

FirePOWER NGFW نیوکت ڈریلے SNMP

تائیوت حملہ

قدمہ ملہ

فیس اس الہاتر لٹمہ

تابلٹ ملہ

قدمہ س ملہ ات انوکمہ

فیس اس ا تامول ع

نیوکت لہ

ڈلے (FXOS) یدعاق لالکیہل (SNMP) طیس ب لہ کب ش لہ قرادا لوکوت ورب FPR4100/FPR9300

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (GUI)

رماؤ لار طس، ڈھج او رب ع (CLI)

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (GUI)

رماؤ لار طس، ڈھج او رب ع (CLI)

ڈلے (SNMP) طیس ب لہ کب ش لہ قرادا لوکوت ورب FPR4100/FPR9300

لینا SNMPv2c

لینا SNMPv3

م داخ دیحوت Blade SNMP 2.12.1 و FTD 7.2 و ASA 9.18.1) ڈیغش ت لاماظن) MIO نم

ف (SNMP) طیس ب لہ کب ش لہ قرادا لوکوت ورب FPR2100

ڈلے (FXOS) یدعاق لالکیہل (SNMP) طیس ب لہ کب ش لہ قرادا لوکوت ورب FPR2100

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (GUI)

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (CLI)

ڈلے (SNMP) طیس ب لہ کب ش لہ قرادا لوکوت ورب FPR2100

حقصلانم ققحت لہ

ب صاخ ل (SNMP) طیس ب لہ کب ش لہ قرادا لوکوت ورب نم ققحت لہ FPR4100/FPR9300

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (CLI)

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (GUI)

ب صاخ ل (SNMP) طیس ب لہ کب ش لہ قرادا لوکوت ورب نم ققحت لہ FPR2100

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (CLI)

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (GUI)

ب صاخ ل (SNMP) طیس ب لہ کب ش لہ قرادا لوکوت ورب نم ققحت لہ FTD

ب روم فکرحب حامس لہ (FXOS) ڈلے FPR4100/FPR9300

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (CLI)

رماؤ لار طس، ڈھج او رب ع (CLI)

ققحت لہ

فایڈ اس ا مادخت س

اھالص او عاطخ اف اش کتسا

طیس ب لہ کب ش لہ قرادا لوکوت ورب نع عاص قتس الاء اعارجا زدعتی (SNMP), FTD LINA

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (CLI)

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (CLI)

فیب نت لیسا سر ڈلے لوص حلہ نکمی ال

رب ع FMC فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (CLI)

فیم وس ب لہ مدخلت س ملہ ڈھج او رب ع (CLI)

اوه الاص او SNMP عاطخاً فاش كتس الا ئي عجم رمل ات امول عمل اقا باروا

پروتکل SNMP

علم و اتم تاذ صل

ةمدقملا

ةيسيس ألا تابلط تملأ

تابلطتما

لوكوتورب ٰيساس افريم دنتسملا اذه بلطتي SNMP.

ةمـدـخـتـسـمـلـا تـانـوـكـمـلـا

.....ةنيعوم ئي دام تانوكم وجمارب تارادصىلىع دنتسىملا اذه رصتقى ال

ڇاخ ڦيلمعم ڦئي ب یف ڏدوجوملا ڙزه جا لالا نم دنتس ملما اذه یف ڏدراولما تامولعملاء شننا مت
تناك اذا (يضارتفا) حوس مم نيو كتب دنتس ملما اذه یف ڦمدخت س ملما ڙزه جا لالا عيمج تأداب
رمأ یأ ل ممت حملار يري ثأت ل ل كمه ف نم دكأت ف ، ليغشت لا ديق كت ك بش

ةيسياساً تاماً ولعم

Firepower NGFW ۆزهجأ ميسقت نكمي نیسیئر نیعرف نیماطن یلإ

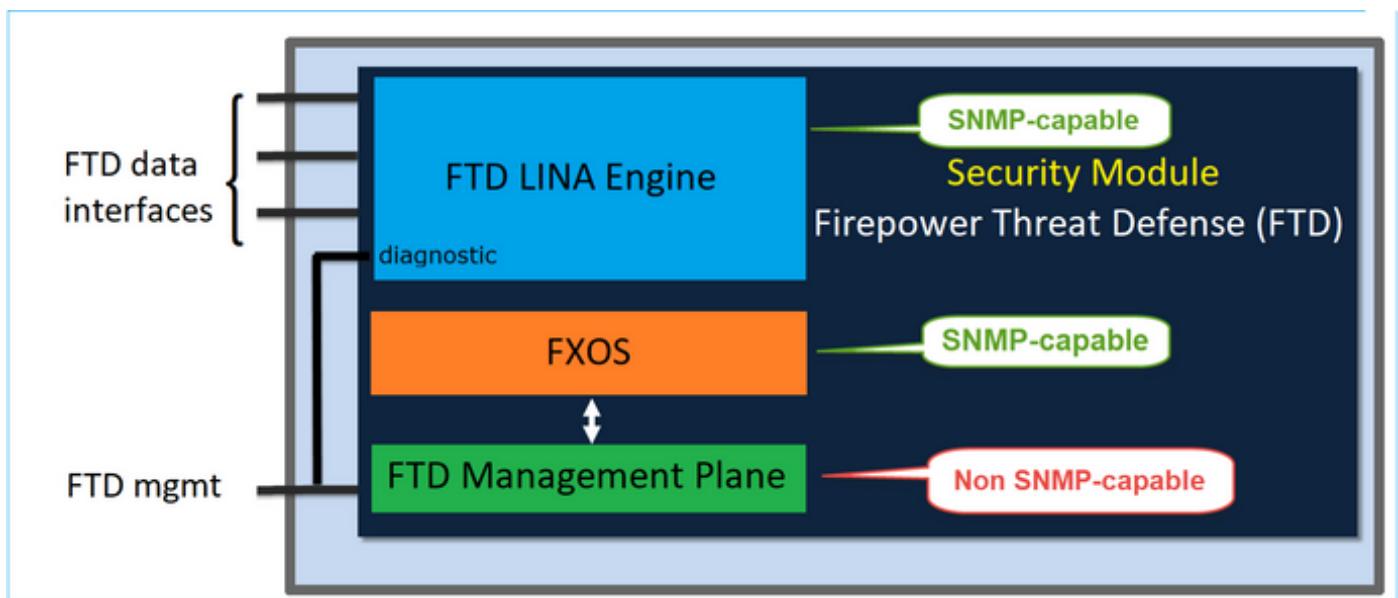
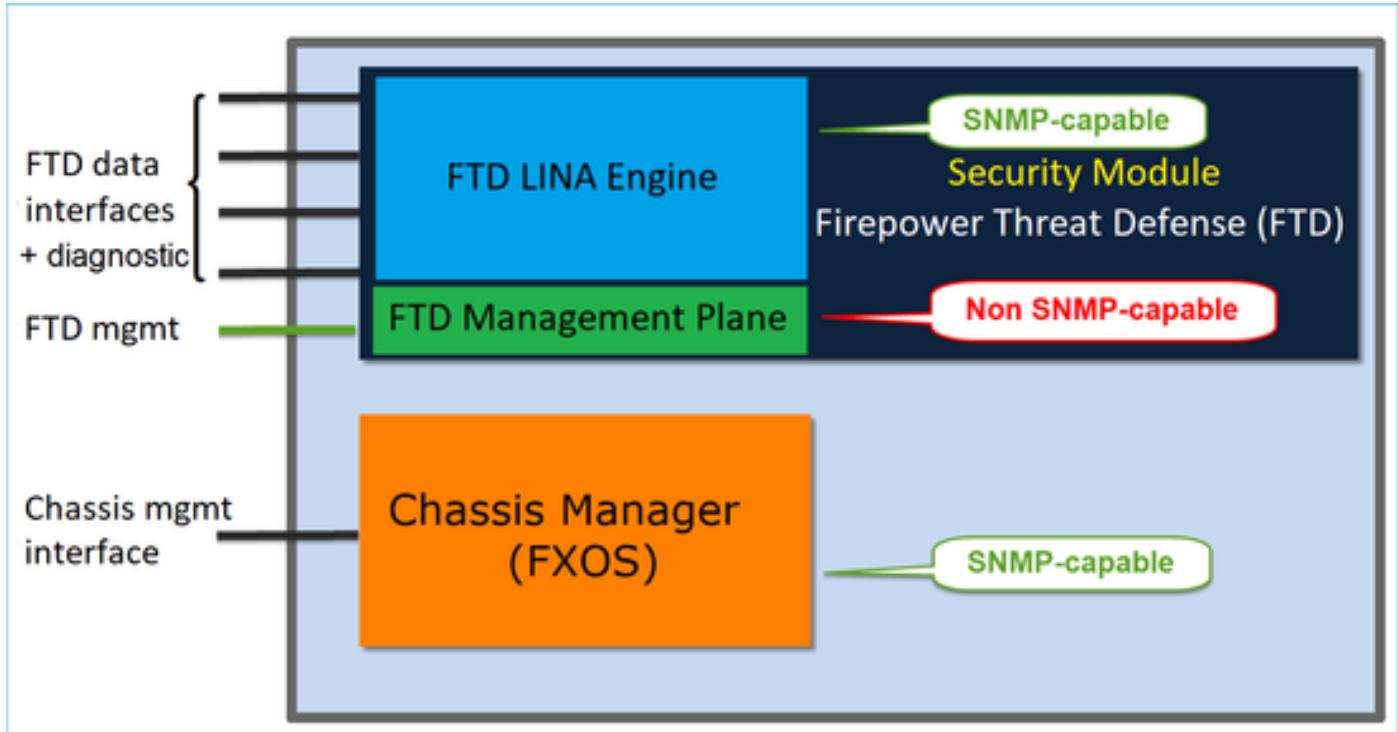
- يدعاقلا لكىهلا ۆزهچأ يف (FX-OS) ۆعسوتلل لباقلا يليغشتلا ماظنلا مكحتي.
 - ئي طمنللا ۆدحوللا لخاد Firepower Threat Defense (FTD) لمعي.

كرحم دمتسي .انييل كرحم ،ريخشلا كرحم ،نييسيلرنيكرحم نم نوكتي دحوم جمانرب و ه FTD
ةيؤر ةيناكما ب عتمتى هنأ امك ةيديلقتلـا ASA ةينقت نم FTD ب صاخـلا يـلـاحـلاـا
ـطـخـلـابـ ةـقـلـعـتـمـلـاـ تـازـيـمـلـاـ.

،ةبقارملأا ضارغألاو ةلقتسم مكحت تايوقتس ميلع FX-OS و FTD ليغشتلا ماظن يوتحي ةفلتخم تامولعم SNMP تاكرحم نم كرحم لك رفوي .ةفلتخم SNMP تاكرحم مهيدل نوكت زاهجلا ةلاحـل الـومـش رـثـكـأ ضـرعـ مـيلـعـ لـوصـحـلـلـ عـاوـسـ دـحـ مـيلـعـ ةـبـقـارـمـلـاـ دـيـرـيلـ هـلـيـحـرـتـ مـتـيـوـ

يەلاتلا لىچلا نم ۋە ئامحلا رادج ۋە جەڭلەنەتلىك سېئىرناتىنبا ايلاح دجوى، ۋە جەڭلەنەتلىك رظن ۋە جەڭلەنەتلىك Firepower: Firepower 2100 Series و Firepower 4100/9300 Series.

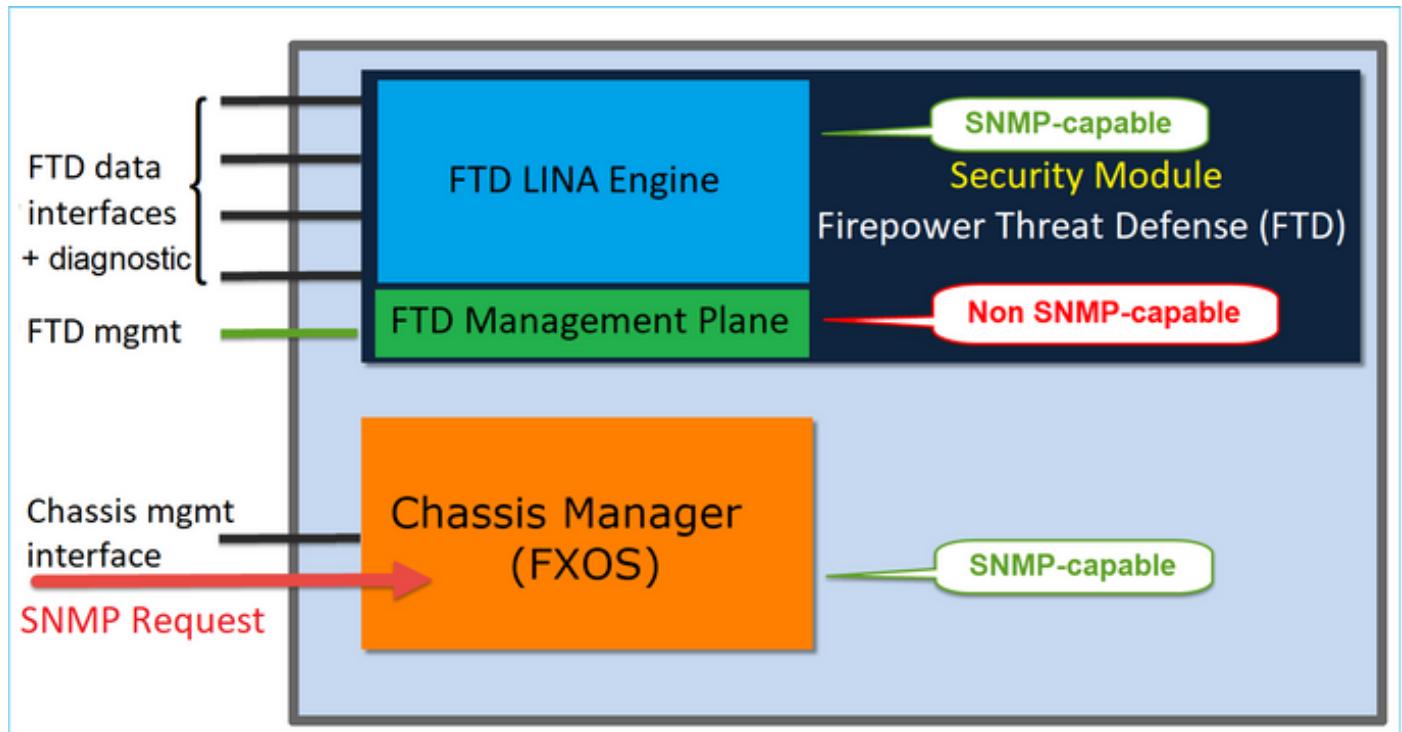
ةهجهأ وردهملا و اذهو ةزهجأا ةرادإل ةصصخم ةهجهأو لع Firepower 4100/9300 ةزهجأا يوتحت قيبطت مدخلتسى، يرخأ ئيحان نم .يعرفلا FXOS ماظن ئىلإ ةهجوملا SNMP رورم ةكرحل ةهجهأو مادختسا نكمي، 6.6 FTD، 6.6 FTD، ئقحاللا تارادصلالا يف .صيخشتلا وأ وتان ايبلالا LINN ةهجهأو SNMP نىوكتل (أضيأ FTD ةرادإ).



تاریخی غتلار ۶.۶+ جمابرلار را داشتند. FTDs یعنی

نیوکرک

ىلع (FXOS) يدعاقلا لكيلو (SNMP) طيسبلالا ئكبشلا ئرادا لوكتورب FPR4100/FPR9300



ةيموس رلا مدخلتسملالا ئهجاو رباع FXOS SNMPv1/v2c نيوكت

ماظنلا تادادعإ ىلإ لقتناو (FCM) مدخلتسنم ئهجاوحتفا 1. ئوطخلا بولطملا عمتجملالا ۋەلسلىس ددحو، SNMP نيكىمت عېرم ددح. يساسألا ظفح مىث، تابلط يف اهمادختسا.

Overview Interfaces Logical Devices Security Modules Platform Settings

NTP
SSH
▶ **SNMP**
HTTPS
AAA
Syslog
DNS
FIPS and Common Criteria
Access List

Admin State:	<input checked="" type="checkbox"/> Enable	1													
Port:	161														
Community/Username:	*****	Set:No	2												
System Administrator Name:															
Location:															
SNMP Traps															
<table border="1"> <thead> <tr> <th>Name</th> <th>Port</th> <th>Version</th> <th>V3 Privilege</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Name	Port	Version	V3 Privilege	Type							
Name	Port	Version	V3 Privilege	Type											
<table border="1"> <thead> <tr> <th colspan="3">SNMP Users</th> <th>Add</th> </tr> <tr> <th>Name</th> <th>Auth Type</th> <th>AES-128</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				SNMP Users			Add	Name	Auth Type	AES-128					
SNMP Users			Add												
Name	Auth Type	AES-128													
<table border="1"> <thead> <tr> <th colspan="2">SNMP Trap Destinations</th> <th>Add</th> </tr> <tr> <th>Name</th> <th>Port</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>				SNMP Trap Destinations		Add	Name	Port	Type						
SNMP Trap Destinations		Add													
Name	Port	Type													
<input type="button" value="Save"/> 3 <input type="button" value="Cancel"/>															

ىلע دوجوملا صنلا نإف ،لعل فلاب انيعم مدخلتسملامسا/عامتجملا لقح ناك اذا: ظحالم دق مدخلتسملامسا/عامتجملا لقح نكى مل اذا . معن: عومجملا أرقى غرافلار لقحلا نيمىي ال: عومجملا أرقى غرافلار لقحلا نيمىي ىلع دوجوملا صنلا نإف ،قميقب دعب ٥٥ميمع م

ا ووطخلا 2. ةجومداخ نيوكت 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

نوکت نأ نكمي و ظلت سم ةممىالملاء فيضم و تامالعتسالل عمتجملا ميق: ظحالء ةفلتخم

لئاسر مداخ نيكوت ظفح متيس و قفاوم ددح .مسالاب وأ IP ناونعك فيضم ملا فيريع نكمي ئيسيرلإ SNMP ظفح نم ظفح لرا رز ديدحتل ظجاح كانه تسيل .أيئاقت هيبنت فيضم فذحب موقع امدنع هسفن عيشلا ثدحي.

رماؤلا رطس ةهجاو رباع FXOS SNMPv1/v2c نيكوت (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 مدخلة ملأ ةهج او ربع ةي مو سرلا (GUI) نيوكت

SNMP بيو بت < يساسألا ماظنلا تادادع إيلإ لقتناو FCM حتفا 1. ةوطخلالا

مسقلالا يف عمتجم ٩لسلس يأ نبييعتل ةجاج دجوت ال SNMP v3 ل ئبسنلاب 2. ةوطخلالا FXOS SNMP كرحم إيلإ تامالعتسالا ليغشت هؤاشن ا مت مدخلتسنم لك عي طتسن ي . يولعلالا، كلذ نم ءاهتنالا درجمب . يساسألا ماظنلا يف SNMP نيكمنت يه إيلولأا ةوطخلالا . حاجن ب يمدخلتسن نم لك ظفح مت ي . ةهجولالا هيبنت لئاسر فيضم و نيمدخلتسنملالا عاشن ا كنكمي . آيئاقلت SNMP هيبنت لئاسر فيضم و SNMP

ا

Local Devices

Security Modules

Platform Settings

Admin State:

 Enable

1

Port: 161

Community/Username: Set:NoSystem Administrator Name: Location:

SNMP Traps

4

 Add

Name	Port	Version	V3 Privilege	Type

SNMP Users

3

 Add

Name	Auth Type
	AES-128

2

 Save Cancel

نکلو SHA آمیاد وه ۆقاداصملا عون . SNMP مدختسەم فضا ، ئروصلایف حضوم وە امك . 3. ۆوطخلە ریفشتلە DES وأ AES مادختسە لەنکەمی :

Add SNMP User



Name:*

Auth Type:

SHA

Use AES-128:



Password:

Confirm Password:

Privacy Password:

Confirm Privacy Password:

*****|

OK

Cancel

ةروصلـا يـف حـضـوم وـه اـمـكـ، ةـمـىـالـمـ فـيـضـمـ ةـفـاضـإـ 4ـةـوـطـخـلـاـ

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

رميوك FXOS SNMPv3 رطس ٤ او ٥ او ٦ او ٧ (CLI)

```
<#root>

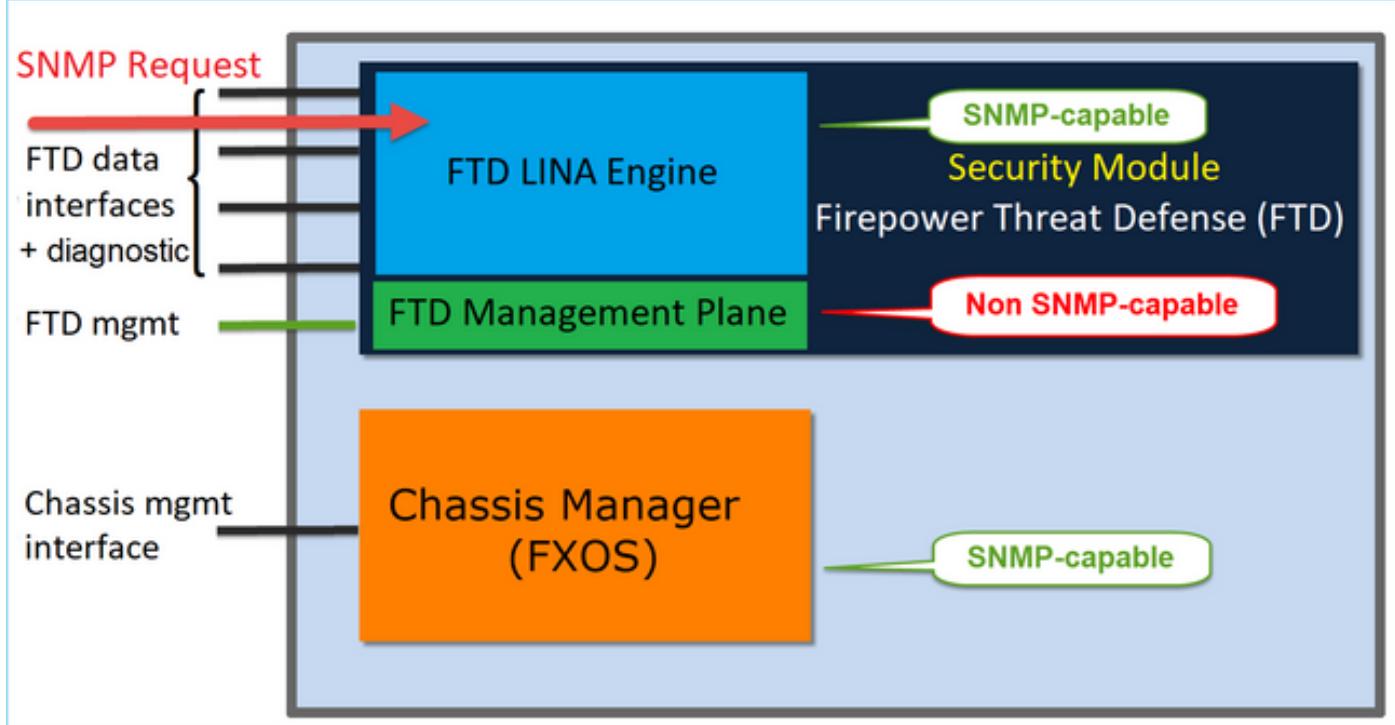
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring #
create snmp-user user1

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* #
```

