Configure SNMP on Firepower NGFW Appliances

Contents

- Introduction
- Prerequisites
  - Requirements
  - Components Used
- Background Information
- Configure
  - Chassis (FXOS) SNMP on FPR4100/FPR9300
    - Configure FXOS SNMPv1/v2c in the GUI
    - Configure FXOS SNMPv1/v2c via Command Line Interface (CLI)
    - Configure FXOS SNMPv3 in the GUI
    - Configure FXOS SNMPv3 in the CLI
  - FTD (LINA) SNMP on FPR4100/FPR9300
    - Changes in 6.6+ Releases
    - Configure LINA SNMPv2c
    - Configure LINA SNMPv3
    - MIO Blade SNMP Unification (FXOS 2.12.1, FTD 7.2, ASA 9.18.1)
  - SNMP in FPR2100
  - Chassis (FXOS) SNMP on FPR2100
    - Configure FXOS SNMPv1/v2c
    - Configure FXOS SNMPv3
  - FTD (LINA) SNMP on FPR2100
    - FTD 6.6+ Releases
- Verify
  - Verify FXOS SNMP for FPR4100/FPR9300
    - FXOS SNMPv2c Verifications
    - FXOS SNMPv3 Verifications
  - Verify FXOS SNMP for FPR2100
    - FXOS SNMPv2 Verifications
    - FXOS SNMPv3 Verifications
  - Verify FTD SNMP
  - Allow SNMP Traffic to FXOS on FPR4100/FPR9300
    - Configure Global Access-list in the GUI
    - Configure Global Access-list in the CLI
    - Verification
  - Use the OID Object Navigator
- Troubleshoot
  - Unable to Poll FTD LINA SNMP
  - Unable to Poll FXOS SNMP
    - Recommended Troubleshooting
  - What SNMP OID Values to Use?
  - Cannot Get SNMP Traps
  - Cannot Monitor FMC via SNMP

SNMP Config on Firepower Device Manager (FDM)
How to Approach SNMP FDM Configuration Issues
SNMP Troubleshooting Cheat Sheets
How to Search for SNMP Defects
Related information

Introduction

This document describes how to configure and troubleshoot Simple Network Management Protocol (SNMP) on Next Generation Firewall (NGFW) FTD appliances.

Prerequisites

Requirements

This document requires basic knowledge of the SNMP protocol.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Firepower NGFW appliances can be split into 2 major subsystems:

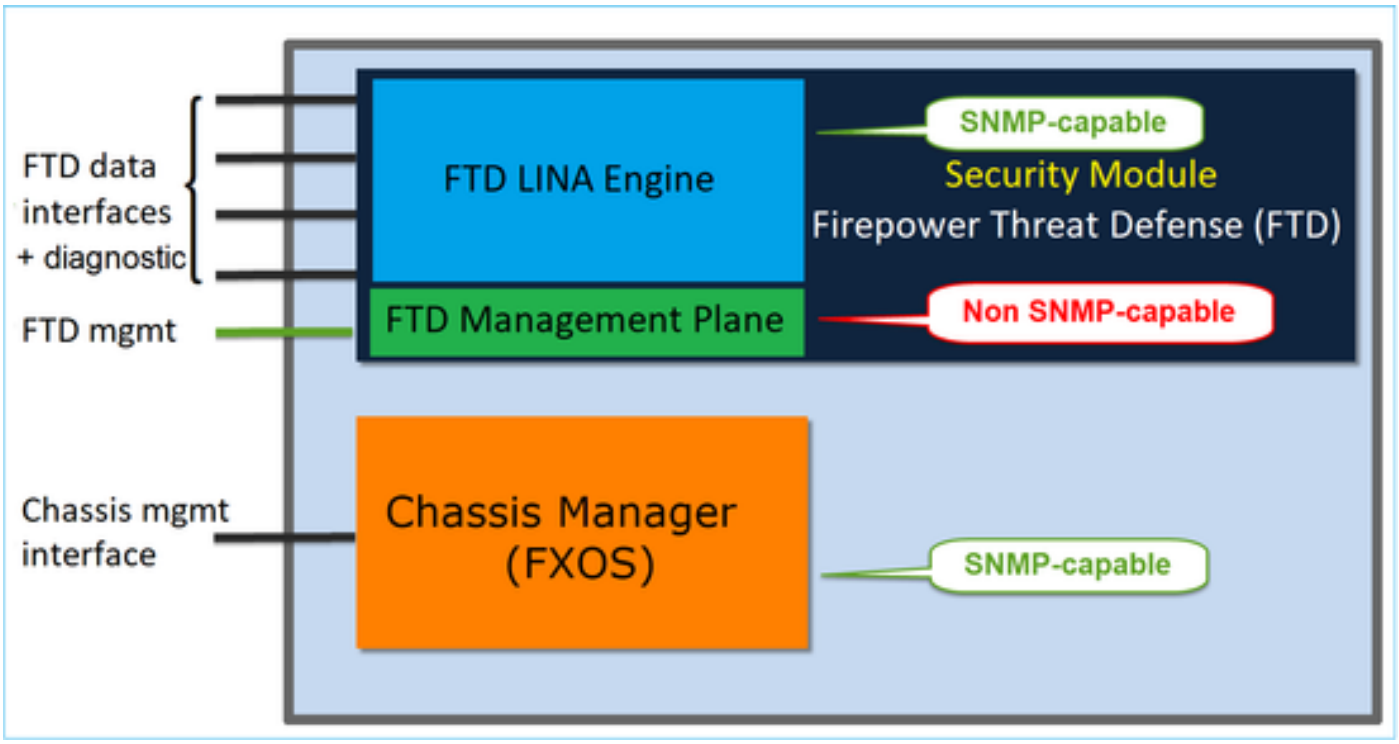
- The Firepower Extensible Operative System (FX-OS) controls the chassis hardware
- The Firepower Threat Defense (FTD) runs within the module

FTD is a unified software that consists of 2 main engines, the Snort engine, and the LINA engine. The current SNMP engine of the FTD derives from the classic ASA and it has visibility to the LINA-related features.

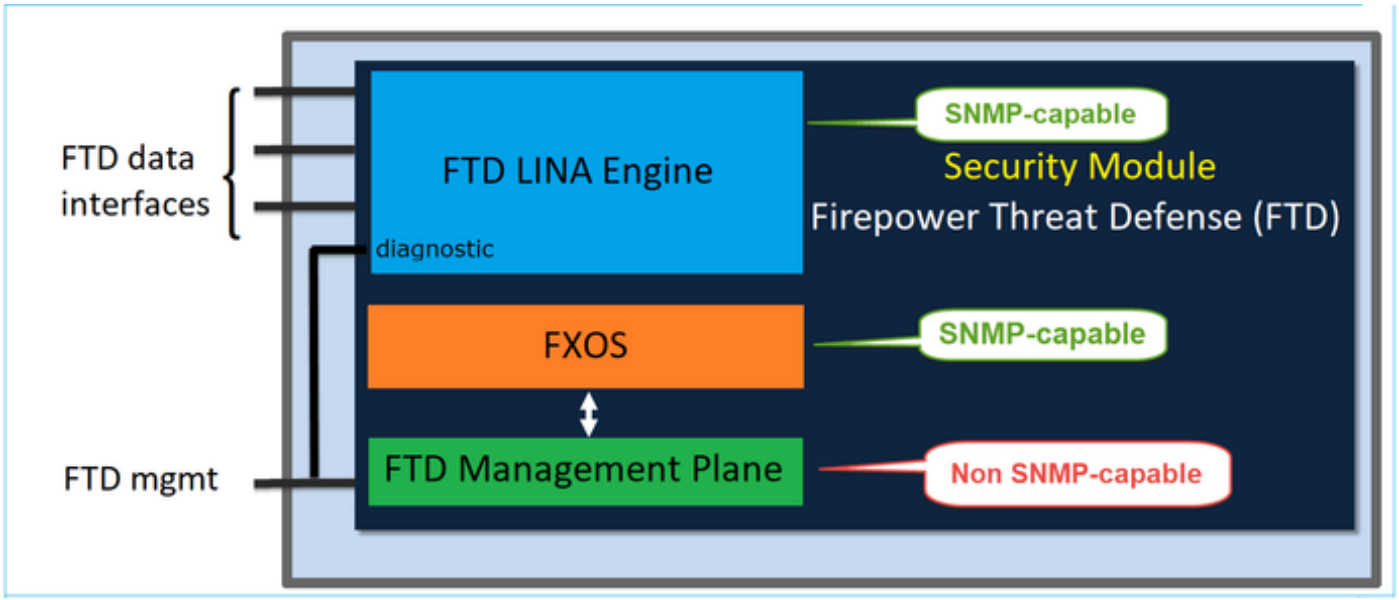
FX-OS and FTD have independent control planes and for monitoring purposes, they have different SNMP engines. Each of the SNMP engines provides different information and monitors both for a more comprehensive view of the device status.

From a hardware point of view, there are currently two major architectures for the Firepower NGFW appliances: the Firepower 2100 series and the Firepower 4100/9300 series.

Firepower 4100/9300 devices have a dedicated interface for device management. This is the source and destination for the SNMP traffic addressed to the FXOS subsystem. On the other hand, the FTD application uses a LINA interface (data and/or diagnostic). In post-6.6 FTD releases, the FTD management interface can be used as well for the SNMP configuration.



The SNMP engine on Firepower 2100 appliances uses the FTD management interface and IP. The appliance itself bridges the SNMP traffic received on this interface and forwards it to the FXOS software.

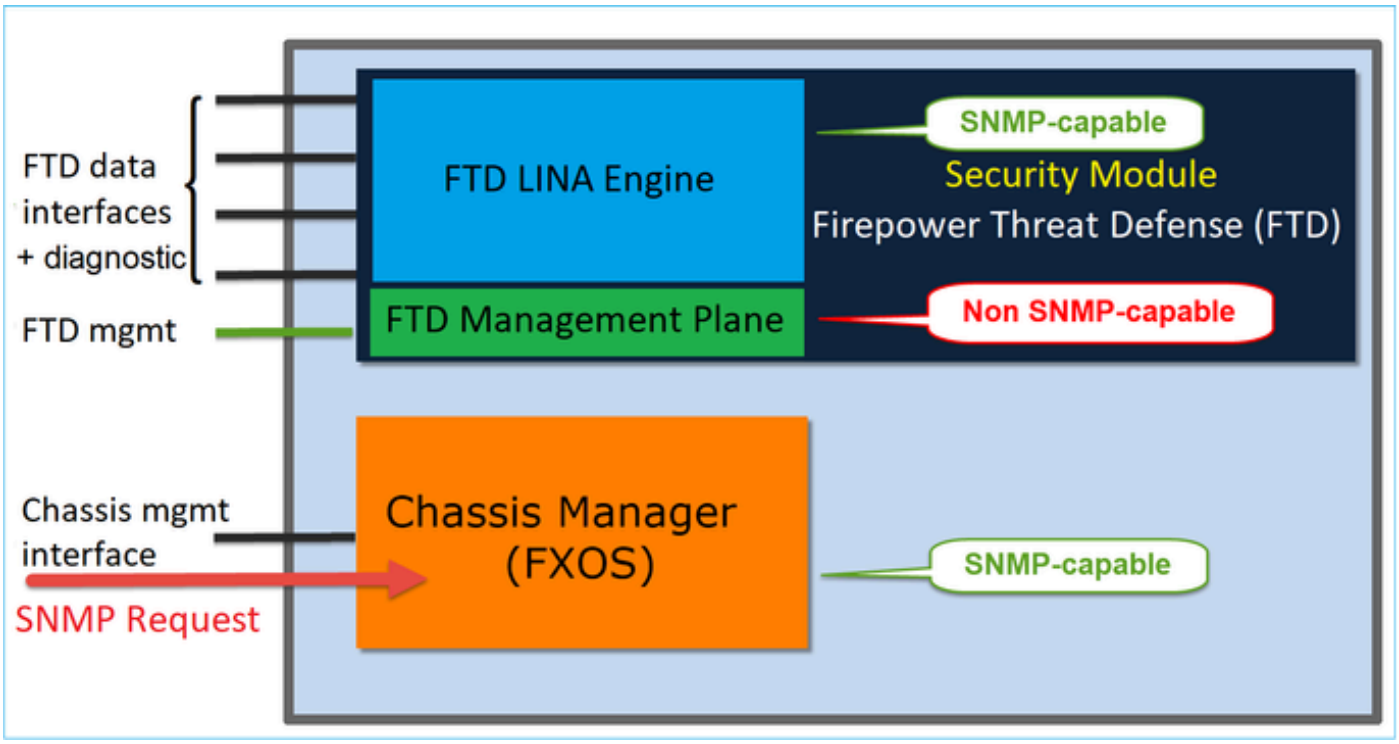


On FTDs that use software release 6.6+, these changes were introduced:

- SNMP over the Management interface.
- On the FPR1000 or FPR2100 Series platforms, it unifies both LINA SNMP and FXOS SNMP over this single Management interface. Additionally, it provides a single configuration point on FMC under **Platform settings > SNMP**.

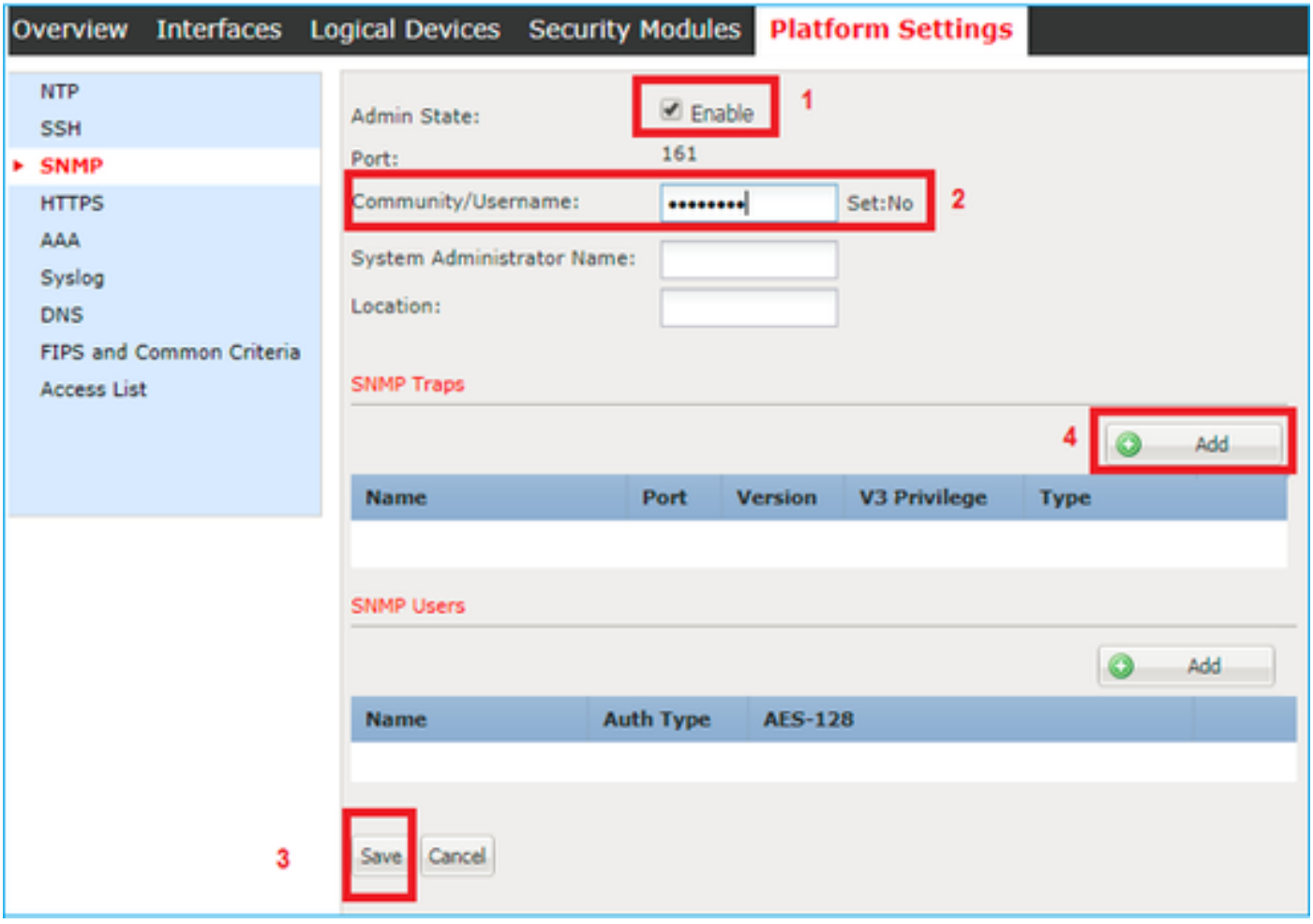
Configure

Chassis (FXOS) SNMP on FPR4100/FPR9300



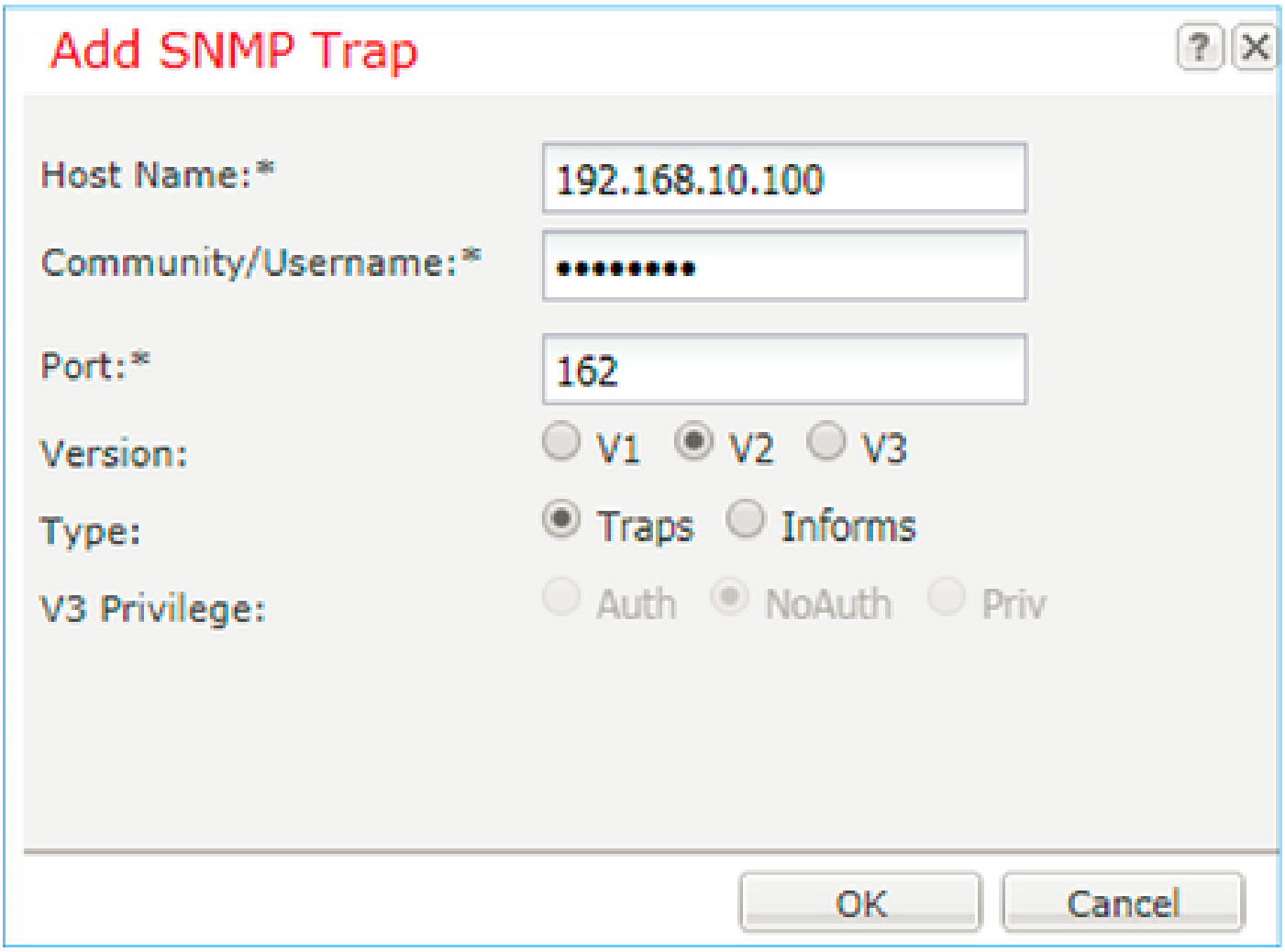
Configure FXOS SNMPv1/v2c in the GUI

Step 1. Open the Firepower Chassis Manager (FCM) UI and navigate to **Platform Settings** > **SNMP** tab. Check the SNMP enable box, specify the **Community** string to use on SNMP requests, and **Save**.



Note: If the Community/Username field is already set, the text to the right of the empty field reads **Set: Yes**. If the Community/Username field is not yet populated with a value, the text to the right of the empty field reads **Set: No**

Step 2. Configure the SNMP traps destination server.



Note: The community values for queries and trap host are independent and can be different

The host can be defined as an IP address or by name. Select **OK** and the configuration of the SNMP Trap server is saved automatically. There is no need to select the save button from the SNMP main page. The same occurs when you delete a host.

Configure FXOS SNMPv1/v2c via Command Line Interface (CLI)

<#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

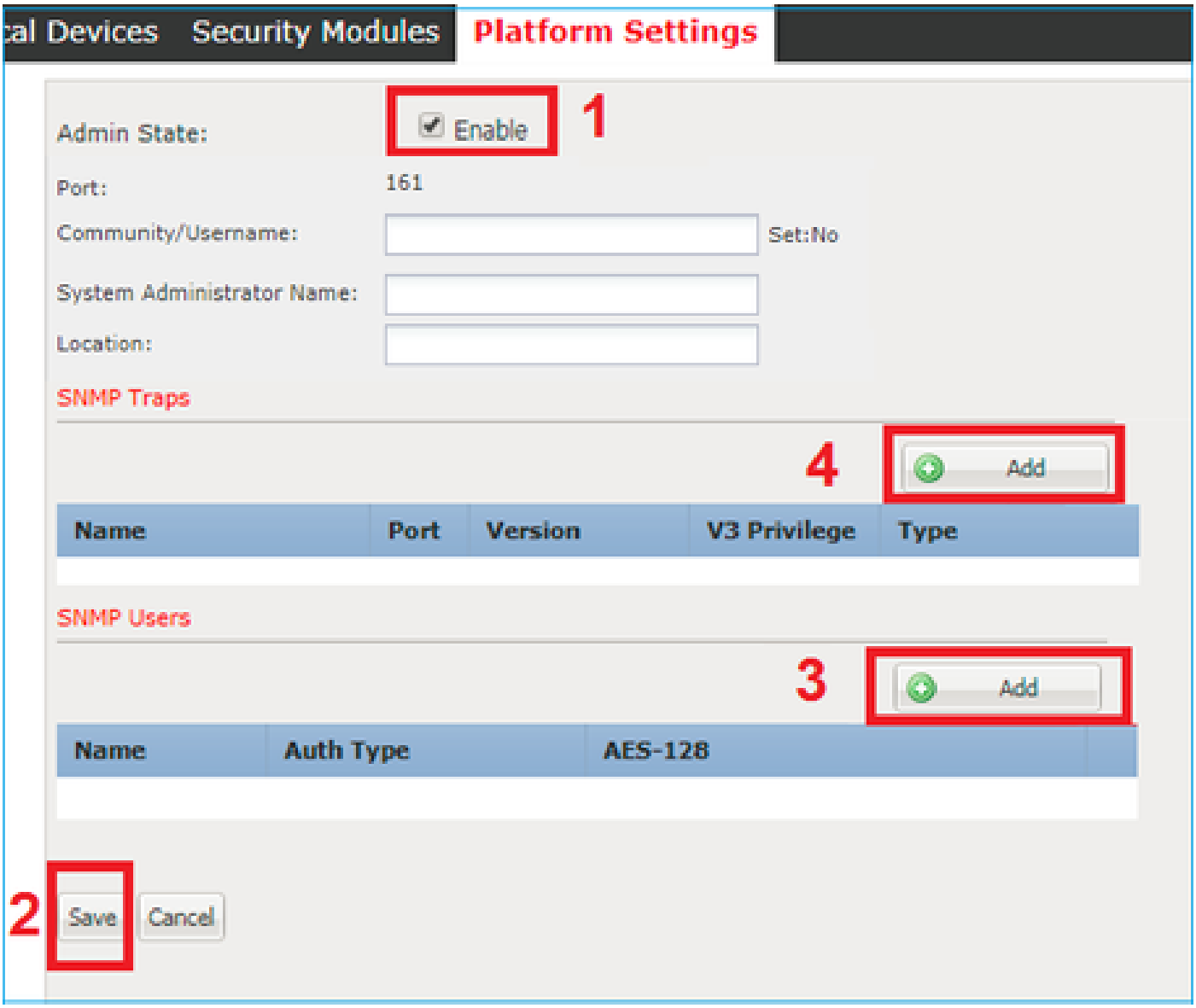
ksec-fpr9k-1-A /monitoring* #

 commit-buffer
```

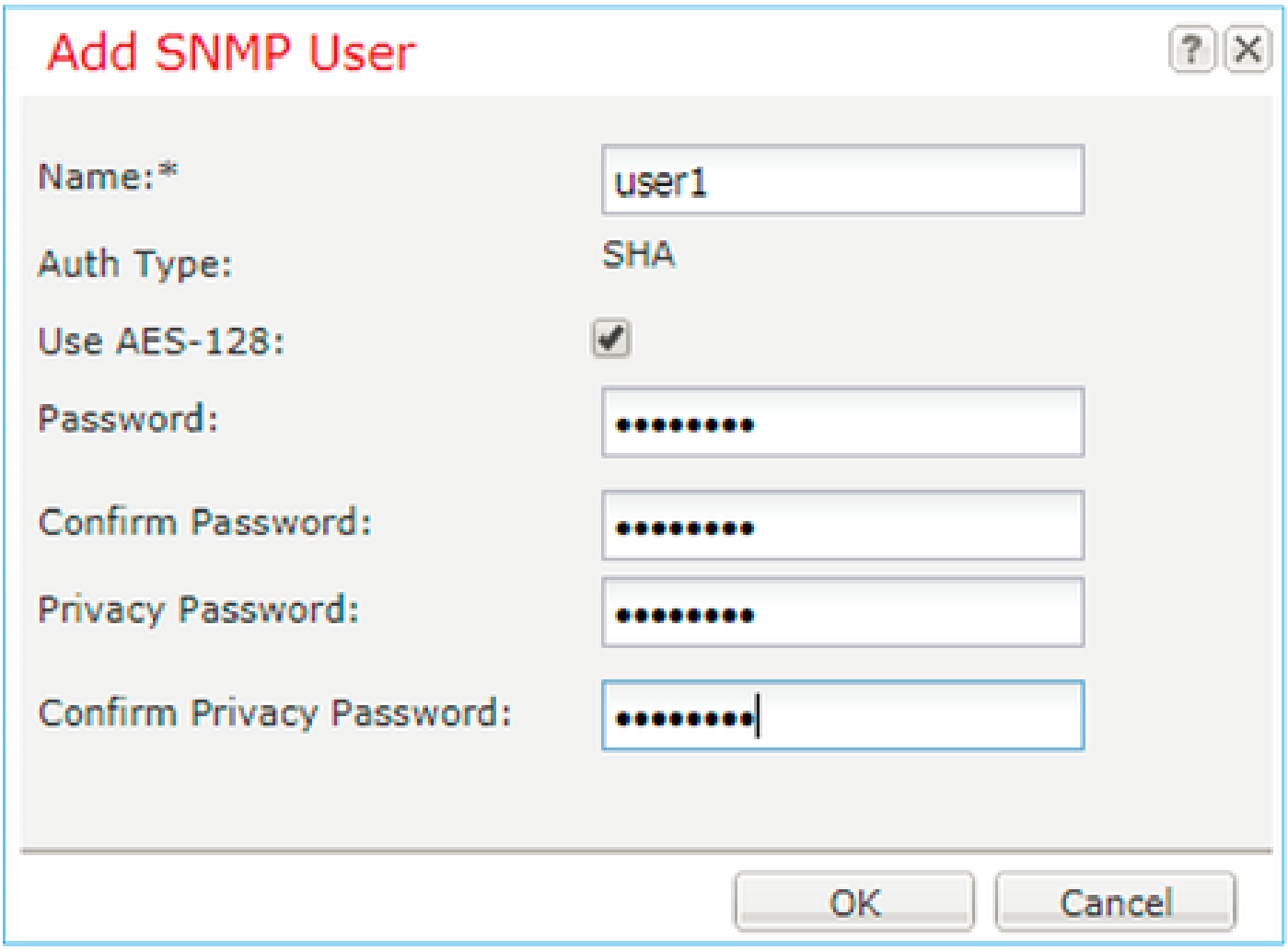
Configure FXOS SNMPv3 in the GUI

Step 1. Open FCM and navigate to **Platform Settings > SNMP** tab.

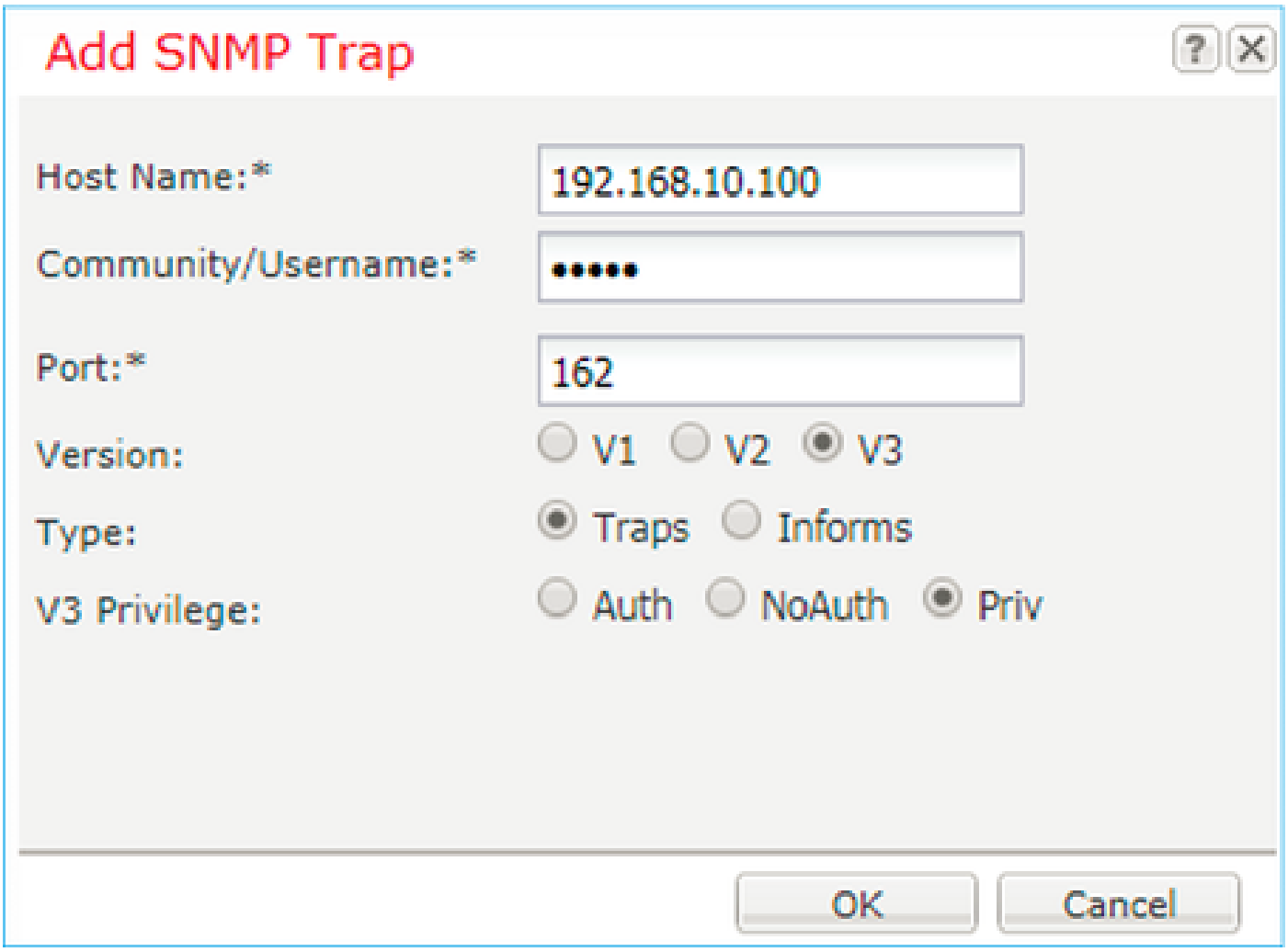
Step 2. For SNMP v3, there is no need to set any community string in the upper section. Every user created is able to successfully run queries to the FXOS SNMP engine. The first step is to enable SNMP in the platform. Once done you can create the users and destination trap host. Both SNMP Users and SNMP Trap hosts are saved automatically.



Step 3. As shown in the image, add the SNMP user. The authentication type is always SHA, but you can use AES or DES for encryption:



Step 4. Add the SNMP trap host as shown in the image:



Configure FXOS SNMPv3 in the CLI

<#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* #
```

