SFMCに到達できない場合のSFTDでのロールバックの設定

内容

はじめに

このドキュメントでは、SFTDへの接続に影響を与えるSecure SFMCから導入の変更をロールバックする方法について説明します。

前提条件

要件

この機能の使用は、Secure FirePOWER Threat Detection®バージョン6.7以降でサポートされています。

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール管理センター(SFMC®)の設定
- Cisco Secure FirePOWER Threat Defense(SFTD)の設定

使用するコンポーネント

- Secure Firewall Management Center for VMwareバージョン7.2.1
- VMware向けSecure Firepower Threat Defenseバージョン7.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

導入の変更がネットワーク接続に影響を与えると、SFMC、SFTDへの通信、またはSFMCとSFTD間の通信が失われるシナリオがあります。SFTDの設定を最後に展開した設定にロールバックして、管理接続を復元できます。

configure policy rollbackコマンドを使用して、脅威対策の設定を最後に展開された設定にロールバックします。

注：configure policy rollback コマンドはバージョン6.7で導入されました

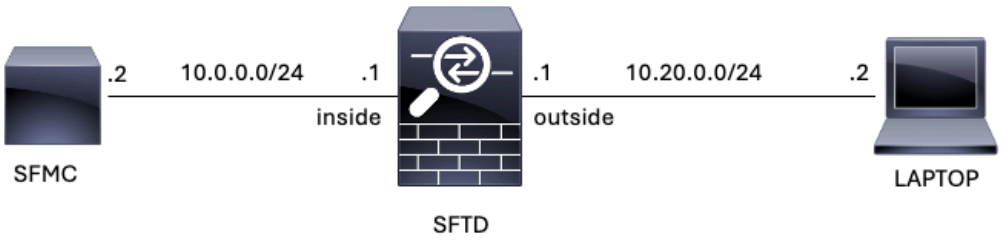
次のガイドラインを参照してください。

- 脅威対策でローカルに使用できるのは以前の展開だけです。以前の展開にロールバックすることはできません。
- ロールバックは、management center 7.2以降のハイアベイラビリティのためにサポートされています。
- ロールバックは、クラスタリングの展開ではサポートされていません。
- ロールバックは、管理センターで設定できる構成にのみ影響します。たとえば、ロールバックは、脅威対策CLIでのみ設定できる専用管理インターフェイスに関連するローカル設定には影響しません。前回の管理センターの導入後に、configure network management-data-interfaceコマンドを使用してデータインターフェイス設定を変更してからrollbackコマンドを使用した場合、これらの設定は保持されず、最後に導入された管理センターの設定にロールバックされます。
- UCAPL/CCモードはロールバックできません。
- 以前の展開で更新されたアウトオブバンドSCEP証明書データはロールバックできません。
- 現在の設定がクリアされているため、ロールバック中に接続がドロップする可能性があります。

