Begrijp poorttoewijzing op Dynamic PAT voor FTD Cluster 7.0

Inhoud

Inleiding

In dit document wordt beschreven hoe op poortblokken gebaseerde distributie in Dynamic PAT for Firewall Cluster na versie 7.0 en hoger werkt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Netwerkadresomzetting (NAT) op Cisco Secure Firewall

Gebruikte componenten

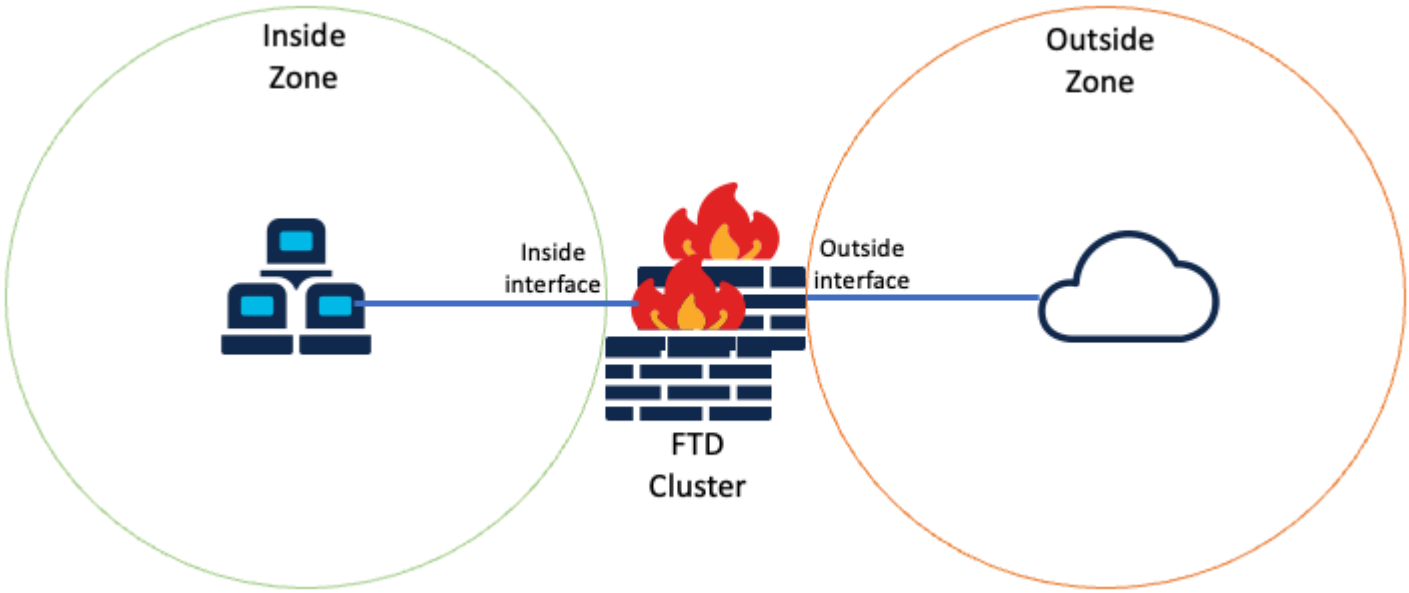
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Management Center 7.3.0
- Firepower Threat Defense 7.2.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram

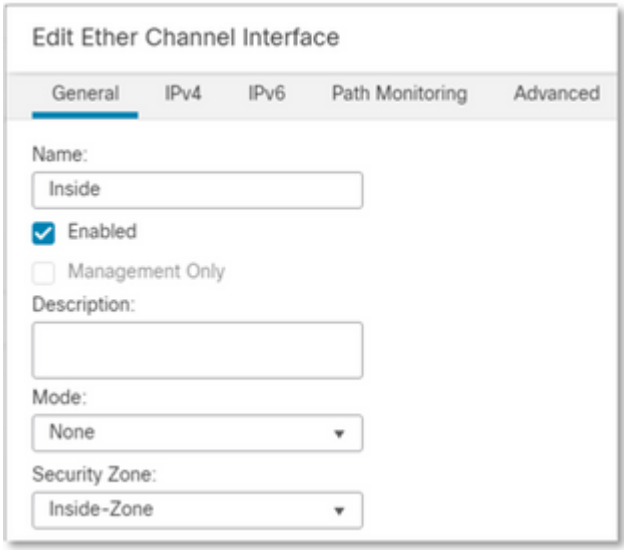


Logische topologie

Interface-configuratie

- Configureer binnen interfacelid van Inside Zone.

