

Configuration du protocole SNMP sur les pare-feu de nouvelle génération Firepower

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Châssis \(FXOS\) SNMP sur FPR4100/FPR9300](#)

[Configurer FXOS SNMPv1/v2c à l'aide de l'interface graphique](#)

[Configurer FXOS SNMPv1/v2c à l'aide de l'interface CLI](#)

[Configurer FXOS SNMPv3 à l'aide de l'interface graphique](#)

[Configurer FXOS SNMPv3 à l'aide de l'interface CLI](#)

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

[Configurer LINA SNMPv2c](#)

[Configurer LINA SNMPv3](#)

[Unification SNMP de lame MIO \(FXOS 2.12.1, FTD 7.2, ASA 9.18.1\)](#)

[SNMP sur FPR2100](#)

[Châssis \(FXOS\) SNMP sur FPR2100](#)

[Configurer FXOS SNMPv1/v2c](#)

[Configurer FXOS SNMPv3](#)

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

[Vérifier](#)

[Vérifier FXOS SNMP pour FPR4100/FPR9300](#)

[Vérifications de FXOS SNMPv2c](#)

[Vérifications de FXOS SNMPv3](#)

[Vérifier FXOS SNMP pour FPR2100](#)

[Vérifications de FXOS SNMPv2](#)

[Vérifications de FXOS SNMPv3](#)

[Vérifier FTD SNMP](#)

[Autoriser le trafic SNMP vers FXOS sur FPR4100/FPR9300](#)

[Configurer la liste d'accès globale sur l'interface graphique](#)

[Configurer la liste d'accès globale sur l'interface CLI](#)

[Vérification](#)

[Utiliser le navigateur d'objets OID \(Object Identifier\)](#)

[Dépannage](#)

[Impossible d'interroger FTD LINA SNMP](#)

[Impossible d'interroger FXOS SNMP](#)

[Quelles valeurs SNMP OID utiliser?](#)

[Impossible d'obtenir les dérouterements SNMP](#)

[Impossible de surveiller FMC à l'aide du protocole SNMP](#)

Introduction

Ce document décrit comment configurer et dépanner le protocole SNMP (Simple Network Management Protocol) sur les appliances FTD de pare-feu de nouvelle génération (NGFW).

Conditions préalables

Exigences

Ce document nécessite des connaissances de base du protocole SNMP.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les appareils Firepower NGFW peuvent être divisés en deux sous-systèmes principaux :

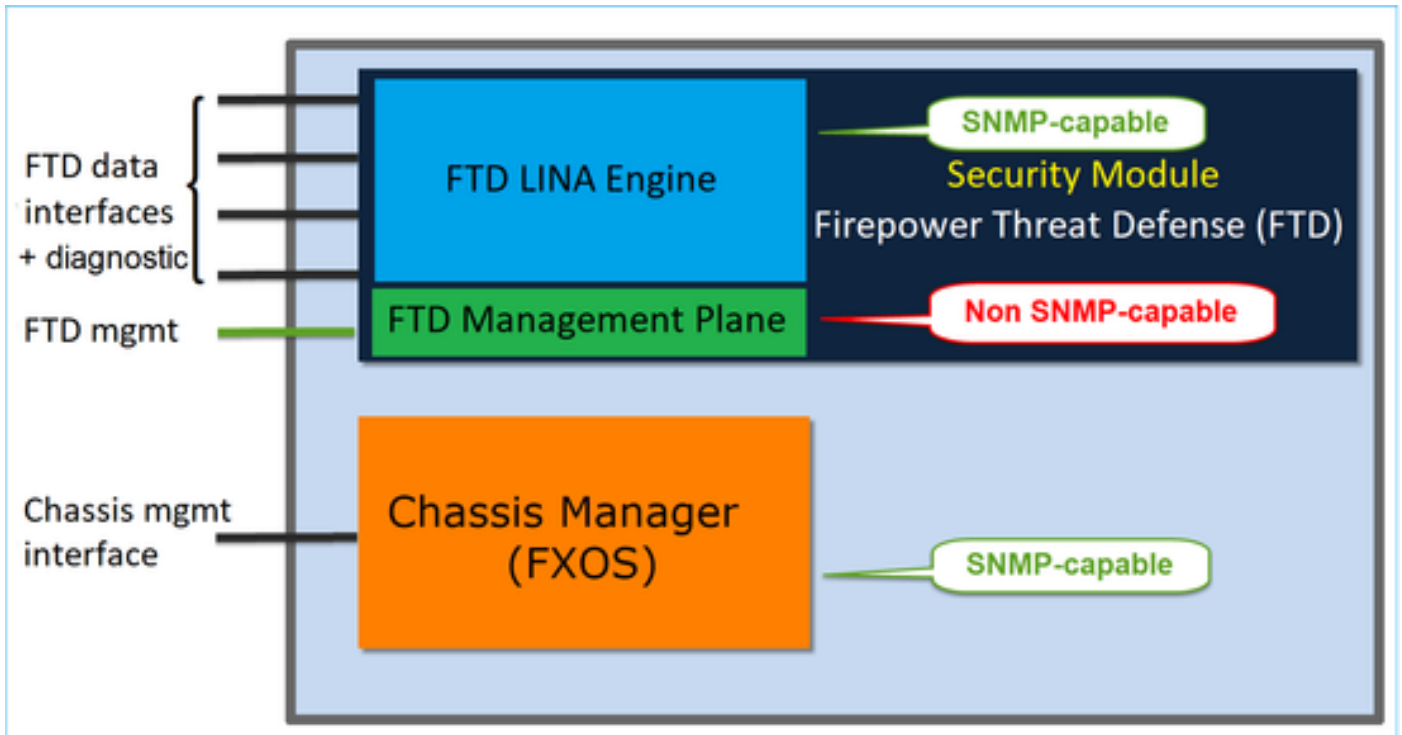
- Le système FX-OS (Firepower Extensible Operative System) contrôle le matériel du châssis.
- L'appareil Firepower Threat Defense (FTD) est exécuté dans le module.

FTD est un logiciel unifié qui se compose de deux moteurs principaux, le moteur Snort et le moteur LINA. Le moteur SNMP actuel de FTD dérive de l'appareil ASA (Adaptive Security Appliance) classique et offre une visibilité sur les fonctions liées à LINA.

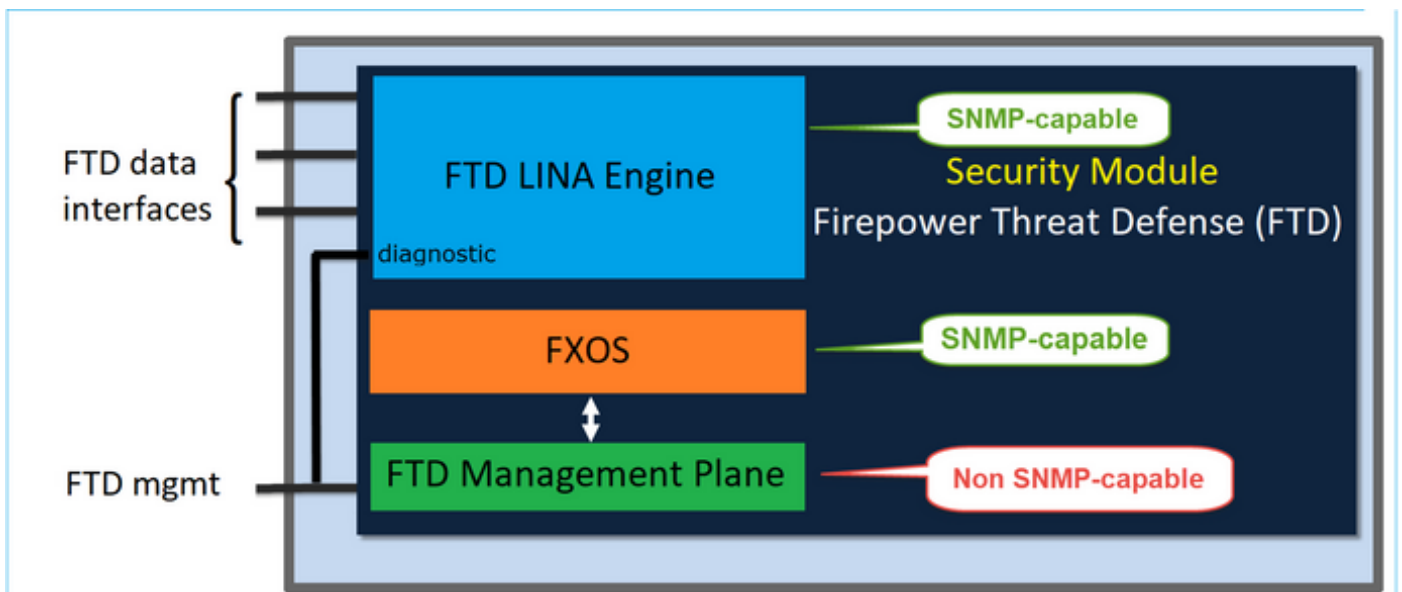
FX-OS et FTD ont des plans de contrôle indépendants et, à des fins de surveillance, ils ont des moteurs SNMP différents. Chaque moteur SNMP fournit des informations différentes et peut vouloir surveiller les deux pour obtenir une vue plus complète de l'état du périphérique.

Du point de vue matériel, il existe actuellement deux architectures principales pour les pare-feu de nouvelle génération Firepower : les séries Firepower 2100 et Firepower 4100/9300.

Les appareils Firepower de série 4100/9300 ont une interface dédiée à la gestion des appareils et constituent la source et de la destination du trafic SNMP adressé au sous-système FXOS. D'un autre côté, l'application FTD utilise une interface LINA (interface de données et/ou interface diagnostique. Dans les versions de l'appareil FMC ultérieures à la version 6.6, l'interface de gestion de FTD peut également être utilisée) pour la configuration SNMP.



Le moteur SNMP, sur les appareils Firepower de série 2100, utilise l'interface de gestion de FTD et le protocole IP. L'appareil lui-même relie le trafic SNMP reçu sur cette interface et le transmet au logiciel FXOS.

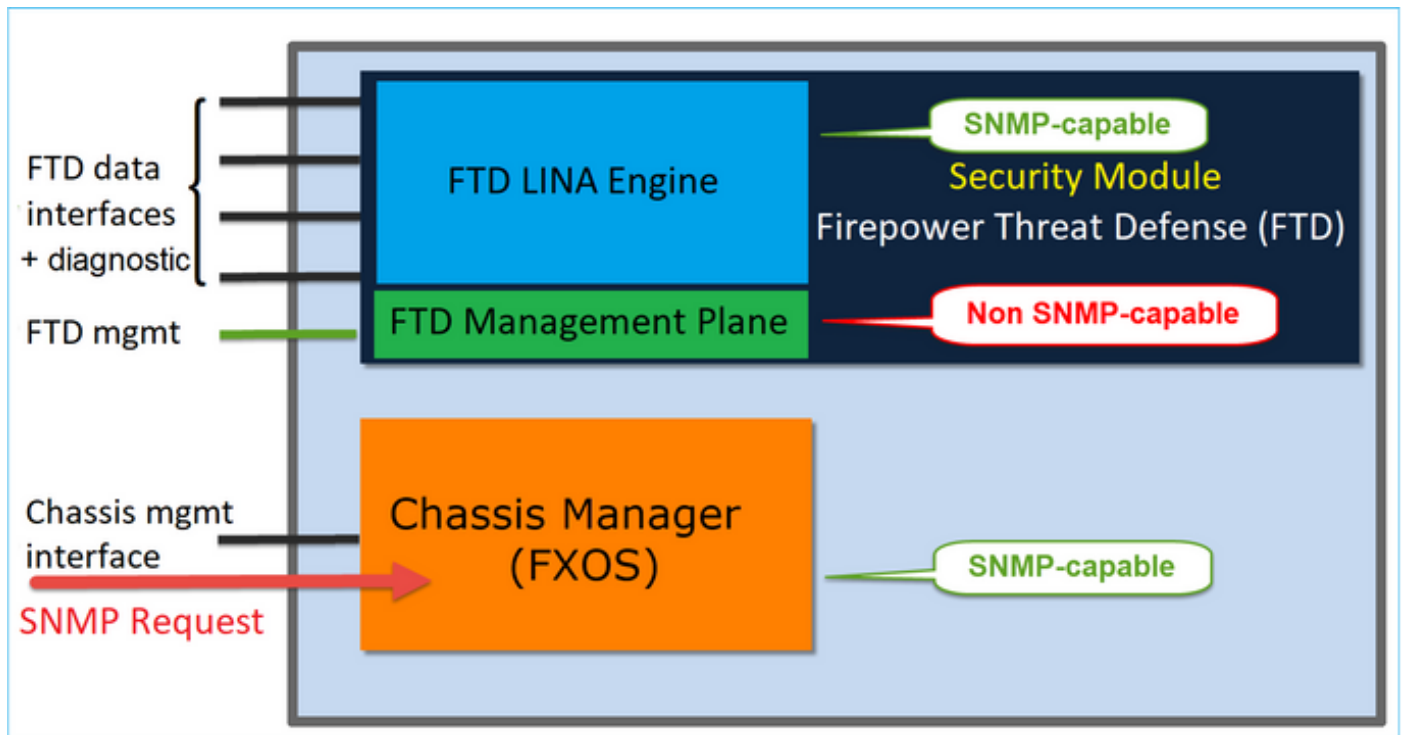


Sur les appareils FTD qui utilisent la version logicielle 6.6 ou une version ultérieure, les modifications suivantes ont été introduites :

- SNMP peut être utilisé avec une interface de gestion.
- Sur les plateformes de la série FPR1000 ou FPR2100, LINA SNMP et FXOS SNMP sont unifiés sur cette interface de gestion unique. En outre, il en résulte un point de configuration unique sur FMC, sous Platform settings > SNMP (paramètres de la plateforme > SNMP).

Configurer

Châssis (FXOS) SNMP sur FPR4100/FPR9300



Configurer FXOS SNMPv1/v2c à l'aide de l'interface graphique

Étape 1. Ouvrez l'interface utilisateur de Firepower Chassis Manager (FCM) et accédez à l'onglet Platform settings > SNMP (paramètres de la plateforme > SNMP). Cochez la case d'activation de SNMP, définissez l'identifiant Community (communauté) à utiliser lors de requêtes SNMP, puis sélectionnez Save (enregistrer).

Overview Interfaces Logical Devices Security Modules **Platform Settings**

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

Admin State: Enable **1**

Port: 161

Community/Username: Set: No **2**

System Administrator Name:

Location:

SNMP Traps


4

Name	Port	Version	V3 Privilege	Type

SNMP Users

Name	Auth Type	AES-128

3

 Remarque : si le champ Communauté/Nom d'utilisateur est déjà défini, le texte à droite du champ vide indique Définir : Oui. Si le champ Communauté/Nom d'utilisateur n'est pas encore renseigné avec une valeur, le texte à droite du champ vide indique Set : No

Étape 2. Configurez le serveur de destination des dérouterements de SNMP.

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

 Remarque : les valeurs de communauté pour les requêtes et les hôtes de déROUTement sont indépendantes et peuvent être différentes

L'hôte peut être défini par son adresse IP ou son nom. Sélectionnez OK pour enregistrer la configuration du serveur de déROUTement SNMP automatiquement. Il n'est pas nécessaire de sélectionner le bouton d'enregistrement sur la page principale du SNMP. La même chose se produit lorsque vous supprimez un hôte.

Configurer FXOS SNMPv1/v2c à l'aide de l'interface CLI

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

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

Configurer FXOS SNMPv3 à l'aide de l'interface graphique

Étape 1. Ouvrez FCM et accédez à l'onglet Platform Settings > SNMP (paramètres de la plateforme > SNMP).

Étape 2. Pour SNMP v3, il n'est pas nécessaire de définir un identifiant de communauté dans la section supérieure. Chaque utilisateur créé est en mesure d'exécuter avec succès des requêtes sur le moteur FXOS SNMP. La première étape consiste à activer SNMP sur la plateforme. Une fois cela fait, vous pouvez créer les utilisateurs et l'hôte de destination du déroulement. Les utilisateurs SNMP et les hôtes de déroulement SNMP sont enregistrés automatiquement.

Local Devices Security Modules Platform Settings

Admin State: Enable 1

Port: 161

Community/Username: Set: No

System Administrator Name:

Location:

SNMP Traps

4

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

SNMP Users

3

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

2

Étape 3. Ajoutez l'utilisateur SNMP en suivant les indications de l'image. Le type d'authentification est toujours « SHA », mais vous pouvez utiliser AES ou DES pour le chiffrement :

Add SNMP User ? X

Name:*

Auth Type: SHA

Use AES-128:

Password:

Confirm Password:

Privacy Password:

Confirm Privacy Password:

Étape 4. Ajoutez l'hôte de déroulement SNMP, comme illustré dans l'image :

Add SNMP Trap

Host Name:*

Community/Username:*

Port:*

Version: V1 V2 V3

Type: Traps Informs

V3 Privilege: Auth NoAuth Priv

Configurer FXOS SNMPv3 à l'aide de l'interface CLI

```

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

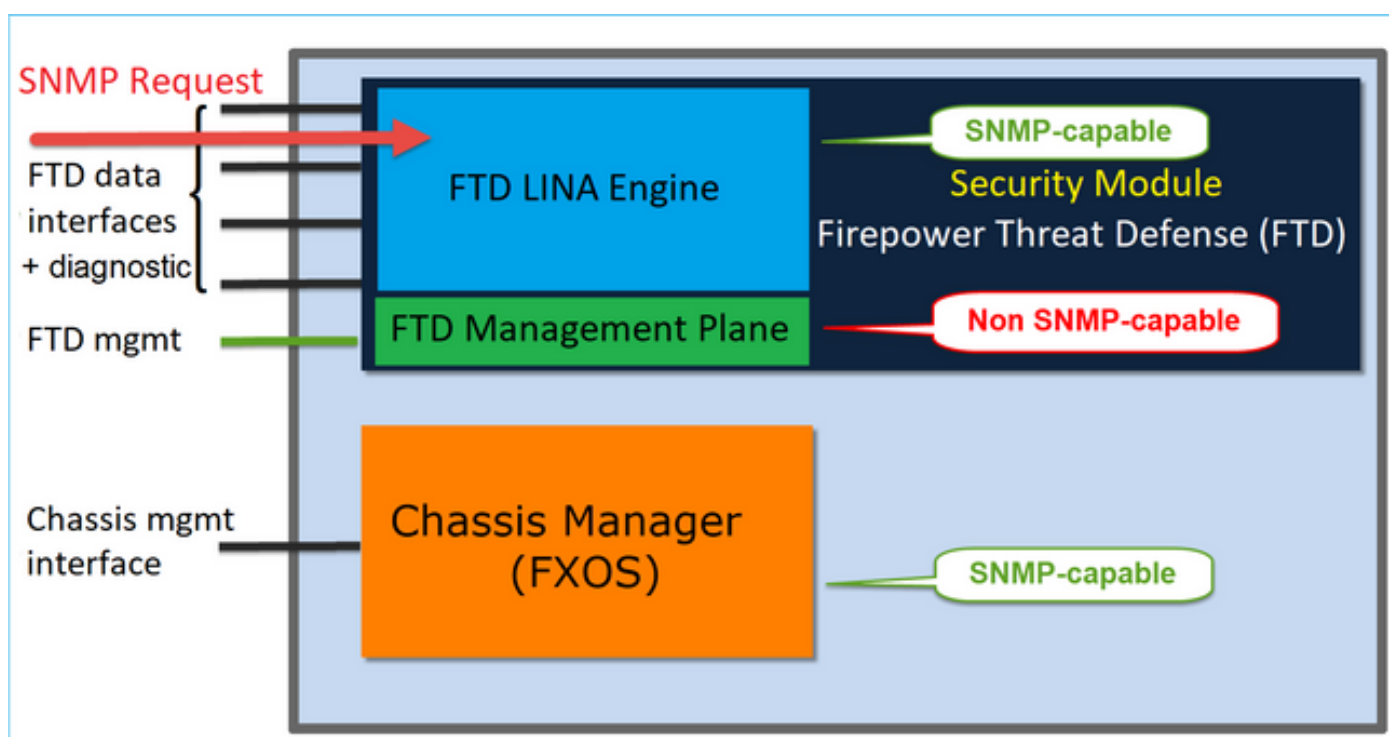
```

```

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

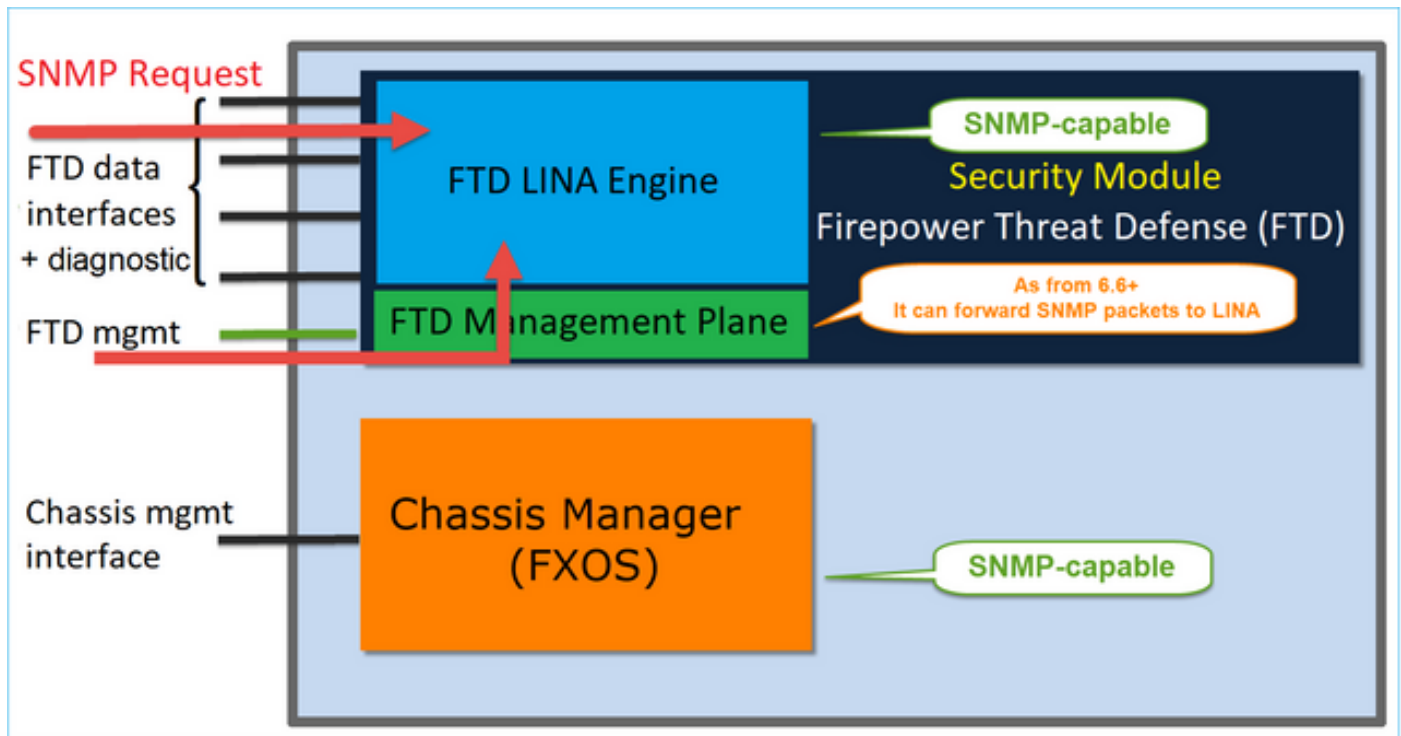
```

FTD (LINA) SNMP sur FPR4100/FPR9300



Changements dans les versions ultérieures à 6.6

- Dans les versions ultérieures à 6.6, vous avez également la possibilité d'utiliser l'interface de gestion de l'appareil FTD pour les interrogations et les dérouterments.



