

在FDM管理的資料介面上的點對點VPN上設定SNMP

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹在FTD裝置資料介面的資料介面上透過點對點VPN設定遠端的SNMP。

必要條件

繼續進行組態之前，請確認您已具備以下必要條件：

- 基本瞭解以下主題：
 - 由Firepower裝置管理器(FDM)管理的Cisco Firepower威脅防禦(FTD)。
 - 思科調適型安全裝置(ASA)。
 - 簡易網路管理通訊協定(SNMP)。
 - 虛擬私人網路(VPN)。
- 對FTD和ASA裝置的管理訪問。
- 確保您的網路處於活動狀態，並瞭解所有命令的潛在影響。

需求

- 由FDM 7.2.7版管理的思科FTD
- Cisco ASA版本9.16
- SNMP伺服器詳細資訊 (包括IP地址、社群字串)
- 站點到站點VPN配置詳細資訊 (包括對等體IP、預共用金鑰)
- FTD必須至少是6.7版，才能使用REST API設定SNMP。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 由Firepower裝置管理器(FDM) 7.2.7版管理的Cisco Firepower威脅防禦(FTD)。
- 思科自適應安全裝置(ASA)版本9.16。
- SNMP伺服器 (任何標準SNMP伺服器軟體)

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

網路管理員可以按照概述的這些步驟確保遠端監控網路裝置。

SNMP (簡單網路管理協定) 用於網路管理和監控。在此設定中，SNMP流量透過與ASA建立的站點到站點VPN從FTD傳送到遠端SNMP伺服器。

本指南旨在幫助網路管理員在FTD裝置的資料介面上透過站點到站點VPN配置遠端端的SNMP。此設定適用於遠端監控和管理網路裝置。在此設定中，使用SNMP v2，SNMP流量透過與ASA建立的站點到站點VPN從FTD資料介面傳送到遠端SNMP伺服器。

