Configuración de la reversión en SFTD cuando SFMC no es accesible

Contenido

Introducción

Este documento describe cómo revertir un cambio de implementación de Secure SFMC que afecta la conectividad a SFTD.

Prerequisites

Requirements

El uso de esta función es compatible con la versión 6.7 o posterior de Secure FirePOWER Threat Detection®.

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Secure Firewall Management Center (SFMC®)
- Configuración de Cisco Secure FirePOWER Threat Defence (SFTD)

Componentes Utilizados

- Secure Firewall Management Center para VMware versión 7.2.1
- Firepower Threat Defense seguro para VMware versión 7.2

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.

Antecedentes

Existen situaciones en las que la comunicación con SFMC, SFTD o entre SFMC y SFTD se pierde cuando un cambio en la implementación afecta a la conectividad de la red. Puede revertir la configuración del SFTD a la última configuración implementada para restaurar la conectividad de administración.

Utilice el comando configure policy rollback para revertir la configuración de la defensa contra amenazas a la última configuración implementada.

Nota: El comando configure policy rollback se introdujo en la versión 6.7

Consulte las directrices:

- Solo la implementación anterior está disponible localmente en Threat Defence; no puede volver a implementaciones anteriores.
- Se admite la reversión para obtener una alta disponibilidad a partir de management center 7.2.
- No se admite la reversión en implementaciones de clústeres.
- La reversión sólo afecta a las configuraciones que se pueden establecer en el centro de administración. Por ejemplo, la reversión no afecta a ninguna configuración local relacionada con la interfaz de administración dedicada, que sólo puede configurar en la CLI de defensa contra amenazas. Tenga en cuenta que si ha cambiado la configuración de la interfaz de datos después de la última implementación del centro de administración mediante el comando configure network management-data-interface y, a continuación, utiliza el comando rollback, esa configuración no se conservará; se revertirá a la última configuración del centro de administración implementada.
- El modo UCAPL/CC no se puede deshacer.
- Los datos de certificados SCEP fuera de banda que se actualizaron durante la implementación anterior no se pueden revertir.
- Durante la reversión, las conexiones pueden interrumpirse porque se ha borrado la configuración actual.

Configurar

Diagrama de la red

En este documento, se utiliza esta configuración de red:

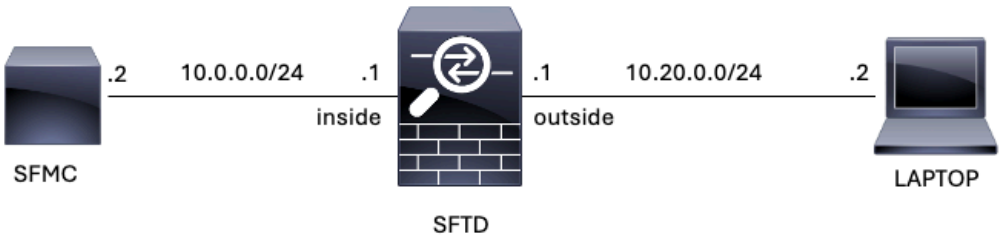


Imagen 1. Diagrama

Situación

En esta configuración, SFTD es administrado por el SFMC mediante la interfaz interna del firewall, hay una regla que permite la accesibilidad desde el portátil al SFMC.

Procedimiento

Paso 1. La regla denominada FMC-Access se deshabilitó en el SFMC. Después de la implementación, se bloquea la comunicación del portátil al SFMC.

