了解FTD集群7.0的动态PAT上的端口分配

目录

简介

本文档介绍在版本7.0及更高版本之后，基于端口块的分发如何在防火墙集群的动态PAT中运行。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙上的网络地址转换(NAT)

使用的组件

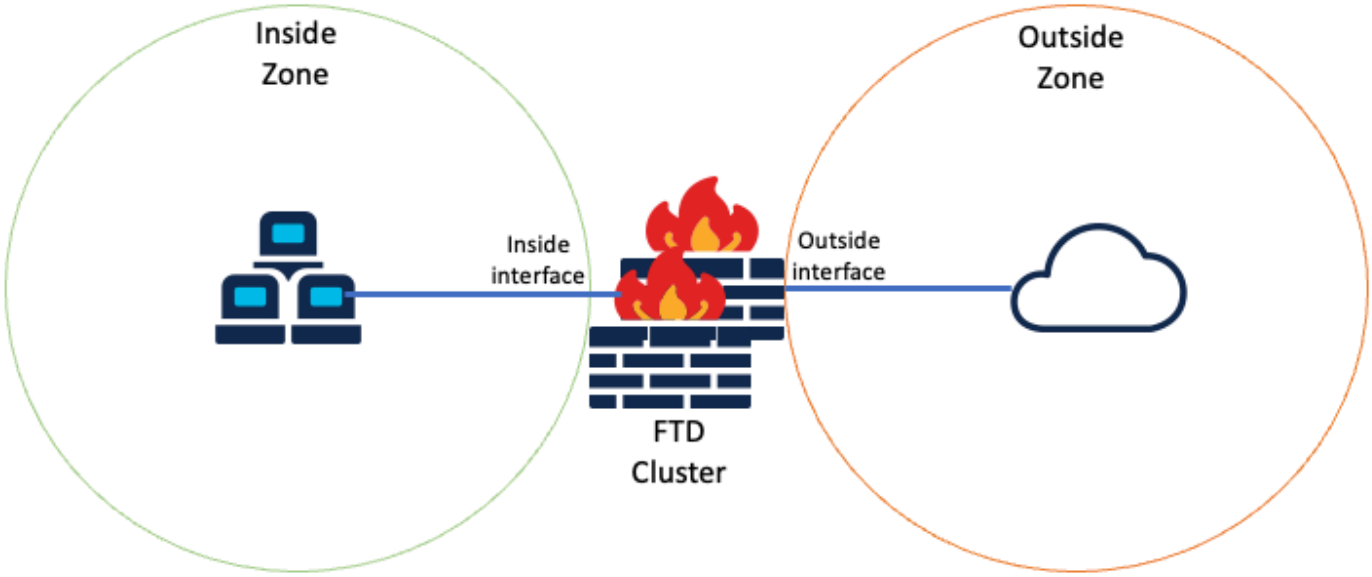
本文档中的信息基于以下软件和硬件版本：

- Firepower管理中心7.3.0
- Firepower威胁防御7.2.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图

