Actualización de FTD HA gestionada por FDM

Contenido

Introducción

Este documento describe el proceso de actualización para Cisco Secure Firewall Threat Defense en alta disponibilidad administrado por un administrador de dispositivos Firepower.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Conceptos y configuración de alta disponibilidad (HA)
- Configuración de Cisco Secure Firepower Device Manager (FDM)
- Configuración de Cisco Secure Firewall Threat Defence (FTD)

Componentes Utilizados

La información de este documento se basa en Virtual Cisco FTD, versión 7.2.8.

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.

Overview

El funcionamiento de FDM consiste en actualizar un par cada vez. Primero el Standby, luego el Active, haciendo una conmutación por fallas antes de que se inicie la actualización Active.

Antecedentes

El paquete de actualización se debe descargar de software.cisco.com antes de la actualización.

En el clish de CLI, ejecute el comando show high-availability config en el FTD activo para verificar el estado del 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)
```

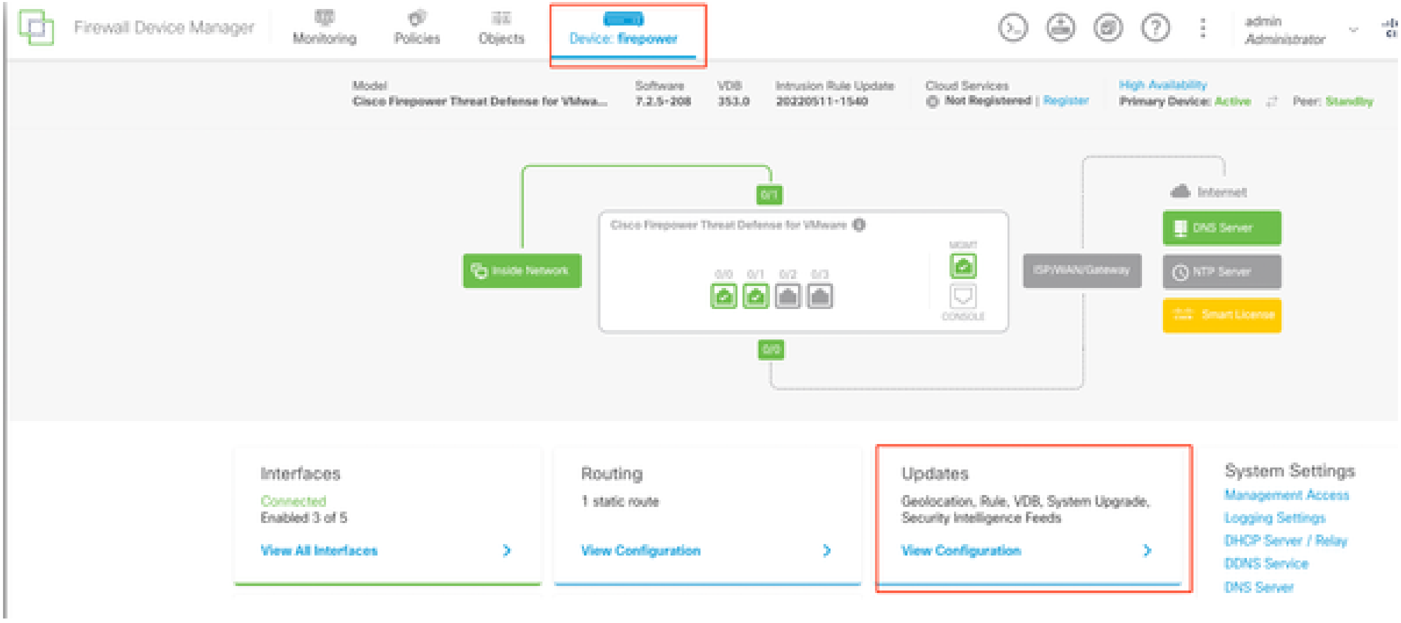
Si no hay errores visibles, continúe con la actualización.

Configurar

Paso 1. Cargar paquete de actualización

- Cargue el paquete de actualización de FTD en FDM mediante la GUI.

Esto debe descargarse previamente del sitio de software de Cisco en función del modelo de FTD y de la versión deseada. Vaya a Device > Updates > System Upgrade.



Model: Cisco Firepower Threat Defense for VMwa...
Software: 7.2.5-208
VDB: 353.0
Intrusion Rule Update: 20220511-1540
Cloud Services: Not Registered | Register
High Availability: Primary Device: Active Peer: Standby

