# تكوين SNMP على أجهزة FirePOWER NGFW

## المحتويات

# المقدمة

يوضح هذا المستند كيفية تكوين برنوتوكول إدارة الشبكة البسيط (SNMP) واستكشاف أخطائه وإصلاحها على أجهزة FTD لجدار الحماية (NGFW) من الجيل التالي.

# المتطلبات الأساسية

## المتطلبات

يتطلب هذا المستند معرفة أساسية ببرنوتوكول SNMP.

## المكونات المستخدمة

ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# معلومات أساسية

يمكن تقسيم أجهزة Firepower NGFW إلى نظامين فرعيين رئيسيين:

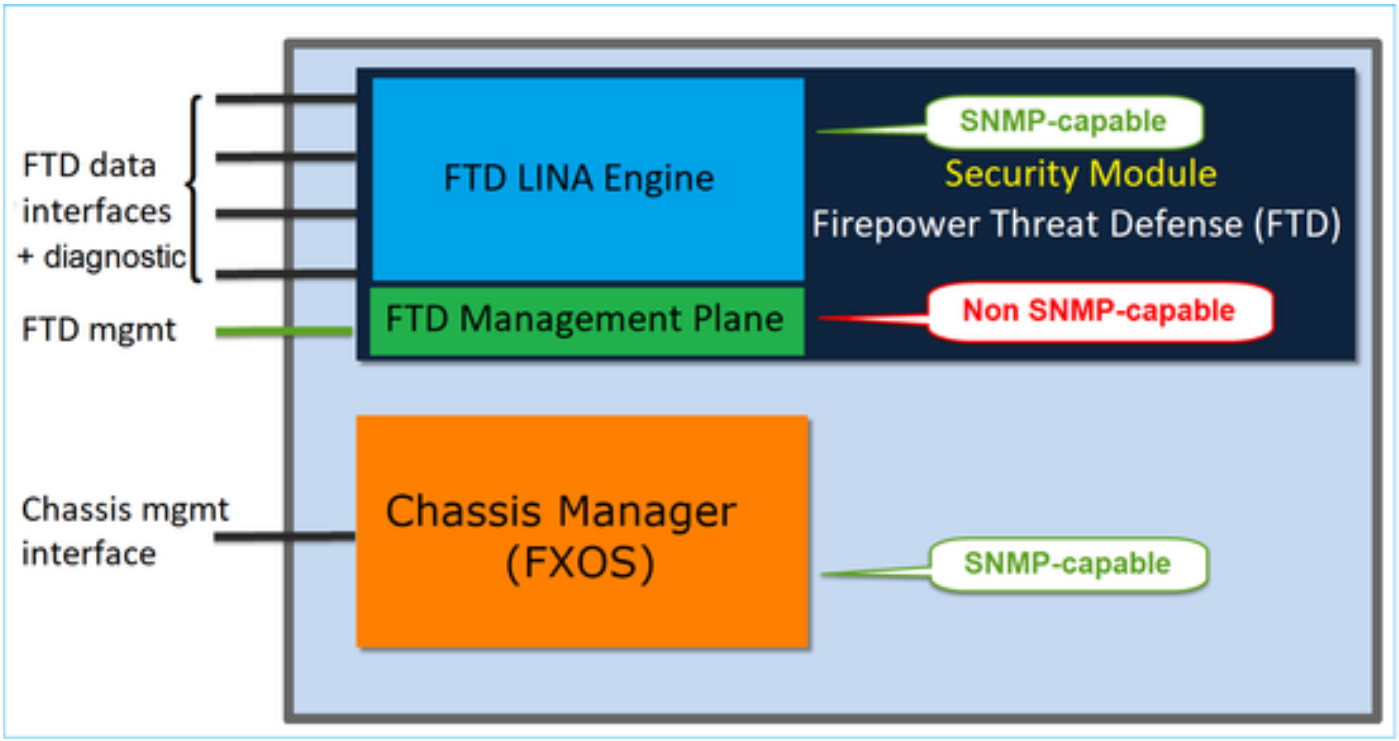
- يتحكم النظام التشغيلي القابل للتوسعة (FX-OS) في أجهزة الهيكل القاعدي.
- يعمل Firepower Threat Defense (FTD) داخل الوحدة النمطية.

FTD هو برنامج موحد يتكون من محركين رئيسيين، محرك الشير، ومحرك لينا. يستمد محرك SNMP الحالي الخاص ب FTD من تقنية ASA التقليدية كما أنه يتمتع بإمكانية رؤية المميزات المتعلقة بالخط.

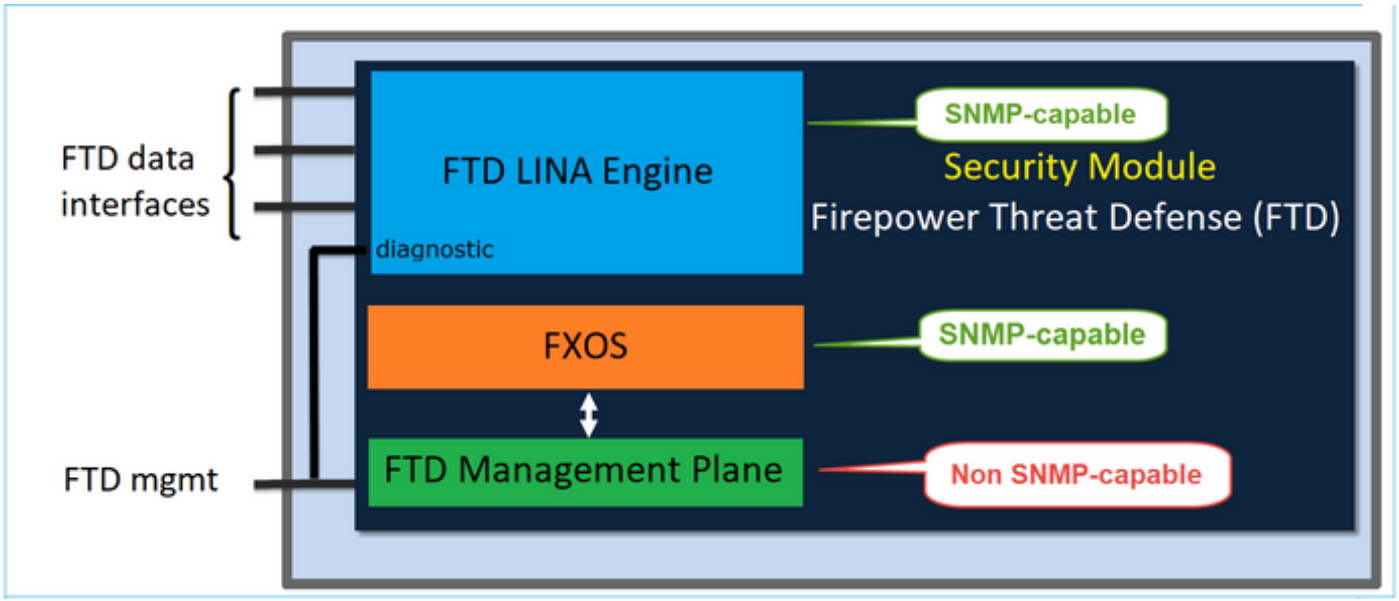
يحتوي نظام التشغيل FX-OS و FTD على مستويات تحكم مستقلة وألغراض المراقبة، تكون لديهم محركات SNMP مختلفة. يوفر كل محرك من محركات SNMP معلومات مختلفة ويتم ترجيله لديه المراقبة على حد سواء للحصول على عرض أكثر شمولا لحالة الجهاز.

من وجهة نظر الأجهزة، يوجد حاليا بنيتان رئيسيتان لأجهزة جدار الحماية من الجيل التالي Firepower: هما Firepower 2100 Series و Firepower 4100/9300 Series.

تحتوي أجهزة Firepower 4100/9300 على واجهة مخصصة لإدارة الأجهزة وهذا هو المصدر والوجهة لحركة مرور SNMP الموجهة إلى نظام FXOS الفرعي. من ناحية أخرى، يستخدم تطبيق FTD واجهة LINA (البيانات و/أو التشخيص. في الإصدارات اللاحقة لـ 6.6 FTD، يمكن استخدام واجهة إدارة FTD أيضاً) لتكوين SNMP.




يستخدم محرك SNMP على أجهزة Firepower 2100 واجهة إدارة FTD وعنوان IP. يقوم الجهاز نفسه بربط حركة مرور SNMP المستلمة على هذه الواجهة وتعيد توجيهها إلى برنامج FXOS.

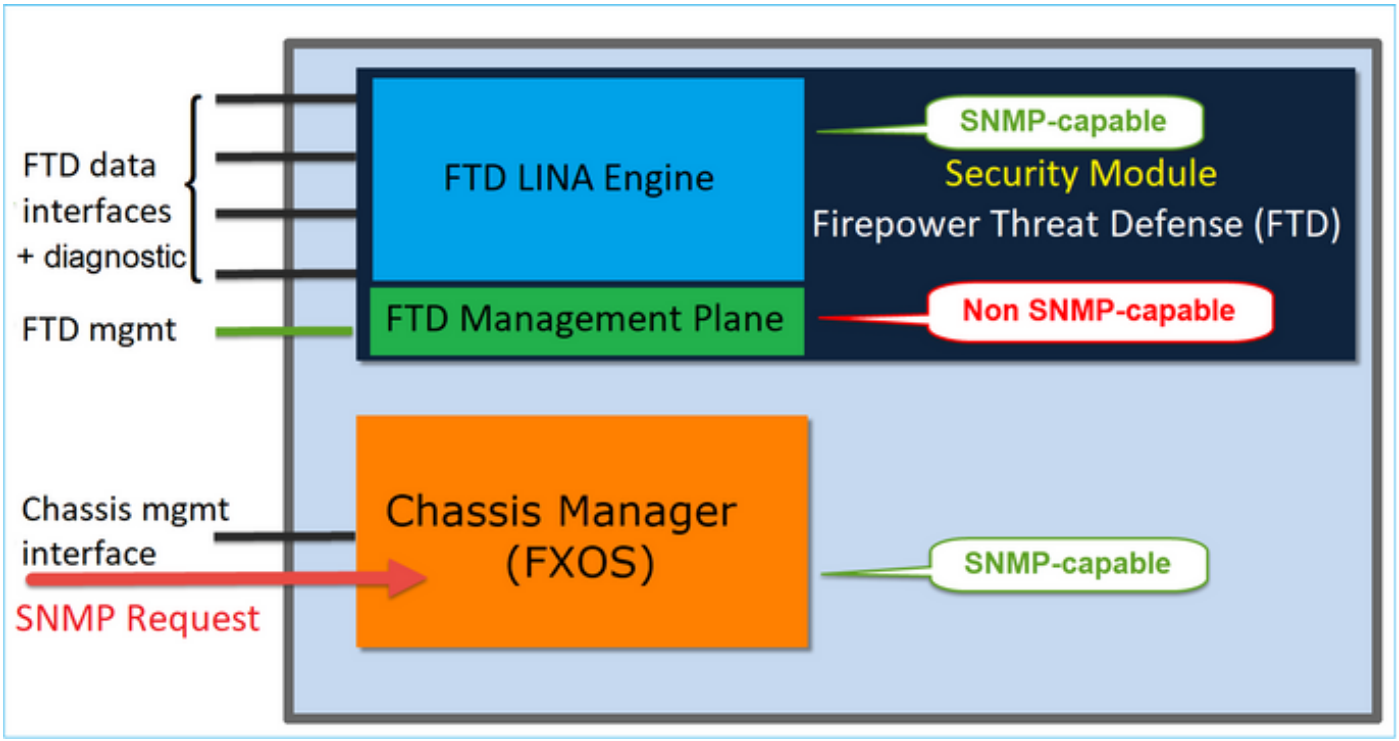



في FTDs التي تستخدم إصدار البرنامج 6.6+، تم تقديم هذه التغييرات:

- SNMP عبر واجهة الإدارة.
- على الأنظمة الأساسية لسلسلة FPR1000 أو FPR2100، يوحّد كل من SNMP LINA وFXOS عبر واجهة الإدارة الفردية هذه. بالإضافة إلى ذلك، فإنه يوفر نقطة تكوين واحدة على FMC ضمن إعدادات النظام الأساسي > SNMP.

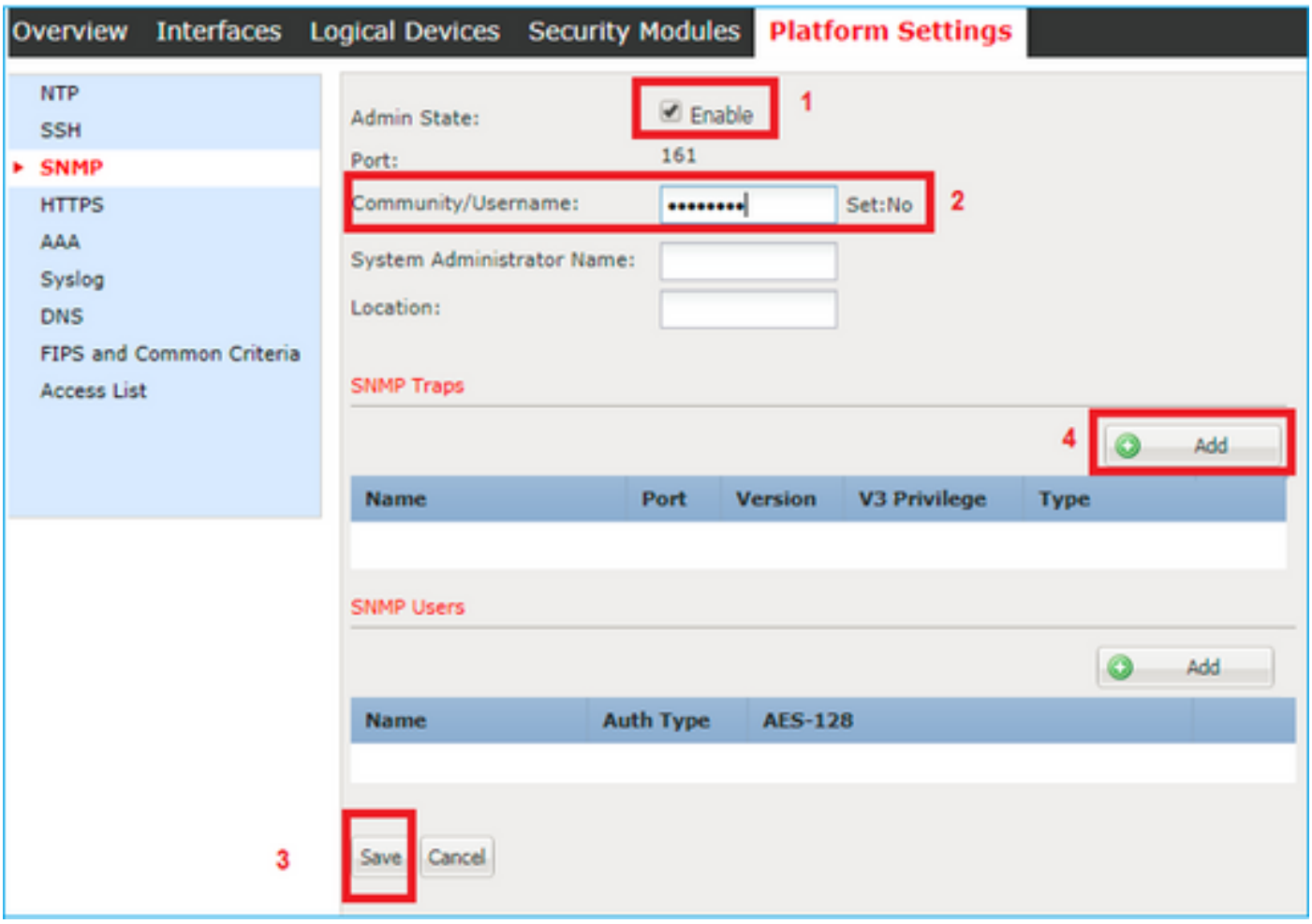
## التكوين

بروتوكول إدارة الشبكة البسيط (SNMP) للهيكل القاعدي (FXOS) على FPR4100/FPR9300



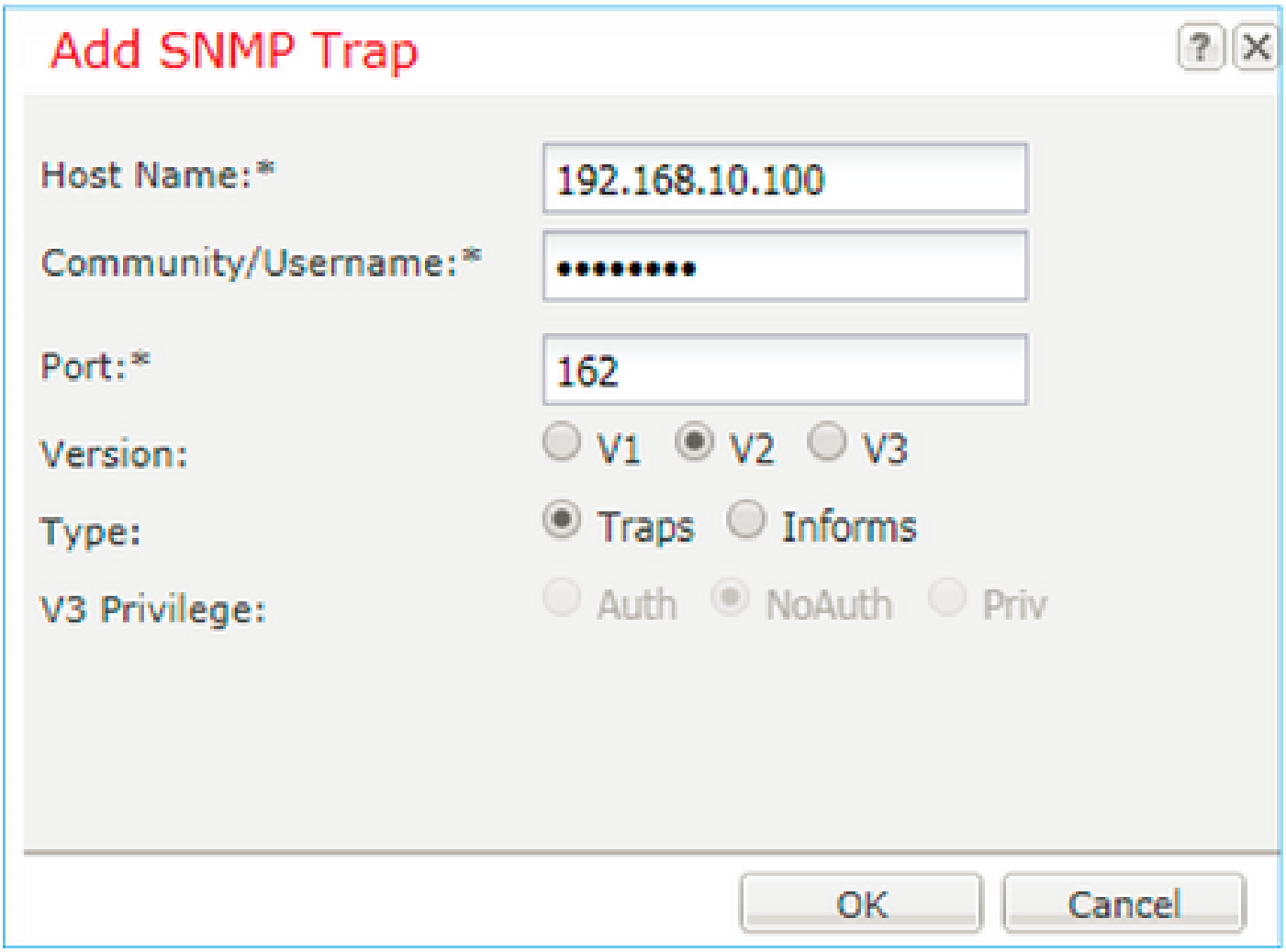

تكوين FXOS SNMPv1/v2c عبر واجهة المستخدم الرسومية (GUI)

الخطوة 1. افتح واجهة مستخدم Firepower Chassis Manager (FCM) وانتقل إلى إعدادات النظام الأساسي > علامة تبويب SNMP. حدد مربع تمكين SNMP، وحدد سلسلة المجتمع المطلوب استخدامها في طلبات SNMP، ثم حفظ.




ملاحظة: إذا كان حقل المجتمع/اسم المستخدم معيناً بالفعل، فإن النص الموجود على يمين الحقل الفارغ يقرأ المجموعة: نعم. إذا لم يكن حقل المجتمع/اسم المستخدم قد تم تعميمه بعد بقيمة، فإن النص الموجود على يمين الحقل الفارغ يقرأ المجموعة: لا

الخطوة 2. تكوين خادم وجهة SNMP TRAPS.




ملاحظة: قيم المجتمع للاستعلامات ومضيف المصيدة مستقلة ويمكن أن تكون مختلفة

يمكن تعريف المضيف كعنوان IP أو باالسم. حدد موافق وسيتم حفظ تكوين خادم رسائل تنبيه SNMP تلقائيًا. ليست هناك حاجة لتحديد زر الحفظ من صفحة SNMP الرئيسية. يحدث الشيء نفسه عندما تقوم بحذف مضيف.

تكوين FXOS SNMPv1/v2c عبر واجهة سطر الأوامر (CLI)

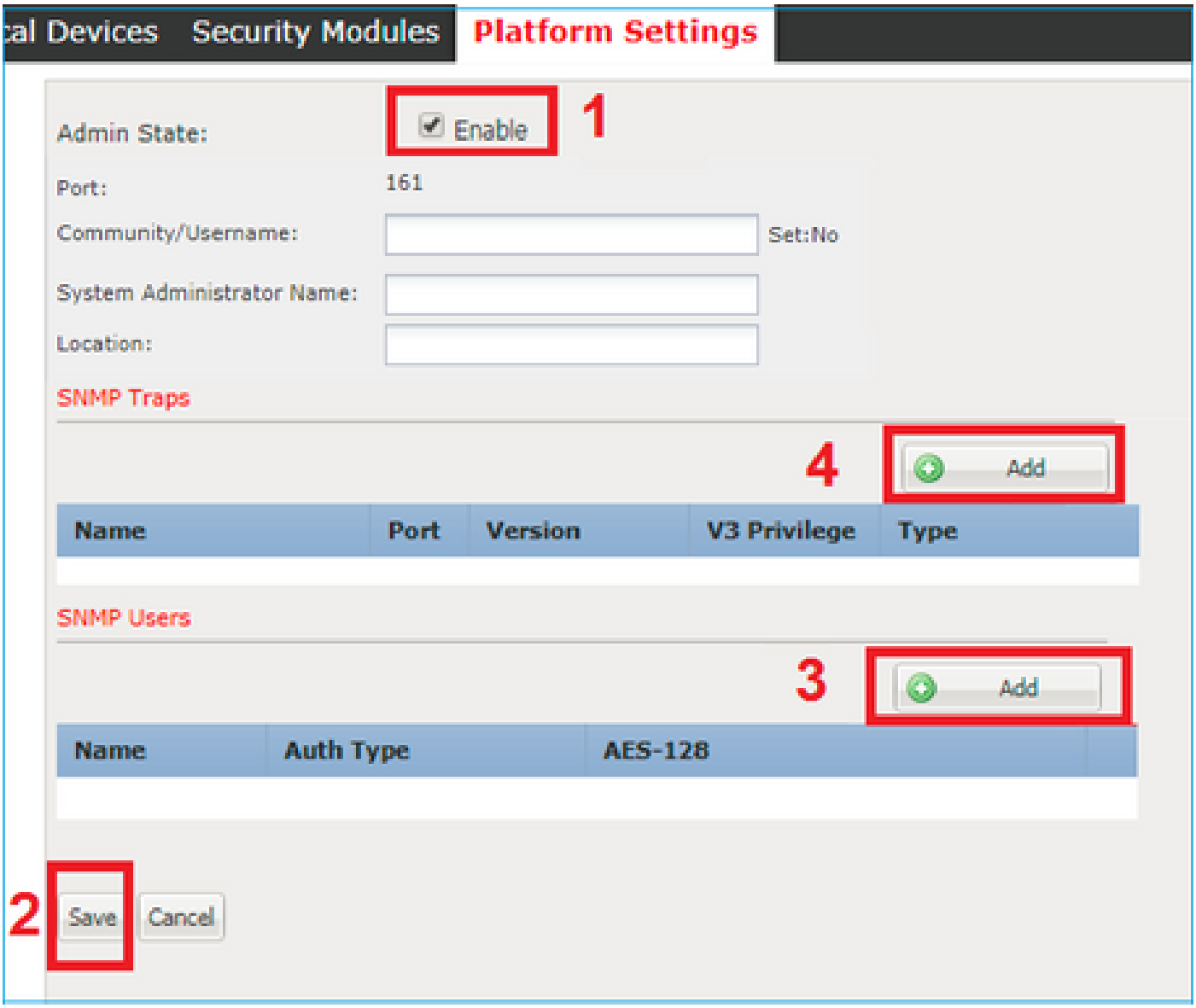
```
<#root>

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
```

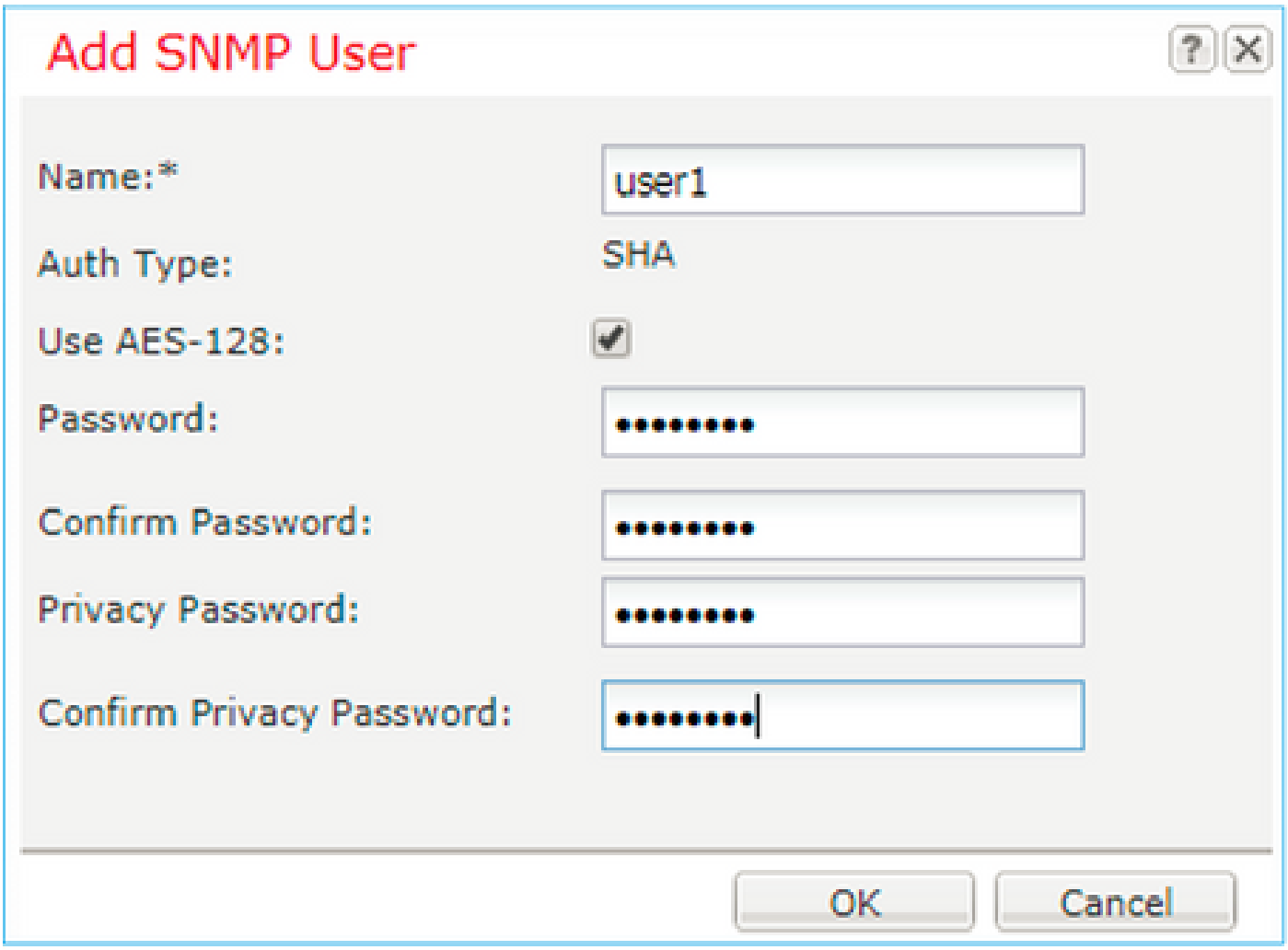
تكوين FXOS SNMPv3 عبر واجهة المستخدم الرسومية (GUI)

الخطوة 1. افتح FCM وانتقل إلى إعدادات النظام الأساسي > تبويب SNMP.

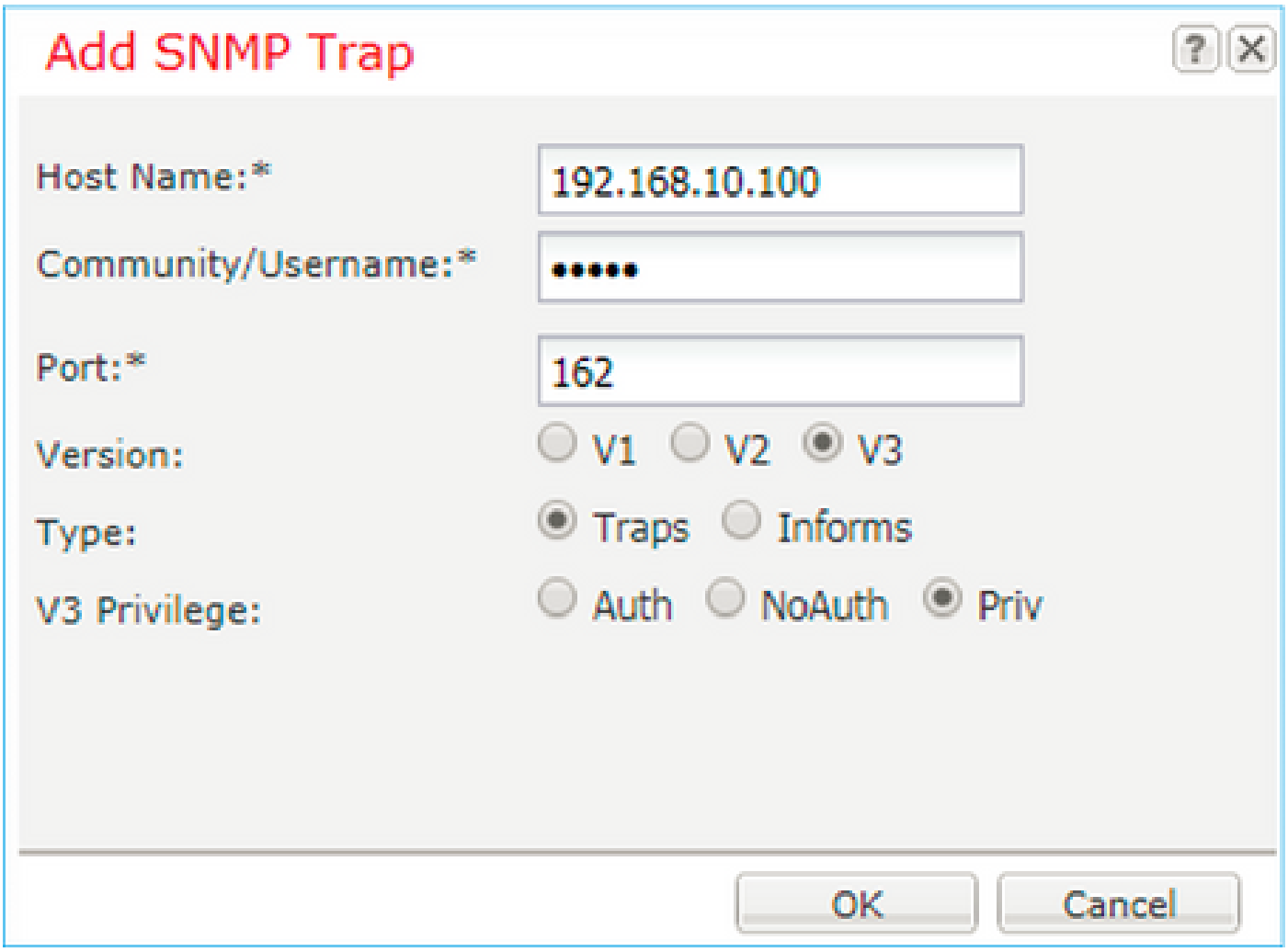
الخطوة 2. بالنسبة ل SNMP v3 ال توجد حاجة لتعيين أي سلسلة مجتمع في القسم العلوي. يستطيع كل مستخدم تم إنشاؤه تشغيل الاستعلامات إلى محرك FXOS SNMP بنجاح. الخطوة الأولى هي تمكين SNMP في النظام الأساسي. بمجرد الانتهاء من ذلك، يمكنك إنشاء المستخدمين وضبط رسائل تنبيه الوجهة. يتم حفظ كل من مستخدمي SNMP وضبط رسائل تنبيه SNMP تلقائياً.




