

SNMP configureren op FirePOWER NGFW-applicaties

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Chassis \(FXOS\) SNMP op FPR4100/FPR9300](#)

[FXOS SNMPv1/v2c configureren via GUI](#)

[FXOS SNMPv1/v2c configureren via Command Line Interface \(CLI\)](#)

[FXOS SNMPv3 configureren via GUI](#)

[FXOS SNMPv3 via CLI configureren](#)

[FTD \(LINA\) SNMP op FPR4100/FPR9300](#)

[LINA SNMPv2c configureren](#)

[LINA SNMPv3 configureren](#)

[SNMP in FPR210](#)

[Chassis \(FXOS\) SNMP op FPR210](#)

[FXOS SNMPv1/v2c configureren](#)

[FXOS SNMPv3 configureren](#)

[FTD \(LINA\) SNMP op FPR2100](#)

[Verifiëren](#)

[Controleer FXOS SNMP voor FPR4100/FPR9300](#)

[FXOS SNMPv2c-verificaties](#)

[FXOS SNMPv3-verificaties](#)

[Controleer FXOS SNMP voor FPR2100](#)

[FXOS SNMPv2-verificaties](#)

[FXOS SNMPv3-verificaties](#)

[Controleer FTD SNMP](#)

[SNMP-verkeer naar FXOS toestaan op FPR4100/FPR9300](#)

[Wereldwijde toegangslijst configureren via GUI](#)

[Wereldwijde toegangslijst configureren via CLI](#)

[Verificatie](#)

[Gebruik de OID Object Navigator](#)

[Problemen oplossen](#)

[Kan FTD LINA SNMP niet ophalen](#)

[Kan FXOS SNMP niet ophalen](#)

[Welke SNMP OID-waarden moeten worden gebruikt?](#)

[Kan SNMP-traps niet ophalen](#)

[Kan FMC niet via SNMP bewaken](#)

[SNMP-configuratie op Firepower Device Manager \(FDM\)](#)

[SNMP-printerbladen voor probleemoplossing](#)

[Hoe te zoeken naar SNMP-defecten](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Simple Network Management Protocol (SNMP) op FTD-apparaten (Next Generation Firewall (NGFW) kunt configureren en problemen kunt oplossen.

Voorwaarden

Vereisten

Dit document vereist basiskennis van het SNMP-protocol.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Firepower NGFW-apparaten kunnen worden opgesplitst in 2 belangrijke subsystemen:

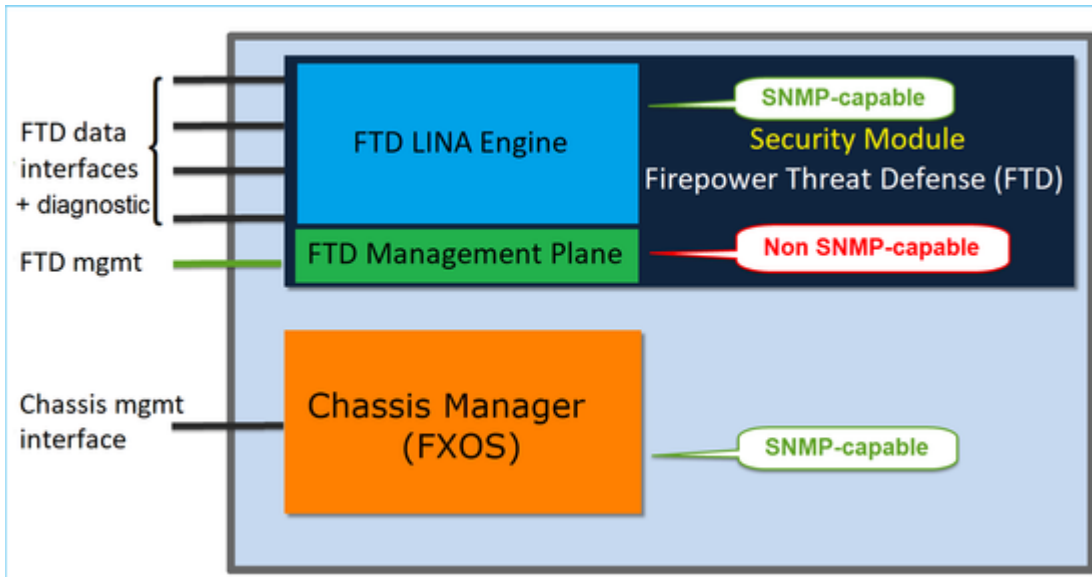
- Het Firepower Extensible Operating System (FX-OS) regelt de hardware van het chassis.
- De Firepower Threat Defense (FTD) wordt uitgevoerd binnen de module.

FTD is een geünificeerde software die bestaat uit 2 hoofdmotoren, de Snort-motor en de LINA-motor. De huidige SNMP-motor van de FTD is afgeleid van de klassieke ASA en het heeft zicht op de LINA-gerelateerde functies.

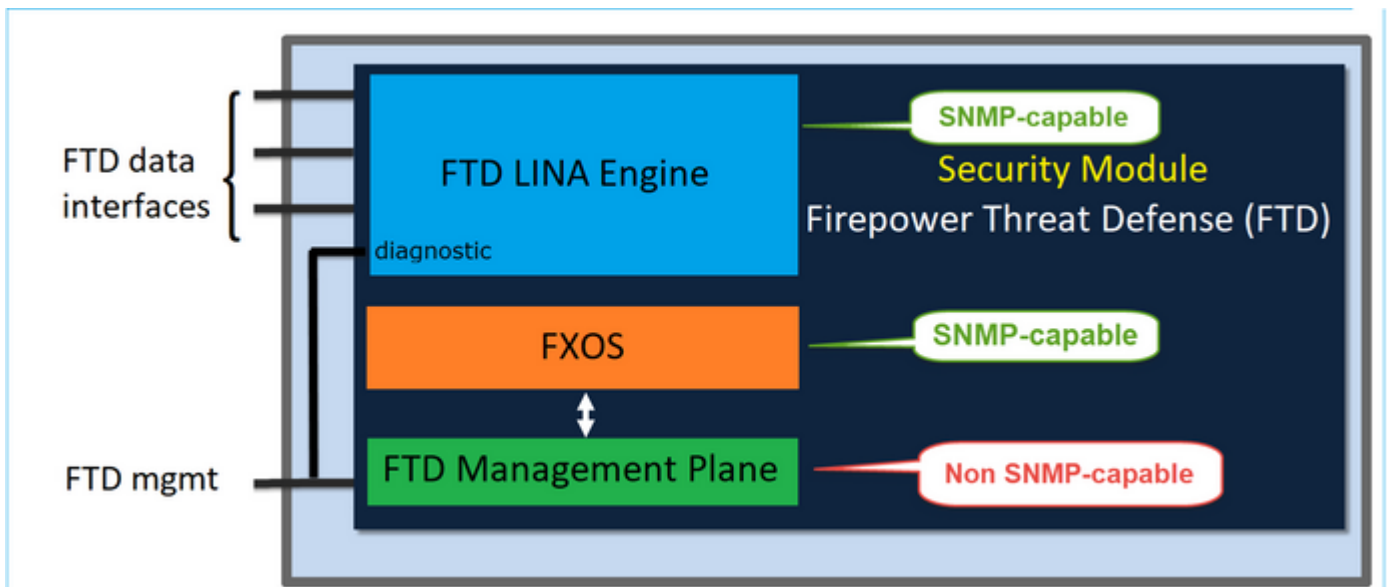
FX-OS en FTD hebben onafhankelijke besturingsplanen en voor monitordoeleinden hebben ze verschillende SNMP-motoren. Elk van de SNMP-motoren biedt verschillende informatie en kan zowel voor een uitgebreidere weergave van de apparaatstatus willen monitoren.

Vanuit hardwarestandpunt zijn er momenteel twee belangrijke architecturen voor de Firepower NGFW-toestellen: de Firepower 2100-serie en de Firepower 4100/9300-serie.

Firepower 4100/9300 apparaten hebben een speciale interface voor apparaatbeheer en dit is de bron en bestemming voor het SNMP-verkeer dat is gericht aan het FXOS-subsysteem. Anderzijds maakt de FTD-applicatie gebruik van een LINA-interface (data en/of diagnostische gegevens). In post-6.6 FTD releases kan ook de FTD management interface worden gebruikt) voor de SNMP configuratie.



De SNMP-engine op FirePOWER 2100-toestellen maakt gebruik van de FTD-beheerinterface en IP. Het apparaat zelf overbrugt het SNMP-verkeer dat op deze interface is ontvangen en stuurt het door naar de FXOS-software.

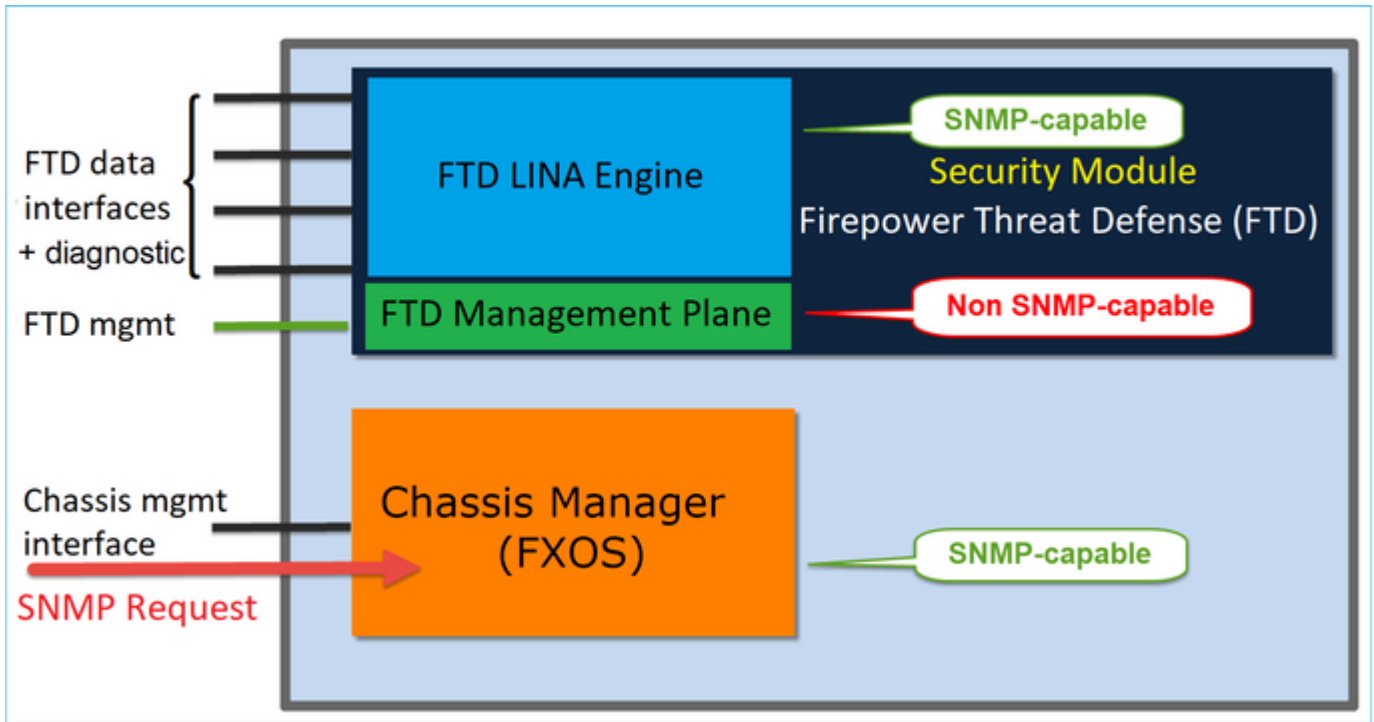


Op FTD's die software release 6.6+ gebruiken, werden deze wijzigingen geïntroduceerd:

- SNMP via de beheerinterface.
- Op de platforms van de FPR1000 of FPR2100 Series worden zowel LINA SNMP als FXOS SNMP gecombineerd via deze single Management interface. Bovendien biedt het één configuratiepunt op FMC onder **Platform Instellingen > SNMP**.

Configureren

Chassis (FXOS) SNMP op FPR4100/FPR9300



FXOS SNMPv1/v2c configureren via GUI

Stap 1. Open de Firepower Chassis Manager (FCM) UI en navigeer naar **Platform Instellingen > SNMP** tabblad. Schakel het vakje **SNMP Enable** in, specificeer de **Community**-string die moet worden gebruikt op SNMP-verzoeken en **Sla op**.

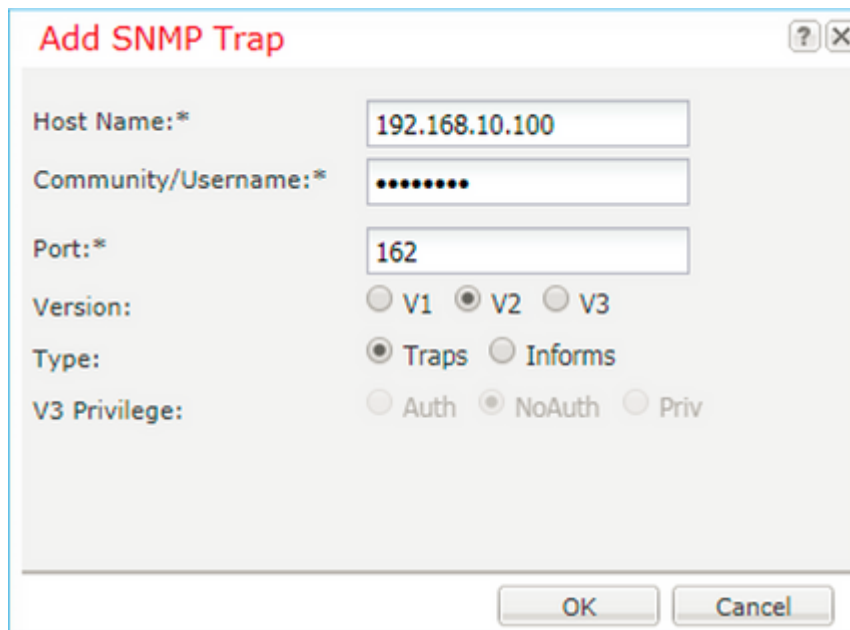
The screenshot shows the 'Platform Settings' tab in the FCM GUI, specifically the 'SNMP' configuration page. The following elements are highlighted with red boxes and numbered:

- Admin State:** The 'Enable' checkbox is checked.
- Community/Username:** A text field containing a masked string (represented by dots).
- Save:** The 'Save' button at the bottom left of the configuration area.
- Add:** The 'Add' button in the 'SNMP Traps' section.

The 'SNMP Traps' section contains a table with the following columns: Name, Port, Version, V3 Privilege, and Type. The 'SNMP Users' section contains a table with the following columns: Name, Auth Type, and AES-128.

Opmerking: als het veld Community/Gebruikersnaam al is ingesteld, wordt de tekst rechts van het lege veld **Ingesteld: Ja**. Als het veld Community/Gebruikersnaam nog niet met een waarde is ingevuld, wordt de tekst rechts van het lege veld **Ingesteld: Nee**

Stap 2. Configureer de doelserver voor SNMP-traps.



Add SNMP Trap

Host Name:* 192.168.10.100

Community/Username:* *****

Port:* 162

Version: V1 V2 V3

Type: Traps Informs

V3 Privilege: Auth NoAuth Priv

OK Cancel

Opmerking: de community-waarden voor queries en trap-host zijn onafhankelijk en kunnen verschillen

De host kan gedefinieerd worden als IP-adres of op naam. Selecteer **OK** en de configuratie van de SNMP Trap server wordt automatisch opgeslagen. U hoeft de knop Opslaan niet op de hoofdpagina van SNMP te selecteren. Het zelfde gebeurt wanneer u een gastheer schraapt.

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

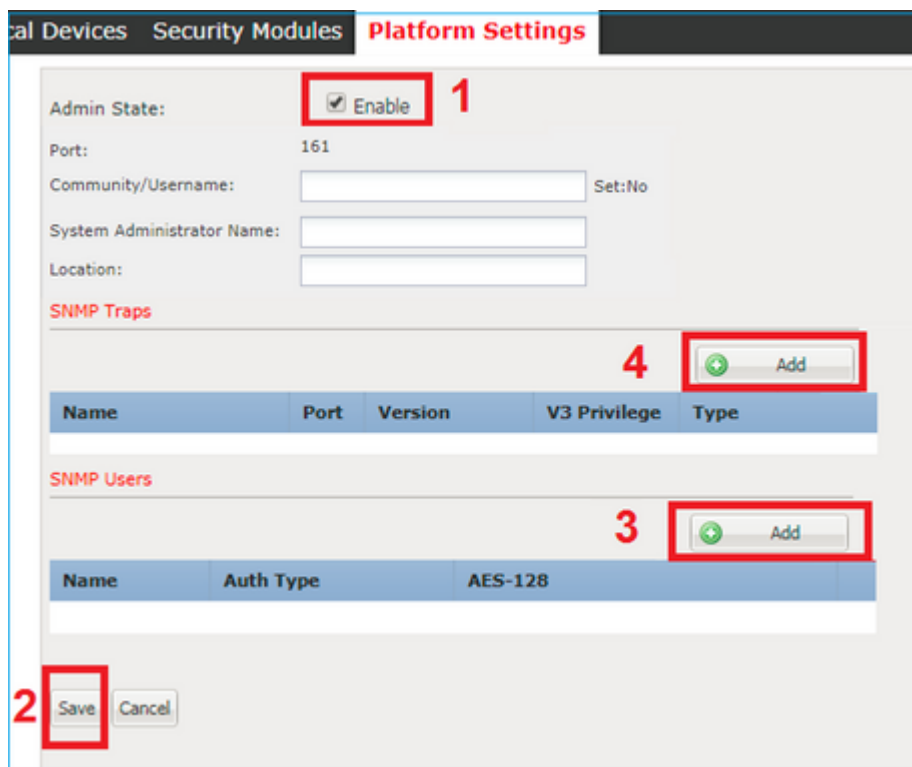
```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring* #
set snmp community
Enter a snmp community:
ksec-fpr9k-1-A /monitoring* #
  enter snmp-trap 192.168.10.100
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /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
```

FXOS SNMPv3 configureren via GUI

Stap 1. Open FCM en navigeer naar **Platform Instellingen > SNMP** tabblad.

Stap 2. Voor SNMP v3 is het niet nodig om een community string in te stellen in het bovenste gedeelte. Elke gebruiker die wordt gemaakt kan met succes vragen naar de FXOS SNMP engine uitvoeren. De eerste stap is SNMP in het platform toe te laten. Als u dit hebt gedaan, kunt u de gebruikers en de doeltrap-host maken. Zowel SNMP-gebruikers als SNMP-traphosts worden automatisch opgeslagen.



The screenshot shows the 'Platform Settings' tab for SNMP configuration. The 'Admin State' is set to 'Enable' (1). The 'Port' is 161. There are 'Add' buttons for 'SNMP Traps' (4) and 'SNMP Users' (3). A 'Save' button is highlighted (2).

