Informationen zur Portzuweisung auf dynamischer PAT für FTD-Cluster 7.0

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die auf Port-Blöcken basierende Verteilung in Dynamic PAT für Firewall-Cluster nach Version 7.0 und höher funktioniert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Network Address Translation (NAT) auf der Cisco Secure Firewall

Verwendete Komponenten

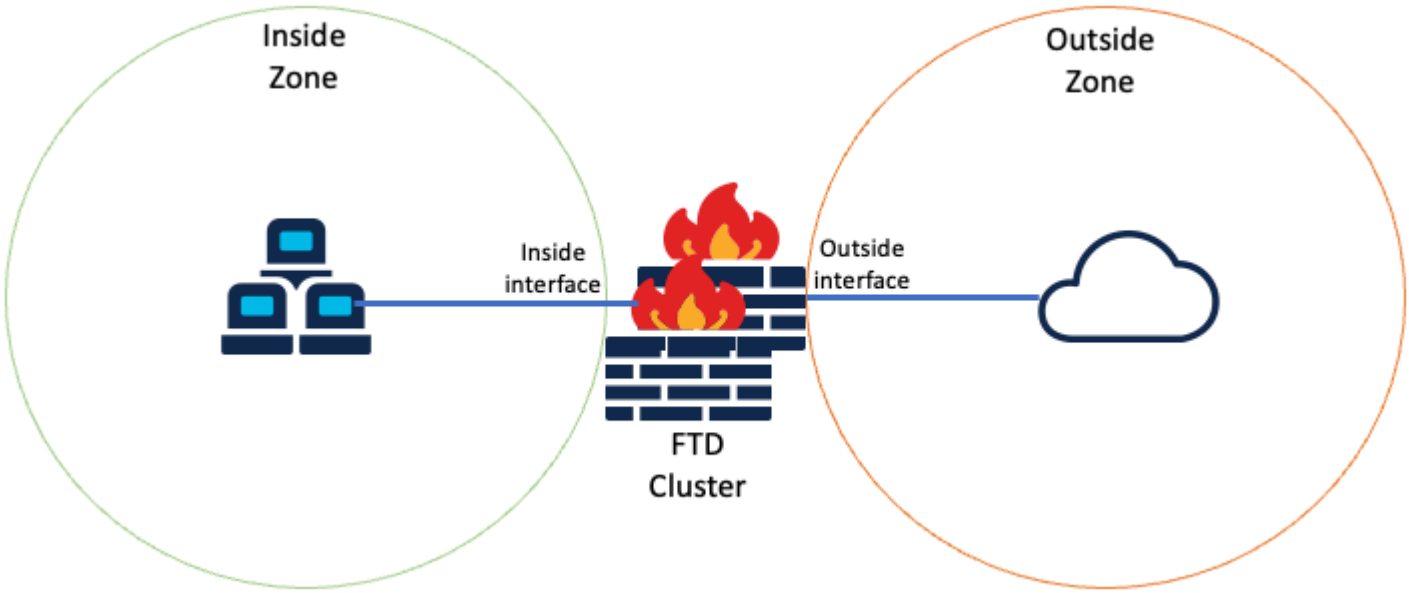
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FirePOWER Management Center 7.3.0
- Firepower Threat Defense 7.2.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm

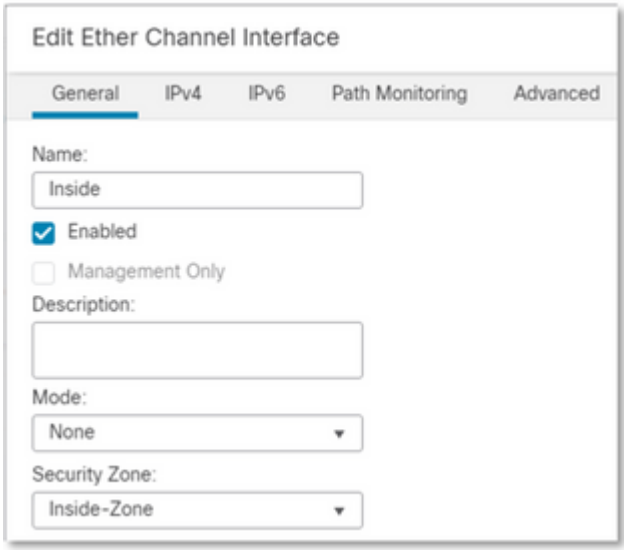


Logische Topologie

Schnittstellenkonfiguration

- Konfigurieren Sie den internen Schnittstellenmember der internen Zone.