La fonction de gestion SNMP pour une seule adresse IP est prise en charge à partir de la version 6.6 sur toutes les plateformes FTD :

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 exécutant FTD
- FTDv

Configurer LINA SNMPv2c

Étape 1. Sur l'interface utilisateur de l'appareil FMC, accédez à **Devices > Platform Settings > SNMP** (appareils > réglages de la plateforme > SNMP). Cochez l'option « **Enable SNMP Servers** » (serveurs SNMP activés) et configurez les paramètres SNMPv2 comme suit :

Étape 2. Dans l'onglet **Hosts** (hôtes), sélectionnez le bouton **Add** (ajouter) et définissez les paramètres du serveur SNMP :

Edit SNMP Management Hosts

IP Address*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port (1 - 65535)

Available Zones

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

Selected Zones/Interfaces

OUTSIDE3

Vous pouvez également définir l'interface de diagnostic comme source pour les messages SNMP. L'interface de diagnostic est une interface de données qui autorise uniquement le trafic entrant et sortant (gestion uniquement).

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

Cette image provient de la version 6.6 et utilise le Light Theme.

En outre, dans les versions ultérieures à la version 6.6 de FTD, vous pouvez également choisir l'interface de gestion :

Add SNMP Management Hosts

IP Address*

SNMP-SERVER



SNMP Version

2c

Username

Community String

Confirm

Poll

Trap

Trap Port

162

(1 - 65535)

Reachable By:

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

Security Zones or Named Interface

Available Zones



Search

Add

2100_inside
2100_outside
cluster_dmz
cluster_inside
cluster_outside

Selected Zones/Interfaces

diagnostic

Interface Name

Add

Cancel

OK

Si vous avez sélectionné la nouvelle interface de gestion, LINA SNMP est disponible sur une

interface de gestion.

Le résultat :

Enable SNMP Servers

Read Community String

Confirm*

System Administrator Name

Location

Port (1 - 65535)

Hosts Users **SNMP Traps**

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

Configurer LINA SNMPv3

Étape 1. Sur l'interface utilisateur de l'appareil FMC, accédez à Devices > Platform Settings > SNMP (appareils > paramètres de la plateforme > SNMP). Cochez l'option Enable SNMP Servers (activer les serveurs SNMP) et configurez l'utilisateur et l'hôte SNMPv3 :

Enable SNMP Servers

Read Community String

Confirm*

System Administrator Name

Location

Port

Hosts **Users** SNMP Traps

Username Encryption Password Type

Add Username

Security Level

Username*

Encryption Password Type

Auth Algorithm Type

Authentication Password*

Confirm*

Encryption Type

Encryption Password*

Confirm*

OK Cancel

Overview Analysis Policies **Devices** Objects AMP Intelligence

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

mzafeiro_FTD4110-HA

Enter Description

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

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Port (1 - 65535)

Hosts Users SNMP Traps

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

Étape 2. Configurez également l'hôte qui recevra les dérivements :

Edit SNMP Management Hosts

IP Address*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port (1 - 65535)

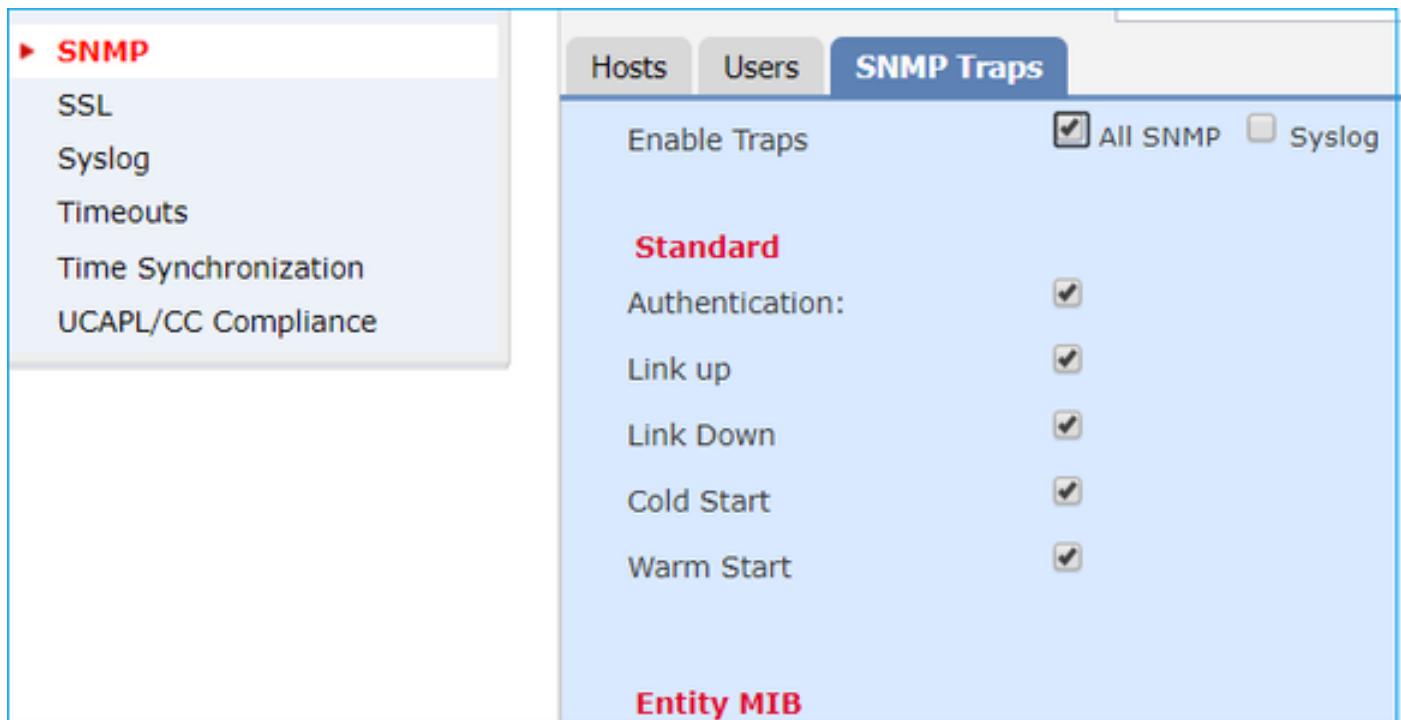
Available Zones

- INSIDE_FTD4110

Selected Zones/Interfaces

- OUTSIDE3

Étape 3. Les dérivements que vous souhaitez recevoir peuvent être sélectionnés dans la section SNMP Traps (dérivements SNMP) :



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

Comportement antérieur à 7.2

- Sur les plates-formes 9300 et 4100, les MIB SNMP pour les informations de châssis ne sont pas disponibles sur le protocole SNMP configuré sur les applications FTD/ASA. Il doit être configuré séparément sur le MIO via le gestionnaire de châssis et accessible séparément. MIO est le module de gestion et d'E/S (Supervisor).
- Deux stratégies SNMP distinctes doivent être configurées, l'une sur Blade/App et l'autre sur MIO pour la surveillance SNMP.
- Des ports distincts sont utilisés, un pour la lame et un pour la MIO pour la surveillance SNMP du même périphérique.
- Cela peut créer de la complexité lorsque vous essayez de configurer et de surveiller les périphériques 9300 et 4100 via SNMP.

Fonctionnement sur les versions plus récentes (FXOS 2.12.1, FTD 7.2, ASA 9.18.1 et versions ultérieures)

- Grâce à l'unification SNMP des lames MIO, les utilisateurs peuvent interroger les MIB LINA et MIO via les interfaces d'application (ASA/FTD).
- La fonction peut être activée ou désactivée via la nouvelle interface de ligne de commande MIO et l'interface utilisateur FCM (Chassis Mgr).
- L'état par défaut est désactivé. Cela signifie que l'agent SNMP MIO s'exécute en tant qu'instance autonome. Les interfaces MIO doivent être utilisées pour interroger les MIB du châssis/DME. Une fois la fonctionnalité activée, les interfaces d'application peuvent être utilisées pour interroger les mêmes MIB.
- La configuration est disponible sur l'interface utilisateur de Chassis Manager sous Platform-settings > SNMP > Admin Instance, où l'utilisateur peut spécifier l'instance FTD qui collationnerait/rassemblerait les MIB du châssis pour les présenter au NMS

- Les applications ASA/FTD natives et MI sont prises en charge.
- Cette fonctionnalité s'applique uniquement aux plates-formes MIO (FPR9300 et FPR4100).

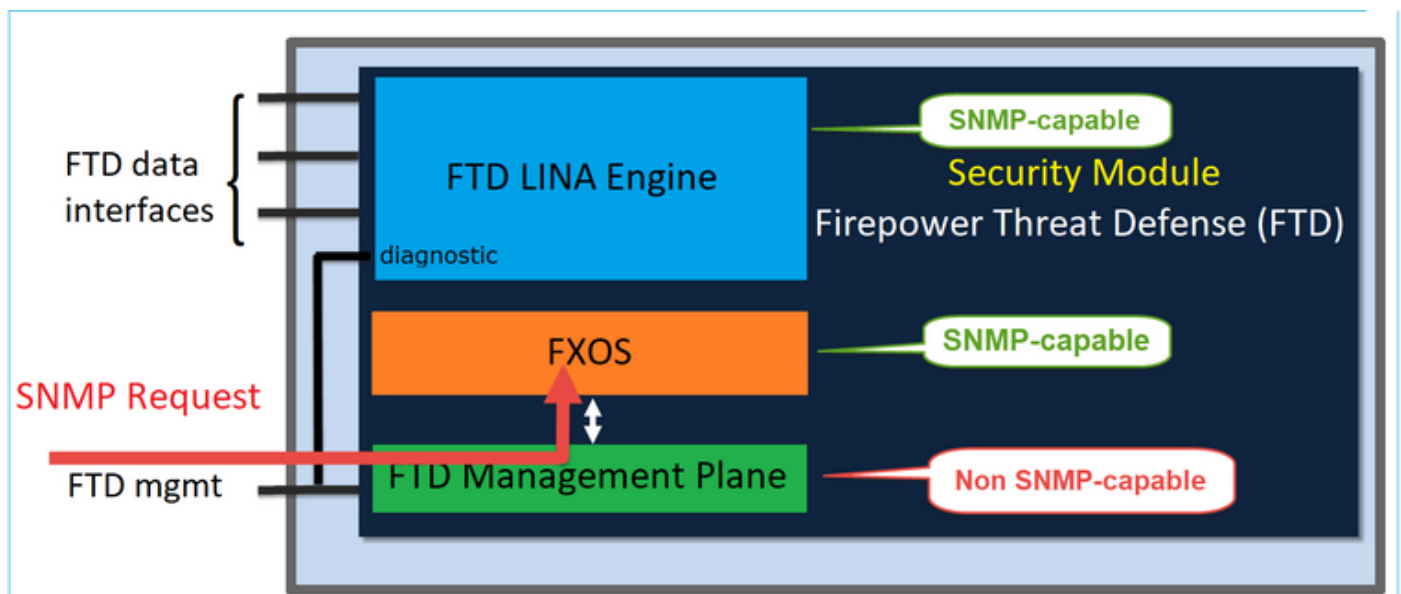
Conditions préalables, plates-formes prises en charge

- Version min. du gestionnaire prise en charge : FCM 2.12.1
- Périphériques gérés : gammes FPR9300 / FP4100
- Version minimale du périphérique géré prise en charge requise : FXOS 2.12.1, FTD 7.2 ou ASA 9.18.1

SNMP sur FPR2100

Il n'y a pas de FCM sur les systèmes FPR2100. La seule façon de configurer SNMP est sur FMC.

Châssis (FXOS) SNMP sur FPR2100



À partir de la version 6.6 de FTD, vous avez également la possibilité d'utiliser l'interface de gestion de FTD pour SNMP. Dans ce cas, les informations FXOS et LINA SNMP sont transférées à l'aide de l'interface de gestion de FTD.

Configurer FXOS SNMPv1/v2c

Ouvrez l'interface utilisateur de l'appareil FMC et rendez-vous à Devices > Device Management (appareils > gestion des appareils). Sélectionnez l'appareil et sélectionnez SNMP :

Overview Analysis Policies **Devices** Objects AMP Intelligence 4 Deploy 20+ System Help itebar

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FT2100-4 You have unsaved changes Save Cancel 3

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

Community: *****

System Admin Name: |

Location:

SNMP Traps Configuration

Hostname	Port	Version	V3 Privilege	Type
No records to display				

2 Add

SNMP Trap Configuration

Hostname:* 10.48.26.190

Community String:* *****

Port:* 162 (1 - 65535)

SNMP Version: V2

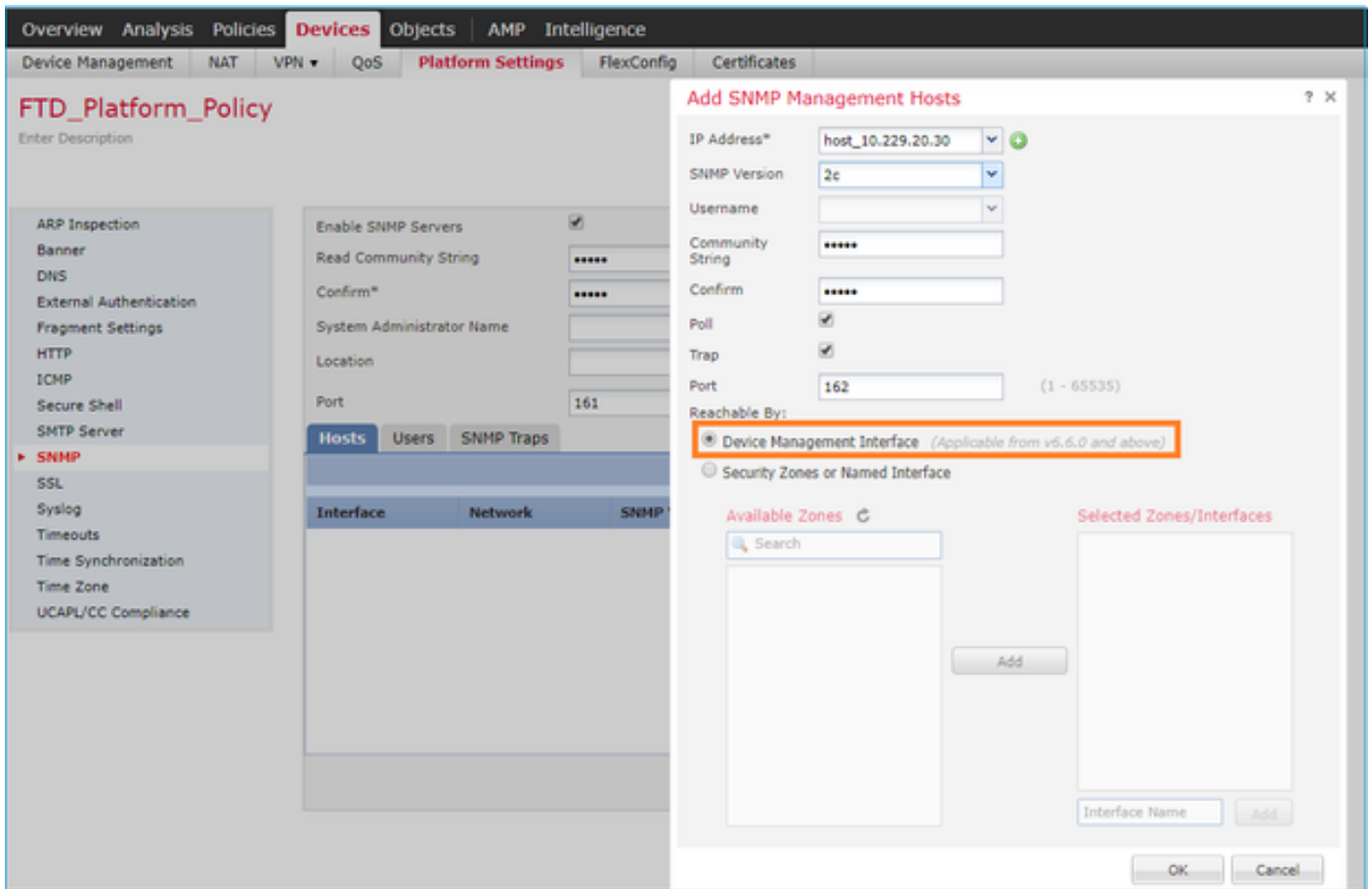
Type: TRAPS

Privilege: NO_AUTH

OK Cancel

Changement à partir de la version 6.6 de FTD

Vous pouvez définir l'interface de gestion de FTD :



Puisque l'interface de gestion peut également être configurée pour SNMP, la page affiche ce message d'avertissement :

La configuration SNMP de la plate-forme de périphérique sur cette page est désactivée si les paramètres SNMP sont configurés avec l'interface de gestion des périphériques via Périphériques > Paramètres de la plate-forme (Défense contre les menaces) > SNMP > Hôtes.

Configurer FXOS SNMPv3

Ouvrez l'interface utilisateur de l'appareil FMC et accédez à Choose Devices > Device Management Sélectionnez le périphérique et sélectionnez SNMP.

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

Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

FTD2100-4 Cisco Firepower 2110 Threat Defense You have unsaved changes Save Cancel 4

Device Routing Interfaces Inline Sets DHCP **SNMP**

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

Admin State: Enable 1

Port: 161

Community:

System Admin Name:

Location:

SNMP Traps Configuration 3 Add

Hostname	Port	Version	V3 Privilege	Type
No records to display				

SNMP Users Configuration 2 Add

Name	Auth Type	AES-128
No records to display		

SNMP User Configuration ? X

Username: *

Auth Algorithm Type: ▾

Use AES:

Password*

Confirm:

Privacy Password*

Confirm:

SNMP Trap Configuration

Hostname:* +

Community String:*

Port:* (1 - 65535)

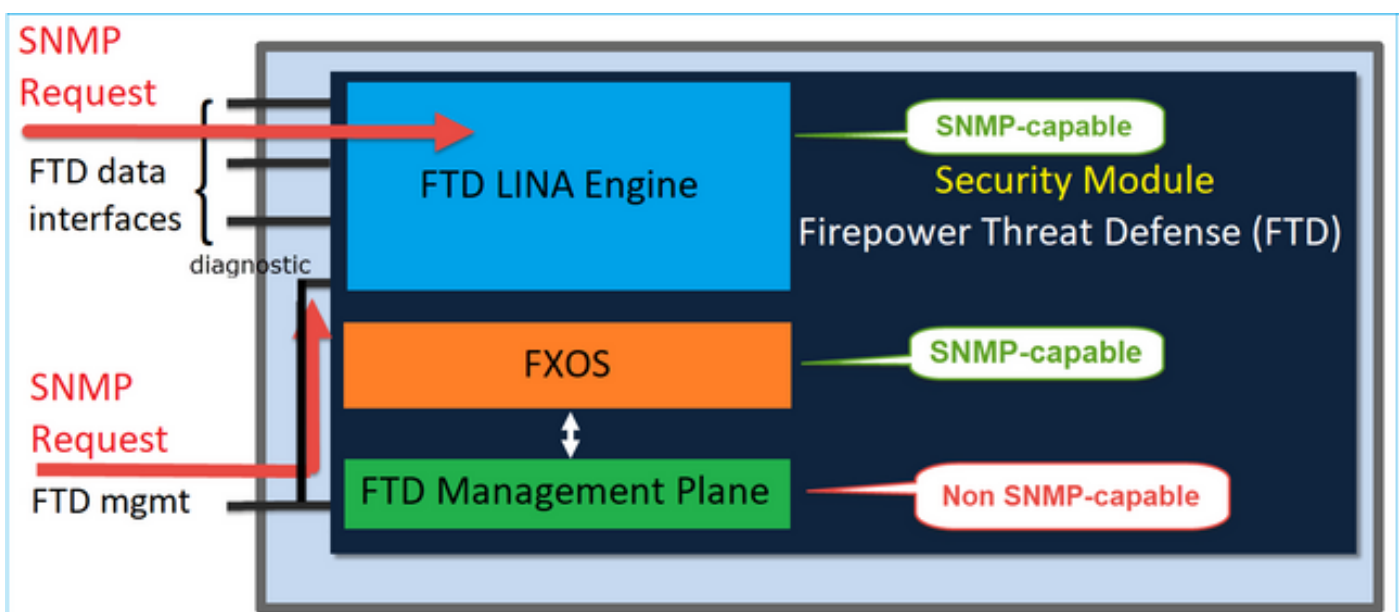
SNMP Version:

Type:

Privilege:

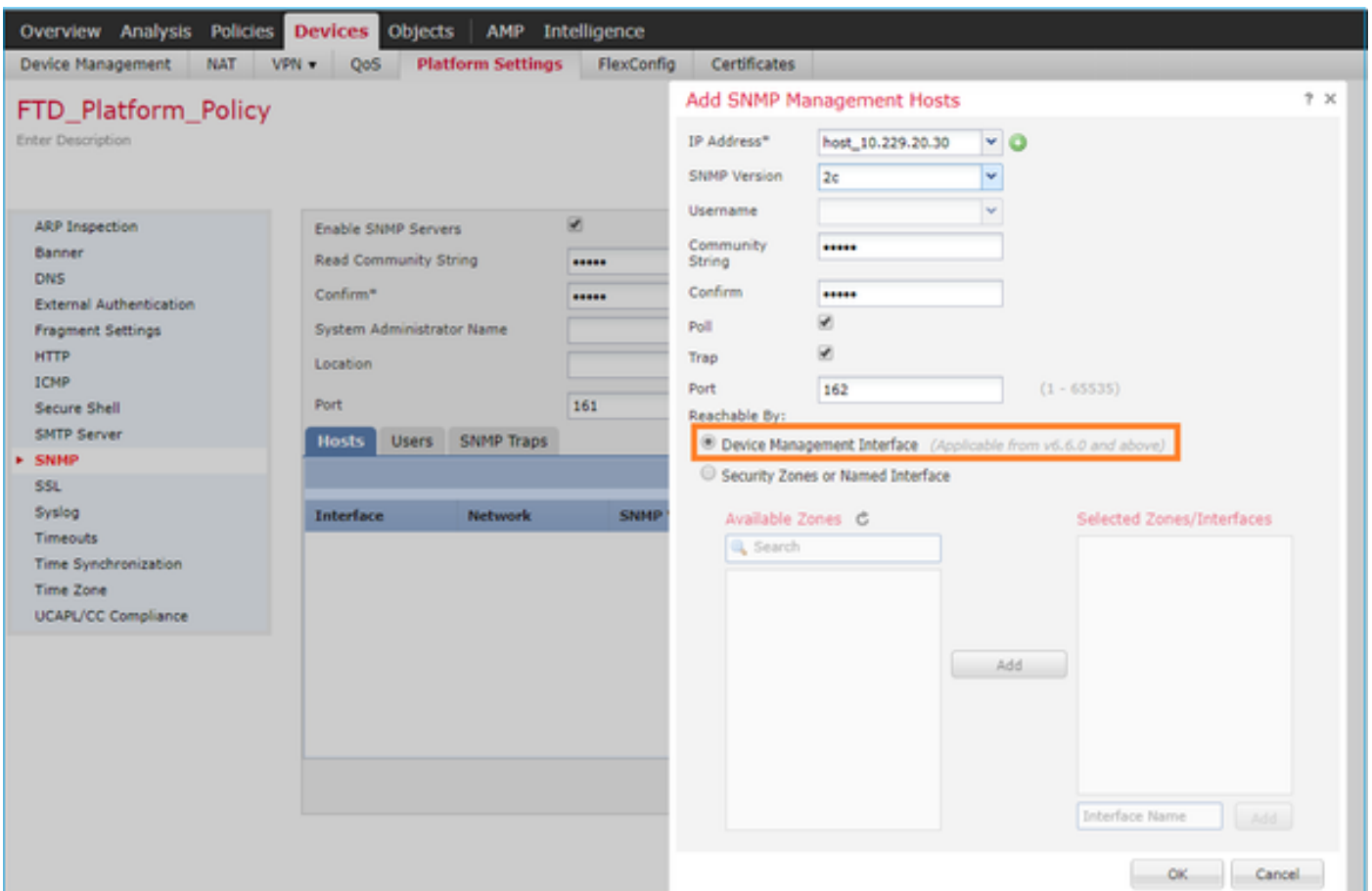
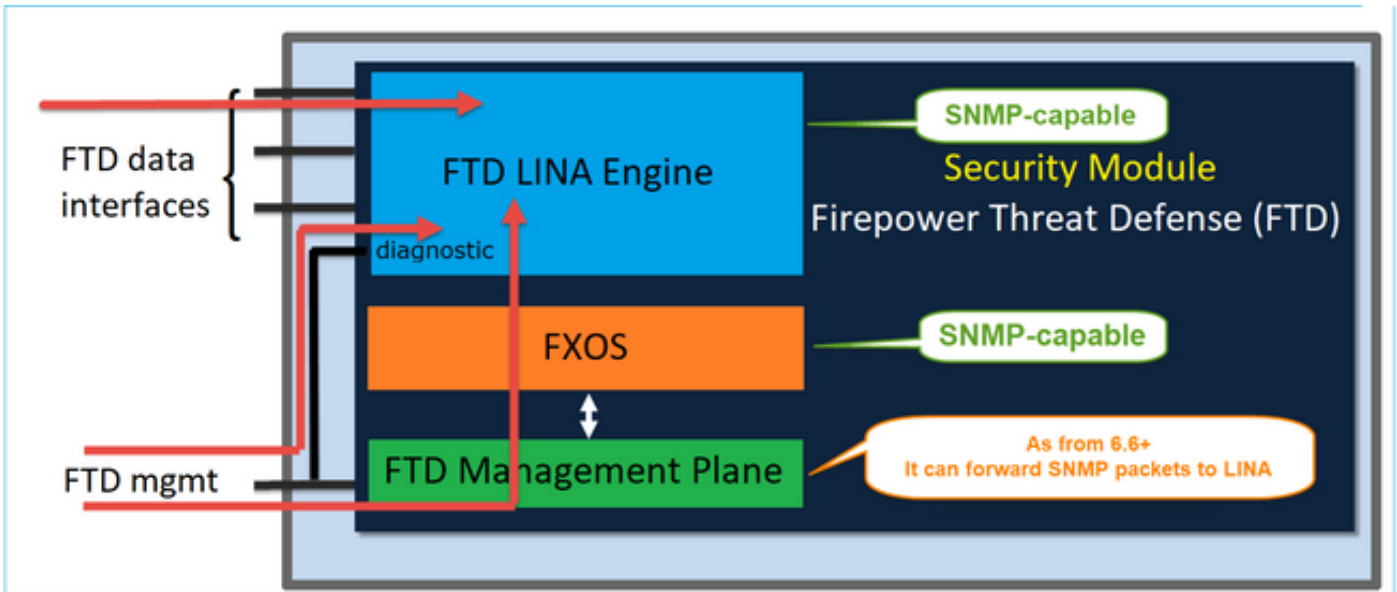
FTD (LINA) SNMP sur FPR2100

- Pour les versions antérieures à 6.6, la configuration de LINA FTD SNMP sur les appareils FTD FP1xxx/FP21xx est identique à celle d'un appareil FTD avec Firepower 4100 ou 9300.