Name	Port	Version	V3 Privilege	Type
------	------	---------	--------------	------

Name	Auth Type	AES-128
------	-----------	---------

Stap 3. Zoals in het beeld wordt getoond, voeg de SNMP-gebruiker toe. Het verificatietype is altijd SHA, maar u kunt AES of DES voor codering gebruiken:

Add SNMP User

Name:* user1

Auth Type: SHA

Use AES-128:

Password:

Confirm Password:

Privacy Password:

Confirm Privacy Password:

OK Cancel

Stap 4. Voeg de SNMP-trap-host toe, zoals in de afbeelding:

Add SNMP Trap

Host Name:* 192.168.10.100

Community/Username:*

Port:* 162

Version: V1 V2 V3

Type: Traps Informs

V3 Privilege: Auth NoAuth Priv

OK Cancel

FXOS SNMPv3 via CLI configureren

```
<#root>
```

```
ksec-fpr9k-1-A#
```

```
scope monitoring
```

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

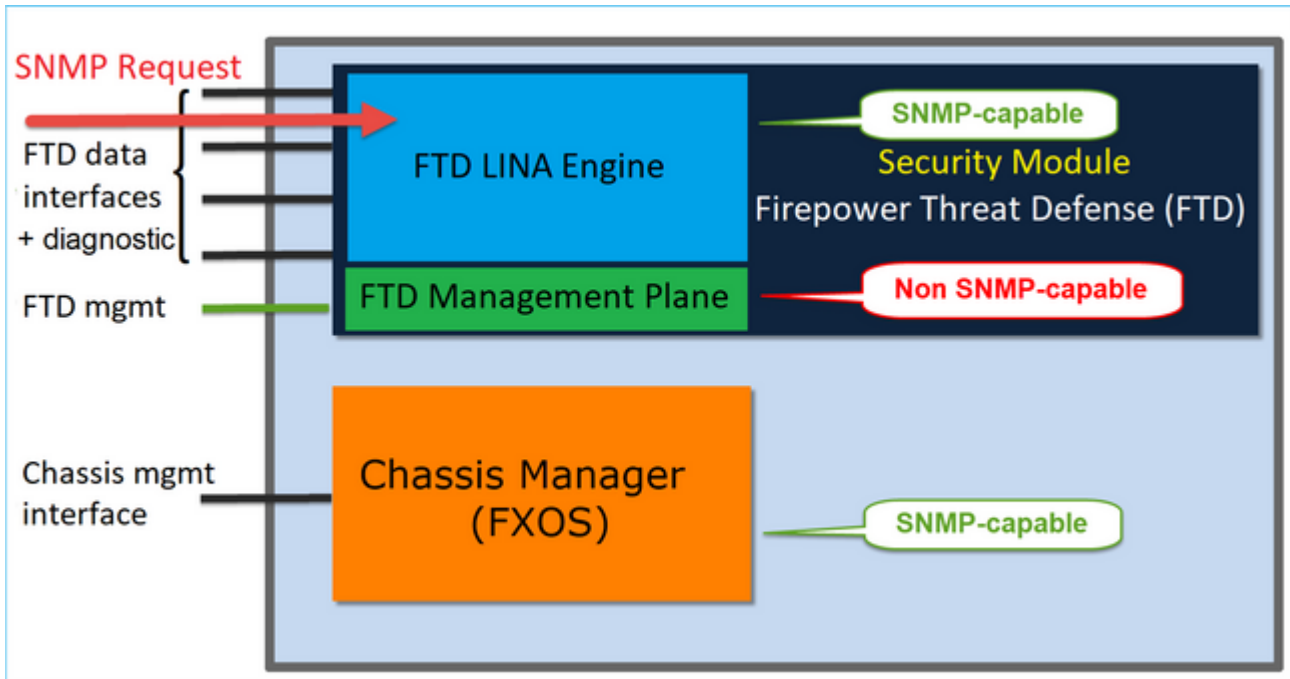
```
enable snmp
```

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

```
create snmp-user user1
```

