

SFMC에 연결할 수 없을 때 SFTD에서 롤백 구성

목차

- [소개](#)
 - [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
 - [배경 정보](#)
 - [구성](#)
 - [네트워크 다이어그램](#)
 - [시나리오](#)
 - [절차](#)
 - [문제 해결](#)
-

소개

이 문서에서는 SFTD와의 연결에 영향을 주는 보안 SFMC에서 구축 변경을 롤백하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

firepower 이 기능은 Secure Monitoring Threat Detection® 버전 6.7 이상에서 지원됩니다.

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SFMC(Secure Firewall Management Center®) 컨피그레이션
- Cisco Secure SFTD(Firepower 위협 방어) 컨피그레이션

사용되는 구성 요소

- Secure Firewall Management Center for VMware 버전 7.2.1
- Secure Firepower Threat Defense for VMware 버전 7.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

구축 변경이 네트워크 연결에 영향을 미칠 경우 SFMC, SFTD 또는 SFMC와 SFTD 간의 통신이 끊

기는 경우가 있습니다. SFTD의 컨피그레이션을 마지막으로 구축된 컨피그레이션으로 롤백하여 관리 연결을 복원할 수 있습니다.

위협 방어의 컨피그레이션을 마지막으로 구축된 컨피그레이션으로 롤백하려면 `configure policy rollback` 명령을 사용합니다.

 참고: `configure policy rollback` 명령이 버전 6.7에 도입되었습니다

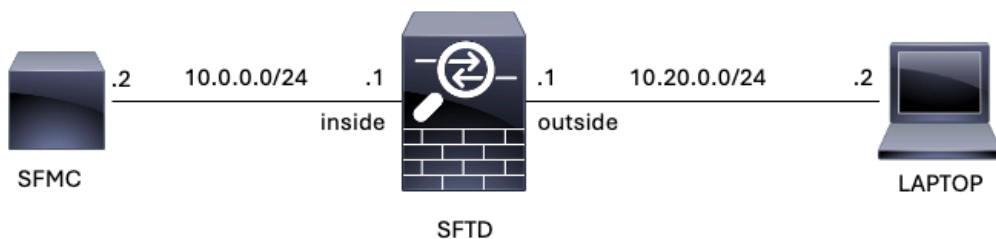
지침을 참조하십시오.

- 이전 구축만 위협 방어에서 로컬로 사용할 수 있으며, 이전 구축으로 롤백할 수 없습니다.
- Management Center 7.2 이상에서는고가용성을 위해 롤백이 지원됩니다.
- 클러스터링 구축에서는 롤백이 지원되지 않습니다.
- 롤백은 관리 센터에서 설정할 수 있는 컨피그레이션에만 영향을 줍니다. 예를 들어, 롤백은 전용 관리 인터페이스와 관련된 로컬 컨피그레이션에는 영향을 주지 않으며, 이는 위협 방어 CLI에서만 구성할 수 있습니다. 마지막 관리 센터 구축 후 `configure network management-data-interface` 명령을 사용하여 데이터 인터페이스 설정을 변경한 다음 `rollback` 명령을 사용하면 이러한 설정은 유지되지 않으며 마지막으로 구축된 관리 센터 설정으로 롤백됩니다.
- UCAPL/CC 모드는 롤백할 수 없습니다.
- 이전 배포 중에 업데이트된 대역외 SCEP 인증서 데이터는 롤백할 수 없습니다.
- 롤백 중에 현재 컨피그레이션이 지워져 연결이 끊어질 수 있습니다.

