在FMC管理的安全防火墙上配置NAT 64

目录

简介

本文档介绍如何在由火力管理中心(FMC)管理的Firepower威胁防御(FTD)上配置NAT64。

先决条件

要求

思科建议您了解安全防火墙威胁防御和安全防火墙管理中心。

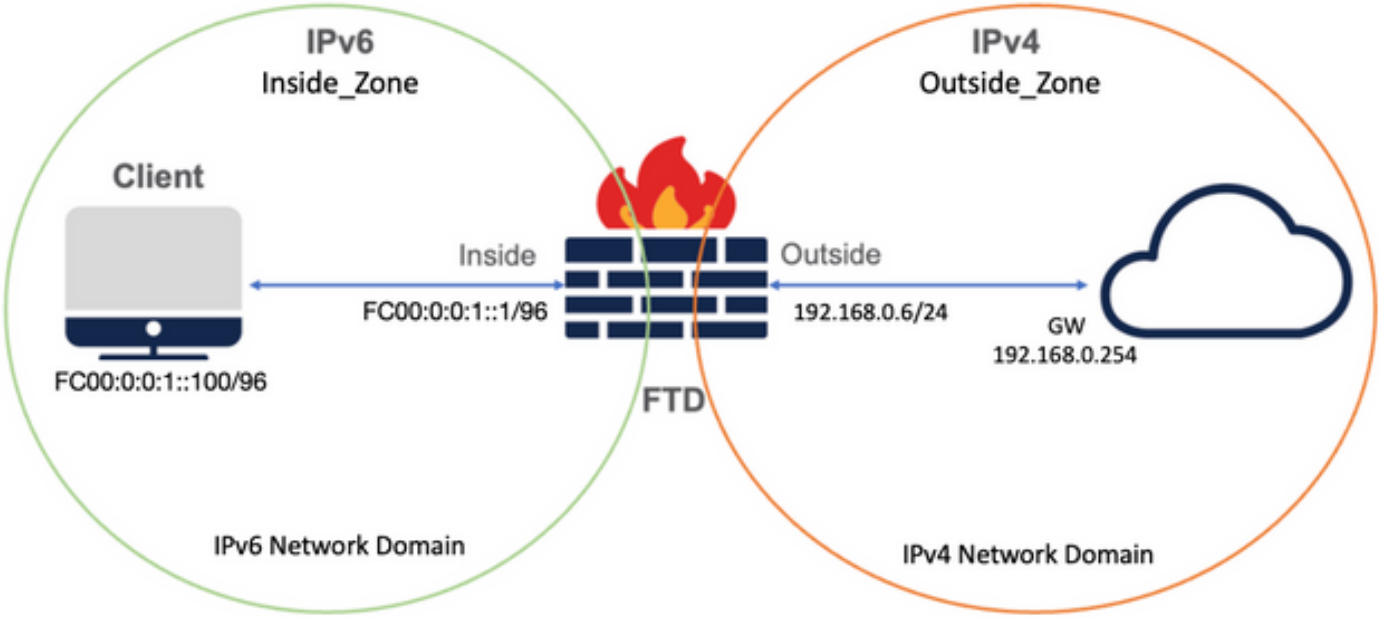
使用的组件

- Firepower管理中心7.0.4。
- Firepower威胁防御7.0.4。

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

网络图

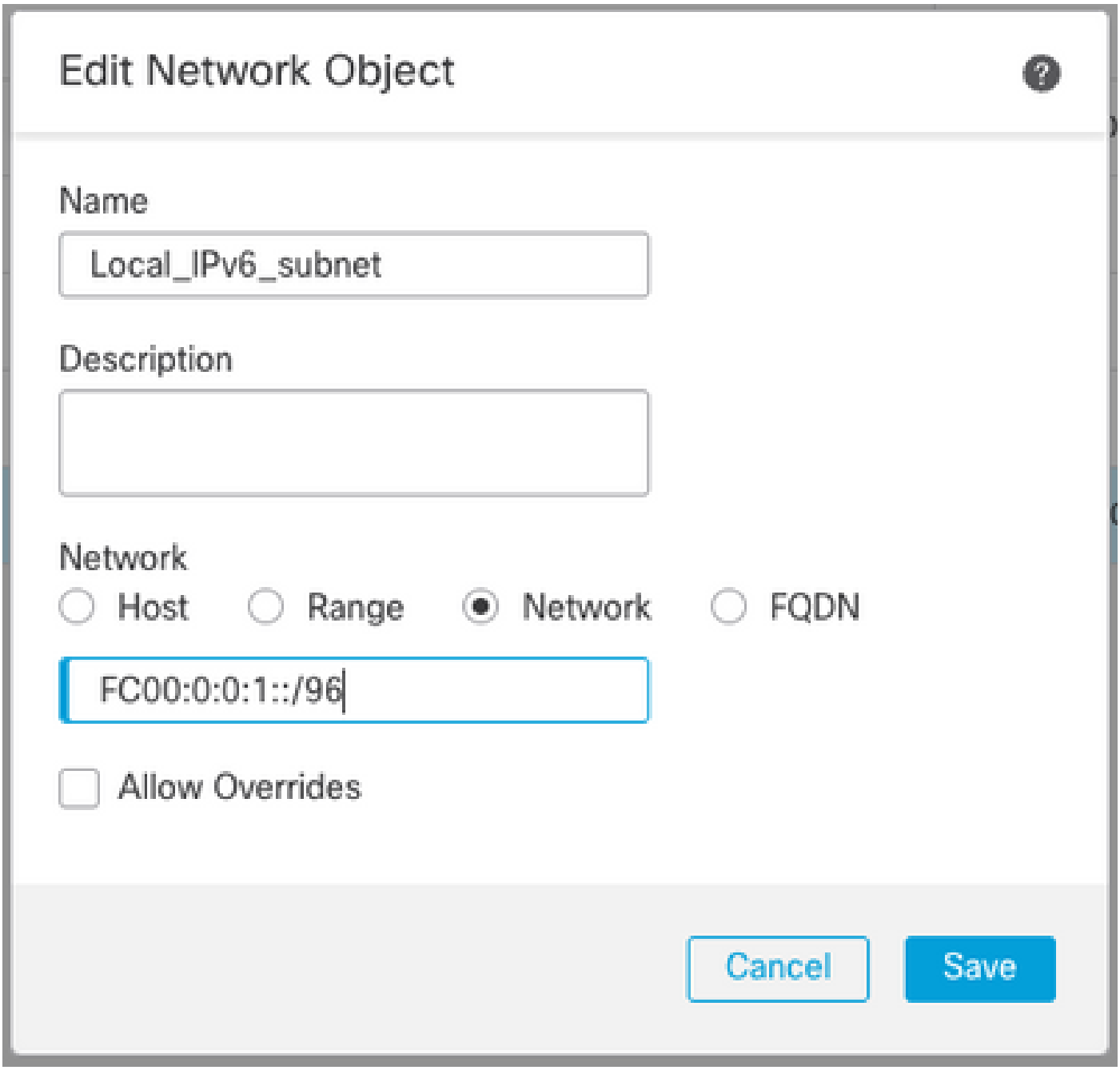


配置网络对象

- IPv6网络对象，用于引用内部IPv6客户端子网。

在FMC GUI上，导航到Objects > Object Management > Select Network from left Menu > Add Network > Add Object。

