

Entender a Alocação de Portas no PAT Dinâmico para o Cluster FTD 7.0

Contents

- [Introdução](#)
- [Pré-requisitos](#)
- [Requisitos](#)
- [Componentes Utilizados](#)
- [Configurar](#)
- [Diagrama de Rede](#)
- [Configuração da interface](#)
- [Configuração de objeto de rede](#)
- [Configuração de PAT dinâmico](#)
- [Configuração final](#)
- [Verificar](#)
- [Verificar a interface IP e a configuração do NAT](#)
- [Verificar Alocação de Bloco de Porta](#)
- [Verificar Recuperação de Bloco de Porta](#)
- [Comandos para Troubleshooting](#)
- [Informações Relacionadas](#)

Introdução

Este documento descreve como a distribuição baseada em bloco de porta opera no PAT dinâmico para o cluster de firewall após a versão 7.0 e posterior.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Network Address Translation (NAT) no Cisco Secure Firewall

Componentes Utilizados

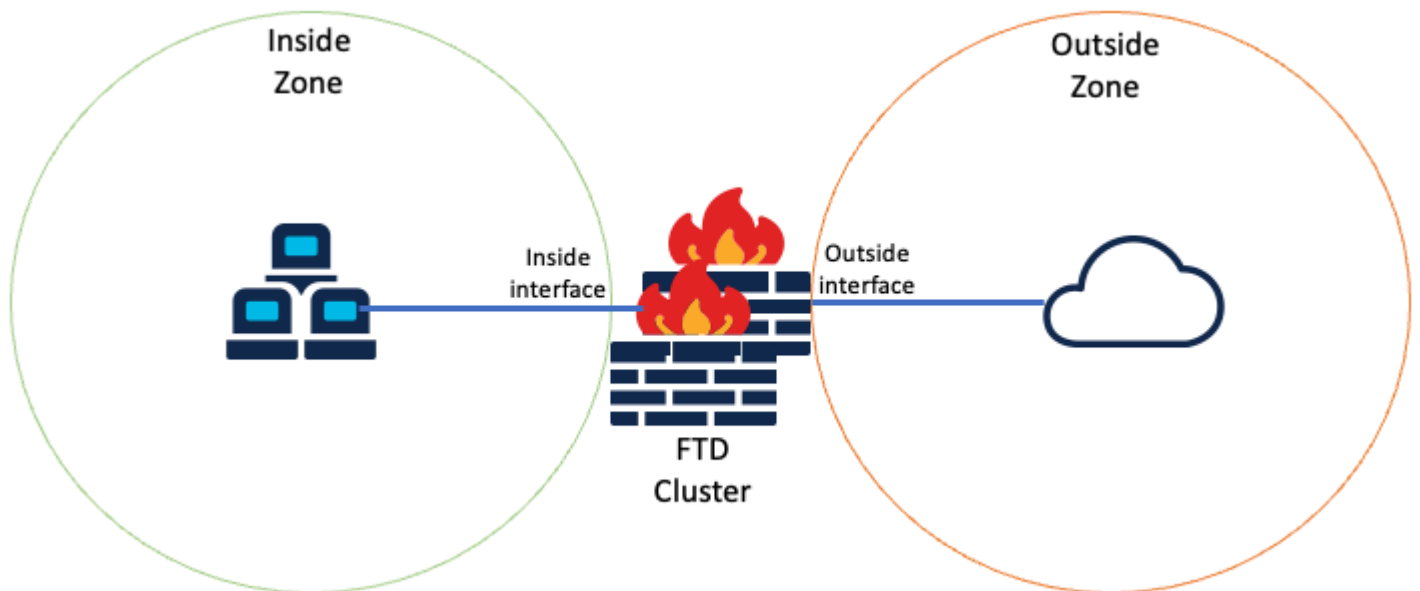
As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Management Center 7.3.0
- Firepower Threat Defense 7.2.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Topologia lógica

Configuração da interface

- Configure o membro da interface Inside da Zona Interna.

