

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

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Antes de Começar](#)

[Identifique a unidade com defeito](#)

[Substitua uma unidade com defeito por uma de backup](#)

[Substitua uma unidade com defeito sem fazer backup](#)

[Informações Relacionadas](#)

---

## 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

Device Name	Status	Model	Version	Security Module	Configuration	Actions
FTD-01(Primary, Active)	Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials Base-ACP	↻ ⋮
FTD-02(Secondary, Failed)	Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials Base-ACP	↻ ⋮

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:

Firewall Management Center  
System / Tools / Backup/Restore / Backup Management

Overview Analysis Policies Devices Objects Integration Deploy

Backup Management Backup Profiles

Firewall Management Backups

<input type="checkbox"/>	System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input type="checkbox"/>	FTD-02 Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:48:04	FTD-02_Secondary_20230926234646.tar	build 365	Local	53	Yes	No	No
<input type="checkbox"/>	FTD-01 Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:47:57	FTD-01_Primary_20230926234637.tar	build 365	Local	52	Yes	No	No

Storage Location: /var/sf/backup/ (Disk Usage: 8%)

Download Delete Move

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:

Device Name	Status	Model	Version	Security Module	Configuration	Actions
FTD-01(Primary, Active)	Snort 3	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials Base-ACP	⌵
FTD-02(Secondary, Standby)	Snort 3	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials Base-ACP	⌵

## 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:

FTD-HA Save Cancel

Cisco Firepower 4110 Threat Defense

Summary **High Availability** Device Routing Interfaces Inline Sets DHCP VTEP

High Availability Configuration

High Availability Link		State Link	
Interface	Ethernet1/5	Interface	Ethernet1/5
Logical Name	FA-LINK	Logical Name	FA-LINK
Primary IP	10.10.10.1	Primary IP	10.10.10.1
Secondary IP	10.10.10.2	Secondary IP	10.10.10.2
Subnet Mask	255.255.255.252	Subnet Mask	255.255.255.252
IPsec Encryption	Disabled	Statistics	🔍

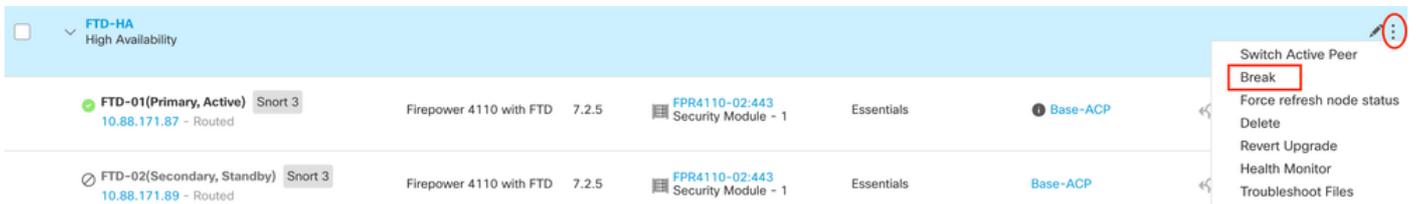
Monitored Interfaces						
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
Inside	192.168.30.1					🟢 ✎
diagnostic						🟢 ✎
Outside	192.168.16.1					🟢 ✎

Failover Trigger Criteria	
Failure Limit	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer Hold Time	15 sec
Interface Poll Time	5 sec
Interface Hold Time	25 sec

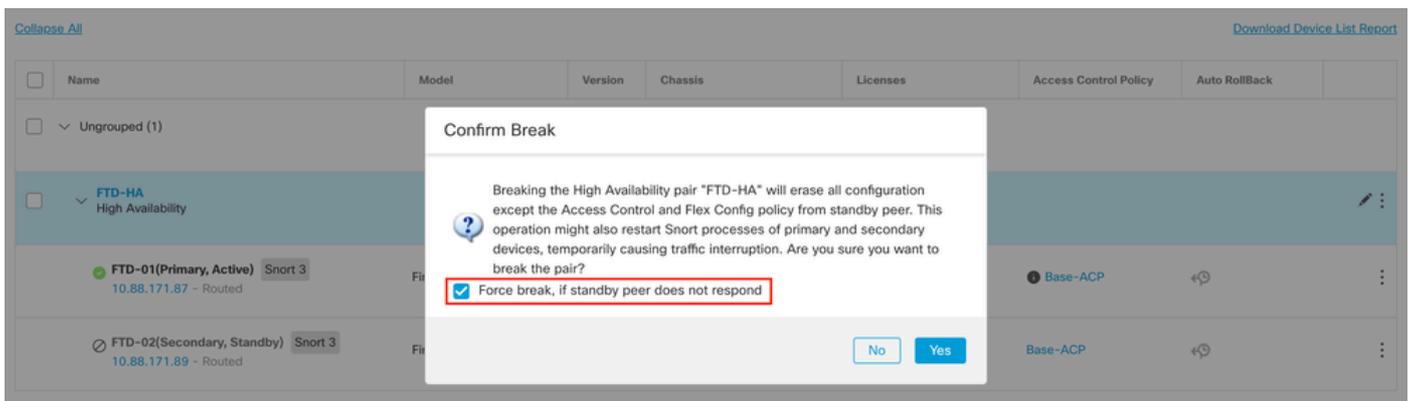
Interface MAC Addresses		
Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

