在FTD上設定從管理到資料介面的管理員存取許可權

目錄

簡介

本檔案介紹將Firepower威脅防禦(FTD)上的Manager訪問許可權從管理介面修改為資料介面的過程。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)

採用元件

- Firepower管理中心虛擬7.4.1
- Firepower威脅防禦虛擬7.2.5

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。

背景資訊

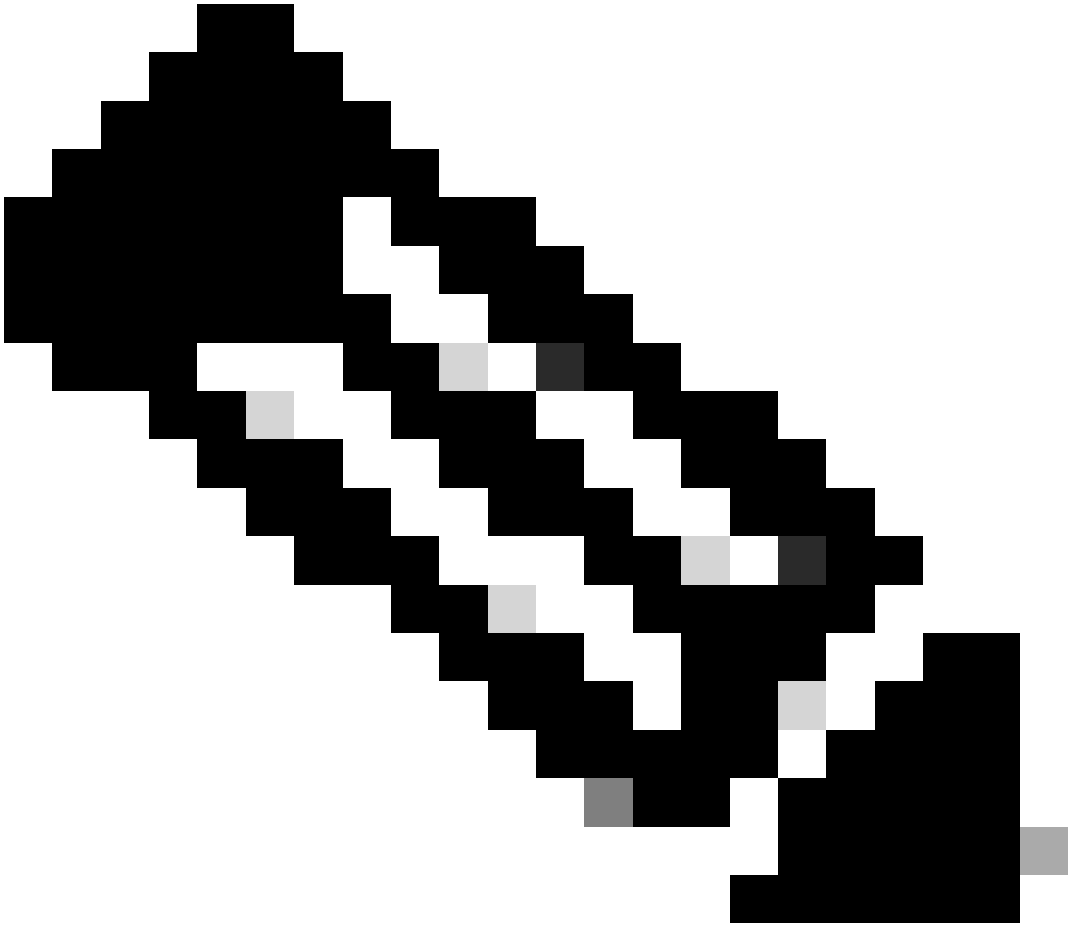
每個裝置都包括用於與FMC通訊的單個專用管理介面。您可以選擇將裝置配置為使用資料介面而不是專用管理介面進行管理。如果要從外部介面遠端管理Firepower威脅防禦，或者沒有單獨的管理網路，資料介面上的FMC訪問非常有用。此更改必須在FMC管理的FTD Firepower管理中心上執行。

從資料介面進行FMC訪問存在一些限制：

- 您只能在一個物理資料介面上啟用管理員訪問。不能使用子介面或EtherChannel。
- 僅路由防火牆模式，使用路由介面。
- 不支援PPPoE。如果您的ISP需要PPPoE，則必須在Firepower威脅防禦和WAN數據機之間放置一台支援PPPoE的路由器。
- 不能使用單獨的管理介面和僅事件介面。