Versions 6.6 et ultérieures de FTD

- Dans les versions ultérieures à 6.6, vous avez également la possibilité d'utiliser l'interface de gestion de FTD pour les interrogations et les dérouterments de LINA.

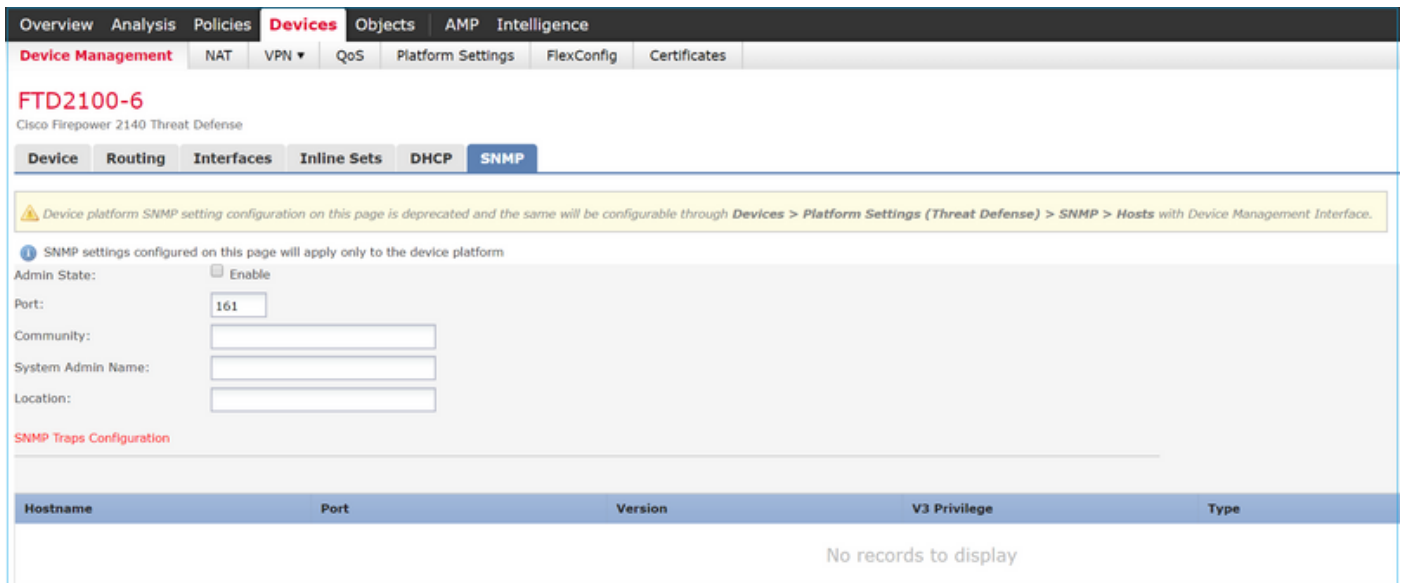


Si la nouvelle interface de gestion est sélectionnée :

- LINA SNMP est disponible sur l'interface de gestion.
- Sous **Devices > Device Management** (appareils > gestion des appareils), l'onglet **SNMP** est désactivé, car il n'est plus nécessaire. Une bannière de notification s'affiche. L'onglet de

l'appareil SNMP n'était visible que sur les plateformes 2100/1100. Cette page n'existe pas sur les plateformes FPR9300/FPR4100 et FTD55xx.

Une fois configurées, les informations combinées d'interrogation/de déROUTement de LINA SNMP + FXOS (sur FP1xxx/FP2xxx) passent par l'interface de gestion de FTD.



La fonction de gestion SNMP pour une seule adresse IP est prise en charge à partir de la version 6.6 sur toutes les plateformes FTD :

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 exécutant FTD
- FTDv

Pour en savoir plus, consultez Configure SNMP for Threat Defense (configurer SNMP pour Threat Defense)

Vérifier

Vérifier FXOS SNMP pour FPR4100/FPR9300

Vérifications de FXOS SNMPv2c

Vérification de la configuration de l'interface 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
```

À partir du mode 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
```

Vérifications supplémentaires :

<#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
...

```

Tester les requêtes SNMP.

Exécutez une requête SNMP à partir d'un hôte valide .

Confirmer la génération de déROUTement.

Vous pouvez faire osciller une interface fonctionnant avec EthAnalyzer pour confirmer que les déROUTements de SNMP sont générés et qu'ils sont envoyés aux hôtes de déROUTement définis :

```
<#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
```



Avertissement : un rabat d'interface peut provoquer une panne de trafic. Effectuez ce test uniquement dans un environnement contrôlé ou dans une fenêtre de maintenance.

Vérifications de FXOS SNMPv3

Étape 1. Ouvrir l'interface utilisateur du FCM en suivant le chemin Platform Settings > SNMP > User (paramètres de la plateforme > SNMP > utilisateur) pour voir si un mot de passe et un mot de passe de protection sont configurés :

Edit user1

?
X

Name:*

Auth Type: SHA

Use AES-128:

Password: Set:Yes

Confirm Password:

Privacy Password: Set:Yes

Confirm Privacy Password:

OK
Cancel

Étape 2. Dans l'interface CLI, vous pouvez vérifier la configuration SNMP prise en compte sous monitoring (surveillance) :

```
<#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
```

Étape 3. En mode FXOS, vous pouvez développer la configuration et les détails de SNMP :

```
<#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
-----
```


Vous pouvez vérifier que vous êtes en mesure d'interroger FXOS et d'envoyer une requête SNMP à partir d'un hôte ou de tout appareil doté de fonctionnalités SNMP .

Utilisez la commande capture-trafic pour afficher la requête SNMP et la réponse :

```
<#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
```

Vérifications de FXOS SNMPv3

Vérifiez la configuration sur l'interface 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
```

Confirmer le comportement de SNMP.

Envoyez une requête SNMP pour vérifier que vous êtes en mesure d'interroger FXOS .

De plus, vous pouvez capturer la requête :

```
<#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
```

Vérifier FTD SNMP

Pour vérifier la configuration de FTD LINA SNMP :

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

Dans les versions ultérieures à 6.6 de FTD, vous pouvez configurer et utiliser l'interface de gestion de FTD pour SNMP :

```
<#root>
```

```
firepower#
```

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

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

Vérification supplémentaire :

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

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

À partir de la l'interface CLI du serveur SNMP, exécutez la commande 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
...
```

Vérification des statistiques de trafic SNMP

```
<#root>
```

```
Firepower-module1#
```

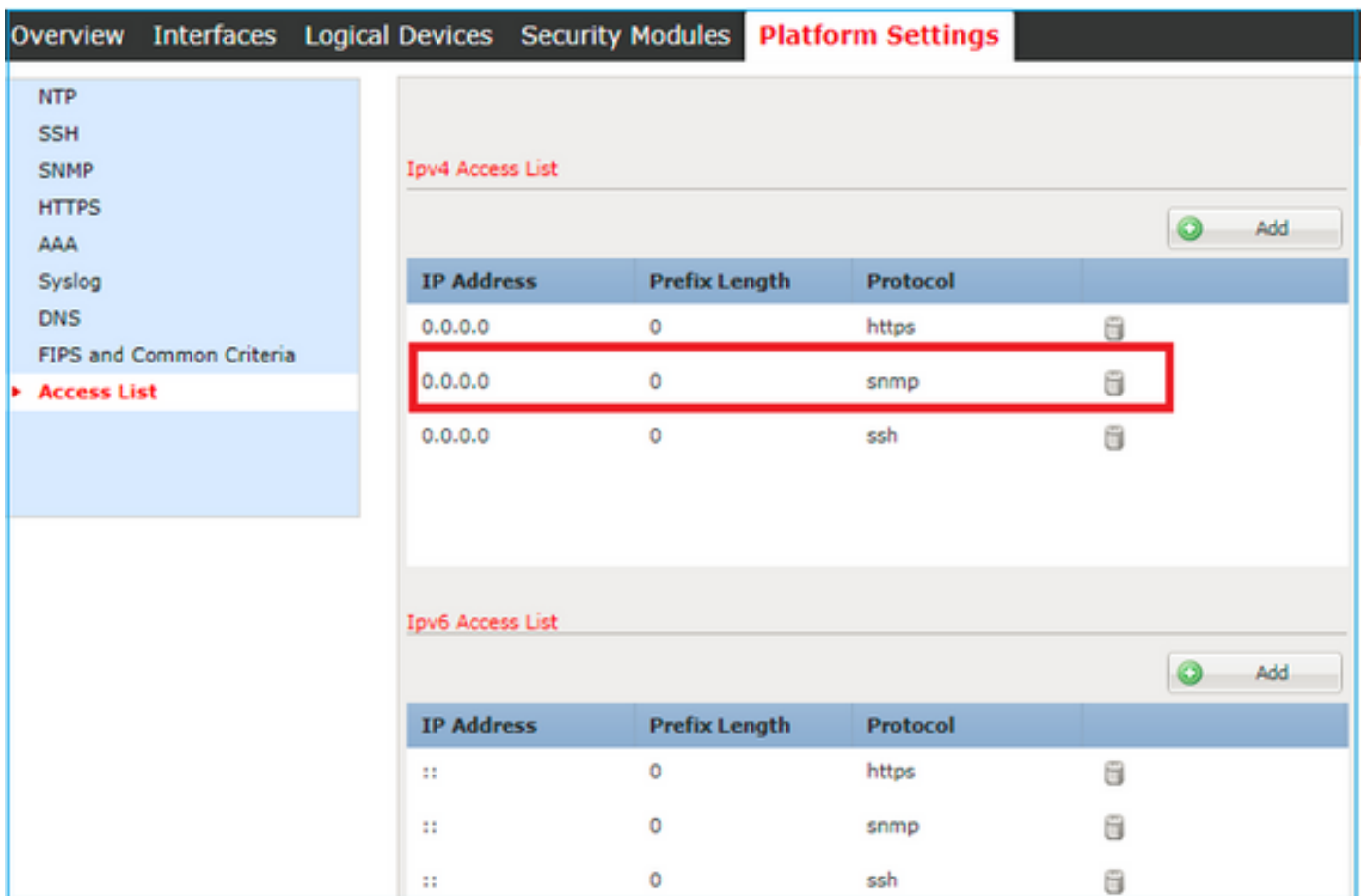
```
show snmp-server statistics
```

```
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
```

Autoriser le trafic SNMP vers FXOS sur FPR4100/FPR9300

La configuration FXOS sur FPR4100/9300 peut restreindre l'accès à SNMP par adresse IP source. La section de configuration de la liste d'accès définit les réseaux/hôtes qui peuvent atteindre l'appareil par SSH, HTTPS ou SNMP. Vous devez vous assurer que les requêtes SNMP de votre serveur SNMP sont autorisées.

Configurer la liste d'accès globale sur l'interface graphique



The screenshot shows the 'Platform Settings' interface with a sidebar on the left containing navigation options: NTP, SSH, SNMP, HTTPS, AAA, Syslog, DNS, FIPS and Common Criteria, and Access List (highlighted). The main content area is divided into two sections: 'Ipv4 Access List' and 'Ipv6 Access List'. Each section has an 'Add' button and a table with columns for IP Address, Prefix Length, Protocol, and a trash icon. In the IPv4 list, the entry for 'snmp' with IP '0.0.0.0' and Prefix Length '0' is highlighted with a red box. The IPv6 list shows entries for 'https', 'snmp', and 'ssh' with IP address '::' and Prefix Length '0'.

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	

Configurer la liste d'accès globale sur l'interface 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
```

Vérification

<#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

Utiliser le navigateur d'objets OID (Object Identifier)

[Cisco SNMP Object Navigator](#) est un outil en ligne qui permet de traduire les différents OID et d'en obtenir une brève description.

The screenshot shows the Cisco SNMP Object Navigator interface. The main heading is "SNMP Object Navigator". There are navigation tabs: HOME, SUPPORT, TOOLS & RESOURCES, and SNMP Object Navigator. The main content area has buttons for TRANSLATE/BROWSE, SEARCH, DOWNLOAD MIBS, and MIB SUPPORT - SW. Below these are links for Translate and Browse The Object Tree. A text input field contains the OID "1.3.6.1.4.1.9.9.109.1.1.1" and a "Translate" button. To the right, it shows "examples - OID: 1.3.6.1.4.1.9.9.27 Object Name: ifIndex". Under "Object Information", a table lists details for the object "cpmCPUTotalTable".

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.

Utilisez la commande `show snmp-server oid` de l'interface CLI de FTD LINA pour récupérer la liste complète des OID de LINA qui peuvent être interrogés.

```
<#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#
```



Remarque : la commande est masquée.

Dépannage

Voici les générateurs de dossiers SNMP les plus couramment vus par Cisco TAC

1. Impossible d'interroger FTD LINA SNMP
2. Impossible d'interroger FXOS SNMP
3. Quelles valeurs SNMP OID utiliser?
4. Impossible d'obtenir les dérouterments SNMP
5. Impossible de surveiller FMC à l'aide du protocole SNMP
6. Échec de la configuration de SNMP
7. Configuration de SNMP sur Firepower Device Manager (FDM)

Impossible d'interroger FTD LINA SNMP

Descriptions des problèmes (exemples de cas réels de Cisco TAC) :

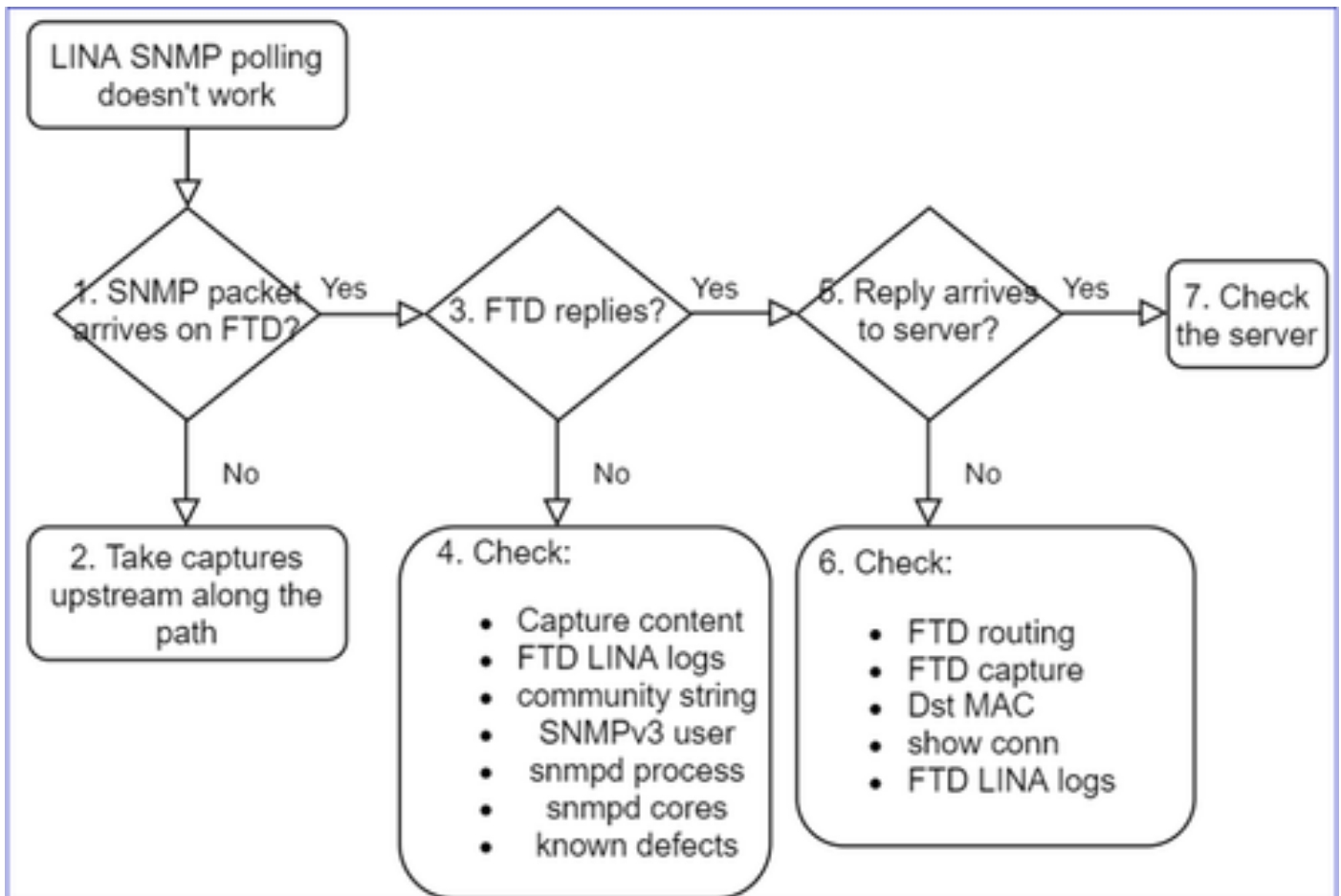
- « Impossible de récupérer les données sur SNMP. »
- « Impossible d'interroger l'appareil sur SNMPv2. »
- « SNMP ne fonctionne pas. Nous tentons surveiller le pare-feu avec SNMP, mais, à la suite

de la configuration, nous rencontrons des problèmes. »

- « Deux systèmes de surveillance ne sont pas en mesure de surveiller FTD à l'aide de SNMP v2c ou 3. »
- « La commande SNMP walk ne fonctionne pas sur le pare-feu. »

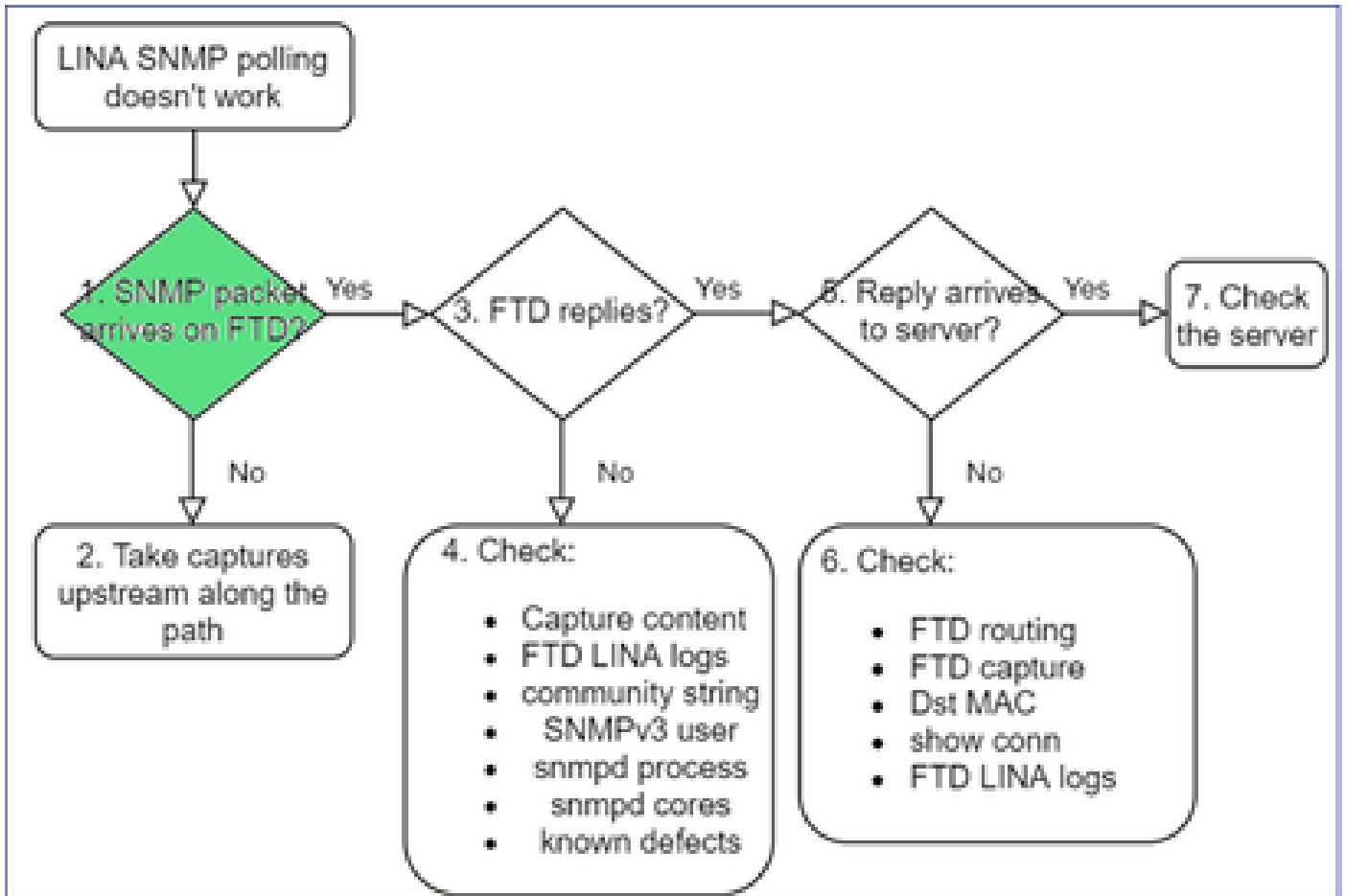
Recommandation sur le dépannage

Cette procédure est recommandée pour dépanner l'organigramme des problèmes d'interrogation LINA SNMP :



Présentation détaillée

1. Le paquet SNMP arrive-t-il sur FTD ?



- Activer les captures pour vérifier l'arrivée des paquets SNMP.