使用的介面稱為「內部」，但此配置可應用於其他型別的「到裝置」流量，並可利用防火牆中非VPN終止介面的任何介面。



注意：當FTD執行版本6.7和更新版本，且由FDM管理時，只能透過REST API設定SNMP。

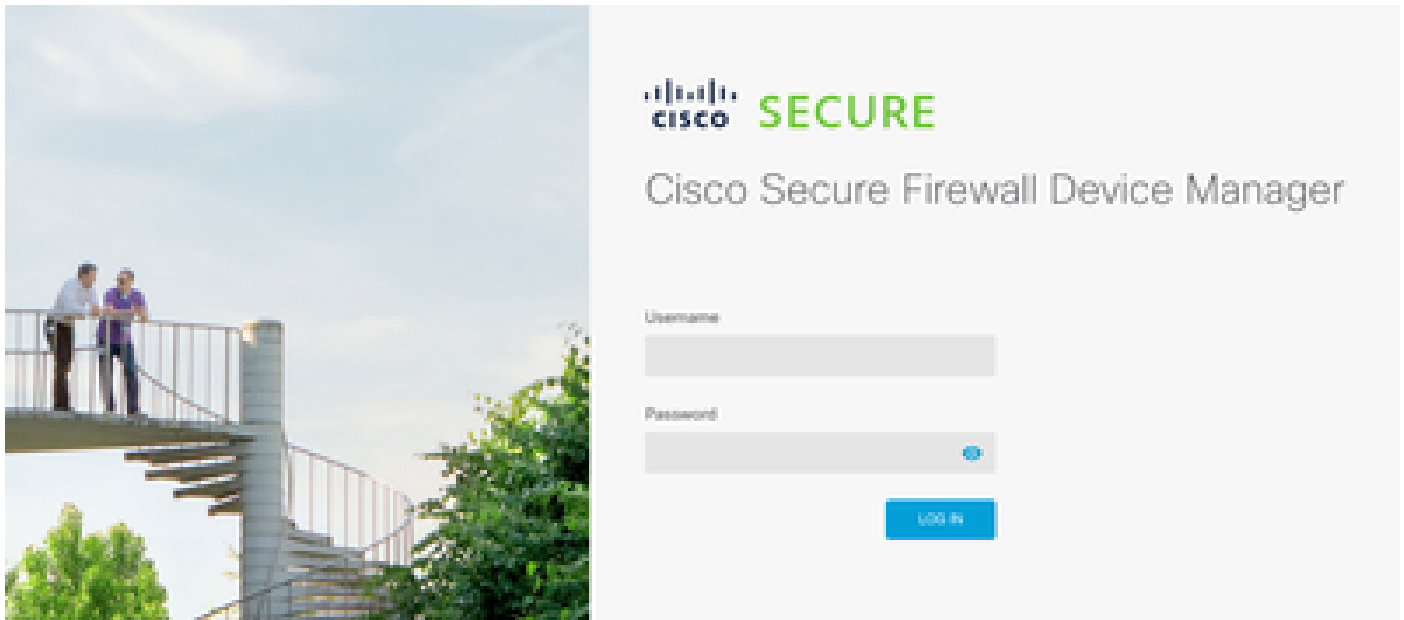
設定



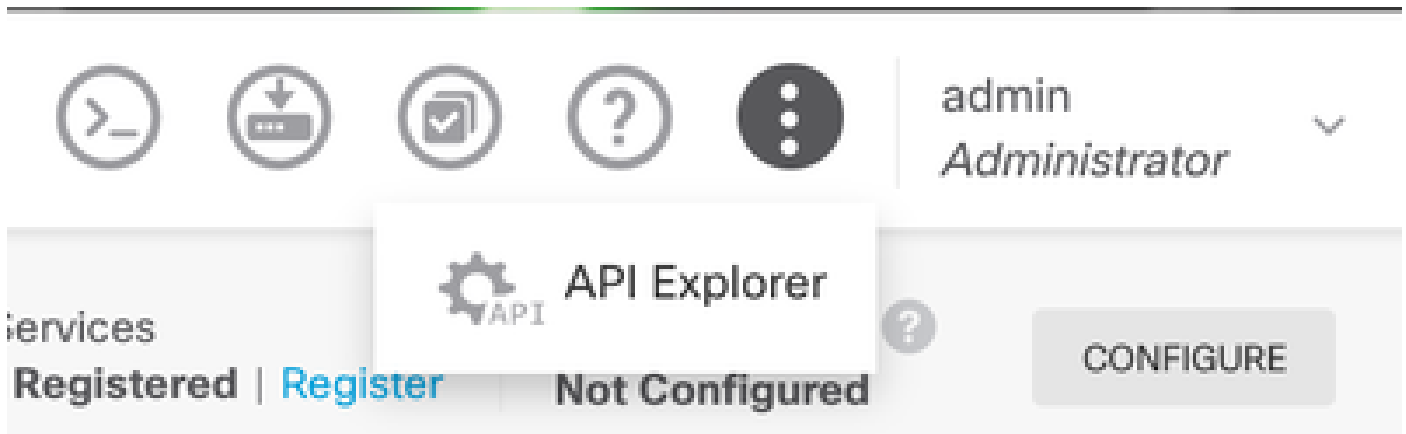
注意：此配置認為已在裝置之間配置站點到站點VPN。有關如何配置站點到站點VPN的其他詳細資訊，請檢視配置指南。[在FDM管理的FTD上設定網站間VPN](#)

組態

1. 登入您的FTD。



2. 在裝置概述下，導航至API瀏覽器。



3. 在FTD上設定SNMPv2

- 獲取介面資訊。



4. 向下滾動並選擇Try it out！按鈕以進行API呼叫。成功的呼叫返回響應代碼200

TRY IT OUT!

Hide Response

Curl

```
curl -X GET --header 'Accept: application/json' 'https://
```

Request URL

```
https://10.57.58.1/34/api/fdm/v6/devices/default/interfaces
```

Response Body

```
{
  "version": "mqjiipiswsgsx",
  "name": "inside",
  "description": null,
  "hardwareName": "GigabitEthernet0/1",
  "monitorInterface": false,
  "ipv4": {
    "ipType": "STATIC",
    "defaultRouteUsingDHCP": false,
    "dhcpRouteMetric": null,
    "ipAddress": {
      "ipAddress": "10.57.58.1",
      "netmask": "255.255.255.0",
      "standbyIpAddress": null,
      "type": "haipv4address"
    },
    "dhcp": false,
    "addressNull": false,
    "type": "interfaceipv4"
  }
}
```

