FTDクラスタ7.0のダイナミックPAT上のポート割り当てについて

内容

はじめに

このドキュメントでは、バージョン7.0以降のファイアウォールクラスタのダイナミックPAT(PAT)でポートブロックベース分散がどのように動作するかについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewallでのネットワークアドレス変換(NAT)

使用するコンポーネント

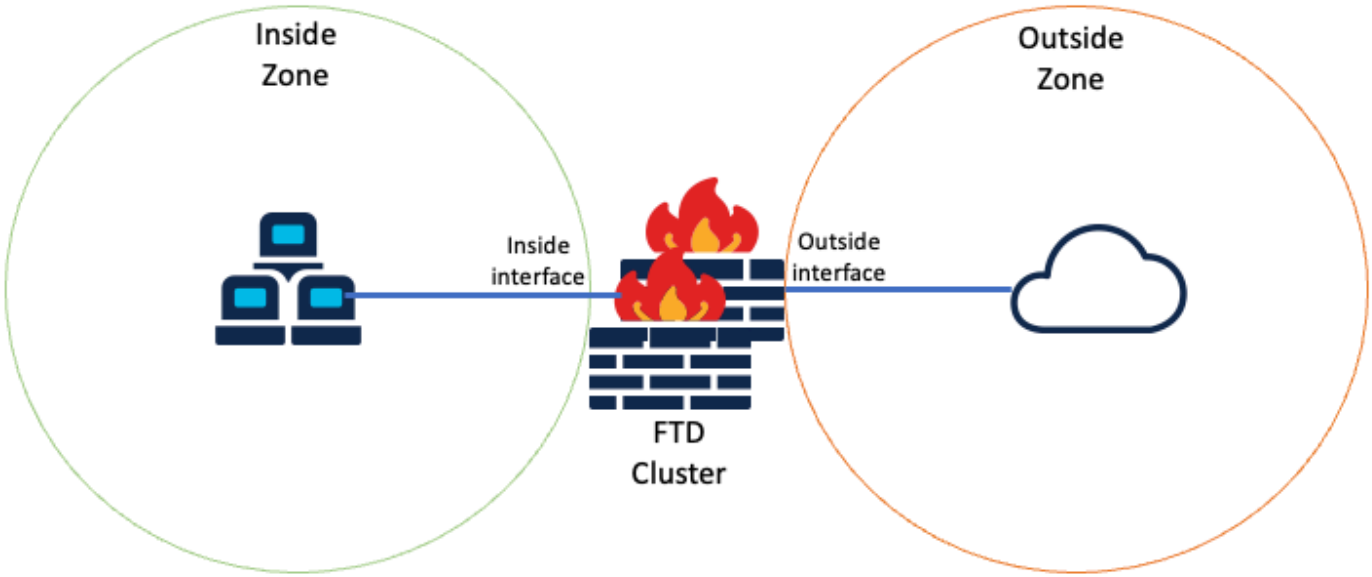
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Management Center(FMC)7.3.0
- Firepower Threat Defense 7.2.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図