Interfaces
Connected
Enabled 3 of 5
View All Interfaces

Routing
1 static route
View Configuration

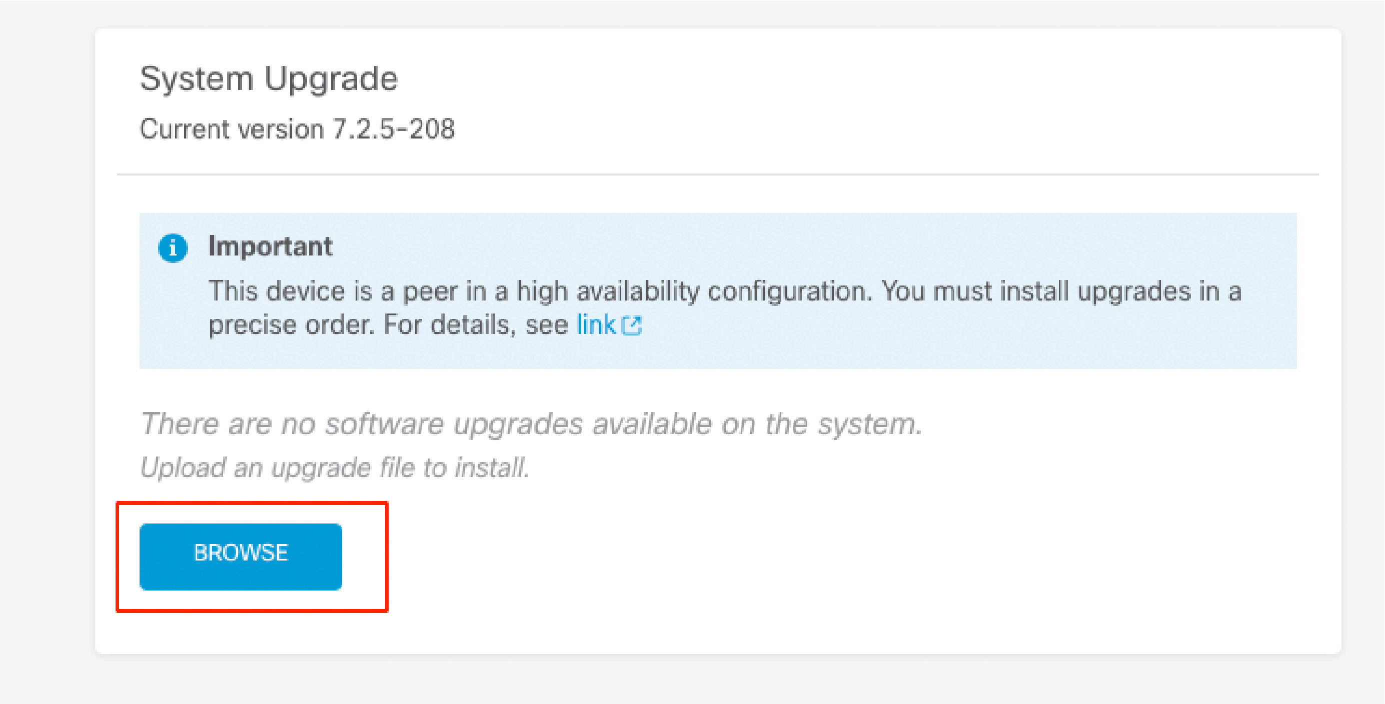
Updates
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds
View Configuration

System Settings
Management Access
Logging Settings
DHCP Server / Relay
DDNS Service
DNS Server

Actualizaciones

- Busque la imagen descargada anteriormente y, a continuación, elijaCargar.

Nota: Cargue la imagen en los nodos activos y en espera.



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.

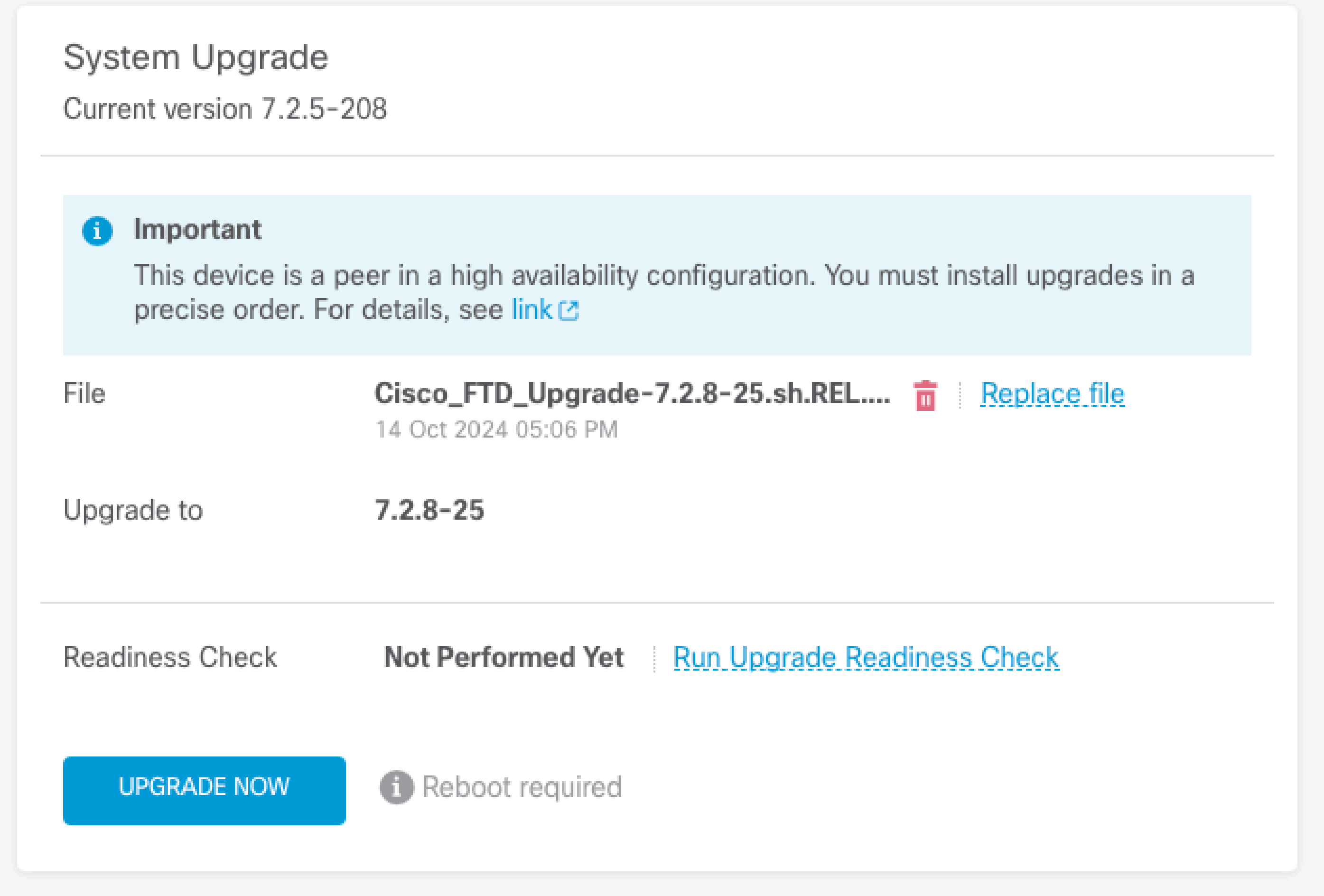
Upload an upgrade file to install.

Ejecutar comprobación de preparación

Paso 2. Comprobar la preparación

Las comprobaciones de preparación confirman si los dispositivos están preparados para continuar con la actualización.

- Elija Run Upgrade Readiness Check.



System Upgrade

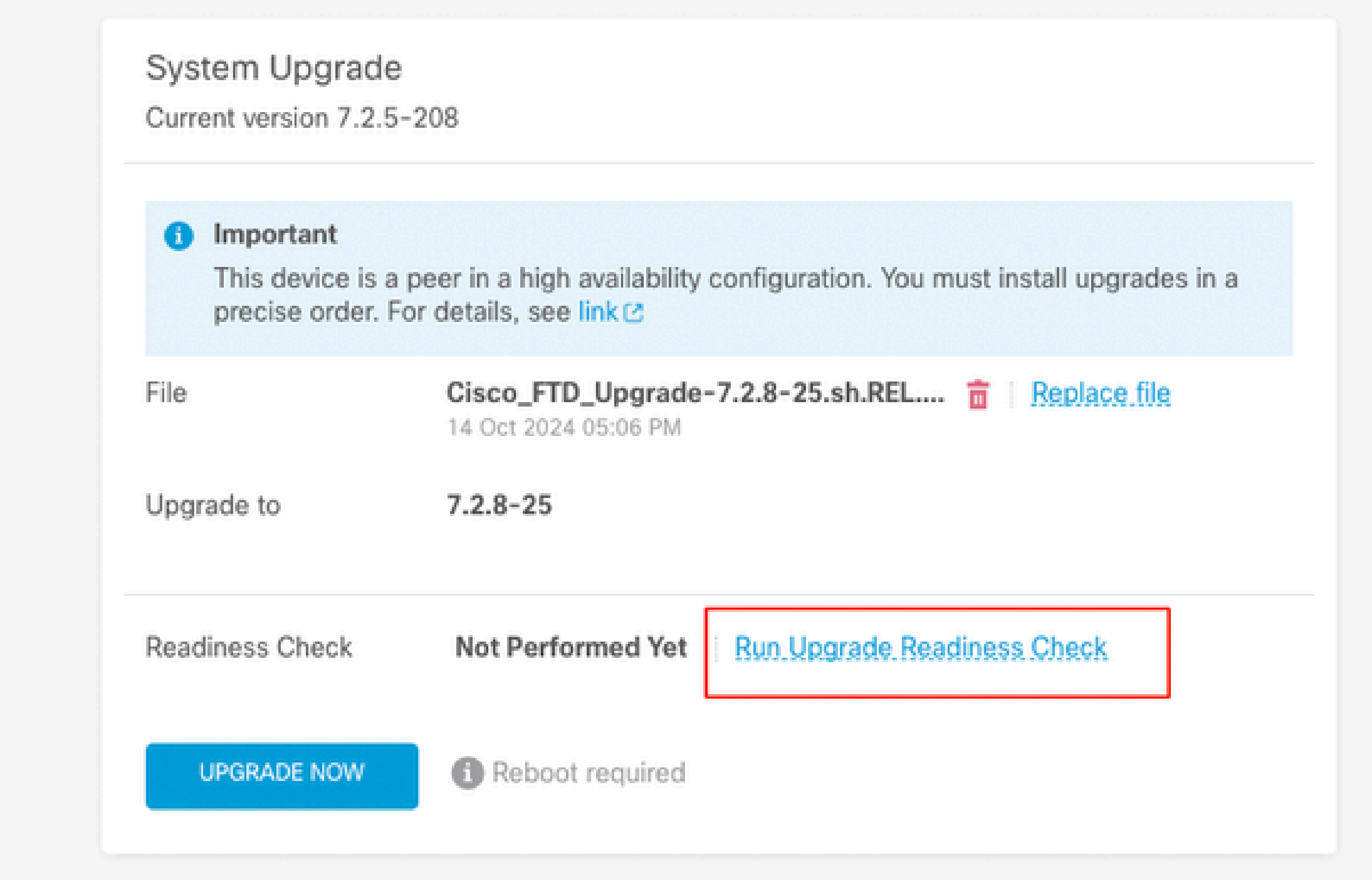
Current version 7.2.5-208

Important

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

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

Ejecutar comprobación de preparación



System Upgrade

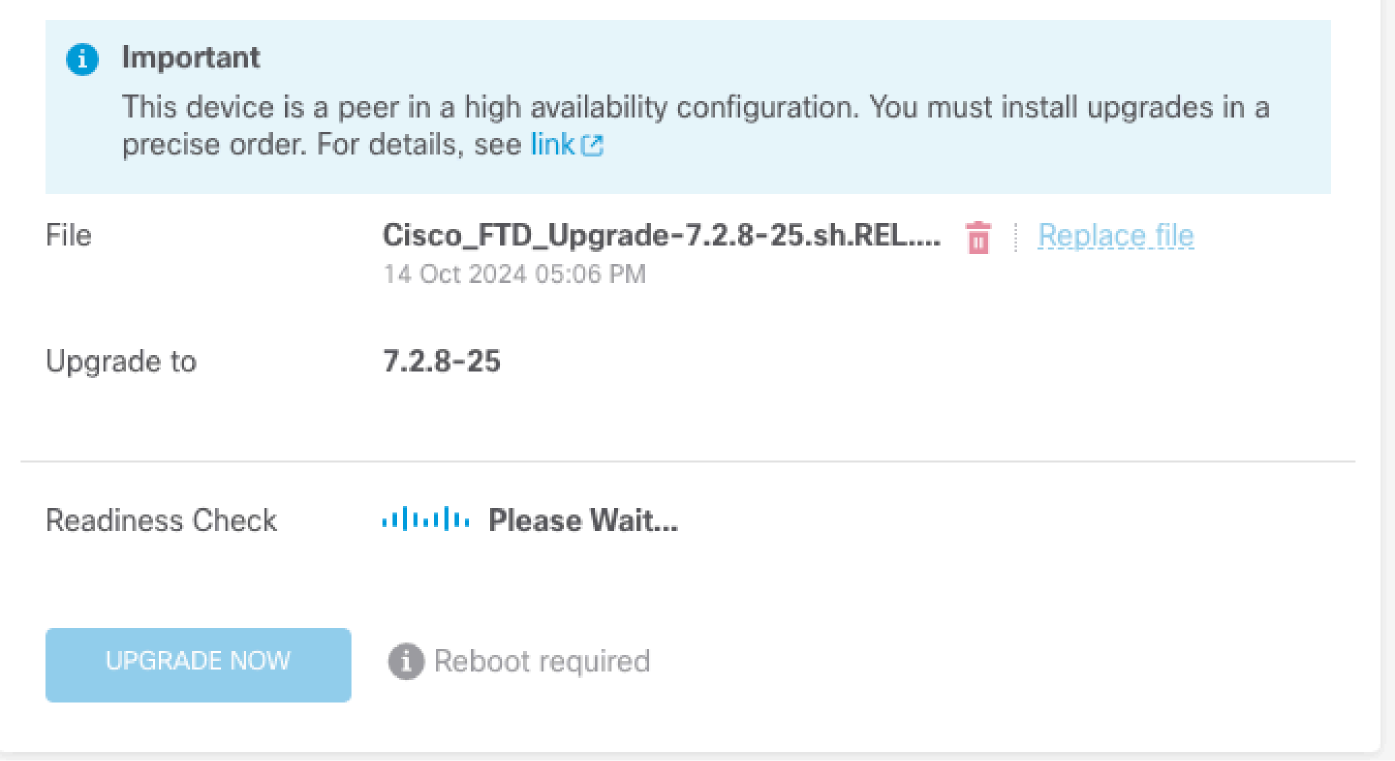
Current version 7.2.5-208

Important

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

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

Comprobación de preparación de ejecución



Important

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

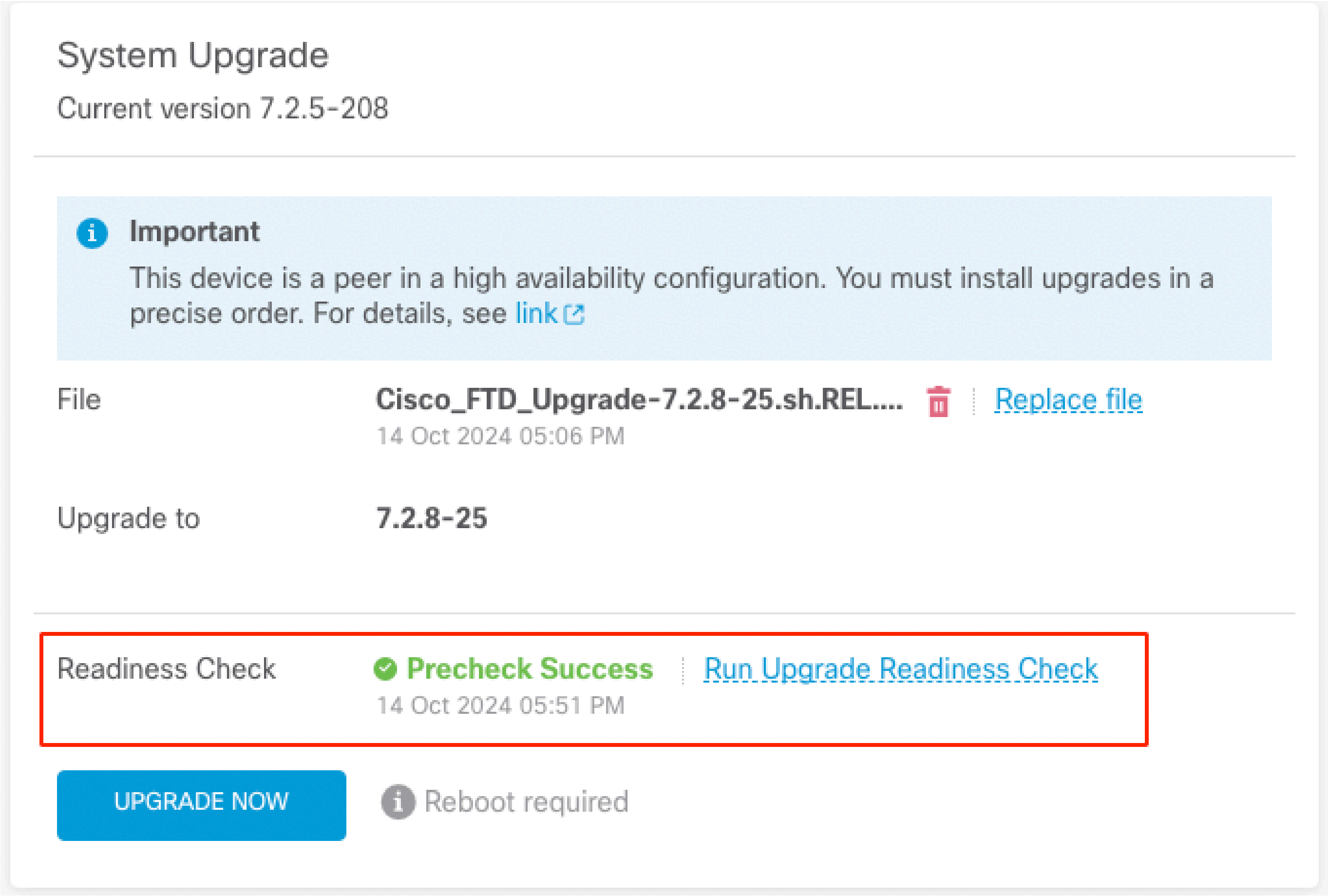
File: **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....** | Replace file
14 Oct 2024 05:06 PM

Upgrade to: **7.2.8-25**

Readiness Check: **Please Wait...**

Ejecutar comprobación de preparación

El progreso se puede verificar navegando hasta System > Upgrade.



