Implantar interface de Dados Redundante no FTD do Azure Gerenciado pelo CD-FMC

Contents

Introdução

Este documento descreve as etapas para configurar um FTD virtual gerenciado de cdFMC para usar o recurso de interface de dados de acesso de gerenciador redundante.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall Management Center
- Cisco Defense Orchestrator

Componentes Utilizados

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

- Centro de gerenciamento de firewall fornecido em nuvem
- Virtual Secure Firewall Threat Defense versão 7.3.1 hospedada na Nuvem do Azure.

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.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- Qualquer dispositivo físico capaz de executar o Firepower Threat Defense versão 7.3.0 ou posterior.

Informações de Apoio

Este documento mostra as etapas para configurar e verificar um vFTD gerenciado por cdFMC para usar duas interfaces de dados para fins de gerenciamento. Esse recurso é frequentemente útil quando os clientes precisam de uma segunda interface de dados para gerenciar seu FTD pela Internet, usando um segundo ISP. Por padrão, o FTD faz um balanceamento de carga de rodízio para o tráfego de gerenciamento entre as duas interfaces; isso pode ser modificado para uma implantação Ativo/Backup, conforme descrito neste documento.

A interface de dados redundante para o recurso de gerenciamento foi introduzida no Secure Firewall Threat Defense versão 7.3.0. Presume-se que o vFTD tenha acessibilidade a um servidor de nomes que possa resolver URLs para acesso de CDO.

Configuração

Diagrama de Rede

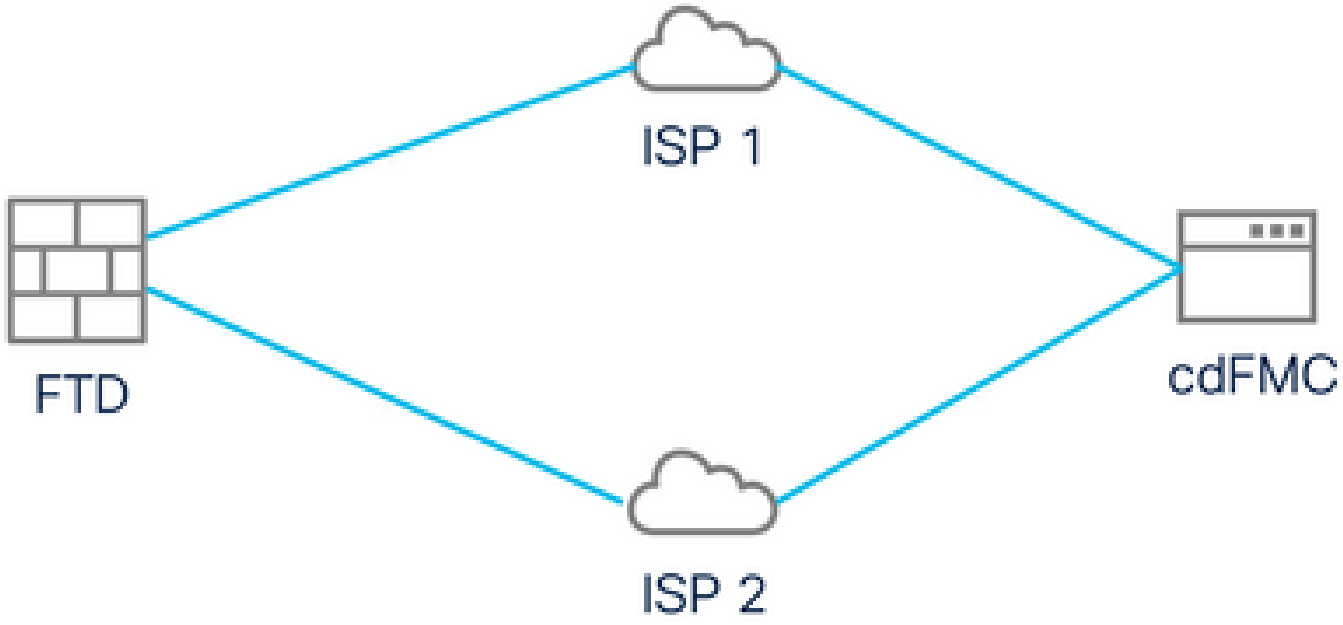


Diagrama de Rede

Configurar uma Interface de Dados para Acesso de Gerenciamento

Faça login no dispositivo através do console e configure uma das interfaces de dados para acesso de gerenciamento com o comando configure network management-data-interface:

<#root>

>

configure network management-data-interface

Note: The Management default route will be changed to route through the data interfaces. If you are conn
interface with SSH, your connection may drop. You must reconnect using the console port.

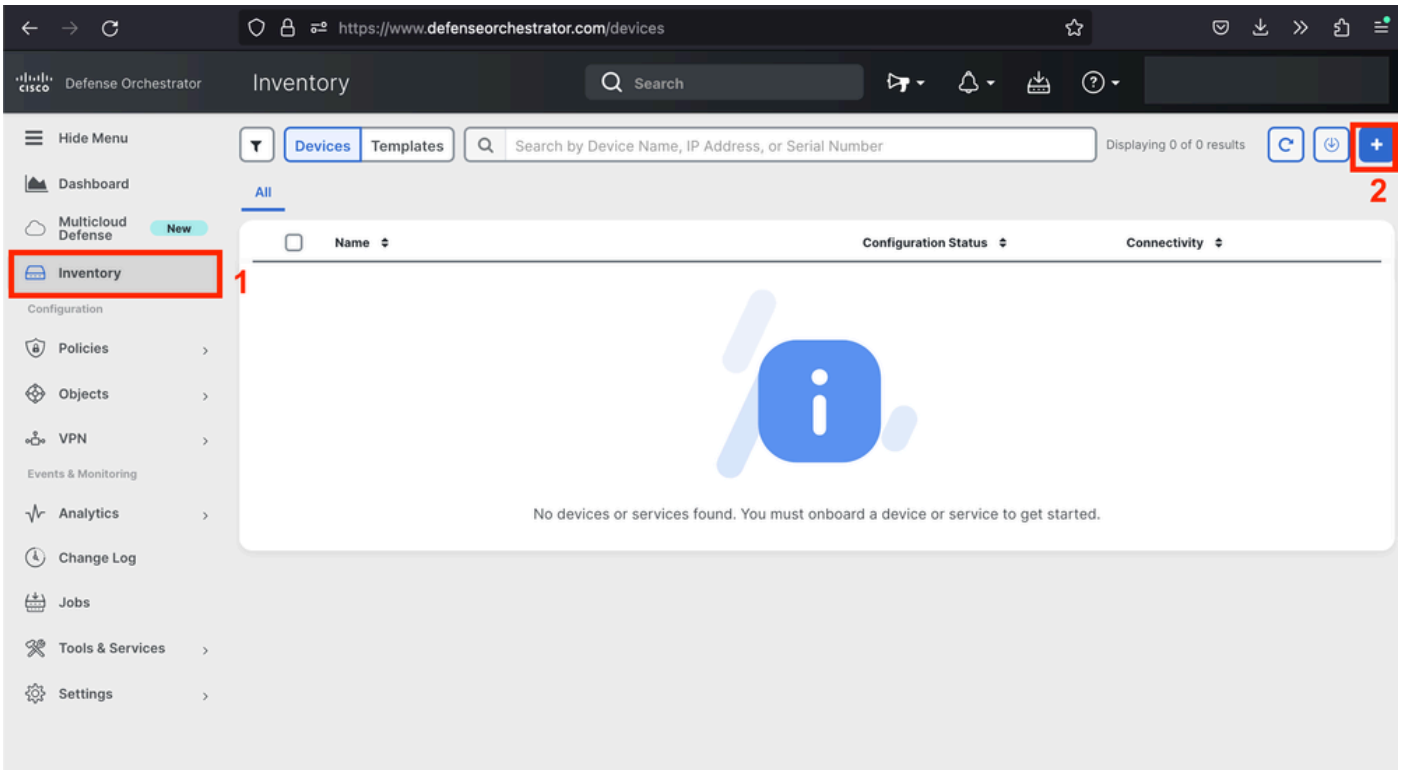
```
Data interface to use for management:

GigabitEthernet0/0

Specify a name for the interface [outside]:

outside-1

IP address (manual / dhcp) [dhcp]:

manual

IPv4/IPv6 address:

10.6.2.4

Netmask/IPv6 Prefix:

 255.255.255.0

Default Gateway:

10.6.2.1
```

Lembre-se de que a interface de gerenciamento original não pode ser configurada para usar DHCP. Você pode usar o comando show network para verificar isso.

Integrar o FTD com CDO

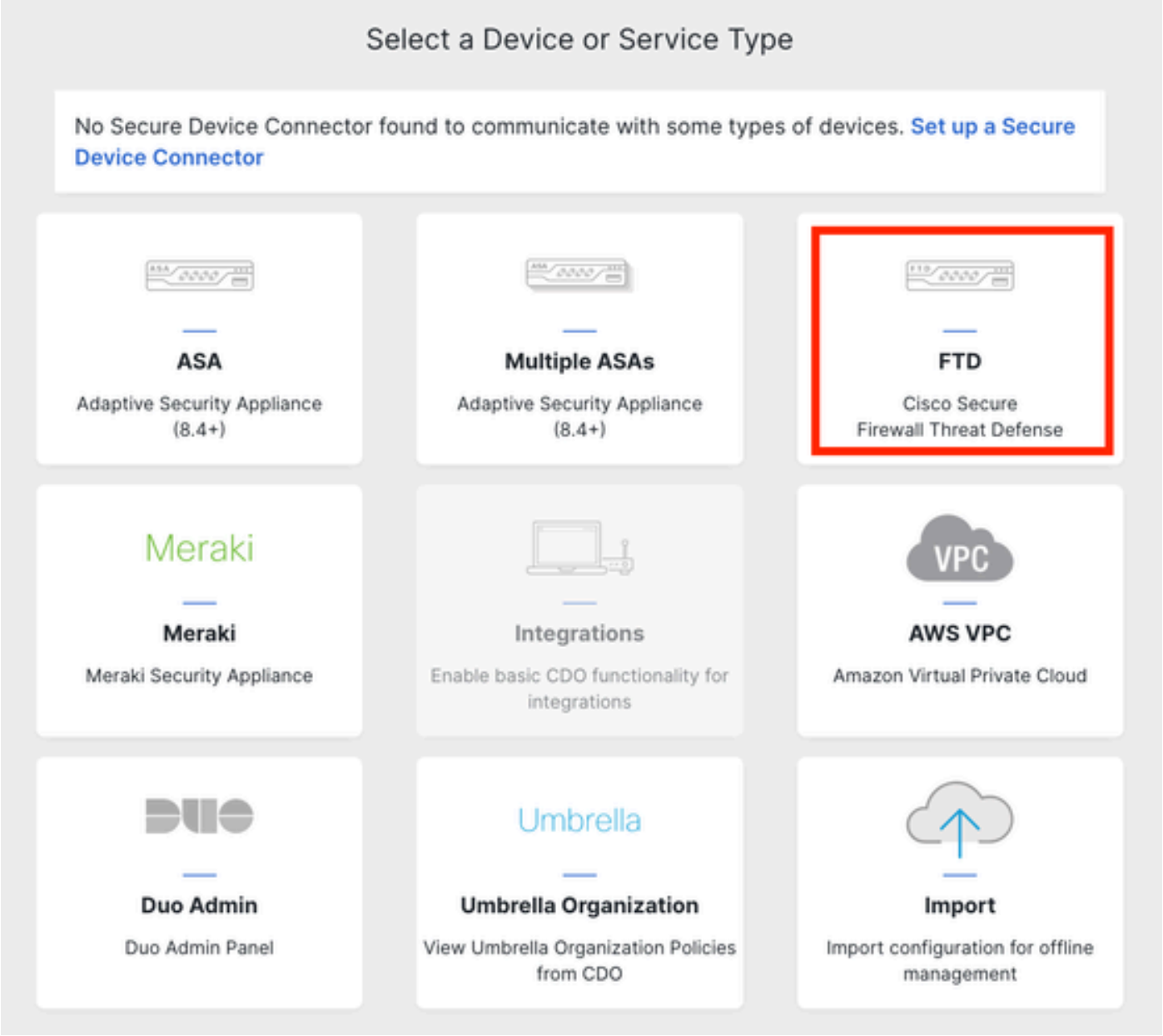
Este processo integra o FTD do Azure com CDO para que possa ser gerenciado por um FMC fornecido na nuvem. O processo usa uma chave de registro CLI, que é útil se o dispositivo tiver um endereço IP atribuído via DHCP. Outros métodos integrados, como o provisionamento por toque de registro e o número de série, são suportados apenas nas plataformas Firepower 1000, Firepower 2100 ou Secure Firewall 3100.

