Comprender la asignación de puertos en PAT dinámica para FTD Cluster 7.0

Contenido

Introducción

Este documento describe cómo funciona la distribución basada en bloques de puertos en PAT Dinámico para el Cluster de Firewall después de la versión 7.0 y posteriores.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Traducción de direcciones de red (NAT) en Cisco Secure Firewall

Componentes Utilizados

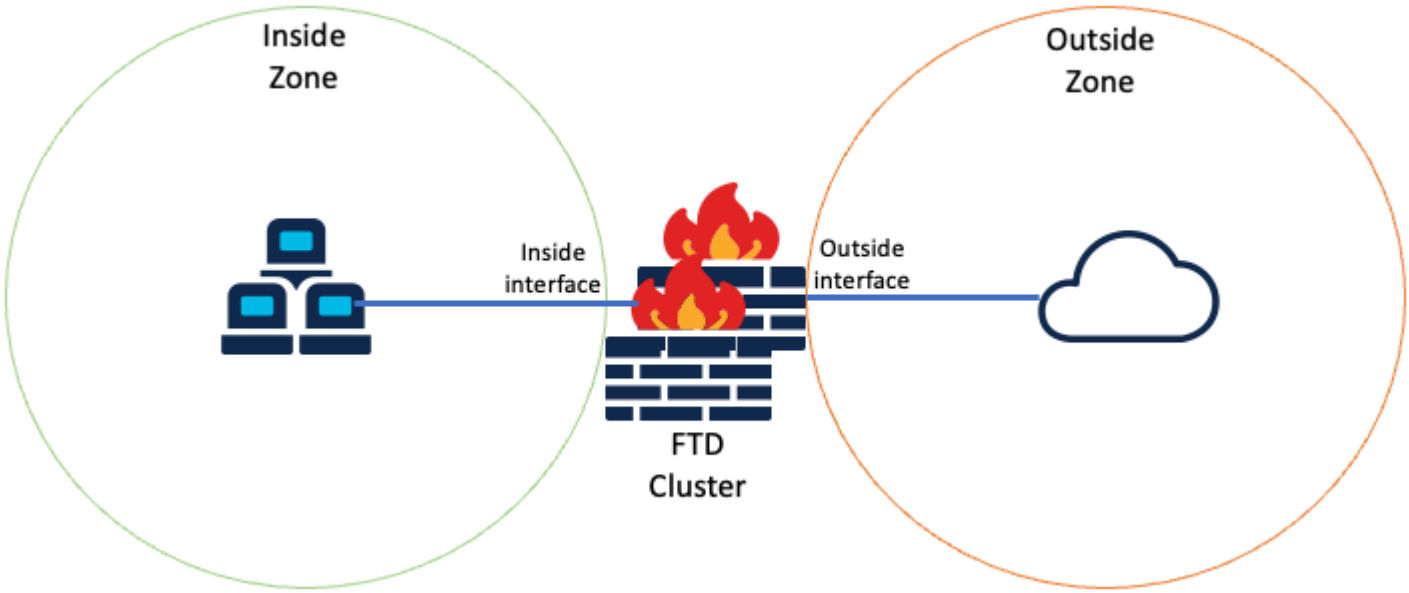
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firepower Management Center 7.3.0
- Firepower Threat Defense 7.2.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

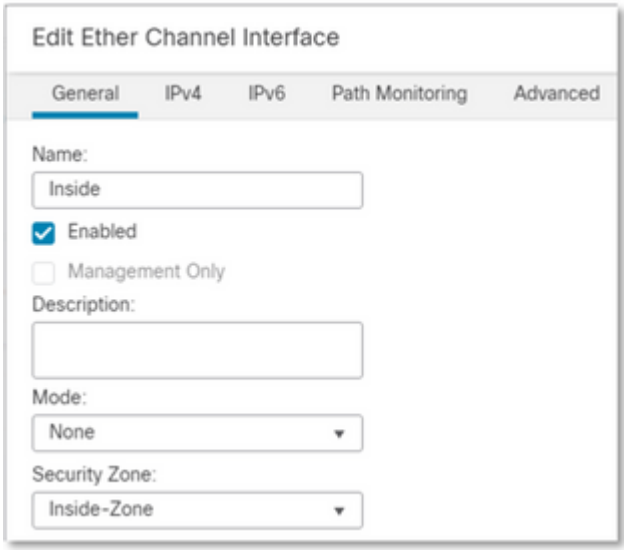


Topología lógica

Configuración de la Interfaz

- Configuración del miembro de interfaz interno de la zona interna.