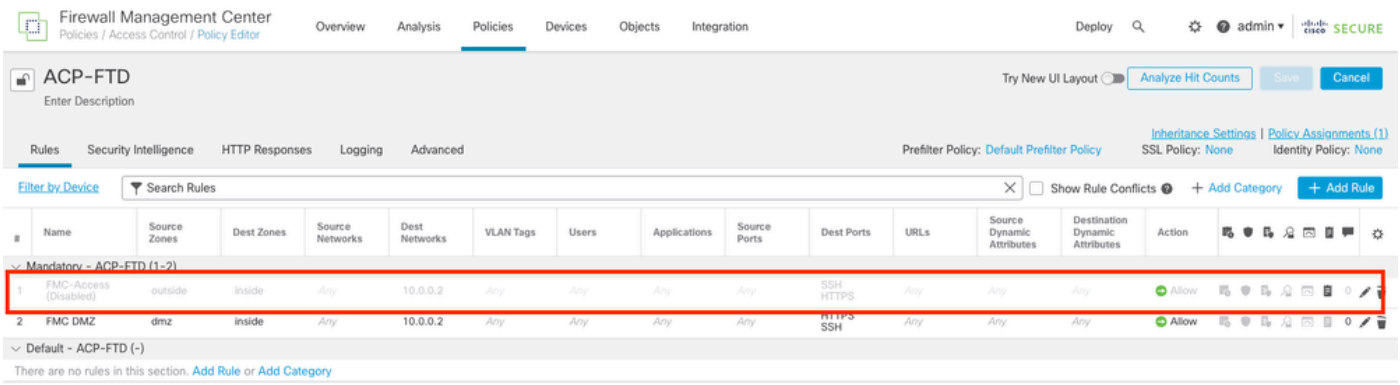


Imagen 2. Regla que permite deshabilitar la disponibilidad de SFMC

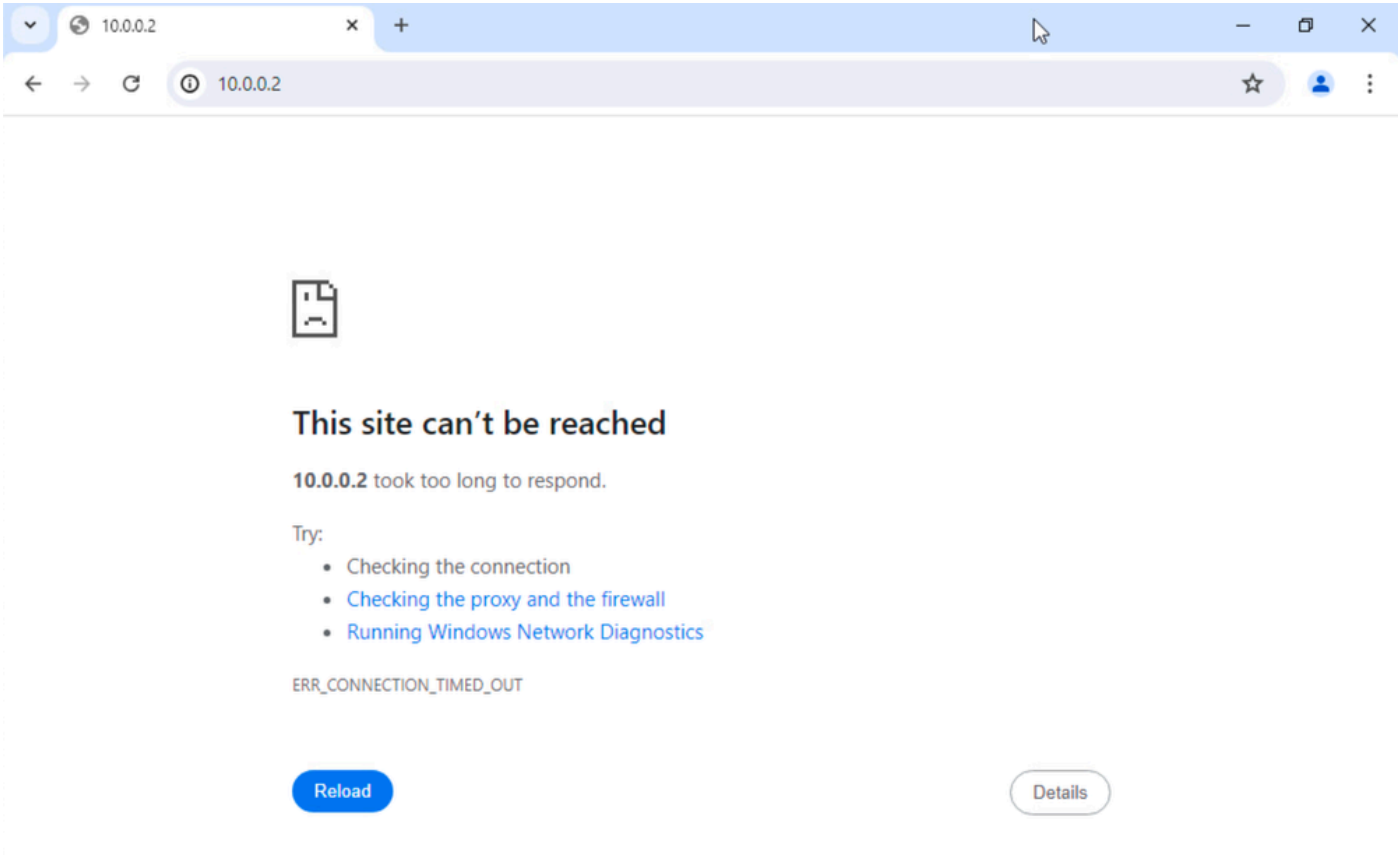


Imagen 3. Alcance de SFMC desde un portátil que no funciona

Paso 2. Inicie sesión en el SFTD a través de SSH o la consola, luego utilice el comando configure policy rollback.

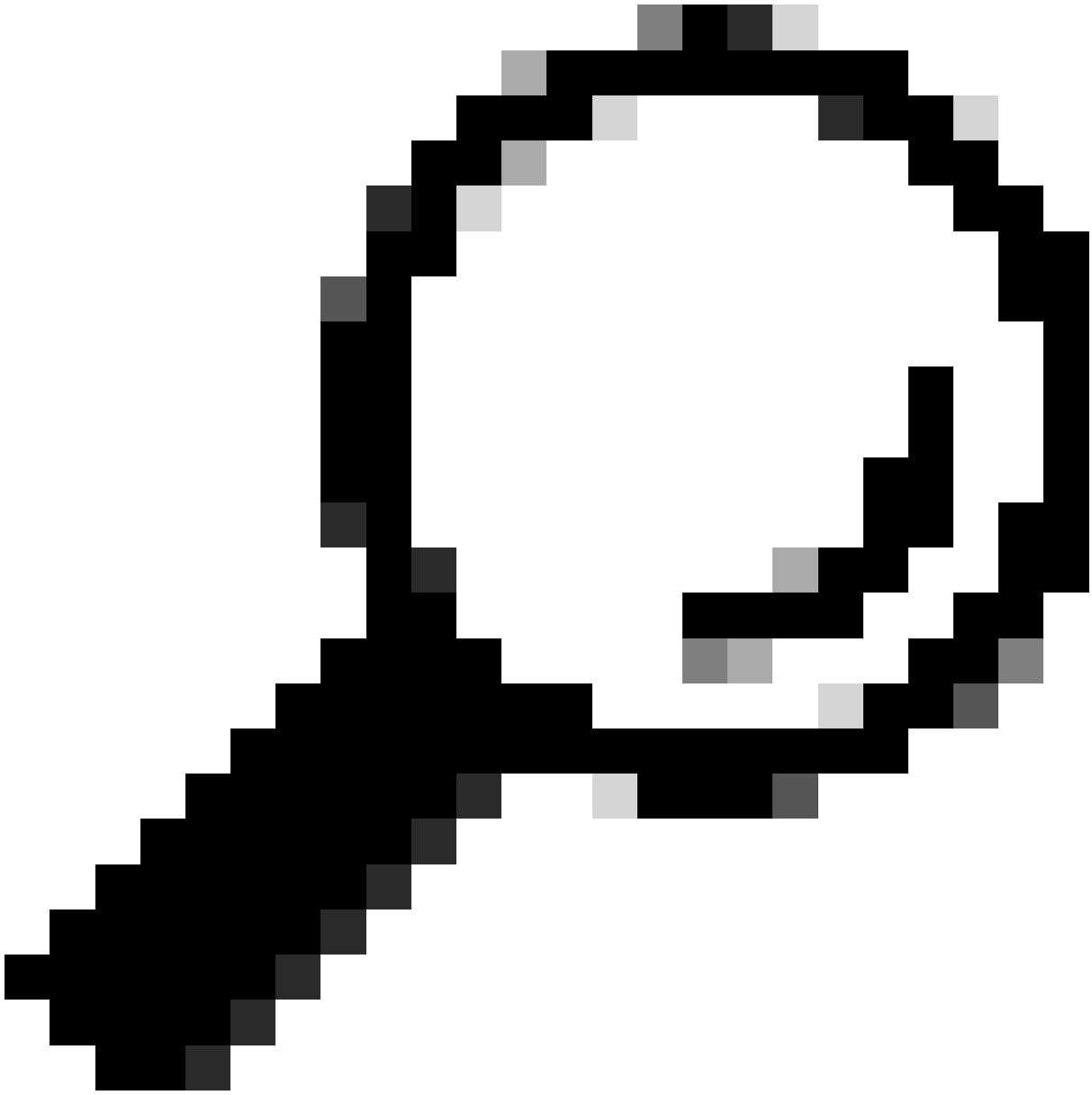
Nota: Si no es posible el acceso a través de SSH, conéctese a través de telnet.

```
<#root>

>

configure policy rollback


----------------------------------------------------------------------------------------------
[Warning] Perform a policy rollback if the FTD communicates with the FMC on a data interface, and it ha
and you want to perform a policy rollback for other purposes, then you should do the rollback on the FM

Checking Eligibility ....
============= DEVICE DETAILS =============
Device Version: 7.2.0
Device Type: FTD
Device Mode: Offbox
Device in HA: false
Device in Cluster: false
Device Upgrade InProgress: false
==========================================
Device is eligible for policy rollback

This command will rollback the policy to the last deployment done on Jul 15 20:38.
[Warning] The rollback operation will revert the convergence mode.
```

```
Do you want to continue (YES/NO)?
```