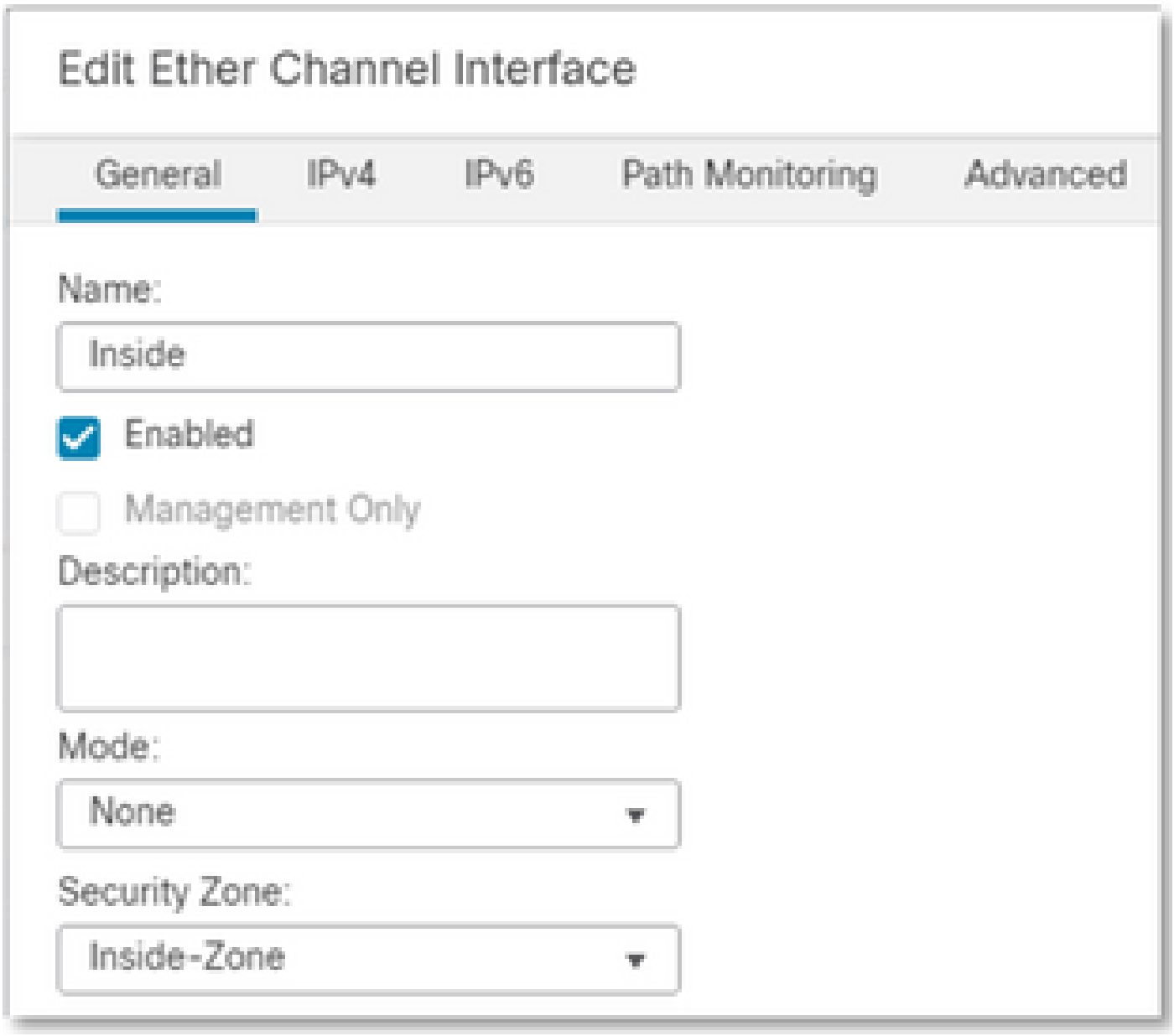


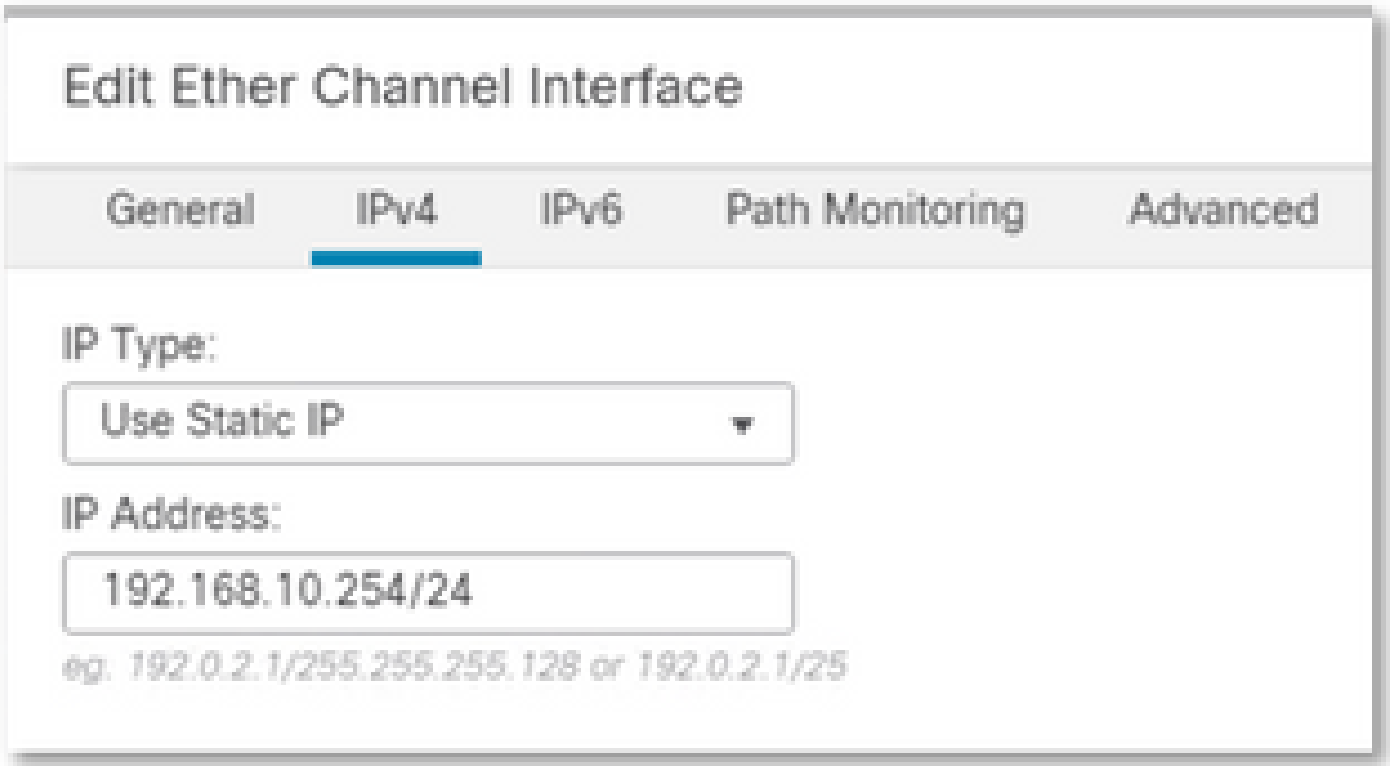
逻辑拓扑

接口配置

- 配置内部区域的内部接口成员。

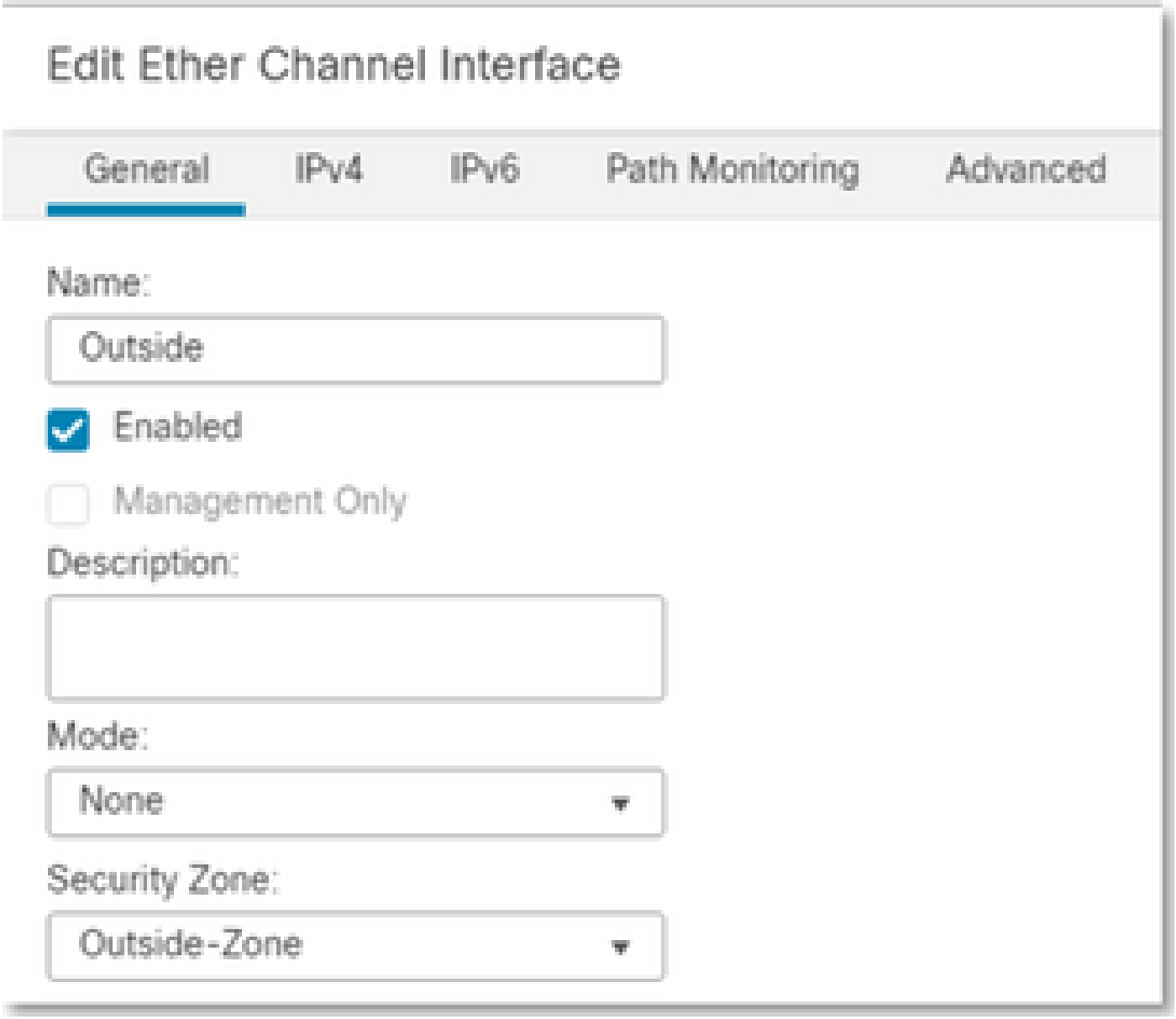
例如，使用IP地址192.168.10.254配置接口并将其命名为Inside。此内部接口是内部网络192.168.10.0/24的网关。

