Understand Port Allocation on Dynamic PAT for FTD Cluster 7.0

Contents

Introduction

This document describes how port block-based distribution operates in Dynamic PAT for Firewall Cluster after version 7.0 and later.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Network Address Translation (NAT) on Cisco Secure Firewall

Components Used

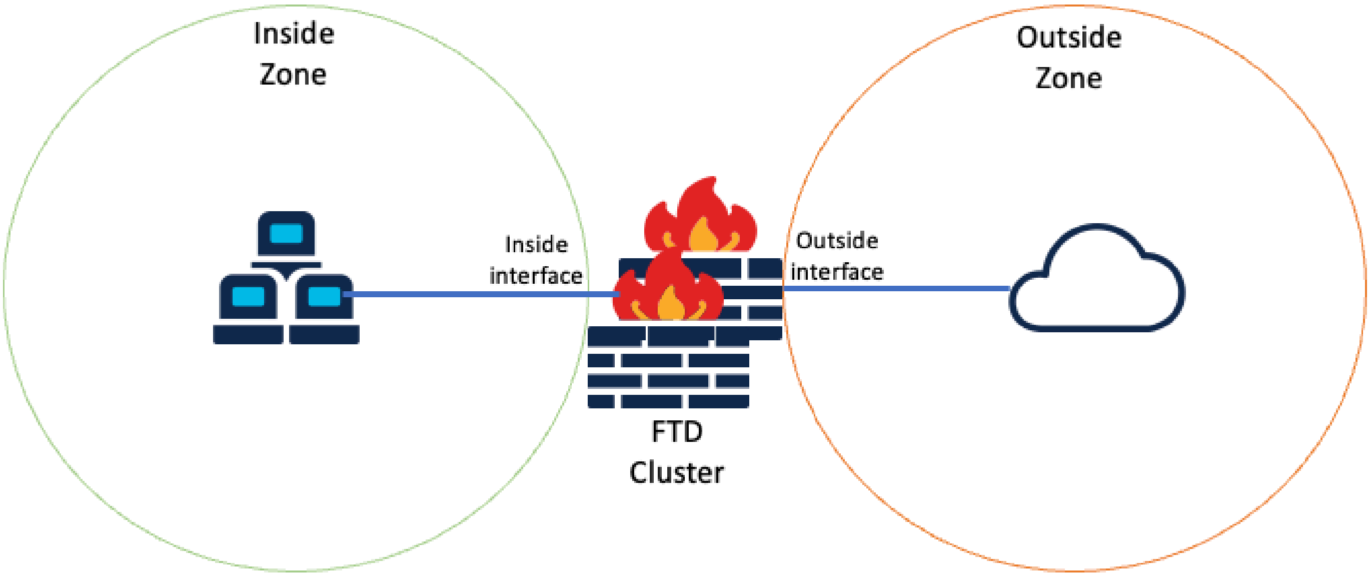
The information in this document is based on these software and hardware versions:

- Firepower Management Center 7.3.0
- Firepower Threat Defense 7.2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram

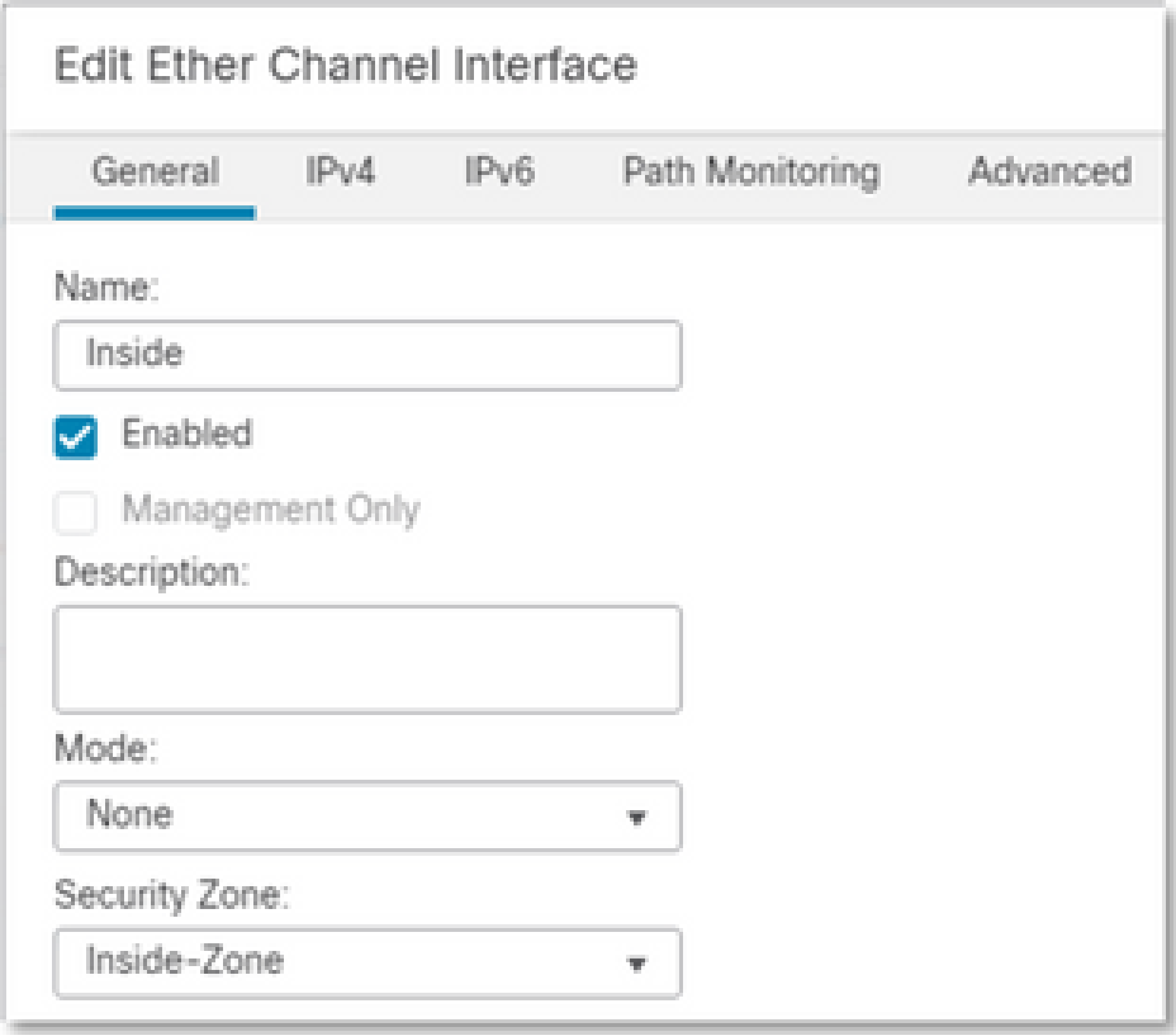


Logical Topology

Interface Configuration

- Configure Inside interface member of Inside Zone.

For example, configure an interface with IP address 192.168.10.254 and name it **Inside**. This Inside interface is the Gateway for internal network 192.168.10.0/24.



Edit Ether Channel Interface

Name: Inside

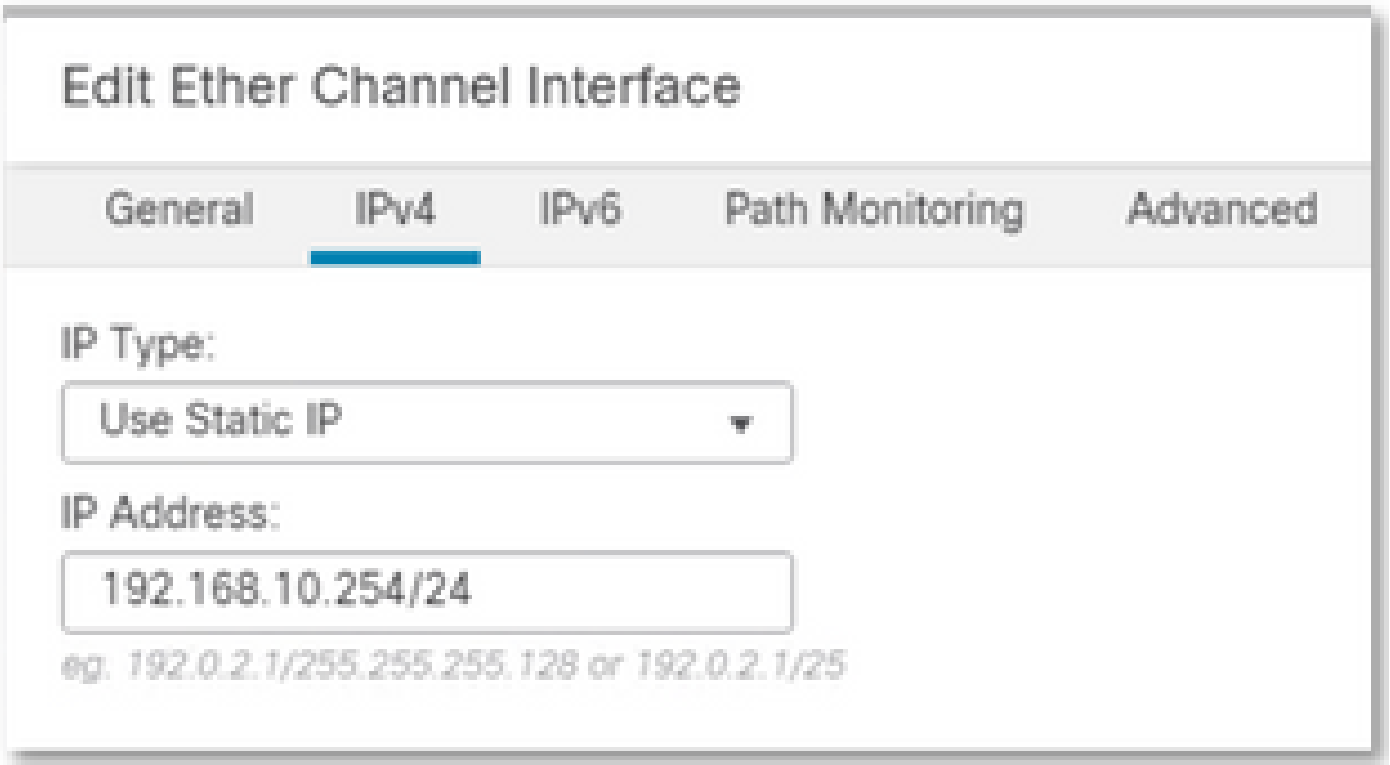
☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: Inside-Zone



