

# Atualizar HA do FTD Gerenciado pelo FDM

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Informações de Apoio](#)

[Configurar](#)

[Etapa 1. Carregar Pacote de Atualização](#)

[Etapa 2. Verificar Preparação](#)

[Etapa 3. Atualizar o FTD no HA](#)

[Etapa 4. Alternar Peer Ativo \(Opcional\)](#)

[Etapa 5. Implantação Final](#)

[Validar](#)

---

## Introdução

Este documento descreve o processo de atualização de um Cisco Secure Firewall Threat Defense em alta disponibilidade gerenciado por um gerenciador de dispositivos Firepower.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Conceitos e configuração de alta disponibilidade (HA)
- Configuração do Cisco Secure Firepower Device Manager (FDM)
- Configuração do Cisco Secure Firewall Threat Defense (FTD)

### Componentes Utilizados

As informações neste documento são baseadas no Virtual Cisco FTD, versão 7.2.8.

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.

### Overview

A maneira como o FDM funciona é atualizar um item de mesmo nível por vez. Primeiro, o Standby e, em seguida, o Ative, realizando um failover antes que o upgrade Ative seja iniciado.

## Informações de Apoio

O pacote de atualização deve ser baixado de [software.cisco.com](https://software.cisco.com) antes da atualização.

Em clish de CLI, execute o comando `show high-availability config` no FTD Ativo para verificar o status do HA.

```
> show high-availability config
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
```

```
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 3 of 311 maximum
```

```
MAC Address Move Notification Interval not set
```

```
failover replication http
```

```
Version: Ours 9.18(3)53, Mate 9.18(3)53
```

```
Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C
```

```
Last Failover at: 11:57:26 UTC Oct 8 2024
```

```
    This host: Primary - Active
```

```
        Active time: 507441 (sec)
```

```
        slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys)
```

```
            Interface diagnostic (0.0.0.0): Normal (Waiting)
```

```
            Interface inside (192.168.45.1): Normal (Waiting)
```

```
            Interface outside (192.168.1.10): Normal (Waiting)
```

```
        slot 1: snort rev (1.0) status (up)
```

```
        slot 2: diskstatus rev (1.0) status (up)
```

```
    Other host: Secondary - Standby Ready
```

```
        Active time: 8 (sec)
```

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (0.0.0.0): Normal (Waiting)

Interface outside (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

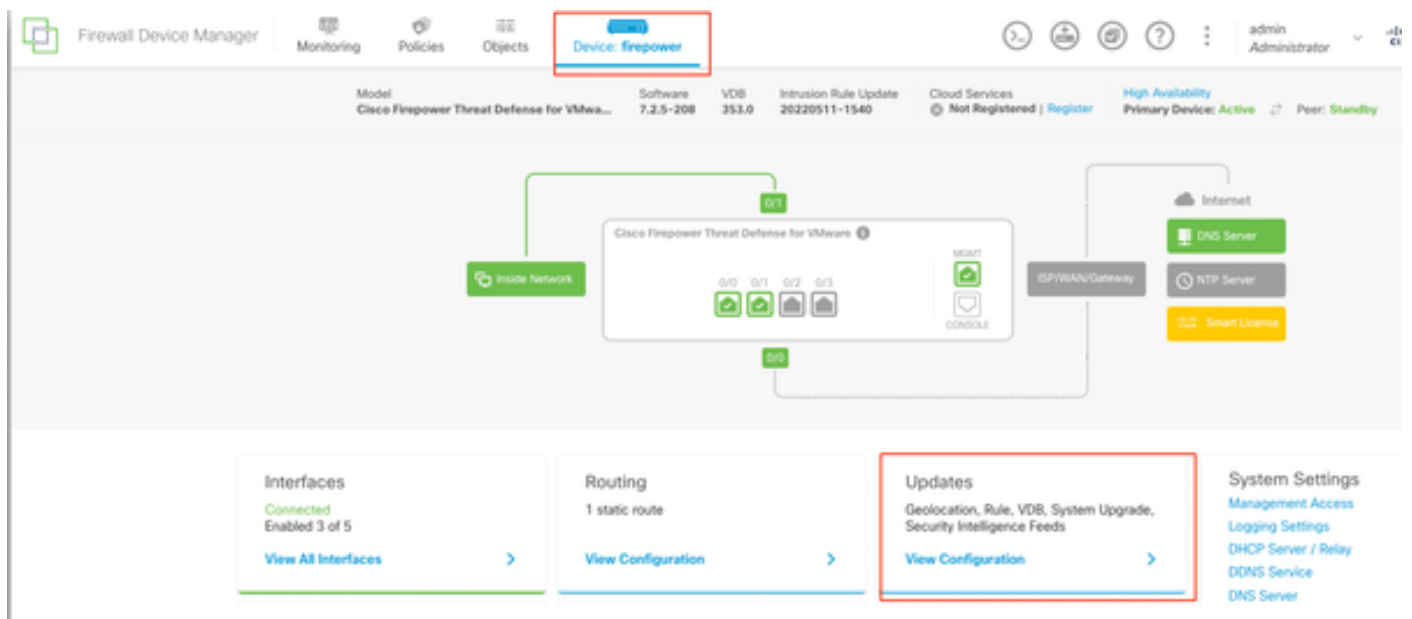
Se nenhum erro estiver visível, prossiga com a atualização.

