在FTD上設定VRF感知系統日誌

目錄

簡介

必要條件

- 需求
- 採用元件
- 最低軟體和硬體平台
- Snort3、多例項/情景和HA/集群支援

設定

- 網路圖表
- 組態
- 工作方式
- 配置虛擬路由器
- 在FMC中配置FTP伺服器的必備條件
- 組態

驗證

- Pre 7.4.1
- Post 7.4.1
- FTP伺服器驗證
- Pre 7.4.1
- Post 7.4.1

簡介

本檔案將介紹FTD上VRF感知系統日誌的設定步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 系統日誌
- Firepower Threat Defense (FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

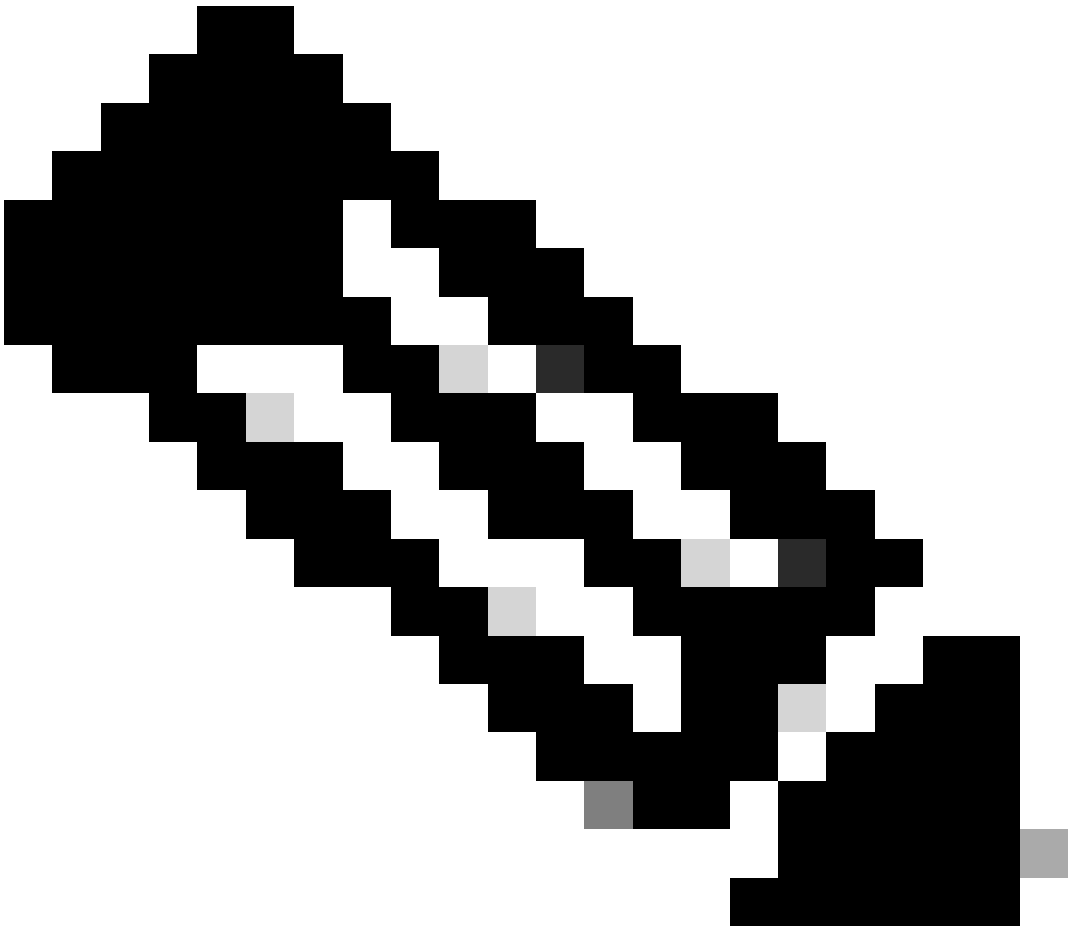
- 安全防火牆管理中心(FMCv)v7.4.2
- 安全防火牆威脅防御虛擬(FTDv)v7.4.2

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。

最低軟體和硬體平台

- 應用程式和最低版本：安全防火牆7.4.1
- 支援的託管平台和版本：所有支援FTD 7.4.1
- 經理：
  1)FMC on-perm + FMC REST API
  2)雲交付的FMC
  3)FDM + REST API

