瞭解適用於FTD叢集7.0的動態PAT上的連線埠分配

目錄

簡介

本文檔介紹在版本7.0及更高版本之後，基於埠塊的分發如何在Dynamic PAT for Firewall Cluster上運行。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆上的網路位址轉譯(NAT)

採用元件

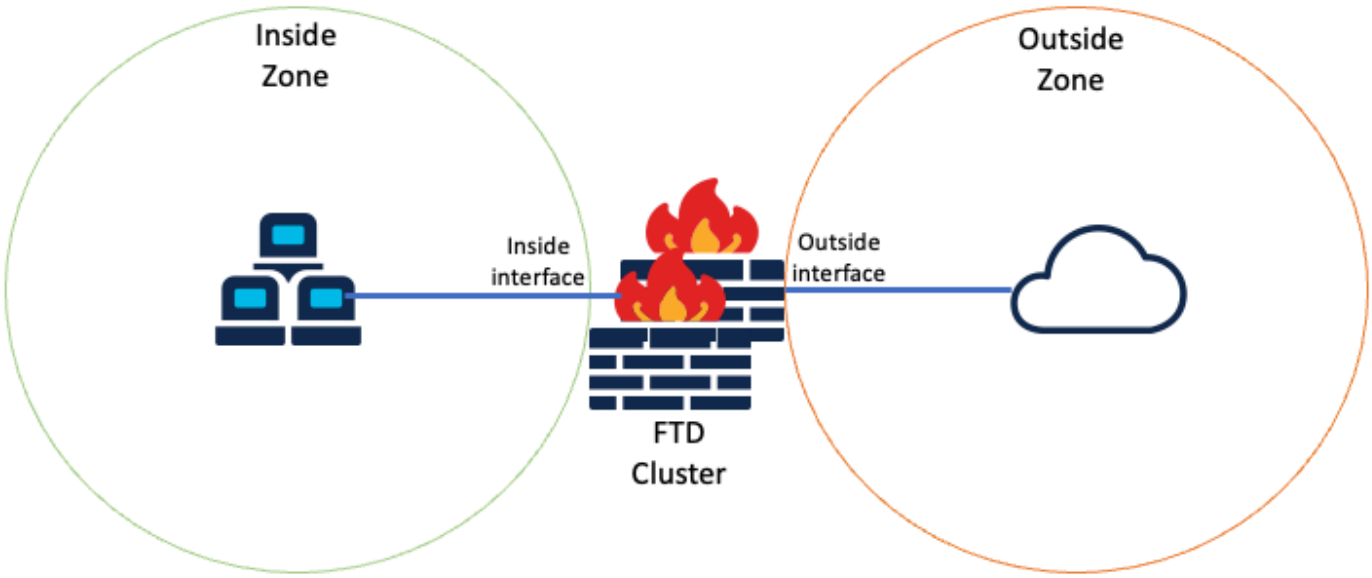
本文中的資訊係根據以下軟體和硬體版本：

- Firepower管理中心7.3.0
- Firepower威脅防禦7.2.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表

