

Terugdraaiing op SFTD configureren wanneer SFMC niet bereikbaar is

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Scenario](#)

[Procedure](#)

[Probleemoplossing](#)

Inleiding

Dit document beschrijft hoe u een implementatiewijziging van het beveiligde SFMC kunt terugdraaien die van invloed is op de connectiviteit met SFTD.

Voorwaarden

Vereisten

Het gebruik van deze functie wordt vanaf versie 6.7 ondersteund bij Secure FirePOWER Threat Detection®.

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van Secure Firewall Management Center (SFMC®)
- Cisco Secure FirePOWER Threat Defence (SFTD)-configuratie

Gebruikte componenten

- Secure Firewall Management Center voor VMware versie 7.2.1
- Secure Firepower Threat Defense voor VMware versie 7.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Er zijn scenario's waarbij de communicatie naar SFMC, SFTD of tussen SFMC en SFTD verloren gaat wanneer een implementatiewijziging de netwerkconnectiviteit beïnvloedt. U kunt de configuratie op de SFTD terugdraaien naar de laatst geïmplementeerde configuratie om de beheerconnectiviteit te herstellen.

Gebruik het commando `Configure policy rollback` om de configuratie op de bedreigingsverdediging terug te draaien naar de laatst gebruikte configuratie.

 **Opmerking:** de opdracht `configureer beleid terugdraaien` is geïntroduceerd in versie 6.7

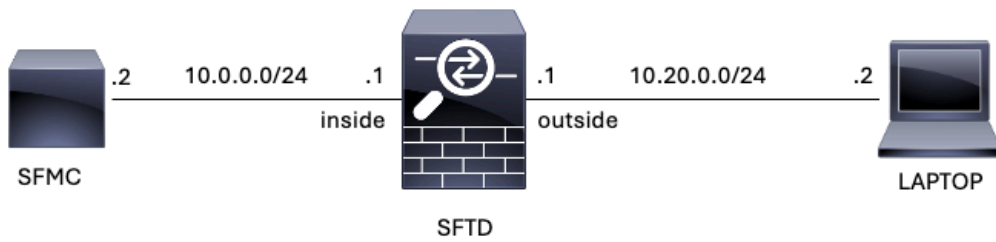
Zie de richtsnoeren:

- Slechts is de vorige plaatsing beschikbaar plaatselijk op de bedreigingsdefensie; u kunt niet terug naar om het even welke vroegere plaatsingen rollen.
- Rollback wordt ondersteund voor hoge beschikbaarheid vanaf management center 7.2.
- Rollback wordt niet ondersteund voor clustering-implementaties.
- Het terugdraaien heeft alleen invloed op configuraties die u in het beheercentrum kunt instellen. Het terugdraaien heeft bijvoorbeeld geen invloed op lokale configuratie die gerelateerd is aan de speciale Management interface, die u alleen kunt configureren bij de bedreigingsverdediging CLI. Merk op dat als u de instellingen van de gegevensinterface na de laatste implementatie van het beheercentrum hebt veranderd met behulp van het commando `configureren netwerkbeheer-data-interface`, en u vervolgens de opdracht `terugdraaien` gebruikt, die instellingen niet worden behouden; ze rollen terug naar de laatste instellingen van het beheercentrum.
- De UCAPL/CC-modus kan niet worden gerold.
- Out-of-band SCEP-certificaatgegevens die tijdens de vorige implementatie zijn bijgewerkt, kunnen niet worden gewist.
- Tijdens het terugdraaien kunnen de verbindingen dalen omdat de huidige configuratie is gewist.

Configureren

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Afbeelding 1. Diagram

Scenario

In deze configuratie wordt SFTD beheerd door de SFMC met behulp van de Firewall binneninterface, is er een regel die de bereikbaarheid van de Laptop aan SFMC toestaat.