例如，使用IPv6子网FC00:0:0:1::/96创建网络对象Local_IPv6_subnet。

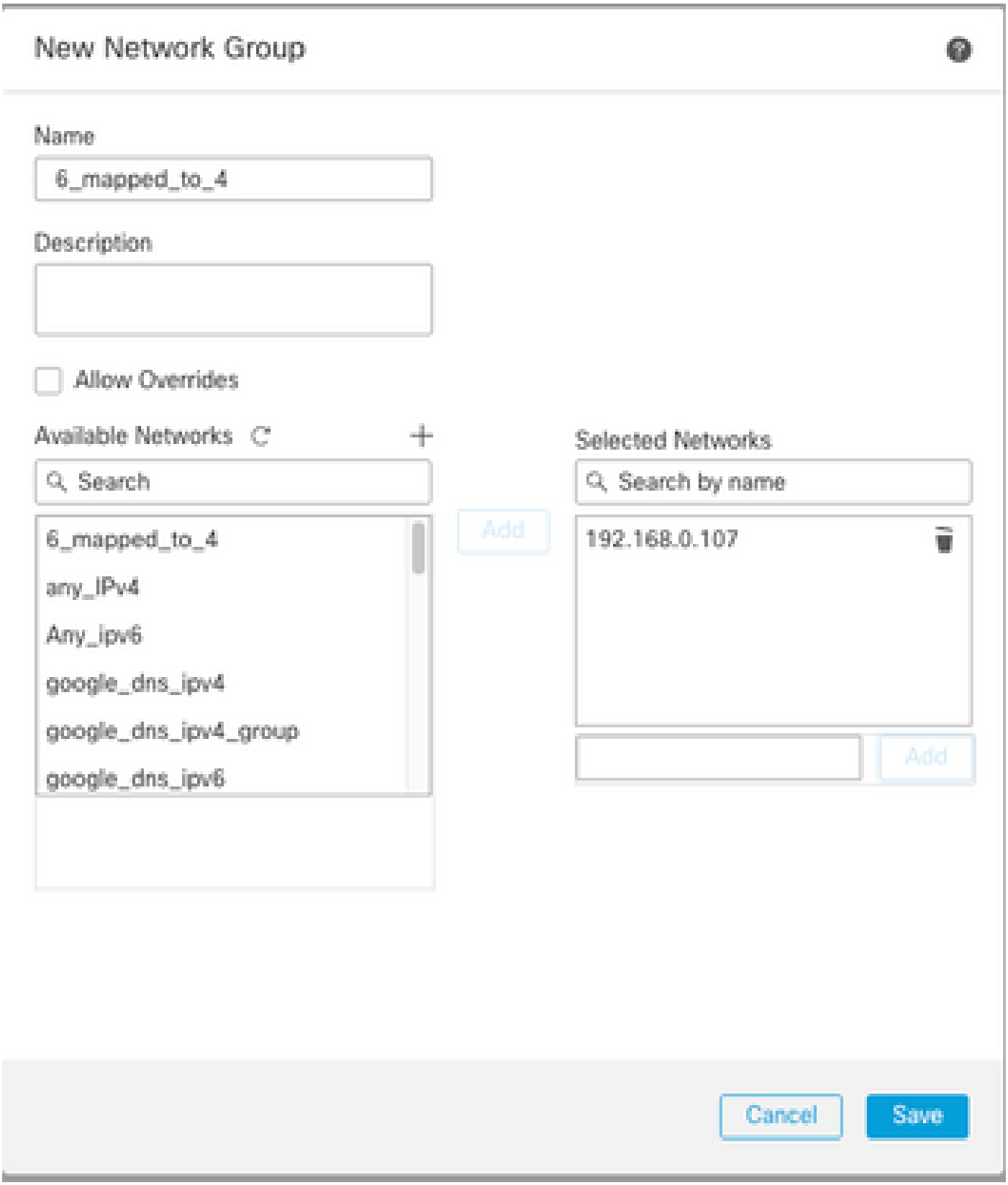


- 将IPv6客户端转换为IPv4的IPv4网络对象。

在FMC GUI上，导航到Objects > Object Management > Select Network from left Menu > Add Network > Add Group。

例如，使用IPv4主机192.168.0.107创建网络对象6_mapped_to_4。

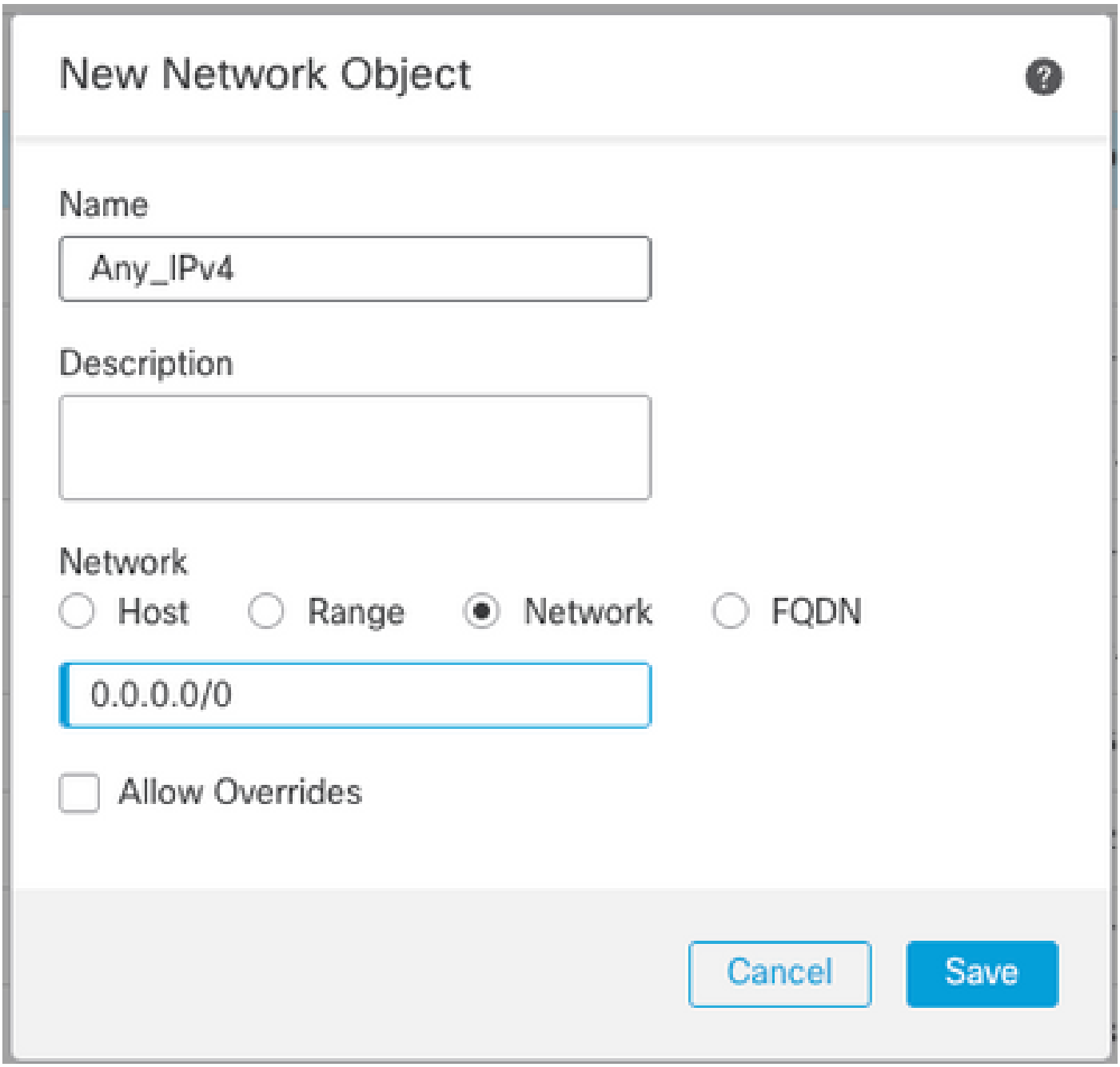
根据要在IPv4中映射的IPv6主机数量，可以使用单个对象网络、具有多个IPv4的网络组，或者仅使用NAT到出口接口。



- IPv4网络对象，用于引用Internet上的外部IPv4主机。

在FMC GUI上，导航到Objects > Object Management > Select Network from left Menu > Add Network > Add Object。

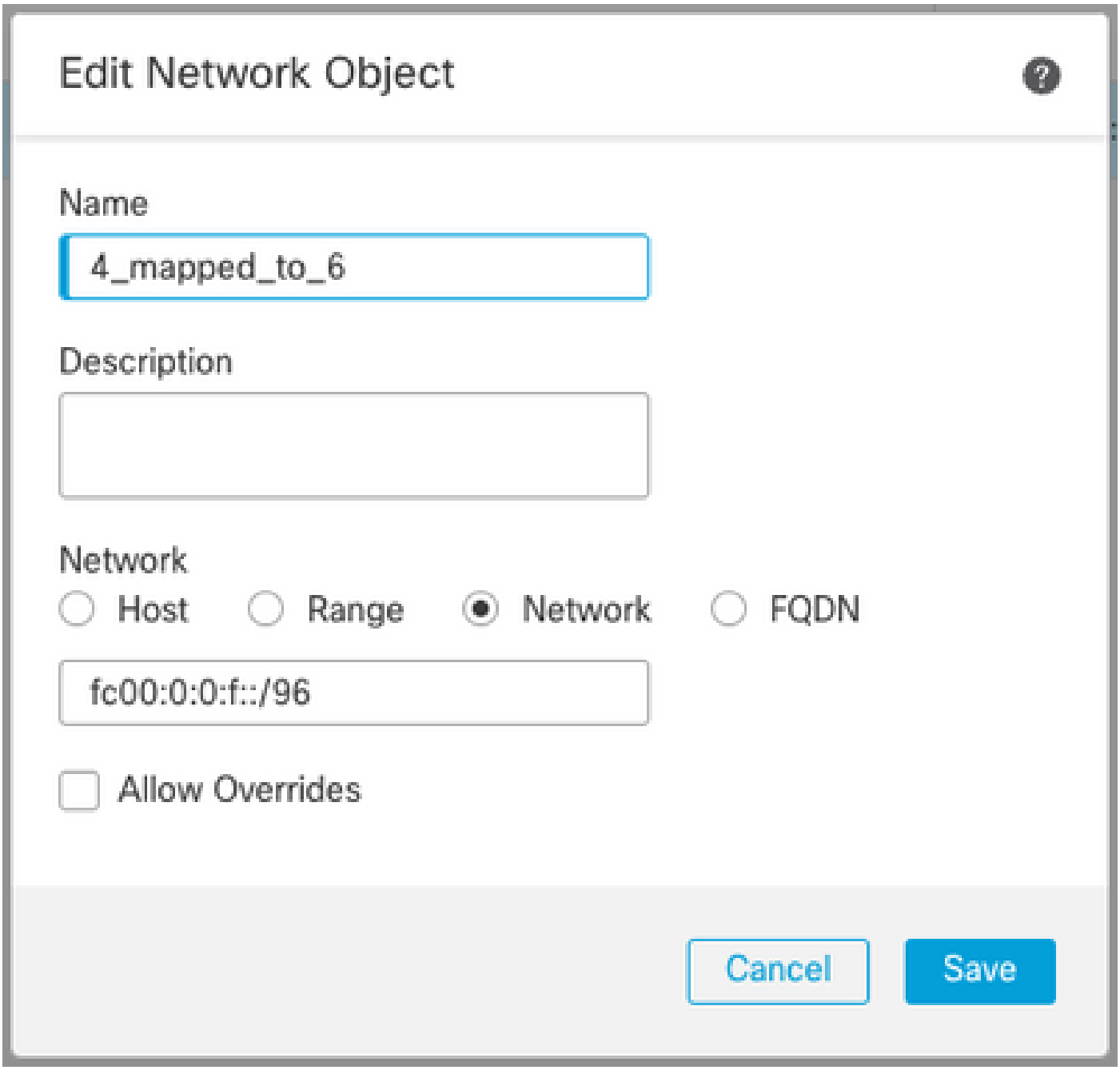
例如，使用IPv4子网0.0.0.0/0创建网络对象Any_IPv4。



- IPv6网络对象，用于将外部IPv4主机转换到IPv6域。

在FMC GUI上，导航到Objects > Object Management > Select Network from left Menu > Add Network > Add Object。

