在FMC管理的安全防火牆上配置NAT 64

目錄

簡介

本文檔介紹如何在由Fire Power Management Center(FMC)管理的Firepower威脅防禦(FTD)上配置NAT64。

必要條件

需求

思科建議您瞭解安全防火牆威脅防禦和安全防火牆管理中心。

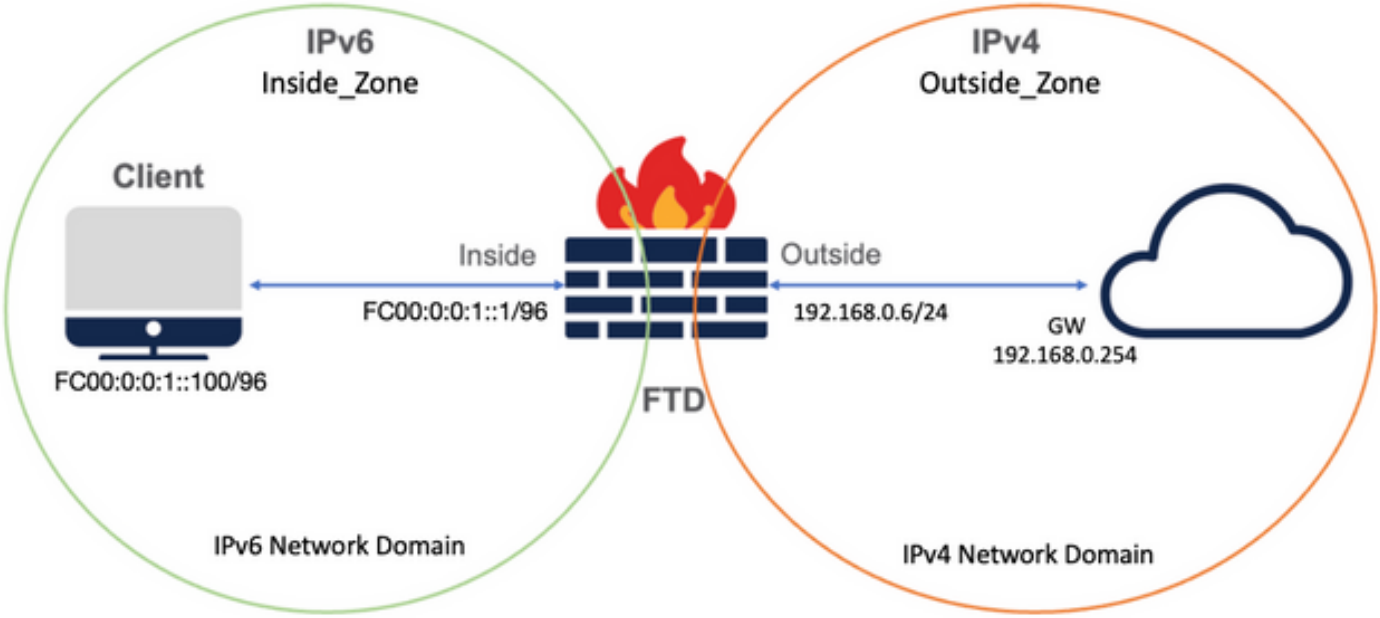
採用元件

- Firepower管理中心7.0.4.
- Firepower威脅防禦7.0.4.

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表

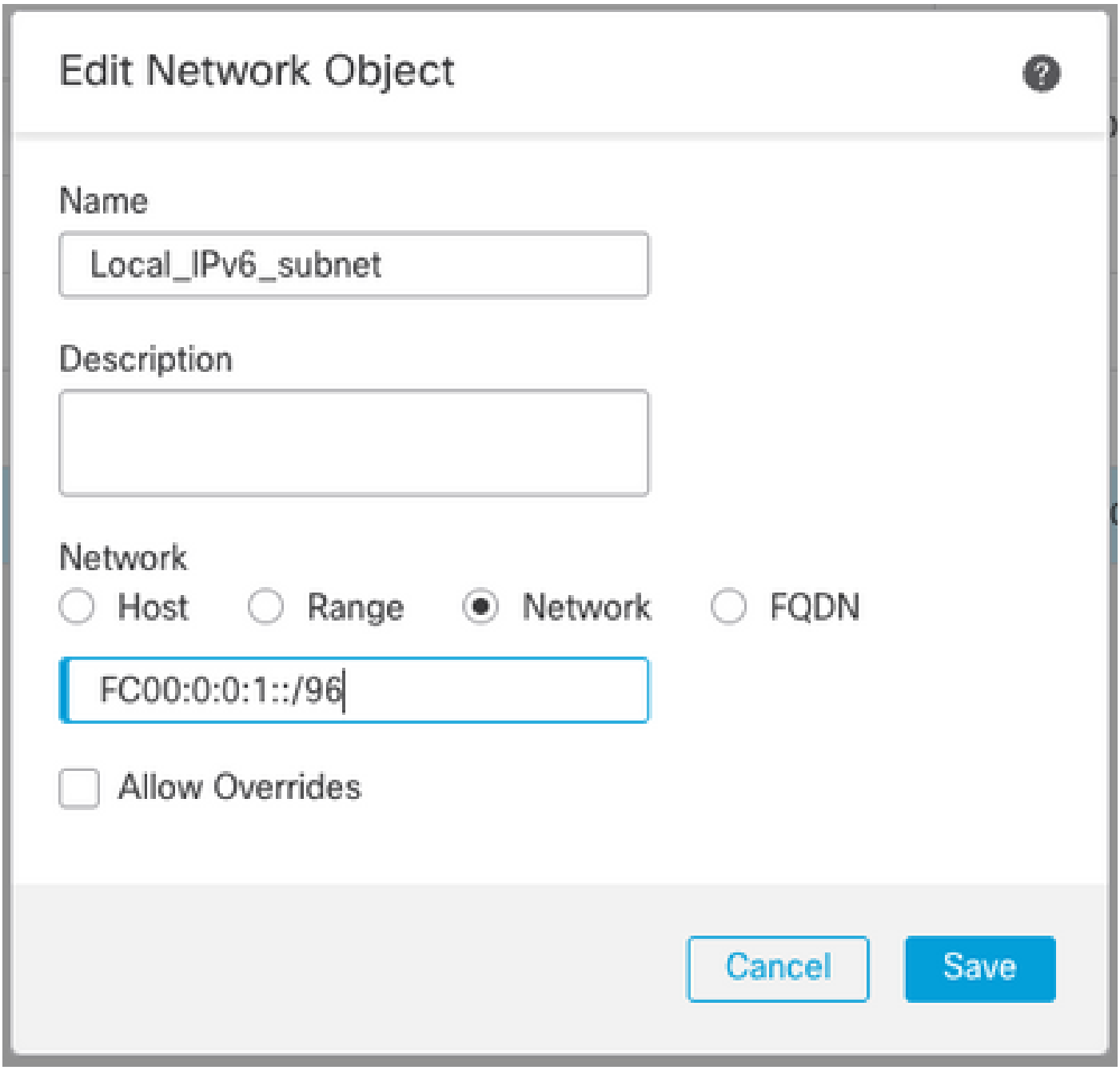


配置網路對象

- 用於引用內部IPv6客戶端子網的IPv6網路對象。

在FMC GUI上，導航至Objects > Object Management > Select Network from Left Menu > Add Network > Add Object。