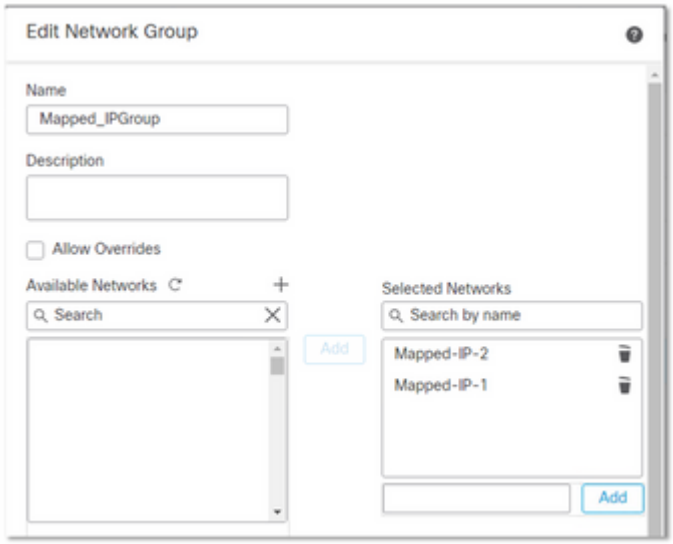
Configureer bijvoorbeeld een interface met IP-adres 192.168.10.254 en noem het **binnen**. Deze Inside interface is de Gateway voor intern netwerk 192.168.10.0/24.

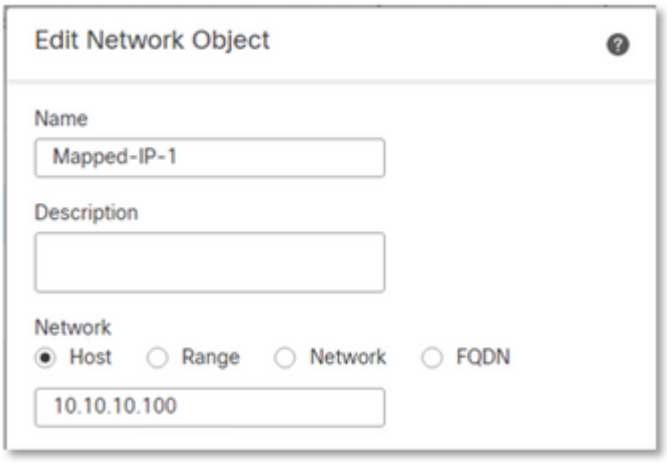


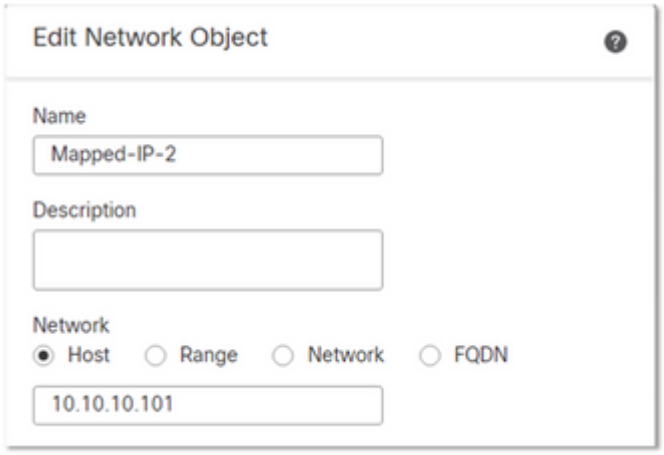
- Configureer de externe interface van Outside Zone.

