# 在Azure FTD中部署冗余数据接口，由CD-FMC管理

## 目录

## 简介

本文档介绍将cdFMC管理的虚拟FTD配置为使用冗余管理器访问数据接口功能的步骤。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科安全防火墙管理中心
- 思科防御协调器

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 云交付的防火墙管理中心
- 在Azure云中托管的虚拟安全防火墙威胁防御7.3.1版。

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。

### 相关产品

本文档也可用于以下硬件和软件版本：

- 任何能够运行Firepower威胁防御7.3.0或更高版本的物理设备。

## 背景信息

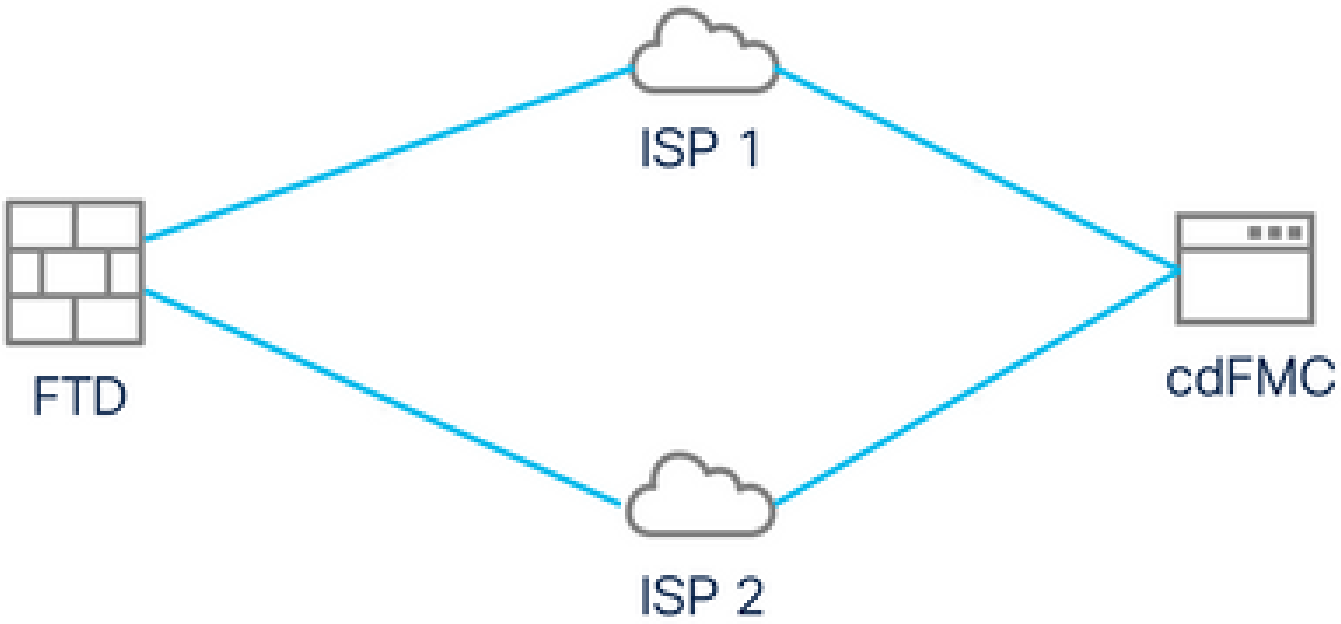
本文档显示配置和验证cdFMC托管vFTD的步骤，以便使用两个数据接口进行管理。当客户需要第二个ISP通过互联网管理其FTD时，此功能通常非常有用。默认情况下，FTD对两个接口之间的管理流量执行轮询负载均衡；可以按照本文档中的说明将其修改为活动/备份部署。

安全防火墙威胁防御7.3.0版中引入了用于管理的冗余数据接口。假设vFTD可以访问能够解析

CDO访问的URL的名称服务器。

# 配置

## 网络图




网络图

## 为管理访问配置数据接口

通过控制台登录设备，然后使用命令configure network management-data-interface为管理访问配置其中一个数据接口：

```
<#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
```

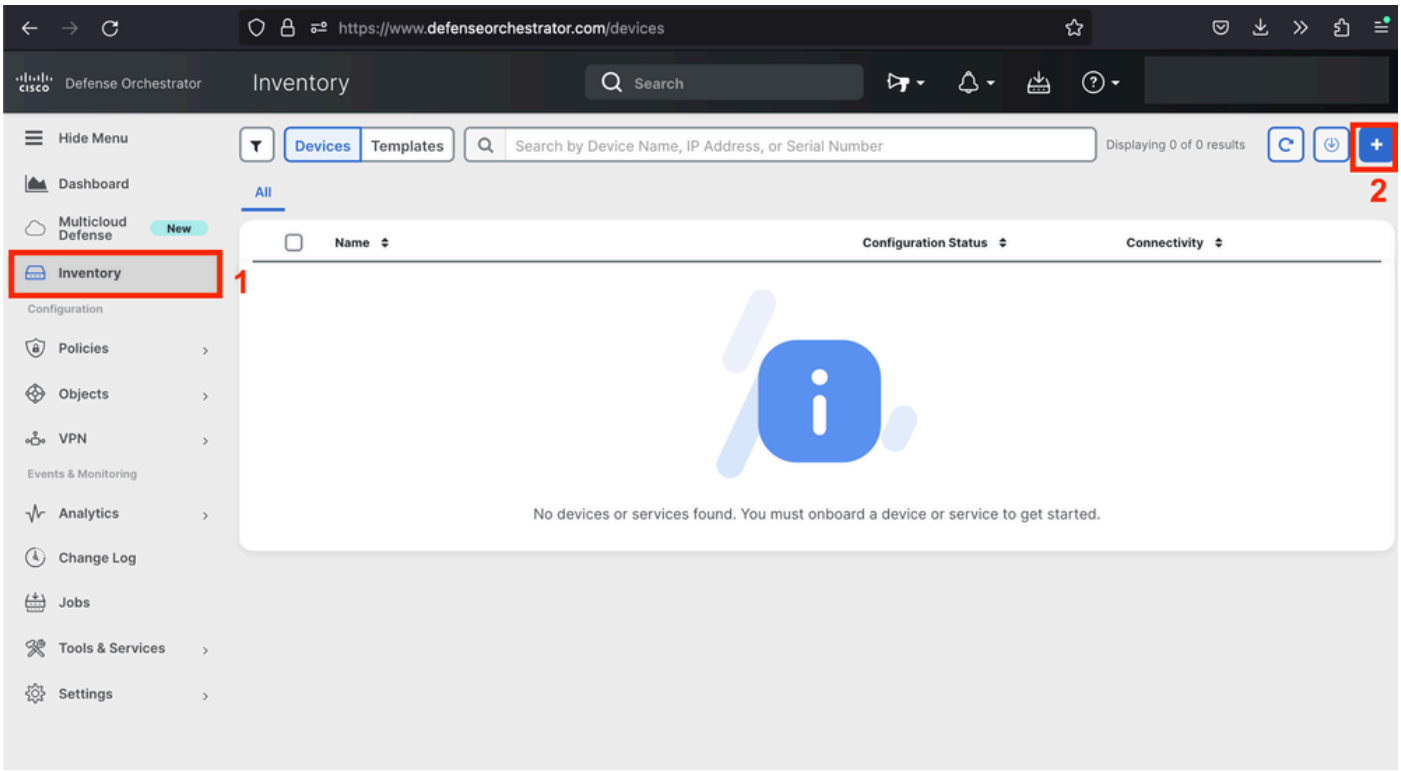
```
IPv4/IPv6 address:

10.6.2.4

Netmask/IPv6 Prefix:

 255.255.255.0

Default Gateway:

10.6.2.1
```

请记住，原始管理接口不能配置为使用DHCP。可以使用命令show network对此进行验证。

## 通过CDO注册FTD

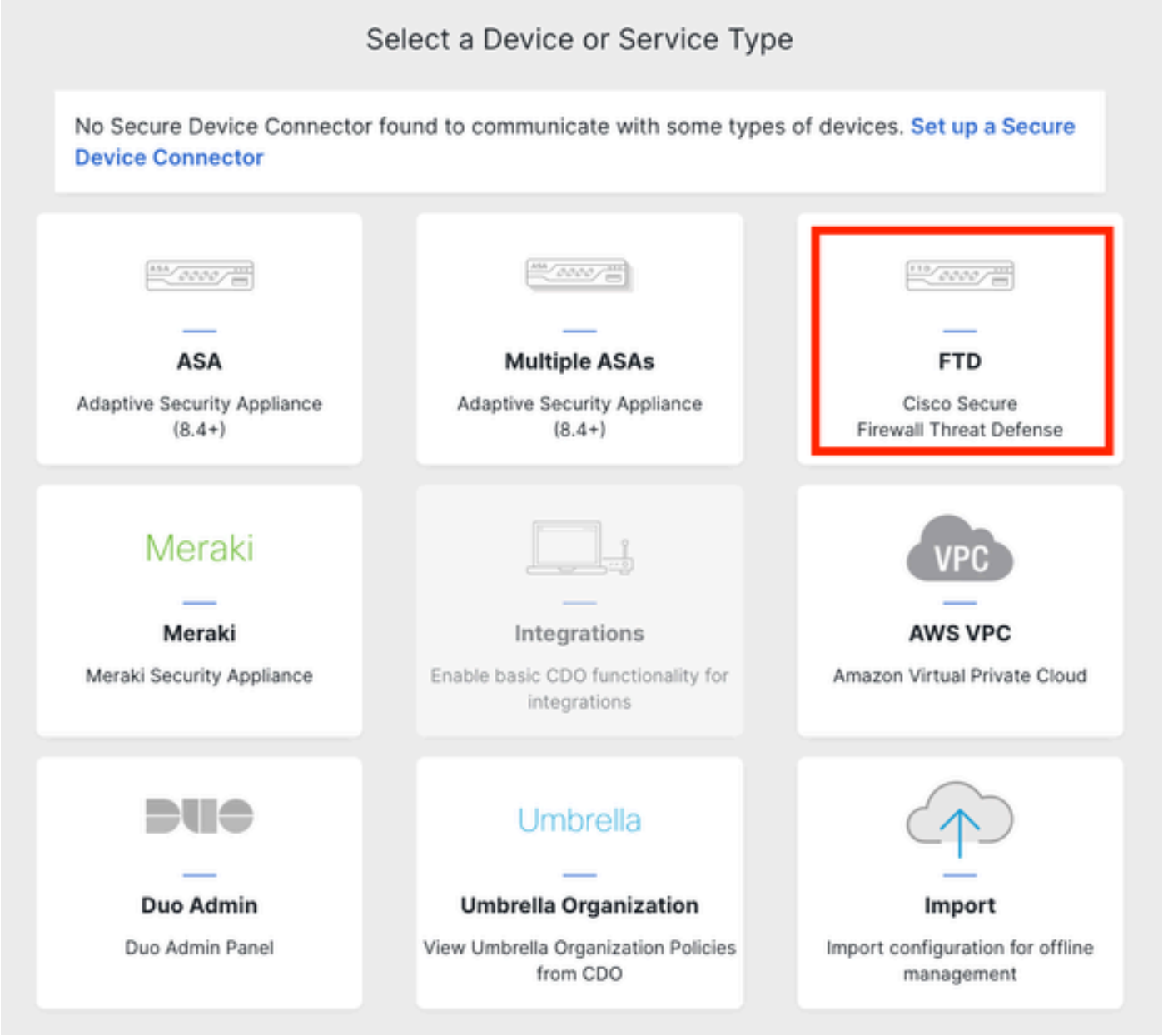
此流程通过CDO在Azure FTD中运行，因此可以由云交付的FMC管理。此过程使用CLI注册密钥，如果您的设备通过DHCP分配IP地址，则此密钥会很有用。只有Firepower 1000、Firepower 2100或Secure Firewall 3100平台支持其他自注册方法，如日志接触调配和序列号。

