

Configurar reversão no SFTD quando o SFMC não estiver acessível

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Cenário](#)

[Procedimento](#)

[Troubleshooting](#)

Introdução

Este documento descreve como reverter uma alteração de implantação do SFMC seguro que afeta a conectividade ao SFTD.

Pré-requisitos

Requisitos

O uso desse recurso é suportado no Secure FirePOWER Threat Detection® versão 6.7 em diante.

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Secure Firewall Management Center (SFMC®)
- Configuração do Cisco Secure FirePOWER Threat Defense (SFTD)

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Há situações em que a comunicação com o SFMC, o SFTD ou entre o SFMC e o SFTD é perdida quando uma alteração de implantação afeta a conectividade da rede. Você pode reverter a configuração no SFTD para a última configuração implantada para restaurar a conectividade de gerenciamento.

Use o comando `configure policy rollback` para reverter a configuração na defesa contra ameaças para a última configuração implantada.



Observação: o comando `configure policy rollback` foi introduzido na versão 6.7

Consulte as diretrizes:

- Somente a implantação anterior está disponível localmente na defesa contra ameaças; não é possível reverter para implantações anteriores.
- A reversão é suportada para alta disponibilidade a partir do centro de gerenciamento 7.2.
- A reversão não tem suporte para implantações de clustering.
- A reversão afeta apenas as configurações que podem ser definidas no centro de gerenciamento. Por exemplo, a reversão não afeta nenhuma configuração local relacionada à interface de gerenciamento dedicada, que você pode configurar somente na CLI de defesa contra ameaças. Observe que, se você alterou as configurações da interface de dados após a última implantação do centro de gerenciamento usando o comando `configure network management-data-interface`, e depois você usa o comando `rollback`, essas configurações não serão preservadas; elas reverterem para as últimas configurações do centro de gerenciamento implantado.
- O modo UCAPL/CC não pode ser revertido.
- Os dados do certificado SCEP fora de banda que foram atualizados durante a implantação anterior não podem ser revertidos.
- Durante a reversão, as conexões podem ser interrompidas porque a configuração atual foi limpa.

Configurar

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

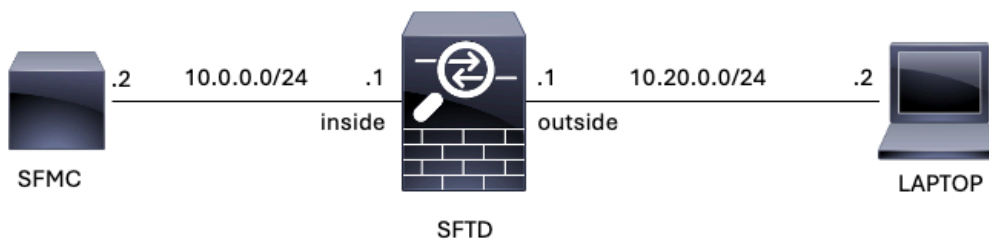


Imagem 1. Diagrama

Cenário

Nessa configuração, o SFTD é gerenciado pelo SFMC usando a interface interna do Firewall. Há uma regra que permite o acesso do Laptop ao SFMC.

Procedimento

Etapa 1. A regra FMC-Access foi desativada no SFMC. Após a implantação, a comunicação do Laptop com o SFMC é bloqueada.

The screenshot shows the 'Policies' page in the Firewall Management Center. The page title is 'ACP-FTD'. Below the title, there are tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. The 'Rules' tab is selected. 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 columns include 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