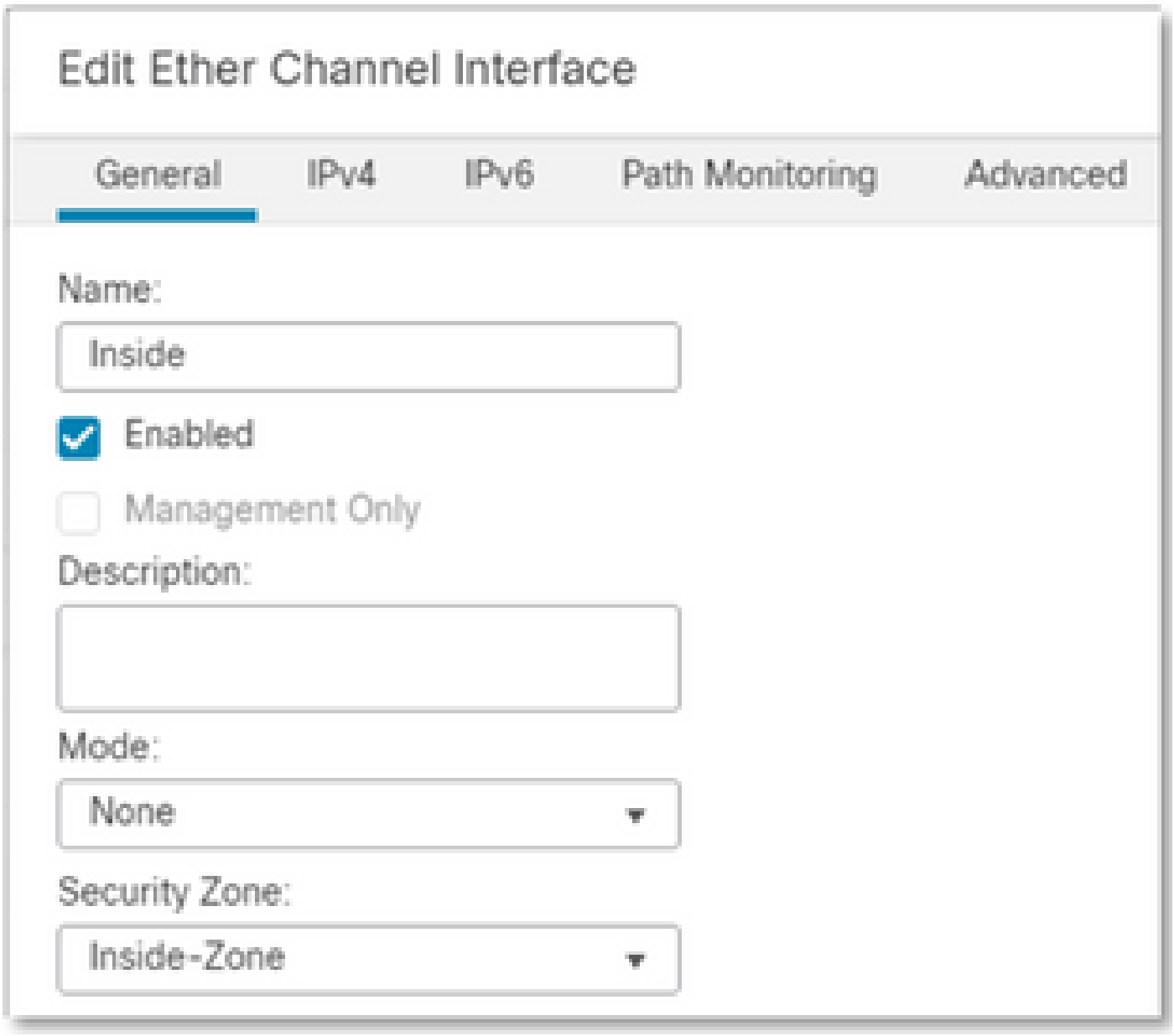


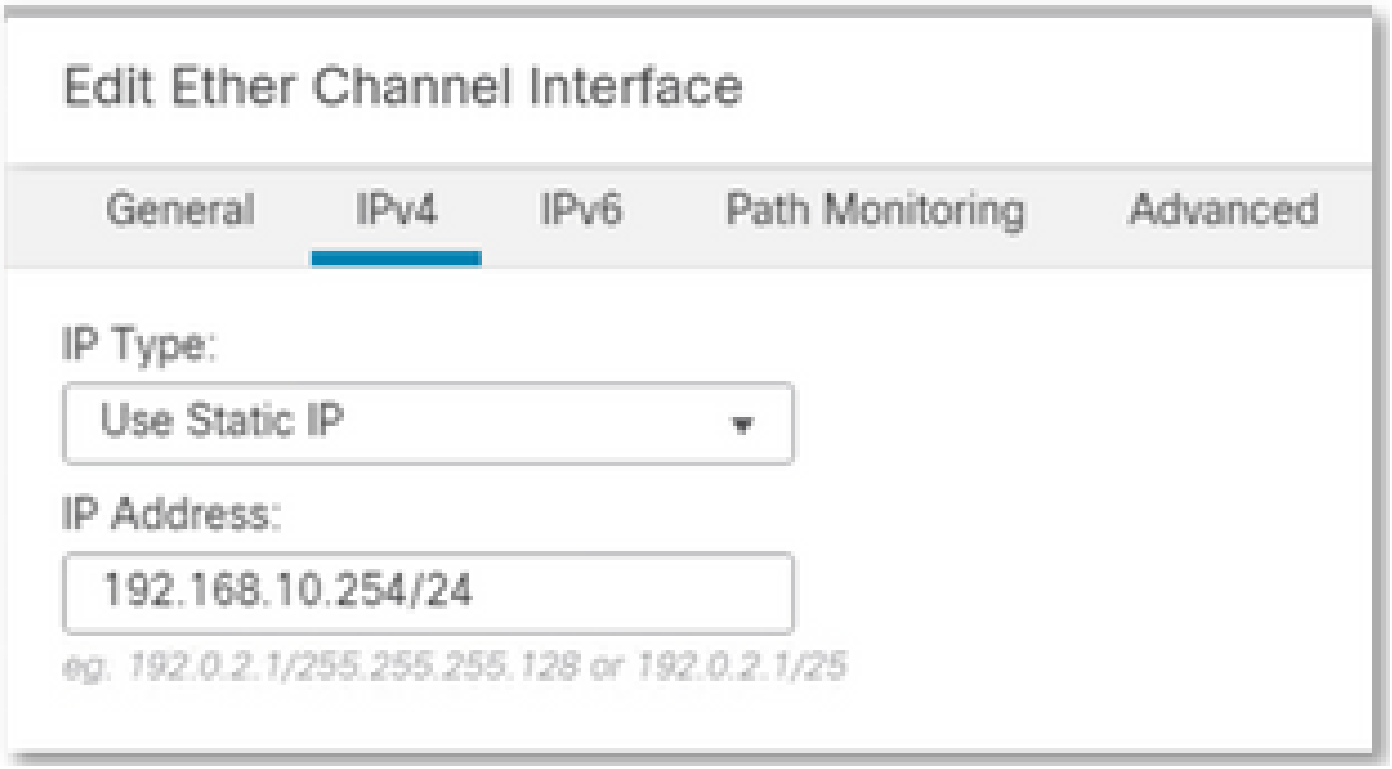
論理トポロジ

インターフェイス設定

- 内部ゾーンの内部インターフェイスメンバーを設定します。

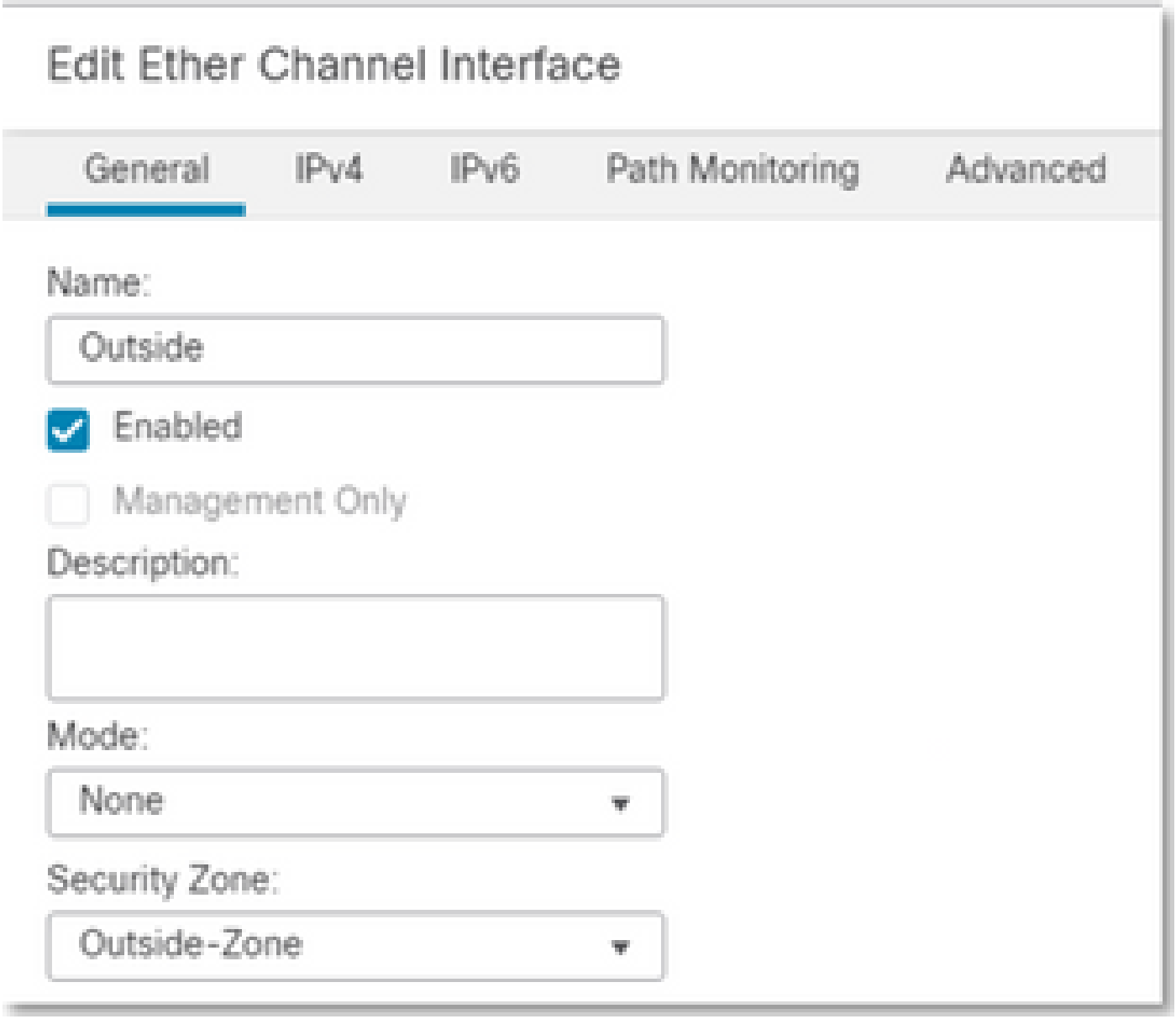
たとえば、IPアドレスが192.168.10.254のインターフェイスを設定し、Insideという名前を付けます。この内部インターフェイスは、内部ネットワーク192.168.10.0/24のゲートウェイです。

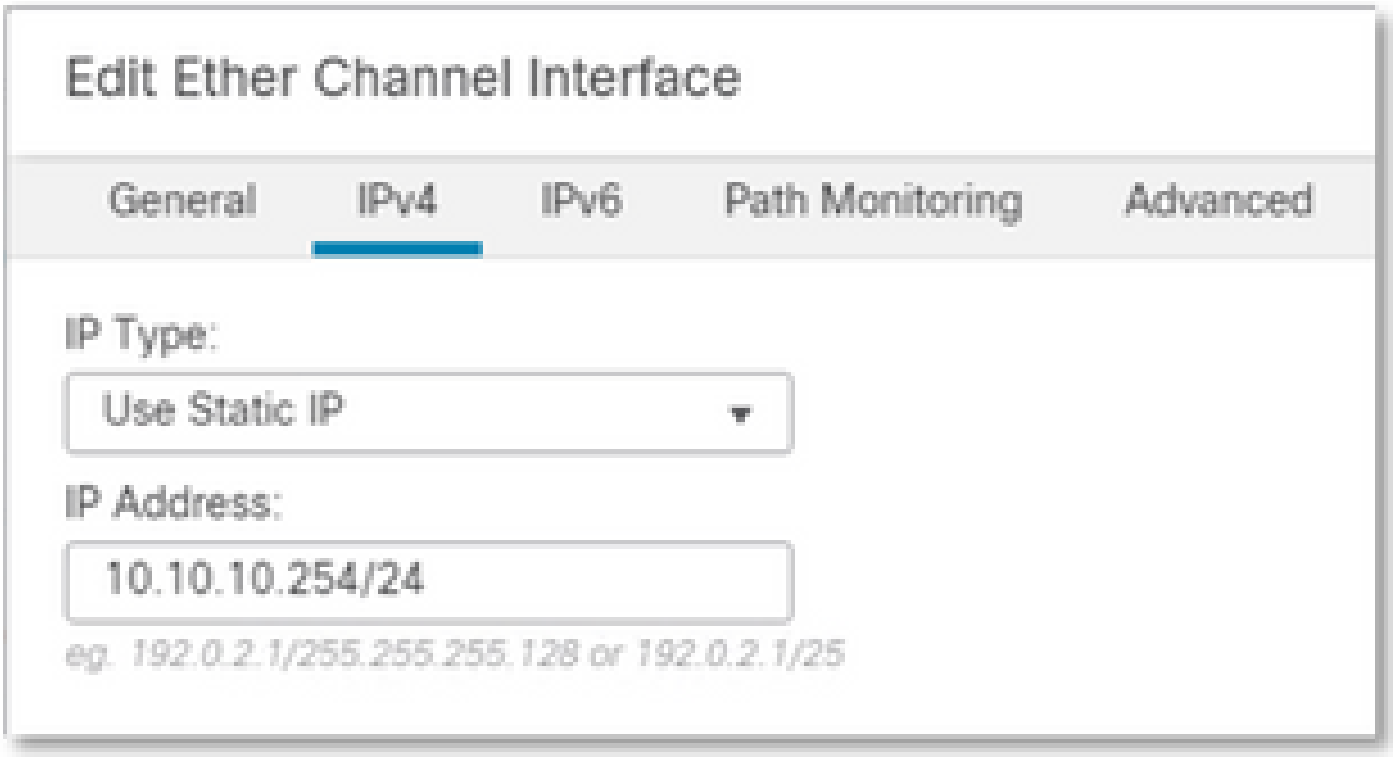

Edit Ether Channel Interface
General
IPv4
IPv6
Path Monitoring
Advanced
Name:
Inside
Enabled
Management Only
Description:
Mode:
None
Security Zone:
Inside-Zone