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:

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (2)							
<input type="checkbox"/>	FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		
<input type="checkbox"/>	FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		<ul style="list-style-type: none"> <li>Delete</li> <li>Packet Tracer</li> <li>Packet Capture</li> <li>Revert Upgrade</li> <li>Health Monitor</li> <li>Troubleshoot Files</li> </ul>

Etapa 4. Adicione o novo FTD.

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

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Roll	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		<ul style="list-style-type: none"> <li>Device</li> <li>High Availability</li> <li>Cluster</li> <li>Chassis</li> <li>Group</li> </ul>

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:†

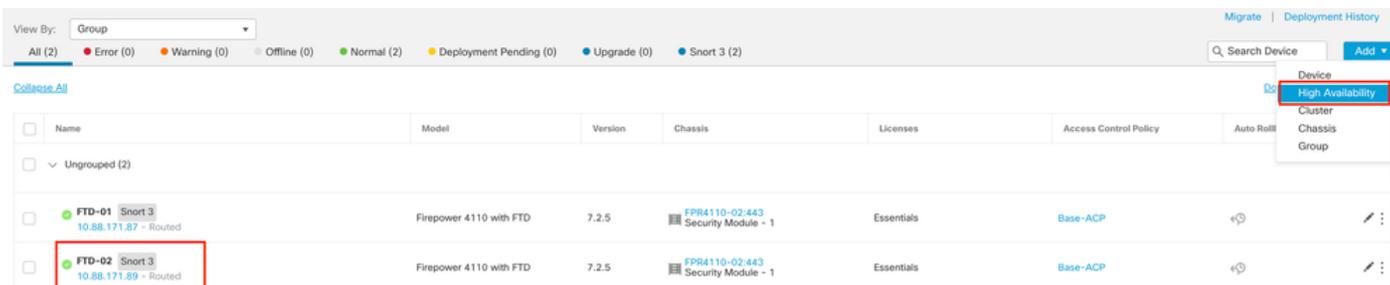
Transfer Packets

Cancel

Register

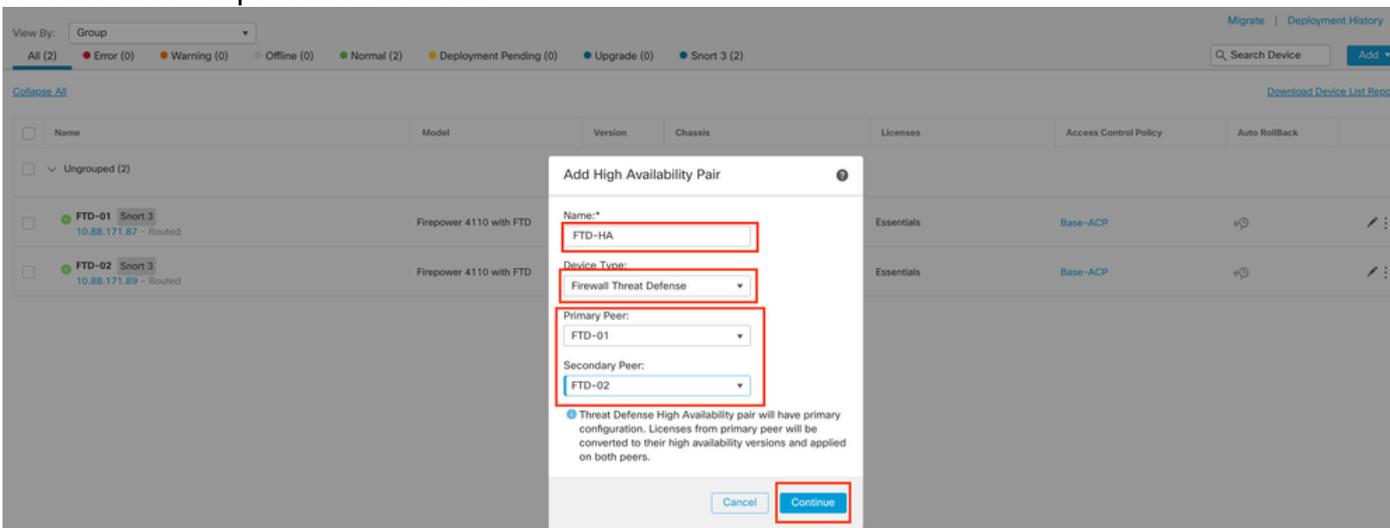
## Etapa 5. Crie o HA.