例如，使用IPv6子网FC00:0:0:F::/96创建网络对象4_mapped_to_6。



在FTD上为IPv4/IPv6配置接口

导航到Devices > Device Management > Edit FTD > Interfaces并配置内部和外部接口。

示例：

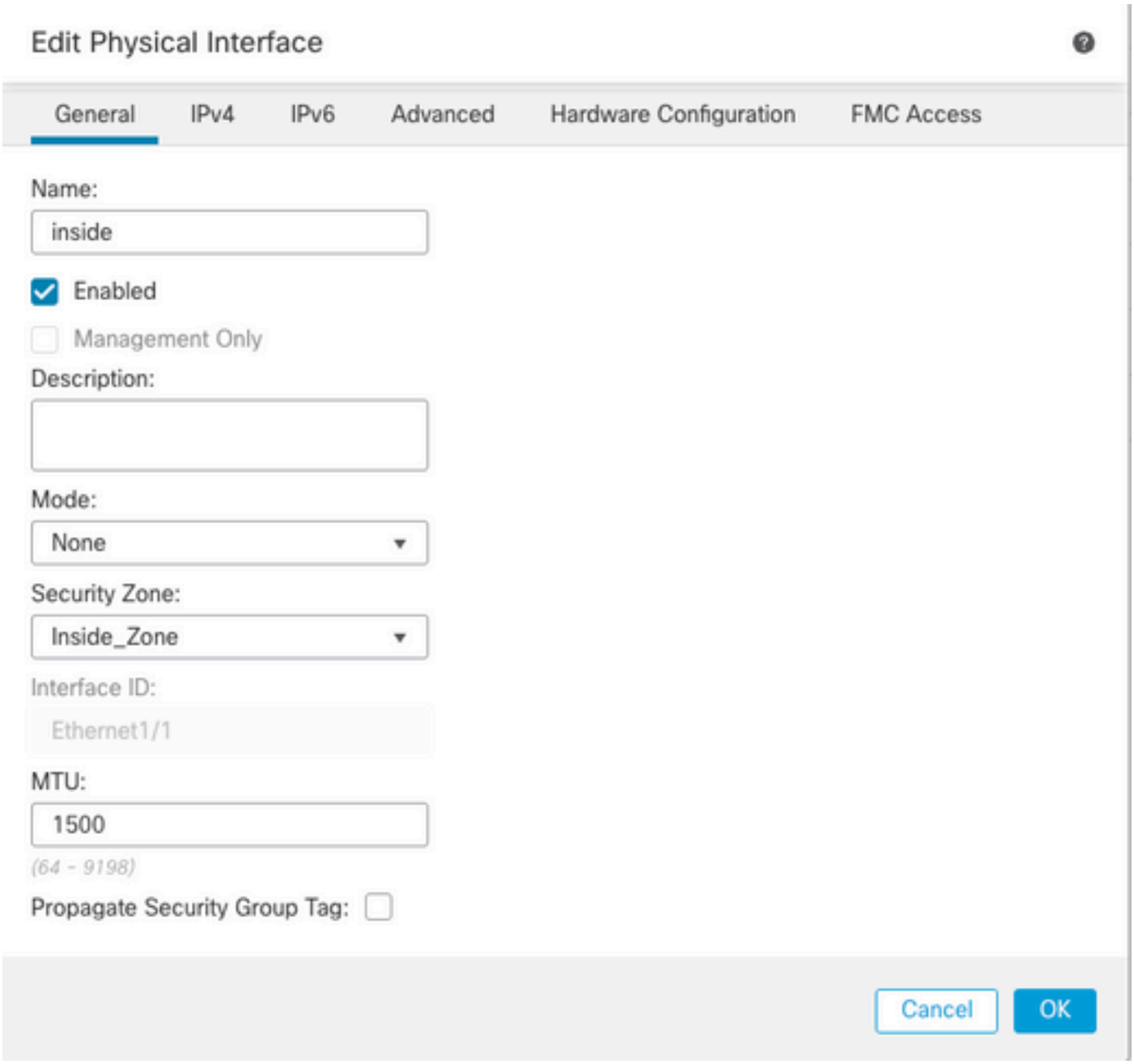
接口Ethernet 1/1

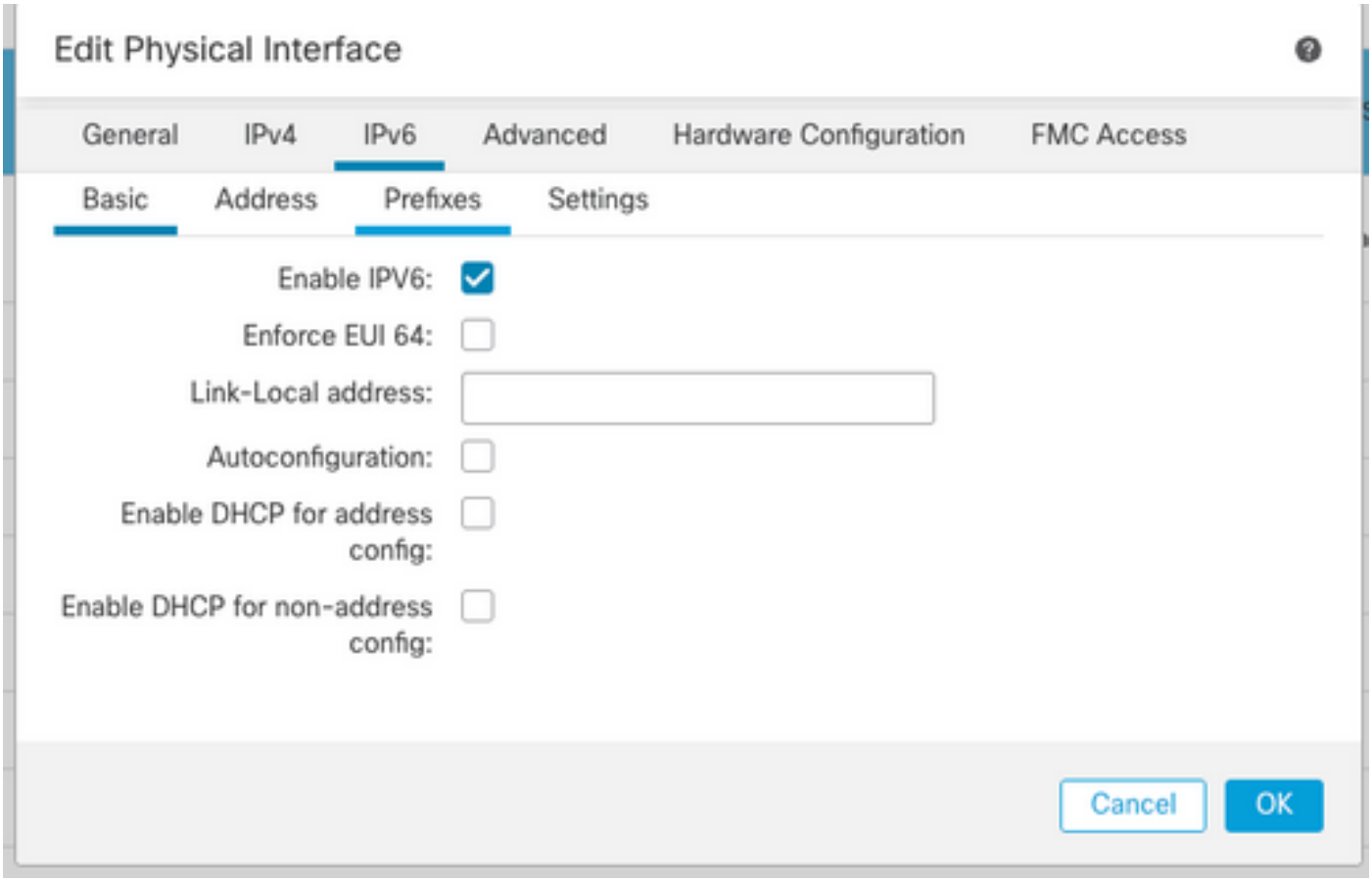
名称：内部

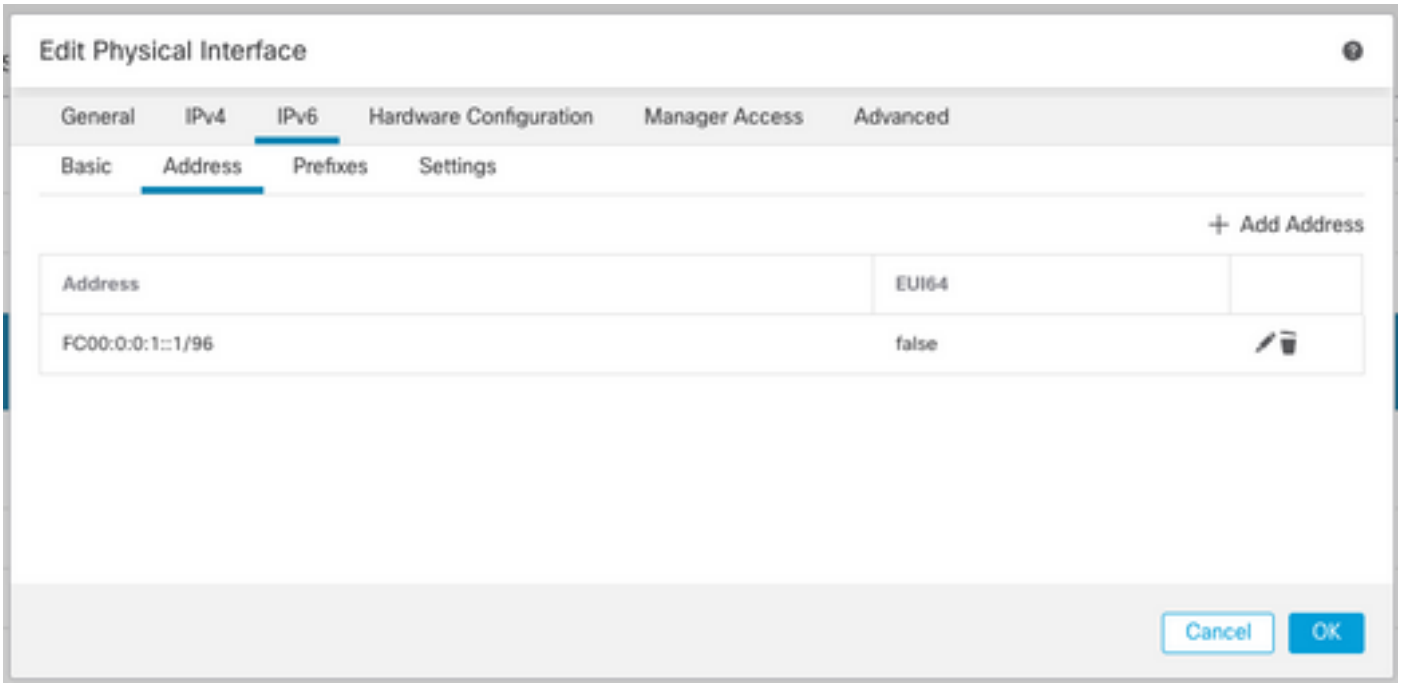
安全区域：Inside_Zone

如果未创建安全区域，您可以在Security Zone（安全区域）下拉菜单> New（新建）中创建安全区域。

IPv6地址：FC00:0:0:1::1/96