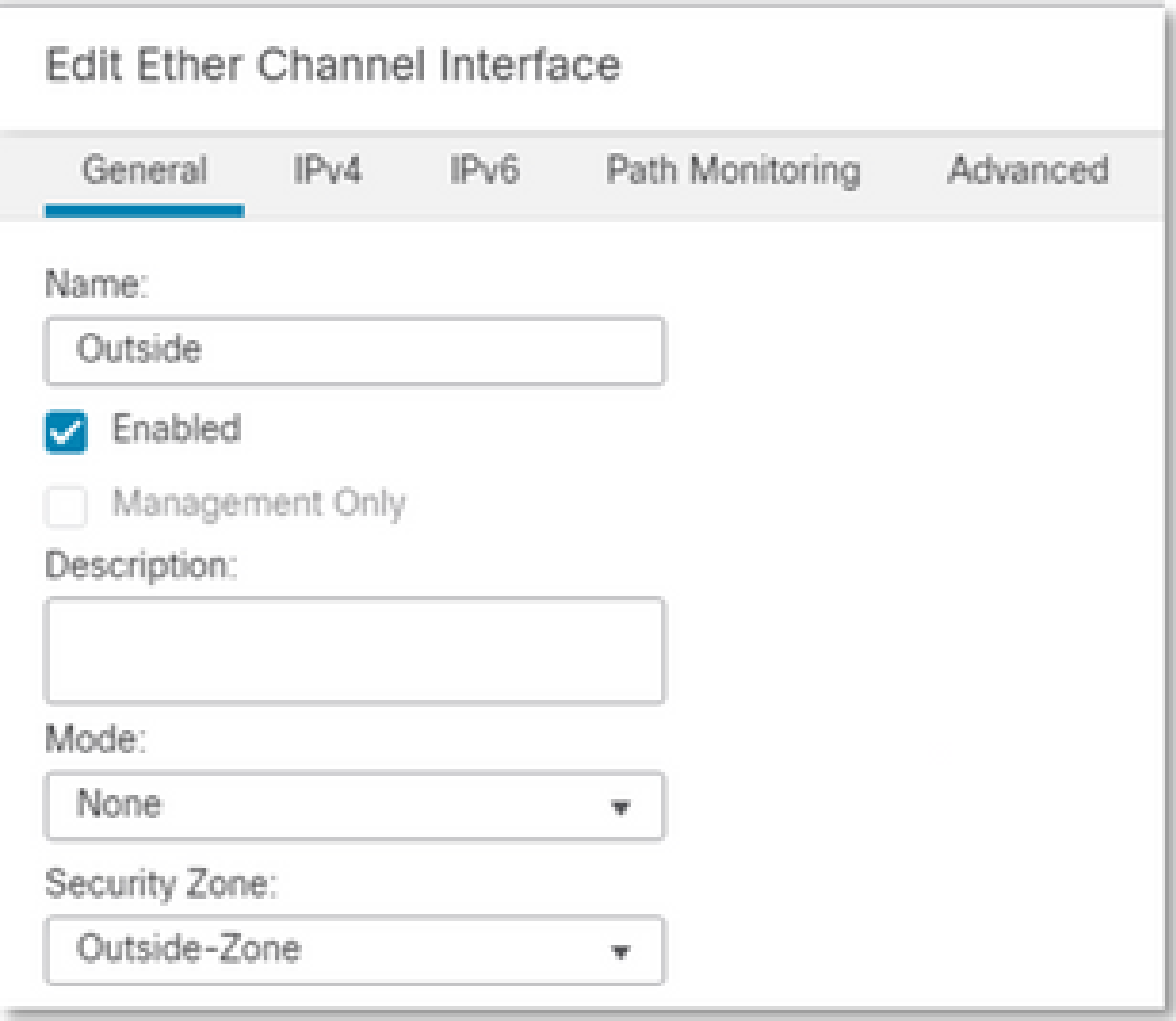
IP Type: Use Static IP

IP Address: 192.168.10.254/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- Configure Outside interface member of Outside Zone.

For example, configure an interface with IP address 10.10.10.254 and name it Outside. This Outside interface is facing external networks.



Edit Ether Channel Interface

Name: Outside

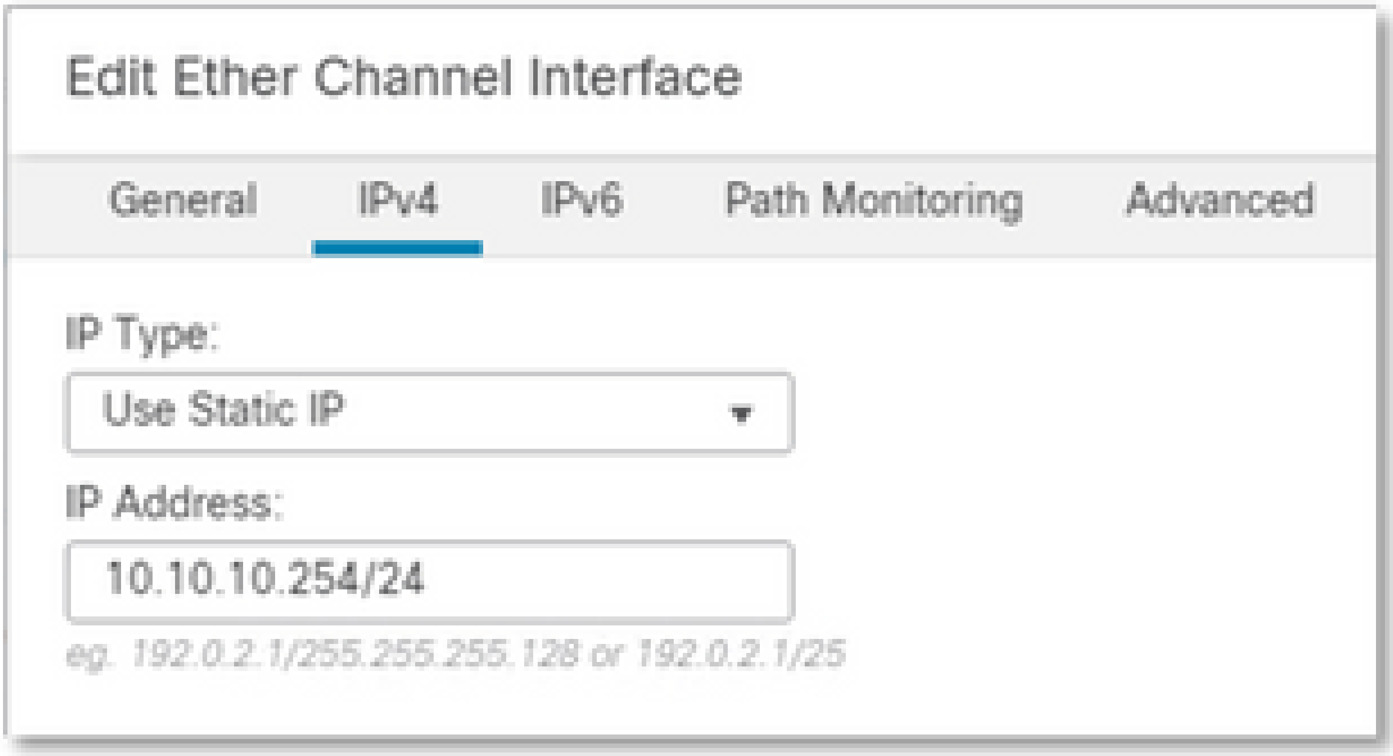
☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: Outside-Zone



