Comprendre l'allocation de ports sur la PAT dynamique pour le cluster FTD 7.0

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configurer
Diagramme du réseau
Configuration de lâ€™interface
Configuration des objets réseau
Configuration PAT dynamique
Configuration finale
Vérifier
Vérification de lâ€™interface IP et de la configuration NAT
Vérifier l'allocation des blocs de ports
Vérification de la récupération des blocs de ports
Dépannage des commandes
Informations connexes

Introduction

Ce document décrit comment la distribution basée sur les blocs de ports fonctionne dans la PAT dynamique pour le cluster de pare-feu après la version 7.0 et ultérieure.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Traduction d'adresses réseau (NAT) sur Cisco Secure Firewall

Composants utilisés

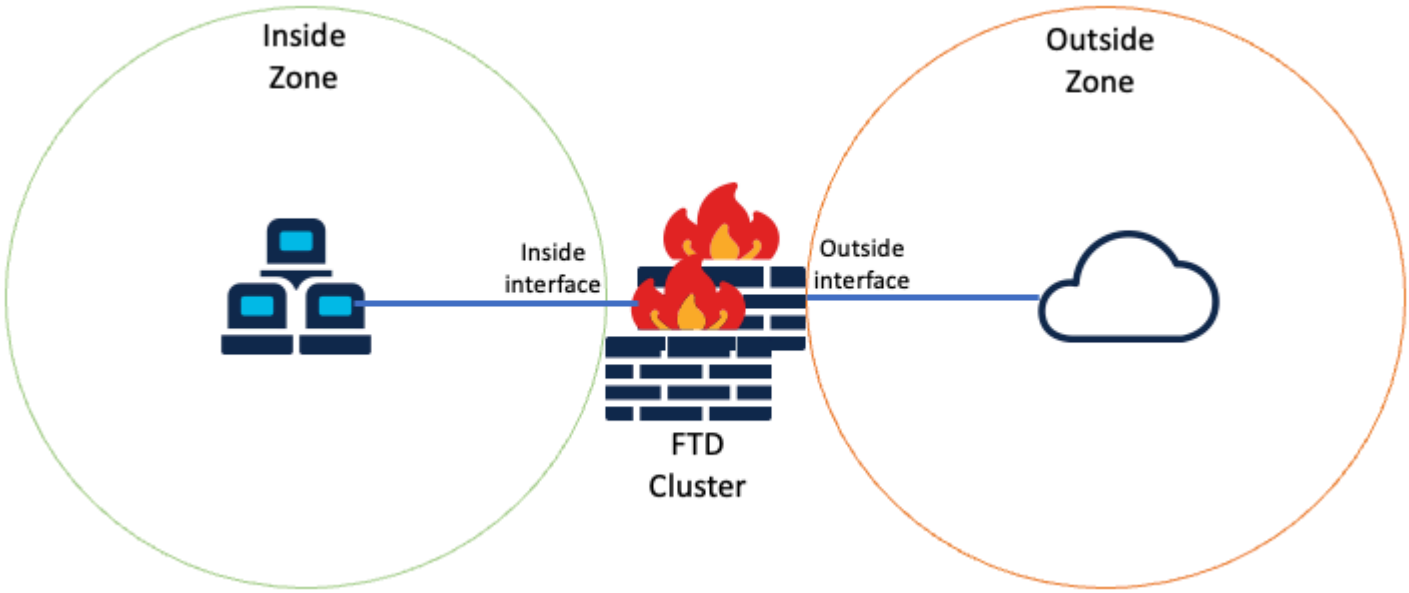
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Management Center 7.3.0
- Défense contre les menaces Firepower 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. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Configurer

