Informazioni sull'allocazione delle porte in Dynamic PAT per il cluster FTD 7.0

Sommario

Introduzione

In questo documento viene descritto come funziona la distribuzione basata su blocchi di porte in Dynamic PAT for Firewall Cluster dopo la versione 7.0 e successive.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Network Address Translation (NAT) su Cisco Secure Firewall

Componenti usati

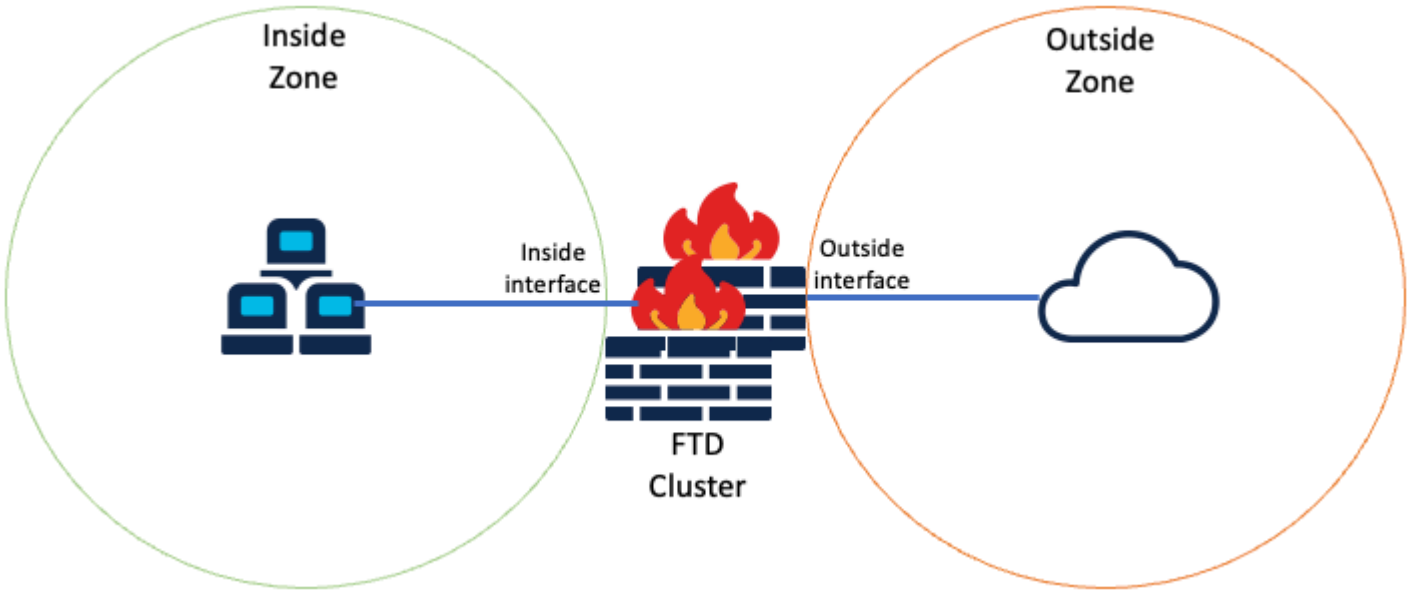
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower Management Center 7.3.0
- Firepower Threat Defense 7.2.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

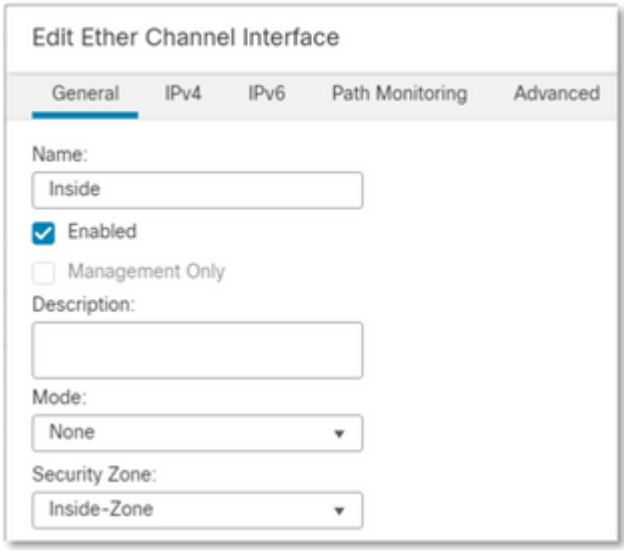


Topologia logica

Configurazione interfaccia

- Configurare il membro di interfaccia Inside della zona interna.