## Configurar

### Etapa 1. Carregar Pacote de Atualização

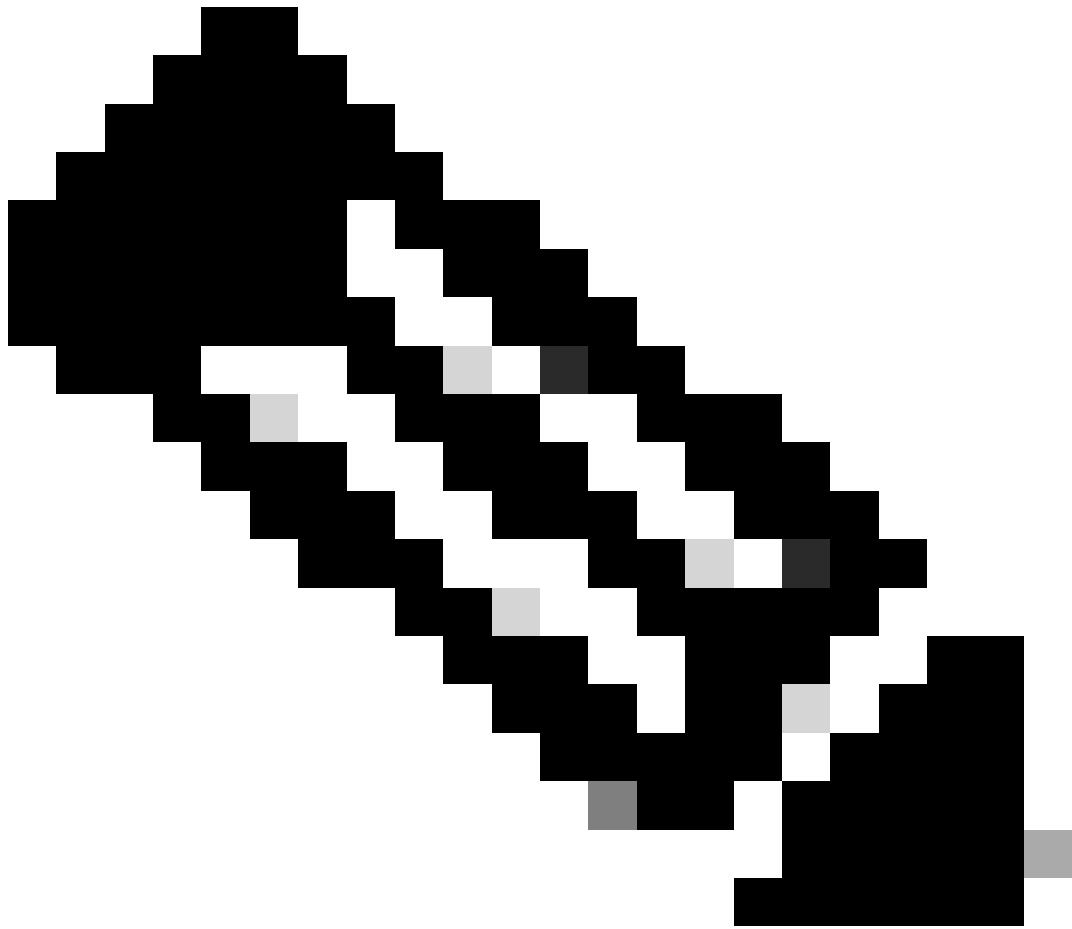
- Carregue o pacote de atualização do FTD no FDM usando a GUI.