Diagramme du réseau

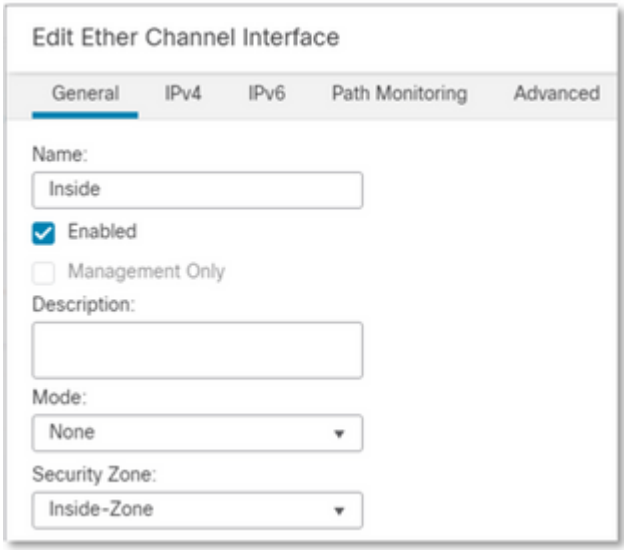


Topologie logique

Configuration de lâ€™interface

- Configurez le membre d'interface interne de la zone interne.

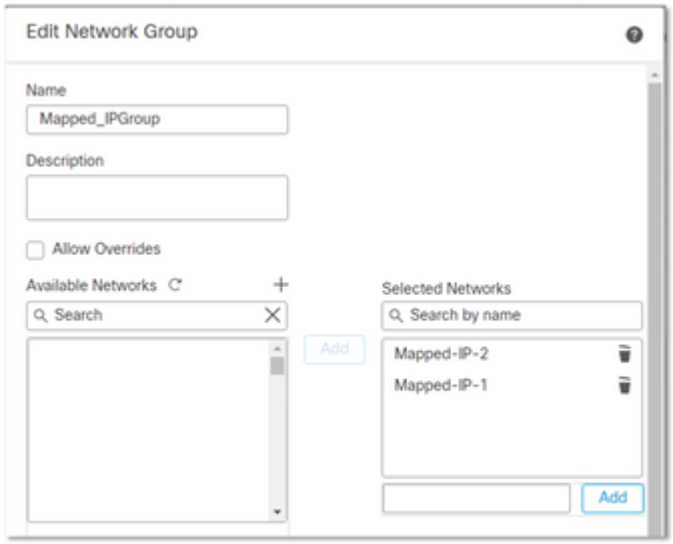
Par exemple, configurez une interface avec l'adresse IP 192.168.10.254 et nommez-la **Inside**. Cette interface interne est la passerelle du réseau interne 192.168.10.0/24.

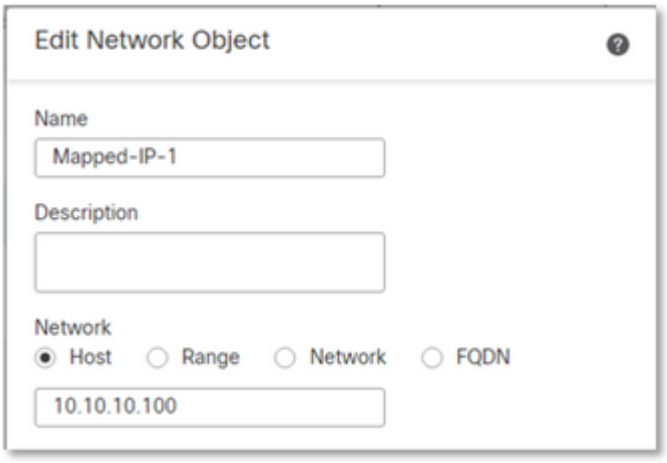


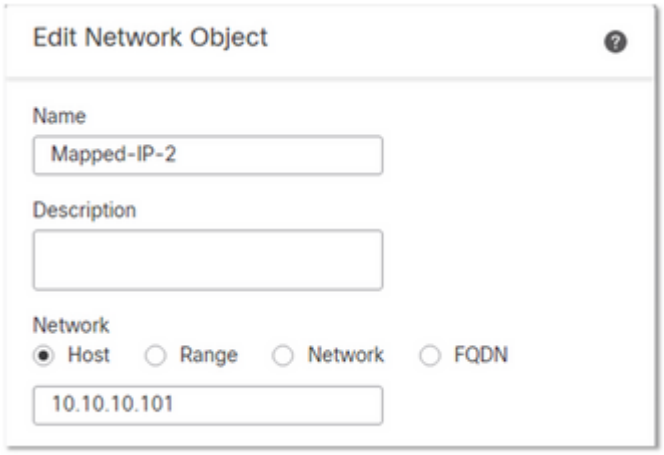
- Configurez le membre d'interface externe de la zone externe.

