

Configuración de SNMP en dispositivos Firepower NGFW

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[SNMP del chasis \(FXOS\) en FPR4100/FPR9300](#)

[Configuración de SNMPv1/v2c en FXOS mediante la GUI](#)

[Configuración de SNMPv1/v2c en FXOS mediante la interfaz de línea de comandos \(CLI\)](#)

[Configuración de SNMPv3 en FXOS mediante la GUI](#)

[Configuración de SNMPv3 en FXOS mediante la CLI](#)

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

[Configuración de SNMPv2c en LINA](#)

[Configuración de SNMPv3 en LINA](#)

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

[SNMP en FPR2100](#)

[SNMP del chasis \(FXOS\) en FPR2100](#)

[Configuración de SNMPv1/v2c en FXOS](#)

[Configuración de SNMPv3 en FXOS](#)

[SNMP de FTD \(LINA\) en FPR2100](#)

[Verificación](#)

[Verificación del SNMP en FXOS para FPR4100/FPR9300](#)

[Verificaciones de SNMPv2c en FXOS](#)

[Verificaciones de SNMPv3 en FXOS](#)

[Verificación del SNMP en FXOS para FPR2100](#)

[Verificaciones de SNMPv2 en FXOS](#)

[Verificaciones de SNMPv3 en FXOS](#)

[Verificación del SNMP en FTD](#)

[Permiso de tráfico del SNMP a FXOS en FPR4100/FPR9300](#)

[Configuración de la lista de acceso global mediante la GUI](#)

[Configuración de la lista de acceso global mediante la CLI](#)

[Verificación](#)

[Utilice OID Object Navigator](#)

[Troubleshoot](#)

[No se puede sondear el SNMP de FTD en LINA](#)

[No se puede sondear el SNMP en FXOS](#)

[¿Qué valores de OID del SNMP se deben utilizar?](#)

[No se pueden obtener operaciones de notificación del SNMP](#)

[No se puede monitorear el FMC a través del SNMP](#)

[Configuración del SNMP en el administrador de dispositivos Firepower \(FDM\)](#)

[Hojas de referencia de solución de problemas del SNMP](#)

[Cómo buscar defectos en el SNMP](#)

[Información Relacionada](#)

Introducción

En este documento se describe cómo configurar y solucionar problemas del protocolo simple de administración de red (SNMP) en dispositivos FTD de firewall de última generación (NGFW).

Prerequisites

Requirements

Este documento requiere conocimientos básicos del SNMP.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los dispositivos de NGFW Firepower se pueden dividir en 2 subsistemas principales:

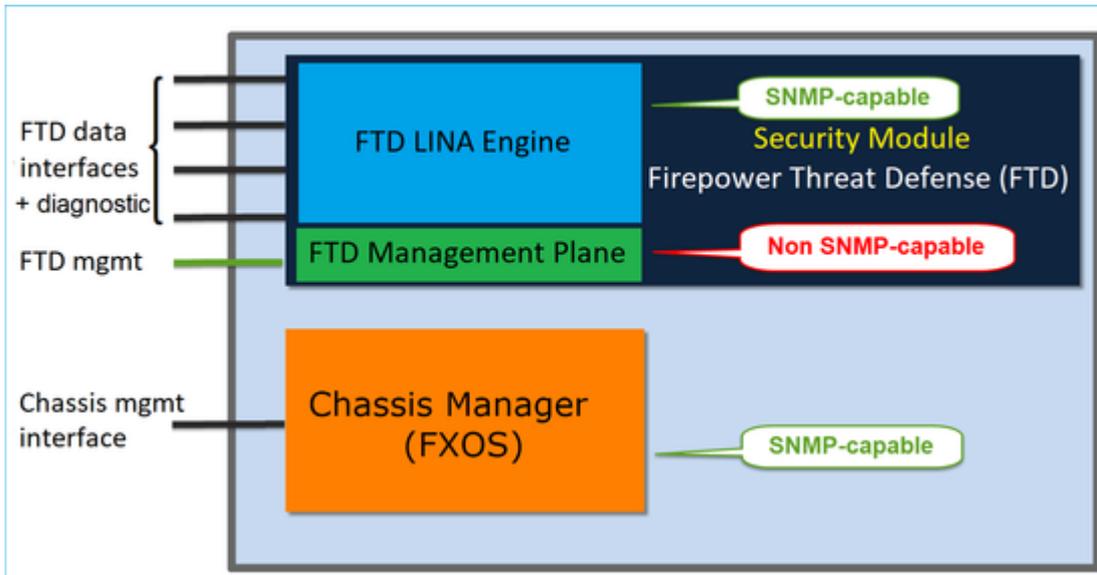
- Firepower Extensible Operative System (FXOS) controla el hardware del chasis.
- Firepower Threat Defense (FTD) se ejecuta dentro del módulo.

FTD es un software unificado que consta de 2 motores principales, el motor Snort y el motor LINA. El motor del SNMP actual de FTD deriva del ASA clásico y tiene visibilidad de las características relacionadas con LINA.

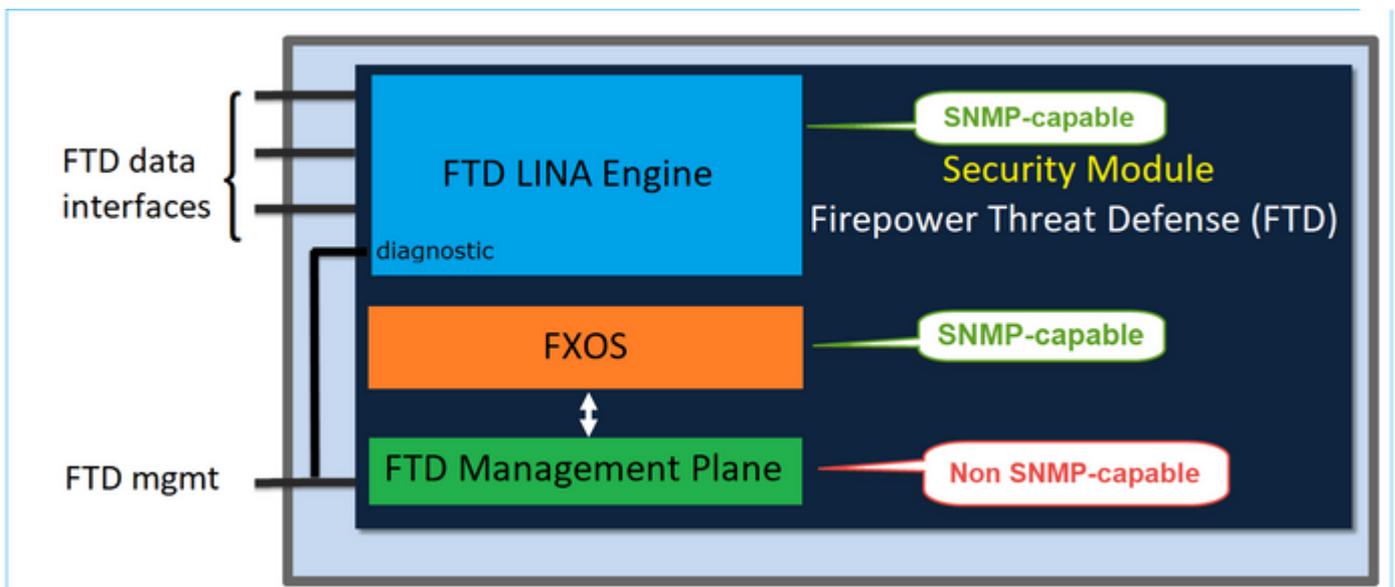
FX-OS y FTD tienen planos de control independientes y para fines de monitoreo, tienen diferentes motores SNMP. Cada uno de los motores SNMP proporciona información diferente y es posible que desee supervisar ambos para obtener una vista más completa del estado del dispositivo.

Desde el punto de vista del hardware, existen actualmente dos arquitecturas principales para los appliances de NGFW Firepower: las series Firepower 2100 y Firepower 4100/9300.

Los dispositivos Firepower 4100/9300 tienen una interfaz dedicada para la administración de dispositivos y este es el origen y el destino del tráfico del SNMP dirigido al subsistema FXOS. Por otro lado, la aplicación FTD utiliza una interfaz LINA (datos y diagnósticos). En las versiones de FTD posteriores a 6.6, también se puede utilizar la interfaz de administración de FTD) para la configuración del SNMP.



El motor del SNMP en los dispositivos Firepower 2100 utiliza la IP y la interfaz de administración de FTD. El propio dispositivo une el tráfico del SNMP recibido en esta interfaz y lo reenvía al software FXOS.

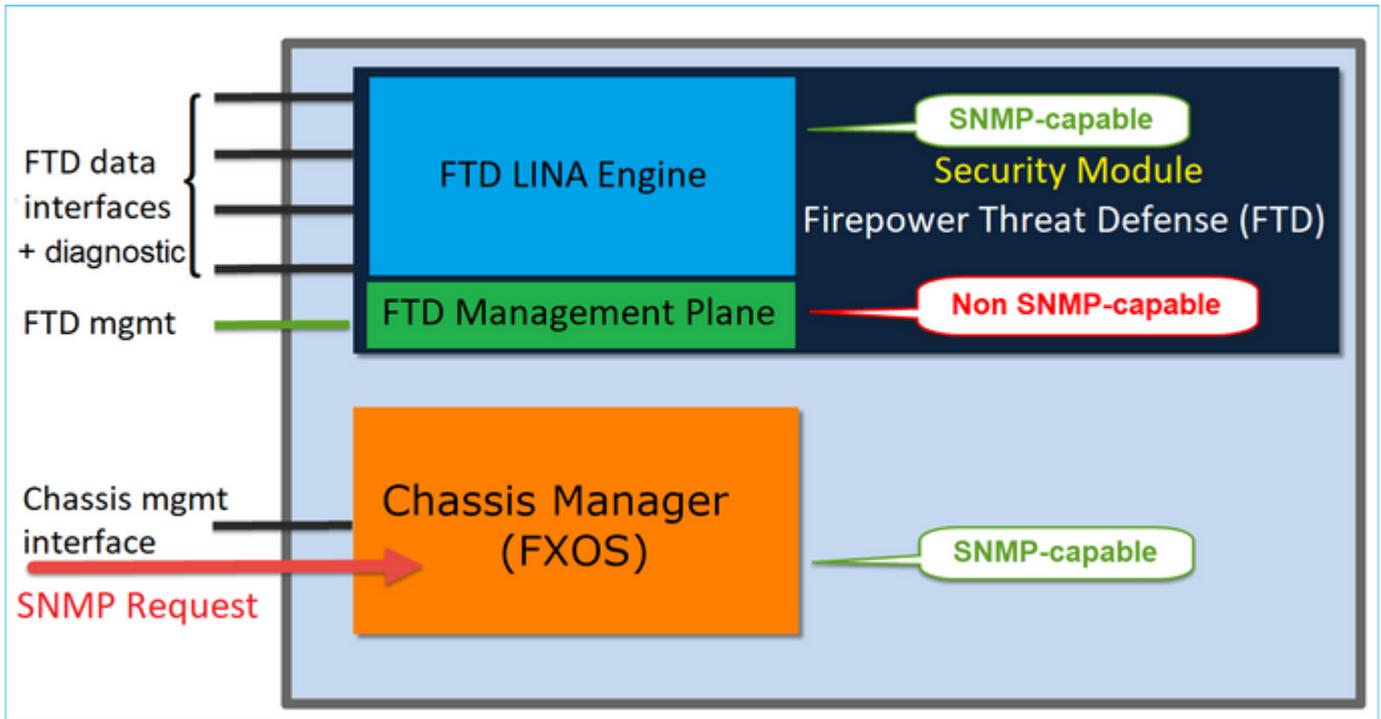


En FTD (que utiliza la versión de software 6.6+) se introdujeron estos cambios:

- SNMP sobre la interfaz de administración.
- En las plataformas de las series FPR1000 o FPR2100, unifica el SNMP de LINA y el SNMP de FXOS en esta única interfaz de administración. Además, proporciona un único punto de configuración en el FMC en **Configuración de la plataforma > SNMP**.

Configurar

SNMP del chasis (FXOS) en FPR4100/FPR9300



Configuración de SNMPv1/v2c en FXOS mediante la GUI

Paso 1. Abra la interfaz de usuario del administrador de chasis Firepower (FCM) y vaya a la ficha **Configuración de la plataforma > SNMP**. Marque la casilla **Habilitar SNMP**, especifique la cadena **Comunidad** que se utilizará en las solicitudes del SNMP y haga clic en **Guardar**.

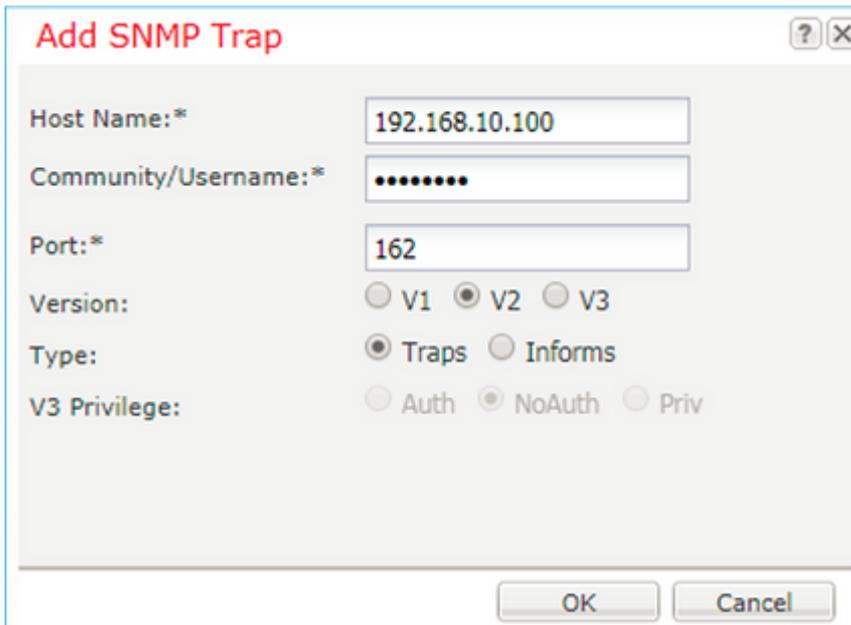
The screenshot shows the **Platform Settings > SNMP** configuration page. The following elements are highlighted with red boxes and numbered:

- Admin State:** The **Enable** checkbox is checked.
- Community/Username:** A text input field containing a masked value (dots).
- Save:** The **Save** button at the bottom left.
- Add:** The **Add** button in the **SNMP Traps** section.

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

Nota: Si el campo **Community/Username** ya está configurado, el texto a la derecha del campo vacío será **Set: Yes**. Si el campo **Community/Username** (Comunidad/Nombre de usuario) aún no se ha rellenado con un valor, el texto situado a la derecha del campo vacío será **Set: No (Establecer: No)**.

Paso 2. Configure el servidor de destino de operaciones de notificación del SNMP.



Nota: Los valores de comunidad para las consultas y el host de capturas son independientes y pueden ser diferentes

El host se puede definir como dirección IP o por nombre. Seleccione **Aceptar** y la configuración del servidor de operaciones de notificación del SNMP se guardará automáticamente. No es necesario seleccionar el botón Guardar en la página principal del SNMP. Lo mismo ocurre cuando se elimina un host.

Configuración de SNMPv1/v2c en FXOS mediante la interfaz de línea de comandos (CLI)

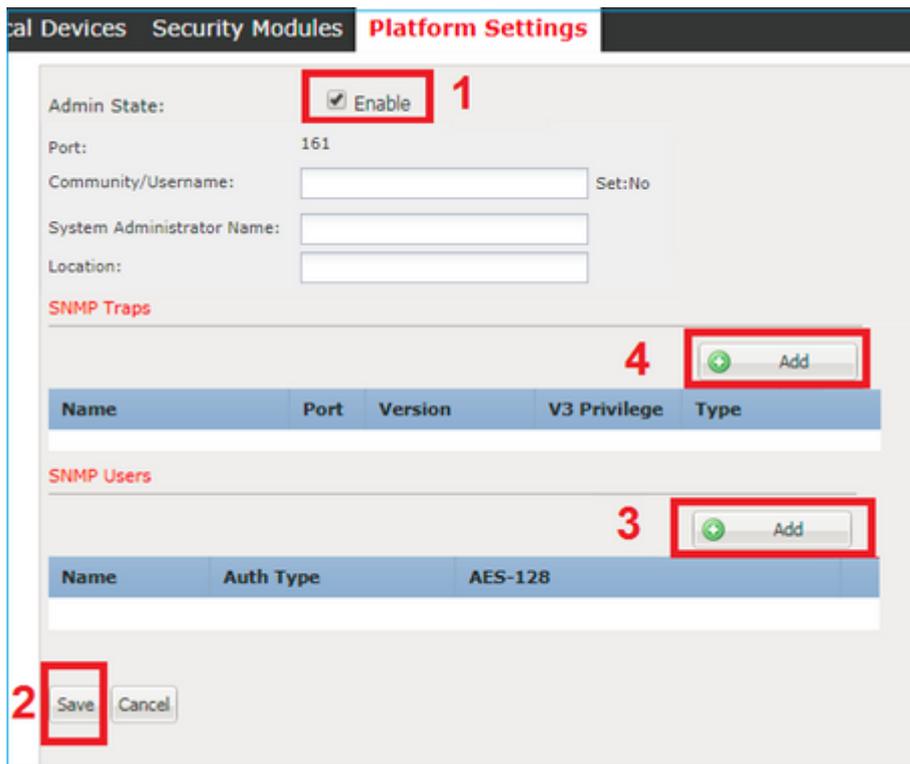
```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring* #
set snmp community
Enter a snmp community:
ksec-fpr9k-1-A /monitoring* #
  enter snmp-trap 192.168.10.100
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A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

Configuración de SNMPv3 en FXOS mediante la GUI

Paso 1. Abra el FCM y vaya a la ficha **Configuración de la plataforma > SNMP**.

Paso 2. Para SNMPv3, no es necesario establecer ninguna cadena de comunidad en la sección superior. Cada usuario creado puede ejecutar correctamente las consultas al motor del SNMP en FXOS. El primer paso es habilitar el SNMP en la plataforma. Una vez hecho esto, puede crear los usuarios y el host de operaciones de notificación de destino. Tanto los usuarios del SNMP como los hosts de operaciones de notificación del SNMP se guardan automáticamente.



Paso 3. Como se muestra en la imagen, agregue el usuario del SNMP. El tipo de autenticación siempre es SHA, pero puede utilizar AES o DES para el cifrado:

Add SNMP User

Name:* user1

Auth Type: SHA

Use AES-128:

Password:

Confirm Password:

Privacy Password:

Confirm Privacy Password:

OK Cancel

Paso 4. Agregue el host de operaciones de notificación del SNMP, como se muestra en la imagen:

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

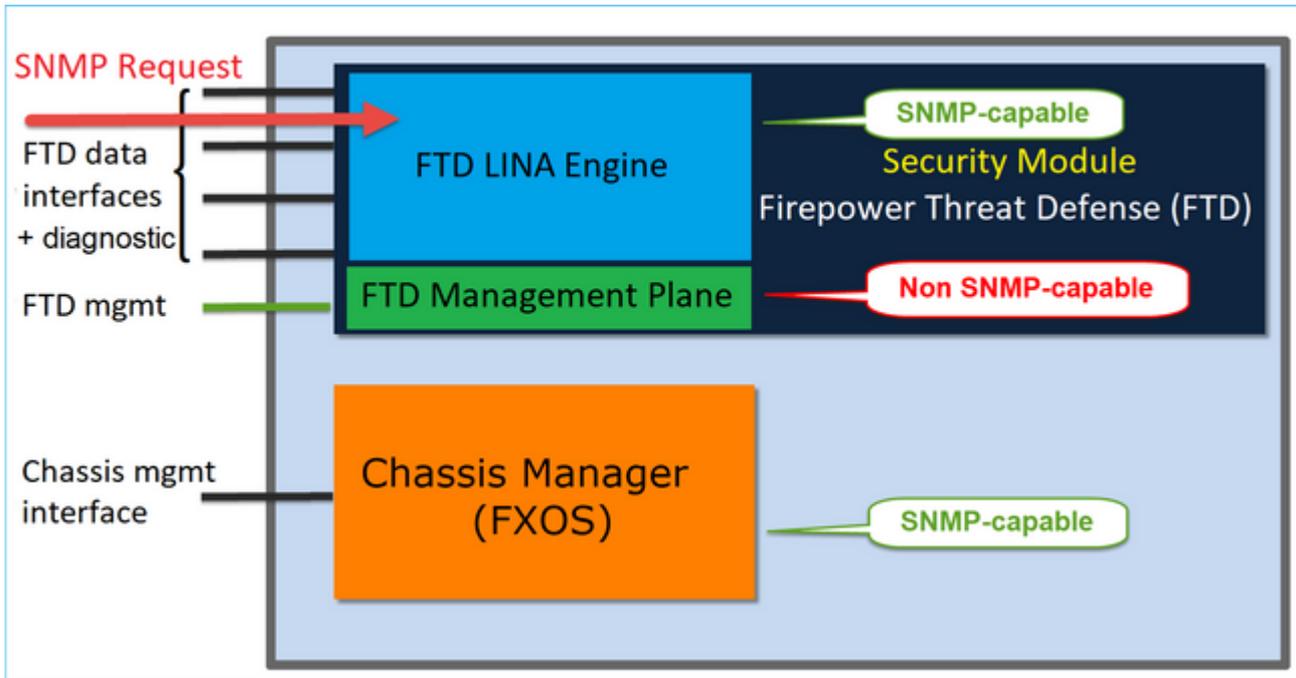
OK Cancel

Configuración de SNMPv3 en FXOS mediante la CLI