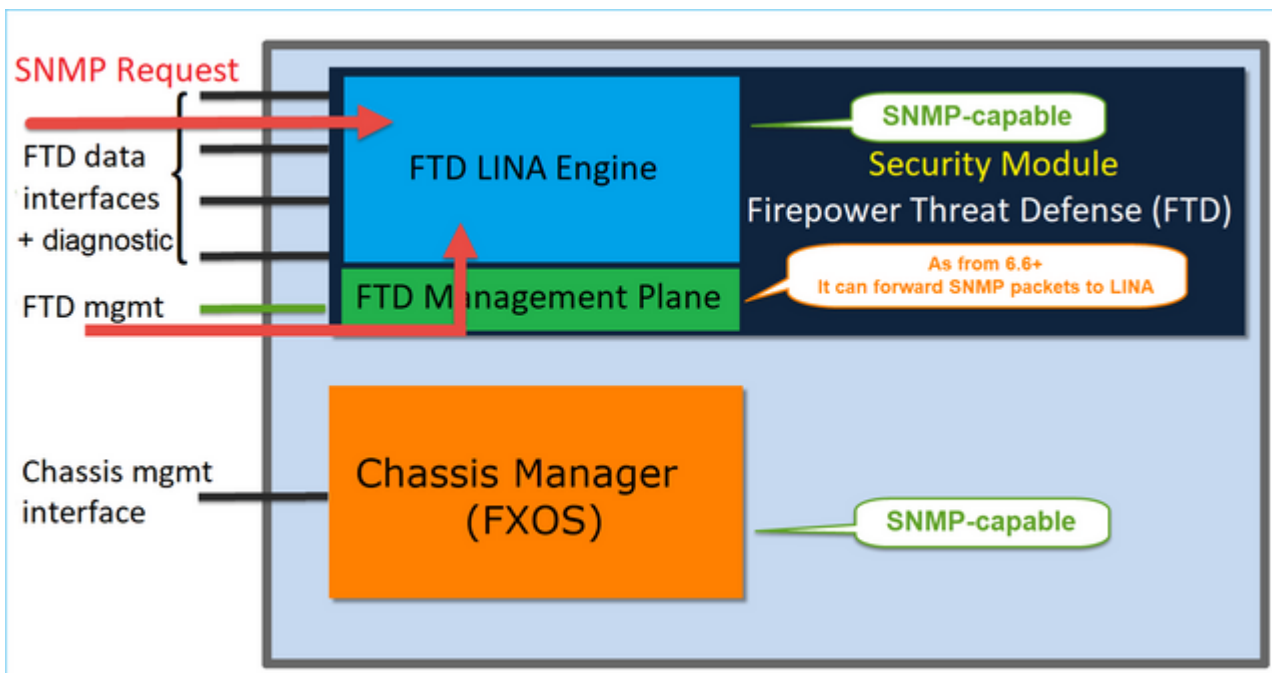
```
Password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set auth sha
ksec-fpr9k-1-A /monitoring/snmp-user* #
set priv-password
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter 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 op FPR4100/FPR9300



Veranderingen in 6.6+ releases

- In post-6.6 releases, hebt u ook de optie om de FTD-beheerinterface te gebruiken voor polls en traps.



SNMP Single IP-beheerfunctie wordt vanaf 6.6 ondersteund op alle FTD-platforms:

- FPR210
- FPR 1000
- FPR4100
- FPR9300
- ASA 5500 die FTD draait
- FTDv

LINA SNMPv2c configureren

Stap 1. Ga op FMC UI naar **Apparaten > Platform-instellingen > SNMP**. Controleer de optie **SNMP-servers inschakelen** en stel de SNMPv2-instellingen als volgt in:

Stap 2. Selecteer op het tabblad **Hosts** de knop **Add** en specificeer de SNMP-serverinstellingen:

Edit SNMP Management Hosts ? X

IP Address* +

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port

Available Zones ↻

- INSIDE_FTD4110
- OUTSIDE1_FTD4110
- OUTSIDE2_FTD4110
- NET1_4100-3
- NET2_4100-3
- NET3_4100-3

Selected Zones/Interfaces

- OUTSIDE3

Add

Interface Name Add

OK Cancel

U kunt de **diagnostische** interface ook opgeven als bron voor de SNMP-berichten. De diagnostische interface is een data-interface die alleen verkeer naar de-box en van-de-box (alleen beheer) toestaat.

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 ⌵

Q Search Add

- 2100_inside
- 2100_outside
- cluster_dmz
- cluster_inside
- cluster_outside

Selected Zones/Interfaces

diagnostic 🗑

Interface Name Add

Cancel OK

Dit beeld is afkomstig van de 6.6 release en gebruikt het Light Theme.

Daarnaast kunt u in post-6.6 FTD releases ook de beheerinterface kiezen:

Add SNMP Management Hosts

IP Address*
 +

SNMP Version

Username

Community String

Confirm

Poll
 Trap

Trap Port

(1 - 65535)

Reachable By:

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

Security Zones or Named Interface

Available Zones

- 2100_inside
- 2100_outside
- cluster_dmz
- cluster_inside
- cluster_outside

Selected Zones/Interfaces

diagnostic

Interface Name

Als de nieuwe beheerinterface is geselecteerd, is LINA SNMP beschikbaar via de beheerinterface.

Het resultaat:

- 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

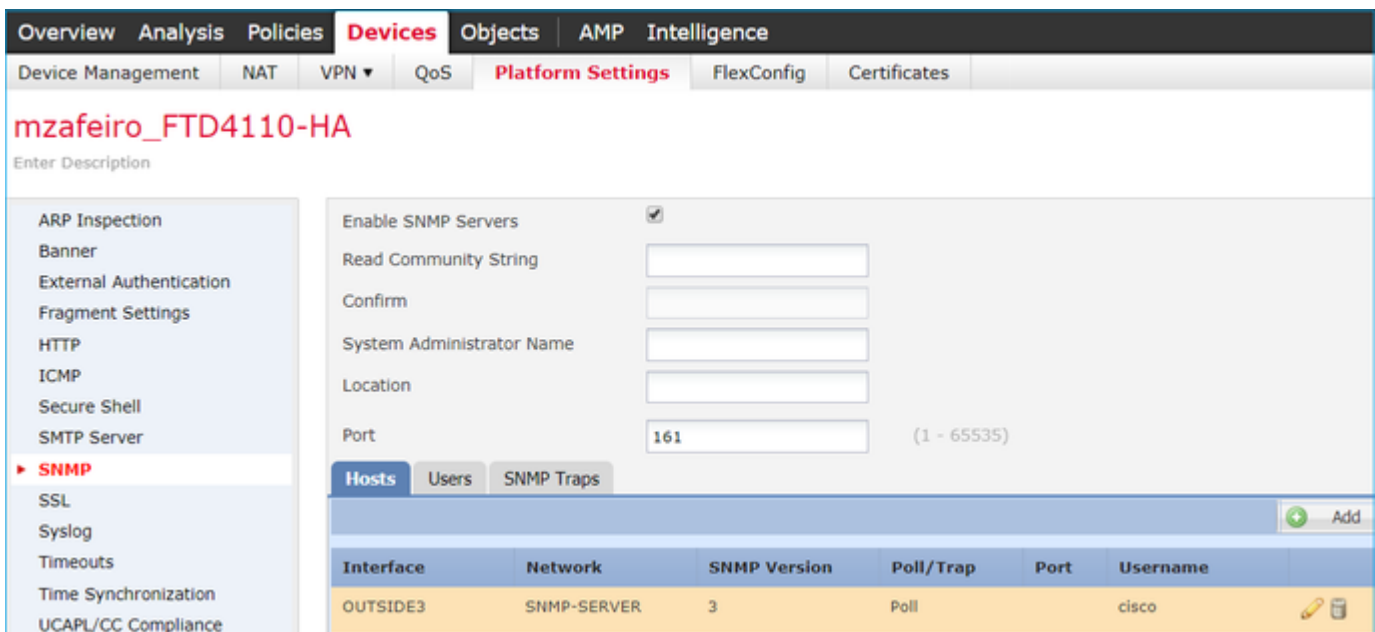
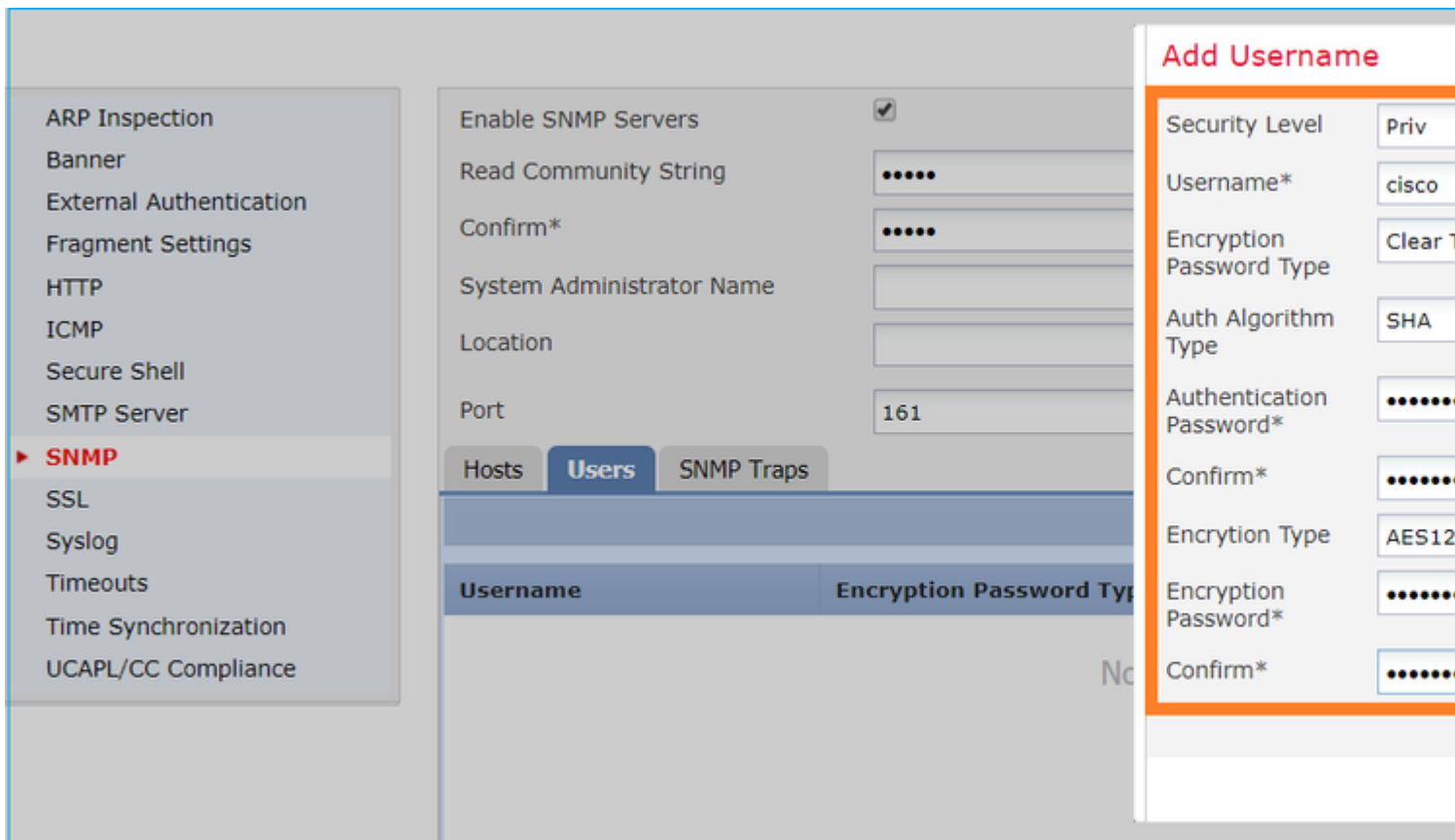
Port (1 - 65535)

Hosts | Users | SNMP Traps

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

LINA SNMPv3 configureren

Stap 1. Ga op FMC UI naar **Apparaten > Platform-instellingen > SNMP**. Controleer de optie **SNMP-servers inschakelen** en de SNMPv3-gebruiker en -host configureren:



Stap 2. Configureer de host ook om traps te ontvangen:

Edit SNMP Management Hosts

IP Address*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port (1 - 65535)

Available Zones

Selected Zones/Interfaces

Search

INSIDE_FTD4110

OUTSIDE3

Stap 3. De traps die u wilt ontvangen, kunnen worden geselecteerd onder Sectie **SNMP-traps**:

► **SNMP**

- SSL
- Syslog
- Timeouts
- Time Synchronization
- UCAPL/CC Compliance

Hosts Users **SNMP Traps**

Enable Traps All SNMP Syslog

Standard

Authentication:

Link up

Link Down

Cold Start

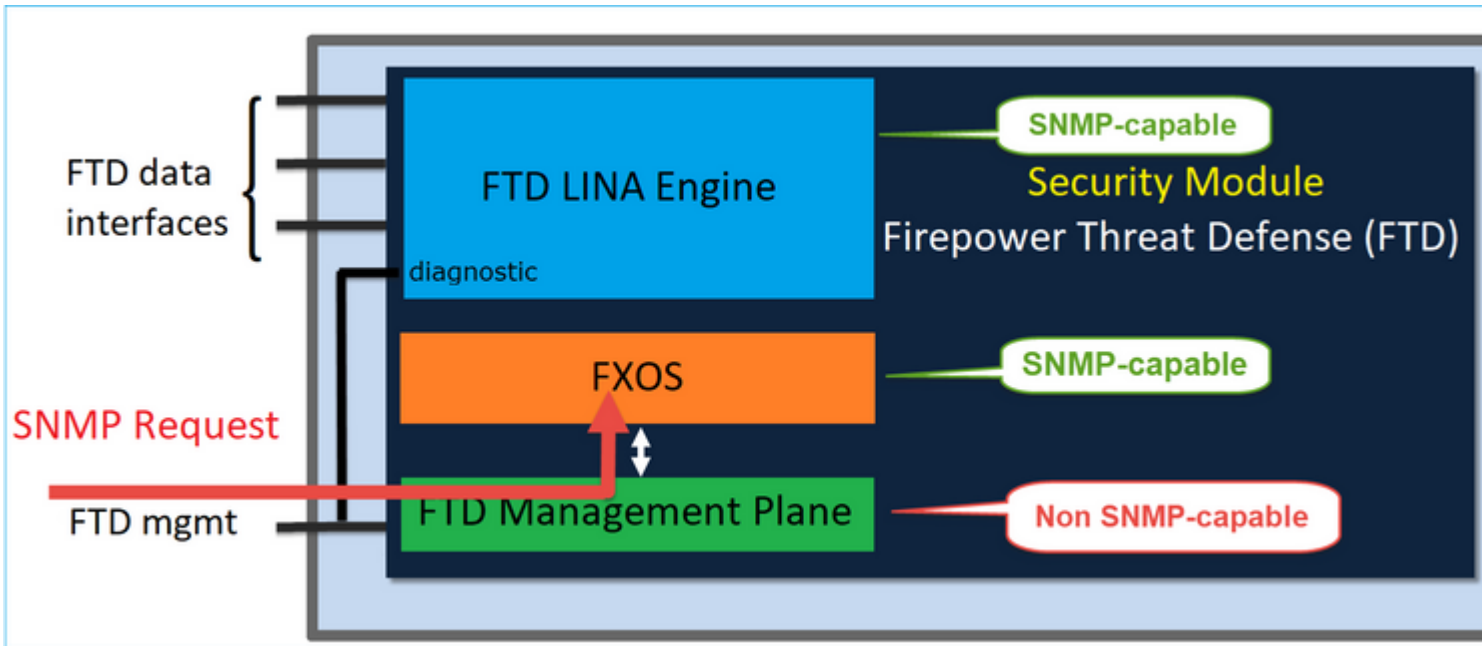
Warm Start

Entity MIB

SNMP in FPR210

Op FPR2100-systemen is er geen FCM. SNMP kan alleen via FMC worden geconfigureerd.

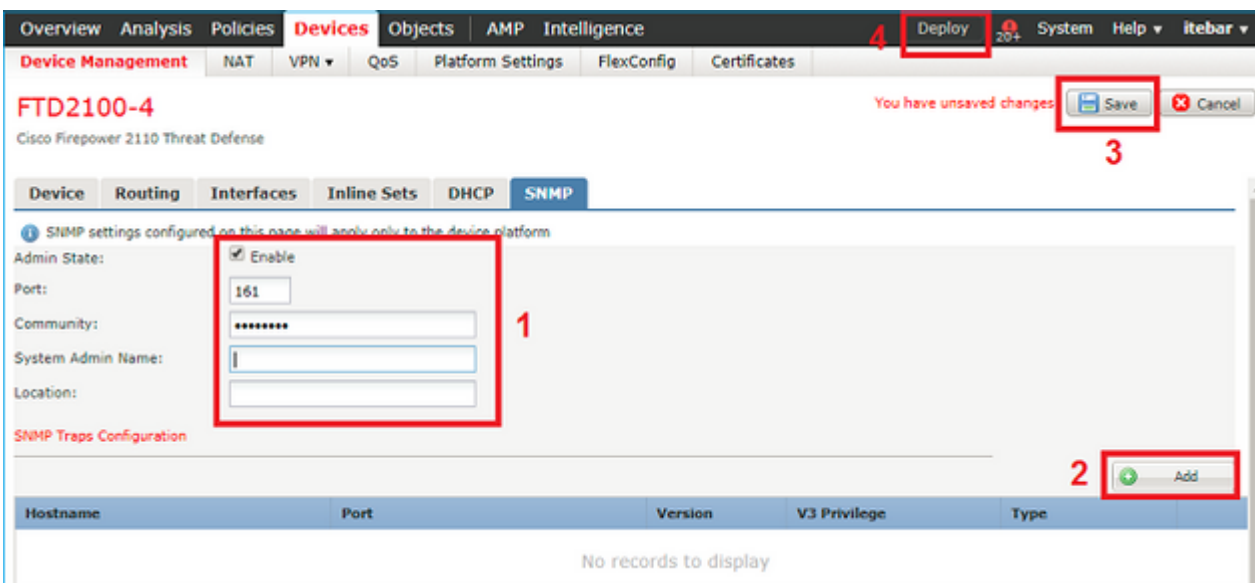
Chassis (FXOS) SNMP op FPR210

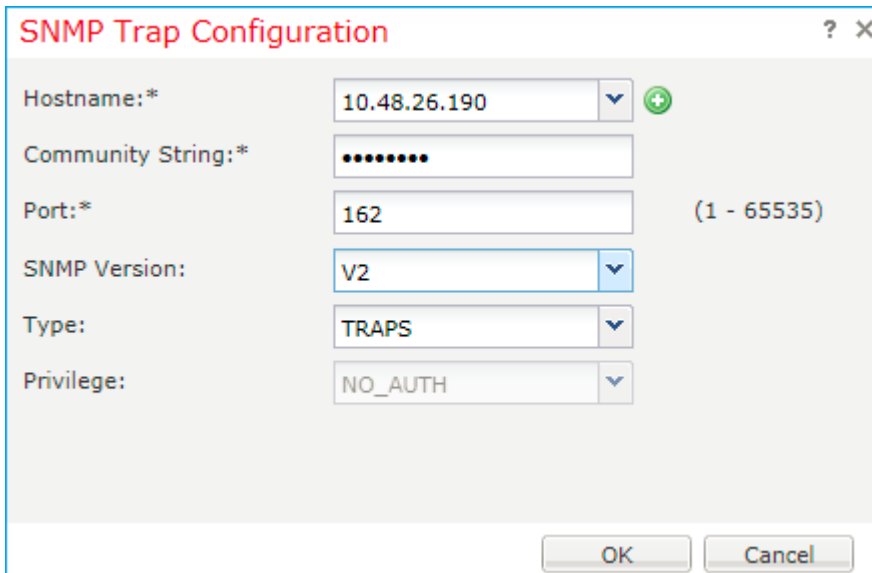


Vanaf FTD 6.6+ hebt u ook de optie om de FTD-beheerinterface voor SNMP te gebruiken. In dit geval worden zowel FXOS- als LINA SNMP-gegevens overgedragen via de FTD-beheerinterface.

FXOS SNMPv1/v2c configureren

Open FMC UI en navigeer naar **Apparaten > Apparaatbeheer**. Selecteer het apparaat en selecteer **SNMP**:





SNMP Trap Configuration

Hostname:* 10.48.26.190

Community String:*

Port:* 162 (1 - 65535)

SNMP Version: V2

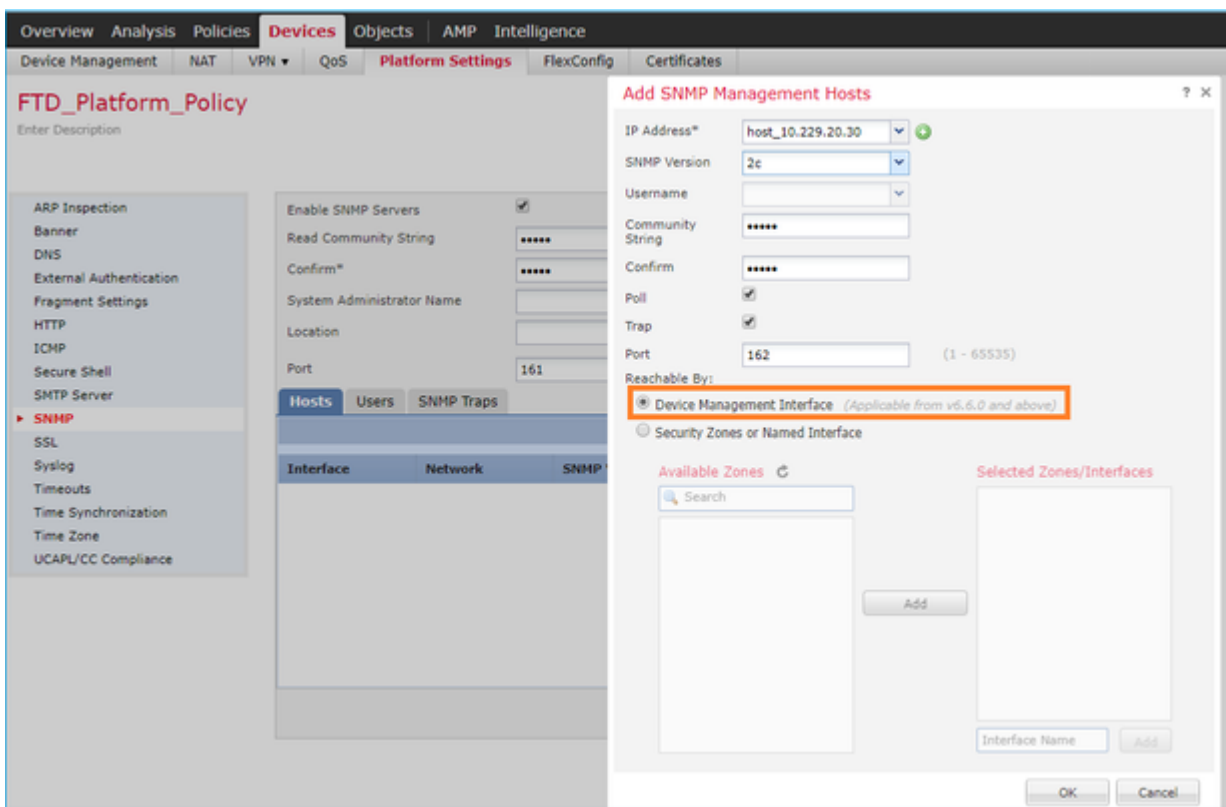
Type: TRAPS

Privilege: NO_AUTH

OK Cancel

Wijziging in FTD 6.6+

U kunt de FTD-beheerinterface instellen:



Overview Analysis Policies **Devices** Objects AMP Intelligence

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

FTD_Platform_Policy

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP

ICMP

Secure Shell

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm*

System Administrator Name

Location

Port 161

Hosts Users SNMP Traps

Interface Network SNMP

Add SNMP Management Hosts

IP Address* host_10.229.20.30

SNMP Version 2c

Username

Community String

Confirm

Poll

Trap

Port 162 (1 - 65535)

Reachable By:

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

Security Zones or Named Interface

Available Zones

Selected Zones/Interfaces

Interface Name Add

OK Cancel

Aangezien de beheerinterface ook voor SNMP kan worden geconfigureerd, toont de pagina dit waarschuwingsbericht:

De configuratie van het apparaatplatform SNMP op deze pagina is uitgeschakeld als SNMP-instellingen zijn geconfigureerd met Apparaatbeheer Interface via **Apparaten > Platform Settings (Threat Defense) > SNMP > Hosts**.

FXOS SNMPv3 configureren

Open FMC UI en navigeer om **Apparaten > Apparaatbeheer** te kiezen. Kies het apparaat en selecteer **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 4

Cisco Firepower 2110 Threat Defense

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

Hostname	Port	Version	V3 Privilege	Type
No records to display				

SNMP Users Configuration 2

Name	Auth Type	AES-128
No records to display		

SNMP User Configuration ? X

Username:* user1

Auth Algorithm Type: SHA

Use AES:

Password*

Confirm:

Privacy Password*

Confirm:

OK Cancel

SNMP Trap Configuration ? X

Hostname:* 10.48.26.190 +

Community String:*

Port:* 163 (1 - 65535)

SNMP Version: V3

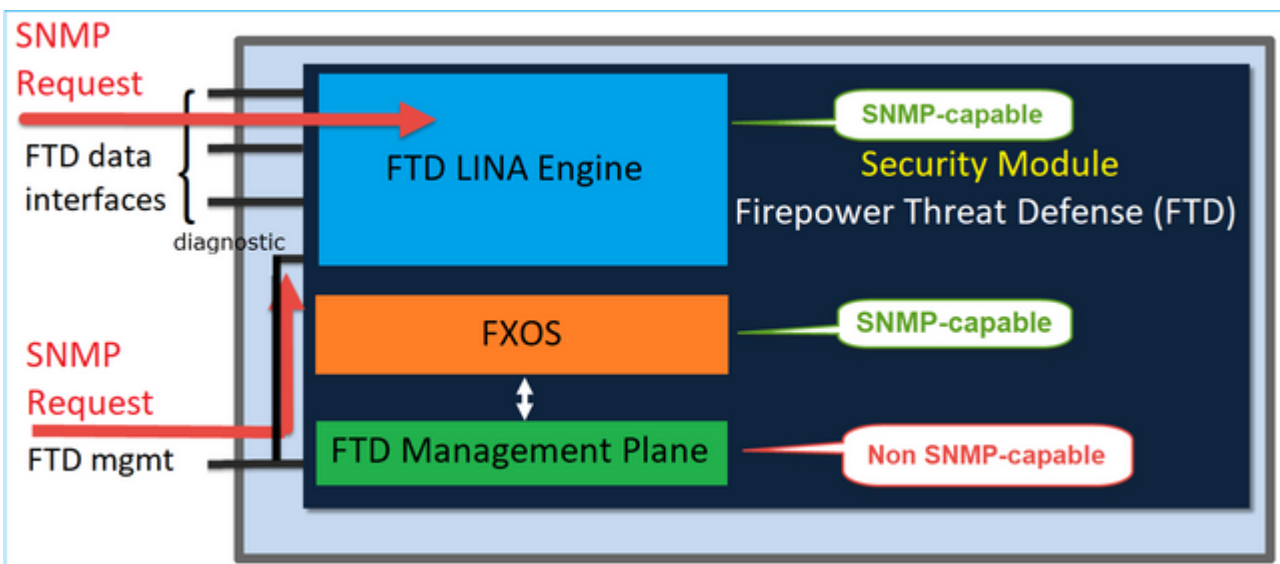
Type: TRAPS

Privilege: PRIV

OK Cancel

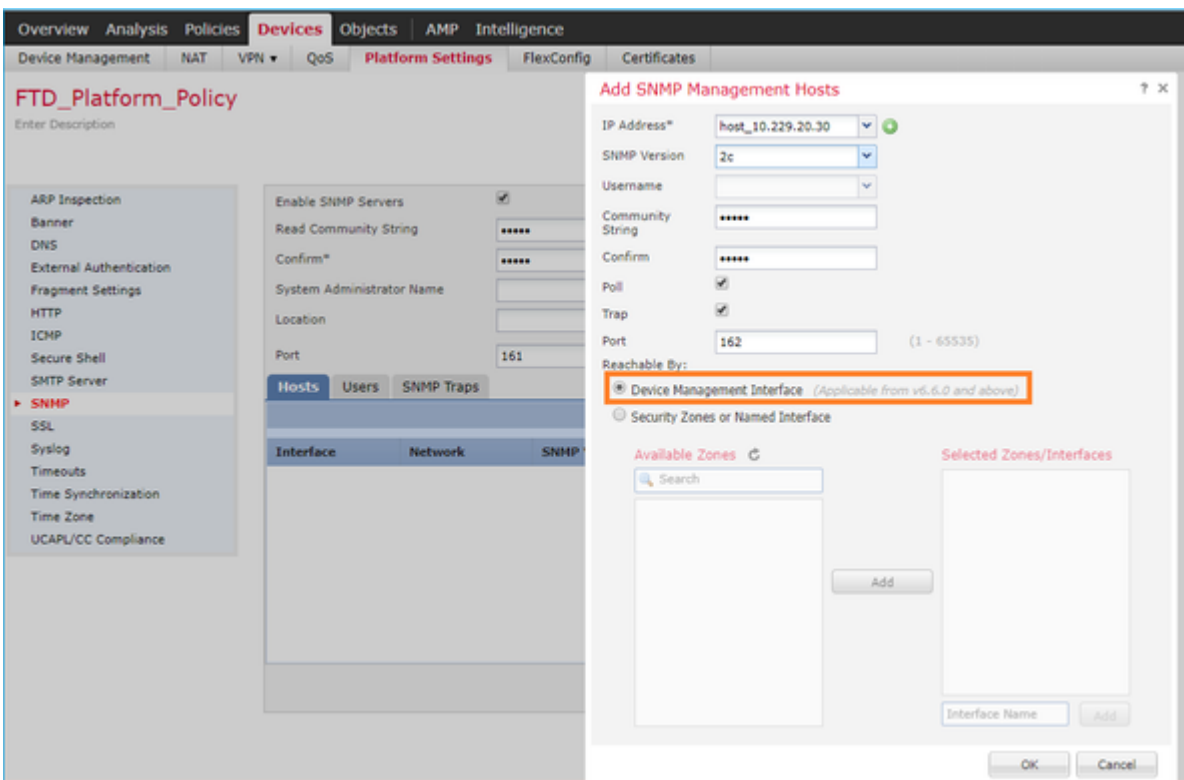
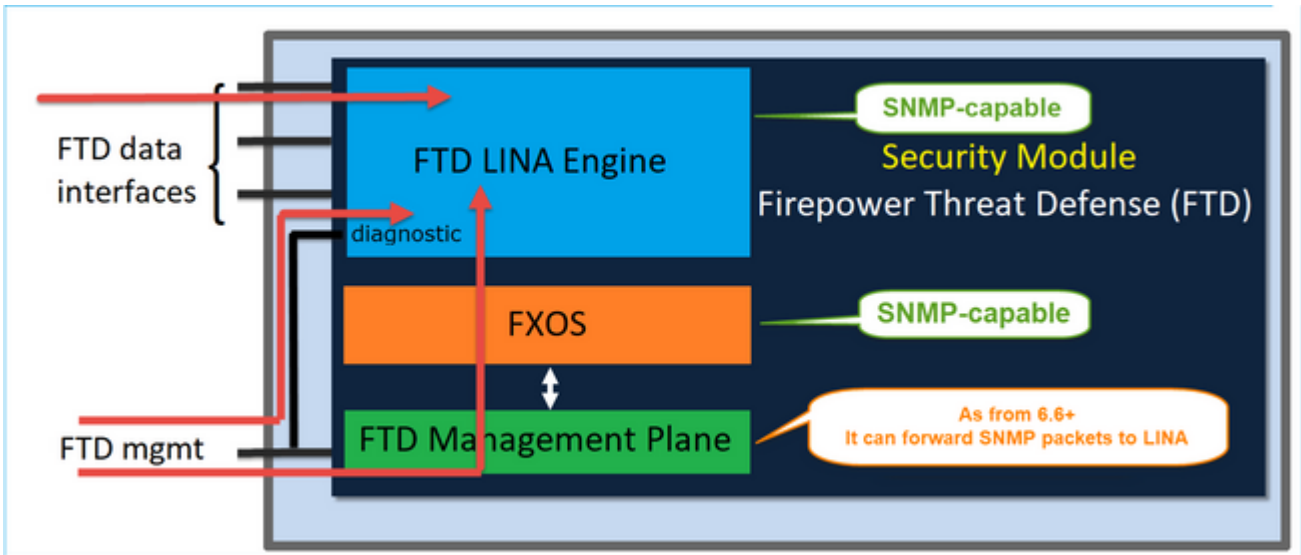
FTD (LINA) SNMP op FPR2100

- Voor pre-6.6 releases is de LINA FTD SNMP-configuratie op FTD FP1xxx/FP21xx-apparaten identiek aan een FTD op FirePOWER 4100 of 9300-apparaten.



FTD 6.6+ releases

- In post-6.6 releases hebt u ook de optie om de FTD-beheerinterface te gebruiken voor LINA polls en traps.



Als de nieuwe beheerinterface wordt geselecteerd:

- LINA SNMP is beschikbaar via de beheerinterface.
- Onder **Apparaten** > **Apparaatbeheer** is het **SNMP**-tabblad uitgeschakeld omdat het niet langer nodig is. Er verschijnt een melding van een banner. Het tabblad SNMP-apparaten was alleen zichtbaar op 2100/1100-platforms. Deze pagina bestaat niet op FPR9300/FPR4100 en FTD55xx-platforms.

Na configuratie is een gecombineerde LINA SNMP + FXOS (op FP1xxx/FP2xxx) SNMP-poll/trap-informatie via FTD-beheerinterface.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD2100-6
Cisco Firepower 2140 Threat Defense

Device Routing Interfaces Inline Sets DHCP **SNMP**

⚠ Device platform SNMP setting configuration on this page is deprecated and the same will be configurable through **Devices > Platform Settings (Threat Defense) > SNMP > Hosts** with Device Management

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

Admin State: Enable

Port:

Community:

System Admin Name:

Location:

SNMP Traps Configuration

Hostname	Port	Version	V3 Privilege	Type
No records to display				

SNMP Single IP-beheerfunctie wordt vanaf 6.6 ondersteund op alle FTD-platforms:

- FPR210
- FPR 1000
- FPR4100
- FPR9300
- ASA 5500 die FTD draait
- FTDv

Controleer voor meer informatie [of SNMP voor bedreigingsverdediging is geconfigureerd](#)

Verifiëren

Controleer FXOS SNMP voor FPR4100/FPR9300

FXOS SNMPv2c-verificaties

CLI-configuratieverificatie:

```
<#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

Vanuit de FXOS-modus:

```
<#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
â€¦! All traps will appear as enable â€¦!
snmp-server enable traps flexlink ifStatusChange
snmp-server context mgmt vrf management
snmp-server community cisco123 group network-operator
```

Aanvullende controles:

```
<#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		

```
...
```

Test SNMP-aanvragen.

Voer een SNMP-aanvraag uit bij een geldige host.

Bevestig de Trap Generation.

U kunt de flap gebruiken in een interface met ethalyzer ingeschakeld om te bevestigen dat SNMP-traps worden gegenereerd en verzonden naar de gedefinieerde trap-hosts:

```
<#root>
```

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

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

```
Capturing on eth0
```

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

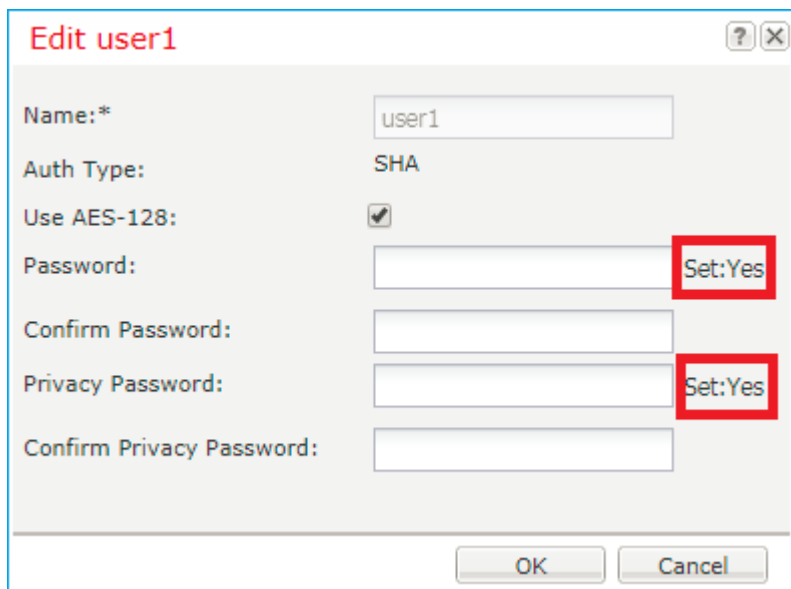
```
2017-11-17 09:01:35.954624 10.62.148.35 -> 192.168.10.100 SNMP sNMPv2-Trap
```

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

Waarschuwing: een interfaceknop kan een verkeersstoring veroorzaken. Voer deze test alleen uit in een laboratoriumomgeving of in een onderhoudsvenster

FXOS SNMPv3-verificaties

Stap 1. Open FCM UI **Platform Instellingen > SNMP > Gebruiker** toont of er een wachtwoord en privacy wachtwoord is ingesteld:



The screenshot shows a dialog box titled "Edit user1". It contains the following fields and controls:

- Name: * user1
- Auth Type: SHA
- Use AES-128:
- Password: [empty] Set:Yes
- Confirm Password: [empty]
- Privacy Password: [empty] Set:Yes
- Confirm Privacy Password: [empty]
- Buttons: OK, Cancel

Stap 2. In CLI kunt u de SNMP-configuratie controleren onder **bewaking** van bereik:

```
<#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
```

Stap 3. In de FXOS-modus kunt u de SNMP-configuratie en -details uitvouwen:

<#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  
-----
```

Test SNMP-aanvragen.