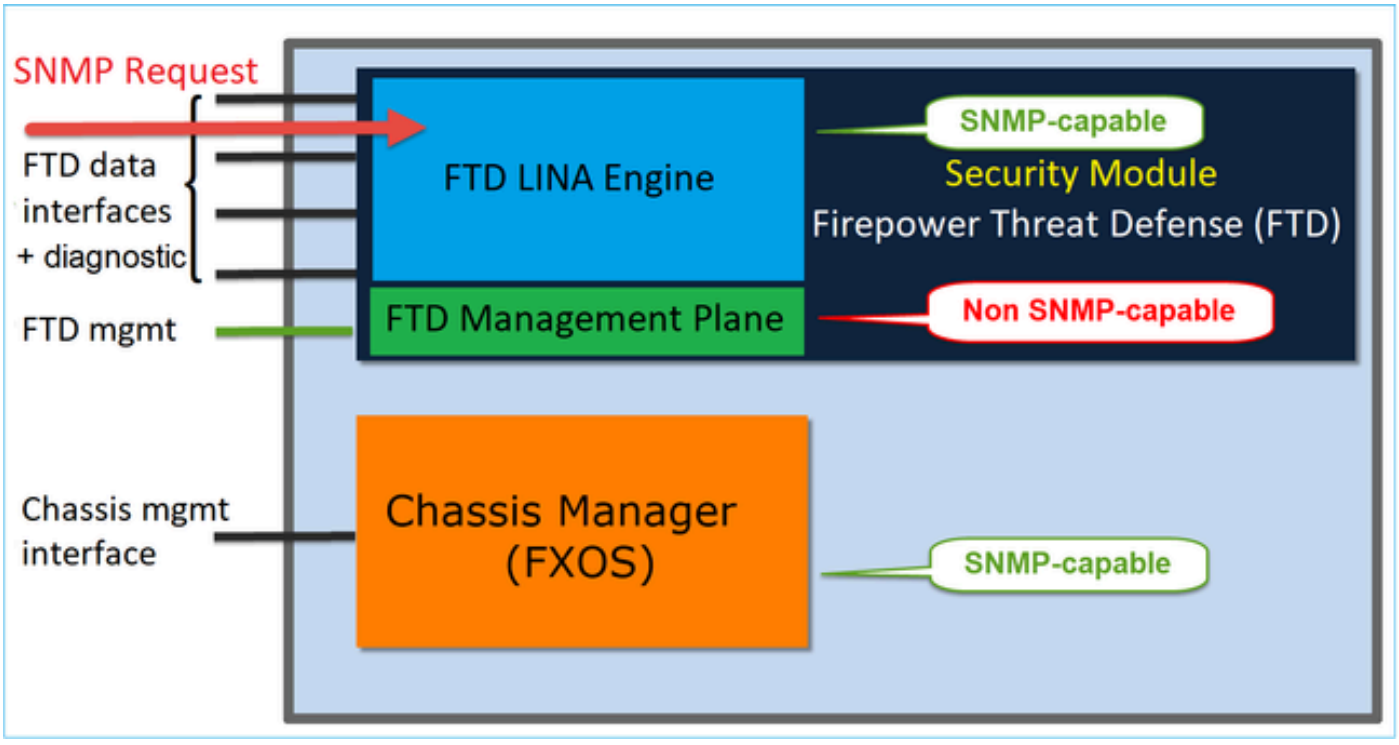
set priv-password

```
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
```

