

設定透過FMC對FTD (HTTPS和SSH) 的管理存取

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[配置管理訪問](#)

[步驟1.透過FMC GUI在FTD介面上設定IP。](#)

[步驟2.配置外部身份驗證。](#)

[步驟3.配置SSH訪問。](#)

[步驟4.配置HTTPS訪問。](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹透過Firesight管理中心(FMC)對Firepower威脅防禦(FTD) (HTTPS和SSH) 進行管理存取的組態。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower技術知識
- ASA基礎知識 (自適應安全裝置)
- 通過HTTPS和SSH (安全外殼) 在ASA上進行管理訪問的知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 適用於ASA(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)的自適應安全裝置 (ASA)Firepower威脅防禦映像，在軟體版本6.0.1或更高版本上運行。
- 適用於ASA(5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)的ASA Firepower威脅防禦映像，運行在軟體版本6.0.1及更高版本上。
- Firepower管理中心(FMC)版本6.0.1及更高版本。

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

隨著Firepower威脅防禦(FTD)的啟動，與ASA相關的整個配置都將在GUI上完成。

在運行軟體版本6.0.1的FTD裝置上，當您進入系統支援diagnostic-cli時，會訪問ASA診斷CLI。但是，在執行軟體版本6.1.0的FTD裝置上，CLI會融合，且整個ASA命令都會在CLISH上設定。

```
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)
```

```
>  CLISH
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> en
Password:
firepower#  DIAGNOSTIC CLI
```

為了直接從外部網路獲得管理訪問許可權，必須通過HTTPS或SSH配置管理訪問許可權。本文檔提供了通過SSH或HTTPS獲取外部管理訪問許可權所需的必要配置。

註：在運行軟體版本6.0.1的FTD裝置上，本地使用者無法訪問CLI，必須配置外部身份驗證才能對使用者進行身份驗證。但是在執行軟體版本6.1.0的FTD裝置上，本地admin使用者可以存取CLI，但所有其他使用者需要外部驗證。

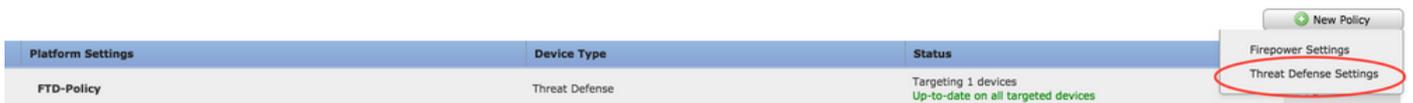
注意：在執行軟體版本6.0.1的FTD裝置上，無法透過針對FTD的br1設定的IP直接存取診斷CLI。但是，在運行軟體版本6.1.0的FTD裝置上，可以通過任何為管理訪問配置的介面來訪問融合的CLI，但是該介面必須配置有IP地址。

