FTD Cluster 7.0에 대한 동적 PAT의 포트 할당 이해

목차

소개

이 문서에서는 포트 블록 기반 배포가 버전 7.0 이후 방화벽 클러스터용 동적 PAT에서 작동하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Firewall의 NAT(Network Address Translation)

사용되는 구성 요소

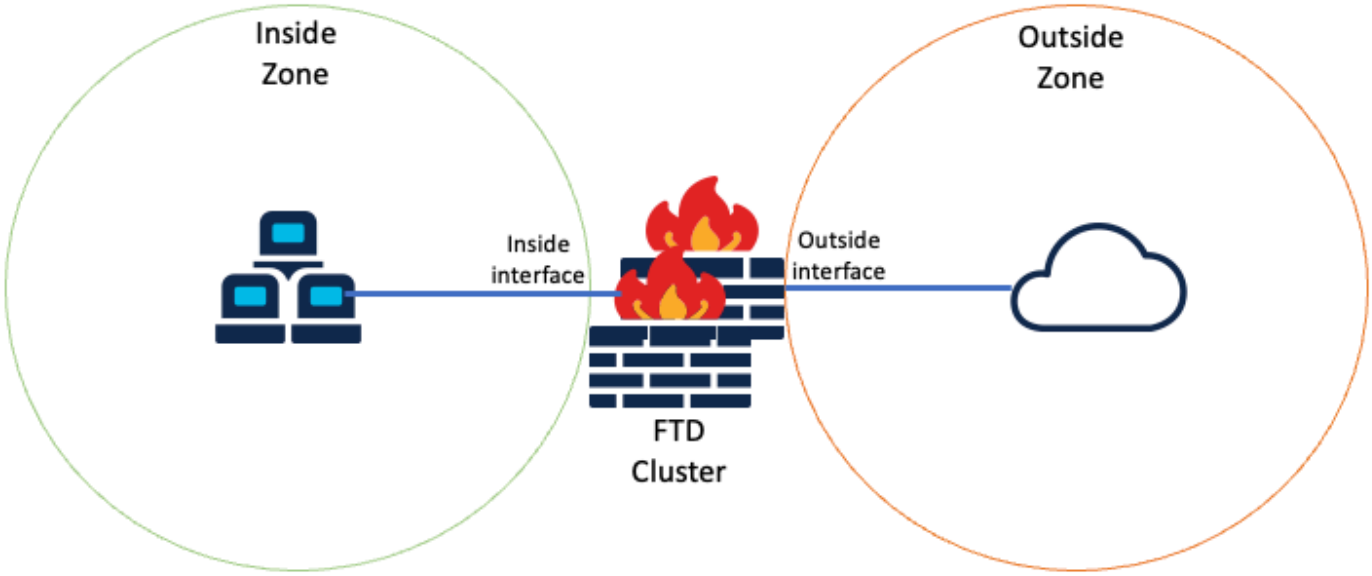
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower Management Center 7.3.0
- Firepower Threat Defense 7.2.0

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

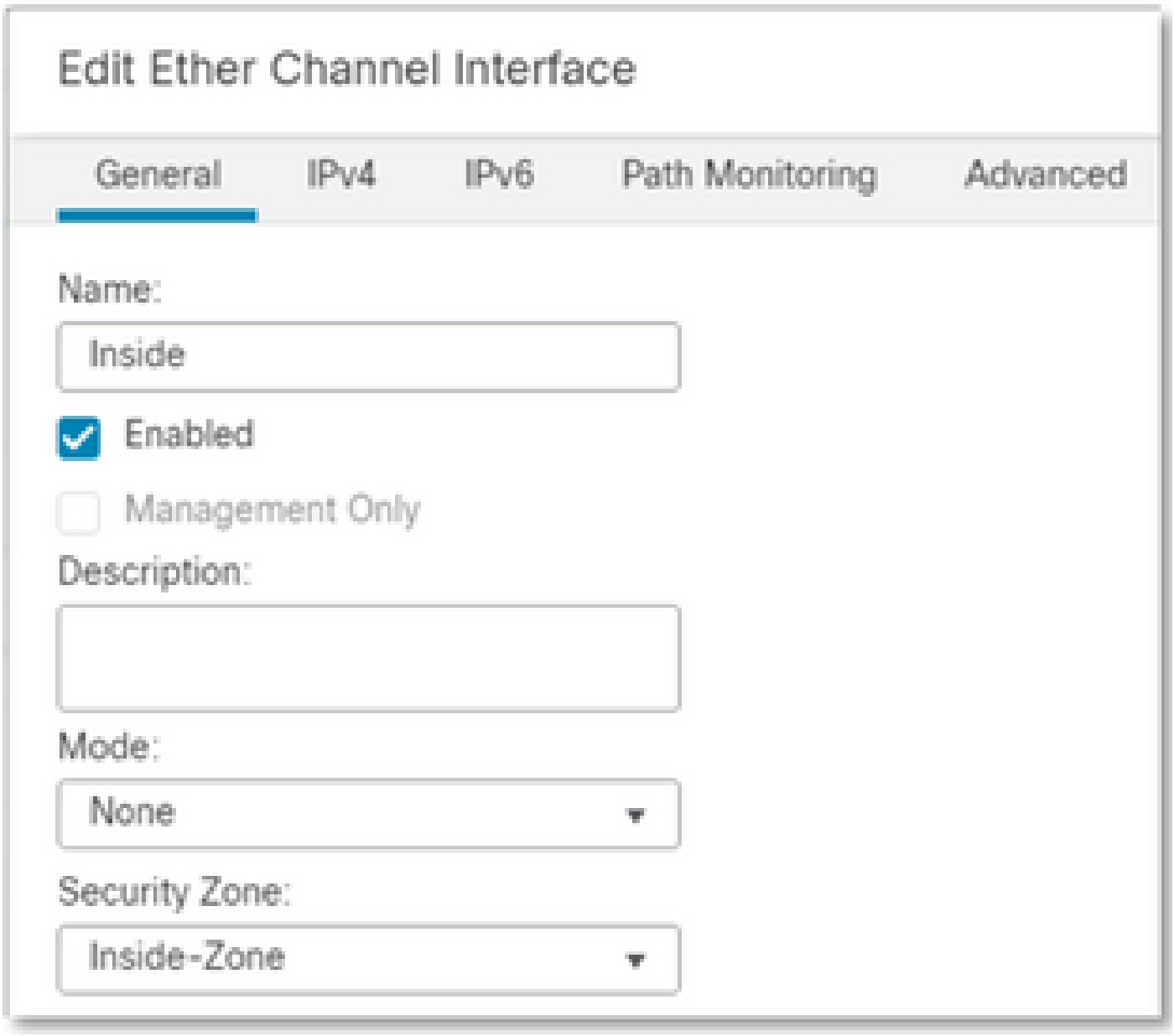


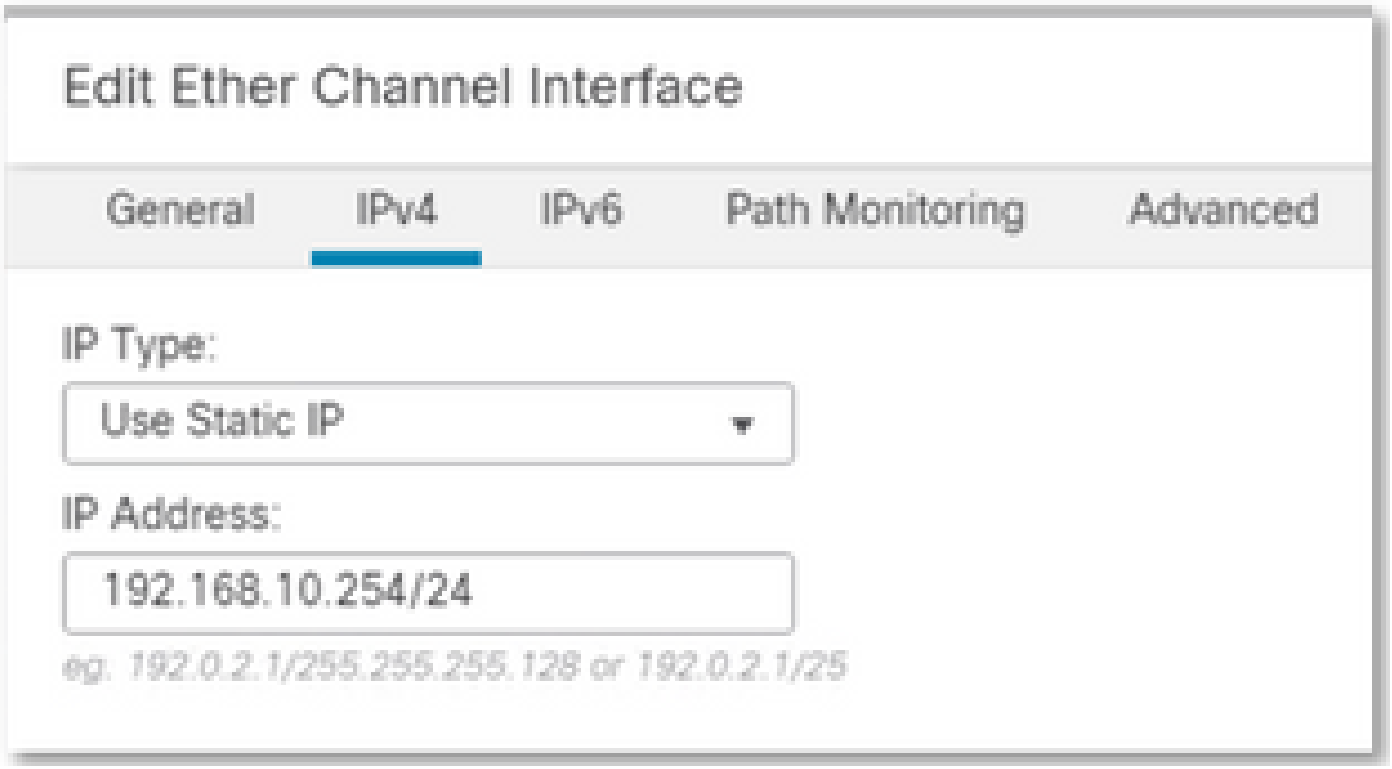
논리적 토폴로지

인터페이스 컨피그레이션

- Inside Zone의 내부 인터페이스 멤버를 구성합니다.