set aes-128 yes

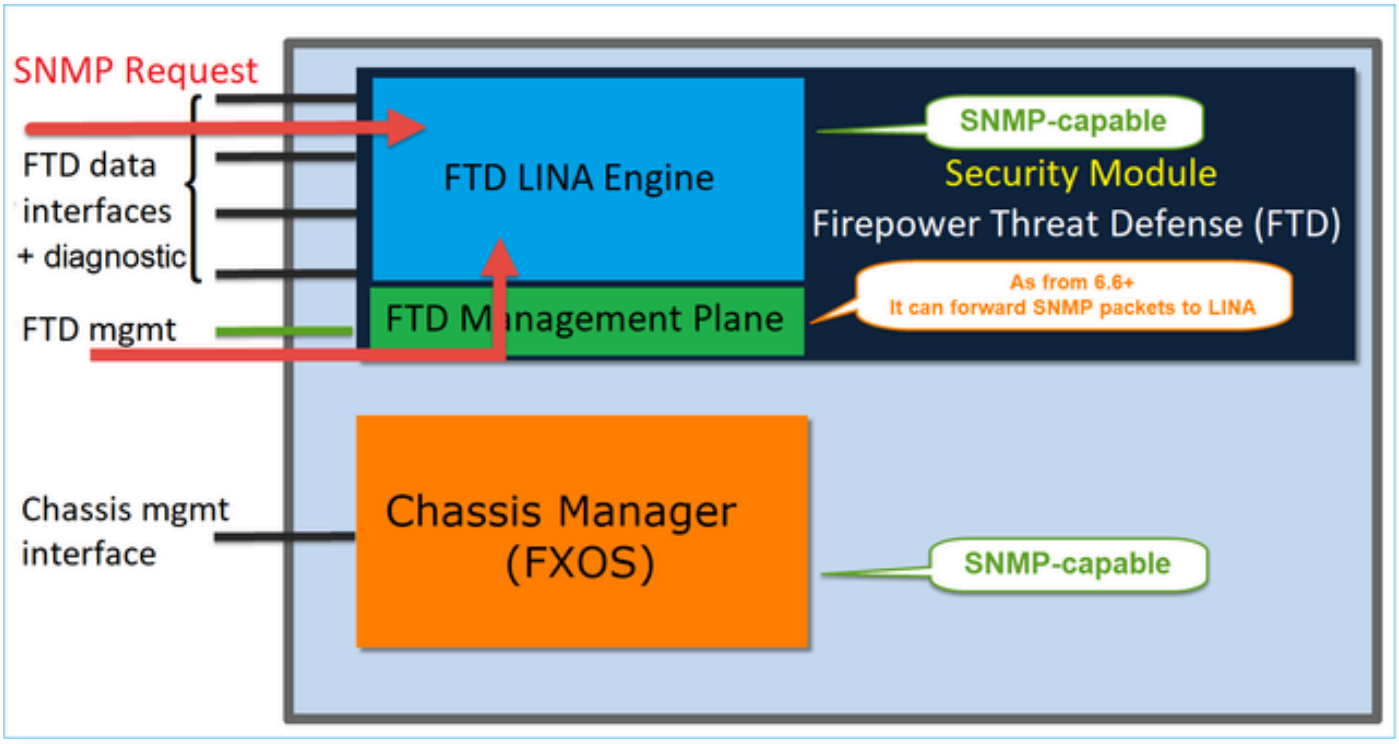
```
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter snmp-trap 10.48.26.190
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v3
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype traps
ksec-fpr9k-1-A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

FTD (LINA) SNMP on FPR4100/FPR9300



Changes in 6.6+ Releases

- In post-6.6 releases, you have also the option to use the FTD management interface for polls and traps.



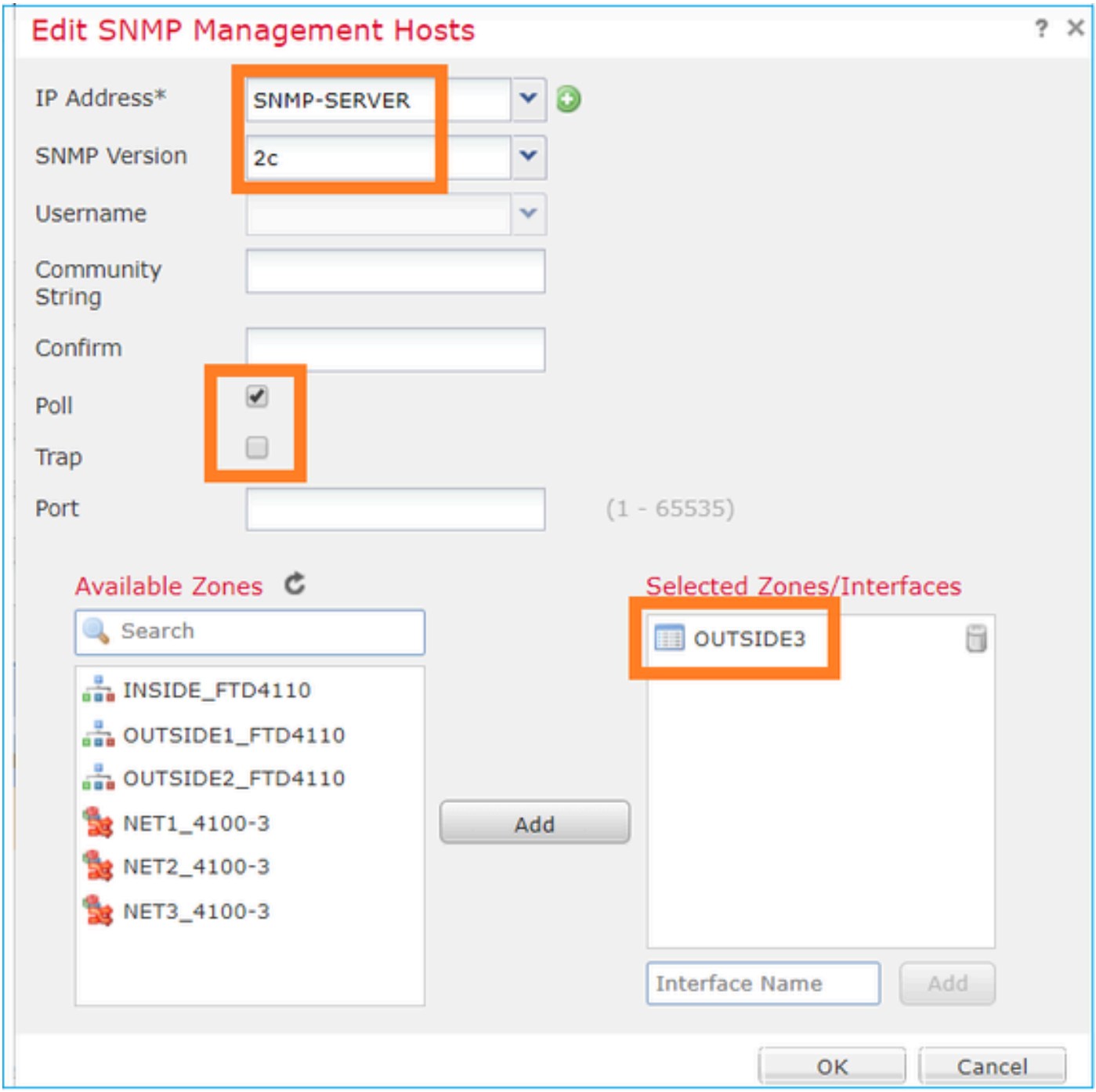
SNMP Single IP management feature is supported from 6.6 onwards on all FTD platforms:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 that runs FTD
- FTDv

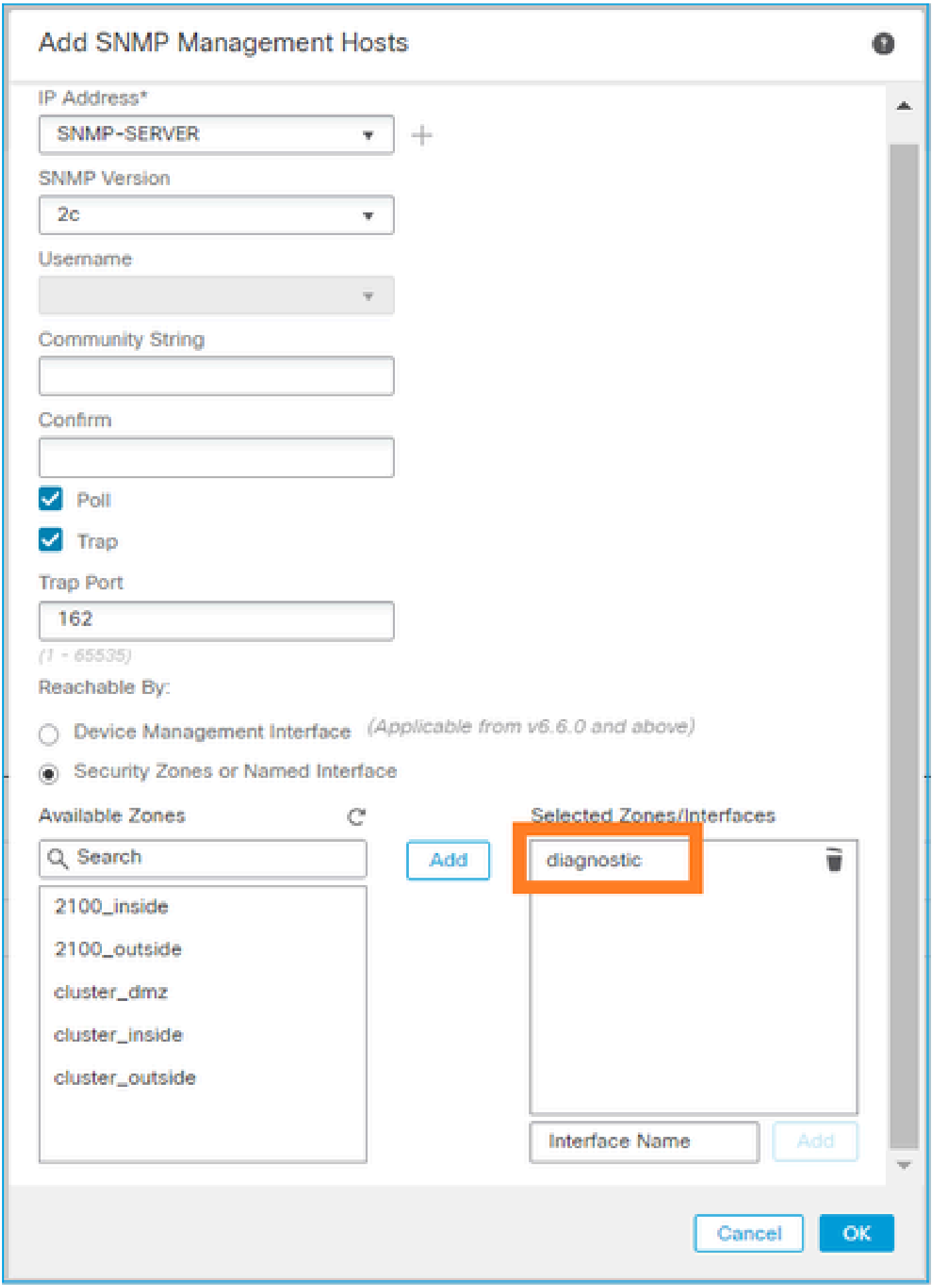
Configure LINA SNMPv2c

Step 1. On FMC UI, navigate to **Devices > Platform Settings > SNMP.** Check the option **Enable SNMP Servers** and configure the SNMPv2 settings.

Step 2. On the **Hosts** tab, select the **Add** button and specify the SNMP server settings:

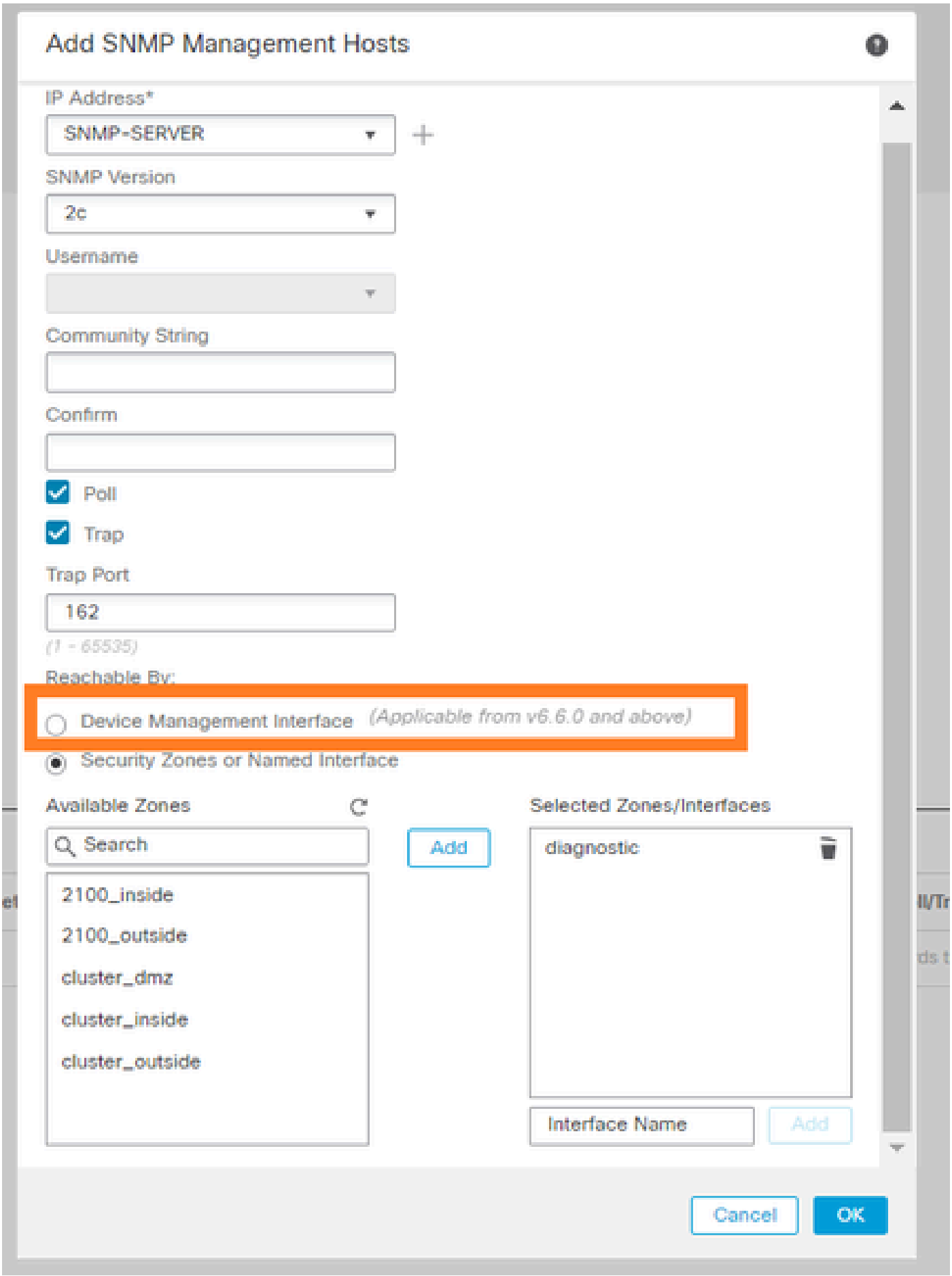


You can also specify the **diagnostic** interface as a source for the SNMP messages. The diagnostic interface it is a data interface that only allows traffic to-the-box and from-the-box (management-only).


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

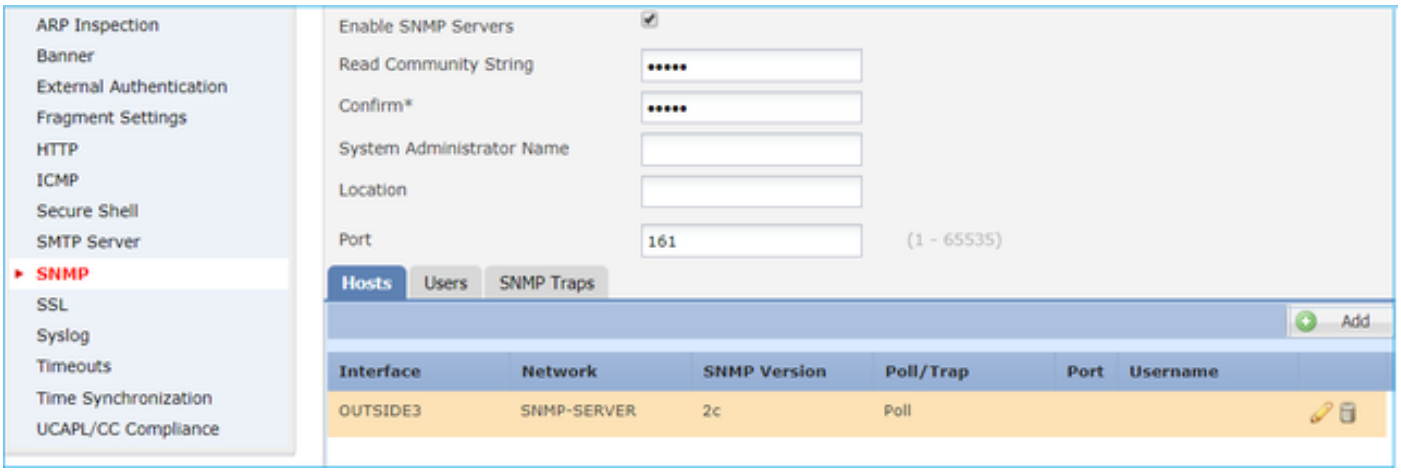
This image is from the 6.6 release and uses the Light Theme.

Additionally, in post-6.6 FTD releases you can also choose the management interface:



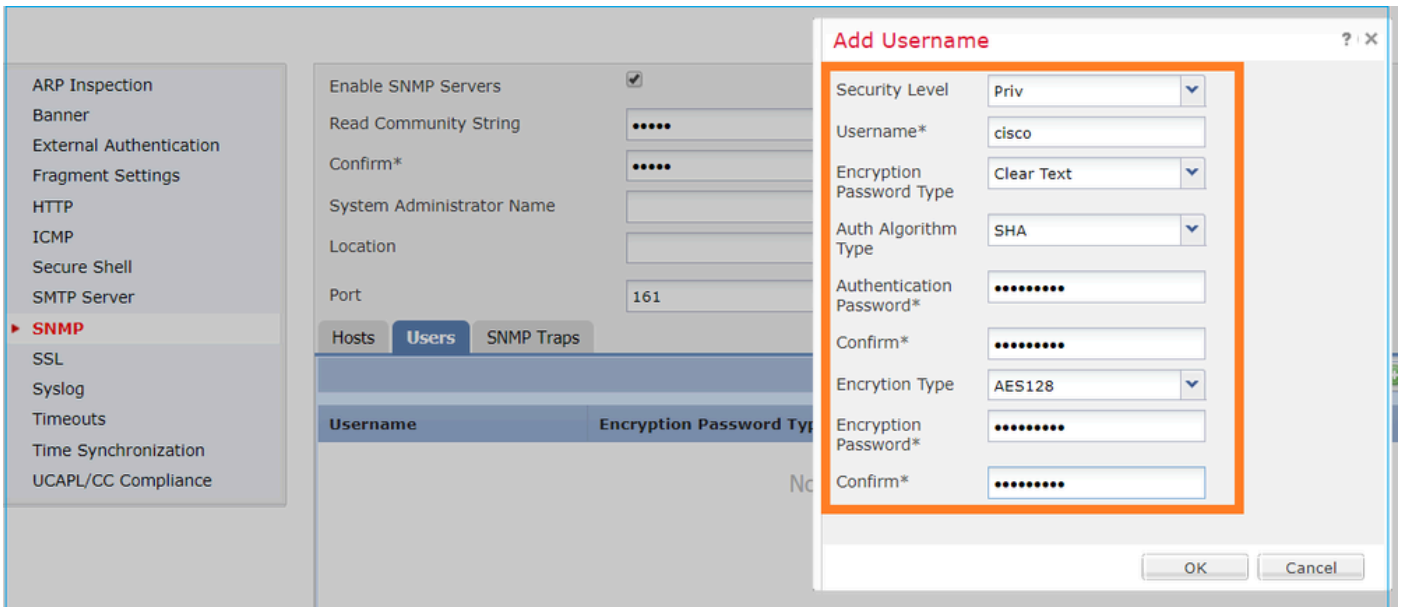
If the new management interface is selected the LINA SNMP is available over the Management interface.

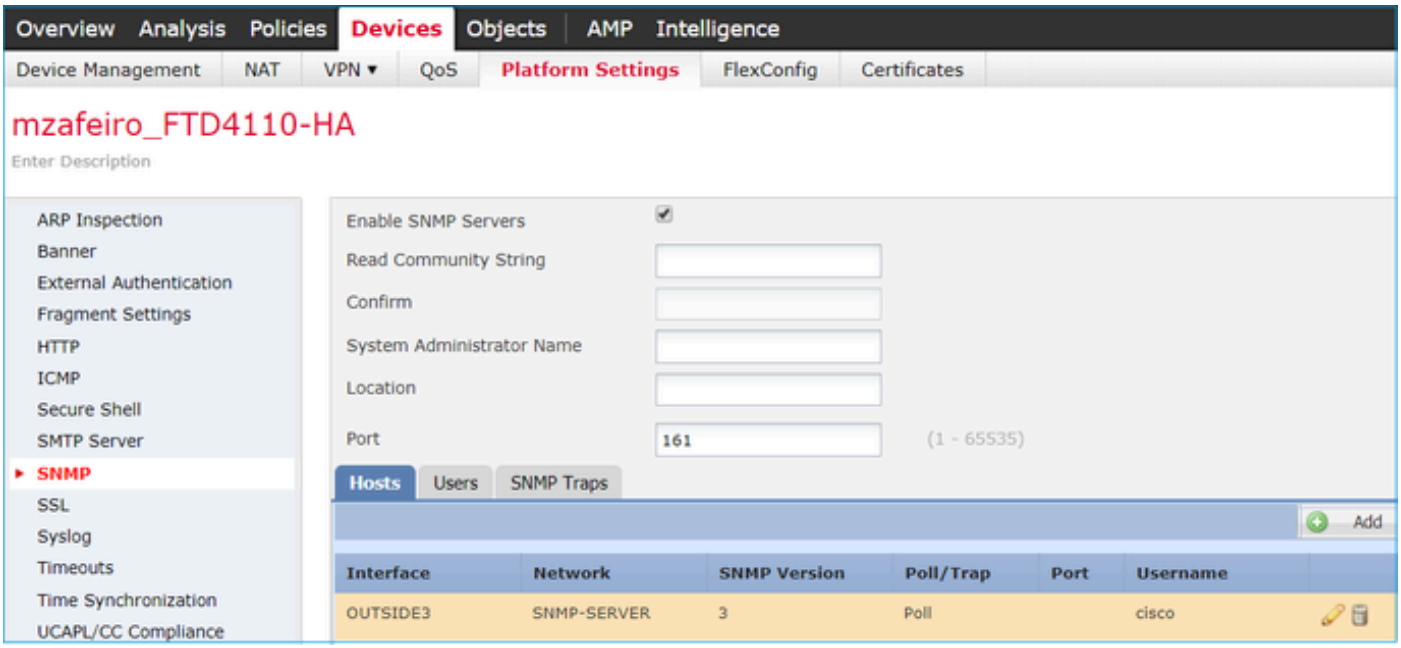
The result:



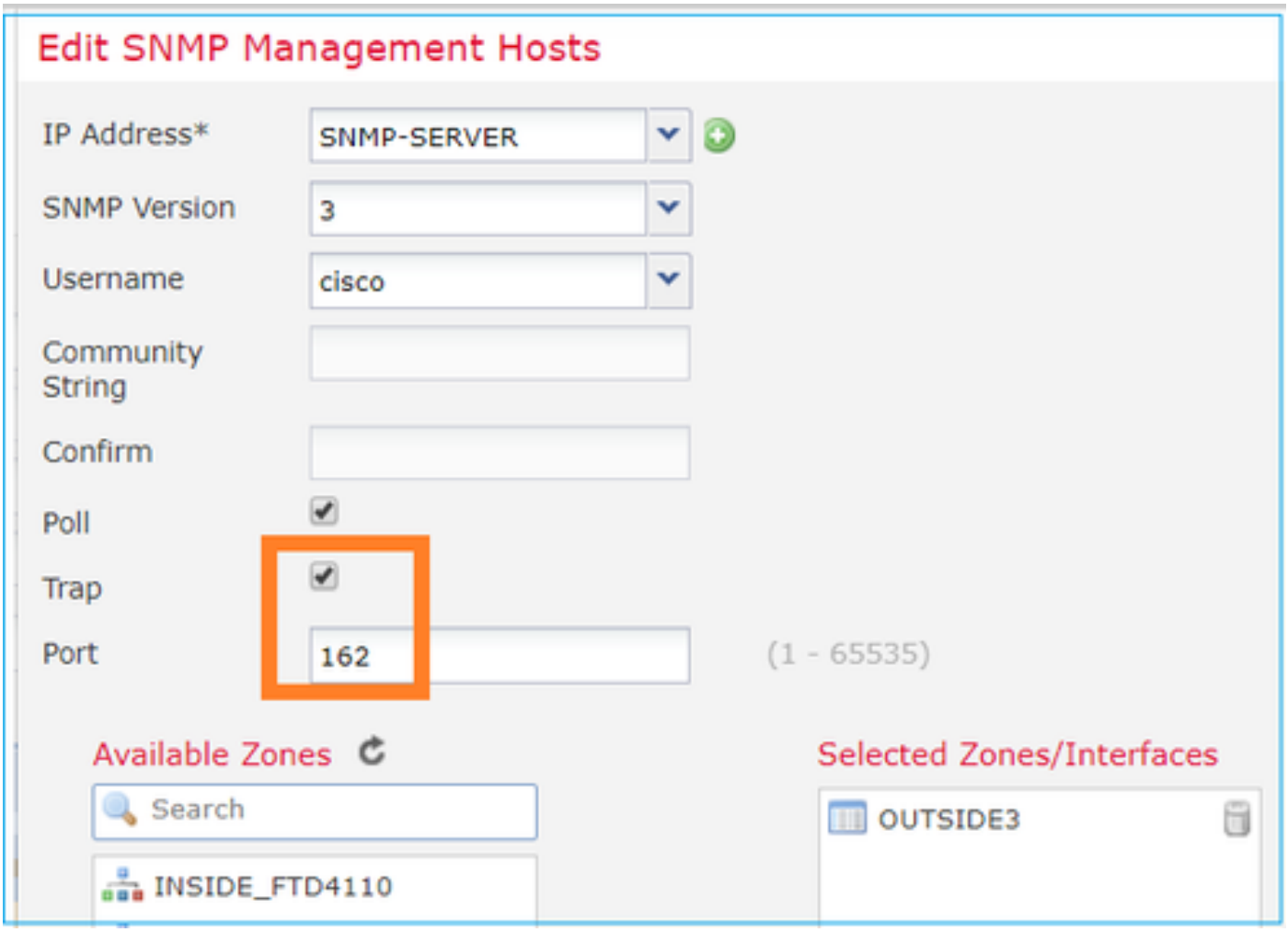
Configure LINA SNMPv3

Step 1. On FMC UI, navigate to **Devices > Platform Settings > SNMP.** Check the option **Enable SNMP Servers** and configure the SNMPv3 User and Host:

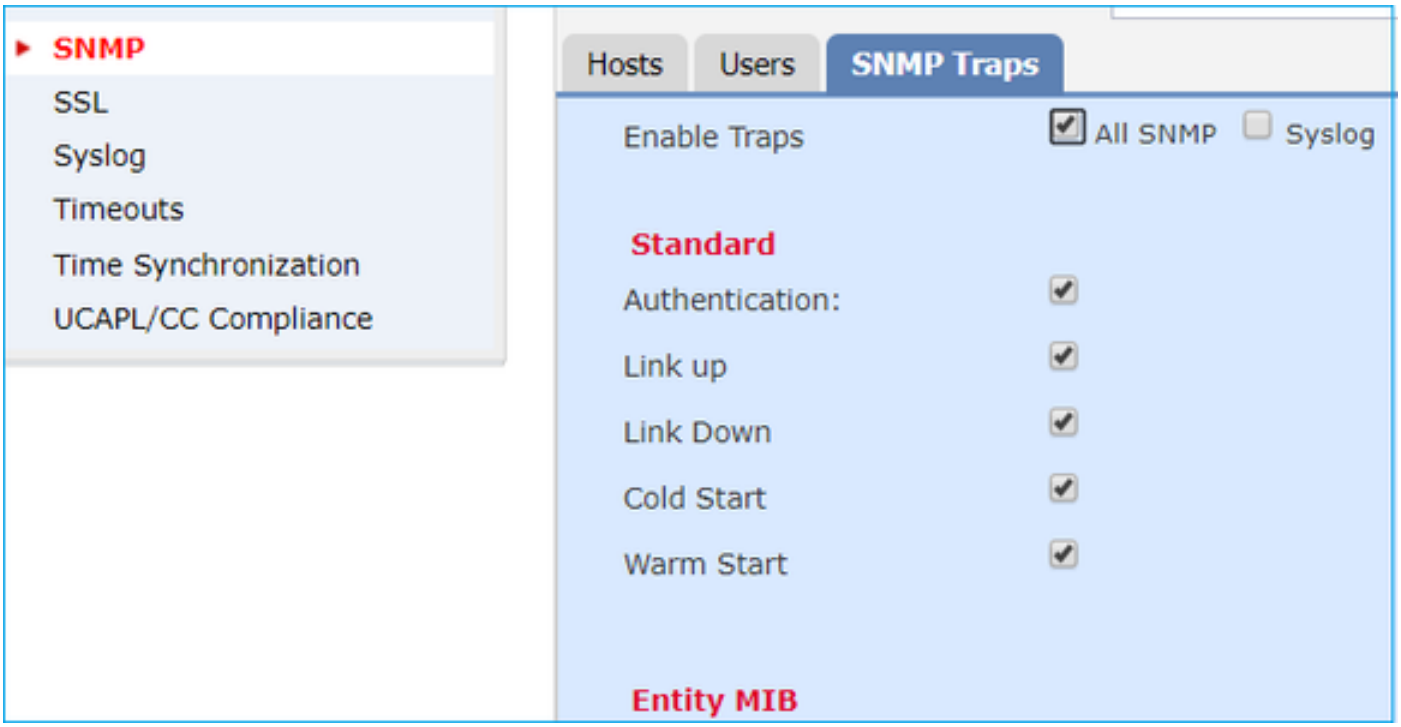




Step 2. Configure the host also to receive traps:



Step 3. The traps that you want to receive can be selected under **SNMP Traps** Section:



MIO Blade SNMP Unification (FXOS 2.12.1, FTD 7.2, ASA 9.18.1)

Pre-7.2 behavior

- On 9300 and 4100 platforms, the SNMP MIBs for Chassis information is not available on SNMP configured on FTD/ASA applications. It needs to be configured separately on the MIO in the chassis manager and accessed separately. MIO is the Management and I/O (Supervisor) module.
- Two separate SNMP policies need to be configured, one on Blade/App and the other on MIO for SNMP monitoring.
- Separate ports are utilized, one for Blade and the other for MIO for SNMP monitoring of the same device.
- This can create complexity when you try to configure and monitor 9300 and 4100 devices via SNMP.

How it Works on newer releases (FXOS 2.12.1, FTD 7.2, ASA 9.18.1 and above)

- With MIO Blade SNMP unification, users can poll LINA and MIO MIBs via the Application (ASA/FTD) interfaces.
- The feature can be enabled or disabled via the new MIO CLI and FCM (Chassis Mgr) UI.
- The default status is disabled. This means that the MIO SNMP agent is running as a standalone instance. MIO interfaces need to be used to poll chassis/DME MIBs. Once the feature is enabled, the application interfaces can be used to poll the same MIBs.
- The configuration is available on the Chassis Manager UI under the **Platform-settings > SNMP > Admin Instance**, where the user can specify the FTD instance that would collate/gather the chassis MIBs to present it to the NMS
- ASA/FTD native and MI applications are supported.
- This feature is applicable only to MIO-based platforms (FPR9300 and FPR4100).

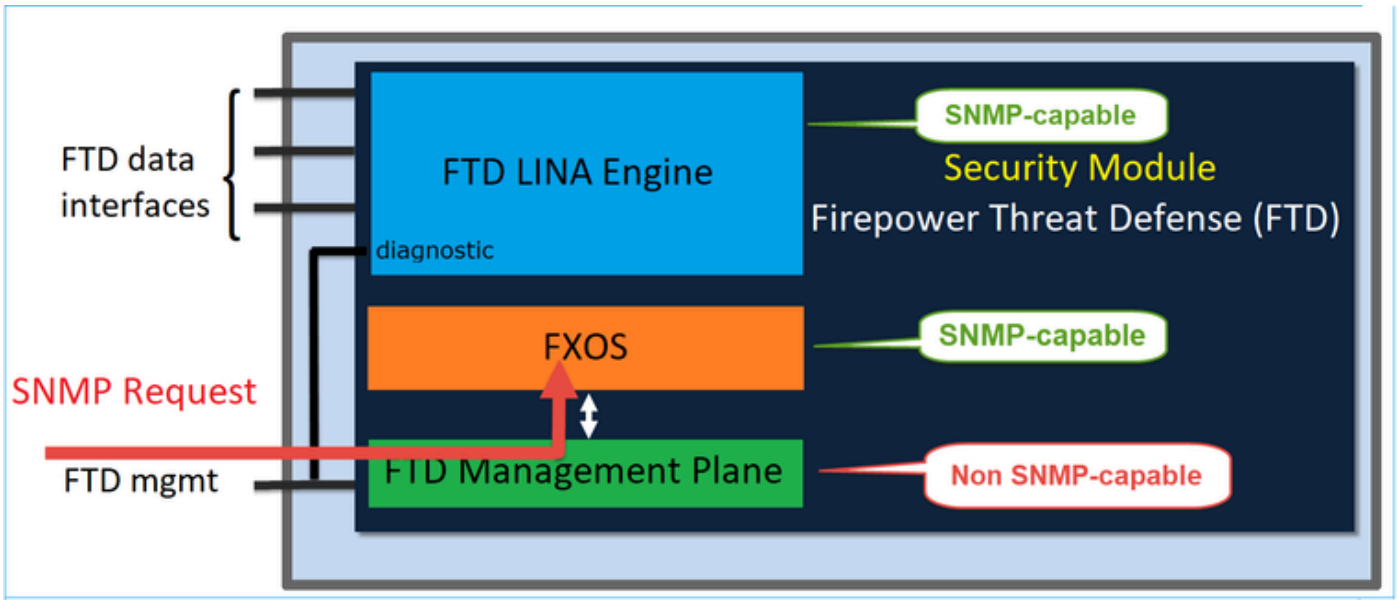
Prerequisites, Supported Platforms

- Min Supported Manager Version: FCM 2.12.1
- Managed Devices: FPR9300 / FP4100 Series
- Min Supported Managed Device Version Required: FXOS 2.12.1, FTD 7.2 or ASA 9.18.1

SNMP in FPR2100

On FPR2100 systems, there is no FCM. The only way to configure SNMP is via FMC.

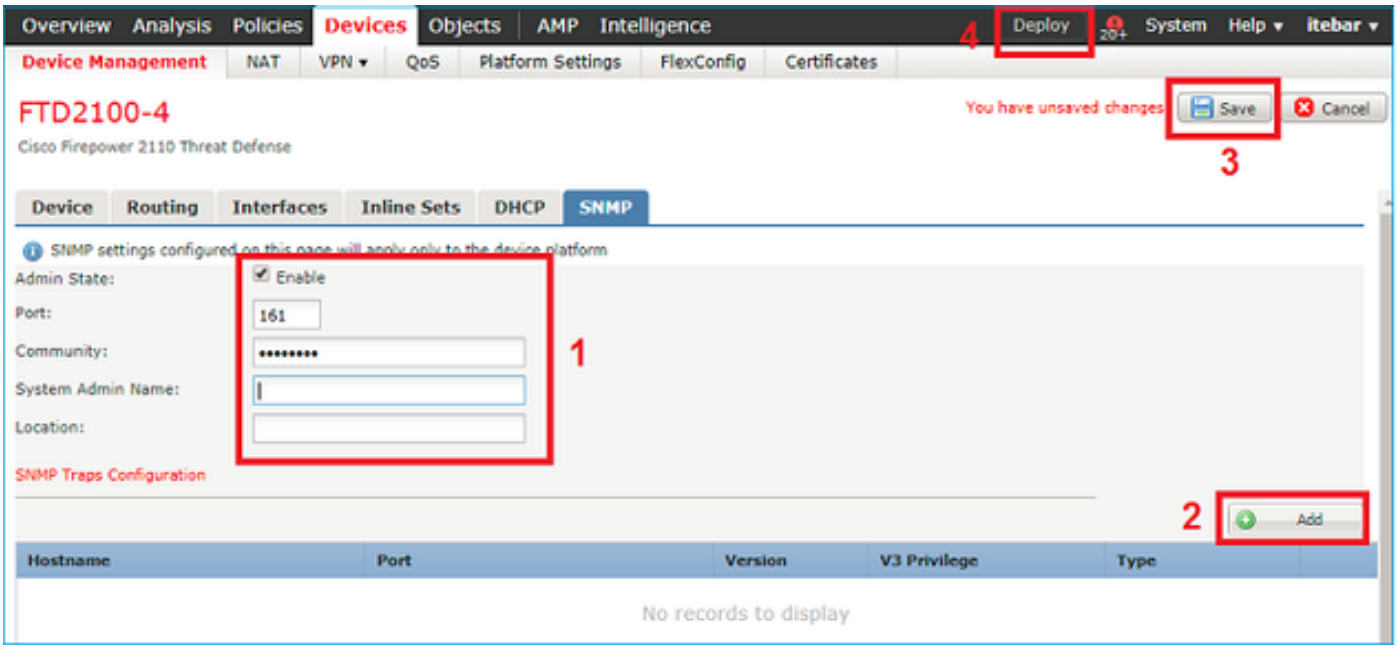
Chassis (FXOS) SNMP on FPR2100

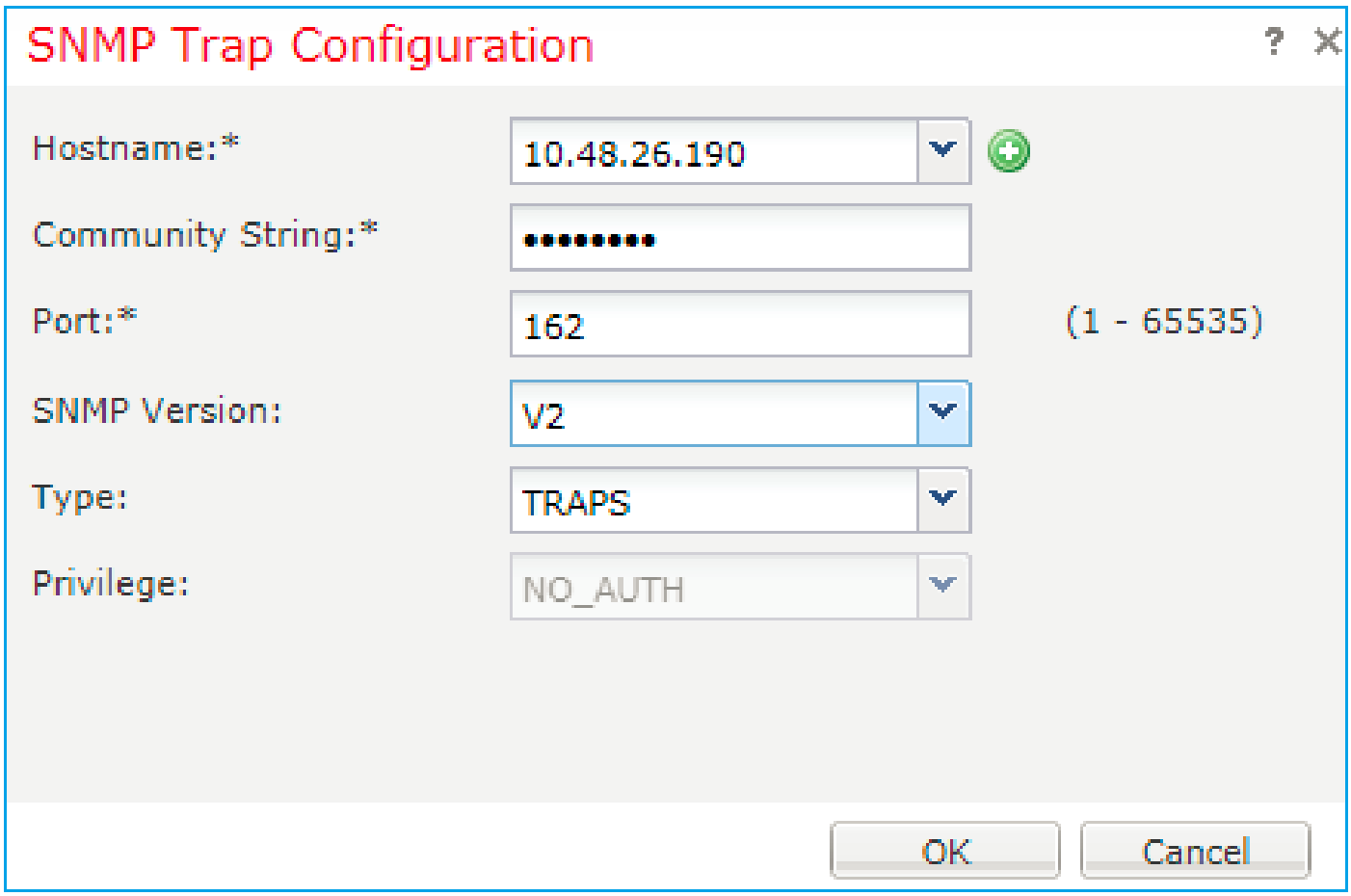


As from FTD 6.6+ you have also the option to use the FTD management interface for SNMP. In this case, both FXOS and LINA SNMP info are transferred through the FTD management interface.

Configure FXOS SNMPv1/v2c

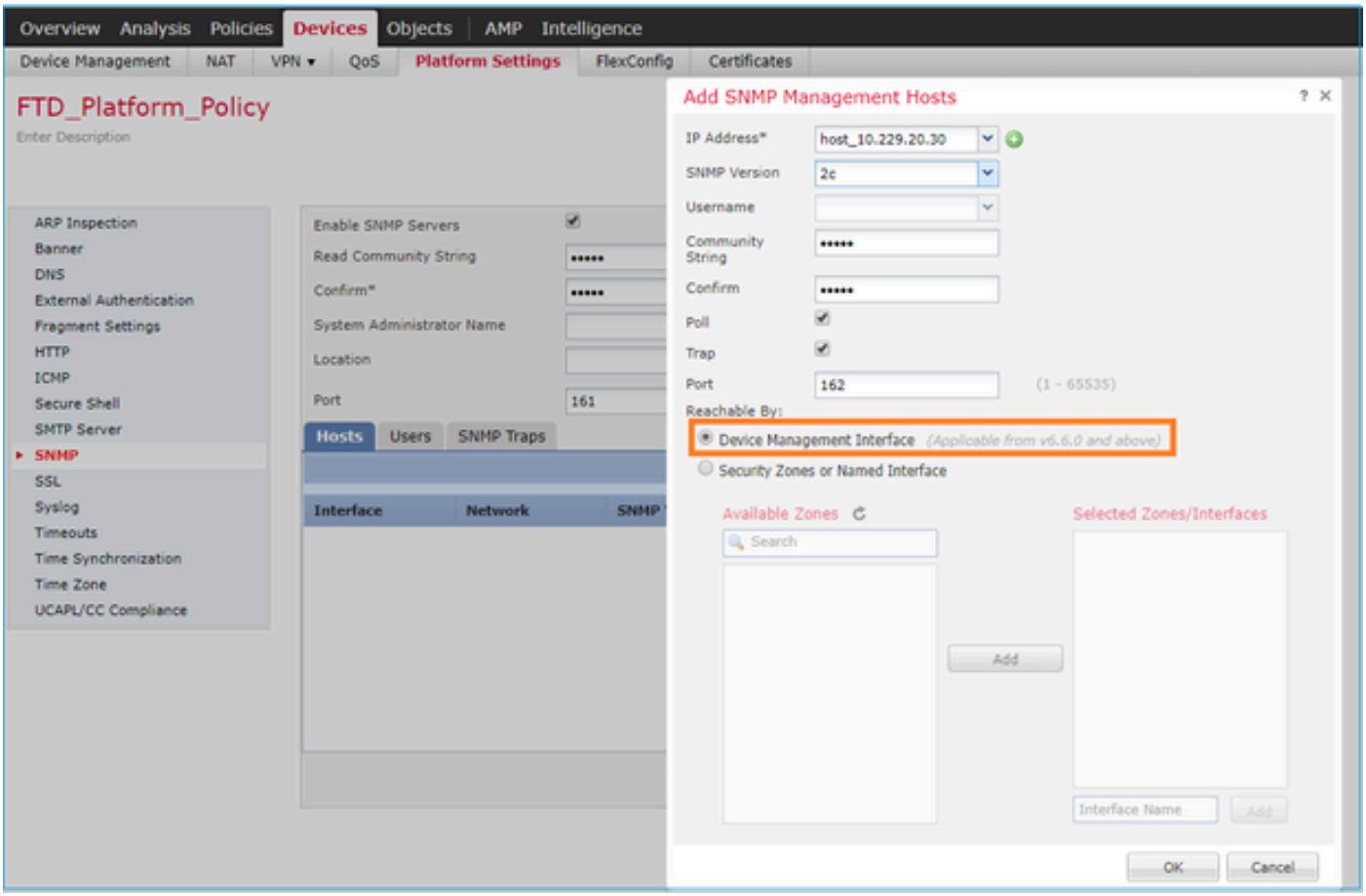
Open FMC UI and navigate to **Devices > Device Management.** Select the device and select **SNMP**:





Change in FTD 6.6+

You can specify the FTD management interface:

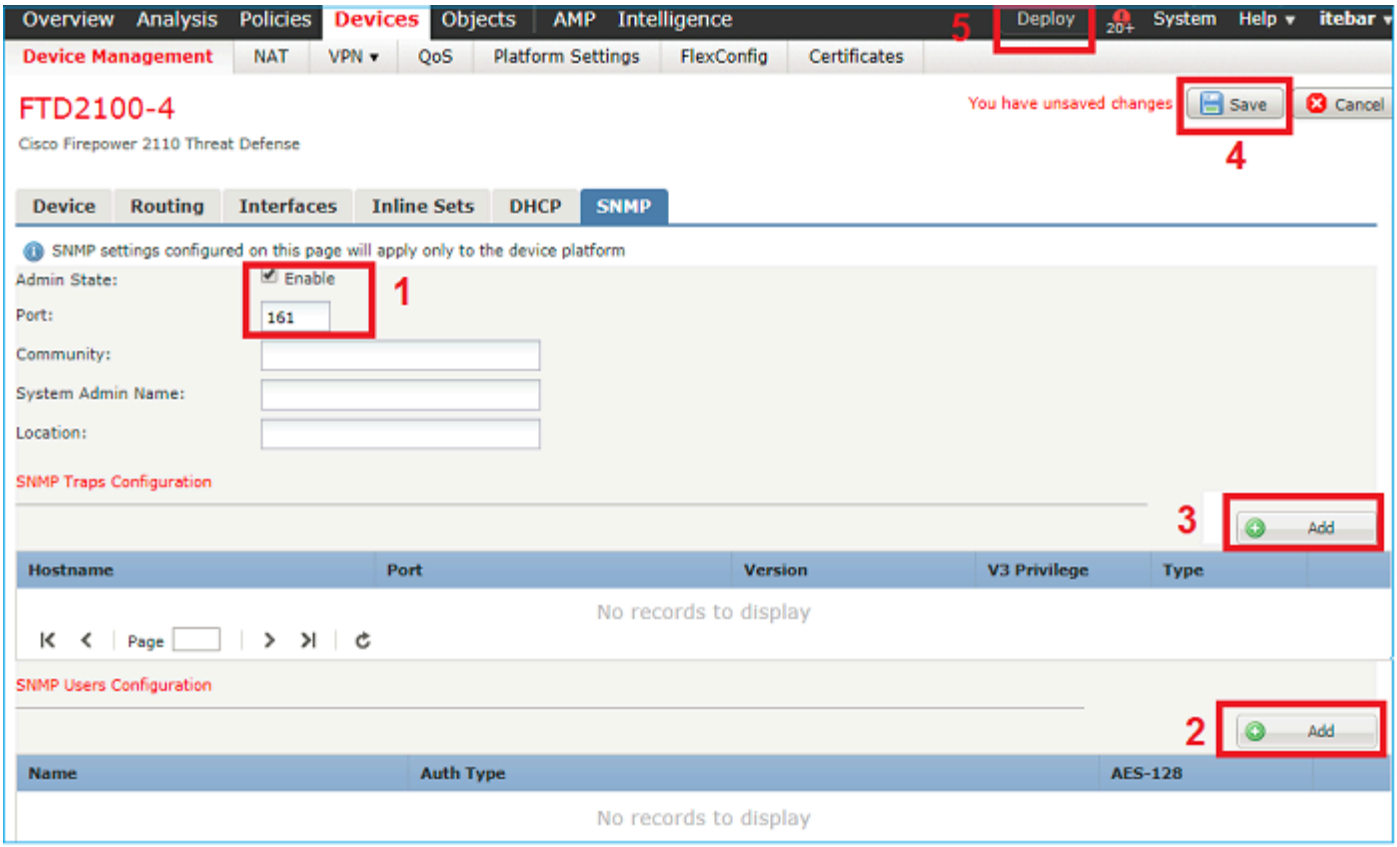


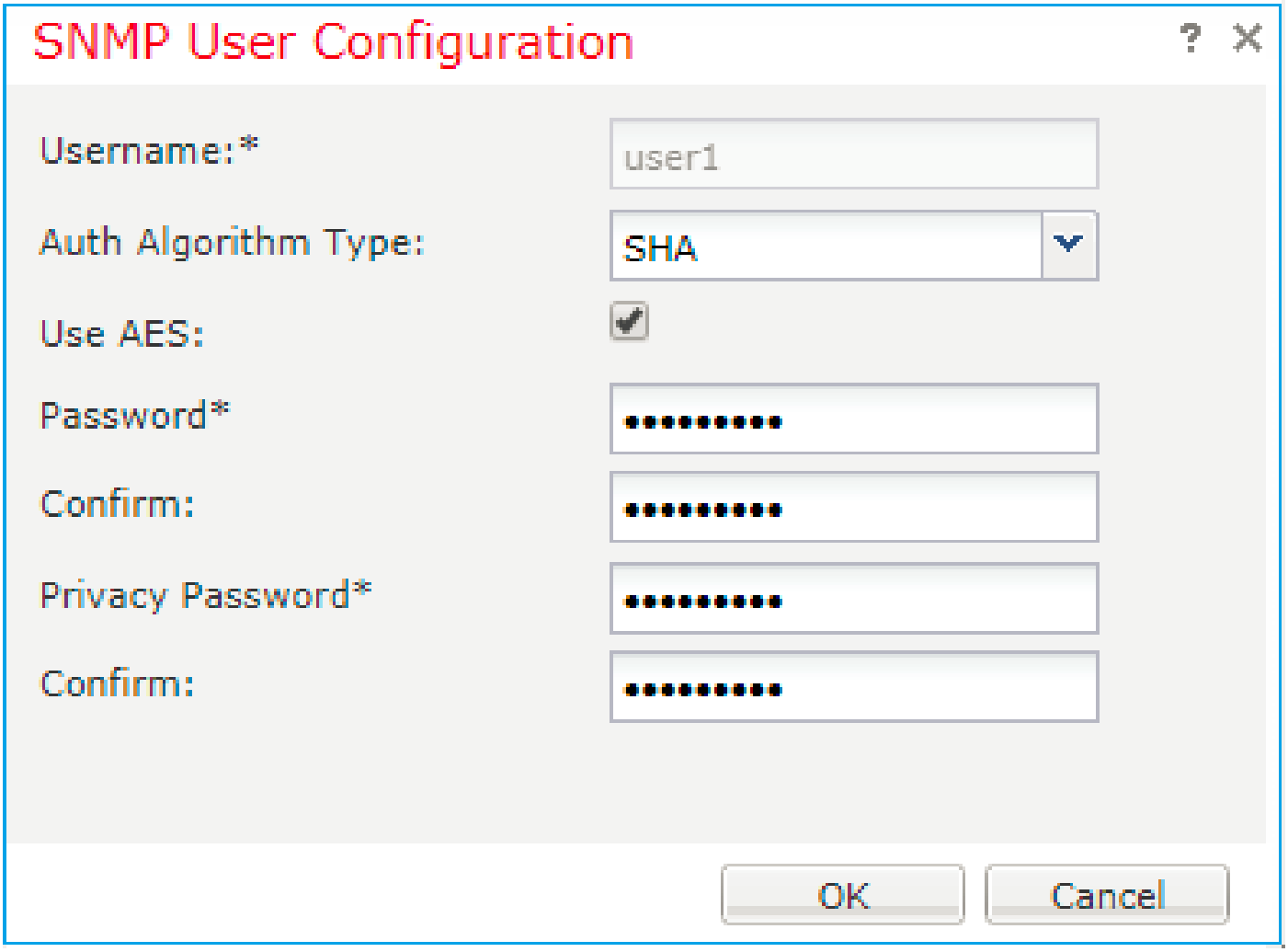
Since the management interface can be also configured for SNMP the page shows this Warning message.

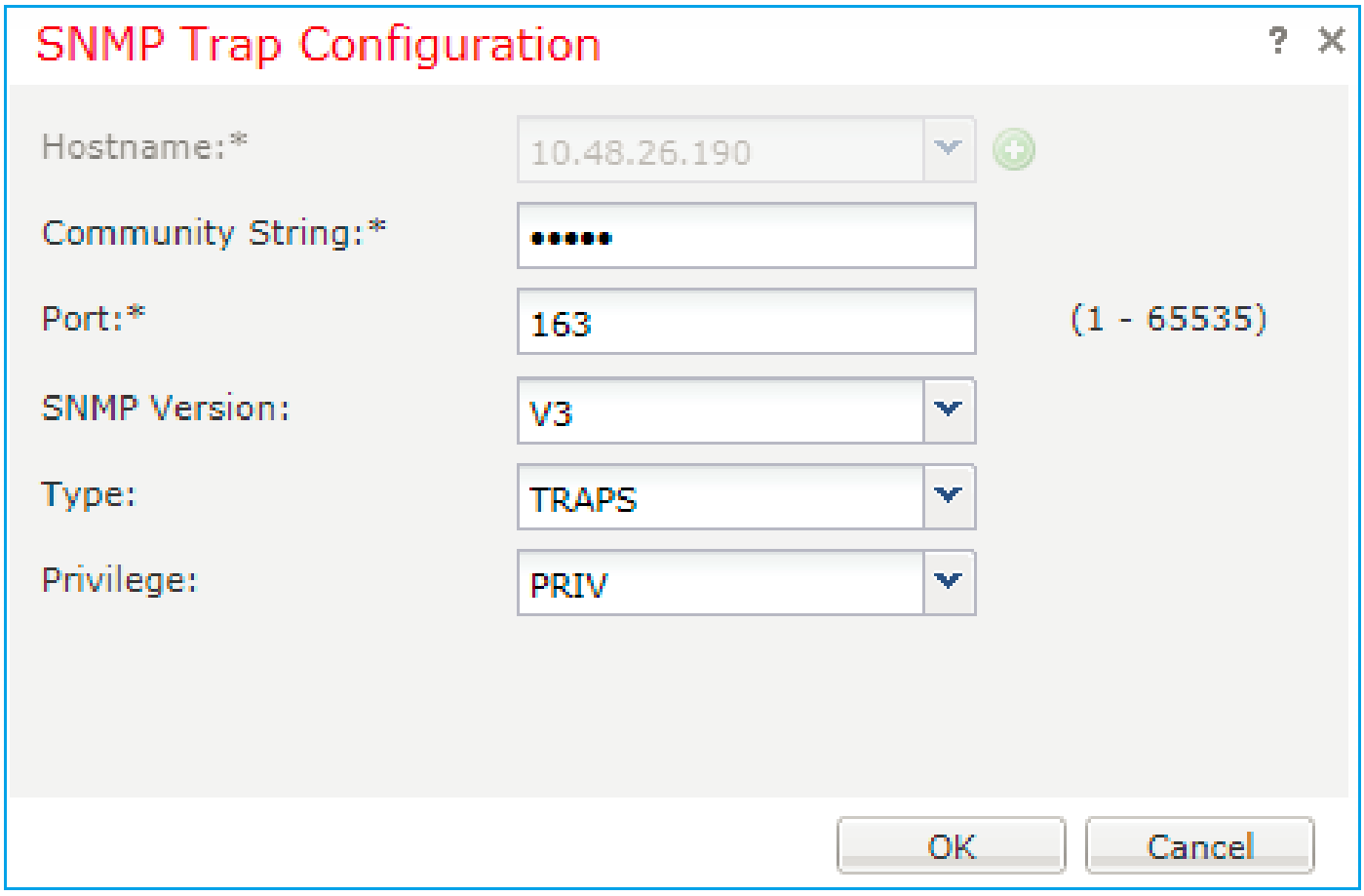
The device platform SNMP configuration on this page is disabled, if SNMP settings configured with Device Management Interface through **Devices > Platform Settings (Threat Defense) > SNMP > Hosts**.

Configure FXOS SNMPv3

Open FMC UI and navigate to **Choose Devices > Device Management.** Choose the device and select **SNMP**.

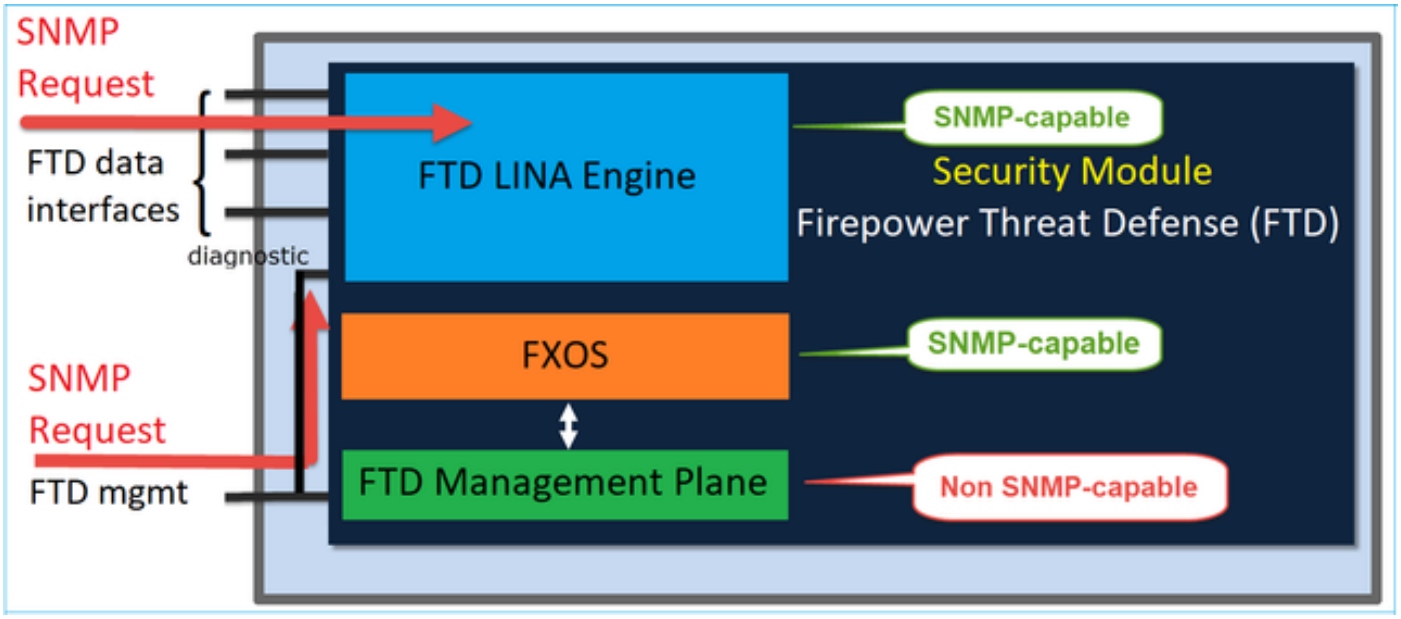

Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
5
Deploy
System
Help
itebar
Device Management
NAT
VPN
QoS
Platform Settings
FlexConfig
Certificates
FTD2100-4
Cisco Firepower 2110 Threat Defense
You have unsaved changes
Save
Cancel
4
Device
Routing
Interfaces
Inline Sets
DHCP
SNMP
SNMP settings 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
Page
SNMP Users Configuration
2
Add
Name
Auth Type
AES-128
No records to display


SNMP User Configuration
Username:*
user1
Auth Algorithm Type:
SHA
Use AES:
Password*
Confirm:
Privacy Password*
Confirm:
OK
Cancel



FTD (LINA) SNMP on FPR2100

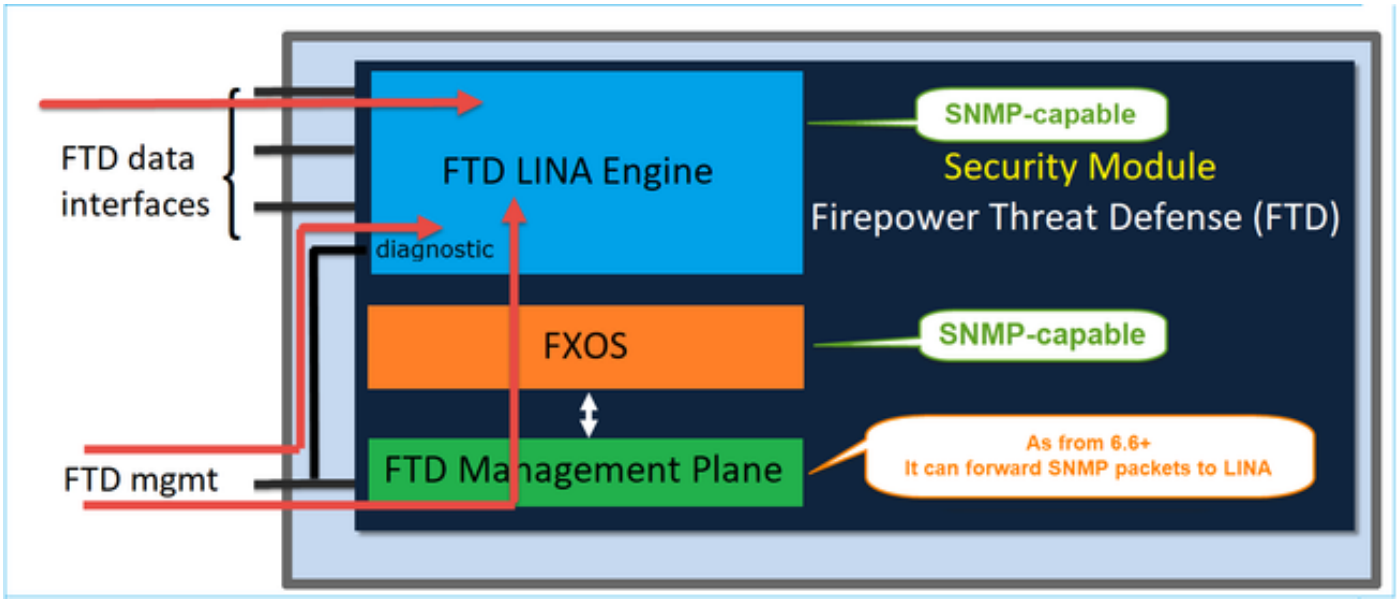
- For pre-6.6 releases, the LINA FTD SNMP configuration on FTD FP1xxx/FP21xx appliances is identical to an FTD on Firepower 4100 or 9300 appliance.

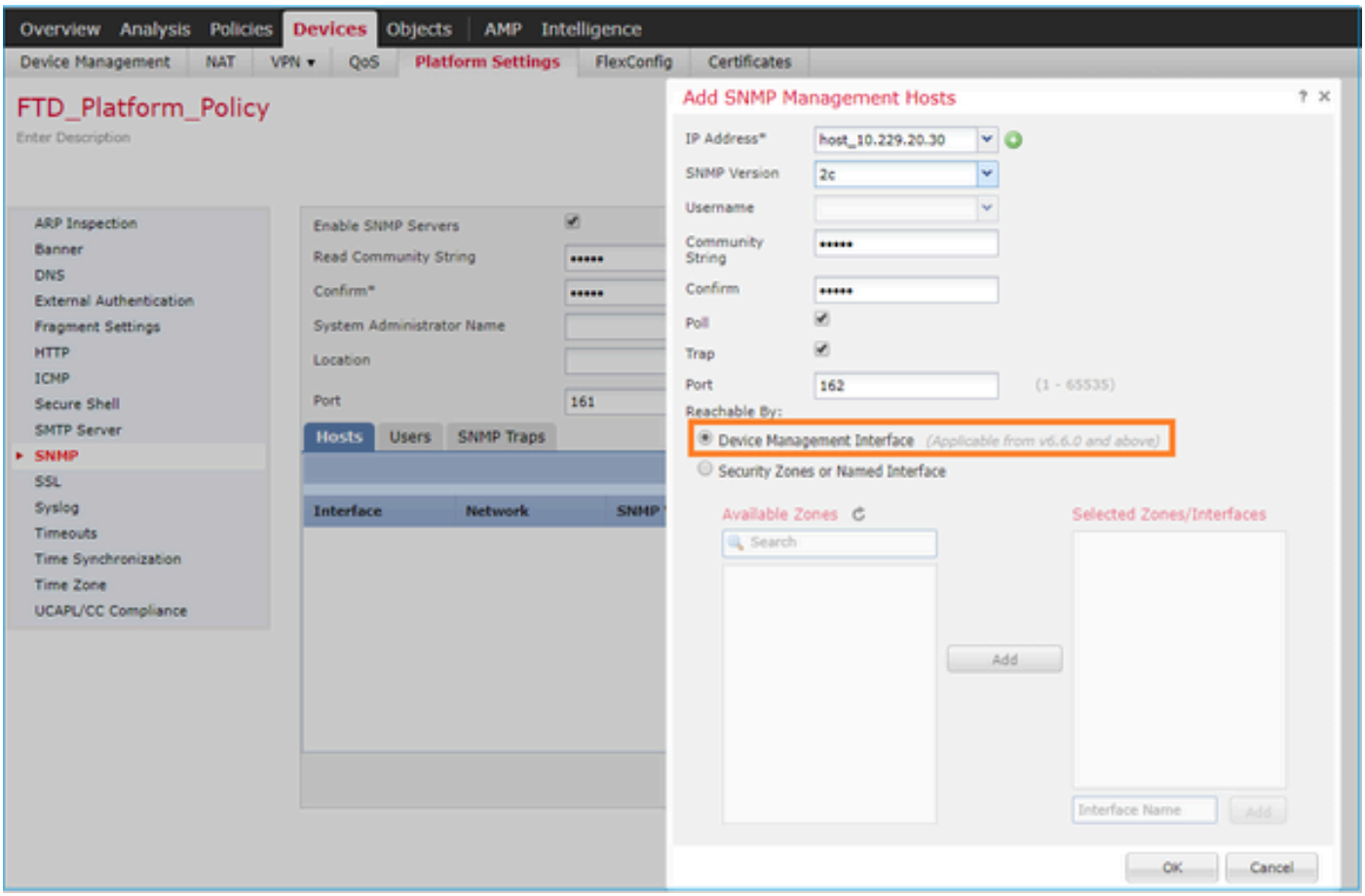


FTD 6.6+ Releases

- In post-6.6 releases, you have also the option to use the FTD management interface for LINA polls

and traps.

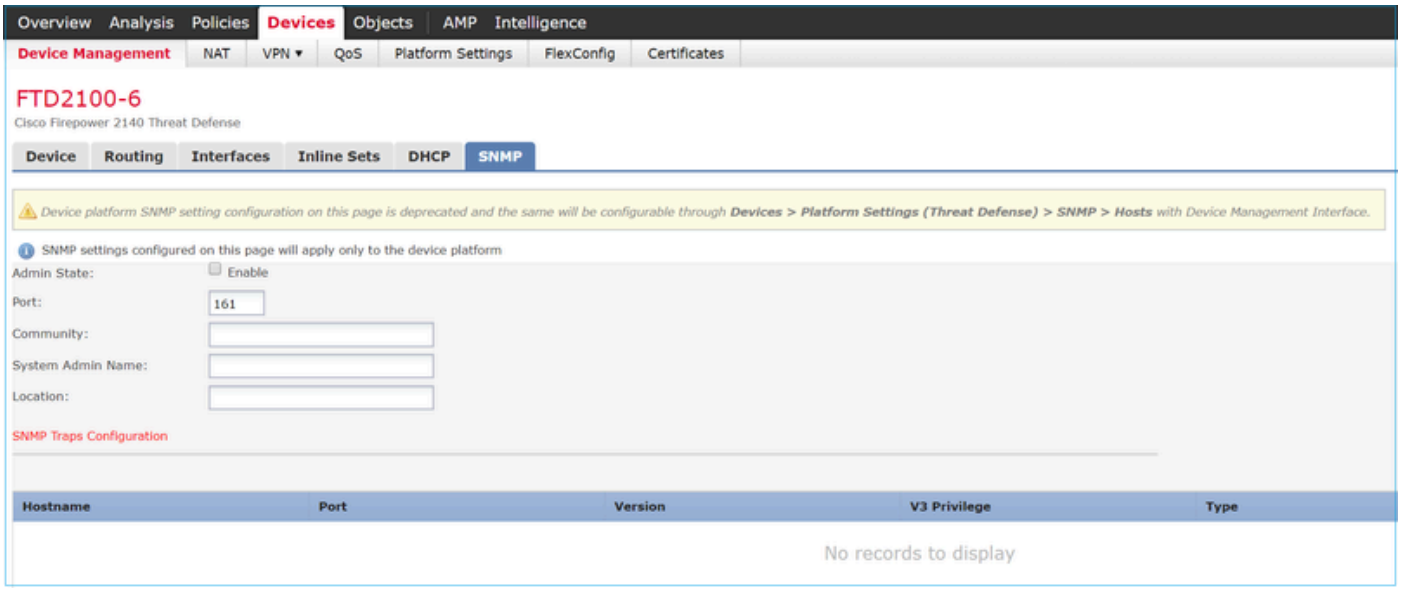




If the new management interface is selected:

- LINA SNMP is available over the Management interface.
- Under **Devices > Device Management**, the **SNMP** tab is disabled as it is no longer required. A notification banner is shown. The SNMP device tab was visible only on 2100/1100 platforms. This page does not exist on FPR9300/FPR4100 and FTD55xx platforms.

Once configured, a combined LINA SNMP + FXOS (on FP1xxx/FP2xxx) SNMP poll/trap info is over FTD management interface.



The SNMP Single IP management feature is supported from 6.6 onwards on all FTD platforms:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 that runs FTD
- FTDv

For more details check Configure SNMP for Threat Defense

Verify

Verify FXOS SNMP for FPR4100/FPR9300

FXOS SNMPv2c Verifications

CLI configuration verification:

<#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
```