Snort3、多例項/情景和HA/集群支援



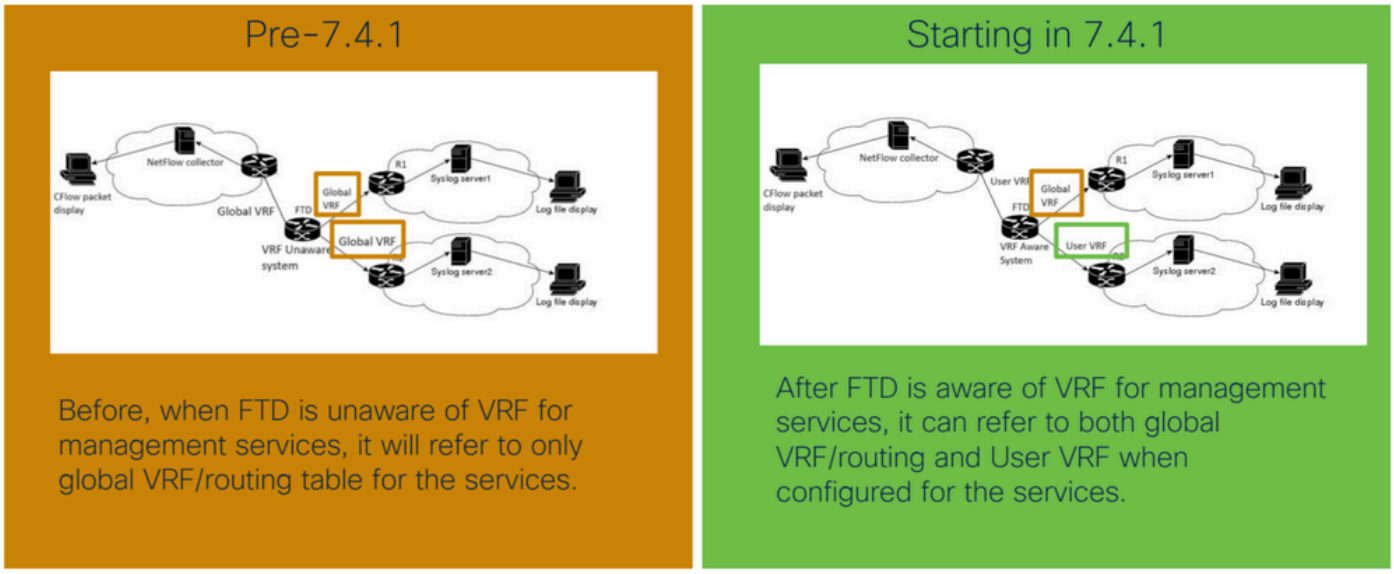
附註：與IPv4和IPv6系統日誌伺服器配合使用。Syslog ftp伺服器尚不支援IPv6。

- 支援多例項。

- 受HA'd裝置支援。
- 群集裝置支援。

設定

網路圖表



7.4之前的版本和之後的網路圖比較。

組態

虛擬路由和轉送(VRF)技術用於網路，允許同一個路由器中同時存在多個路由表例項，從而在不同的虛擬網路之間提供網路隔離。每個VRF例項與其他例項無關，它們之間的流量保持獨立。多VRF功能使服務提供商能夠支援多個VPN和服務，即使其IP地址重疊。它使用輸入介面為各種服務指定路由，並通過為每個VRF分配第3層介面來建立虛擬資料包轉發表。管理服務（系統日誌、NetFlow）預設使用全域性VRF。使用者希望將使用者VRF用於管理服務和全域性VRF，因為並非所有上傳目標都可通過全域性VRF訪問。

