

# 在Firepower NGFW设备上配置SNMP

## 目录

---

### [简介](#)

### [先决条件](#)

[要求](#)

[使用的组件](#)

### [背景信息](#)

### [配置](#)

[在 FPR4100/FPR9300 上配置机箱 \(FXOS\) SNMP](#)

[通过 GUI 配置 FXOS SNMPv1/v2c](#)

[通过命令行界面 \(CLI\) 配置 FXOS SNMPv1/v2c](#)

[通过 GUI 配置 FXOS SNMPv3](#)

[通过 CLI 配置 FXOS SNMPv3](#)

[在 FPR4100/FPR9300 上配置 FTD \(LINA\) SNMP](#)

[配置 LINA SNMPv2c](#)

[配置 LINA SNMPv3](#)

[MIO刀片SNMP统一\(FXOS 2.12.1、FTD 7.2、ASA 9.18.1\)](#)

[在 FPR2100 上配置 SNMP](#)

[在 FPR2100 上配置机箱 \(FXOS\) SNMP](#)

[配置 FXOS SNMPv1/v2c](#)

[配置 FXOS SNMPv3](#)

[在 FPR2100 上配置 FTD \(LINA\) SNMP](#)

### [验证](#)

[验证 FPR4100/FPR9300 的 FXOS SNMP](#)

[FXOS SNMPv2c 验证](#)

[FXOS SNMPv3 验证](#)

[验证 FPR2100 的 FXOS SNMP](#)

[FXOS SNMPv2 验证](#)

[FXOS SNMPv3 验证](#)

[验证 FTD SNMP](#)

[允许 SNMP 流量进入 FPR4100/FPR9300 的 FXOS](#)

[通过 GUI 配置全局访问列表](#)

[通过 CLI 配置全局访问列表](#)

[确认](#)

[使用 OID Object Navigator](#)

### [故障排除](#)

[无法轮询 FTD LINA SNMP](#)

[无法轮询 FXOS SNMP](#)

[需要使用哪些 SNMP OID 值？](#)

[无法获取 SNMP 陷阱](#)

[无法通过 SNMP 监控 FMC](#)

[Firepower Device Manager \(FDM\) 上的 SNMP 配置](#)

[SNMP 故障排除速查表](#)

---

## 简介

本文档介绍如何在下一代防火墙(NGFW) FTD设备上配置简单网络管理协议(SNMP)并对其进行故障排除。

## 先决条件

### 要求

阅读本文档之前，需要对 SNMP 协议有基本的了解。

### 使用的组件

本文档不限于特定的软件和硬件版本。

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

Firepower NGFW 设备可分为两大子系统：

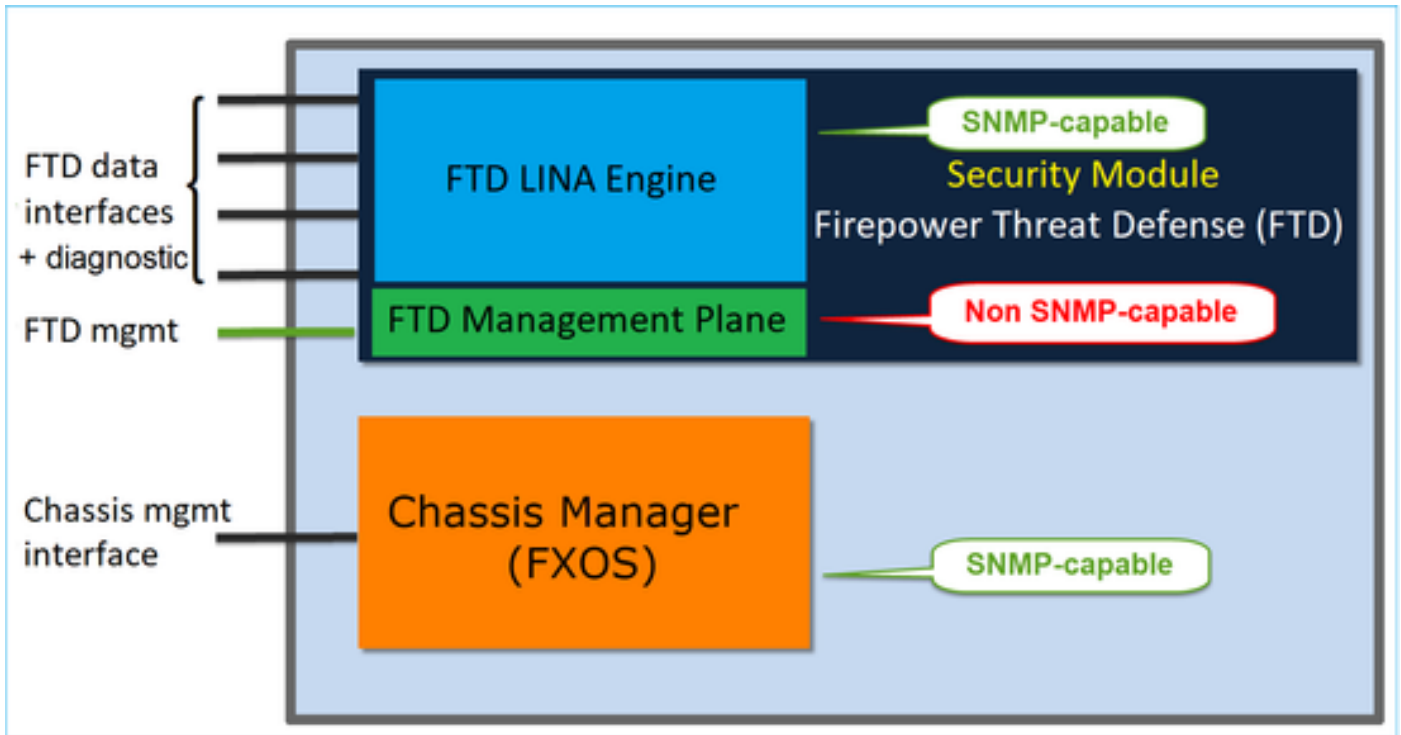
- 负责控制机箱硬件的 Firepower 可扩展操作系统 (FX-OS)；
- 在模块内运行的 Firepower Threat Defense (FTD)。

FTD是一个统一的软件，由2个主引擎（Snort引擎和LINA引擎）组成。FTD的当前SNMP引擎源于传统ASA，并且它可查看LINA相关功能。

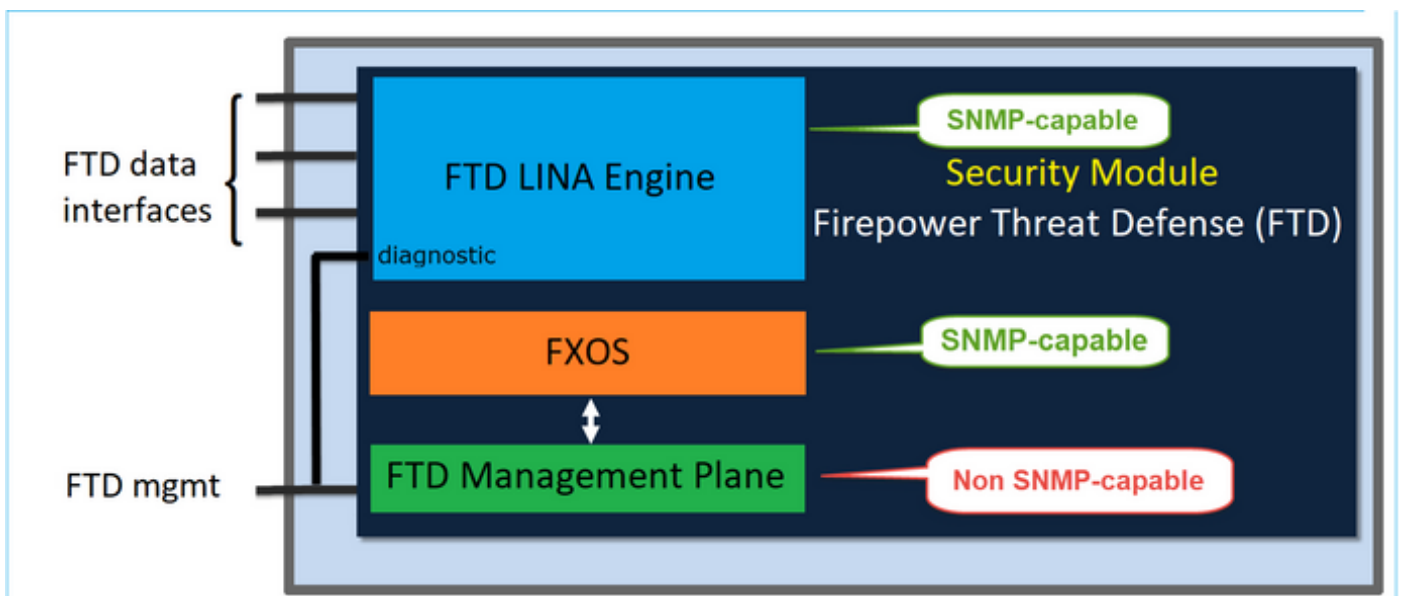
FX-OS和FTD具有独立的控制平面，并且出于监控目的，它们具有不同的SNMP引擎。每个SNMP引擎提供不同的信息，可能希望同时监控这两者，以获得更全面的设备状态视图。

从硬件角度看，Firepower NGFW设备目前有两个主要架构：Firepower 2100系列和Firepower 4100/9300系列。

Firepower 4100/9300 设备具有专用的设备管理接口，这是发往 FXOS 子系统的 SNMP 流量的源和目的。另一方面，FTD 应用使用 LINA 接口（数据和/或诊断接口。在 FTD 6.6 及更高版本中，也可使用 FTD 管理接口）进行 SNMP 配置。



Firepower 2100 设备上的 SNMP 引擎使用 FTD 管理接口和 IP。设备本身可桥接此接口上接收的 SNMP 流量，并将其转发到 FXOS 软件。

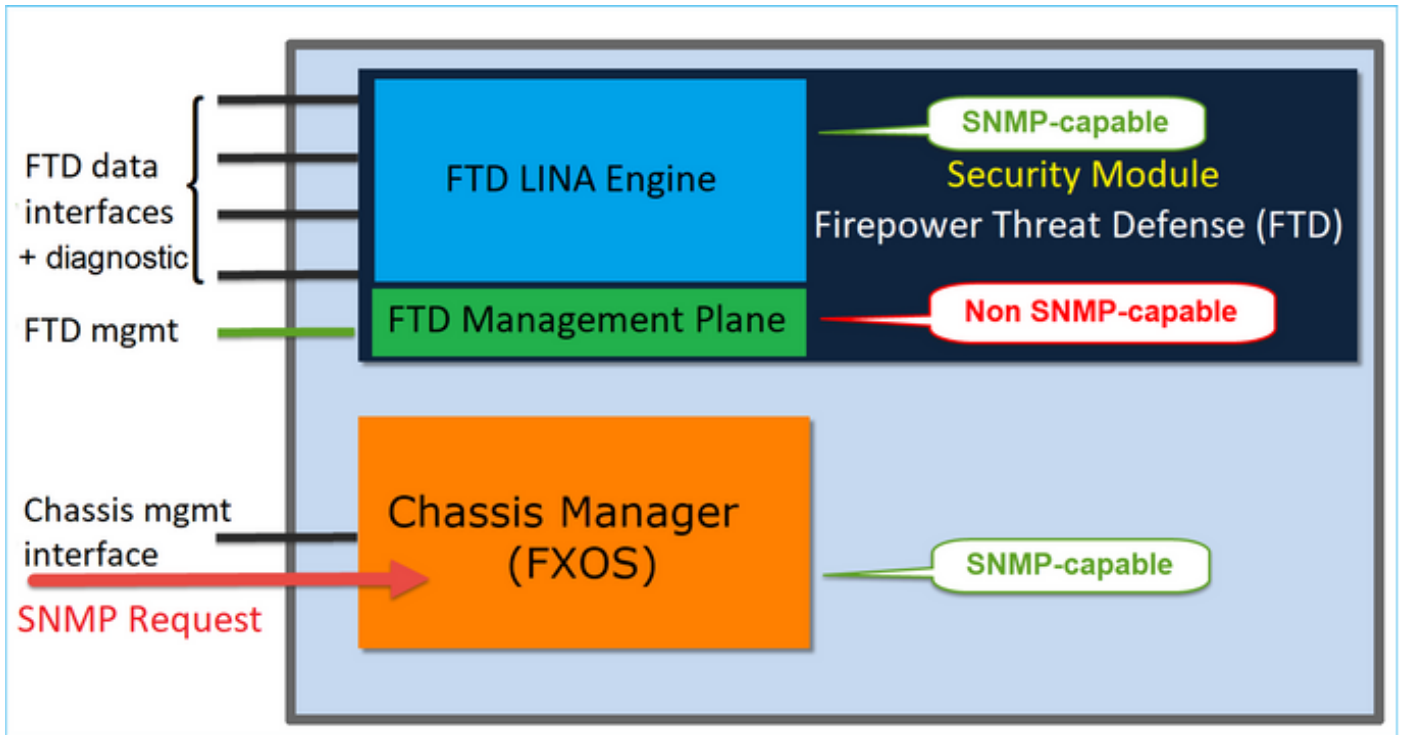


我们对使用 6.6 及更高软件版本的 FTD 进行了如下更改：

- 通过管理接口使用 SNMP。
- 在 FPR1000 或 FPR2100 系列平台上，通过此单个管理接口统一 LINA SNMP 和 FXOS SNMP。此外，在 FMC 的平台设置 > SNMP 下提供单个配置点。

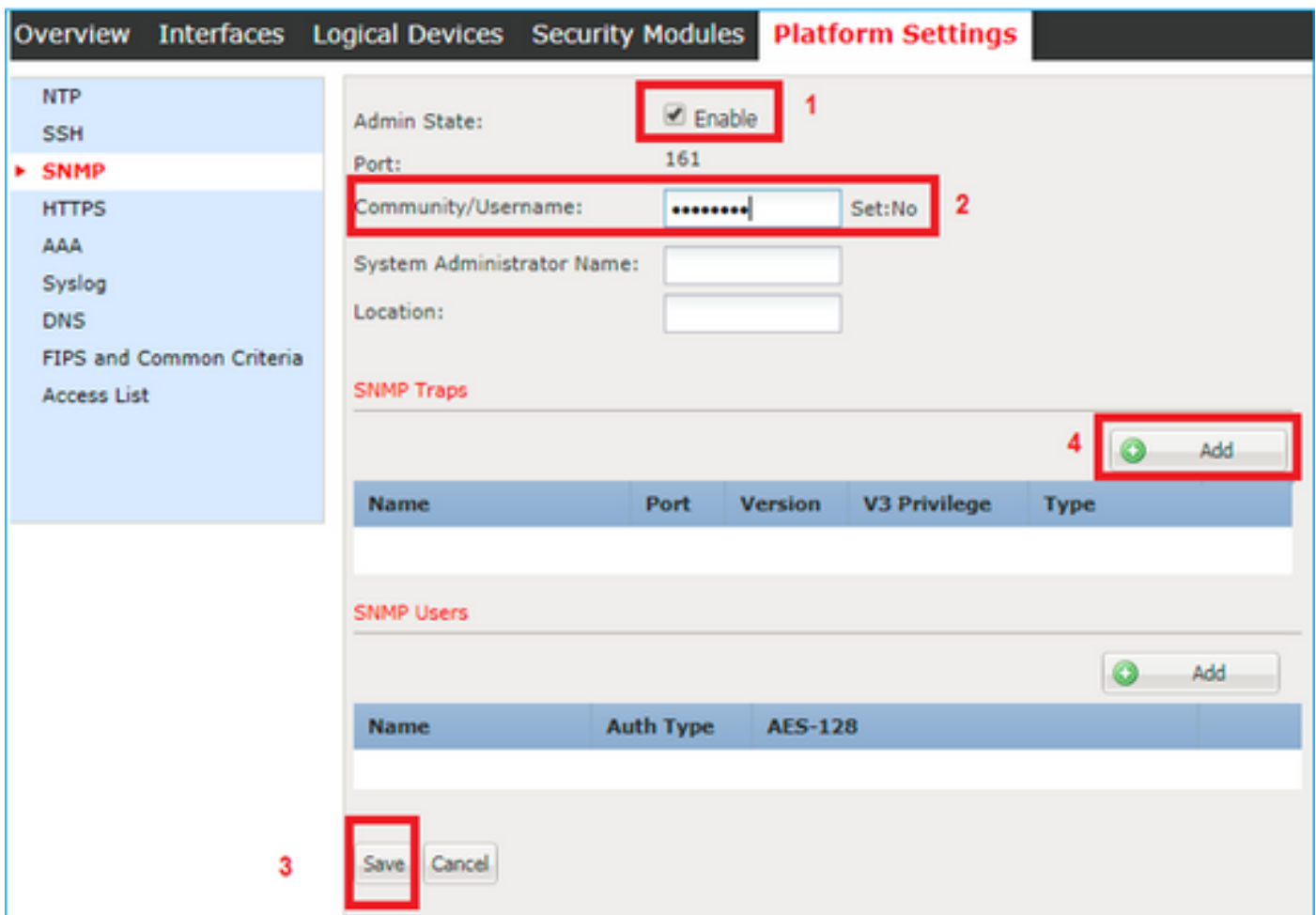
## 配置


在 FPR4100/FPR9300 上配置机箱 (FXOS) SNMP



通过 GUI 配置 FXOS SNMPv1/v2c

步骤1:打开Firepower机箱管理器(FCM) UI，导航至平台设置> SNMP选项卡。选中 SNMP“启用”复选框，指定要在 SNMP 请求中使用的社区字符串，然后点击保存。



 注：如果已设置“社区/用户名”字段，则空字段右侧的文本为“设置：是”。如果 Community/Username 字段尚未填充值，则空字段右侧的文本写着 Set：No

第二步：配置SNMP陷阱目标服务器。

## Add SNMP Trap ? X

Host Name:\*


Community/Username:\*

Port:\*

Version:  V1  V2  V3

Type:  Traps  Informs

V3 Privilege:  Auth  NoAuth  Priv

 注意：查询和陷阱主机的社区值是独立的，可以不同

主机可以按 IP 地址或名称进行定义。选择确定，系统会自动保存 SNMP 陷阱服务器的配置，无需在 SNMP 主页中选择“保存”按钮。删除主机时亦是如此。

通过命令行界面 (CLI) 配置 FXOS SNMPv1/v2c

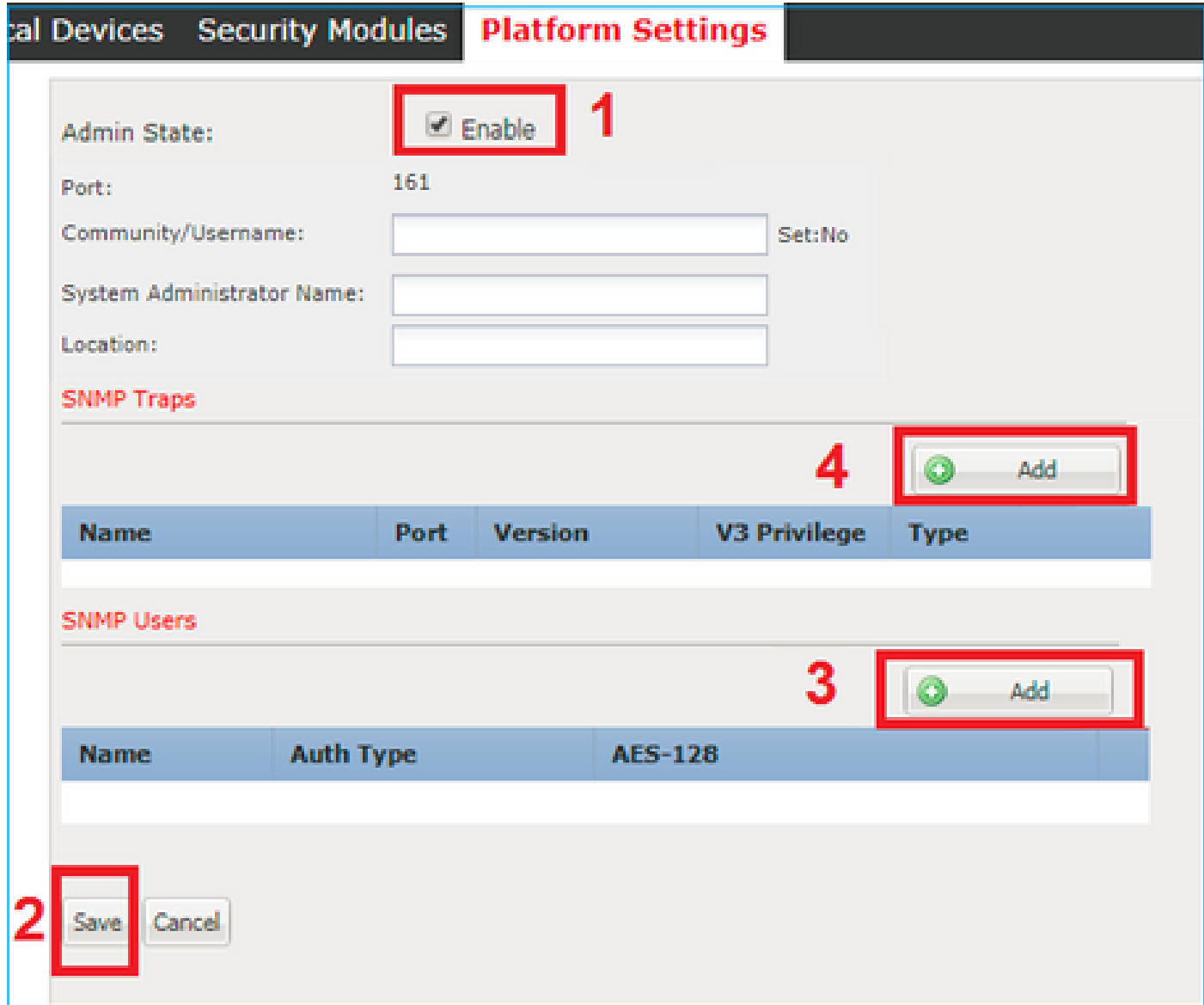
```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
```

```
enable snmp
ksec-fpr9k-1-A /monitoring* #
set snmp community
Enter a snmp community:
ksec-fpr9k-1-A /monitoring* #
  enter snmp-trap 192.168.10.100
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v2c
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype traps
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set port 162
ksec-fpr9k-1-A /monitoring/snmp-trap* #
exit
ksec-fpr9k-1-A /monitoring* #
  commit-buffer
```

## 通过 GUI 配置 FXOS SNMPv3

步骤1:打开FCM并导航到Platform Settings > SNMP选项卡。

第二步：对于SNMP v3，无需在上部设置任何社区字符串。所创建的每位用户均能在 FXOS SNMP 引擎上成功运行查询。第一步就是在平台中启用 SNMP。完成后，即可创建用户和目的陷阱主机。SNMP 用户和 SNMP 陷阱主机均会自动保存。



第三步：如图所示，添加SNMP用户。身份验证类型始终为 SHA，但可以使用 AES 或 DES 进行加密：

**Add SNMP User** ? X

Name:\*

Auth Type: SHA

Use AES-128:

Password:

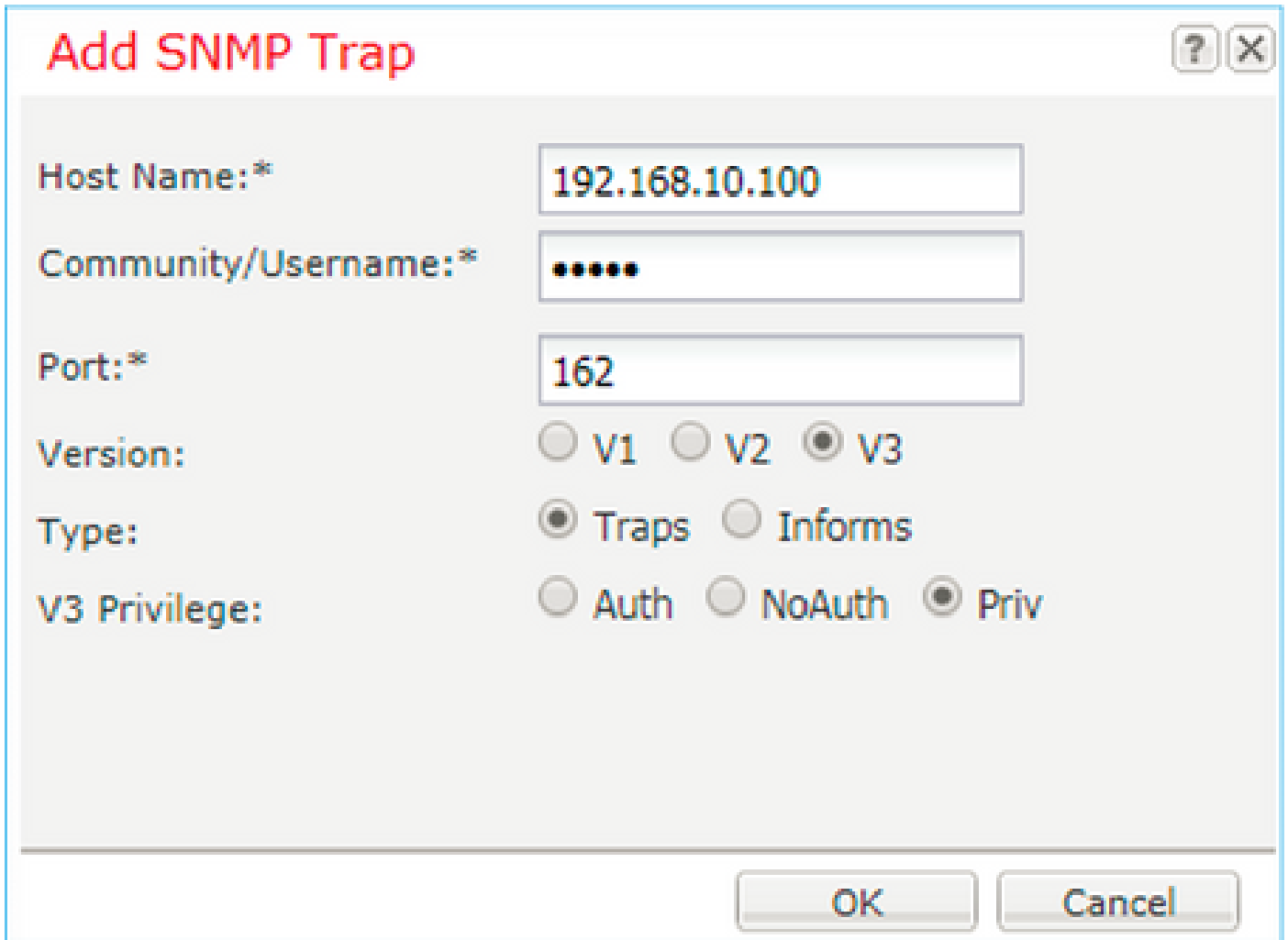
Confirm Password:

Privacy Password:

Confirm Privacy Password:

第四步：添加SNMP陷阱主机，如图所示：





The image shows a 'Add SNMP Trap' dialog box with the following fields and options:

- Host Name: \* 192.168.10.100
- Community/Username: \* ●●●●●
- Port: \* 162
- Version:  V1  V2  V3
- Type:  Traps  Informs
- V3 Privilege:  Auth  NoAuth  Priv