Response Code

200

- 為SNMP主機建立網路對象配置。

NetworkObject

GET

/object/networks

POST

/object/networks

- 建立新的SNMPv2c主機對象。

SNMP

GET	/devicesettings/default/snmpservers
GET	/devicesettings/default/snmpservers/{objId}
PUT	/devicesettings/default/snmpservers/{objId}
GET	/object/snmpusers
POST	/object/snmpusers
DELETE	/object/snmpusers/{objId}
GET	/object/snmpusers/{objId}
PUT	/object/snmpusers/{objId}
GET	/object/snmpusergroups
POST	/object/snmpusergroups
DELETE	/object/snmpusergroups/{objId}
GET	/object/snmpusergroups/{objId}
PUT	/object/snmpusergroups/{objId}
GET	/object/snmphosts
POST	/object/snmphosts
DELETE	/object/snmphosts/{objId}
GET	/object/snmphosts/{objId}
PUT	/object/snmphosts/{objId}

有關其他詳細資訊，請檢視《配置指南》[，在Firepower FDM上配置SNMP並對其進行故障排除](#)

5. 在裝置上配置SNMP之後，導航到高級配置部分中的裝置，然後選擇檢視配置。

Advanced Configuration

Includes: FlexConfig, Smart CLI

[View Configuration](#)



6. 在FlexConfig部分中，選擇FlexConfig objects，然後建立一個新對象，命名該對象並在模板部分增加management-access命令，指定介面，然後在模板否定部分增加命令否定項。

FlexConfig

FlexConfig Objects

FlexConfig Policy

Edit FlexConfig Object

Name

Description

This command gives mgmt access to the inside interface.


Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template Expand Reset

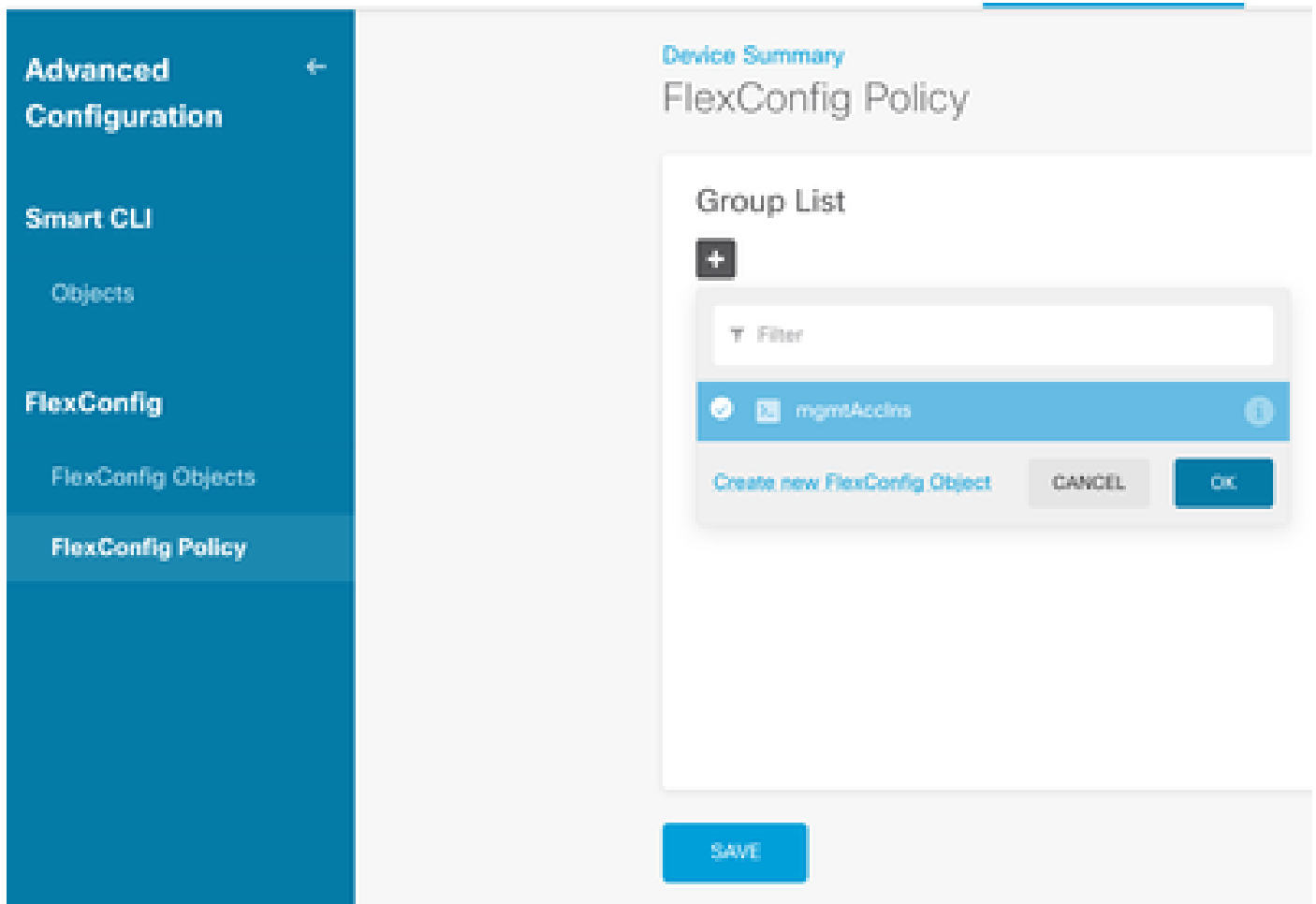
```
1 management-access Inside
```

Negate Template  Expand Reset

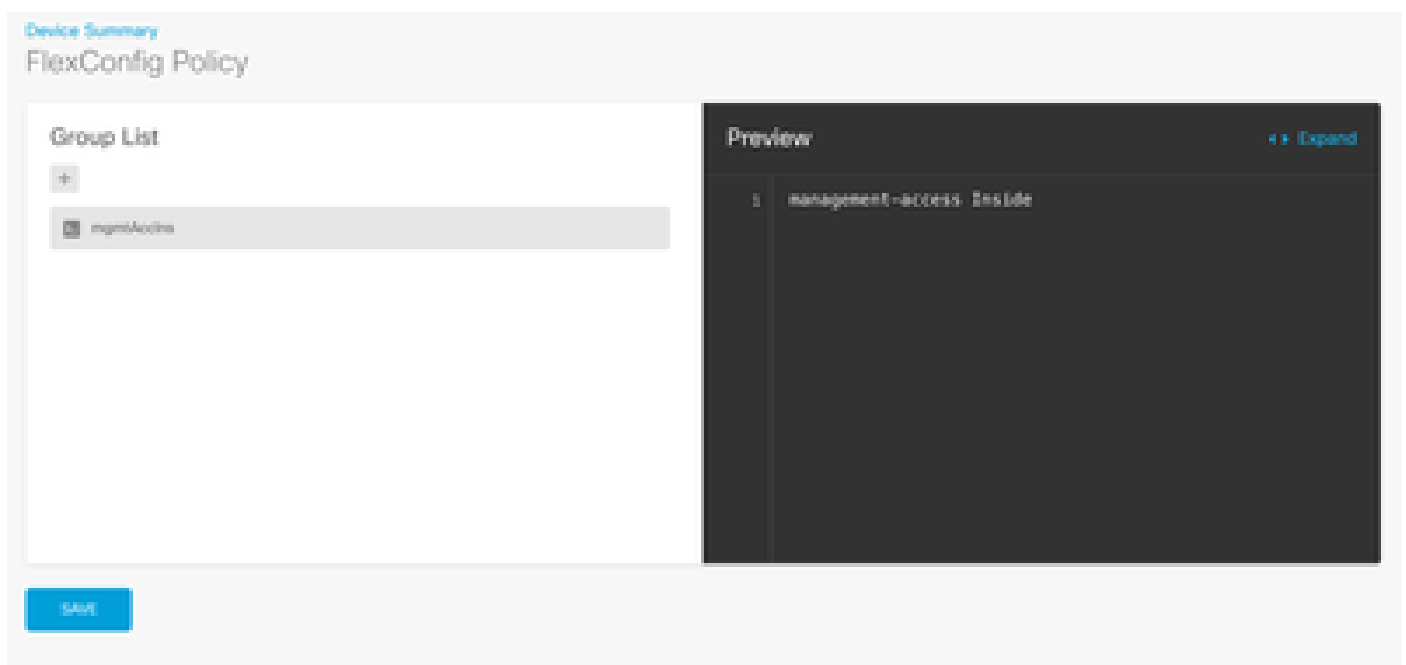
```
1 no management-access Inside
```

CANCEL OK

7. 在FlexConfig部分中，選擇FlexConfig策略，按一下「增加」圖示，然後選擇我們在上一步中建立的flexConfig對象，然後選擇「確定」。



8. 然後，預覽要應用於裝置的命令。選擇Save。



9. 部署組態，選取部署圖示，然後按一下立即部署。



Pending Changes



Last Deployment Completed Successfully
15-Oct-2024 08:06 PM. [See Deployment History](#)

