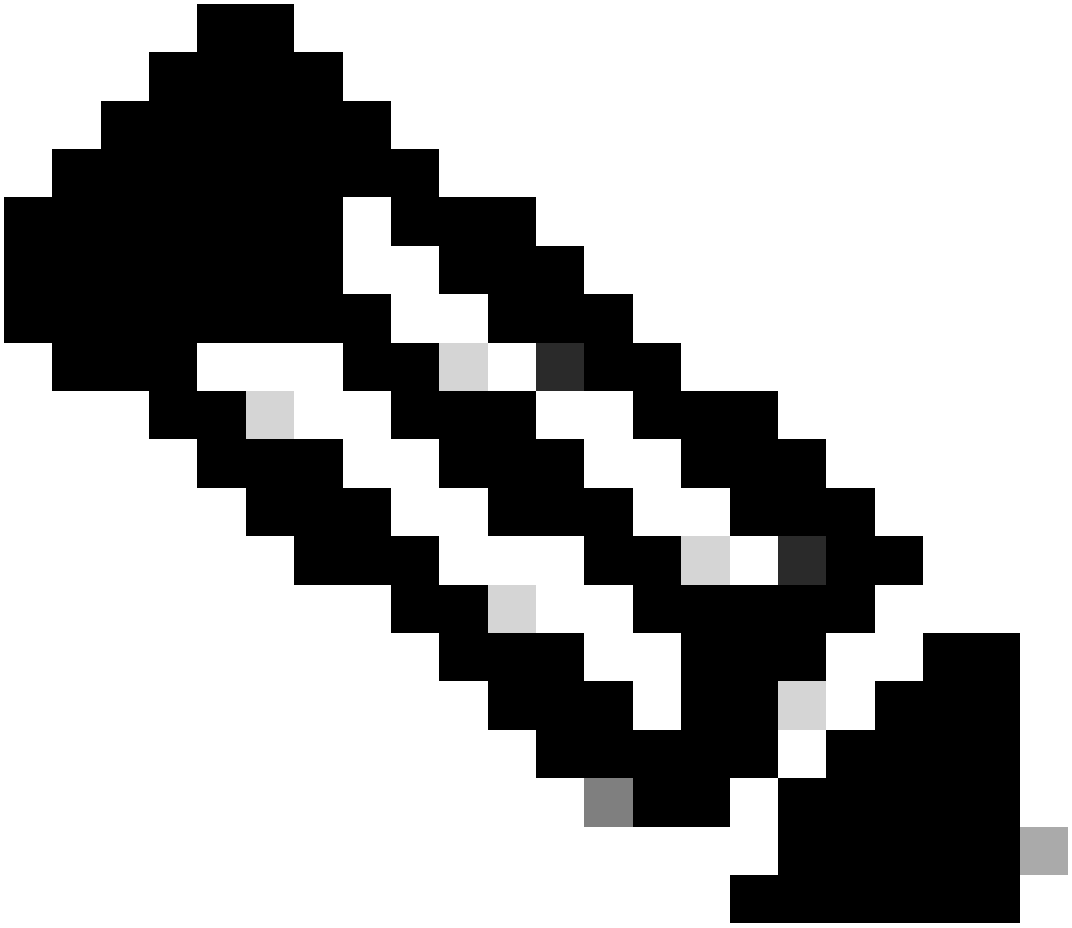
- Virtual Cisco Secure Firewall Threat Defense (FTD), versão 7.4.2
- Virtual Cisco Secure Firewall Manager Center (FMC), versão 7.4.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Se você atualizou para a versão 7.4 ou posterior e tiver configuração para a interface de Diagnóstico, você poderá optar por mesclar as interfaces manualmente ou continuar a usar a interface de Diagnóstico separada.

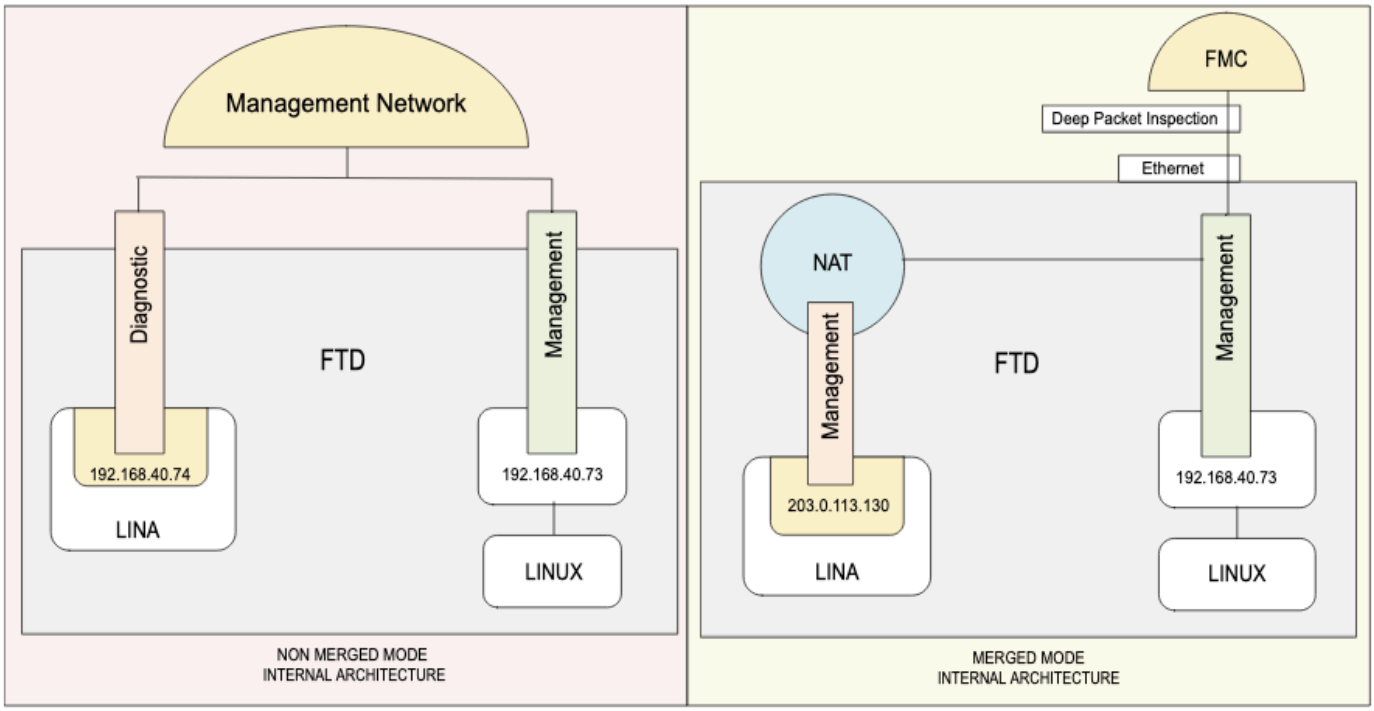
Caso você não tenha nenhuma configuração para a interface de Diagnóstico, a mesclagem de interfaces é feita automaticamente.



Note: O suporte para a interface de diagnóstico deve ser removido em uma versão posterior, portanto, planeje mesclar as interfaces o mais rápido possível.

Diagrama de arquitetura interna do FTD

Visão geral da interface de gerenciamento convergente



Visão geral da arquitetura interna antes e depois da interface de gerenciamento de convergência

À esquerda, estão a arquitetura interna para a Lina (Diagnostic logical interface, interface lógica de diagnóstico) e a Linux (Management logical interface, interface lógica de gerenciamento). Versão 7.3 e anterior.

À direita, a arquitetura interna para uma única interface de gerenciamento. O acesso da linha à rede de gerenciamento usa o serviço NAT.

Procedimento de convergência

No caso em que a configuração existe na interface de Diagnóstico, as interfaces não são mescladas automaticamente após uma atualização e você precisa executar o procedimento de convergência.

Este procedimento requer que você confirme as alterações de configuração e, em alguns casos, corrija manualmente a configuração.

