在SFMC無法連線時設定SFTD的回覆

目錄

簡介

本文檔介紹如何從影響到SFTD連線的安全SFMC回滾部署更改。

必要條件

需求

Secure FirePOWER Threat Detection® 6.7版本以後支援使用此功能。

思科建議您瞭解以下主題：

- 安全防火牆管理中心(SFMC®)配置
- 思科安全FirePOWER威脅防禦(SFTD)配置

採用元件

- 適用於VMware的安全防火牆管理中心7.2.1版
- 適用於VMware 7.2版的安全Firepower威脅防禦

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在某些情況下，當部署更改影響網路連線時，與SFMC、SFTD或SFMC與SFTD之間的通訊將會丟失。您可以將SFTD上的配置回滾到上次部署的配置，以恢復管理連線。

使用configure policy rollback命令可將威脅防禦上的配置回滾到上次部署的配置。

注意：configure policy rollback 命令是在版本6.7中引入的

請參閱準則：

- 在威脅防禦上，只有以前的部署才可用於本地；您無法回滾到任何早期的部署。
- 從管理中心7.2開始支援回滾以實現高可用性。
- 群集部署不支援回滾。
- 回滾只影響可以在管理中心設定的配置。例如，回滾不會影響與專用管理介面相關的任何本地配置，您只能在威脅防禦CLI中配置該介面。請注意，如果在上次部署管理中心後使用configure network management-data-interface命令更改了資料介面設定，然後使用rollback命令，則不會保留這些設定；它們將回滾到上次部署的管理中心設定。
- 無法回滾UCAPL/CC模式。
- 無法回滾在上一次部署期間更新的帶外SCEP證書資料。
- 在回滾期間，連線可能會因為當前配置被清除而斷開。