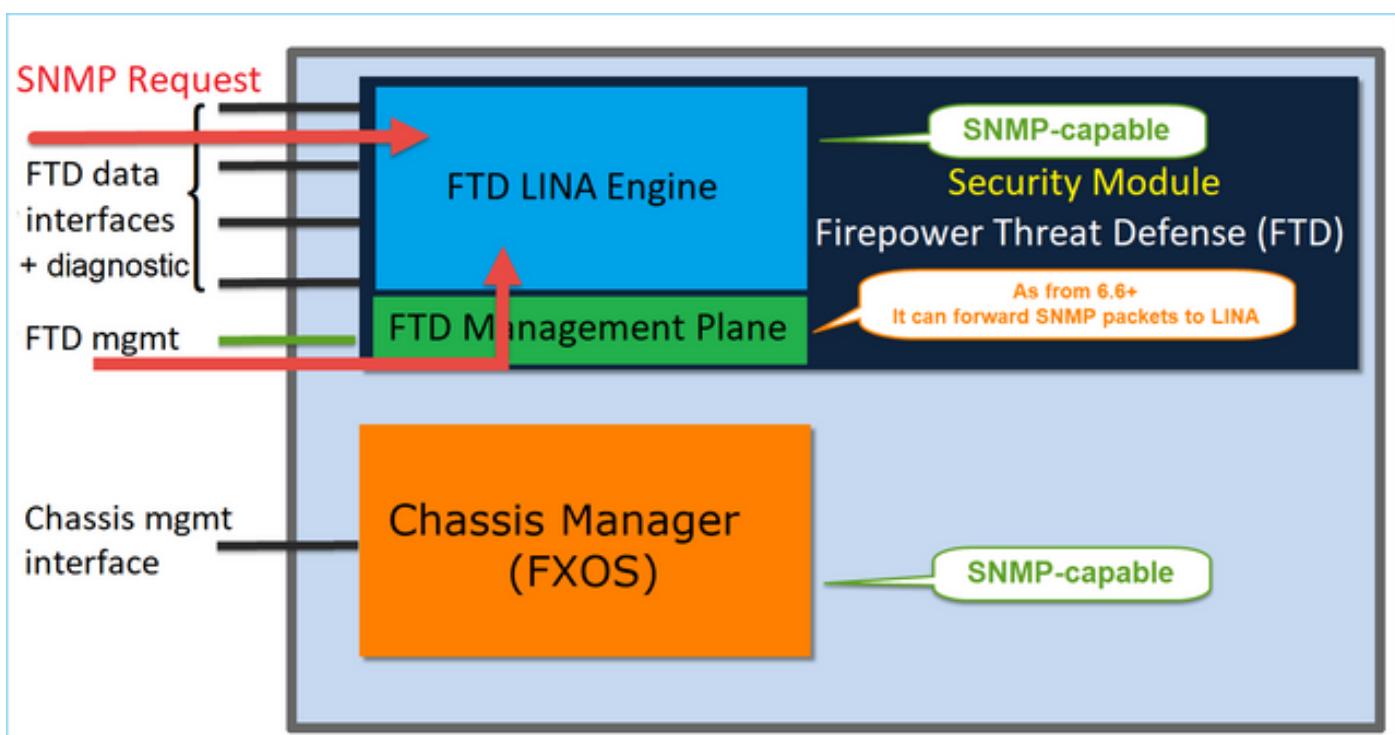
```
set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter snmp-trap 10.48.26.190
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v3
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype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

ىلع FTD (LINA) طيسبلا ةكبشلا ةرادا لوكوتورب
FPR4100/FPR9300



تارادصا يف تارييغتلما 6.6+

- تاعالطتسال FTD ۋارادا ۋەجاو مادختسا رايخ آپسيا كىدل نوكي، 6.6 دىب ام تارادصا يف ھېبىنتلار ئاسرو يارلا.



ةمظنألا عىمج ىلع ًادعاصف 6.6 نم لوكوتوربلى درفل IP ناونع ۋارادا ۋەزىم معىد متى لـ FTD:

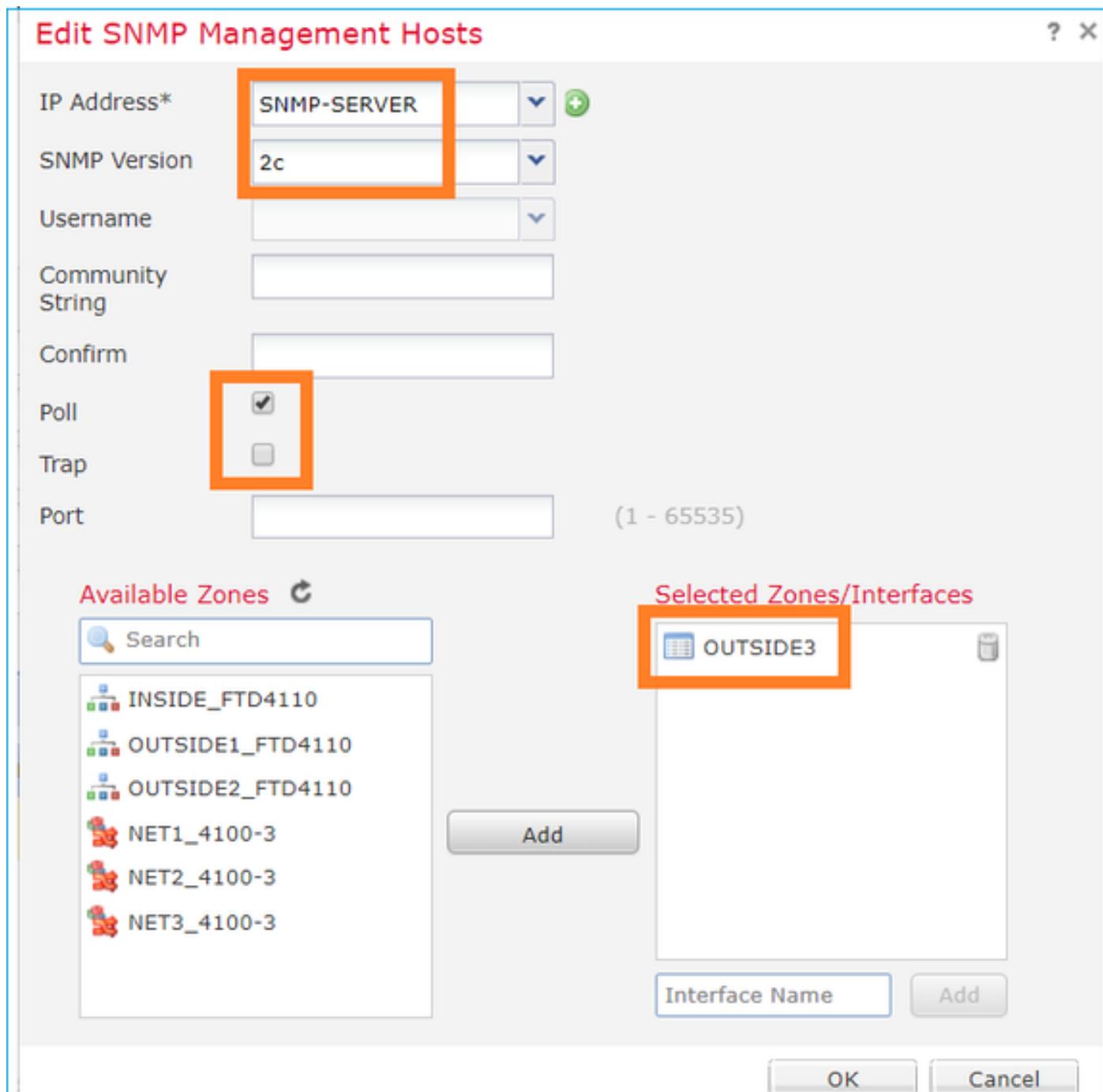
- FPR2100
- FPR1000
- FPR4100

- FPR9300
- ASA5500 لىغشتب موقى يذلا FTD
- FTDv

نېوكت LINA SNMPv2c

دەج. يساسەلە ماظنلە تادادعى > ئەزىزلىكىندا FMC، مەختىسىم ئەجأولىع 1. ئەوطخلە: يلى امك SNMPv2 تادادعى نېوكت بىرەتىپ 'رايىخ' SNMP مداخنى كەمت:

مداخ تادادعى دەج و ئەفاضى رىزلا دەج ئەفيض مەلە تايىبلا بىوبتىلا ئەم الىع يە. 2. ئەوطخلە: SNMP:



ئەج اويه ئەي سەخنىنىڭ ئەجأولىا SNMP. لىاسىرلە دىرىمىك سەخنىنىڭ ئەجأو دىدەت كەنگەمىي امك طققى ئەرادىلە) عبىرمەلە نەم و عبىرمەلە ئەلە رورىمەلە ئەلە طققى حىيتت تانايىب.

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



Selected Zones/Interfaces

Search

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

Add

diagnostic



Interface Name

Add

Cancel

OK

ةـ حتـ اـ فـ لـ اـ مـ دـ خـ تـ سـ تـ وـ 6.6ـ رـ اـ دـ صـ إـ لـ اـ نـ مـ ةـ ذـ فـ أـ مـ ةـ روـ صـ لـ اـ هـ ذـ هـ.

ةـ رـ اـ دـ إـ لـ اـ ةـ هـ جـ اوـ رـ ايـ تـ خـ اـ أـ ضـ يـ اـ كـ نـ كـ مـ يـ ،ـ كـ لـ ذـ لـ اـ ةـ فـ اـ ضـ إـ لـ اـ بـ

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



Add

2100_inside

2100_outside

cluster_dmz

cluster_inside

cluster_outside

Selected Zones/Interfaces

diagnostic



Interface Name

Add

Cancel

OK

ةرادلـا ةـهـجـ اوـ ربـع LINA SN~MP رـفـوتـي ،ـهـدـيـدـجـلـا ةـهـجـ اوـ دـيـدـحـتـ ةـلـاحـ يـفـ.

ةجيتنل:

The screenshot shows the LINA SNMPv3 configuration interface. On the left sidebar, under the 'SNMP' section, the 'Users' tab is selected. In the main panel, the 'Hosts' tab is active, displaying a table with one row: OUTSIDE3, SNMP-SERVER, 2c, Poll. Below this table, there are tabs for 'Users' and 'SNMP Traps'. A modal window titled 'Add Username' is open, containing fields for Security Level (Priv), Username (cisco), Encryption Password Type (Clear Text), Auth Algorithm Type (SHA), Authentication Password*, Confirm*, Encrytion Type (AES128), Encryption Password*, and Confirm*. The 'Username' field is highlighted with a red border.

نیوکت LINA SNMPv3

دەج > يساس ألا ماظنلە تادادعى > ۋەزەجىلىلى لى قىتنى، FMC مەختىسىم ۋەجأولىع. 1. ۋەطخىلى فېيىضمۇ مەختىسىم نیوکتەوە SNMPv3:

The screenshot shows the LINA SNMPv3 configuration interface. On the left sidebar, under the 'SNMP' section, the 'Users' tab is selected. In the main panel, the 'Users' tab is active, displaying a table with columns 'Username' and 'Encryption Password Type'. A modal window titled 'Add Username' is open, containing fields for Security Level (Priv), Username (cisco), Encryption Password Type (Clear Text), Auth Algorithm Type (SHA), Authentication Password*, Confirm*, Encrytion Type (AES128), Encryption Password*, and Confirm*. The 'Username' field is highlighted with a red border.

Overview Analysis Policies Devices Objects | AMP Intelligence

Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

mzafeiro_FTD4110-HA

Enter Description

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

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Port (1 - 65535)

Hosts **Users** **SNMP Traps**

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

Add  

تامیالم یقلتل اضیأ فیضملا نیوکتب مق. 2. ۋەطخىل:

Edit SNMP Management Hosts

IP Address*	<input type="text" value="SNMP-SERVER"/> 
SNMP Version	<input type="text" value="3"/>
Username	<input type="text" value="cisco"/>
Community String	<input type="text"/>
Confirm	<input type="text"/>
Poll	<input checked="" type="checkbox"/>
Trap	<input checked="" type="checkbox"/>
Port	<input type="text" value="162"/> (1 - 65535)

Available Zones 

-  INSIDE_FTD4110

Selected Zones/Interfaces

-  OUTSIDE3  

تامیالم مسق نموض اهمالتسا دىرت يىتللا تامیالملا دىدحت نكمى. 3. ۋەطخىل SNMP:

مدادخ دیحوت FXOS 2.12.1 و FTD 7.2 و ASA 9.18.1) Blade SNMP میغشتلا ماظن (MIO نم

لوبق ام کولس 7.2

قرادإلا تامولعم دعاؤق رفوتت ال، 4100 و 9300 اهدع غلبی یتللا ةیساسألا ۃمظنألا یف ممت یذلا SNMP لوكوتورب یلع لکیهلا تامولعمب ۃصالخا SNMP لوكوتوربل (MIB) لاخدا لا ۃدحو یلع لصفنم لکشب هتئیهت مزلي FTD/ASA. ۃراديلا ۃدحو و هنیوکت ۃراديلا ۃدحو و هنیوکت MIO. لصفنم لکشب هیلا لوصولالکیهلا ریدم رباع (MIO) جارخالا او فرشملالا) جارخالا/لاخدا لا او.

- مدادخا یلع ۃدحاو، SNMP لوكوتوربل نیتلصفنم نیتسایس نیوکت مزلي لوكوتورب ةبقارمل (MIO) جارخالا/لاخدا لا ۃدحو یلع یرخالا او قیبطتللایلصننلا دحاو ذفنم و یلصننلا مدادخلل دحاو ذفنم عقاوب، ۃلصفنملا ذفانملما مادختس ا متی زاهجلل (SNMP) طیسبلا لاصتا لا ۃکبش ۃرادإ لوكوتورب ةبقارمل (MIO) جارخالا/لاخدا لا سفن ۵.
- اهتبقارم و 4100 و 9300 ۃزهجأ نیوکت ۃلواحم دنع دیقعت عاشن ایل اذه یدؤی نأ نکمی لوكوتورب رباع SNMP.

(یلعأو ۱ و ASA 9.18.1 و FTD 7.2 و FXOS 2.12.1) ثدحألا تارادصلالا عم هلمع ةیفیک

- دعاؤق عالطتسا نیمدختسمملل نکمی، ۃزیمل MIO، Blade SNMP مدادخ دیحوت لالخ نم (ASA/FTD). ۃراديلا تامولعم MIO و LINA ماظنل (MIB).
- ۃدحوب ۃصالخا ۃدیدجل (CLI) رمأولا رطس ۃھج او رباع اھلیطعات و ۃزیمل نیکمی ۃرادإلا یف مکحتلا ۃدحومدختسم ۃھج او (MIO) جارخالا/لاخدا لا (FCM) (Chassis mgr).
- لقتسم لیثمک لمعی MIO SNMP لیکونأ ینعی اذهو. ۃلطعم ةیضارتفالا ۃلاحلا ۃصالخا (MIB) ۃرادإلا تامولعم دعاؤق عالطتسا MIO تاهجاو مادختس ا مزلي عالطتسا ل قیبطتللا تاهجاو مادختس ا نکمی، ۃزیمل نیکمی درجمب و لکیهلا ب (DME) ۃرادإلا تامولعم دعاؤق سفن (MIB).
- > یساسألا ماظنلا تادادع نم ض "لکیهلا ریدم" مدختسا ۃھج او یلع نیوکتلا رفوتی SNMP > موقیس یذلا FTD لیثم دیدحت مدختسا مل نکمی ثیح، لوؤسملالا لیثم

- NMS ىلـا هـمـيـدـقـتـلـلـلـكـيـهـلـلـ (MIB) ةـرـادـالـاـ تـامـوـلـعـمـ دـعـاـوـقـ عـيـمـجـتـ /ـعـيـمـجـتـ بـ
- ـةـمـوـعـدـمـ MI وـةـيـلـصـأـلـاـ ASA/FTDـ تـاقـيـبـ طـ.
- جـاخـالـاـ /ـلـاخـدـالـاـ تـادـحـوـ ىـلـاـ ةـدـنـتـسـمـلـاـ ةـيـسـاسـأـلـاـ ةـمـظـنـأـلـاـ ىـلـعـ الـاـ ئـيـمـلـاـ هـذـهـ قـبـطـنـتـ الـ
- (FPR9300 و FPR4100).

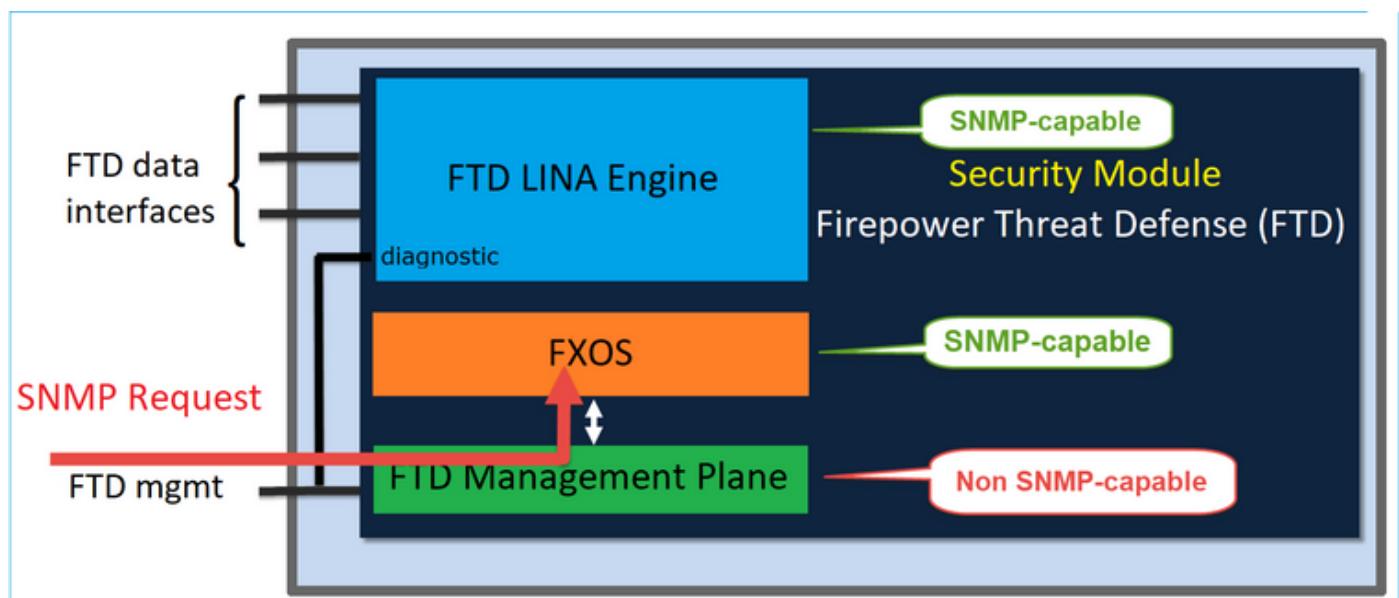
موعدملا ئيساسألا ئمظنألاو ئيساسألا تابلطتملا

- "موعدملا ريدملارادصلالىندألا دحلا": FCM 2.12.1
 - "ةرادرادملالىندألا دحلا": FPR9300 / FP4100
 - "بولطمملاموعدملا رادملازاهجلا رادصلالىندألا دحلا": FXOS 2.12.1 و FTD 7.2 و ASA 9.18.1

FPR2100 يف (SNMP) طيسبلا ۃكبشلا ۃرادا لوكوتورب

FCM. FPR2100 ۋە ئەن ئۆچۈن ئەن سەرەتلىك SNMP ىچىرىنىڭ ئەن سەرەتلىك FMC.

FXOS (FXOS) يدعاقلا لکيهل (SNMP) طيسبلأا ةكبشلا ةرادا لوكوتورب FPR2100



هذه يف SNMP لوكوتوربل FTD ۀرادا ۀ وج او مادختسا راي خ آضيأ كل رفوتي ، FTD 6.6+ نم آعدب FXOS و LINA SNMP نم لك تامولعم لقون متى ، ؤلاحلا FTD.

FXOS SNMPv1/v2c نى وكت

لوكوتورب ددح و زاهجلا ددح .**قرهجألا** **قرادإ** > **قرهجألا** **يل** **لقتن** او **FMC** **مدختسم** **قرهجأوحتف** **SNMP**:

Overview Analysis Policies Devices Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD2100-4 Cisco Firepower 2110 Threat Defense

You have unsaved changes

4 Deploy 20+ System Help Itebar

Device Routing Interfaces Inline Sets DHCP SNMP

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

Admin State: Enable Port: 161
Community: ***** System Admin Name:
Location:

SNMP Traps Configuration

2

Hostname	Port	Version	V3 Privilege	Type
No records to display				

SNMP Trap Configuration

Hostname: * 10.48.26.190

Community String: * *****

Port: * 162 (1 - 65535)

SNMP Version: V2

Type: TRAPS

Privilege: NO_AUTH

OK Cancel

ي ف ر ي ي غ ت ل ا FTD 6.6+

ة رادا ة ه ج او د ي د ح ت ك ن ك م ي FTD:

The screenshot shows the 'Devices' tab selected in the navigation bar. Under 'Platform Settings', the 'FTD_Platform_Policy' is selected. On the left, a sidebar lists various security features like ARP Inspection, Banner, DNS, etc., with 'SNMP' being the active section. The main panel shows the configuration for SNMP servers, with fields for IP Address (host_10.229.20.30), SNMP Version (2c), Username, Community String, Poll, Trap, and Port (161). A modal window titled 'Add SNMP Management Hosts' is open, prompting for 'IP Address*', 'SNMP Version', 'Username', 'Community String', 'Poll', 'Trap', and 'Port' (162). The 'Reachable By:' section has two options: 'Device Management Interface (Applicable from v6.6.0 and above)' (selected) and 'Security Zones or Named Interface'. Below this are 'Available Zones' and 'Selected Zones/Interfaces' sections, with an 'Add' button between them. At the bottom of the modal are 'OK' and 'Cancel' buttons.

قلاسر ضرعت ٰحفصىلا نإف، لوكوتورب ل ٰرادل ٰهنجاونيوكت ًاضيأ نكمي هنأ ًارظن و
ذه ريدختل:

تادادعإ نيوكت مت اذإ، ٰحفصىلا هذه ىلع زاهجلل يساسألا ماظنلل SNMP نيوكت ليطبعت مت
ي
ن عافدلا) يساسألا ماظنلا تادادعإ > ٰزهجألا لالخ نم ٰزهجألا ٰرادا ٰهنجاومادختساب
ـيضرمل ٰزهجألا > SNMP >

نیوکت FXOS SNMPv3

لوكوتورب ددحو زاهجل رت خا. ٰزهجألا ٰرادا > ٰزهجألا راي تحال لقتنا او FMC مدختسم ٰهنجاوح تف
ـي SNM.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

FTD2100-4 Cisco Firepower 2110 Threat Defense

You have unsaved changes **Save** Cancel

Device Routing Interfaces Inline Sets DHCP **SNMP**

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

Admin State: Enable **1**

Port:

Community:

System Admin Name:

Location:

SNMP Traps Configuration

No records to display

K < | Page | > >> | C

SNMP Users Configuration

No records to display

2

3

4

5 Deploy 20+ System Help ▾ Sidebar ▾

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:

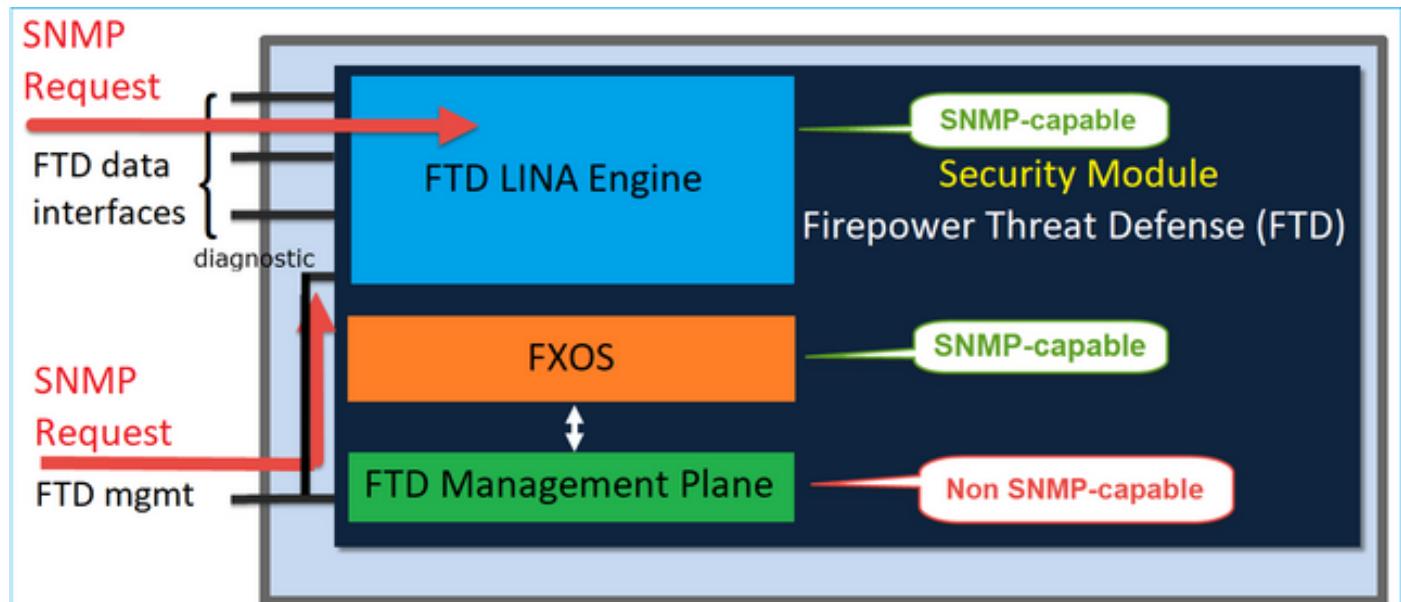
PRIV

OK

Cancel

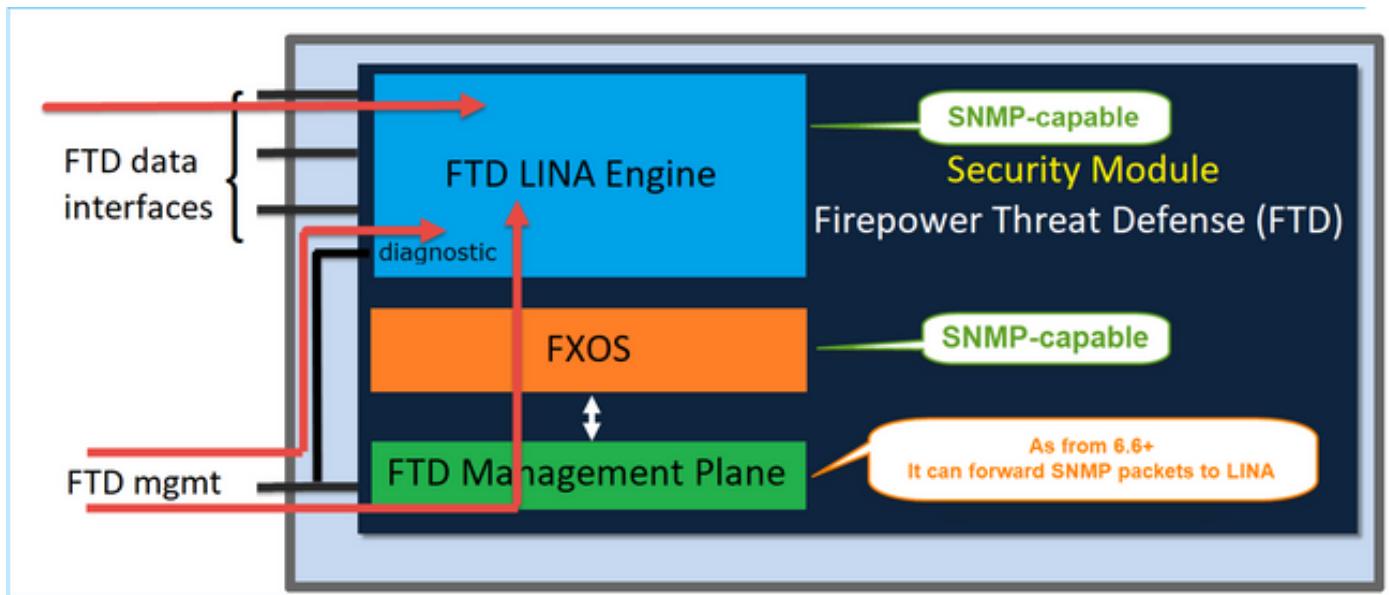
لوكوتورب FTD (LINA) طيسبل اوكبشا لارادا (SNMP) ىلع FPR2100

- بـ صالح SNMP لوكوتورب نيوكـت نوكـي ، 6.6 لـ بـ اـم تـارـادـصـاـل ئـبـسـنـلـابـ LINA FTD زـاهـجـ ىـلـعـ FP1xxx/FP21xx FTD FirePower 4100 وـاـ 9300.



تـارـادـصـاـلـاـ FTD 6.6+

- يأر تاعال طتسال FTD ۋارادى ۋەجاو مادختسا رايىخ ًاضيًأ كىدىل نوكىي، 6.6 دىپ ام تارادى يىف ھىبىنەت لئاسرو LINA.



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
UCAPI/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

Search

Selected Zones/Interfaces

Add

Interface Name

OK Cancel

دی دجلا ۋارادىلا ۋە جا دىرەت مەتىي مەل لاح يىف

- ٤رادٌالا ٤زهٌج او ربٌع LINA SNMP رفوتٌي.
 - ٤بٌولطٌم دعٌت مل اهٌنأ SNMP بٌيوبٌتلا ٤مٌالع لٌي طعٌت مٌتي، ٤زهٌج الٌا ٤رادٌا > ٤زهٌج الٌا نمٌض.
 - ٤مٌظن الٌا ٤لٌع طقٌف ٤يٌئرم SNMP زاهٌج بٌيوبٌت ٤مٌالع تٌنٌاک. ٤مٌالع ا٤راغٌش ضرٌع مٌتي ٤يٌس ا٤س الٌا FPR9300/FPR4100 ٤يٌس ا٤س الٌا ٤مٌظن الٌا ٤لٌع ٤حٌفٌصٌلٌا هذٌه دجٌوت ال 2100/1100.

و FTD55xx.

نیجدم FXOS ىل افاض الاب LINA SNMP حبصي، اهن يوكت درجمب FP1xxx/FP2xxx) ىلع) ئارادا ئەھج او رباع SNMP ھېبنت لىاسر ئاصقىتسالا تامولعم FTD.

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 Interface.

① SNMP settings configured on this page will apply only to the device platform

Admin State: Enable

Port: 161

Community:

System Admin Name:

Location:

SNMP Traps Configuration

Hostname	Port	Version	V3 Privilege	Type
No records to display				

- FPR2100
 - FPR1000
 - FPR4100
 - FPR9300
 - ASA5500 لیغشتب موقی یذل FTD
 - FTDv

تادي ده تلا دض عافدلل SNMP نیوکت نم ققحت، لیصافتلا نم دیزمل

ةحصـلـا نـم قـقـحتـلـا

FXOS SNMPv2c تايلمع ققحتلا نم

(CLI) رم وألا رطاس ۋەجىءەن يۈكىت نم قىقحتلار

<#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