Ele deve ser baixado anteriormente do site do software Cisco com base no modelo do FTD e na versão desejada. Navegue até Device > Updates > System Upgrade.



Atualizações

- Procure a imagem baixada anteriormente e escolha Carregar.



Note: Carregue a imagem nos nós ativo e standby.

---

## System Upgrade

Current version 7.2.5-208

### Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

*There are no software upgrades available on the system.*

*Upload an upgrade file to install.*

BROWSE

Executar Verificação de Preparação

## Etapa 2. Verificar Preparação

As verificações de prontidão confirmam se os dispositivos estão prontos para continuar com a atualização.


- Escolha Executar Verificação de Preparação para Atualização.

## System Upgrade

Current version 7.2.5-208

### **i** Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco\_FTD\_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)  
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **Not Performed Yet** | [Run Upgrade Readiness Check](#)

**UPGRADE NOW**

**i** Reboot required

Executar Verificação de Preparação

## System Upgrade

Current version 7.2.5-208

### **i** Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco\_FTD\_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)  
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**


Readiness Check **Not Performed Yet** | [Run Upgrade Readiness Check](#)

**UPGRADE NOW**

**i** Reboot required


Executar verificação de preparação

**i Important**  
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco\_FTD\_Upgrade-7.2.8-25.sh.REL....**  [Replace file](#)  
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

---

Readiness Check  **Please Wait...**

**UPGRADE NOW** **i Reboot required**


Executar Verificação de Preparação

O andamento pode ser verificado navegando até System > Upgrade.

**System Upgrade**  
Current version 7.2.5-208

---

**i Important**  
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco\_FTD\_Upgrade-7.2.8-25.sh.REL....**  [Replace file](#)  
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