Configureer bijvoorbeeld een interface met IP-adres 10.10.10.254 en noem het buiten. Deze buiteninterface

(gemaakt van in kaart gebracht-IP-1 10.10.10.100 en in kaart gebracht-IP-2 10.10.10.10.101), wordt gebruikt om al het interne verkeer aan de Buiten-Zone in kaart te brengen.



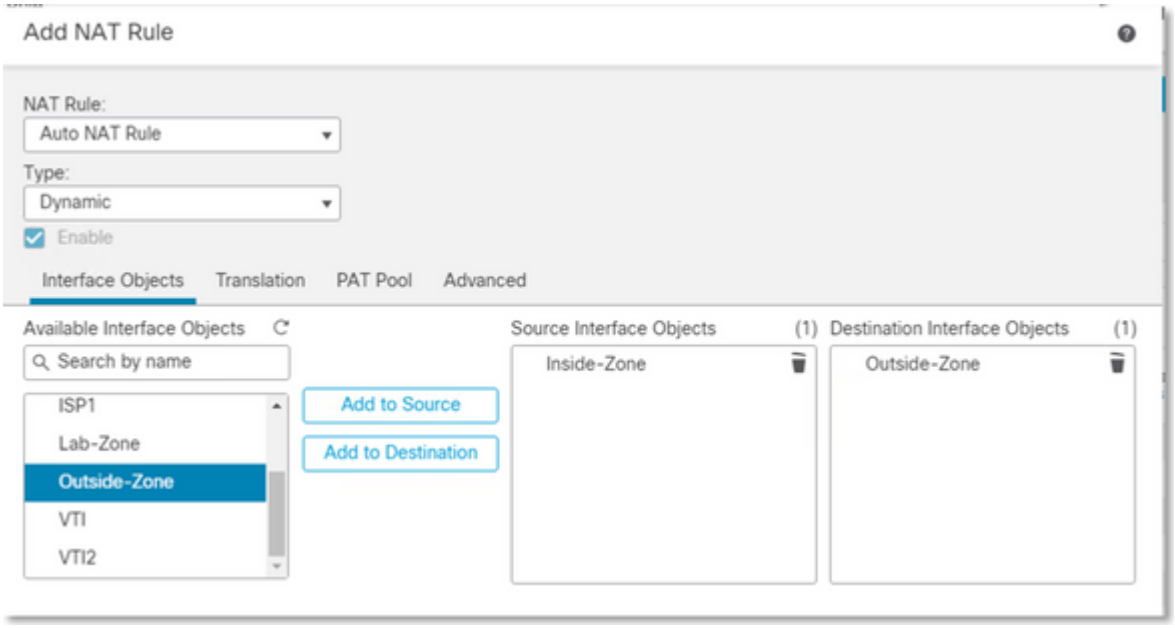


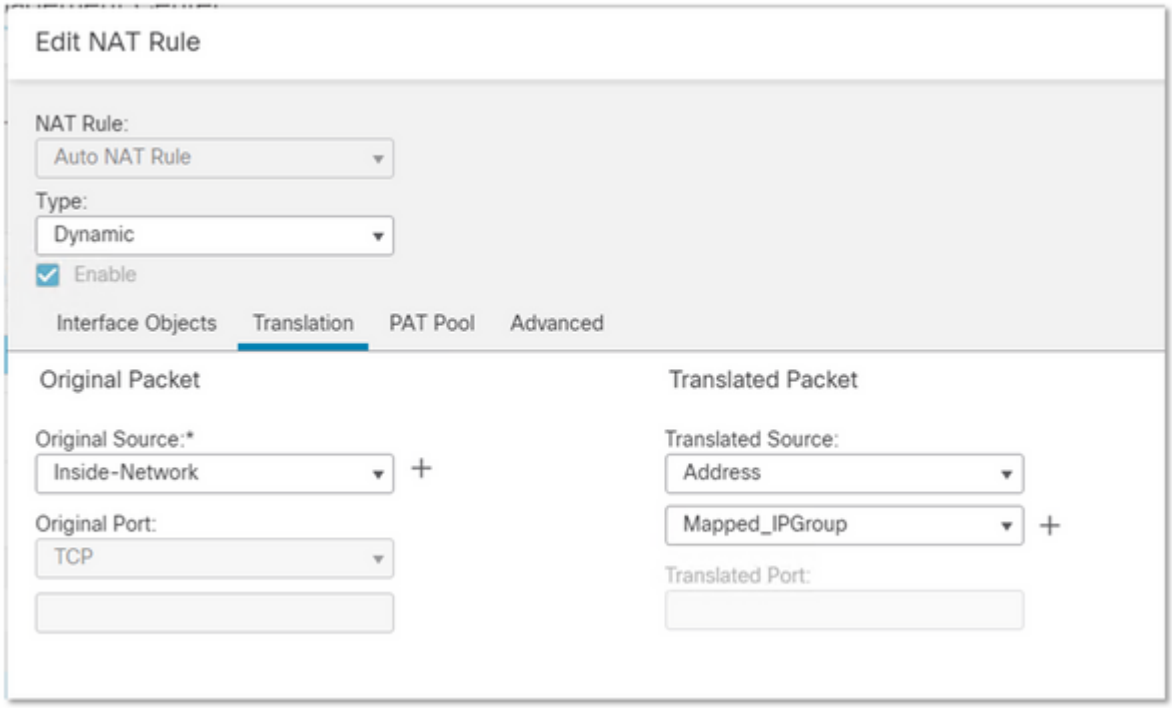


Dynamische PAT-configuratie

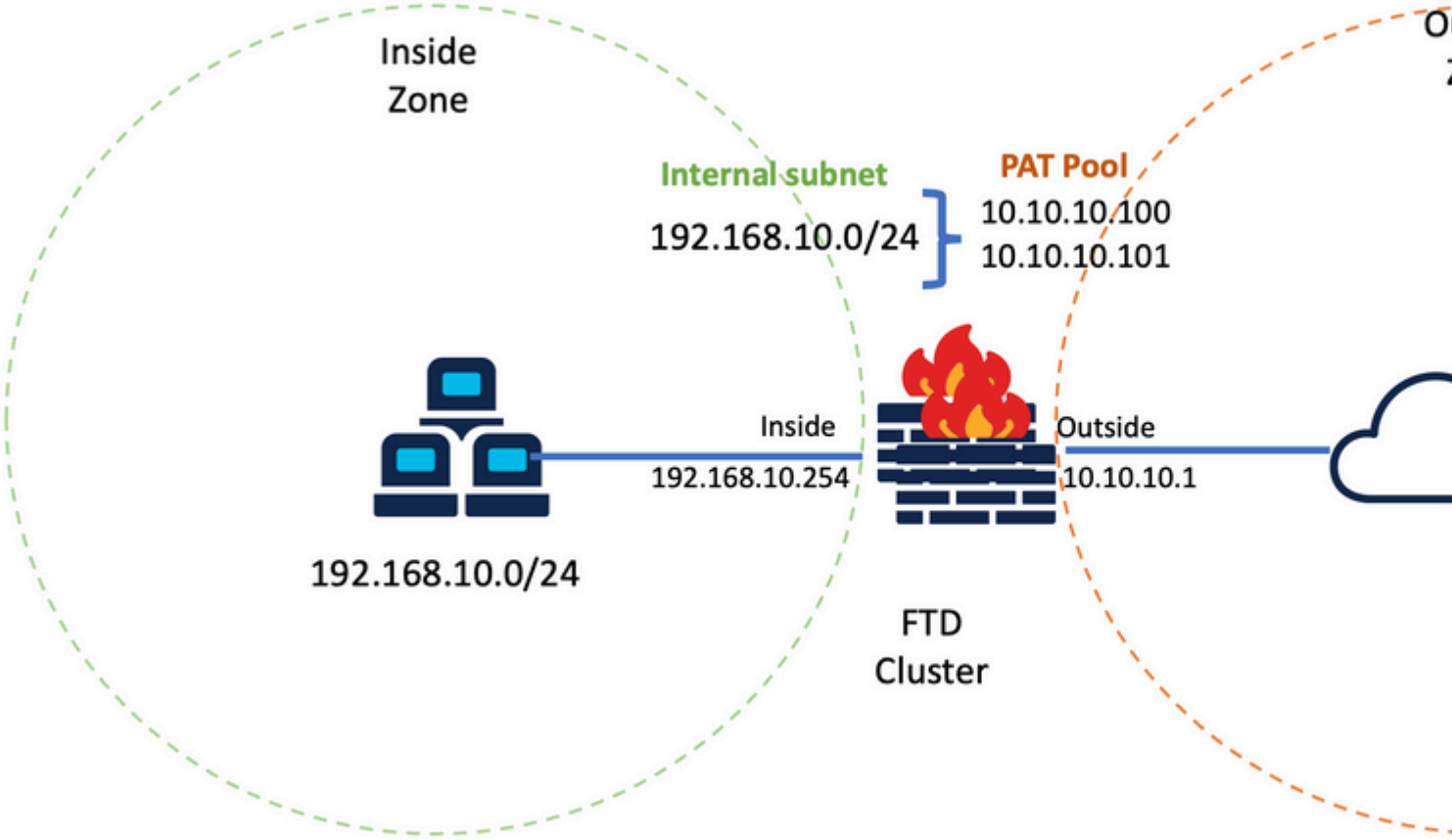
- Configureer een dynamische NAT-regel voor uitgaand verkeer. Deze NAT-regel koppelt het interne netwerksubnet aan de externe NAT-pool.