```

عزم و نم FXOS:

```

<#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

```

هيكل قواعد البيانات تايلم:

```

<#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
...

```

تابل ط رابتخا SNMP.

حلاص فيضم نم SNMP بلط ذي فنتب مق.

يىبنتل لئاسر ئاشن ديكأت.

لئاسر ئاشن ديكأتل ethanalyzer ليلىحتلا ئادأ نيكمت عم ۋەج او بلق مادختسا كنكمي: ددھملا ھيىبنتل لئاسرل ۋېيىضملار ئەزەج ئەلە ئەلەسراو SNMP ھيىبنت

```

<#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

```

⚠ رابتخالا اذه ئارجاپ مق. رورملا ئەكەن عاطقىنا يف ۋەج او ئەفرەر بېسىتىي نأ نكمى: رىذحت ئەنايىصلار ئەذفان يف وا طقق ئەيلەمعم ئېيىب يف

نم ققحتلا تايىلمع FXOS SNMPv3

اذا مدختسىملا رەظىي > FCM > SNMP مىختىسم ۋەج اول يىس اسالا ماظنلى تادادعى حىتف 1. ۋەطخىل ئەيىصوصخ و رورم ئەملەك يأ نىيوكت مت ام:

Edit user1

Name:*	<input type="text" value="user1"/>			
Auth Type:	SHA			
Use AES-128:	<input checked="" type="checkbox"/>			
Password:	<input type="password"/>	Set:Yes		
Confirm Password:	<input type="password"/>			
Privacy Password:	<input type="password"/>	Set:Yes		
Confirm Privacy Password:	<input type="password"/>			

OK **Cancel**

بة قارم تحت SNMP نیوکت نم ققحتلا کنکمی ، رم اولا رطس ۃجاویف . 2 ۃوطخل اقاطن لـ :

```
<#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:	Port	Community	Version	V3 Privilege	Notification	Type
SNMP Trap	162		V3	Priv		Traps
192.168.10.100						

لیص افتل او SNMP نیوکت عیس ووت کنکمی FXOS، عرض و تخت 3. ۃ و ط خ ل ا:

```
<#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

SNMP رابطہ تابلٹ

تاردقب دوزم زاهج يأ نم SNMP بلط ذيفنتو نيوكتلا نم ققحتلا كنكمي SNMP.

SNMP: اطّاخ حيّحصت مادختسَا كنكمي ، SNMP بـ لـ طـ ظـ جـ لـ اـ عـمـ ةـ يـ فـ يـ كـ نـ مـ قـ قـ حـ تـ لـ لـ

<#root>

ksec-fpr9k-1-A(fxos) #

```
debug snmp pkt-dump
```



**!
راهجلا ءادأ لعل ءاطخألا حي حصن رثؤي نأ نكمي :ريذحت**

FXOS - ب صالحا (SNMP) طيسبل اوكبشا لرادا لوكوتورب نم قحتلا FPR2100

FXOS SNMPv2 نم ققحتلا تايلمع

(CLI) نم ققحت نیوکتلا او رباع ٥٥ جا رطس اوألا رم:

<#root>

FP2110-4 /monitoring #

show snmp

Name: snmp

Admin State: Enabled

Port: 161

Is Community Set: Yes

Sys Contact:

Sys Location:

SNMP Trap:

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

SNMP کا ول س دکاؤ

وأفيضم زاهج نم SNMP بـ FXOS نع مالعـتسـالـاـىـلـعـ كـتـرـدـقـ نـمـ قـقـحـتـلـاـ كـنـكـمـيـ تـارـدـقـبـ دـوـزـمـ زـاهـجـ يـأـ

هـلـ ةـبـاجـتـسـالـاـ اوـ سـنـمـ بـلـطـ عـالـ طـالـلـ capture-traffic رـمـأـلـاـ مـدـخـتـسـاـ:

```
<#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
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
```

نم ققـحـتـلـاـ تـايـلـمـعـ FXOS SNMPv3

(رمـأـلـاـ رـطـسـ ةـهـجـ اوـ رـبـعـ نـيـوـكـتـلـاـ نـمـ قـقـحـتـ)

```
<#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
```

كولس دكأ SNMP.

FXOS نع مالعتسا لىع كتردق نم ققحتل SNMP بـلـطـلـسـرـا.

:ـبـلـطـلـاـ لـيـجـسـتـ كـنـكـمـيـ ،ـكـلـذـلـكـ ةـفـاضـإـلـابـ

```
<#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= [|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
```

بـ صاخـلـا (SNMP) طـيـسـبـلـا ةـكـبـشـلـا ةـرـادـا لـوـكـوـتـورـبـ نـم قـقـحـتـلـا

بـ صاخـلـا SNMP لـوـكـوـتـورـبـ نـيـوـكـتـ نـم قـقـحـتـلـلـا FTD LINA:

```
<#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 *****
```

اهـمـاـدـخـتـسـ اوـ SNMP لـوـكـوـتـورـبـ لـ FTD ةـرـادـا ةـهـجـاـوـ نـيـوـكـتـ كـنـكـمـيـ،ـ 6.6ـ دـعـبـ اـمـ تـارـادـصـاـ يـفـ

```
<#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
```

يـفـاصـاـ قـقـحـتـ

```
<#root>
```

```
Firepower-module1#
show snmp-server host

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

لُغش ، SNMP م داخ رم اوأ رطس ٰج او نم snmpwalk:

<#root>

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

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

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

رورم ٰك رح تايئا صحا نم ققحتلـا SNMP.

<#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
```

لـ FXOS لـ FPR4100/FPR9300 رورم ٰك رح بـ حامـ سـ لـ

دەھىي .رەصم IP ناونع لەكلى لوصۇ دىيىقت FXOS 9300/4100 ئىلەن SNMP ئىلەن نىوكتل نىكمى زاھىجلا ئىلەن لوصۇلا ئىلەن ئەرداق ئەفييەنىمىلا ئەزەجألا /اتاكبىشلا يەن لوصۇلا ئەمئاقدىن ئىوكت مىسىقى مداخ نەم SNMP تامالۇتساب حامىسىلا نەم دەكأتلا ئىلەن جاتحت كەن .وأ HTTPS وأ SNMP .SNMP رېبى ئىمەرسىلەن مەختىسىملا ئەجأو رېبى ئەيمەل اعلان لوصۇلا ئەمئاقدىن ئىوكت

ئەيمەرسىلەن مەختىسىملا ئەجأو رېبى ئەيمەل اعلان لوصۇلا ئەمئاقدىن ئىوكت

The screenshot shows the 'Platform Settings' tab selected in the navigation bar. On the left, a sidebar lists various system settings like NTP, SSH, SNMP, HTTPS, AAA, Syslog, and DNS. Under 'Access List', there are two sections: 'Ipv4 Access List' and 'Ipv6 Access List'. Both sections have a table with columns: IP Address, Prefix Length, and Protocol. In the Ipv4 section, the second row (IP 0.0.0.0, Prefix 0, Protocol snmp) is highlighted with a red box. In the Ipv6 section, all three rows (IP ::, Prefix 0, Protocols https, snmp, ssh) are highlighted with a red box.

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

(CLI) رەم اۋالا رەطس ئەجأو رېبى ئەيمەل اعلان لوصۇلا ئەمئاقدىن ئىوكت

```
<#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
```

ققحتل

```
<#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

مادختسـا OID Object Navigator

نـاـكـلـاـ تـافـرـعـمـ ةـمـجـرـتـ اـهـلـالـخـ نـمـ كـنـكـمـيـ تـنـرـتـنـ إـلـاـ رـبـعـ ةـادـأـ يـهـ رـيـصـقـ فـصـوـلـعـ لـوـصـحـلـاوـ ةـفـلـتـخـمـلـاـ.

Tools & Resources

SNMP Object Navigator

HOME SUPPORT TOOLS & RESOURCES SNMP Object Navigator

TRANSLATE/BROWSE SEARCH DOWNLOAD MIBS MIB SUPPORT - SW

Translate | Browse The Object Tree

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

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

Translate

Object Information

Specific Object Information

Object	cpmCPUTotalTable
OID	1.3.6.1.4.1.9.9.109.1.1.1
Type	SEQUENCE
Permission	not-accessible
Status	current
MIB	CISCO-PROCESS-MIB ; - View Supporting Images
Description	A table of overall CPU statistics.

ةـلـمـاـكـلـاـ ةـمـيـاـقـلـاـ دـادـرـتـسـاـلـ FTD LINA show snmp-server oid رـمـأـلـاـ مـدـخـتـسـاـ اـهـنـعـ مـاـلـعـتـسـاـلـاـ نـكـمـيـ يـتـلـاـ LINA تـافـرـعـمـلـاـ.

```

<#root>
>
system support diagnostic-cli

firepower#
show snmp-server oid

-----
[0] 10.10.1.10.10.1.1.      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#

```

 يف خم رمألا: ظاحل م.

اهحالص او عاطخألا فاشكتسا

نم ينفلا معدلا زكرم اهاري يتلا آعويش رثكألا SNMP ۋە Cisco:

1. SNMP (SNMP) طيسبلا ۋە كېشلا ۋە لوكوتورب نع عاصقتسىلا ئارجى رىذعتى.
2. FXOS SNMP نع عاصقتسىلا ئارجى رىذعتى
3. اهمادختسا بولطملا SNMP OID مىق ام
4. هيپنتلىسىرلىع لوصحلا نكمى ال SNMP
5. ربىق قارم نكمى ال FMC SNMP
6. SNMP نىوكت رىذعتى
7. SNMP یف FirePower Device Manager نىوكت

(SNMP) طيسبلا ۋە كېشلا ۋە لوكوتورب نع عاصقتسىلا ئارجى رىذعتى FTD LINA

يقيقىحلا Cisco TAC تالاح نم جذومن) ۋە لىكشملا فاصلو:

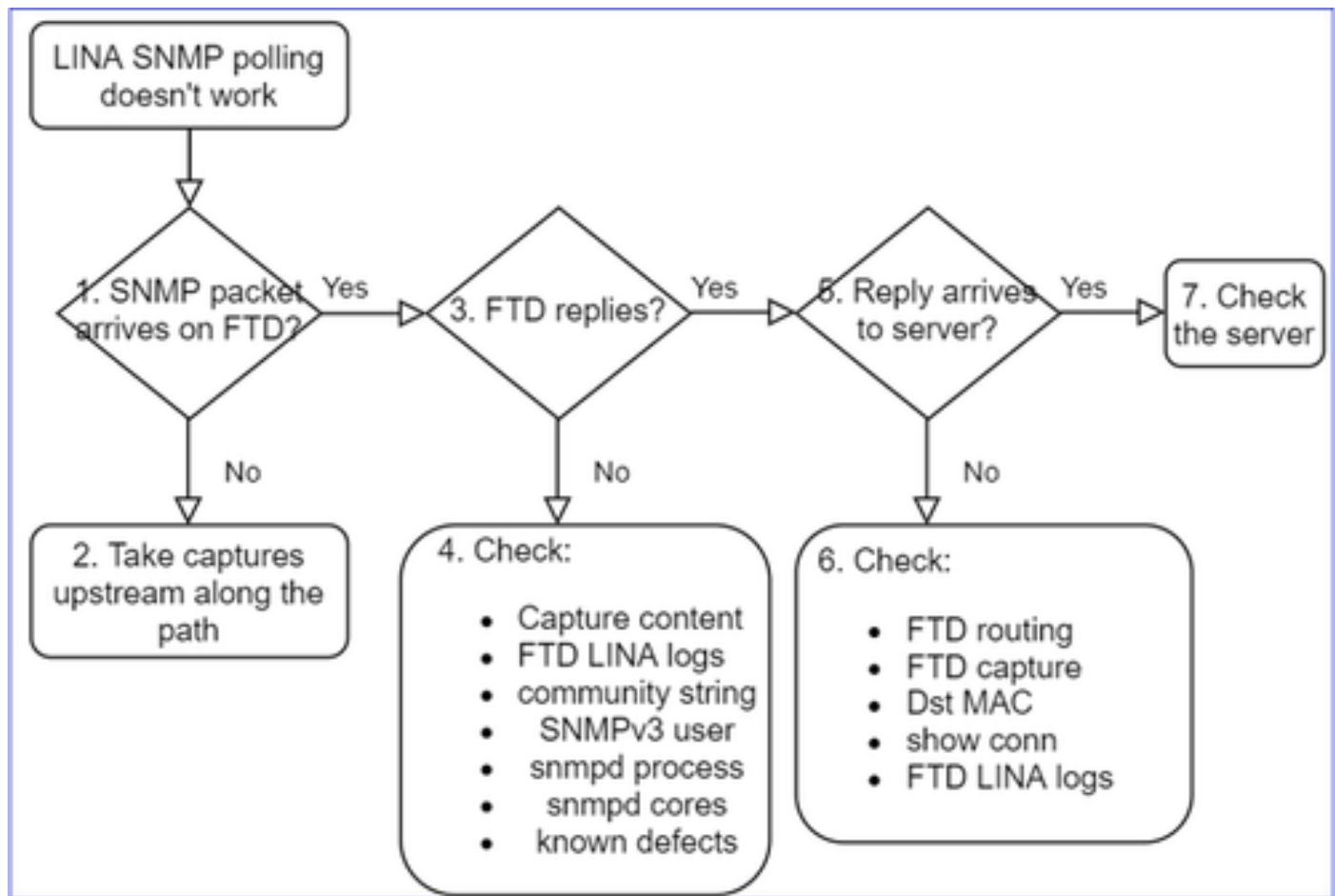
- "SNMP" ربع تانايىبلاب لىچ رىذعتى.
- "SNMPv2" ربع زاھىللا نع مالعتسالا رىذعتى.
- "SNMP" مادختساب ئامحلا رادج ئامحلا دىرن. لەمعى ال جاون، نىوكتلا دعب نكلو

تالكشم

- "3. FTD SNMP v2c رباعي ريداق قبارم لىع نياردىل انىدلىل." اىامحلا رادج لىع SNMP لوكوتورب لمعي ال."

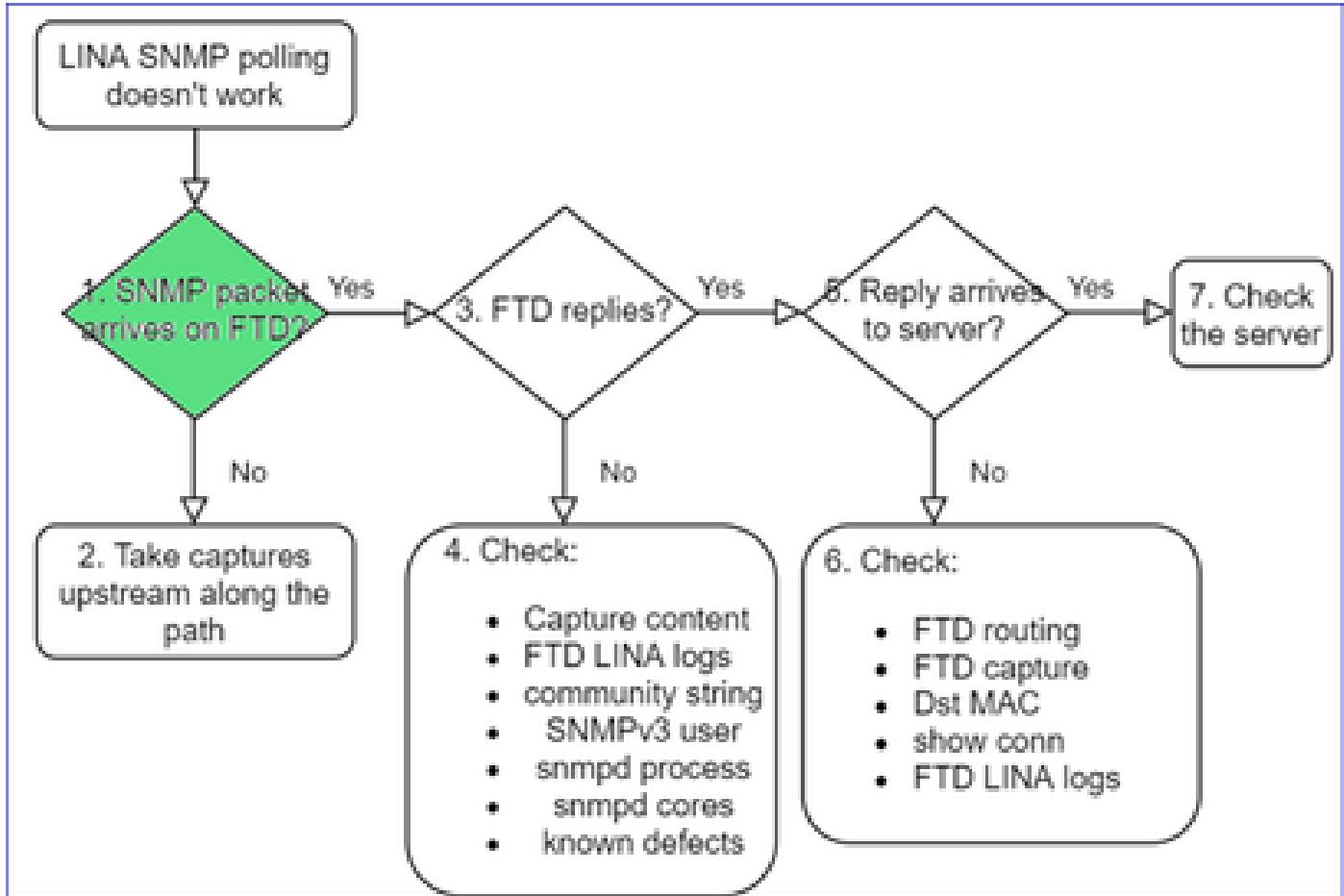
اھالص او عاطخاً فاشكتسأ ئيفيك نأشب ئيصوت

ربيع SNMP عالطتسا تالكشم مل تالكشم مل يبايسنالا ططخم مل اھب ئيصل مع ذه LINA:



قۇمۇتلا

1. FTD لىلەي SNMP ئۆمىزەنلىرىنىڭ لىرىنىڭ



• ةمزح لوصحونم ققحتلل تاطاقتلا نيكمت SNMP.

:ةرادل ئيساسألا ئملكل (6.6 دعب ام رادصا) FTD ئرادا ھجاوىل ع SNMP مدخلتسى

```

<#root>
firepower#
show run snmp-server

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

ةھجوا لا مسلا FTD تانايىب تاھجاويف SNMP مدخلتسى:

```

<#root>
firepower#
show run snmp-server

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

ةرادا ةهجاو لع طاقتل الا FTD:

```
<#root>
>
capture-traffic

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

1
```

تانايب ةهجاو لع طاقتل الا FTD:

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

تانايب ةهجاو ةمزح عبّت (لبق ام) FTD 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)

تانايب ةهجاو ةمزح عبّت (دعّب) FTD 6.6/9.14.1:

```

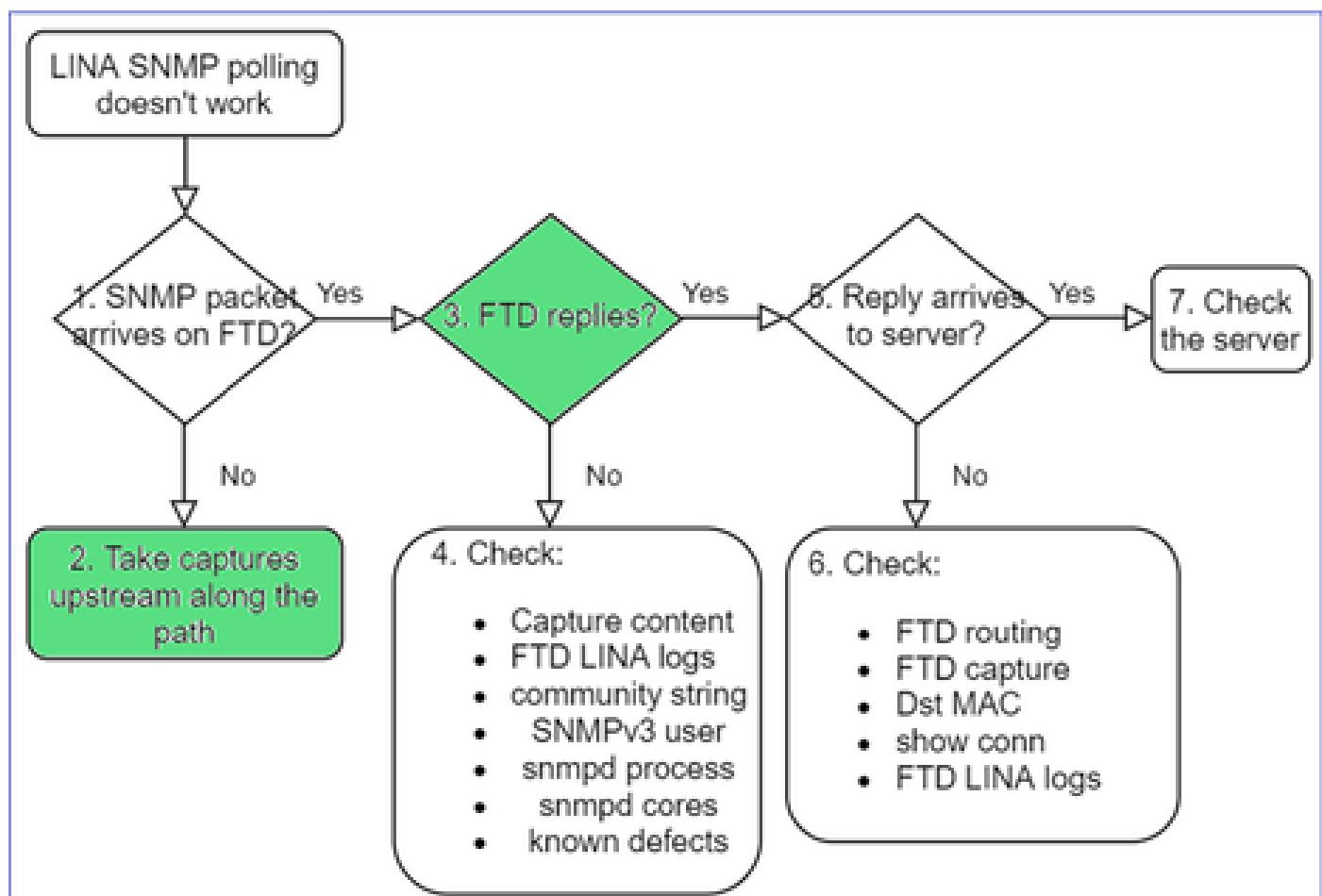
firepower# show capture SNMP packet-number 1 trace
1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.21.100.58255 > 192.168.21.50.161:  udp 39
...
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 9ms
Config:
nat (nlp_int_tap,net201) source static nlp_server_snmp_192.168.21.100_intf4 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)**

لخ دم طاقتلا يف SNMP مزح ئيور مدع ئلاح يف 2.