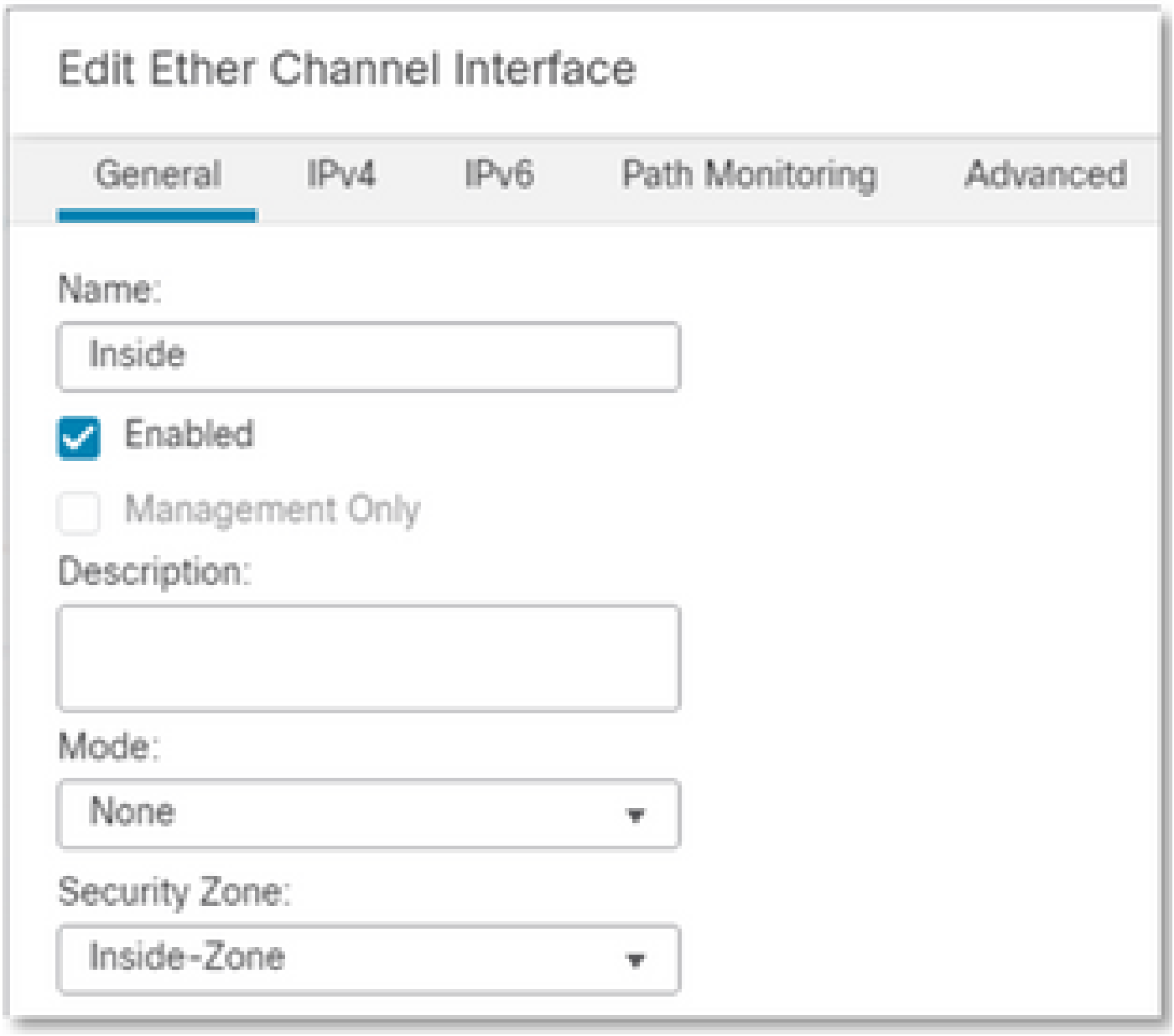


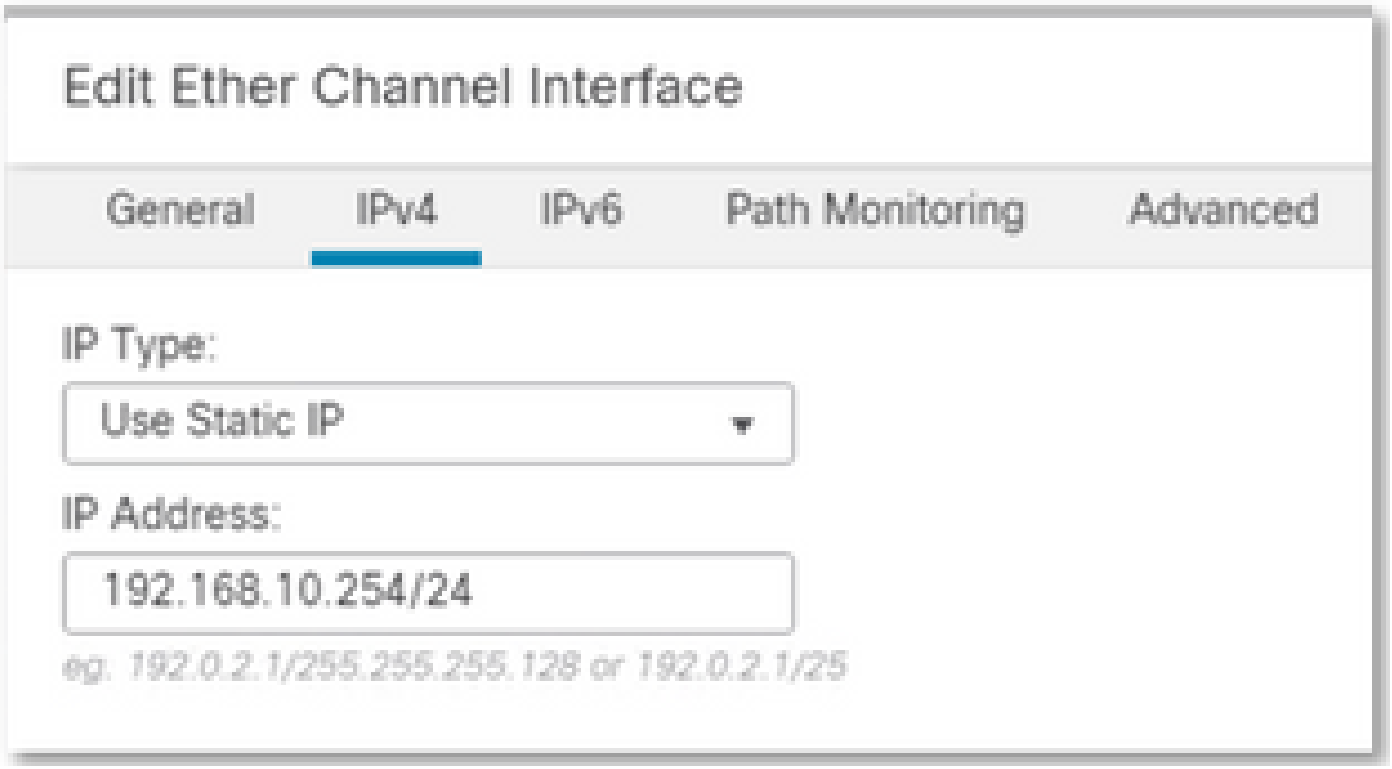
邏輯拓撲

介面配置

- 配置Inside Zone的Inside介面成員。

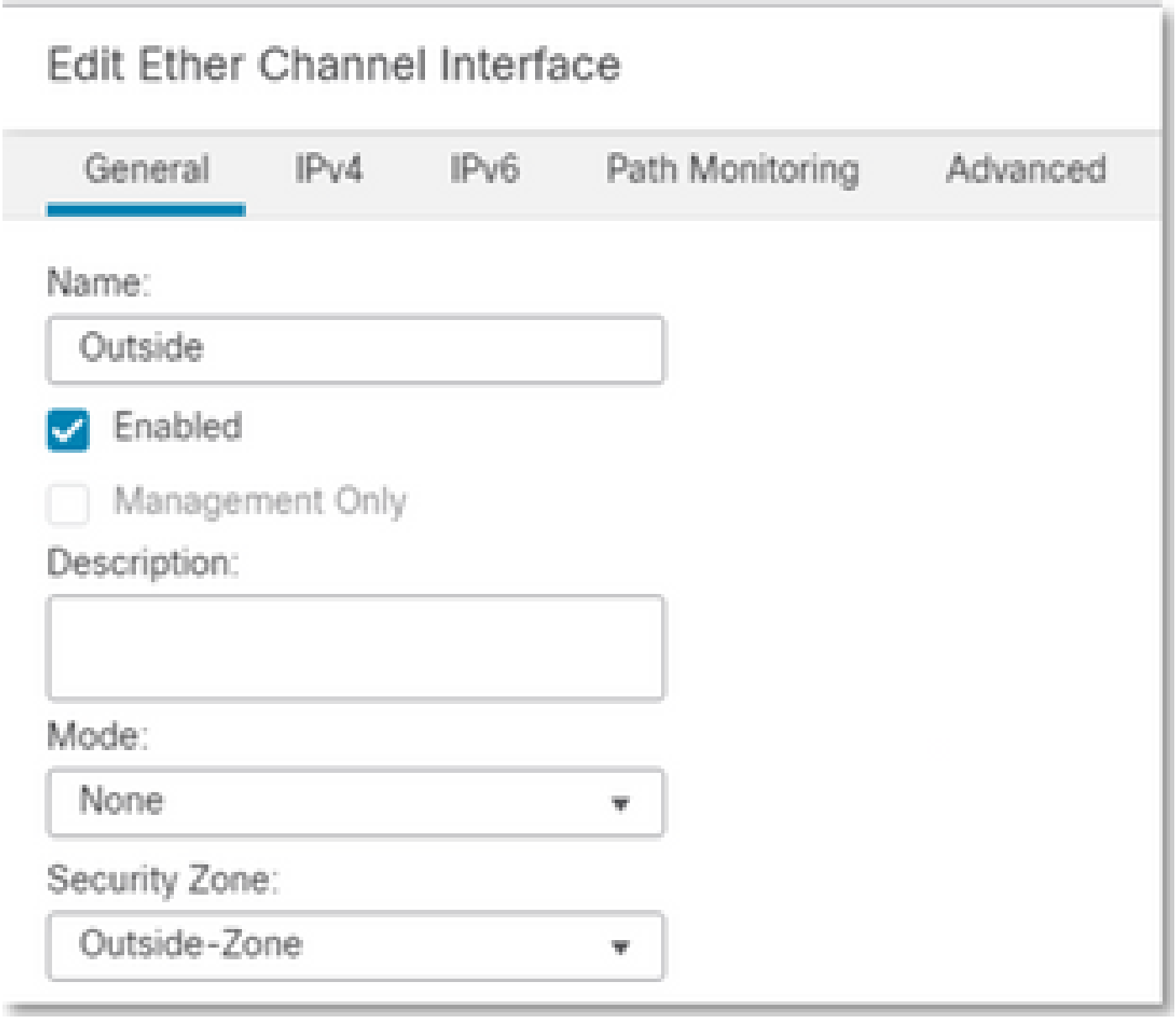
例如，使用IP地址192.168.10.254配置介面並將其命名為Inside。此Inside介面是內部網路192.168.10.0/24的網關。

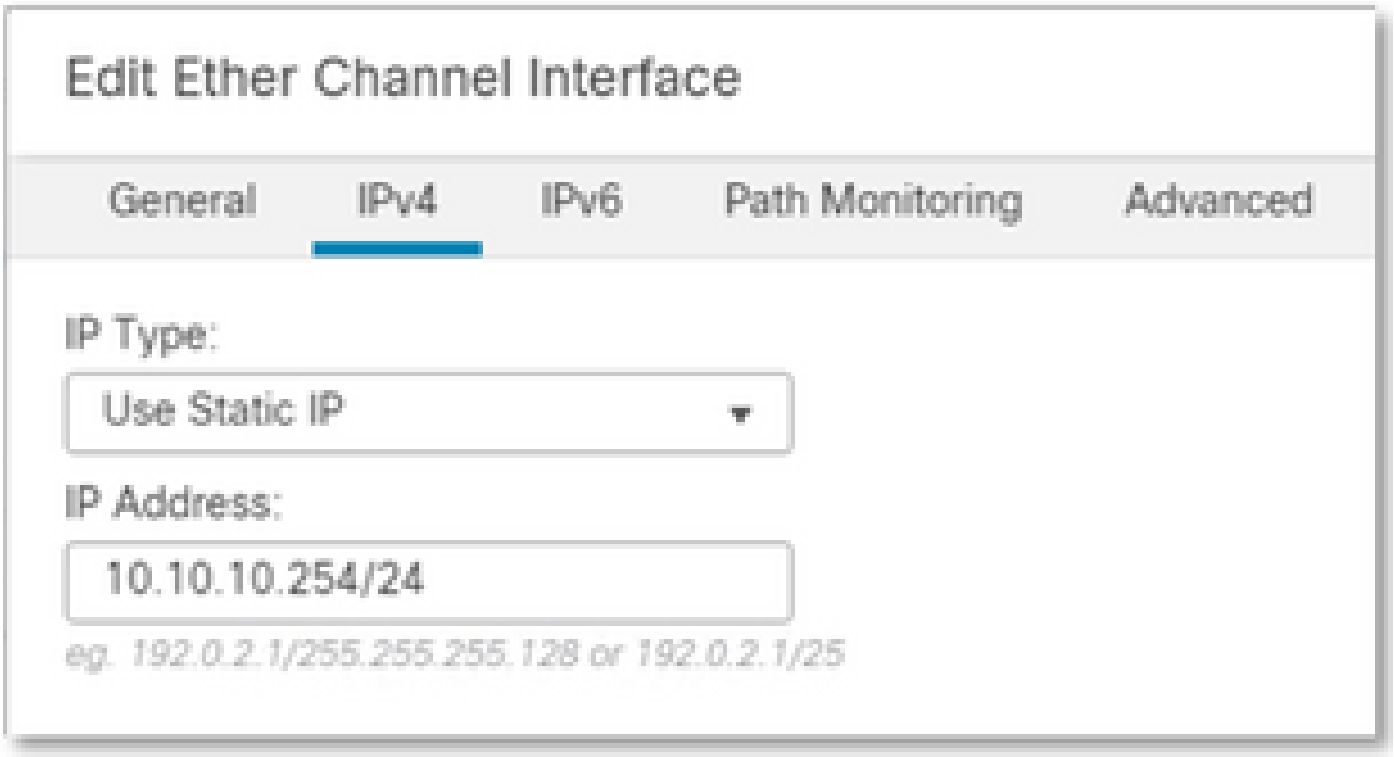

Edit Ether Channel Interface
General
IPv4
IPv6
Path Monitoring
Advanced
Name:
Inside
Enabled
Management Only
Description:
Mode:
None
Security Zone:
Inside-Zone



