

在FDM管理的数据接口上配置站点到站点VPN上的SNMP

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何在FTD设备数据接口的数据接口上配置通过站点到站点VPN到远程端的SNMP。

先决条件

在继续进行配置之前，请确保满足以下前提条件：

- 基本了解以下主题：
 - 由Firepower设备管理器(FDM)管理的Cisco Firepower威胁防御(FTD)。
 - 思科自适应安全设备(ASA)。
 - 简单网络管理协议(SNMP)。
 - 虚拟专用网络(VPN)。
- 对FTD和ASA设备的管理访问权限。
- 确保您的网络处于活动状态，并且您了解所有命令的潜在影响。

要求

- 由FDM版本7.2.7管理的思科FTD
- Cisco ASA版本9.16
- SNMP服务器详细信息（包括IP地址、社区字符串）
- 站点到站点VPN配置详细信息（包括对等体IP、预共享密钥）
- FTD必须至少为6.7版，才能使用REST API配置SNMP。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 由Firepower设备管理器(FDM) 7.2.7版管理的Cisco Firepower威胁防御(FTD)。
- Cisco 自适应安全设备 (ASA) 版本 9.16.
- SNMP服务器 (任何标准SNMP服务器软件)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

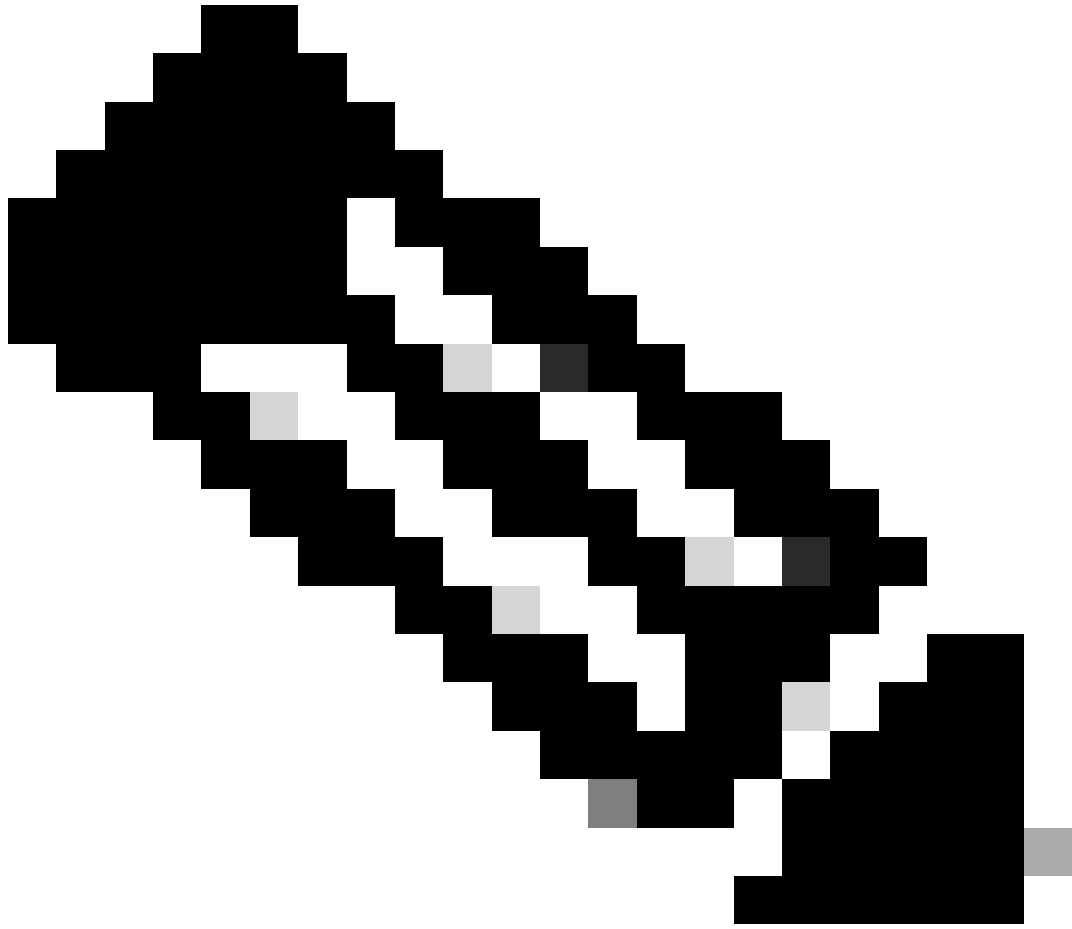
背景信息

网络管理员可以按照这些步骤确保远程监控网络设备。

SNMP (简单网络管理协议) 用于网络管理和监控。在此设置中，SNMP流量通过与ASA建立的站点到站点VPN从FTD发送到远程SNMP服务器。

本指南旨在帮助网络管理员在FTD设备的数据接口上通过站点到站点VPN为远程终端配置SNMP。此设置对于远程监控和管理网络设备十分有用。在此设置中，使用SNMP v2，并且SNMP流量通过与ASA建立的站点到站点VPN从FTD数据接口发送到远程SNMP服务器。