Imagem 2. A regra que permite a acessibilidade do SFMC desativada

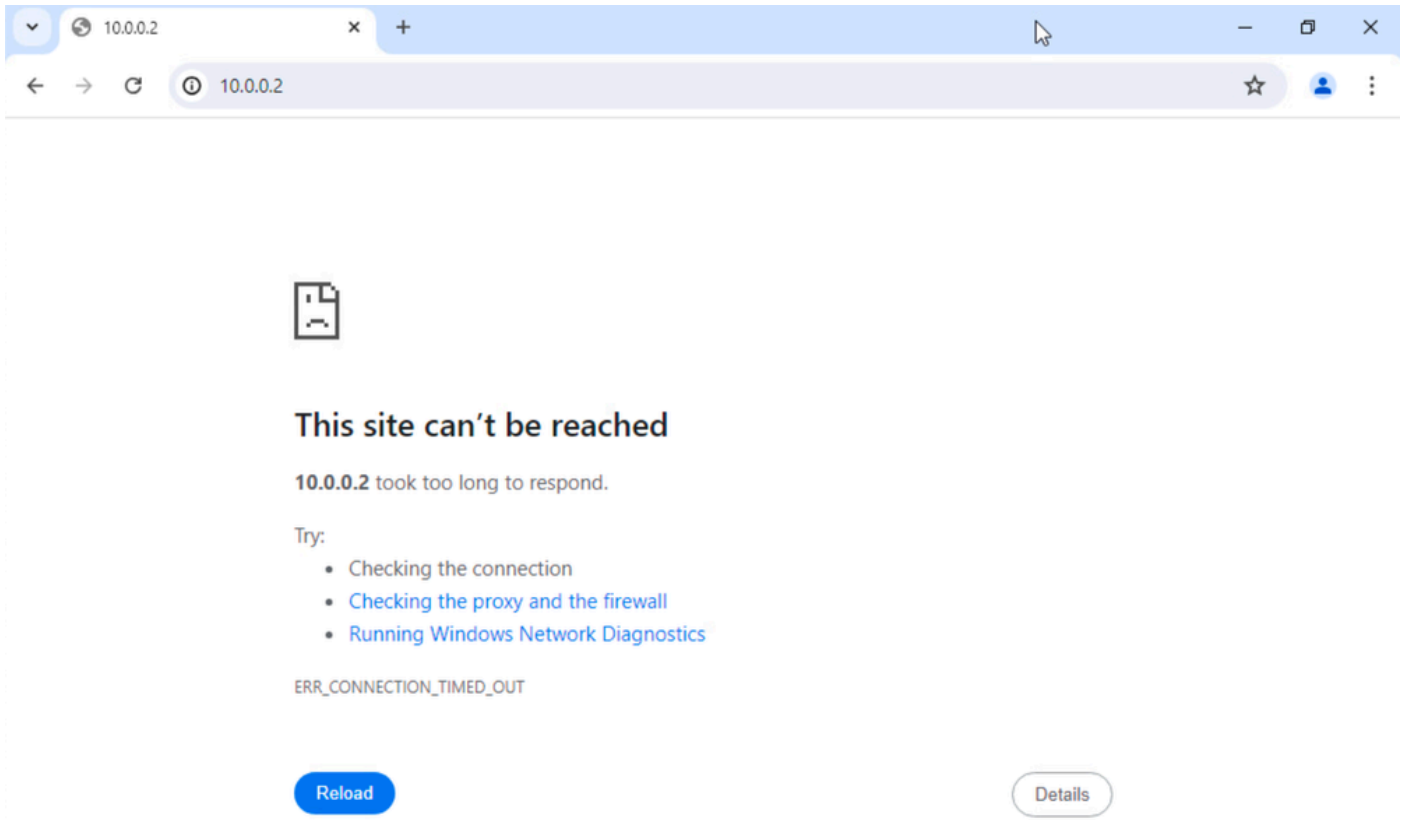


Imagem 3. Alcance do SFMC do notebook não está funcionando

Etapa 2. Efetue login no SFTD via SSH ou console e, em seguida, use o comando `configure policy rollback`.