Par exemple, configurez une interface avec l'adresse IP 10.10.10.254 et nommez-la Outside. Cette interface

(composé de Mapped-IP-1 10.10.10.100 et Mapped-IP-2 10.10.10.101), est utilisé pour mapper tout le trafic interne vers la zone externe.



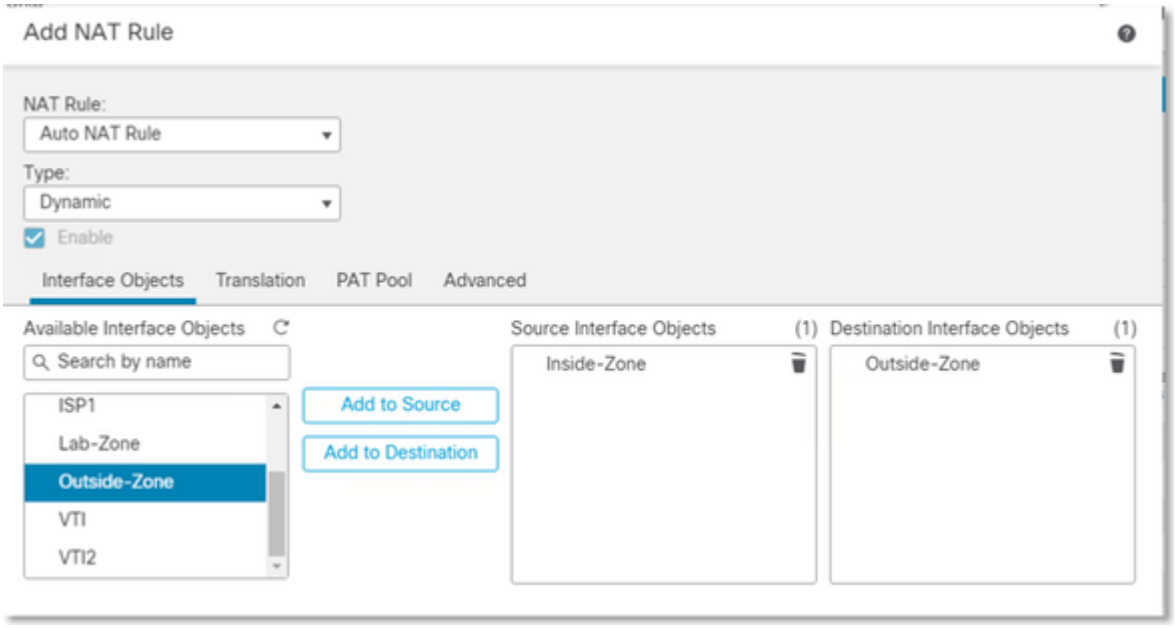