الخطوة 3. كما هو موضح في الصورة، أضف مستخدم SNMP. نوع المصادقة هو دائماً SHA ولكن يمكنك استخدام AES أو DES للتشفير:




الخطوة 4. إضافة مضيف مالئمة SNMP، كما هو موضح في الصورة:

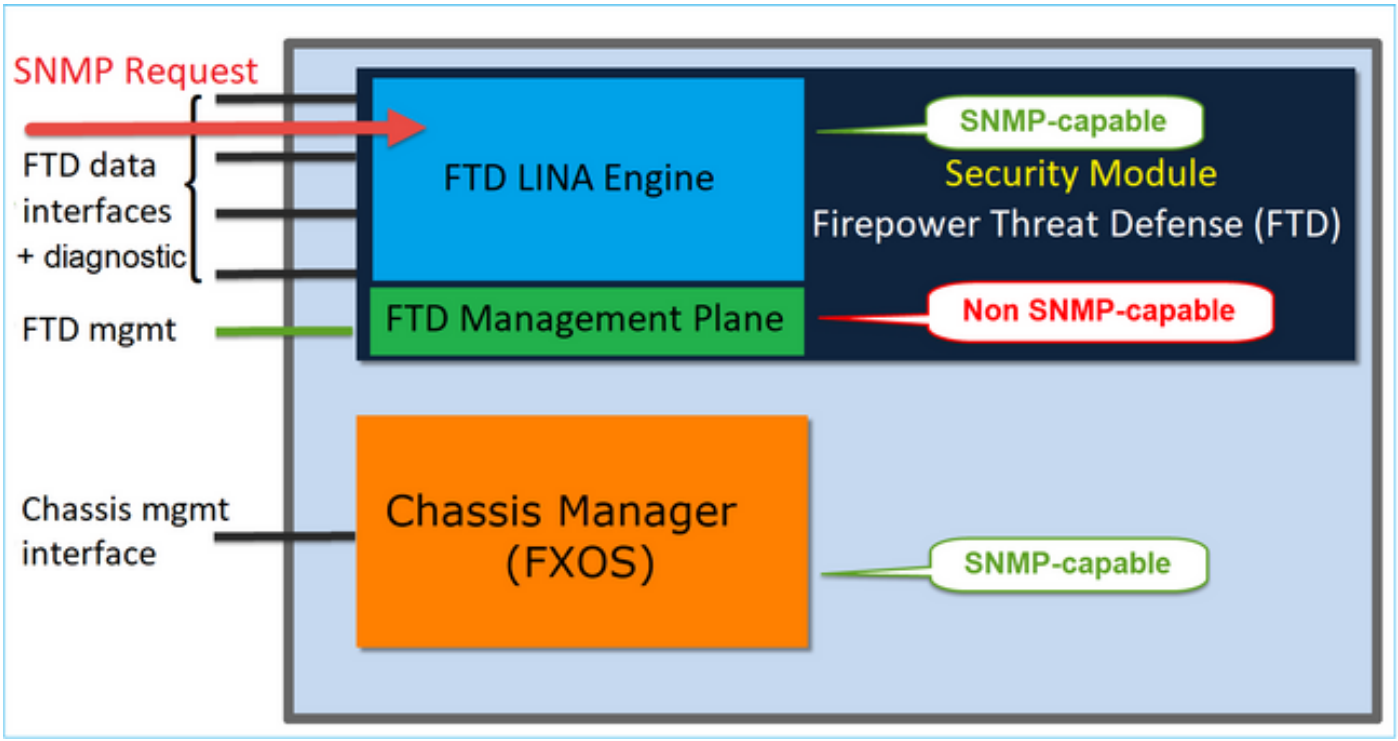



تكوين FXOS SNMPv3 عبر واجهة سطر الأوامر (CLI)

```
<#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* #
```