SNMP sur l'interface de gestion FTD (version post-6.6) utilise le mot clé management :

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

Sur les interfaces de données de FTD, SNMP utilise le nom de l'interface :

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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


Capture sur l'interface de gestion de FTD :

```
<#root>
```

```
>
```

```
capture-traffic
```

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

```
0 - management1
```

```
1 - management0
```

```
2 - Global
```

```
Selection?
```

```
1
```

Capture sur l'interface de données de FTD :

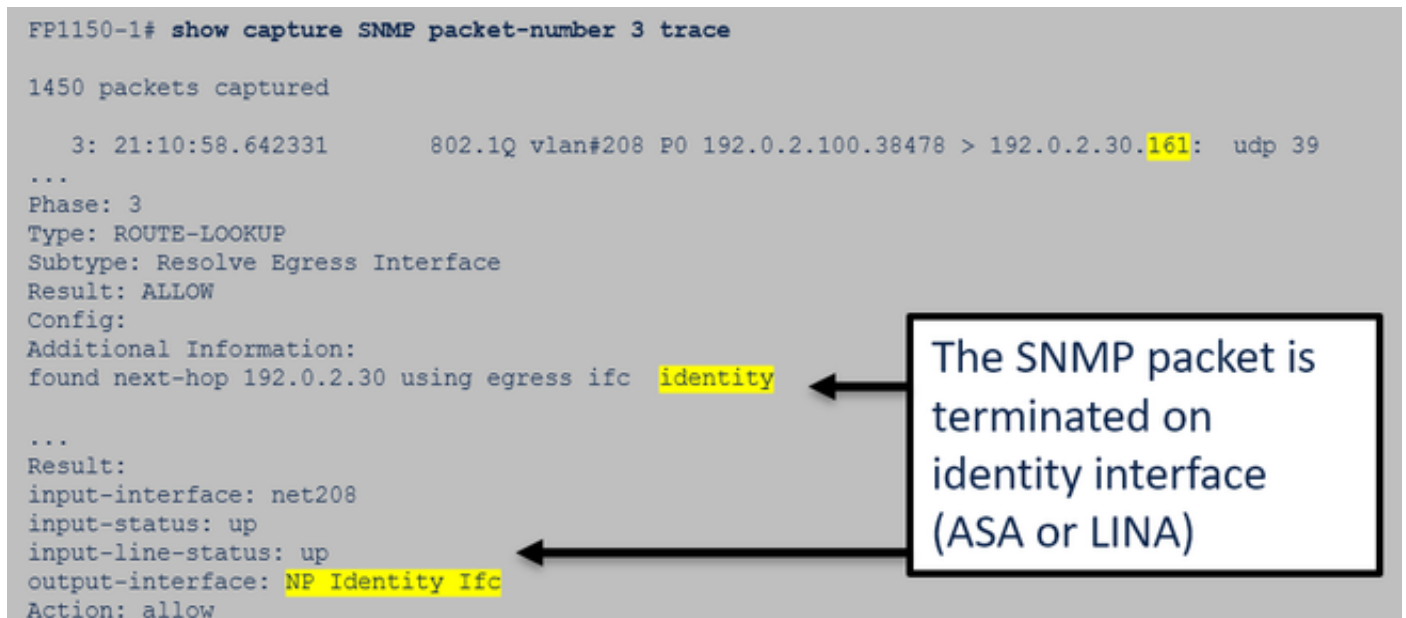
```
<#root>
```

```
firepower#
```

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

Suivi des paquets de l'interface de données FTD (antérieur à 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
```



Suivi des paquets de l'interface de données FTD (post 6.6/9.14.1) :

```

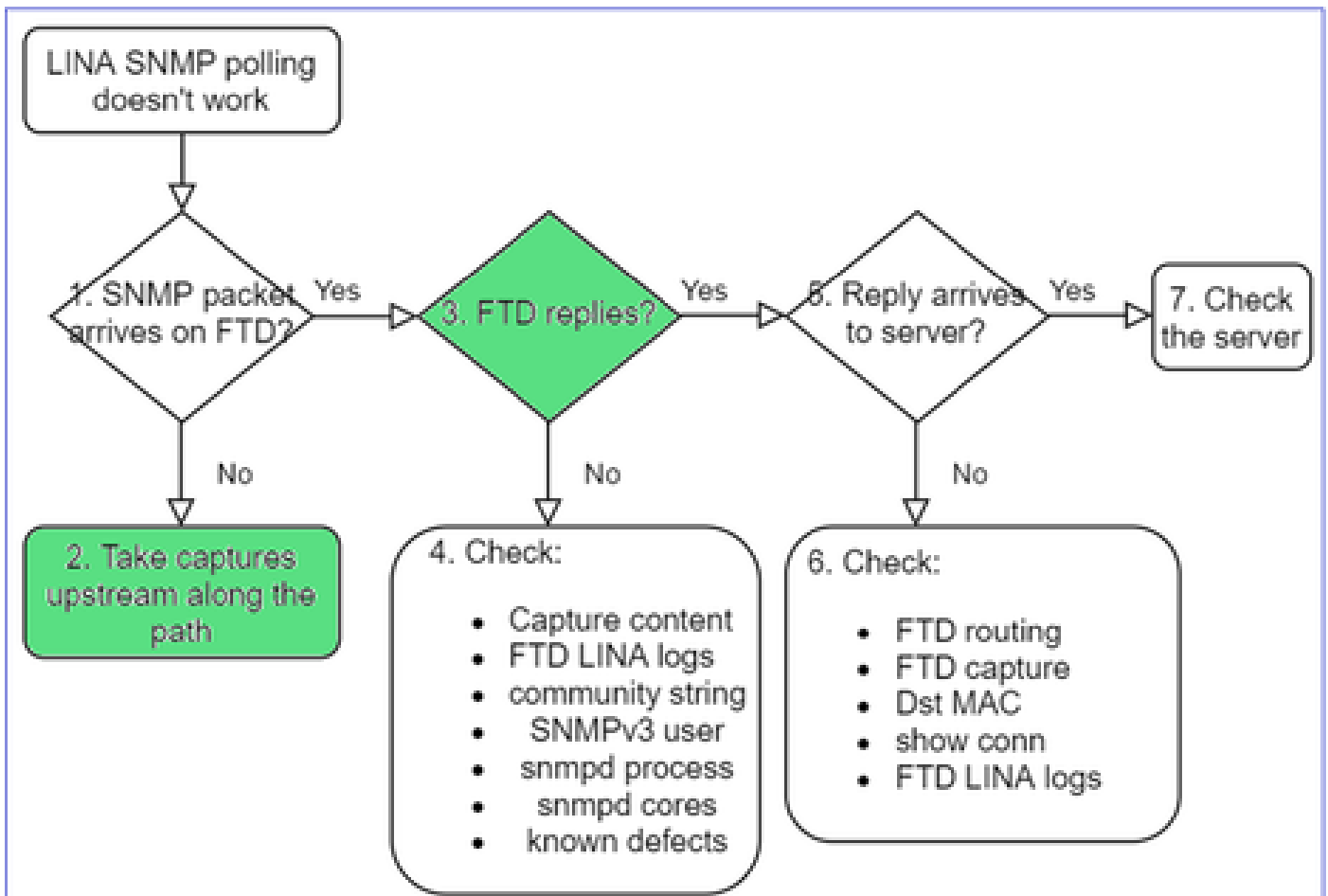
firepower# show capture SNMP packet-number 1 trace
1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.21.100.58255 > 192.168.21.50.161:  udp 39
...
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 9
Config:
nat (nlp_int_tap,net201) source static nlp_server__snmp_192.168.21.100_intf4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

```

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

2. Si vous ne voyez pas de paquets SNMP dans les captures d'entrée FTD :

- Effectuez des captures vers l'amont le long du chemin.
- Assurez-vous que le serveur SNMP utilise l'adresse IP FTD appropriée.
- Commencez par le port de commutation qui fait face à l'interface FTD et remontez.



3. Voyez-vous des réponses FTD SNMP ?

Pour vérifier si FTD répond, vous devez vérifier :

1. La capture de sortie de FTD (interface de LINA ou interface de gestion)

Vérifiez les paquets SNMP à l'aide du port source 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
```

Dans les versions postérieures à la version 6.6/9.14.1, vous disposez d'un point de capture supplémentaire : Capture sur l'interface de prise NLP. L'adresse IP NATed est comprise dans la plage 162.254.x.x :

```
<#root>
```

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

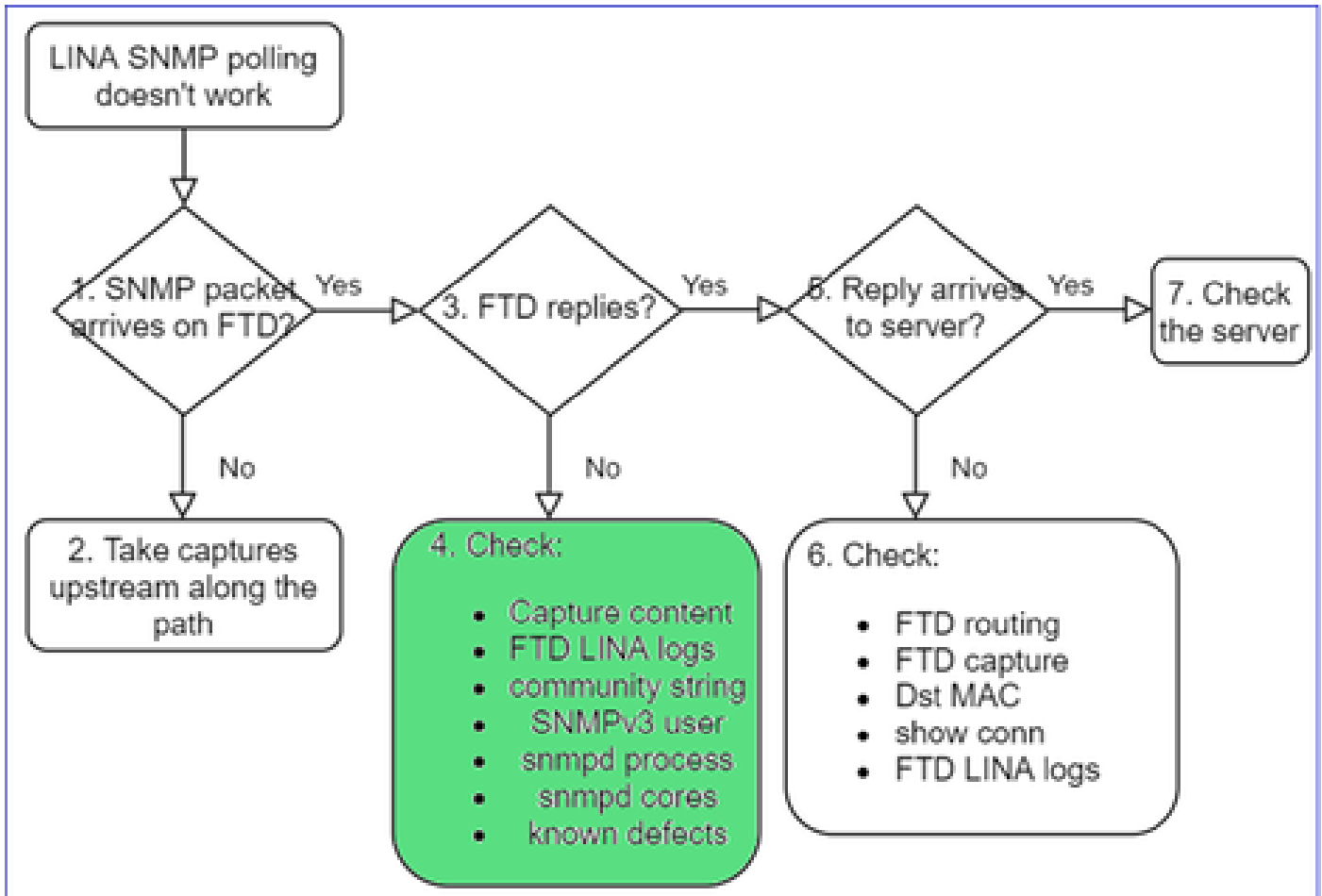
```
sudo tcpdump -i tap_nlp
```

```
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. Contrôles supplémentaires



a. Pour les périphériques Firepower 4100/9300, vérifiez la [table de compatibilité 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)+ Note FXOS 2.13(0.198)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	9.19(x) (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	7.3.0 (recommended) 7.2.0 7.1.0 7.0.0 6.7.0 6.6.x		
	Firepower 4145 Firepower 4125 Firepower 4115	9.19(x) (recommended) 9.18(x) 9.17(x) 9.16(x)	7.3.0 (recommended) 7.2.0 7.1.0 7.0.0		
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)	6.7.0 6.6.x 6.5.0 6.4.0		
	2.12(0.31)+ Note FXOS 2.12(0.31)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	7.2.0 (recommended) 7.1.0 7.0.0 6.7.0 6.6.x	
		Firepower 4145 Firepower 4125 Firepower 4115	9.18(x) (recommended) 9.17(x) 9.16(x)	7.2.0 (recommended) 7.1.0 7.0.0	
		Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)	6.7.0 6.6.x 6.5.0 6.4.0	
		Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x) 9.13(x)	7.2.0 (recommended) 7.1.0 7.0.0 6.7.0 6.6.x 6.5.0	
		Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.12(x) 9.10(x) 9.9(x) 9.8(x)	6.4.0 6.3.0	
		2.11(1.154)+ Note FXOS 2.11(1.154)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use	Firepower 4112	9.17(x) (recommended) 9.16(x) 9.15(1) 9.14(x)	7.1.0 (recommended) 7.0.0 6.7.0 6.6.x

b. Vérifiez les statistiques FTD LINA snmp-server :

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

firepower#
show snmp-server statistics

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

c. Table de connexion FTD LINA

Cette vérification est très utile dans le cas où vous ne voyez pas de paquets dans la capture sur l'interface d'entrée FTD. Notez qu'il s'agit d'une vérification valide uniquement pour SNMP sur l'interface de données. Si SNMP est sur l'interface de gestion (post-6.6/9.14.1), aucune connexion n'est créée.

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

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

d. Syslogs LINA FTD

Il s'agit également d'une vérification valide uniquement pour SNMP sur l'interface de données. Si SNMP est sur l'interface de gestion, aucun journal n'est créé :

```
<#root>
```

```
firepower#
```

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

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

e. Vérifiez si le FTD abandonne les paquets SNMP en raison d'une adresse IP source d'hôte incorrecte

```
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=169.254.1.2, mask=255.255.255.255, port=161, tag=any, dscp=0x0, nsg_id=none
input_ifc=net201(vrfid:0), output_ifc=any
```

f. Identifiants incorrects (communauté SNMP)

Dans le contenu de la capture, vous pouvez voir les valeurs de la communauté (SNMP v1 et 2c) :

```
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. Configuration incorrecte (par exemple, version SNMP ou chaîne de communauté)

Il existe plusieurs façons de vérifier la configuration SNMP et les identifiants de communauté de l'appareil :

```
<#root>
```

```
firepower#
```

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

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

Autre méthode :

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

h. Abandons FTD LINA/ASA ASP

Il s'agit d'une vérification utile pour vérifier si les paquets SNMP sont abandonnés par FTD. Tout d'abord, effacez les compteurs (commande « clear asp drop »), puis effectuez un test :

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

firepower#
show asp drop
```

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

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

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

i. Captures ASP

Les captures ASP permettent de voir les paquets abandonnés (p. ex., ACL ou contiguïté) :

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

Effectuez un test puis vérifiez le contenu de la capture :

```
<#root>
firepower#
show capture

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

j. Noyau SNMP (retraçage) - méthode de vérification 1

Cette méthode de vérification est utile si vous soupçonnez des problèmes de stabilité du système :

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

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

Fichier principal SNMP (recherche de la source) – Méthode de vérification 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
```

Si vous voyez un fichier principal SNMP, collectez ces éléments et communiquez avec Cisco TAC :

- Fichier FTD TS (ou fichier d'affichage technique ASA)
- Fichiers principaux de SNMP

Débogage de SNMP (ces commandes masquées sont disponibles uniquement sur les versions les plus récentes) :

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



```

debug snmp trace [255]

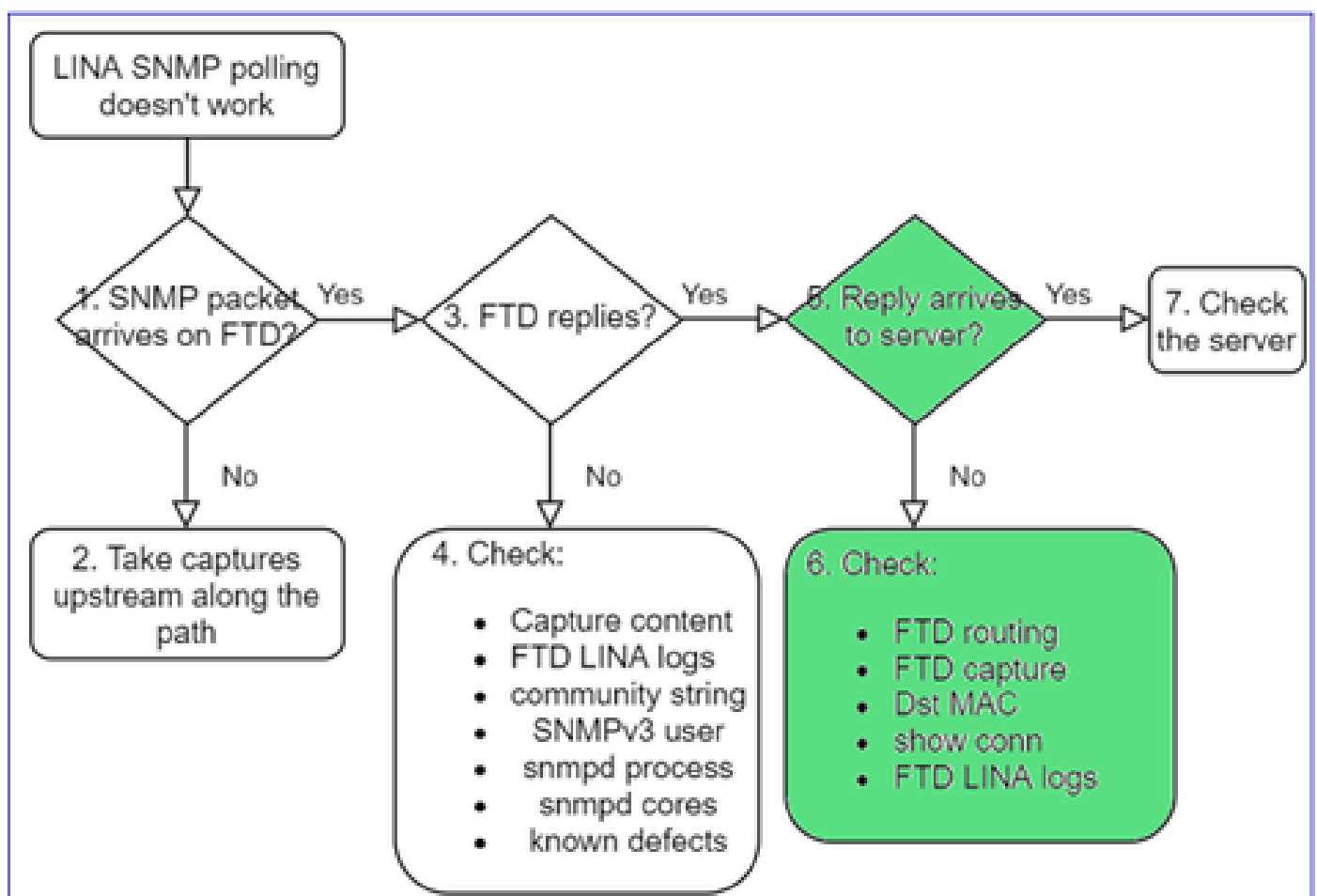
firepower#
debug snmp verbose [255]

firepower#
debug snmp error [255]

firepower#
debug snmp packet [255]

```

La réponse SNMP du pare-feu atteint-elle le serveur?



Si FTD répond, mais que la réponse n'atteint pas le serveur, vérifiez :

a. Routage FTD

Pour le routage de l'interface de gestion de FTD :

```
<#root>
```

```
>
```

```
show network
```

Pour le routage de l'interface de données de FTD LINA :

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

b. Vérification MAC de destination

Vérification MAC de destination de l'interface de gestion de 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
```

Vérification MAC de destination de l'interface de données de FTD LINA :

```
<#root>
```

```
firepower#
```

```
show capture SNMP detail
```

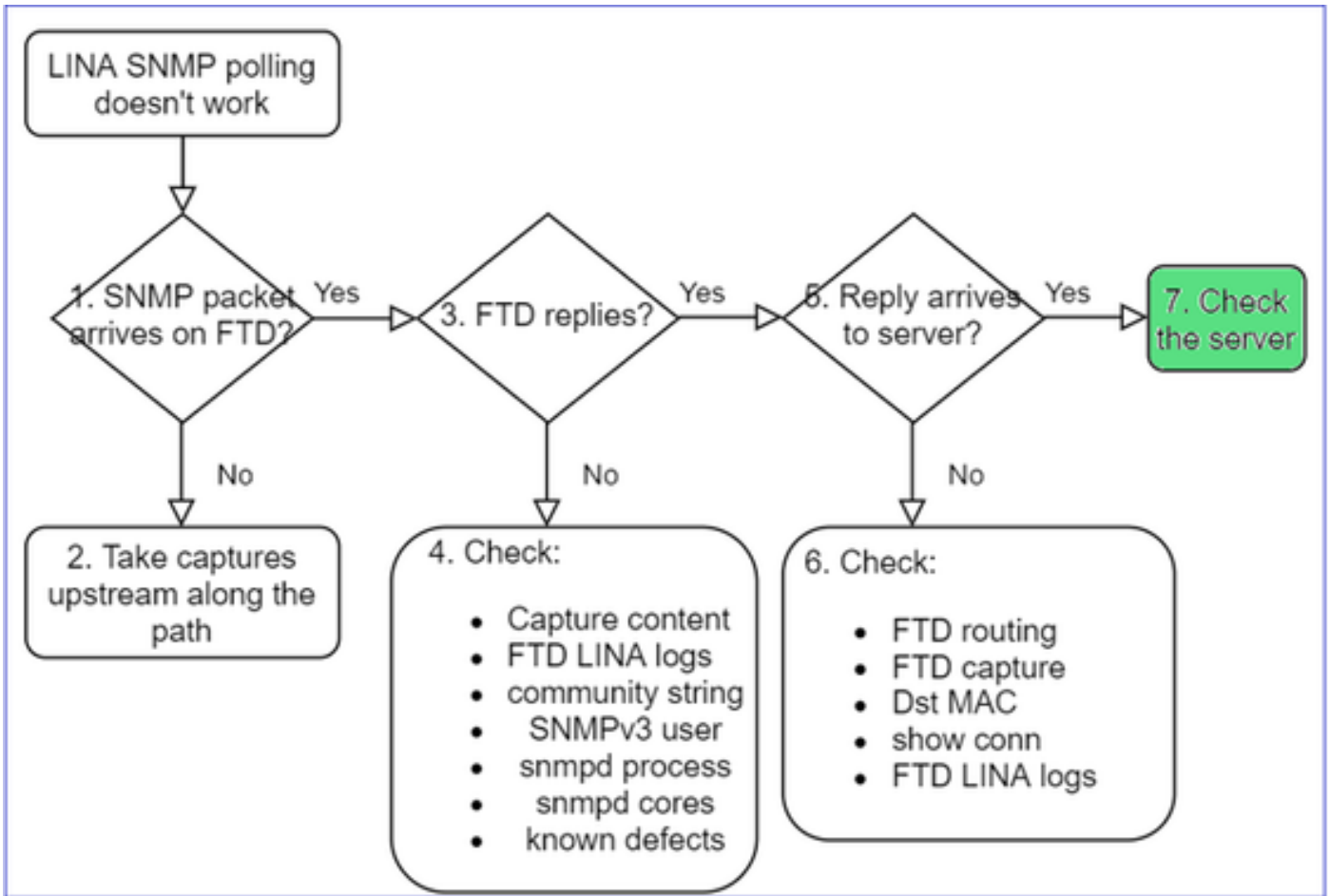
```
...
```

```
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,
```

c. Vérifiez les périphériques situés le long du chemin qui risquent d'abandonner/de bloquer les paquets SNMP.

Vérifier le serveur SNMP



a. Vérifiez le contenu de la capture pour vérifier les paramètres.

b. Vérifiez la configuration du serveur.

c. Essayez de modifier le nom de la communauté SNMP (par exemple, sans caractères spéciaux).