Edit Ether Channel Interface

IP Type: Use Static IP

IP Address: 10.10.10.254/24

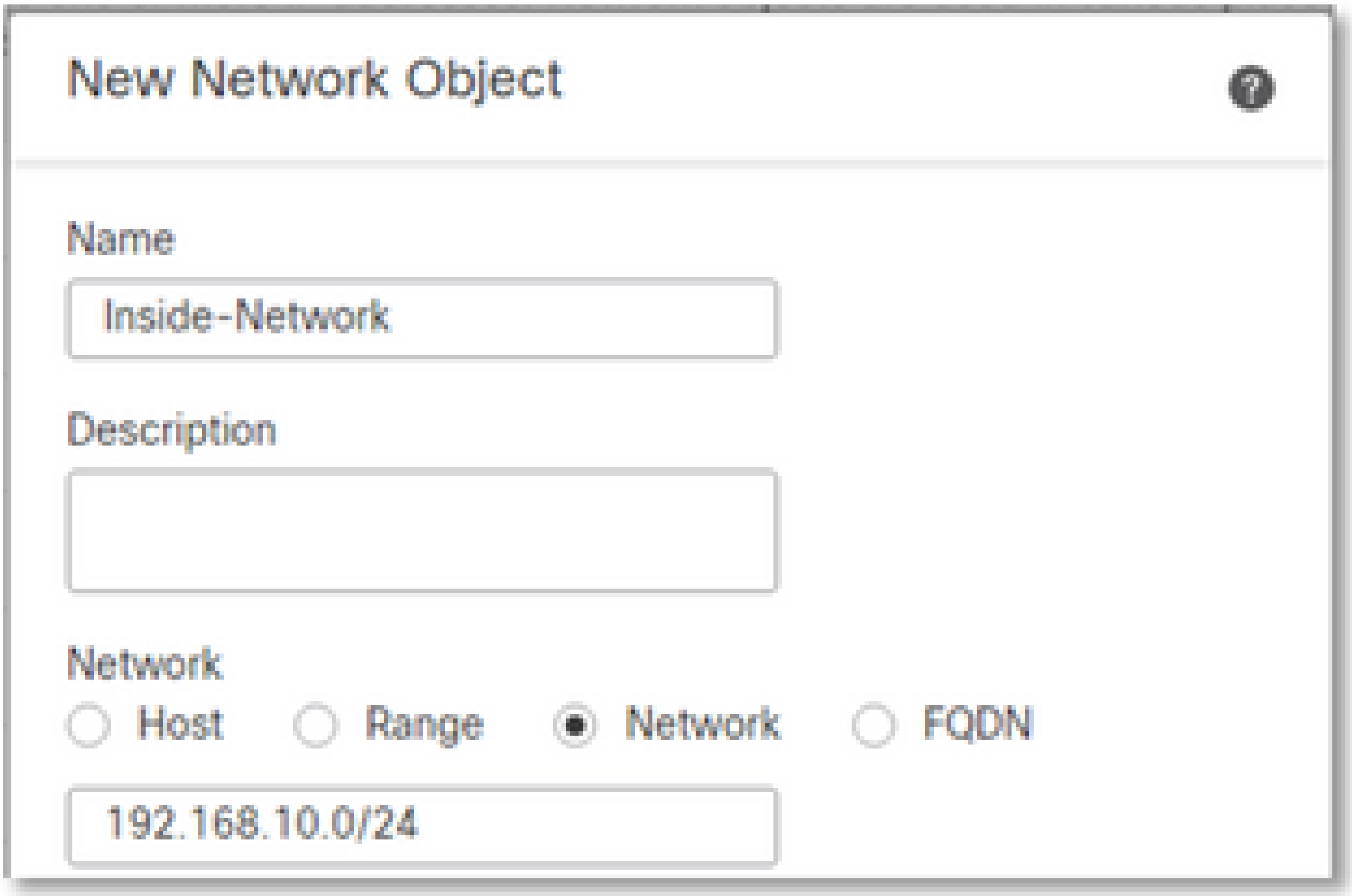
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Network Object Configuration

Even though cluster PAT can work with the egress interface or even a single IP to map all traffic, the best practice is to use an IP pool with at least the same number of IPs as the number of FTD units in the cluster.

For example, the network objects used for Real and mapped IP addresses are **Inside-Network** and **Mapped-IPGroup** respectively.

Inside-Network represents the internal network 192.168.10.0/24.


New Network Object

Name

Inside-Network

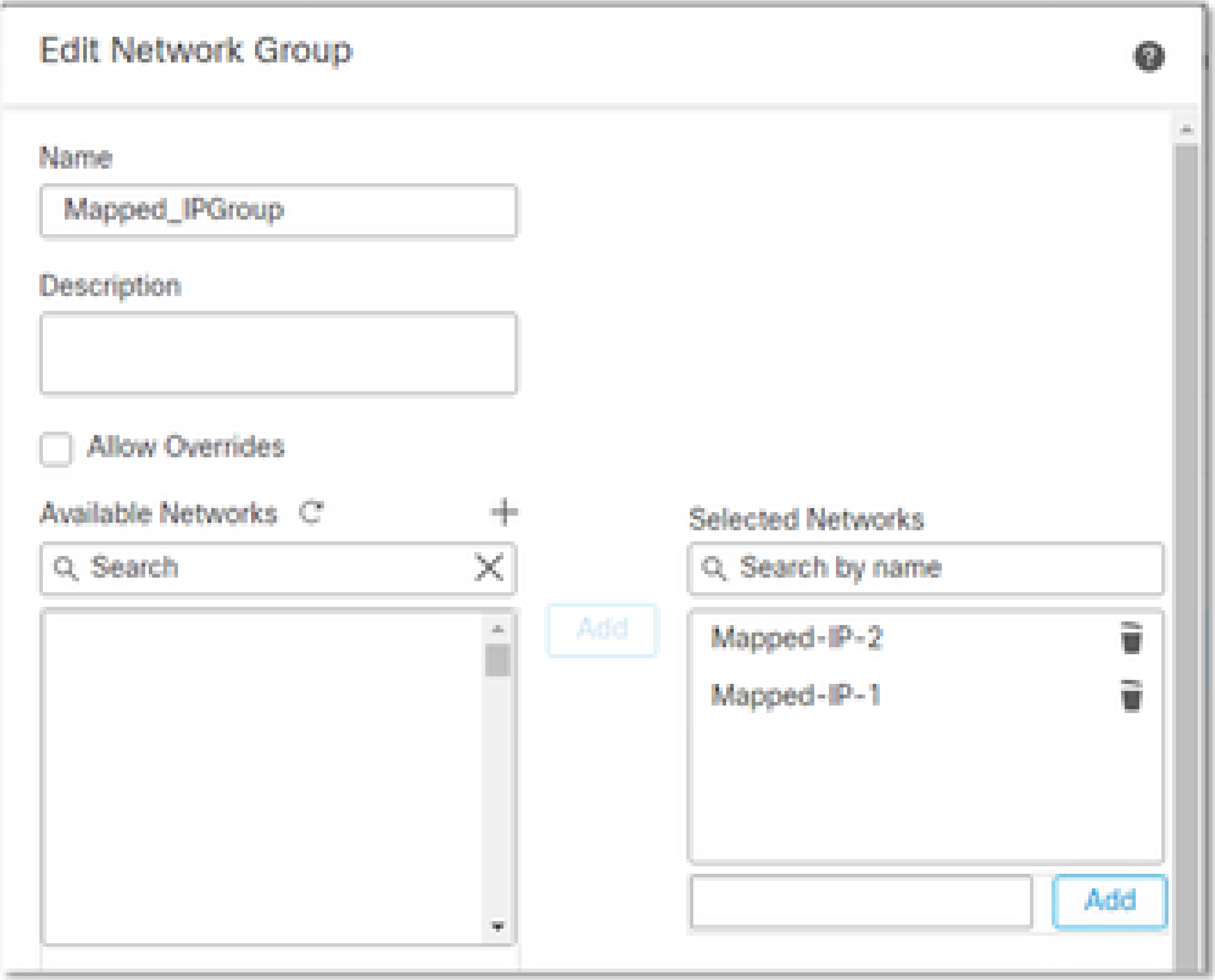
Description

Network

○ Host ○ Range ● Network ○ FQDN

192.168.10.0/24

Mapped-IPGroup (made of Mapped-IP-1 10.10.10.100 and Mapped-IP-2 10.10.10.101), is used to map all internal traffic to the Outside-Zone.