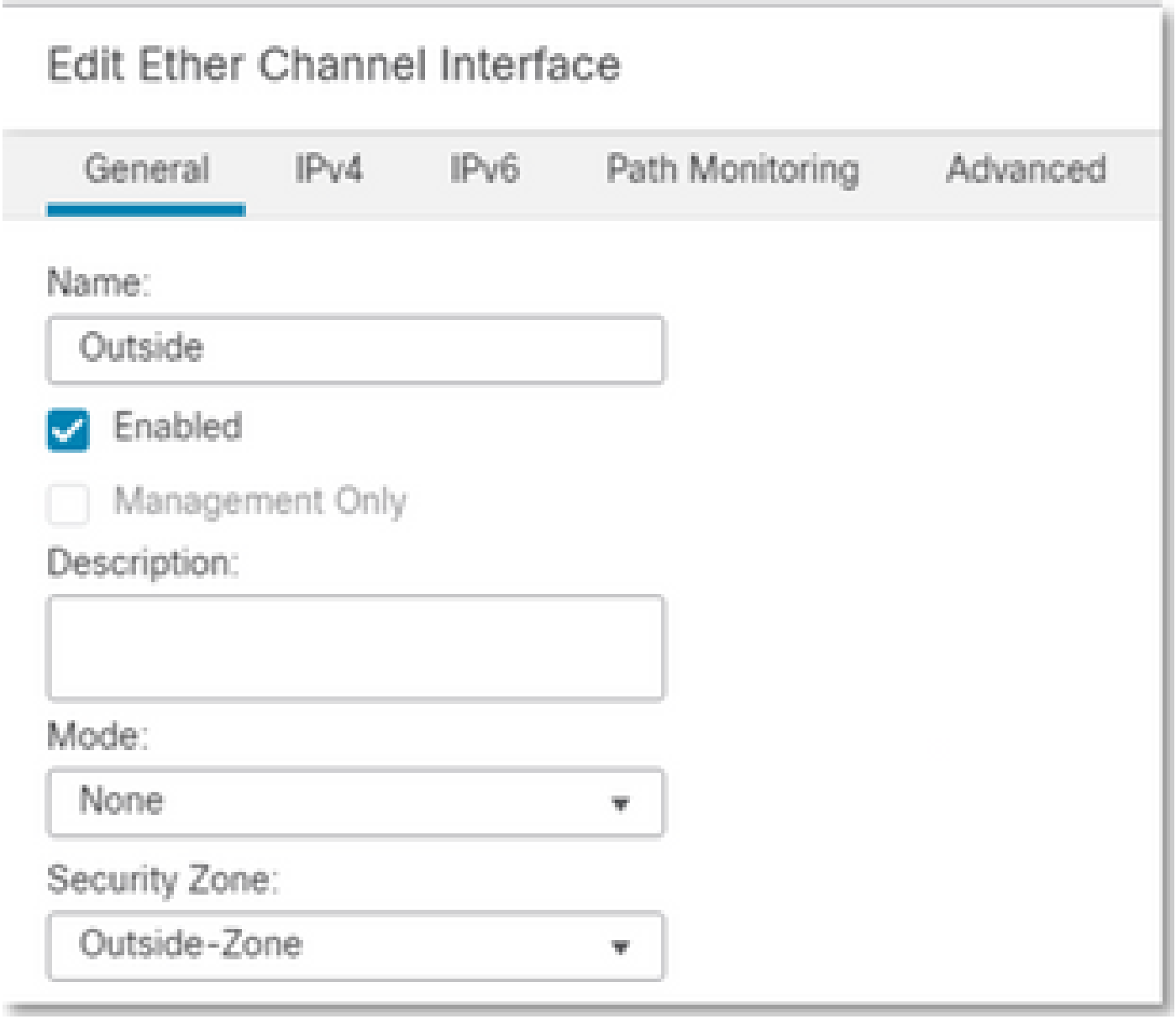
예를 들어 IP 주소가 192.168.10.254인 인터페이스를 구성하고 이름을 Inside로 지정합니다. 이 내부 인터페이스는 내부 네트워크 192.168.10.0/24용 게이트웨이입니다.

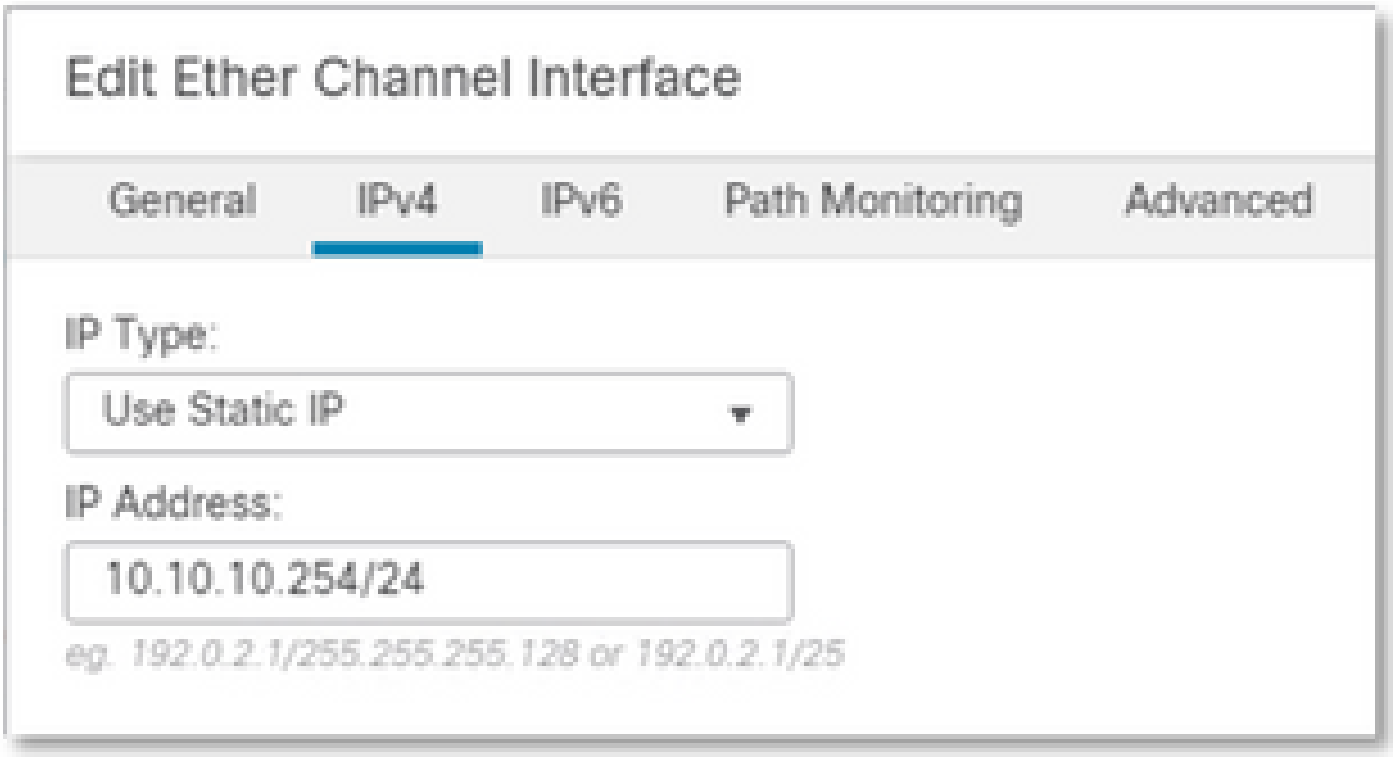

Edit Ether Channel Interface
General
IPv4
IPv6
Path Monitoring
Advanced
Name:
Inside
Enabled
Management Only
Description:
Mode:
None
Security Zone:
Inside-Zone



- 외부 영역의 외부 인터페이스 멤버를 구성합니다.