在本文檔中，全域性+使用者VRF =多VRF

為使用者VRF啟用系統日誌。

- 系統日誌可以在多VRF環境中使用ftp服務。

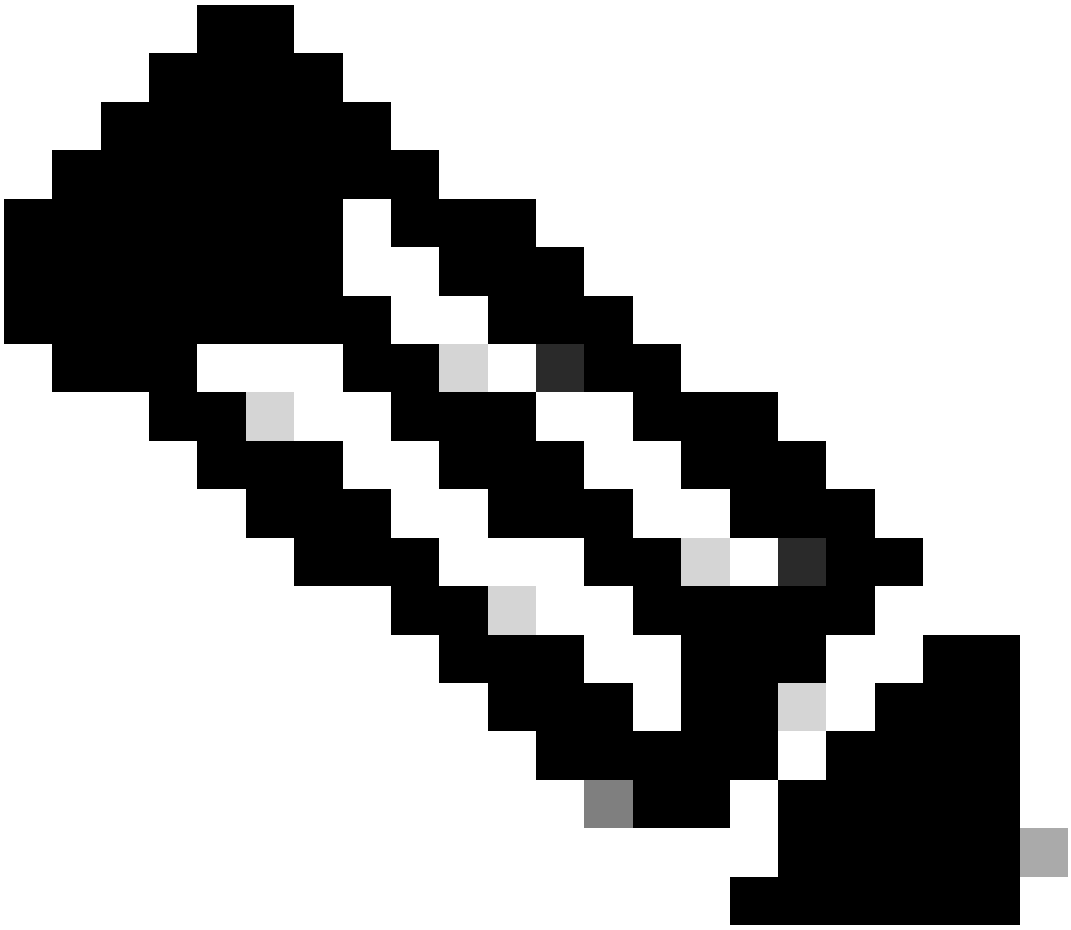
工作方式

當介面配置有使用者VRF時，路由查詢在VRF路由域而非預設全域性路由域中進行。

- 支援兩種型別的伺服器配置：

1. 將日誌記錄消息傳送到系統日誌伺服器，以監控網路流量並對其進行故障排除。
2. 將日誌緩衝區內容作為文本檔案傳送到FTP伺服器

- 系統日誌將日誌傳送到該VRF中各自的UDP/TCP伺服器。
- 對於緩衝區封裝系統日誌，會將日誌傳送到該VRF中配置的FTP伺服器。

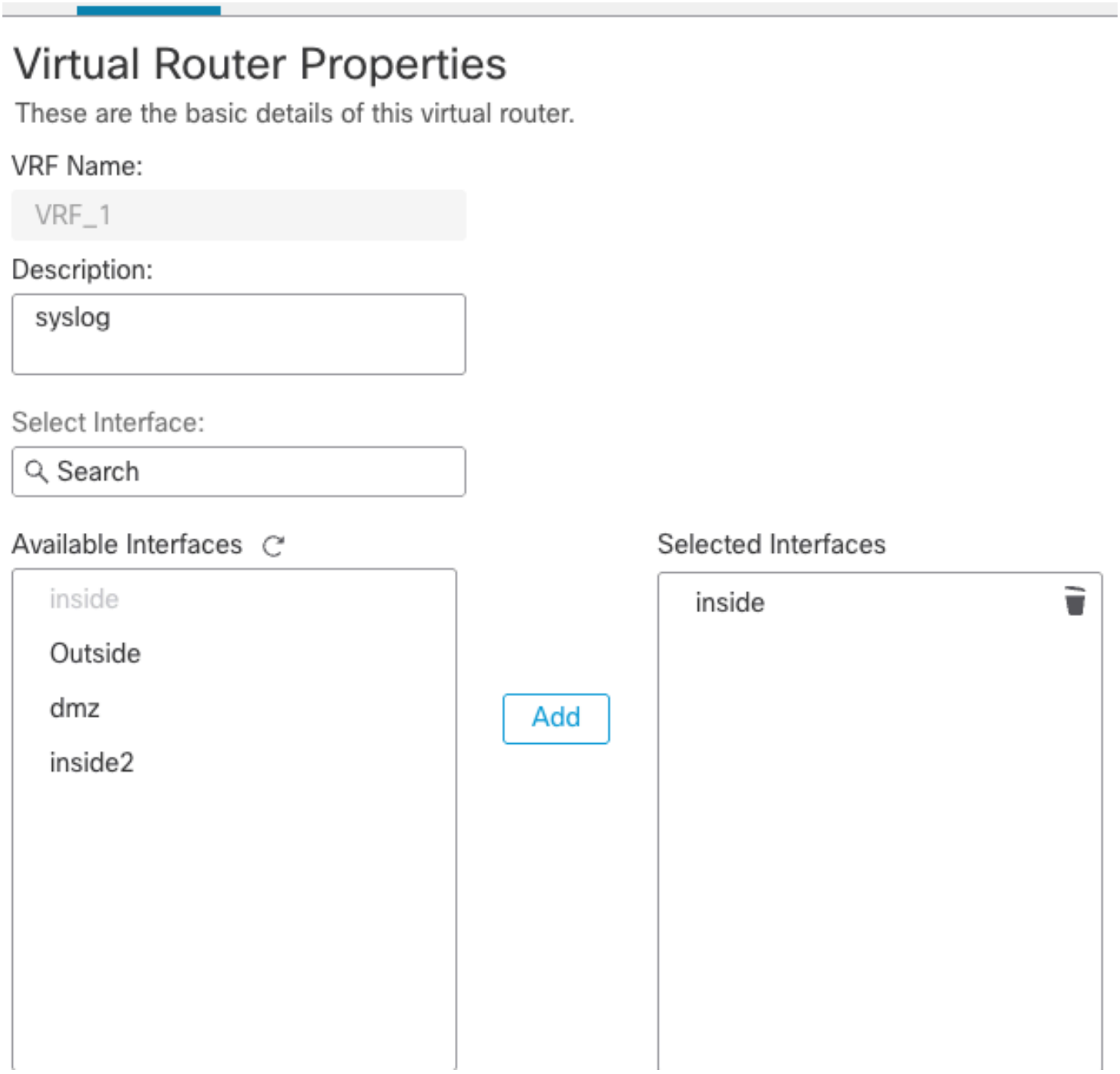


附註：系統日誌伺服器和FTP伺服器可以是不同VRF的一部分。

配置虛擬路由器

步驟1.建立VRF

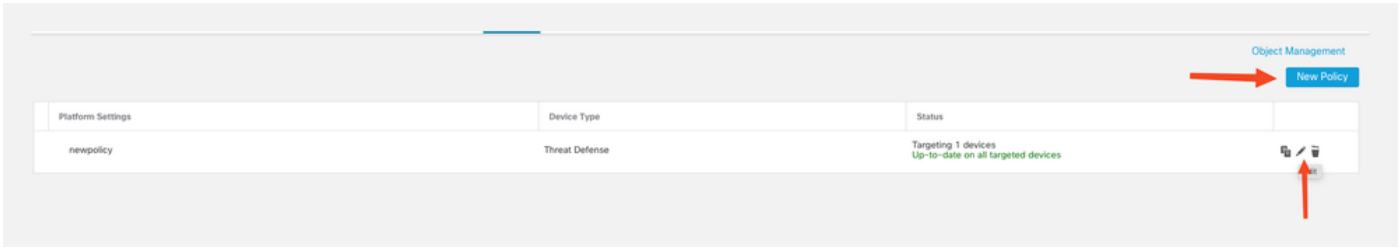
- 登入到FMC，然後導航到Device > Device Management。
- 選擇Device，然後按一下Pencil圖示進行編輯。
- 導覽至Routing> Manage Virtual Router > Add Virtual Router。
- 在VRF Name中輸入name。
- 選擇interface，然後按一下Add和Save。