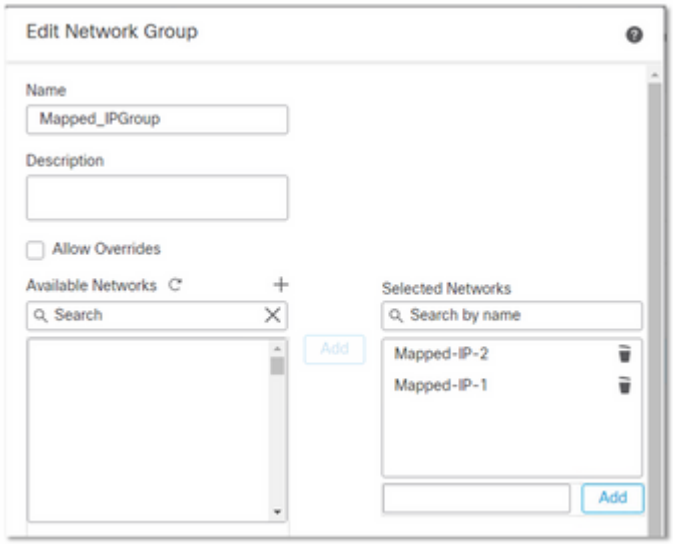
Por ejemplo, configure una interfaz con la dirección IP 192.168.10.254 y denomínela **Inside**. Esta interfaz interna es la puerta de enlace para la red interna 192.168.10.0/24.

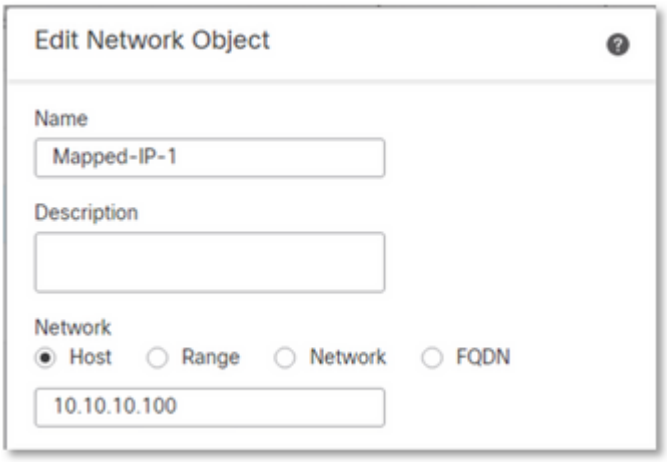


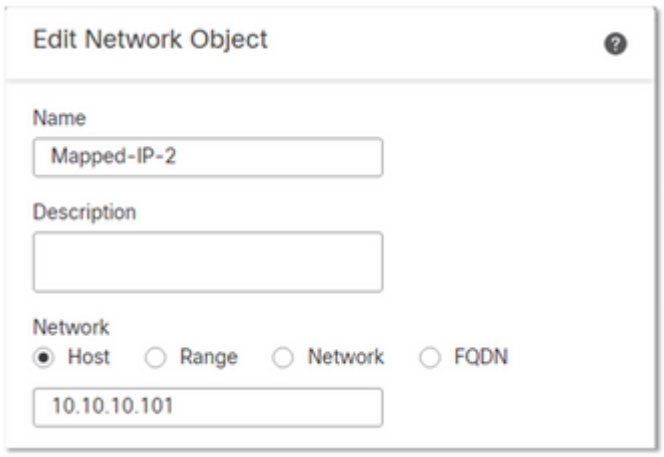
- Configuración del miembro de la interfaz externa de la zona externa.