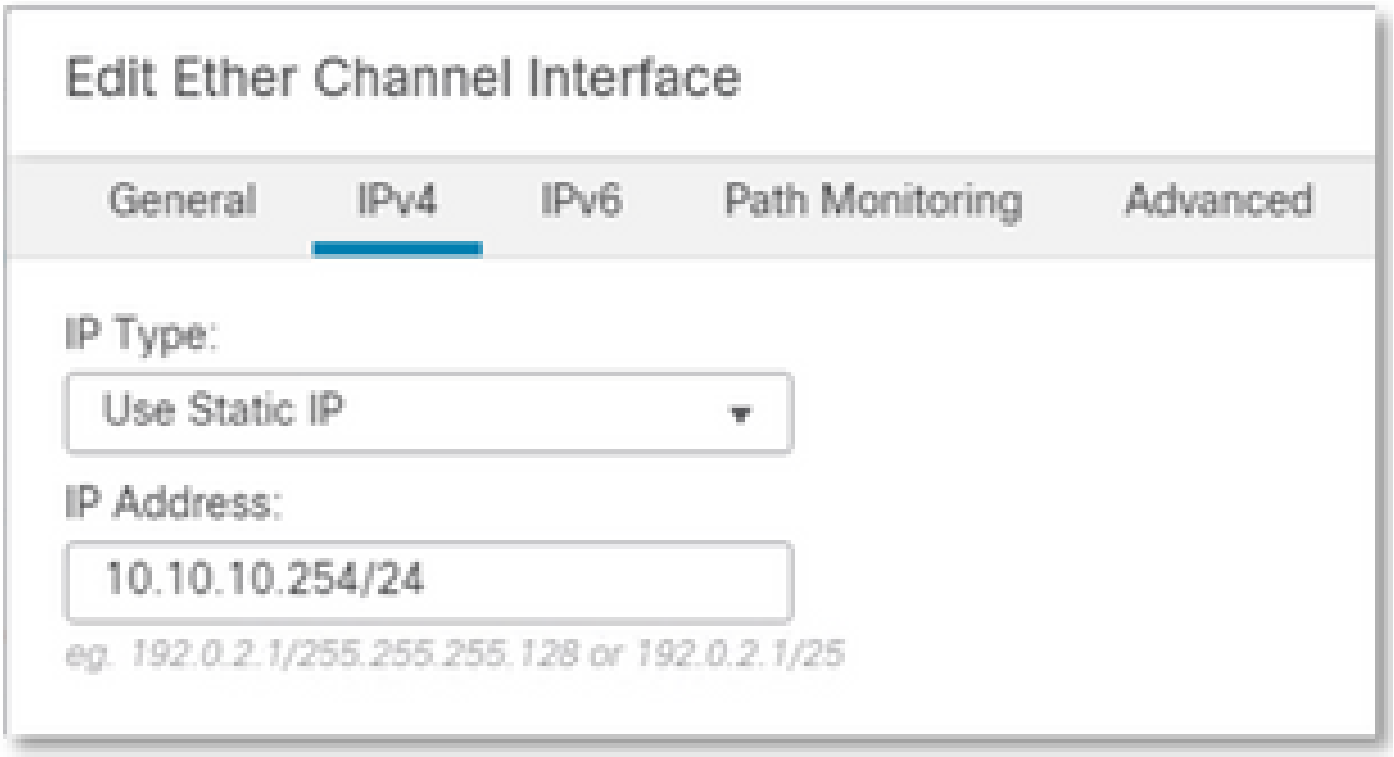

Edit Ether Channel Interface
General
IPv4
IPv6
Path Monitoring
Advanced
Name:
Inside
Enabled
Management Only
Description:
Mode:
None
Security Zone:
Inside-Zone