設定

網路圖表

此文件使用以下網路設定：

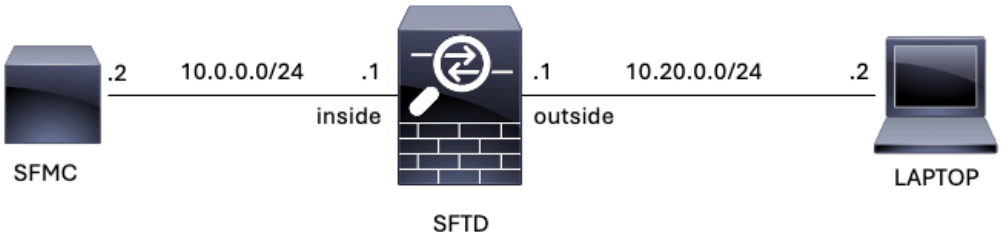


圖1.圖表

案例

在此配置中，SFTD由SFMC使用防火牆內部介面管理，有一個規則允許從筆記型電腦到SFMC的可達性。

程式

第1步：在SFMC上停用了名為FMC-Access 的規則，部署之後，從筆記型電腦到SFMC的通訊將被阻止。

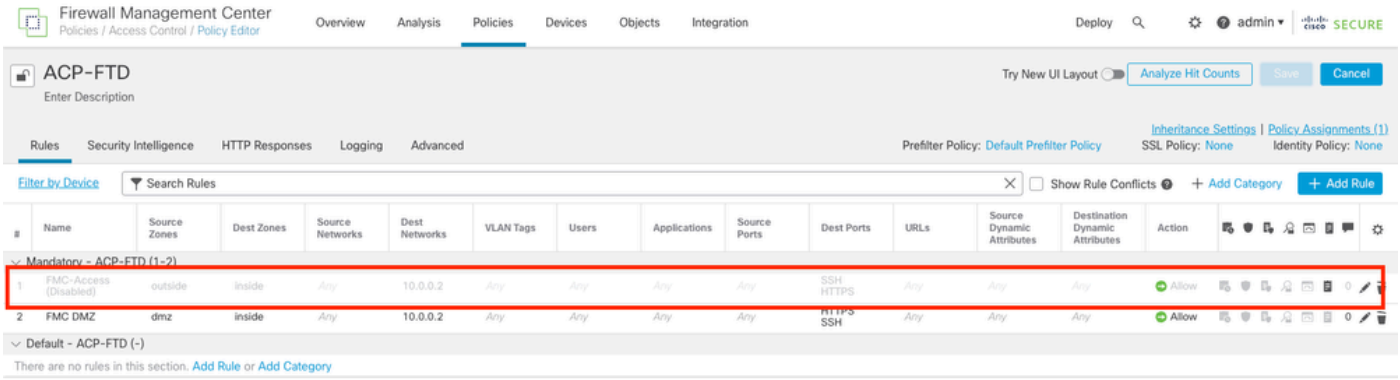


圖2.允許停用SFMC可達性的規則