예를 들어 IP 주소가 10.10.10.254이고 이름을 Outside로 지정하는 인터페이스를 구성합니다. 이 외부 인터페이스는 외부 네트워크를 향하고 있습니다.


Edit Ether Channel Interface
General
IPv4
IPv6
Path Monitoring
Advanced
Name:
Outside
Enabled
Management Only
Description:
Mode:
None
Security Zone:
Outside-Zone

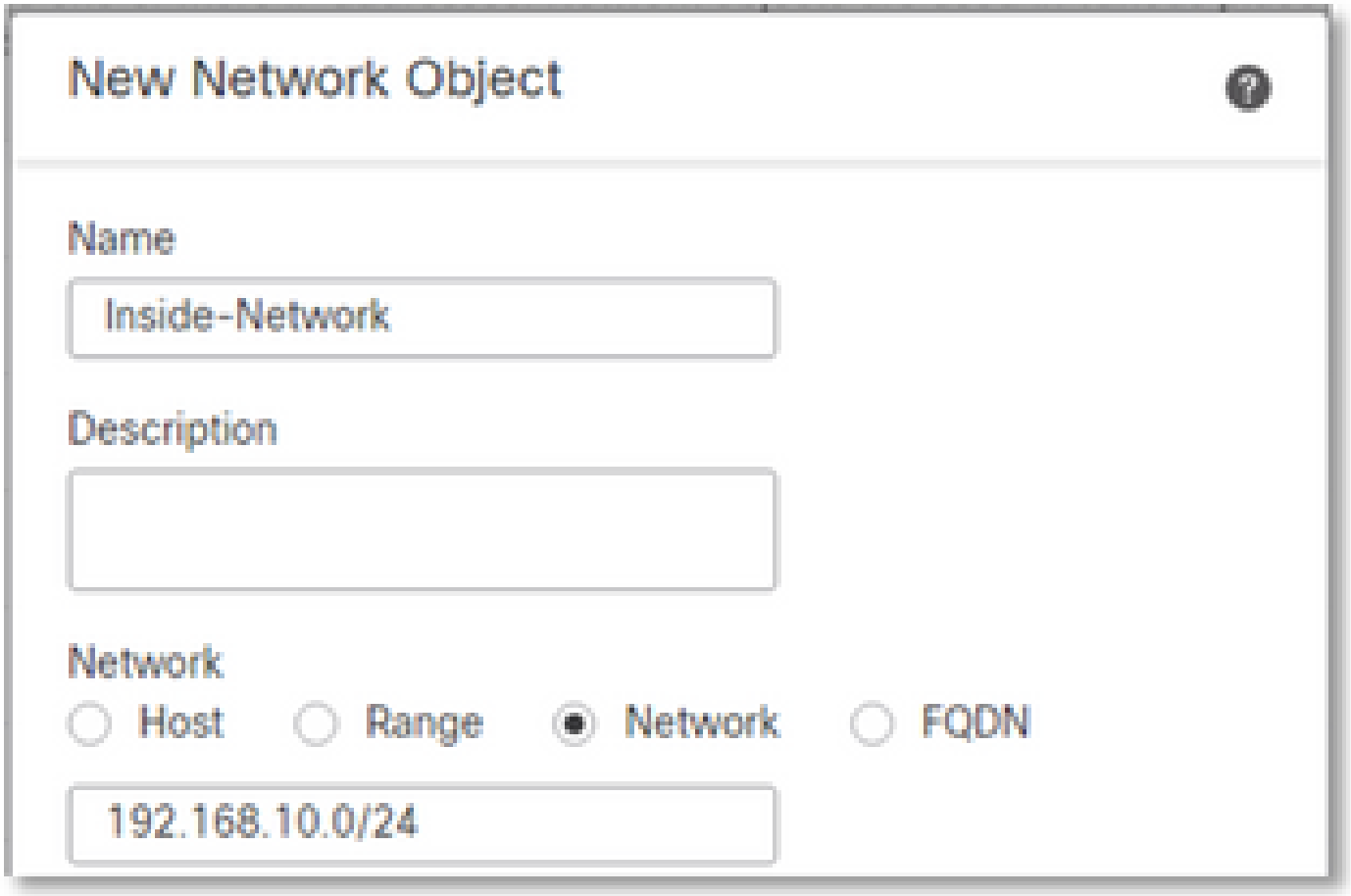


네트워크 개체 컨피그레이션

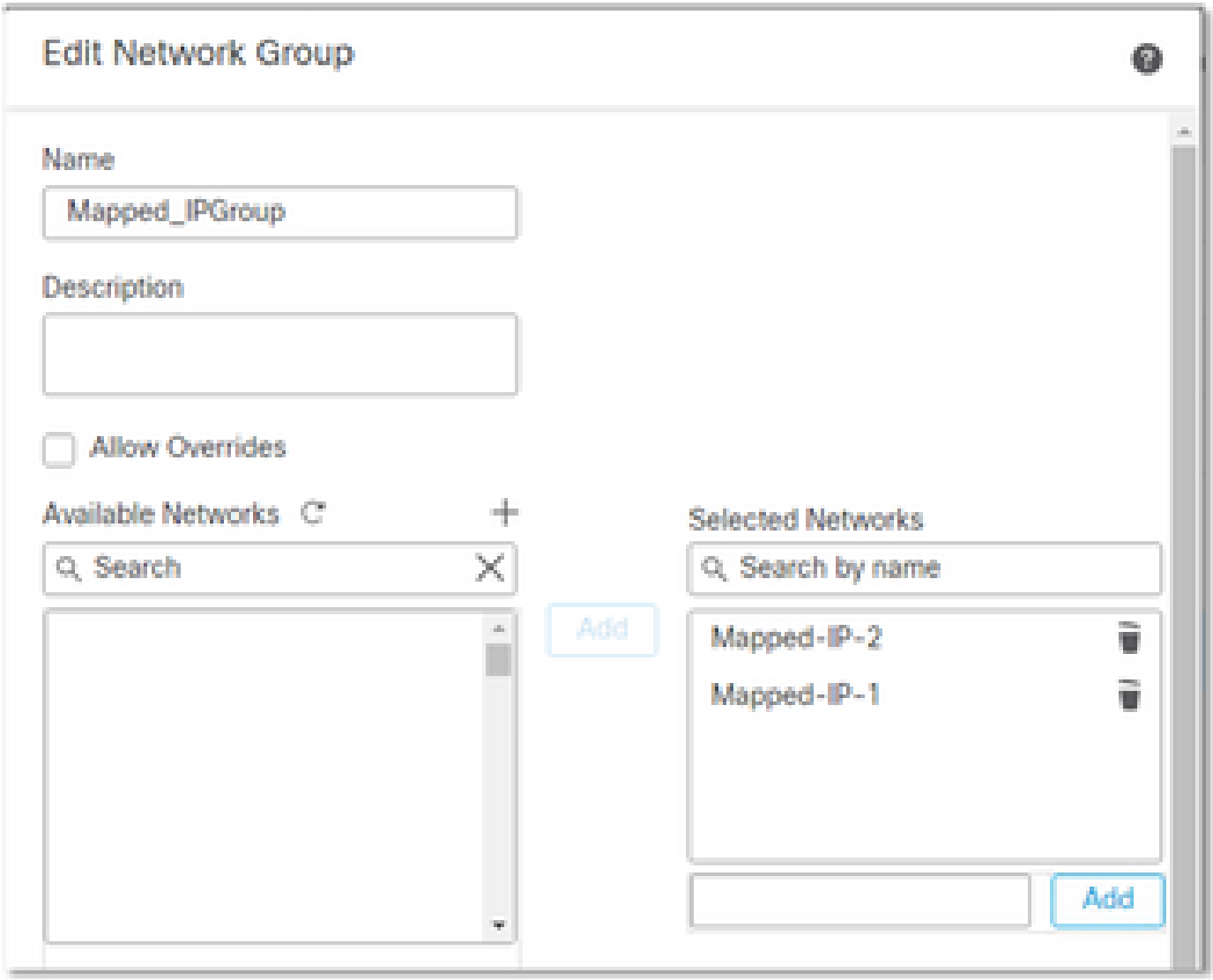
클러스터 PAT가 이그레스 인터페이스 또는 단일 IP와 함께 모든 트래픽을 매핑할 수 있지만 모범 사례는 클러스터의 FTD 유닛 수와 적어도 동일한 수의 IP를 가진 IP 풀을 사용하는 것입니다.