例如，使用IPv6子網FC00:0:0:1::/96建立網路對象Local_IPv6_subnet。

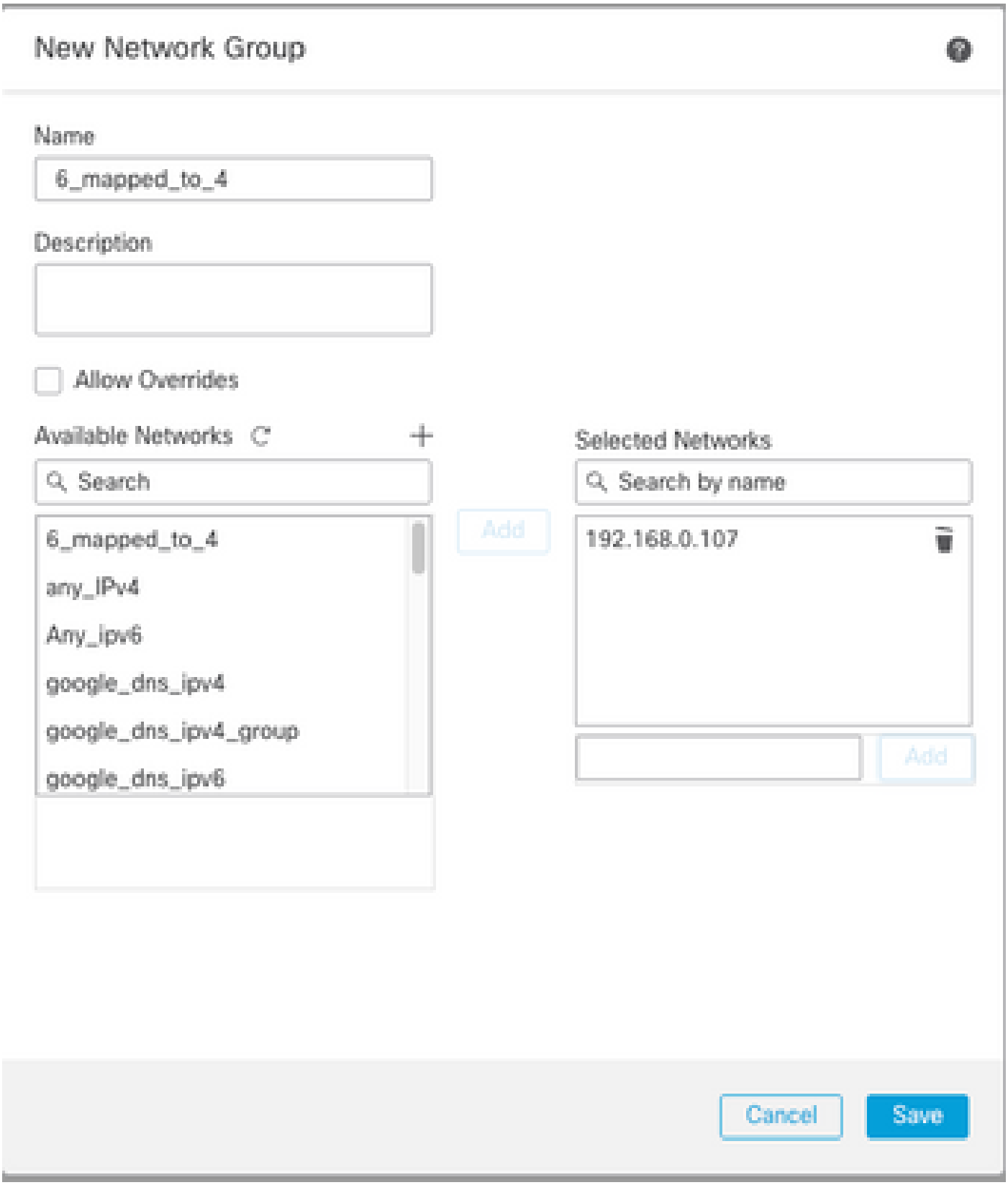


- IPv4網路對象，用於將IPv6客戶端轉換為IPv4。

在FMC GUI上，導航至Objects > Object Management > Select Network from Left Menu > Add Network > Add Group。

例如，使用IPv4主機192.168.0.107建立網路對象6_mapped_to_4。

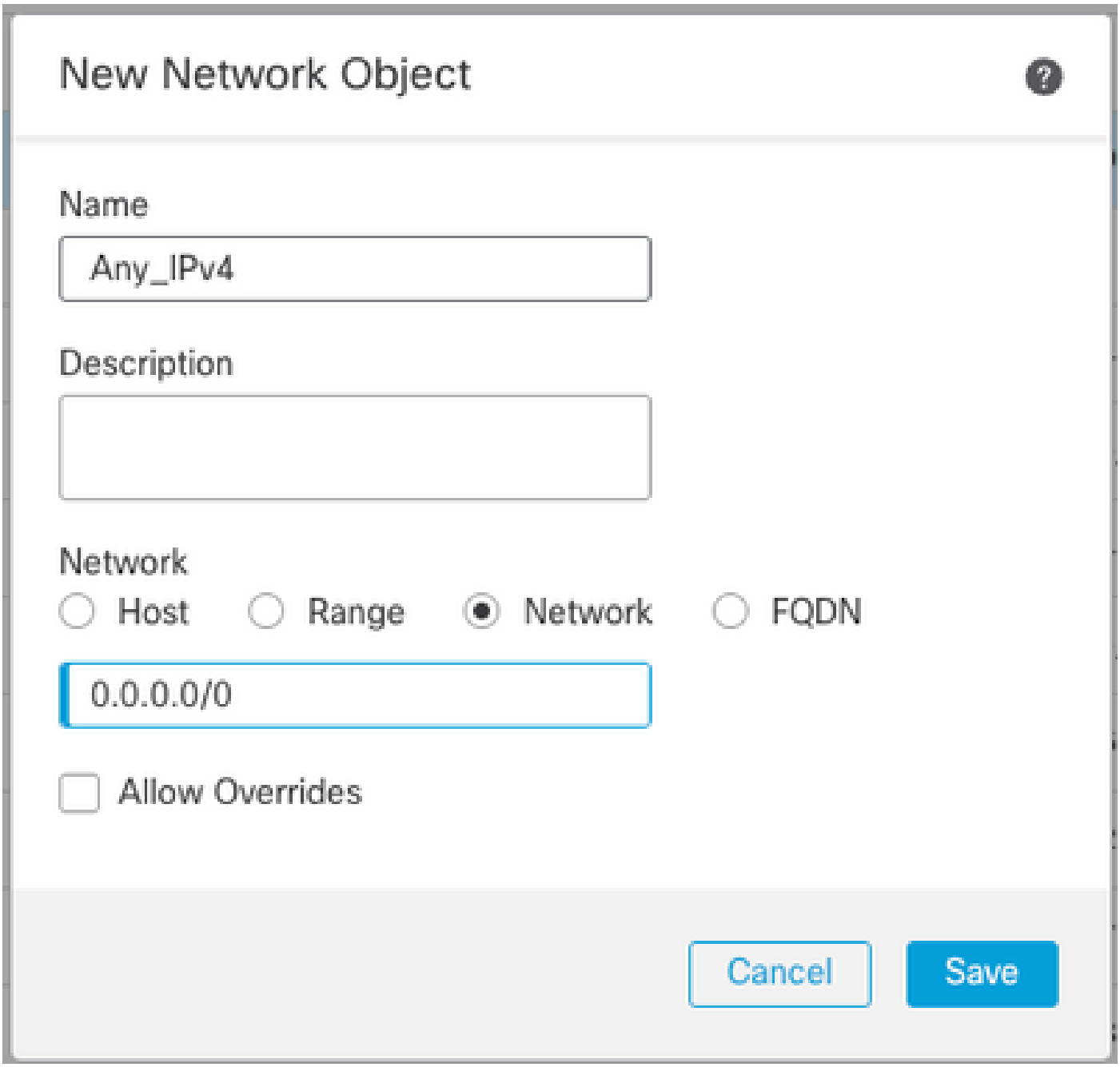
根據要在IPv4中對映的IPv6主機數量，可以使用單個對象網路、具有多個IPv4的網路組，或者僅使用NAT到輸出介面。



- IPv4網路對象，用於引用Internet上的外部IPv4主機。

在FMC GUI上，導航至Objects > Object Management > Select Network from Left Menu > Add Network > Add Object。