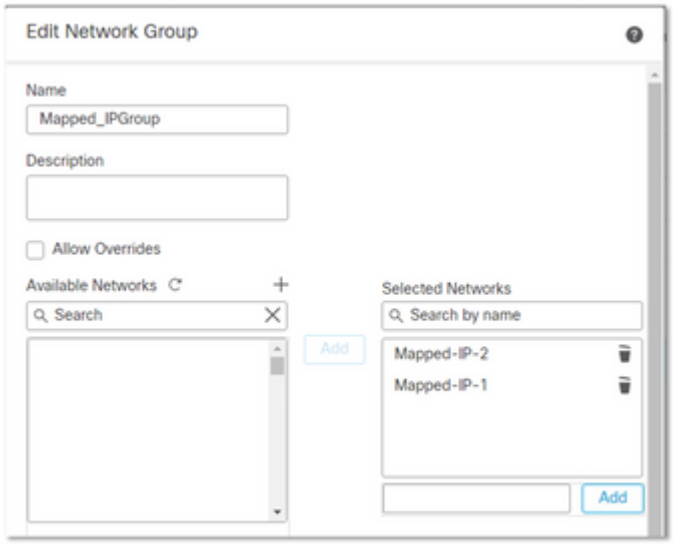
Ad esempio, configurare un'interfaccia con indirizzo IP 192.168.10.254 e denominarla **Inside**. Questa interfaccia interna è il gateway per la rete interna 192.168.10.0/24.

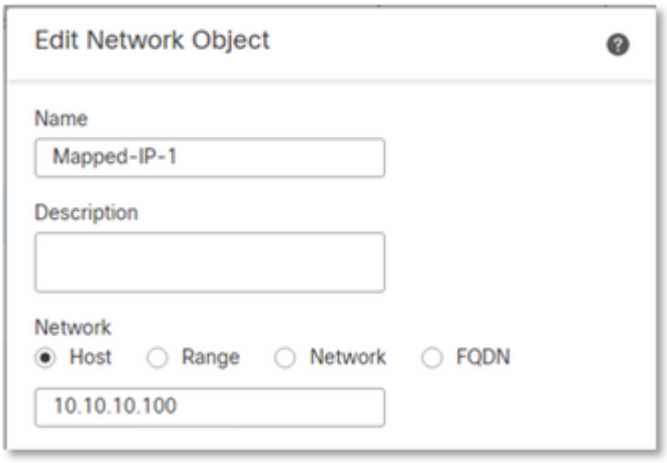


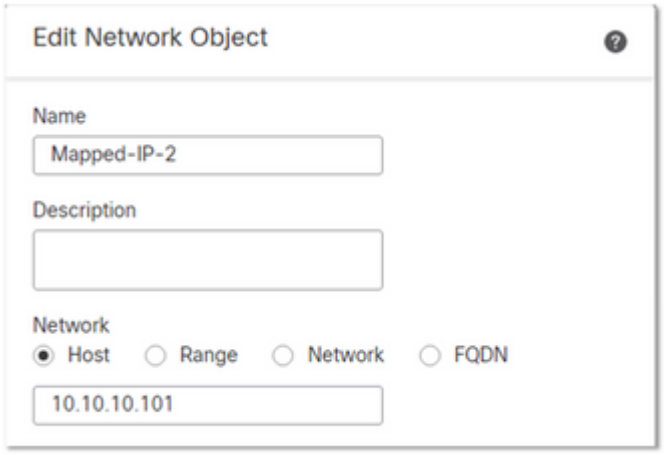
- Configurare il membro dell'interfaccia esterna di Zona esterna.

Ad esempio, configurare un'interfaccia con indirizzo IP 10.10.10.254 e denominarla Esterna. L'interfaccia es

(costituito da Mapped-IP-1 10.10.10.100 e Mapped-IP-2 10.10.10.101), è utilizzato per mappare tutto il traffico interno alla zona esterna.