設定

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



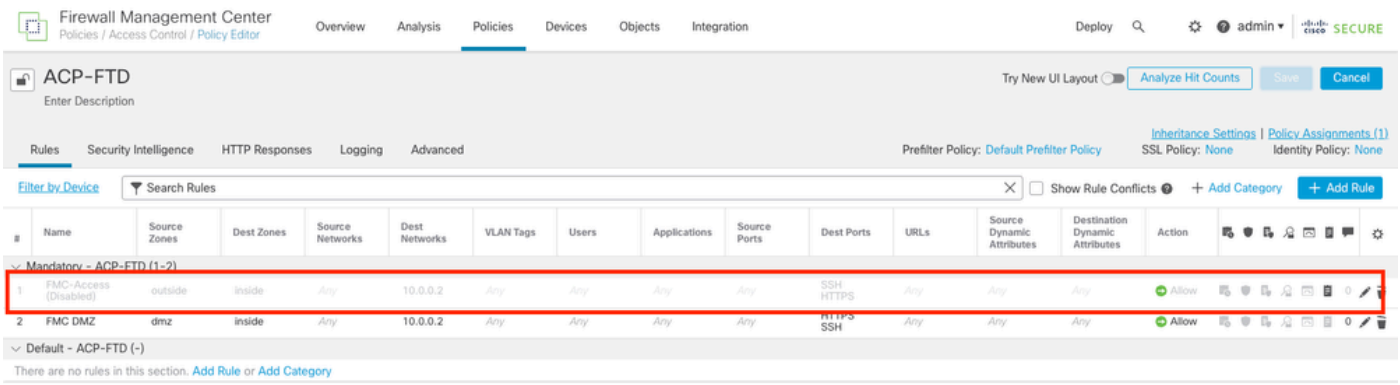
画像 1.図

シナリオ

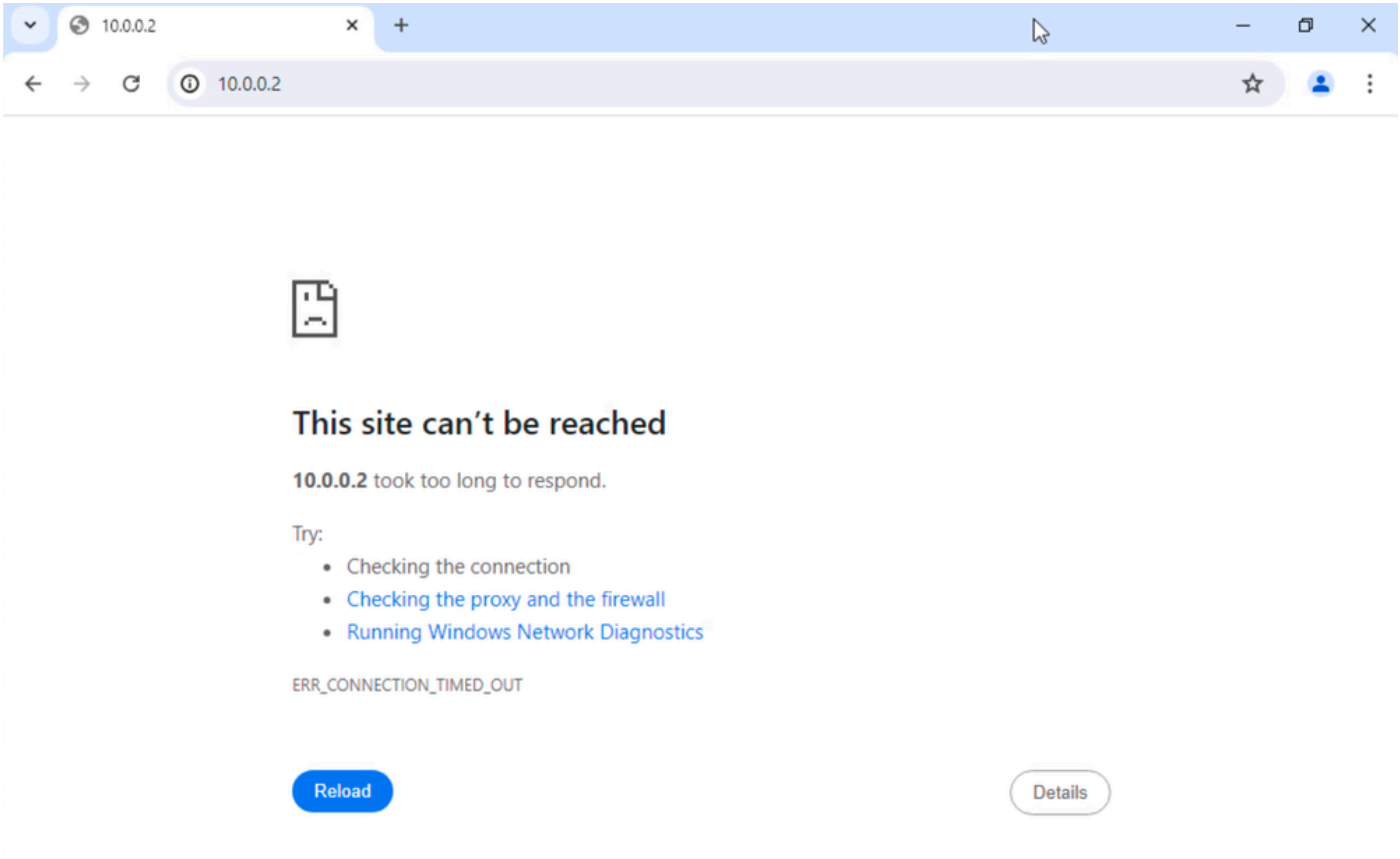
この設定では、SFTDはファイアウォール内部インターフェイスを使用してSFMCによって管理され、ラップトップからSFMCへの到達可能性を許可するルールがあります。