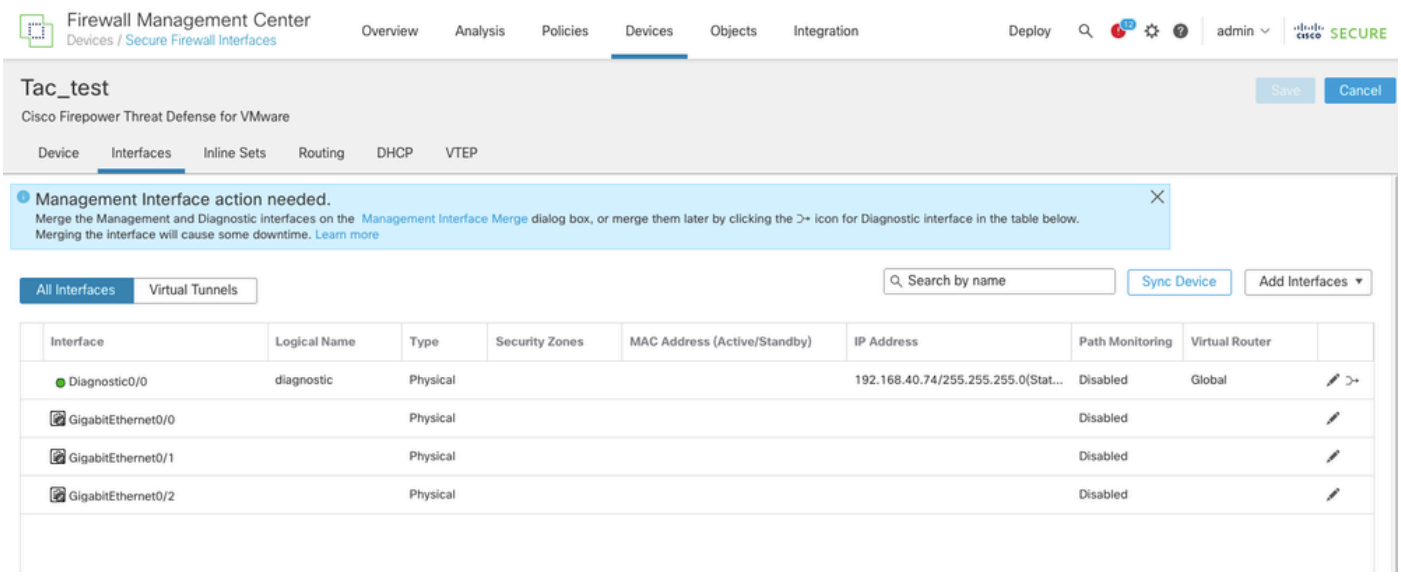
Para visualizar o modo atual do dispositivo, insira o comando show management-interface converge no FTD CLI Clish

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

Esse resultado mostra que as interfaces de gerenciamento não são mescladas.

Etapa 1.
Na interface do FMC, navegue para Devices > Device Management e selecione o FTD a ser

editado. Ele é aberto diretamente na guia Interfaces.

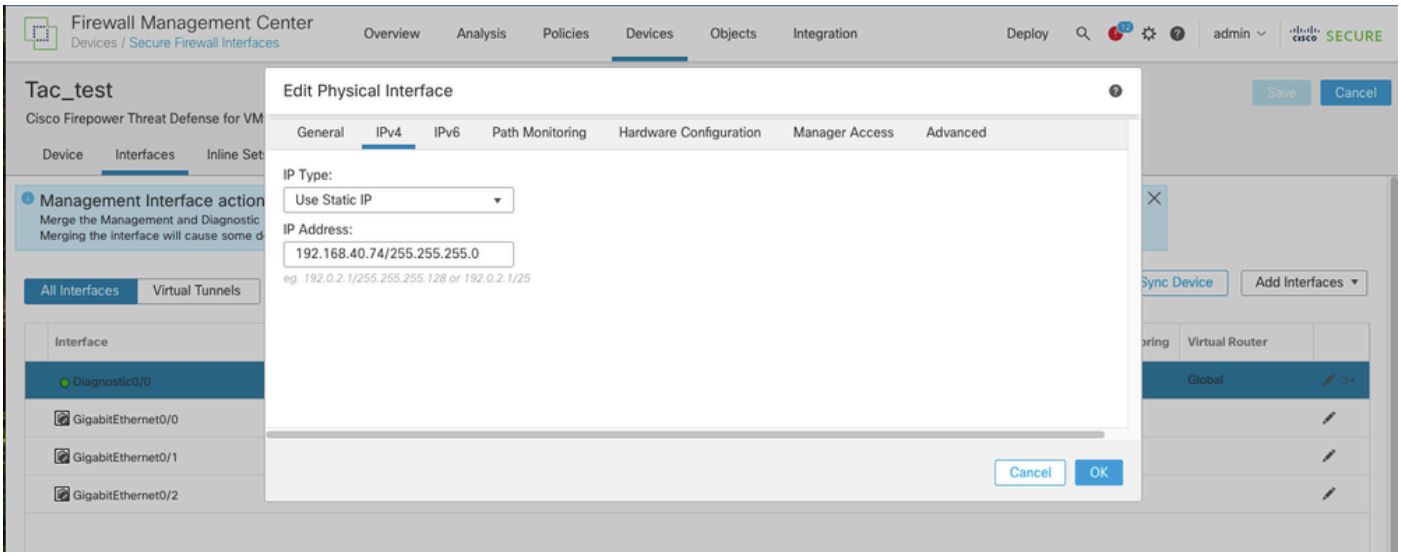


Ação necessária para mesclar a interface de diagnóstico e gerenciamento após a atualização do dispositivo para o software versão 7.4.2

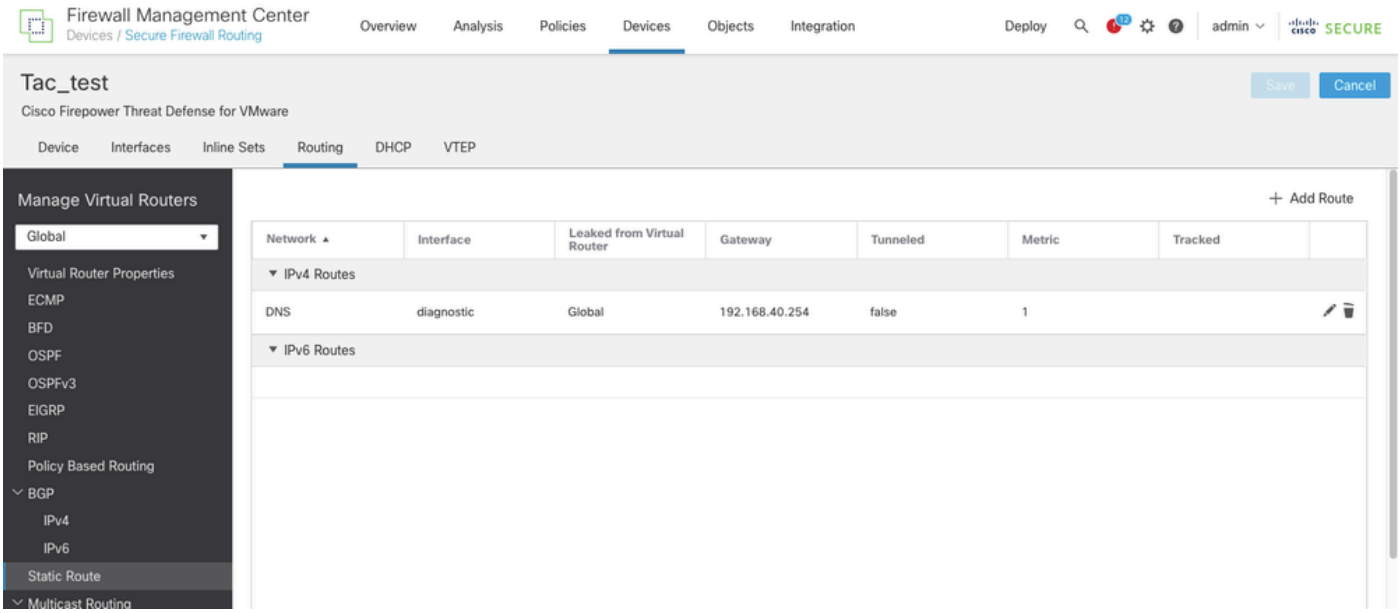
Etapa 2.

Remova toda a configuração na interface de Diagnóstico. É obrigatório que a interface de Diagnóstico não tenha nenhuma configuração para continuar com a mesclagem.

Por exemplo, nesta interface de Diagnóstico, há: Endereço IP e rota estática.