步骤1:在CDO门户中，导航到资产，然后点击入职选项：



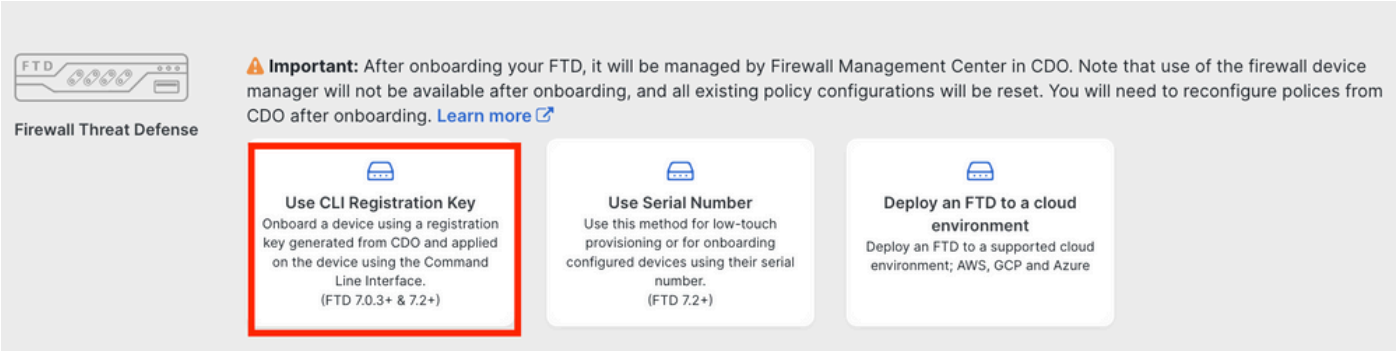

“清单”页

第2步：点击FTD图块：



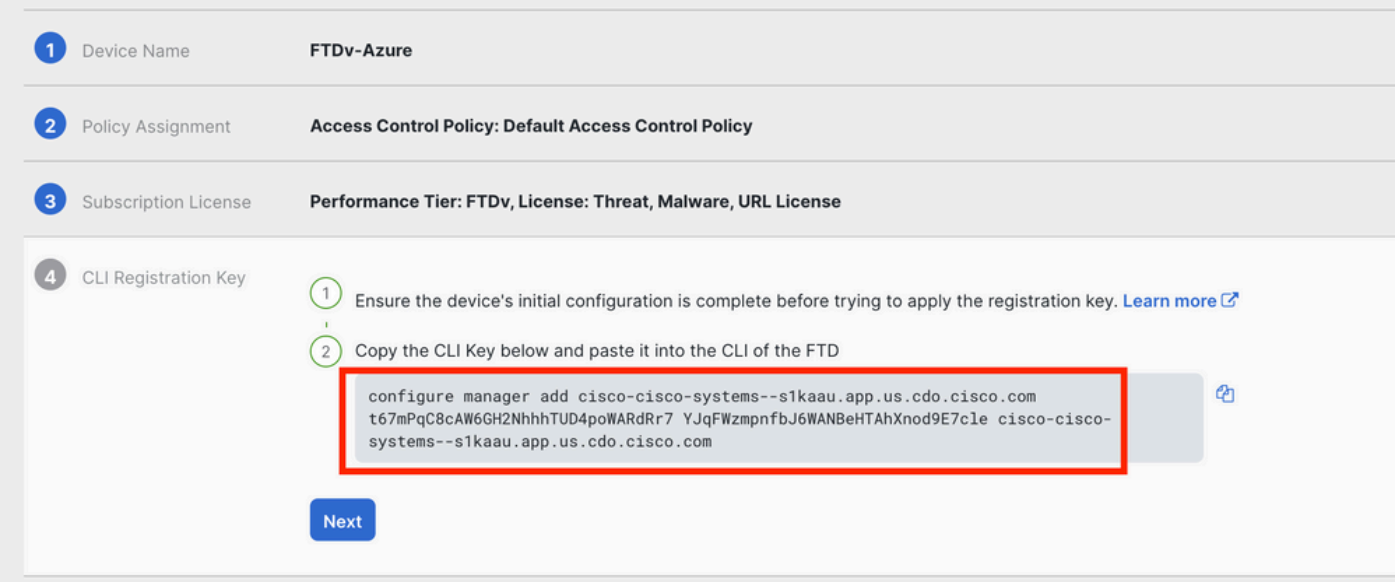

注册FTD

第3步：选择使用CLI注册密钥选项：

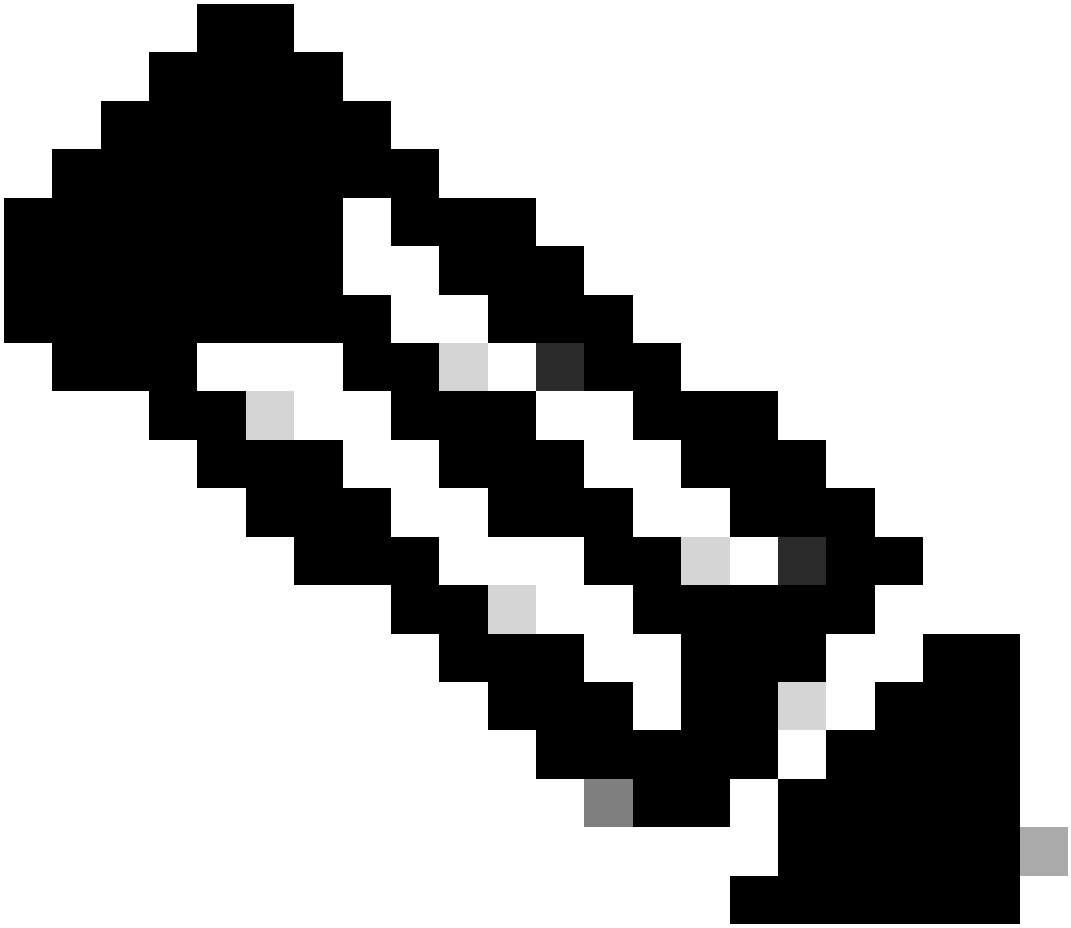



使用CLI注册密钥

第四步：从configure manager命令开始复制CLI密钥：




复制Configure Manager命令



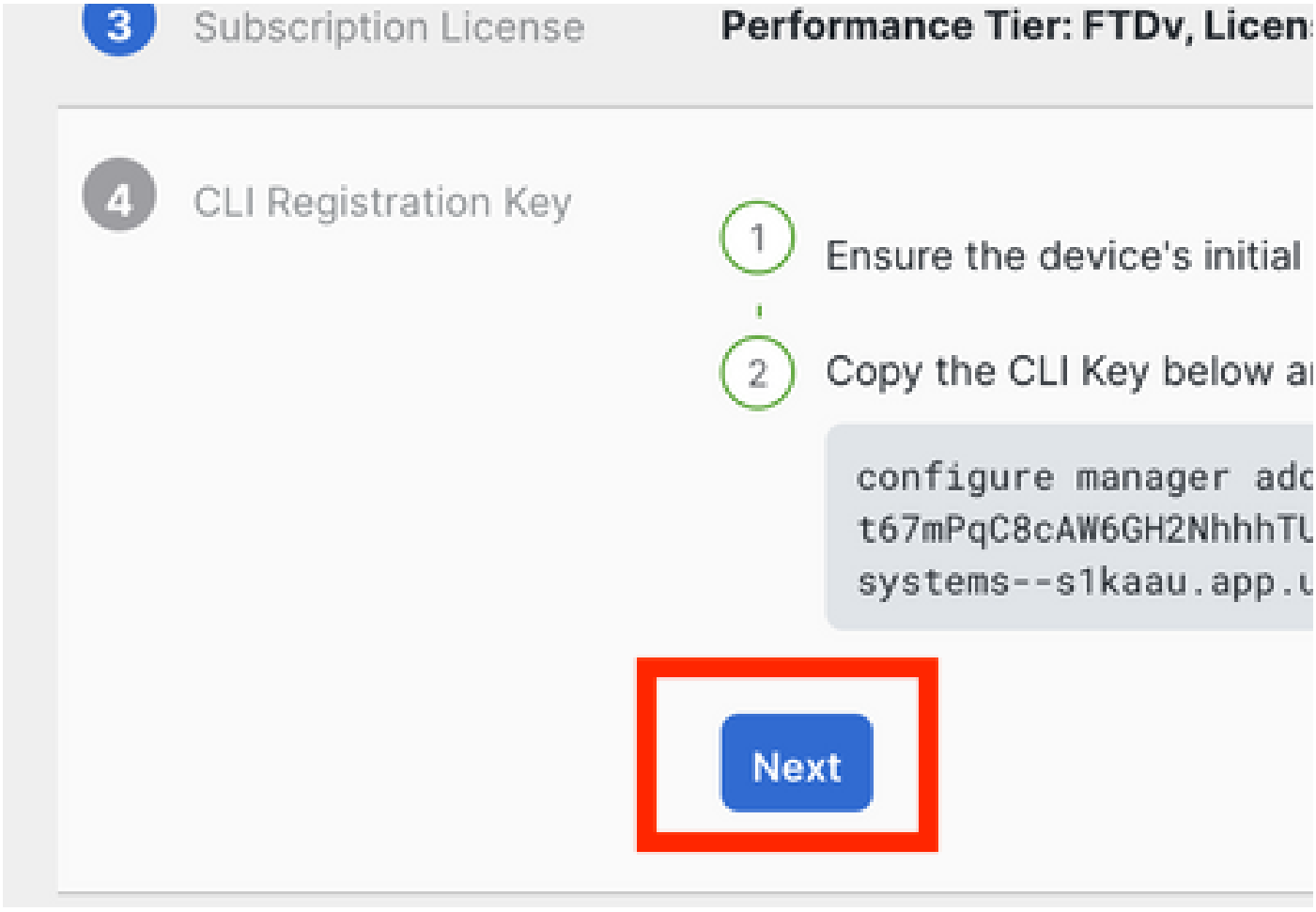
注：CLI密钥与注册带有内置FMC的FTD中使用的格式相匹配，在自置FMC中，您可以配置