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

File: **Cisco_FTD_Upgrade-7.2.8-25.sh.REL....** | Replace file
14 Oct 2024 05:06 PM

Upgrade to: **7.2.8-25**

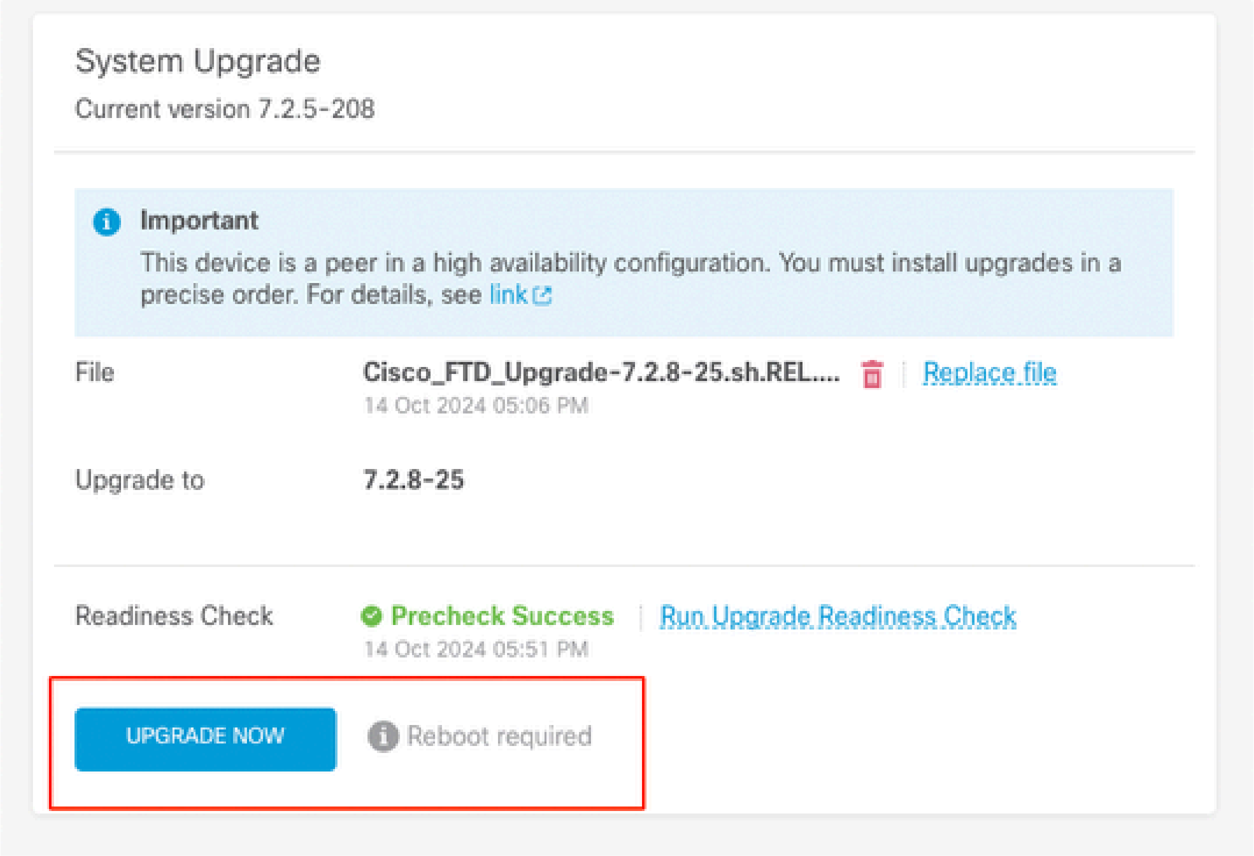
Readiness Check: ✓ **Precheck Success** | Run Upgrade Readiness Check
14 Oct 2024 05:51 PM

Ejecutar comprobación de preparación

La actualización se puede realizar cuando la comprobación de preparación se haya completado en ambos FTD y el resultado sea Correcto.

Paso 3. Actualización del FTD en HA

- Elija Standby FDM y haga clic en Upgrade Now.



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

File: Cisco_FTD_Upgrade-7.2.8-25.sh.REL.... | Replace file
14 Oct 2024 05:06 PM

Upgrade to: 7.2.8-25

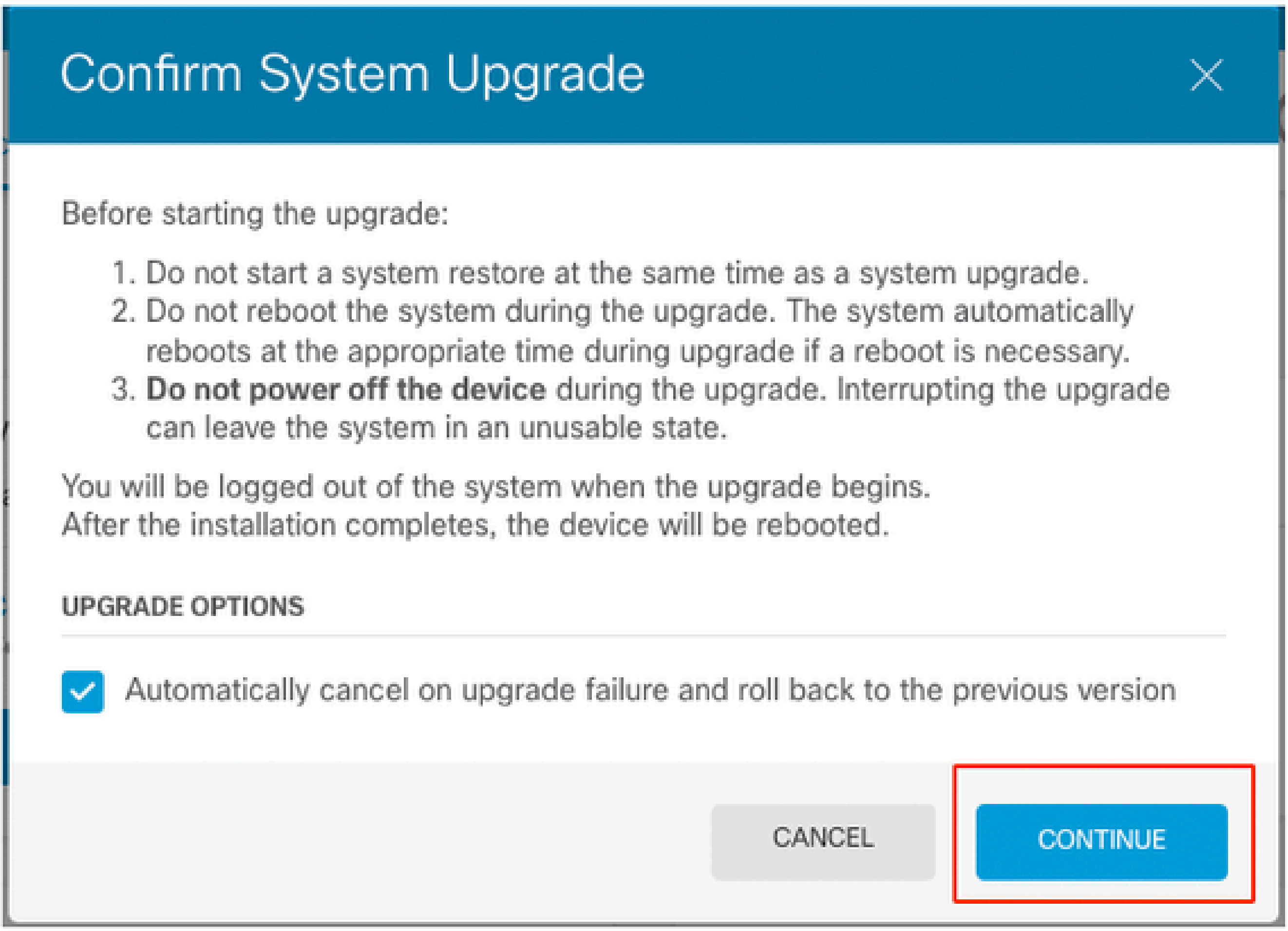
Readiness Check: Precheck Success | Run Upgrade Readiness Check
14 Oct 2024 05:51 PM

Actualice ahora

Antes de iniciar la actualización:

1. No inicie una restauración del sistema al mismo tiempo que una actualización del sistema.
2. No reinicie el sistema durante la actualización. El sistema se reinicia automáticamente en el momento adecuado durante la actualización, si es necesario reiniciar.
3. No apague el dispositivo durante la actualización. Si interrumpe la actualización, el sistema puede quedar inutilizable.

Se cerrará su sesión en el sistema cuando comience la actualización.
Una vez finalizada la instalación, el dispositivo se reinicia.



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

Continúe

Nota: La actualización tarda aproximadamente 20 minutos por FTD.

En CLI, el progreso se puede verificar en la carpeta de actualización /ngfw/var/log/sf; pase al modo experto y acceda a enterroot.

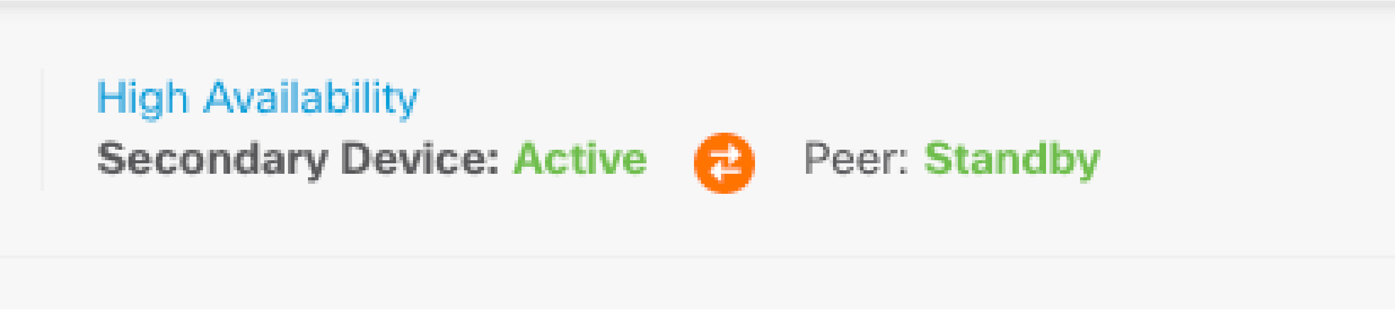
```
> expert