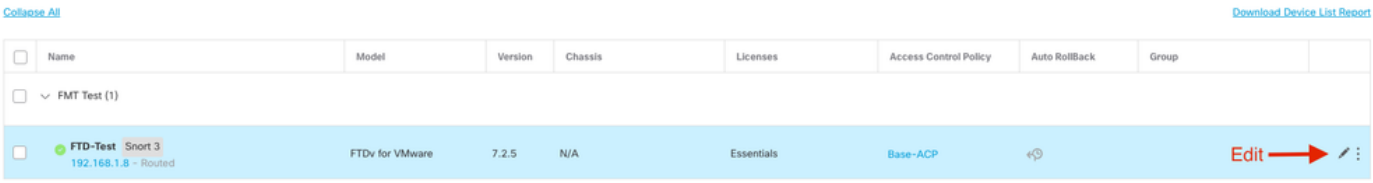
設定

繼續介面遷移



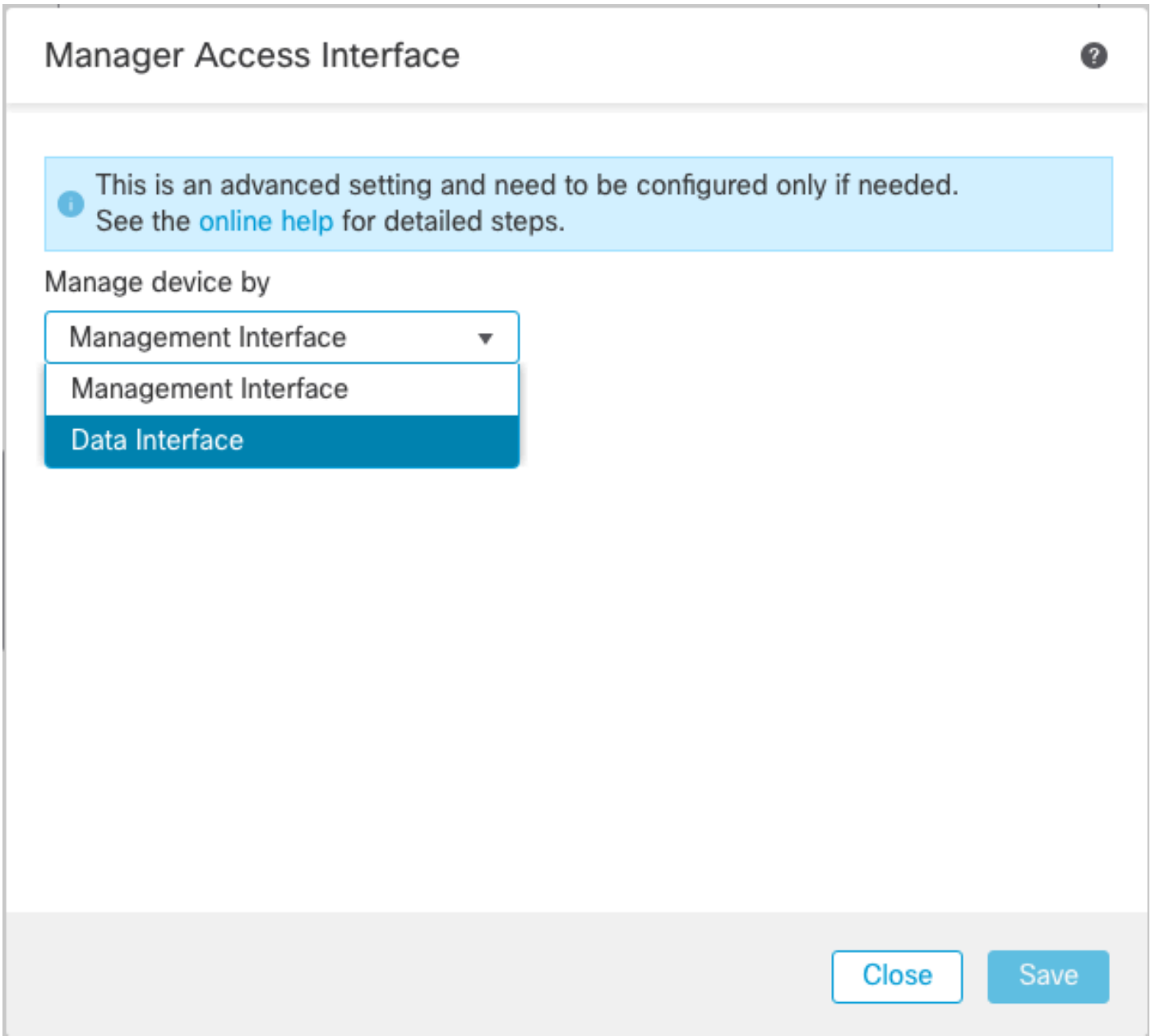
附註：強烈建議先對FTD和FMC進行最新備份，然後再繼續進行更改。

1. 導航到Devices > Device Management頁面，然後點選要更改的裝置的Edit。