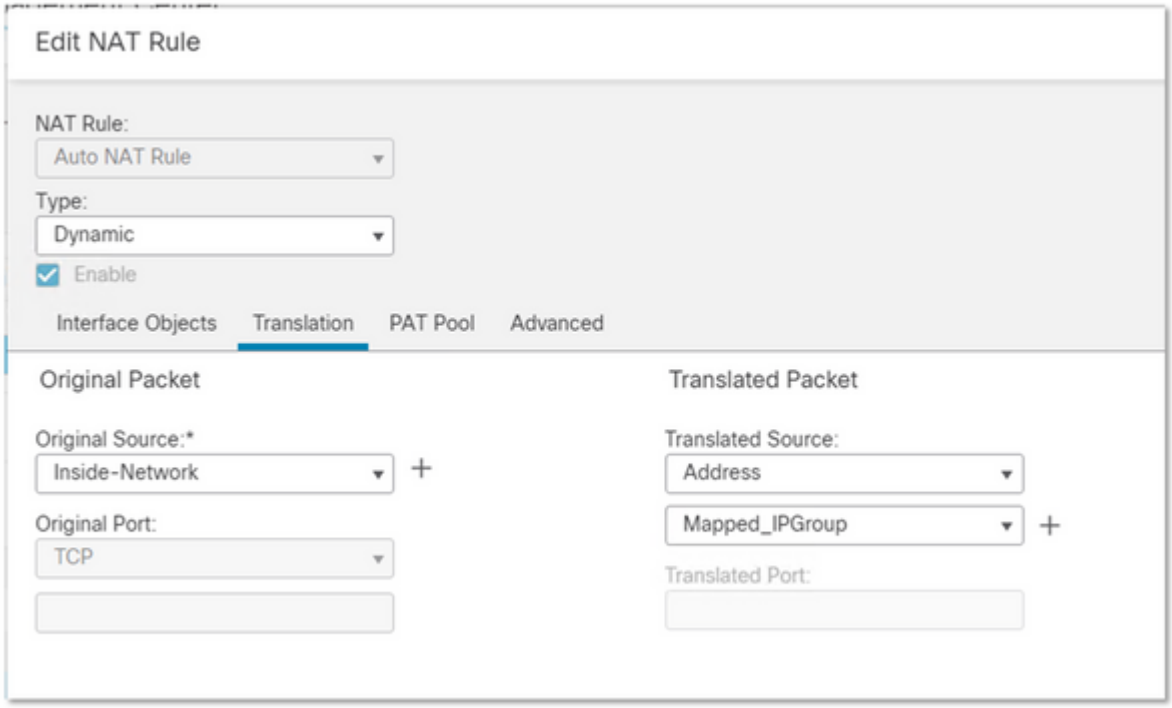


Configuration PAT dynamique

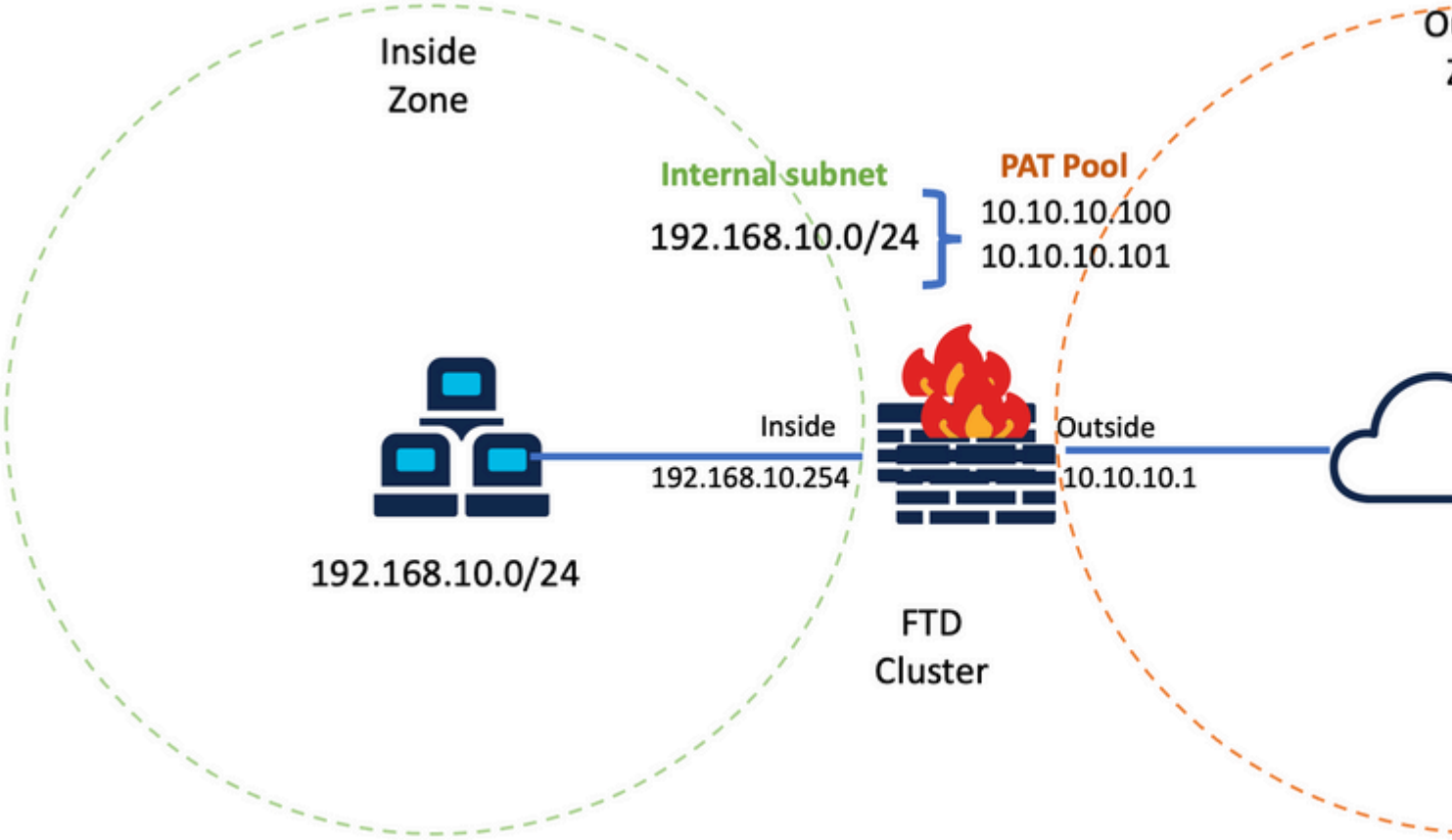
- Configurez une règle NAT dynamique pour le trafic sortant. Cette règle NAT mappe le sous-réseau du réseau interne au pool NAT externe.

