通過FDM配置FTD上SSH和HTTPS的管理訪問

目錄

簡介

本檔案介紹在本地或遠端管理的FTD上設定和驗證SSH和HTTPS管理存取清單的程式。

必要條件

需求

本文件沒有特定需求。

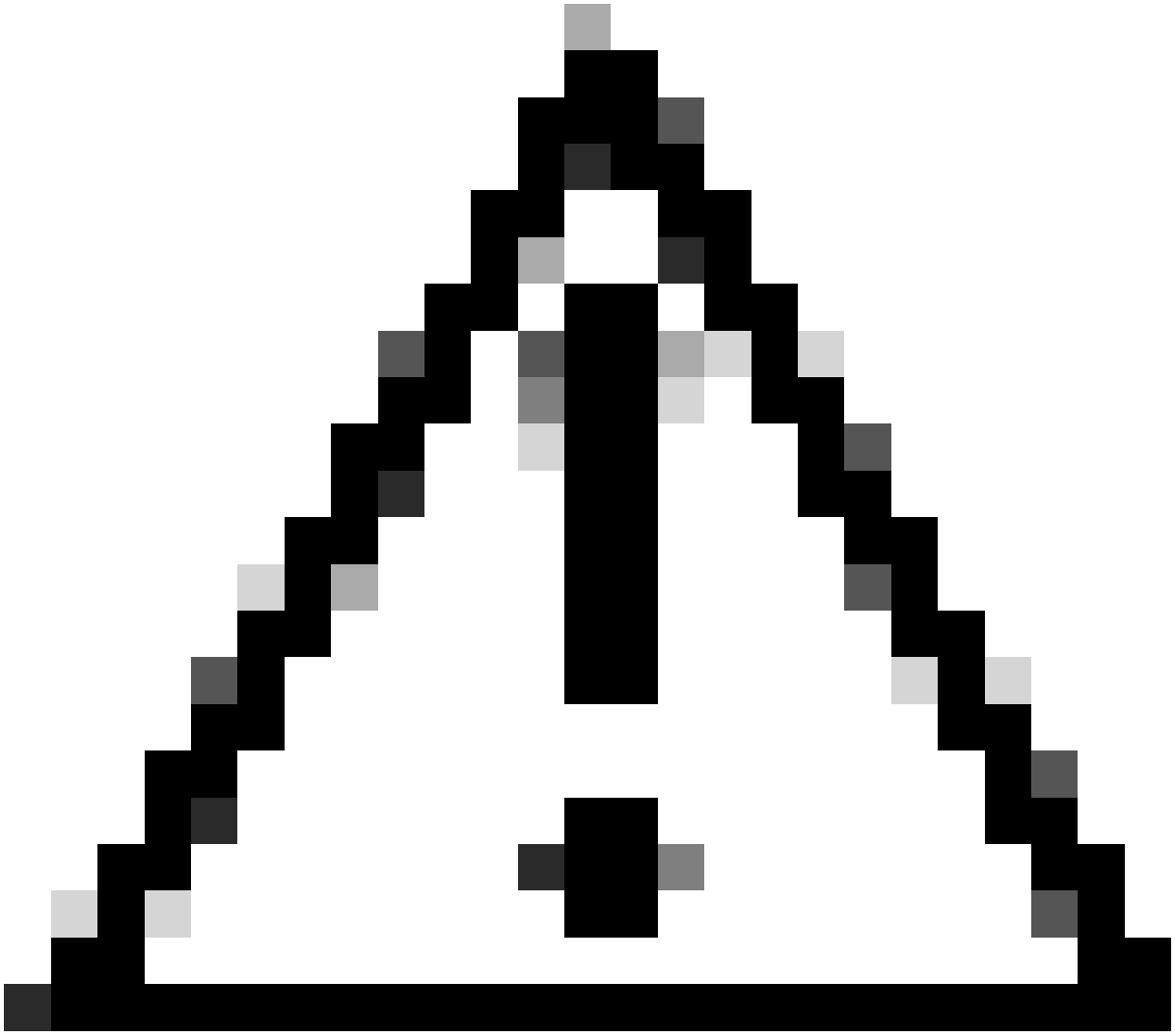
採用元件

- 運行由FDM管理的7.4.1版本的思科安全防火牆威脅防禦。