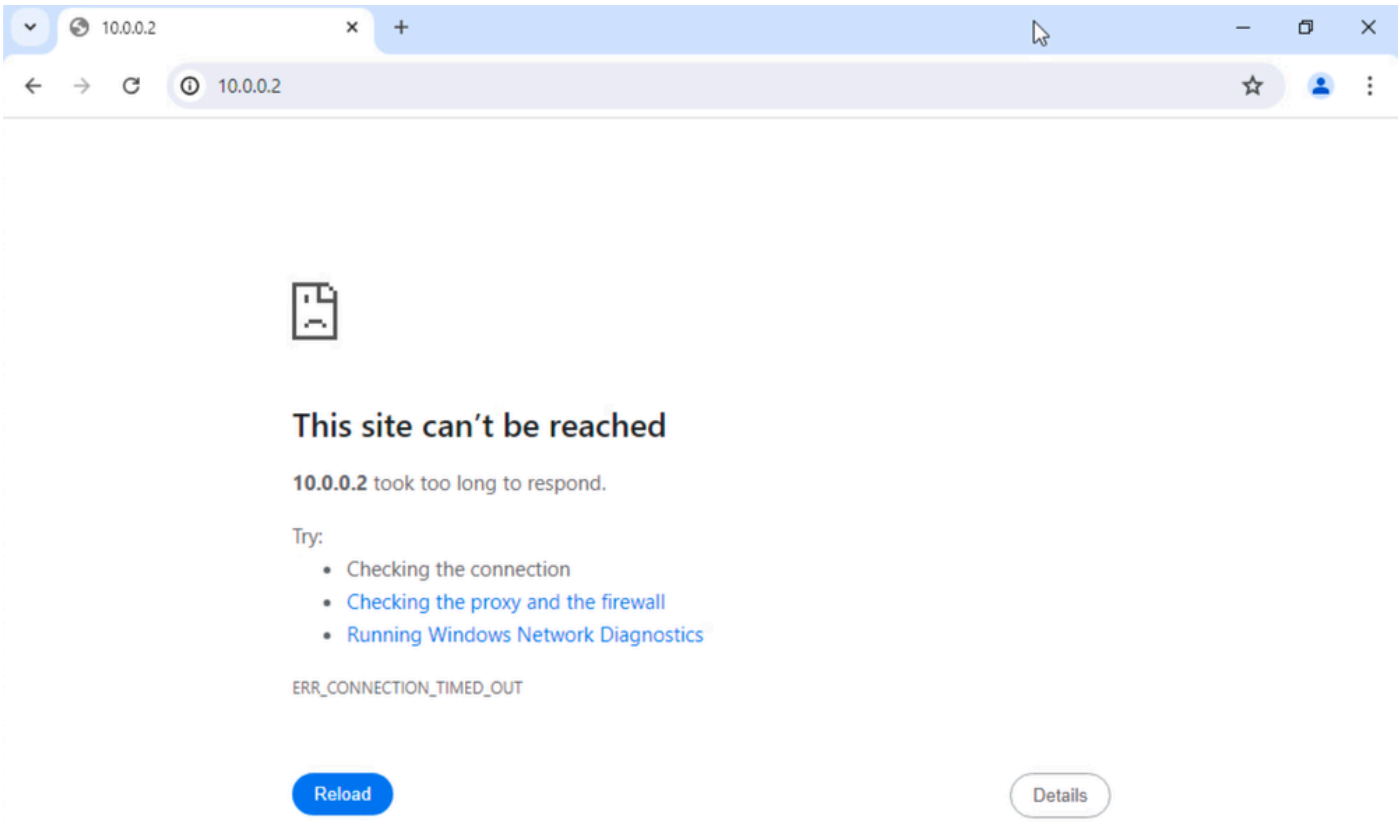


圖3.SFMC從筆記型電腦無法連線

步驟 2.透過SSH或控制檯登入到SFTD，然後使用configure policy rollback命令。

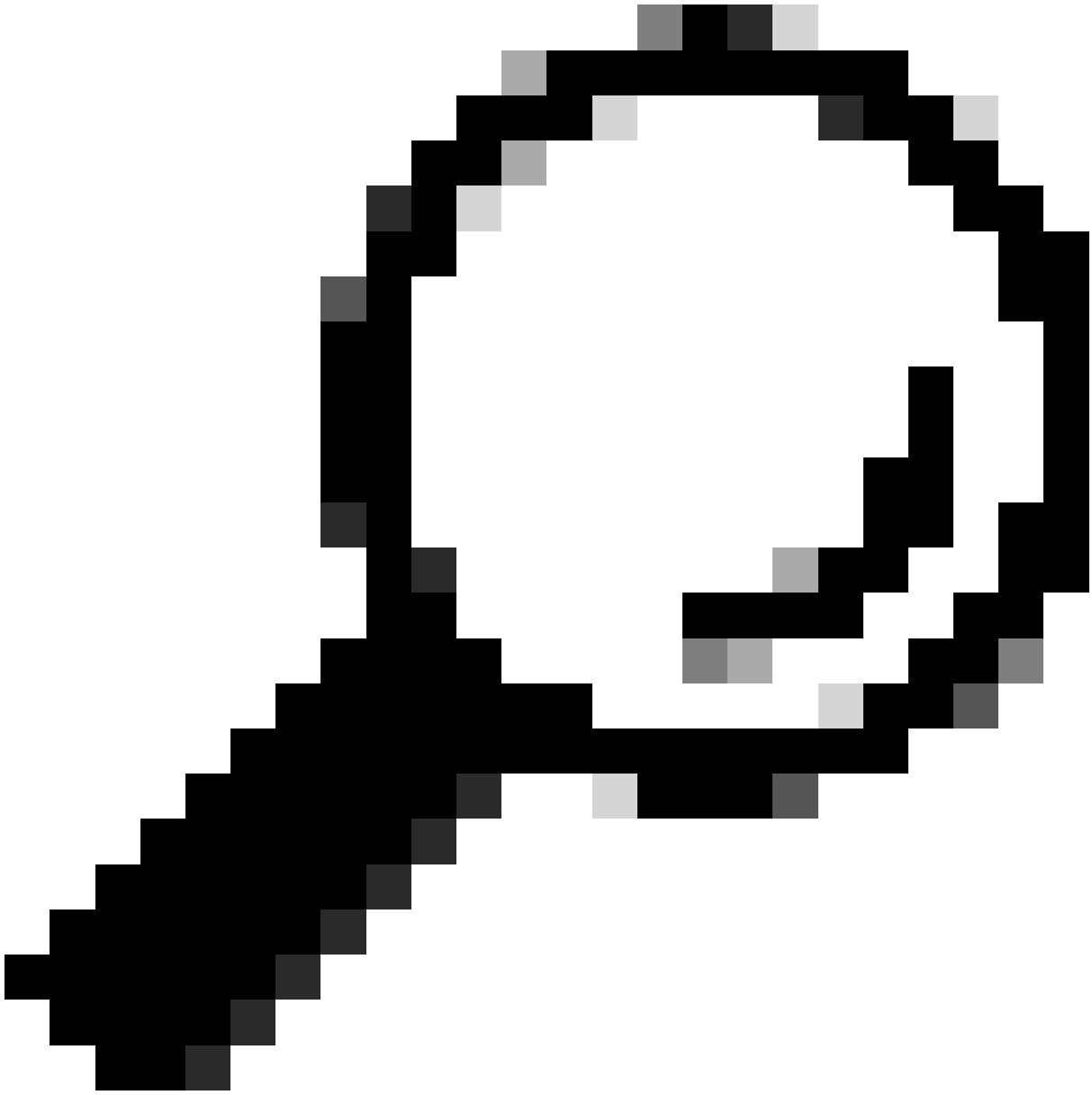
注意：如果無法通過SSH進行訪問，請透過telnet進行連線。

```
<#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)?
```