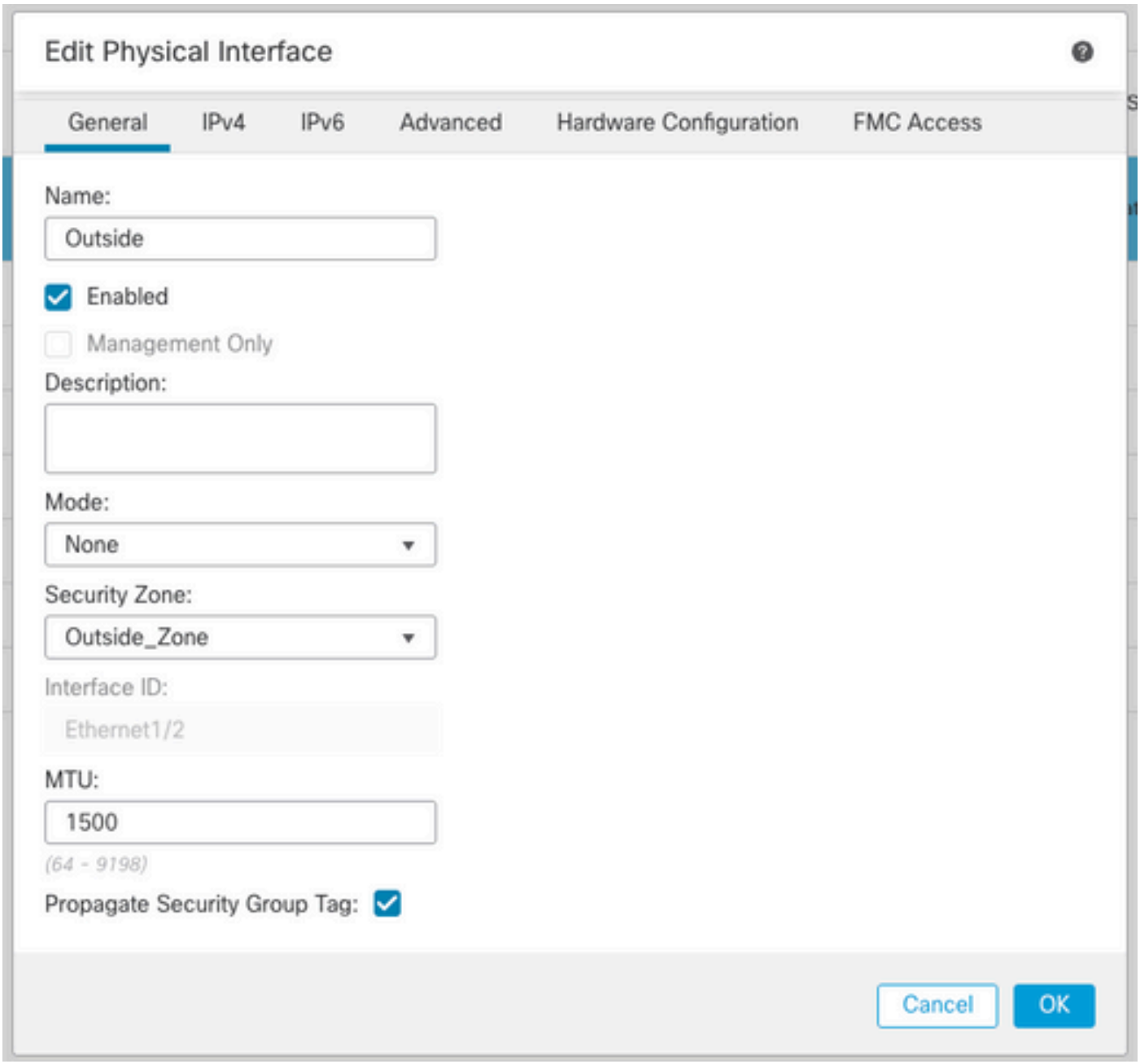
接口Ethernet 1/2

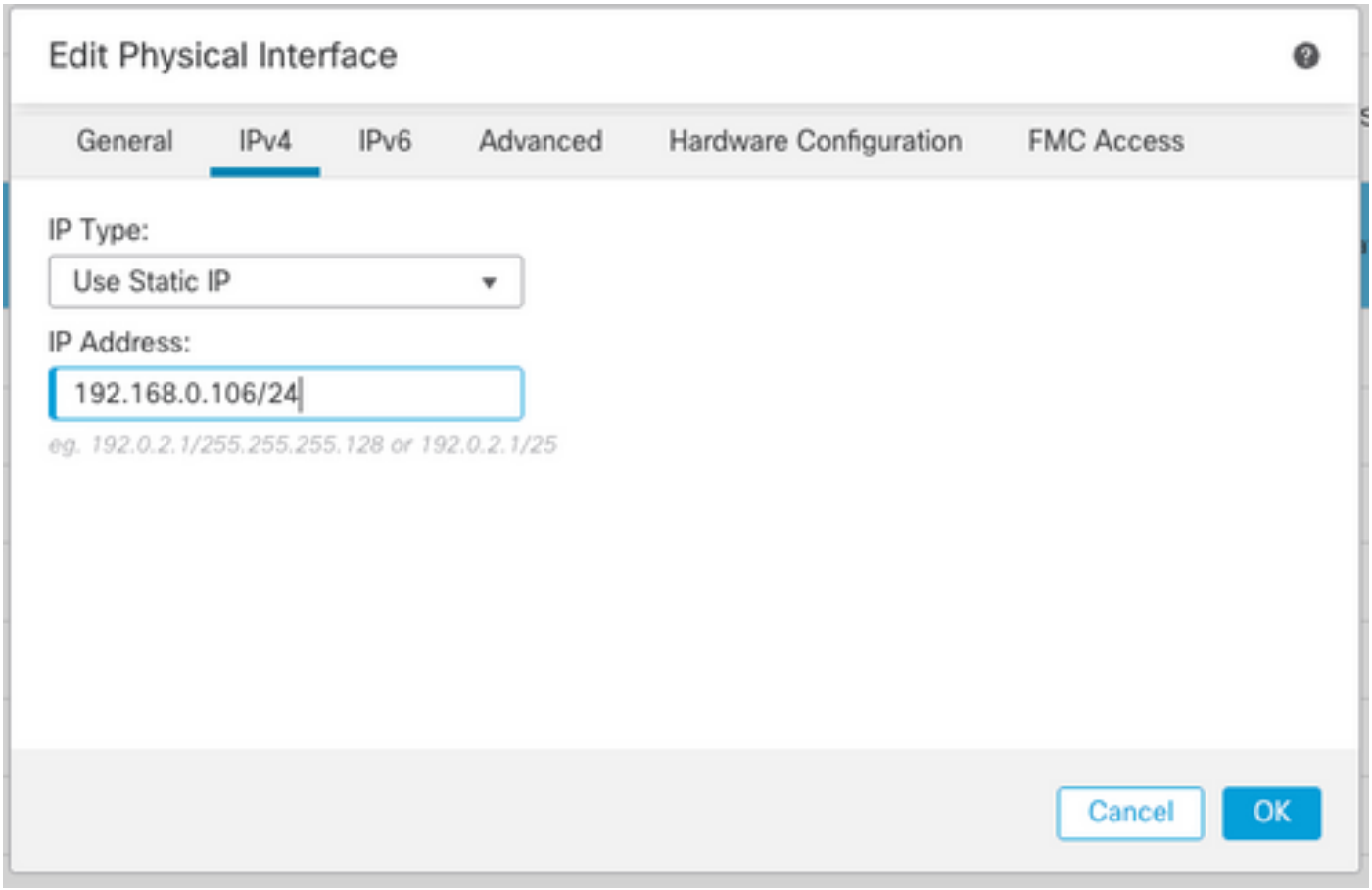
名称：外部

安全区域：Outside_Zone

如果未创建安全区域，您可以在“安全区域”(Security Zone)下拉菜单>“新建”(New)中创建安全区域。

IPv4地址：192.168.0.106/24

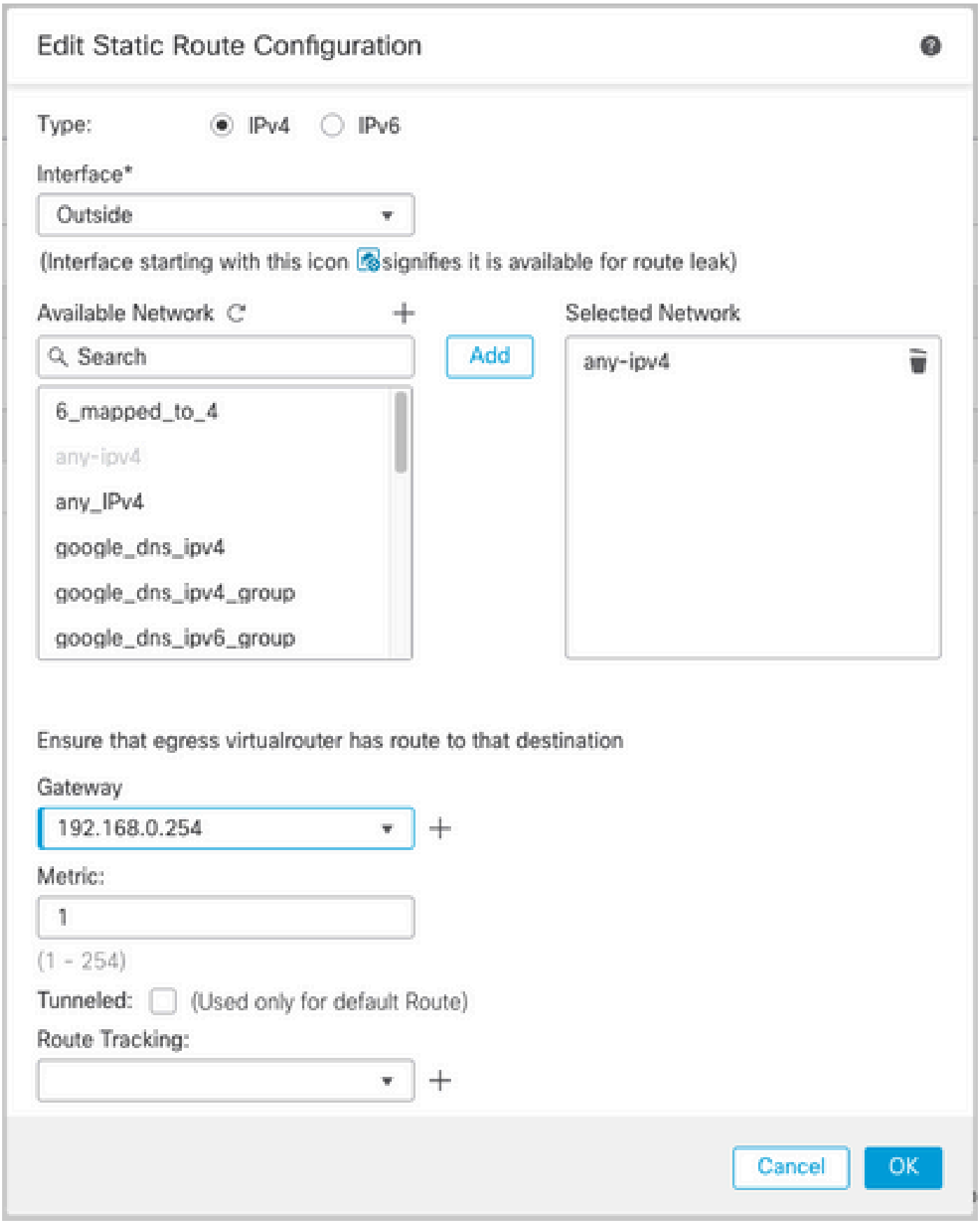


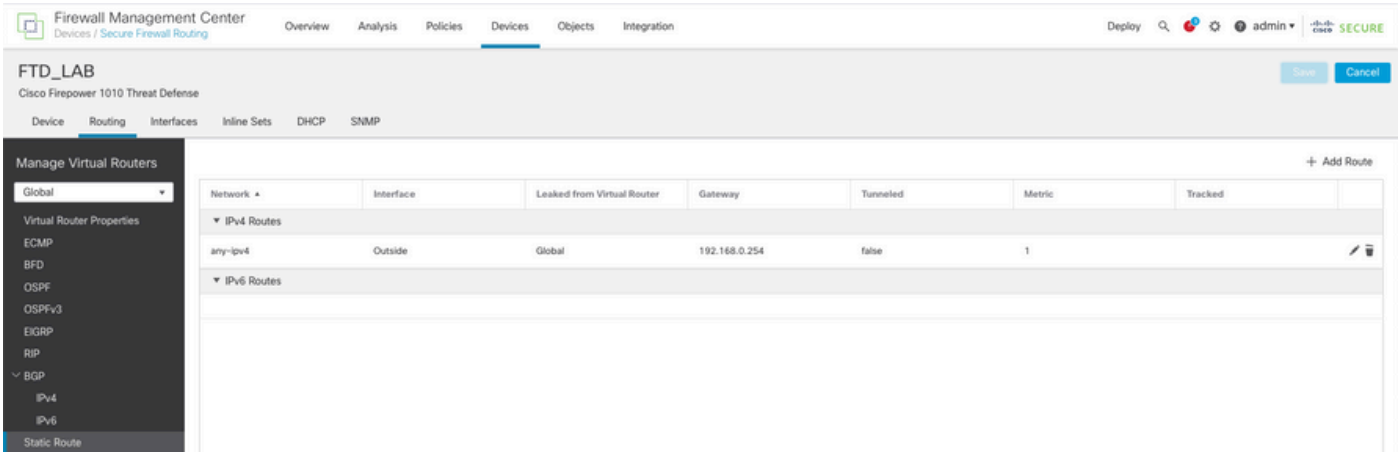


配置默认路由

导航到Devices > Device Management > Edit FTD > Routing > Static Routing > Add Route。