- 配置外部区域的外部接口成员。

例如，使用IP地址10.10.10.254配置接口并将其命名为Outside。此外部接口面向外部网络。


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

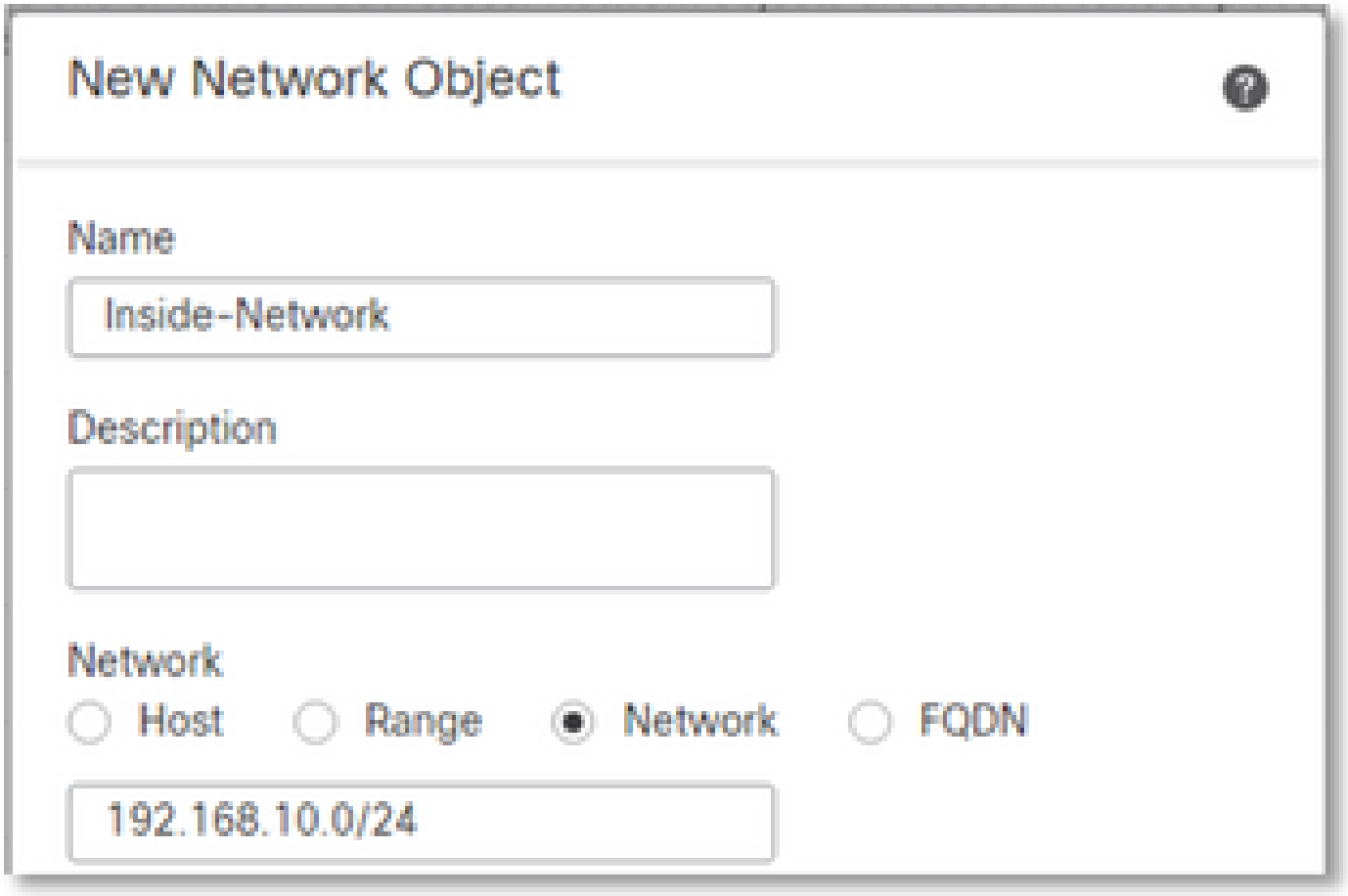


网络对象配置

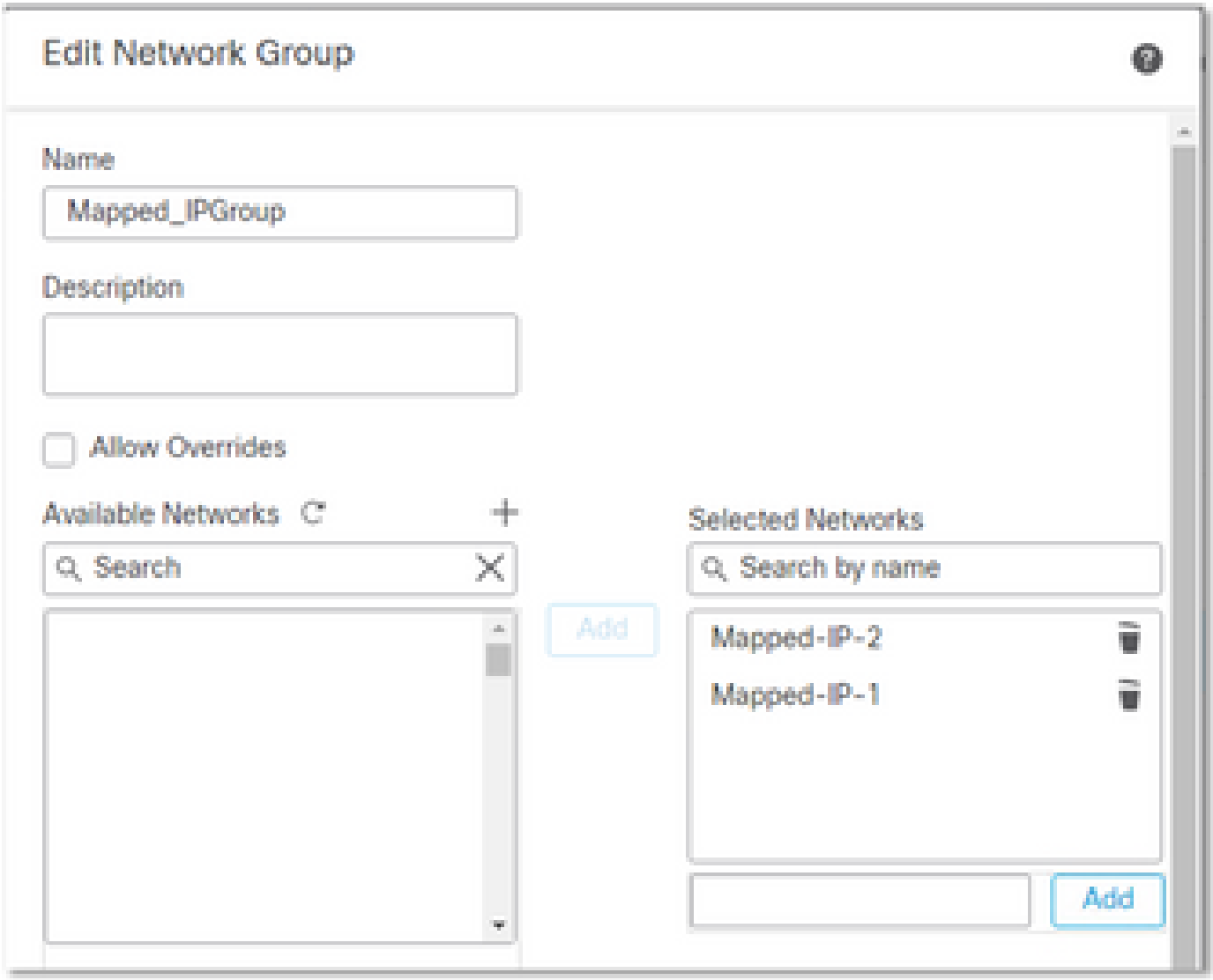
即使集群PAT可以与出口接口或单个IP配合使用以映射所有流量，最佳实践是使用一个IP地址池，该IP地址池的IP地址数量至少与集群中的FTD设备数量相同。

