

Configura rollback su SFTD quando SFMC non è raggiungibile

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Scenario](#)

[Procedura](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come eseguire il rollback di una modifica della distribuzione da SFMC protetto che influisce sulla connettività a SFTD.

Prerequisiti

Requisiti

L'uso di questa funzione è supportato a partire dalla versione 6.7 di Secure FirePOWER Threat Detection®.

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Secure Firewall Management Center (SFMC®)
- Configurazione Cisco Secure FirePOWER Threat Defense (SFTD)

Componenti usati

- Secure Firewall Management Center per VMware versione 7.2.1
- Secure Firepower Threat Defense per VMware versione 7.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In alcuni scenari la comunicazione con SFMC, SFTD o tra SFMC e SFTD viene persa quando una modifica della distribuzione influisce sulla connettività di rete. È possibile eseguire il rollback della configurazione nell'SFTD all'ultima configurazione distribuita per ripristinare la connettività di gestione.

Utilizzare il comando `configure policy rollback` per eseguire il rollback della configurazione nella difesa dalle minacce all'ultima configurazione distribuita.



Nota: il comando `configure policy rollback` è stato introdotto nella versione 6.7

Vedere le linee guida:

- Solo la distribuzione precedente è disponibile localmente nella difesa contro le minacce; non è possibile eseguire il rollback a distribuzioni precedenti.
- Il rollback è supportato per l'elevata disponibilità dal centro di gestione 7.2 in poi.
- Il rollback non è supportato per le distribuzioni di clustering.
- Il rollback influisce solo sulle configurazioni che è possibile impostare nel centro di gestione. Ad esempio, il rollback non influisce sulle configurazioni locali relative all'interfaccia di gestione dedicata, che è possibile configurare solo nella CLI di difesa dalle minacce. Si noti che se dopo l'ultima distribuzione del centro di gestione sono state modificate le impostazioni dell'interfaccia dati utilizzando il comando `configure network management-data-interface` e quindi si utilizza il comando `rollback`, tali impostazioni non verranno mantenute e verranno ripristinate alle ultime impostazioni del centro di gestione distribuite.
- Non è possibile eseguire il rollback della modalità UCAPL/CC.
- Impossibile eseguire il rollback dei dati del certificato SCEP fuori banda aggiornati durante la distribuzione precedente.
- Durante il rollback, le connessioni possono interrompersi perché la configurazione corrente viene cancellata.

Configurazione

Esempio di rete

Il documento usa la seguente configurazione di rete:

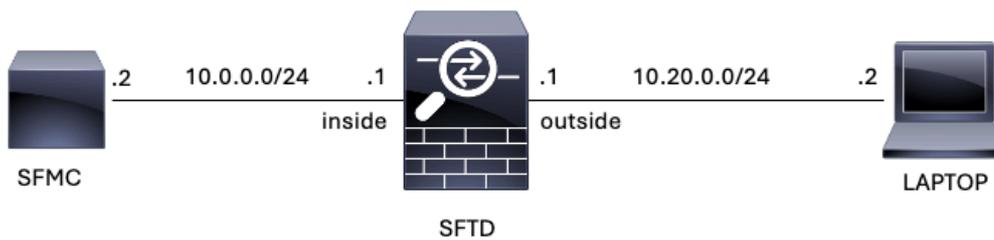


Immagine 1. Diagramma

Scenario

In questa configurazione, SFTD viene gestito dall'SFMC utilizzando l'interfaccia interna del firewall, esiste una regola che consente la raggiungibilità dal notebook all'SFMC.

Procedura

Passaggio 1. La regola denominata FMC-Access è stata disabilitata in SFMC. Dopo la distribuzione, la comunicazione tra il laptop e SFMC viene bloccata.

The screenshot shows the 'Policies' section of 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 active. A search bar is present with the text 'Filter by Device' and 'Search Rules'. Below the search bar, there is a table of rules. 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. Two rules are listed under the 'Mandatory - ACP-FTD (1-2)' section:

| # | 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 |

The first rule, 'FMC-Access (Disabled)', is highlighted with a red border. Below the table, there is a section for 'Default - ACP-FTD (-)' with the text 'There are no rules in this section. Add Rule or Add Category'.

