

# Configuration de NAT 64 sur le pare-feu sécurisé géré par FMC

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration des objets réseau](#)

[Configuration des interfaces sur FTD pour IPv4/IPv6](#)

[Configurer la route par défaut](#)

[Configurer la stratégie NAT](#)

[Configurer les règles NAT](#)

[Vérification](#)

## Introduction

Ce document décrit comment configurer NAT64 sur Firepower Threat Defense (FTD) géré par Fire Power Management Center (FMC).

## Conditions préalables

### Exigences

Cisco vous recommande d'avoir des connaissances sur Secure Firewall Threat Defense et Secure Firewall Management Center.

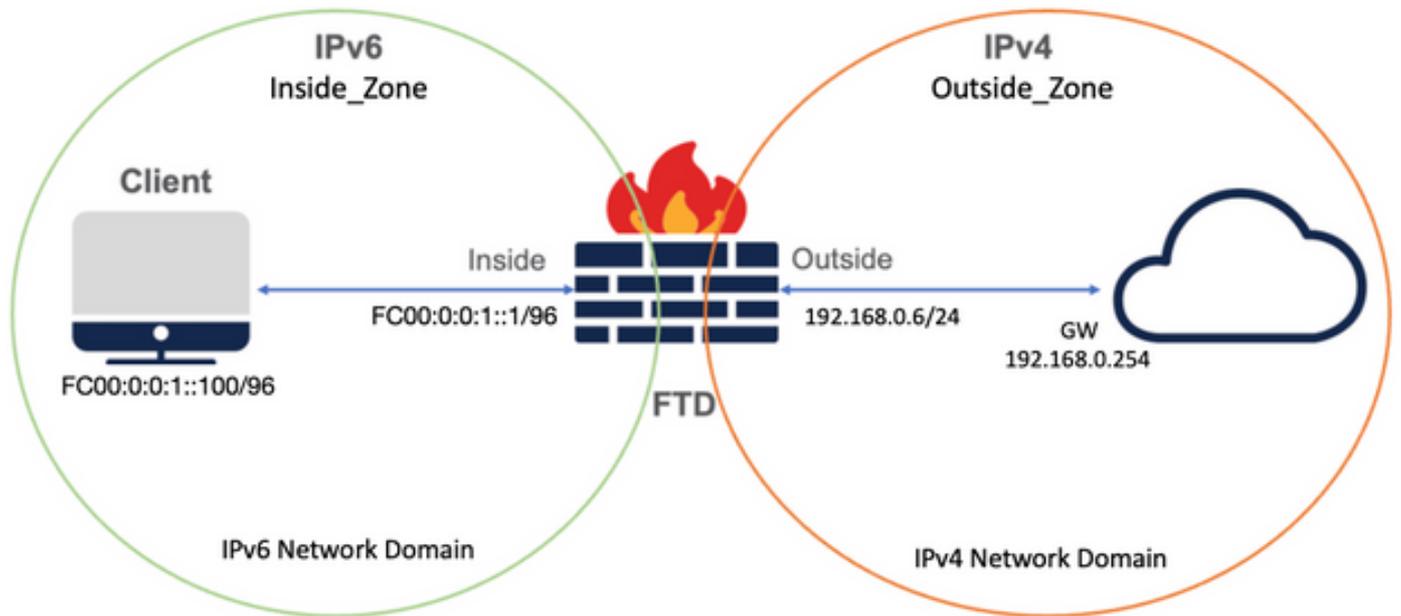
### Composants utilisés

- Firepower Management Center 7.0.4.
- Défense contre les menaces Firepower 7.0.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configurer

## Diagramme du réseau



## Configuration des objets réseau

- IPv6 Network Object pour référencer le sous-réseau client IPv6 interne.

Dans l'interface utilisateur graphique de FMC, accédez à Objets > Gestion des objets > Sélectionnez Réseau dans le menu de gauche > Ajouter un réseau > Ajouter un objet.

Par exemple, l'objet réseau `Local_IPv6_subnet` est créé avec le sous-réseau IPv6 `FC00:0:0:1::/96`.

## Edit Network Object ?

**Name**

**Description**

**Network**

Host    Range    Network    FQDN

Allow Overrides

- IPv4 Network Object pour traduire les clients IPv6 en IPv4.

Dans l'interface utilisateur graphique de FMC, accédez à Objets > Gestion des objets > Sélectionner le réseau dans le menu de gauche > Ajouter le réseau > Ajouter un groupe.

Par exemple, l'objet réseau 6\_mapped\_to\_4 est créé avec l'hôte IPv4 192.168.0.107.