From the FXOS mode:

```
<#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
```

Additional verifications:

```
<#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

...
```

1. Test SNMP Requests.
2. Perform an SNMP request from a valid host.
3. Confirm Trap Generation.

You can use flap an interface with ethanalyzer enabled to confirm that SNMP traps are generated and sent to

the trap hosts defined:

```
<#root>

ksec-fpr9k-1-A(fxos)#

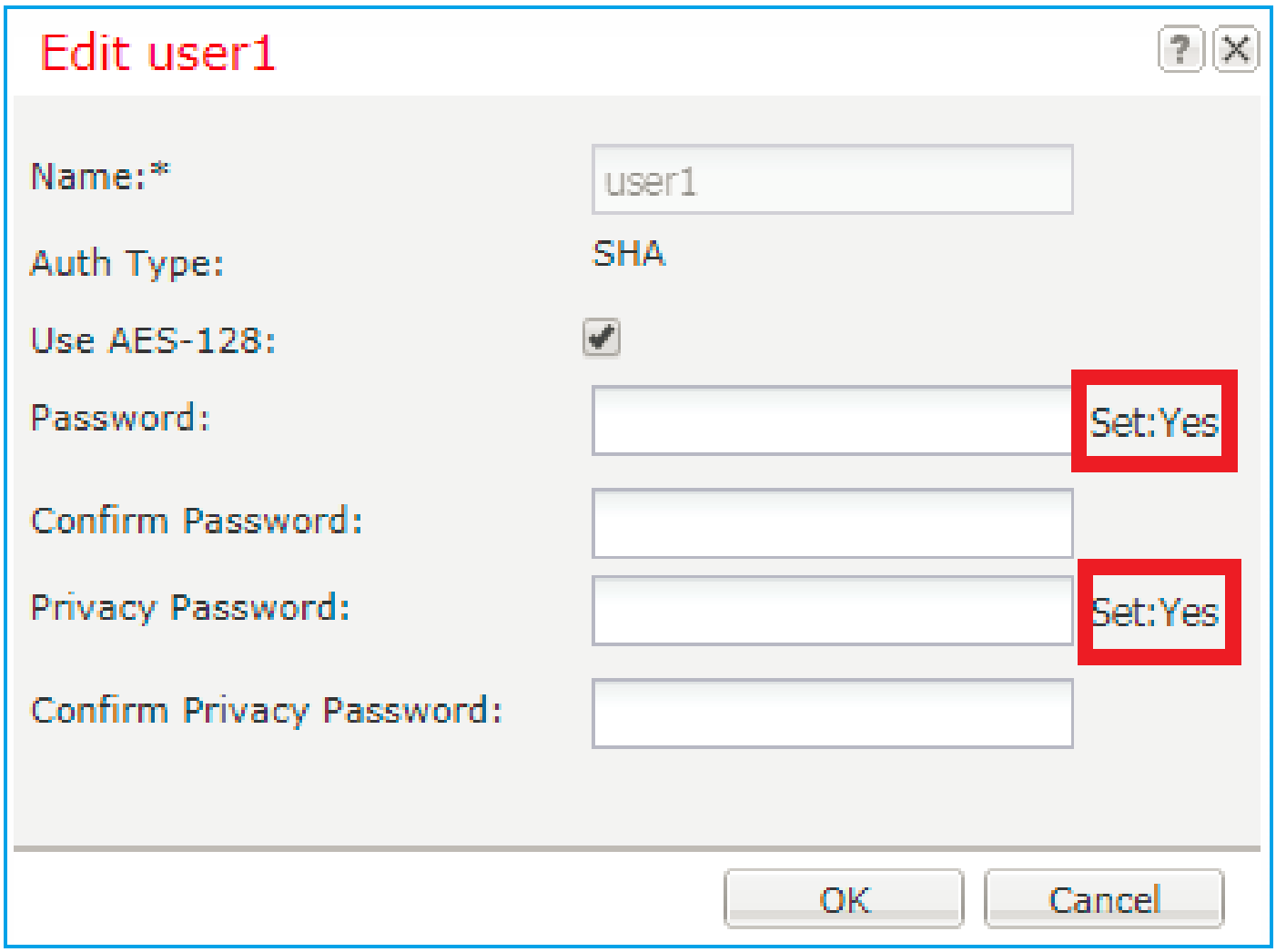
ethanalyzer local interface mgmt capture-filter "udp port 162"

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
```

Warning: An interface flap can cause a traffic outage. Do this test only in a lab environment or in a maintenance window.

FXOS SNMPv3 Verifications

Step 1. Open the FCM UI **Platform Settings > SNMP > User** shows if there is any password and privacy password configured:



Step 2. In the CLI, you can verify the SNMP configuration under scope **monitoring**:

```
<#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
```

Step 3. Under FXOS mode, you can expand the SNMP configuration and details:

```
<#root>

ksec-fpr9k-1-A(fxos)#

show running-config snmp all

…
snmp-server user user1 network-operator auth sha 0x022957ee4690a01f910f1103433e4b7b07d4b5fc priv aes-12
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
-------------------------------------------------------------------------
```

1. Test SNMP Requests.
2. Verify the configuration and do an SNMP request from any device with SNMP capabilities.

To check how the SNMP request is processed, you can use SNMP debug:

<#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 0.000
2017 Oct 16 17:11:54.683952 snmpd: 1281064976.000000:iso.10.10.1.2.10.10.10.10.2.83886080 = STRING: "mgm
2017 Oct 16 17:11:54.684370 snmpd:  SNMPPKTSTRT: 3.000000 162 1281064976.000000 1647446526.000000 0.000
```

⚠ Caution: A debug can impact the device performance.

Verify FXOS SNMP for FPR2100

FXOS SNMPv2 Verifications

Check the configuration in the CLI:

<#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
```

1. Confirm the SNMP Behavior.
2. Verify that you are able to poll the FXOS and send an SNMP request from a host or any device with SNMP capabilities.

Use the **capture-traffic** command to see the SNMP request and response:

```
<#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 Verifications

Check the configuration in the CLI:

```
<#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
```

1. Confirm the SNMP Behavior.
2. Send an SNMP request to verify that you are able to poll the FXOS.

Additionally, you can capture the request:

<#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
```

Verify FTD SNMP

To verify the FTD LINA SNMP configuration:

<#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 *****
```

In post-6.6 FTD, you can configure and use the FTD management interface for 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
```

Additional verification:

<#root>

```
Firepower-module1#
```

```
show snmp-server host
```

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

From the SNMP Server CLI run a **snmpwalk** command:

<#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
...
```

Verification of the SNMP traffic statistics.

<#root>

```
Firepower-module1#
```

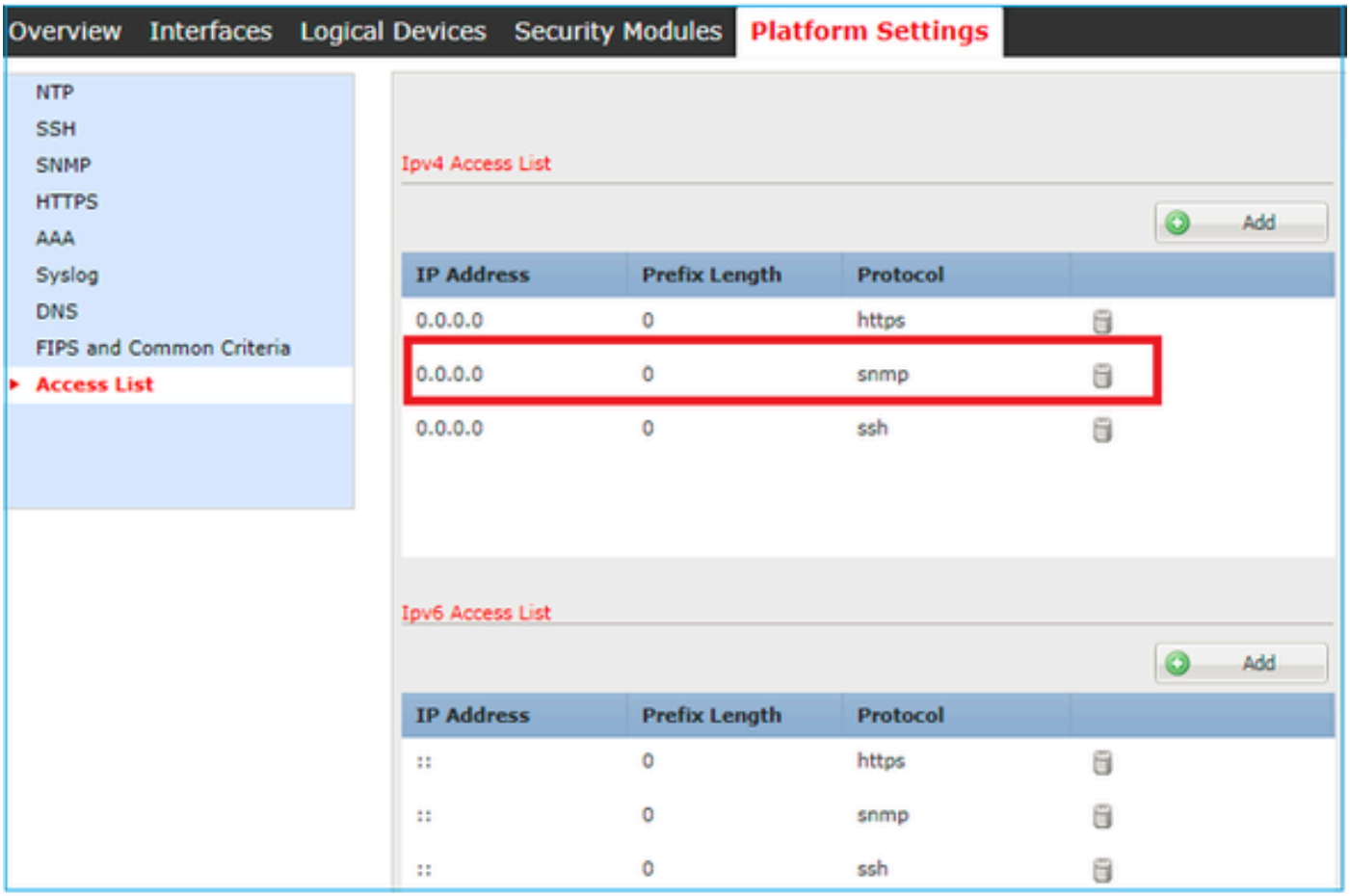
```
show snmp-server statistics
```

```
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
```

Allow SNMP Traffic to FXOS on FPR4100/FPR9300

FXOS configuration on FPR4100/9300 can restrict SNMP access per source IP address. The Access List configuration section defines which networks/hosts are able to reach the device via SSH, HTTPS or SNMP. You need to ensure that SNMP queries from your SNMP server are allowed.

Configure Global Access-list in the GUI



Configure Global Access-list in the CLI

<#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
```

Verification

<#root>

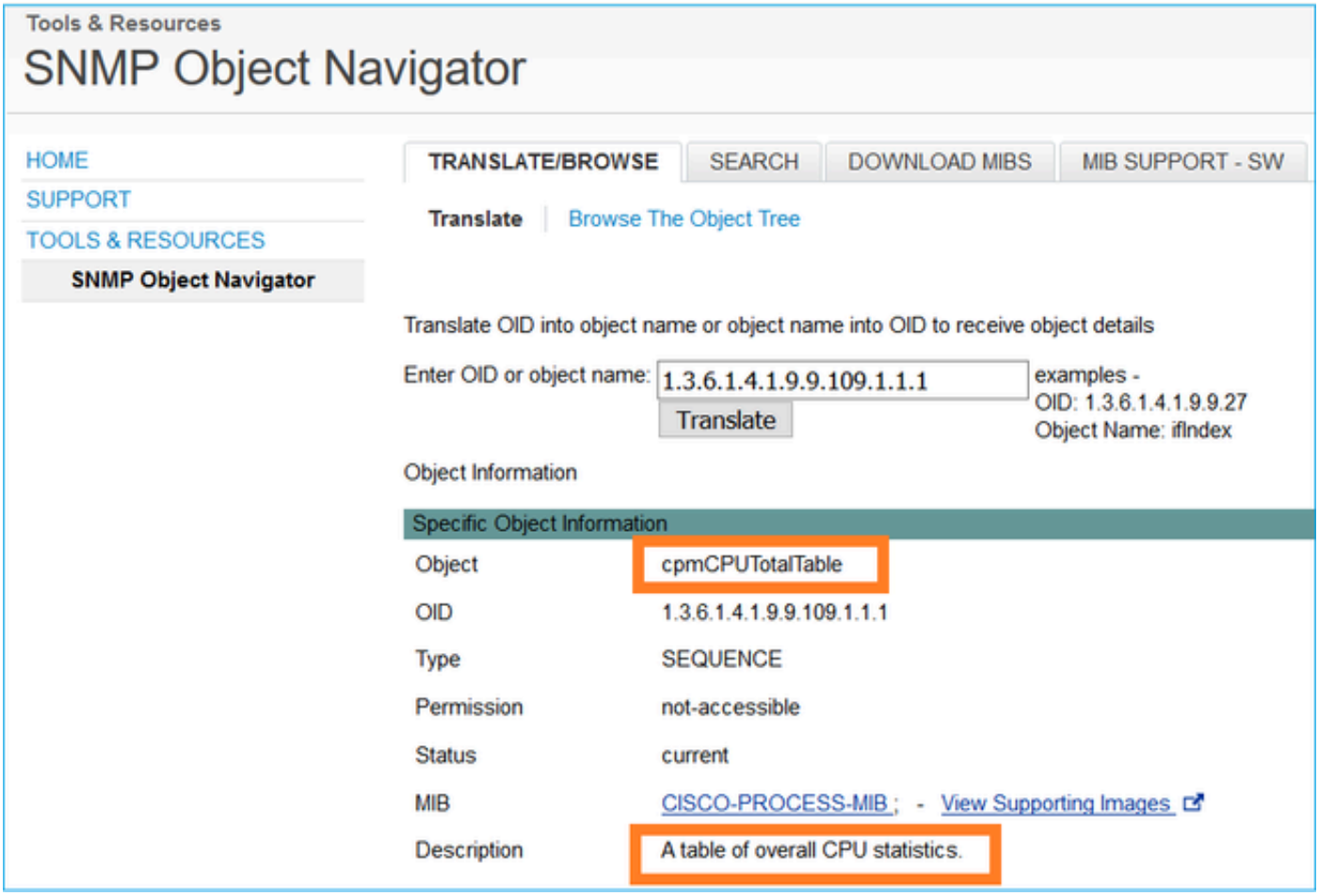
```
ksec-fpr9k-1-A /system/services #
```

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
```

Use the OID Object Navigator

Cisco SNMP Object Navigator is an online tool that lets you translate the different OIDs and get a short description.



Use the command **show snmp-server oid** from the FTD LINA CLI to retrieve the whole list of LINA OIDs that can be polled.

<#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#
```

Note: The command is hidden.

Troubleshoot

These are the most common SNMP case generators seen by Cisco TAC:

- Unable to Poll FTD LINA SNMP
- Unable to Poll FXOS SNMP
- What SNMP OID Values to Use?
- Cannot Get SNMP Traps
- Cannot Monitor FMC via SNMP
- Unable to Configure SNMP
- SNMP Config on Firepower Device Manager

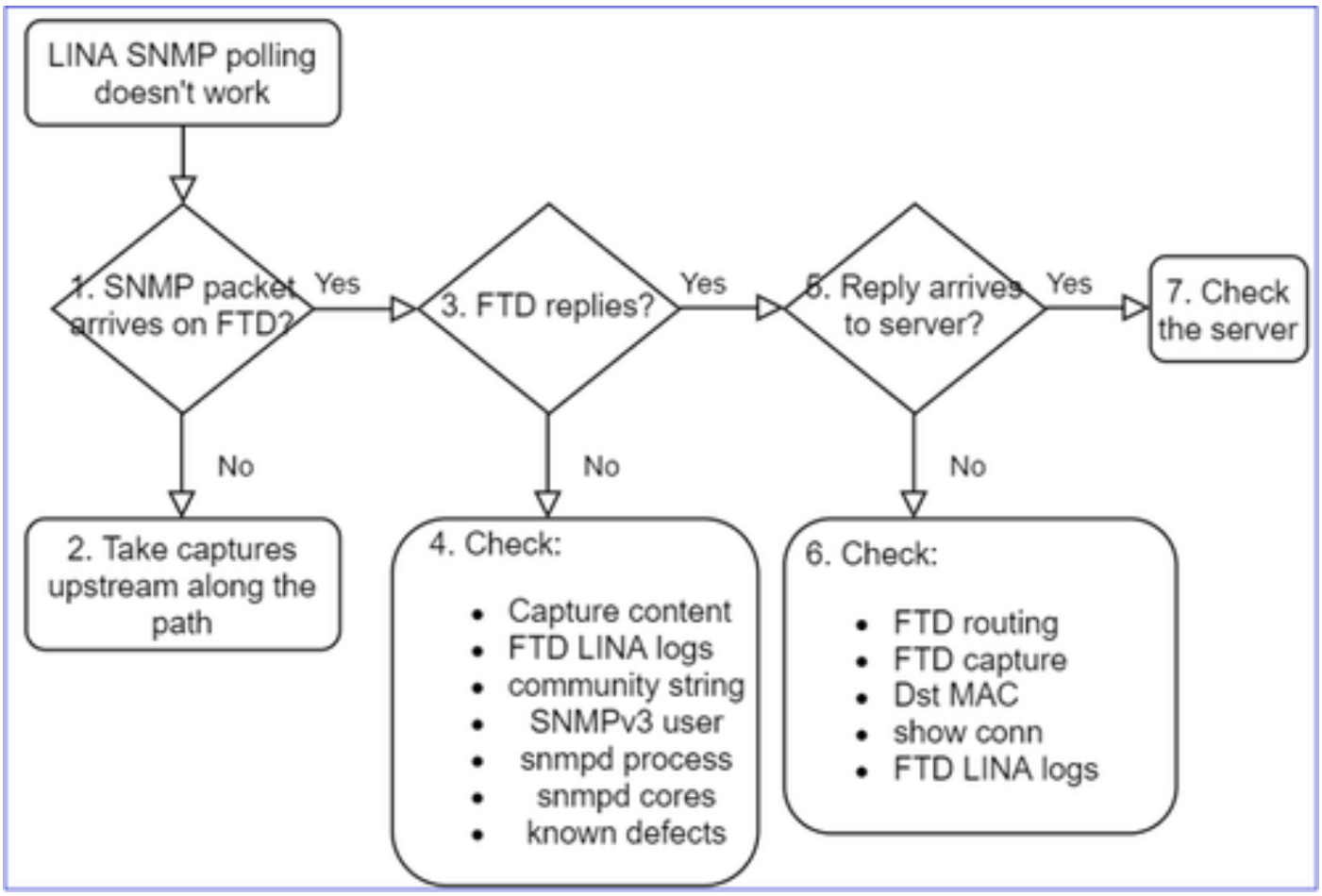
Unable to Poll FTD LINA SNMP

Problem Descriptions (sample from real Cisco TAC cases):

- "Unable to fetch data over SNMP."
- "Unable to poll device over SNMPv2."
- "SNMP does not work. We want to monitor the firewall with SNMP but after the configuration, we face issues."
- "We have two monitoring systems that are not able to monitor the FTD via SNMP v2c or 3."
- "SNMP walk does not work on the firewall."

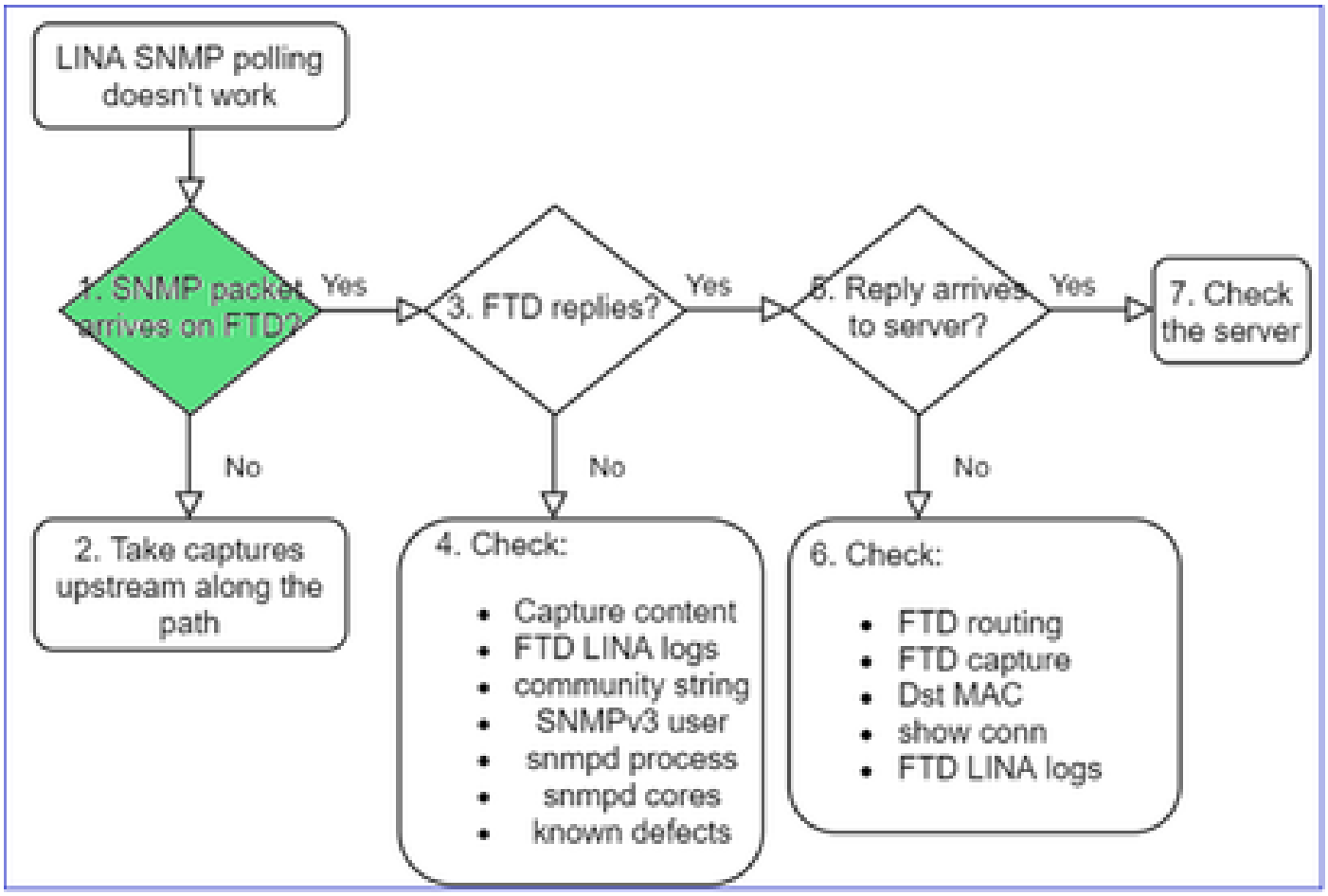
Recommendation on how to Troubleshoot

This is recommended process to troublshoot flowchart for LINA SNMP poll issues:



Deep dive

1. Does SNMP packet arrive on FTD?



- Enable captures to verify the SNMP packet arrival.

SNMP on FTD mgmt interface (post-6.6 release) uses the management keyword:

```
<#root>
firepower#
show run snmp-server

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

SNMP on FTD data interfaces uses the name of the interface:

```
<#root>
firepower#
show run snmp-server

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

Capture on FTD mgmt interface:

<#root>

>

capture-traffic

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

1

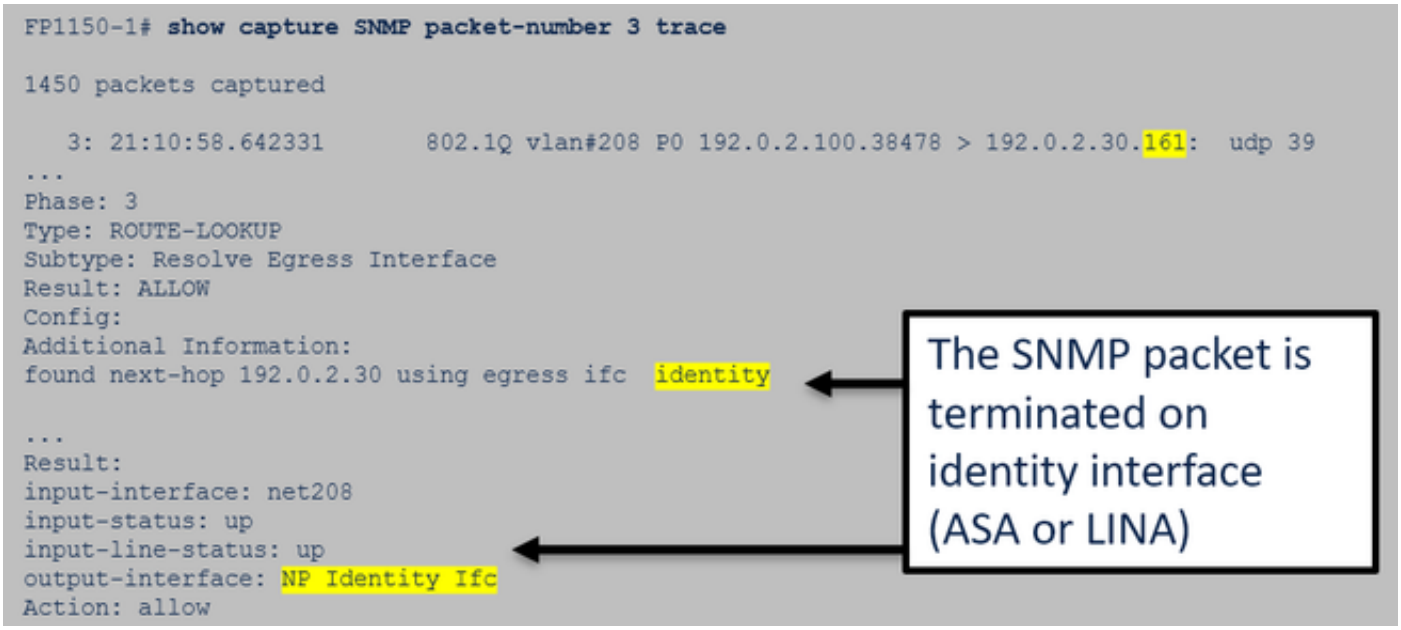
Capture on FTD data interface:

<#root>

```
firepower#
```

capture SNMP interface net201 trace match udp any any eq 161

FTD data interface packet trace (pre 6.6/9.14.1):



FTD data interface packet trace (post 6.6/9.14.1):

```
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:
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
```

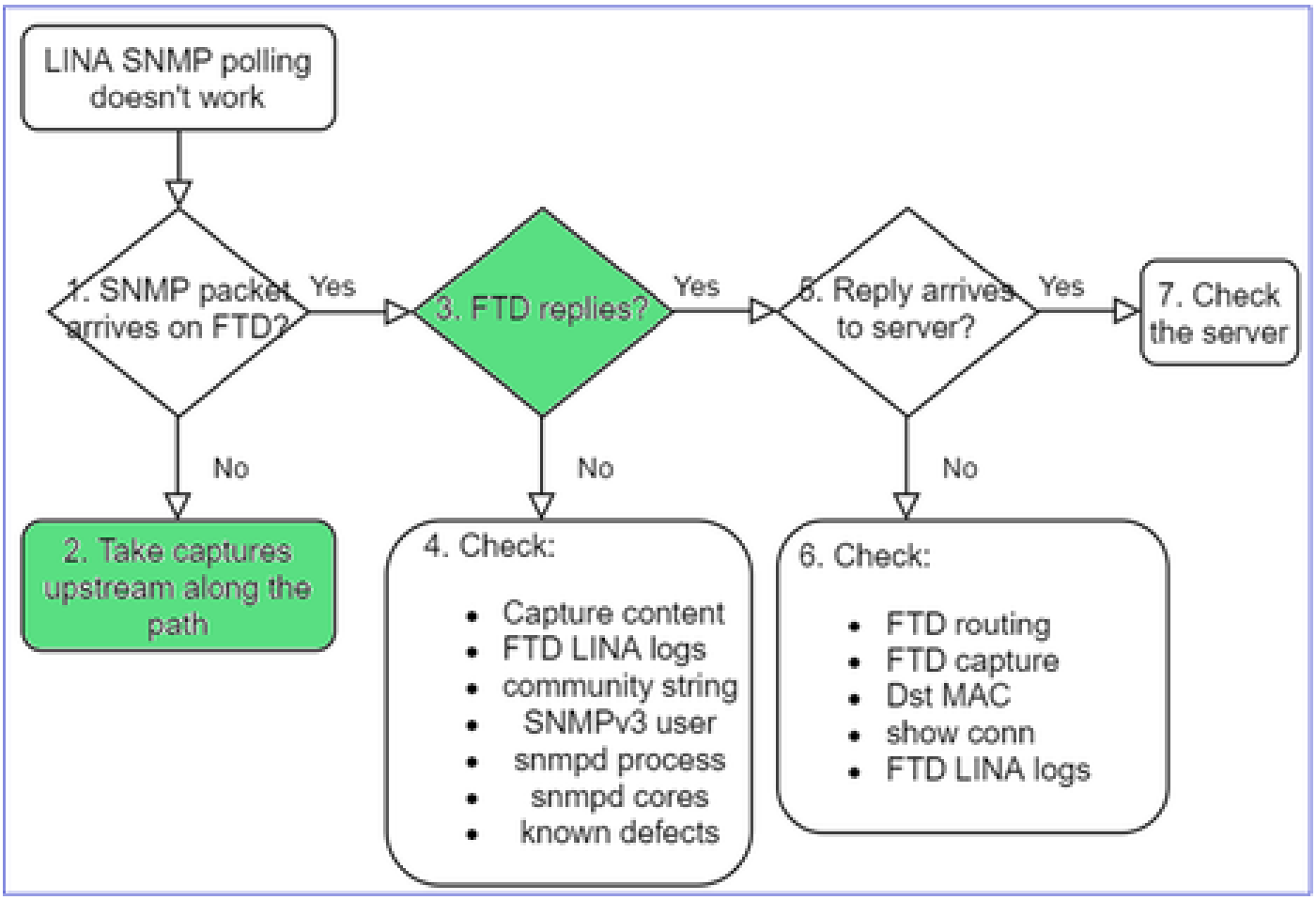
NAT diverts the packet to Snort engine
(NLP – Non-Lina Process tap interface)

2. In case you do not see SNMP packets in the FTD ingress captures:

a. Take captures upstream along the path.

b. Ensure that the SNMP server uses the proper FTD IP.

c. Start from the switchport that faces the FTD interface and move upstream.



