

在SFMC不可达时在SFTD上配置回滚

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[场景](#)

[步骤](#)

[故障排除](#)

简介

本文档介绍如何从影响到SFTD连接的安全SFMC回滚部署更改。

先决条件

要求

Secure FirePOWER Threat Detection® 6.7版以后支持使用此功能。

Cisco 建议您了解以下主题：

- 安全防火墙管理中心(SFMC®)配置
- 思科安全FirePOWER威胁防御(SFTD)配置

使用的组件


- 适用于VMware 7.2.1版的安全防火墙管理中心
- 适用于VMware 7.2版的安全Firepower威胁防御

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在某些情况下，当部署更改影响网络连接时，与SFMC、SFTD或SFMC与SFTD之间的通信会丢失。您可以将SFTD中的配置回滚到上次部署的配置，以恢复管理连接。

使用configure policy rollback命令可将威胁防御上的配置回滚到上次部署的配置。

 注意：configure policy rollback命令在版本6.7中引入

请参阅指南：

- 威胁防御仅在本地提供以前的部署；您无法回滚到任何以前的部署。
- 从管理中心7.2开始支持回滚，以实现高可用性。
- 集群部署不支持回滚。
- 回滚仅影响可在管理中心设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在威胁防御CLI上配置该接口。请注意，如果在上次管理中心部署后使用configure network management-data-interface命令更改数据接口设置，然后使用rollback命令，则不会保留这些设置；它们将回滚到上次部署的管理中心设置。
- 无法回滚UCAPL/CC模式。
- 无法回滚之前部署期间更新的带外SCEP证书数据。
- 在回滚期间，由于当前配置被清除，连接可能会中断。