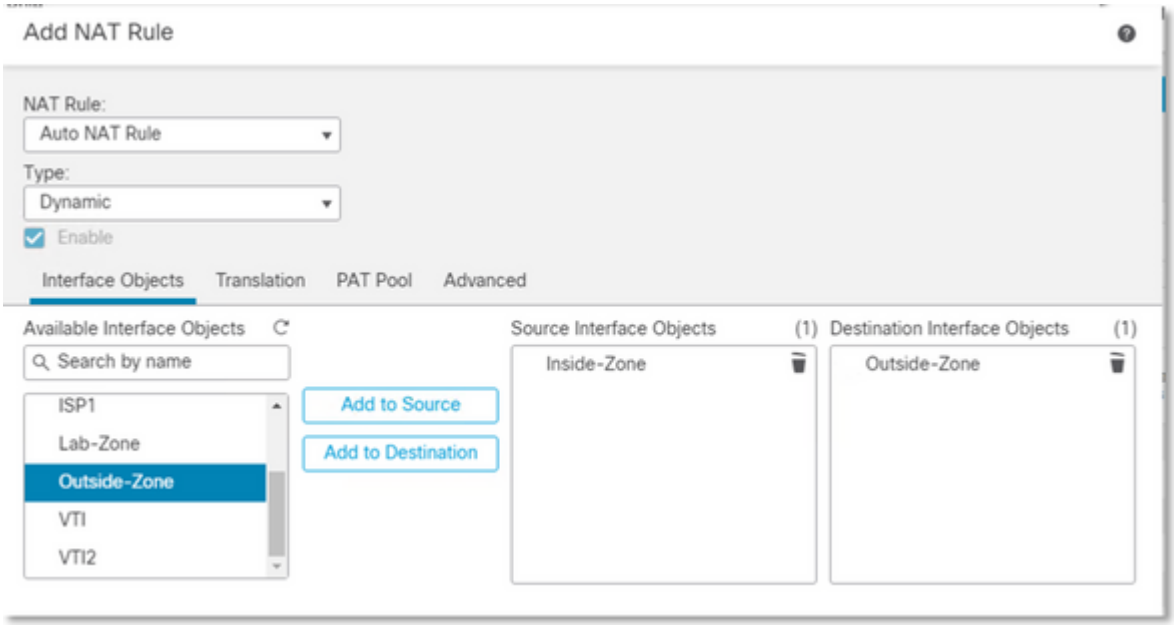


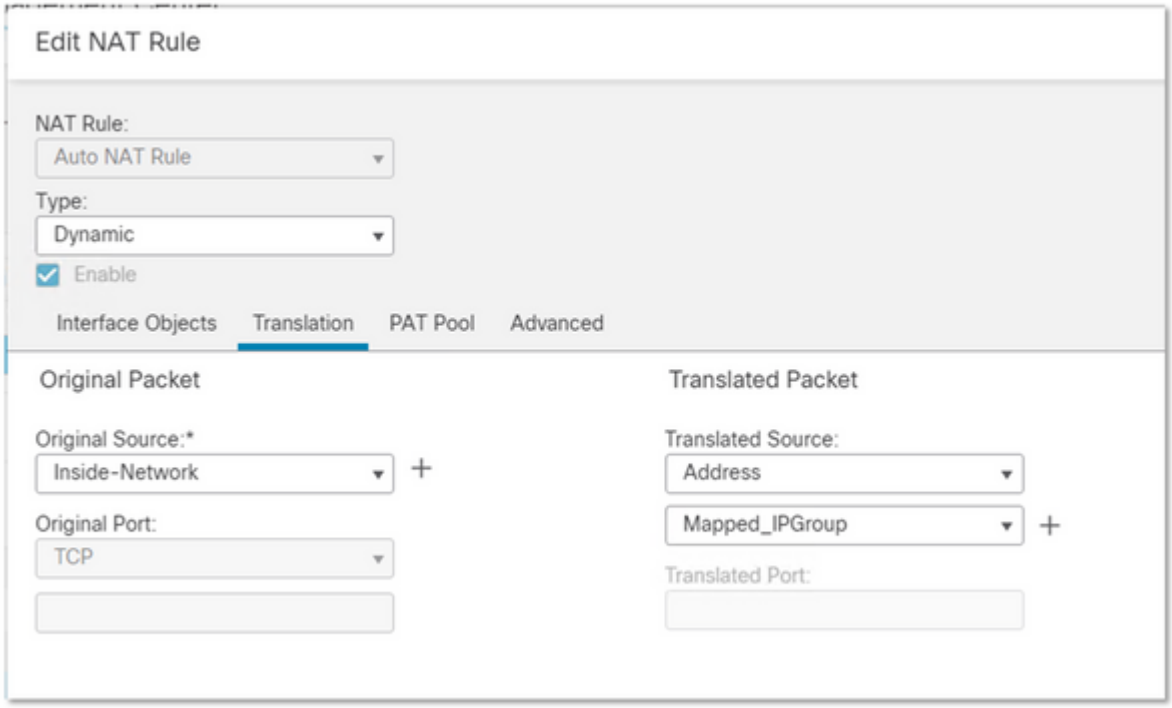


Configurazione PAT dinamico

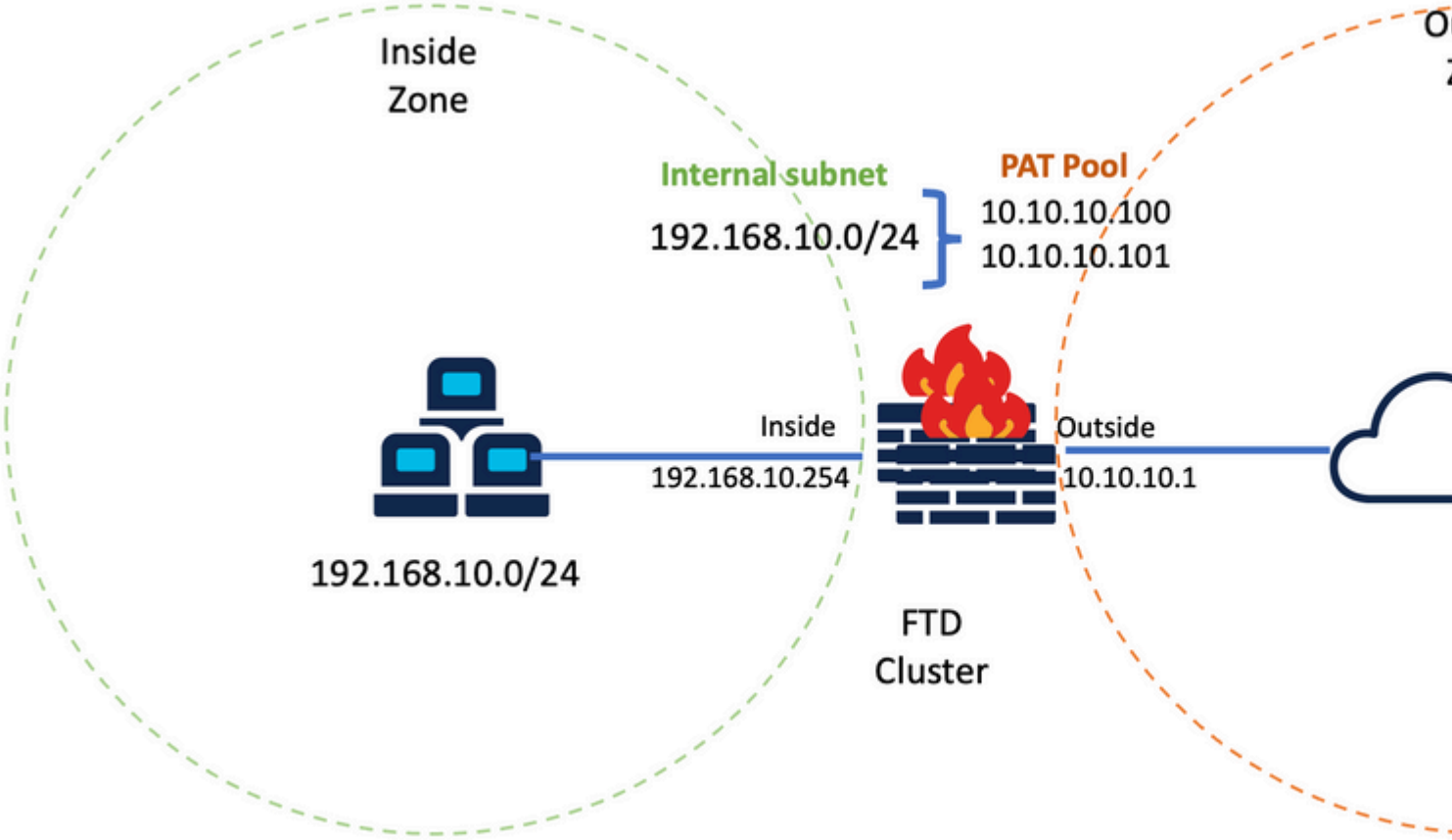
- Configurare una regola NAT dinamica per il traffico in uscita. Questa regola NAT mappa la subnet della rete interna al pool NAT esterno.