3. Do you see FTD SNMP replies?

To verify if the FTD replies, check FTD egress capture (LINA or mgmt interface).

To do so, check for SNMP packets with source port 161:

<#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
```

In post-6.6/9.14.1 releases, you have one additional capture point: Capture on the NLP tap interface. The NATed IP is from the 162.254.x.x range:

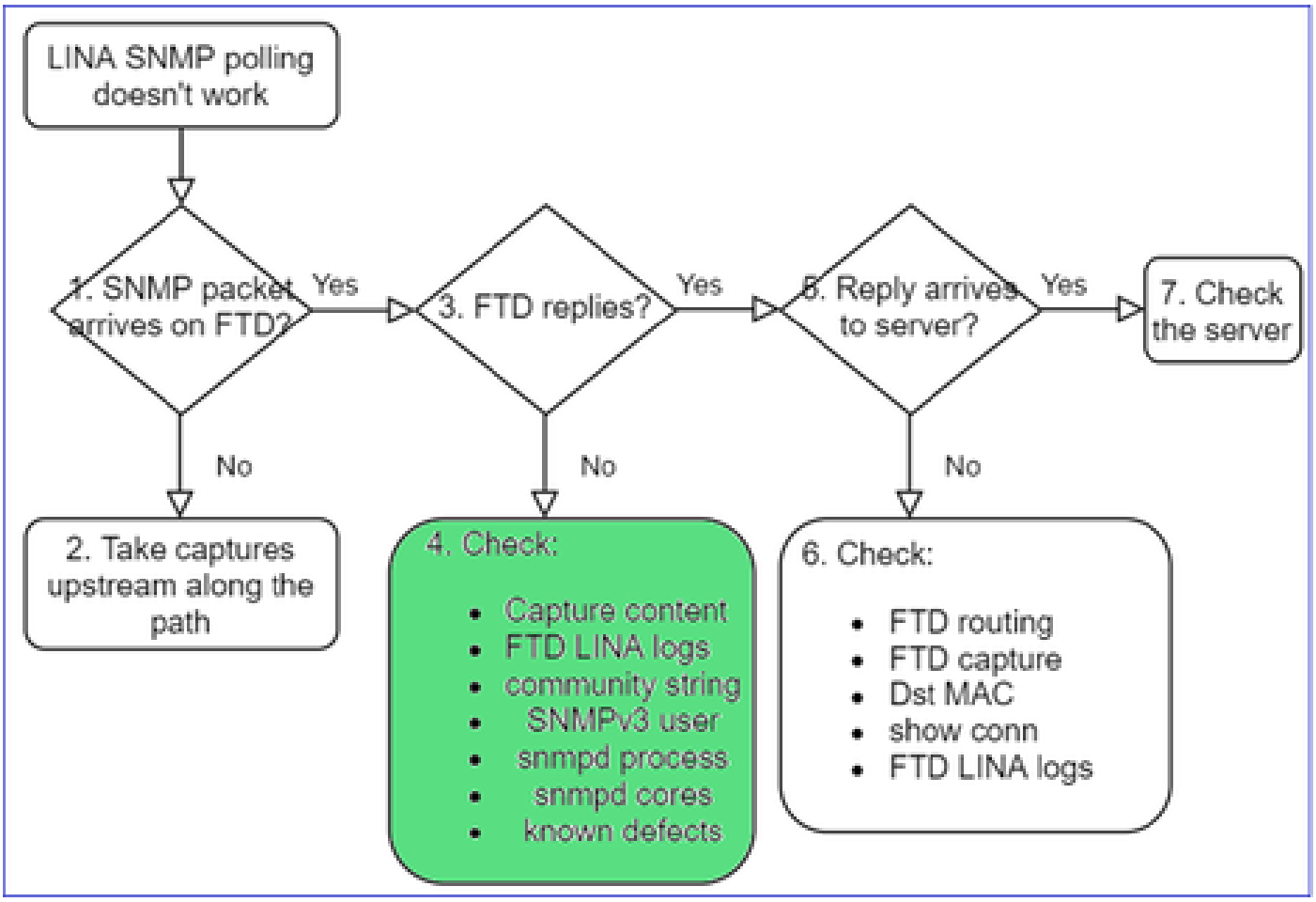
<#root>

```
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. Additional checks



a. For Firepower 4100/9300 devices, check the FXOS compatibility table.

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)+ Note 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	**9.19(x)** (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	**7.3.0** (recommended) 7.2.0 7.1.0 7.0.0 6.7.0 6.6.x
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19(x)** (recommended) 9.18(x) 9.17(x) 9.16(x)	**7.3.0** (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)+ Note 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	**9.18(x)** (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	**7.2.0** (recommended) 7.1.0 7.0.0 6.7.0 6.6.x
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18(x)** (recommended) 9.17(x) 9.16(x)	**7.2.0** (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	**9.18(x)** (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x) 9.13(x)	**7.2.0** (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)+ Note 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	**9.17(x)** (recommended) 9.16(x) 9.15(1) 9.14(x)	**7.1.0** (recommended) 7.0.0 6.7.0 6.6.x

b. Check the FTD LINA snmp-server statistics:

<#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 connection table

This check is very useful in case you do not see packets in the capture on the FTD ingress interface. Note that this is a valid verification only for SNMP on the data interface. If SNMP is on mgmt interface (post-6.6/9.14.1), no conn is created.

```
<#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 syslogs

This also is a valid verification only for SNMP on the data interface! If SNMP is on mgmt interface no log is created:

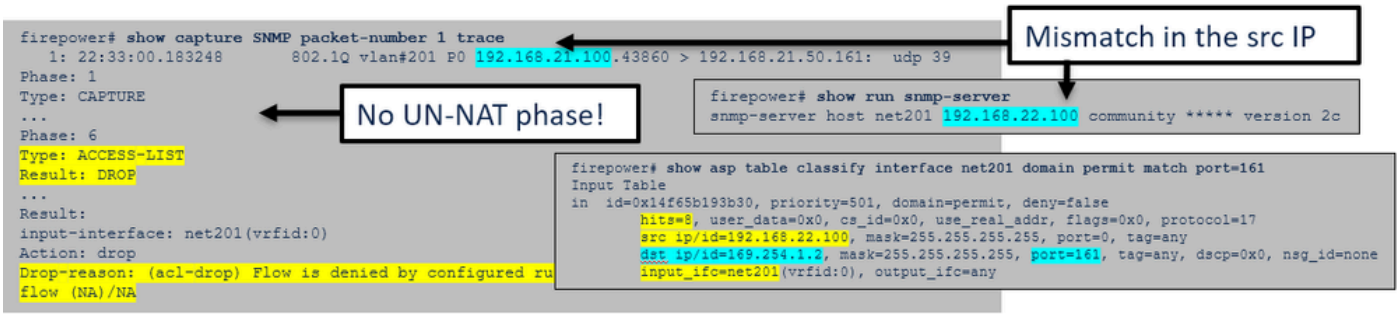
```
<#root>

firepower#

show log | i 302015.*161

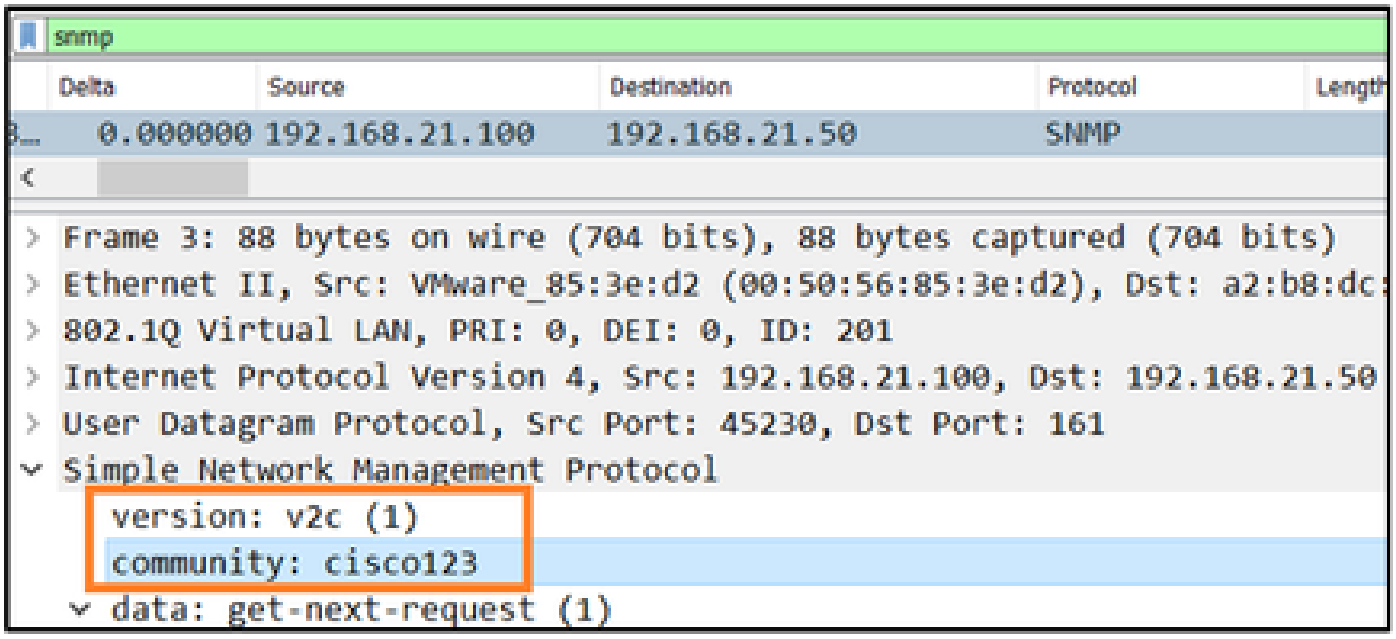

Jul 13 2021 21:24:45: %FTD-6-302015: Built inbound UDP connection 5292 for net201:192.0.2.100/42909 (19
```

e. Check if the FTD drops the SNMP packets due to incorrect host source IP



f. Incorrect credentials (SNMP community)

In the capture contents you can see the community values (SNMP v1 and 2c):



g. Incorrect configuration (for example, SNMP version or Community string)

There are a few ways to verify the device SNMP configuration and Community strings:

<#root>

```
firepower#
```

more system:running-config | i community

```
snmp-server host net201 192.168.2.100 community cISCO123 version 2c
```

Another way:

<#root>

```
firepower#
```

debug menu netsnmp 4

h. FTD LINA/ASA ASP drops

This is a useful check in order to verify if the SNMP packets are dropped by the FTD. First, clear the counters (clear asp drop) and then test:

<#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 captures

ASP captures provide visibility into the dropped packets (for example, ACL or adjacency):

<#root>

```
firepower#
```

```
capture ASP type asp-drop all
```

Test and then check the capture contents:

<#root>

```
firepower#
```

```
show capture
```

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

j. SNMP core (traceback) – verification way 1

This check is useful in case you suspect system stability issues:

<#root>

```
firepower#
```

```
show disk0: | i core
```

```
13  52286547    Jun 11 2021 12:25:16  coredumpfsys/core.snmpd.6208.1626214134.gz
```

SNMP core (traceback) – verification way 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
```

If you see an SNMP core file, collect these items and contact Cisco TAC:

- FTD TS file (or ASA show tech)
- snmpd core files

SNMP debugs (these are hidden commands and available only on newer versions):

<#root>

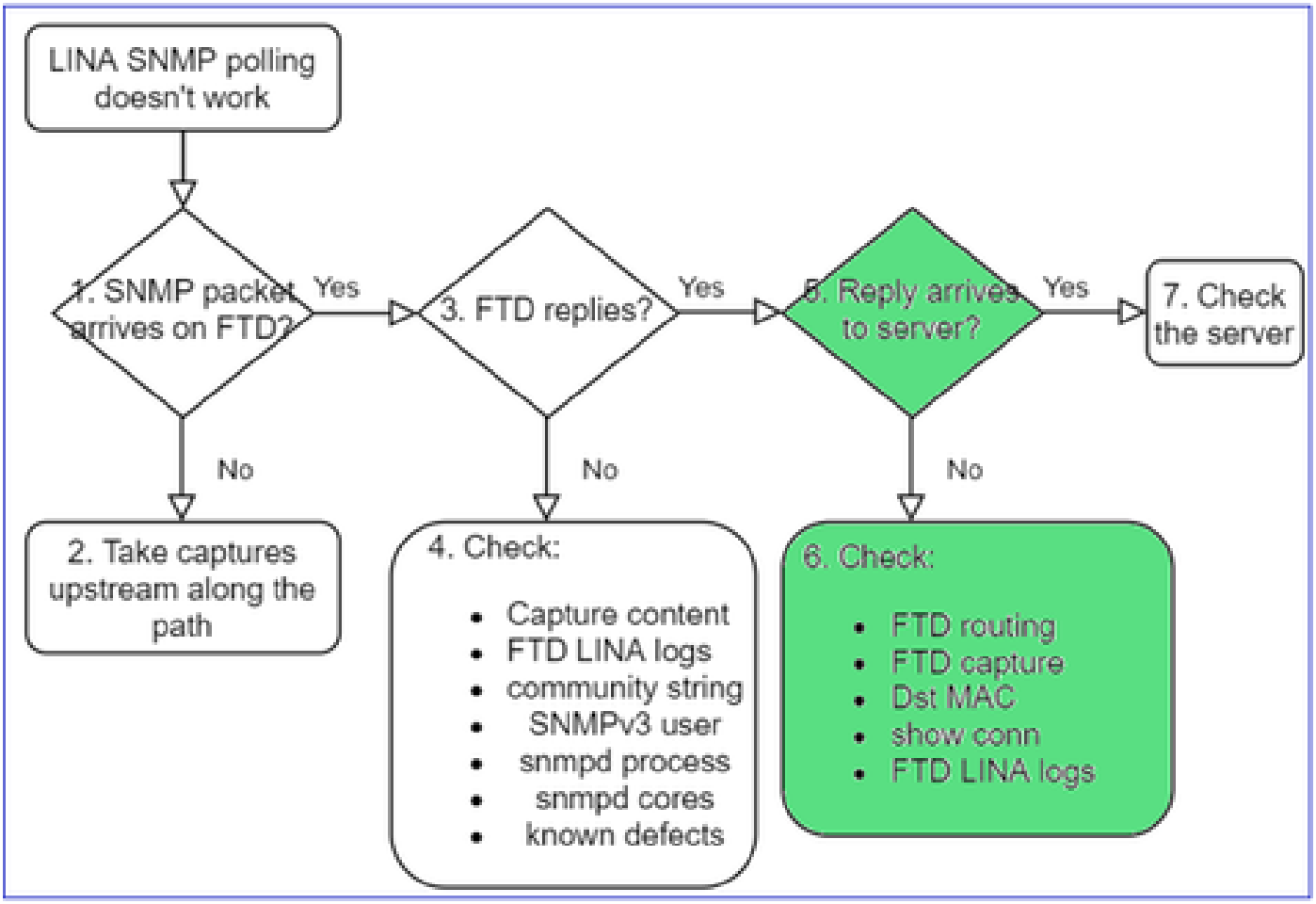
```
firepower#
debug snmp trace [255]

firepower#
debug snmp verbose [255]

firepower#
debug snmp error [255]

firepower#
debug snmp packet [255]
```

Does firewall SNMP reply arrive at the server?



If the FTD replies, but the reply does not reach the server, check:

a. FTD routing

For the FTD management interface routing:

```
<#root>

>

show network
```

For FTD LINA data interface routing:

```
<#root>

firepower#

show route
```

b. Destination MAC verification

FTD mgmt dst MAC verification:

```
<#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 data interface destination MAC verification:

```
<#root>

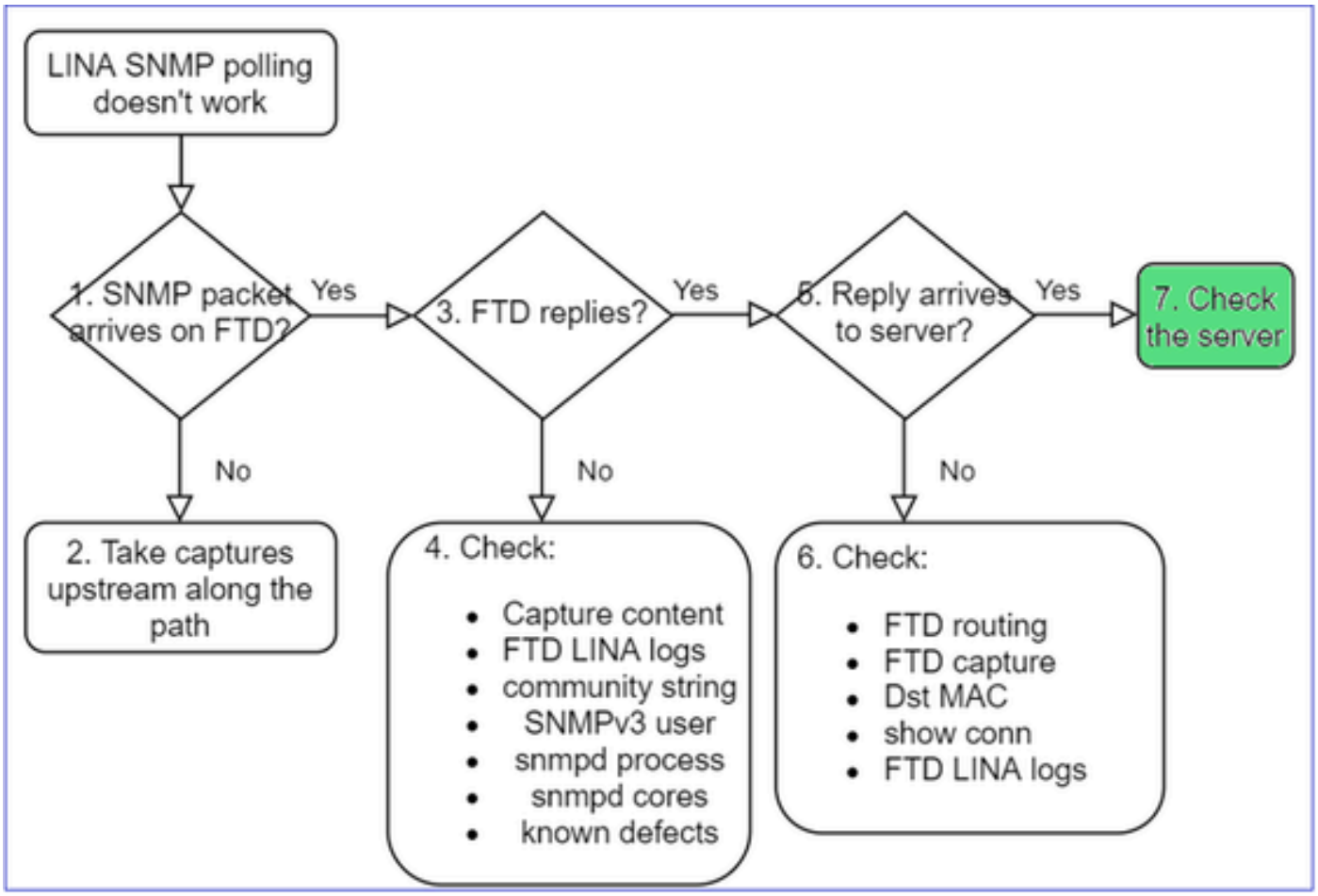
firepower#

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. Check devices along the path that potentially drop/block the SNMP packets.

Check the SNMP server



a. Check the capture contents to verify the settings.

b. Check the server configuration.

c. Try to modify the SNMP community name (for example, without special characters).

d. You can use an end-host or even the FMC to test the poll as long as the 2 conditions are met:

i. SNMP connectivity is in place.

ii. The source IP is allowed to poll the device.

<#root>

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

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

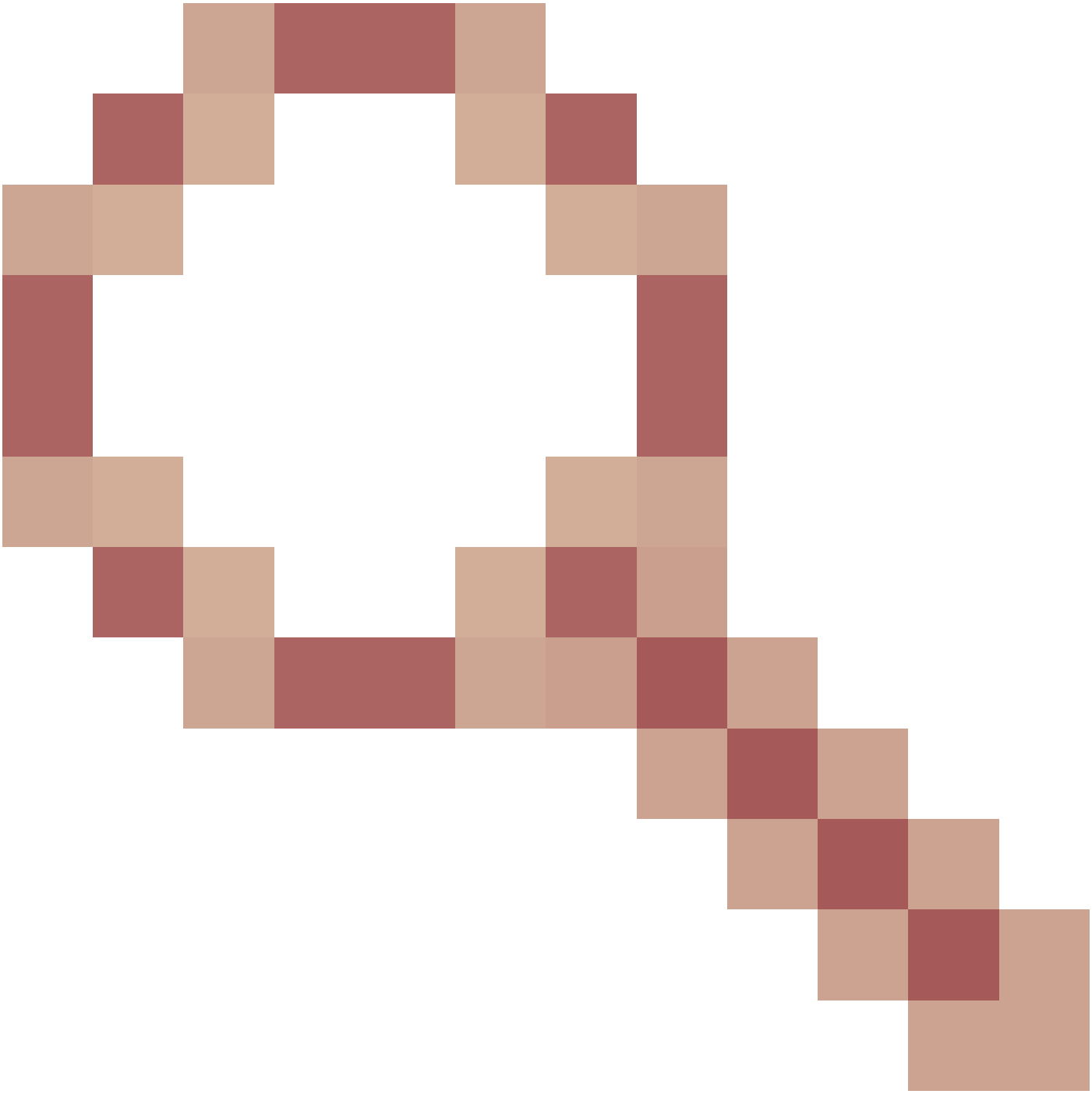
```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9
```

SNMPv3 Poll Considerations

- License: SNMPv3 requires Strong Encryption License. Ensure that you have Export Controlled Functionality enabled on the Smart Licensing portal
- To troubleshoot, you can try with a new user/credentials
- If encryption is used, you can decrypt the SNMPv3 traffic and check the payload as described in:

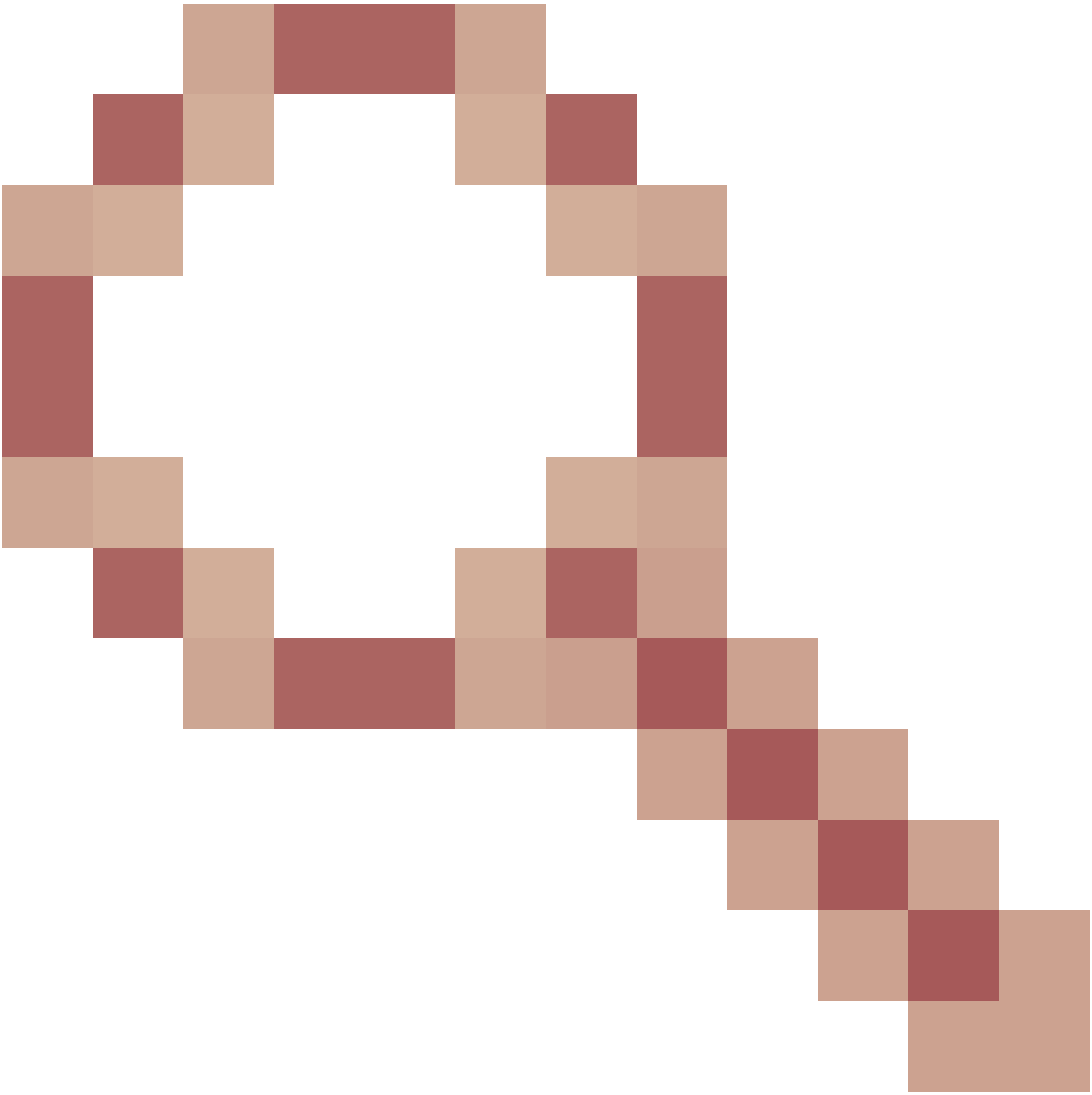
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59

- Consider AES128 for encryption in case your software is affected by defects like:
- Cisco bug ID CSCvy27283



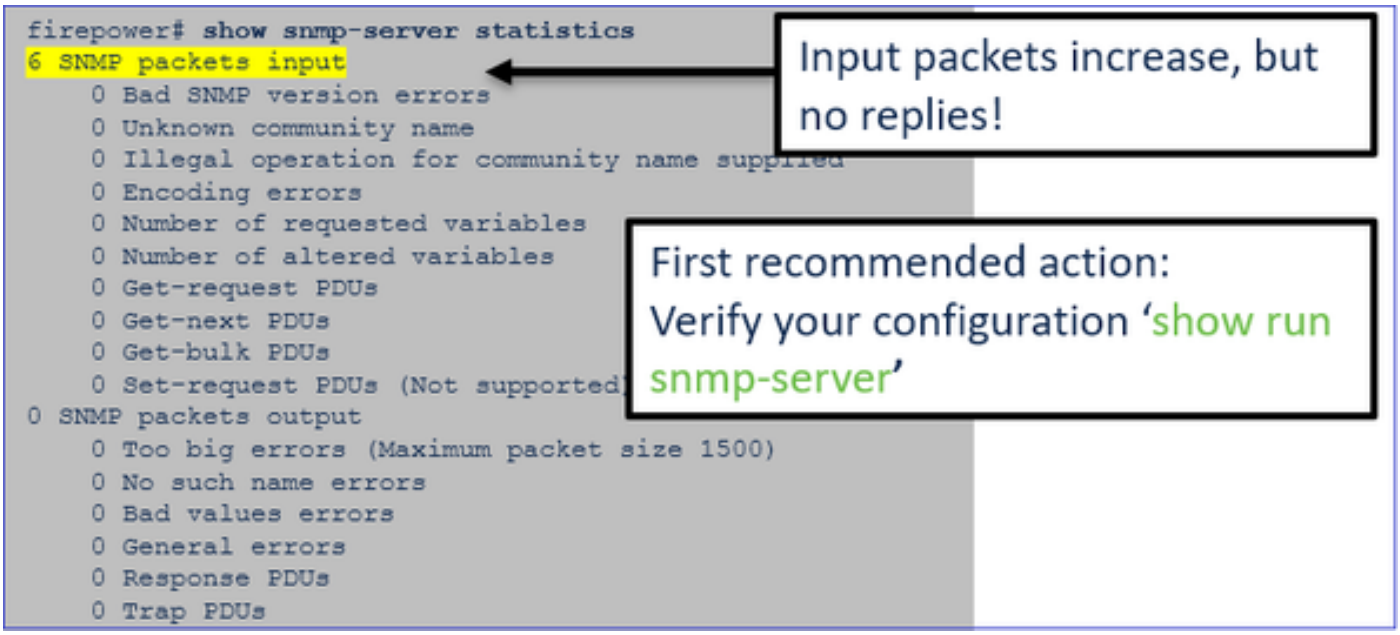
ASA/FTD SNMPv3 polling can fail using privacy algorithms AES192/AES256

Cisco bug ID CSCvx45604



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

Note: If SNMPv3 fails due to algorithm mismatch the show outputs and the logs do not show anything obvious.