Por ejemplo, configure una interfaz con la dirección IP 10.10.10.254 y asígnele el nombre Outside (Fuera).

(formado por Mapped-IP-1 10.10.10.100 y Mapped-IP-2 10.10.10.101), se utiliza para asignar todo el tráfico interno a Outside-Zone.



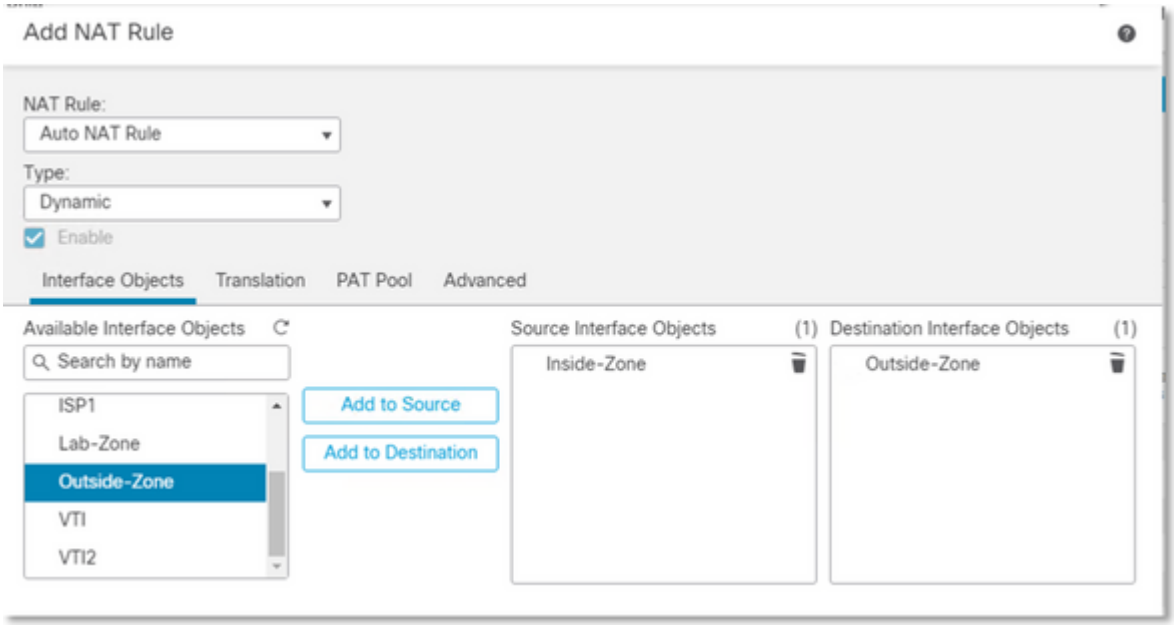