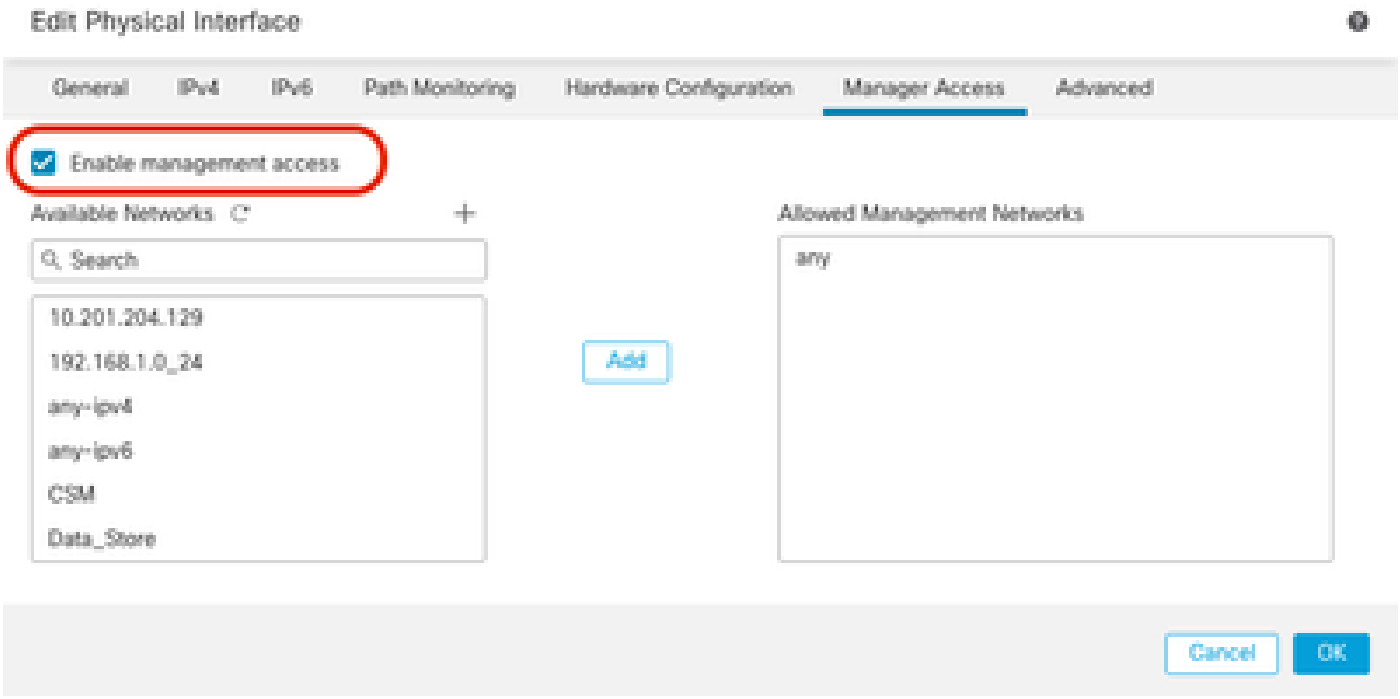


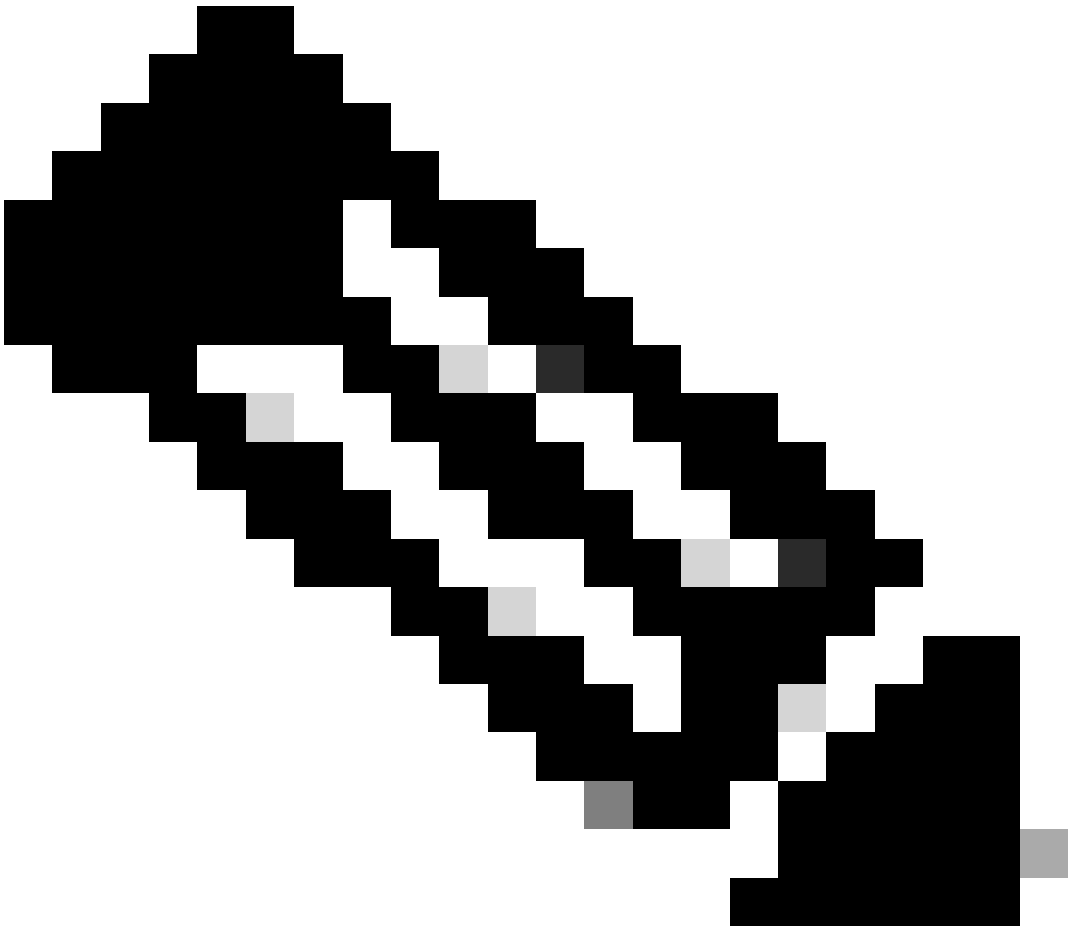
2.轉到Device > Management部分，然後按一下Manager Access Interface的連結。

