Configuración de NAT 64 en firewall seguro gestionado por FMC

Contenido

Introducción

Este documento describe cómo configurar NAT64 en Firepower Threat Defence (FTD) gestionado por Fire Power Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre Secure Firewall Threat Defence y Secure Firewall Management Center.

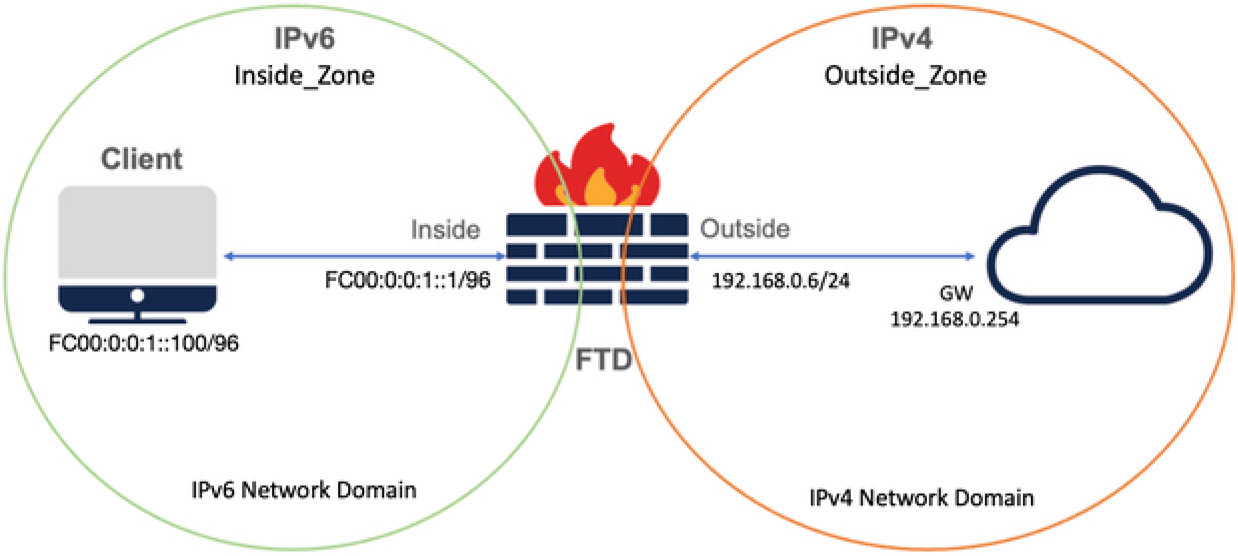
Componentes Utilizados

- Firepower Management Center 7.0.4.
- Firepower Threat Defense 7.0.4.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

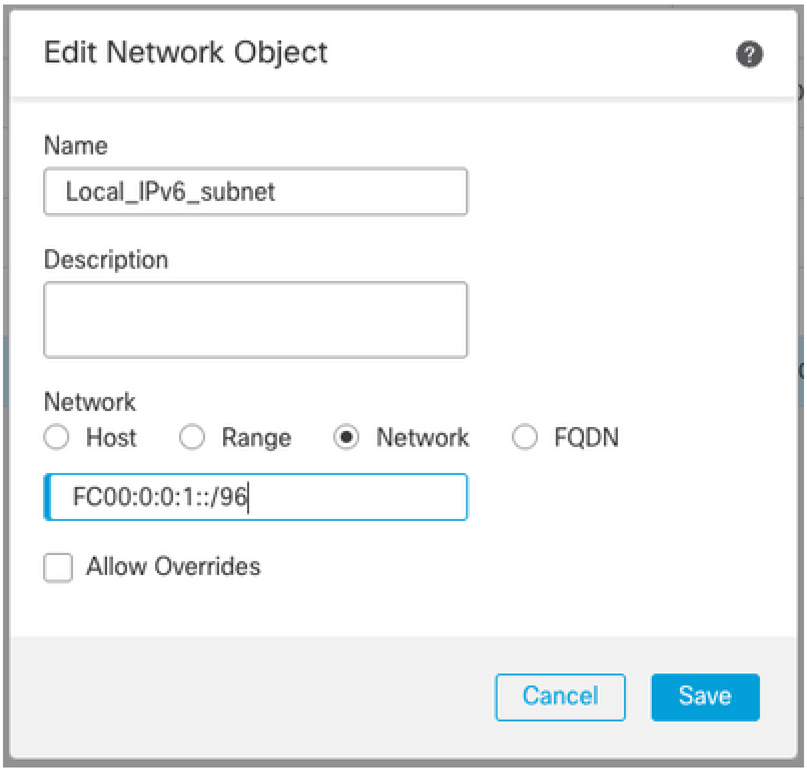


Configurar objetos de red

- Objeto de red IPv6 para hacer referencia a la subred de cliente IPv6 interna.

En la GUI de FMC, navegue hasta **Objetos** > **Administración de objetos** > **Seleccionar red desde el menú de la izquierda** > **Agregar red** > **Agregar objeto**.

Por ejemplo, el objeto de red Local_IPv6_subnet se crea con la subred IPv6 FC00:0:0:1::/96.


Edit Network Object

Name
Local_IPv6_subnet

Description

Network
○ Host ○ Range ● Network ○ FQDN
FC00:0:0:1::/96

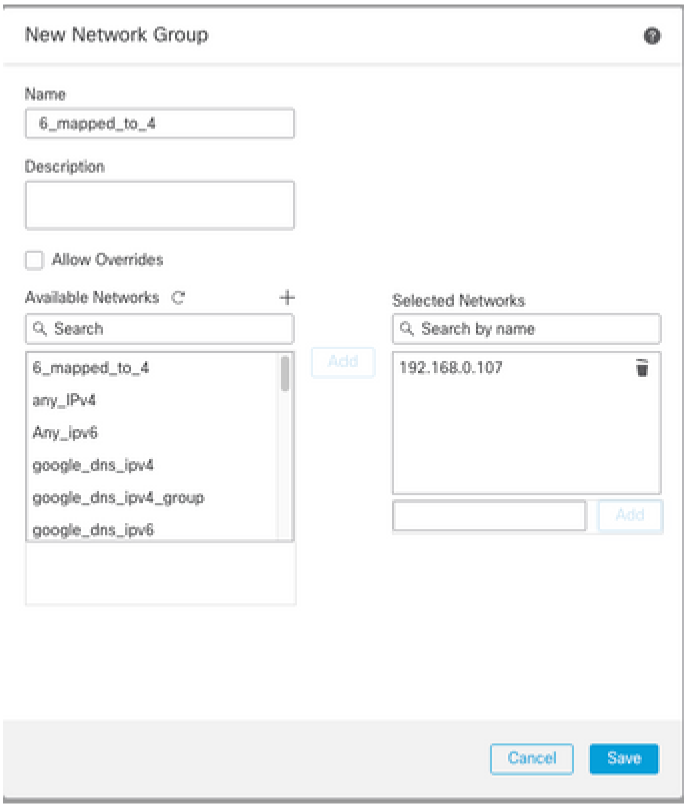
□ Allow Overrides

- Objeto de red IPv4 para traducir clientes IPv6 a IPv4.

En la GUI de FMC, navegue hasta **Objetos** > **Gestión de objetos** > **Seleccionar red desde el menú de la izquierda** > **Agregar red** > **Agregar grupo**.

Por ejemplo, el objeto de red 6_mapeado_a_4 se crea con el host IPv4 192.168.0.107.

En función de la cantidad de hosts IPv6 que se asignarán en IPv4, puede utilizar una red de un solo objeto, un grupo de red con varios IPv4 o solo NAT para la interfaz de salida.