- راسملا لوطىل ع مداخلا ىل انانايبلالا لاقتنان اتاطاقتلا ذخأ.
- بـ صالحلا حيحصلالا IP ناونع مدخلتسىي SNMP مداخ نأ نم دكأت.
- مـ داخللا ىل انانايبلالا لاقتنان او FTD ۋە جاوايى يذلا (لـدبـمـلـا ذـفـنـمـ) نـم عـدـبـلـا.



3. دودرىت لە FTD SNMP؟

ال مـأ كـيـلـعـ درـيـ FTDـ نـاكـ اذاـ اـمـمـ قـقـحـتـلـلـ

1. FTD ۋە LINA چاواجىخـ طـاقـتـلـا

ردىمىل اذىن مۇزىقىنىڭ 161:

```
<#root>
firepower#
show capture SNMP

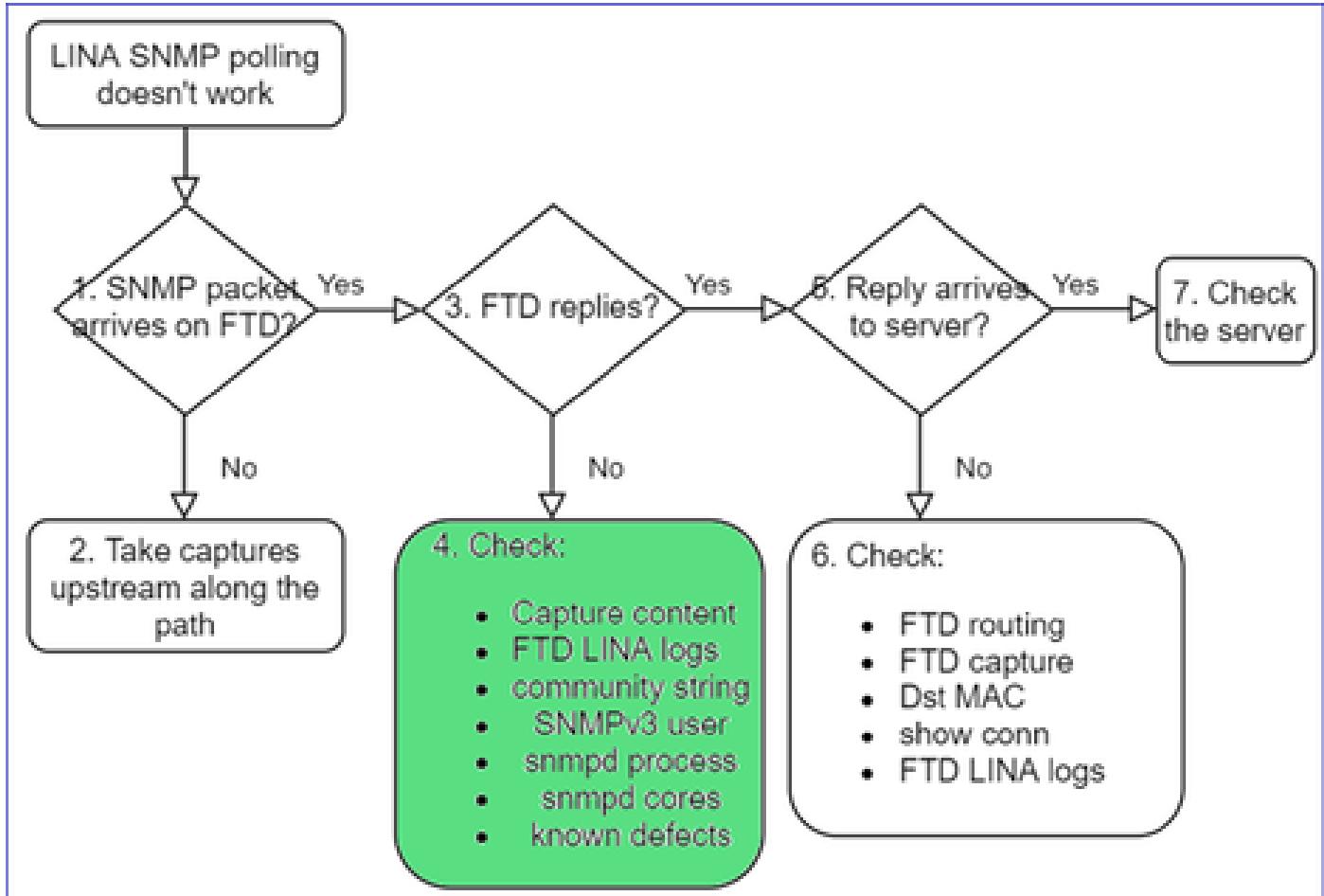
75 packets captured
1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.2.100.58255 > 192.168.2.50.161: udp 39
2: 22:43:39.568329      802.1Q vlan#201 P0 192.168.2.100.58255 > 192.168.2.50.161: udp 39
3: 22:43:39.569611      802.1Q vlan#201 P0 192.168.2.50.161 > 192.168.2.100.58255: udp 119
```

6.6/9.14.1 دىم ئەلە طاقىتلا: دەھاو ئېفاضا طاقىتلا ئەطقىن كىيىدىل، ام تارادصا يەن ئەلە NLP. IP 162.254.x.x نەم ئەطغىض:

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

4 - ئەلە ئەلە تاكىشلار ئېفاضا



أ. قفاؤت لودج نم ققحت، FirePOWER 4100/9300، ةبسنلاب FXOS.

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)*	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
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.		
2.12(0.31)*	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.19(x) (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	7.2.0 (recommended) 7.2.0 7.2.0 7.1.0 7.0.0 6.7.0 6.6.x
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.		
2.11(1.154)*	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
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 9.14(1.15)*. Other releases that are paired with 2.11(1.154)*, such as 9.13 or 9.12, are not affected.		
2.11	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

ب صاخ لـ SNMP مـاـخ تـايـيـاصـحـا نـم قـقـحـتـلـا . بـ

```
<#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
```

جـ لـ اـصـتـا لـ وـدـجـ FTD LINA

ظـاحـاـلـ . نـرـاقـ لـخـدـمـ FTDـ لـاـىـلـعـ طـاقـتـلـالـاـ يـفـ طـبـرـتـنـأـ يـرـيـ الـ نـأـ ظـلاحـ يـفـ اـدـجـ دـيـفـمـ قـقـحـتـلـاـ اـذـهـ

ـهـجـاـوـىـلـعـ SNMPـ نـاـكـ اـذـاـ . تـانـاـيـبـلـاـ ـهـجـاـوـىـلـعـ SNMPـ لـوـكـوـتـورـبـلـ طـقـفـ حـلـاـصـ قـقـحـتـ اـذـهـ نـأـ

ـطـوـرـخـمـ يـأـ عـاـشـنـاـ مـتـيـ الـ ،ـعـدـبـ اـمـ (ـ6.6/9.14.1ـ)ـ ةـرـادـإـلـاـ.

```
<#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
```

دـ مـاظـنـ لـ LINAـ مـاظـنـ

ـهـجـاـوـىـلـعـ SNMPـ نـاـكـ اـذـاـ !ـتـانـاـيـبـلـاـ ـهـجـاـوـىـلـعـ SNMPـ لـوـكـوـتـورـبـلـ حـلـاـصـ قـقـحـتـ اـضـيـأـ اـذـهـ

ـلـجـسـ عـاـشـنـاـ مـتـيـ نـلـفـ ،ـةـرـادـإـلـاـ:

```
<#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)

حیحص لاریغ فیضم ملار ددصمل IP ببس ب SNMP مزح طاقس اب FTD مایق نم ققحتلا.

```
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 community ***** version 2c
```

Mismatch in the src IP

```
firepower# show asp table classify interface net201 domain permit match port=161
Input Table
in  id=0x14f65b193b30, priority=501, domain=permit, deny=false
    hits=8, user_data=0x0, cs_id=0x0, use_real_addr, flags=0x0, protocol=17
    src_ip/id=192.168.22.100, mask=255.255.255.255, port=0, tag=any
    dst_ip/id=192.168.21.100, mask=255.255.255.255, port=161, tag=any, dscp=0x0, nsg_id=none
    input_ifc=net201(vrfid:0), output_ifc=any
```

f. عمتجم (SNMP) ریغ دامتع اتانا ياب

عمتجملا ميقي ئيور كنكمي، طاقتللا تاي وتحم يف (SNMP v1 و v2c):

snmp				
Delta	Source	Destination	Protocol	Length
0.000000	192.168.21.100	192.168.21.50	SNMP	
<				
Frame 3: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) Ethernet II, Src: VMware_85:3e:d2 (00:50:56:85:3e:d2), Dst: a2:b8:dc: 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 201 Internet Protocol Version 4, Src: 192.168.21.100, Dst: 192.168.21.50 User Datagram Protocol, Src Port: 45230, Dst Port: 161 Simple Network Management Protocol version: v2c (1) community: cisco123 data: get-next-request (1)				

g. عمتجملا ئلسلىس و/or SNMP رادصا، لاثملالىبسىلع) حيحس رىغ نىوكت.

عمتجملا لسالس و زاهج لـ SNMP نىوكت نم ققحتلل قرط ئدع كانه:

```
<#root>
firepower#
more system:running-config | i community

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

ىرط قويّة خا:

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

ح اتالاج طاقس ا ASP نم عون

اًلواً FTD . اه طاس او ب اه طاقس ا م ت دق SNMP مزح تناك اذا امم ققحتل لاديفم اًققحت اذه دعي و رب تخا مث (اه طشن لامداخ لاه حفص طاقس ا حسم ا) تادادع لاح سما:

```
<#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

ASP - طاقتلا

ىلع) اه طاقس ا م ت يتلا مزح لاه يفريت اكم (ASP) (اه طشن لامداخ لاه حفص تا طاق تلا رفوت (رواج تلا وأ (ACL) لوصولاب مكحتلا ومئاق، لاثمل لابس:

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

اهنم ققحت مث طاقتلا ا تاي وتحم رب تخا:

```

<#root>

firepower#
show capture

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

```

j. ققحتلا ١ - SNMP (traceback)

ماظنلا رارقتسا يف تالكشم دوجويf كشلا ٰلاح يف آديفم ققحتلا اذه دعى:

```

<#root>

firepower#
show disk0: | i core

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

```

2 - SNMP (رثألا عُبَّتْ) يساسألا

```

<#root>

admin@firepower:~$

ls -l /var/data/cores

-rw-r--r-- 1 root root 685287 Jul 14 00:08 core.snmpd.6208.1626214134.gz

```

يـفـ يـنـفـلـاـ مـعـدـلـاـ زـكـرـمـبـ لـصـتـاـوـرـصـانـعـلـاـ هـذـهـ عـمـجـفـ ،ـيـسـاسـأـلـاـ SـNـMـPـ فـلـمـ تـيـأـرـاـ Cisco:

- FTD TS (وأ) ASA show tech
- يـسـاسـأـلـاـ snmpd تـافـلـمـ

(ثـدـحـأـلـاـ تـارـادـصـإـلـاـ يـفـ طـقـفـ ةـرـفـوـتـمـ وـةـيـفـخـمـ رـمـاـوـاـ هـذـهـ) SـNـMـPـ ءـاطـخـأـ حـيـحـصـتـ:

```

<#root>

firepower#
debug snmp trace [255]

firepower#
debug snmp verbose [255]

firepower#

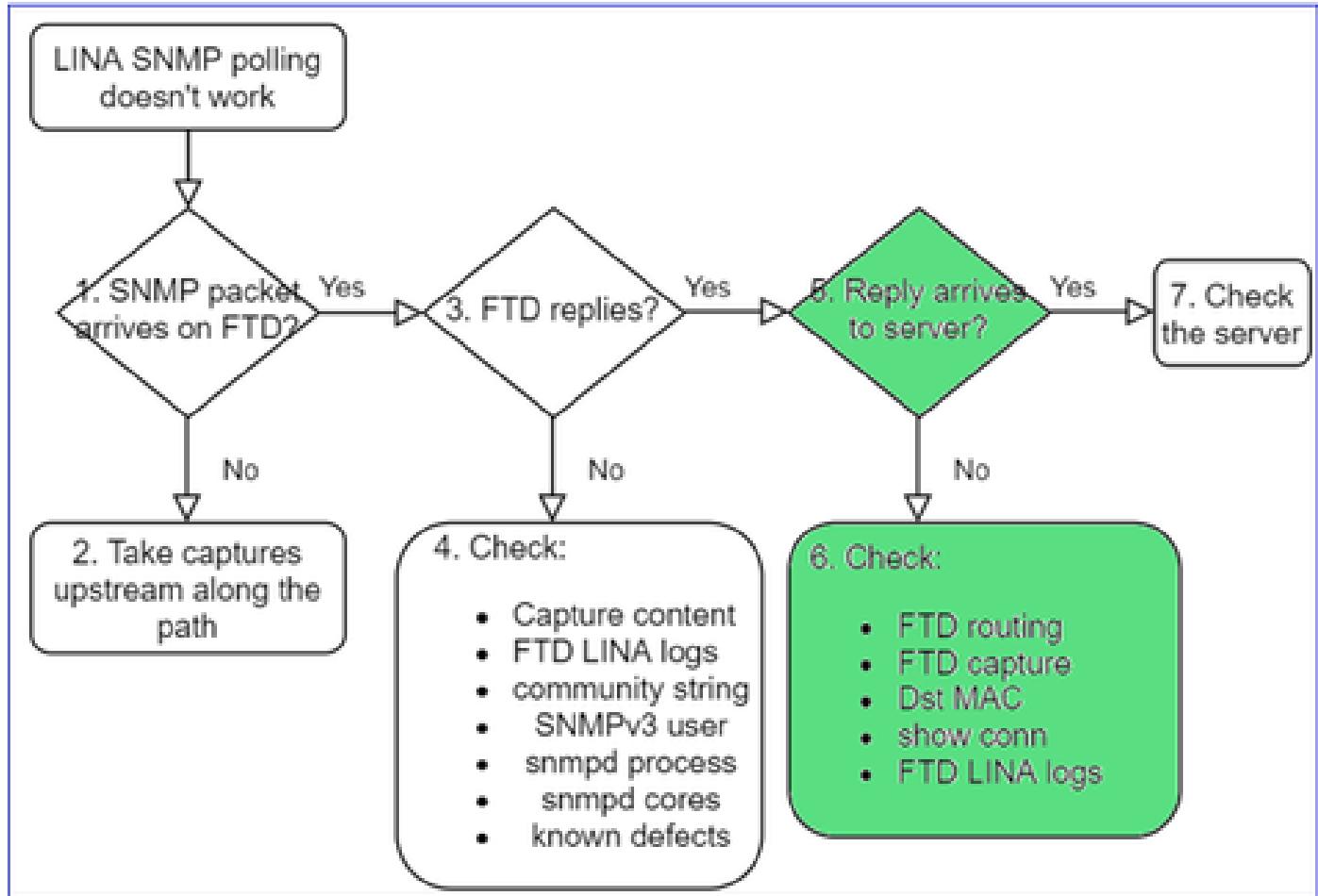
```

debug snmp error [255]

firepower#

debug snmp packet [255]

؟مداخلا ىلإ ئيامحلا رادجل SNMP در لصي له



کلذ نم ققحتف، مداخلا یلصی مل درلا نکل، FTD در لاح یف

اے جو ت FTD

ڦادا ڦاڻا او هڃوٽل ڦبسن لاب FTD:

<#root>

>

show network

تانا يب ٥٥ جا او ٥٧ جو تل ئېس نلاپ FTD LINA:

<#root>

```
firepower#
```

```
show route
```

بـ قـقـحـتـلـا مـاـكـ نـمـ جـوـلـاـ

فـتـدـاـ لـاـخـلـاـ مـاـكـ نـمـ جـوـلـاـ

```
<#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
```

فـتـدـاـ لـاـخـلـاـ مـاـكـ نـمـ جـوـلـاـ

```
<#root>
```

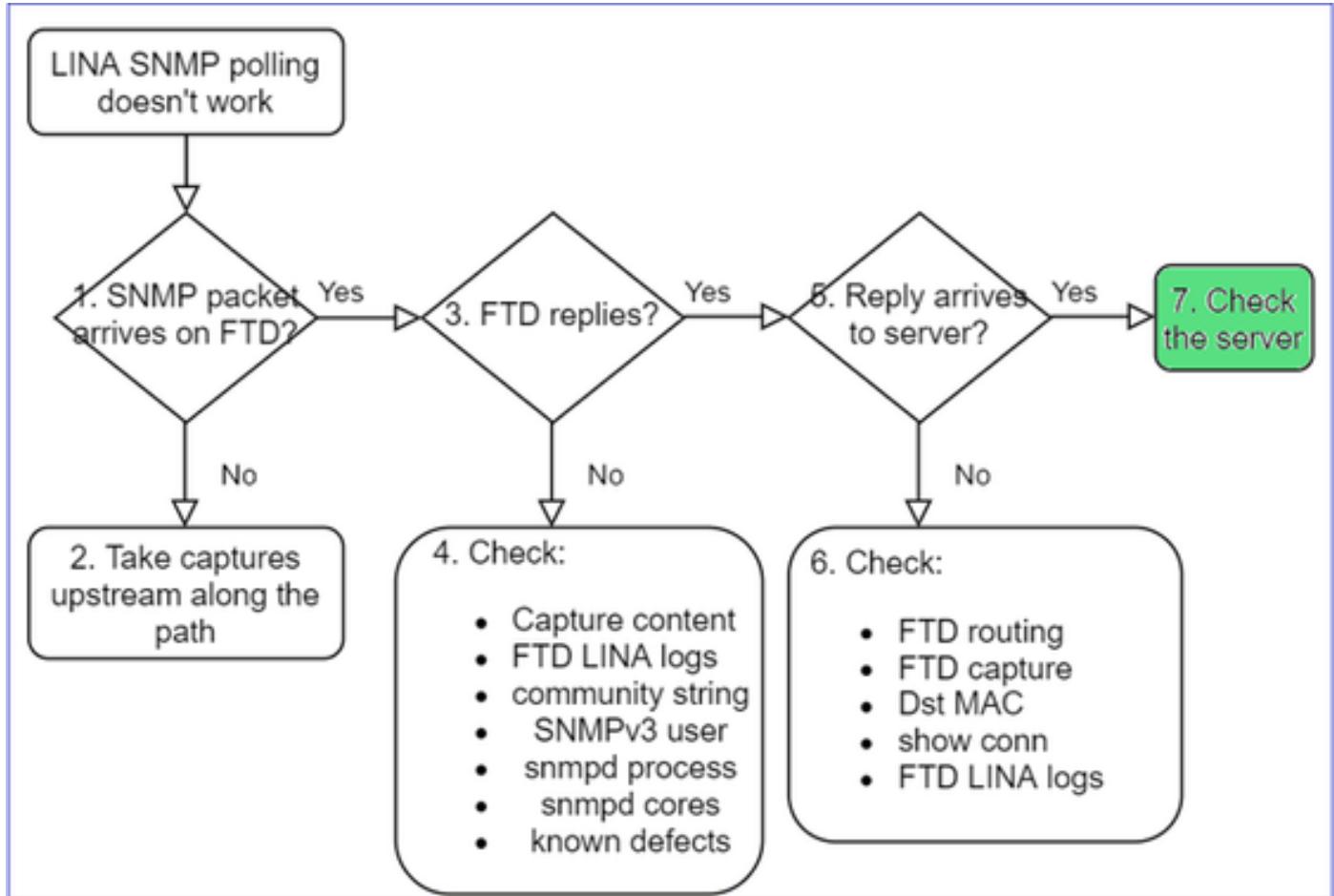
```
firepower#
```

```
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,
```

جـ مـزـحـ رـظـحـتـ / طـقـسـتـ نـأـ لـمـتـحـمـلـاـ نـمـ يـتـلـاـ رـاسـمـلـاـ لـوـطـىـلـعـ ةـزـهـجـأـلـاـ نـمـ قـقـحـتـ

فـتـدـاـ لـاـخـلـاـ مـاـكـ نـمـ جـوـلـاـ



تادادع إلأ نم ققحتل ل طاقتل إلأ تاي وتحم نم ققحت .

مداخلا نيوكت نم ققحت . ب.

ةصاخ فورح نودب ، لاثملالا ليبس ىلع) SNMP عمتجم مسا لي دعت لواج ج).

عافيتس ا مـت اـملـاط ءـاصـقـتـسـالـا رـابـتـخـالـ FMCـىـتـحـ وـأـيـاهـنـ فـيـضـمـ مـادـخـتـسـاـ كـنـكـمـيـ 2ـنـيـطـرـشـلـا:

1. هـنـاكـمـ يـفـ SNMPـ لـاصـتـاـ.
2. زـاهـجـلـاـ نـعـ مـالـعـتـسـالـاـبـ رـدـصـمـلـاـ IPـ نـاـونـعـلـ حـمـسـيـ.

<#root>

admin@FS2600-2:~\$

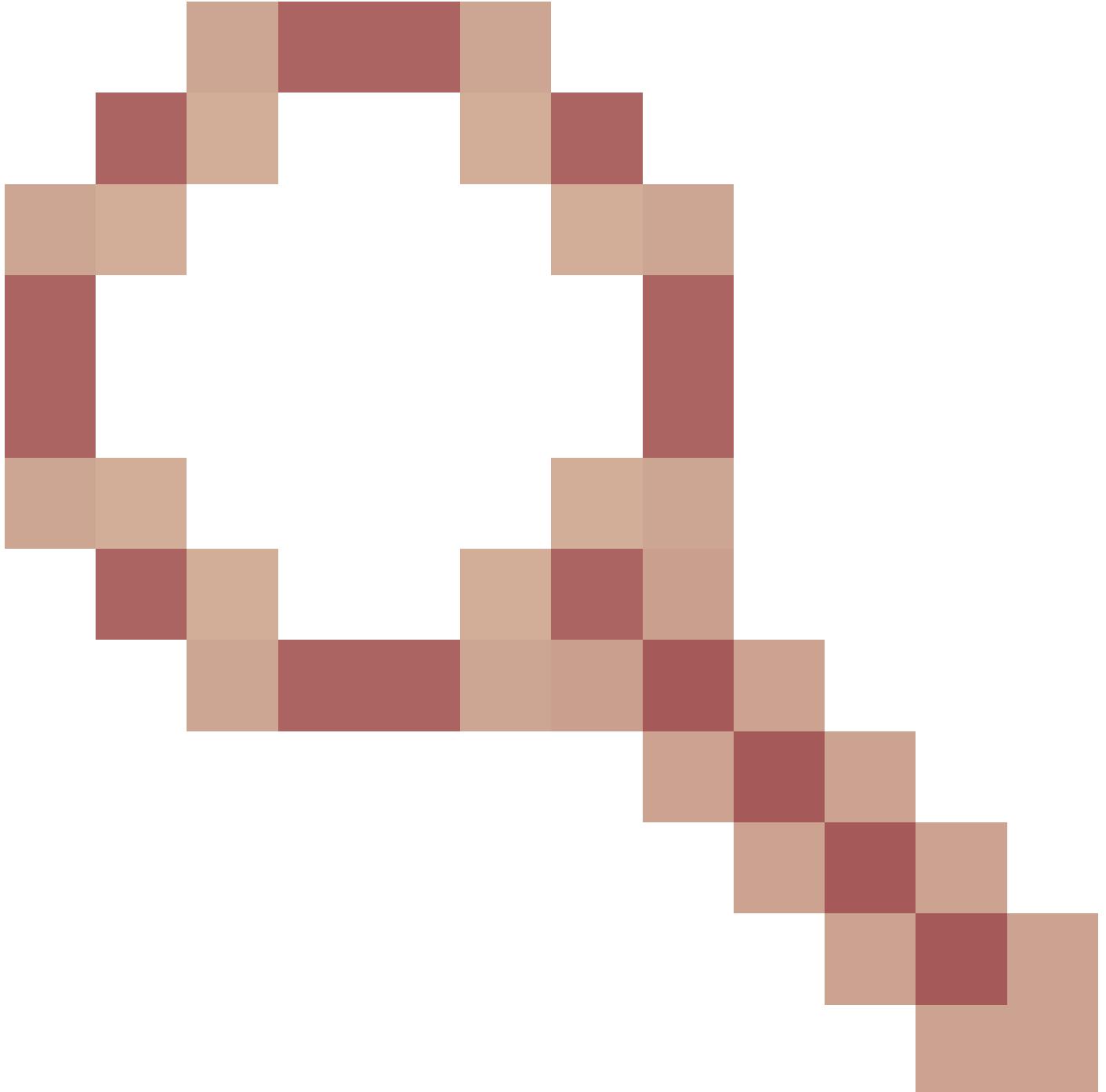
snmpwalk -c cisco -v2c 192.0.2.197

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9.0(1)
```