- OutsideゾーンのOutsideインターフェイスメンバーを設定します。

たとえば、IPアドレスが10.10.10.254のインターフェイスを設定し、Outsideという名前を付けます。この外部インターフェイスは外部ネットワークに面しています。


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

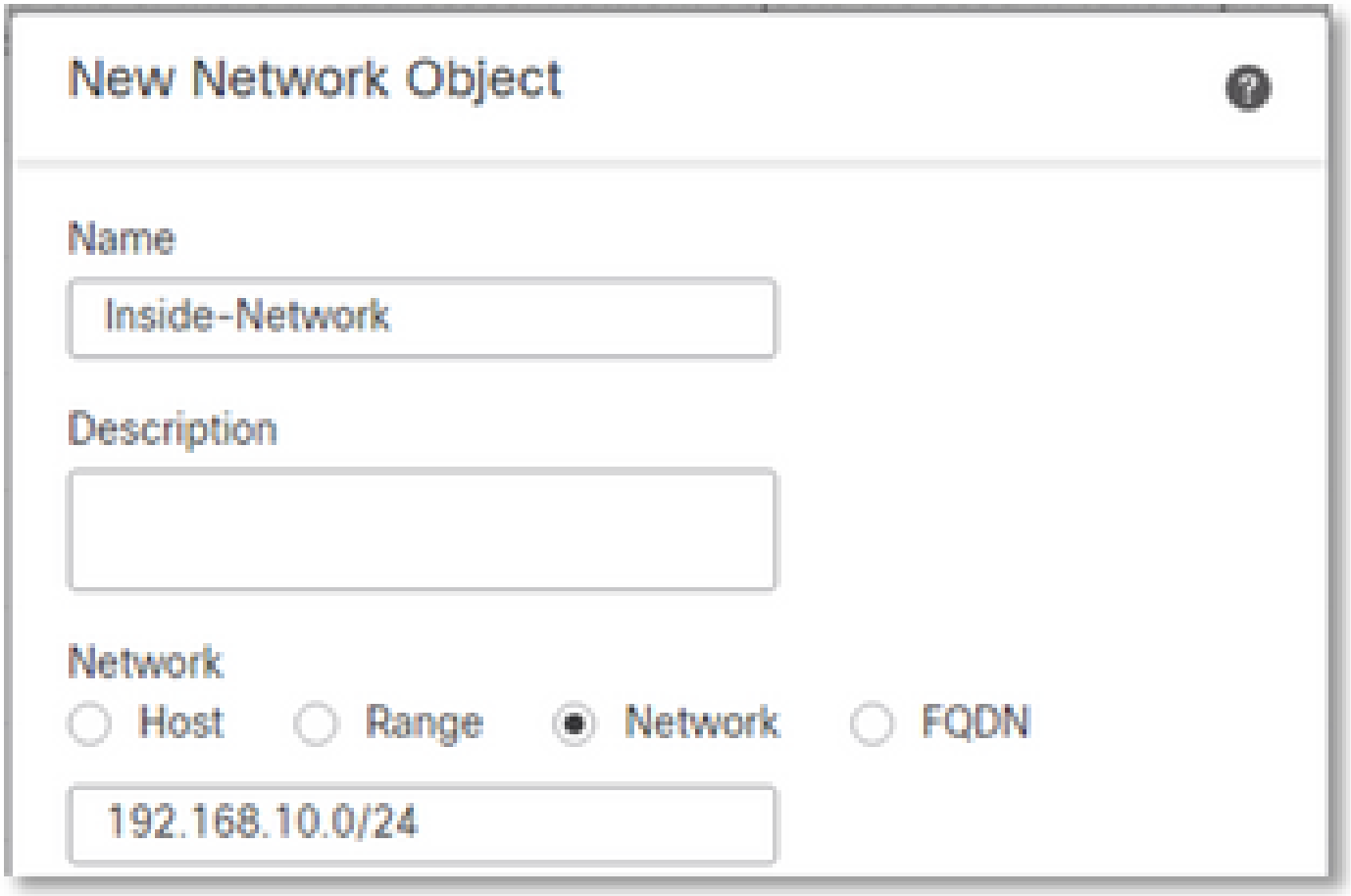


ネットワークオブジェクトの設定

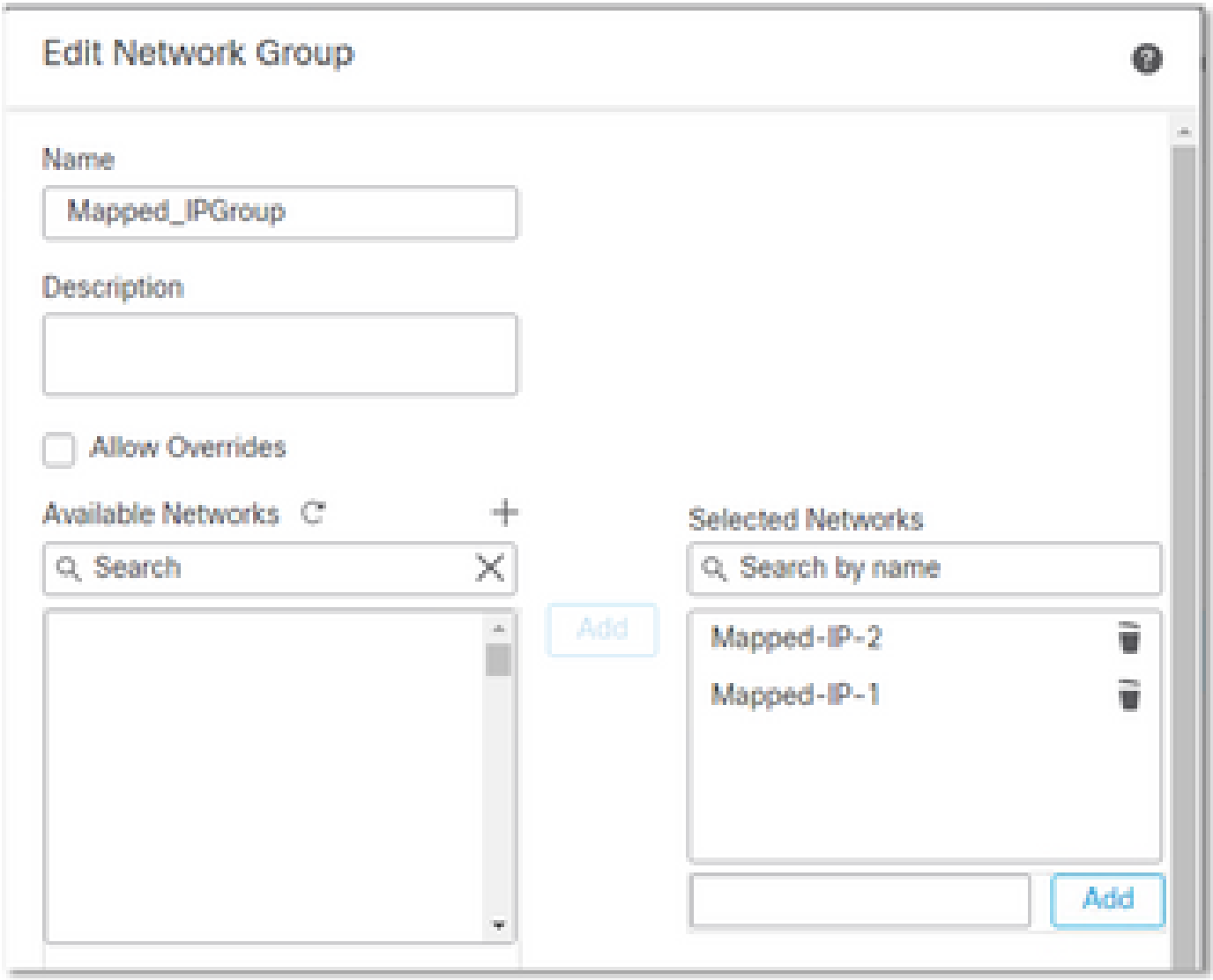
クラスタPATは出力インターフェイスまたは1つのIPと連携してすべてのトラフィックをマップできますが、ベストプラクティスは、クラスタ内のFTDユニットの数と少なくとも同数のIPを持つIPプールを使用することです。