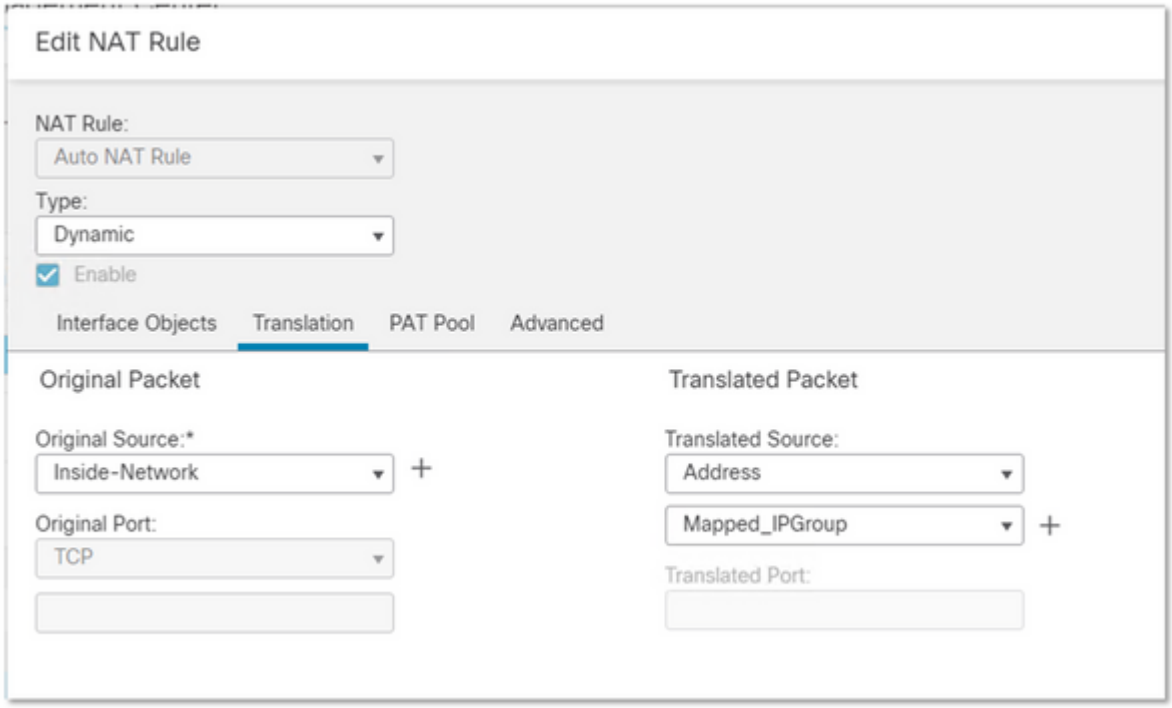


Configuración de PAT dinámica

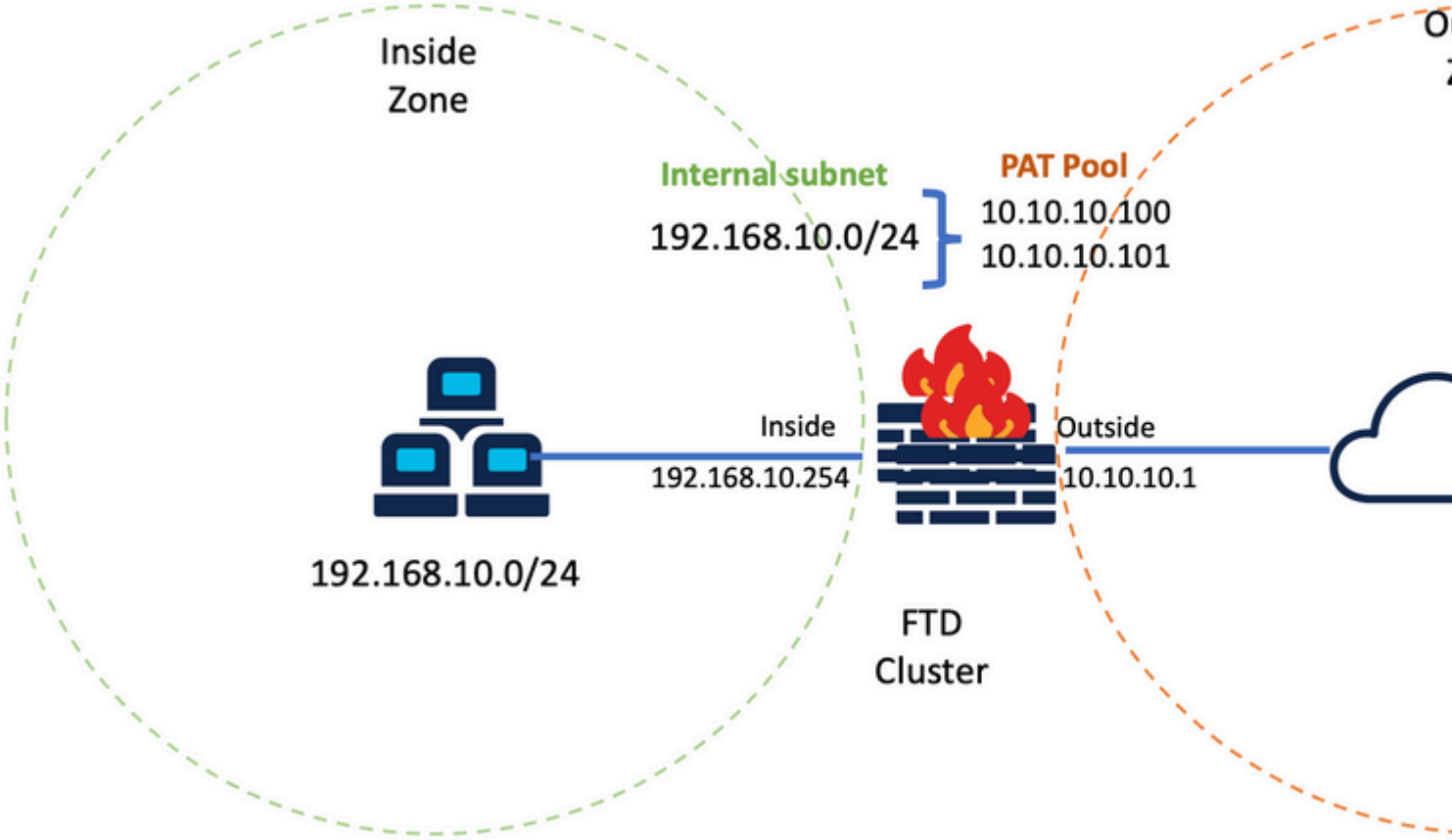
- Configure una regla NAT dinámica para el tráfico saliente. Esta regla NAT asigna la subred de la red interna al conjunto NAT externo.

