

# FMCによって管理されるセキュアファイアウォールでのNAT 64の設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ネットワークオブジェクトの設定](#)

[FTDでのIPv4/IPv6用インターフェイスの設定](#)

[デフォルトルートの設定](#)

[NATポリシーの設定](#)

[NATルールの設定](#)

[検証](#)

## 概要

このドキュメントでは、Fire Power Management Center(FMC)によって管理されるFirepower脅威対策(FTD)でNAT64を設定する方法について説明します。

## 前提条件

### 要件

Secure Firewall Threat DefenseおよびSecure Firewall Management Centerに関する知識があることが推奨されます。

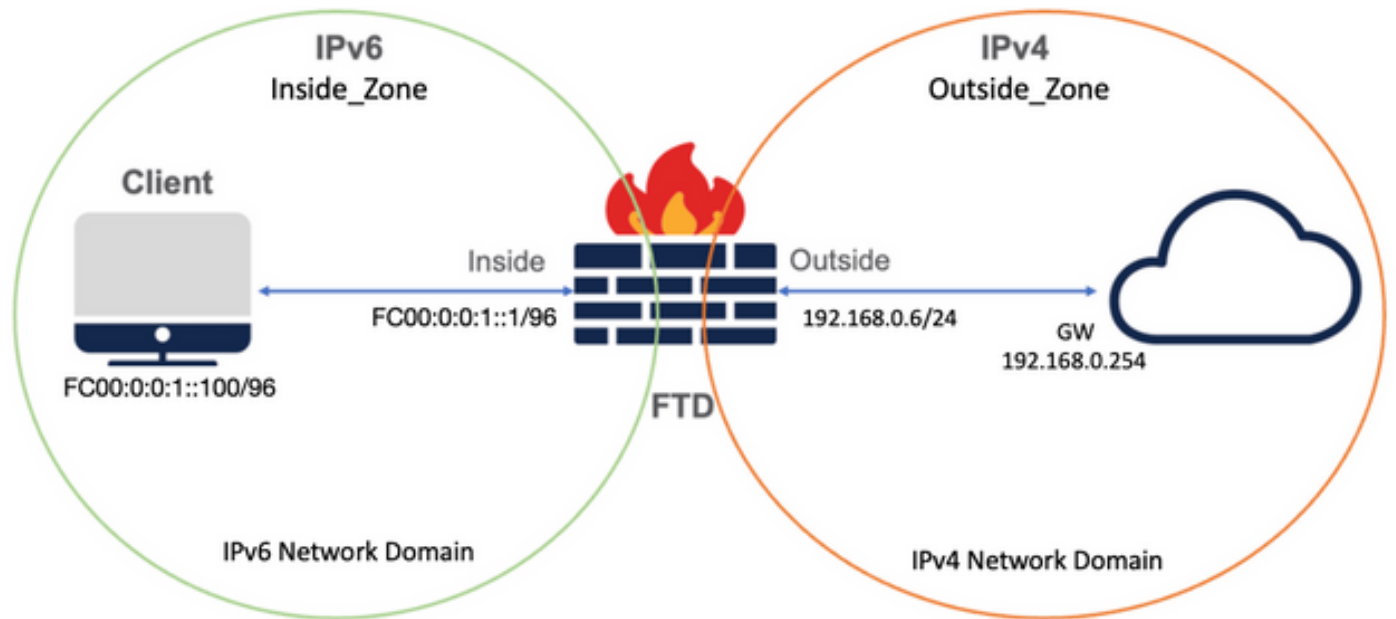
### 使用するコンポーネント

- Firepower Management Center 7.0.4
- Firepower脅威対策7.0.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

## ネットワーク図



## ネットワークオブジェクトの設定

- 内部IPv6クライアントサブネットを参照するIPv6ネットワークオブジェクト。

FMC GUIで、左のメニューからObjects > Object Management > Select Network > Add Network > Add Objectの順に移動します。

たとえば、ネットワークオブジェクトLocal\_IPv6\_subnetは、IPv6サブネットFC00:0:0:1::/96で作成されます。

## Edit Network Object ?

Name

Description

Network

Host    Range    Network    FQDN

Allow Overrides

- IPv4ネットワークオブジェクトを使用して、IPv6クライアントをIPv4に変換します。

FMC GUIで、左側のメニューからObjects > Object Management > Select Network > Add Network > Add Groupの順に移動します。

たとえば、ネットワークオブジェクト6\_mapped\_to\_4はIPv4ホスト192.168.0.107で作成されます。

IPv4でマッピングするIPv6ホストの量に応じて、単一のオブジェクトネットワーク、複数のIPv4を持つネットワークグループ、または出カインターフェイスへのNATだけを使用できます。

## 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

- インターネット上の外部IPv4ホストを参照するIPv4ネットワークオブジェクト。

FMC GUIで、左のメニューからObjects > Object Management > Select Network > Add Network > Add Objectの順に移動します。

たとえば、Network Object Any\_IPv4はIPv4サブネット0.0.0.0/0で作成されます。

## New Network Object ?

Name

Description

Network  
 Host    Range    Network    FQDN

Allow Overrides

- 外部IPv4ホストをIPv6ドメインに変換するIPv6ネットワークオブジェクト。

FMC GUIで、左メニューからObjects > Object Management > Select Network > Add Network > Add Objectに移動します。

たとえば、ネットワークオブジェクト4\_mapped\_to\_6はIPv6サブネットFC00:0:0:F::/96で作成されます。

## Edit Network Object ?

Name

Description

Network  
 Host    Range    Network    FQDN

Allow Overrides

### FTDでIPv4/IPv6用のインターフェイスを設定する

Devices > Device Management > Edit FTD > Interfacesの順に移動し、内部インターフェイスと外部インターフェイスを設定します。

