

FMC에서 관리하는 보안 방화벽에 NAT 64 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[네트워크 개체 구성](#)

[IPv4/IPv6용 FTD의 인터페이스 구성](#)

[기본 경로 구성](#)

[NAT 정책 구성](#)

[NAT 규칙 구성](#)

[확인](#)

소개

이 문서에서는 FMC(Fire Power Management Center)에서 관리하는 FTD(Firepower Threat Defense)에서 NAT64를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Secure Firewall Threat Defense 및 Secure Firewall Management Center에 대해 알고 있는 것이 좋습니다.

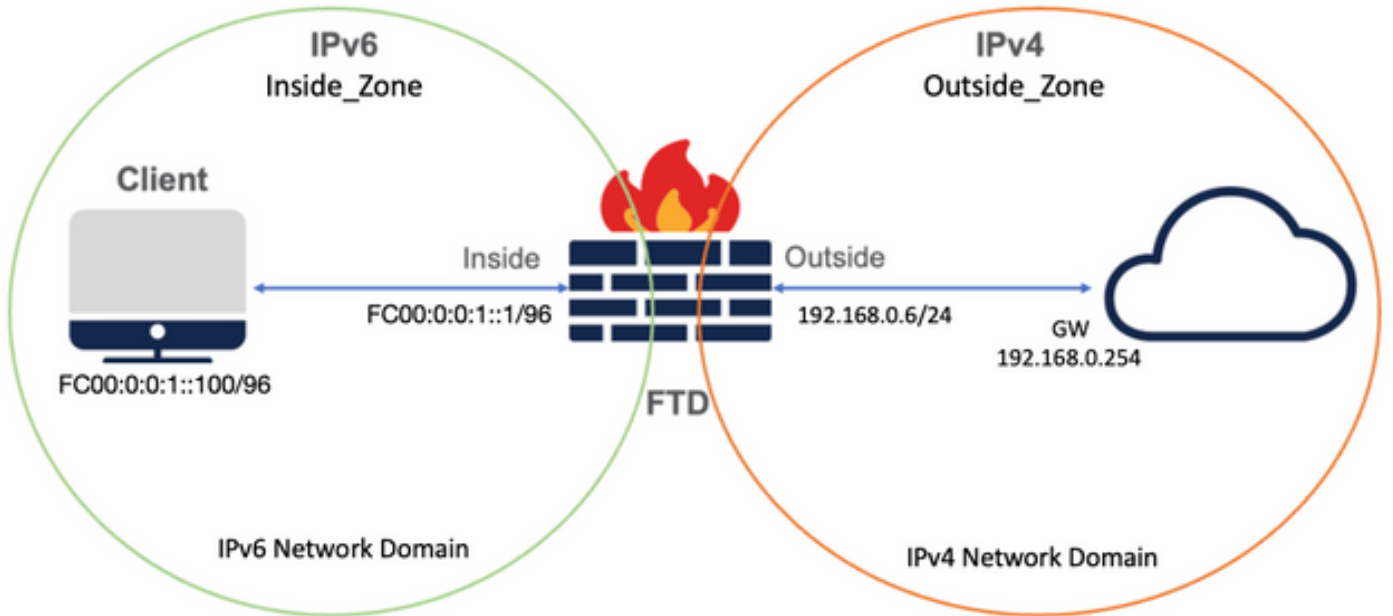
사용되는 구성 요소

- Firepower Management Center 7.0.4
- Firepower Threat Defense 7.0.4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



네트워크 개체 구성

- 내부 IPv6 클라이언트 서브넷을 참조하는 IPv6 네트워크 개체입니다.

FMC GUI에서 Objects(개체) > Object Management(개체 관리) > Select Network from left Menu(왼쪽 메뉴에서 네트워크 선택) > Add Network(네트워크 추가) > Add Object(개체 추가)로 이동합니다.

예를 들어 네트워크 객체 Local_IPv6_subnet은 IPv6 서브넷 FC00:0:0:1::/96으로 생성됩니다.

Edit Network Object ?

Name

Description

Network

Host
 Range
 Network
 FQDN

Allow Overrides

- IPv6 클라이언트를 IPv4로 변환하는 IPv4 네트워크 객체

FMC GUI에서 Objects(객체) > Object Management(객체 관리) > Select Network from left Menu(왼쪽 메뉴에서 네트워크 선택) > Add Network(네트워크 추가) > Add Group(그룹 추가)으로 이동합니다.