NAT-ID以在受管设备位于NAT设备之后时允许注册：configure manager add <fmc-hostname-or-ipv4> <registration-key> <nat-id> <display-name>

第五步：将命令粘贴到FTD CLI中。如果通信成功，您必须收到此消息：

```
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.
```

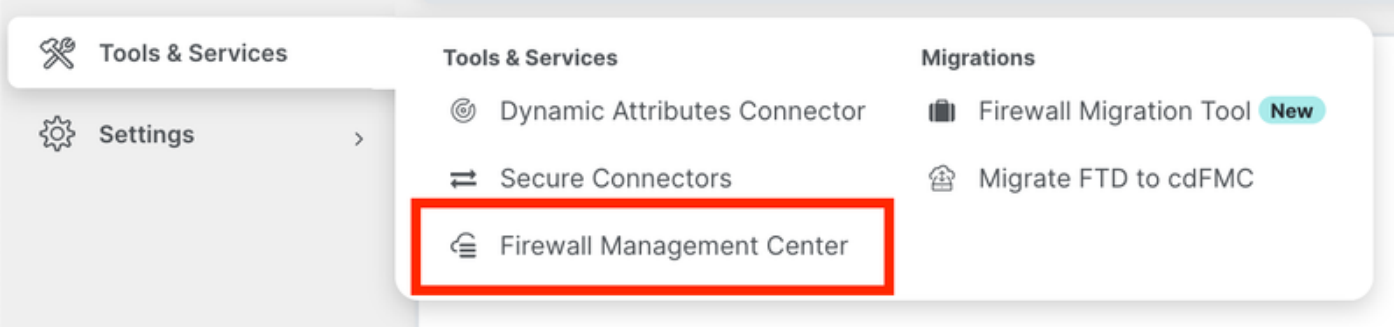
第六步：返回CDO，然后单击Next：




单击“下一步”

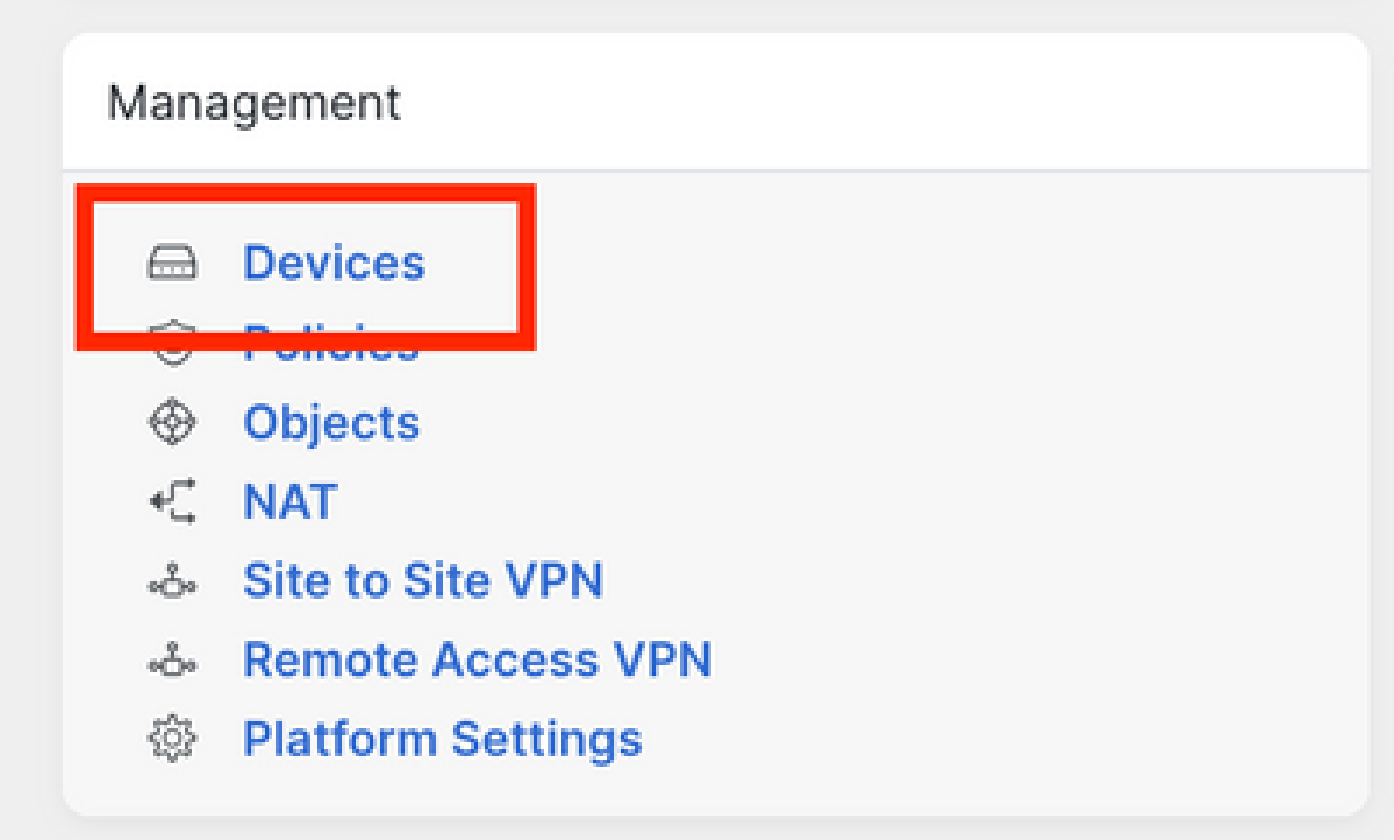
CDO继续注册过程，并显示一条消息，提示需要很长时间才能完成。您可以点击服务页面中的设备链接来检查注册过程的状态。