使用的接口称为“内部”，但是此配置可以应用于其他类型的“到机箱”流量，并且可以使用防火墙中任何非VPN终止的接口。



注意：当FTD运行版本6.7及更高版本并由FDM管理时，只能通过REST API配置SNMP。

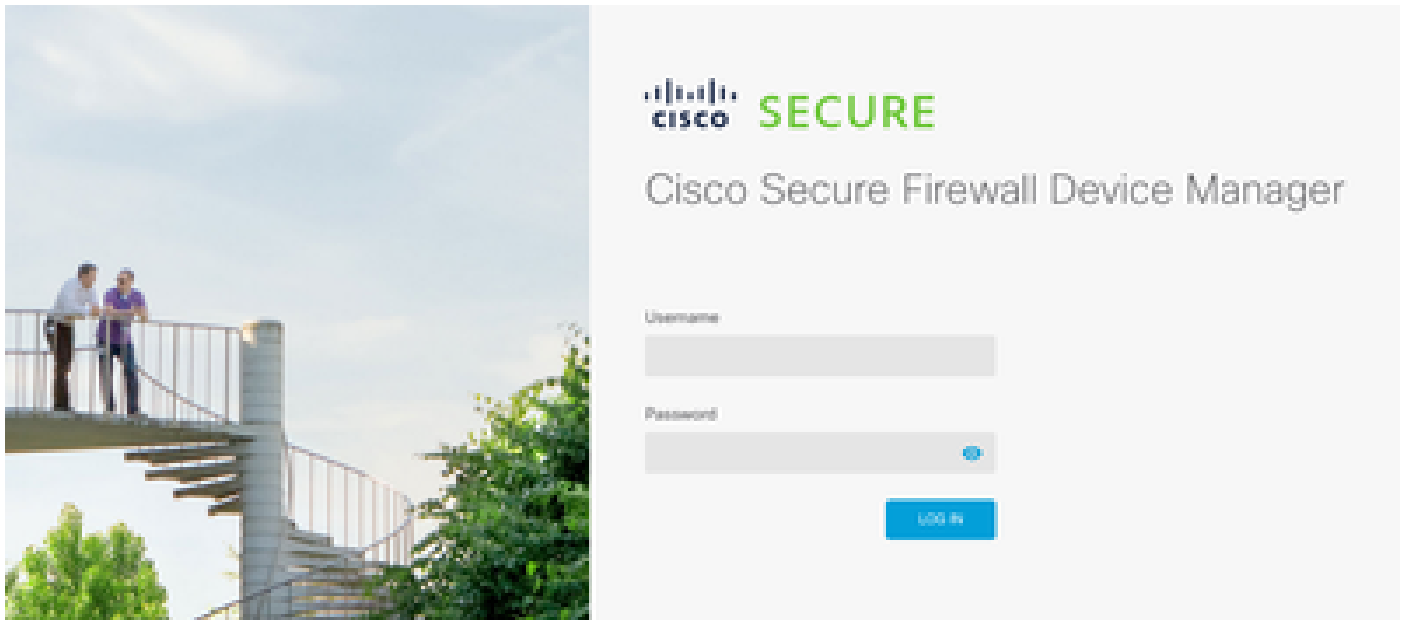
配置



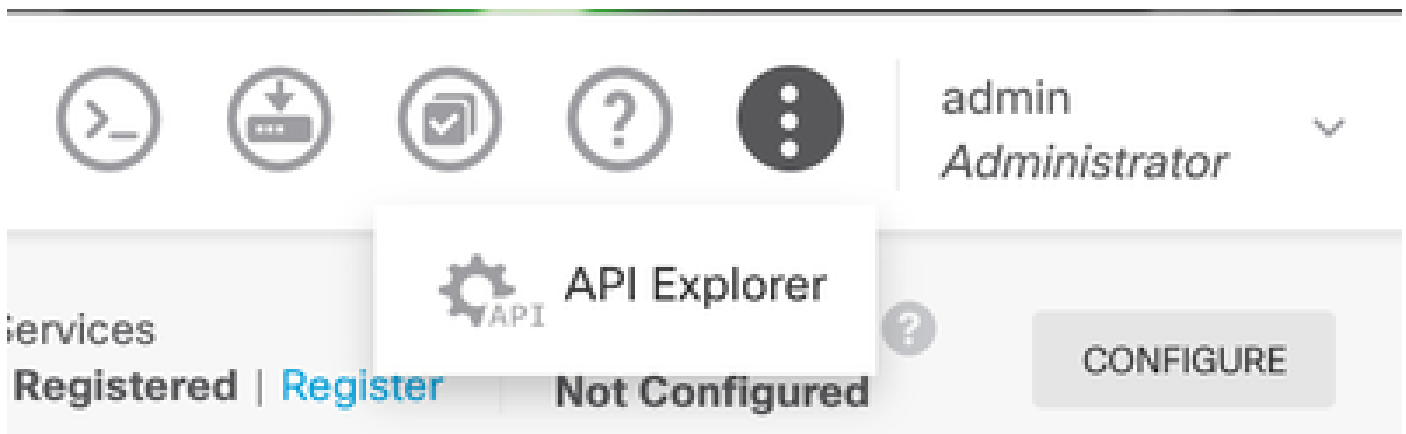
注意：此配置认为已在设备之间配置站点到站点VPN。有关如何配置站点到站点VPN的其他详细信息，请查看配置指南。[在FDM管理的FTD上配置站点到站点VPN](#)

配置

1. 登录到FTD。



2. 在设备概述下，导航至API资源管理器。



3. 在FTD上配置SNMPv2

- 获取接口信息。



4. 向下滚动并选择Try it out按钮进行API调用。成功的调用返回响应代码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

- 为SNMP主机创建网络对象配置。

NetworkObject

GET

/object/networks

POST

/object/networks

- 创建新的SNMPv2c主机对象。

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}

有关其他详细信息，请查阅配置指南，[在Firepower FDM上配置并排除SNMP故障](#)

5. 在设备上配置SNMP之后，导航到高级配置部分中的设备，然后选择查看配置。

Advanced Configuration

Includes: FlexConfig, Smart CLI

[View Configuration](#)



6. 在FlexConfig部分中，选择FlexConfig objects，然后创建新对象，命名并在模板部分中添加management-access命令，指定接口，然后在模板否定部分中添加命令否定形式。