設定

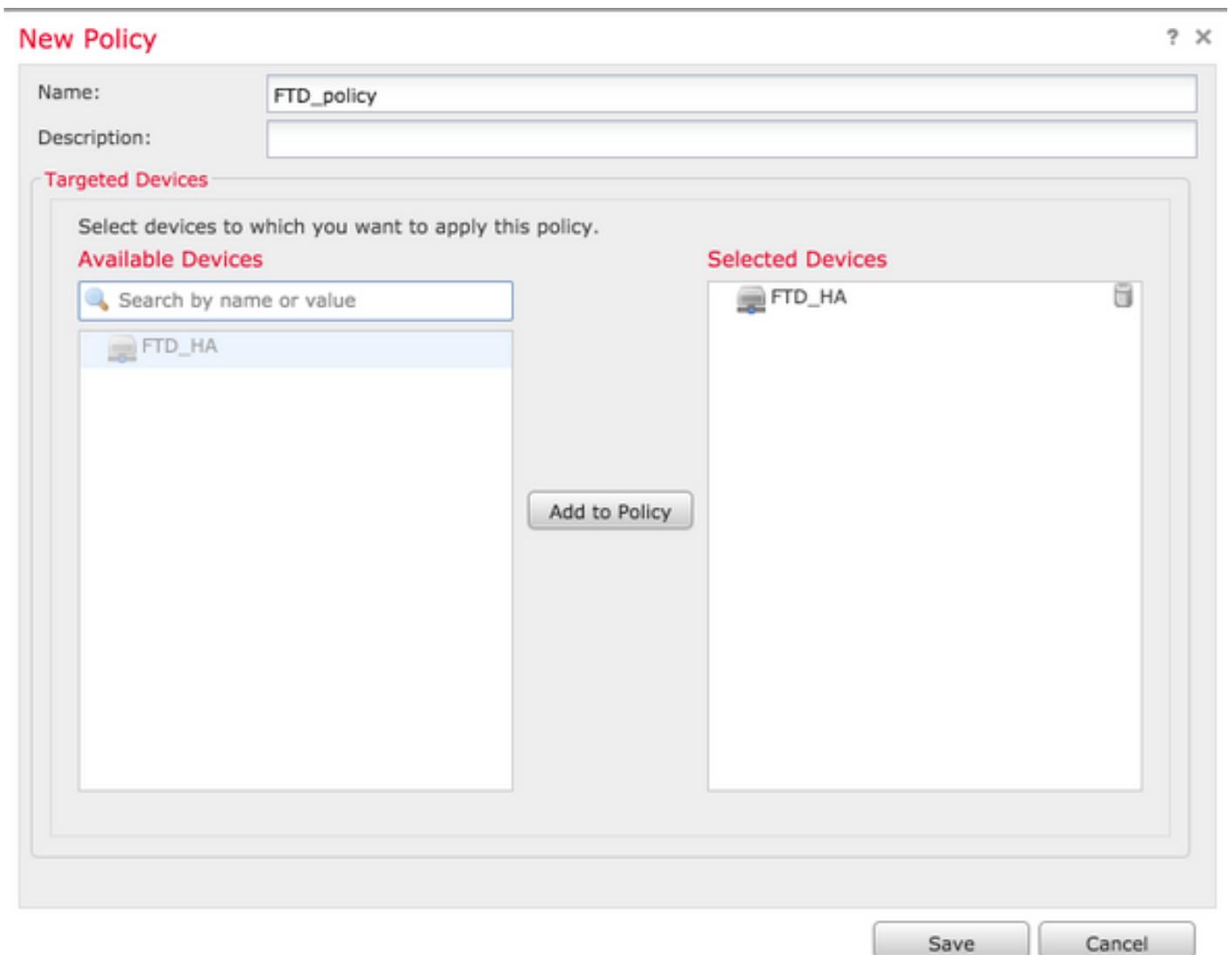
導覽至Devices中的Platform Settings索引標籤時，會設定所有管理存取相關的組態，如下圖所示：



您可以編輯點選鉛筆圖示時存在的策略，或在點選New Policy 按鈕並選擇型別作為Threat Defense Settings時建立新的FTD策略，如下圖所示：



選擇要應用此策略的FTD裝置，然後按一下Save，如下圖所示：



配置管理訪問

以下是設定管理存取的四個主要步驟。

步驟1.透過FMC GUI在FTD介面上設定IP。

在FTD可透過SSH或HTTPS存取的介面上設定IP。導覽至FTD的Interfaces索引標籤時，編輯現有的介面。

註：在執行軟體版本6.0.1的FTD裝置上，FTD上的預設管理介面是diagnostic0/0介面。但是在執行軟體版本6.1.0的FTD裝置上，除診斷介面外，所有介面都支援管理存取。