步驟 3.寫下單詞YES以確認上次部署的回滾，然後等待回滾過程結束。

```
<#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


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



提示：如果回滾失敗，請與思科TAC聯絡

步驟 4.回滾後，請確認SFMC的可達性。SFTD通知SFMC已成功完成回滾。在SFMC中，部署螢幕將顯示一條標語，指示配置已回滾。

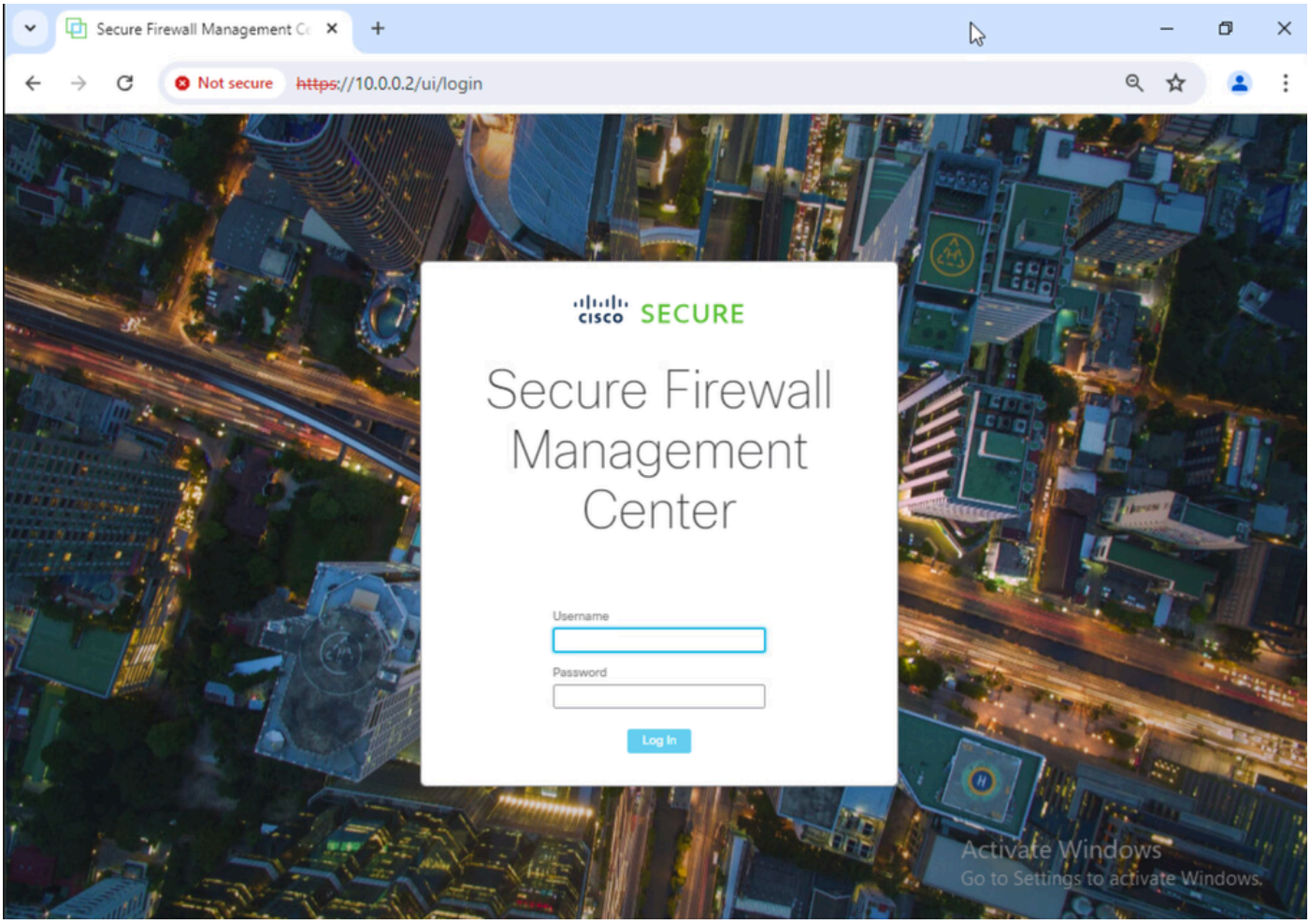