步骤 7.通过工具和服务页面访问您的FMC。



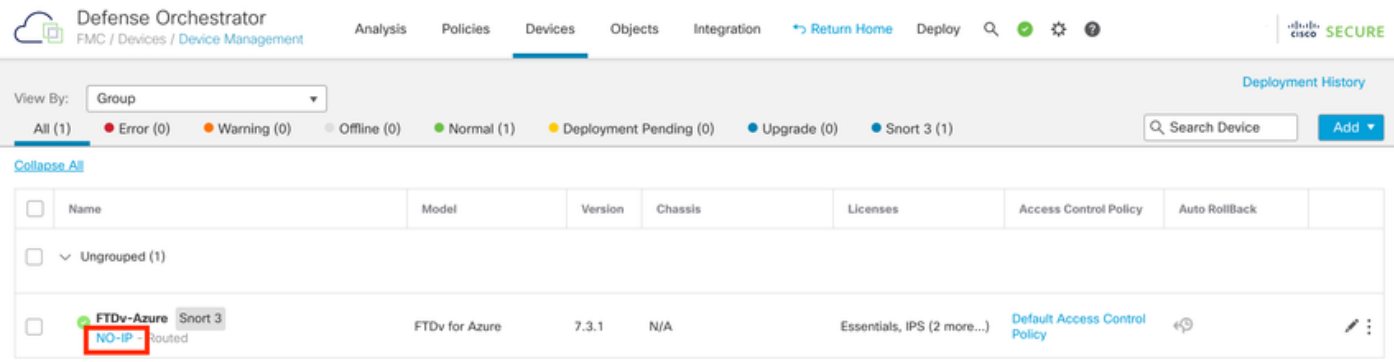

访问cdFMC

点击设备链接。




点击设备(Devices)

您的FTD现已在CDO中注册，并可由云交付的FMC管理。请注意，在下一个映像中，设备名称下列出了NO-IP。使用CLI注册密钥的自行激活过程中会发生这种情况。

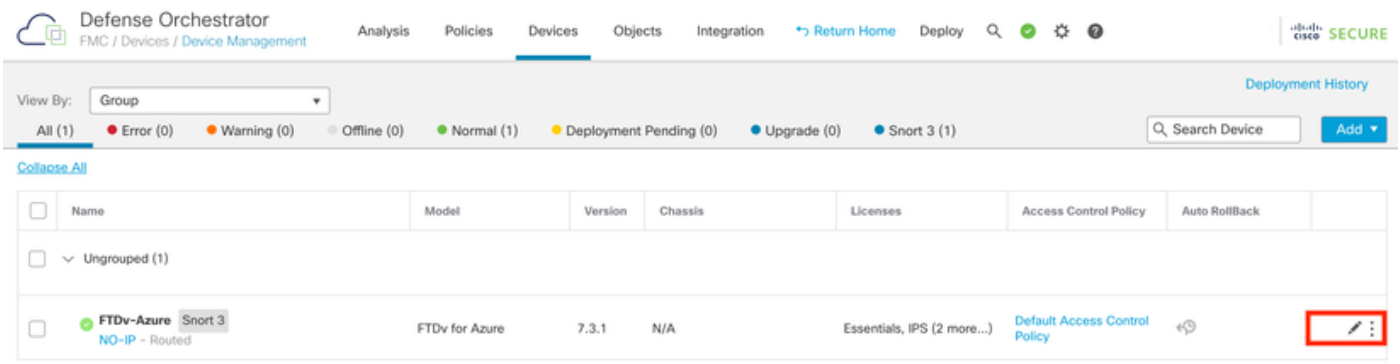


托管FTD

## 为Manager访问配置冗余数据接口

此过程为管理访问分配第二个数据接口。

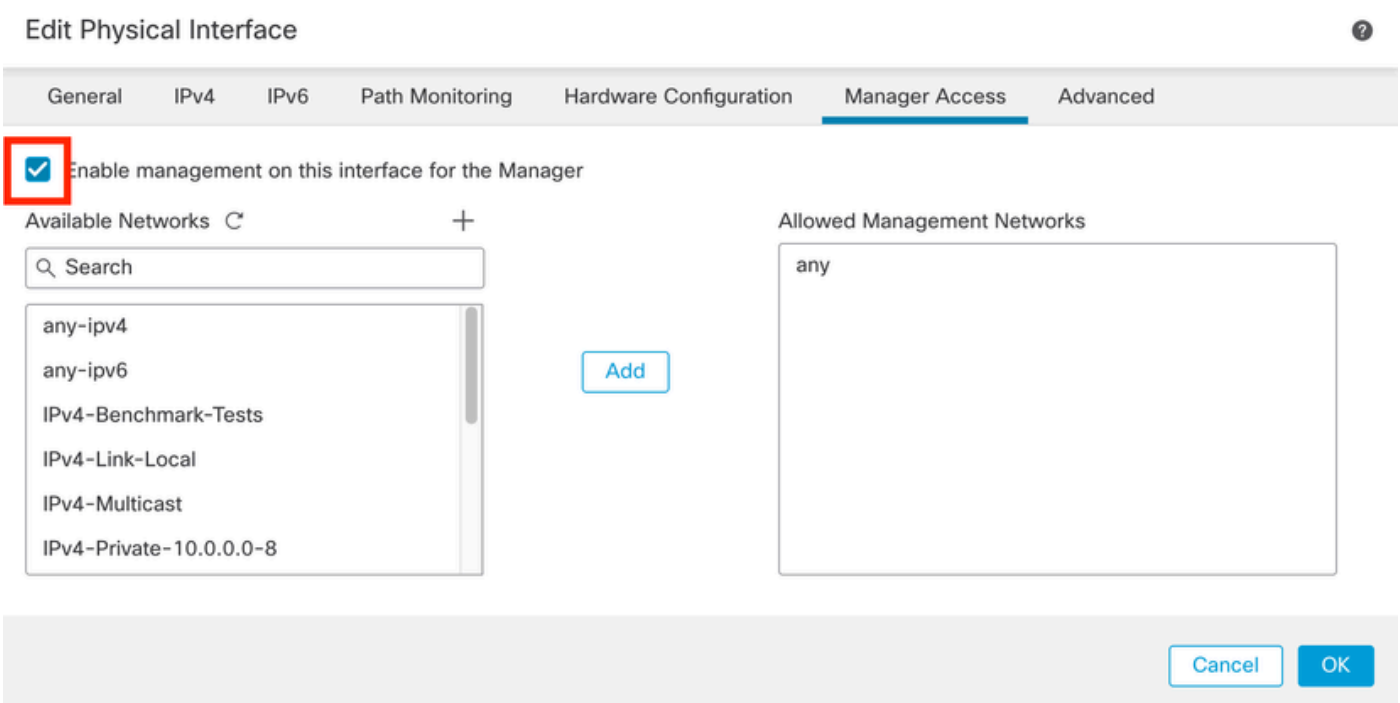
步骤1:在设备选项卡中，点击铅笔图标以访问FTD编辑模式：




编辑FTD

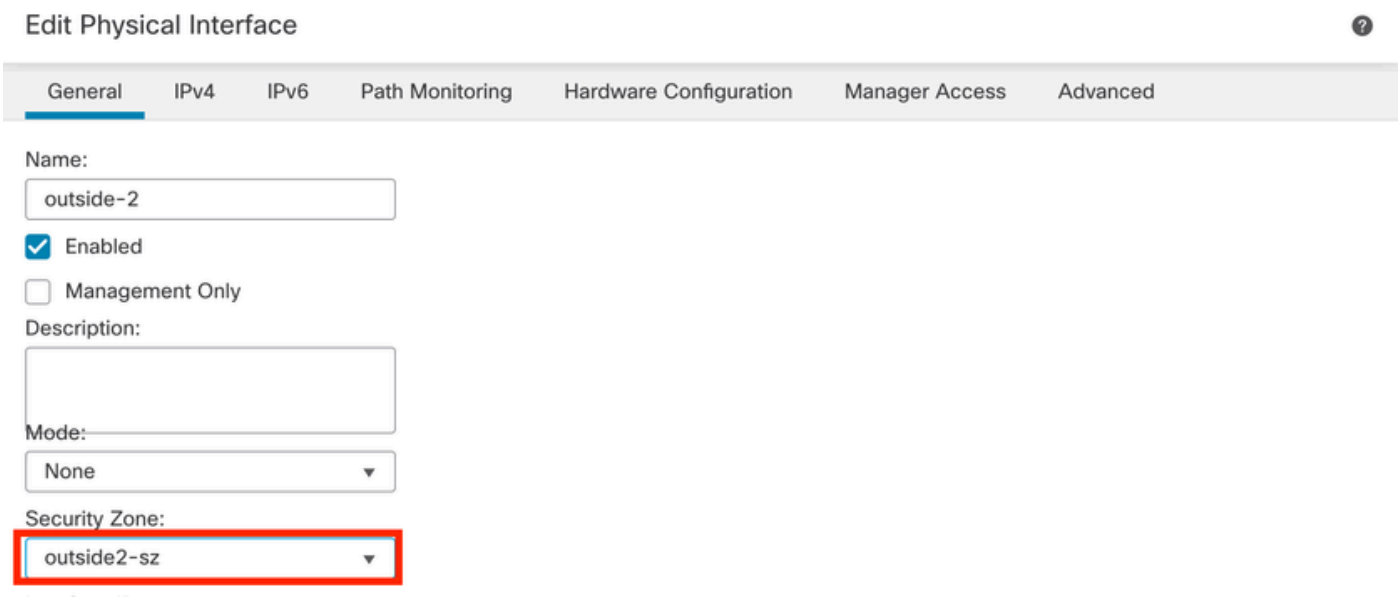
第二步：在Interface选项卡中，编辑要指定为冗余管理接口的接口。如果之前未执行此操作，请配置接口名称和IP地址。

第三步：在Manager Access 选项卡中启用Enable management on this interface for the manager 复选框：