U kunt de configuratie controleren en een SNMP-aanvraag uitvoeren vanaf elk apparaat met SNMP-functies.

Om te controleren hoe het SNMP-verzoek wordt verwerkt, kunt u SNMP-debug gebruiken:

```
<#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.10.10.1.1.10.10.10.1 =  
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.10.10.1.2.10.10.10.2.83886080 = STRING: "mg  
2017 Oct 16 17:11:54.684370 snmpd:  SNMPPKTSTRT: 3.000000 162 1281064976.000000 1647446526.000000 0.000000
```

Waarschuwing: debug kan van invloed zijn op de prestaties van het apparaat.

Controleer FXOS SNMP voor FPR2100

FXOS SNMPv2-verificaties

Controleer de configuratie via 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
```

Bevestig het SNMP-gedrag.

U kunt controleren of u de FXOS kunt opvragen en een SNMP-aanvraag kunt verzenden vanaf een host of een apparaat met SNMP-functies.

Gebruik de opdracht **Capture-Traffic** om het SNMP-verzoek en de respons te zien:

```
<#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.ifTable.i
```

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

```
^C
```

```
Caught interrupt signal
```

```
Exiting.
```

```
2 packets captured
```

```
2 packets received by filter
```

```
0 packets dropped by kernel
```

FXOS SNMPv3-verificaties

Controleer de configuratie via 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
```

Bevestig het SNMP-gedrag.

Verzend een SNMP-verzoek om te verifiëren dat u de FXOS kunt opvragen.

Daarnaast kunt u het verzoek opnemen:

```
<#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
```

Controleer FTD SNMP

Zo verifieert u de FTD LINA SNMP-configuratie:

```
<#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 kunt u de FTD-beheerinterface voor SNMP configureren en gebruiken:

```
<#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
```

Aanvullende verificatie:

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

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

Vanaf de SNMP-server voert de CLI een momentopname uit:

```
<#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 Versio
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
...
```

Verificatie van de SNMP-verkeersstatistieken.

```
<#root>
```

```
Firepower-module1#
```

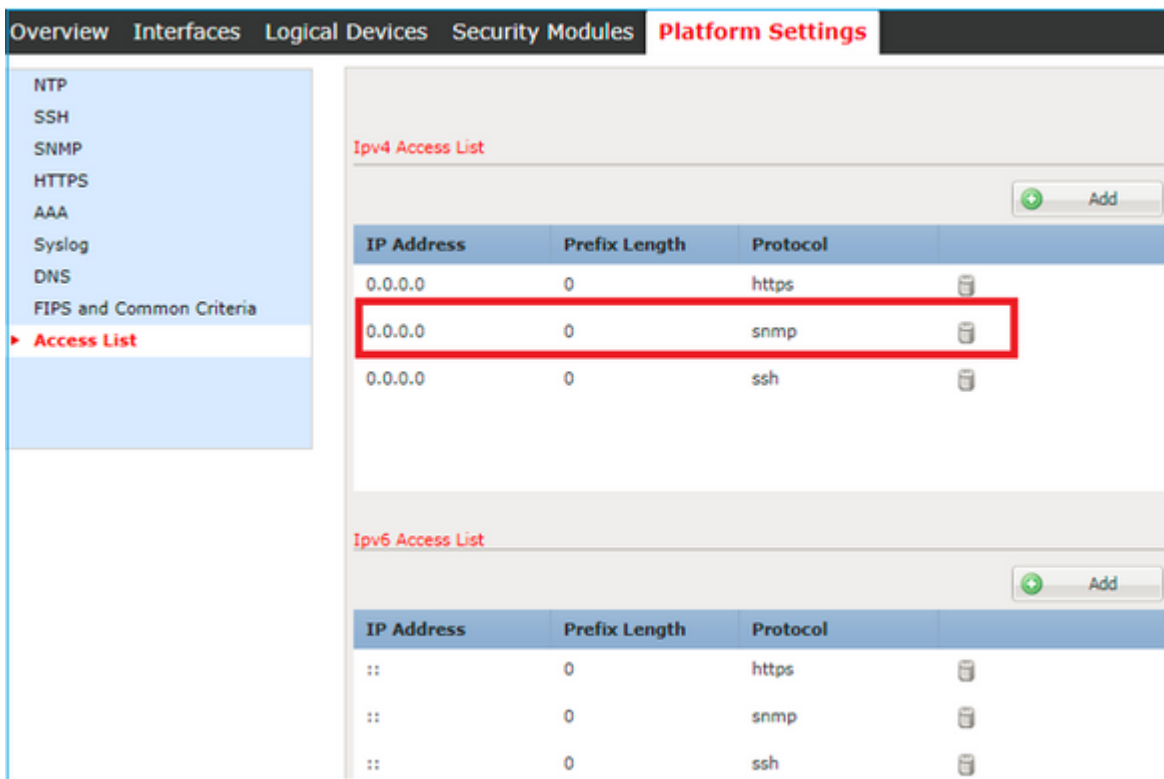
```
show snmp-server statistics
```

```
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
```

SNMP-verkeer naar FXOS toestaan op FPR4100/FPR9300

Door de FXOS-configuratie op FPR4100/9300 kan SNMP-toegang per IP-bronadres worden beperkt. In het configuratiegedeelte van de toegangslijst wordt gedefinieerd welke netwerken/hosts het apparaat kunnen bereiken via SSH, HTTPS of SNMP. U moet ervoor zorgen dat SNMP-vragen vanaf uw SNMP-server zijn toegestaan.

Wereldwijde toegangslijst configureren via GUI



The screenshot shows the 'Platform Settings' tab in the GUI. On the left, a navigation menu includes 'Access List'. The main area displays two sections: 'IPv4 Access List' and 'IPv6 Access List'. Each section has an 'Add' button and a table with columns for 'IP Address', 'Prefix Length', and 'Protocol'. In the IPv4 section, the row for '0.0.0.0' with 'snmp' protocol is highlighted with a red box. The IPv6 section shows similar entries for '::' with 'https', 'snmp', and 'ssh' protocols.

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

Wereldwijde toegangslijst configureren via 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
```

Verificatie

```
<#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

Gebruik de OID Object Navigator

[Cisco SNMP Object Navigator](#) is een online tool waarmee u de verschillende OID's kunt vertalen en een korte beschrijving kunt krijgen.

The screenshot shows the Cisco SNMP Object Navigator interface. The main heading is "SNMP Object Navigator". Below the heading, there are navigation tabs: "HOME", "SUPPORT", and "TOOLS & RESOURCES". Under "TOOLS & RESOURCES", the "SNMP Object Navigator" tab is selected. The main content area has a "TRANSLATE/BROWSE" tab selected, with "SEARCH", "DOWNLOAD MIBS", and "MIB SUPPORT - SW" tabs also visible. Below the tabs, there are two options: "Translate" and "Browse The Object Tree". The "Translate" option is selected. The instruction reads: "Translate OID into object name or object name into OID to receive object details". There is a text input field containing "1.3.6.1.4.1.9.9.109.1.1.1" and a "Translate" button. To the right, there are examples: "examples - OID: 1.3.6.1.4.1.9.9.27 Object Name: ifIndex". Below the input field, there is a section titled "Object Information" with a sub-section "Specific Object Information". This section contains a table with the following details:

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; - View Supporting Images
Description	A table of overall CPU statistics.

Gebruik de opdracht **tonen snmp-server video** van de FTD LINA CLI om de gehele lijst van LINA OIDs die kan worden ingepolderd terug te halen.

```
<#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#
```

Opmerking: de opdracht is verborgen.

Problemen oplossen

Dit zijn de meest gebruikelijke SNMP-casegeneratoren die door Cisco TAC worden gezien:

1. Kan FTD LINA SNMP niet ophalen
2. Kan FXOS SNMP niet ophalen
3. Welke SNMP OID-waarden moeten worden gebruikt?
4. Kan SNMP-traps niet ophalen
5. Kan FMC niet via SNMP bewaken
6. Kan SNMP niet configureren
7. SNMP-configuratie op Firepower Device Manager

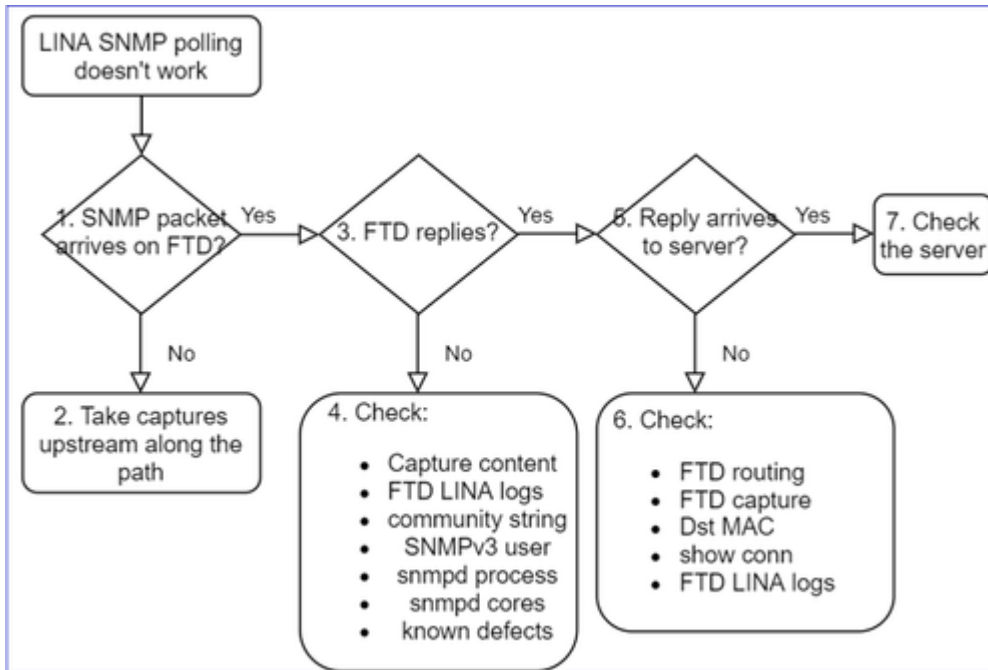
Kan FTD LINA SNMP niet ophalen

Probleembeschrijvingen (voorbeeld van echte Cisco TAC-cases):

- "Kan geen gegevens ophalen via SNMP."
- "Kan apparaat niet opvragen via SNMPv2."
- "SNMP werkt niet. We willen de firewall met SNMP bewaken, maar na de configuratie hebben we problemen."
- "We hebben twee monitoringsystemen die niet in staat zijn om de FTD via SNMP v2c of 3 te monitoren."
- "SNMP walk werkt niet op de firewall."

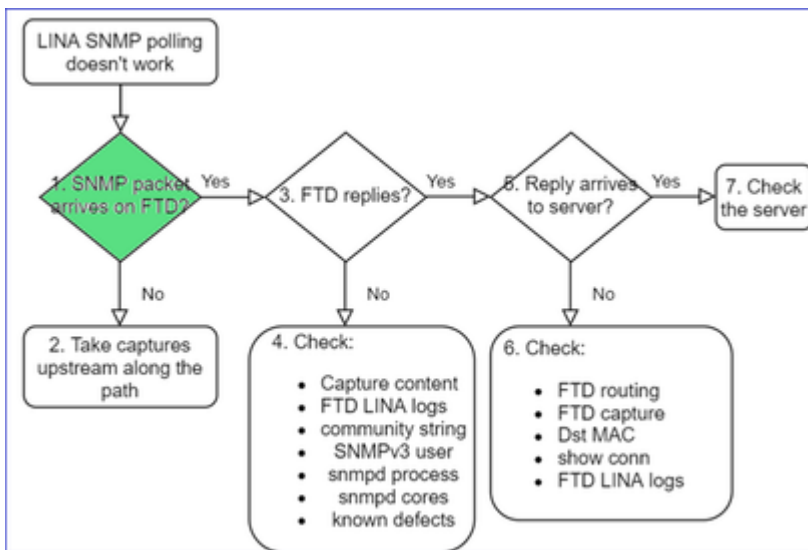
Aanbeveling voor probleemoplossing

Dit wordt geadviseerd proces om stroomschema's voor de kwesties van de SNMP-opiniepeiling van LINA op te stellen:



Diepduiken

1. Komt SNMP-pakket op FTD aan



- Opnamen inschakelen om de aankomst van het SNMP-pakket te controleren.

SNMP op FTD-beheerinterface (na 6.6 release) gebruikt het trefwoord voor beheer:

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

SNMP op FTD-gegevensinterfaces gebruikt de naam van de interface:


```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

Opname via FTD-beheerinterface:

```
<#root>
```

```
>
```

```
capture-traffic
```

Please choose domain to capture traffic from:

0 - management1

1 - management0

2 - Global

Selection?

1

Opname via FTD-gegevensinterface:

```
<#root>
```

```
firepower#
```

```
capture SNMP interface net201 trace match udp any any eq 161
```

FTD-pakkettracering voor gegevensinterface (functioneel scenario - vóór 6.6/9.14.1):

```
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)

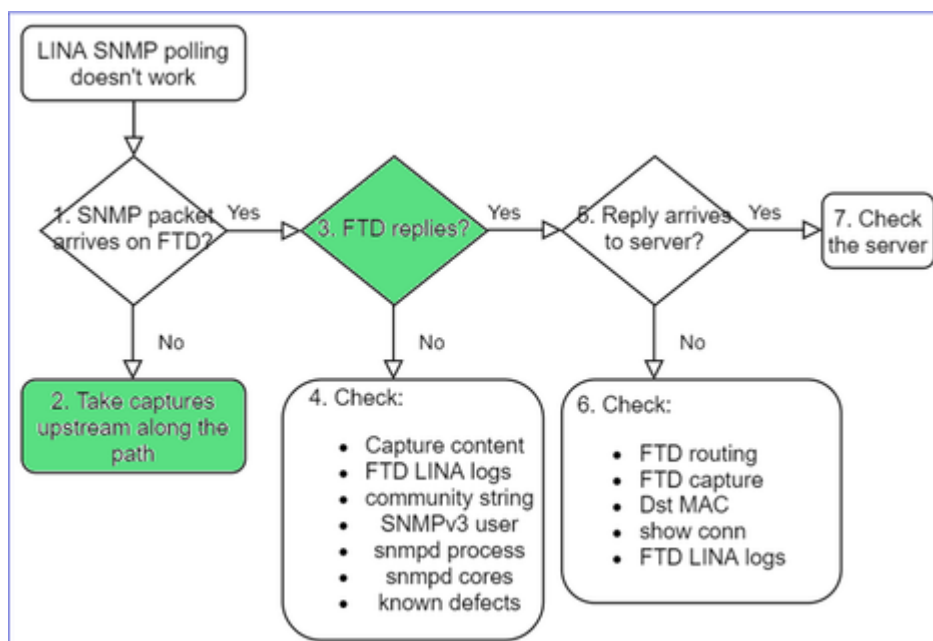
FTD-pakkettracing voor gegevensinterface (niet-functioneel scenario - post 6.6/9.14.1):

```
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: 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. Als u SNMP-pakketten niet ziet in de FTD-ingangen, worden de volgende bestanden opgenomen:

- Leg stroomopwaarts opnamen vast langs het pad.
- Zorg ervoor dat de SNMP-server de juiste FTD IP gebruikt.
- Begin van de switchport die naar de FTD-interface kijkt en ga stroomopwaarts.



3. Zien jullie FTD SNMP-antwoorden?

Om te controleren of de FTD antwoordt, controleert u:

1. FTD uitgaande vastlegging (LINA- of mgmt-interface)

Controleer op SNMP-pakketten met bronpoort 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 de versies na 6.6/9.14.1 hebt u nog een opnamepunt: Capture on the NLP tap interface. De NATed IP komt uit het 162.254.x.x-bereik:

```
<#root>
```

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

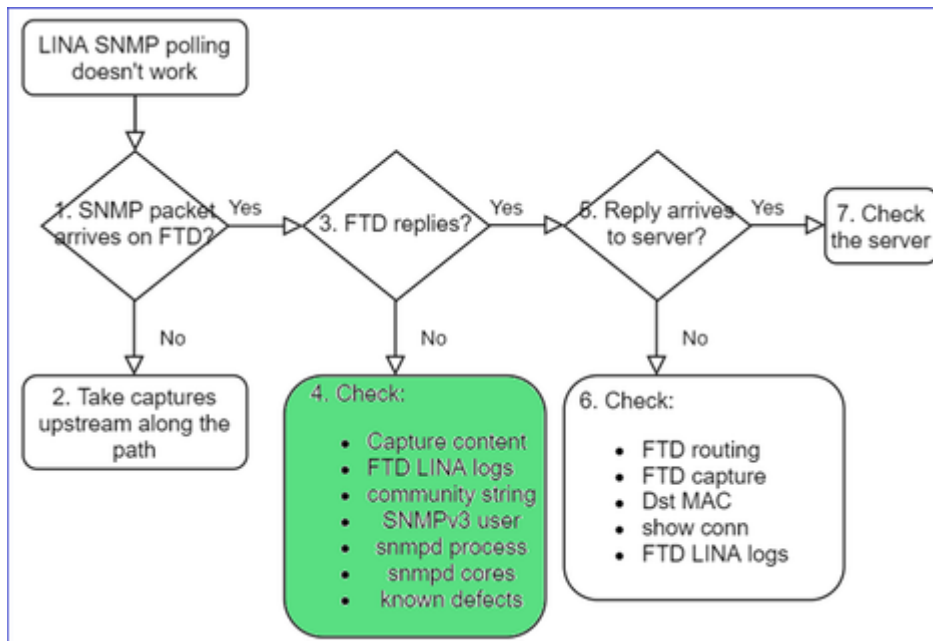
```
sudo tcpdump -i tap_nlp
```

```
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.9.1
```

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

4. Aanvullende controles



a. Controleer voor FirePOWER 4100/9300-apparaten de [FXOS-compatibiliteitstabel](#).

