Rollback auf SFTD konfigurieren, wenn SFMC nicht erreichbar ist

Inhalt

Einleitung

In diesem Dokument wird das Rollback einer Bereitstellungsänderung vom sicheren SFMC beschrieben, die sich auf die Verbindung zu SFTD auswirkt.

Voraussetzungen

Anforderungen

Die Verwendung dieser Funktion wird von Secure FirePOWER Threat Detection® ab Version 6.7 unterstützt.

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Secure Firewall Management Center (SFMC®)-Konfiguration
- Konfiguration von Cisco Secure FirePOWER Threat Defense (SFTD)

Verwendete Komponenten

- Secure Firewall Management Center für VMware Version 7.2.1
- Sicherer Schutz vor Firepower-Bedrohungen für VMware Version 7.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Es gibt Szenarien, in denen die Kommunikation mit SFMC, SFTD oder zwischen SFMC und SFTD verloren geht, wenn eine Bereitstellungsänderung die Netzwerkverbindung beeinträchtigt. Sie können die Konfiguration auf der SFTD auf die zuletzt bereitgestellte Konfiguration zurücksetzen, um die Managementverbindung wiederherzustellen.

Verwenden Sie den Befehl configure policy rollback, um ein Rollback der Konfiguration auf der Threat Defence-Website auf die zuletzt bereitgestellte Konfiguration durchzuführen.

Hinweis: Der Befehl configure policy rollback wurde in Version 6.7 eingeführt

---

Siehe Richtlinien:

- Nur die vorherige Bereitstellung ist lokal auf der Bedrohungsabwehr verfügbar. Ein Rollback auf frühere Bereitstellungen ist nicht möglich.
- Rollback wird für eine hohe Verfügbarkeit ab Management Center 7.2 unterstützt.
- Rollback wird für Clustering-Bereitstellungen nicht unterstützt.
- Der Rollback wirkt sich nur auf Konfigurationen aus, die Sie im Management Center festlegen können. Beispielsweise hat der Rollback keine Auswirkungen auf die lokale Konfiguration der dedizierten Management-Schnittstelle, die Sie nur über die Threat Defense-CLI konfigurieren können. Beachten Sie, dass die Einstellungen für die Datenschnittstelle nach der letzten Bereitstellung des Verwaltungscenters mit dem Befehl configure network management-data-interface und dem Befehl rollback nicht beibehalten werden. Sie werden auf die zuletzt bereitgestellten Verwaltungscenter-Einstellungen zurückgesetzt.
- Für den UCAPL/CC-Modus kann kein Rollback ausgeführt werden.
- Out-of-Band-SCEP-Zertifikatdaten, die während der vorherigen Bereitstellung aktualisiert wurden, können nicht zurückgesetzt werden.
- Während des Rollbacks können Verbindungen getrennt werden, da die aktuelle Konfiguration gelöscht wird.

Konfigurieren

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

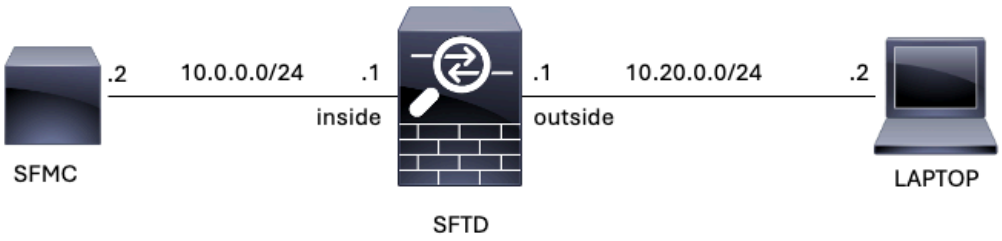


Bild 1. Diagramm

Szenario

In dieser Konfiguration wird SFTD vom SFMC über die Firewall-interne Schnittstelle verwaltet. Es gibt eine Regel, die die Erreichbarkeit vom Laptop zum SFMC ermöglicht.

Vorgehensweise

Schritt 1: Die Regel mit dem Namen FMC-Access wurde auf dem SFMC deaktiviert. Nach der Bereitstellung wird die Kommunikation vom Laptop zum SFMC blockiert.

