

Configure NAT 64 on Secure Firewall Managed by FMC

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Network Diagram](#)
[Configure Network Objects](#)
[Configure Interfaces on FTD for IPv4/IPv6](#)
[Configure Default Route](#)
[Configure NAT policy](#)
[Configure NAT rules](#)
[Verification](#)

Introduction

This document describes how to configure NAT64 on Firepower Threat Defense (FTD) managed by Fire Power Management Center (FMC).

Prerequisites

Requirements

Cisco recommends that you have knowledge about Secure Firewall Threat Defense and Secure Firewall Management Center.

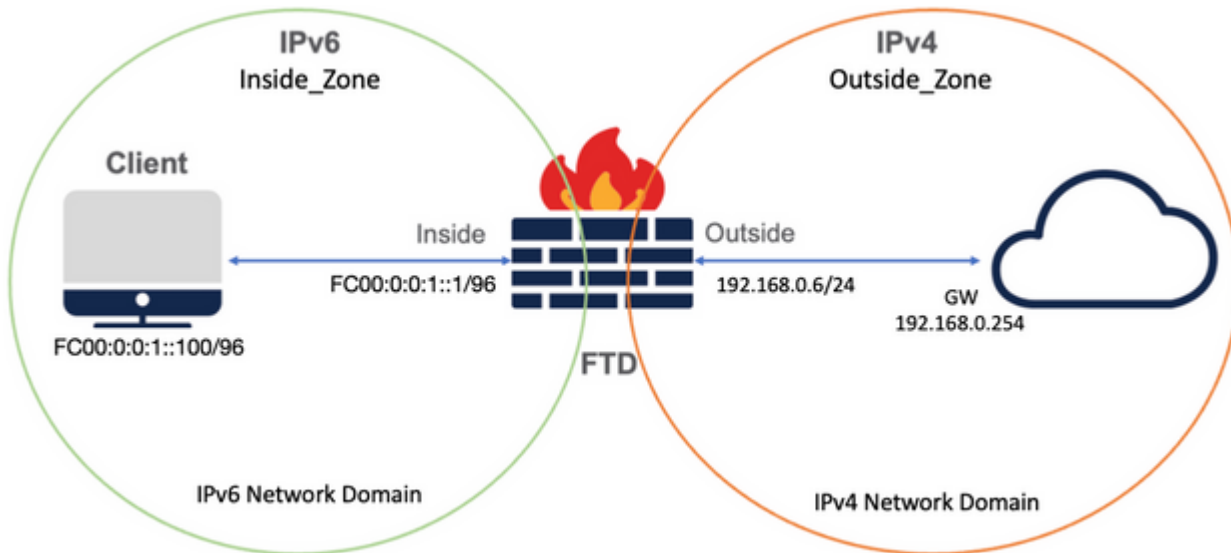
Components Used

- Firepower Management Center 7.0.4.
- Firepower Threat Defense 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. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configure Network Objects

- IPv6 Network Object to reference the internal IPv6 client subnet.

On FMC GUI, navigate to **Objects > Object Management > Select Network from left Menu > Add Network > Add Object**.

For example, Network Object Local_IPv6_subnet is created with the IPv6 subnet FC00:0:0:1::/96.

Edit Network Object ?

Name

Description

Network
 Host Range Network FQDN

Allow Overrides

- IPv4 Network Object to translate IPv6 clients to IPv4.

On FMC GUI, navigate to **Objects > Object Management > Select Network from left Menu > Add Network > Add Group**.

For example, Network Object 6_mapped_to_4 is created with the IPv4 host 192.168.0.107.

Depending on the amount of IPv6 hosts to map in IPv4, you can use a single object network, a network group with multiple IPv4, or just NAT to the egress interface.

The screenshot shows the 'New Network Group' configuration window. The 'Name' field is filled with '6_mapped_to_4'. The 'Description' field is empty. The 'Allow Overrides' checkbox is unchecked. The 'Available Networks' list on the left includes '6_mapped_to_4', 'any_IPv4', 'Any_ipv6', 'google_dns_ipv4', 'google_dns_ipv4_group', and 'google_dns_ipv6'. The 'Selected Networks' list on the right contains '192.168.0.107'. There are 'Add' buttons between the lists and at the bottom right of the 'Selected Networks' list. At the bottom of the window are 'Cancel' and 'Save' buttons.

- IPv4 Network Object to reference the external IPv4 hosts on the Internet.

On FMC GUI, navigate to **Objects > Object Management > Select Network from left Menu > Add Network > Add Object**.

For example, Network Object Any_IPv4 is created with the IPv4 subnet 0.0.0.0/0.

New Network Object

Name
Any_IPv4

Description

Network
 Host Range Network FQDN

0.0.0.0/0

Allow Overrides

Cancel Save

- IPv6 Network Object to translate external IPv4 host into our IPv6 domain.

On FMC GUI, navigate to **Objects > Object Management > Select Network from left Menu > Add Network > Add Object**.