Edit Network Group

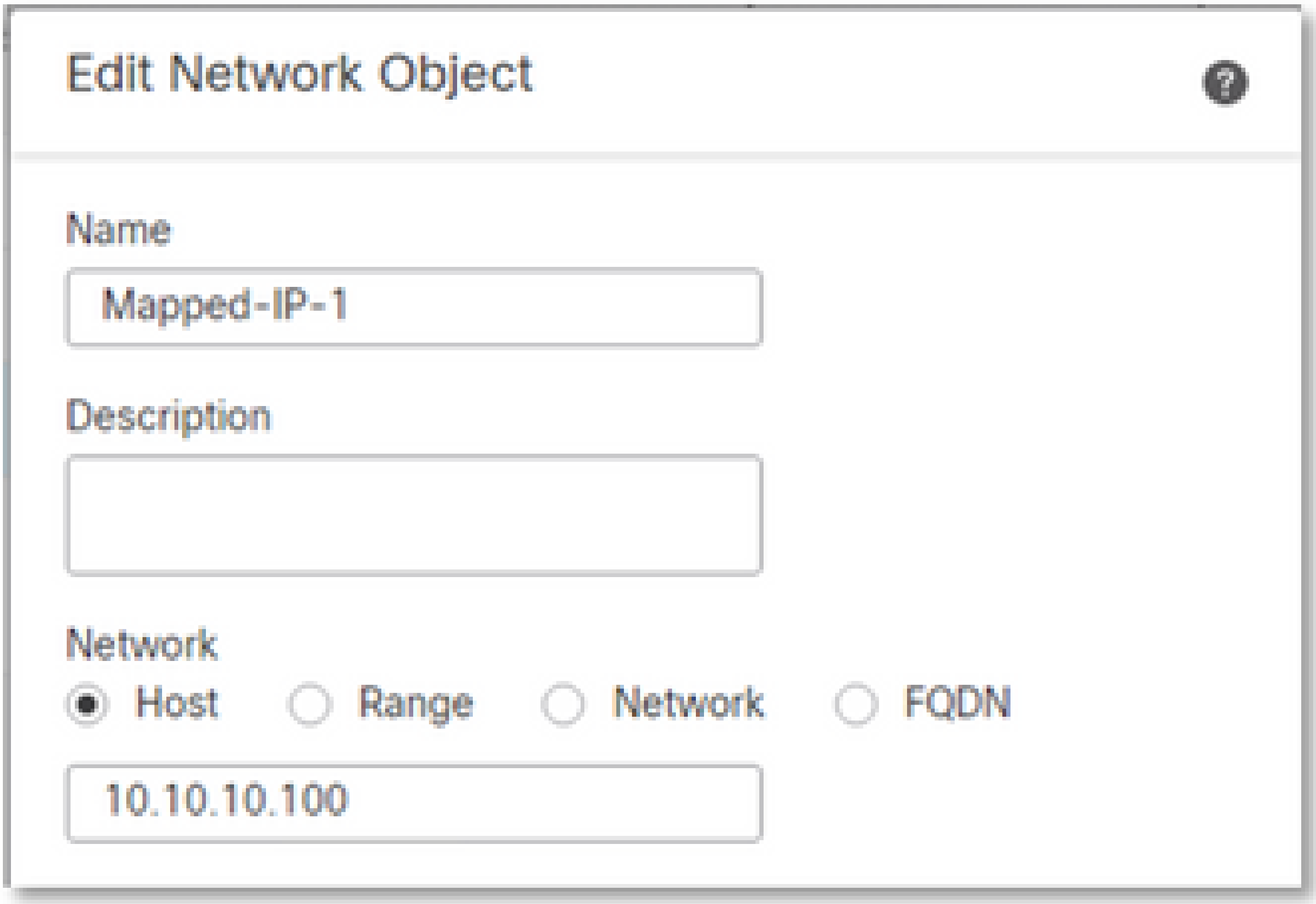
Name: Mapped_IPGroup

Description:

□ Allow Overrides

Selected Networks:

- Mapped-IP-2
- Mapped-IP-1



Edit Network Object

Name

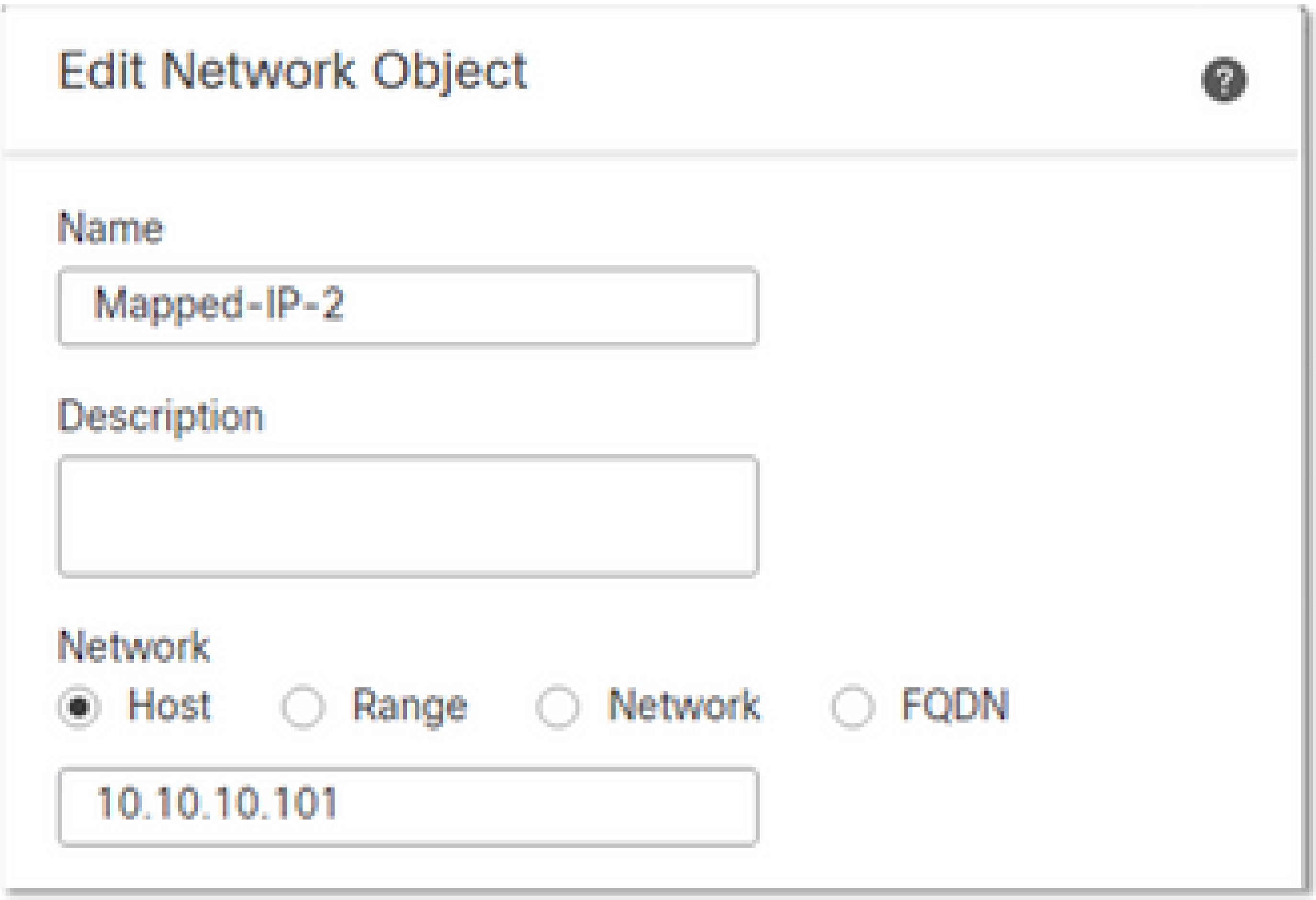
Mapped-IP-1

Description

Network

● Host ○ Range ○ Network ○ FQDN

10.10.10.100



Edit Network Object

Name

Mapped-IP-2

Description

Network

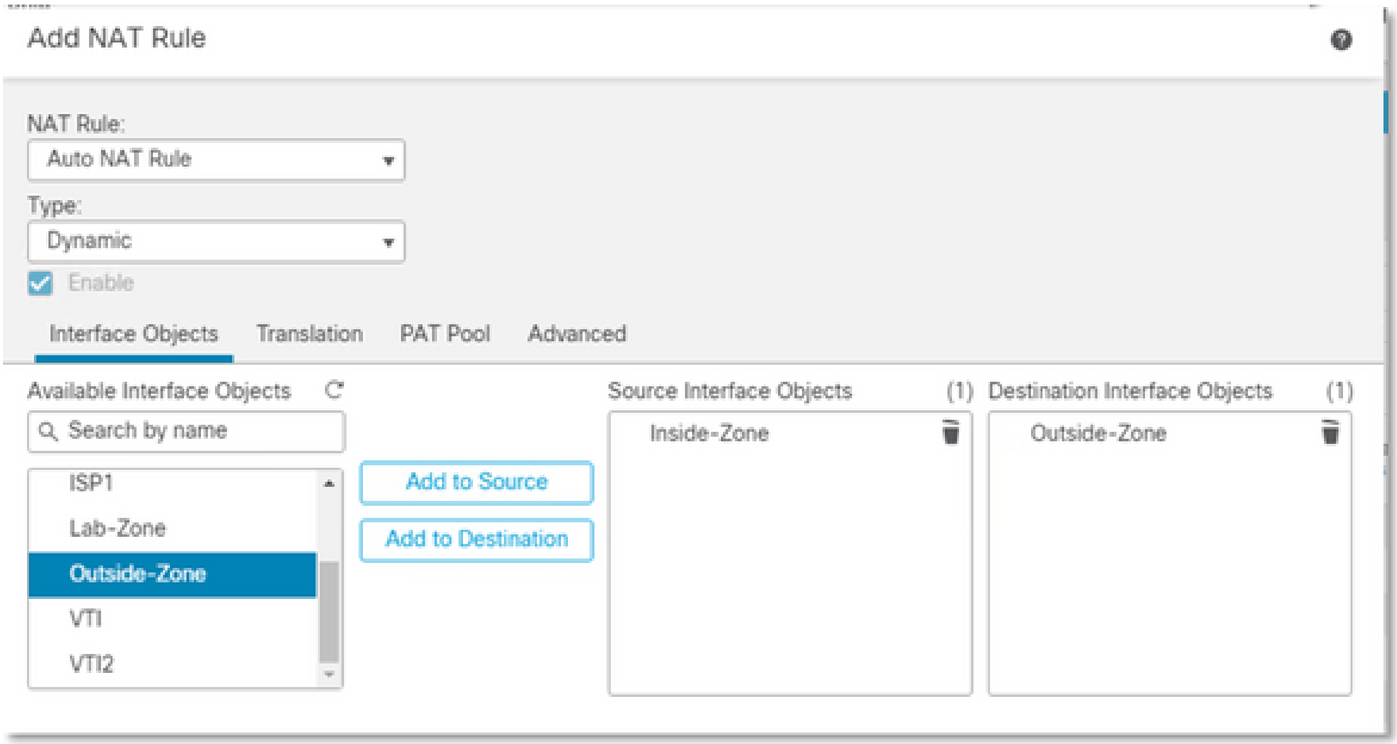
● Host ○ Range ○ Network ○ FQDN

10.10.10.101

Dynamic PAT Configuration

- Configure a Dynamic NAT rule for outbound traffic. This NAT rule maps the internal network subnet to the external NAT Pool.

