變更FTD管理員存取資料介面

目錄

簡介

本檔案介紹變更安全防火牆威脅防禦(FTD)管理員存取資料介面的步驟。

必要條件

需求

- 基本產品知識。
- 熟悉資料介面上的FTD管理和管理。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

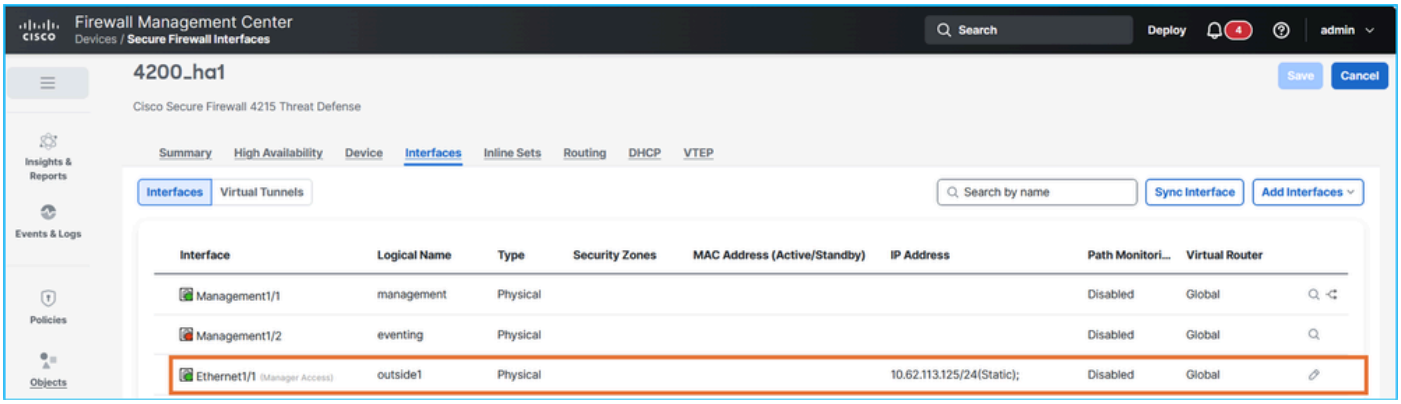
本文中的資訊係根據以下軟體和硬體版本：

- 安全防火牆4200

- 安全防火牆威脅防禦(FTD)10.0.x、7.6.4
- 安全防火牆管理中心(FMC)10.0.x

初始配置

1. FMC使用主用IP地址10.62.113.125和10.62.113.126分別透過名為nameif outside1的資料介面Ethernet1/1以高可用性(HA)方式管理FTD:



驗證FTD CLISH:

<#root>

>

show network management-data-interface

Physical Interface Name of the Interface

Ethernet1/1 outside1

>

show network

```
==============[ System Information ]==============
Hostname                : CSF4215-3
..
DNS from router         : enabled
Management port         : 8305
IPv4 Default route
```

```
  Gateway                : data-interfaces
…
======[ System Information - Data Interfaces ]======
DNS Servers              : 192.0.2.100

Interfaces               : Ethernet1/1



==================[

Ethernet1/1

 ]==================

State                    : Enabled
Link                     : Up

Name                     : outside1


MTU                      : 1500
MAC Address              : 40:F4:9F:3D:5A:0E

----------------------[ IPv4 ]----------------------



Configuration            : Manual



Address                  : 10.62.113.125



Netmask                  : 255.255.255.0



Gateway                  : 10.62.113.1

…
```

2.在FTD HA裝置和FMC之間建立SFTUNNEL連線：

<#root>

```
>

sftunnel-status-brief



PEER:fmc.example.org


        SFTunnel Status:-

                Channel A: Connected



                Channel B: Connected


        Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' v
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
        Registration: Completed.
        IPv4 Connection to peer 'fmc.example.org' Start Time: Fri Jul 17 08:22:31 2026 UTC
        Heartbeat Send Time:     Fri Jul 17 08:52:42 2026 UTC
        Heartbeat Received Time: Fri Jul 17 08:53:03 2026 UTC
        Last disconnect time   : Fri Jul 17 08:22:16 2026 UTC
        Last disconnect reason : Process shutdown due to stop request from PM
```

