Configureer NAT 64 op beveiligde firewall die door FMC wordt beheerd

Inhoud

Inleiding

Dit document beschrijft hoe u NAT64 kunt configureren bij Firepower Threat Defence (FTD), beheerd door Fire Power Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over Secure Firewall Threat Defence en Secure Firewall Management Center.

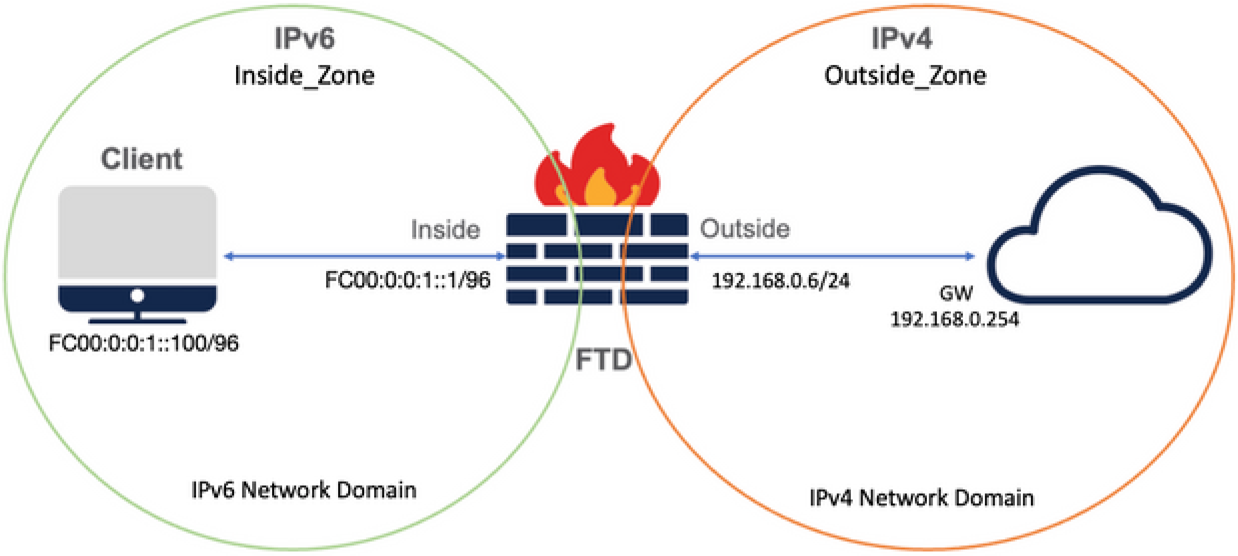
Gebruikte componenten

- Firepower Management Center 7.0.4
- Verdediging van vuurkracht 7.0.4.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram

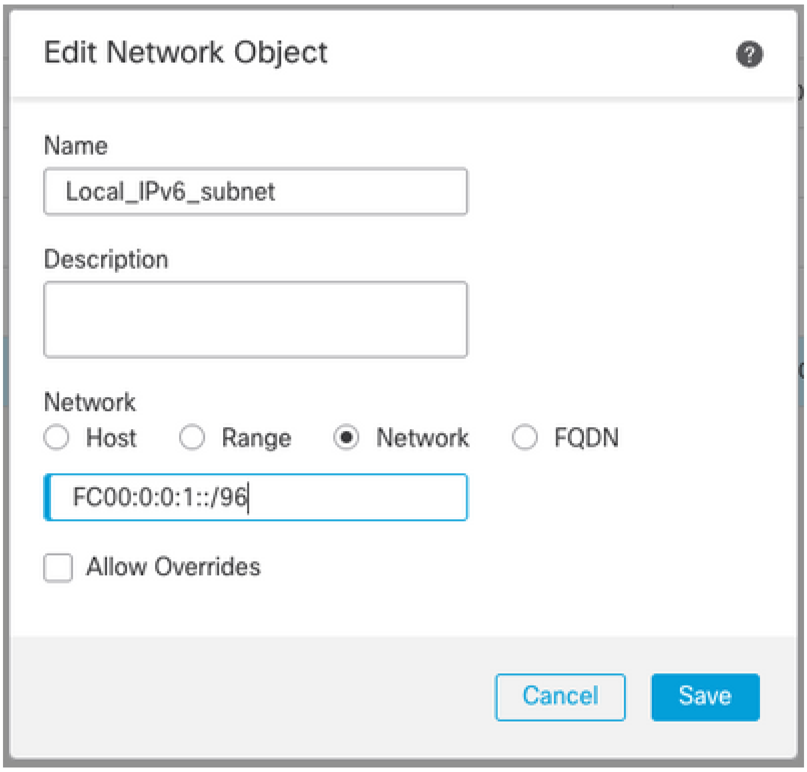


Netwerkobjecten configureren

- IPv6-netwerkobject voor verwijzing naar het interne IPv6-clientsubsysteem.

In de FMC GUI, navigeer naar **Objecten** > **Objectbeheer** > **Selecteer Netwerk uit linkermenu** > **Netwerk toevoegen** > **Object toevoegen**.

Zo wordt bijvoorbeeld Network Object Local_IPv6_Subnet gemaakt met het IPv6-subnetbestand FC00:0:0:1::/96.


Edit Network Object

Name: Local_IPv6_subnet

Description:

Network

○ Host ○ Range ● Network ○ FQDN

FC00:0:0:1::/96

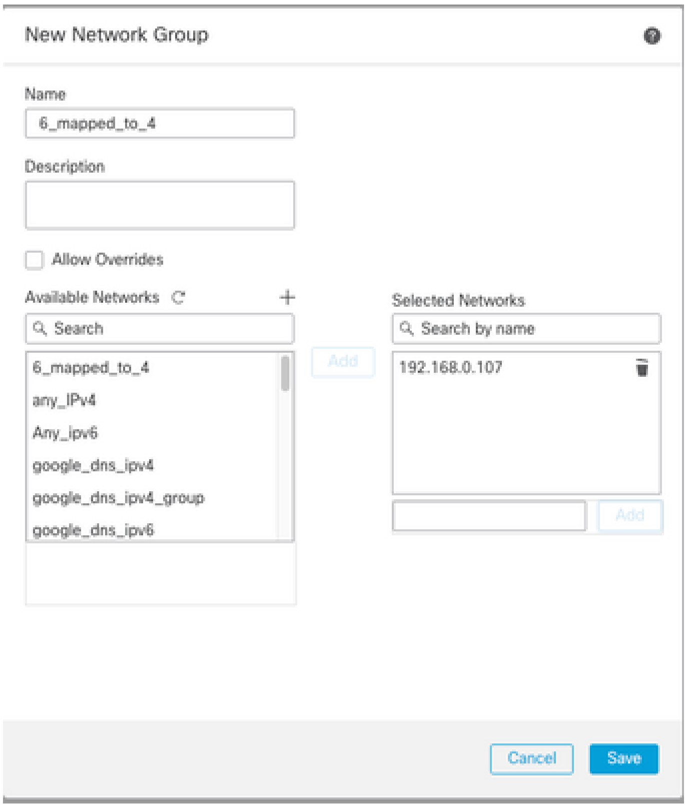
□ Allow Overrides

- IPv4-netwerkobject om IPv6-clients naar IPv4 te vertalen.

Ga in de FMC GUI naar **Objecten** > **Objectbeheer** > **Netwerk selecteren in het linkermenu** > **Netwerk toevoegen** > **Groep toevoegen**.

Zo is bijvoorbeeld Network Object 6_mapped_to_4 gemaakt met IPv4 host 192.168.0.107.