Por ejemplo, el tráfico de la zona interna a la zona externa de la red interna se traduce al conjunto Mapped-IPGroup.





Configuración final



Configuración final del laboratorio.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verificar la interfaz IP y la configuración 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
```

Verificar asignación de bloque de puertos

Después de Firepower 7.0

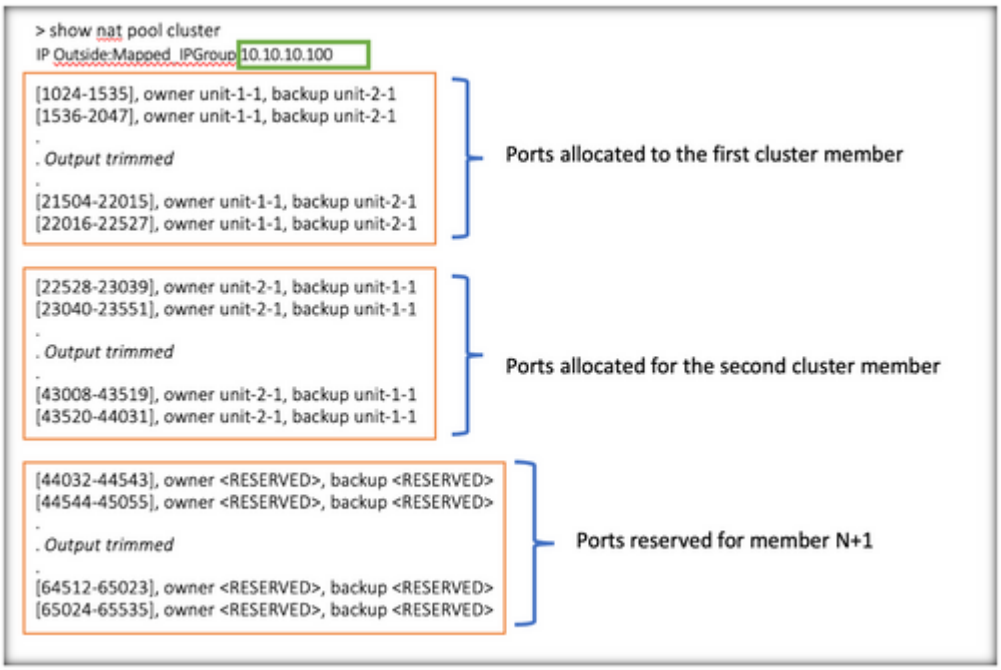
la asignación de bloques de puertos PAT mejorada garantiza que la unidad de control mantenga los puertos en reserva para unirse a los nodos y reclama de forma proactiva los puertos no utilizados. Así es como funciona la asignación de puertos:

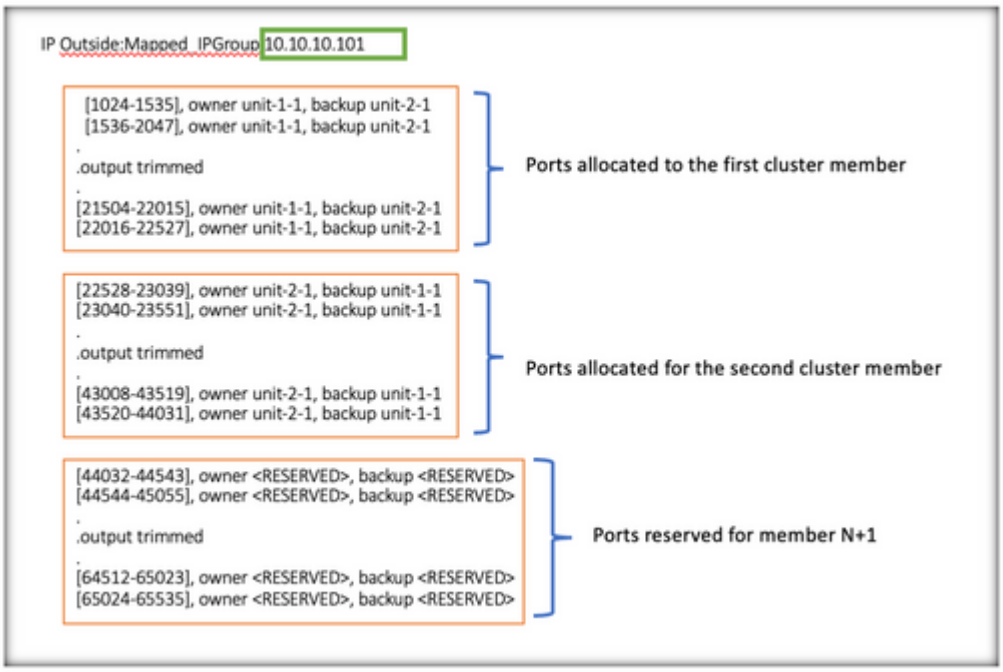
- En un clúster que se acaba de activar, la unidad de control posee inicialmente el 50% de los puertos y el resto está reservado.
- El número de bloques de puertos propiedad de cada unidad se ajusta a medida que más nodos se unen al clúster.
- La unidad de control reserva bloques de puertos para nodos (N+1) hasta que el clúster esté lleno**.** El límite de miembros del clúster lo define el cluster-member-limit , configurado en el nivel de configuración del grupo de clústeres.
- De forma predeterminada, cluster-member-limit es 16.
  <#root>

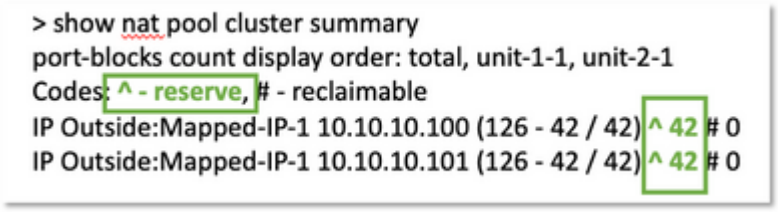
```
> show cluster info