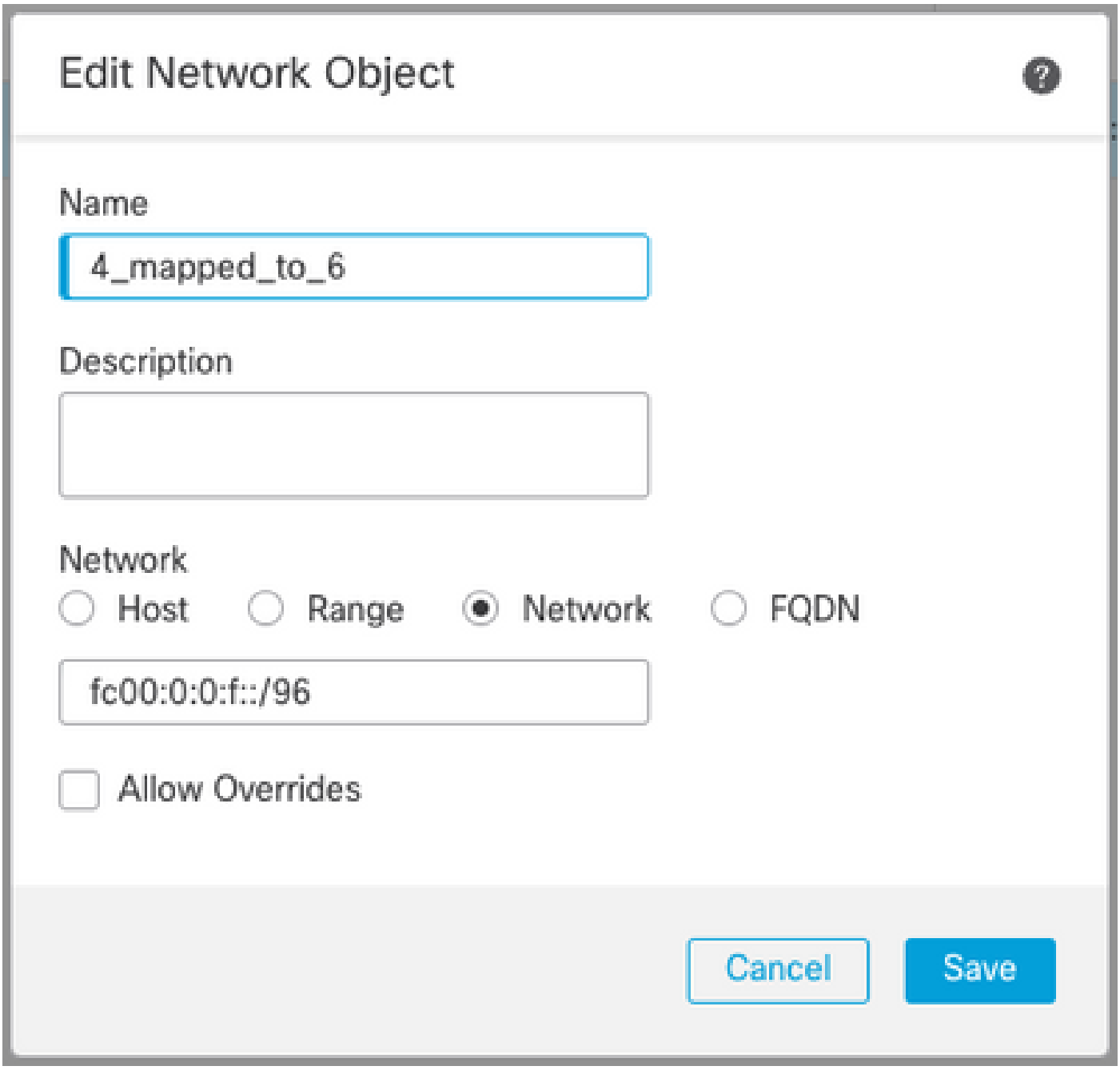
例如，使用IPv4子網0.0.0.0/0建立網路對象Any_IPv4。



- IPv6網路對象，用於將外部IPv4主機轉換為我們的IPv6域。

在FMC GUI上，導航至Objects > Object Management > Select Network from Left Menu > Add Network > Add Object。