Afhankelijk van de hoeveelheid IPv6-hosts die in IPv4 moeten worden toegewezen, kunt u één objectnetwerk, een netwerkgroep met meerdere IPv4, of alleen NAT gebruiken voor de uitgaande interface.



New Network Group

Name: 6_mapped_to_4

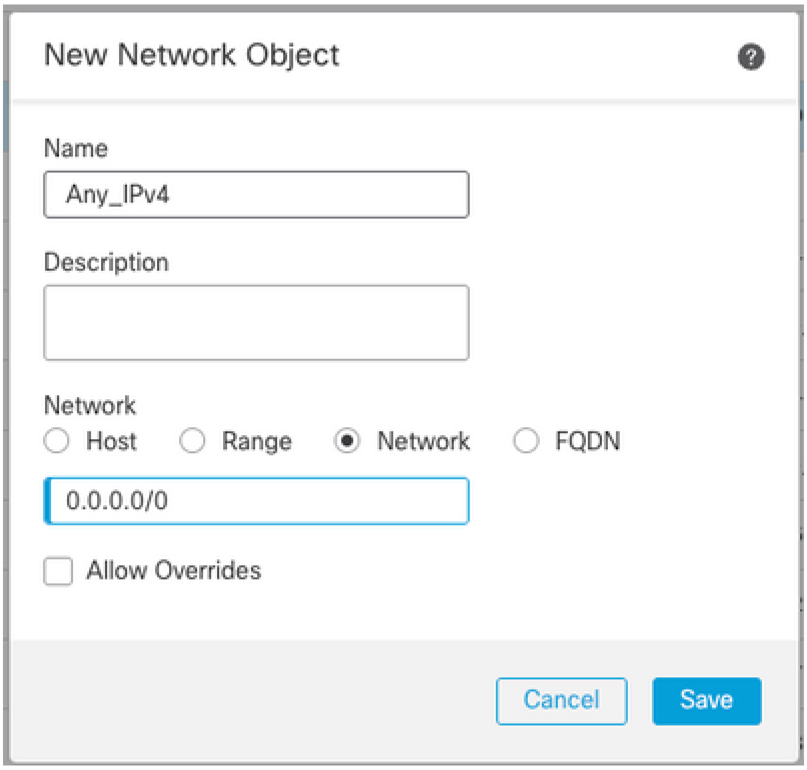
Available Networks: 6_mapped_to_4, any_IPv4, Any_ipv6, google_dns_ipv4, google_dns_ipv4_group, google_dns_ipv6

Selected Networks: 192.168.0.107

- IPv4 Network Object voor verwijzing naar de externe IPv4-hosts op internet.

In de FMC GUI, navigeer naar **Objecten** > **Objectbeheer** > **Selecteer Netwerk uit linkermenu** > **Netwerk toevoegen** > **Object toevoegen**.

Netwerkobject Any_IPv4 wordt bijvoorbeeld gemaakt met het IPv4-subnetnummer 0.0.0.0/0.



New Network Object

Name

Any_IPv4

Description

Network

○ Host ○ Range ● Network ○ FQDN

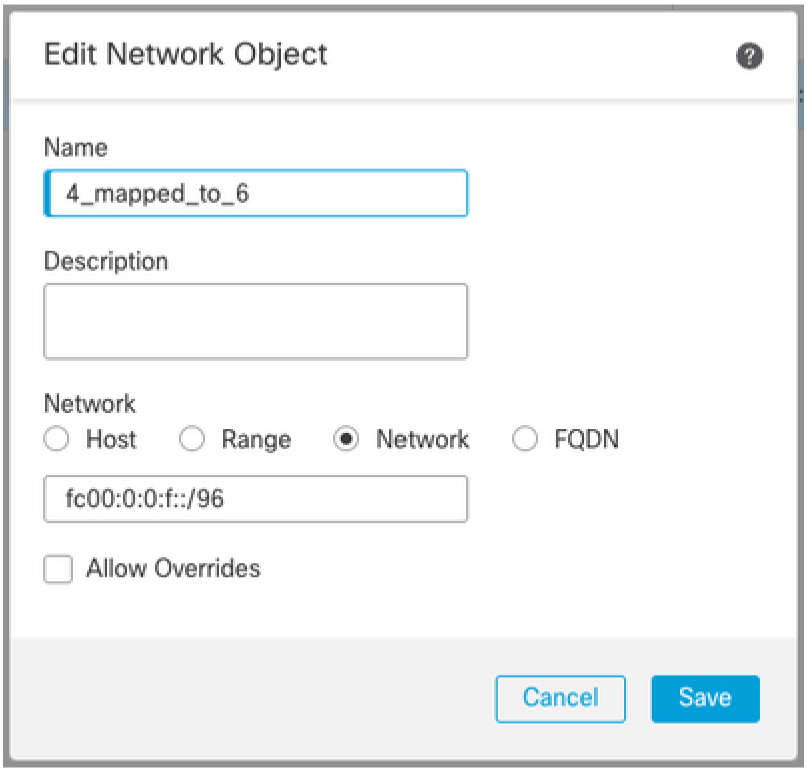
0.0.0.0/0

□ Allow Overrides

- IPv6 Network Object om externe IPv4-host naar ons IPv6-domein te vertalen.

Op FMC GUI, navigeer naar **Objecten** > **Objectbeheer** > **Selecteer Netwerk uit linkermenu** > **Netwerk toevoegen** > **Object toevoegen**.

Zo is bijvoorbeeld Network Object 4_mapped_to_6 gemaakt met IPv6-subnetwerkkaart 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

Interfaces op FTD voor IPv4/IPv6 configureren

Navigeren naar **Apparaten** > **Apparaatbeheer** > **FTD bewerken** > **Interfaces** en Inside en Outside interfaces configureren.

Voorbeeld:

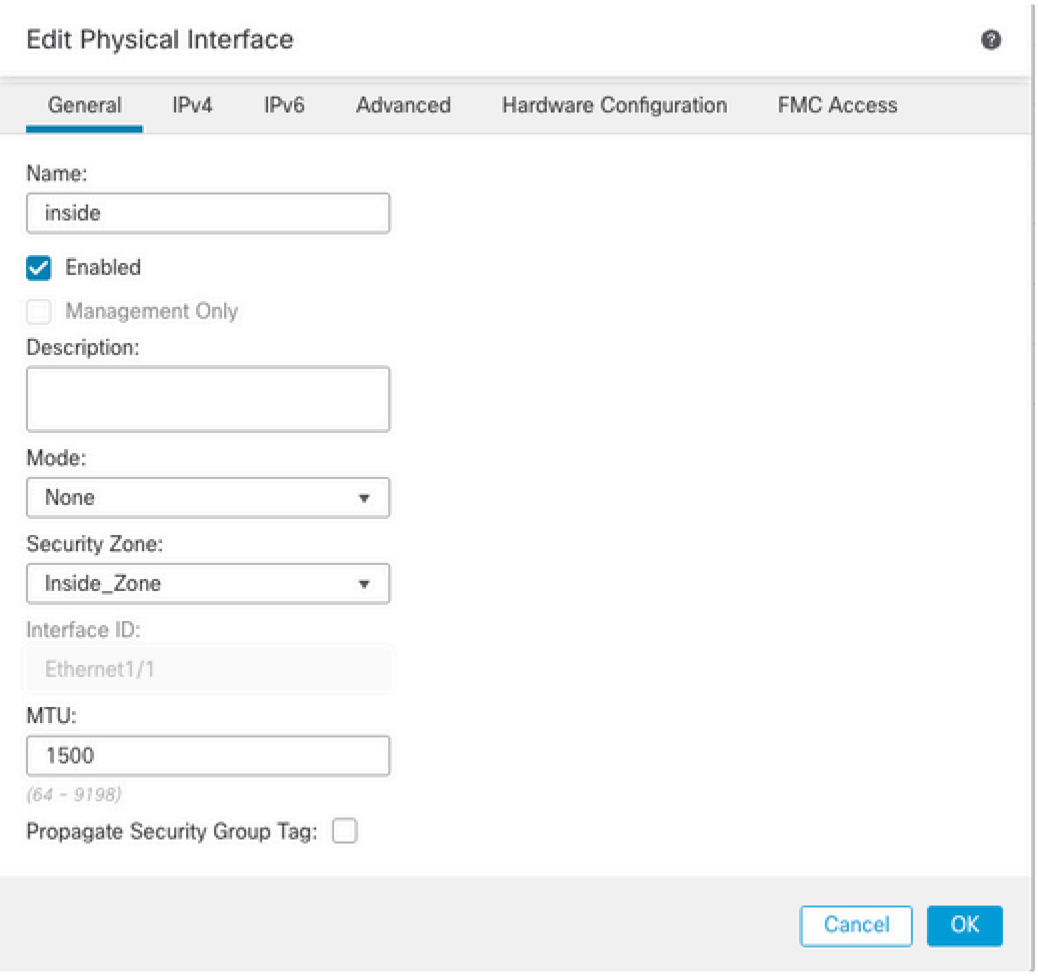
Interface Ethernet 1/1

Naam: Inside

Security Zone: binnen_zone

Als de security zone niet is gemaakt, kunt u deze maken in het **vervolgkeuzemenu Security Zone > Nieuw**.

IPv6-adres: FC00:0:0:1:1/96



Edit Physical Interface

Name: inside

☑ Enabled

□ Management Only

Description:

Mode: None

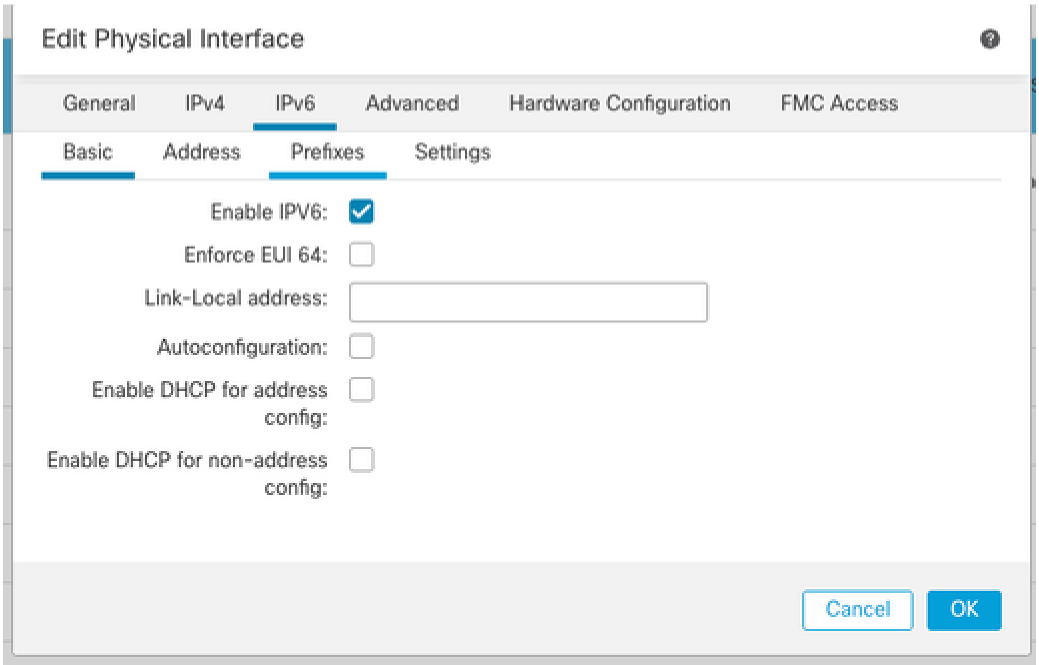
Security Zone: Inside_Zone

Interface ID: Ethernet1/1

MTU: 1500

(64 - 9198)

Propagate Security Group Tag: □



Enable IPV6: ☑

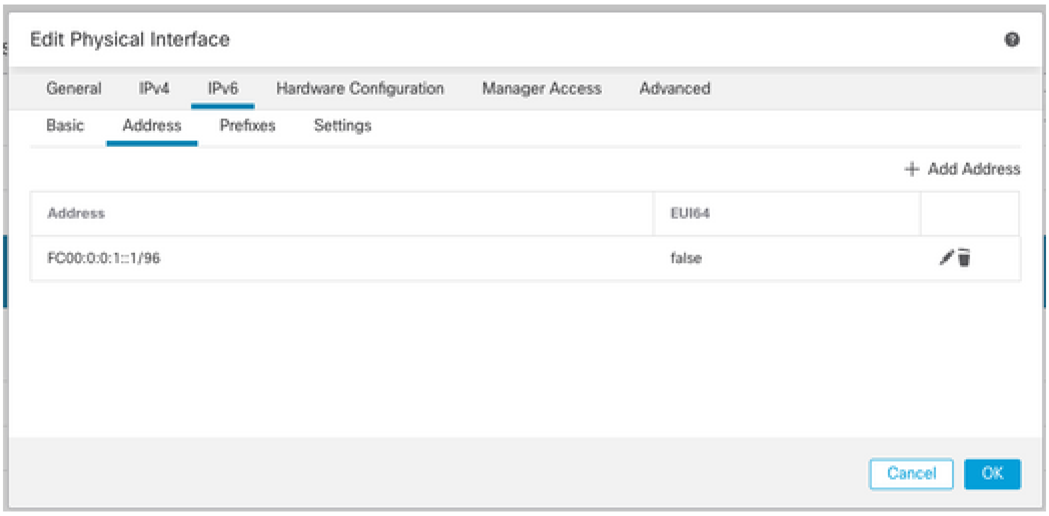
Enforce EUI 64: □

Link-Local address:

Autoconfiguration: □

Enable DHCP for address config: □

Enable DHCP for non-address config: □



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

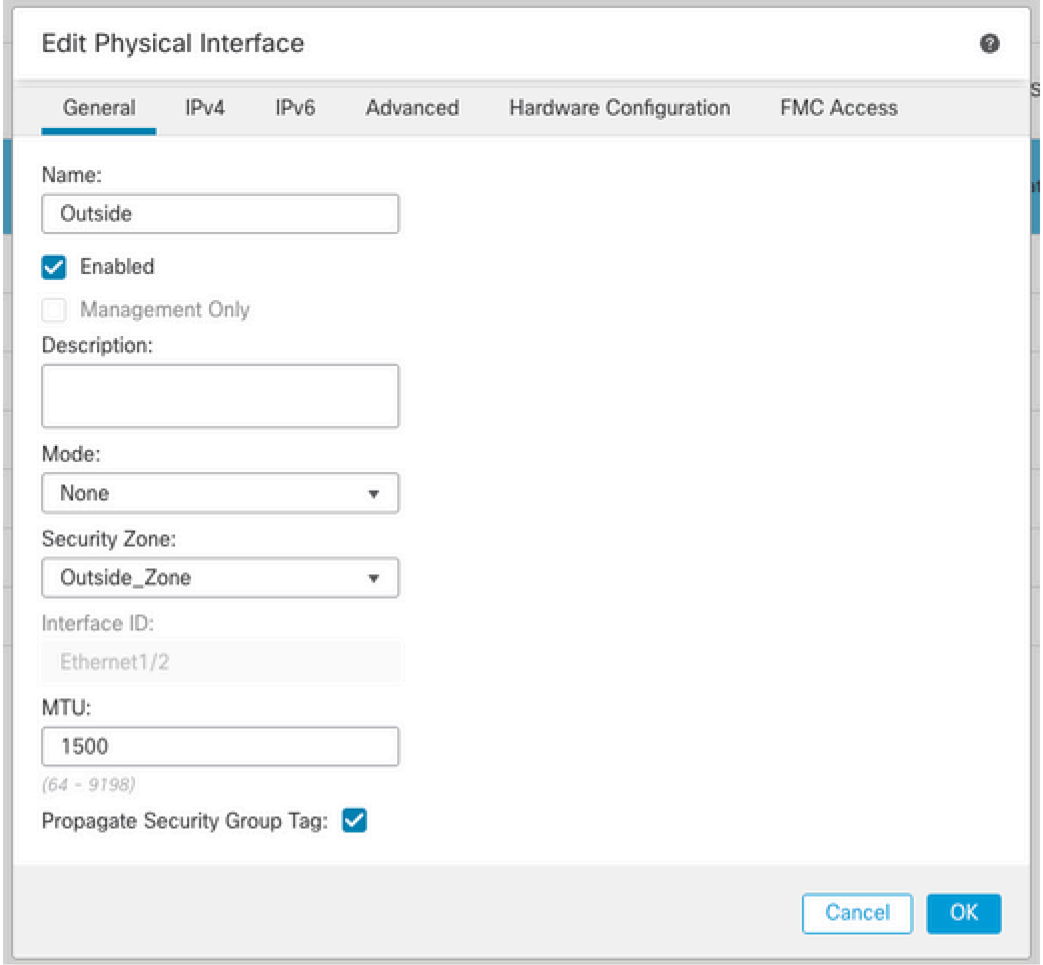
Interface Ethernet 1/2

Naam: Buiten

Security Zone: buiten_zone

Als security zone niet is gemaakt, kunt u deze maken in het **Security Zone vervolgkeuzemenu > Nieuw**.

IPv4-adres: 192.168.0.106/24



Edit Physical Interface

Name: Outside

☑ Enabled

□ Management Only

Description:

Mode: None

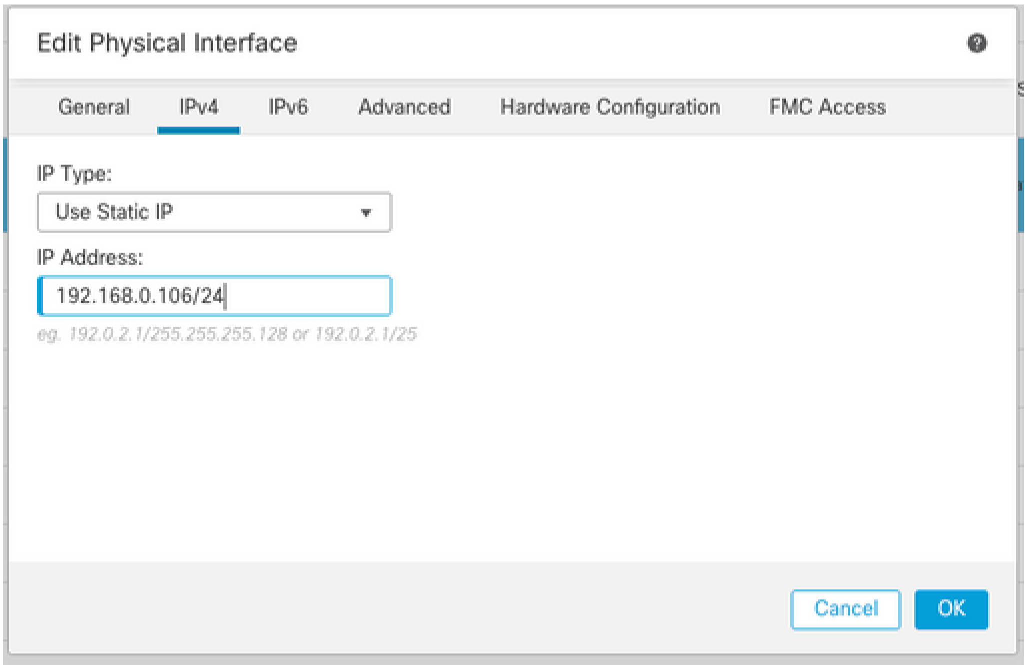
Security Zone: Outside_Zone

Interface ID: Ethernet1/2

MTU: 1500

(64 - 9198)

Propagate Security Group Tag: ☑



Edit Physical Interface

IP Type: Use Static IP

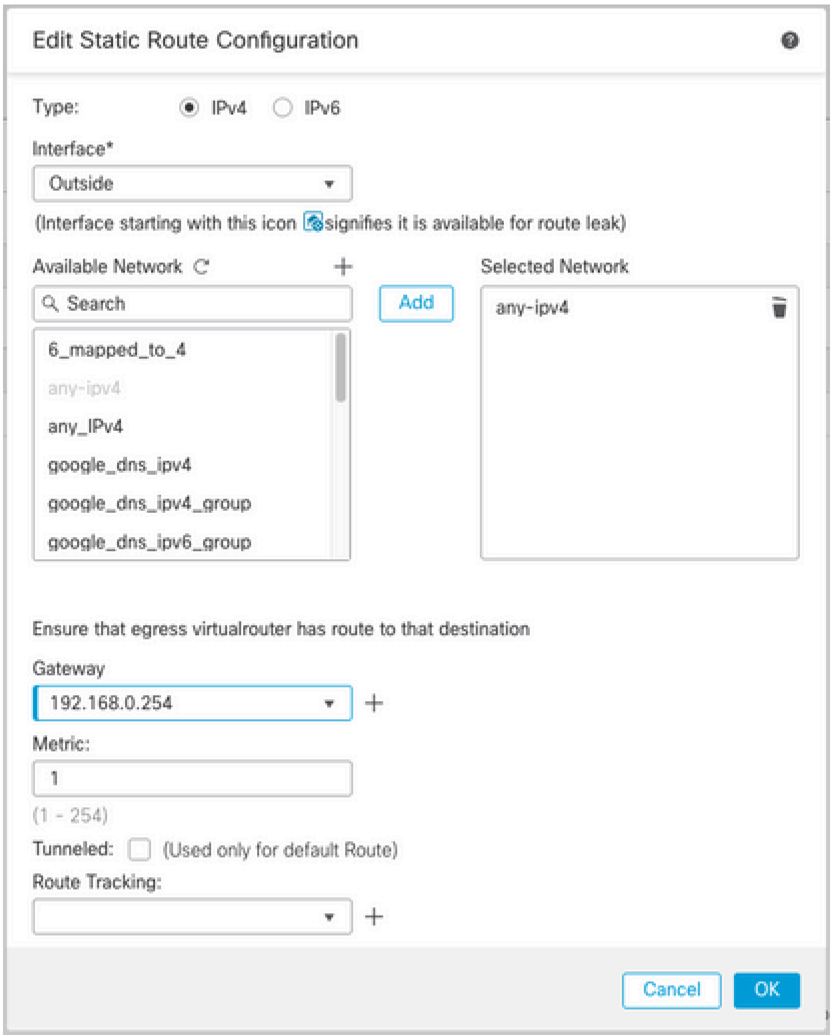
IP Address: 192.168.0.106/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Standaardroute configureren

Navigeer naar **Apparaten > Apparaatbeheer > FTD bewerken > Routing > Statische routing > Add Route**.