Manager Access Interface欄位顯示現有的管理介面。按一下link選擇新的介面型別，這是Manage device by下拉選單中的Data Interface選項，然後按一下Save。



3.現在，必須繼續執行在資料介面上啟用管理訪問，導航到Devices > Device Management > Interfaces > Edit Physical Interface > Manager Access。


Edit Physical Interface
General
IPv4
IPv6
Path Monitoring
Hardware Configuration
Manager Access
Advanced
Enable management access
Available Networks
Search
10.201.204.129
192.168.1.0_24
any-ipv4
any-ipv6
CSM
Data_Store
Add
Allowed Management Networks
any
Cancel
OK



註：（可選）如果使用輔助介面進行冗餘，請在用於冗餘的介面上啟用管理訪問。

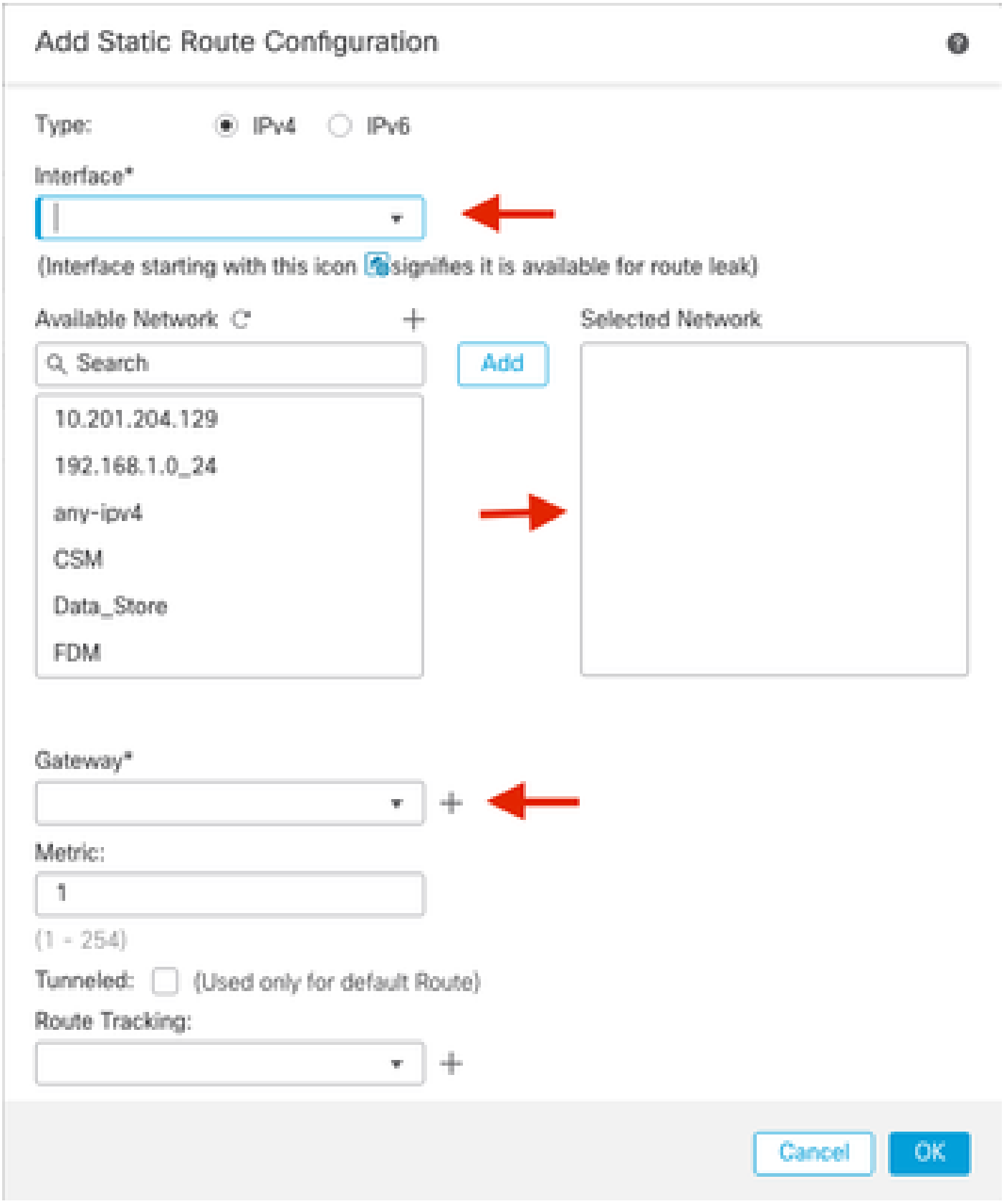
（可選）如果使用DHCP作為介面，請在Devices > Device Management > DHCP > DDNS對話方塊上啟用Web型別DDNS方法。

（可選）在「平台設定」策略中配置DNS，並在Devices > Platform Settings > DNS中將其應用到此裝置。

4.確保威脅防御能夠通過資料接口路由到管理中心；如有必要，在Devices > Device Management > Routing > Static Route上新增靜態路由。