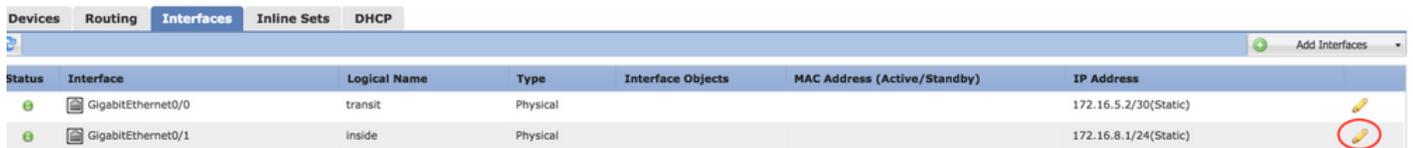
配置診斷介面有六個步驟。

步驟1.導航至 Device > Device Management。

步驟2.選擇Device或FTD HA Cluster。

步驟3.導航到Interfaces頁籤。

步驟4.按一下鉛筆圖標，設定/編輯介面以取得管理存取許可權，如下圖所示：



Status	Interface	Logical Name	Type	Interface Objects	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0	transit	Physical			172.16.5.2/30(Static)
	GigabitEthernet0/1	inside	Physical			172.16.8.1/24(Static)

步驟5.選中enable竅取方塊以啟用介面。導航到Ipv4頁籤，選擇IP Type作為static或DHCP。現在，輸入介面的IP位址，然後按一下OK，如下圖所示：

Edit Physical Interface



Mode: ▾

Name: Enabled Management Only

Security Zone: ▾

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▾

IP Address: eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

步驟6.按一下「Save」，然後將原則部署到FTD。

註：在軟體版本為6.1.0的裝置上，診斷介面無法用於通過SSH訪問已收斂的CLI

步驟2.配置外部身份驗證。

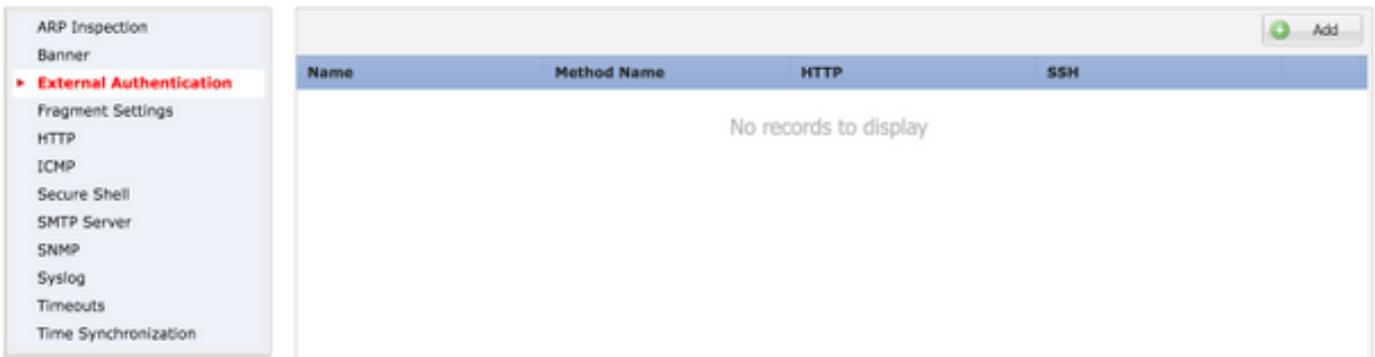
外部驗證便於將FTD整合到Active Directory或RADIUS伺服器以進行使用者驗證。這是必要步驟，因為本地配置的使用者不能直接訪問診斷CLI。只有通過輕量型目錄訪問協定(LDAP)或RADIUS進行身份驗證的使用者才能訪問診斷CLI和GUI。