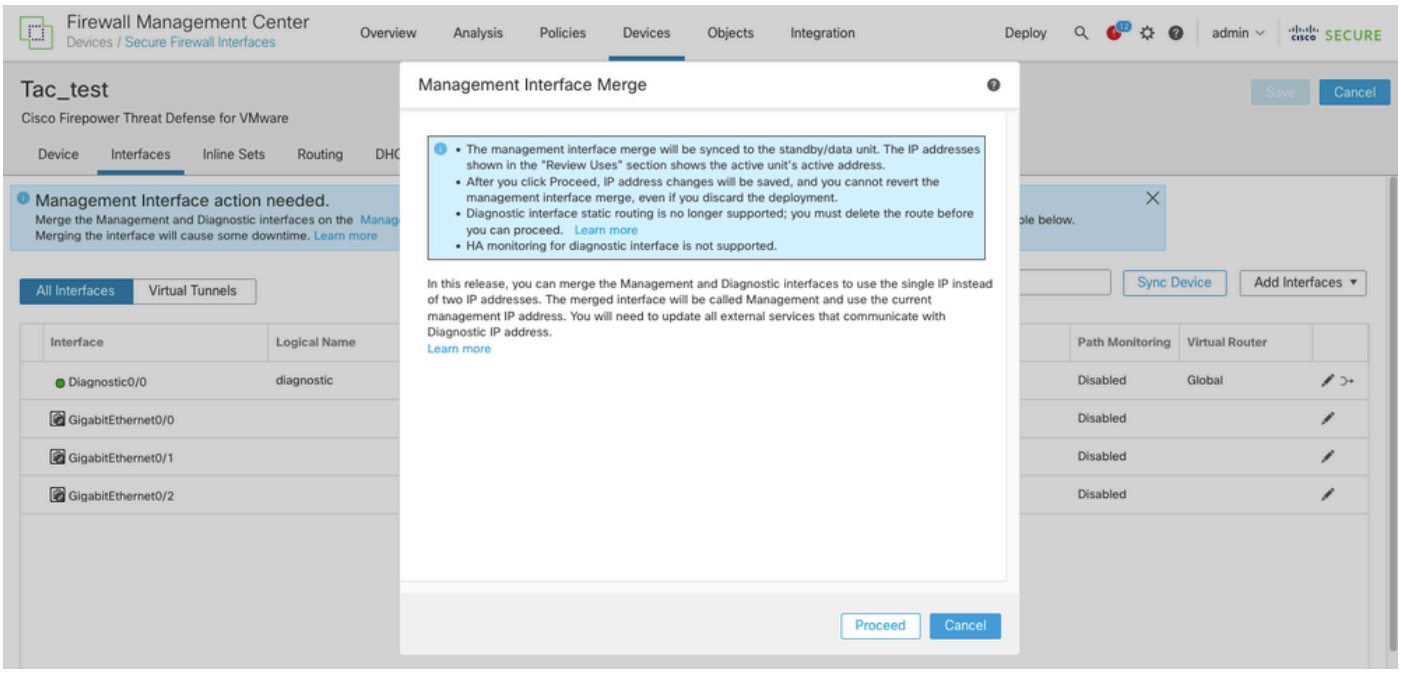
Remova o endereço IP da interface de diagnóstico



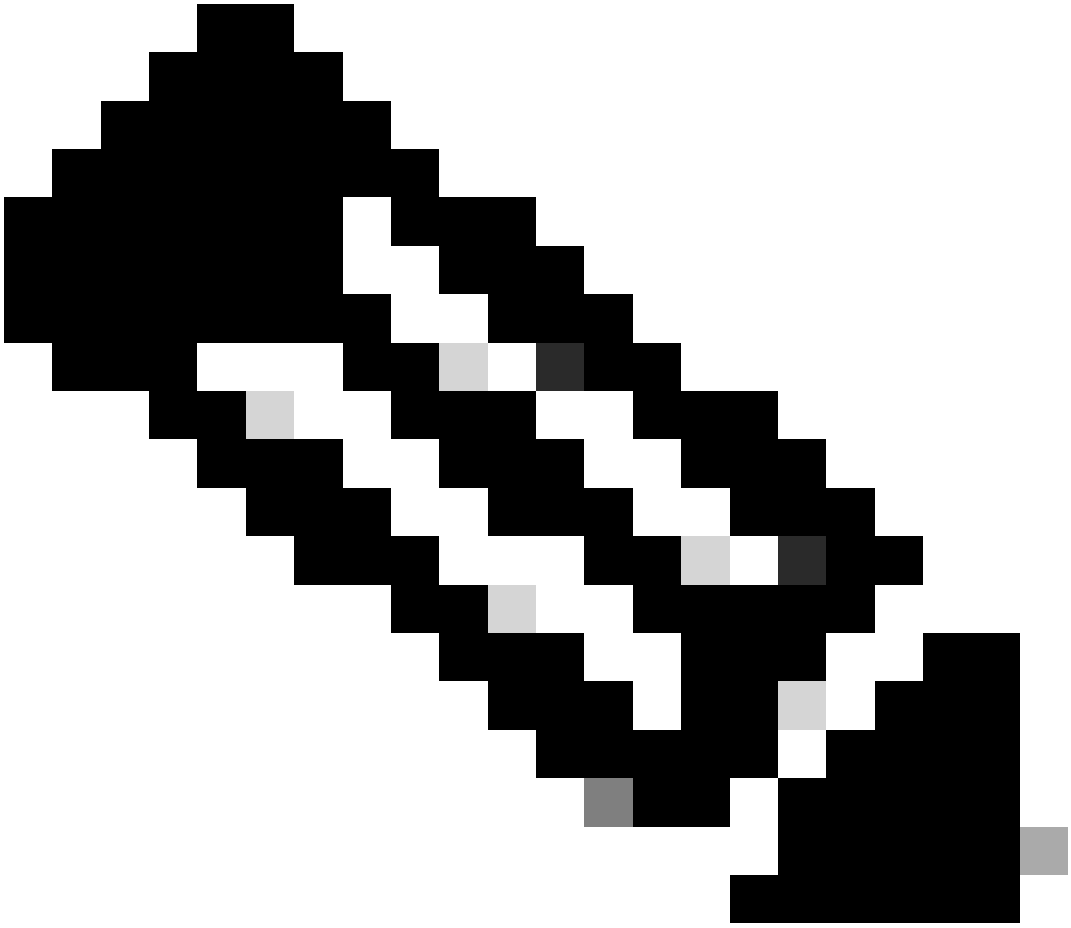
Configuração de rota estática na interface de diagnóstico

Etapa 3.

Clique na área Management Interface Merge action needed ou no ícone Merge ao lado do ícone Edit (lápis) na interface Diagnostic.

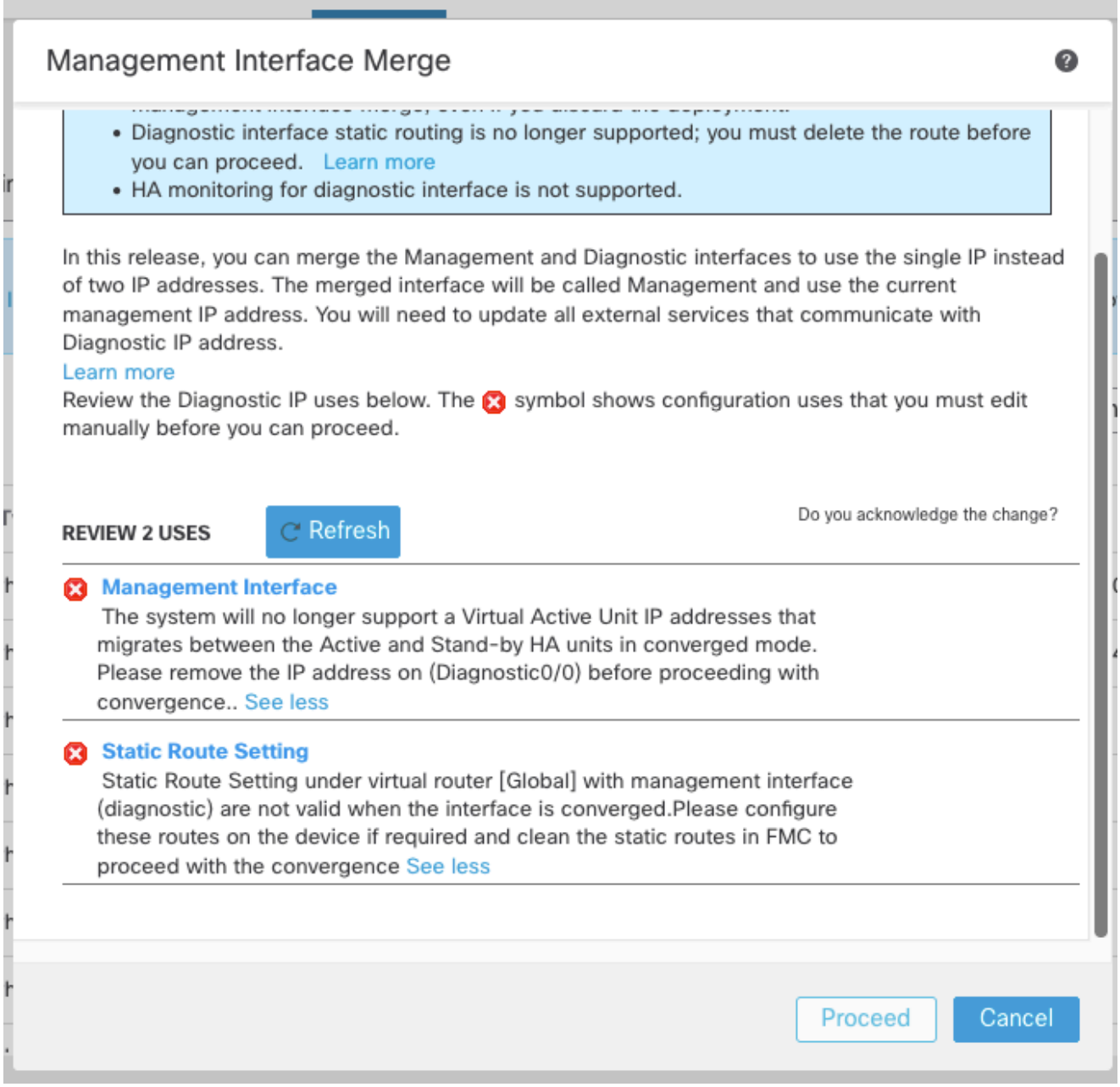


Interface de gerenciamento mesclar informações antes de continuar



Note: Para pares e clusters de alta disponibilidade, execute esta tarefa na unidade ativa/de controle. A configuração mesclada é replicada automaticamente para as unidades de standby/dados.