Vous pouvez utiliser un hôte d'extrémité ou même le FMC pour tester l'interrogation tant que les deux conditions suivantes sont remplies :

1. La connectivité SNMP est en place.
2. L'adresse IP source est autorisée à interroger le périphérique.

```
<#root>
```

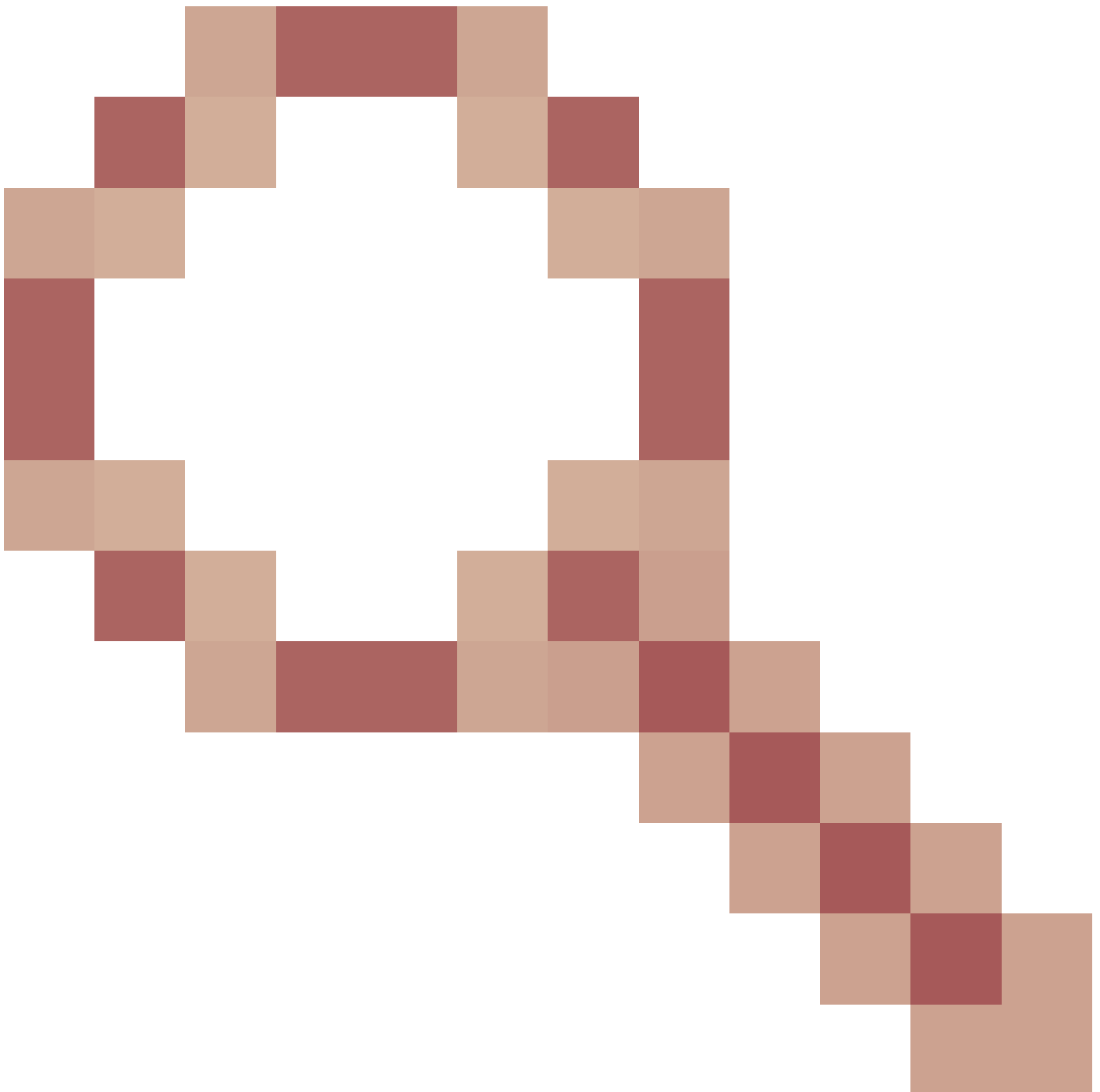
```
admin@FS2600-2:~$
```

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

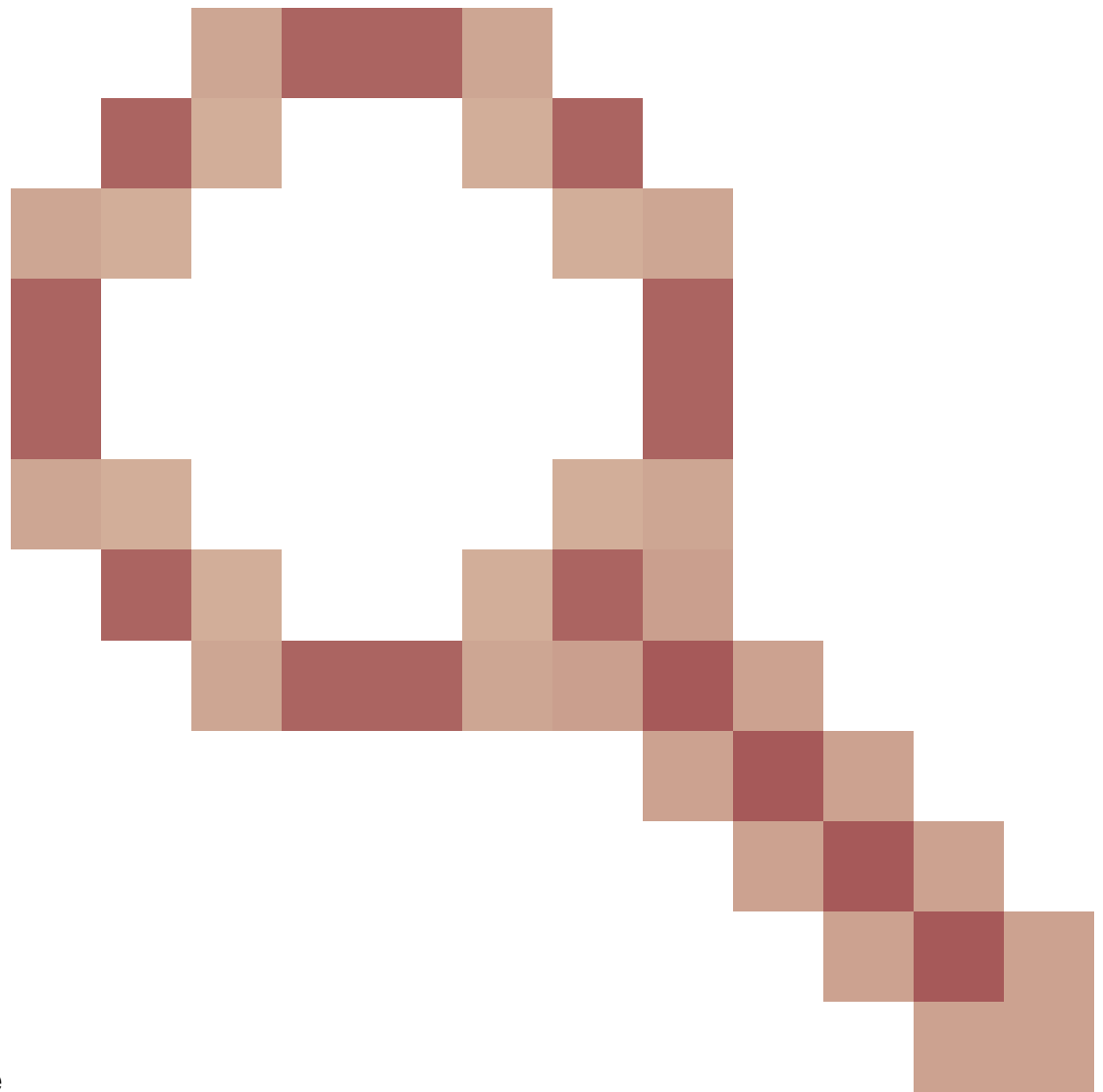
```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.0.0 (Build 3), ASA Version 9.
```

Considérations relatives aux interrogations SNMPv3

- Licence : SNMPv3 nécessite une licence de cryptage fort. Assurez-vous que la fonction Export Controlled Fonctionnalité est activée sur le portail de licences Smart.
- Pour résoudre le problème, vous pouvez essayer avec un nouvel utilisateur/de nouvelles informations d'identification
- Si le cryptage est utilisé, vous pouvez décrypter le trafic SNMPv3 et vérifier la charge utile comme décrit dans : <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>
- Pensez à utiliser AES128 pour le chiffrement au cas où votre logiciel connaît des défaillances comme :
- ID de bogue Cisco [CSCvy27283](#)




L'interrogation SNMPv3 ASA/FTD peut échouer en utilisant les algorithmes de confidentialité



Échec de la marche

Snmpv3 sur l'utilisateur avec auth sha et priv aes 192 avec l'ID de bogue Cisco [CSCvx45604](https://tools.cisco.com/bugtools/bugs/show_bug.do?bugID=CSCvx45604)

 Remarque : si SNMPv3 échoue en raison d'une non-concordance d'algorithme, les résultats de la commande show et les journaux n'affichent rien d'évident

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

Input packets increase, but no replies!

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

Considérations relatives à l'interrogation SNMPv3 – Études de cas

1. Commande snmpwalk SNMPv3 – Scénario fonctionnel

<#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

Dans la capture (commande snmpwalk), vous voyez une réponse pour chaque paquet :

```
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
```

Le fichier de capture ne montre rien d'anormal :

```

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

```

2. Commande snmpwalk SNMPv3 – Échec du chiffrement

Indice #1 : il y a un dépassement de délai :

```
<#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
```

Indice #2 : Il y a beaucoup de demandes et 1 réponse :

```
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

```

Indice #3 : échec du déchiffrement Wireshark :

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

Conseil n° 4. Vérifiez le fichier ma_ctx2000.log pour les messages « error parsing ScopedPDU (erreur dans l'analyse 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
```

L'erreur d'analyse de ScopedPDU est un indice fort d'une erreur de chiffrement. Le fichier ma_ctx2000.log affiche uniquement les événements pour SNMPv3 !

3. Commande snmpwalk SNMPv3 – Échec de l'authentification

Indice #1 : échec de l'authentification

```
<#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)
```


Indice #2 : Il y a beaucoup de demandes et beaucoup de réponses

```
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
```

Indice #3 : paquet mal formé Wireshark

```
> 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]
```

Conseil n° 4. Vérifiez le fichier ma_ctx2000.log pour repérer des messages « Authentication failed » (échec de l'authentification) :

```
<#root>
```

```
>
```

```
expert
```

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

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

```
Authentication failed for Cisco123
```

```
Authentication failed for Cisco123
```

Impossible d'interroger FXOS SNMP

Descriptions des problèmes (exemples de cas réels de Cisco TAC) :

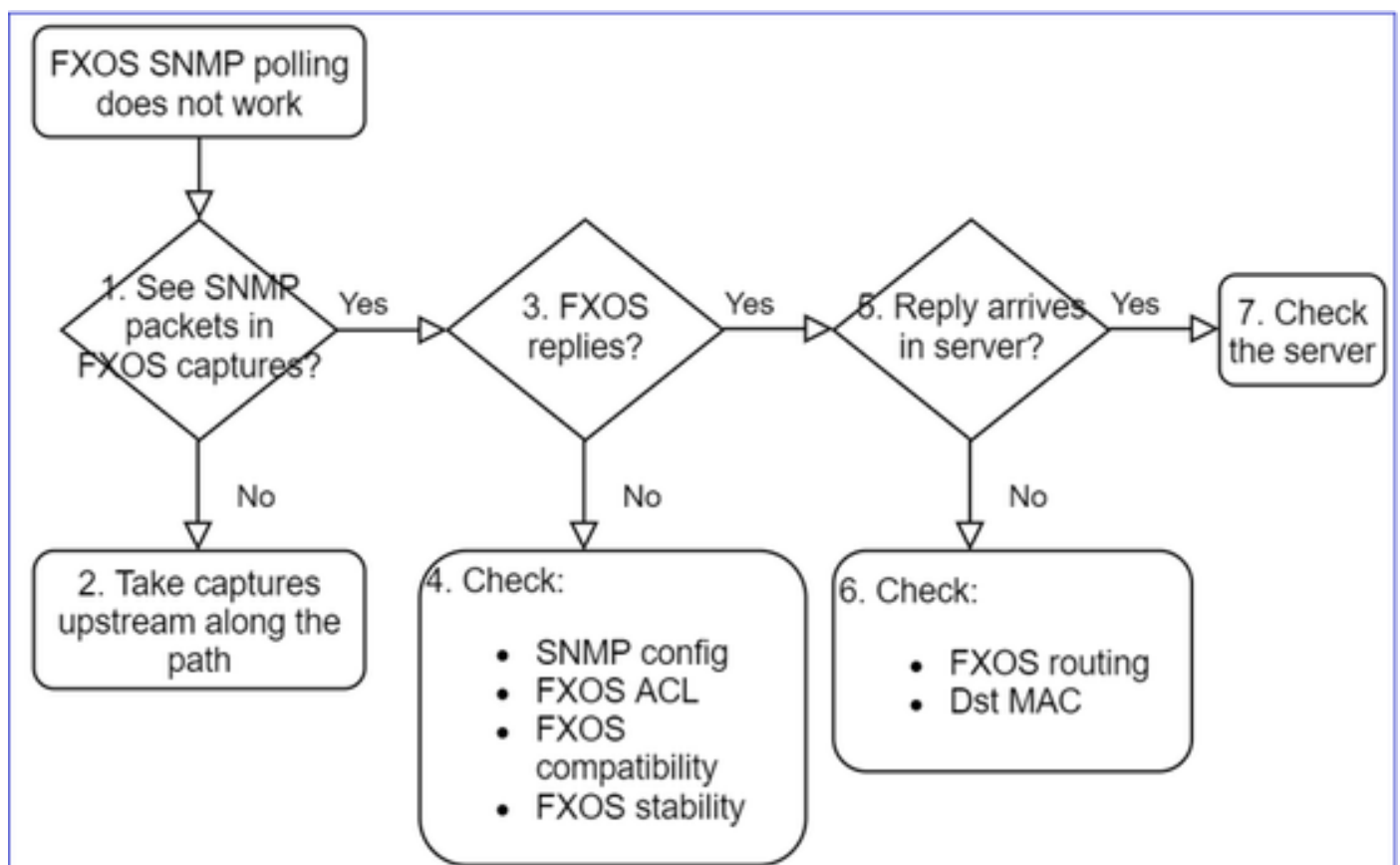
- « SNMP affiche une mauvaise version pour FXOS. Les résultats de l'interrogation avec SNMP pour la version de FXOS sont difficiles à comprendre. »
- « Impossible de configurer la communauté SNMP sur FXOS FTD4115. »
- « Après une mise à niveau de FXOS de la version 2.8 à 2.9 sur le pare-feu de secours, nous obtenons un délai d'expiration lorsque nous essayons de recevoir des informations par

SNMP. »

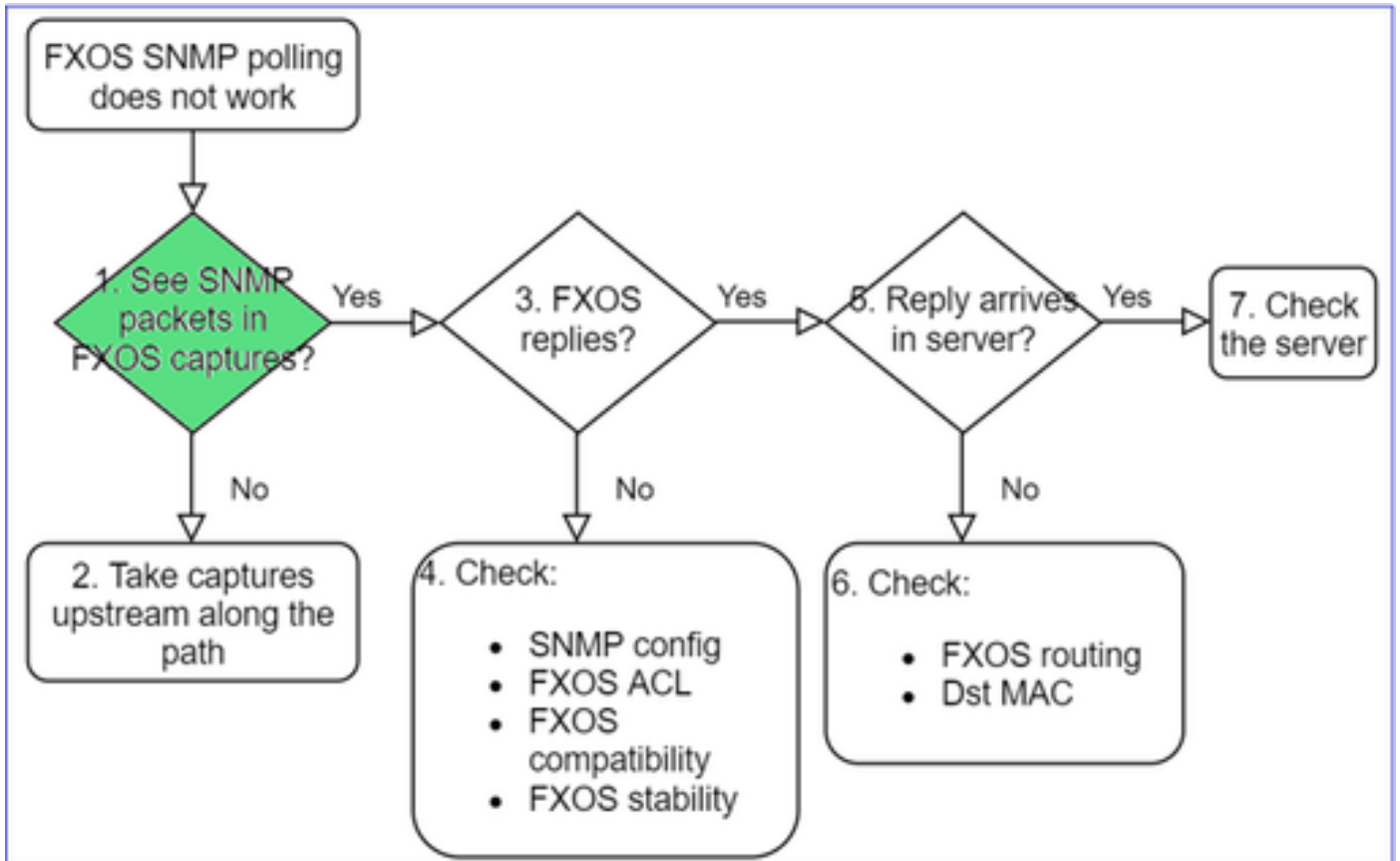
- « La commande snmpwalk échoue sur FXOS 9300 mais fonctionne sur FXOS 4140 sur la même version. L'accessibilité et la communauté ne sont pas le problème. »
- « Nous voulons ajouter 25 serveurs SNMP sur FXOS FPR4K, mais cela est impossible. »

Dépannage recommandé

Voici le processus de dépannage de l'organigramme pour les problèmes d'interrogation FXOS SNMP :



1. Voyez-vous des paquets SNMP dans les captures FXOS ?



FPR1xxx/21xx

- Sur FPR1xxx/21xx, il n'y a pas de gestionnaire de châssis (mode appliance).
- Vous pouvez interroger le logiciel FXOS à partir de l'interface de gestion.

<#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

- Sur Firepower 41xx/93xx, utilisez l'outil d'interface CLI EthAnalyzer pour effectuer une capture du châssis :

```
<#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
```

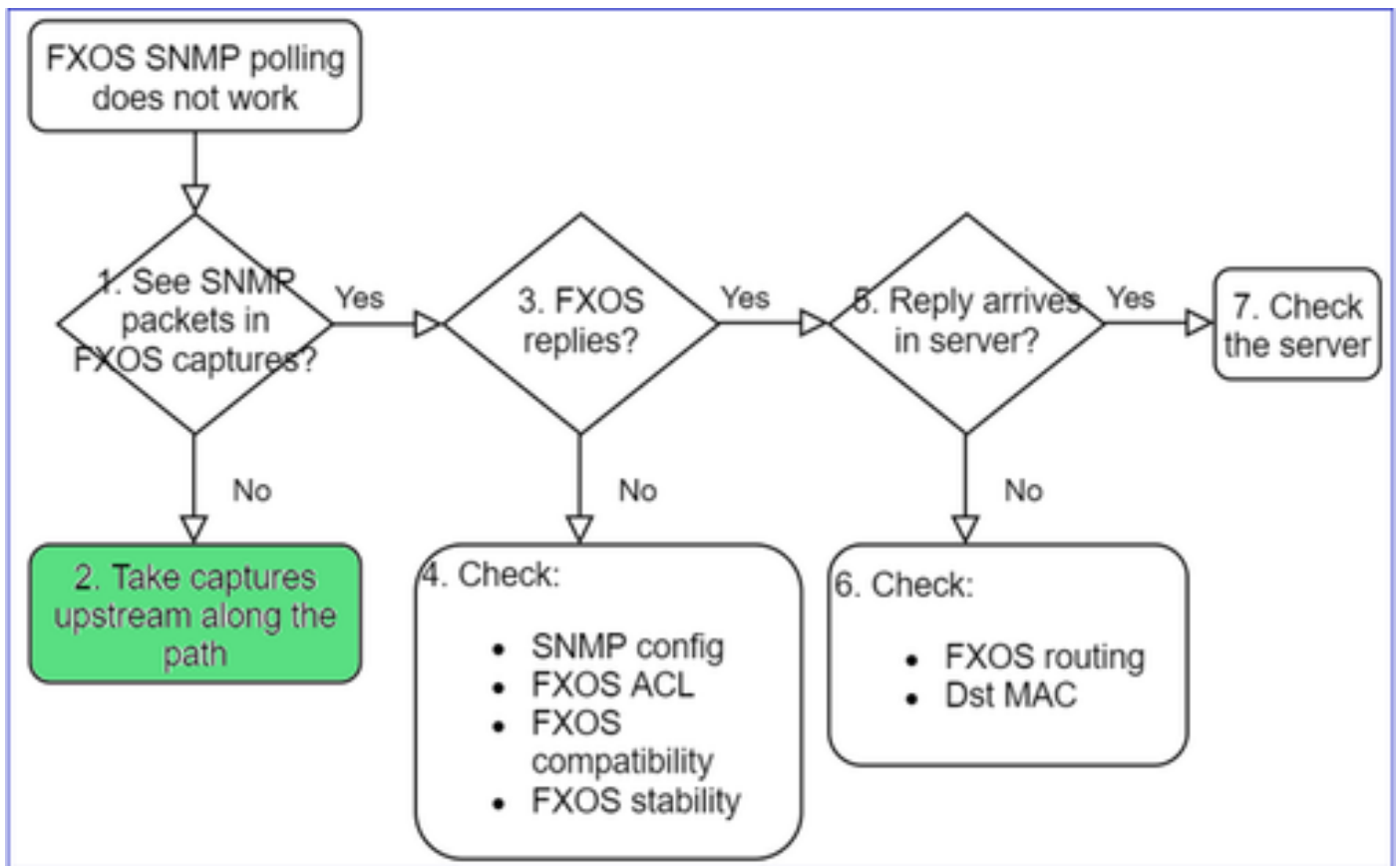
```
1
```

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

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

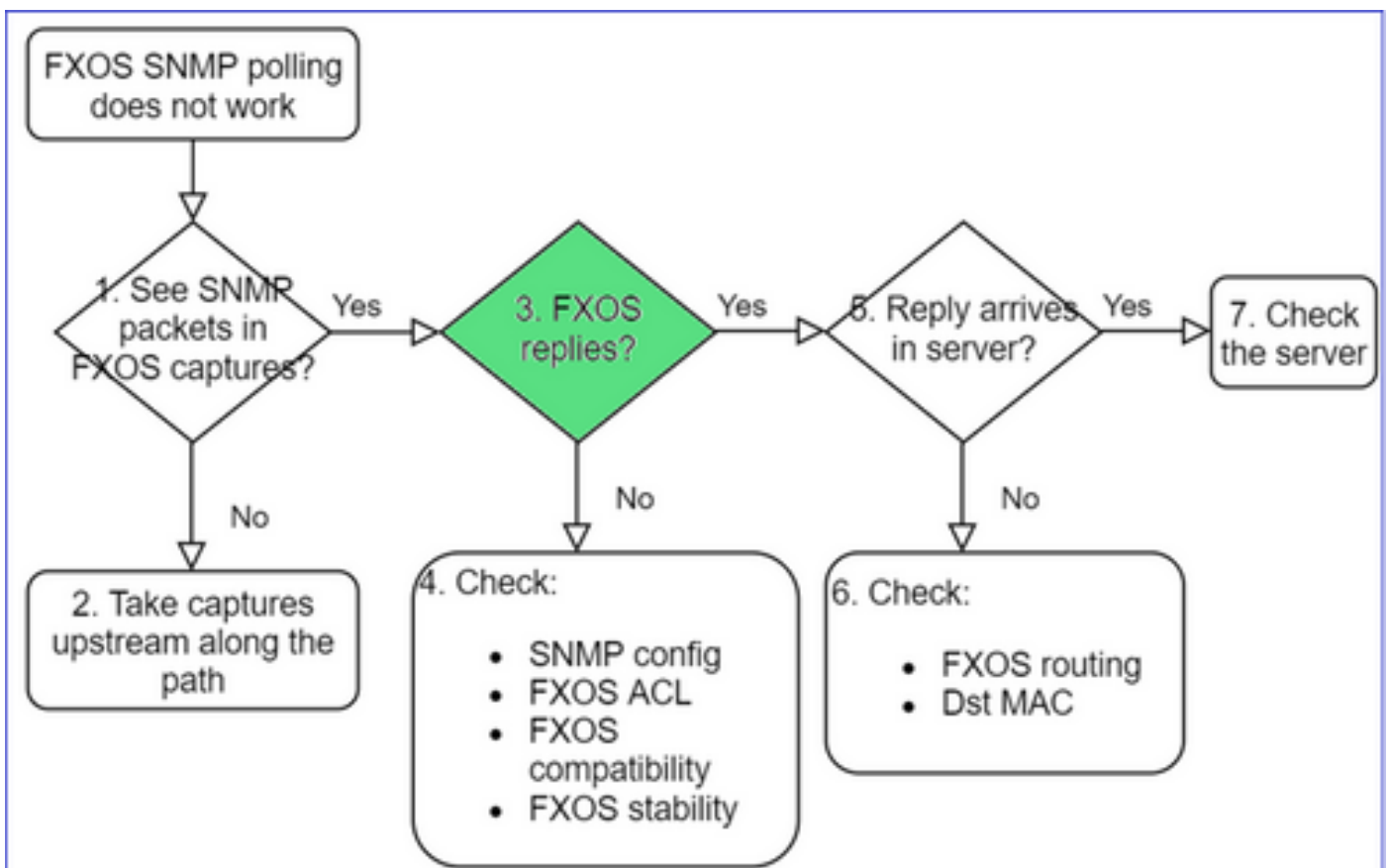
```
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. Aucun paquet dans les captures FXOS ?



