firepowerNGFWアプライアンスでのSNMPの設定

内容

はじめに

このドキュメントでは、Next Generation Firewall(NGFW)FTDアプライアンスでSimple Network Management Protocol(SNMP)を設定し、トラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントには、SNMP プロトコルの基本的な知識が必要です。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Firepower NGFW アプライアンスは、2 つの主要なサブシステムに分割できます。

- Firepower Extensible Operative System（FX-OS）は、シャーシハードウェアを制御します。
- Firepower Threat Defense（FTD）はモジュール内で実行されます。

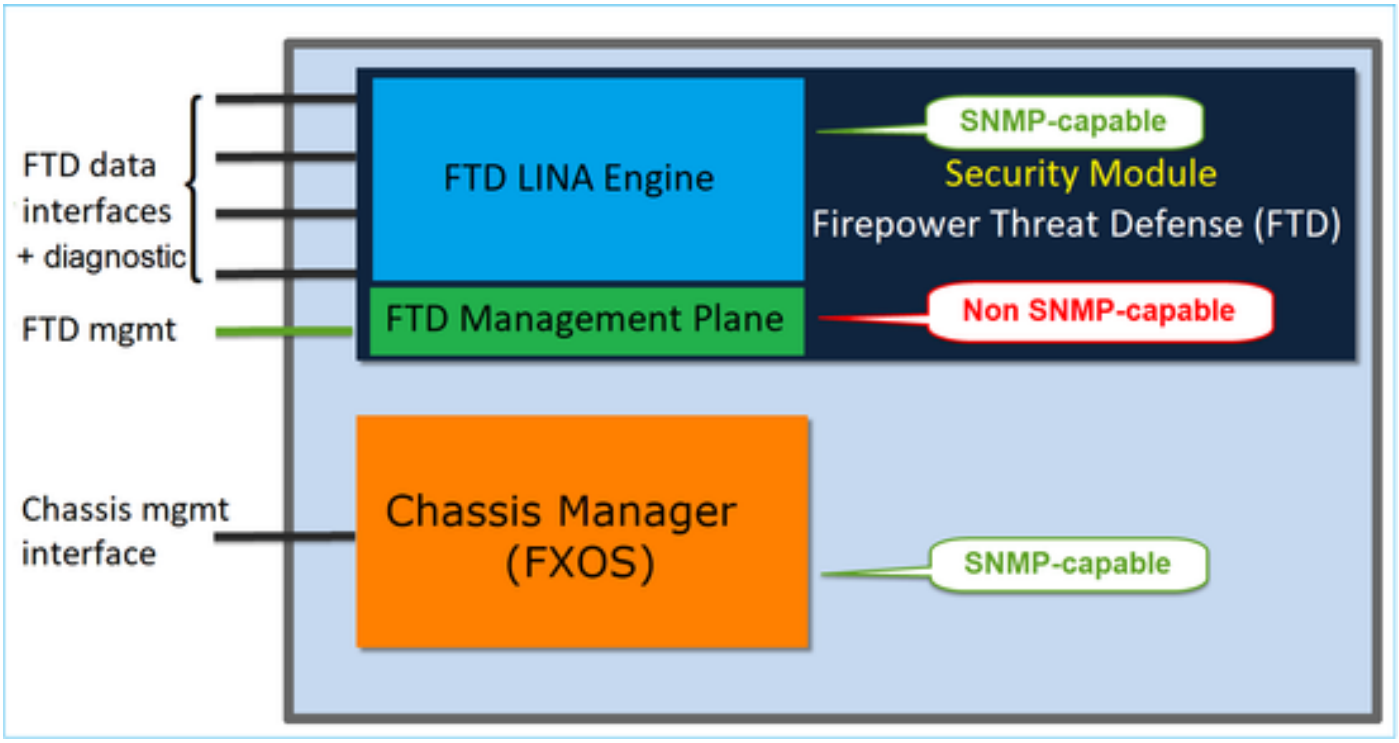
FTDは、2つのメインエンジン、Snortエンジン、およびLINAエンジンで構成される統合ソフトウェアです。 FTDの現在のSNMPエンジンは従来のASAから派生しており、LINA関連の機能を表示できます。

FX-OSとFTDは独立したコントロールプレーンを持ち、モニタの目的で異なるSNMPエンジンを使用します。各SNMPエンジンは異なる情報を提供するため、両方をモニタしてデバイスのステータスをより包括的に確認する必要があります。

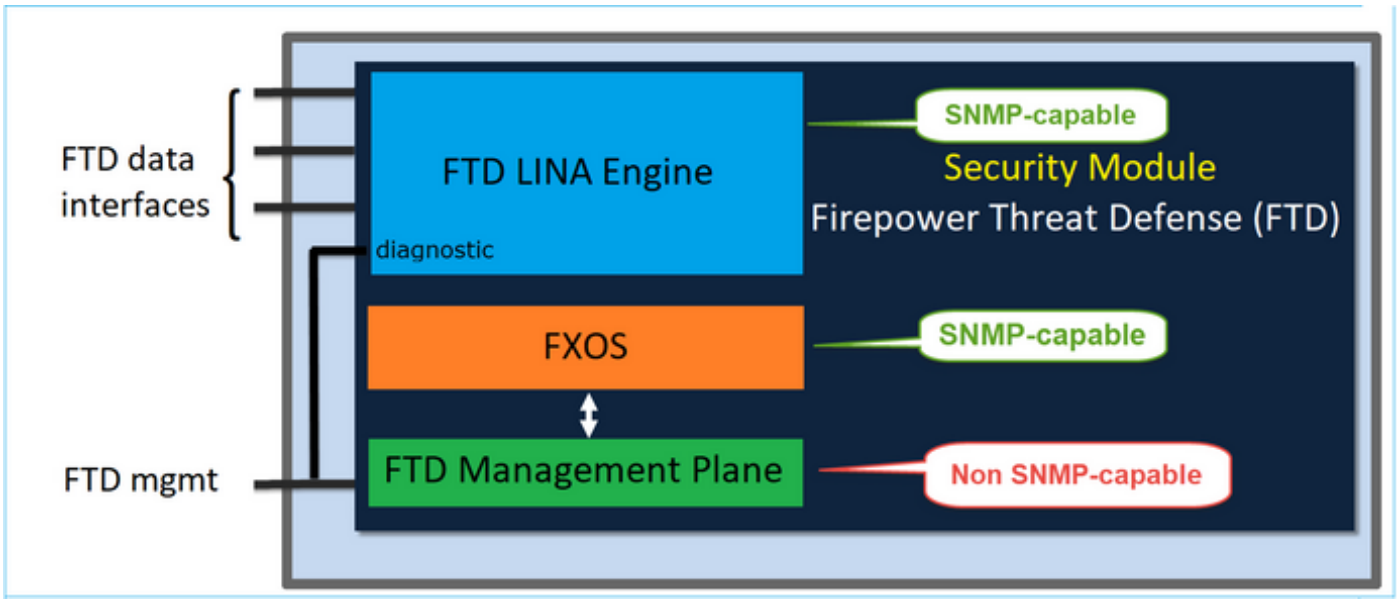
ハードウェアの観点から見ると、FirepowerNGFWアプライアンスには現在、Firepower2100シリーズとFirepower4100/9300シリーズの2つの主要なアーキテクチャがあります。

Firepower 4100/9300 デバイスには、デバイス管理用の専用インターフェイスがあり、これが FXOS サブシステム宛ての SNMP トラフィックの送信元および宛先です。一方、FTD アプリケ

ーションは LINA インターフェイス (データおよび/または diagnostic。6.6 以降の FTD リリースでは、FTD 管理インターフェイスも使用可能) を使用して SNMP 構成を行います。