例如，在网关为192.168.0.254的外部接口上的默认静态路由。

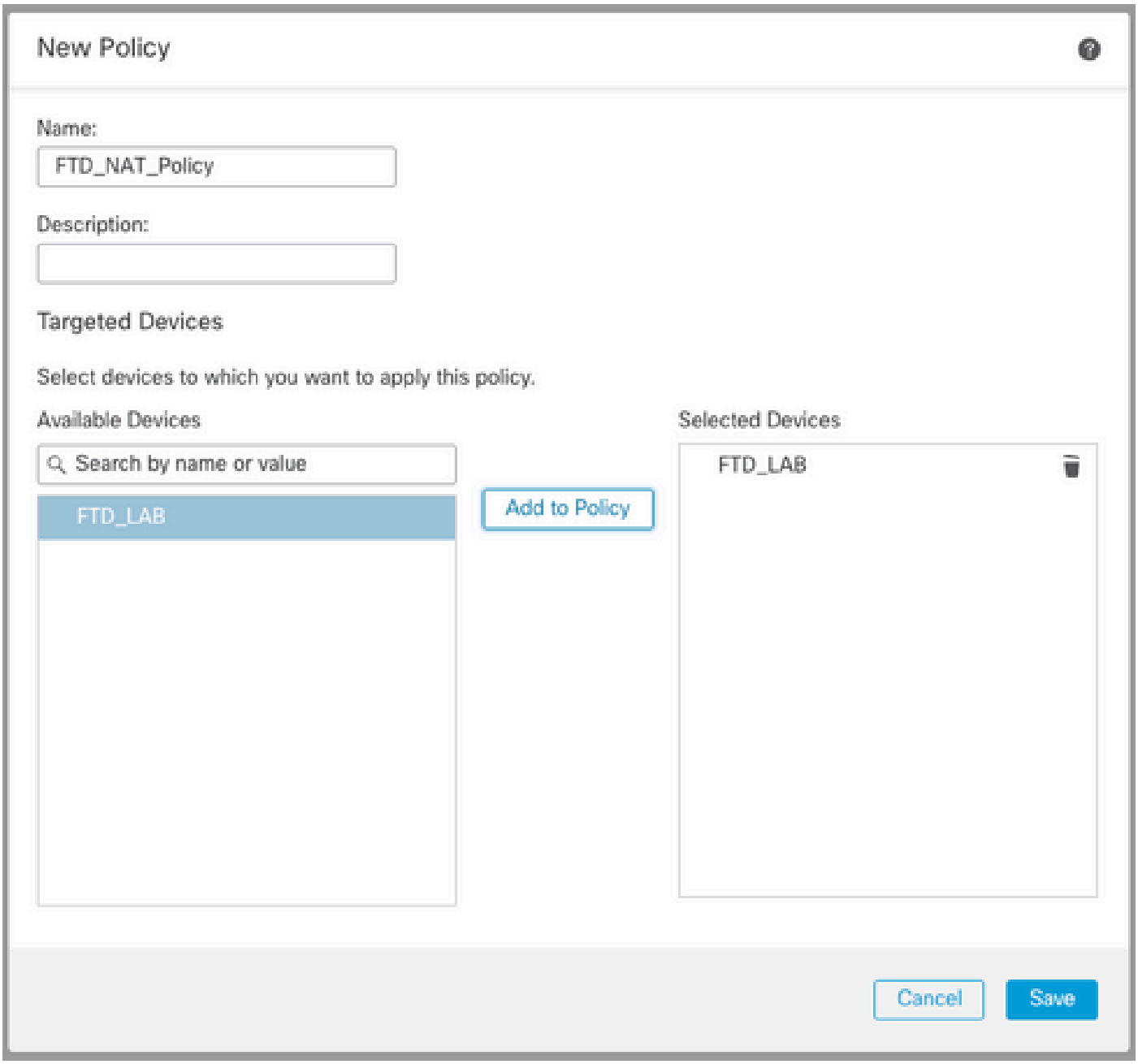

Edit Static Route Configuration
Type:
IPv4
IPv6
Interface*
Outside
(Interface starting with this icon signifies it is available for route leak)
Available Network
Search
6_mapped_to_4
any-ipv4
any_IPv4
google_dns_ipv4
google_dns_ipv4_group
google_dns_ipv6_group
Add
Selected Network
any-ipv4
Ensure that egress virtualrouter has route to that destination
Gateway
192.168.0.254
Metric:
1
(1 - 254)
Tunneled:
(Used only for default Route)
Route Tracking:
Cancel
OK



配置NAT策略

在FMC GUI上，导航到设备(Devices)> NAT >新策略(New Policy)>威胁防御NAT，并创建NAT策略。

例如，创建NAT策略FTD_NAT_Policy并将其分配给测试FTD FTD_LAB。



配置NAT规则

出站NAT。

在FMC GUI上，导航到Devices > NAT > Select the NAT policy > Add Rule 并创建NAT规则，以将内部IPv6网络转换为外部IPv4池。