配置外部身份驗證有6個步驟。

步驟1.導航至 Devices > Platform Settings。

步驟2.在按一下鉛筆圖示時編輯已存在的策略，或在按一下New Policy按鈕時建立新的FTD策略並選擇型別 威脅防禦設定。

步驟3.導覽至External Authentication索引標籤，如下圖所示：



步驟4.按一下Add時，系統會顯示一個對話方塊，如下圖所示：

- Enable for HTTP — 啟用此選項可透過HTTPS提供存取FTD。
- Enable for SSH — 啟用此選項可提供透過SSH存取FTD。
- 名稱 — 輸入LDAP連線的名稱。
- Description — 輸入外部身份驗證對象的可選說明。
- IP地址 — 輸入儲存外部身份驗證伺服器的IP的網路對象。如果沒有配置網路對象，請建立一個新對象。按一下(+)圖標。
- 身份驗證方法 — 選擇用於身份驗證的RADIUS或LDAP協定。
- Enable SSL-Enable此選項可加密身份驗證流量。
- 伺服器類型 — 選擇伺服器型別。眾所周知的伺服器型別是MS Active Directory、Sun、OpenLDAP和Novell。預設情況下，該選項設定為自動檢測伺服器型別。
- Port — 輸入進行驗證的連線埠。
- Timeout — 輸入身份驗證請求的超時值。
- 基本DN — 輸入基本DN以提供使用者可存在的範圍。
- LDAP範圍 — 選擇要查詢的LDAP範圍。作用域在同一級別內，或在子樹內查詢。
- Username — 輸入要繫結到LDAP目錄的使用者名稱。
- Authentication password — 輸入此使用者的密碼。

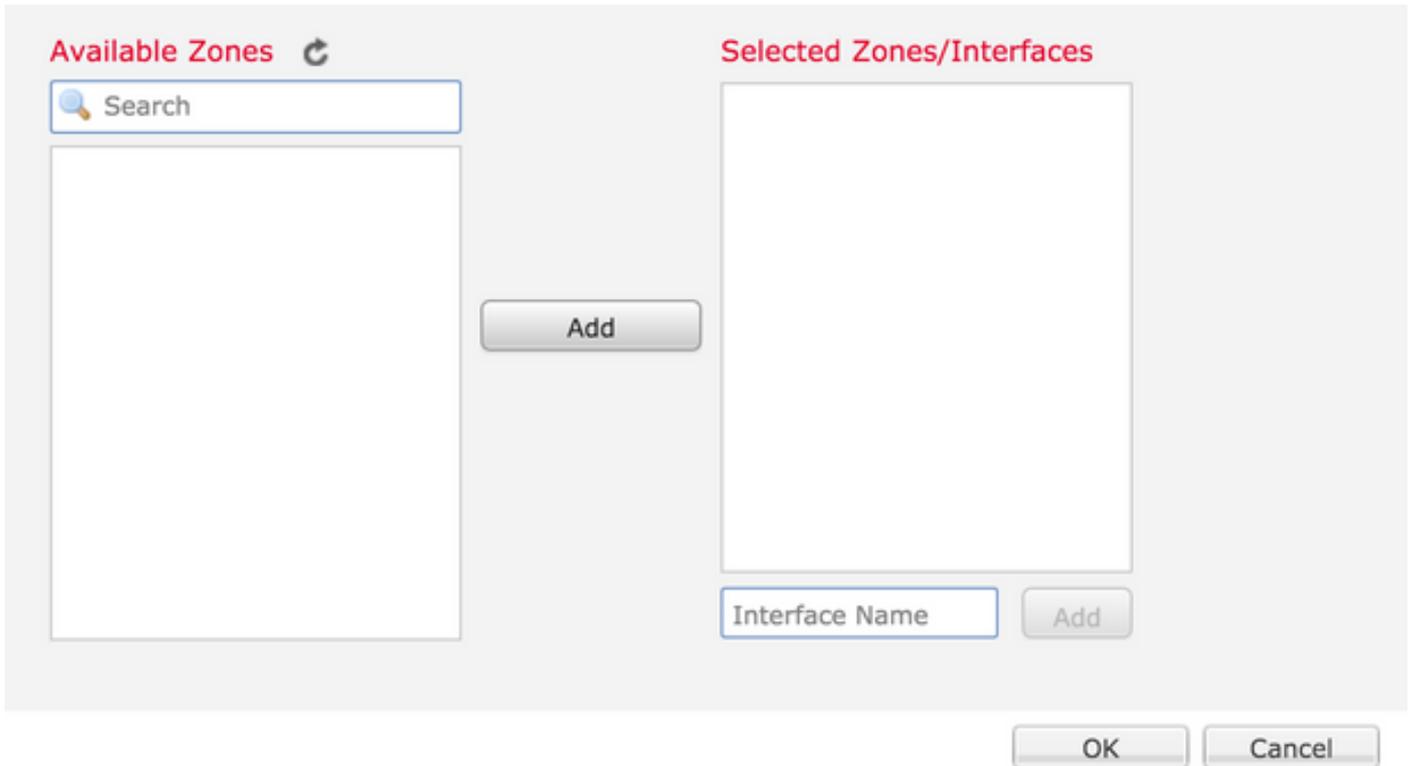
- Confirm — 重新輸入密碼。
- 可用接口 — 顯示FTD上可用介面的清單。
- 選定的區域和接口 — 顯示從中訪問身份驗證伺服器的介面的清單。