Etapa 1. No portal do CDO, navegue para Inventory e clique na opção Onboard :



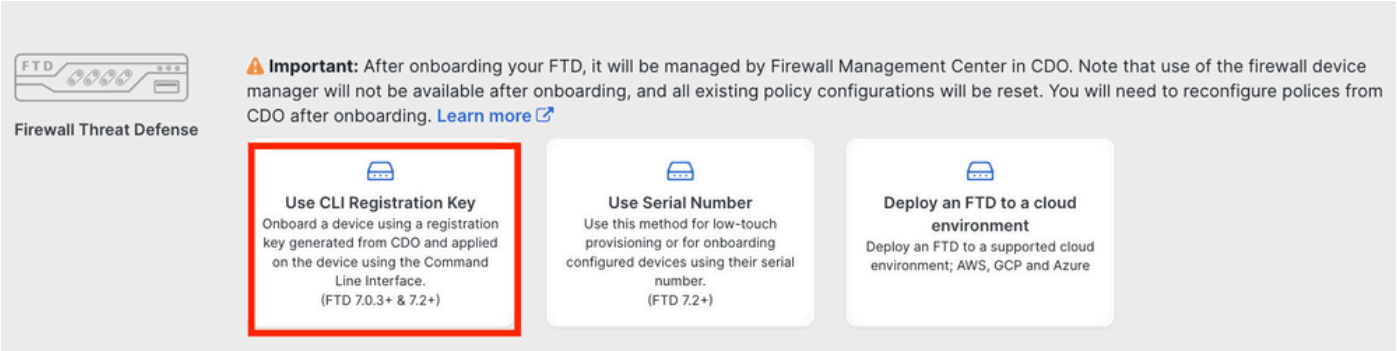
Página Inventário

Etapa 2. Clique no bloco FTD:



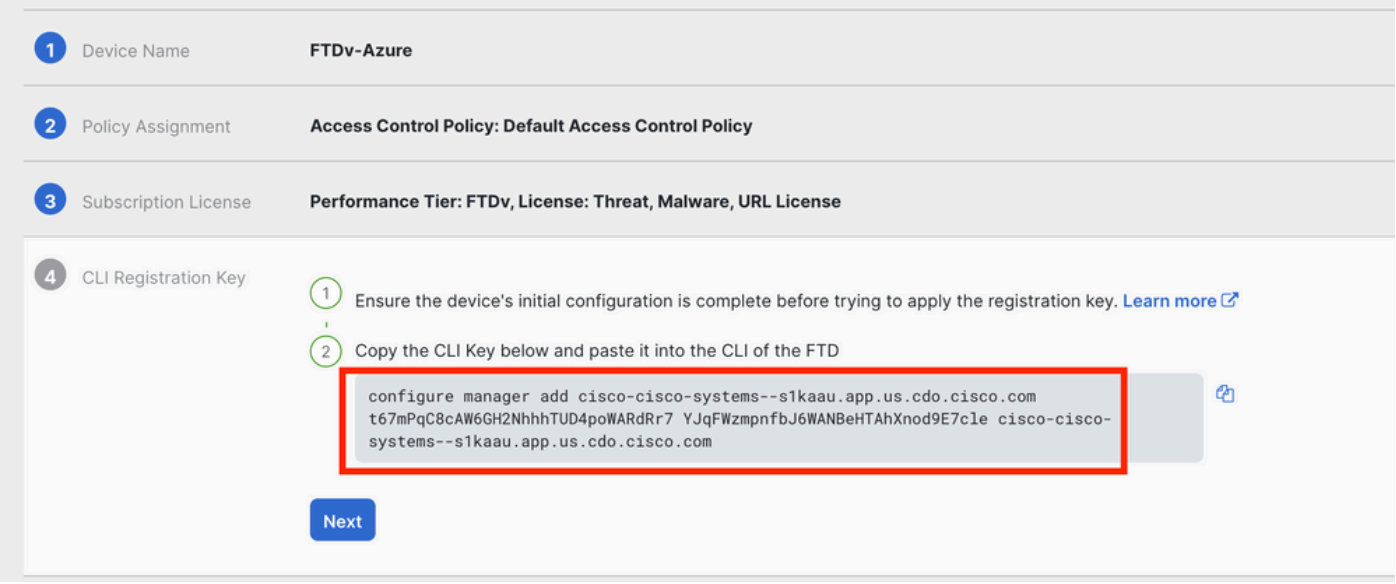
Integração do FTD

Etapa 3. Escolha a opção Use CLI Registration key:

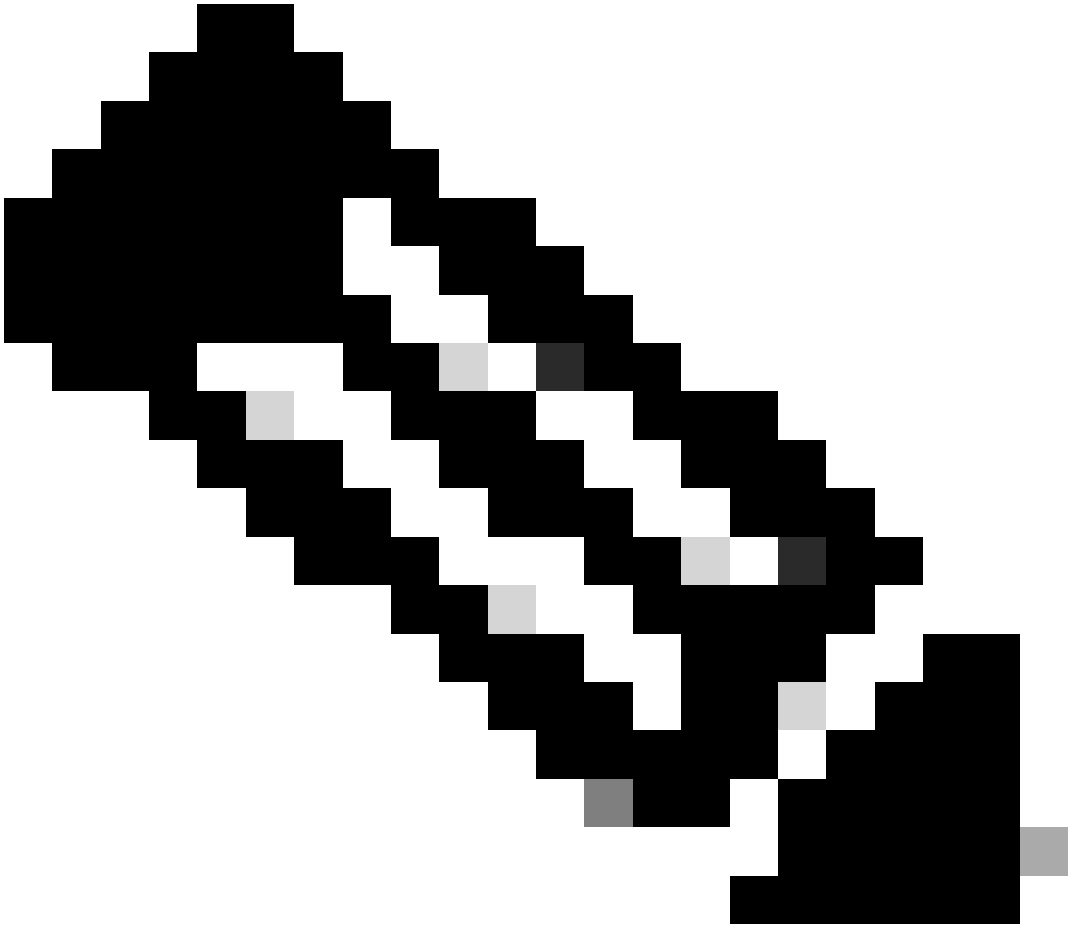


Usar a chave de registro CLI

Etapa 4. Copie a chave CLI começando pelo comando configure manager:



Comando Copiar Gerenciador de Configuração



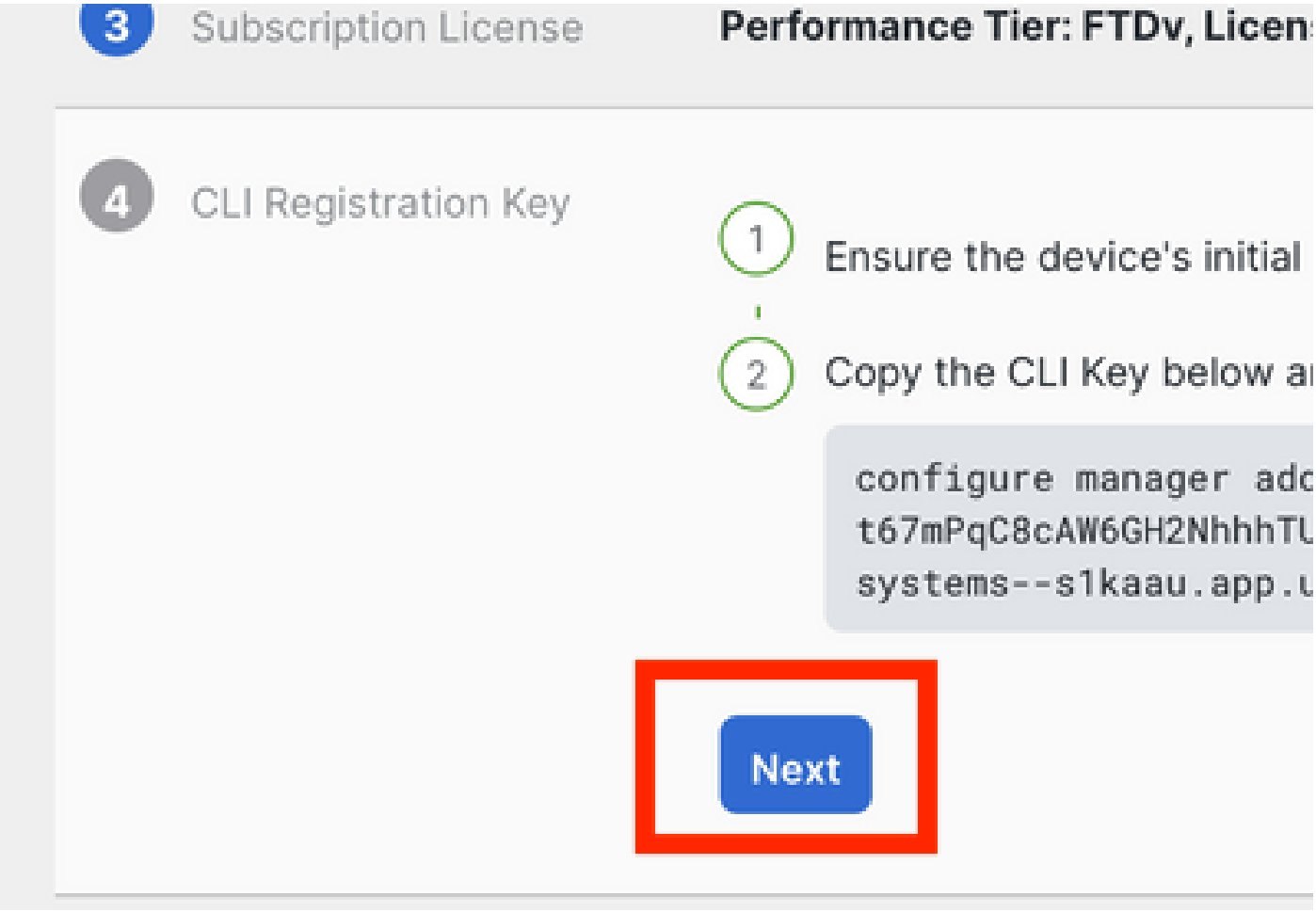
Observação: a chave CLI corresponde ao formato usado nos registros de FTDs com

FMCs no local, onde você pode configurar um NAT-ID para permitir o registro quando seu dispositivo gerenciado estiver atrás de um dispositivo NAT: configure manager add <fmc-hostname-or-ipv4> <registration-key> <nat-id> <display-name>