配置

网络图

本文档使用以下网络设置：

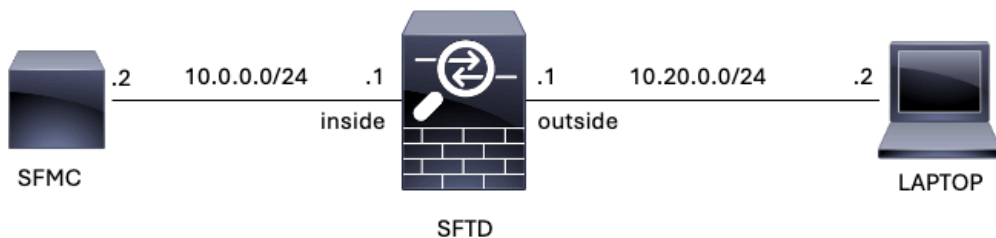


图 1.图解

场景

在此配置中，SFTD由SFMC使用防火墙内部接口进行管理，有一个规则允许从笔记本电脑访问SFMC。

步骤

第1步：在SFMC上禁用了名为FMC-Access的规则，部署后，将阻止从笔记本电脑到SFMC的通信。

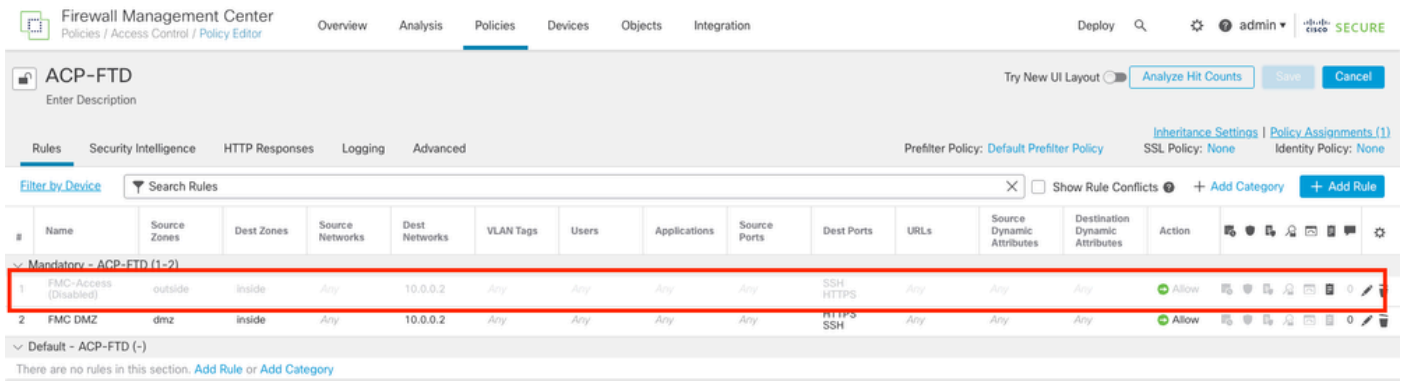


图 2. 已禁用允许SFMC可达性的规则

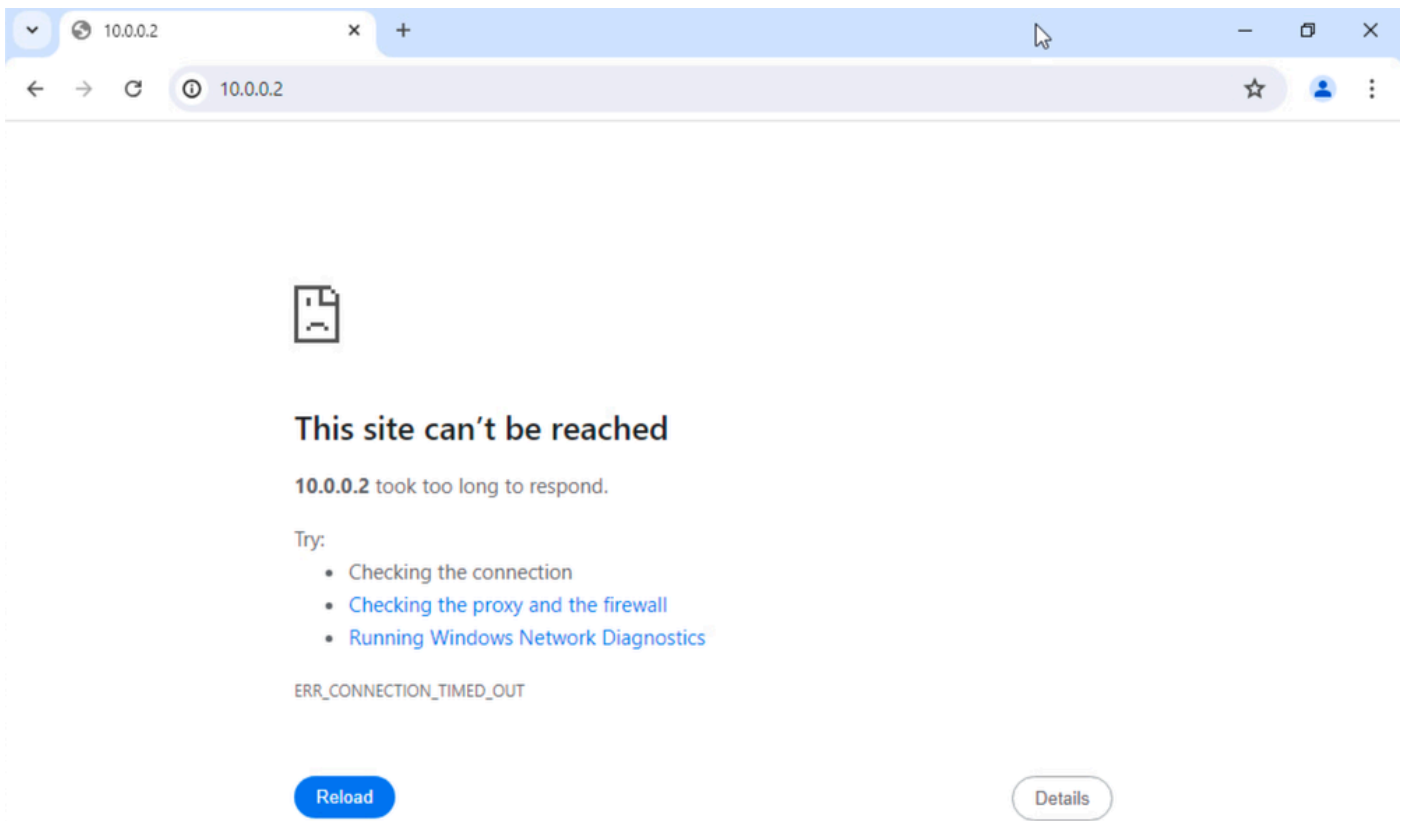