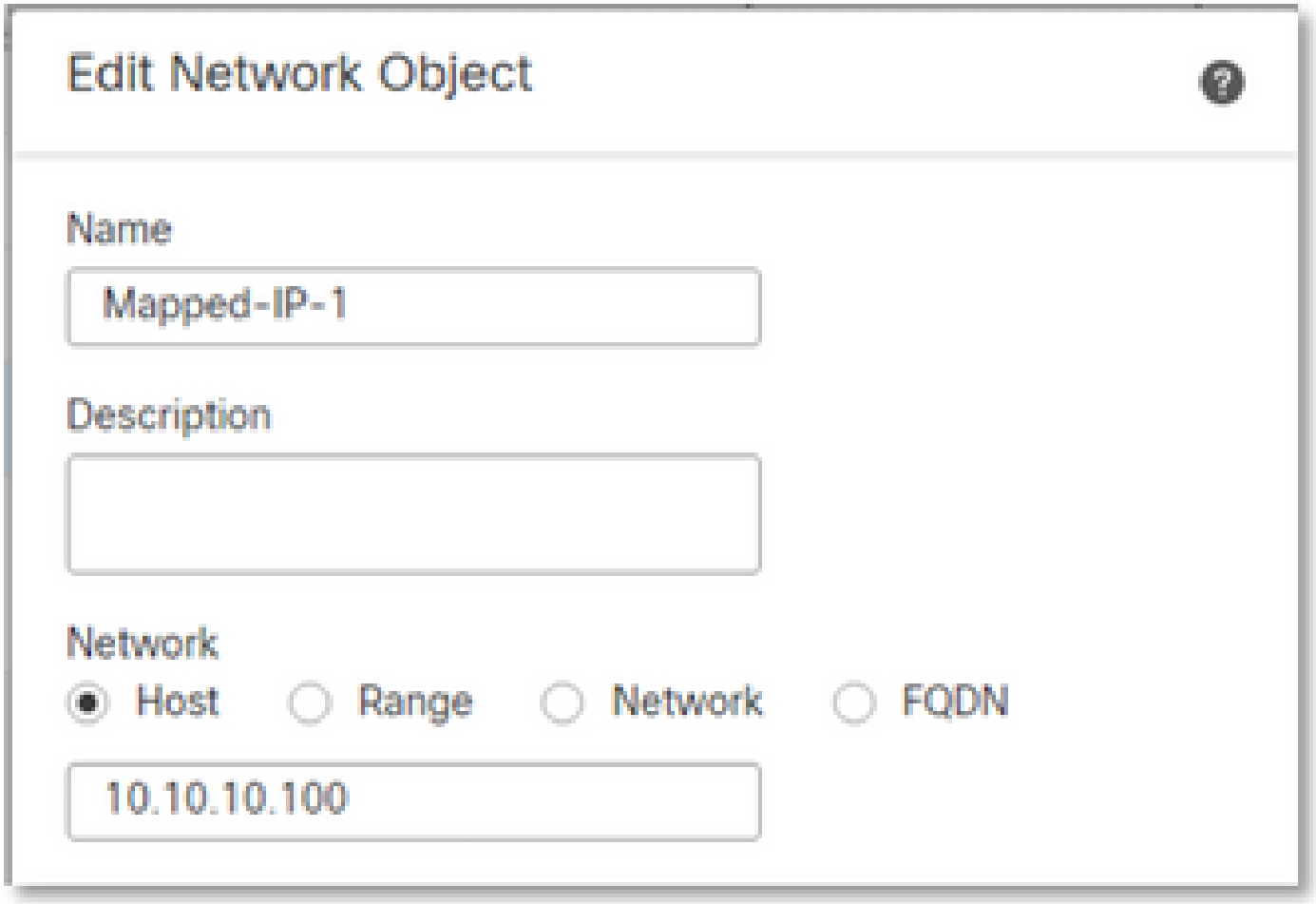
例如，用于实际IP地址和映射IP地址的网络对象分别为Inside-Network和Mapped-IPGroup。

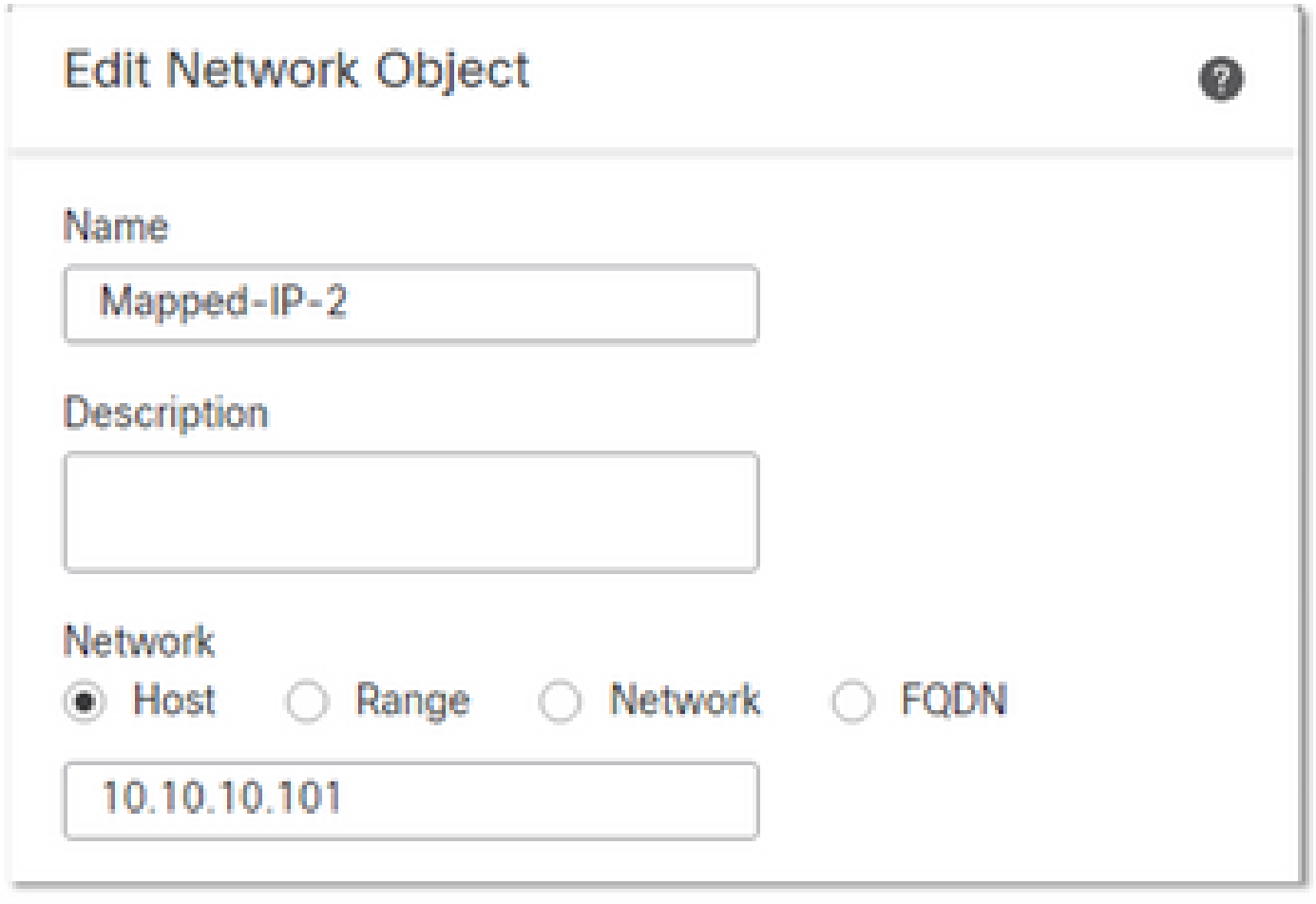
Inside-Network表示内部网络192.168.10.0/24。



Mapped-IPGroup（由Mapped-IP-1 10.10.10.100和Mapped-IP-2 10.10.10.101组成）用于将所有内部流量映射到外部区域。