1. 根據所新增的靜態路由型別，按一下IPv4或IPv6。
2. 選擇應用此靜態路由的介面。
3. 在「Available Network」清單中，選擇目的地網路。
4. 在「Gateway or IPv6 Gateway」欄位中，輸入或選擇gateway router，此路由的下一躍點。

（可選）要監控路由可用性，請在路由跟蹤(Route Tracking)欄位中輸入或選擇定義監控策略的服務級別協議(Service Level Agreement，SLA)監控對象的名稱。

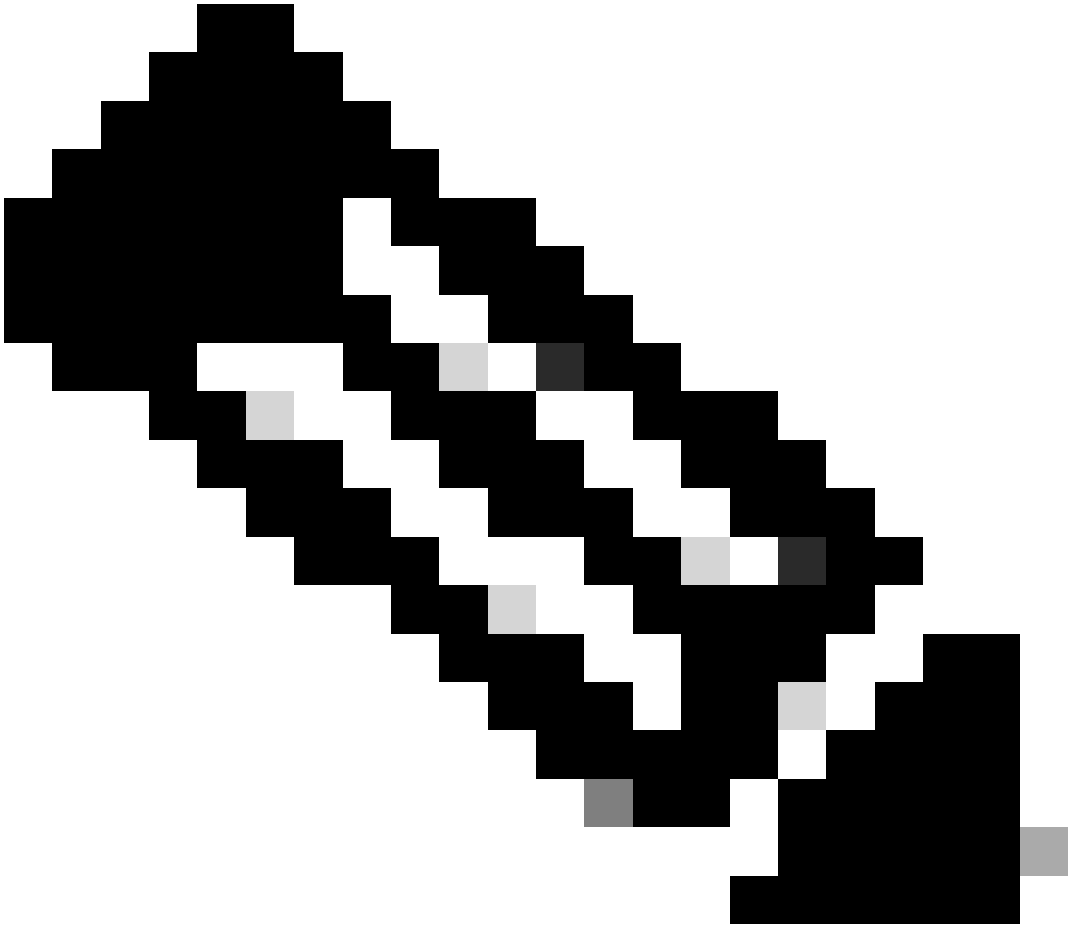


5. Deploy組態變更。配置更改現在通過當前管理介面進行部署。

6.在FTD CLI上，將管理介面設定為使用靜態IP地址，並將網關設定為資料介面。

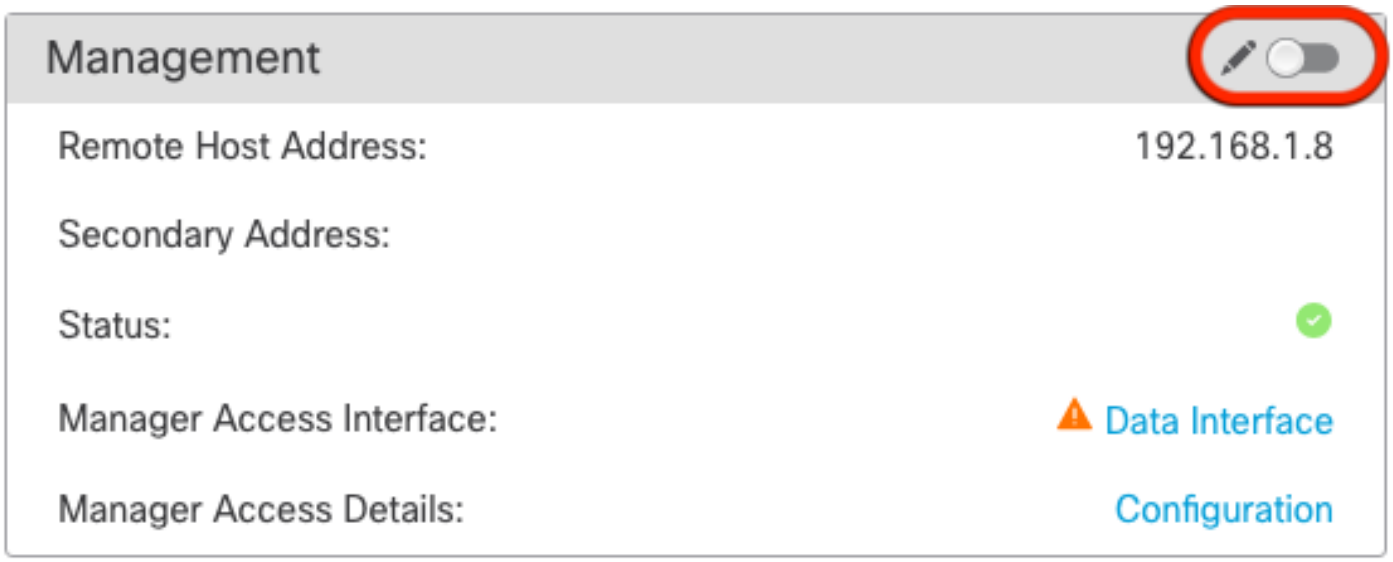
- configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

```
>
>                                    IP_ADDRESS      NETMASK         GATEWAY