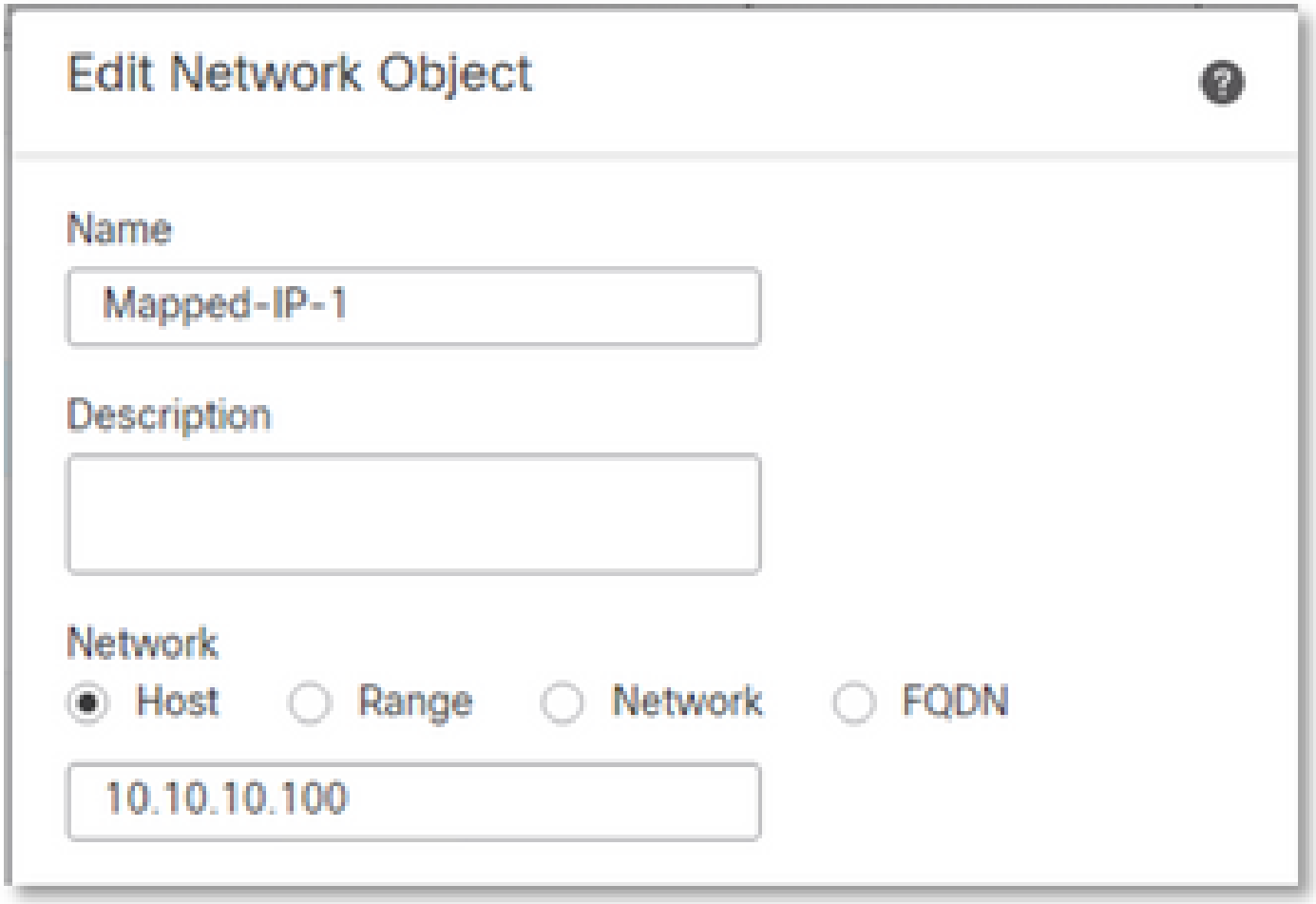
たとえば、RealとマッピングされたIPアドレスに使用されるネットワークオブジェクトは、それぞれInside-NetworkとMapped-IPGroupです。

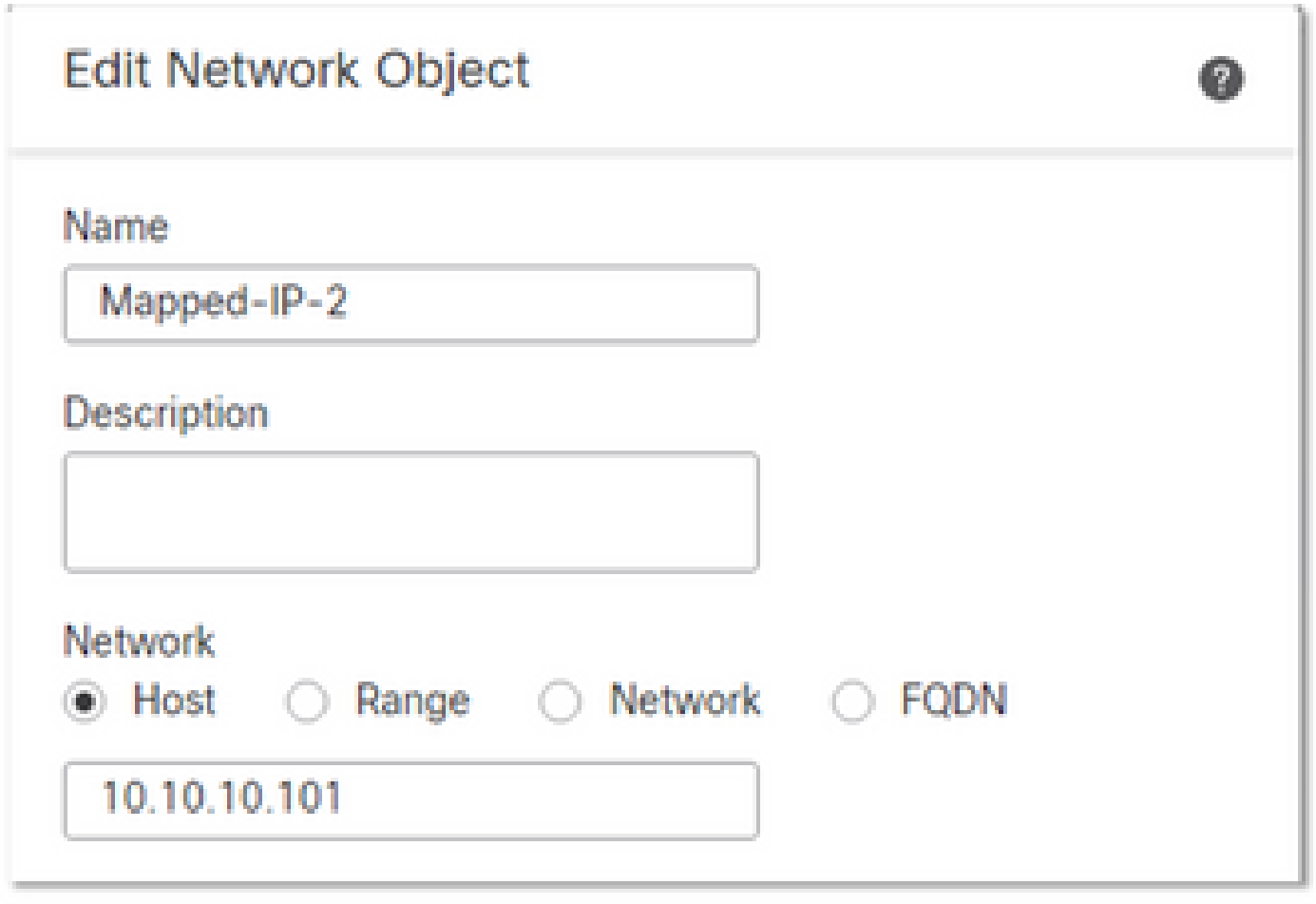
Inside-Networkは内部ネットワーク192.168.10.0/24を表します。