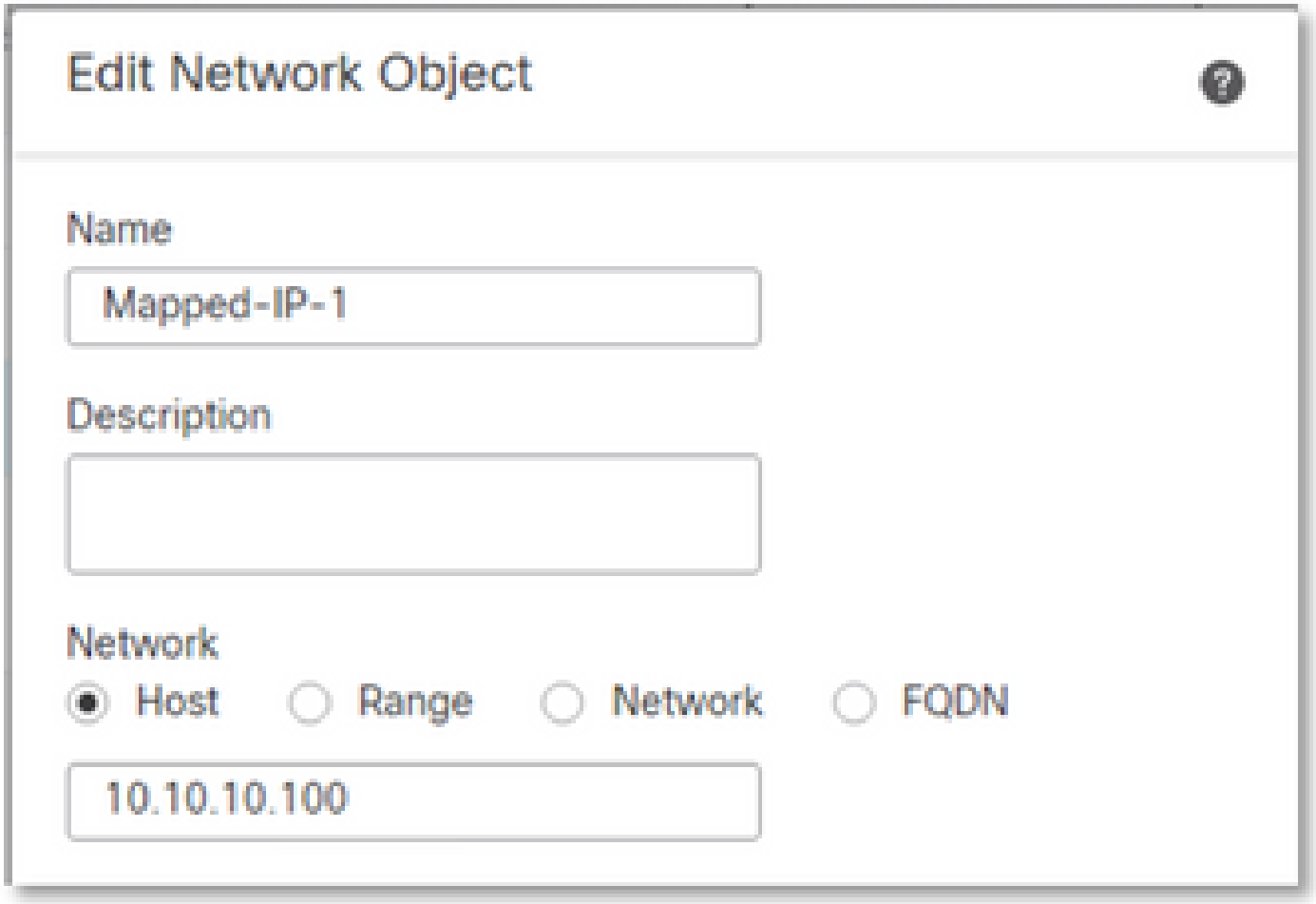
예를 들어 실제 및 매핑된 IP 주소에 사용되는 네트워크 개체는 각각 Inside-Network 및 Mapped-IPGroup입니다.

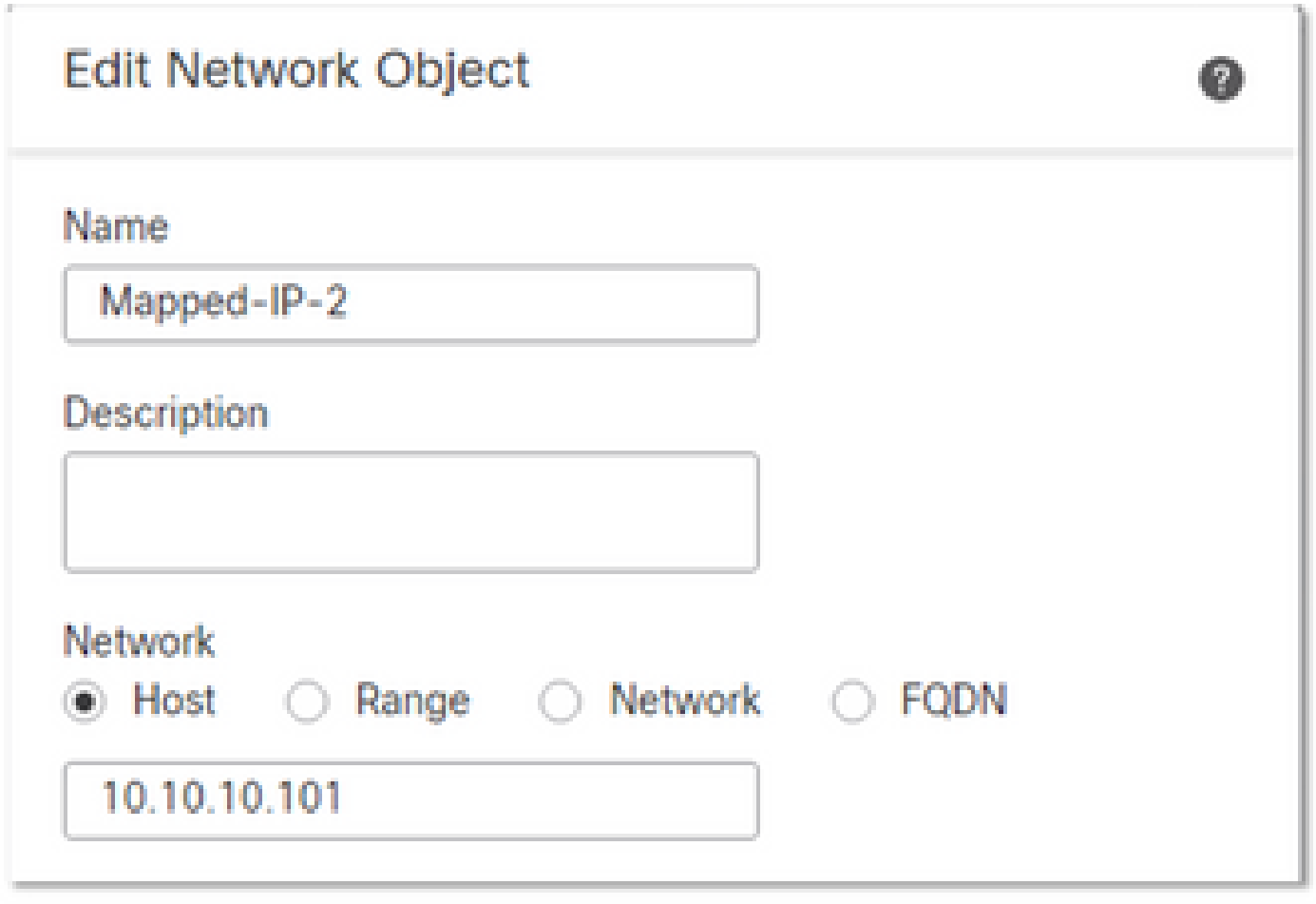
Inside-Network는 내부 네트워크 192.168.10.0/24을 나타냅니다.



Mapped-IPGroup(Mapped-IP-1 10.10.10.100 및 Mapped-IP-2 10.10.10.101)은 모든 내부 트래픽을 외부 영역에 매핑하는 데 사용됩니다.


Edit Network Group
Name
Mapped_IPGroup
Description
Allow Overrides
Available Networks
Search
Add
Selected Networks
Search by name
Mapped-IP-2
Mapped-IP-1
Add