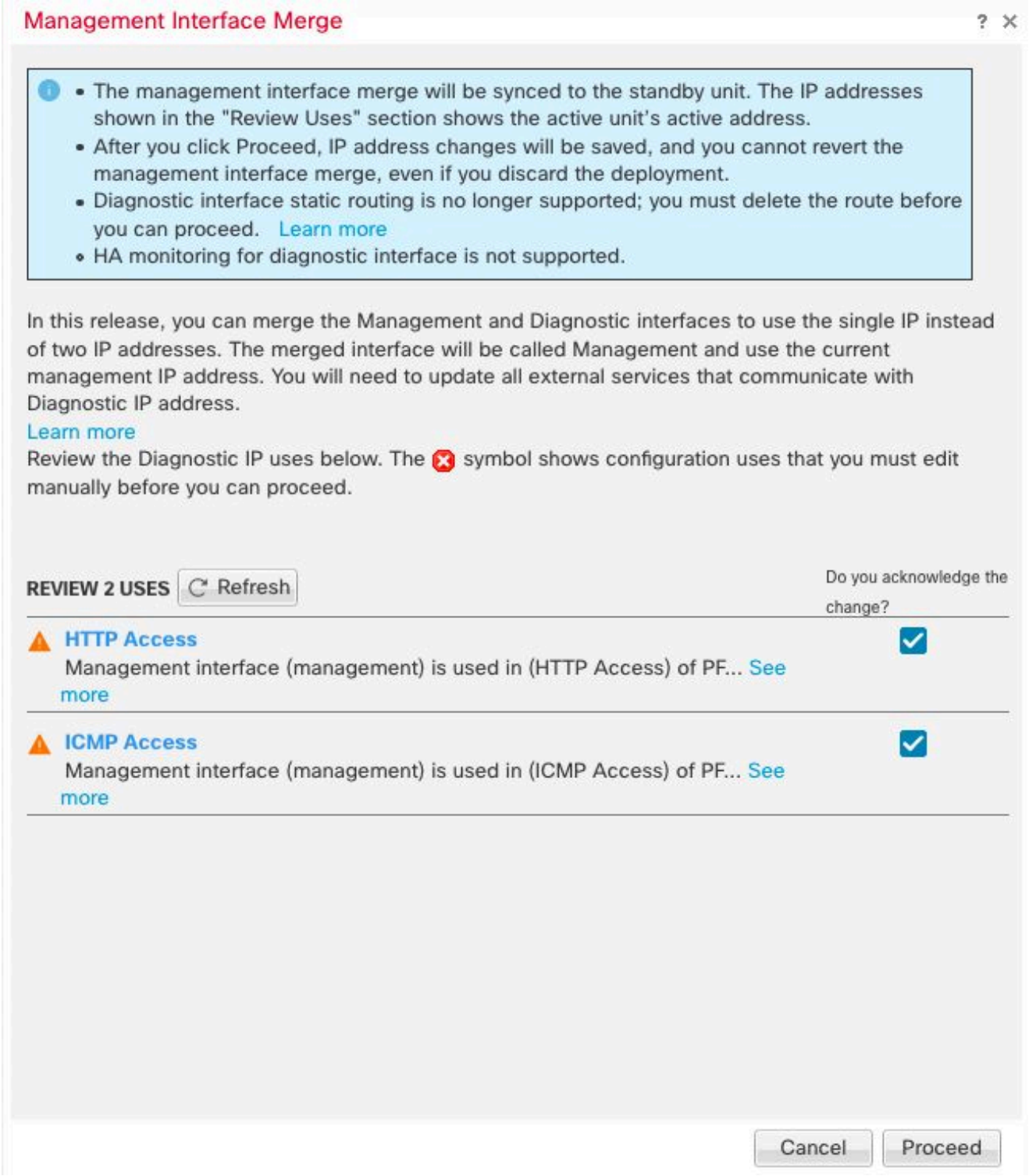
- Para qualquer ocorrência que exija alteração ou remoção manual, um ícone de aviso pode ser exibido.



Exemplo de aviso sobre as configurações que precisam ser removidas antes da mesclagem

Se for esse o caso: cancele a caixa de diálogo, prossiga com a remoção da configuração ou reconfiguração e, em seguida, reabra a caixa de diálogo Mesclagem da interface de gerenciamento.

- As configurações de plataforma que funcionarão no dispositivo serão marcadas com um ícone de cuidado e exigem confirmação.



Exemplo de aviso de configurações de configurações de plataforma que devem ser editadas

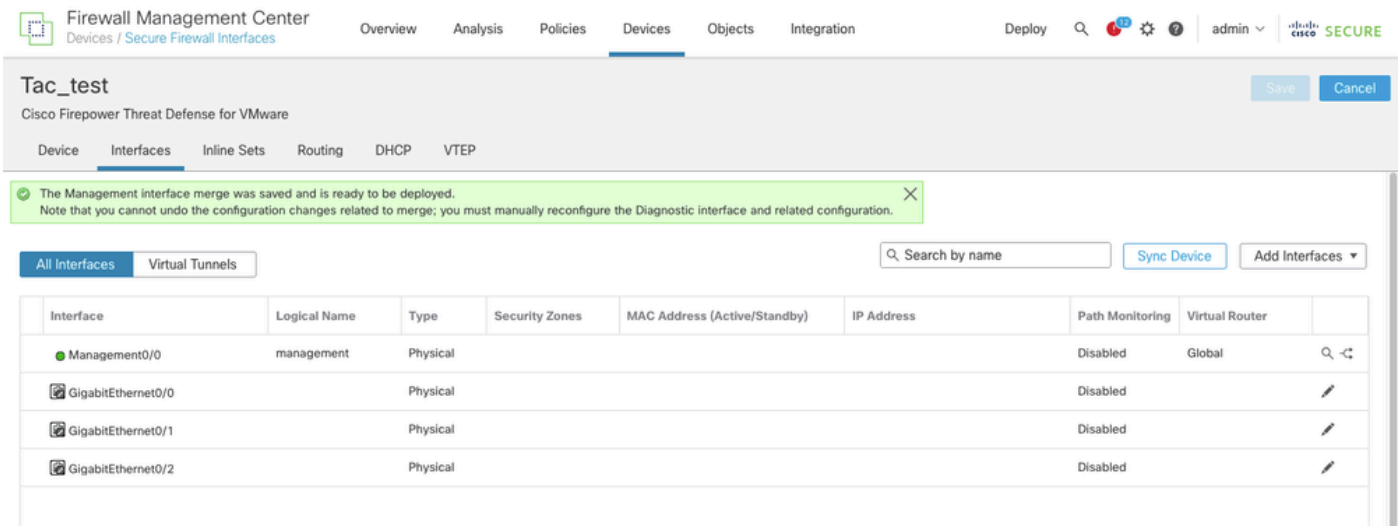
- Clique na caixa em Você reconhece a alteração? e clique em Prosseguir.

Etapa 4.

Depois que a configuração é mesclada, um banner de sucesso é mostrado:
"A mesclagem da interface de Gerenciamento foi salva e está pronta para ser implantada.
Observe que você não pode desfazer as alterações de configuração relacionadas à mesclagem;

você deve reconfigurar manualmente a interface de Diagnóstico e a configuração relacionada."

Implante a nova configuração mesclada.



A mesclagem da interface de gerenciamento foi salva e está pronta para ser implantada

A interface de gerenciamento é mostrada na página Interfaces, embora seja somente leitura.

Após a implantação, o procedimento de convergência na interface de gerenciamento é concluído.

Etapa 5. Opcional

Se você tiver serviços externos que se comunicaram com a interface de Diagnóstico, será necessário alterar a configuração deles para usar o endereço IP da interface de Gerenciamento, pois o fallback da Rota de Gerenciamento foi removido no modo convergente.