Etapa 5. Cole o comando na CLI do FTD. Você deverá receber esta mensagem se a comunicação for bem-sucedida:

```
Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

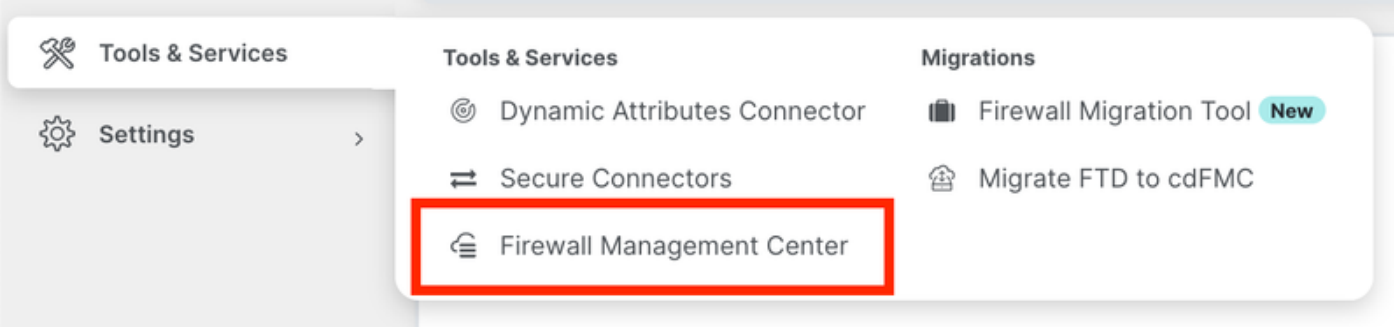
Etapa 6. Volte para o CDO e clique em Avançar:



Clique em Next

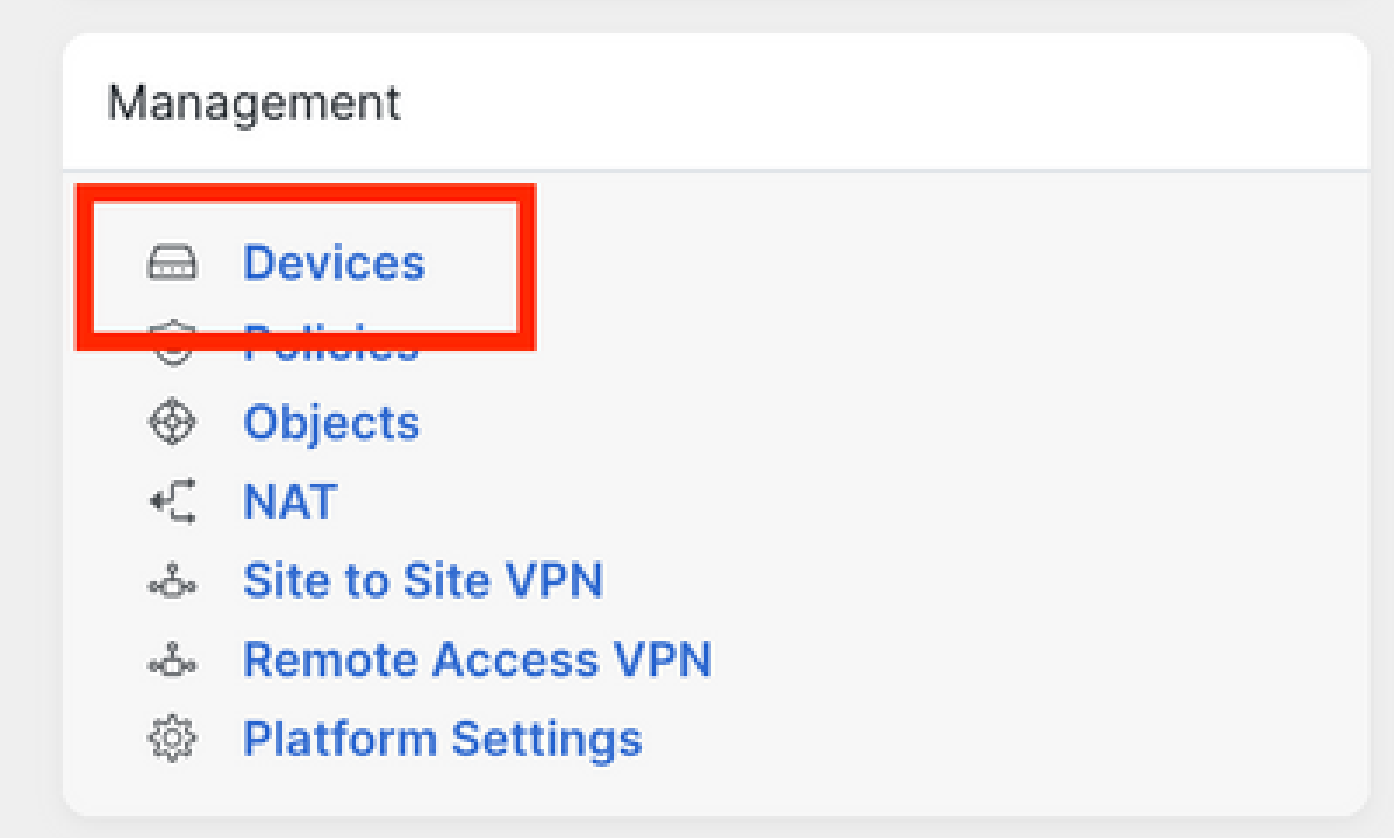
O CDO continua o processo de inscrição e uma mensagem é exibida mencionando que levará muito tempo para ser concluída. Você pode verificar o status do processo de inscrição clicando no link Devices na página Services.

Passo 7. Acesse o FMC pela página Tools & Services.



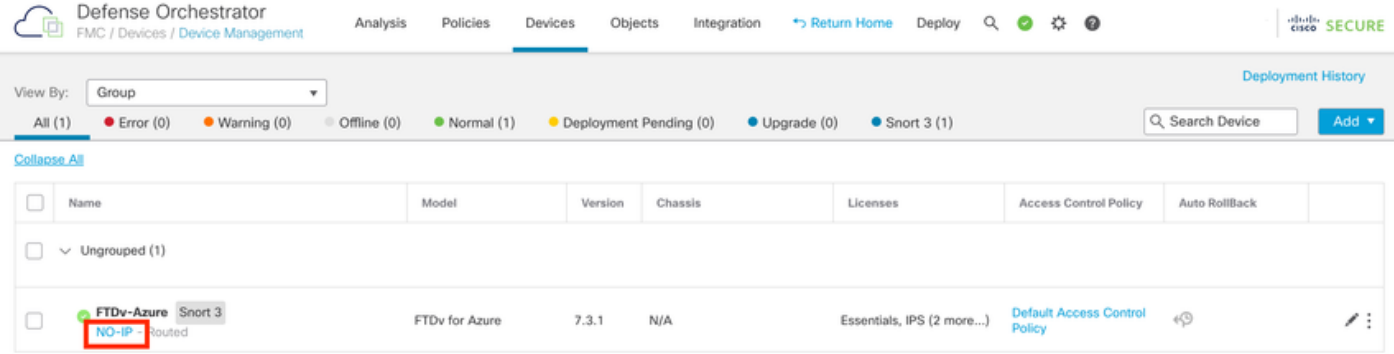
Acesso ao cdFMC

Clique no link Devices.



Clique em Dispositivos

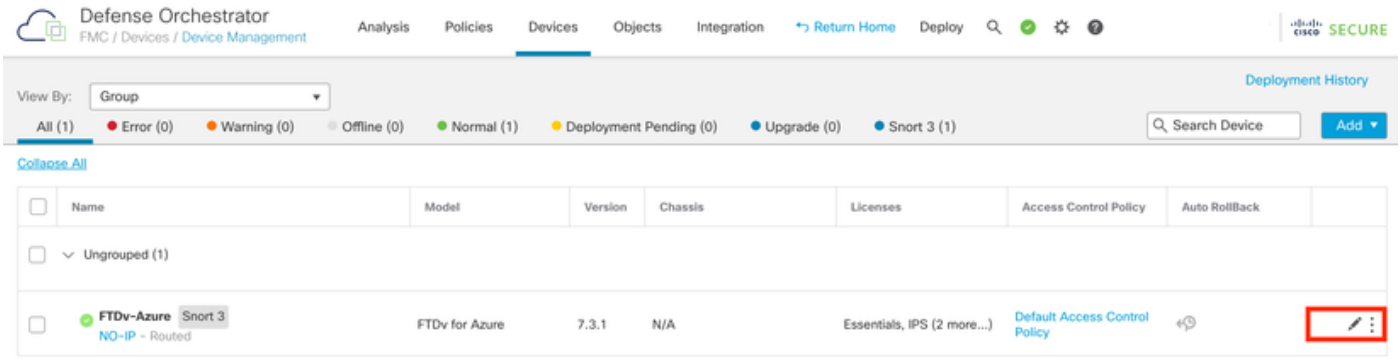
Seu FTD agora está integrado no CDO e pode ser gerenciado pelo FMC fornecido na nuvem. Observe na próxima imagem que há um NO-IP listado sob o nome do dispositivo. Isso é esperado em um processo de integração usando a chave de registro CLI.



Configurar uma interface de dados redundante para acesso do gerente

Esse processo atribui uma segunda interface de dados para acesso de gerenciamento.

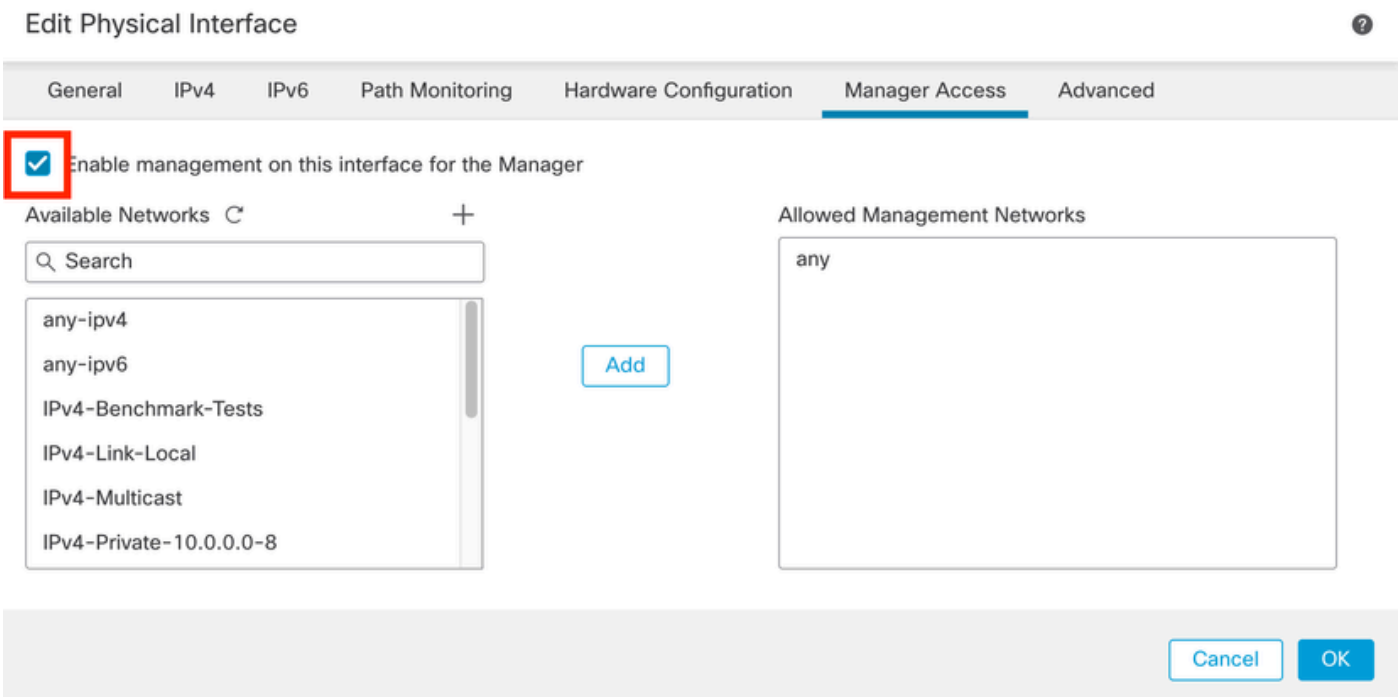
Etapa 1. Na guia Devices, clique no ícone do lápis para acessar o modo de edição do FTD:



Editar o FTD

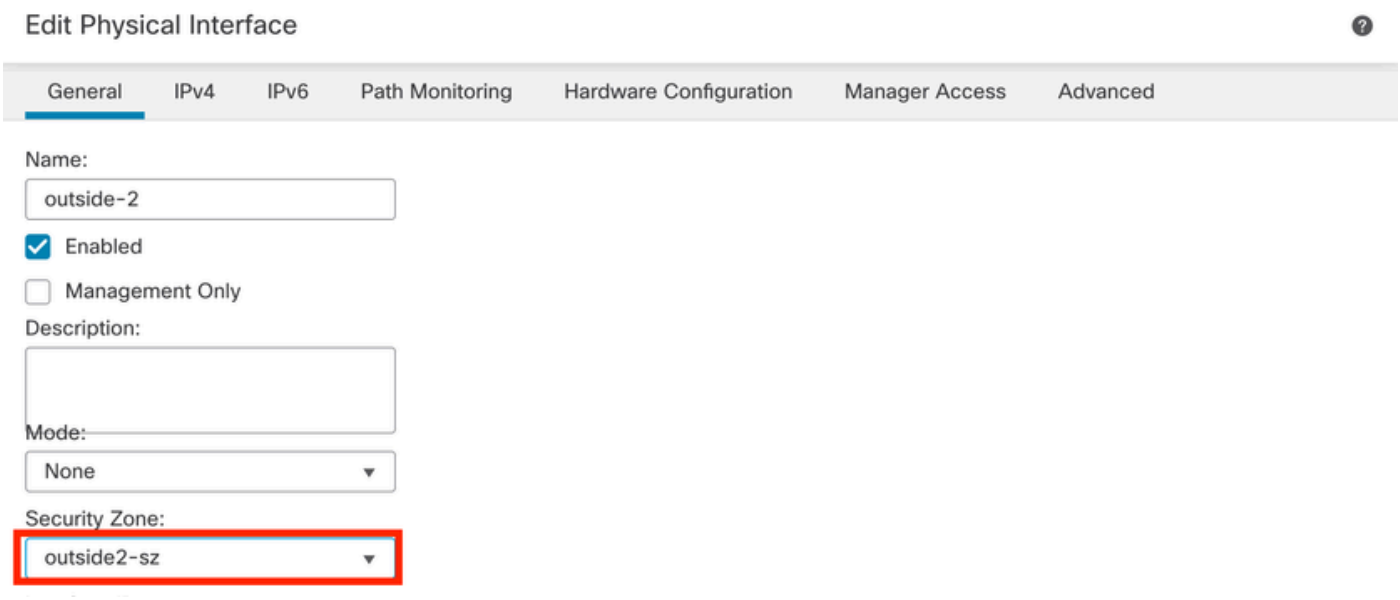
Etapa 2. Na guia Interface, edite a interface que será atribuída como a interface de gerenciamento redundante. Se isso não tiver sido feito anteriormente, configure um nome de interface e um endereço IP.