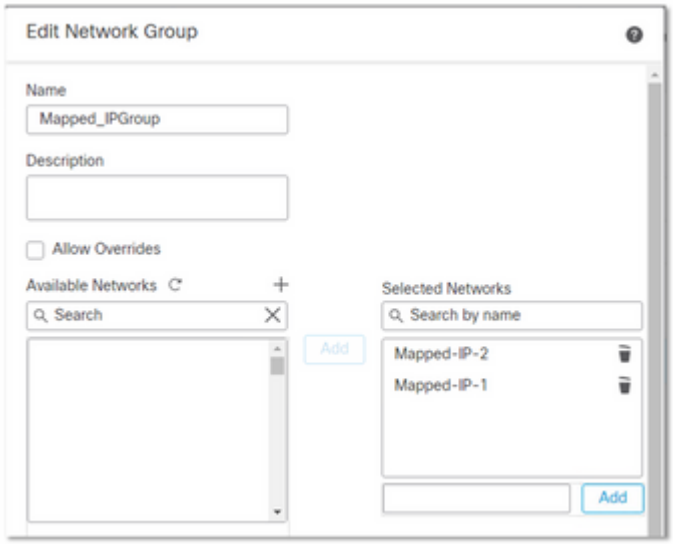
Konfigurieren Sie beispielsweise eine Schnittstelle mit der IP-Adresse 192.168.10.254, und nennen Sie sie **Inside**. Diese interne Schnittstelle ist das Gateway für das interne Netzwerk 192.168.10.0/24.

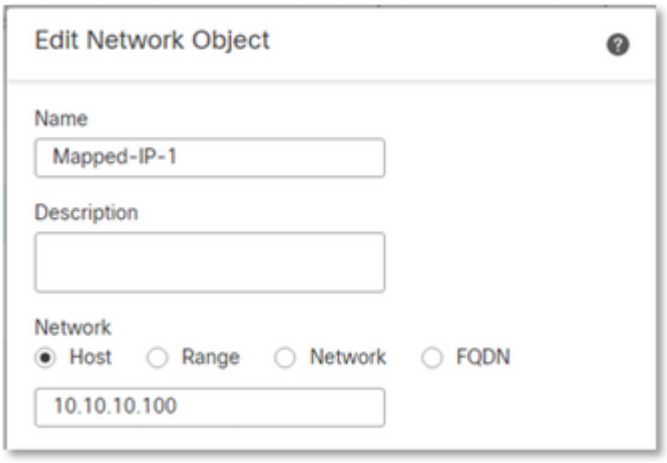


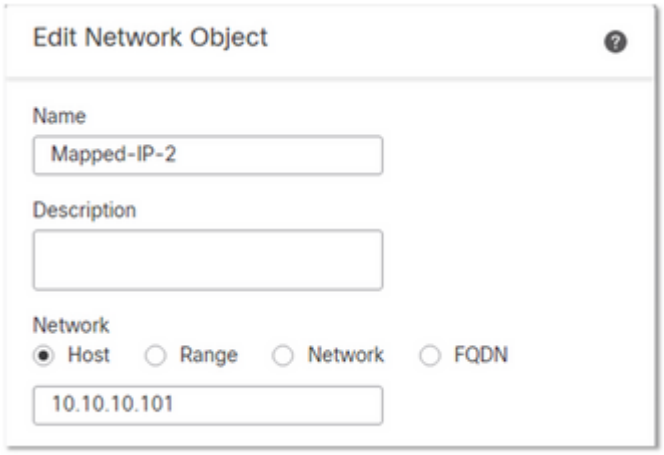
- Konfigurieren Sie den externen Schnittstellenmember der externen Zone.