Por exemplo:

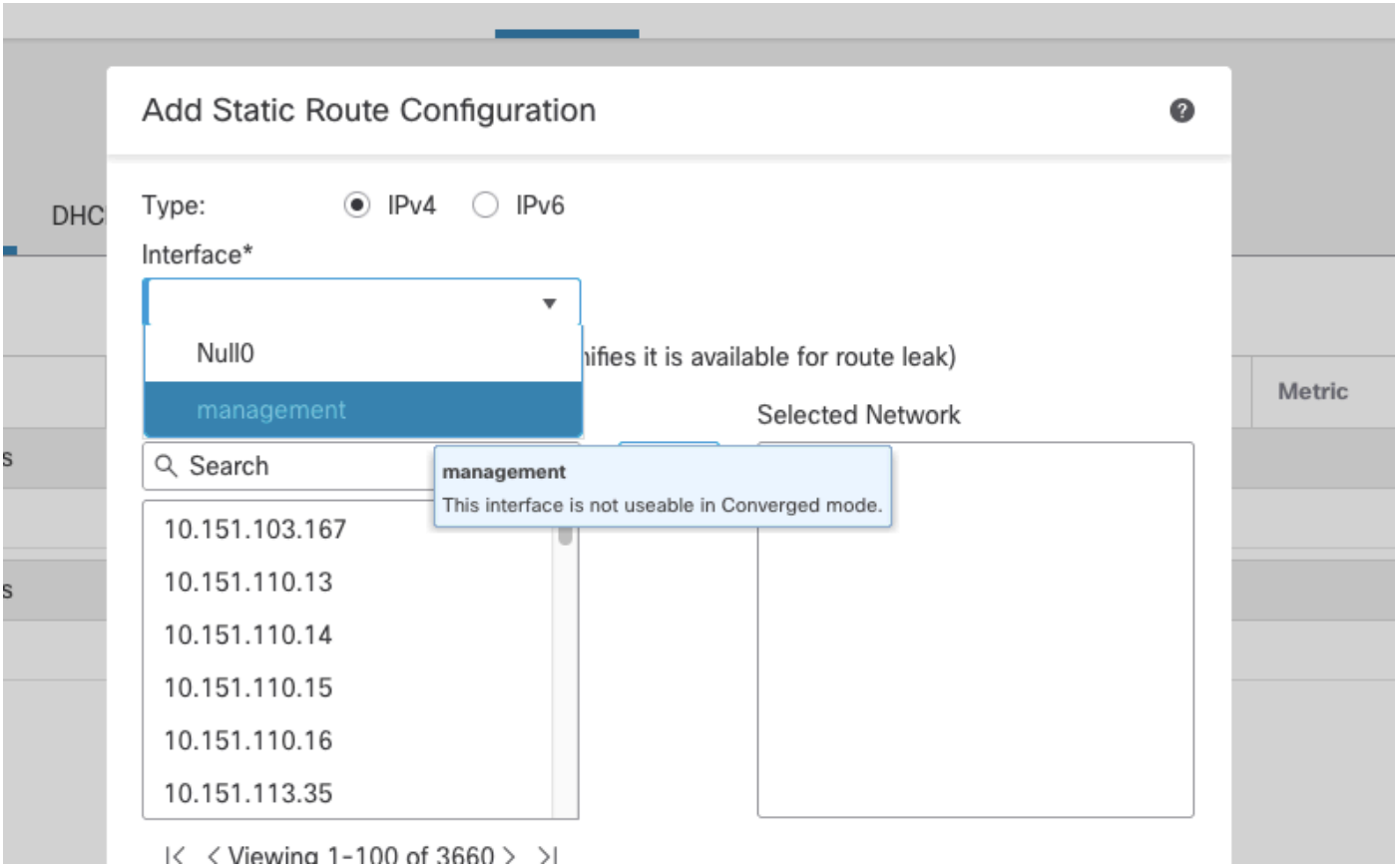
- cliente SNMP
- servidor RADIUS
- Servidor DNS para ser alcançável através da rede de gerenciamento, o usuário deve selecionar explicitamente "Habilitar pesquisa de DNS via interface de gerenciamento/diagnóstico também." em Platform Settings > DNS configuration como uma exceção é definida para consultas de DNS e ICMP (ping e traceroute): nesses casos, a defesa contra ameaças usa dados e depois retorna ao gerenciamento automaticamente se uma rota não for encontrada.

O uso de rotas estáticas para a interface de gerenciamento pode ser configurado somente através do FTD CLI Clish (Linux)

A rota padrão da porta de gerenciamento de linha envia todos os quadros para o 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
```

Na interface do FMC, a interface de gerenciamento fica acinzentada para seleção.



A interface de gerenciamento não está disponível para seleção em rotas estáticas após a conclusão da mesclagem.

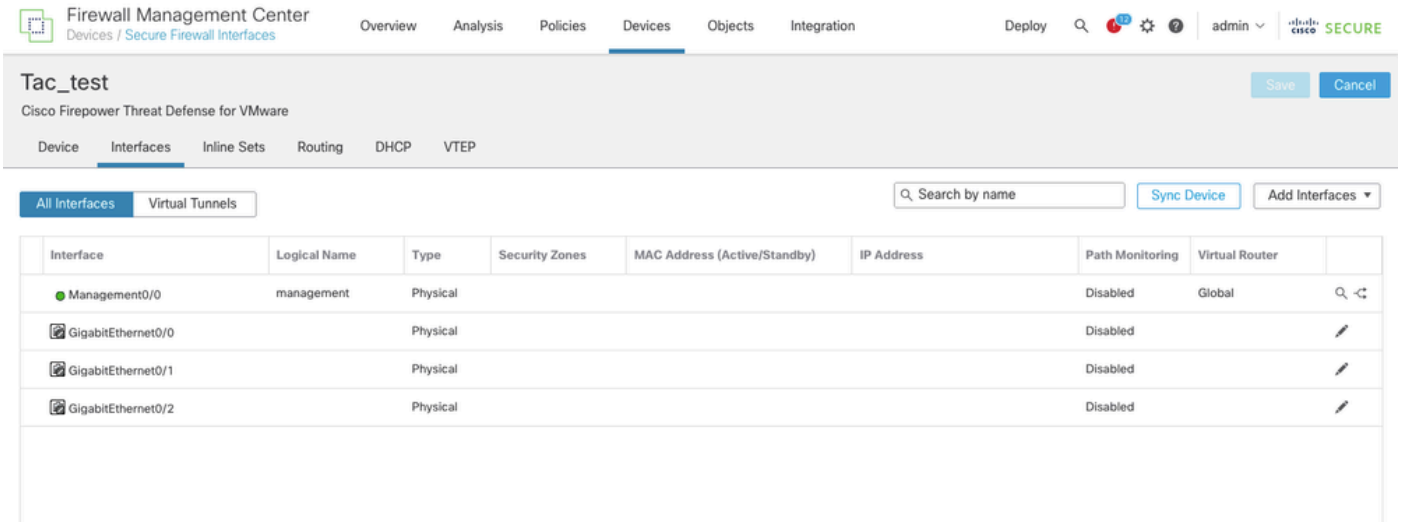
Verificar

Alterações esperadas após a mesclagem na interface de gerenciamento

- Verifique o modo de convergência em FTD CLI Clish executando o comando

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

- Na interface do FMC, o nome da interface é alterado para Management0/0 , nome lógico para management.



Mesclar confirmação no nome da Interface de Gerenciamento e no nome Lógico

- Em FTD CLI Clish, os novos endereços IP são configurados automaticamente em Lina para a interface de gerenciamento.
  O NAT é usado como uma implementação interna: Os endereços IPv4 privados internos 203.0.113.130 e IPv6 fd00:0:1:1::2 são os atribuídos (ambos sujeitos a alteração).
  Esses IPs são NATed para os endereços IPv4 e IPv6 públicos do FTD do kernel do Linux, portanto, não há mais necessidade de IPs públicos no Lina.

  No modo especialista, "ifconfig" exibe o endereço IPv4 (203.0.113.129) e IPv6 (fd00:0:1:1::1) interno 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
```

Solução de problemas - Estudo de caso

Neste caso de estudo, a interface de diagnóstico em um FTD virtual configurou endereços IP separados para conectividade com serviços externos de DNS Lookup, antes da atualização para 7.4.2.

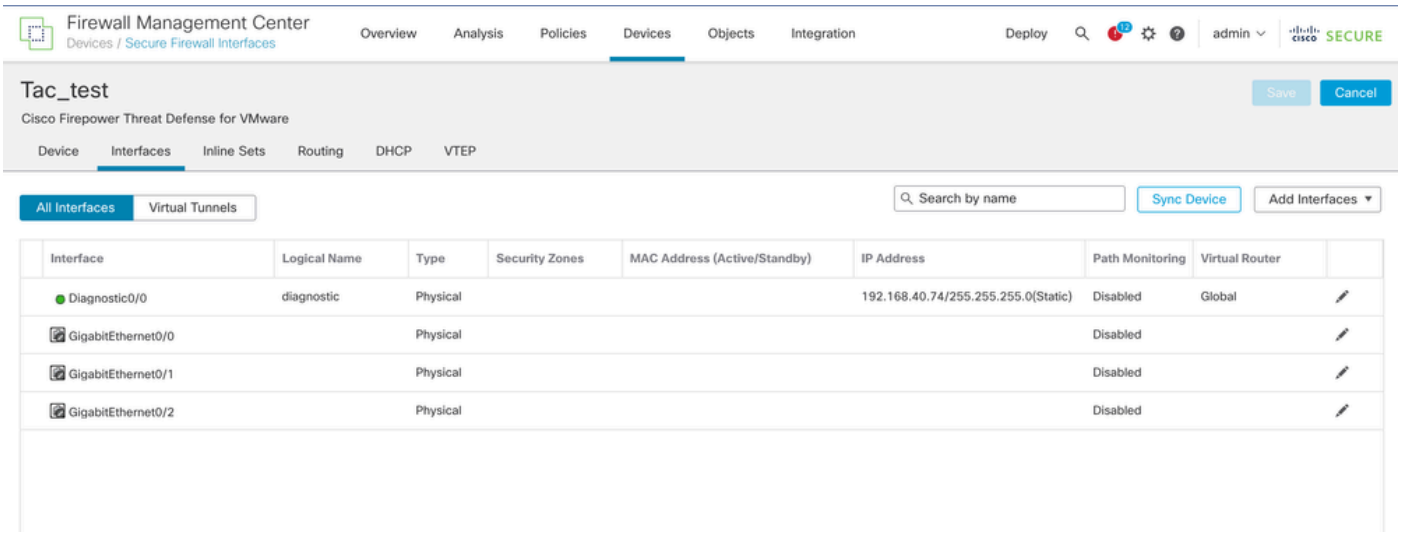
Após a atualização para a versão 7.4.2, a convergência é necessária; é assim que a configuração na interface do usuário do FMC, FTD CLI Lina e Linux é, antes e depois da fusão.