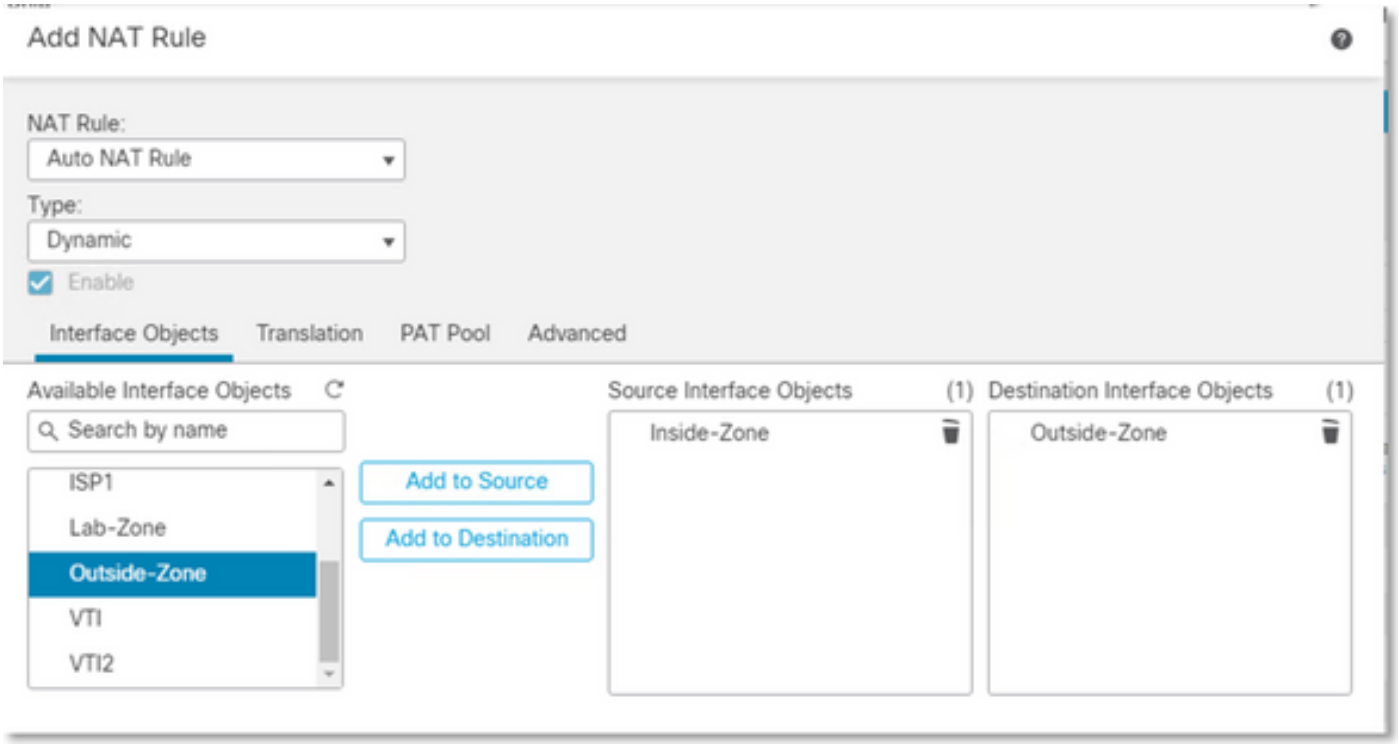

Edit Network Object
Name
Mapped-IP-1
Description
Network
Host
Range
Network
FQDN
10.10.10.100

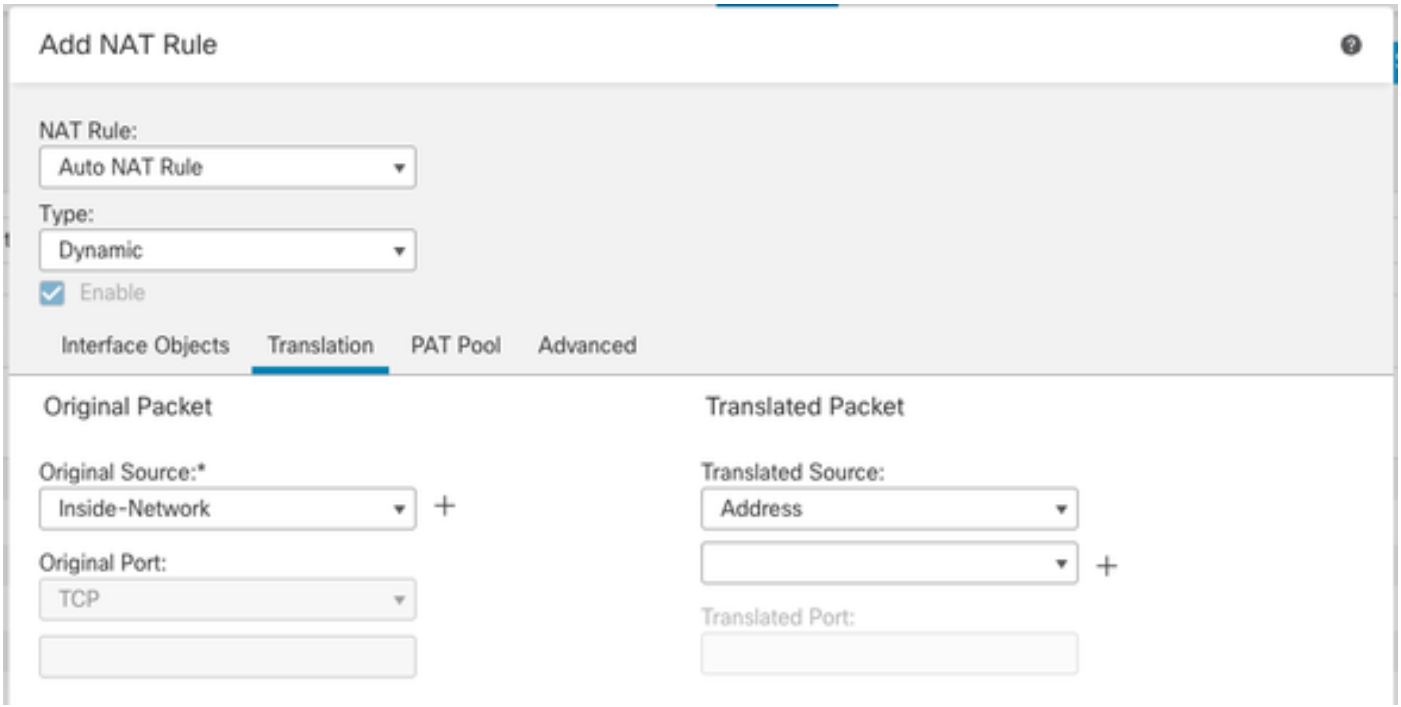

Edit Network Object
Name
Mapped-IP-2
Description
Network
Host
Range
Network
FQDN
10.10.10.101

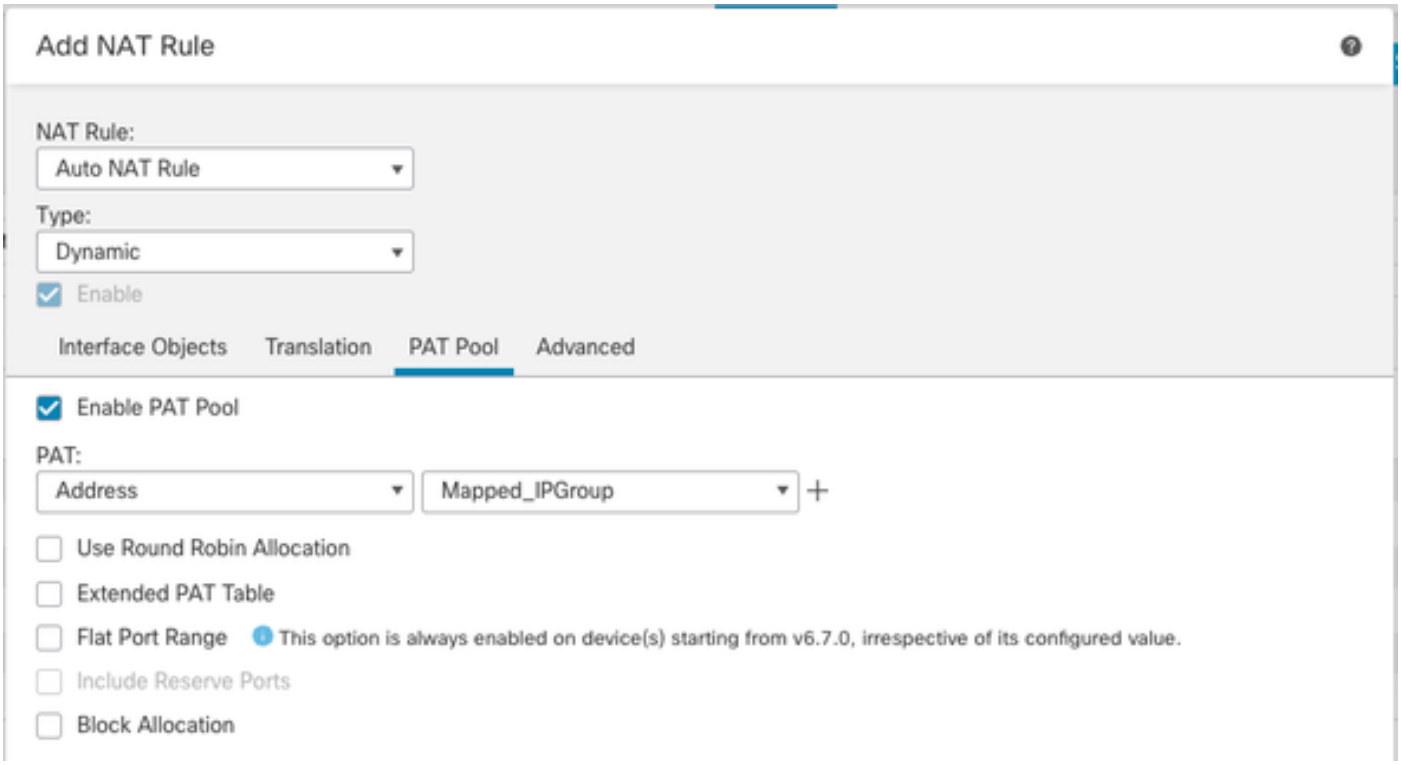
동적 PAT 컨피그레이션

- 아웃바운드 트래픽에 대한 동적 NAT 규칙을 구성합니다. 이 NAT 규칙은 내부 네트워크 서브넷을 외부 NAT 풀에 매핑합니다.