例如，使用IPv6子網FC00:0:0:F::/96建立網路對象4_mapped_to_6。



在FTD上為IPv4/IPv6配置介面

導覽至Devices > Device Management > Edit FTD > Interfaces，然後設定內部和外部介面。

範例：

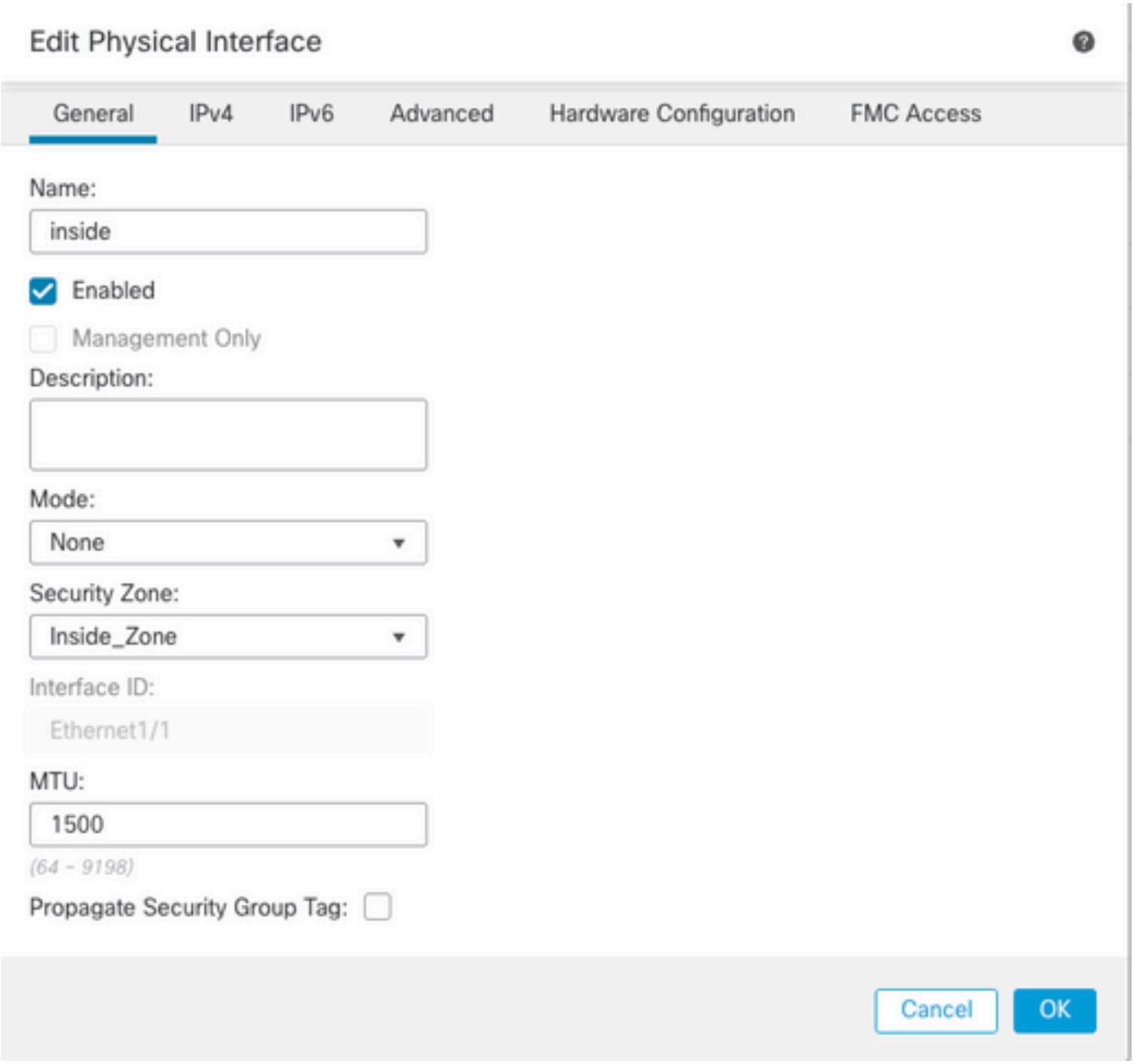
Interface Ethernet 1/1

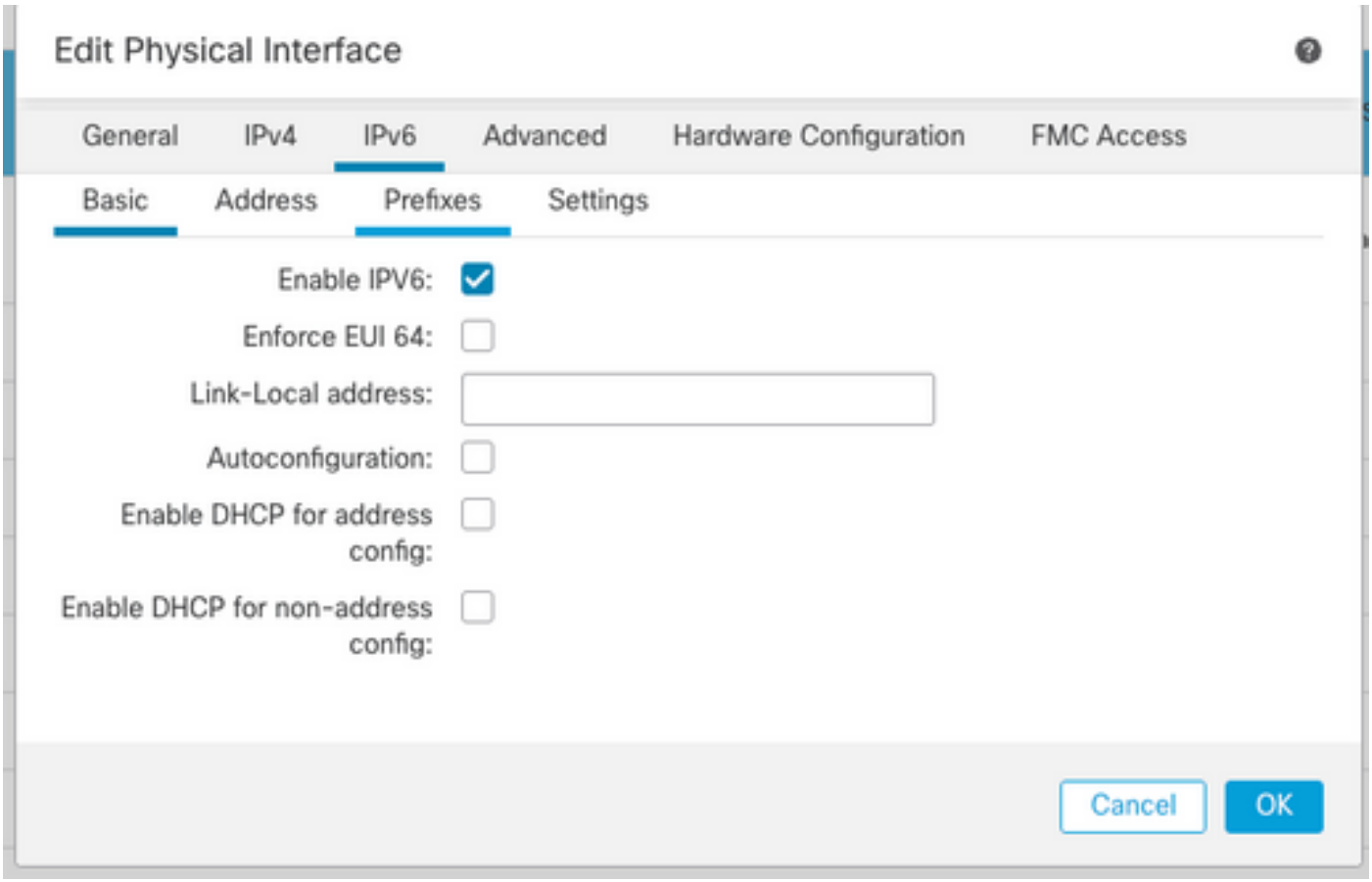
名稱：Inside

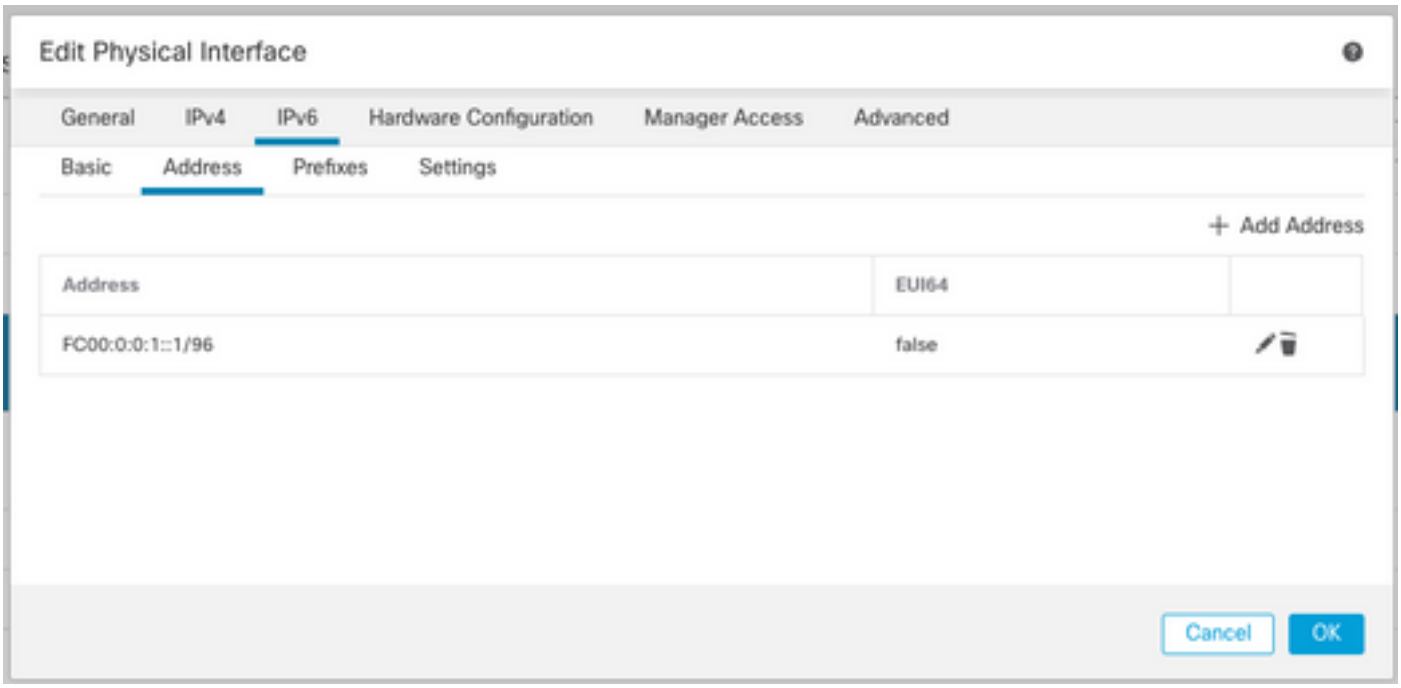
安全區域：Inside_Zone

如果未建立安全區域，您可以在「安全區域」(Security Zone)下拉選單>「新建」(New)中建立安全區域。

IPv6地址：FC00:0:0:1::1/96







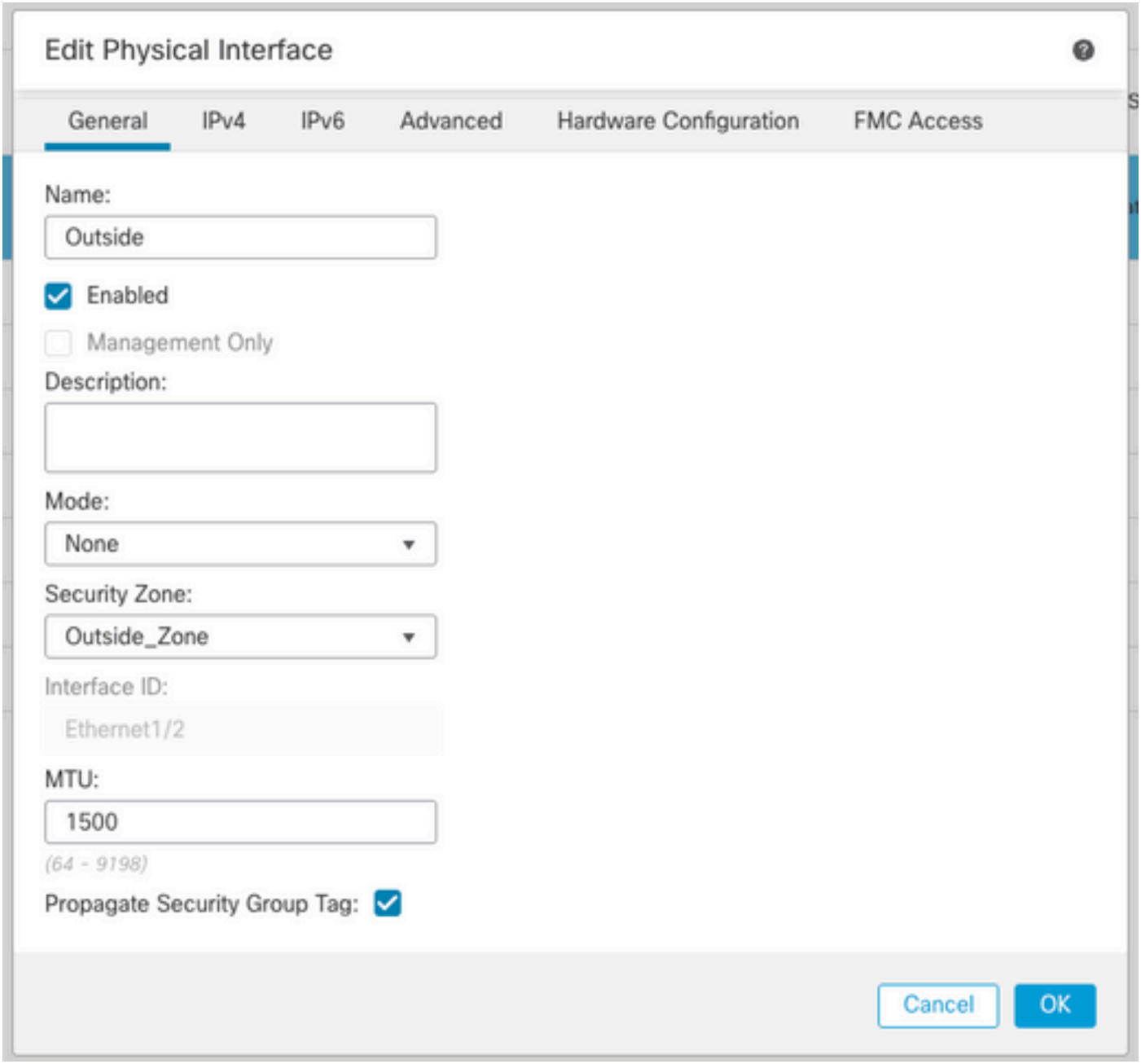
