

Konfigurieren von NAT 64 auf einer von FMC verwalteten sicheren Firewall

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Konfigurieren](#)
- [Netzwerkdiagramm](#)
- [Netzwerkobjekte konfigurieren](#)
- [FTD-Schnittstellen für IPv4/IPv6 konfigurieren](#)
- [Standard-Route konfigurieren](#)
- [Konfigurieren der NAT-Richtlinie](#)
- [NAT-Regeln konfigurieren](#)
- [Verifizierung](#)

Einleitung

In diesem Dokument wird die Konfiguration von NAT64 für FirePOWER Threat Defense (FTD) erläutert, die vom Fire Power Management Center (FMC) verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse über Secure Firewall Threat Defense und Secure Firewall Management Center verfügen.

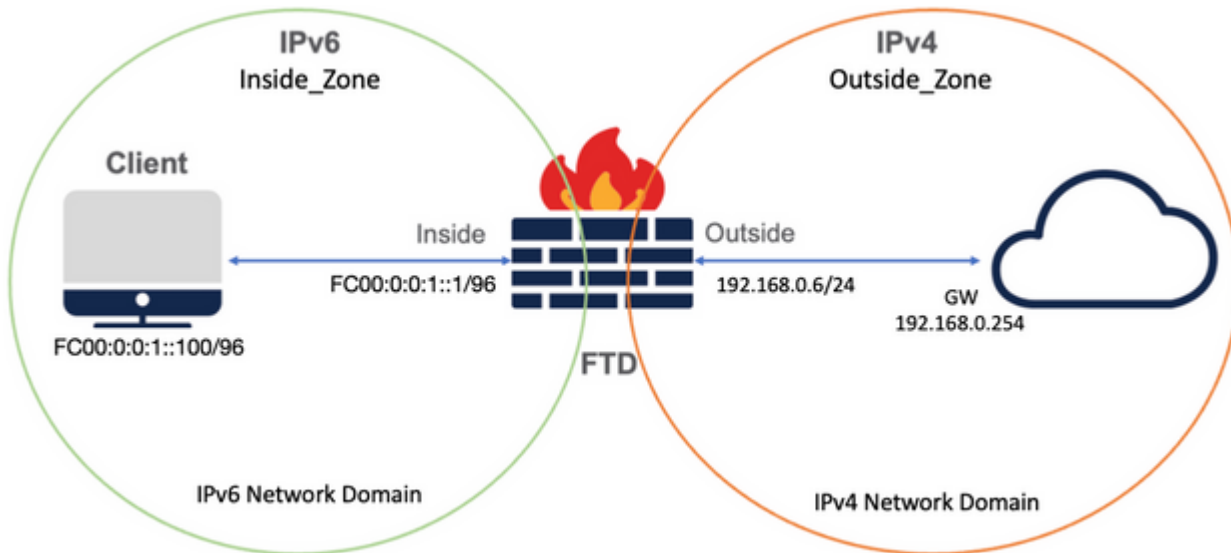
Verwendete Komponenten

- Firepower Management Center 7.0.4
- Firepower Threat Defense 7.0.4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Netzwerkobjekte konfigurieren

- IPv6-Netzwerkobjekt, das auf das interne IPv6-Client-Subnetz verweist.

Navigieren Sie in der FMC-GUI zu **Objekte > Objektverwaltung > Netzwerk auswählen aus dem Menü links > Netzwerk hinzufügen > Objekt hinzufügen**.

Beispielsweise wird das Netzwerkobjekt Local_IPv6_subnet mit dem IPv6-Subnetz FC00:0:0:1::/96 erstellt.

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 'Network' field contains 'FC00:0:0:1::/96'. The 'Allow Overrides' checkbox is unchecked. At the bottom, there are 'Cancel' and 'Save' buttons.

- IPv4-Netzwerkobjekt, um IPv6-Clients in IPv4 zu übersetzen.

Navigieren Sie in der FMC-GUI zu **Objekte > Objektverwaltung > Netzwerk auswählen aus dem Menü links > Netzwerk hinzufügen > Gruppe hinzufügen**.

Beispielsweise wird das Netzwerkobjekt 6_mapped_to_4 mit dem IPv4-Host 192.168.0.107 erstellt.

Je nach Anzahl der IPv6-Hosts, die in IPv4 zugeordnet werden müssen, können Sie ein einzelnes Objektnetzwerk, eine Netzwerkgruppe mit mehreren IPv4-Hosts oder nur NAT für die Ausgangsschnittstelle verwenden.

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 contains several options, with '6_mapped_to_4' selected. The 'Selected Networks' list contains the IP address '192.168.0.107'. An 'Add' button is located between the two lists. At the bottom right, there are 'Cancel' and 'Save' buttons.

- IPv4-Netzwerkobjekt, das auf die externen IPv4-Hosts im Internet verweist.

Navigieren Sie in der FMC-GUI zu **Objekte > Objektverwaltung > Netzwerk auswählen aus dem Menü links > Netzwerk hinzufügen > Objekt hinzufügen**.

Beispielsweise wird das Netzwerkobjekt Any_IPv4 mit dem IPv4-Subnetz 0.0.0.0/0 erstellt.

- IPv6 Network Object zur Übersetzung eines externen IPv4-Hosts in unsere IPv6-Domäne.

Navigieren Sie in der FMC-GUI zu **Objekte > Objektverwaltung > Netzwerk auswählen aus dem Menü links > Netzwerk hinzufügen > Objekt hinzufügen**.