For example, Inside-Zone to Outside-Zone traffic from Inside-Network is translated to Mapped-IPGroup Pool.



Add NAT Rule

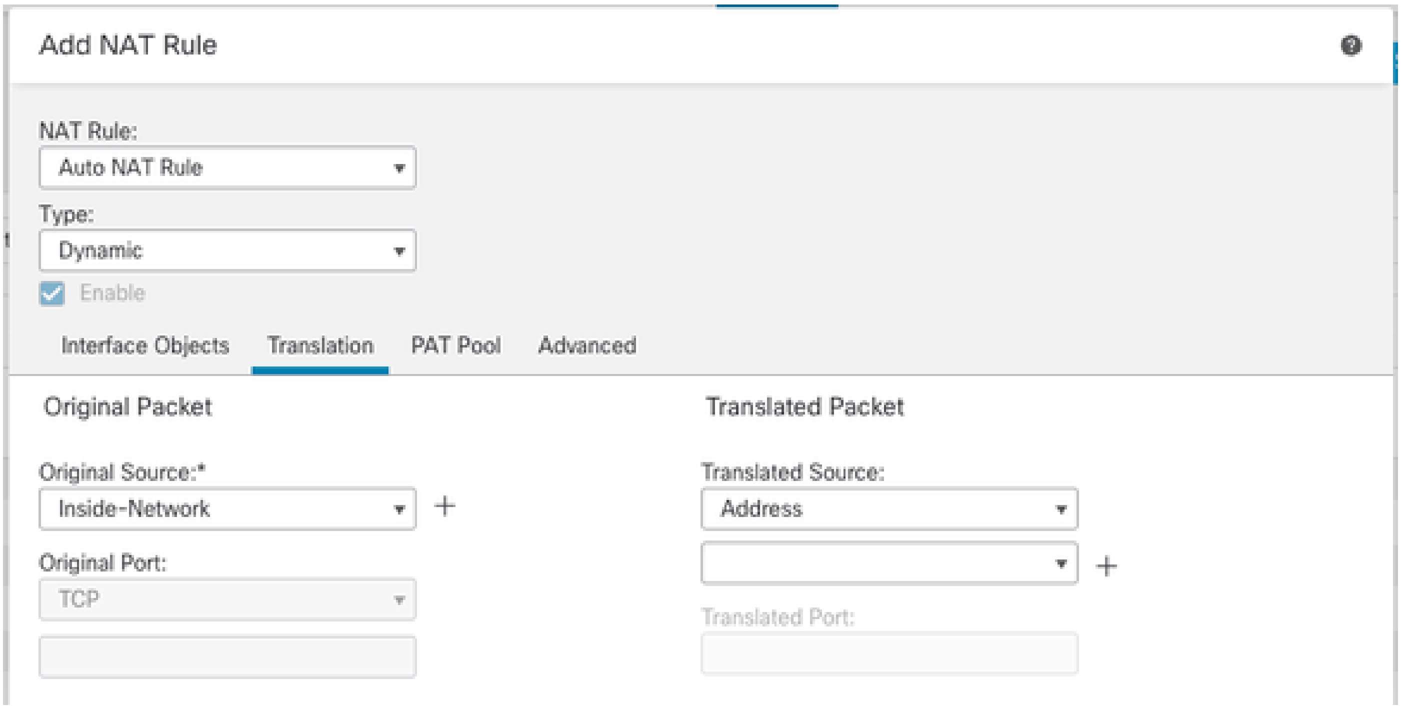
NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Source Interface Objects (1): Inside-Zone

Destination Interface Objects (1): Outside-Zone



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Original Packet

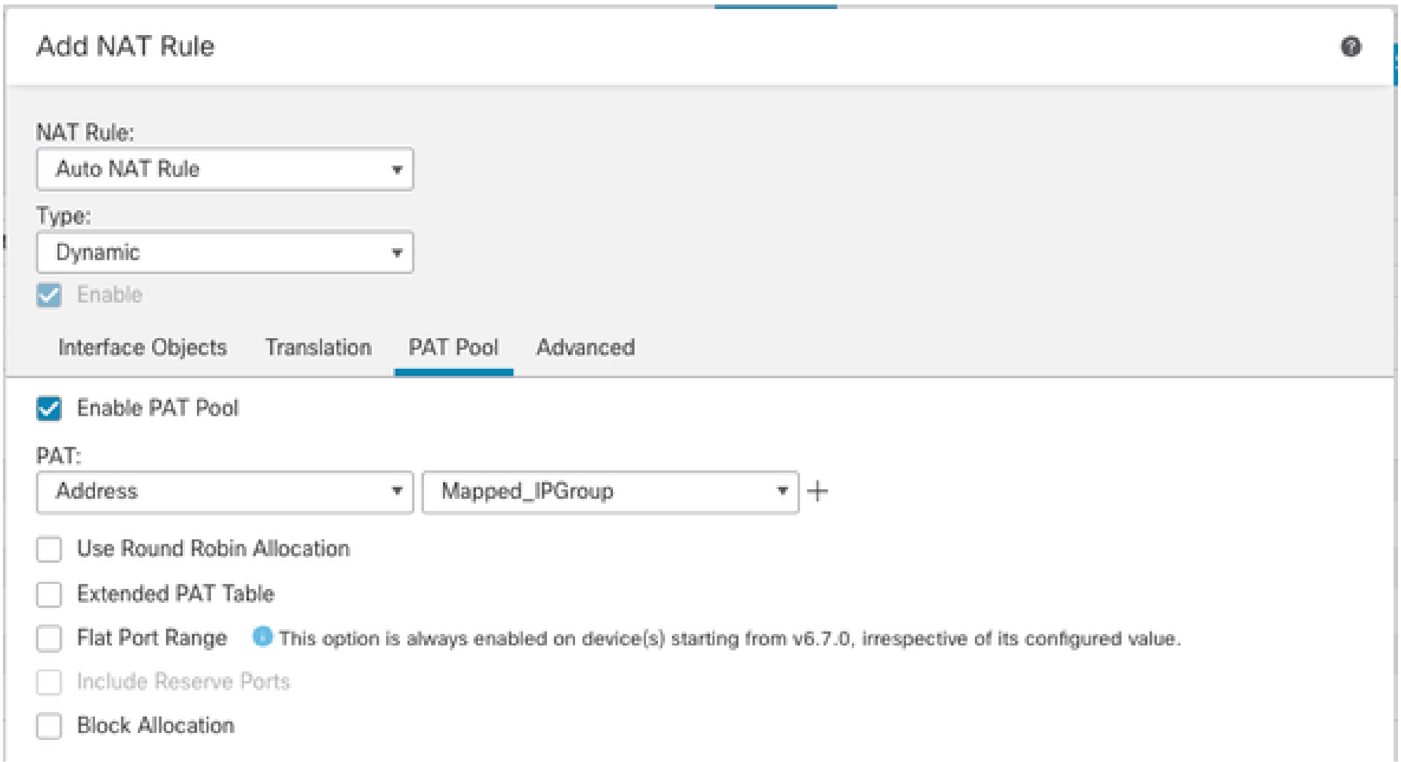
Original Source:* Inside-Network

Original Port: TCP

Translated Packet

Translated Source: Address

Translated Port:



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

☑ Enable PAT Pool

PAT: Address | Mapped_IPGroup +

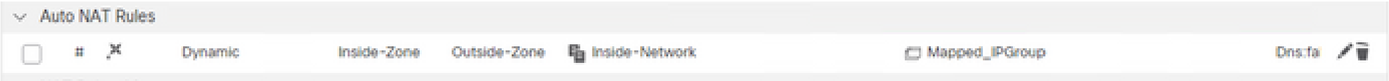
□ Use Round Robin Allocation

□ Extended PAT Table

□ Flat Port Range This option is always enabled on device(s) starting from v6.7.0, irrespective of its configured value.