구성

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



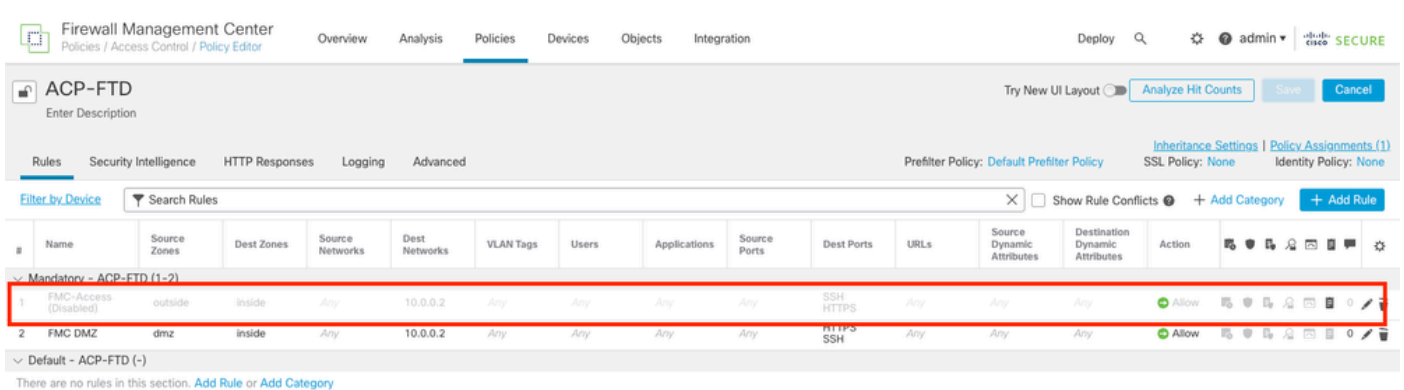
이미지 1. 다이어그램

시나리오