Par exemple, le trafic de la zone interne à la zone externe de Inside-Network est traduit en pool de groupes IP mappés.





Configuration finale



Configuration finale des travaux pratiques.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérification de lâ€™interface IP et de la configuration NAT

<#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 Mapped_IPGroup
```

Vérifier l'allocation des blocs de ports

Après Firepower 7.0

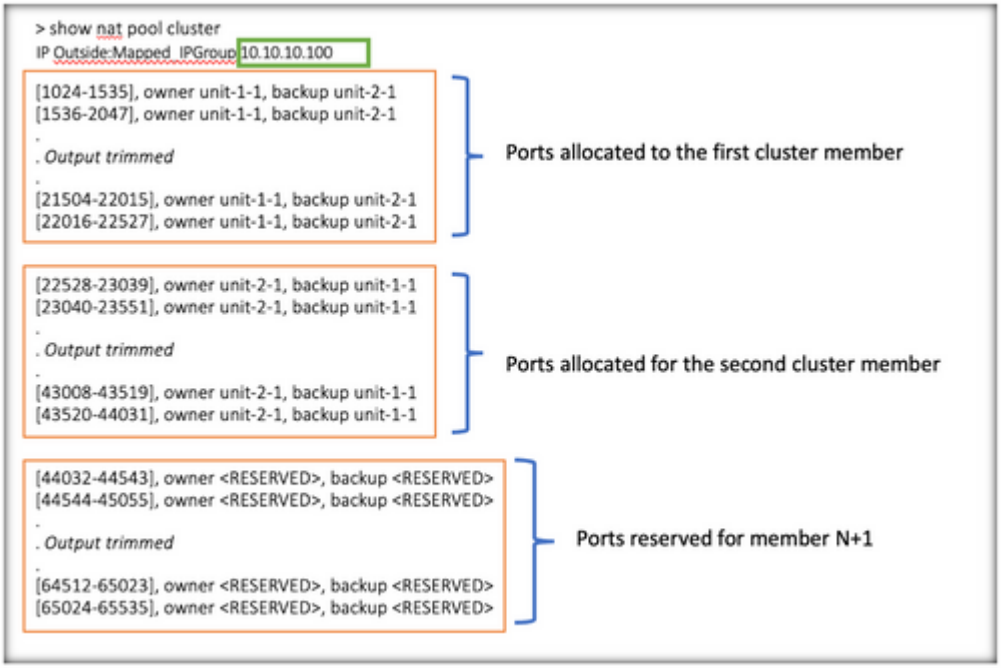
l'allocation de blocs de ports PAT améliorée garantit que l'unité de contrôle conserve les ports en réserve pour joindre les noeuds et récupère de manière proactive les ports inutilisés. Voici comment fonctionne l'allocation de ports :

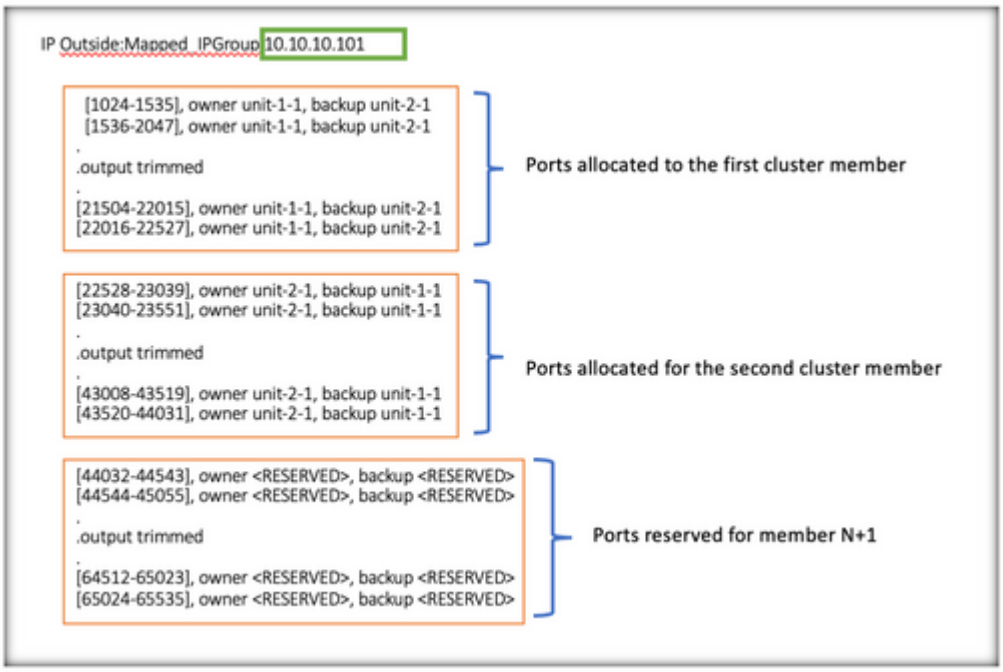
- Sur un cluster qui vient d'être mis en place, l'unité de contrôle possède initialement 50 % des ports et les autres sont réservés.
- Le nombre de blocs de ports détenus par unité est ajusté à mesure que d'autres noeuds rejoignent le cluster.
- L'unité de contrôle réserve des blocs de ports pour les noeuds (N+1) jusqu'à ce que le cluster soit plein**.** La limite de membres du cluster est définie par le cluster-member-limit , configuré sous le niveau de configuration du groupe de clusters.
- Par défaut, cluster-member-limit est 16.
  <#root>

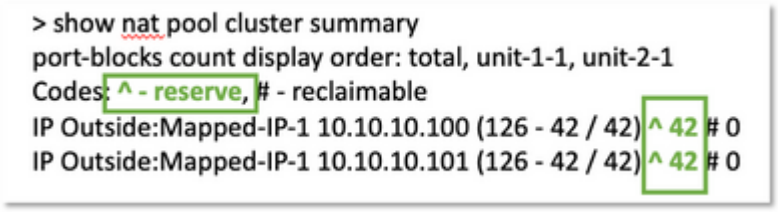
```
> show cluster info