Ad esempio, il traffico da zona interna a zona esterna dalla rete interna viene convertito in pool Mapped-IPGroup.





Configurazione finale



Configurazione finale di Lab.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verifica dell'interfaccia IP e della configurazione 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
```

Verifica allocazione blocchi porte

Dopo Firepower 7.0

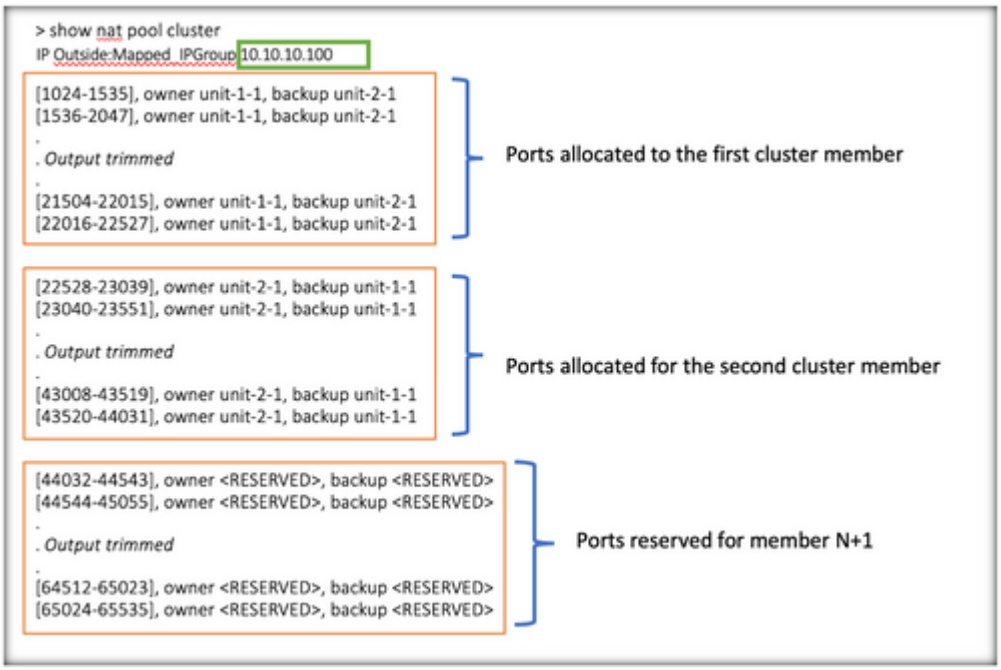
la migliorata allocazione dei blocchi di porte PAT garantisce che l'unità di controllo mantenga le porte in riserva per unire i nodi e recuperi proattivamente le porte inutilizzate. L'allocazione della porta funziona in questo modo:

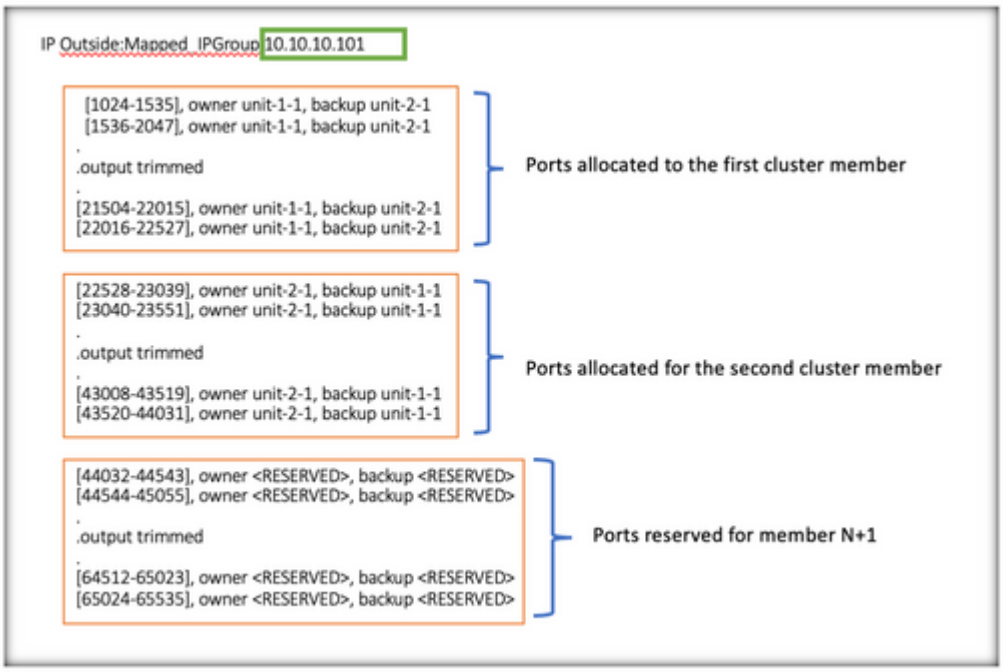
- In un cluster appena avviato, l'unità di controllo inizialmente possiede il 50% delle porte e le altre sono riservate.
- Il numero di blocchi di porte di proprietà per unità viene modificato quando più nodi si uniscono al cluster.
- L'unità di controllo riserva i blocchi di porte per i nodi (N+1) finché il cluster non è pieno**.** Il limite di membri del cluster è definito dal cluster-member-limit , configurato nel livello di configurazione del gruppo di cluster.
- Per impostazione predefinita, il limite di membri del cluster è 16.
  <#root>

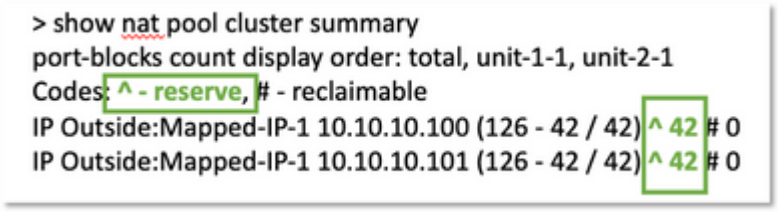
```
> show cluster info