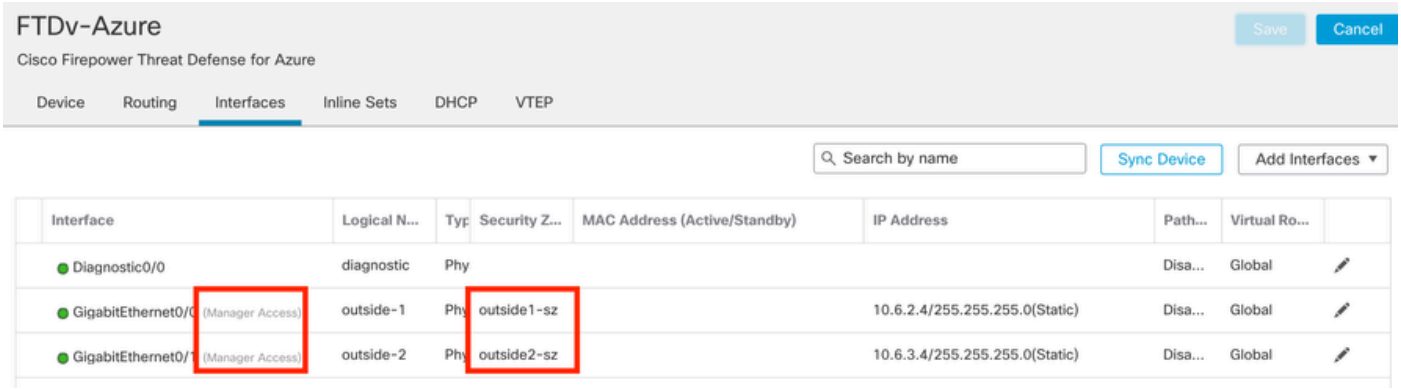

启用管理器访问

第四步：在常规选项卡中，确保将接口分配给安全区域，然后单击确定：




冗余数据接口的安全区

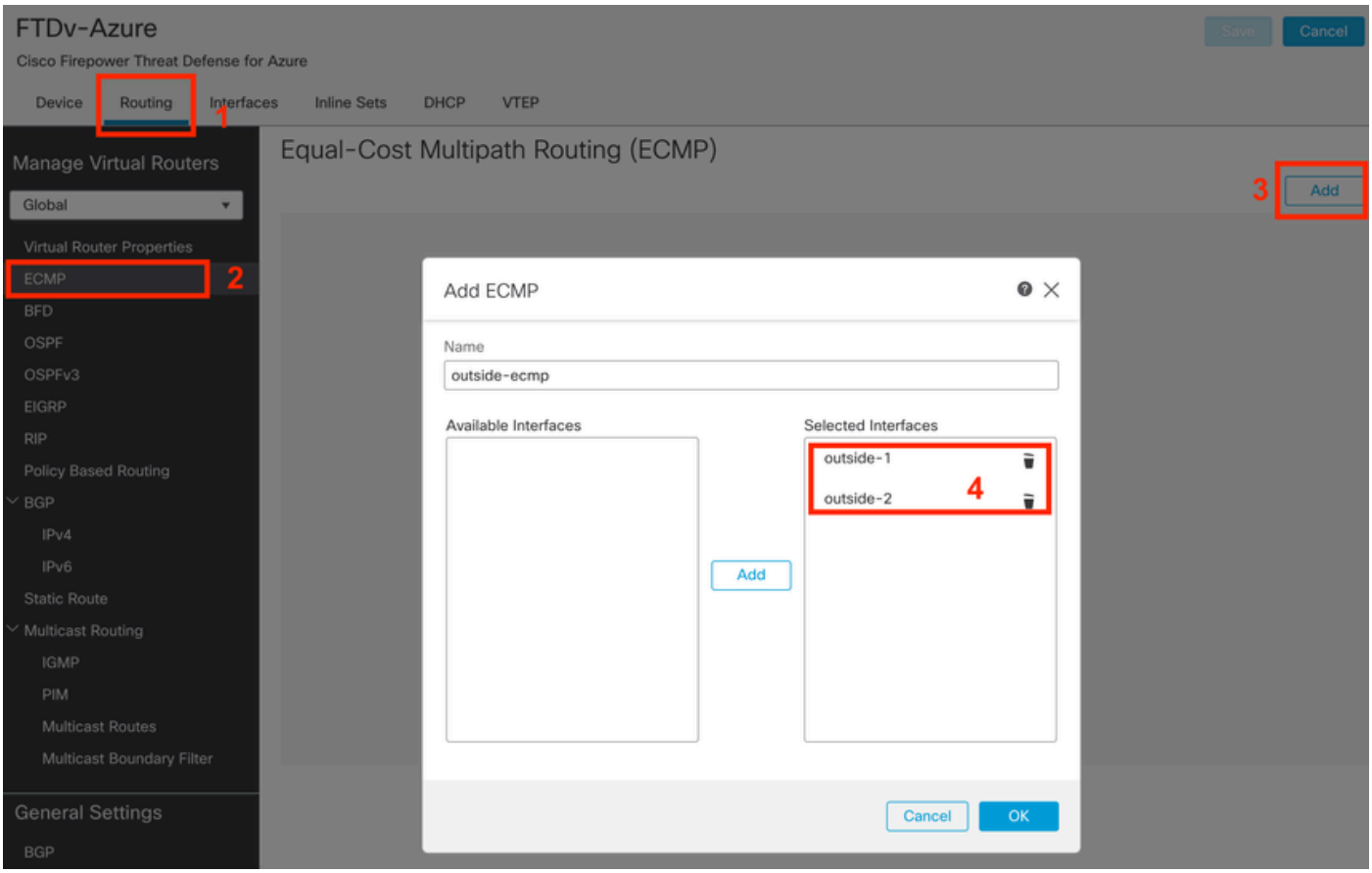
第五步：请注意，现在两个接口都具有Manager Access标记。此外，请确保已将主数据接口分配给其他安全区域：




