

Configurar o SNMP em dispositivos Firepower NGFW

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[SNMP do chassi \(FXOS\) no FPR4100/FPR9300](#)

[Configurar o SNMPv1/v2c do FXOS usando a GUI](#)

[Configurar o SNMPv1/v2c do FXOS usando a interface de linha de comando \(CLI\)](#)

[Configurar o SNMPv3 do FXOS usando a GUI](#)

[Configurar o SNMPv3 do FXOS usando a CLI](#)

[SNMP do FTD \(LINA\) no FPR4100/FPR9300](#)

[Configurar o SNMPv2c do LINA](#)

[Configurar o SNMPv3 do LINA](#)

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

[SNMP no FPR2100](#)

[SNMP do chassi \(FXOS\) no FPR2100](#)

[Configurar o SNMPv1/v2c do FXOS](#)

[Configurar o SNMPv3 do FXOS](#)

[SNMP do FTD \(LINA\) no FPR2100](#)

[Verificar](#)

[Verificar o SNMP do FXOS para FPR4100/FPR9300](#)

[Verificações do SNMPv2c do FXOS](#)

[Verificações do SNMPv3 do FXOS](#)

[Verificar o SNMP do FXOS para FPR2100](#)

[Verificações do SNMPv2 do FXOS](#)

[Verificações do SNMPv3 do FXOS](#)

[Verificar o SNMP do FTD](#)

[Permitir o tráfego do SNMP para o FXOS no FPR4100/FPR9300](#)

[Configurar a lista de acesso global usando a GUI](#)

[Configurar a lista de acesso global usando a CLI](#)

[Verificação](#)

[Usar o navegador de objetos da OID](#)

[Troubleshooting](#)

[Não é possível pesquisar o SNMP do LINA do FTD](#)

[Não é possível pesquisar o SNMP do FXOS](#)

[Quais valores de OID do SNMP devem ser usados?](#)

[Não é possível obter as interceptações do SNMP](#)

[Não é possível monitorar o FMC usando o SNMP](#)

[Configuração do SNMP no Firepower Device Manager \(FDM\)](#)

[Dicas de solução de problemas do SNMP](#)

[Como procurar defeitos do SNMP](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e solucionar problemas de dispositivos de FTD do protocolo de gerenciamento de rede simples (SNMP - Simple Network Management Protocol) no firewall de próxima geração (NGFW - Next Generation Firewall).

Pré-requisitos

Requisitos

Este documento exige conhecimento básico do protocolo SNMP.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os dispositivos Firepower NGFW podem ser divididos em dois subsistemas principais:

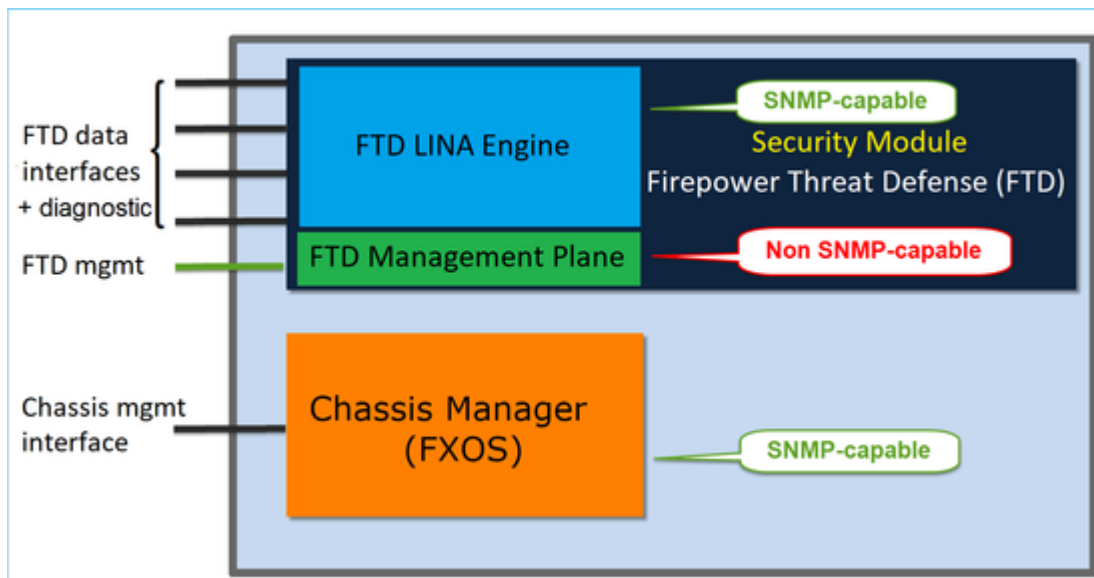
- O Firepower Extensible Operative System (FX-OS) controla o hardware do chassi.
- O Firepower Threat Defense (FTD) é executado dentro do módulo.

O FTD é um software unificado que consiste em dois mecanismos principais: o mecanismo Snort e o mecanismo LINA. O mecanismo SNMP atual do FTD é derivado do ASA clássico e tem visibilidade dos recursos relacionados ao LINA.

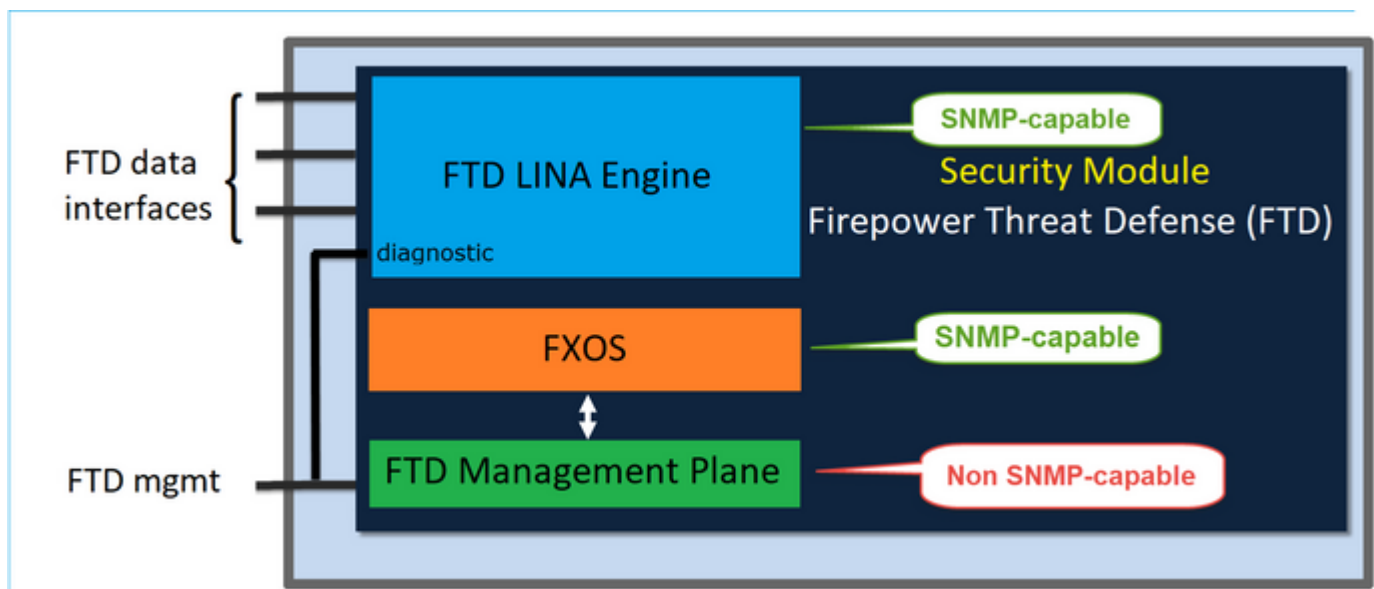
O FX-OS e o FTD têm planos de controle independentes e, para fins de monitoramento, têm diferentes mecanismos SNMP. Cada um dos mecanismos SNMP fornece informações diferentes e pode querer monitorar ambos para obter uma visão mais abrangente do status do dispositivo.

Do ponto de vista do hardware, há atualmente duas arquiteturas principais para os dispositivos Firepower NGFW: o Firepower 2100 Series e o Firepower 4100/9300 Series.

Os dispositivos Firepower 4100/9300 têm uma interface dedicada para o gerenciamento de dispositivos e essa é a origem e o destino do tráfego SNMP endereçado ao subsistema do FXOS. Por outro lado, a aplicação do FTD usa uma interface LINA (dados e/ou diagnóstico). Nas versões do FTD posteriores a 6.6, a interface de gerenciamento do FTD também pode ser usada para a configuração do SNMP.



O mecanismo SNMP nos dispositivos Firepower 2100 usa a interface de gerenciamento do FTD e o IP. O próprio dispositivo faz a ponte com o tráfego de SNMP recebido nessa interface e o encaminha para o software do FXOS.

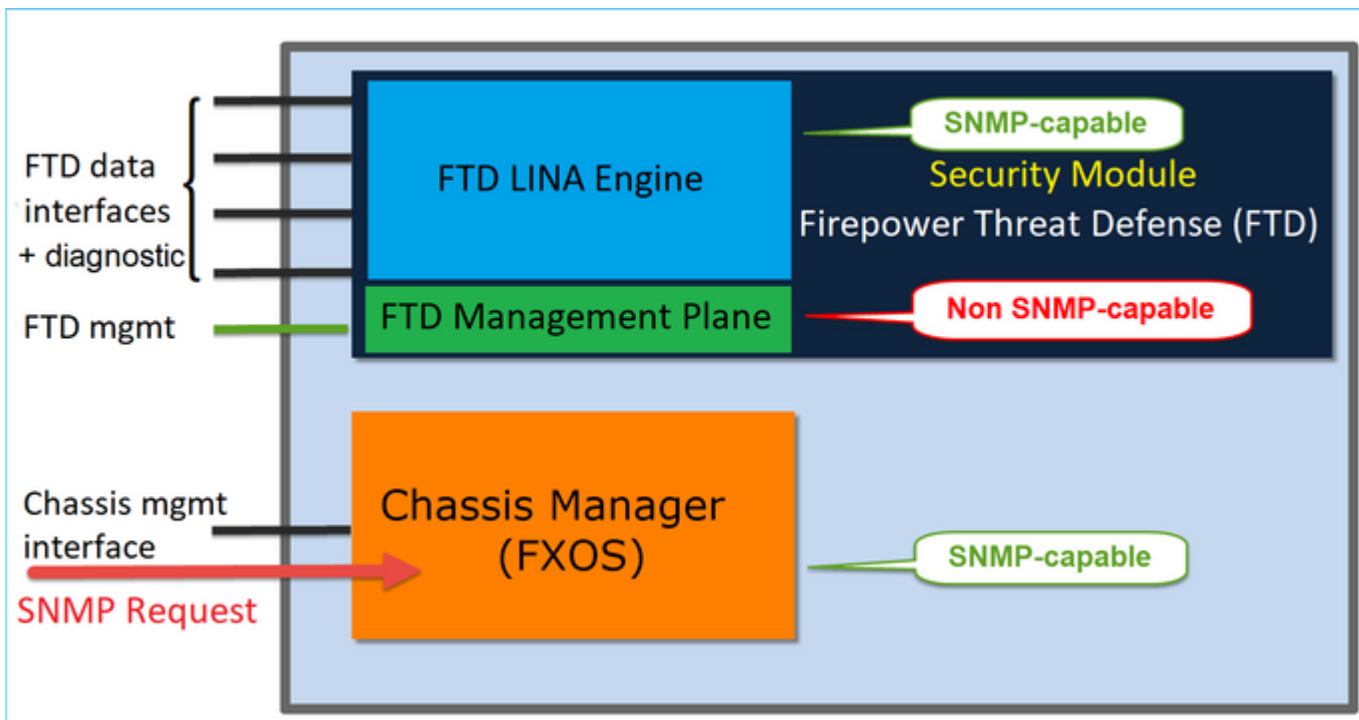


Nos FTDs que usam a versão de software 6.6 ou superior, foram implementadas estas alterações:

- SNMP na interface de gerenciamento.
- Nas plataformas do FPR1000 ou FPR2100 Series, o SNMP do LINA e o SNMP do FXOS foram unificados nessa única interface de gerenciamento. Além disso, é fornecido um único ponto de configuração no FMC em **Configurações da plataforma > SNMP**.

Configurar

SNMP do chassi (FXOS) no FPR4100/FPR9300



Configurar o SNMPv1/v2c do FXOS usando a GUI

Etapa 1. Abra a interface do usuário do Firepower Chassis Manager (FCM) e navegue até a guia **Configurações da plataforma > SNMP**. Marque a caixa de ativação SNMP, especifique a string de **comunidade** a ser usada nas solicitações do SNMP e clique em **Salvar**.

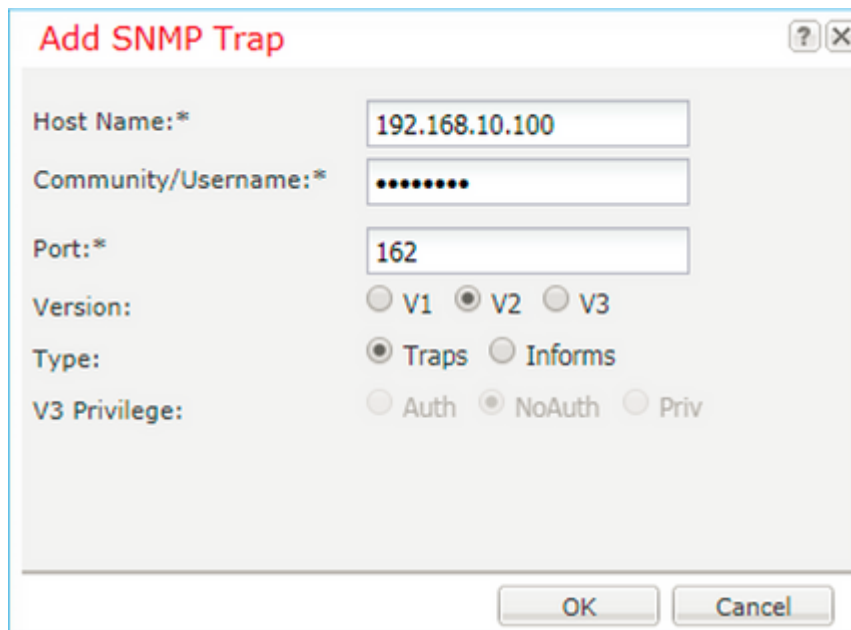
The screenshot shows the 'Platform Settings' tab in the GUI. The 'SNMP' section is active. The 'Admin State' is checked (labeled 1). The 'Port' is set to 161. The 'Community/Username' field contains a masked string (labeled 2). Below this, there are fields for 'System Administrator Name' and 'Location'. The 'SNMP Traps' section has an 'Add' button (labeled 4). At the bottom, there is a 'Save' button (labeled 3) and a 'Cancel' button.

Name	Port	Version	V3 Privilege	Type

Name	Auth Type	AES-128

Observação: se o campo Comunidade/Nome de usuário já estiver definido, o texto à direita do campo vazio exibirá **Conjunto: Sim**. Se o campo Comunidade/Nome de usuário ainda não estiver preenchido com um valor, o texto à direita do campo vazio exibirá **Set: No**

Etapa 2. Configure o servidor de destino das interceptações do SNMP.



Observação: os valores de comunidade para consultas e host de interceptação são independentes e podem ser diferentes

O host pode ser definido como endereço IP ou por nome. Selecione **OK** e a configuração do servidor de interceptação do SNMP será salva automaticamente. Não há necessidade de selecionar o botão Salvar na página principal do SNMP. O mesmo ocorre quando você exclui um host.

Configurar o SNMPv1/v2c do FXOS usando a interface de linha de comando (CLI)