將介面新增到VRF

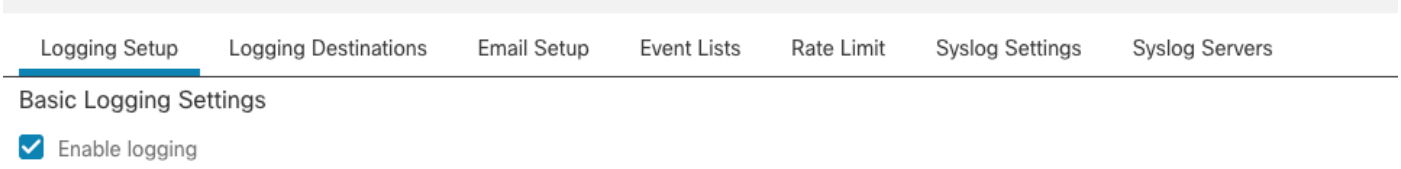
步驟2.配置日誌記錄設定。

- 導覽至Devices > Platform Settings。
- 建立新策略或編輯現有策略上的Pencil圖示。



建立平台設定

- 選擇Logging Setup和Enable logging。

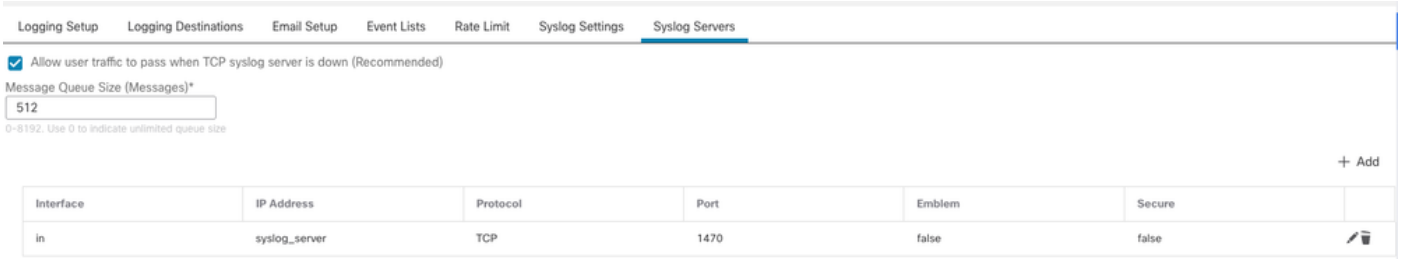


啟用記錄

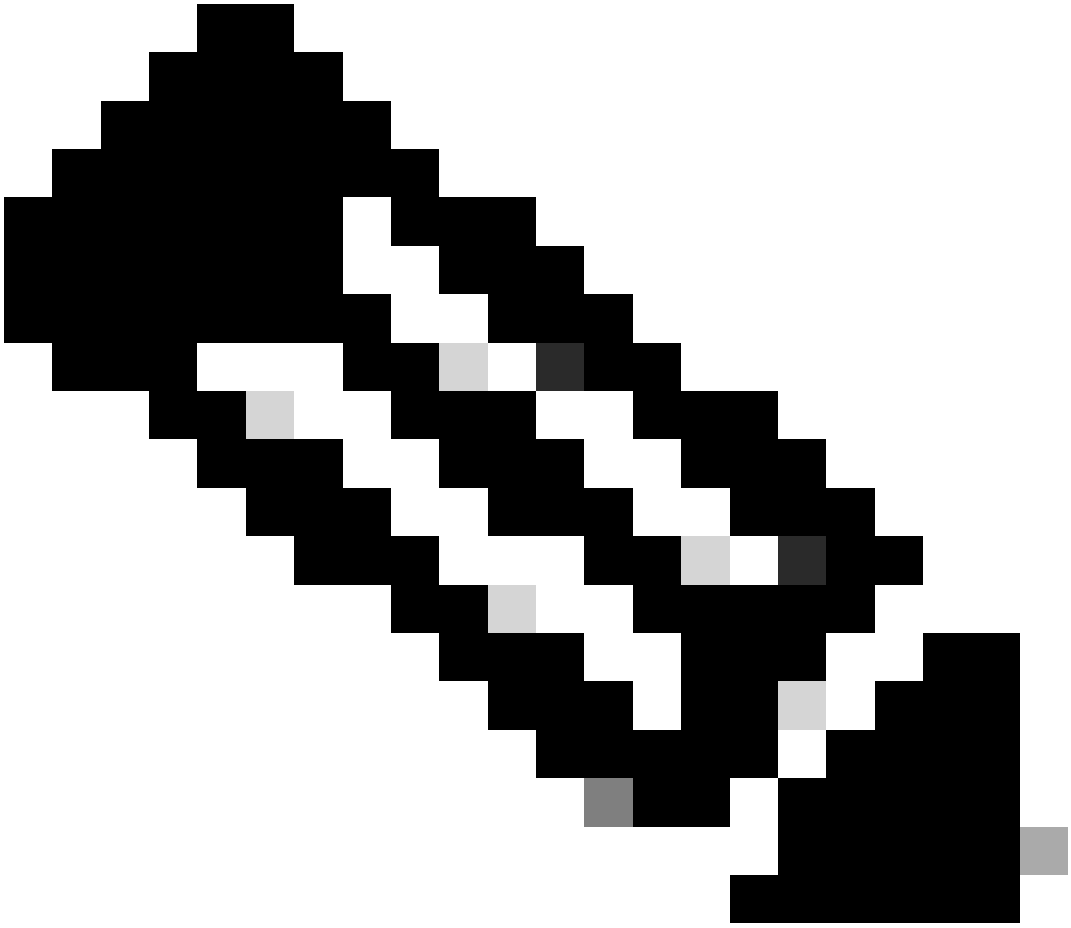
- 選擇Logging Destination，然後按一下Add。
- 將Logging Destination設置為Syslog伺服器。