□ Include Reserve Ports

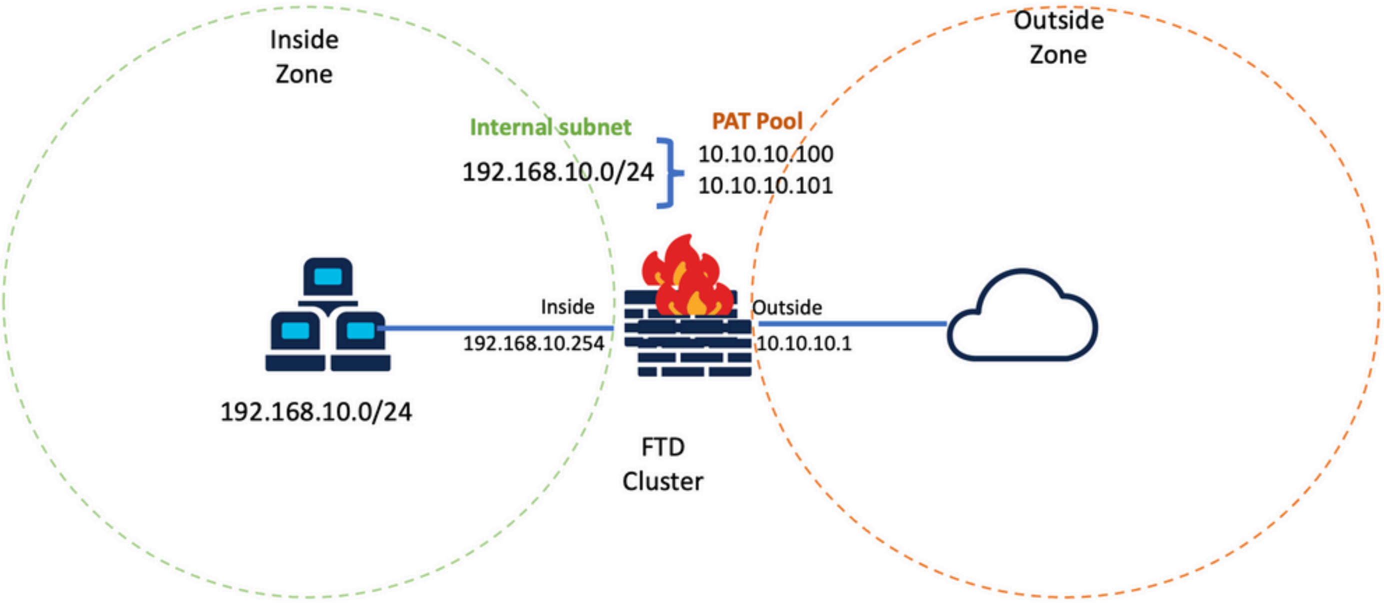
□ Block Allocation



Auto NAT Rules

□ # Dynamic Inside-Zone Outside-Zone Inside-Network Mapped_IPGroup Dns:fa

Final Configuration



Final Lab Setup.

Verify

Use this section to confirm that your configuration works properly.

Verify IP Interface and NAT Configuration

<#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
```

Verify Port Block Allocation

After Firepower 7.0, the improved PAT port block allocation ensures that the control unit keeps ports in reserve for joining nodes, and proactively reclaims unused ports. This is how the port allocation works:

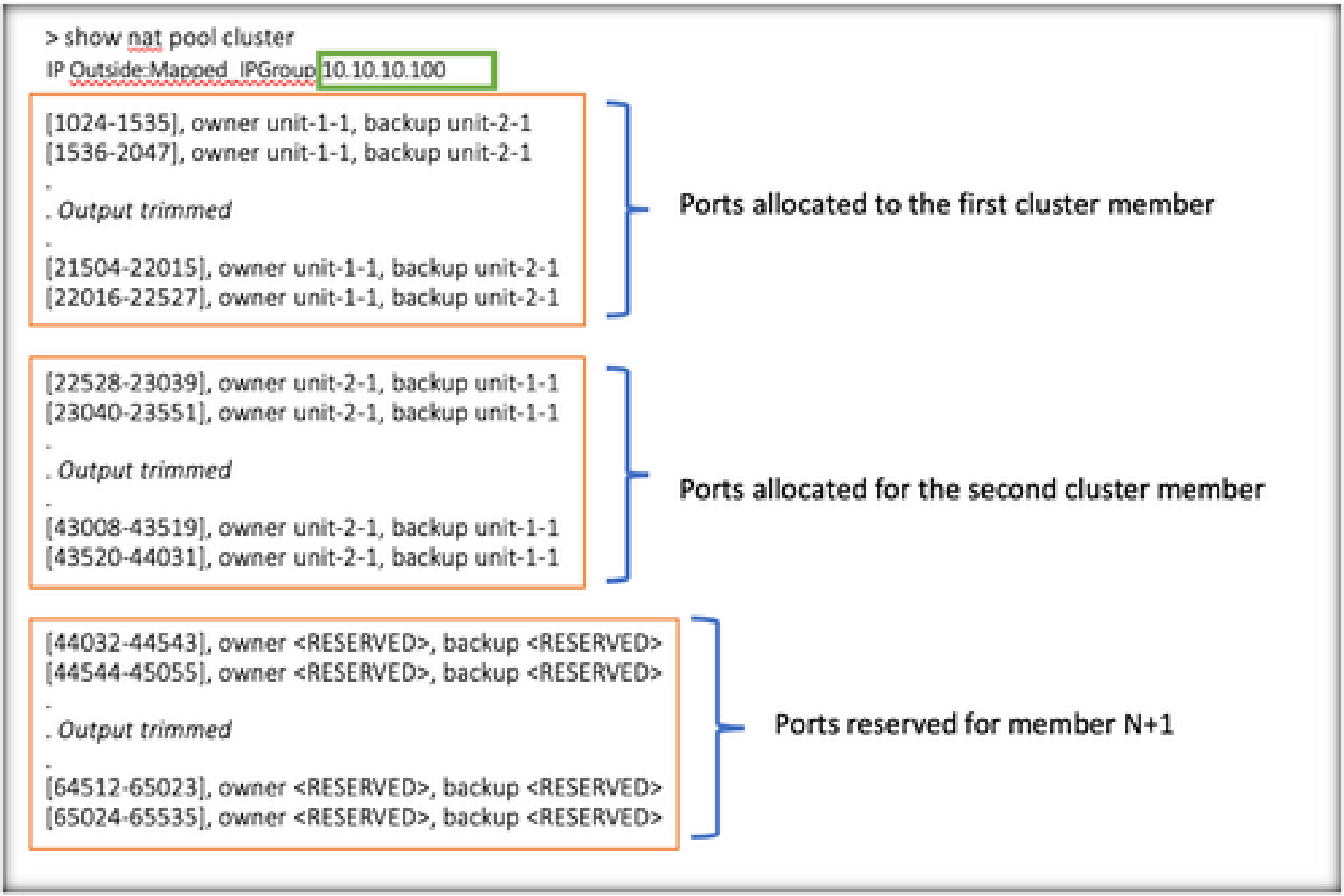
- On a cluster that is just being brought up, the Control unit initially owns 50% of ports and the rest are reserved.
- The number of port blocks owned per unit are adjusted as more nodes join the cluster.
- Control unit reserves port blocks for (N+1) nodes until the cluster is full**.** Cluster member limit is defined by the cluster-member-limit command, configured under the cluster group configuration level.
- By default, cluster-member-limit is 16.

  <#root>

  ```
  > show cluster info

  Cluster FTD-Cluster: On
  Interface mode: spanned

  Cluster Member Limit : 16


  [...]
  ```

- When the amount of cluster members reaches the value configured with **cluster-member-limit**, all the port blocks are distributed across cluster members.

For example, in a cluster group made of two units (N=2) with a default value of cluster member limit of 16, it is observed that port allocation is defined for N+1 members, in this case, 3. This leaves some ports reserved for the next unit until maximum cluster limit is reached.

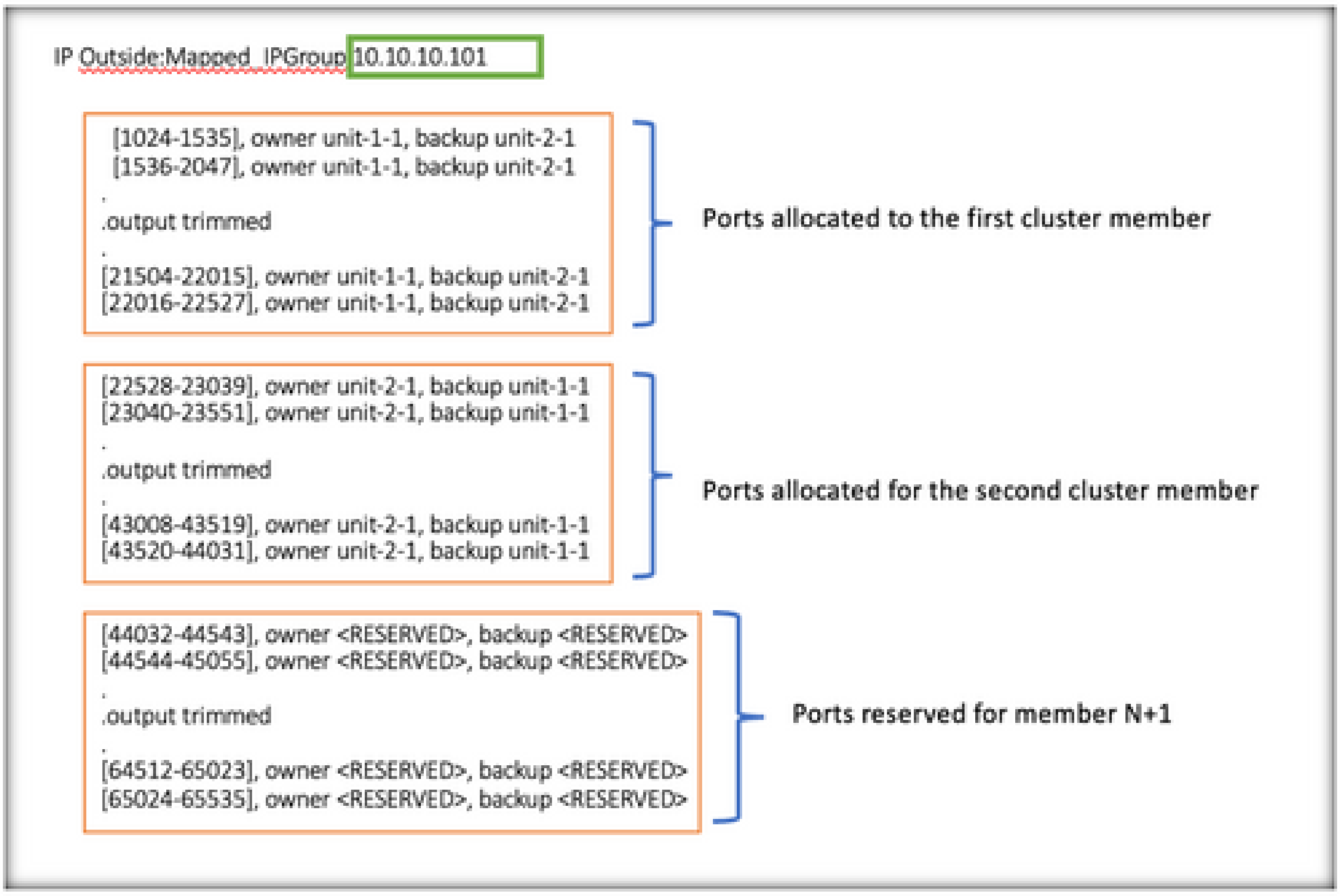