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



The screenshot shows the Palo Alto Networks Device Management interface. At the top, there is a 'View By:' dropdown set to 'Group' and a status bar showing 'All (2)', 'Error (0)', 'Warning (0)', 'Offline (0)', 'Normal (2)', 'Deployment Pending (0)', 'Upgrade (0)', and 'Snort 3 (2)'. A search bar and an 'Add' button are visible. The 'Add' button is highlighted with a red box, and a dropdown menu is open, showing options: 'Device', 'High Availability', 'Cluster', 'Chassis', and 'Group'. The 'High Availability' option is selected and highlighted with a red box. Below the menu, a table lists two devices: 'FTD-01' and 'FTD-02', both 'Firepower 4110 with FTD' with version '7.2.5'. The 'FTD-02' row is highlighted with a red box.

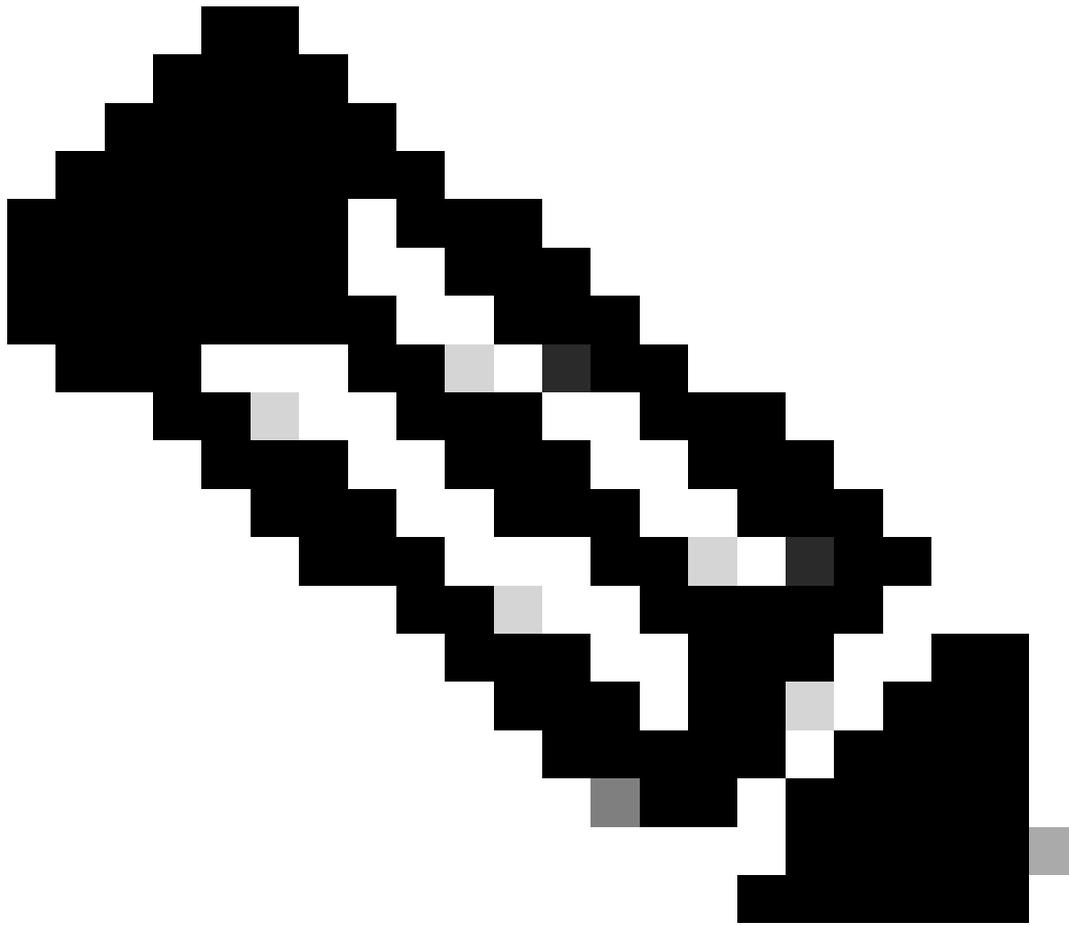
### 5.2. Configure o Add High Availability Pair (Adicionar par de alta disponibilidade). Configure o Nome, o Tipo de dispositivo, selecione FTD-01 como o Par primário e FTD-02 como o Par secundário e clique em Continuar.