New Network Group

Name: 6_mapped_to_4

Description:

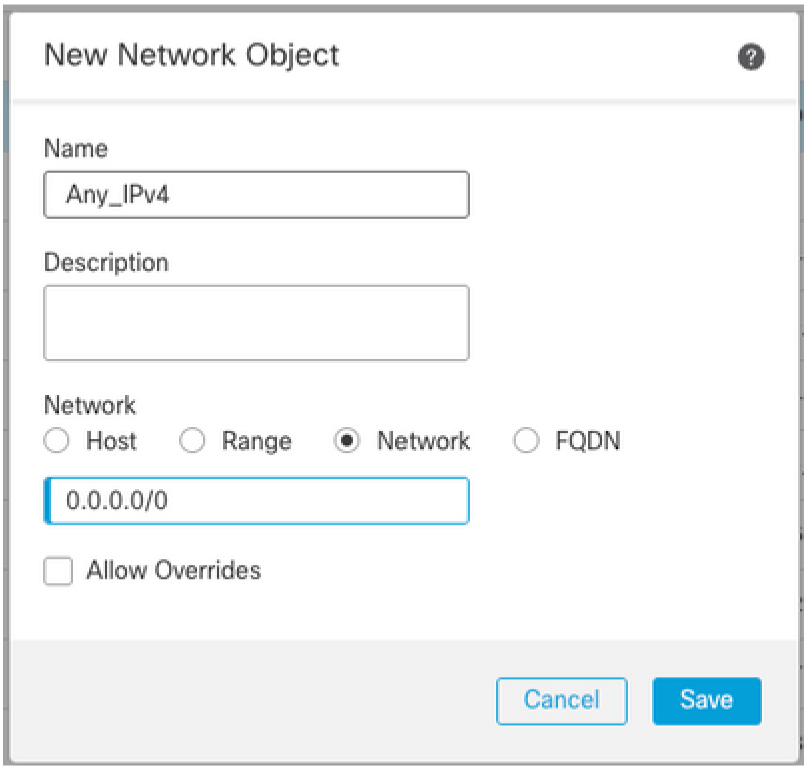
□ Allow Overrides

192.168.0.107

- Objeto de red IPv4 para hacer referencia a los hosts IPv4 externos en Internet.

En la GUI de FMC, navegue hasta **Objetos** > **Administración de objetos** > **Seleccionar red desde el menú de la izquierda** > **Agregar red** > **Agregar objeto**.

Por ejemplo, el objeto de red Any_IPv4 se crea con la subred IPv4 0.0.0.0/0.


New Network Object

Name
Any_IPv4

Description

Network
○ Host ○ Range ● Network ○ FQDN

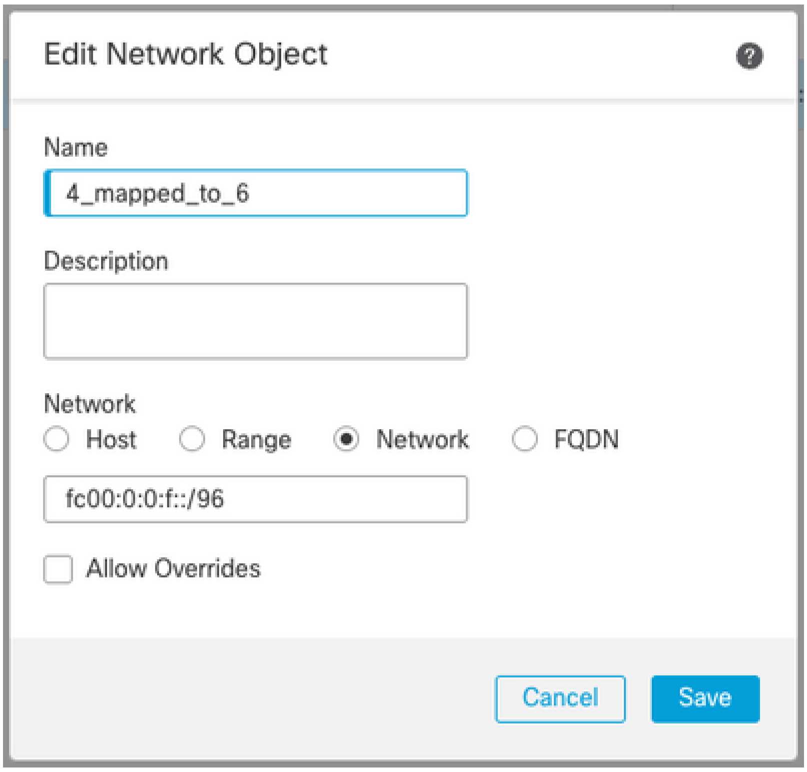
0.0.0.0/0

□ Allow Overrides

- Objeto de red IPv6 para traducir un host IPv4 externo a nuestro dominio IPv6.

En la GUI de FMC, navegue hasta **Objetos > Gestión de objetos > Seleccionar red desde el menú de la izquierda > Agregar red > Agregar objeto**.

Por ejemplo, el objeto de red 4_mapeado_a_6 se crea con la subred IPv6 FC00:0:0:F::/96.


Edit Network Object

Name
4_mapped_to_6

Description

Network
○ Host ○ Range ● Network ○ FQDN

fc00:0:0:f::/96

□ Allow Overrides

Configuración de interfaces en FTD para IPv4/IPv6

Vaya a **Devices > Device Management > Edit FTD > Interfaces** y configure las interfaces interna y externa.

Ejemplo:

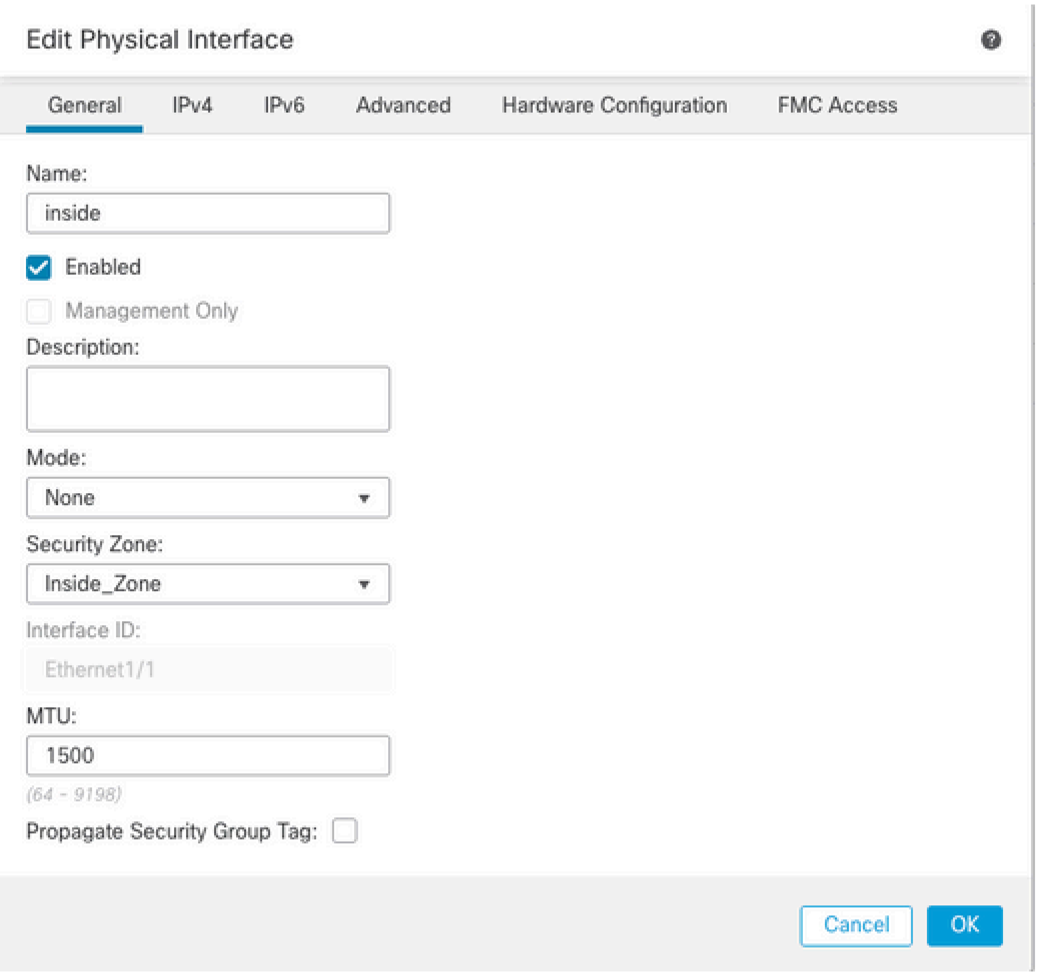
interfaz Ethernet 1/1

Nombre: Interior

Zona de seguridad: Inside_Zone

Si no se crea la zona de seguridad, puede crearla en el **menú desplegable Zona de seguridad > Nuevo**.

Dirección IPv6: FC00:0:0:1::1/96



Edit Physical Interface

Name: inside

☑ Enabled

□ Management Only

Description:

Mode: None

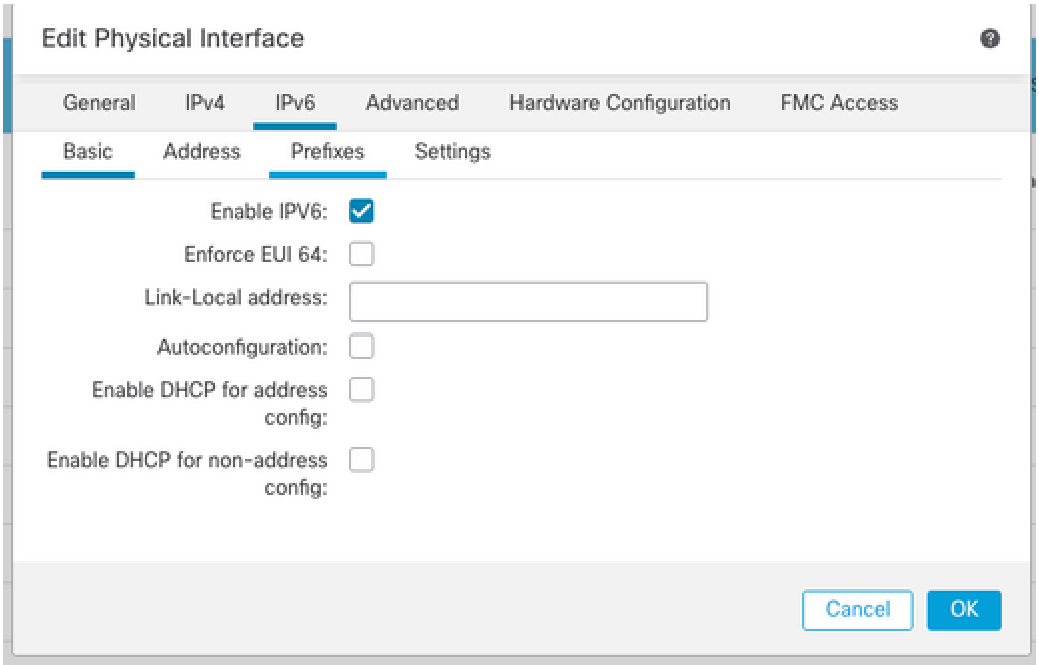
Security Zone: Inside_Zone

Interface ID: Ethernet1/1

MTU: 1500

(64 - 9198)

Propagate Security Group Tag: □



Enable IPV6: ☑

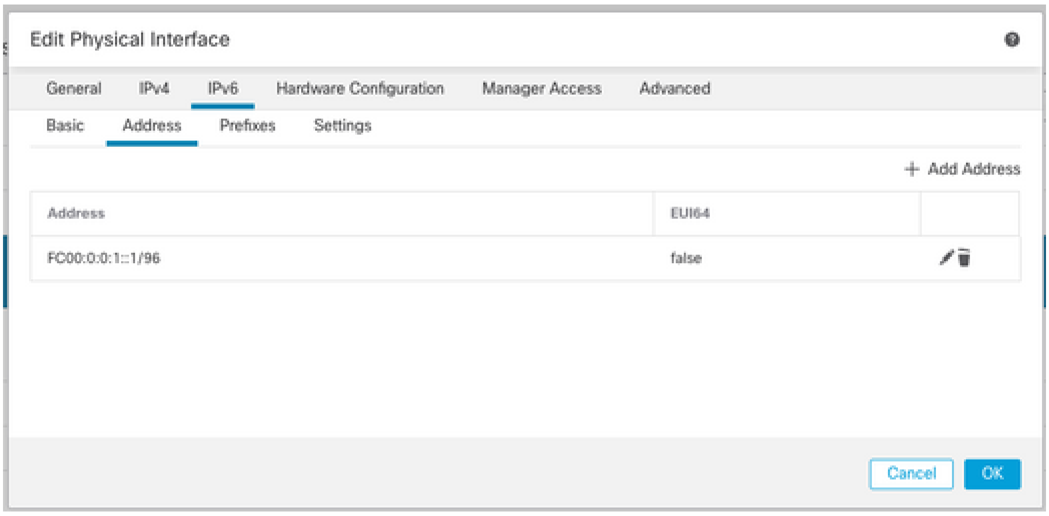
Enforce EUI 64: □

Link-Local address:

Autoconfiguration: □

Enable DHCP for address config: □

Enable DHCP for non-address config: □



Address	EUI64	
FC00:0:0:1::1/96	false	

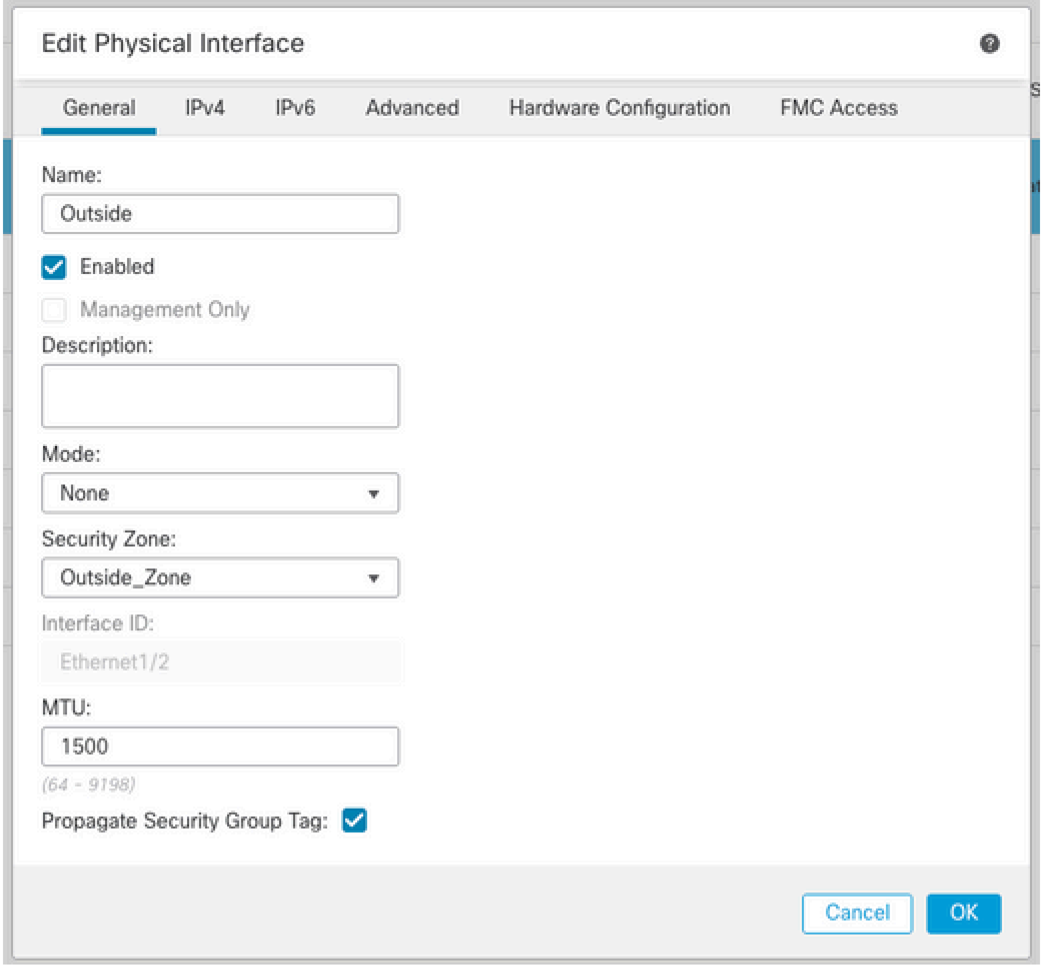
interfaz Ethernet 1/2

Nombre: Fuera

Zona de seguridad: Outside_Zone

Si no se crea la zona de seguridad, puede crearla en el **menú desplegable Zona de seguridad** > **Nuevo**.

Dirección IPv4: 192.168.0.106/24



Edit Physical Interface

Name: Outside

☑ Enabled

□ Management Only

Description:

Mode: None

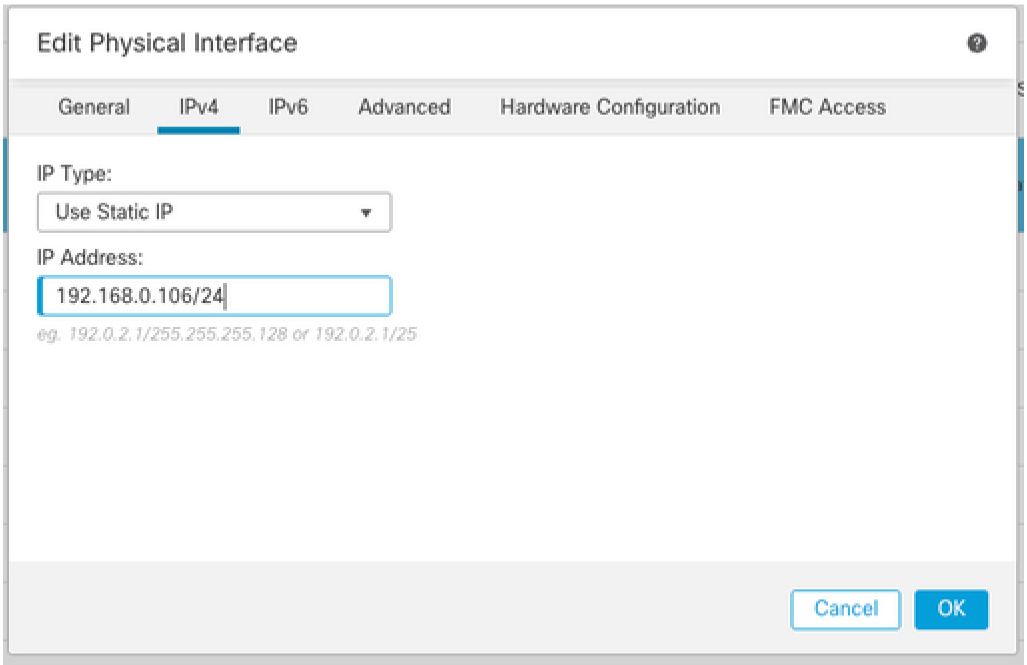
Security Zone: Outside_Zone

Interface ID: Ethernet1/2

MTU: 1500

(64 - 9198)

Propagate Security Group Tag: ☑



Edit Physical Interface

IP Type: Use Static IP

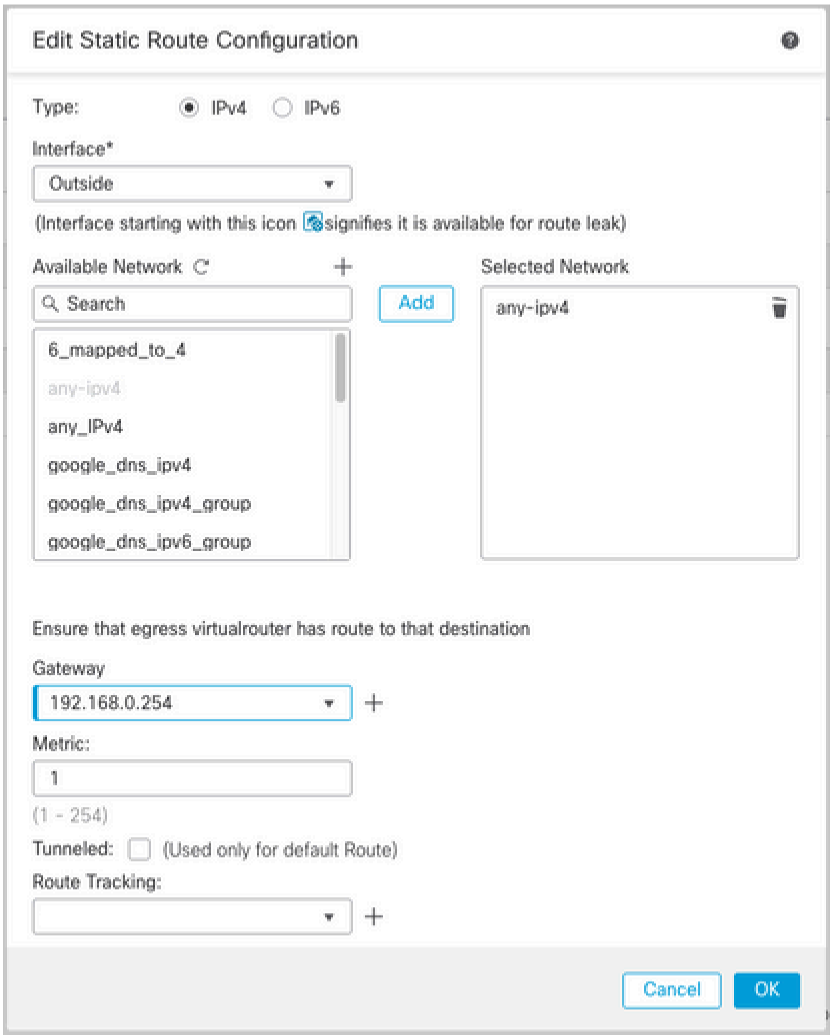
IP Address: 192.168.0.106/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Configurar ruta predeterminada

Vaya a **Dispositivos > Administración de dispositivos > Editar FTD > Enrutamiento > Enrutamiento estático > Agregar ruta**.

Por ejemplo, la ruta estática predeterminada en la interfaz externa con el gateway 192.168.0.254.