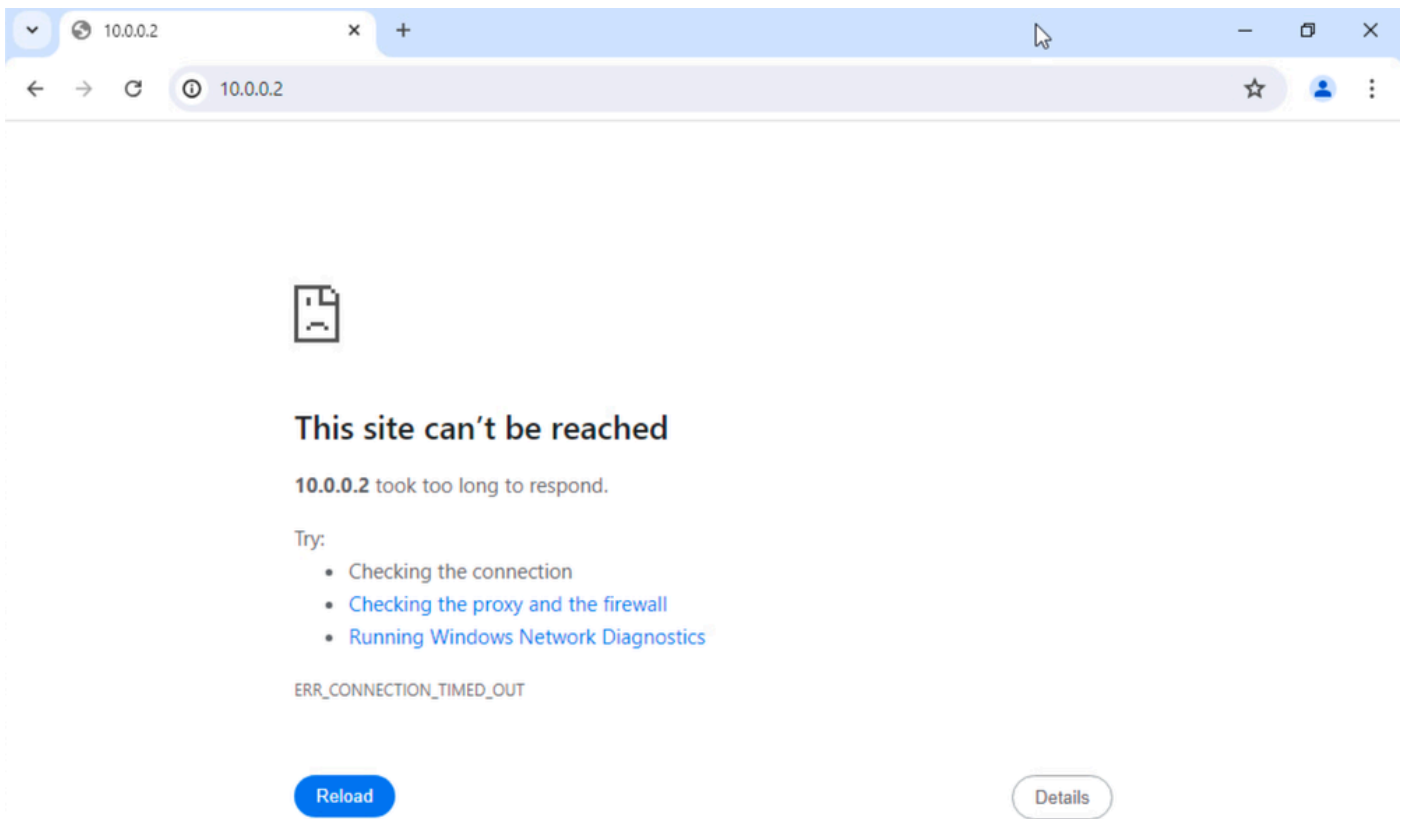
이 컨피그레이션에서는 SFTD가 방화벽 내부 인터페이스를 사용하여 SFMC에 의해 관리됩니다. 여기에는 랩톱에서 SFMC로의 연결을 허용하는 규칙이 있습니다.