```
<#root>  
ksec-fpr9k-1-A#  
scope monitoring  
ksec-fpr9k-1-A /monitoring #  
enable snmp  
ksec-fpr9k-1-A /monitoring #  
create snmp-user user1
```

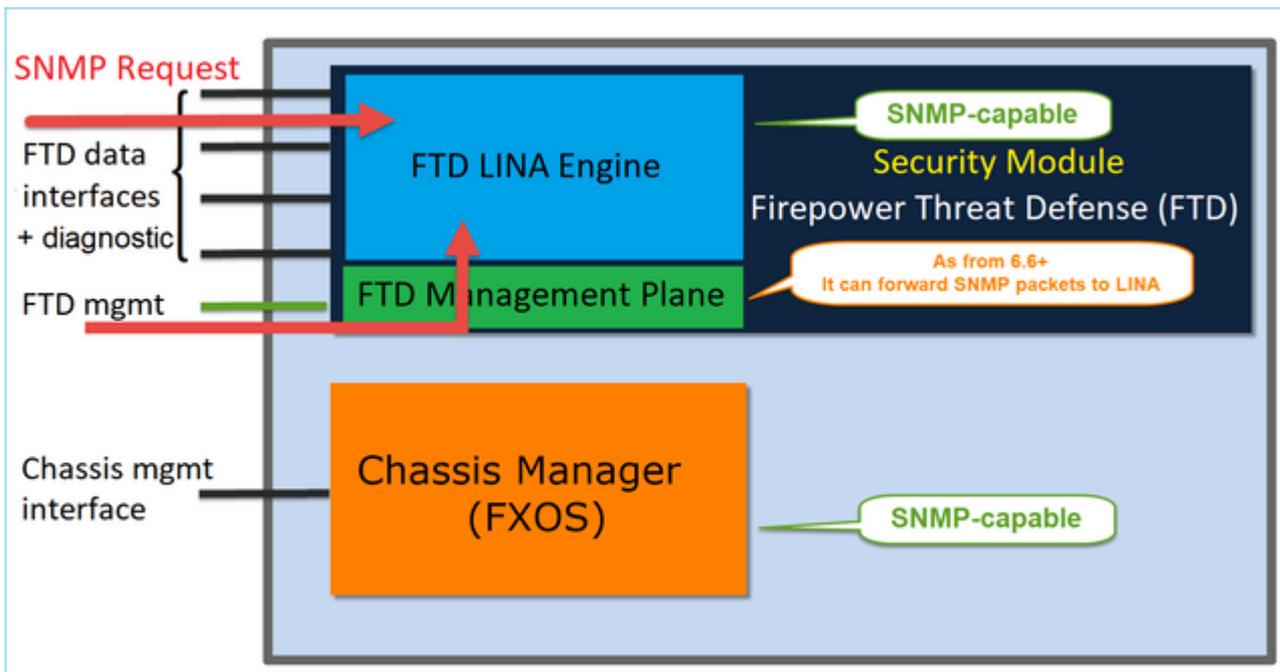
```
Password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set auth sha
ksec-fpr9k-1-A /monitoring/snmp-user* #
set priv-password
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter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

SNMP de FTD (LINA) en FPR4100/FPR9300



Cambios en las versiones 6.6+

- En las versiones posteriores a 6.6, también tiene la opción de utilizar la interfaz de administración de FTD para sondeos y operaciones de notificación.



La función de administración de IP única del SNMP se admite desde la versión 6.6 en todas las plataformas de FTD:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 que ejecuta FTD
- FTDv

Configuración de SNMPv2c en LINA

Paso 1. En la interfaz de usuario del FMC, vaya a **Dispositivos > Configuración de la plataforma > SNMP**. Marque la opción 'Habilitar servidores SNMP' y configure los parámetros de SNMPv2 de la siguiente manera:

Paso 2. En la ficha **Hosts**, seleccione el botón **Agregar** y especifique la configuración del servidor SNMP.

The screenshot displays the 'Edit SNMP Management Hosts' configuration window. The 'IP Address*' field is set to 'SNMP-SERVER' and the 'SNMP Version' is set to '2c'. The 'Poll' checkbox is checked, and the 'Trap' checkbox is unchecked. The 'Port' field is empty, with a range of '(1 - 65535)' indicated. Below the main configuration fields, there are two sections: 'Available Zones' and 'Selected Zones/Interfaces'. The 'Available Zones' section lists several zones: INSIDE_FTD4110, OUTSIDE1_FTD4110, OUTSIDE2_FTD4110, NET1_4100-3, NET2_4100-3, and NET3_4100-3. The 'Selected Zones/Interfaces' section contains the zone 'OUTSIDE3'. An 'Add' button is positioned between the two lists. At the bottom of the window, there are 'OK' and 'Cancel' buttons.

También puede especificar la interfaz de **diagnóstico** como origen para los mensajes del SNMP. La interfaz de diagnóstico es una interfaz de datos que solo permite el tráfico directo y listo para usar (solo administración).

Add SNMP Management Hosts

IP Address*
SNMP-SERVER +

SNMP Version
2c

Username

Community String

Confirm

Poll
 Trap

Trap Port
162
(1 - 65535)

Reachable By:

Device Management Interface (Applicable from v6.6.0 and above)
 Security Zones or Named Interface

Available Zones ⌵

Q Search Add

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

Selected Zones/Interfaces

diagnostic 🗑️

Interface Name Add

Cancel OK

Esta imagen es de la versión 6.6 y utiliza un tema liviano.

Además, en las versiones de FTD posteriores a 6.6 también puede elegir la interfaz de administración:

Add SNMP Management Hosts

IP Address*
 SNMP-SERVER +

SNMP Version
 2c

Username
 [Empty]

Community String
 [Empty]

Confirm
 [Empty]

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

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

Selected Zones/Interfaces

- diagnostic

Interface Name

Si se selecciona la nueva interfaz de administración, el SNMP de LINA está disponible en la interfaz de administración.

El resultado:

Enable SNMP Servers

Read Community String

Confirm*

System Administrator Name

Location

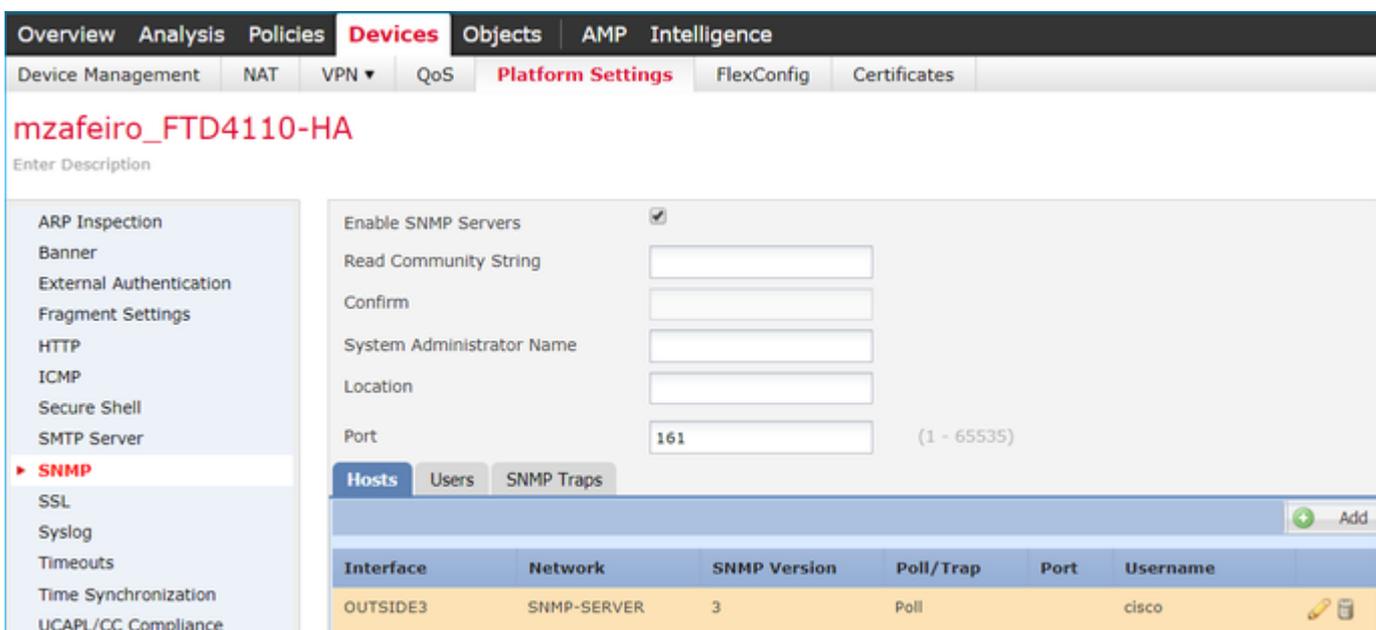
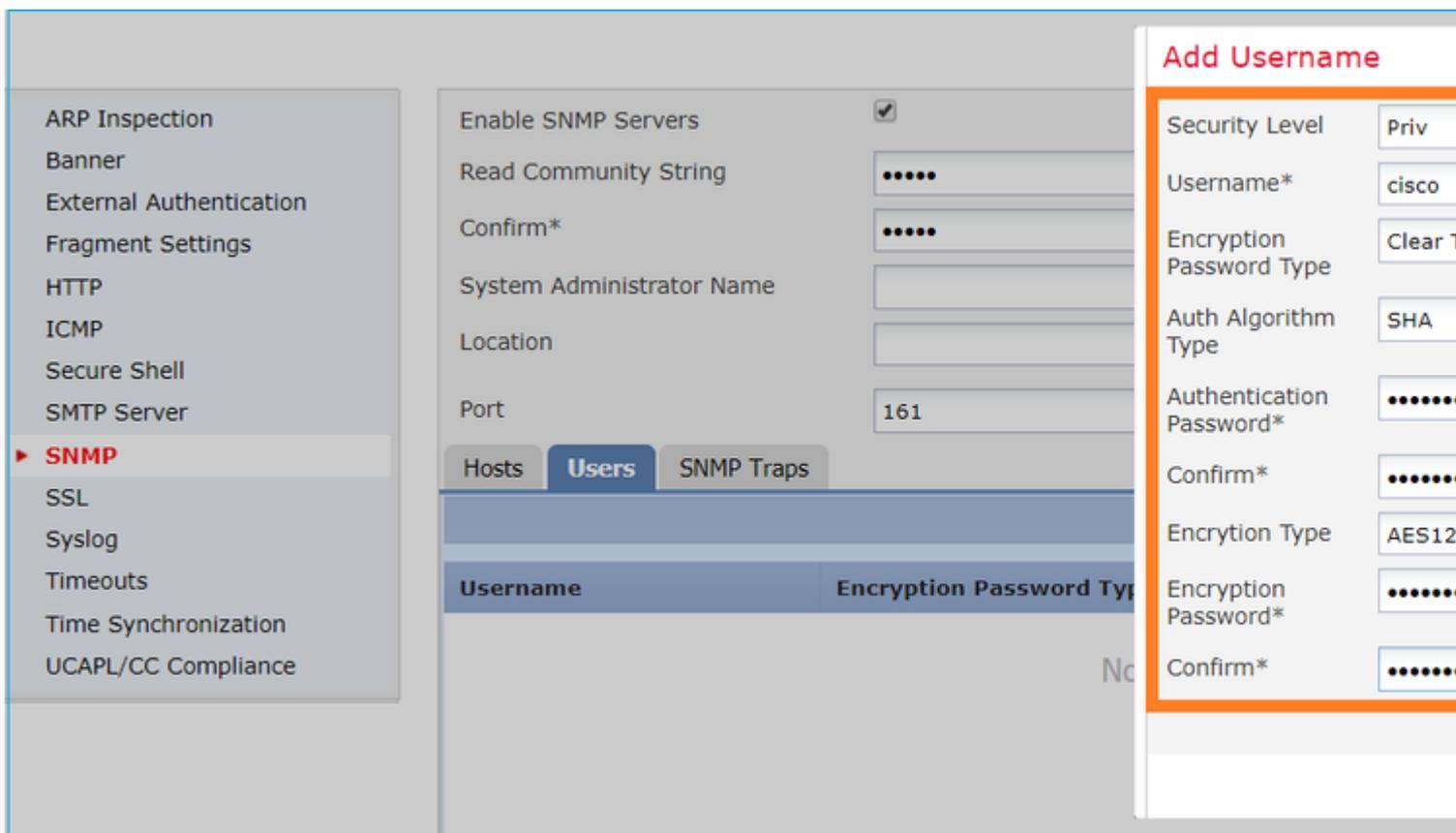
Port (1 - 65535)

Hosts Users SNMP Traps

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

Configuración de SNMPv3 en LINA

Paso 1. En la interfaz de usuario del FMC, vaya a **Dispositivos > Configuración de la plataforma > SNMP**. Marque la opción **Habilitar servidores SNMP** y configure el usuario y el host de SNMPv3:



Paso 2. Configure el host también para recibir operaciones de notificación:

Edit SNMP Management Hosts

IP Address*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port (1 - 65535)

Available Zones

Selected Zones/Interfaces

Paso 3. Las operaciones de notificación que desea recibir se pueden seleccionar en la sección **Operaciones de notificación del SNMP**:

SNMP

SSL

Syslog

Timeouts

Time Synchronization

UCAPL/CC Compliance

Hosts Users **SNMP Traps**

Enable Traps All SNMP Syslog

Standard

Authentication:

Link up

Link Down

Cold Start

Warm Start

Entity MIB

Unificación SNMP de blade MIO (FXOS 2.12.1, FTD 7.2, ASA 9.18.1)

Comportamiento anterior a 7.2

- En las plataformas 9300 y 4100, los MIB SNMP para la información del chasis no están disponibles en SNMP configurados en aplicaciones FTD/ASA. Es necesario configurarlo por separado en la tarjeta MIO mediante el administrador del chasis y acceder a él por separado. MIO es el módulo de administración y E/S (supervisor).
- Se deben configurar dos políticas SNMP independientes, una en el blade/aplicación y otra en MIO para la supervisión SNMP.
- Se utilizan puertos independientes, uno para el blade y otro para MIO para la supervisión SNMP del mismo dispositivo.
- Esto puede crear complejidad cuando intenta configurar y monitorear los dispositivos 9300 y 4100 a

través de SNMP.

Funcionamiento en versiones más recientes (FXOS 2.12.1, FTD 7.2, ASA 9.18.1 y posteriores)

- Con la unificación SNMP de MIO Blade, los usuarios pueden consultar los MIB de LINA y MIO a través de las interfaces de aplicación (ASA/FTD).
- La función se puede activar o desactivar mediante la nueva interfaz de usuario de MIO CLI y FCM (Chassis Mgr).
- El estado predeterminado es desactivado. Esto significa que el agente SNMP de MIO se está ejecutando como una instancia independiente. Las interfaces MIO deben utilizarse para sondear MIB de chasis/DME. Una vez habilitada la función, las interfaces de aplicación se pueden utilizar para sondear los mismos MIB.
- La configuración está disponible en la interfaz de usuario del administrador de chasis en **Platform-settings > SNMP > Admin Instance**, donde el usuario puede especificar la instancia de FTD que cotejaría/recopilaría las MIB del chasis para presentarla al NMS
- Se admiten aplicaciones ASA/FTD nativas y MI.
- Esta función solo es aplicable a plataformas basadas en MIO (FPR9300 y FPR4100).