Bijvoorbeeld, binnen-zone naar buiten-zone verkeer van binnen-netwerk wordt vertaald aan in kaart gebracht-IProup Pool.





Laatste configuratie



Definitieve installatie van het lab.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Controleer IP-interface en NAT-configuratie

<#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
```

Controleer de toewijzing van poortblokken

Na Firepower 7.0

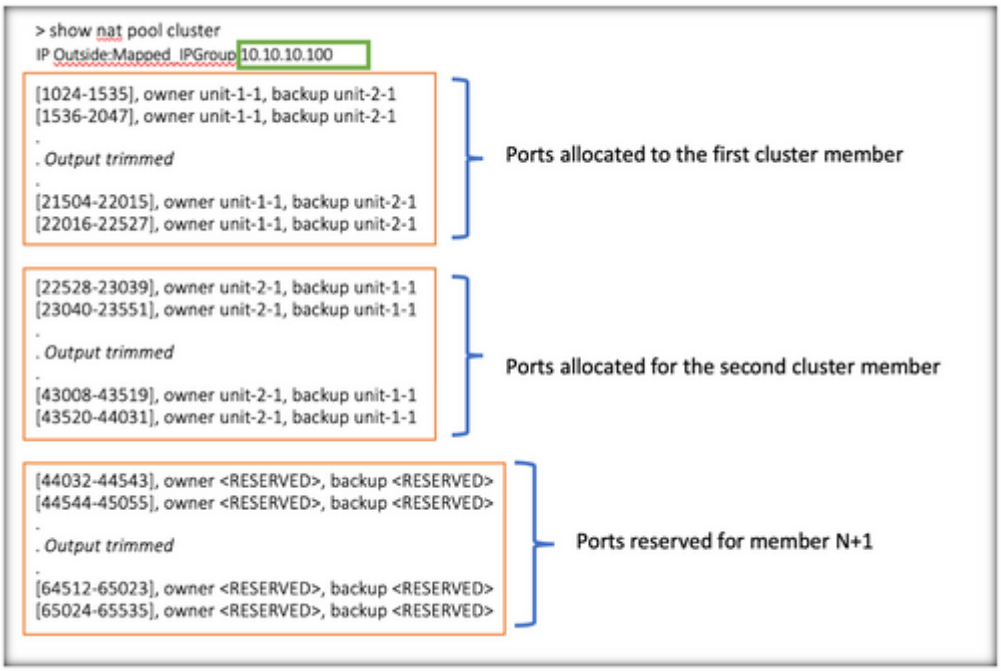
zorgt de verbeterde PAT-poortbloktoewijzing ervoor dat de regeleenheid poorten in reserve houdt voor het aansluiten van knooppunten en proactief ongebruikte poorten terugwint. Zo werkt de haventoewijzing:

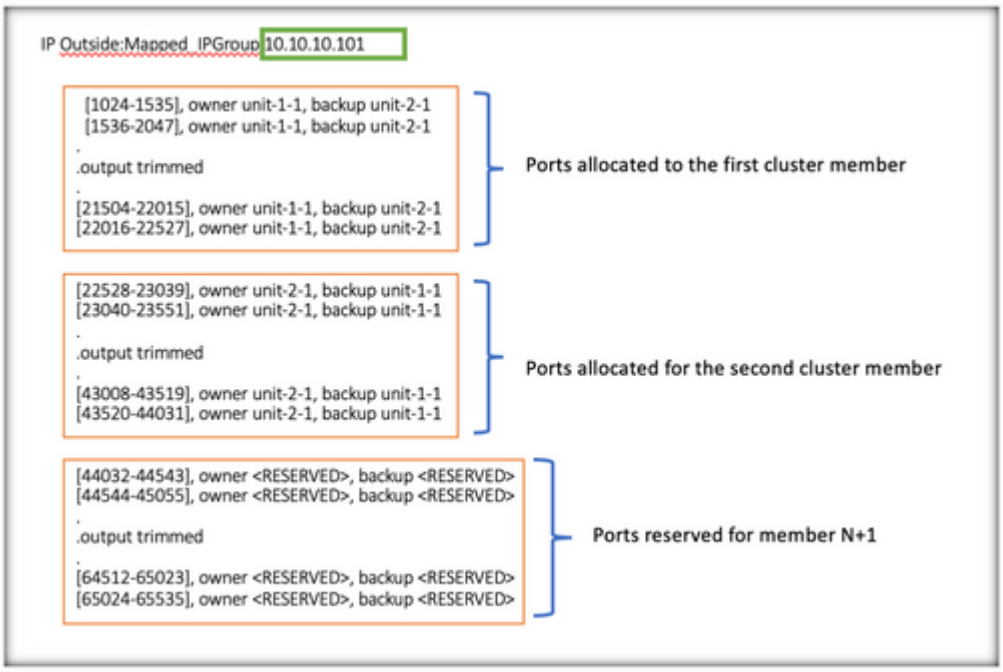
- Op een cluster dat net wordt opgevoed, bezit de Control unit aanvankelijk 50 procent van de havens en de rest is gereserveerd.
- Het aantal havenblokken per eenheid wordt aangepast aangezien meer knooppunten zich bij het cluster aansluiten.
- Control unit reserveert poortblokken voor (N+1) knooppunten totdat het cluster vol is**.** De limiet voor clusterleden wordt bepaald door de cluster-member-limit opdracht, geconfigureerd onder het configuratieniveau van de clustergroep.
- Standaard is de clusterlid-limiet 16.
  <#root>

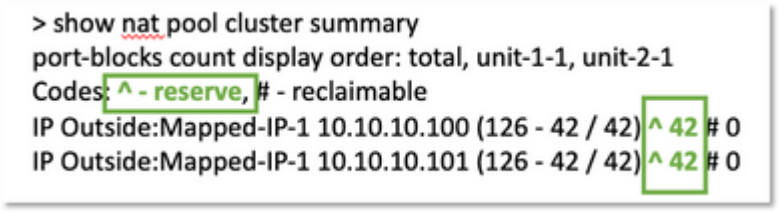
```
> show cluster info