Cluster FTD-Cluster: On
Interface mode: spanned

Cluster Member Limit : 16


[...]
```

- Quando la quantità di membri del cluster raggiunge il valore configurato con **cluster-member-limit,** tutti i blocchi di porte vengono distribuiti tra i membri del cluster.

Ad esempio, in un gruppo di cluster composto da due unità (N=2) con un valore predefinito di limite di membri del cluster pari a 16, si osserva che l'allocazione delle porte è definita per i membri N+1, in questo caso 3. In questo modo alcune porte rimangono riservate per l'unità successiva fino al raggiungimento del limite massimo di cluster.

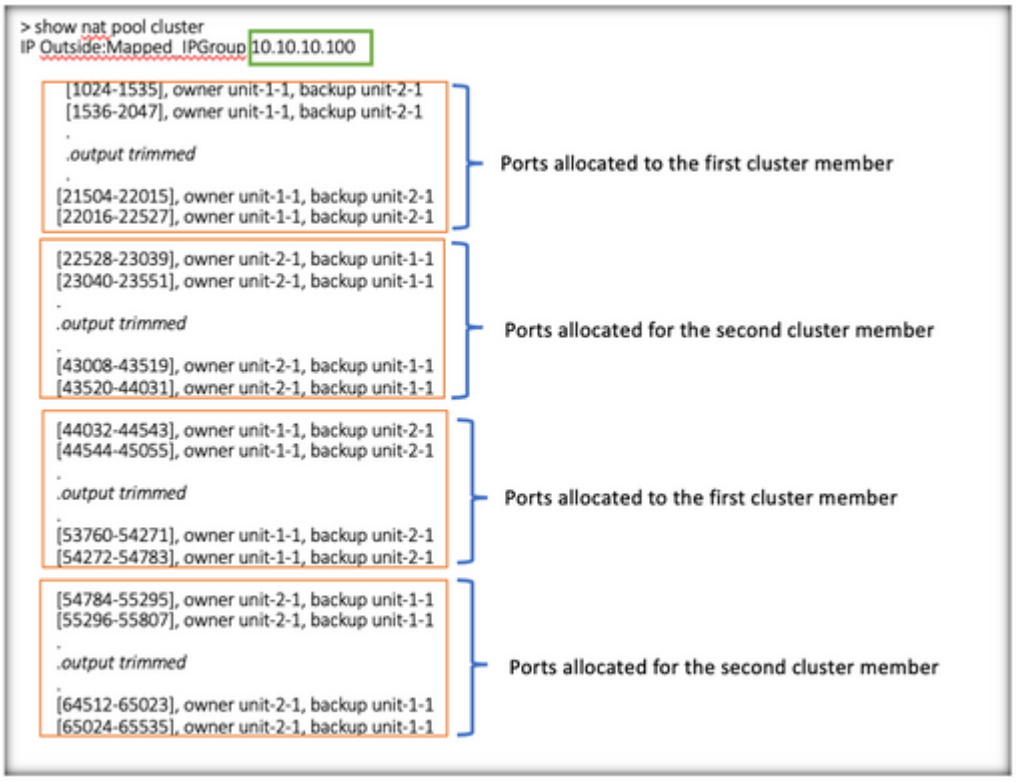


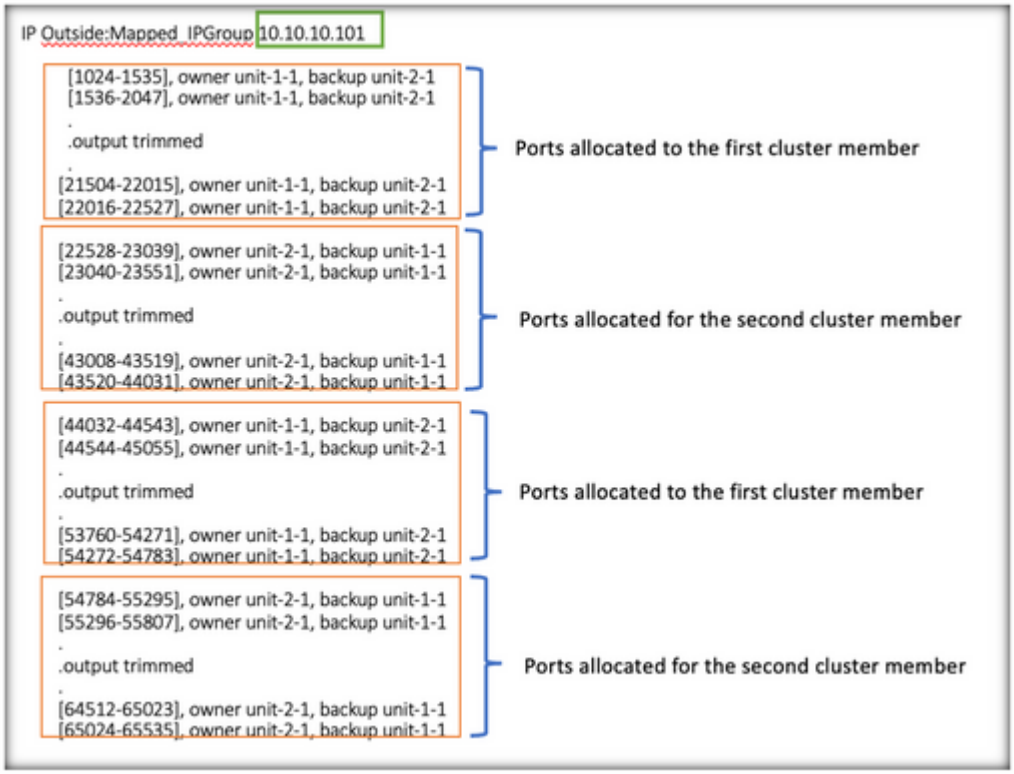




Inoltre, è buona norma configurare il **cluster-member-limit** per far corrispondere il numero di unità pianificate per la distribuzione cluster.

Ad esempio, in un gruppo di cluster composto da due unità (N=2) con il valore del limite di membri del cluster pari a 2, l'allocazione delle porte viene distribuita in modo uniforme tra tutte le unità del cluster. Nessuna delle porte riservate è rimasta.

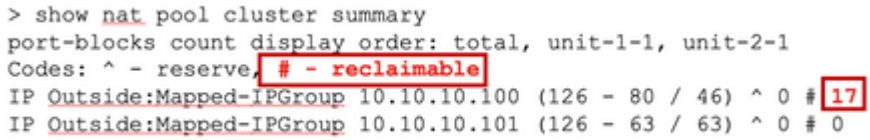