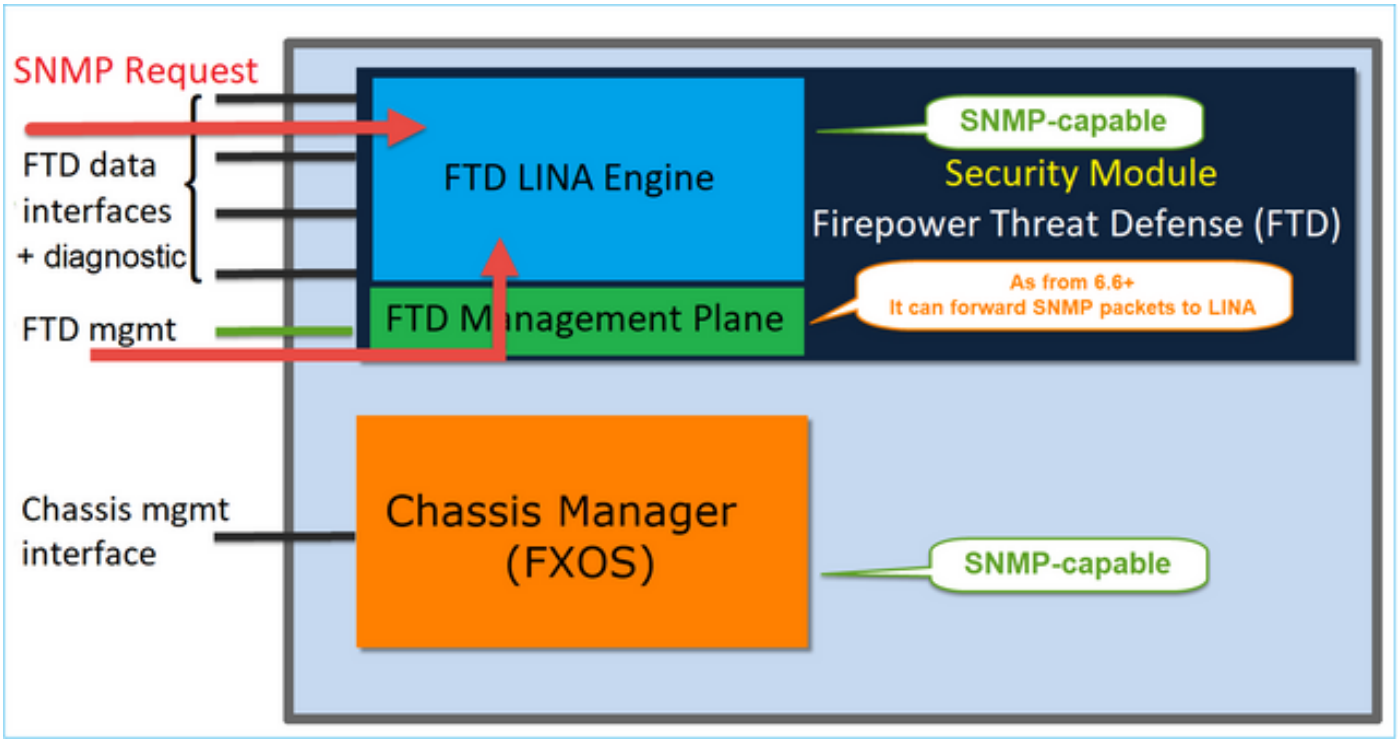
```
set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter snmp-trap 10.48.26.190
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v3
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype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

## بروتوكول إدارة الشبكة البسيط (SNMP) لـ FTD (LINA) على FPR4100/FPR9300




التغييرات في إصدارات 6.6+

- في إصدارات ما بعد 6.6، يكون لديك أيضًا خيار استخدام واجهة إدارة FTD لاستطلاعات الرأي ورسائل التنبيه.




يتم دعم ميزة إدارة عنوان IP الفردي لبروتوكول SNMP من 6.6 فصاعدًا على جميع الأنظمة الأساسية لـ FTD:

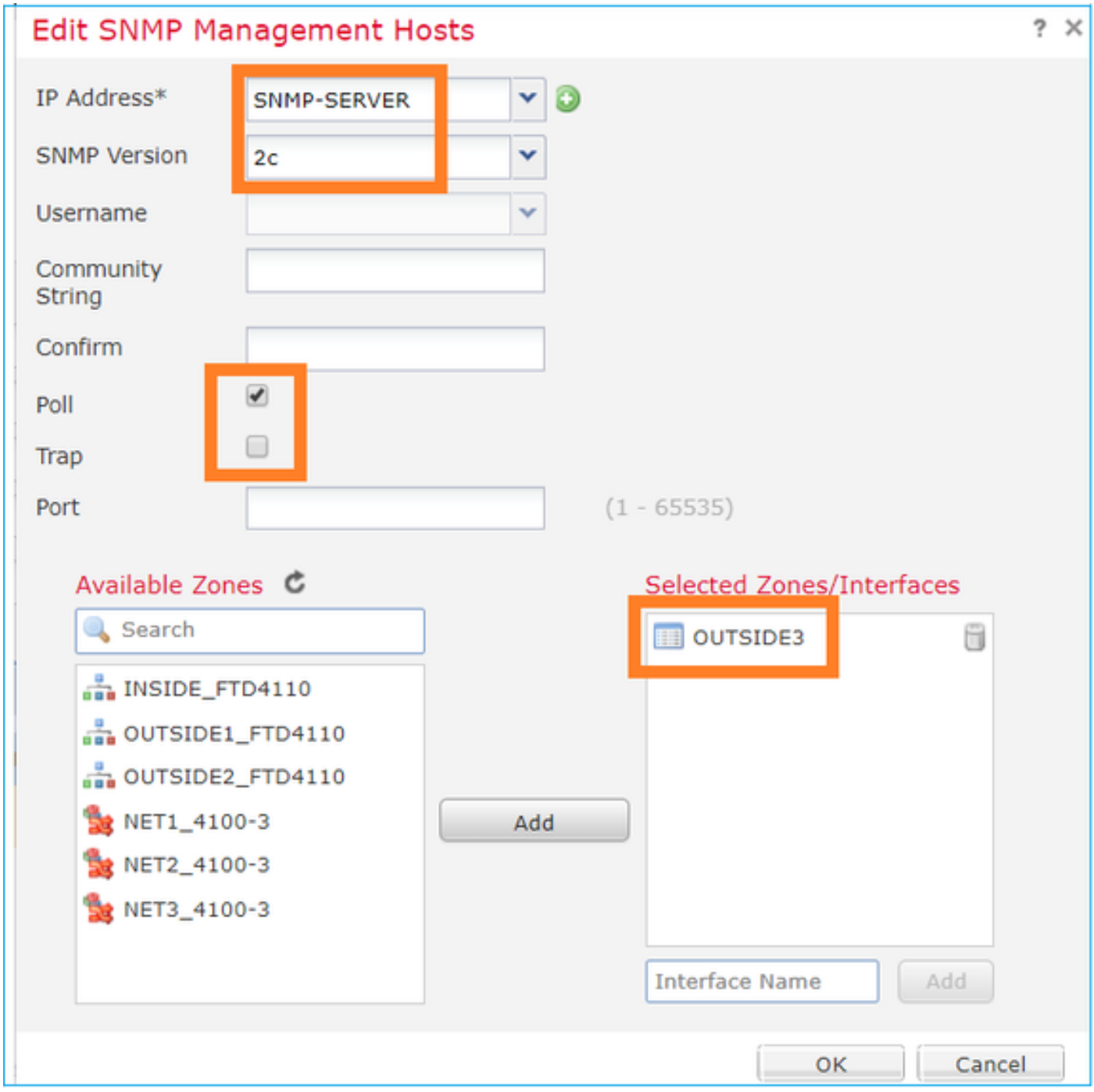
- FPR2100
- FPR1000
- FPR4100

- FPR9300
- ASA5500 الذي يقوم بتشغيل FTD
- FTDv

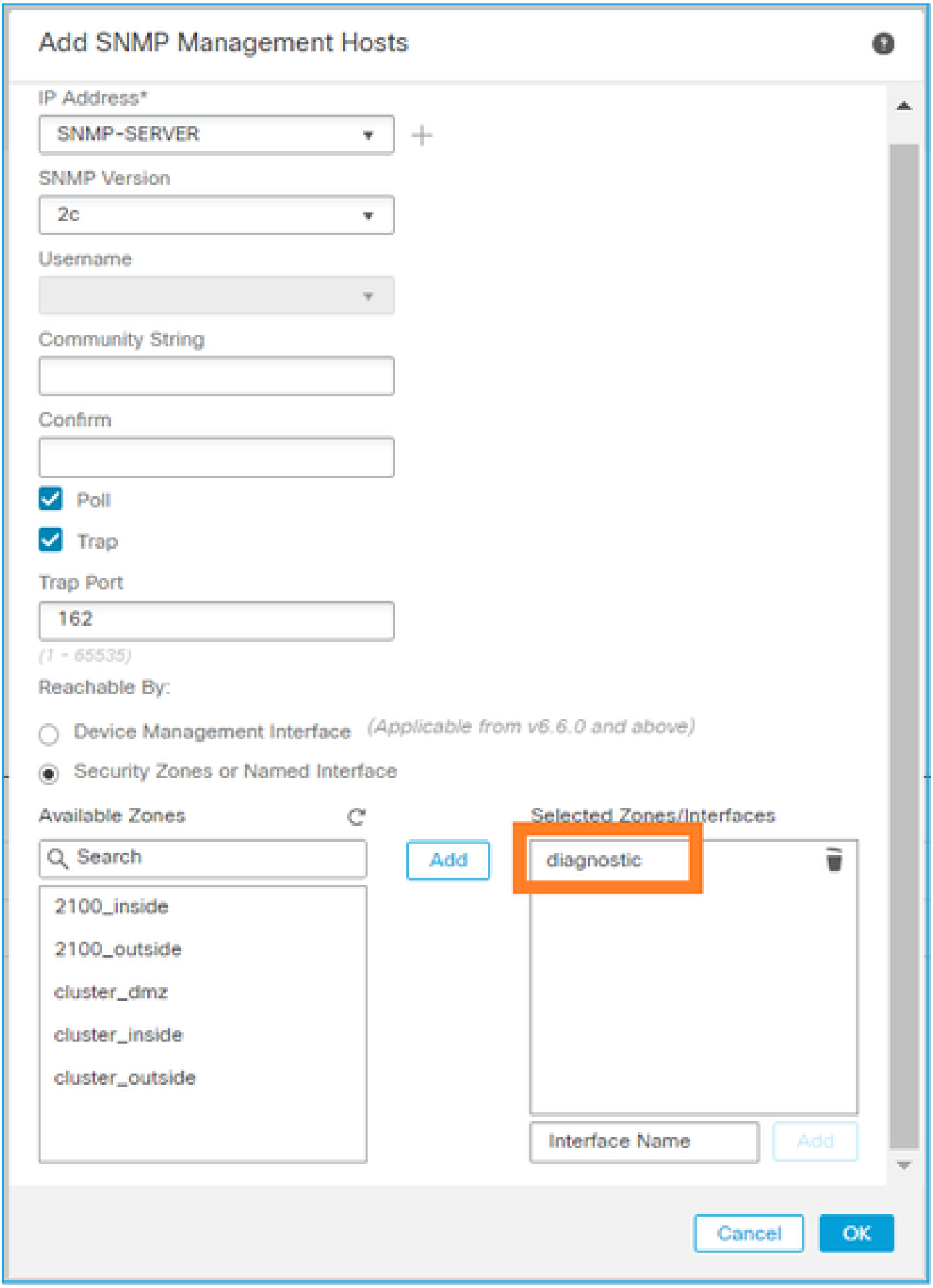
تكوين LINA SNMPv2c

الخطوة 1. على واجهة مستخدم FMC، انتقل إلى الأجهزة > إعدادات النظام الأساسي > SNMP. حدد الخيار 'تمكين خوادم SNMP' وقم بتكوين إعدادات SNMPv2 كما يلي:

الخطوة 2. في علامة التبويب البيئات المضيفة حدد الزر إضافة وحدد إعدادات خادم SNMP:

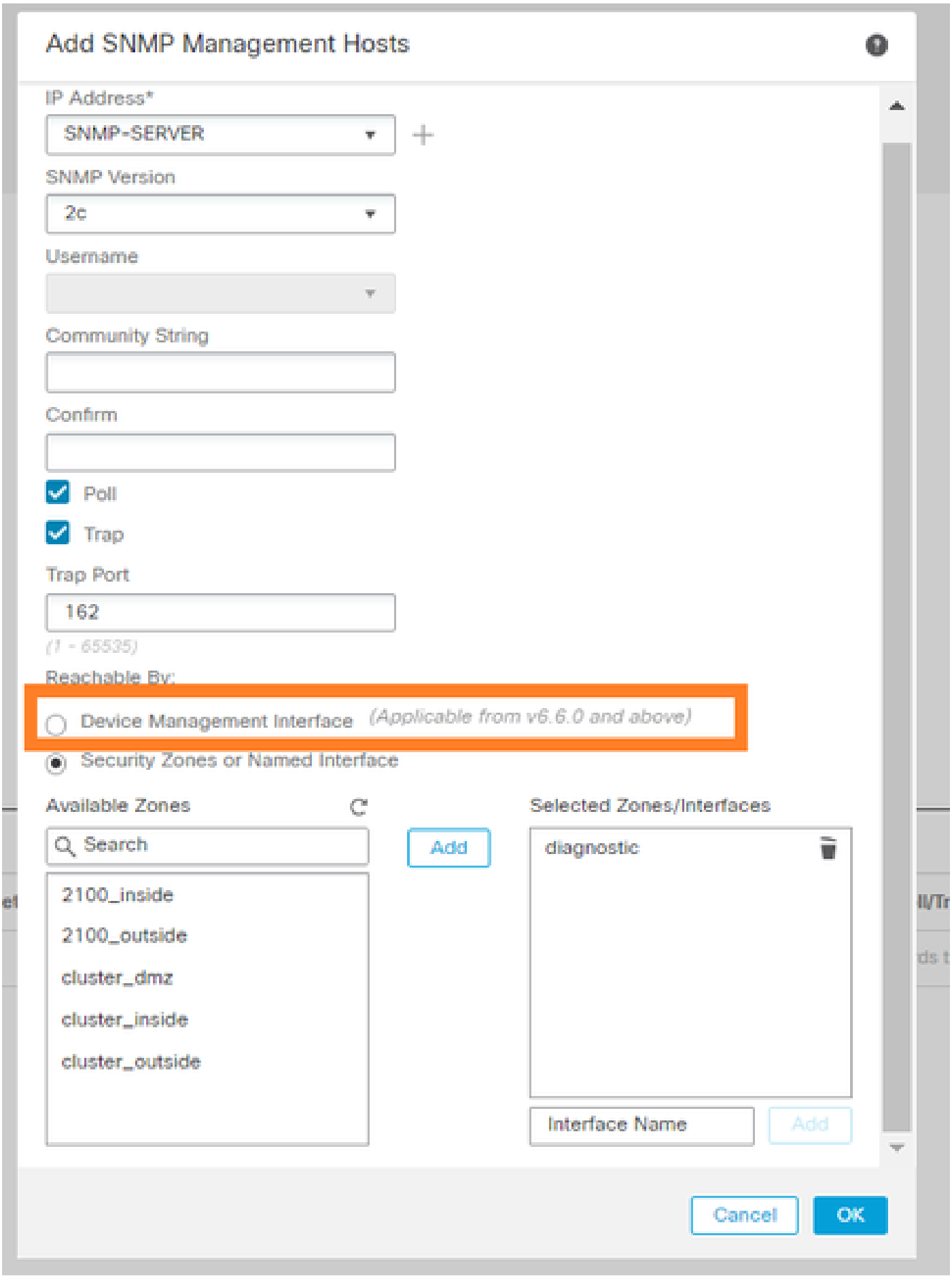



كما يمكنك تحديد واجهة التشخيص كمصدر لرسائل SNMP. الواجهة التشخيصية هي واجهة بيانات تتيح فقط حركة المرور إلى المربع ومن المربع (الإدارة فقط).


Add SNMP Management Hosts
IP Address*
SNMP-SERVER
SNMP Version
2c
Username
Community String
Confirm
Poll
Trap
Trap Port
162
(1 - 65535)
Reachable By:
Device Management Interface
(Applicable from v6.6.0 and above)
Security Zones or Named Interface
Available Zones
Search
2100_inside
2100_outside
cluster_dmz
cluster_inside
cluster_outside
Add
Selected Zones/Interfaces
diagnostic
Interface Name
Add
Cancel
OK

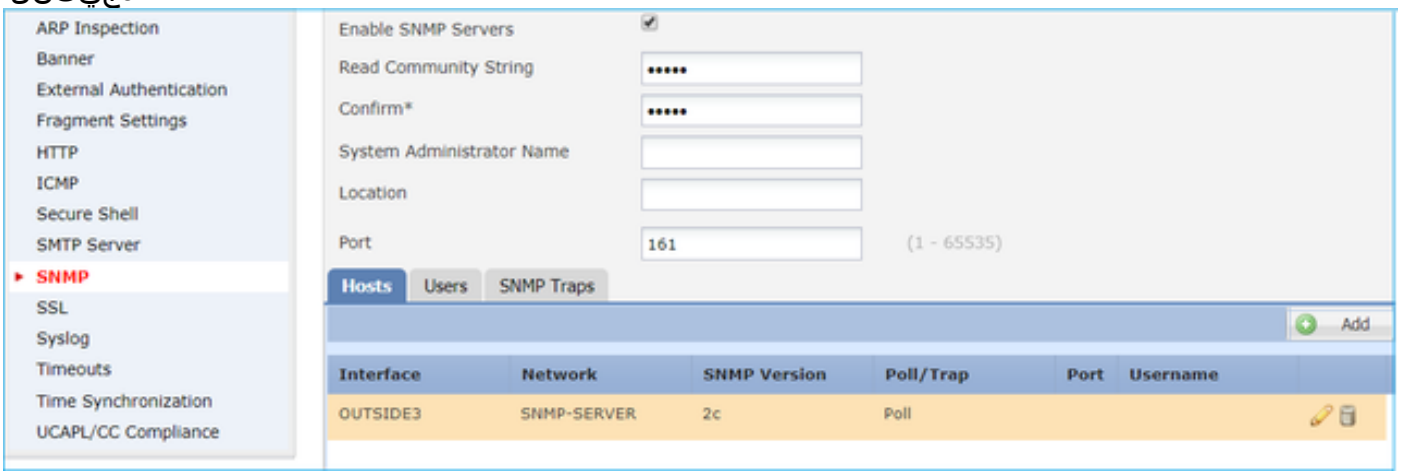
هذه الصورة مأخوذة من الإصدار 6.6 وتستخدم السمة الفاتحة.

بالإضافة إلى ذلك، في إصدارات ما بعد 6.6 FTD، يمكنك أيضاً اختيار واجهة الإدارة:



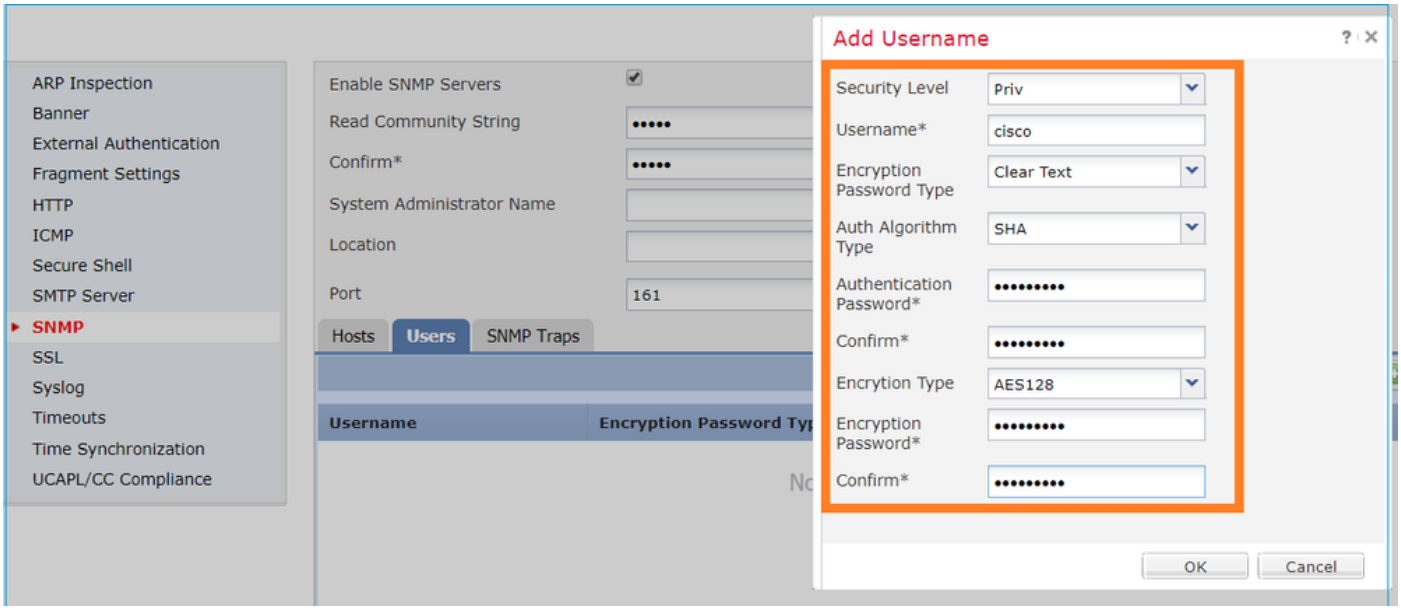

في حالة تحديد واجهة الإدارة الجديدة، يتوفر LINA SNMP عبر واجهة الإدارة.

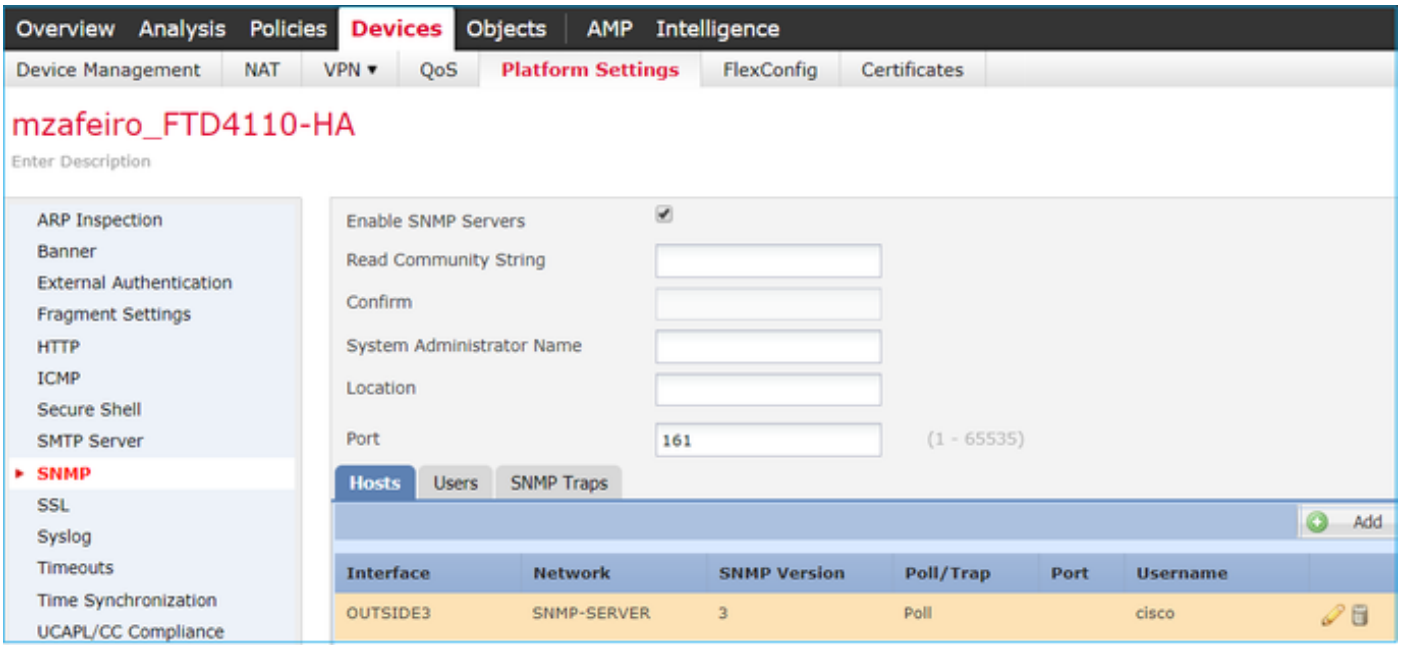
النتيجة:



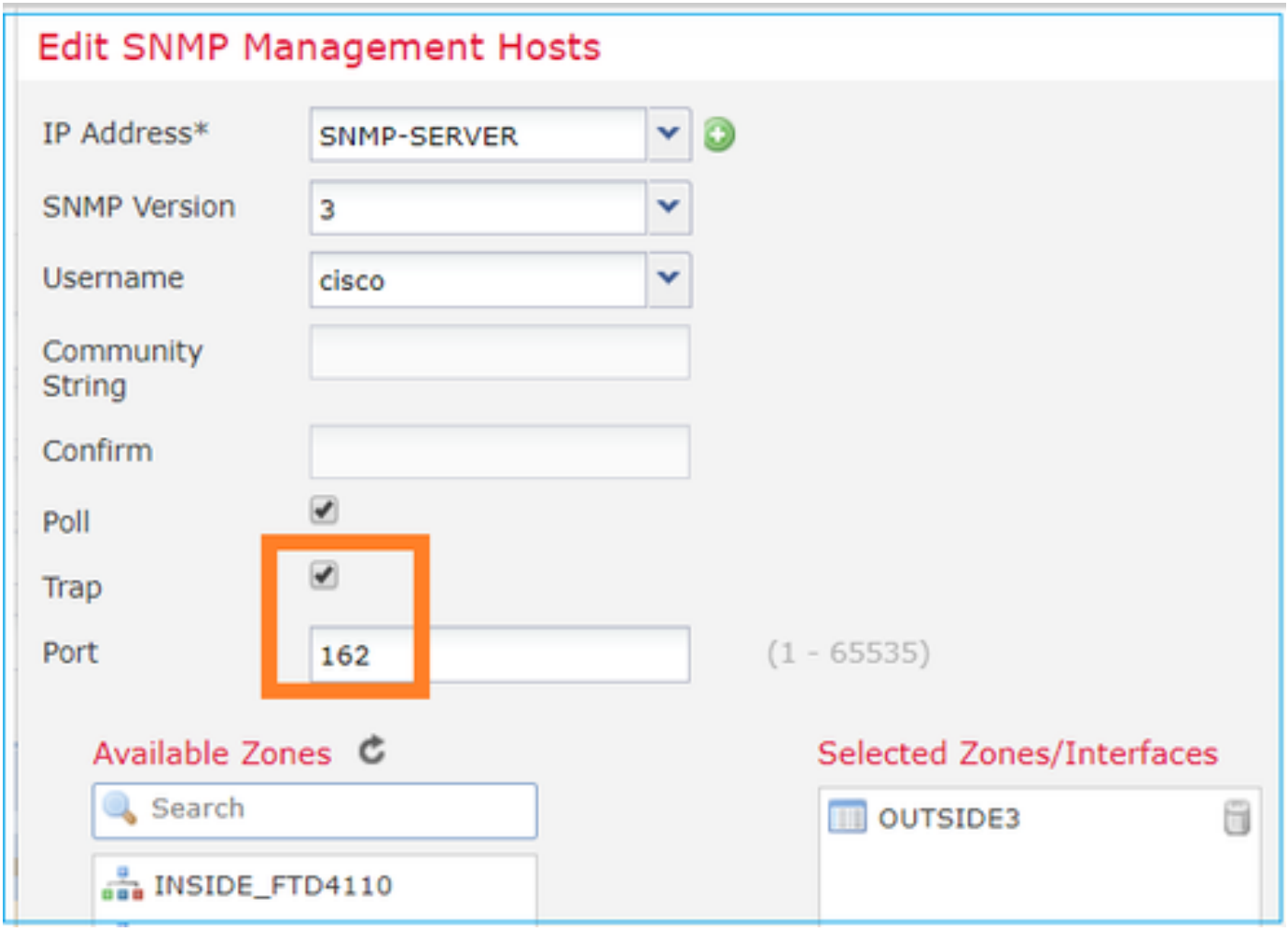

تكوين LINA SNMPv3

الخطوة 1. على واجهة مستخدم FMC، انتقل إلى الأجهزة > إعدادات النظام الأساسي > SNMP. حدد الخيار تمكين خوادم SNMP وتكوين مستخدم ومضيف SNMPv3:

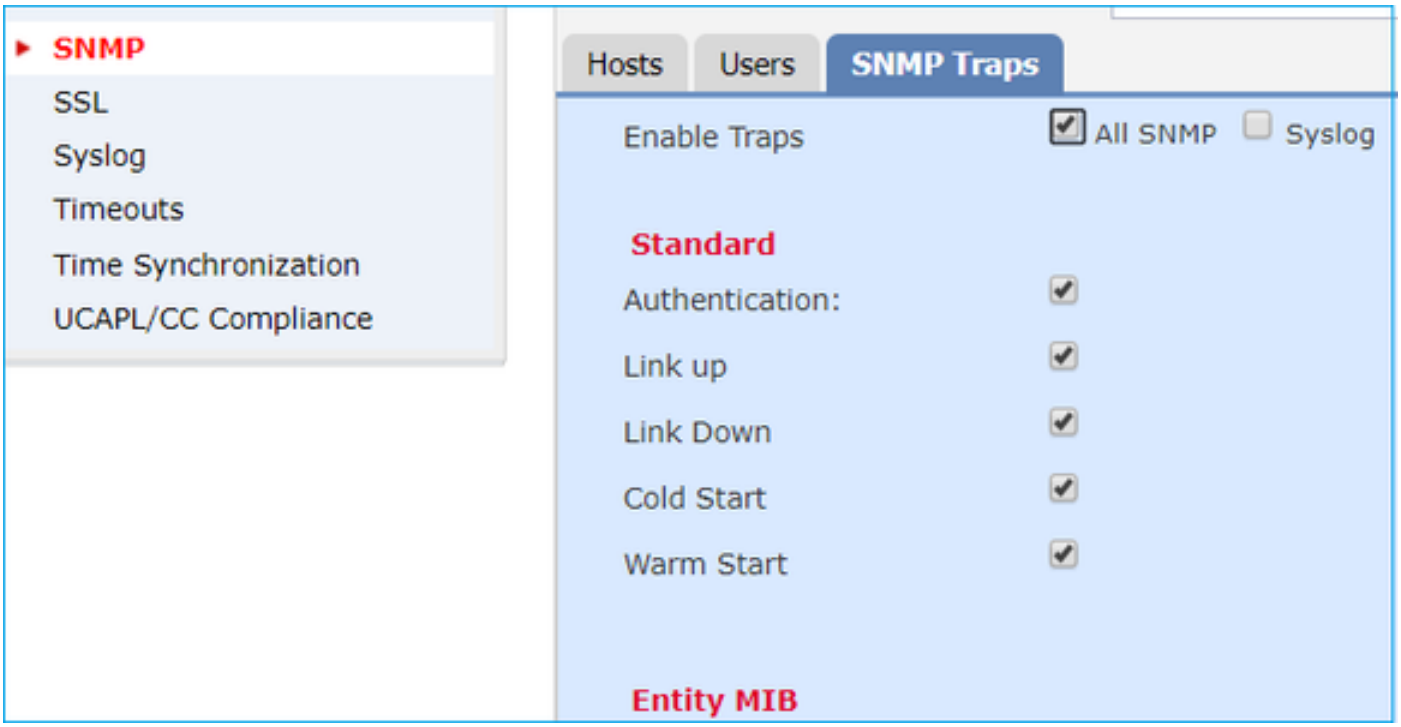





الخطوة 2. قم بتكوين المضيف أيضا لتلقي مصائد:




الخطوة 3. يمكن تحديد المصائد التي تريد إستلامها ضمن قسم مصائد SNMP:




توحيد خادم Blade SNMP من MIO (نظام التشغيل FXOS 2.12.1 و FTD 7.2 و ASA 9.18.1)

سلوك ما قبل 7.2

- في الأنظمة الأساسية التي يبلغ عددها 9300 و 4100، لا تتوفر قواعد معلومات الإدارة (MIB) لبروتوكول SNMP الخاصة بمعلومات الهيكل على بروتوكول SNMP الذي تم تكوينه على تطبيقات FTD/ASA. يلزم تهيئته بشكل منفصل على وحدة الإدخال والإخراج (MIO) عبر مدير الهيكل والوصول إليه بشكل منفصل. MIO هو وحدة الإدارة والإدخال/الإخراج (المشرف).
- يلزم تكوين سياستين منفصلتين لبروتوكول SNMP، واحدة على الخادم النصلي/التطبيق والأخرى على وحدة الإدخال/الإخراج (MIO) لمراقبة بروتوكول SNMP.
- يتم إستخدام المنافذ المنفصلة، بواقع منفذ واحد للخادم النصلي ومنفذ واحد للإدخال/الإخراج (MIO) لمراقبة بروتوكول إدارة شبكة الاتصال البسيط (SNMP) للجهاز نفسه.
- يمكن أن يؤدي هذا إلى إنشاء تعقيد عند محاولة تكوين أجهزة 9300 و 4100 ومراقبتها عبر بروتوكول SNMP.

كيفية عمله مع الإصدارات الأحدث (FXOS 2.12.1 و FTD 7.2 و ASA 9.18.1 أو أعلى)

- من خلال توحيد خادم Blade SNMP لميزة Mio، يمكن للمستخدمين إستطلاع قواعد معلومات الإدارة (MIB) لنظام LINA و MIO عبر واجهات التطبيقات (ASA/FTD).
- يمكن تمكين الميزة أو تعطيلها عبر واجهة سطر الأوامر (CLI) الجديدة الخاصة بوحدة الإدخال/الإخراج (MIO) وواجهة مستخدم وحدة التحكم في الإدارة (FCM) (Chassis mgr).
- الحالة الافتراضية معطلة. وهذا يعني أن وكيل MIO SNMP يعمل كمثيل مستقل. يلزم إستخدام واجهات MIO لاستطلاع قواعد معلومات الإدارة (MIB) الخاصة بالهيكل/DME. وبمجرد تمكين الميزة، يمكن إستخدام واجهات التطبيق لاستطلاع نفس قواعد معلومات الإدارة (MIB).
- يتوفر التكوين على واجهة مستخدم "مدير الهيكل" ضمن إعدادات النظام الأساسي > SNMP > مثيل المؤول، حيث يمكن للمستخدم تحديد مثيل FTD الذي سيقوم

بتجميع/تجميع قواعد معلومات الإدارة (MIB) للهيكل لتقديمه إلى NMS
- تطبيقات ASA/FTD الأصلية و MI مدعومة.
- لا تنطبق هذه الميزة إلا على الأنظمة الأساسية المستندة إلى وحدات الإدخال/الإخراج (FPR9300 و FPR4100).

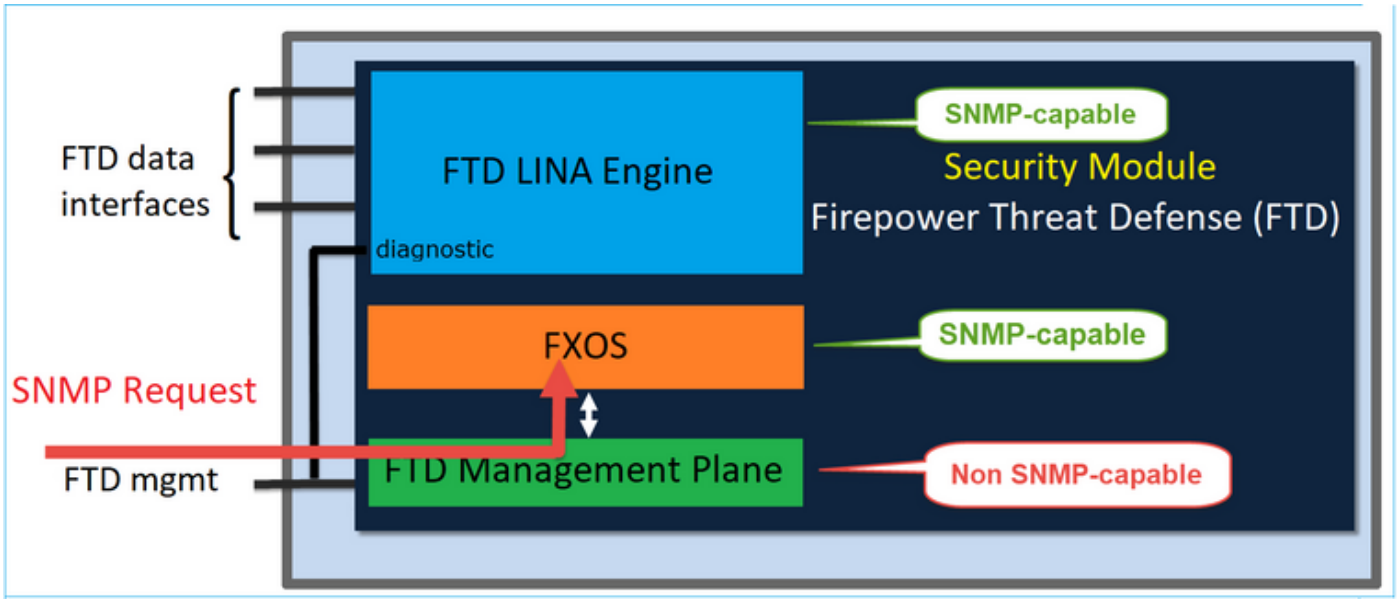
المتطلبات الأساسية والأنظمة الأساسية المدعومة

- الحد الأدنى لإصدار "المدير المدعوم": FCM 2.12.1
- الأجهزة المدارة: سلسلة FPR9300 / FP4100
- الحد الأدنى لإصدار الجهاز المدار المدعوم المطلوب: FXOS 2.12.1 أو FTD 7.2 أو ASA 9.18.1

## بروتوكول إدارة الشبكة البسيط (SNMP) في FPR2100

في أنظمة FPR2100، لا يوجد FCM. الطريقة الوحيدة لتكوين SNMP هي عبر FMC.

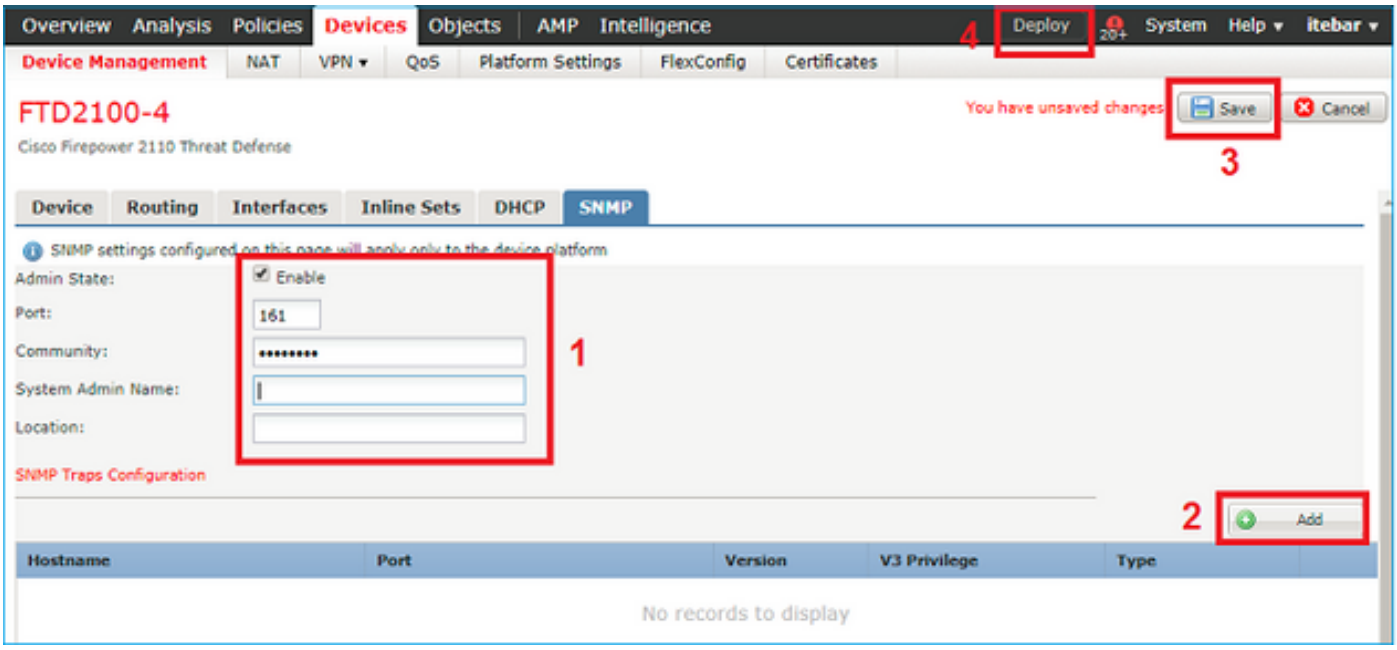
## بروتوكول إدارة الشبكة البسيط (SNMP) للهيكل القاعدي (FXOS) على FPR2100

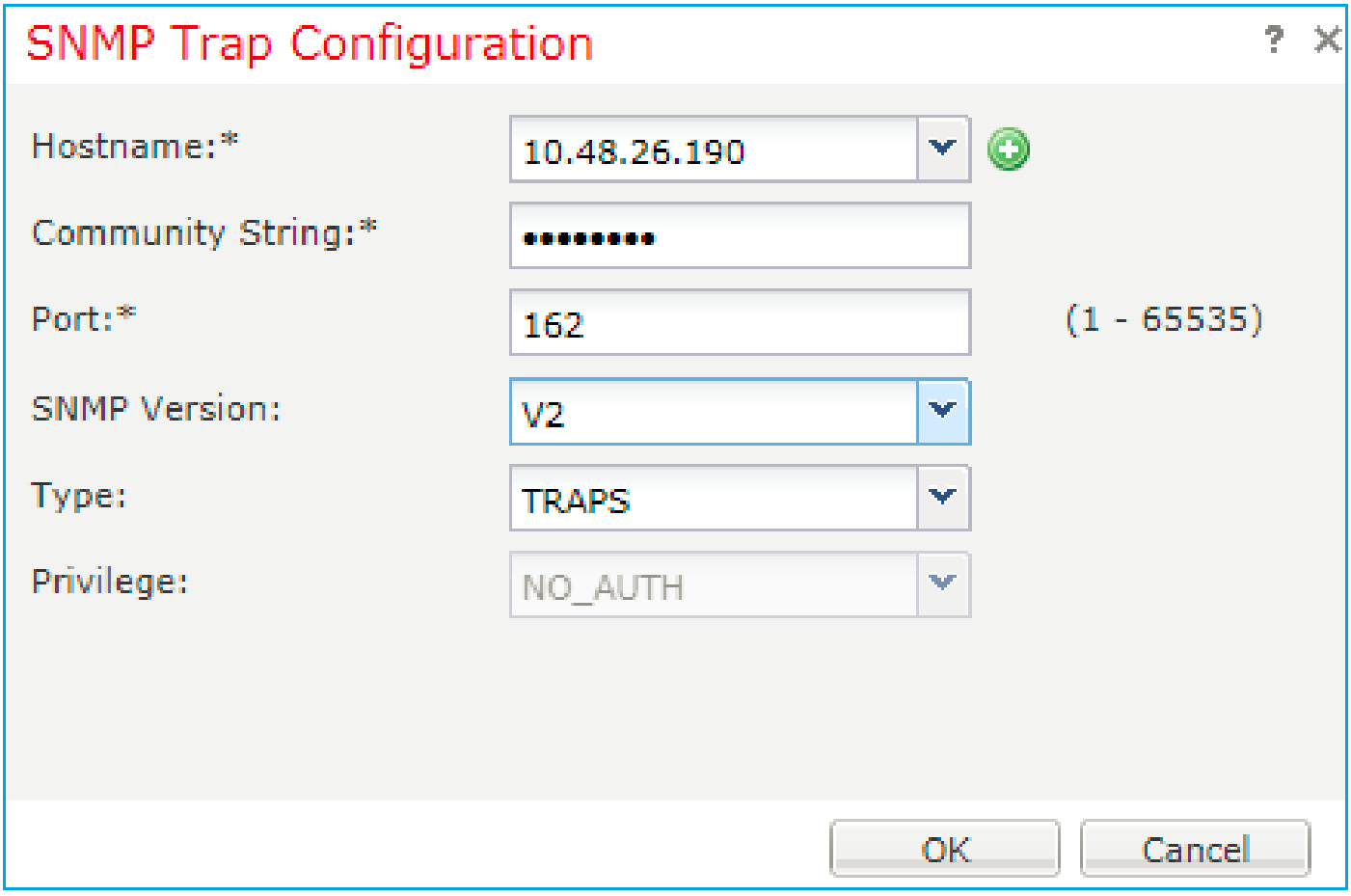



بدءاً من FTD 6.6+، يتوفر لك أيضاً خيار استخدام واجهة إدارة FTD لبروتوكول SNMP. في هذه الحالة، يتم نقل معلومات كل من FXOS وLINA SNMP من خلال واجهة إدارة FTD.

تكوين FXOS SNMPv1/v2c

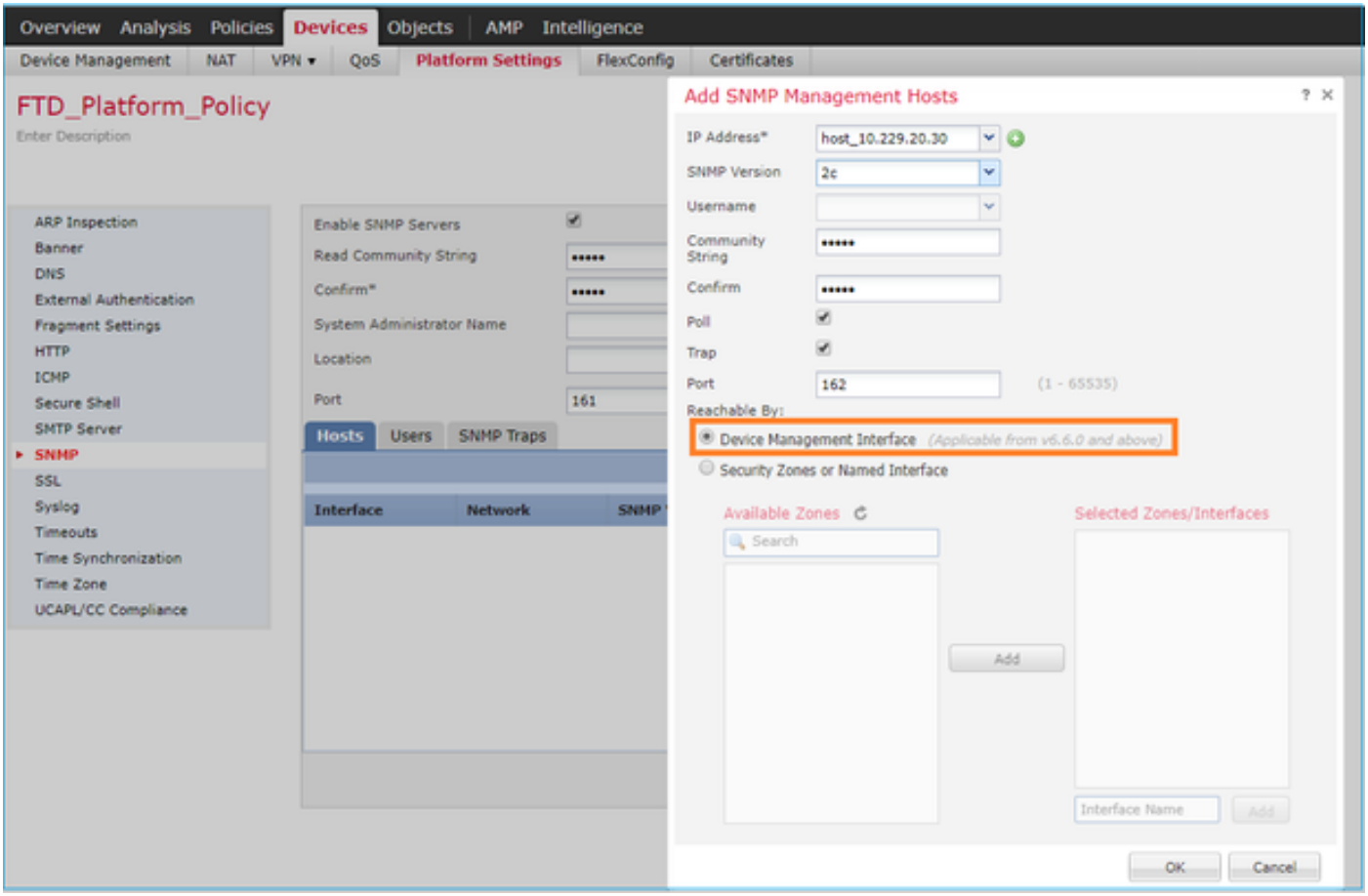
افتح واجهة مستخدم FMC وانتقل إلى الأجهزة > إدارة الأجهزة. حدد الجهاز وحدد بروتوكول SNMP:




التغيير في FTD 6.6+

يمكنك تحديد واجهة إدارة FTD:

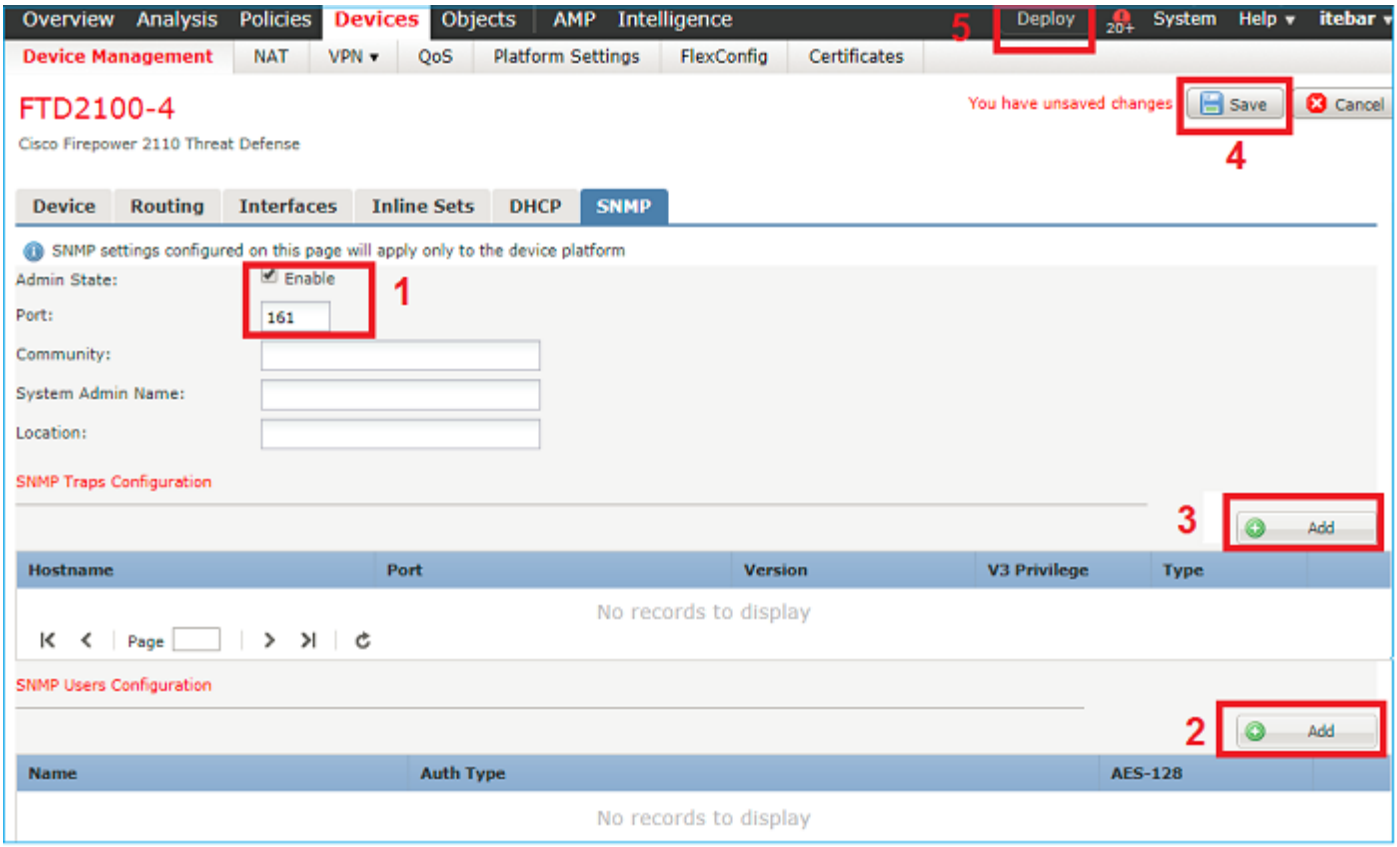


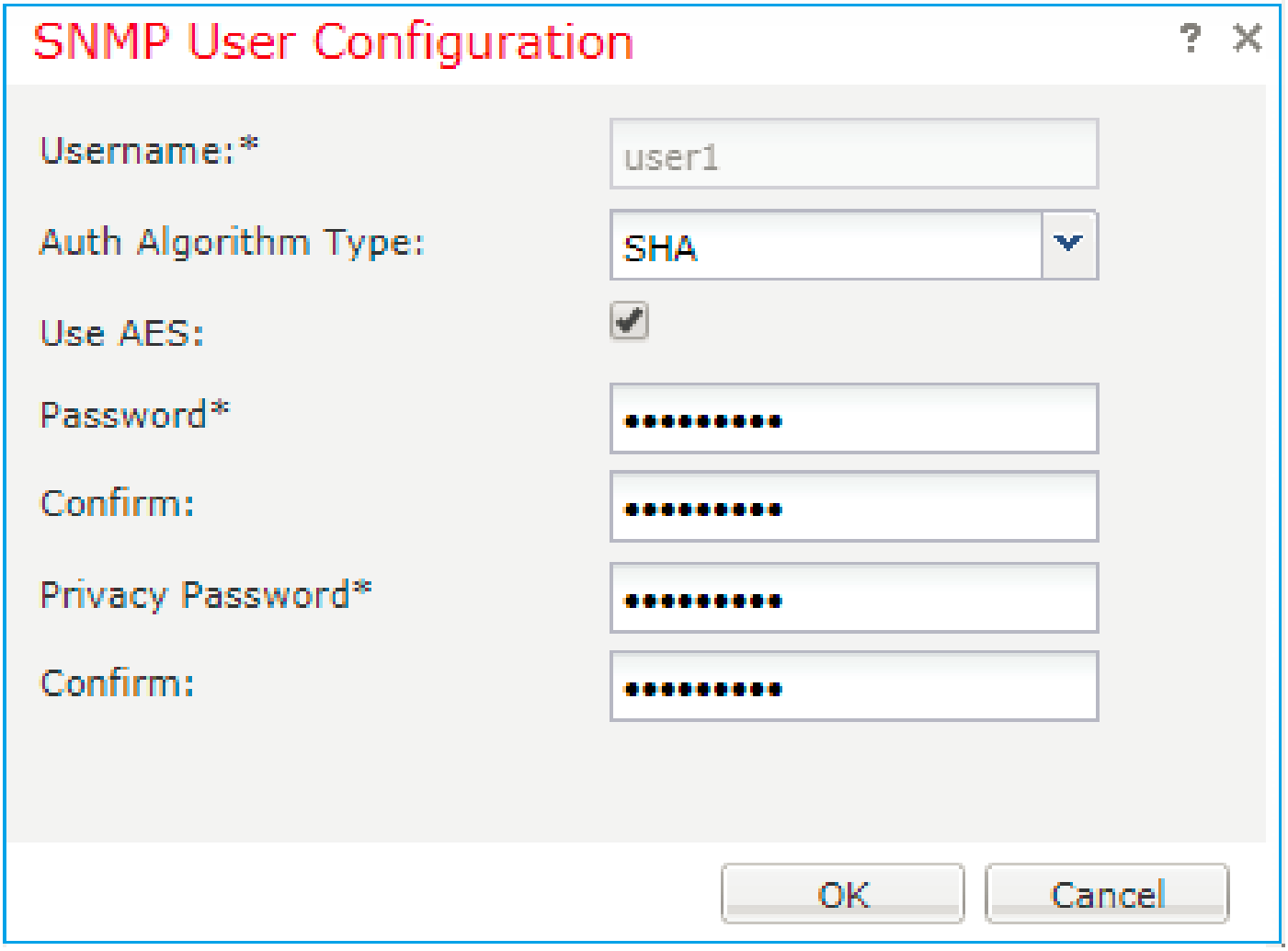

ونظرًا لأنه يمكن أيضًا تكوين واجهة الإدارة لبروتوكول SNMP، فإن الصفحة تعرض رسالة التحذير هذه:

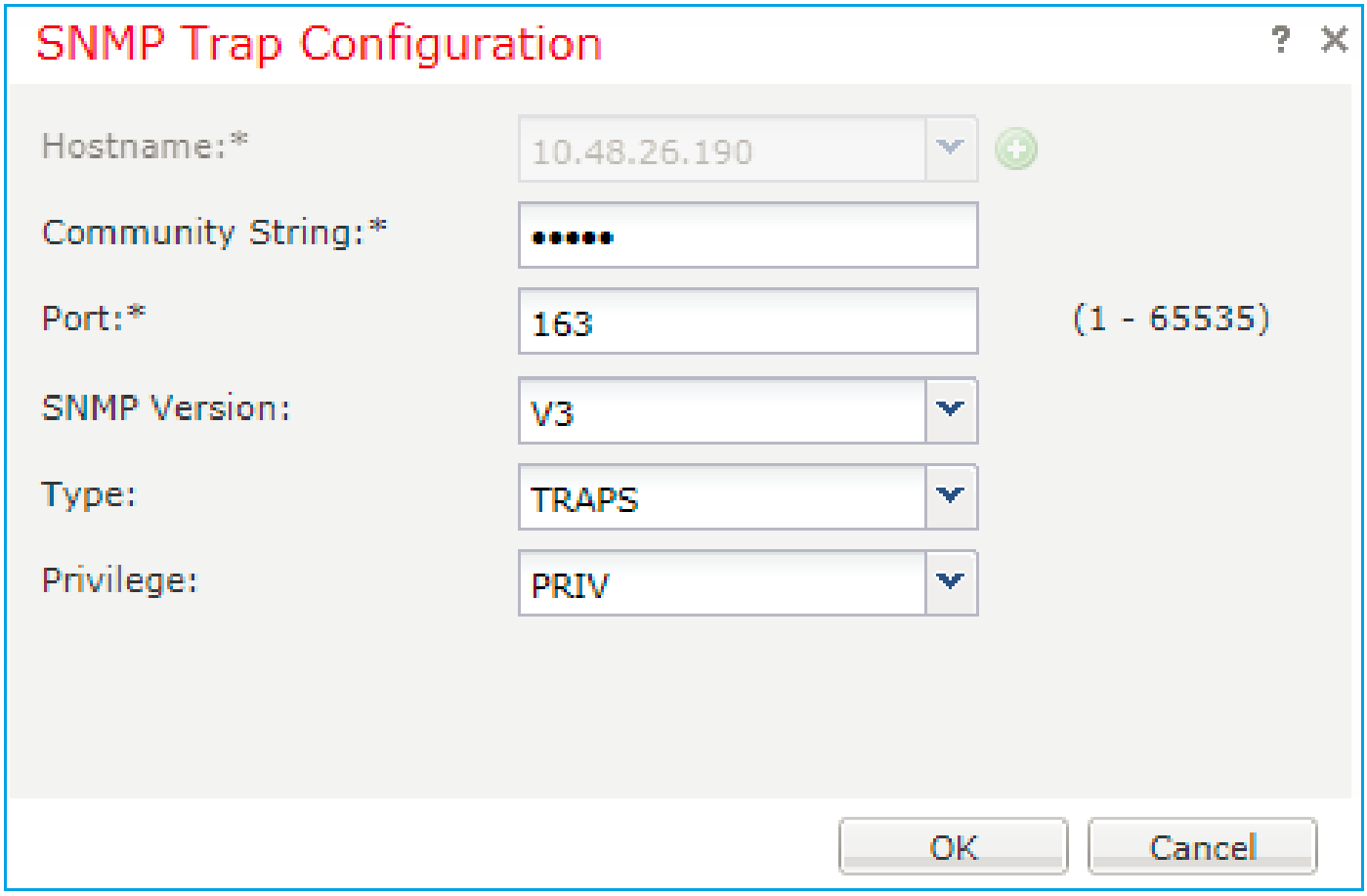
يتم تعطيل تكوين SNMP للنظام الأساسي للجهاز على هذه الصفحة، إذا تم تكوين إعدادات SNMP باستخدام واجهة إدارة الأجهزة من خلال الأجهزة > إعدادات النظام الأساسي (الدفاع عن التهديد) > SNMP > الأجهزة المضيفة.

تكوين FXOS SNMPv3

افتح واجهة مستخدم FMC وانتقل لاختيار الأجهزة > إدارة الأجهزة. أختر الجهاز وحدد بروتوكول SNMP.

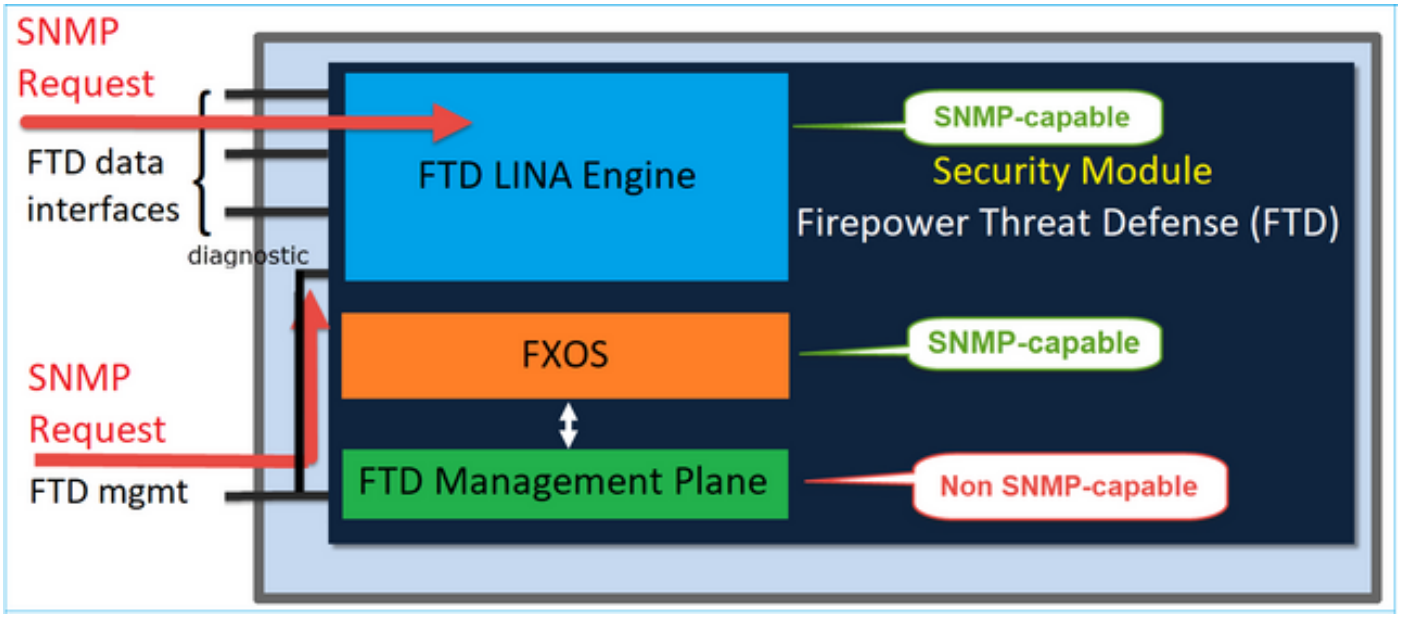

Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
5
Deploy
System
Help
itebar
Device Management
NAT
VPN
QoS
Platform Settings
FlexConfig
Certificates
FTD2100-4
Cisco Firepower 2110 Threat Defense
You have unsaved changes
Save
Cancel
4
Device
Routing
Interfaces
Inline Sets
DHCP
SNMP
SNMP settings configured on this page will apply only to the device platform
Admin State:
Enable
Port:
161
1
Community:
System Admin Name:
Location:
SNMP Traps Configuration
3
Add
Hostname
Port
Version
V3 Privilege
Type
No records to display
Page
SNMP Users Configuration
2
Add
Name
Auth Type
AES-128
No records to display


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



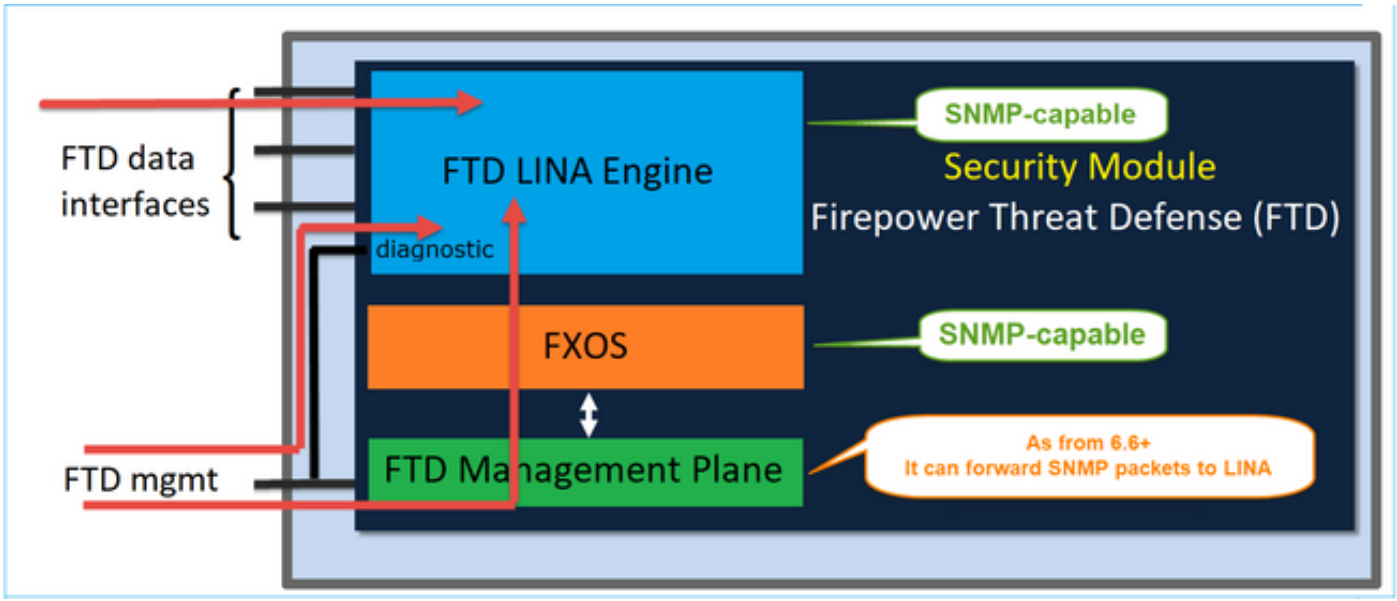

## بروتوكول إدارة الشبكة البسيط (SNMP) لـ FTD (LINA) على FPR2100

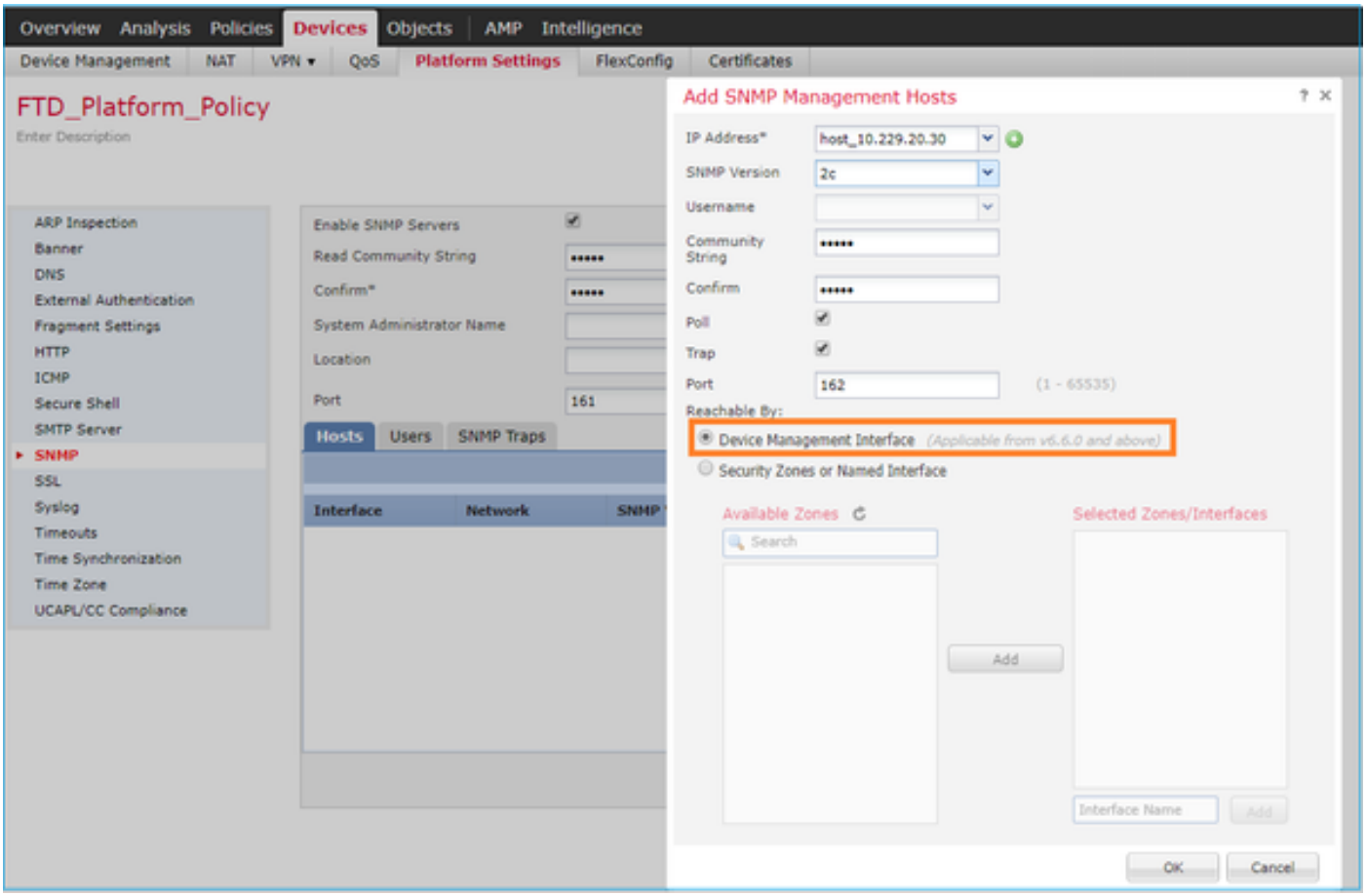
- بالنسبة لإصدارات ما قبل 6.6، يكون تكوين بروتوكول SNMP الخاص بـ LINA FTD على أجهزة FTD FP1xxx/FP21xx مطابقًا لـ FTD على جهاز FirePower 4100 أو 9300.




### إصدارات FTD 6.6+

- في إصدارات ما بعد 6.6، يكون لديك أيضًا خيار استخدام واجهة إدارة FTD لاستطلاعات رأي ورسائل تنبيه LINA.



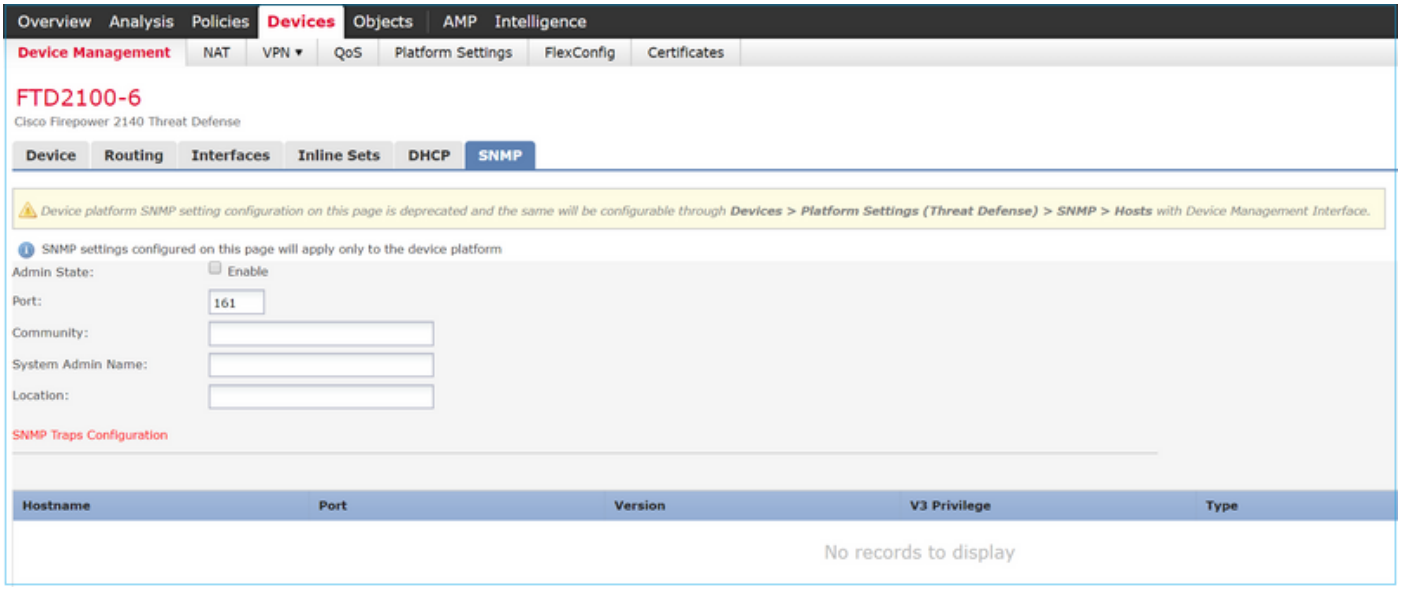




في حال لم يتم تحديد واجهة الإدارة الجديدة:

- يتوفر LINA SNMP عبر واجهة الإدارة.
- ضمن الأجهزة > إدارة الأجهزة، يتم تعطيل علامة التبويب SNMP لأنها لم تعد مطلوبة. يتم عرض شعار إعلام. كانت علامة تبويب جهاز SNMP مرئية فقط على الأنظمة الأساسية 2100/1100. لا توجد هذه الصفحة على الأنظمة الأساسية FPR9300/FPR4100

وFTD55xx.

بمجرد تكوينها، يصبح LINA SNMP بالإضافة إلى FXOS مدمجين (على FP1xxx/FP2xxx) معلومات الاستقصاء/رسائل تنبيه SNMP عبر واجهة إدارة FTD.




يتم دعم ميزة إدارة عنوان IP الفردي لبروتوكول SNMP من 6.6 فصاعدًا على جميع الأنظمة الأساسية لـ FTD:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 الذي يقوم بتشغيل FTD
- FTDv

لمزيد من التفاصيل، تحقق من تكوين SNMP للدفاع ضد التهديدات

# التحقق من الصحة

التحقق من بروتوكول إدارة الشبكة البسيط (SNMP) الخاص بـ FXOS لـ FPR4100/FPR9300

عمليات التحقق من FXOS SNMPv2c

التحقق من تكوين واجهة سطر الأوامر (CLI):

```
<#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
```

من وضع 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
```

عمليات التحقق الإضافية:

```
<#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

...
```

اختبار طلبات SNMP.