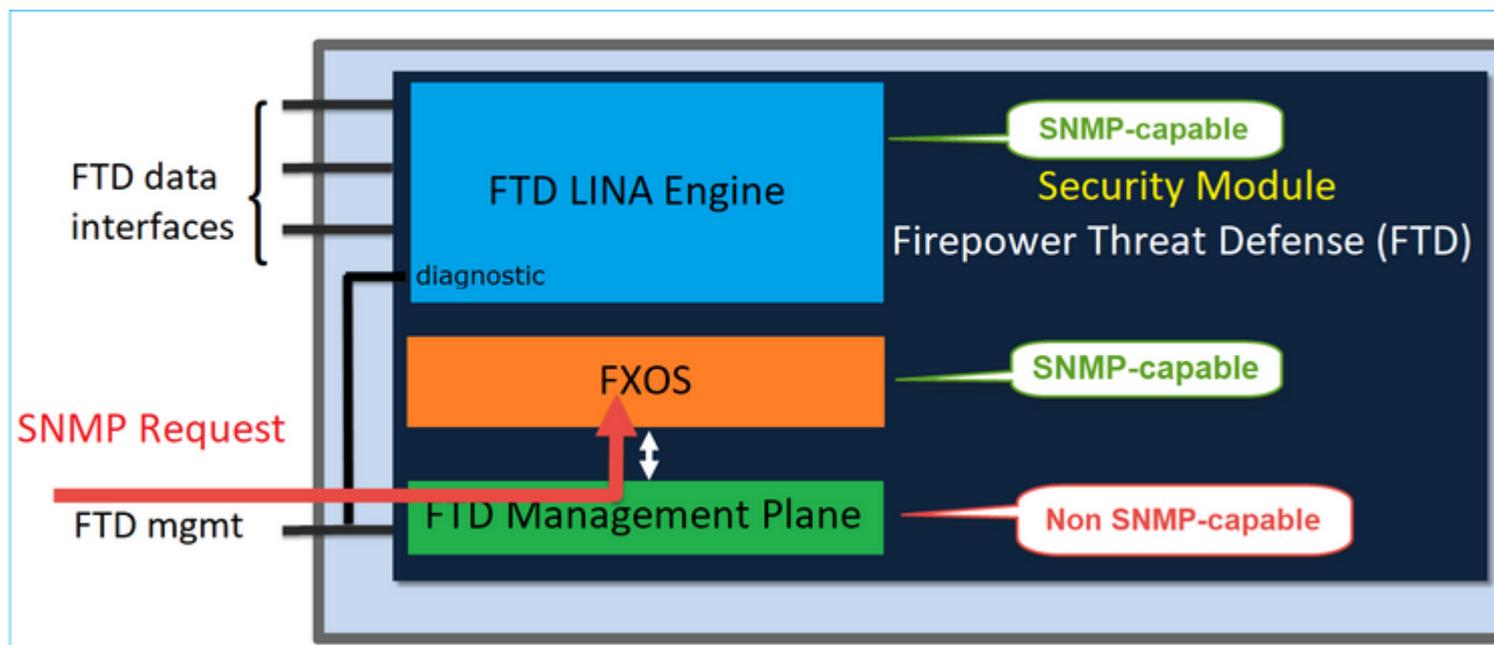
Prerrequisitos, Plataformas Compatibles

- Versión mínima de administrador compatible: FCM 2.12.1
- Dispositivos gestionados: FPR9300 / FP4100 Series
- Versión mínima de dispositivos administrados admitidos requerida: FXOS 2.12.1, FTD 7.2 o ASA 9.18.1

SNMP en FPR2100

En los sistemas FPR2100, no hay FCM. La única manera de configurar el SNMP es mediante el FMC.

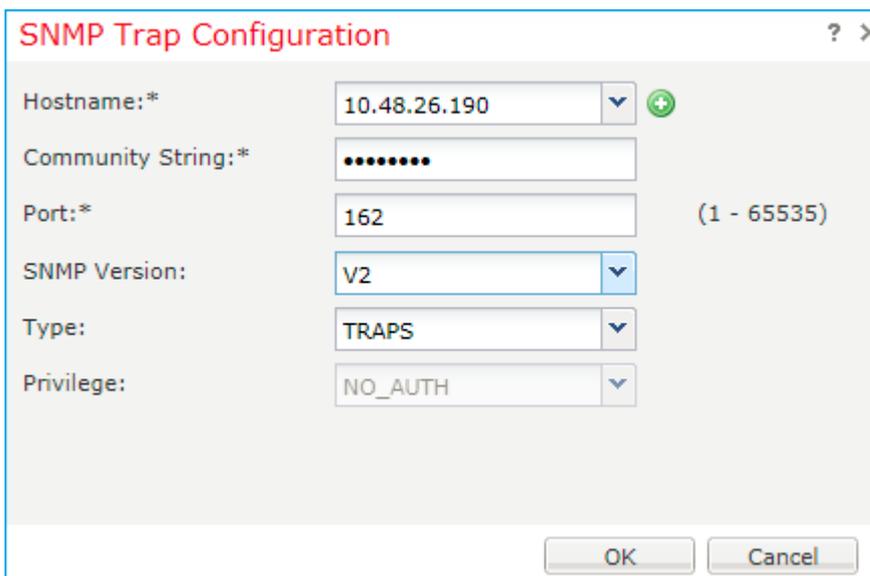
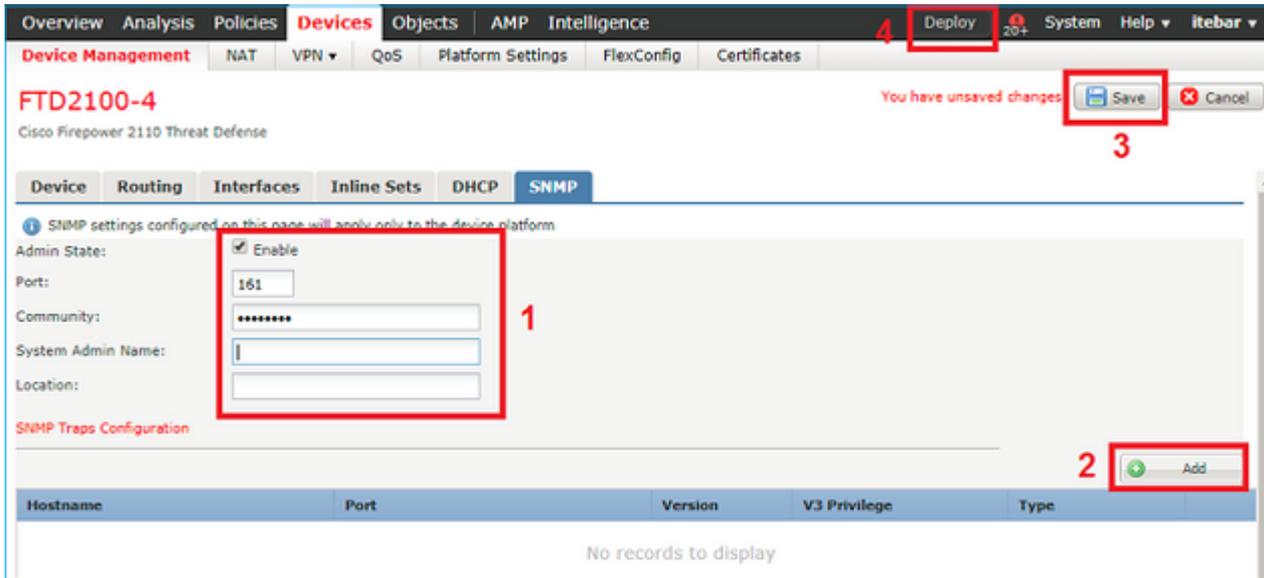
SNMP del chasis (FXOS) en FPR2100



A partir de FTD 6.6+, también tiene la opción de utilizar la interfaz de administración de FTD para el SNMP. En este caso, la información del SNMP en LINA y FXOS se transfiere a través de la interfaz de administración de FTD.

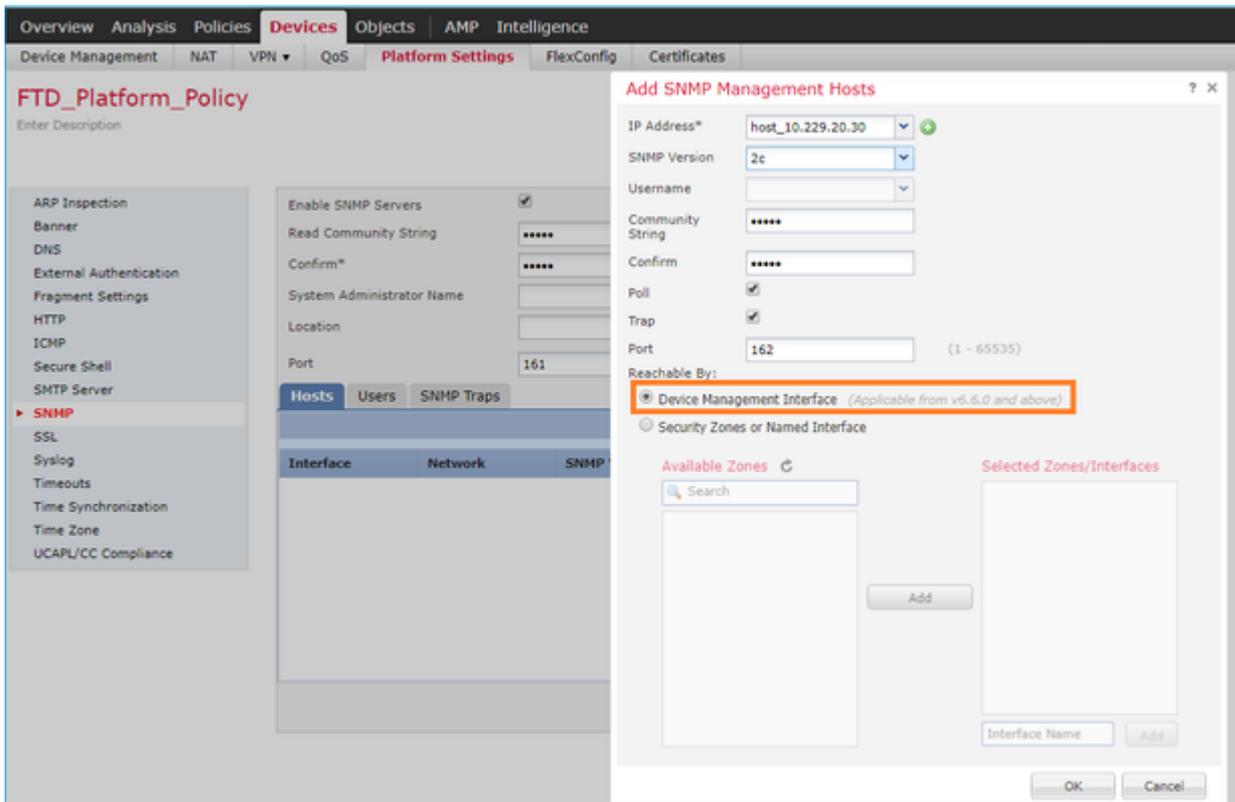
Configuración de SNMPv1/v2c en FXOS

Abra la interfaz de usuario del FMC y vaya a **Dispositivos > Administración de dispositivos**. Seleccione el dispositivo y, luego, SNMP:



Cambio en FTD 6.6+

Puede especificar la interfaz de administración de FTD:



Dado que la interfaz de administración también se puede configurar para el SNMP, la página muestra este mensaje de advertencia:

La configuración SNMP de la plataforma del dispositivo en esta página está inhabilitada, si la configuración SNMP está configurada con la interfaz de administración del dispositivo a través de **Dispositivos > Configuración de la plataforma (Threat Defence) > SNMP > Hosts**.

Configuración de SNMPv3 en FXOS

Abra la interfaz de usuario del FMC y vaya a **Elegir dispositivos > Administración de dispositivos**. Elija el dispositivo y seleccione **SNMP**.

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD2100-4 You have unsaved changes Save Cancel

Cisco Firepower 2110 Threat Defense 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: v

Use AES:

Password*

Confirm:

Privacy Password*

Confirm:

SNMP Trap Configuration ? X

Hostname:* 10.48.26.190 +

Community String:*

Port:* 163 (1 - 65535)

SNMP Version: V3

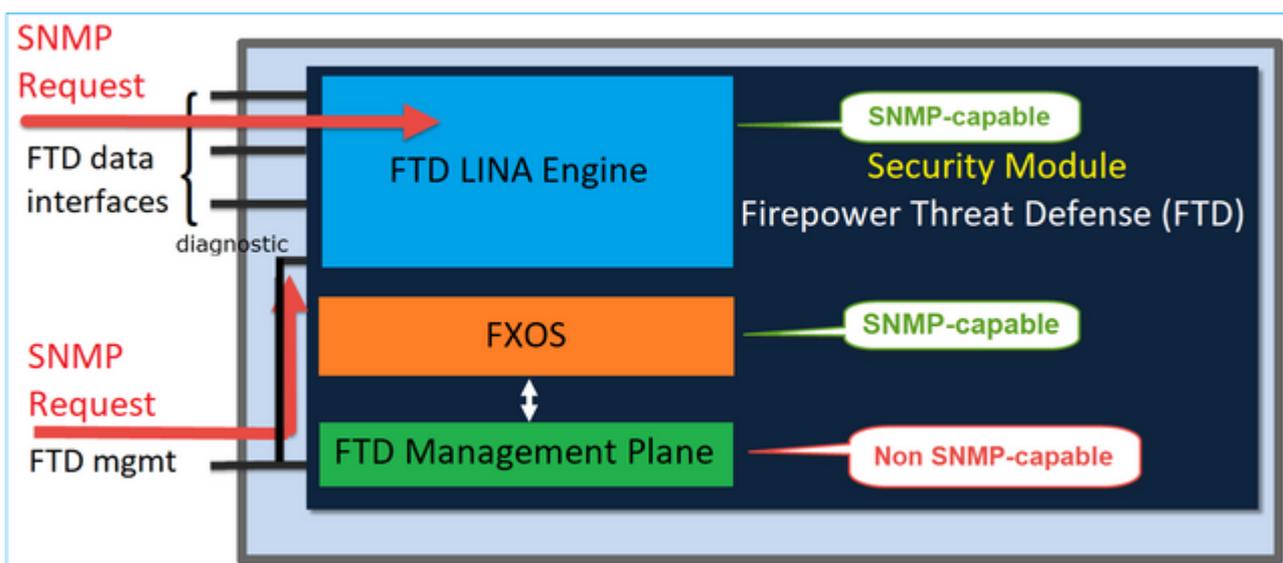
Type: TRAPS

Privilege: PRIV

OK Cancel

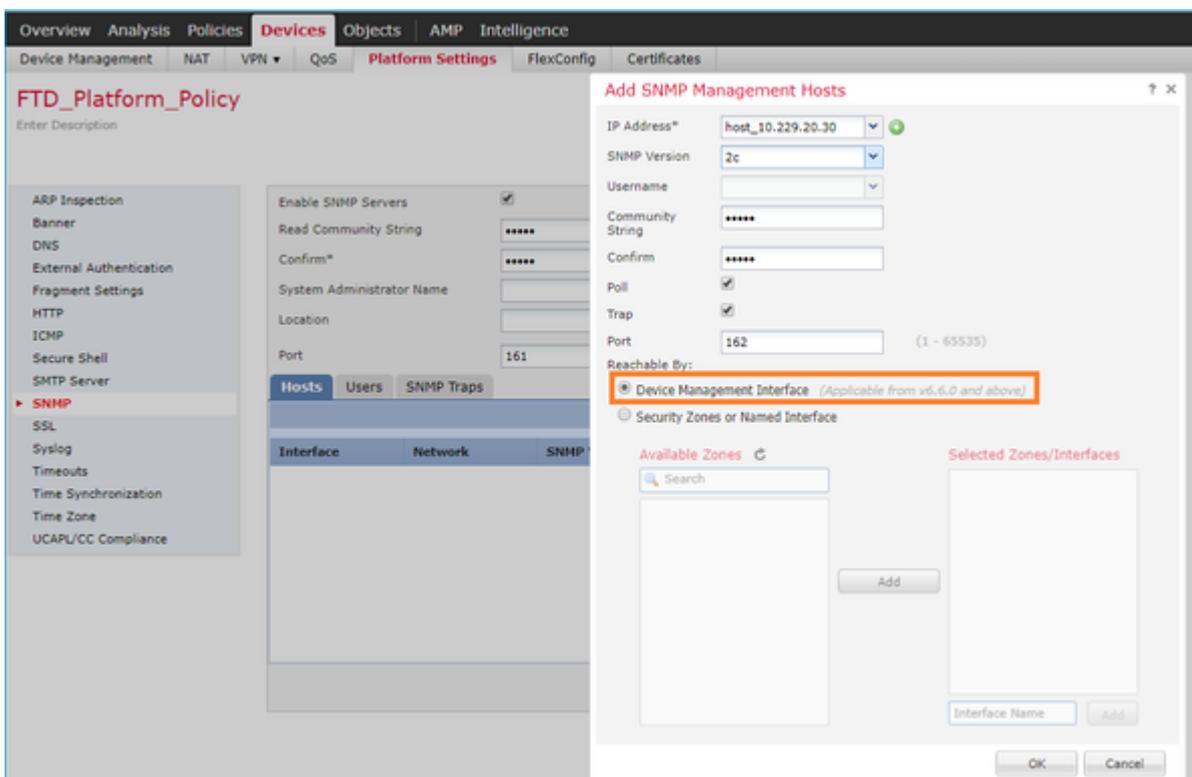
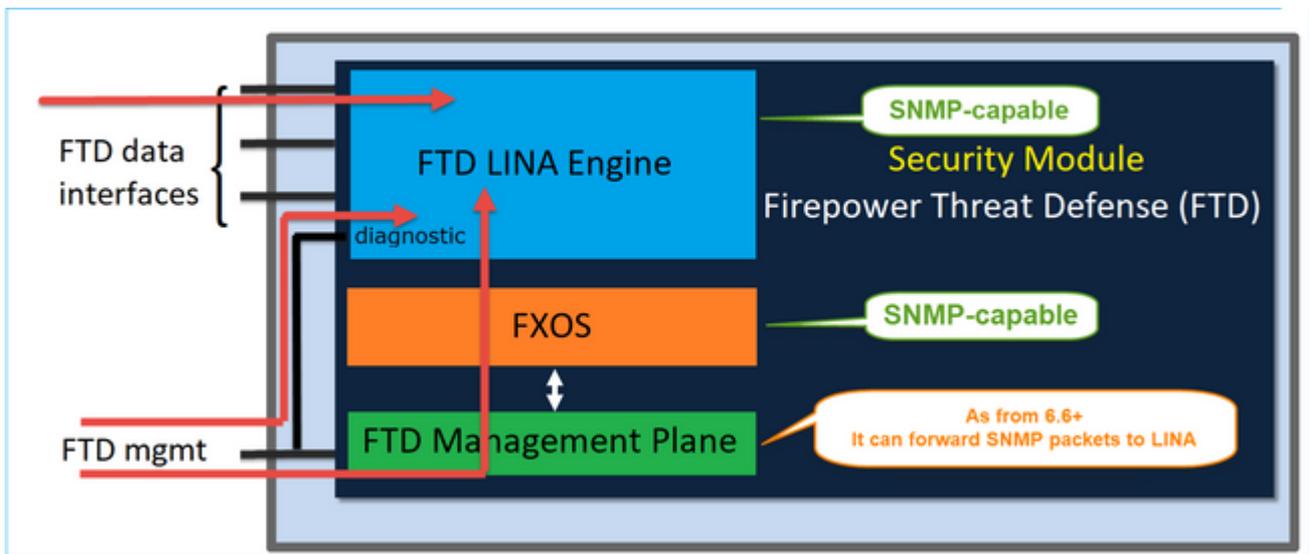
SNMP de FTD (LINA) en FPR2100

- Para las versiones anteriores a 6.6, la configuración del SNMP en LINA de FTD en los dispositivos FTD FP1xxx/FP21xx es idéntica a la de FTD en los dispositivos Firepower 4100 o 9300.