Konfigurieren Sie beispielsweise eine Schnittstelle mit der IP-Adresse 10.10.10.254, und nennen Sie sie Out

(bestehend aus Mapped-IP-1, 10.10.10.100 und Mapped-IP-2, 10.10.10.101) dient der Zuordnung des gesamten internen Datenverkehrs zur Außenzone.



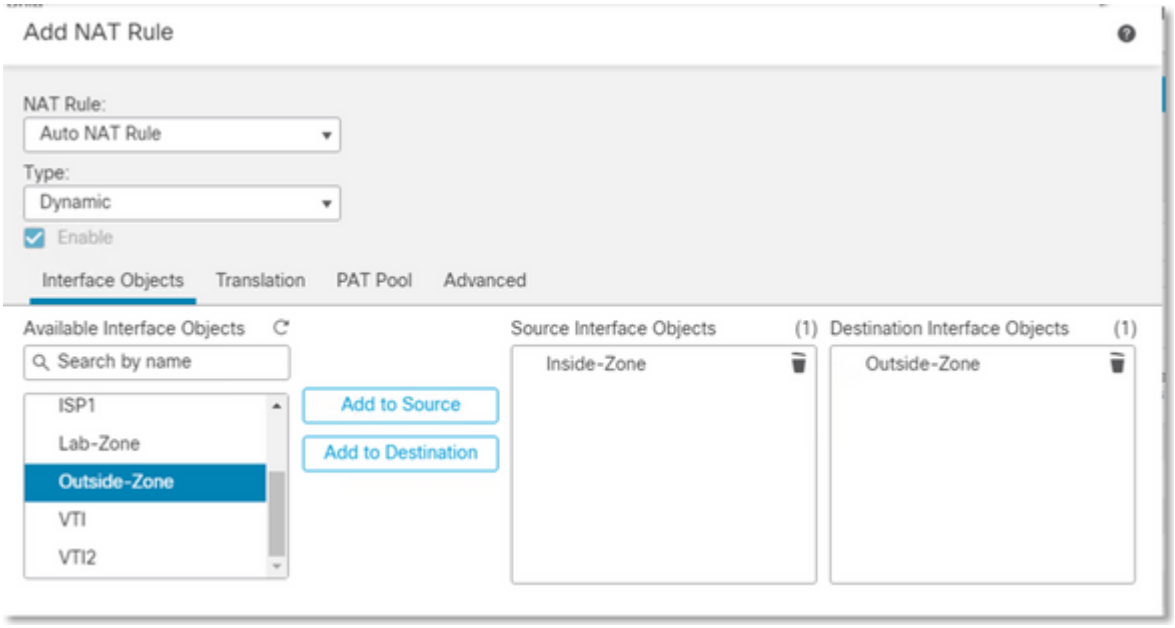