3. FTD依賴DNS解析來連線到FMC。管理器基於完全限定的域名(FQDN)進行配置：

```
<#root>

>

show managers


Type                      : Manager

Host                      : fmc.example.org



Display name              : fmc.example.org


Version                   : 10.0.1 (Build 1)
Identifier                : 6d86efc4-c095-11f0-9244-48f1a7894b18
Registration              : Completed
Management type           : Configuration and analytics
```

```
>

show network


===============[ System Information ]===============
Hostname                  : KSEC-FPR-4215-3

Domains                   : example.org



DNS Servers               : 192.0.2.100


DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
…
```

DNS伺服器可通過outside1介面訪問。

4.sftunnel連線是透過Lina引擎建立的：

<#root>

```
>

show conn all port 8305


26 in use, 32 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect


TCP nlp_int_tap  10.62.113.125(169.254.1.3):8305 outside1  198.51.100.23:45647, idle 0:00:03, bytes 2129



TCP nlp_int_tap  10.62.113.125(169.254.1.3):37141 outside1  198.51.100.23:8305, idle 0:00:04, bytes 1485
```

設定步驟

目標是將管理器訪問從當前outside1移動到目標outside2介面。active和standby outside2 IP地址分別為10.62.114.51/24和10.62.114.52/24。

請注意，FTD版本7.7.0或更高版本支援冗餘管理器訪問資料介面，允許配置和部署超過1個管理器訪問介面。低於7.7.0的版本不支援此功能。

因此，將跳過特定步驟或包含不同的操作。

⚠ 注意：請勿在任何步驟中從FMC中註銷/刪除FTD。

1. 建議使用FTD的控制台存取許可權：

- 對於Firepower 4100/9300，您可以使用SSH連線到機箱，然後使用connect module x console命令連線到本地FTD控制檯，其中x是插槽/安全模組ID。
- 在多例項(MI)模式下運行FTD的Firepower 4100/9300中，可以使用SSH連線到機箱，然後使用connect module x telnet 命令連線到本地FTD控制檯，其中x是插槽/安全模組ID。然後使用connect ftd <ftd_id> 命令連線到FTD例項。
- 在MI模式下的安全防火牆3100/4200中，可以使用SSH連線到機箱，然後使用connect ftd <identifier> 命令連線到FTD控制檯。