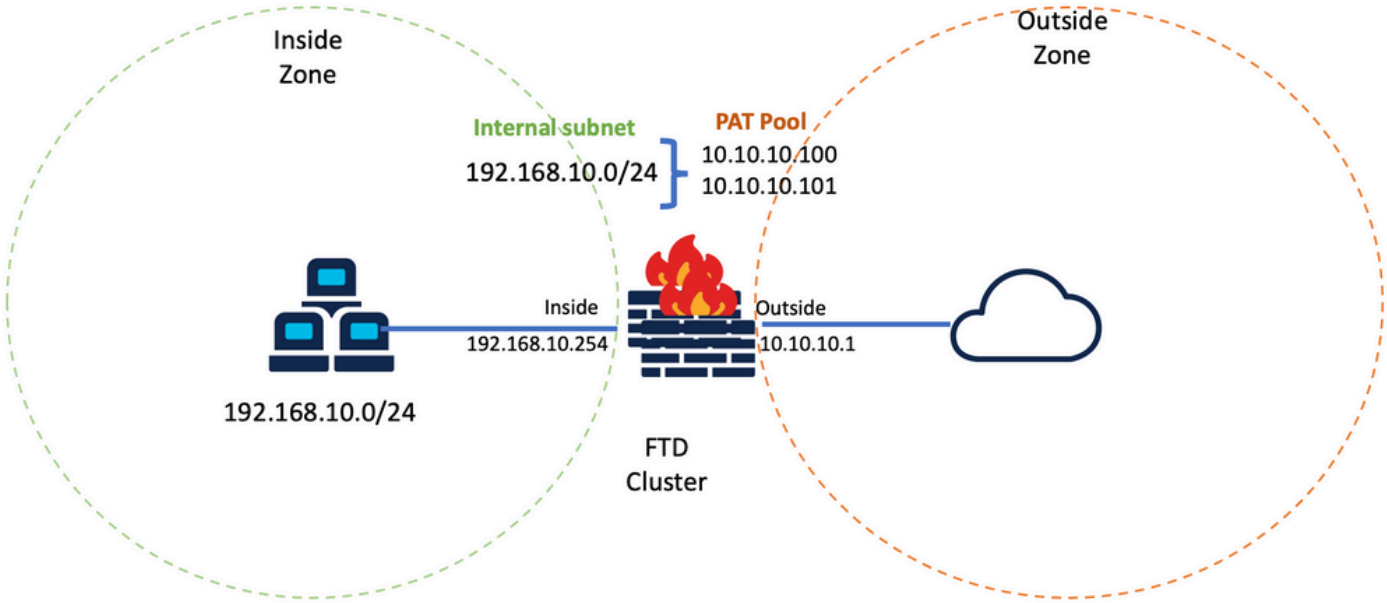
예를 들어 내부 네트워크에서 내부 영역 간 트래픽은 매핑된 IPGroup 풀로 변환됩니다.







최종 컨피그레이션



최종 실습 설정.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

IP 인터페이스 및 NAT 컨피그레이션 확인

<#root>

> show ip

```
System IP Addresses:
Interface Name IP address Subnet mask Method
Port-channel1 Inside 192.168.10.254 255.255.255.0 manual
Port-channel2 Outside 10.10.10.254 255.255.255.0 manual
```

<#root>

> show running-config nat

```
!
object network Inside-Network
nat (Inside,Outside) dynamic pat-pool Mapped_IPGroup
```

포트 블록 할당 확인

Firepower 7.0 이후의 향상된 PAT 포트 블록 할당은 제어 유닛이 노드를 조인할 수 있도록 포트를 예약 상태로 유지하고 미사용 포트를 사전에 회수하도록 보장합니다. 포트 할당은 다음과 같은 방식으로 이루어집니다.

- 이제 막 가동되는 클러스터에서 제어 유닛은 처음에 포트의 50%를 소유하며 나머지는 예약됩니다.
- 클러스터에 가입하는 노드가 늘어나면 유닛당 소유하는 포트 블록의 수가 조정됩니다.
- 제어 유닛은 클러스터가 가득 찰 때까지 (N+1) 노드에 대한 포트 블록을 예약합니다. 클러스터 멤버 제한은 클러스터 그룹 컨피그레이션 레벨에 구성된cluster-member-limit 명령에 의해 정의됩니다.
- 기본적으로 cluster-member-limit는 16입니다.
  <#root>

  > show cluster info

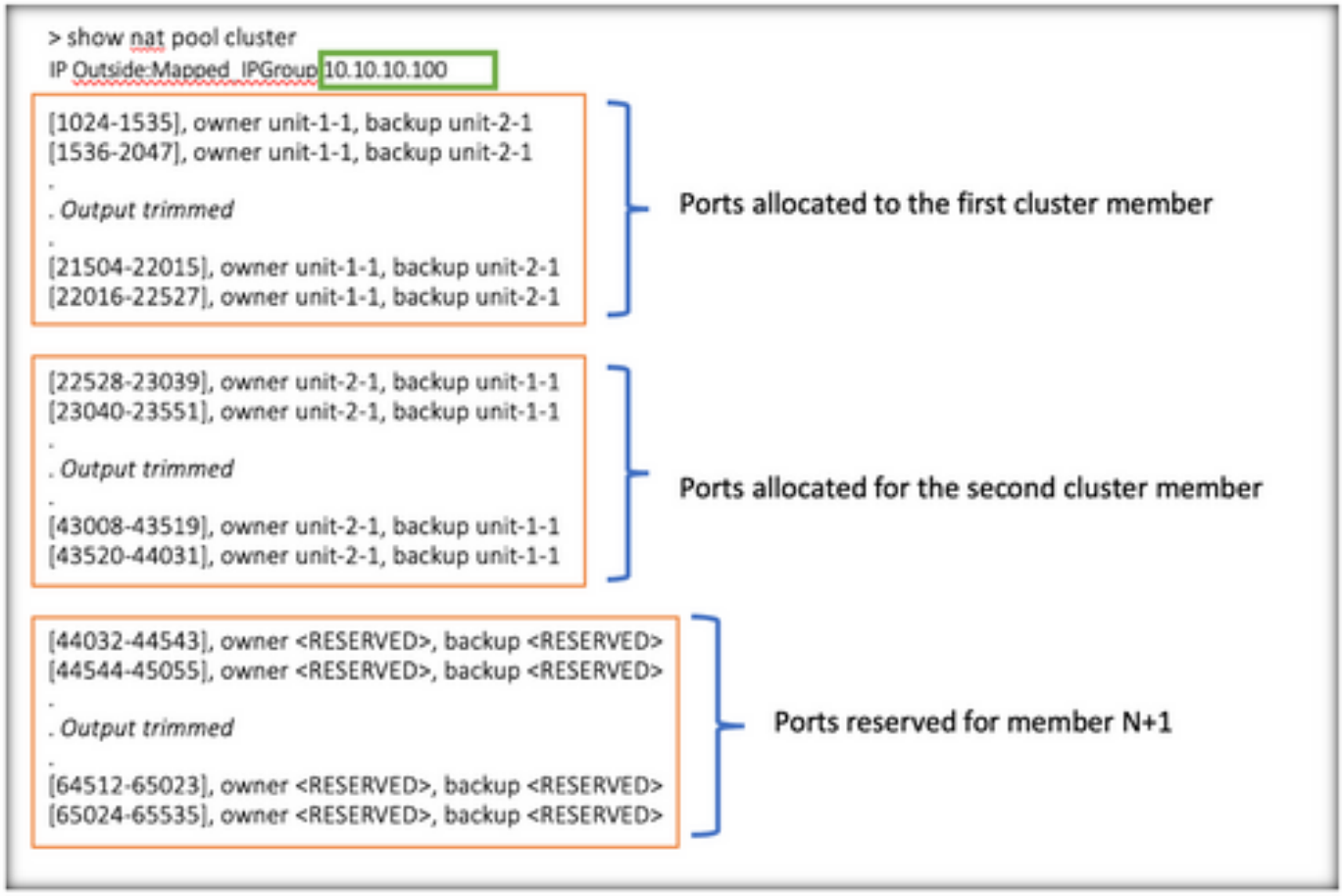
  ```
  Cluster FTD-Cluster: On
  Interface mode: spanned
  ```