Firepower 2100 アプライアンスの SNMP エンジンは、FTD 管理インターフェイスと IP を使用します。アプライアンス自体は、このインターフェイスで受信した SNMP トラフィックをブリッジし、FXOS ソフトウェアに転送します。

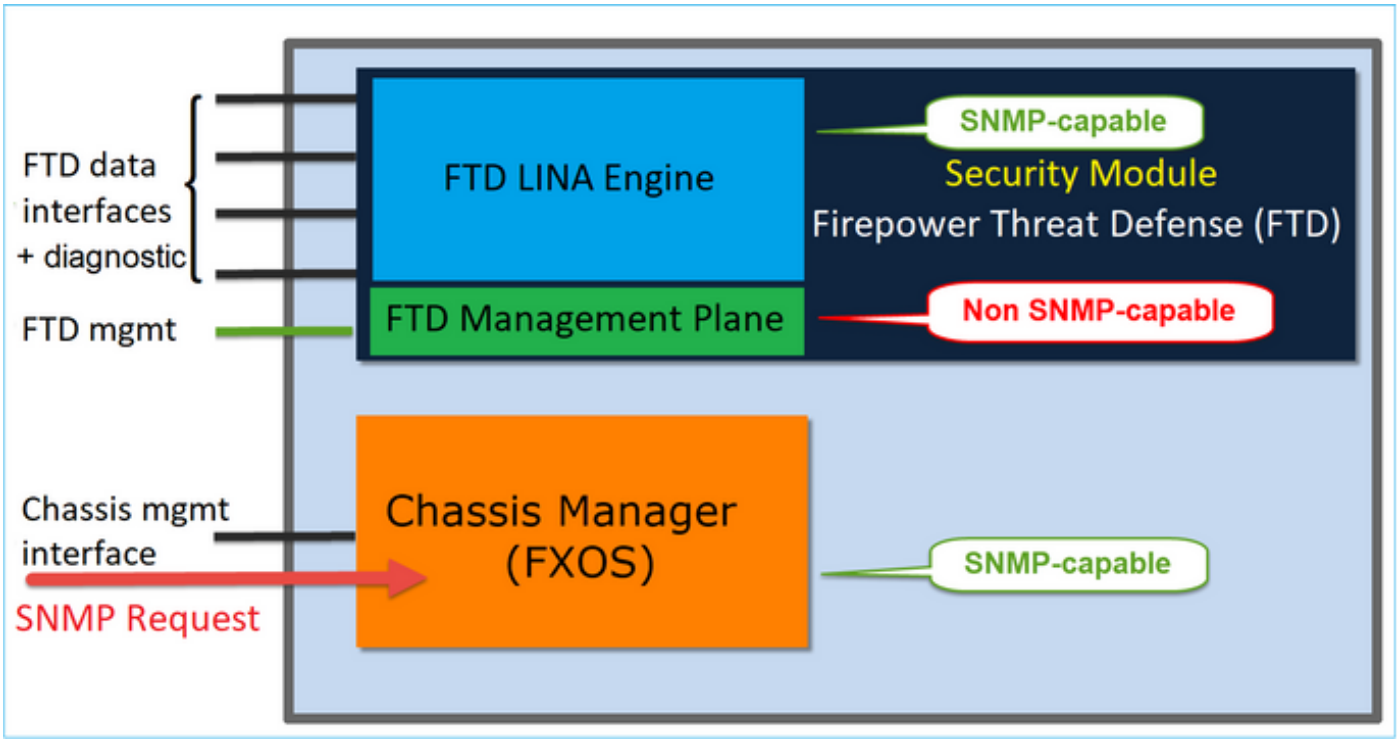


ソフトウェアリリース 6.6 以降を使用する FTD では、次の変更が導入されました。

- 管理インターフェイス上の SNMP。
- FPR1000 または FPR2100 シリーズ プラットフォームでは、この単一の管理インターフェイス上で LINA SNMP と FXOS SNMP の両方を統合します。さらに、[Platform settings] > [SNMP] の下にある FMC に単一の構成ポイントを提供します。