將目標籤錄為系統日誌伺服器

- 選擇Syslog Servers > Add。



新增具有VRF感知介面的Syslog伺服器



附註：內部介面是中的安全區域的一部分。

- logging host命令中配置的介面現在可識別VRF。
- 按一下「Save」。

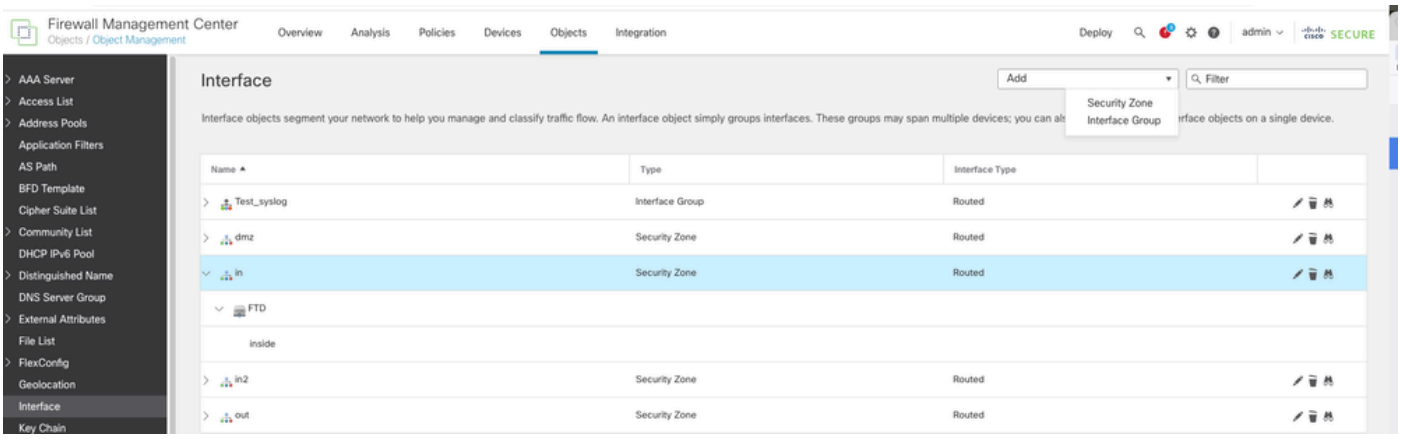
在FMC中配置FTP伺服器的必備條件

- 使用Interface Group Object。
- 介面組對象可以同時具有使用者和全域性VRF。

組態

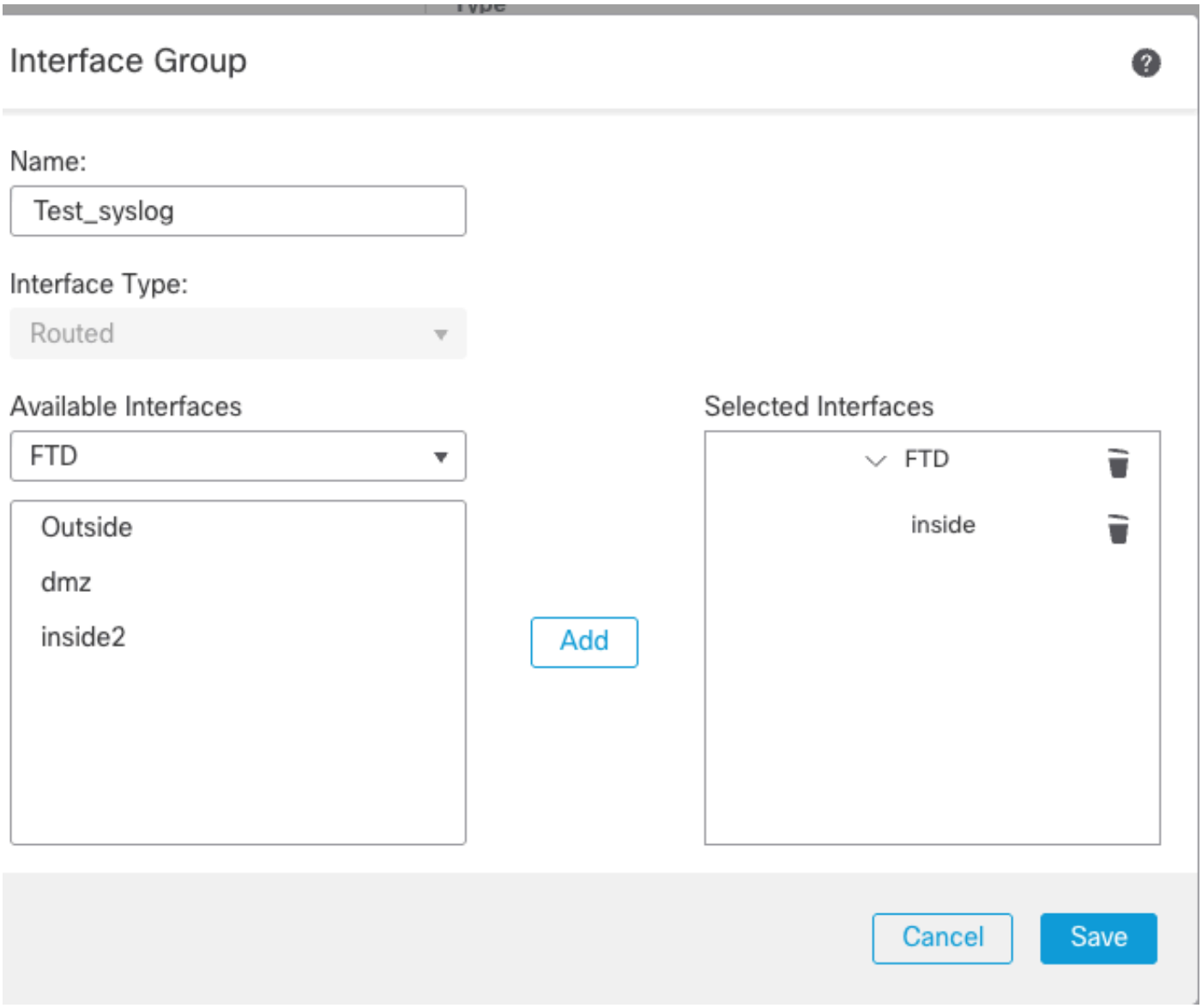
步驟 1.

