Substitua a unidade defeituosa no Secure Firewall Threat Defense of High Availability

Contents

Introdução

Este documento descreve como substituir um módulo Secure Firewall Threat Defense defeituoso que faz parte de uma configuração de alta disponibilidade (HA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall Management Center (FMC)
- Sistema operacional extensível Cisco Firepower (FXOS)
- Defesa contra ameaças (FTD) do Cisco Secure Firewall

Componentes Utilizados

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

- O Firepower 4110 executa o FXOS v2.12(0.498)
- O dispositivo lógico executa o Cisco Secure Firewall v7.2.5
- O Secure Firewall Management Center 2600 é executado na v7.4
- Conhecimento de Secure Copy Protocol (SCP)

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.

Informações de Apoio

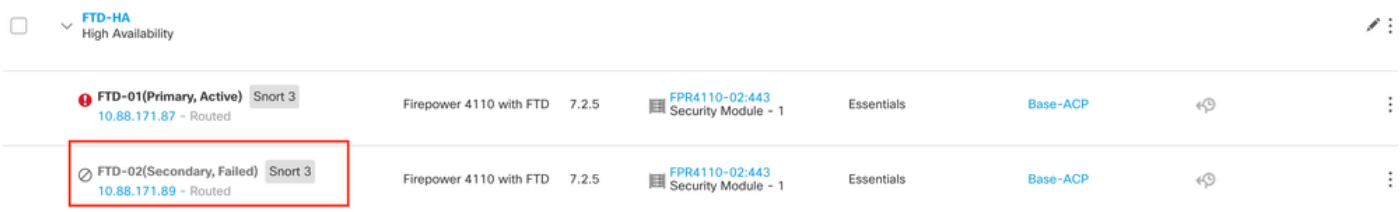
Este procedimento é compatível com dispositivos:

- Dispositivos Cisco Secure Firewall 1000 Series
- Dispositivos Cisco Secure Firewall 2100 Series
- Dispositivos Cisco Secure Firewall 3100 Series
- Dispositivos Cisco Secure Firewall 4100 Series
- Dispositivos Cisco Secure Firewall 4200 Series
- Dispositivo Cisco Secure Firewall 9300
- Cisco Secure Firewall Threat Defense para VMWare

Antes de Começar

Este documento requer que você tenha a nova unidade configurada com as mesmas versões de FXOS e FTD.

Identifique a unidade com defeito

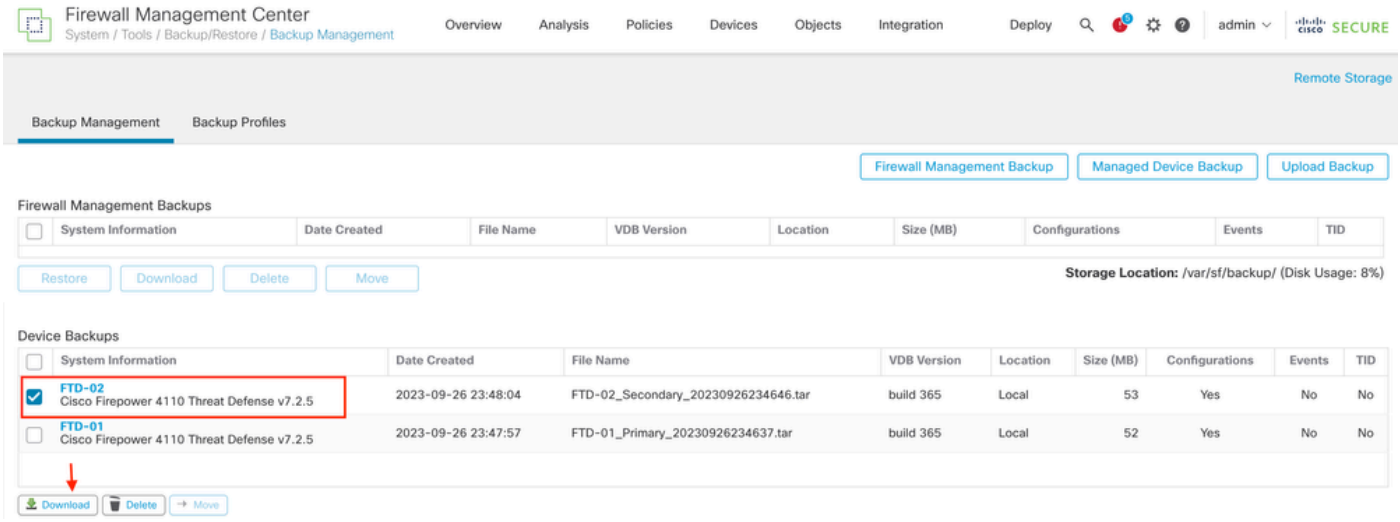


Neste cenário, a unidade secundária (FTD-02) está em um estado de falha.

Substitua uma unidade com defeito por uma de backup

Use este procedimento para substituir a unidade Primária ou Secundária. Este guia pressupõe que você tenha um backup da unidade defeituosa que será substituída.

Etapa 1. Faça o download do arquivo de backup do FMC. Navegue até System > Tools > Restore > Device Backups e selecione o backup correto. Clique em Download:



Etapa 2. Fazer upload do backup FTD para o diretório /var/sf/backup/ do novo FTD:

2.1 No test-pc (cliente SCP), faça upload do arquivo de backup para o FTD no diretório /var/tmp/:

```
@test-pc ~ % scp FTD-02_Secondary_20230926234646.tar cisco@10.88.243.90:/var/tmp/
```

2.2 Do modo especialista em FTD CLI, mova o arquivo de backup de /var/tmp/ para /var/sf/backup/:

```
root@firepower:/var/tmp# mv FTD-02_Secondary_20230926234646.tar /var/sf/backup/
```

Etapa 3. Restaure o backup FTD-02, aplicando o próximo comando a partir do modo clish:

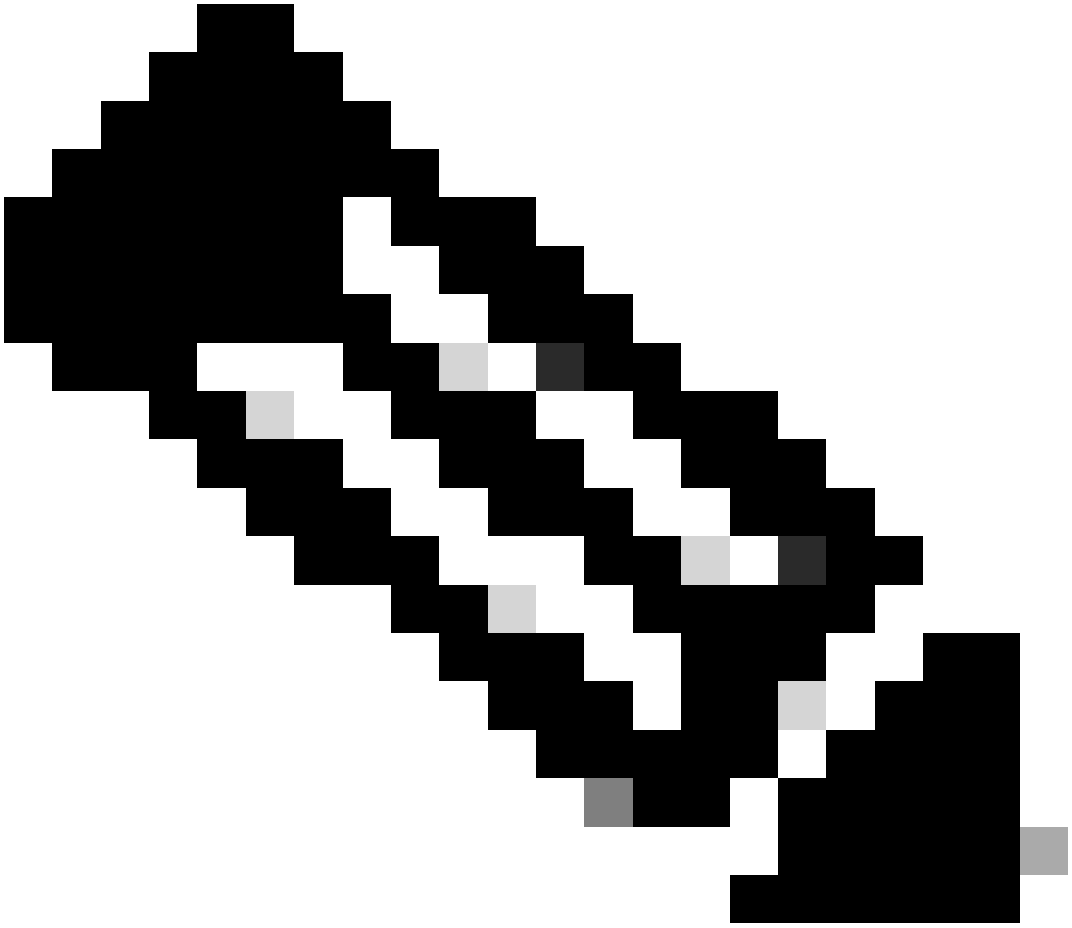
```
>restore remote-manager-backup FTD-02_Secondary_20230926234646.tar
```

```
Device model from backup :: Cisco Firepower 4110 Threat Defense
This Device Model  :: Cisco Firepower 4110 Threat Defense
************************************************
Backup Details
************************************************
Model = Cisco Firepower 4110 Threat Defense
Software Version = 7.2.5
Serial = FLM22500791
Hostname = firepower
Device Name = FTD-02_Secondary
IP Address = 10.88.171.89
Role = SECONDARY
VDB Version = 365
SRU Version =
FXOS Version = 2.12(0.498)
Manager IP(s) = 10.88.243.90
Backup Date = 2023-09-26 23:46:46
Backup Filename = FTD-02_Secondary_20230926234646.tar
************************************************

********************* Caution ****************************
Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest be
Restore operation will overwrite all configurations on this device with configurations in backup.
If this restoration is being performed on an RMA device then ensure old device is removed from network
************************************************************
Are you sure you want to continue (Y/N)Y
Restoring device . . . . . .
Added table audit_log with table_id 1
Added table health_alarm_syslog with table_id 2
Added table dce_event with table_id 3
Added table application with table_id 4
Added table rna_scan_results_tableview with table_id 5
Added table rna_event with table_id 6
Added table ioc_state with table_id 7
Added table third_party_vulns with table_id 8
Added table user_ioc_state with table_id 9
Added table rna_client_app with table_id 10
Added table rna_attribute with table_id 11
Added table captured_file with table_id 12
Added table rna_ip_host with table_id 13
Added table flow_chunk with table_id 14
Added table rua_event with table_id 15
Added table wl_dce_event with table_id 16
Added table user_identities with table_id 17
Added table whitelist_violations with table_id 18
Added table remediation_status with table_id 19
Added table syslog_event with table_id 20
Added table rna_service with table_id 21
Added table rna_vuln with table_id 22
Added table SRU_import_log with table_id 23
Added table current_users with table_id 24

Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023):

The system is going down for reboot NOW!
```

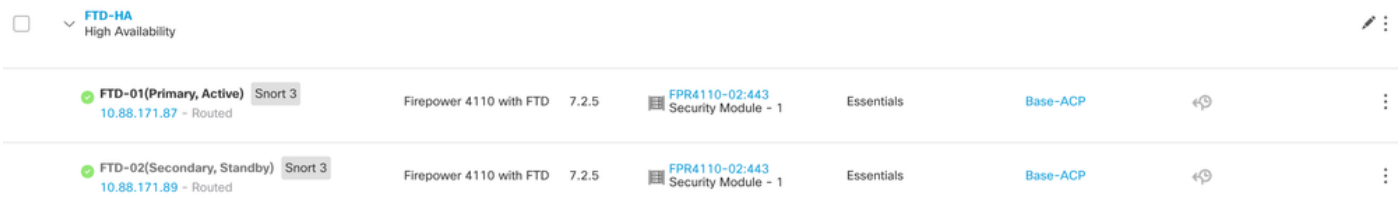


Note: Quando a restauração é concluída, o dispositivo encerra a sessão da CLI, reinicializa e se conecta automaticamente ao FMC. Neste momento, o dispositivo parecerá desatualizado.