قم بتنفيذ طلب SNMP من مضيف صالح.

تأكيد إنشاء رسائل التنبيه.

يمكنك استخدام قلب واجهة مع تمكين أداة التحليل ethanalyzer لتأكيد إنشاء رسائل تنبيه SNMP وإرسالها إلى الأجهزة المضيفة لرسائل التنبيه المحددة:

```
<#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
```

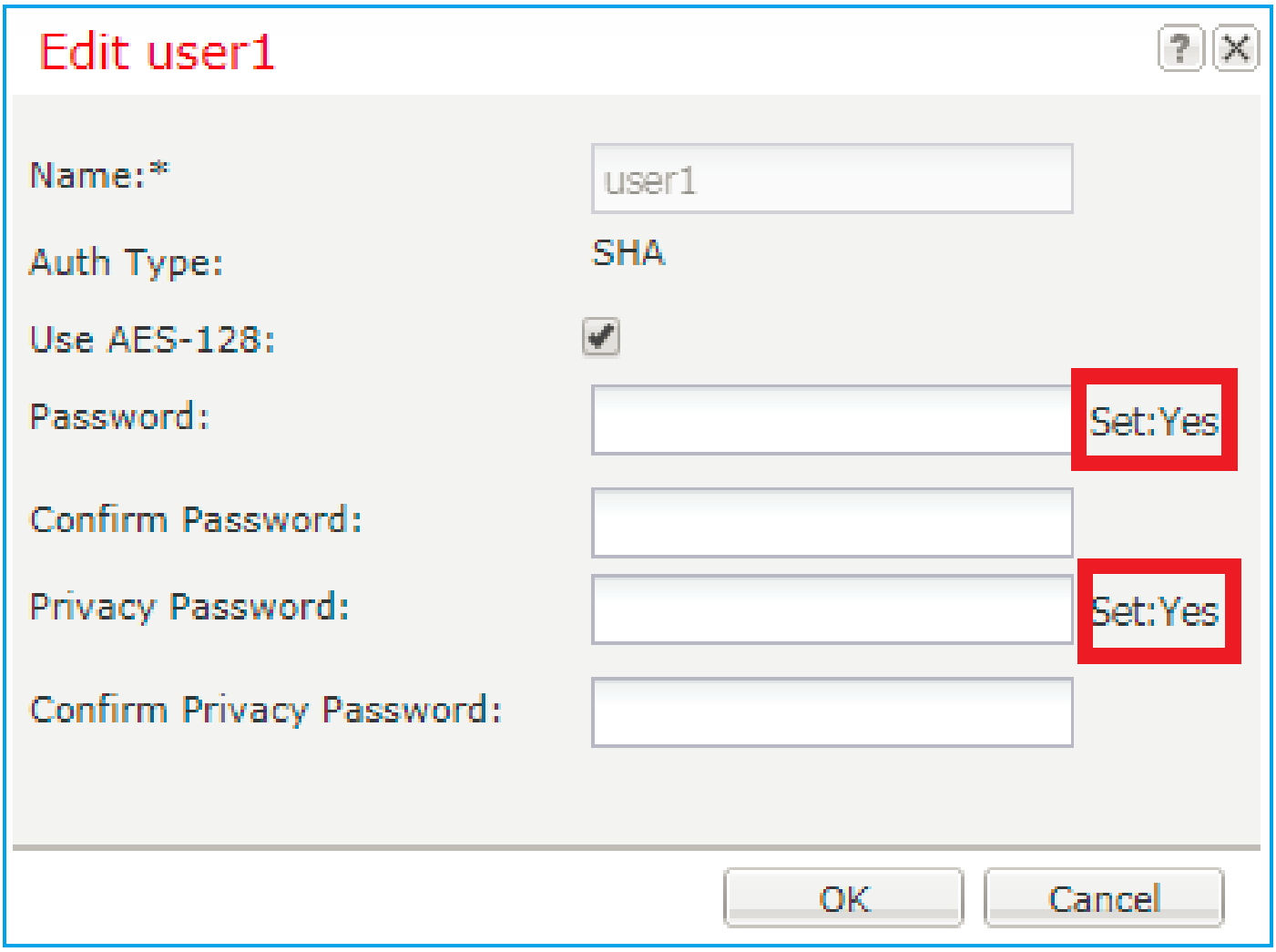
---

تحذير: يمكن أن يتسبب رفرفة واجهة في انقطاع حركة المرور. قم بإجراء هذا الاختبار في بيئة معملية فقط أو في نافذة الصيانة

---

عمليات التحقق من FXOS SNMPv3

الخطوة 1. فتح إعدادات النظام الأساسي لواجهة مستخدم FCM > SNMP > إذا ظهر المستخدم وخصوصية مرور كلمة أي تم تكوين ما:




الخطوة 2. في واجهة سطر الأوامر (CLI)، يمكنك التحقق من تكوين SNMP تحت مراقبة النطاق:

```
<#root>

ksec-fpr9k-1-A /monitoring #

show snmp

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

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

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

ksec-fpr9k-1-A /monitoring #

show snmp-user detail
```

```
SNMPv3 User:
    Name: user1
    Authentication type: Sha
    Password: ****
    Privacy password: ****
    Use AES-128: Yes

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

**show snmp-trap**

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

الخطوة 3. تحت وضع FXOS، يمكنك توسيع تكوين SNMP والتفاصيل:

<#root>

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

**show running-config snmp all**

```
…
snmp-server user user1 network-operator auth sha 0x022957ee4690a01f910f1103433e4b7b07d4b5fc priv aes-12
snmp-server host 192.168.10.100 traps version 3 priv user1

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

**show snmp user**

```
_____________________________________________________________
                   SNMP USERS
_____________________________________________________________

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

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

User                          Auth  Priv
____                          ____  ____

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

**show snmp host**

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

اختبار طلبات SNMP.

يمكنك التحقق من التكوين وتنفيذ طلب SNMP من أي جهاز مزوّد بقدرات SNMP.

للتحقق من كيفية معالجة طلب SNMP، يمكنك استخدام تصحيح أخطاء SNMP:

```
<#root>

ksec-fpr9k-1-A(fxos)#

 debug snmp pkt-dump

ksec-fpr9k-1-A(fxos)# 2017 Oct 16 17:11:54.681396 snmpd: 1281064976.000000:iso.10.10.1.1.10.10.10.10.1 =
2017 Oct 16 17:11:54.681833 snmpd:  SNMPPKTSTRT: 3.000000 161 1281064976.000000 1647446526.000000 0.000
2017 Oct 16 17:11:54.683952 snmpd: 1281064976.000000:iso.10.10.1.2.10.10.10.10.2.83886080 = STRING: "mg
2017 Oct 16 17:11:54.684370 snmpd:  SNMPPKTSTRT: 3.000000 162 1281064976.000000 1647446526.000000 0.000
```

⚠ تحذير: يمكن أن يؤثر تصحيح الأخطاء على أداء الجهاز.

## التحقق من بروتوكول إدارة الشبكة البسيط (SNMP) الخاص بـ FXOS لـ FPR2100

عمليات التحقق من FXOS SNMPv2

تحقق من التكوين عبر واجهة سطر الأوامر (CLI):

```
<#root>

FP2110-4 /monitoring #

 show snmp

Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact:
    Sys Location:
FP2110-4 /monitoring #

show snmp-trap


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

أكّد سلوك SNMP.

يمكنك التحقق من قدرتك على الاستعلام عن FXOS وإرسال طلب SNMP من جهاز مضيف أو أي جهاز مزوّد بقدرات SNMP.

استخدم الأمر capture-traffic للاطّلاع على طلب SNMP والاستجابة له:

```
<#root>

>

capture-traffic


Please choose domain to capture traffic from:
  0 - management0

Selection?

0


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes
13:50:50.521383 IP 10.48.26.190.42224 > FP2110-4.snmp:  C=cisco123 GetNextRequest(29)  interfaces.ifTab
13:50:50.521533 IP FP2110-4.snmp > 10.48.26.190.42224:  C=cisco123 GetResponse(32)  interfaces.ifTable.
^C
Caught interrupt signal

Exiting.

2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

## عمليات التحقق من FXOS SNMPv3

تحقق من التكوين عبر واجهة سطر الأوامر (CLI):

```
<#root>

FP2110-4 /monitoring #

show snmp

Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: No
    Sys Contact:
    Sys Location:
FP2110-4 /monitoring #
```

```
show snmp-user detail


SNMPv3 User:
    Name: user1
    Authentication type: Sha
    Password: ****
    Privacy password: ****
    Use AES-128: Yes
FP2110-4 /monitoring #
```

```
show snmp-trap detail


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

أكّد سلوك SNMP.

أرسل طلب SNMP للتحقق من قدرتك على الاستعلام عن FXOS.

بالإضافة إلى ذلك، يمكنك تسجيل الطلب:

```
<#root>

>

capture-traffic


Please choose domain to capture traffic from:
  0 - management0

Selection?

0


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes
14:07:24.016590 IP 10.48.26.190.38790 > FP2110-4.snmp:  F=r U= E=  C= [|snmp]
14:07:24.016851 IP FP2110-4.snmp > 10.48.26.190.38790:  F= [|snmp][|snmp]
14:07:24.076768 IP 10.48.26.190.38790 > FP2110-4.snmp:  F=apr [|snmp][|snmp]
14:07:24.077035 IP FP2110-4.snmp > 10.48.26.190.38790:  F=ap [|snmp][|snmp]
^C4 packets captured
Caught interrupt signal

Exiting.
```

```
4 packets received by filter
0 packets dropped by kernel
```

## التحقق من بروتوكول إدارة الشبكة البسيط (SNMP) الخاص بـ FTD

للتحقق من تكوين بروتوكول SNMP الخاص بـ 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 *****
```

في إصدارات ما بعد FTD 6.6، يمكنك تكوين واجهة إدارة FTD لبروتوكول SNMP واستخدامها:

```
<#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
```

تحقق إضافي:

```
<#root>

Firepower-module1#

show snmp-server host

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

من واجهة سطر أوامر خادم SNMP، شغّل 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
...
```

التحقق من إحصائيات حركة مرور SNMP.

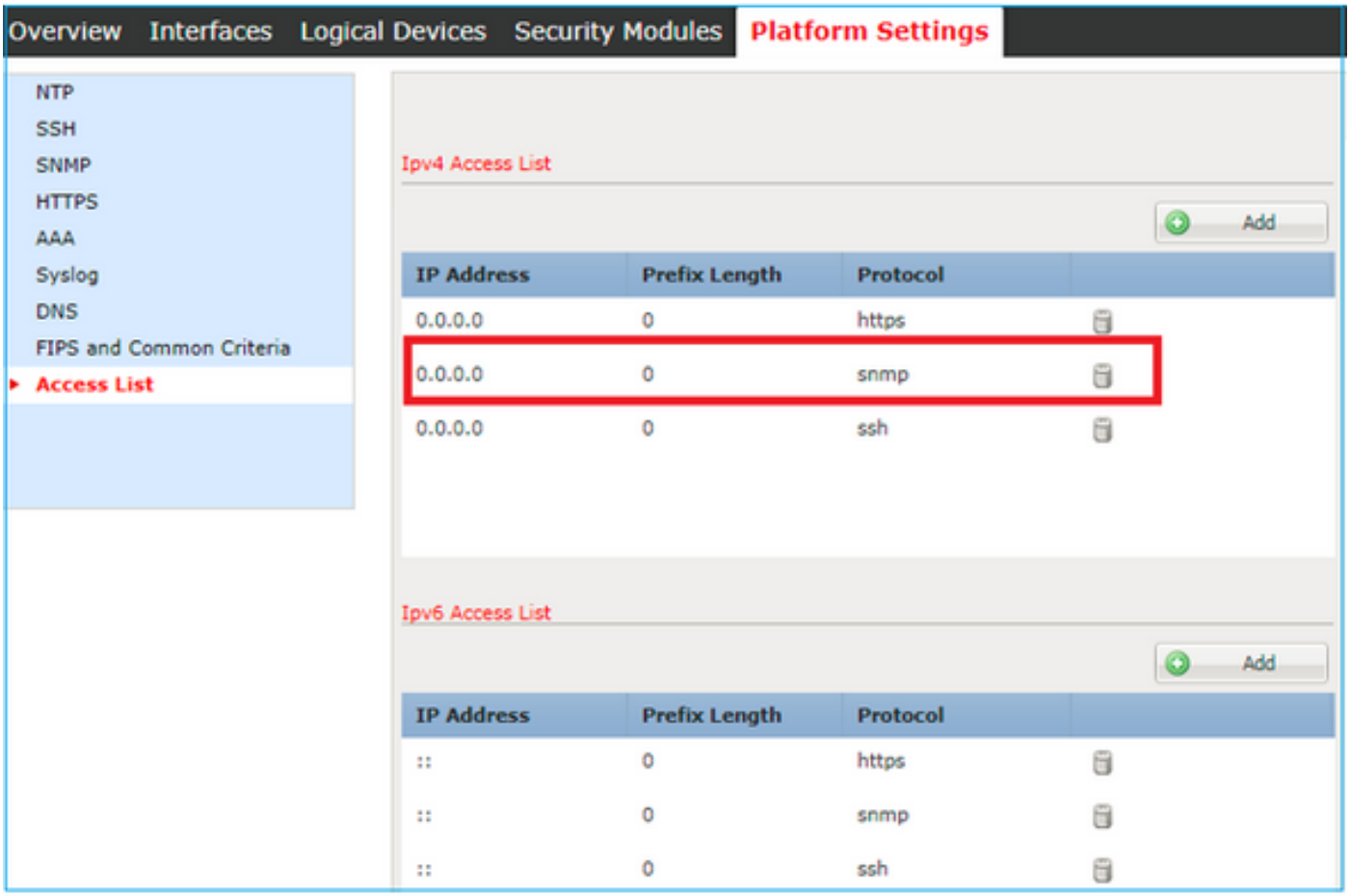
<#root>

```
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
```

السماح بحركة مرور SNMP إلى FXOS على FPR4100/FPR9300

يمكن لتكوين FXOS على FPR4100/9300 تقييد وصول SNMP لكل عنوان IP مصدر. يحدد قسم تكوين قائمة الوصول أي الشبكات/الأجهزة المضيفة قادرة على الوصول إلى الجهاز عبر SSH أو HTTPS أو SNMP. إنك تحتاج إلى التأكد من السماح باستعلامات SNMP من خادم SNMP.

تكوين قائمة الوصول العالمية عبر واجهة المستخدم الرسومية




تكوين قائمة الوصول العالمية عبر واجهة سطر الأوامر (CLI)

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

التحقق

<#root>

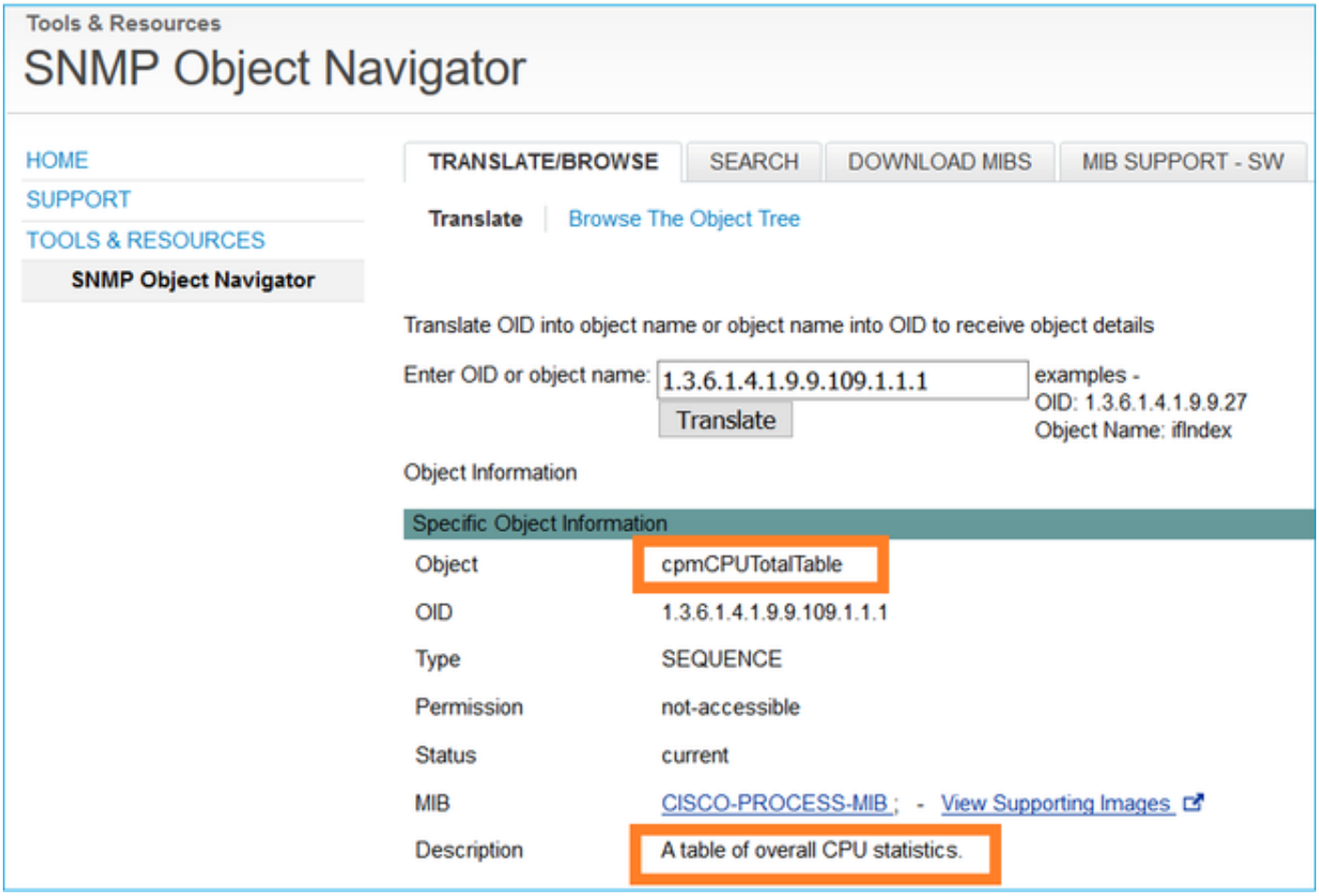
```
ksec-fpr9k-1-A /system/services #
```

**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
```

## استخدام OID Object Navigator

Cisco SNMP Object Navigator هي أداة عبر الإنترنت يمكنك من خلالها ترجمة معرّفات الكائن المختلفة والحصول على وصف قصير.




استخدم الأمر show snmp-server oid من واجهة سطر أوامر FTD LINA لاسترداد القائمة الكاملة لمعرّفات LINA التي يمكن الاستعلام عنها.

```
<#root>

>

system support diagnostic-cli


firepower#

show snmp-server oid


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

ملاحظة: الأمر مخفي.

## استكشاف الأخطاء وإصلاحها

هذه هي مولدات حالة SNMP الأكثر شيوعاً التي يراها مركز الدعم الفني من Cisco:

1. تعذّر إجراء الاستقصاء عن برنامج إدارة الشبكة البسيط (SNMP) لـ FTD LINA
2. تعذّر إجراء الاستقصاء عن FXOS SNMP
3. ما قيمة SNMP OID المطلوب استخدامها؟
4. لا يمكن الحصول على رسائل تنبيه SNMP
5. لا يمكن مراقبة FMC عبر SNMP
6. تعذّر تكوين SNMP
7. تكوين SNMP في FirePower Device Manager

### تعذّر إجراء الاستقصاء عن برنامج إدارة الشبكة البسيط (SNMP) لـ FTD LINA

أوصاف المشكلة (نموذج من حالات Cisco TAC الحقيقية):

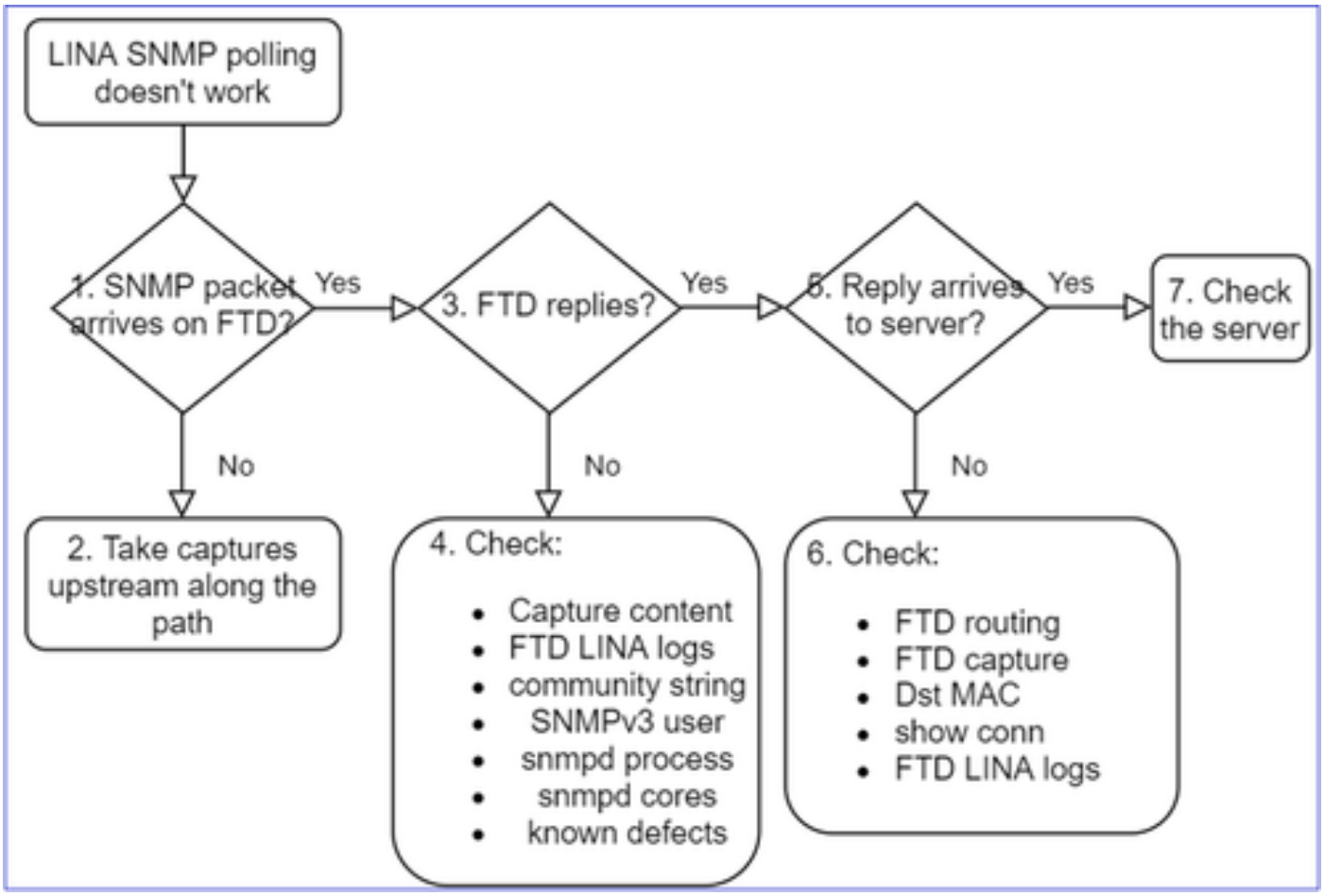
- "تعذّر جلب البيانات عبر SNMP."
- "تعذّر الاستعلام عن الجهاز عبر SNMPv2."
- "SNMP لا يعمل. نريد مراقبة جدار الحماية باستخدام SNMP ولكن بعد التكوين، واجه

مشكلات."

- "ديناان نظامان للمراقبة غير قادرين على مراقبة FTD عبر SNMP v2c أو 3."
- "لا يعمل بروتوكول SNMP على جدار الحماية."

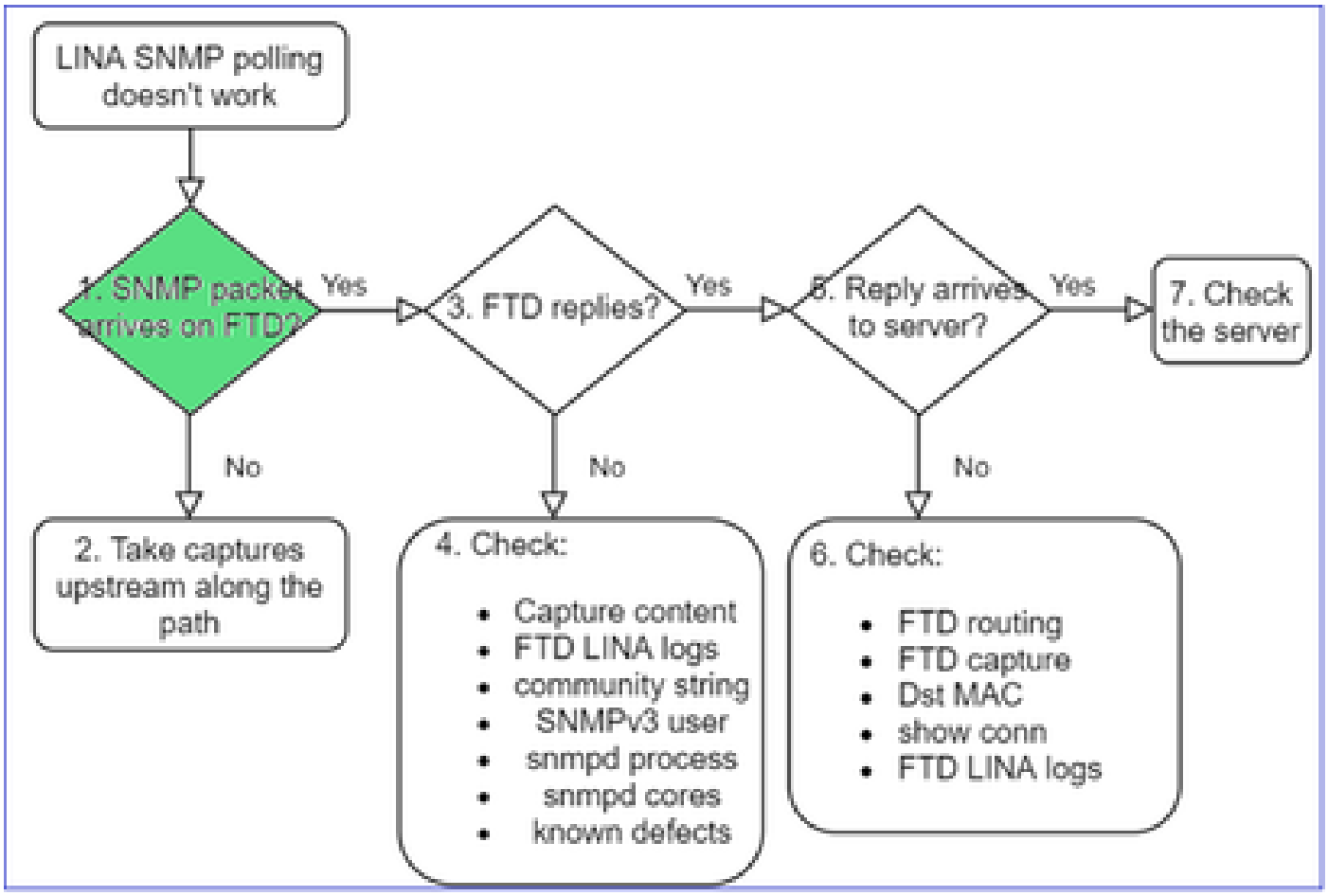
توصية بشأن كيفية أستكشاف الأخطاء وإصلاحها

هذه عملية موصى بها للمخطط الانسيابي لحل المشكلات لمشكلات إستطلاع SNMP عبر LINA:




التعمق

1. هل تصل حزمة SNMP إلى FTD




- تمكين الالتقاطات للتحقق من وصول حزمة SNMP.

يستخدم SNMP على واجهة إدارة FTD (إصدار ما بعد 6.6) الكلمة الأساسية للإدارة:

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

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

يستخدم SNMP في واجهات بيانات FTD اسم الواجهة:

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

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

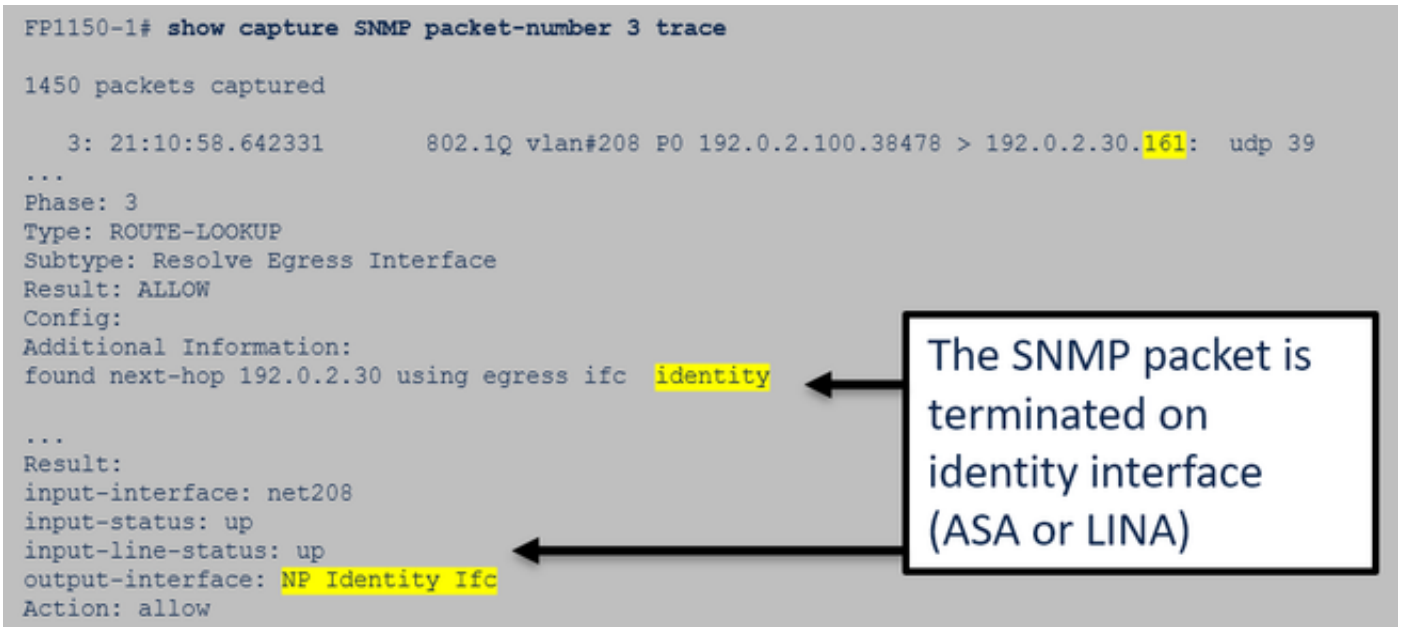
الالتقاط على واجهة إدارة FTD:

```
<#root>

>

capture-traffic


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

1
```

التقاط على واجهة بيانات FTD:

```
<#root>

firepower#

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

تتبع حزمة واجهة بيانات FTD (ما قبل 6.6/9.14.1):



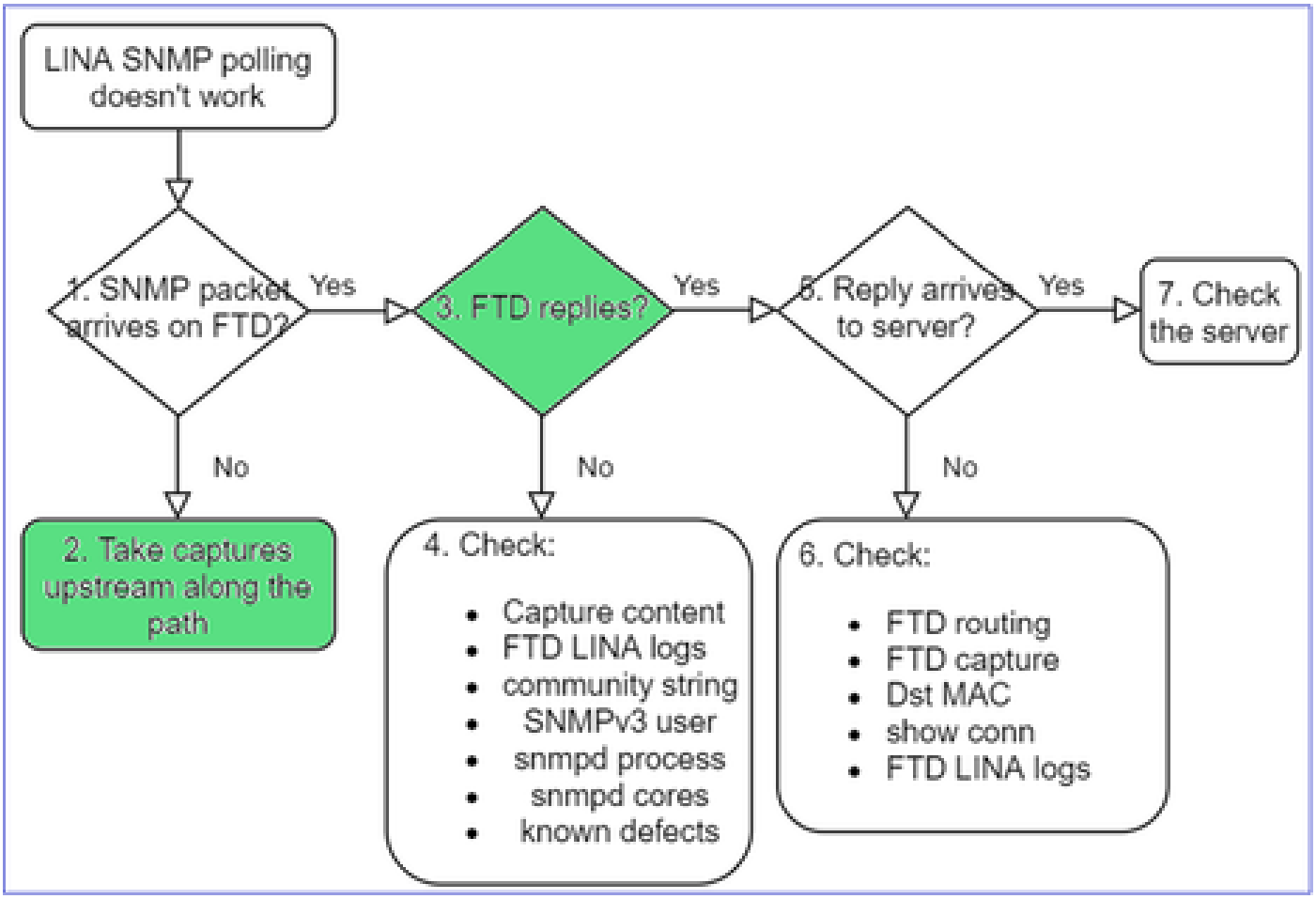

تتبع حزمة واجهة بيانات FTD (بعد 6.6/9.14.1):

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

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

2. في حالة عدم رؤية حزم SNMP في التقاط مدخل FTD:

- أخذ التقاطات انتقال البيانات إلى الخادم على طول المسار.
- تأكد من أن خادم SNMP يستخدم عنوان IP الصحيح الخاص بـ FTD.
- البدء من switchport (منفذ المبدّل) الذي يواجه واجهة FTD وانتقال البيانات إلى الخادم.