Deployed Version (15-Oct-2024 08:06 PM)

Pending Version

LEGEND

FlexConfig Policy Edited: default-group

MORE ACTIONS ▾

CANCEL

DEPLOY NOW ▾

附註：請確定已順利完成，您可以檢查工作清單來確認它。

驗證

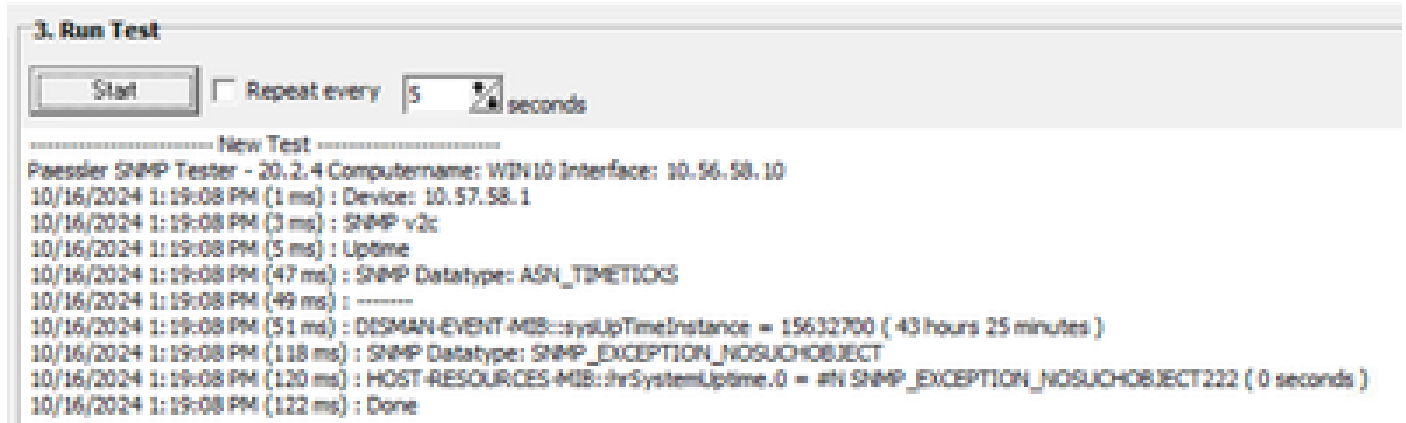
若要驗證組態，請執行這些檢查、透過SSH或主控台登入FTD，然後執行下列命令：

- 驗證裝置的運行配置是否包含我們所做的更改。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password:
firepower# show running-config
<some outputs are omitted>
object network snmpHost
host 10.56.58.10
<some outputs are omitted>
```

```
snmp-server host inside 10.56.58.10 community ***** version 2c
snmp-server location null
snmp-server contact null
snmp-server community *****
<some outputs are omitted>
management-access inside
```

- 從SNMP測試器執行測試，並確保測試成功完成。



疑難排解

如果您遇到任何問題，請考慮以下步驟：

- 確保VPN隧道已啟動並正在運行，您可以運行以下命令來驗證VPN隧道。

```
firepower# show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote fvrf/ivrf Status Role
```

```
442665449 10.197.225.82/500 10.197.225.81/500 READY RESPONDER
```

```
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

```
Life/Active Time: 86400/10 sec
```

```
Child sa: local selector 10.57.58.0/0 - 10.57.58.255/65535
```

```
remote selector 10.56.58.0/0 - 10.56.58.255/65535
```

```
ESP spi in/out: 0x3c8ba92b/0xf79c95a9
```

```
firepower# show crypto ikev2 stats
```

```
Global IKEv2 Statistics
```

```
Active Tunnels: 1
```

```
Previous Tunnels: 2
```

