

Configurazione di NAT 64 su Secure Firewall gestito da FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configura oggetti di rete](#)

[Configurazione delle interfacce su FTD per IPv4/IPv6](#)

[Configura route predefinita](#)

[Configura NATpolicy](#)

[Configura regole NAT](#)

[Verifica](#)

Introduzione

Questo documento descrive come configurare NAT64 su Firepower Threat Defense (FTD) gestito da Fire Power Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Secure Firewall Threat Defense e Secure Firewall Management Center.

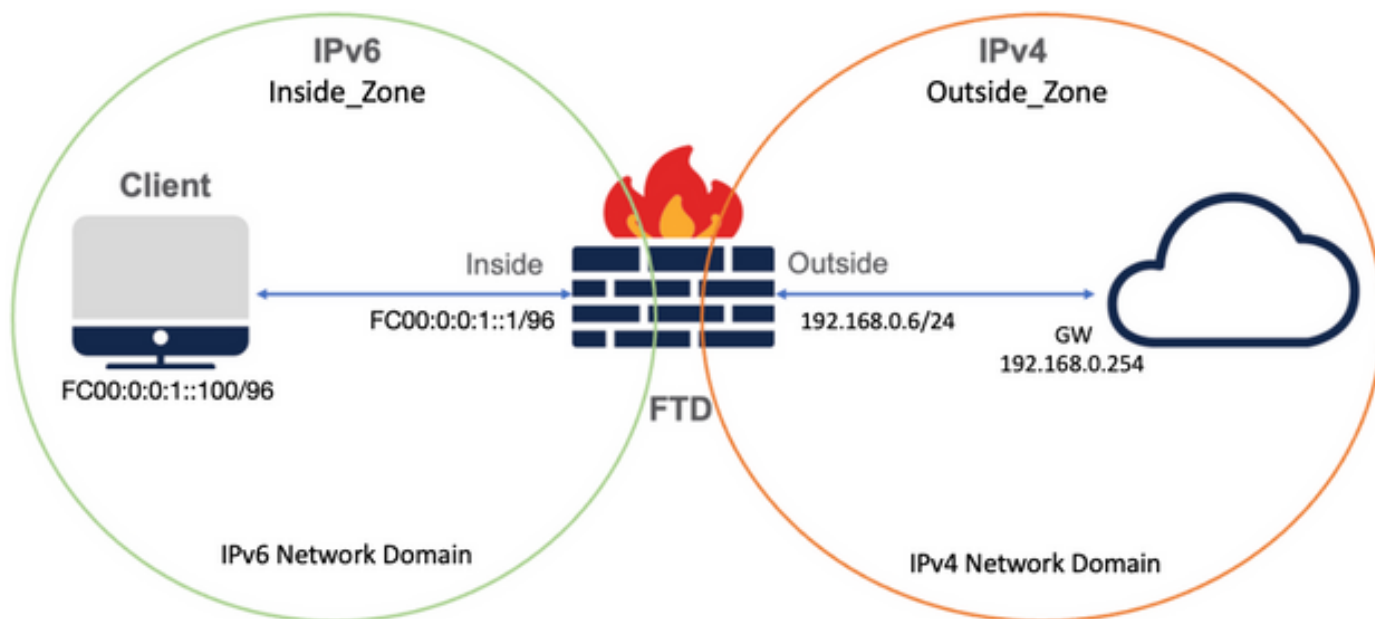
Componenti usati

- Firepower Management Center 7.0.4.1
- Firepower Threat Defense 7.0.4.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configura oggetti di rete

- Oggetto di rete IPv6 per fare riferimento alla subnet client IPv6 interna.

Nell'interfaccia utente di FMC, selezionare Oggetti > Gestione oggetti > Seleziona rete dal menu a sinistra > Aggiungi rete > Aggiungi oggetto.

Ad esempio, l'oggetto di rete `Local_IPv6_subnet` viene creato con la subnet IPv6 `FC00:0:0:1::/96`.

Edit Network Object ?

Name

Description

Network

Host Range Network FQDN

Allow Overrides

- Oggetto di rete IPv4 per convertire i client IPv6 in IPv4.

Dalla GUI di FMC, selezionare Oggetti > Gestione oggetti > Seleziona rete dal menu a sinistra > Aggiungi rete > Aggiungi gruppo.

Ad esempio, l'oggetto di rete 6_mapped_to_4 viene creato con l'host IPv4 192.168.0.107.

A seconda della quantità di host IPv6 da mappare in IPv4, è possibile utilizzare una rete a oggetto singolo, un gruppo di rete con più IPv4 o solo NAT per l'interfaccia in uscita.

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

- Oggetto di rete IPv4 per fare riferimento agli host IPv4 esterni su Internet.

Nell'interfaccia utente di FMC, selezionare Oggetti > Gestione oggetti > Seleziona rete dal menu a sinistra > Aggiungi rete > Aggiungi oggetto.

Ad esempio, l'oggetto di rete Any_IPv4 viene creato con la subnet IPv4 0.0.0.0/0.

New Network Object ?

Name

Description

Network
 Host Range Network FQDN

Allow Overrides

- Oggetto di rete IPv6 per convertire l'host IPv4 esterno nel dominio IPv6.

Dalla GUI di FMC, selezionare Oggetti > Gestione oggetti > Seleziona rete dal menu a sinistra > Aggiungi rete > Aggiungi oggetto.

Ad esempio, l'oggetto di rete 4_mapped_to_6 viene creato con la subnet IPv6 FC00:0:0:F::/96.

