為使用VPN通道的系統日誌配置FTD資料介面

目錄

簡介

本檔案介紹如何將Cisco FTD資料介面設定為透過VPN通道傳送的Syslogs的來源。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆威脅防禦(FTD)上的系統日誌配置
- 常規系統日誌
- 思科安全防火牆管理中心(FMC)

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- Cisco FTD版本7.3.1
- Cisco FMC版本7.3.1

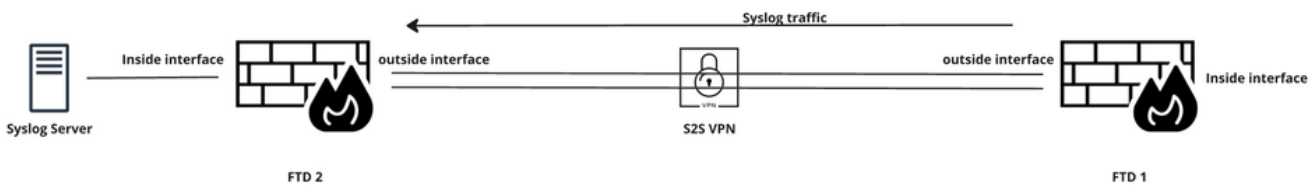
免責宣告：本檔案所引用的網路和IP位址未與任何個別使用者、群組或組織關聯。此配置專為實驗室環境而建立。