SNMPv3 Polling Considerations – Case Studies

1. SNMPv3 **snmpwalk** - Functional scenario

<#root>

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

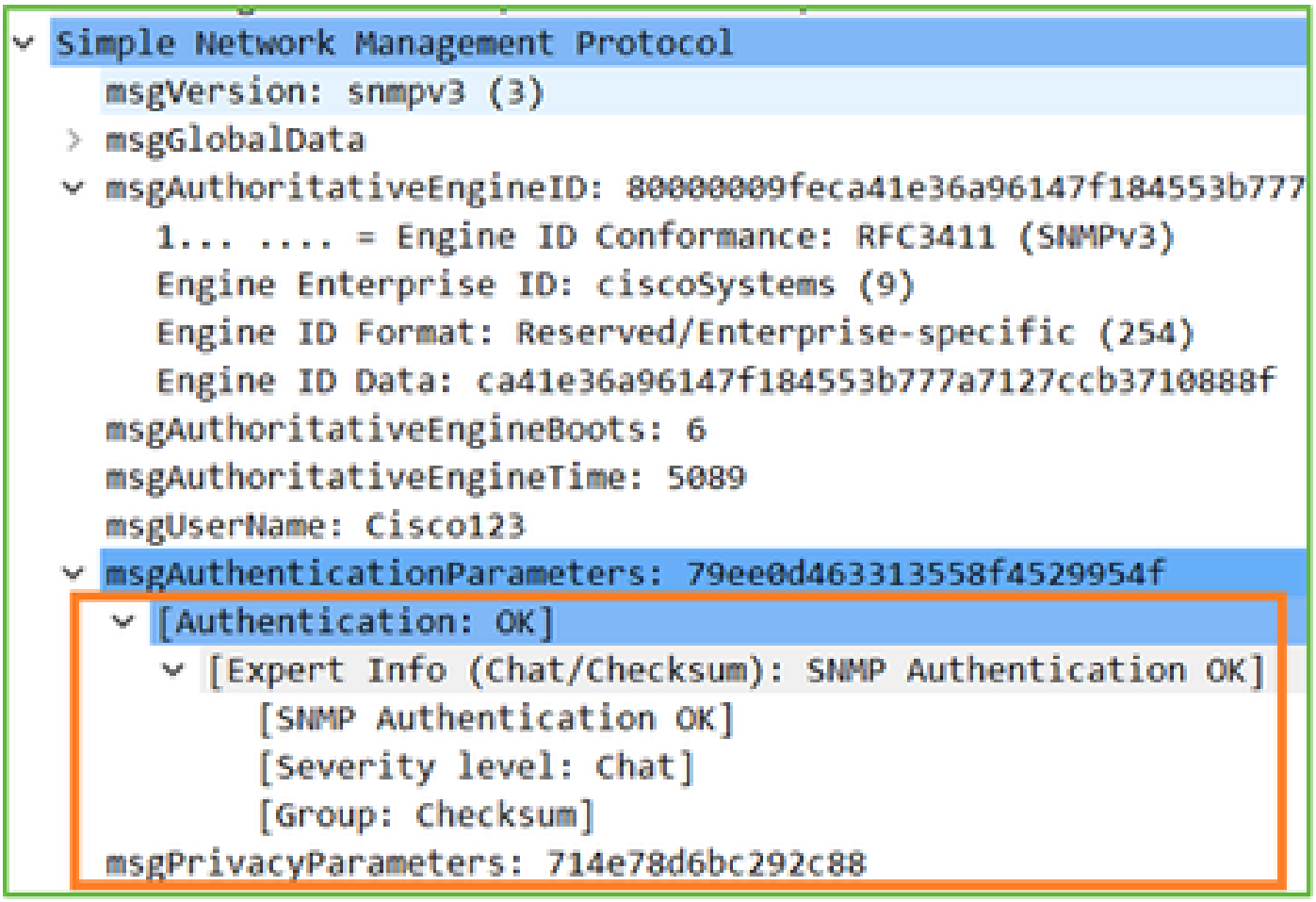
```
snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x AES -X Cisco123 192.168.21.50
```

```
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
```

In the capture (**snmpwalk**) you see a reply for each packet:

```
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
```

The capture file shows nothing unusual:



2. SNMPv3 **snmpwalk** - Encryption failure

Hint #1: There is a Timeout:

<#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
```

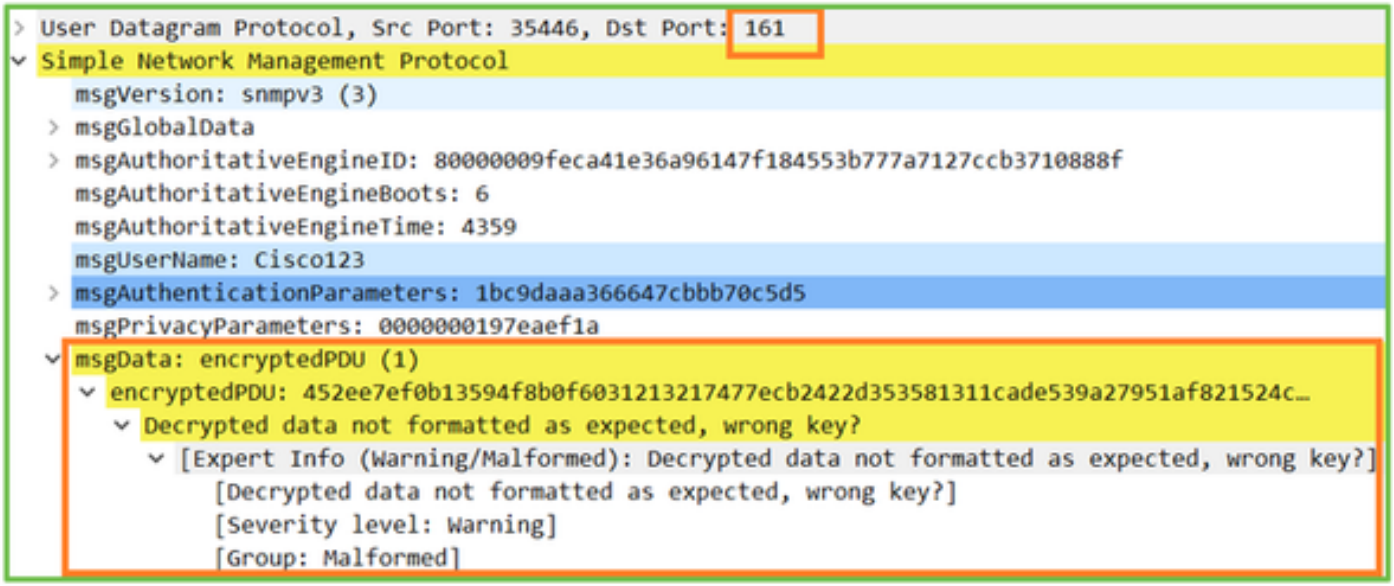
Hint #2: There are many requests and 1 reply:

```
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
```

Hint #3: Wireshark decryption failure:



Hint #4. Check the ma_ctx2000.log file for ‘error parsing ScopedPDU’ messages:

<#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
```

The error parsing ScopedPDU is a strong hint of an encryption error. The ma_ctx2000.log file shows events only for SNMPv3!

3. SNMPv3 **snmpwalk** – Authentication failure

Hint #1: Authentication failure

<#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)
```

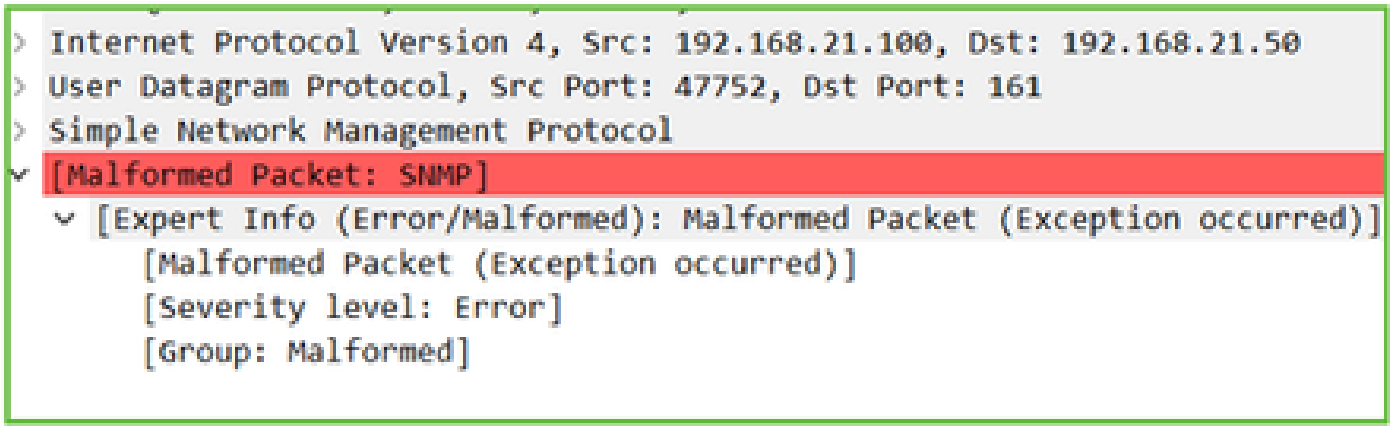
Hint #2: There are many requests and many replies

```
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
```

Hint #3: Wireshark Malformed Packet



Hint #4. Check the ma_ctx2000.log file for 'Authentication failed' messages:

<#root>

>

expert

admin@firepower:~$

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

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

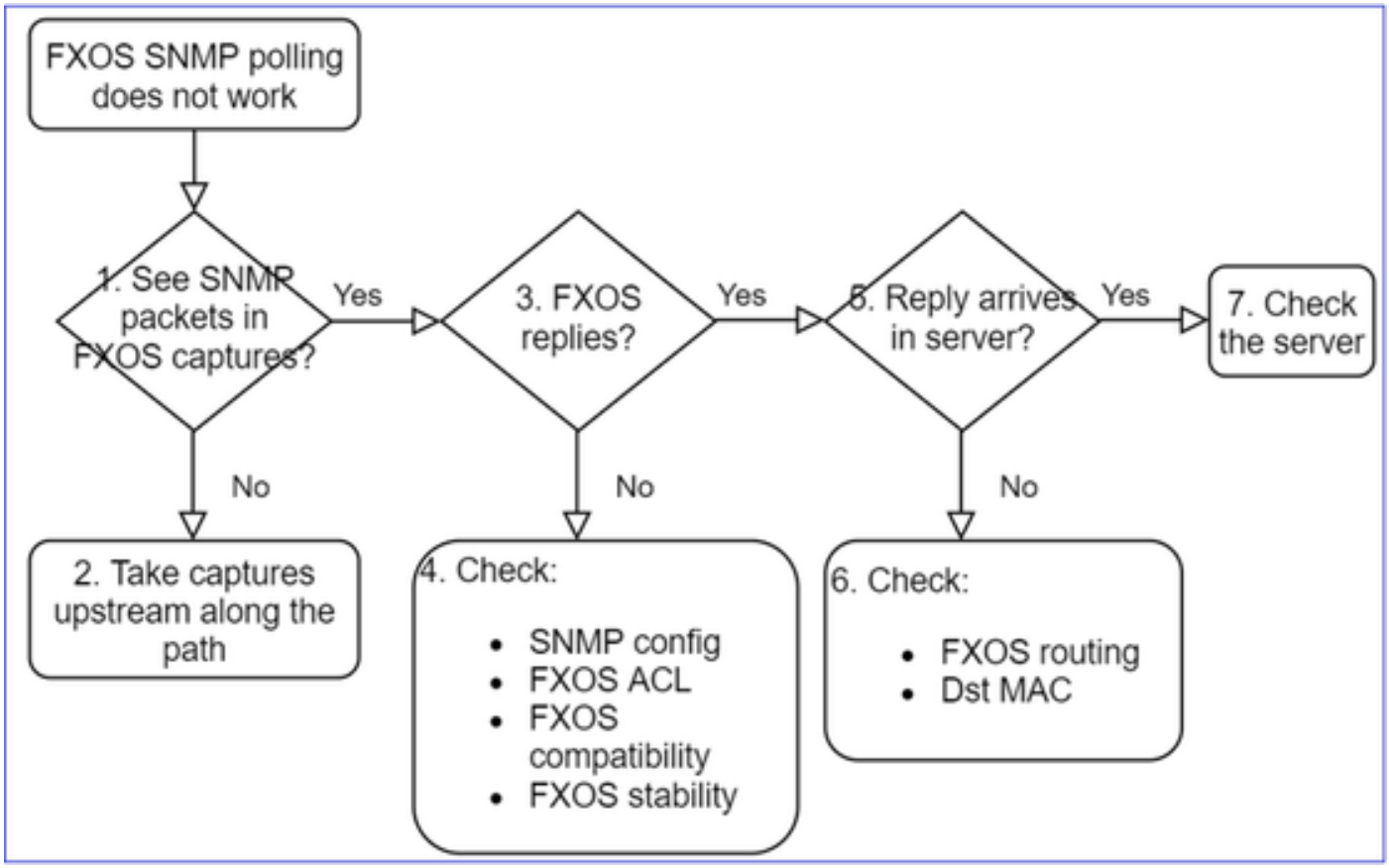
Unable to Poll FXOS SNMP

Problem Descriptions (sample from real Cisco TAC cases):

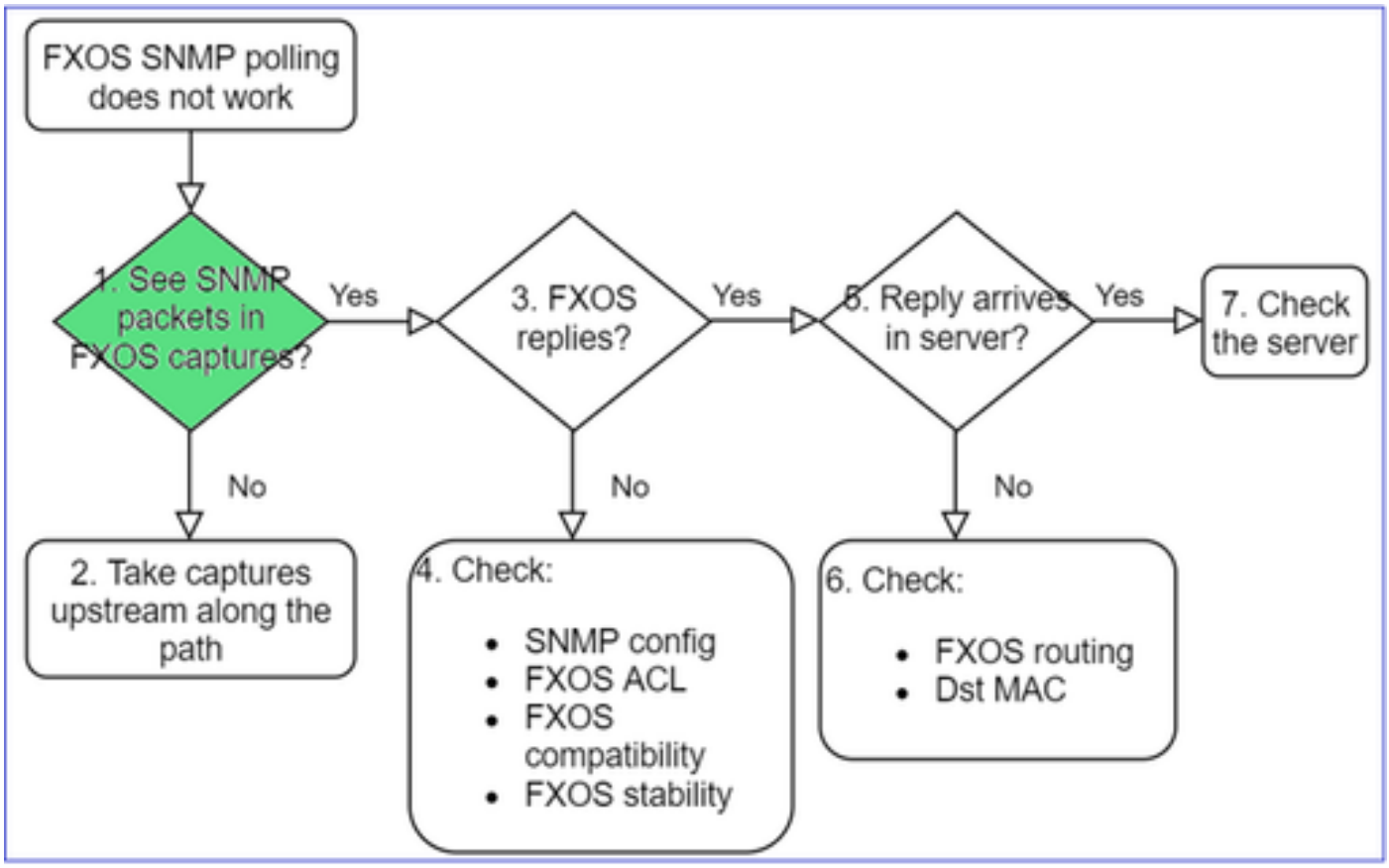
- "SNMP gives a wrong version for FXOS. When polling with SNMP for version of the FXOS the output is difficult to understand."
- "Unable to setup snmp community on FXOS FTD4115."
- "After an FXOS upgrade from 2.8 to 2.9 on standby firewall, we get a timeout when we try to receive any information via SNMP."
- "snmpwalk fails on 9300 fxos but works on 4140 fxos on same version. Reachability and community are not the issue."
- "We want to add 25 SNMP servers on FPR4K FXOS, but we cannot."

Recommended Troubleshooting

This is the process to troubleshoot flowchart for FXOS SNMP polling issues:



1. Do you see SNMP packets in FXOS captures?



FPR1xxx/21xx

- On FPR1xxx/21xx there is no chassis manager (appliance mode).
- You can poll the FXOS software from the mgmt interface.

```
<#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

- On Firepower 41xx/93xx use the Ethanalyzer CLI tool to take a chassis capture:

```
<#root>

firepower#

connect fxos


firepower(fxos)#

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


firepower(fxos)#

exit


firepower#

connect local-mgmt


firepower(local-mgmt)#

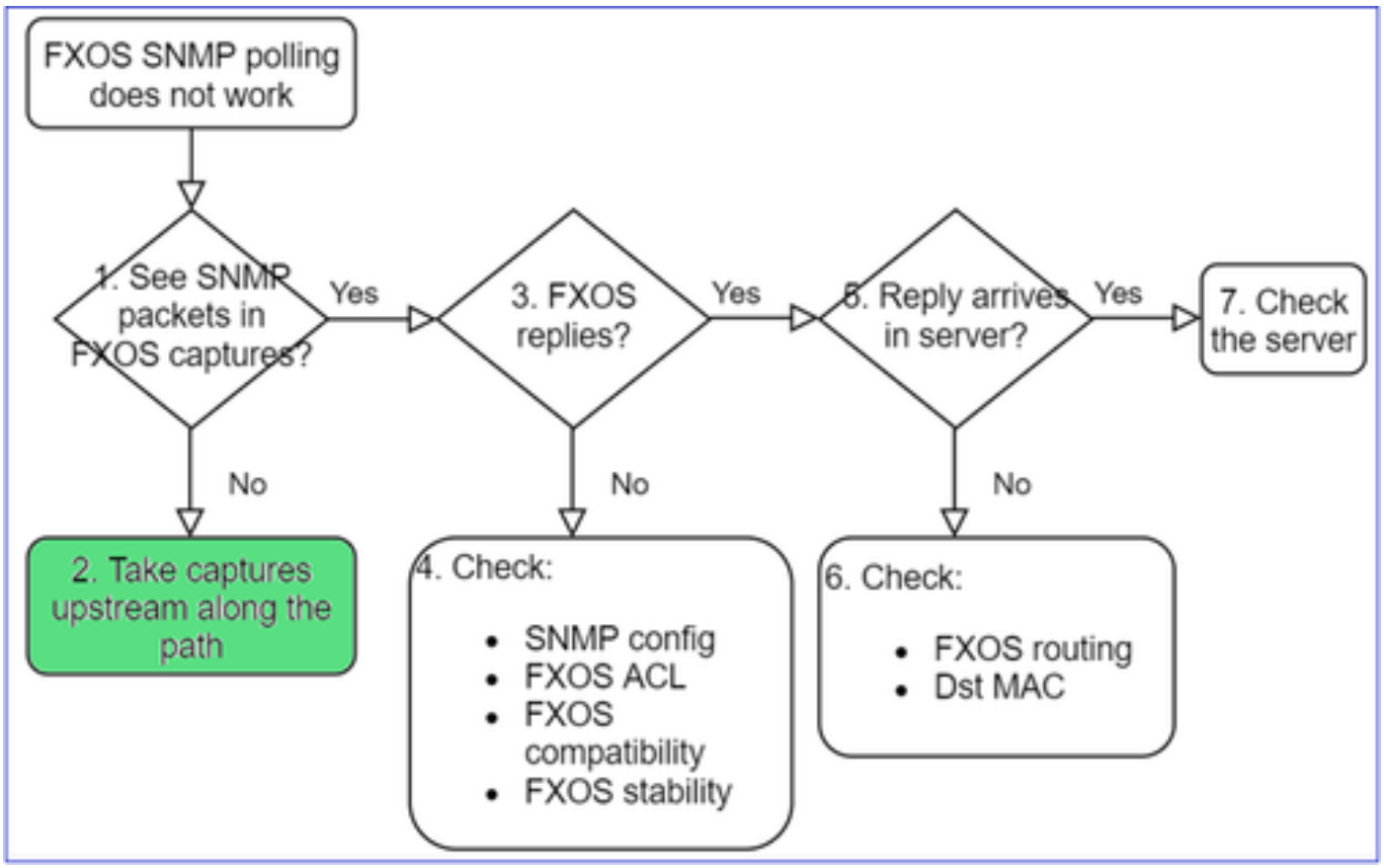
dir


1

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

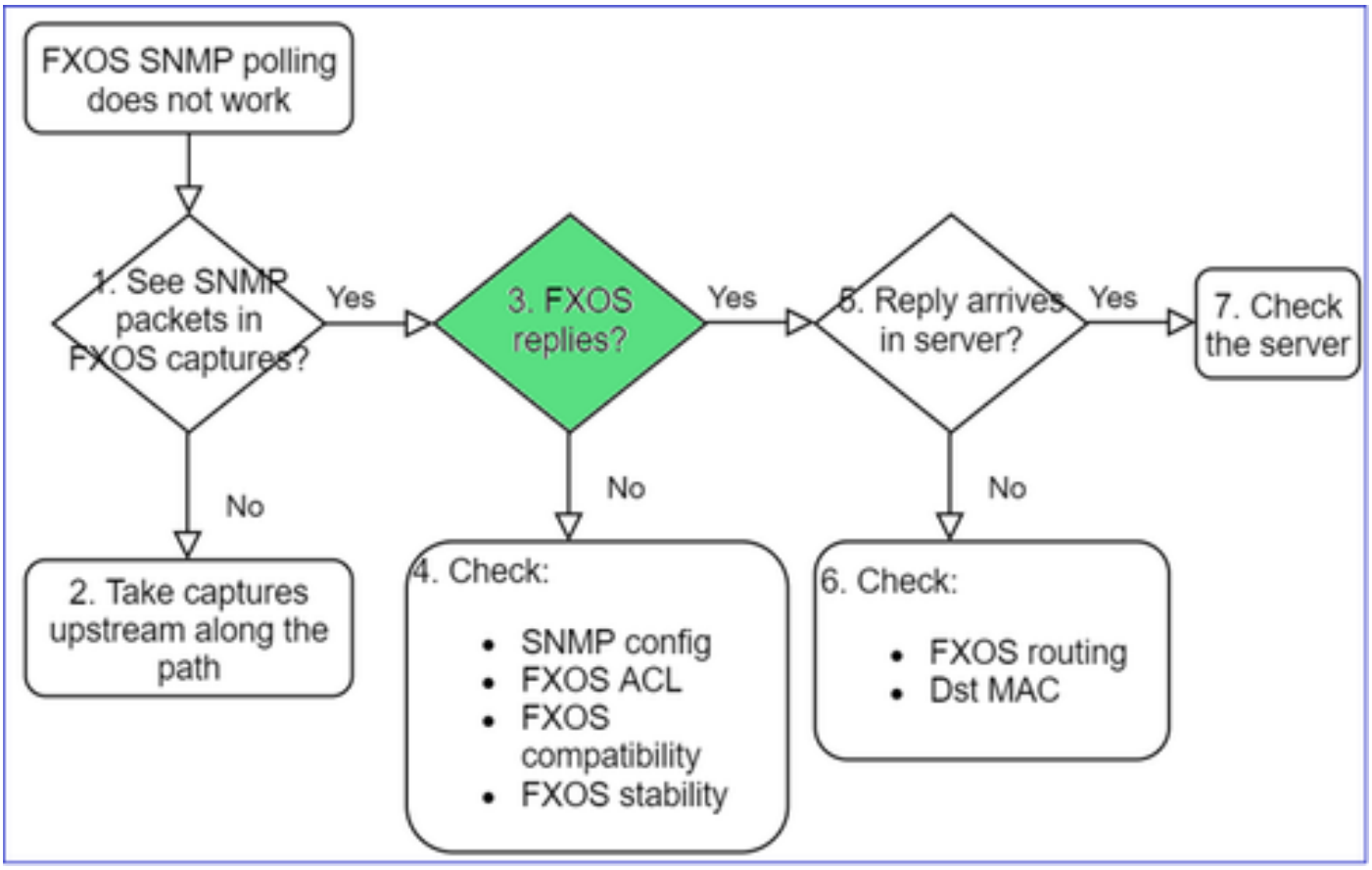
```
firepower(local-mgmt)#
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. No packets in FXOS captures?



- Take captures upstream along the path

3. FXOS replies?



- Functional scenario:

<#root>

>

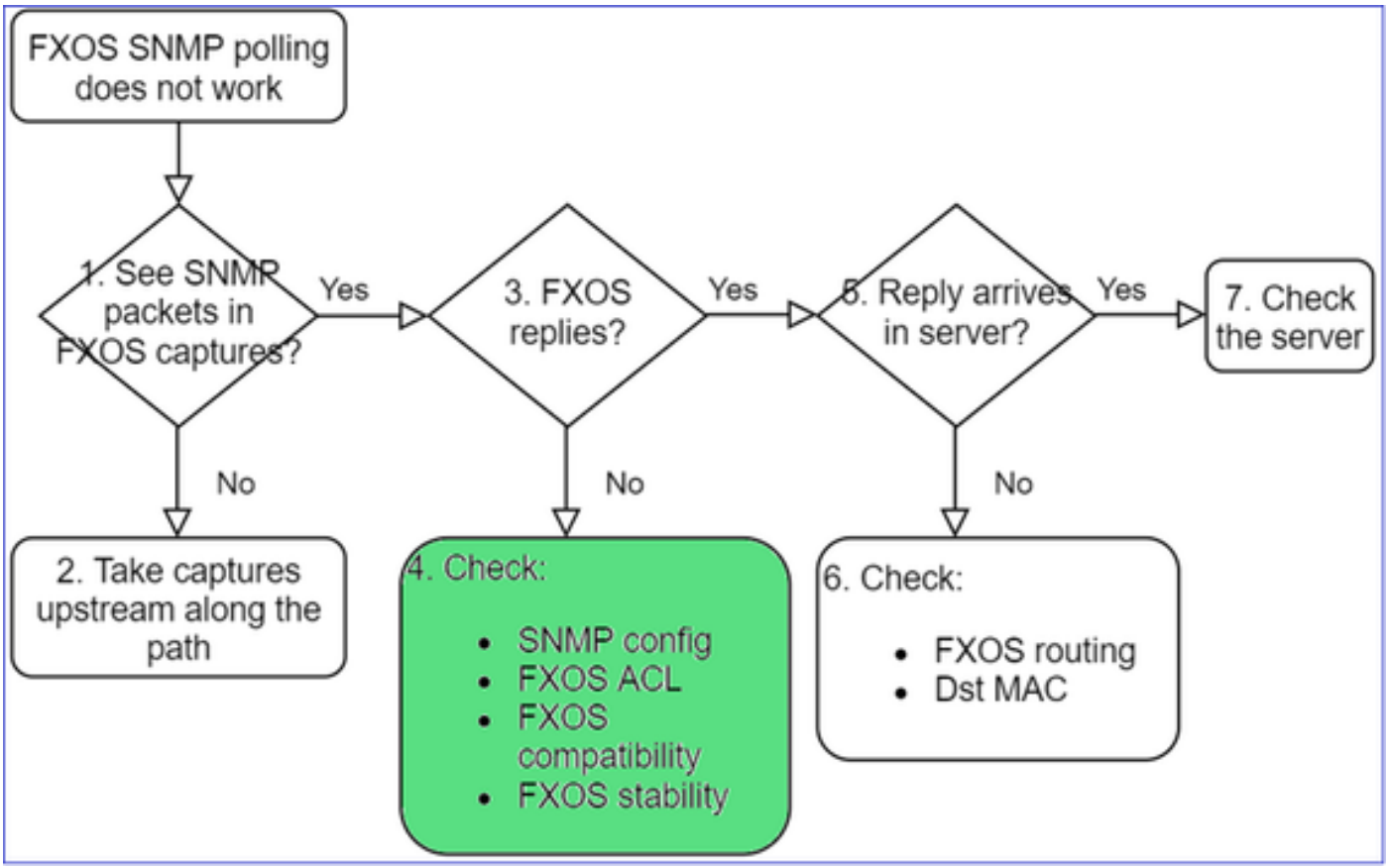
capture-traffic

```
...
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 does not reply



Additional checks

- Verify the SNMP configuration (from the UI or CLI):

```
<#root>

firepower#

scope monitoring


firepower /monitoring #

show snmp


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

- Be careful with the special characters (for example, "$"):

```
<#root>

FP4145-1#

connect fxos


FP4145-1(fxos)#
```

```
show running-config snmp all


FP4145-1(fxos)#
show snmp community

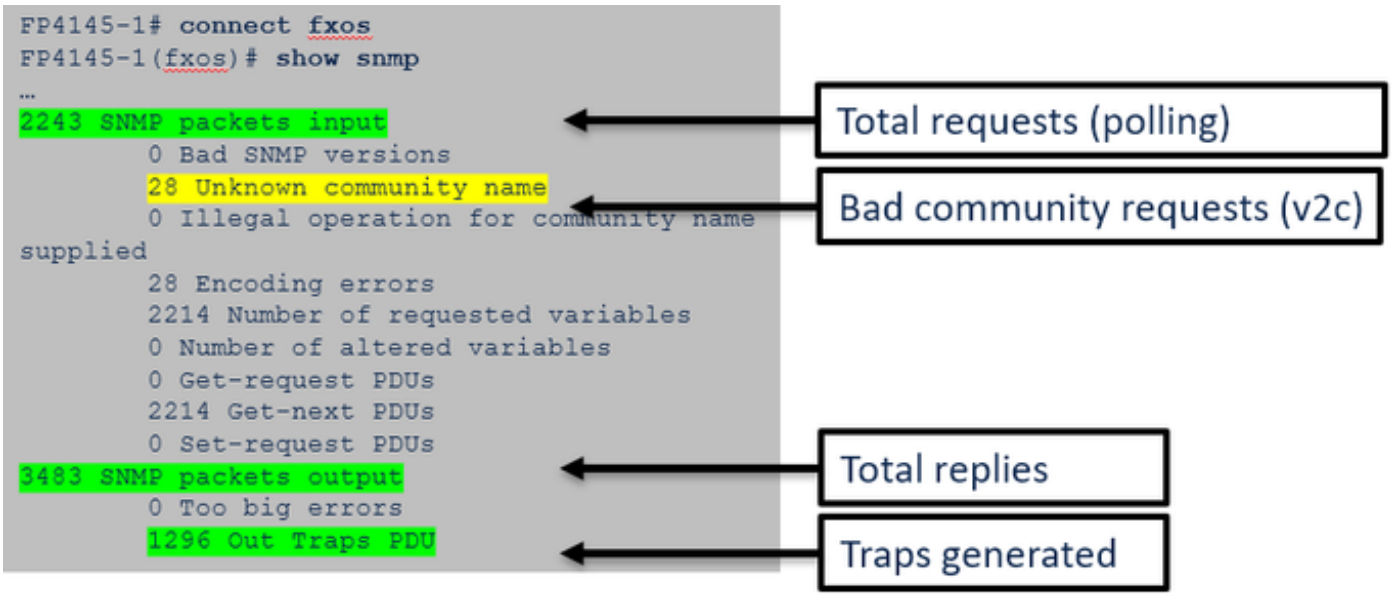

Community             Group / Access       context    acl_filter
---------             --------------       -------    ----------
Cisco123               network-operator
```

- For SNMP v3 use show snmp-user [detail]
- Verify the FXOS Compatibility

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id_59069

4. In case FXOS does not reply

Verify the FXOS SNMP counters:



- Verify the FXOS Access Control List (ACL). This is applicable only on FPR41xx/9300 platforms.