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
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)
	Firepower 4145 Firepower 4125 Firepower 4115	9.19(x) (recommended) 9.18(x) 9.17(x) 9.16(x)
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)
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)
	Firepower 4145 Firepower 4125 Firepower 4115	9.18(x) (recommended) 9.17(x) 9.16(x)
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.13(x) 9.12(x) 9.10(x) 9.9(x) 9.8(x)
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)

b. Controleer de FTD LINA snmp-server statistieken:

```
<#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
&#x2013;
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-verbindingstabel

Deze controle is erg handig als u geen pakketten ziet in de opname op de FTD-toegangsinterface. Merk op dat dit een geldige verificatie is voor alleen SNMP op de data-interface. Als SNMP zich op beheerinterface bevindt (na 6.6/9.14.1), wordt er geen verbinding gemaakt.

```
<#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

Dit is ook een geldige verificatie alleen voor SNMP op de data-interface! Als SNMP zich op beheerinterface bevindt, wordt er geen logbestand gemaakt:

```
<#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 (192.0.2.100:161 -> 192.168.2.100:55048)
```

e. Controleer of de FTD de SNMP-pakketten laat vallen vanwege een incorrecte host-bron voor IP

```

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

```

No UN-NAT phase!

```

firepower# show run snmp-server
snmp-server host net201 192.168.22.100

```

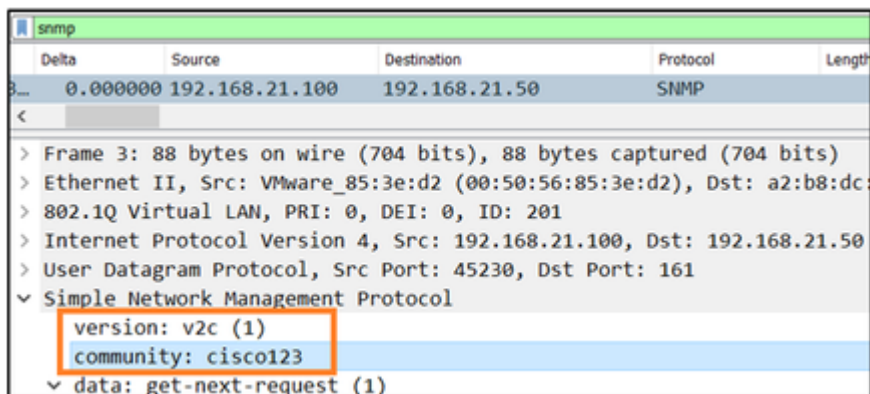
```

firepower# show asp table classify interface net201 do
Input Table
in id=0x14f65b193b30, priority=501, domain=permit, den
hits=8, user_data=0x0, cs_id=0x0, use_real_addr
src ip/id=192.168.22.100, mask=255.255.255.255,
dst ip/id=169.254.1.2, mask=255.255.255.255, pa
input_ifc=net201(vrfid:0), output_ifc=any

```

f. Onjuiste referenties (SNMP-community)

In de opnameinhoud kunt u de communitywaarden (SNMP v1 en 2c) zien:



g. Onjuiste configuratie (bijvoorbeeld SNMP-versie of Community-string)

Er zijn een paar manieren om de SNMP-configuratie van het apparaat en Community-strings te controleren:

```
<#root>
```

```
firepower#
```

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

```
snmp-server host net201 192.168.2.100 community cISC0123 version 2c
```

Een andere manier:

```
<#root>
```

```
firepower#
```

```
debug menu netsnmp 4
```

h. FTD LINA/ASA ASP-druppels

Dit is een handige controle om te verifiëren of de SNMP-pakketten door de FTD worden losgelaten. Schakel eerst de tellers uit (asp-druppel wissen) en test vervolgens:

```
<#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

ASP vangt zichtbaarheid in de gedropte pakketten op (bijvoorbeeld ACL of nabijheid):

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

Test en controleer vervolgens de opnameinhoud:

```
<#root>
firepower#
show capture

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

j. SNMP-kern (traceback) - verificatieweg 1

Deze controle is handig als u problemen met de systeemstabiliteit vermoedt:

```
<#root>
firepower#
show disk0: | i core

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

SNMP-kern (traceback) - verificatieweg 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
```

Als u een SNMP-kernbestand ziet, verzamelt u deze items en neemt u contact op met Cisco TAC:

- FTD TS-bestand (of ASA show tech)
- SNMP-kernbestanden

SNMP-debuggs (dit zijn verborgen opdrachten en alleen beschikbaar voor nieuwere versies):

```
<#root>
```

```
firepower#
```

```
debug snmp trace [255]
```

```
firepower#
```

```
debug snmp verbose [255]
```

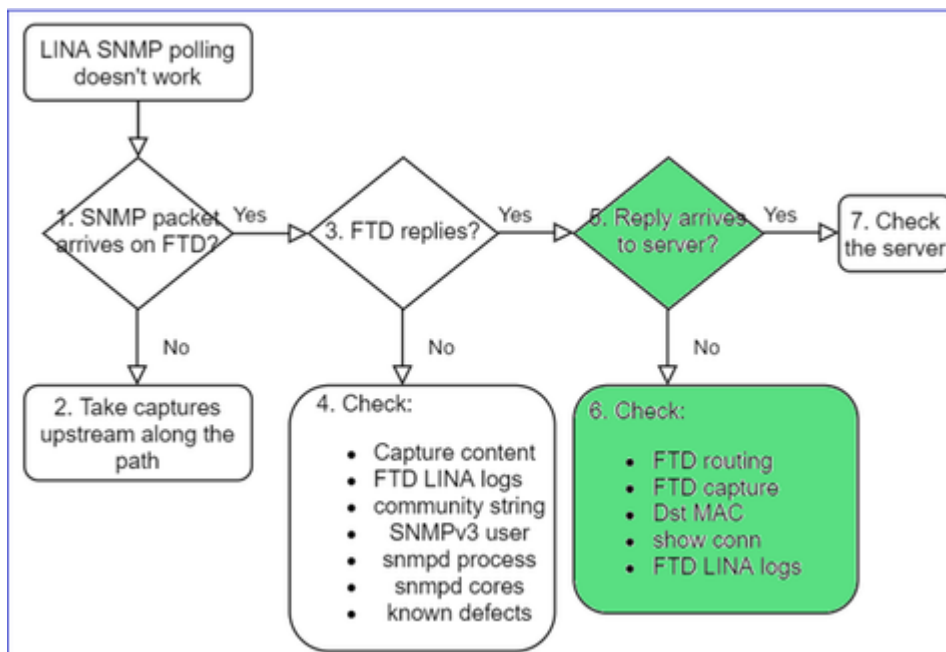
```
firepower#
```

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

```
firepower#
```

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

Komt de firewall SNMP-antwoord op de server aan?



Als het FTD antwoordt, maar het antwoord niet de servercontrole bereikt:

a. FTD-routing

Voor de FTD-beheerinterface met routing:

```
<#root>  
>  
show network
```

Voor FTD LINA data interface routing:

```
<#root>  
firepower#  
show route
```

b. MAC-verificatie bestemming

FTD-beheer dst MAC-verificatie:

```
<#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: 10.62.148.19
```

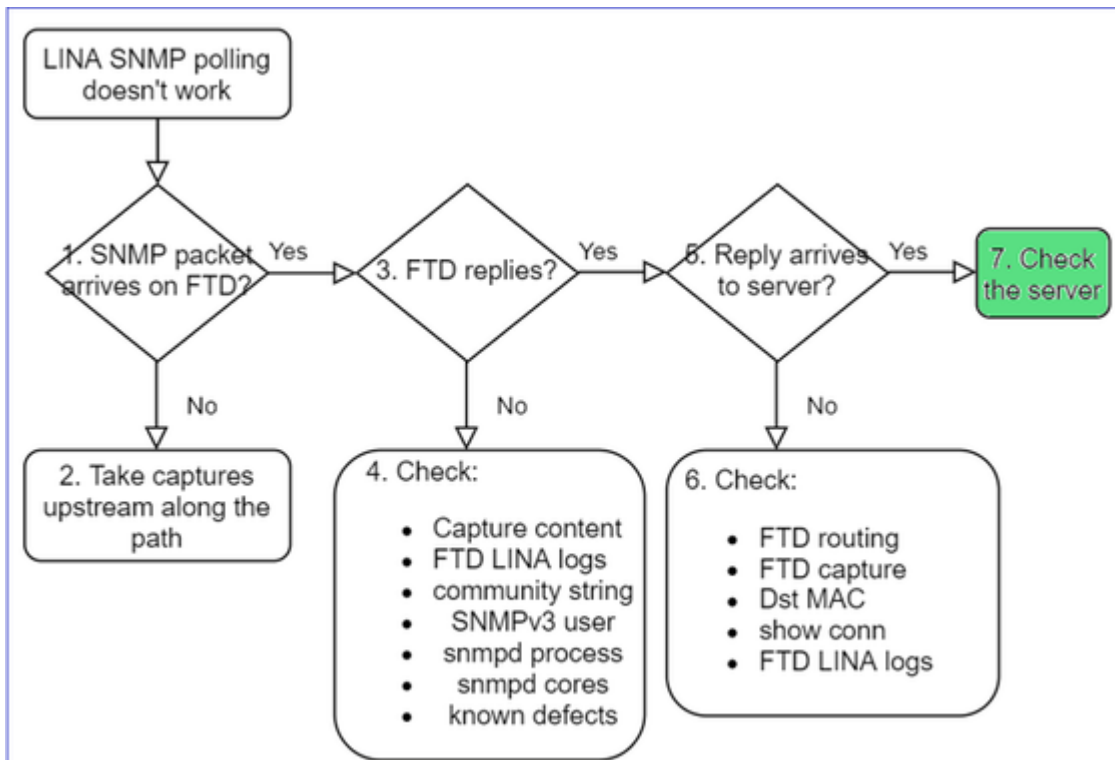
FTD LINA data interface bestemming MAC verificatie:

```
<#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, i

c. Controleer apparaten langs het pad die de SNMP-pakketten mogelijk laten vallen of blokkeren.

Controleer de SNMP-server



a. Controleer de opnameinhoud om de instellingen te verifiëren.

b. Controleer de serverconfiguratie.

c. Probeer de SNMP-communitynaam te wijzigen (bijvoorbeeld zonder speciale tekens).

U kunt een eindhost of zelfs het VCC gebruiken om de stemming te testen zolang aan de 2 voorwaarden wordt voldaan:

1. SNMP-connectiviteit is aanwezig.
2. De bron IP mag het apparaat opvragen.

```
<#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-opiniepeilingen

- Licentie: SNMPv3 vereist een sterke encryptie-licentie. Zorg ervoor dat u de functie voor exportcontrole hebt ingeschakeld op het Smart Licensing-portal
- Om problemen op te lossen, kunt u proberen met een nieuwe gebruiker/referenties
- Als er encryptie wordt gebruikt, kunt u het SNMPv3-verkeer decoderen en de payload controleren zoals beschreven in: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>
- Overweeg AES128 voor encryptie in het geval dat uw software door defecten zoals wordt beïnvloed:
- Cisco bug-id [CSCvy27283](#)

ASA/FTD SNMPv3-opiniepeiling kan mislukken met behulp van privacy-algoritmen AES192/AES256

Cisco bug-id [CSCvx45604](#) Snmpv3 lopen mislukt op gebruiker met auth sha en priv aes 192

Opmerking: Als SNMPv3 mislukt vanwege algoritme mismatch de show outputs en de logs tonen niets duidelijk

```
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 pollingoverwegingen - casestudyâ€™s

1. SNMPv3-momentopname - functioneel 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 de opname (snmpwalk) ziet u een antwoord voor elk pakket:

```
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
```

Het opnamebestand toont niets ongebruikelijks:

```

v 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-firewall - coderingsfout

Hint #1: Er is een time-out:

```
<#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

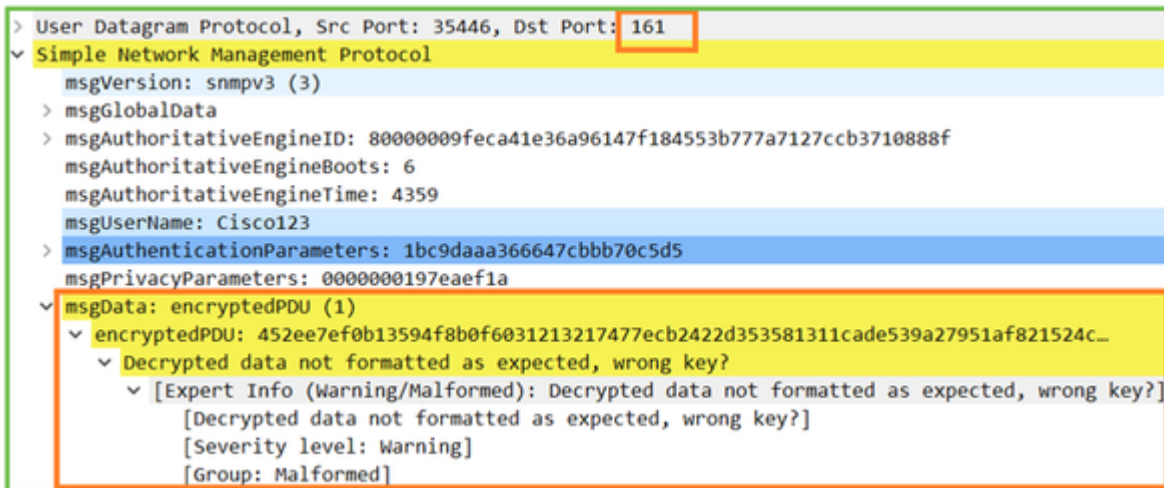
Hint #2: Er zijn veel verzoeken en 1 antwoord:

```
firepower# show capture SNMP
```

```
7 packets captured
```

```
1: 23:25:06.248446      802.1Q vlan#201 PO 192.168.21.100.55137 > 192.168.21.50.161:  udp 64
2: 23:25:06.248613      802.1Q vlan#201 PO 192.168.21.100.55137 > 192.168.21.50.161:  udp 64
3: 23:25:06.249224      802.1Q vlan#201 PO 192.168.21.50.161 > 192.168.21.100.55137:  udp 132
4: 23:25:06.252992      802.1Q vlan#201 PO 192.168.21.100.55137 > 192.168.21.50.161:  udp 163
5: 23:25:07.254183      802.1Q vlan#201 PO 192.168.21.100.55137 > 192.168.21.50.161:  udp 163
6: 23:25:08.255388      802.1Q vlan#201 PO 192.168.21.100.55137 > 192.168.21.50.161:  udp 163
7: 23:25:09.256624      802.1Q vlan#201 PO 192.168.21.100.55137 > 192.168.21.50.161:  udp 163
```

Hint #3: Wireshark-decryptie is mislukt:



```
> 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]
```

#4. Controleer of het bestand ma_ctx2000.log bestand is voor foutmeldingen bij ScopedPDU:

```
<#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
```

De fout die ScopedPDU ontleedt is een sterke wenk van een encryptiefout. Het bestand ma_ctx2000.log toont alleen gebeurtenissen voor SNMPv3!

3. SNMPv3-snelkiezer - verificatiefout

Hint #1: verificatiefout

```
<#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: Er zijn veel verzoeken en veel antwoorden

```
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: misvormd Wireshark-pakket

```
> 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
▼ [Malformed Packet: SNMP]
  ▼ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```

#4. Controleer het logbestand ma_ctx2000.log op "Verificatie mislukt" berichten:

```
<#root>
```

```
>
```

```
expert
```

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

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

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

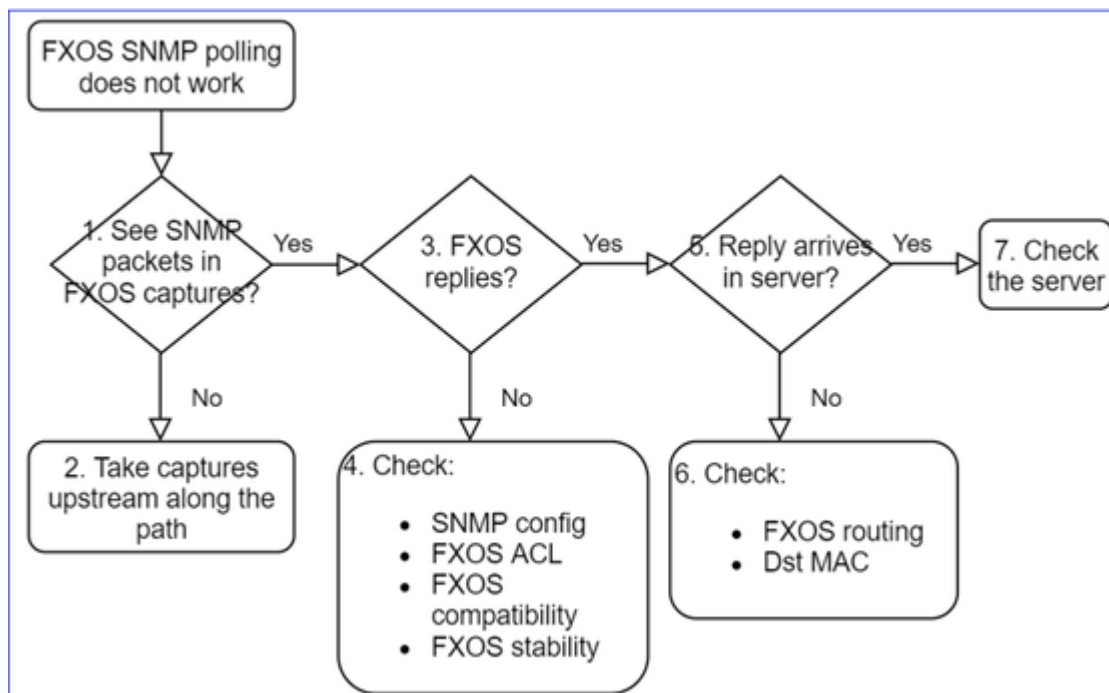
Kan FXOS SNMP niet ophalen

Probleembeschrijvingen (voorbeeld van echte Cisco TAC-cases):

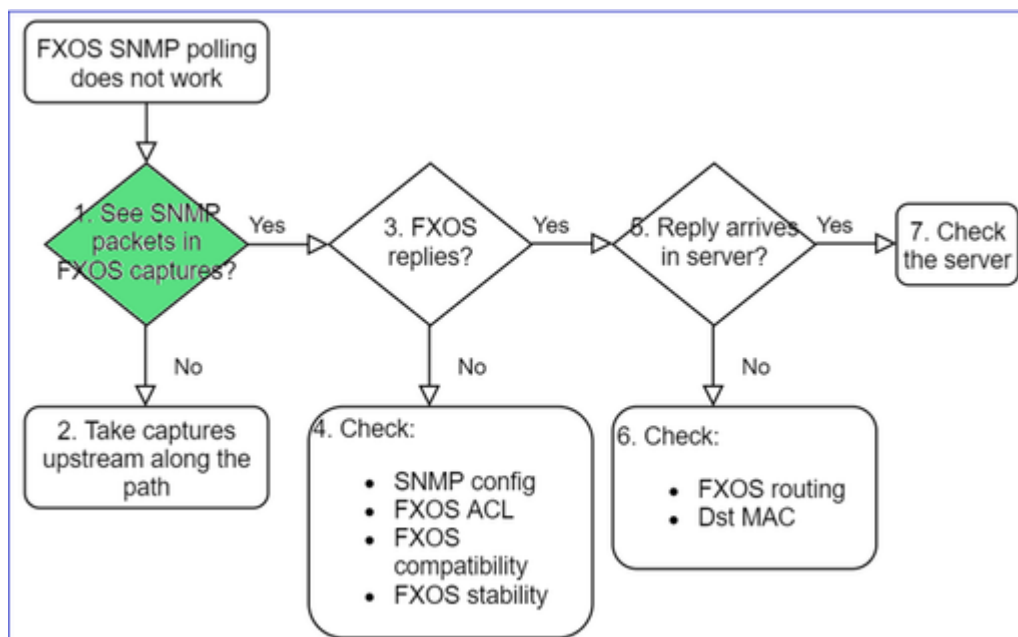
- "SNMP geeft een verkeerde versie voor FXOS. Bij opiniepeiling met SNMP voor versie van FXOS is de uitvoer moeilijk te begrijpen."
- "Kan de SNMP-community niet instellen op FXOS FTD4115."
- "Na een FXOS upgrade van 2.8 naar 2.9 op standby firewall, krijgen we een time-out wanneer we proberen om informatie te ontvangen via SNMP."
- "snmpwalk werkt niet op 9300 fxos maar op 4140 fxos op dezelfde versie. Bereikbaarheid en gemeenschapszin zijn niet het probleem."
- "We willen 25 SNMP-servers toevoegen aan FPR4K FXOS, maar dat kunnen we niet."