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!
```

Actualice la segunda unidad.

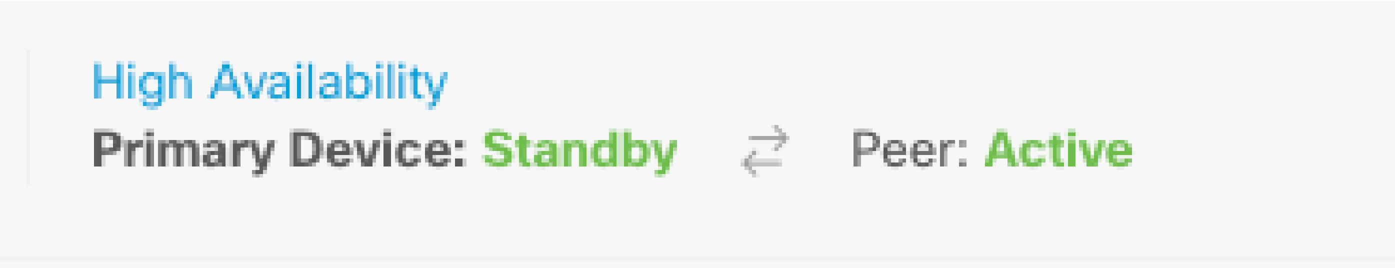
Cambie de función para activar este dispositivo: Elija Device> High Availability y, a continuación, elija Switch Mode en el menú de engranajes. Espere a que el estado de la unidad cambie a activo y confirme que el tráfico fluye normalmente. A continuación, desconéctese.

Actualizar: Repita los pasos anteriores para iniciar sesión en el nuevo modo de espera, cargar el paquete, actualizar el dispositivo, supervisar el progreso y verificar el éxito.


High Availability

Secondary Device: Active ⇄ Peer: Standby

Alta disponibilidad


High Availability

Primary Device: Standby ⇄ Peer: Active

Alta disponibilidad

En CLI, vaya a LINA (system support diagnostic-cli) y verifique el estado de failover en el FTD en espera mediante el 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#
```