Paso 3. Escriba la palabra YES para confirmar la reversión de la última implementación y espere hasta que finalice el proceso de reversión.

```
<#root>

Do you want to continue (YES/NO)?

YES


Starting rollback...
 Deployment of Platform Settings to device.              Status: success
 Preparing policy configuration on the device.           Status: success
 Applying updated policy configuration on the device.    Status: success
 Applying Lina File Configuration on the device.         Status: success
INFO: Security level for "diagnostic"set to 0 by default.
 Applying Lina Configuration on the device.             Status: success
 Commit Lina Configuration.                             Status: success
 Commit Lina File Configuration.                        Status: success
 Finalizing policy configuration on the device.         Status: success

===============================================

POLICY ROLLBACK STATUS: SUCCESS


===============================================
```



Consejo: En caso de que la reversión falle, póngase en contacto con Cisco TAC

Paso 4. Después de la reversión, confirme la disponibilidad de SFMC. El SFTD notifica al SFMC que la reversión se ha completado correctamente. En SFMC, la pantalla de implementación muestra un banner que indica que la configuración se ha revertido.

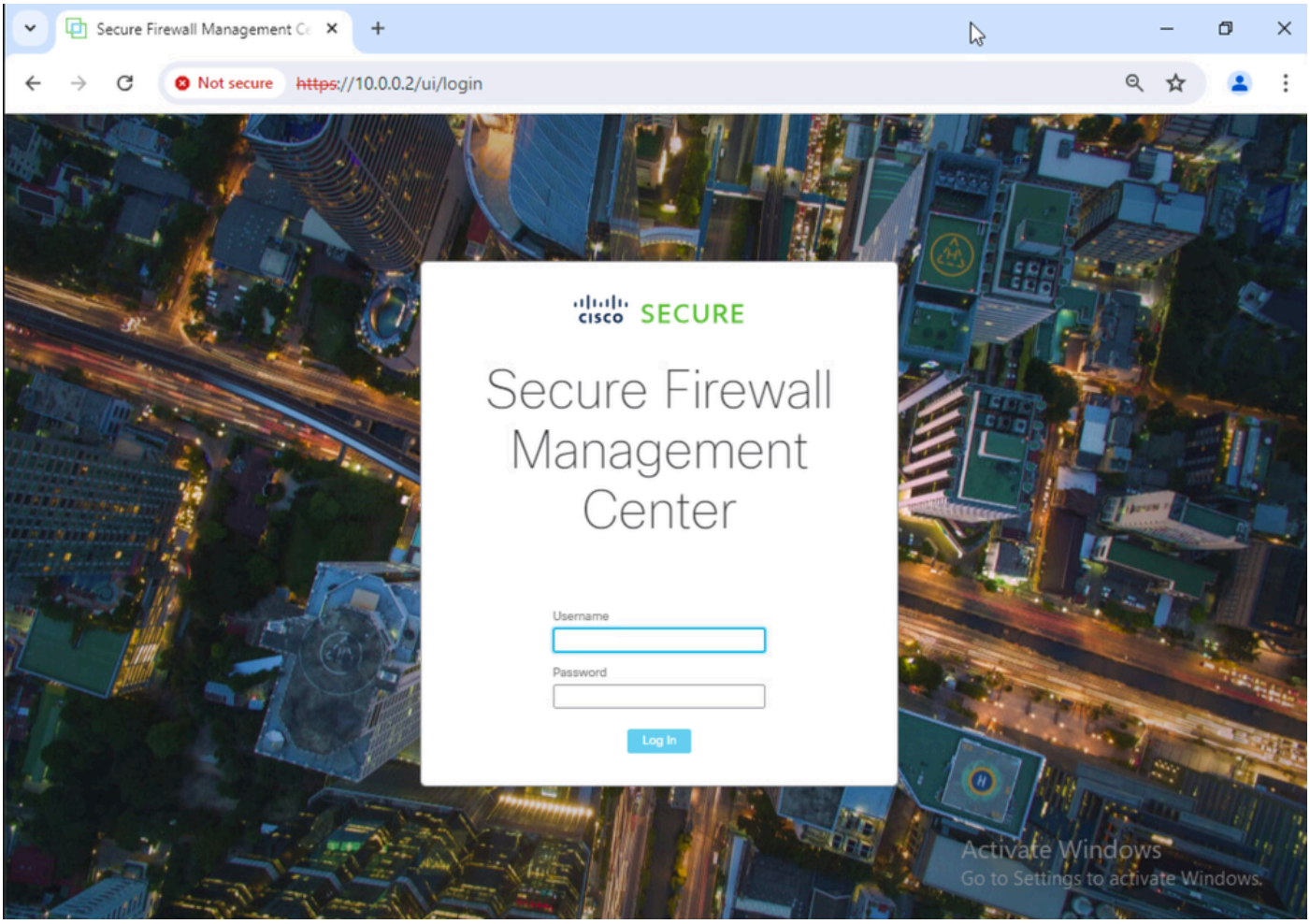