- Effectuez des captures en amont le long du chemin.

3. Réponses FXOS ?



- Scénario fonctionnel :

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.

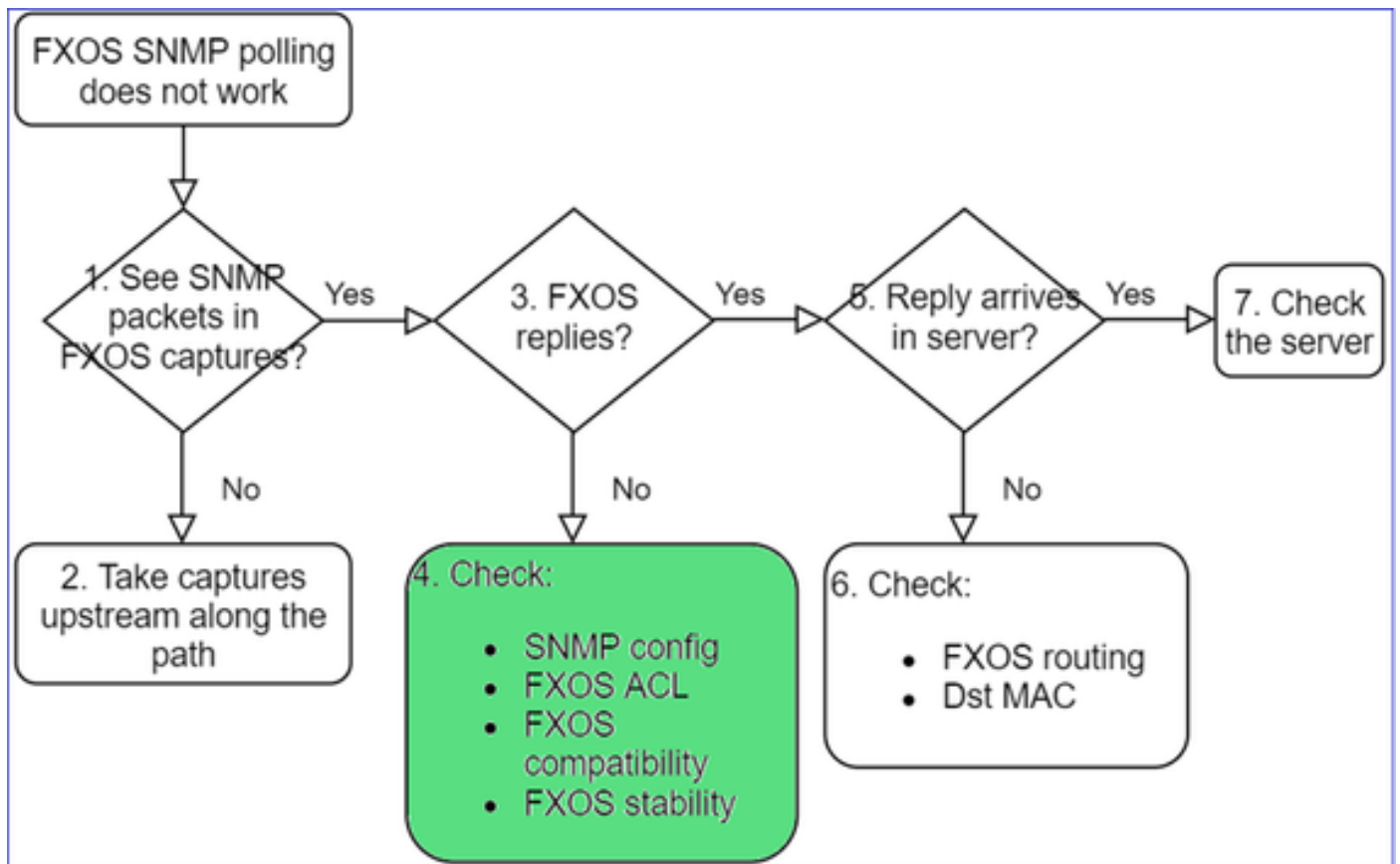
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

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 ne répond pas.



Vérifications supplémentaires

- Vérifiez la configuration SNMP (à partir de l'interface utilisateur ou de l'interface CLI) :

<#root>

```
firepower#
scope monitoring

firepower /monitoring #
show snmp

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

- Soyez prudent avec les caractères spéciaux (p. ex., « \$ ») :

```
<#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
```

- Pour SNMPv3, utilisez la commande `show snmp-user [detail]`.
- Vérifier la compatibilité de FXOS

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

4. Dans le cas où FXOS ne répond pas

Vérifiez les compteurs de 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

```

- Vérifiez la liste de contrôle d'accès FXOS (ACL). Cela s'applique uniquement aux plateformes FPR41xx/9300.

Si le trafic est bloqué par la liste de contrôle d'accès FXOS, vous voyez des requêtes, mais vous ne voyez aucune réponse :

```
<#root>
```

```
firepower (fxos)#
```

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

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

```
Capturing on 'eth0'
```

```

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

```

Vous pouvez vérifier la liste de contrôle d'accès de FXOS à partir de l'interface utilisateur :

The screenshot shows the 'Platform Settings' tab in the management interface. Under 'IPv4 Access List', there is a table with columns 'IP Address', 'Prefix Length', and 'Protocol'. Two entries are visible, both with IP Address '0.0.0.0' and Prefix Length '0'. The first entry has Protocol 'https' and the second has Protocol 'ssh'. An 'Add IPv4 Block' dialog box is overlaid on the table, with the following fields: IP Address: * (0.0.0.0), Prefix Length: * (0), and Protocol: (radio buttons for https, snmp, ssh, with snmp selected). The dialog has 'OK' and 'Cancel' buttons.

Vous pouvez également vérifier la liste de contrôle d'accès de FXOS à partir de l'interface CLI :

```
<#root>
firepower#
scope system

firepower /system #
scope services

firepower /system/services #
show ip-block detail
```

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

- Commande « debug SNMP » (paquets uniquement) – cela fonctionne uniquement sur FPR41xx/9300 :

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

FP4145-1(fxos)#
terminal monitor

FP4145-1(fxos)#
debug snmp pkt-dump

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

- Debug SNMP (all) - Cette sortie de débogage est très détaillée.

```
<#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
```

- Vérifiez s'il y a des erreurs FXOS liées à 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
```

- Vérifiez s'il y a des fichiers principaux SNMPD :

Sur 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
```

Sur FPR1xxx/21xx :

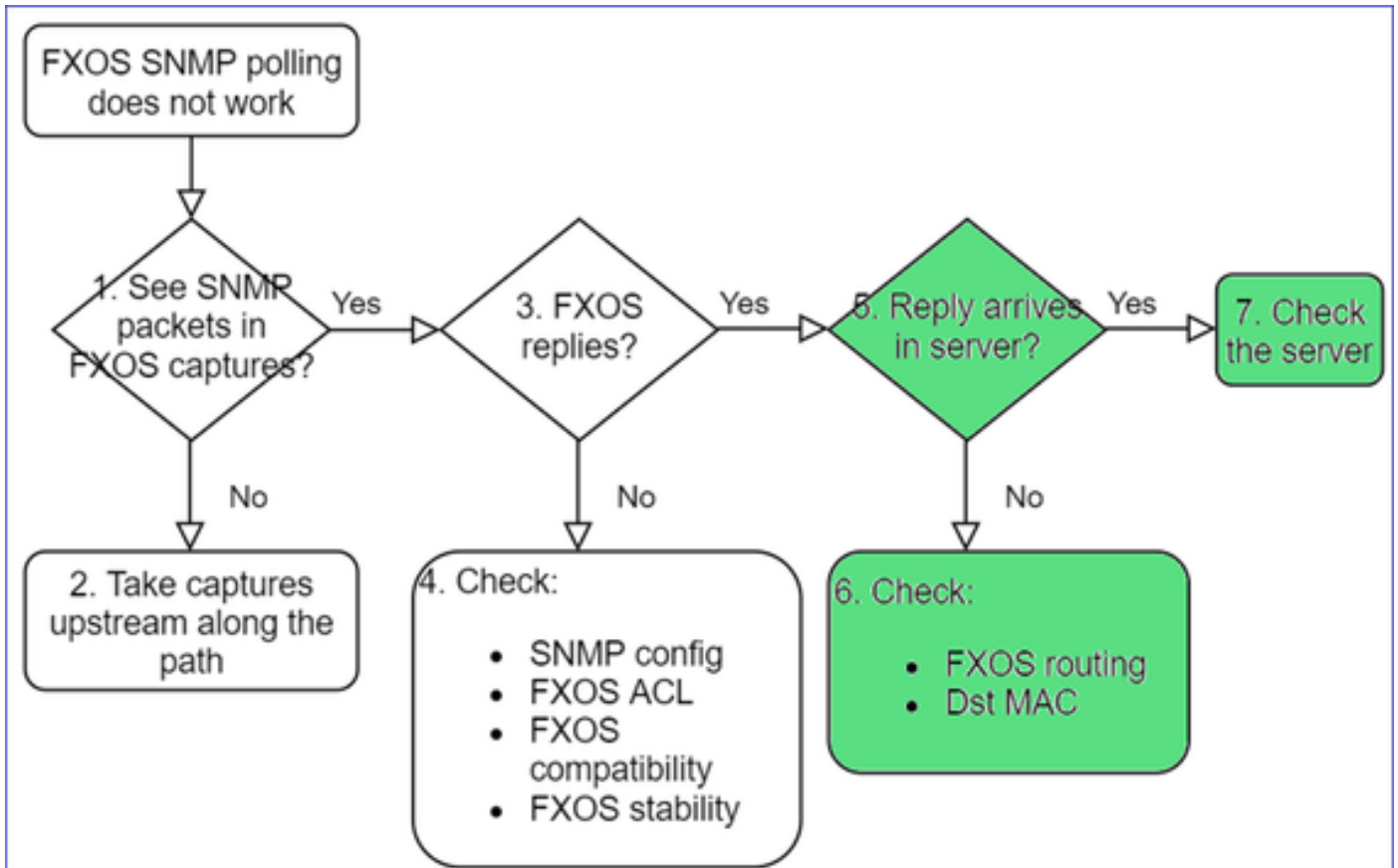
```
<#root>
```

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

```
dir cores_fxos
```

Si des fichiers principaux SNMPD s'affichent, récupérez-les avec l'ensemble de dépannage FXOS et communiquez avec Cisco TAC.

5. La réponse SNMP arrive-t-elle dans le serveur SNMP ?



- Vérifiez le routage de FXOS.

Ces données de sortie proviennent de FPR41xx/9300 :

```
<#root>
```

```
firepower#
```

```
show fabric-interconnect
```

```
Fabric Interconnect:
```

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

- Effectuez une capture, exportez le fichier PCAP et vérifiez le MAC de destination de la réponse.
- Enfin, vérifiez le serveur SNMP (captures, configuration, application, etc.).

Quelles valeurs SNMP OID utiliser?

Descriptions des problèmes (exemples de cas réels de Cisco TAC) :

- « Nous voulons surveiller l'équipement Cisco Firepower. Veuillez fournir les OID de SNMP pour chaque processeur principal, mémoire et disques. »

- « Y a-t-il un OID pouvant être utilisé pour surveiller l'état de l'alimentation sur l'appareil ASA 5555? »
- « Nous voulons récupérer l'OID SNMP du châssis sur FPR2K et FPR4K. »
- « Nous voulons interroger le cache ARP de l'appareil ASA. »
- « Nous avons besoin de connaître l'OID du SNMP pour l'homologue BGP en panne. »

Comment trouver les valeurs OID de SNMP?

Ces documents fournissent des renseignements sur les OID de SNMP sur les appareils Firepower :

- Livre blanc sur la surveillance de SNMP pour Cisco Firepower Threat Defense (FTD) :

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

- Guide de référence de la base d'informations de gestion (MIB) de FXOS pour Cisco Firepower 4100/9300 :

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

- Comment effectuer une recherche pour un OID précis sur les plateformes FXOS :

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

- Vérifiez les OID de SNMP à partir de l'interface CLI (ASA/LINA).

```
<#root>
```

```
firepower#
```

```
show snmp-server ?
```

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

```
firepower#
```

```
show snmp-server oid
```

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

- Pour en savoir plus sur les OID, consultez l'outil SNMP Object Navigator.

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

- Sur FXOS (41xx/9300), exécutez ces deux commandes à partir de l'interface CLI :

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

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

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

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

```
show snmp internal oids supported
```

```
- SNMP All supported MIB OIDs -0x11a72920
```

```
Subtrees for Context:
```

```
ccitt
```

```
1
```

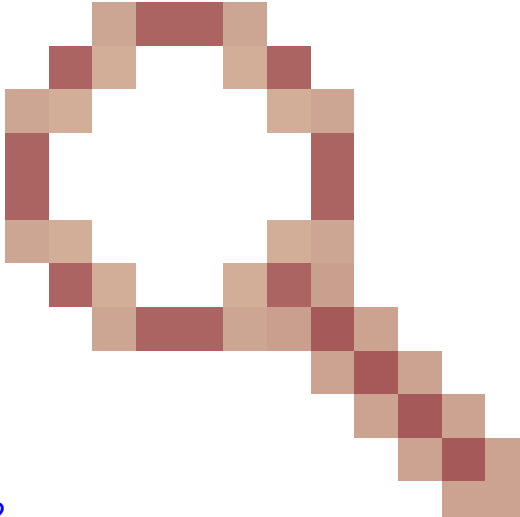
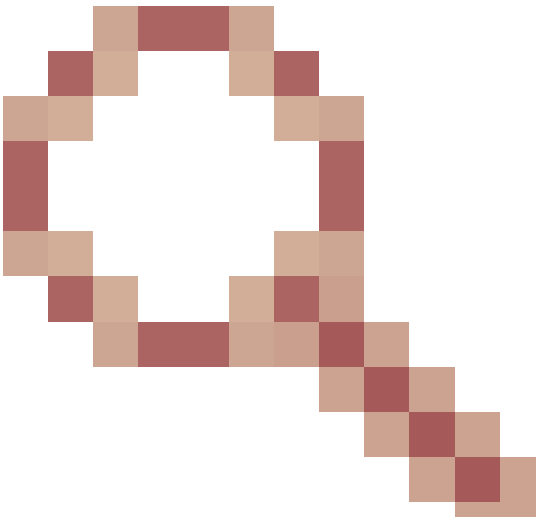
```
1.0.88010.1.1.1.1.1.1 ieee8021paeMIB
```

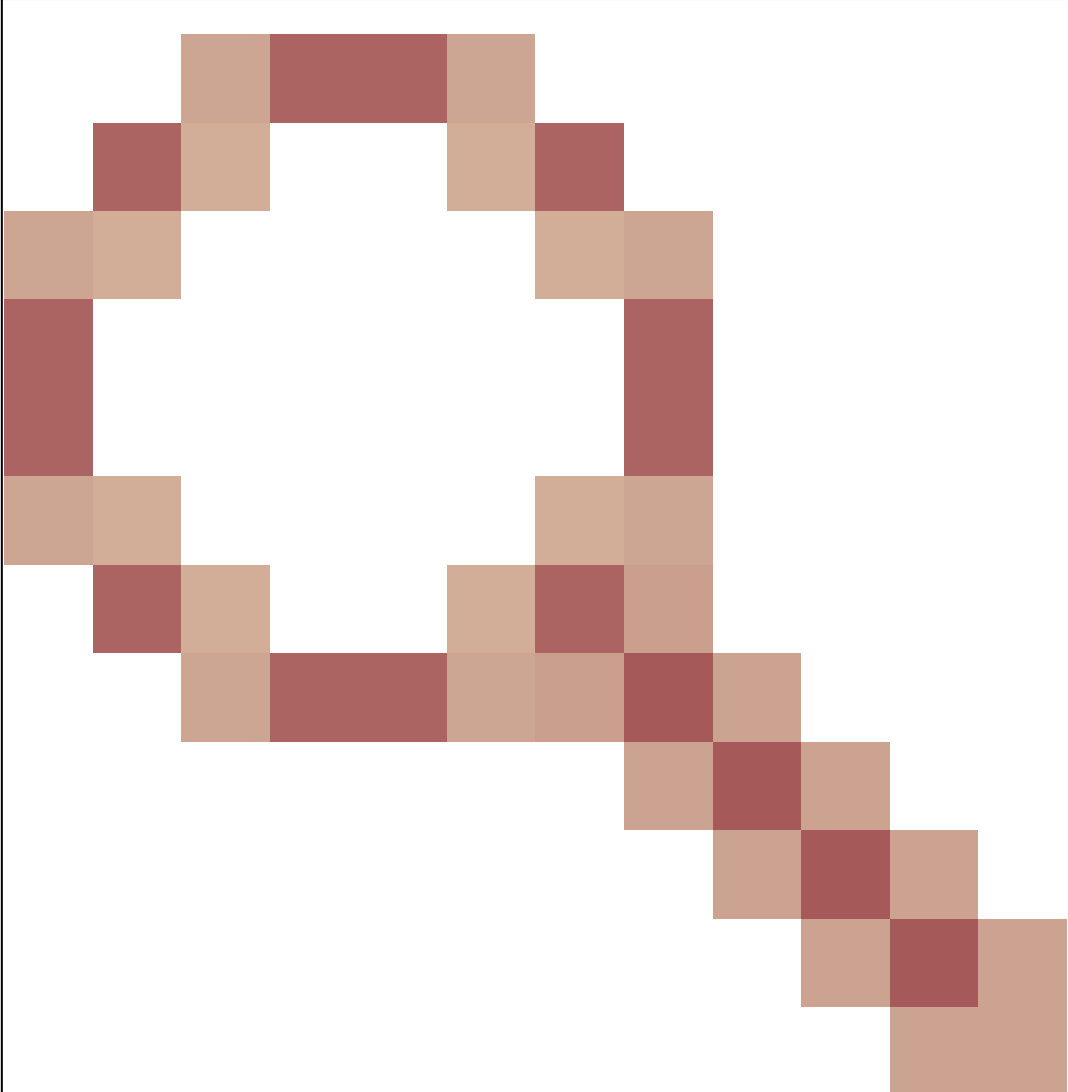
```
1.0.88010.1.1.1.1.1.2
```

```
...
```

Référence rapide – OID courants

Exigence	OID
CPU (LINA)	1.3.6.1.4.1.9.9.109.1.1.1
CPU (Snort)	1.3.6.1.4.1.9.9.109.1.1.1 (FP >= 6,7)
Mémoire (LINA)	1.3.6.1.4.1.9.9.221.1.1
Mémoire (Linux/FMC)	1.3.6.1.1.4.1.2021.4
Informations sur la haute disponibilité	1.3.6.1.4.1.9.9.491.1.4.2
Informations sur la grappe	1.3.6.1.4.1.9.9.491.1.8.1

<p>Informations sur le VPN</p>	<p>Nombre de sessions RA-VPN : 1.3.6.1.4.1.9.9.392.1.3.1 (7.x)</p> <p>Nombre d'utilisateurs RA-VPN : 1.3.6.1.4.1.9.9.392.1.3.3 (7.x)</p> <p>Nombre maximal de sessions RA-VPN : 1.3.6.1.4.1.9.9.392.1.3.41 (7.x)</p> <p>Nombre de sessions VPN S2S : 1.3.6.1.4.1.9.9.392.1.3.29</p> <p>Nombre maximal de sessions VPN S2S : 1.3.6.1.4.1.9.9.392.1.3.31</p> <p>- Conseil : firepower# show snmp-server oid j'aime</p>
<p>État BGP</p>	 <p>ENH ID de bogue Cisco CSCux13512 : Ajouter MIB BGP pour interrogation SNMP</p>
<p>Licences Smart FPR1K/2K ASA/ASAv</p>	 <p>ENH ID de bogue Cisco CSCv83590 : ASAv/ASA sur le FPR1k/2k : besoin d'un OID SNMP pour suivre l'état des licences Smart</p>
<p>OID de SNMP LINA pour un canal de port au niveau de</p>	<p>ENH ID de bogue Cisco CSCvu91544</p>

<p>FXOS</p>	 <p>: prise en charge des OID Lina SNMP pour les statistiques d'interface port-channel de niveau FXOS</p>
-------------	---

Ajouts FMC 7.3 (pour FMC 1600/2600/4600 et versions ultérieures)

Exigence	OID
<p>Déroutement d'état du ventilateur</p>	<p>ID d'interruption : 1.3.6.1.4.1.9.9.117.2.0.6</p> <p>OID de valeur : 1.3.6.1.4.1.9.9.117.1.4.1.1.1.<index></p> <p>0 - le ventilateur ne fonctionne pas</p> <p>1 - le ventilateur fonctionne</p>
<p>Déroutement de température du processeur/bloc d'alimentation</p>	<p>ID d'interruption : 1.3.6.1.4.1.9.9.91.2.0.1</p> <p>OID de seuil : 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<index>.1</p> <p>OID de la valeur : 1.3.6.1.4.1.9.9.91.1.1.1.1.4.<index></p>

Interruption d'état PSU	ID d'interruption : 1.3.6.1.4.1.9.9.117.2.0.2 OperStatus OID : 1.3.6.1.4.1.9.9.117.1.1.2.1.2.<index> OID AdminStatus : 1.3.6.1.4.1.9.9.117.1.1.2.1.1.<index> 0 - présence de l'alimentation non détectée 1 - présence de l'alimentation détectée, ok
-------------------------	--