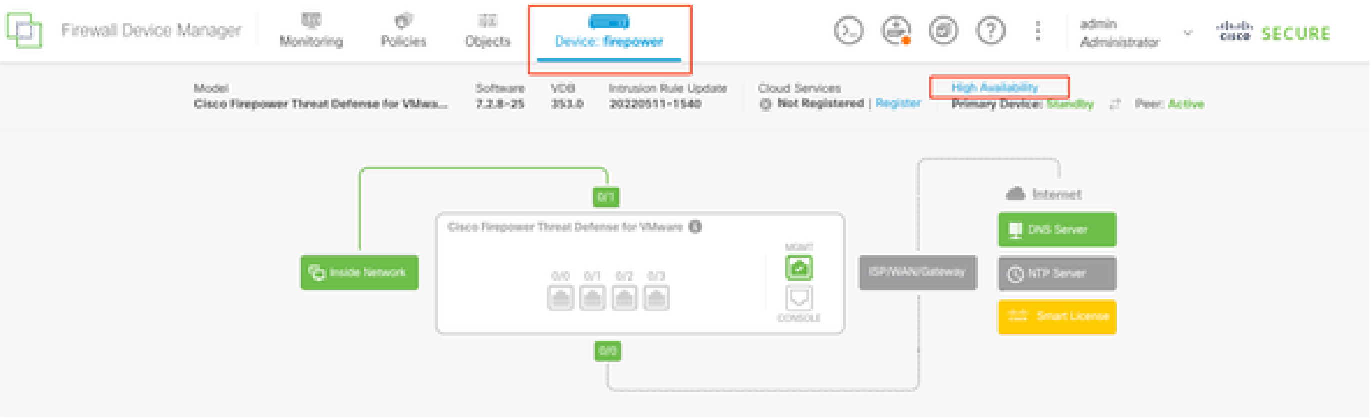
Paso 4. Switch Par Activo (Opcional)