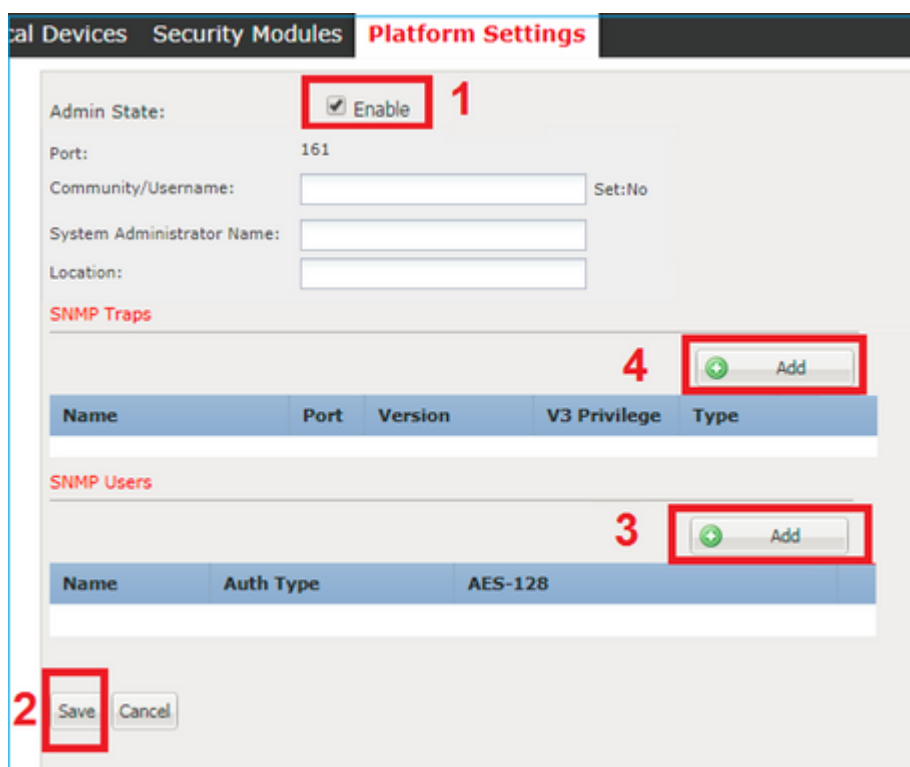
```
<#root>
ksec-fpr9k-1-A#
scope monitoring
ksec-fpr9k-1-A /monitoring #
enable snmp
ksec-fpr9k-1-A /monitoring* #
set snmp community
Enter a snmp community:
ksec-fpr9k-1-A /monitoring* #
  enter snmp-trap 192.168.10.100
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A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

Configurar o SNMPv3 do FXOS usando a GUI

Etapa 1. Abra o FCM e navegue até a guia **Configurações da plataforma > SNMP**.

Etapa 2. Para o SNMP v3, não há necessidade de definir uma string de comunidade na seção superior. Cada usuário criado pode executar com êxito as consultas para o mecanismo SNMP do FXOS. A primeira etapa é ativar o SNMP na plataforma. Uma vez feito isso, você pode criar os usuários e o host de interceptação de destino. Os usuários do SNMP e os hosts de interceptação do SNMP são salvos automaticamente.



Etapa 3. Conforme mostrado na imagem, adicione o usuário do SNMP. O tipo de autenticação é sempre SHA, mas você pode usar AES ou DES para criptografia:

Add SNMP User

Name:* user1

Auth Type: SHA

Use AES-128:

Password:

Confirm Password:

Privacy Password:

Confirm Privacy Password:

OK Cancel

Etapa 4. Adicione o host de interceptação do SNMP, conforme mostrado na imagem:

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

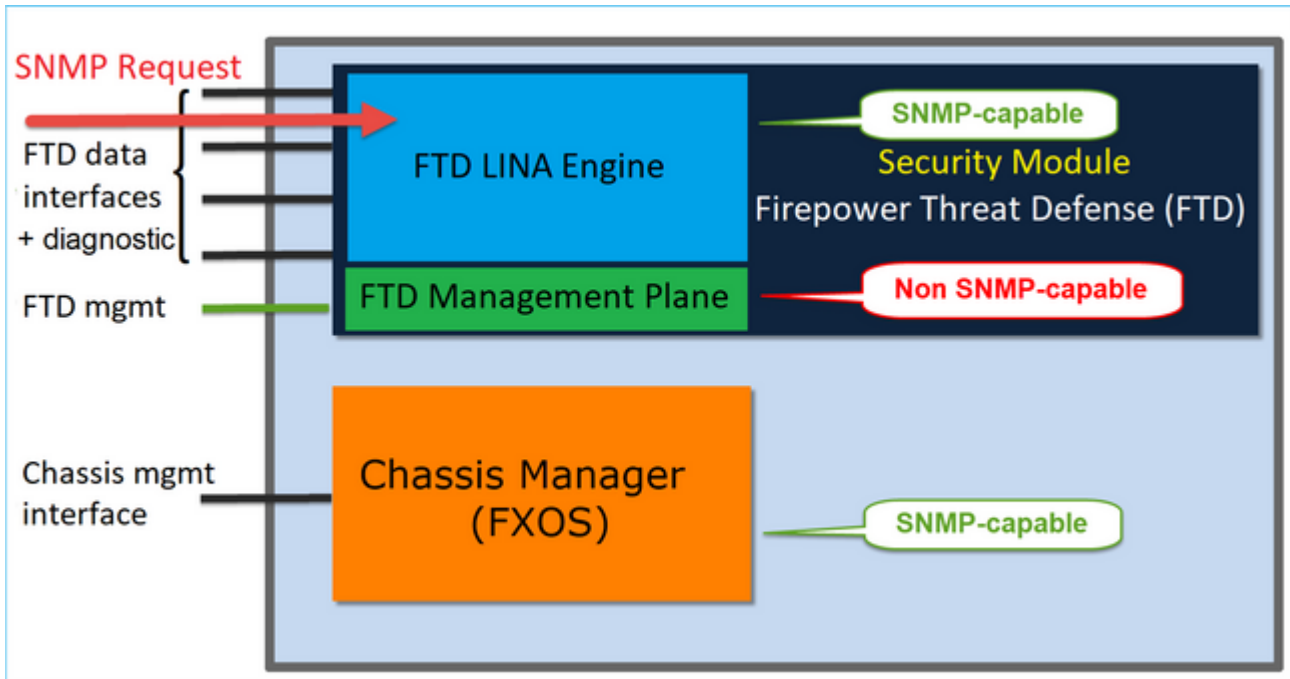
OK Cancel

Configurar o SNMPv3 do FXOS usando a CLI

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

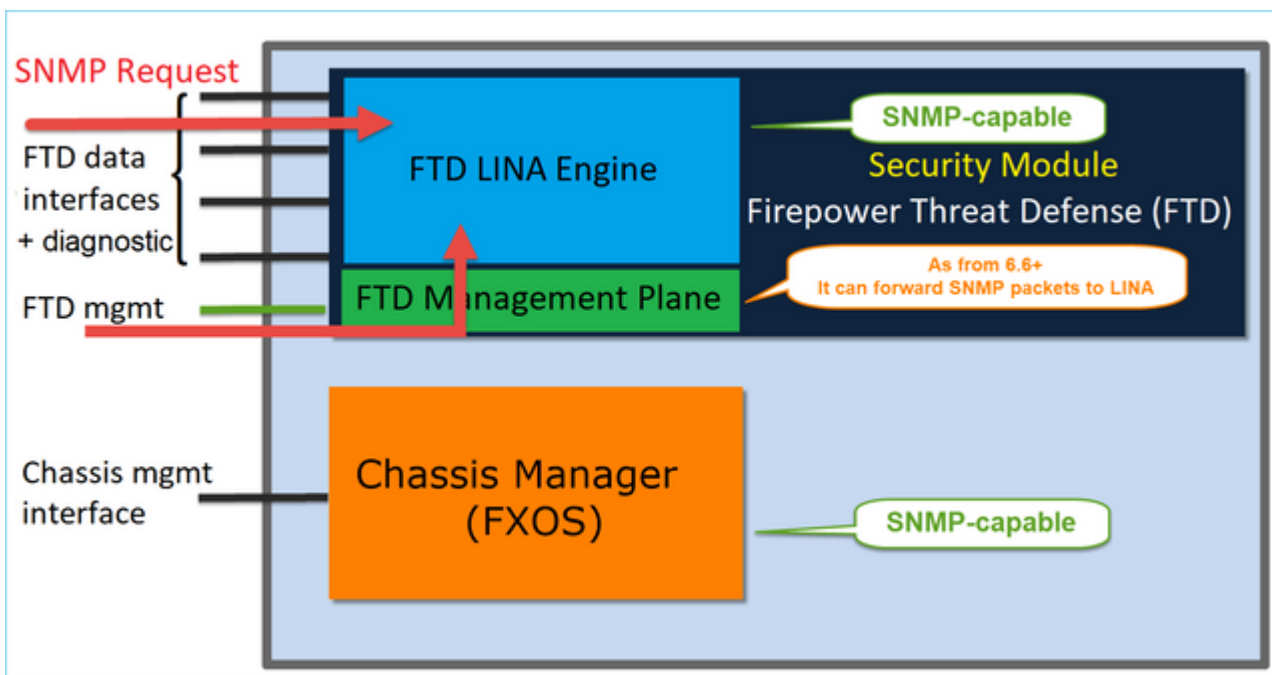
```
Password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set auth sha
ksec-fpr9k-1-A /monitoring/snmp-user* #
set priv-password
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter 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 do FTD (LINA) no FPR4100/FPR9300



Alterações nas versões posteriores a 6.6

- Nas versões posteriores a 6.6, você também tem a opção de usar a interface de gerenciamento do FTD para pesquisas e interceptações.



Há suporte para o recurso de gerenciamento de IP único do SNMP a partir da versão 6.6 em todas as plataformas do FTD:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 que executa o FTD
- FTDv

Configurar o SNMPv2c do LINA

Etapa 1. Na interface do usuário do FMC, navegue até **Dispositivos > Configurações da plataforma > SNMP**. Marque a opção "Ativar servidores do SNMP" e defina as configurações do SNMPv2c da seguinte forma:

Etapa 2. Na guia **Hosts**, selecione o botão **Adicionar** e especifique as configurações do servidor do 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 shows 'OUTSIDE3' selected. An 'Add' button is located between the two sections. At the bottom of the window, there are 'OK' and 'Cancel' buttons.

Você também pode especificar a interface de **diagnóstico** como fonte para as mensagens do SNMP. A interface de diagnóstico é uma interface de dados que permite apenas o tráfego de entrada e de saída (somente gerenciamento).

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

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

Selected Zones/Interfaces

diagnostic

Interface Name

Esta imagem é da versão 6.6 e usa o Light Tema.

Além disso, nas versões do FTD posteriores a 6.6, você também pode escolher a interface de gerenciamento:

Add SNMP Management Hosts

IP Address*
 +

SNMP Version

Username

Community String

Confirm

Poll
 Trap

Trap Port

(1 - 65535)

Reachable By:

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

Security Zones or Named Interface

Available Zones

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

Selected Zones/Interfaces

diagnostic

Interface Name

Se a nova interface de gerenciamento for selecionada, o SNMP do LINA estará disponível na interface de gerenciamento.

O resultado:

Enable SNMP Servers

Read Community String

Confirm*

System Administrator Name

Location

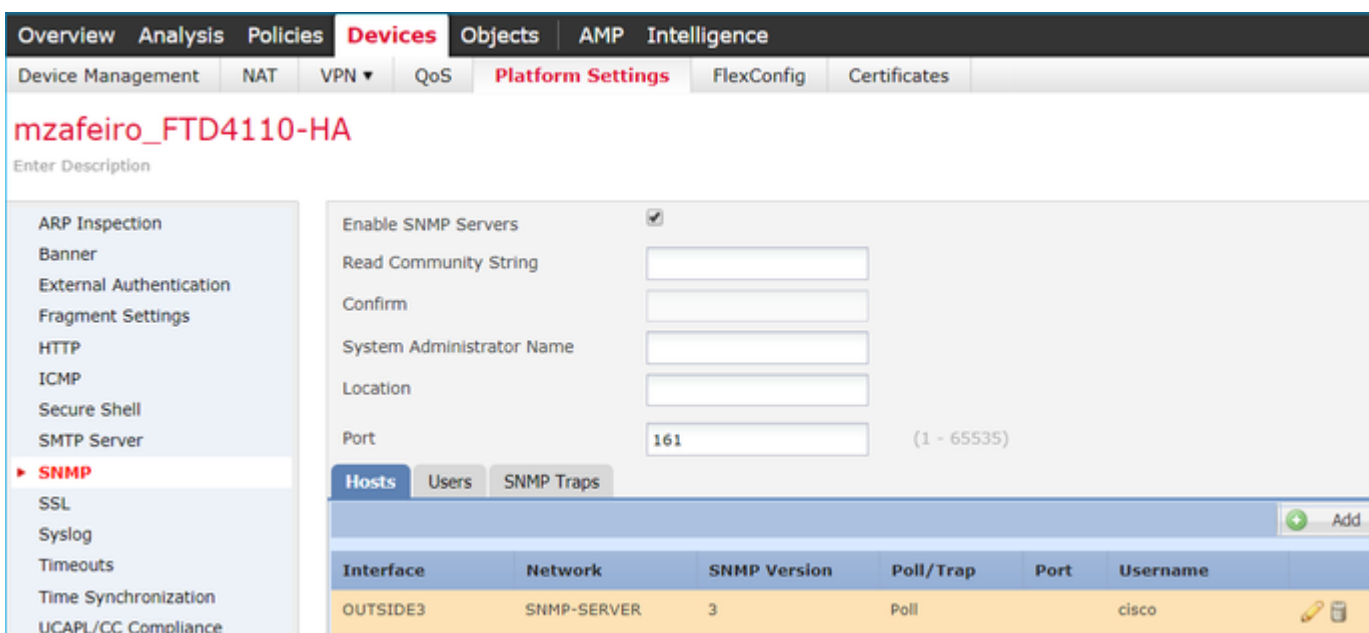
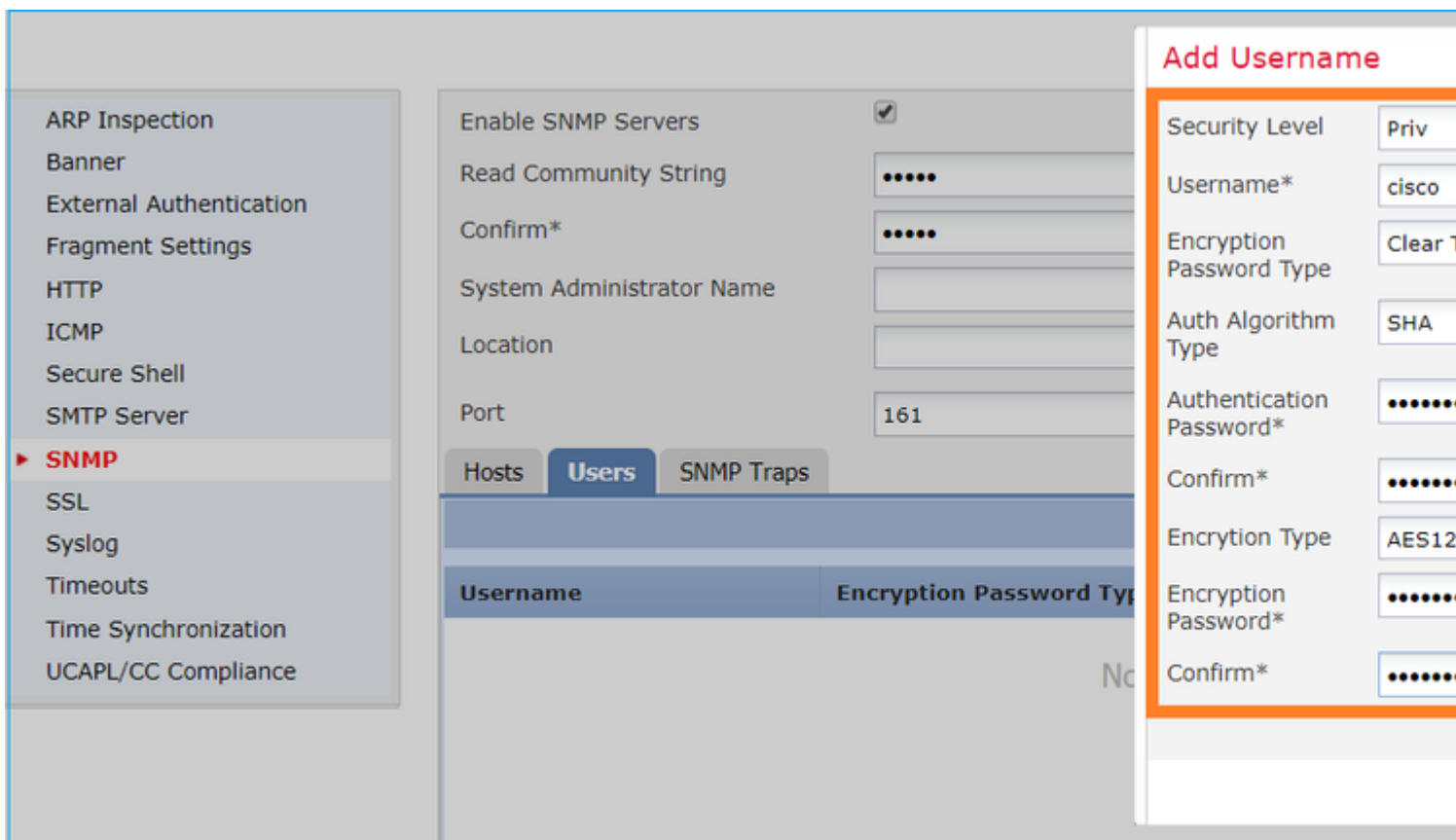
Port (1 - 65535)

Hosts Users SNMP Traps

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

Configurar o SNMPv3 do LINA

Etapa 1. Na interface do usuário do FMC, navegue até **Dispositivos > Configurações da plataforma > SNMP**. Marque a opção "Ativar servidores do SNMP" e configure o usuário e o host do SNMPv3:



Etapa 2. Configure o host também para receber as interceptações:

Edit SNMP Management Hosts

IP Address*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port (1 - 65535)

Available Zones

Selected Zones/Interfaces

Etapa 3. As intercepções que você deseja receber podem ser selecionadas na seção **Intercepções do 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

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

Comportamento anterior ao 7.2

- Nas plataformas 9300 e 4100, as MIBs SNMP para informações de chassi não estão disponíveis no SNMP configurado em aplicativos FTD/ASA. Ele precisa ser configurado separadamente no MIO através do gerenciador de chassis e acessado separadamente. O MIO é o módulo de gerenciamento e E/S (Supervisor).
- Duas políticas de SNMP separadas precisam ser configuradas, uma no Blade/App e outra no MIO para monitoramento de SNMP.
- Portas separadas são utilizadas, uma para Blade e outra para MIO para monitoramento SNMP do mesmo dispositivo.
- Isso pode criar complexidade quando você tenta configurar e monitorar dispositivos 9300 e 4100 via

SNMP.

Como funciona em versões mais recentes (FXOS 2.12.1, FTD 7.2, ASA 9.18.1 e posterior)

- Com a unificação SNMP de blade MIO, os usuários podem pesquisar MIBs LINA e MIO através das interfaces de aplicativo (ASA/FTD).
- O recurso pode ser ativado ou desativado por meio da nova interface de usuário do MIO CLI e do FCM (Chassis Mgr).
- O status padrão é desabilitado. Isso significa que o agente SNMP MIO está sendo executado como uma instância autônoma. As interfaces MIO precisam ser usadas para pesquisar MIBs chassis/DME. Uma vez que o recurso esteja habilitado, as interfaces de aplicativo podem ser usadas para pesquisar os mesmos MIBs.
- A configuração está disponível na interface do usuário do Gerenciador de chassis em **Platform-settings > SNMP > Admin Instance**, onde o usuário pode especificar a instância de FTD que agruparia/reuniria os MIBs do chassis para apresentá-lo ao NMS
- As aplicações ASA/FTD nativas e MI são suportadas.
- Esse recurso é aplicável somente a plataformas baseadas em MIO (FPR9300 e FPR4100).