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

本檔案介紹一種解決方案，該方案將FTD的一個資料介面用作系統日誌的來源，這些系統日誌必須透過VPN通道傳送到位於遠端站點中的Syslog伺服器。

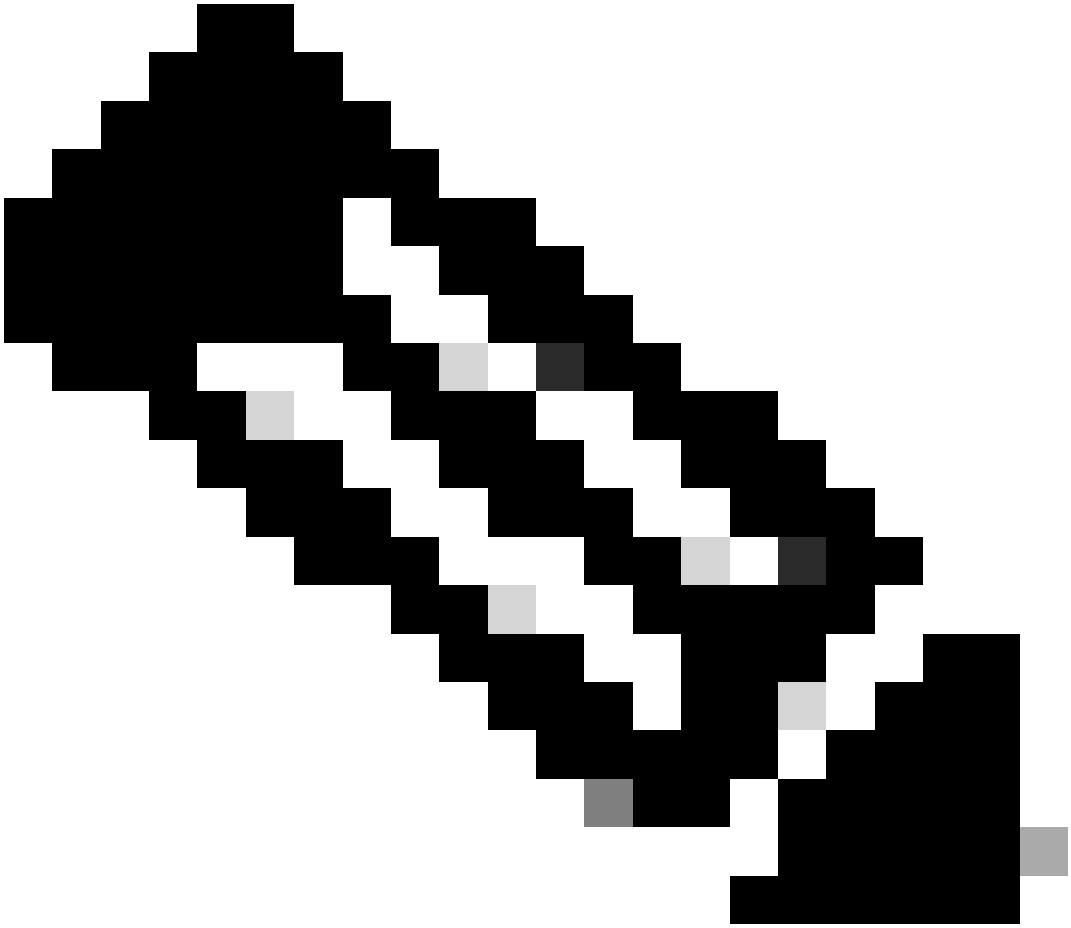
圖表



網路圖表

若要指定來源透過通道傳送的Syslog流量的介面，可以透過Flex Config套用**management**-access指令。

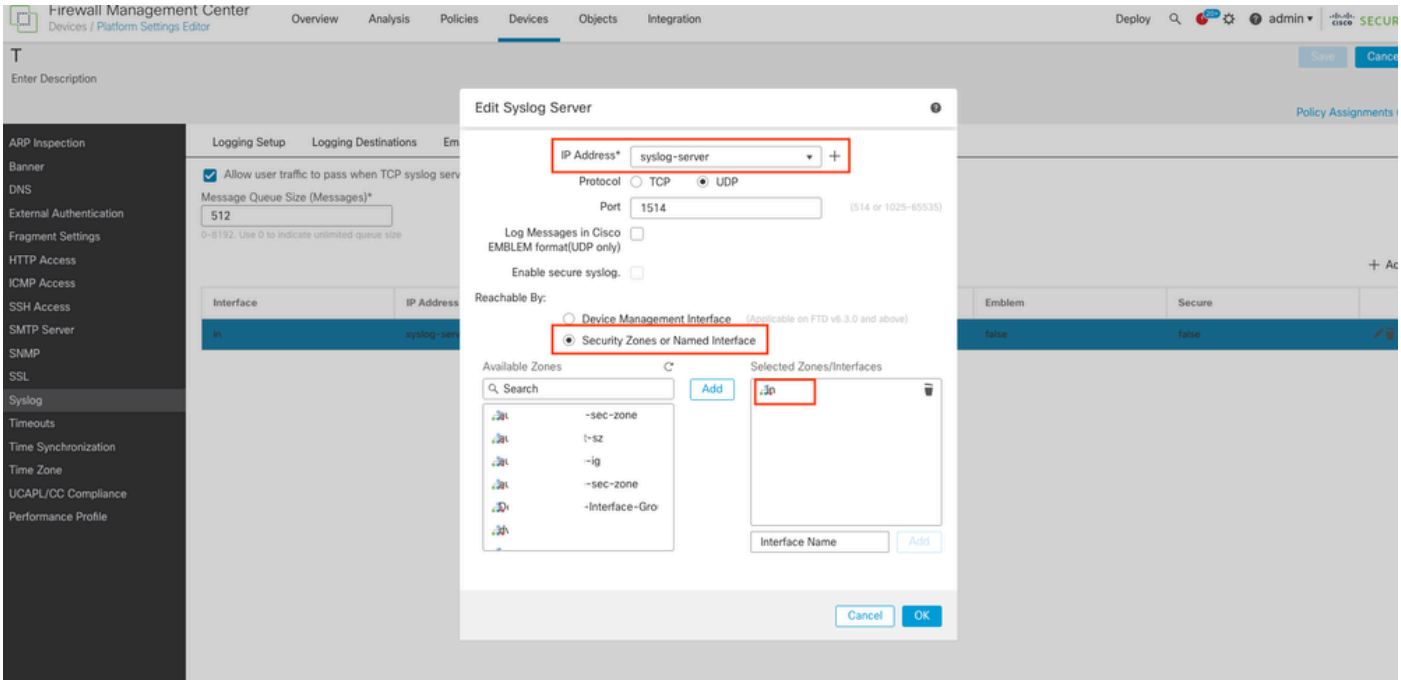
此命令不僅允許您使用管理訪問介面作為通過VPN隧道傳送的系統日誌消息的源介面，還允許您在使用全隧道IPsec VPN或SSL VPN客戶端或跨站點間IPsec隧道時通過SSH和Ping連線到資料介面。