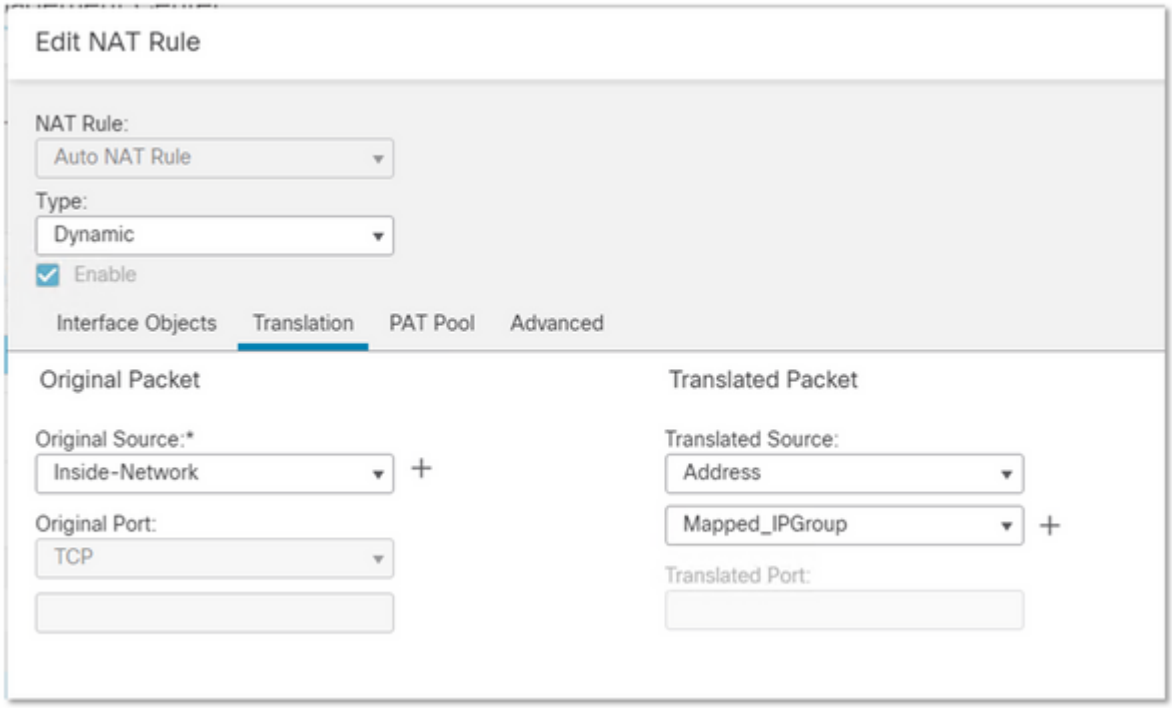


Dynamische PAT-Konfiguration

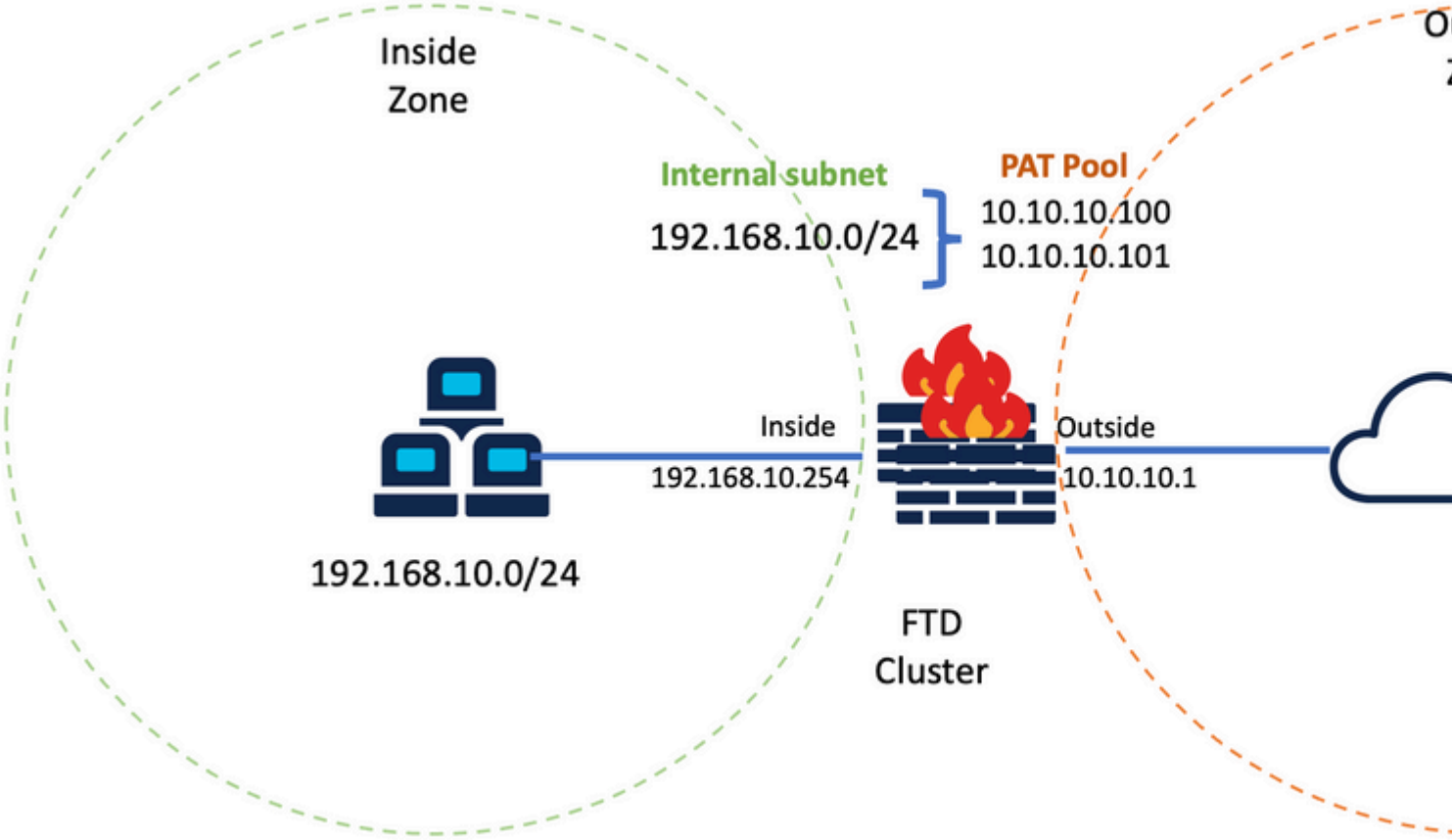
- Konfigurieren Sie eine dynamische NAT-Regel für ausgehenden Datenverkehr. Diese NAT-Regel ordnet das Subnetz des internen Netzwerks dem externen NAT-Pool zu.