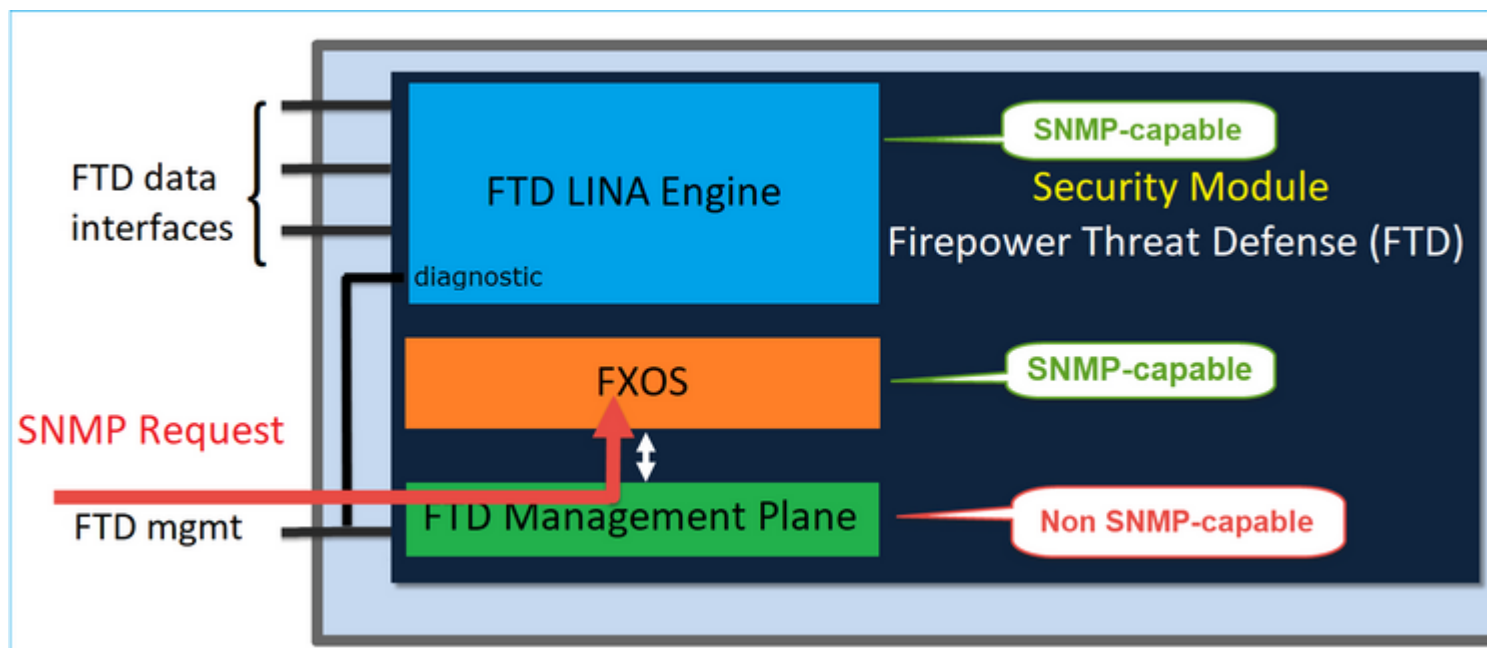
Pré-requisitos, plataformas suportadas

- Versão mínima do gerente com suporte: FCM 2.12.1
- Dispositivos gerenciados: FPR9300 / FP4100 Series
- Versão mínima de dispositivo gerenciado suportado necessária: FXOS 2.12.1, FTD 7.2 ou ASA 9.18.1

SNMP no FPR2100

Nos sistemas FPR2100, não há FCM. A única maneira de configurar o SNMP é usando o FMC.

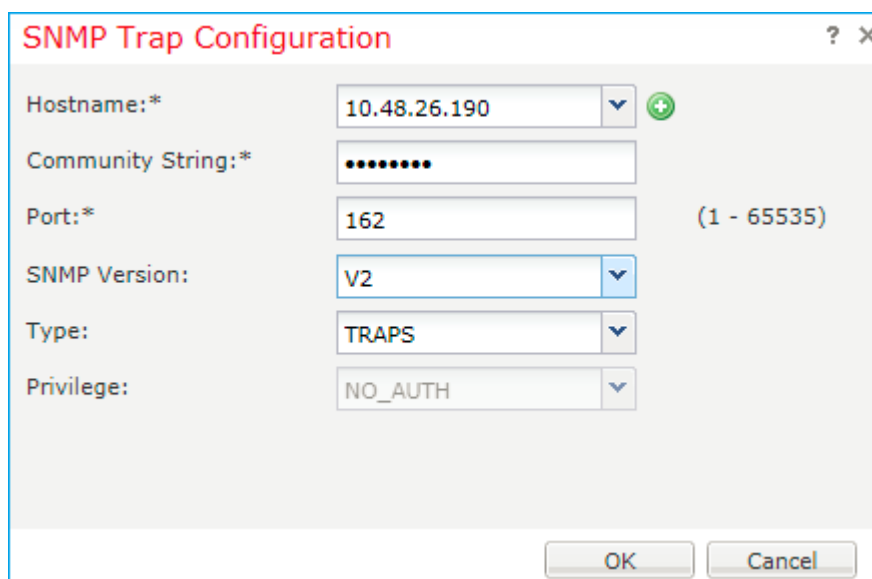
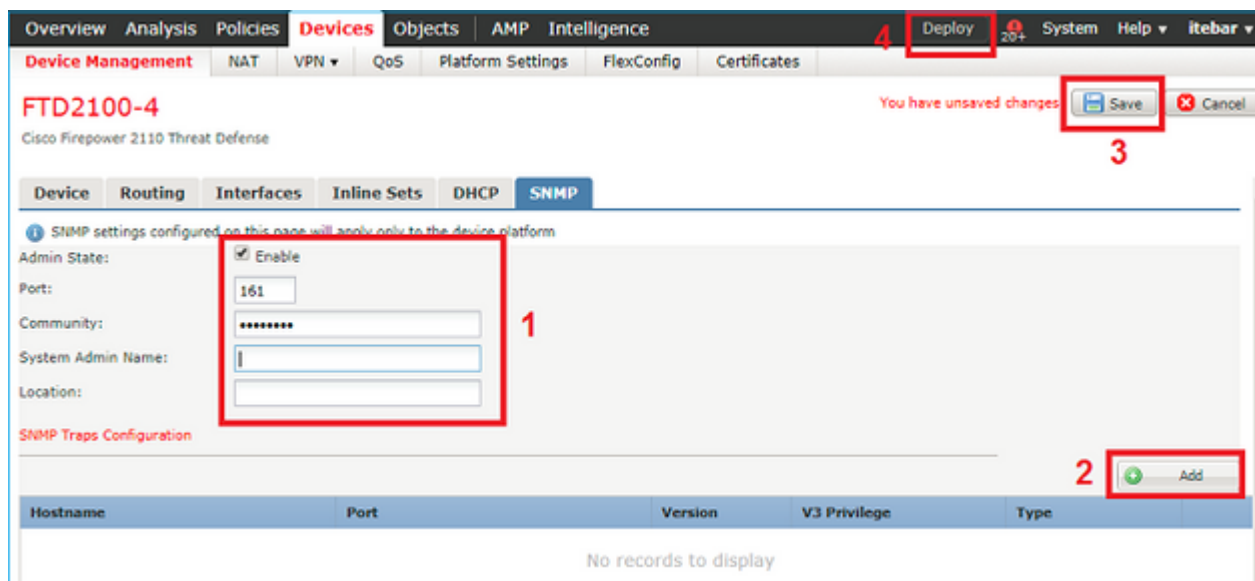
SNMP do chassis (FXOS) no FPR2100



A partir do FTD 6.6, você também tem a opção de usar a interface de gerenciamento do FTD para SNMP. Nesse caso, as informações do SNMP do FXOS e do LINA são transferidas por meio da interface de gerenciamento do FTD.

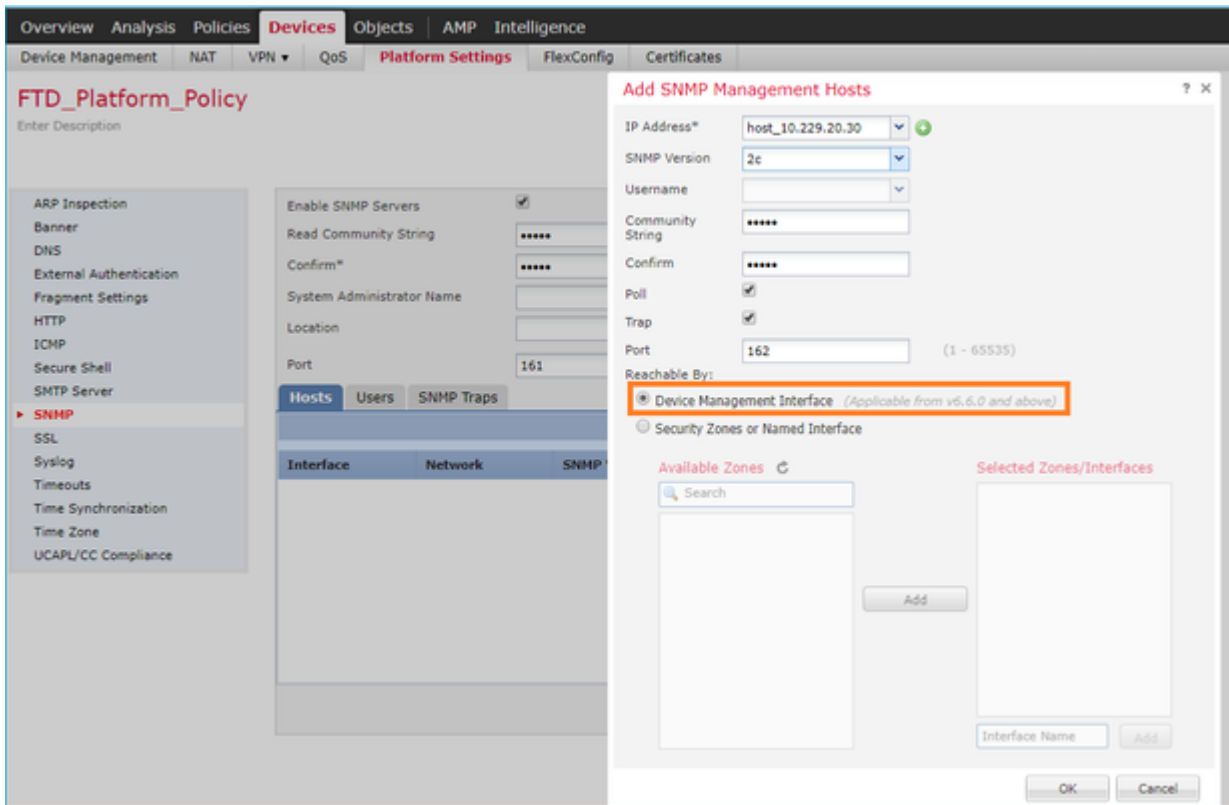
Configurar o SNMPv1/v2c do FXOS

Abra a interface do usuário do FMC e navegue até **Dispositivos > Gerenciamento de dispositivos**. Selecione o dispositivo e selecione SNMP:



Alteração no FTD 6.6 ou posteriores

Você pode especificar a interface de gerenciamento do FTD:



Como a interface de gerenciamento também pode ser configurada para SNMP, a página mostra esta mensagem de aviso:

A configuração SNMP da plataforma do dispositivo nesta página será desativada se as configurações de SNMP forem definidas com a interface de gerenciamento do dispositivo através de **dispositivos > configurações da plataforma (Threat Defense) > SNMP > hosts**.

Configurar o SNMPv3 do FXOS

Abra a interface do usuário do FMC e navegue até **Escolher dispositivos > Gerenciamento de dispositivos**. Escolha o dispositivo e selecione 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: ▼

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

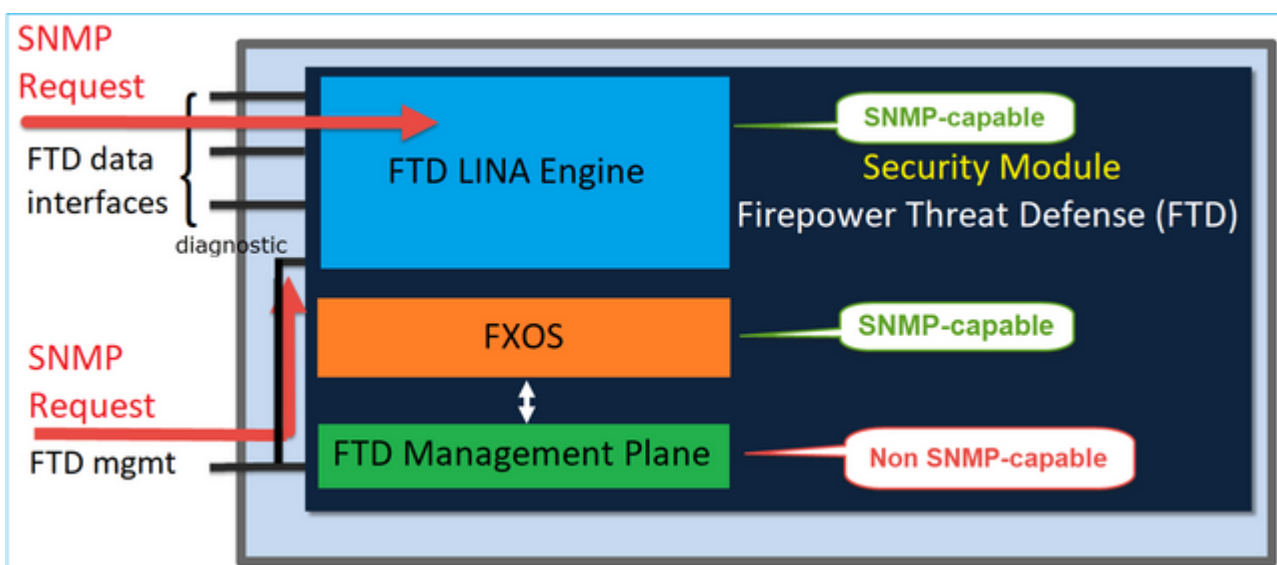
Type: TRAPS

Privilege: PRIV

OK Cancel

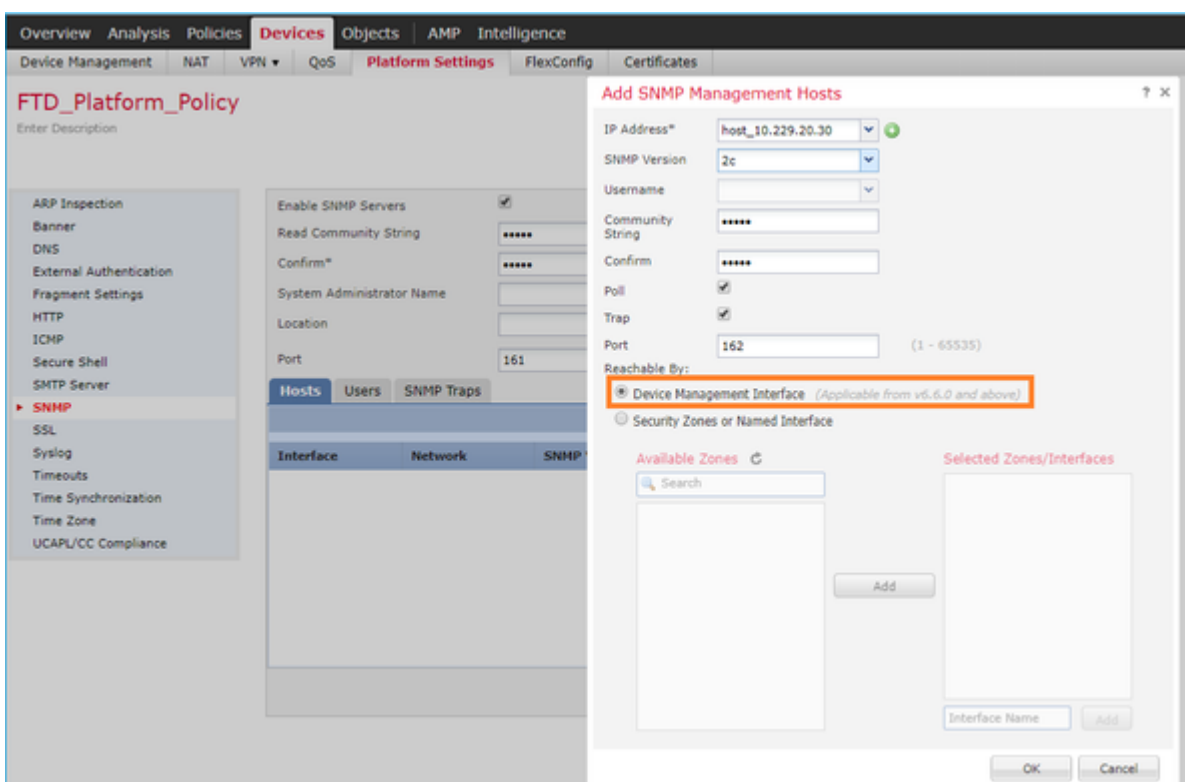
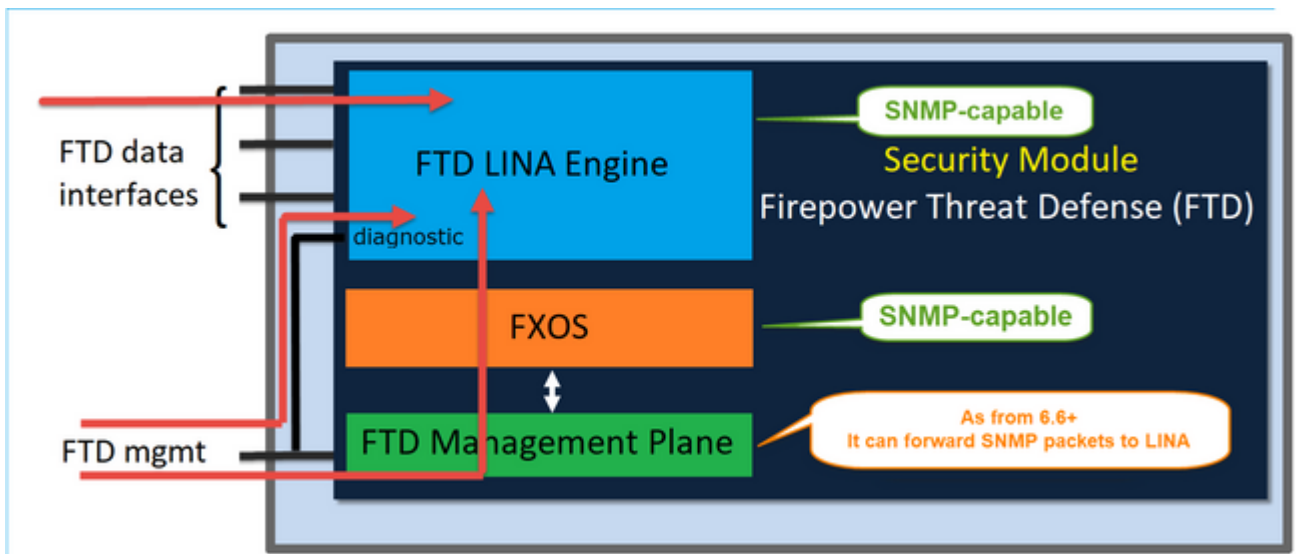
SNMP do FTD (LINA) no FPR2100

- Para versões anteriores a 6.6, a configuração do SNMP do FTD do LINA nos dispositivos FP1xxx/FP21xx do FTD é idêntica a um FTD nos dispositivos Firepower 4100 ou 9300.