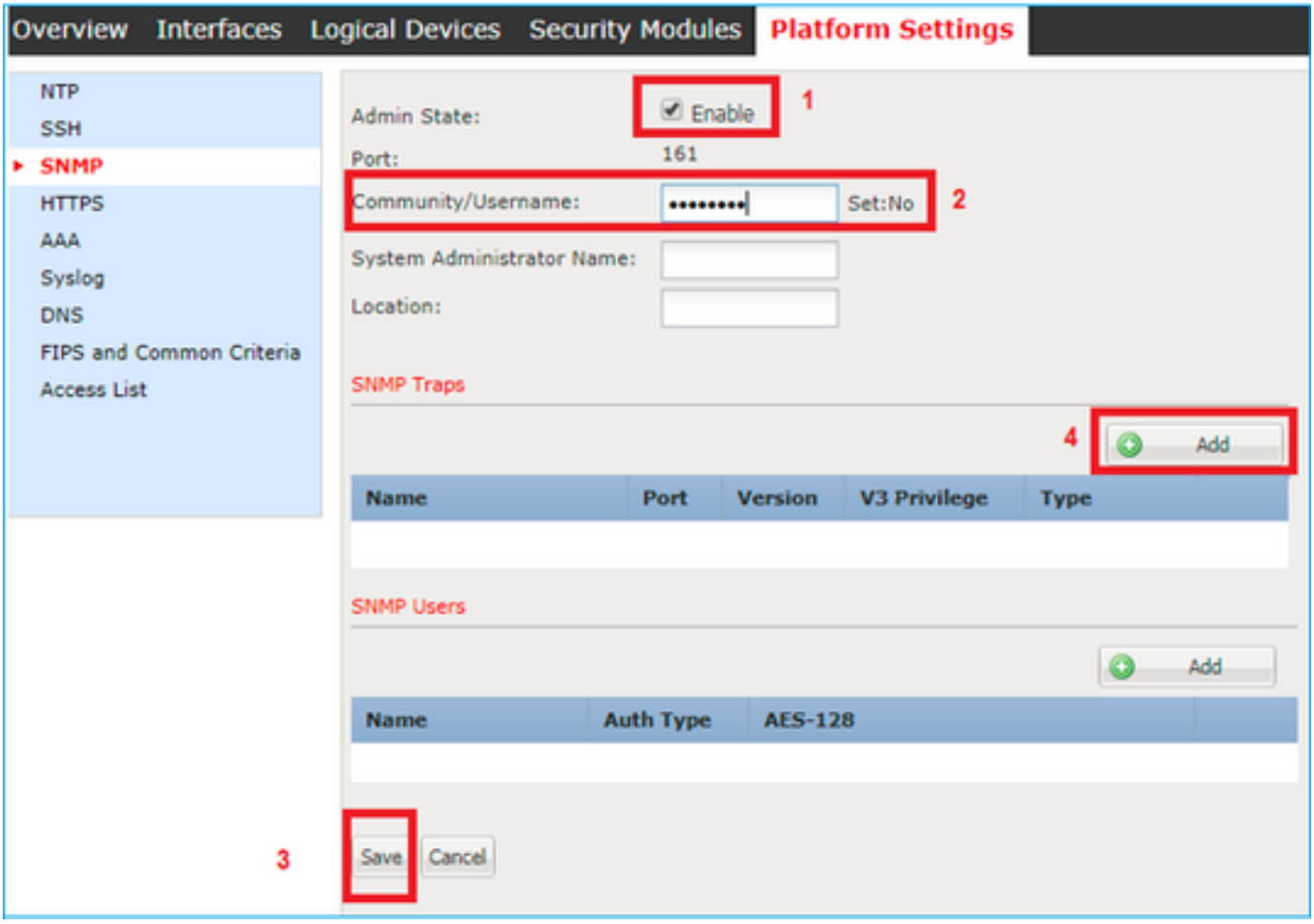
設定

FPR4100/FPR9300 のシャーシ（FXOS）SNMP



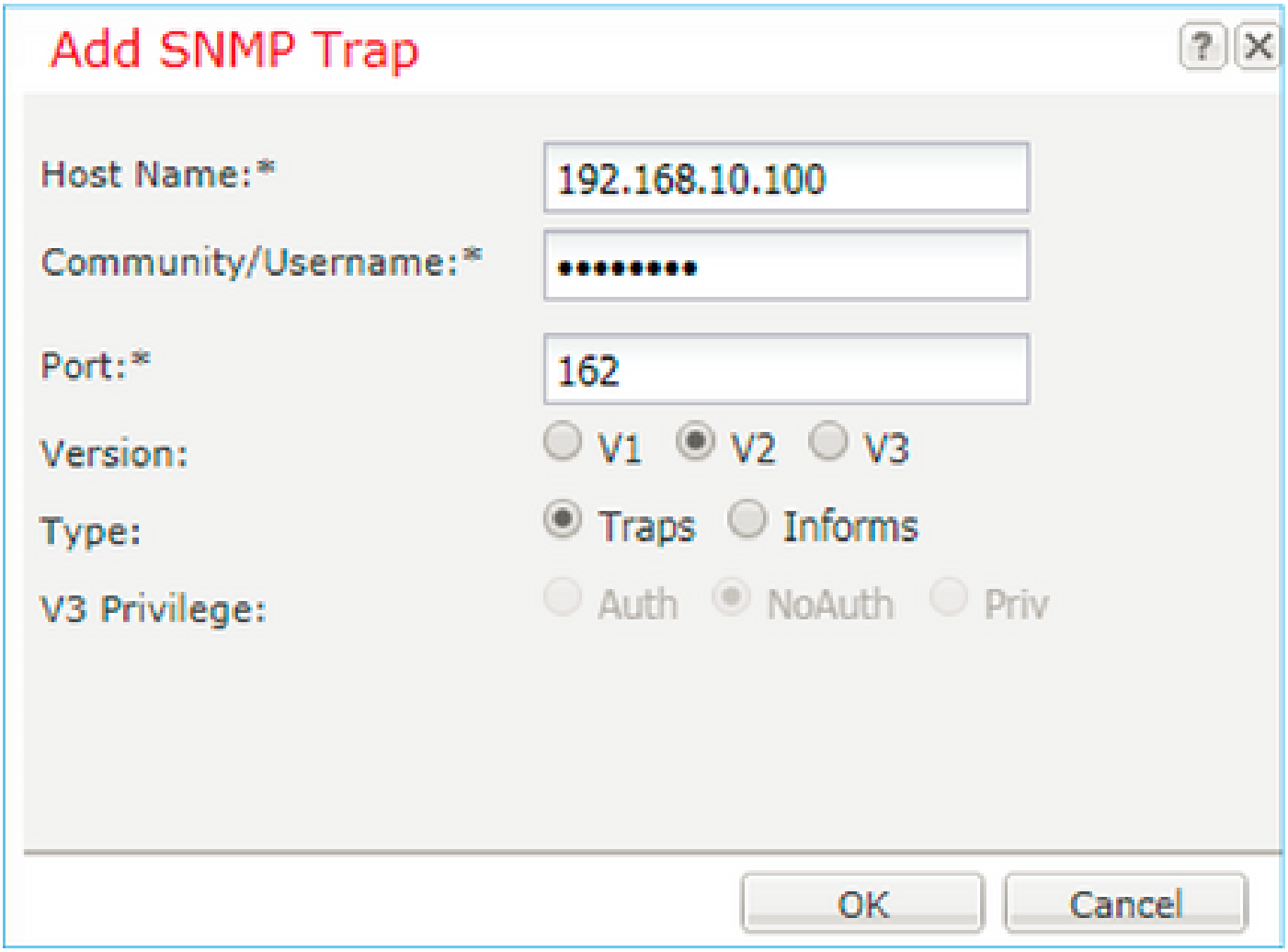
GUI による FXOS SNMPv1/v2c の構成

ステップ 1：firepower Chassis Manager(FCM)UIを開き、Platform Settings > SNMPタブに移動します。SNMP の有効化ボックスをチェックし、SNMP 要求で使用するコミュニティストリングを指定して、保存します。



注:Community/Usernameフィールドがすでに設定されている場合、空のフィールドの右側にあるテキストはSet: Yesです。Community/Usernameフィールドに値が入力されていない場合、空のフィールドの右側にあるテキストはSet: Noになります