Cluster FTD-Cluster: On
Interface mode: spanned

Cluster Member Limit : 16


[...]
```

- Cuando la cantidad de miembros del clúster alcanza el valor configurado con **cluster-member-limit,** todos los bloques de puerto se distribuyen a través de los miembros del clúster.

Por ejemplo, en un grupo de clústeres formado por dos unidades (N=2) con un valor predeterminado de límite de miembro de clúster de 16, se observa que la asignación de puertos se define para los miembros N+1, en este caso, 3. Esto deja algunos puertos reservados para la siguiente unidad hasta que se alcance el límite máximo de agrupamiento.

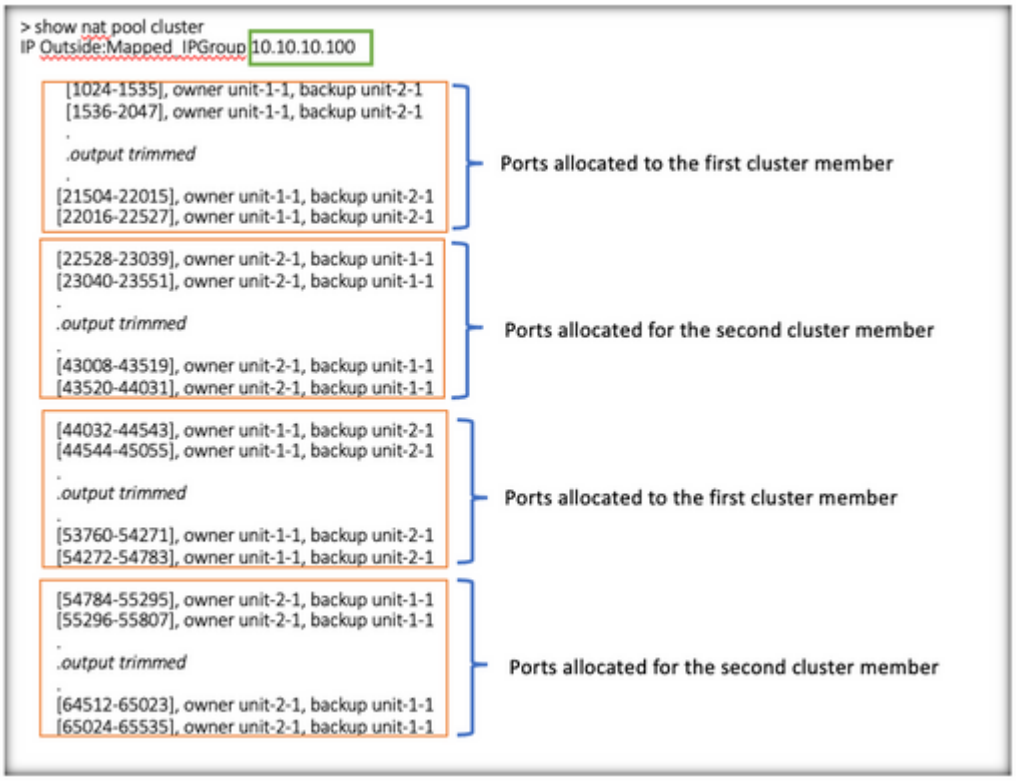


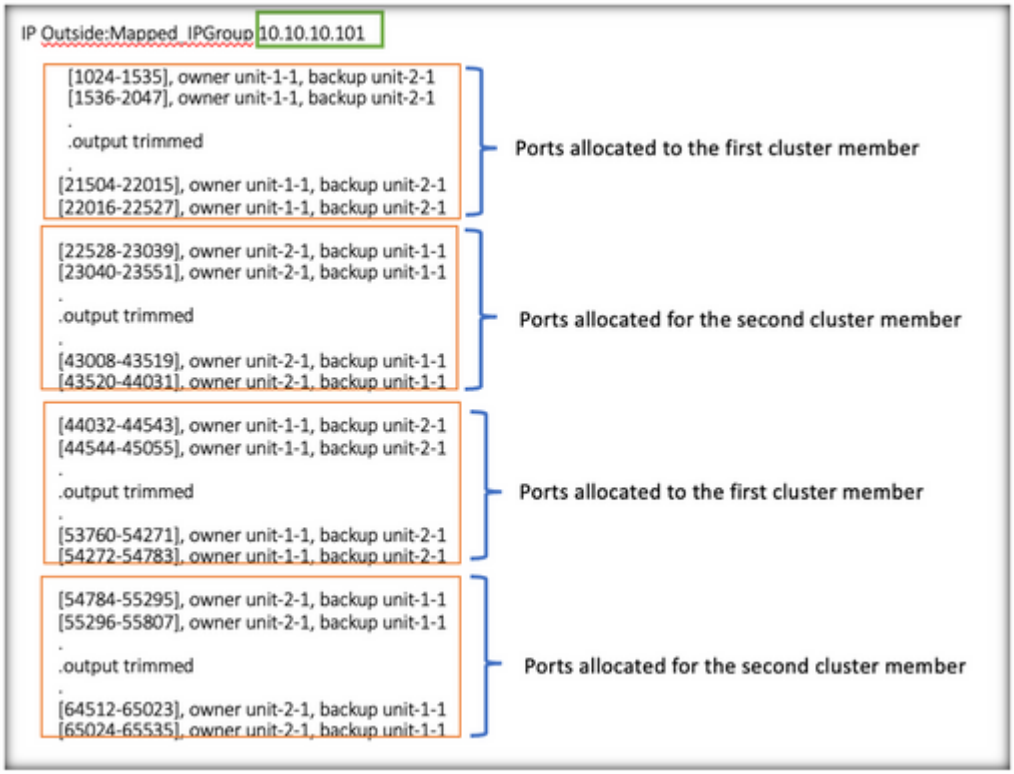




Además, se recomienda configurar la función **cluster-member-limit** para que coincida con el número de unidades planificadas para la implementación del clúster.

Por ejemplo, en un grupo de clúster formado por dos unidades (N=2) con un valor de límite de miembro de clúster de 2, se observa que la asignación de puertos se distribuye uniformemente en todas las unidades de clúster. No queda ninguno de los puertos reservados.