> configure network ipv4 manual 192.168.1.8 255.255.255.0 data-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```



附註：雖然不打算使用管理介面，但必須設定靜態IP地址。例如，私有地址，以便您可以將網關設定為資料介面。此管理用於使用tap_nlp介面將管理流量轉發到資料介面。

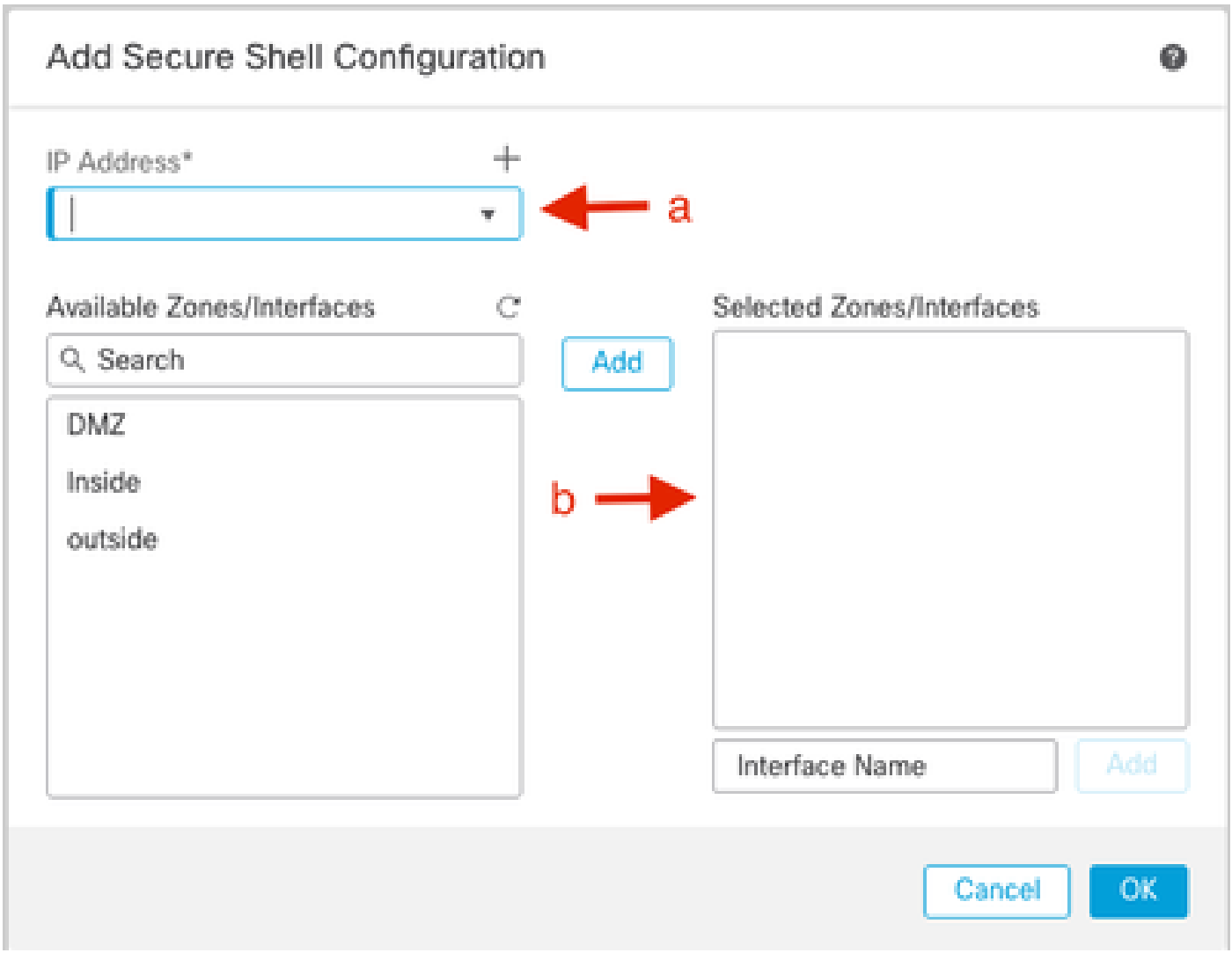
7.在管理中心中禁用管理。在Devices > Device Management > Device > Management部分中，按一下Edit and update the Remote Host Address IP address and(Optional)Secondary Address for the threat defense，然後啟用連線。

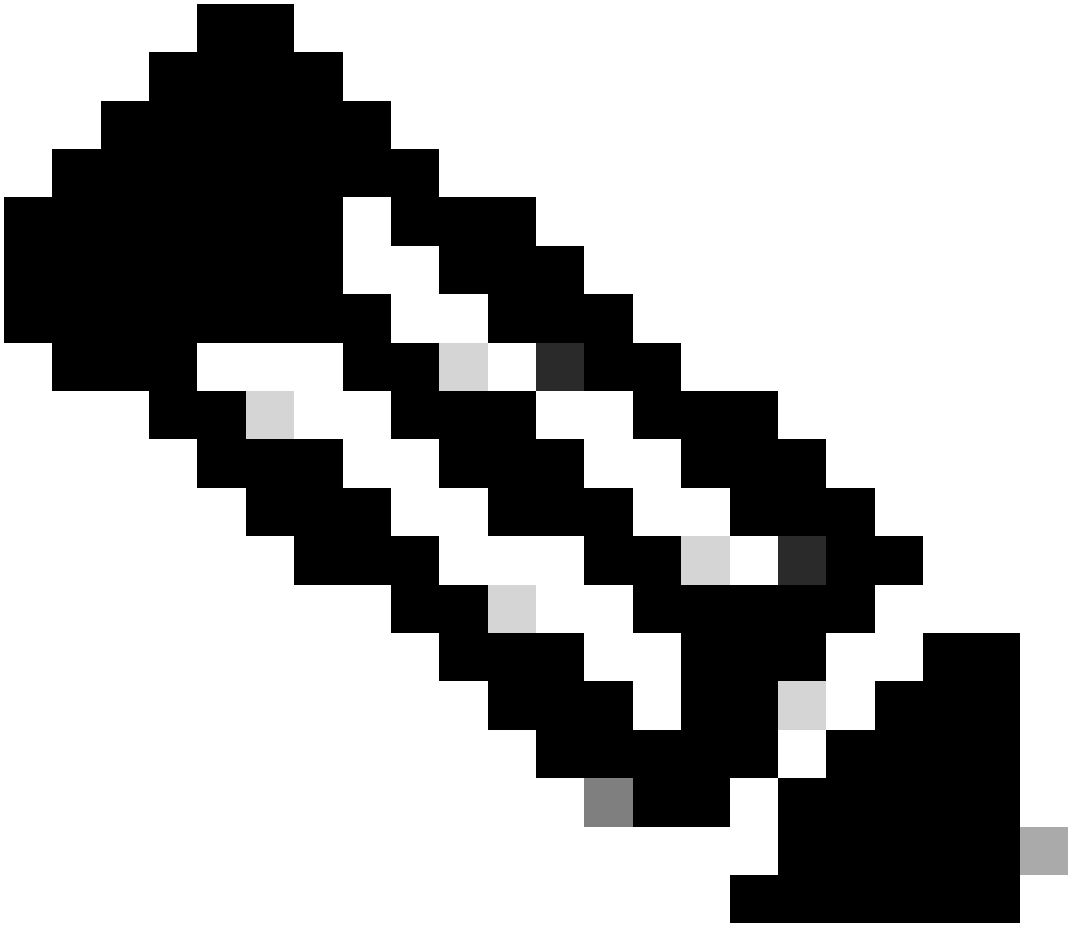


在平台設定上啟用SSH

在「平台設定」策略中啟用資料介面的SSH，並在「裝置」>「平台設定」>「SSH訪問」處將SSH應用到此裝置。按一下Add。

1. 允許進行SSH連線的主機或網路。