Buttons: OK, Cancel

### 通过 CLI 配置 FXOS SNMPv3

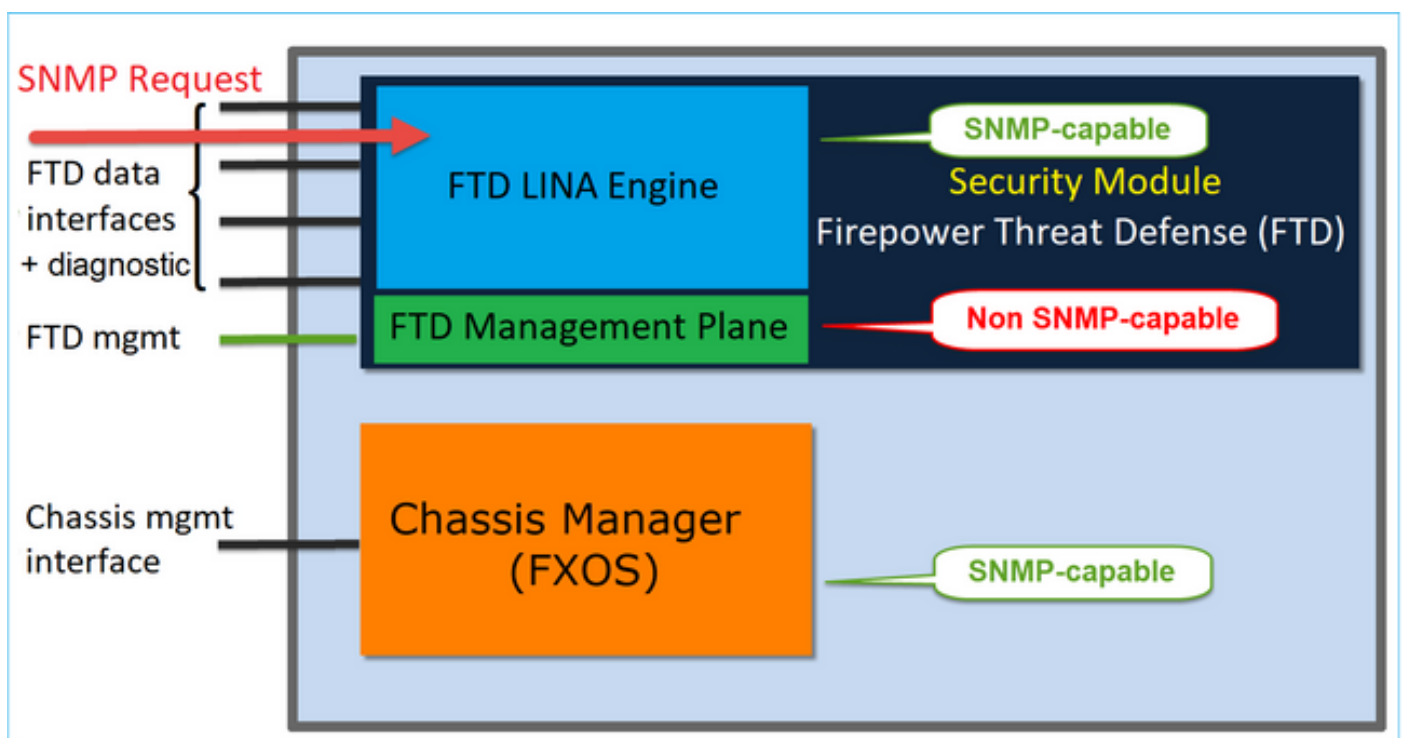
```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring #
create snmp-user user1
Password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set auth sha
ksec-fpr9k-1-A /monitoring/snmp-user* #
set priv-password
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
```

```

set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter snmp-trap 10.48.26.190
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v3
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype traps
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set port 162
ksec-fpr9k-1-A /monitoring/snmp-trap* #
exit
ksec-fpr9k-1-A /monitoring* #
commit-buffer

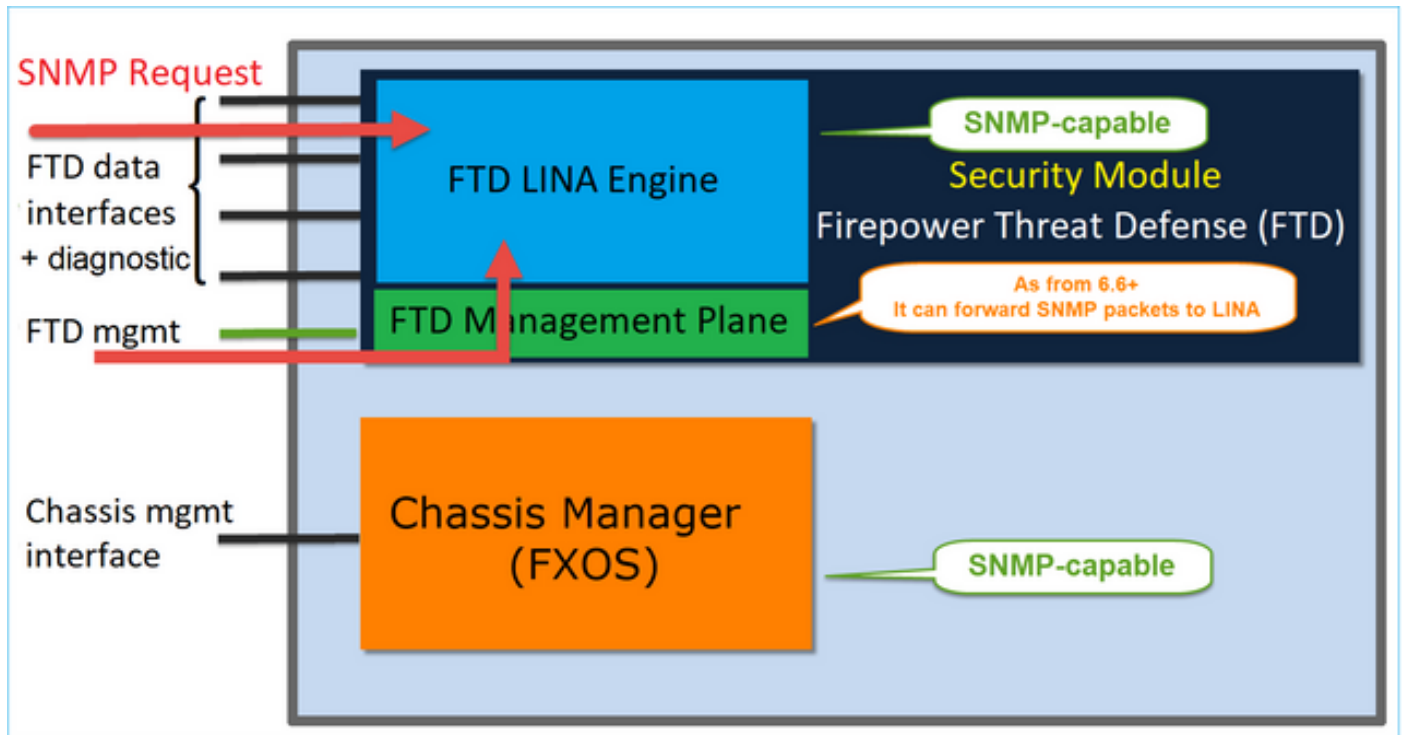
```

## 在 FPR4100/FPR9300 上配置 FTD (LINA) SNMP



## 6.6 及更高版本中的变化

- 在 6.6 及更高版本中，还可以选择将 FTD 管理接口用于轮询和陷阱。



从 6.6 版本开始，所有 FTD 平台均支持 SNMP 单一 IP 管理功能：

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- 运行 FTD 的 ASA5500
- FTDv

### 配置 LINA SNMPv2c

步骤1:在FMC UI上，导航到设备>平台设置> SNMP。选中Enable SNMP Servers 选项并配置 SNMPv2设置，如下所示：

第二步：在主机选项卡上，选择添加按钮并指定SNMP服务器设置：

### Edit SNMP Management Hosts

IP Address\*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port  (1 - 65535)

**Available Zones**

- INSIDE\_FTD4110
- OUTSIDE1\_FTD4110
- OUTSIDE2\_FTD4110
- NET1\_4100-3
- NET2\_4100-3
- NET3\_4100-3

**Selected Zones/Interfaces**

- OUTSIDE3

您还可以指定诊断接口作为 SNMP 消息的源。诊断接口是一种数据接口，仅允许发往设备和发自设备的流量（仅限管理流量）。

## Add SNMP Management Hosts



IP Address\*

SNMP-SERVER



SNMP Version

2c

Username



Community String

Confirm

Poll

Trap

Trap Port

162

(1 - 65535)

Reachable By:

Device Management Interface *(Applicable from v6.6.0 and above)*

Security Zones or Named Interface

Available Zones



Search

2100\_inside  
2100\_outside  
cluster\_dmz  
cluster\_inside  
cluster\_outside

Add

Selected Zones/Interfaces

diagnostic



Interface Name

Add

Cancel

OK

此图来自 6.6 版本，使用浅色主题。

此外，在 FTD 6.6 及更高版本中，还可以选择管理接口：

## Add SNMP Management Hosts

IP Address\*

SNMP-SERVER



SNMP Version

2c

Username

Community String

Confirm

Poll

Trap

Trap Port

162

(1 - 65535)

Reachable By:

Device Management Interface *(Applicable from v6.6.0 and above)*

Security Zones or Named Interface

Available Zones



Search

Add

2100\_inside  
2100\_outside  
cluster\_dmz  
cluster\_inside  
cluster\_outside

Selected Zones/Interfaces

diagnostic



Interface Name

Add

Cancel

OK

如果选择全新管理接口，则可通过管理接口使用 LINA SNMP。

结果：

Interface	Network	SNMP Version	Poll/Trap	Port	Username
OUTSIDE3	SNMP-SERVER	2c	Poll		

### 配置 LINA SNMPv3

步骤1:在FMC UI上，导航到设备>平台设置> SNMP。选中选项Enable SNMP Servers 并配置 SNMPv3 User and Host：

**Add Username**

Security Level: Priv

Username\*: cisco

Encryption Password Type: Clear Text

Auth Algorithm Type: SHA

Authentication Password\*: .....

Confirm\*: .....

Encryption Type: AES128

Encryption Password\*: .....

Confirm\*: .....

OK Cancel



Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS **Platform Settings** FlexConfig Certificates

### mzafeiro\_FTD4110-HA

Enter Description

- ARP Inspection
- Banner
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- SNMP**
- SSL
- Syslog
- Timeouts
- Time Synchronization
- UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Port  (1 - 65535)

**Hosts** Users SNMP Traps

Interface	Network	SNMP Version	Poll/Trap	Port	Username
OUTSIDE3	SNMP-SERVER	3	Poll		cisco

第二步：将主机也配置为接收陷阱：

### Edit SNMP Management Hosts

IP Address\*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port  (1 - 65535)

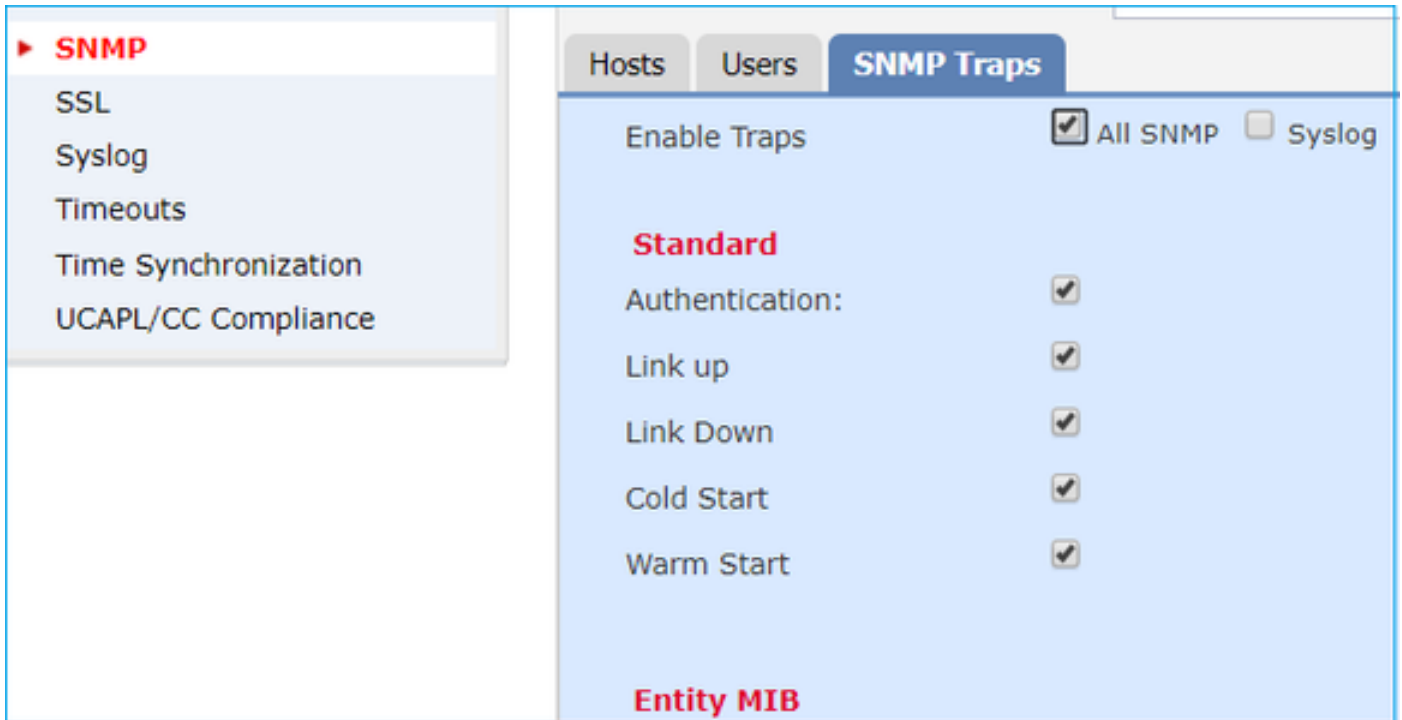
**Available Zones**

- INSIDE\_FTD4110

**Selected Zones/Interfaces**

- OUTSIDE3

第三步：可以在SNMP陷阱部分下选择要接收的陷阱：



## MIO刀片SNMP统一(FXOS 2.12.1、FTD 7.2、ASA 9.18.1)

### 7.2之前版本的行为

- 在9300和4100平台上，在FTD/ASA应用上配置的SNMP上不提供机箱信息的SNMP MIB。需要在MIO上通过机箱管理器单独配置并单独访问。MIO是管理和I/O (Supervisor)模块。
- 需要配置两个单独的SNMP策略，一个在刀片/应用上，另一个在MIO上，以进行SNMP监控。
- 使用单独的端口，一个用于刀片，一个用于MIO，用于同一设备的SNMP监控。
- 当您尝试通过SNMP配置和监控9300和4100设备时，可能会造成复杂性。

### 它在新版本 ( FXOS 2.12.1、FTD 7.2、ASA 9.18.1及更高版本 ) 上的工作原理

- 借助MIO刀片SNMP统一，用户可以通过应用(ASA/FTD)接口轮询LINA和MIO MIB。
- 可以通过新的MIO CLI和FCM ( 机箱管理器 ) 用户界面启用或禁用此功能。
- 默认状态为disabled。这意味着MIO SNMP代理作为独立实例运行。需要使用MIO接口轮询机箱/DME MIB。启用此功能后，应用程序接口可用于轮询相同的MIB。
- 该配置位于机箱管理器UI的Platform-settings > SNMP > Admin Instance下，用户可以在其中指定FTD实例，以便整理/收集机箱MIB并将其提供给NMS
- 支持ASA/FTD本地和MI应用。
- 此功能仅适用于基于MIO的平台 ( FPR9300和FPR4100 )。

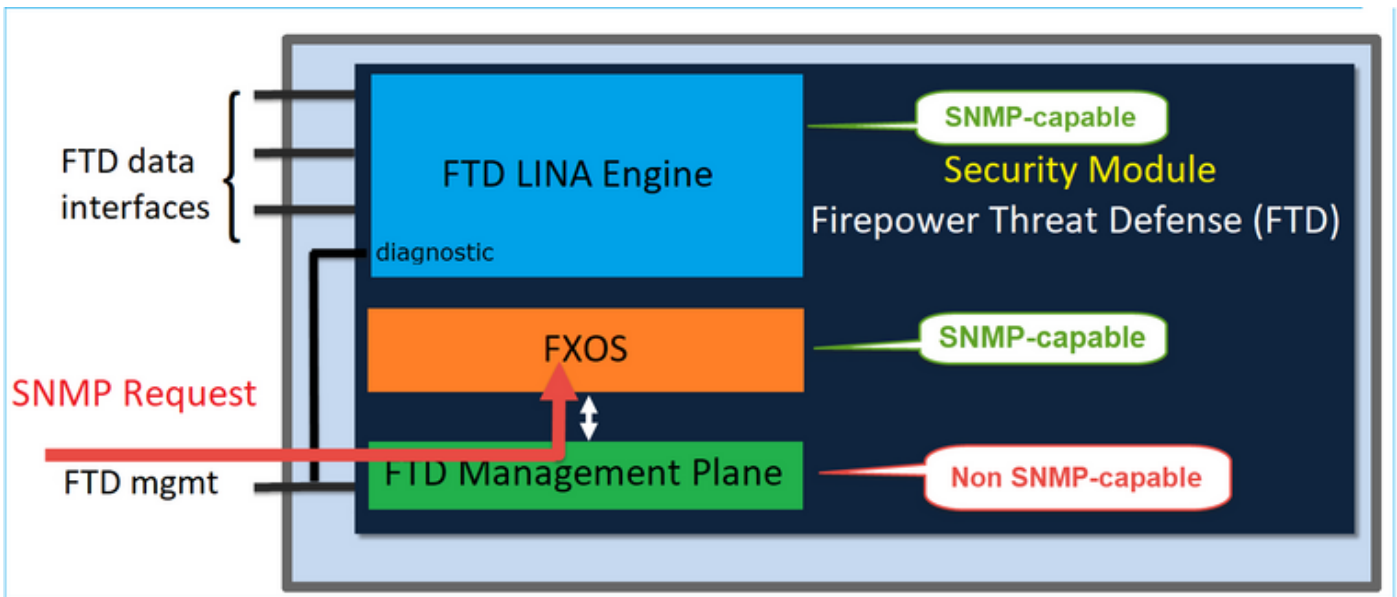
### 必备条件，支持的平台

- 支持的最低管理器版本：FCM 2.12.1
- 受管设备：FPR9300 / FP4100系列
- 所需的最低支持受管设备版本：FXOS 2.12.1、FTD 7.2或ASA 9.18.1

## 在 FPR2100 上配置 SNMP

FPR2100 系统中没有 FCM。只能通过 FMC 配置 SNMP。

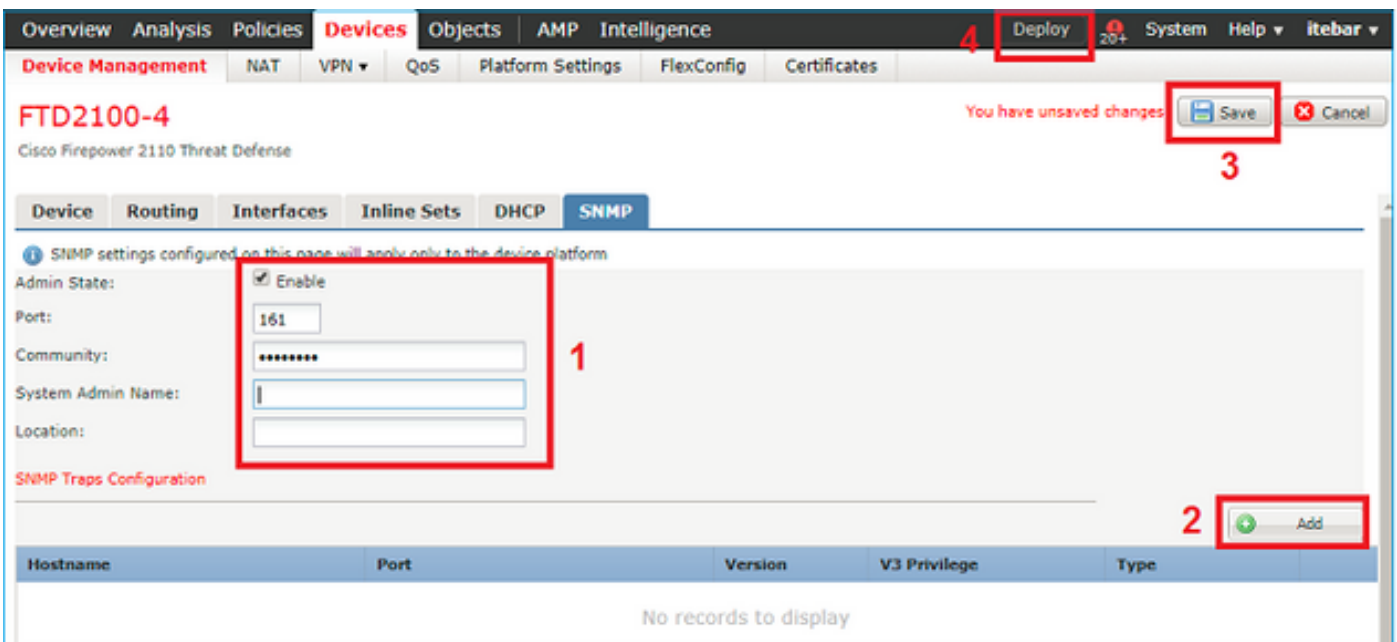
## 在 FPR2100 上配置机箱 (FXOS) SNMP




在 FTD 6.6 及更高版本中，还可以选择将 FTD 管理接口用于 SNMP。在这种情况下，FXOS 和 LINA SNMP 信息均通过 FTD 管理接口传输。

## 配置 FXOS SNMPv1/v2c

打开 FMC UI 并导航至设备 > 设备管理。选择设备并选择 SNMP：



### SNMP Trap Configuration

Hostname:\* 10.48.26.190 

Community String:\* .....

Port:\* 162 (1 - 65535)

SNMP Version: V2

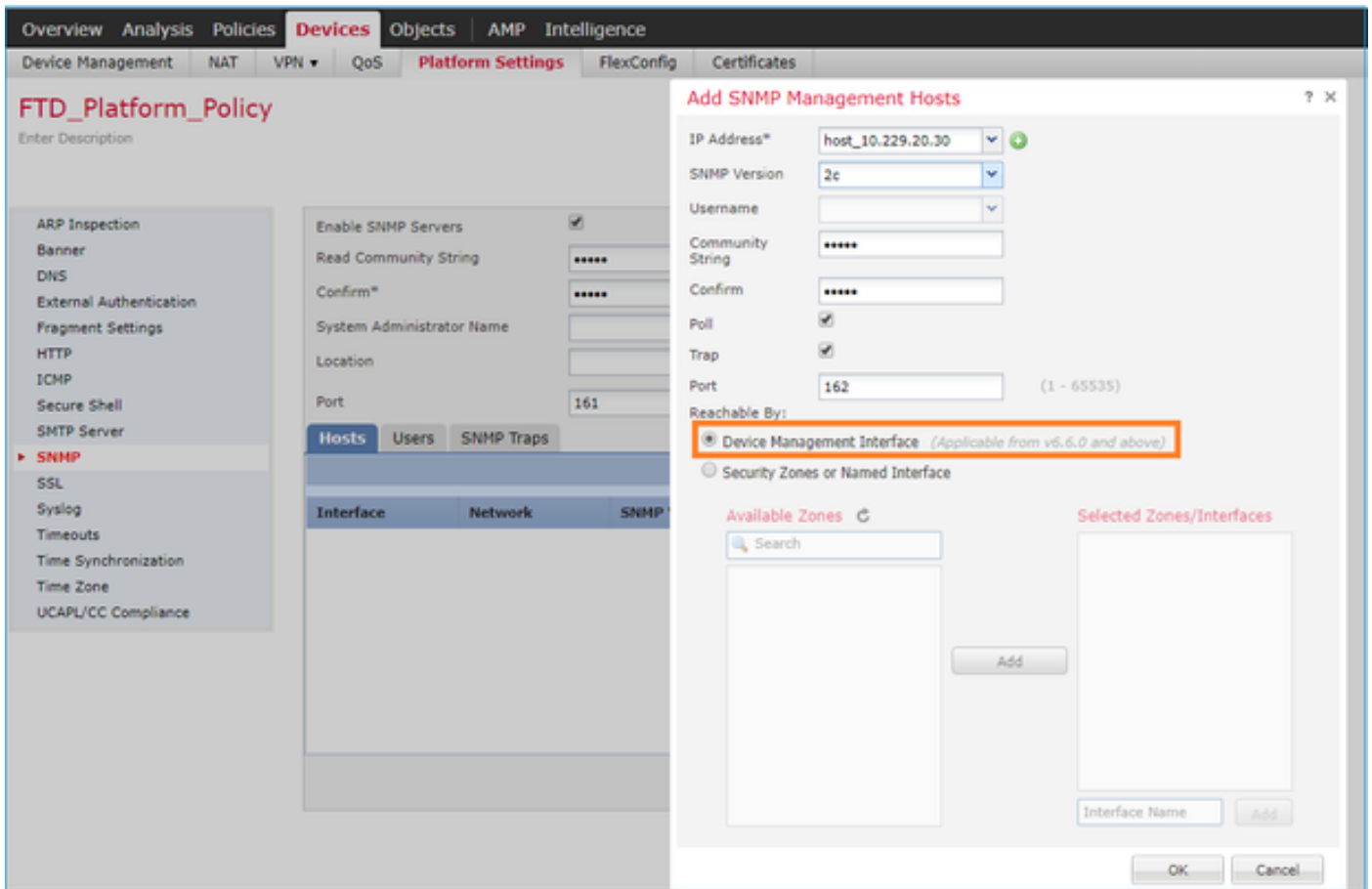
Type: TRAPS

Privilege: NO\_AUTH

OK Cancel

FTD 6.6 及更高版本中的变化

您可以指定 FTD 管理接口：



由于还可以将管理接口配置用于 SNMP，因此页面会显示以下警告消息：

如果通过 Devices > Platform Settings (Threat Defense) > SNMP > Hosts 使用设备管理接口配置的 SNMP 设置，则禁用此页上的设备平台 SNMP 配置。

### 配置 FXOS SNMPv3

打开 FMC UI 并导航至 选择设备 > 设备管理。选择设备并选择 SNMP。

Overview Analysis Policies **Devices** Objects AMP Intelligence 5 Deploy 20+ System Help ▾ itebar ▾

**Device Management** NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

**FTD2100-4** You have unsaved changes Save Cancel

Cisco Firepower 2110 Threat Defense 4

Device Routing Interfaces Inline Sets DHCP **SNMP**

SNMP settings configured on this page will apply only to the device platform

Admin State:  Enable 1

Port: 161

Community:

System Admin Name:

Location:

SNMP Traps Configuration 3 Add

Hostname	Port	Version	V3 Privilege	Type
No records to display				

SNMP Users Configuration 2 Add

Name	Auth Type	AES-128
No records to display		

## SNMP User Configuration ? X

Username: \*

Auth Algorithm Type:  ▾

Use AES:

Password\*:

Confirm:

Privacy Password\*:

Confirm:

### SNMP Trap Configuration

Hostname:\*  +

Community String:\*

Port:\*  (1 - 65535)

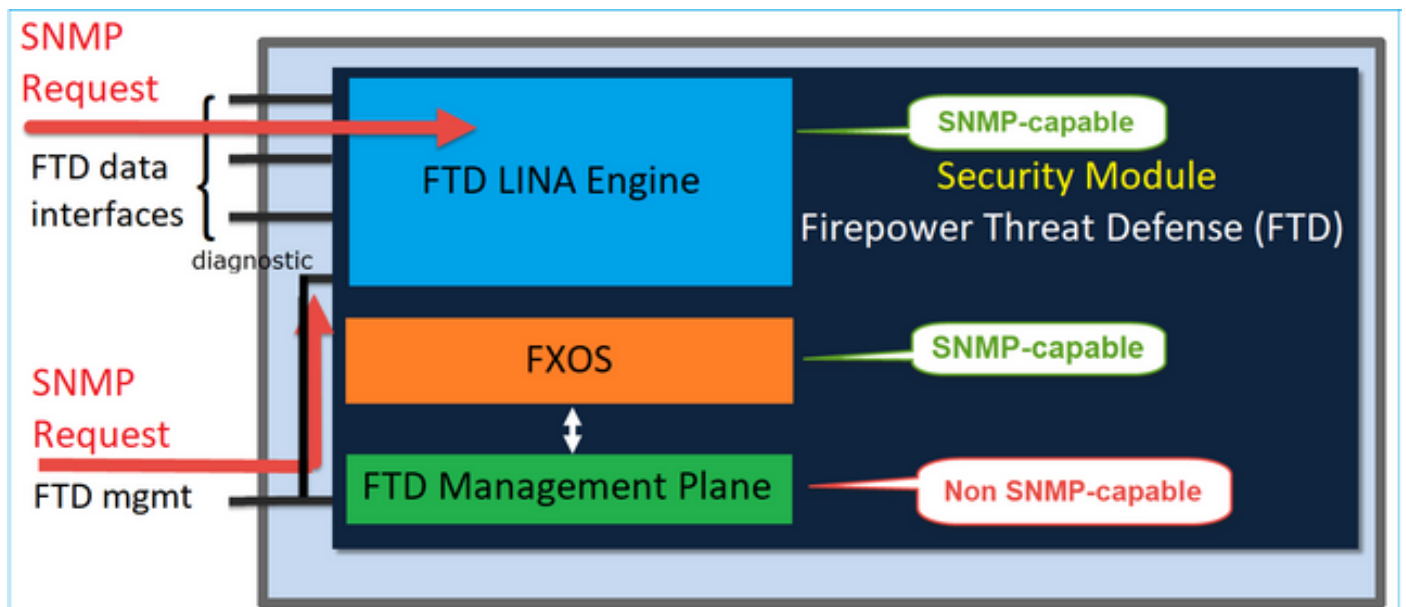
SNMP Version:

Type:

Privilege:

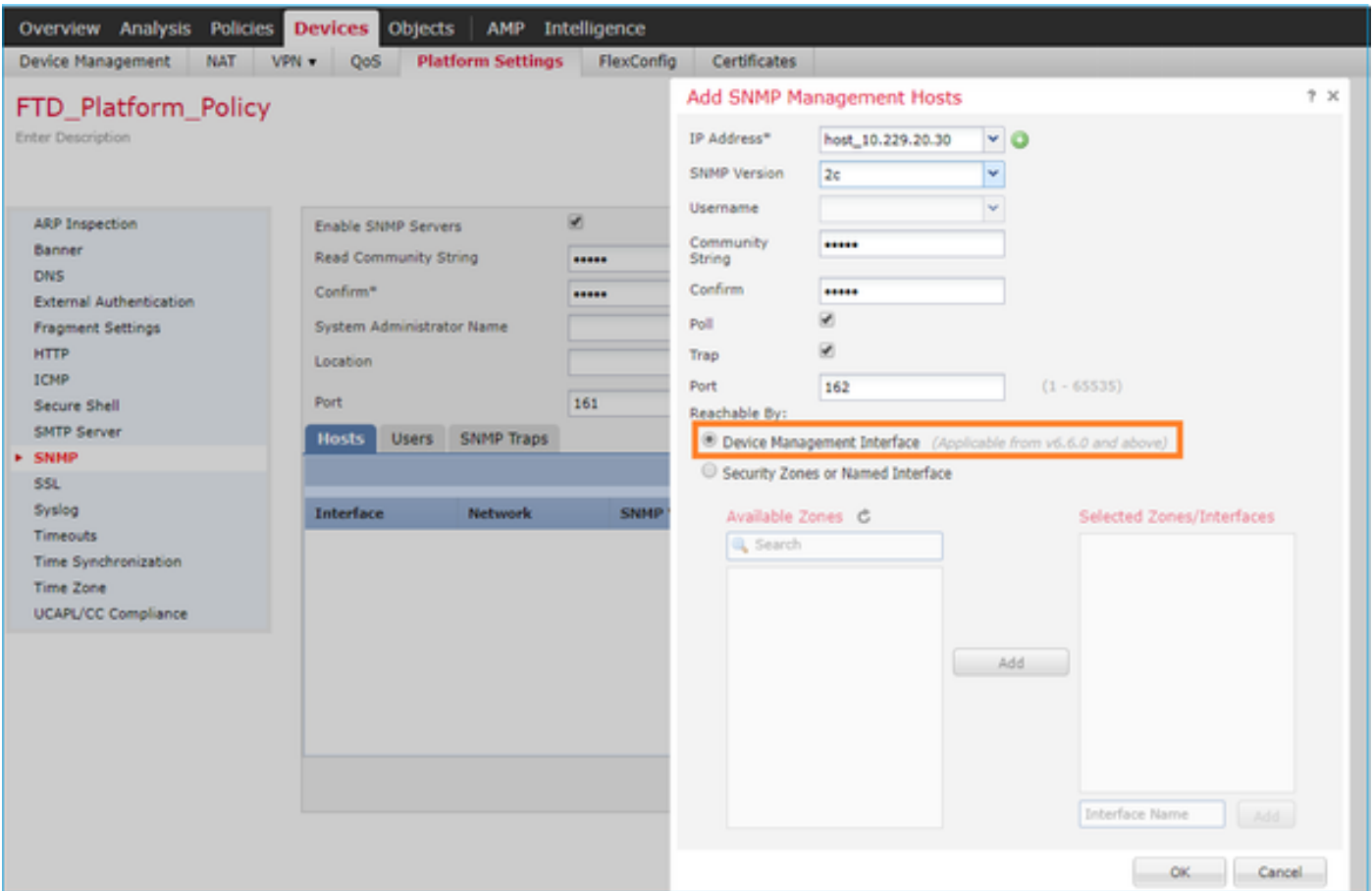
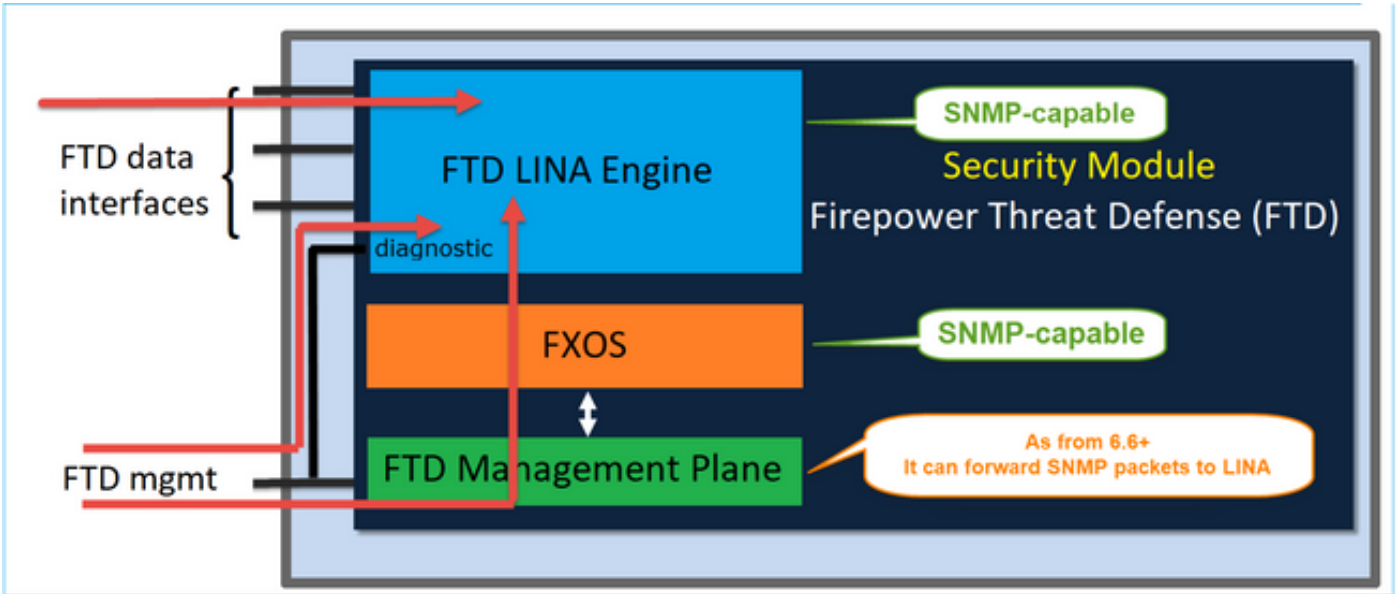
### 在 FPR2100 上配置 FTD (LINA) SNMP

- 对于 6.6 之前的版本，FTD FP1xxx/FP21xx 设备上的 LINA FTD SNMP 配置与 Firepower 4100 或 9300 设备上的 FTD 完全相同。



FTD 6.6 及更高版本

- 在 6.6 及更高版本中，还可以选择将 FTD 管理接口用于 LINA 轮询和陷阱。



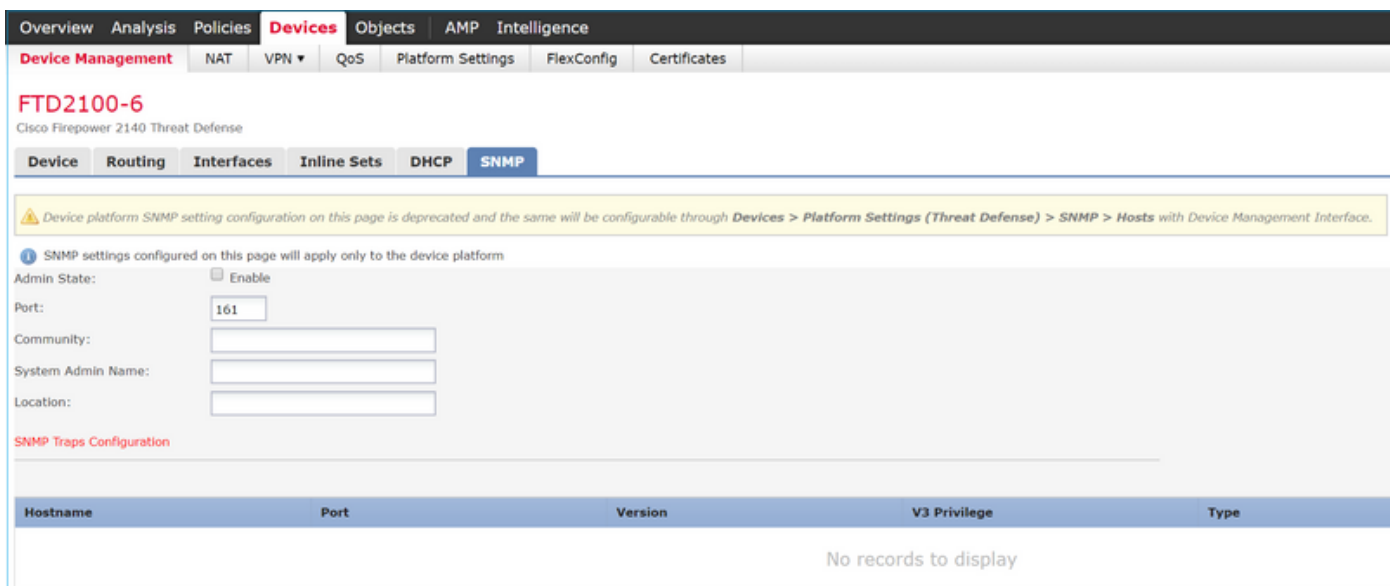
如果选择全新管理接口：

- 可通过管理接口使用 LINA SNMP。
- 在设备 > 设备管理下，不再需要 SNMP 选项卡，因此系统已禁用该选项卡。系统将显示通知横幅。“SNMP 设备”选项卡仅在 2100/1100 平台上可见。FPR9300/FPR4100 和 FTD55xx 平台上不存在此页面。

配置完成后，LINA SNMP 和 FXOS ( FP1xxx/FP2xxx 上 ) SNMP 轮询/陷阱组合信息通过 FTD 管



理接口传输。



从 6.6 版本开始，所有 FTD 平台均支持 SNMP 单一 IP 管理功能：

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- 运行 FTD 的 ASA5500
- FTDv

详情请参阅“配置用于 Threat Defense 的 SNMP”

## 验证

验证 FPR4100/FPR9300 的 FXOS SNMP

FXOS SNMPv2c 验证

CLI 配置验证：

```
<#root>
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

```
Sys Contact:
```

```
Sys Location:
```

```
ksec-fpr9k-1-A /monitoring # show snmp-trap
```

```
SNMP Trap:
  SNMP Trap          Port      Community  Version V3 Privilege Notification Type
-----
  192.168.10.100    162      V2c        Noauth   Traps
```

在 FXOS 模式下 :

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show run snmp
```

```
!Command: show running-config snmp
!Time: Mon Oct 16 15:41:09 2017
```

```
version 5.0(3)N2(4.21)
snmp-server host 192.168.10.100 traps version 2c cisco456
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
... All traps will appear as enable ...
snmp-server enable traps flexlink ifStatusChange
snmp-server context mgmt vrf management
snmp-server community cisco123 group network-operator
```

其他验证 :

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp host
```

```
-----
Host          Port Version  Level  Type  SecName
-----
192.168.10.100  162  v2c      noauth trap  cisco456
-----
```

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp
```

```
Community      Group / Access  context  acl_filter
-----
cisco123       network-operator
```

```
...
```

测试 SNMP 请求.

从有效主机执行SNMP请求。

确认生成陷阱.

您可以在启用 ethanalyzer 的情况下摆动接口，确认 SNMP 陷阱已生成且已发送到已定义的陷阱主机：

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
ethanalyzer local interface mgmt capture-filter "udp port 162"
```

```
Capturing on eth0
```

```
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0
```

```
2017-11-17 09:01:35.954624 10.62.148.35 -> 192.168.10.100 SNMP sNMPv2-Trap
```

```
2017-11-17 09:01:36.054511 10.62.148.35 -> 192.168.10.100 SNMP sNMPv2-Trap
```

---

 **警告：**接口摆动可能导致流量中断。请仅在实验室环境或维护窗口中执行此测试

---

## FXOS SNMPv3 验证

步骤1:打开FCM UI Platform Settings > SNMP > User，显示是否配置了任何密码和隐私密码：

## Edit user1

?
X

Name:\*

Auth Type: SHA

Use AES-128:

Password:  Set:Yes

Confirm Password:

Privacy Password:  Set:Yes

Confirm Privacy Password:

---

OK
Cancel

第二步：在CLI中，您可以在范围monitoring下验证SNMP配置：

```
<#root>
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp
```

```
Name: snmp
  Admin State: Enabled
  Port: 161
  Is Community Set: No
  Sys Contact:
  Sys Location:
```

```
ksec-fpr9k-1-A /monitoring # show snmp-user
```

```
SNMPv3 User:
  Name                Authentication type
  -----
  user1                Sha
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp-user detail
```

```
SNMPv3 User:
```

```
Name: user1
Authentication type: Sha
Password: ****
Privacy password: ****
Use AES-128: Yes
```

```
ksec-fpr9k-1-A /monitoring #
```

```
show snmp-trap
```

```
SNMP Trap:
```

SNMP Trap	Port	Community	Version	V3 Privilege	Notification Type
192.168.10.100	162		V3	Priv	Traps

第三步：在FXOS模式下，您可以展开SNMP配置和详细信息：

```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show running-config snmp all
```

```
...
snmp-server user user1 network-operator auth sha 0x022957ee4690a01f910f1103433e4b7b07d4b5fc priv aes-128
snmp-server host 192.168.10.100 traps version 3 priv user1
```

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp user
```

```
SNMP USERS
```

User	Auth	Priv(enforce)	Groups
user1	sha	aes-128(yes)	network-operator

```
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
```

User	Auth	Priv

```
ksec-fpr9k-1-A(fxos)#
```

```
show snmp host
```

Host	Port	Version	Level	Type	SecName
10.48.26.190	162	v3	priv	trap	user1

测试 SNMP 请求.

您可以验证配置并从任何具有SNMP功能的设备发出SNMP请求。

要检查 SNMP 请求的处理情况，可以使用 SNMP 调试：


```
<#root>
```

```
ksec-fpr9k-1-A(fxos)#
```

```
debug snmp pkt-dump
```

```
ksec-fpr9k-1-A(fxos)# 2017 Oct 16 17:11:54.681396 snmpd: 1281064976.000000:iso.10.10.1.1.10.10.10.10.1 :
2017 Oct 16 17:11:54.681833 snmpd:  SNMPPKTSTRT: 3.000000 161 1281064976.000000 1647446526.000000 0.000000
2017 Oct 16 17:11:54.683952 snmpd: 1281064976.000000:iso.10.10.1.2.10.10.10.10.2.83886080 = STRING: "mg
2017 Oct 16 17:11:54.684370 snmpd:  SNMPPKTSTRT: 3.000000 162 1281064976.000000 1647446526.000000 0.000000
```

---

 注意：调试可能会影响设备性能。

---

## 验证 FPR2100 的 FXOS SNMP

### FXOS SNMPv2 验证

通过 CLI 检查配置：

```
<#root>
```

```
FP2110-4 /monitoring #
```

```
show snmp
```

```
Name: snmp
  Admin State: Enabled
  Port: 161
  Is Community Set: Yes
  Sys Contact:
  Sys Location:
```

```
FP2110-4 /monitoring #
```

```
show snmp-trap
```

```
SNMP Trap:
  SNMP Trap          Port    Version V3 Privilege Notification Type
  -----
  10.48.26.190      162    V2c     Noauth     Traps
```

确认 SNMP 行为。

您可以验证您是否能够轮询FXOS并从主机或任何具有SNMP功能的设备发送SNMP请求。

使用 capture-traffic 命令查看 SNMP 请求和响应：

<#root>

>

capture-traffic

Please choose domain to capture traffic from:

0 - management0

Selection?

0

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options:

udp port 161

HS\_PACKET\_BUFFER\_SIZE is set to 4.

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes

13:50:50.521383 IP 10.48.26.190.42224 > FP2110-4.snmp: C=cisco123 GetNextRequest(29) interfaces.ifTab

13:50:50.521533 IP FP2110-4.snmp > 10.48.26.190.42224: C=cisco123 GetResponse(32) interfaces.ifTable.

^C

Caught interrupt signal

Exiting.

2 packets captured

2 packets received by filter

0 packets dropped by kernel

## FXOS SNMPv3 验证

通过 CLI 检查配置：

<#root>

FP2110-4 /monitoring #

show snmp

Name: snmp

Admin State: Enabled

Port: 161

Is Community Set: No

Sys Contact:

Sys Location:

FP2110-4 /monitoring #

show snmp-user detail

SNMPv3 User:

Name: user1

Authentication type: Sha

Password: \*\*\*\*

Privacy password: \*\*\*\*

```
Use AES-128: Yes
FP2110-4 /monitoring #
```

```
show snmp-trap detail
```

```
SNMP Trap:
SNMP Trap: 10.48.26.190
Port: 163
Version: V3
V3 Privilege: Priv
Notification Type: Traps
```

确认 SNMP 行为。

发送SNMP请求以验证您能够轮询FXOS。

此外，还可以捕获请求：

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management0
```

```
Selection?
```

```
0
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options:
```

```
udp port 161
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```
14:07:24.016590 IP 10.48.26.190.38790 > FP2110-4.snmp: F=r U= E= C= [|snmp]
```

```
14:07:24.016851 IP FP2110-4.snmp > 10.48.26.190.38790: F= [|snmp][|snmp]
```

```
14:07:24.076768 IP 10.48.26.190.38790 > FP2110-4.snmp: F=apr [|snmp][|snmp]
```

```
14:07:24.077035 IP FP2110-4.snmp > 10.48.26.190.38790: F=ap [|snmp][|snmp]
```

```
^C4 packets captured
```

```
Caught interrupt signal
```

```
Exiting.
```

```
4 packets received by filter
```

```
0 packets dropped by kernel
```



## 验证 FTD SNMP

验证 FTD LINA SNMP 配置：

```
<#root>
```

```
Firepower-module1#
```

```
show run snmp-server
```

```
snmp-server host OUTSIDE3 10.62.148.75 community ***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
```

在 FTD 6.6 及更高版本中，可以配置 FTD 管理接口并将其用于 SNMP：

```
<#root>
```

```
firepower#
```

```
show running-config snmp-server
```

```
snmp-server group Priv v3 priv
snmp-server group NoAuth v3 noauth
snmp-server user uspriv1 Priv v3 engineID
80000009fe99968c5f532fc1f1b0dbdc6d170bc82776f8b470 encrypted auth sha256
6d:cf:98:6d:4d:f8:bf:ee:ad:01:83:00:b9:e4:06:05:82:be:30:88:86:19:3c:96:42:3b
:98:a5:35:1b:da:db priv aes 128
6d:cf:98:6d:4d:f8:bf:ee:ad:01:83:00:b9:e4:06:05
snmp-server user usnoauth NoAuth v3 engineID
80000009fe99968c5f532fc1f1b0dbdc6d170bc82776f8b470
snmp-server host ngfw-management 10.225.126.168 community ***** version 2c
snmp-server host ngfw-management 10.225.126.167 community *****
snmp-server host ngfw-management 10.225.126.186 version 3 uspriv1
no snmp-server location
no snmp-server contact
```

其他验证：

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

```
host ip = 10.62.148.75, interface = OUTSIDE3 poll community ***** version 2c
```

通过 SNMP 服务器 CLI 运行 snmpwalk：

```
<#root>
```

```
root@host:/Volume/home/admin#
```

```
snmpwalk -v2c -c cisco -OS 10.62.148.48
```

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 10.2.3.1 (Build 43), ASA Versi
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2313
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8350600) 23:11:46.00
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: Firepower-module1
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 4
IF-MIB::ifNumber.0 = INTEGER: 10
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifIndex.6 = INTEGER: 6
IF-MIB::ifIndex.7 = INTEGER: 7
IF-MIB::ifIndex.8 = INTEGER: 8
IF-MIB::ifIndex.9 = INTEGER: 9
IF-MIB::ifIndex.10 = INTEGER: 10
IF-MIB::ifIndex.11 = INTEGER: 11
...
```

验证 SNMP 流量统计信息。

```
<#root>
```

```
Firepower-module1#
```

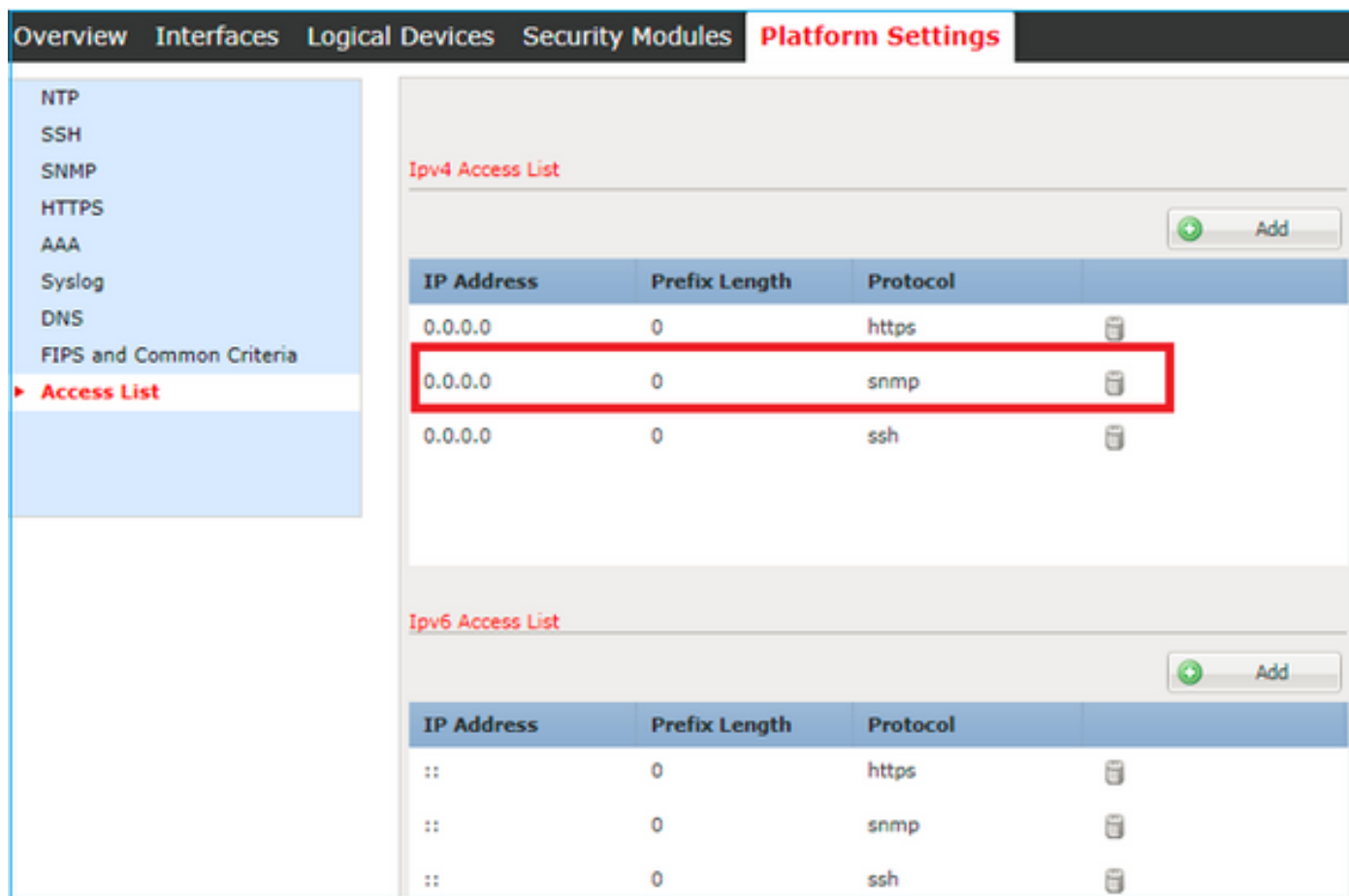
```
show snmp-server statistics
```

```
1899 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  1899 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  1899 Get-next PDUs
  0 Get-bulk PDUs
  0 Set-request PDUs (Not supported)
1904 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  1899 Response PDUs
  5 Trap PDUs
```

## 允许 SNMP 流量进入 FPR4100/FPR9300 的 FXOS

FPR4100/9300 上的 FXOS 配置可以根据源 IP 地址限制 SNMP 访问。“访问列表”配置部分用于定义哪些网络/主机能够通过 SSH、HTTPS 或 SNMP 访问设备。您需要确保允许来自 SNMP 服务器的 SNMP 查询。

## 通过 GUI 配置全局访问列表



The screenshot shows the 'Platform Settings' tab in a network management GUI. On the left is a navigation menu with 'Access List' selected. The main area is divided into two sections: 'Ipv4 Access List' and 'Ipv6 Access List'. Each section has an 'Add' button and a table of entries.

IP Address	Prefix Length	Protocol	
0.0.0.0	0	https	
0.0.0.0	0	snmp	
0.0.0.0	0	ssh	

IP Address	Prefix Length	Protocol	
::	0	https	
::	0	snmp	
::	0	ssh	

## 通过 CLI 配置全局访问列表

```
<#root>  
ksec-fpr9k-1-A#  
scope system  
ksec-fpr9k-1-A /system #  
  scope services  
ksec-fpr9k-1-A /system/services #  
  enter ip-block 0.0.0.0 0 snmp  
ksec-fpr9k-1-A /system/services/ip-block* #  
commit-buffer
```

确认

```
<#root>
```

```
ksec-fpr9k-1-A /system/services #
```

```
show ip-block
```

Permitted IP Block:

IP Address	Prefix Length	Protocol
0.0.0.0		0 https
0.0.0.0		0 snmp
0.0.0.0		0 ssh

## 使用 OID Object Navigator

[Cisco SNMP Object Navigator](#) 是一款在线工具，可用于转换不同的 OID 并提供简短说明。

Tools & Resources

# SNMP Object Navigator

HOME | SUPPORT | TOOLS & RESOURCES

TRANSLATE/BROWSE | SEARCH | DOWNLOAD MIBS | MIB SUPPORT - SW

Translate | Browse The Object Tree

Translate OID into object name or object name into OID to receive object details

Enter OID or object name:  examples -  
OID: 1.3.6.1.4.1.9.9.27  
Object Name: ifIndex

Translate

Object Information

Specific Object Information

Object	cpmCPUTotalTable
OID	1.3.6.1.4.1.9.9.109.1.1.1
Type	SEQUENCE
Permission	not-accessible
Status	current
MIB	CISCO-PROCESS-MIB; - <a href="#">View Supporting Images</a>
Description	A table of overall CPU statistics.