- 配置外部區域的外部介面成員。

例如，使用IP地址10.10.10.254配置介面並將其命名為Outside。此外部介面面向外部網路。


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

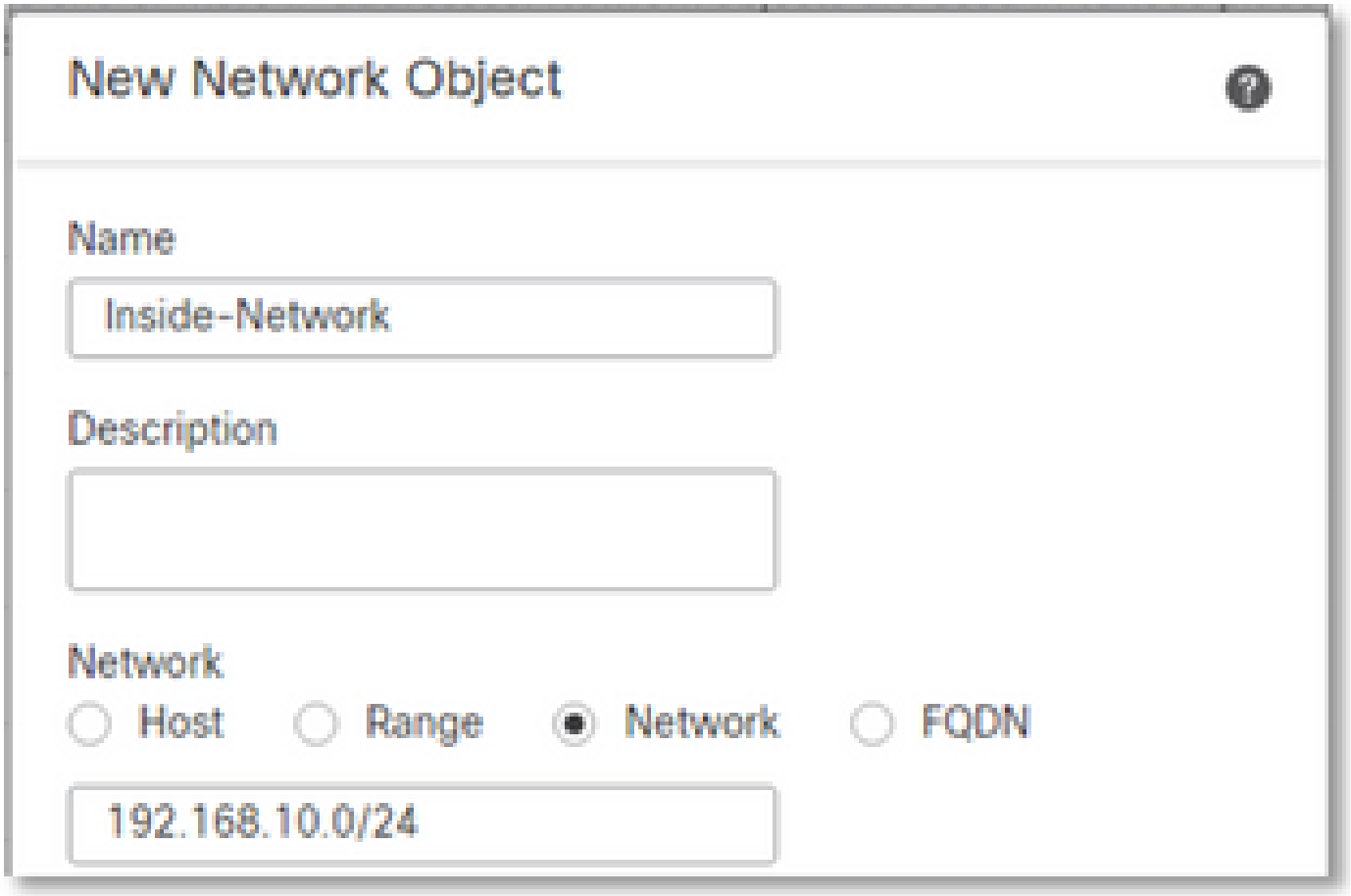


網路對象配置

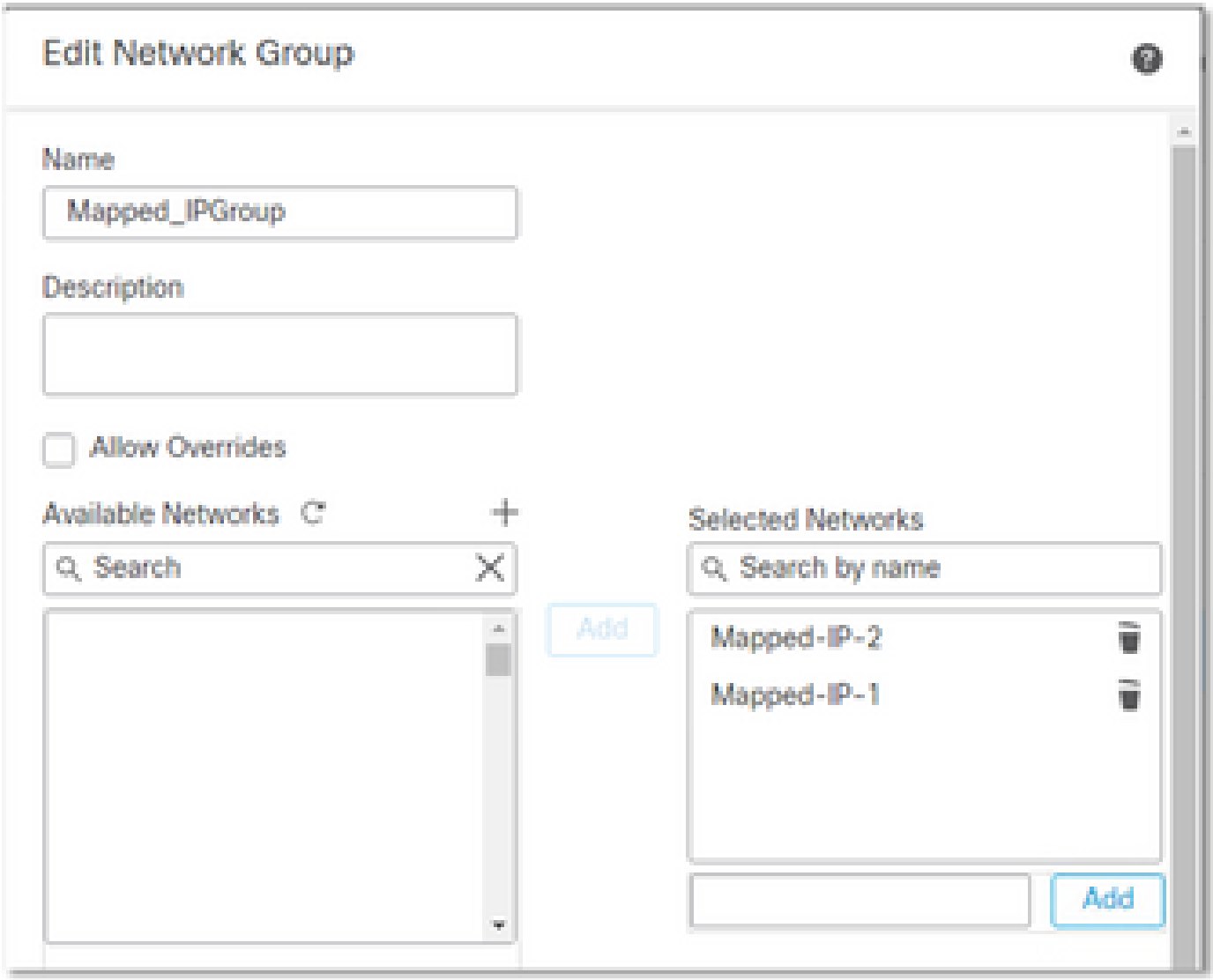
即使群集PAT可以使用出口介面或單個IP來對映所有流量，最佳實踐是使用一個IP地址池，該IP地址池的IP數量至少與群集中FTD裝置的數量相同。