---

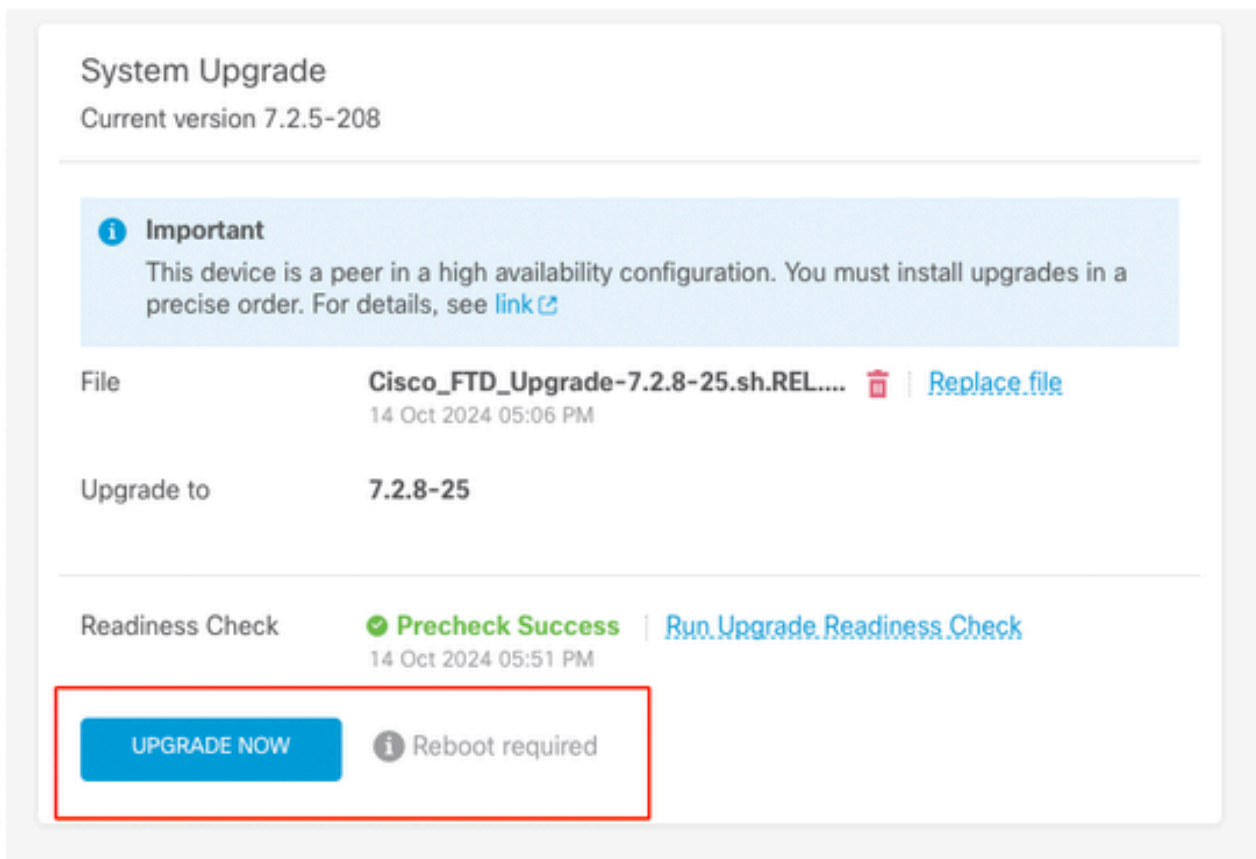
Readiness Check **✔ Precheck Success** [Run Upgrade Readiness Check](#)  
14 Oct 2024 05:51 PM

**UPGRADE NOW** **i Reboot required**

A atualização pode ser feita quando a verificação de preparação for concluída no FTD e o resultado for Êxito.

### Etapa 3. Atualizar o FTD no HA

- Escolha FDM em Espera e clique em Atualizar Agora.



The screenshot shows the 'System Upgrade' page for a device with the current version 7.2.5-208. It features an 'Important' warning box stating that the device is a peer in a high availability configuration and that upgrades must be installed in a precise order. Below this, there is a file entry for 'Cisco\_FTD\_Upgrade-7.2.8-25.sh.REL....' with a 'Replace file' link. The 'Upgrade to' version is '7.2.8-25'. A 'Readiness Check' section shows a 'Precheck Success' status with a 'Run Upgrade Readiness Check' link. At the bottom, a red box highlights a blue 'UPGRADE NOW' button and a 'Reboot required' notification.

Atualizar agora

Antes de iniciar a atualização:

1. Não inicie uma restauração do sistema ao mesmo tempo que uma atualização do sistema.
2. Não reinicialize o sistema durante a atualização. O sistema reinicializa automaticamente no momento apropriado durante a atualização, se uma reinicialização for necessária.
3. Não desligue o dispositivo durante a atualização. Interromper a atualização pode tornar o sistema inutilizável.

Você será desconectado do sistema quando a atualização for iniciada.

Após a conclusão da instalação, o dispositivo é reinicializado.



## Confirm System Upgrade



Before starting the upgrade:

1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. **Do not power off the device** during the upgrade. Interrupting the upgrade can leave the system in an unusable state.

You will be logged out of the system when the upgrade begins.  
After the installation completes, the device will be rebooted.

### UPGRADE OPTIONS

- Automatically cancel on upgrade failure and roll back to the previous version

CANCEL

CONTINUE

Continuar



Note: A atualização leva cerca de 20 min por FTD.