Nota: Si el dispositivo secundario está activo, no tiene ningún impacto operativo.

Tener el dispositivo principal como activo y secundario como en espera es una práctica recomendada que ayuda a realizar un seguimiento de cualquier fallo que se pueda producir.

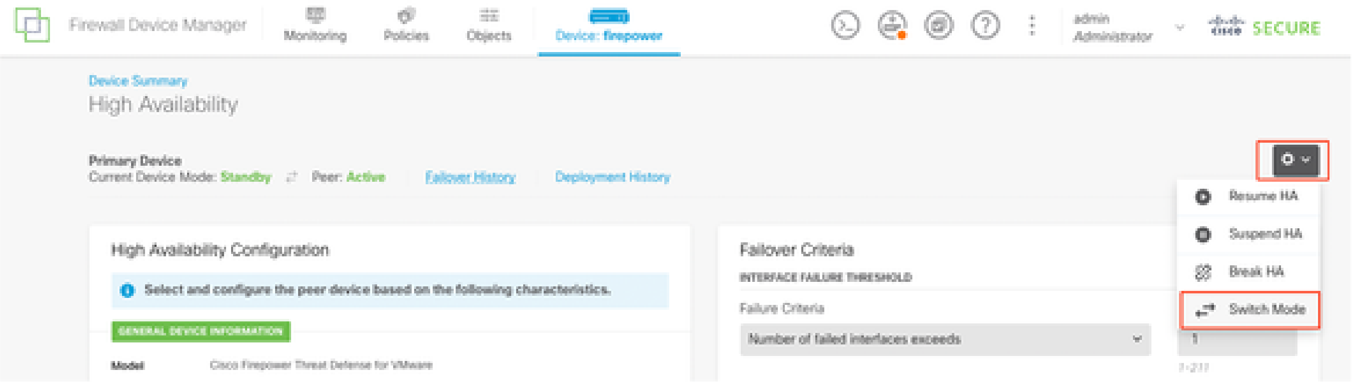
En este caso, el FTD activo está ahora en espera, se puede utilizar una conmutación por fallo manual para volver a activarlo.

- Vaya a Devices > High Availability.