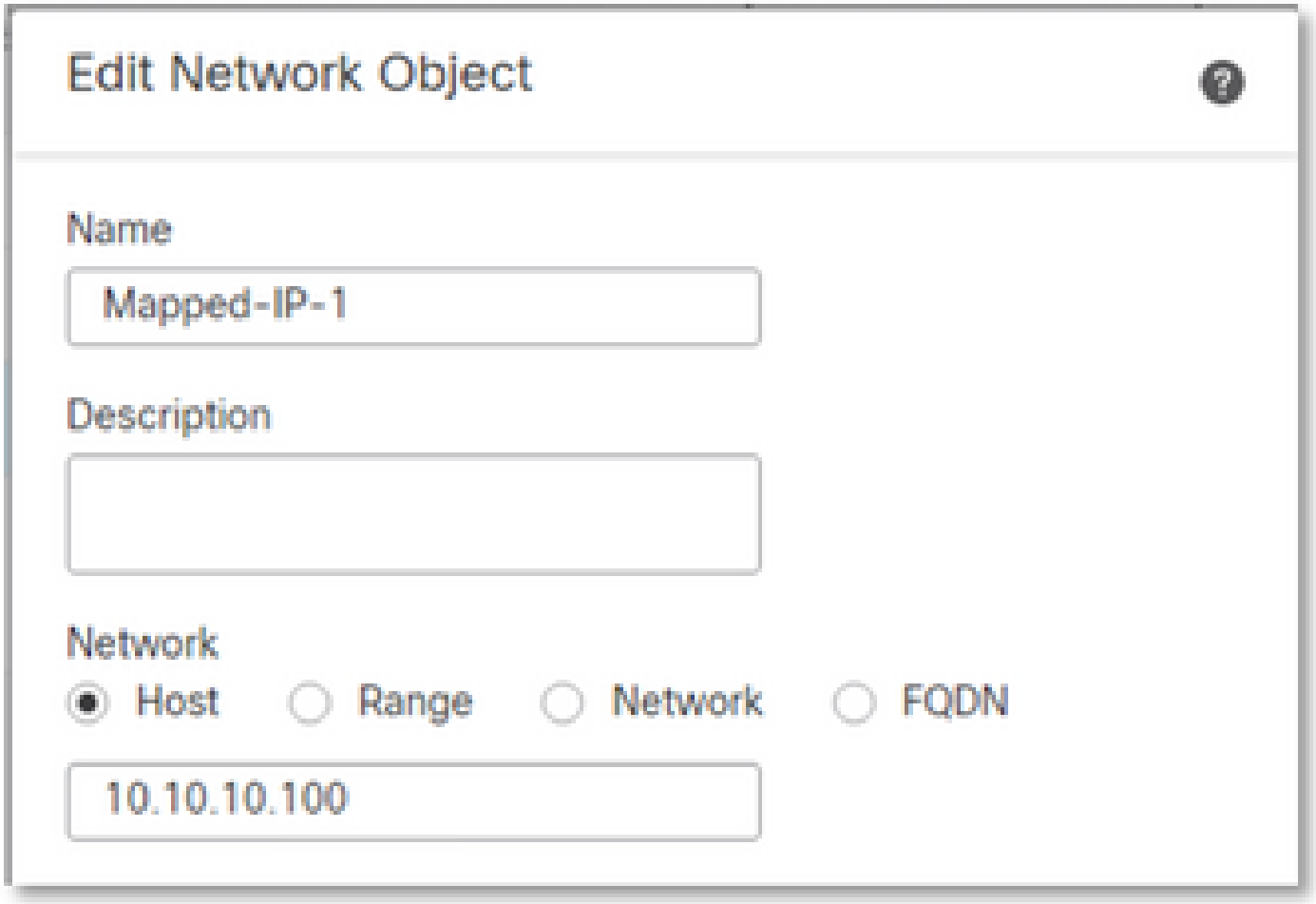
例如，用於Real和對映IP地址的網路對象分別為Inside-Network和Mapped-IPGroup。

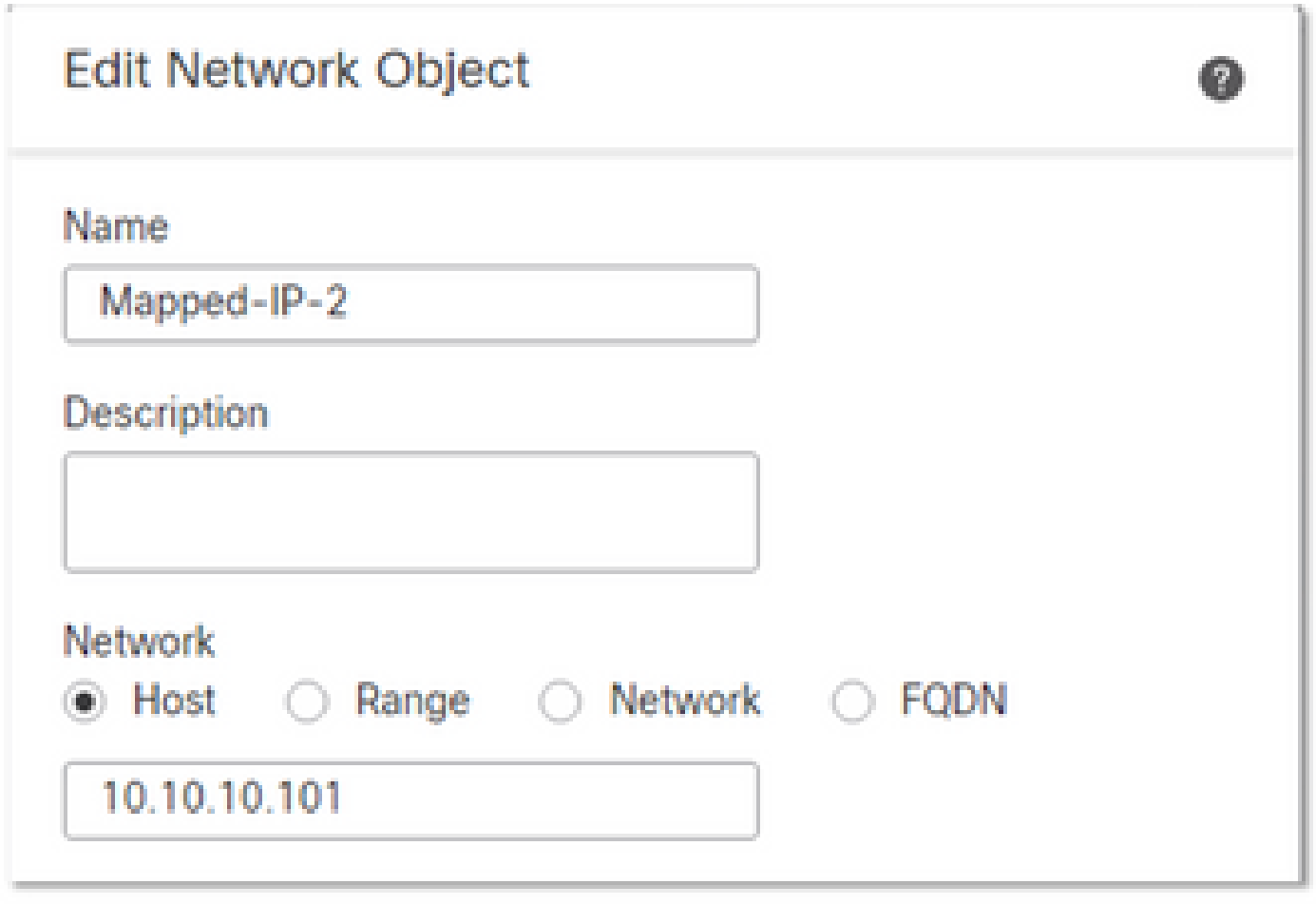
Inside-Network表示內部網路192.168.10.0/24。



Mapped-IPGroup（由Mapped-IP-1 10.10.10.100和Mapped-IP-2 10.10.10.101組成）用於將所有內部流量對映到外部區域。