3. هل ترى ردود FTD SNMP؟

للتحقق مما إذا كان FTD يرد عليك أم لا:

1. التقاط خروج FTD (واجهة LINA أو MGMT)

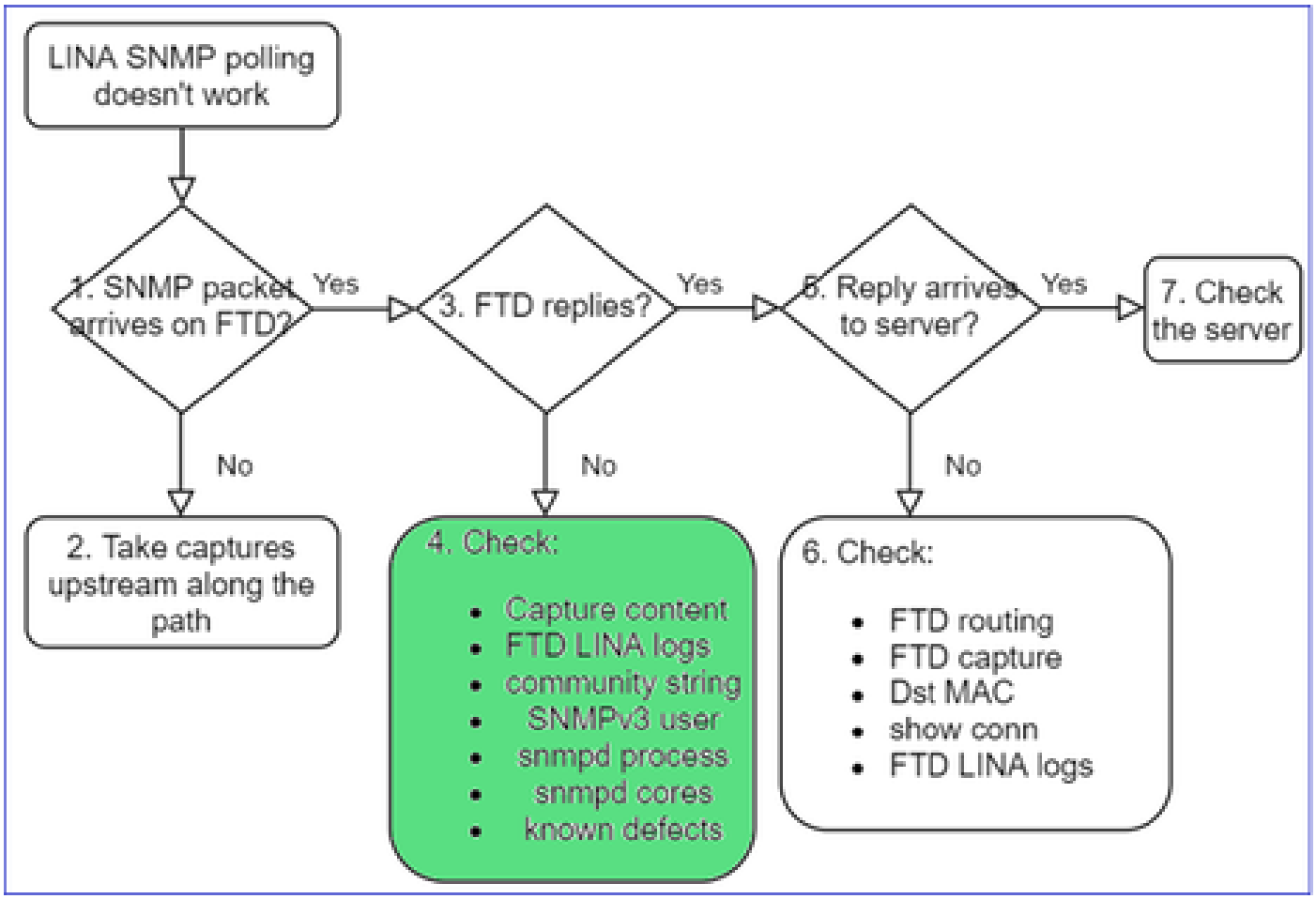
تحقق من حزم SNMP مع منفذ المصدر 161:

```
<#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
```

في إصدارات ما بعد 6.6/9.14.1، لديك نقطة التقاط إضافية واحدة: التقاط على واجهة المنطقة NLP. الـ NATed IP من الـ 162.254.x.x مدى:

```
<#root>

admin@firepower:~$

sudo tcpdump -i tap_nlp


listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
16:46:28.372018 IP 192.168.2.100.49008 > 169.254.1.2.snmp:  C="Cisc0123" GetNextRequest(28)  E:cisco.9.
16:46:28.372498 IP 192.168.1.2.snmp > 192.168.2.100.49008:  C="Cisc0123" GetResponse(35)  E:cisco.9.109
```

4 - التكوينات الإضافية




أ. بالنسبة لأجهزة FirePOWER 4100/9300، تحقق من جدول توافق 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)+<br>**Note** FXOS 2.13(0.198)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected. | Firepower 4112 | **9.19(x)** (recommended)<br>9.18(x)<br>9.17(x)<br>9.16(x)<br>9.15(1)<br>9.14(x) | **7.3.0** (recommended)<br>7.2.0<br>7.1.0<br>7.0.0<br>6.7.0<br>6.6.x |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.19(x)** (recommended)<br>9.18(x)<br>9.17(x)<br>9.16(x)<br>9.15(1)<br>9.14(x)<br>9.13(1)<br>9.12(x) | **7.3.0** (recommended)<br>7.2.0<br>7.1.0<br>7.0.0<br>6.7.0<br>6.6.x<br>6.5.0<br>6.4.0 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| 2.12(0.31)+<br>**Note** FXOS 2.12(0.31)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected. | Firepower 4112 | **9.18(x)** (recommended)<br>9.17(x)<br>9.16(x)<br>9.15(1)<br>9.14(x) | **7.2.0** (recommended)<br>7.1.0<br>7.0.0<br>6.7.0<br>6.6.x |
| | Firepower 4145<br>Firepower 4125<br>Firepower 4115 | **9.18(x)** (recommended)<br>9.17(x)<br>9.16(x)<br>9.15(1)<br>9.14(x)<br>9.13(1)<br>9.12(x) | **7.2.0** (recommended)<br>7.1.0<br>7.0.0<br>6.7.0<br>6.6.x<br>6.5.0<br>6.4.0 |
| | Firepower 9300 SM-56<br>Firepower 9300 SM-48<br>Firepower 9300 SM-40 | | |
| | Firepower 4150<br>Firepower 4140<br>Firepower 4120<br>Firepower 4110 | **9.18(x)** (recommended)<br>9.17(x)<br>9.16(x)<br>9.15(1)<br>9.14(x)<br>9.13(x)<br>9.12(x)<br>9.10(x)<br>9.9(x)<br>9.8(x) | **7.2.0** (recommended)<br>7.1.0<br>7.0.0<br>6.7.0<br>6.6.x<br>6.5.0<br>6.4.0<br>6.3.0 |
| | Firepower 9300 SM-44<br>Firepower 9300 SM-36<br>Firepower 9300 SM-24 | | |
| 2.11(1.154)+<br>**Note** FXOS 2.11(1.154)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use | Firepower 4112 | **9.17(x)** (recommended)<br>9.16(x)<br>9.15(1)<br>9.14(x) | **7.1.0** (recommended)<br>7.0.0<br>6.7.0<br>6.6.x |

ب. التحقق من إحصائيات خادم SNMP الخاص ب FTD LINA:

```
<#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
```

ج. جدول اتصال FTD LINA

ظاحال. قارن مدخل FTD على التقاط في حالة أن ترى أن الاتصال في جدول FTD LINA هذا مفيد في التحقق من أن هذا التحقق صالح فقط لبروتوكول SNMP على واجهة البيانات. إذا كان SNMP على واجهة FTD (الإدارة بعد الإصدار 6.6/9.14.1)، فلن يتم إنشاء أي مخرج.

```
<#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
```

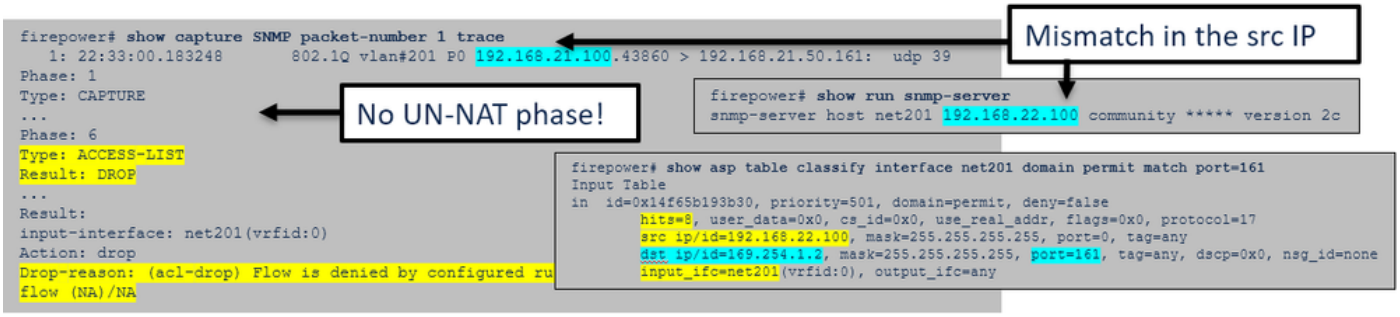
د - نظام LINA لنظام FTD

وهذا أيضاً تحقق صالح لبروتوكول SNMP على واجهة البيانات! إذا كان SNMP على واجهة الإدارة، فلن يتم إنشاء سجل:

```
<#root>
```

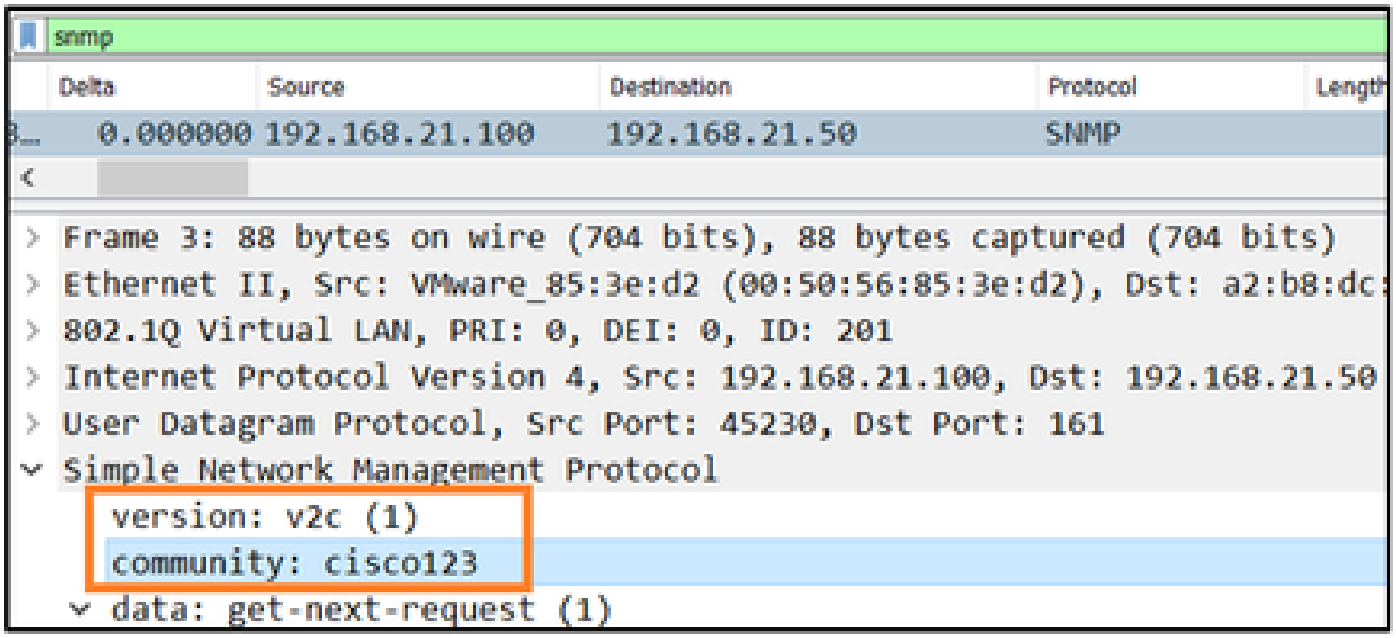
```
firepower#
show log | i 302015.*161

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

ه. التحقق من قيام FTD بإسقاط حزم SNMP بسبب IP لمصدر المضيف غير الصحيح




f. بيانات اعتماد غير صحيحة (مجتمع SNMP)

في محتويات الالتقاط، يمكنك رؤية قيم المجتمع (SNMP v1 و2c):




g. تكوين غير صحيح (على سبيل المثال، إصدار SNMP أو سلسلة المجتمع)

هناك عدة طرق للتحقق من تكوين SNMP للجهاز وسلاسل المجتمع:

<#root>

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

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

طريقة أخرى:

```
<#root>

firepower#

debug menu netsnmp 4
```

ح. حالات إسقاط ASP من نوع FTD LINA/ASA

وهذا مفيد للتحقق مما إذا كانت حزم SNMP قد تم إسقاطها بواسطة FTD. أولاً، امسح العدادات (امسح إسقاط صفحة الخادم النشطة) ثم اختبر:

```
<#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
```

ط - التقاط ASP

توفر التقاطات صفحة الخادم النشطة (ASP) إمكانية رؤية الحزم التي تم إسقاطها (على سبيل المثال، قائمة التحكم بالوصول (ACL) أو التجاوز):

```
<#root>

firepower#

capture ASP type asp-drop all
```

اختبر محتويات الالتقاط ثم تحقق منها:

```
<#root>
firepower#
show capture

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

j. لب SNMP (traceback) - طريقة التحقق 1

يُعد هذه التحقق مفيدًا في حالة الشك في وجود مشكلات في استقرار النظام:

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

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

SNMP الأساسي (تتبُّع الأثر) – طريقة التحقق 2

```
<#root>
admin@firepower:~$
ls -l /var/data/cores

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

إذا رأيت ملف SNMP الأساسي، فجمّع هذه العناصر واتصل بمركز الدعم الفني في Cisco:

- ملف FTD TS (أو ASA show tech)
- ملفات snmpd الأساسية

تصحيح أخطاء SNMP (هذه أوامر مخفية ومتوفرة فقط في الإصدارات الأحدث):

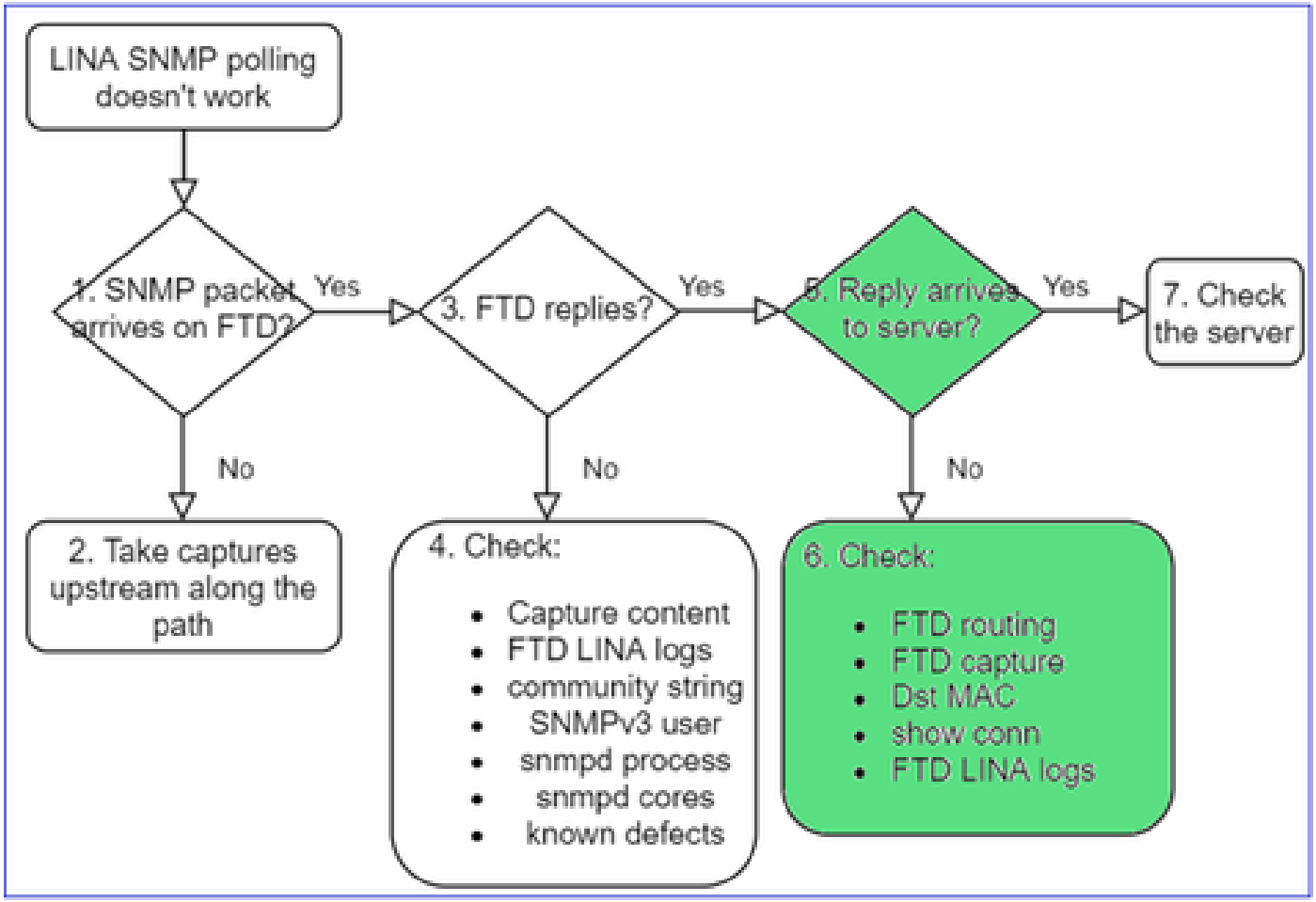
```
<#root>
firepower#
debug snmp trace [255]

firepower#
debug snmp verbose [255]

firepower#
```

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

```
firepower#
```

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

هل يصل در SNMP لجدار الحماية إلى الخادم؟




في حال در FTD، لكن الدرد لم يصل إلى الخادم، فتحقق من ذلك:

أ - توجيه FTD

بالنسبة لتوجيه واجهة إدارة FTD:

```
<#root>
```

```
>
```

```
show network
```

بالنسبة لتوجيه واجهة بيانات FTD LINA:

```
<#root>
```

```
firepower#
```

**show route**

ب. التحقق من MAC الوجهة

التحقق من عنوان MAC الخاص بواجهة إدارة FTD:

<#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
```

التحقق من عنوان MAC الخاص بواجهة بيانات FTD LINA:

<#root>

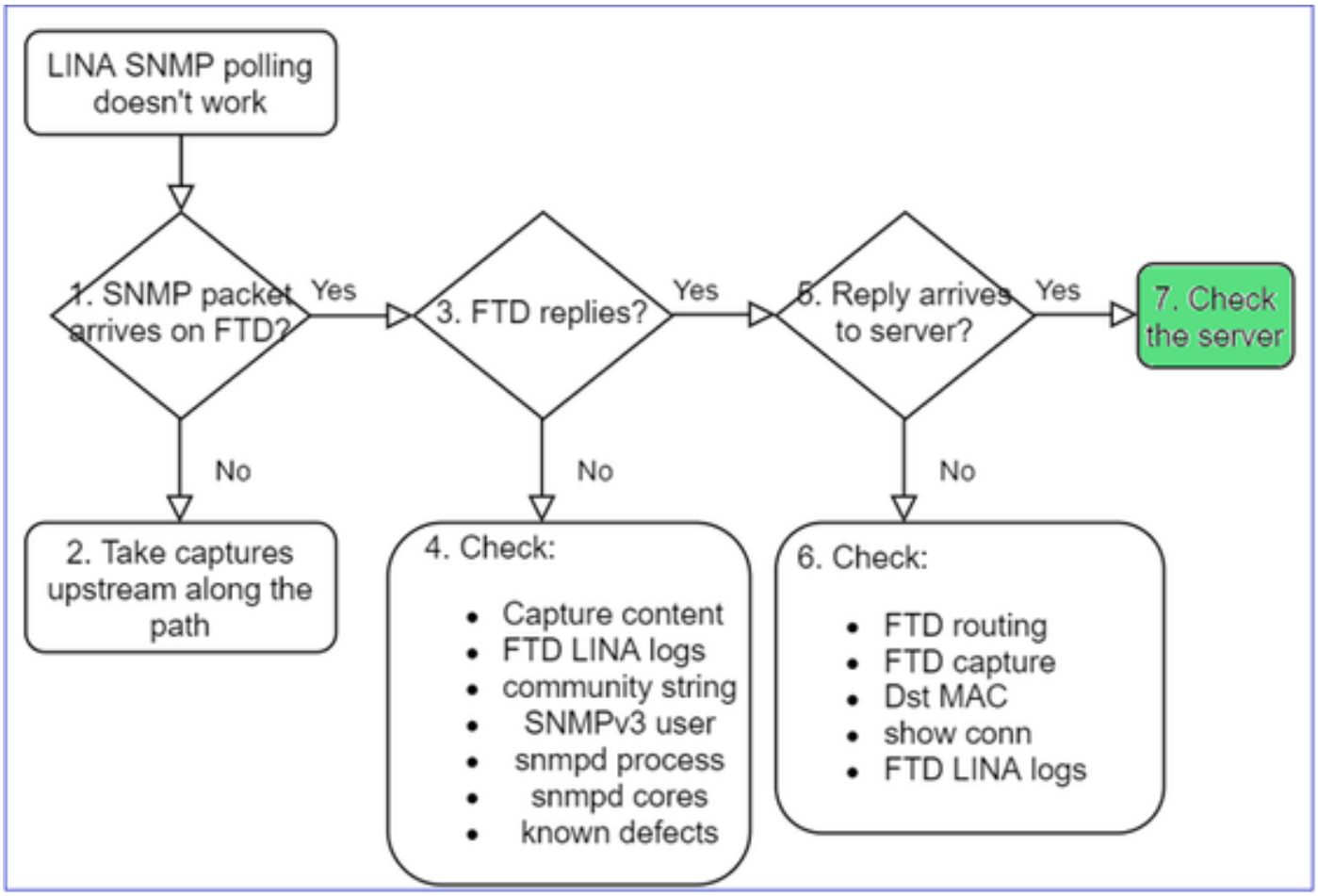
```
firepower#
```

**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,
```

ج. تحقّق من الأجهزة على طول المسار التي من المحتمل أن تُسقط/تحظر حزم SNMP.

التحقق من خادم SNMP




أ. تحقق من محتويات الالتقاط للتحقق من الإعدادات.

ب. تحقق من تكوين الخادم.

ج. حاول تعديل اسم مجتمع SNMP (على سبيل المثال، بدون حروف خاصة).

يمكنك إستخدام مضيف نهائي أو حتى FMC لاختبار الاستقصاء طالما تم استيفاء الشرطين 2:

1. اتصال SNMP في مكانه.
2. يُسمح لعنوان IP المصدر بالاستعلام عن الجهاز.

<#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.
```

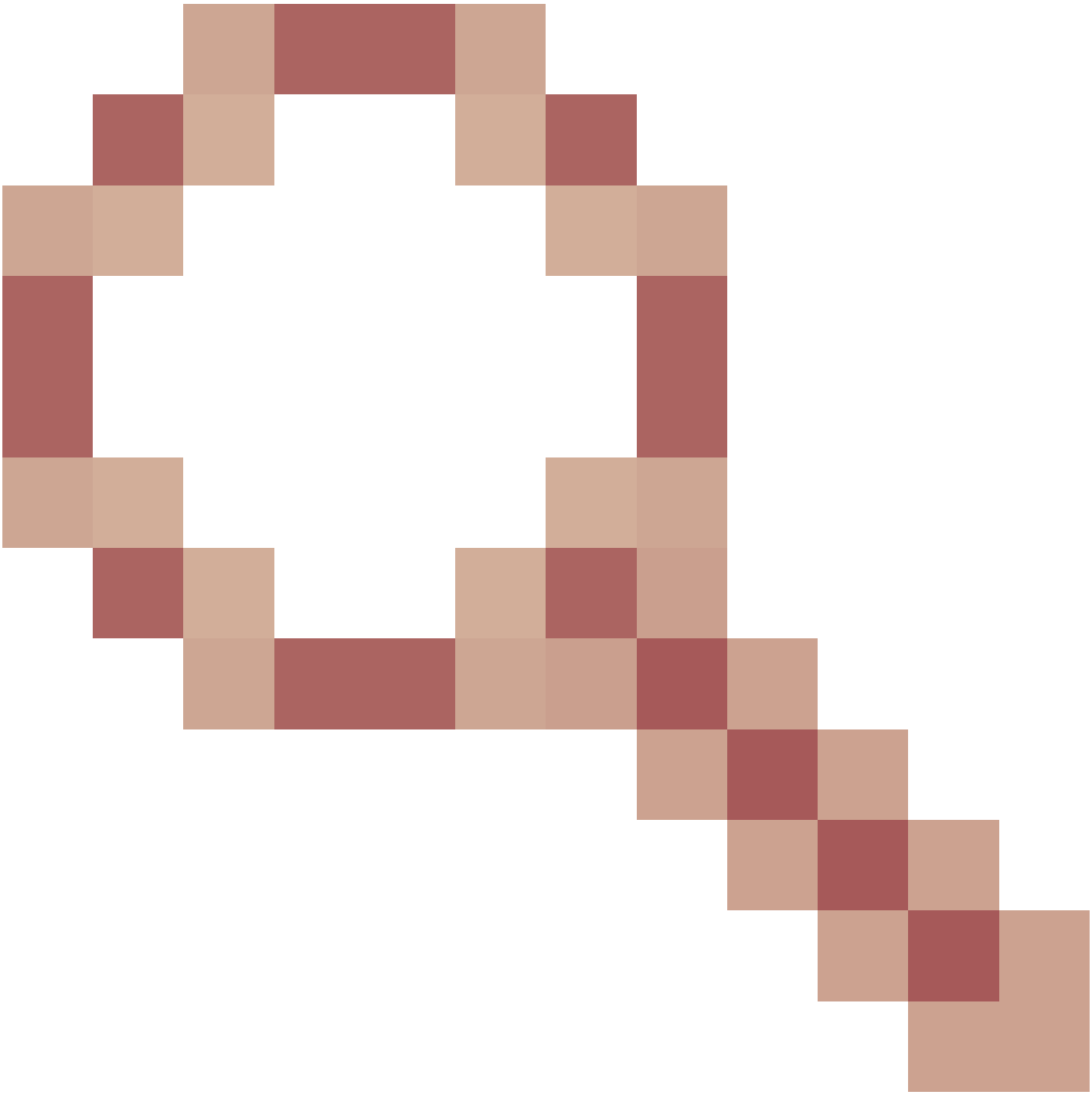
اعتبارات إستطلاع SNMPv3

- الترخيص: يتطلب SNMPv3 ترخيص تشفير قوي. تأكد من تمكين وظيفة التحكم في التصدير في بوابة الترخيص الذكي

- لاستكشاف الأخطاء وإصلاحها، يمكنك محاولة إستخدام مستخدم/بيانات اعتماد جديدة
- إذا تم إستخدام التشفير، يمكنك فك تشفير حركة مرور SNMPv3 والتحقق من الحمولة كما هو موضح في: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59
- ضع في اعتبارك AES128 للتشفير في حالة تأثر برنامجك بالعيوب مثل:
- معرف تصحيح الأخطاء من Cisco CSCvy27283

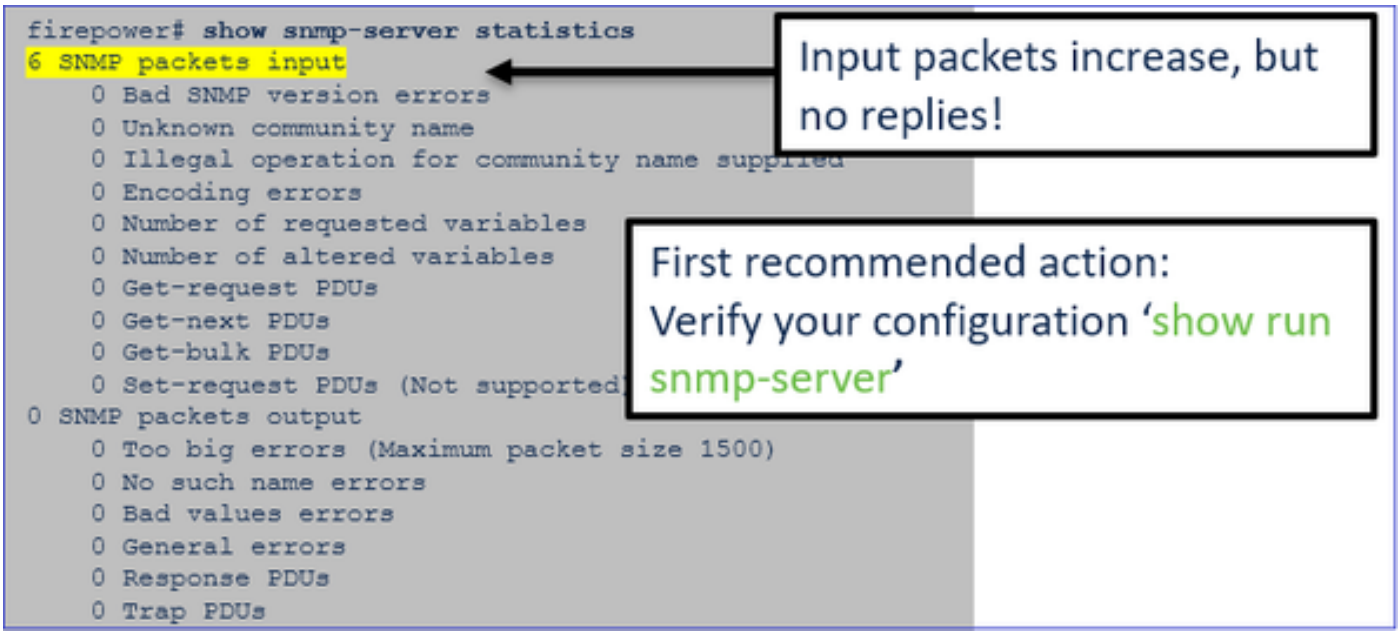
يمكن أن يفشل إستطلاع ASA/FTD SNMPv3 باستخدام خوارزميات الخصوصية AES192/AES256

يفشل معرف تصحيح الأخطاء من Cisco CSCvx45604



SnmpV3 في تشغيل المستخدم مع المصادقة SHA و AES 192

ملاحظة: إذا فشل SNMPv3 بسبب عدم تطابق الخوارزمية، فلن تظهر مخرجات العرض والسجلات أي شيء واضح