Interface Ethernet 1/2

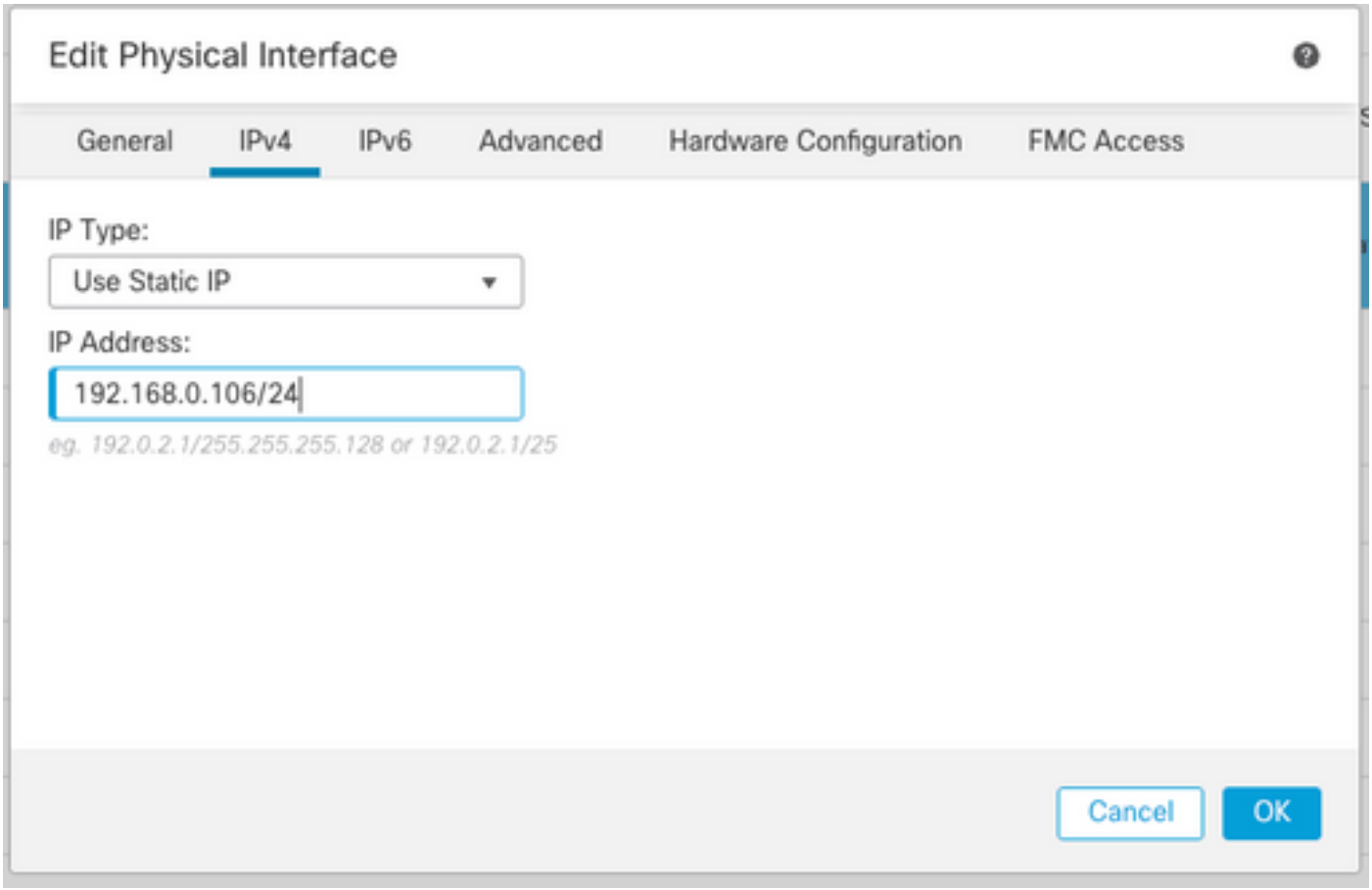
名稱：Outside

安全區域：Outside_Zone

如果未建立安全區域，您可以在Security Zone（安全區域）下拉菜單> New（新建）中建立安全區域。

IPv4地址：192.168.0.106/24





配置預設路由

導覽至Devices > Device Management > Edit FTD > Routing > Static Routing > Add Route。

例如，使用網關192.168.0.254的外部介面上的預設靜態路由。

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:

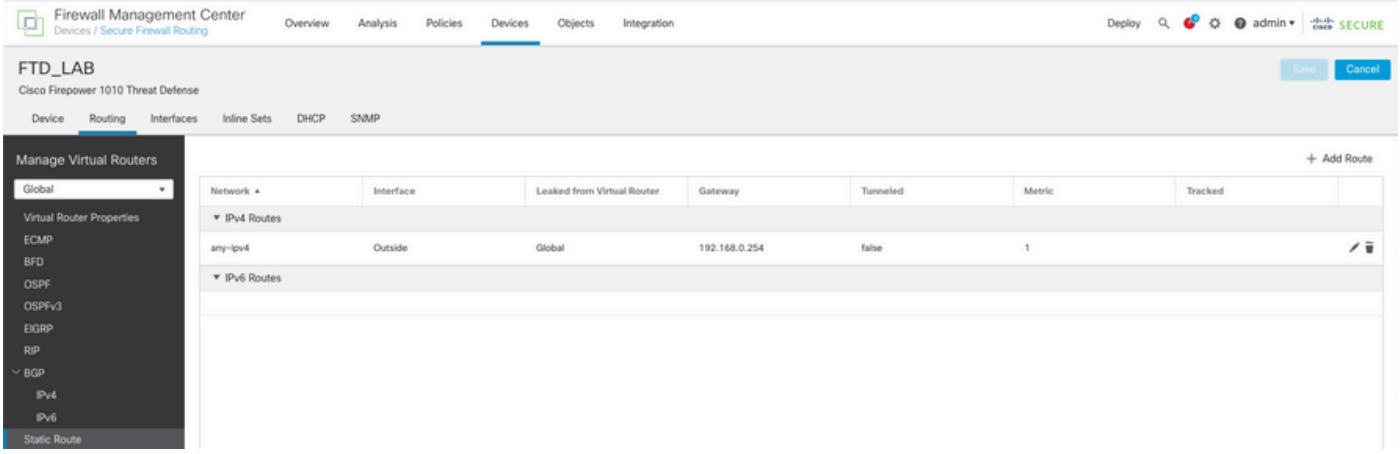
1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