절차

1단계. SFMC에서 FMC-Access라는 규칙이 비활성화되었습니다. 구축 후에는 랩톱에서 SFMC로의 통신이 차단됩니다.




이미지 2. SFMC 연결 기능을 사용하지 않도록 설정하는 규칙



이미지 3. 노트북 컴퓨터에서 SFMC 연결 불가

2단계. SSH 또는 콘솔을 통해 SFTD에 로그인한 다음 `configure policy rollback` 명령을 사용합니다.

 참고: SSH를 통한 액세스가 불가능한 경우 텔넷을 통해 연결합니다.

<#root>

>

configure policy rollback

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

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)?

3단계. 마지막 구축의 롤백을 확인하려면 YES를 쓴 다음 롤백 프로세스가 끝날 때까지 기다립니다.

<#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

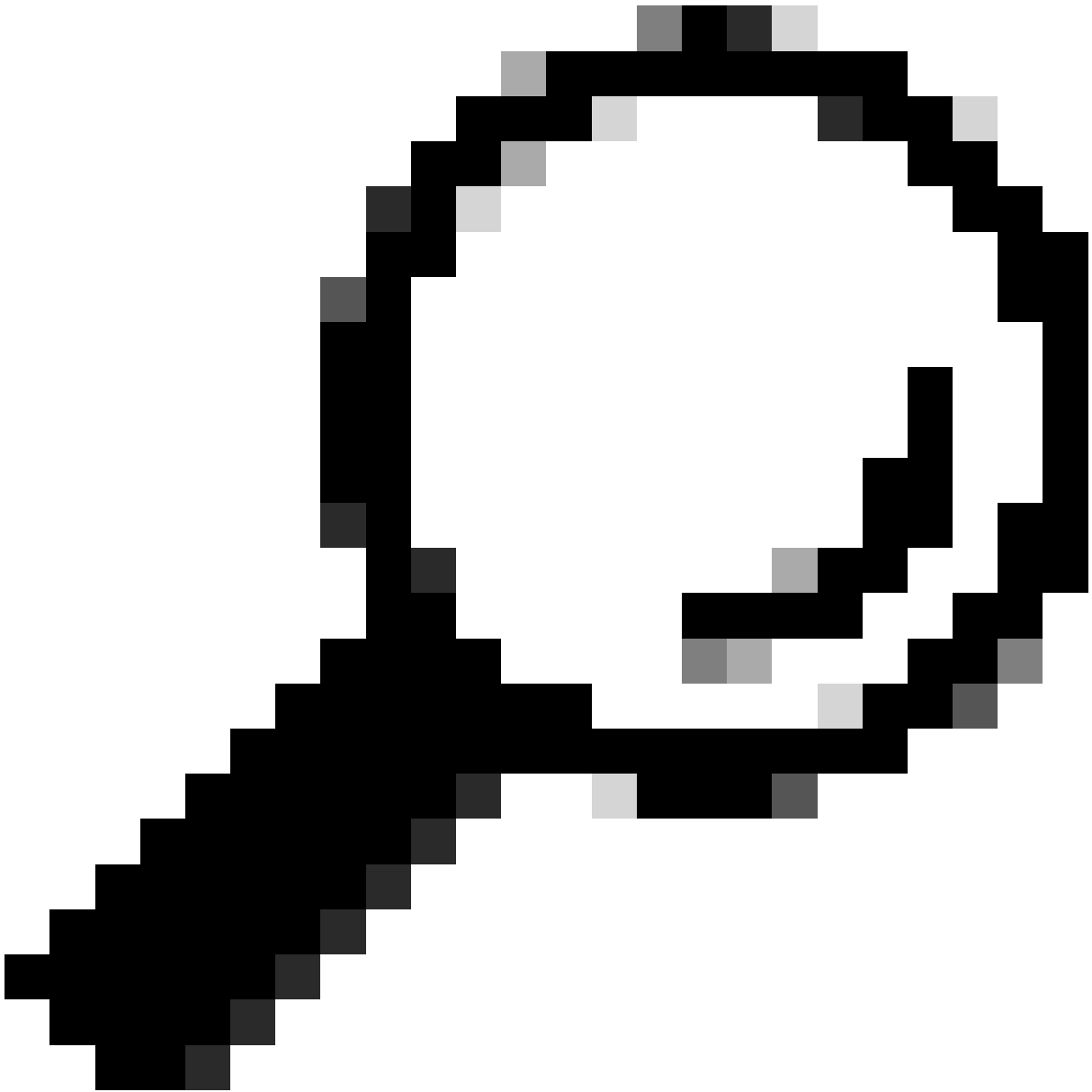
Commit Lina File Configuration. Status: success