Aanbevolen probleemoplossing

Dit is het proces om stroomschema voor FXOS SNMP-opiniepeilingen problemen op te lossen:



1. Ziet u SNMP-pakketten in FXOS-opnamen?



FPR1xxx/21xx

- Op FPR1xxx/21xx is er geen chassisbeheerder (toestelmodus).
- U kunt de FXOS-software opvragen via de beheerinterface.

<#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

- Gebruik in Firepower 41xx/93xx de Ethanalyzer CLI tool om een chassisopname te maken:

```
<#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
```

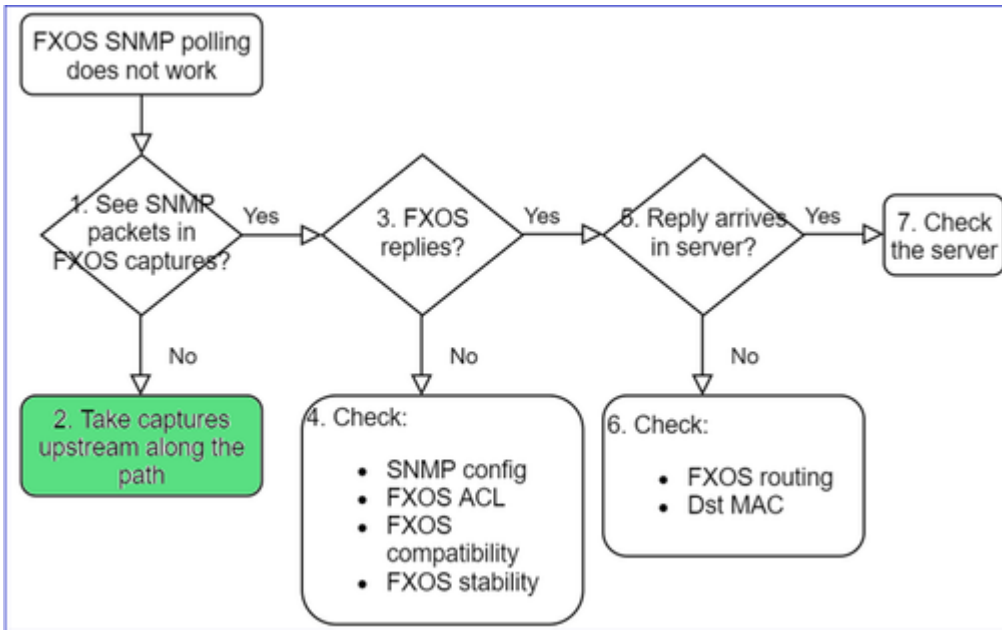
```
1
```

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

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

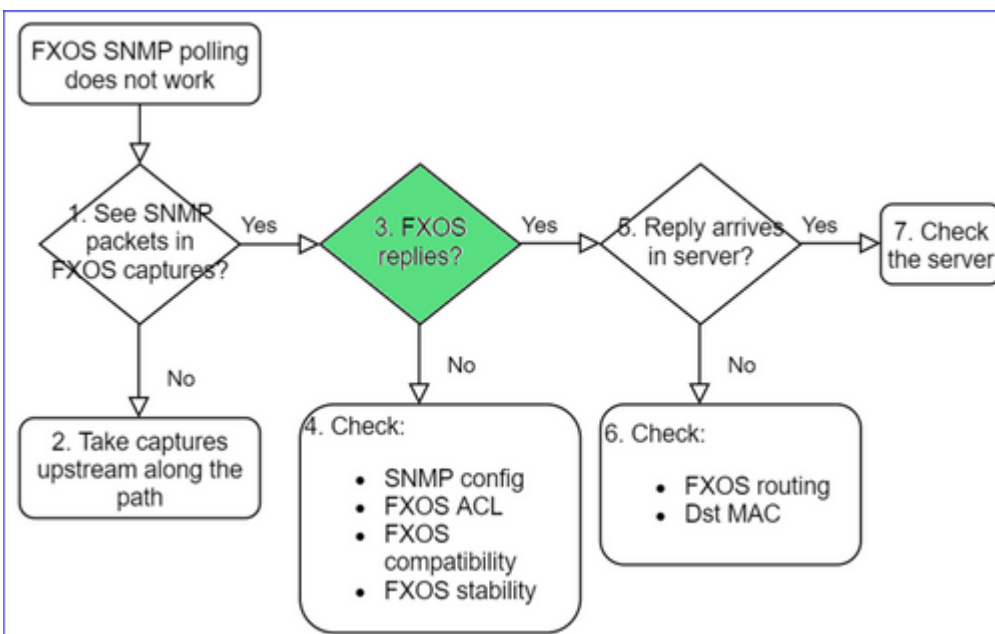
```
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. Geen pakketten in FXOS-opnamen?



- Leg stroomopwaarts opnemen vast langs het pad

3. Antwoorden van FXOS?



- Functioneel scenario:

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.

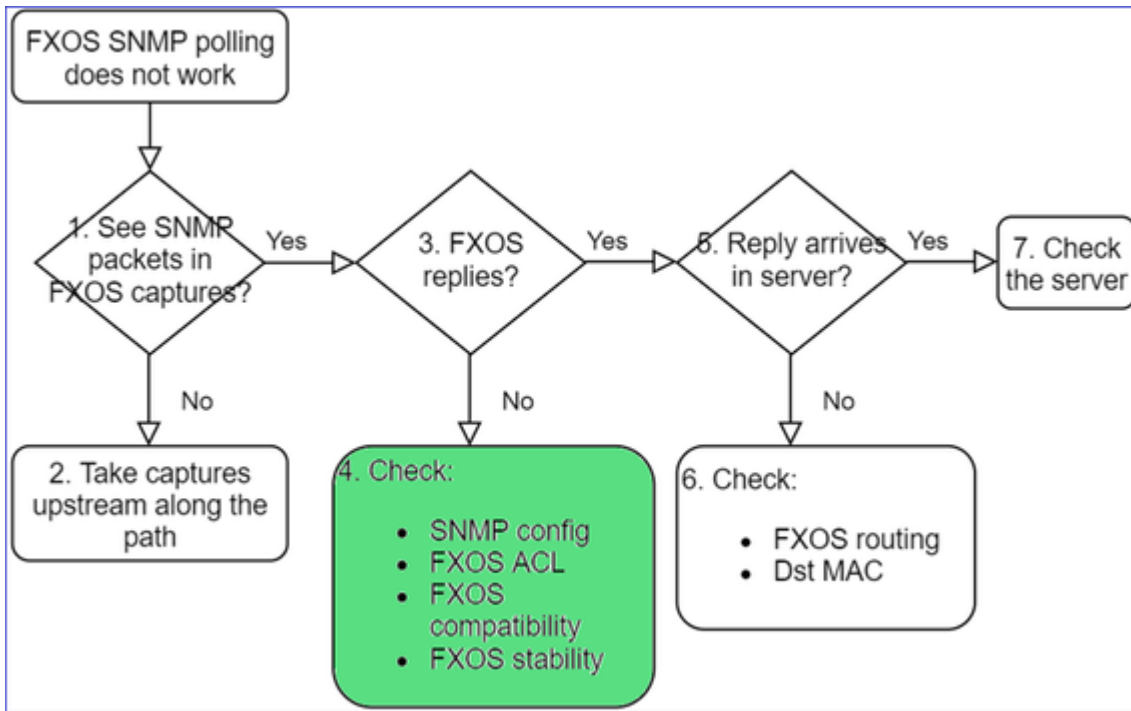
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

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 antwoordt niet



Aanvullende controles

- Controleer de SNMP-configuratie (van UI of CLI):

```
<#root>
```

```
firepower#
```

```
scope monitoring
```

```
firepower /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

- Wees voorzichtig met de speciale tekens (bijvoorbeeld '\$'):

```
<#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		

- Voor SNMP v3 gebruik tonen snmp-user [detail]
- Controleer de FXOS-compatibiliteit

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

4. Indien FXOS niet antwoordt

Controleer de FXOS SNMP-tellers:

```
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
```

Callouts from the terminal output:

- 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

- Controleer de FXOS-toegangscontrolelijst (ACL). Dit is alleen van toepassing op FPR41xx/9300-platforms.

Als het verkeer wordt geblokkeerd door FXOS ACL, ziet u verzoeken, maar u ziet geen antwoorden:

```
<#root>
```

```
firepower(fxos)#
```

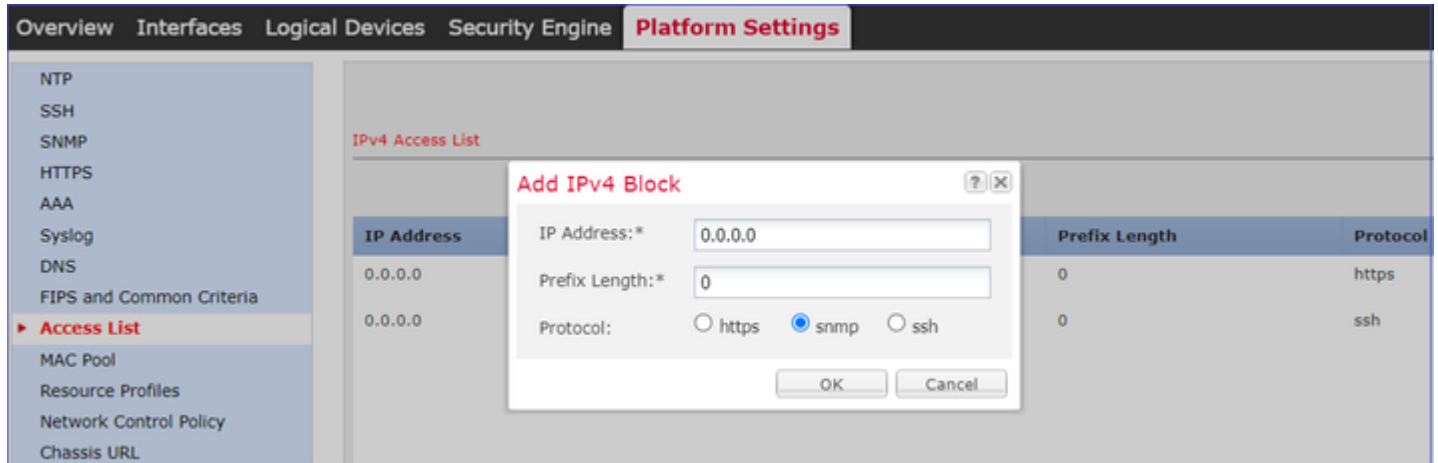
```
ethalyzer local interface mgmt capture-filter
```

```
"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 â†’ 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 â†’ 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 â†’ 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1
```

U kunt FXOS ACL verifiëren via de gebruikersinterface (UI):



U kunt ook de FXOS-ACL op de CLI verifiëren:

```
<#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 (alleen pakketten). Alleen van toepassing op 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 (alles) - Deze debug uitvoer is zeer breedspakig.

```
<#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
```

- Controleer of er SNMP-gerelateerde FXOS-fouten zijn:

```
<#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
```

- Controleer of er SNMP-cores zijn:

```
In 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
```

Op FPR1xxx/21xx:

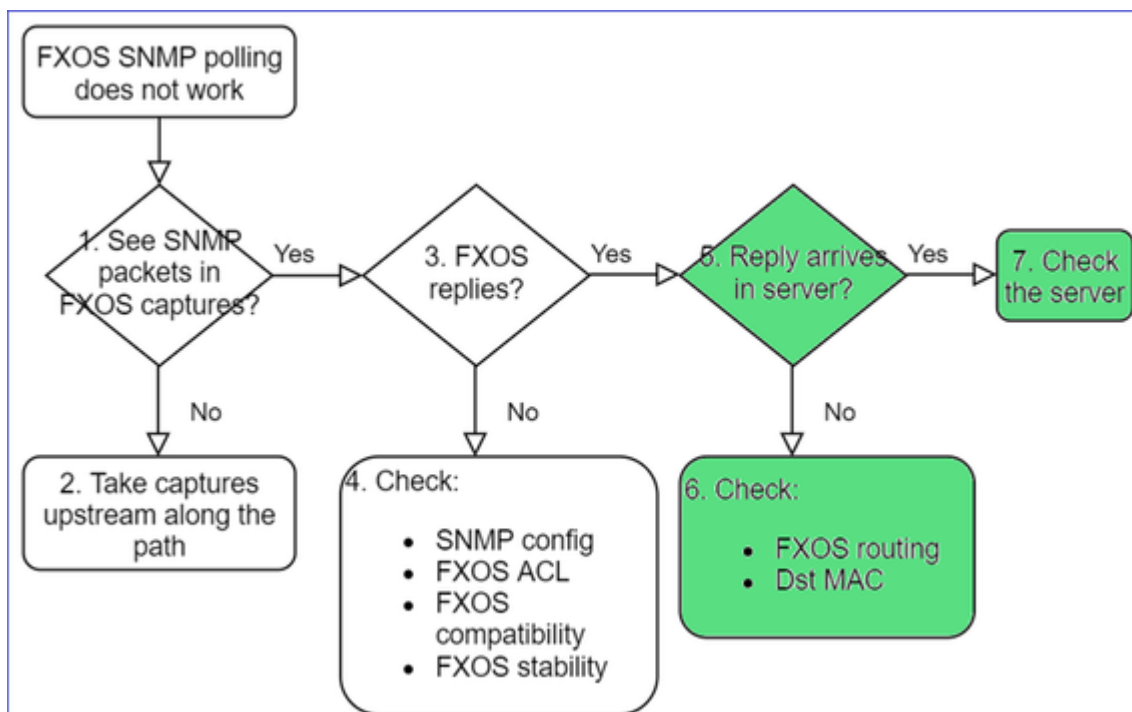
```
<#root>
```

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

```
dir cores_fxos
```

Als u snmpd-cores ziet, verzamelt u de cores samen met de FXOS-probleemoplossingsbundel en neemt u contact op met Cisco TAC.

5. Komt SNMP-antwoord in SNMP-server aan?



- Controleer de FXOS-routing

Deze uitvoer is van FPR41xx/9300:

```
<#root>
```

```
firepower#
```

```
show fabric-interconnect
```

```
Fabric Interconnect:
```

ID	00B IP Addr	00B Gateway	00B Netmask	00B IPv6 Address	00B IPv6 Gateway	Prefix	Operab
A	192.168.2.37	192.168.2.1	10.255.255.128 ::	::		64	Operable

- Neem een opname, exporteer de pcap en controleer de dst MAC van het antwoord
- Controleer tot slot de SNMP-server (opneemt, configuratie, toepassing enzovoort)

Welke SNMP OID-waarden moeten worden gebruikt?

Probleembeschrijvingen (voorbeeld van echte Cisco TAC-cases):

- "We willen de Cisco FirePOWER-apparatuur controleren. Gelieve SNMP OIDs te verstrekken voor elke kern CPU, geheugen, schijven"
- "Is er een OID die kan worden gebruikt om de status van de stroomvoorziening op ASA 5555-apparaat te controleren?"
- "We willen chassis SNMP OID op FPR 2K en FPR 4K halen."
- "We willen de ASA ARP Cache."
- "We moeten SNMP OID kennen voor BGP peer down."