FTD 6.6 ou versões posteriores

- Nas versões posteriores a 6.6, você também tem a opção de usar a interface de gerenciamento do FTD para pesquisas e interceptações do LINA.



Se a nova interface de gerenciamento for selecionada:

- O SNMP do LINA está disponível na interface de gerenciamento.
- Em **Dispositivos > Gerenciamento de dispositivos**, a guia **SNMP** está desativada, pois não é mais necessária. Um banner de notificação será exibido. A guia de dispositivo SNMP estava visível apenas nas plataformas 2100/1100. Esta página não existe nas plataformas FPR9300/FPR4100 e FTD55xx.

Depois da configuração, as informações de pesquisa/interceptação do SNMP de uma combinação de SNMP do LINA e FXOS (no FP1xxx/FP2xxx) estão na interface de gerenciamento do 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				

Há suporte para o recurso de gerenciamento de IP único do SNMP a partir da versão 6.6 em todas as plataformas do FTD:

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- ASA5500 que executa o FTD
- FTDv

Para obter mais detalhes, selecione Configurar o SNMP para defesa contra ameaças

Verificar

Verificar o SNMP do FXOS para FPR4100/FPR9300

Verificações do SNMPv2c do FXOS

Verificação da configuração da CLI:

```
<#root>
```

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

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

```
Sys Contact:
```

```
Sys Location:
```

```
ksec-fpr9k-1-A /monitoring # show snmp-trap
```

```
SNMP Trap:
  SNMP Trap          Port      Community  Version V3 Privilege Notification Type
  -----
  192.168.10.100    162          V2c        Noauth      Traps
```

No modo do 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
```

Verificações adicionais:

```
<#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
...
```

Testar as solicitações do SNMP.

Execute uma solicitação do SNMP em um host válido.

Confirmar a geração de interceptação.

Você pode usar o flap de uma interface com o EthAnalyzer ativado para confirmar se as interceptações do SNMP foram geradas e enviadas para os hosts de interceptação 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
```

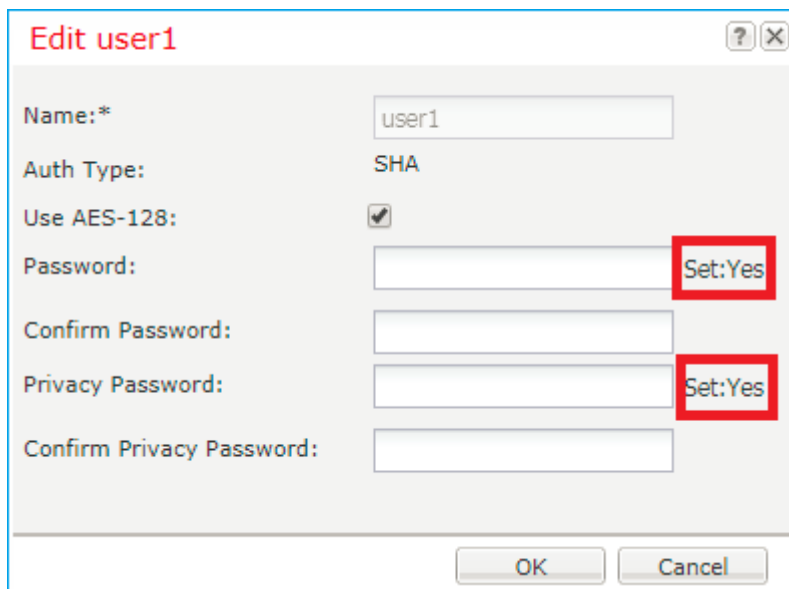
```
2017-11-17 09:01:35.954624 10.62.148.35 -> 192.168.10.100 SNMP sNMPv2-Trap
```

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

Aviso: uma oscilação de interface pode causar uma interrupção de tráfego. Faça esse teste apenas em um ambiente de laboratório ou em uma janela de manutenção

Verificações do SNMPv3 do FXOS

Etapa 1. Abrir a interface do usuário do FCM **Configurações da plataforma > SNMP > Usuário** mostra se há senhas e senhas de privacidade configuradas:



Edit user1 [?] [X]

Name:* user1

Auth Type: SHA

Use AES-128:

Password: Set:Yes

Confirm Password:

Privacy Password: Set:Yes

Confirm Privacy Password:

OK Cancel

Etapa 2. Na CLI, você pode verificar a configuração do SNMP no **monitoramento de escopo**:

```
<#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
```

Etapa 3. No modo do FXOS, você pode expandir a configuração e os detalhes do 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
-----
```

Testar as solicitações do SNMP.

Você pode verificar a configuração e fazer uma solicitação do SNMP em qualquer dispositivo com os recursos do SNMP.

Para verificar como a solicitação do SNMP é processada, você pode usar a depuração do 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
```

Cuidado: uma depuração pode afetar o desempenho do dispositivo.

Verificar o SNMP do FXOS para FPR2100

Verificações do SNMPv2 do FXOS

Verifique a configuração usando a 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
```

Confirme o comportamento do SNMP.

Você pode verificar se é possível pesquisar o FXOS e enviar uma solicitação do SNMP em um host ou qualquer dispositivo com os recursos do SNMP.

Use o comando **capture-traffic** para ver a solicitação e a resposta do 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

Verificações do SNMPv3 do FXOS

Verifique a configuração usando a 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

Confirme o comportamento do SNMP.

Envie uma solicitação do SNMP para verificar se é possível pesquisar o FXOS.

Além disso, você pode capturar a solicitação:

<#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
```

Verificar o SNMP do FTD

Para verificar a configuração do SNMP do LINA do 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 *****
```

A partir do FTD 6.6, você pode configurar e usar a interface de gerenciamento do FTD para 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
```

Verificação adicional:

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

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

Na CLI do servidor do SNMP, execute um 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
```

```
...
```

Verificação das estatísticas de tráfego do 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
```

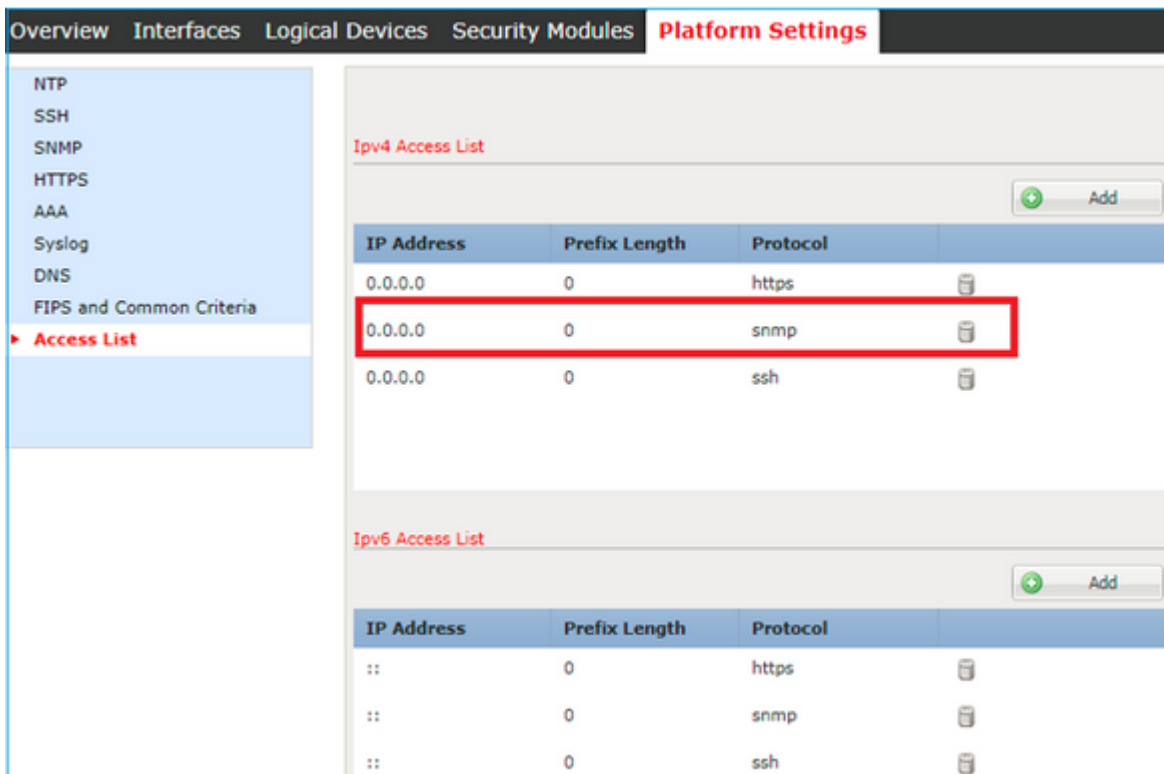
```
0 General errors
```

```
1899 Response PDUs
```

Permitir o tráfego do SNMP para o FXOS no FPR4100/FPR9300

A configuração do FXOS no FPR4100/9300 pode restringir o acesso do SNMP por endereço IP de origem. A seção de configuração da lista de acesso define quais redes/hosts podem acessar o dispositivo usando o SSH, HTTPS ou SNMP. Você precisa verificar se as consultas do SNMP no servidor do SNMP são permitidas.

Configurar a lista de acesso global usando a GUI



The screenshot shows the Juniper GUI configuration page for 'Platform Settings'. The left sidebar has 'Access List' selected. The main content area is titled 'IPv4 Access List' and contains a table with the following data:

IP Address	Prefix Length	Protocol	
0.0.0.0	0	https	
0.0.0.0	0	snmp	
0.0.0.0	0	ssh	

Below the IPv4 table is the 'IPv6 Access List' section, which also has an 'Add' button and a table with three entries for protocols https, snmp, and ssh, all with IP Address '::' and Prefix Length '0'.

Configurar a lista de acesso global usando a 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
```

Verificação

<#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

Usar o navegador de objetos da OID

O [Cisco SNMP Object Navigator](#) é uma ferramenta on-line em que você pode converter as diferentes OIDs e obter uma breve descrição.

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

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

Use o comando **show snmp-server oid** na CLI do LINA do FTD para recuperar toda a lista de OIDs do LINA que podem ser pesquisadas.

<#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#
```

Observação: o comando está oculto.

Troubleshooting

Estes são os geradores de caso do SNMP mais comuns observados pelo Cisco TAC:

1. Não é possível pesquisar o SNMP do LINA do FTD
2. Não é possível pesquisar o SNMP do FXOS
3. Quais valores de OID do SNMP devem ser usados?
4. Não é possível obter as interceptações do SNMP
5. Não é possível monitorar o FMC usando o SNMP
6. Não é possível configurar o SNMP
7. Configuração do SNMP no Firepower Device Manager

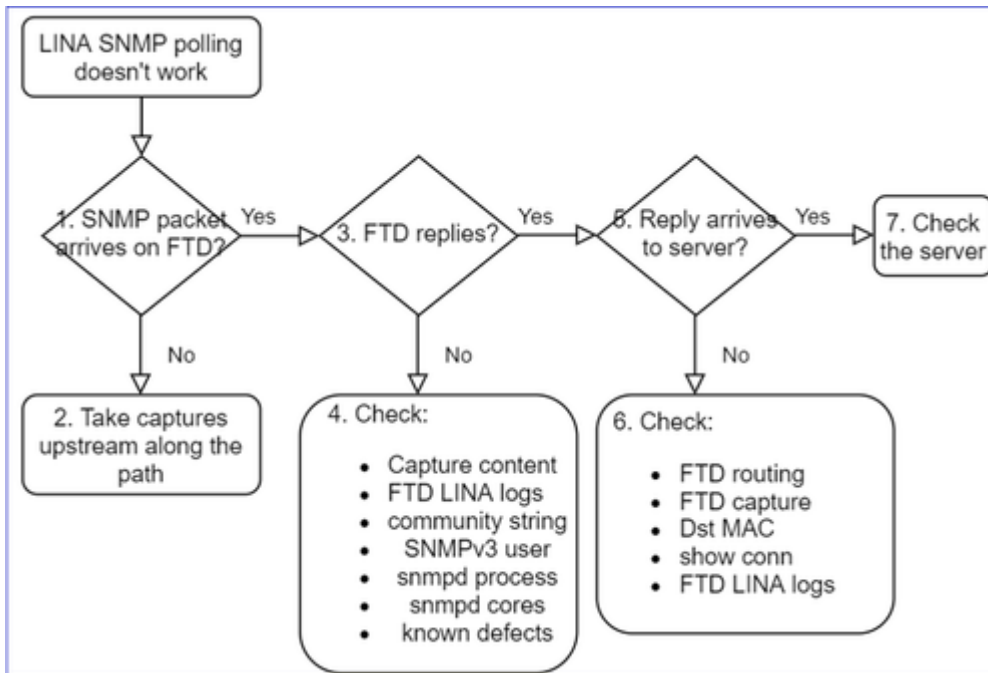
Não é possível pesquisar o SNMP do LINA do FTD

Descrições dos problemas (exemplo de casos reais do Cisco TAC):

- "Não é possível buscar os dados no SNMP."
- "Não é possível pesquisar o dispositivo no SNMPv2."
- "O SNMP não funciona. Queremos monitorar o firewall com o SNMP, mas, enfrentamos problemas após a configuração."
- "Temos dois sistemas de monitoramento que não podem monitorar o FTD usando o SNMP v2c ou 3."
- "O snmpwalk não funciona no firewall."

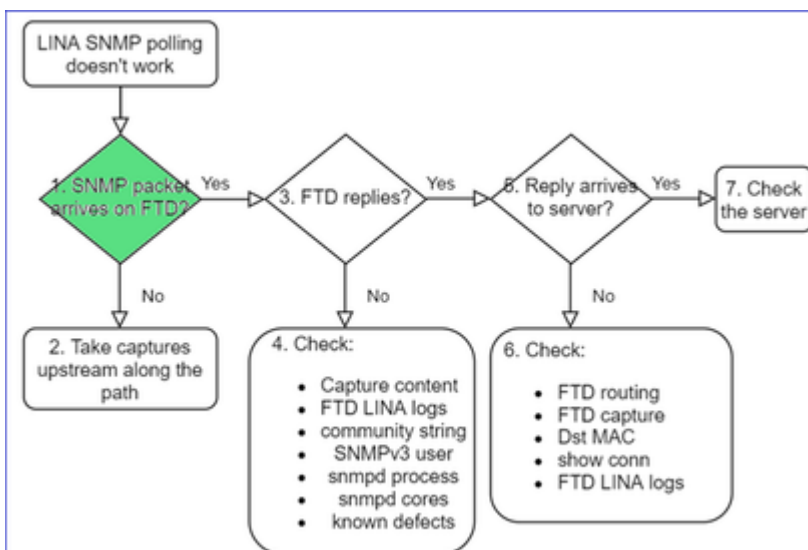
Recomendação sobre como solucionar problemas

Este é o processo recomendado para solucionar problemas do fluxograma de pesquisa SNMP LINA:



Análise detalhada

1. O pacote SNMP chega no FTD



- Ativar capturas para verificar a chegada de pacotes do SNMP.

O SNMP na interface de gerenciamento FTD (versão pós-6.6) usa a palavra-chave de gerenciamento:

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

O SNMP nas interfaces de dados do FTD usa o nome da interface:

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

Capture na interface de gerenciamento do FTD:

```
<#root>
```

```
>
```

```
capture-traffic
```

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

```
0 - management1
```

```
1 - management0
```

```
2 - Global
```

```
Selection?
```

```
1
```

Capture na interface de dados do FTD:

```
<#root>
```

```
firepower#
```

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

Rastreamento de pacotes da interface de dados do FTD (cenário funcional “versões anteriores 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)

Rastreamento de pacotes da interface de dados do FTD (cenário não funcional “versões posteriores a 6.6/9.14.1):

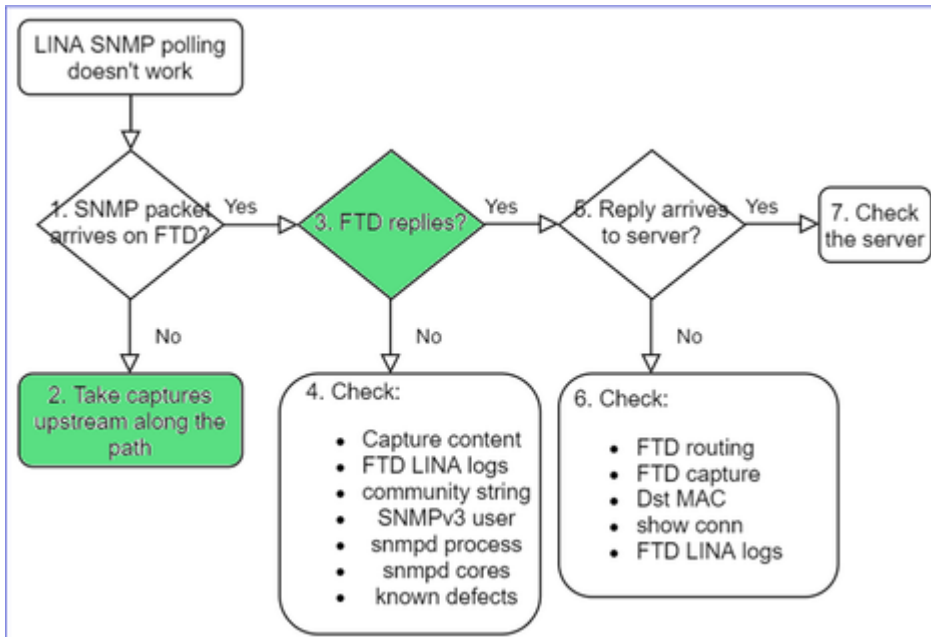
```
firepower# show capture SNMP packet-number 1 trace

  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: 9
Config:
nat (nlp_int_tap,net201) source static nlp_server_snmp_192.168.21.100_intf4 interface destination static
0_192.168.21.100_4 0_192.168.21.100_4
Additional Information:
NAT divert to egress interface nlp_int_tap(vrfid:0)
Untranslate 192.168.21.50/161 to 169.254.1.2/161
```

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

2. Caso não veja pacotes SNMP nas capturas de entrada de FTD:

- Fazer capturas upstream ao longo do caminho.
- Verifique se o servidor do SNMP usa o IP apropriado do FTD.
- Comece pela porta do switch voltada para a interface do FTD e mova-se upstream.