For example, Network Object 4_mapped_to_6 is created with the IPv6 subnet 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

Cancel Save

Configure Interfaces on FTD for IPv4/IPv6

Navigate to **Devices > Device Management > Edit FTD > Interfaces** and configure Inside and Outside

interfaces.

Example:

Interface Ethernet 1/1

Name: Inside

Security Zone: Inside_Zone

If security zone is not created, you can create it in the **Security Zone drop-down menu > New**.

IPv6 Address: FC00:0:0:1::1/96

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

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

Name: Outside

Security Zone: Outside_Zone

If security zone is not created, you can create it in the **Security Zone drop-down menu > New**.

IPv4 Address: 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:

IP Address:

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Configure Default Route


Navigate to **Devices > Device Management > Edit FTD > Routing > Static Routing > Add Route**.


For example, default static route on the outside interface with 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  +

Search

- 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

Overview Analysis Policies **Devices** Objects Integration

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
IPv4 Routes					
any-ipv4	Outside	Global	192.168.0.254	false	1
IPv6 Routes					

Configure NAT policy

On the FMC GUI, navigate to **Devices > NAT > New Policy > Threat Defense NAT** and create a NAT policy.

For example, NAT policy FTD_NAT_Policy is created and assigned to the test FTD FTD_LAB.

New Policy

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Q Search by name or value

FTD_LAB

Add to Policy

Selected Devices

FTD_LAB

Cancel Save

Configure NAT rules

Outbound NAT.

On the FMC GUI, navigate to **Devices > NAT > Select the NAT policy > Add Rule** and create NAT rule to translate Internal IPv6 network to external IPv4 pool.

For example, Network Object Local_IPv6_subnet is dynamically translated to Network Object 6_mapped_to_4.

NAT Rule: Auto NAT rule

Type: Dynamic

Source Interface Objects: Inside_Zone

Destination Interface Objects: Outside_Zone

Original Source: Local_IPv6_subnet

Translated Source: 6_mapped_to_4

Edit NAT Rule

NAT Rule:

Type:

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- Group_Inside
- Group_Outside
- Inside_Zone
- Outside_Zone

Source Interface Objects (1)

Destination Interface Objects (1)

Edit NAT Rule

NAT Rule:

Type:

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* +

Original Port:

Translated Packet

Translated Source:

Translated Port: +

Inbound NAT.

On the FMC GUI, navigate to **Devices > NAT > Select the NAT policy > Add Rule** and create NAT rule to translate external IPv4 traffic to Internal IPv6 network pool. This allows internal communication with your local IPv6 subnet.

Additionally, enable DNS rewrite on this rule so that replies from the external DNS server can be converted from A (IPv4) to AAAA (IPv6) records.

For example, Outside Network Any_IPv4 is statically translated to IPv6 subnet 2100:6400::/96 defined in the object 4_mapped_to_6.

NAT rule: Auto NAT Rule

Type: Static

Source Interface Objects: Outside_Zone

Destination Interface Objects: Inside_Zone

Original Source: Any_IPv4

Translated Source: 4_mapped_to_6

Translate DNS replies that match this rule: Yes (Enable checkbox)

The screenshot shows the 'Edit NAT Rule' configuration window. At the top, the 'NAT Rule' is set to 'Auto NAT Rule' and the 'Type' is 'Static'. The 'Enable' checkbox is checked. Below this, there are four tabs: 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Interface Objects' tab is selected. It contains three main sections: 'Available Interface Objects' on the left, 'Source Interface Objects' in the middle, and 'Destination Interface Objects' on the right. The 'Available Interface Objects' section has a search bar and a list of objects: 'Group_Inside', 'Group_Outside', 'Inside_Zone', and 'Outside_Zone'. The 'Source Interface Objects' section contains 'Outside_Zone'. The 'Destination Interface Objects' section contains 'Inside_Zone'. There are 'Add to Source' and 'Add to Destination' buttons between the available and source/destination lists. At the bottom right, there are 'Cancel' and 'OK' buttons.

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: Auto NAT Rule

Type: Static

Enable

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Falthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Cancel OK

FTD_NAT_Policy

Enter Description

Rules

Filter by Device Filter Rules

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translate Sources
					Original Sources	Original Destinations	Original Services	
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								

Proceed to deploy changes to FTD.

Verification

- Display interface names and IP configuration.

```
<#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
```

- Confirm IPv6 connectivity from FTD inside interface to client.

IPv6 internal 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
```

- Display NAT configuration on the FTD CLI.

```
<#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
```

- Capture traffic.

For example, capture traffic from internal IPv6 host fc00:0:0:1::100 to DNS server is fc00::f:0:0:ac10:a64

UDP 53.

Here, the destination DNS server is fc00::f:0:0:ac10:a64. The last 32 bits are ac10:0a64. These bits are the octet-by-octet equivalent to 172,16,10,100. Firewall 6-to-4 translates IPv6 DNS server fc00::f:0:0:ac10:a64 to the equivalent 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
```