Beispielsweise wird das Netzwerkobjekt 4_mapped_to_6 mit dem IPv6-Subnetz FC00:0:0:F::/96 erstellt.

Konfigurieren von Schnittstellen auf FTD für IPv4/IPv6

Navigieren Sie zu **Devices (Geräte) > Device Management (Geräteverwaltung) > Edit FTD (FTD**

bearbeiten) > **Interfaces (Schnittstellen)**, und konfigurieren Sie Inside (Interne) und Outside Interfaces (Externe Schnittstellen).

Beispiel:

Schnittstelle Ethernet 1/1

Name: Innenbereich

Sicherheitszone: Inside_Zone

Wenn keine Sicherheitszone erstellt wird, können Sie sie im **Dropdown-Menü Sicherheitszone > Neu** erstellen.

IPv6-Adresse: 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

Schnittstelle Ethernet 1/2

Name: Außenbereich

Sicherheitszone: Outside_Zone

Wenn keine Sicherheitszone erstellt wird, können Sie sie im **Dropdown-Menü Sicherheitszone > Neu** erstellen.

IPv4-Adresse: 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

Standard-Route konfigurieren


Navigieren Sie zu **Devices (Geräte) > Device Management (Geräteverwaltung) > Edit FTD (FTD bearbeiten) > Routing (Routing) > Static Routing (Statisches Routing) > Add Route (Route hinzufügen)**.


Beispielsweise statische Standardroute an der externen Schnittstelle mit 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					

Konfigurieren der NAT-Richtlinie

Navigieren Sie auf der FMC-GUI zu **Devices (Geräte) > NAT (NAT) > New Policy (Neue Richtlinie) > Threat Defense NAT (NAT zum Schutz vor Bedrohungen)**, und erstellen Sie eine NAT-Richtlinie.

Beispielsweise wird die NAT-Richtlinie FTD_NAT_Policy erstellt und dem Test FTD FTD_LAB zugewiesen.

New Policy

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Selected Devices

NAT-Regeln konfigurieren

Ausgehende NAT.

Navigieren Sie in der FMC-GUI zu **Devices (Geräte) > NAT (NAT) > Select the NAT policy (NAT-Richtlinie auswählen) > Add Rule (Regel hinzufügen)**, und erstellen Sie eine NAT-Regel, um das interne IPv6-Netzwerk in einen externen IPv4-Pool zu übersetzen.

Beispielsweise wird das Netzwerkobjekt `Local_IPv6_subnet` dynamisch in das Netzwerkobjekt `6_mapped_to_4` übersetzt.

NAT-Regel: Automatische NAT-Regel

Typ: Dynamisch

Quellschnittstellenobjekte: `Inside_Zone`

Zielschnittstellenobjekte: `outside_zone`

Ursprüngliche Quelle: `Local_IPv6_subnet`

Übersetzte Quelle: `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: +

Eingehende NAT.

Navigieren Sie in der FMC-GUI zu **Devices > NAT > Select the NAT policy > Add Rule (Geräte > NAT)**, und erstellen Sie eine NAT-Regel, um externen IPv4-Datenverkehr in internen IPv6-Netzwerkpool zu übersetzen. Dies ermöglicht die interne Kommunikation mit Ihrem lokalen IPv6-Subnetz.

Aktivieren Sie außerdem für diese Regel das DNS-Umschreiben, sodass Antworten vom externen DNS-Server aus A- (IPv4) in AAAA- (IPv6) Einträgen konvertiert werden können.

Beispielsweise wird "Outside Network Any_IPv4" statisch in das IPv6-Subnetz 2100:6400::/96 übersetzt, das im Objekt 4_mapped_to_6 definiert ist.

NAT-Regel: Automatische NAT-Regel

Typ: Statisch

Quellschnittstellenobjekte: Outside_Zone

Zielschnittstellenobjekte: Inside_Zone

Ursprüngliche Quelle: Any_IPv4

Übersetzte Quelle: 4_mapped_to_6

Übersetzen von DNS-Antworten, die dieser Regel entsprechen: Ja (Kontrollkästchen aktivieren)

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 tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Interface Objects' tab is active, showing a search bar and a list of 'Available Interface Objects' (Group_Inside, Group_Outside, Inside_Zone, Outside_Zone). Two buttons, 'Add to Source' and 'Add to Destination', are positioned between the available and selected objects. The 'Source Interface Objects' list contains 'Outside_Zone' and the 'Destination Interface Objects' list contains 'Inside_Zone'. 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								

Setzen Sie die Bereitstellung von Änderungen an FTD fort.

Verifizierung

- Schnittstellennamen und IP-Konfiguration anzeigen.

```
<#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
```

- Bestätigen der IPv6-Konnektivität von der FTD innerhalb der Schnittstelle zum Client

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

FTD Inside Schnittstelle 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
```

- Anzeigen der NAT-Konfiguration in der 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
```

- Datenverkehr erfassen.

Beispielsweise lautet der Erfassungsdatenverkehr vom internen IPv6-Host fc00:0:0:1::100 zum DNS-Server

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

Hier lautet der Ziel-DNS-Server fc00::f:0:0:ac10:a64. Die letzten 32 Bit sind ac10:0a64. Diese Bits sind das Oktett-für-Oktett-Äquivalent von 172,16,10,100. Firewall 6-to-4 übersetzt IPv6 DNS-Server fc00::f:0:0:ac10:a64 in den entsprechenden 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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.