 Observação: se o acesso via SSH não for possível, conecte via telnet.

```
<#root>
```

```
>
```

```
configure policy rollback
```

```
-----  
[Warning] Perform a policy rollback if the FTD communicates with the FMC on a data interface, and it has  
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)?

Etapa 3. Escreva a palavra YES para confirmar a reversão da última implantação e, em seguida, aguarde até que o processo de reversão termine.

<#root>

Do you want to continue (YES/NO)?

YES

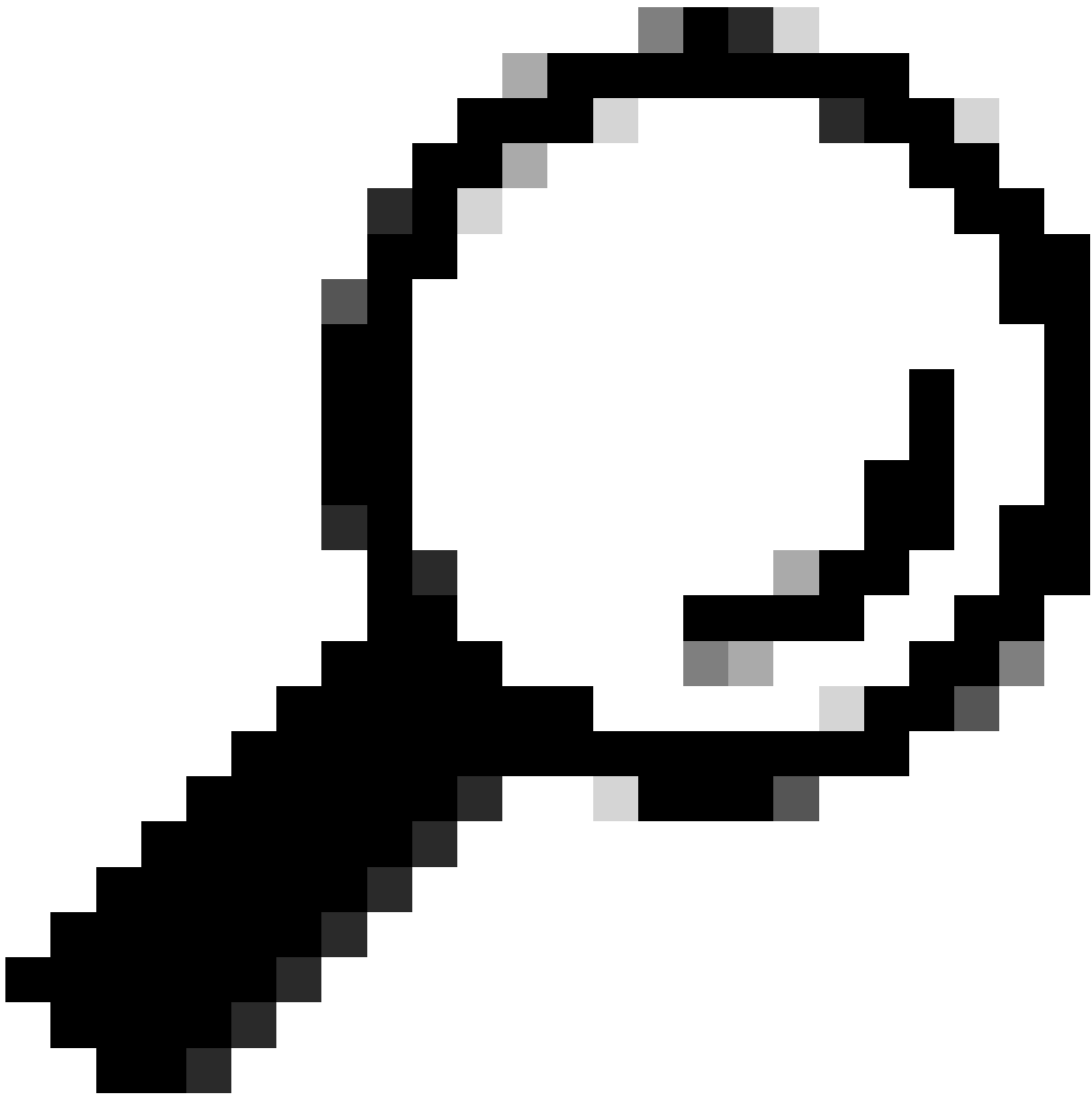
Starting rollback...

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

=====



Dica: em caso de falha na reversão, entre em contato com o TAC da Cisco