手順

ステップ1:FMC-Access という名前のルールがSFMCで無効にされています。展開後に、ラップトップからSFMCへの通信がブロックされます。



画像 2.SFMCの到達可能性を許可するルールの無効化



画像 3.ラップトップからのSFMC到達可能性が機能しない

ステップ2.SSHまたはコンソールを使用してSFTDにログインし、configure policy rollbackコマンドを使用します。

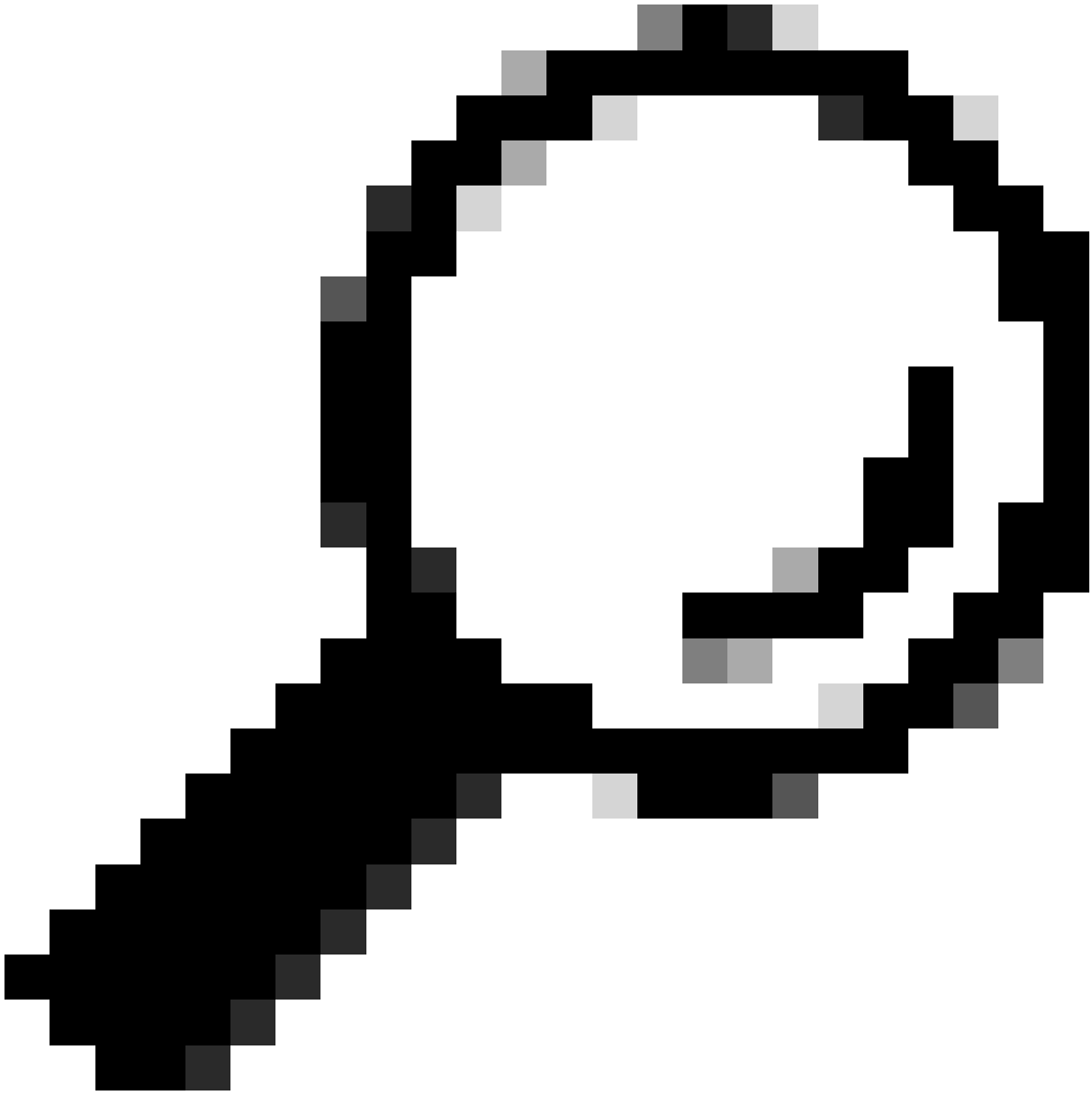
注:SSH経由でアクセスできない場合は、Telnet経由で接続してください。

```
<#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)?
```