FTD versiones 6.6+

- En las versiones posteriores a 6.6, también tiene la opción de utilizar la interfaz de administración de FTD para sondeos y operaciones de notificación de LINA.



Si se selecciona la nueva interfaz de administración:

- SNMP en LINA disponible sobre la interfaz de administración.
- En **Dispositivos > Administración de dispositivos**, la ficha **SNMP** está deshabilitada porque ya no es necesaria. Se muestra un anuncio de notificación. La ficha del dispositivo del SNMP solo era visible en las plataformas 2100/1100. Esta página no existe en las plataformas FPR9300/FPR4100 y FTD55xx.

Una vez configurada, la información combinada de sondeo/operación de notificación del SNMP en FXOS (en FP1xxx/FP2xxx) + el SNMP en LINA se completa en la interfaz de administración de FTD.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD2100-6
Cisco Firepower 2140 Threat Defense

Device Routing Interfaces Inline Sets DHCP **SNMP**

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

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

Admin State: Enable

Port:

Community:

System Admin Name:

Location:

SNMP Traps Configuration

Hostname	Port	Version	V3 Privilege	Type
No records to display				

La función de administración de IP única del SNMP se admite desde la versión 6.6 en todas las plataformas de FTD:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 que ejecuta FTD
- FTDv

Para obtener más detalles, consulte Configuración del SNMP para Threat Defense

Verificación

Verificación del SNMP en FXOS para FPR4100/FPR9300

Verificaciones de SNMPv2c en FXOS

Verificación de la configuración de la 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          cisco456  V2c     Noauth      Traps
```

Desde el modo 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
```

Verificaciones adicionales:

```
<#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
...
```

Prueba de solicitudes del SNMP.

Realice una solicitud del SNMP de un host válido.

Confirmación de la generación de operaciones de notificación.

Puede utilizar una interfaz intermitente con el analizador EthAnalyzer habilitado para confirmar que se generen operaciones de notificación del SNMP y se envíen a los hosts de operación de notificación definidos:

```
<#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
```

Advertencia: una inestabilidad de la interfaz puede provocar una interrupción del tráfico. Haga esta prueba solo en un entorno de laboratorio o en una ventana de mantenimiento

Verificaciones de SNMPv3 en FXOS

Paso 1. Abra la interfaz de usuario del FCM y vaya a **Configuración de la plataforma > SNMP > Usuario** para ver si hay alguna contraseña o contraseña de privacidad configuradas:

The screenshot shows a configuration window titled "Edit user1". It contains the following fields and values:

- Name: user1
- Auth Type: SHA
- Use AES-128:
- Password: [Redacted] Set:Yes
- Confirm Password: [Redacted]
- Privacy Password: [Redacted] Set:Yes
- Confirm Privacy Password: [Redacted]

At the bottom of the window are "OK" and "Cancel" buttons.

Paso 2. En la CLI, puede verificar la configuración del SNMP en **Supervisión del alcance:**

```
<#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
```

Paso 3. En el modo FXOS, puede expandir la configuración y los detalles del 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
-----
```

Prueba de solicitudes del SNMP.

Puede verificar la configuración y realizar una solicitud del SNMP desde cualquier dispositivo con capacidades del SNMP.

Para comprobar cómo se procesa la solicitud del SNMP, puede utilizar la depuración del SNMP:

<#root>

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

```
  debug snmp pkt-dump
```

```
ksec-fpr9k-1-A(fxos)# 2017 Oct 16 17:11:54.681396 snmpd: 1281064976.000000:iso.10.10.1.1.10.10.10.1 =
2017 Oct 16 17:11:54.681833 snmpd:  SNMPPKTSTRT: 3.000000 161 1281064976.000000 1647446526.000000 0.0000
2017 Oct 16 17:11:54.683952 snmpd: 1281064976.000000:iso.10.10.1.2.10.10.10.2.83886080 = STRING: "mg
2017 Oct 16 17:11:54.684370 snmpd:  SNMPPKTSTRT: 3.000000 162 1281064976.000000 1647446526.000000 0.0000
```

Precaución: una depuración puede afectar al rendimiento del dispositivo.

Verificación del SNMP en FXOS para FPR2100

Verificaciones de SNMPv2 en FXOS

Verifique la configuración mediante la CLI:

<#root>

```
FP2110-4 /monitoring #
```

```
  show snmp
```

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

FP2110-4 /monitoring #

show snmp-trap

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

Confirmación del comportamiento del SNMP.

Puede verificar que pueda sondear FXOS y enviar una solicitud del SNMP desde un host o cualquier dispositivo con capacidades de SNMP.

Utilice el comando **capture-traffic** para ver la solicitud y la respuesta del SNMP:

<#root>

>

capture-traffic

Please choose domain to capture traffic from:

0 - management0

Selection?

0

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options:

udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.

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

listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes

13:50:50.521383 IP 10.48.26.190.42224 > FP2110-4.snmp: C=cisco123 GetNextRequest(29) interfaces.ifTable

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

^C

Caught interrupt signal

Exiting.

2 packets captured

2 packets received by filter

0 packets dropped by kernel

Verificaciones de SNMPv3 en FXOS

Verifique la configuración mediante la 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

Confirmación del comportamiento del SNMP.

Envíe una solicitud del SNMP para verificar que puede sondear FXOS.

Además, puede capturar la solicitud:

<#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
```

Verificación del SNMP en FTD

Para verificar la configuración del SNMP en LINA de FTD:

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

En FTD posterior a 6.6, puede configurar y utilizar la interfaz de administración de FTD para el 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
```

Verificación adicional:

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

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

Desde la CLI del servidor SNMP, ejecute 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 Versio
```

```
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.2313
```

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8350600) 23:11:46.00
```

```
SNMPv2-MIB::sysContact.0 = STRING:
```

```
SNMPv2-MIB::sysName.0 = STRING: Firepower-module1
```

```
SNMPv2-MIB::sysLocation.0 = STRING:
```

```
SNMPv2-MIB::sysServices.0 = INTEGER: 4
```

```
IF-MIB::ifNumber.0 = INTEGER: 10
```

```
IF-MIB::ifIndex.5 = INTEGER: 5
```

```
IF-MIB::ifIndex.6 = INTEGER: 6
```

```
IF-MIB::ifIndex.7 = INTEGER: 7
```

```
IF-MIB::ifIndex.8 = INTEGER: 8
```

```
IF-MIB::ifIndex.9 = INTEGER: 9
```

```
IF-MIB::ifIndex.10 = INTEGER: 10
```

```
IF-MIB::ifIndex.11 = INTEGER: 11
```

```
...
```

Verificación de las estadísticas de tráfico del 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
```

Permiso de tráfico del SNMP a FXOS en FPR4100/FPR9300

La configuración de FXOS en FPR4100/9300 puede restringir el acceso al SNMP por dirección IP de origen. La sección de configuración de la lista de acceso define qué redes/hosts pueden llegar al dispositivo a través de SSH, HTTPS o SNMP. Debe asegurarse de que las consultas del SNMP de su servidor SNMP estén permitidas.

Configuración de la lista de acceso global mediante la GUI

The screenshot shows the 'Platform Settings' tab in the GUI. On the left, a navigation menu includes 'Access List'. The main area displays two tables: 'IPv4 Access List' and 'IPv6 Access List'. Each table has columns for 'IP Address', 'Prefix Length', and 'Protocol'. In the IPv4 table, the entry with IP Address '0.0.0.0', Prefix Length '0', and Protocol 'snmp' is highlighted with a red box. The IPv6 table shows similar entries for 'https', 'snmp', and 'ssh' with IP Address '::'.

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

Configuración de la lista de acceso global mediante la 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
```

Verificación

<#root>

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

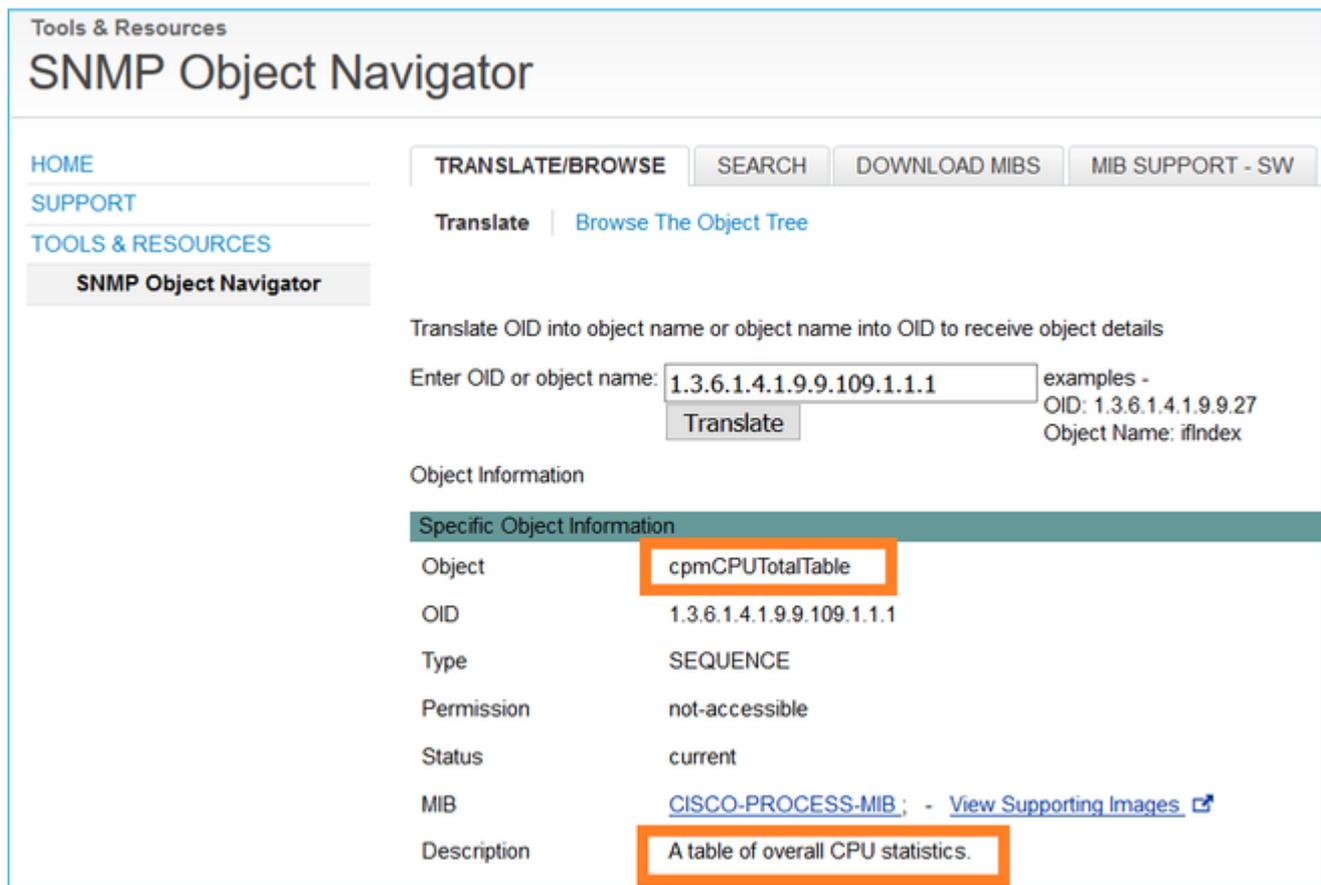
```
show ip-block
```

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

Utilice OID Object Navigator

[Cisco SNMP Object Navigator](#) es una herramienta en línea donde puede traducir los diferentes OID y obtener una breve descripción.



The screenshot shows the Cisco SNMP Object Navigator interface. The main heading is "SNMP Object Navigator". There are navigation tabs: "HOME", "SUPPORT", and "TOOLS & RESOURCES". Under "TOOLS & RESOURCES", "SNMP Object Navigator" is selected. The main content area has a "Translate/Browse" section with a "Translate" button and a "Browse The Object Tree" link. Below this, there is a text input field containing the OID "1.3.6.1.4.1.9.9.109.1.1.1" and a "Translate" button. To the right, there are examples: "examples - OID: 1.3.6.1.4.1.9.9.27" and "Object Name: ifIndex". Below the input field, there is a section for "Object Information" with a sub-section "Specific Object Information". This section contains a table with the following details:

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

Utilice el comando **show snmp-server oid** de la CLI de LINA en FTD para recuperar la lista completa de OID de LINA que se pueden sondear.

<#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#
```

Nota: El comando está oculto.

Troubleshoot

Estos son los generadores de casos de SNMP más comunes vistos por Cisco TAC:

1. No se puede sondear el SNMP de FTD en LINA
2. No se puede sondear el SNMP en FXOS
3. ¿Qué valores de OID del SNMP se deben utilizar?
4. No se pueden obtener operaciones de notificación del SNMP
5. No se puede monitorear el FMC a través del SNMP
6. No se puede configurar el SNMP
7. Configuración del SNMP en el administrador de dispositivos Firepower

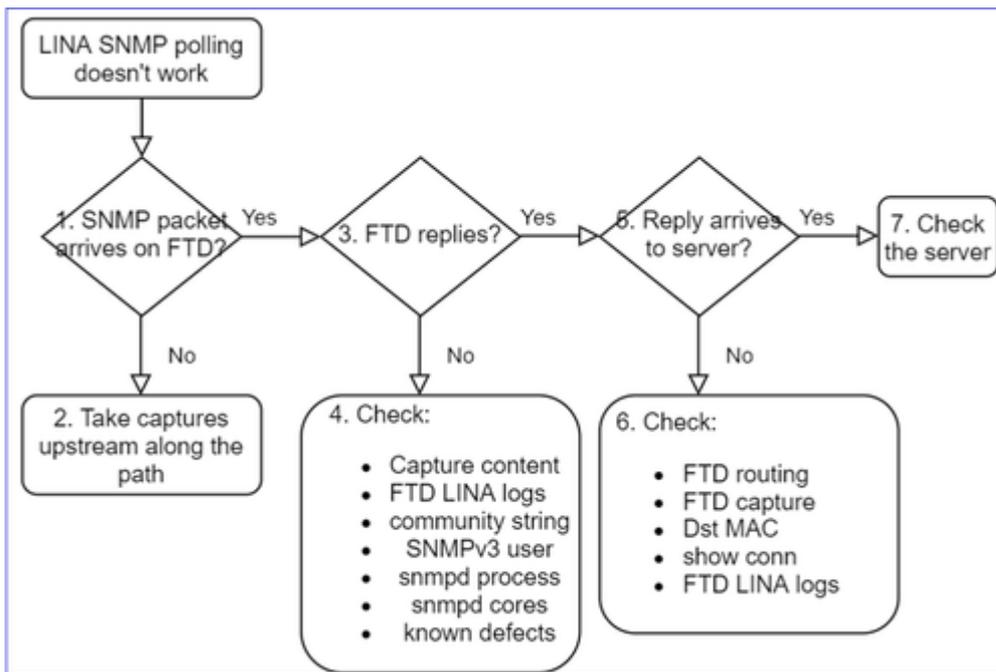
No se puede sondear el SNMP de FTD en LINA

Descripciones del problema (ejemplo de casos reales de Cisco TAC):

- "No se pueden obtener datos a través del SNMP".
- "No se puede sondear el dispositivo mediante SNMPv2".
- "El SNMP no funciona. Queremos monitorear el firewall con el SNMP, pero después de la configuración, nos enfrentamos a problemas".
- "Tenemos dos sistemas de monitoreo que no pueden monitorear FTD a través de SNMPv2c o 3".
- "El recorrido del SNMP no funciona en el firewall".

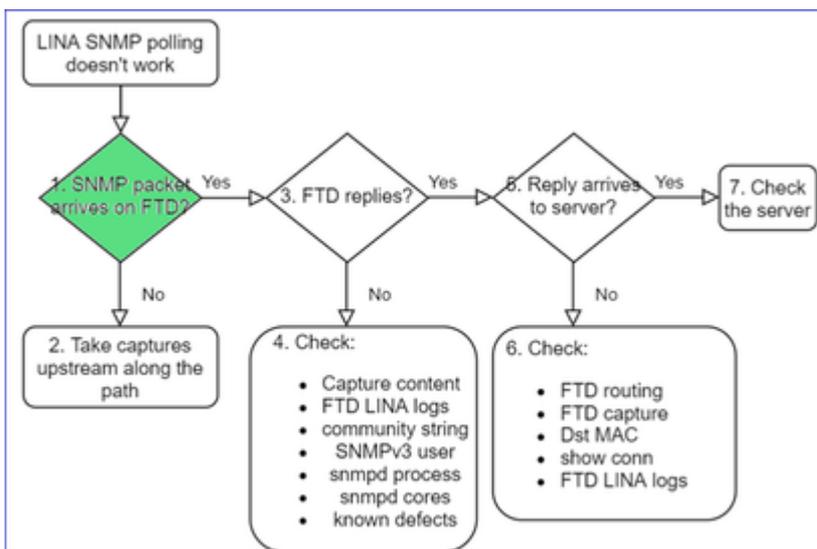
Recomendación sobre cómo solucionar problemas

Este es el proceso recomendado para crear un diagrama de flujo para problemas de sondeo SNMP LINA:



Profundización

1. ¿Llega el paquete SNMP al FTD?



- Active las capturas para verificar la llegada del paquete SNMP.

SNMP en la interfaz de gestión de FTD (posterior a la versión 6.6) utiliza la palabra clave management:

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

El SNMP en las interfaces de datos de FTD utiliza el nombre de la interfaz:

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

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

Captura en la interfaz de administración de FTD:

```
<#root>
>
capture-traffic

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

Captura en la interfaz de datos de FTD:

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

Rastreo de paquetes en la interfaz de datos de FTD (situación funcional: anterior a 6.6/9.14.1):

```
FP1150-1# show capture SNMP packet-number 3 trace

1450 packets captured

  3: 21:10:58.642331      802.1Q vlan#208 P0 192.0.2.100.38478 > 192.0.2.30.161:  udp 39
...
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.0.2.30 using egress ifc identity
...
Result:
input-interface: net208
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
```

The SNMP packet is terminated on identity interface (ASA or LINA)

Rastreo de paquetes en la interfaz de datos de FTD (situación no funcional, posterior a 6.6/9.14.1):

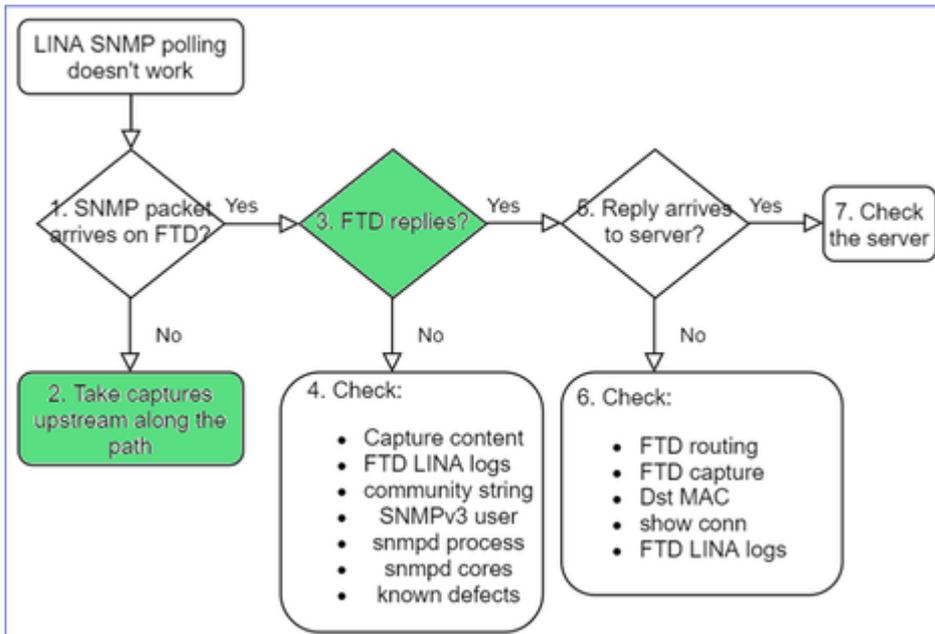
```
firepower# show capture SNMP packet-number 1 trace

  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: 0.000000
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. En caso de que no vea paquetes SNMP en las capturas de ingreso FTD:

- Toma de capturas ascendentes en el camino.
- Asegúrese de que el servidor SNMP utiliza la IP de FTD adecuada.
- Comience desde el puerto de switch que está frente a la interfaz FTD y muévase en sentido ascendente.