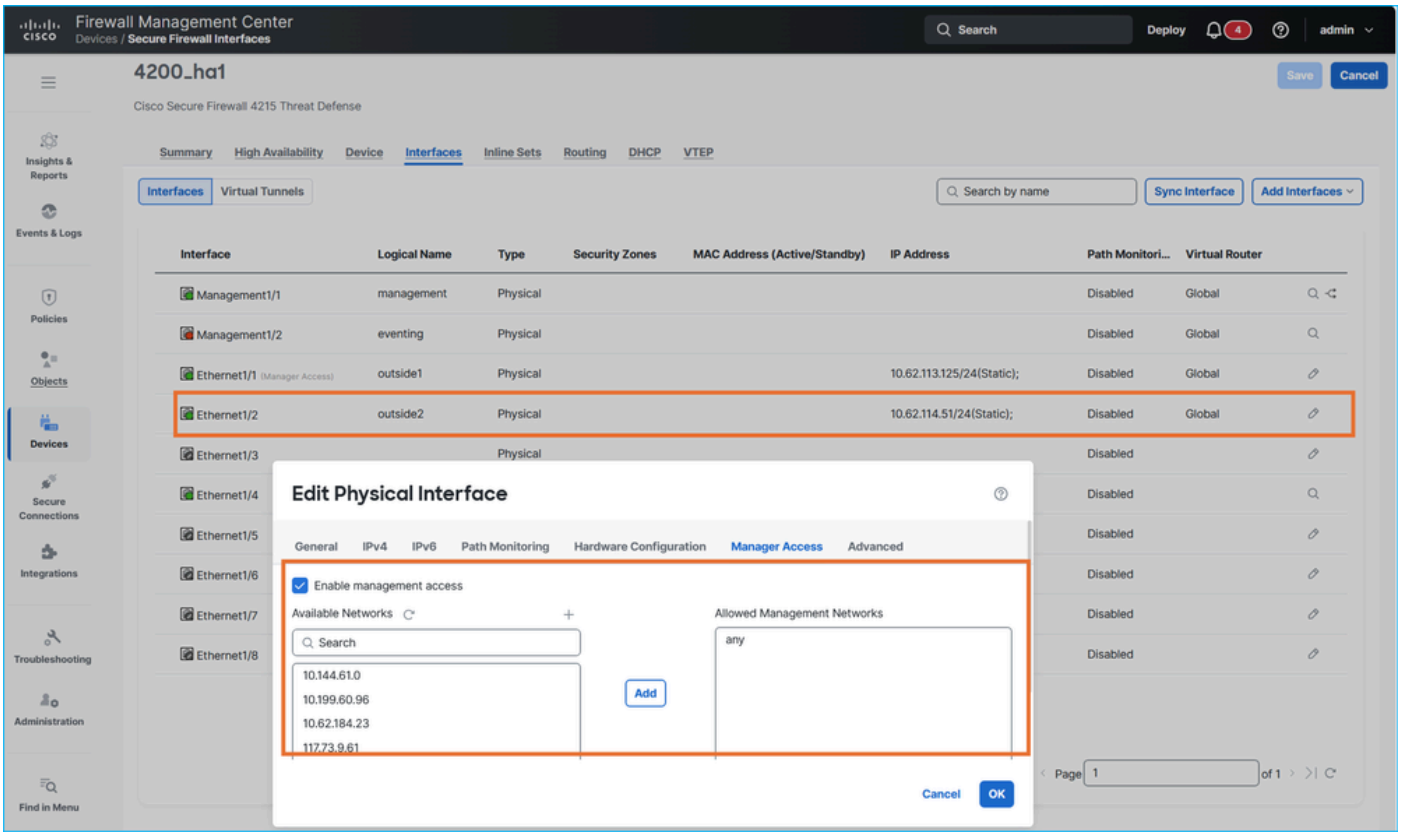
2. 部署掛起的策略。

3. 強烈建議進行FTD和FMC備份。在FTD HA的情況下，請備份兩個裝置。

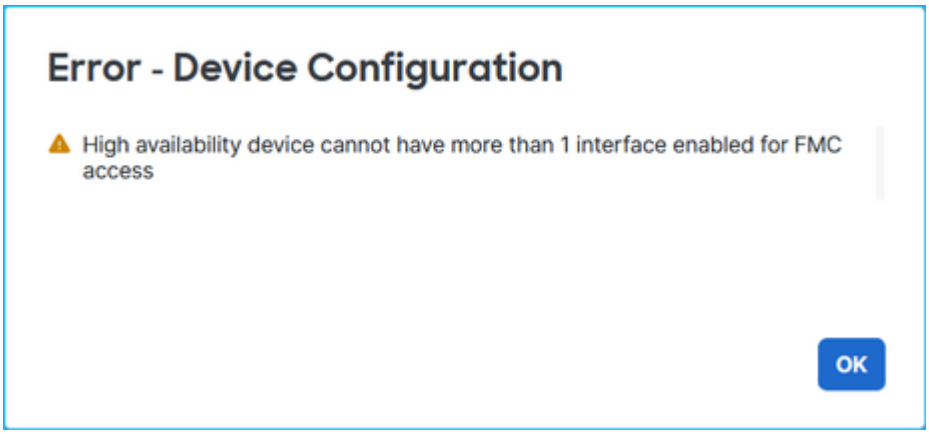
4. 配置目標介面名稱if、IP地址、安全區域和其他與介面相關的設定（如果適用）。