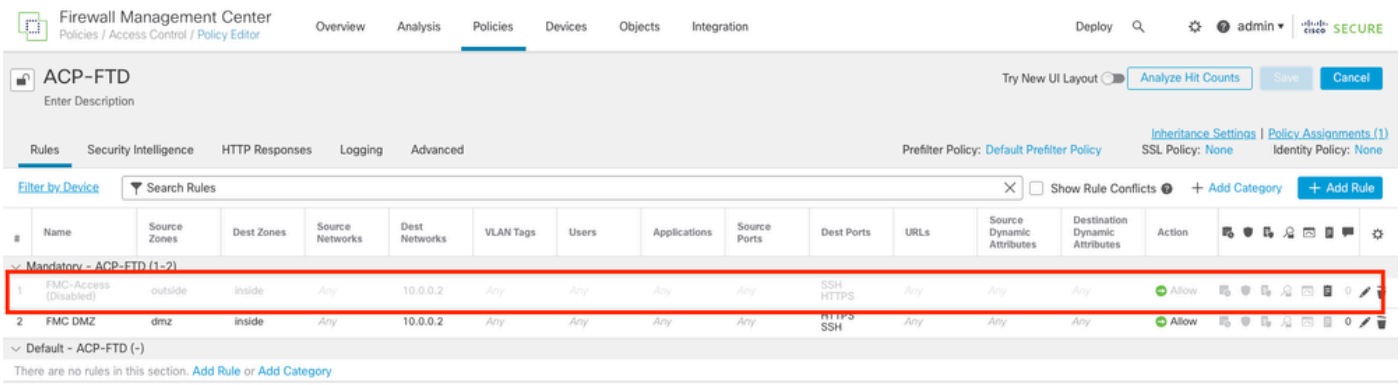


Bild 2. Die Regel, die die SFMC-Erreichbarkeit deaktiviert lässt

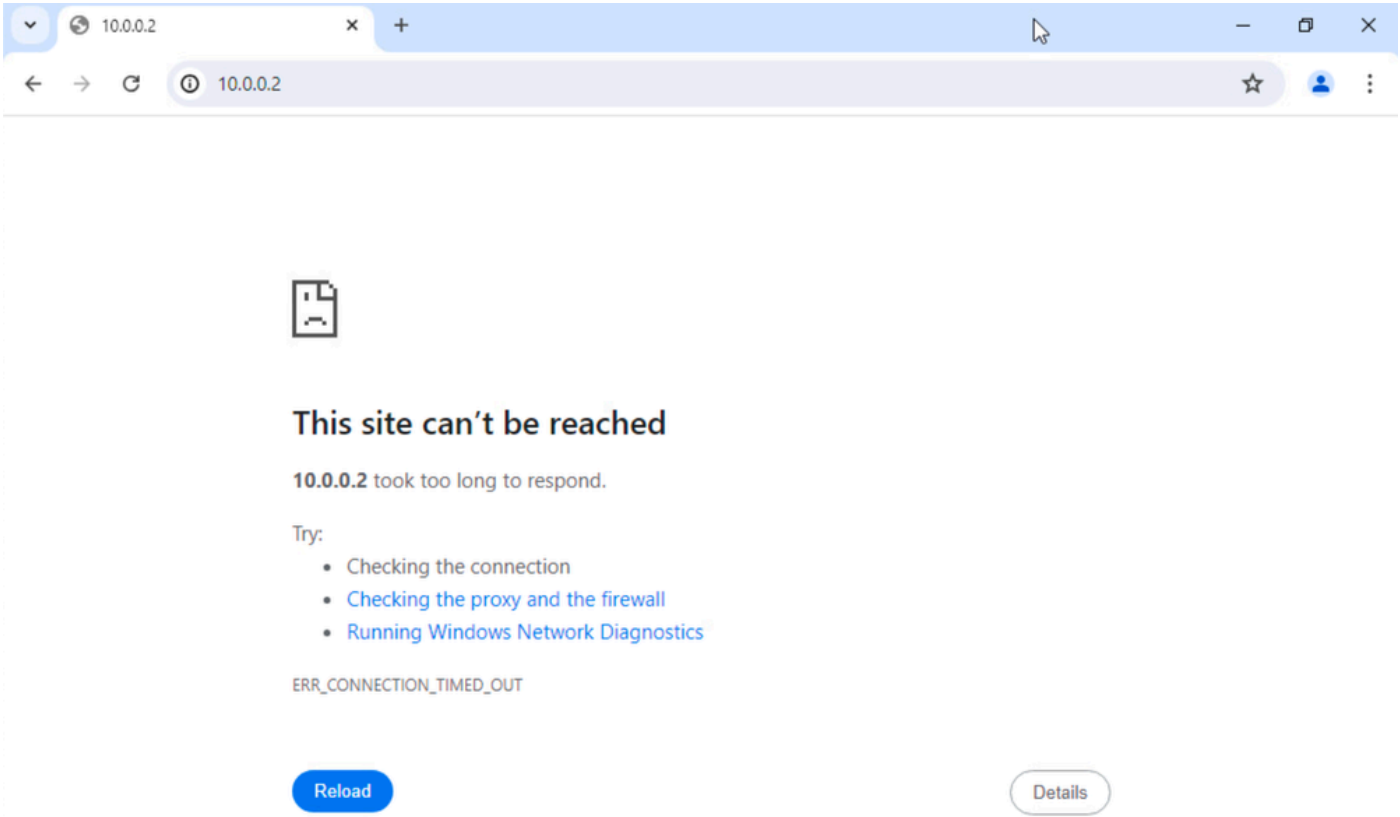


Bild 3. SFMC-Erreichbarkeit vom Laptop aus nicht möglich

Schritt 2: Melden Sie sich über SSH oder die Konsole beim SFTD