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。

設定

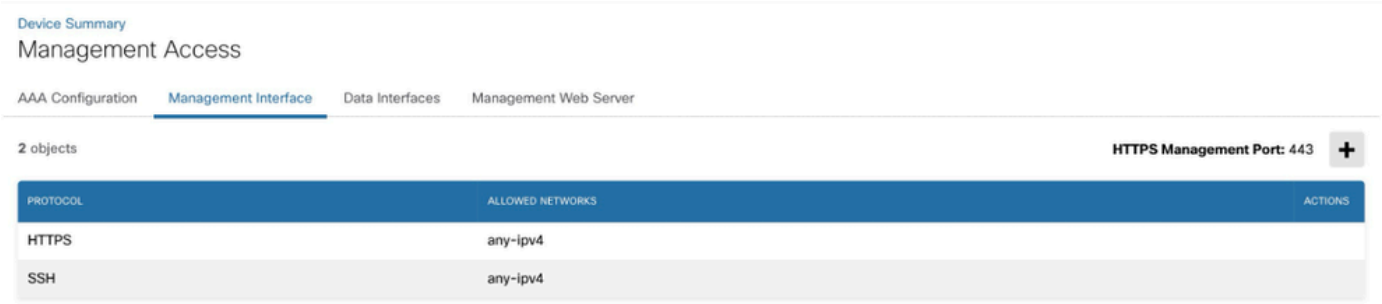
FTD可以使用FDM本地管理，或透過FMC管理。本文檔重點介紹通過FDM和CLI進行的管理訪問。使用CLI，您可以更改方案FDM和FMC。