---

Na CLI, o progresso pode ser verificado na pasta de atualização /ngfw/var/log/sf; mova para o modo expert e acesso enterroot.

```
> expert
```

```
admin@firepower:~$ sudo su
```

```
Password:
```

```
root@firepower:/home/admin# cd /ngfw/var/log/sf
```

```
root@firepower:/ngfw/var/log/sf# ls
```

```
Cisco_FTD_Upgrade-7.2.8.
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self.
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm.
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf
```

```
ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst
```

```
ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com
```

```
ui: Upgrade complete
```

```
ui: The system will now reboot.
```

```
ui: System will now reboot.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024):
```

```
System will reboot in 5 seconds due to system upgrade.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024):
```

```
System will reboot now due to system upgrade.
```

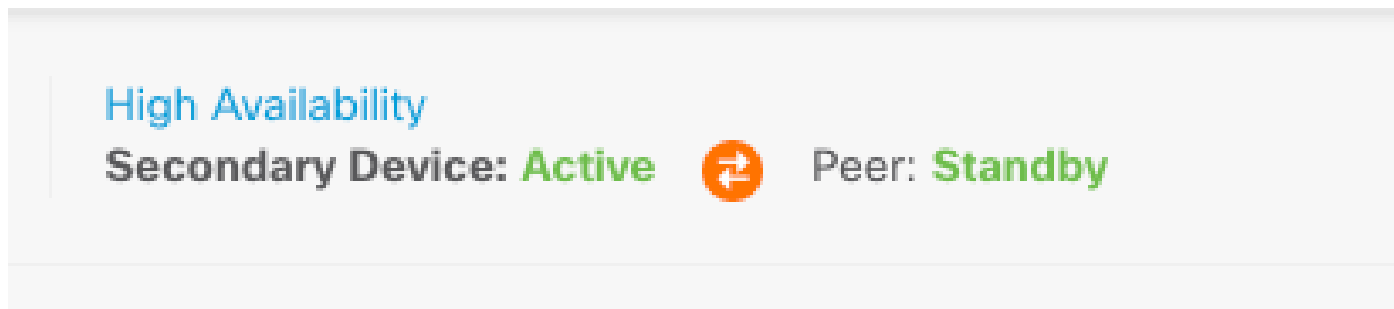
```
Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024):
```

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

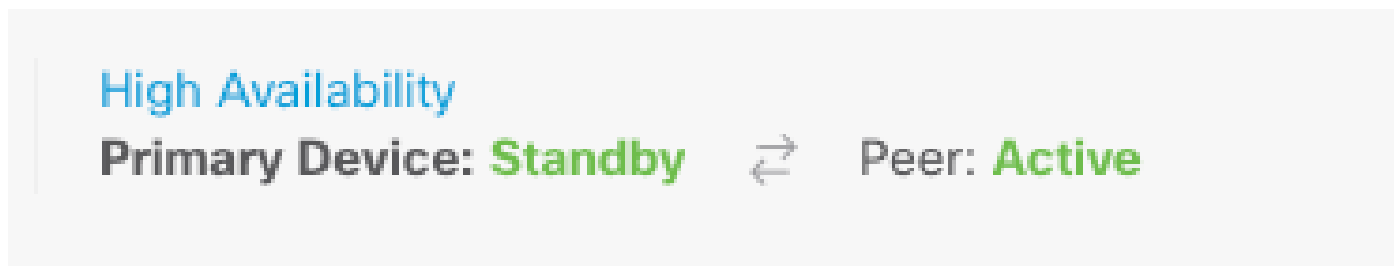
Atualize a segunda unidade.

Alternar funções para tornar este dispositivo ativo: Selecione Device> High Availability e, em seguida, selecione Switch Mode no menu de engrenagens. Aguarde o status da unidade para mudar para ativo e confirme se o tráfego está fluindo normalmente. Em seguida, faça logoff.

Atualização: Repita as etapas anteriores para fazer login no novo standby, carregar o pacote, atualizar o dispositivo, monitorar o progresso e verificar o sucesso.