在 FTD LINA CLI 中使用 `show snmp-server oid` 命令，以检索可轮询的 LINA OID 的完整列表。

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
firepower#
```

```
show snmp-server oid
```

```

-----
[0]      10.10.1.10.10.10.1.1.      sysDescr
[1]      10.10.1.10.10.10.1.2.      sysObjectID
[2]      10.10.1.10.10.10.1.3.      sysUpTime
[3]      10.10.1.1.10.1.1.4.         sysContact
[4]      10.10.1.1.10.1.1.5.         sysName
[5]      10.10.1.1.10.1.1.6.         sysLocation
[6]      10.10.1.1.10.1.1.7.         sysServices
[7]      10.10.1.1.10.1.1.8.         sysORLastChange
...
[1081]   10.3.1.1.10.0.10.1.10.1.9. vacmAccessStatus
[1082]   10.3.1.1.10.0.10.1.10.1.   vacmViewSpinLock
[1083]   10.3.1.1.10.0.10.1.10.2.1.3. vacmViewTreeFamilyMask
[1084]   10.3.1.1.10.0.10.1.10.2.1.4. vacmViewTreeFamilyType
[1085]   10.3.1.1.10.0.10.1.10.2.1.5. vacmViewTreeFamilyStorageType
[1086]   10.3.1.1.10.0.10.1.10.2.1.6. vacmViewTreeFamilyStatus
-----
firepower#

```

 注意：命令是隐藏的。

## 故障排除

Cisco TAC 收到的常见 SNMP 支持案例如下：

1. 无法轮询 FTD LINA SNMP
2. 无法轮询 FXOS SNMP
3. 需要使用哪些 SNMP OID 值？
4. 无法获取 SNMP 陷阱
5. 无法通过 SNMP 监控 FMC
6. 无法配置 SNMP
7. Firepower Device Manager 上的 SNMP 配置

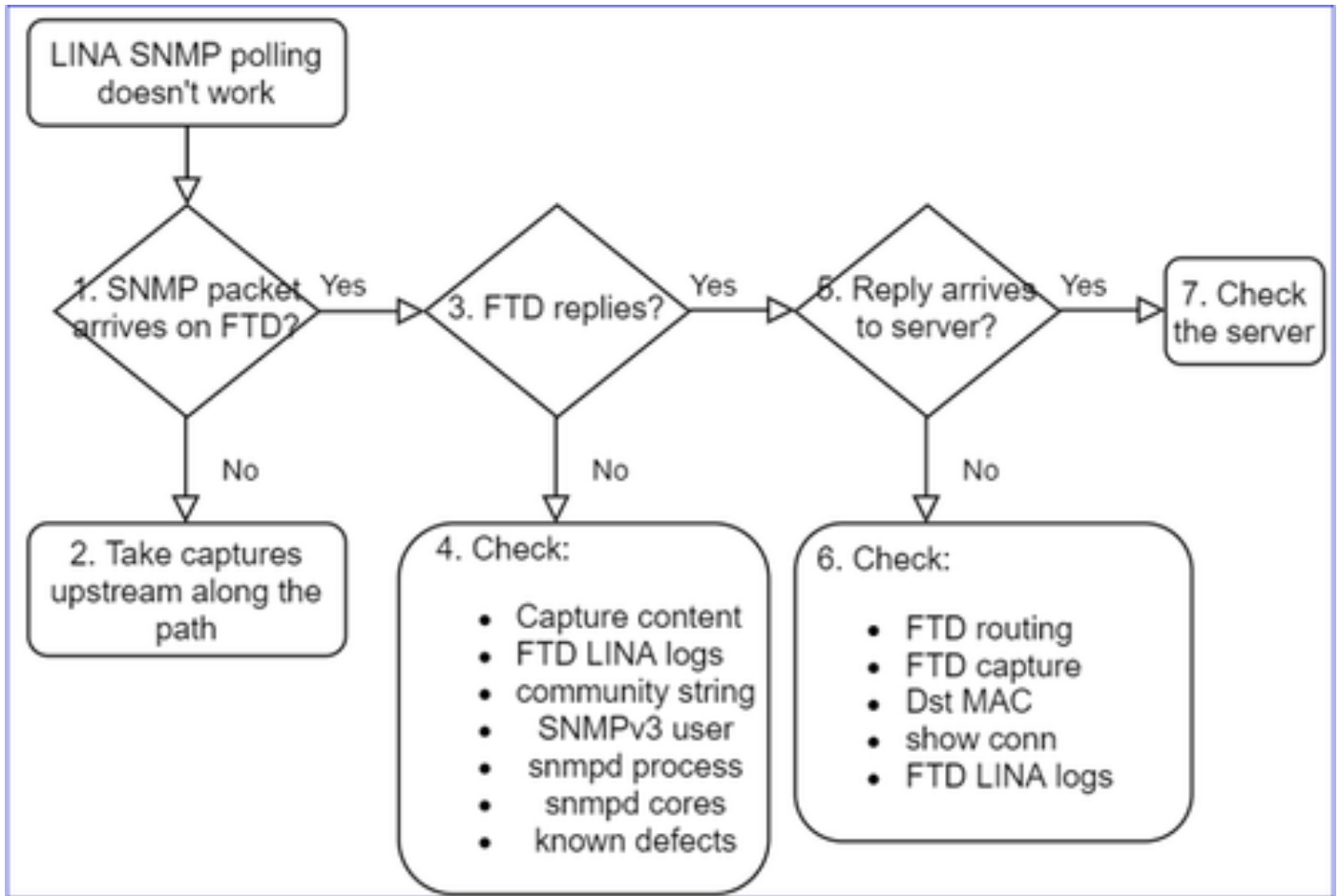
### 无法轮询 FTD LINA SNMP

问题描述（Cisco TAC 真实案例示例）：

- “无法通过 SNMP 获取数据。”
- “无法通过 SNMPv2 轮询设备。”
- “SNMP 不正常工作。我们想要使用 SNMP 监控防火墙，但配置之后，遇到了问题。”
- “我们的两个监控系统无法通过 SNMP v2c 或 3 监控 FTD。”
- “SNMP 遍历对防火墙失效。”

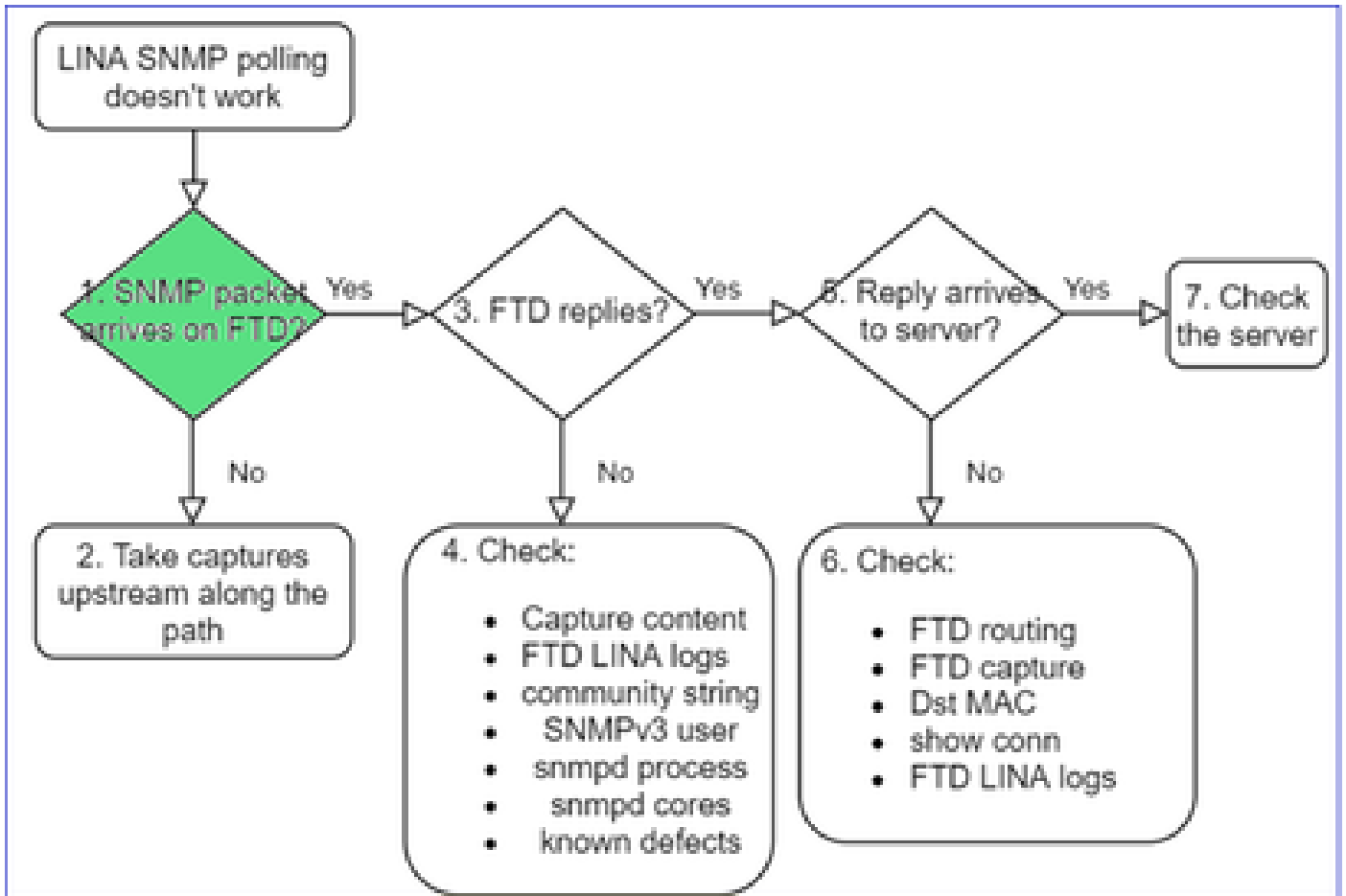
关于如何排除故障的建议

下面是排除 LINA SNMP 轮询问题故障流程图的推荐过程：



深入了解

1. SNMP数据包是否到达FTD



- 启用捕获功能以验证 SNMP 数据包是否可到达。

FTD管理接口 ( 6.6版之后 ) 上的SNMP使用管理关键字 :

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

```
snmp-server host management 192.168.2.100 community ***** version 2c
```

如果是 FTD 数据接口上的 SNMP , 请使用接口名称 :

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

```
snmp-server host net201 192.168.2.100 community ***** version 2c
```

FTD 管理接口上的捕获：

```
<#root>
>
capture-traffic

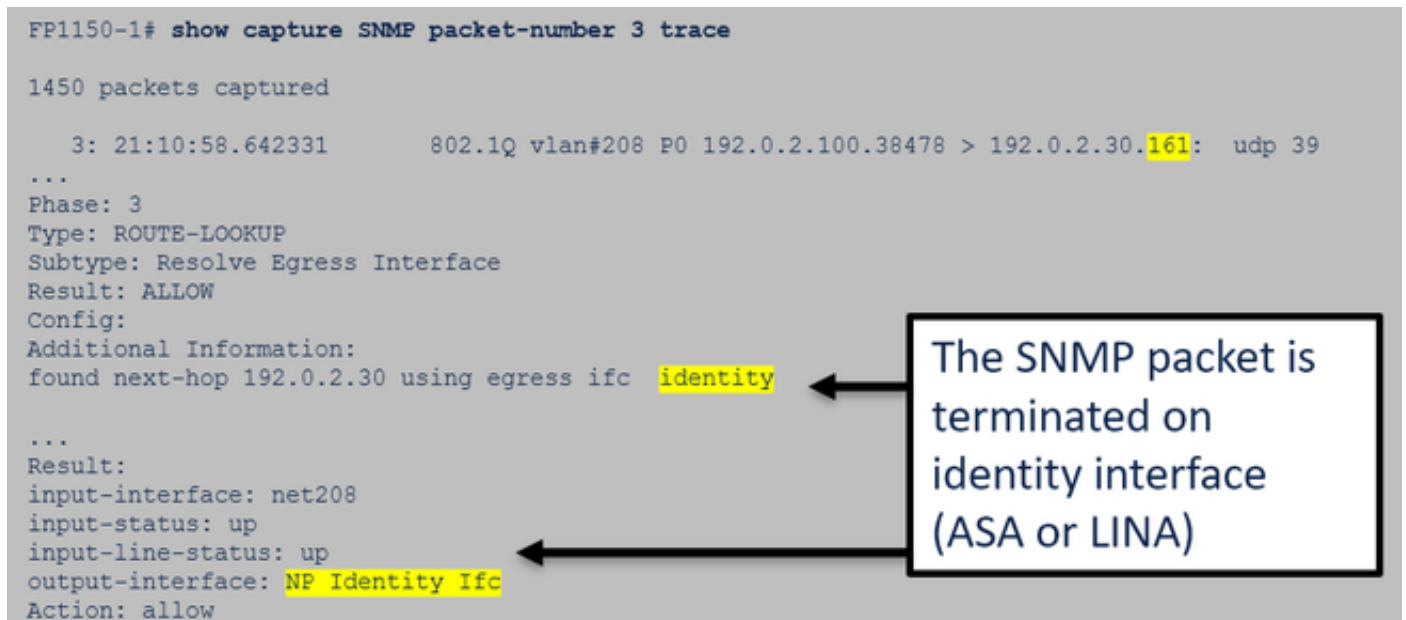
Please choose domain to capture traffic from:
 0 - management1
 1 - management0
 2 - Global
Selection?
1
```

FTD 数据接口上的捕获：

```
<#root>
firepower#
capture SNMP interface net201 trace match udp any any eq 161
```

FTD数据接口数据包跟踪（6.6/9.14.1之前的版本）：

```
FP1150-1# show capture SNMP packet-number 3 trace
1450 packets captured
 3: 21:10:58.642331      802.1Q vlan#208 P0 192.0.2.100.38478 > 192.0.2.30.161:  udp 39
...
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.0.2.30 using egress ifc identity
...
Result:
input-interface: net208
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
```



The SNMP packet is terminated on identity interface (ASA or LINA)

FTD数据接口数据包跟踪（6.6/9.14.1之后）：



```

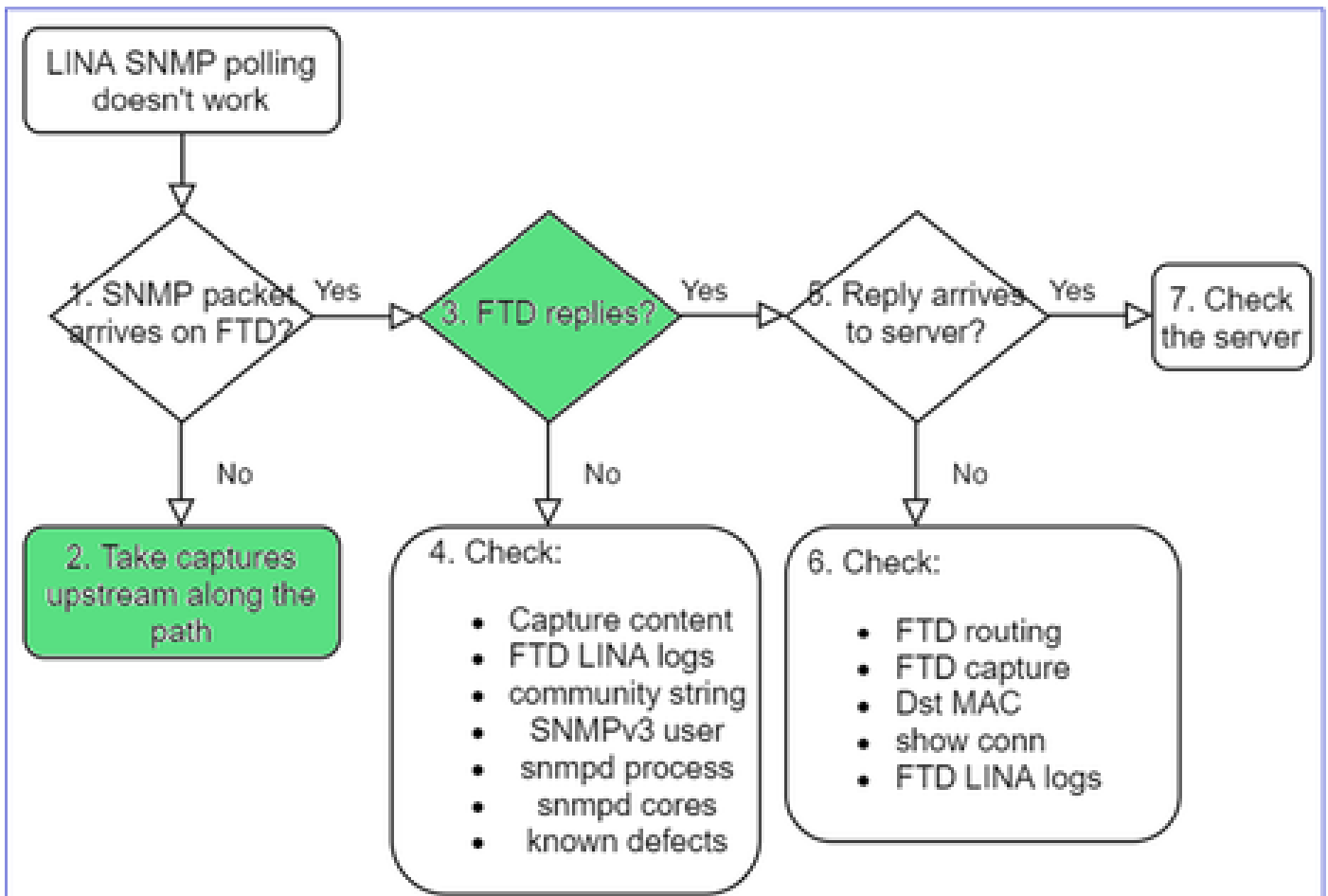
firepower# show capture SNMP packet-number 1 trace
1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.21.100.58255 > 192.168.21.50.161:  udp 39
...
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 9
Config:
nat (nlp_int_tap,net201) source static nlp_server__snmp_192.168.21.100_intf4 interface destination static
0_192.168.21.100_4 0_192.168.21.100_4
Additional Information:
NAT divert to egress interface nlp_int_tap(vrfid:0)
Untranslate 192.168.21.50/161 to 169.254.1.2/161

```

NAT diverts the packet to Snort engine  
(NLP – Non-Lina Process tap interface)

2. 如果您在FTD入口捕获中看不到SNMP数据包：

- 沿路径进行上游捕获.
- 确保 SNMP 服务器使用的 FTD IP 正确无误.
- 从面向 FTD 接口的交换机端口开始，向上游移动.



3. 是否看到FTD SNMP应答？

要验证 FTD 是否已应答，请检查：

1. FTD 出口捕获 ( LINA 或管理接口 )

检查源端口为 161 的 SNMP 数据包：

```
<#root>
```

```
firepower#
```

```
show capture SNMP
```

```
75 packets captured
```

```
1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.2.100.58255 > 192.168.2.50.161:  udp 39
2: 22:43:39.568329      802.1Q vlan#201 P0 192.168.2.100.58255 > 192.168.2.50.161:  udp 39
3: 22:43:39.569611      802.1Q vlan#201 P0 192.168.2.50.161 > 192.168.2.100.58255:  udp 119
```

在6.6/9.14.1之后的版本中，您还有另一个捕获点：在NLP分路器界面上捕获。NATed IP来自162.254.x.x范围：

```
<#root>
```

```
admin@firepower:~$
```

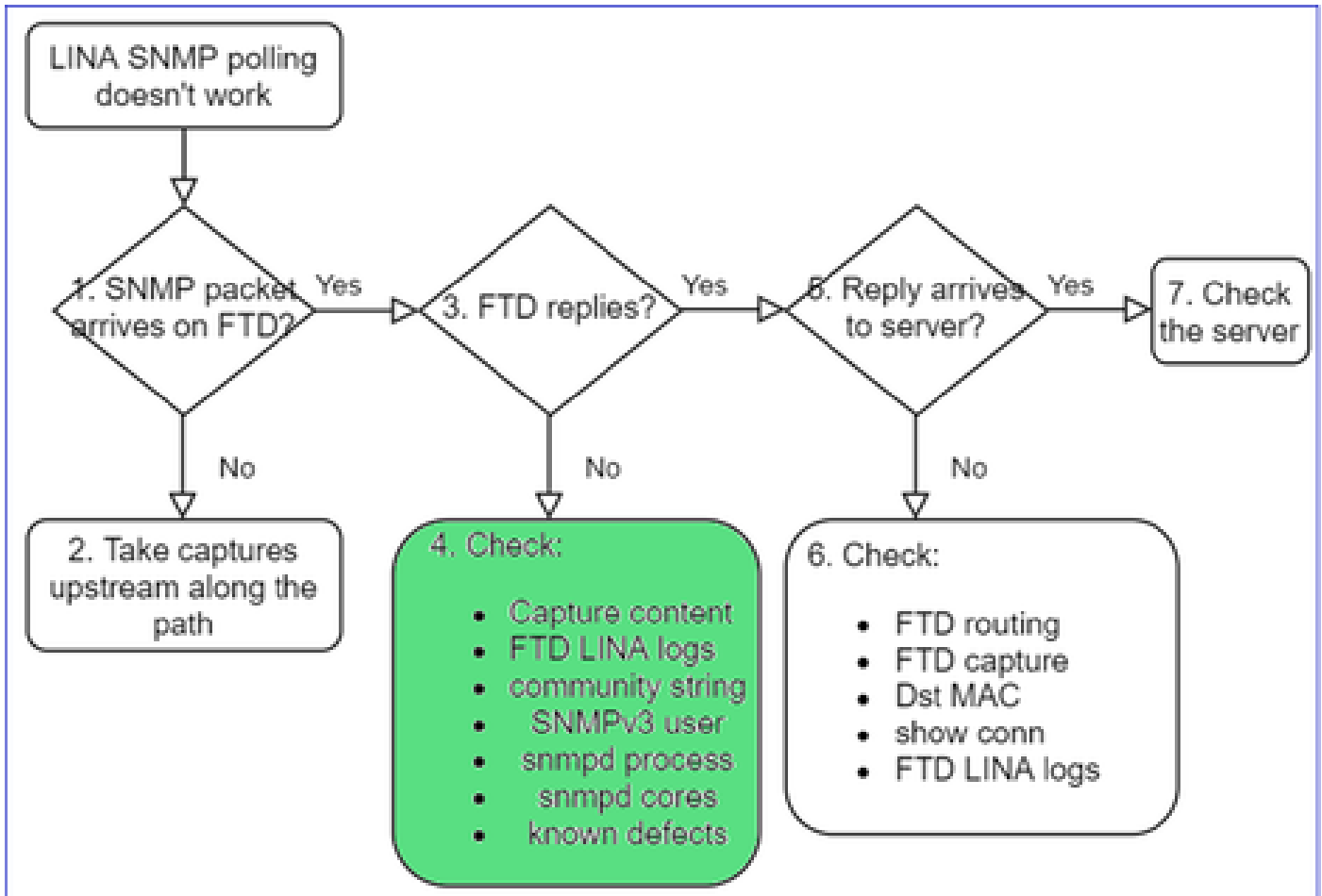
```
sudo tcpdump -i tap_nlp
```

```
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
16:46:28.372018 IP 192.168.2.100.49008 > 169.254.1.2.snmp: C="Cisc0123" GetNextRequest(28) E:cisco.9.
```

```
16:46:28.372498 IP 192.168.1.2.snmp > 192.168.2.100.49008: C="Cisc0123" GetResponse(35) E:cisco.9.109
```

#### 4. 额外支票



a.对于Firepower 4100/9300设备，请检查[FXOS兼容性表](#)。

#### Firepower 4100/9300 Compatibility with ASA and Threat Defense

The following table lists compatibility between the ASA or threat defense applications with the Firepower 4100/9300. The FXOS versions with (EoL) appended have reached their end of life (EoL), or end of support.

**Note** The bold versions listed below are specially-qualified companion releases. You should use these software combinations whenever possible because Cisco performs enhanced testing for these combinations.

**Note** Firepower 1000/2100 appliances utilize FXOS only as an underlying operating system that is included in the ASA and threat defense unified image bundles.

**Note** FXOS 2.12/ASA 9.18/Threat Defense 7.2 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.

Table 2. ASA or Threat Defense, and Firepower 4100/9300 Compatibility

FXOS Version	Model	ASA Version	Threat Defense Version		
2.13(0.198)+ <b>Note</b> FXOS 2.13(0.198)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	<b>9.19(x)</b> (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.3.0</b> (recommended) 7.2.0 7.1.0 7.0.0 6.7.0 6.6.x		
	Firepower 4145 Firepower 4125 Firepower 4115	<b>9.19(x)</b> (recommended) 9.18(x) 9.17(x) 9.16(x)	<b>7.3.0</b> (recommended) 7.2.0 7.1.0 7.0.0		
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)	6.7.0 6.6.x 6.5.0 6.4.0		
	2.12(0.31)+ <b>Note</b> FXOS 2.12(0.31)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0 6.7.0 6.6.x	
		Firepower 4145 Firepower 4125 Firepower 4115	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0	
		Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)	6.7.0 6.6.x 6.5.0 6.4.0	
		Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x) 9.13(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0 6.7.0 6.6.x 6.5.0	
		Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.12(x) 9.10(x) 9.9(x) 9.8(x)	6.4.0 6.3.0	
		2.11(1.154)+ <b>Note</b> FXOS 2.11(1.154)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use	Firepower 4112	<b>9.17(x)</b> (recommended) 9.16(x) 9.15(1) 9.14(x)	<b>7.1.0</b> (recommended) 7.0.0 6.7.0 6.6.x

## b.检查FTD LINA snmp-server统计信息：

```
<#root>
firepower#
clear snmp-server statistics

firepower#
show snmp-server statistics

379 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  351 Number of requested variables    <- SNMP requests in
...
360 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  351 Response PDUs                    <- SNMP replies out
  9 Trap PDUs
```

## c. FTD LINA连接表

如果在FTD入口接口上的捕获中看不到数据包，此检查非常有用。请注意，此验证仅对数据接口上的SNMP有效。如果SNMP在管理接口（6.6/9.14.1之后）上，则不创建连接。

```
<#root>
firepower#
show conn all protocol udp port 161

13 in use, 16 most used
...
UDP nlp_int_tap 192.168.1.2:161 net201 192.168.2.100:55048, idle 0:00:21, bytes 70277, flags -c
```

## d. FTD LINA系统日志

此检查也仅能有效验证数据接口上的SNMP！如果SNMP位于管理接口，则不会创建日志：

```
<#root>
firepower#
```

```
show log | i 302015.*161
```

```
Jul 13 2021 21:24:45: %FTD-6-302015: Built inbound UDP connection 5292 for net201:192.0.2.100/42909 (19
```

### e.检查FTD是否由于不正确的主机源IP而丢弃SNMP数据包

```
firepower# show capture SNMP packet-number 1 trace
1: 22:33:00.183248      802.1Q vlan#201 P0 192.168.21.100.43860 > 192.168.21.50.161: udp 39
Phase: 1
Type: CAPTURE
...
Phase: 6
Type: ACCESS-LIST
Result: DROP
...
Result:
input-interface: net201(vrfid:0)
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
flow (NA)/NA

firepower# show run snmp-server
snmp-server host net201 192.168.22.100 community ***** version 2c

firepower# show asp table classify interface net201 domain permit match port=161
Input Table
in id=0x14f65b193b30, priority=501, domain=permit, deny=false
hits=8, user_data=0x0, cs_id=0x0, use_real_addr, flags=0x0, protocol=17
src ip/id=192.168.22.100, mask=255.255.255.255, port=0, tag=any
dst ip/id=169.254.1.2, mask=255.255.255.255, port=161, tag=any, dscp=0x0, nsg_id=none
input_ifc=net201(vrfid:0), output_ifc=any
```

### f.凭证不正确 ( SNMP社区 )

可在捕获内容中查看社区值 ( SNMP v1 和 2c ) :

Delta	Source	Destination	Protocol	Length
0.000000	192.168.21.100	192.168.21.50	SNMP	

```
> Frame 3: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
> Ethernet II, Src: VMware_85:3e:d2 (00:50:56:85:3e:d2), Dst: a2:b8:dc:
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 201
> Internet Protocol Version 4, Src: 192.168.21.100, Dst: 192.168.21.50
> User Datagram Protocol, Src Port: 45230, Dst Port: 161
Simple Network Management Protocol
  version: v2c (1)
  community: cisco123
  data: get-next-request (1)
```

### g.配置不正确 ( 例如 , SNMP版本或社区字符串 )

可以采用多种方式验证设备 SNMP 配置和社区字符串 :

```
<#root>
```

```
firepower#
```

```
more system:running-config | i community
```

```
snmp-server host net201 192.168.2.100 community CISC0123 version 2c
```

另一种方式：

```
<#root>
firepower#
debug menu netsnmp 4
```

#### h. FTD LINA/ASA ASP丢弃

此检查非常实用，可验证 FTD 是否丢弃 SNMP 数据包。首先，清除计数器（清除 ASP 丢包），然后测试：

```
<#root>
firepower#
clear asp drop

firepower#
show asp drop
```

```
Frame drop:
  No valid adjacency (no-adjacency)                6
  No route to host (no-route)                       204
  Flow is denied by configured rule (acl-drop)      502
  FP L2 rule drop (l2_acl)                          1
```

```
Last clearing: 19:25:03 UTC Aug 6 2021 by enable_15
```

```
Flow drop:
Last clearing: 19:25:03 UTC Aug 6 2021 by enable_15
```

#### i. ASP捕获

ASP 捕获可帮助发现丢包（例如 ACL 或邻接）：

```
<#root>
firepower#
capture ASP type asp-drop all
```

测试并检查捕获内容：

```
<#root>
```

```
firepower#  
show capture  
  
capture ASP type asp-drop all [Capturing - 196278 bytes]
```

## j. SNMP核心 ( 回溯 ) -验证方式1

如果怀疑系统中存在稳定性问题，此检查非常有用：

```
<#root>  
firepower#  
show disk0: | i core  
  
13 52286547 Jun 11 2021 12:25:16 coredumpfsys/core.snmpd.6208.1626214134.gz
```

## SNMP 核心 ( 回溯 ) – 验证方式 2