例如，网络对象Local_IPv6_subnet动态转换为网络对象6_mapped_to_4。

NAT规则：自动NAT规则

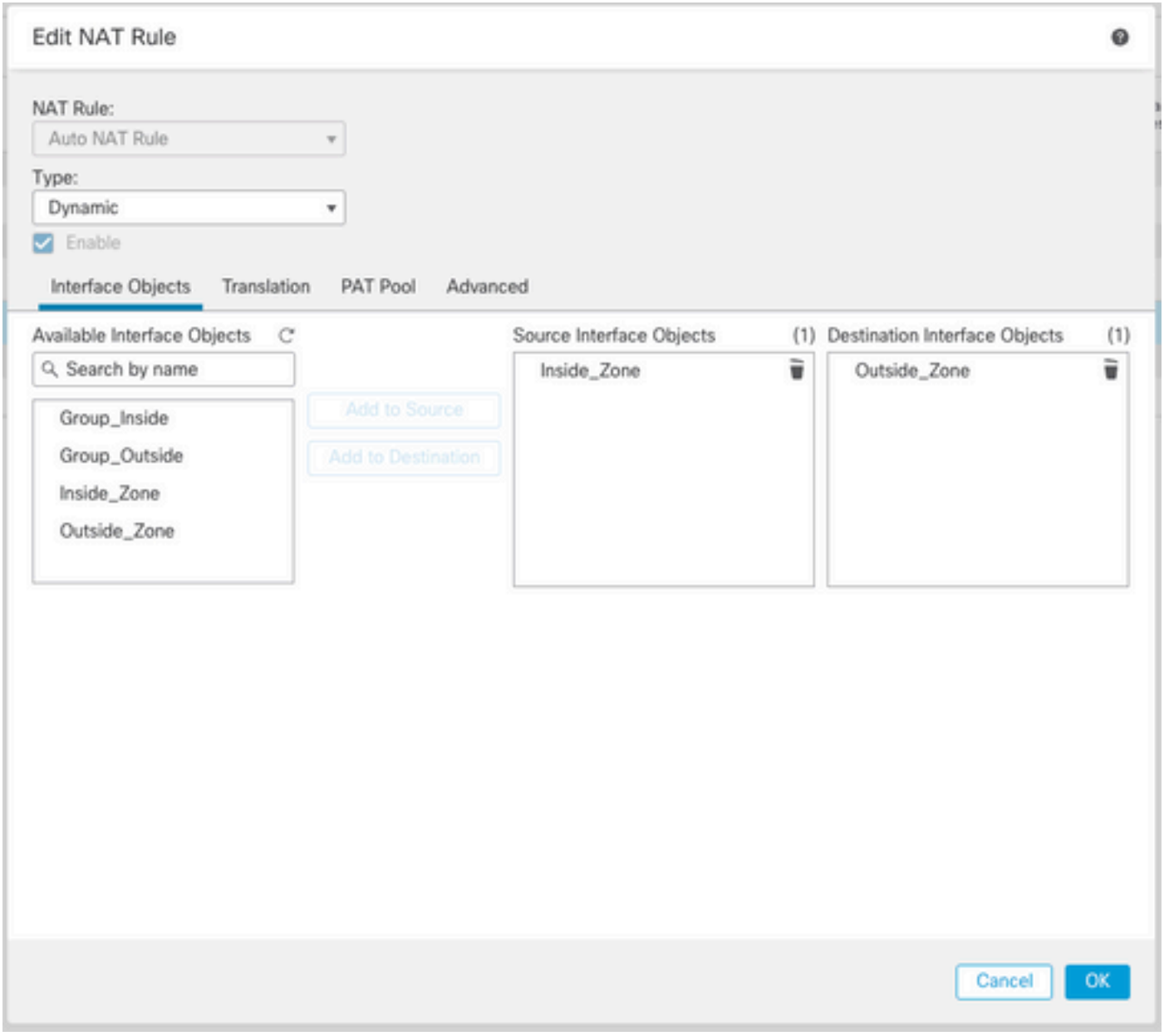
类型：动态

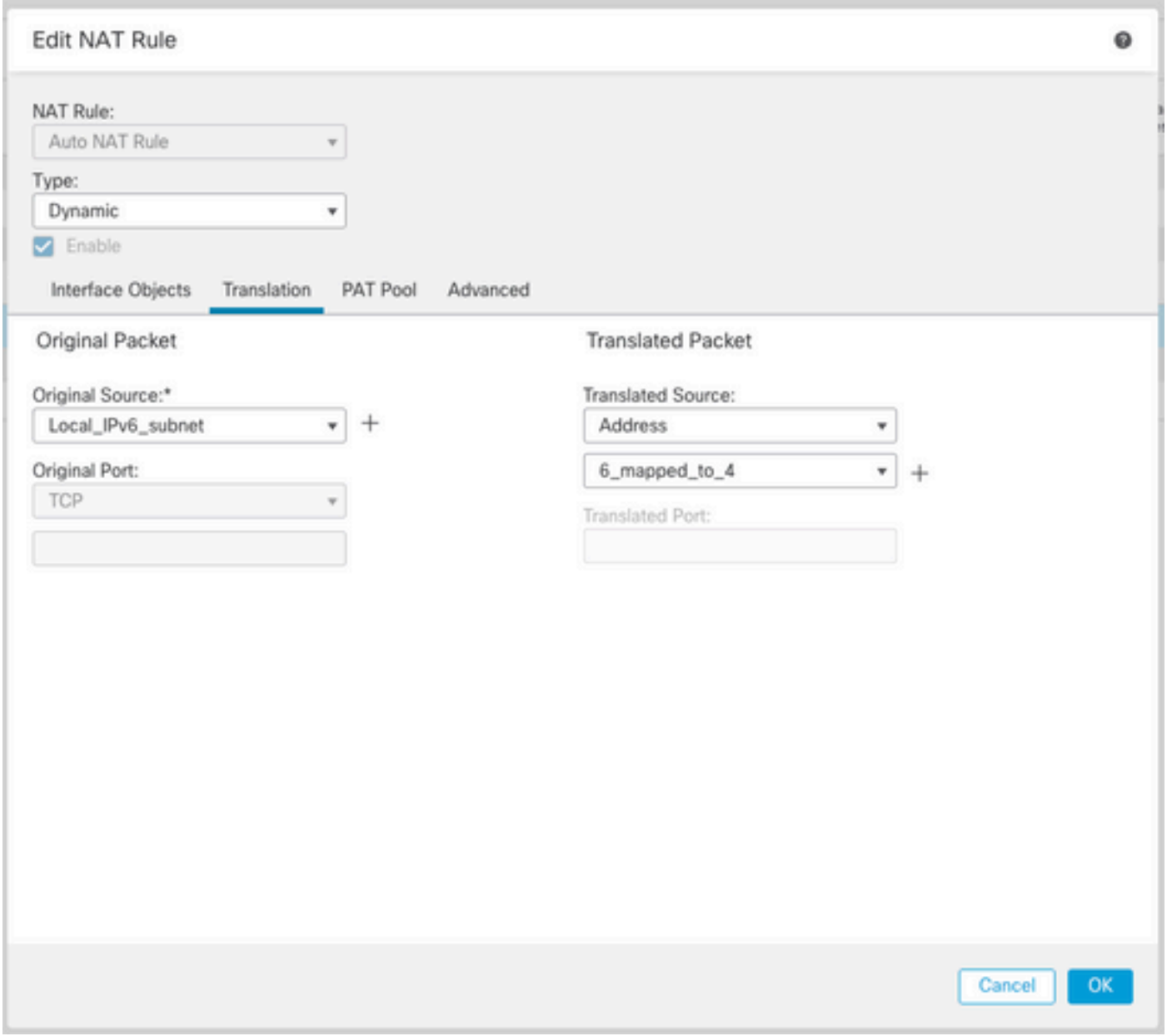
源接口对象：Inside_Zone

目标接口对象：Outside_Zone

原始源：Local_IPv6_subnet

转换后的源：6_mapped_to_4





入站NAT。

在FMC GUI上，导航到Devices > NAT > Select the NAT policy > Add Rule，并创建NAT规则，以将外部IPv4流量转换为内部IPv6网络池。这允许与本地IPv6子网进行内部通信。