ステップ 2：SNMPトラップの宛先サーバを設定します。



注：クエリとトラップホストのコミュニティ値は独立しており、異なる場合があります

ホストは、IP アドレスまたは名前で定義できます。[OK] を選択すると、SNMP トラップサーバーの構成が自動的に保存されます。SNMP メインページから保存ボタンを選択する必要はありません。ホストを削除する場合も同様です。

コマンド ライン インターフェイス (CLI) による FXOS SNMPv1/v2c の構成

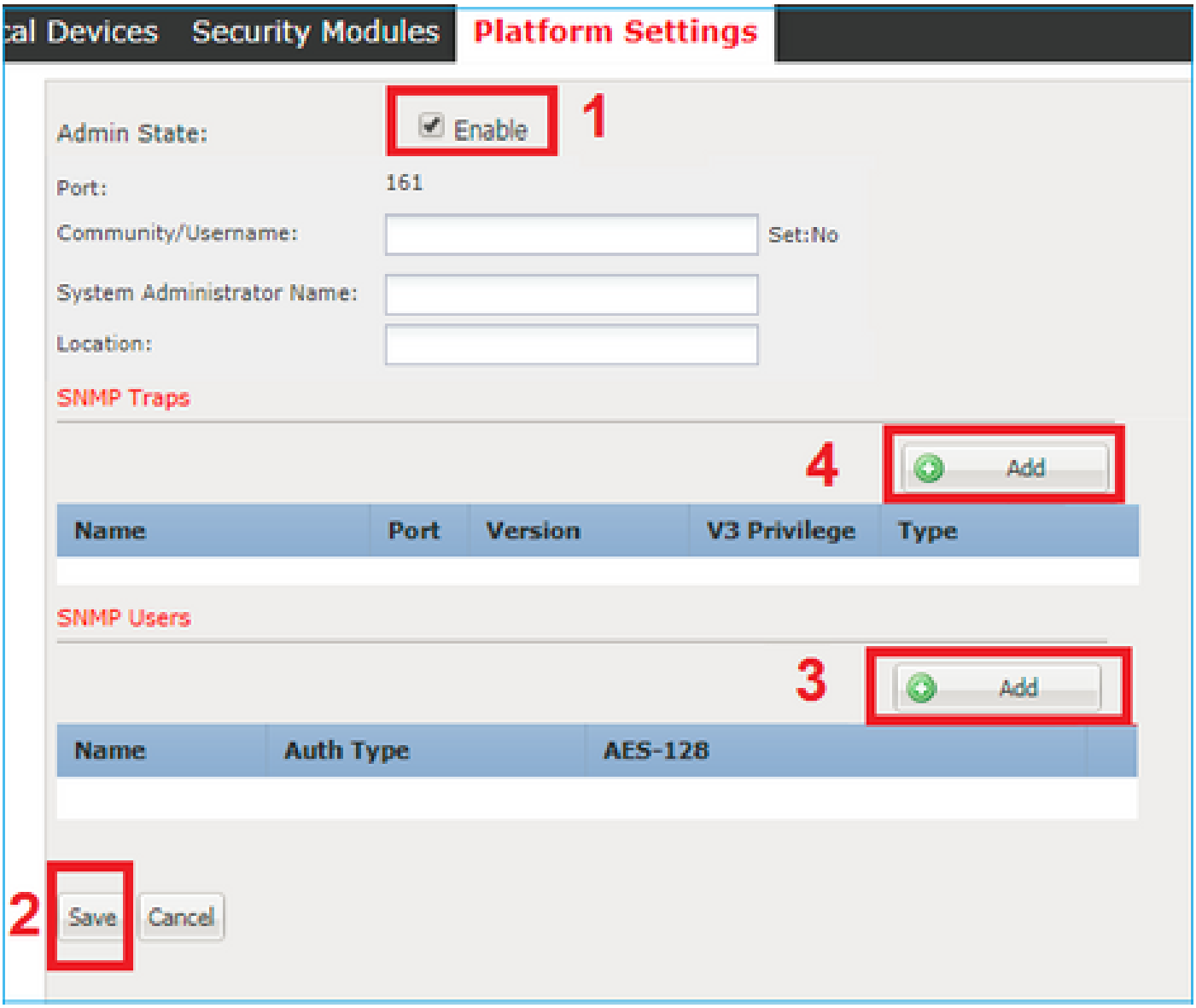
```
<#root>

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
```