Etapa 3. Na guia Acesso do gerente ative a caixa de seleção Habilitar gerenciamento nesta interface para o gerente:



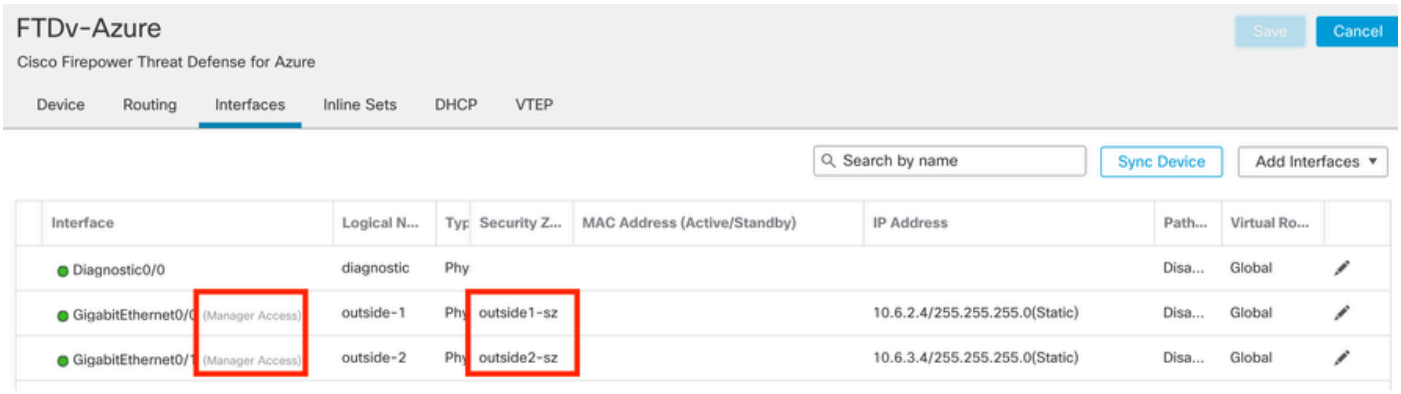
Ativando o acesso do gerente

Etapa 4. Na guia Geral, verifique se a interface está atribuída a uma zona de segurança e clique em OK:



Zona de segurança para interface de dados redundante

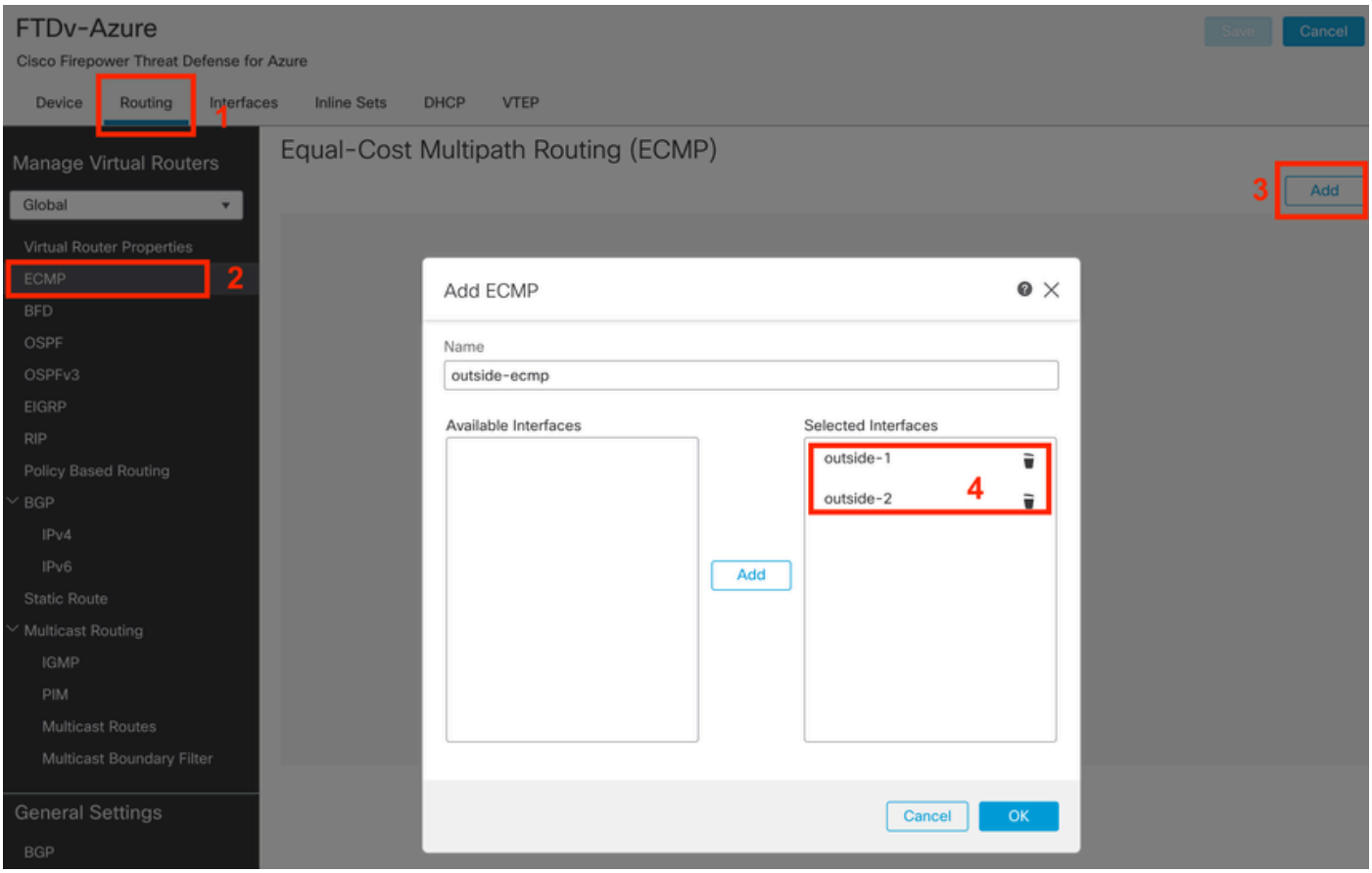
Etapa 5. Observe que agora ambas as interfaces têm a marca Acesso de gerenciador. Além disso, certifique-se de que a interface de dados primária tenha sido atribuída a uma Zona de segurança diferente:



Revisão da configuração da interface

Na próxima seção, as etapas de 6 a 10 têm como objetivo configurar duas rotas padrão de custo igual para acessar o CDO, cada uma sendo monitorada por um processo de rastreamento de SLA independente. O rastreamento de SLA garante que haja um caminho funcional para comunicação com o cdFMC usando a interface monitorada.

Etapa 6. Navegue até a guia Routing e, no menu ECMP, crie uma nova zona ECMP com ambas as interfaces:

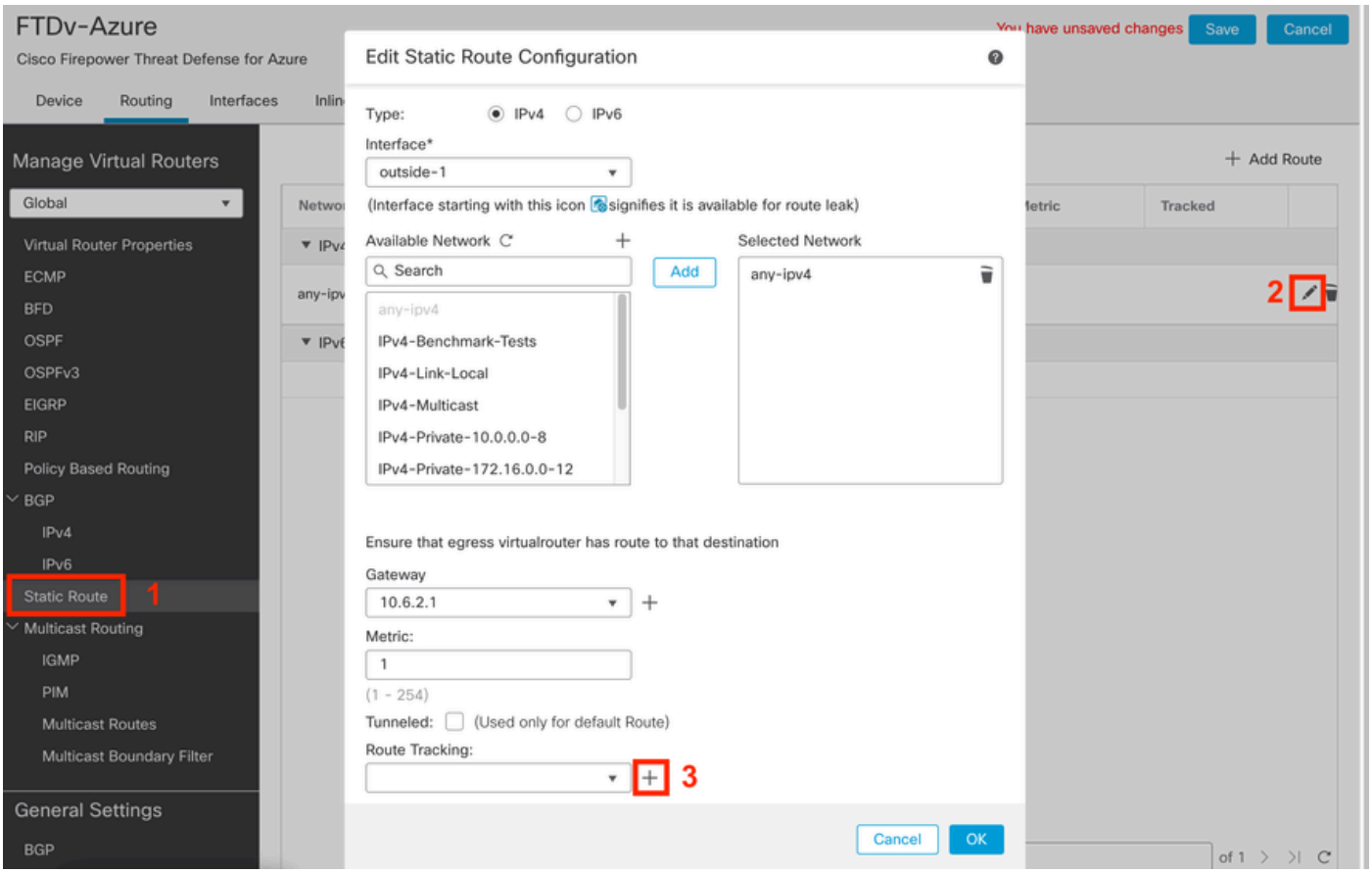


Configurar uma região ECMP

Clique em OK e em Salvar.

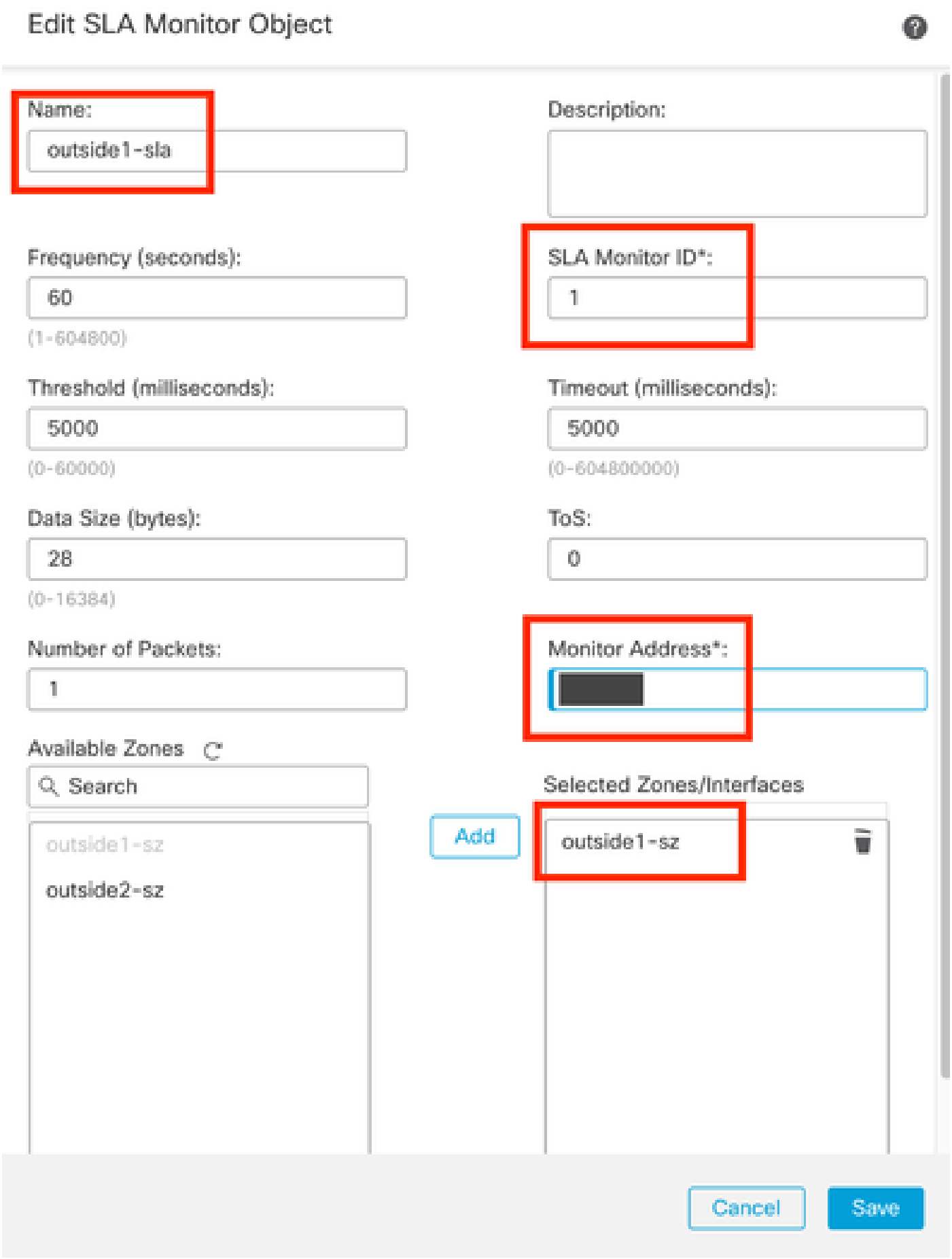
Passo 7. Na guia Roteamento, navegue até Rotas estáticas.

Clique no ícone do lápis para editar sua rota principal. Em seguida, clique no sinal de mais para adicionar um novo objeto de rastreamento de SLA:



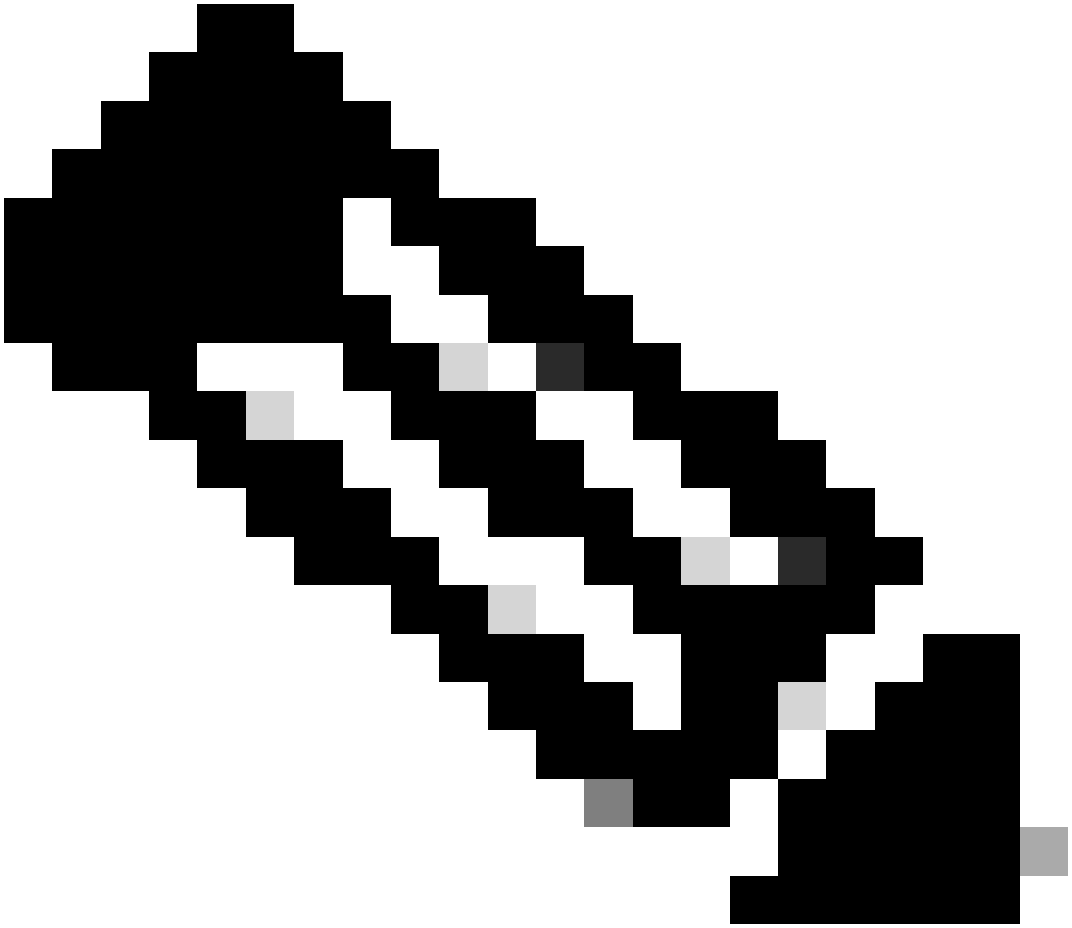
Editar rota primária para adicionar o rastreamento de SLA