3. ¿Ve las respuestas SNMP de FTD?

Para verificar si el FTD responde, marque:

1. Captura de salida de FTD (interfaz de LINA o de administración)

Verifique los paquetes del SNMP con el puerto de origen 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

```

En las versiones posteriores a 6.6/9.14.1, tiene un punto de captura adicional: Capturar en la interfaz de NLP tap. La IP NATed pertenece al rango 162.254.x.x:

```
<#root>
```

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

```
sudo tcpdump -i tap_nlp
```

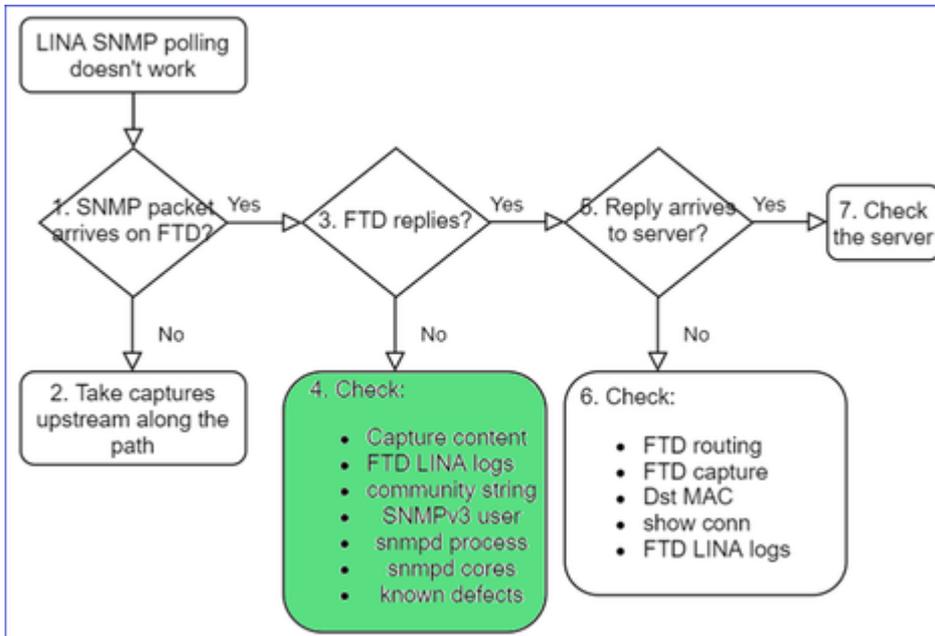
```
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```

16:46:28.372018 IP 192.168.2.100.49008 > 169.254.1.2.snmp: C="Cisc0123" GetNextRequest(28) E:cisco.9.1
16:46:28.372498 IP 192.168.1.2.snmp > 192.168.2.100.49008: C="Cisc0123" GetResponse(35) E:cisco.9.109

```

4. Controles adicionales



a. Para dispositivos Firepower 4100/9300, consulte la [tabla de compatibilidad 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
2.13(0.198)+ Note FXOS 2.13(0.198)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	9.19(x) (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 4145 Firepower 4125 Firepower 4115	9.19(x) (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.15(1) 9.14(x) 9.13(1) 9.12(x)
2.12(0.31)+ Note FXOS 2.12(0.31)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.12(0.31)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 4145 Firepower 4125 Firepower 4115	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.13(1) 9.12(x)
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.18(x) (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x) 9.13(x)
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.12(x) 9.10(x) 9.9(x) 9.8(x)
2.11(1.154)+ Note FXOS 2.11(1.154)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use	Firepower 4112	9.17(x) (recommended) 9.16(x) 9.15(1) 9.14(x)

b. Consulte las estadísticas de snmp-server de LINA en FTD:

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

firepower#
show snmp-server statistics

379 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  351 Number of requested variables    <- SNMP requests in
&#x2013;
360 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  351 Response PDUs                    <- SNMP replies out
  9 Trap PDUs
```

c. Tabla de conexión LINA FTD

Esta comprobación es muy útil en caso de que no vea paquetes en la captura en la interfaz de ingreso FTD. Tenga en cuenta que esta es una verificación válida sólo para SNMP en la interfaz de datos. Si SNMP está en la interfaz de administración (posterior a 6.6/9.14.1), no se crea ninguna conexión.

```
<#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 de LINA en FTD

¡Esto también es una verificación válida solo para el SNMP en la interfaz de datos! Si el SNMP está en la interfaz de administración, no se crea ningún registro:

```
<#root>
firepower#
show log | i 302015.*161
```

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

e. Verifique si FTD descarta los paquetes del SNMP debido a una IP de origen de host incorrecta.

```
firepower# show capture SNMP packet-number 1 trace
 1: 22:33:00.183248      802.1Q vlan#201 P0 192.168.21.100.43860 > 192.168.21.50.161: udp 39
Phase: 1
Type: CAPTURE
...
Phase: 6
Type: ACCESS-LIST
Result: DROP
...
Result:
input-interface: net201(vrfid:0)
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
flow (NA)/NA
```

No UN-NAT phase!

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

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

f. Credenciales incorrectas (comunidad del SNMP)

En el contenido de la captura puede ver los valores de la comunidad (SNMPv1 y 2c):

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
v Simple Network Management Protocol
  version: v2c (1)
  community: cisco123
  data: get-next-request (1)
```

g Configuración incorrecta (por ejemplo, versión del SNMP o cadena de la comunidad)

Existen algunas maneras de verificar la configuración del SNMP del dispositivo y las cadenas de la comunidad:

<#root>

firepower#

more system:running-config | i community

snmp-server host net201 192.168.2.100 community cISC0123 version 2c

Otra forma:

<#root>

```
firepower#
```

```
debug menu netsnmp 4
```

h. Caídas del ASP de LINA/ASA en FTD

Esta es una verificación útil para verificar si FTD descarta los paquetes del SNMP. Primero, borre los contadores (borre la eliminación de ASP) y, luego, pruebe:

```
<#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. Capturas ASP

Las capturas de ASP proporcionan visibilidad de los paquetes descartados (por ejemplo, ACL o adyacencia):

```
<#root>
```

```
firepower#
```

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

Pruebe y, luego, verifique el contenido de la captura:

```
<#root>
```

```
firepower#
```

```
show capture
```

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

j. Núcleo del SNMP (rastreo de origen): modo de verificación 1

Esta comprobación es útil si sospecha que hay problemas de estabilidad del sistema:

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

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

Núcleo del SNMP (rastreo de origen): modo de verificación 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 ve un archivo principal del SNMP, recopile estos elementos y comuníquese con Cisco TAC:

- Archivo TS de FTD (o show tech en ASA)
- Archivos snmpd principales

Depuración del SNMP (estos son comandos ocultos y están disponibles solo en las versiones más recientes):

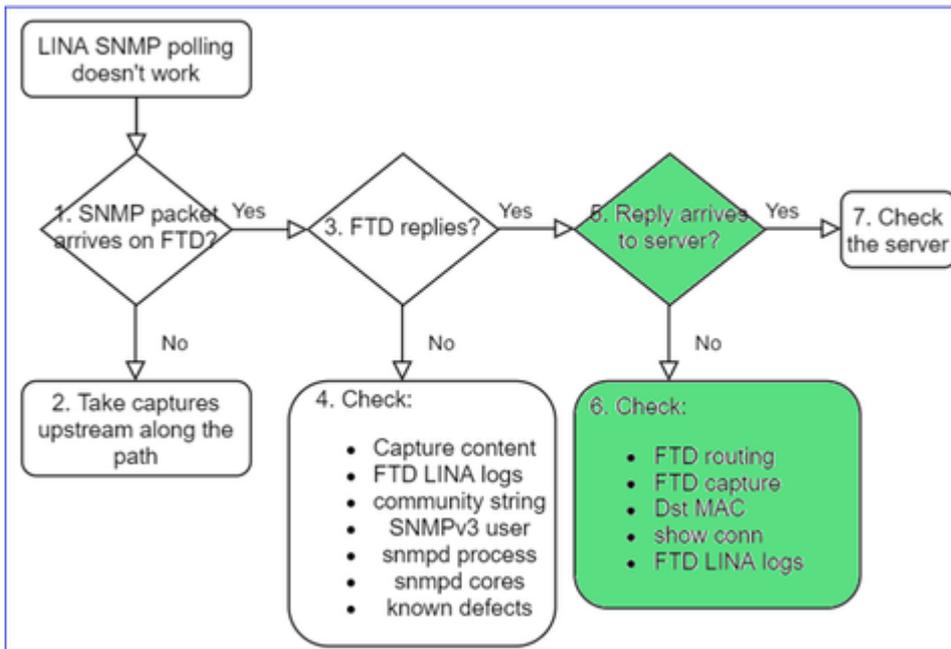
```
<#root>
firepower#
debug snmp trace [255]

firepower#
debug snmp verbose [255]

firepower#
debug snmp error [255]

firepower#
debug snmp packet [255]
```

¿La respuesta del SNMP del firewall llega al servidor?



Si FTD responde pero la respuesta no llega al servidor, verifique:

a. Routing de FTD

Para el routing de la interfaz de administración de FTD:

```

<#root>
>
show network
  
```

Para el routing de la interfaz de datos de LINA de FTD:

```

<#root>
firepower#
show route
  
```

b. Verificación de la MAC de destino

Verificación de la MAC de destino de administración 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: 10.62.148.19

Verificación de la MAC de destino de la interfaz de datos de LINA de FTD:

<#root>

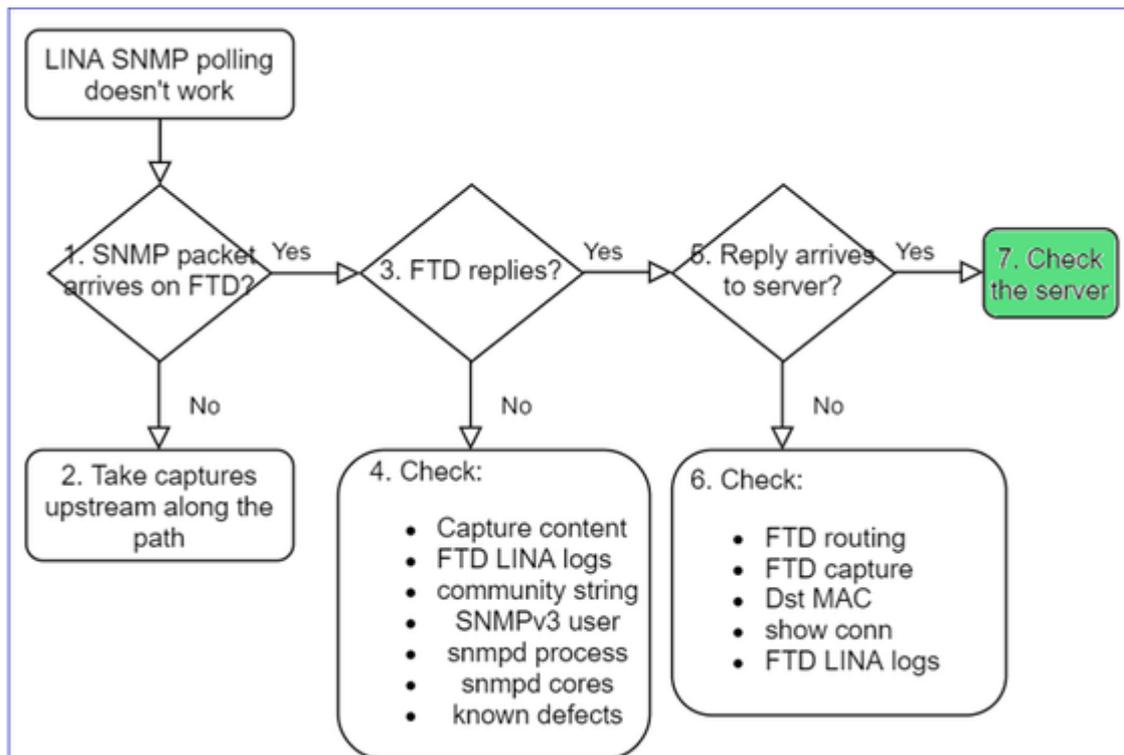
firepower#

show capture SNMP detail

...
6: 01:03:01.391886 a2b8.dc00.0003 0050.5685.3ed2 0x8100 Length: 165
802.1Q vlan#201 P0 192.168.21.50.161 > 192.168.21.100.40687: [udp sum ok] udp 119 (DF) (ttl 64, i

c. Verifique los dispositivos a lo largo de la trayectoria que potencialmente descartan/bloquean los paquetes SNMP.

Verificación del servidor del SNMP



- a. Verifique el contenido de la captura para comprobar la configuración.
- b. Verificación de la configuración del servidor.
- c. Intente modificar el nombre de la comunidad SNMP (por ejemplo, sin caracteres especiales).

Puede utilizar un host final o incluso el FMC para probar el sondeo siempre que se cumplan las 2 condiciones:

1. La conectividad SNMP está en su lugar.
2. La IP de origen puede sondear el dispositivo.

```
<#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
```

Consideraciones de sondeo SNMPv3

- Licencia: SNMPv3 requiere una licencia de cifrado segura. Asegúrese de tener habilitada la funcionalidad de exportación controlada en el portal de Smart Licensing.
- Para solucionar problemas, puede probar con un nuevo usuario/credenciales
- Si se utiliza el cifrado, puede descifrar el tráfico SNMPv3 y comprobar la carga como se describe en: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>
- Considere la posibilidad de cifrar AES128 en caso de que su software se vea afectado por defectos como los siguientes:
- ID de bug de Cisco [CSCvy27283](#)

El sondeo de SNMPv3 de ASA/FTD puede fallar mediante los algoritmos de privacidad AES192/AES256

ID de bug de Cisco [CSCvx45604](#) Snmpv3 walk falla en el usuario con auth sha y priv aes 192

Nota: Si SNMPv3 falla debido a una discordancia del algoritmo, las salidas show y los registros no muestran nada obvio

```

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'

Consideraciones de sondeo de SNMPv3: casos prácticos

1. snmpwalk en SNMPv3: escenario funcional

<#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
```

En la captura (snmpwalk) verá una respuesta para cada paquete:

```

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

```

El archivo de captura no muestra nada inusual:

```

Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  > msgAuthoritativeEngineID: 80000009feca41e36a96147f184553b777
    1... .... = Engine ID Conformance: RFC3411 (SNMPv3)
    Engine Enterprise ID: ciscoSystems (9)
    Engine ID Format: Reserved/Enterprise-specific (254)
    Engine ID Data: ca41e36a96147f184553b777a7127ccb3710888f
  msgAuthoritativeEngineBoots: 6
  msgAuthoritativeEngineTime: 5089
  msgUserName: Cisco123
  > msgAuthenticationParameters: 79ee0d463313558f4529954f
    > [Authentication: OK]
      > [Expert Info (Chat/Checksum): SNMP Authentication OK]
        [SNMP Authentication OK]
        [Severity level: Chat]
        [Group: Checksum]
      msgPrivacyParameters: 714e78d6bc292c88

```

2. snmpwalk en SNMPv3: falla de cifrado

Sugerencia #1: Hay un tiempo de espera:

```
<#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

Sugerencia #2: Hay muchas solicitudes y 1 respuesta:

```

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

Sugerencia #3: fallo de descifrado de 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]
```

Sugerencia n.º 4. Consulte el archivo ma_ctx2000.log para ver si hay mensajes de 'error de análisis de 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
```

El error al analizar ScopedPDU es un indicio fuerte de un error de cifrado. El archivo ma_ctx2000.log muestra eventos sólo para SNMPv3.

3. snmpwalk en SNMPv3: falla de autenticación

Sugerencia #1: fallo de autenticación

```
<#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)
```

Sugerencia #2: Hay muchas solicitudes y muchas respuestas

```
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
```

Sugerencia #3: Paquete malformado de 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]
```

Sugerencia n.º 4. Revise el archivo ma_ctx2000.log para ver si hay mensajes de 'Error de autenticación':

```
<#root>
```

```
>
```

```
expert
```

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

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

```
Authentication failed for Cisco123
```

```
Authentication failed for Cisco123
```

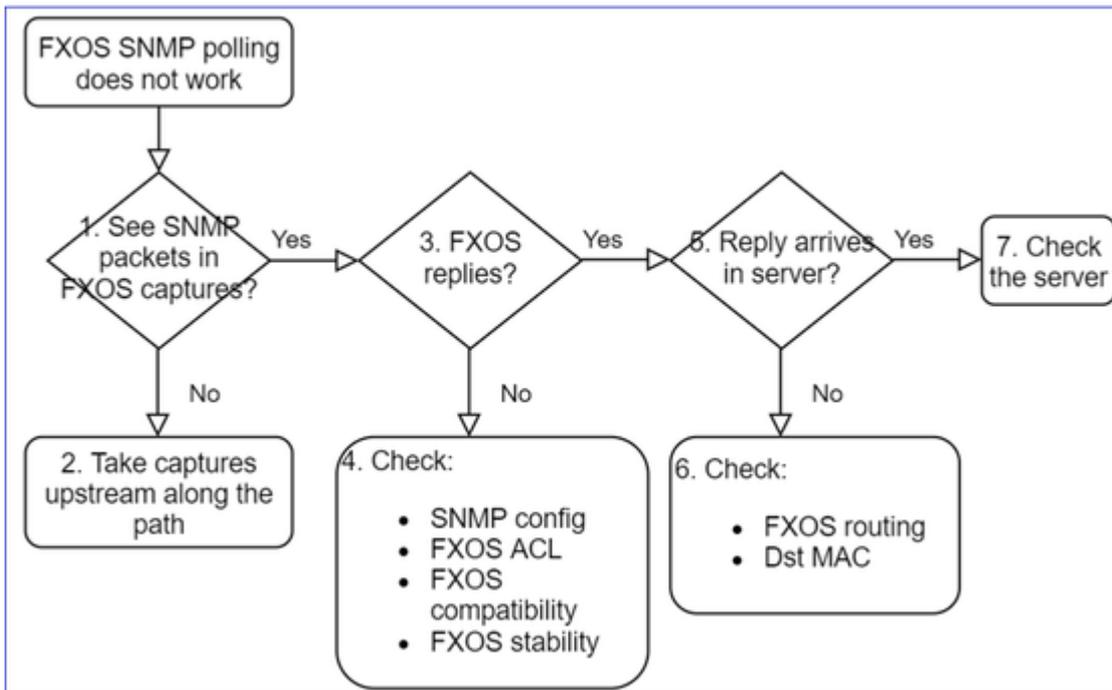
No se puede sondear el SNMP en FXOS

Descripciones del problema (ejemplo de casos reales de Cisco TAC):