En fonction de la quantité d'hôtes IPv6 à mapper dans IPv4, vous pouvez utiliser un réseau à objet unique, un groupe de réseaux avec plusieurs adresses IPv4 ou simplement la fonction NAT vers l'interface de sortie.

## New Network Group



Name

Description

Allow Overrides

Available Networks  

- 6\_mapped\_to\_4
- any\_IPv4
- Any\_ipv6
- google\_dns\_ipv4
- google\_dns\_ipv4\_group
- google\_dns\_ipv6

Add

Selected Networks

192.168.0.107 

Add

Cancel

Save

- IPv4 Network Object pour référencer les hôtes IPv4 externes sur Internet.

Dans l'interface utilisateur graphique de FMC, accédez à Objets > Gestion des objets > Sélectionnez Réseau dans le menu de gauche > Ajouter un réseau > Ajouter un objet.

Par exemple, Network Object Any\_IPv4 est créé avec le sous-réseau IPv4 0.0.0.0/0.

## New Network Object ?

Name

Description

Network

Host    Range    Network    FQDN

Allow Overrides

- IPv6 Network Object pour traduire l'hôte IPv4 externe en domaine IPv6.

Dans l'interface utilisateur graphique de FMC, accédez à Objets > Gestion des objets > Sélectionner le réseau dans le menu de gauche > Ajouter le réseau > Ajouter un objet.

Par exemple, l'objet réseau 4\_mapped\_to\_6 est créé avec le sous-réseau IPv6 FC00:0:0:F::/96.

## Edit Network Object ?

Name

Description

Network  
 Host    Range    Network    FQDN

Allow Overrides

### Configuration des interfaces sur FTD pour IPv4/IPv6

Accédez à **Devices > Device Management > Edit FTD > Interfaces** et configurez les interfaces Interne et Externe.

Exemple :

Interface Ethernet 1/1

Nom : Intérieur

Zone de sécurité : Inside\_Zone

Si la zone de sécurité n'est pas créée, vous pouvez la créer dans le menu déroulant **Zone de sécurité > Nouveau**.

Adresse IPv6 : FC00:0:0:1::1/96

## Edit Physical Interface



General

IPv4

IPv6

Advanced

Hardware Configuration

FMC Access

Name:

inside

Enabled

Management Only

Description:

Mode:

None

Security Zone:

Inside\_Zone

Interface ID:

Ethernet1/1

MTU:

1500

(64 - 9198)

Propagate Security Group Tag:

Cancel

OK

### Edit Physical Interface

General IPv4 **IPv6** Advanced Hardware Configuration FMC Access

Basic Address **Prefixes** Settings

Enable IPV6:

Enforce EUI 64:

Link-Local address:

Autoconfiguration:

Enable DHCP for address config:

Enable DHCP for non-address config:

Cancel OK

### Edit Physical Interface

General IPv4 **IPv6** Hardware Configuration Manager Access Advanced

Basic Address **Prefixes** Settings

+ Add Address

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

Cancel OK

Interface Ethernet 1/2

Nom : Externe

Zone de sécurité : Outside\_Zone

Si la zone de sécurité n'est pas créée, vous pouvez la créer dans le menu déroulant Zone de sécurité > Nouveau.

Adresse IPv4 : 192.168.0.106/24

### Edit Physical Interface ?

**General**   IPv4   IPv6   Advanced   Hardware Configuration   FMC Access

Name:

Enabled  
 Management Only

Description:

Mode:  ▼

Security Zone:  ▼

Interface ID:

MTU:

(64 - 9198)

Propagate Security Group Tag:

**Edit Physical Interface**

General **IPv4** IPv6 Advanced Hardware Configuration FMC Access

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*

Cancel OK

## Configurer la route par défaut

Accédez à **Devices > Device Management > Edit FTD > Routing > Static Routing > Add Route**.

Par exemple, route statique par défaut sur l'interface externe avec la passerelle 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 



Search

Add

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:



Cancel

OK

The screenshot shows the Firewall Management Center (FMC) interface for a Cisco Firepower 1010 Threat Defense device. The main navigation tabs are Overview, Analysis, Policies, Devices, Objects, and Integration. The current view is 'Devices' for the device 'FTD\_LAB'. The left sidebar shows 'Manage Virtual Routers' with a dropdown menu set to 'Global'. The main content area displays a table of routes:

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

## Configurer la stratégie NAT

Dans l'interface graphique FMC, accédez à **Devices > NAT > New Policy > Threat Defense NAT** et créez une stratégie NAT.

Par exemple, la stratégie NAT `FTD_NAT_Policy` est créée et attribuée au test `FTD_LAB`.