接口配置审核

在下一节中，步骤6到10用于配置两条到达CDO的等价默认路由，每条路由都由独立的SLA跟踪进程监控。SLA跟踪确保存在使用受监控接口与cdFMC通信的功能路径。

第六步：导航到路由选项卡并在ECMP菜单下创建包含两个接口的新ECMP区域：

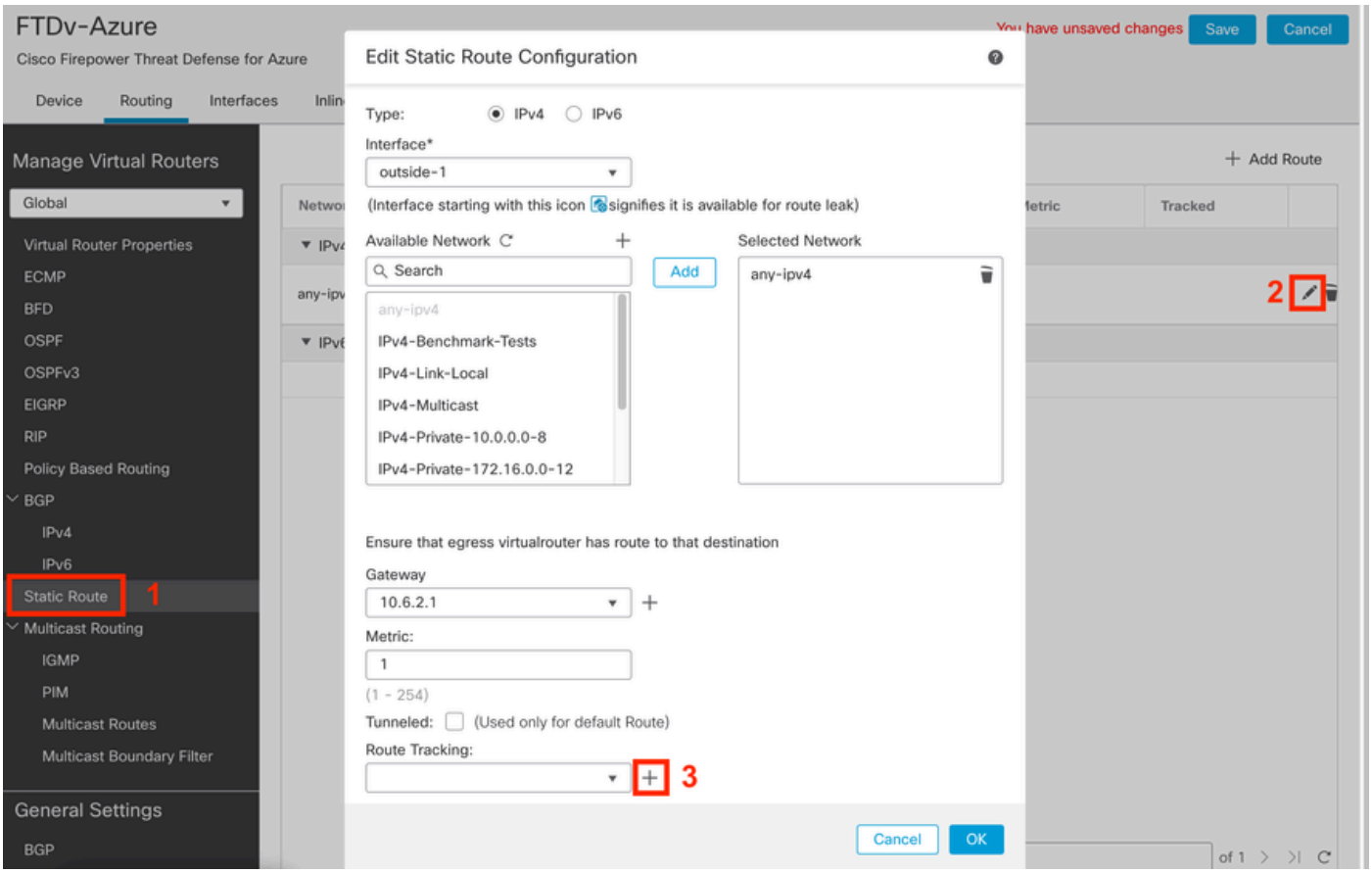



配置ECMP区域

单击OK 和Save。

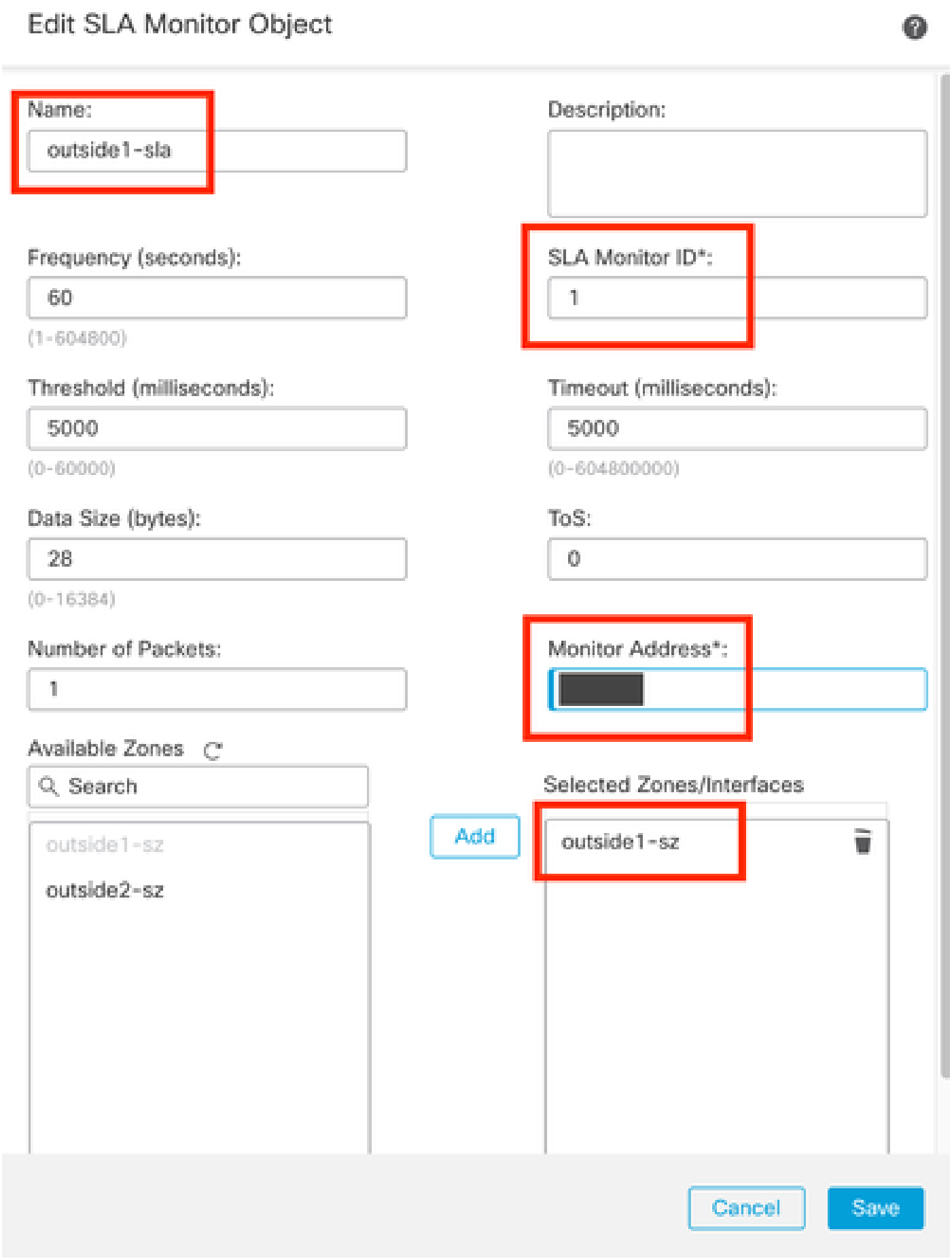
步骤 7.在路由选项卡中，导航到静态路由。

点击铅笔图标编辑您的主要路由。然后点击加号添加新的SLA跟踪对象：



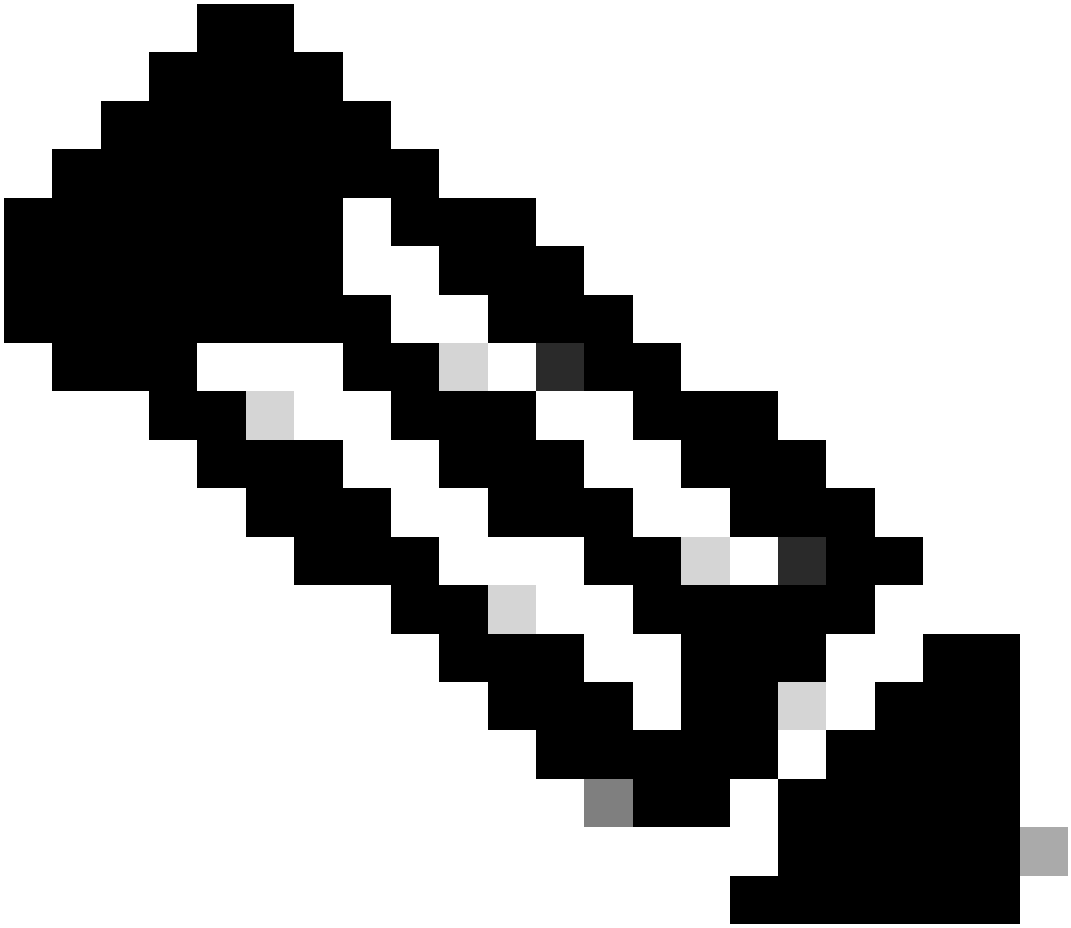

编辑主要路由以添加SLA跟踪

步骤 8功能SLA跟踪所需的参数在下一幅图中突出显示。或者，您可以调整其他设置，如数据包数量、超时和频率。




配置ISP 1的SLA跟踪

在本示例中，Google DNS IP用于监控通过outside1接口访问Internet（和CDO）的FTD功能。准备就绪后，单击ok。



注意：确保您正在跟踪已从您的FTD外部接口验证为可访问的IP。使用不可达IP配置跟踪可能会使此FTD中的默认路由关闭，然后阻止其与CDO进行通信。

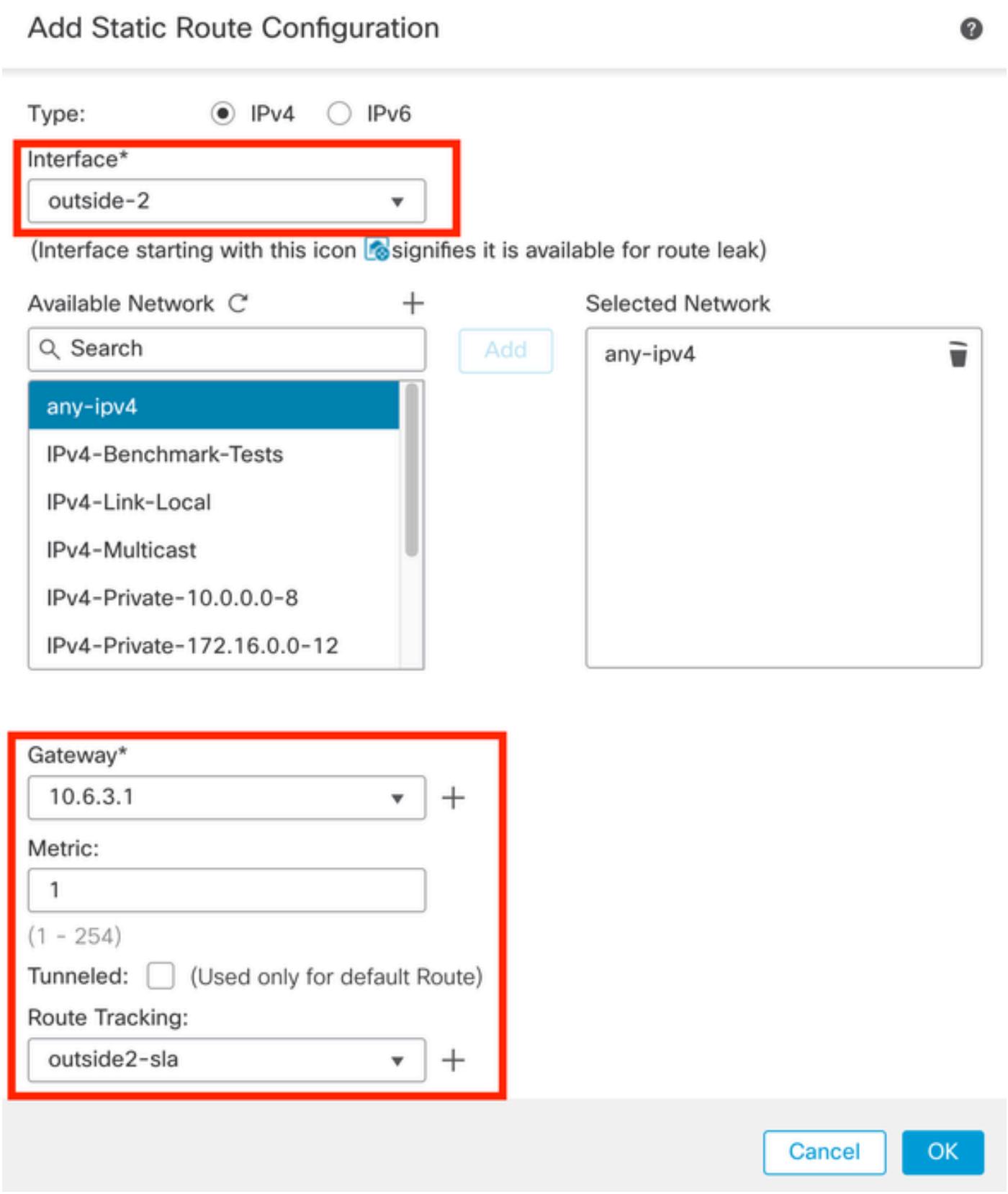
步骤 9单击Save，并确保新的SLA跟踪已分配给指向主接口的路由：

外部1 SLA跟踪

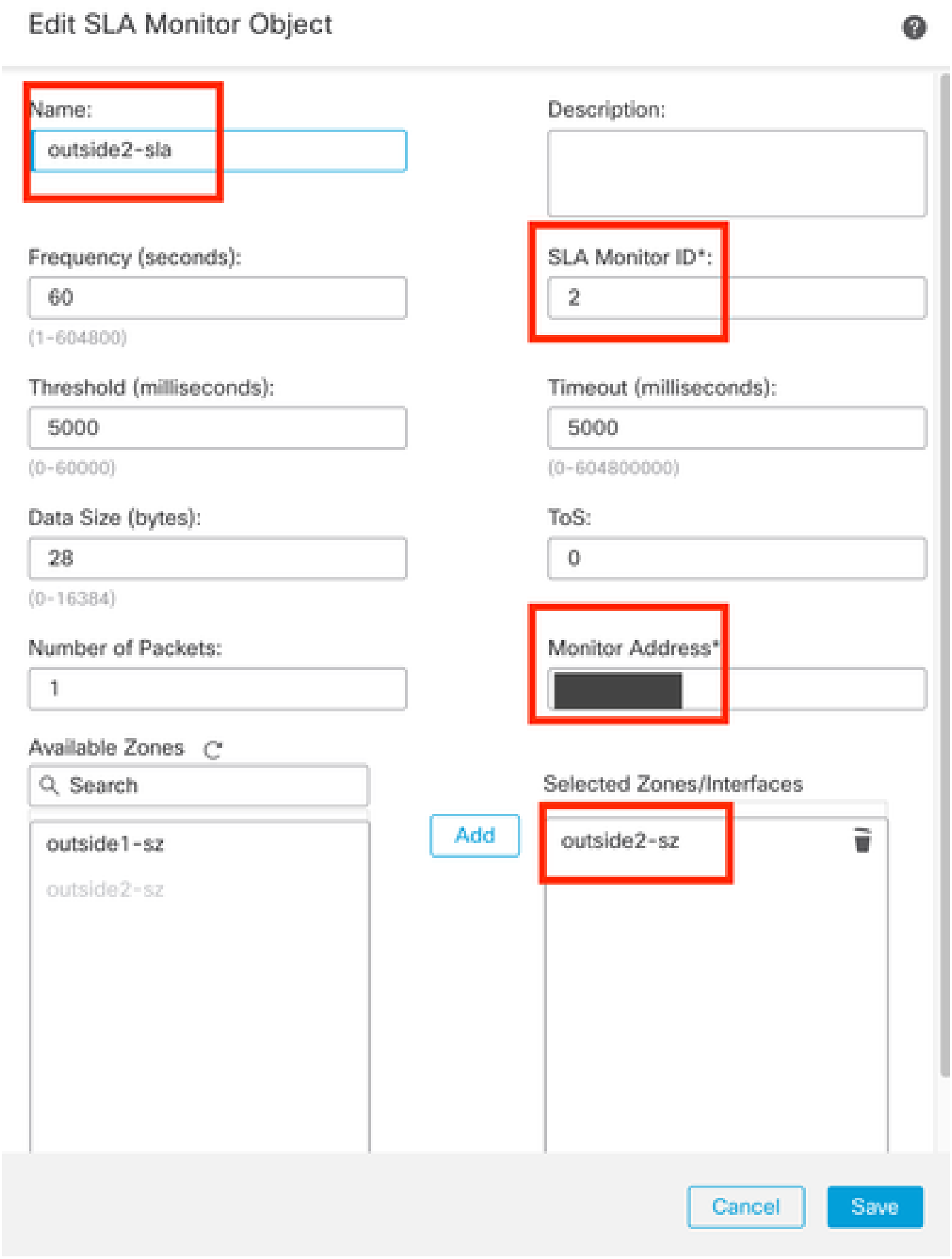
单击OK后，将显示一个弹出窗口，其中包含下一条WARNING消息：


配置警告

步骤 10单击Add Route选项为冗余数据接口添加新路由。请注意，从下一张图可以看出，路由的度量值相同；此外，SLA跟踪还具有不同的ID：