Mapped-IPGroup（Mapped-IP-1 10.10.10.100およびMapped-IP-2 10.10.10.101で構成）は、すべての内部トラフィックをOutside-Zoneにマップするために使用されます。


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

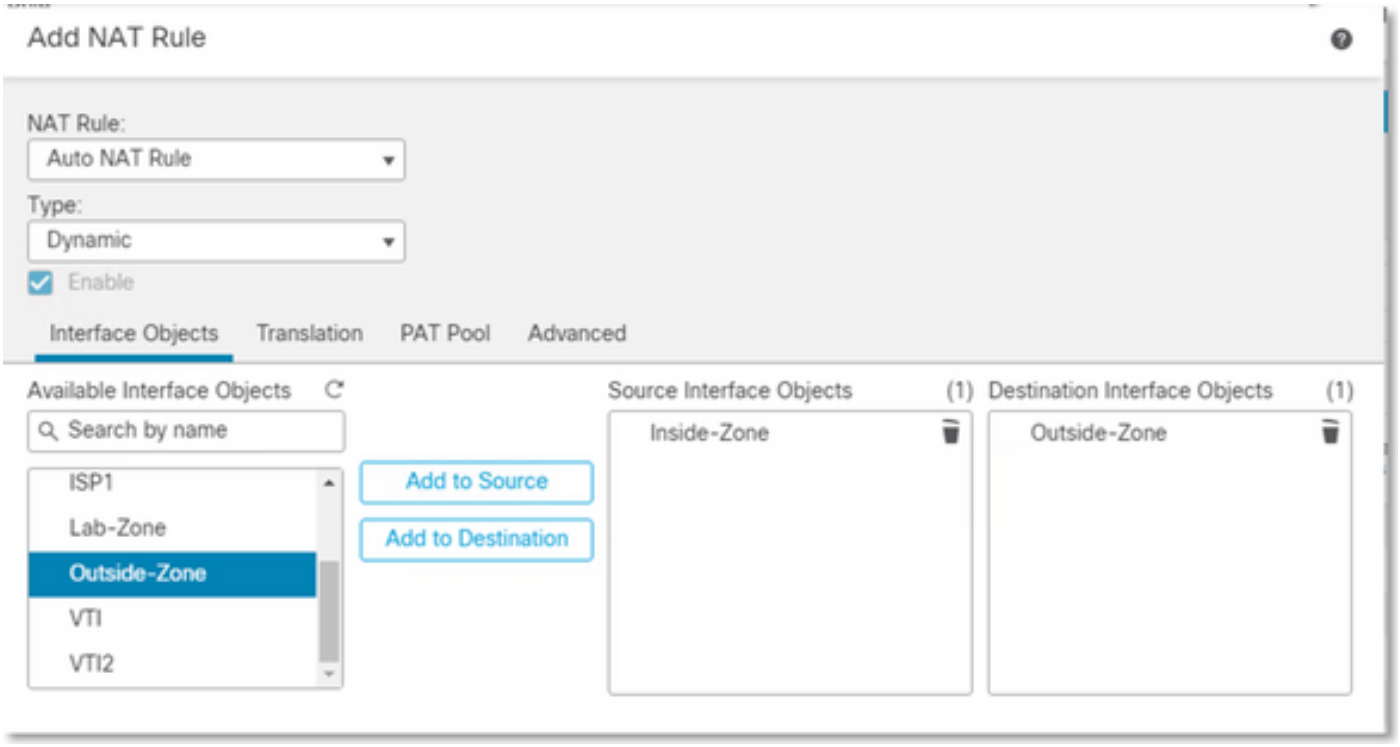

Edit Network Object
Name
Mapped-IP-1
Description
Network
Host
Range
Network
FQDN
10.10.10.100

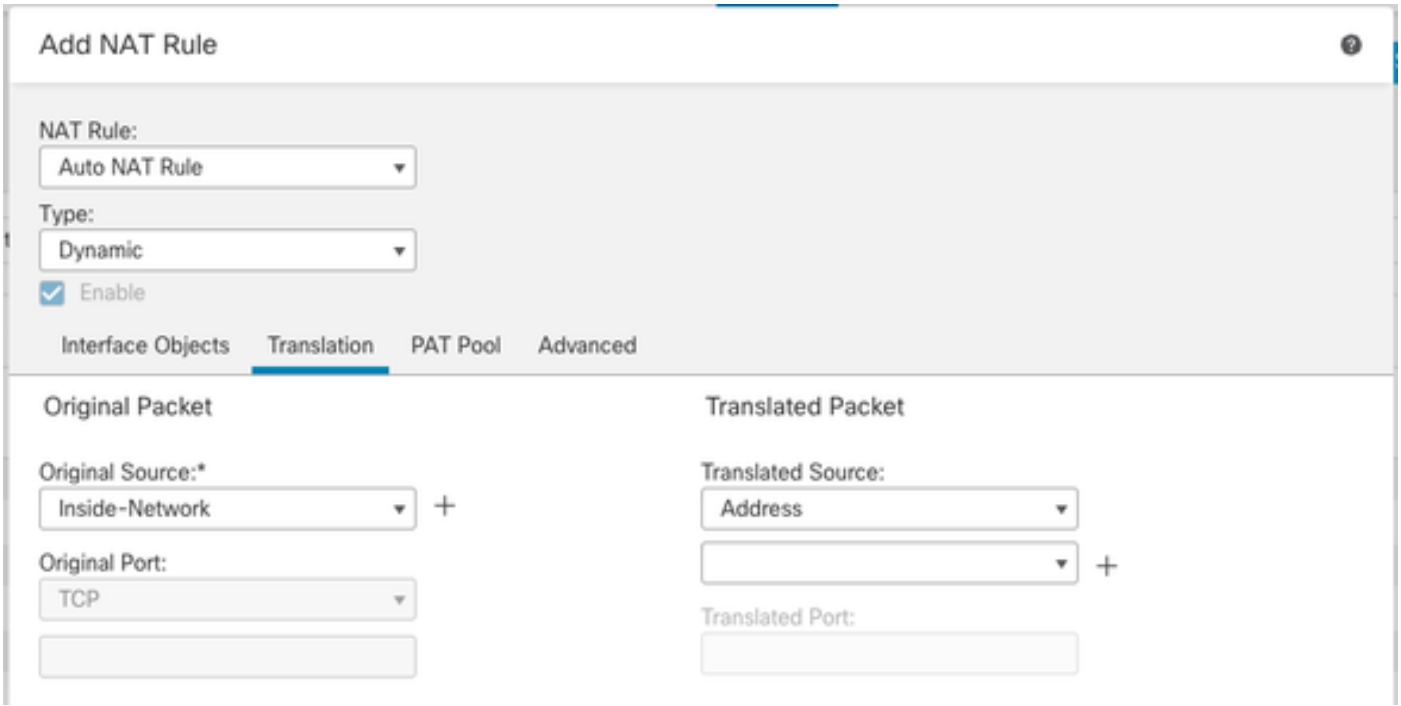

Edit Network Object
Name
Mapped-IP-2
Description
Network
Host
Range
Network
FQDN
10.10.10.101