Edit Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: Outside

(Interface starting with this icon signifies it is available for route leak)

Available Network: 6_mapped_to_4, any-ipv4, any_IPv4, google_dns_ipv4, google_dns_ipv4_group, google_dns_ipv6_group

Selected Network: any-ipv4

Ensure that egress virtualrouter has route to that destination

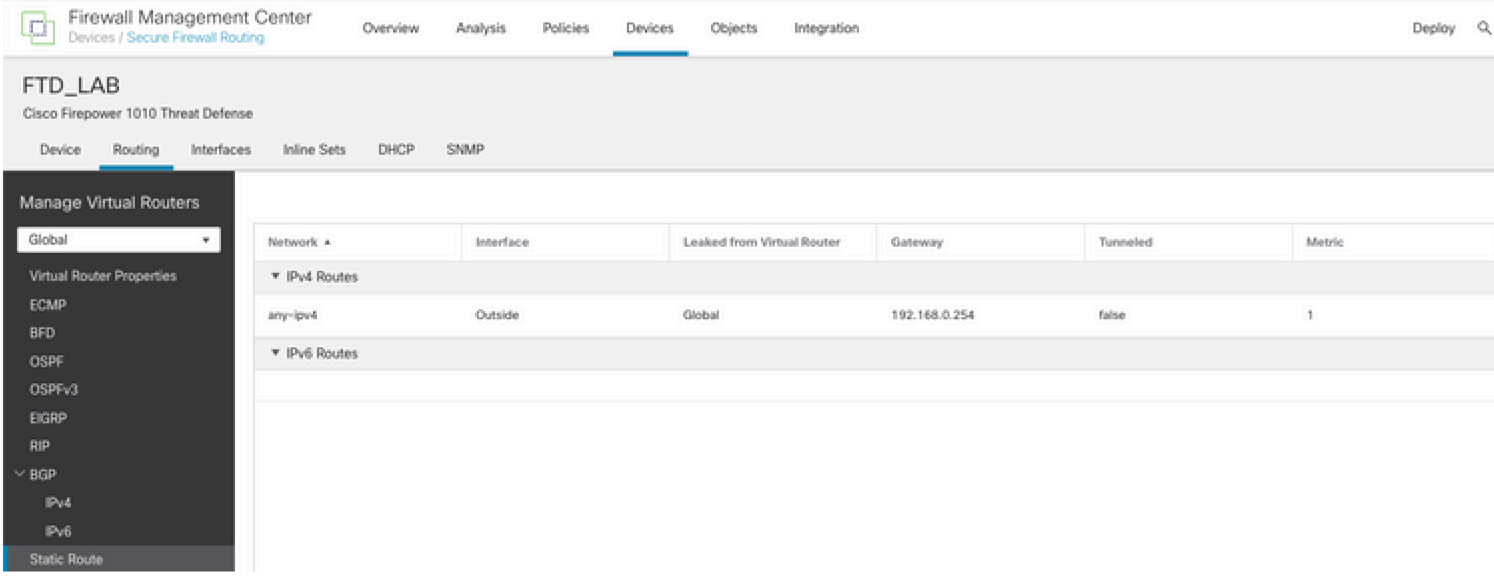
Gateway: 192.168.0.254

Metric: 1

(1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:



Firewall Management Center

Devices / Secure Firewall Routing

FTD_LAB

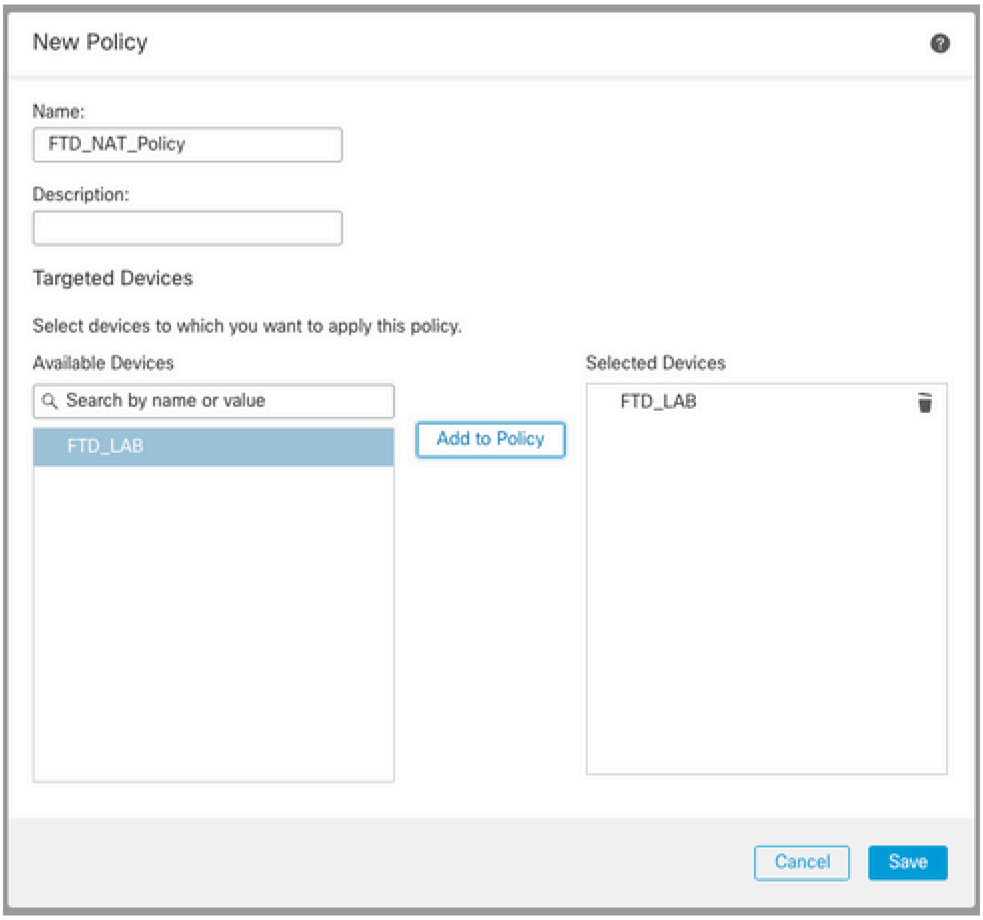
Cisco Firepower 1010 Threat Defense

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▼ IPv4 Routes					
any-ipv4	Outside	Global	192.168.0.254	false	1
▼ IPv6 Routes					

Configuración de la política NAT

En la GUI de FMC, navegue hasta **Devices > NAT > New Policy > Threat Defence NAT** y cree una política NAT.

Por ejemplo, la política NAT FTD_NAT_Policy se crea y se asigna al FTD FTD_LAB de prueba.



New Policy

Name: FTD_NAT_Policy

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices: FTD_LAB

Selected Devices: FTD_LAB

Configurar reglas NAT

NAT de salida.

En la GUI de FMC, navegue hasta **Dispositivos** > **NAT** > **Seleccione la política NAT** > **Agregar regla** y cree la regla NAT para traducir la red IPv6 interna al conjunto IPv4 externo.

Por ejemplo, Objeto de red Local_IPv6_subnet se traduce dinámicamente al Objeto de red 6_mapeado_a_4.