عالـطـتـسـاـ تـارـابـتـعـاـ SNMPv3

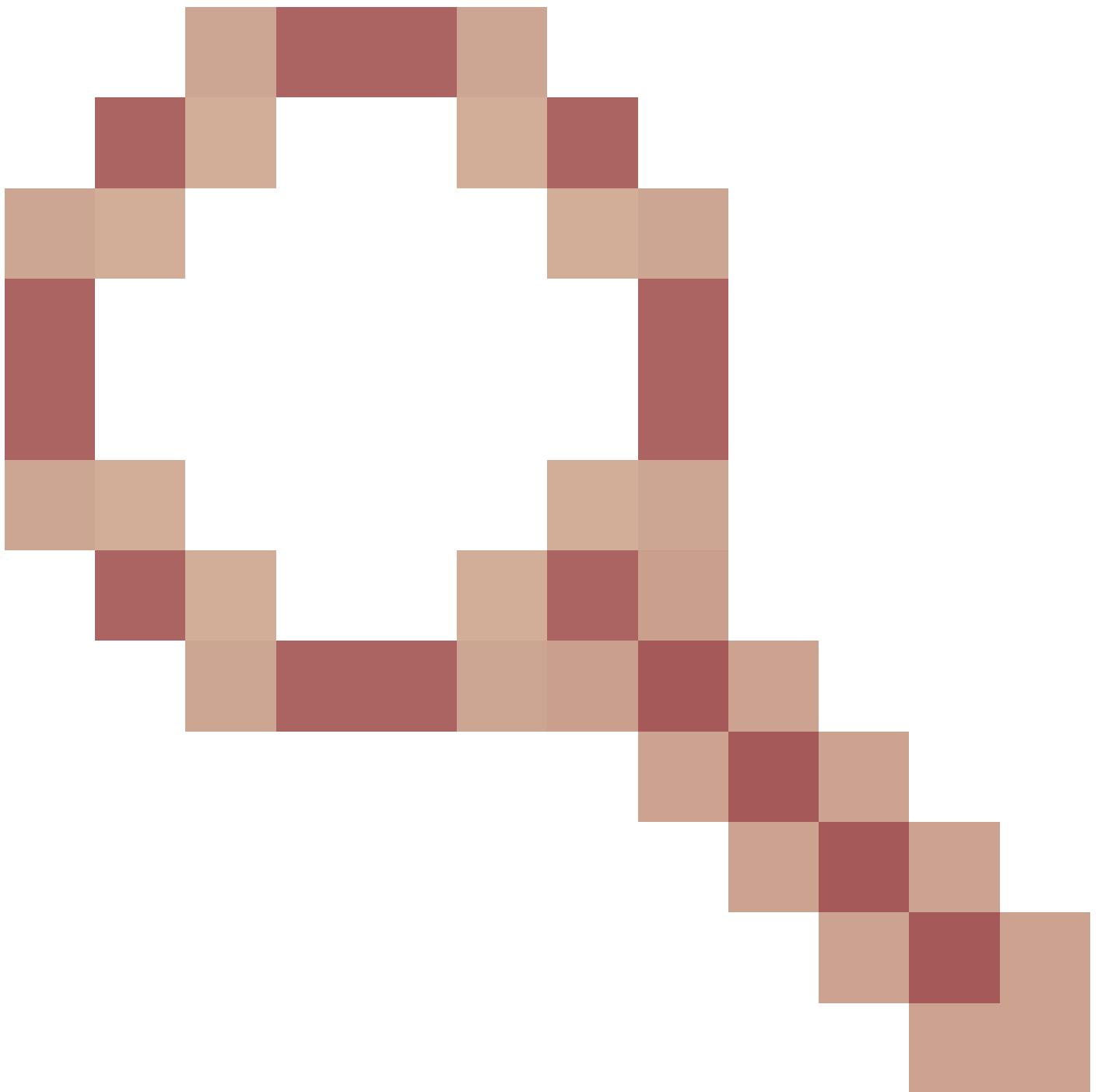
- مـكـحـتـلـاـ ةـفـيـظـوـنـيـكـمـتـ نـمـ دـكـأـتـ .ـيـوقـ رـيـفـشـتـ صـيـخـرـتـ SNMPv3ـ بـلـطـتـيـ :ـصـيـخـرـتـلـاـ يـكـذـلـاـ صـيـخـرـتـلـاـ ةـبـاوـبـ يـفـ رـيـدـصـتـلـاـ يـفـ

- ةدي دج دامتعا تان اي ب / مدخلتسا مادختسا ئلوا حم كنك مي ، احالص او ئاطخالا فاشكتسال
- نم ققحتل او SNMPv3 رورم ئكرح ريفشت كف كنك مي ، ريفشتلا مادختسا مت اذا يف حضوم وامك ئلومحلا <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>
- لثم بويعلا ب كجم انرب رثأت ئلاح يف ريفشتلل AES128 كرابتغا يف عرض Cisco نم ئاطخالا حي حصت فرع [CSCvy27283](#)



ةي صوص خلا تاي مزراوخ مادختسا ب ASA/FTD SNMPv3 عال طتسا لش في نأ نك مي AES192/AES256

Cisco نم ئاطخالا حي حصت فرع لش في [CSCvx45604](#)



SnmpV3 و SHA و AES 192 ميغشت ملا سمل عمو مدع ببساب قباطت زرارم ئىم زىلە

ضرعلا تاجرم رەھەن نەلەف، ئىم زرارخلا قباطت مدع ببساب SNMPv3 لشىف اذا: ئەظحالىم حض او عىش يأ تالجىسىل او

```
firepower# show snmp-server statistics
6 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supp...
    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'

ةلأجل ا تاسارد – SNMPv3 نع مالعتس إلأ تارابت عا

1. SNMPv3 snmpwalk - ظرفی وی رانی س

<#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 9.0(1)SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2315

نظام مراقبة كل آدرس (snmpwalk) طاقي لـ `if`

```
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
```

يادع ریغ عیش يأ طاقتلاا فلم ضرعی ال

```

` Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  > msgAuthoritativeEngineID: 80000009feca41e36a96147f184553b777
    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
` msgAuthenticationParameters: 79ee0d463313558f4529954f
  > [Authentication: OK]
    > [Expert Info (Chat/Checksum): SNMP Authentication OK]
      [SNMP Authentication OK]
      [Severity level: Chat]
      [Group: Checksum]
  msgPrivacyParameters: 714e78d6bc292c88

```

2. SNMPv3 snmpwalk - ریفشت لالش ف

ۃلہم کانہ #1: حیملت:

<#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

دھاو درل او تابل طلا نم دیدعال کانہ 2: مقرحیملت:

```
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
```

ریفشت کف لش ف 3: مقرحیملتل

```
> 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: 0000000197eaef1a
  < msgData: encryptedPDU (1)
    < encryptedPDU: 452ee7ef0b13594f8b0f6031213217477ecb2422d353581311cade539a27951af821524...
      < 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]
```

لئاسر لیلحت يف أطخ" نع اثحب ma_ctx2000.log فلم نم ققحت 4. مقرحیملتل "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
```

ب ۃصالح ثادحألا ma_ctx2000.log فلم ضرعی. ریفشت أطخل یوق حیملت ScopedPDU SNMPv3 طقف!

3. SNMPv3 snmpwalk - ۃصالصملالش ف

ۃصالصملالش ف 1: مقرحیملتل

```
<#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)
```

دو درل او تابل طلا نم ديدعلا كانه 2: مقرحيم لتل

```
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
```

ئطاخلا نيوكتلاتا تاذ ۋەمىز: مقرحيم لتل

```
> 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]
```

"قىداشىلا لشىف" لىاسىرىلىع عالطاالل ma_ctx2000.log فلم نم قىقحت 4. مقرحيم لتل:

```
<#root>
>
expert

admin@firepower:~$
tail -f /mnt/disk0/log/ma_ctx2000.log

Authentication failed for Cisco123
Authentication failed for Cisco123
```

نۇع ئاصقىتسالا ئارجا رىذعنىي FXOS SNMP

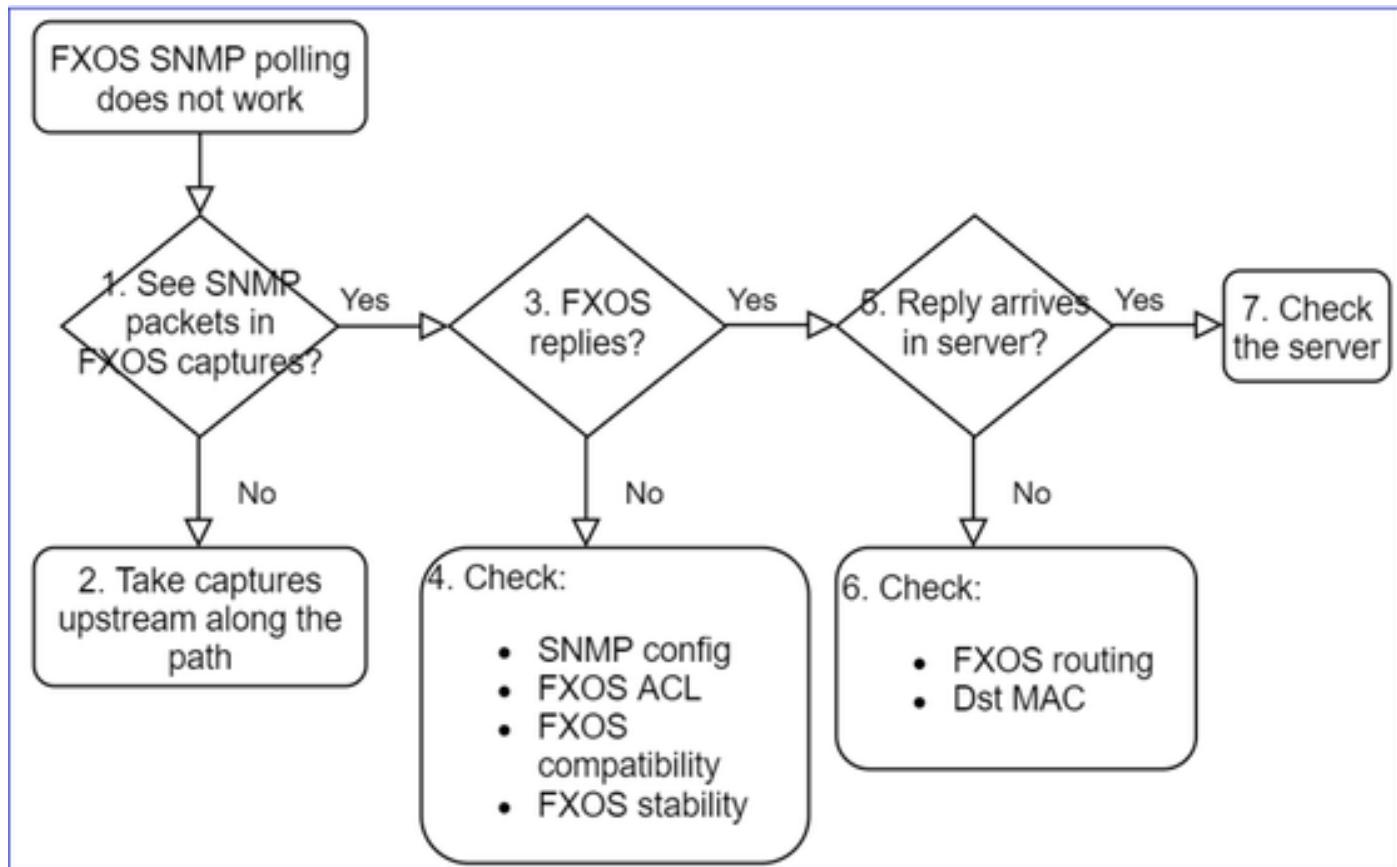
قىيقىچىلا Cisco TAC تالاح نم جذومن) ۋېلىكىشملا فاصلو:

- FXOS، SNMP رادصى نۇع مادختساب مالعىتسالا دىنۇع. FXOS، SNMP يىطعىي "لەئىطاخ رادصى" دىنۇع.
- "تاجىخملە مەھى بىعىسىلە نم نوکىي" عەمەتجم دادعا رىذعنىي."
- "snmp ئىلىع FXOS FTD4115."
- "ام دىنۇع ۋېلىكىشملا فاصلو، يىطايىتحالا ئىامەحلى رادج ئىلىع 2.9 نم FXOS ئىقىردى دىنۇع."
- "ربۇ تامۇلۇم يىأ لابقتىسالا لواحنى SNMP."
- "snmpwalk ئىلىع 4140 fxos سفن ئىلىع لەمعىي ھەنكىلە."

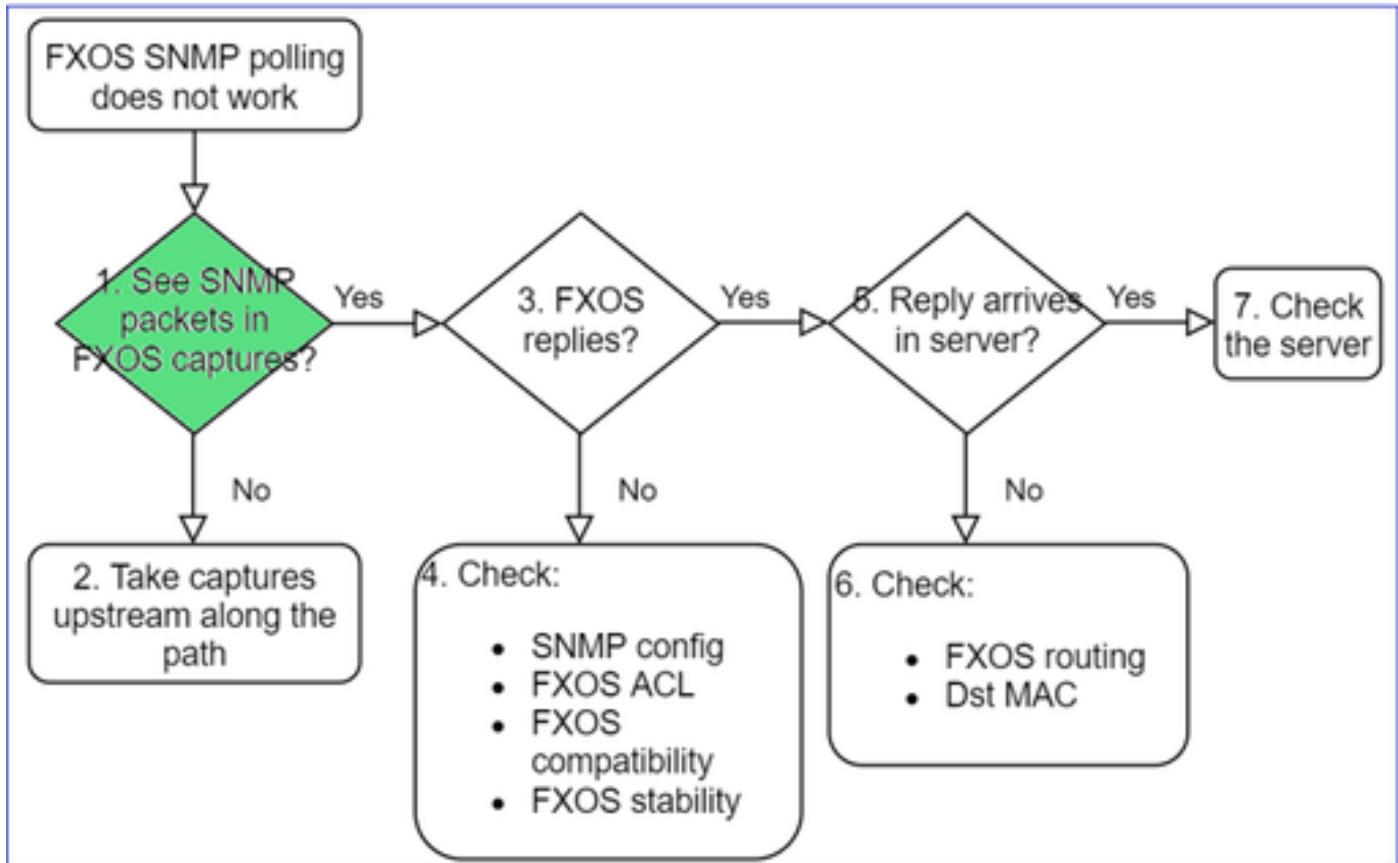
- "کل ذان نکمی اال نکل، FPR4K FXOS ىلع SNMP مداوخ نم ًامداخ 25 ًفاضا ديرن." "لکش ملا امه اس يل عمتجمل او لوصولا."

احوال ص اور عاطخآل افashکتساپ یص وم

FXOS لکاشم عالطتساب ۆصاخلا یبایسنالا ططخملاءاطخأ فاشكتسالا ۆيلمعلا یه ٥ ذه
SNMP اوەحالصا:



تاطقل يف SNMP مزح ىرت لـ FXOS؟



FPR1xxx/21xx

- زاھجلا عضو لکیه ریدم دجوی ال FPR1xxx/21xx یف.
- ةرادلإا ڈھج او نم FXOS جمانرب نع راسفتسالا کنکمی.

<#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

- يدع اقل ا لكيل ا طا قتل ال Ethalyzer CLI مدخل مادا FirePower 41xx/93xx.

```
<#root>

firepower#
connect fxos

firepower(fxos)#
ethalyzer local interface mgmt capture-filter "udp port 161" limit-captured-frames 50 write workspace

firepower(fxos)#
exit

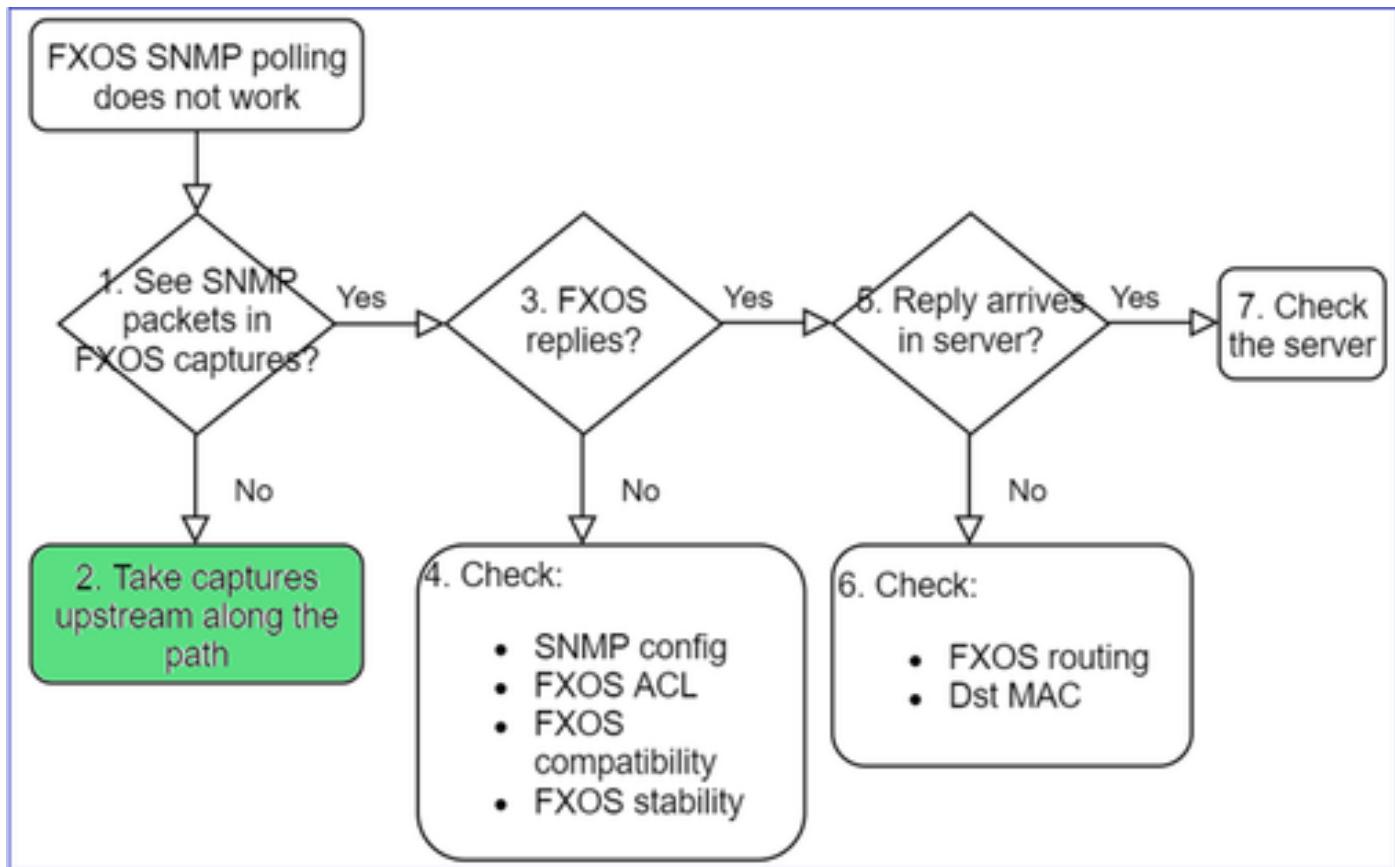
firepower#
connect local-mgmt

firepower(local-mgmt)#
dir

1
11152 Jul 26 09:42:12 2021 SNMP.pcap
firepower(local-mgmt)#

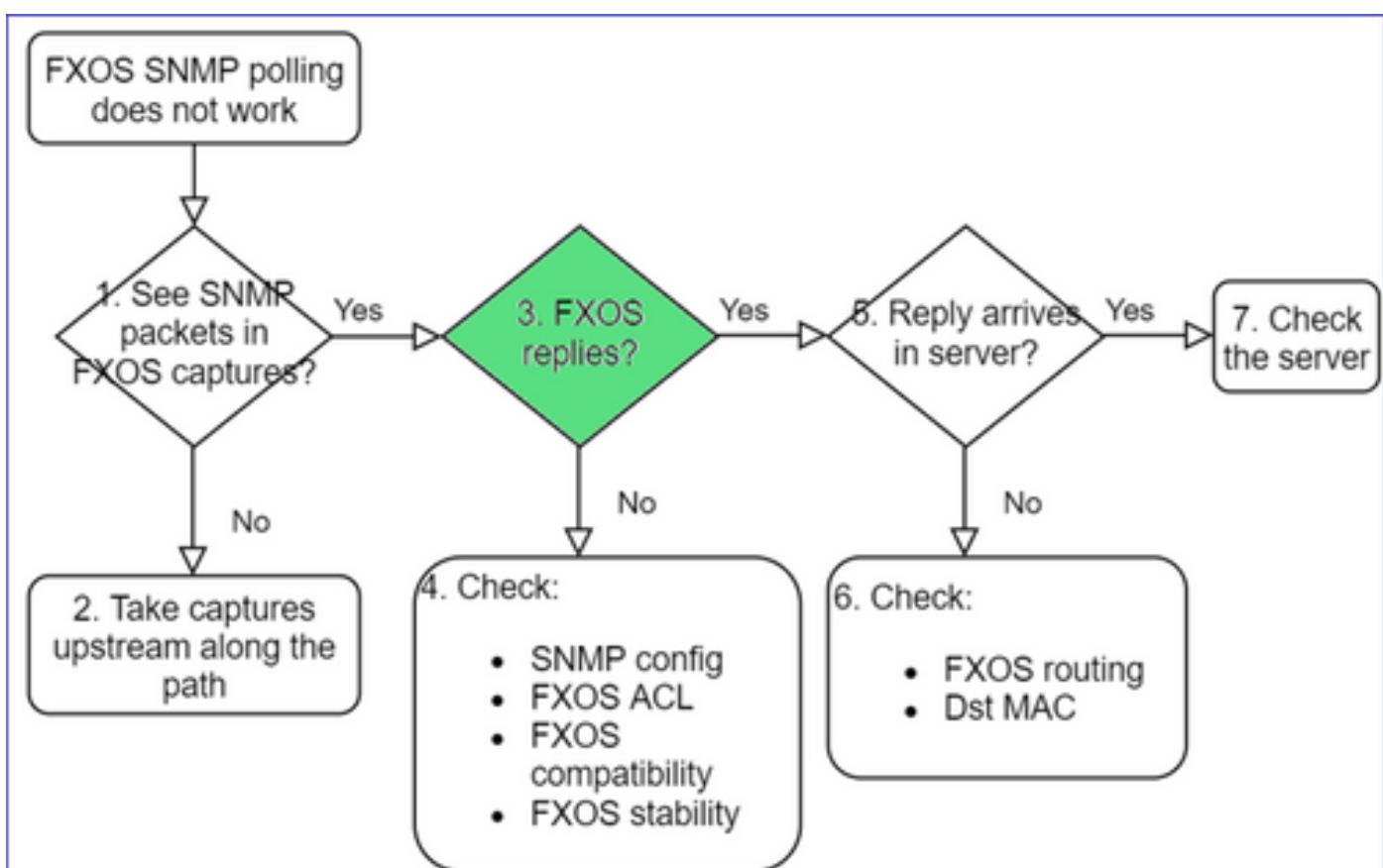
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. FXOS؟ مزح دجوت ال ا طا قتل اي ف FXOS؟



• راسمل ا لوط ىلع مداخلا ىل ا تانايبل ا لاقتنا تاطاقتلا ذخأ

3. درت له FXOS؟



- ## • یفی ظو ویرانیس