Cluster FTD-Cluster: On
Interface mode: spanned

Cluster Member Limit : 16


[...]
```

- Lorsque la quantité de membres du cluster atteint la valeur configurée avec **cluster-member-limit,** tous les blocs de ports sont distribués entre les membres du cluster.

Par exemple, dans un groupe de grappes constitué de deux unités (N=2) avec une valeur par défaut de limite de membre de grappe de 16, on observe que l'allocation de port est définie pour N+1 membres, en l'occurrence 3. Certains ports restent ainsi réservés à l'unité suivante jusqu'à ce que la limite maximale de cluster soit atteinte.

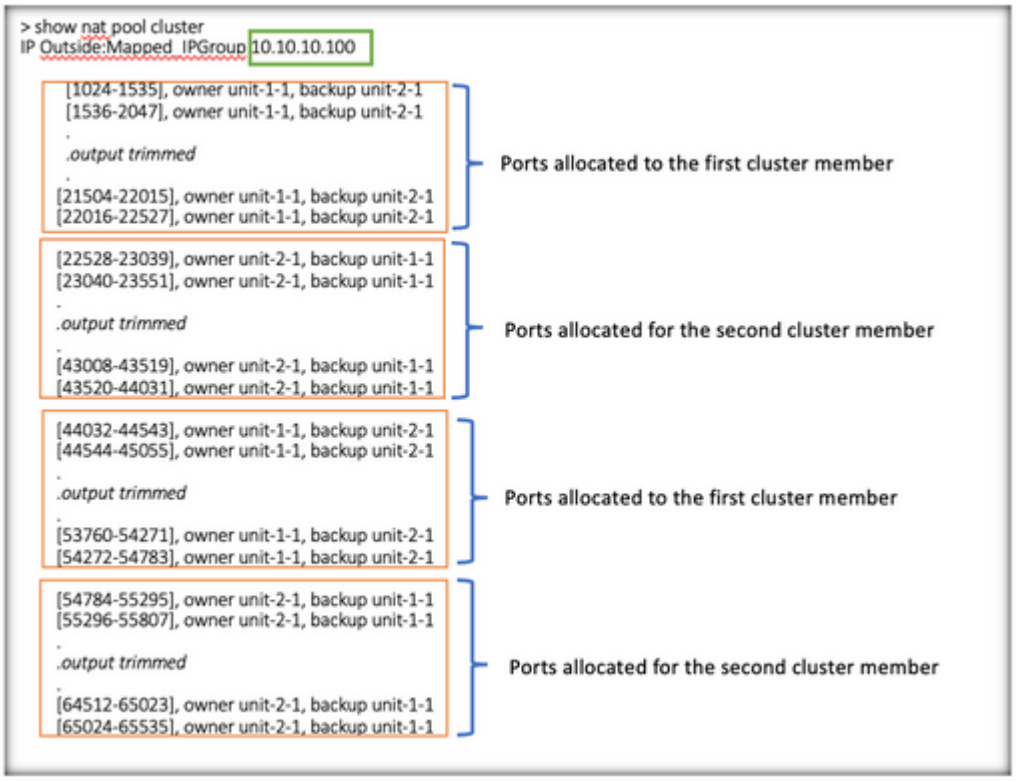


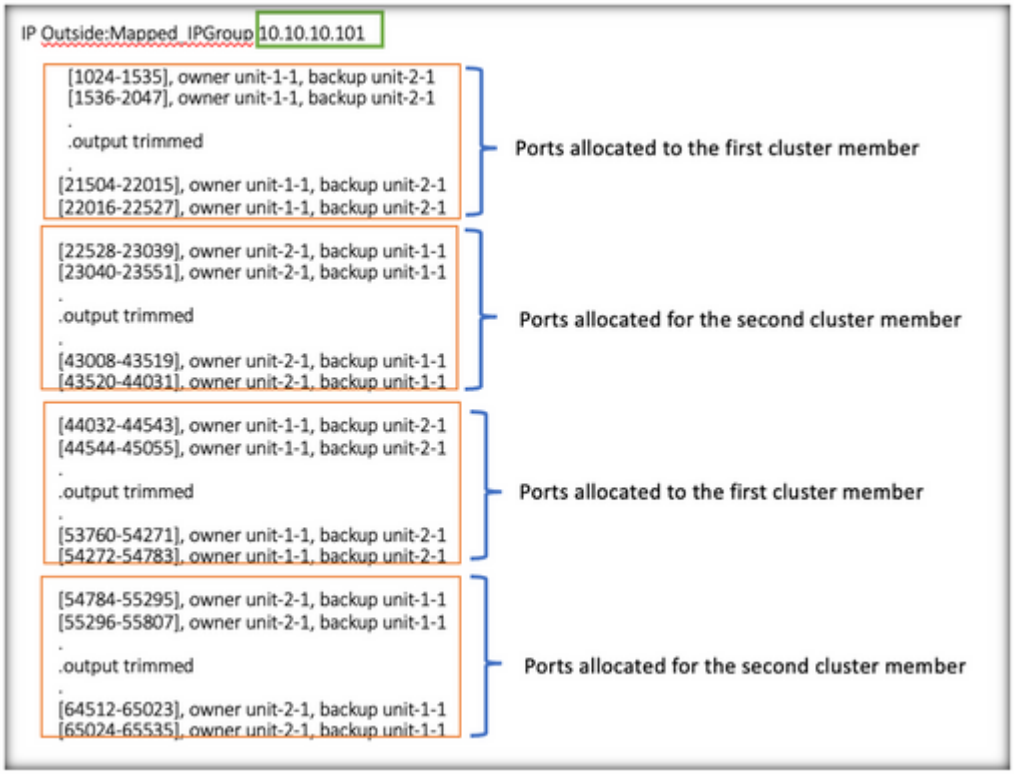




En outre, il est recommandé de configurer le **cluster-member-limit** pour correspondre au nombre d'unités planifiées pour le déploiement de cluster.

Par exemple, dans un groupe de grappes constitué de deux unités (N=2) avec une valeur de limite de membre de grappe de 2, on observe que l'allocation de port est répartie uniformément sur toutes les unités de grappes. Aucun des ports réservés n'est conservé.