Regla NAT: regla NAT automática

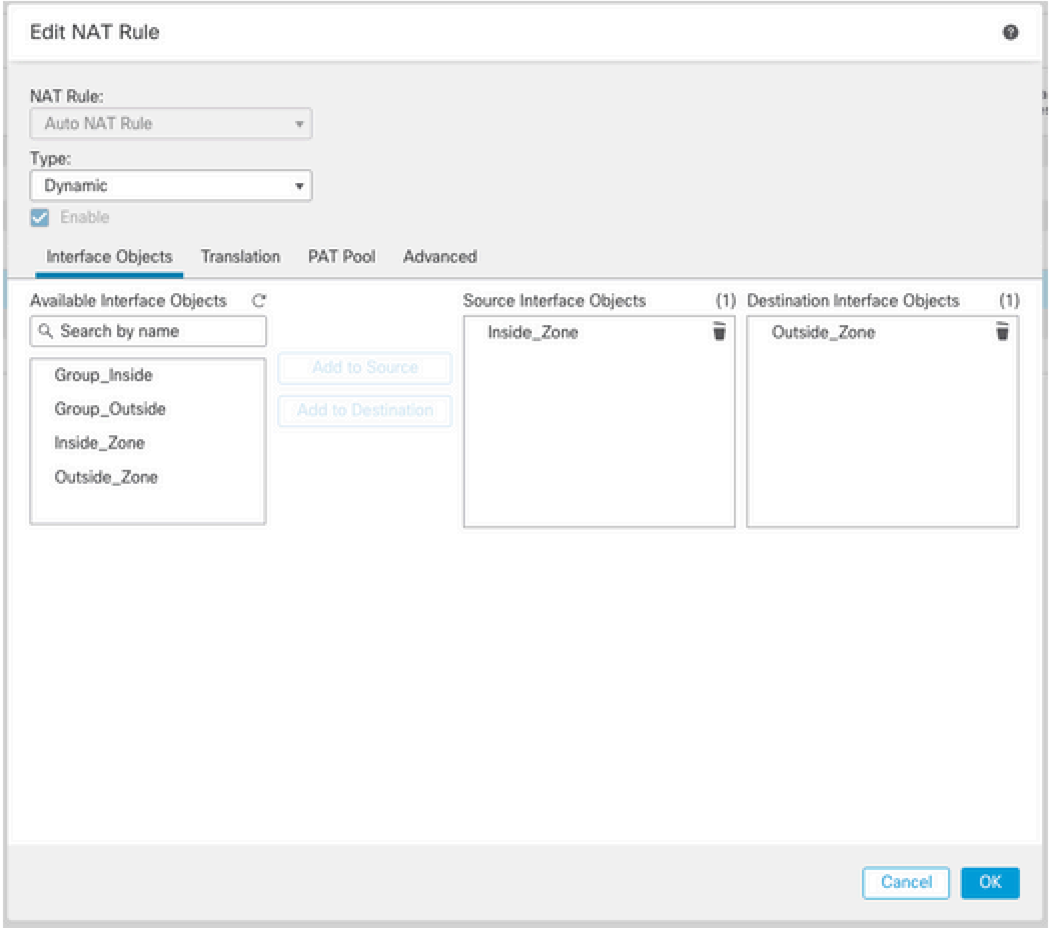
Tipo: Dinámico

Objetos de la interfaz de origen: Inside_Zone

Objetos de interfaz de destino: Outside_Zone

Origen original: Local_IPv6_subnet

Origen traducido: 6_mapeado_a_4



Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

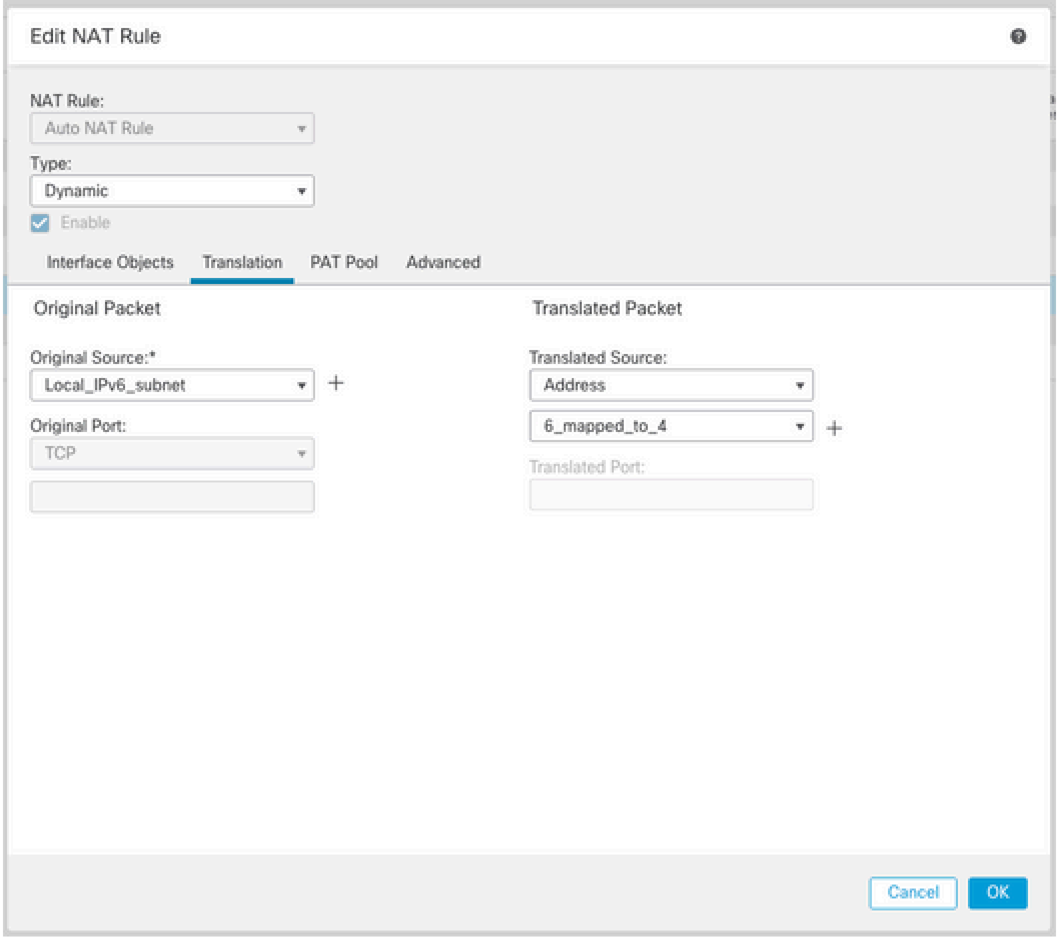
☑ Enable

Available Interface Objects

Group_Inside
Group_Outside
Inside_Zone
Outside_Zone

Source Interface Objects (1): Inside_Zone

Destination Interface Objects (1): Outside_Zone



Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Original Packet

Original Source:* Local_IPv6_subnet

Original Port: TCP

Translated Packet

Translated Source: Address

6_mapped_to_4

Translated Port:

NAT entrante.

En la GUI de FMC, navegue hasta **Devices** > **NAT** > **Select the NAT policy** > **Add Rule** y cree la regla NAT para traducir el tráfico IPv4 externo al conjunto de redes IPv6 interno. Esto permite la comunicación interna con la subred IPv6 local.

Además, habilite la reescritura de DNS en esta regla para que las respuestas del servidor DNS externo se puedan convertir de registros A (IPv4) a registros AAAA (IPv6).

Por ejemplo, Red externa Any_IPv4 se traduce estáticamente a la subred IPv6 2100:6400::/96 definida en el objeto 4_mapeado_a_6.