예를 들어 네트워크 객체 6_mapped_to_4는 IPv4 호스트 192.168.0.107로 생성됩니다.

IPv4에 매핑할 IPv6 호스트의 양에 따라 단일 객체 네트워크, 여러 IPv4가 있는 네트워크 그룹 또는 이그레스 인터페이스에 대한 NAT만 사용할 수 있습니다.

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

- 인터넷에서 외부 IPv4 호스트를 참조하기 위한 IPv4 네트워크 개체입니다.

FMC GUI에서 Objects(개체) > Object Management(개체 관리) > Select Network from left Menu(왼쪽 메뉴에서 네트워크 선택) > Add Network(네트워크 추가) > Add Object(개체 추가)로 이동합니다.

예를 들어 네트워크 객체 Any_IPv4는 IPv4 서브넷 0.0.0.0/0으로 생성됩니다.

New Network Object ?

Name

Description

Network
 Host Range Network FQDN

Allow Overrides

- 외부 IPv4 호스트를 IPv6 도메인으로 변환하는 IPv6 네트워크 개체

FMC GUI에서 Objects(개체) > Object Management(개체 관리) > Select Network from left Menu(왼쪽 메뉴에서 네트워크 선택) > Add Network(네트워크 추가) > Add Object(개체 추가)로 이동합니다.

예를 들어 네트워크 객체 4_mapped_to_6은 IPv6 서브넷 FC00:0:0:F::/96으로 생성됩니다.

Edit Network Object ?

Name

Description

Network

Host
 Range
 Network
 FQDN

Allow Overrides

IPv4/IPv6용 FTD의 인터페이스 구성

Devices(디바이스) > Device Management(디바이스 관리) > Edit FTD(FTD 편집) > Interfaces(인터페이스)로 이동하고 Inside(내부) 및 Outside(외부) 인터페이스를 구성합니다.

예:

인터페이스 이더넷 1/1

이름: Inside

보안 영역: Inside_Zone

보안 영역이 생성되지 않은 경우 Security Zone(보안 영역) 드롭다운 메뉴 > New(새로 만들기)에서 생성할 수 있습니다.

IPv6 주소: 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

인터페이스 이더넷 1/2

이름: 외부

보안 영역: Outside_Zone

보안 영역이 생성되지 않은 경우 보안 영역 드롭다운 메뉴 > 새로 만들기에서 생성할 수 있습니다

IPv4 주소: 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

기본 경로 구성

Devices(디바이스) > Device Management(디바이스 관리) > Edit FTD(FTD 편집) > Routing(라우팅) > Static Routing(고정 라우팅) > Add Route(경로 추가)로 이동합니다.

예를 들어 게이트웨이 192.168.0.254를 사용하는 외부 인터페이스의 기본 고정 경로입니다.

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)

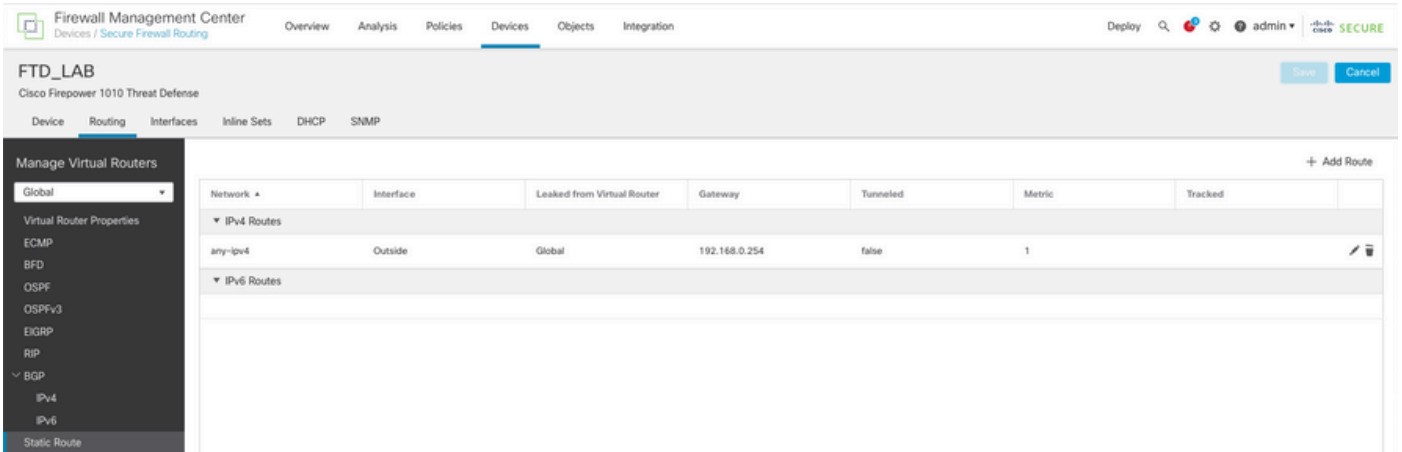
Tunneled: (Used only for default Route)