- 導航到Object > Object Management > Interface > Add > Interface Group。



新增介面組

- 從下拉選單中選擇Device,Add the VRF Interface。

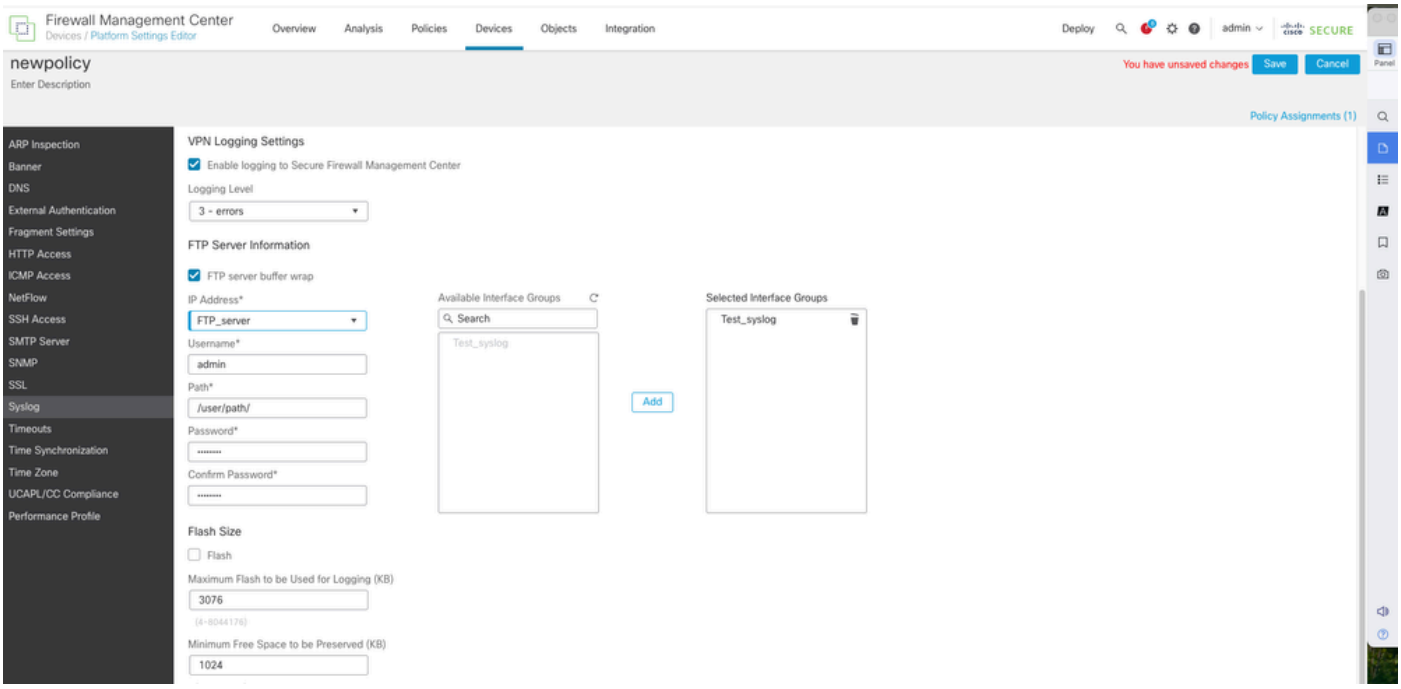


新增VRF感知介面

步驟 2.