3. Você vê respostas SNMP de FTD?

Para verificar se o FTD responde, confira:

1. Captura de saída do FTD (LINA ou interface de gerenciamento)

Verifique se há pacotes do SNMP com porta de origem 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

```

Nas versões posteriores à 6.6/9.14.1, você tem um ponto de captura adicional: Capturar na interface NLP tap. O IP NATed é do intervalo 162.254.x.x:

```
<#root>
```

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

```
sudo tcpdump -i tap_nlp
```

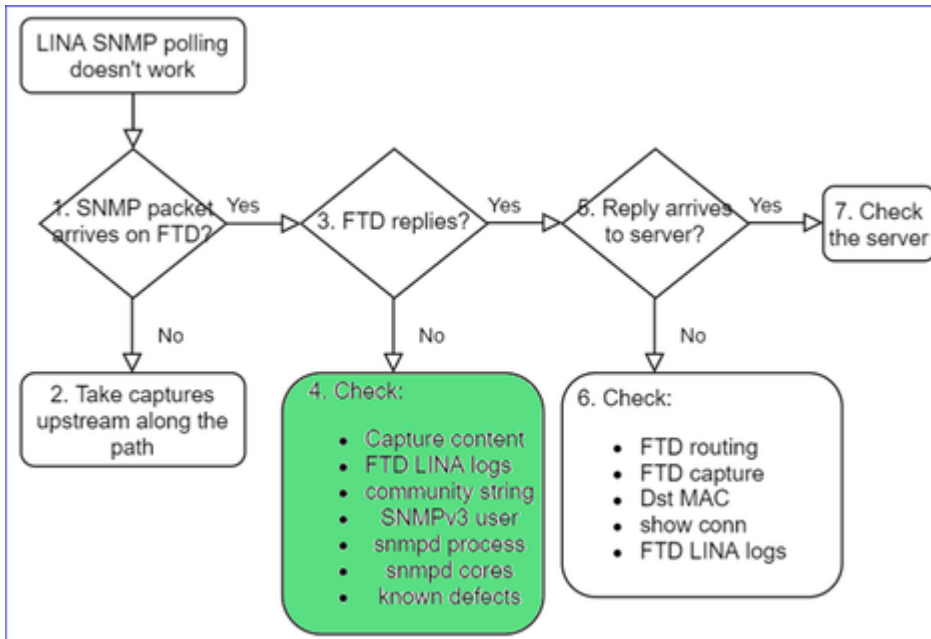
```
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```

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. Controlos complementares



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

b. Verifique as estatísticas do snmp-server do LINA do 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
â€¦
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. Tabela de conexão LINA FTD

Essa verificação é muito útil caso você não veja pacotes na captura na interface de ingresso do FTD. Observe que essa é uma verificação válida apenas para SNMP na interface de dados. Se o SNMP estiver na interface de gerenciamento (pós-6.6/9.14.1), nenhuma conexão será criada.

```
<#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 do LINA do FTD

Esta também é uma verificação válida apenas para SNMP na interface de dados. Se o SNMP estiver na interface de gerenciamento, o registro não será criado:

```
<#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 se o FTD descarta os pacotes do SNMP devido ao IP de origem do host incorreto

```
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. Credenciais incorretas (comunidade do SNMP)

No conteúdo da captura, você pode ver os valores da comunidade (SNMP v1 e 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. Configuração incorreta (por exemplo, versão do SNMP ou string de comunidade)

Há algumas maneiras de verificar a configuração do SNMP do dispositivo e as strings de comunidade:

<#root>

firepower#

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

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

Outra maneira:

<#root>

firepower#

```
debug menu netsnmp 4
```

h. Descartes do LINA do FTD/ASP do ASA

Esta é uma verificação útil para ver se os pacotes do SNMP foram descartados pelo FTD. Primeiro, limpe os contadores (clear asp drop) e depois teste:

```
<#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

As capturas do ASP fornecem visibilidade dos pacotes descartados (por exemplo, ACL ou adjacência):

```
<#root>
```

```
firepower#
```

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

Teste e verifique o conteúdo da captura:

```
<#root>
```

```
firepower#
```

```
show capture
```

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


j) Núcleo do SNMP (traceback) – forma de verificação 1

Esta verificação será útil caso você suspeite de problemas de estabilidade do sistema:

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

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

Núcleo do SNMP (traceback) – forma de verificação 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
```

Se você vir um arquivo de núcleo do SNMP, colete estes itens e entre em contato com o Cisco TAC:

- Arquivo TS do FTD (ou show tech do ASA)
- snmpd core files

Depurações do SNMP (estes são comandos ocultos e disponíveis somente nas versões mais recentes):

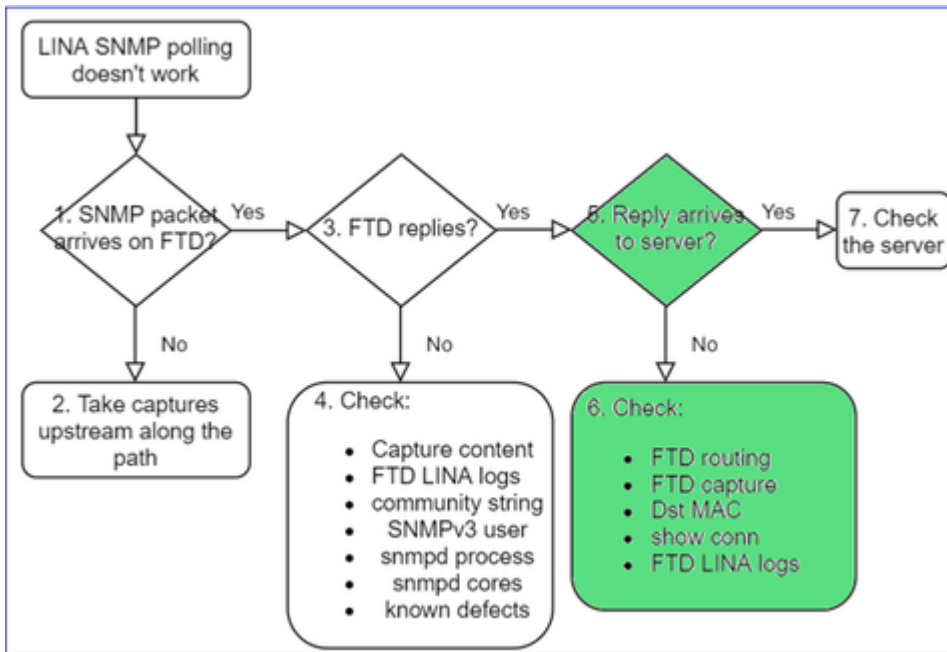
```
<#root>
firepower#
debug snmp trace [255]

firepower#
debug snmp verbose [255]

firepower#
debug snmp error [255]

firepower#
debug snmp packet [255]
```

A resposta do SNMP do firewall chega ao servidor?



Se o FTD responder, mas a resposta não chegar ao servidor, verifique:

a. Roteamento do FTD

Para o roteamento da interface de gerenciamento do FTD:

```

<#root>
>
show network
  
```

Para o roteamento da interface de dados do LINA do FTD:

```

<#root>
firepower#
show route
  
```

b. Verificação do MAC de destino

Verificação do MAC de destino do gerenciamento do 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

Verificação do MAC de destino da interface de dados do LINA do FTD:

<#root>

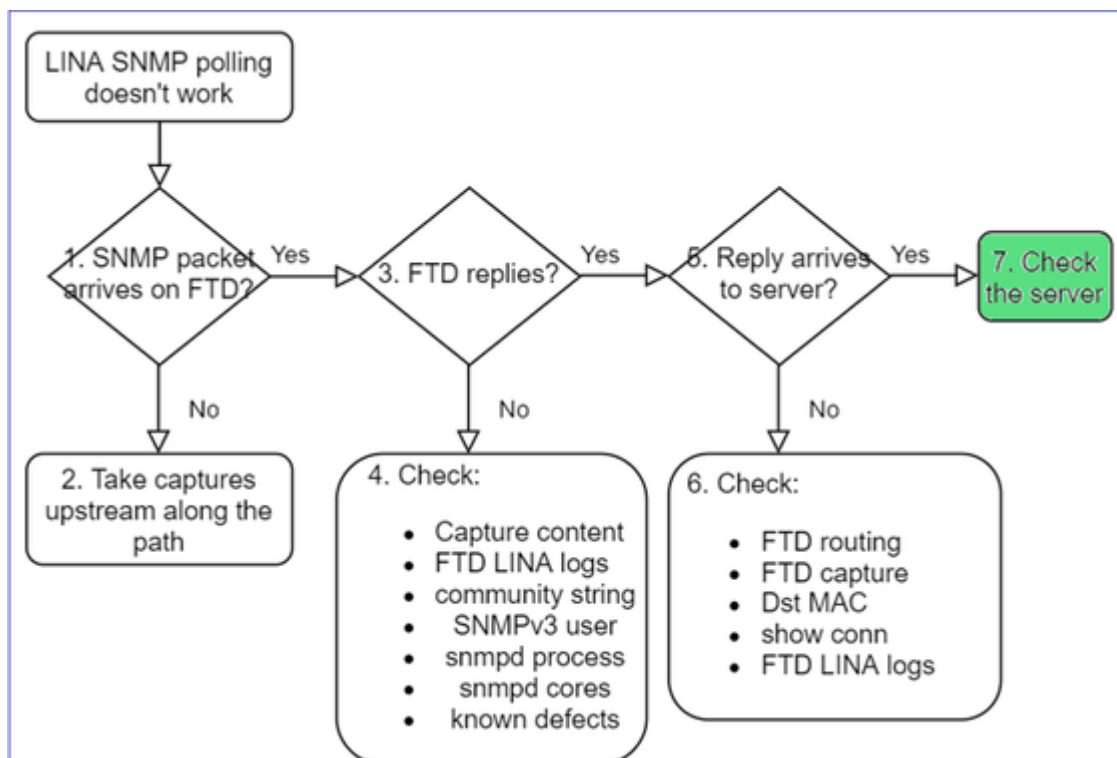
firepower#

`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 os dispositivos ao longo do caminho que potencialmente descartam/bloqueiam os pacotes SNMP.

Verifique o servidor do SNMP



- a. Verifique o conteúdo da captura para ver as configurações.
- b. Verifique a configuração do servidor.
- c. Tente modificar o nome da comunidade SNMP (por exemplo, sem caracteres especiais).

Você pode usar um host final ou até mesmo o FMC para testar a pesquisa, desde que as duas condições sejam atendidas:

1. A conectividade do SNMP foi estabelecida.
2. O IP de origem tem permissão para pesquisar o 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
```

Considerações de pesquisa SNMPv3

- Licença: o SNMPv3 requer uma licença de criptografia forte. Verifique se a funcionalidade de exportação controlada está ativada no Smart Licensing Portal
- Para solucionar problemas, você pode tentar com um novo usuário/credenciais
- Se a criptografia for usada, você poderá descriptografar o tráfego SNMPv3 e verificar o payload conforme descrito em: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>
- Considere o AES128 para criptografia caso o software seja afetado por defeitos como:
- ID de bug da Cisco [CSCvy27283](#)

A pesquisa SNMPv3 ASA/FTD pode falhar usando os algoritmos de privacidade AES192/AES256

ID de bug da Cisco [CSCvx45604](#) Falha de walk de Snmpv3 no usuário com auth sha e priv aes 192

Observação: se o SNMPv3 falhar devido a uma incompatibilidade de algoritmo, as saídas show e os registros não mostrarão nada óbvio

```

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'

Considerações sobre a pesquisa do SNMPv3 “ Estudos de caso

1. snmpwalk do SNMPv3 “ Cenário 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
```

Na captura (snmpwalk), você verá uma resposta para cada pacote:

```

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

```

O arquivo de captura não mostra nada incomum:

```

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 do SNMPv3 â€“ Falha na criptografia

Dica #1: há um tempo limite:

```
<#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

Dica #2: há muitas solicitações e 1 resposta:

```

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

Dica #3: falha na descriptografia do 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]
```

Dica 4. Verifique o arquivo ma_ctx2000.log para ver as mensagens "erro ao analisar ScopePDU":

```
<#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
```

O erro de análise de ScopedPDU é uma dica forte de um erro de criptografia. O arquivo ma_ctx2000.log mostra eventos somente para SNMPv3!

3. snmpwalk do SNMPv3 – Falha na autenticação

Dica #1: falha na autenticação

```
<#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)
```

Dica #2: há muitas solicitações e respostas

```
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
```

Dica #3: Pacote Malformado do 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]
```

Dica 4. Verifique o arquivo ma_ctx2000.log para ver as mensagens "Falha na autenticação":

```
<#root>
```

```
>
```

```
expert
```

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

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

```
Authentication failed for Cisco123
```

```
Authentication failed for Cisco123
```

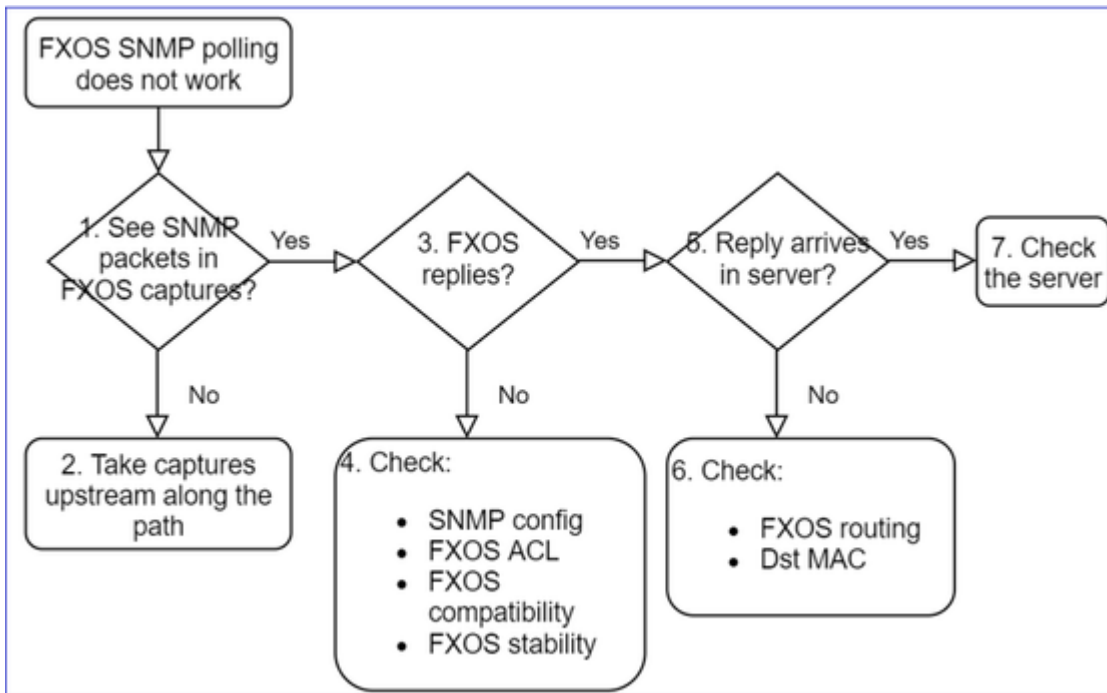
Não é possível pesquisar o SNMP do FXOS

Descrições dos problemas (exemplo de casos reais do Cisco TAC):

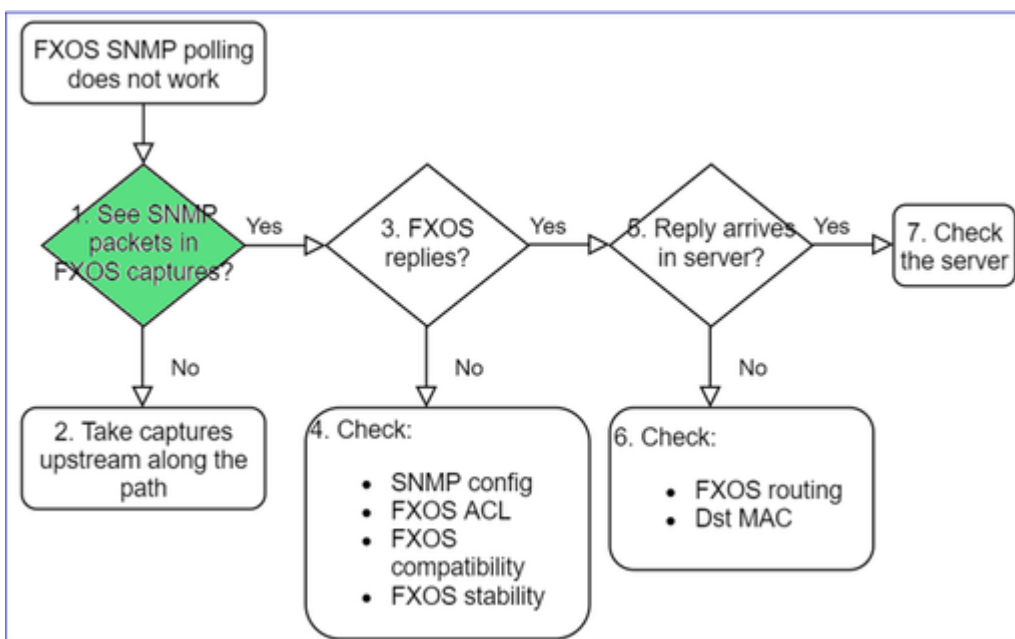
- "O SNMP fornece uma versão errada do FXOS. Ao pesquisar a versão do FXOS usando o SNMP, a saída é difícil de entender."
- "Não foi possível configurar a comunidade de snmp no FXOS FTD4115."
- "Após um upgrade do FXOS de 2.8 para 2.9 no firewall em standby, obtemos um limite de tempo ao tentar receber informações usando o SNMP."
- "O snmpwalk falha no FXOS 9300, mas funciona no FXOS 4140 na mesma versão. A acessibilidade e a comunidade não são o problema."
- "Queremos adicionar 25 servidores do SNMP no FXOS FPR4K, mas não é possível."

Solução de problemas recomendada

Este é o processo para solucionar problemas do fluxograma de polling SNMP FXOS:



1. Você vê pacotes SNMP em capturas FXOS?



FPR1xxx/21xx

- No FPR1xxx/21xx não há gerenciador de chassis (modo de dispositivo).
- Você pode pesquisar o software do FXOS na interface de gerenciamento.

<#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

- No Firepower 41xx/93xx, use a ferramenta CLI do EthAnalyzer para fazer uma captura de chassi:

```
<#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
```

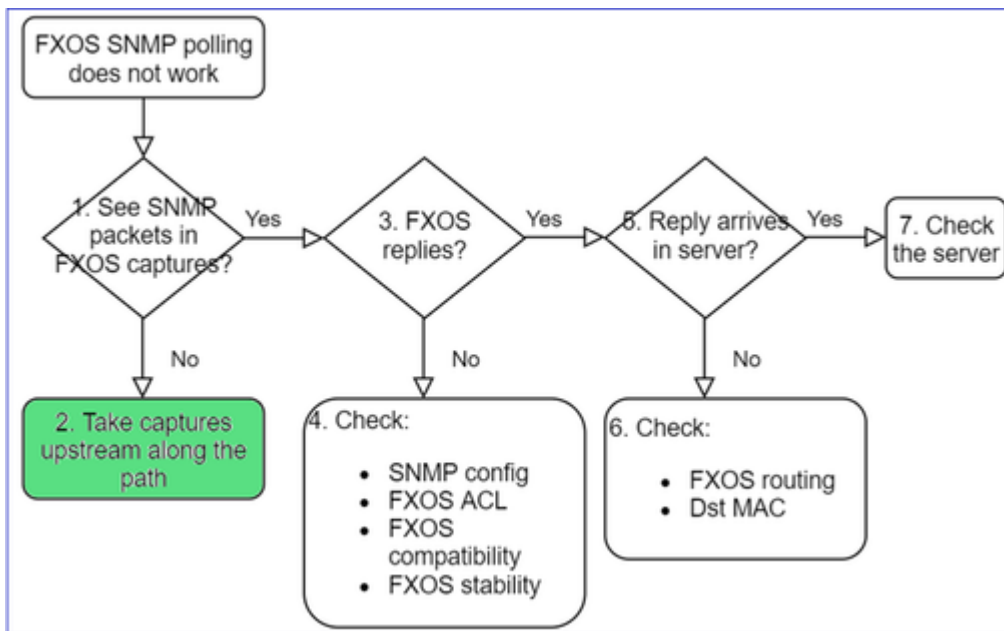
```
1
```

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

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

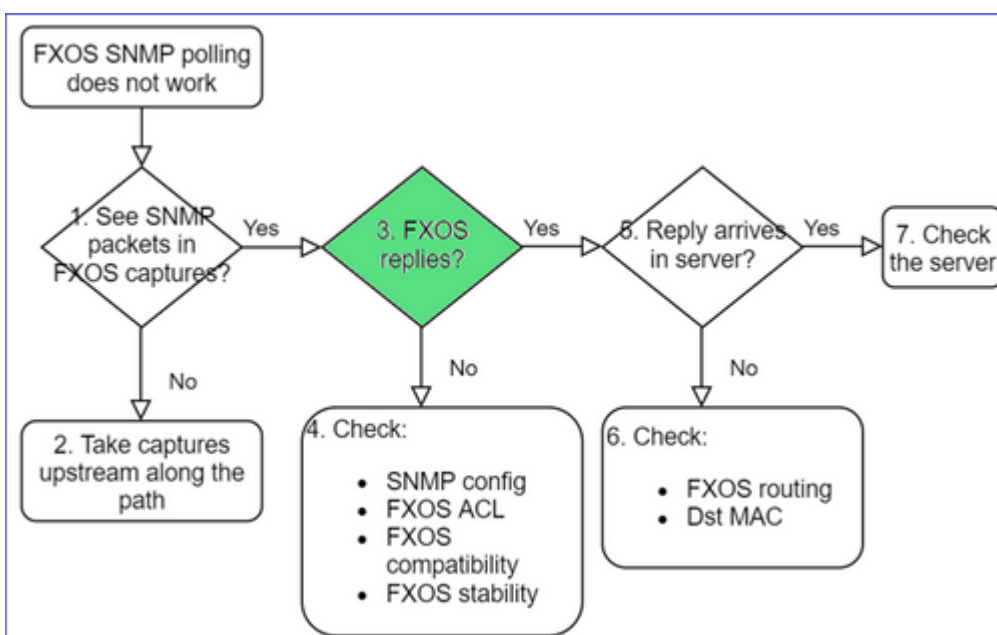
```
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. Nenhum pacote nas capturas FXOS?



- Fazer capturas upstream ao longo do caminho

3. Respostas FXOS?



- Cenário funcional:

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.

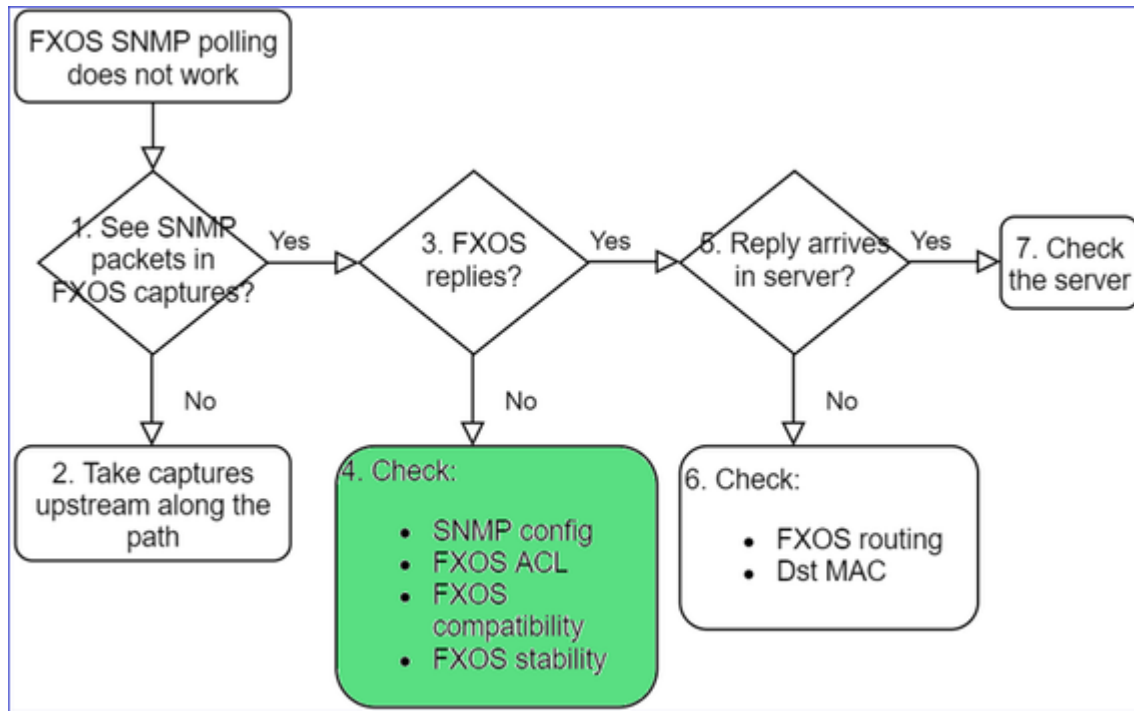
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

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. O FXOS não responde



Verificações adicionais

- Verifique a configuração do SNMP (na interface do usuário ou CLI):

```
<#root>
```

```
firepower#
```

```
scope monitoring
```

```
firepower /monitoring #
```

```
show snmp
```

```
Name: snmp
```

```
Admin State: Enabled
```

```
Port: 161
```

```
Is Community Set: Yes
```

- Tenha cuidado com os caracteres especiais (por exemplo, '\$'):

```
<#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 o SNMP v3, use show snmp-user [detail]
- Verifique a compatibilidade do FXOS

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

4. Caso a FXOS não responda

Verifique os contadores do SNMP do 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
```

← Total requests (polling)

← Bad community requests (v2c)

← Total replies

← Traps generated

- Verifique a lista de controle de acesso (ACL) do FXOS. Isso é aplicável apenas nas plataformas FPR41xx/9300.

Se o tráfego for bloqueado pela ACL FXOS, você verá as solicitações, mas não verá nenhuma resposta:

```
<#root>
```

```
firepower(fxos)#
```

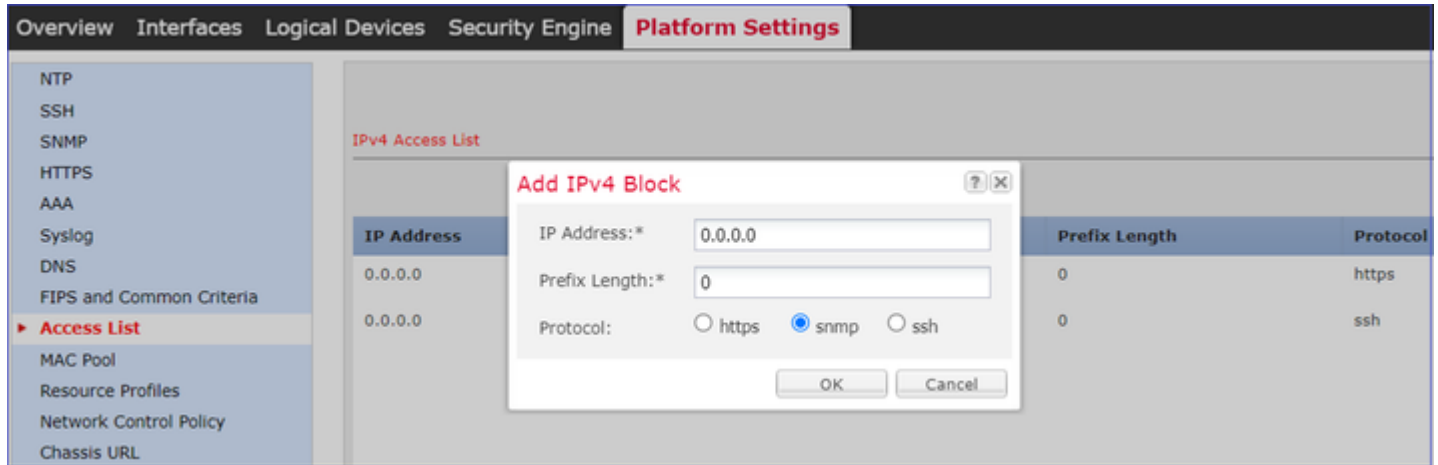
```
ethalyzer local interface mgmt capture-filter
```

```
"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
```

Você pode verificar a ACL do FXOS na interface do usuário:



Você também pode verificar a ACL do FXOS na 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
```

- Depuração do SNMP (somente pacotes). Aplicável somente no 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) - Esta saída de depuração é muito detalhada.

```
<#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 se há falhas do FXOS relacionadas ao 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 se há núcleos de snmpd:

```
No 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
```

No FPR1xxx/21xx:

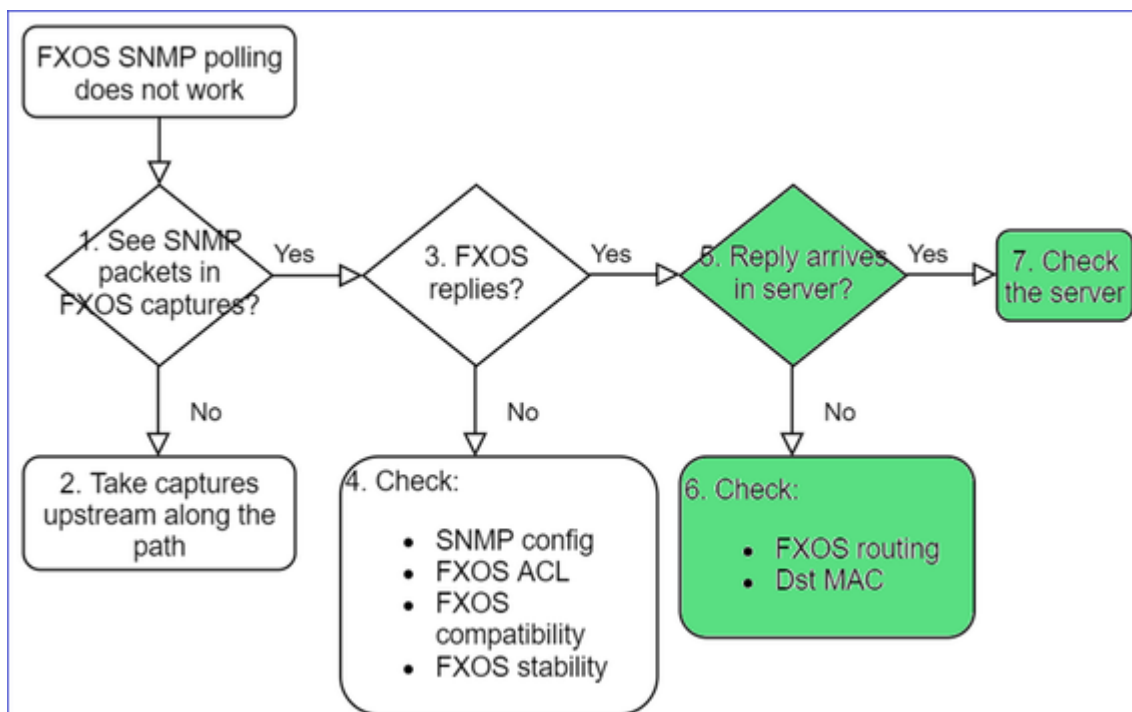
```
<#root>
```

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

```
dir cores_fxos
```

Se houver núcleos de snmpd, colete os núcleos juntamente com o pacote de solução de problemas do FXOS e entre em contato com o Cisco TAC.

5. A resposta SNMP chega ao servidor SNMP?



- Verifique o roteamento do FXOS

Esta saída é do 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

- Faça uma captura, exporte o pcap e verifique o dst MAC da resposta
- Por fim, verifique o servidor do SNMP (capturas, configuração, aplicação e assim por diante)

Quais valores de OID do SNMP devem ser usados?

Descrições dos problemas (exemplo de casos reais do Cisco TAC):

- "Queremos monitorar o equipamento Cisco Firepower. Forneça as OIDs do SNMP para cada CPU, memória e disco do núcleo"
- "Há OIDs que possam ser usadas para monitorar o status da fonte de alimentação no dispositivo ASA 5555?"
- "Queremos buscar a OID do SNMP do chassi no FPR 2K e no FPR 4K."
- "Queremos pesquisar o cache do ARP do ASA."
- "Precisamos saber a OID do SNMP para BGP peer inativo."

Como encontrar os valores de OID do SNMP

Estes documentos fornecem informações sobre as OIDs do SNMP nos dispositivos Firepower:

- White paper sobre o monitoramento do SNMP do Cisco Firepower Threat Defense (FTD):

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

- Guia de referência de MIB do FXOS do Cisco Firepower 4100/9300:

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

- Como procurar uma OID específica nas plataformas do 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>

- Verifique as OIDs do SNMP na 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 obter mais informações sobre as OIDs, consulte o SNMP Object Navigator

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

- No FXOS (41xx/9300), execute estes dois comandos na CLI do 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
```

```
...
```

Referência rápida de OIDs comuns

Requisitos	OID
CPU (LINA)	1.3.6.1.4.1.9.9.109.1.1.1
CPU (Snort)	1.3.6.1.4.1.9.9.109.1.1.1 (FP >= 6,7)
Memória (LINA)	1.3.6.1.4.1.9.9.221.1.1
Memória (Linux/FMC)	1.3.6.1.1.4.1.2021.4
Informações de HA	1.3.6.1.4.1.9.9.491.1.4.2
Informações de cluster	1.3.6.1.4.1.9.9.491.1.8.1

Informações de VPN	<p>Sessões de número RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.1 (7.x)</p> <p>Número de usuários de RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.3 (7.x)</p> <p>Sessões de pico de número RA-VPN: 1.3.6.1.4.1.9.9.392.1.3.41 (7.x)</p> <p>Sessões de número de VPN S2S: 1.3.6.1.4.1.9.9.392.1.3.29</p> <p>Sessões de pico de número de VPN S2S: 1.3.6.1.4.1.9.9.392.1.3.31</p> <p>- Dica: firepower# show snmp-server oid i ike</p>
Status de BGP	ID de bug ENH Cisco CSCux13512 :Adicionar o MIB do BGP para pesquisa do SNMP
Smart Licensing do ASA/ASAv do FPR1K/2K	ID de bug ENH da Cisco CSCvv83590 : ASAv/ASA no FPR1k/2k: precisa de OID SNMP para rastrear o status do Smart Licensing
OIDs do SNMP do LINA para port-channel no nível do FXOS	ID de bug ENH da Cisco CSCvu91544 :Suporte para OIDs do SNMP do LINA para estatísticas de interface do port-channel no nível do FXOS

FMC 7.3 Adições (para FMC 1600/2600/4600 e mais recente)

Requisitos	OID
Trava de status do ventilador	<p>OID de interceptação: 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.<índice></p> <p>0 - ventilador não está funcionando</p> <p>1 - o ventilador está funcionando</p>
armadilha de temperatura de CPU/PSU	<p>OID de interceptação: 1.3.6.1.4.1.9.9.91.2.0.1</p> <p>OID de limite: 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<índice>.1</p> <p>Valor OID: 1.3.6.1.4.1.9.9.91.1.1.1.1.4.<índice></p>
armadilha de status de PSU	<p>OID de interceptação: 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.<índice></p> <p>OID do status do administrador: 1.3.6.1.4.1.9.9.117.1.1.2.1.1.<índice></p>

	<p>0 - presença de fonte de alimentação não detectada</p> <p>1 - presença de fonte de alimentação detectada, ok</p>
--	---

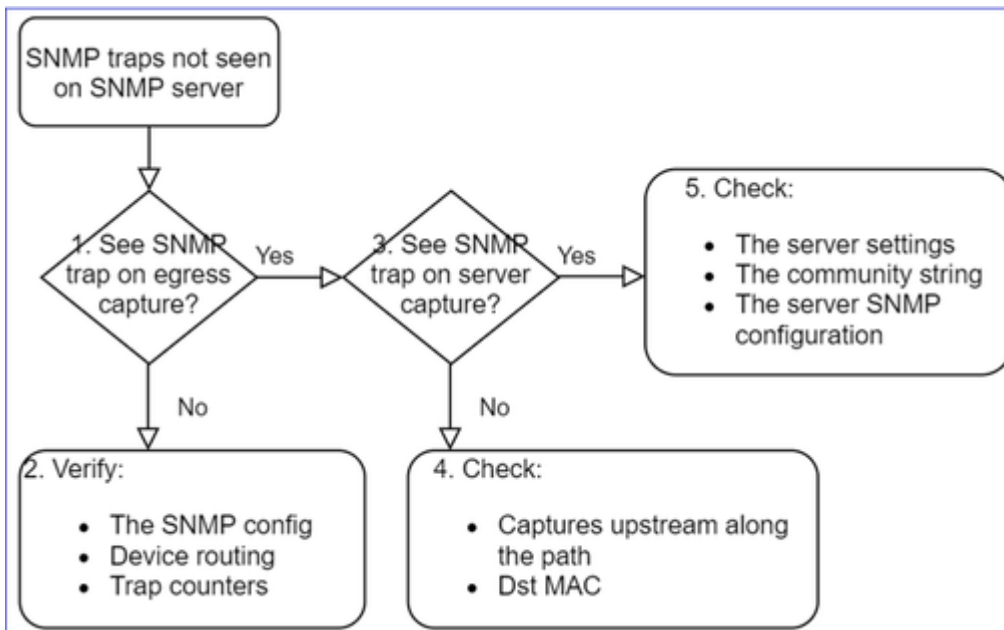
Não é possível obter as interceptações do SNMP

Descrições dos problemas (exemplo de casos reais do Cisco TAC):

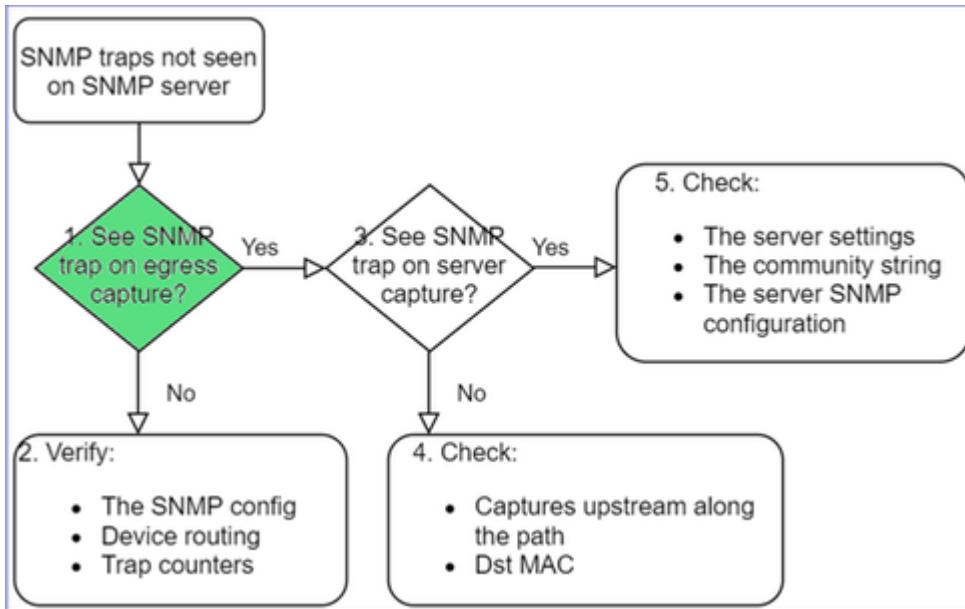
- "O SNMPv3 do FTD não envia interceptações para o servidor do SNMP."
- "O FMC e o FTD não enviam as mensagens de interceptação do SNMP."
- "Configuramos o SNMP no FTD 4100 para FXOS e tentamos usar o SNMPv3 e o SNMPv2, mas ambos não podem enviar interceptações."
- "O SNMP do Firepower não envia interceptações para a ferramenta de monitoramento."
- "O FTD do Firewall não envia a interceptação do SNMP para o NMS."
- "As interceptações do servidor do SNMP não funcionam."
- "Configuramos o SNMP no FTD 4100 para FXOS e tentamos usar o SNMPv3 e o SNMPv2, mas ambos não podem enviar interceptações."

Solução de problemas recomendada

Este é o processo para solucionar problemas de fluxograma para problemas de interceptação SNMP do Firepower:



1. Você vê interceptações SNMP na captura de saída?



Para capturar as interceptações do LINA/ASA na interface de gerenciamento:

```

<#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 as interceptações do LINA/ASA na interface de dados:

```

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

Para capturar as interceptações do FXOS (41xx/9300):

```

<#root>
firepower#
connect fxos
  
```

```

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

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

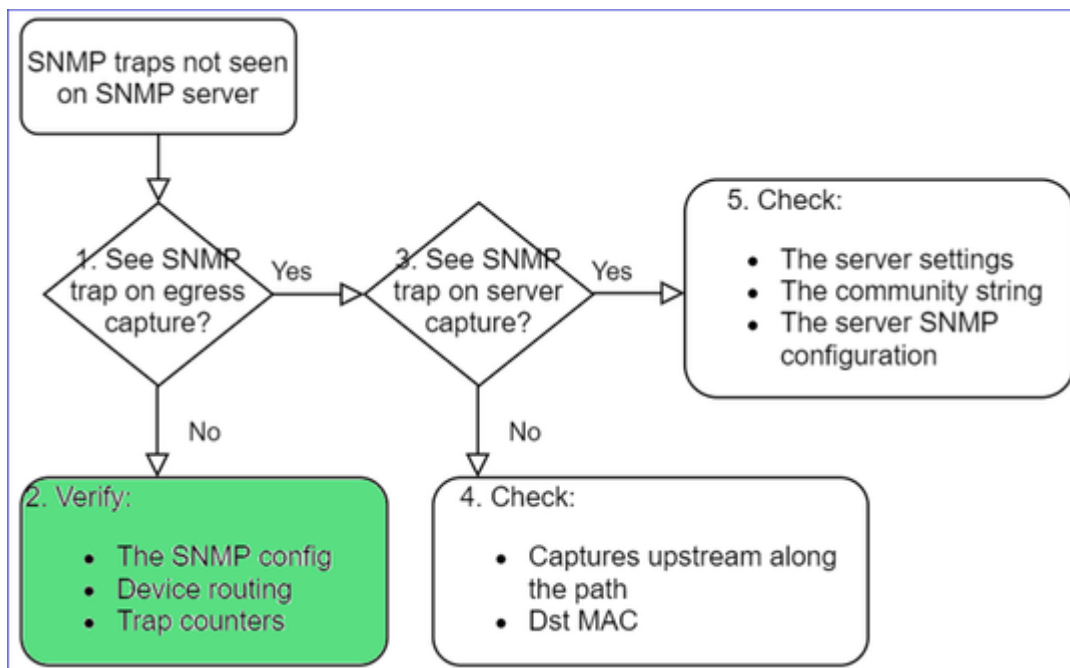
firepower#
connect local-mgmt

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. Se você não vir pacotes na interface de saída



<#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

```

Configuração de interceptações do SNMP do 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

Observação: em 1xxx/21xx, você verá essas configurações somente no caso de **Devices > Device Management > SNMP** config!

- Roteamento do LINA/ASA para interceptações através da interface de gerenciamento:

```
<#root>
```

```
>
```

```
show network
```

- Roteamento do LINA/ASA para interceptações através da interface de dados:

```
<#root>
```

```
firepower#
```

```
show route
```

- Roteamento do FXOS (41xx/9300):

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- Contadores de interceptação (LINA/ASA):

```
<#root>
```

```
firepower#
```

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

20 Trap PDUs

E FXOS:

```
<#root>
```

```
FP4145-1#
```

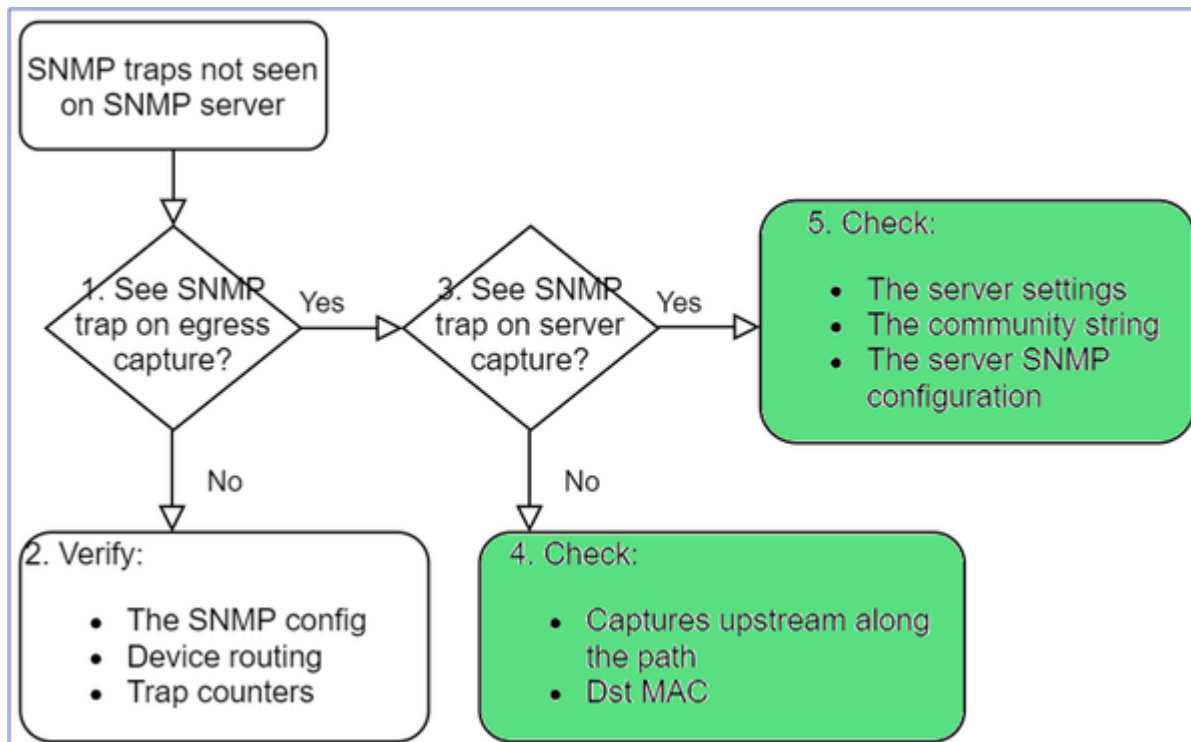
```
connect fxos
```

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

```
show snmp | grep Trap
```

1296 Out Traps PDU

Verificações adicionais



- Faça uma captura no servidor do SNMP de destino.

Outras questões a verificar:

- Capturas ao longo do caminho.
- Endereço MAC de destino dos pacotes de interceptação do SNMP.
- As configurações e o status do servidor SNMP (por exemplo, firewall, portas abertas etc.).
- A string de comunidade do SNMP.

- A configuração do servidor do SNMP.

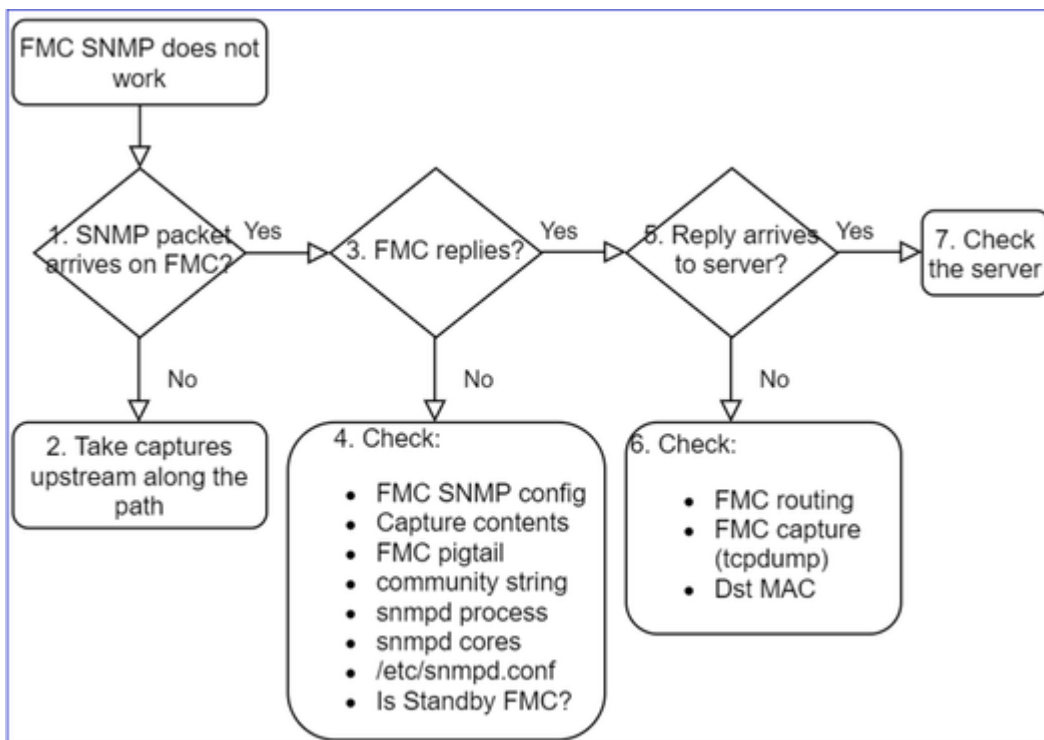
Não é possível monitorar o FMC usando o SNMP

Descrições dos problemas (exemplo de casos reais do Cisco TAC):

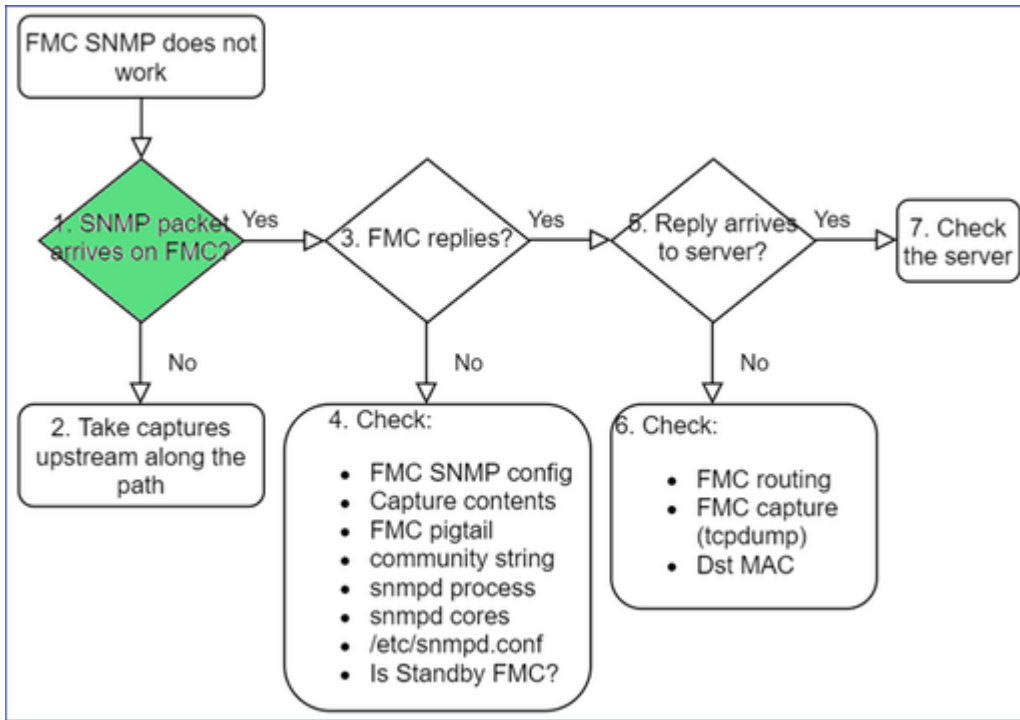
- "O SNMP não funciona no FMC em standby."
- "Precisa monitorar a memória do FMC."
- "O SNMP deve funcionar no FMC 192.168.4.0.8 em standby?"
- "Temos que configurar as FMCs para monitorar seus recursos, como CPU, memória etc."

Como solucionar problemas

Este é o processo para solucionar problemas do fluxograma do FMC SNMP:



1. O pacote SNMP chega ao FMC?



- Capture na interface de gerenciamento do 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.
```

Dica: salve a captura no diretório FMC /var/common/ e baixe-a da interface do usuário do FMC

<#root>

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

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

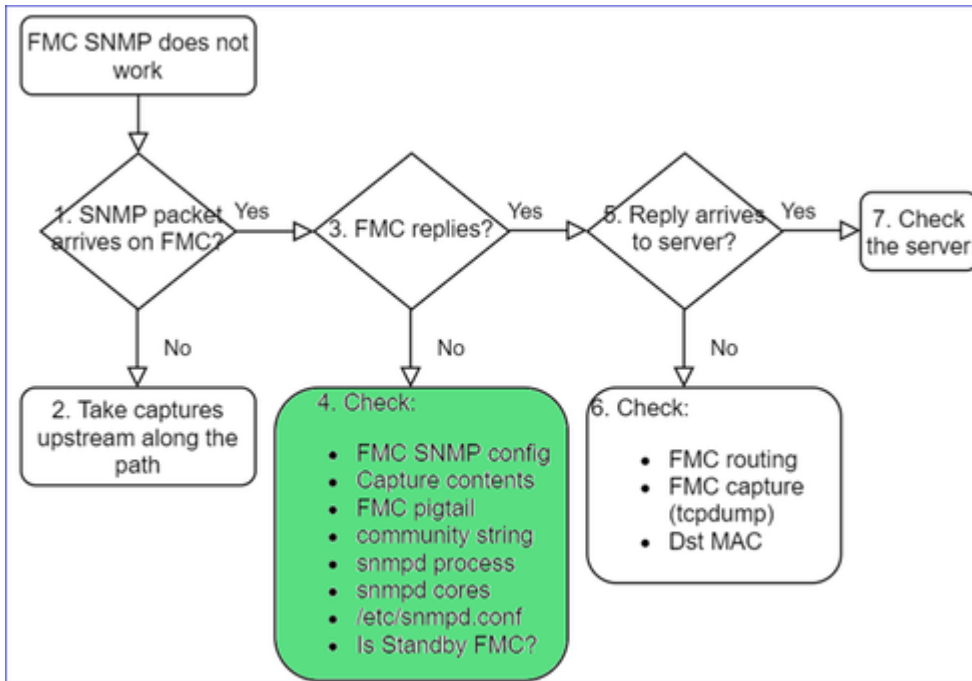
```
HS_PACKET_BUFFER_SIZE is set to 4.
```

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

```
^C46 packets captured
```

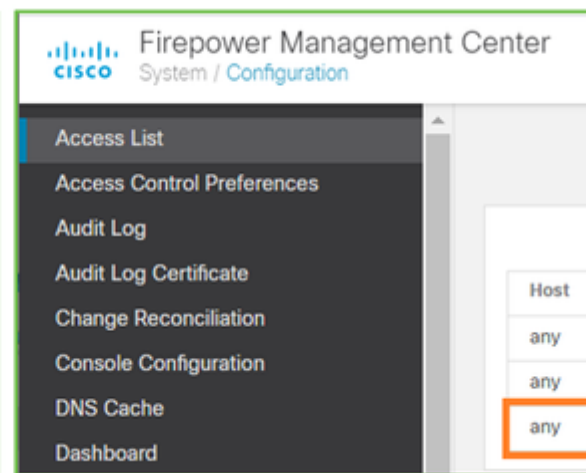
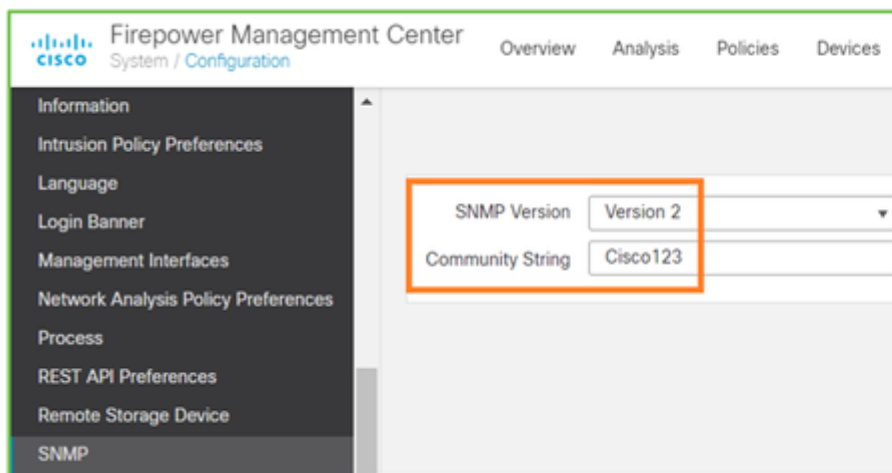
```
46 packets received by filter
```

O FMC responde?