The screenshot shows the 'Add High Availability Pair' dialog box in the Palo Alto Networks Device Management interface. The dialog box has a title bar 'Add High Availability Pair' and a close button. It contains the following fields and options:

- Name:** FTD-HA (highlighted with a red box)
- Device Type:** Firewall Threat Defense (highlighted with a red box)
- Primary Peer:** FTD-01 (highlighted with a red box)
- Secondary Peer:** FTD-02 (highlighted with a red box)

Below the fields, there is a note: "Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers." At the bottom of the dialog box, there are two buttons: 'Cancel' and 'Continue' (highlighted with a red box).



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

### 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

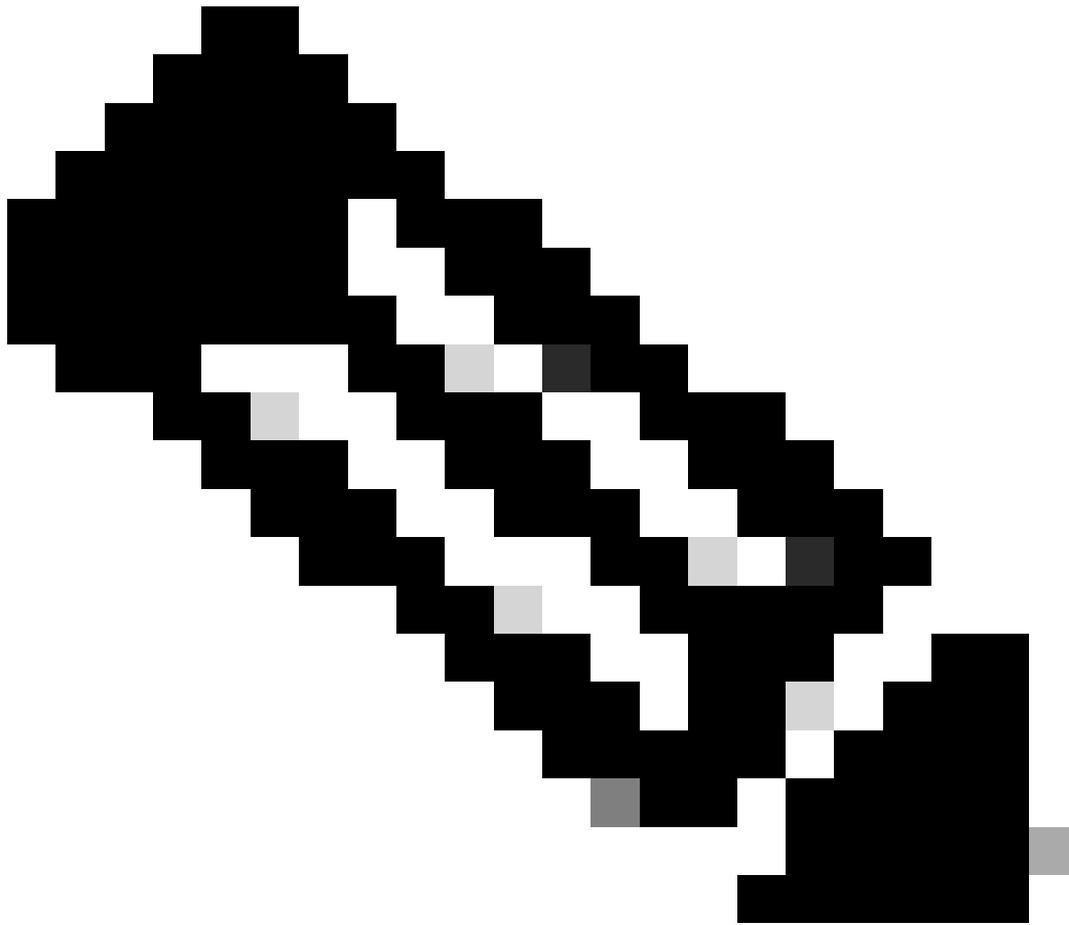
No

Yes

Configuration changes from primary peer will be 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:

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (0) Snort 3 (2)

Migrate | Deployment History

Search Device Add

Download Device List Report

Collaps All

Name

Ungrouped (2)

FTD-01 Snort 3  
10.88.171.87 - Routed

FTD-02 Snort 3  
10.88.171.89 - Routed

Access Control Policy Auto RollBack

Base-ACP

Base-ACP

**Add High Availability Pair**

**High Availability Link**

Interface: Ethernet1/5

Logical Name: FA-LINK

Primary IP: 10.10.10.1

Use IPv6 Address

Secondary IP: 10.10.10.2

Subnet Mask: 255.255.255.252

**State Link**

Interface: Same as LAN Failover Link

Logical Name: FA-LINK

Primary IP: 10.10.10.1

Use IPv6 Address

Secondary IP: 10.10.10.2

Subnet Mask: 255.255.255.252

**IPsec Encryption**

Enabled

Key Generation: Auto

LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

Cancel Add

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

FTD-HA  
High Availability

FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	↻	⋮
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	↻	⋮



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.