图 3. SFMC从无法工作的笔记本电脑可达性

步骤 2通过SSH或控制台登录到SFTD，然后使用configure policy rollback命令。

 注意：如果无法通过SSH进行访问，请通过telnet进行连接。

```
<#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)?

第 3 步：请写下单词YES以确认上次部署的回滚，然后等待回滚过程结束。

<#root>

Do you want to continue (YES/NO)?

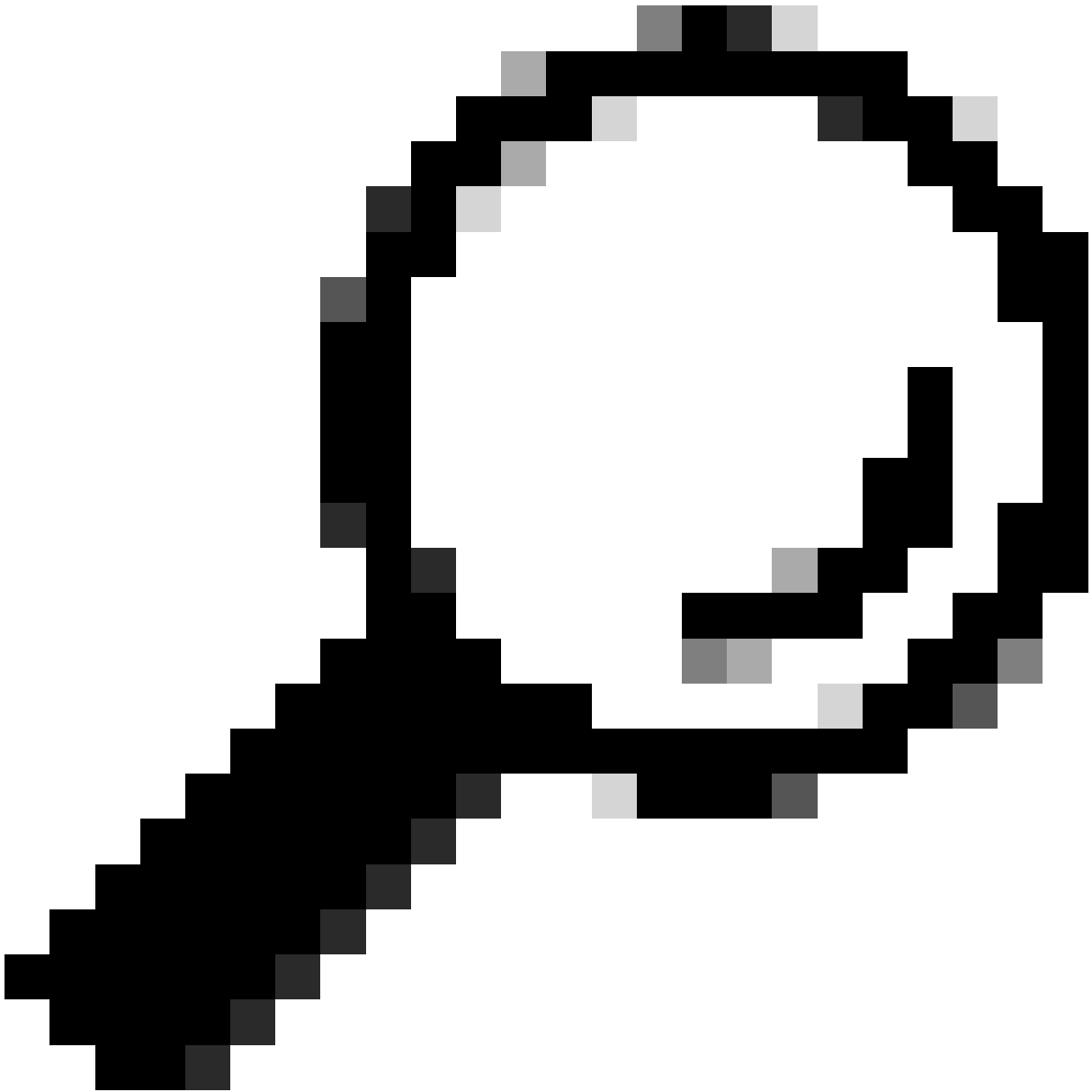
YES