- 導航到Devices > Platform Settings > Syslog > Logging Setup。啟用FTP服務器緩衝區wrap。

- 按一下「Save」。



啟用具有VRF感知介面的FTP伺服器

驗證

Pre 7.4.1

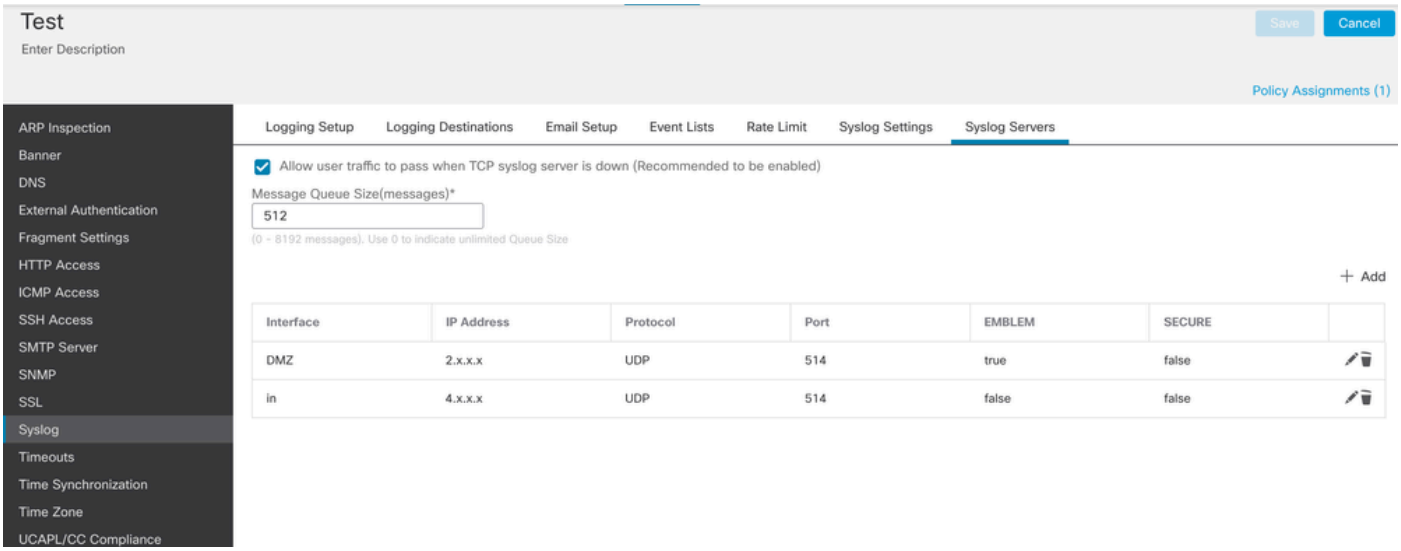
在本測試中，FTD和FMC為7.0.5。

FTD設定為VRF，且dmz介面已指派給VRF。

dmz介面配置有syslog server logging host。

此外，內部介面還配置了syslog設定。

內部介面是全域性VRF的一部分。

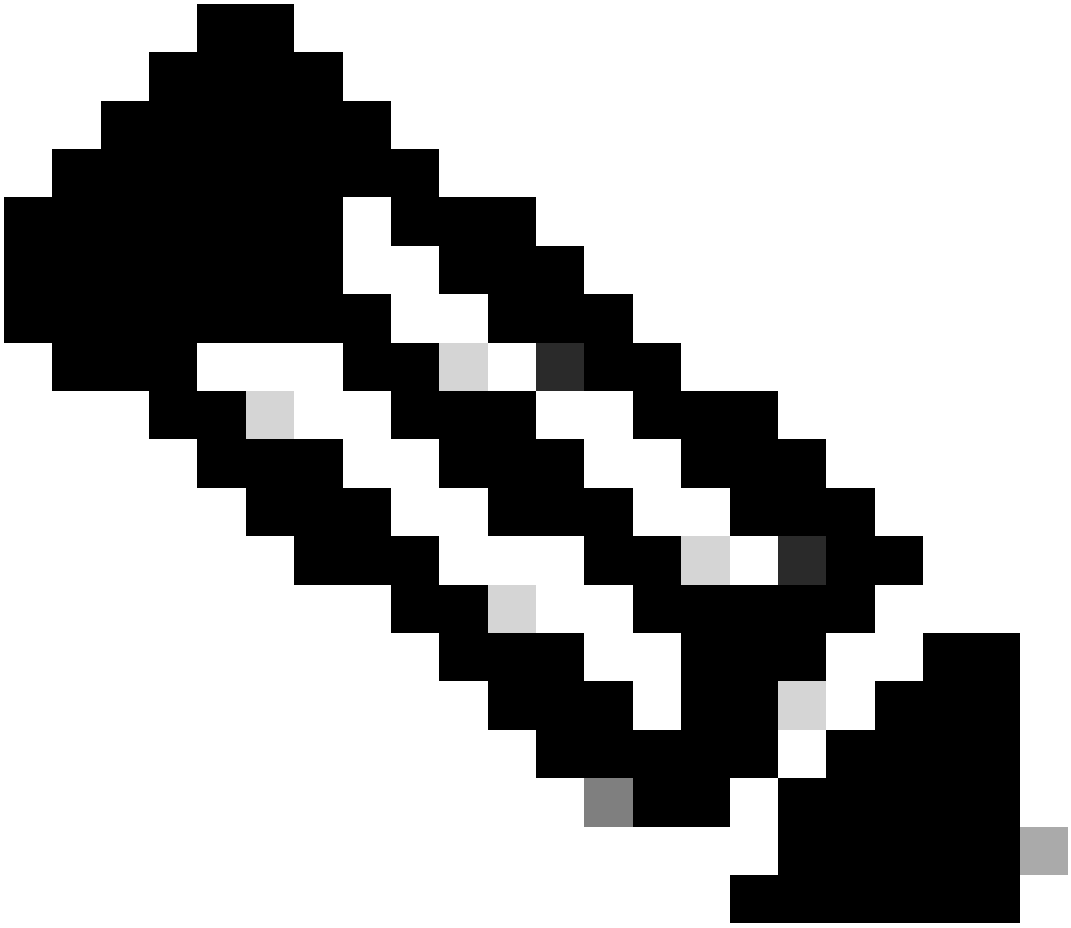


CLI 驗證

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 1193 messages logged
        Logging to inside 4.x.x.x, UDP TX:52
    Global TCP syslog stats::
        NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
        CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
        PARTIAL_REWRITE_CNT: 0
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, 0 messages logged
```