an, und verwenden Sie dann den Befehl configure policy rollback.

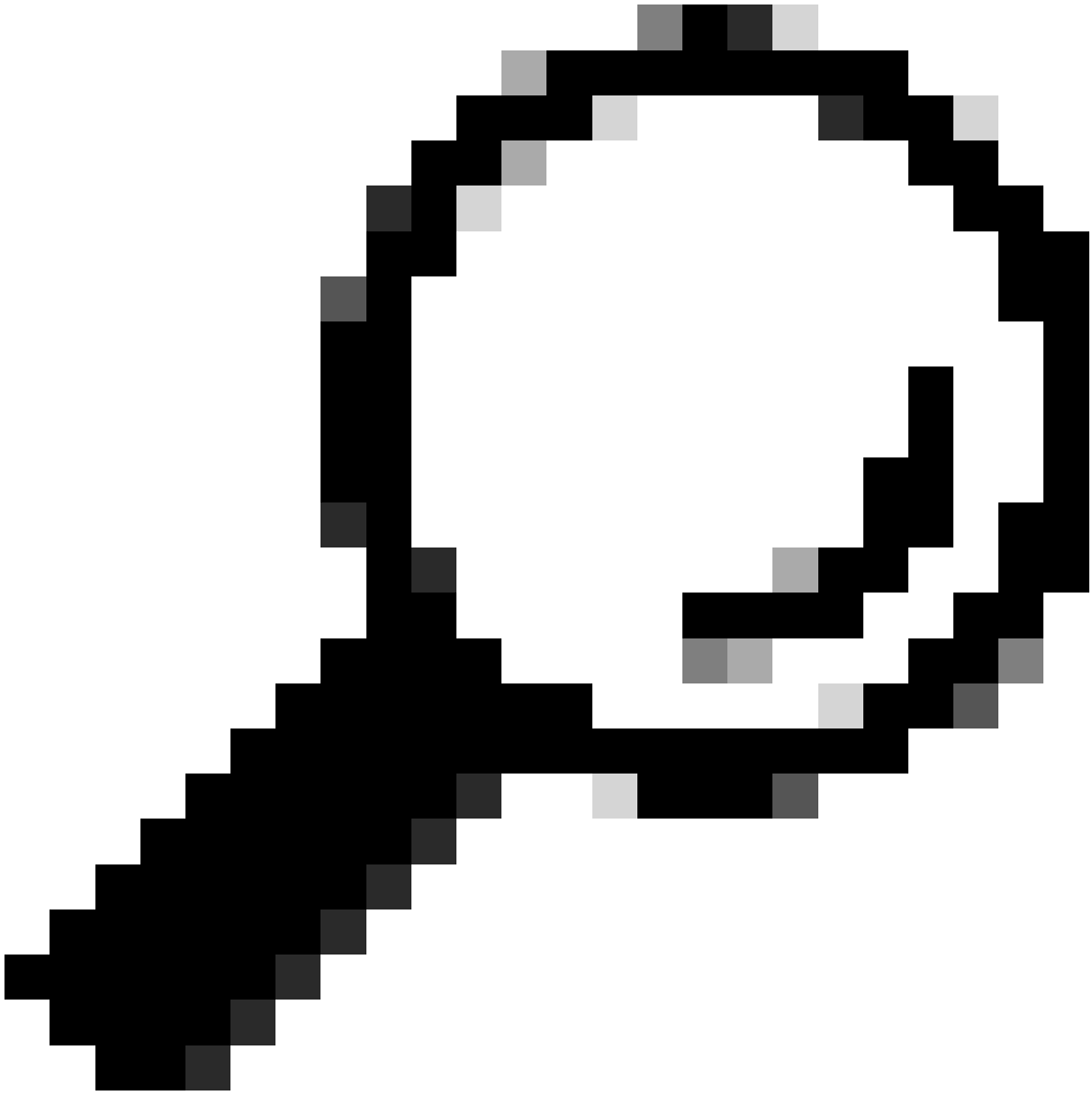
Hinweis: Wenn kein Zugriff über SSH möglich ist, stellen Sie eine Verbindung über Telnet her.

```
<#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)?
```