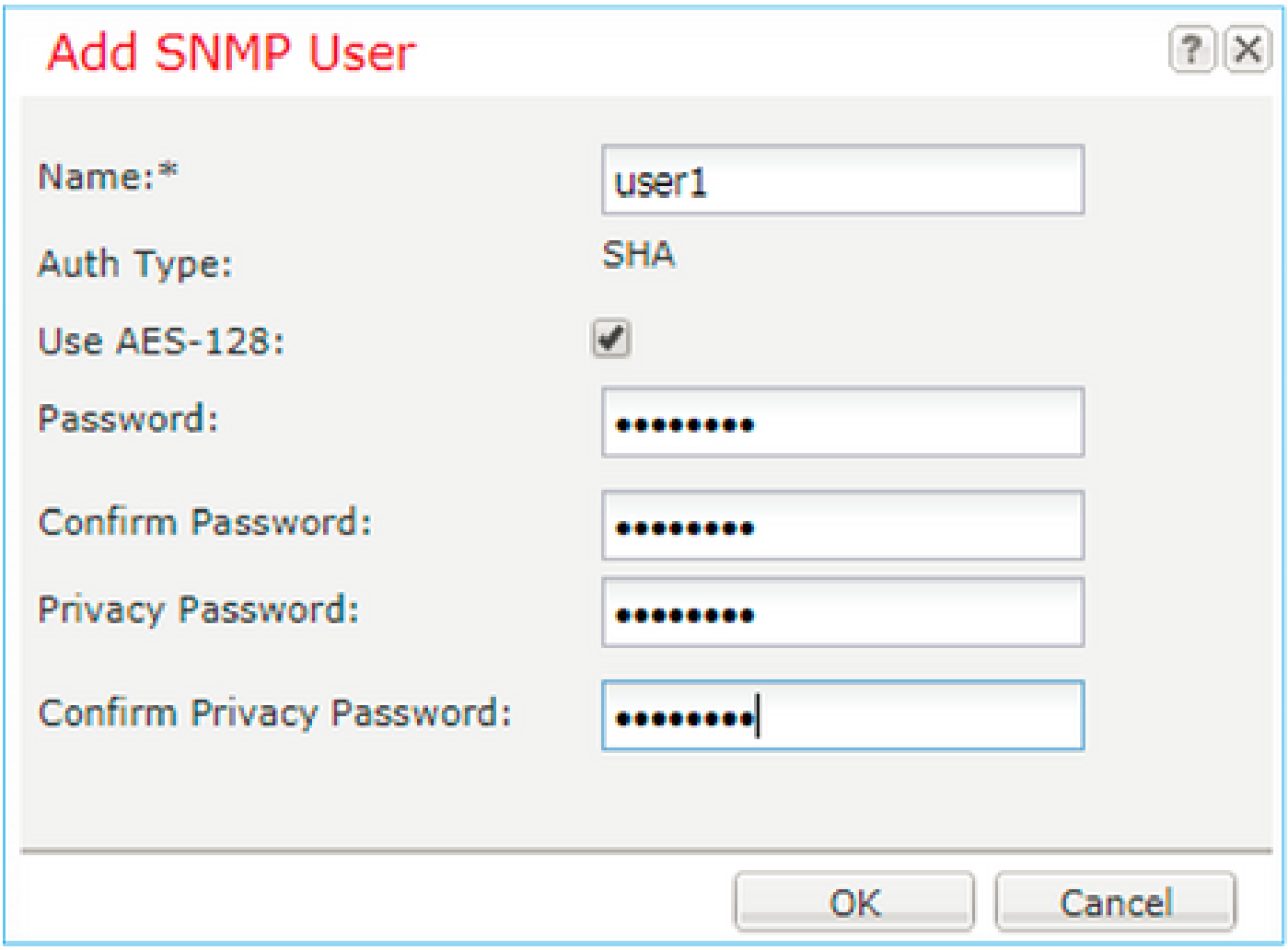
GUI による FXOS SNMPv3 の構成

ステップ 1：FCMを開き、Platform Settings > SNMPタブに移動します。

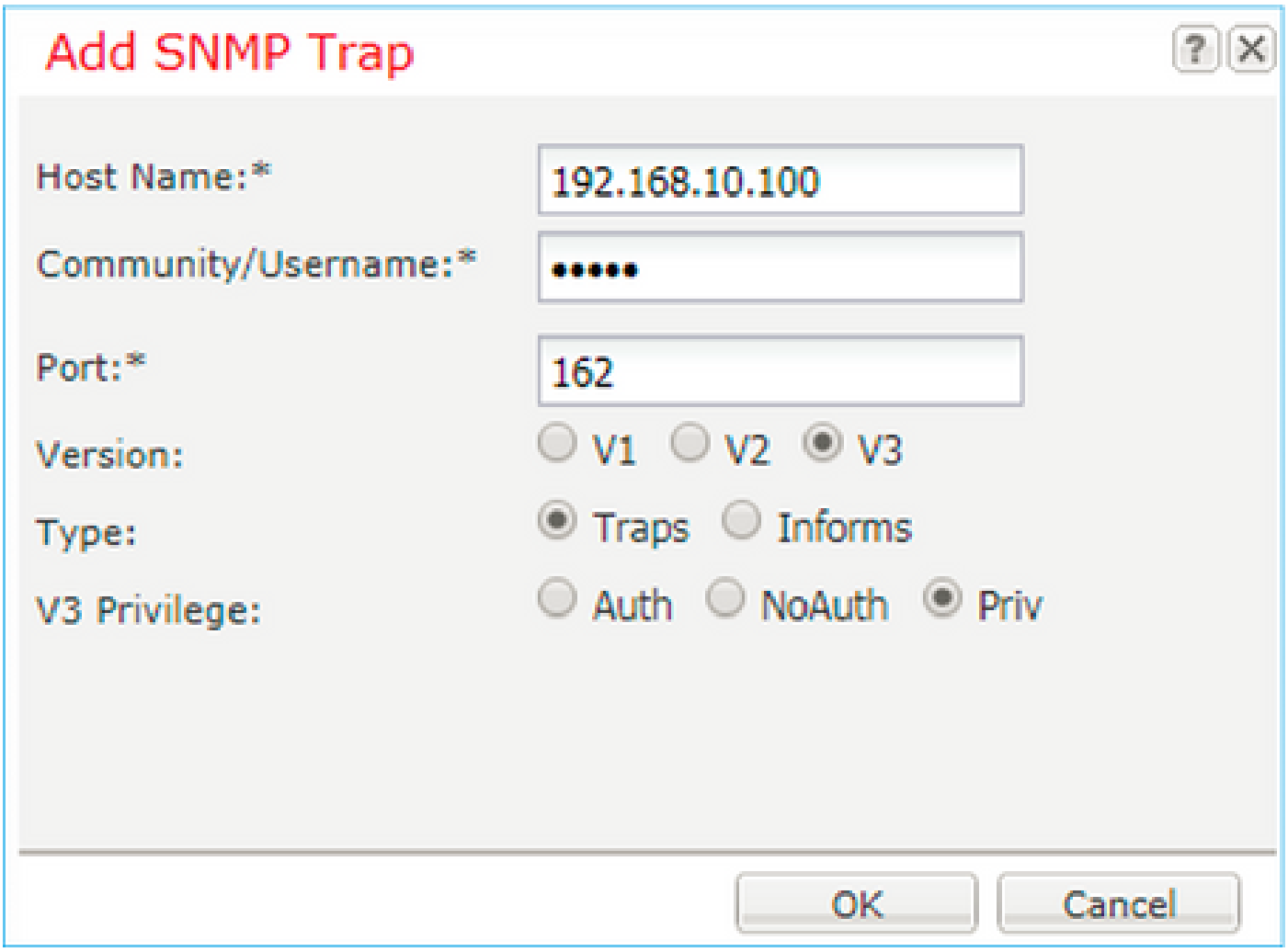
ステップ 2：SNMP v3の場合、上部のセクションでコミュニティストリングを設定する必要はありません。作成されたすべてのユーザーは、FXOS SNMP エンジンへのクエリを正常に実行できます。最初のステップは、プラットフォームで SNMP を有効にすることです。完了したら、ユーザーと宛先トラップホストを作成できます。SNMP ユーザーと SNMP トラップホストの両方が自動的に保存されます。



ステップ 3：図に示すように、SNMPユーザを追加します。認証タイプは常に SHA ですが、暗号化には AES または DES を使用できます。



ステップ 4：図に示すように、SNMPトラップホストを追加します。



CLI による FXOS SNMPv3 の構成

<#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

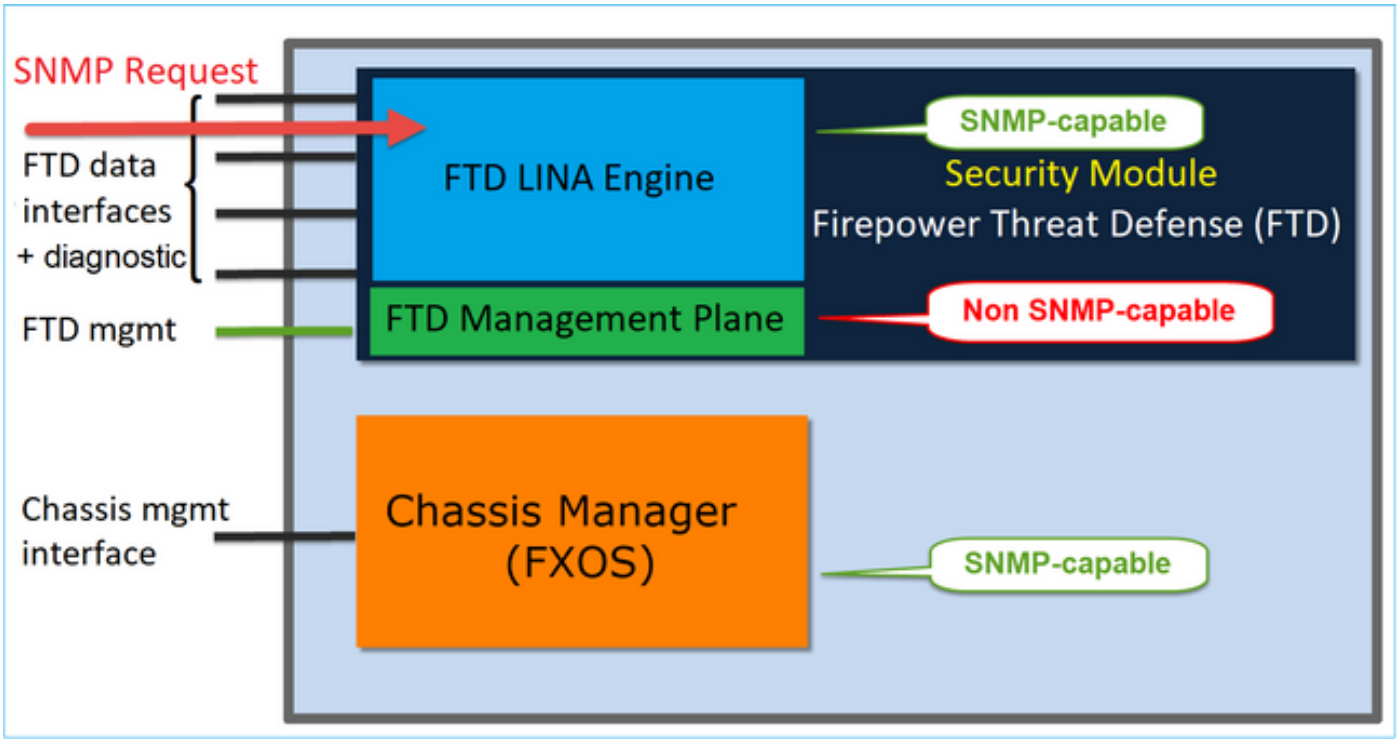
```
ksec-fpr9k-1-A /monitoring/snmp-user* #
```

set priv-password

```
Enter a password:
Confirm the password:
ksec-fpr9k-1-A /monitoring/snmp-user* #
```