Há também capturas de tráfego no FTD CLI Lina e no Linux para mostrar o tráfego usando a movimentação da interface lógica de Diagnóstico para usar a interface de Gerenciamento.

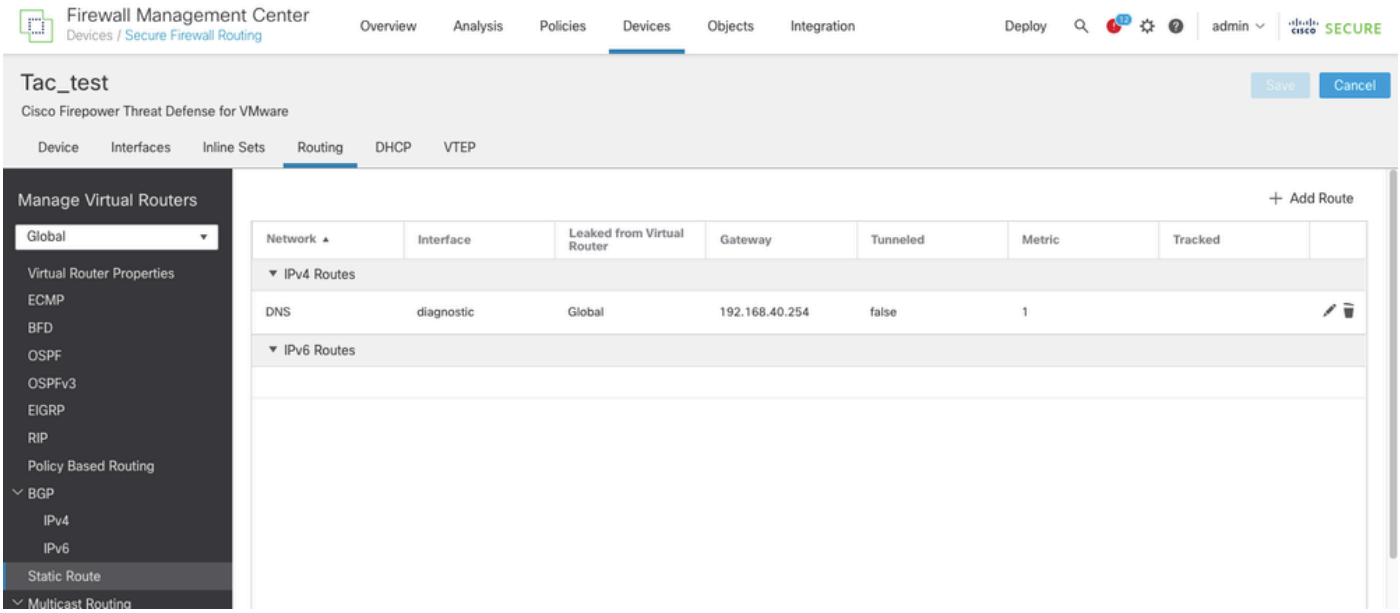
Antes da configuração de convergência

A interface de Diagnóstico tem um IP separado e uma rota estática para o DNS Lookup; dessa forma, ela funciona usando as duas interfaces lógicas de Lina para Linux no FTD.

Configuração da interface do usuário do FMC



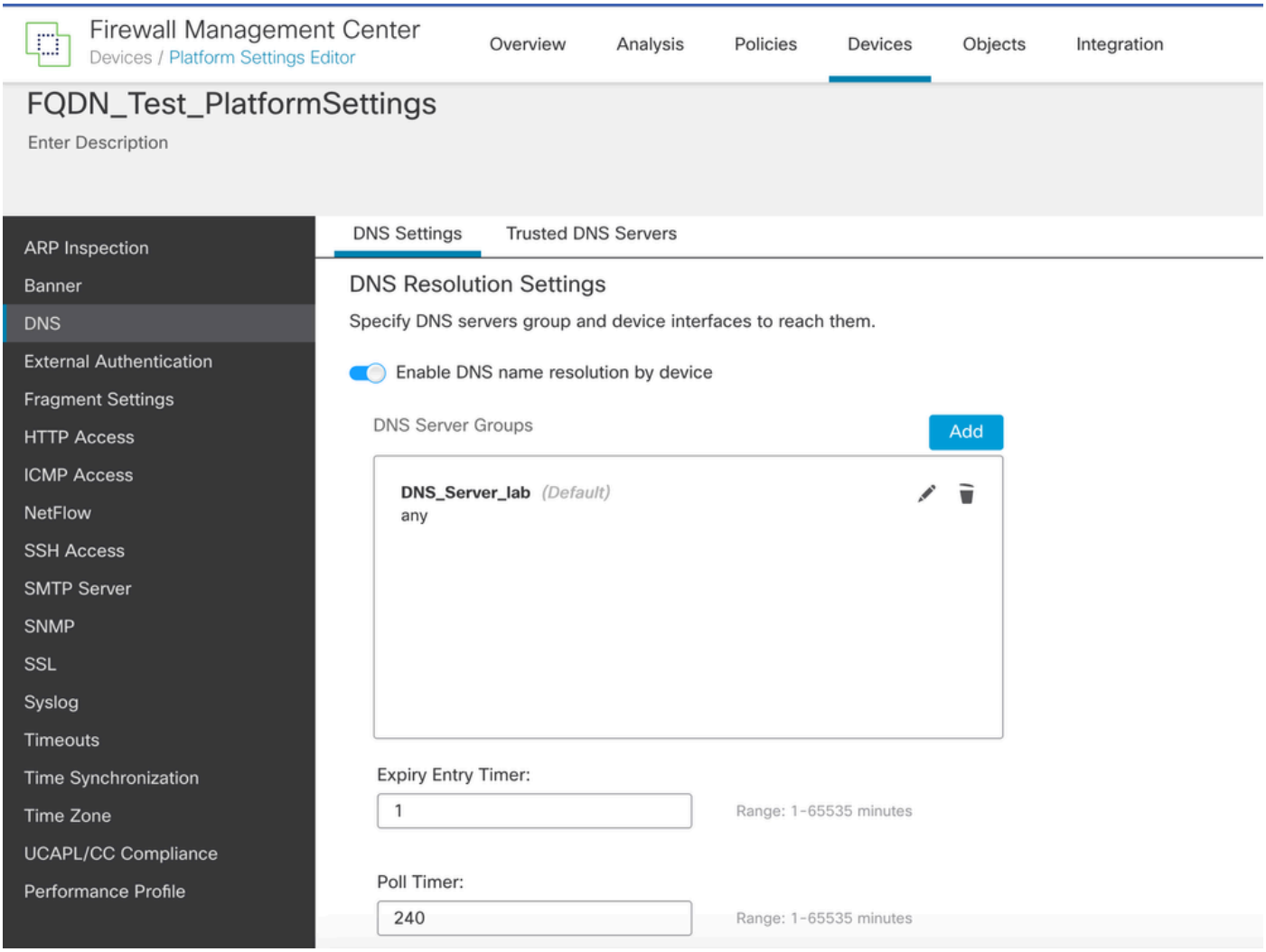
Configuração de interface de diagnóstico antes da mesclagem