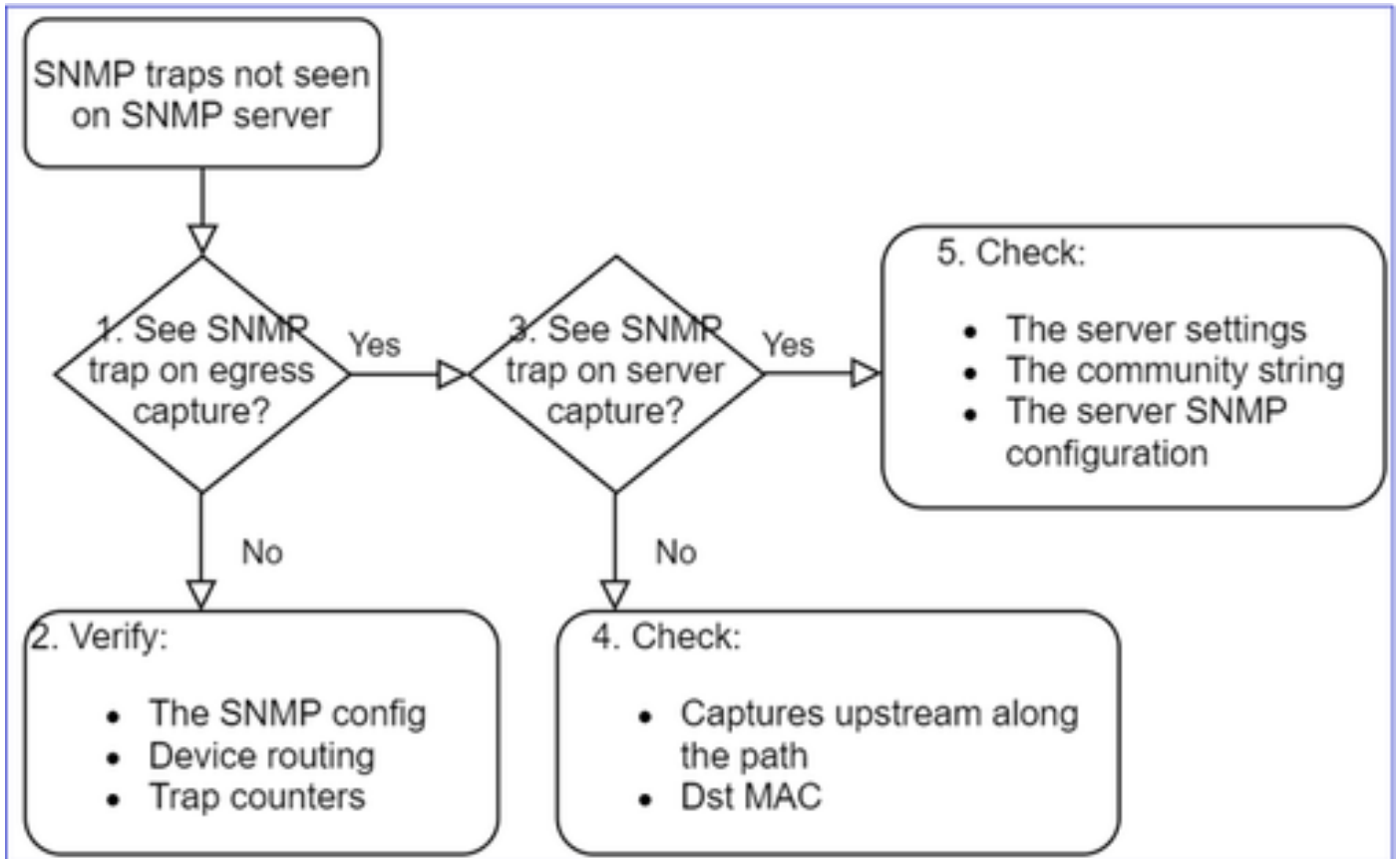
Impossible d'obtenir les dérouterments SNMP

Descriptions des problèmes (exemples de cas réels de Cisco TAC) :

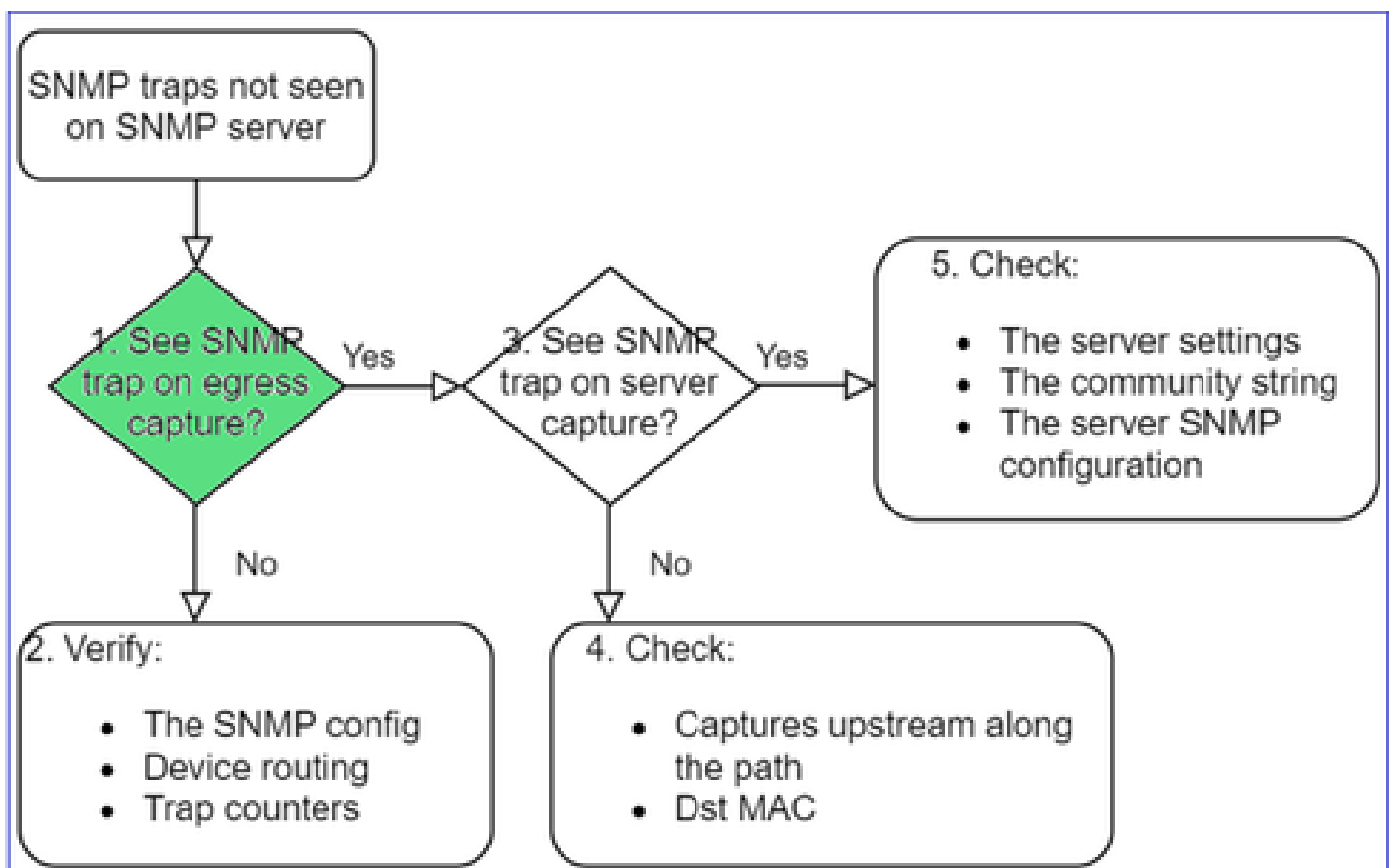
- « SNMPv3 de l'appareil FTD n'envoie aucun dérouterment au serveur SNMP. »
- « FMC et FTD n'envoient pas de messages de dérouterment SNMP. »
- « Nous avons configuré SNMP sur notre appareil FTD 4100 pour FXOS et essayé SNMPv3 et SNMPv2, mais les deux protocoles n'arrivent pas à envoyer des dérouterments. »
- « Firepower SNMP n'envoie pas de dérouterment à l'outil de surveillance. »
- « Le pare-feu de l'appareil FTD n'envoie pas de dérouterment SNMP au système de gestion de réseau. »
- « Les dérouterments du serveur SNMP ne fonctionnent pas. »
- « Nous avons configuré SNMP sur notre appareil FTD 4100 pour FXOS et essayé SNMPv3 et SNMPv2, mais les deux protocoles n'arrivent pas à envoyer des dérouterments. »

Dépannage recommandé

Voici le processus de dépannage de l'organigramme pour les problèmes de dérouterment SNMP Firepower :



1. Voyez-vous des dérouterments SNMP lors de la capture de sortie ?



Pour capturer les dérouterments de LINA/ASA sur l'interface de gestion :

```
<#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
```

Pour capturer les dérouterments de LINA/ASA sur l'interface de données :

```
<#root>
```

```
firepower#
```

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

Pour capturer les dérouterments de FXOS (41xx/9300) :

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
firepower(fxos)#
```

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

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

```
firepower(fxos)#
```

```
exit
```

```
firepower#
```

```
connect local-mgmt
```

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

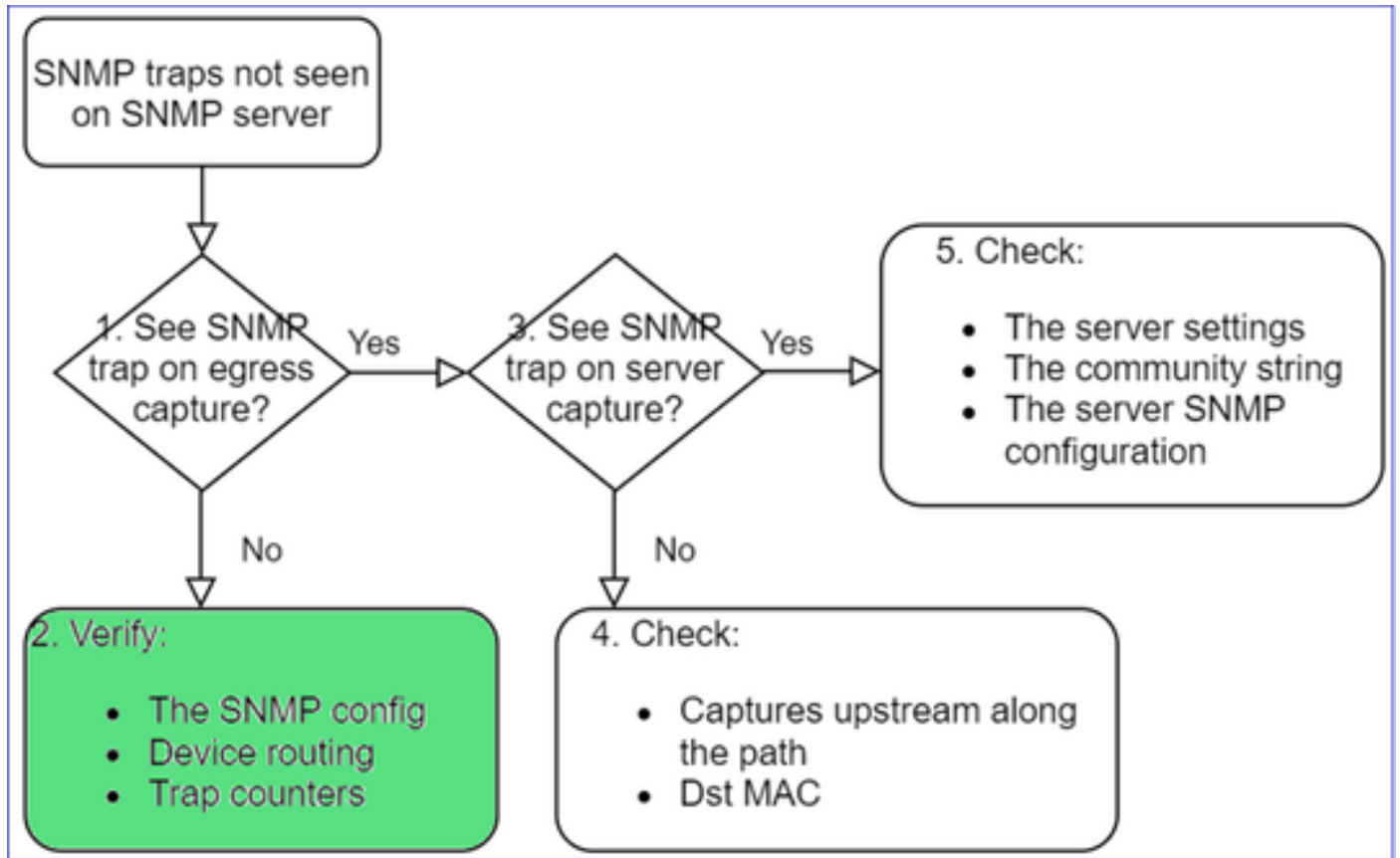
```
dir
```

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

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

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

2. Si vous ne voyez pas de paquets sur l'interface de sortie



<#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
```

Configuration des dérouterements de 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

Remarque : sur 1xxx/21xx, ces paramètres s'affichent uniquement dans le cas de Devices > Device Management > SNMP config !

- Routage de LINA/ASA pour les dérivements sur l'interface de gestion :

```
<#root>
```

```
>
```

```
show network
```

- Routage de LINA/ASA pour les dérivements sur l'interface de données :

```
<#root>
```

```
firepower#
```

```
show route
```

- Routage de FXOS (41xx/9300) :

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- Compteurs de dérivements (LINA/ASA) :

```
<#root>
```

```
firepower#
```

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

```
20 Trap PDUs
```

Et FXOS :

```
<#root>
```

```
FP4145-1#
```

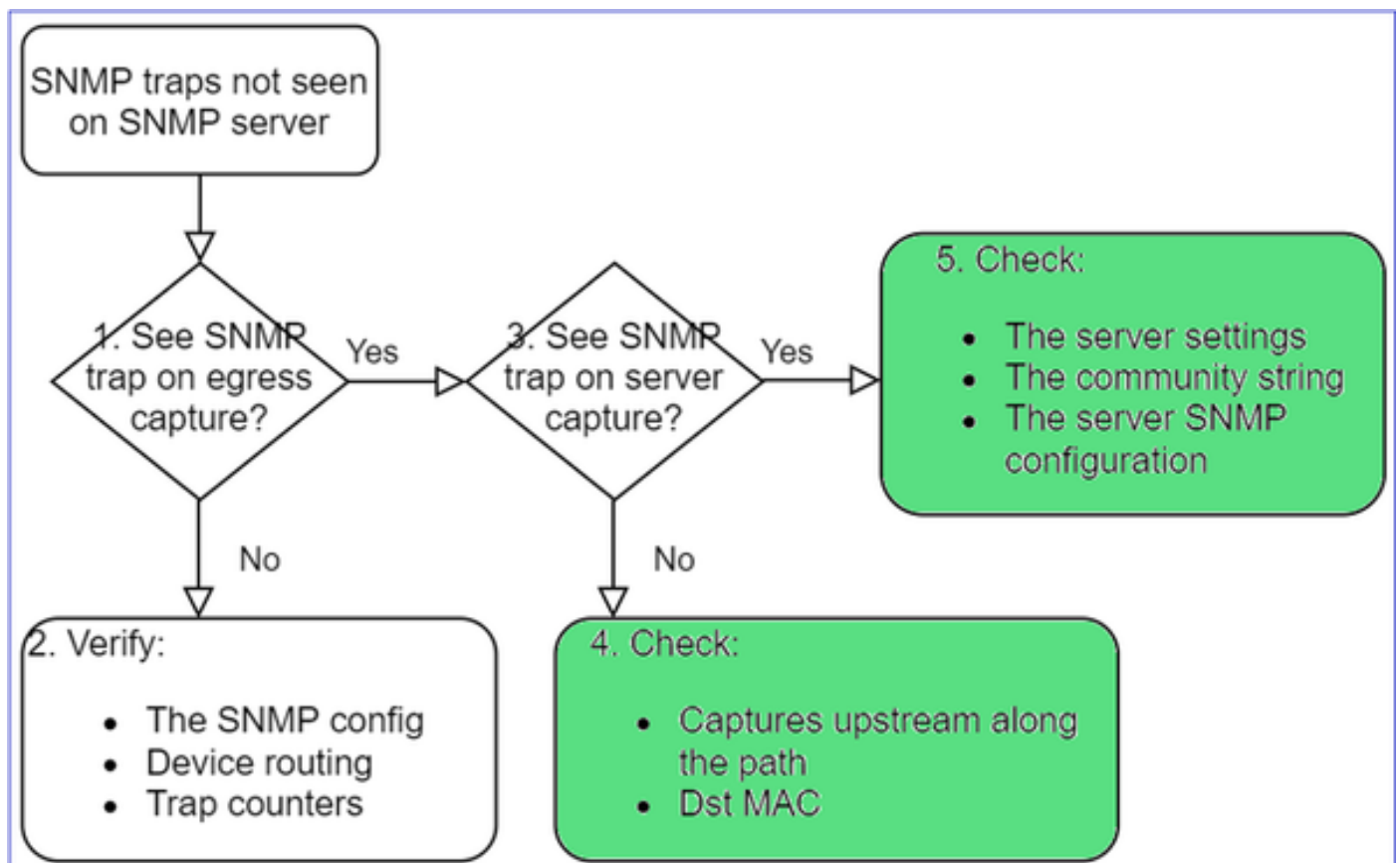
```
connect fxos
```

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

```
show snmp | grep Trap
```

```
1296 Out Traps PDU
```

Vérifications supplémentaires



- Effectuez une capture sur le serveur SNMP de destination.

Autres éléments à vérifier :

- Captures le long du chemin.
- Adresse MAC de destination des paquets de déROUTement de SNMP.
- Paramètres et état du serveur SNMP (par exemple, pare-feu, ports ouverts, etc.).
- Identifiant de communauté de SNMP.
- Configuration du serveur SNMP.

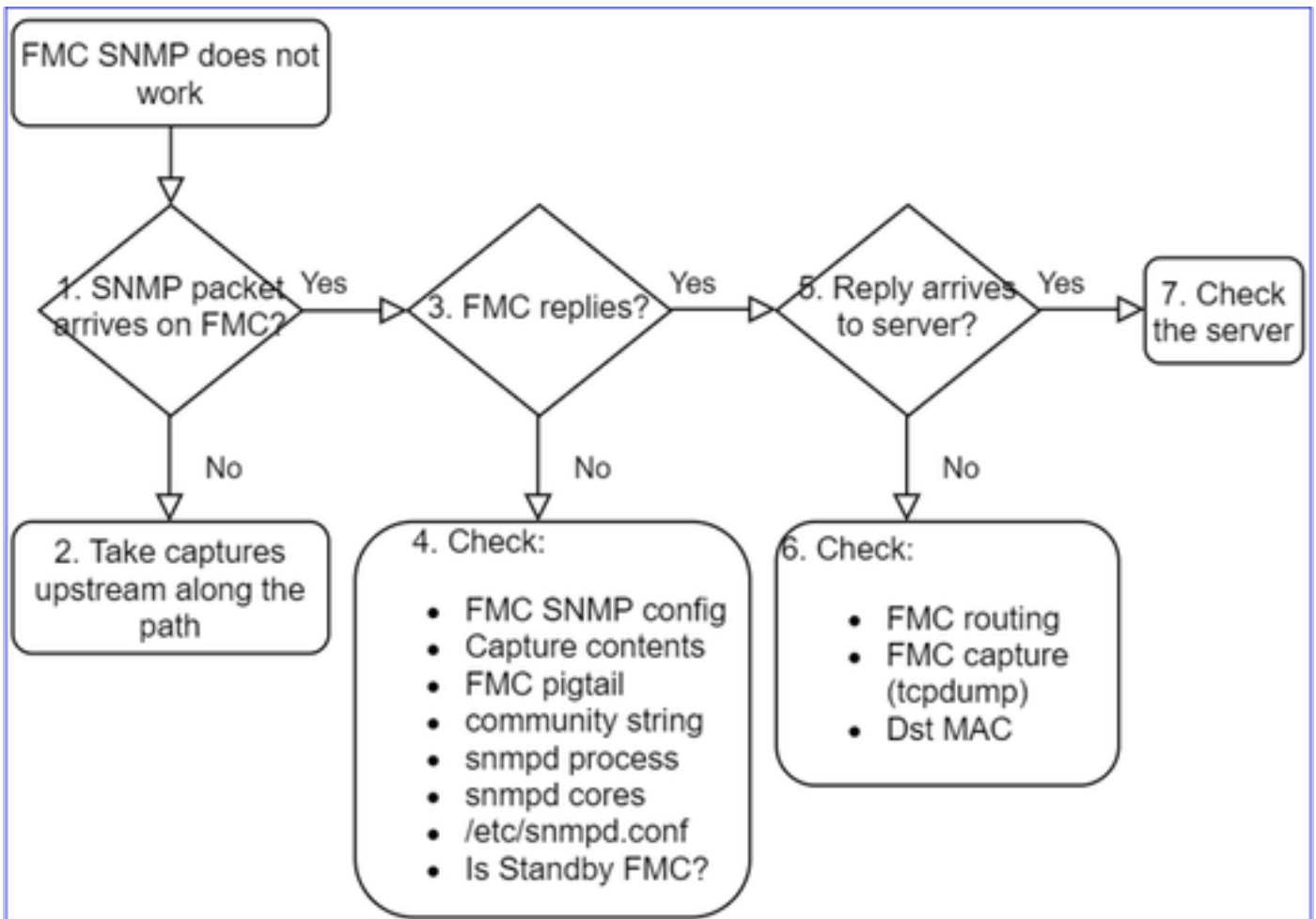
Impossible de surveiller FMC à l'aide du protocole SNMP

Descriptions des problèmes (exemples de cas réels de Cisco TAC) :

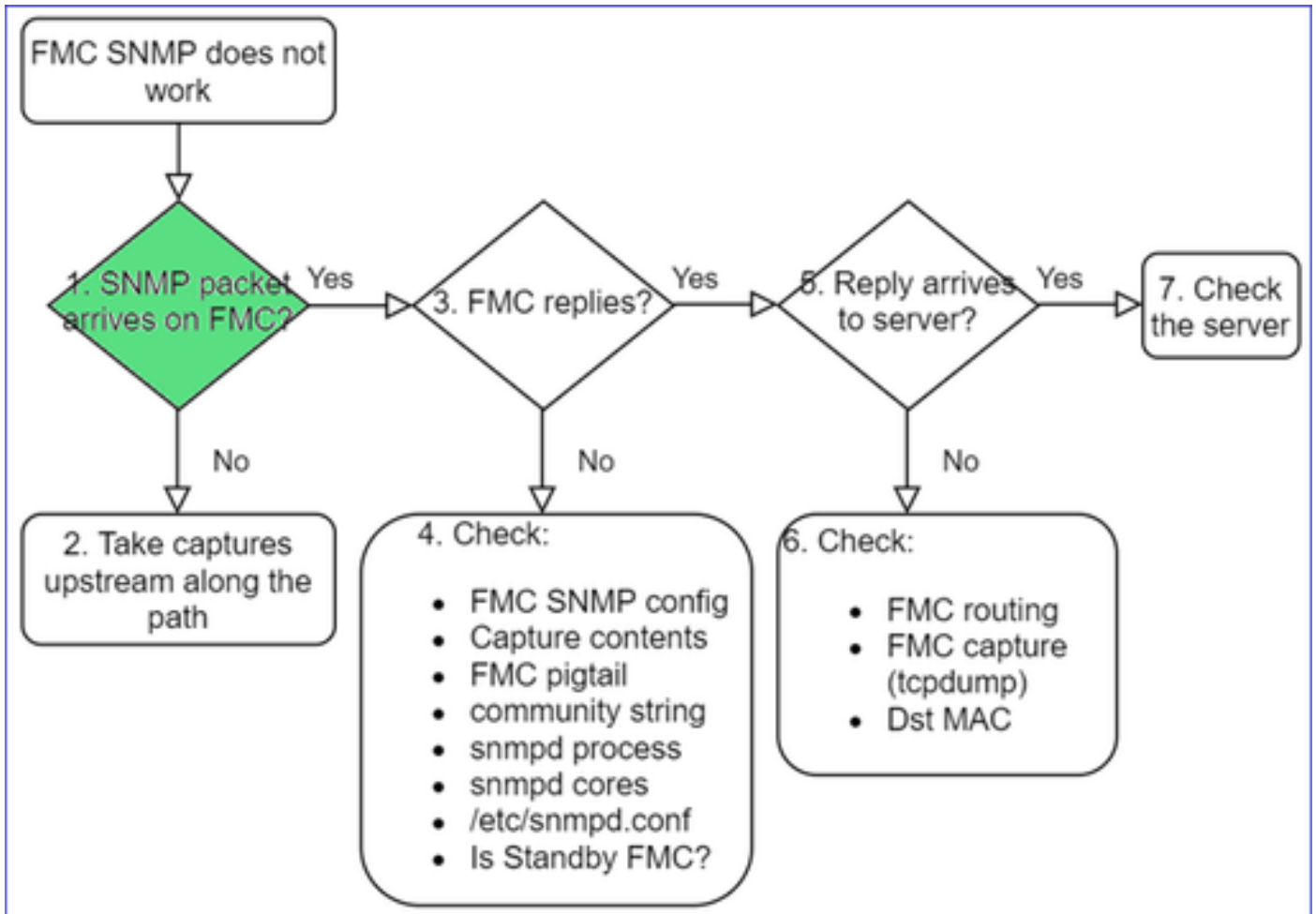
- « SNMP ne fonctionne pas sur FMC en veille. »
- « Besoin de surveiller la mémoire du FMC. »
- « SNMP devrait-il être fonctionnel sur FMC 192.168.4.0.8 en veille? »
- « Nous devons configurer les FMC pour qu'ils surveillent leurs ressources telles que le processeur, la mémoire, etc. ».