Por exemplo, configure uma interface com o endereço IP 192.168.10.254 e nomeie-a **Inside**. Essa interface interna é o Gateway para a rede interna 192.168.10.0/24.

Edit Ether Channel Interface

General IPv4 IPv6 Path Monitoring Advanced

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Edit Ether Channel Interface

General IPv4 IPv6 Path Monitoring Advanced

IP Type:

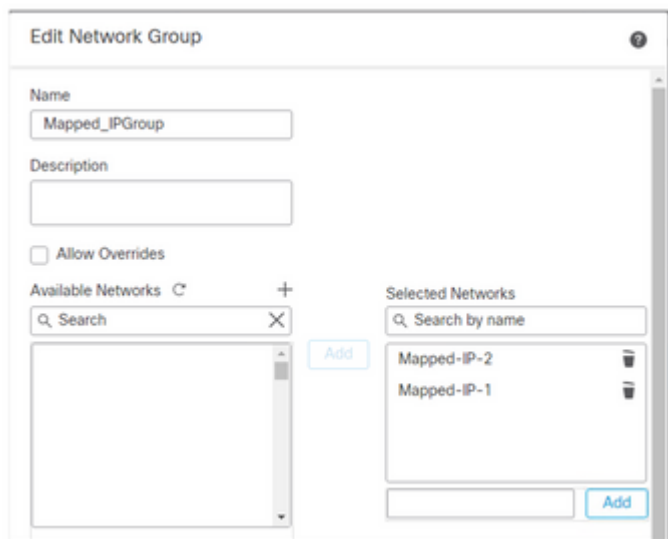
IP Address:

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- Configure o membro da interface Externa da Zona Externa.

Por exemplo, configure uma interface com o endereço IP 10.10.10.254 e nomeie-a como Outside. Essa inter

(feito de Mapped-IP-1 10.10.10.100 e Mapped-IP-2 10.10.10.101), é usado para mapear todo o tráfego interno para a Zona Externa.



Edit Network Group

Name: Mapped_IPGroup

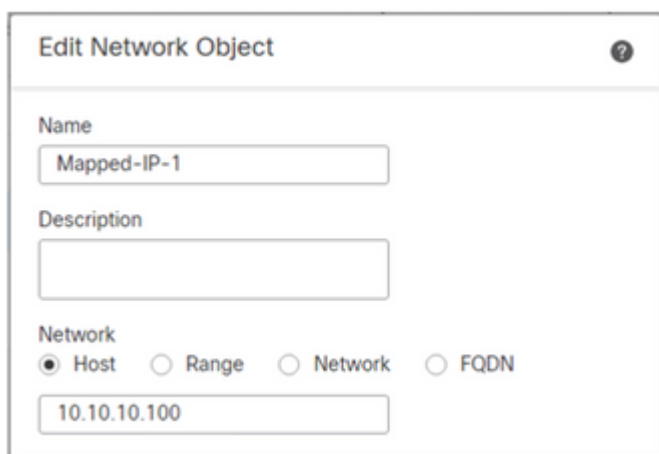
Description:

Allow Overrides

Available Networks:

Selected Networks:

- Mapped-IP-2
- Mapped-IP-1

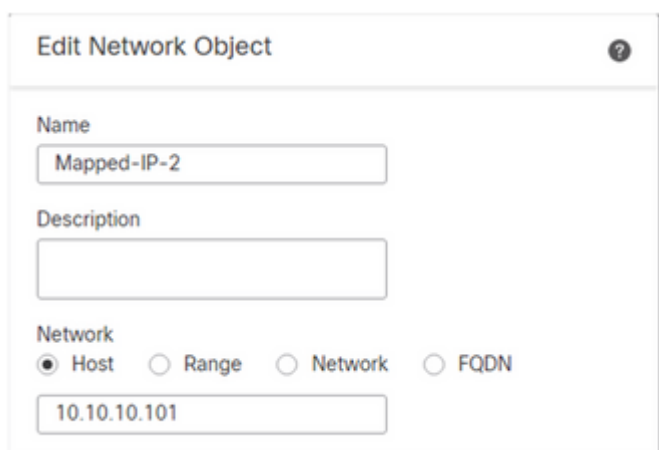


Edit Network Object

Name: Mapped-IP-1

Description:

Network: Host Range Network FQDN



Edit Network Object

Name: Mapped-IP-2

Description:

Network: Host Range Network FQDN

Configuração de PAT dinâmico

- Configure uma regra de NAT dinâmico para o tráfego de saída. Esta regra de NAT mapeia a sub-rede da rede interna para o pool de NAT externo.

Por exemplo, o tráfego de Zona Interna para Zona Externa de Rede Interna é convertido em Pool Mapped-IPGroup.

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- ISP1
- Lab-Zone
- Outside-Zone**
- VT1
- VT12

Source Interface Objects (1): Inside-Zone

Destination Interface Objects (1): Outside-Zone

Buttons: Add to Source, Add to Destination

Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

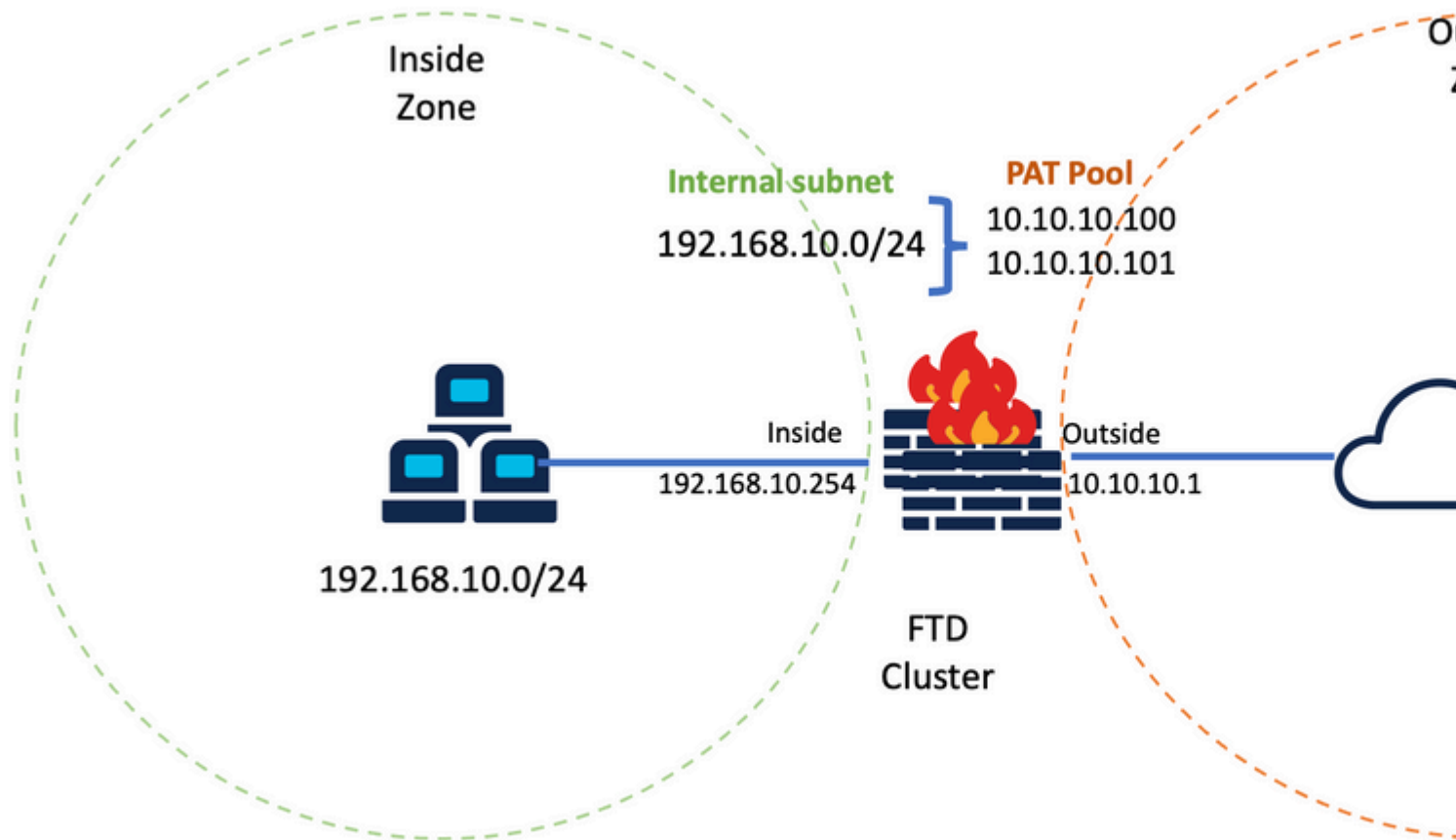
Interface Objects Translation PAT Pool Advanced