```
<#root>  
admin@firepower:~$  
ls -l /var/data/cores  
  
-rw-r--r-- 1 root root 685287 Jul 14 00:08 core.snmpd.6208.1626214134.gz
```

如果看到 SNMP 核心文件，请收集这些文件并联系 Cisco TAC：

- FTD TS 文件 ( 或 ASA show tech )
- snmpd 核心文件

SNMP 调试 ( 隐藏命令，仅在较新版本中可用 )：

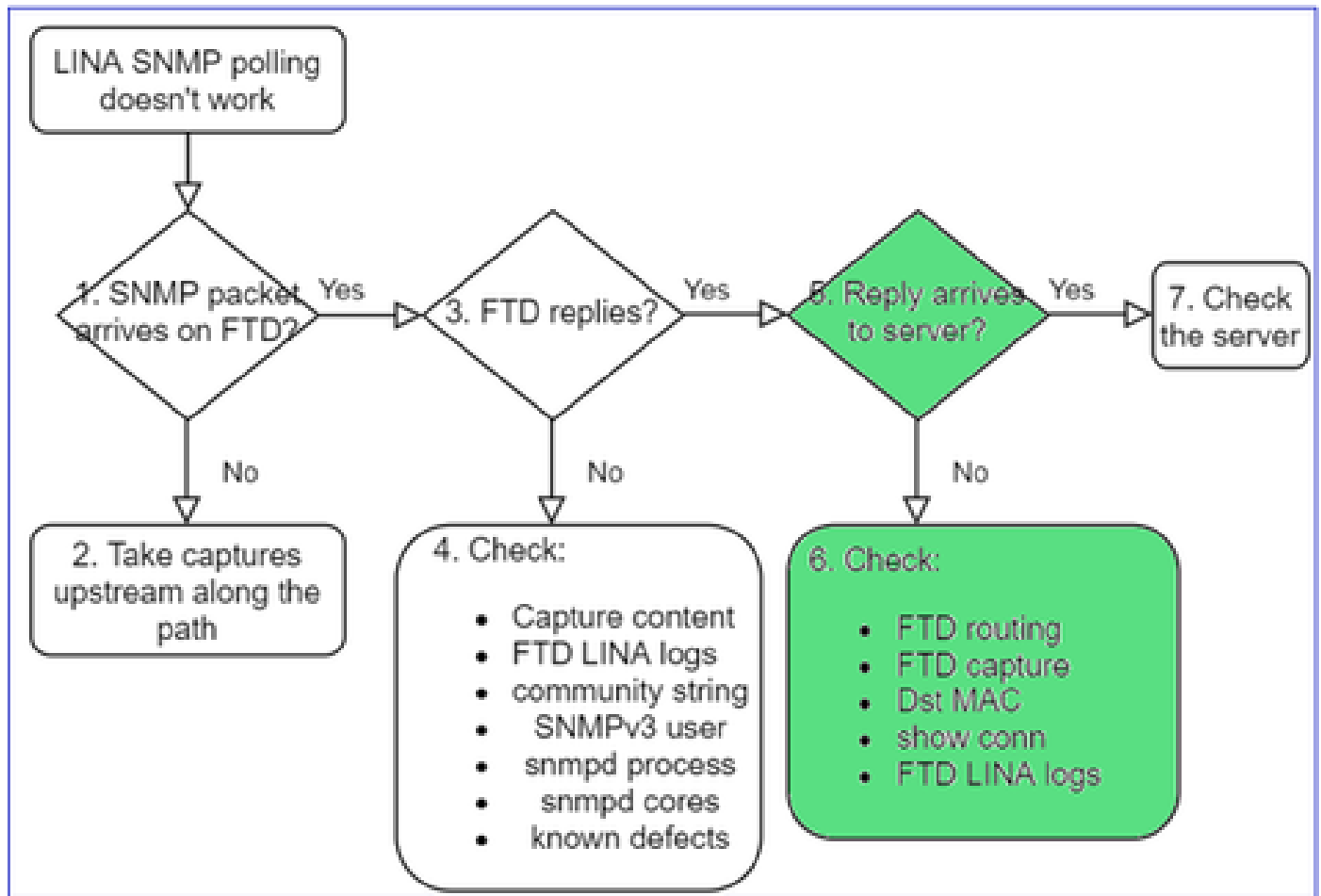
```
<#root>  
firepower#  
debug snmp trace [255]  
  
firepower#  
debug snmp verbose [255]  
  
firepower#
```

```
debug snmp error [255]
```

```
firepower#
```

```
debug snmp packet [255]
```

防火墙 SNMP 应答是否到达服务器？



如果 FTD 已应答，但应答未到达服务器，请检查：

a. FTD路由

FTD 管理接口路由：

```
<#root>
```

```
>
```

```
show network
```

FTD LINA 数据接口路由：

```
<#root>
```



```
firepower#
```

```
show route
```

## b. 目的MAC验证

FTD 管理目的 MAC 验证：

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management1
```

```
1 - management0
```

```
2 - Global
```

```
Selection?
```

```
1
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options:
```

```
-n -e udp port 161
```

```
01:00:59.553385 a2:b8:dc:00:00:02 > 5c:fc:66:36:50:ce, ethertype IPv4 (0x0800), length 161: 10.62.148.1
```

FTD LINA 数据接口目的 MAC 验证：

```
<#root>
```

```
firepower#
```

```
show capture SNMP detail
```

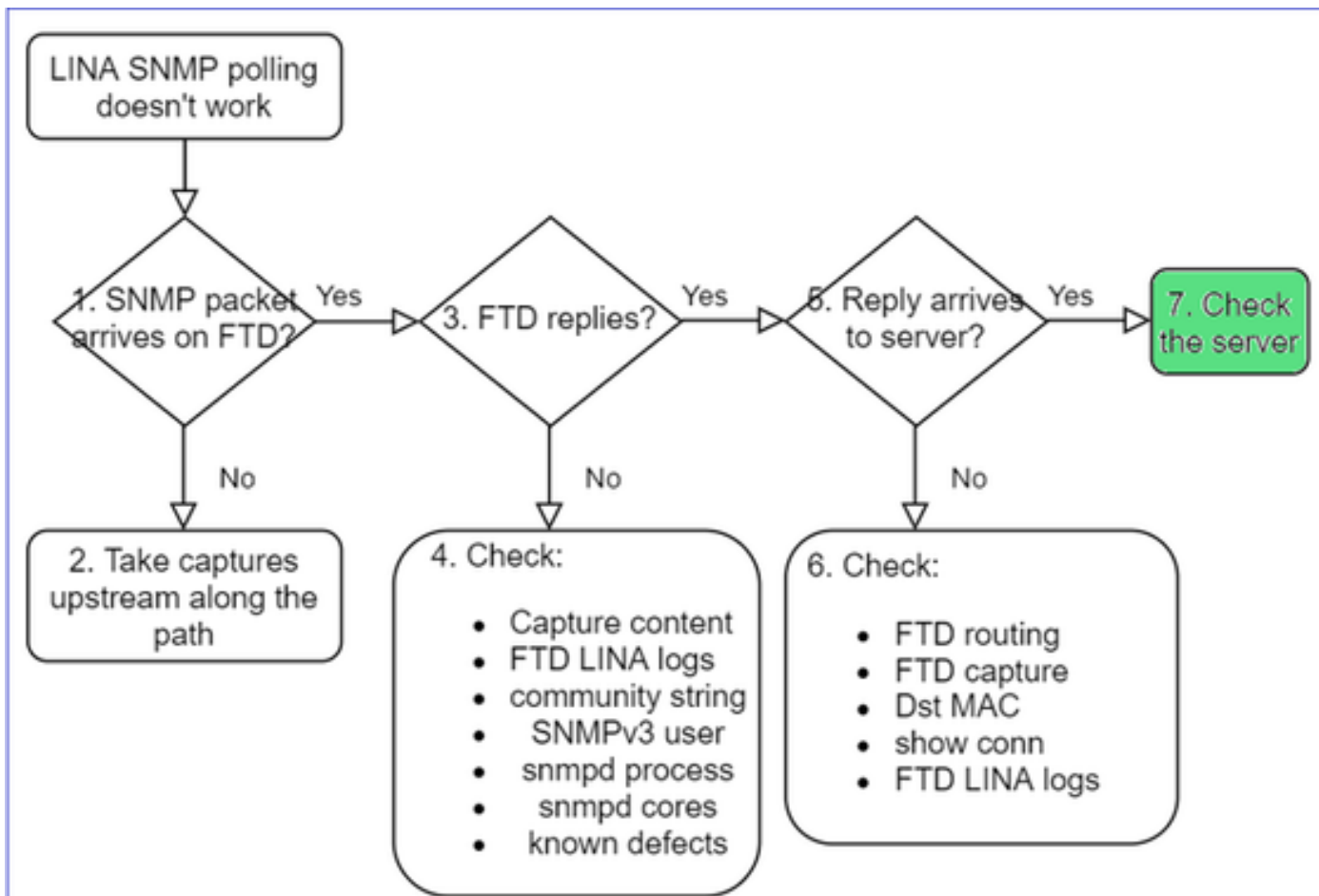
```
...
```

```
6: 01:03:01.391886 a2b8.dc00.0003 0050.5685.3ed2 0x8100 Length: 165
```

```
802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.40687: [udp sum ok] udp 119 (DF) (ttl 64,
```

c. 检查路径上可能丢弃/阻止 SNMP 数据包的设备。

检查 SNMP 服务器



a.检查捕获内容以验证设置。

b.检查服务器配置。

c.尝试修改SNMP社区名称（例如，不含特殊字符）。

只要符合以下两个条件，您就可以使用终端主机甚至FMC来测试轮询：

1. 已建立 SNMP 连接.
2. 允许源 IP 轮询设备.

<#root>

```
admin@FS2600-2:~$
```

```
snmpwalk -c cisco -v2c 192.0.2.197
```

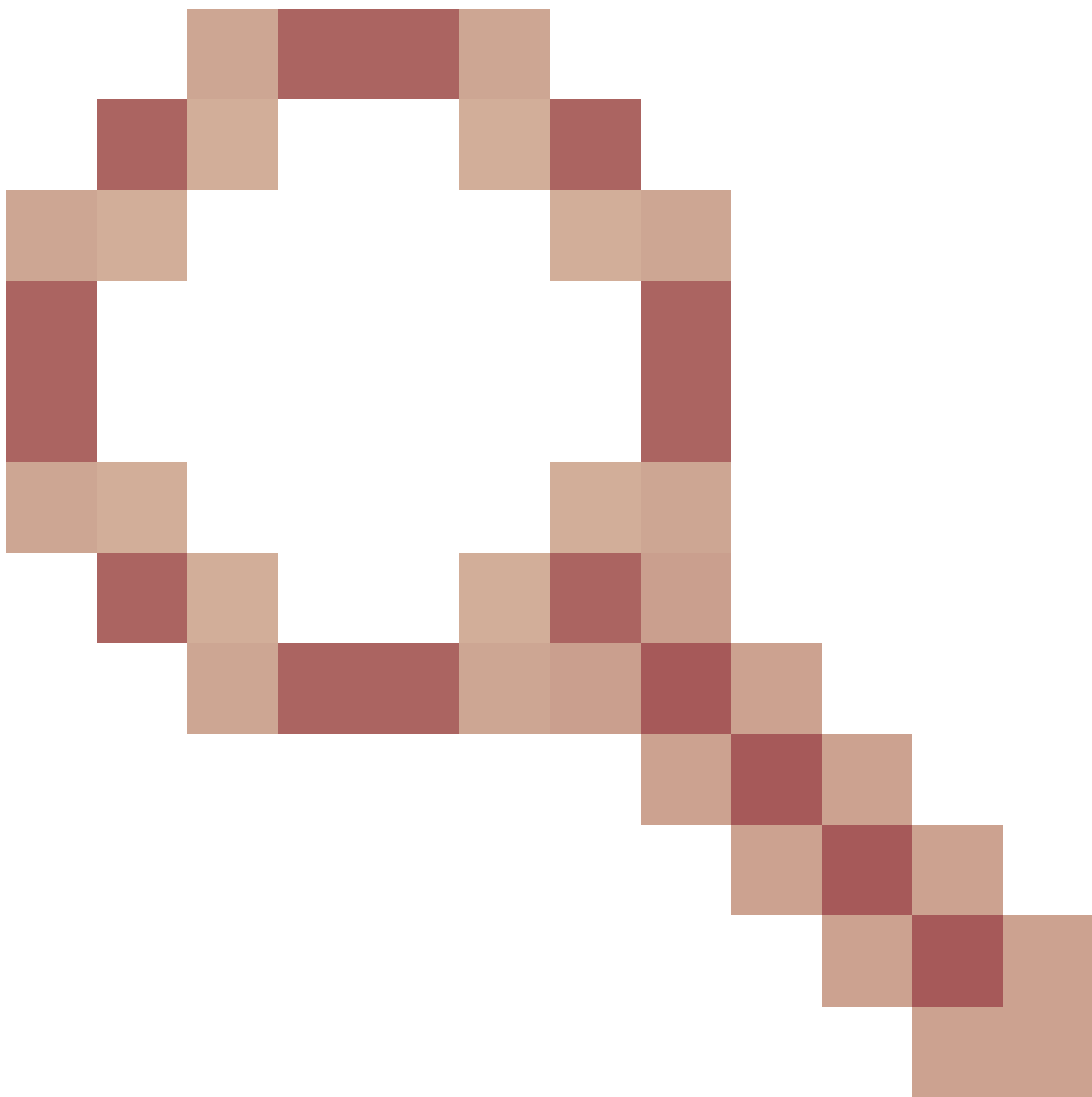
```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9.
```

### SNMPv3轮询注意事项

- 许可证：SNMPv3需要强加密许可证。确保您已在智能许可门户上启用导出受控功能
- 要排除故障，您可以尝试使用新用户/凭证
- 如果使用加密，则可以解密SNMPv3流量并检查负载，如中所述

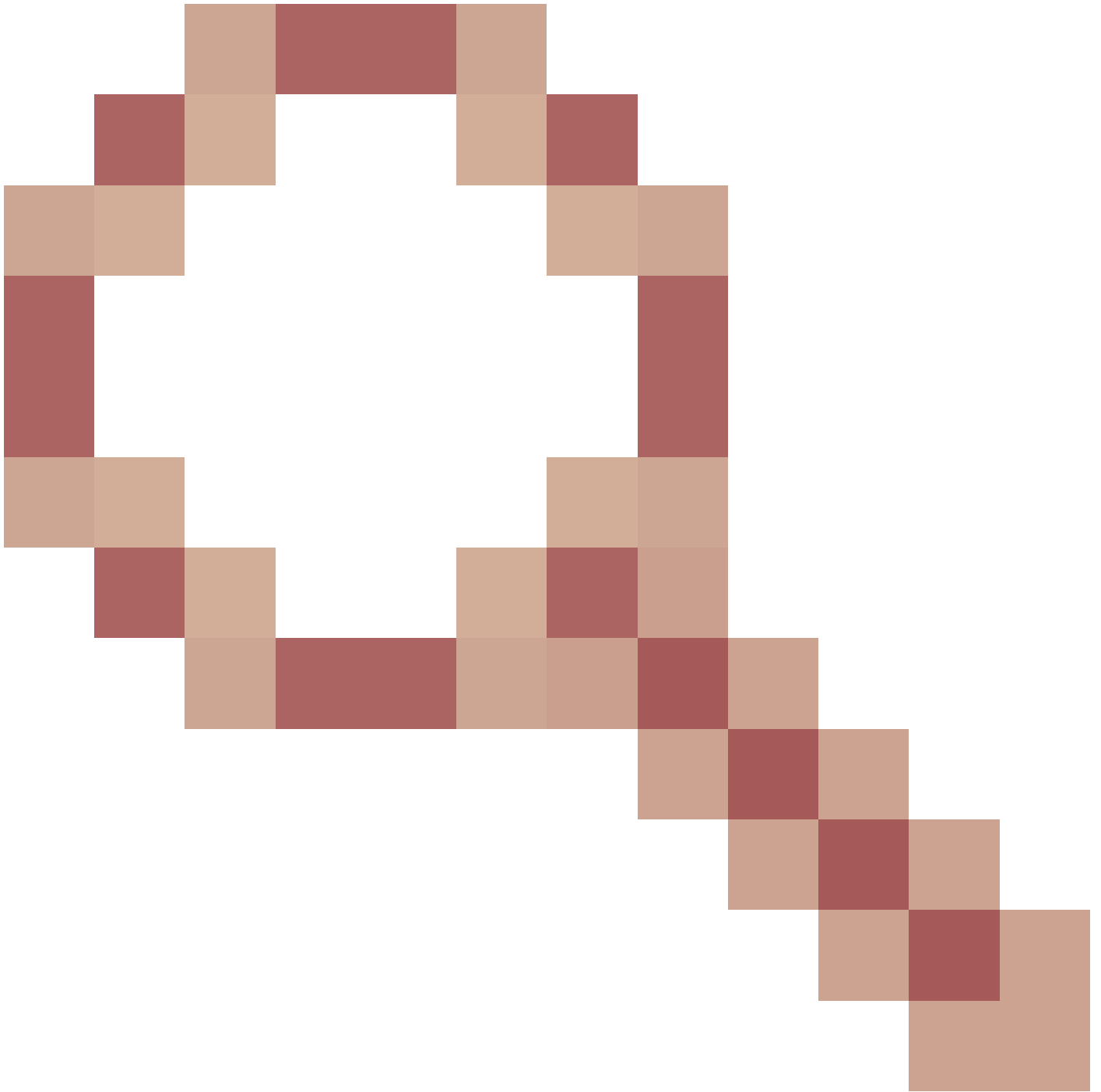
: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>

- 如果软件受到以下缺陷的影响，不妨考虑使用 AES128 进行加密：
- 思科漏洞ID [CSCvy27283](#)




使用隐私算法AES192/AES256时，ASA/FTD SNMPv3轮询可能会失败

Cisco Bug ID [CSCvx45604](#)



Snmpv3 walk fails on user with auth sha and priv aes 192

---

 注意：如果由于算法不匹配导致SNMPv3失败，则show输出和日志不会显示任何明显信息

---

```
firepower# show snmp-server statistics
6 SNMP packets input
 0 Bad SNMP version errors
 0 Unknown community name
 0 Illegal operation for community name supplied
 0 Encoding errors
 0 Number of requested variables
 0 Number of altered variables
 0 Get-request PDUs
 0 Get-next PDUs
 0 Get-bulk PDUs
 0 Set-request PDUs (Not supported)
0 SNMP packets output
 0 Too big errors (Maximum packet size 1500)
 0 No such name errors
 0 Bad values errors
 0 General errors
 0 Response PDUs
 0 Trap PDUs
```

Input packets increase, but no replies!

First recommended action:  
Verify your configuration 'show run snmp-server'

## SNMPv3 轮询注意事项 – 案例研究

### 1. SNMPv3 snmpwalk - 功能场景

<#root>

admin@FS2600-2:~\$

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x AES -X Cisco123 192.168.21.50
```

SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9  
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2315

在捕获 (snmpwalk) 中，您可查看各数据包的应答情况：

```
firepower# show capture SNMP
...
14: 23:44:44.156714      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 64
15: 23:44:44.157325      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 132
16: 23:44:44.160819      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 157
17: 23:44:44.162039      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 238
18: 23:44:44.162375      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 160
19: 23:44:44.197850      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 168
20: 23:44:44.198262      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 160
21: 23:44:44.237826      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 162
22: 23:44:44.238268      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 160
23: 23:44:44.277909      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 159
24: 23:44:44.278260      802.1Q vlan#201 P0 192.168.21.100.54240 > 192.168.21.50.161:  udp 160
25: 23:44:44.317869      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.54240:  udp 168
```

捕获文件未显示任何异常：

```

Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  <v> msgAuthoritativeEngineID: 80000009fec41e36a96147f184553b777
    1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
    Engine Enterprise ID: ciscoSystems (9)
    Engine ID Format: Reserved/Enterprise-specific (254)
    Engine ID Data: ca41e36a96147f184553b777a7127ccb3710888f
  msgAuthoritativeEngineBoots: 6
  msgAuthoritativeEngineTime: 5089
  msgUserName: Cisco123
  <v> msgAuthenticationParameters: 79ee0d463313558f4529954f
    <v> [Authentication: OK]
      <v> [Expert Info (Chat/Checksum): SNMP Authentication OK]
        [SNMP Authentication OK]
        [Severity level: Chat]
        [Group: Checksum]
      msgPrivacyParameters: 714e78d6bc292c88

```

## 2. SNMPv3 snmpwalk - 加密失败

提示#1：存在超时：

```
<#root>
```

```
admin@FS2600-2:~$
```

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x DES -X Cisco123 192.168.21.50
```

Timeout: No Response from 192.168.2.1

提示#2：存在许多请求和1个回复：

```

firepower# show capture SNMP
7 packets captured
  1: 23:25:06.248446      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161: udp 64
  2: 23:25:06.248613      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161: udp 64
  3: 23:25:06.249224      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.55137: udp 132
  4: 23:25:06.252992      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161: udp 163
  5: 23:25:07.254183      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161: udp 163
  6: 23:25:08.255388      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161: udp 163
  7: 23:25:09.256624      802.1Q vlan#201 P0 192.168.21.100.55137 > 192.168.21.50.161: udp 163

```

提示#3 : Wireshark解密失败 :

```
> User Datagram Protocol, Src Port: 35446, Dst Port: 161
  Simple Network Management Protocol
    msgVersion: snmpv3 (3)
    > msgGlobalData
    > msgAuthoritativeEngineID: 80000009feca41e36a96147f184553b777a7127ccb3710888f
    msgAuthoritativeEngineBoots: 6
    msgAuthoritativeEngineTime: 4359
    msgUserName: Cisco123
    > msgAuthenticationParameters: 1bc9daaa366647cbbb70c5d5
    msgPrivacyParameters: 0000000197eae1a
  > msgData: encryptedPDU (1)
    > encryptedPDU: 452ee7ef0b13594f8b0f6031213217477ecb2422d353581311cade539a27951af821524c...
      > Decrypted data not formatted as expected, wrong key?
        > [Expert Info (Warning/Malformed): Decrypted data not formatted as expected, wrong key?]
          [Decrypted data not formatted as expected, wrong key?]
          [Severity level: Warning]
          [Group: Malformed]
```

提示#4。检查ma\_ctx2000.log文件，查找“error parsing ScopedPDU”（分析ScopedPDU时出错）消息：

```
<#root>
```

```
> expert
admin@firepower:~$
```

```
tail -f /mnt/disk0/log/ma_ctx2000.log
```

```
security service 3 error parsing ScopedPDU
security service 3 error parsing ScopedPDU
security service 3 error parsing ScopedPDU
```

分析ScopedPDU时出错，强烈提示存在加密错误。ma\_ctx2000.log文件仅显示SNMPv3的事件！

### 3. SNMPv3 snmpwalk – 身份验证失败

提示#1：身份验证失败

```
<#root>
```

```
admin@FS2600-2:~$
```

```
snmpwalk -v 3 -u Cisco123 -l authPriv -a MD5 -A Cisco123 -x AES -X Cisco123 192.168.21.50
```

```
snmpwalk: Authentication failure (incorrect password, community or key)
```

提示#2：有许多请求和回复

```
firepower# show capture SNMP
4 packets captured
1: 23:25:28.468847      802.1Q vlan#201 P0 192.168.21.100.34348 > 192.168.21.50.161: udp 64
2: 23:25:28.469412      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.34348: udp 132
3: 23:25:28.474386      802.1Q vlan#201 P0 192.168.21.100.34348 > 192.168.21.50.161: udp 157
4: 23:25:28.475561      802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.34348: udp 137
```

提示#3 : Wireshark格式错误数据包

```
> Internet Protocol Version 4, Src: 192.168.21.100, Dst: 192.168.21.50
> User Datagram Protocol, Src Port: 47752, Dst Port: 161
> Simple Network Management Protocol
v [Malformed Packet: SNMP]
  v [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```

提示#4。检查ma\_ctx2000.log文件以查找“Authentication failed”消息：

```
<#root>
```

```
>
```

```
expert
```

```
admin@firepower:~$
```

```
tail -f /mnt/disk0/log/ma_ctx2000.log
```

```
Authentication failed for Cisco123
Authentication failed for Cisco123
```

## 无法轮询 FXOS SNMP

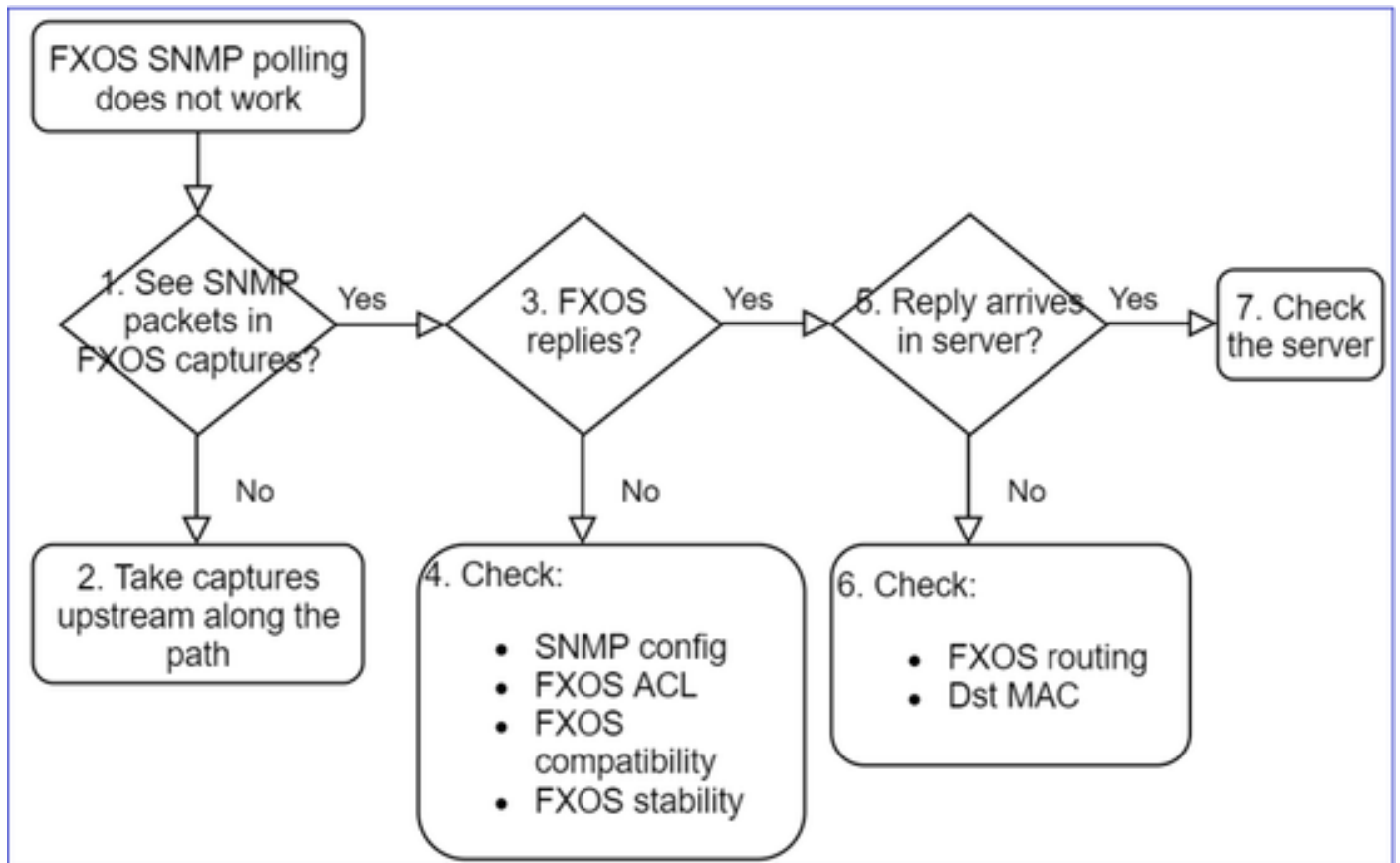
问题描述 ( Cisco TAC 真实案例示例 ) :

- “SNMP 提供的 FXOS 版本有误。使用 SNMP 轮询此版 FXOS 时，输出内容难以理解。”
- “无法在 FXOS FTD4115 上设置 SNMP 社区。”
- “在备用防火墙上将 FXOS 从 2.8 升级到 2.9 后，尝试通过 SNMP 接收信息时总会超时。”
- “snmpwalk 在 9300 FXOS 上失败，但在相同版本的 4140 FXOS 上却能正常工作。连通性和社区不是问题所在。”
- “我们想要在 FPR4K FXOS 上添加 25 台 SNMP 服务器，但无法添加。”

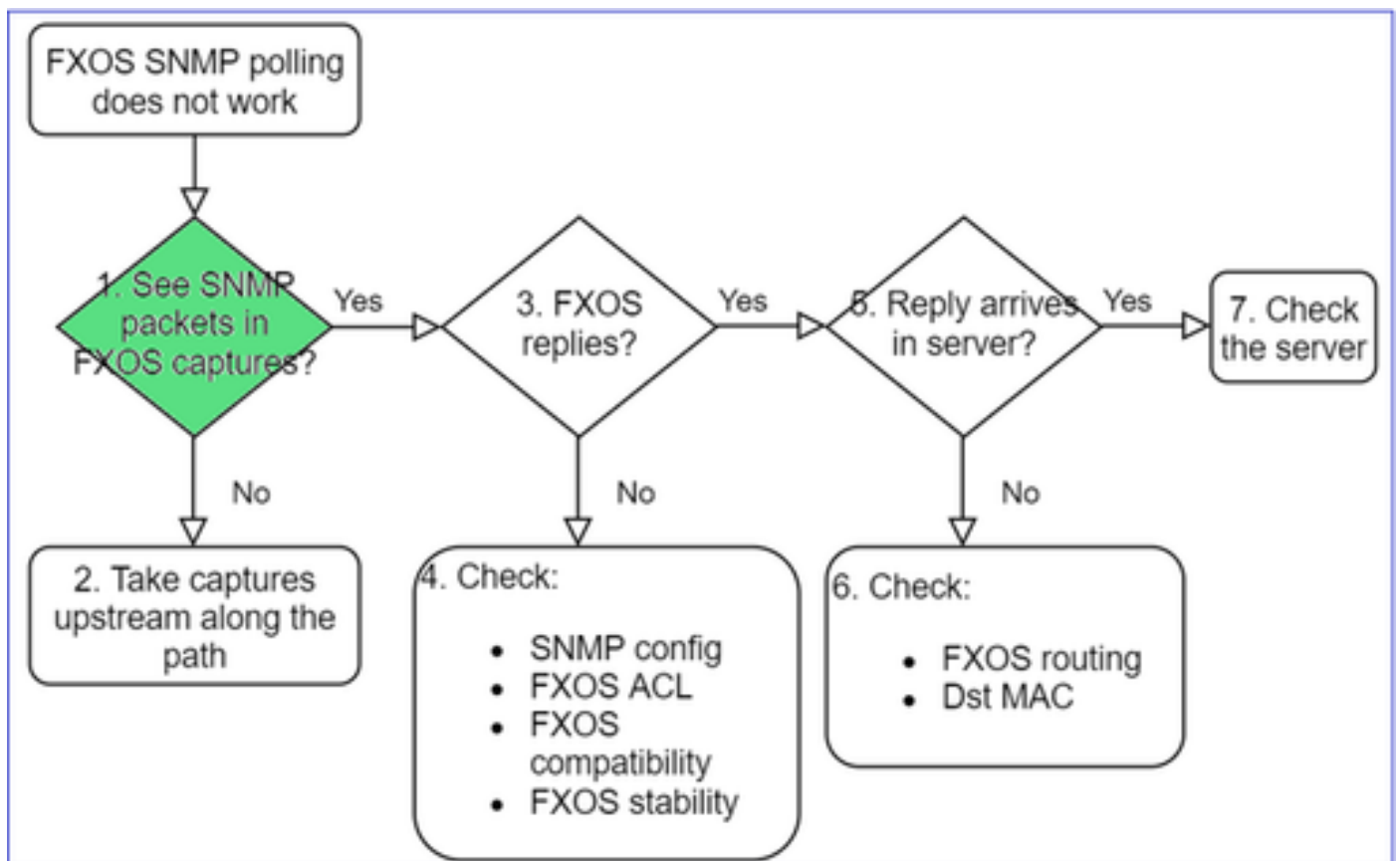
故障排除建议



以下是FXOS SNMP轮询问题的故障排除流程图：



1. 您是否在FXOS捕获中看到SNMP数据包？



## FPR1xxx/21xx

- 在FPR1xxx/21xx上没有机箱管理器（设备模式）。
- 您可以从管理接口轮询 FXOS 软件。

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management0
```

```
1 - Global
```

```
Selection?
```

```
0
```

```
Please specify tcpdump options desired.
```

```
(or enter '?' for a list of supported options)
```

```
Options:
```

```
-n host 192.0.2.100 and udp port 161
```