```
> 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
```

Vérification de la récupération des blocs de ports

- Chaque fois qu'un nouveau noeud rejoint ou quitte une grappe, les ports inutilisés et les blocs de ports excédentaires de toutes les unités doivent être libérés vers l'unité de contrôle.
- Si les blocs de ports sont déjà utilisés, les moins utilisés sont marqués pour la récupération.
- Les nouvelles connexions ne sont pas autorisées sur les blocs de ports récupérés. Ils sont libérés vers l'unité de contrôle lorsque le dernier port est effacé.

```
> 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
```

Dépannage des commandes

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Vérifiez la valeur cluster-member-limit configurée :

<#root>

> show cluster info

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

Cluster Member Limit : 2

```
[...]
```

> show running-config cluster

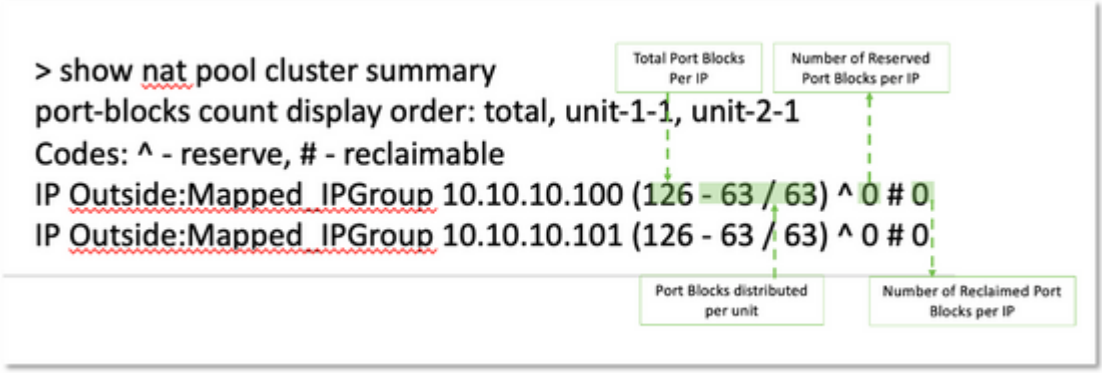
```
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0
```

cluster-member-limit 2
[...]

- Affichez un résumé de la distribution des blocs de ports parmi les unités du cluster :

<#root>

> show nat pool cluster summary



- Affichez l'attribution actuelle des blocs de ports par adresse PAT au propriétaire et à l'unité de sauvegarde :

<#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
[...]
```

- Afficher les informations relatives à la distribution et à l'utilisation des blocs de ports :

<#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
[...]
```

Informations connexes

- **Assistance technique et téléchargements Cisco**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.