Add Static Route Configuration
Type:
IPv4
IPv6
Interface*
outside-2
(Interface starting with this icon signifies it is available for route leak)
Available Network
Search
any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8
IPv4-Private-172.16.0.0-12
Add
Selected Network
any-ipv4
Gateway*
10.6.3.1
Metric:
1
(1 - 254)
Tunneled:
(Used only for default Route)
Route Tracking:
outside2-sla
Cancel
OK

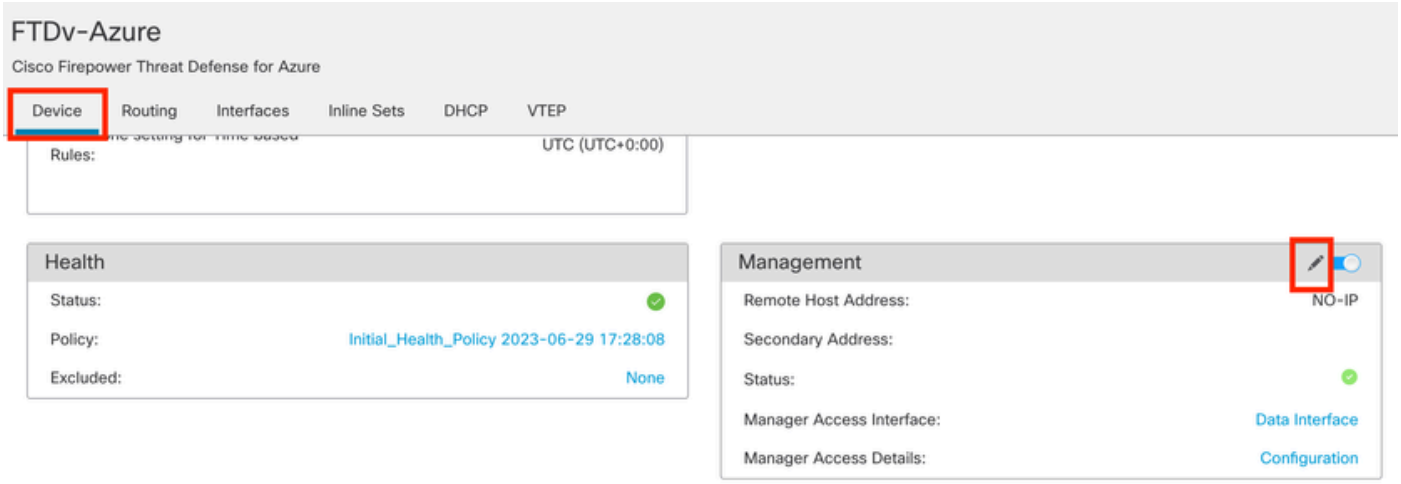
配置冗余静态路由




配置冗余数据接口的跟踪

Click Save.

步骤 11或者，您可以在Device > Management下指定辅助数据接口IP。 即使如此，由于当前的注册方法使用了CLI注册密钥过程，因此也不需要这样做：



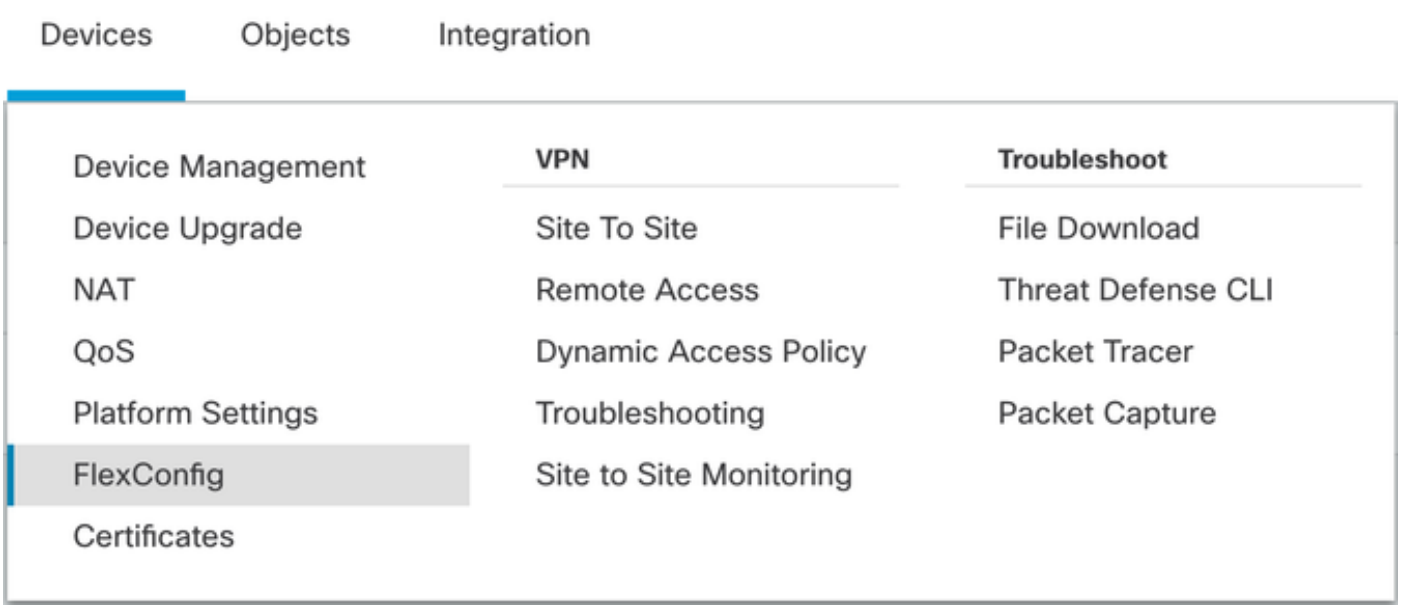

（可选）在管理字段中为冗余数据接口指定IP

步骤 12部署更改。

## （可选）设置主用/备用接口模式的接口成本：

默认情况下，数据接口上的冗余管理使用轮询在两个接口之间分配管理流量。或者，如果某个WAN链路的带宽高于其他链路，并且您希望将其用作主管理链路，而另一个链路仍作为备用链路，则可以将主链路的开销设置为1，将备用链路的开销设置为2。在下一个示例中，接口GigabitEthernet0/0保留为主广域网链路，而GigabiEthernet0/1用作备份管理链路：