2. 新增包含介面的區域以允許SSH連線。對於不在區域中的介面，可以在Selected Zones/Interfaces欄位中鍵入interface name，然後按一下Add。
3. 按一下「OK」。「Deploy」變更。


Add Secure Shell Configuration
IP Address*
a
Available Zones/Interfaces
Search
DMZ
Inside
outside
Add
b
Selected Zones/Interfaces
Interface Name
Add
Cancel
OK



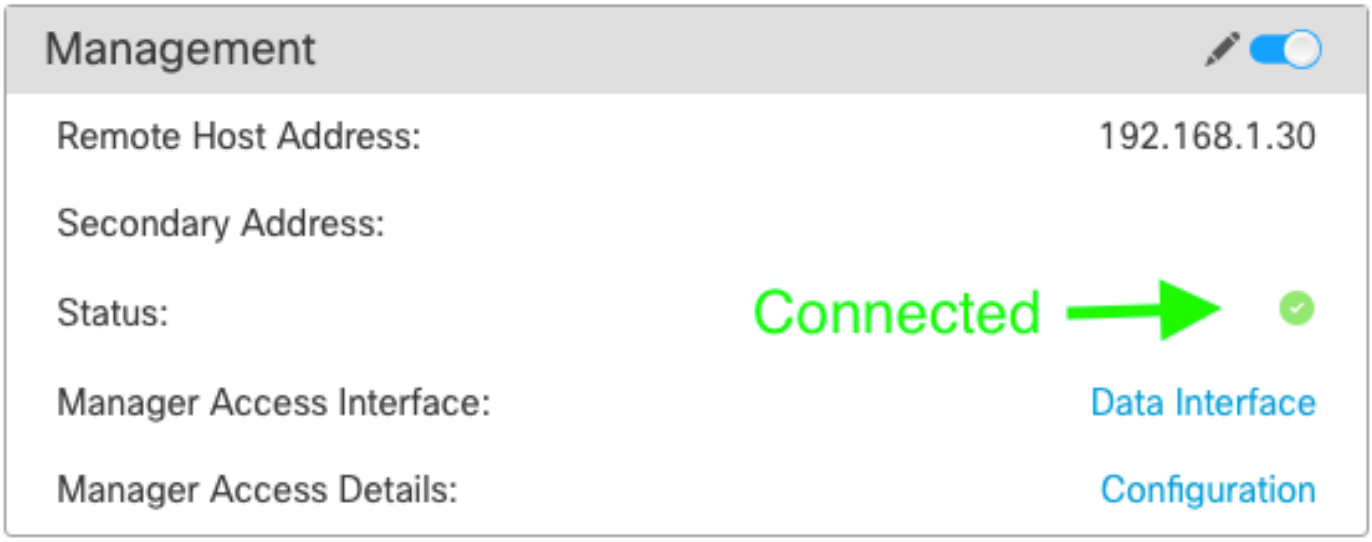
附註：預設情況下，資料介面上未啟用SSH，因此，如果您希望使用SSH管理威脅防禦，則需要明確允許它。

驗證

確保通過Data介面建立管理連線。

從FMC圖形使用者介面(GUI)進行驗證

在管理中心，在Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status頁面上檢查管理連線狀態。



從FTD命令列介面(CLI)驗證

在threat defenseCLI上，輸入theftunnel-status-briefcommand以檢視管理連線狀態。