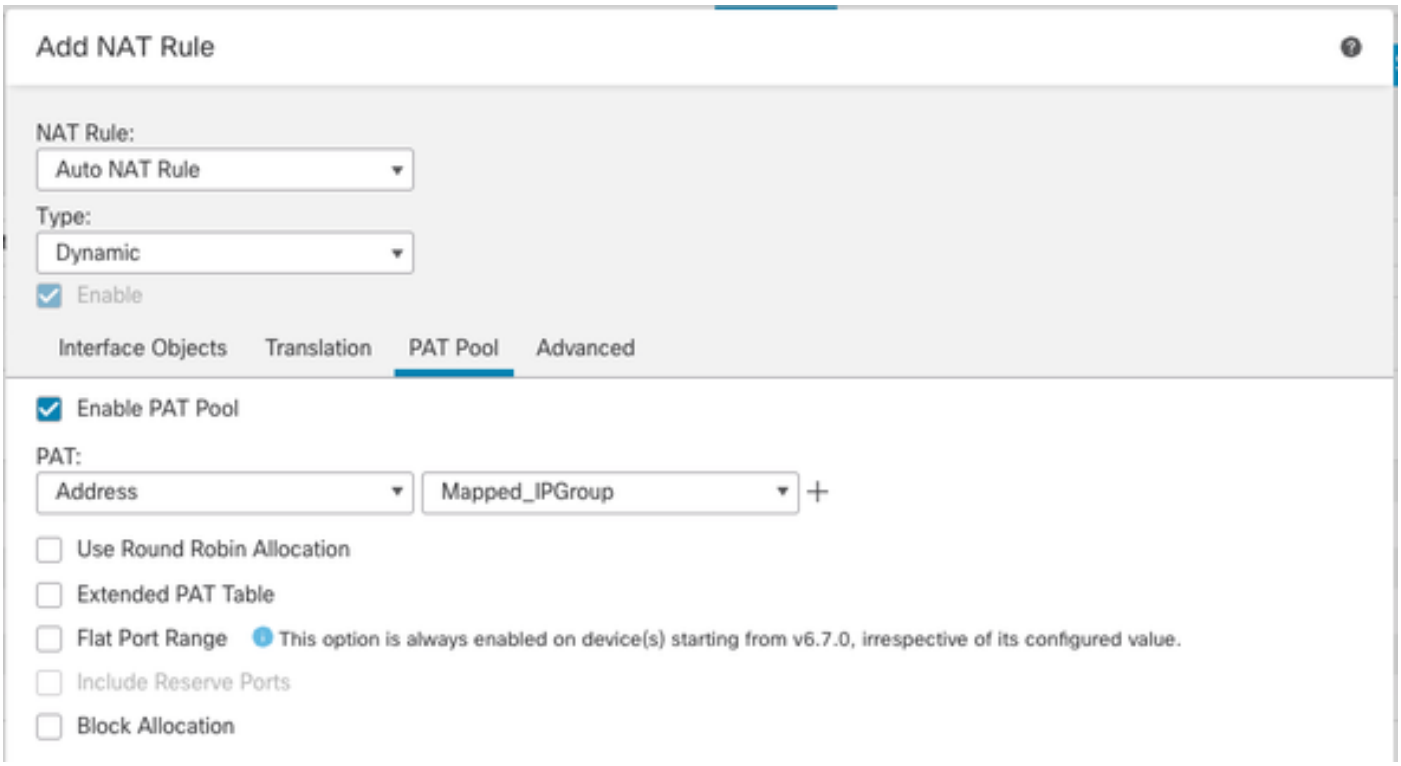
ダイナミックPATの設定

- 発信トラフィックのダイナミックNATルールを設定します。このNATルールは、内部ネットワークサブネットを外部NATプールにマッピングします。

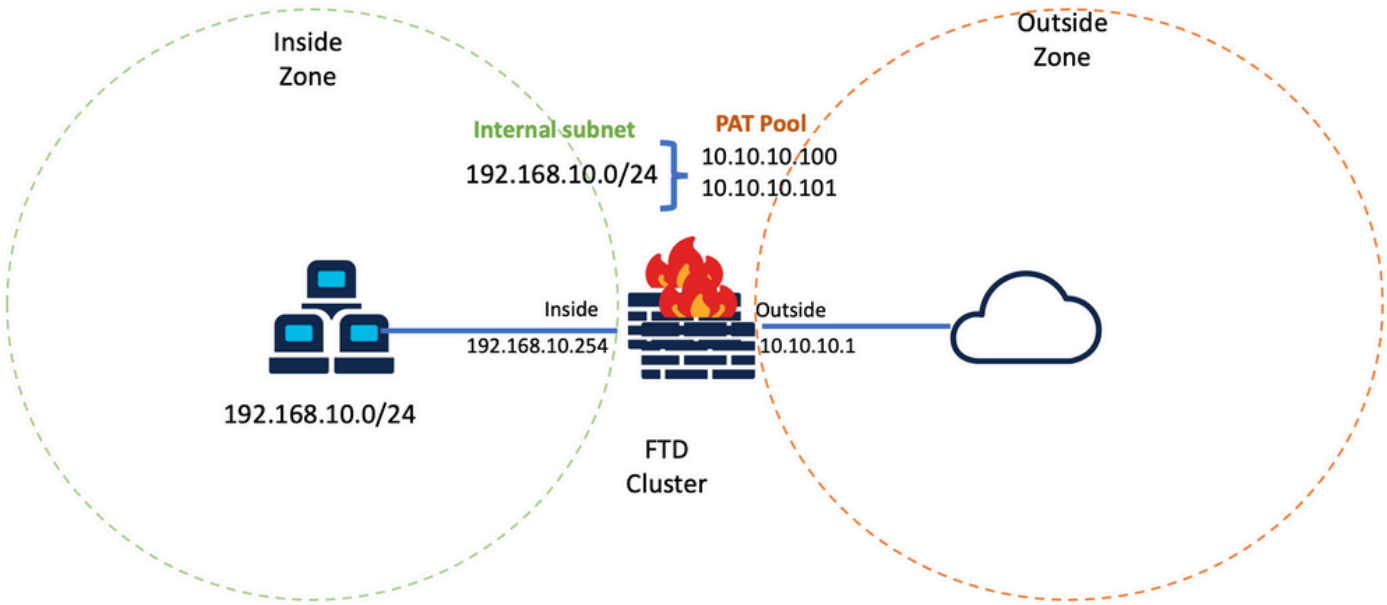
たとえば、Inside-NetworkからのInside-ZoneからOutside-Zoneへのトラフィックは、Mapped-IPGroup Poolに変換されます。