Immagine 2. Regola che consente di disabilitare la raggiungibilità di SFMC

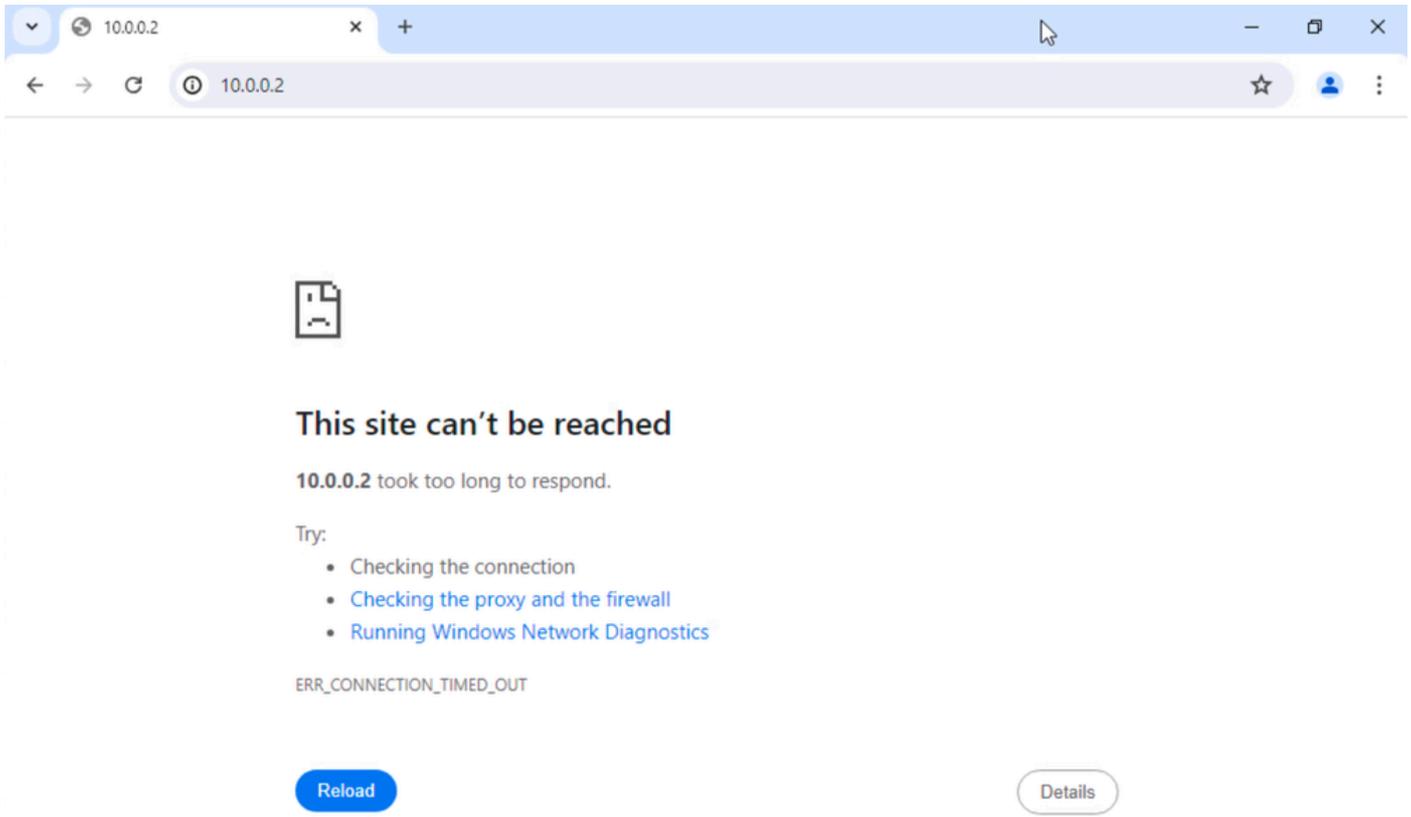


Immagine 3. Raggiungibilità di SFMC dal notebook non funzionante

Passaggio 2. Accedere all'SFTD tramite SSH o la console, quindi usare il comando `configure policy rollback`.

 Nota: se non è possibile accedere tramite SSH, collegarsi in modalità 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)?

Passaggio 3. Scrivere la parola YES per confermare il rollback dell'ultima distribuzione, quindi attendere il termine del processo di rollback.

<#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

=====



Suggerimento: se il rollback non riesce, contattare Cisco TAC

Passaggio 4. Dopo il rollback, verificare la raggiungibilità di SFMC. L'SFTD notifica all'SFMC che il rollback è stato completato. Nella schermata di distribuzione di SFMC viene visualizzato un banner che indica che è stato eseguito il rollback della configurazione.