اعتبارات الاستعلام عن SNMPv3 – دراسات الحالة

1. SNMPv3 snmpwalk - سيناريو وظيفي

<#root>

admin@FS2600-2:~$

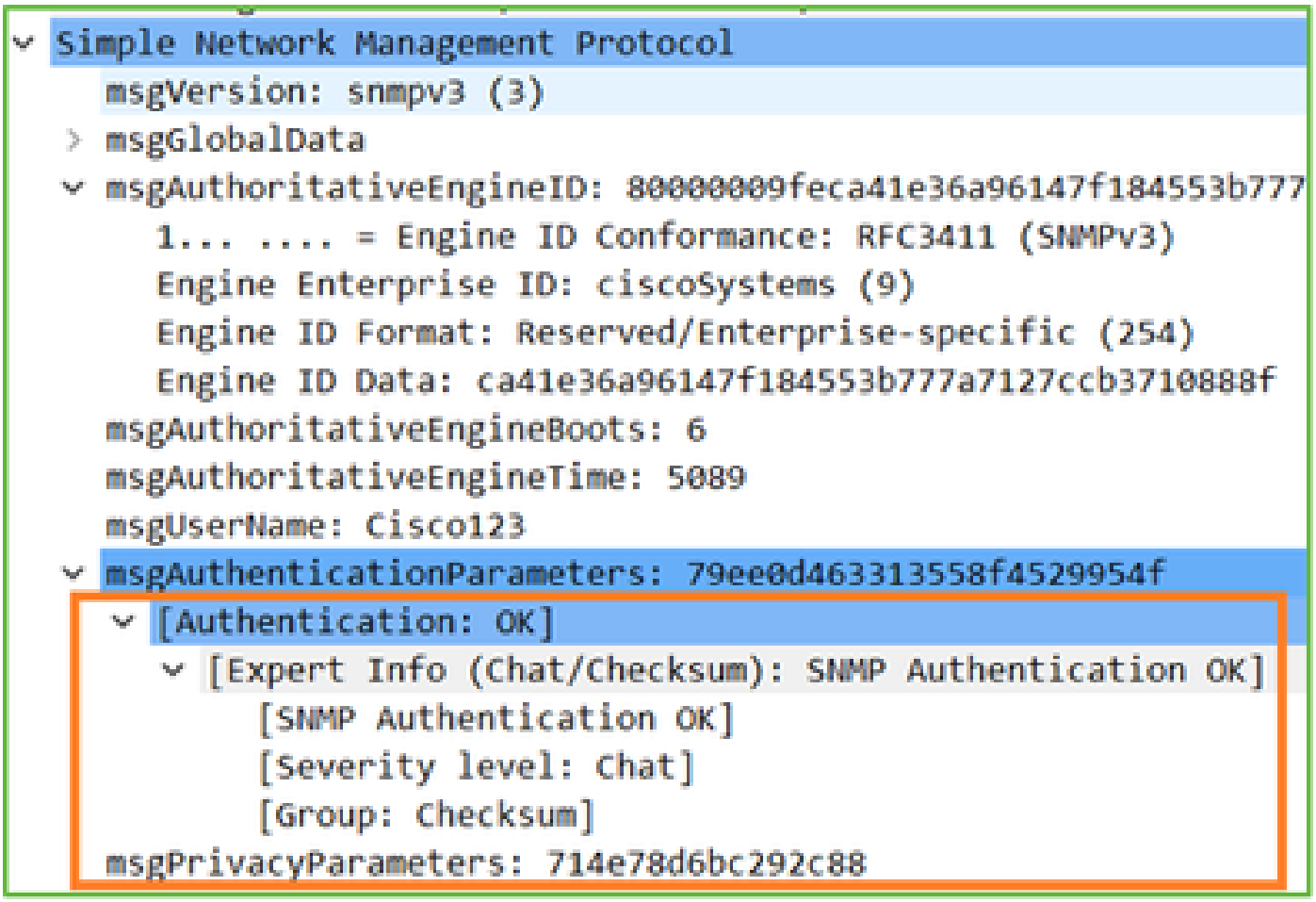
**snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x AES -X Cisco123 192.168.21.50**

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

في الالتقاط (snmpwalk) ستري أدًا لكل حزمة:

```
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
```

ال يعرض ملف الالتقاط أي شيء غير عادي:




2. SNMPv3 snmpwalk - فشل التشفير

تلميح #1: هناك مهلة:

<#root>

admin@FS2600-2:~$

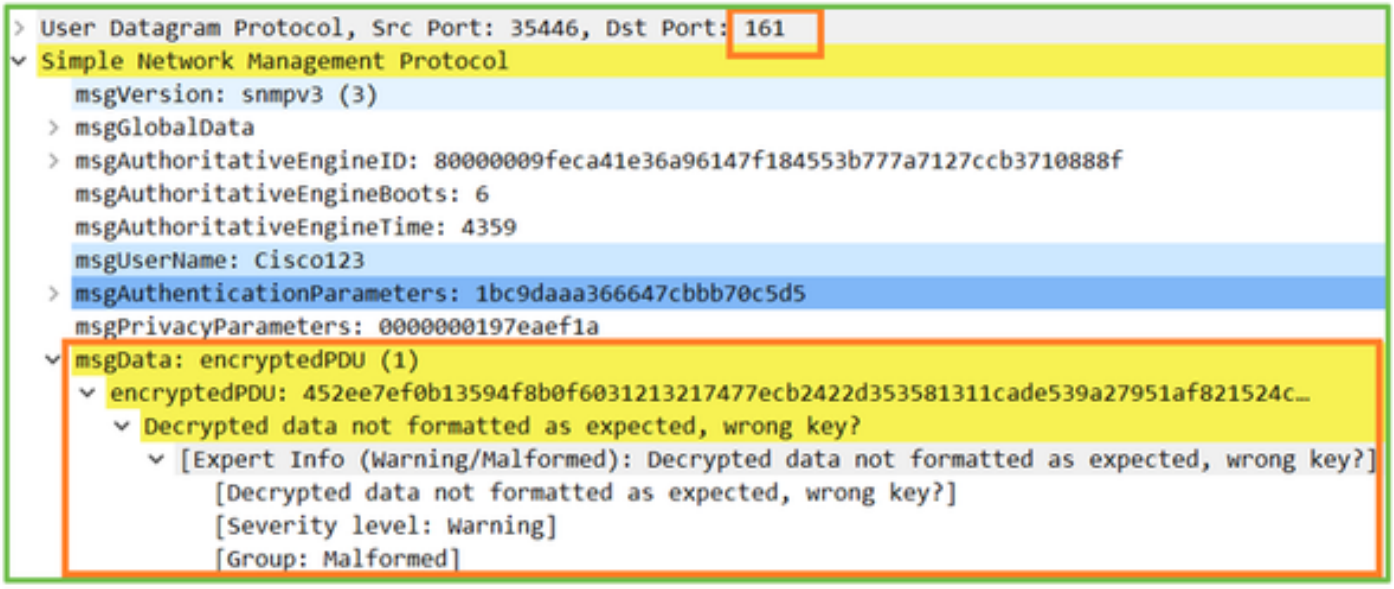
**snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x DES -X Cisco123 192.168.21.50**

Timeout: No Response from 192.168.2.1

تلميح رقم 2: هناك العديد من الطلبات والرد واحد:

```
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
```

الخطوة 3: فشل فك تشفير Wireshark:




الخطوة 4. تحقق من ملف ma_ctx2000.log بحثا عن "خطأ في تحليل رسائل 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
```

الخطأ ScopedPDU تلميح قوي لخطأ تشفير. يعرض ملف ma_ctx2000.log الأحداث الخاصة ب SNMPv3 فقط!

3. SNMPv3 snmpwalk - فشلت المصادقة

الخطوة 1: فشل المصادقة

<#root>

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

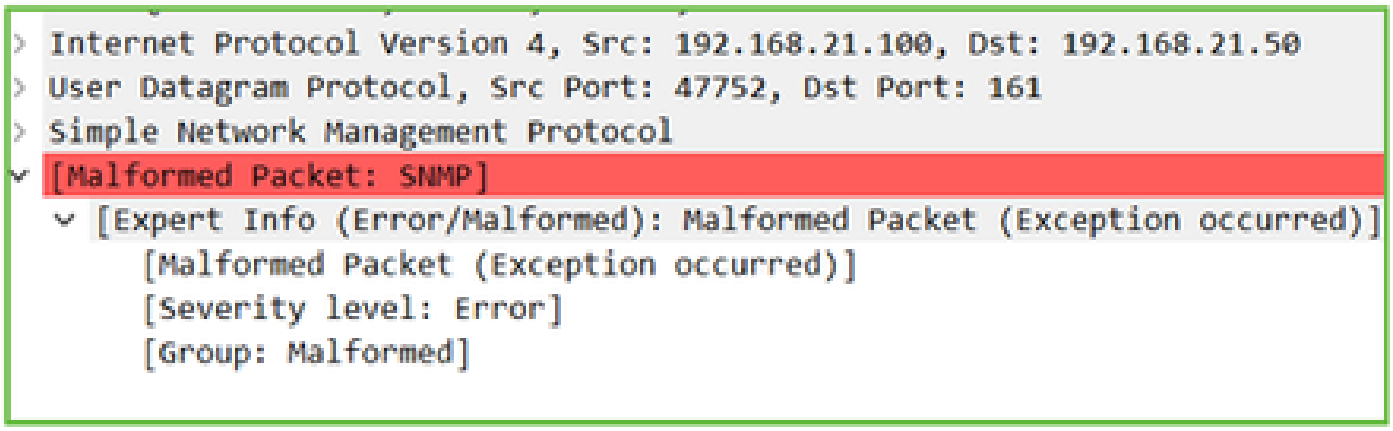
**snmpwalk -v 3 -u Cisco123 -l authPriv -a MD5 -A Cisco123 -x AES -X Cisco123 192.168.21.50**

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

التلميح رقم 2: هناك العديد من الطلبات والردود

```
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
```

التلميح رقم 3: حزمة Wireshark ذات التكوين الخاطئ




التلميح رقم 4. تحقق من ملف ma_ctx2000.log للاطلاع على رسائل "فشل المصادقة":

<#root>

>

**expert**

admin@firepower:~$

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

Authentication failed for Cisco123
Authentication failed for Cisco123

## يتعذّر إجراء الاستقصاء عن FXOS SNMP

أوصاف المشكلة (نموذج من حالات Cisco TAC الحقيقية):

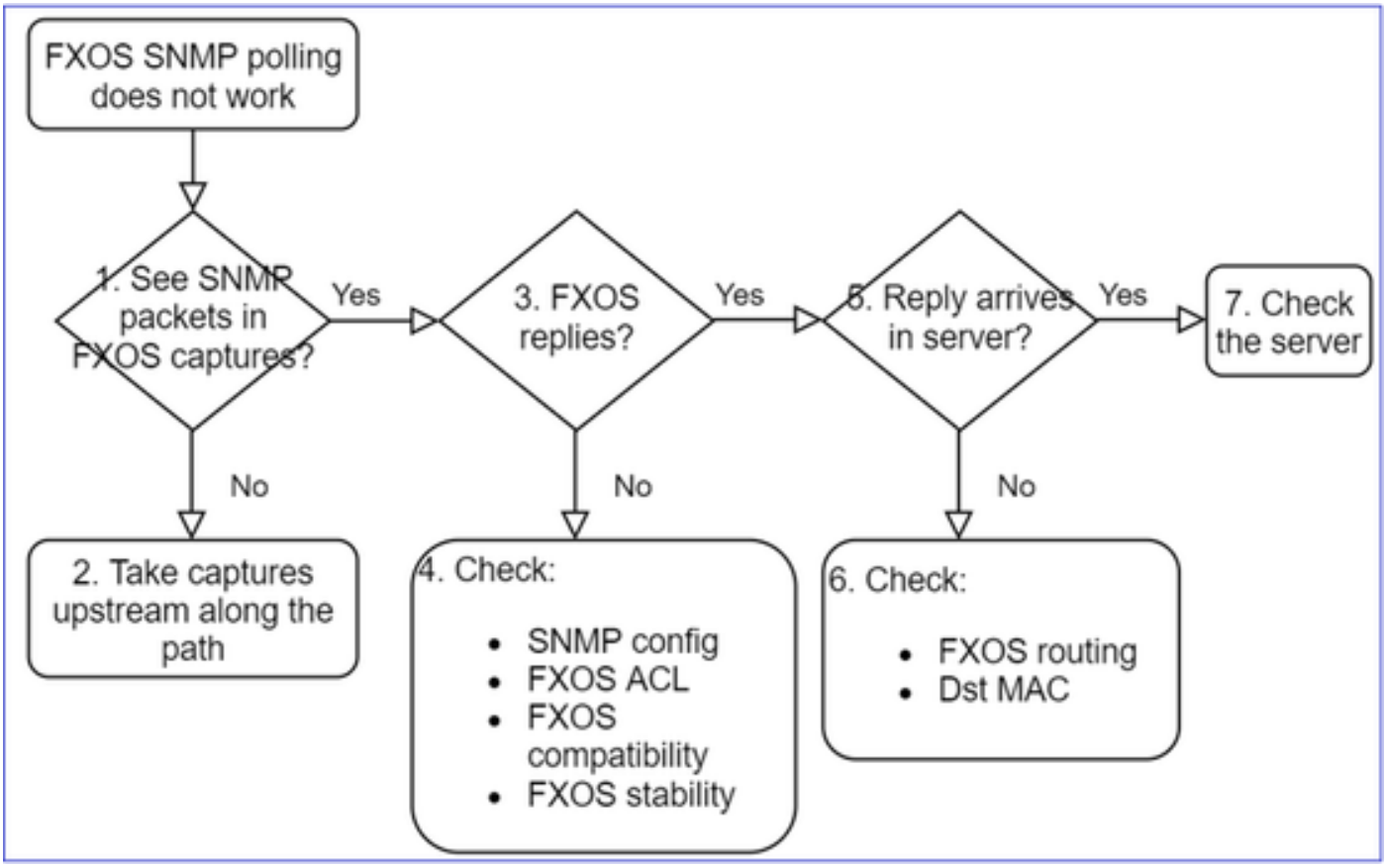
- "يعطي SNMP إصداراً خاطئاً لـ FXOS. عند الاستعلام باستخدام SNMP عن إصدار FXOS، يكون من الصعب فهم المخرجات."
- "يتعذّر إعداد مجتمع snmp على FXOS FTD4115."
- "بعد ترقية FXOS من 2.8 إلى 2.9 على جدار الحماية الاحتياطي، نحصل على مهلة عندما نحاول استقبال أي معلومات عبر SNMP."
- "snmpwalk على 9300 fxos ولكنه يعمل على 4140 fxos على نفس الإصدار. قابلية

الوصول والمجتمع ليس اهما المشكلة."

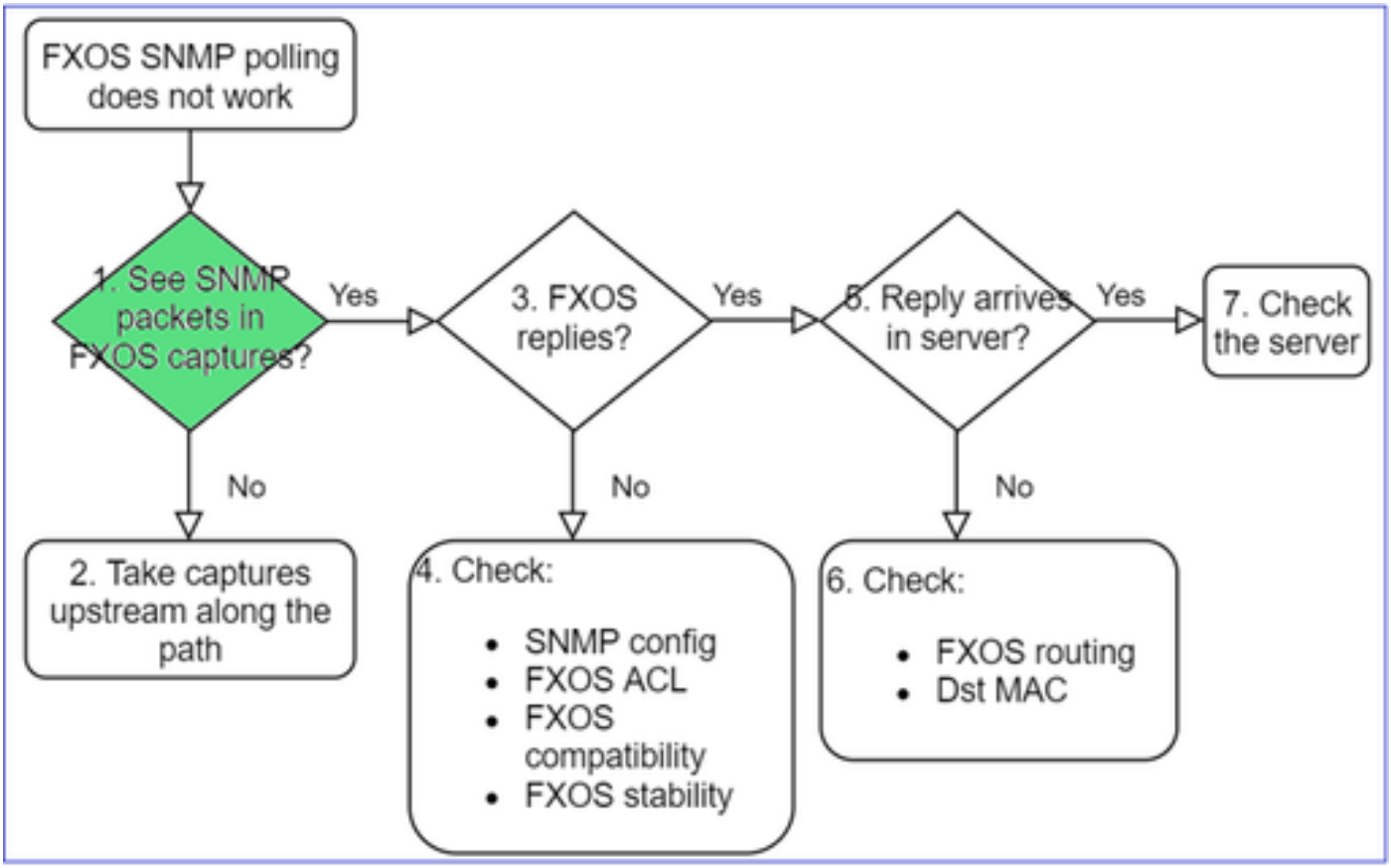
- "نريد إضافة 25 خادم آخر من خوادم SNMP على FPR4K FXOS، لكن ال يمكننا ذلك."

## موصى باستكشاف الأخطاء وإصلاحها

هذه هي العملية لاستكشاف أخطاء المخطط الانسيابي الخاصة باستطلاع مشاكل FXOS SNMP وإصلاحها:




1. هل ترى حزم SNMP في لقطات FXOS؟




FPR1xxx/21xx

- في FPR1xxx/21xx ال يوجد مدير هيكل (وضع الجهاز).
- يمكنك الاستفسار عن برنامج FXOS من واجهة الإدارة.

<#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
```

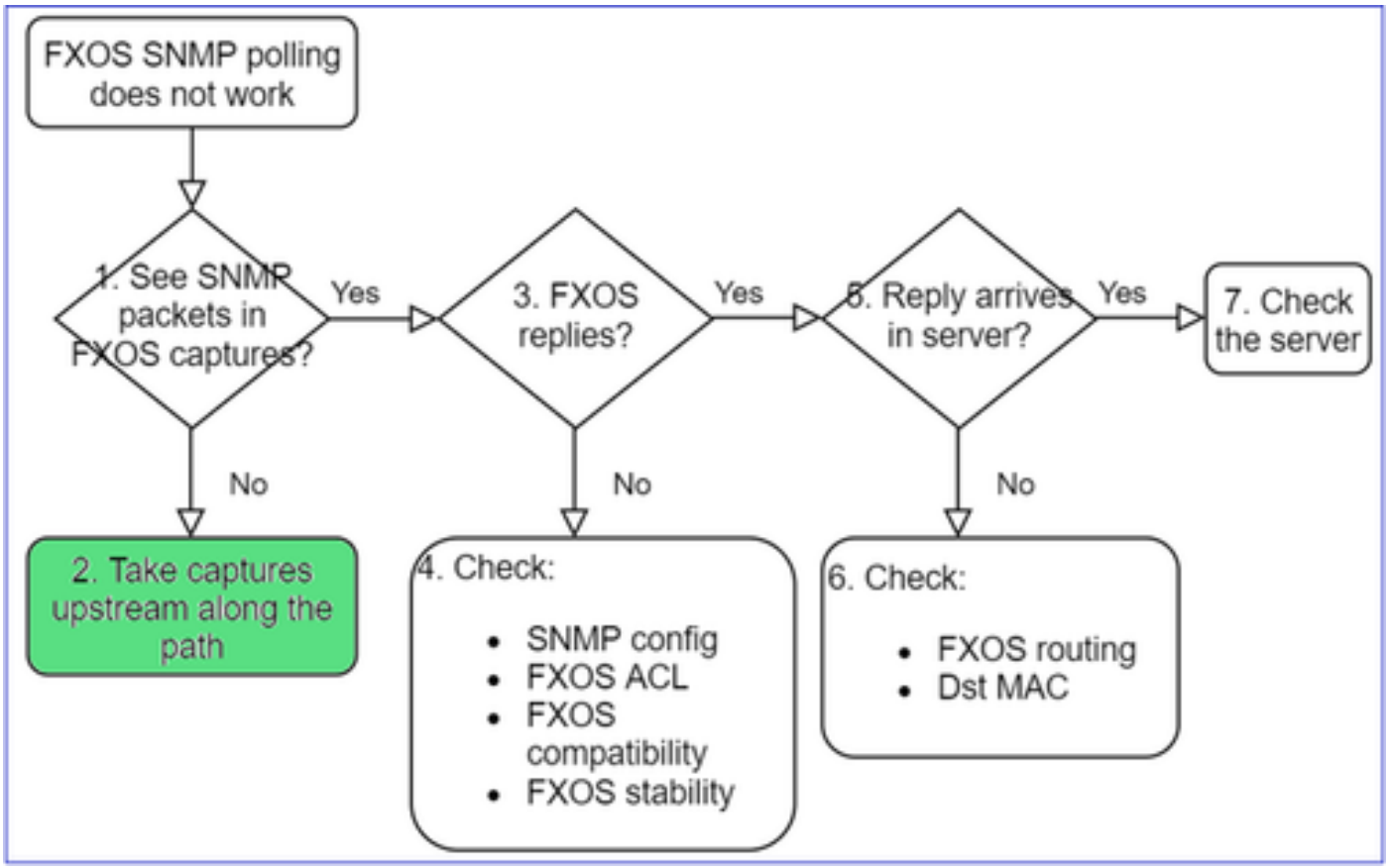
41xx/9300

- على FirePower 41xx/93xx، استخدم أداة Ethanalyzer CLI لالتقاط الهيكل القاعدي:

<#root>

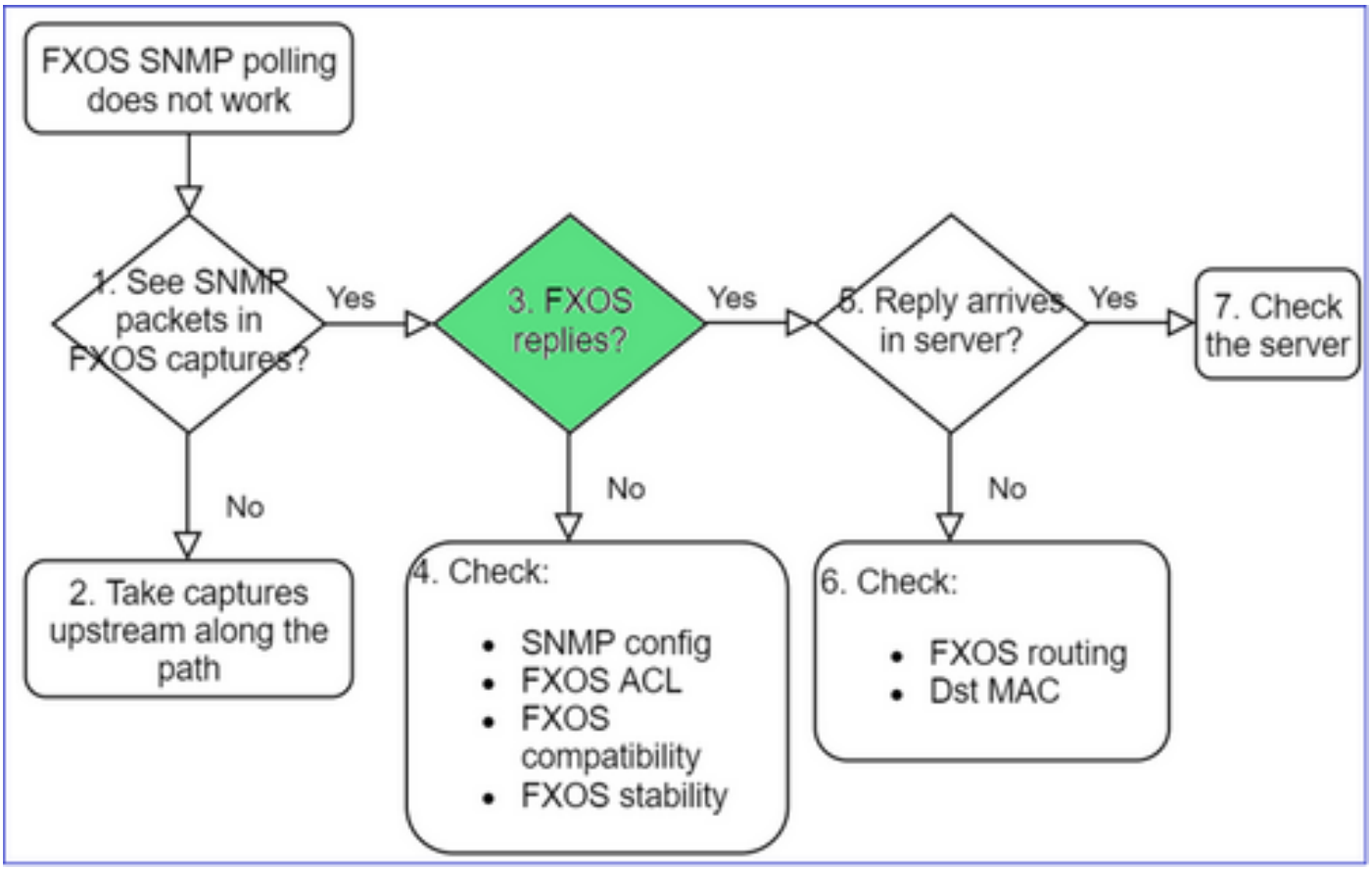
```
firepower#

connect fxos

firepower(fxos)#

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

firepower(fxos)#

exit

firepower#

connect local-mgmt

firepower(local-mgmt)#

dir


1

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

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

2. ألا توجد حزم في التقاطات FXOS؟




- أخذ التقاطات انتقال البيانات إلى الخادم على طول المسار

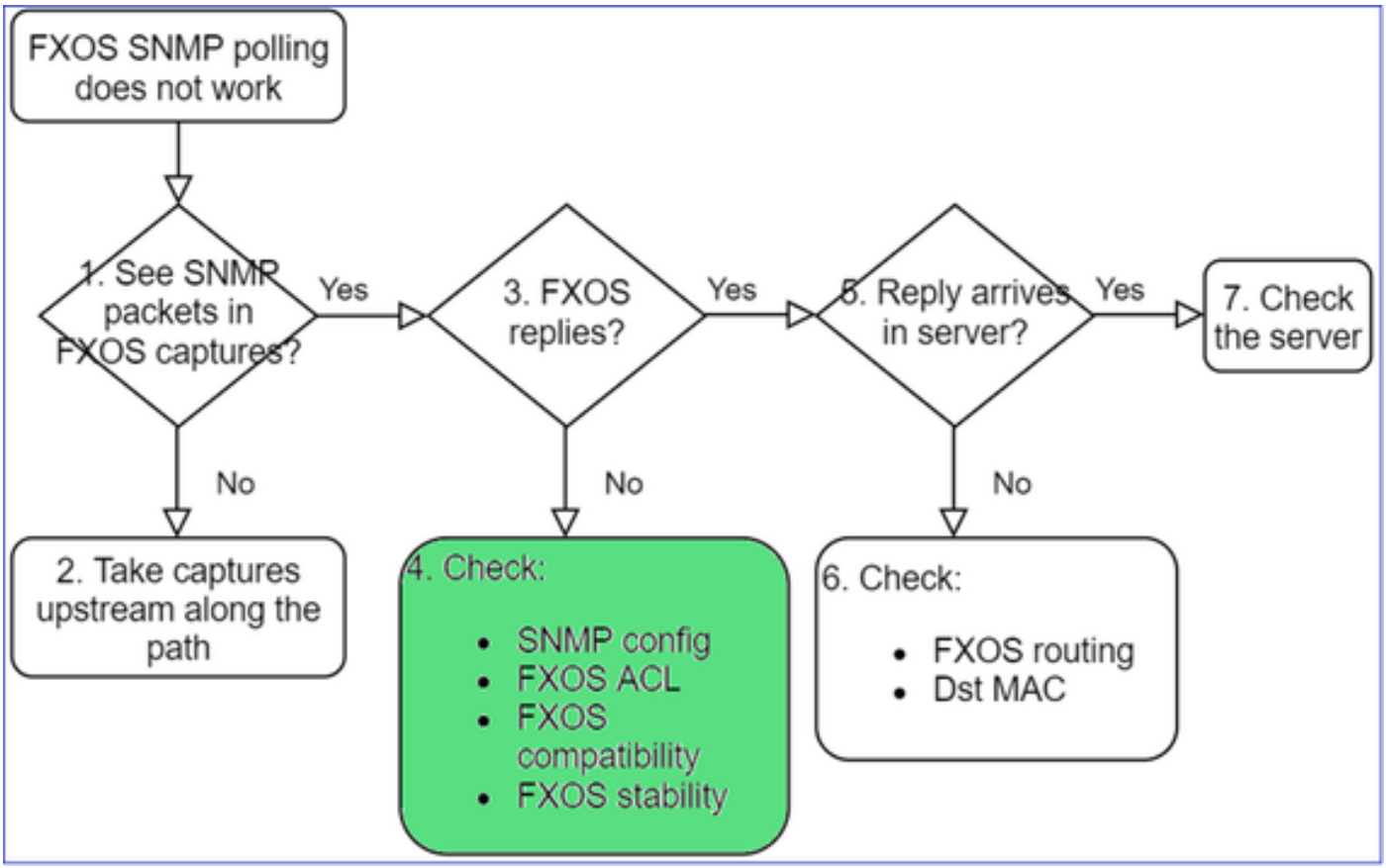
3. هل ترد FXOS؟



- سيناريو وظيفي:

```
<#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 الى درت




عمليات تحقق إضافية

- تحقق من تكوين SNMP (من واجهة المستخدم أو واجهة سطر الأوامر):

```
<#root>
```

```
firepower#
scope monitoring

firepower /monitoring #
show snmp

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

- كن حذرًا عند التعامل مع الأحرف الخاصة (على سبيل المثال، "$"):

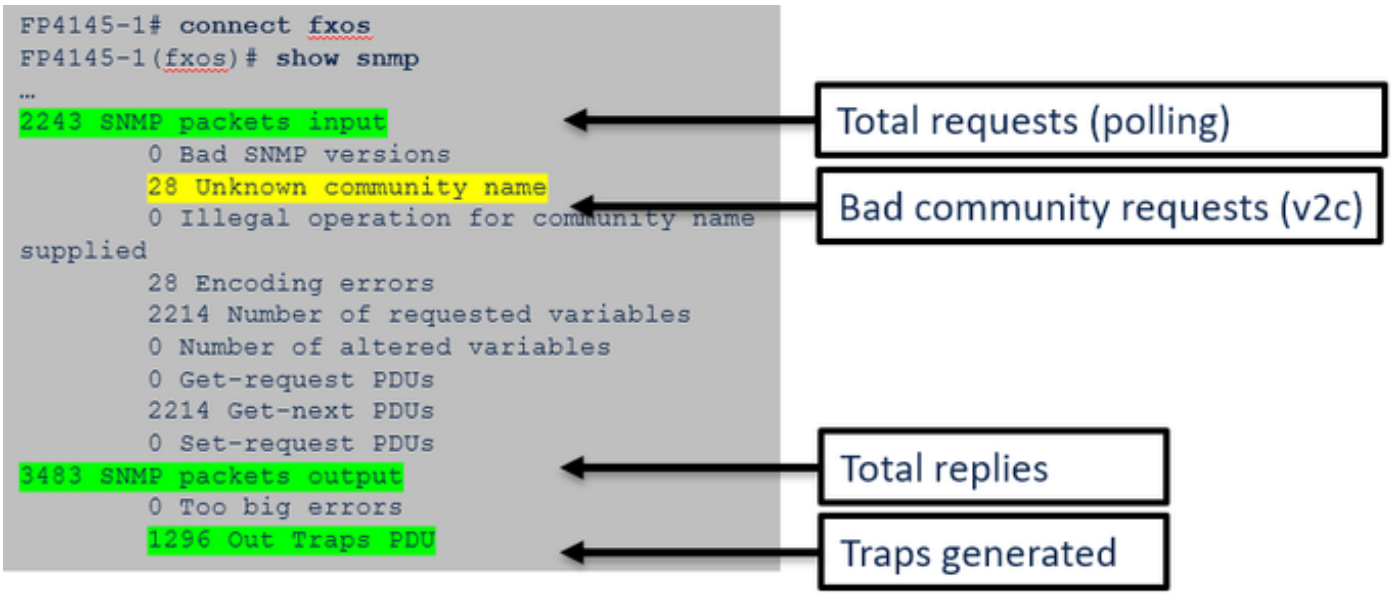
```
<#root>
FP4145-1#
connect fxos

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

FP4145-1(fxos)#
show snmp community

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

- بالنسبة إلى SNMP v3، استخدم show snmp-user [detail]
- التحقق من توافق FXOS

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

4. في حالة عدم رد FXOS

تحقّق من عدادات FXOS SNMP:




- تحقق من قائمة التحكم في الوصول (ACL) إلى FXOS. وهذا ينطبق فقط على الأنظمة الأساسية FPR41xx/9300.

