

Configure o NAT 64 no firewall seguro gerenciado pelo FMC

Contents

- [Introdução](#)
- [Pré-requisitos](#)
- [Requisitos](#)
- [Componentes Utilizados](#)
- [Configurar](#)
- [Diagrama de Rede](#)
- [Configurar objetos de rede](#)
- [Configurar interfaces em FTD para IPv4/IPv6](#)
- [Configurar Rota Padrão](#)
- [Configurar NATpolicy](#)
- [Configurar regras de NAT](#)
- [Verificação](#)

Introdução

Este documento descreve como configurar o NAT64 no Firepower Threat Defense (FTD) gerenciado pelo Fire Power Management Center (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre o Secure Firewall Threat Defense e o Secure Firewall Management Center.

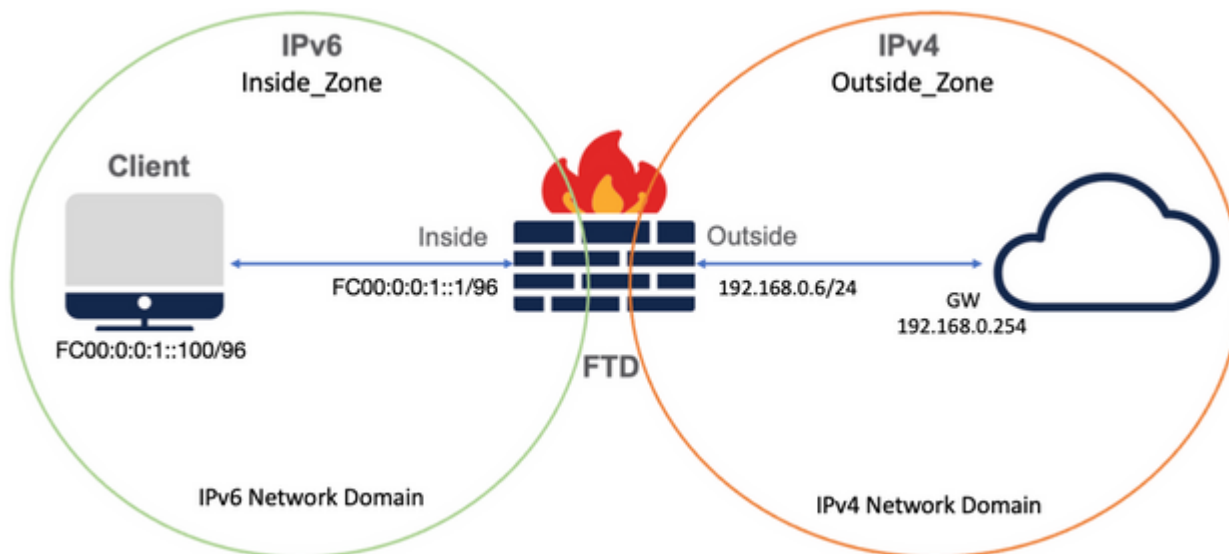
Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Configurar objetos de rede

- Objeto de Rede IPv6 para fazer referência à sub-rede interna do cliente IPv6.

Na GUI do FMC, navegue até **Objetos > Gerenciamento de objetos > Selecionar rede no menu à esquerda > Adicionar rede > Adicionar objeto**.

Por exemplo, o objeto de rede Local_IPv6_subnet é criado com a sub-rede IPv6 FC00:0:0:1::/96.

The screenshot shows the 'Edit Network Object' configuration window. The 'Name' field contains 'Local_IPv6_subnet'. The 'Description' field is empty. Under the 'Network' section, the 'Network' radio button is selected, and the IP address 'FC00:0:0:1::/96' is entered in the text box. The 'Allow Overrides' checkbox is unchecked. At the bottom, there are 'Cancel' and 'Save' buttons.

- Objeto de Rede IPv4 para converter clientes IPv6 em IPv4.

Na GUI do FMC, navegue até **Objetos > Gerenciamento de objetos > Selecionar rede no menu à esquerda > Adicionar rede > Adicionar grupo**.

Por exemplo, o Objeto de Rede 6_mapped_to_4 é criado com o host IPv4 192.168.0.107.

Dependendo da quantidade de hosts IPv6 para mapear em IPv4, você pode usar uma rede de objeto único, um grupo de rede com vários IPv4 ou apenas NAT para a interface de saída.

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' pane shows a list of network objects, including '6_mapped_to_4', 'any_IPv4', 'Any_ipv6', 'google_dns_ipv4', 'google_dns_ipv4_group', and 'google_dns_ipv6'. The 'Selected Networks' pane shows the IP address '192.168.0.107'. The 'Add' button is located between the two panes, and another 'Add' button is located below the 'Selected Networks' pane. The 'Cancel' and 'Save' buttons are at the bottom of the window.