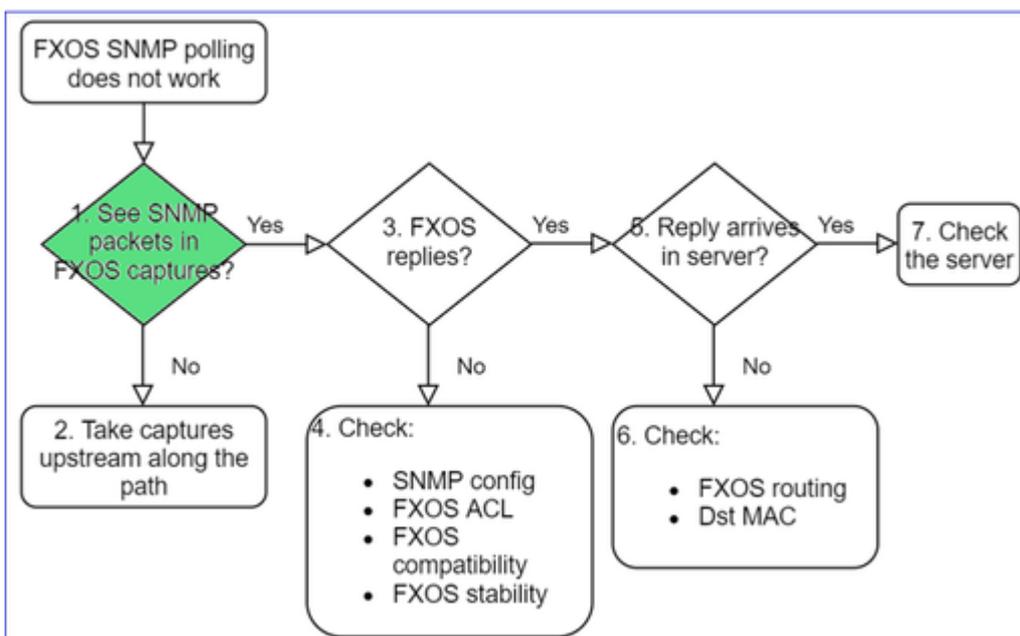
- "El SNMP proporciona una versión incorrecta para FXOS. Al sondear con el SNMP para la versión de FXOS, el resultado es difícil de comprender".
- "No se puede configurar la comunidad snmp en FXOS FTD4115".
- "Después de una actualización de FXOS de 2.8 a 2.9 en el firewall de reserva, tenemos un tiempo de espera cuando intentamos recibir cualquier información a través del SNMP".
- "snmpwalk falla en FXOS 9300, pero funciona en FXOS 4140 en la misma versión. El alcance y la comunidad no son el problema".
- "Queremos agregar 25 servidores SNMP a FXOS FPR4K, pero no podemos".

Solución de problemas recomendada

Este es el proceso para resolver problemas de diagrama de flujo para los problemas de sondeo SNMP de FXOS:



1. ¿Ve los paquetes SNMP en las capturas FXOS?



FPR1xxx/21xx

- En FPR1xxx/21xx no hay ningún administrador de chasis (modo de dispositivo).
- Puede consultar el software FXOS desde la interfaz de gestión.

<#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

- En Firepower 41xx/93xx, utilice la herramienta CLI de Ethalyzer para tomar una captura del chasis:

```
<#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
```

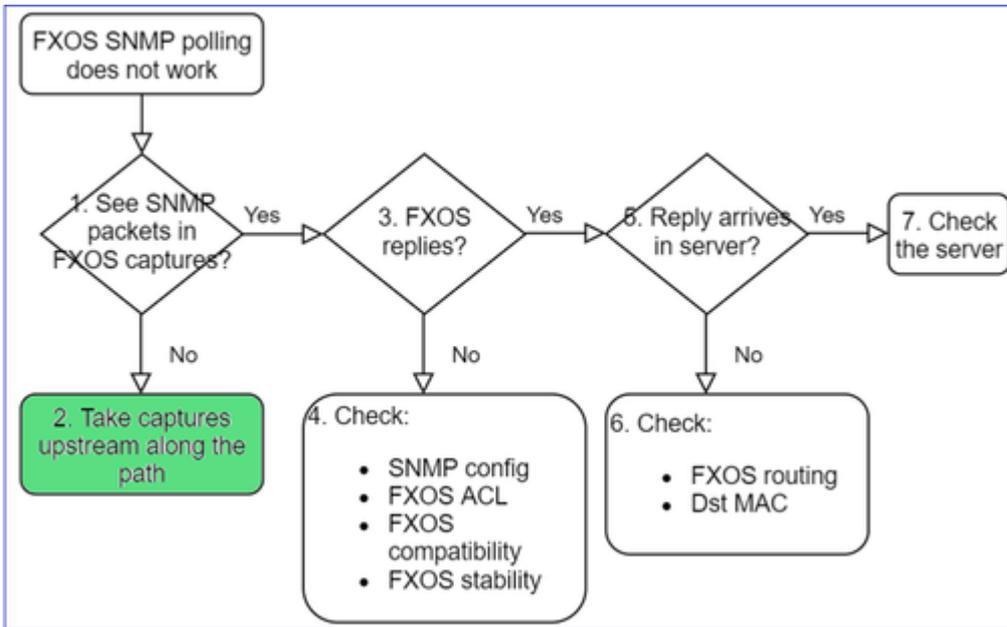
```
1
```

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

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

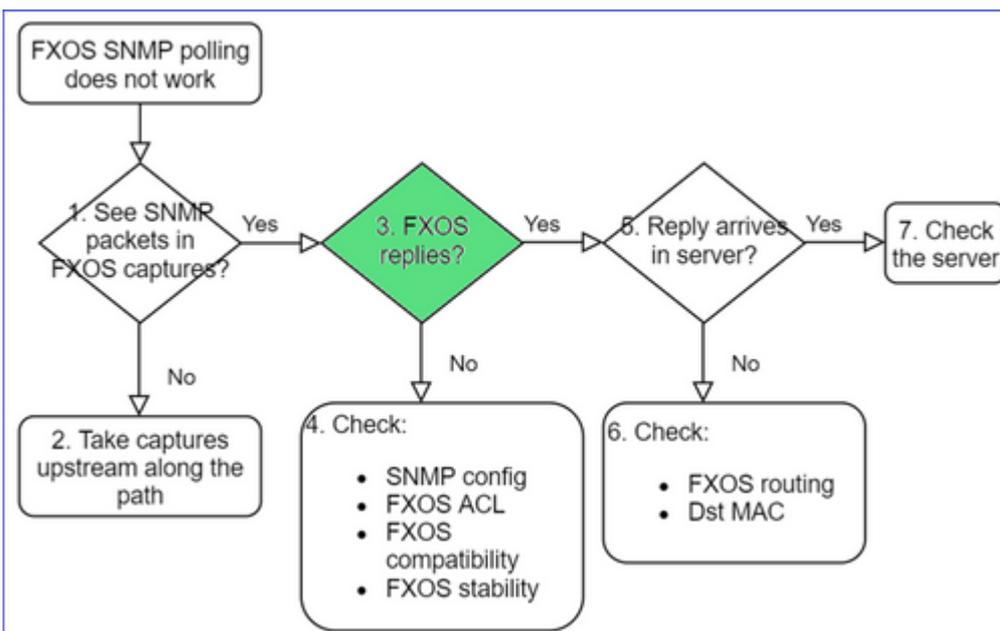
```
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. ¿No hay paquetes en las capturas de FXOS?



- Toma de capturas ascendentes en el camino

3. FXOS respuestas?



- Escenario funcional:

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.

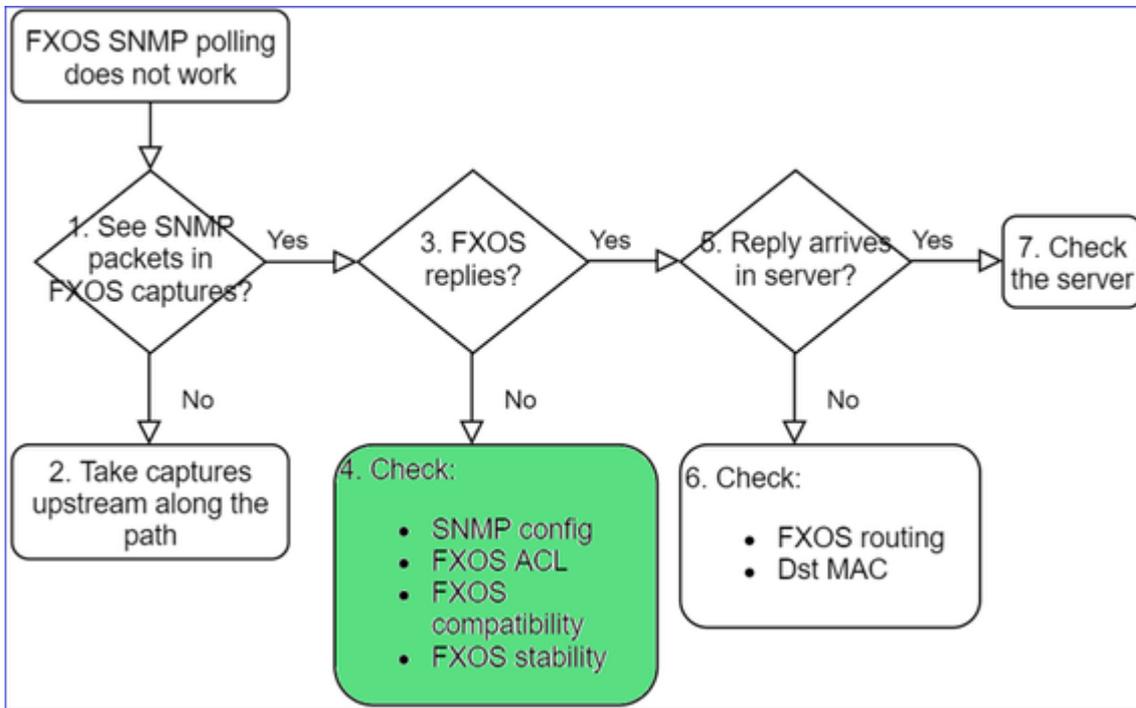
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

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 no responde



Verificaciones adicionales

- Verifique la configuración del SNMP (desde la UI o la CLI):

```
<#root>
```

```
firepower#
```

```
scope monitoring
```

```
firepower /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

- Tenga cuidado con los caracteres especiales (por ejemplo, '\$'):

```
<#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		

- Para SNMPv3, use show snmp-user [detail].
- Verifique la compatibilidad de FXOS.

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

4. En caso de que FXOS no responda

Verifique los contadores del SNMP de FXOS:

```
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
```

Diagram illustrating the output of the `show snmp` command on FXOS, with callouts for specific counters:

- Total requests (polling) (2243 SNMP packets input)
- Bad community requests (v2c) (28 Unknown community name)
- Total replies (3483 SNMP packets output)
- Traps generated (1296 Out Traps PDU)

- Verifique la lista de control de acceso (ACL) de FXOS. Esto solo se aplica a las plataformas FPR41xx/9300.

Si el tráfico es bloqueado por la ACL de FXOS, verá las solicitudes, pero no verá ninguna respuesta:

```
<#root>
```

```
firepower(fxos)#
```

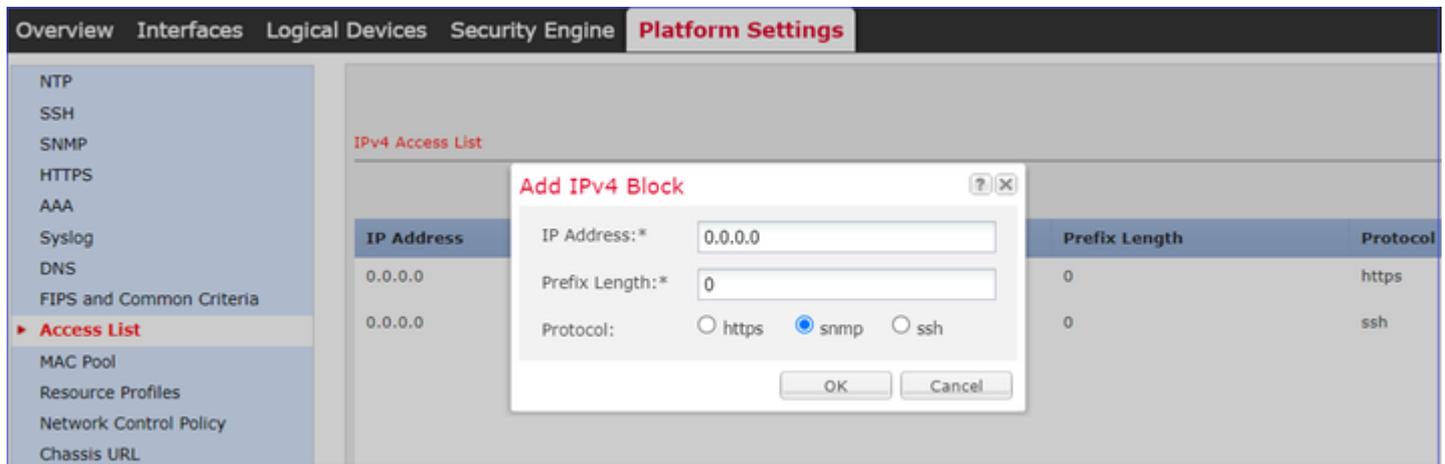
```
ethalyzer local interface mgmt capture-filter
```

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

```
Capturing on 'eth0'
```

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

Puede verificar la ACL de FXOS desde la interfaz de usuario (UI):



También puede verificar la ACL de FXOS desde la 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
```

- Depure el SNMP (solo paquetes). Aplicable solo a 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): este resultado de depuración es muy detallado.

```
<#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
```

- Verifique si hay alguna falla de FXOS relacionada con el 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
```

- Verifique si hay algún núcleo snmpd:

```
En 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
```

En FPR1xxx/21xx:

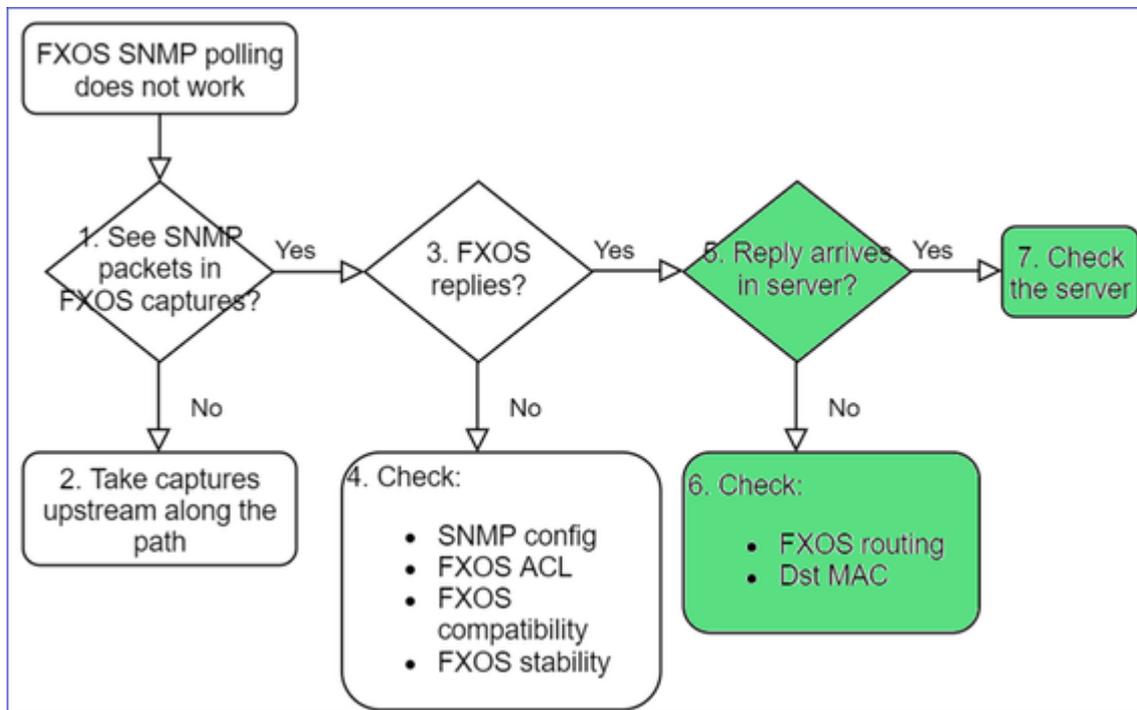
```
<#root>
```

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

```
dir cores_fxos
```

Si ve algún núcleo snmpd, recopile los núcleos junto con el paquete de solución de problemas de FXOS y comuníquese con Cisco TAC.

5. ¿Llega la respuesta SNMP al servidor SNMP?



- Verifique el routing de FXOS.

Este resultado pertenece a FPR41xx/9300:

```
<#root>
```

```
firepower#
```

```
show fabric-interconnect
```

```
Fabric Interconnect:
```

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

- Tome una captura, exporte el PCAP y verifique la MAC de destino de la respuesta.
- Por último, verifique el servidor SNMP (capturas, configuración, aplicación, etc.).

¿Qué valores de OID del SNMP se deben utilizar?

Descripciones del problema (ejemplo de casos reales de Cisco TAC):

- "Queremos monitorear el equipo Cisco Firepower. Necesitamos los OID de SNMP para cada CPU principal, memoria, disco".
- "¿Hay algún OID que pueda utilizarse para monitorear el estado de la fuente de alimentación en el ASA 5555?"
- "Queremos obtener el OID de SNMP del chasis en FPR 2K y FPR 4K".
- "Queremos sondear la memoria caché del ARP del ASA".
- "Necesitamos conocer el OID de SNMP cuando se cae la conexión del BGP".

Cómo encontrar los valores de OID de SNMP

Estos documentos proporcionan información sobre los OID de SNMP en los dispositivos Firepower:

- Informe técnico de monitoreo del SNMP de Cisco Firepower Threat Defense (FTD):

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

- Guía de referencia de la MIB de Cisco Firepower FXOS 4100/9300:

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

- Cómo buscar un OID específico en las plataformas 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>

- Verificación de los OID de SNMP desde la 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
```

- Para obtener más información sobre los OID, consulte SNMP Object Navigator.