Finalizing policy configuration on the device. Status: success

=====

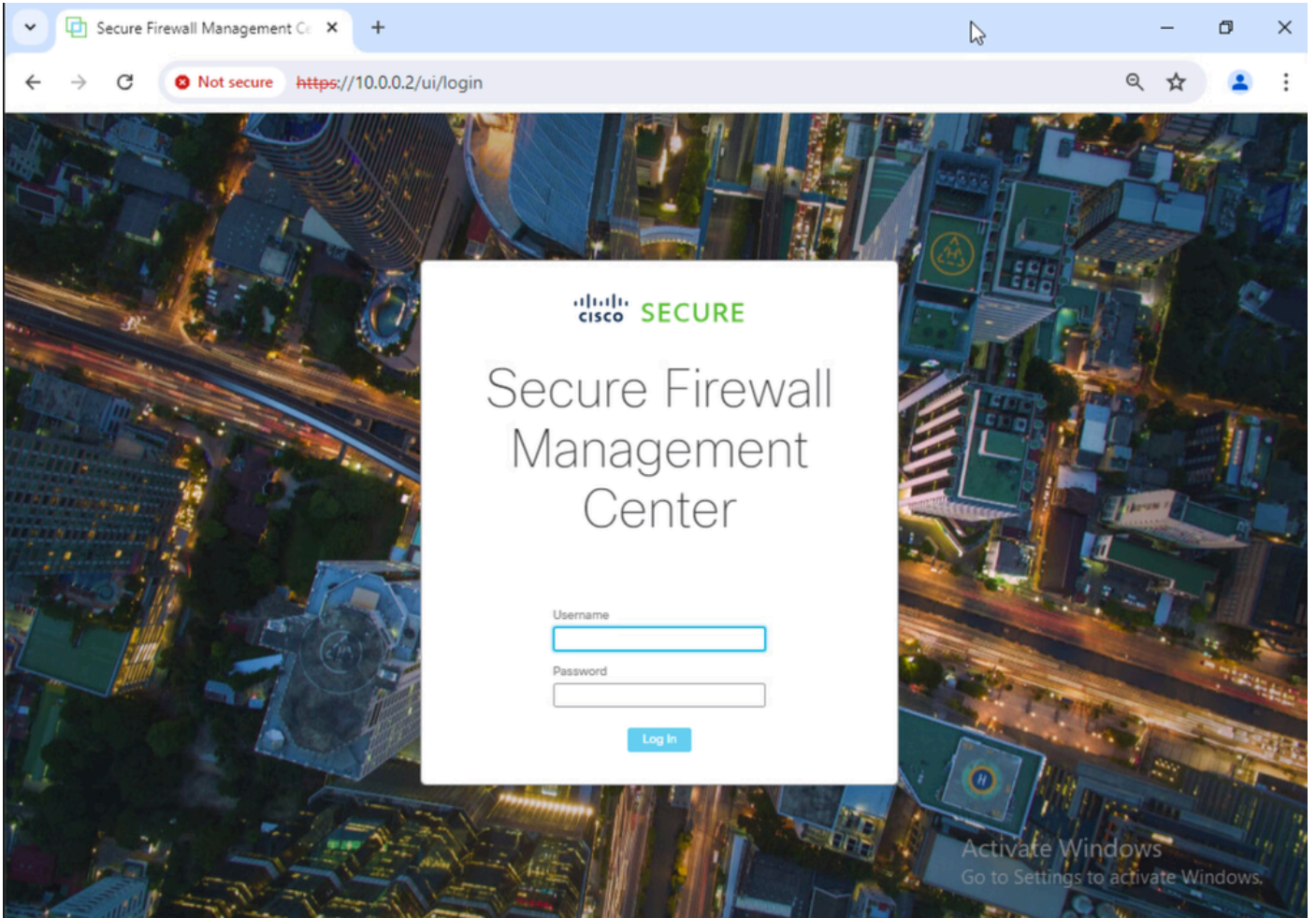
POLICY ROLLBACK STATUS: SUCCESS

=====



팁: 롤백이 실패할 경우 Cisco TAC에 문의하십시오.

4단계. 롤백 후 SFMC 연결성을 확인합니다. SFTD는 롤백이 성공적으로 완료되었음을 SFMC에 알립니다. SFMC에서 구축 화면에는 컨피그레이션이 롤백되었음을 알리는 배너가 표시됩니다.



이미지 4. 랩톱에서 SFMC 연결 복원됨

FTD Rollback triggered from device is successful.

[Show deployment history](#)

이미지 5. SFTD에서 롤백을 확인하는 SFMC 메시지

5단계. SFMC 액세스가 복원되면 SFMC 컨피그레이션 문제를 해결하고 재구축합니다.

#	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	Tools
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	Tools
2	FMC DMZ	dmz	inside	Any	10.0.0.2	Any	Any	Any	Any	HTTPS SSH	Any	Any	Any	Allow	Tools
Default - ACP-FTD (-)															

이미지 6. 변경 내용 되돌리기

문제 해결

롤백이 실패할 경우 Cisco TAC에 연락하여 프로세스 중 추가 문제에 대해 다음 문서를 검토하십시오.

· [구축 롤백](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.