Final Configuration



ラボの最終セットアップ。

確認

このセクションでは、設定が正常に動作していることを確認します。

IPインターフェイスとNAT設定の確認

<#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
```

ポートブロック割り当ての確認

Firepower 7.0以降では、改良されたPATポートブロック割り当てにより、コントロールユニットがノードの結合のためにポートを予約し、未使用のポートを予防的に再要求します。 ポート割り当ては次のように機能します。

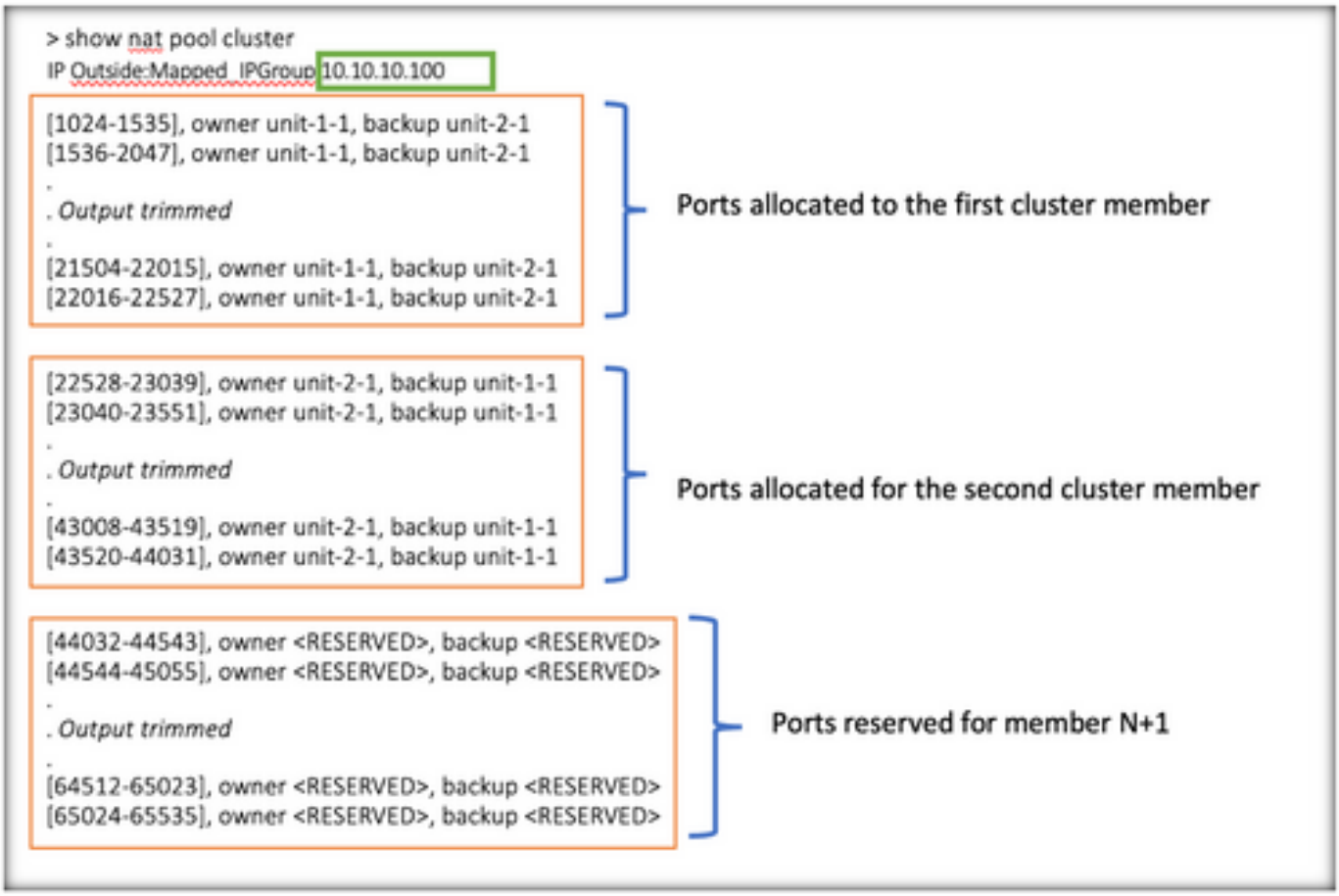
- 起動中のクラスタでは、最初は制御ユニットがポートの50%を所有し、残りは予約されています。
- ユニットあたりの所有ポートブロック数は、クラスタに参加するノードが増えるにつれて調整されます。
- 制御装置は、クラスタがいっぱいになるまで(N+1)ノードのポートブロックを予約します。 クラスタメンバーの制限は、コマンドで定義されcluster-member-limit 、クラスタグループ設定レベルで設定されます。
- デフォルトでは、cluster-member-limitは16です。
  <#root>

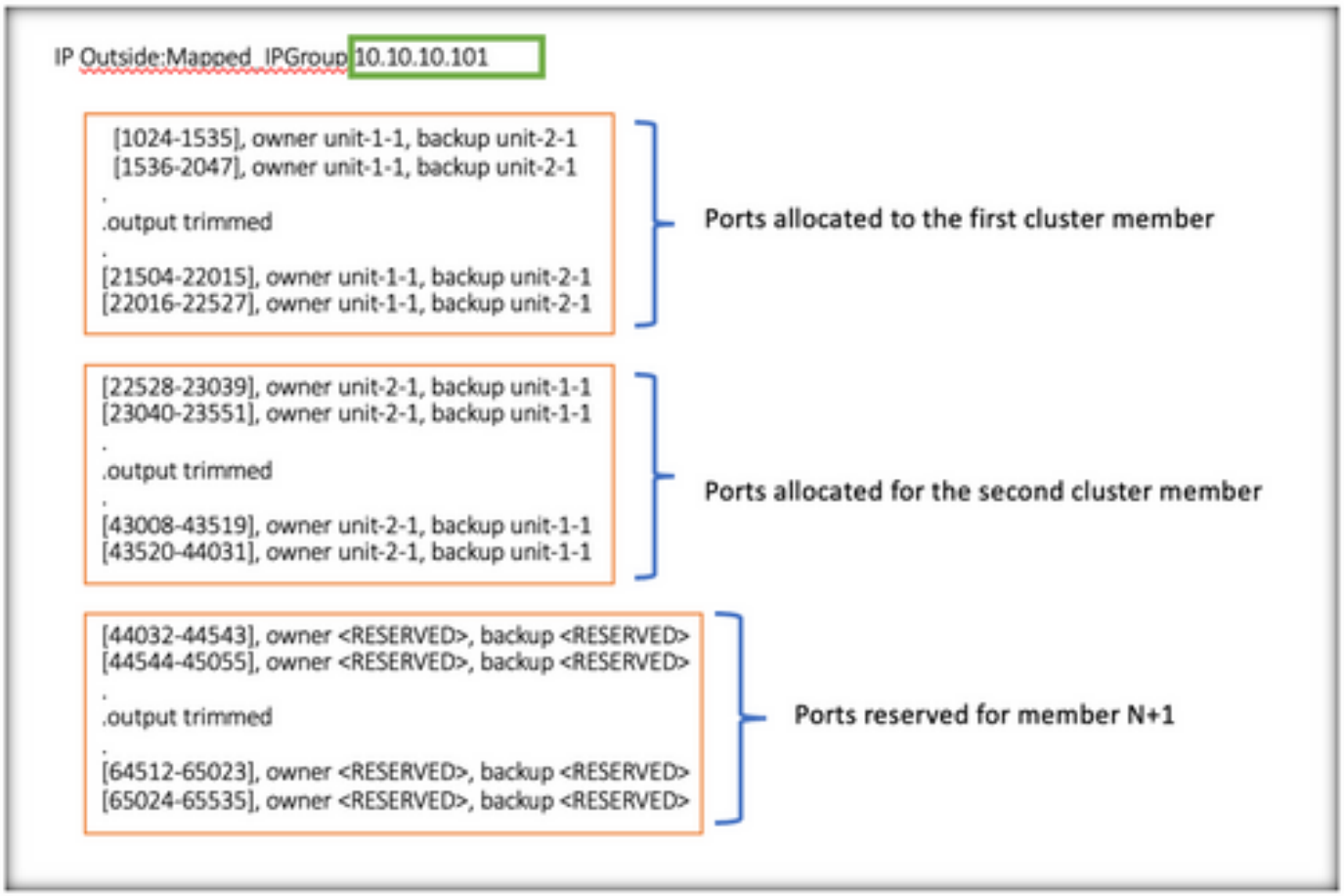
  ```
  > show cluster info