Beispielsweise wird der Inside-Zone-zu-Outside-Zone-Datenverkehr vom Inside-Network in den Mapped-IPGroup-Pool umgewandelt.





Abschließende Konfiguration



Abschließende Einrichtung

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfung der IP-Schnittstelle und der NAT-Konfiguration

<#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
```

Portblockzuweisung überprüfen

Nach FirePOWER 7.0

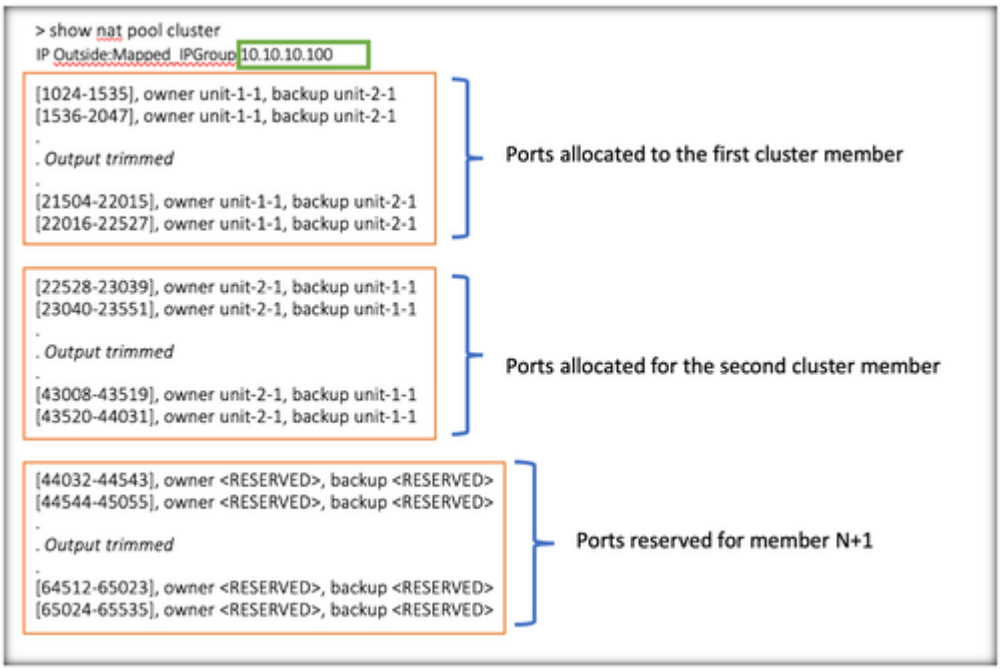
stellt die verbesserte PAT-Portblockzuweisung sicher, dass die Steuereinheit Ports für das Zusammenführen von Knoten reserviert hält und nicht genutzte Ports proaktiv zurückfordert. So funktioniert die Portzuweisung:

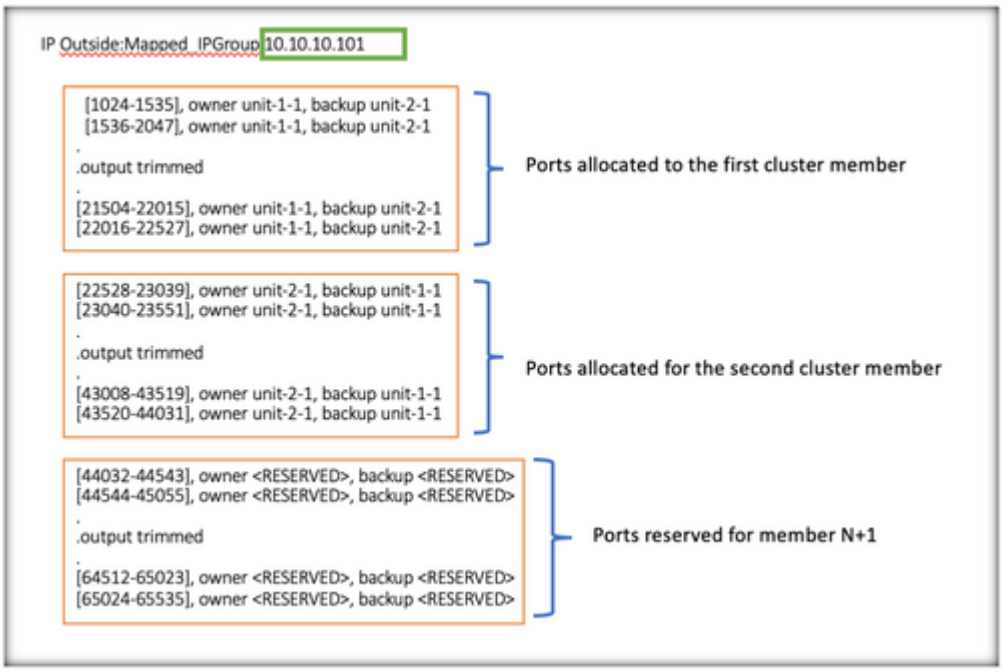
- Auf einem Cluster, der gerade hochgefahren wird, besitzt die Steuereinheit zunächst 50 % der Ports und der Rest ist reserviert.
- Die Anzahl der Port-Blöcke pro Einheit wird angepasst, wenn weitere Knoten zum Cluster hinzugefügt werden.
- Die Steuereinheit reserviert Port-Blöcke für (N+1)-Knoten, bis der Cluster voll ist**.** Der Grenzwert für Cluster-Mitglieder wird definiert durch cluster-member-limit -Befehl, der auf der Ebene der Cluster-Gruppenkonfiguration konfiguriert wird.
- Standardmäßig ist "cluster-member-limit" 16.
  <#root>

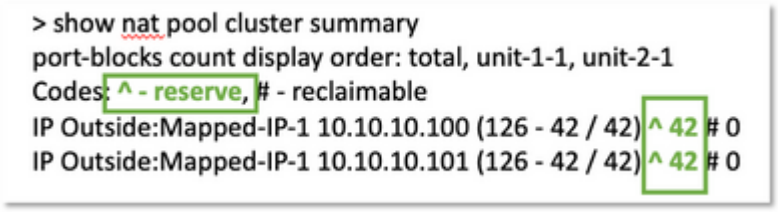
```
> show cluster info