```
<#root>

>

capture-traffic

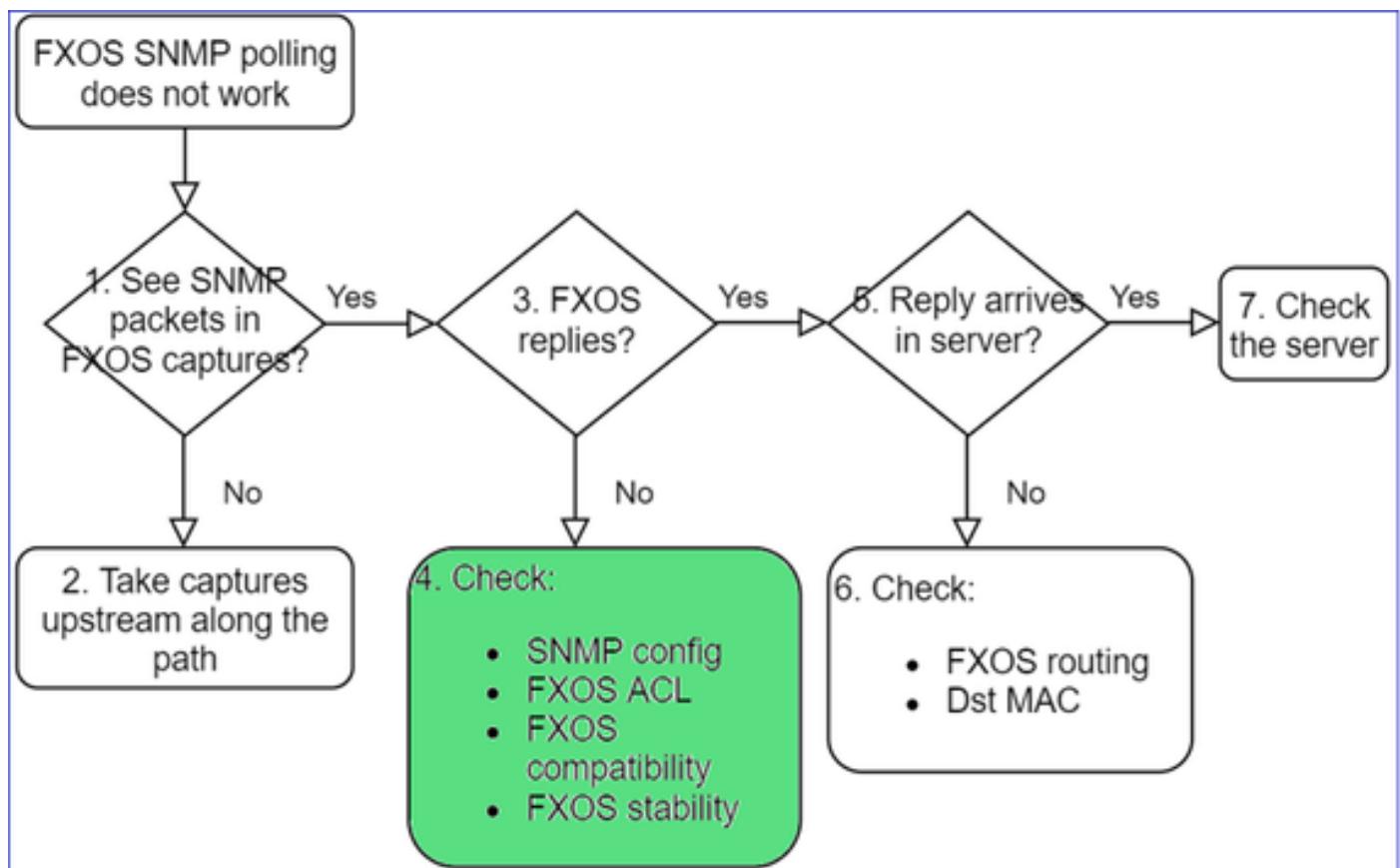
...

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 درت ال



ءيضاً ققحت تايلمع

- (رم أوّلا رطس ۃھجاو و مدخلت سملاء ۃھجاو نم) SNMP نیوکت نم ققحت

<#root>

```

firepower#
scope monitoring

firepower /monitoring #
show snmp

```

```

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

```

- ،لاثملال ليبس ىلع) ةصالحأا فرحأا عم لماعتلا دنبع ًارذح نك " \$" :

```

<#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

```

- SNMP v3، ا ئىلإ مدخلتسا ئىلإ ئابSNMP show snmp-user [detail]
- FXOS قفاوت نم ققحتلا

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

4. درمدع ئالج يف FXOS

تادادع نم ققحت FXOS SNMP:

```

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

```

Total requests (polling)

Bad community requests (v2c)

Total replies

Traps generated

- ةمظنألا يلע طقف قبطنى اذهو FXOS (ACL) لوصولاييف مكحتلا ةممياق نم ققحت . FPR41xx/9300.

تابلطلا يرتس، FXOS (ACL) لوصولاب مكحتلا ةممياق ةطساوب رورملاب كرح رطح مت اذا دودريأ يرت ال نكلو:

<#root>

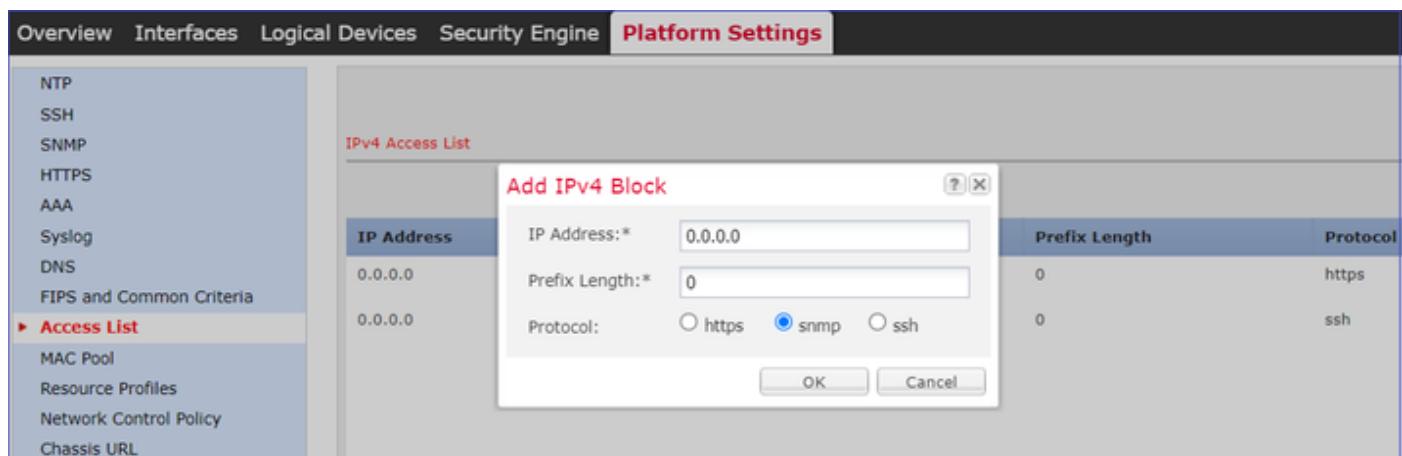
```

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

```

مدختسملا ةهجاو نم FXOS (UI):



رم اوألا رطس ةهجاو نم FXOS ىلإ لوصولاب مكحتلا ٖمئاق نم ققحتلا كنكمي امك:

```
<#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
```

- ىلع طقف قبطنی (طقف مزح) SNMP ءاطخأ حيحصت 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
```

- ئياغلل بەسم اذه ءاطخألا حيحصت جارخ - (لكل) SNMP ءاطخأ حيحصت.

```
<#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
```

- FXOS لوكوتورب ئەلص تاڭ ئا طاخأ يأ دوجو نم قّقحت SNMP:

```
<#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
```

- snmpd نم ئىس اسأ تاقب ط يأ كانه تناناك اذى امم قّقحت:

ىلۇع FPR41xx/FPR9300:

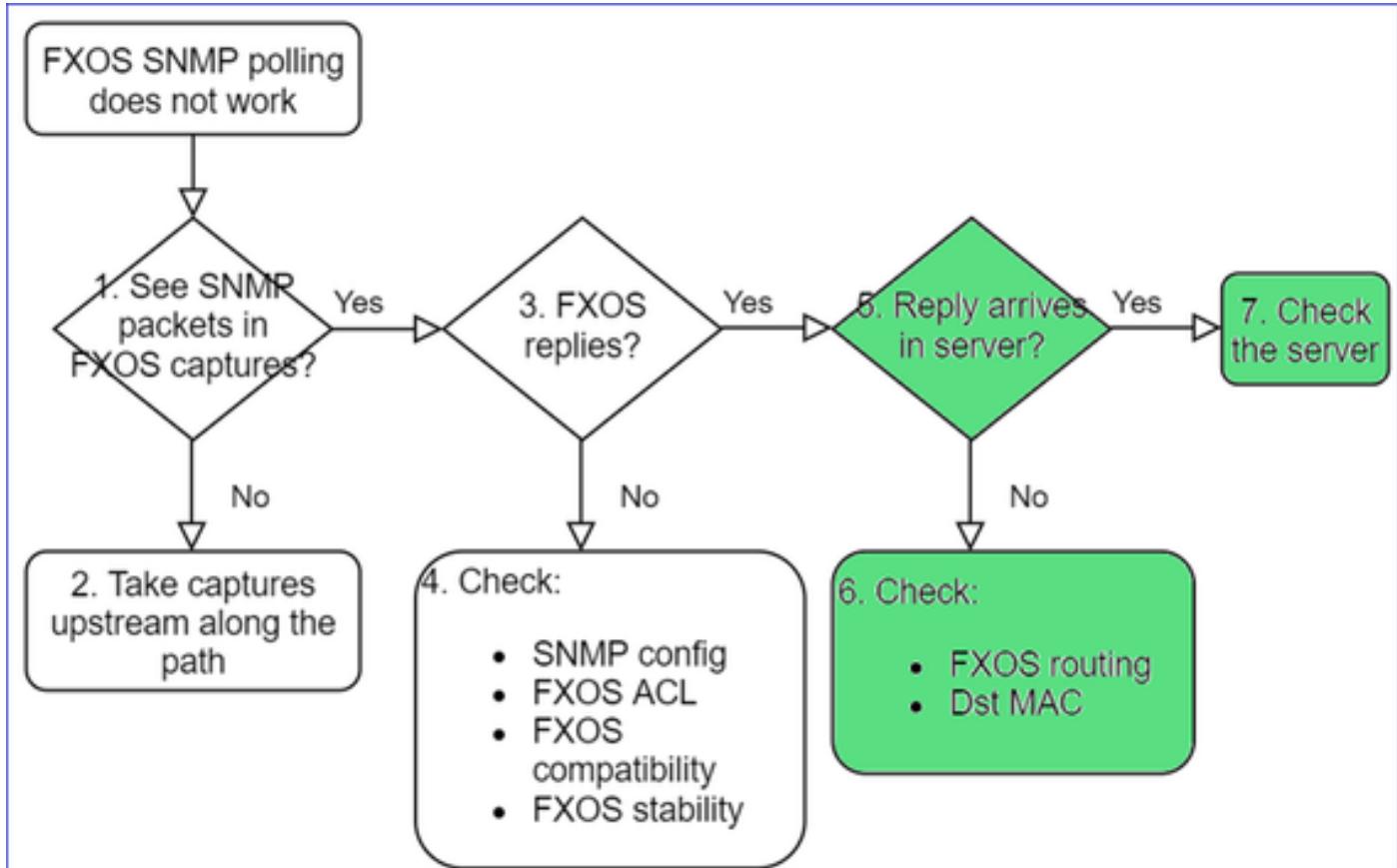
```
<#root>  
  
firepower#  
  
connect local-mgmt  
  
firepower(local-mgmt)#  
  
dir cores  
  
1 1983847 Apr 01 17:26:40 2021 core.snmpd.10012.1585762000.gz  
1 1984340 Apr 01 16:53:09 2021 core.snmpd.10018.1585759989.gz
```

ىلۇع FPR1xxx/21xx:

```
<#root>  
  
firepower(local-mgmt)#  
  
dir cores_fxos
```

FXOS ئەللا تاقب طلا عّمچىف، snmpd نم ئىس اسأ تاقب ط يأ تىيار اذى Cisco نم (TAC) ئىنفلە دەعاسىملا زىرمۇ لىصت او اھحالص او ئاطاخألا فاشكىتسالا.

5. SNMP مداخ يىف SNMP ئەلصىي لە.



- هیجوت نم ققحتل FXOS

اذه جارخإلا نم FPR41xx/9300:

<#root>

firepower#

show fabric-interconnect

Fabric Interconnect:

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

- درلل ةهجاولاب صاخلا MAC ناونع نم ققحتل او pcap ريدصتب مف ، ةطقـل ذـخ
- (كلـذـىـلـاـ اـمـ وـقـيـبـ طـتـلـاـ وـنـيـوـكـتـلـاـ وـطـاـقـتـلـاـ اـتـايـلـمـعـ) SNMP مـداـخـ نـمـ قـقـحـتـ ،ـأـرـيـخـأـوـ

امـيـقـ اـمـ مـادـخـتـسـاـ بـوـلـطـمـلـاـ SNMP OIDـاـ

فـاصـواـ Cisco TACـاـ قـيقـحـلـاـ تـالـاحـ نـمـ جـذـومـنـ (ـلـكـشـمـلـاـ فـاصـواـ):

- كلـلـ SNMPـ لـوكـوـرـبـلـ OIDـاـ تـافـرـعـمـ مـيـدـقـتـ يـجـرـيـ Cisco Firepowerـ "ـصـارـقـأـلـاـ وـةـرـكـاـذـلـاـ وـةـيـسـاسـأـ ةـيـزـكـرـمـ ةـجـلـاعـمـ ةـدـحـوـ"
- زـاهـجـ ئـلـعـ ةـقـاطـلـاـ دـادـمـاـ ةـلـاحـ ةـبـقـارـمـلـ ـهـمـادـخـتـسـاـ نـكـمـيـ ASA 5555ـ؟ـ"

- "FPR 2K و FPR 4K . SNMP OID لكيه بلج ديرن" يدعاقل اقلع."
 - "ASA ARP . عالطتس الا ديرن" نع ئركاذ نيزختلا تقوفملا لـ."
 - "جاتحن اجا لـ SNMP OID ئفرعم ئىل رىظنل BGP ."

SNMP OID ميقات لروتاعل

FirePower مل سمتا تادن تامولعم لوح تافرعم OID SNMP یلع ۆزهجأ:

- - بـ صـاـخـلـاـ لـوـكـوـتـورـبـ ظـقـارـمـلـلـ يـنـقـتـلـاـ دـنـتـسـمـلـاـ Firepower Threat Defense (FTD) Cisco:

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

- Cisco نم FXOS MIB لىل دلا Firepower 4100/9300 جرملا يع لىل دلا

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

- FXOS ميسيس الـ OID نع ثحبلا ةيفيك

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

- (ASA/LINA) قـقـحـتـلـاـ نـمـ قـقـحـتـلـاـ تـافـرـعـمـ نـمـ ةـهـجـاوـ رـطـسـ اـوـاـلـاـ

```
<#root>

firepower#  
  
show snmp-server ?  
  


|            |      |
|------------|------|
| engineID   | Show |
| group      | Show |
| host       | Show |
| statistics | Show |
| user       | Show |

  
firepower#  
  
show snmp-server o  
  
      <- hidden options  
[1] .1.10.1.1.10.  
[2] .1.10.1.1.1.1  
[3] .1.10.1.1.1.1  
[4] 1.10.1.1.1.1
```

- SNMP Object Navigator نم قّقحت، OID لوح تامولعملانم دیزم یلع لوصحلل

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

- FXOS (41xx/9300) نیزه لیغشتپ مق، FXOS رم او رطس ٥٥٥ جاو نم رم ملأا نیذه لیغشتپ مق،

```

<#root>

FP4145-1#
connect fxos

FP4145-1(fxos)#
show snmp internal oids supported create

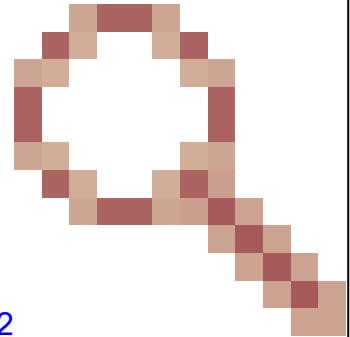
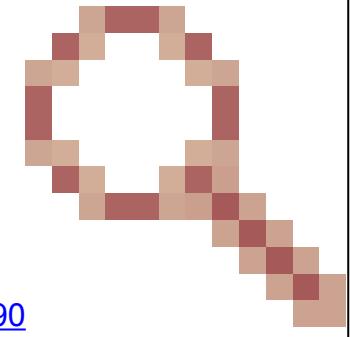
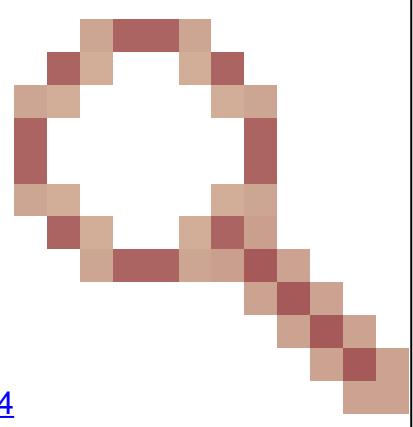
FP4145-1(fxos)#
show snmp internal oids supported