## 41xx/9300

- 在 Firepower 41xx/93xx 上，请使用 Ethalyzer CLI 工具进行机箱捕获：

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
firepower(fxos)#
```

```
ethalyzer local interface mgmt capture-filter "udp port 161" limit-captured-frames 50 write workspace
```

```
firepower(fxos)#
```

```
exit
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

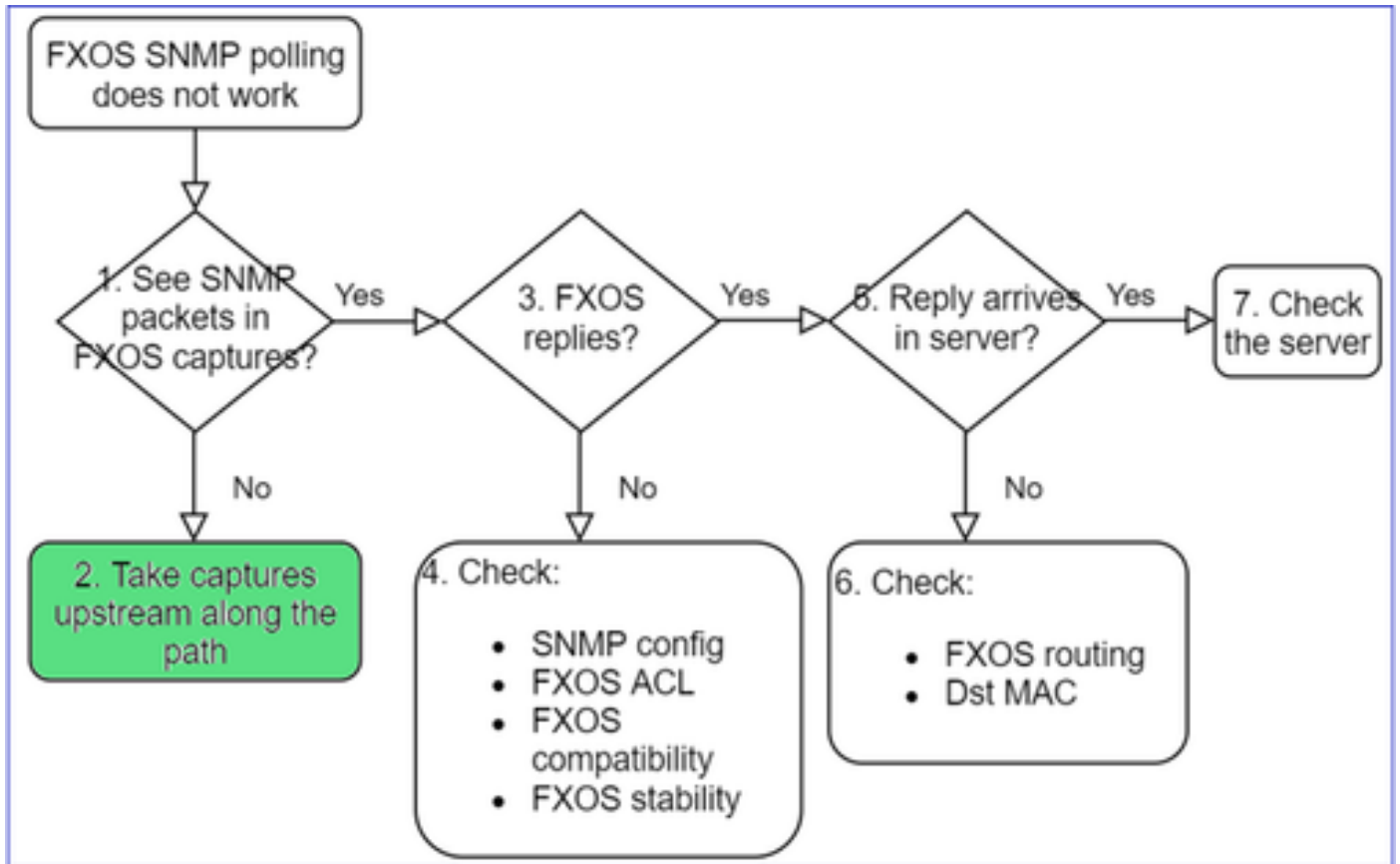
```
dir
```

11152 Jul 26 09:42:12 2021 SNMP.pcap

firepower(local-mgmt)#

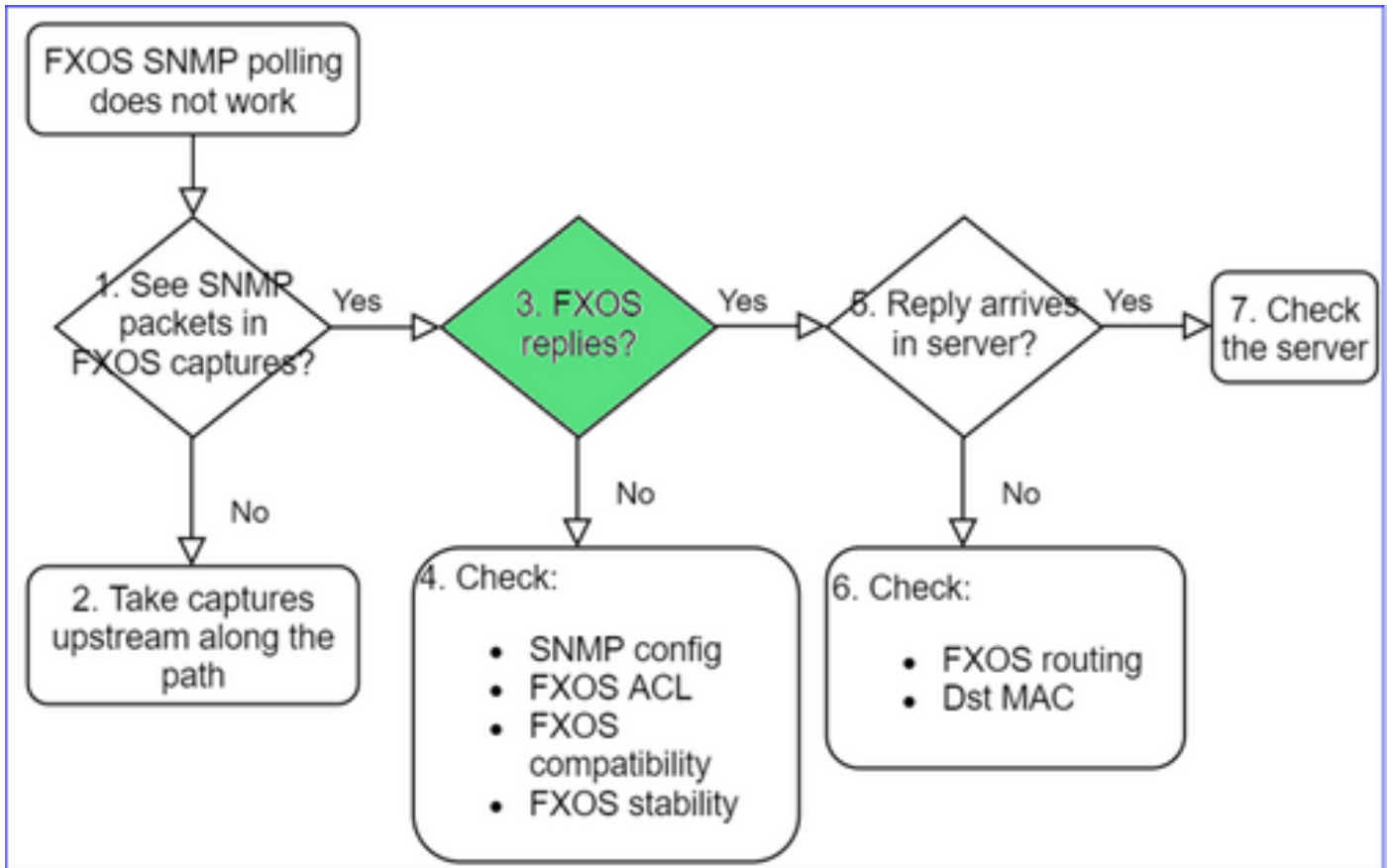
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap

## 2. FXOS捕获中没有数据包？



- 沿路径进行上游捕获

## 3. FXOS应答？



- 功能场景：

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS\_PACKET\_BUFFER\_SIZE is set to 4.

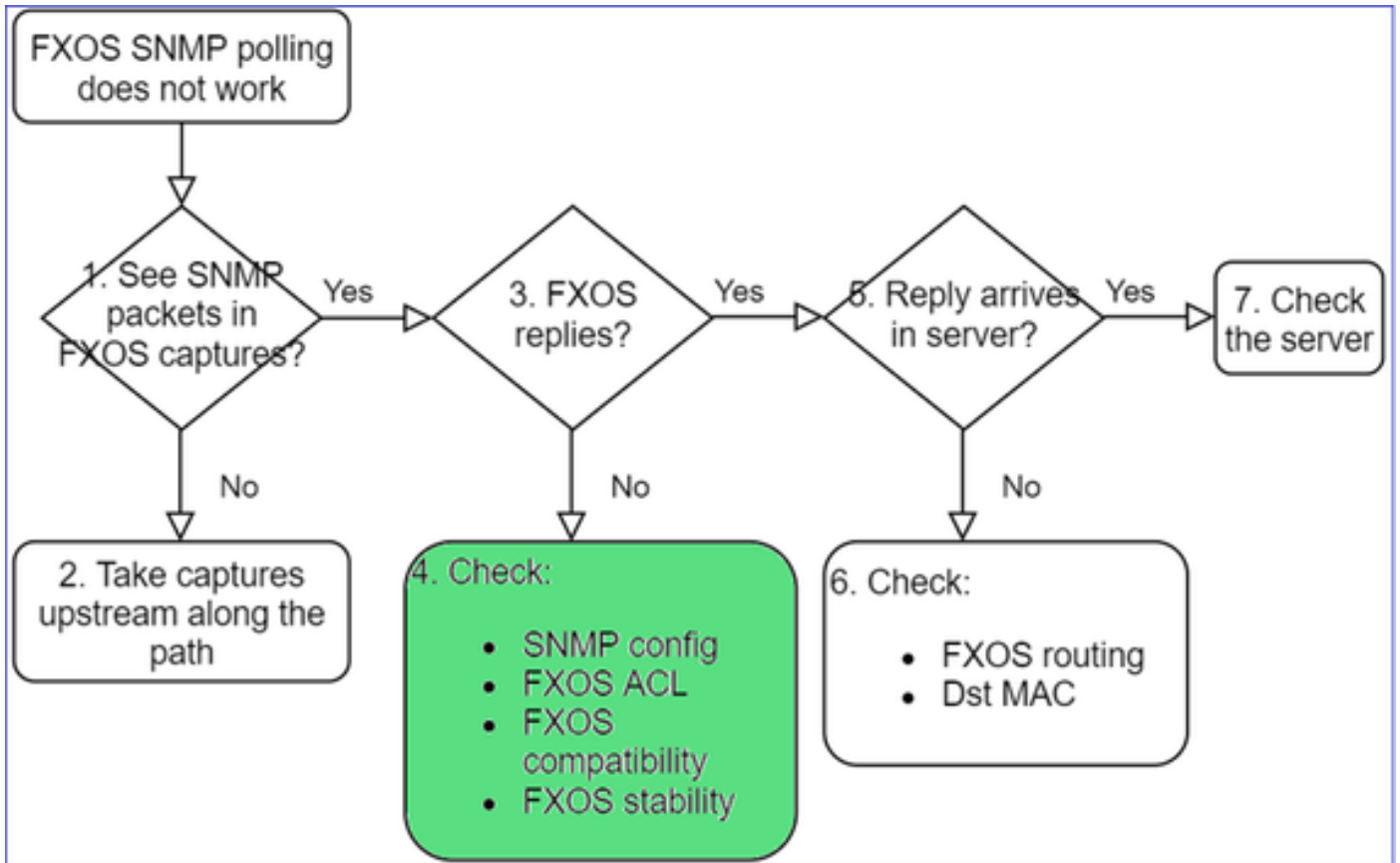
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on management0, link-type EN10MB (Ethernet), capture size 262144 bytes

08:17:25.952457 IP 192.168.2.23.36501 > 192.168.2.28.161: C="Cisco123" GetNextRequest(25) .10.3.1.1.2

08:17:25.952651 IP 192.168.2.28.161 > 192.168.2.23.36501: C="Cisco123" GetResponse(97) .1.10.1.1.1.1.

#### 4. FXOS 无应答



### 其他检查

- ( 通过 UI 或 CLI ) 验证 SNMP 配置 :

```
<#root>
```

```
firepower#
```

```
scope monitoring
```

```
firepower /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

- 请谨慎使用特殊字符 ( 例如 "\$" ) :

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

```
FP4145-1(fxos)#
show running-config snmp all
```

```
FP4145-1(fxos)#
show snmp community
```

Community	Group / Access	context	acl_filter
Cisco123	network-operator		

- 对于 SNMP v3，请使用 show snmp-user [detail]
- 验证 FXOS 兼容性

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id\\_59069](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id_59069)

#### 4. 如果FXOS未回复

验证 FXOS SNMP 计数器：

```
FP4145-1# connect fxos
FP4145-1(fxos)# show snmp
...
2243 SNMP packets input
  0 Bad SNMP versions
  28 Unknown community name
  0 Illegal operation for community name
supplied
  28 Encoding errors
  2214 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  2214 Get-next PDUs
  0 Set-request PDUs
3483 SNMP packets output
  0 Too big errors
  1296 Out Traps PDU
```

Diagram illustrating SNMP statistics and their corresponding labels:

- 2243 SNMP packets input → Total requests (polling)
- 28 Unknown community name → Bad community requests (v2c)
- 3483 SNMP packets output → Total replies
- 1296 Out Traps PDU → Traps generated

- 验证 FXOS 访问控制列表 (ACL)。这仅适用于 FPR41xx/9300 平台。

如果流量被FXOS ACL阻止，您将看到请求，但不会看到任何回复：

```
<#root>
```

```
firepower(fxos)#
```

```
ethalyzer local interface mgmt capture-filter
```

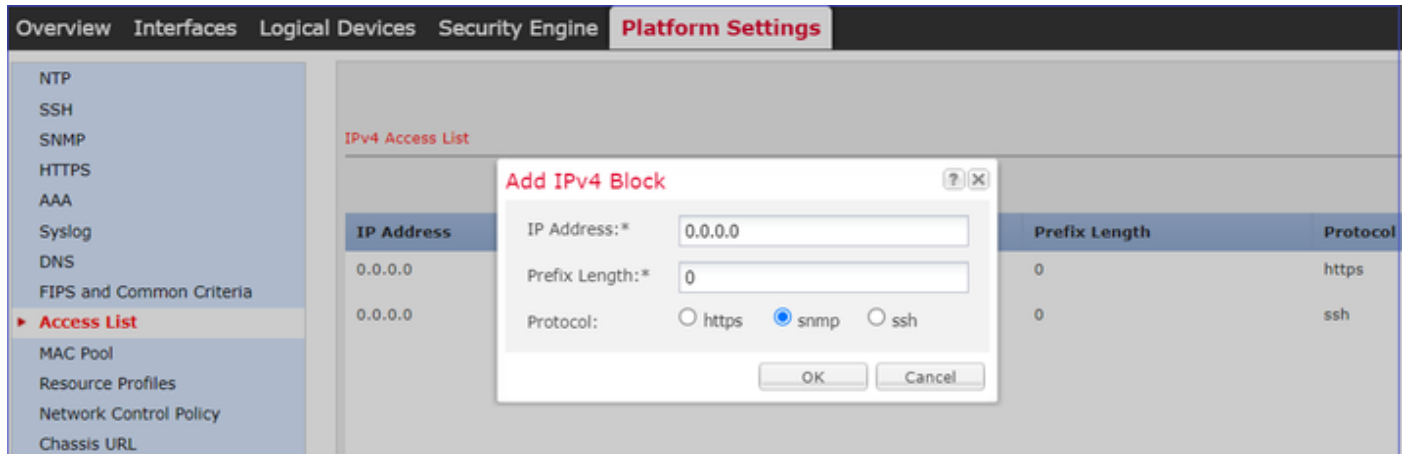
```
"udp port 161" limit-captured-frames 50 write workspace:///SNMP.pcap
Capturing on 'eth0'
```

```

1 2021-07-26 11:56:53.376536964 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1
2 2021-07-26 11:56:54.377572596 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.10.1.10.1.1
3 2021-07-26 11:56:55.378602241 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1

```

您可以通过用户界面 (UI) 验证 FXOS ACL :



您也可以通过 CLI 验证 FXOS ACL :

```

<#root>
firepower#
scope system

firepower /system #
scope services

firepower /system/services #
show ip-block detail

```

```

Permitted IP Block:
  IP Address: 0.0.0.0
  Prefix Length: 0
  Protocol: snmp

```

- 调试 SNMP ( 仅限数据包 ) 。仅适用于 FPR41xx/9300 :

```

<#root>
FP4145-1#
connect fxos

FP4145-1(fxos)#

```

```
terminal monitor
```

```
FP4145-1(fxos)#
```

```
debug snmp pkt-dump
```

```
2021 Aug 4 09:51:24.963619 snmpd: SNMPPKTSTRT: 1.000000 161 495192988.000000 0.000000 0.000000 0.000000
```

- Debug SNMP (all) -此调试输出非常详细。

```
<#root>
```

```
FP4145-1(fxos)#
```

```
debug snmp all
```

```
2021 Aug 4 09:52:19.909032 snmpd: SDWRAP message Successfully processed
```

```
2021 Aug 4 09:52:21.741747 snmpd: Sending it to SDB-Dispatch
```

```
2021 Aug 4 09:52:21.741756 snmpd: Sdb-dispatch did not process
```

- 验证是否存在与 SNMP 相关的 FXOS 故障：

```
<#root>
```

```
FXOS#
```

```
show fault
```

```
Severity Code Last Transition Time ID Description
```

```
-----  
Warning F78672 2020-04-01T21:48:55.182 1451792 [FSM:STAGE:REMOTE-ERROR]: Result: resource-unavailable C
```

- 验证是否存在 snmpd 核心：

```
FPR41xx/FPR9300 上：
```

```
<#root>
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

```
dir cores
```

```
1 1983847 Apr 01 17:26:40 2021 core.snmpd.10012.1585762000.gz
```



FPR1xxx/21xx 上：

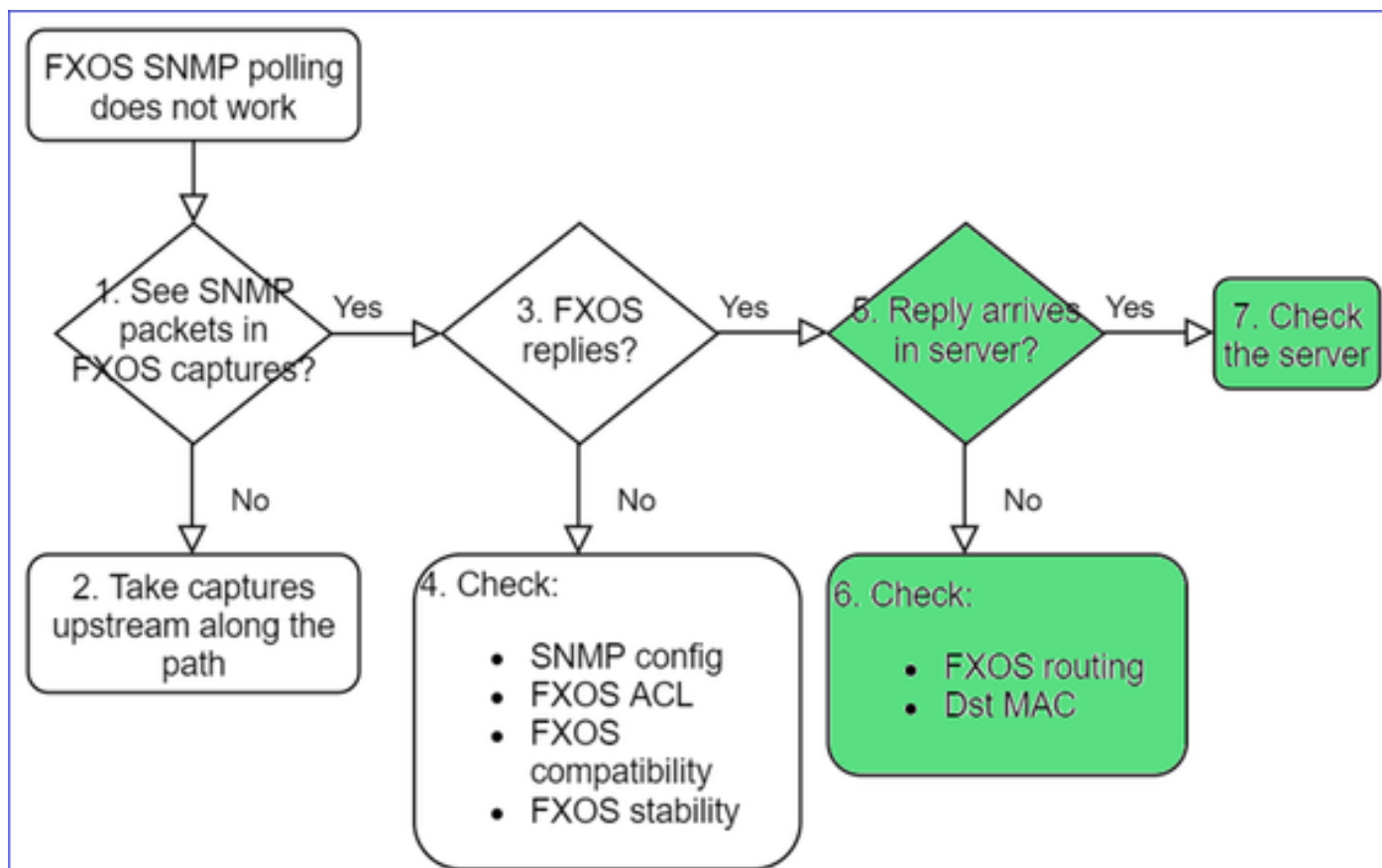
```
<#root>
```

```
firepower(local-mgmt)#
```

```
dir cores_fxos
```

如果发现 snmpd 核心，请收集这些核心以及 FXOS 故障排除捆绑包，并联系 Cisco TAC。

### 5. SNMP应答是否到达SNMP服务器？



- 检查 FXOS 路由

此输出结果来自 FPR41xx/9300：

```
<#root>
```

```
firepower#
```

```
show fabric-interconnect
```

Fabric Interconnect:

ID	OOB IP Addr	OOB Gateway	OOB Netmask	OOB IPv6 Address	OOB IPv6 Gateway	Prefix	Operable
A	192.168.2.37	192.168.2.1	10.255.255.128 ::	::		64	Operable

- 捕获、导出数据包捕获并检查应答的目的 MAC
- 最后，检查 SNMP 服务器（捕获、配置、应用等）

## 需要使用哪些 SNMP OID 值？

问题描述（Cisco TAC 真实案例示例）：

- “我们想要监控 Cisco Firepower 设备。请为每个核心 CPU、内存、磁盘提供 SNMP OID”
- “是否有 OID 可用于监控 ASA 5555 设备的电源状态？”
- “我们想要获取 FPR 2K 和 FPR 4K 的机箱 SNMP OID。”
- “我们想要轮询 ASA ARP 缓存。”
- “我们需要了解可用于 BGP 对等体故障的 SNMP OID。”

如何查找 SNMP OID 值

有关 Firepower 设备上 SNMP OID 的信息，请参阅下列文档：

- 《Cisco Firepower Threat Defense (FTD) SNMP 监控白皮书》：

<https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/white-paper-c11-741739.html>

- 《Cisco Firepower 4100/9300 FXOS MIB 参考指南》：

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b\\_FXOS\\_4100\\_9300\\_MIBRef.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b_FXOS_4100_9300_MIBRef.html)

- 如何在 FXOS 平台上搜索特定 OID：

<https://www.cisco.com/c/en/us/support/docs/security/firepower-9000-series/214337-how-to-look-for-an-specific-oid-on-fxos.html>

- 通过 CLI (ASA/LINA) 检查 SNMP OID

```
<#root>
```

```
firepower#
```

```
show snmp-server ?
```

```
engineID    Show snmp engineID
group       Show snmp groups
host        Show snmp host's
statistics  Show snmp-server statistics
user        Show snmp users
```

```
firepower#
```

```
show snmp-server oid
```

```
<- hidden option!  
[1] .1.10.1.1.10.1.2.1 IF-MIB::ifNumber  
[2] .1.10.1.1.1.10.2.2.1.1 IF-MIB::ifIndex  
[3] .1.10.1.1.1.10.2.2.1.2 IF-MIB::ifDescr  
[4] .1.10.1.1.1.10.2.2.1.3 IF-MIB::ifType
```

- 有关 OID 的详细信息，请参阅 SNMP Object Navigator

<https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en>

- 在 FXOS (41xx/9300) 上，通过 FXOS CLI 运行以下 2 个命令：

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

```
FP4145-1(fxos)#
```

```
show snmp internal oids supported create
```

```
FP4145-1(fxos)#
```