注意：配置SSH或HTTPS訪問清單，一次配置一個，以避免會話鎖定。首先，更新並部署一個協定，驗證訪問，然後繼續執行另一個協定。

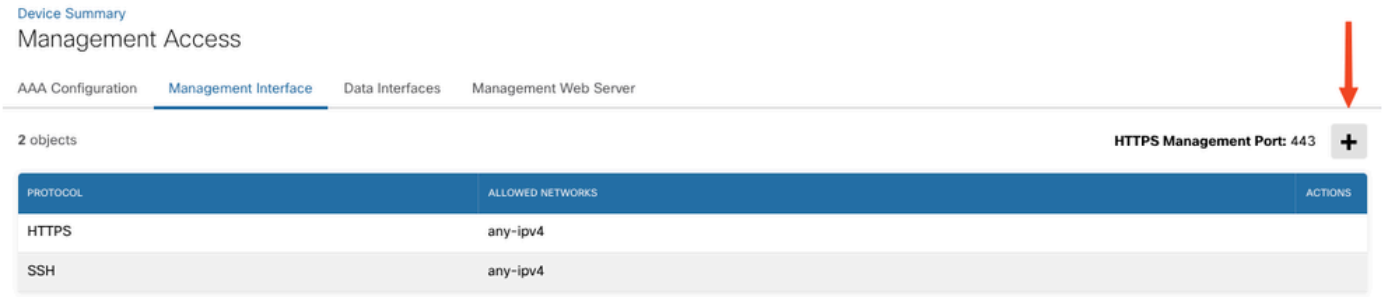
FDM步驟：

步驟 1:登入到Firepower裝置管理器(FDM)，然後導航到系統設定>管理訪問>管理介面。



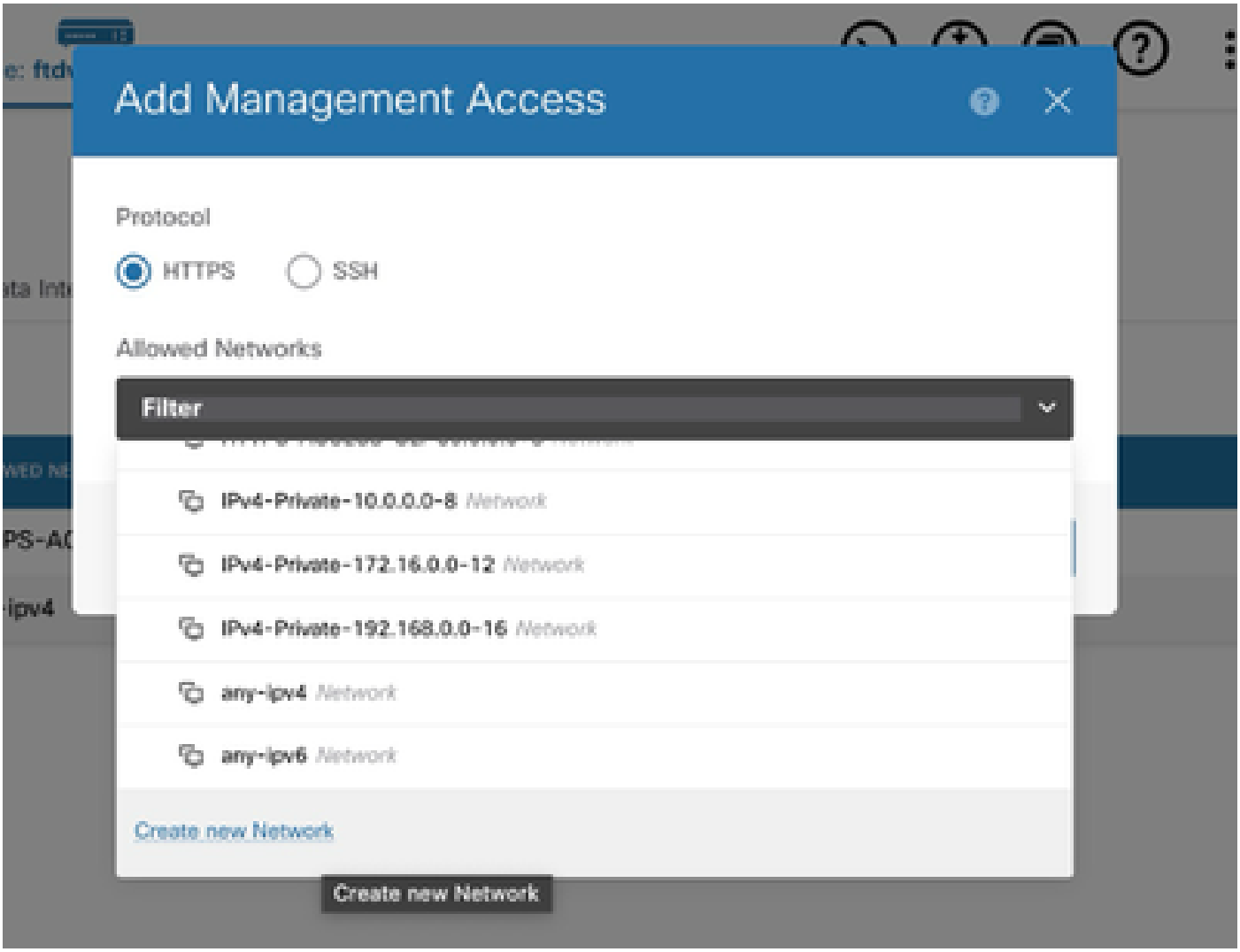