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

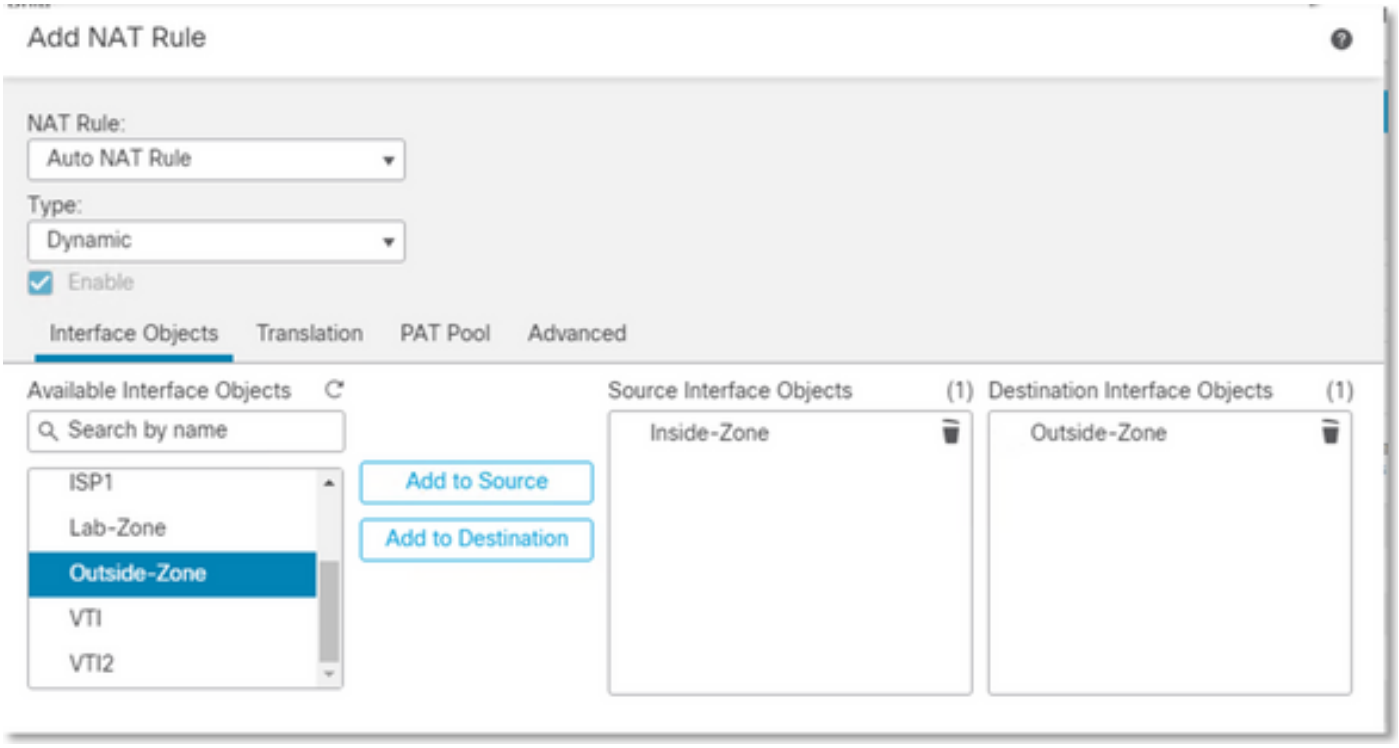

Edit Network Object
Name
Mapped-IP-1
Description
Network
Host
Range
Network
FQDN
10.10.10.100

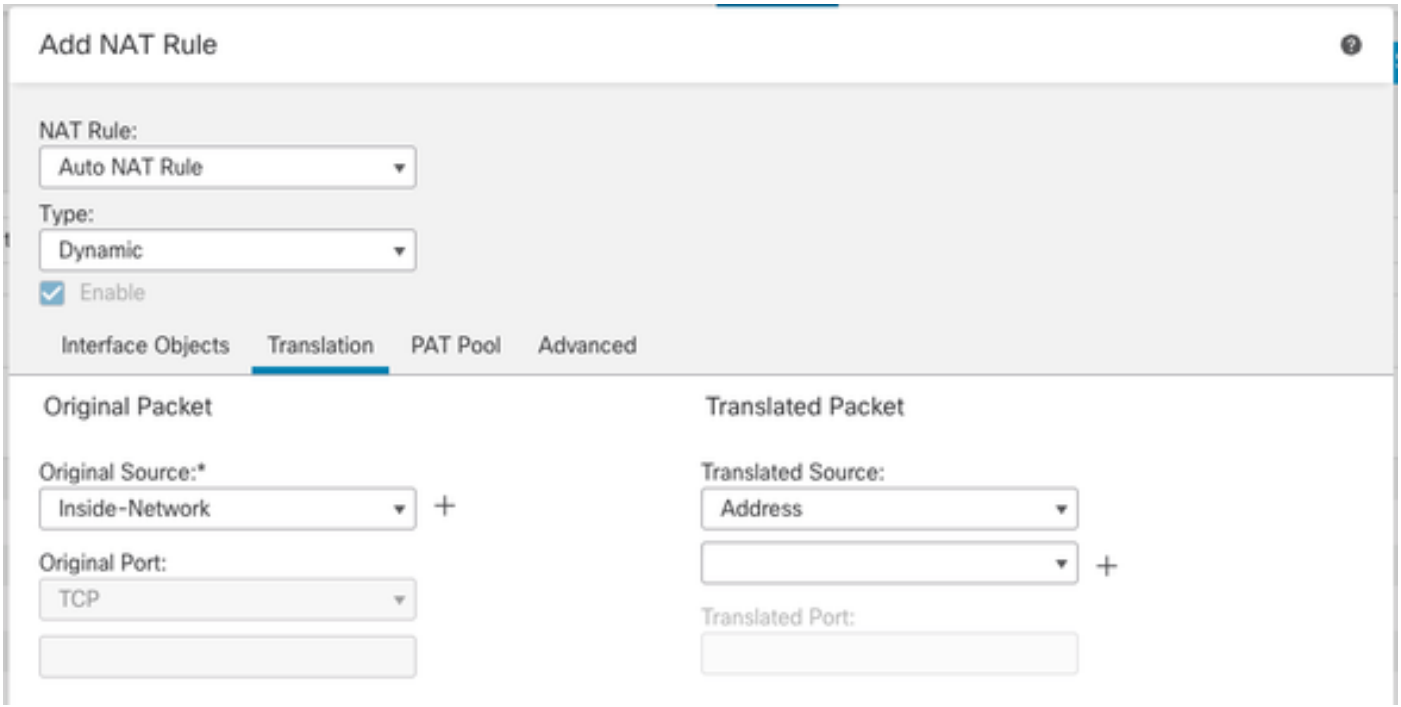

Edit Network Object
Name
Mapped-IP-2
Description
Network
Host
Range
Network
FQDN
10.10.10.101