Bijvoorbeeld, standaard statische route op de buiteninterface met 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

Selected Network

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway

192.168.0.254

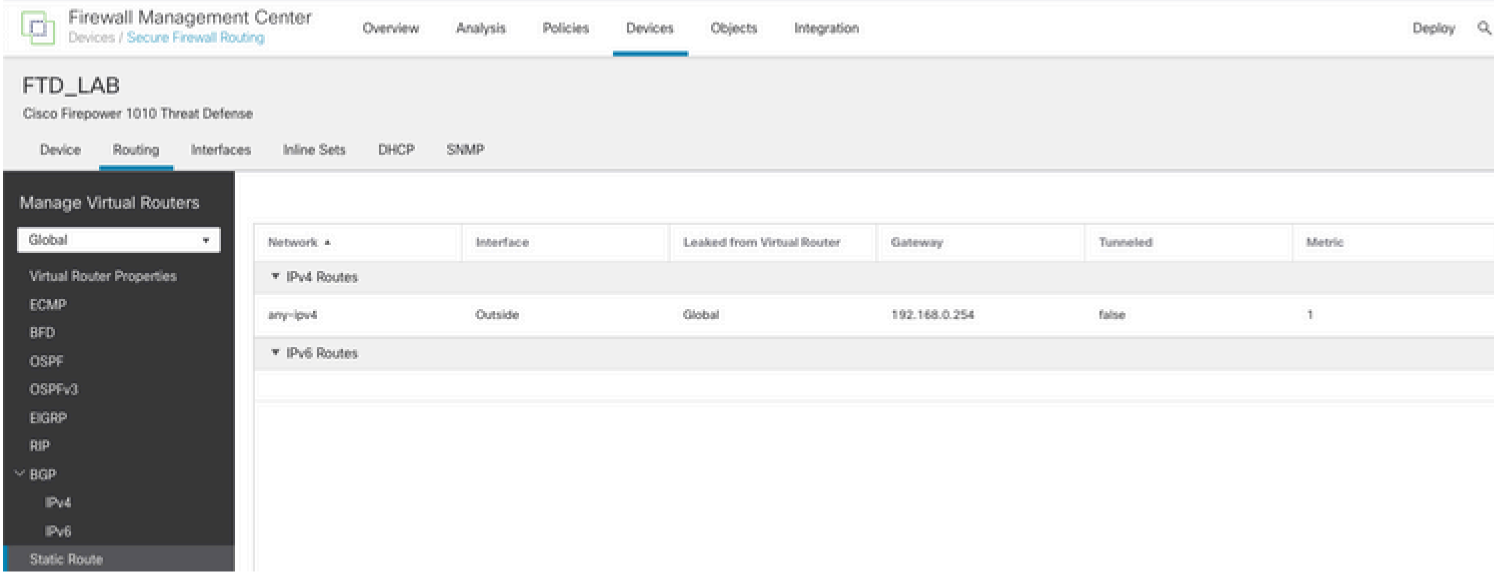
Metric:

1

(1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:



FTD_LAB

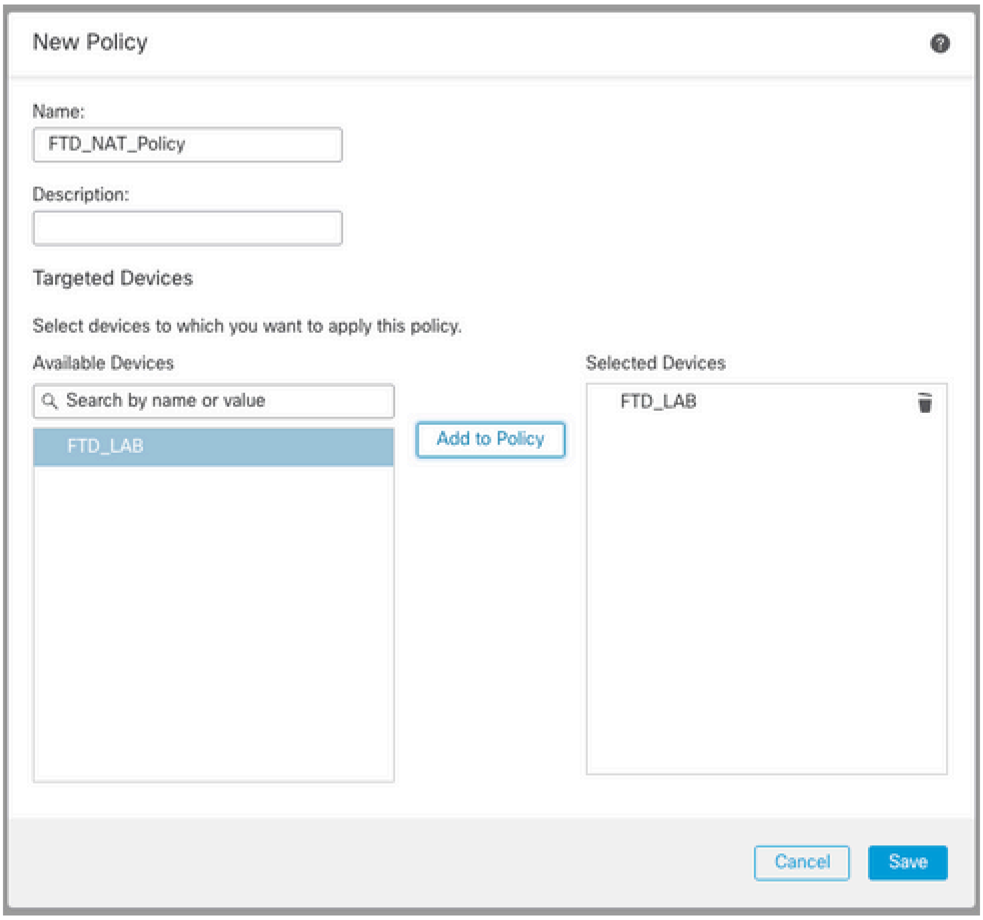
Cisco Firepower 1010 Threat Defense

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

NAT-beleid configureren

Ga in de FMC GUI naar **Apparaten > NAT > Nieuw Beleid > Threat Defense NAT** en voer een NAT-beleid in.

Zo wordt NAT-beleid FTD_NAT_Policy gemaakt en toegewezen aan de test FTD_LAB.



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

NAT-regels configureren

Uitgaande NAT.

Ga in de FMC GUI naar **Apparaten** > **NAT** > **Selecteer het NAT-beleid** > **Regel toevoegen** en creëer NAT-regel om het interne IPv6-netwerk naar de externe IPv4-pool te vertalen.

Zo is bijvoorbeeld Network Object Local_IPv6_subnet dynamisch vertaald naar Network Object 6_mapped_to_4.