對於RADIUS身份驗證，沒有伺服器型別Base DN或LDAP Scope。埠是RADIUS埠1645。

Secret — 輸入RADIUS的金鑰。

Add External Authentication ? X

Enable for HTTP	<input type="checkbox"/>	
Enable for SSH	<input type="checkbox"/>	
Name*	<input type="text" value="LDAP"/>	
Description	<input type="text"/>	
IP Address*	<input type="text"/> +	
Authentication Method	<input type="text" value="LDAP"/>	
Enable SSL	<input type="checkbox"/>	
Server Type	<input type="text" value="AUTO-DETECT"/>	
Port	<input type="text" value="389"/>	
Timeout	<input type="text" value="10"/> (0 - 300 Seconds)	
Base DN	<input type="text"/> <input type="button" value="Fetch DN's"/>	ex. dc=cisco,dc=com
Ldap Scope	<input type="text"/>	
Username	<input type="text"/>	ex. cn=jsmith,dc=cisco,dc=com
Authentication Password	<input type="text"/>	
Confirm	<input type="text"/>	



步驟5.完成配置後，按一下OK。

步驟6. 儲存策略並將其部署到Firepower威脅防禦裝置。

注意：在軟體版本為6.1.0的裝置上，外部身份驗證不能用於通過SSH訪問融合的CLI

步驟3.配置SSH訪問。

通過SSH可以直接訪問融合的CLI。使用此選項直接訪問CLI和運行debug命令。本節介紹如何配置SSH以訪問FTD CLI。

註：在運行軟體版本6.0.1的FTD裝置上，平台設定上的SSH配置可直接訪問診斷CLI，而非CLISH。您需要連線到br1上配置的IP地址才能訪問CLISH。但是，在運行軟體版本6.1.0的FTD裝置上，通過SSH訪問時，所有介面都會導航到融合的CLI

在ASA上配置SSH有6個步驟

僅適用於6.0.1裝置：

這些步驟在軟體版本低於6.1.0和高於6.0.1的FTD裝置上執行。在6.1.0裝置上，這些引數是從作業系統繼承的。

步驟1.導覽至Devices>Platform Settings。

步驟2.您可以編輯點選鉛筆圖示時存在的策略，也可以在按一下New Policy 按鈕時建立新的Firepower威脅防禦策略，並選擇型別作為Threat Defense Settings。