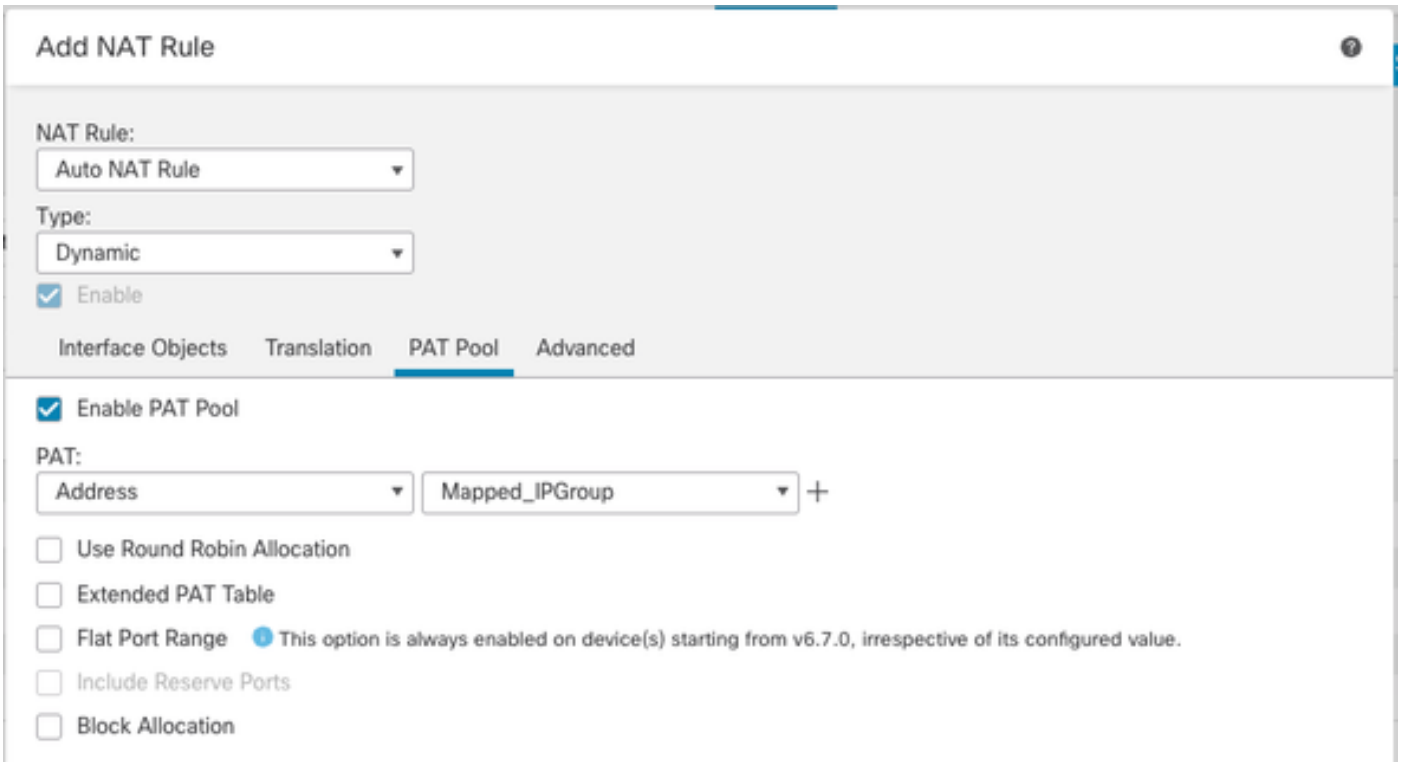
动态PAT配置

- 为出站流量配置动态NAT规则。此NAT规则将内部网络子网映射到外部NAT池。

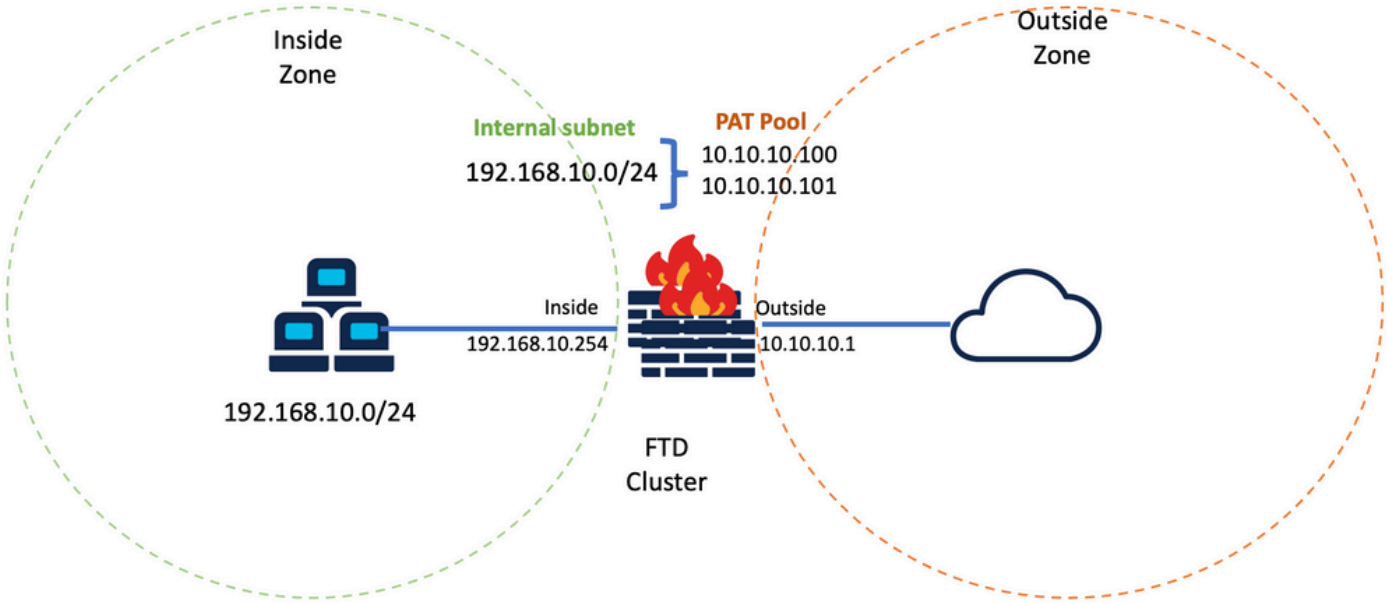
例如，从内部网络到外部区域的内部区域流量被转换为映射的IPGroup池。







最终配置



最终实验设置。

验证

使用本部分可确认配置能否正常运行。

检验IP接口和NAT配置

<#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
```

检验端口块分配

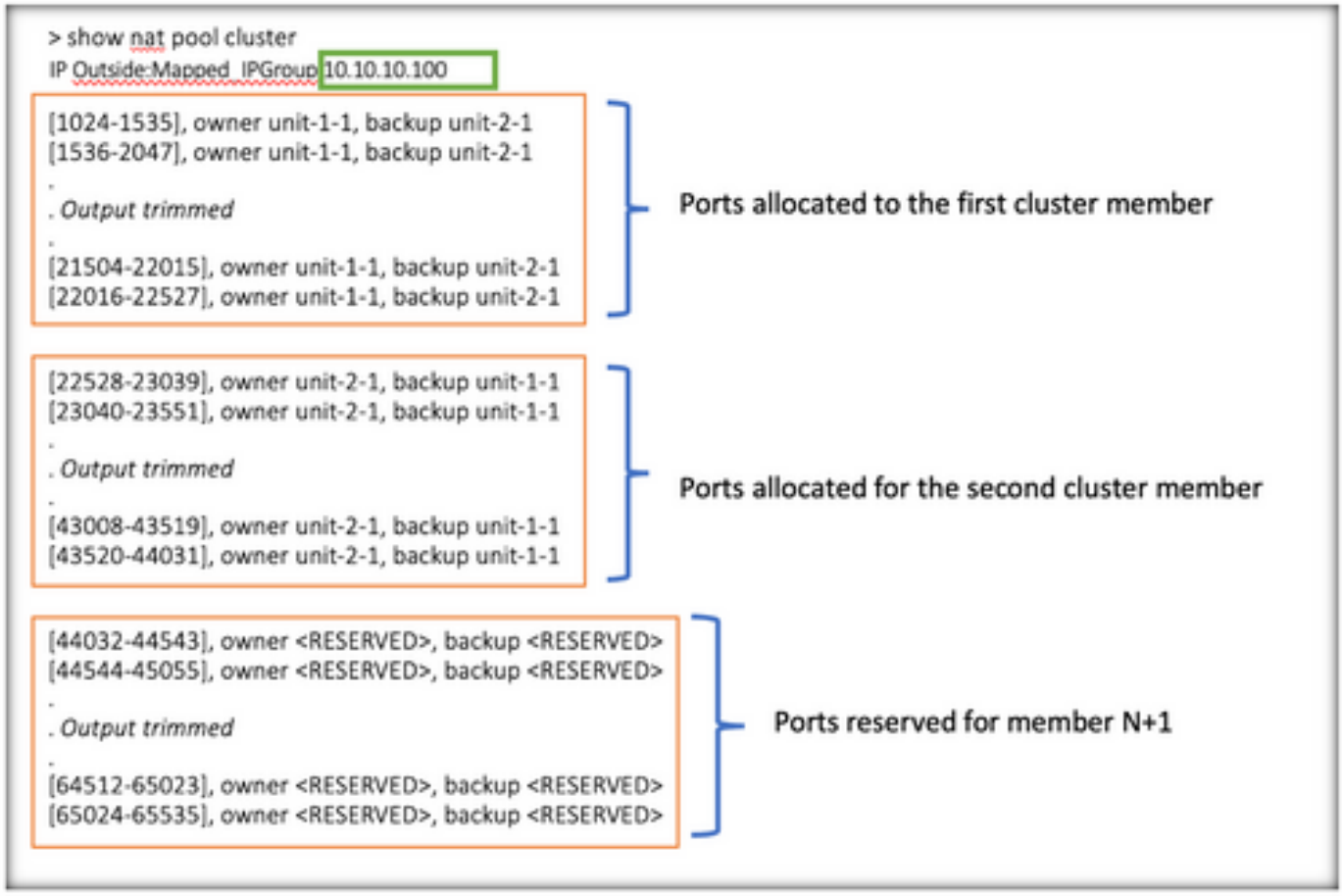
在Firepower 7.0之后，改进的PAT端口块分配可确保控制单元保留端口供加入节点使用，并主动回收未使用的端口。 端口分配的工作原理如下：

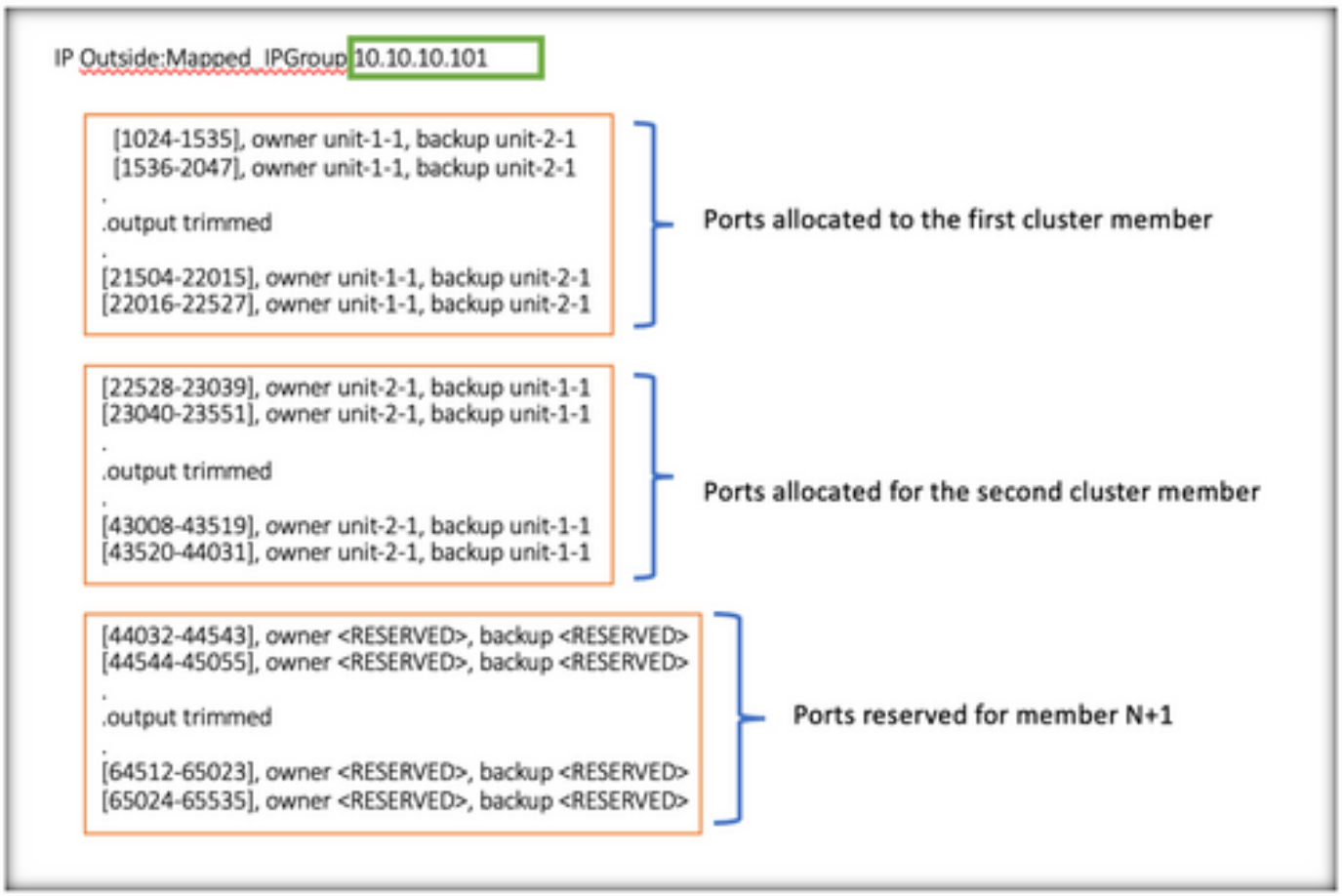
- 在刚刚启动的集群上，控制单元最初拥有50%的端口，其余端口则予以保留。
- 随着更多节点加入集群，每台设备拥有的端口块数量会相应调整。
- 控制单元为(N+1)节点保留端口块，直到集群已满。 集群成员限制由在集群组配置级别下配置的cluster-member-limit 命令定义。
- 默认情况下，cluster-member-limit为16。
  <#root>