Etapa 4. Retome a sincronização de alta disponibilidade. Na CLI do FTD, insira configure high-availability resume:

```
>configure high-availability resume
```

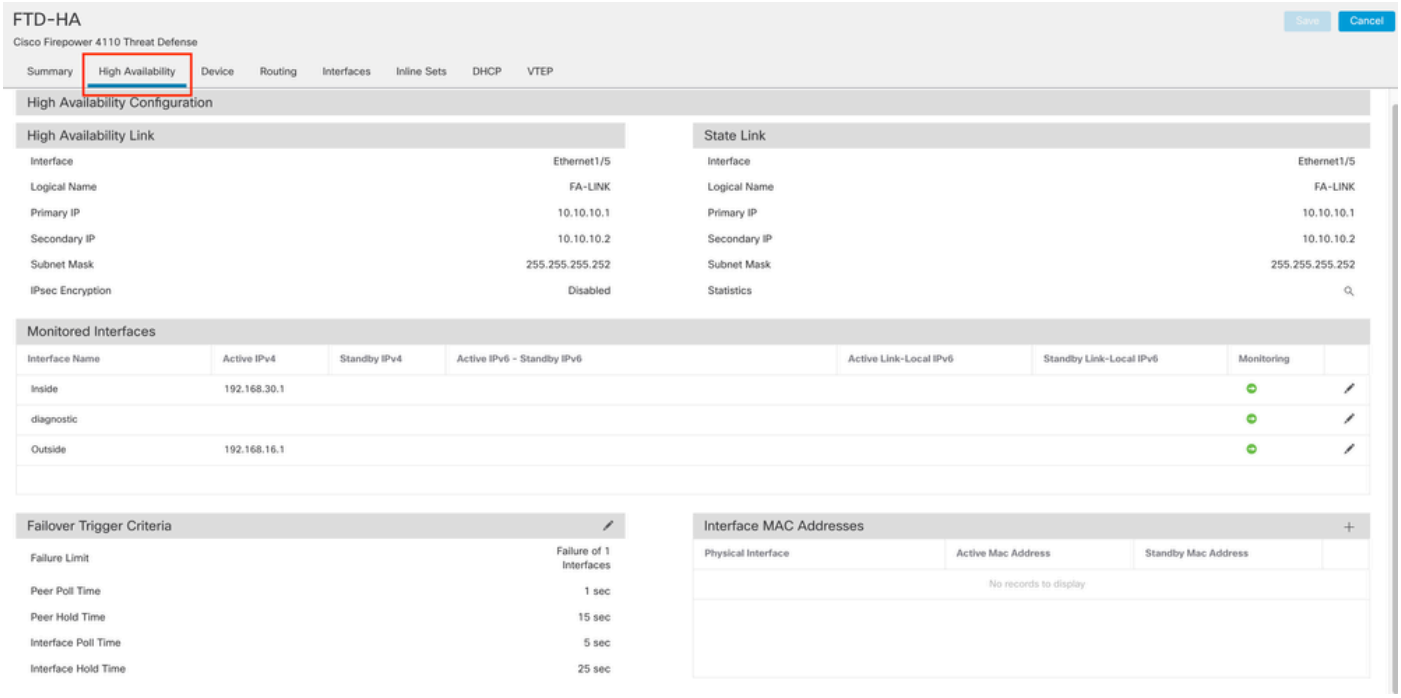
A configuração de alta disponibilidade do FTD agora está concluída:



Substitua uma unidade com defeito sem fazer backup

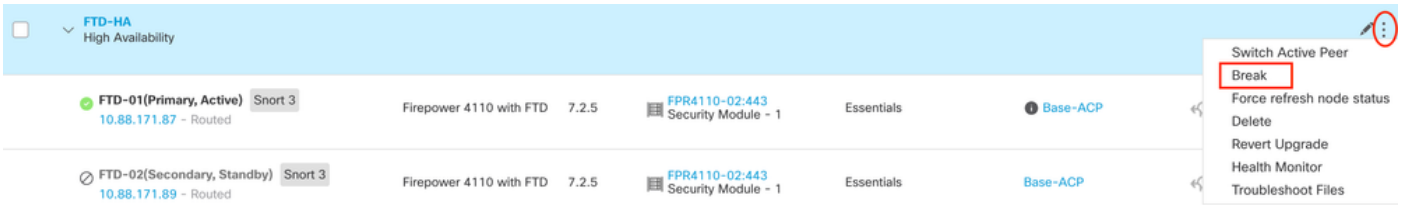
Se você não tiver um backup do dispositivo com falha, prossiga com este guia. Você pode substituir a unidade Primária ou Secundária, tO processo varia dependendo se o dispositivo é primário ou secundário. Todas as etapas descritas neste guia são para restaurar uma unidade secundária com defeito. Se quiser restaurar uma unidade primária com defeito, na Etapa 5, configure a alta disponibilidade, usando a unidade secundária/ativa existente como dispositivo primário e o dispositivo de substituição como dispositivo secundário/standby durante o registro.

Etapa 1. Faça uma captura de tela (backup) da configuração de alta disponibilidade navegando até Device > Device Management. Edite o par HA FTD correto (clique no ícone do lápis) e clique na opção High Availability:

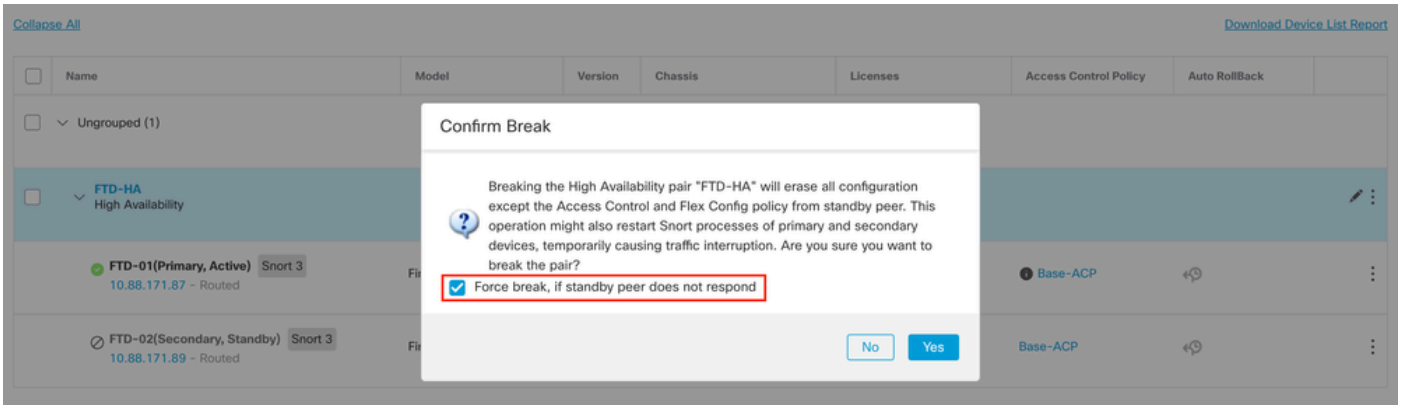


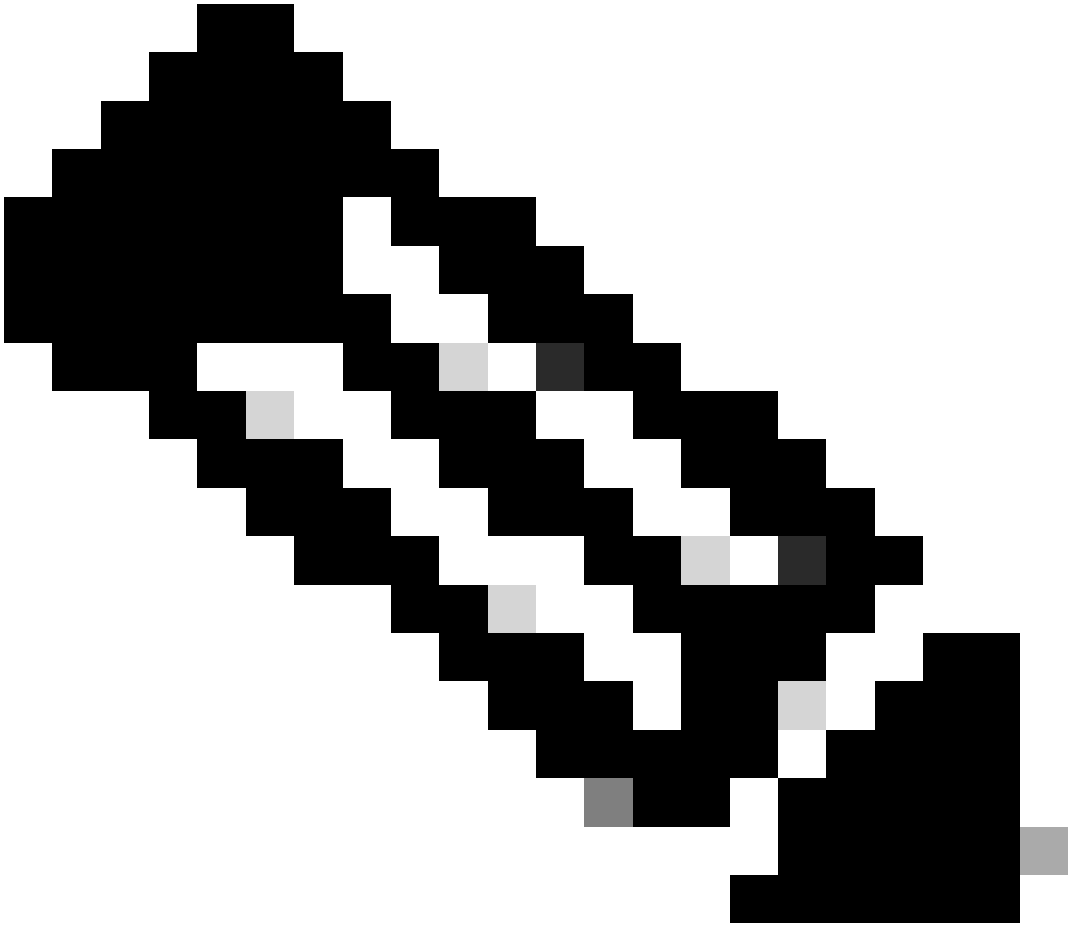
Etapa 2. Quebre o HA.

2.1 Navegue até Devices > Device Management e clique no menu de três pontos no canto superior direito. Em seguida, clique na opção Break:



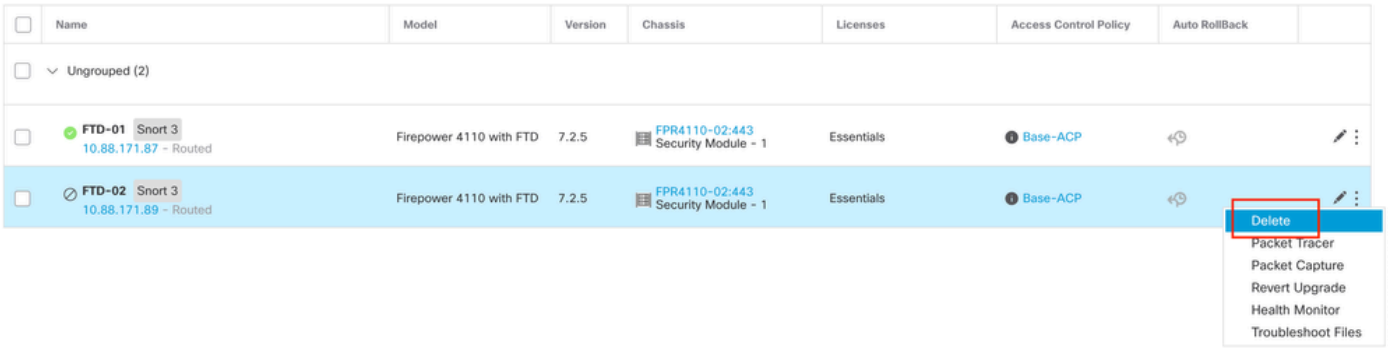
2.2. Selecione Forçar interrupção, se o peer em standby não responder opção:





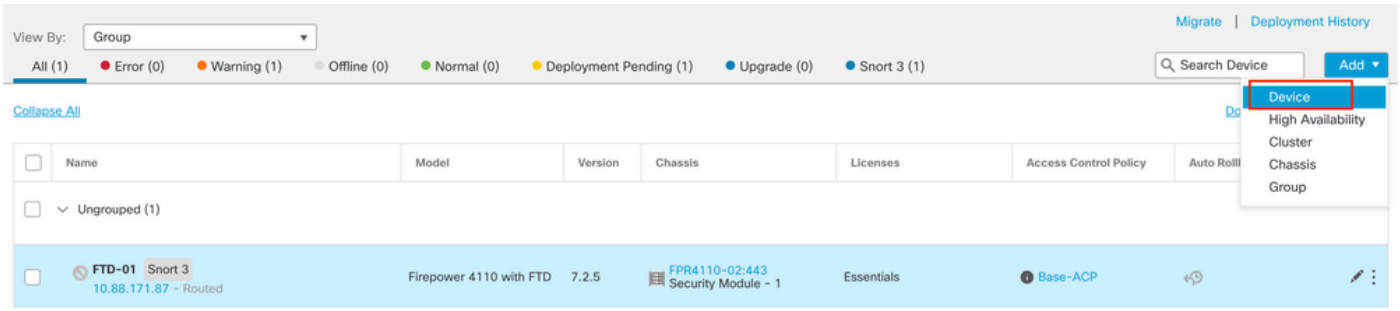
Note: Como a unidade não responde, você precisa forçar a interrupção do HA. Quando você quebra um par de alta disponibilidade, o dispositivo ativo retém a funcionalidade implantada completa. O dispositivo em standby perde suas configurações de failover e interface e torna-se um dispositivo autônomo.

Etapa 3. Excluir FTD com defeito. Identifique o FTD a ser substituído e clique no menu de três pontos. Clique em Excluir:



Etapa 4. Adicione o novo FTD.

4.1. Navegue até Devices > Device Management > Add e clique em Device:



4.2. Selecione o Método de Provisionamento, neste caso, Chave de Registro, configure Host, Exibir Nome, Chave de Registro. Configure uma Política de Controle de Acesso e clique em Registrar.

Add Device

Select the Provisioning Method:

(•) Registration Key ( ) Serial Number

[ ] CDO Managed Device

Host:†

10.88.171.89

Display Name:

FTD-02

Registration Key:*

••••••••

Group:

None

Access Control Policy:*

Base-ACP

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Select a recommended Tier

[ ] Carrier
[ ] Malware Defense
[ ] IPS
[ ] URL

Advanced

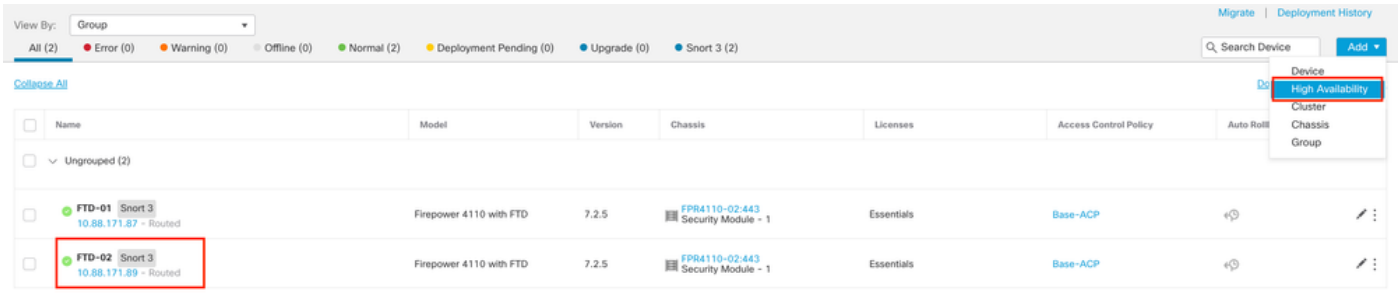
Unique NAT ID:†

[ ] Transfer Packets

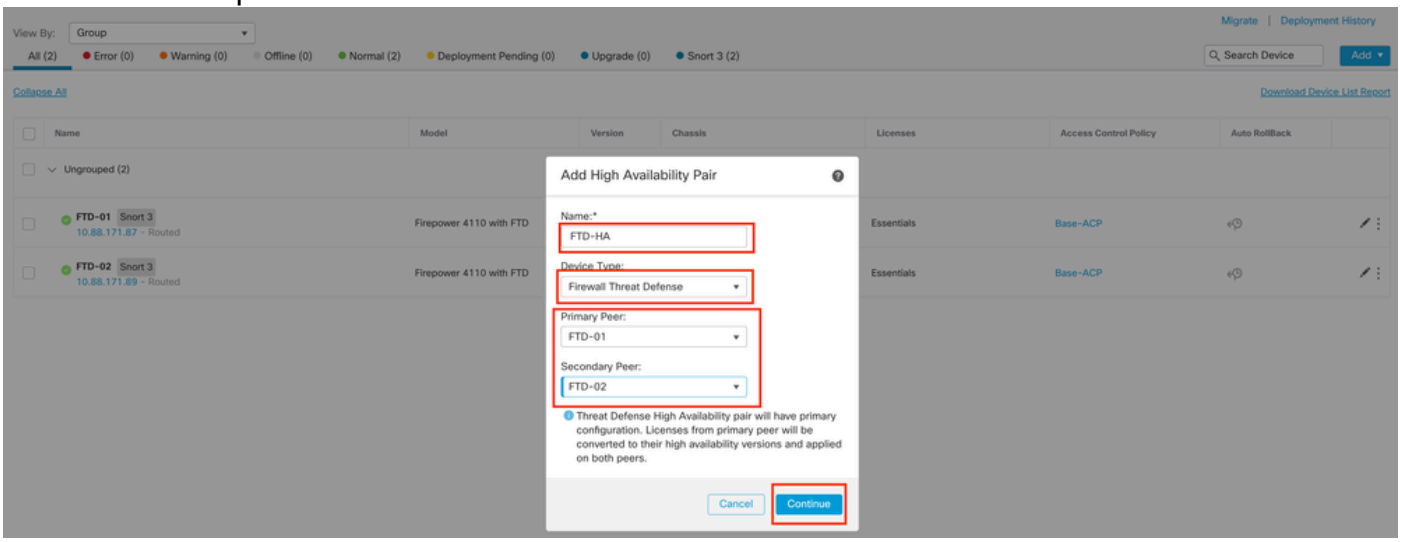
Cancel Register

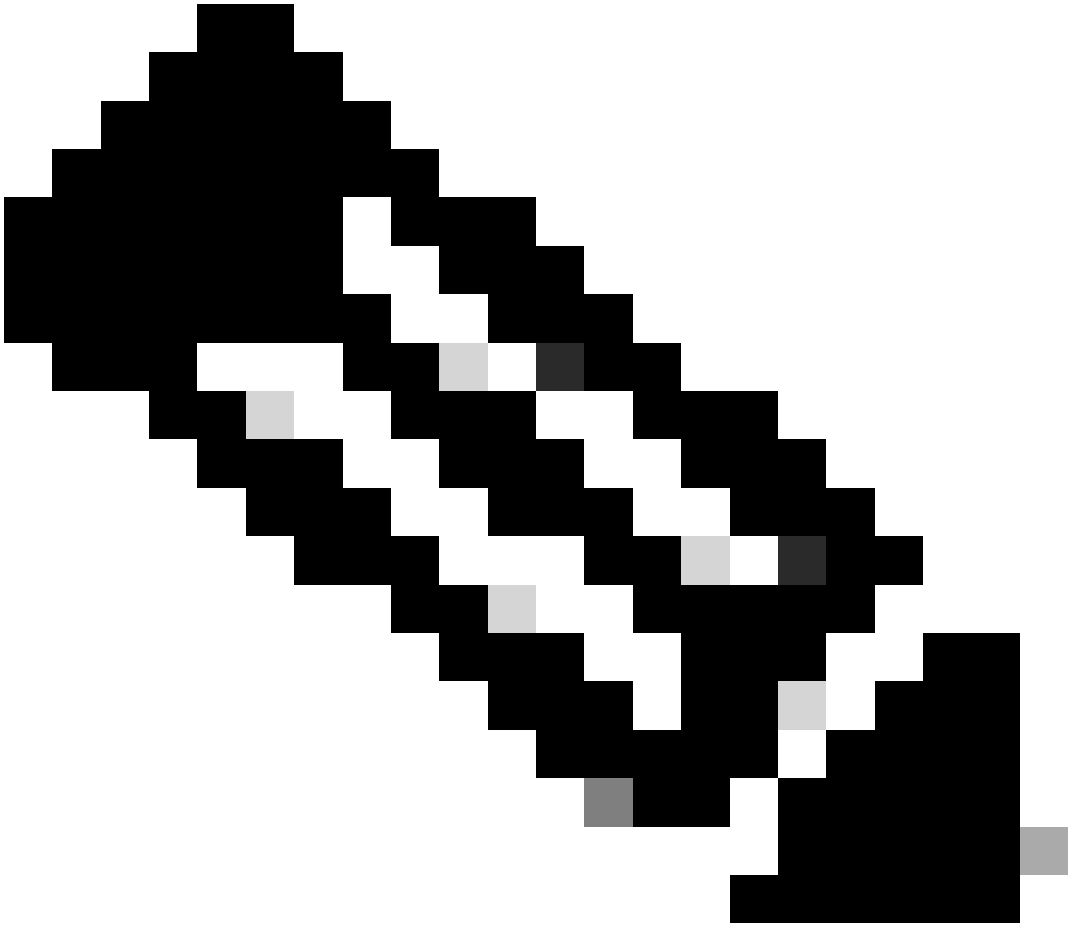
Etapa 5. Crie o HA.

5.1 Navegue até Devices > Device Management > Add e clique na opção High Availability.



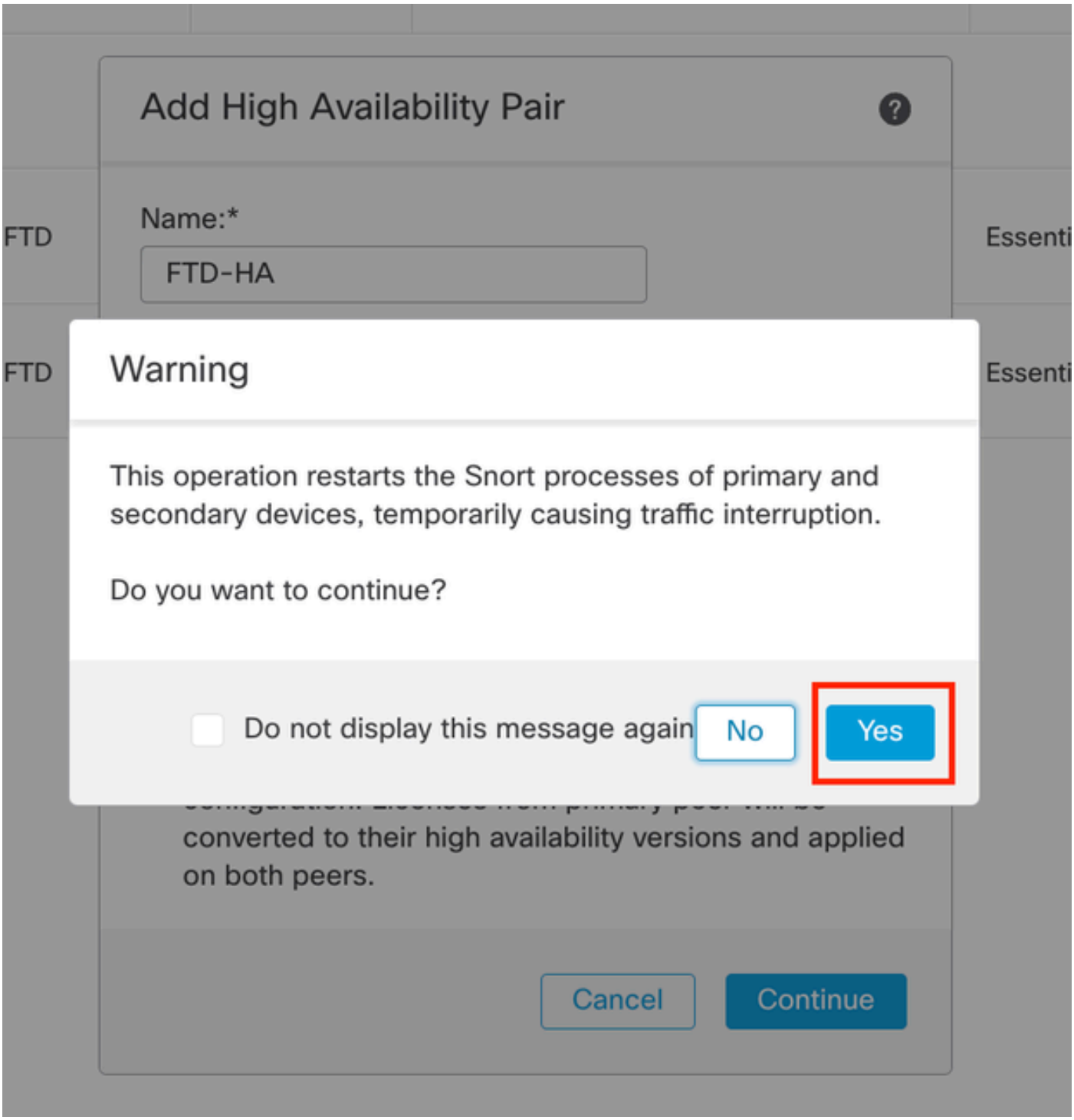
5.2. Configure o Add High Availability Pair (Adicionar par de alta disponibilidade). Configure o Nome, o Tipo de dispositivo, selecione FTD-01 como o Par primário e FTD-02 como o Par secundário e clique em Continuar.