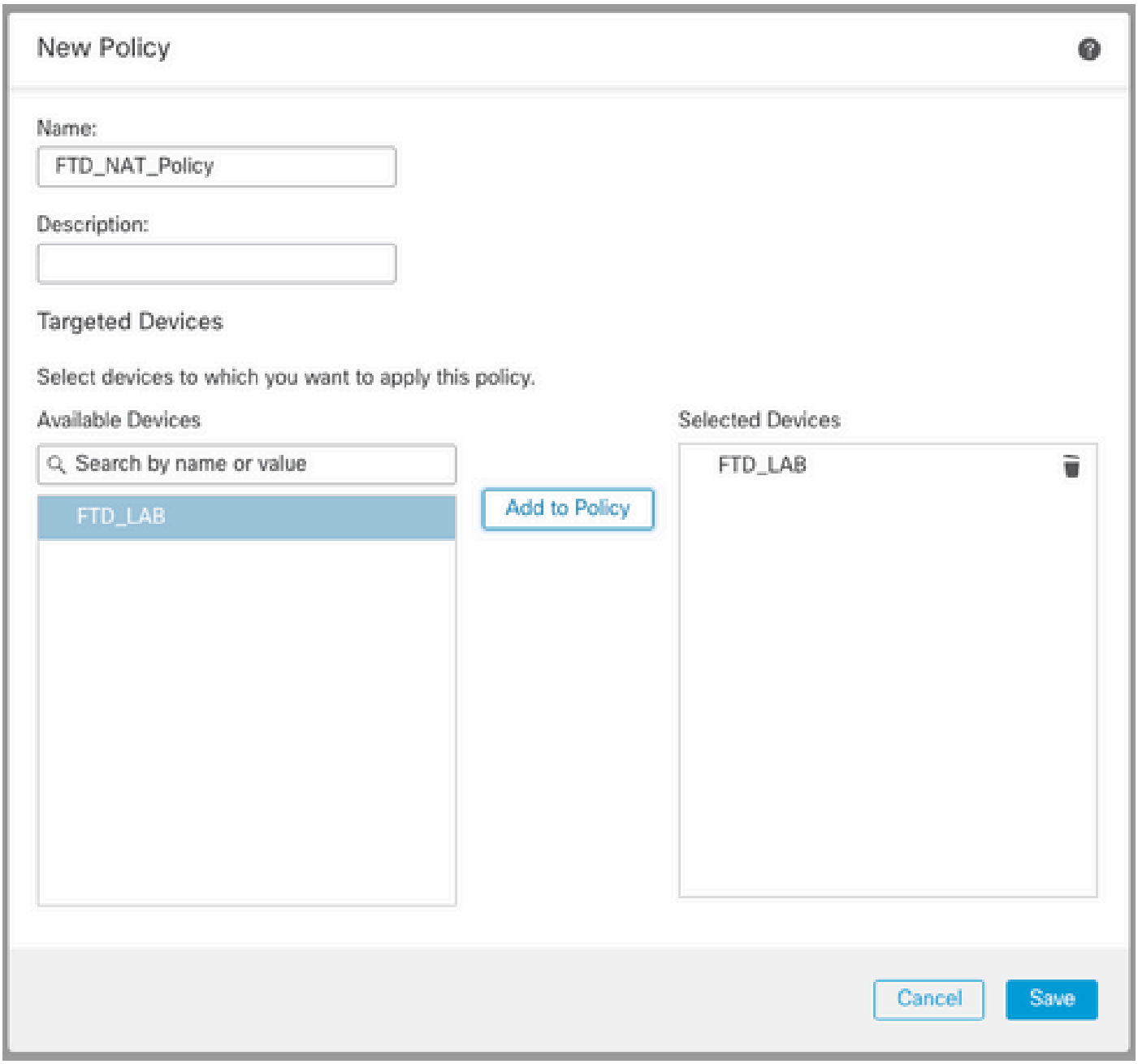
Cancel OK



配置NAT策略

在FMC GUI上，導航到Devices > NAT > New Policy > Threat Defense NAT，然後建立NAT策略。

例如，建立NAT策略FTD_NAT_Policy並將其分配給測試FTD FTD_LAB。



配置NAT規則

出站NAT。

在FMC GUI上，導航到Devices > NAT > Select the NAT policy > Add Rule，然後建立NAT規則以將內部IPv6網路轉換為外部IPv4池。