以下に例を挙げます。

```
interface ethernet 1/1
```

名前 : Inside

セキュリティゾーン : Inside\_Zone

セキュリティゾーンが作成されていない場合は、Security Zoneドロップダウンメニュー→Newで作成できます。

IPv6アドレス : 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

名前：外部

セキュリティゾーン：Outside\_Zone

セキュリティゾーンが作成されていない場合は、Security Zoneドロップダウンメニュー→Newで作成できます。



IPv4アドレス : 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

## デフォルトルートの設定

Devices > Device Management > Edit FTD > Routing > Static Routing > Add Routeの順に移動します。

たとえば、ゲートウェイ192.168.0.254を持つ外部インターフェイス上のデフォルトスタティックルートです。

## 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

Firewall Management Center  
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

**FTD\_LAB**  
Cisco Firepower 1010 Threat Defense

Device Routing Interfaces Inline Sets DHCP SNMP

Manage Virtual Routers

Global

Virtual Router Properties

- ECMP
- BFD
- OSPF
- OSPFv3
- EIGRP
- RIP
- BGP
  - IPv4
  - IPv6
- Static Route

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

## NATポリシーの設定

FMC GUIで、Devices > NAT > New Policy > Threat Defense NATの順に移動し、NATポリシーを作成します。

たとえば、NATポリシーFTD\_NAT\_Policyが作成され、テストFTD FTD\_LABに割り当てられます。

### 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

## NATルールの設定

アウトバウンドNAT。

FMC GUIで、Devices > NAT > Select the NAT policy > Add Ruleの順に移動し、内部IPv6ネットワークを外部IPv4プールに変換するNATルールを作成します。

たとえば、ネットワークオブジェクトLocal\_IPv6\_subnetは、ネットワークオブジェクト6\_mapped\_to\_4に動的に変換されます。

NATルール：自動NATルール

タイプ：ダイナミック

送信元インターフェイスオブジェクト：Inside\_Zone

宛先インターフェイスオブジェクト : Outside\_Zone

元の送信元 : Local\_IPv6\_subnet

変換済みソース : 6\_mapped\_to\_4

**Edit NAT Rule**

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

Enable

Interface Objects   Translation   PAT Pool   Advanced

Available Interface Objects   Search by name

- 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	Translated Packet
Original Source:* <span style="border: 1px solid #ccc; padding: 2px;">Local_IPv6_subnet</span> +	Translated Source: <span style="border: 1px solid #ccc; padding: 2px;">Address</span>
Original Port: <span style="border: 1px solid #ccc; padding: 2px;">TCP</span> <input style="width: 100%; height: 20px;" type="text"/>	Translated Port: <span style="border: 1px solid #ccc; padding: 2px;">6_mapped_to_4</span> + <input style="width: 100%; height: 20px;" type="text"/>

Cancel
OK

インバウンドNAT。

FMC GUIで、Devices > NAT > Select the NAT policy > Add Ruleの順に移動し、外部IPv4トラフィックを内部IPv6ネットワークプールに変換するNATルールを作成します。これにより、ローカルIPv6サブネットとの内部通信が可能になります。

さらに、外部DNSサーバからの応答をA(IPv4)レコードからAAAA(IPv6)レコードに変換できるように、このルールでDNS書き換えを有効にします。

たとえば、外部ネットワークAny\_IPv4は、オブジェクト4\_mapped\_to\_6で定義されたIPv6サブネット2100:6400::/96に静的に変換されます。

NATルール：自動NATルール

タイプ：スタティック

送信元インターフェイスオブジェクト：Outside\_Zone

宛先インターフェイスオブジェクト : Inside\_Zone

元の送信元 : Any\_IPv4

翻訳済みソース : 4\_mapped\_to\_6

このルールに一致するDNS応答を変換する : はい ( チェックボックスをオンにする )

**Edit NAT Rule**

NAT Rule:  
Auto NAT Rule

Type:  
Static

Enable

Interface Objects   Translation   PAT Pool   Advanced

Available Interface Objects   Search by name

- 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

Original Source:\*

any\_IPv4 +

Original Port:

TCP

Translated Packet

Translated Source:

Address

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

Rules Policy Assignments (1)

Filter by Device  Filter Rules

#	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	<input type="button" value="edit"/>
#	↔	Dyna...	Inside_Zone	Outside_Zone	Local_IPv6_subnet			6_mapped_to_4			Dns:false	<input type="button" value="edit"/>
NAT Rules After												

FTDへの変更の導入に進みます。

## 検証

- インターフェイス名とIP設定を表示します。

<#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
```

- FTD内部インターフェイスからクライアントへのIPv6接続を確認します。

IPv6内部ホストIP fc00:0:0:1::100。

FTD内部インターフェイス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

- FTD CLIでNAT設定を表示します。

```
<#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
```

- トラフィックのキャプチャ.

たとえば、内部IPv6ホストfc00:0:0:1::100からDNSサーバへのキャプチャトラフィックは、fc00::f:0:0:ac10:a64 UDP 53です。

ここでは、宛先DNSサーバはfc00::f:0:0:ac10:a64です。最後の32ビットはac10:0a64です。これらのビットは、オクテット単位で172、16、10、100に相当します。ファイアウォール6-to-4は、IPv6 DNSサーバfc00::f:0:0:ac10:a64を同等のIPv4 172.16.10.100に変換します。

```
<#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
```



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。