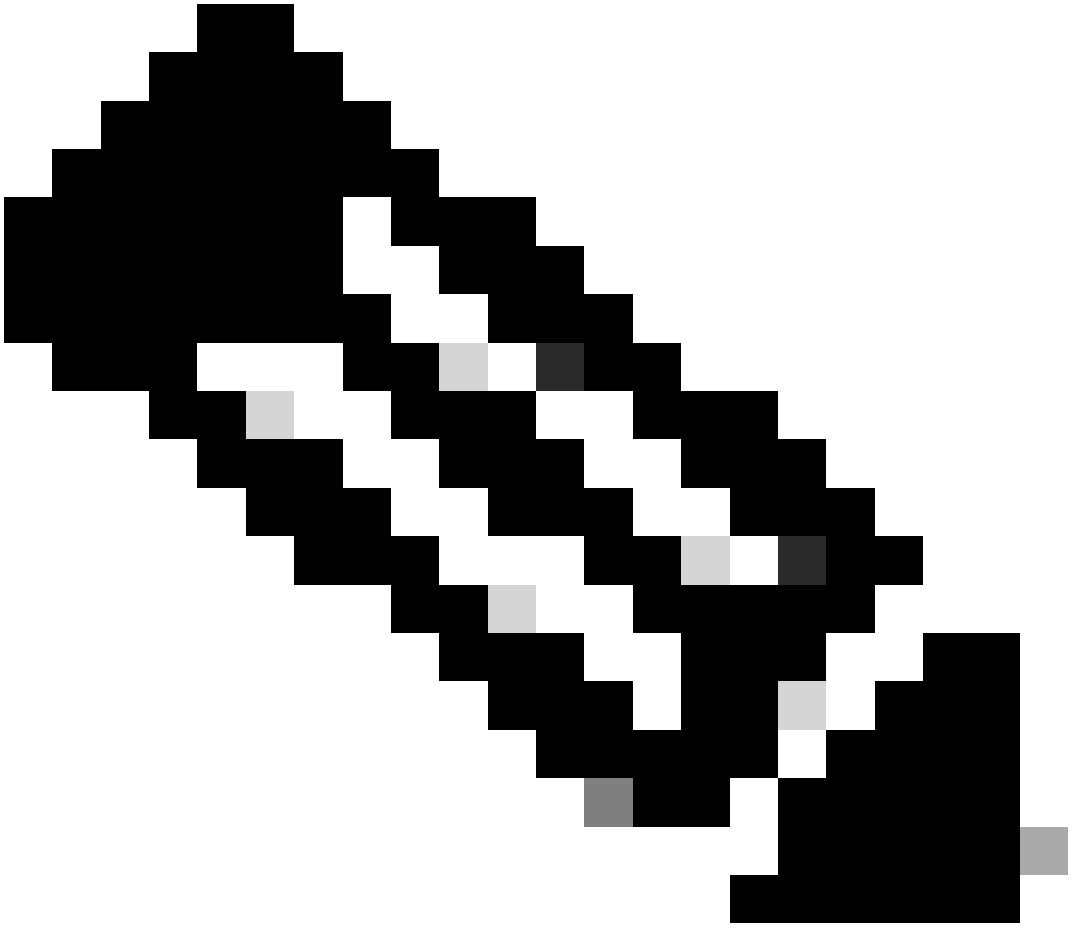




Note: Lembre-se de selecionar a unidade Primária como o dispositivo que ainda tem a configuração, neste caso, FTD-01.

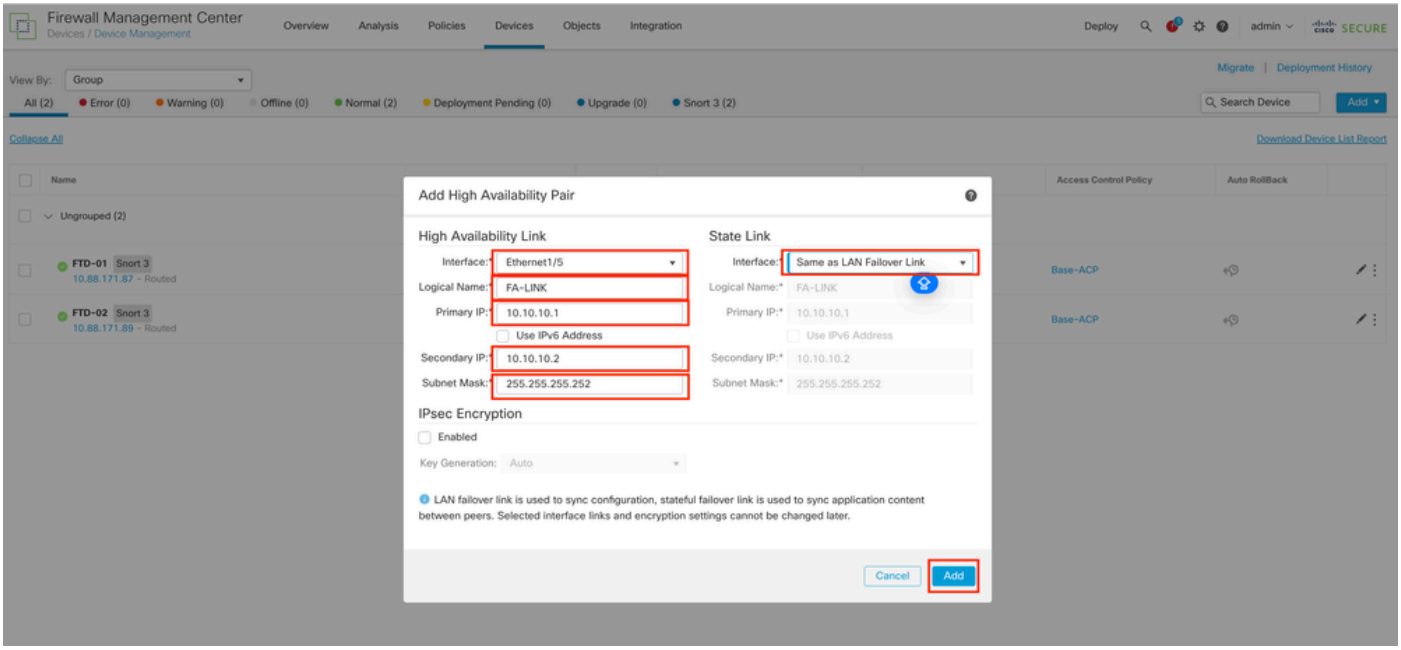
5.3. Confirme a criação de HA e clique em Sim.