此外，请在此规则上启用DNS重写，以便将来自外部DNS服务器的回复从A(IPv4)转换为AAAA(IPv6)记录。

例如，Outside Network Any_IPv4被静态转换到对象4_mapped_to_6中定义的IPv6子网2100:6400::/96。

NAT规则：自动NAT规则

类型：静态

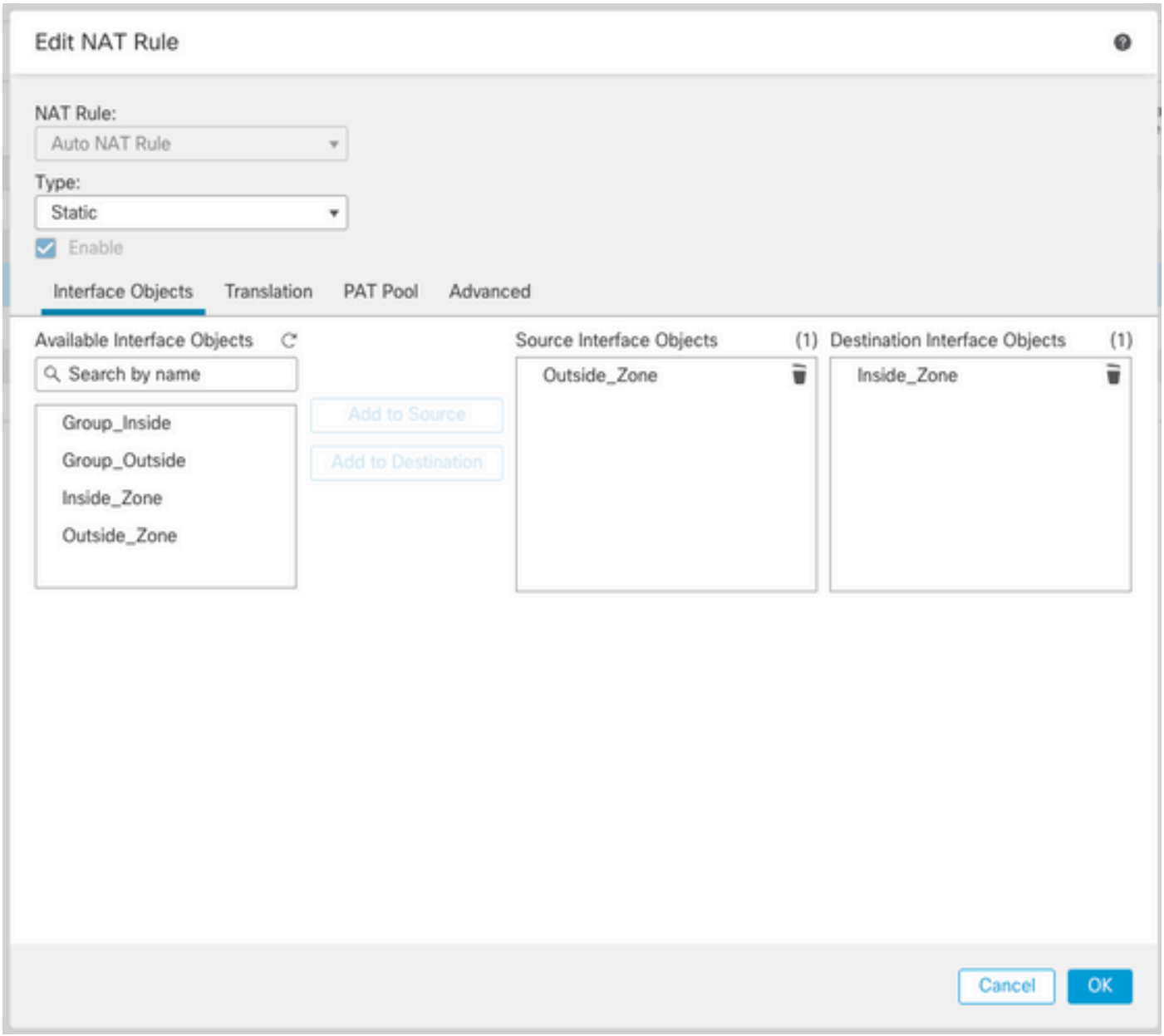
源接口对象：Outside_Zone

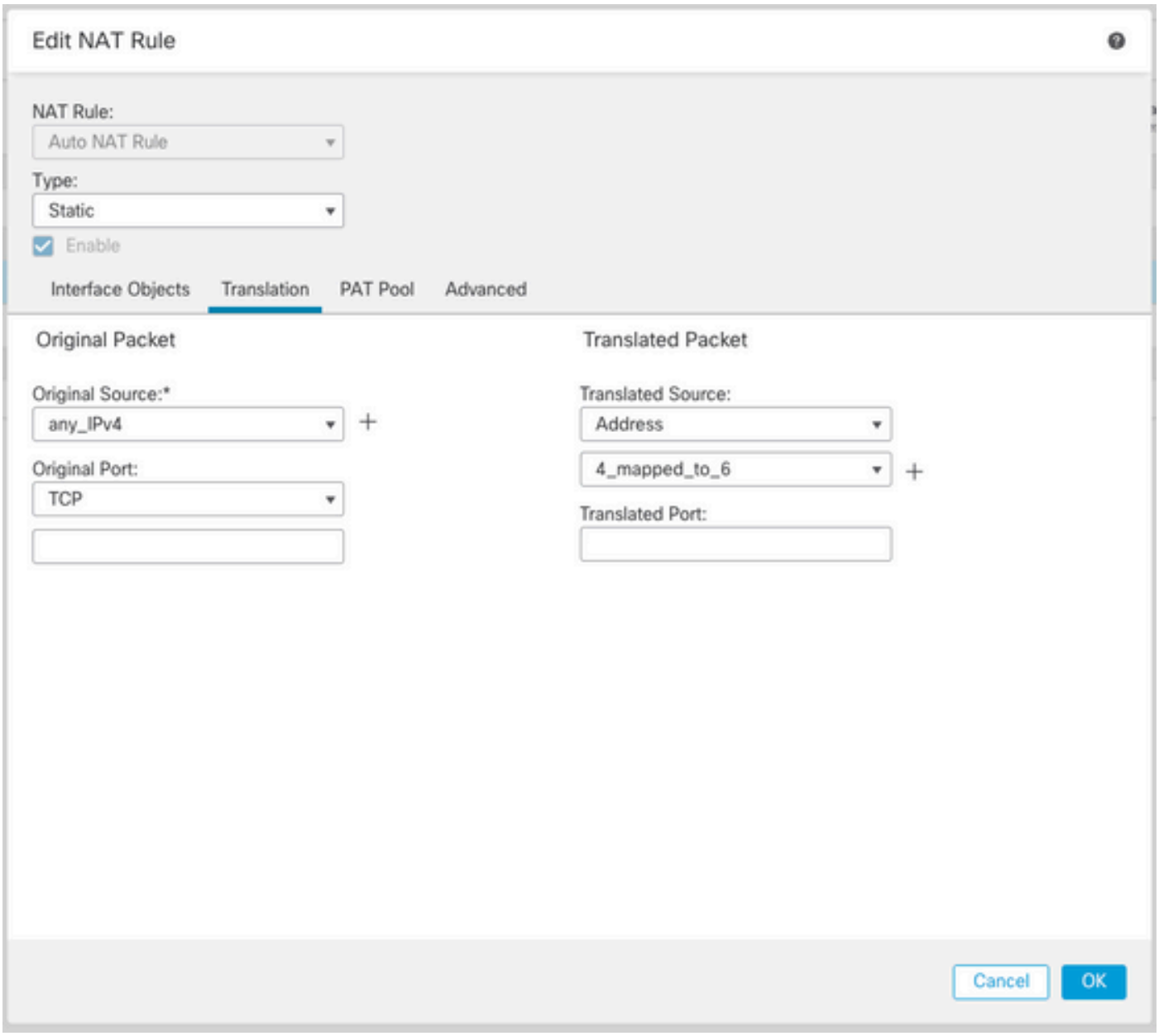
目标接口对象：Inside_Zone

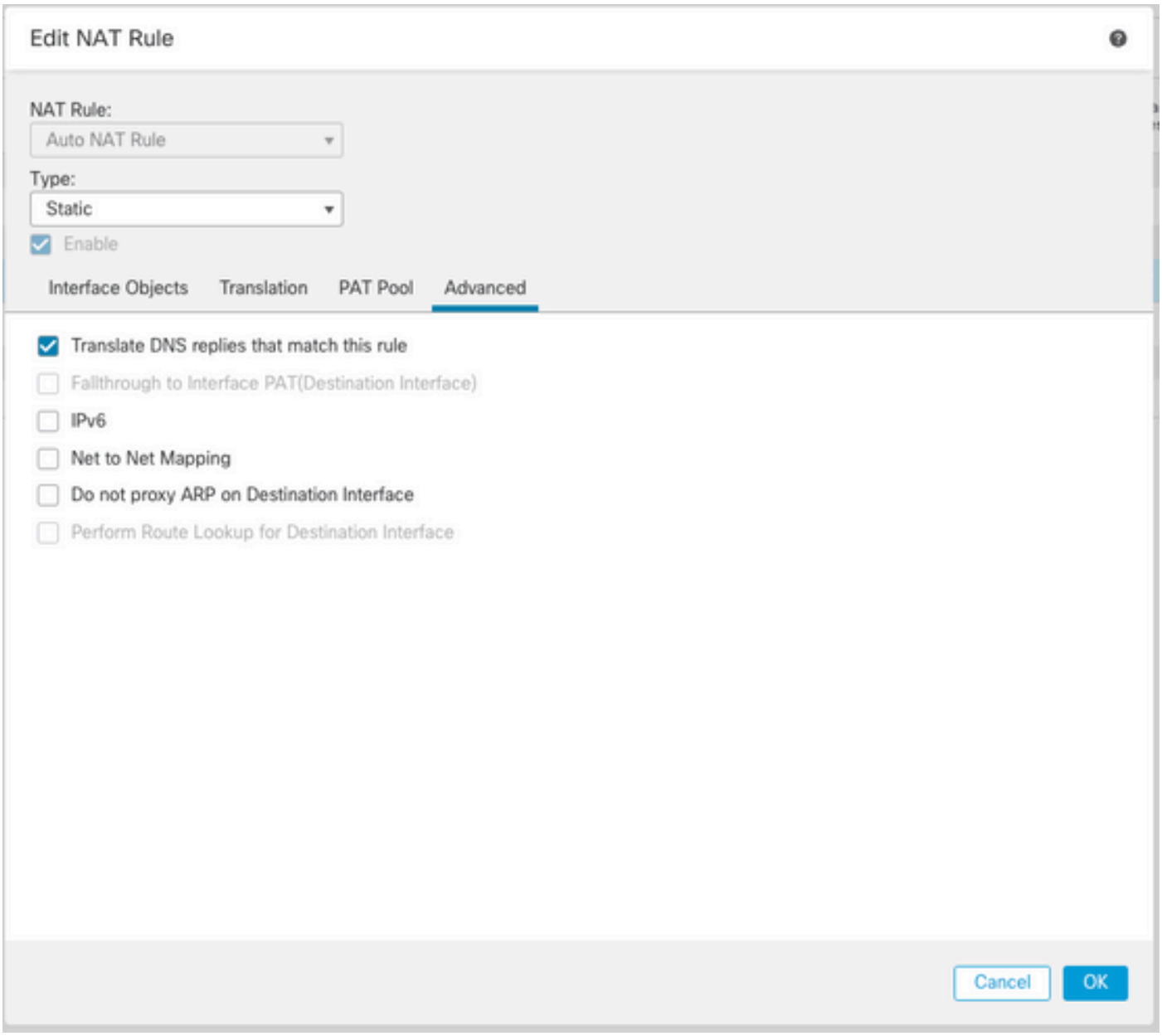
原始源：Any_IPv4

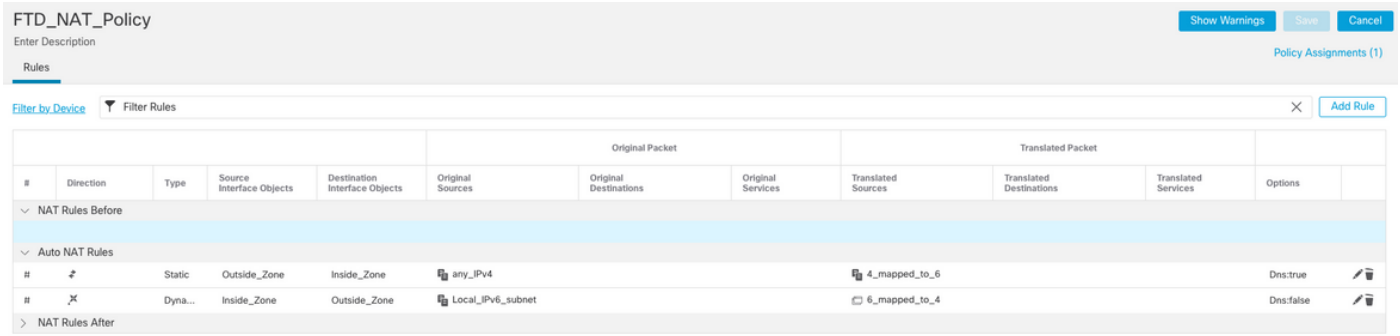
转换后的源：4_mapped_to_6

转换与此规则匹配的DNS应答：是（Enable复选框）




Edit NAT Rule
NAT Rule:
Auto NAT Rule
Type:
Static
Enable
Interface Objects
Translation
PAT Pool
Advanced
Original Packet
Original Source:*
any_IPv4
Original Port:
TCP
Translated Packet
Translated Source:
Address
4_mapped_to_6
Translated Port:
Cancel
OK





继续将更改部署到FTD。

确认

- 显示接口名称和IP配置。

<#root>

```
> show nameif

Interface Name Security
Ethernet1/1 inside 0
Ethernet1/2 Outside 0

> show ipv6 interface brief

inside [up/up]
fe80::12b3:d6ff:fe20:eb48
fc00:0:0:1::1

> show ip

System IP Addresses:
Interface    Name      IP address     Subnet mask
Ethernet1/2  Outside   192.168.0.106  255.255.255.0
```

- 确认从FTD内部接口到客户端的IPv6连接。

IPv6内部主机IP fc00:0:0:1::100

FTD内部接口fc00:0:0:1::1。

<#root>

```
> ping fc00:0:0:1::100

Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to fc00:0:0:1::100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- 显示FTD CLI上的NAT配置。

<#root>

```
> show running-config nat
!

object network Local_IPv6_subnet
nat (inside,Outside) dynamic 6_mapped_to_4