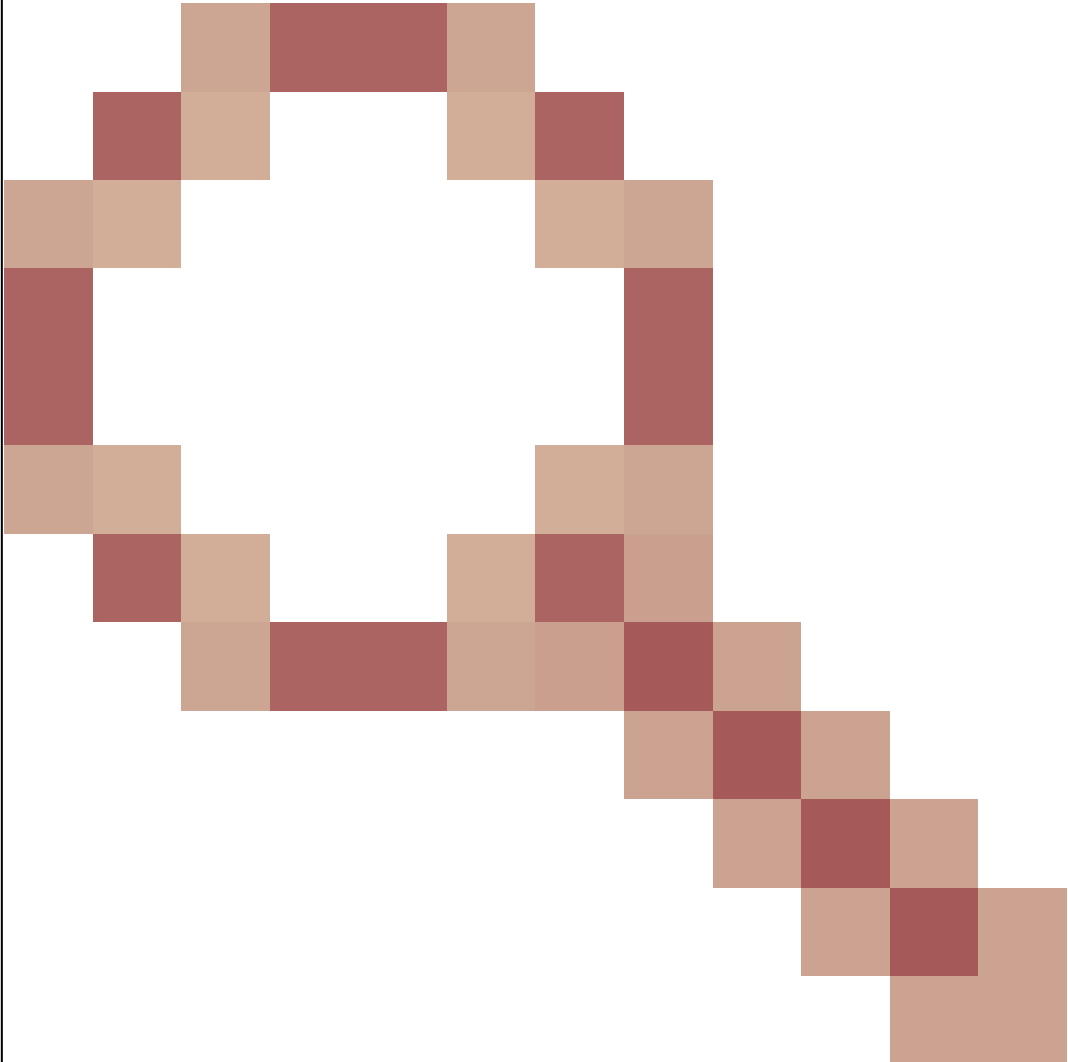
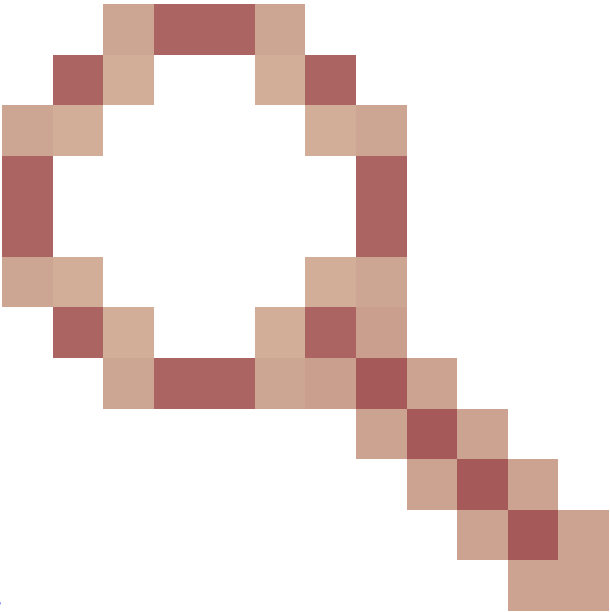
```
show snmp internal oids supported
```

```
- SNMP All supported MIB OIDs -0x11a72920  
Subtrees for Context:  
ccitt  
1  
1.0.88010.1.1.1.1.1.1.1 ieee8021paeMIB  
1.0.88010.1.1.1.1.1.1.2  
...
```

## 常见 OID 快速参考

要求	OID
CPU (LINA)	1.3.6.1.4.1.9.9.109.1.1.1
CPU (Snort)	1.3.6.1.4.1.9.9.109.1.1.1 (FP >= 6.7)
内存 (LINA)	1.3.6.1.4.1.9.9.221.1.1

内存 (Linux/FMC)	1.3.6.1.1.4.1.2021.4
HA 信息	1.3.6.1.4.1.9.9.491.1.4.2
集群信息	1.3.6.1.4.1.9.9.491.1.8.1
VPN 信息	RA-VPN会话数 : 1.3.6.1.4.1.9.9.392.1.3.1 (7.x) RA-VPN用户数 : 1.3.6.1.4.1.9.9.392.1.3.3 (7.x) RA-VPN峰值会话数 : 1.3.6.1.4.1.9.9.392.1.3.41 (7.x) S2S VPN会话数 : 1.3.6.1.4.1.9.9.392.1.3.29 S2S VPN峰值会话数 : 1.3.6.1.4.1.9.9.392.1.3.31 - 提示 : firepower# show snmp-server oid   我喜欢
BGP 状态	 增强型思科漏洞ID <a href="#">CSCux13512</a> : 为SNMP轮询添加BGP MIB
FPR1K/2K ASA/ASA v 智能许可	增强型思科漏洞ID <a href="#">CSCvv83590</a>

	 <p data-bbox="405 1205 1366 1240">: FPR1k/2k上的ASAv/ASA : 需要SNMP OID来跟踪智能许可的状态</p>
<p data-bbox="97 1581 368 1697">用于 FXOS 级别端口通道的 LINA SNMP OID</p>	 <p data-bbox="395 1886 1161 1966">增强型思科漏洞ID <a href="#">CSCvu91544</a> : 支持Lina SNMP OID进行FXOS级端口信道接口统计</p>

要求	OID
风扇状态陷阱	陷阱OID : 1.3.6.1.4.1.9.9.117.2.0.6 值OID : 1.3.6.1.4.1.9.9.117.1.4.1.1.1.<index> 0 -风扇未运行 1 -风扇正在运行
CPU/PSU温度陷阱	陷阱OID : 1.3.6.1.4.1.9.9.91.2.0.1 阈值OID : 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<index>.1 值OID : 1.3.6.1.4.1.9.9.91.1.1.1.1.4.<index>
PSU状态陷阱	陷阱OID : 1.3.6.1.4.1.9.9.117.2.0.2 OperStatus OID : 1.3.6.1.4.1.9.9.117.1.1.2.1.2.<index> AdminStatus OID : 1.3.6.1.4.1.9.9.117.1.1.2.1.1.<index> 0 -未检测到电源 1 -检测到电源存在 , 正常

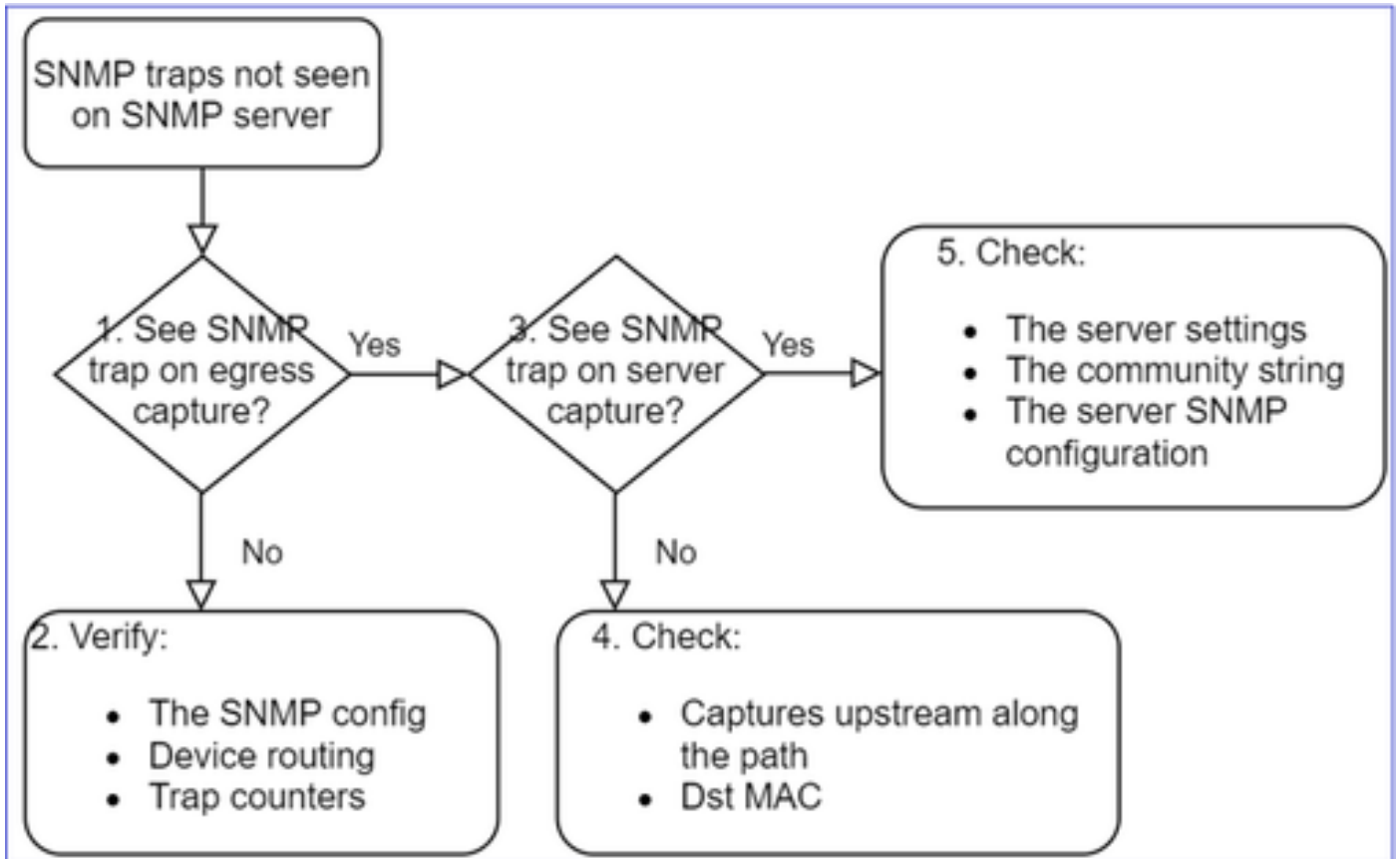
## 无法获取 SNMP 陷阱

问题描述 ( Cisco TAC 真实案例示例 ) :

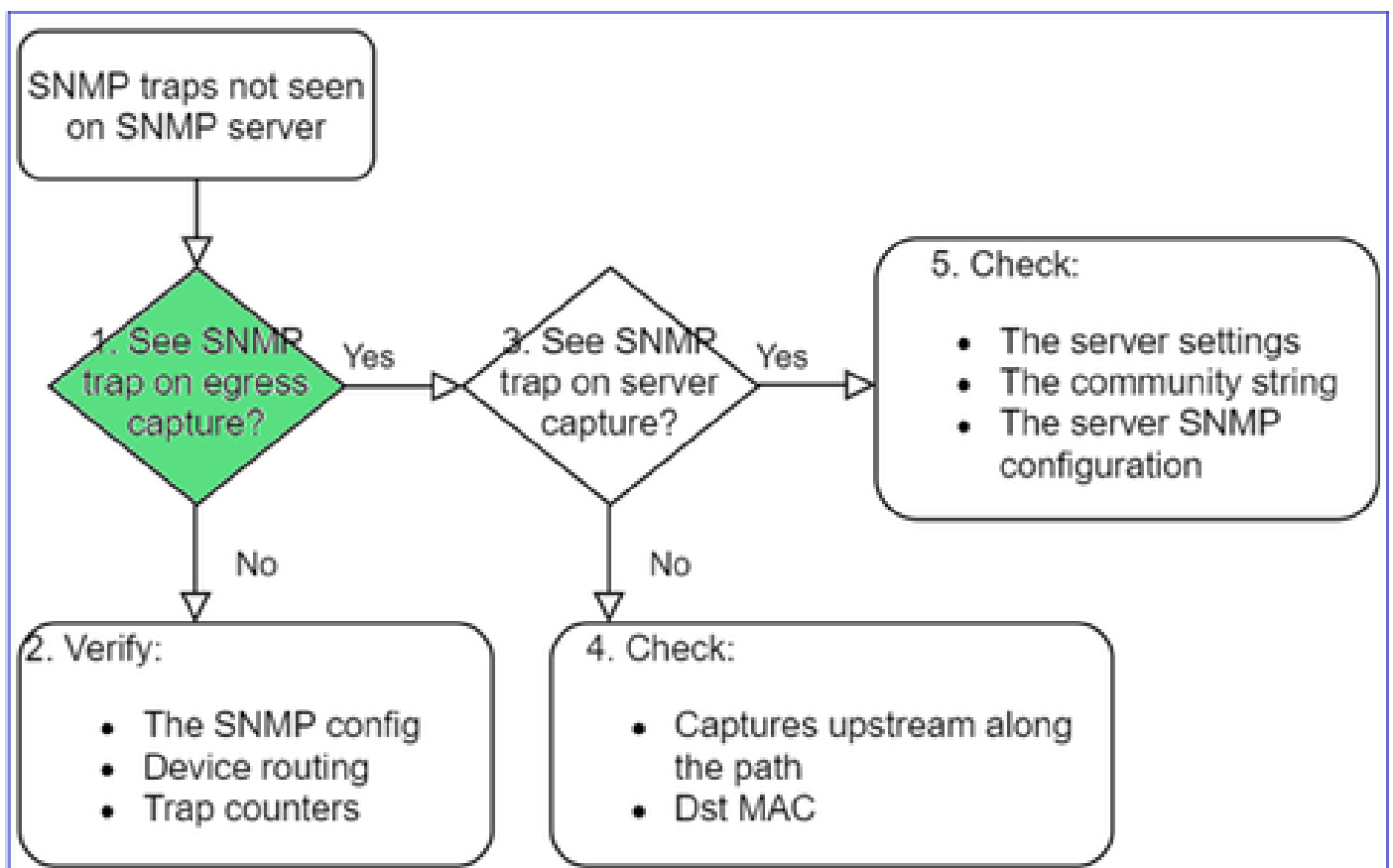
- “FTD 的 SNMPv3 不会向 SNMP 服务器发送任何陷阱。”
- “FMC 和 FTD 不发送 SNMP 陷阱消息。”
- “我们已在 FTD 4100 上为 FXOS 配置 SNMP , 并尝试使用 SNMPv3 和 SNMPv2 , 但两者均无法发送陷阱。”
- “Firepower SNMP 不向监控工具发送陷阱。”
- “防火墙 FTD 不向 NMS 发送 SNMP 陷阱。”
- “SNMP 服务器陷阱不正常工作。”
- “我们已在 FTD 4100 上为 FXOS 配置 SNMP , 并尝试使用 SNMPv3 和 SNMPv2 , 但两者均无法发送陷阱。”

## 故障排除建议

以下是Firepower SNMP陷阱问题的故障排除流程图 :



1. 您是否看到出口捕获上的SNMP陷阱？



捕获管理接口上的 LINA/ASA 陷阱：

```
<#root>
```

```
>
```

```
capture-traffic
```

```
Please choose domain to capture traffic from:
```

```
0 - management0
```

```
1 - Global
```

```
Selection?
```

```
0
```

```
Options:
```

```
-n host 192.168.2.100 and udp port 162
```

捕获数据接口上的 LINA/ASA 陷阱：

```
<#root>
```

```
firepower#
```

```
capture SNMP interface net208 match udp any any eq 162
```

捕获 FXOS 陷阱 (41xx/9300)：

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
firepower(fxos)#
```

```
ethalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 500 write workspace
```

```
1 2021-08-02 11:22:23.661436002 10.62.184.9 → 10.62.184.23 SNMP 160 snmpV2-trap 10.3.1.1.2.1.1.3.0 10.3.1.1.1.3.0
```

```
firepower(fxos)#
```

```
exit
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

```
dir
```

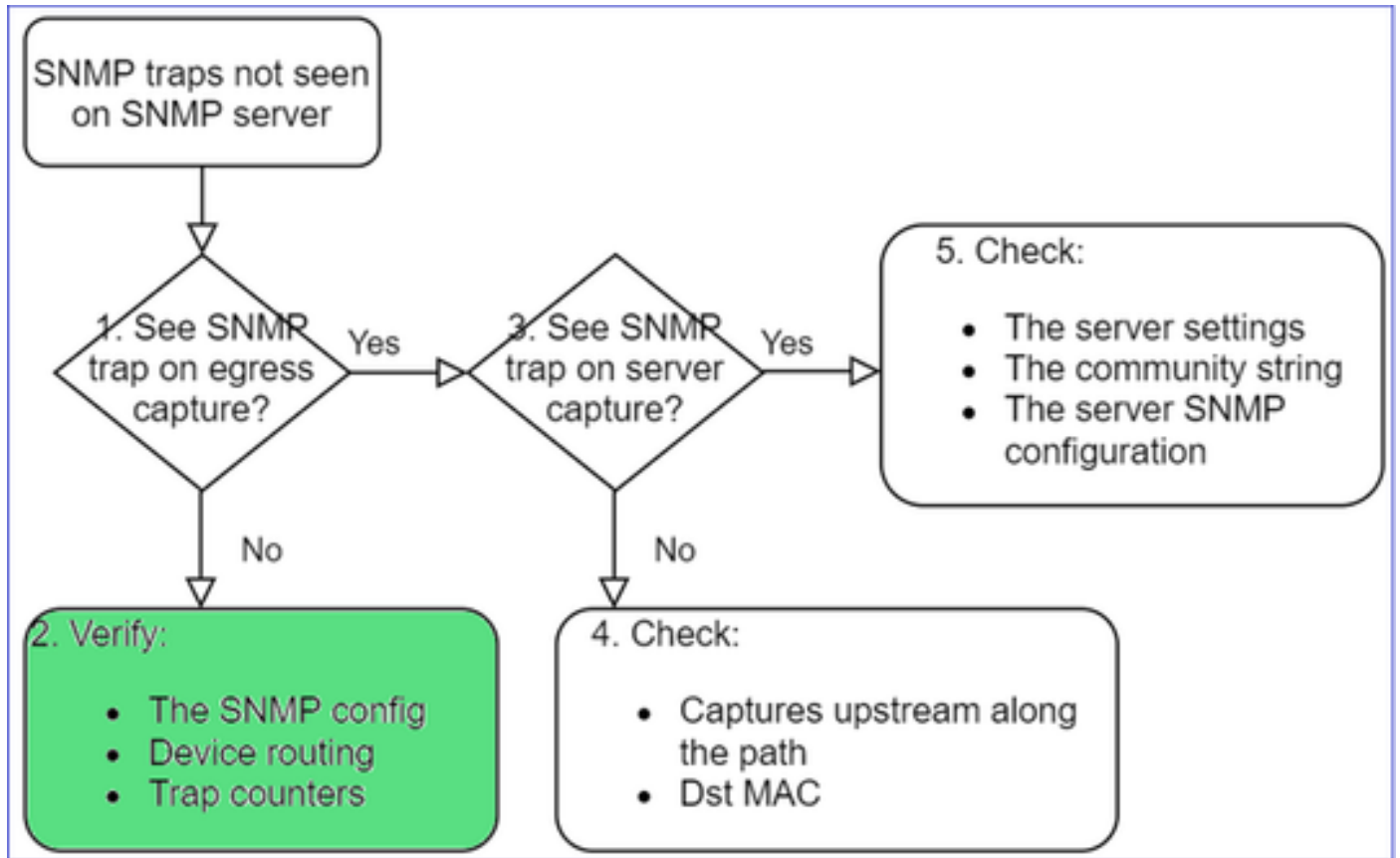
```
1 11134 Aug 2 11:25:15 2021 SNMP.pcap
```

```
firepower(local-mgmt)#
```



copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap

## 2. 如果在出口接口上未看到数据包



<#root>

firepower#

```
show run all snmp-server
```

```
snmp-server host ngfw-management 10.62.184.23 version 3 Cisco123 udp-port 162
snmp-server host net208 192.168.208.100 community ***** version 2c udp-port 162
snmp-server enable traps failover-state
```

## FXOS SNMP 陷阱配置：

<#root>

FP4145-1#

```
scope monitoring
```

FP4145-1 /monitoring #

```
show snmp-trap
```

SNMP Trap:

SNMP Trap	Port	Community	Version	V3 Privilege	Notification Type
192.168.2.100	162	****	V2c	Noauth	Traps

注意：在1xxx/21xx上，只有在Devices > Device Management > SNMP config ! 的情况下才看到这些设置。

- 用于通过管理接口的陷阱的 LINA/ASA 路由：

```
<#root>
```

```
>
```

```
show network
```

- 用于通过数据接口的陷阱的 LINA/ASA 路由：

```
<#root>
```

```
firepower#
```

```
show route
```

- FXOS 路由 (41xx/9300)：

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- 陷阱计数器 (LINA/ASA)：

```
<#root>
```

```
firepower#
```

```
show snmp-server statistics | i Trap
```

```
20 Trap PDUs
```

FXOS :

```
<#root>
```

```
FP4145-1#
```

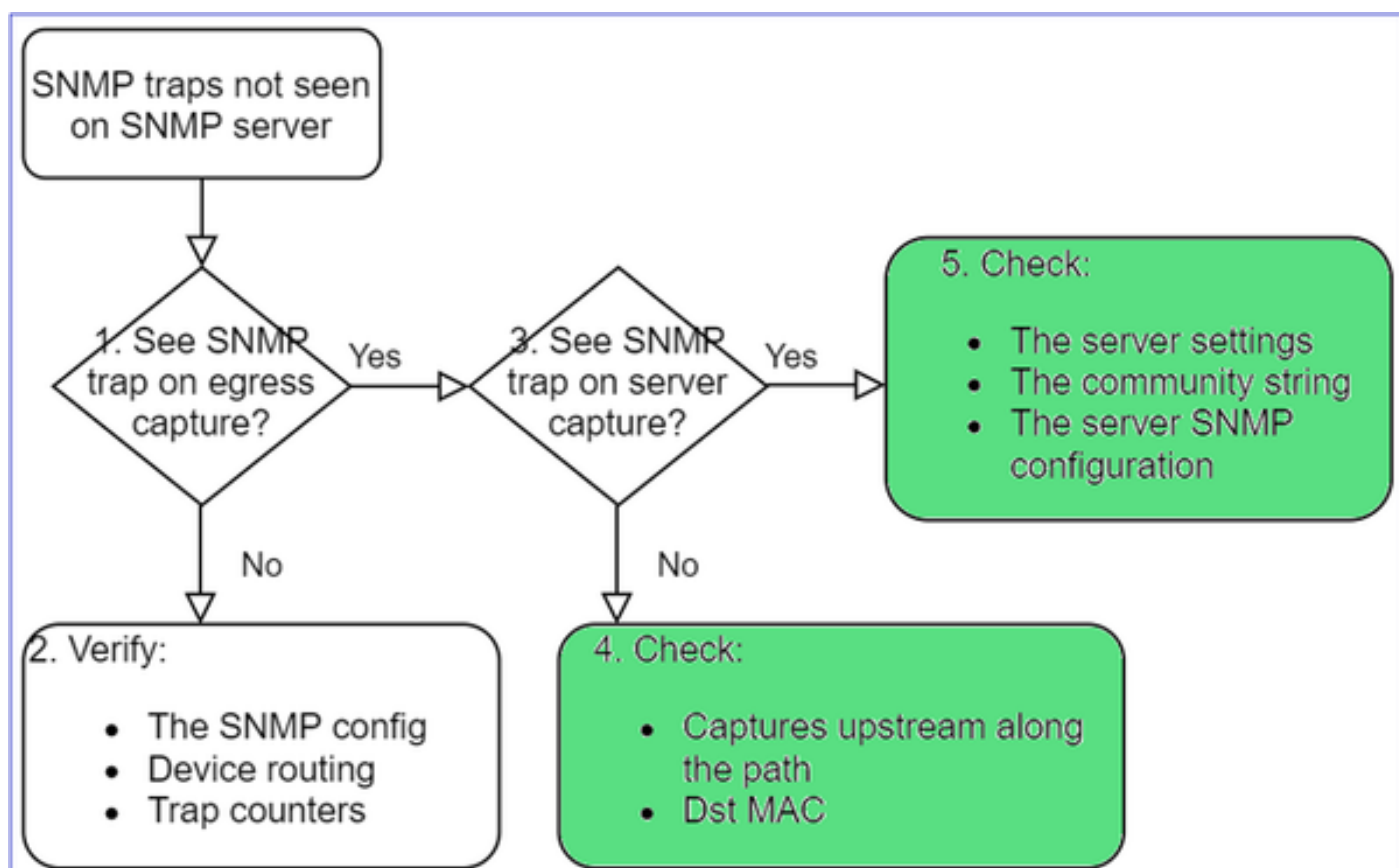
```
connect fxos
```

```
FP4145-1(fxos)#
```

```
show snmp | grep Trap
```

```
1296 Out Traps PDU
```

### 其他检查



- 在目的 SNMP 服务器上进行捕获.

其他需要检查的事项：

- 沿路径捕获.
- SNMP 陷阱数据包的目的 MAC 地址.
- SNMP 服务器设置和状态（例如，防火墙、开放端口等）。
- SNMP 社区字符串.
- SNMP 服务器配置.

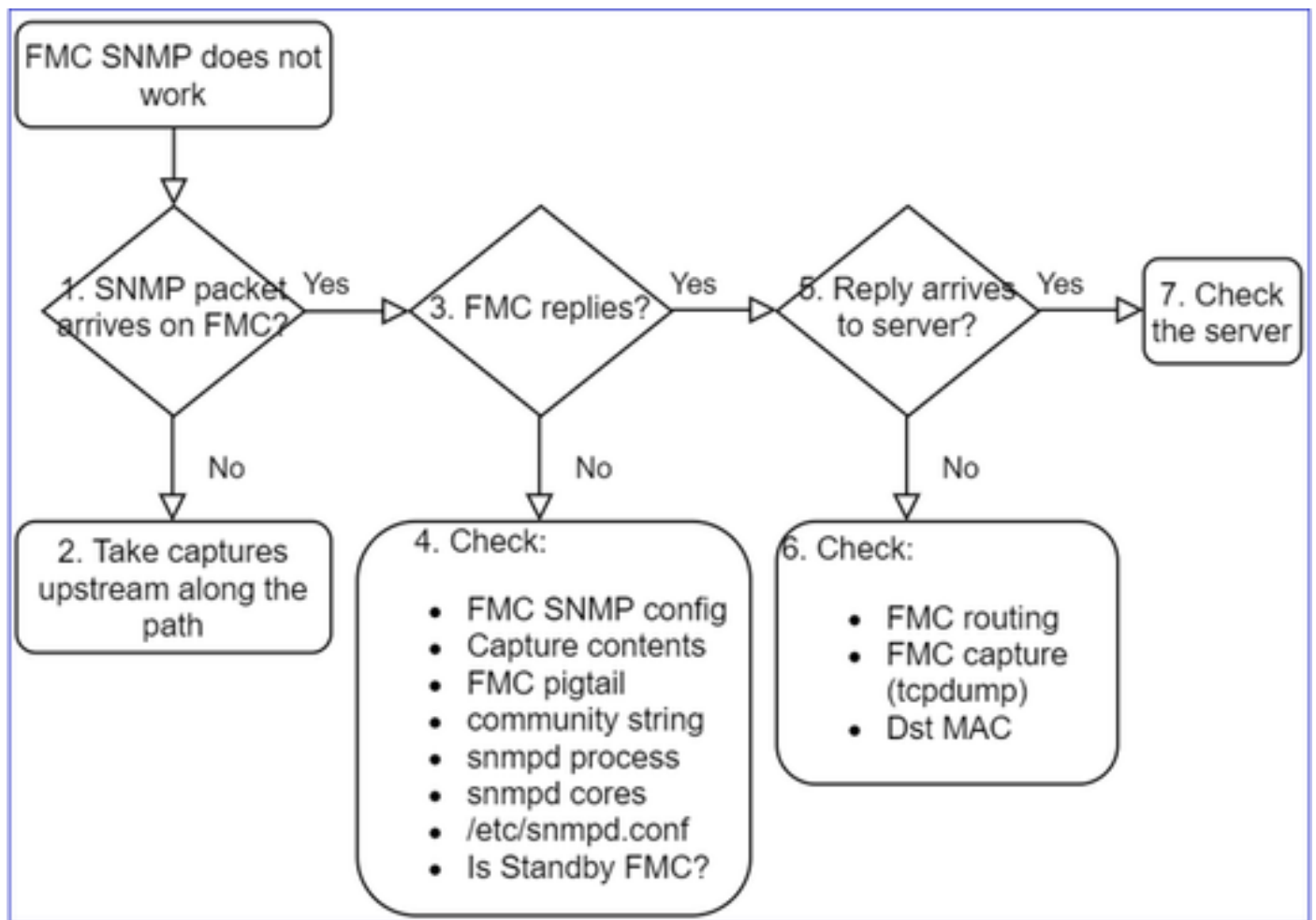
## 无法通过 SNMP 监控 FMC

问题描述 ( Cisco TAC 真实案例示例 ) :