```
> show nat pool cluster
IP Outside:Mapped_IPGroup 10.10.10.100
[1024-1535], owner unit-1-1, backup unit-2-1
[1536-2047], owner unit-1-1, backup unit-2-1
.
. Output trimmed
.
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1

[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

[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 allocated to the first cluster member

Ports allocated for the second cluster member

Ports reserved for member N+1

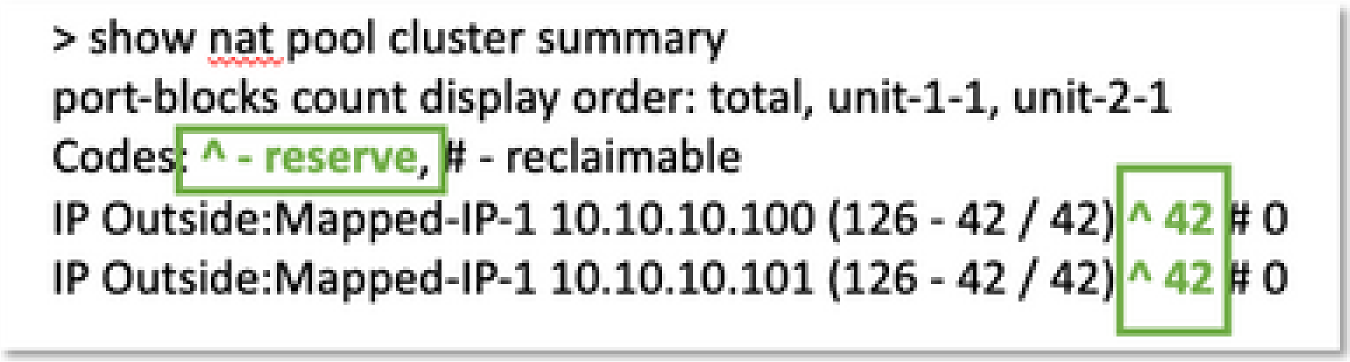


```
IP Outside:Mapped_IPGroup 10.10.10.101

  [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

[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

[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 allocated to the first cluster member

Ports allocated for the second cluster member

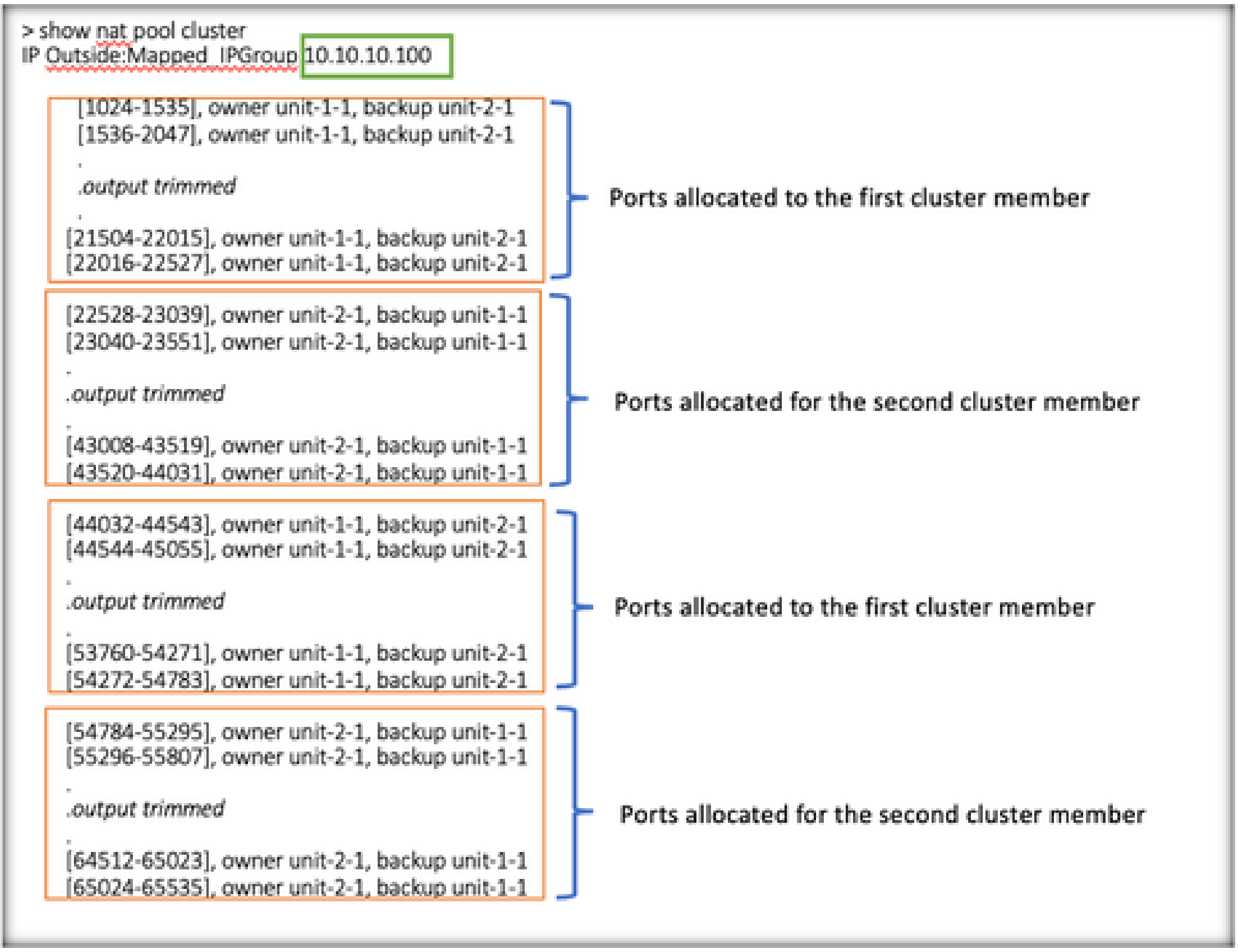
Ports reserved for member N+1