Schritt 3: Schreiben Sie das Wort JA, um das Rollback der letzten Bereitstellung zu bestätigen, und warten Sie dann, bis der Rollbackprozess beendet ist.

```
<#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


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



Tipp: Wenden Sie sich bei einem Rollback an das Cisco TAC.

Schritt 4: Bestätigen Sie nach dem Rollback die SFMC-Erreichbarkeit. Der SFTD benachrichtigt den SFMC, dass das Rollback erfolgreich abgeschlossen wurde. Im SFMC wird auf dem Bereitstellungsbildschirm ein Banner mit der Meldung angezeigt, dass ein Rollback der Konfiguration durchgeführt wurde.

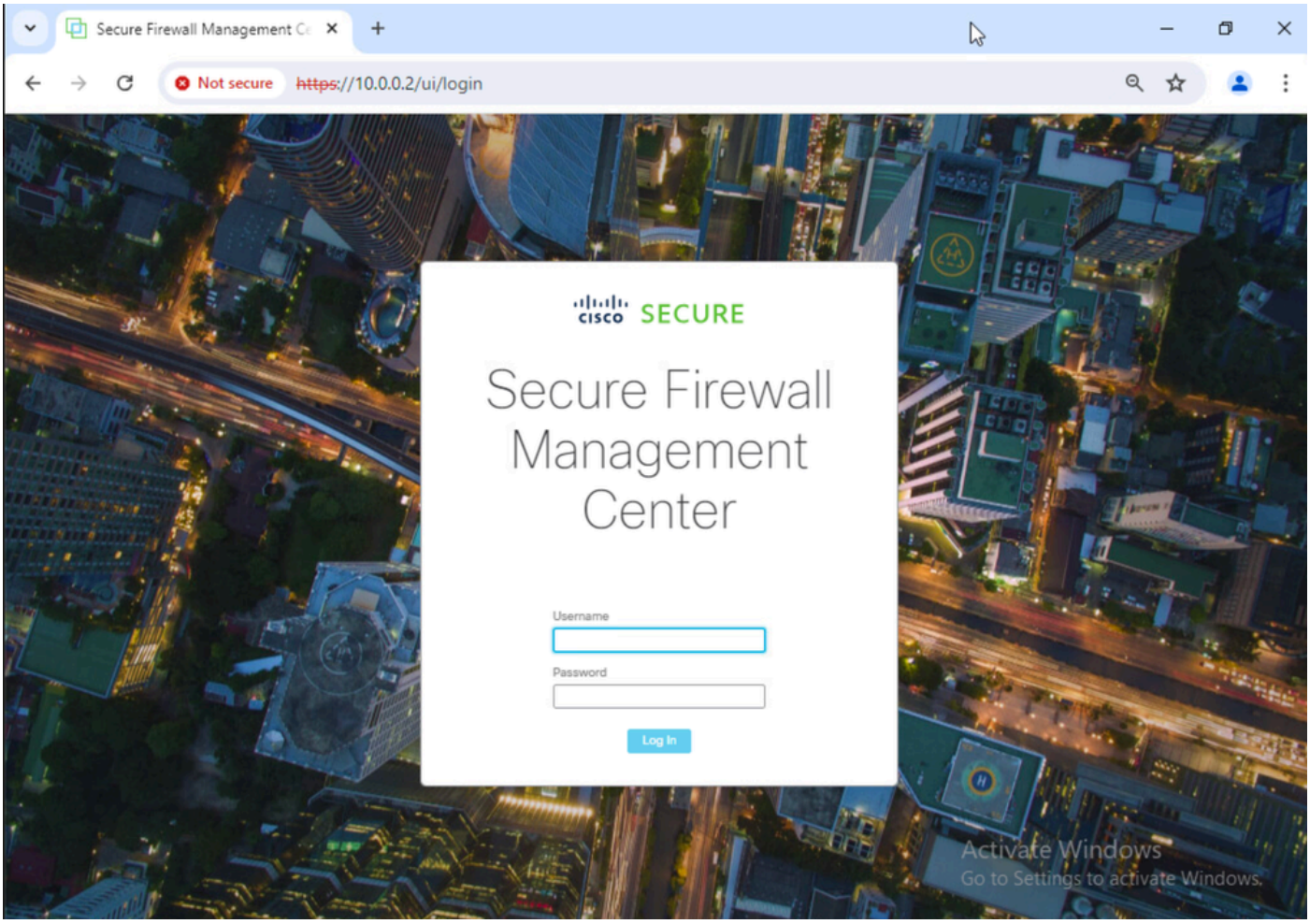


Abbildung 4: SFMC-Erreichbarkeit vom Laptop wiederhergestellt

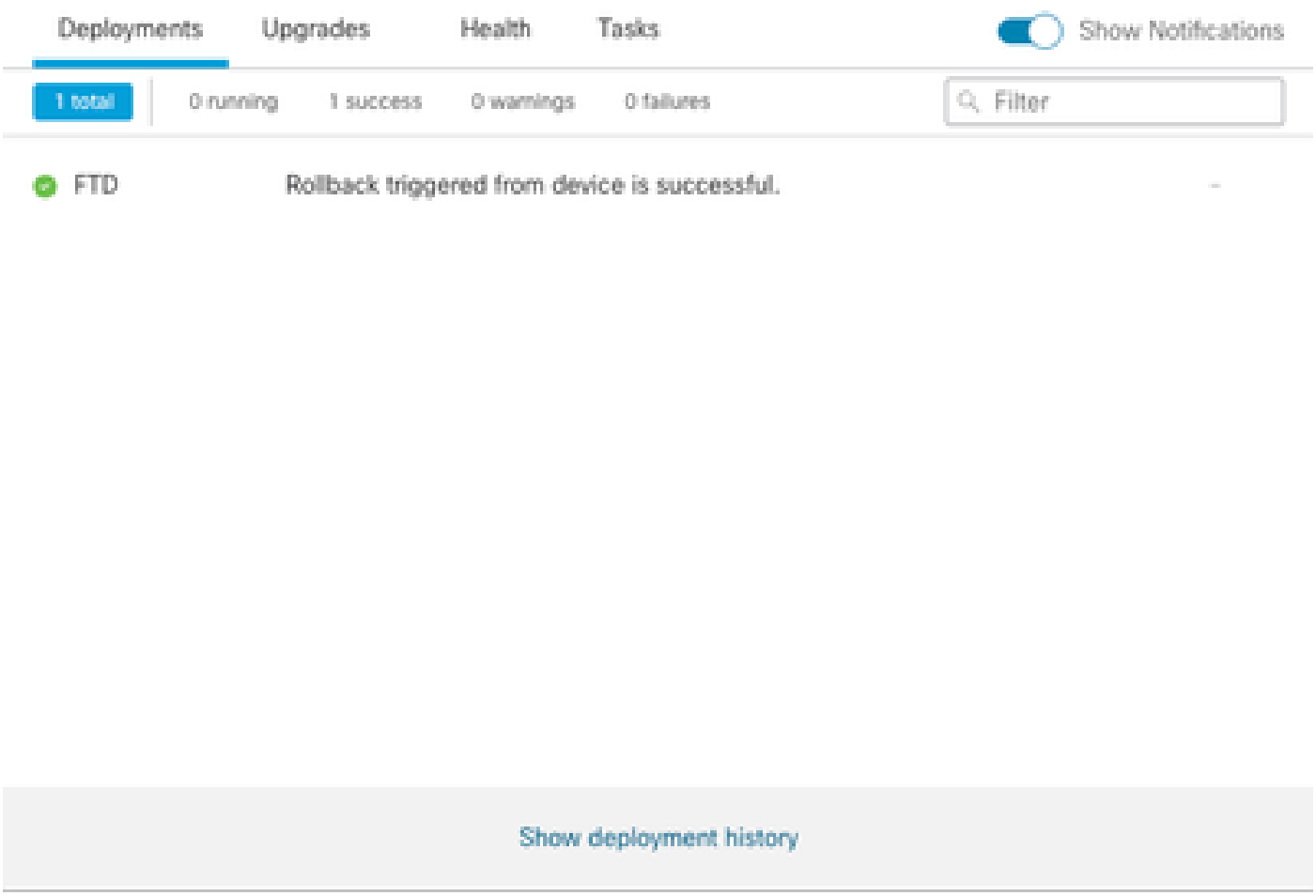


Bild 5. SFMC-Meldung bestätigt Rollback von SFTD