Etapa 8. Os parâmetros necessários para um rastreamento de SLA funcional são destacados na próxima imagem. Opcionalmente, você pode ajustar outras configurações como Número de pacotes, Tempo limite e Frequência.



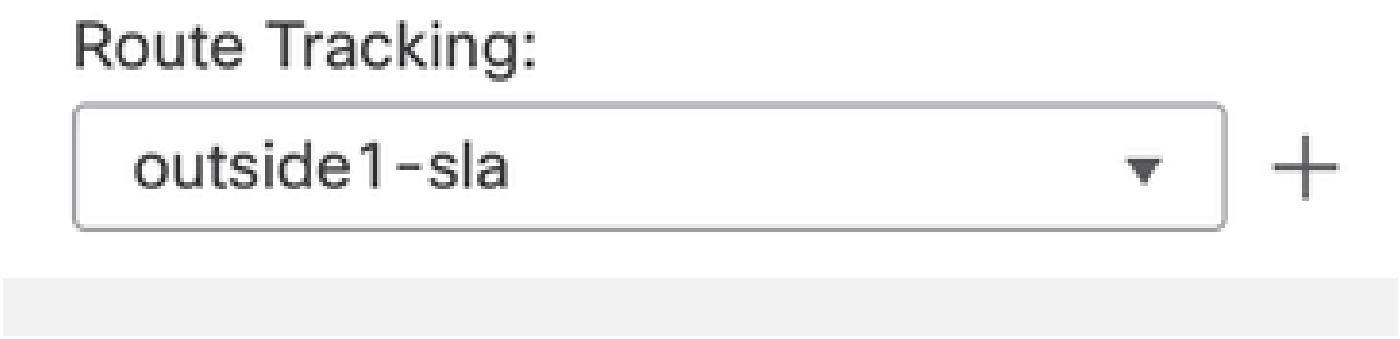
Configurar rastreamento de SLA para ISP 1

Neste exemplo, o IP do Google DNS foi usado para monitorar recursos de FTD para acessar a Internet (e CDO) através da interface outside1. Clique em ok quando estiver pronto.



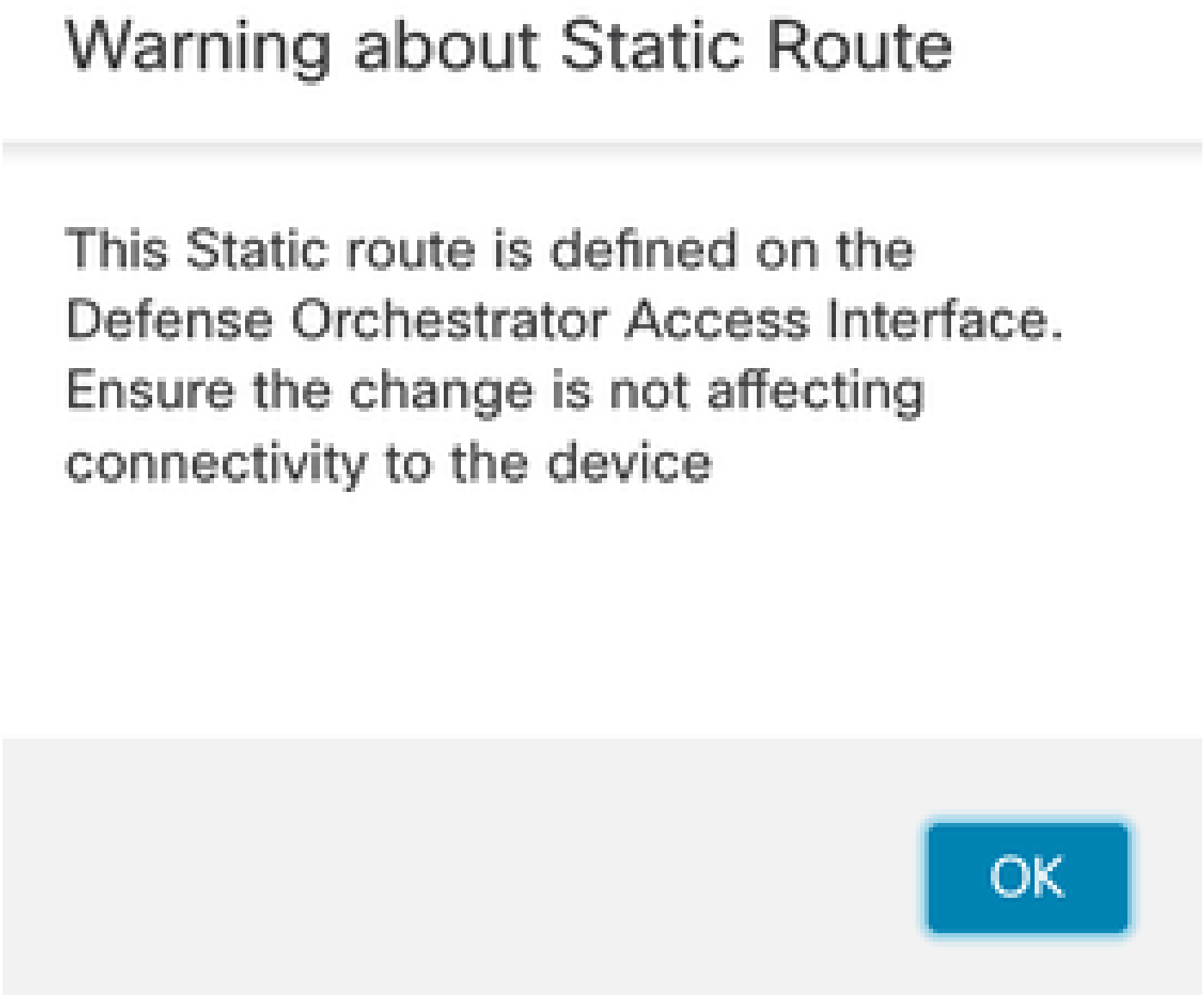
Observação: certifique-se de estar rastreando um IP que já tenha sido verificado como alcançável a partir da interface externa do FTD. Configurar uma trilha com um IP inalcançável pode desativar a rota padrão neste FTD e impedir sua capacidade de se comunicar com o CDO.

Etapa 9. Clique em Salvar e verifique se o novo rastreamento de SLA está atribuído à rota que aponta para a interface primária:



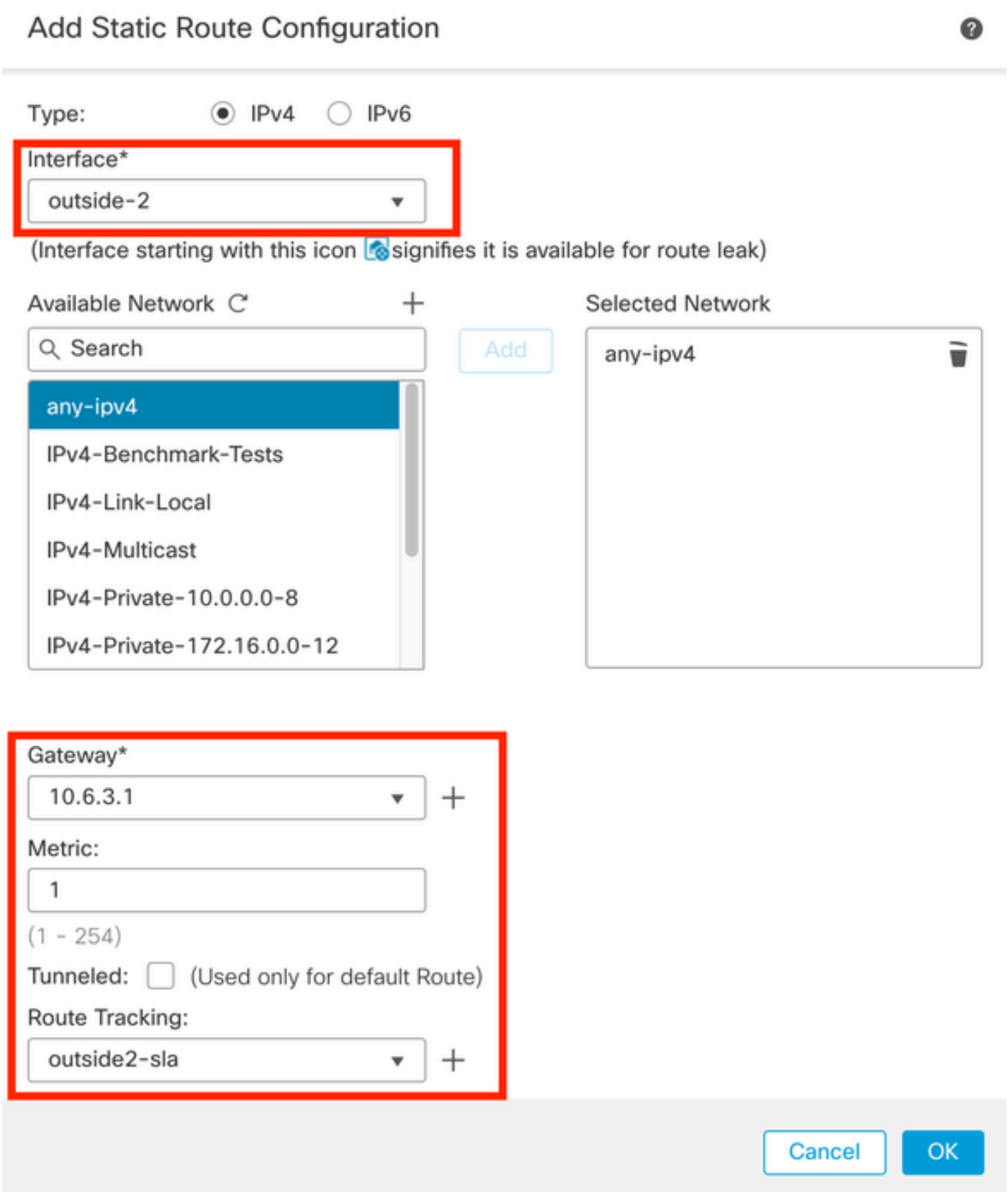
Fora do rastreamento de SLA 1

Quando você clicar em OK, uma janela pop-up será exibida com a próxima mensagem de AVISO:

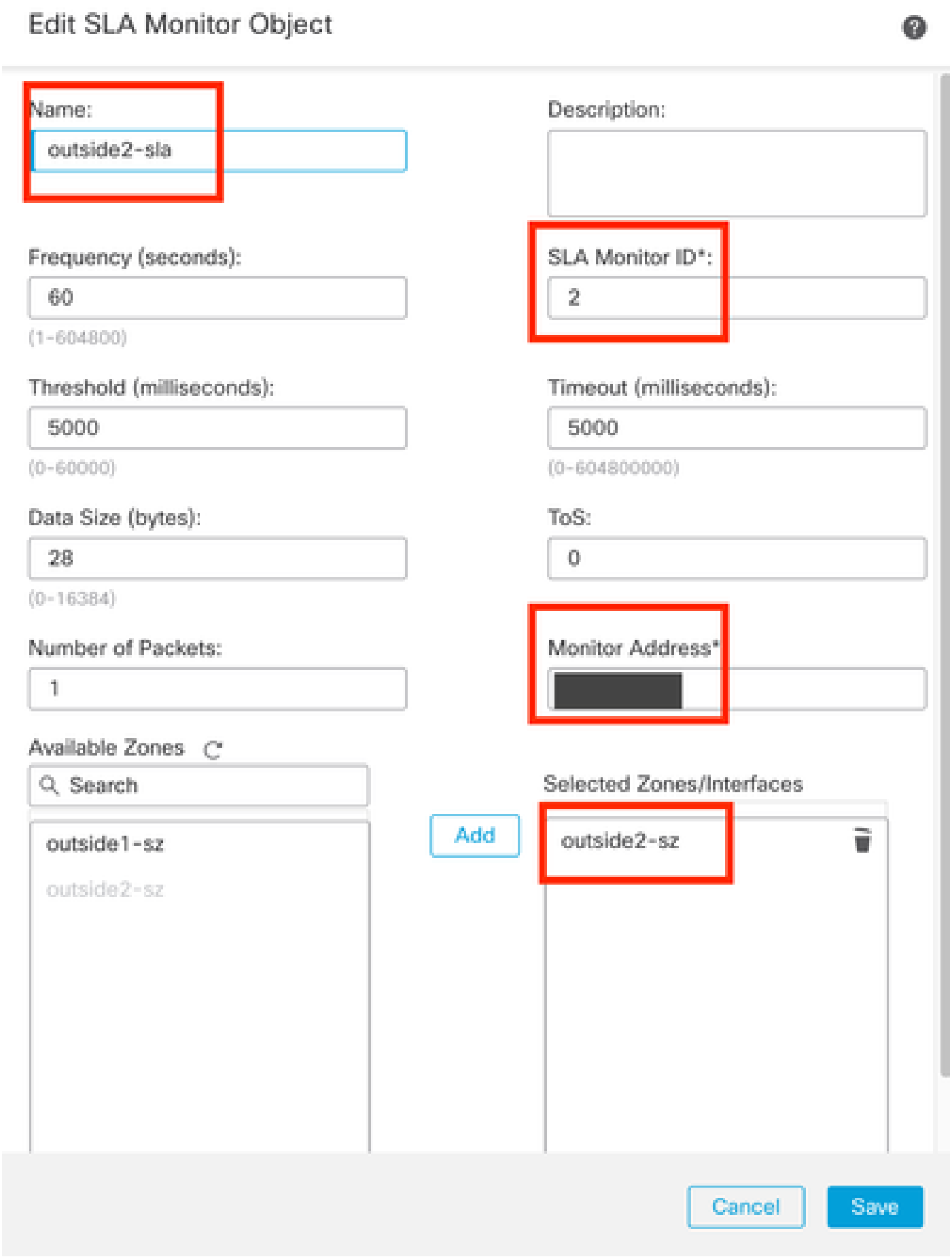


Aviso de configuração

Etapa 10. Clique na opção Add Route para adicionar uma nova rota para a interface de dados redundante. Observe na imagem seguinte que o valor de Métrica para a rota é o mesmo; além disso, o rastreamento de SLA tem um ID diferente:



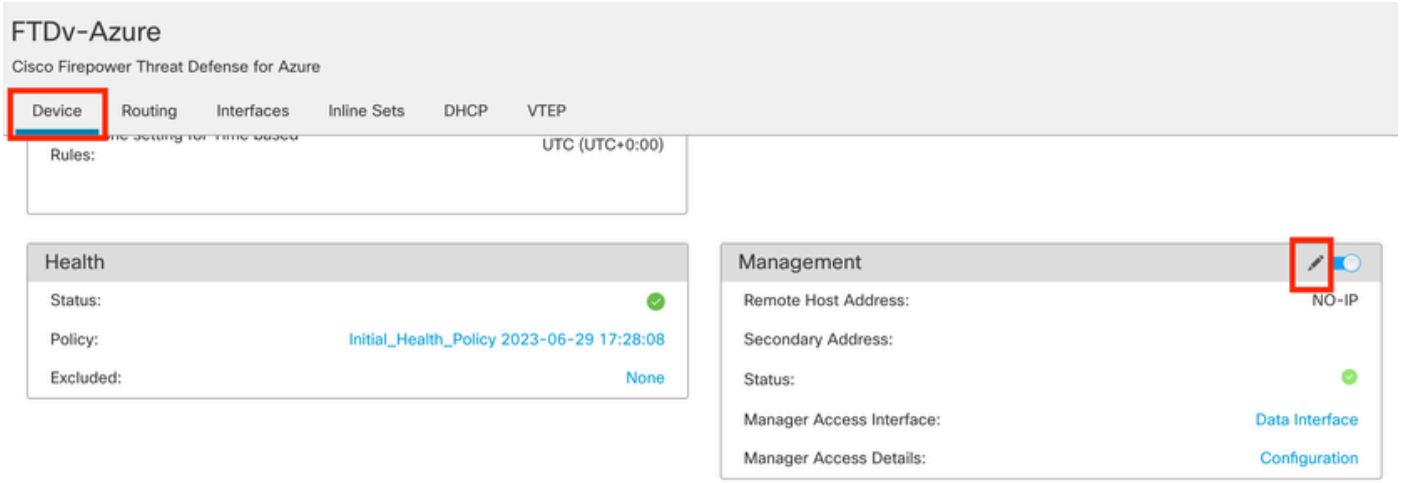
Configurar a rota estática redundante



Configurar rastreamento para interface de dados redundante

Click Save.