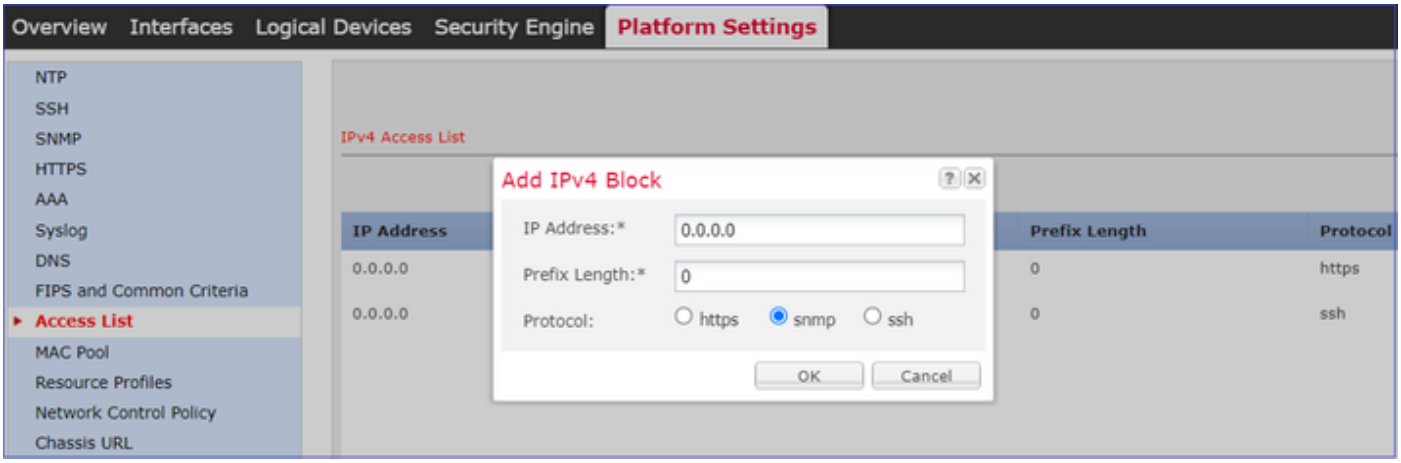
If the traffic is blocked by the FXOS ACL, you see requests, but you do not see any replies:

<#root>

```
firepower(fxos)#
ethanalyzer 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
```

You can verify the FXOS ACL from the User Interface (UI):



You can also verify the FXOS ACL from the CLI:

```
<#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
```

- Debug SNMP (packets only). Applicable only on 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 0.0000
```

- Debug SNMP (all) - This debug output is very verbose.

<#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
```

- Verify if there are any SNMP-related FXOS faults:

<#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
```

- Verify if there are any snmpd cores.

On FPR41xx/FPR9300:

<#root>

```
firepower#
```

connect local-mgmt

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

dir cores

```
1 1983847 Apr 01 17:26:40 2021 core.snmpd.10012.1585762000.gz
1 1984340 Apr 01 16:53:09 2021 core.snmpd.10018.1585759989.gz
```

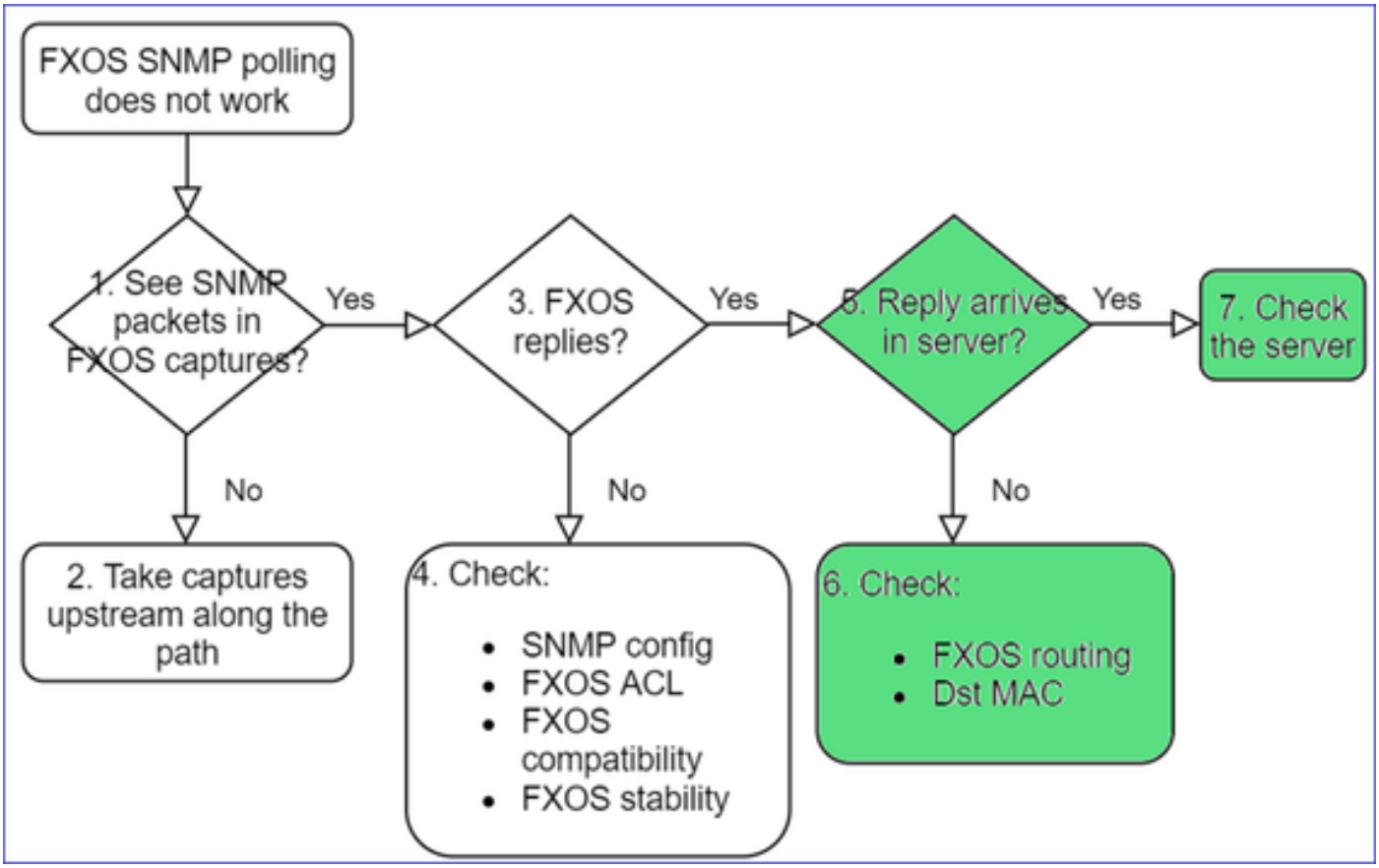
On FPR1xxx/21xx:

<#root>

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

If you see any snmpd cores, collect the cores along with the FXOS troubleshoot bundle and contact Cisco TAC.

5. Does SNMP reply arrive in SNMP server?



a. Check the FXOS routing.

This output is from FPR41xx/9300:

<#root>

```
firepower#
show fabric-interconnect
```

```
Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway Prefix Opera
    ---- --------------- --------------- --------------- ---------------- ---------------- ------ -----
A    192.168.2.37    192.168.2.1     10.255.255.128 ::               ::               64     Operable
```

b. Take a capture, export the pcap and check the dst MAC of the reply

c. Finally, check the SNMP server (captures, configuration, application, and so on)

What SNMP OID Values to Use?

Problem Descriptions (sample from real Cisco TAC cases):

- "We want monitor the Cisco Firepower equipment. Please provide SNMP OIDs for each core CPU, memory, disks"
- "Is there any OID that can be used to monitor status of powers supply on ASA 5555 device?"
- "We want to fetch chassis SNMP OID on FPR 2K and FPR 4K."
- "We want to poll the ASA ARP Cache."
- "We need to know the SNMP OID for BGP peer down."

How to Find the SNMP OID Values

These documents provide info about SNMP OIDs on Firepower devices:

- Cisco Firepower Threat Defense (FTD) SNMP Monitoring White Paper:

https://www.cisco.com/c/en/us/products/index.html

- Cisco Firepower 4100/9300 FXOS MIB Reference Guide:

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b_FXOS_4100_9300_MIBRef.html

- How to Search for a Specific OID on FXOS Platforms:

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

- Check SNMP OIDs from the CLI (ASA/LINA)

<#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
```

- For more info about OIDs check the SNMP Object Navigator, refer to:

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

- On FXOS (41xx/9300) run these 2 commands from the FXOS CLI:

```
<#root>

FP4145-1#

connect fxos


FP4145-1(fxos)#

show snmp internal oids supported create

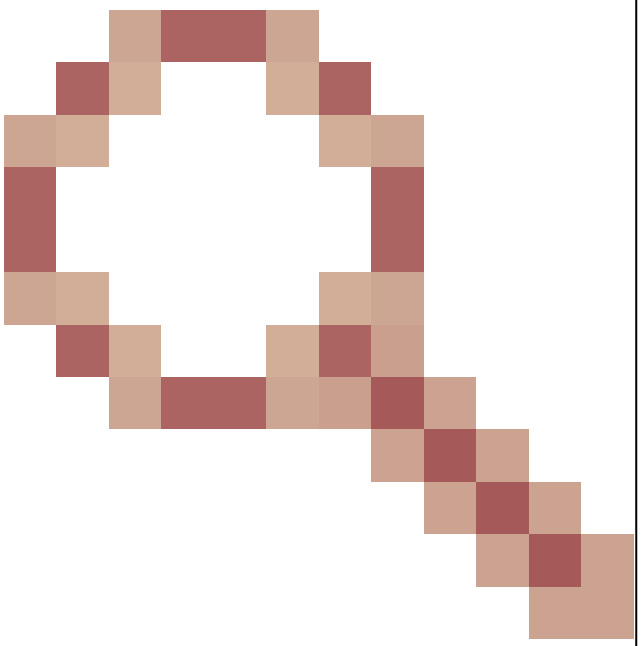
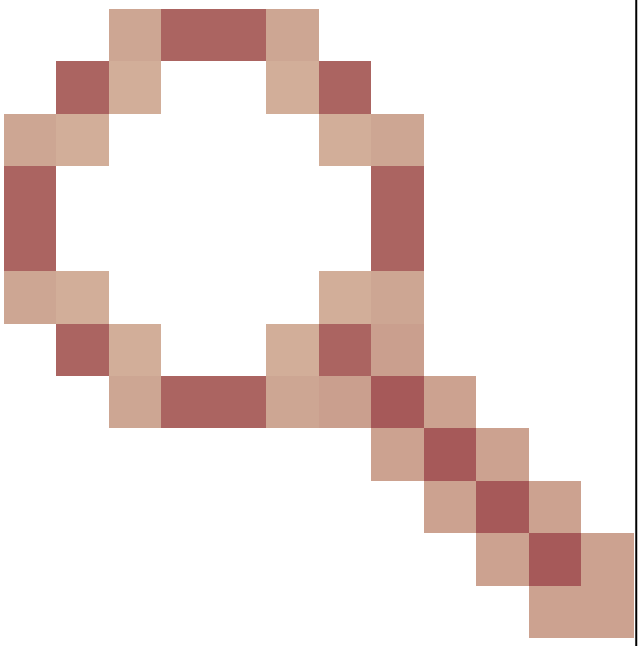

FP4145-1(fxos)#

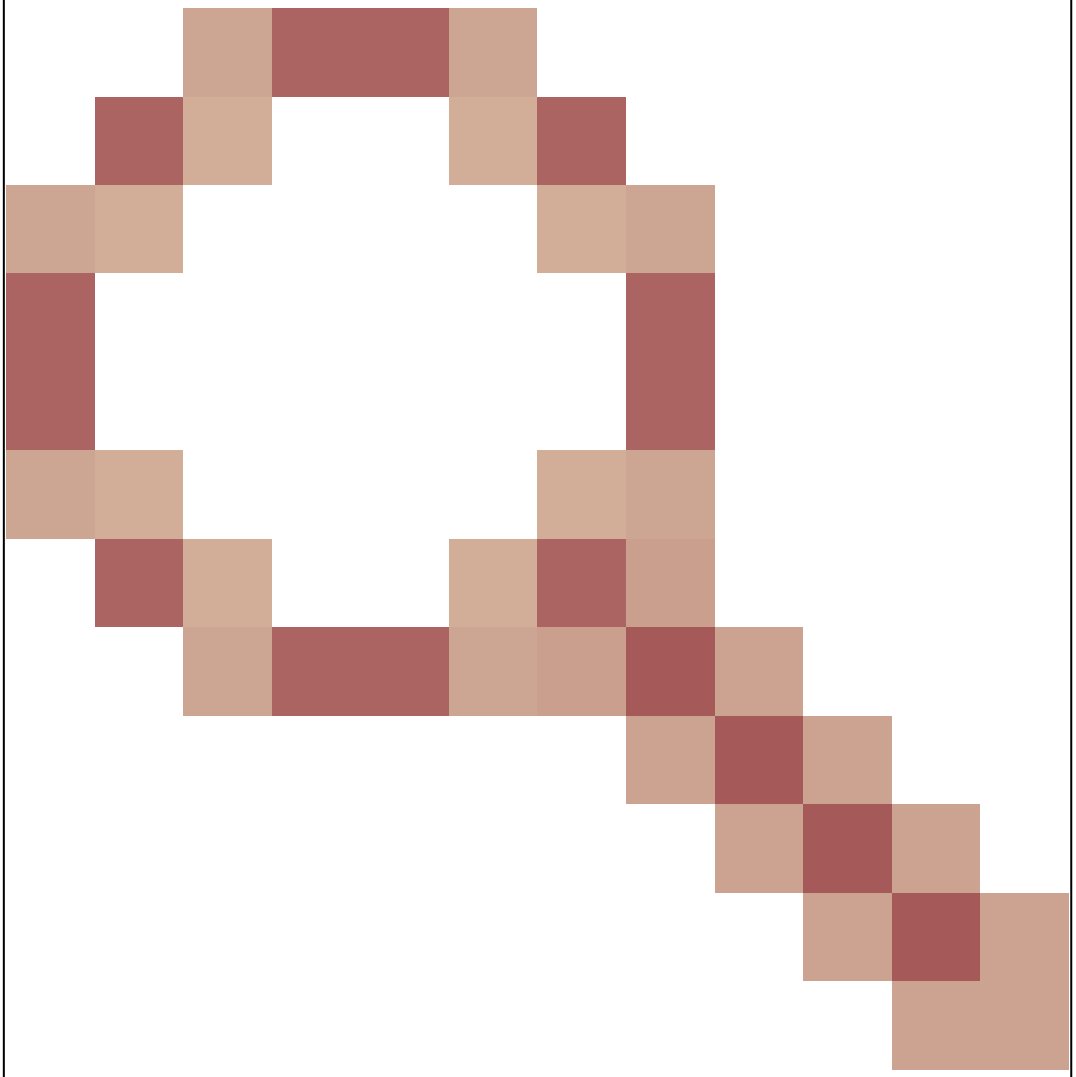
show snmp internal oids supported


- SNMP All supported MIB OIDs -0x11a72920
Subtrees for Context:
ccitt
1
1.0.88010.1.1.1.1.1.1  ieee8021paeMIB
1.0.88010.1.1.1.1.1.2
...
```

Common OIDs Quick Reference

Requirement	**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)
Memory (LINA)	1.3.6.1.4.1.9.9.221.1.1
Memory (Linux/FMC)	1.3.6.1.1.4.1.2021.4
HA info	1.3.6.1.4.1.9.9.491.1.4.2
Cluster info	1.3.6.1.4.1.9.9.491.1.8.1
VPN info	RA-VPN num sessions: 1.3.6.1.4.1.9.9.392.1.3.1 (7.x) RA-VPN num users: 1.3.6.1.4.1.9.9.392.1.3.3 (7.x) RA-VPN num peak sessions: 1.3.6.1.4.1.9.9.392.1.3.41 (7.x)

	S2S VPN num sessions: 1.3.6.1.4.1.9.9.392.1.3.29 S2S VPN num peak sessions: 1.3.6.1.4.1.9.9.392.1.3.31 - Tip: firepower# show snmp-server oid | i ike
BGP status	 ENH Cisco bug ID CSCux13512 : Add BGP MIB for SNMP polling
FPR1K/2K ASA/ASAv Smart Licensing	 ENH Cisco bug ID CSCvv83590 : ASAv/ASA on the FPR1k/2k: Need SNMP OID for tracking the status of Smart Licensing
Lina SNMP OIDs for FXOS-level port-channel	ENH Cisco bug ID CSCvu91544

	 : Support for Lina SNMP OIDs for FXOS-level port-channel interface statistics

FMC 7.3 Additions (for FMC 1600/2600/4600 and newer)

Requirement	**OID**
Fan status trap	Trap OID: 1.3.6.1.4.1.9.9.117.2.0.6 Value OID: 1.3.6.1.4.1.9.9.117.1.4.1.1.1.<index> 0 - fan not running 1 - fan is running
CPU/PSU temperature trap	Trap OID: 1.3.6.1.4.1.9.9.91.2.0.1 Threshold OID: 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<index>.1 Value OID: 1.3.6.1.4.1.9.9.91.1.1.1.1.4.<index>
PSU status trap	Trap 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 - power supply presence not detected 1 - power supply presence detected, ok

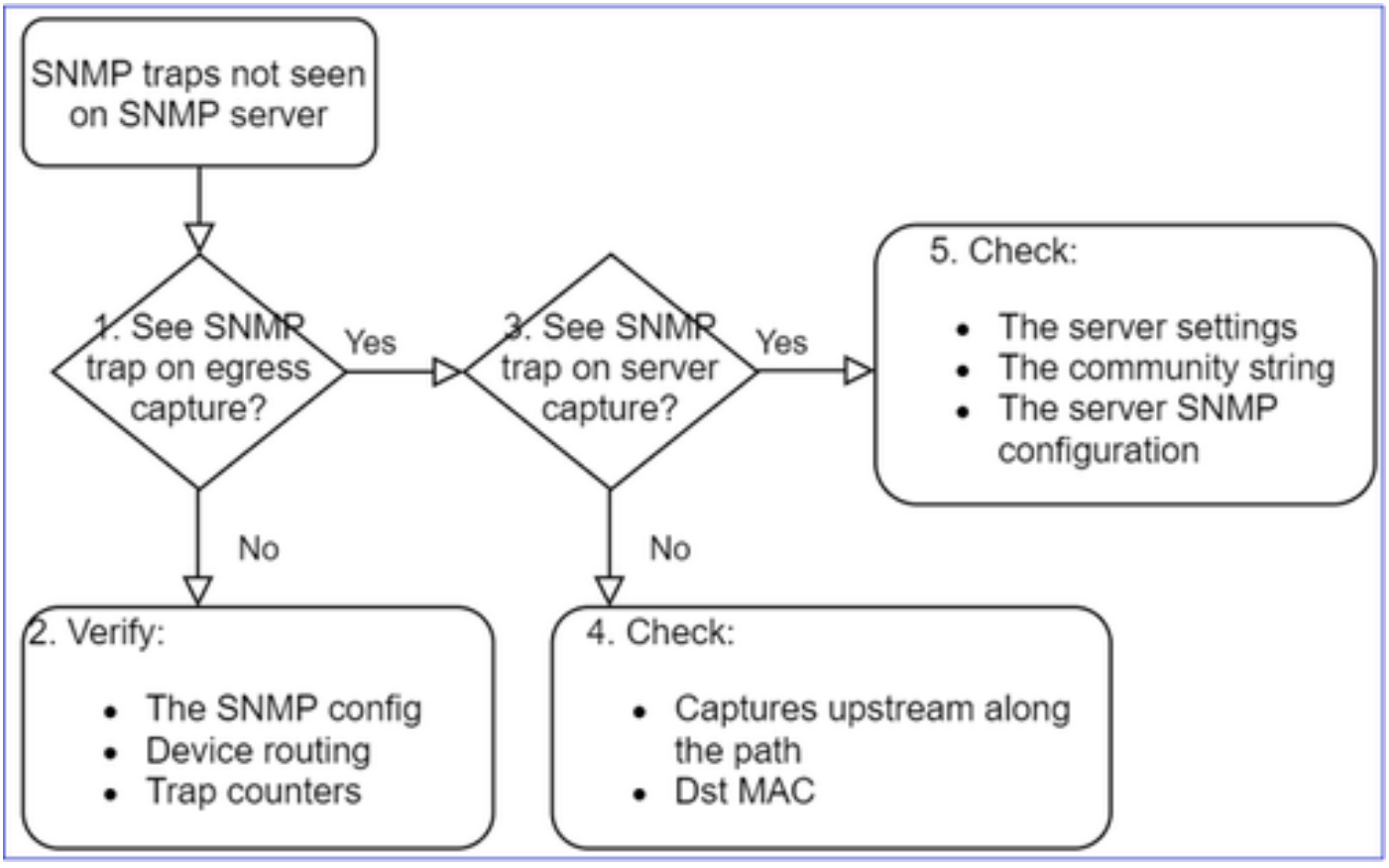
Cannot Get SNMP Traps

Problem Descriptions (sample from real Cisco TAC cases):

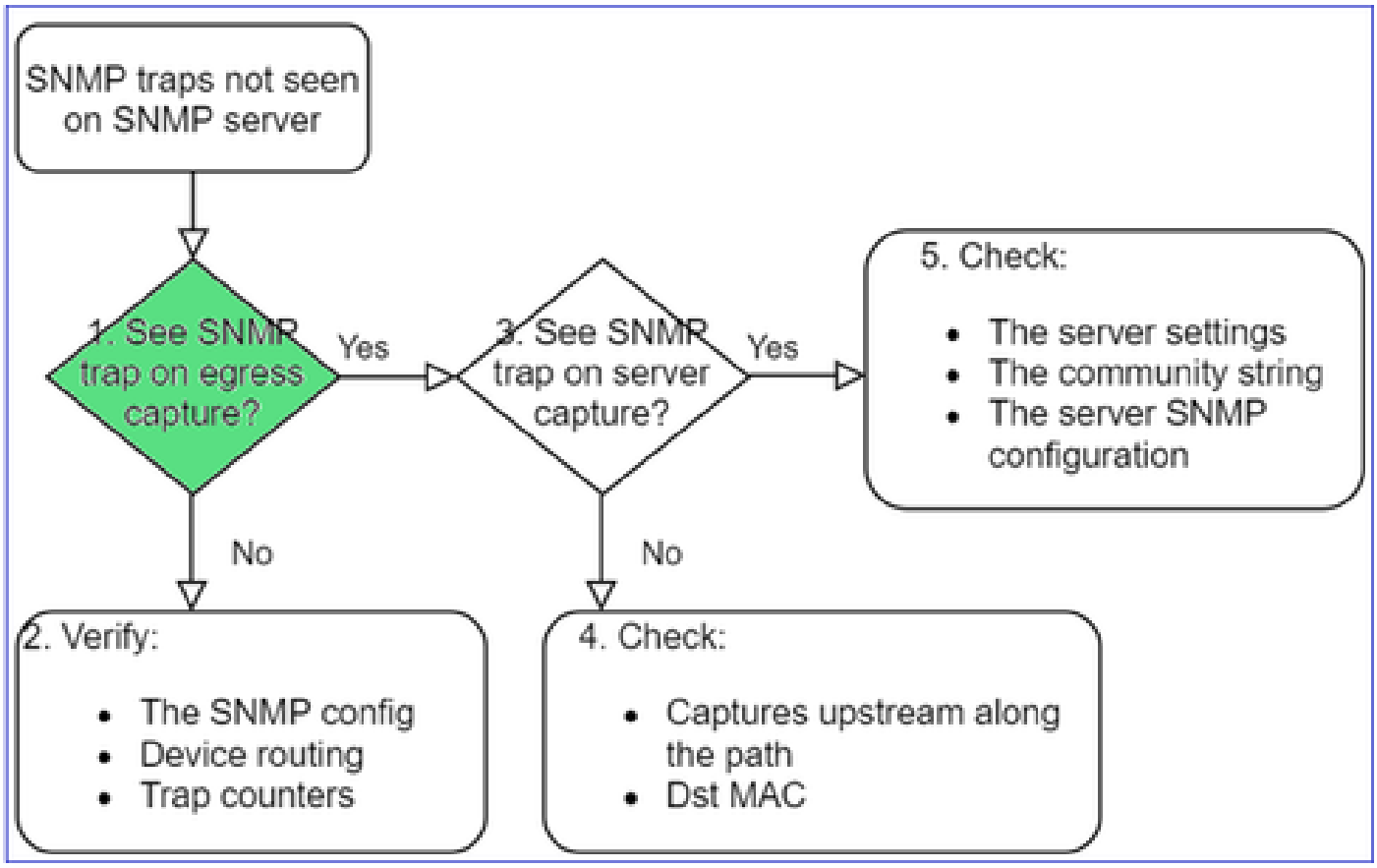
- "SNMPv3 of FTD does not send any trap to SNMP server."
- "FMC and FTD do not send SNMP Trap Messages."
- "We have configured SNMP at our FTD 4100 for FXOS and tried SNMPv3 and SNMPv2, but both cannot send traps."
- "Firepower SNMP does not send traps to the monitoring tool."
- "Firewall FTD does not send SNMP Trap to NMS."
- "SNMP server traps do not function."
- "We have configured SNMP at our FTD 4100 for FXOS and tried SNMPv3 and SNMPv2, but both cannot send traps."

Recommended Troubleshooting

This is the process to troubleshoot flowchart for Firepower SNMP trap issues:



1. Do you see SNMP traps on egress capture?



To capture LINA/ASA traps on mgmt interface:

```
<#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
```

To capture LINA/ASA traps on data interface:

```
<#root>

firepower#

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

To capture FXOS traps (41xx/9300):

```
<#root>

firepower#

connect fxos


firepower(fxos)#

ethanalyzer 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
firepower(fxos)#

exit


firepower#

connect local-mgmt

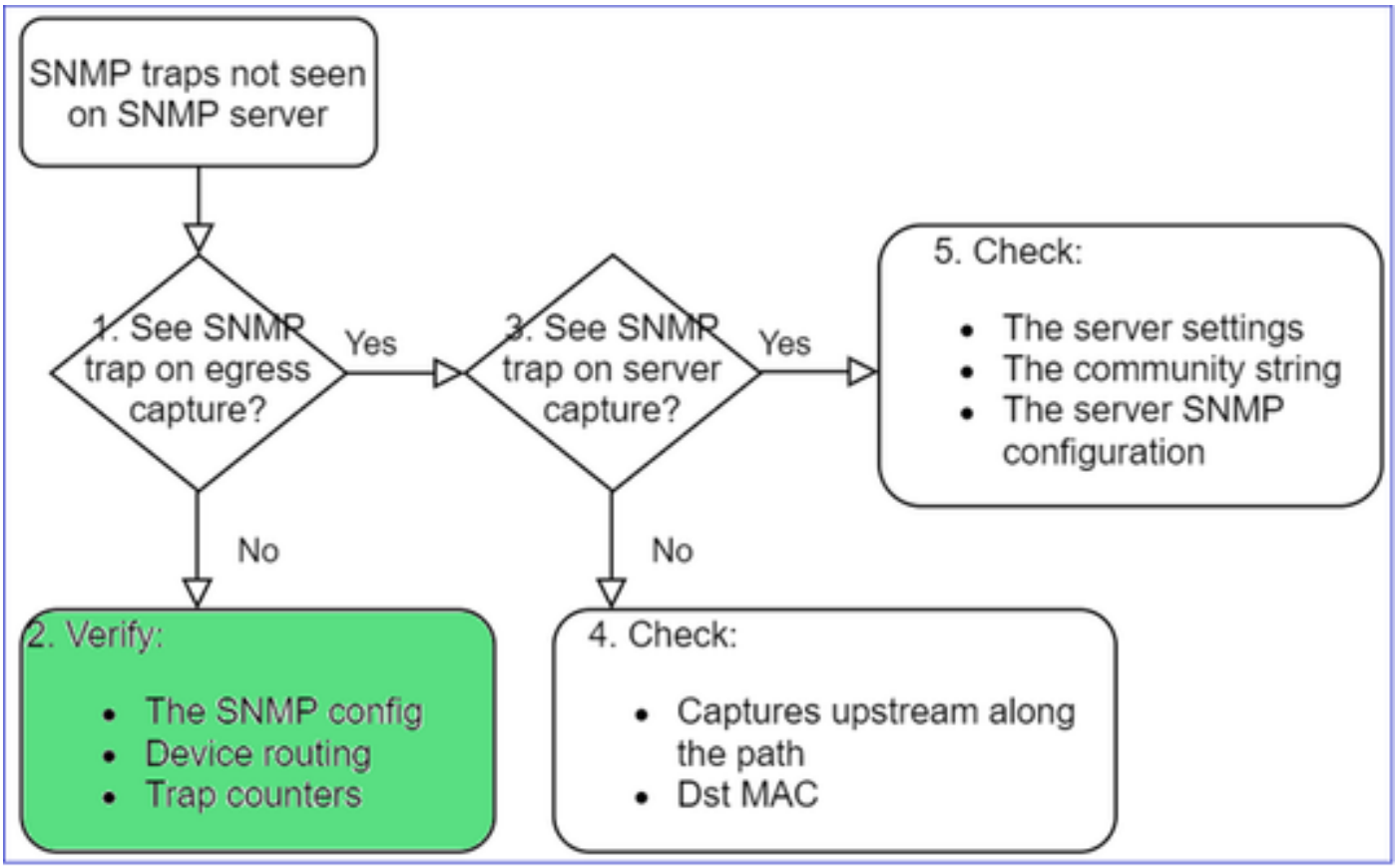

firepower(local-mgmt)#

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. If you don’t see packets on the egress interface:



<#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 traps configuration:

<#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
```

Note: On 1xxx/21xx you see these settings only in the case of **Devices > Device Management > SNMP** config!

- LINA/ASA routing for traps through mgmt interface:

```
<#root>

>

show network
```

- LINA/ASA routing for traps through data interface:

```
<#root>

firepower#

show route
```

- FXOS routing (41xx/9300):

```
<#root>

FP4145-1#

show fabric-interconnect
```

- Trap counters (LINA/ASA):

```
<#root>

firepower#

show snmp-server statistics | i Trap

    20 Trap PDUs
```

And FXOS:

```
<#root>

FP4145-1#

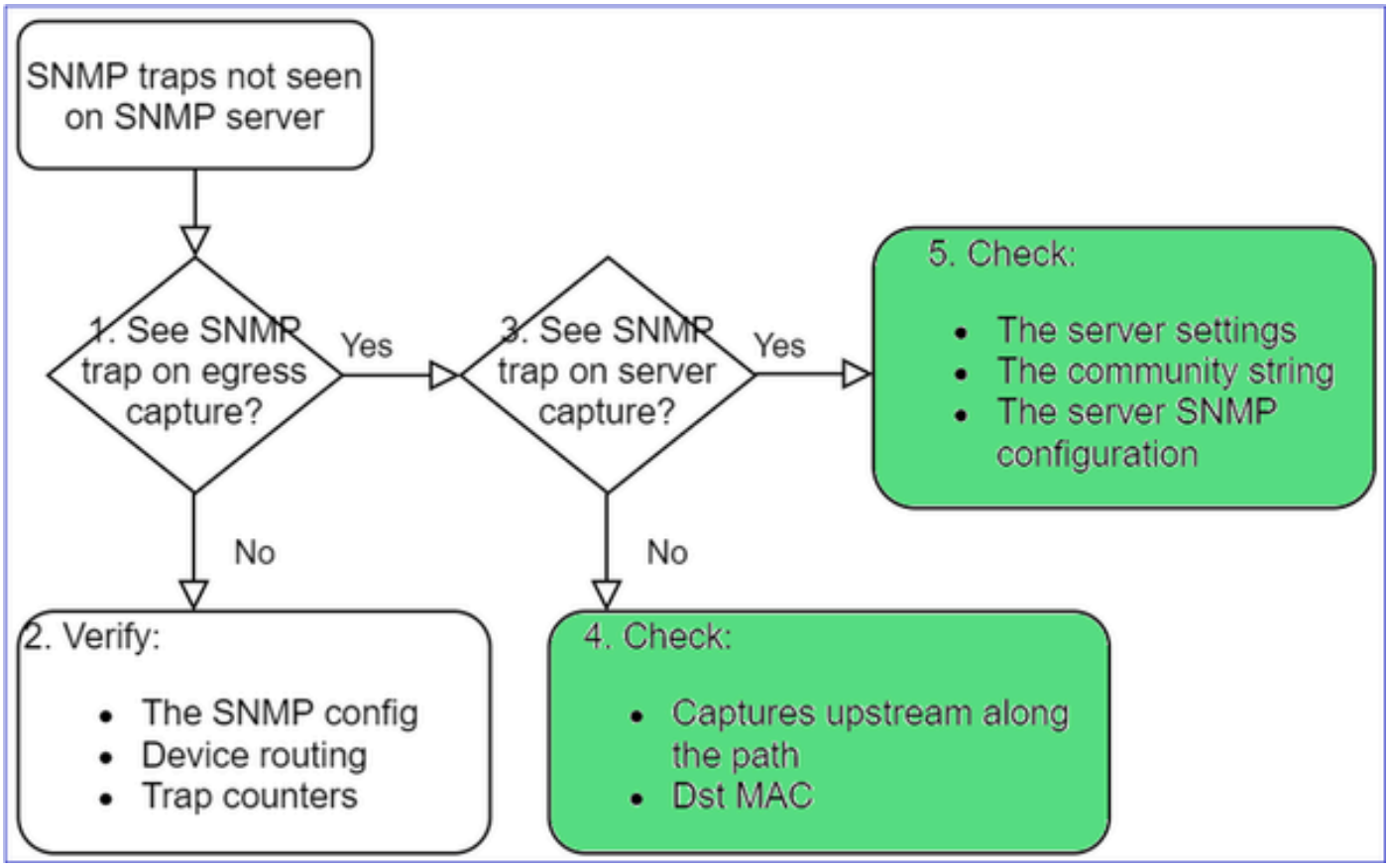
connect fxos

FP4145-1(fxos)#

show snmp | grep Trap
```

```
1296 Out Traps PDU
```

Additional Checks



- Take a capture on the destination SNMP server.

Other things to check:

- Captures along the path.
- Destination MAC address of SNMP trap packets.
- The SNMP server settings and status (for example, firewall, open ports, and so on).
- The SNMP community string.
- The SNMP server configuration.

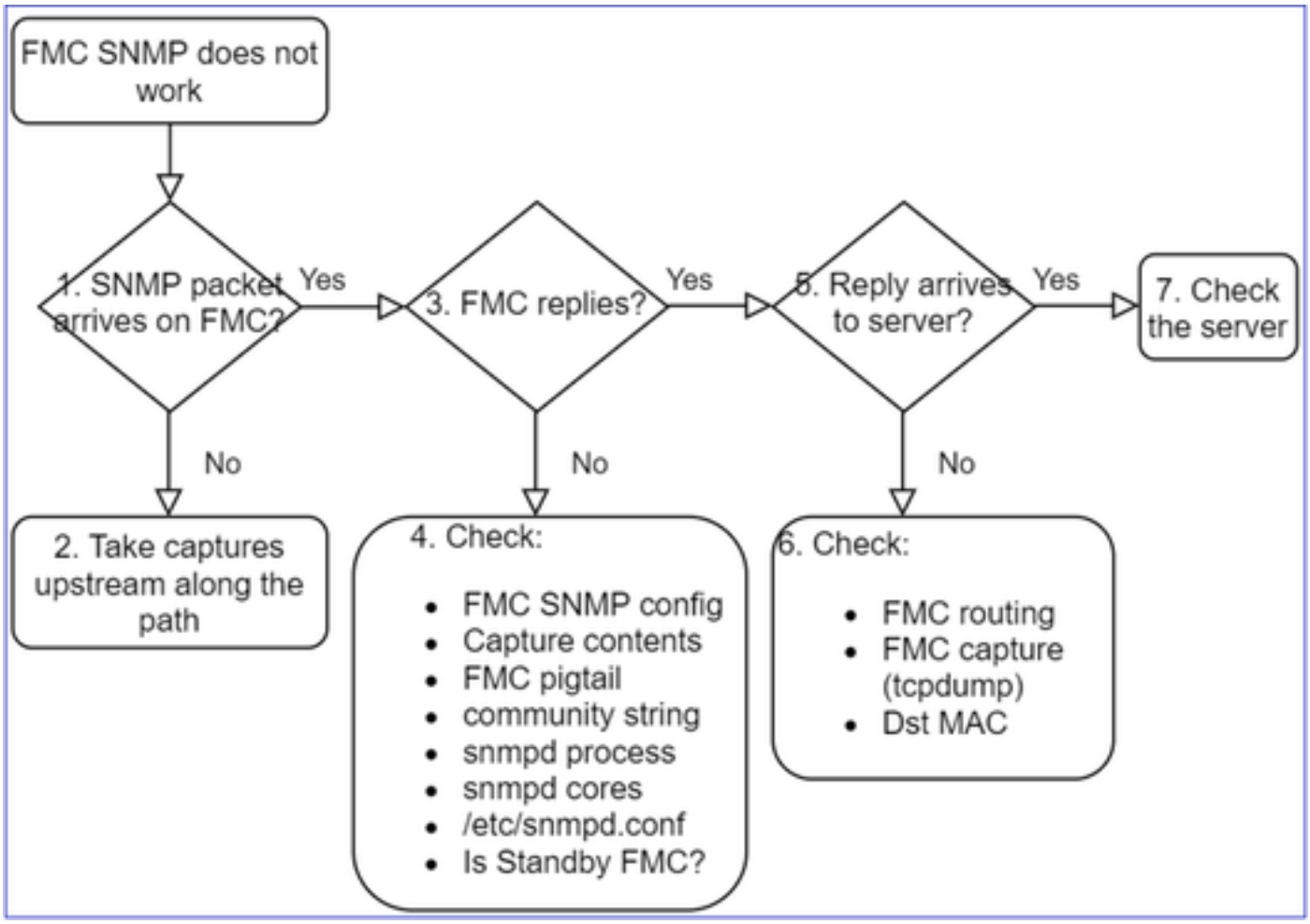
Cannot Monitor FMC via SNMP

Problem Descriptions (sample from real Cisco TAC cases):

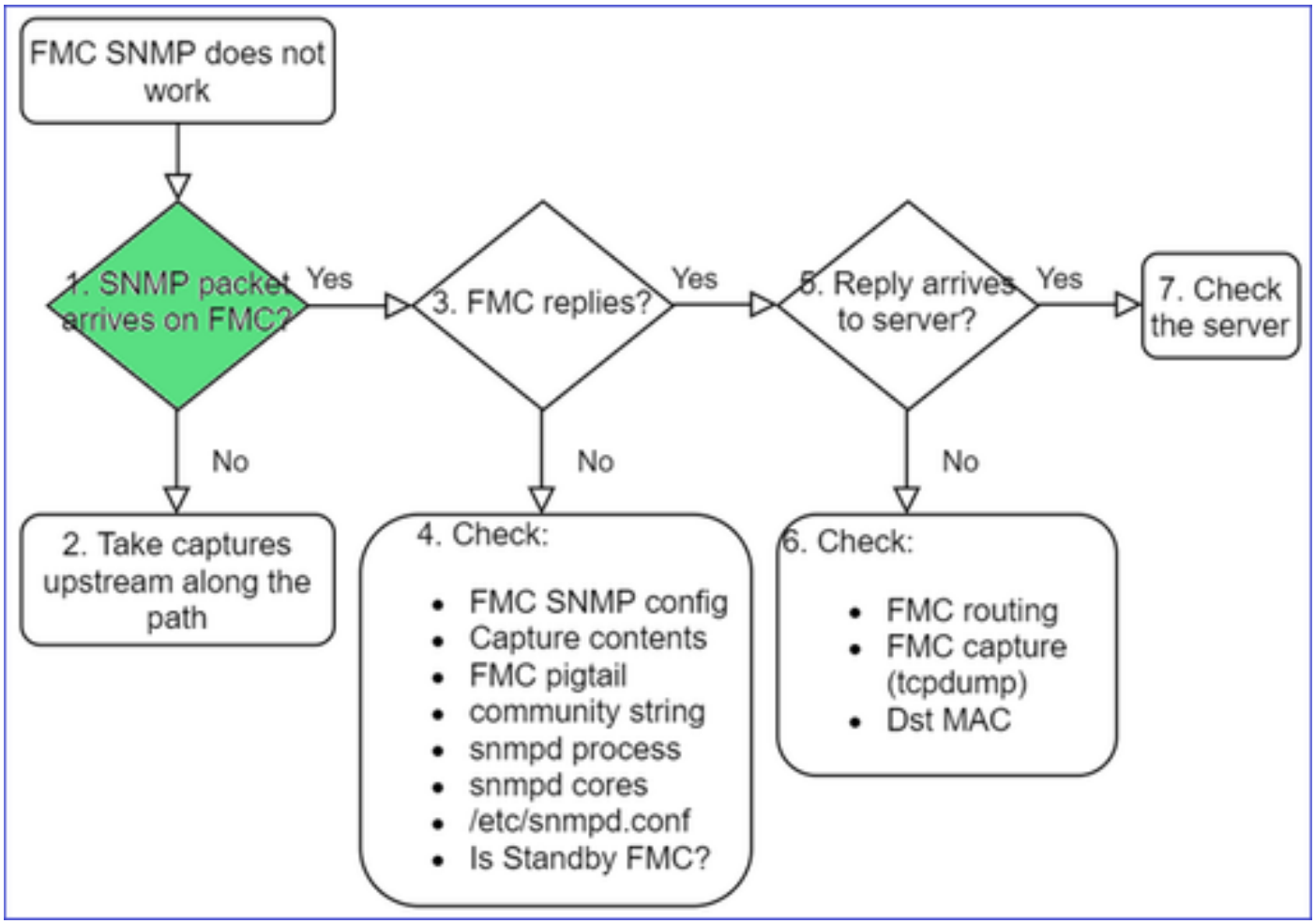
- "SNMP does not work on Standby FMC."
- "Need to monitor the FMC memory."
- "Should SNMP be functional on Standby 192.168.4.0.8 FMC?"
- "We have to configure the FMCs to monitor their resources like CPU, memory, and so on".

How to Troubleshoot

This is the process to troubleshoot flowchart for FMC SNMP issues:



1. SNMP packet arrives on FMC?



- Capture on FMC management interface:

<#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
```