- SNMP All supported MIB OIDs -0x11a72920
Subtrees for Context:
ccitt
1
1.0.88010.1.1.1.1.1 ieee8021paeMIB
1.0.88010.1.1.1.1.2
...

```

ةعئاشلا OID تافّرعمل عيرسلأ عجرملأ

تابلطتملا	OID
وّجلاعملأا وّدح وّيذكرملأ (LINA)	1.3.6.1.4.1.9.9.109.1.1.1
وّجلاعملأا وّدح وّيذكرملأ (Snort)	1.3.6.1.4.1.9.9.109.1.1.1 (FP >= 6.7)
وّركاذلأا (LINA)	1.3.6.1.4.1.9.9.221.1.1
وّركاذلأا (Linux/FMC)	1.3.6.1.1.4.1.2021.4
رفاوّتلا تامولعم يلاعلأ (HA)	1.3.6.1.4.1.9.9.491.1.4.2
عيمجّتلا تامولعم	1.3.6.1.4.1.9.9.491.1.8.1
وّVPN تامولعم	وّكبشب وّصالخا وّكبشلأ تاسلح RA-VPN: 1.3.6.1.4.1.9.392.1.3.1 (7.x)

	<p>ةكبشب ةصاخلا ةكبشلا ومدختسم RA-VPN: 1.3.6.1.4.1.9.392.1.3.3 (7.x)</p> <p>ةورذ تاسلجم RA-VPN: 1.3.6.1.4.1.9.392.1.3.41 (7.x)</p> <p>ةكبشتاسلجم S2S VPN: 1.3.6.1.4.1.9.392.1.3.29</p> <p>VPN S2S: 1.3.6.1.4.1.9.392.1.3.31</p> <p>- حيملي: Firepower# show snmp server oid معن ، معن</p>
ةلاح BGP	 <p>ن姆 عاطخألا حيحصت فرع ميف Cisco CSCux13512 : عالطتسال SNMP ةفاضا</p>
صيخرت FPR1K/2K يكلزا ASA/ASAv	 <p>ENH نم عاطخألا حيحصت فرع Cisco CSCvv83590 : ASAv/ASA جاتحي SNMP OID يكلزا FPR1k/2k</p>
OID SNMP تافرع ةانقل لـ Lina ىلع ذفنمل ىوتسم FXOS	 <p>ن姆 عاطخألا حيحصت فرع Cisco CSCvu91544 : ذفنمل ةانقل ةهجا تايئاصح ال OIDs Lina SNMP نم ۆزهجأ مع د FXOS</p>

(ثدحألاو مكحتلا ةدحول) FMC 1600/2600/4600 تافاضا

تابل طتملا	OID
ةحورملالا ةلاح ةديصم	1.3.6.1.4.1.9.9.117.2.0.6 1.3.6.1.4.1.9.9.117.1.4.1.1.<index> لمعت ال ةحورملالا - 0 - ليغشتلا ديق ةحورملالا - 1
ةرارح ةجرد ةديصم ةجلاعملالا ةدحو ةيزكرملالا (CPU) ديوزتلالا ةدحو/ (PSU) ةقاطلاب	1.3.6.1.4.1.9.91.2.0.1 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<index>.1 1.3.6.1.4.1.9.91.1.1.1.4.<index>
PSU ةلاح ةديصم	1.3.6.1.4.1.9.9.117.2.0.2 OperStatus: 1.3.6.1.4.1.9.9.117.1.1.2.1.2.<index> AdminStatus: 1.3.6.1.4.1.9.9.117.1.1.2.1.1.<index> ةقاطلاب ديوزتلالا ةدحو دوجو فاشتكا متيم - 0 - قفاص، ةقاطلاب ديوزتلالا ةدحو دوجو فاشتكا - 1

هـيـبـنـتـ لـئـاسـرـ لـعـلـوـصـ حـلـاـ نـكـمـيـ الـ

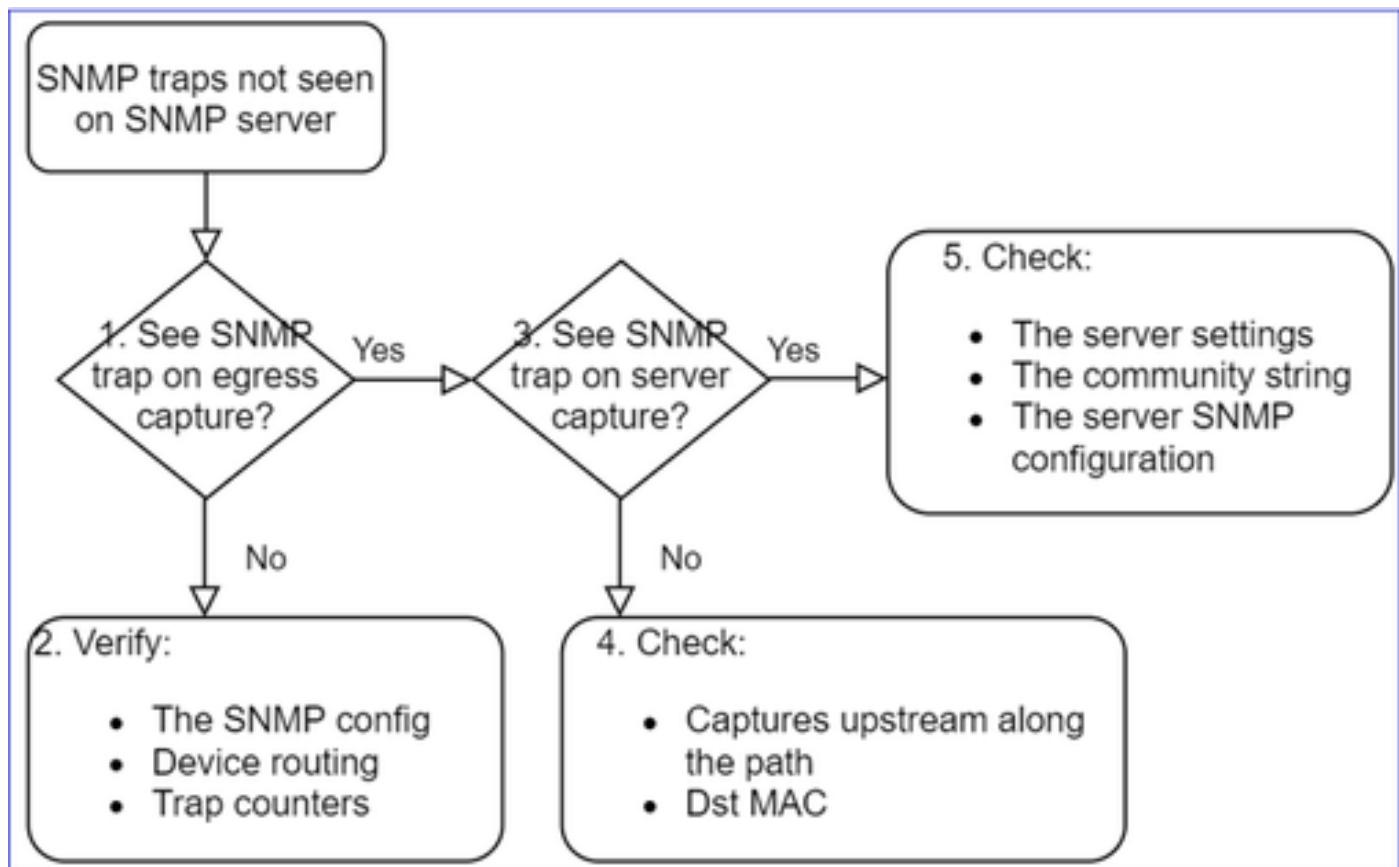
ـهـيـقـحـلـاـ Cisco TACـ تـالـاحـ نـمـ جـذـومـنـ)ـ ةـلـكـشـمـلـاـ فـاصـوـاـ:

- ـ بـ صـاخـلـاـ هـيـبـنـتـ ةـلـاسـرـ يـأـ SNMPv3ـ FTDـ لـسـرـيـ الـ "ـ SNMPـ."
- ـ هـيـبـنـتـ لـئـاسـرـ FMCـ وـ FTDـ نـمـ لـكـ لـسـرـيـ الـ "ـ SNMPـ."
- ـ اـنـبـجـوـ FXOSـ لـ اـنـبـ صـاخـلـاـ FTDـ 4100ـ ئـلـعـ SNMPـ نـيـوـكـتـبـ اـنـمـقـ دـقـلـ "ـ هـيـبـنـتـلـاـ لـئـاسـرـ لـاسـرـاـ اـمـهـيـلـكـلـ نـكـمـيـ الـ نـكـلـوـ،ـ وـSNMPv2ـ،ـ وـSNMPv3ـ."
- ـ ةـبـقـارـمـلـاـ ةـادـأـ ئـلـ هـيـبـنـتـ لـئـاسـرـ Firepowerـ لـ لوـكـوـتـورـبـ لـسـرـيـ الـ "ـ .ـ ةـبـقـارـمـلـاـ ةـادـأـ ئـلـ هـيـبـنـتـ لـئـاسـرـ NMSـ لـ اـسـرـ Firewallـ FTDـ لـسـرـيـ الـ "ـ .ـ ةـبـقـارـمـلـاـ ةـادـأـ ئـلـ هـيـبـنـتـ لـئـاسـرـ SNMPـ لـ اـسـرـ NMSـ لـسـرـيـ الـ "ـ .ـ ةـبـقـارـمـلـاـ ةـادـأـ ئـلـ هـيـبـنـتـ لـئـاسـرـ SNMPـ لـ اـسـرـ Firepowerـ FTDـ 4100ـ لـ اـنـبـ صـاخـلـاـ FTDـ 4100ـ ئـلـعـ SNMPـ نـيـوـكـتـبـ اـنـمـقـ دـقـلـ "ـ هـيـبـنـتـلـاـ لـئـاسـرـ لـاسـرـاـ اـمـهـيـلـكـلـ نـكـمـيـ الـ نـكـلـوـ،ـ وـSNMPv2ـ،ـ وـSNMPv3ـ."

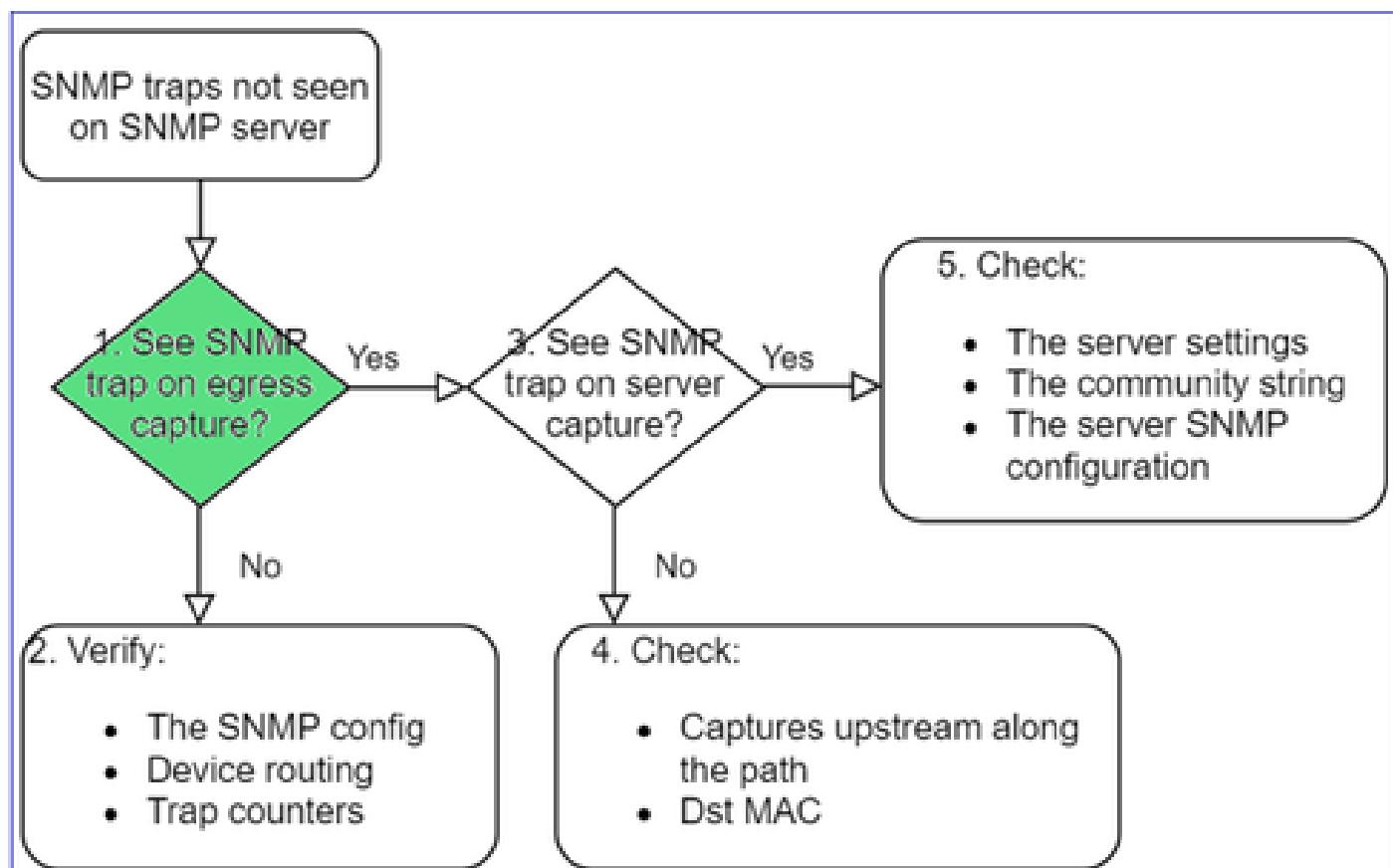
ـاهـالـصـ اوـ ءـاطـخـأـلـاـ فـاشـكـتـسـابـ يـصـومـ

ـهـيـلـمـعـ يـهـ ـهـيـلـمـعـ ةـمـئـالـمـ لـئـاسـمـلـ اـهـالـصـ اوـ يـبـاـيـسـنـالـاـ طـطـخـمـلـاـ ءـاطـخـأـ فـاشـكـتـسـأـ ةـيـلـمـعـ

SNMP:



جو خلا طاقت لایل عیوب نت لی اس ریوت له؟



ةرادل ا هج او لع LINA/ASA هي بن ت لى اس ر طاق ت ل ال:

```
<#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
```

ت ان اي بل ا هج او لع LINA/ASA هي بن ت لى اس ر طاق ت ل ال:

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

ت ان اي بل FXOS (41xx/9300) هي بن ت لى اس ر طاق ت ل ال:

```
<#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 10.3.1.1.2.1.1.3.0
firepower(fxos)#
exit

firepower#
connect local-mgmt

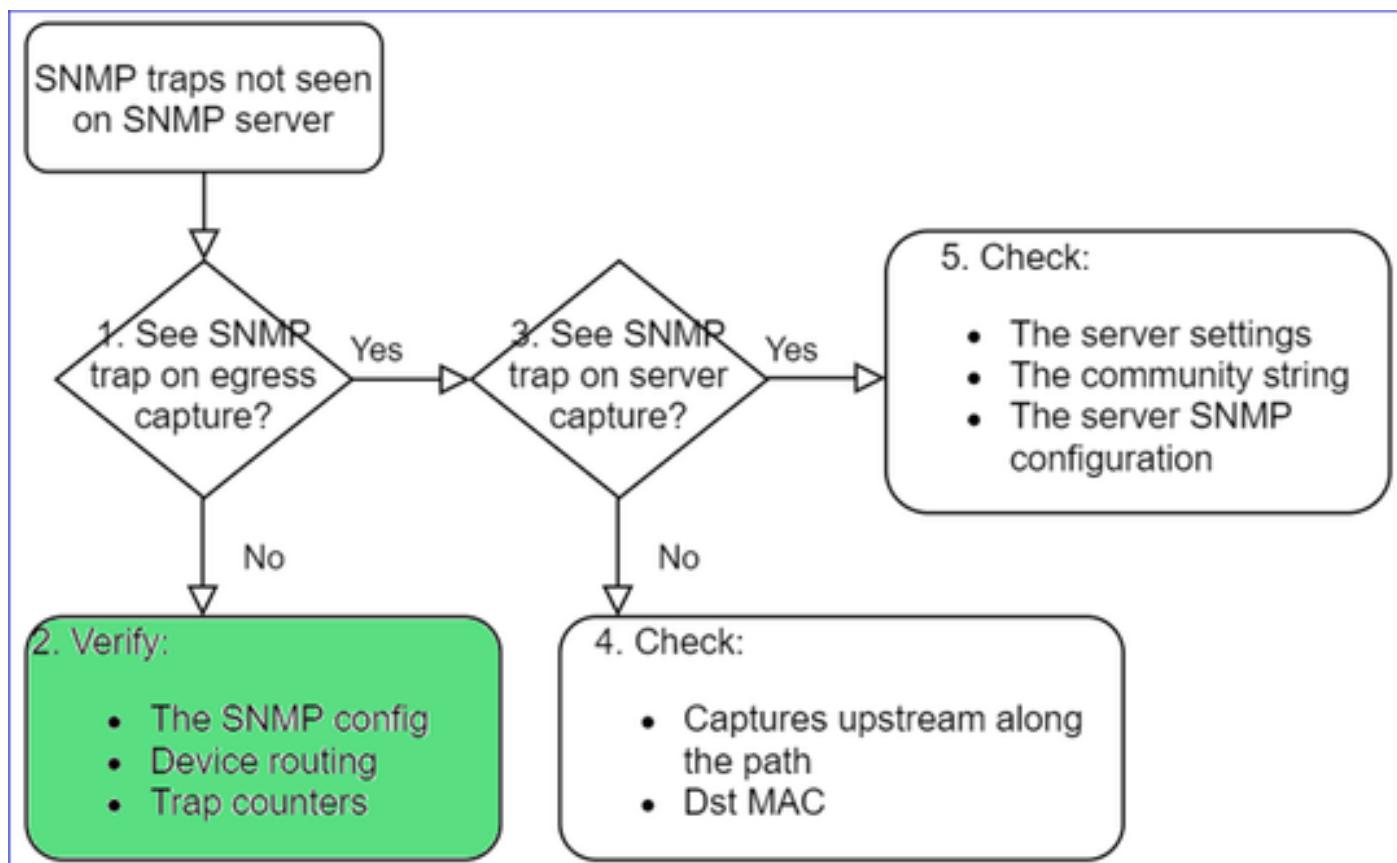
firepower(local-mgmt)#

```

dir

```
1 11134 Aug 2 11:25:15 2021 SNMP.pcap
firepower(local-mgmt)#
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

جورخ لايوج اوىل ع منح لايىرت ال تىن ك اذى.



<#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 نىيوكت لئااسر:

```
<#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

نیوکت > ۆزهجألا ۆرادا > ۆزهجألا ۆلاح یف الـ تادادعإلا هـذـه ىـرت الـ 1xxx/21xx عـضـوـيـفـ: ۆـظـحـالـمـ SNMP!

- ۆرادإلا ۆھجاو لالخ نـمـ ھـيـبـنـتـلـاـ لـئـاسـرـلـ LINA/ASA ھـيـجـوـتـ:

```
<#root>
```

```
>
```

```
show network
```

- تـانـايـبـلـاـ ۆـھـجـاوـ لـالـخـ نـمـ ھـيـبـنـتـلـاـ لـئـاسـرـلـ LINA/ASA ھـيـجـوـتـ:

```
<#root>
```

```
firepower#
```

```
show route
```

- ھـيـجـوـتـ FXOS (41xx/9300):

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- ھـيـبـنـتـلـاـ لـئـاسـرـ تـادـادـعـ (LINA/ASA):

```
<#root>
```

```
firepower#
```

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

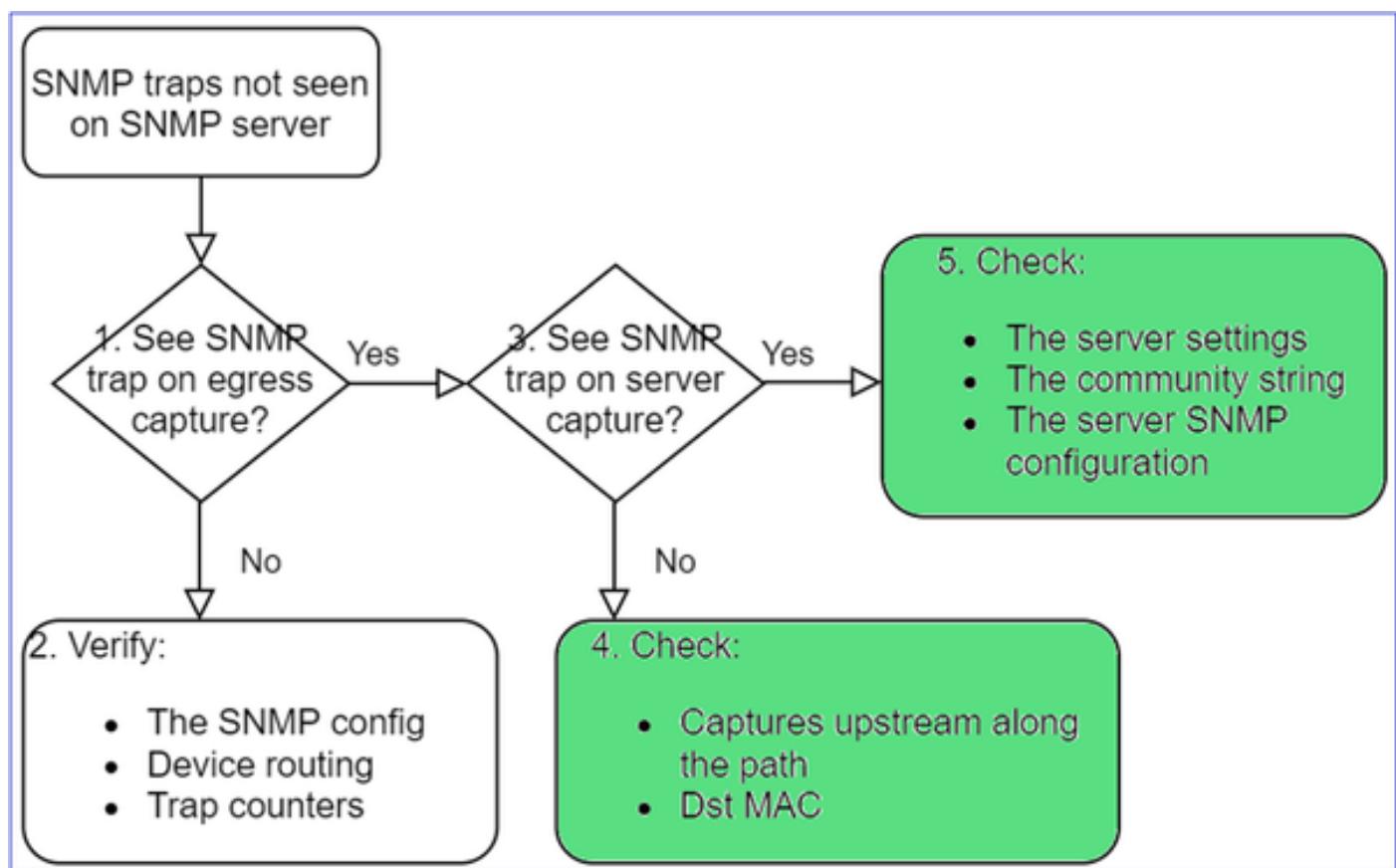
و FXOS:

```
<#root>
FP4145-1#
connect fxos

FP4145-1(fxos)#
show snmp | grep Trap

1296 Out Traps PDU
```

ةيافاضإلا ققحتل اتاي لم مع



- هجولاب صاخلا SNMP م داخل ةروص طقتل ا.

اهنم ققحتللى يرخأ عايشأ:

- راسملالوطىل ع طقتلت.
- هيبنت لئاسر مزحل هجولاب صاخلا MAC ناونع.
- هلا امو هجوفملا ذفانمل او هيامحلا رادج، لاثملال يبسىل (ع) هتللاحو SNMP م داخل تدادع ا.

(كـلـذـ).

- عـمـتـجـمـ ةـلـسـلـسـ SNMP.
- مـدـاـخـ نـيـوـكـتـ SNMP.

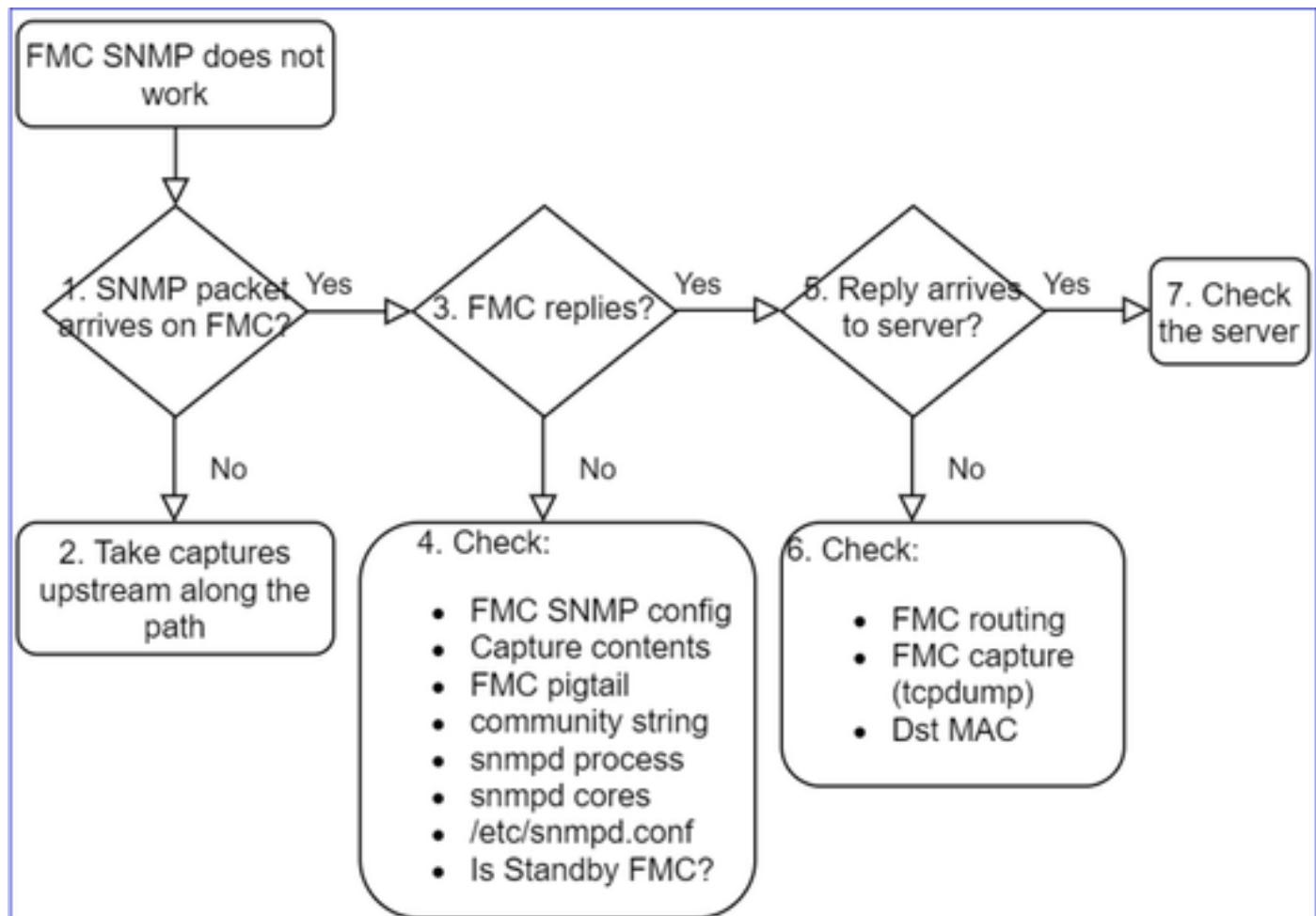
رابـعـ ةـبـقـارـمـ نـكـمـيـ الـ FMCـ

ةـيـقـيـقـحـلـاـ Cisco TACـ تـالـاحـ نـمـ جـذـوـمـنـ) ةـلـكـشـمـلـاـ فـاصـوـأـ:

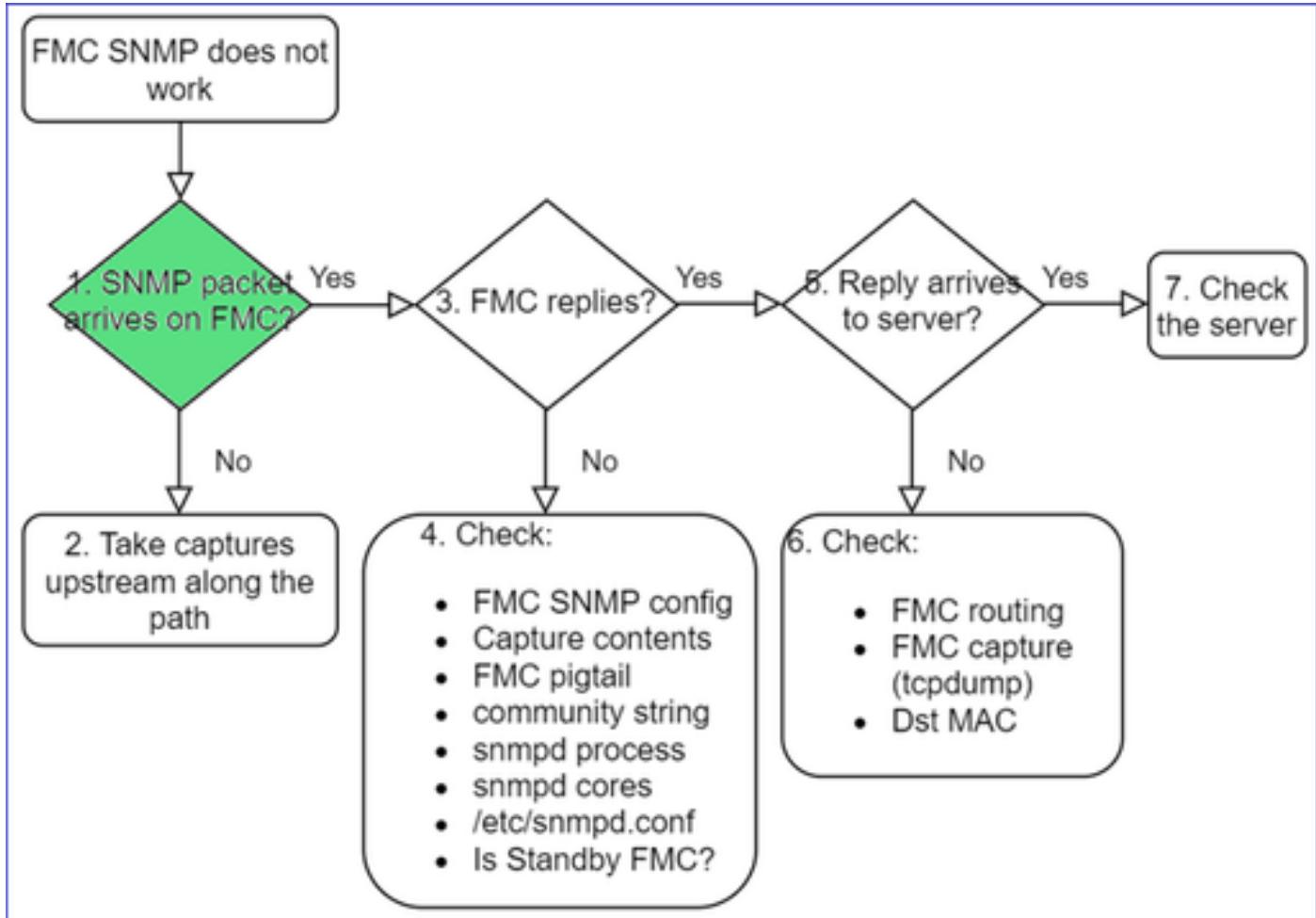
- دـادـعـتـسـاـ عـضـوـيـفـ لـمـعـيـ الـ "FMC."
- ةـرـكـاـذـ ةـبـقـارـمـ ئـلـاـ ةـجـاحـلـاـ "FMC."
- "192.168.4.0.8 FMC؟" دـادـعـتـسـاـ عـضـوـيـفـ لـمـعـيـ نـأـ بـجـيـ لـهـ
- ئـلـاـ اـمـ وـ ةـرـكـاـذـلـ اوـ ةـيـزـكـرـمـلـاـ ةـجـلـاعـمـلـاـ ـدـحـوـلـمـ اـهـدـرـاـوـمـ ةـبـقـارـمـلـ FMCsـ نـيـوـكـتـ اـنـيـلـعـ "كـلـذـ".

اهـالـصـ اوـ ءـاطـخـأـلـاـ فـاشـكـتـسـأـ ةـيـفـيـكـ

ةـصـاخـلـاـ SNMPـ تـالـكـشـمـبـ ةـصـاخـلـاـ يـبـاـيـسـنـالـاـ طـطـخـمـلـاـ ءـاطـخـأـ فـاشـكـتـسـالـ ةـيـلـمـعـلـاـ يـهـ هـذـهـ اـهـالـصـ اوـ ةـيـسـاسـأـلـاـ ةـحـولـلـاـ ةـرـادـاـيـفـ مـكـحـتـلـاـ ةـدـحـوـبـ:



1. ئـلـاـ اـهـقـيـرـطـ يـفـ SNMPـ ةـمـزـحـ لـهـ FMCـ؟



- ةرادا ڈھاویل ع طاقتل الـ FMC:

<#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.