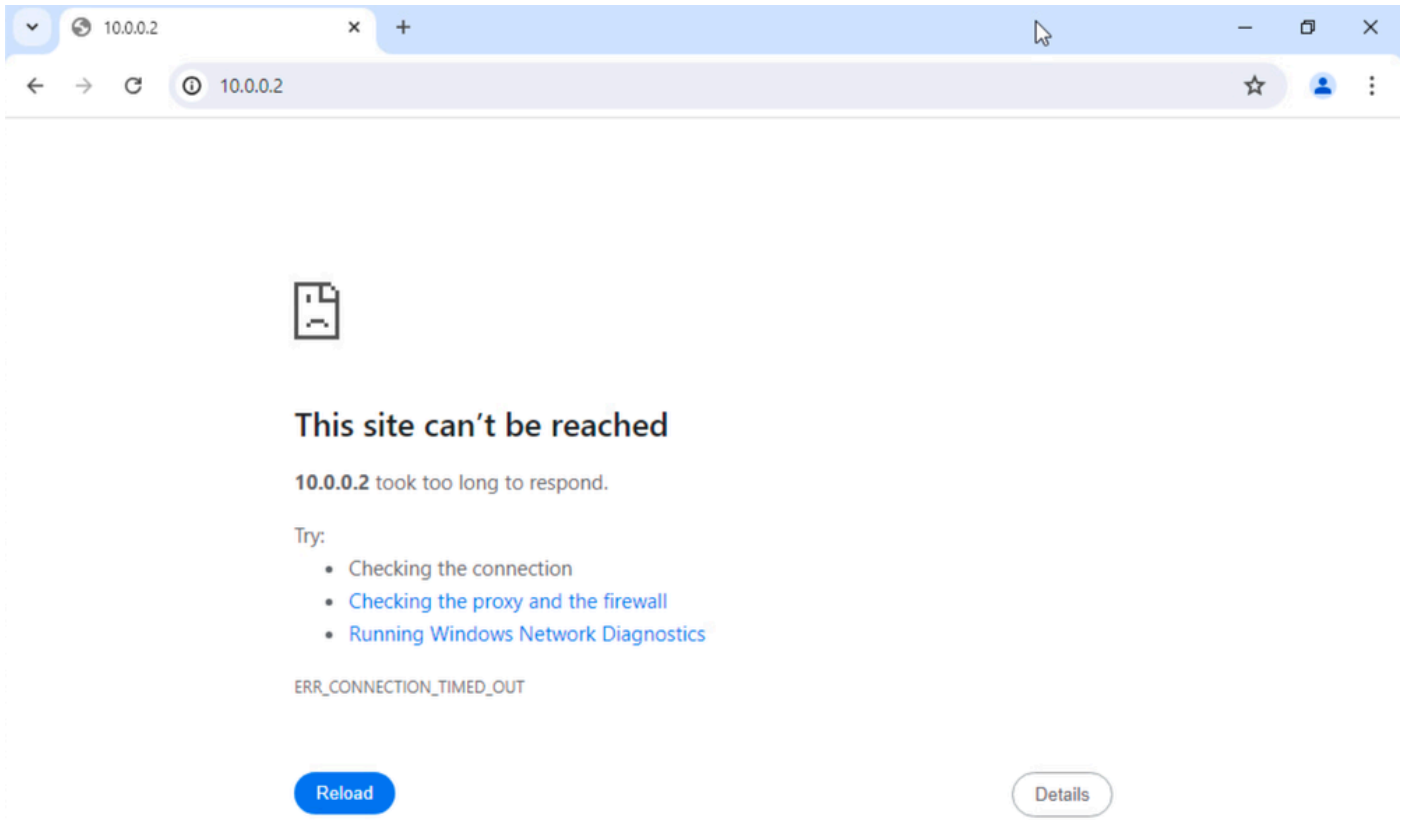
Procedure

Stap 1. De regel met de naam FMC-Access is uitgeschakeld op het SFMC, nadat de communicatie van de laptop naar het SFMC is geblokkeerd.

The screenshot shows the 'Policies' tab in the Firewall Management Center. The main heading is 'ACP-FTD'. Below the heading, there are tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. The 'Rules' tab is active. A search bar and 'Filter by Device' option are visible. Below the search bar is a table of rules. The first rule, 'FMC-Access (Disabled)', is highlighted with a red box. The second rule is 'FMC DMZ'. The table has columns for Name, Source Zones, Dest Zones, Source Networks, Dest Networks, VLAN Tags, Users, Applications, Source Ports, Dest Ports, URLs, Source Dynamic Attributes, Destination Dynamic Attributes, and Action.

#	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
1	FMC-Access (Disabled)	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	HTTP, SSH	Any	Any	Any	Allow

Afbeelding 2. De regel die SFMC-bereikbaarheid uitschakelt



Afbeelding 3. SFMC Bereikbaarheid van laptop werkt niet

Stap 2. Log in op de SFTD via SSH of console en gebruik vervolgens de opdracht Configure policy rollback.