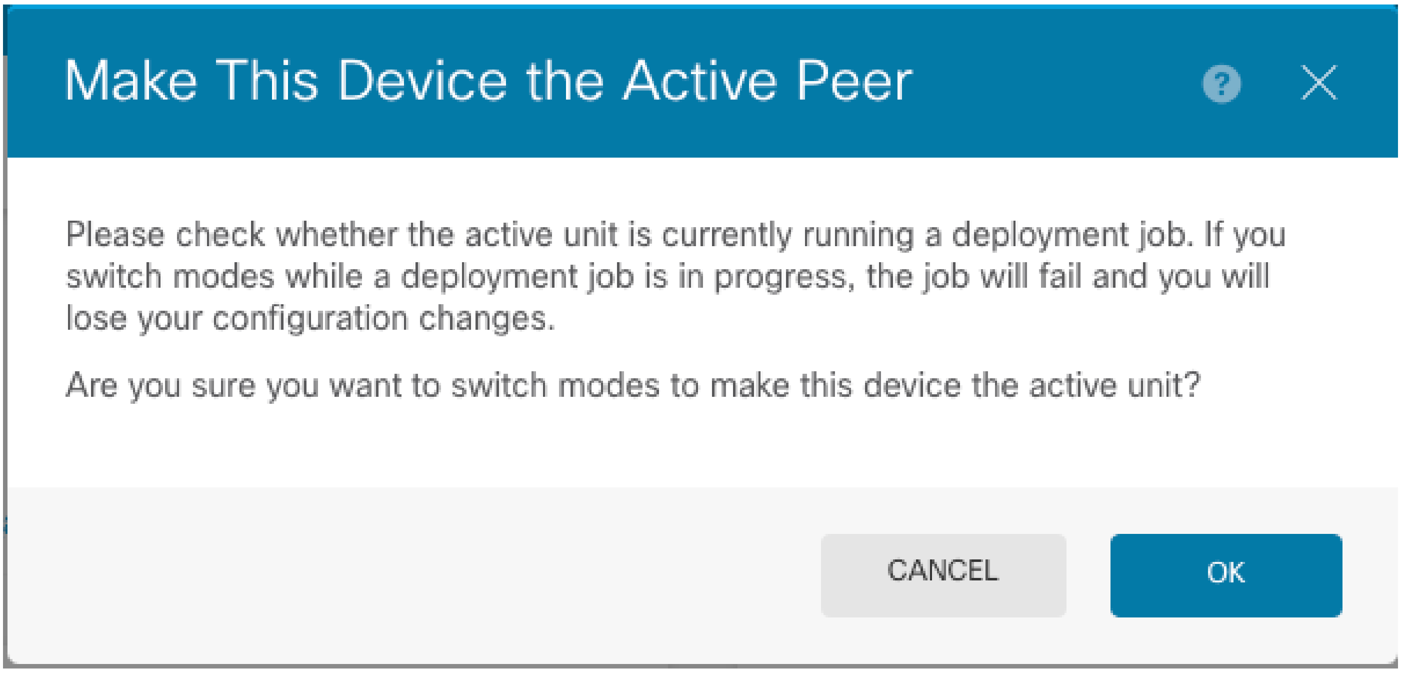
Alta disponibilidad

- Seleccione Modo de switch.


Firewall Device Manager
Monitoring
Policies
Objects
Device: firepower
admin
Administrator
SECURE
Device Summary
High Availability
Primary Device
Current Device Mode: Standby
Peer: Active
Failover History
Deployment History
Resume HA
Suspend HA
Break HA
Switch Mode
High Availability Configuration
Select and configure the peer device based on the following characteristics.
GENERAL DEVICE INFORMATION
Model
Cisco Firepower Threat Defense for VMware
Failover Criteria
INTERFACE FAILURE THRESHOLD
Failure Criteria
Number of failed interfaces exceeds
1
1-211

Modo de switch

- Elija OK para confirmar el failover.



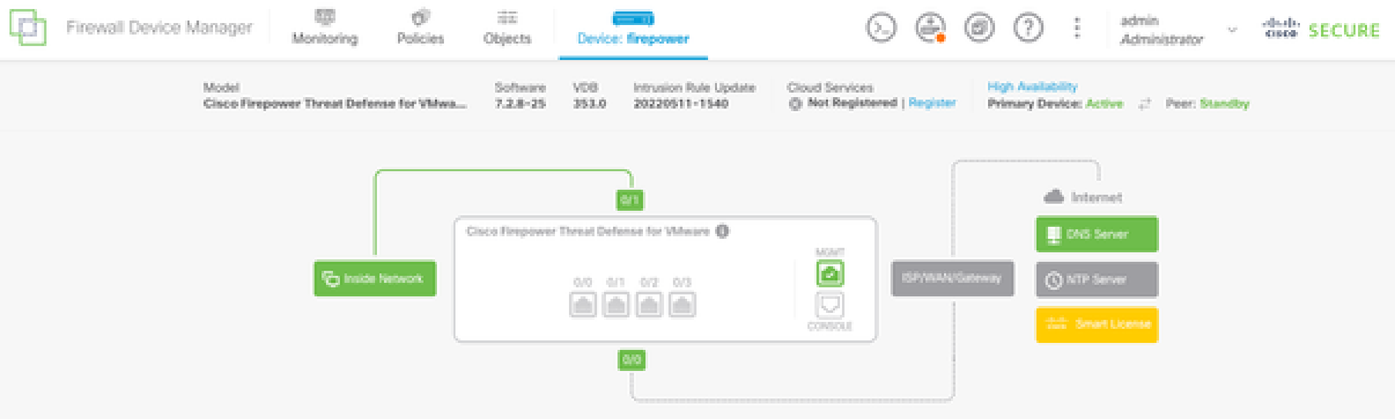
Make This Device the Active Peer

Please check whether the active unit is currently running a deployment job. If you switch modes while a deployment job is in progress, the job will fail and you will lose your configuration changes.

Are you sure you want to switch modes to make this device the active unit?

Peer activo

Validación del estado de HA al final de la actualización y conmutación por fallo realizada.



Model
Cisco Firepower Threat Defense for VMwa...

Software
7.2.8-25

VDB
353.0

Intrusion Rule Update
20220511-1540

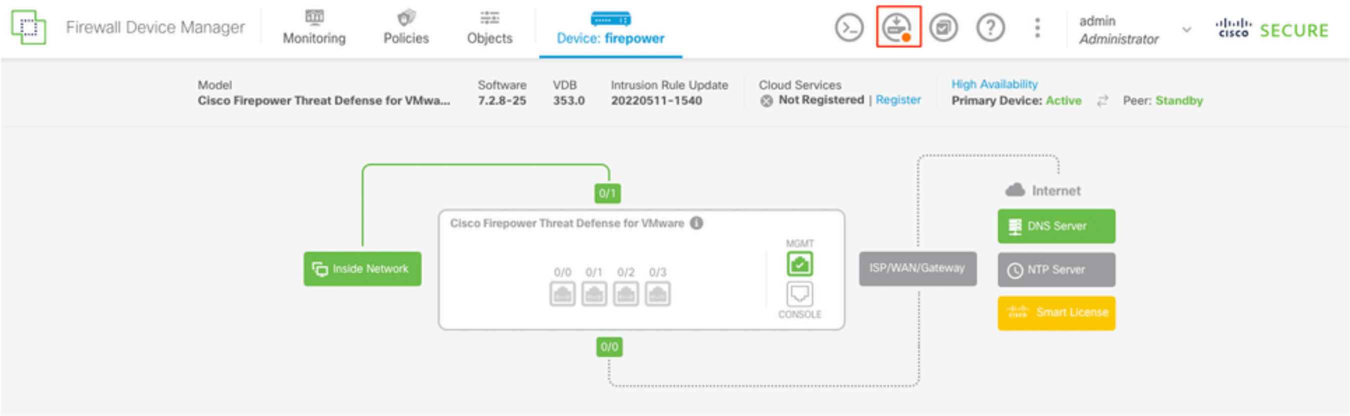
Cloud Services
Not Registered | Register

High Availability
Primary Device: Active ⇄ Peer: Standby

Dispositivos

Paso 5. Implementación final

- Implemente la política en los dispositivos haciendo clic en IMPLEMENTAR AHORA en la pestaña Implementación.



Model
Cisco Firepower Threat Defense for VMwa...