Add High Availability Pair
Name:*
FTD-HA
FTD
Essenti
FTD
Essenti
Warning
This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.
Do you want to continue?
Do not display this message again
No
Yes
converted to their high availability versions and applied on both peers.
Cancel
Continue

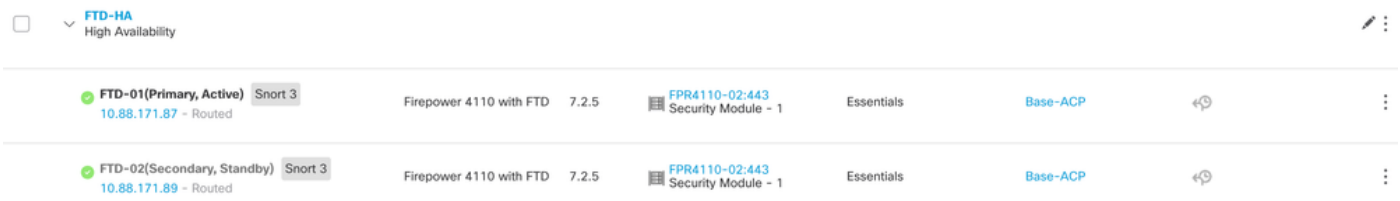


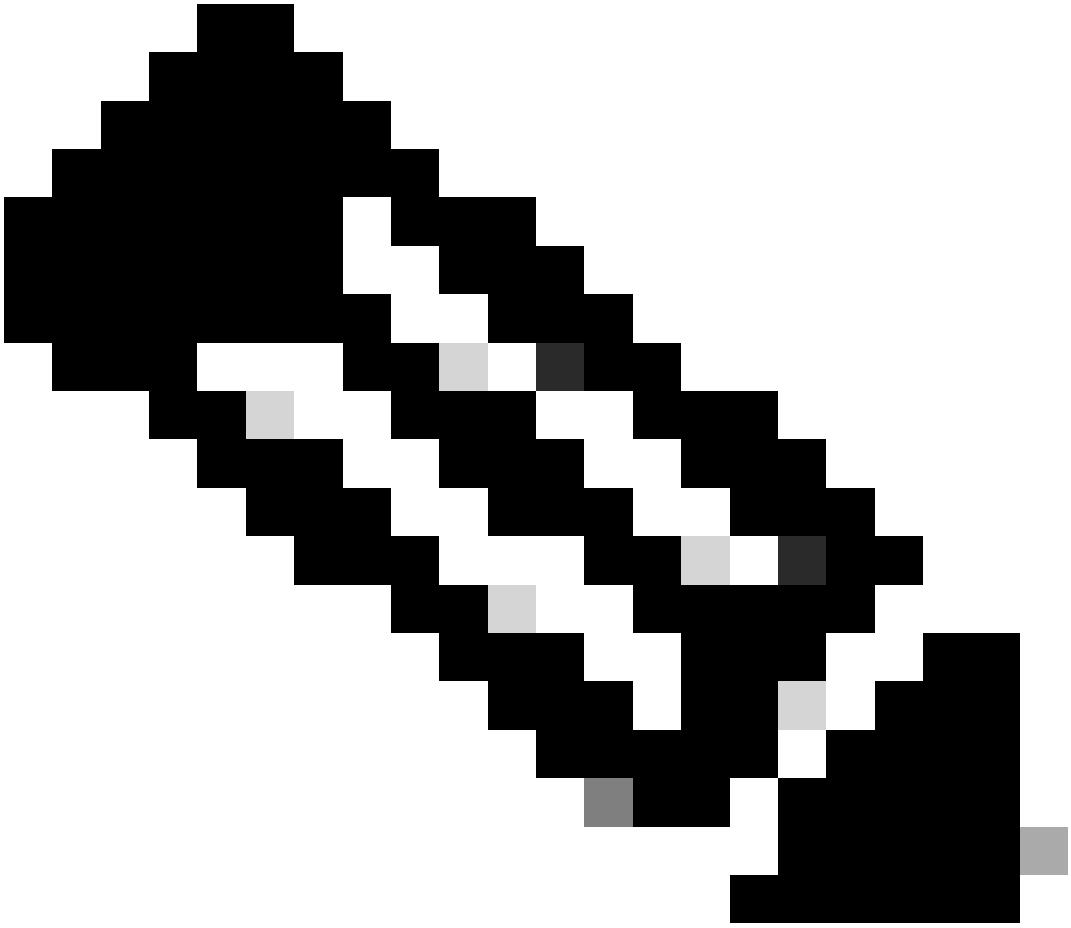
Note: A configuração de alta disponibilidade reinicia o mecanismo de snort de ambas as unidades e isso pode causar a interrupção do tráfego.

5.4. Configure os parâmetros de alta disponibilidade obtidos na etapa 2 e clique na opção Add:



6. A configuração de Alta Disponibilidade do FTD agora está concluída:





Note: Se você não configurar endereços MAC virtuais, precisará limpar as tabelas ARP nos roteadores conectados para restaurar o fluxo de tráfego em caso de substituição da unidade Primária. Para obter mais informações, consulte Endereços MAC e Endereços IP em Alta Disponibilidade.

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.