Alta Disponibilidade



Alta Disponibilidade

Na CLI, vá para LINA (system support diagnostic-cli) e verifique o estado de failover no FTD de standby usando o comando show failover state.

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
primary_ha> enable
```

```
Password:
```

```
primary_ha# show failover state
```

	State	Last Failure Reason	Date/Time
This host	-	Primary	

```
Standby Ready None
Other host - Secondary
Active None
```

```
====Configuration State====
```

```
Sync Skipped - STANDBY
```

```
====Communication State====
```

```
Mac set
```

```
primary_ha#
```

#### Etapa 4. Alternar Peer Ativo (Opcional)



Note: Se o dispositivo secundário estiver Ativo, ele não terá nenhum impacto operacional.

---

Ter o dispositivo primário como ativo e secundário como em espera é uma prática recomendada que ajuda a rastrear qualquer failover que possa ocorrer.

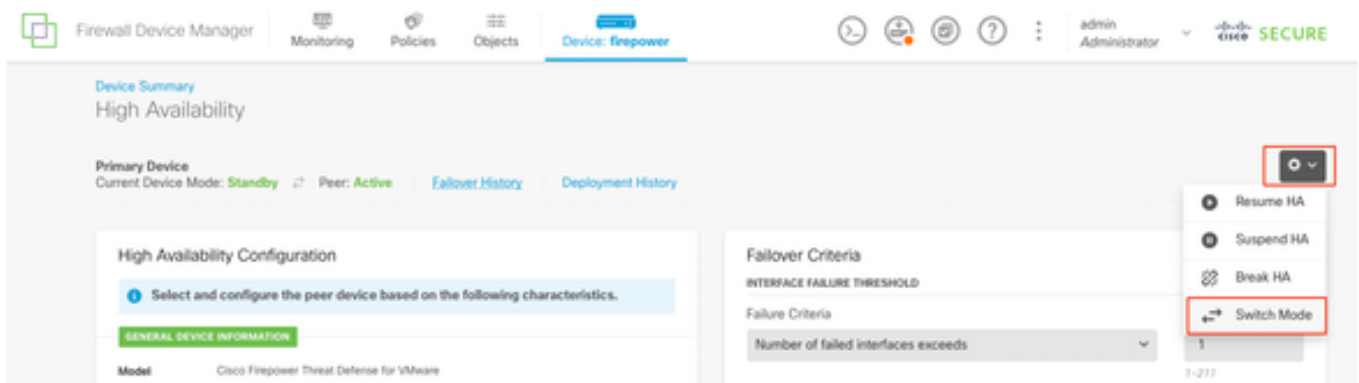
Nesse caso, o FTD Ativo agora está em Espera, um failover manual pode ser usado para redefini-lo como Ativo.

- Navegue até Devices > High Availability.



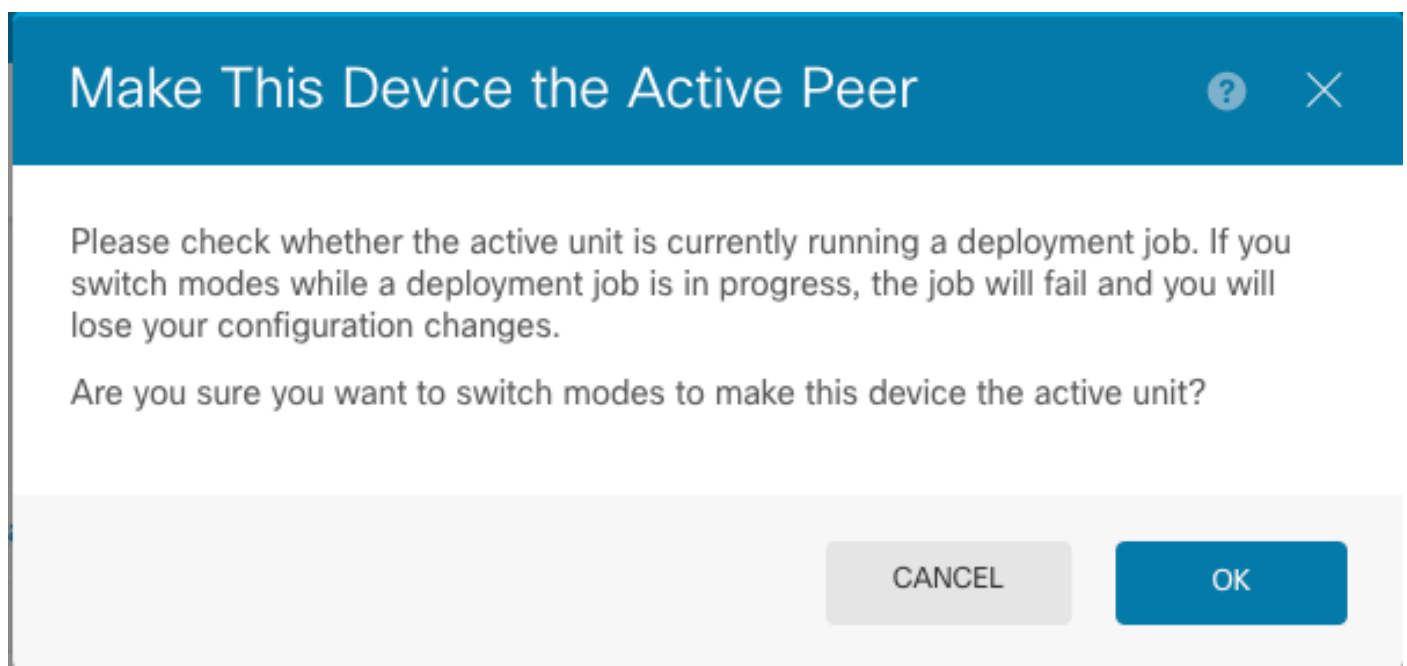
Alta Disponibilidade

- Escolha Alternar modo.



Modo de comutação

- Escolha OK para confirmar o failover.



Par Ativo

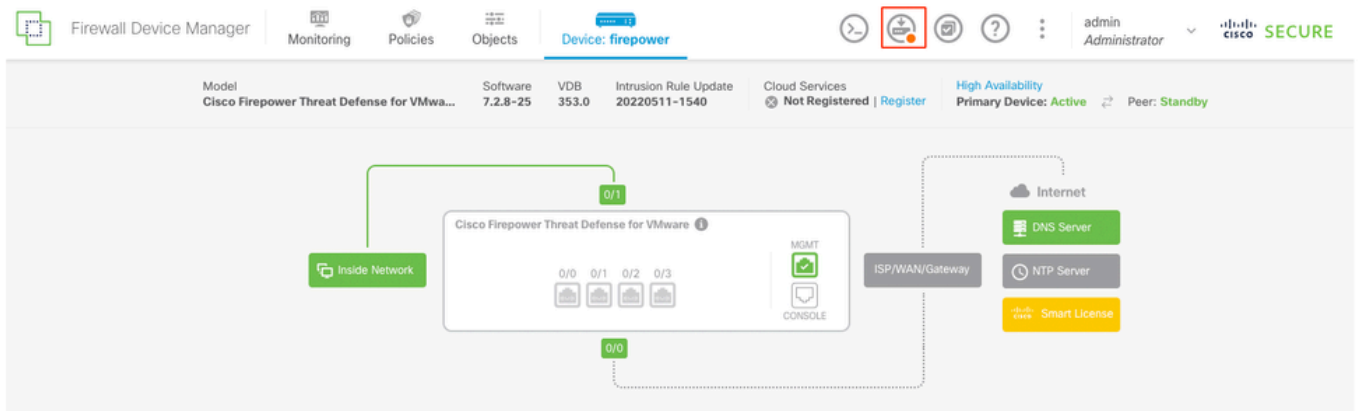
Validação do status de alta disponibilidade ao final da atualização e failover concluída.



Dispositivos

## Etapa 5. Implantação Final

- Implante a política nos dispositivos clicando em **IMPLANTAR AGORA** na guia Implantação.