| Original Packet | Translated Packet |
|-------------------------------------|-------------------------------|
| Original Source:* Inside-Network | Translated Source: Address |
| Original Port: TCP | Mapped_IPGroup |
| | Translated Port: |

Auto NAT Rules

| | | | | | | | | | |
|--------------------------|---|---|---------|-------------|--------------|----------------|----------------|--------|--|
| <input type="checkbox"/> | # | x | Dynamic | Inside-Zone | Outside-Zone | Inside-Network | Mapped_IPGroup | Dns:fa | |
|--------------------------|---|---|---------|-------------|--------------|----------------|----------------|--------|--|

Configuração final



Configuração Final do Laboratório.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verificar a interface IP e a configuração do 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 Alocação de Bloco de Porta

Após o Firepower 7.0

a alocação de bloco de porta PAT aprimorada garante que a unidade de controle mantenha as portas na reserva para unir nós e recupere proativamente as portas não utilizadas. É assim que funciona a alocação de porta:

- Em um cluster que acaba de ser criado, a unidade de controle possui inicialmente 50% das portas e o restante é reservado.
- O número de blocos de porta possuídos por unidade é ajustado à medida que mais nós ingressam no cluster.
- A unidade de controle reserva blocos de porta para nós (N+1) até que o cluster esteja cheio. O limite de membros do cluster é definido pelo `cluster-member-limit`, configurado no nível de configuração do grupo de clusters.
- Por padrão, `cluster-member-limit` é 16.

```
<#root>
> show cluster info
```