```
>
> sftunnel-status-brief

PEER:192.168.1.2
        Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Registration: Completed.
        IPv4 Connection to peer '192.168.1.2' Start Time: Tue Jul 16 22:23:54 2024 UTC
        Heartbeat Send Time:     Tue Jul 16 22:39:52 2024 UTC
        Heartbeat Received Time: Tue Jul 16 22:39:52 2024 UTC
        Last disconnect time   : Tue Jul 16 22:17:42 2024 UTC
        Last disconnect reason : Both control and event channel connections with peer went down
```

狀態顯示資料介面連線成功，顯示內部tap_nlp介面。

疑難排解

在管理中心，在Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status頁面上檢查管理連線狀態。

在threat defenseCLI上，輸入theftunnel-status-briefcommand以檢視管理連線狀態。您還可以使用ftunnel-statuss來檢視更完整的資訊。

管理連線狀態

工作場景

```
> sftunnel-status-brief

PEER:192.168.1.2
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to '192.168.1.2' via '192.168.1.8'
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Registration: Completed.
        IPv4 Connection to peer '192.168.1.2' Start Time: Wed Jul 17 06:21:15 2024 UTC
        Heartbeat Send Time:     Wed Jul 17 17:15:20 2024 UTC
        Heartbeat Received Time: Wed Jul 17 17:16:55 2024 UTC
        Last disconnect time   : Wed Jul 17 06:21:12 2024 UTC
        Last disconnect reason : Process shutdown due to stop request from PM
```

非工作場景

```
> sftunnel-status-brief

PEER:192.168.1.2
        Registration: Completed.
        Connection to peer '192.168.1.2' Attempted at Wed Jul 17 17:20:26 2024 UTC
        Last disconnect time   : Wed Jul 17 17:20:26 2024 UTC
        Last disconnect reason : Both control and event channel connections with peer went down
```

驗證網路資訊

在threat defenseCLI中，檢視管理和管理器訪問資料介面網路設定：

> show network

```
> show network
==============[ System Information ]==============
Hostname                : ftdcdo.breakstuff.com
Domains                 : breakstuff.com
DNS Servers             : 192.168.1.103
DNS from router         : enabled
Management port         : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

======================[ eth0 ]======================
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 00:0C:29:54:D4:47
----------------------[ IPv4 ]----------------------
Configuration           : Manual
Address                 : 192.168.1.8
Netmask                 : 255.255.255.0
Gateway                 : 192.168.1.1
----------------------[ IPv6 ]----------------------
Configuration           : Disabled

==============[ Proxy Information ]================
State                   : Disabled
Authentication          : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers             :
Interfaces              : GigabitEthernet0/0

==============[ GigabitEthernet0/0 ]==============
State                   : Enabled
Link                    : Up
Name                    : Outside
MTU                     : 1500
MAC Address             : 00:0C:29:54:D4:5B
```

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）。