附註：您只能定義一個管理訪問介面。

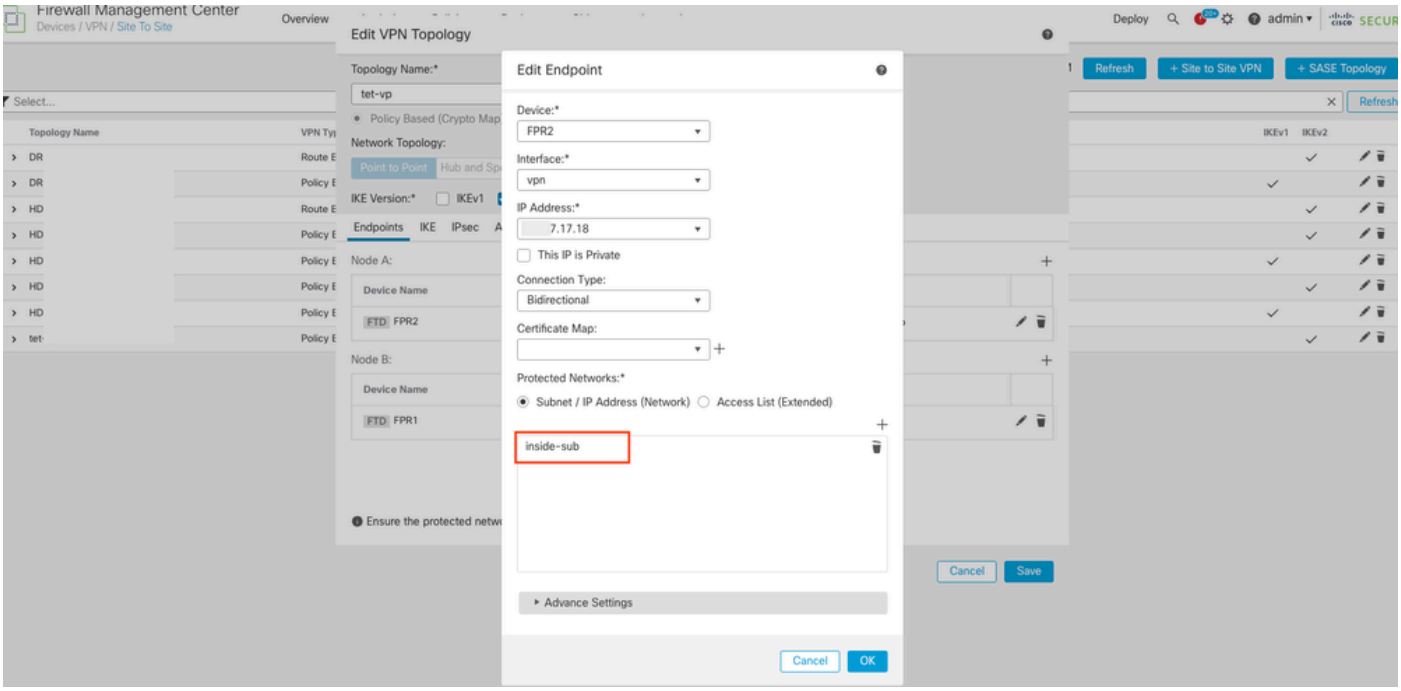
設定

1.在Devices > Platform Settings下為FTD設定系統日誌。配置系統日誌伺服器時，請確保選擇Security Zones或Named Interface選項而不是Device Management Interface，然後選擇management-access interface以源系統日誌流量。



系統日誌伺服器配置

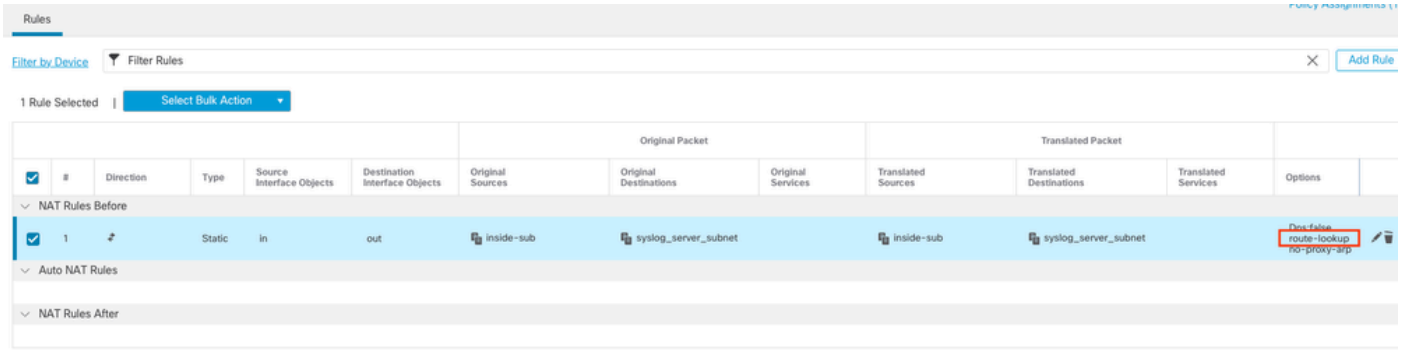
2.確保在VPN端點的受保護網路下新增管理訪問介面網路。(在Devices > Site To Site > VPN Topology > Node下)。



受保護網路配置

3.確保在管理訪問介面網路和VPN網路之間配置身份NAT（VPN流量的通用NAT配置）。 必須在NAT規則的Advanced 部分下選擇Perform Route Lookup for Destination Interface 選項。