Cluster FTD-Cluster: On
Interface mode: spanned

Cluster Member Limit : 16


[...]
```

- Wenn die Anzahl der Cluster-Mitglieder den Wert erreicht, der mit **cluster-member-limit**sind alle Port-Blöcke auf Cluster-Elemente verteilt.

Beispielsweise wird in einer Clustergruppe aus zwei Einheiten (N=2) mit einem Standardwert von 16 Clustergruppengrenzen beobachtet, dass die Portzuweisung für N+1 Mitglieder definiert ist, in diesem Fall 3. Dadurch bleiben einige Ports für die nächste Einheit reserviert, bis die maximale Cluster-Grenze erreicht ist.

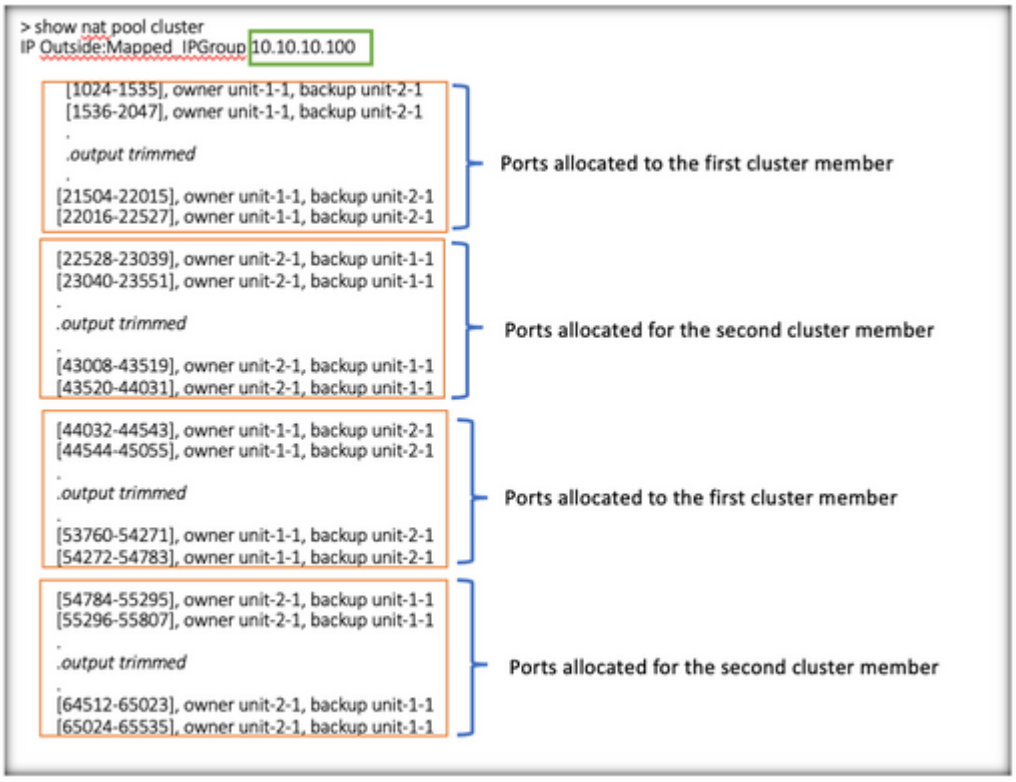


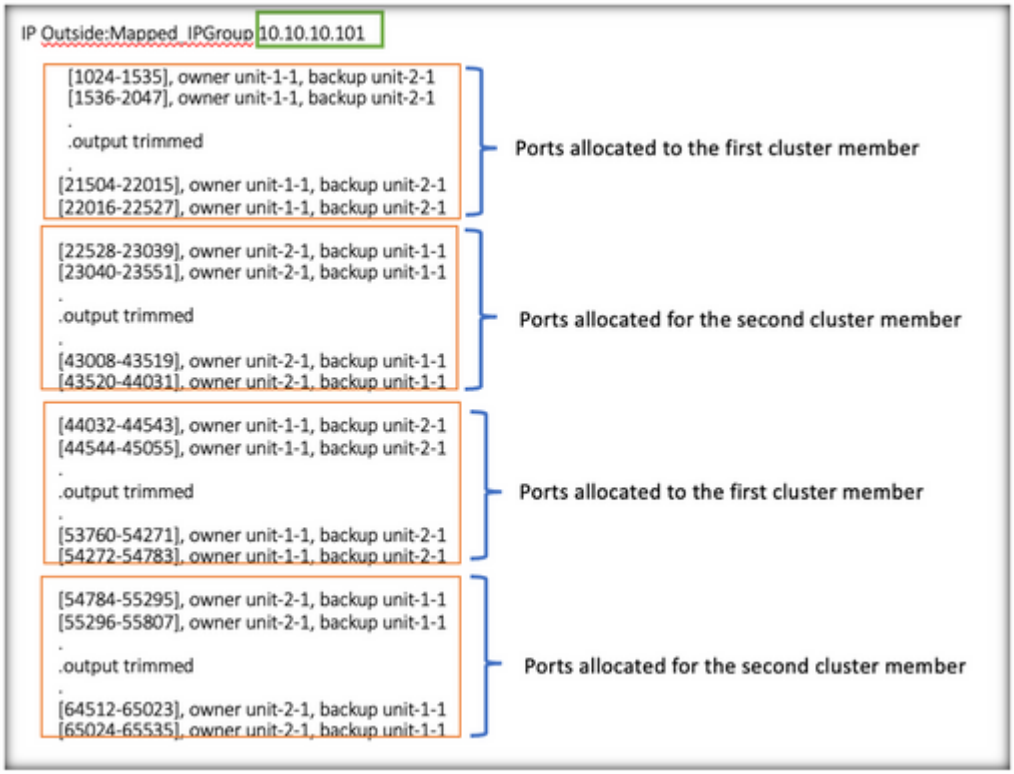




Darüber hinaus empfiehlt es sich, die **cluster-member-limit** , um der Anzahl der für die Cluster-Bereitstellung geplanten Einheiten zu entsprechen.

Beispielsweise wird in einer aus zwei Einheiten (N=2) bestehenden Clustergruppe mit dem Wert der Cluster-Mitgliedergrenze von 2 beobachtet, dass die Portzuweisung gleichmäßig auf alle Cluster-Einheiten verteilt ist. Keiner der reservierten Ports bleibt übrig.