Imagen 4. SFMC Disponibilidad restaurada desde un ordenador portátil

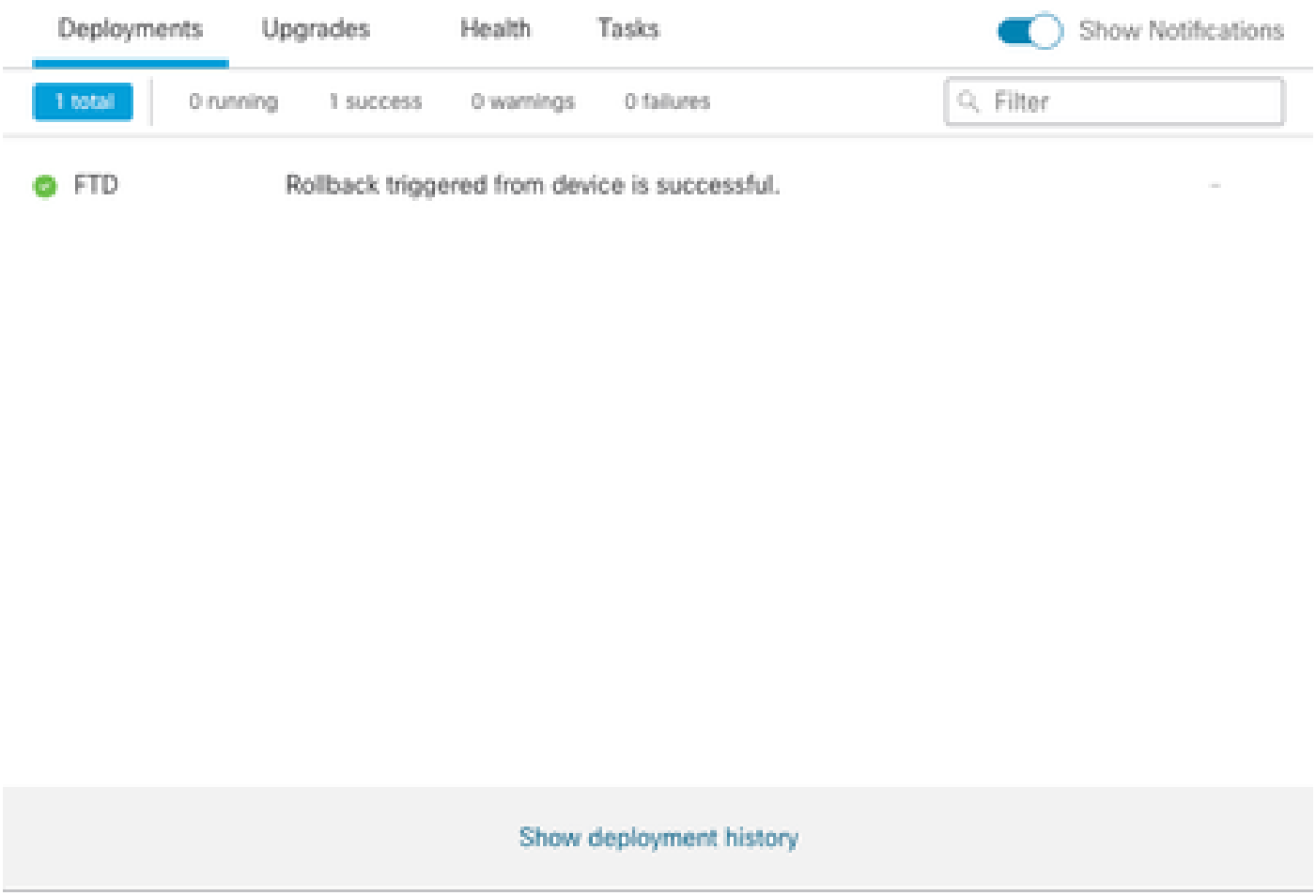


Imagen 5. Mensaje de SFMC que confirma la reversión de SFTD

Paso 5. Cuando se restaure el acceso a SFMC, resuelva el problema de configuración de SFMC y vuelva a implementarlo.

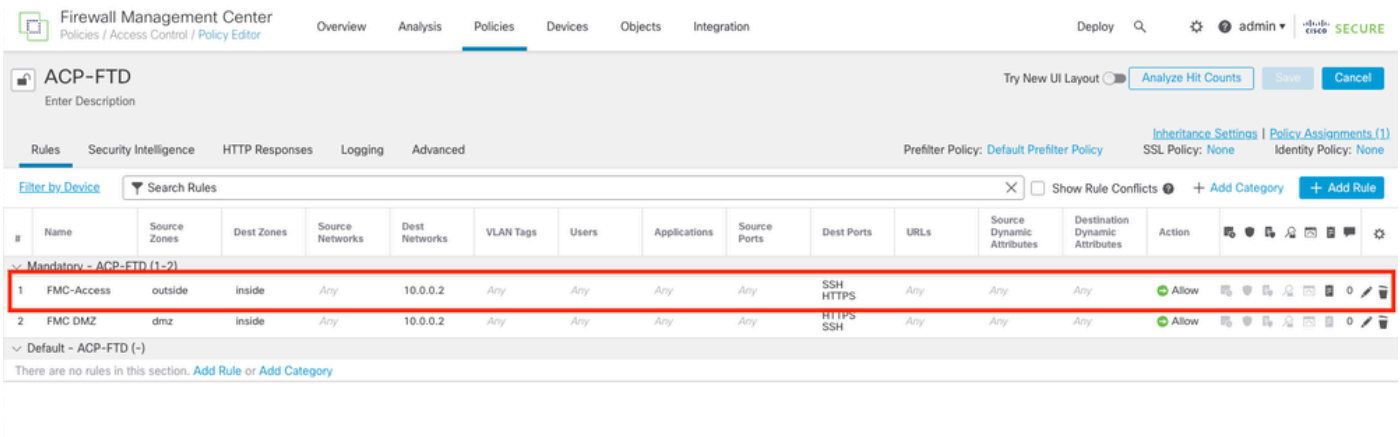


Imagen 6. Revertir los cambios

Resolución de problemas

En caso de que la reversión falle, póngase en contacto con Cisco TAC. Para obtener información sobre problemas adicionales durante el proceso, consulte el siguiente artículo:

· Reversión de la implementación

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).