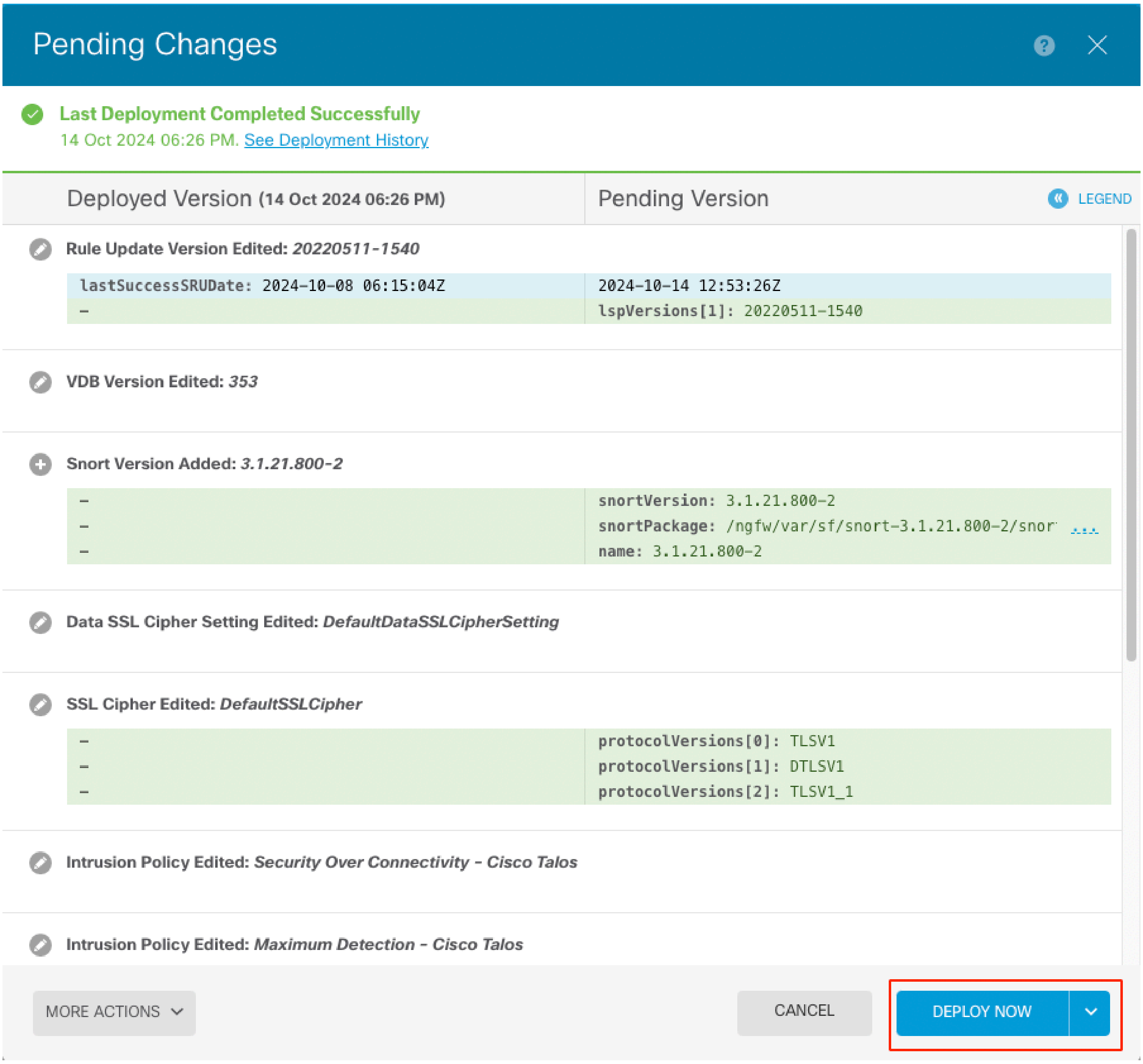
Software
7.2.8-25

VDB
353.0

Intrusion Rule Update
20220511-1540

Cloud Services
Not Registered | Register

High Availability
Primary Device: Active ⇄ Peer: Standby



Pending Changes

Last Deployment Completed Successfully
14 Oct 2024 06:26 PM. See Deployment History

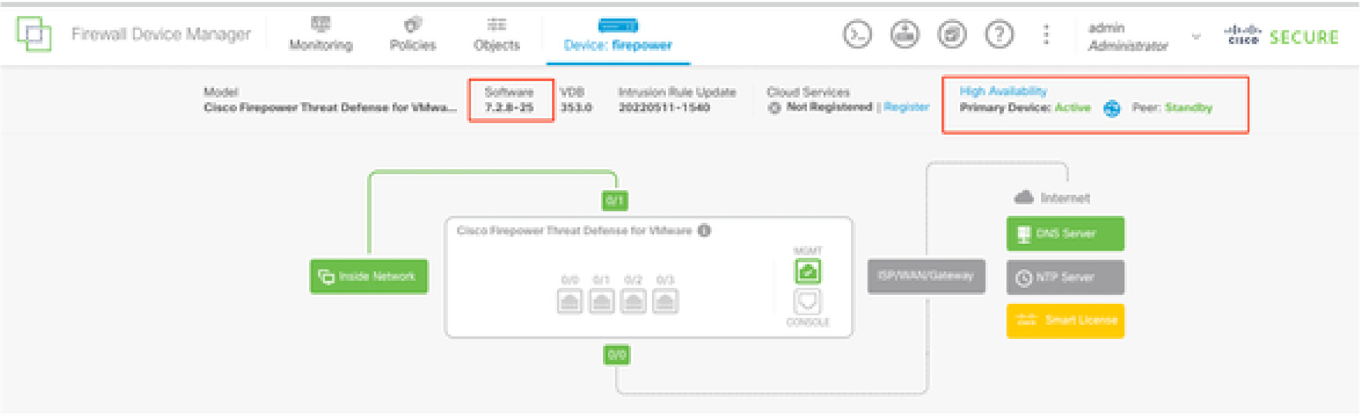
Deployed Version (14 Oct 2024 06:26 PM)	Pending Version
Rule Update Version Edited: *20220511-1540*	
lastSuccessSRUDate: 2024-10-08 06:15:04Z	2024-10-14 12:53:26Z
-	lspVersions[1]: 20220511-1540
VDB Version Edited: *353*	
Snort Version Added: *3.1.21.800-2*	
-	snortVersion: 3.1.21.800-2
-	snortPackage: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

Implementación de políticas

Validar

Para validar que el estado de HA y la actualización han finalizado, debe confirmar el estado:
Principal: Activo
Secundario: Preparado para espera

Ambos se encuentran en la versión que es la que se ha cambiado recientemente (7.2.8 en este ejemplo).



Model
Cisco Firepower Threat Defense for VMwa...

Software
7.2.8-25

VDB
353.0

Intrusion Rule Update
20220511-1540

Cloud Services
Not Registered | Register

High Availability
Primary Device: Active   Peer: Standby

Failover

- Durante el clish de CLI, verifique el estado de failover usando los comandos show failover stateand show failover para obtener información más detallada.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.1 (versión 73)
Cisco Firepower Threat Defense para VMware v7.2.8 (compilación 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
```

Si ambos FTD están en la misma versión y el estado de HA es correcto, la actualización ha finalizado.

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).