Hoe de SNMP OID-waarden te vinden

Deze documenten bieden informatie over SNMP-OID™s op FirePOWER-apparaten:

- Cisco Firepower Threat Defence (FTD) SNMP-bewaking - Witboek:

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

- Cisco Firepower 4100/9300 FXOS MIB handleiding referentie:

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

- Hoe te zoeken naar een specifieke OID op 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>

- Controleer SNMP-OID™s van de 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
```

- Voor meer informatie over OIDs check de SNMP Object Navigator

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

- Op FXOS (41xx/9300) voert u deze 2 opdrachten uit de FXOS CLI uit:

```
<#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
```

```
...
```

Gemeenschappelijke OIDs™s – Snelle referentie

Vereiste	OID
CPU (LINA)	10.3.1.1.4.1.9.9.109
CPU (snort)	10.3.1.1.4.1.9.9.109.1.1.1.1.7, 10.3.1.1.4.1.9.9.109.1.1.1.1.10 (FP >= 6.7)
Geheugen (LINA)	10.3.1.1.4.1.9.9.48, 10.3.1.1.4.1.9.9.221
Geheugen (Linux/FMC)	10.3.1.1.4.1.2021.4
Gebruikt/vrij geheugen (41xx/93xx)	10.3.1.1.4.1.9.9.109.1.1.1.1.12.1, 10.3.1.1.4.1.9.9.109.1.1.1.1.13.1

Interfaces	1.10.1.1.1.2
HA-informatie	10.3.1.1.4.1.9.9.147.1.10.1.1.1
Clusterinformatie	10.3.1.1.4.1.9.9.491.1.8.1
VPN-informatie	10.3.1.1.4.1.9.9.171.1 - Tip: vuurkracht# tonen snmp-server oid Ja
BGP-status	NAT Cisco-bug-id CSCux13512 : Voeg BGP MIB toe voor SNMP-polling
FPR1K/2K ASA/ASA v slimme licentiëring	NAT Cisco-bug-id CSCv83590 : ASA v/ASA op de FPR1k/2k: SNMP OID nodig voor het bijhouden van de status van slimme licenties
Lina SNMP- OID's voor poortkanaal op FXOS-niveau	NAT Cisco-bug-id CSCvu91544 : Ondersteuning voor Lina SNMP OID's voor FXOS-niveau poortkanaalinterfacestatistieken

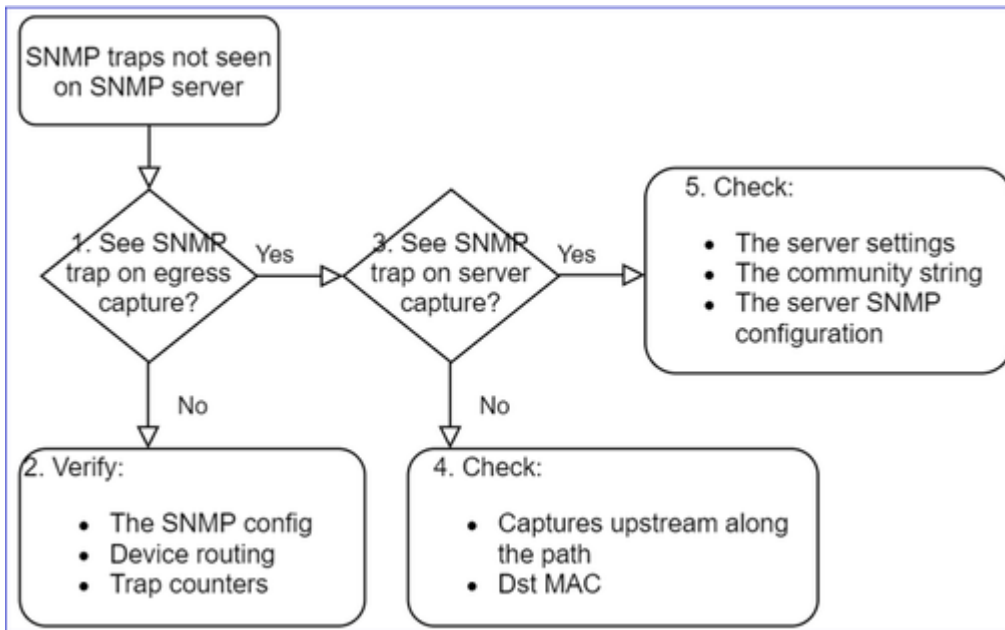
Kan SNMP-traps niet ophalen

Probleembeschrijvingen (voorbeeld van echte Cisco TAC-cases):

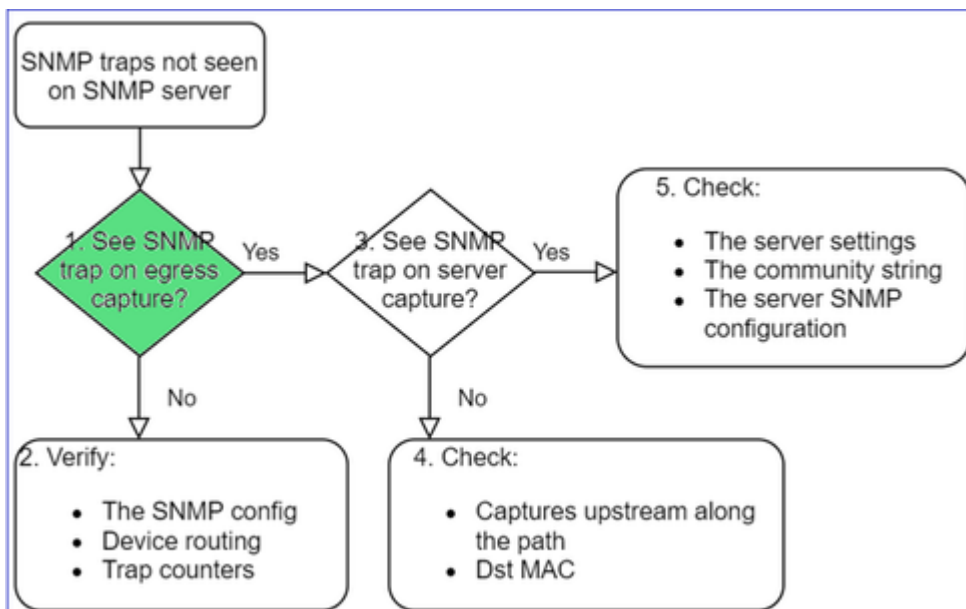
- "SNMPv3 van FTD verzendt geen val naar SNMP-server."
- "FMC en FTD verzenden geen SNMP Trap-berichten."
- "We hebben SNMP geconfigureerd op onze FTD 4100 voor FXOS en geprobeerd SNMPv3 en SNMPv2, maar beide kunnen geen vallen verzenden."
- "Firepower SNMP verstuurt geen vallen naar de bewakingstool."
- "Firewall FTD verzendt SNMP Trap niet naar NMS."
- "SNMP-servertraps werken niet."
- "We hebben SNMP geconfigureerd op onze FTD 4100 voor FXOS en geprobeerd SNMPv3 en SNMPv2, maar beide kunnen geen vallen verzenden."

Aanbevolen probleemoplossing

Dit is het proces voor het oplossen van problemen met het stroomschema voor Firepower SNMP-trap:



1. Ziet u SNMP-traps bij uitgaande opname?



Zo vangt u LINA/ASA-vallen op beheerinterface:

```
<#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
```

Zo vangt u LINA/ASA-vallen op de gegevensinterface:

```
<#root>
firepower#
  capture SNMP interface net208 match udp any any eq 162
```

Zo vangt u FXOS-vallen (41xx/9300) op:

```
<#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 â†’ 10.62.184.23 SNMP 160 snmpV2-trap 10.3.1.1.2.1.1.3.0 1
firepower(fxos)#

exit

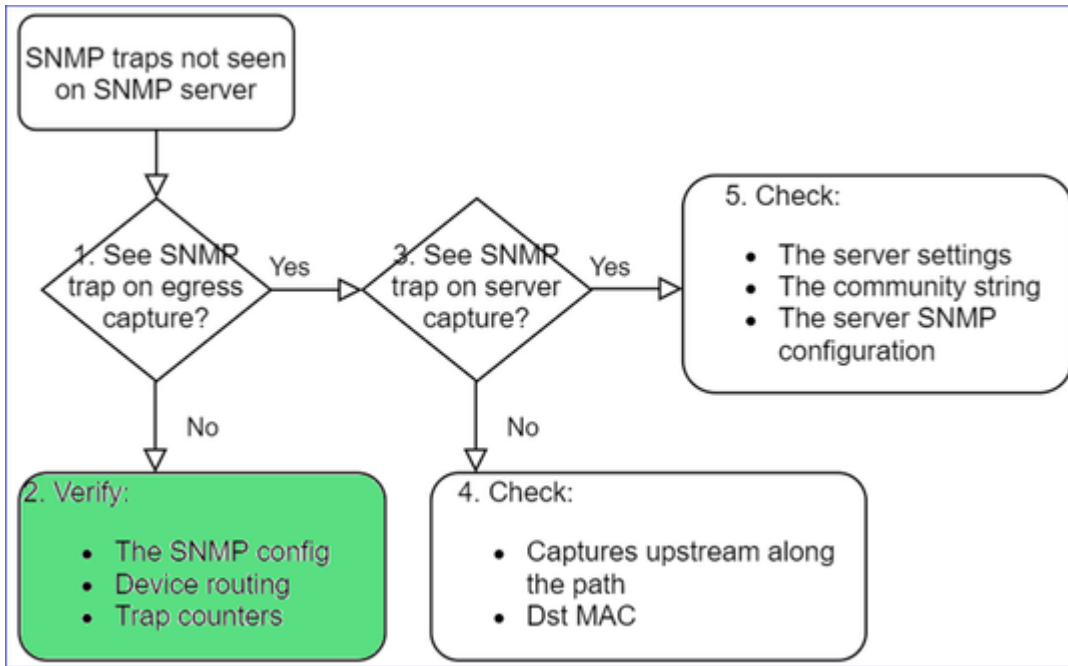
firepower#
connect local-mgmt

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. Als u geen pakketten op uitgaande interface ziet



<#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
  
```

Configuratie FXOS SNMP-traps:

<#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	

Opmerking: op 1xxx/21xx ziet u deze instellingen alleen in het geval van **Apparaten > Apparaatbeheer > SNMP-configuratie!**

- LINA/ASA routing voor vallen via beheerinterface:

```
<#root>
```

```
>
```

```
show network
```

- LINA/ASA routing voor vallen door middel van data-interface:

```
<#root>
```

```
firepower#
```

```
show route
```

- FXOS-routing (41x/9300):

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- Trap-tellers (LINA/ASA):

```
<#root>
```

```
firepower#
```

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

```
20 Trap PDUs
```

En FXOS:

```
<#root>
```

```
FP4145-1#
```

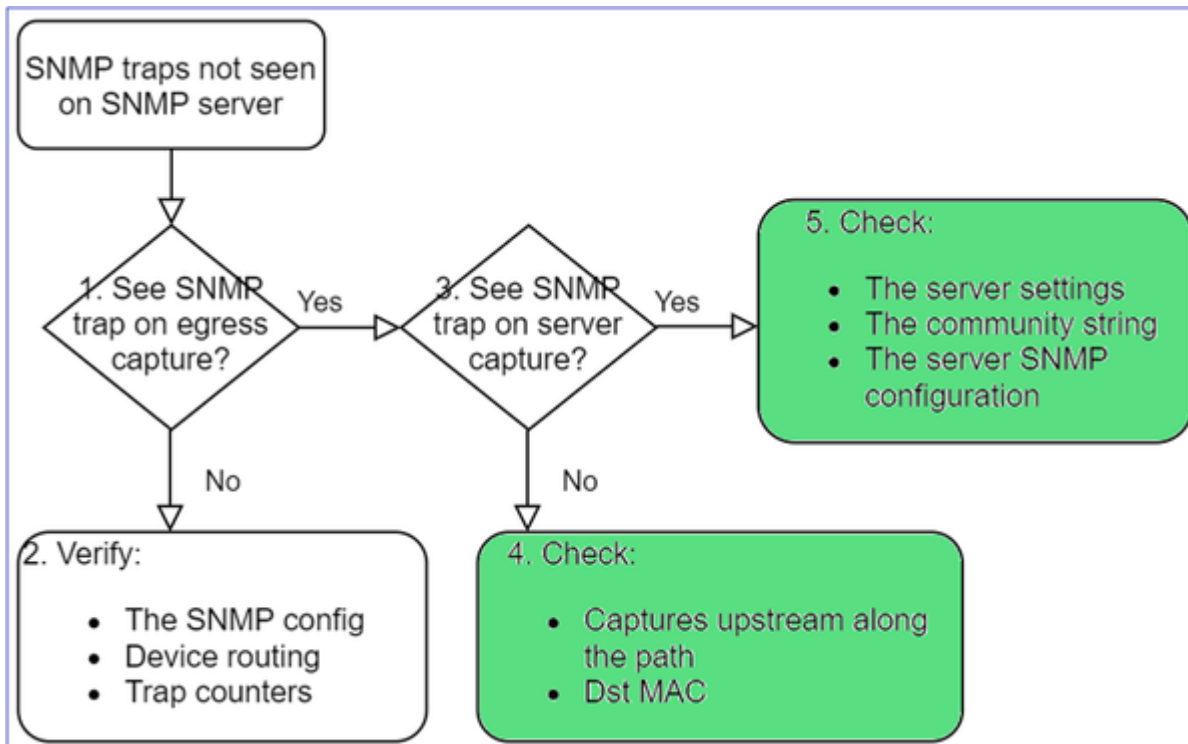
```
connect fxos
```

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

```
show snmp | grep Trap
```

```
1296 Out Traps PDU
```

Aanvullende controles



- Neem een opname op de doel-SNMP server.

Overige te controleren punten:

- Leg vast op het pad.
- Doeladres MAC-adres van SNMP-trap-pakketten.
- De SNMP-serverinstellingen en -status (bijvoorbeeld firewall, open poorten enzovoort).
- De SNMP community-string.
- De SNMP-serverconfiguratie.

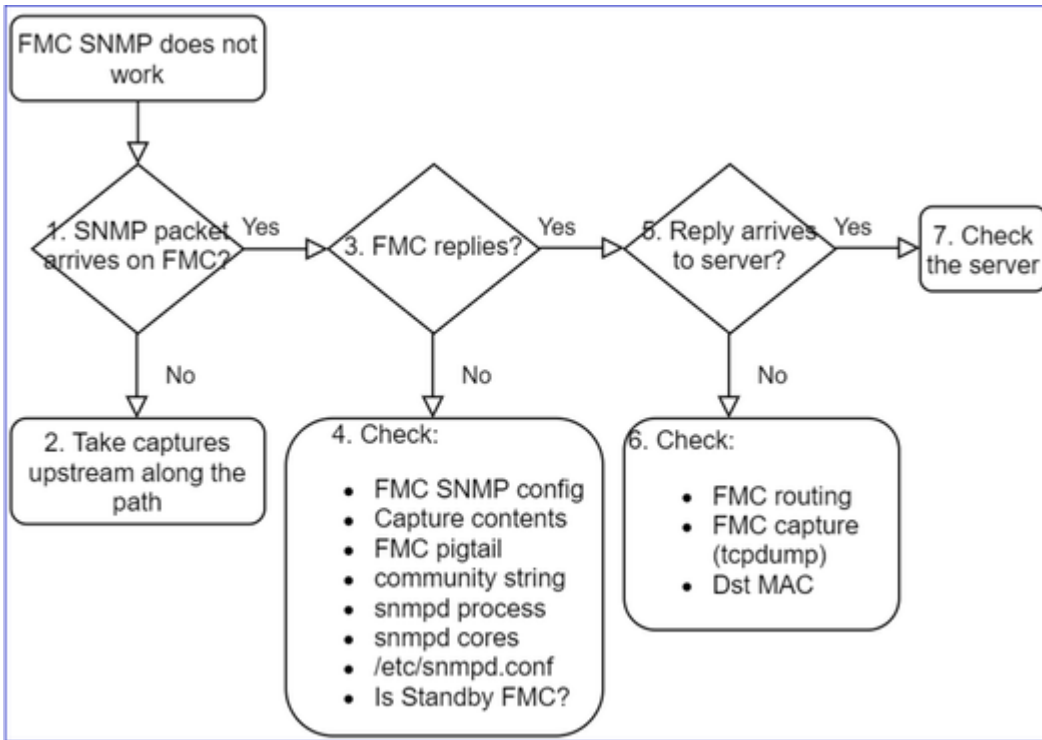
Kan FMC niet via SNMP bewaken

Probleembeschrijvingen (voorbeeld van echte Cisco TAC-cases):

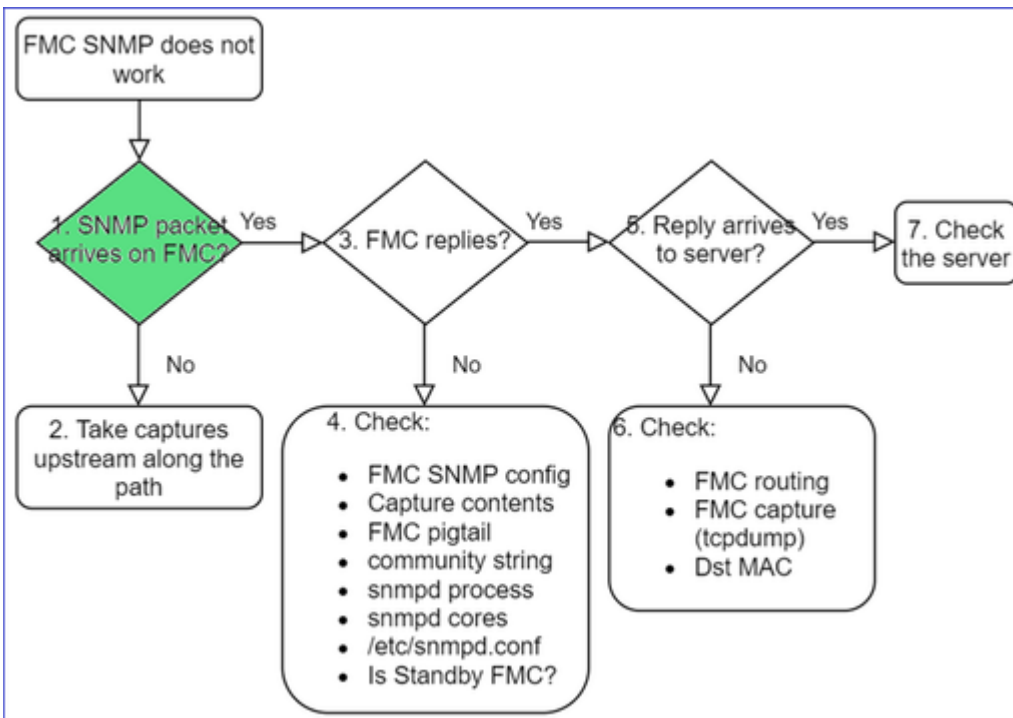
- "SNMP werkt niet op Standby FMC."
- "Behoeftte om het geheugen van de VCC te controleren."
- "Moet SNMP functioneren op Standby 192.168.4.0.8 FMC?"
- "We moeten de VCC's configureren om hun bronnen te bewaken, zoals de CPU, het geheugen enzovoort."

Probleemoplossing

Dit is het proces om stroomschema's voor FMC SNMP-problemen op te lossen:



1. SNMP-pakket wordt ontvangen op FMC?



- Opname via FMC-beheerinterface:

<#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: Sla de opname op FMC /var/common/ directory op en download deze vanuit de FMC UI

<#root>

admin@FS2600-2:~\$

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

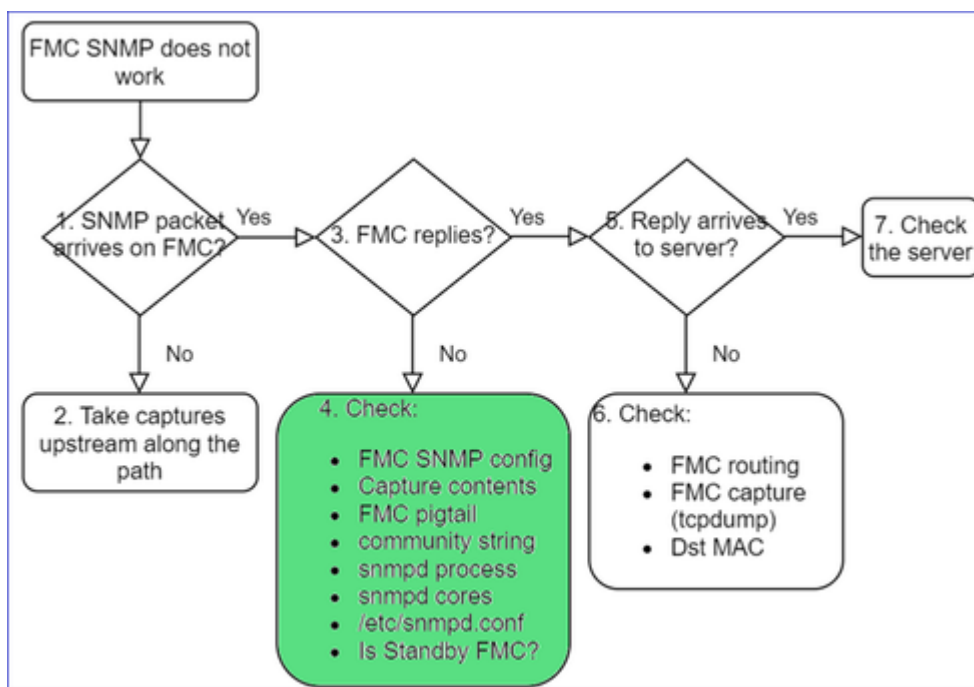
HS_PACKET_BUFFER_SIZE is set to 4.

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

^C46 packets captured

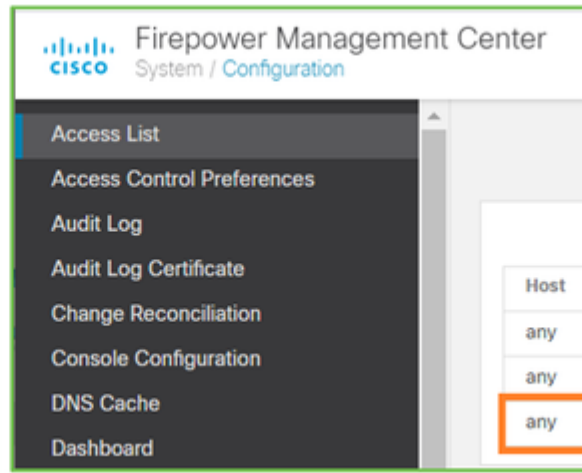
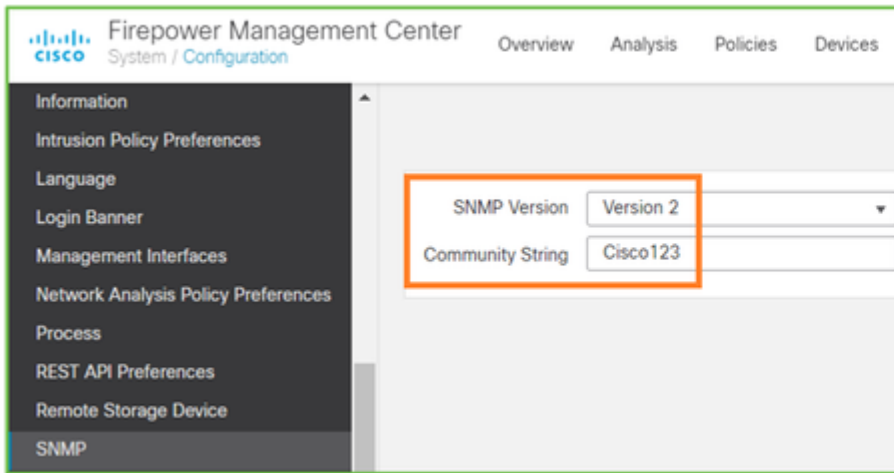
46 packets received by filter

Reageert het VCC?



Als het VCC geen antwoord geeft, controleert u:

- FMC SNMP-configuratie (systeem > configuratie)
 1. SNMP-sectie
 2. Sectie Toeganglijsten



Als het VCC geen antwoord geeft, controleert u:

- Inhoud (dop)
- Community-string (dit kan worden gezien in de captures)
- FMC pigtail output (zoek naar fouten, fouten, sporen) en inhoud van /var/log/snmpd.log
- SNMP-proces

<#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
```