Cluster FTD-Cluster: On
Interface mode: spanned

Cluster Member Limit : 16


[...]
```

- Wanneer de hoeveelheid clusterleden de met **cluster-member-limit**Alle poortblokken zijn verdeeld over de clusterleden.

In een clustergroep van twee eenheden (N=2) met een standaardwaarde van de clusterlidlimiet van 16, wordt bijvoorbeeld opgemerkt dat de poorttoewijzing is gedefinieerd voor N+1-leden, in dit geval 3. Hierdoor blijven enkele poorten gereserveerd voor de volgende eenheid totdat de maximale clusterlimiet is bereikt.

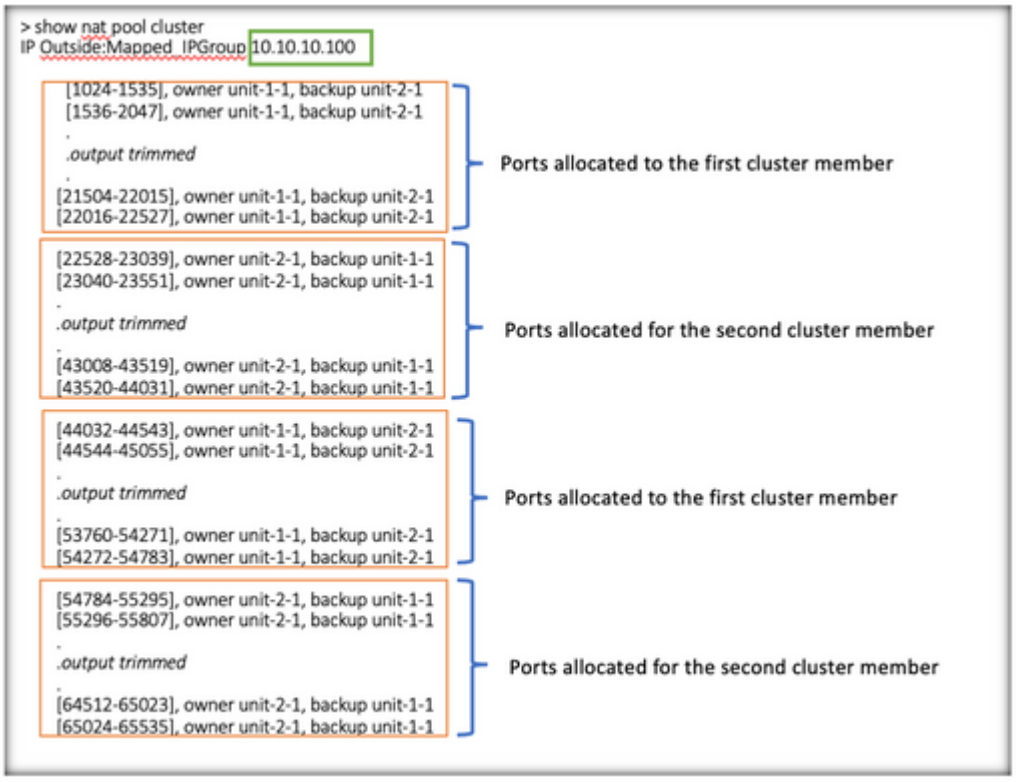


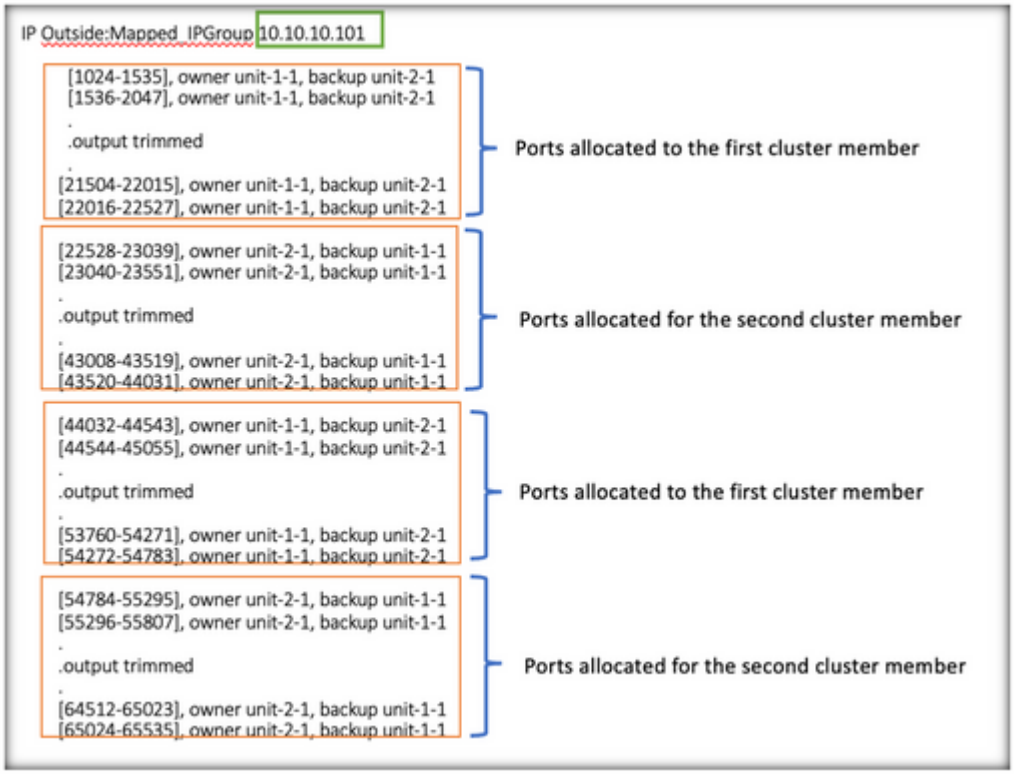




Bovendien is het de beste praktijk om de **cluster-member-limit** het aantal eenheden dat voor de clusterinzet is gepland.

In een clustergroep van twee eenheden (N=2) met een waarde van de clusterlidlimiet van 2, wordt bijvoorbeeld opgemerkt dat de poorttoewijzing gelijkmatig over alle clustereenheden is verdeeld. Geen van de gereserveerde poorten blijft over.