إذا تم حظر حركة المرور بواسطة قائمة التحكم بالوصول (ACL) إلى FXOS، ستري الطلبات، ولكن لا ترى أي ردود:

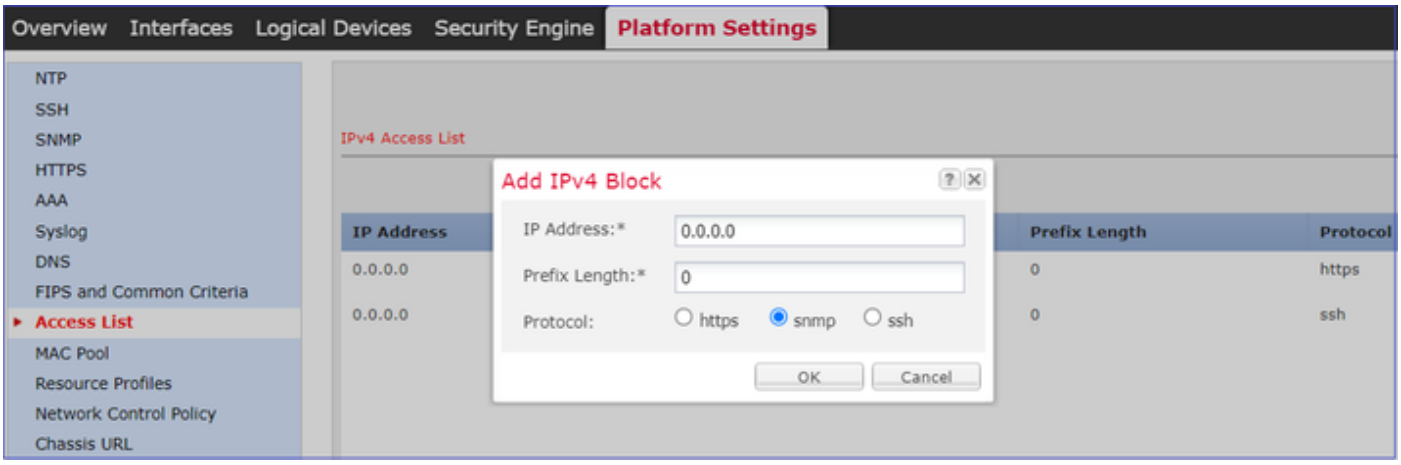
<#root>

```
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
```

يمكنك التحقق من قائمة التحكم بالوصول إلى FXOS من واجهة المستخدم (UI):



كما يمكنك التحقق من قائمة التحكم بالوصول إلى FXOS من واجهة سطر الأوامر:

```
<#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
```

- تصحيح أخطاء SNMP (الحزم فقط). ينطبق فقط على FPR41xx/9300:

```
<#root>

FP4145-1#

connect fxos

FP4145-1(fxos)#

 terminal monitor

FP4145-1(fxos)#

debug snmp pkt-dump

2021 Aug  4 09:51:24.963619 snmpd:  SNMPPKTSTRT: 1.000000 161 495192988.000000 0.000000 0.000000 0.0000
```

- تصحيح أخطاء SNMP (الكل) - إخراج تصحيح الأخطاء هذا مسهب للغاية.

```
<#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
```

- تحقّق من وجود أي أخطاء FXOS ذات صلة بروتوكول 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
```

- تحقّق مما إذا كانت هناك أي طبقات أساسية من snmpd:

على 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
```

على FPR1xxx/21xx:

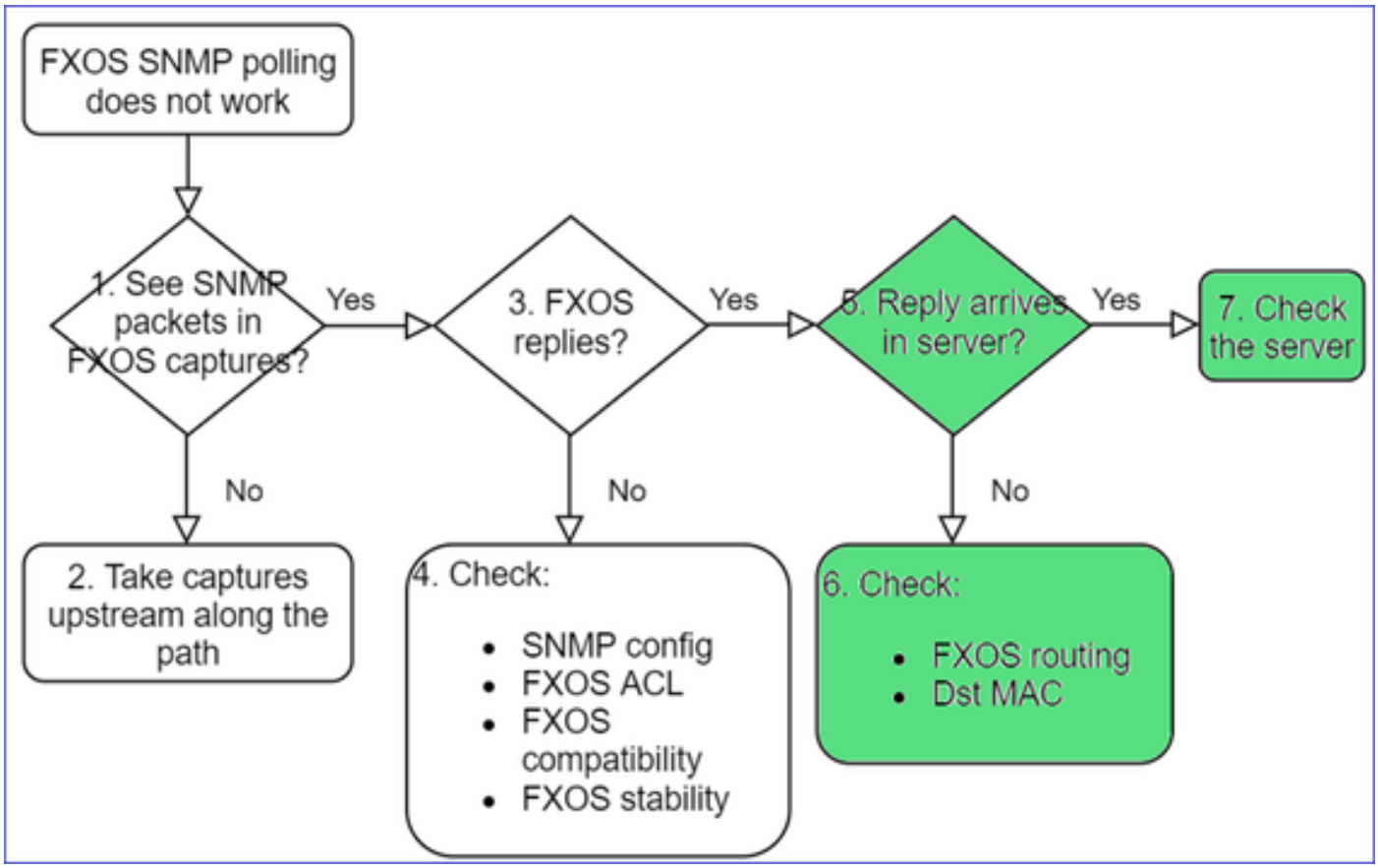
<#root>

firepower(local-mgmt)#

**dir cores_fxos**

إذا رأيت أي طبقات أساسية من snmpd، فجمّع الطبقات الأساسية مع حزمة FXOS وإتصل بمركز المساعدة الفنية (TAC) من Cisco للاستكشاف الأخطاء وإصلاحها.

5. هل يصل SNMP إلى خادم SNMP؟




- التحقق من توجيه FXOS

هذا الإخراج من FPR41xx/9300:

<#root>

```
firepower#
```

**show fabric-interconnect**

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

- خذ لقطة، قم بتصدير pcap والتحقق من عنوان MAC الخاص بالواجهة للرد
- وأخيرًا، تحقّق من خادم SNMP (عمليات الالتقاط والتكوين والتطبيق وما إلى ذلك)

## ما قيم SNMP OID المطلوب استخدامها؟

أوصاف المشكلة (نموذج من حالات Cisco TAC الحقيقية):

- "نريد مراقبة أجهزة Cisco Firepower. يُرجى تقديم معرّفات OID لبروتوكول SNMP لكل وحدة معالجة مركزية أساسية والذاكرة والأقراص"
- "هل هناك أي OID يمكن استخدامه لمراقبة حالة إمداد الطاقة على جهاز ASA 5555؟"

- "نريد جلب هيكل SNMP OID القاعدي على FPR 2K وFPR 4K."
- "نريد الاستطلاع عن ذاكرة التخزين المؤقت لـ ASA ARP."
- "نحتاج إلى معرفة SNMP OID لنظير BGP المعطل."

كيفية العثور على قيم SNMP OID

توفر هذه المستندات معلومات حول معرّفات OID SNMP على أجهزة FirePower:

- المستند التقني للمراقبة بروتوكول SNMP الخاص بـ Firepower Threat Defense (FTD) من Cisco:

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

- الدليل المرجعي لـ Firepower 4100/9300 FXOS MIB من Cisco:

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

- كيفية البحث عن OID محدد على أنظمة FXOS الأساسية:

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

- التحقق من معرّفات SNMP من واجهة سطر الأوامر (ASA/LINA)

<#root>

```
firepower#
```

**show snmp-server ?**

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

firepower#
```

**show snmp-server oid**

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

- للحصول على مزيد من المعلومات حول OID، تحقّق من SNMP Object Navigator

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

- على FXOS (41xx/9300)، قم بتشغيل هذين الأمرين من واجهة سطر أوامر FXOS:

<#root>

**FP4145-1#**

**connect fxos**

**FP4145-1(fxos)#**

**show snmp internal oids supported create**

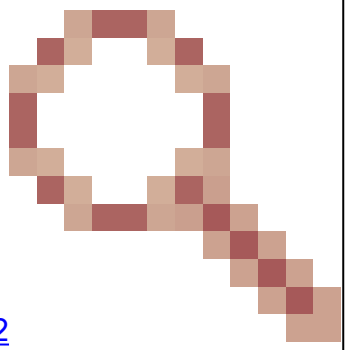
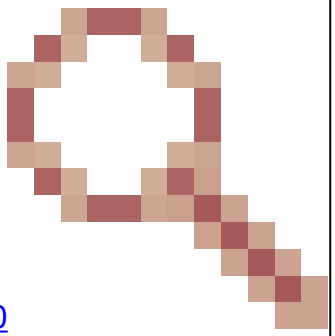
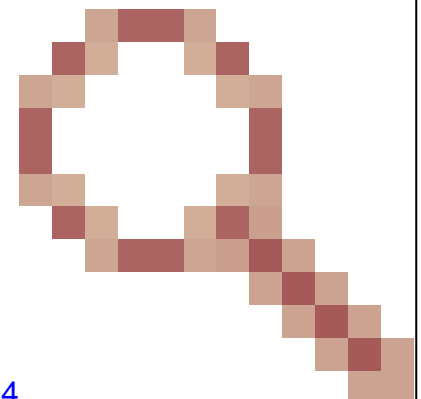
**FP4145-1(fxos)#**

**show snmp internal oids supported**

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

المرجع السريع لمعرّفات OID الشائعة

| المتطلبات | OID |
|---|---|
| وحدة المعالجة المركزية (LINA) | 1.3.6.1.4.1.9.9.109.1.1.1 |
| وحدة المعالجة المركزية (Snort) | 1.3.6.1.4.1.9.9.109.1.1.1 (FP >= 6.7) |
| الذاكرة (LINA) | 1.3.6.1.4.1.9.9.221.1.1 |
| الذاكرة (Linux/FMC) | 1.3.6.1.1.4.1.2021.4 |
| معلومات التوافر العالي (HA) | 1.3.6.1.4.1.9.9.491.1.4.2 |
| معلومات التجميع | 1.3.6.1.4.1.9.9.491.1.8.1 |
| معلومات VPN | جلسات الشبكة الخاصة بشبكة RA-VPN: 1.3.6.1.4.1.9.392.1.3.1 (7.x) |

| | |
|---|---|
| | مستخدمو الشبكة الخاصة بشبكة RA-VPN: 1.3.6.1.4.1.9.392.1.3.3 (7.x)<br><br>جلسات ذروة RA-VPN: 1.3.6.1.4.1.9.392.1.3.41 (7.x)<br><br>جلسات شبكة S2S VPN: 1.3.6.1.4.1.9.392.1.3.29<br><br>جلسات ذروة VPN S2S: 1.3.6.1.4.1.9.392.1.3.31<br><br>- تلميح: Firepower# show snmp server oid \| نعم، نعم |
| حالة BGP |  <br>في معرف تصحيح الأخطاء من Cisco CSCux13512<br>: إضافة BGP MIB لاستطلاع SNMP |
| ترخيص FPR1K/2K ASA/ASAv الذكي |  <br>ENH معرف تصحيح الأخطاء من Cisco CSCvv83590<br>: ASAv/ASA على FPR1k/2k: يحتاج SNMP OID لتعقب حالة الترخيص الذكي |
| معرّفات OID SNMP لـ Lina لقناة المنفذ على مستوى FXOS |  <br>معرف تصحيح الأخطاء من Cisco CSCvu91544<br>: دعم أجهزة OIDs من Lina SNMP لإحصائيات واجهة قناة المنفذ على مستوى FXOS |

إضافات FMC 7. 3 (لوحدة التحكم FMC 1600/2600/4600 والأحدث)

| المتطلبات | OID |
| --- | --- |
| مصيدة حالة المروحة | معرف المالئمة: 1.3.6.1.4.1.9.9.117.2.0.6<br>معرف القيمة: 1.3.6.1.4.1.9.9.117.1.4.1.1.1.<index><br>0 - المروحة ال تعمل<br>1 - المروحة قيد التشغيل |
| مصيدة درجة حرارة وحدة المعالجة المركزية (CPU)/وحدة التزويد باطاقة (PSU) | معرف المالئمة: 1.3.6.1.4.1.9.91.2.0.1<br>معرف العتبة: 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<index>.1<br>معرف القيمة: 1.3.6.1.4.1.9.91.1.1.1.1.4.<index> |
| مصيدة حالة PSU | معرف المالئمة: 1.3.6.1.4.1.9.9.117.2.0.2<br>معرف OperStatus: 1.3.6.1.4.1.9.9.117.1.1.2.1.2.<index><br>معرف AdminStatus: 1.3.6.1.4.1.9.9.117.1.1.2.1.1.<index><br>0 - لم يتم اكتشاف وجود وحدة التزويد باطاقة<br>1 - اكتشاف وجود وحدة تزويد باطاقة، موافق |

## ال يمكن الحصول عل رسائل تنبيه SNMP

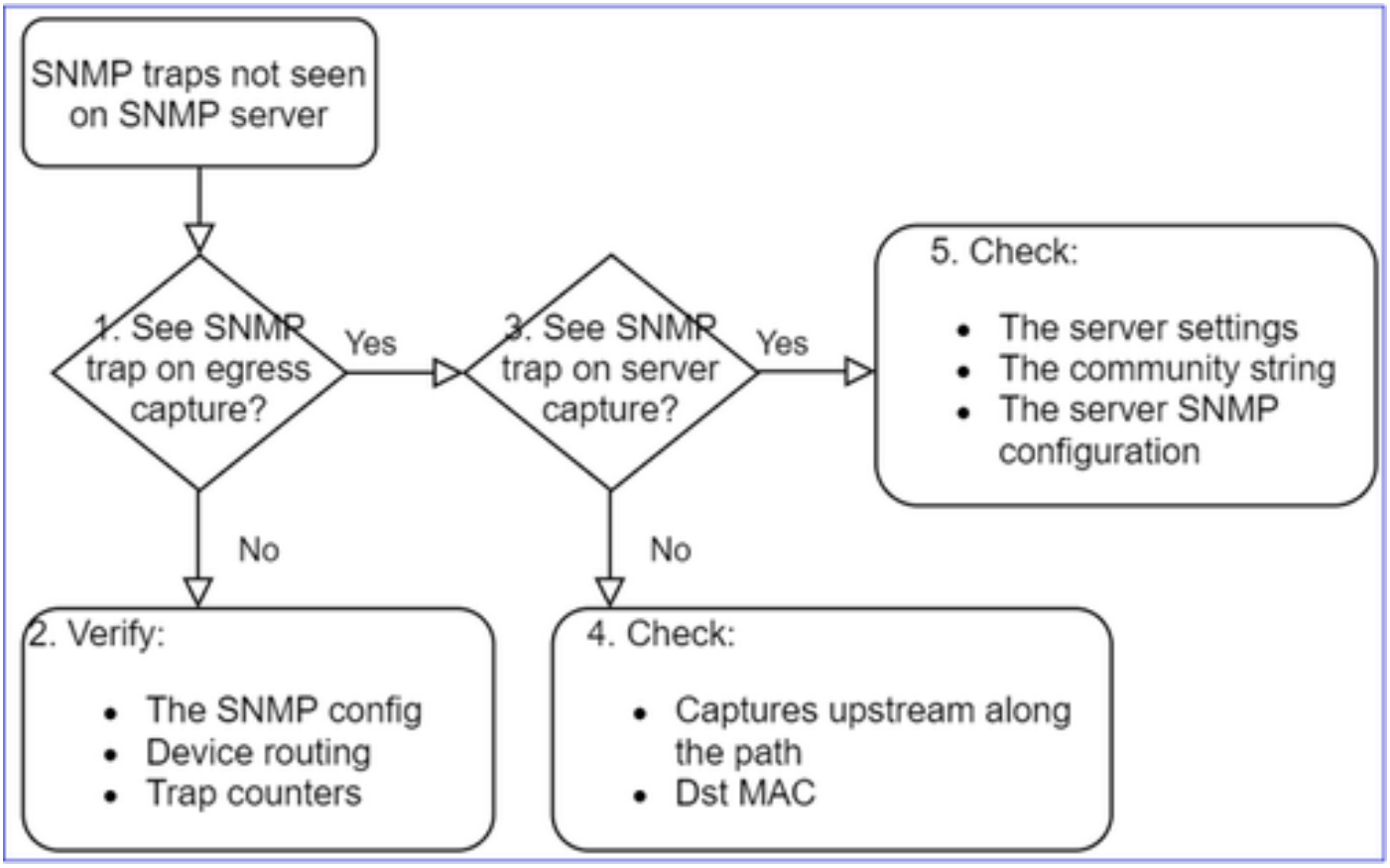
أوصاف المشكلة (نموذج من حالات Cisco TAC الحقيقية):

- "ال يرسل SNMPv3 الخاص بـ FTD أي رسالة تنبيه إلى خادم SNMP."
- "ال يرسل كل من FMC وFTD رسائل تنبيه SNMP."
- "لقد قمنا بتكوين SNMP عل FTD 4100 الخاص بنا لـ FXOS وجرّبنا SNMPv3 وSNMPv2، ولكن ال يمكن لكليهما إرسال رسائل التنبيه."
- "ال يُرسل بروتوكول SNMP لـ Firepower رسائل تنبيه إلى أداة المراقبة."
- "ال يُرسل Firewall FTD رسالة تنبيه SNMP إلى NMS."
- "رسائل تنبيه خادم SNMP ال تعمل."
- "لقد قمنا بتكوين SNMP عل FTD 4100 الخاص بنا لـ FXOS وجرّبنا SNMPv3 وSNMPv2، ولكن ال يمكن لكليهما إرسال رسائل التنبيه."

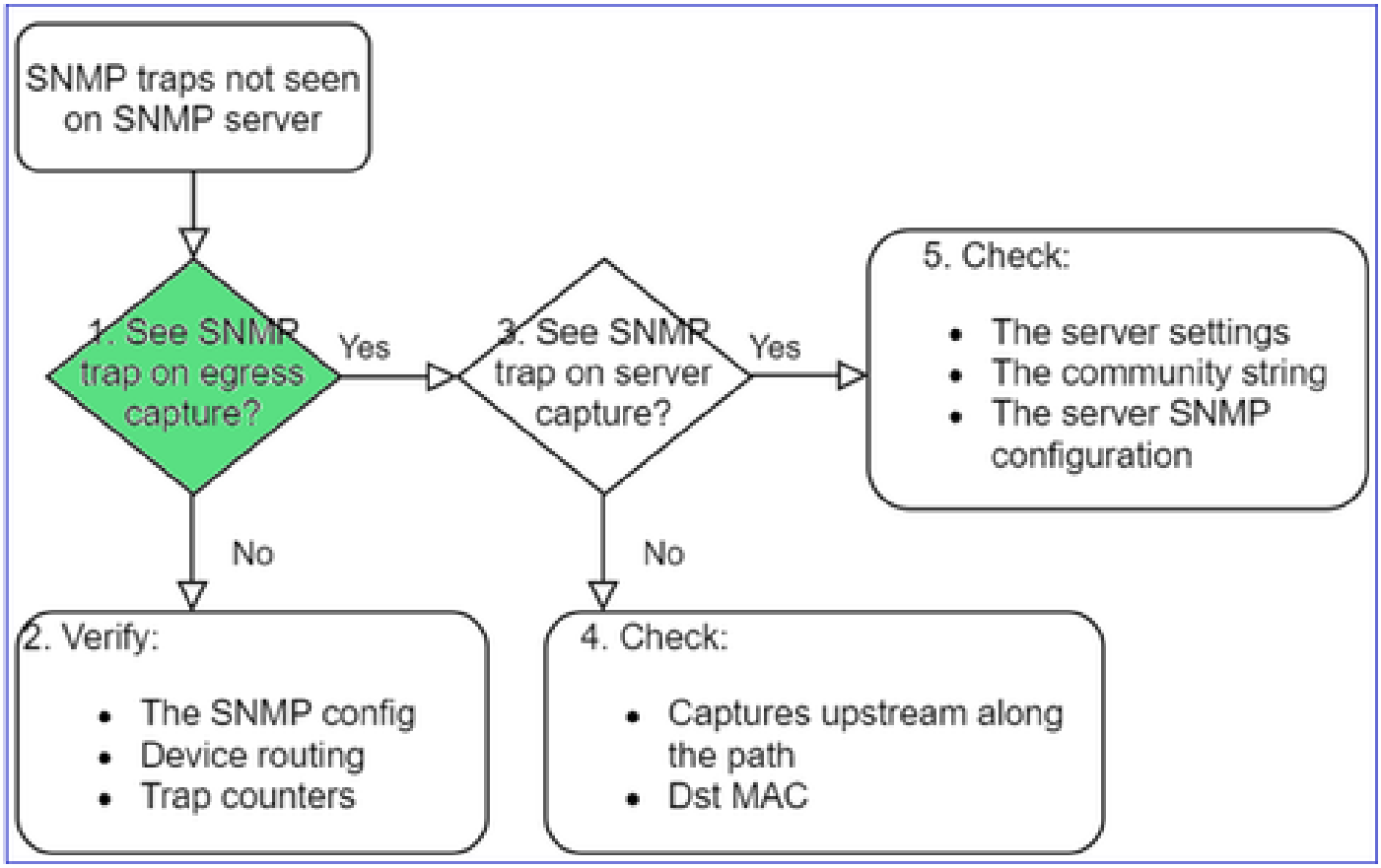
موصى باستكشاف الأخطاء وإصلاحها

هذه هي عملية أستكشاف أخطاء المخطط البانسيابي وإصلاحها لمسائل مالئمة FirePOWER

SNMP:




1. هل ترى رسائل تنبيه SNMP على التقاط الخروج؟



للالتقاط رسائل تنبيه LINA/ASA على واجهة الإدارة:

```
<#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
```

للالتقاط رسائل تنبيه LINA/ASA على واجهة البيانات:

```
<#root>

firepower#

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

للالتقاط رسائل تنبيه FXOS (41xx/9300):

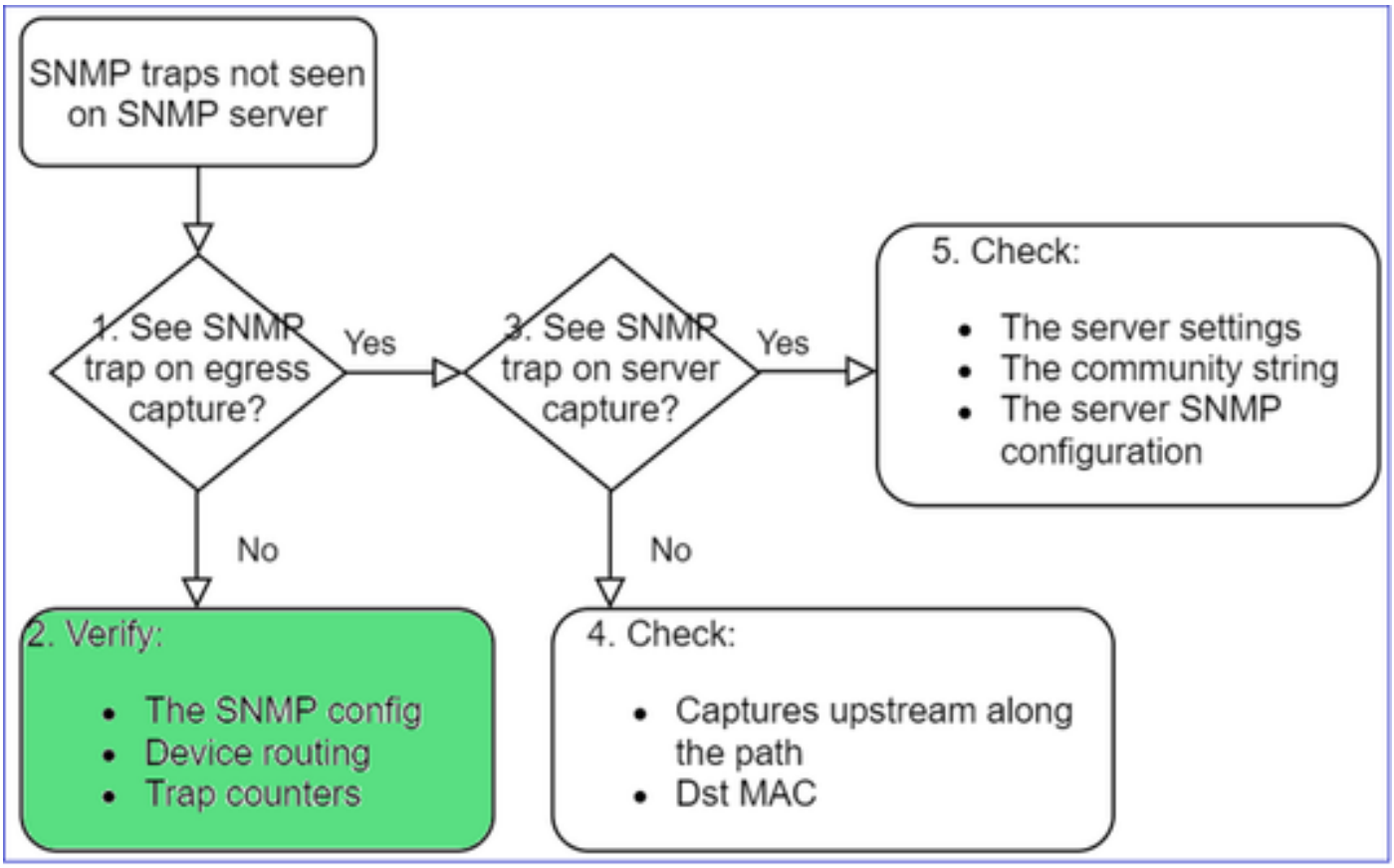
```
<#root>

firepower#

connect fxos


firepower(fxos)#

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


 1 2021-08-02 11:22:23.661436002  10.62.184.9 → 10.62.184.23 SNMP 160 snmpV2-trap 10.3.1.1.2.1.1.3.0 10.3.1.1
firepower(fxos)#

exit


firepower#

connect local-mgmt


firepower(local-mgmt)#
```

```
dir
```

```
1 11134 Aug 2 11:25:15 2021 SNMP.pcap
firepower(local-mgmt)#
```

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

2. إذا كنت ال ترى الحزم على واجهة الخروج




<#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
```

تكوين رسائل تنبيه FXOS SNMP:

<#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
```

ملاحظة: في وضع 1xxx/21xx، لا ترى هذه الإعدادات إلا في حالة الأجهزة > إدارة الأجهزة > تكوين SNMP!

- توجيه LINA/ASA لرسائل التنبيه من خلال واجهة الإدارة:

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

- توجيه LINA/ASA لرسائل التنبيه من خلال واجهة البيانات:

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

- توجيه FXOS (41xx/9300):

```
<#root>
FP4145-1#
show fabric-interconnect
```

- عدادات رسائل التنبيه (LINA/ASA):

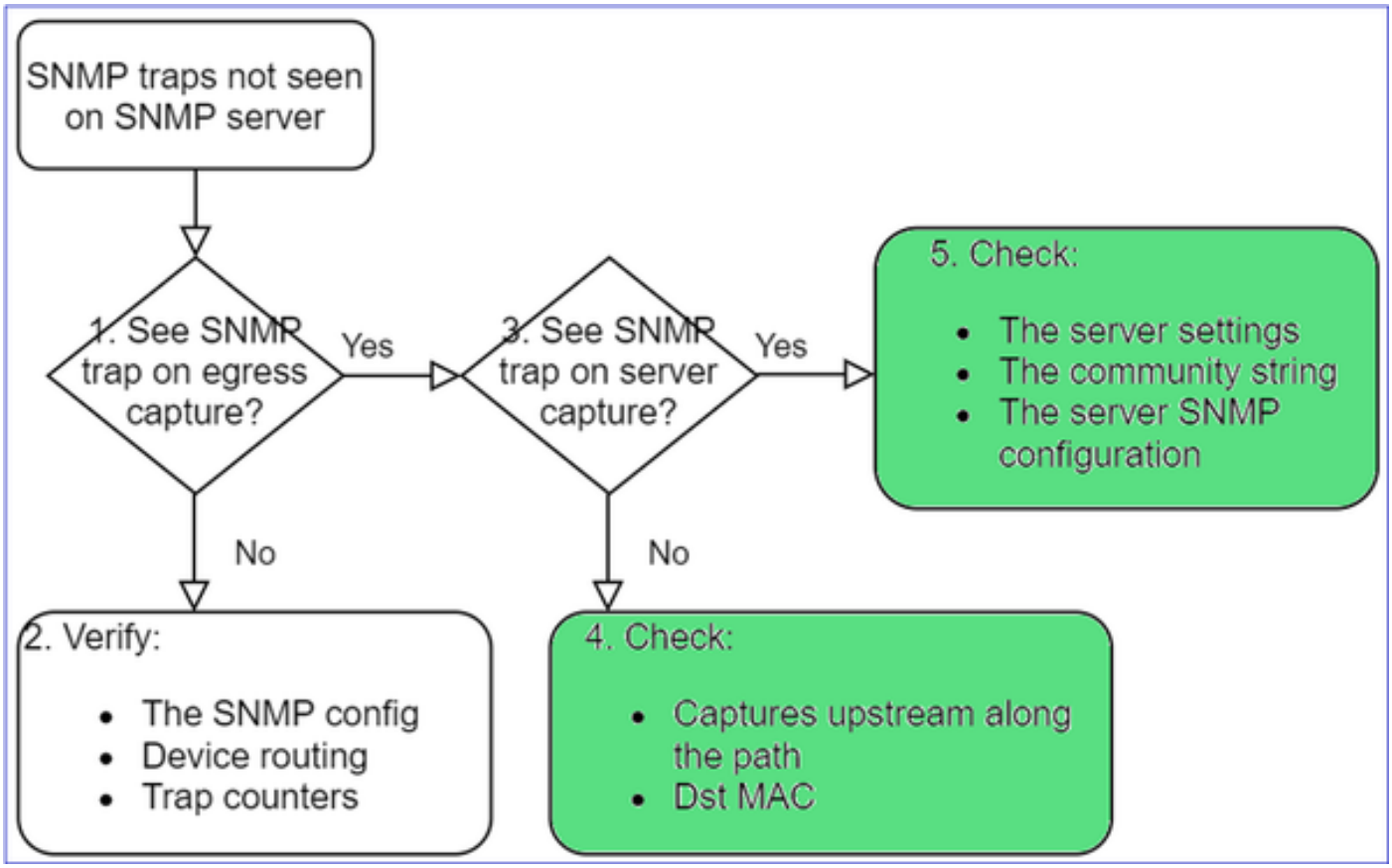
```
<#root>
firepower#
show snmp-server statistics | i Trap
```

```
    20 Trap PDUs
```

وFXOS:

```
<#root>

FP4145-1#

connect fxos


FP4145-1(fxos)#

show snmp | grep Trap

        1296 Out Traps PDU
```

عمليات التحقق الإضافية




- التقط صورة لخادم SNMP الخاص بالوجهة.

أشياء أخرى للتحقق منها:

- تلتقط على طول المسار.
- عنوان MAC الخاص بالوجهة لحزم رسائل تنبيه SNMP.
- إعدادات خادم SNMP وحالته (على سبيل المثال، جدار الحماية والمنافذ المفتوحة وما إلى

ذلك).
- سلسلة مجتمع SNMP.
- تكوين خادم SNMP.

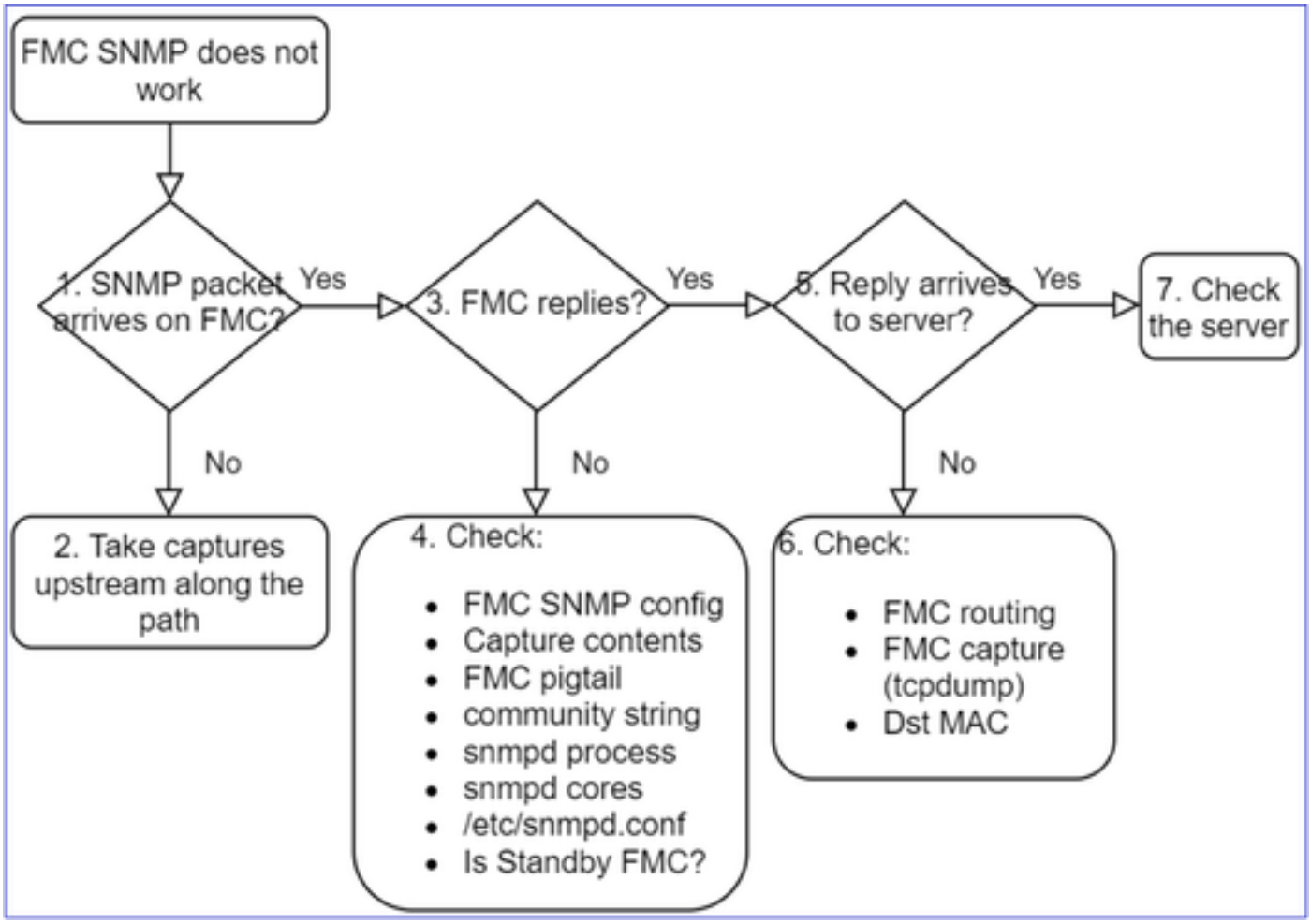
## ال يمكن مراقبة FMC عبر SNMP

أوصاف المشكلة (نموذج من حالات Cisco TAC الحقيقية):

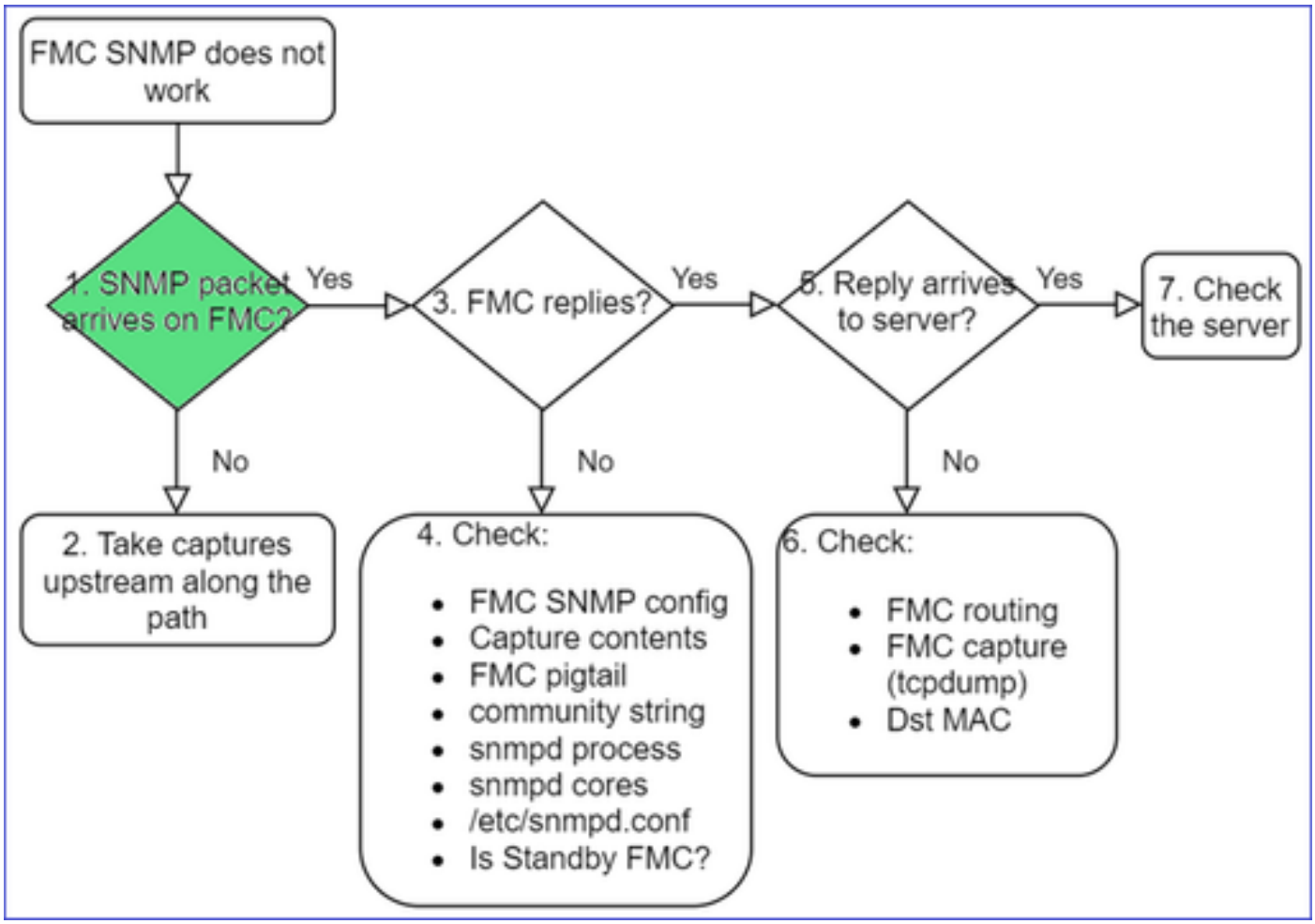
- "ال يعمل SNMP في وضع استعداد FMC."
- "الحاجة إلى مراقبة ذاكرة FMC."
- "هل يجب أن يعمل SNMP في وضع استعداد 192.168.4.0.8 FMC؟"
- "علينا تكوين FMCs لمراقبة موارده مثل وحدة المعالجة المركزية والذاكرة وما إلى ذلك".