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

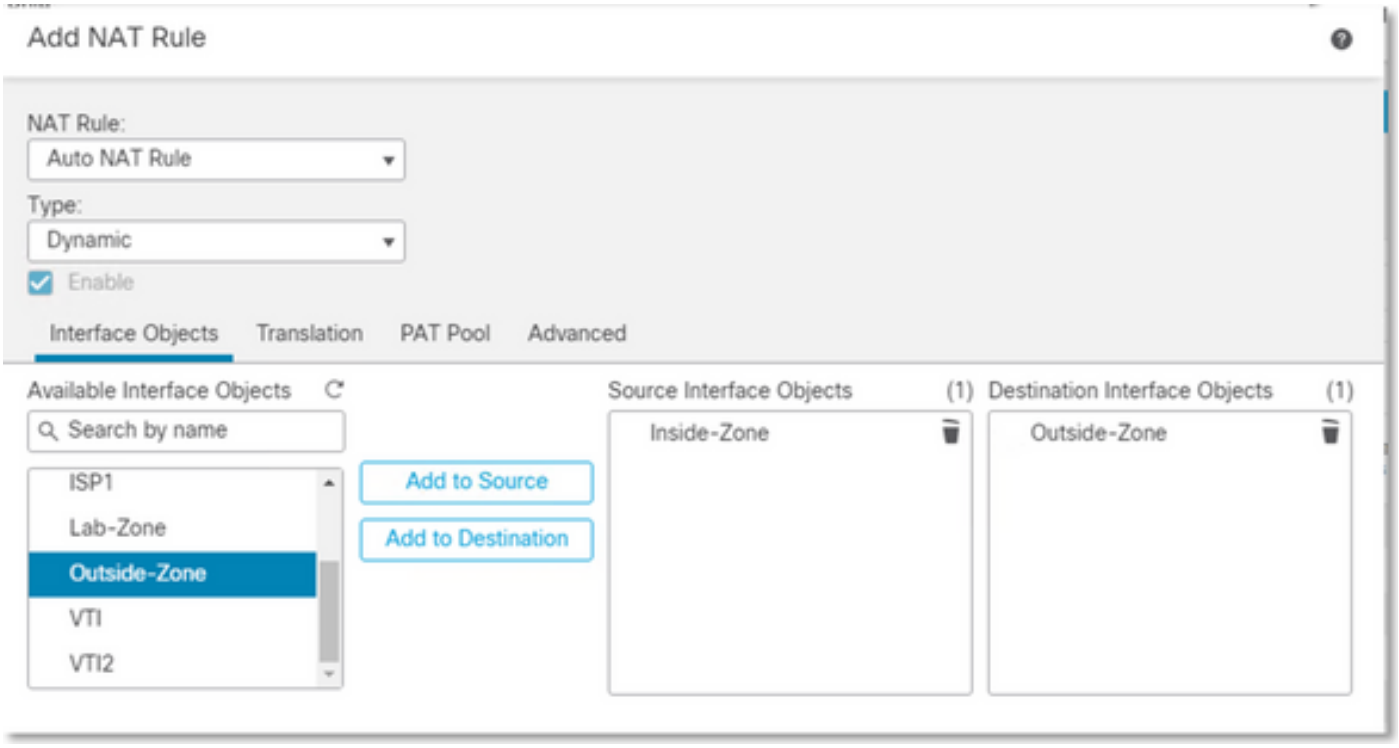

Edit Network Object
Name
Mapped-IP-1
Description
Network
Host
Range
Network
FQDN
10.10.10.100

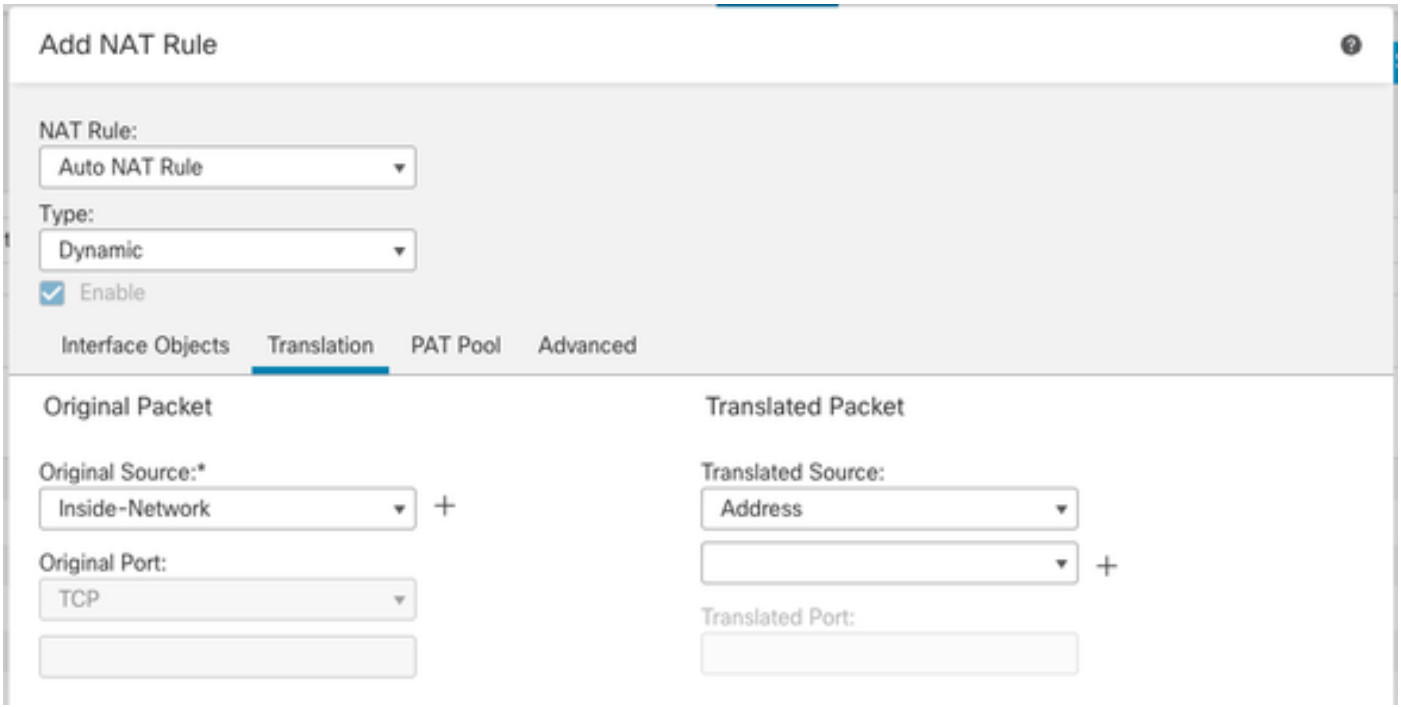

Edit Network Object
Name
Mapped-IP-2
Description
Network
Host
Range
Network
FQDN
10.10.10.101