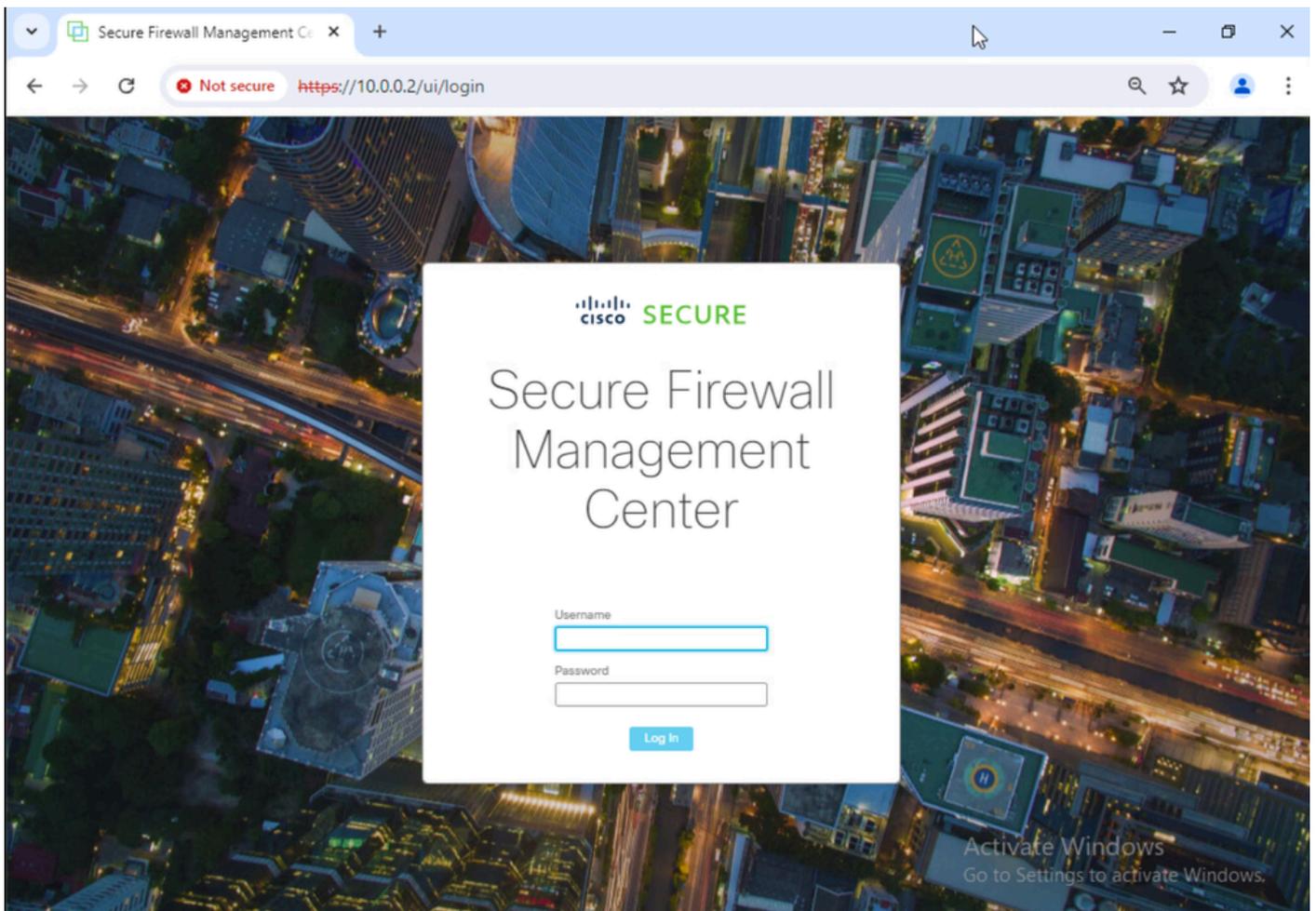


Immagine 4. Raggiungibilità di SFMC dal notebook ripristinato

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](#)

Immagine 5. Messaggio SFMC di conferma del rollback da SFTD

Passaggio 5. Una volta ripristinato l'accesso a SFMC, risolvere il problema di configurazione di SFMC e ridistribuirlo.

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 | 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 | | | | | | | | | | | | | | | |

Immagine 6. Annulla le modifiche

Risoluzione dei problemi

Se il rollback non riesce, contattare Cisco TAC; per ulteriori problemi durante il processo, leggere l'articolo successivo:

· [Rollback dell'installazione](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).