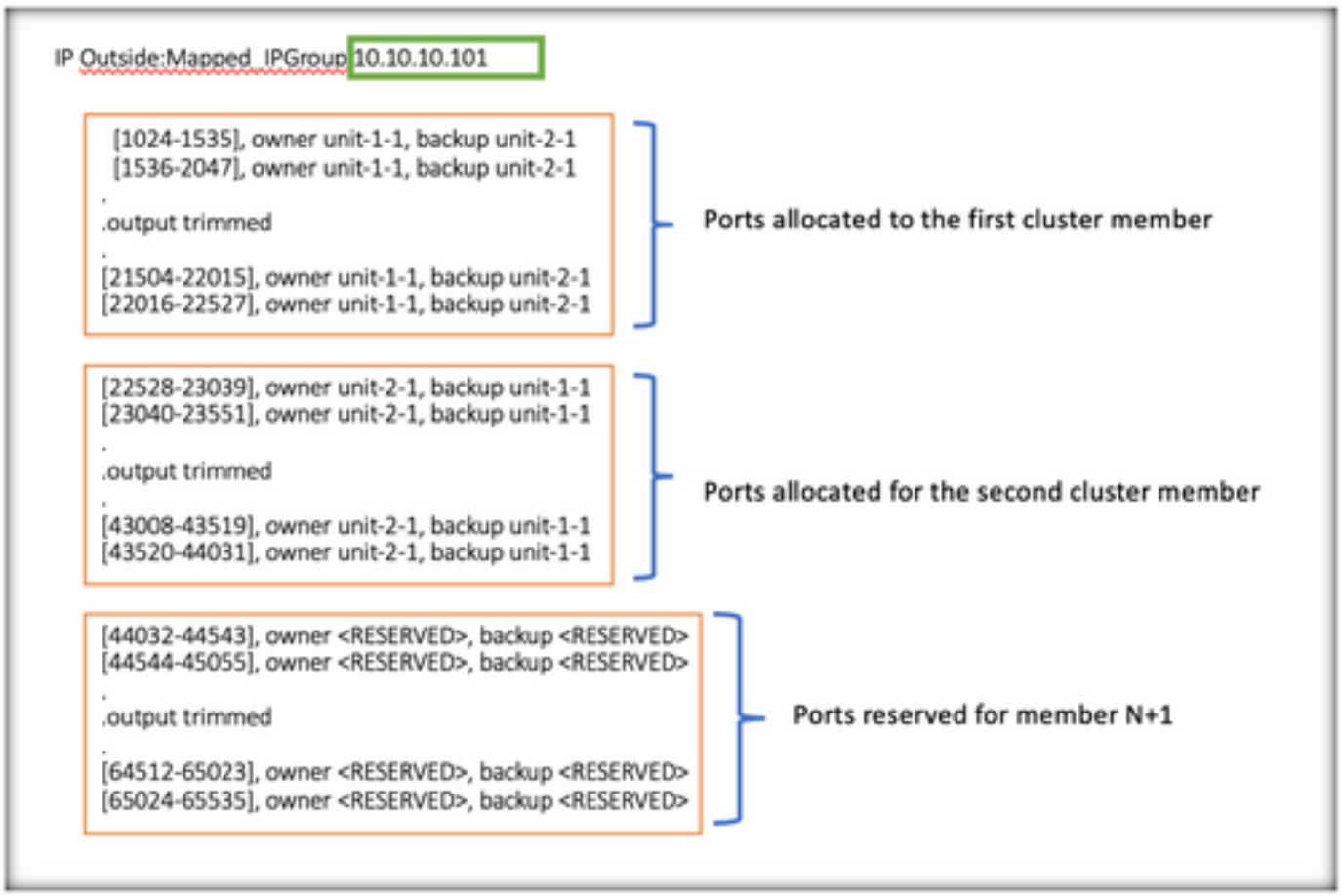
  Cluster Member Limit : 16

  ```
  [...]
  ```

- 클러스터 멤버의 양이 로 구성된 값에 도달하면 **cluster-member-limit**모든 포트 블록이 클러스터 멤버 간에 분산됩니다.

예를 들어, 두 단위(N=2)로 구성된 클러스터 그룹(기본값: 클러스터 멤버 제한 16)에서는 N+1 멤버(이 경우 3)에 대해 포트 할당이 정의되었습니다. 이렇게 하면 최대 클러스터 제한에 도달할 때까지 일부 포트가 다음 유닛에 예약된 상태로 유지됩니다.

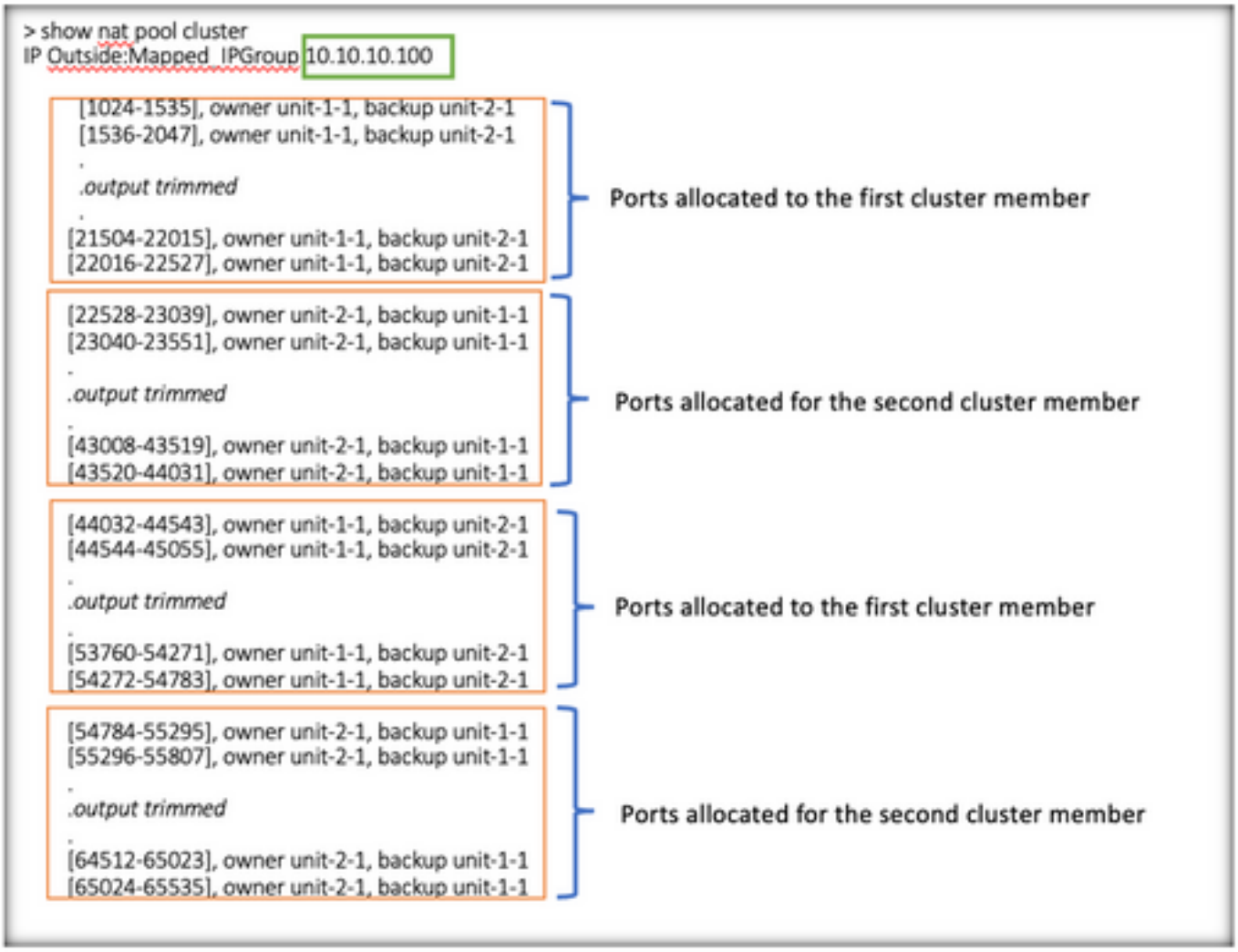

> show nat pool cluster
IP Outside:Mapped IPGroup 10.10.10.100
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
. Output trimmed
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1
Ports allocated to the first cluster member
[22528-23039], owner unit-2-1, backup unit-1-1
[23040-23551], owner unit-2-1, backup unit-1-1
. Output trimmed
[43008-43519], owner unit-2-1, backup unit-1-1
[43520-44031], owner unit-2-1, backup unit-1-1
Ports allocated for the second cluster member
[44032-44543], owner <RESERVED>, backup <RESERVED>
[44544-45055], owner <RESERVED>, backup <RESERVED>
. Output trimmed
[64512-65023], owner <RESERVED>, backup <RESERVED>
[65024-65535], owner <RESERVED>, backup <RESERVED>
Ports reserved for member N+1