 **Opmerking:** als toegang via SSH niet mogelijk is, sluit u een verbinding aan via telnet.

```
<#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)?

Stap 3. Schrijf het woord JA om het terugdraaien van de laatste implementatie te bevestigen en wacht vervolgens tot het terugdraaiproces is afgelopen.

<#root>

Do you want to continue (YES/NO)?

YES

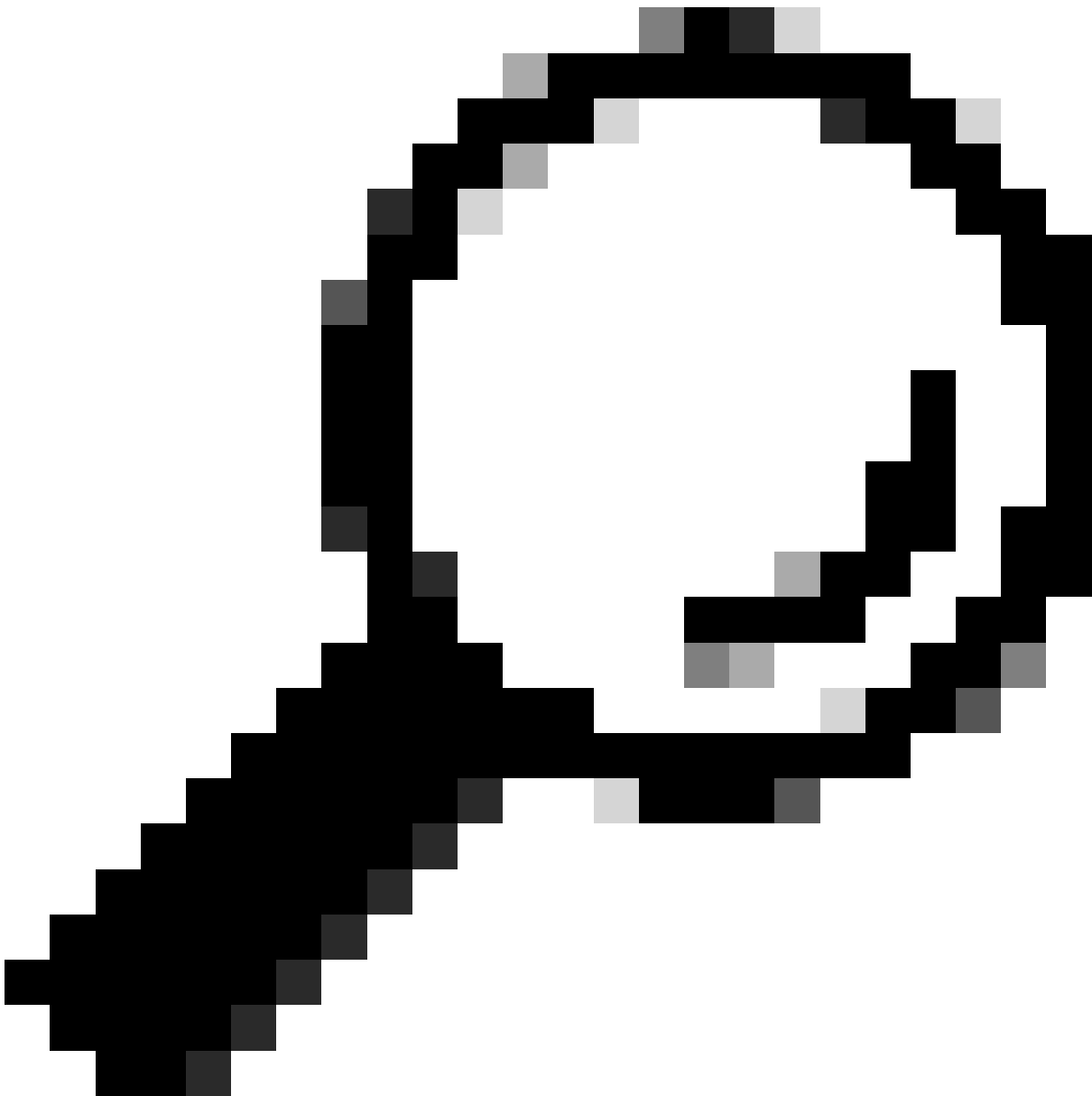
Starting rollback...

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

=====

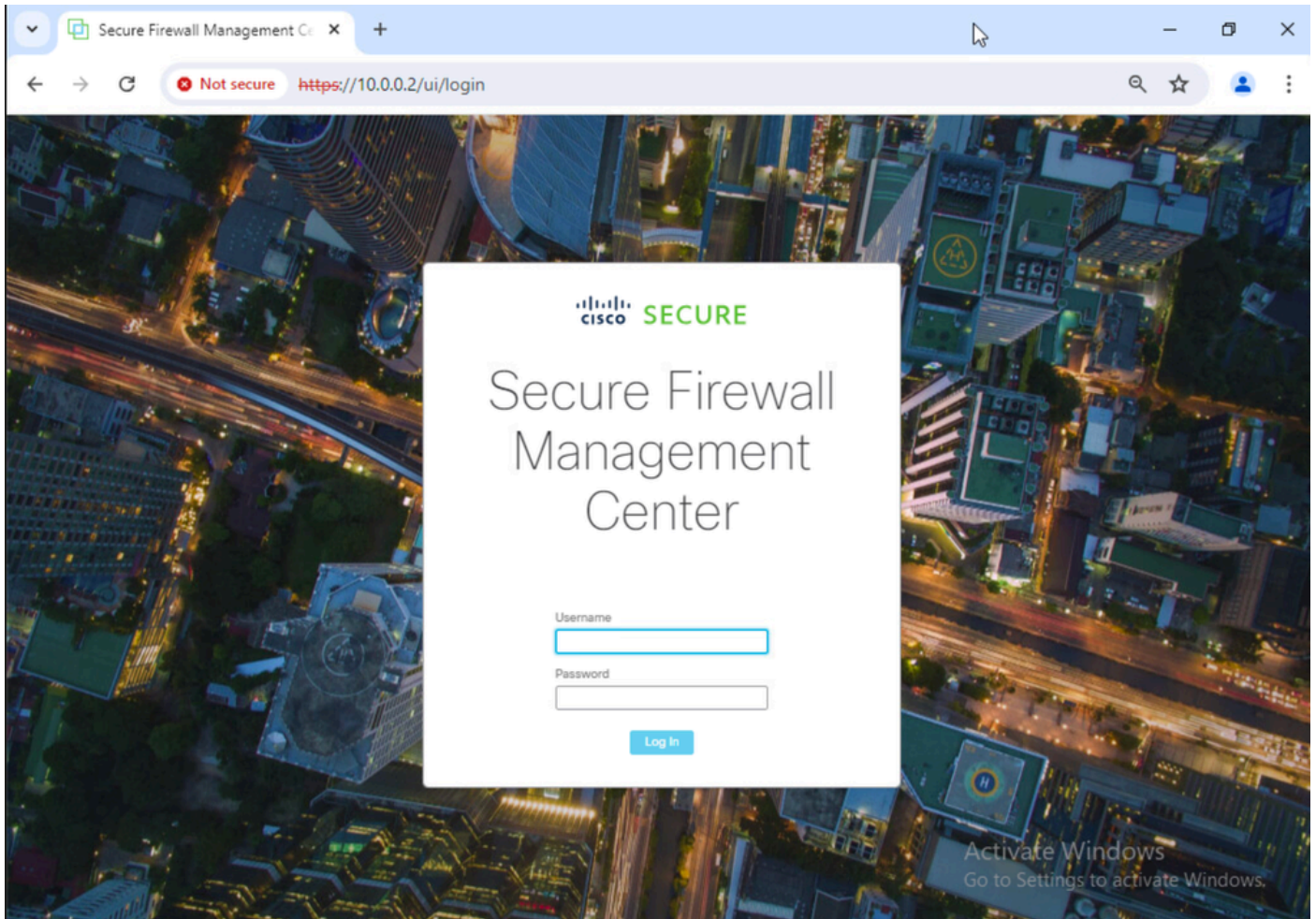
POLICY ROLLBACK STATUS: SUCCESS

=====



Tip: indien terugdraaien mislukt, neem contact op met Cisco TAC

Stap 4. Bevestig na het terugdraaien de SFMC-bereikbaarheid. De SFTD meldt de SFMC dat het terugdraaien met succes is voltooid. In het SFMC toont het implementatiescherm een banner die aangeeft dat de configuratie is gerold.



Afbeelding 4. SFMC-bereikbaarheid vanaf laptop hersteld

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](#)

Afbeelding 5. SFMC-bericht ter bevestiging van terugdraaiing van SFTD

Stap 5. Wanneer de SFMC-toegang is hersteld, lost u het probleem met de SFMC-configuratie op en herimplementeert u het.

Firewall Management Center Policies / Access Control / Policy Editor 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	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 (-)															

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

Afbeelding 6. De wijzigingen terugdraaien

Probleemoplossing

Als het terugdraaien mislukt, neemt u contact op met Cisco TAC. Bekijk het volgende artikel voor extra problemen tijdens het proces:

· [Terugdraaiing van implementaties](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.