例如，網路對象Local_IPv6_subnet會動態轉換為網路對象6_mapped_to_4。

NAT規則：自動NAT規則

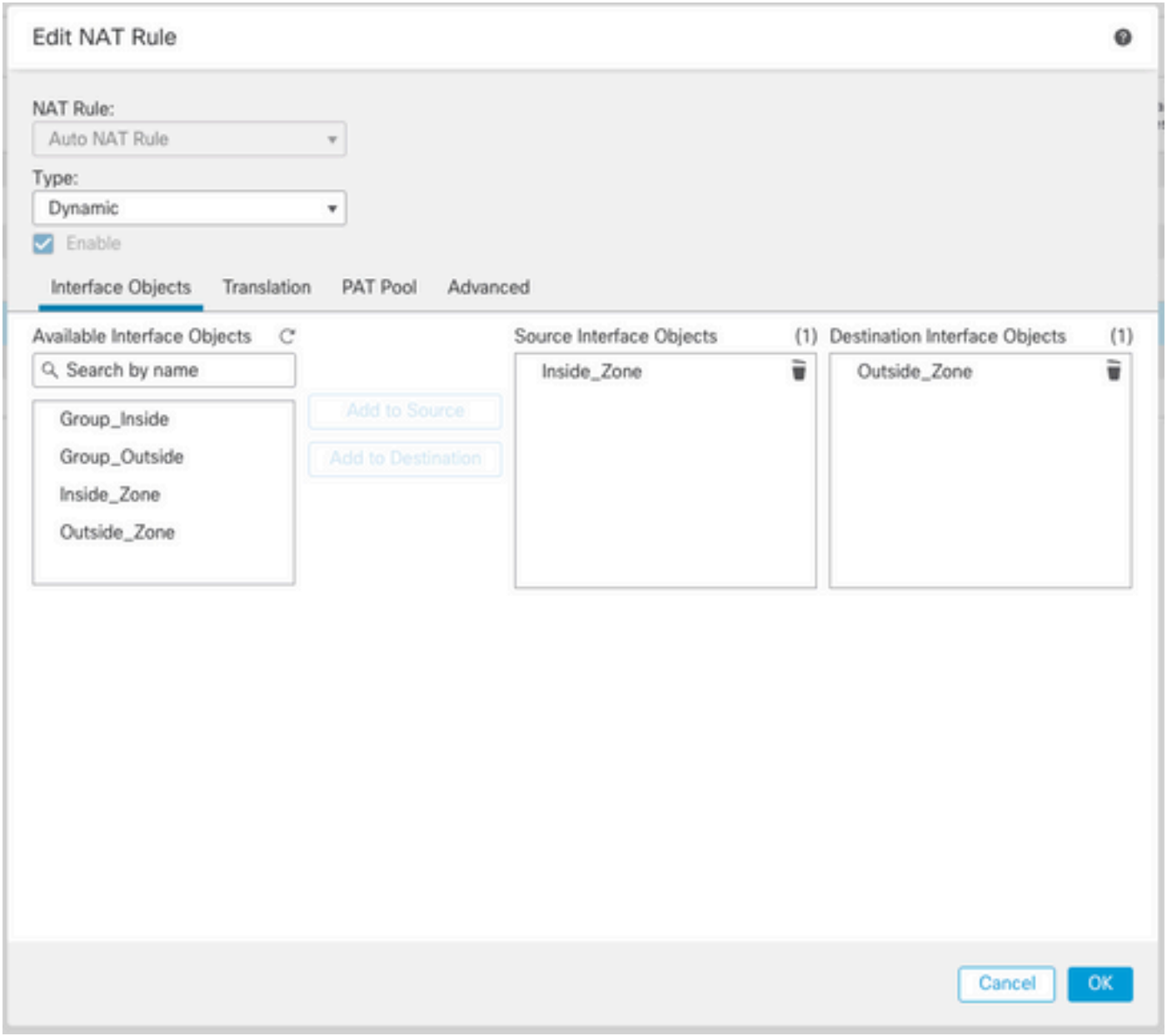
型別：動態

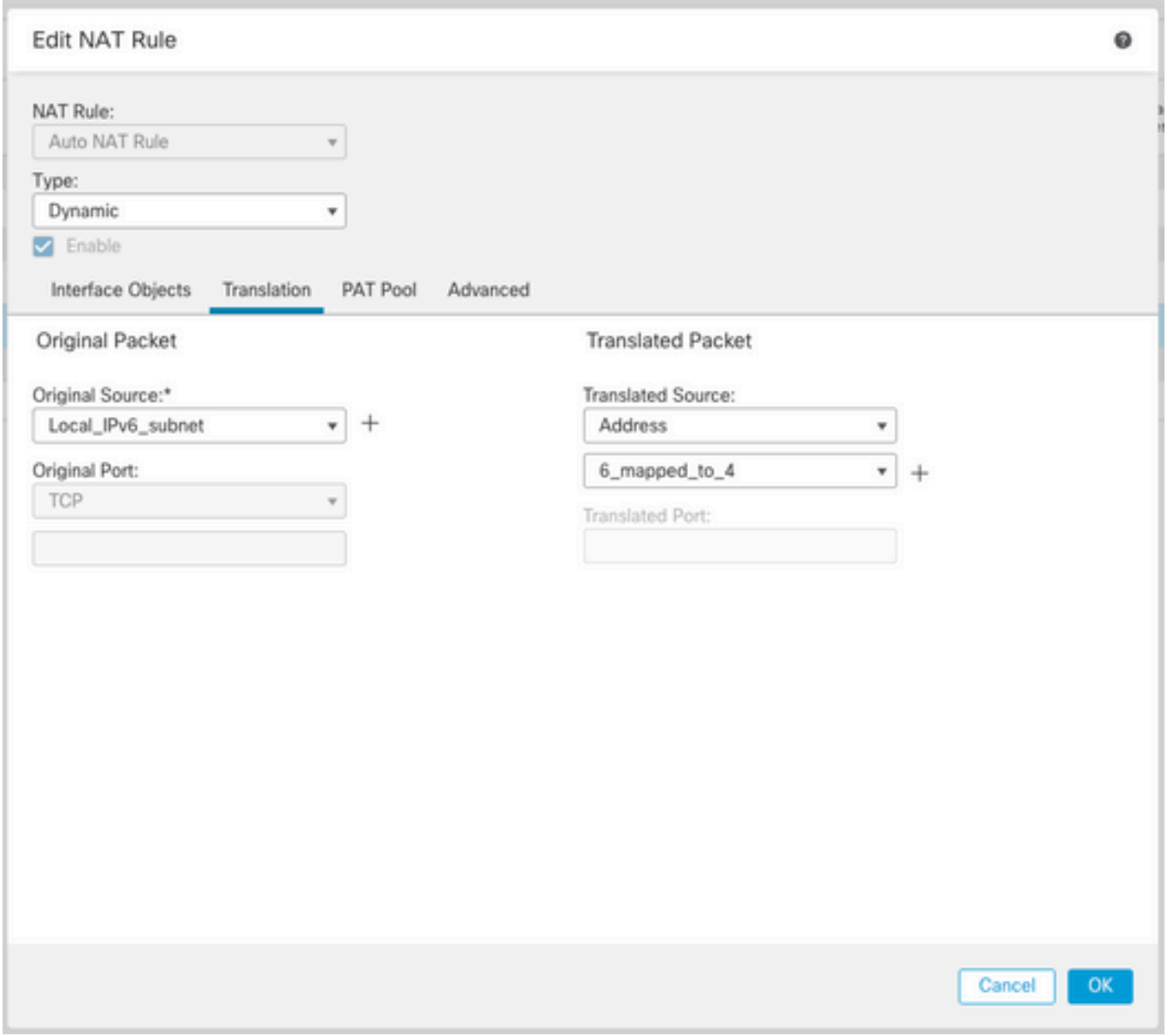
源介面對象：Inside_Zone

目標介面對象：Outside_Zone

原始源：Local_IPv6_subnet

轉換後的源：6_mapped_to_4





入站NAT。

在FMC GUI上，導航到Devices > NAT > Select the NAT policy > Add Rule and create NAT rule to translate external IPv4 traffic to Internal IPv6 network pool。這樣，您就可以與本地IPv6子網進行內部通訊。