Schritt 5: Wenn der SFMC-Zugriff wiederhergestellt ist, beheben Sie das SFMC-Konfigurationsproblem, und stellen Sie es erneut bereit.

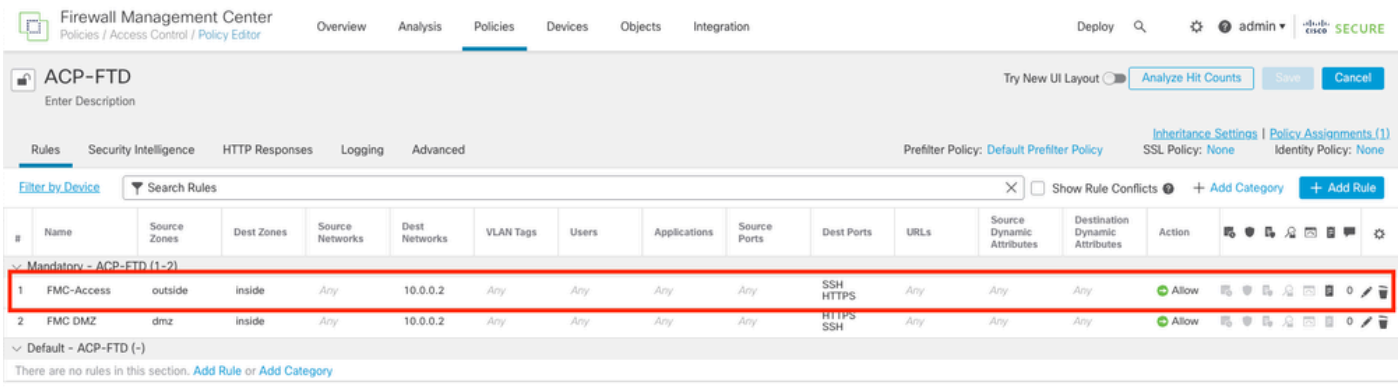


Bild 6. Änderungen rückgängig machen

Fehlerbehebung

Falls das Rollback fehlschlägt, wenden Sie sich an das Cisco TAC. Weitere Informationen dazu erhalten Sie im nächsten Artikel:

- Rollback der Bereitstellung

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.