Etapa 11. Opcionalmente, você pode especificar o IP da interface de dados secundária em Device > Management. Mesmo assim, isso não é necessário, já que o método de integração atual usou o processo de chave de registro CLI:



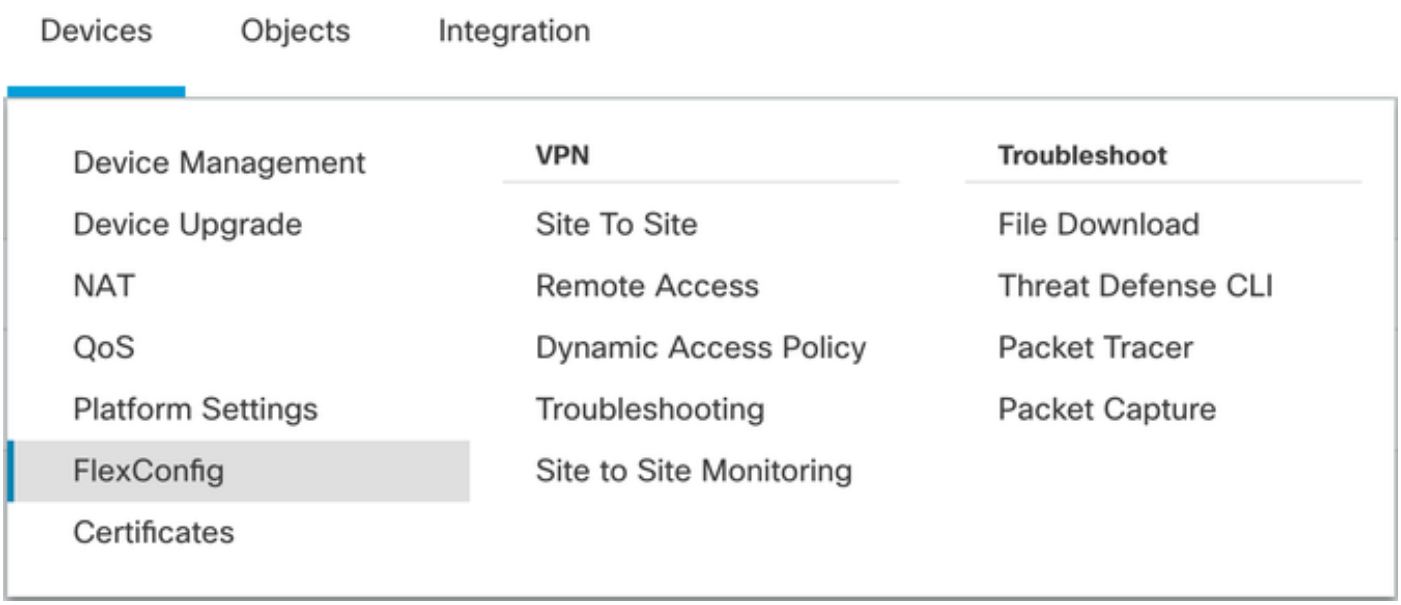
(Opcional) Especifique um IP para a interface de dados redundante no campo Gerenciamento

Etapa 12. Implante as alterações.

(Opcional) Defina um Custo de Interface para um Modo de Interface Ativa/de Backup:

Por padrão, o gerenciamento redundante na interface de dados usa o round robin para distribuir o tráfego de gerenciamento entre as duas interfaces. Como alternativa, se um link de WAN tiver uma largura de banda maior que o outro e você preferir que esse seja o link de gerenciamento principal, enquanto o outro permanece como um backup, você poderá atribuir ao link principal um custo de 1 e atribuir ao link de backup um custo de 2. No próximo exemplo, a interface GigabitEthernet0/0 é mantida como o link WAN principal, enquanto a GigabitEthernet0/1 está servindo como o link de gerenciamento de backup:

1. Navegue até o link Devices > FlexConfig e crie uma política flexConfig. Caso já exista uma política flexConfig configurada e atribuída ao seu FTD, edite-a:

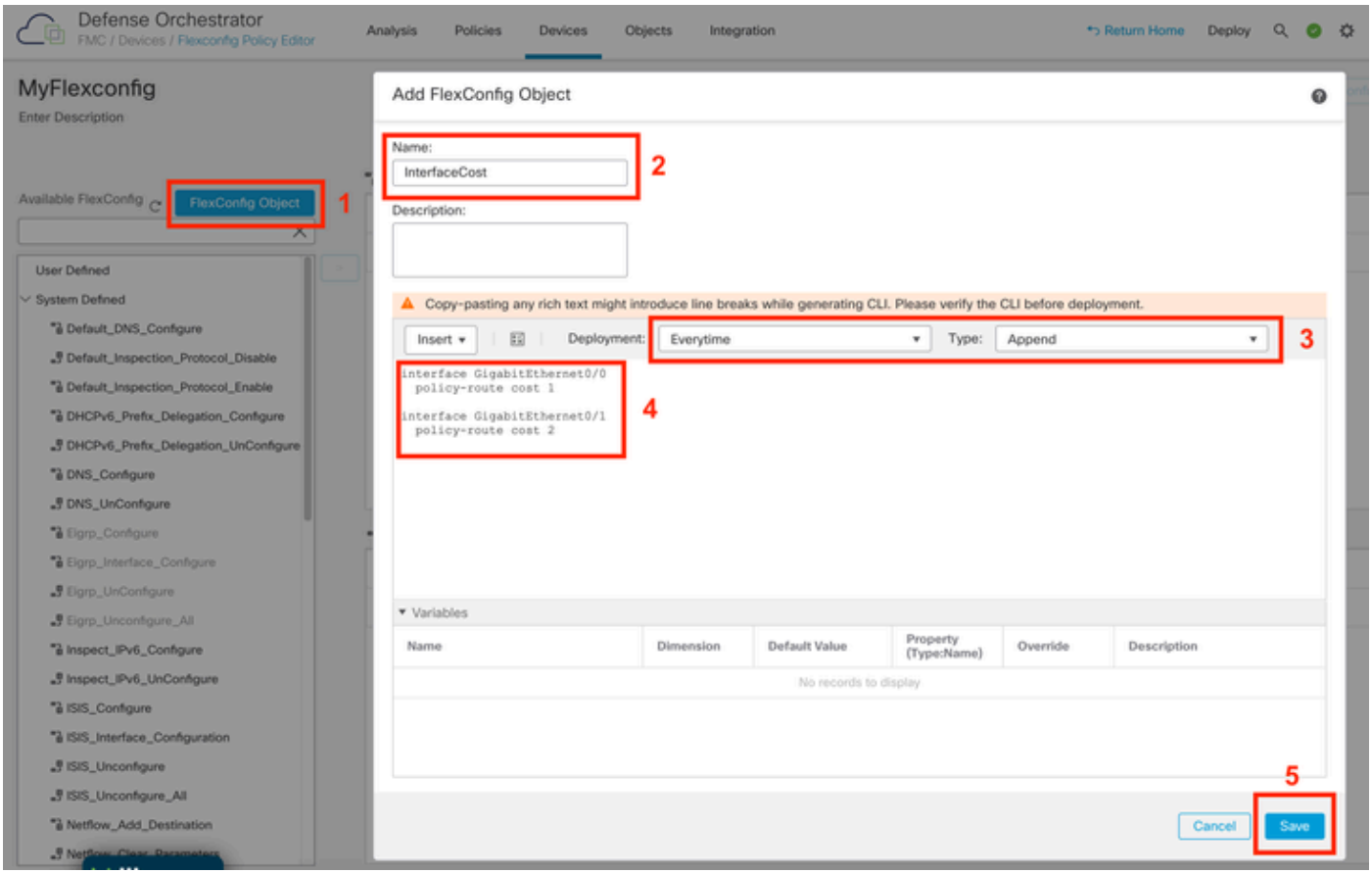


Acesso ao Menu FlexConfig

2. Crie um novo Objeto FlexConfig:

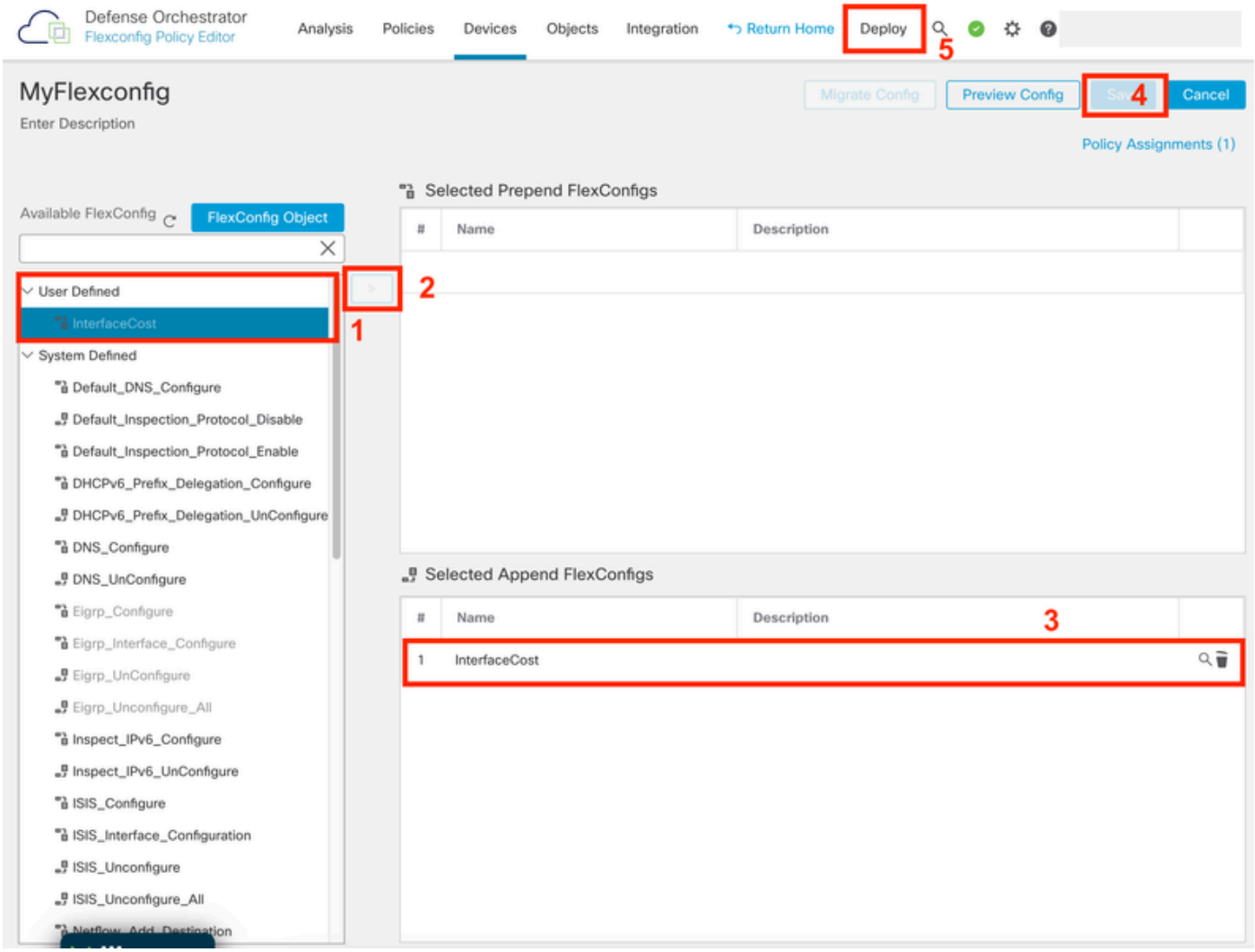
- Dê um nome ao objeto FlexConfig.
- Escolha Everytime e Append nas seções Deployment e Type, respectivamente.
- Defina o custo das interfaces com os próximos comandos, conforme descrito na Imagem 22.
- Click Save.