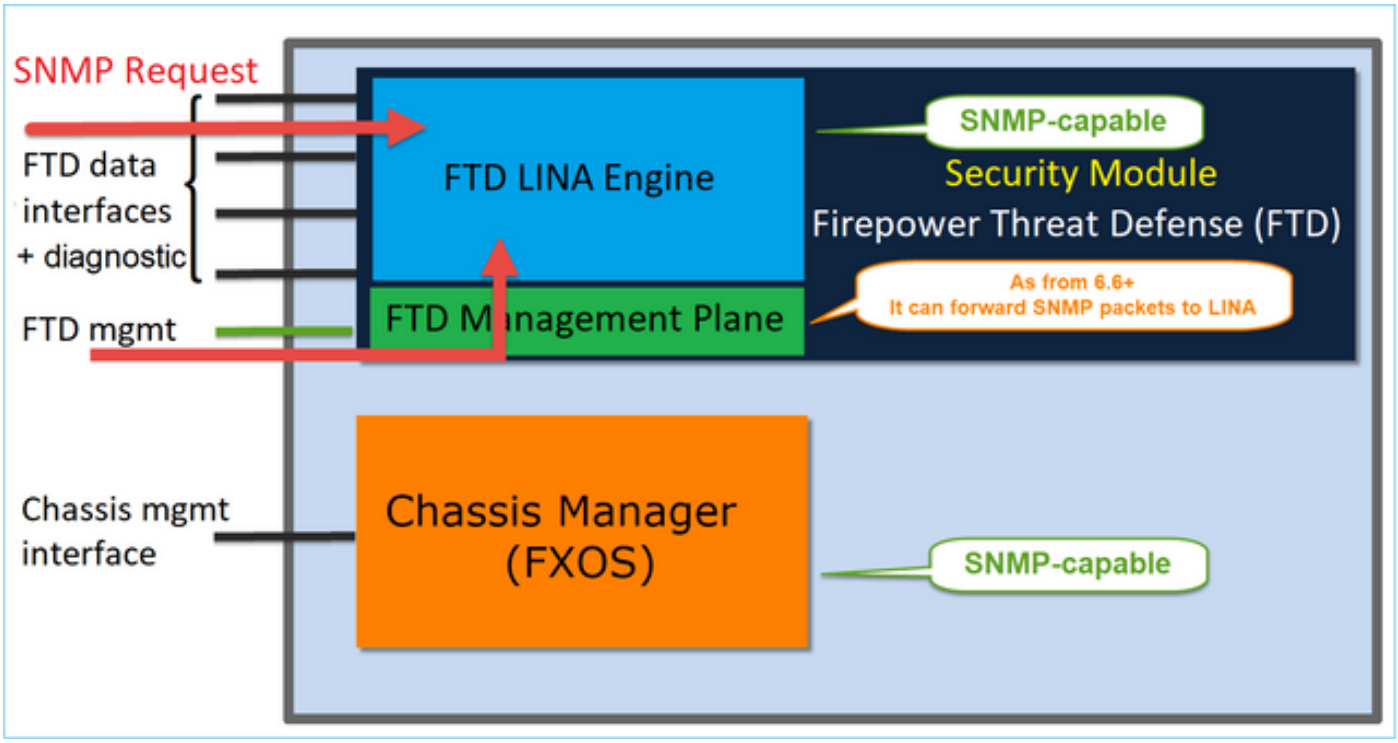
```
set aes-128 yes
ksec-fpr9k-1-A /monitoring/snmp-user* #
exit
ksec-fpr9k-1-A /monitoring* #
enter snmp-trap 10.48.26.190
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set community
Community:
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set version v3
ksec-fpr9k-1-A /monitoring/snmp-trap* #
set notificationtype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

FPR4100/FPR9300 の FTD (LINA) SNMP



6.6 以降のリリースでの変更点