手順 3：最後の展開のロールバックを確認するためにYESと入力し、ロールバックプロセスが終了するまで待ちます。

```
<#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


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



ヒント：ロールバックが失敗した場合は、Cisco TACにお問い合わせください

ステップ4.ロールバック後、SFMCの到達可能性を確認します。SFTDは、ロールバックが正常に完了したことをSFMCに通知します。SFMCでは、導入画面に設定がロールバックされたことを示すバナーが表示されます。

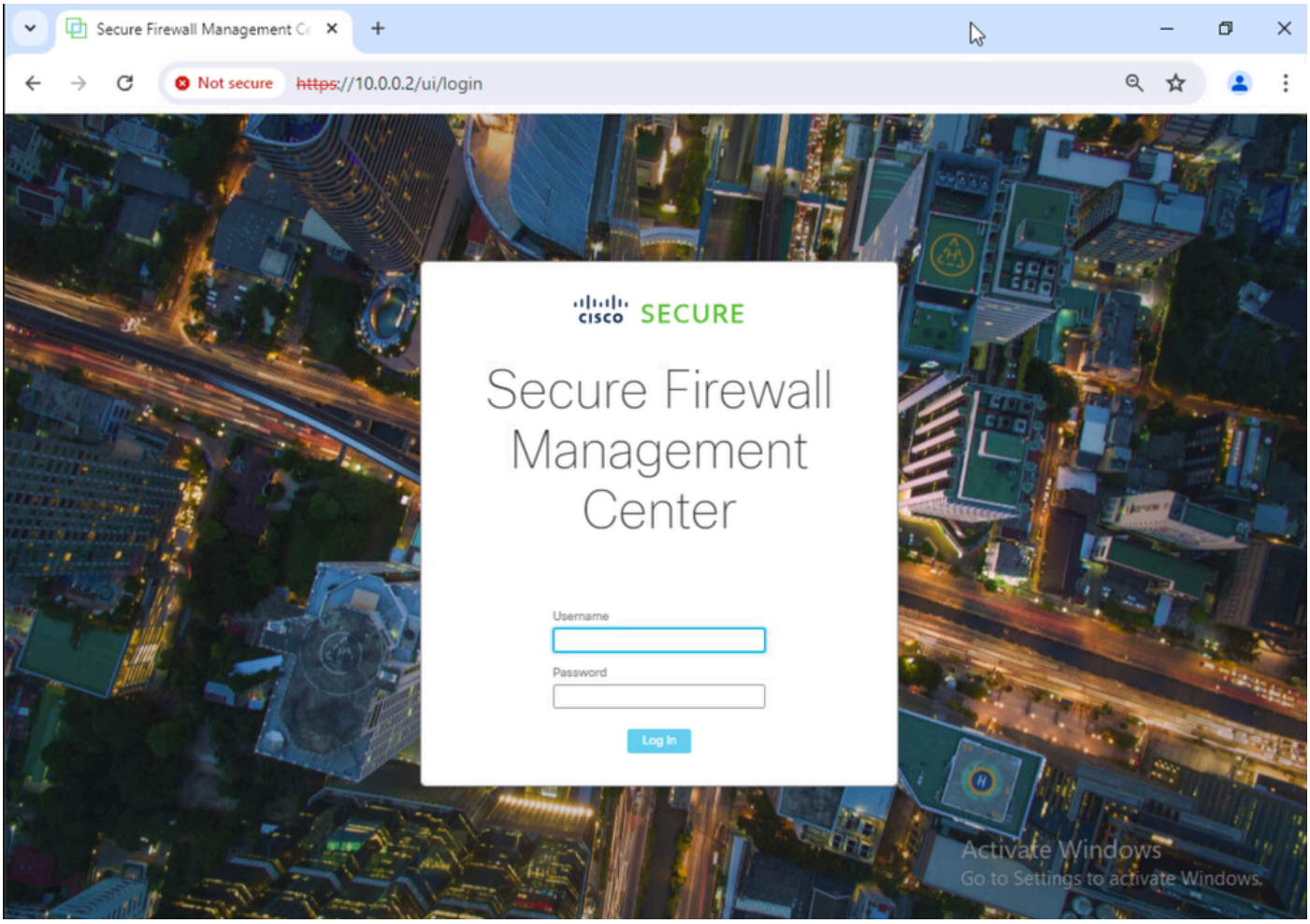


図 4.ラップトップからのSFMC到達可能性の復元

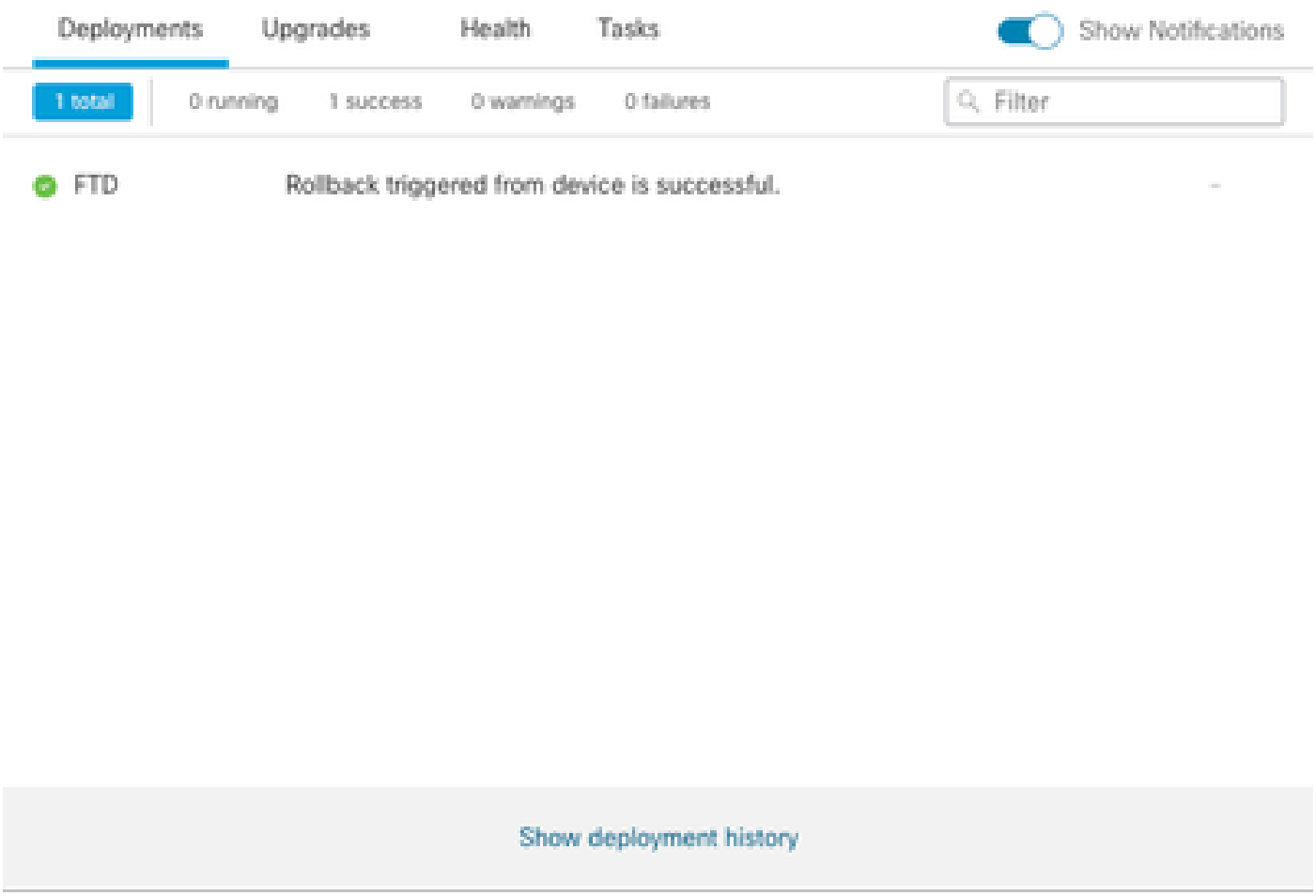


図 5.SFTDからのSFMCメッセージ確認ロールバック