```
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：如果回滚失败，请联系思科TAC

第 4 步：回滚后，请确认SFMC的可达性。SFTD通知SFMC回滚已成功完成。在SFMC中，部署屏幕会显示一条标语，表明配置已回滚。

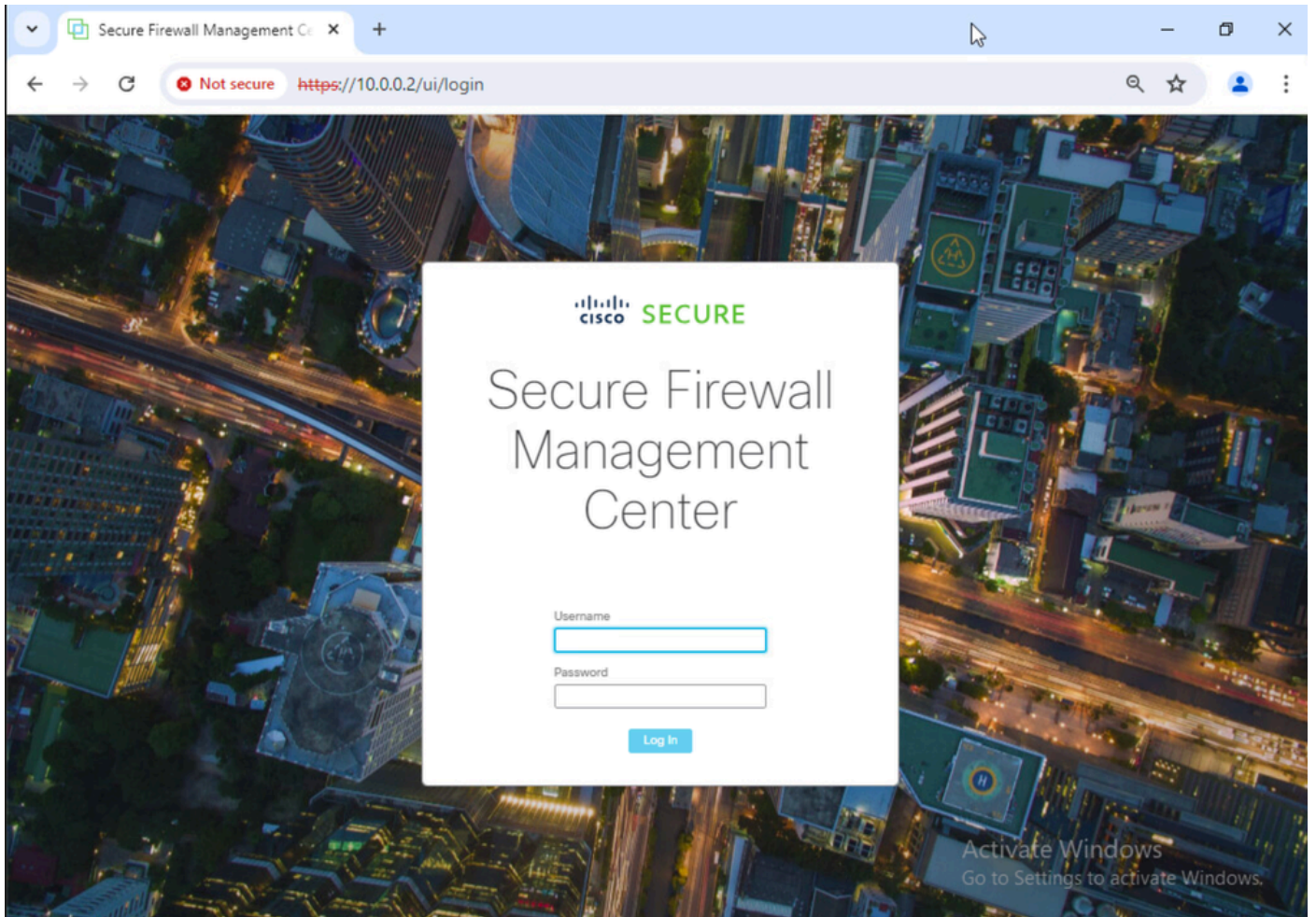


图 4.从笔记本电脑恢复的SFMC可达性

Deployments Upgrades Health Tasks Show Notifications

1 total 0 running 1 success 0 warnings 0 failures

FTD Rollback triggered from device is successful.

[Show deployment history](#)

图 5.SFMC消息确认从SFTD回滚

第 5 步：恢复SFMC访问权限后，请解决SFMC配置问题并重新部署。

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy admin **SECURE**

ACP-FTD Enter Description Try New UI Layout Analyze Hit Counts Save Cancel

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy Inheritance Settings | Policy Assignments (1) SSL Policy: None Identity Policy: None

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action						
Mandatory - ACP-FTD (1-2)																				
1	FMC-Access	outside	inside	Any	10.0.0.2	Any	Any	Any	Any	SSH HTTPS	Any	Any	Any	Allow						
2	FMC DMZ	dmz	inside	Any	10.0.0.2	Any	Any	Any	Any	HTTPS SSH	Any	Any	Any	Allow						
Default - ACP-FTD (-)																				

There are no rules in this section. [Add Rule](#) or [Add Category](#)

图 6.恢复更改

故障排除

如果回滚失败，请与Cisco TAC联系，有关过程中出现的其他问题，请查看以下文章：

· [部署回滚](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。