```
> show nat pool cluster summary
port-blocks count display order: total, unit-1-1, unit-2-1
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IP-1 10.10.10.100 (126 - 63 / 63) ^ 0 # 0
IP Outside:Mapped-IP-1 10.10.10.100 (126 - 63 / 63) ^ 0 # 0
```

Verifica del recupero dei blocchi delle porte

- Quando un nuovo nodo si unisce o esce da un cluster, le porte inutilizzate e i blocchi di porte in eccesso di tutte le unità devono essere rilasciati all'unità di controllo.
- Se i blocchi della porta sono già in uso, quelli meno utilizzati vengono contrassegnati per il recupero.
- Nuove connessioni non consentite su blocchi di porte recuperati. e vengono rilasciate all'unità di controllo quando l'ultima porta viene azzerata.



Comandi per la risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

- Verificare il valore di limite dei membri del cluster configurato:

<#root>

> show cluster info

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

Cluster Member Limit : 2

```
[...]
```

> show running-config cluster

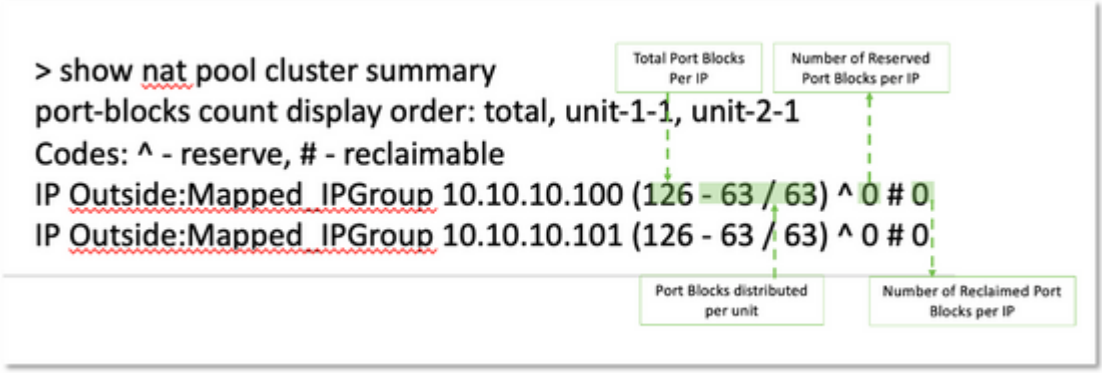
```
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0
```

cluster-member-limit 2
[...]

- Visualizzare un riepilogo della distribuzione dei blocchi di porte tra le unità nel cluster:

<#root>

> show nat pool cluster summary



- Visualizzare l'assegnazione corrente dei blocchi di porte per indirizzo PAT al proprietario e all'unità di backup:

<#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
[...]
```

- Visualizza informazioni correlate alla distribuzione e all'utilizzo dei blocchi di porte:

<#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
[...]
```

Informazioni correlate

- **Supporto tecnico e download Cisco**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).