圖4.從筆記型電腦恢復的SFMC連線能力

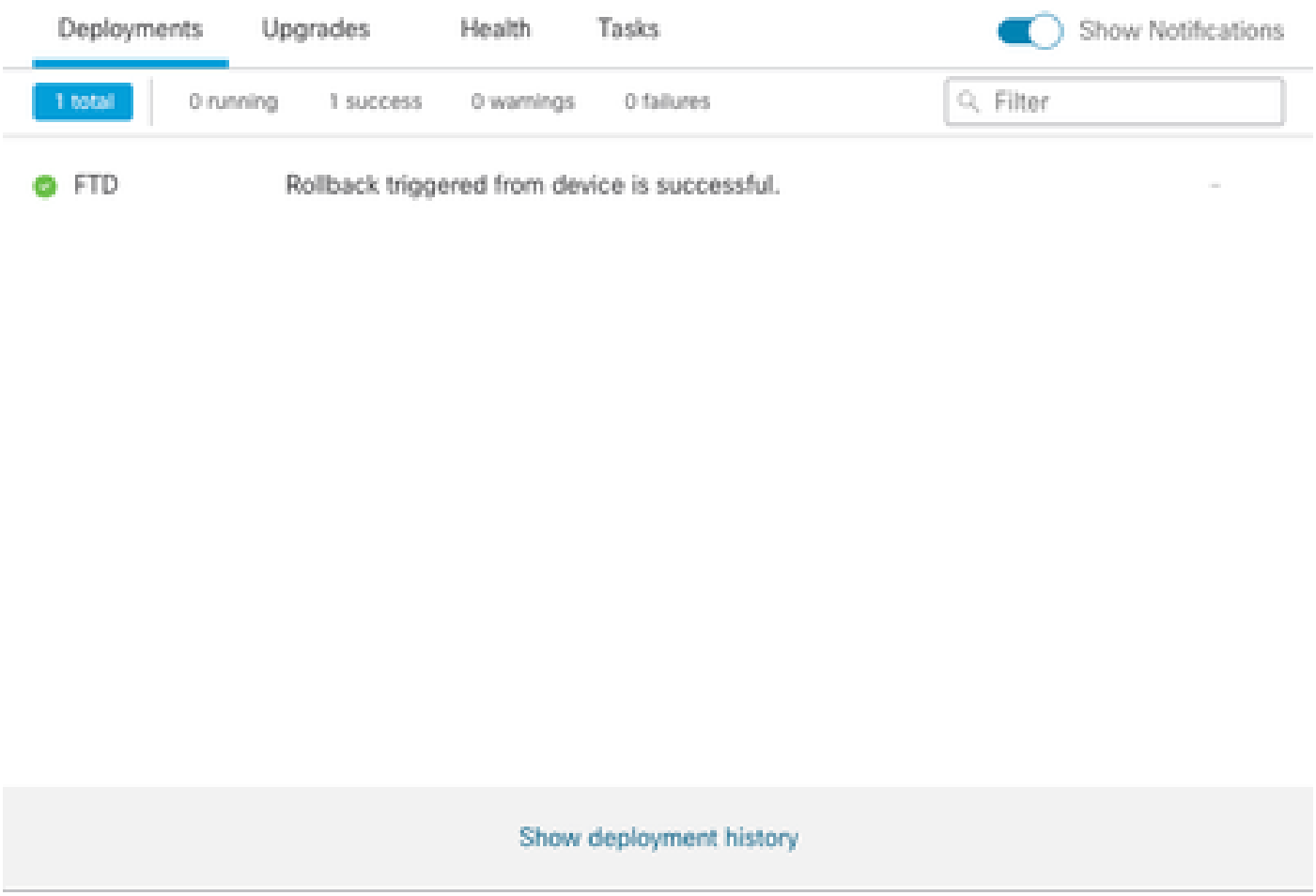


圖5.確認從SFTD復原的SFMC訊息

步驟 5.恢復SFMC訪問後，請解決SFMC配置問題並重新部署。

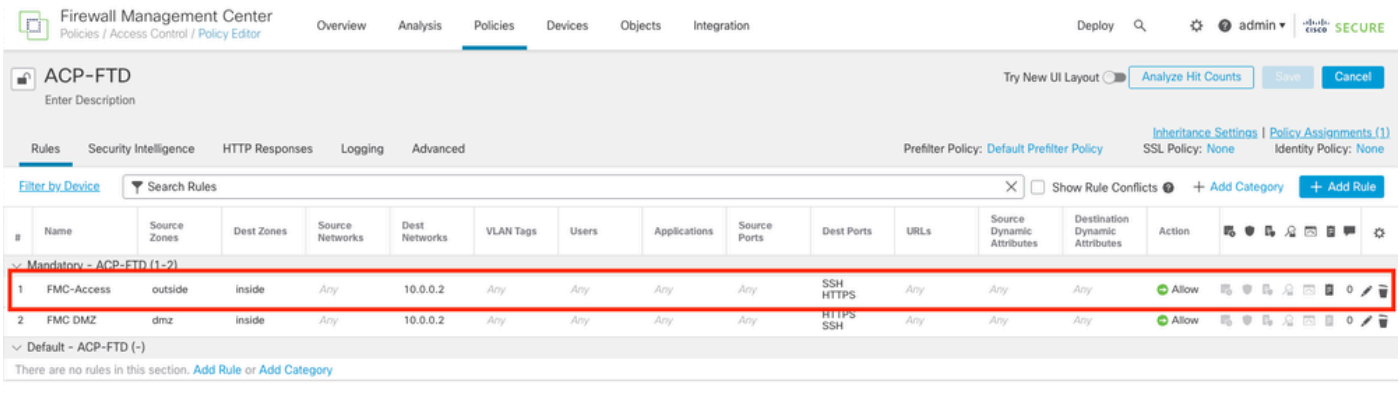


圖6.還原變更

疑難排解

如果回滾失敗，請與Cisco TAC聯絡，有關過程中出現的其他問題，請檢視下一條：

·部署回滾

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。