كيفية أستكشاف الأخطاء وإصلاحها

هذه هي العملية لاستكشاف أخطاء المخطط الانسيابي الخاصة بمشكلات SNMP الخاصة بوحدة التحكم في إدارة للوحة الأساسية (FMC) وإصلاحها:




1. هل حزمة SNMP في طريقها إلى FMC؟




- الالتقاط على واجهة إدارة 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.
```

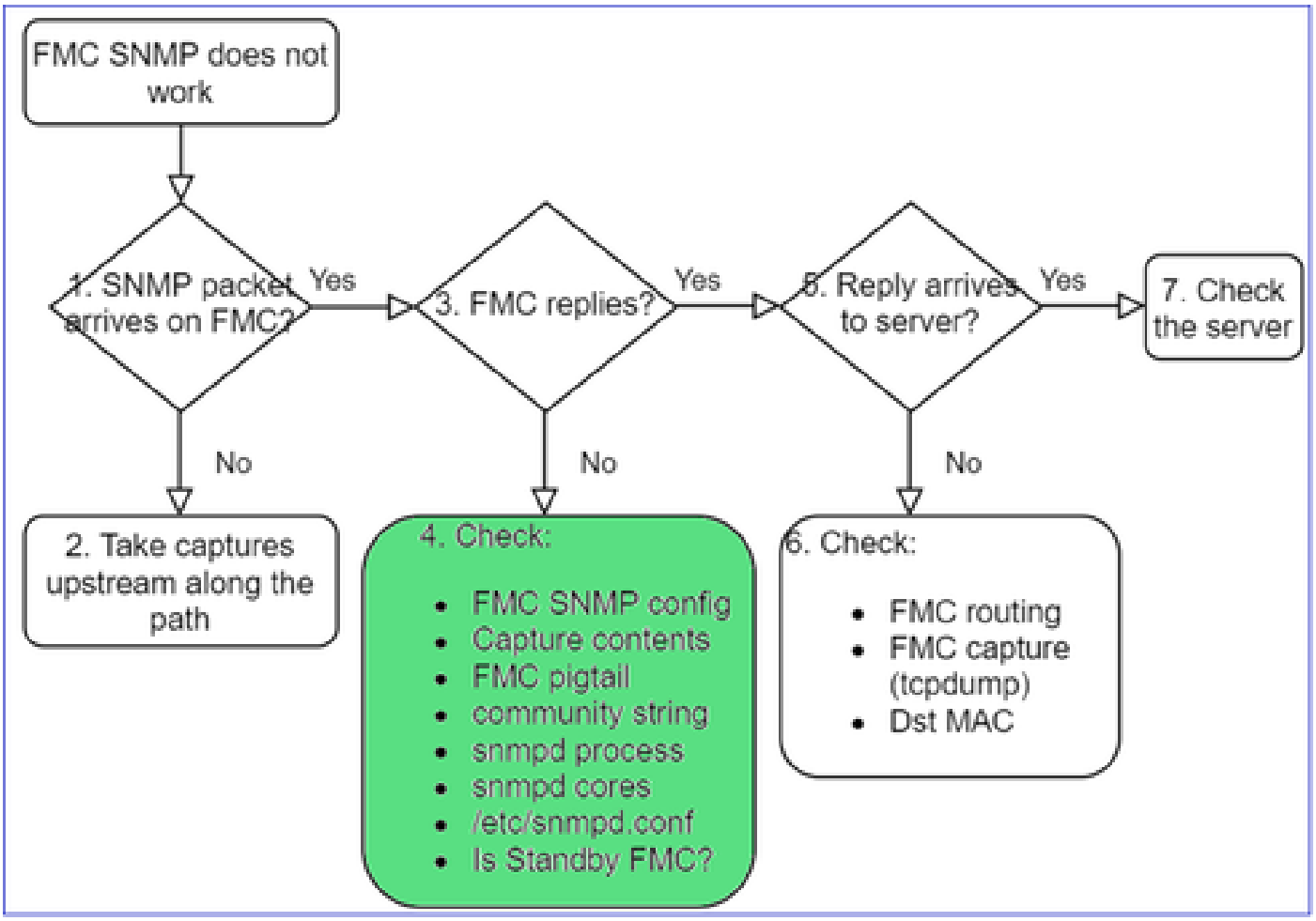
تلميح: حفظ الالتقاط على FMC /var/common/ directory وتنزيله من واجهة مستخدم FMC

<#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.
```

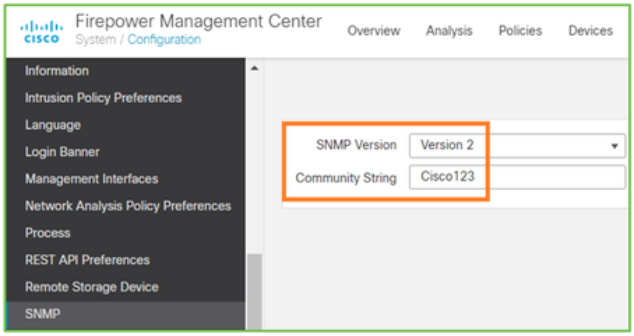
```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C46 packets captured
46 packets received by filter
```

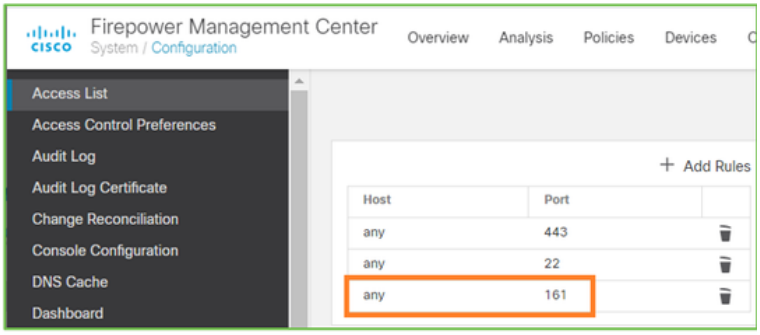
هل يرد FMC؟




إذا لم يرد FMC بالتحقق:

- تكوين FMC SNMP (النظام > التكوين)
  1. قسم SNMP
  2. قسم قائمة الوصول




إذا لم يرد FMC بالتحقق:

- التقاط محتويات (pcap)
- سلسلة المجتمع (يمكن مالحظة ذلك في اللقطات)
- إخراج ألمر pigtail الخاص بـ FMC (البحث عن ألخطاء، حالات الفشل، اآلثار) ومحتويات /var/log/snmpd.log
- عملية 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

- ملفات snmpd ألأساسية

<#root>

admin@FS2600-2:~$

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

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

- ملف تكوين الواجهة الخلفية في /etc/snmpd.conf:

<#root>

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

**sudo cat /etc/snmpd.conf**

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

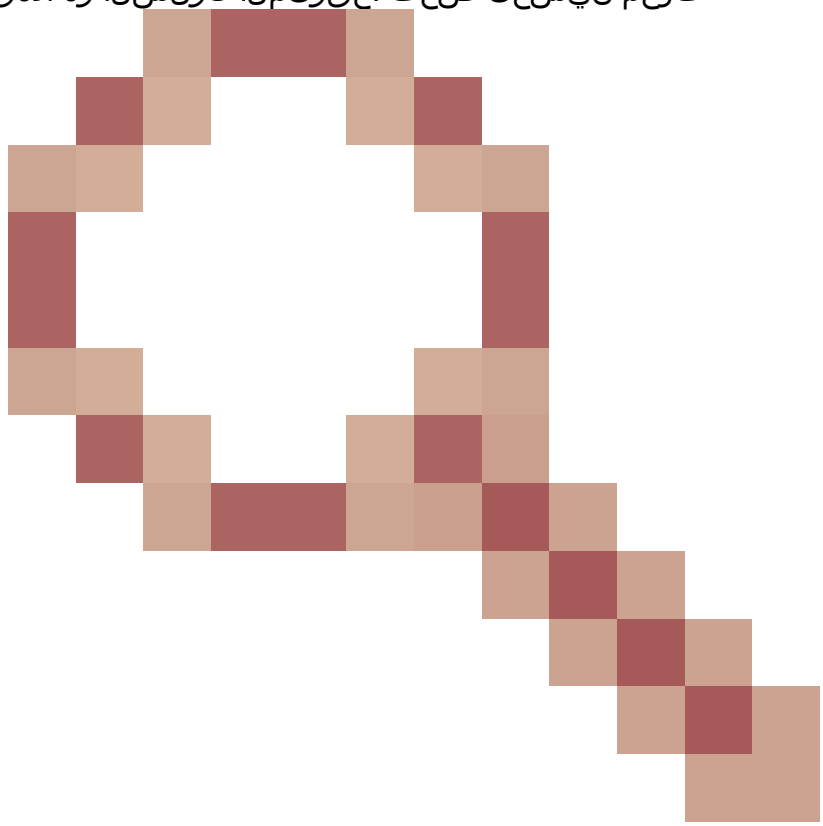
---

مالحظة: إذا تم تعطيل بروتوكول SNMP، فإن ملف snmpd.conf غير موجود

---

- هل FMC في وضع االستعداد؟

في إصدارات ما قبل 6.4.0-9 وما قبل 6.6.0، الـ FMC في وضع الاستعداد بإرسال بيانات SNMP (يكون snmpd في حالة انتظار). وهذا هو السلوك المتوقع. فحص تحسين معرف



تصحيح الأخطاء من Cisco CSCvs32303

يتعذّر تكوين SNMP

أوصاف المشكلة (نموذج من حالات Cisco TAC الحقيقية):

- "نريد تكوين بروتوكول SNMP لـ Cisco Firepower Management Center وFirepower 4115 Threat Defense."
- "الدعم باستخدام تكوين SNMP على FTD".
- "نريد تمكين مراقبة SNMP على جهاز FTD الخاص بي."
- "نحاول تكوين خدمة SNMP في FXOS، لكن النظام لا يتيح لنا التخزين المؤقت في النهاية. يقول خطأ: التغييرات غير مسموح بها. أستخدم 'Connect ftd' لإجراء التغييرات.
- "نريد تمكين مراقبة SNMP على جهاز FTD الخاص بنا."
- "يتعذّر تكوين SNMP على FTD واكتشاف الجهاز في المراقبة."

كيفية التعامل مع مشكلات تكوين SNMP

الأشياء الأولى: التوثيق!

- اقرأ المستند الحالي!
- دليل تكوين FMC:

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

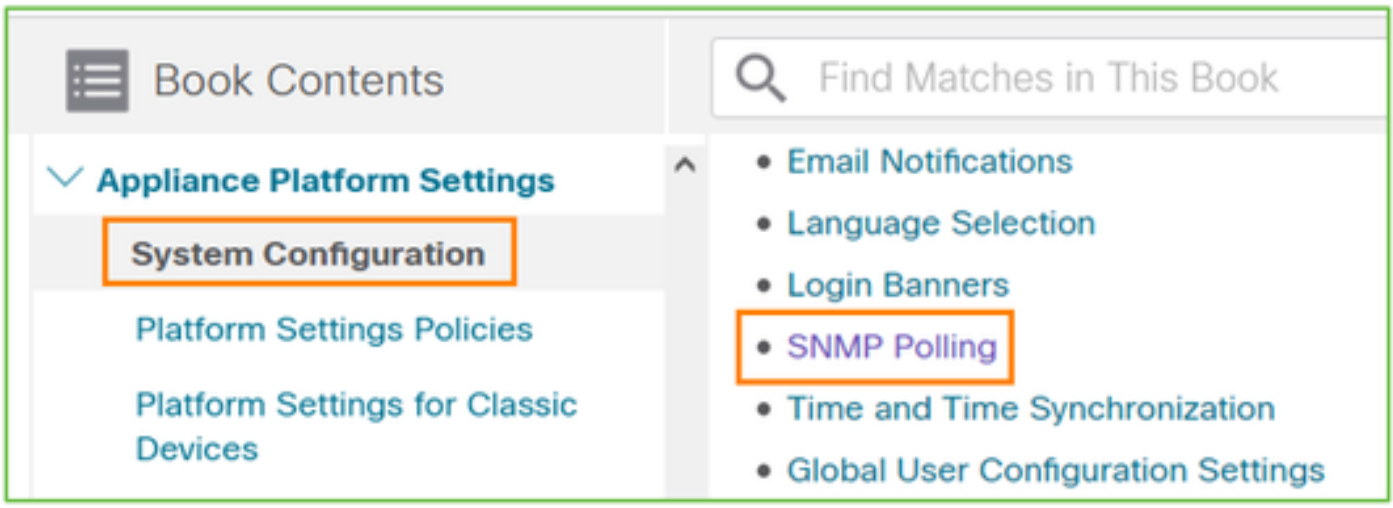
- دليل تكوين FXOS:

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

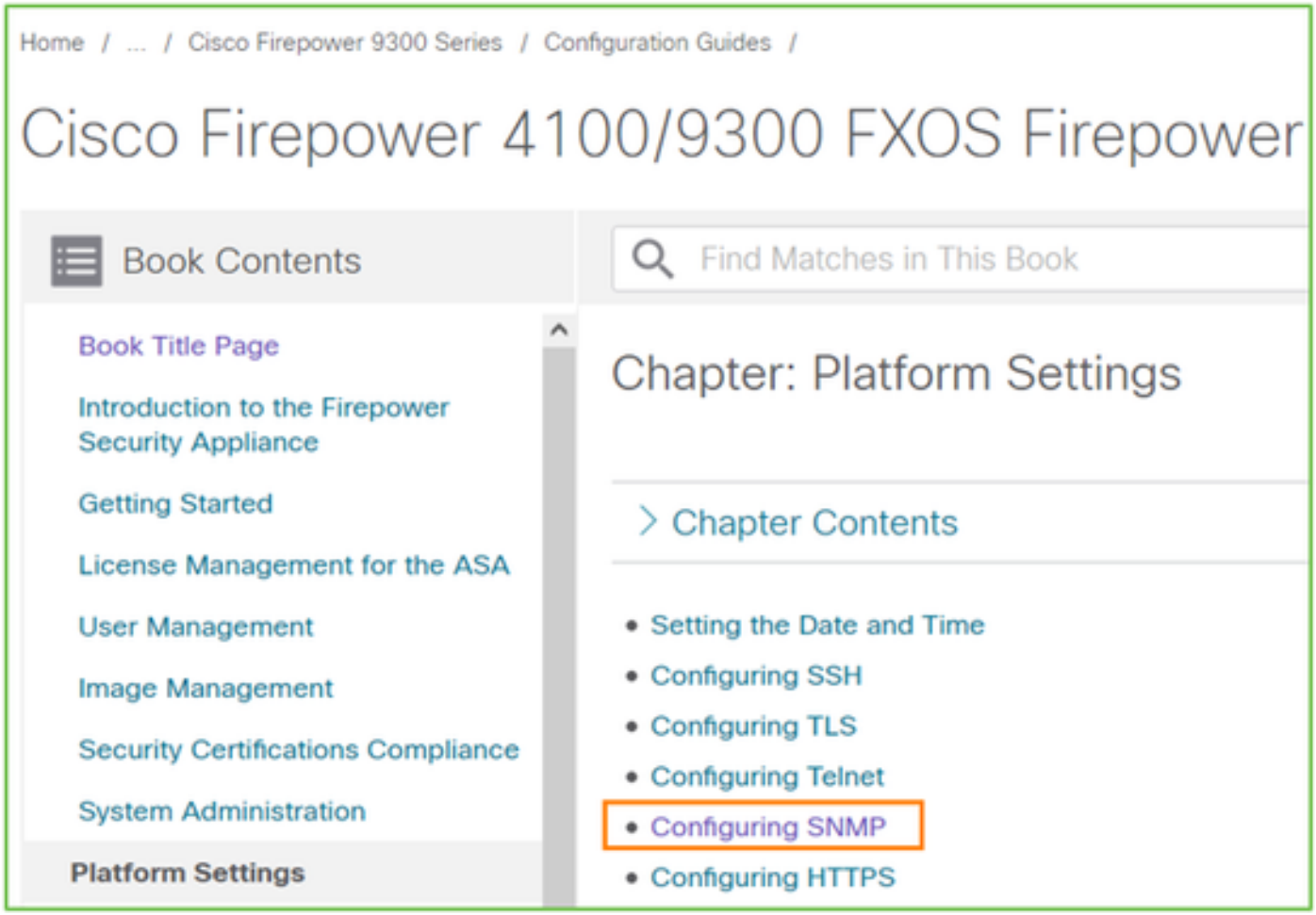
guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB

انتبه إلى مستندات SNMP المختلفة!

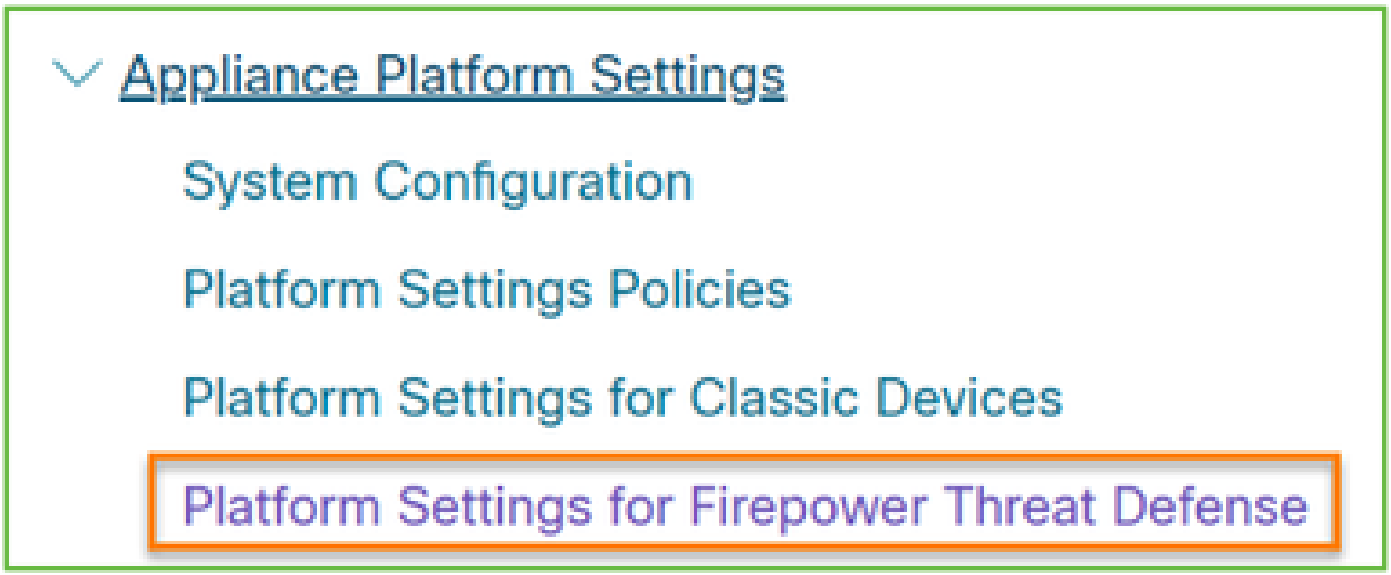
بروتوكول SNMP الخاص بـ FMC:




بروتوكول SNMP الخاص بـ FXOS:




تكوين FirePower 41xx/9300 SNMP:




تكوين Firepower 1xxx/21xx SNMP:


## تكوين SNMP في FirePower Device Manager (FDM)

أوصاف المشكلة (نموذج من حالات Cisco TAC الحقيقية):

- "نحن بحاجة إلى إرشادات حول SNMPv3 في FirePower على الجهاز باستخدام FDM."
- "تكوين SNMP لا يعمل على جهاز FPR 2100 من FDM."
- "يتعذّر الحصول على تكوين SNMP v3 ليعمل على FDM."
- "مساعدة تكوين FDM 6.7 SNMP."
- "تمكين SNMP v3 في Firepower FDM."

كيفية التعامل مع مشكلات تكوين SNMP FDM

- بالنسبة للإصدار pre-6.7، يمكنك إجراء تكوين SNMP باستخدام FlexConfig:

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

- بدءاً من الإصدار 6.7 من Firepower، لم يعد يتم تكوين SNMP باستخدام FlexConfig، بل

باستخدام واجهة برمجة تطبيقات REST:

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

## أوراق المعلومات المرجعية لاستكشاف أخطاء SNMP وإصلاحها

1xxx/21xx/41xx/9300 (LINA/ASA) - ما يجب تجميعه قبل فتح حالة مع مركز المساعدة الفنية (TAC) في Cisco

| | الوصف |
|---|---|
| firepower# show run snmp-server | تحقق من تكوين بروتوكول SNMP الخاص بـ ASA/FTD LINA. |
| firepower# show snmp-server statistics | تحقق من إحصائيات SNMP على ASA/FTD LINA. ركّز على عدادات إدخال حزم SNMP وإخراج حزم SNMP. |
| > capture-traffic | التقاط حركة المرور على واجهة الإدارة. |
| firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161 | التقاط حركة مرور البيانات على واجهة البيانات (اسم 'net201') لـ UDP 161 (استطلاع SNMP). |
| firepower# capture SNMP-TRAP interface net208 match udp any any eq 162 | التقاط حركة مرور البيانات على واجهة البيانات (nameIf 'net208') لـ UDP 162. (اختبارات SNMP). |
| firepower# show capture SNMP-POLL packet-number 1 trace | تتبع حزمة SNMP الخاصة بالمدخل التي تصل إلى واجهة بيانات ASA/FTD LINA. |
| admin@firepower:~$ sudo tcpdump -i tap_nlp | التقاط على واجهة الضغط الداخلية لـ NLP (عملية LINA التي لا تدعم عملية). |
| firepower# show conn all protocol udp port 161 | تحقق من جميع اتصالات ASA/FTD LINA على UDP 161 (استطلاع SNMP). |
| firepower# show log \| i 302015.*161 | التحقق من سجل ASA/FTD LINA 302015 لاستطلاع SNMP. |

| | |
|---|---|
| firepower# more system:running-config \| ا عمتجم | التحقق من سلسلة مجتمع SNMP. |
| firepower# debug menu netsnmp 4 | التحقق من تكوين SNMP وموعّ فلعملية. |
| firepower# show asp table classify interface net201 domain permit match port=161 | تحقق من قوائم التحكم في الوصول (ACL) المسموح بها على واجهة "Net201" لحركة مرور SNMP الخاصة. |
| firepower# show disk0: \| بل i | تحقّق مما إذا كانت هناك أي ملفات أساسية لحركة مرور SNMP. |
| admin@firepower:~$ ls -l /var/data/cores | تحقّق مما إذا كانت هناك أي ملفات أساسية لحركة مرور SNMP. ينطبق فقط على FTD. |
| firepower# show route | التحقق من جدول توجيه ASA/FTD LINA. |
| > show network | التحقق من جدول توجيه مستوى إدارة FTD. |
| admin@firepower:~$ tail -f /mnt/disk0/log/ma_ctx2000.log | التحقق من/استكشاف أخطاء SNMPv3 وإصلاحها على FTD. |
| firepower# debug snmp trace [255]<br>firepower# debug snmp verbose [255]<br>firepower# debug snmp error [255]<br>firepower# debug snmp packet [255] | الأوامر المخفية في الإصدارات الأحدث. عمليات تصحيح الأخطاء الداخلية، مفيدة لاستكشاف أخطاء SNMP وإصلاحها من خلال مركز المساعدة الفنية (TAC) في Cisco. |

41xx/9300 (FXOS) – ما يجب تجميعه قبل فتح حالة مع مركز المساعدة الفنية (TAC) في Cisco

| | الوصف |
|---|---|
| firepower# connect fxos<br>firepower(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 161" limit-captured-frames 50 write workspace:///SNMP-POLL.pcap | التقاط FXOS للاستطلاع عن SNMP (UDP 161)<br>تحميل إلى خادم FTP بعيد |

| | |
|---|---|
| firepower(fxos)# exit<br><br>firepower# connect local-mgmt<br><br>firepower(local-mgmt)# dir<br><br>1 11152 Jul 26 09:42:12 2021 SNMP.pcap<br><br>firepower(local-mgmt)# copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap | FTP IP: 192.0.2.100<br><br>اسم مستخدم FTP: ftp |
| firepower# connect fxos<br><br>firepower(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap | التقاط FXOS لرسائل تنبيه SNMP (UDP 162) |
| firepower# scope system<br><br>firepower /system # scope services<br><br>firepower /system/services # show ip-block detail | تحقق من قائمة التحكم بالوصول في FXOS |
| firepower# show fault | تحقق من أعطال FXOS |
| firepower# show fabric-interconnect | تحقق من تكوين واجهة FXOS وإعدادات العبّارة الافتراضية |
| firepower# connect fxos<br><br>firepower(fxos)# show running-config snmp all | التحقق من تكوين FXOS SNMP |
| firepower# connect fxos<br><br>firepower(fxos)# show snmp internal oids supported create<br><br>firepower(fxos)# show snmp internal oids supported | التحقق من معرّفات OID الخاصة بـ FXOS SNMP |
| firepower# connect fxos<br><br>firepower(fxos)# show snmp | التحقق من إعدادات وعدادات FXOS SNMP |
| firepower# connect fxos | تصحيح أخطاء FXOS SNMP ("الحزم" |

| | |
|---|---|
| firepower(fxos)# terminal monitor<br>firepower(fxos)# debug snmp pkt-dump<br>firepower(fxos)# debug snmp all | ("الكل" وأ<br>استخدم "terminal no monitor" و"undebug all" لإيقافها |

1xxx/21xx (FXOS) – ما يجب تجميعه قبل فتح حالة مع مركز المساعدة الفنية (TAC) في Cisco

| | الوصف |
|---|---|
| > capture-traffic | التقاط حركة المرور على واجهة الإدارة |
| > show network | التحقق من جدول توجيه مستوى إدارة FTD |
| firepower# scope monitoring<br>firepower /monitoring # show snmp [host]<br>firepower /monitoring # show snmp-user [detail]<br>firepower /monitoring # show snmp-trap | التحقق من تكوين FXOS SNMP |
| firepower# show fault | تحقق من أعطال FXOS |
| firepower# connect local-mgmt<br>firepower(local-mgmt)# dir cores_fxos<br>firepower(local-mgmt)# dir cores | التحقق من ملفات FXOS الأساسية (tracebacks) |

FMC – ما يجب تجميعه قبل فتح حالة مع مركز المساعدة الفنية (TAC) في Cisco

| | الوصف |
|---|---|
| admin@FS2600-2:~$ sudo tcpdump -i eth0 udp port 161 -n | التقاط حركة المرور على واجهة الإدارة للاستطلاع عن SNMP |
| admin@FS2600-2:~$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap | التقاط حركة المرور على واجهة الإدارة للاستطلاع عن SNMP وحفظها في ملف عيانم |

| | |
|---|---|
| admin@FS2600-2:~$ sudo pmtool status \| جيب صغير | التحقق من حالة عملية SNMP |
| admin@FS2600-2:~$ ls -al /var/common \| جيب صغير | التحقق من ملفات SNMP الأساسية (تتبع الأثر) |
| admin@FS2600-2:~$ sudo cat /etc/snmpd.conf | التحقق من محتويات ملف تكوين SNMP |

أمثلة على snmpwalk

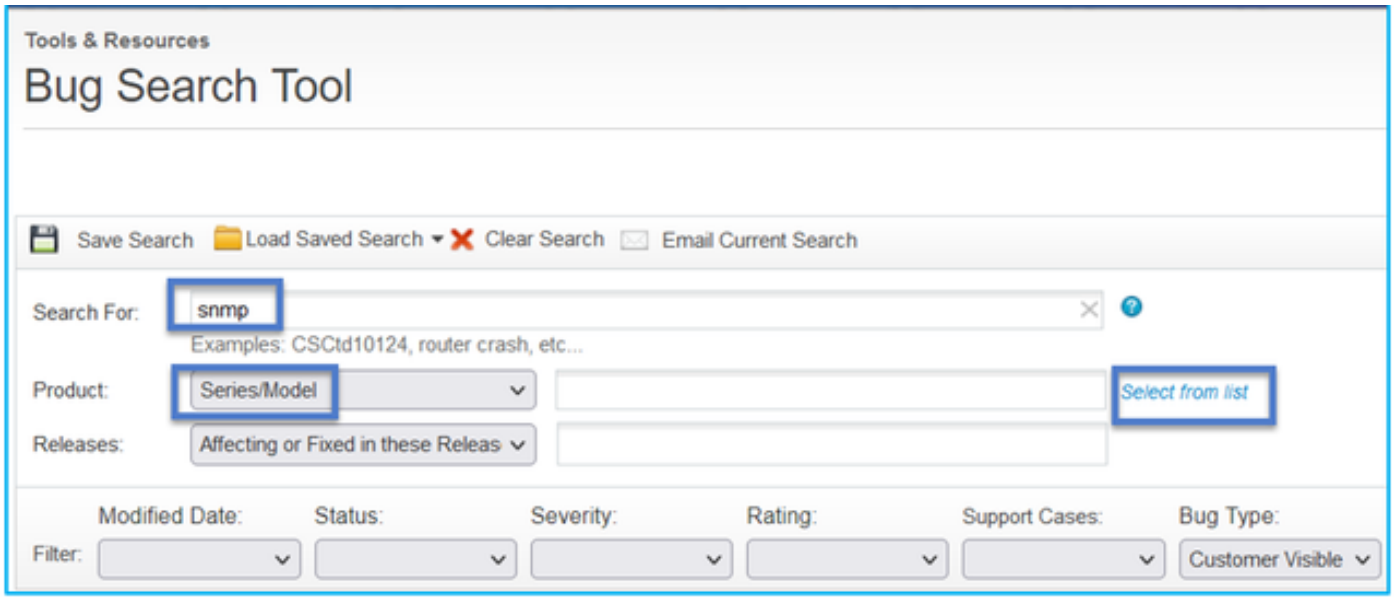
يمكن استخدام هذه الأوامر للتحقق واستكشاف الأخطاء وإصلاحها:

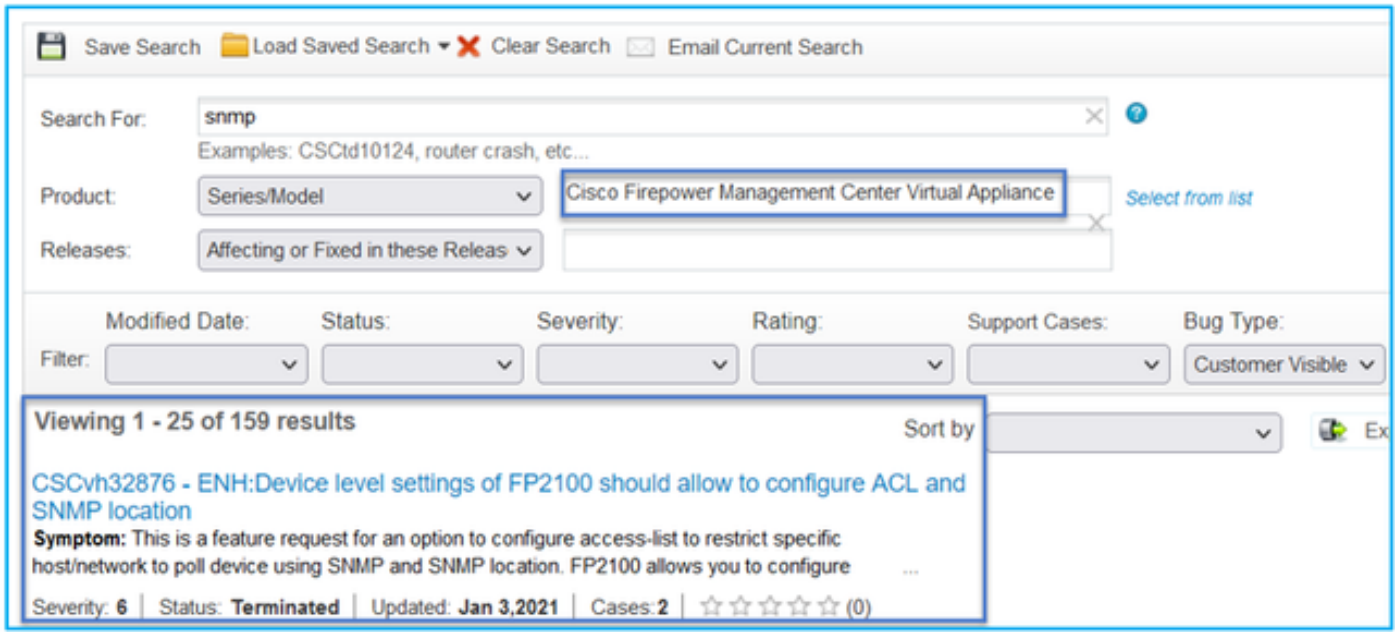
| | الوصف |
|---|---|
| # snmpwalk -c Cisco123 -v2c 192.0.2.1 | يجلب جميع معرّفات OID من المضيف البعيد باستخدام SNMP v2c.<br><br>Cisco123 = Community string<br><br>192.0.2.1 = destination host |
| # snmpwalk -v2c -Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.109.1.1.1.1.3<br><br>أي.3.6.1.4.1.9.109.1.1.1.3.1 = Gigabit32: 0 | يجلب OID محدد من المضيف البعيد باستخدام SNMP v2c |
| # snmpwalk -c Cisco123 -v2c 192.0.2.1.10.3.1.1.4.1.9.109.1.1.1.1 -on<br><br>.10.3.1.4.1.9.109.1.1.1.1.6.1 = G32: 0 | يُظهر معرّفات الكائنات التي تم جلبها بتنسيق رقمي |
| # snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1 | يجلب جميع OID من المضيف البعيد باستخدام SNMP v3.<br><br>مستخدم SNMPv3 = cisco<br><br>مصادقة SNMPv3 = SHA.<br><br>ترخيص SNMPv3 = AES |
| # snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 - | يجلب جميع OID من المضيف |

| | |
|---|---|
| x AES -X Cisco123 192.0.2.1 | البعيد باستخدام SNMP v3 (MD5 وAES128) |
| # snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1 | SNMPv3 مع المصادقة فقط |

## كيفية البحث عن عيوب SNMP

1. انتقل إلى https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV
2. أدخل الكلمة الأساسية SNMP واختر تحديد من القائمة.




المنتجات الأكثر شيوعاً:

- برنامج Cisco Adaptive Security Appliance (ASA)

- Firepower 9300 Series
- الجهاز الظاهري Cisco Firepower Management Center
- جدار الحماية من الجيل التالي من Cisco Firepower

## معلومات ذات صلة

- قم بتكوين SNMP للدفاع ضد التهديدات
- تكوين SNMP على FXOS (UI)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).