```
> 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
```

Additionally, it is a best practice to configure the **cluster-member-limit** to match the number of units planned for the cluster deployment.

For example, in a cluster group made of two units (N=2) with value of cluster member limit of 2,it is observed that port allocation is distributed evenly across all cluster units. None of the reserved ports are left.



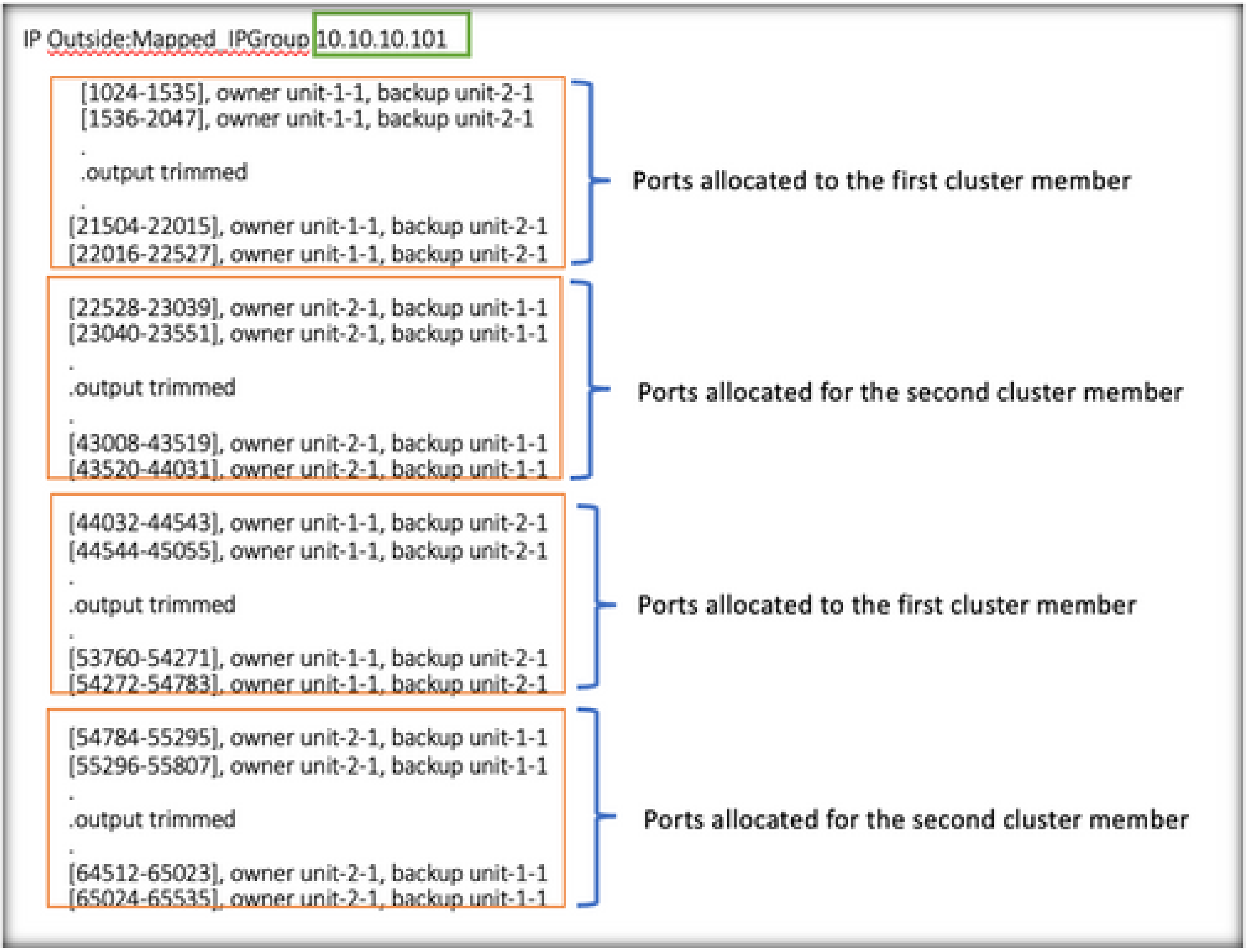
```
> show nat pool cluster
IP Outside:Mapped_IPGroup 10.10.10.100
  [1024-1535], owner unit-1-1, backup unit-2-1
  [1536-2047], owner unit-1-1, backup unit-2-1
  .
  .output trimmed
  .
 [21504-22015], owner unit-1-1, backup unit-2-1
 [22016-22527], owner unit-1-1, backup unit-2-1
 [22528-23039], owner 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
 [44032-44543], owner unit-1-1, backup unit-2-1
 [44544-45055], owner unit-1-1, backup unit-2-1
 .
 .output trimmed
 .
 [53760-54271], owner unit-1-1, backup unit-2-1
 [54272-54783], owner unit-1-1, backup unit-2-1
 [54784-55295], owner unit-2-1, backup unit-1-1
 [55296-55807], owner unit-2-1, backup unit-1-1
 .
 .output trimmed
 .
 [64512-65023], owner unit-2-1, backup unit-1-1
 [65024-65535], owner unit-2-1, backup unit-1-1
```

Ports allocated to the first cluster member

Ports allocated for the second cluster member

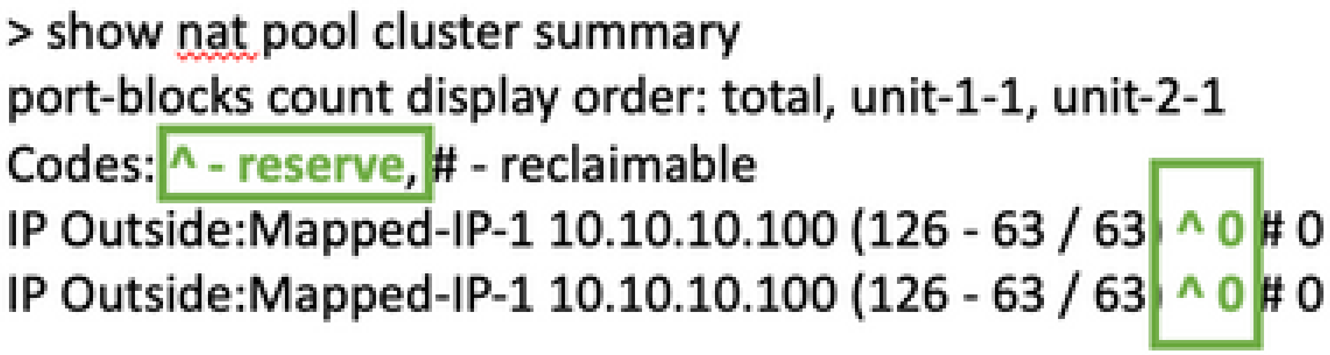
Ports allocated to the first cluster member

Ports allocated for the second cluster member



```
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
  [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
  [44032-44543], owner unit-1-1, backup unit-2-1
  [44544-45055], owner unit-1-1, backup unit-2-1
  .
  .output trimmed
  .
  [53760-54271], owner unit-1-1, backup unit-2-1
  [54272-54783], owner unit-1-1, backup unit-2-1
  [54784-55295], owner unit-2-1, backup unit-1-1
  [55296-55807], owner unit-2-1, backup unit-1-1
  .
  .output trimmed
  .
  [64512-65023], owner unit-2-1, backup unit-1-1
  [65024-65535], owner unit-2-1, backup unit-1-1
```

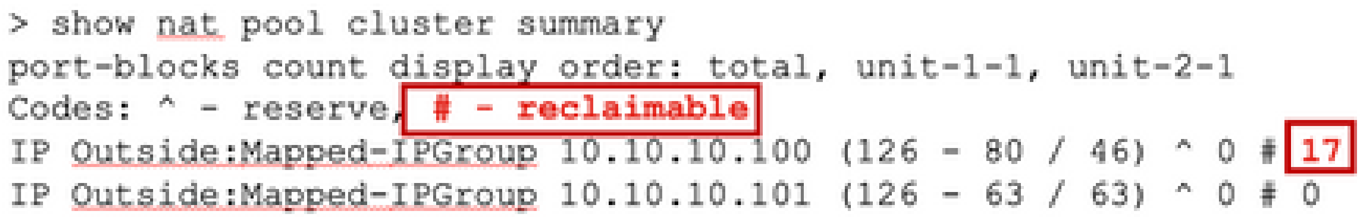
Ports allocated to the first cluster member
Ports allocated for the second cluster member
Ports allocated to the first cluster member
Ports allocated for the second cluster member



```
> 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
```

Verify Port Block Reclamation

- Whenever a new node joins or leaves a cluster, unused ports and excess port blocks from all units must be released to the control unit.
- If the port blocks are already being used, the least-used ones are marked for reclamation.
- New connections are not allowed on reclaimed port blocks. They are released to the control unit when the last port is cleared.



```
> 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
```

Troubleshooting Commands

This section provides information you can use to troubleshoot your configuration.

- Check the cluster-member-limit value configured:

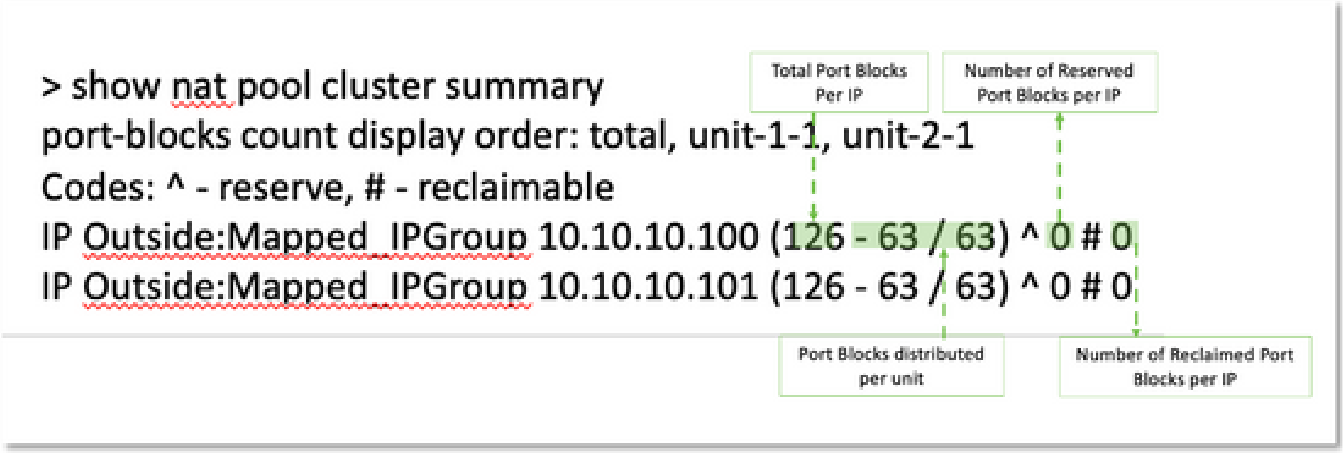
<#root>

```
> 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
[...]
```

- Display a summary of the port blocks distribution among the units in the cluster:

<#root>

```
> show nat pool cluster summary
```



```
> 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 - 63 / 63) ^ 0 # 0
IP Outside:Mapped_IPGroup 10.10.10.101 (126 - 63 / 63) ^ 0 # 0
```

Total Port Blocks Per IP
Number of Reserved Port Blocks per IP
Port Blocks distributed per unit
Number of Reclaimed Port Blocks per IP

- Display the current assignment of port blocks per PAT address to the owner and backup unit:

<#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
[...]
```

- Display information related to distribution and usage of port blocks:

<#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
[...]
```

Related Information

- **Cisco Technical Support & Downloads**