此外，請在此規則上啟用DNS重寫，以便來自外部DNS伺服器的回覆可以從A(IPv4)記錄轉換為AAAA(IPv6)記錄。

例如，Outside Network Any_IPv4被靜態轉換為IPv6子網2100:6400::/96（在對象4_mapped_to_6中定義）。

NAT規則：自動NAT規則

型別：靜態

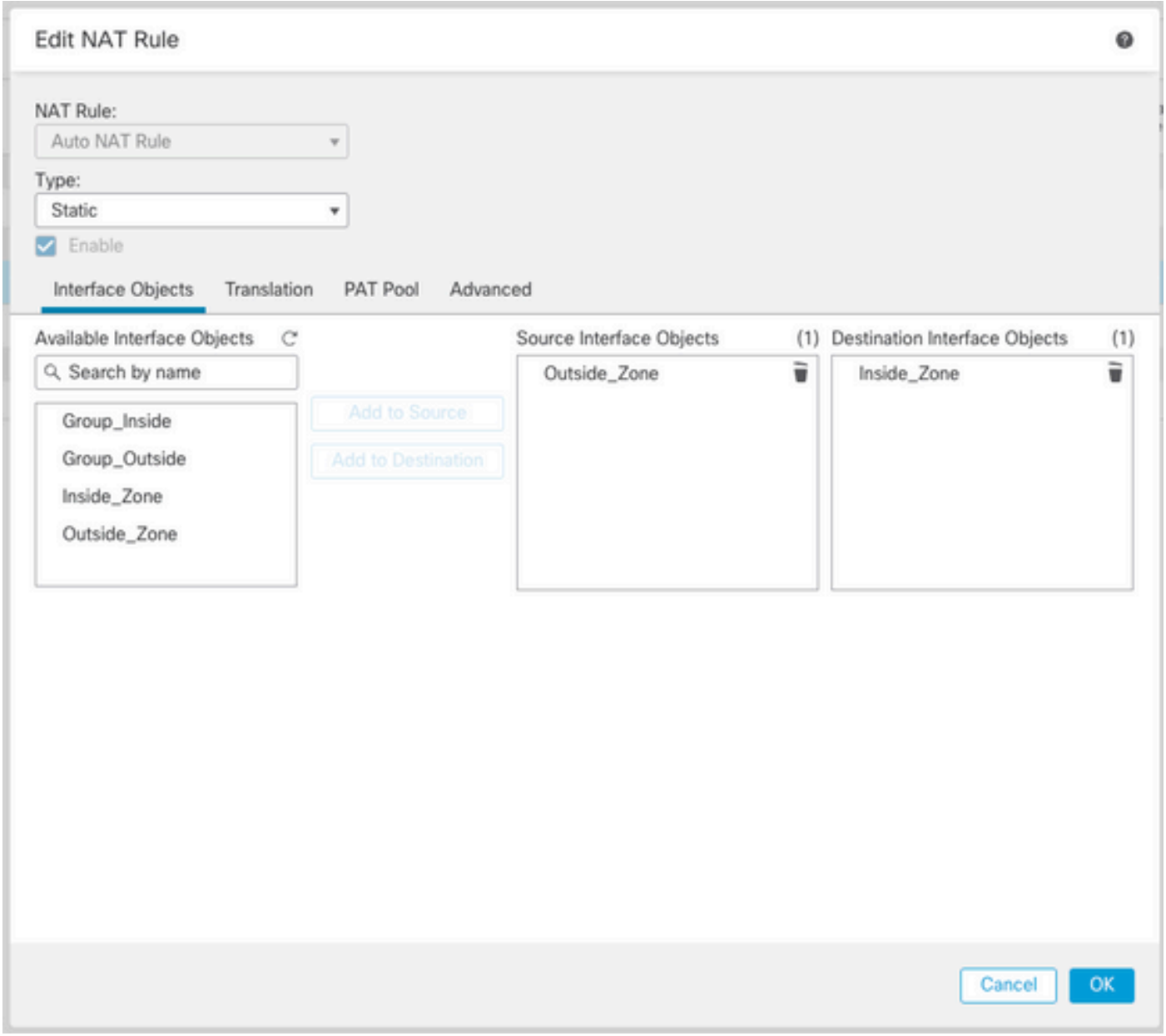
源介面對象：Outside_Zone

目標介面對象：Inside_Zone

原始來源：Any_IPv4

轉換後的源：4_mapped_to_6

轉換與此規則匹配的DNS應答：是（啟用覈取方塊）



Edit NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Static

Enable

Interface Objects | Translation | PAT Pool | Advanced

Original Packet

Original Source:*
any_IPv4

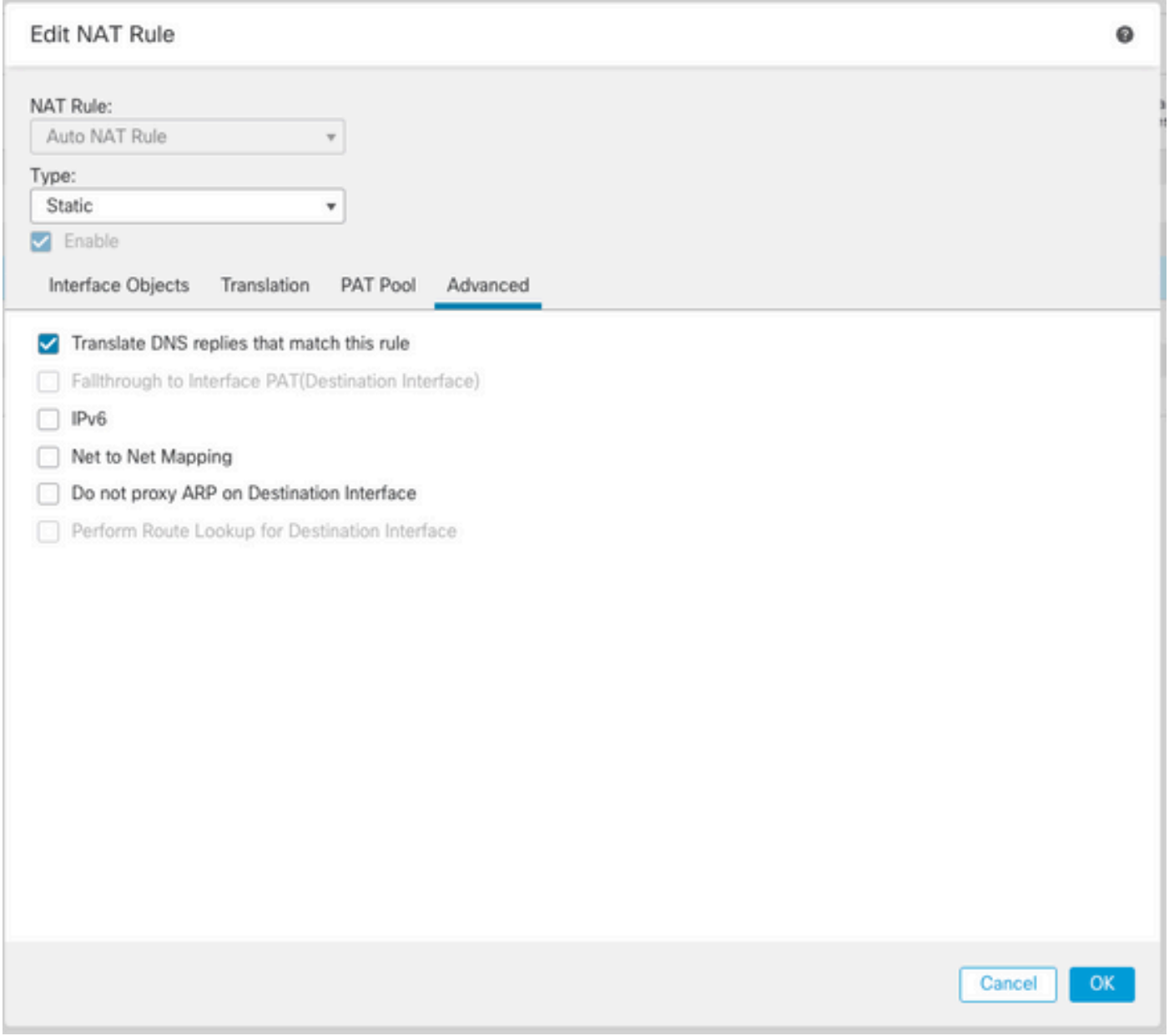
Original Port:
TCP

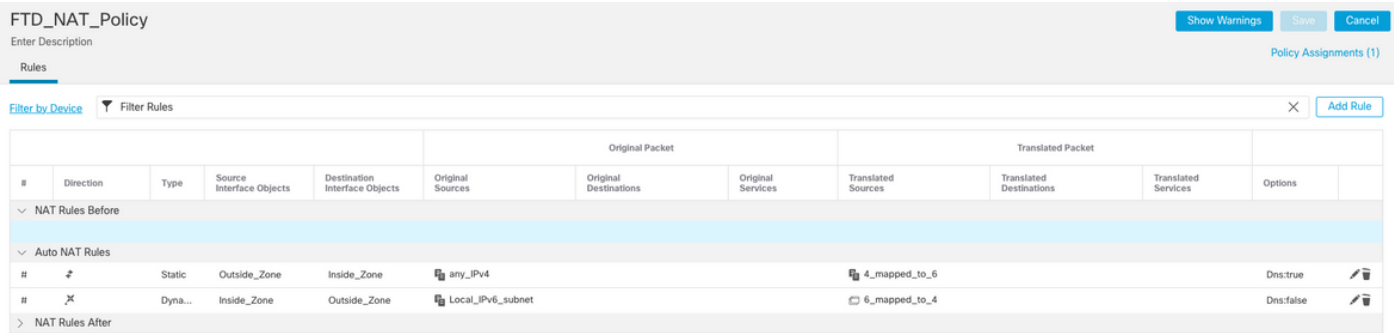
Translated Packet

Translated Source:
Address
4_mapped_to_6

Translated Port:

Cancel | OK





繼續將變更部署到FTD。

驗證

- 顯示介面名稱和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
```

- 確認從FTD內部介面到客戶端的IPv6連線。

IPv6內部主機IP fc00:0:1::100。

FTD內部介面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
```

- 在FTD CLI上顯示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
```

- 擷取流量。

例如，捕獲從內部IPv6主機fc00:0:0:1::100到DNS伺服器的流量為fc00::f:0:0:ac10:a64 UDP 53。

這裡，目標DNS伺服器是fc00::f:0:0:ac10:a64。最後32位是ac10:0a64。這些位是二進位制八位數，相當於172、16、10、100。Firewall 6-to-4將IPv6 DNS伺服器fc00::f:0:0:ac10:a64轉換為等效的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
```