```

 مدختسم ڈھاو نم ہلیزن تو و فتح حیملت FMC /var/common/ directory ع طاقتل الـ FMC

<#root>

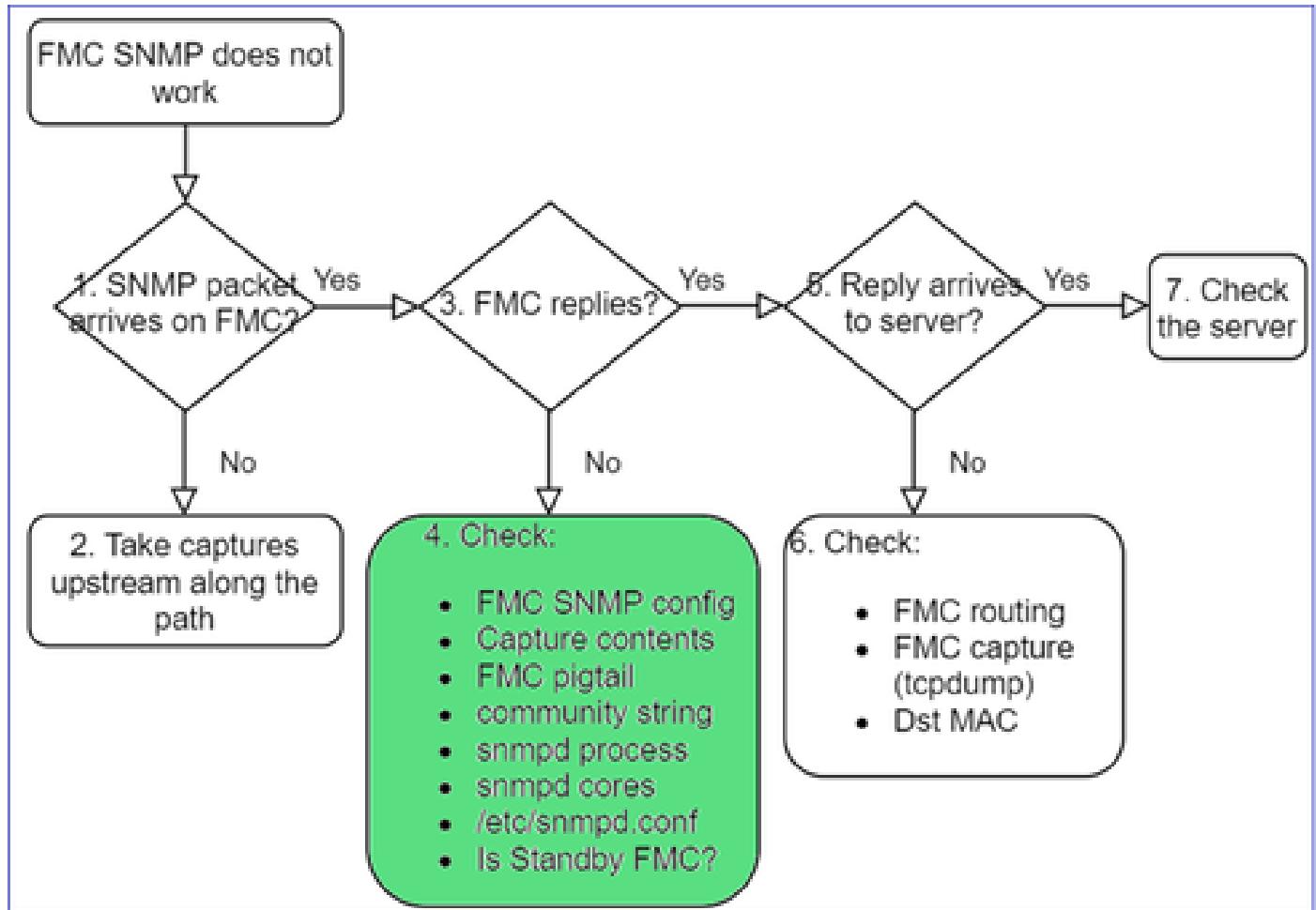
```

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
```

۵ دری FMC؟



فقط FMC دری مل اذی:

- نیوکتل ا > ماظنل ا FMC SNMP نیوکت
 1. SNMP مسق
 2. لوصول ا فمیا ق مسق

The screenshot shows two side-by-side views of the Firepower Management Center interface. The left view displays configuration settings for SNMP Version 2, specifically the Community String set to 'Cisco123'. The right view shows the 'Access List' configuration, listing a rule for port 161.

SNMP Version: Version 2

Community String: Cisco123

Host	Port
any	443
any	22
any	161

فقط FMC دری مل اذی:

- تاي وتحم طاقتلا (pcap)
 - (تاطقللإا يف كلذ ظحالم نكمي) عمتجملأا ٖلس
 - تاي وتحم و (راتآلإا، لشفلا تالاح، عاطخلأا نع ثحبلا) FMC -ب صالح pigtail رمألا جارخا /var/log/snmpd.log
 - ةيملع snmpd

<#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
```

- ةيسيس snmpd تاـفـلـمـ

<#root>

admin@ES2600-2:~\$

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

```
-rw----- 1 root root      5840896 Aug  3 11:28 core.1627990129 ES2600-2 snmpd 3.12948
```

- /etc/snmpd.conf: نیوکت فلم جاولان ڈھل کے لئے

<#root>

admin@FS2600-2: ~\\$

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

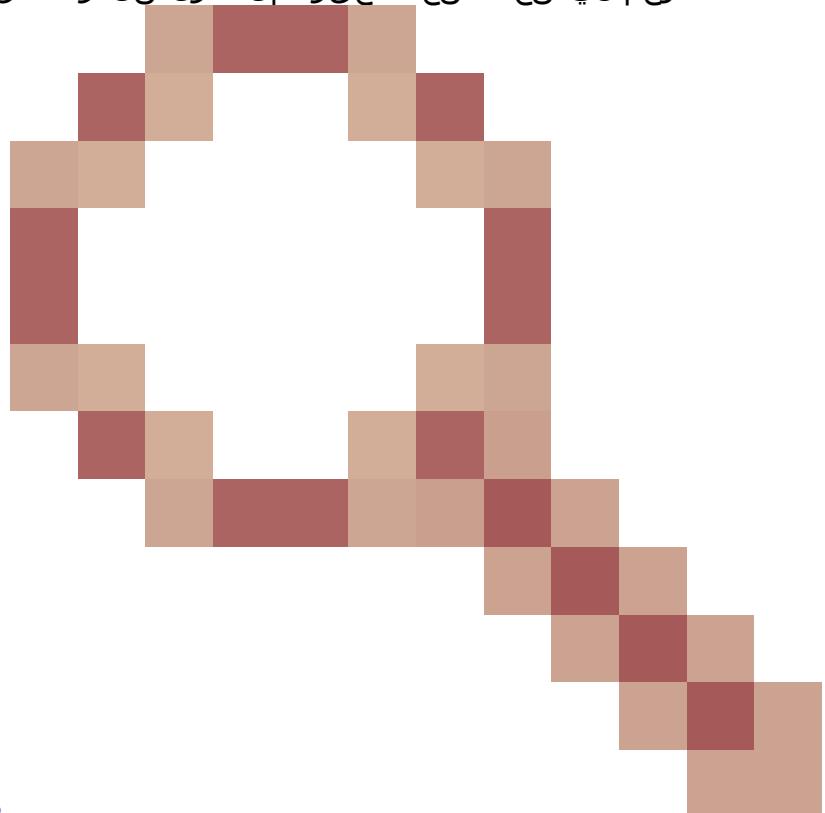
```
# additional user/custom config can be defined in *.conf files in this folder
includeDir /etc/snmp/config.d
engineIDType 3
agentaddress udp:161,udp6:161
rocommunity Cisco123
rocommunityv6 Cisco123
```



دوچوم ریغ snmpd.conf فلم ناف، SNMP لوكوتورب لي طعut مت اذا: ظحالم

- دادعت س الا عرض ويف FMC لـ ٥

تانا يب لاسراب دادعتس الاعضويه FMC موقعي الـ 6.6.0، لبقي ام 6.4.0-9 لبقي ام تارادصا يف فرع نيسح صحف. عقوتملا كولسلا وه اذهو. (راظتنا ةلاح يف snmpd نوكى)



Cisco نم عاطخألا حيحصت

نيوكت رّذعتي SNMP

ةيقيقجلا Cisco TAC تالاح نم جذومن) ةلكشملا فاص وأ:

- "لوكوتورب نيوكت ديرن" SNMP لـ Cisco Firepower Management Center وFirepower 4115 Threat Defense."
- "يلع SNMP نيوكت مادختساب معدلاء" FTD".
- "يب صاخلا زاهج ىلع SNMP ةبقارم نيكمت ديرن"
- "يف تقوملانيزختلا انل حيتي ال ماظنلا نكل، يف FXOS، SNMP ةمدخ نيوكت لواحن"
- "تاريغتلاءانجلإا 'Connect ftd' مدختسا. اهب حومسم ريع تارييغتلاءانل لوقى. ئيابنلا
- "انب صاخلا زاهج ىلع SNMP ةبقارم نيكمت ديرن"
- "ةبقارملاءافاشتكاو FTD نيوكت رّذعتي"

نيوكت تالكشم عم لماعتلا ئيفيك

اقي ثوتلا: ئلاؤلا ءاييشألا

- "يلاحلا دنتسملا أرقا!
- "نيوكت ليلد FMC:

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

- "نيوكت ليلد FXOS:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web->

ةفلىخملا SNMP تادنتسم ىلا هبتنا!

فیلتر FMC: SNMP لوکوت ورب صاخلا بـ

Book Contents

- Appliance Platform Settings
 - System Configuration
 - Platform Settings Policies
 - Platform Settings for Classic Devices

Find Matches in This Book

- Email Notifications
- Language Selection
- Login Banners
- SNMP Polling
- Time and Time Synchronization
- Global User Configuration Settings

FXOS: -ب ساخلا SNMP لوكوتورب

Home / ... / Cisco Firepower 9300 Series / Configuration Guides /

Cisco Firepower 4100/9300 FXOS Firepower

 Book Contents

[Book Title Page](#)

[Introduction to the Firepower Security Appliance](#)

[Getting Started](#)

[License Management for the ASA](#)

[User Management](#)

[Image Management](#)

[Security Certifications Compliance](#)

[System Administration](#)

[Platform Settings](#)

 Find Matches in This Book

Chapter: Platform Settings

> Chapter Contents

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

FirePower 41xx/9300 SNMP:

▽ Appliance Platform Settings

System Configuration

Platform Settings Policies

Platform Settings for Classic Devices

Platform Settings for Firepower Threat Defense

نیوکت Firepower 1xxx/21xx SNMP:

▽ Firepower Threat Defense Interfaces and Device Settings

Interface Overview for Firepower Threat Defense

Regular Firewall Interfaces for Firepower Threat Defense

Inline Sets and Passive Interfaces for Firepower Threat Defense

DHCP and DDNS Services for Threat Defense

SNMP for the Firepower 1000/2100

نیوکت SNMP يف FirePower Device Manager (FDM)

ةيقيقحلا Cisco TAC تالاح نم جذومن) ۃلکشملا فاصلوا:

- "FDM." مادختساب زاهجلا ىلع SNMPv3 يف FirePower زاهجلا ىلا ۃجاھب نحن."
- "FDM." نم FPR 2100 زاهج ىلع لمعي ای SNMP نیوکت."
- "FDM." ىلع لمعیل SNMP v3 نیوکت ىلع لوصحلا رّذعنی."
- "SNMP." نیوکت ۃدعاسم FDM 6.7 SNMP."
- "FDM." يف SNMP v3 Firepower نیکمت.

نیوکت تالکشم ع ملماعتلا ۃيفيك

- "FlexConfig: مادختساب SNMP نیوکت ءارج| کنكمي pre-6.7 رادصايل ۃبسنلاب"

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

- "FlexConfig،" مادختساب SNMP نیوکت متی دعی مل، Firepower، 6.7 رادصايل نم آعدب"

تاقیب طت ةجمرب ةهجاو مادختساب REST:

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

اھالص او SNMP ءاطخاً فاشكتسال ٽيعجرملا تامولعملا قاروا

ٽينفل ا ٽدعاسمل زكرم عم ٽلاح حتف لبقي عيمجت بجي ام - (LINA/ASA) (TAC) يف Cisco

فصولا	
firepower# show run snmp-server	بـ صاخلا SNMP لوكوتورب نيوكـت نـم قـقـحـت ASA/FTD LINA.
firepower# show snmp-server statistics	ىـلـعـ تـايـيـاصـحـاـ نـمـ قـقـحـتـ SNMPـ ASA/FTD LINAـ. مـزـحـ جـاـخـ اوـ SNMPـ مـزـحـ لـاخـداـ تـادـادـعـ ىـلـعـ زـكـرـ SNMPـ.
> capture-traffic	ةـرـادـاـ ٽـهـجـاـوـ ىـلـعـ رـوـرـمـلاـ ٽـكـرـحـ طـاـقـتـلـاـ.
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	ٽـهـجـاـوـ ىـلـعـ تـانـايـبـلـاـ رـوـرـمـ ٽـكـرـحـ طـاـقـتـلـاـ عـالـطـتـسـاـ (net201) 161ـ لـ UDPـ (مسـاـ)ـ تـانـايـبـلـاـ SNMPـ.
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	ٽـهـجـاـوـ ىـلـعـ تـانـايـبـلـاـ رـوـرـمـ ٽـكـرـحـ طـاـقـتـلـاـ تـارـابـتـخـاـ (namelf 'net208')ـ لـ UDPـ 162ـ. (namelf 'net208')ـ تـانـايـبـلـاـ SNMPـ.
firepower# show capture SNMP-POLL packet-number 1 trace	لـصـتـ يـتـلـاـ لـخـدـمـلـاـ ٽـصـاخـلـاـ SNMPـ ٽـمـزـحـ عـبـتـتـ ASA/FTD LINAـ.
admin@firepower:~\$ sudo tcpdump -i tap_nlp	لـ NLPـ لـ ٽـيـلـخـادـلـاـ طـغـضـلـاـ ٽـهـجـاـوـ ىـلـعـ طـاـقـتـلـاـ (tap_nlpـ).
firepower# show conn all protocol udp port 161	ىـلـعـ تـالـاـصـتـاـ عـيـمـجـ نـمـ قـقـحـتـ ASA/FTD LINAـ. عـالـطـتـسـاـ (net201)ـ SNMPـ.
firepower# show log i 302015.*161	لـجـسـ نـمـ قـقـحـتـلـاـ ASA/FTD LINAـ 302015ـ عـالـطـتـسـاـ SNMPـ.

firepower# more system:running-config مۇتجمۇع	عەمەتجمۇم ئەلسلىس نم قىقەتلىا SNMP.
firepower# debug menu netsnmp 4	ةيىلمۇلا فرّعەم و SNMP نىيوكت نم قىقەتلىا.
firepower# show asp table classify interface net201 domain permit match port=161	لۇصۇلما يەنەن مەئاوقىنەم قىقەت (ACL) مەساب ئەجاوىلىع SNMP لۆكۆتۈرۈب ئەصاخلى "Net201".
firepower# show disk0: بىل	ةيىساسأ تافلمۇ ئىأ كانە تىنەك اذىامم قىقەت لۆكۆتۈرۈپ SNMP.
admin@firepower:~\$ ls -l /var/data/cores	ةيىساسأ تافلمۇ ئىأ كانە تىنەك اذىامم قىقەت ئىلىع طقىق قېبطنى لۆكۆتۈرۈپ FTD.
firepower# show route	ھېجوت لودج نم قىقەتلىا ASA/FTD LINA.
> show network	ةرادا ئىوتسم ھېجوت لودج نم قىقەتلىا FTD.
admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	ئەاطخاً فاشكەتساً نم قىقەتلىا SNMPv3 ئىلىع اھالىسى او FTD.
firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	تايمۇ . ثەحڭىلە تارادىسىلا يەنەن فاشكەتساً ئەدىفم ، ئىلخادلى ئەاطخاً حىچھىت ئەدعاسملا زىرىم لالخ نم اھالىسى او SNMP ئەاطخاً يەنەن (TAC) Cisco.

يەنەن (TAC) ئەدعاسملا زىرىم ئەلەحەتلىق لباق ھەيمىجت بىچى ام – Cisco

فصۇلما	
firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 161" limit-captured-frames 50 write workspace:///SNMP-POLL.pcap	نەعەلەتلىك FXOS طاقەتلىا SNMP (UDP 161) دىيغىب FTP مەداخىلىلىيەمەت

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	FTP IP: 192.0.2.100 م دخـتـسـم مـسـا FTP: ftp
firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap	هـيـبـنـتـ لـيـاسـرـلـ FXOS طـاقـتـلـاـ SNMP (UDP 162)
firepower# scope system firepower /system # scope services firepower /system/services # show ip-block detail	لوـصـوـلـابـ مـكـحـتـلـاـ ةـمـيـاـقـ نـمـ قـقـحـتـ FXOS
firepower# show fault	لـاطـعـأـ نـمـ قـقـحـتـ FXOS
firepower# show fabric-interconnect	ةـهـجـاـوـ نـيـوـكـتـ نـمـ قـقـحـتـ FXOS ةـيـضـارـتـفـالـاـ ةـرـأـبـعـلـاـ تـادـدـاعـاـوـ
firepower# connect fxos firepower(fxos)# show running-config snmp all	نـيـوـكـتـ نـمـ قـقـحـتـلـاـ FXOS SNMP
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	-بـ ةـصـاخـلـاـ OIـDـ تـافـرـعـمـ نـمـ قـقـحـتـلـاـ FXOS SNMP
firepower# connect fxos firepower(fxos)# show snmp	تـادـدـاعـوـ تـادـدـاعـإـ نـمـ قـقـحـتـلـاـ FXOS SNMP
firepower# connect fxos	"مـزـحـلـاـ"ـ ئـاطـخـأـ حـيـحـصـتـ FXOS SNMP

firepower(fxos)# terminal monitor	لكل "ا" وأ
firepower(fxos)# debug snmp pkt-dump	مدخلات "terminal no monitor" و "undebug all" اهافقى إال
firepower(fxos)# debug snmp all	

يـف (TAC) ةـينـفـلـا ةـدـعـاسـمـلـا زـكـرـمـعـمـ ةـلـاحـحـتـفـ لـبـقـ هـعـيـمـجـتـ بـجـيـ اـمـ Cisco

فـصـوـلـا	
> capture-traffic	ةـرـادـإـلـا ةـهـجـاـوـىـلـعـ رـوـرـمـلـا ةـكـرـحـ طـاقـتـلـا
> show network	ةـرـادـإـا ئـوـتـسـمـ هـيـجـوـتـ لـوـدـجـ نـمـ قـقـحـتـلـا FTD
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail] firepower /monitoring # show snmp-trap	FXOS SNMP نـيـوـكـتـ نـمـ قـقـحـتـلـا
firepower# show fault	FXOS لـاطـعـأـ نـمـ قـقـحـتـا
firepower# connect local-mgmt firepower(local-mgmt)# dir cores_fxos firepower(local-mgmt)# dir cores	FXOS ةـسـاسـأـلـا تـافـلـمـ نـمـ قـقـحـتـلـا (tracebacks)

يـف (TAC) ةـينـفـلـا ةـدـعـاسـمـلـا زـكـرـمـعـمـ ةـلـاحـحـتـفـ لـبـقـ هـعـيـمـجـتـ بـجـيـ اـمـ Cisco FMC

فـصـوـلـا	
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n	ةـرـادـإـلـا ةـهـجـاـوـىـلـعـ رـوـرـمـلـا ةـكـرـحـ طـاقـتـلـا نـعـ عـالـطـتـسـاـلـلـ SNMP
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	ةـرـادـإـلـا ةـهـجـاـوـىـلـعـ رـوـرـمـلـا ةـكـرـحـ طـاقـتـلـا فـلـمـ يـفـ اـهـظـفـحـوـ SNMP نـعـ عـالـطـتـسـاـلـلـ

admin@FS2600-2:~\$ sudo pmtool status بيج ريقص	SNMP ققحتلا نم ةلاح يليلمع ئيلام
admin@FS2600-2:~\$ ls -al /var/common بيج ريقص	SNMP تافلم نم ققحتلا (رثألا عبّت)
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	SNMP ققحتلا تايوتحم فلم نويوك

ىلع ئلثمأ snmpwalk

اهحالص او ءاطخألا فاشكتس او ققحتلل رماؤألا هذه مادختسا نكمي:

	فصولا
# snmpwalk -c Cisco123 -v2c 192.0.2.1	<p>نم OID تافّرم عيمج بلجي مادختساب ديعبلا فيضملا SNMP v2c.</p> <p>Cisco123 = Community string</p> <p>192.0.2.1 = destination host</p>
# snmpwalk -v2c -Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.109.1.1.1.1.3 .3.6.1.4.1.9.109.1.1.1.3.1 = Gigabit32: 0	ديعبلا فيضملا نم ددم OID بلجي مادختساب SNMP v2c
# snmpwalk -c Cisco123 -v2c 192.0.2.1.10.3.1.1.4.1.9.109.1.1.1.1 -on .10.3.1.4.1.9.109.1.1.1.1.6.1 = G32: 0	مت يتلا تانئاكللا تافّرم رهظي يمرقرقي سنتب اهبلج
# snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1	<p>فيضملا نم عيمج بلجي مادختساب ديعبلا SNMP v3.</p> <p>SNMPv3 = cisco</p> <p>SNMPv3 = SHA.</p> <p>SNMPv3 = AES</p>
# snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -	فيضملا نم OID عيمج بلجي

x AES -X Cisco123 192.0.2.1	مادختس اب دیعبلما و AES128) SNMP v3 (MD5
# snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1	طقف ټق داصل مل اع SNMPv3

بویع نع ثحبلا ټي فيك

کلما لقتنا.

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

2. ئاقلا نم ديدحت رتخارو ئيساساً ئاملا كلار خدا.

Tools & Resources

Bug Search Tool

The screenshot shows the 'Bug Search Tool' interface. The search parameters are set as follows:

- Search For: snmp
- Product: Series/Model
- Releases: Affecting or Fixed in these Releases
- Modified Date, Status, Severity, Rating, Support Cases, Bug Type, Filter, and Customer Visible dropdowns are present but not explicitly selected.

The screenshot shows the search results for 'snmp'. The product selected is 'Cisco Firepower Management Center Virtual Appliance'. The results table displays the following information for the first result:

Viewing 1 - 25 of 159 results	Sort by
CSCvh32876 - ENH:Device level settings of FP2100 should allow to configure ACL and SNMP location	Ex
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)	

اعويش رثکالا تاجتنملما:

- جمانرب Cisco Adaptive Security Appliance (ASA)

- Firepower 9300 Series
- Cisco Firepower Management Center یرها ئاظلا زاھجلا
- Cisco Firepower نم يلاتلا لىچلارا ئامحلا رادج

ةلص تاذ تامولعم

- [تادي دهتلارا دض عافدلل SNMP نيوكتب مق](#)
- [تادي FXOS \(UI\) SNMP ىلىع نيوكت](#)
- [- تادنتسملاوي نقتلا مع دلا Cisco Systems](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).