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

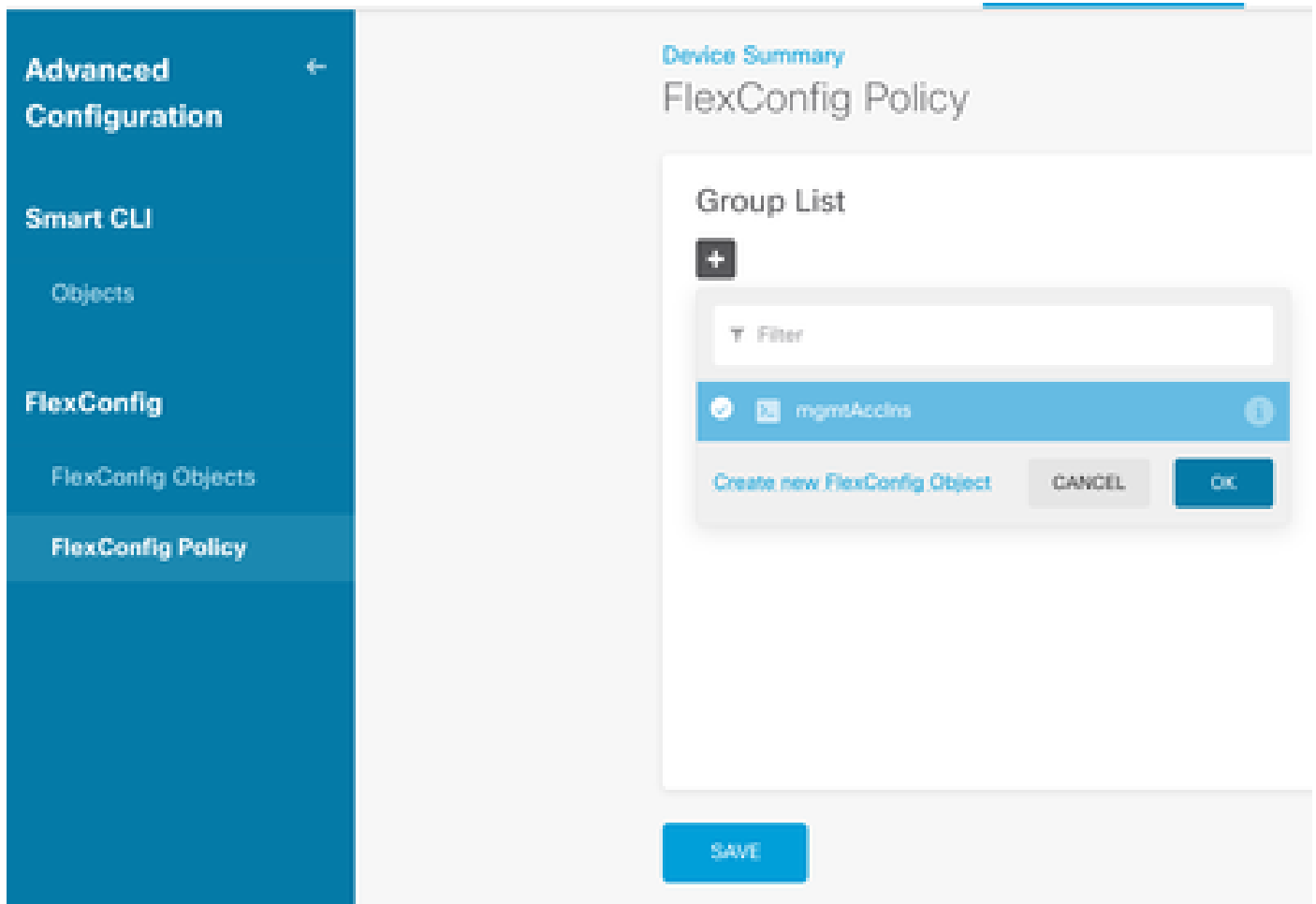
```
1 management-access Inside
```

Negate Template  Expand Reset

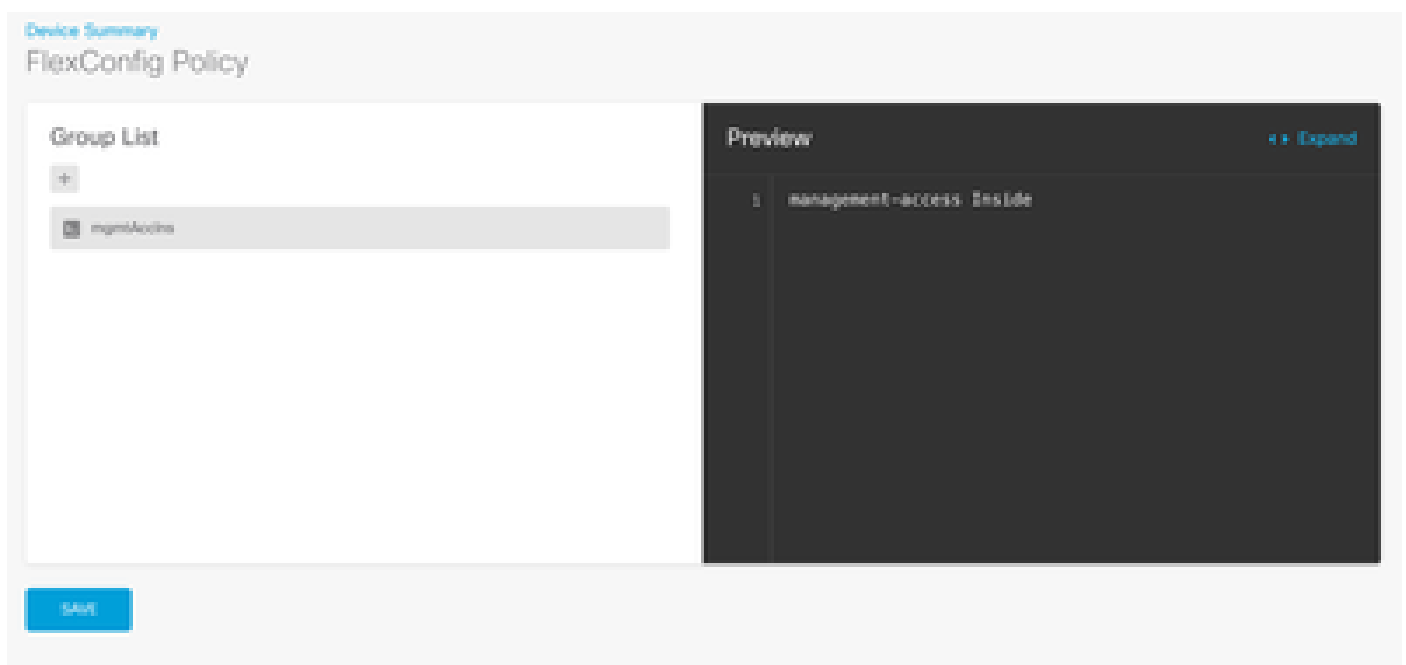
```
1 no management-access Inside
```

CANCEL OK

7. 在FlexConfig部分中，选择FlexConfig策略，单击添加图标并选择我们在上一步中创建的flexConfig对象，然后选择“确定”。