```
> 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
```

Controleer of poortblokkering is hersteld

- Wanneer een nieuw knooppunt zich aansluit bij of een cluster verlaat, moeten ongebruikte poorten en overtollige poortblokken van alle eenheden worden vrijgegeven aan de controle-eenheid.
- Als de havenblokken reeds worden gebruikt, worden de minst gebruikte gemarkeerd voor regeneratie.
- Nieuwe aansluitingen zijn niet toegestaan op geregenereerde havenblokken. Zij worden aan de controle-eenheid vrijgegeven wanneer de laatste haven wordt ontruimd.

```
> 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
```

Opdrachten voor troubleshooting

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

- Controleer of de clusterlid-limiet ingesteld is:

<#root>

> show cluster info

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

Cluster Member Limit : 2

```
[...]
```

> show running-config cluster

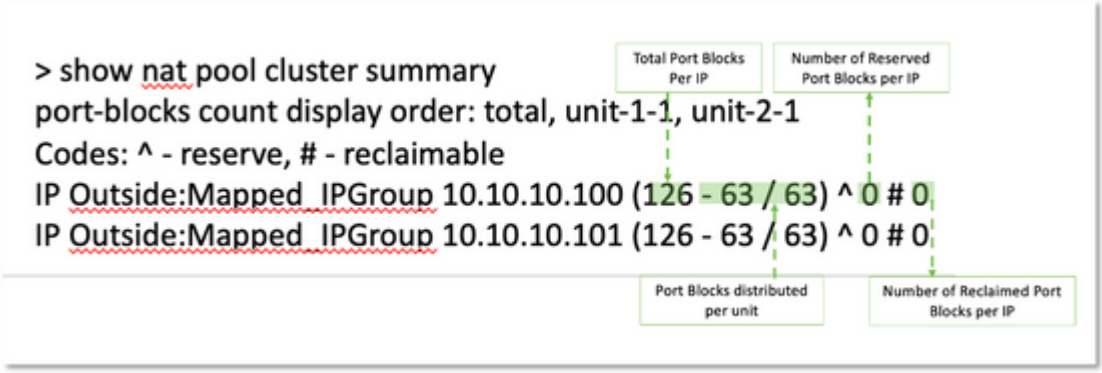
```
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0
```

cluster-member-limit 2
[...]

- Geef een samenvatting van de verdeling van de poortblokken tussen de eenheden in het cluster weer:

<#root>

> show nat pool cluster summary



- Geef de huidige toewijzing van poortblokken per PAT-adres aan de eigenaar en back-upeenheid weer:

<#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
[...]
```

- Informatie over de verspreiding en het gebruik van havenblokken weergeven:

<#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
[...]
```

Gerelateerde informatie

- [Cisco technische ondersteuning en downloads]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.