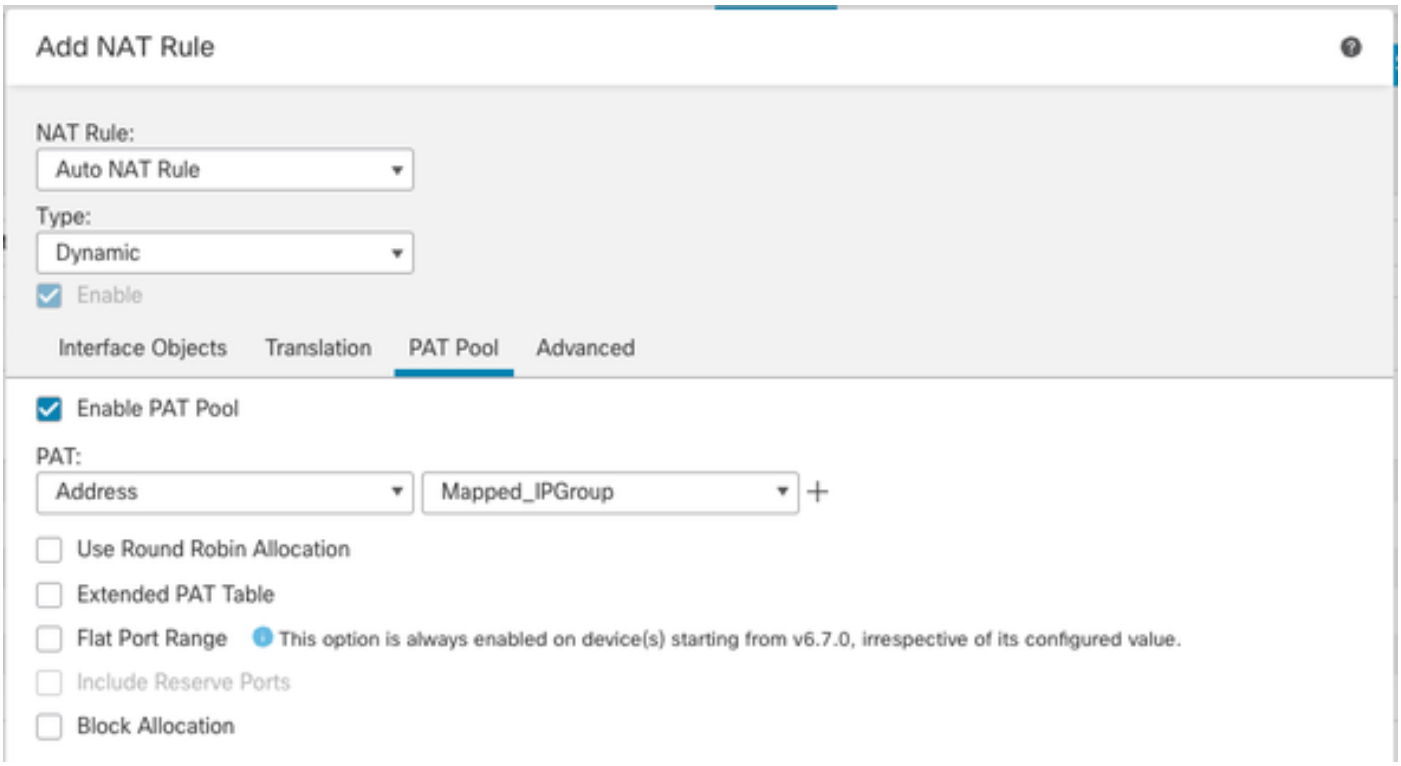
動態PAT配置

- 為出站流量配置動態NAT規則。此NAT規則將內部網路子網對映到外部NAT池。

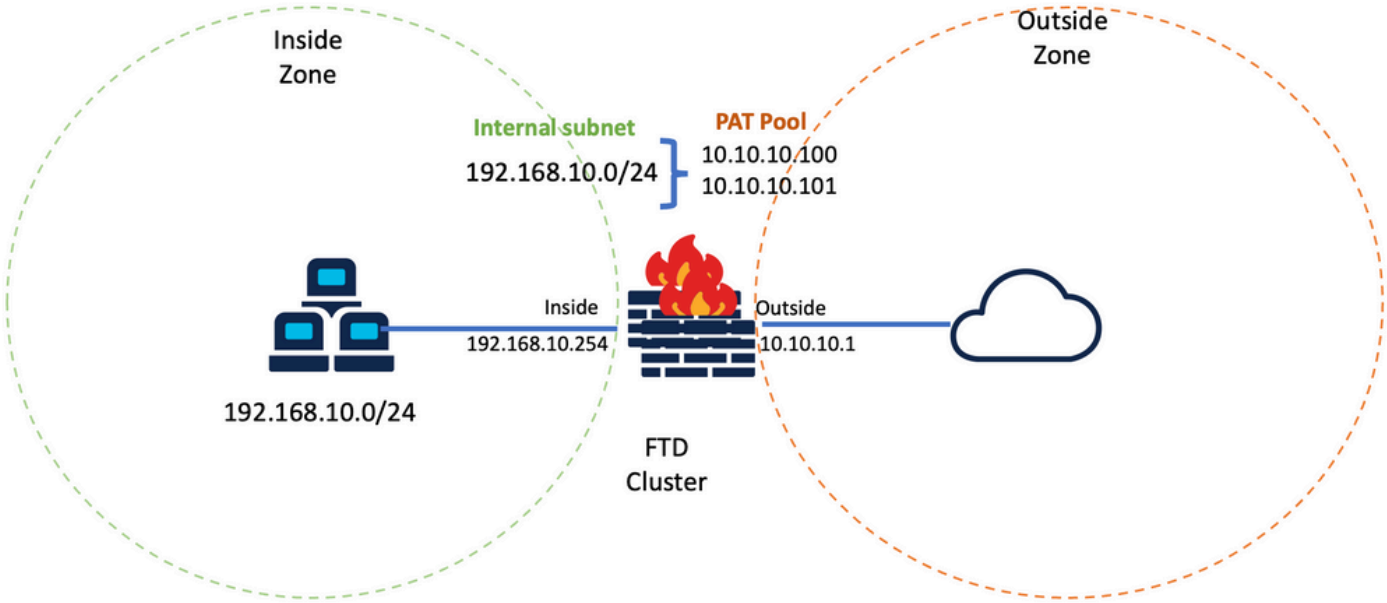
例如，從內部網路到外部區域的內部區域流量轉換為對映的IPGroup池。







最終配置



最終實驗設定。

驗證

使用本節內容，確認您的組態是否正常運作。

檢驗IP介面和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
```

驗證埠塊分配

在Firepower 7.0之後，改進的PAT埠塊分配可確保控制單元將埠保留為用於加入節點的保留狀態，並主動回收未使用的埠。 以下是連線埠分配的運作方式：

- 在剛剛啟動的群集上，控制單元最初擁有50%的埠，其餘埠是保留的。
- 隨著更多節點加入群集，每個單元擁有的埠塊數量也會隨之調整。
- 控制單元為(N+1)節點保留埠塊，直到集群已滿。 集群成員限制由在集群組配置級別下配置的 cluster-member-limit 命令定義。
- 預設情況下，cluster-member-limit為16。
  <#root>