### New Policy

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Selected Devices

Search by name or value

FTD\_LAB

Add to Policy

FTD\_LAB

Cancel Save

## Configurer les règles NAT

NAT sortante.

Dans l'interface utilisateur graphique de FMC, accédez à Devices > NAT > Select the NAT policy > Add Rule et créez une règle NAT pour traduire le réseau IPv6 interne en pool IPv4 externe.

Par exemple, l'objet réseau Local\_IPv6\_subnet est converti dynamiquement en objet réseau 6\_mapped\_to\_4.

Règle NAT : règle NAT automatique

Type : dynamique

Objets d'interface source : Inside\_Zone

Objets d'interface de destination : Outside\_Zone

Source d'origine : Local\_IPv6\_subnet

Source traduite : 6\_mapped\_to\_4

**Edit NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- Group\_Inside
- Group\_Outside
- Inside\_Zone
- Outside\_Zone

Add to Source

Add to Destination

Source Interface Objects (1)

- Inside\_Zone

Destination Interface Objects (1)

- Outside\_Zone

Cancel OK

**Edit NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

**Original Packet**

Original Source:\* Local\_IPv6\_subnet +

Original Port: TCP

**Translated Packet**

Translated Source: Address +

Translated Port:

Cancel OK

NAT entrante.

Dans l'interface utilisateur graphique de FMC, accédez à Devices > NAT > Select the NAT policy > Add Rule et créez une règle NAT pour traduire le trafic IPv4 externe en pool de réseau IPv6 interne. Cela permet la communication interne avec votre sous-réseau IPv6 local.

En outre, activez la réécriture DNS sur cette règle afin que les réponses du serveur DNS externe puissent être converties des enregistrements A (IPv4) en enregistrements AAAA (IPv6).

Par exemple, Outside Network Any\_IPv4 est converti de manière statique en sous-réseau IPv6 2100:6400::/96 défini dans l'objet 4\_mapped\_to\_6.

Règle NAT : règle NAT automatique

Type : Statique

Objets d'interface source : Outside\_Zone

Objets d'interface de destination : Inside\_Zone

Source originale : Any\_IPv4

Source traduite : 4\_mapped\_to\_6

Traduire les réponses DNS qui correspondent à cette règle : Oui (case à cocher Activer)

**Edit NAT Rule**

NAT Rule:  
Auto NAT Rule

Type:  
Static

Enable

Interface Objects   Translation   PAT Pool   Advanced

Available Interface Objects  

- Group\_Inside
- Group\_Outside
- Inside\_Zone
- Outside\_Zone

Add to Source

Add to Destination

Source Interface Objects (1)  
Outside\_Zone

Destination Interface Objects (1)  
Inside\_Zone

Cancel   OK

## Edit NAT Rule



NAT Rule:

Auto NAT Rule

Type:

Static

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet

Translated Packet

Original Source:\*

any\_IPv4 +

Translated Source:

Address

Original Port:

TCP

4\_mapped\_to\_6 +

Translated Port:

Cancel

OK

### Edit NAT Rule

NAT Rule:

Type:

Enable

Interface Objects   Translation   PAT Pool   **Advanced**

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 Show Warnings Save Cancel

Enter Description Policy Assignments (1)

Rules Filter by Device Filter Rules Add Rule

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
NAT Rules Before											
Auto NAT Rules											
#	↔	Static	Outside_Zone	Inside_Zone	any_IPv4			4_mapped_to_6			Dns:true
#	↔	Dyna...	Inside_Zone	Outside_Zone	Local_IPv6_subnet			6_mapped_to_4			Dns:false
NAT Rules After											

Poursuivez le déploiement des modifications apportées au FTD.

## Vérification

- Affichez les noms des interfaces et la configuration 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
```

- Confirmez la connectivité IPv6 de l'interface interne FTD au client.

IPv6 internal host IP fc00:0:0:1::100.

FTD Interface interne 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

- Affichez la configuration NAT sur l'interface CLI 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
```

- Capturez le trafic.

Par exemple, capturer le trafic de l'hôte IPv6 interne fc00:0:0:1::100 vers le serveur DNS est fc00::f:0:0:ac10:a64 UDP 53.

Ici, le serveur DNS de destination est fc00::f:0:0:ac10:a64. Les 32 derniers bits sont ac10:0a64. Ces bits sont l'équivalent octet par octet de 172,16,10,100. Le pare-feu 6-to-4 traduit le serveur DNS IPv6 fc00::f:0:0:ac10:a64 en IPv4 équivalent 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
```



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.