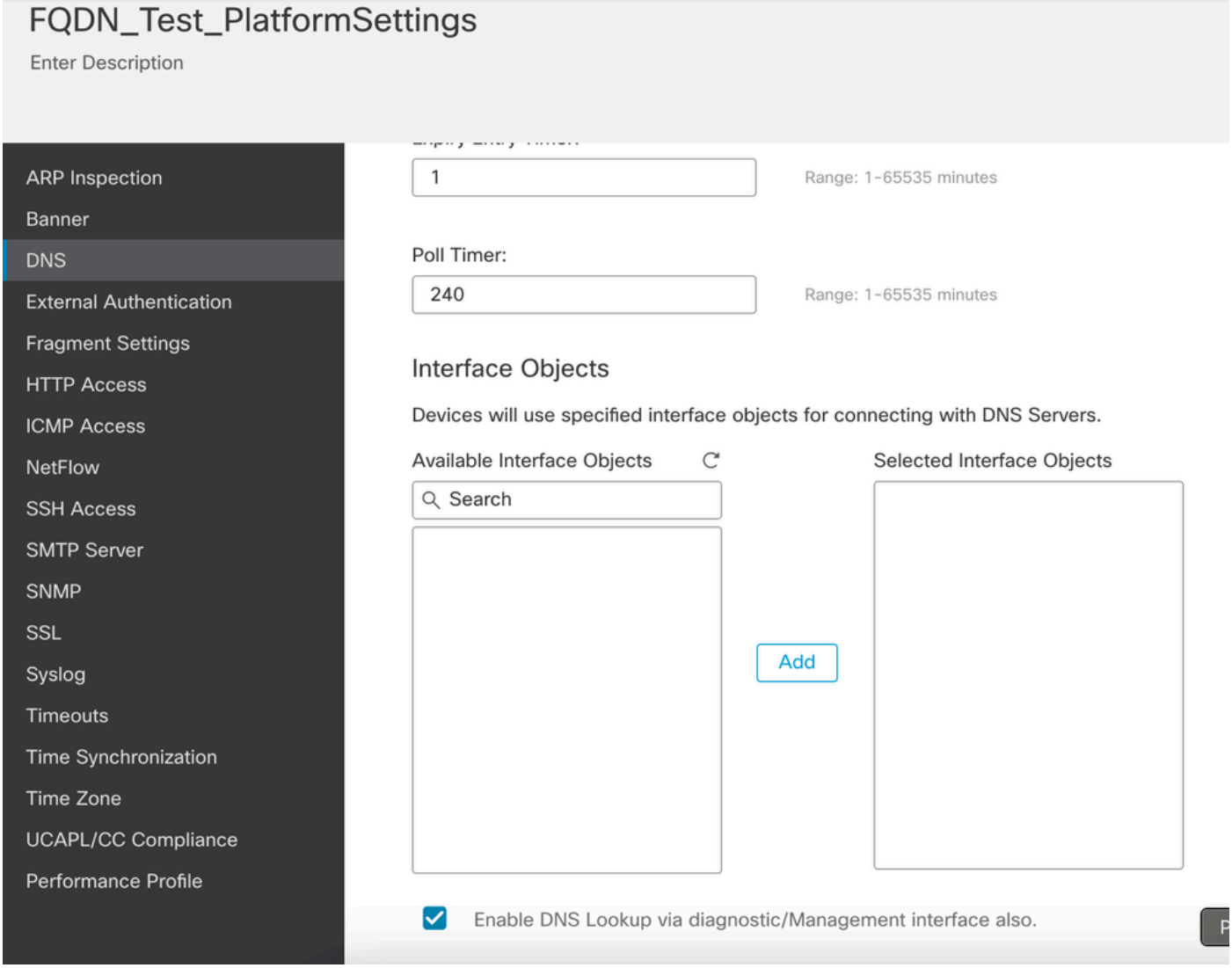
Rota estática configurada na interface de diagnóstico

configuração DNS sobre

Devices > Platform Settings, selecione a política e, em seguida, a guia DNS.



Configuração DNS em Configurações de Plataforma



Caixa de seleção marcada para Habilitar pesquisa de DNS via interface de diagnóstico/gerenciamento também

Configuração da Interface de Diagnóstico sobre 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
```

Configuração DNS em 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
```

Capturar na interface de diagnóstico o tráfego DNS que vai para o 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#
```

Capturar no modo especialista em Linux para confirmar o fluxo correto do tráfego de pesquisa de DNS na interface de gerenciamento a partir da interface 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)
```

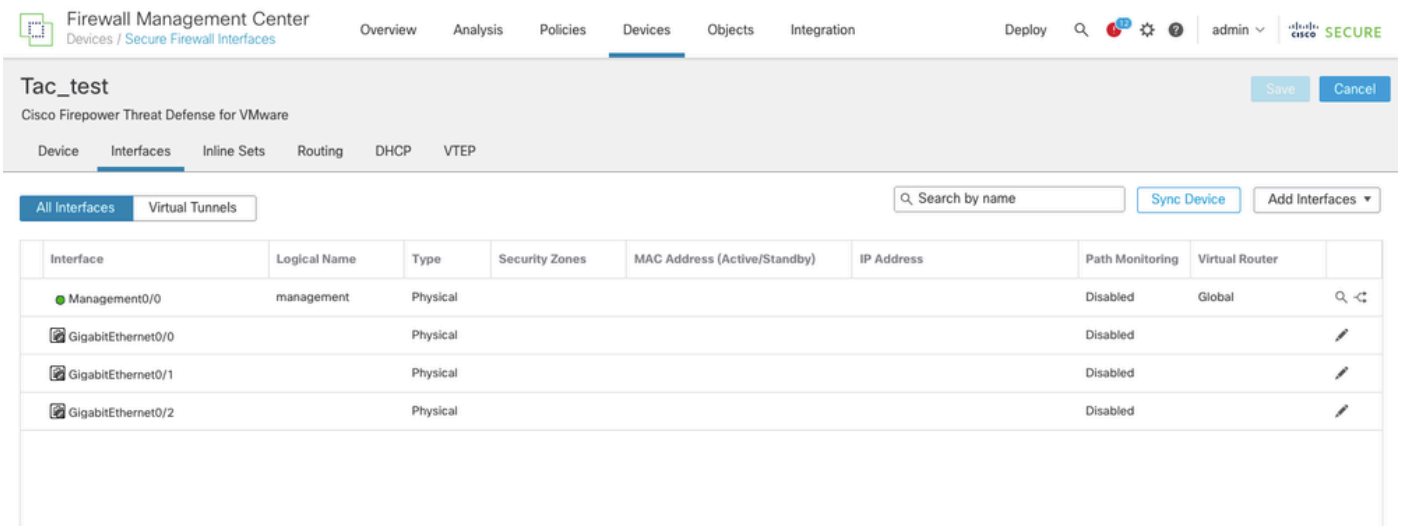
Após a configuração de convergência

Como mencionado no procedimento de convergência, para fazer a mesclagem, todas as configurações na Interface de diagnóstico devem ser removidas.

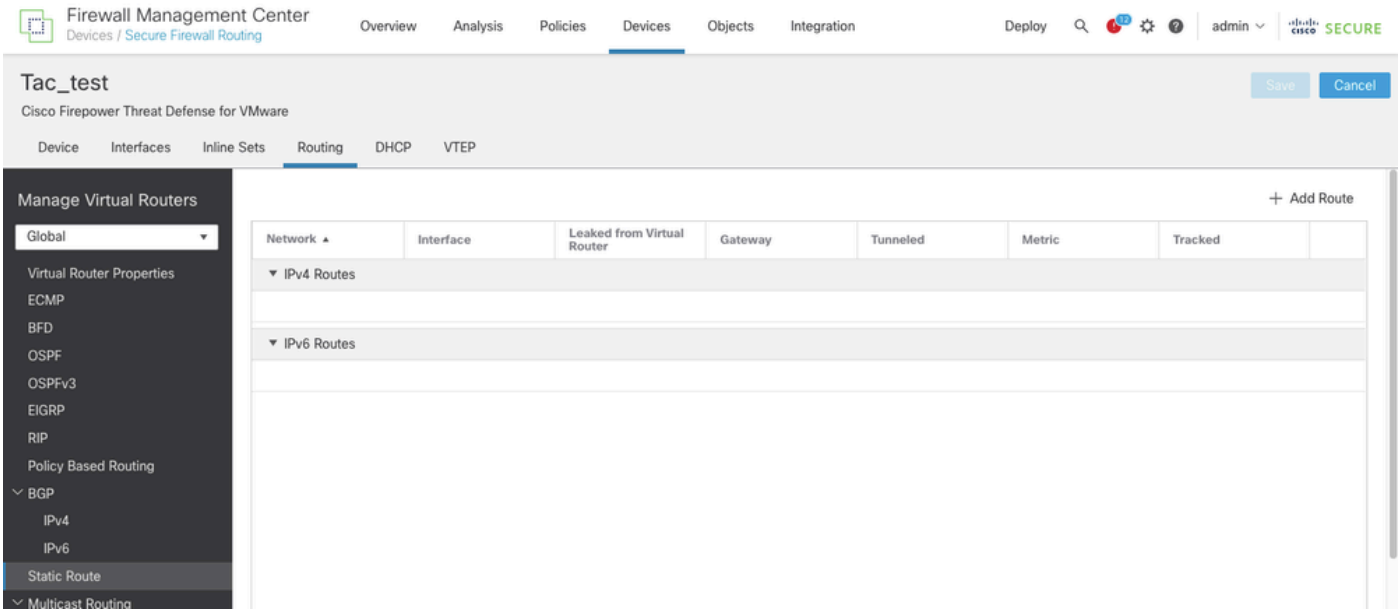
Estas são as informações no FMC e no FTD CLI quando a fusão é concluída.