Etapa 4. Após a reversão, confirme a acessibilidade do SFMC. O SFTD notifica o SFMC de que a reversão foi concluída com êxito. No SFMC, a tela de implantação mostra um banner informando que a configuração foi revertida.

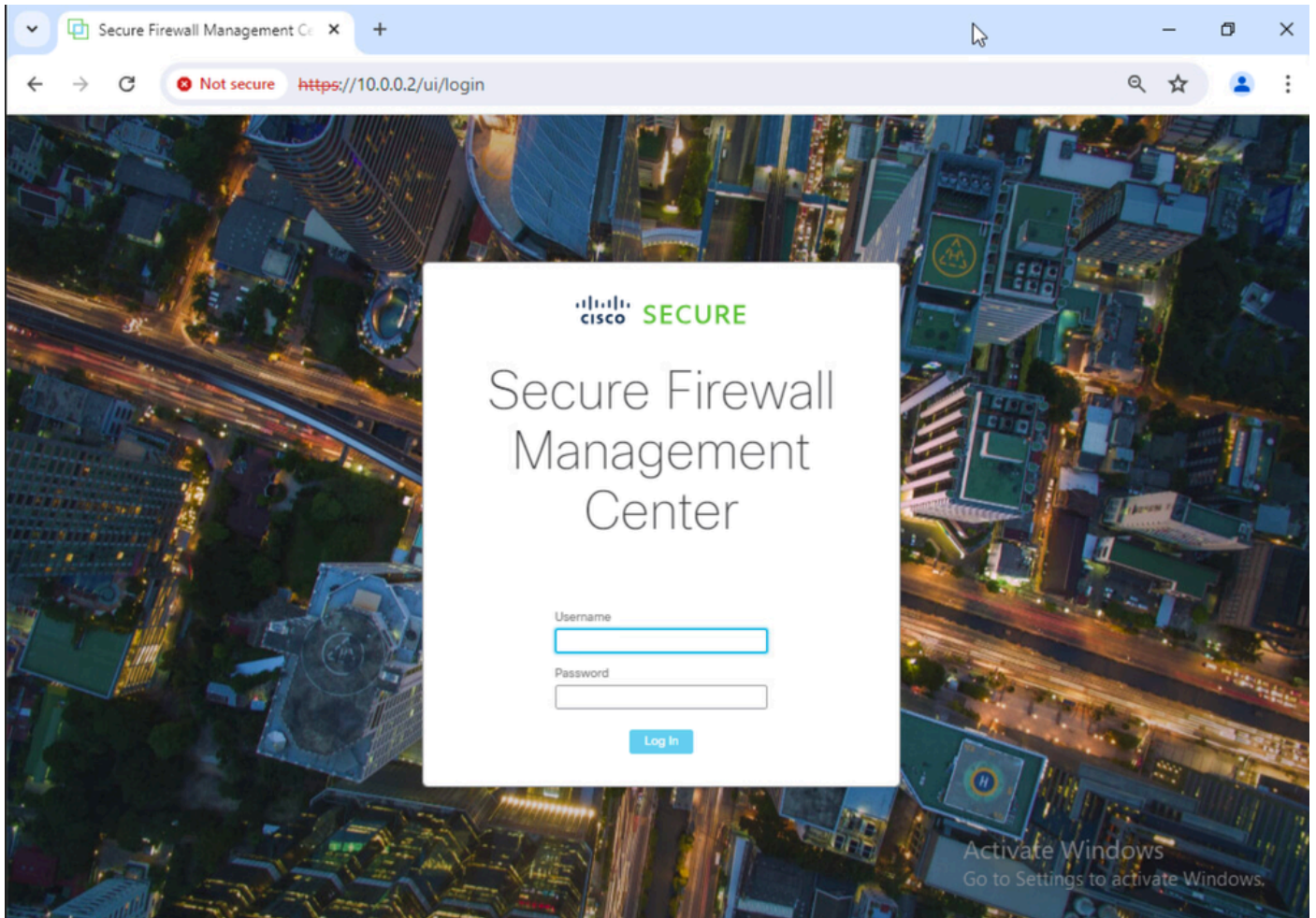


Imagem 4. Alcance do SFMC do notebook restaurado

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](#)

Imagem 5. Mensagem do SFMC confirmando reversão do SFTD

Etapa 5. Quando o acesso ao SFMC for restaurado, resolva o problema de configuração do SFMC e reimplante.

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](#)

Imagem 6. Reverter as alterações

Troubleshooting

Caso a reversão falhe, entre em contato com o TAC da Cisco, para problemas adicionais durante o processo, leia o próximo artigo:

· [Reversão da implantação](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.