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

- En FXOS (41xx/9300), ejecute estos 2 comandos desde la CLI de FXOS:

```
<#root>
```

```
FP4145-1#
```

```
connect fxos
```

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

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

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

```
show snmp internal oids supported
```

```
- SNMP All supported MIB OIDs -0x11a72920
Subtrees for Context:
ccitt
1
1.0.88010.1.1.1.1.1.1.1 ieee8021paeMIB
1.0.88010.1.1.1.1.1.1.2
...
```

Referencia rápida de OID comunes

Requisito	OID (ID del objeto)
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)
Memoria (LINA)	1.3.6.1.4.1.9.9.221.1.1
Memoria (Linux/FMC)	1.3.6.1.1.4.1.2021.4
Información de HA	1.3.6.1.4.1.9.9.491.1.4.2
Información del clúster	1.3.6.1.4.1.9.9.491.1.8.1

Información de VPN	<p>Sesiones núm. RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.1 (7.x)</p> <p>Número de usuarios de RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.3 (7.x)</p> <p>Sesiones pico núm. RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.41 (7.x)</p> <p>Sesiones de número de VPN S2S: 1.3.6.1.4.1.9.9.392.1.3.29</p> <p>Sesiones pico de número de VPN S2S: 1.3.6.1.4.1.9.9.392.1.3.31</p> <p>- Sugerencia: firepower# show snmp-server oid i ike</p>
Estado de BGP	<p>ENH ID de bug de Cisco CSCux13512 :Adición de la MIB del BGP para sondeo del SNMP</p>
Smart Licensing FPR1K/2K ASA/ASA v	<p>ENH ID de bug de Cisco CSCvv83590 : ASA v/ASA en FPR1k/2k: Se necesita SNMP OID para realizar un seguimiento del estado de las licencias inteligentes</p>
OID del SNMP en LINA para el canal de puertos a nivel de FXOS	<p>ENH ID de bug de Cisco CSCvu91544 :Compatibilidad con el OID del SNMP de LINA para estadísticas de interfaz de canal de puertos a nivel de FXOS</p>

FMC 7.3 Adiciones (para FMC 1600/2600/4600 y posteriores)

Requisito	OID (ID del objeto)
Captura de estado de ventilador	<p>OID de trampa: 1.3.6.1.4.1.9.9.117.2.0.6</p> <p>Valor OID: 1.3.6.1.4.1.9.9.117.1.4.1.1.1.<index></p> <p>0 - el ventilador no funciona</p> <p>1 - el ventilador está funcionando</p>
Captura de temperatura de CPU/PSU	<p>OID de trampa: 1.3.6.1.4.1.9.9.91.2.0.1</p> <p>Umbral OID: 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<index>.1</p> <p>Valor OID: 1.3.6.1.4.1.9.9.91.1.1.1.1.4.<index></p>
Trampa de estado de PSU	<p>OID de trampa: 1.3.6.1.4.1.9.9.117.2.0.2</p> <p>OperStatus OID: 1.3.6.1.4.1.9.9.117.1.1.2.1.2.<index></p> <p>AdminStatus OID: 1.3.6.1.4.1.9.9.117.1.1.2.1.1.<index></p>

	<p>0 - presencia de fuente de alimentación no detectada</p> <p>1 - presencia de la fuente de alimentación detectada, correcto</p>
--	---

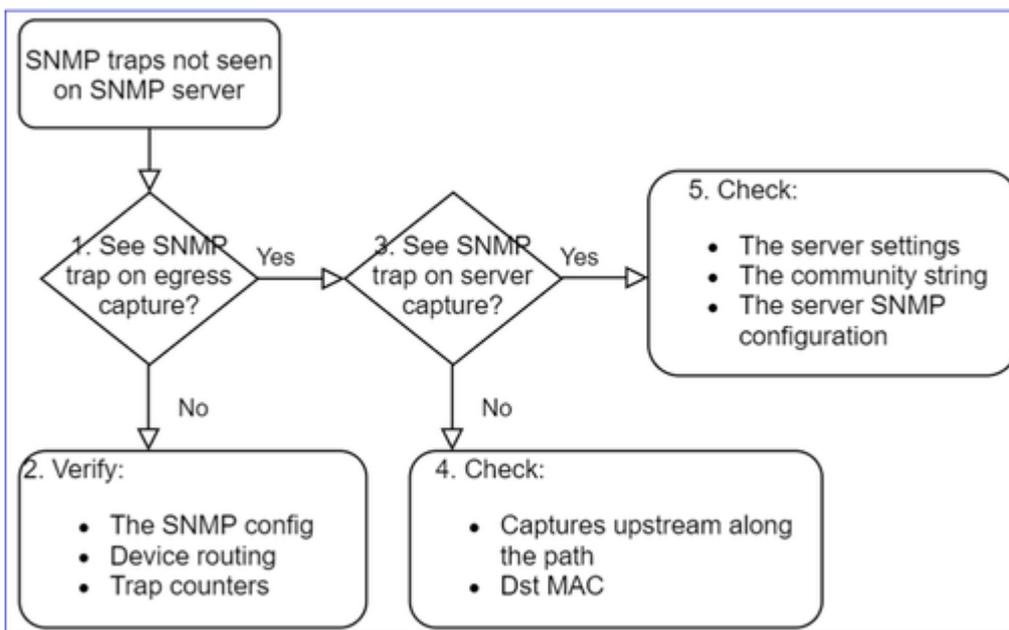
No se pueden obtener operaciones de notificación del SNMP

Descripciones del problema (ejemplo de casos reales de Cisco TAC):

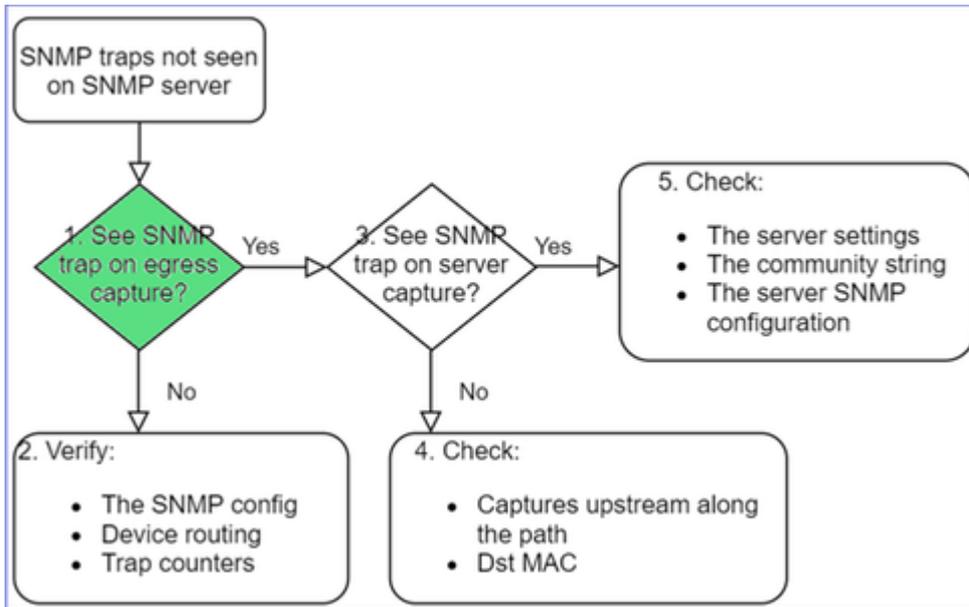
- "SNMPv3 de FTD no envía ninguna operación de notificación al servidor SNMP".
- "El FMC y FTD no envían mensajes de operación de notificación al SNMP".
- "Hemos configurado el SNMP en FTD 4100 para FXOS y hemos probado SNMPv3 y SNMPv2, pero ninguno puede enviar operaciones de notificación".
- "El SNMP de Firepower no envía operaciones de notificación a la herramienta de monitoreo".
- "El firewall de FTD no envía operaciones de notificación del SNMP al NMS".
- "Las operaciones de notificación del servidor SNMP no funcionan".
- "Hemos configurado el SNMP en FTD 4100 para FXOS y hemos probado SNMPv3 y SNMPv2, pero ninguno puede enviar operaciones de notificación".

Solución de problemas recomendada

Este es el proceso para resolver problemas de diagrama de flujo para problemas de trampa SNMP de Firepower:



1. ¿Ve las trampas SNMP en la captura de salida?



Para capturar las operaciones de notificación de LINA/ASA en la interfaz de administración:

```

<#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

```

Para capturar las operaciones de notificación de LINA/ASA en la interfaz de datos:

```

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

```

Para capturar las operaciones de notificación de FXOS (41xx/9300):

```

<#root>
firepower#
connect fxos

```

```

firepower(fxos)#
ethanalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 500 write workspace

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

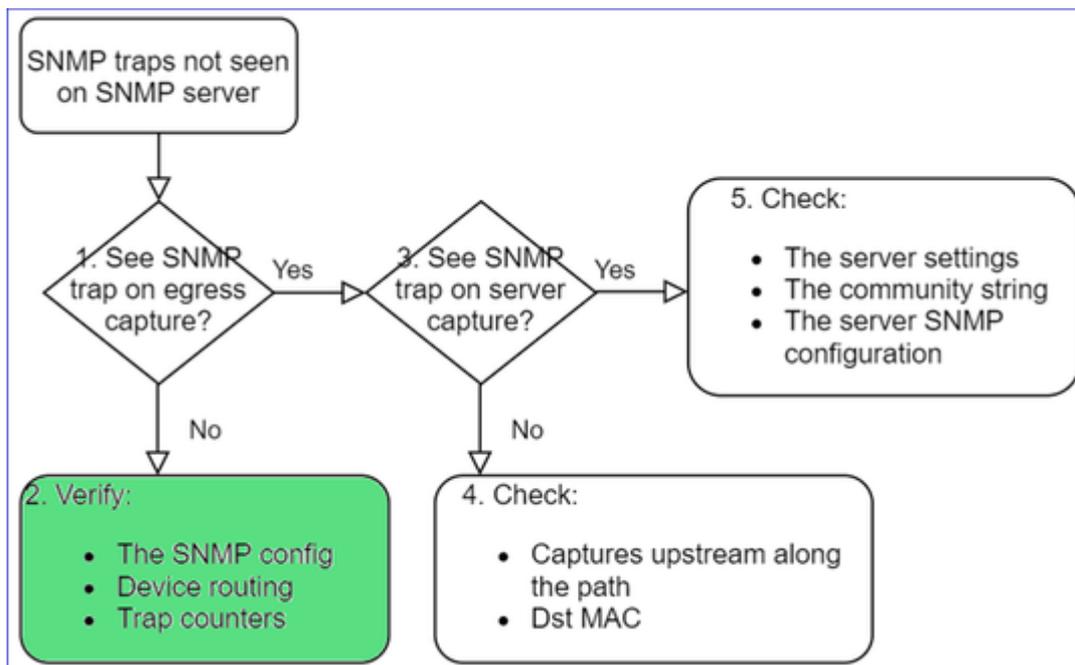
firepower#
connect local-mgmt

firepower(local-mgmt)#
dir

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

```

2. Si no ve los paquetes en la interfaz de salida



<#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

```

Configuración de operaciones de notificación del SNMP en FXOS:

```
<#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

Nota: En 1xxx/21xx verá esta configuración sólo en el caso de **Devices > Device Management > SNMP** config.

- Routing de LINA/ASA para operaciones de notificación a través de la interfaz de administración:

```
<#root>
```

```
>
```

```
show network
```

- Routing de LINA/ASA para operaciones de notificación a través de la interfaz de datos:

```
<#root>
```

```
firepower#
```

```
show route
```

- Routing de FXOS (41xx/9300):

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- Contadores de operaciones de notificación (LINA/ASA):

```
<#root>
```

firepower#

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

20 Trap PDUs

Y FXOS:

<#root>

FP4145-1#

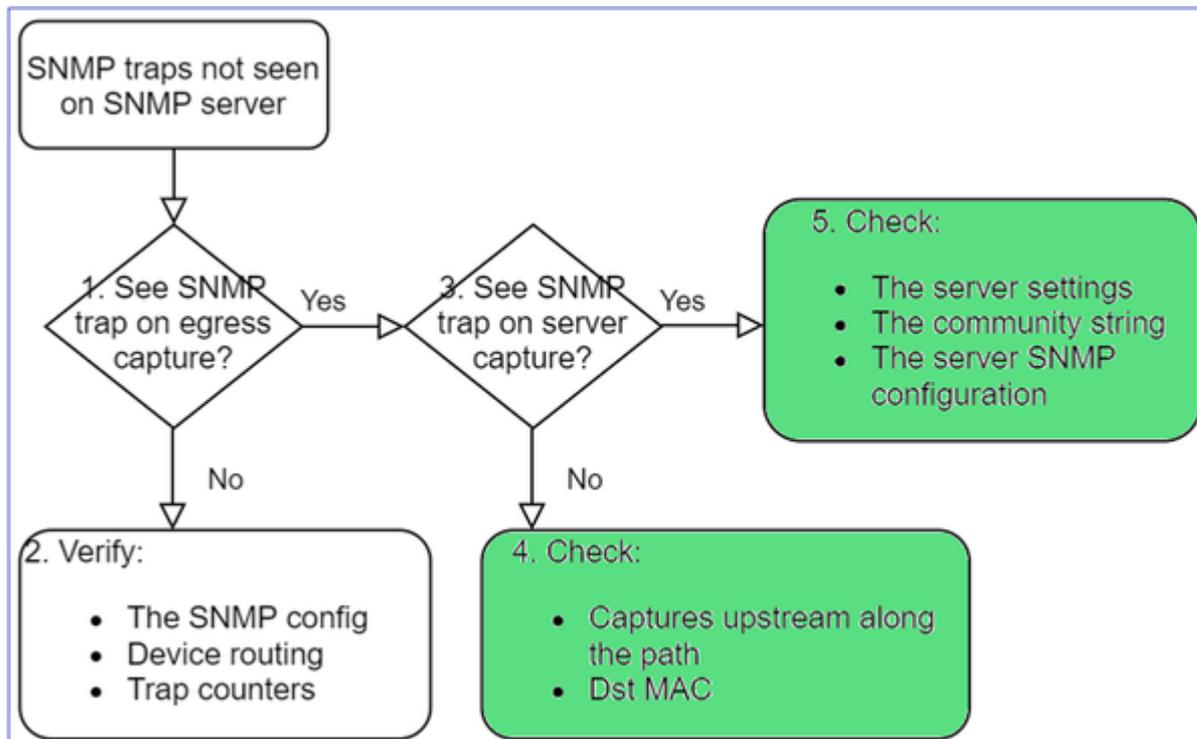
```
connect fxos
```

FP4145-1(fxos)#

```
show snmp | grep Trap
```

1296 Out Traps PDU

Verificaciones adicionales



- Captura del servidor SNMP de destino.

Otras cosas para verificar:

- Capturas a lo largo del camino.
- Dirección MAC de destino de todos los paquetes de operaciones de notificación del SNMP.
- Configuración y estado del servidor SNMP (por ejemplo, firewall, puertos abiertos, etc.).
- Cadena de la comunidad de SNMP.

- Configuración del servidor SNMP.

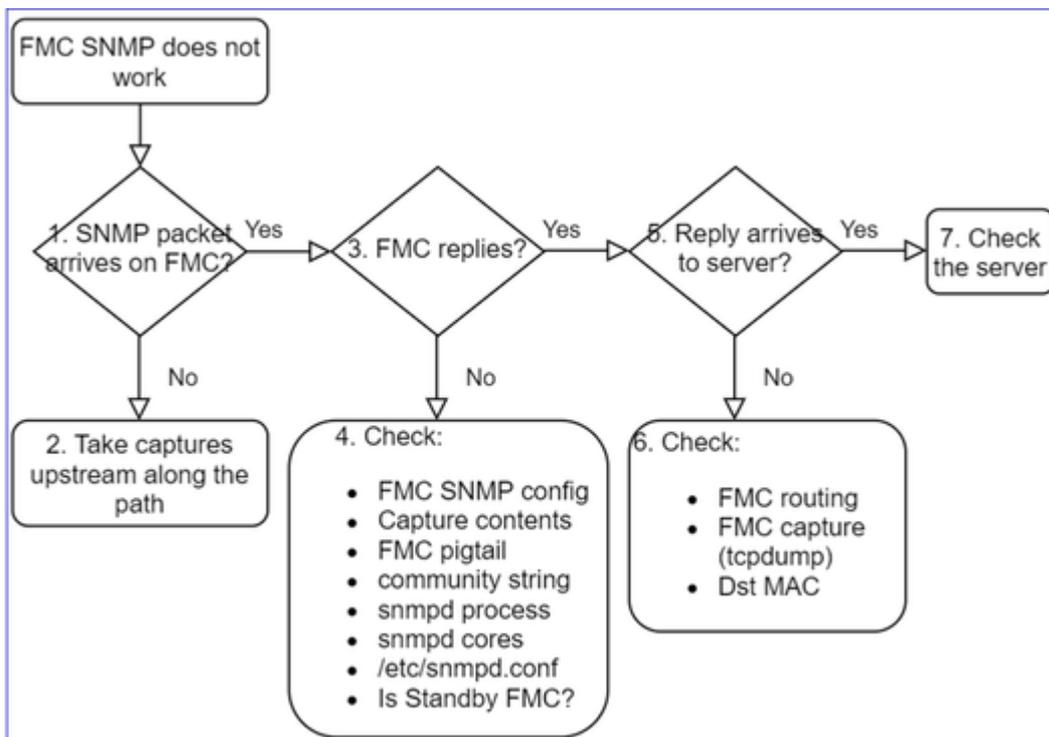
No se puede monitorear el FMC a través del SNMP

Descripciones del problema (ejemplo de casos reales de Cisco TAC):

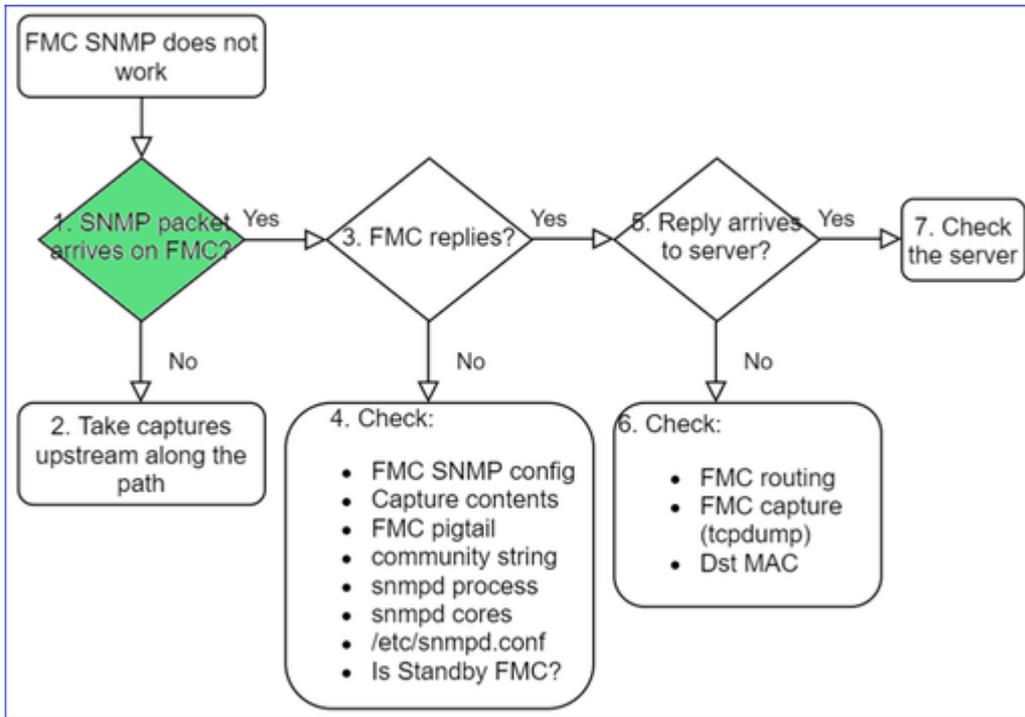
- "El SNMP no funciona en el FMC de reserva".
- "Necesito monitorear la memoria del FMC".
- "¿Debería funcionar el SNMP en el FMC de reserva 192.168.4.0.8?"
- "Tenemos que configurar los CSP para supervisar sus recursos, como la CPU, la memoria, etc.".