## Pending Changes



✓ **Last Deployment Completed Successfully**  
14 Oct 2024 06:26 PM. [See Deployment History](#)

Deployed Version (14 Oct 2024 06:26 PM)	Pending Version	LEGEND
<b>Rule Update Version Edited: 20220511-1540</b>		
lastSuccessSRUDate: 2024-10-08 06:15:04Z	2024-10-14 12:53:26Z	
-	lspVersions[1]: 20220511-1540	
<b>VDB Version Edited: 353</b>		
<b>+ Snort Version Added: 3.1.21.800-2</b>		
-	snortVersion: 3.1.21.800-2	
-	snortPackage: /ngfw/var/sf/snort-3.1.21.800-2/snor...	
-	name: 3.1.21.800-2	
<b>Data SSL Cipher Setting Edited: DefaultDataSSLCipherSetting</b>		
<b>SSL Cipher Edited: DefaultSSLCipher</b>		
-	protocolVersions[0]: TLSV1	
-	protocolVersions[1]: DTLSV1	
-	protocolVersions[2]: TLSV1_1	
<b>Intrusion Policy Edited: Security Over Connectivity - Cisco Talos</b>		
<b>Intrusion Policy Edited: Maximum Detection - Cisco Talos</b>		
MORE ACTIONS ▾	CANCEL	DEPLOY NOW ▾

Implantação de política

## Validar

Para validar se o status do HA e a atualização foram concluídos, você deve confirmar o status:

Preliminar: Ativo

Secundário: Pronto para espera

Ambos estão na versão que foi alterada recentemente (7.2.8 neste exemplo).



## Failover

- Em cliques de CLI, verifique o estado de failover usando os comandos `show failover state` and `show failover para` obter informações mais detalhadas.

Sistema operacional extensível Cisco Firepower (FX-OS) v2.12.1 (build 73)

Defesa contra ameaças do Cisco Firepower para VMware v7.2.8 (compilação 25)