預設情況下，允許SSH和HTTPS的管理埠訪問any-ipv4

第2步：點選+圖標以開啟新增網路的視窗。



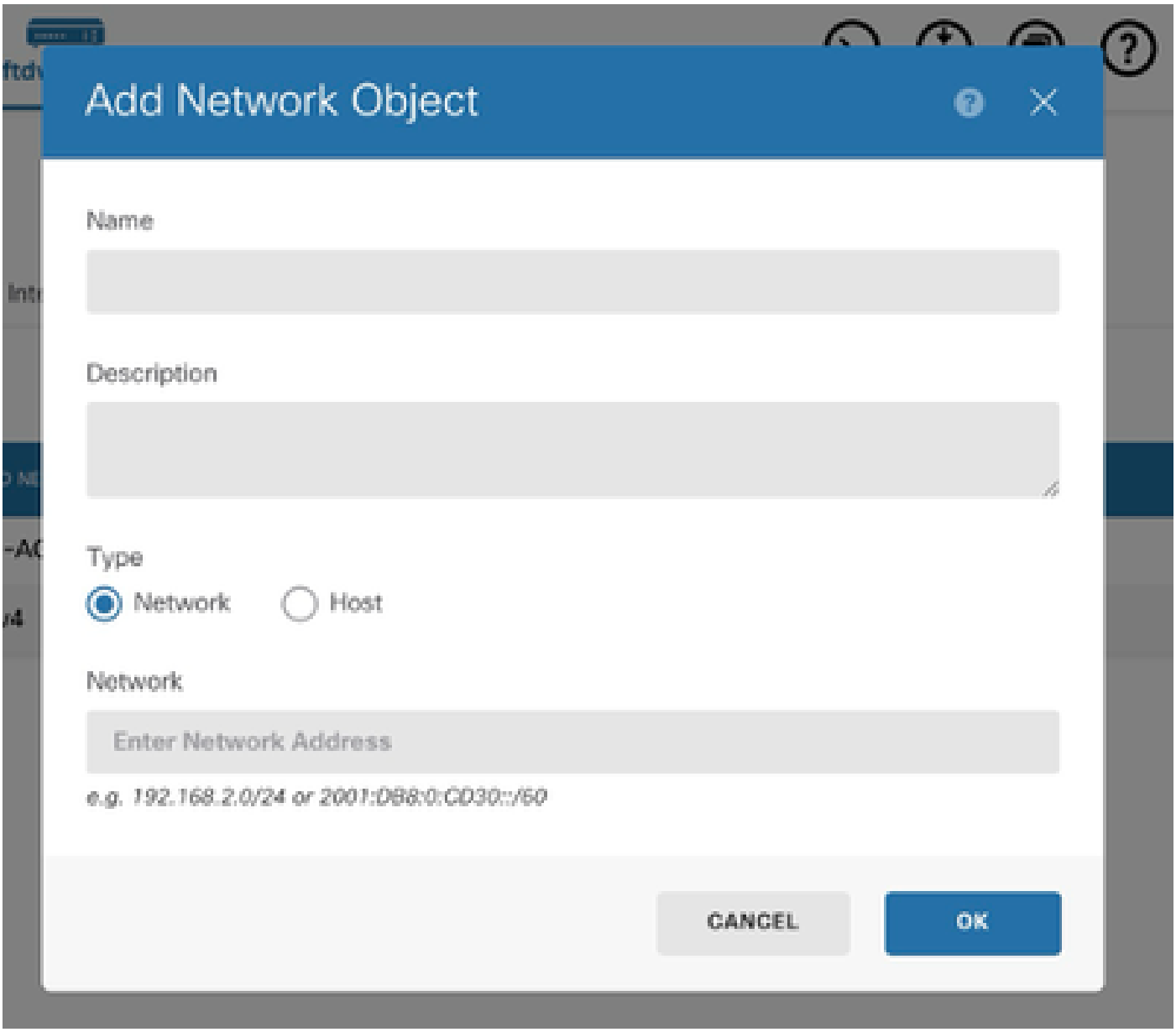
按一下右上角的「新增」按鈕。

第3步：新增網路對象以具有SSH或HTTPS訪問許可權。如果需要建立新網路，請選擇Create new Network選項。您可以在管理訪問中為網路或主機新增多個條目。