  ```
  > show cluster info
  ```

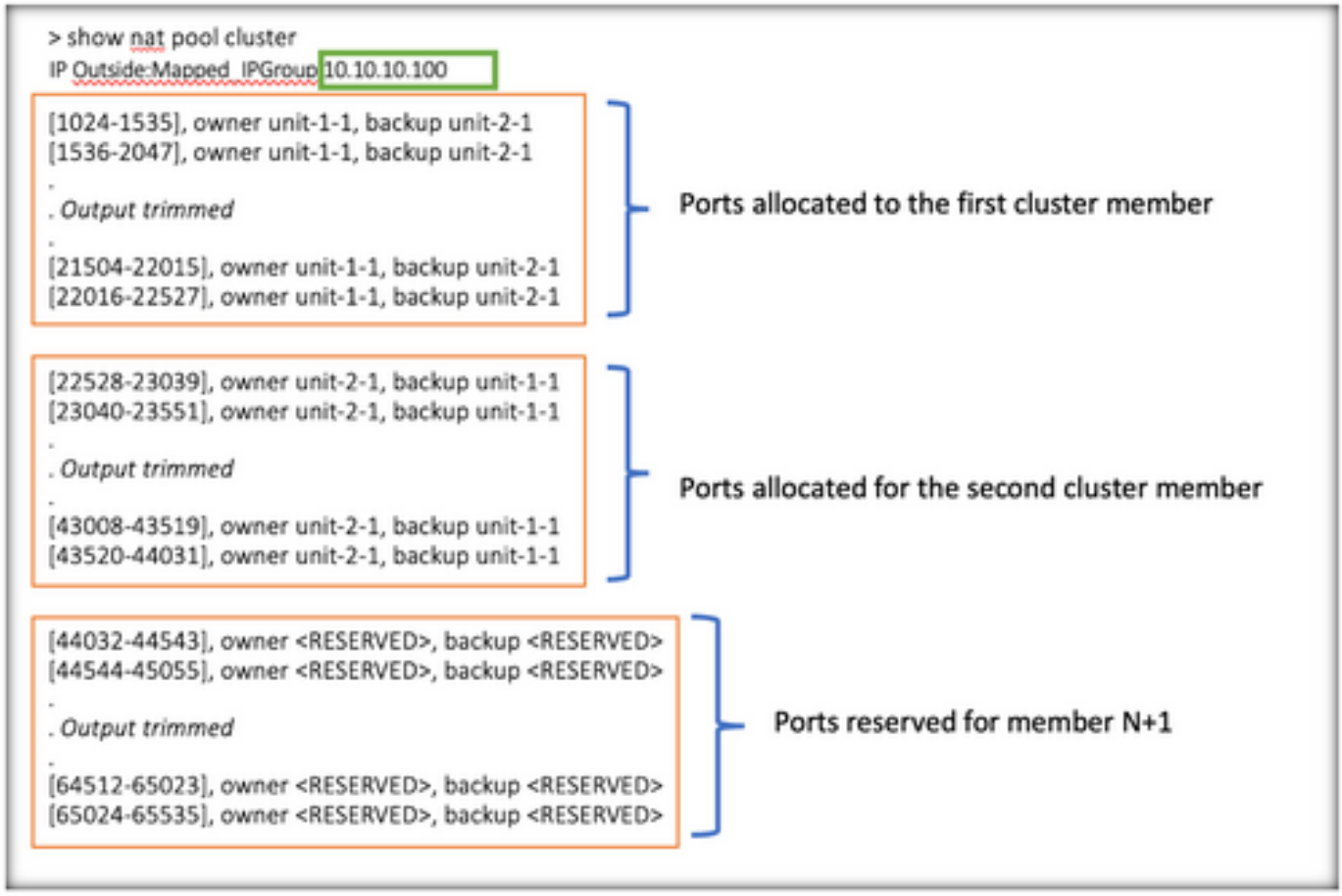
  ```
  Cluster FTD-Cluster: On
  Interface mode: spanned
  ```

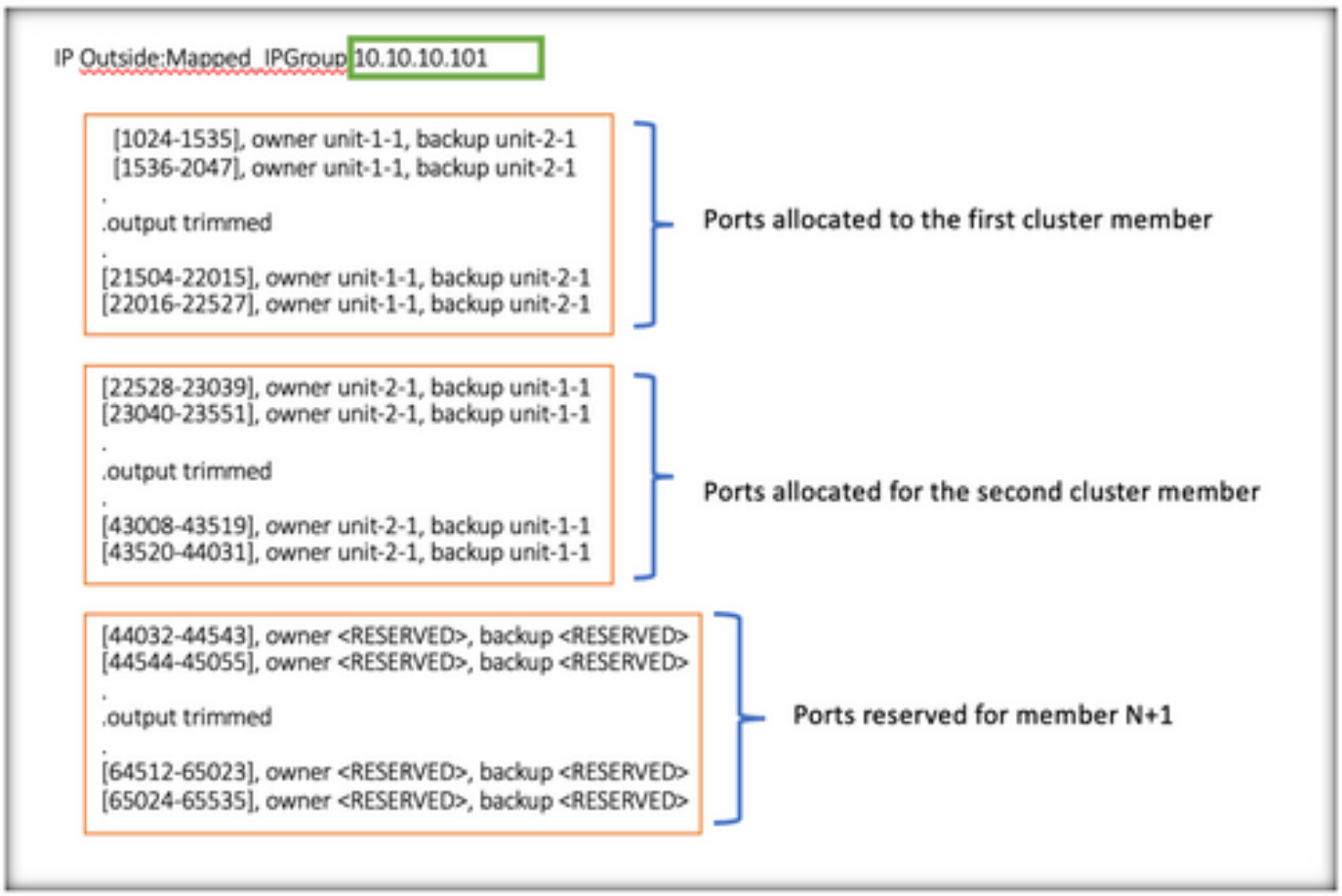
  ```
  Cluster Member Limit : 16
  ```