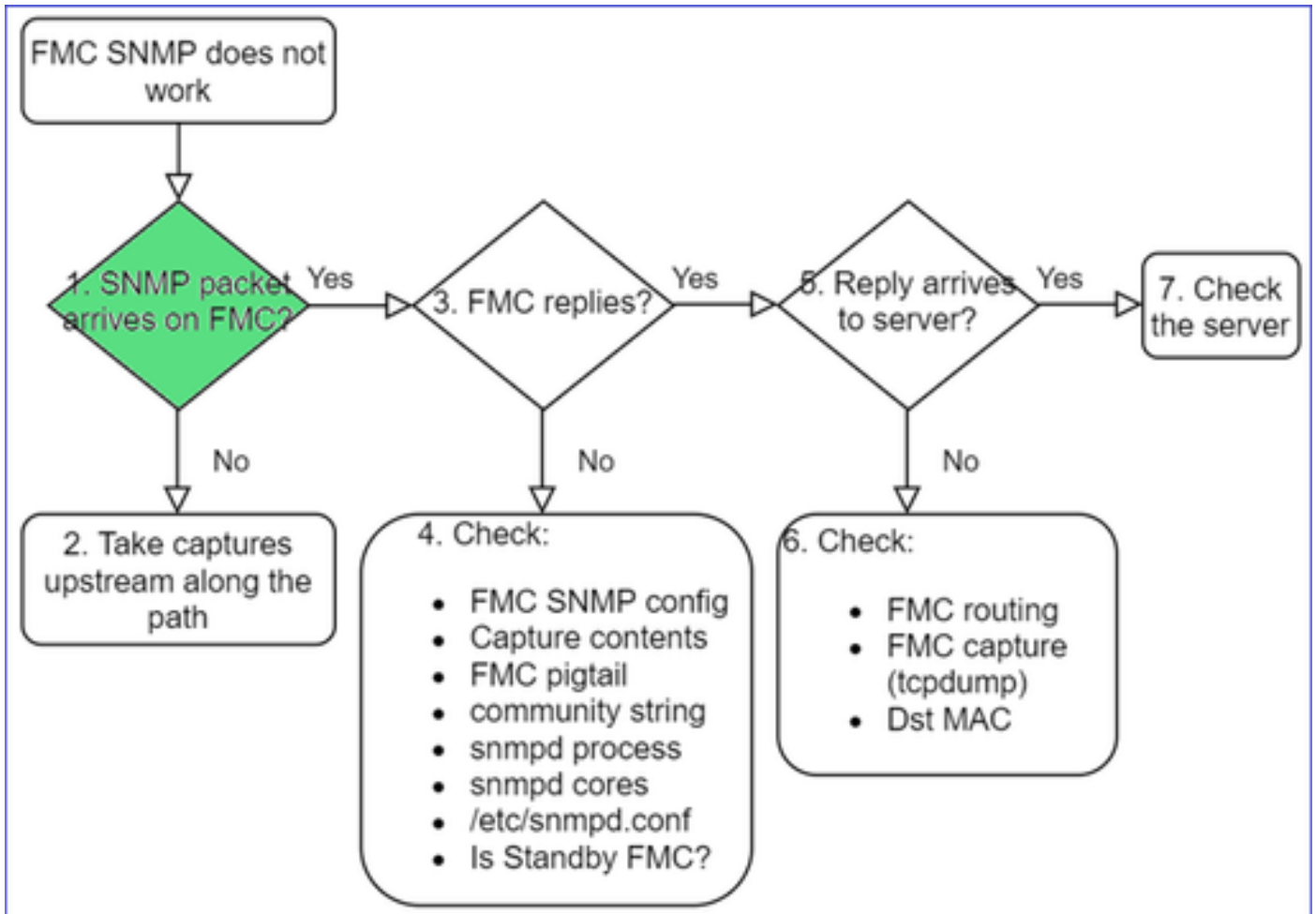
- “SNMP 在备用 FMC 上不正常工作。”
- “需要监控 FMC 内存。”
- “SNMP 是否应该在备用 192.168.4.0.8 FMC 上也能正常工作？”
- “我们必须配置FMC以监控它们的资源，如CPU、内存等。”

如何排除故障

以下是FMC SNMP问题故障排除流程图：



1. SNMP 数据包是否到达 FMC ?



- FMC 管理接口上的捕获：

<#root>

```
admin@FS2600-2:~$
```

```
sudo tcpdump -i eth0 udp port 161 -n
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
10:58:45.961836 IP 192.168.2.10.57076 > 192.168.2.23.161: C="Cisco123" GetNextRequest(28) .10.3.1.1.4
```



提示：将捕获保存在FMC /var/common/目录下，然后从FMC UI进行下载

<#root>

```
admin@FS2600-2:~$
```

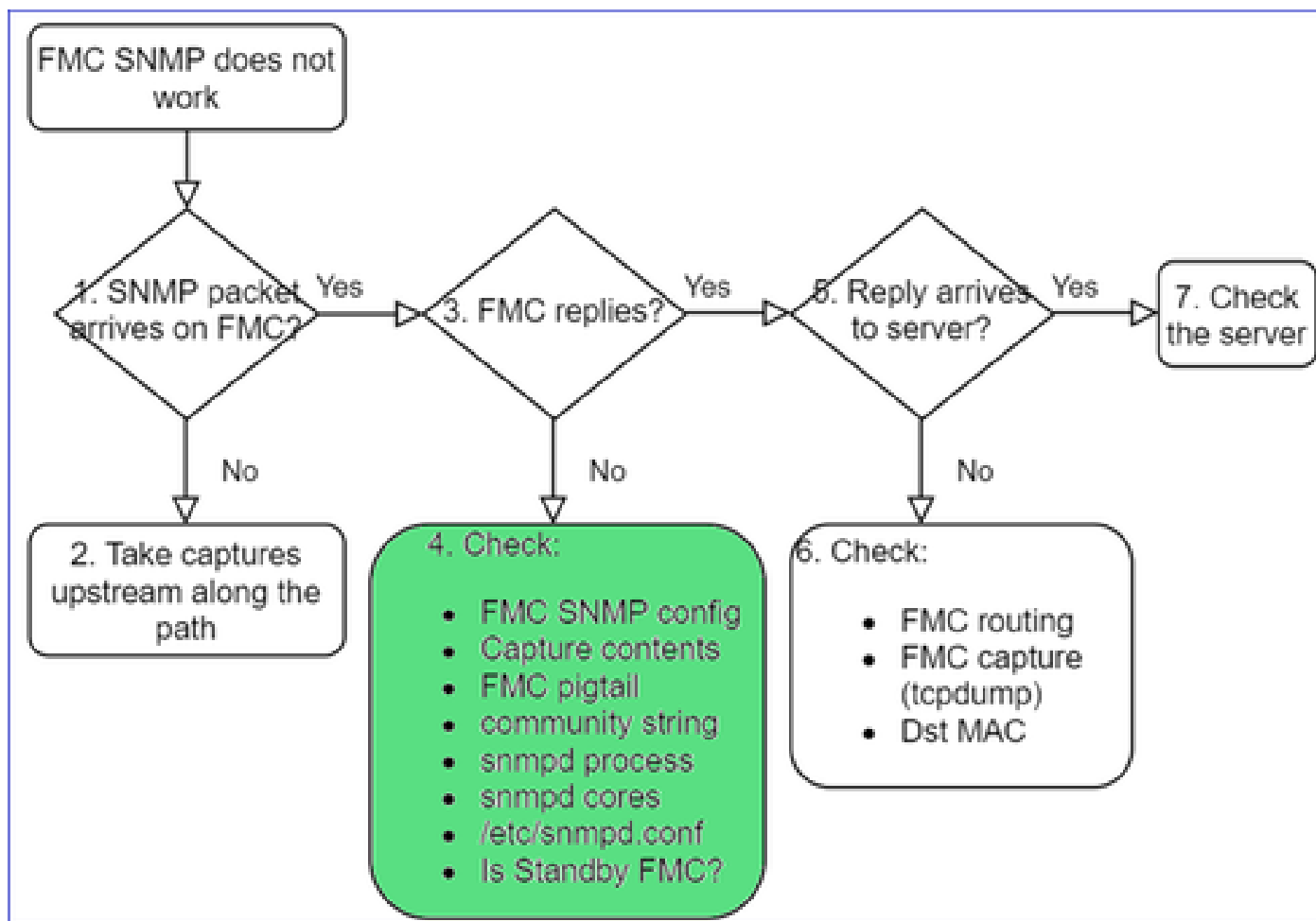
```
sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap
```

```
HS_PACKET_BUFFER_SIZE is set to 4.
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

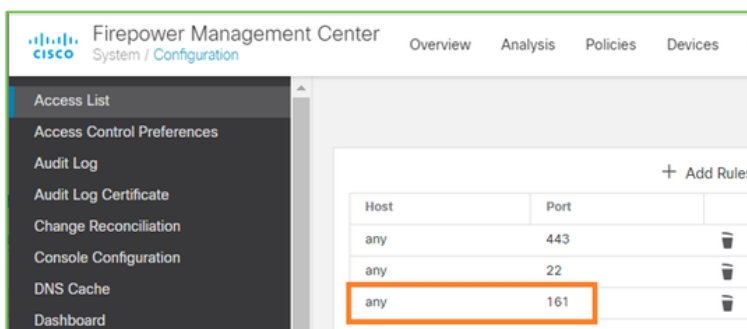
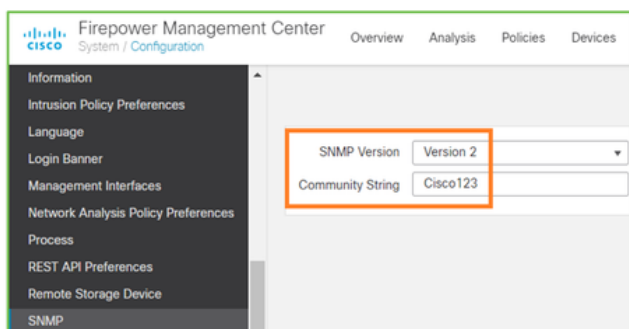
^C46 packets captured  
46 packets received by filter

FMC 是否应答？



如果 FMC 无应答，请检查：

- FMC SNMP 配置 (“系统”>“配置”)
  1. SNMP 部分
  2. “访问列表”部分



如果 FMC 无应答，请检查：

- 捕获 (数据包捕获) 内容

- 社区字符串 ( 可于捕获内容中查看 )
- FMC 尾纤输出 ( 查找错误、故障、踪迹 ) 和 /var/log/snmpd.log 中的内容
- snmpd 进程

<#root>

```
admin@FS2600-2:~$
```

```
sudo pmtool status | grep snmpd
```

```
snmpd (normal) - Running 12948
Command: /usr/sbin/snmpd -c /etc/snmpd.conf -Ls daemon -f -p /var/run/snmpd.pid
PID File: /var/run/snmpd.pid
Enable File: /etc/snmpd.conf
```

- snmpd 核心

<#root>

```
admin@FS2600-2:~$
```

```
ls -al /var/common | grep snmpd
```

```
-rw----- 1 root root          5840896 Aug  3 11:28 core_1627990129_FS2600-2_snmpd_3.12948
```

- /etc/snmpd.conf 中的后端配置文件 :

<#root>

```
admin@FS2600-2:~$
```

```
sudo cat /etc/snmpd.conf
```

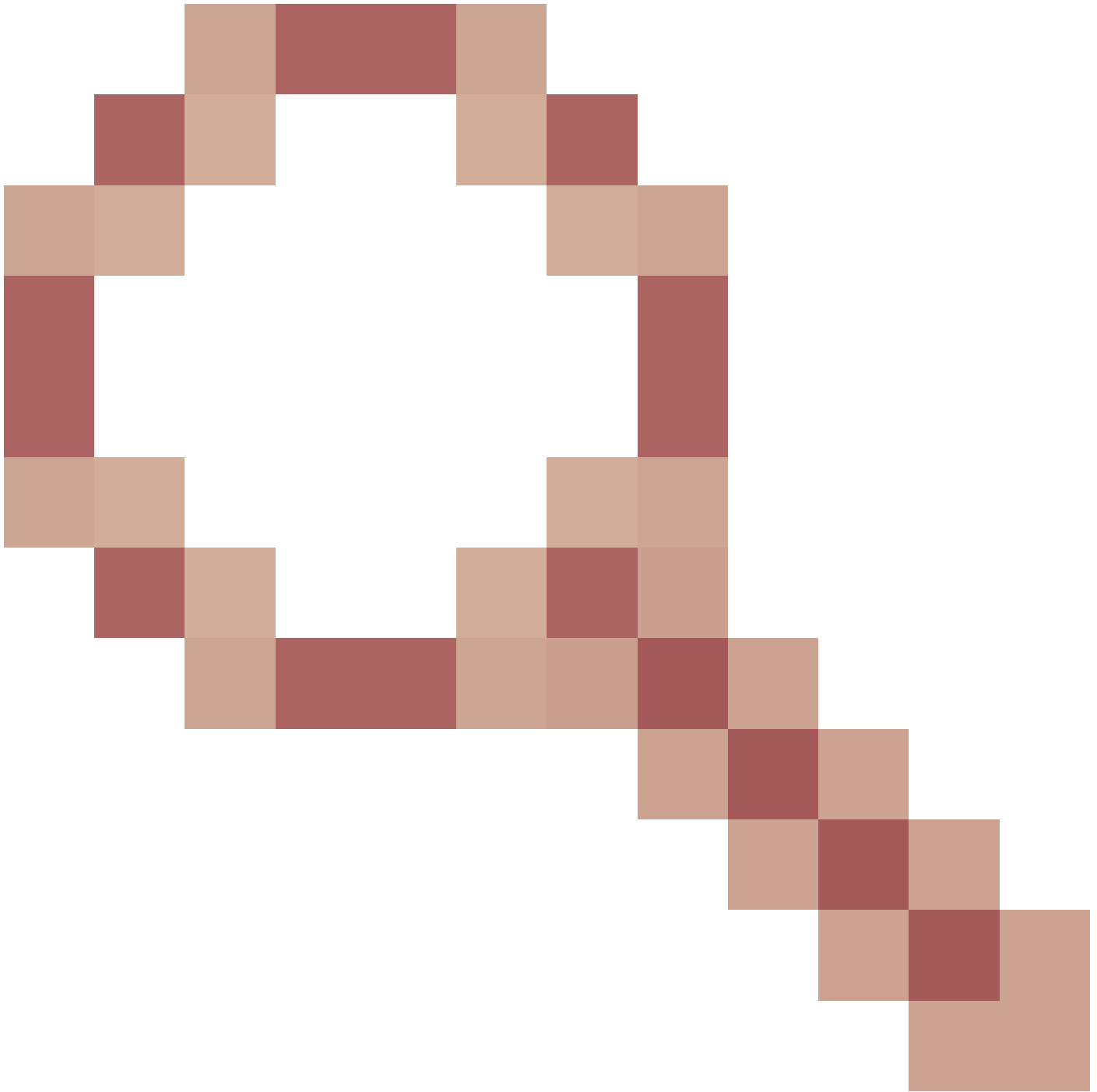
```
# additional user/custom config can be defined in *.conf files in this folder
includeDir /etc/snmp/config.d
engineIDType 3
agentaddress udp:161,udp6:161
rocommunity Cisco123
rocommunity6 Cisco123
```



注意：如果已禁用SNMP，则snmpd.conf文件不存在

- 是否为备用 FMC ?

在 6.4.0-9 和 6.6.0 及更低版本中，备用 FMC 不发送 SNMP 数据 ( snmpd 处于“等待”状态 )。这是预料之中的现象。检查增强功能思科漏洞ID [CSCvs32303](#)



## 无法配置 SNMP

问题描述 ( Cisco TAC 真实案例示例 ) :

- “我们想要为 Cisco Firepower Management Center 和 Firepower 4115 Threat Defense 配置 SNMP。”
- “FTD上的SNMP配置支持”。
- “我们想要在 FTD 设备上启用 SNMP 监控。”
- “我们尝试在 FXOS 中配置 SNMP 服务，但最后系统不允许使用 commit-buffer。显示错误：不允许更改。使用‘连接ftd’进行更改。”
- “我们想要在 FTD 设备上启用 SNMP 监控。”
- “无法在 FTD 上配置 SNMP，也无法在监控中发现设备。”



## 如何处理 SNMP 配置问题

首要任务：文档！

- 阅读本文档！
- 《FMC 配置指南》：

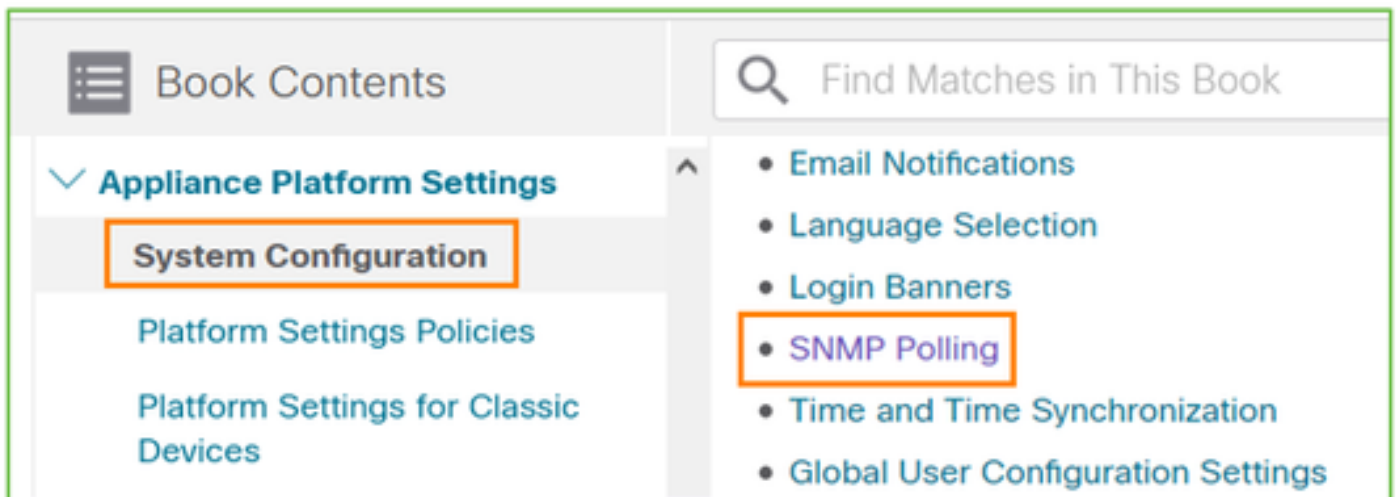
<https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html>

- 《FXOS 配置指南》：

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b\\_GUI\\_FXOS\\_ConfigGuide\\_2101/platform\\_settings.html#topic\\_6C6725BBF4BC4333BA207BE9DB](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB)

请留意各种 SNMP 文档！

FMC SNMP：



FXOS SNMP：

# Cisco Firepower 4100/9300 FXOS Firepower

Book Contents

Find Matches in This Book

Book Title Page

Introduction to the Firepower Security Appliance

Getting Started

License Management for the ASA

User Management

Image Management

Security Certifications Compliance

System Administration

**Platform Settings**

Chapter: Platform Settings

> Chapter Contents

- Setting the Date and Time
- Configuring SSH
- Configuring TLS
- Configuring Telnet
- **Configuring SNMP**
- Configuring HTTPS

Firepower 41xx/9300 SNMP 配置 :

✓ Appliance Platform Settings

System Configuration

Platform Settings Policies

Platform Settings for Classic Devices

**Platform Settings for Firepower Threat Defense**

Firepower 1xxx/21xx SNMP 配置 :

## Firepower Threat Defense Interfaces and Device Settings

Interface Overview for Firepower Threat Defense

Regular Firewall Interfaces for Firepower Threat Defense

Inline Sets and Passive Interfaces for Firepower Threat Defense

DHCP and DDNS Services for Threat Defense

SNMP for the Firepower 1000/2100

### Firepower Device Manager (FDM) 上的 SNMP 配置

问题描述 ( Cisco TAC 真实案例示例 ) :

- “我们需要相关指导，以使用 FDM 在 Firepower 设备上配置 SNMPv3。”
- “通过 FDM 无法在 FPR 2100 设备上配置 SNMP。”
- “无法通过 FDM 配置 SNMP v3。”
- “需要获取 FDM 6.7 SNMP 配置的帮助。”
- “在 Firepower FDM 中启用 SNMP v3。”

如何处理 SNMP FDM 配置问题

- 对于 6.7 之前的版本，可以使用 FlexConfig 执行 SNMP 配置：

<https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-advanced.html>

- 从 Firepower 6.7 开始，SNMP 配置不再使用 FlexConfig，而是使用 REST API：

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/216551-configure-and-troubleshoot-snmp-on-firep.html>

### SNMP 故障排除速查表

1xxx/21xx/41xx/9300 (LINA/ASA) – 在向 Cisco TAC 提交支持案例之前需要收集的内容

命令	描述
firepower# show run snmp-server	验证 ASA/FTD LINA SNMP 配置.
firepower# show snmp-server statistics	验证 ASA/FTD LINA 上的 SNMP 统计信息。重点关注 SNMP 数据包输入和输出计数器。

> capture-traffic	捕获管理接口上的流量.
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	在UDP 161的数据接口 ( 名为“net201” ) 上捕获流量 ( SNMP轮询 ) 。
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	捕获UDP 162的数据接口 ( 名为“net208” ) 上的流量。 ( SNMP陷阱 ) 。
firepower# show capture SNMP-POLL packet-number 1 trace	跟踪到达ASA/FTD LINA数据接口的入口SNMP数据包。
admin@firepower:~\$ sudo tcpdump -i tap_nlp	在 NLP ( 非 LINA 进程 ) 内部 tap 接口上进行捕获.
firepower# show conn all protocol udp port 161	检查UDP 161上的所有ASA/FTD LINA连接 ( SNMP轮询 ) 。
firepower# show log   我302015.*161	检查 SNMP 轮询的 ASA/FTD LINA 日志 302015.
firepower# more system:running-config   i社区	检查 SNMP 社区字符串.
firepower# debug menu netsnmp 4	验证 SNMP 配置和进程 ID.
firepower# show asp table classify interface net201 domain permit match port=161	检查名为“net201”的接口的SNMP ACL上的命中数。
firepower# show disk0:   i核心	检查是否存在任何 SNMP 核心。
admin@firepower:~\$ ls -l /var/data/cores	检查是否存在任何 SNMP 核心。仅适用于 FTD.
firepower# show route	验证 ASA/FTD LINA 路由表.
> show network	验证 FTD 管理平面路由表.
admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	检验/排除FTD上的SNMPv3故障。

<pre>firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]</pre>	较新版本中的隐藏命令。内部调试，有助于 Cisco TAC 对 SNMP 进行故障排除。
---	--

41xx/9300 (FXOS) – 在向 Cisco TAC 提交支持案例之前需要收集的内容

命令	描述
<pre>firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture- filter "udp port 161" limit-captured-frames 50 write workspace:///SNMP-POLL.pcap firepower(fxos)# exit firepower# connect local-mgmt firepower(local-mgmt)# dir 1 11152 Jul 26 09:42:12 2021 SNMP.pcap firepower(local-mgmt)# copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap</pre>	SNMP 轮询 (UDP 161) 的 FXOS 捕获 上传到远程 FTP 服务器 FTP IP : 192.0.2.100 FTP用户名 : ftp
<pre>firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture- filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap</pre>	SNMP 陷阱 (UDP 162) 的 FXOS 捕获
<pre>firepower# scope system firepower /system # scope services firepower /system/services # show ip-block detail</pre>	检查 FXOS ACL
<pre>firepower# show fault</pre>	检查 FXOS 故障
<pre>firepower# show fabric-interconnect</pre>	验证 FXOS 接口配置和默认网关设置

firepower# connect fxos firepower(fxos)# show running-config snmp all	验证 FXOS SNMP 配置
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	验证 FXOS SNMP OID
firepower# connect fxos firepower(fxos)# show snmp	验证 FXOS SNMP 设置和计数器
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	调试 FXOS SNMP ( “数据包”或“全部” ) 使用“terminal no monitor”和“undebug all”停止调试

1xxx/21xx (FXOS) – 在向 Cisco TAC 提交支持案例之前需要收集的内容

命令	描述
> capture-traffic	捕获管理接口上的流量
> show network	验证 FTD 管理平面路由表
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail] firepower /monitoring # show snmp-trap	验证 FXOS SNMP 配置
firepower# show fault	检查 FXOS 故障
firepower# connect local-mgmt	检查 FXOS 核心文件 ( 回溯 )

firepower(local-mgmt)# dir cores_fxos	
firepower(local-mgmt)# dir cores	

### FMC – 在向 Cisco TAC 提交支持案例之前需要收集的内容

命令	描述
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n	捕获管理接口上用于 SNMP 轮询的流量
admin@FS2600-2 : ~\$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	捕获管理接口上用于 SNMP 轮询的流量并将其保存到文件中
admin@FS2600-2:~\$ sudo pmtool status   grep snmpd	检查 SNMP 进程状态
admin@FS2600-2:~\$ ls -al /var/common   grep snmpd	检查 SNMP 核心文件 ( 回溯 )
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	检查 SNMP 配置文件的内容

### snmpwalk 示例

下列命令可用于验证和故障排除：

命令	描述
# snmpwalk -c Cisco123 -v2c 192.0.2.1	使用 SNMP v2c 获取远程主机的所有 OID。 Cisco123 = 社区字符串 192.0.2.1 = 目的主机
# snmpwalk -v2c -c Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.9.109.1.1.1.3 iso.3.6.1.4.1.9.9.109.1.1.1.3.1 = Gauge32 : 0	使用 SNMP v2c 获取远程主机的特定 OID

<pre># snmpwalk -c Cisco123 -v2c 192.0.2.1 .10.3.1.1.4.1.9.9.109.1.1.1.1 -On .10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 = Gauge32 : 0</pre>	<p>以数字格式显示获取的 OID</p>
<pre># snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 - x AES -X Cisco123 192.0.2.1</pre>	<p>使用 SNMP v3 获取远程主机的所有 OID。</p> <p>SNMPv3 用户 = cisco</p> <p>SNMPv3 身份验证 = SHA。</p> <p>SNMPv3 授权 = AES</p>
<pre># snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 - x AES -X Cisco123 192.0.2.1</pre>	<p>使用 SNMP v3 ( MD5 和 AES128 ) 获取远程主机的所有 OID</p>
<pre># snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1</pre>	<p>仅具有身份验证的 SNMPv3</p>

## 如何搜索 SNMP 缺陷

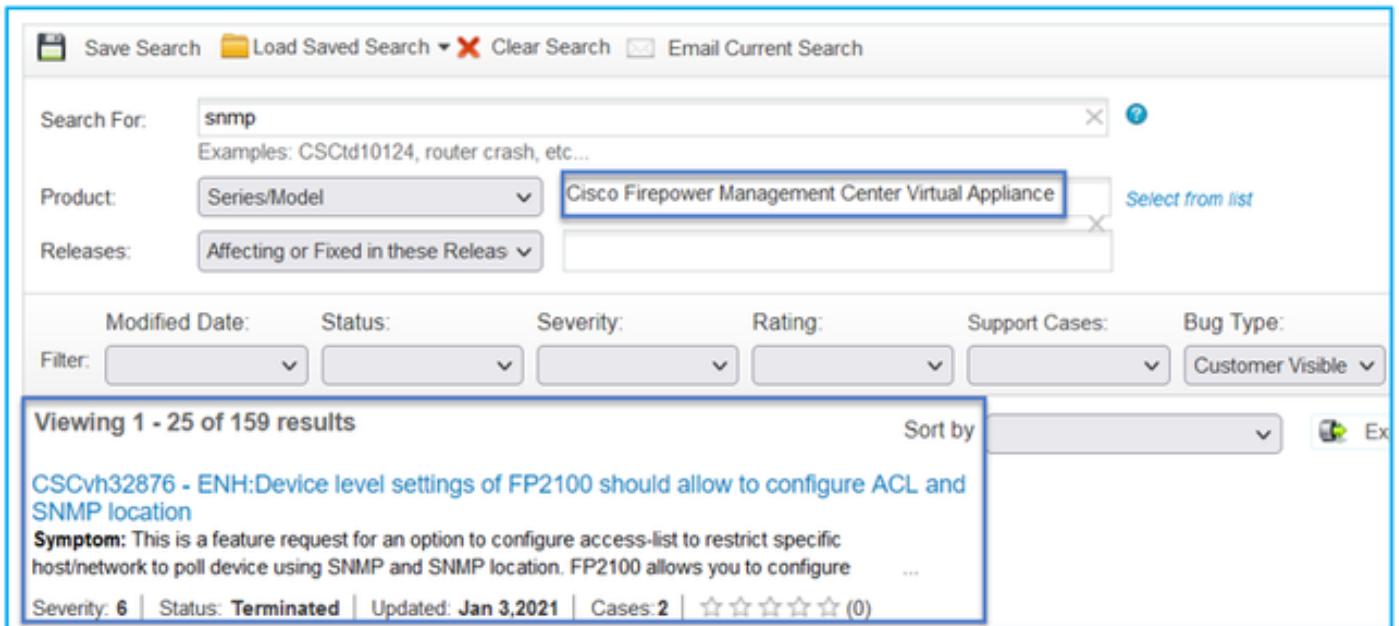
### 1. 导航至

<https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV>

### 2. 输入关键字snmp并选择Select from list。

The screenshot shows the Cisco Bug Search Tool interface. The search term "snmp" is entered in the "Search For" field. The "Product" dropdown is set to "Series/Model", and the "Releases" dropdown is set to "Affecting or Fixed in these Releas". A "Select from list" button is highlighted. At the bottom, there are filter options for Modified Date, Status, Severity, Rating, Support Cases, and Bug Type.





最常见的产品：

- 思科自适应安全设备 (ASA) 软件
- Cisco Firepower 9300 系列
- Cisco Firepower Management Center 虚拟设备
- Cisco Firepower NGFW

## 相关信息

- [配置用于 Threat Defense 的 SNMP](#)
- [在FXOS \(UI\)上配置SNMP](#)
- [技术支持和文档 - Cisco Systems](#)

## 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）。