- 6.6 以降のリリースでは、ポーリングとトラップに FTD 管理インターフェイスを使用するオプションもあります。



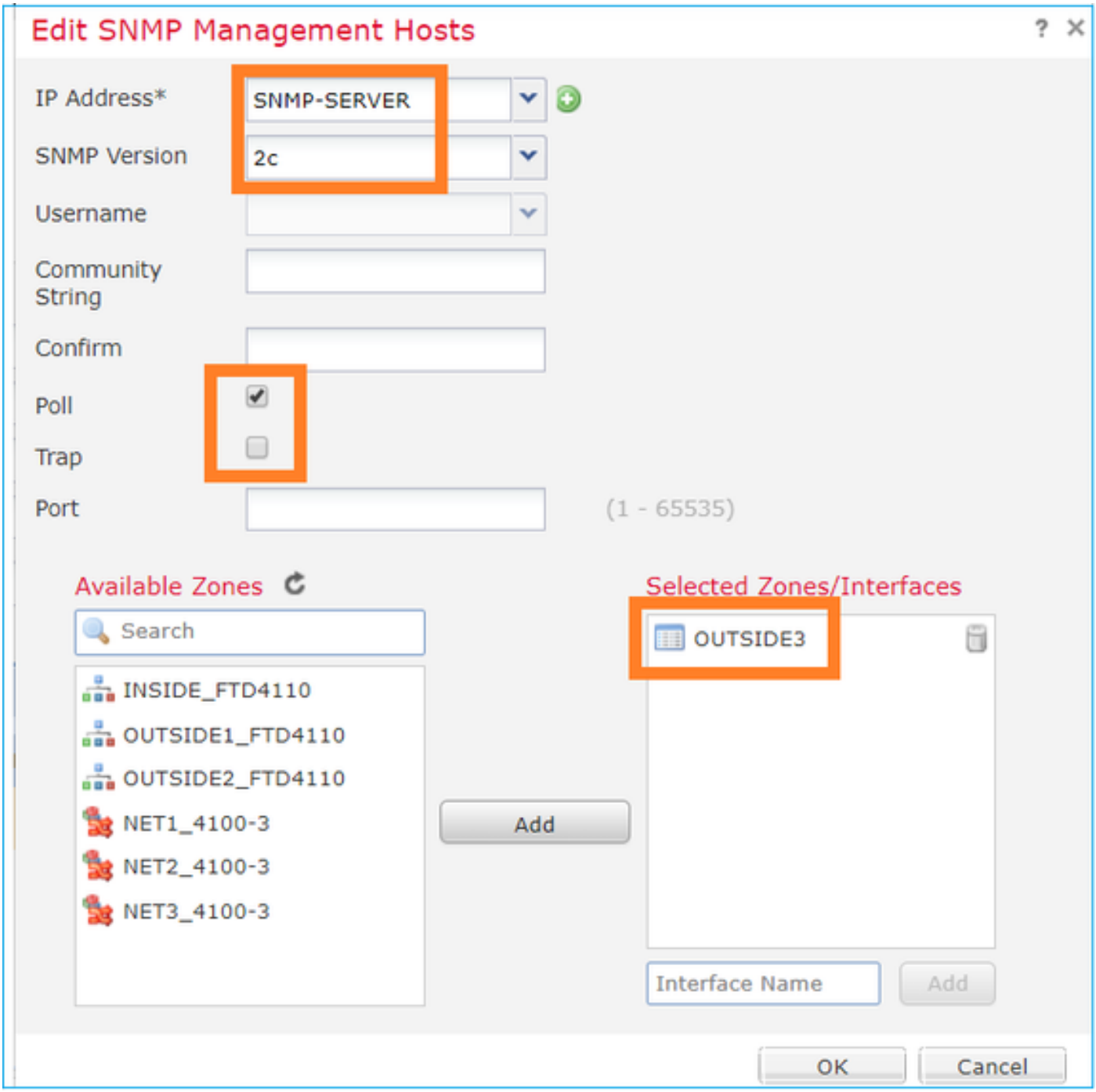
SNMP シングル IP 管理機能は、すべての FTD プラットフォームで 6.6 以降サポートされています。

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- FTD を実行する ASA5500
- FTDv

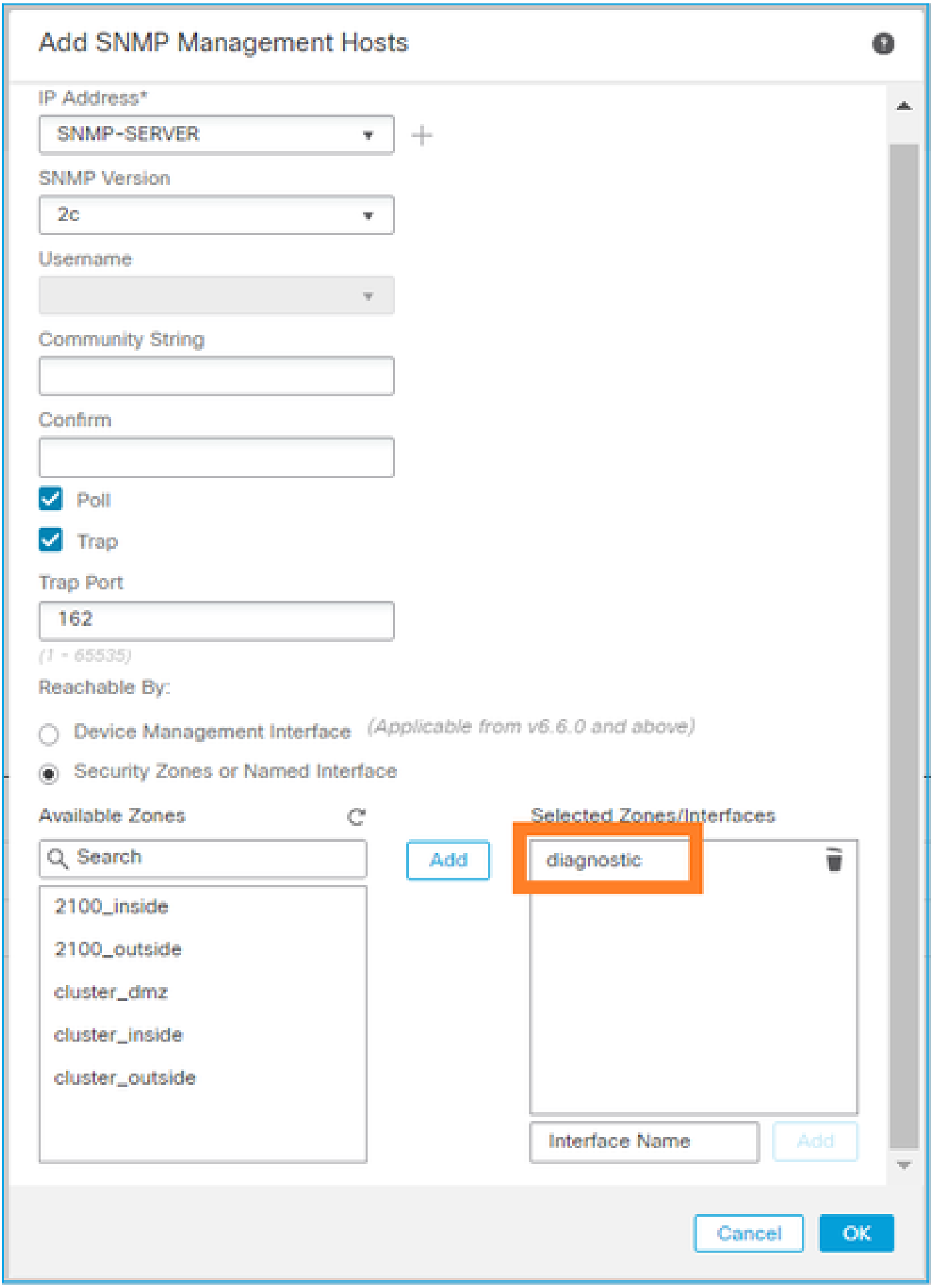
LINA SNMPv2c の構成

ステップ 1：FMCのUIで、Devices > Platform Settings > SNMPの順に移動します。 Enable SNMP Serversオプションにチェックマークを入れて、次のようにSNMPv2設定を行います。

ステップ 2：HostsタブでAddボタンを選択し、SNMPサーバの設定を指定します。

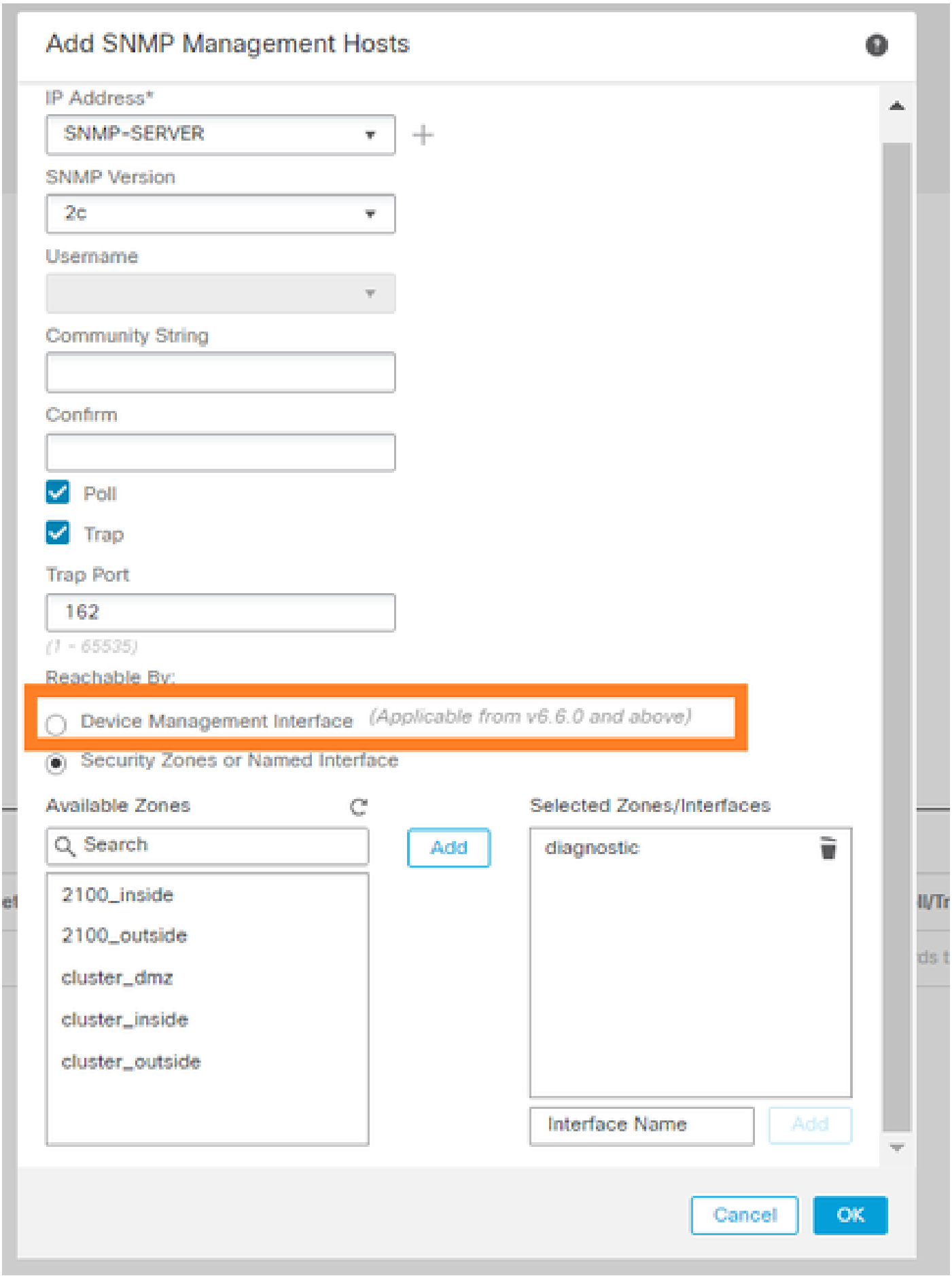