- Objeto de Rede IPv4 para fazer referência a hosts IPv4 externos na Internet.

Na GUI do FMC, navegue até **Objetos > Gerenciamento de objetos > Selecionar rede no menu à esquerda > Adicionar rede > Adicionar objeto**.

Por exemplo, o objeto de rede Any_IPv4 é criado com a sub-rede 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

Cancel Save

- Objeto de Rede IPv6 para converter o host IPv4 externo em nosso domínio IPv6.

Na GUI do FMC, navegue até **Objetos > Gerenciamento de objetos > Selecionar rede no menu à esquerda > Adicionar rede > Adicionar objeto**.

Por exemplo, o Objeto de Rede 4_mapped_to_6 é criado com a sub-rede 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

Cancel Save

Configurar interfaces em FTD para IPv4/IPv6

Navegue até **Devices > Device Management > Edit FTD > Interfaces** e configure interfaces internas e

externas.

Exemplo:

interface ethernet 1/1

Nome: Dentro

Zona de segurança: Inside_Zone

Se a zona de segurança não for criada, você poderá criá-la no **menu suspenso Zona de segurança > Novo**.

Endereço IPv6: 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:

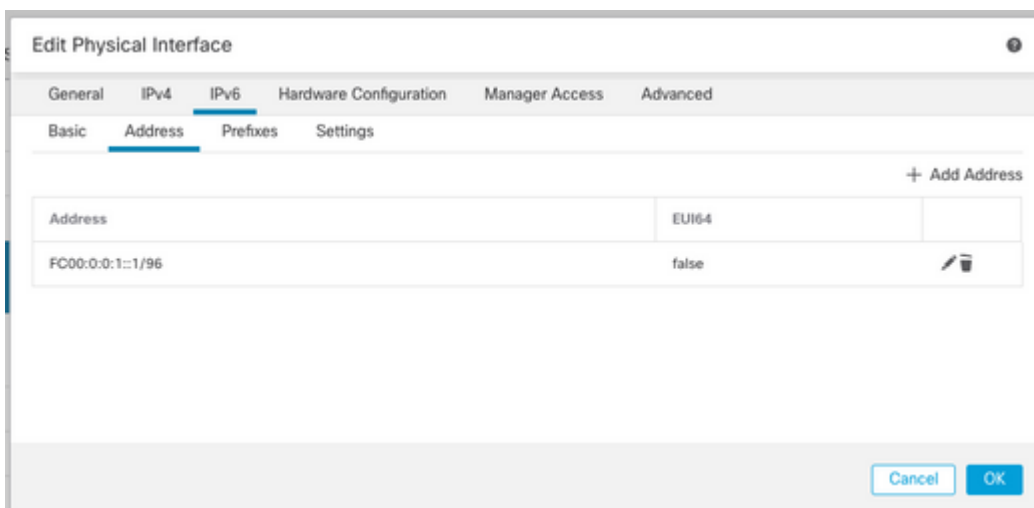
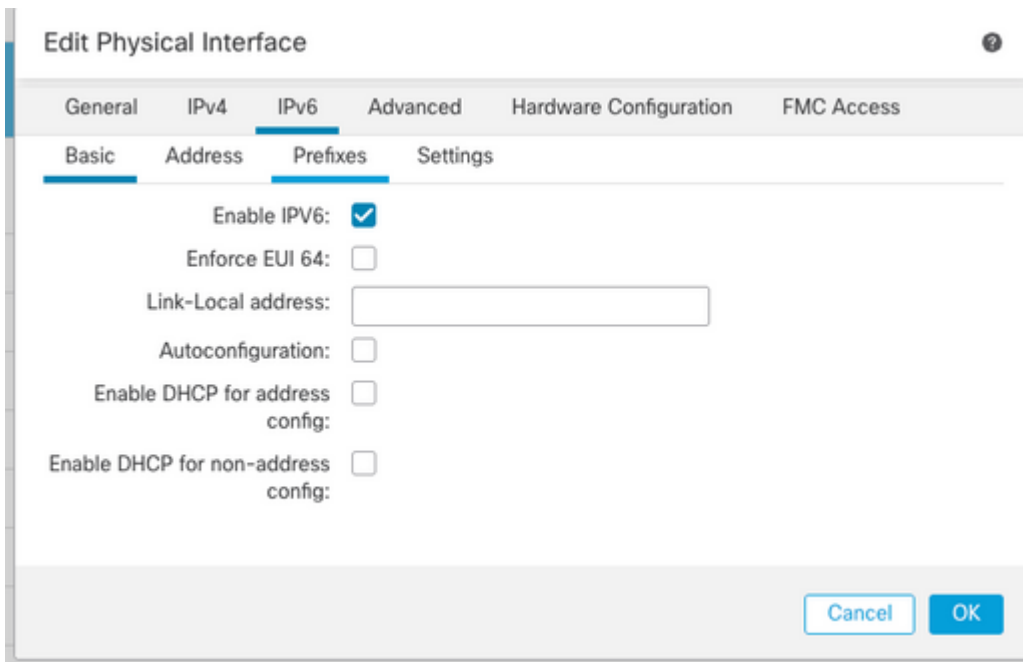
Interface ID:

MTU:

(64 - 9198)

Propagate Security Group Tag:

Cancel OK



interface ethernet 1/2

Nome: Externo

Zona de segurança: Outside_Zone

Se a zona de segurança não for criada, você poderá criá-la no **menu suspenso Zona de segurança > Novo**.

Endereço IPv4: 192.168.0.106/24

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration FMC Access

Name:
Outside

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
Outside_Zone

Interface ID:
Ethernet1/2

MTU:
1500
(64 - 9198)

Propagate Security Group Tag:

Cancel OK

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

Configurar Rota Padrão


Navegue até **Devices > Device Management > Edit FTD > Routing > Static Routing > Add Route**.


Por exemplo, a rota estática padrão na interface externa com o 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					

Configurar a política de NAT

Na GUI do FMC, navegue para **Devices > NAT > New Policy > Threat Defense NAT** e crie uma política de NAT.

Por exemplo, a política de NAT **FTD_NAT_Policy** é criada e atribuída ao teste **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

Configurar regras de NAT

NAT de saída.

Na GUI do FMC, navegue para **Devices > NAT > Select the NAT policy > Add Rule** e crie uma regra NAT para converter a rede IPv6 interna para o pool IPv4 externo.

Por exemplo, o objeto de rede `Local_IPv6_subnet` é convertido dinamicamente para o objeto de rede `6_mapped_to_4`.

Regra NAT: regra NAT automática

Tipo: Dinâmico

Objetos da interface de origem: `Inside_Zone`

Objetos de interface de destino: `Outside_Zone`

Origem Original: `Local_IPv6_subnet`

Origem Convertida: `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: 6_mapped_to_4 +

Cancel OK

NAT de entrada.

Na GUI do FMC, navegue para **Devices > NAT > Select the NAT policy > Add Rule** e crie uma regra NAT para converter o tráfego IPv4 externo para o pool de rede IPv6 interno. Isso permite a comunicação interna com a sub-rede IPv6 local.

Além disso, habilite a regravação de DNS nesta regra para que as respostas do servidor DNS externo possam ser convertidas de registros A (IPv4) para registros AAAA (IPv6).

Por exemplo, Outside Network Any_IPv4 é convertido estaticamente para a sub-rede IPv6 2100:6400::/96 definida no objeto 4_mapped_to_6.

Regra NAT: regra NAT automática

Tipo: estático

Objetos da interface de origem: Outside_Zone

Objetos da interface de destino: Inside_Zone

Fonte original: Any_IPv4

Origem Convertida: 4_mapped_to_6

Traduzir respostas DNS que correspondam a esta regra: Sim (caixa de seleção Habilitar)

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 active, showing three columns: 'Available Interface Objects', 'Source Interface Objects', and 'Destination Interface Objects'. The 'Available Interface Objects' list includes 'Group_Inside', 'Group_Outside', 'Inside_Zone', and 'Outside_Zone'. The 'Source Interface Objects' column contains 'Outside_Zone' and the 'Destination Interface Objects' column contains 'Inside_Zone'. There are 'Add to Source' and 'Add to Destination' buttons between the columns. 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:

Type:

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

FTD_NAT_Policy
Enter Description

Rules

[Filter by Device](#)

#	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								

Continue a implantar as alterações no FTD.

Verificação

- Exiba os nomes das interfaces e a configuração 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 a conectividade IPv6 da interface interna do FTD com o cliente.

IPv6 host interno fc00:0:0:1::100.

FTD Interface 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

- Exiba a configuração do NAT na CLI do 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 tráfego.

Por exemplo, o tráfego de captura do host IPv6 interno fc00:0:0:1::100 para o servidor DNS é

fc00::f:0:0:ac10:a64 UDP 53.

Aqui, o servidor DNS de destino é fc00::f:0:0:ac10:a64. Os últimos 32 bits são ac10:0a64. Esses bits são o equivalente octeto por octeto a 172,16,10,100. O Firewall 6-to-4 converte o servidor DNS IPv6 fc00::f:0:0:ac10:a64 para o IPv4 172.16.10.100 equivalente.

```
<#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
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.