Dépannage : procédure

Voici le processus de dépannage de l'organigramme pour les problèmes FMC SNMP :



1. Le paquet SNMP arrive sur FMC ?



- Effectuez la capture suivante sur l'interface de gestion de l'appareil 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.
```

 Conseil : enregistrez la capture dans le répertoire FMC /var/common/ et téléchargez-la à partir de l'interface utilisateur FMC

```
<#root>
```

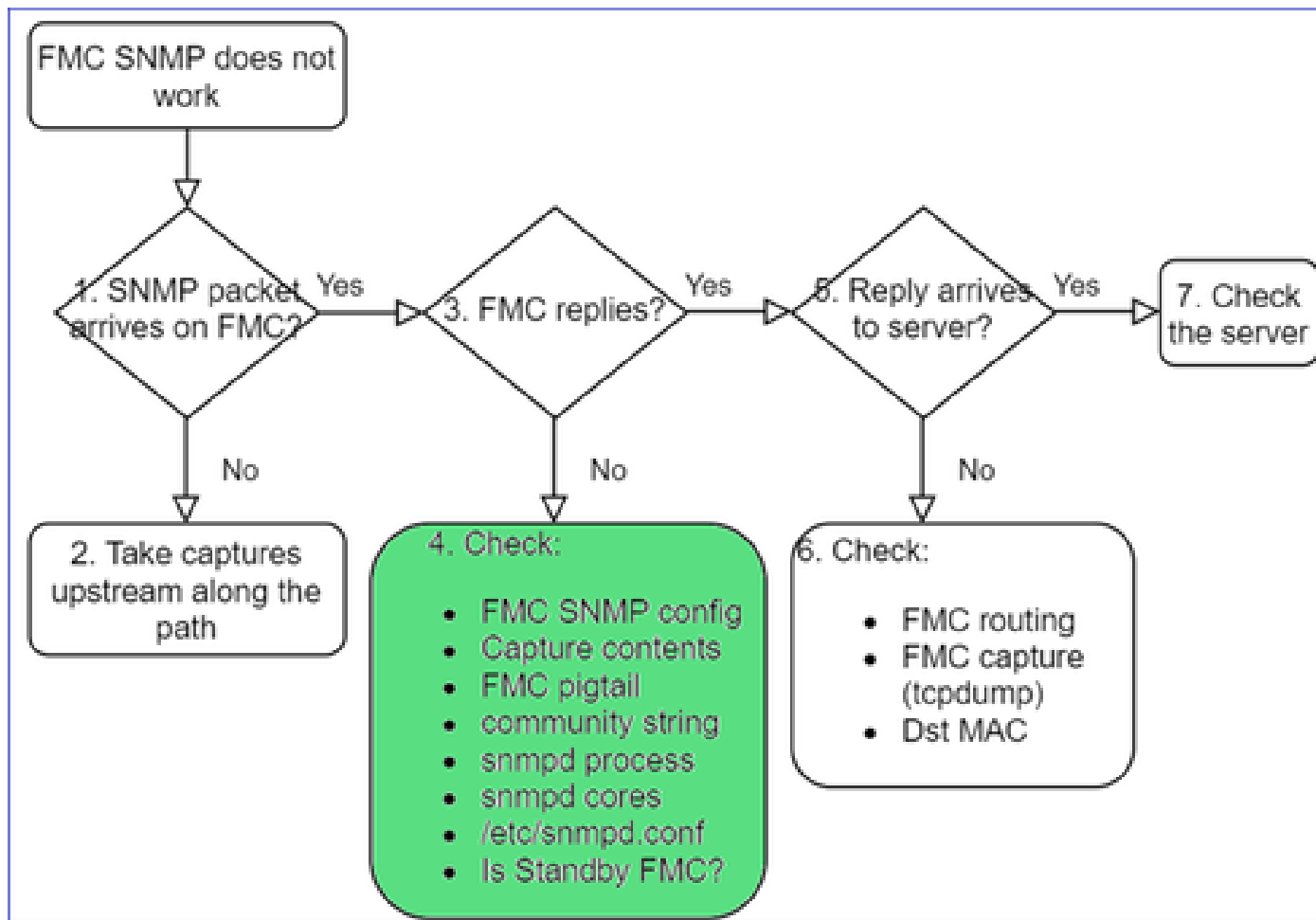
```
admin@FS2600-2:~$
```

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

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

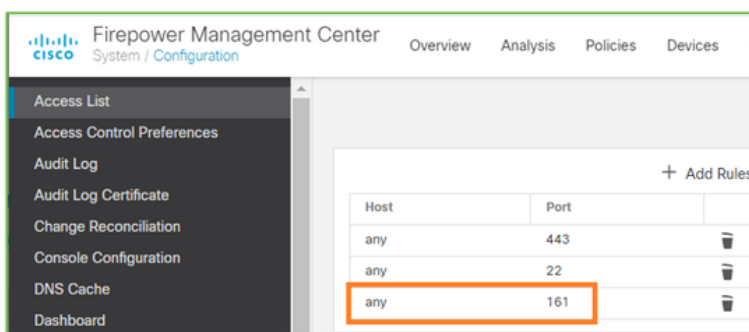
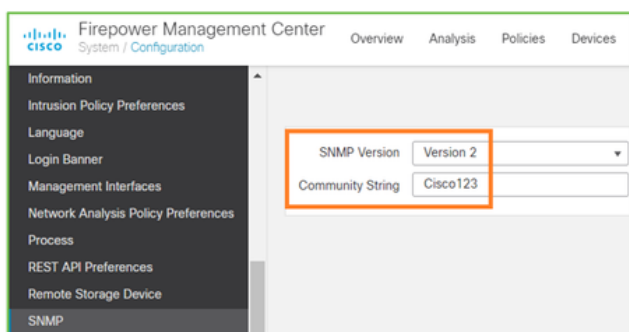
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C46 packets captured
46 packets received by filter

L'appareil FMC répond-il?



Si l'appareil FMC ne répond pas, vérifiez :

- La configuration SNMP de l'appareil FMC (System > Configuration [système > configuration]).
 1. Section SNMP
 2. Section de la liste d'accès



Si l'appareil FMC ne répond pas, vérifiez :

- Le contenu de la capture (fichier PCAP)
- L'identifiant de communauté (il peut être vu dans les captures)
- Le résultat de la queue de cochon de l'appareil FMC (recherche d'erreurs, de défaillances, de suivis) et contenu du journal /var/log/snmpd.log
- Le processus 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
```

- Les fichiers principaux snmpd

<#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
```

- Fichier de configuration dorsal dans /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
```

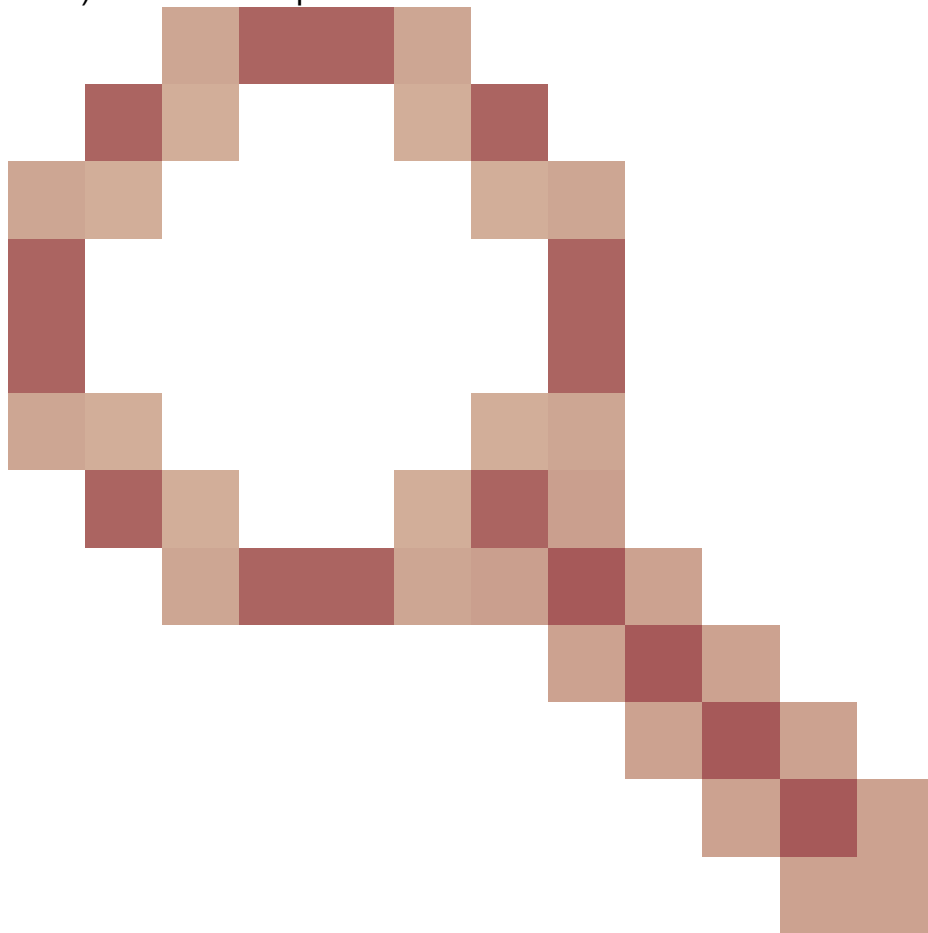
```
rocommunity6 Cisco123
```



Remarque : si SNMP est désactivé, le fichier snmpd.conf n'existe pas

- S'agit-il d'un appareil FMC en veille?

Dans les versions antérieures à 6.4.0-9 et à 6.6.0, l'appareil FMC en veille n'envoie pas de données SNMP (snmpd est en attente). C'est un comportement attendu. Consultez l'amélioration :



ID de bogue Cisco [CSCvs32303](https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-)

Échec de la configuration de SNMP

Descriptions des problèmes (exemples de cas réels de Cisco TAC) :

- « Nous voulons configurer SNMP pour Cisco Firepower Management Center et Firepower 4115 Threat Defense. »
- "Prise en charge de la configuration SNMP sur FTD".
- « Nous voulons activer la surveillance SNMP sur l'appareil FTD. »
- « Nous essayons de configurer le service SNMP dans FXOS, mais le système ne nous laisse pas entrer la commande "commit-buffer" à la fin du processus. Il indique Erreur : les modifications ne sont pas autorisées. utilisez 'Connect ftd' pour effectuer les modifications." »
- « Nous voulons activer la surveillance SNMP sur notre appareil FTD. »
- « Impossible de configurer SNMP sur l'appareil FTD et de détecter l'appareil dans la surveillance. »

Comment aborder les problèmes de configuration de SNMP?

Premiers éléments : la documentation !

- Lisez le document à jour!
- Guide de configuration de l'appareil FMC :

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

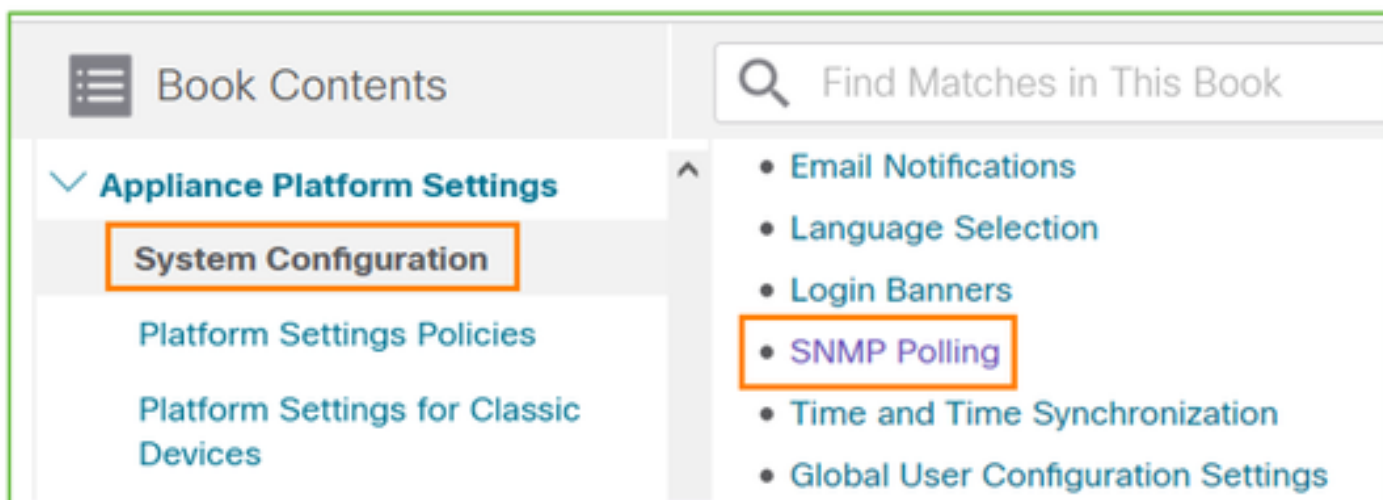
[guide-v70.html](#)

- Guide de configuration de FXOS :

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB

Prenez connaissance des différents documents relatifs au SNMP!

FMC SNMP :



FXOS SNMP :

Cisco Firepower 4100/9300 FXOS Firepower

Book Contents

Find Matches in This Book

Book Title Page

Introduction to the Firepower Security Appliance

Getting Started

License Management for the ASA

User Management

Image Management

Security Certifications Compliance

System Administration

Platform Settings

Chapter: Platform Settings

> Chapter Contents

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

Configuration de Firepower 41xx/9300 SNMP :

✓ Appliance Platform Settings

System Configuration

Platform Settings Policies

Platform Settings for Classic Devices

Platform Settings for Firepower Threat Defense

Configuration de 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

Configuration de SNMP sur Firepower Device Manager (FDM)

Descriptions des problèmes (exemples de cas réels de Cisco TAC) :

- « Nous avons besoin de conseils au sujet de SNMPv3 sur l'appareil Firepower avec FDM. »
- « La configuration de SNMP ne fonctionne pas sur l'appareil FPR 2100 à partir de FDM. »
- « Impossible de faire fonctionner la configuration de SNMPv3 sur FDM. »
- « Besoin d'aide avec la configuration de SNMP pour FDM 6.7. »
- « Activer SNMPv3 dans Firepower FDM. »

Comment aborder les problèmes de configuration de SNMP FDM

- Pour les versions antérieures à 6.7, vous pouvez effectuer la configuration de SNMP à l'aide de FlexConfig :

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

- À partir de la version 6.7 de Firepower, la configuration de SNMP ne se fait plus avec FlexConfig, mais avec l'API REST :

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

Aide-mémoire pour le dépannage de SNMP

1xxx/21xx/41xx/9300 (LINA/ASA) – Ce qu'il vous faut avant d'ouvrir un dossier auprès de Cisco TAC

Commande	Description
firepower# show run snmp-server	Vérifiez la configuration SNMP ASA/FTD LINA.

firepower# show snmp-server statistics	Vérifier les statistiques de SNMP sur ASA/FTD LINA, en particulier sur les compteurs de paquets SNMP entrants et sortants.
> capture-traffic	Capturez le trafic sur l'interface de gestion.
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	Capturez le trafic sur l'interface de données (nom : « net201 ») pour UDP 161 (interrogation SNMP).
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	Capturez le trafic sur l'interface de données (nom : « net208 ») pour UDP 162. (déroutements SNMP).
firepower# show capture SNMP-POLL packet-number 1 trace	Suivez un paquet SNMP entrant qui arrive sur l'interface de données LINA ASA/FTD.
admin@firepower:~\$ sudo tcpdump -i tap_nlp	Capture sur l'interface de prise interne NLP (Non-Lina Process).
firepower# show conn all protocol udp port 161	Vérifiez toutes les connexions ASA/FTD LINA sur UDP 161 (sondage SNMP).
firepower# show log i 302015.*161	Recherchez l'interrogation SNMP dans le journal ASA/FTD LINA 302015.
firepower# more system:running-config communauté i	Vérifiez la chaîne de communauté SNMP.
firepower# debug menu netsnmp 4	Vérifiez la configuration SNMP et l'ID de processus.
firepower# show asp table classify interface net201 domain allow match port = 161	Vérifiez le nombre d'occurrences de la liste de contrôle d'accès SNMP sur l'interface nommée « net201 ».
firepower# show disk0: coeur en l	Vérifier s'il y a des fichiers principaux SNMP.
admin@firepower:~\$ ls -l /var/data/cores	Vérifier s'il y a des fichiers principaux SNMP.

	Applicable uniquement sur le FTD.
firepower# show route	Vérifiez la table de routage ASA/FTD LINA.
> show network	Vérifiez la table de routage du plan de gestion FTD.
admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	Vérification/dépannage de SNMPv3 sur FTD.
firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	Ces commandes sont masquées sur les versions les plus récentes. Débogages internes, utiles pour dépanner SNMP avec le centre d'assistance technique Cisco.

41xx/9300 (FXOS) – Ce qu'il vous faut avant d'ouvrir un dossier auprès de Cisco TAC

Commande	Description
<pre>firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture- filter "udp port 161" limit-captured-frames 50 write workspace:///SNMP-POLL.pcap firepower(fxos)# exit firepower# connect local-mgmt firepower(local-mgmt)# dir 1 11152 Jul 26 09:42:12 2021 SNMP.pcap firepower(local-mgmt)# copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap</pre>	<p>Prendre un capture de FXOS pour l'interrogation de SNMP (UDP 161).</p> <p>Charger sur un serveur FTP distant.</p> <p>IP FTP : 192.0.2.100</p> <p>Nom d'utilisateur FTP : ftp</p>
<pre>firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture- filter "udp port 162" limit-captured-frames 50 write</pre>	<p>Effectuer une capture de FXOS pour les dérouterments de SNMP (UDP 162).</p>

workspace:///SNMP-TRAP.pcap	
firepower# scope system firepower /system # scope services firepower /system/services # show ip-block detail	Vérifier la liste de contrôle d'accès de FXOS.
firepower# show fault	Vérifier les défaillances de FXOS.
firepower# show fabric-interconnect	Vérifier la configuration de l'interface et les paramètres de passerelle par défaut de FXOS.
firepower# connect fxos firepower(fxos)# show running-config snmp all	Vérifier la configuration de SNMP FXOS.
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	Vérifier les OID de FXOS SNMP.
firepower# connect fxos firepower(fxos)# show snmp	Vérifier les paramètres et les compteurs de FXOS SNMP.
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	Débogage de FXOS SNMP (« packets » pour les paquets seulement, ou « all » pour tout). Utiliser les commandes « terminal no monitor » et « undebug all » pour l'arrêter.

1xxx/21xx (FXOS) – Ce qu'il vous faut avant d'ouvrir un dossier auprès de Cisco TAC

Commande	Description
> capture-traffic	Capturer le trafic sur l'interface de gestion.

> show network	Vérifier le tableau de routage du plan de gestion de FTD.
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail] firepower /monitoring # show snmp-trap	Vérifier la configuration de FXOS SNMP
firepower# show fault	Vérifier les défaillances de FXOS.
firepower# connect local-mgmt firepower(local-mgmt)# dir cores_fxos firepower(local-mgmt)# dir cores	Vérifier les fichiers principaux de FXOS (recherche de la source)

FMC – Ce qu'il vous faut avant d'ouvrir un dossier auprès de Cisco TAC

Commande	Description
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n	Capturer le trafic sur l'interface de gestion pour l'interrogation de SNMP.
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	Capturer le trafic sur l'interface de gestion pour l'interrogation de SNMP et l'enregistrer dans un fichier.
admin@FS2600-2:~\$ sudo pmtool status grep snmpd	Vérifier l'état du processus de SNMP.
admin@FS2600-2:~\$ ls -al /var/common grep snmpd	Vérifier les fichiers principaux de SNMP (recherche de la source).
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	Vérifier le contenu du fichier de configuration de SNMP.

Exemples pour la commande snmpwalk

Ces commandes peuvent être utilisées pour la vérification et le dépannage :

Commande	Description
<pre># snmpwalk -c Cisco123 -v2c 192.0.2.1</pre>	Récupérer tous les OID de l'hôte distant à l'aide de SNMPv2c. Cisco123 = identifiant de communauté 192.0.2.1 = hôte de destination
<pre># snmpwalk -v2c -c Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.9.109.1.1.1.3 iso.3.6.1.4.1.9.9.109.1.1.1.3.1 = jauge32 : 0</pre>	Récupérer un OID précis de l'hôte distant à l'aide de SNMPv2c.
<pre># snmpwalk -c Cisco123 -v2c 192.0.2.1 .10.3.1.1.4.1.9.9.109.1.1.1.1 -On 0.10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 = Jauge32 : 0</pre>	Afficher les OID récupérés au format numérique.
<pre># snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 - x AES -X Cisco123 192.0.2.1</pre>	Récupérer tous les OID de l'hôte distant à l'aide de SNMPv3. Utilisateur SNMPv3 = cisco Authentification SNMPv3 = SHA. Autorisation SNMPv3 = AES
<pre># snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 - x AES -X Cisco123 192.0.2.1</pre>	Récupérer tous les OID de l'hôte distant à l'aide de SNMPv3 (MD5 et AES128).
<pre># snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1</pre>	SNMPv3 avec authentification uniquement.

Comment rechercher des défaillances sur SNMP

1. Rendez-vous à la page suivante :

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

2. Entrez le mot clé snmp et choisissez Select from list.

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

The screenshot shows the 'Bug Search Tool' interface with search results. The search criteria are the same as in the previous screenshot. The 'Product:' dropdown menu is now set to 'Cisco Firepower Management Center Virtual Appliance'. Below the search criteria, there are filter options for 'Modified Date:', 'Status:', 'Severity:', 'Rating:', 'Support Cases:', and 'Bug Type:'. The 'Bug Type:' filter is set to 'Customer Visible'. Below the filters, there is a section for 'Viewing 1 - 25 of 159 results'. The first result is highlighted: 'CSCvh32876 - ENH:Device level settings of FP2100 should allow to configure ACL and SNMP location'. The 'Symptom' is: '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 ...'. The 'Severity' is 6, 'Status' is 'Terminated', 'Updated' is 'Jan 3, 2021', and 'Cases' is 2. There are also star ratings and a 'Sort by' dropdown menu.

Produits les plus courants :

- Logiciel Cisco ASA (Adaptative Security Appliance)
- Cisco Firepower, série 9300
- Appareil virtuel Cisco Firepower Management Center (FMC)
- Cisco Firepower NGFW

Informations connexes

- [Configurer SNMP pour Threat Defense](#)
- [Configuration de SNMP sur FXOS \(interface utilisateur\)](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.