```
> show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	None	

```
====Configuration State====
```

```
    Sync Skipped
```

```
====Communication State====
```

```
    Mac set
```

```
> show failover
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(4)210, Mate 9.18(4)210

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

Last Failover at: 14:13:56 UTC Oct 15 2024

This host: Primary - Active

Active time: 580 (sec)

slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (192.168.45.1): Normal (Waiting)

Interface outside (192.168.1.10): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Other host: Secondary - Standby Ready

Active time: 91512 (sec)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (0.0.0.0): Normal (Waiting)

Interface outside (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

#### Stateful Failover Logical Update Statistics

Link : failover-link GigabitEthernet0/2 (up)

Stateful Obj	xmit	xerr	rcv	rerr
General	11797	0	76877	0

sys cmd	11574	0	11484	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	176	0	60506	0
ARP tbl	45	0	4561	0
Xlate_Timeout	0	0	0	0
IPv6 ND tbl	0	0	0	0
VPN IKEv1 SA	0	0	0	0
VPN IKEv1 P2	0	0	0	0
VPN IKEv2 SA	0	0	0	0
VPN IKEv2 P2	0	0	0	0
VPN CTCP upd	0	0	0	0
VPN SDI upd	0	0	0	0
VPN DHCP upd	0	0	0	0
SIP Session	0	0	0	0
SIP Tx	0	0	0	0
SIP Pinhole	0	0	0	0
Route Session	1	0	0	0
Router ID	0	0	0	0
User-Identity	0	0	30	0
CTS SGTNAME	0	0	0	0
CTS PAC	0	0	0	0
TrustSec-SXP	0	0	0	0
IPv6 Route	0	0	0	0
STS Table	0	0	0	0
Umbrella Device-ID	0	0	0	0
Rule DB B-Sync	0	0	30	0
Rule DB P-Sync	1	0	266	0
Rule DB Delete	0	0	0	0

#### Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	31	123591
Xmit Q:	0	1	12100

Se ambos os FTDs estiverem na mesma versão e o status do HA estiver íntegro, a atualização será concluída.

## 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.