5. 配置目標介面備用IP地址。

6. 如果FTD軟體版本是7.7.0或更新版本，請在目標介面上啟用管理員存取並根據需要調整管理存取網路：



請注意，低於7.7.0的FTD版本不支援冗餘管理器訪問資料介面。嘗試配置第二個Manager訪問介面會導致出現以下錯誤消息：



對於7.7.0之前的FTD版本，請確保跳過步驟7和步驟8。

7.部署策略並驗證FTD CLISH上的設定。在本範例中，名稱為outside2的Ethernet1/2介面的IP位址分別為10.62.114.51和10.62.114.52:

<#root>

>

```
show ip


System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Ethernet1/1              outside1            10.62.113.125   255.255.255.0   manual <- source interf

Ethernet1/2              outside2            10.62.114.51    255.255.255.0   manual

<- target interface
Ethernet1/4              fover               10.9.0.21       255.255.255.0   unset
```

outside2介面新增到sftunnel組態中：

```
<#root>

>

show running-config sftunnel



sftunnel interface outside2

<- target interface

sftunnel interface outside1

<- source interface
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

雖然在Network Address Translation(NAT)表中安裝了其他規則，但仍在使用outside1介面的規則：

```
<#root>

>

show nat detail


Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_0.0.0.0_intf5 interface  destination s
    translate_hits = 1448, untranslate_hits = 1448
    Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
```

```
    Service - Protocol: tcp Real: 8305 Mapped: 8305

2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface  destination st



    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_::_intf5 interface ipv6  destination s
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
4

(nlp_int_tap) to (outside2) source static nlp_server__sftunnel_::_intf6 interface ipv6  destination stat



    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
5 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_intf5 interface
    translate_hits = 653, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
6

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface



    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
7 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_ipv6_intf5 interface ipv6
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
8

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6



    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
```

8.驗證高可用性狀態和介面監控：

```
<#root>

>

show monitor-interface
```

```
        This host: Primary - Active

                Interface management (203.0.113.130): Normal (Monitored)
                Interface outside1 (10.62.113.125): Normal (Monitored)
                Interface outside2 (10.62.114.51): Normal (Monitored)

        Other host: Secondary - Standby Ready

                Interface management (203.0.113.131): Normal (Monitored)
                Interface outside1 (10.62.113.126): Normal (Monitored)
                Interface outside2 (10.62.114.52): Normal (Monitored)
```

9.如果計畫通過outside2介面管理FTD，請確保允許通過平台設定的SSH Access部分進行訪問。

10.進行必要的更改，以允許通過目標介面連線到域名伺服器(DNS)和FMC:

- 如果FMC和FTD之間的連線需要網域名稱解析(DNS)，請確保FTD可從目標介面連線至用於連線DNS伺服器的下一個躍點。在傳輸路徑中還必須允許DNS解析。
- 確保FTD可透過目標介面連線至用於到達FMC的下一個躍點。
- 確保在傳輸路徑中允許通過目標介面的TCP埠8305上的FMC和FTD之間的雙向連線。必須允許雙向連線。

在這種情況下，需要將IP 10.62.114.1用作目標介面的預設網關。使用網際網路控制訊息通訊協定(ICMP)可存取下一個躍點的IP位址：

```
<#root>

>

ping 10.62.114.1

Please use 'CTRL+C' to cancel/abort...

Sending 5, 100-byte ICMP Echos to 10.62.114.1, timeout is 2 seconds:

!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

如果在傳輸路徑或下一躍點上管理性封鎖ICMP，請確保下一個躍點的媒體存取控制(MAC)位址在show arp命令的輸出中可見且有效：

<#root>

>

show arp

```
        fover 10.9.0.22 4c01.f7e9.e111 13275
        outside1 10.62.113.1 c02c.1782.2cbf 1
        outside1 10.62.113.126 4c01.f7e9.e10e 5453
```

outside2 10.62.114.1 c02c.1782.2cbf 0

```
        outside2 10.62.114.52 4c01.f7e9.e10f 5453
```