```
<#root>
interface GigabitEthernet0/0

  policy-route cost 1

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant.
interface GigabitEthernet0/1

  policy-route cost 2

<=== Cost 2 sets this interface as a backup interface.
```



Adição de um Objeto Flexconfig

3. Escolha o objeto criado recentemente e adicione-o à seção Seleted Append FlexConfigs, conforme descrito na figura. Salve as alterações e implante sua configuração.



Atribuindo o Objeto à Política Flexconfig

4. Implante as alterações.

Verificar

1. Para verificar, use o comando show network. Uma nova instância para a interface de gerenciamento redundante é formada:

```
> show network

<<---------- output omitted for brevity ---------->>

======================[ eth0 ]======================
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 60:45:BD:D8:62:D7
----------------------[ IPv4 ]----------------------
Configuration : Manual
```

```
Address : 10.6.0.4
Netmask : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration : Disabled

================[ Proxy Information ]================
State : Disabled
Authentication : Disabled
. . .

===============[ GigabitEthernet0/0 ]===============
State : Enabled
Link : Up
Name : outside-1
MTU : 1500
MAC Address : 60:45:BD:D8:6F:5C
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.2.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled

===============[ GigabitEthernet0/1 ]===============
State : Enabled
Link : Up
Name : outside-2
MTU : 1500
MAC Address : 60:45:BD:D8:67:CA
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.3.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled
```

2. A interface agora faz parte do domínio sftunnel. Você pode confirmar isso com os comandos show sftunnel interfaces e show running-config sftunnel :

```
<#root>

>

show sftunnel interfaces


Physical Interface Name of the Interface
GigabitEthernet0/0 outside-1
GigabitEthernet0/1 outside-2

>

show running-config sftunnel


sftunnel interface outside-2
sftunnel interface outside-1
```

```
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

3. Uma rota baseada em políticas é automaticamente soletrada. Se você não tiver especificado um custo de interface, a opção adaptive-interface definirá o processamento em rodízio para balancear a carga do tráfego de gerenciamento entre as duas interfaces:

```
<#root>

>

show running-config route-map


!
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
 match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
 set adaptive-interface cost outside-1 outside-2

>

show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392


access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392; 1 elements; name hash: 0x8e8cb508
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392 line 1 extended permit tcp any any eq 8305 (hi
```

4. Use o comando show running-config interface <interface> para verificar as configurações da interface:

```
<#root>

>

 show running-config interface GigabitEthernet 0/0


!
interface GigabitEthernet0/0
nameif outside-1
security-level 0
zone-member outside-ecmp
ip address 10.6.2.4 255.255.255.0
policy-route cost 1

>

show running-config interface GigabitEthernet 0/1


!
interface GigabitEthernet0/1
nameif outside-2
security-level 0
zone-member outside-ecmp
ip address 10.6.3.4 255.255.255.0
```

```
policy-route cost 2
```

Alguns comandos adicionais podem ser usados para verificar o rastreamento das rotas configuradas:

```
<#root>

>

show track


Track 1
Response Time Reporter 2 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interf
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 10
Tracked by:
STATIC-IP-ROUTING 0
Track 2
Response Time Reporter 1 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interf
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
STATIC-IP-ROUTING 0


>

show route



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 10.6.3.1 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2
                   [1/0] via 10.6.2.1, outside-1
C 10.6.2.0 255.255.255.0 is directly connected, outside-1
L 10.6.2.4 255.255.255.255 is directly connected, outside-1
C 10.6.3.0 255.255.255.0 is directly connected, outside-2
L 10.6.3.4 255.255.255.255 is directly connected, outside-2
```

Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Gerenciamento da defesa contra ameaças de firewall com o Centro de gerenciamento de firewall fornecido em nuvem no Cisco Defense Orchestrator

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.