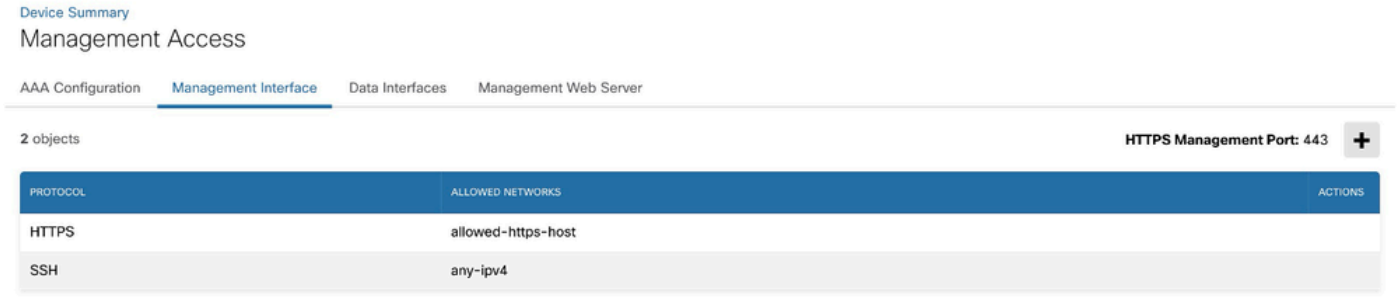
選擇網路。

第4步（可選）：Create new Network選項開啟Add Network Object窗口。

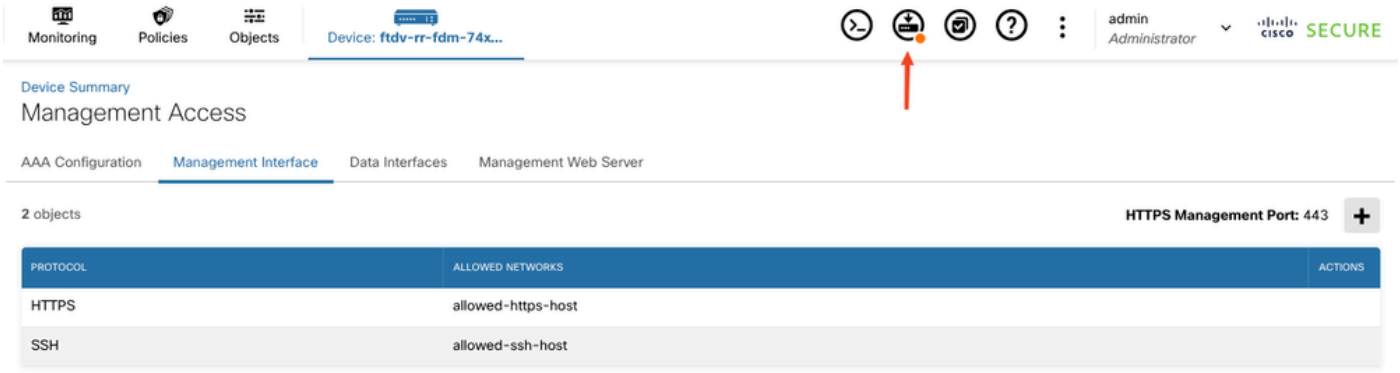


根據您的要求建立主機網路。

第5步：驗證所做的更改並進行部署。

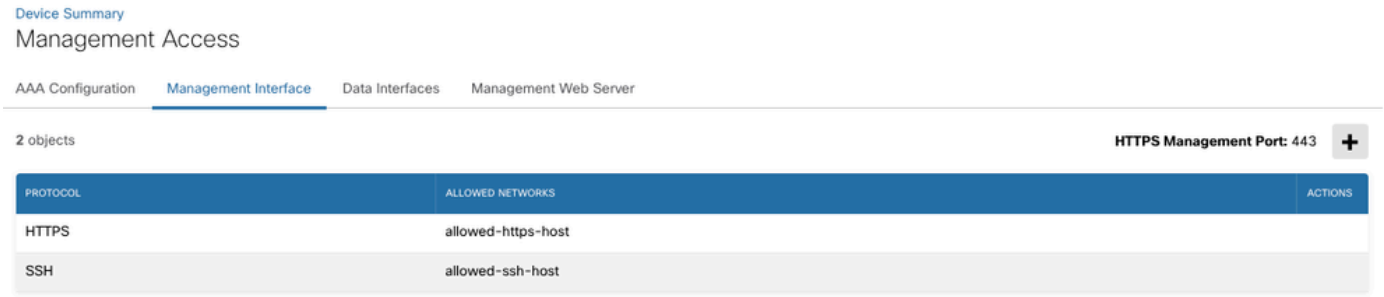


HTTPS管理訪問已更改，並且any-ipv4已刪除。



在FDM上部署

第6步（可選）：在驗證之前對HTTPS所做的更改後，對SSH重複相同的操作。



已為SSH和HTTPS新增網路對象。

步驟 7:最後，部署變更並驗證您從允許的網路和主機對FTD的存取許可權。

CLISH步驟:

CLI步驟可用於FDM或FMC管理的情況。

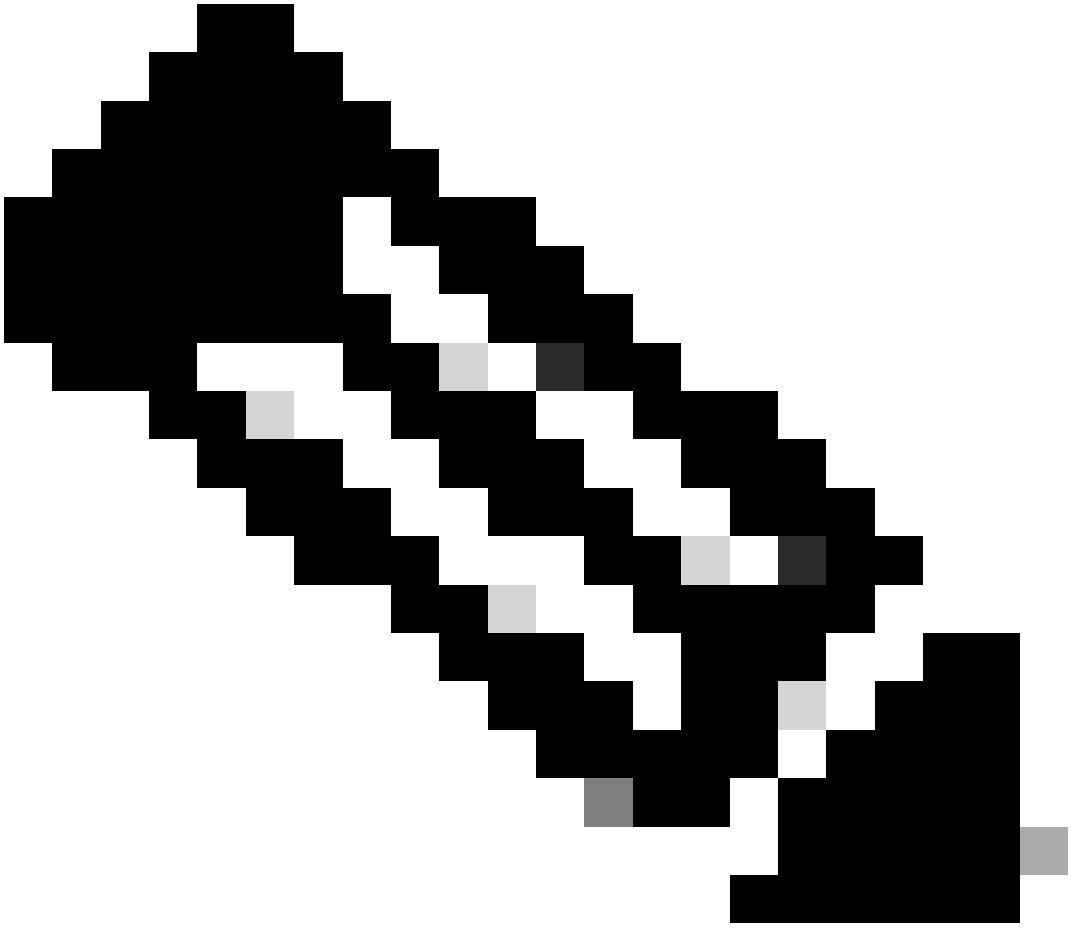
要將裝置配置為接受來自指定IP地址或網路的HTTPS或SSH連線，請使用configure https-access-listconfigure ssh-access-listtheorcommand。

- 必須在單個命令中包括所有支援的主機或網路。此命令中指定的地址將覆蓋各個訪問清單的當前內容。
- 如果裝置是本地管理的高可用性組中的裝置，則下次活動裝置部署配置更新時，您的更改將覆蓋該裝置。如果是活動裝置，則在部署過程中更改將傳播到對等裝置。

```
> configure https-access-list x.x.x.x/x,y.y.y.y/y

The https access list was changed successfully.

> show https-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:https
ACCEPT     tcp  --  y.y.y.y/y            anywhere             state NEW tcp dpt:https
```