Regla NAT: regla NAT automática

Tipo: Estático

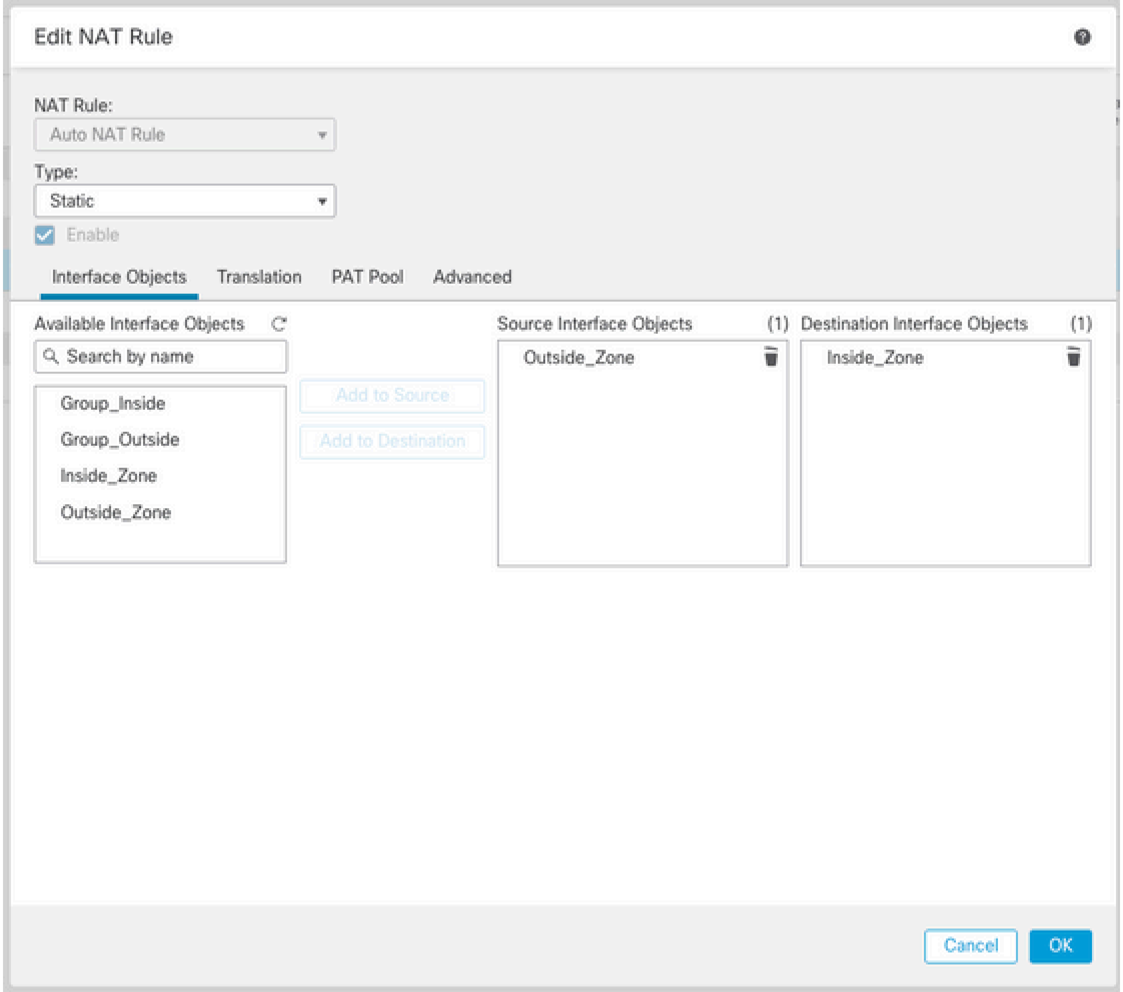
Objetos de la interfaz de origen: Outside_Zone

Objetos de interfaz de destino: Inside_Zone

Origen original: Any_IPv4

Origen traducido: 4_mapeado_a_6

Traducir respuestas DNS que coincidan con esta regla: Sí (casilla de verificación Habilitar)



Edit NAT Rule

NAT Rule: Auto NAT Rule

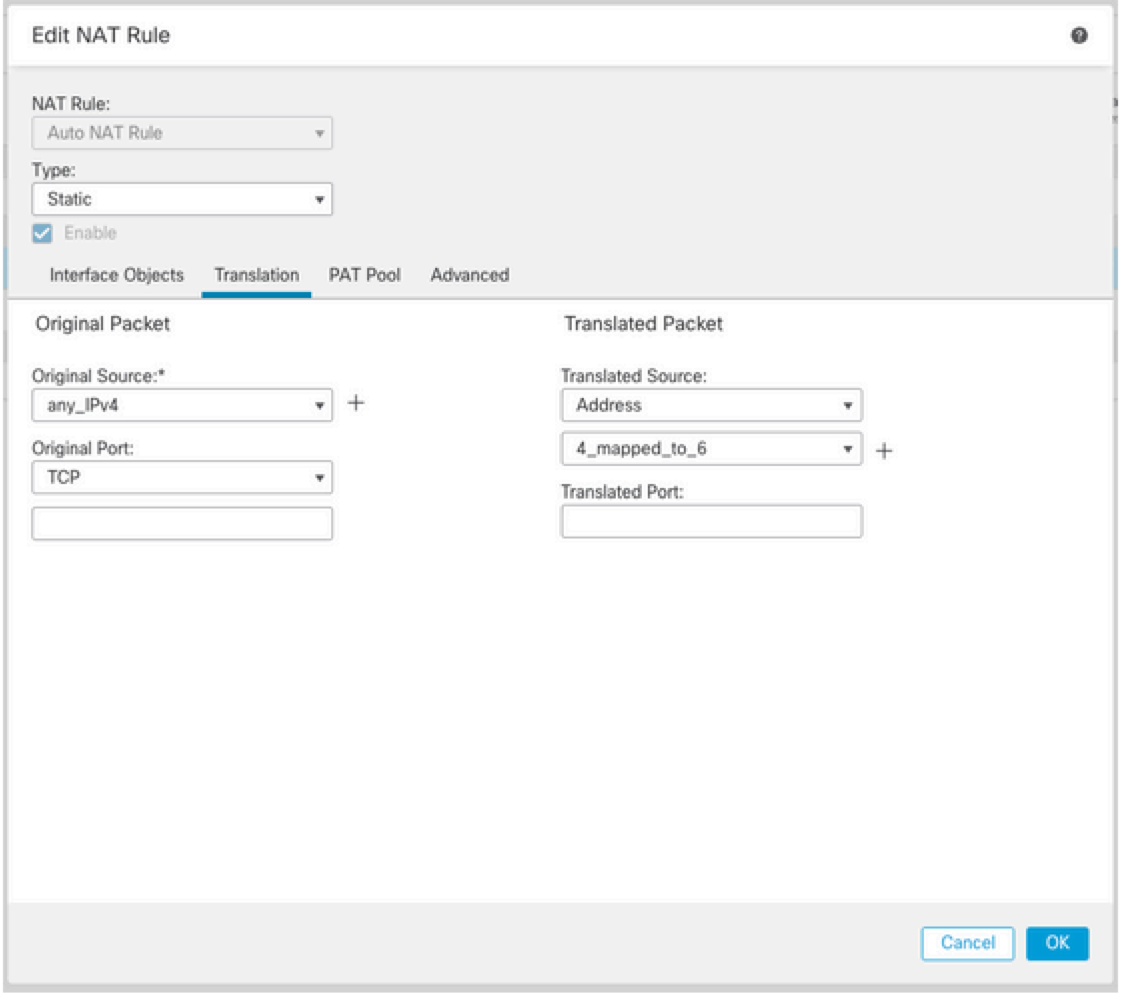
Type: Static

☑ Enable

Available Interface Objects: Group_Inside, Group_Outside, Inside_Zone, Outside_Zone