```
> 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
```

Überprüfung der Port-Blockreklamation

- Immer wenn ein neuer Knoten zu einem Cluster hinzukommt oder diesen verlässt, müssen ungenutzte Ports und überschüssige Portblöcke aller Einheiten an die Steuereinheit freigegeben werden.
- Wenn die Port-Blöcke bereits verwendet werden, werden die am wenigsten genutzten für die Rückgewinnung markiert.
- Neue Verbindungen sind auf freigegebenen Port-Blöcken nicht zulässig. Sie werden bei Freigabe des letzten Ports an die Regelung abgegeben.

```
> 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
```

Befehle für die Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

- Überprüfen Sie den konfigurierten Grenzwert für Cluster-Mitglieder:

<#root>

> show cluster info

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

Cluster Member Limit : 2

```
[...]
```

> show running-config cluster

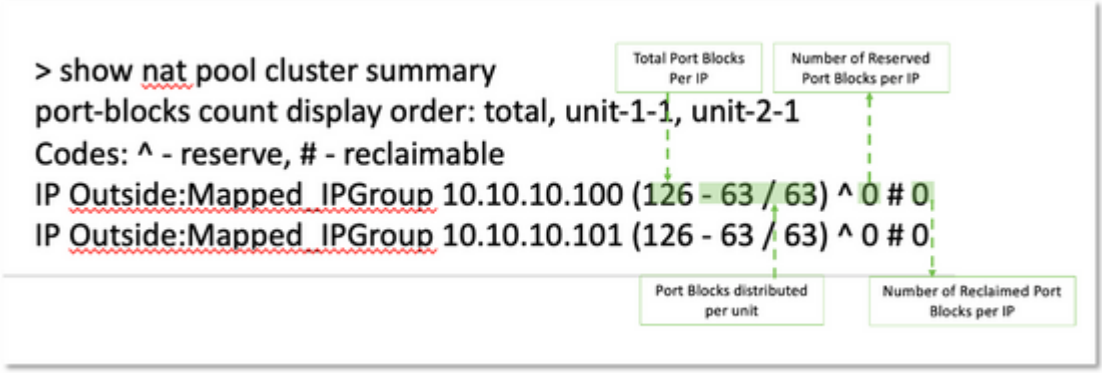
```
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0
```

cluster-member-limit 2
[...]

- Zeigt eine Zusammenfassung der Port-Blöcke an, die auf die Einheiten im Cluster verteilt sind:

<#root>

> show nat pool cluster summary



- Zeigt die aktuelle Zuweisung der Port-Blöcke pro PAT-Adresse zum Eigentümer und zur Sicherungseinheit an:

<#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
[...]
```

- Informationen zur Verteilung und Nutzung von Port-Blöcken anzeigen:

<#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
[...]
```

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.