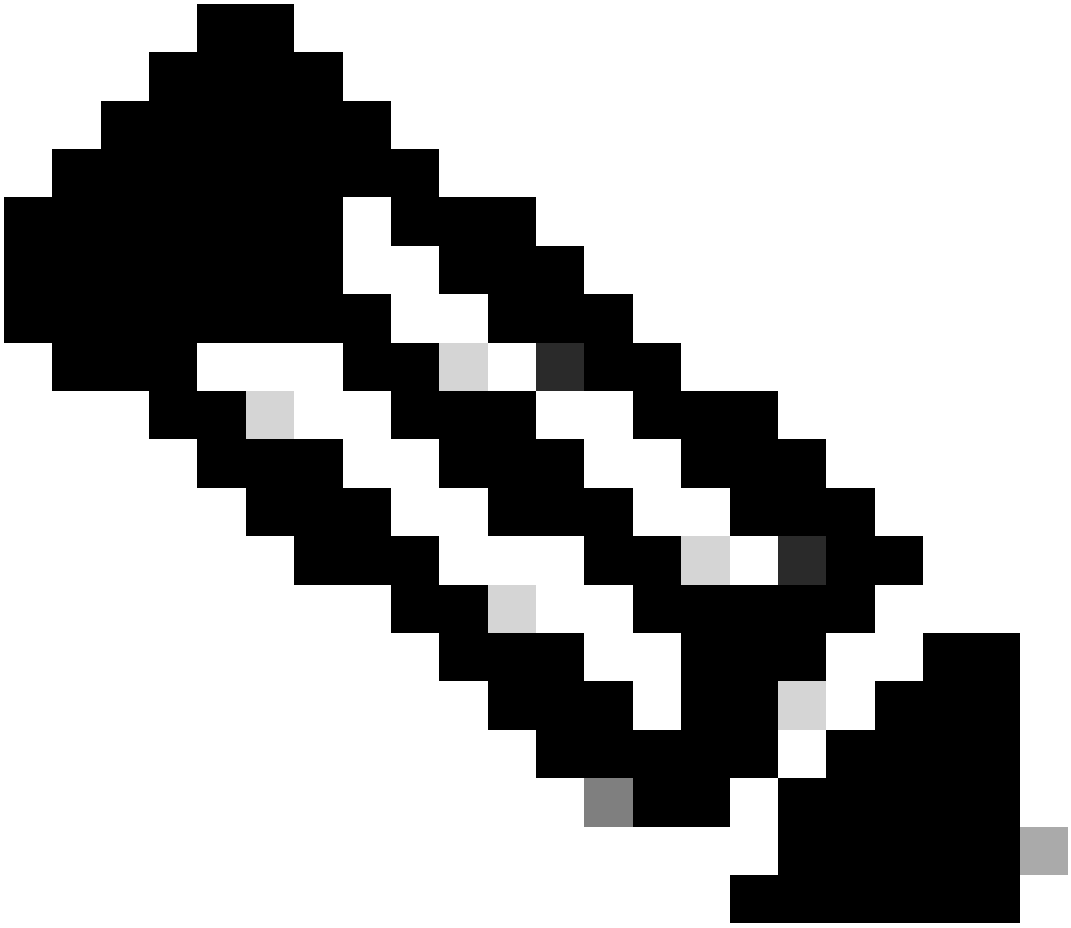
附註：x.x.x.x/x和y.y.y.y/y表示使用CIDR表示法的ipv4地址。

同樣，對於SSH連線，請使用configure ssh-access-list命令，並將單個或多個命令分開。

```
> configure ssh-access-list x.x.x.x/x

The ssh access list was changed successfully.

> show ssh-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere            state NEW tcp dpt:ssh
```



附註：可以使用命令**configure disable-https-access**或configure disable-ssh-access分別禁用HTTPS或SSH訪問。確保您知道這些更改，因為這會將您鎖定在會話之外。

驗證

要通過CLISH進行驗證，您可以使用命令：

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh

> show https-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:https
```

參考資料

思科安全防火牆威脅防禦命令參考

適用於Firepower裝置管理器的Cisco Firepower威脅防禦配置指南

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）。