NAT-regel: automatische NAT-regel

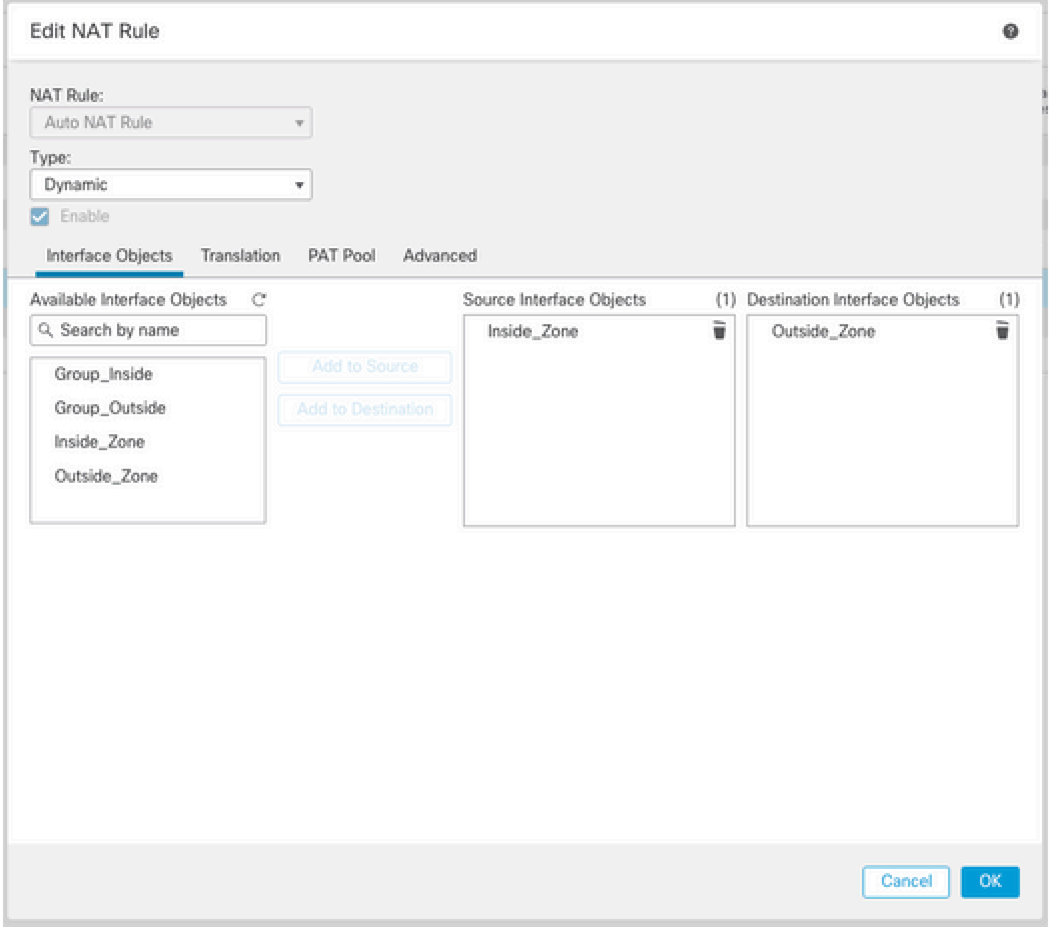
Type: Dynamisch

Source Interface Objects: Inside_Zone

Bestemmingsinterface-objecten: Outside_Zone

Oorspronkelijke bron: Local_IPv6_Subnet

Vertaalde bron: 6_mapped_to_4



Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Available Interface Objects

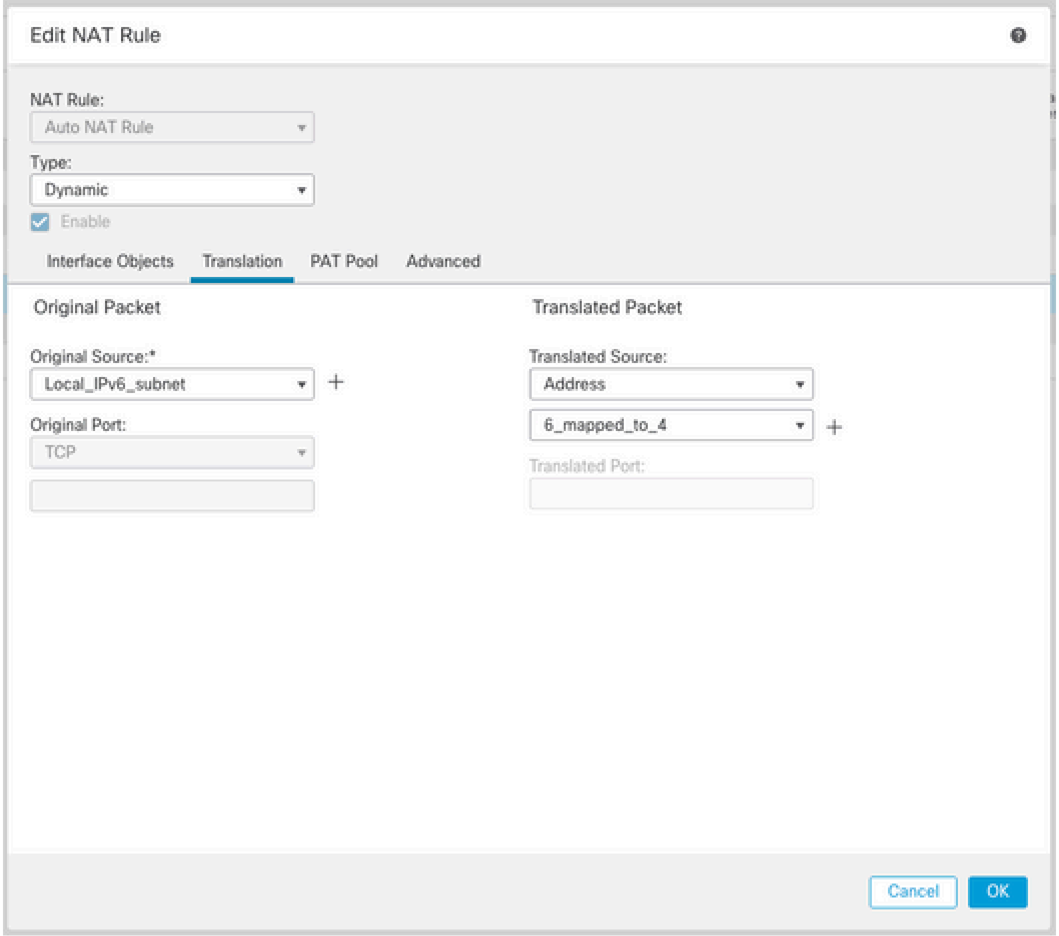
- Group_Inside
- Group_Outside
- Inside_Zone
- Outside_Zone

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:

Inkomende NAT.

Ga in de FMC GUI naar **Apparaten** > **NAT** > **Selecteer het NAT-beleid** > **Regel toevoegen** en creëer NAT-regel om extern IPv4-verkeer naar interne IPv6-netwerkpool te vertalen. Dit maakt interne communicatie met uw lokale IPv6-subnetverbinding mogelijk.

Schakel bovendien DNS-herschrijving in op deze regel zodat antwoorden van de externe DNS-server kunnen worden geconverteerd van A-records (IPv4) naar AAA-records (IPv6).

Bijvoorbeeld, buiten netwerk Any_IPv4 wordt statisch vertaald naar IPv6-subnetwerkknooppunt 2100:6400::/96 gedefinieerd in het object 4_mapped_to_6.