1. 导航到设备> FlexConfig 链接并创建flexConfig策略。如果已配置并分配给FTD的flexConfig策略，请对其进行编辑：

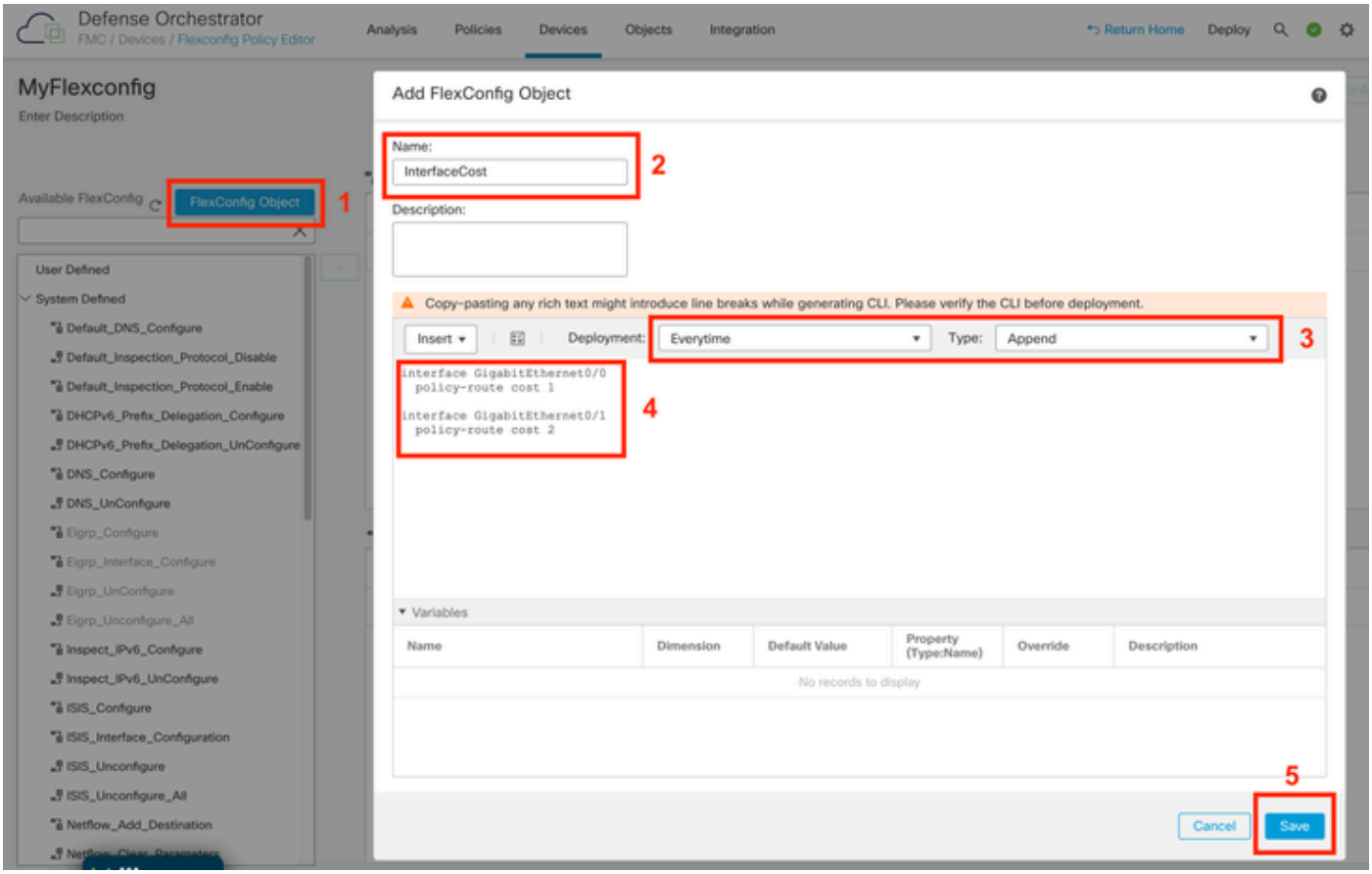



访问FlexConfig菜单

2. 创建新的FlexConfig对象：

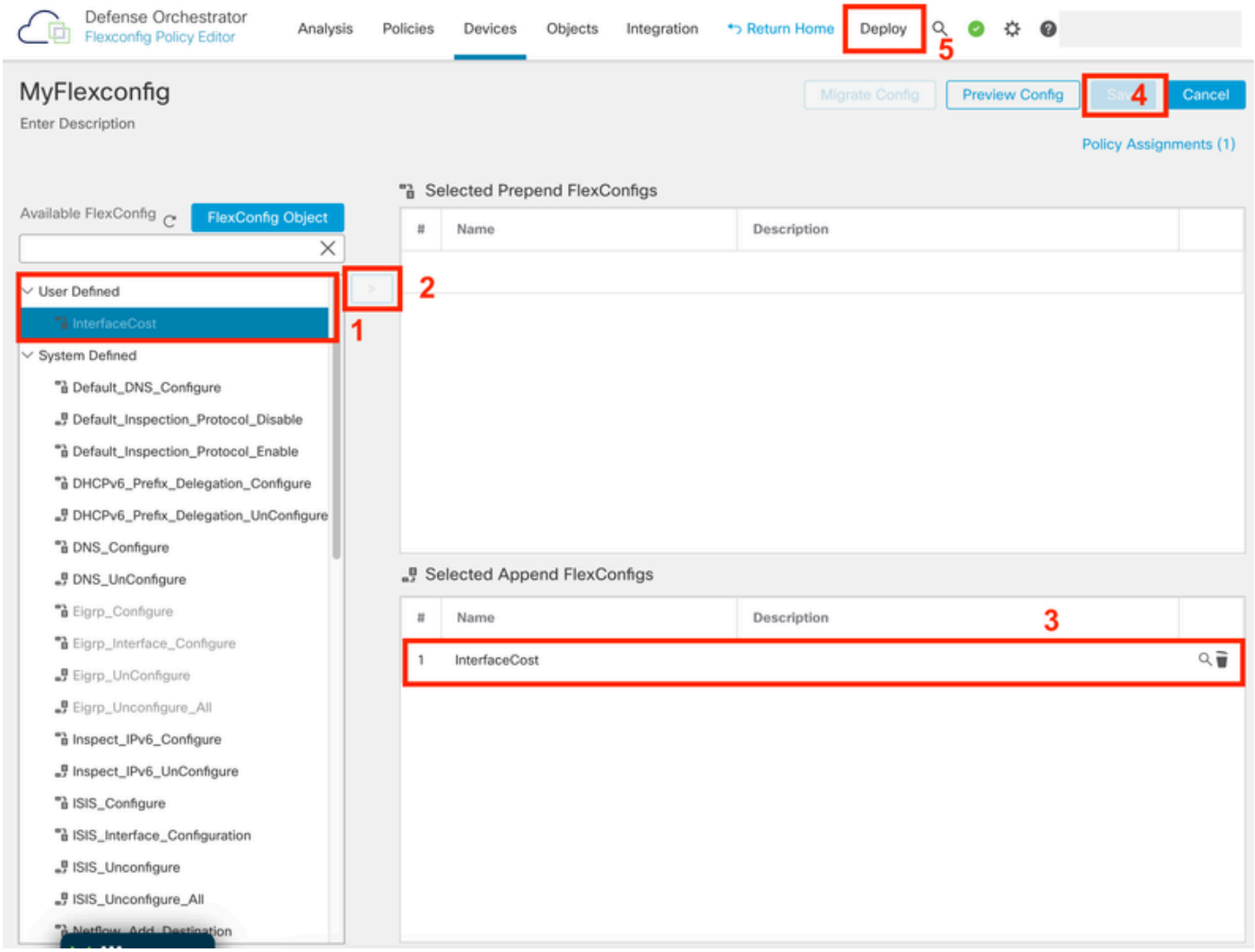
- 为FlexConfig对象命名。
- 在Deployment和Type部分中分别选择Everytime和Append。
- 使用图22所示的下一命令设置接口的开销。
- Click Save.

```
<#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.
```



添加Flexconfig对象

3. 选择最近创建的对象，并将其添加到“选定的添加FlexConfigs”部分，如图所示。保存更改并部署配置。




将对象分配到Flexconfig策略

4. 部署更改。

# 验证

1. 要进行验证，请使用命令show network。形成冗余管理接口的新实例：

```
> 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. 现在接口是sftunnel域的一部分。您可以通过show sftunnel interfaces 和show running-config sftunnel 命令确认这一点：

```
<#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. 系统会自动拼写出基于策略的路由。如果未指定接口开销，则adaptive-interface选项会设置轮询处理以在两个接口之间负载均衡管理流量：

```
<#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. 使用show running-config interface <interface> 命令检查接口设置：

```
<#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
```

下列一些附加命令可用于检查已配置路由的跟踪：

<#root>

>

**show track**

```
Track 1
Response Time Reporter 2 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interfa
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 interfa
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
```

# 相关信息

- 思科技术支持和下载
- 通过Cisco Defense Orchestrator中的云交付防火墙管理中心管理防火墙威胁防御

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）。