8. 然后，系统将显示要应用于设备的命令的预览。选择Save。



9. 部署配置，选择“部署”图标，然后单击“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 ▾

注意：确保任务列表已圆满完成，您可以检查任务列表进行确认。

验证

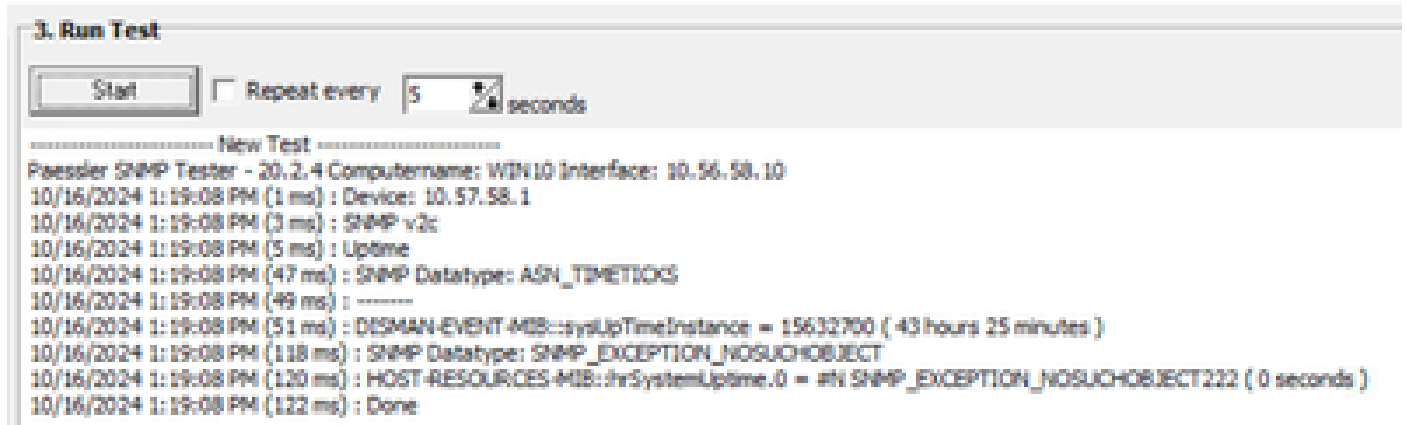
要验证配置，请执行以下检查，通过SSH或控制台登录到FTD，然后运行以下命令：

- 确认设备的运行配置包含我们所做的更改。

```
> 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
```