NAT-regel: Auto NAT-regel

Type: Statisch

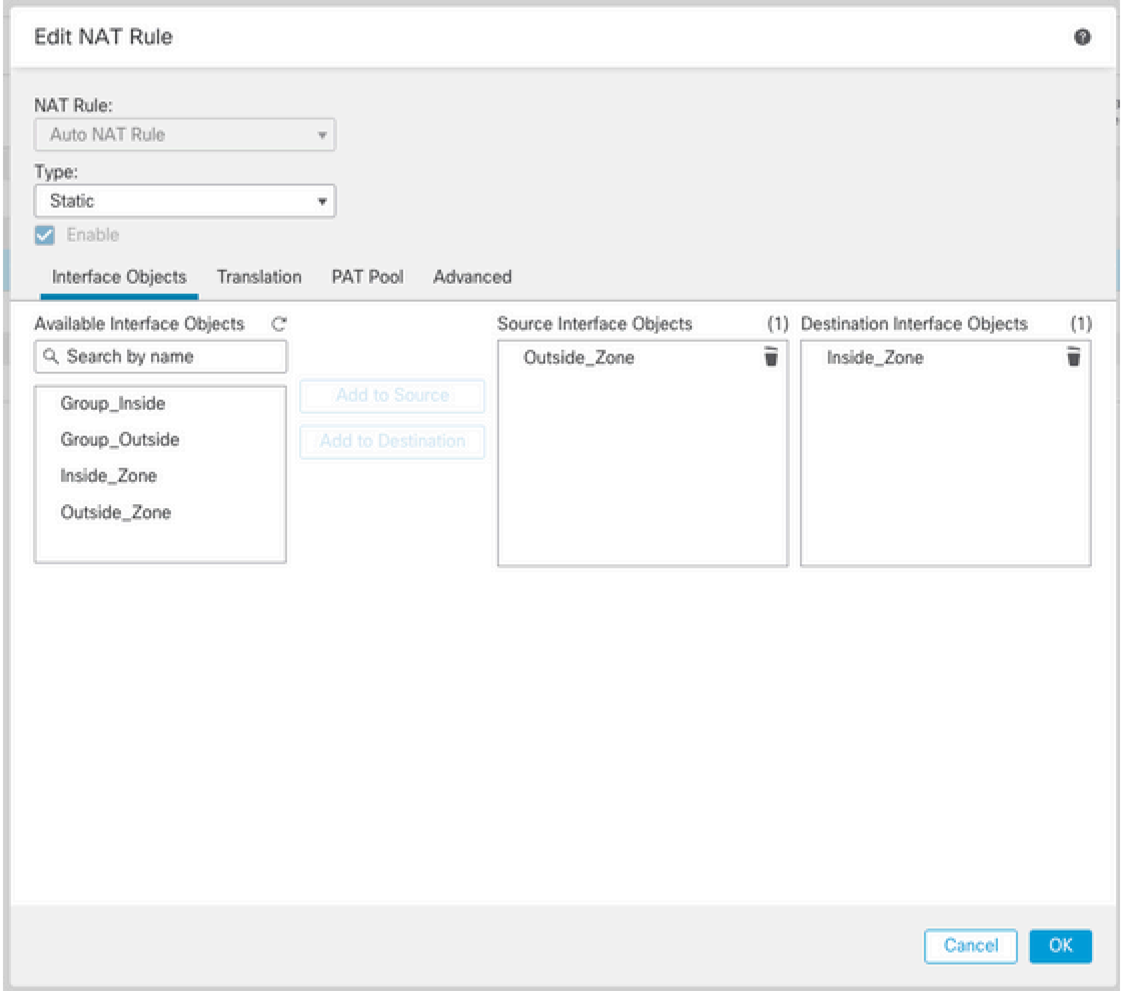
Bron interface-objecten: Outside_Zone

Bestemmingsinterface-objecten: Inside_Zone

Oorspronkelijke bron: Any_IPv4

Vertaalde bron: 4_mapped_to_6

Vertaal DNS antwoorden die overeenkomen met deze regel: Ja (Schakel selectievakje in)



Edit NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Static

☑ Enable

Available Interface Objects

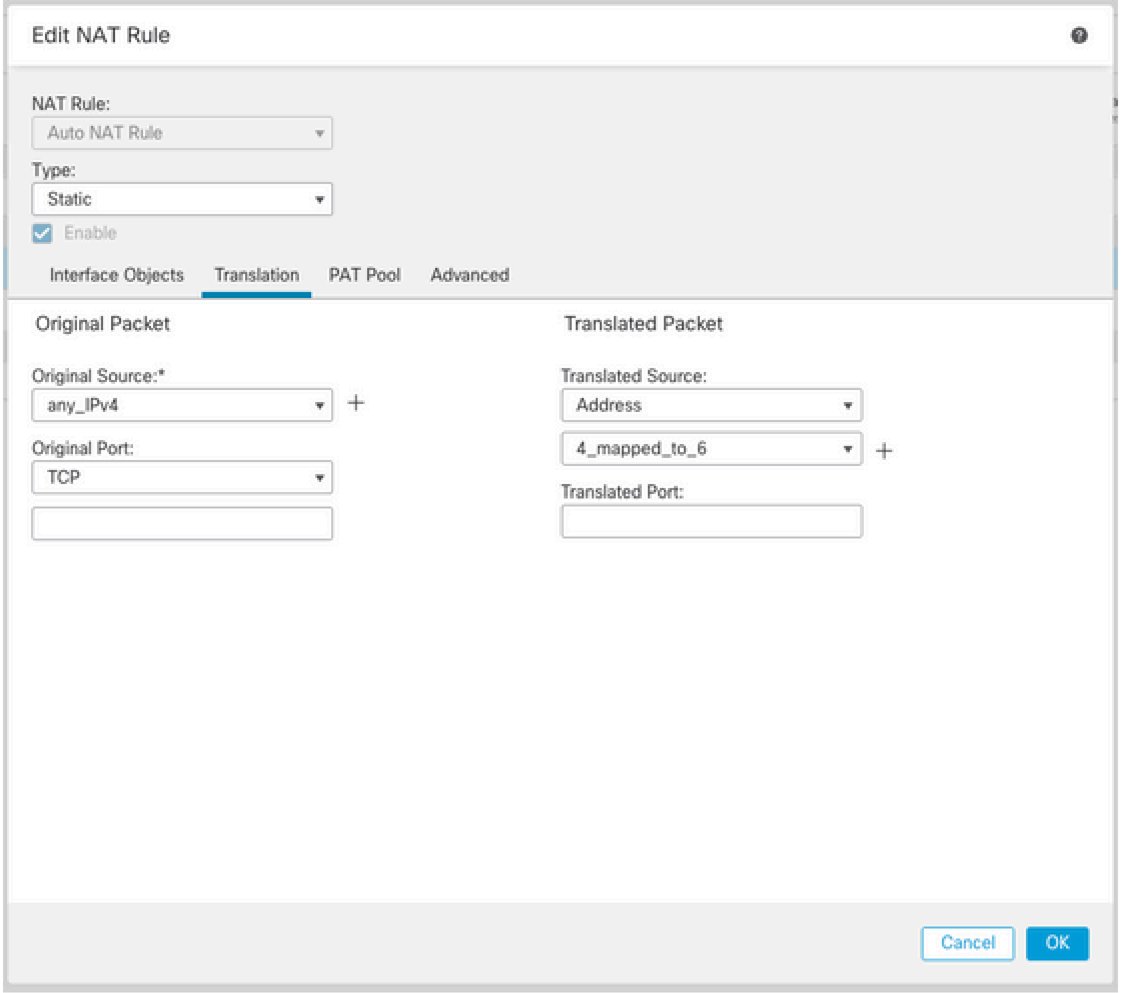
Group_Inside
Group_Outside
Inside_Zone
Outside_Zone