Source Interface Objects (1): Outside_Zone

Destination Interface Objects (1): Inside_Zone



Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

Original Packet

Original Source:* any_IPv4

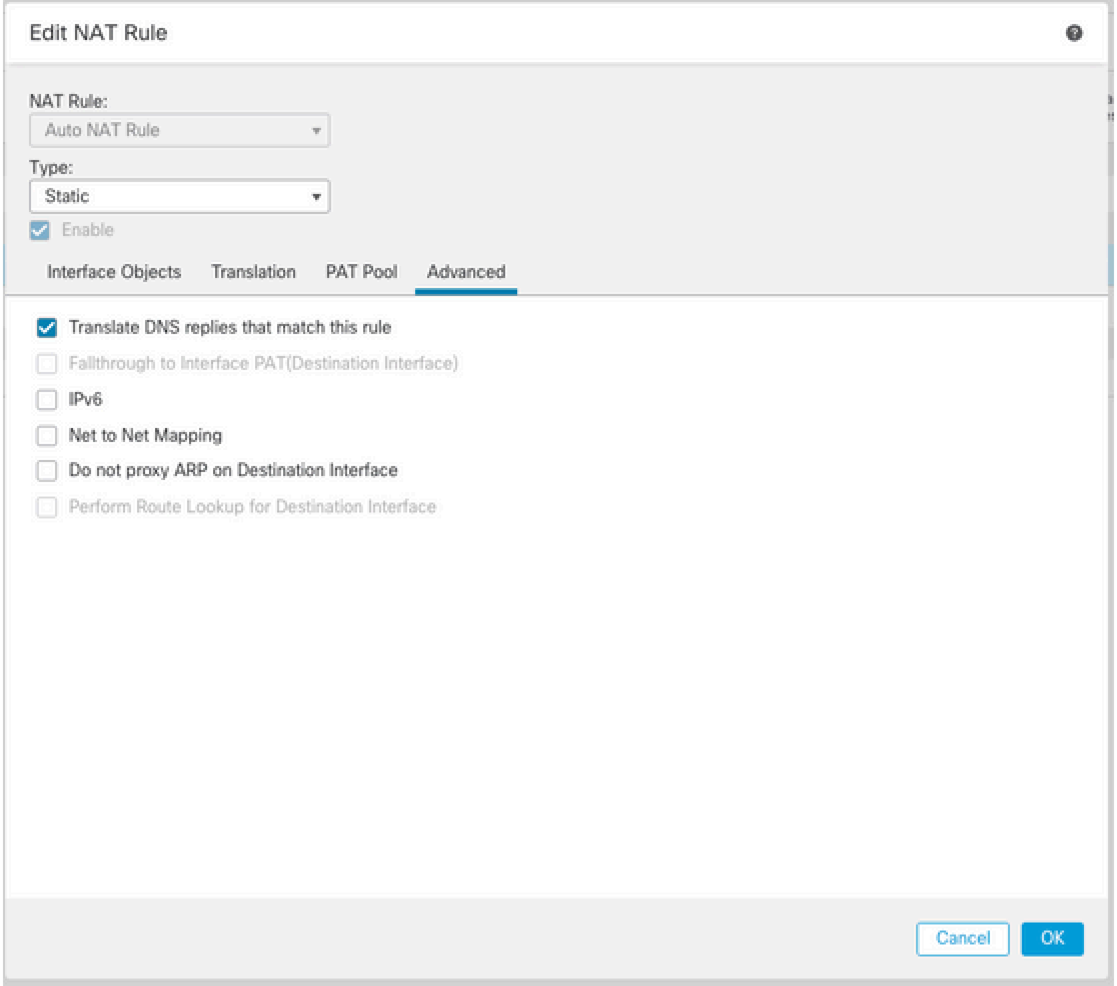
Original Port: TCP

Translated Packet

Translated Source: Address

4_mapped_to_6

Translated Port:



Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

☑ Translate DNS replies that match this rule

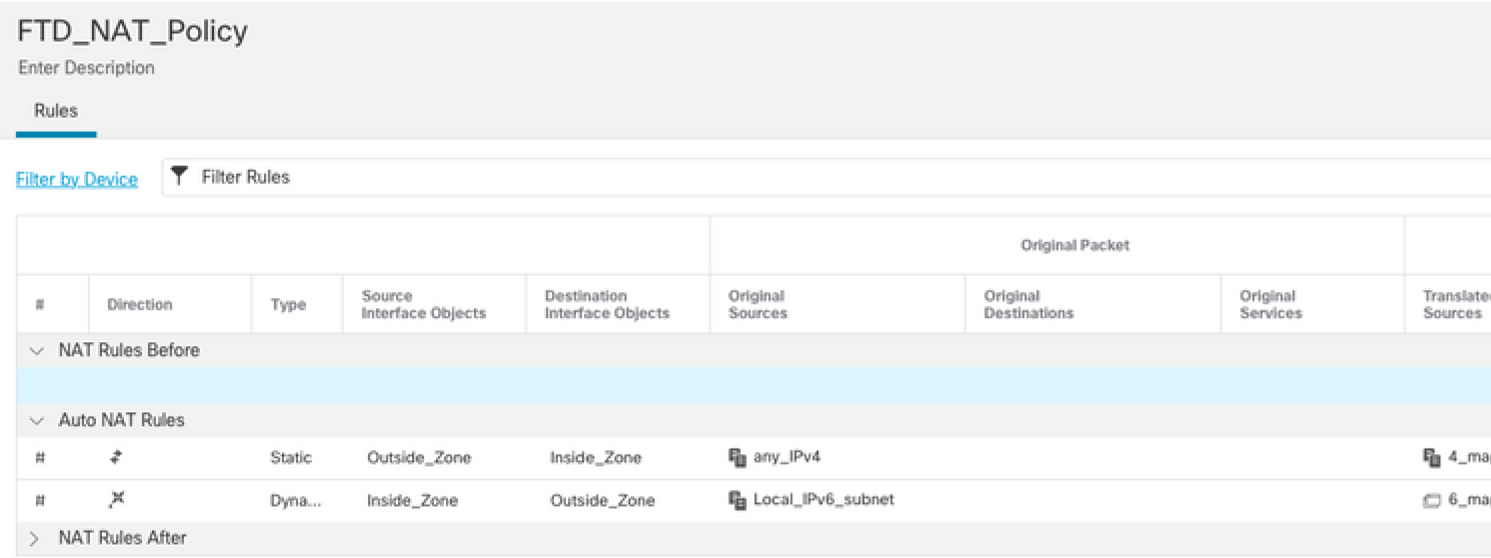
□ Fallthrough to Interface PAT(Destination Interface)

□ IPv6

□ Net to Net Mapping

□ Do not proxy ARP on Destination Interface

□ Perform Route Lookup for Destination Interface



FTD_NAT_Policy

Enter Description

					Original Packet			
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translate Sources
NAT Rules Before								
Auto NAT Rules								
#	⇄	Static	Outside_Zone	Inside_Zone	any_IPv4			4_ma
#	⤨	Dyna...	Inside_Zone	Outside_Zone	Local_IPv6_subnet			6_ma
NAT Rules After								

Continúe con la implementación de cambios en FTD.

Verificación

- Mostrar los nombres de interfaz y la configuración IP.

<#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
```

- Confirme la conectividad IPv6 desde la interfaz interna de FTD al cliente.

Host interno IPv6 IP fc00:0:0:1::100.

FTD Interfaz interna 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
```

- Mostrar la configuración de NAT en la CLI de FTD.

<#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
```

- Capturar tráfico.

Por ejemplo, la captura del tráfico del host IPv6 interno fc00:0:0:1::100 al servidor DNS es fc00::f:0:0:ac10:a64 UDP 53.

Aquí, el servidor DNS de destino es fc00::f:0:0:ac10:a64. Los últimos 32 bits son ac10:0a64. Estos bits son el octeto por octeto equivalente a 172,16,10,100. Firewall 6-to-4 traduce el servidor DNS fc00::f:0:0:ac10:a64 de IPv6 al equivalente 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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).