Cómo solucionar problemas

Este es el proceso para resolver los problemas de FMC SNMP en el diagrama de flujo:



1. ¿Llega el paquete SNMP al FMC?



- Capture en la interfaz de administración del 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.
```

Sugerencia: guarde la captura en el directorio FMC /var/common/ y descárguela de la interfaz de usuario de FMC

<#root>

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

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

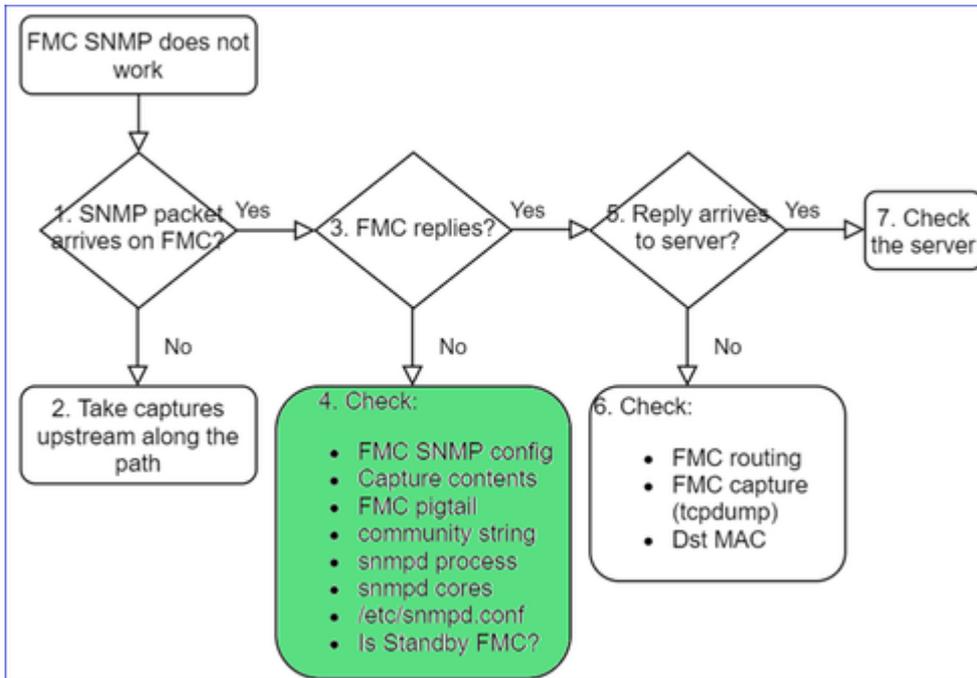
```
HS_PACKET_BUFFER_SIZE is set to 4.
```

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

```
^C46 packets captured
```

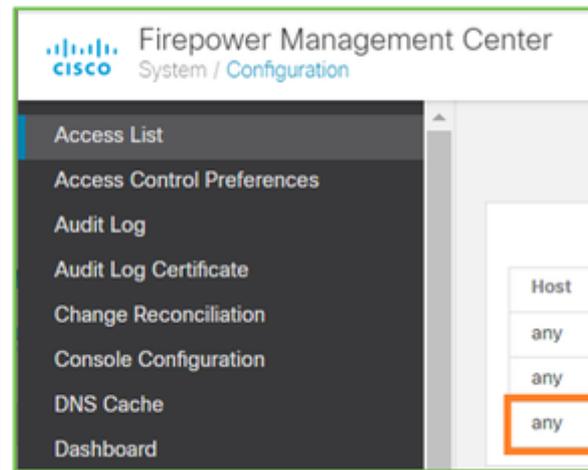
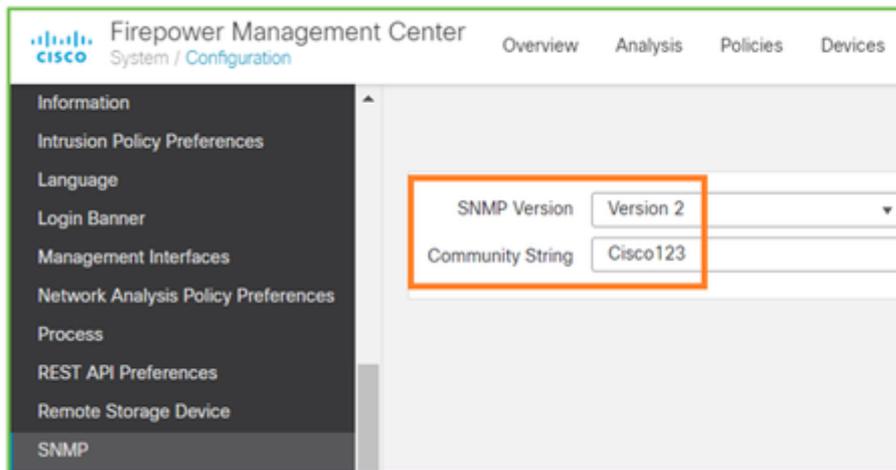
```
46 packets received by filter
```

¿Responde el FMC?



Si el FMC no responde, verifique:

- La configuración del SNMP en el FMC (Sistema > Configuración)
 1. La sección SNMP
 2. La sección Lista de acceso



Si el FMC no responde, verifique:

- El contenido (PCAP) de la captura
- La cadena de la comunidad (esto se puede ver en las capturas)
- El resultado del espiral del FMC (busque errores, fallas, seguimientos) y el contenido de /var/log/snmpd.log
- Proceso 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
```

- Núcleos 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
```

- Archivo de configuración del backend en /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
```

Nota: Si SNMP está inhabilitado, el archivo snmpd.conf no existe

- ¿Es un FMC de reserva?

En versiones anteriores a 6.4.0-9 y 6.6.0, el FMC de reserva no envía datos del SNMP (snmpd está en estado de espera). Debe ocurrir lo siguiente. Verifique la mejora de la ID de error de Cisco [CSCvs32303](#)

No se puede configurar el SNMP

Descripciones del problema (ejemplo de casos reales de Cisco TAC):

- "Queremos configurar el SNMP para el centro de administración Firepower de Cisco y Firepower Threat Defense 4115".
- "Compatibilidad con configuración SNMP en FTD".
- "Queremos habilitar el monitoreo del SNMP en mi dispositivo FTD".
- "Intentamos configurar el servicio del SNMP en FXOS, pero el sistema no nos permite confirmar el búfer al final. Dice Error: No se permiten cambios. use 'Conectar ftd' para realizar cambios."
- "Queremos habilitar el monitoreo del SNMP en nuestro dispositivo FTD".
- "No se puede configurar el SNMP en FTD ni detectar el dispositivo en monitoreo".

Cómo abordar los problemas de configuración del SNMP

Lo primero es lo primero: ¡Documentación!

- Lea el presente documento.
- Guía de configuración del FMC:

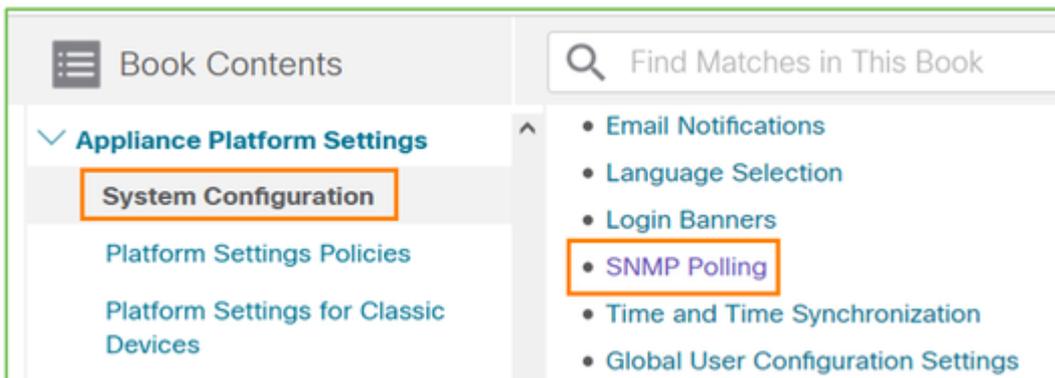
<https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html>

- Guía de configuración de FXOS:

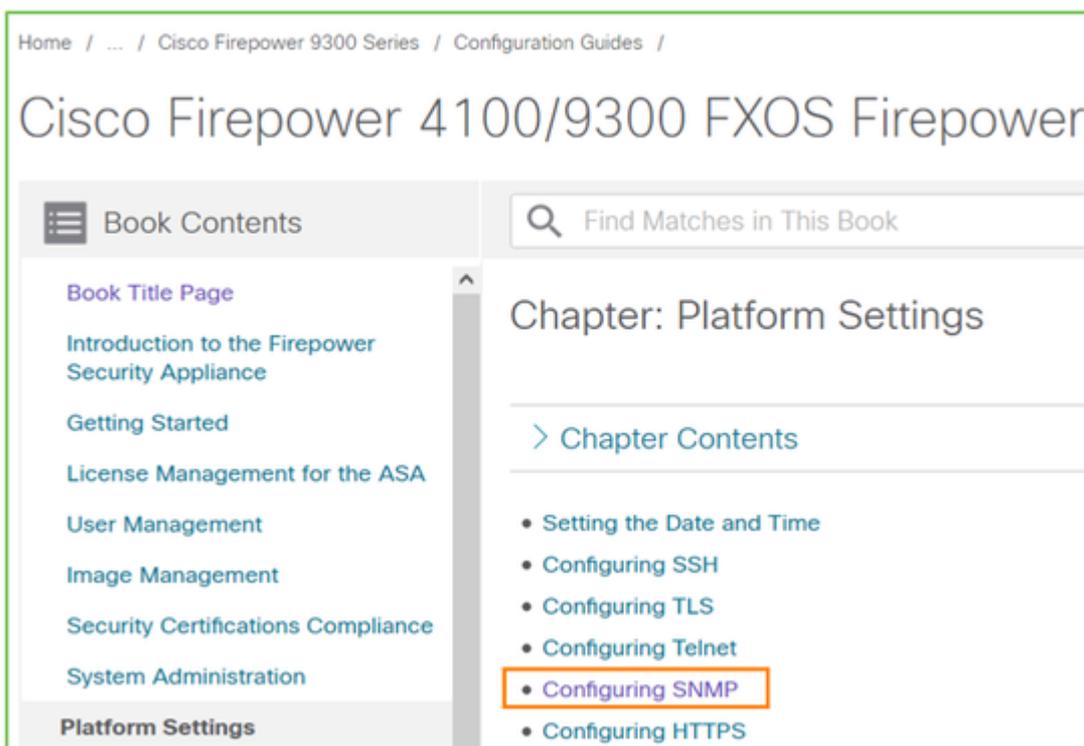
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB115F5

¡Tenga en cuenta los diversos documentos del SNMP!

SNMP del FMC:



SNMP de FXOS:



Configuración del SNMP de Firepower 41xx/9300:



Configuración del SNMP de Firepower 1xxx/21xx:



Configuración del SNMP en el administrador de dispositivos Firepower (FDM)

Descripciones del problema (ejemplo de casos reales de Cisco TAC):

- "Necesitamos orientación sobre SNMPv3 en el dispositivo Firepower con el FDM".
- "La configuración del SNMP no funciona en el dispositivo FPR 2100 del FDM".
- "No podemos lograr que la configuración de SNMPv3 funcione en el FDM".
- "Necesitamos asistencia de configuración del SNMP en el FDM 6.7".
- "Queremos habilitar SNMPv3 en el FDM".

Cómo abordar los problemas de configuración del FDM del SNMP

- Para la versión anterior a 6.7, puede hacer la configuración del SNMP con FlexConfig:

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

- A partir de la versión 6.7 de Firepower, la configuración del SNMP ya no se realiza con FlexConfig, sino con la API de REST:

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

Hojas de referencia de solución de problemas del SNMP

1xxx/21xx/41xx/9300 (LINA/ASA): qué debe recopilar antes de abrir un caso con Cisco TAC

Comando	Descripción
---------	-------------

firepower# show run snmp-server	Verifique la configuración SNMP de ASA/FTD LINA.
firepower# show snmp-server statistics	Verifique las estadísticas del SNMP del ASA/LINA en FTD. Concéntrese en los contadores de entrada y salida de paquetes del SNMP.
> capture-traffic	Capturar tráfico en la interfaz de gestión.
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	Capture el tráfico en la interfaz de datos (nombre si es net201) para UDP 161 (sondeo SNMP).
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	Capturar tráfico en la interfaz de datos (nombre si es net208) para UDP 162. (Capturas SNMP).
firepower# show capture SNMP-POLL packet-number 1 trace	Rastrear un paquete SNMP de ingreso que llega a la interfaz de datos LINA de ASA/FTD.
admin@firepower:~\$ sudo tcpdump -i tap_nlp	Capturar en la interfaz de toque interna de NLP (proceso no lineal).
firepower# show conn all protocol udp port 161	Verifique todas las conexiones LINA ASA/FTD en UDP 161 (sondeo SNMP).
firepower# show log i 302015.*161	Verifique ASA/FTD LINA log 302015 para el sondeo SNMP.
firepower# more system:running-config i community	Verifique la cadena de comunidad SNMP.
firepower# debug menu netsnmp 4	Verifique la configuración SNMP y el ID de proceso.
firepower# show asp table classify interface net201 domain permit match port=161	Verifique los hitcounts en la ACL SNMP en la interfaz denominada net201.
firepower# show disk0: i core	Verifique si hay núcleos del SNMP.
admin@firepower:~\$ ls -l /var/data/cores	Verifique si hay núcleos del SNMP. Aplicable únicamente en FTD.
firepower# show route	Verifique la tabla de routing del ASA/LINA de FTD.

> show network	Verifique la tabla de ruteo del plano de administración FTD.
admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	Verifique/resuelva problemas de SNMPv3 en FTD.
firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	Comandos ocultos en versiones más recientes. Depuraciones internas, útiles para solucionar problemas de SNMP con Cisco TAC.

41xx/9300 (FXOS): qué recopilar antes de abrir un caso con Cisco TAC

Comando	Descripción
firepower# connect fxos firepower(fxos)# ethalyzer 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	Captura de FXOS para sondeo del SNMP (UDP 161) Carga en un servidor FTP remoto FTP IP: 192.0.2.100 Nombre de usuario FTP: ftp
firepower# connect fxos firepower(fxos)# ethalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap	Captura de FXOS para las operaciones de notificación del SNMP (UDP 162)
firepower# scope system firepower /system # scope services firepower /system/services # show ip-block detail	Verificación de la ACL de FXOS
firepower# show fault	Verificación de las fallas de FXOS

firepower# show fabric-interconnect	Verificación de la configuración de la interfaz de FXOS y la configuración del gateway predeterminado
firepower# connect fxos firepower(fxos)# show running-config snmp all	Verificación de la configuración del SNMP de FXOS
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	Verificación de los OID del SNMP de FXOS
firepower# connect fxos firepower(fxos)# show snmp	Verificación de la configuración del SNMP de FXOS y sus contadores
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	Depuración del SNMP de FXOS ('paquetes' o 'todo') Uso de 'terminal no monitor' y 'undebug all' para su detención

1xxx/21xx (FXOS): qué recopilar antes de abrir un caso con Cisco TAC

Comando	Descripción
> capture-traffic	Capture el tráfico en la interfaz de administración.
> show network	Verifique la tabla de routing del plano de administración de FTD.
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail] firepower /monitoring # show snmp-trap	Verifique la configuración del SNMP de FXOS.
firepower# show fault	Verificación de las fallas de FXOS

<pre>firepower# connect local-mgmt firepower(local-mgmt)# dir cores_fxos firepower(local-mgmt)# dir cores</pre>	<p>Verifique los archivos principales de FXOS (rastreo de origen).</p>
---	--

FMC: qué recopilar antes de abrir un caso con Cisco TAC

Comando	Descripción
<pre>admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n</pre>	Captura de tráfico en la interfaz de administración para sondeo del SNMP
<pre>admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap</pre>	Captura de tráfico en la interfaz de administración para sondeo del SNMP y guardado en archivo
<pre>admin@FS2600-2:~\$ sudo pmtool status grep snmpd</pre>	Verificación del estado del proceso del SNMP
<pre>admin@FS2600-2:~\$ ls -al /var/common grep snmpd</pre>	Verificación de archivos principales del SNMP (rastreo de origen)
<pre>admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf</pre>	Verificación del contenido del archivo de configuración del SNMP

Ejemplos de snmpwalk

Estos comandos se pueden utilizar para la verificación y solución de problemas:

Comando	Descripción
<pre># snmpwalk -c Cisco123 -v2c 192.0.2.1</pre>	<p>Obtiene todos los OID del host remoto con SNMPv2c.</p> <p>Cisco123 = Cadena de comunidad</p> <p>192.0.2.1 = Host de destino</p>
<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 = Gage32: 0</pre>	Obtiene un OID específico del host remoto con SNMPv2c.
<pre># snmpwalk -c Cisco123 -v2c 192.0.2.1</pre>	Muestra los OID recuperados en formato

.10.3.1.1.4.1.9.9.109.1.1.1.1 -On .10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 = Gálibo32: 0	numérico.
# snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1	Obtiene todos los OID del host remoto con SNMPv3. Usuario de SNMPv3 = cisco Autenticación de SNMPv3 = SHA Autorización de SNMPv3 = AES
# snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -x AES -X Cisco123 192.0.2.1	Obtiene todos los OID del host remoto con SNMPv3 (MD5 y AES128).
# snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1	SNMPv3 con autenticación solamente.

Cómo buscar defectos en el SNMP

1. Vaya a <https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV>.
2. Ingrese la palabra clave **snmp** y elija **Select from list**.

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

The screenshot shows a search interface with the following elements:

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

Productos más comunes:

- Software Cisco Adaptive Security Appliance (ASA)
- Cisco Firepower de la serie 9300
- Dispositivo virtual del centro de administración Firepower de Cisco
- NGFW Cisco Firepower

Información Relacionada

- [Configuración del SNMP para Threat Defense](#)
- [Configuración de SNMP en FXOS \(IU\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).