```
> show vrf

Name            VRF ID          Description             Interfaces
VRF-1           1                                   dmz
```



附註：目標2.x.x.x的syslog伺服器在FTD CLI的日誌設定中不可用。這是使用者VRF的一部分。
目標4.x.x.x的Syslog伺服器可在FTD CLI的日誌記錄設定中找到。這是全球VRF的一部分。

Post 7.4.1

CLI 驗證

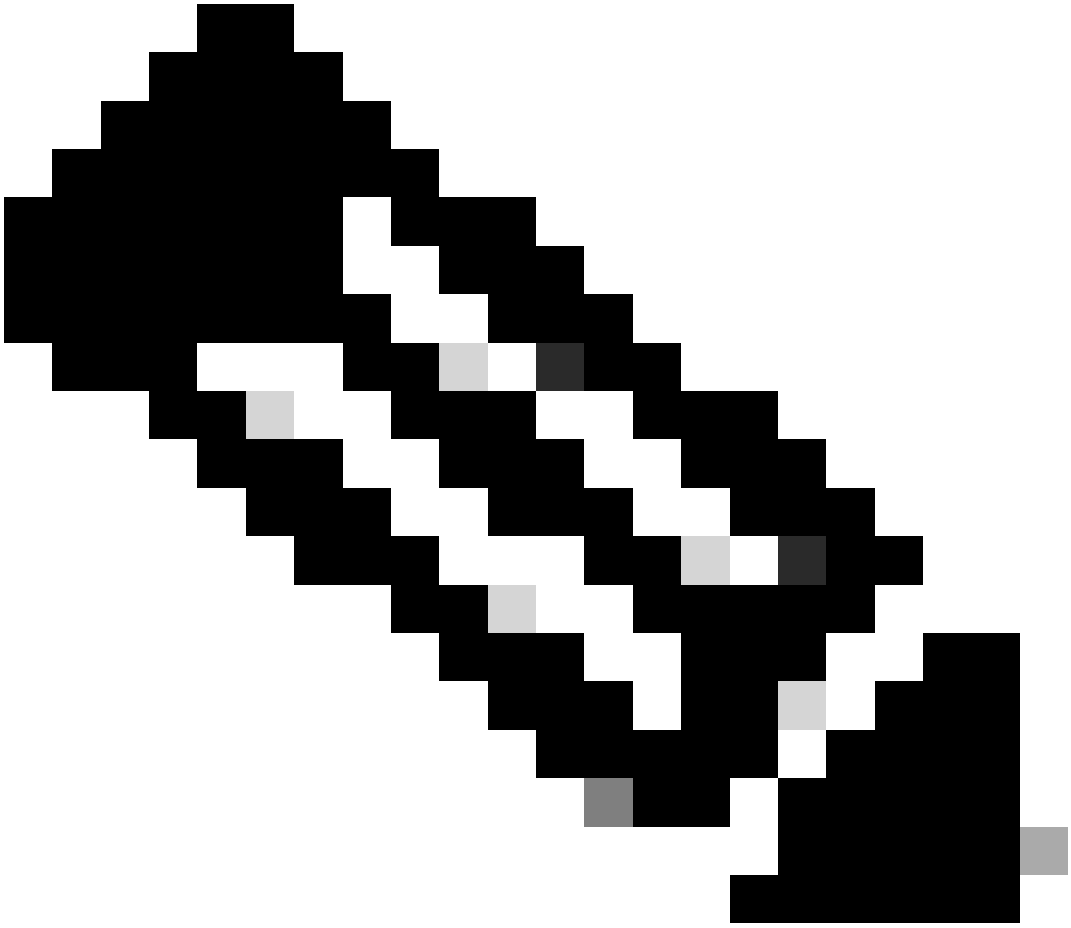
```
ftd1# show vrf

Name                            VRF ID     Description     Interfaces
VRF_1                           1          syslog          inside
```

```
td1# show logging
Syslog logging: enabled
```

```
Facility: 20
Timestamp logging: disabled
Hide Username logging: enabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: level informational, class auth, facility 20, 19284 messages logged
    Logging to inside 192.x.x.x tcp/1470 Not connected since Thu, 20 Mar 2025 01:53:17 UTC TX:0
        TCP SYSLOG_PKT_LOSS:0
        TCP [Channel Idx/Not Putable counts]: [0/0]
        TCP [Channel Idx/Not Putable counts]: [1/0]
        TCP [Channel Idx/Not Putable counts]: [2/0]
        TCP [Channel Idx/Not Putable counts]: [3/0]

Global TCP syslog stats::
    NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 1584
    CHANNEL_FLAP_CNT: 1584, SYSLOG_PKT_LOSS: 0
    PARTIAL_REWRITE_CNT: 0
Permit-hostdown logging: enabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
FMC logging: list MANAGER_VPN_EVENT_LIST, class auth, 0 messages logged
```



附註：Syslog伺服器主機192.x.x.x使用VRF感知內部介面。

FTP伺服器驗證

Pre 7.4.1

- 在FMC上，FTP伺服器設定沒有選擇要使用的介面的選項。只有syslog伺服器選項的IP地址可用。

Specify FTP Server Information

☑ FTP Server Buffer Wrap

IP Address*

Username*

Path*

Password*

Confirm*

Specify Flash Size

☐ Flash

Maximum Flash to be used by Logging(KB)

3076

(4-8044176)

Minimum free Space to be preserved(KB)

1024

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）。