```
> 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
```

Verificar recuperación del bloque de puertos

- Siempre que un nuevo nodo se una o abandona un clúster, los puertos no utilizados y los bloques de puertos en exceso de todas las unidades deben liberarse a la unidad de control.
- Si los bloques de puerto ya están siendo utilizados, los menos utilizados están marcados para reclamación.
- No se permiten nuevas conexiones en los bloques de puertos reclamados. Se liberan en la unidad de control cuando se borra el último puerto.

```
> 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
```

Comandos para resolución de problemas

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Verifique el valor de cluster-member-limit configurado:

<#root>

> show cluster info

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

Cluster Member Limit : 2

```
[...]
```

> show running-config cluster

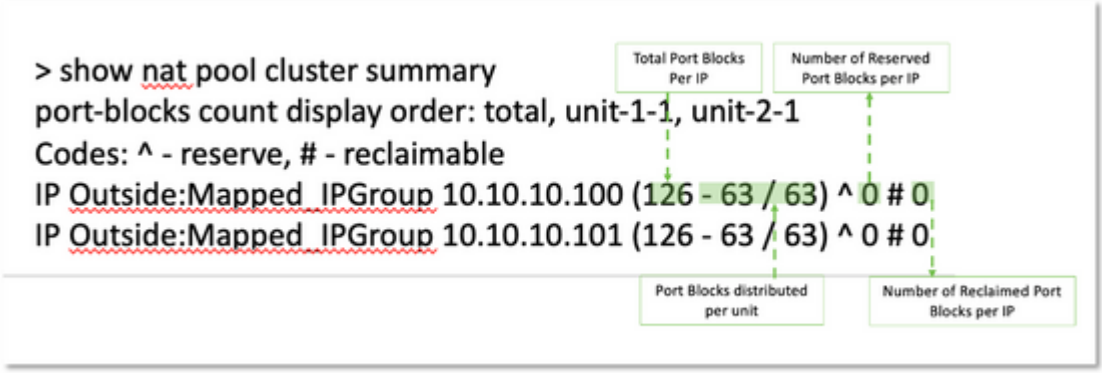
```
cluster group FTD-Cluster
key *****
local-unit unit-2-1
cluster-interface Port-channel48 ip 172.16.2.1 255.255.0.0
```

cluster-member-limit 2
[...]

- Muestra un resumen de la distribución de bloques de puertos entre las unidades del clúster:

<#root>

> show nat pool cluster summary



- Muestra la asignación actual de bloques de puertos por dirección PAT al propietario y a la unidad de copia de seguridad:

<#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
[...]
```

- Mostrar información relacionada con la distribución y el uso de los bloques de puertos:

<#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
[...]
```

Información Relacionada

- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).