Edit Network Object ?

Name

Description

Network
 Host Range Network FQDN

Allow Overrides

Configurazione delle interfacce su FTD per IPv4/IPv6

Selezionare Dispositivi > Gestione dispositivi > Modifica FTD > Interfacce e configurare le interfacce interne ed esterne.

Esempio:

Interfaccia Ethernet 1/1

Nome: Interno

Area di protezione: Inside_Zone

Se l'area di protezione non viene creata, è possibile crearla nel menu a discesa Area di protezione > Nuovo.

Indirizzo 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

Interfaccia Ethernet 1/2

Nome: Esterno

Area di sicurezza: Outside_Zone

Se l'area di protezione non viene creata, è possibile crearla nel menu a discesa Area di protezione > Nuovo.

Indirizzo 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

Configura route predefinita

Selezionare Dispositivi > Gestione dispositivi > Modifica FTD > Ciclo > Ciclo statico > Aggiungi ciclo.

Ad esempio, il percorso statico predefinito sull'interfaccia esterna è il 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

Add

Selected Network

any-ipv4

6_mapped_to_4

any-ipv4

any_IPv4

google_dns_ipv4

google_dns_ipv4_group

google_dns_ipv6_group

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						

Configura criterio NAT

Dalla GUI del FMC, selezionare Devices > NAT > New Policy > Threat Defense NAT e creare una policy NAT.

Ad esempio, il criterio NAT FTD_NAT_Policy viene creato e assegnato all'FTD FTD_LAB di test.

New Policy

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTD_LAB

Selected Devices

FTD_LAB

Configura regole NAT

NAT in uscita.

Nell'interfaccia utente di FMC, selezionare Dispositivi > NAT > Selezionare il criterio NAT > Aggiungi regola e creare la regola NAT per convertire la rete IPv6 interna in un pool IPv4 esterno.

Ad esempio, l'oggetto di rete Local_IPv6_subnet viene convertito dinamicamente in Oggetto di rete 6_mapped_to_4.

Regola NAT: regola NAT automatica

Tipo: dinamico

Oggetti interfaccia di origine: Inside_Zone

Oggetti interfaccia di destinazione: Outside_Zone

Origine originale: Local_IPv6_subnet

Origine tradotta: 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:* <div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;">Local_IPv6_subnet</div> <div style="margin: 0 5px;">+</div> </div>	Translated Source: <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;">Address</div>
Original Port: <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;">TCP</div>	Translated Port: <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;">6_mapped_to_4</div>
<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>

Cancel

OK

NAT in entrata.

Nell'interfaccia utente di FMC, selezionare Dispositivi > NAT > Selezionare il criterio NAT > Aggiungi regola e creare la regola NAT per convertire il traffico IPv4 esterno nel pool di rete IPv6 interno. Ciò consente la comunicazione interna con la subnet IPv6 locale.

Abilitare inoltre la riscrittura DNS in questa regola in modo che le risposte dal server DNS esterno possano essere convertite dai record A (IPv4) a AAAA (IPv6).

Ad esempio, la subnet Any_IPv4 della rete esterna viene convertita in modo statico nella subnet IPv6 2100:6400::/96 definita nell'oggetto 4_mapped_to_6.

Regola NAT: regola NAT automatica

Tipo: statico

Oggetti interfaccia di origine: Outside_Zone

Oggetti interfaccia di destinazione: Inside_Zone

Originale: Any_IPv4

Origine tradotta: 4_mapped_to_6

Traduci le risposte DNS che soddisfano questa regola: Sì (casella di controllo Abilita)

The screenshot shows the 'Edit NAT Rule' configuration window. At the top, the title is 'Edit NAT Rule'. Below the title, there are several configuration options:

- NAT Rule:** A dropdown menu set to 'Auto NAT Rule'.
- Type:** A dropdown menu set to 'Static'.
- Enable:** A checked checkbox.

Below these options are four tabs: 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Interface Objects' tab is selected and highlighted.

The 'Interface Objects' tab contains three main sections:

- Available Interface Objects:** A list of objects with a search bar above it. The search bar contains the text 'Search by name'. The list includes: Group_Inside, Group_Outside, Inside_Zone, and Outside_Zone. There are two buttons: 'Add to Source' and 'Add to Destination'.
- Source Interface Objects:** A box containing one object: 'Outside_Zone'. It has a trash icon to its right and a '(1)' count above it.
- Destination Interface Objects:** A box containing one object: 'Inside_Zone'. It has a trash icon to its right and a '(1)' count above it.

At the bottom right of the window, there are two buttons: 'Cancel' and '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												

Continuare a distribuire le modifiche a FTD.

Verifica

- Visualizza i nomi delle interfacce e la configurazione 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
```

- Confermare la connettività IPv6 da FTD all'interno dell'interfaccia al client.

Host interno IPv6 IP fc00:0:1::100.

FTD Interfaccia 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
```

- Visualizzare la configurazione NAT sulla 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
```

- Acquisire il traffico.

Ad esempio, il traffico di acquisizione dall'host IPv6 interno fc00:0:0:1::100 al server DNS è fc00::f:0:0:ac10:a64 UDP 53.

Il server DNS di destinazione è fc00::f:0:0:ac10:a64. Gli ultimi 32 bit sono ac10:0a64. Questi bit sono l'equivalente ottetto per ottetto di 172,16,10,100. Il firewall 6-4 converte il server DNS IPv6 fc00::f:0:0:ac10:a64 nell'equivalente 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
```


Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).