11.根據FTD版本執行以下步驟：

- 7.7.0或更高版本：在FMC上，禁用通過源介面(outside1)的管理器訪問，調整路由，包括到DNS伺服器的路由（如果使用DNS訪問FMC）和通過目標介面(outside2)的FMC。例如，配置特定靜態路由或配置通過目標介面的預設網關。
- 低於7.7.0的版本：在FMC上，禁用通過源介面(outside1)的Manager訪問，啟用通過目標介面(outside2)的Manager訪問，調整路由，包括到DNS伺服器的路由（如果使用DNS訪問FMC）和通過目標介面(outside2)的FMC。例如，配置特定靜態路由或配置通過目標介面的預設網關。

12.部署策略。

13.驗證FTD CLISH:

<#root>

>

show route 0.0.0.0

```
Routing entry for 0.0.0.0 0.0.0.0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:

  * 10.62.114.1, via outside2

<- default route over outside2
      Route metric is 0, traffic share count is 1


>

show running-config sftunnel



sftunnel interface outside2

<- sftunnel is enabled only over outside2
sftunnel port 8305


>

show nat detail



Manual NAT Policies Implicit (Section 0)

1 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface  destination st



    translate_hits = 3, untranslate_hits = 3



    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_::_intf6 interface ipv6  destination s
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface
    translate_hits = 407, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
4 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:


>

show conn all port 8305
```

```
31 in use, 42 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect


TCP nlp_int_tap  10.62.114.51(169.254.1.3):56853 outside2  198.51.100.23:8305, idle 0:00:06, bytes 33008

<- connectivity over outside2

TCP nlp_int_tap  10.62.114.51(169.254.1.3):32905 outside2  198.51.100.23:8305, idle 0:00:00, bytes 15959

<- connectivity over outside2
```

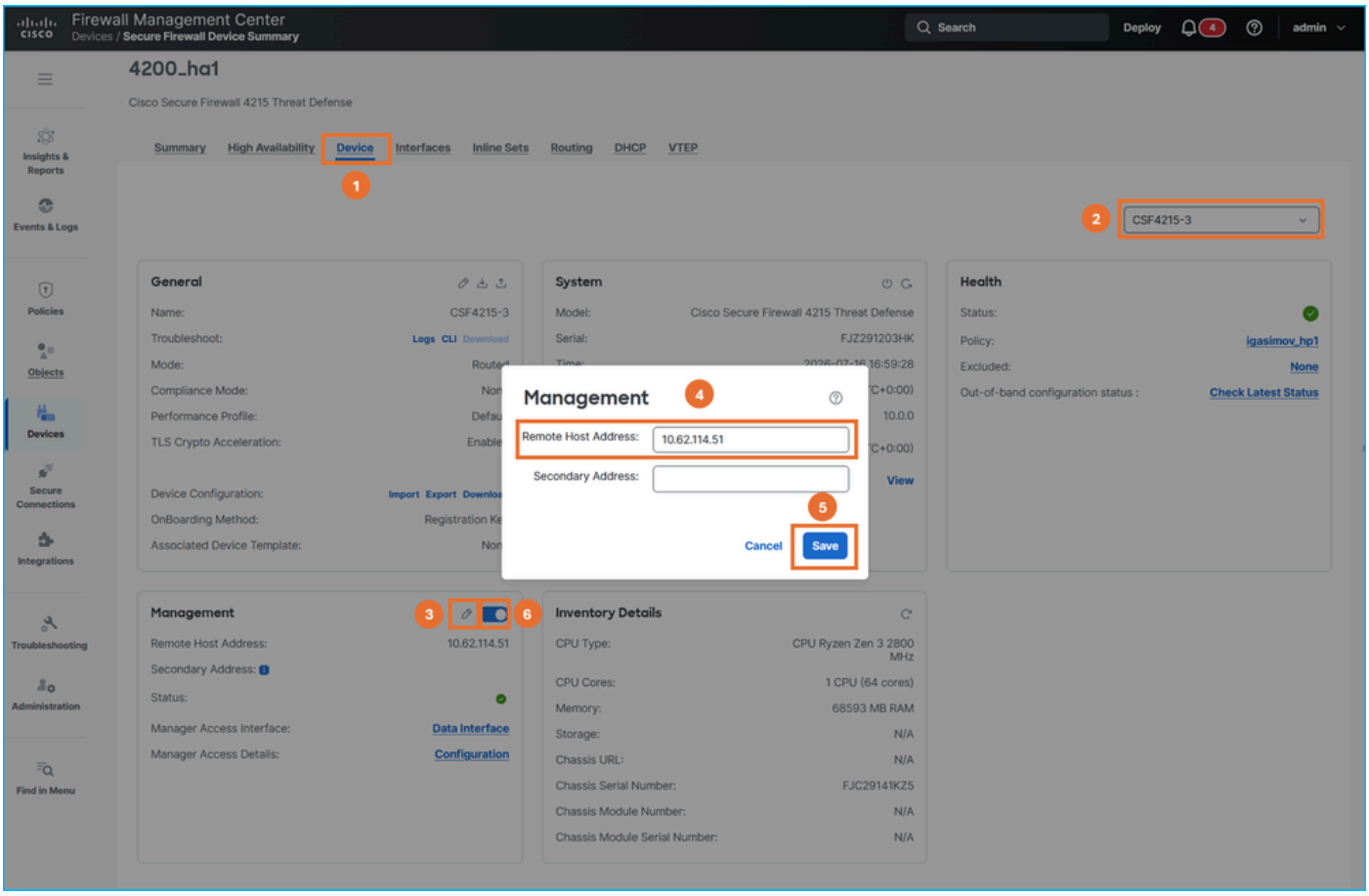
14.如果需要更改「show network」CLISH命令輸出中的DNS伺服器，請配置新的DNS伺服器：

```
<#root>

>

configure network dns servers 192.0.2.184
```