  Cluster FTD-Cluster: On
  Interface mode: spanned

  Cluster Member Limit : 16


  [...]
  ```

- クラスタメンバの量がで設定された値に達すると、すべてのポートブロックがクラスタメンバ間で分散さcluster-member-limitれます。

たとえば、クラスタメンバー制限のデフォルト値が16の2つのユニット(N=2)で構成されるクラスタグループでは、ポート割り当てがN+1メンバー（この場合は3）に対して定義されていることが

確認されます。これにより、クラスタの最大数に達するまで、次のユニット用に予約されたポートが残ります。

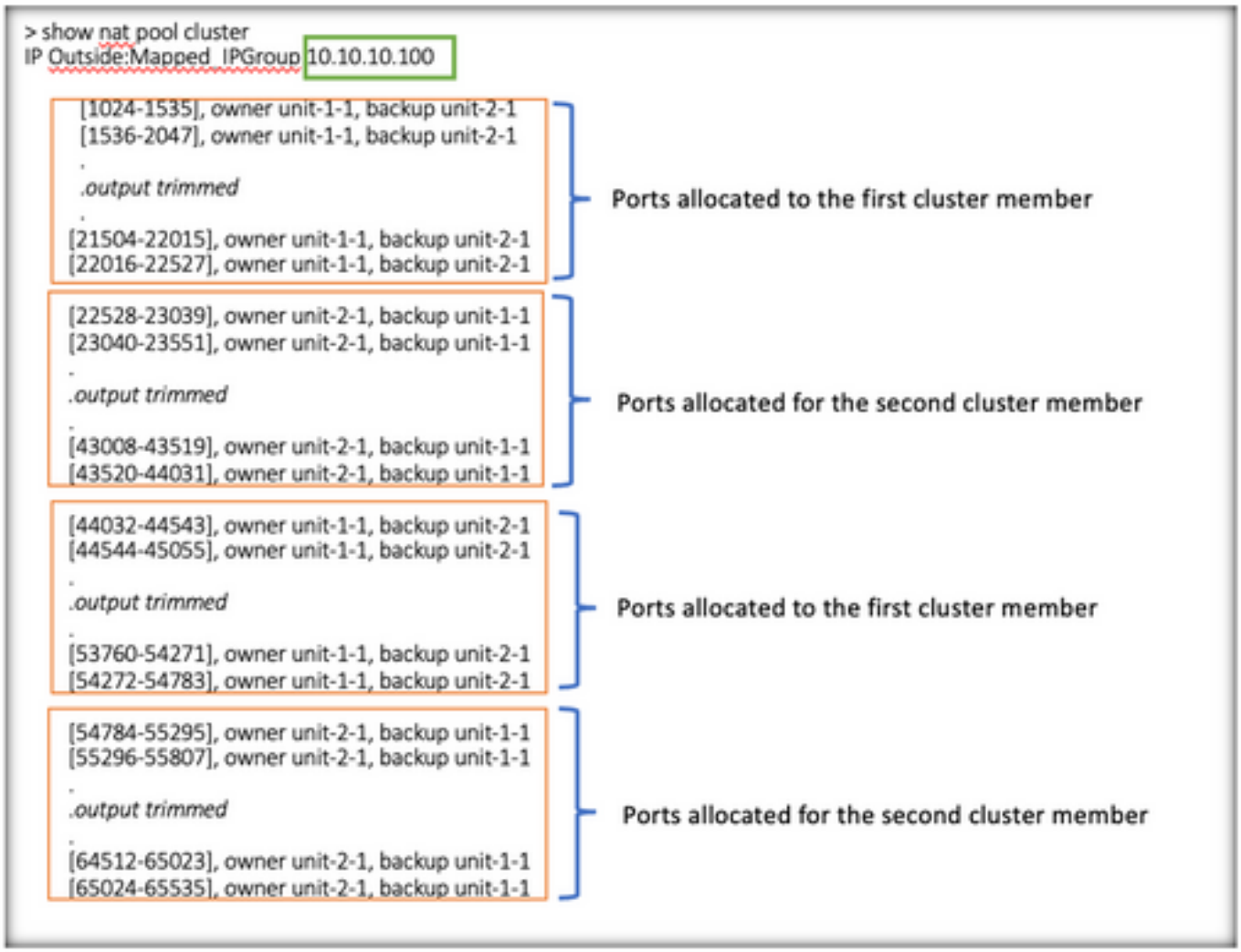


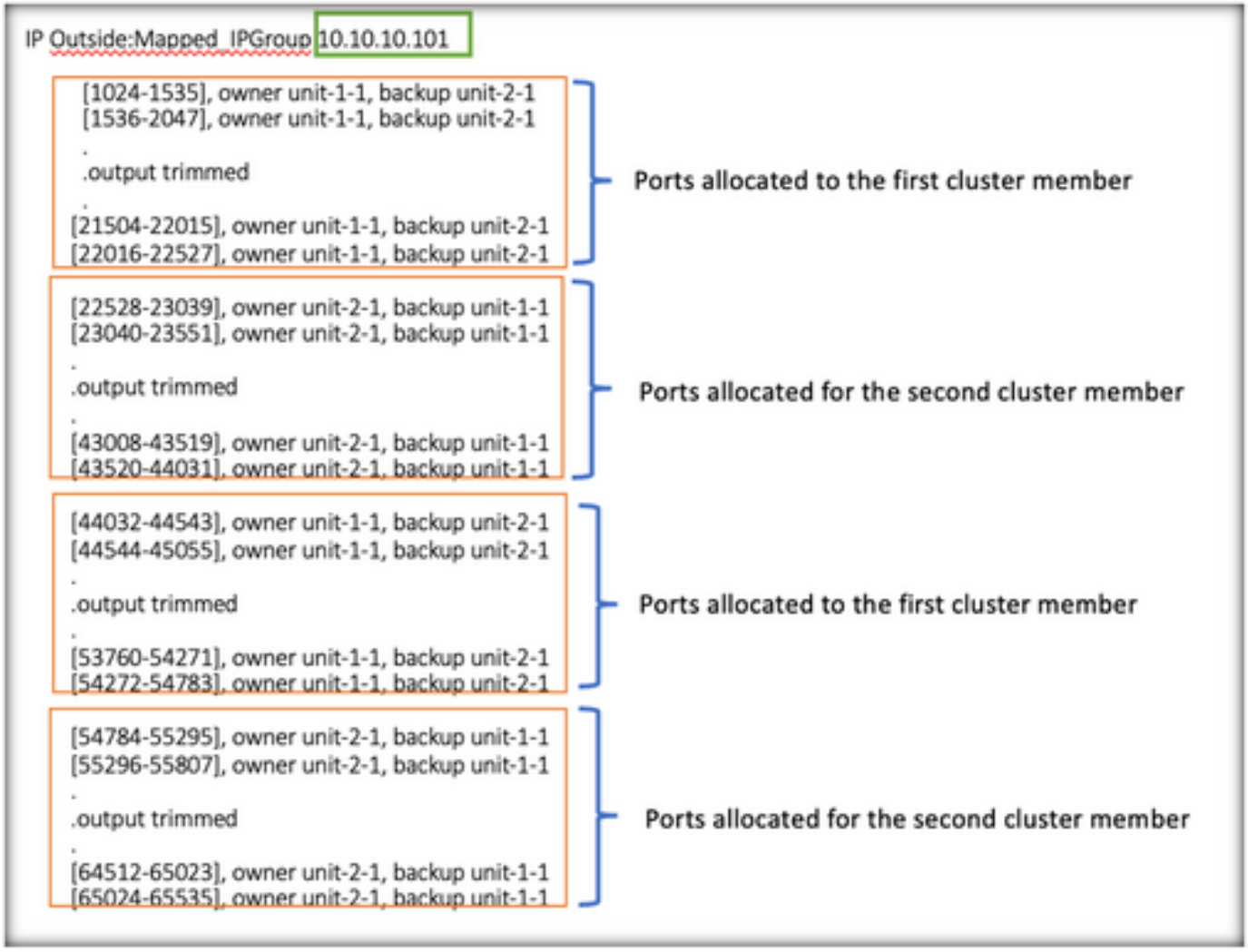



```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IP-1 10.10.10.100 (126 - 42 / 42) ^ 42 # 0
IP Outside:Mapped-IP-1 10.10.10.101 (126 - 42 / 42) ^ 42 # 0
```

また、クラスタの導入で計画されたユニット数cluster-member-limit に合わせてを設定することがベストプラクティスです。

たとえば、クラスタメンバー制限の値が2の2つのユニット(N=2)で構成されるクラスタグループでは、ポート割り当てがすべてのクラスタユニットに均等に分散されることが確認されます。予約済みポートは残っていません。


> 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 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
Ports allocated to the first cluster member
[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 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
```

ポートブロック再利用の確認

- 新しいノードがクラスタに参加またはクラスタから離れるたびに、すべてのユニットの未使用ポートと超過ポートブロックをコントロールユニットに解放する必要があります。
- ポートブロックがすでに使用されている場合、最も使用率の低いポートブロックが再利用のためにマークされます。
- 再要求されたポートブロックでは、新しい接続は許可されません。最後のポートがクリアされると、コントロールユニットに解放されます。

```
> 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
```

トラブルシューティングのためのコマンド

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

- 設定されているcluster-member-limit値を確認します。

<#root>

> show cluster info

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

Cluster Member Limit : 2

```
[...]
```

> show running-config cluster

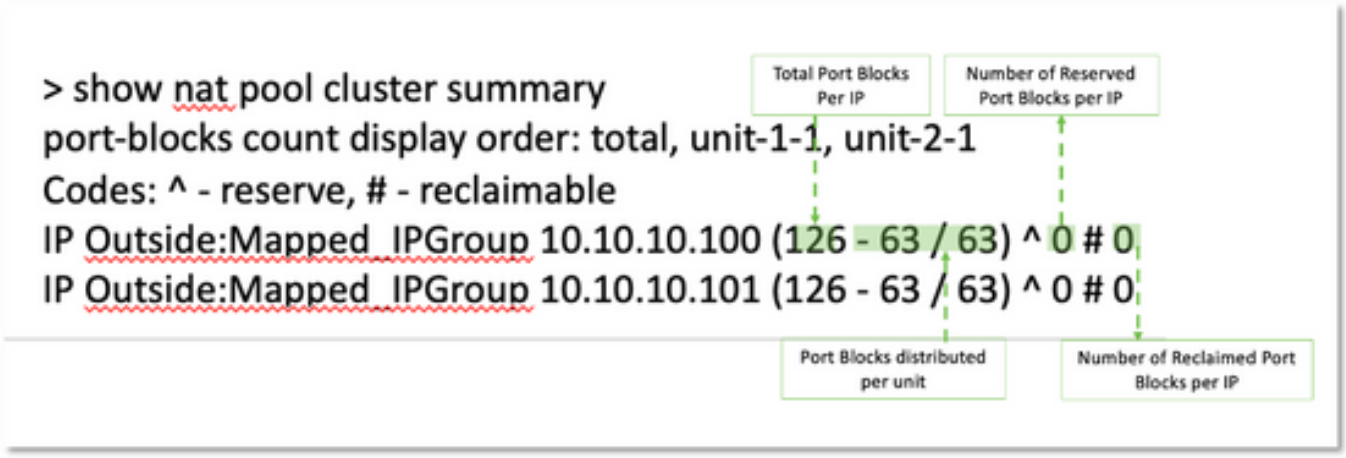
```
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0
```

cluster-member-limit 2
[...]

- クラスタ内のユニット間の分散をブロックするポートの要約を表示します。

<#root>

> show nat pool cluster summary



- PATアドレスごとのポートブロックの所有者とバックアップユニットへの現在の割り当てを表示します。

<#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
[...]
```

- ポートブロックの配布と使用に関連する情報を表示します。

<#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
[...]
```

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。