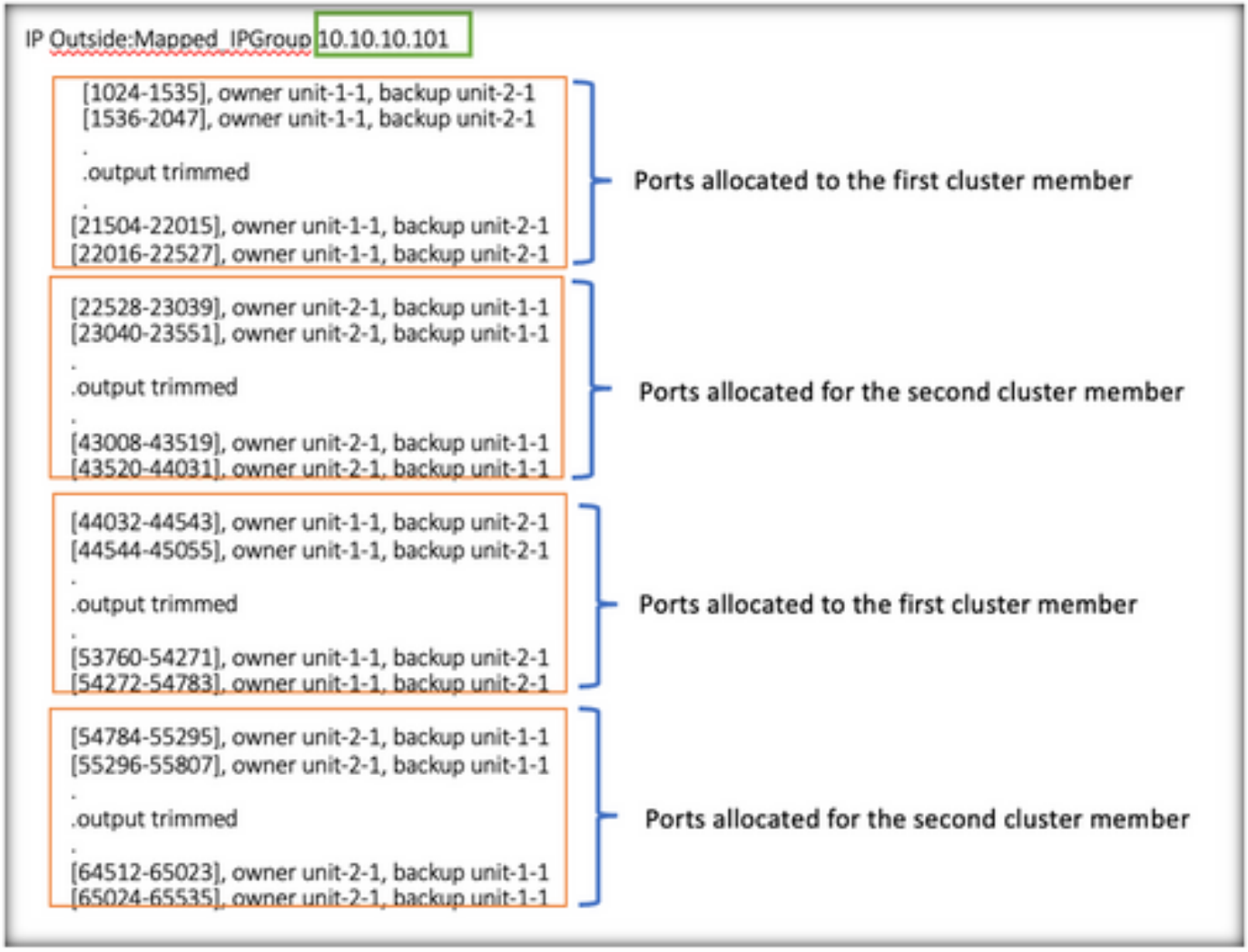

IP Outside:Mapped IPGroup 10.10.10.101
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
.output trimmed
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1
Ports allocated to the first cluster member
[22528-23039], owner unit-2-1, backup unit-1-1
[23040-23551], owner unit-2-1, backup unit-1-1
.output trimmed
[43008-43519], owner unit-2-1, backup unit-1-1
[43520-44031], owner unit-2-1, backup unit-1-1
Ports allocated for the second cluster member
[44032-44543], owner <RESERVED>, backup <RESERVED>
[44544-45055], owner <RESERVED>, backup <RESERVED>
.output trimmed
[64512-65023], owner <RESERVED>, backup <RESERVED>
[65024-65535], owner <RESERVED>, backup <RESERVED>
Ports reserved for member N+1

```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IP-1 10.10.10.100 (126 - 42 / 42) ^ 42 # 0
IP Outside:Mapped-IP-1 10.10.10.101 (126 - 42 / 42) ^ 42 # 0
```

또한 클러스터 구축에 계획된 유닛 수와 일치하도록 **cluster-member-limit** 를 구성하는 것이 좋습니다.

예를 들어, 클러스터 멤버 제한 값이 2인 두 유닛(N=2)으로 구성된 클러스터 그룹에서 포트 할당은 모든 클러스터 유닛에 고르게 분배됩니다. 예약된 포트가 남아 있지 않습니다.






```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IP-1 10.10.10.100 (126 - 63 / 63) ^ 0 # 0
IP Outside:Mapped-IP-1 10.10.10.100 (126 - 63 / 63) ^ 0 # 0
```

포트 블록 재확보 확인

- 새 노드가 클러스터에 가입하거나 클러스터를 벗어날 때마다 모든 유닛의 미사용 포트 및 초과 포트 블록을 제어 유닛으로 해제해야 합니다.
- 포트 블록이 이미 사용되고 있는 경우 가장 적게 사용된 포트 블록은 재확보 대상으로 표시됩니다.
- 재확보된 포트 블록에서는 새 연결이 허용되지 않습니다. 마지막 포트가 제거되면 제어 유닛으로 해제됩니다.

```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IPGroup 10.10.10.100 (126 - 80 / 46) ^ 0 # 17
IP Outside:Mapped-IPGroup 10.10.10.101 (126 - 63 / 63) ^ 0 # 0
```

트러블슈팅 명령

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

- 구성된 cluster-member-limit 값을 확인합니다.

<#root>

> show cluster info

```
Cluster FTD-Cluster: On
Interface mode: spanned
```

Cluster Member Limit : 2

```
[...]
```

> show running-config cluster

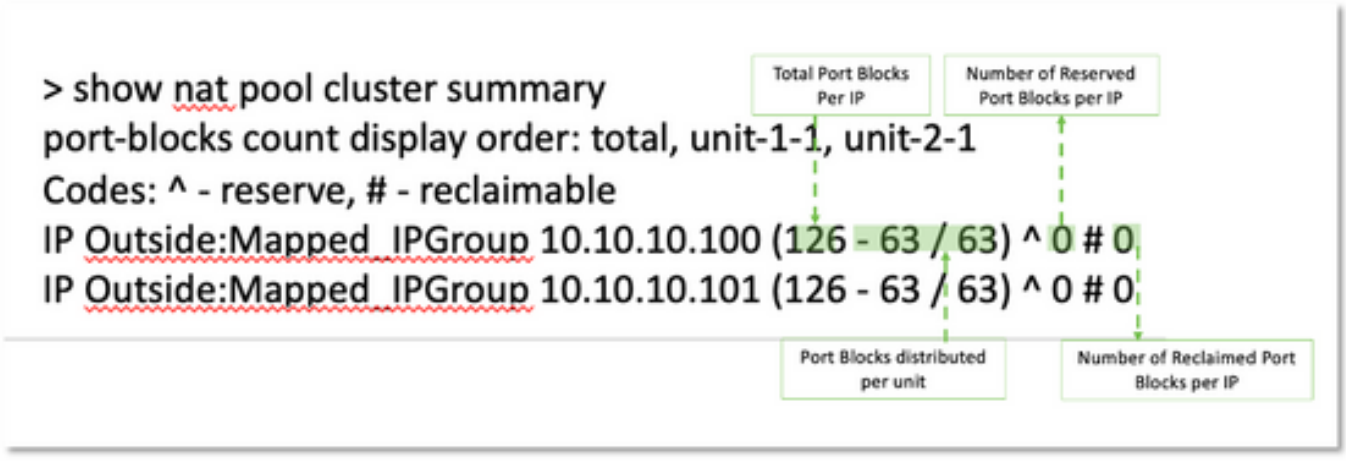
```
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0
```

cluster-member-limit 2
[...]

- 클러스터에 있는 유닛 간의 포트 블록 분포에 대한 요약을 표시합니다.

<#root>

> show nat pool cluster summary



- 소유자 및 백업 유닛에 대한 PAT 주소당 포트 블록의 현재 할당을 표시합니다.

<#root>

```
> show nat pool cluster
```

```
IP Outside:Mapped_IPGroup 10.10.10.100
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
[2048-2559], owner unit-1-1, backup unit-2-1
[2560-3071], owner unit-1-1, backup unit-2-1
[...]
IP Outside:Mapped_IPGroup 10.10.10.101
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
[2048-2559], owner unit-1-1, backup unit-2-1
[2560-3071], owner unit-1-1, backup unit-2-1
[...]
```

- 포트 블록의 배포 및 사용과 관련된 정보 표시:

<#root>

```
> show
```

```
nat
```

```
 pool detail
```

```
TCP PAT pool Outside, address 10.10.10.100
        range 17408-17919, allocated 2 *
        range 27648-28159, allocated 2
TCP PAT pool Outside, address 10.10.10.101
        range 17408-17919, allocated 1 *
        range 27648-28159, allocated 2
[...]
```

관련 정보

- Cisco 기술 지원 및 다운로드

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.