15.在FMC上，將FTD管理IP地址更改為outside2 IP地址，然後使用滑塊禁用並重新啟用連線。對HA中的兩台裝置重複此步驟：



16.驗證所有FTD上的sftunnel連線：

<#root>

>

sftunnel-status-brief

PEER:198.51.100.23
        SFTunnel Status:-

                Channel A: Connected

                Channel B: Connected

        Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '198.51.100.23'
        Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
        Registration: Completed.
        IPv4 Connection to peer '198.51.100.23' Start Time: Thu Jul 16 16:37:14 2026 UTC
        Heartbeat Send Time: Thu Jul 16 16:38:13 2026 UTC
        Heartbeat Received Time: Thu Jul 16 16:39:13 2026 UTC
        Last disconnect time   : Thu Jul 16 16:37:11 2026 UTC
        Last disconnect reason : Both control and event channel connections with peer went down

```
>

show conn all port 8305


32 in use, 42 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect


TCP nlp_int_tap  10.62.114.51(169.254.1.3):8305 outside2  198.51.100.23:36383, idle 0:00:00, bytes 23575

<- new connection over different source port

TCP nlp_int_tap  10.62.114.51(169.254.1.3):8305 outside2  198.51.100.23:50963, idle 0:00:01, bytes 12319

<- new connection over different source port
```

17.如果需要更改平台設定中的DNS伺服器，請進行相應的配置更改並部署策略。

管理連線故障排除

使用以下命令進行驗證：

1. show network — 顯示管理介面的配置。
2. sftunnel-status-brief — 顯示sftunnel連線狀態。
3. show run sftunnel — 顯示防火牆引擎(Lina)中的sftunnel配置。
4. show conn all port 8305 - 顯示透過Lina引擎的sftunnel連線。

要排除管理連線故障，請參閱官方指南中的排除管理連線故障部分。

參考資料

1. 思科安全防火牆管理中心裝置配置指南，10.x
2. 更改Manager訪問介面
3. 管理連線故障排除

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。