- SNMP-kernen

<#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-configuratiebestand 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
```

Opmerking: als SNMP is uitgeschakeld, bestaat het bestand snmpd.conf niet

- Is het een stand-by FMC?

In pre-6.4.0-9 en pre-6.6.0 verzendt het standby-VCC geen SNMP-gegevens (SNMP heeft de status Waiting). Dit is verwacht gedrag. Verbetering in Cisco bug-id [CSCvs32303 controleren](#)

Kan SNMP niet configureren

Probleembeschrijvingen (voorbeeld van echte Cisco TAC-cases):

- "We willen SNMP configureren voor Cisco Firepower Management Center en Firepower 4115 Threat Defence."
- "Ondersteuning met SNMP-configuratie op FTD".
- "We willen SNMP-bewaking op mijn FTD-apparaat inschakelen."
- "We proberen de SNMP-service in FXOS te configureren, maar het systeem laat ons uiteindelijk geen commit-buffer toe. Fout: Wijzigingen niet toegestaan. Gebruik 'Connect ftd' om wijzigingen aan te brengen."
- "We willen SNMP-bewaking op ons FTD-apparaat mogelijk maken."
- "Kan SNMP niet configureren op FTD en het apparaat niet detecteren tijdens de bewaking."

Hoe SNMP-configuratieproblemen aan te pakken

Eerste dingen: Documentatie!

- Lees het huidige document!
- Handleiding FMC-configuratie:

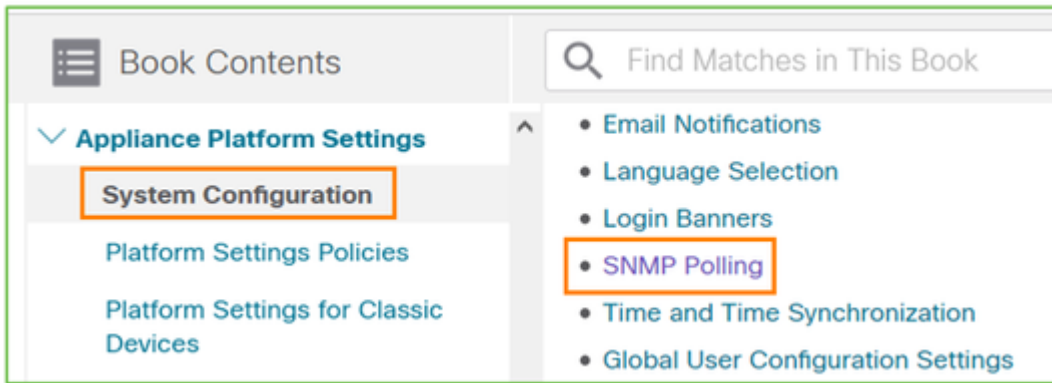
<https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html>

- Handleiding FXOS-configuratie:

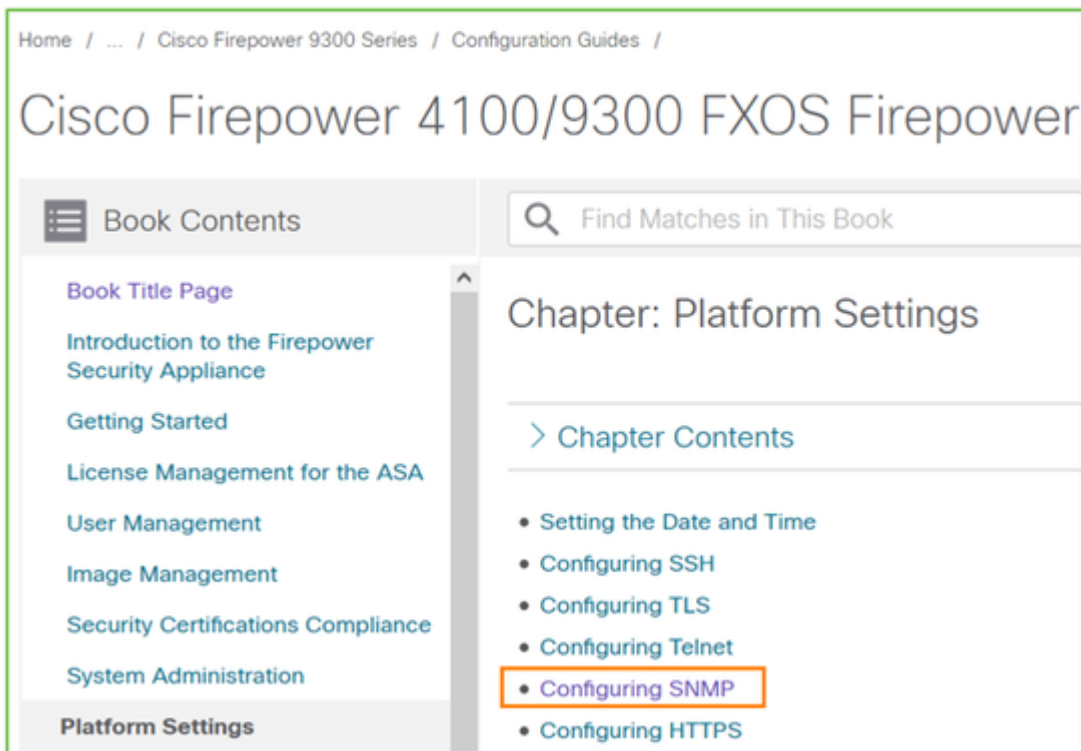
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB115F5

Let op de verschillende SNMP-documenten!

FMC SNMP:



FXOS SNMP:



Firepower 41xx/9300 SNMP-configuratie:



Firepower 1xxx/21xx SNMP-configuratie:

<ul style="list-style-type: none"> ✓ Firepower Threat Defense Interfaces and Device Settings <ul style="list-style-type: none"> 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

SNMP-configuratie op Firepower Device Manager (FDM)

Probleembeschrijvingen (voorbeeld van echte Cisco TAC-cases):

- "We hebben richtlijnen nodig over SNMPv3 op apparaat Firepower met FDM."
- "SNMP-configuratie werkt niet op FPR 2100-apparaat vanuit FDM."
- "Kan SNMP v3-configuratie niet aan de FDM laten werken."
- "FDM 6.7 SNMP-configuratieassistentie."
- "SNMP v3 inschakelen in Firepower FDM."

Hoe SNMP FDM-configuratieproblemen aan te pakken

- Voor versie pre-6.7 kunt u SNMP-configuratie uitvoeren met behulp van FlexConfig:

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

- Vanaf Firepower versie 6.7 wordt SNMP-configuratie niet meer gemaakt met FlexConfig, maar met REST API:

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

SNMP-printerbladen voor probleemoplossing

1xxx/21xx/41xx/9300 (LINA/ASA) - Wat moet worden verzameld voordat u een case opent met Cisco TAC

Opdracht	Beschrijving
FirePOWER# toont uitgevoerde SNMP-server	Controleer de ASA/FTD LINA SNMP-configuratie.
firepower# toon snmp-server statistieken	Controleer de SNMP-statistieken op ASA/FTD LINA. Stel scherp op de uitvoertellers voor SNMP-pakketten en SNMP-pakketten.
> Opnameverkeer	Leg verkeer vast op beheerinterface.

firepower# Capture SNMP-POLL interface net201 trace match upp elke willekeurige eq 161	Leg verkeer vast op data-interface (naam "net201") voor UDP 161 (SNMP-enquête).
FirePOWER# Capture SNMP-TRAP interface net208 match up elke willekeurige eq 162	Leg verkeer vast op data-interface (naam "net208") voor UDP 162. (SNMP-traps).
FirePOWER# geeft opnamen van SNMP-POLL-pakketnummer 1 weer	Traceer een SNMP-pakket met toegangsrechten dat op ASA/FTD LINA-gegevensinterface wordt ontvangen.
admin@firepower:~\$ sudo tcpdump -i tap_nlp	Leg vast op de interne tapinterface van het NLP (Non-Lina Process).
FirePOWER# toont controlepoort 161 van het protocol	Controleer alle ASA/FTD LINA-verbindingen op UDP 161 (SNMP-poll).
FirePOWER# logbestand weergeven i 302015.*161	Controleer ASA/FTD LINA log 302015 op SNMP-poll.
firepower# meer systeem:in werking stellen-configuratie i-Gemeenschap	Controleer de SNMP community-string.
firepower# debug menu netsnmp 4	Controleer de SNMP-configuratie en de proces-ID.
firepower# tonen asp tabel classificeren interface net201 domeinvergunning match port=161	Controleer of de hittellingen op de SNMP-ACL op de interface met de naam "net201"™.
FirePOWER# toont disk0: i-kern	Controleer of er SNMP-cores zijn.
admin@firepower:~\$ ls -l /var/data/cores	Controleer of er SNMP-cores zijn. Alleen van toepassing op FTD.
FirePOWER# route weergeven	Controleer de ASA/FTD LINA-routingstabel.
> netwerk weergeven	Controleer het FTD-beheervliegtuig dat tabel routeert.
admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	Controleer/los problemen op SNMPv3 op FTD.

FirePOWER# debug SNMP-spoor [255]	Verborgen opdrachten op nieuwere releases. Interne debugs, handig om SNMP met Cisco TAC op te lossen.
FirePOWER# debug van SNMP-breedsprakig [25]	
FirePOWER# debug SNMP-fout [25]	
FirePOWER# debug SNMP-pakket [25]	

41x/9300 (FXOS) - Wat te verzamelen voordat u een case opent met Cisco TAC

Opdracht	Beschrijving
<p>FirePOWER# fxos verbinden</p> <p>FirePOWER (fxos)# ethalyzer voor lokaal interfacebeheer, opnamefilter, 'udp port 161', limiet-opgenomen-frames 50 schrijven workspace:///SNMP-POLL.pcap</p> <p>vuurkracht (fxos)# afsluiten</p> <p>firepower# lokale beheertaken verbinden</p> <p>vuurkracht (lokaal beheer)# d</p> <p>1 11152 jul 26 09:42:12 2021 SNMP.pcap</p> <p>FirePOWER (Local-Management)# kopiëren workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap</p>	<p>FXOS-opname voor SNMP-poll (UDP 161)</p> <p>Upload naar een externe FTP-server</p> <p>FTP IP: 192.0.2.100</p> <p>FTP-gebruikersnaam: ftp</p>
<p>FirePOWER# fxos verbinden</p> <p>FirePOWER (fxos)# ethalyzer voor lokaal interfacebeheer, opnamefilter, 'udp port 162', limiet-opgenomen-frames 50 schrijven workspace:///SNMP-TRAP.pcap</p>	<p>FXOS-opname voor SNMP-traps (UDP 162)</p>
<p>FirePOWER# scope-systeem</p> <p>FirePOWER/system # scope services</p> <p>vuurkracht/systeem/services # toon ip-block details</p>	<p>Controleer FXOS-ACL</p>
<p>vuurkracht# defect weergeven</p>	<p>Op FXOS-fouten controleren</p>
<p>vuurkracht# toont stof-interconnect</p>	<p>Controleer de FXOS-interfaceconfiguratie en standaardinstellingen van de gateway</p>

FirePOWER# fxos verbinden firepower (fxos)# tonen in werking stelt -in werking stellen -in werking stellen SNMP allen	Controleer de FXOS SNMP-configuratie
FirePOWER# fxos verbinden FirePOWER (fxos)# tonen SNMP interne oids ondersteund maken FirePOWER (fxos)# tonen SNMP interne oids ondersteund	Controleer de FXOS SNMP-idâ€™s
FirePOWER# fxos verbinden FirePOWER (fxos)# SNMP weergeven	Controleer de FXOS SNMP-instellingen en -tellers
FirePOWER# fxos verbinden FirePOWER (fxos)# terminalmonitor FirePOWER (fxos)# debug snmp-pkt-dump FirePOWER (fxos)# debug van SNMP alles	Debug FXOS SNMP (â€™ pakkettenâ€™ of â€™ alleâ€™) Gebruik â€™ terminal no monitorâ€™ en â€™ undebg allâ€™ om dit te stoppen

1xxx/21xx (FXOS) - Wat moet worden verzameld voordat u een case opent met Cisco TAC

Opdracht	Beschrijving
> Opnameverkeer	Leg verkeer op beheerinterface vast
> netwerk weergeven	Controleer het FTD-beheervliegtuig dat de routingstabel maakt
Firepower# scope bewaking vuurkracht/monitoring # toon snmp [host] vuurkracht/monitoring # tonen snmp-gebruiker [detail] vuurkracht/monitoring # toon snmp-trap	Controleer de FXOS SNMP-configuratie
vuurkracht# defect weergeven	Op FXOS-fouten controleren

firepower# lokale beheertaken verbinden vuurkracht (lokaal beheer)# dirkercores_fxos vuurkracht (lokaal beheer)# donkere kernen	Controleer op FXOS-kernbestanden (tracebacks)
---	---

FMC - Wat te verzamelen voordat u een case opent met Cisco TAC

Opdracht	Beschrijving
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp poort 161 -n	Leg verkeer op beheerinterface voor SNMP-poll vast
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp poort 161 -n -w /var/common/FMC_SNMP.pcap	Leg verkeer op beheerinterface voor SNMP-enquête vast en sla het op in een bestand
admin@FS2600-2:~\$ supertool status groene gmp	Controleer de SNMP-processtatus
admin@FS2600-2:~\$ ls -al/var/common groene gmp	Controleer op SNMP-kernbestanden (tracebacks)
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	Controleer de inhoud van het SNMP-configuratiebestand

voorbeelden van momentopnames

Deze opdrachten kunnen worden gebruikt voor verificatie en probleemoplossing:

Opdracht	Beschrijving
# momentopname - c Cisco123 - v2c 192.0.2.1	Hiermee haalt u alle OID's van de externe host op met behulp van SNMP v2c. Cisco123 = Community-string 192.0.2.1 = bestemmingshost
# momentopname -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 = omgrenzingsprofiel32: 0	Ontvangt een specifieke OID van de externe host met het gebruik van SNMP v2c

<pre># momentopname -c Cisco123 -v2c 192.0.2.1 .10.3.1.1.4.1.9.9.109.1.1.1.1 - Aan .10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 = profiel32: 0</pre>	<p>Toont de gehaalde OID's in numerieke indeling</p>
<pre># momentopname -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1</pre>	<p>Hiermee haalt u alle OID's van de externe host op met behulp van SNMP v3.</p> <p>SNMPv3-gebruiker = cisco</p> <p>SNMPv3-verificatie = SHA.</p> <p>SNMPv3-autorisatie = AES</p>
<pre># momentopname -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -x AES -X Cisco123 192.0.2.1</pre>	<p>Voert alle OID's van de externe host op met het gebruik van SNMP v3 (MD5 en AES128)</p>
<pre># momentopname -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1</pre>	<p>SNMPv3 met alleen verificatie</p>

Hoe te zoeken naar SNMP-defecten

1. Navigeren naar <https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV>
2. Voer het trefwoord **snmp in** en kies **Selecteren uit lijst**.

The screenshot shows the Cisco Bug Search Tool interface. At the top, it says "Tools & Resources" and "Bug Search Tool". Below that, there are buttons for "Save Search", "Load Saved Search", "Clear Search", and "Email Current Search". The "Search For:" field contains the text "snmp". Below this field, there are examples: "Examples: CSCtd10124, router crash, etc...". The "Product:" dropdown menu is set to "Series/Model", and there is a "Select from list" button next to it. The "Releases:" dropdown menu is set to "Affecting or Fixed in these Releases". At the bottom, there are several filter options: "Modified Date:", "Status:", "Severity:", "Rating:", "Support Cases:", and "Bug Type:". The "Bug Type:" dropdown is currently set to "Customer Visible".

The screenshot shows a search interface with the following elements:

- Search For: (Examples: CSCtd10124, router crash, etc...)
- Product: (Selected: Cisco Firepower Management Center Virtual Appliance)
- Releases:
- Filters: Modified Date, Status, Severity, Rating, Support Cases, Bug Type (Customer Visible)
- Viewing 1 - 25 of 159 results
- Sort by:
- Result 1: **CSCvh32876 - ENH:Device level settings of FP2100 should allow to configure ACL and SNMP location**
- Symptom: This is a feature request for an option to configure access-list to restrict specific host/network to poll device using SNMP and SNMP location. FP2100 allows you to configure ...
- Severity: 6 | Status: Terminated | Updated: Jan 3, 2021 | Cases: 2 | ☆☆☆☆☆ (0)

Meest gebruikelijke producten:

- Software voor Cisco adaptieve security applicatie (ASA)
- Cisco Firepower 9300 Series
- Cisco Firepower Management Center virtuele applicatie
- Cisco Firepower NGFW

Gerelateerde informatie

- [SNMP configureren voor bescherming tegen bedreigingen](#)
- [SNMP configureren op FXOS \(UI\)](#)
- [Technische ondersteuning en documentatie â€™ Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.