步驟3. 導航到Secure Shell部分。此時會顯示一頁，如下圖所示：

SSH版本：選擇要在ASA上啟用的SSH版本。有三種選擇：

- 1：僅啟用SSH版本1
- 2：僅啟用SSH版本2
- 1和2：啟用SSH版本1和2

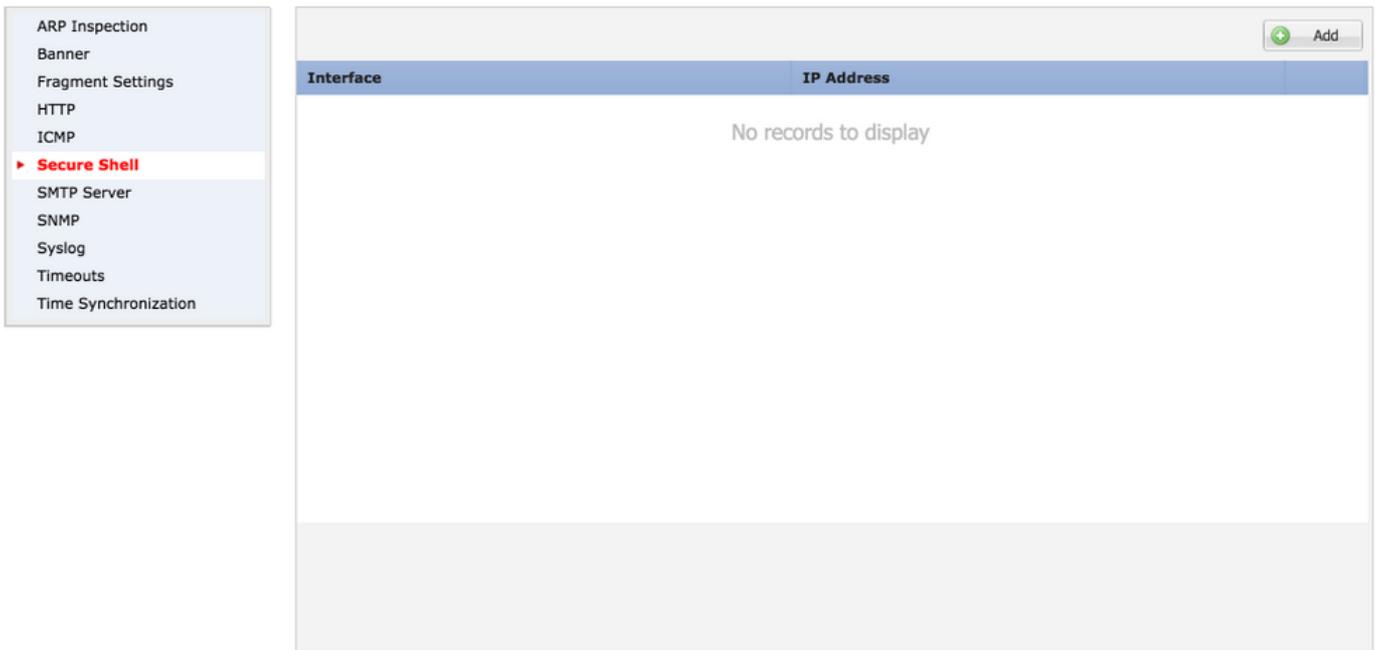
超時：輸入所需的SSH超時（分鐘）。

啟用安全複製 — 啟用此選項可將裝置配置為允許安全複製(SCP)連線並充當SCP伺服器。

The screenshot shows the configuration page for Secure Shell. On the left is a navigation menu with the following items: ARP Inspection, Banner, External Authentication, Fragment Settings, HTTP, ICMP, **Secure Shell** (highlighted), SMTP Server, SNMP, Syslog, Timeouts, and Time Synchronization. The main configuration area includes: SSH Version (dropdown menu set to '1 and 2'), Timeout (input field with '5', range '(1 - 60 mins)'), and Enable Secure Copy (checkbox, currently unchecked). An 'Add' button is located in the top right corner. Below these settings is a table with two columns: 'Interface' and 'IP Address'. The table is currently empty, displaying 'No records to display'.