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

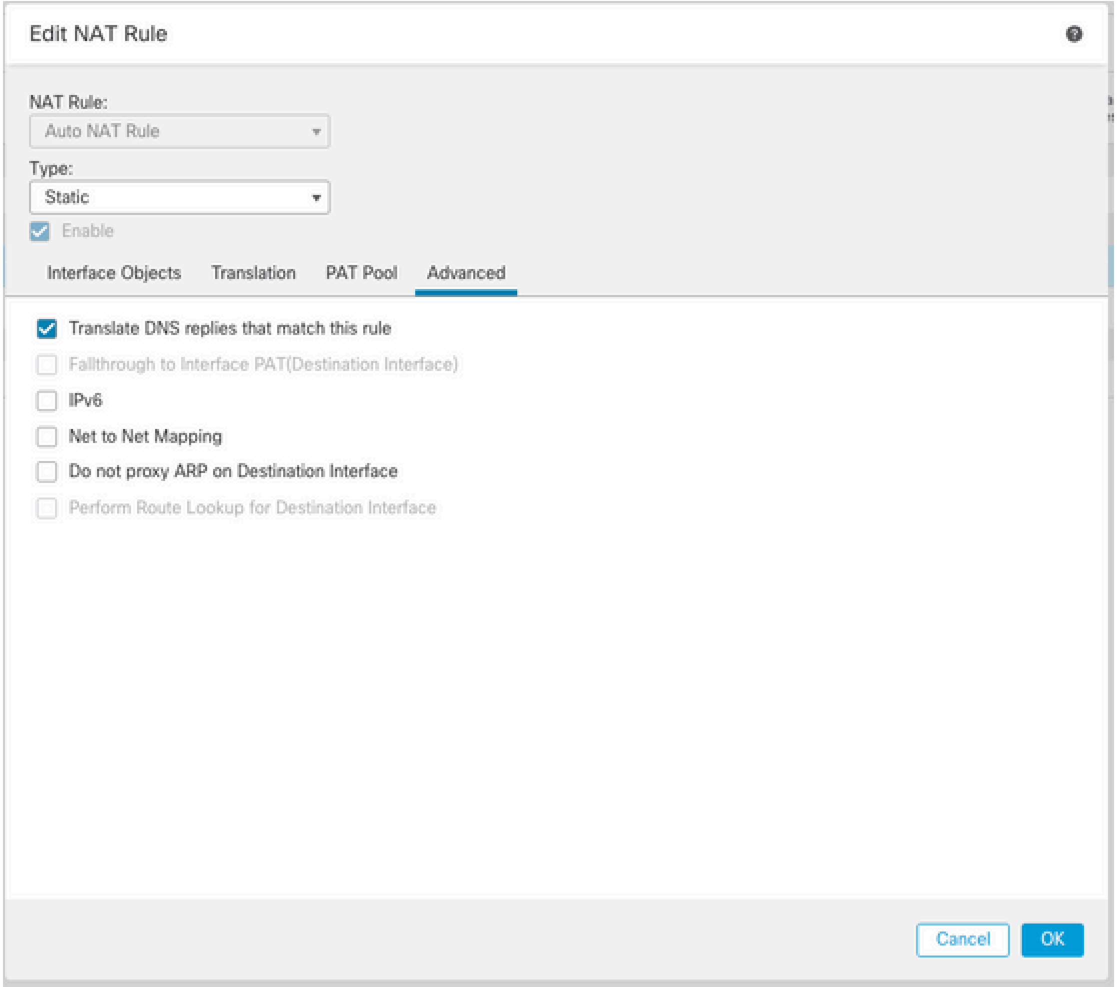
Original Port: TCP

Translated Packet

Translated Source: Address

4_mapped_to_6

Translated Port:



NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

☑ Translate DNS replies that match this rule

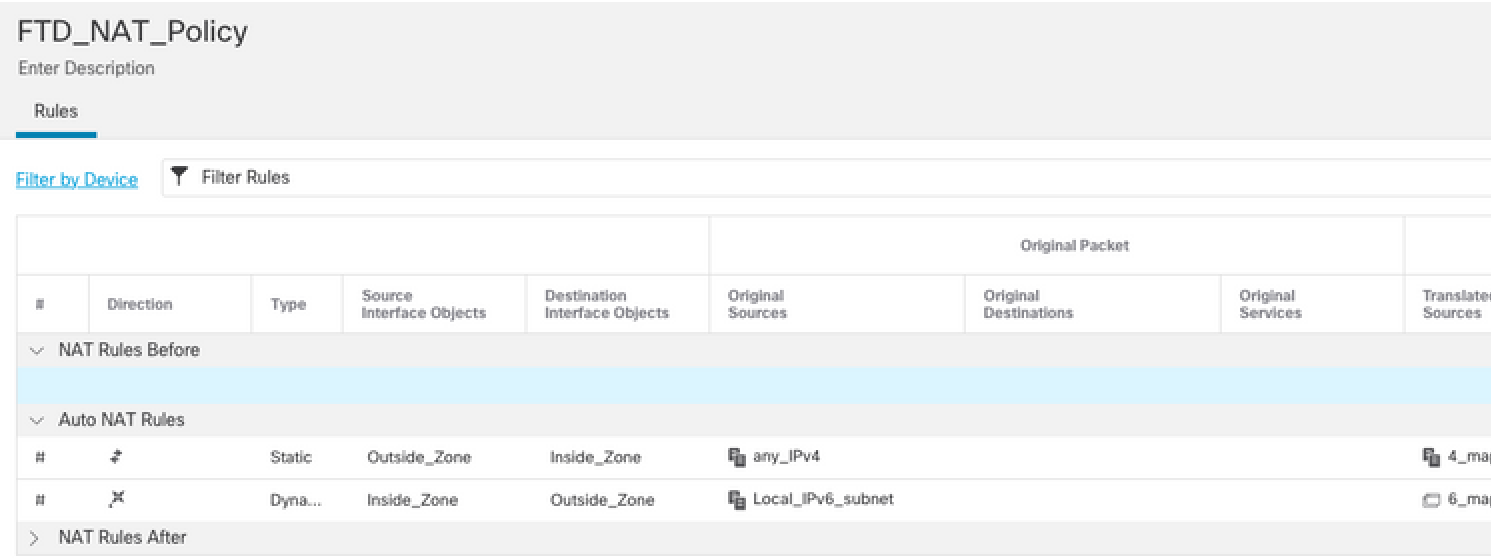
□ Fallthrough to Interface PAT(Destination Interface)

□ 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								

Vervolg de implementatie van wijzigingen in het FTD.

Verificatie

- Geef interfacenamen en IP-configuratie weer.

<#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
```

- Bevestig IPv6-connectiviteit van FTD-binnenkant van interface naar client.

IPv6 interne host-IP fc00:0:0:1:100.

FTD Inside interface 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
```

- Geef NAT-configuratie op de FTD CLI weer.

<#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
```

- Leg verkeer vast.

Neem bijvoorbeeld verkeer op van interne IPv6-host fc00:0:0:1::100 naar DNS-server is fc00::f:0:0:ac10:a64 UDP 53.

Hier is de doelDNS-server fc00::f:0:ac10:a64. De laatste 32 bits zijn ac10:0a64. Deze bits zijn het octet-voor-octet equivalent aan 172,16,10,100. Firewall 6-to-4 vertaalt IPv6 DNS-server fc00:f:0:0:ac10:a64 naar het equivalent van 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
```

Over deze vertaling