object network any_IPv4
nat (Outside,inside) static 4_mapped_to_6 dns
```

- 捕获流量。

例如，捕获从内部IPv6主机fc00:0:0:1::100到DNS服务器的流量为fc00::f:0:0:ac10:a64 UDP 53。

此处，目的DNS服务器为fc00::f:0:0:ac10:a64。最后32位是ac10:0a64。这些位逐个二进制八位数等于172、16、10、100。Firewall 6-to-4将IPv6 DNS服务器fc00::f:0:0:ac10:a64转换为等效的IPv4 172.16.10.100。

<#root>

```
> capture test interface inside trace match udp host fc00:0:0:1::100 any6 eq 53


> show capture test

2 packets captured
 1: 00:35:13.598052 fc00:0:0:1::100.61513 > fc00::f:0:0:ac10:a64.53: udp
 2: 00:35:13.638882 fc00::f:0:0:ac10:a64.53 > fc00:0:0:1::100.61513: udp



> show capture test packet-number 1



[...]
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network any_IPv4
nat (Outside,inside) static 4_mapped_to_6 dns
Additional Information:
NAT divert to egress interface Outside(vrfid:0)
Untranslate fc00::f:0:0:ac10:a64/53 to 172.16.10.100/53 <<<< Destination NAT

[...]
Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
object network Local_IPv6_subnet
nat (inside,Outside) dynamic 6_mapped_to_4
Additional Information:
Dynamic translate fc00:0:0:1::100/61513 to 192.168.0.107/61513 <<<<<<<< Source NAT



> capture test2 interface Outside trace match udp any any eq 53


2 packets captured

 1: 00:35:13.598152 192.168.0.107.61513 > 172.16.10.100.53: udp
 2: 00:35:13.638782 172.16.10.100.53 > 192.168.0.107.61513: udp
```

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）。