在6.0.1和6.1.0裝置上：

這些步驟配置為限制通過SSH對特定介面和特定IP地址的管理訪問。



步驟1.按一下「Add」，然後設定以下選項：

IP地址：選擇包含允許通過SSH訪問CLI的子網的網路對象。如果不存在網路對象，請在按一下 (+)圖示時創建一個對象。

選定的區域/介面：選擇從中訪問SSH伺服器的區域或介面。

步驟2.按一下「OK」，如下圖所示：

Edit Secure Shell Configuration



IP Address*

Available Zones

Selected Zones/Interfaces

outside

使用此命令，可以在融合CLI（6.0.1裝置中的ASA診斷CLI）中檢視SSH配置。

```
> show running-config ssh
ssh 172.16.8.0 255.255.255.0 inside
```

步驟3.完成SSH配置後，按一下Save，然後將原則部署到FTD。

步驟4.配置HTTPS訪問。

要啟用對一個或多個介面的HTTPS訪問，請導航到平台設定中的HTTP部分。HTTPS訪問對於直接從診斷安全Web介面下載資料包捕獲進行分析，特別有用。

配置HTTPS訪問需執行6個步驟。

步驟1.導覽至Devices > Platform Settings

步驟2.編輯在按一下策略旁邊的鉛筆圖示時存在的平台設定策略，或在單擊「新建策略」(New

Policy)時建立新的FTD策略。選擇型別為Firepower威脅防禦。

步驟3.導覽至HTTP區時，會顯示頁面，如下圖所示。

啟用HTTP伺服器：啟用此選項以啟用FTD上的HTTP伺服器。

連線埠：選擇FTD接受管理連線的連線埠。

FTD-Policy

Enter a description

The screenshot shows the configuration interface for an FTD Policy. On the left is a navigation menu with the following items: ARP Inspection, Banner, External Authentication, Fragment Settings, HTTP (highlighted with a red arrow), ICMP, Secure Shell, SMTP Server, SNMP, Syslog, Timeouts, and Time Synchronization. The main content area is titled 'Enable HTTP Server' and has a checked checkbox. Below this is a 'Port' field containing the value '443', with a note '(Please don't use 80 or 1443)'. An 'Add' button is located in the top right corner. At the bottom, there is a table with two columns: 'Interface' and 'Network'. The table is currently empty, displaying the text 'No records to display'.

步驟4.按一下Add，頁面隨即顯示，如下圖所示：

IP地址 — 輸入允許對診斷介面進行HTTPS訪問的子網。如果網路對象不存在，請建立一個網路對象並使用(+)選項。

所選區域/接口 — 與SSH類似，HTTPS配置需要配置一個介面，通過該介面可通過HTTPS訪問。選擇通過HTTPS訪問FTD的區域或介面。

Edit HTTP Configuration



IP Address* 10.0.0.0_16

Available Zones

Search

Selected Zones/Interfaces

outside

Add

Interface Name Add

OK Cancel

在融合CLI (6.0.1裝置中的ASA診斷CLI) 中檢視HTTPS配置並使用此命令。

```
> show running-config http  
http 172.16.8.0 255.255.255.0 inside
```

步驟5.完成必要的配置後，選擇OK。

步驟6.輸入所有必需資訊後，按一下Save，然後將策略部署到裝置。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

以下是對FTD上的管理存取問題進行疑難排解的基本步驟。

步驟1.確保該介面已啟用且配置有IP地址。

步驟2.確保外部身份驗證按配置工作，並可從平台設定的外部身份驗證部分中指定的相應介面訪問。

步驟3.確保FTD上的路由準確。在FTD軟體版本6.0.1中，導覽至system support diagnostic-cli。分別運行show route和show route management-only命令以檢視FTD和管理介面的路由。

在FTD軟體版本6.1.0中，直接在融合的CLI中執行命令。

相關資訊

- [技術支援與文件 - Cisco Systems](#)

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）。