  ```
  [...]
  ```

- 當集群成員數量達到配置的值時，所有**cluster-member-limit**埠塊都會分佈到集群成員中。

例如，在由兩個單元(N=2)組成的集群組中，集群成員限制的預設值為16，可以觀察到為N+1個成員定義了埠分配，在本例中為3。這會將某些埠保留給下一個裝置，直到達到最大群集限制。

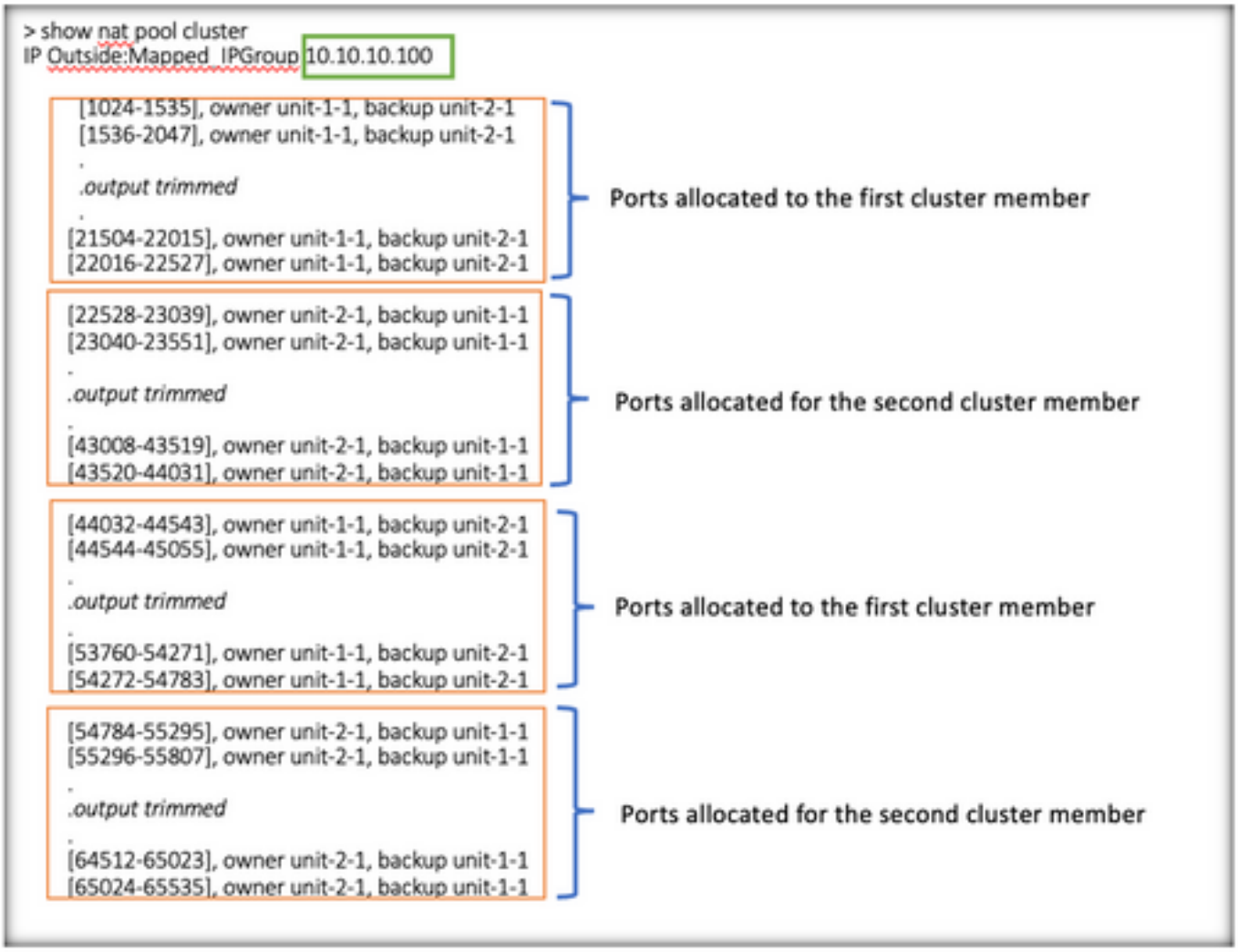

> show nat pool cluster
IP Outside:Mapped IPGroup 10.10.10.100
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
. Output trimmed
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1
Ports allocated to the first cluster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

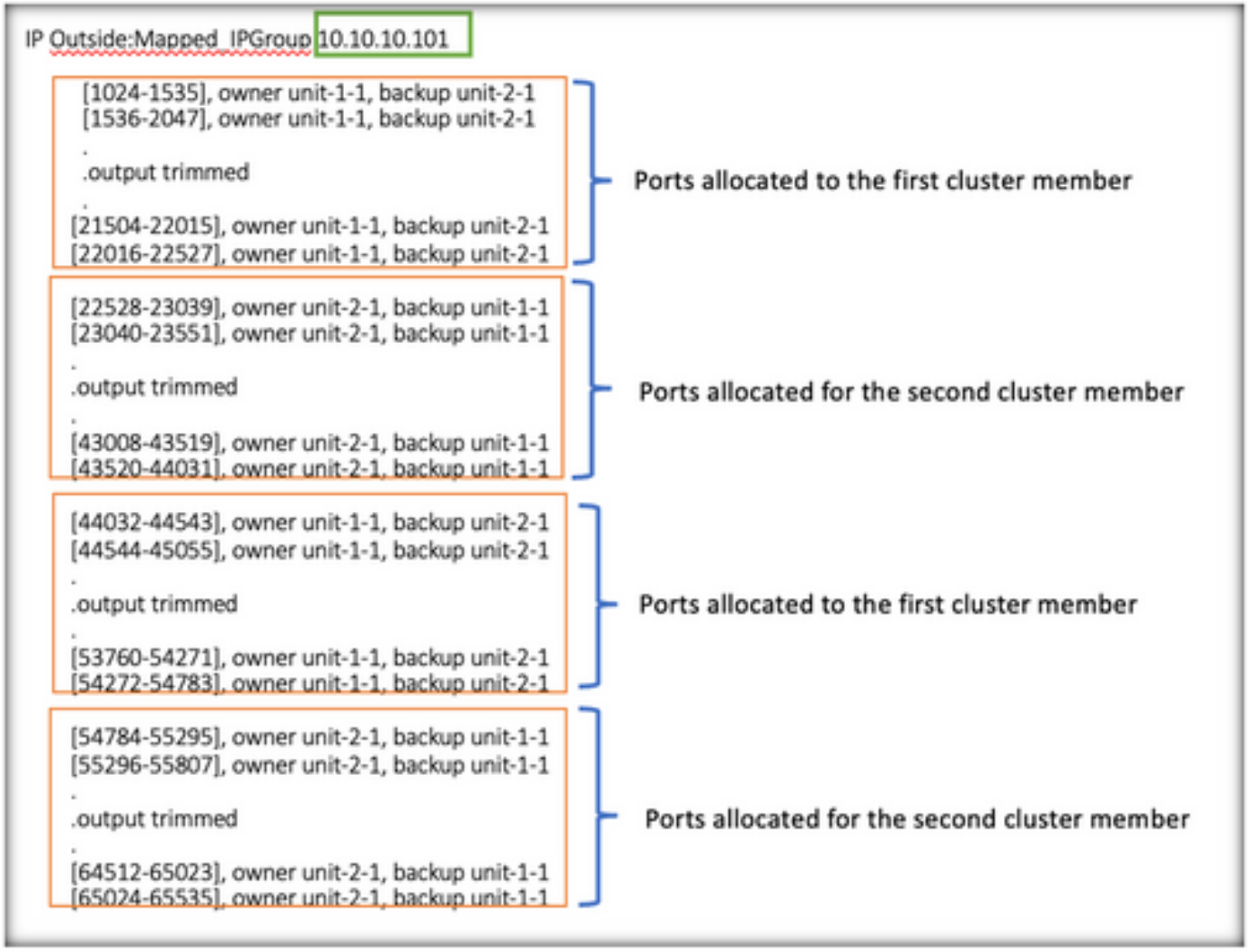

IP Outside:Mapped IPGroup 10.10.10.101
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
.output trimmed
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1
Ports allocated to the first cluster member
[22528-23039], owner 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，最佳實踐是配置**cluster-member-limit** 以匹配為集群部署計畫的裝置數。

例如，在由兩個單元(N=2)組成的集群組中，集群成員限制值為2，可以觀察到埠分配均勻地分佈在所有集群單元上。保留的所有埠都不剩餘。

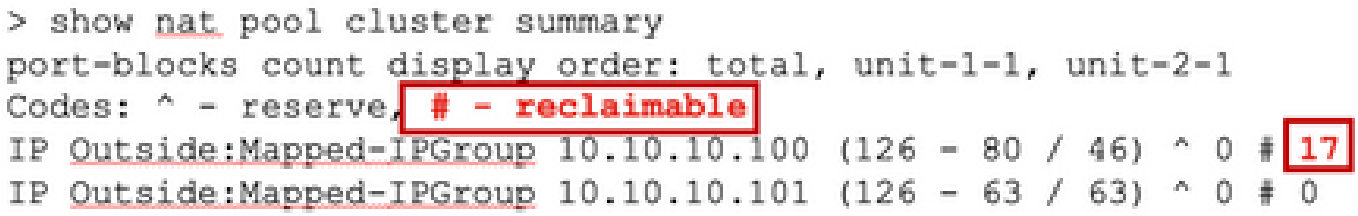





```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IP-1 10.10.10.100 (126 - 63 / 63) ^ 0 # 0
IP Outside:Mapped-IP-1 10.10.10.100 (126 - 63 / 63) ^ 0 # 0
```

驗證埠塊回收

- 每當新節點加入或離開集群時，必須將未使用的埠和所有單元的超額埠塊釋放給控制單元。
- 如果埠塊已被使用，則使用最少的那些，將被標籤為回收。
- 回收的埠塊上不允許新連線。當最後一個連線埠清除時，這些連線埠會釋放到控制單元。



疑難排解指令

本節提供的資訊可用於對組態進行疑難排解。

- 檢查配置的cluster-member-limit值：

<#root>

> show cluster info

Cluster FTD-Cluster: On
Interface mode: spanned

Cluster Member Limit : 2

[...]

> show running-config cluster

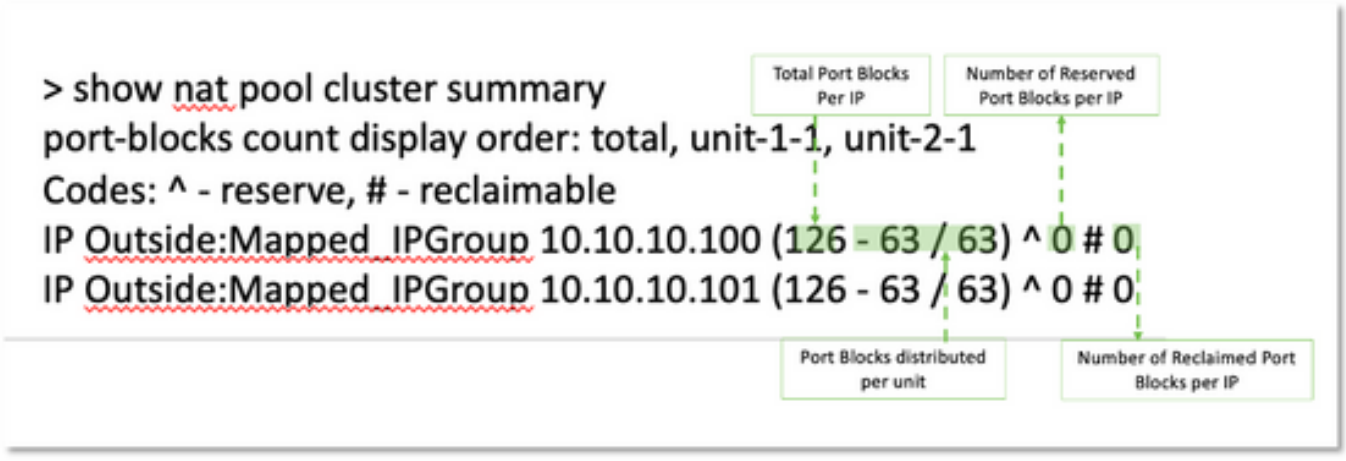
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0

cluster-member-limit 2
[...]

- 顯示集群中裝置之間的埠塊分佈摘要：

<#root>

> show nat pool cluster summary



- 顯示每個PAT地址的埠塊當前分配給所有者和備份單元：

<#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
[...]
```

- 顯示與埠塊的分發和使用相關的資訊：

<#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
[...]
```

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。