- 从SNMP测试仪执行测试并确保其成功完成。



故障排除

如果遇到任何问题，请考虑以下步骤：

- 确保VPN隧道已启动并正在运行，您可以运行这些命令以验证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
```

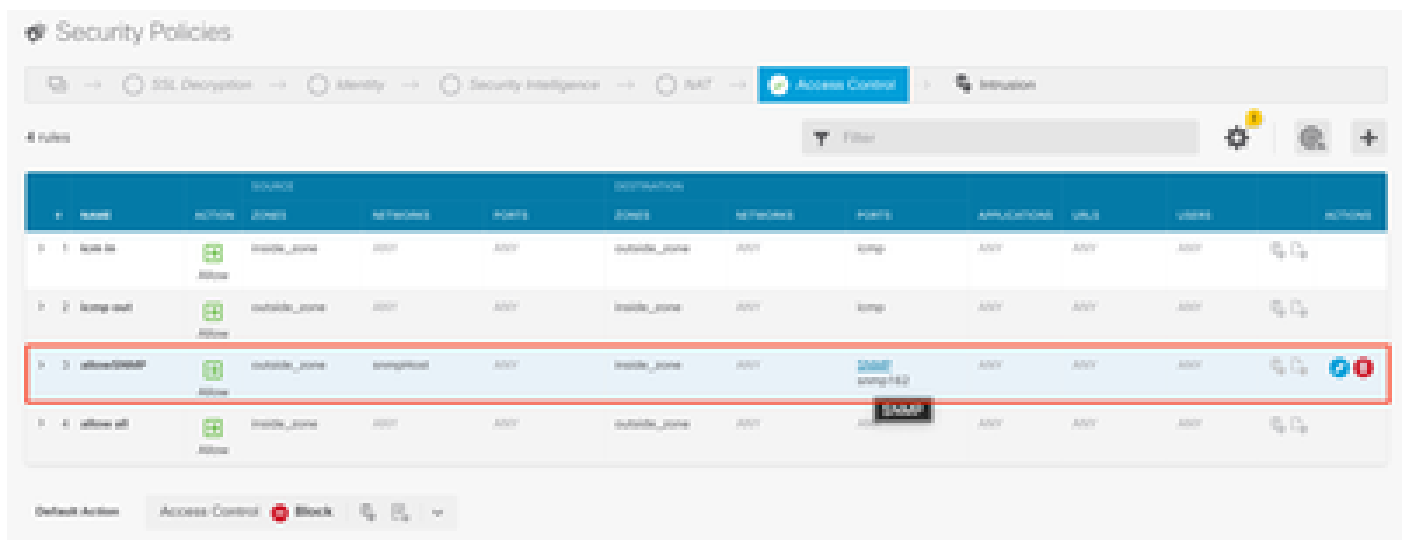
有关如何调试IKEv2隧道的详细指南可在此处找到：[如何调试IKEv2 VPN](#)

- 验证SNMP配置并确保两端的社区字符串和访问控制设置正确。

```
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 *****
```

- 确保允许SNMP流量通过FTD。

导航到Policies (策略) > Access Control (访问控制) ，验证您是否有允许SNMP流量的规则。



- 使用数据包捕获来监控SNMP流量并确定任何问题。

在防火墙上启用带跟踪的捕获：

```
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
```

有关其他详细信息，请查看《SNMP配置指南》，[在Firepower FDM上配置并排除SNMP故障](#)

相关信息

- [思科安全Firepower设备管理器配置指南](#)
- [Cisco ASA配置指南](#)
- [思科设备上的SNMP配置](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。