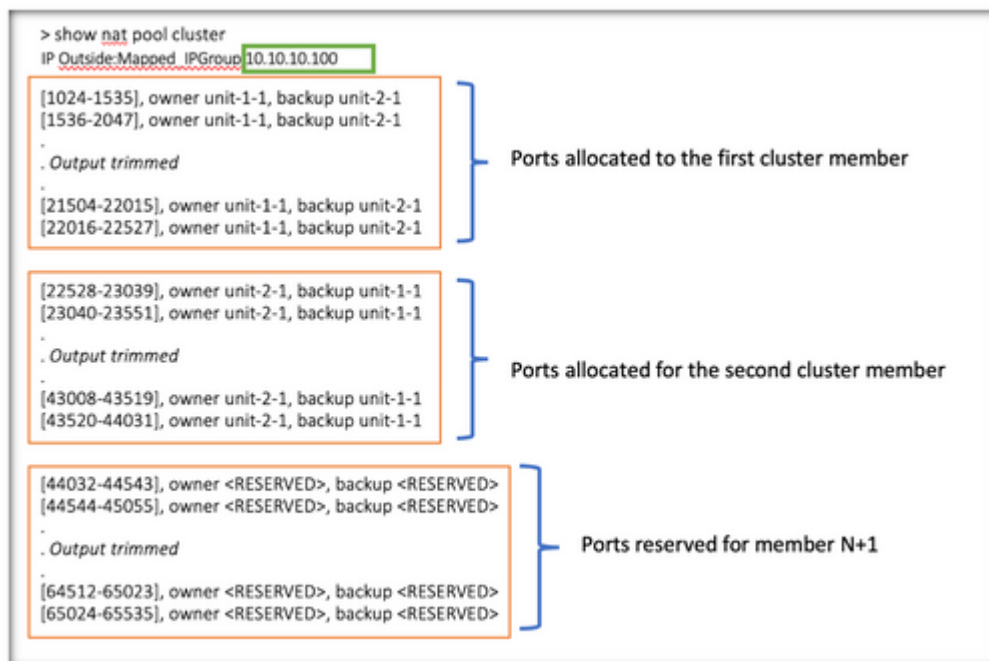
```
Cluster FTD-Cluster: On
Interface mode: spanned
```

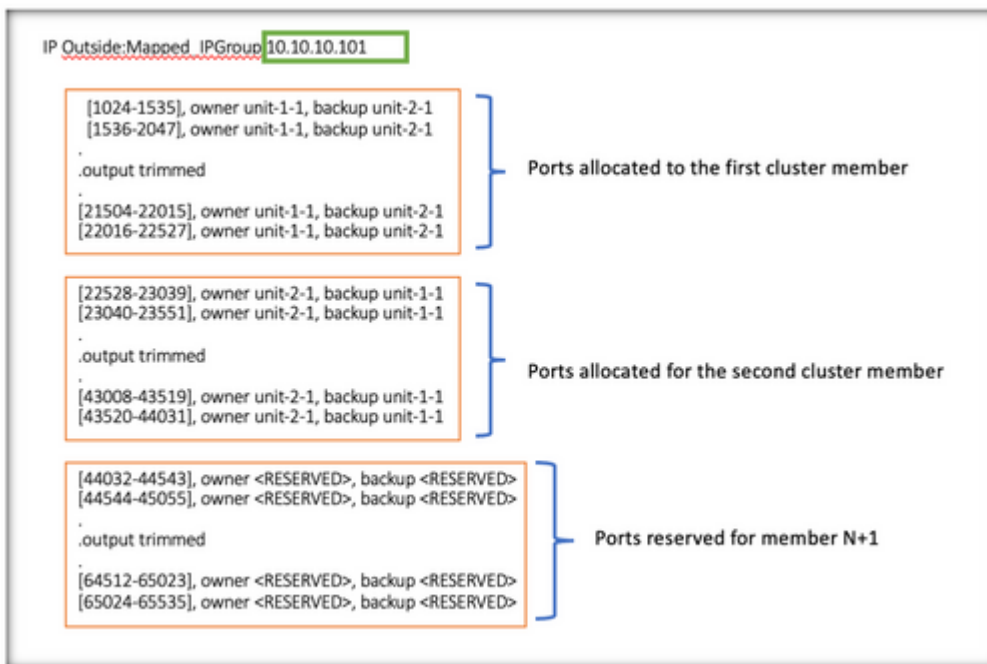
```
Cluster Member Limit : 16
```

```
[...]
```

- Quando a quantidade de membros do cluster atingir o valor configurado com `cluster-member-limit`, todos os blocos de porta são distribuídos entre os membros do cluster.