Configuração da interface de gerenciamento na interface do usuário do FMC

Devices > Device Management, selecione o FTD. Ele é aberto diretamente na guia Interfaces.



Interface de gerenciamento após a mesclagem

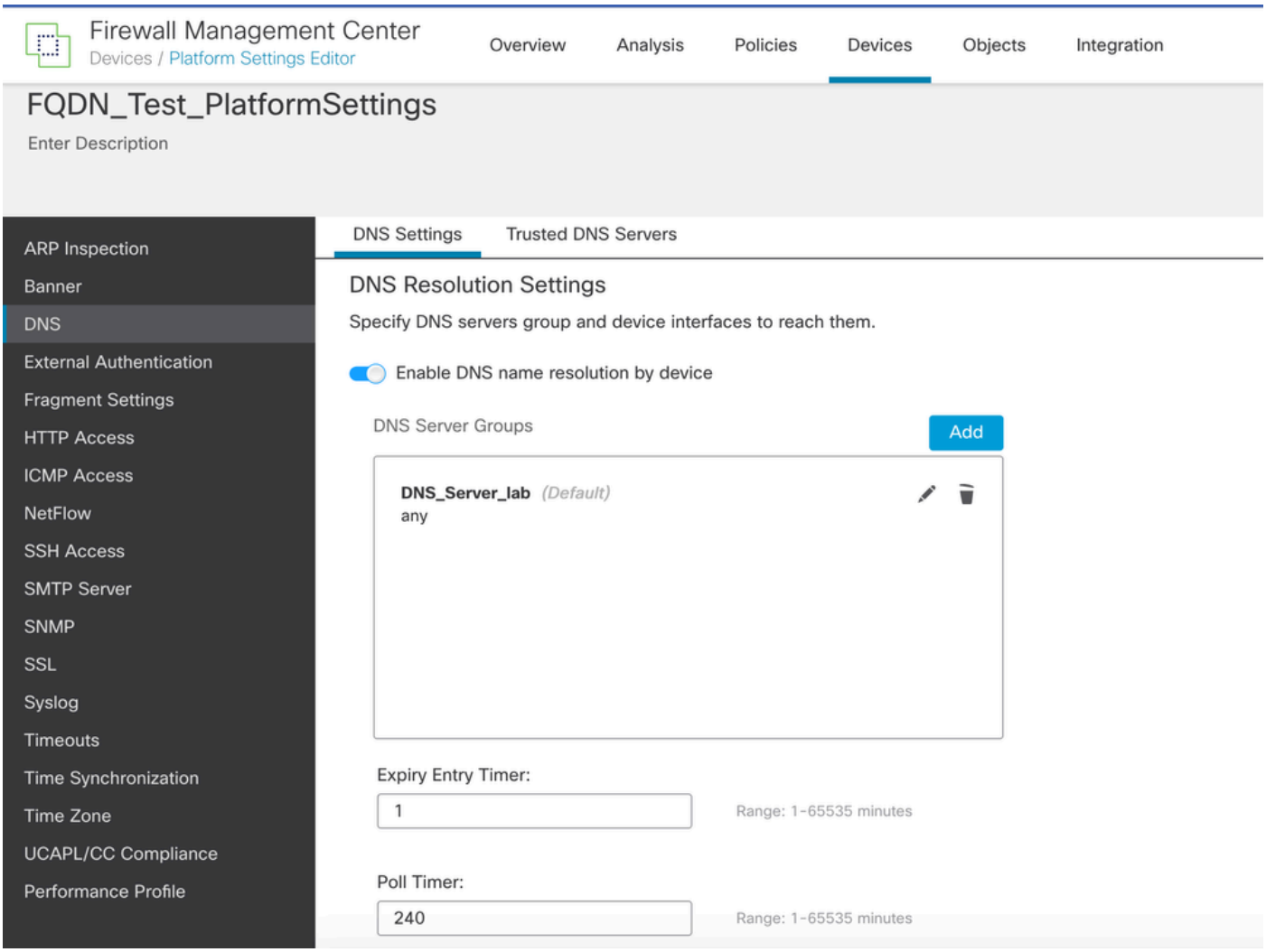


Nenhuma rota estática para o servidor DNS é adicionada

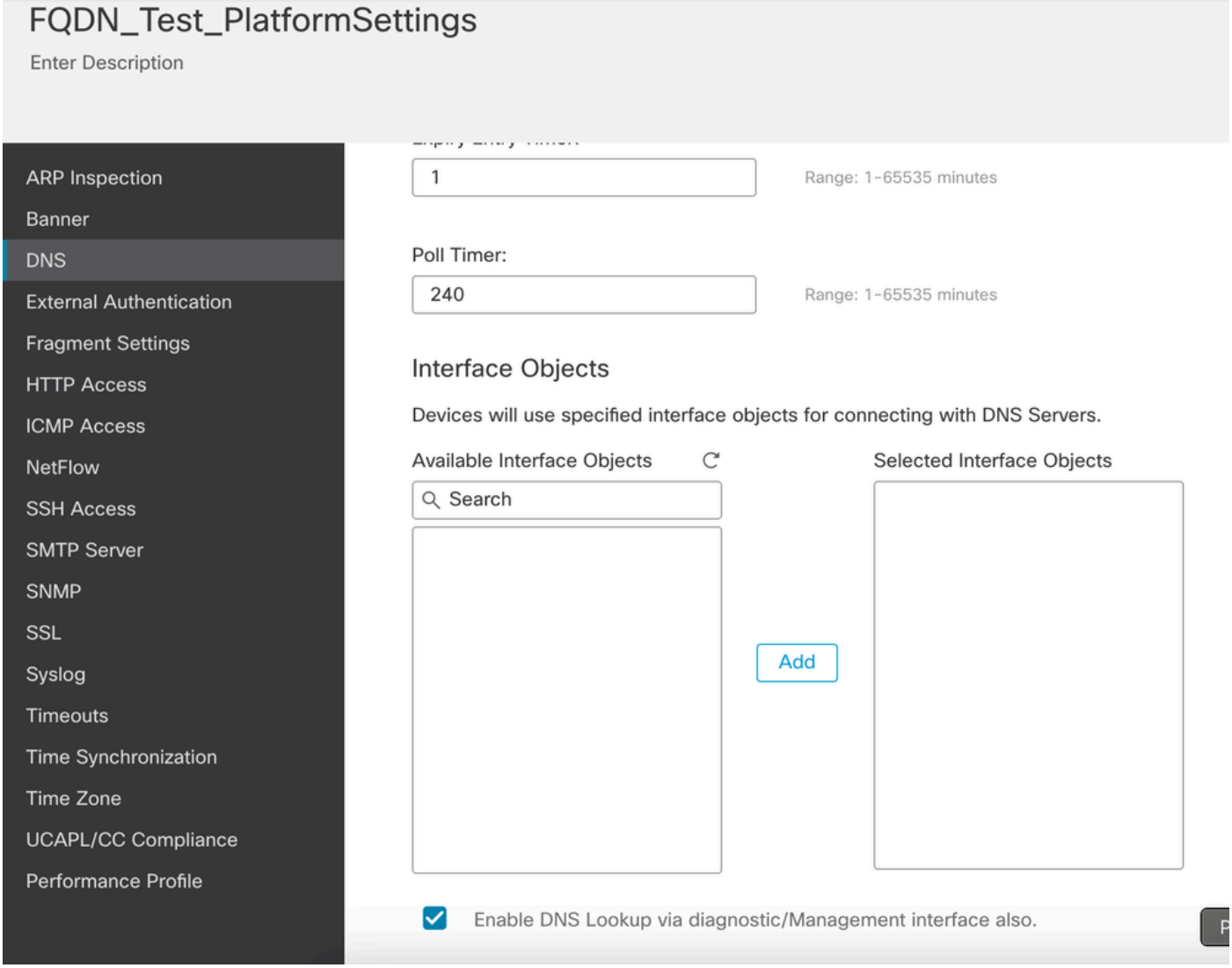
A configuração DNS deve permanecer a mesma em Configurações de plataforma.

Devices > Platform Settings, selecione a política e, em seguida, a guia DNS.

Para que a pesquisa de DNS continue a ser enviada para a interface de gerenciamento sem a necessidade de adicionar uma rota estática, o comando "Enable DNS Lookup via diagnostic/Management interface also". deve permanecer selecionado.



Configuração DNS em Configurações de Plataforma



A opção para Habilitar a Pesquisa DNS via interface de diagnóstico/Gerenciamento também deve permanecer a mesma

Configuração na CLI do 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
```

Configuração DNS na CLI FTD no 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
```

Capturar no modo especialista em Linux para confirmar o fluxo correto do tráfego de pesquisa de DNS na interface de gerenciamento.

```
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)
```

Com essa evidência, pode-se confirmar que a pesquisa de DNS continua a funcionar mesmo se nenhuma rota estática for adicionada à interface de gerenciamento via Linux.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.