Se o FMC não responder, verifique:

- Configuração do SNMP do FMC (Sistema > Configuração)
 1. Seção SNMP
 2. Seção Lista de acesso



Se o FMC não responder, verifique:

- Conteúdo da captura (pcap)
- String de comunidade (pode ser vista nas capturas)
- Saída de rabinho do FMC (procure erros, falhas, rastreamentos) e conteúdo de /var/log/snmpd.log
- snmpd process

```
<#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
```

- snmpd cores

```
<#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
```

- Arquivo de configuração de back-end em /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
```

Observação: se o SNMP estiver desativado, o arquivo snmpd.conf não existirá

- É um FMC em standby?

Nas versões anteriores a 6.4.0-9 e anteriores a 6.6.0, o FMC em standby não envia os dados do SNMP (o snmpd está no status Aguardando). Este é um comportamento esperado. Verificar aprimoramento ID de erro da Cisco [CSCvs32303](#)

Não é possível configurar o SNMP

Descrições dos problemas (exemplo de casos reais do Cisco TAC):

- "Queremos configurar o SNMP para Cisco Firepower Management Center e Firepower 4115 Threat Defense."
- "Suporte com configuração SNMP em FTD".
- "Queremos ativar o monitoramento do SNMP no meu dispositivo do FTD."
- "Tentamos configurar o serviço do SNMP no FXOS, mas o sistema não deixa executar o commit-buffer no final. Ela diz Erro: alterações não permitidas. use 'Connect ftd' para fazer alterações."
- "Queremos ativar o monitoramento do SNMP no nosso dispositivo do FTD."
- "Não é possível configurar o SNMP no FTD e descobrir o dispositivo no monitoramento."

Como abordar os problemas de configuração do SNMP

Primeiras Coisas Primeiro: Documentação!

- Leia o documento atual.
- Guia de configuração do FMC:

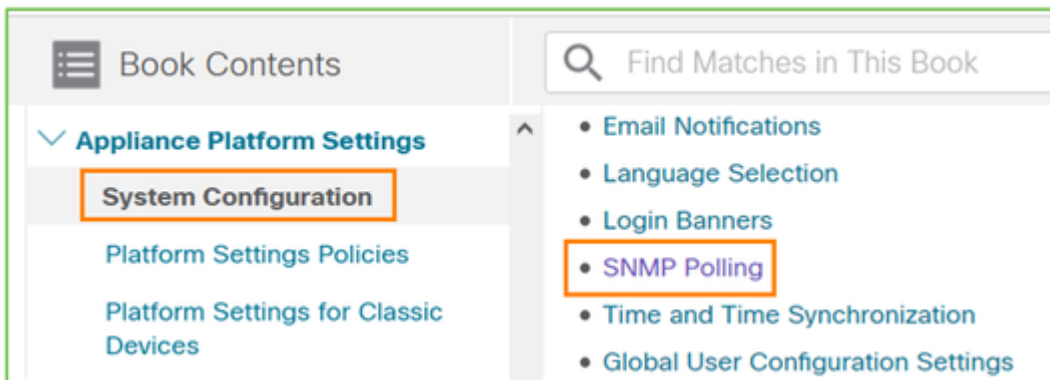
<https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html>

- Guia de configuração do FXOS:

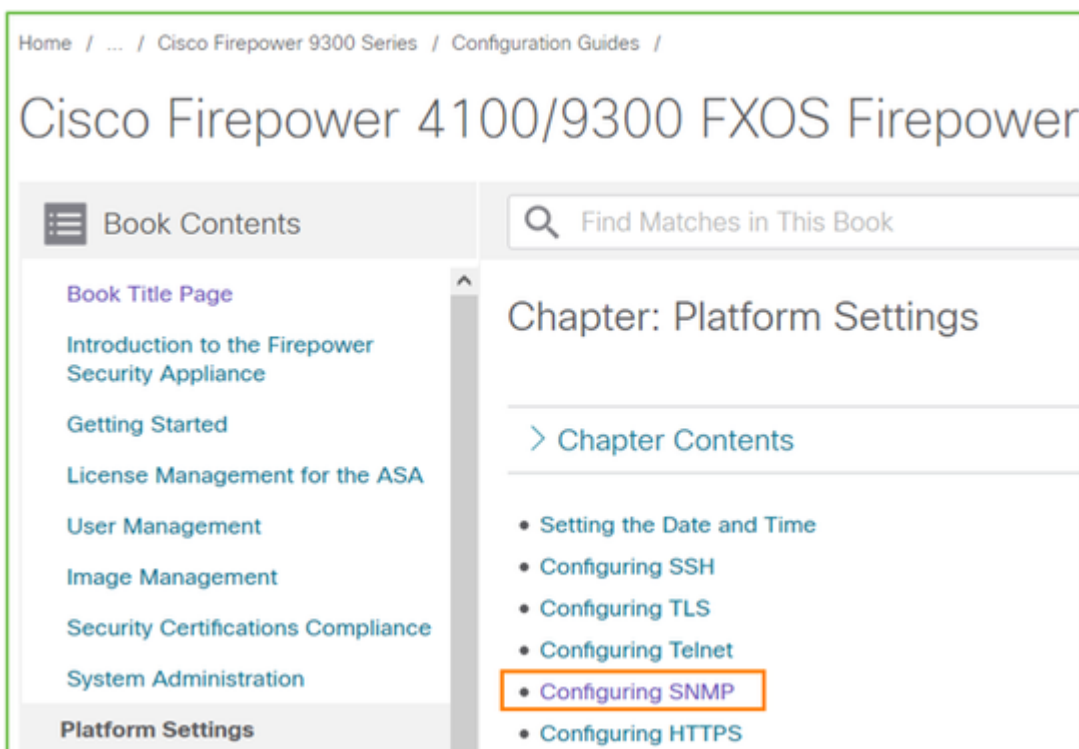
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB115F5

Tome conhecimento dos vários documentos do SNMP.

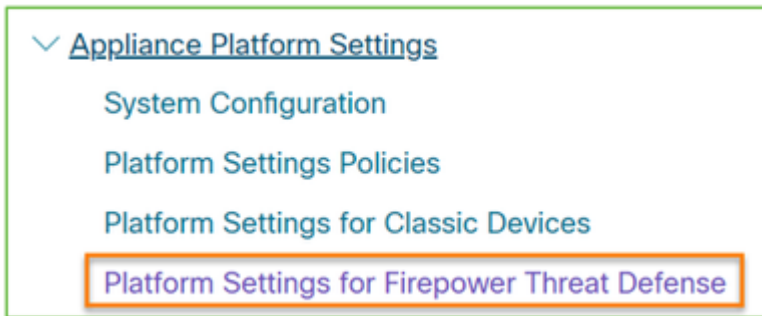
SNMP do FMC:



SNMP do FXOS:



Configuração do SNMP do Firepower 41xx/9300:



Configuração do SNMP do Firepower 1xxx/21xx:



Configuração do SNMP no Firepower Device Manager (FDM)

Descrições dos problemas (exemplo de casos reais do Cisco TAC):

- "Precisamos de orientação sobre o SNMPv3 no dispositivo Firepower com o FDM."
- "A configuração do SNMP não funciona no dispositivo FPR 2100 no FDM."
- "Não é possível fazer com que a configuração do SNMP v3 funcione no FDM."
- "FDM 6.7 SNMP Configuration Assistance."
- "Ativar o SNMP v3 no Firepower FDM."

Como abordar os problemas de configuração do SNMP do FDM

- Para versões anteriores a 6.7, é possível fazer a configuração do SNMP usando o 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 do Firepower versão 6.7, a configuração do SNMP não é mais feita com o FlexConfig, mas com a API REST:

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

Dicas de solução de problemas do SNMP

1xxx/21xx/41xx/9300 (LINA/ASA) – O que coletar antes de abrir um caso com o Cisco TAC

Comando	Descrição
---------	-----------

firepower# show run snmp-server	Verificar a configuração do SNMP do LINA do ASA/FTD.
firepower# show snmp-server statistics	Verifique as estatísticas do SNMP no LINA do ASA/FTD. Concentre-se nos contadores de entrada e saída de pacotes do SNMP.
> capture-traffic	Capture o tráfego na interface de gerenciamento.
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	Capturar o tráfego na interface de dados (nomeif $\hat{\sim}$ net201 $\hat{\sim}$ ™) para UDP 161 (poll SNMP).
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	Capturar o tráfego na interface de dados (nome $\hat{\sim}$ net208 $\hat{\sim}$ ™) para UDP 162. (interceptações SNMP).
firepower# show capture SNMP-POLL packet-number 1 trace	Rastreie um pacote SNMP de entrada que chega à interface de dados ASA/FTD LINA.
admin@firepower:~\$ sudo tcpdump -i tap_nlp	Capturar na interface de toque interna NLP (Non-Line Process).
firepower# show conn all protocol udp port 161	Verifique todas as conexões LINA ASA/FTD no UDP 161 (pesquisa SNMP).
firepower# show log i 302015.*161	Verifique o registro 302015 do LINA do ASA/FTD para pesquisa do SNMP.
firepower# more system:running-config i community	Verifique a string de comunidade do SNMP.
firepower# debug menu netsnmp 4	Verifique a configuração do SNMP e a ID do processo.
firepower# show asp table classify interface net201 domain permit match port=161	Verifique as contagens de ocorrências na ACL de SNMP na interface chamada $\hat{\sim}$ net201 $\hat{\sim}$ ™.
firepower# show disk0: i core	Verifique se há núcleos do SNMP.
admin@firepower:~\$ ls -l /var/data/cores	Verifique se há núcleos do SNMP. Aplicável somente no FTD.

firepower# show route	Verifique a tabela de roteamento do LINA do ASA/FTD.
> show network	Verifique a tabela de roteamento do plano de gerenciamento do FTD.
admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	Verifique/solucione problemas do SNMPv3 no FTD.
firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	Comandos ocultos nas versões mais recentes. Depurações internas, úteis para solucionar problemas do SNMP com o Cisco TAC.

41xx/9300 (FXOS) – O que coletar antes de abrir um caso com o Cisco TAC

Comando	Descrição
firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 161" limit-captured-frames 50 write workspace:///SNMP-POLL.pcap firepower(fxos)# exit firepower# connect local-mgmt firepower(local-mgmt)# dir 1 11152 Jul 26 09:42:12 2021 SNMP.pcap firepower(local-mgmt)# copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap	Captura do FXOS para pesquisa do SNMP (UDP 161) Carregue em um servidor remoto do FTP IP FTP: 192.0.2.100 Nome de usuário do FTP: ftp
firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap	Captura do FXOS para interceptações do SNMP (UDP 162)
firepower# scope system firepower /system # scope services	Verifique a ACL do FXOS

firepower /system/services # show ip-block detail	
firepower# show fault	Verifique se há falhas do FXOS
firepower# show fabric-interconnect	Verifique a configuração de interface e as configurações de gateway padrão do FXOS
firepower# connect fxos firepower(fxos)# show running-config snmp all	Verifique a configuração do SNMP do FXOS
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	Verifique as OIDs do SNMP do FXOS
firepower# connect fxos firepower(fxos)# show snmp	Verifique as configurações e os contadores do SNMP do FXOS
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	Depuração do SNMP do FXOS ('packets' ou 'all') Use 'terminal no monitor' e 'undebug all' para pará-lo

1xxx/21xx (FXOS) – O que coletar antes de abrir um caso com o Cisco TAC

Comando	Descrição
> capture-traffic	Capture o tráfego na interface de gerenciamento
> show network	Verifique a tabela de roteamento do plano de gerenciamento do FTD
firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail]	Verifique a configuração do SNMP do FXOS

firepower /monitoring # show snmp-trap	
firepower# show fault	Verifique se há falhas do FXOS
firepower# connect local-mgmt firepower(local-mgmt)# dir cores_fxos firepower(local-mgmt)# dir cores	Verifique se há arquivos de núcleo do FXOS (tracebacks)

FMC “ O que coletar antes de abrir um caso com o Cisco TAC

Comando	Descrição
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n	Capture o tráfego na interface de gerenciamento para pesquisa do SNMP
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	Capture o tráfego na interface de gerenciamento para pesquisa do SNMP e salve-o em um arquivo
admin@FS2600-2:~\$ sudo pmtool status grep snmpd	Verifique o status de processo do SNMP
admin@FS2600-2:~\$ ls -al /var/common grep snmpd	Verifique se há arquivos de núcleo do SNMP (tracebacks)
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	Verifique o conteúdo do arquivo de configuração do SNMP

Exemplos de snmpwalk

Estes comandos podem ser usados para verificação e solução de problemas:

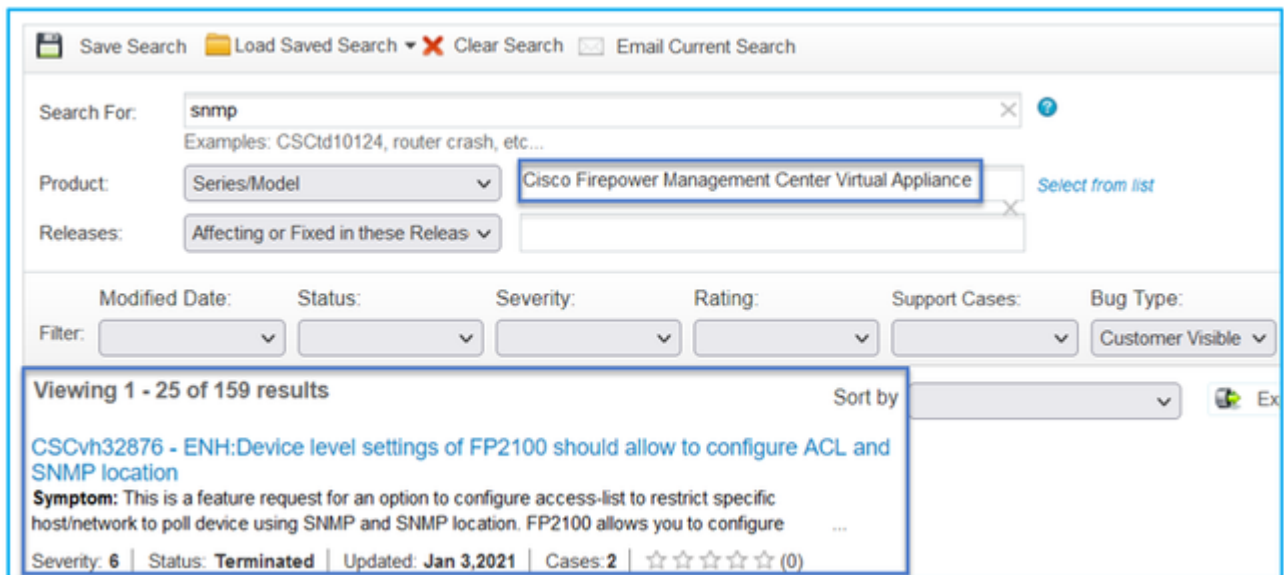
Comando	Descrição
# snmpwalk -c Cisco123 -v2c 192.0.2.1	Busca todas as OIDs no host remoto usando o SNMP v2c. Cisco123 = string de comunidade 192.0.2.1 = host de destino
# snmpwalk -v2c -c Cisco123 -OS 192.0.2.1	Busca uma OID específica no host remoto

10.3.1.1.4.1.9.9.109.1.1.1.1.3 iso.3.6.1.4.1.9.9.109.1.1.1.1.3.1 = Medidor32: 0	usando o SNMP v2c
# snmpwalk -c Cisco123 -v2c 192.0.2.1 .10.3.1.1.4.1.9.9.109.1.1.1.1.1 -On .10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 = Medidor32: 0	Mostra as OIDs buscadas no formato numérico
# snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1	Busca todas as OIDs no host remoto usando o SNMP v3. Usuário do SNMPv3 = cisco Autenticação do SNMPv3 = SHA. Autorização do SNMPv3 = AES
# snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -x AES -X Cisco123 192.0.2.1	Busca todas as OIDs no host remoto usando o SNMP v3 (MD5 e AES128)
# snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1	Somente SNMPv3 com autenticação

Como procurar defeitos do SNMP

1. Navegue até <https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV>
2. Insira a palavra-chave **snmp** e escolha **Selecionar na lista**.

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



Save Search Load Saved Search Clear Search Email Current Search

Search For: Examples: CSCtd10124, router crash, etc...

Product: [Select from list](#)

Releases:

Modified Date: Status: Severity: Rating: Support Cases: Bug Type: Customer Visible

Filter:

Viewing 1 - 25 of 159 results Sort by

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)

Produtos mais comuns:

- Software do Cisco Adaptive Security Appliance (ASA)
- Cisco Firepower 9300 Series
- Cisco Firepower Management Center Virtual Appliance
- Cisco Firepower NGFW

Informações Relacionadas

- [Configurar o SNMP para defesa contra ameaças](#)
- [Configurar SNMP em FXOS \(UI\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.