Tip: Save the capture on FMC /var/common/ directory and download it from the FMC UI

<#root>

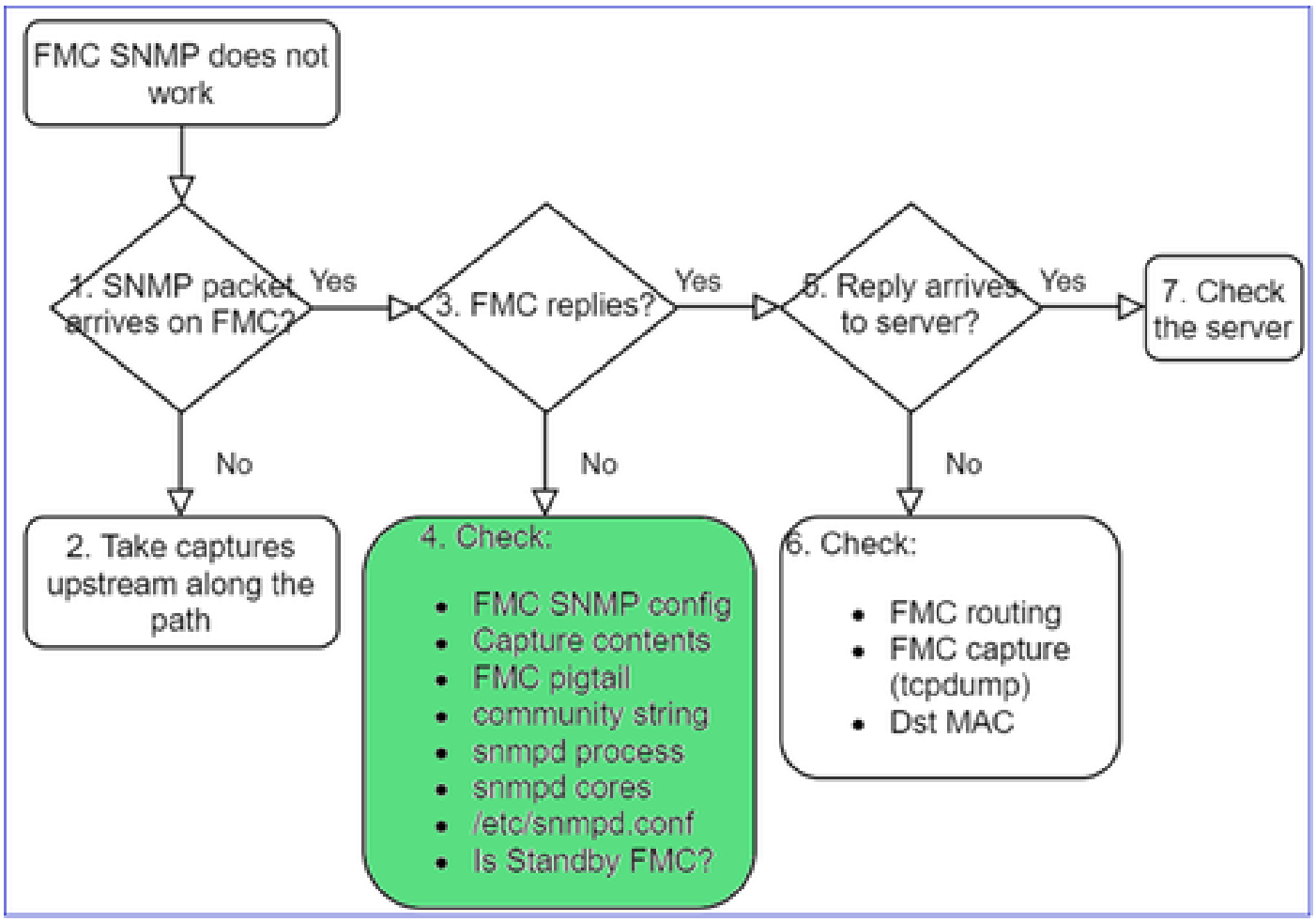
```
admin@FS2600-2:~$
```

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
```

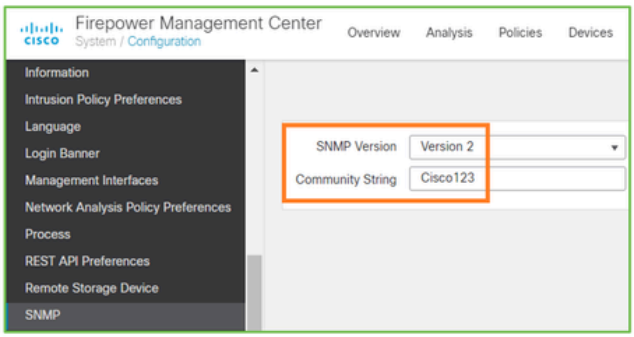
```
46 packets received by filter
```

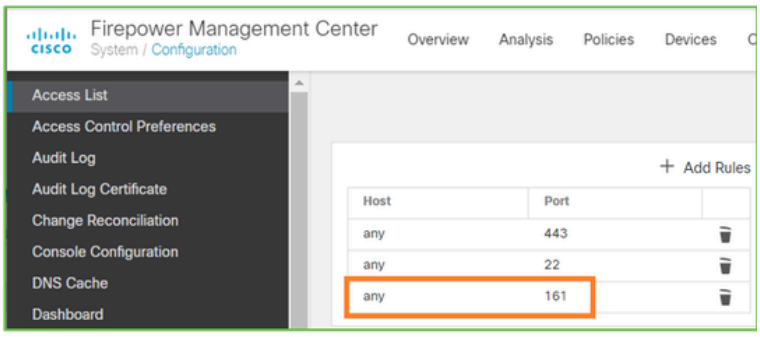
Does FMC reply?



If FMC does not reply check:

- FMC SNMP config (System > Configuration)
    1. SNMP section
    2. Access List section





If FMC does not reply check:

- Capture (pcap) contents
- Community string (this can be seen in the captures)
- FMC pigtail output (look for errors, failures, traces) and contents of /var/log/snmpd.log

- snmpd process

<#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 cores

<#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
```

- Backend configuration file in /etc/snmpd.conf:

<#root>

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

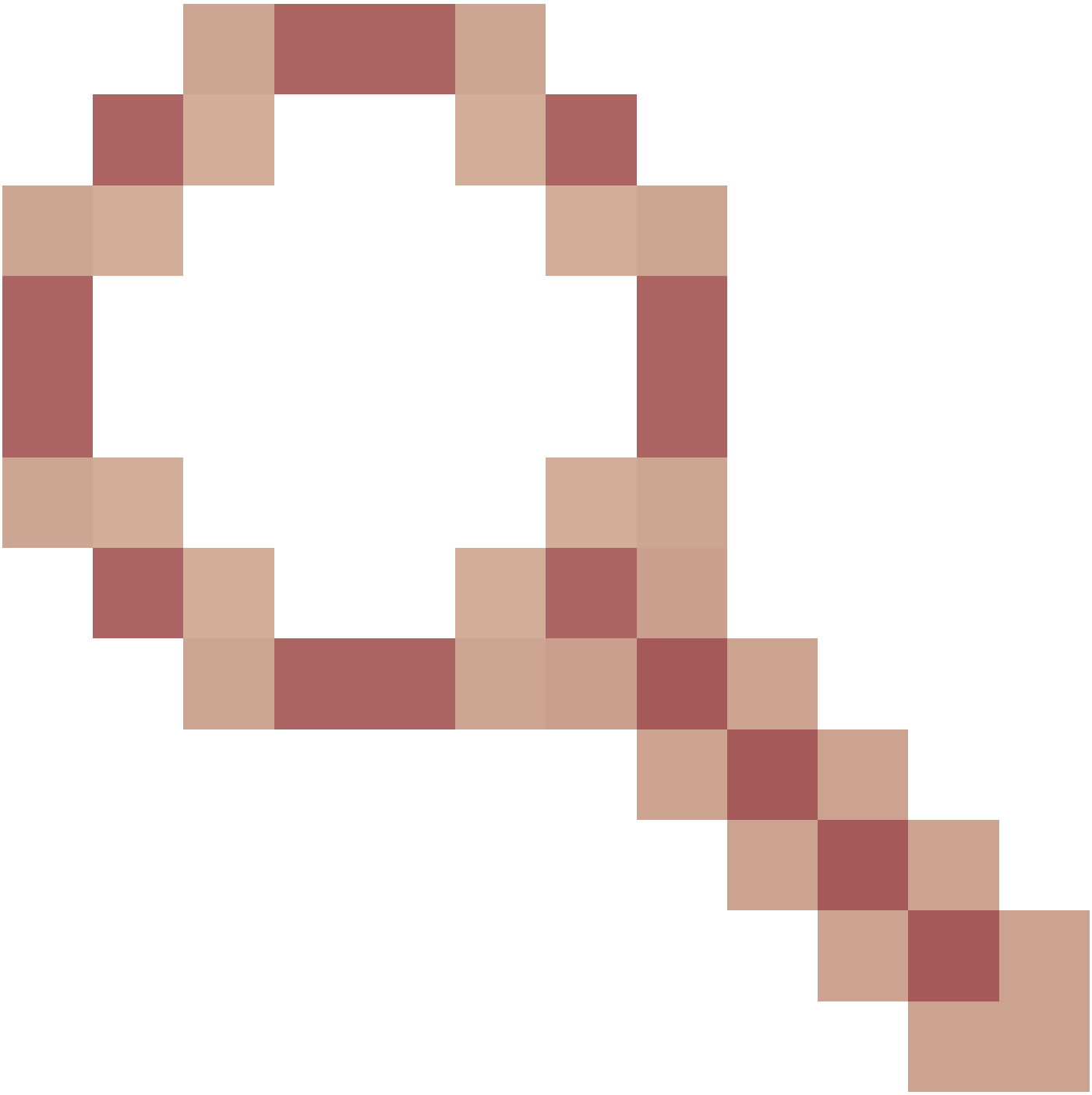
sudo cat /etc/snmpd.conf

```
# 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
```

Note: If SNMP is disabled, the snmpd.conf file does not exist

- Is it a standby FMC?

In pre-6.4.0-9 and pre-6.6.0, the standby FMC does not send SNMP data (snmpd is in Waiting status). This is expected behavior. Check Enhancement Cisco bug ID CSCvs32303



Unable to Configure SNMP

Problem Descriptions (sample from real Cisco TAC cases):

- "We want to configure SNMP for Cisco Firepower Management Center and Firepower 4115 Threat Defense."
- "Support with SNMP config on FTD".
- "We want to enable SNMP monitoring on my FTD appliance."
- "We try to configure the SNMP service in FXOS, but the system does not let us commit-buffer in the end. It says Error: Changes not allowed. use 'Connect ftd' to make changes."
- "We want to enable SNMP monitoring on our FTD appliance."
- "Unable to configure SNMP on FTD and discover the device in monitoring."

How to Approach SNMP Configuration Issues

Read the current documentation:

- FMC Config Guide:

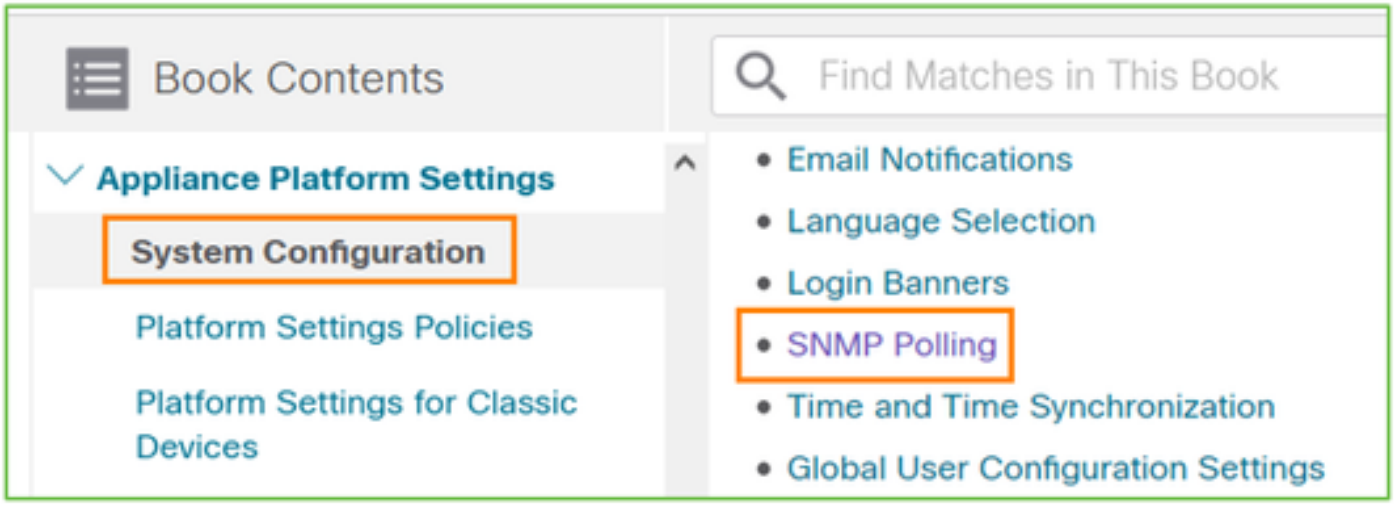
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html

- FXOS Config Guide:

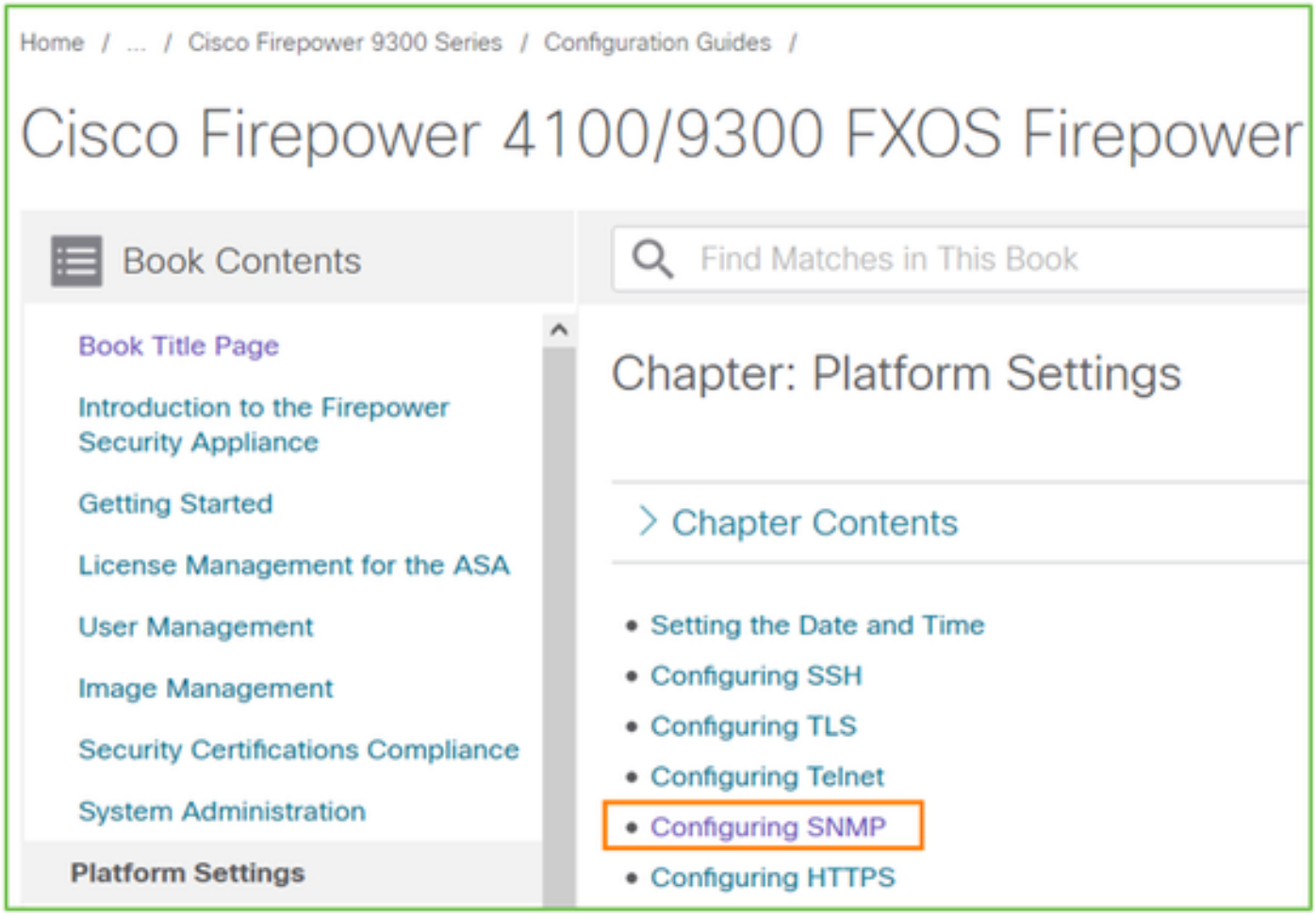
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB115F5

Be familiar with the SNMP documentation, specifically.

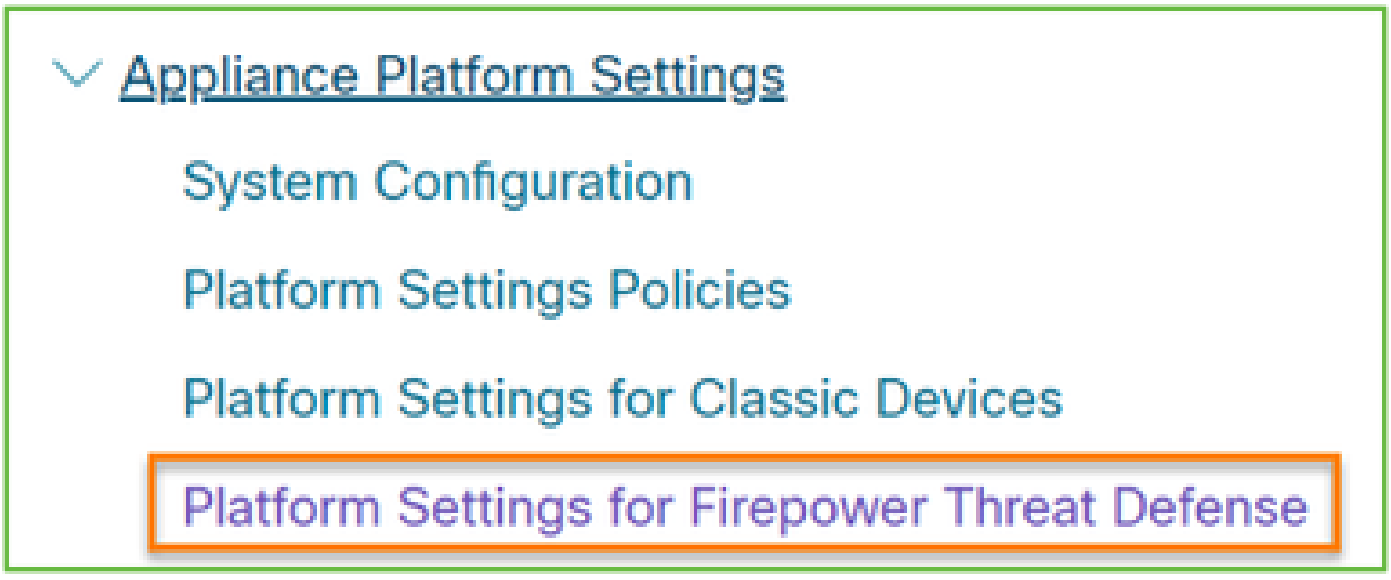
FMC SNMP:



FXOS SNMP:



Firepower 41xx/9300 SNMP Configuration:



Firepower 1xxx/21xx SNMP Configuration:



SNMP Config on Firepower Device Manager (FDM)

Problem Descriptions (sample from real Cisco TAC cases):

- "We need guidance about SNMPv3 on device Firepower with FDM."
- "SNMP configuration does not work on FPR 2100 device from FDM."
- "Cannot get SNMP v3 configuration to work on the FDM."
- "FDM 6.7 SNMP Configuration Assistance."
- "Enable SNMP v3 in Firepower FDM."

How to Approach SNMP FDM Configuration Issues

- For version pre-6.7, you can do SNMP configuration with the use of FlexConfig:

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

- As from Firepower version 6.7, SNMP configuration is no longer made with FlexConfig, but with REST API:

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

SNMP Troubleshooting Cheat Sheets

1xxx/21xx/41xx/9300 (LINA/ASA) – What to collect before you open a case with Cisco TAC

Command	**Description**
firepower# show run snmp-server	Verify the ASA/FTD LINA SNMP configuration.
firepower# show snmp-server statistics	Verify the SNMP statistics on ASA/FTD LINA. Focus on the SNMP packets input and SNMP packets output counters.

> capture-traffic	Capture traffic on mgmt interface.
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	Capture traffic on data interface (nameif ‘net201’) for UDP 161 (SNMP poll).
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	Capture traffic on data interface (nameif ‘net208’) for UDP 162. (SNMP traps).
firepower# show capture SNMP-POLL packet-number 1 trace	Trace an ingress SNMP packet that arrives on ASA/FTD LINA data interface.
admin@firepower:~$ sudo tcpdump -i tap_nlp	Capture on the NLP (Non-Lina Process) internal tap interface.
firepower# show conn all protocol udp port 161	Check all ASA/FTD LINA connections on UDP 161 (SNMP poll).
firepower# show log | i 302015.*161	Check ASA/FTD LINA log 302015 for SNMP poll.
firepower# more system:running-config | i community	Check the SNMP community string.
firepower# debug menu netsnmp 4	Verify the SNMP configuration and process ID.
firepower# show asp table classify interface net201 domain permit match port=161	Check the hitcounts on the SNMP ACL on interface named ‘net201’.
firepower# show disk0: | i core	Check if there are any SNMP cores.
admin@firepower:~$ ls -l /var/data/cores	Check if there are any SNMP cores. Applicable only on FTD.
firepower# show route	Verify the ASA/FTD LINA routing table.
> show network	Verify the FTD mgmt plane routing table.
admin@firepower:~$ tail -f /mnt/disk0/log/ma_ctx2000.log	Verify/Troubleshoot SNMPv3 on FTD.
firepower# debug snmp trace [255]	Hidden commands on newer releases. Internal debugs,

firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	useful to troubleshoot SNMP with Cisco TAC.

41xx/9300 (FXOS) – What to collect before you open a case with Cisco TAC

Command	**Description**
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	FXOS capture for SNMP poll (UDP 161) Upload to a remote FTP server FTP IP: 192.0.2.100 FTP username: ftp
firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap	FXOS capture for SNMP traps (UDP 162)
firepower# scope system firepower /system # scope services firepower /system/services # show ip-block detail	Check the FXOS ACL
firepower# show fault	Check for FXOS faults
firepower# show fabric-interconnect	Verify the FXOS interface configuration and default gateway settings
firepower# connect fxos firepower(fxos)# show running-config snmp all	Verify the FXOS SNMP configuration

firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	Verify the FXOS SNMP OIDs
firepower# connect fxos firepower(fxos)# show snmp	Verify the FXOS SNMP settings and counters
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	Debug FXOS SNMP (‘packets’ or ‘all’) Use ‘terminal no monitor’ and ‘undebug all’ to stop it

1xxx/21xx (FXOS) – What to collect before you open a case with Cisco TAC

Command	**Description**
> capture-traffic	Capture traffic on mgmt interface
> show network	Verify the FTD mgmt plane routing table
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail] firepower /monitoring # show snmp-trap	Verify FXOS SNMP configuration
firepower# show fault	Check for FXOS faults
firepower# connect local-mgmt firepower(local-mgmt)# dir cores_fxos firepower(local-mgmt)# dir cores	Check for FXOS core files (tracebacks)

FMC – What to collect before you open a case with Cisco TAC

Command	Description
admin@FS2600-2:~$ sudo tcpdump -i eth0 udp port 161 -n	Capture traffic on mgmt interface for SNMP poll
admin@FS2600-2:~$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	Capture traffic on mgmt interface for SNMP poll and save it to a file
admin@FS2600-2:~$ sudo pmtool status | grep snmpd	Check the SNMP process status
admin@FS2600-2:~$ ls -al /var/common | grep snmpd	Check for SNMP core files (tracebacks)
admin@FS2600-2:~$ sudo cat /etc/snmpd.conf	Check the contents of the SNMP config file

snmpwalk Examples

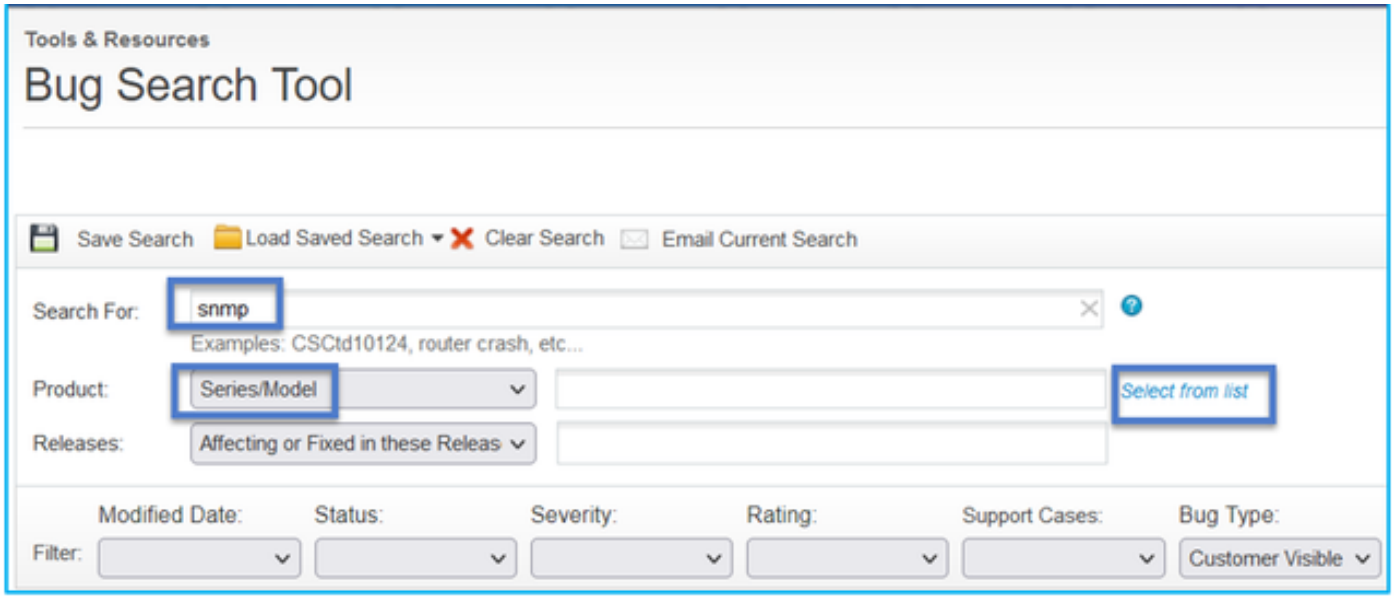
These commands can be used for verification and troubleshooting:

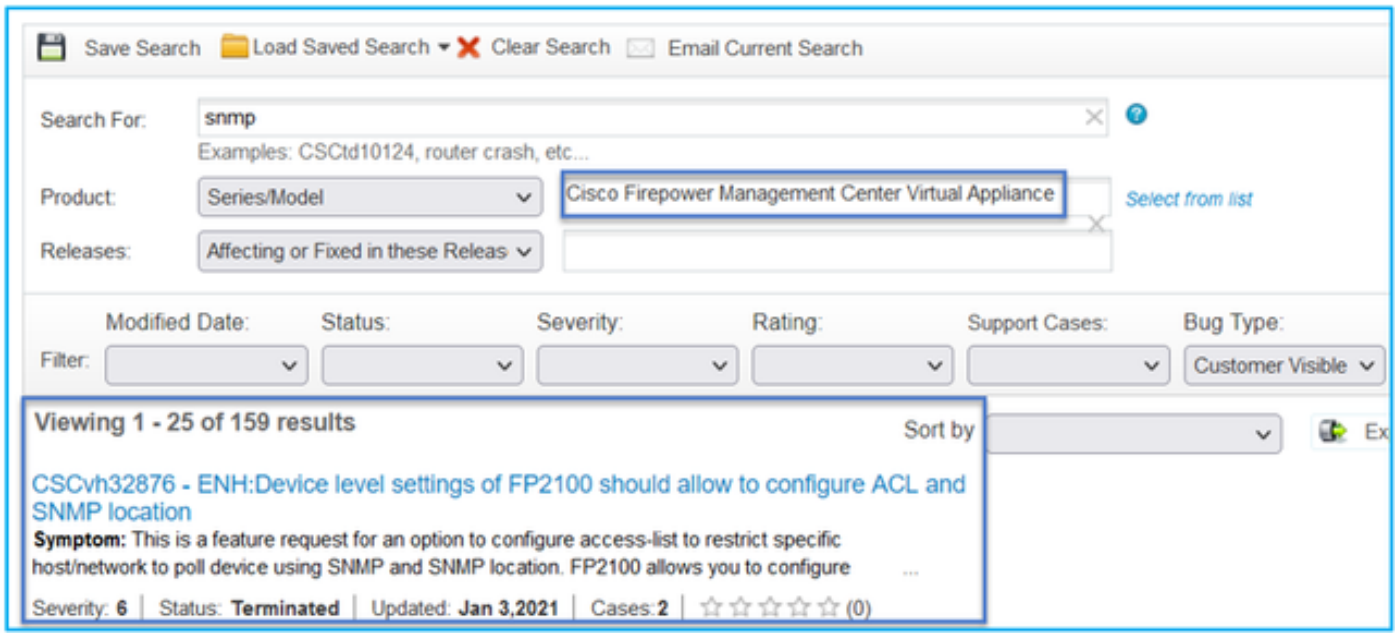
Command	Description
# snmpwalk -c Cisco123 -v2c 192.0.2.1	Fetches all OIDs from the remote host with the use of SNMP v2c. Cisco123 = Community string 192.0.2.1 = destination host
# snmpwalk -v2c -c Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.9.109.1.1.1.1.3 iso.3.6.1.4.1.9.9.109.1.1.1.1.3.1 = Gauge32: 0	Fetches a specific OID from the remote host with the use of SNMP v2c
# 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	Shows the fetched OIDs in numeric format
# snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1	Fetches all OIDs from the remote host with the use of SNMP v3. SNMPv3 user = cisco SNMPv3 authentication = SHA. SNMPv3 authorization = AES

# snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -x AES -X Cisco123 192.0.2.1	Fetches all OIDs from the remote host with the use of SNMP v3 (MD5 and AES128)
# snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1	SNMPv3 with Authentication only

How to Search for SNMP Defects

1. Navigate to https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV
2. Enter the keyword **snmp** and choose **Select from list**.





Most common Products:

- Cisco Adaptive Security Appliance (ASA) Software
- Cisco Firepower 9300 Series
- Cisco Firepower Management Center Virtual Appliance

- Cisco Firepower NGFW

Related information

- **Configure SNMP for Threat Defense**
- **Configure SNMP on FXOS (UI)**
- **Technical Support & Documentation - Cisco Systems**