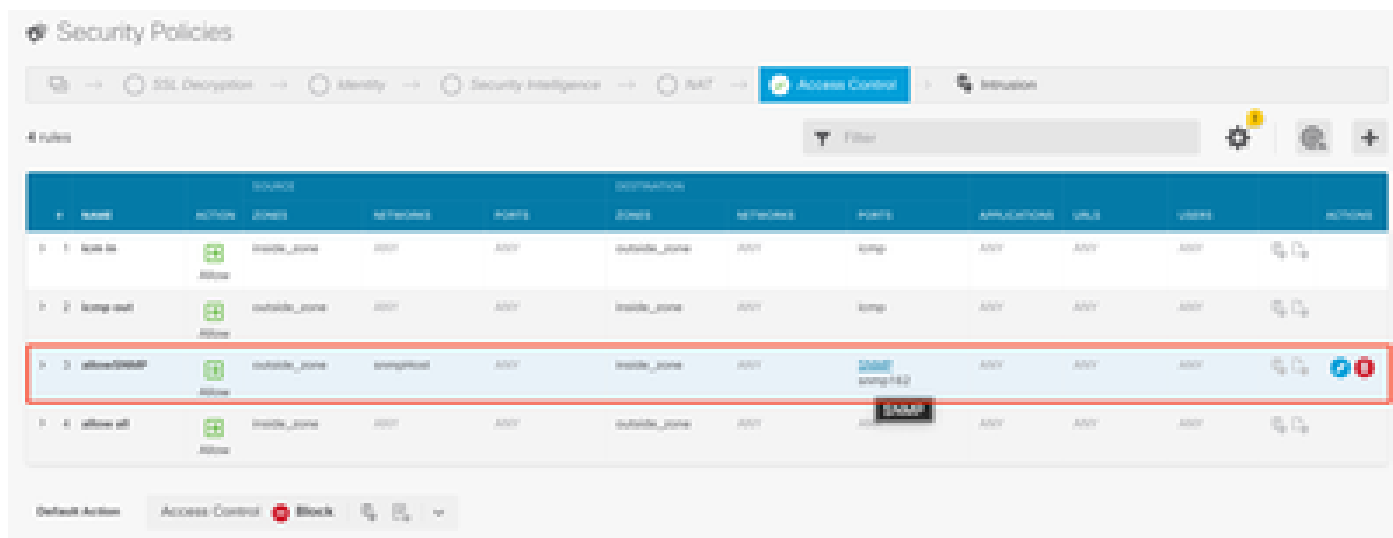
您可以在此處找到有關如何調試IKEv2隧道的詳細指南：[如何調試IKEv2 VPN](#)

- 驗證SNMP配置並確保兩端的社群字串和訪問控制設定正確。

```
firepower# sh run snmp-server
snmp-server host inside 10.56.58.10 community ***** version 2c
snmp-server location null
snmp-server contact null
snmp-server community *****
```

- 確定已允許SNMP流量透過FTD。

導航到Policies (策略) > Access Control (訪問控制) ，驗證您擁有允許SNMP流量的規則。



- 使用資料包捕獲來監控SNMP流量並辨識任何問題。

在防火牆上啟用含有追蹤軌跡的擷取：

```
capture snmp interface inside trace detail match udp any any eq snmp
```

```
firepower# show capture
capture snmp type raw-data trace detail interface inside include-decrypted [Capturing - 405 bytes]
match udp host 10.57.58.10 host 10.56.58.1 eq snmp
```

```
firepower# sh capture snmp
4 packets captured
```

```
1: 17:50:42.271806 10.56.58.10.49830 > 10.57.58.1.161: udp 43
2: 17:50:42.276551 10.56.58.10.49831 > 10.57.58.1.161: udp 43
3: 17:50:42.336118 10.56.58.10.49832 > 10.57.58.1.161: udp 44
4: 17:50:42.338803 10.56.58.10.49833 > 10.57.58.1.161: udp 43
4 packets shown
```

有關其他詳細資訊，請檢視《SNMP配置指南》[對Firepower FDM上的SNMP進行配置和故障排](#)

[除](#)

相關資訊

- [Cisco Secure Firepower 裝置管理器配置指南](#)
- [Cisco ASA 配置指南](#)
- [思科裝置上的SNMP配置](#)

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）。