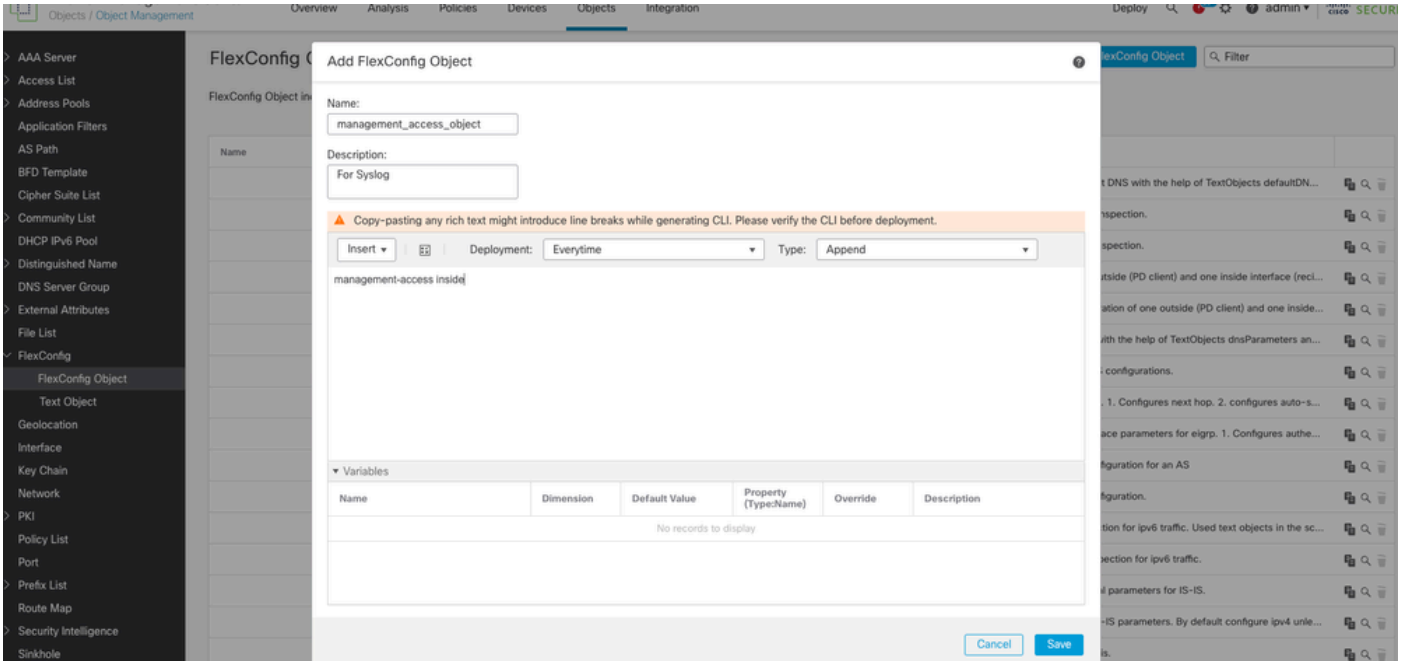
如果沒有路由查詢，FTD會通過NAT配置中指定的介面傳送流量，無論路由表如何顯示。



身份NAT配置

4.您現在可以在對象>對象管理> FlexConfig對象下配置management-access <interface name> (在此情況中為management-access inside)。

將其分配給目標設備FlexConfig策略並部署配置。



FlexConfig配置

驗證

管理訪問配置：

<#root>

firepower#

show run | in management-access

management-access inside

系統日誌配置：

<#root>

firepower#

show run logging

logging enable
logging timestamp
logging trap debugging
logging FMC MANAGER_VPN_EVENT_LIST

logging host inside 192.168.17.17 17/1514

logging debug-trace persistent
logging permit-hostdown
logging class vpn trap debugging

通過VPN隧道傳送的系統日誌流量：

<#root>

FTD 2:
firepower#

show conn

36 in use, 46 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

UDP vpn 192.168.17.17:1514 inside 10.17.17.18:514, idle 0:00:02, bytes 35898507, flags -

FTD 1:
firepower#

show conn

6 in use, 9 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

UDP server 192.168.17.17:1514 vpn 10.17.17.18:514, idle 0:00:00, bytes 62309790, flags -

firepower#

show crypto ipsec sa

interface: vpn
Crypto map tag: CSM_vpn_map, seq num: 1, local addr: 17.xx.xx.18

access-list CSM_IPSEC_ACL_2 extended permit ip 10.17.17.0 255.255.255.0 192.168.17.0 255.255.255.0
Protected vrf (ivrf):

local ident (addr/mask/prot/port): (10.17.17.0/255.255.255.0/0/0)

----------> Inside interface subnet

remote ident (addr/mask/prot/port): (192.168.17.0/255.255.255.0/0/0)

```
------------> Syslog server subnet
current_peer: 17.xx.xx.17


#pkts encaps: 309957, #pkts encrypt: 309957, #pkts digest: 309957


#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 309957, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

相關資訊

- 透過 FMC 設定 FTD 中的記錄
- 在FMC管理的FTD上配置站點到站點VPN

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）。