Route Tracking:



Cancel

OK



NAT 정책 구성

FMC GUI에서 Devices(디바이스) > NAT(NAT) > New Policy(새 정책) > Threat Defense NAT로 이동하고 NAT 정책을 생성합니다.

예를 들어, NAT 정책 FTD_NAT_Policy가 생성되어 테스트 FTD FTD_LAB에 할당됩니다.

New Policy ?

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTD_LAB

Selected Devices

FTD_LAB ✕

NAT 규칙 구성

아웃바운드 NAT.

FMC GUI에서 Devices(디바이스) > NAT > Select the NAT policy(NAT 정책 > Add Rule(규칙 추가)을 선택하고 NAT 규칙을 만들어 Internal IPv6 네트워크를 외부 IPv4 풀로 변환합니다.

예를 들어 네트워크 객체 Local_IPv6_subnet은 네트워크 객체 6_mapped_to_4로 동적으로 변환됩니다.

NAT 규칙: 자동 NAT 규칙

유형: Dynamic

소스 인터페이스 개체: Inside_Zone

대상 인터페이스 개체: Outside_Zone

원래 소스: Local_IPv6_subnet

변환된 소스: 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	Translated Packet
Original Source:* Local_IPv6_subnet +	Translated Source: Address
Original Port: TCP 	Translated Port: 6_mapped_to_4 +

Cancel
OK

인바운드 NAT.

FMC GUI에서 Devices(디바이스) > NAT > Select the NAT policy(NAT 정책 > Add Rule(규칙 추가)을 선택하고 외부 IPv4 트래픽을 Internal IPv6 네트워크 풀로 변환하는 NAT 규칙을 만듭니다. 이렇게 하면 로컬 IPv6 서브넷과의 내부 통신이 가능합니다.

또한 외부 DNS 서버의 회신을 A(IPv4)에서 AAAA(IPv6) 레코드로 변환할 수 있도록 이 규칙에서 DNS 재작성을 활성화합니다.

예를 들어, 외부 네트워크 Any_IPv4는 4_mapped_to_6 객체에 정의된 IPv6 서브넷 2100:6400::/96으로 정적으로 변환됩니다.

NAT 규칙: 자동 NAT 규칙

유형: 정적

소스 인터페이스 객체: Outside_Zone

대상 인터페이스 개체: Inside_Zone

원래 소스: Any_IPv4

변환된 소스: 4_mapped_to_6

이 규칙과 일치하는 DNS 회신 변환: 예(사용 확인란)

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: Auto NAT Rule

Type: Static

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

Cancel OK

FTD_NAT_Policy Show Warnings Save Cancel

Enter Description

Rules Policy Assignments (1)

Filter by Device Filter Rules × Add Rule

#	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	
#	↔	Dyna...	Inside_Zone	Outside_Zone	Local_IPv6_subnet			6_mapped_to_4			Dns:false	
NAT Rules After												

FTD에 변경 사항을 구축합니다.

확인

- 인터페이스 이름 및 IP 구성을 표시합니다.

<#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 내부 인터페이스에서 클라이언트로의 IPv6 연결을 확인합니다.

IPv6 내부 호스트 IP fc00:0:0:1::100.

FTD 내부 인터페이스 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 CLI에 NAT 컨피그레이션을 표시합니다.

```
<#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
```

- 트래픽 캡처.

예를 들어 내부 IPv6 호스트 fc00:0:0:1::100에서 DNS 서버로 전송되는 캡처 트래픽은 fc00::f:0:0:ac10:a64 UDP 53입니다.

여기서 목적지 DNS 서버는 fc00::f:0:0:ac10:a64입니다. 마지막 32비트는 ac10:0a64입니다. 이 비트는 172,16,10,100에 해당하는 옥텟과 옥텟이다. 방화벽 6-to-4는 IPv6 DNS 서버 fc00::f:0:0:ac10:a64를 동등한 IPv4 172.16.10.100으로 변환합니다.

<#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
```


이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.