  ```
  > show cluster info

  Cluster FTD-Cluster: On
  Interface mode: spanned

  Cluster Member Limit : 16


  [...]
  ```

- 当集群成员数量达到配置的值时，所cluster-member-limit有端口块将分布到集群成员之间。

例如，在由两台设备(N=2)组成的集群组中，集群成员限制的默认值为16，可以观察到为N+1个成员定义了端口分配，在本例中为3。这会保留一些端口供下一设备使用，直到达到最大集群限制。

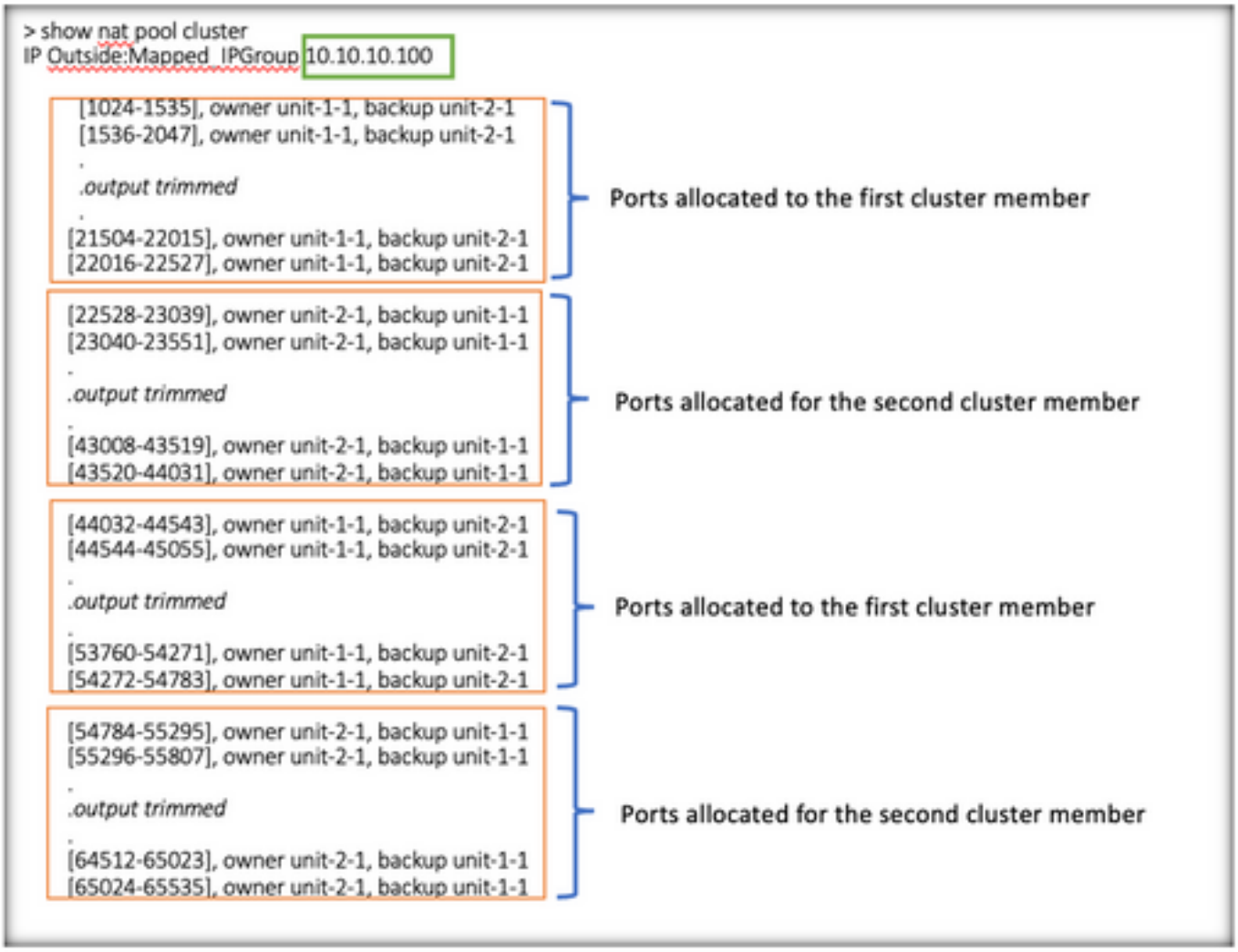

> show nat pool cluster
IP Outside:Mapped IPGroup 10.10.10.100
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
. Output trimmed
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1
Ports allocated to the first cluster 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

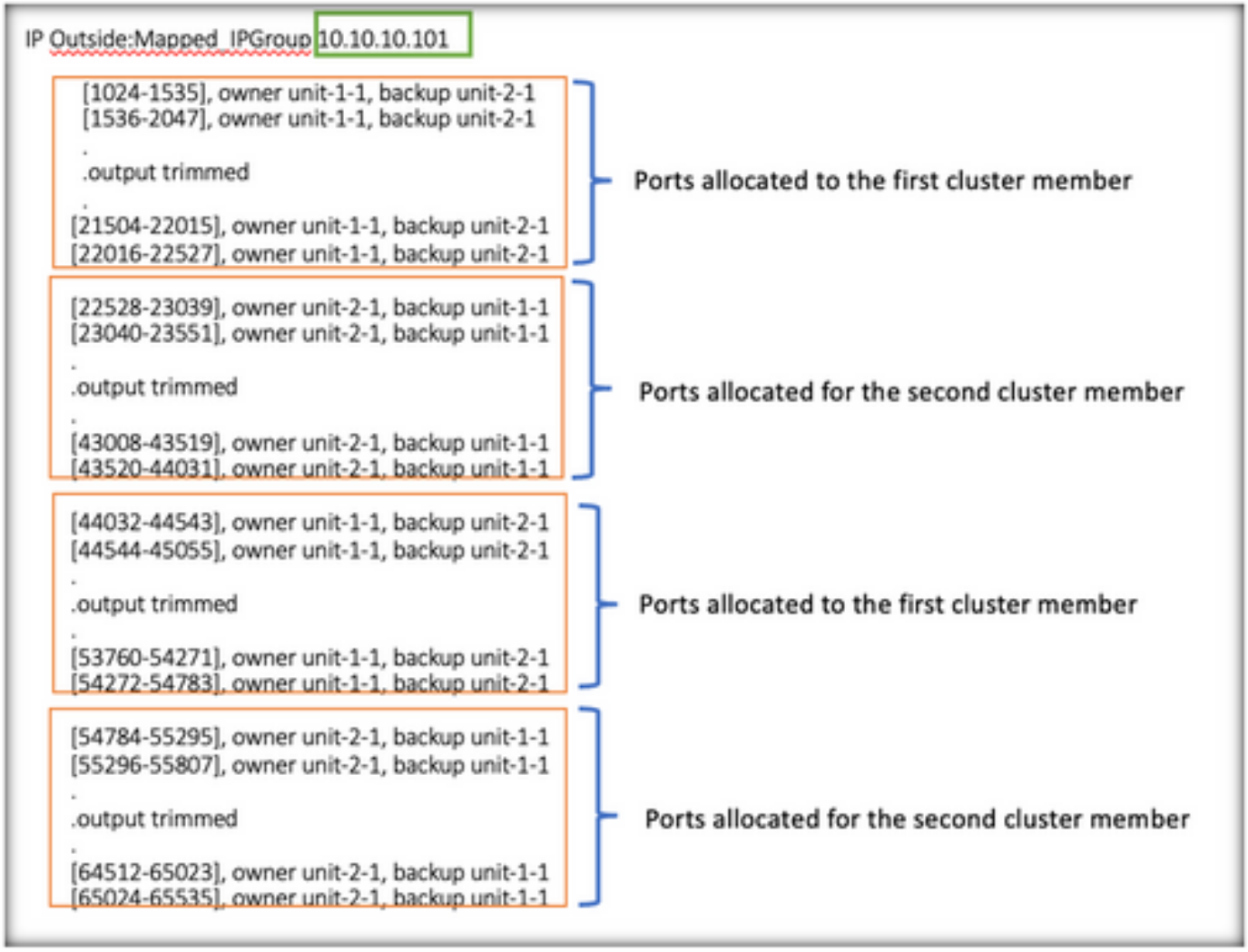

IP Outside:Mapped IPGroup 10.10.10.101
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
.output trimmed
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1
Ports allocated to the first cluster member
[22528-23039], owner 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
```

此外，最佳做法是将配置为与**cluster-member-limit** 为集群部署计划的设备数量匹配。

例如，在由两台设备(N=2)组成的集群组中，集群成员限制值为2，可以观察到端口分配均匀分布在所有集群设备上。保留的所有端口均未保留。






```
> 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
```

检验端口块回收

- 每当新节点加入或离开集群时，必须将未使用的端口和来自所有单元的超额端口块释放给控制单元。
- 如果端口块已在使用中，则使用最少的端口块将标记为回收。
- 已回收的端口块上不允许新连接。当最后一个端口被清除时，它们被释放到控制单元。

```
> 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
```

故障排除命令

本部分提供的信息可用于对配置进行故障排除。

- 检查配置的cluster-member-limit值：

<#root>

> show cluster info

Cluster FTD-Cluster: On
Interface mode: spanned

Cluster Member Limit : 2

[...]

> show running-config cluster

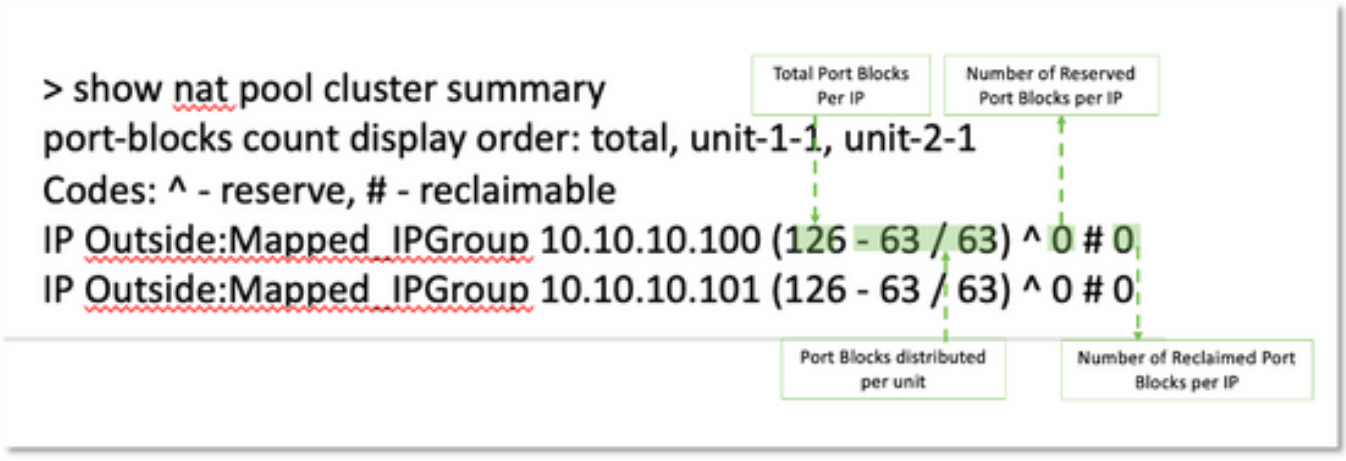
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0

cluster-member-limit 2
[...]

- 显示集群中设备之间的端口块分布摘要：

<#root>

> show nat pool cluster summary



- 显示每个PAT地址的端口块当前分配给所有者和备用单元：

<#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
[...]
```

- 显示与端口块的分发和使用相关的信息：

<#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
[...]
```

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。