ステップ5:SFMCへのアクセスが復旧したら、SFMCの設定の問題を解決し、再導入します。

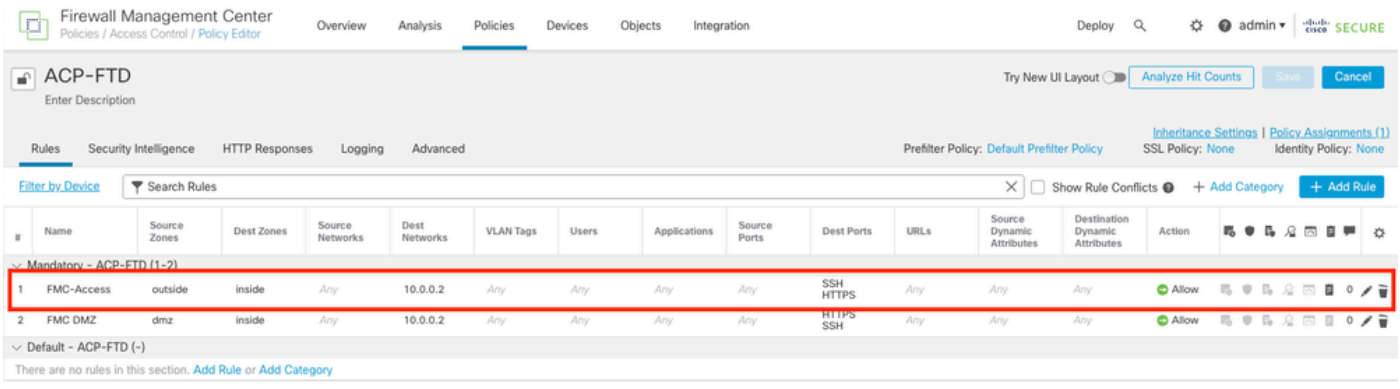


図 6.変更を元に戻す

トラブルシューティング

ロールバックが失敗した場合は、Cisco TACにお問い合わせください。プロセス中に発生したその他の問題については、次の記事を参照してください。

- 導入のロールバック

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。