Por exemplo, em um grupo de cluster composto de duas unidades (N=2) com um valor padrão de limite de membro de cluster de 16, observa-se que a alocação de porta é definida para membros N+1, neste caso, 3. Isso deixa algumas portas reservadas para a próxima unidade até que o limite máximo de cluster seja atingido.





```
> 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 - 42 / 42) ^ 42 # 0
IP Outside:Mapped-IP-1 10.10.10.101 (126 - 42 / 42) ^ 42 # 0
```

Além disso, é uma prática recomendada configurar o `cluster-member-limit` para corresponder ao número de unidades planejadas para a implantação do cluster.

Por exemplo, em um grupo de cluster composto de duas unidades (N=2) com o valor do limite de membro de cluster de 2, observa-se que a alocação de porta é distribuída uniformemente em todas as unidades de cluster. Nenhuma das portas reservadas foi deixada.


```

> 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
.
.output trimmed
.
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1
.
[22528-23039], owner unit-2-1, backup unit-1-1
[23040-23551], owner unit-2-1, backup unit-1-1
.
.output trimmed
.
[43008-43519], owner unit-2-1, backup unit-1-1
[43520-44031], owner unit-2-1, backup unit-1-1
.
[44032-44543], owner unit-1-1, backup unit-2-1
[44544-45055], owner unit-1-1, backup unit-2-1
.
.output trimmed
.
[53760-54271], owner unit-1-1, backup unit-2-1
[54272-54783], owner unit-1-1, backup unit-2-1
.
[54784-55295], owner unit-2-1, backup unit-1-1
[55296-55807], owner unit-2-1, backup unit-1-1
.
.output trimmed
.
[64512-65023], owner unit-2-1, backup unit-1-1
[65024-65535], owner unit-2-1, backup unit-1-1
.

```

Ports allocated to the first cluster member

Ports allocated for the second cluster member

Ports allocated to the first cluster member

Ports allocated for the second cluster member

```

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
.
.output trimmed
.
[21504-22015], owner unit-1-1, backup unit-2-1
[22016-22527], owner unit-1-1, backup unit-2-1
.
[22528-23039], owner unit-2-1, backup unit-1-1
[23040-23551], owner unit-2-1, backup unit-1-1
.
.output trimmed
.
[43008-43519], owner unit-2-1, backup unit-1-1
[43520-44031], owner unit-2-1, backup unit-1-1
.
[44032-44543], owner unit-1-1, backup unit-2-1
[44544-45055], owner unit-1-1, backup unit-2-1
.
.output trimmed
.
[53760-54271], owner unit-1-1, backup unit-2-1
[54272-54783], owner unit-1-1, backup unit-2-1
.
[54784-55295], owner unit-2-1, backup unit-1-1
[55296-55807], owner unit-2-1, backup unit-1-1
.
.output trimmed
.
[64512-65023], owner unit-2-1, backup unit-1-1
[65024-65535], owner unit-2-1, backup unit-1-1
.

```

Ports allocated to the first cluster member

Ports allocated for the second cluster member

Ports allocated to the first cluster member

Ports allocated for the second cluster member

```

> 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 Recuperação de Bloco de Porta

- Sempre que um novo nó ingressa ou sai de um cluster, as portas não utilizadas e os blocos de portas em excesso de todas as unidades devem ser liberados para a unidade de controle.
- Se os blocos de portas já estiverem sendo usados, os menos usados serão marcados para recuperação.
- Novas conexões não são permitidas em blocos de porta recuperados. Eles são liberados para a unidade de controle quando a última porta é limpa.

```
> 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 Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Verifique o 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
```

```
[...]
```

- Exiba um resumo da distribuição dos blocos de porta entre as unidades no cluster:

```
<#root>
```

```
> show nat pool cluster summary
```

```

> 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 - 63 / 63) ^ 0 # 0
IP Outside:Mapped IPGroup 10.10.10.101 (126 - 63 / 63) ^ 0 # 0

```

- Exiba a atribuição atual de blocos de porta por endereço PAT para o proprietário e a unidade de 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
[...]

```

- Exibir informações relacionadas à distribuição e ao uso de blocos de porta:

<#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
[...]

```

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.