SNMP メッセージのソースとして diagnostic インターフェイスを指定することもできます。diagnostic インターフェイスは、to-the-box および from-the-box（管理のみ）のトラフィックのみを許可するデータインターフェイスです。


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

この画像は 6.6 リリースのもので、ライトテーマを使用しています。

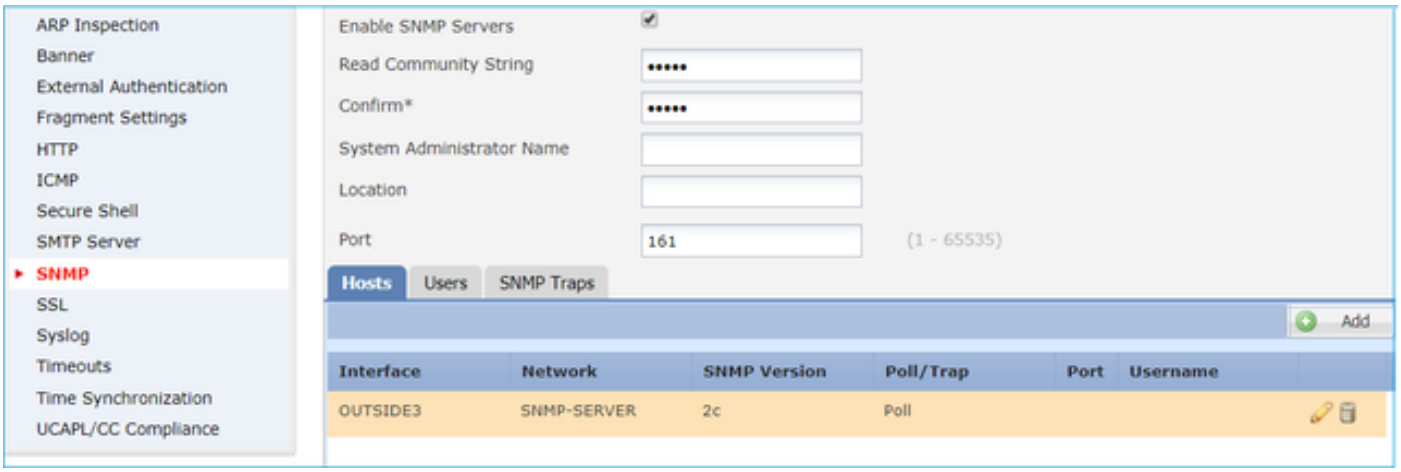
さらに、6.6 以降の FTD リリースでは、管理インターフェイスを選択することもできます。



新しい管理インターフェイスが選択されている場合、LINA SNMP は管理インターフェイス経由

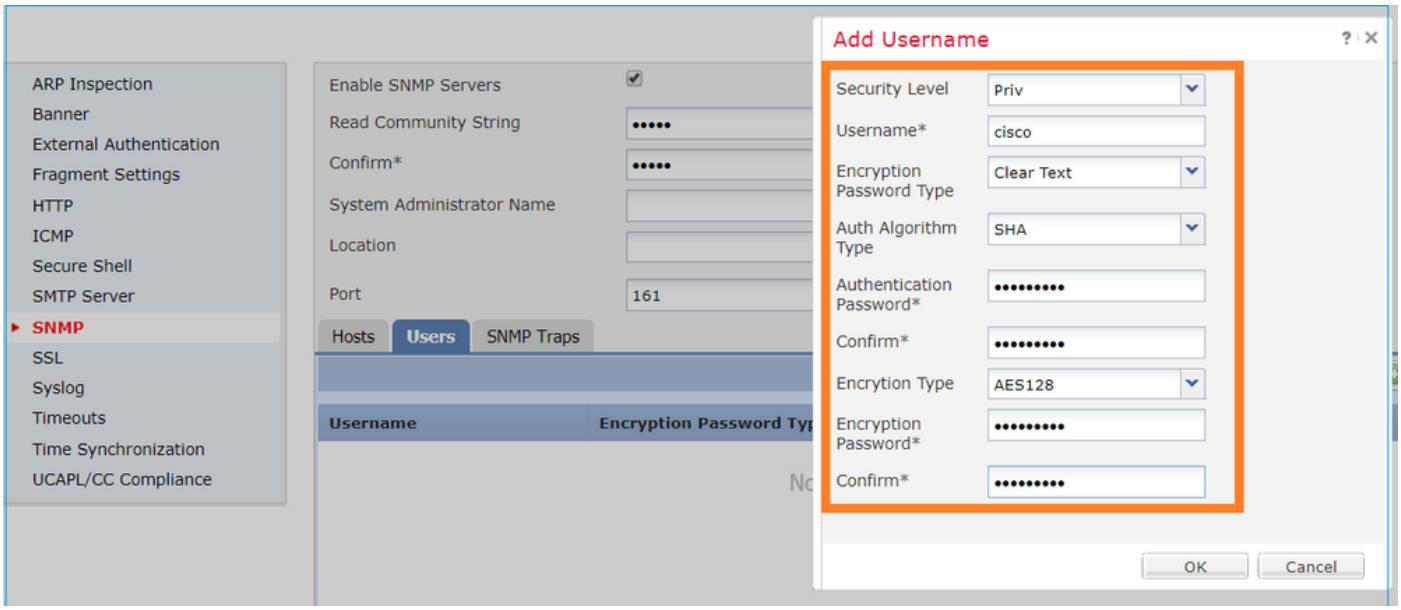
で使用できます。

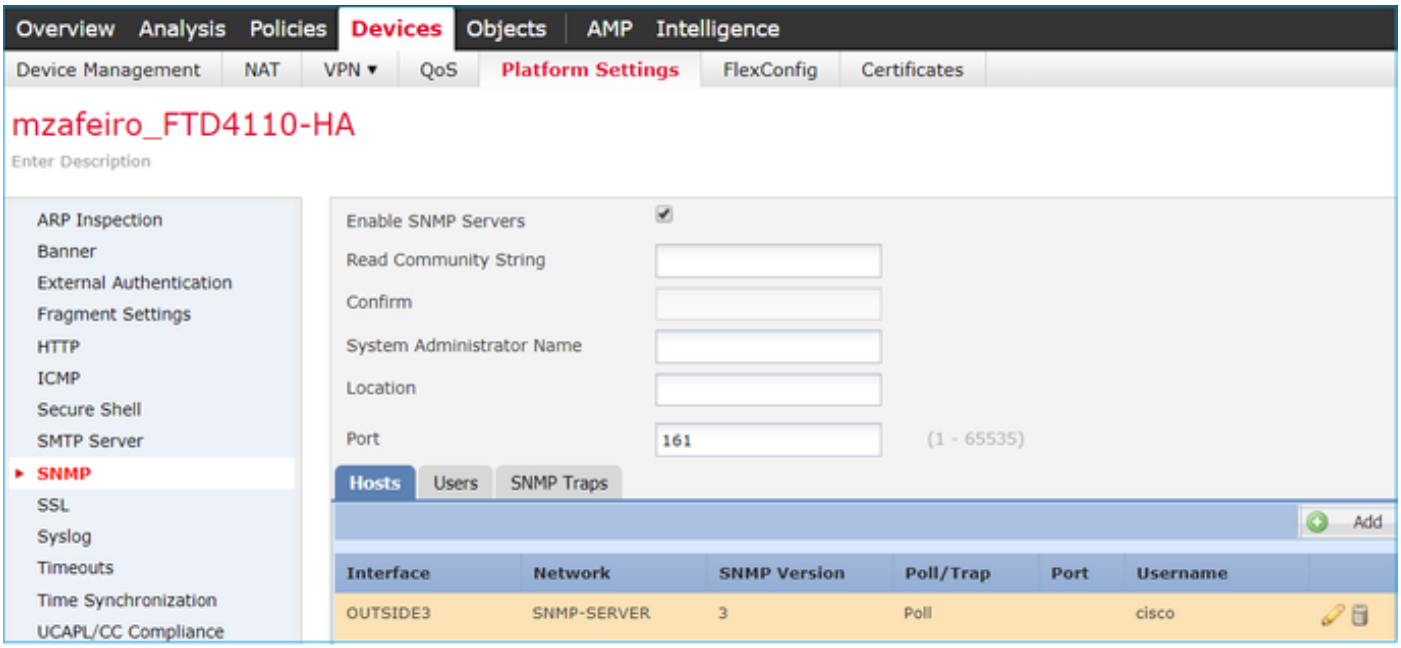
結果は、次のとおりです。



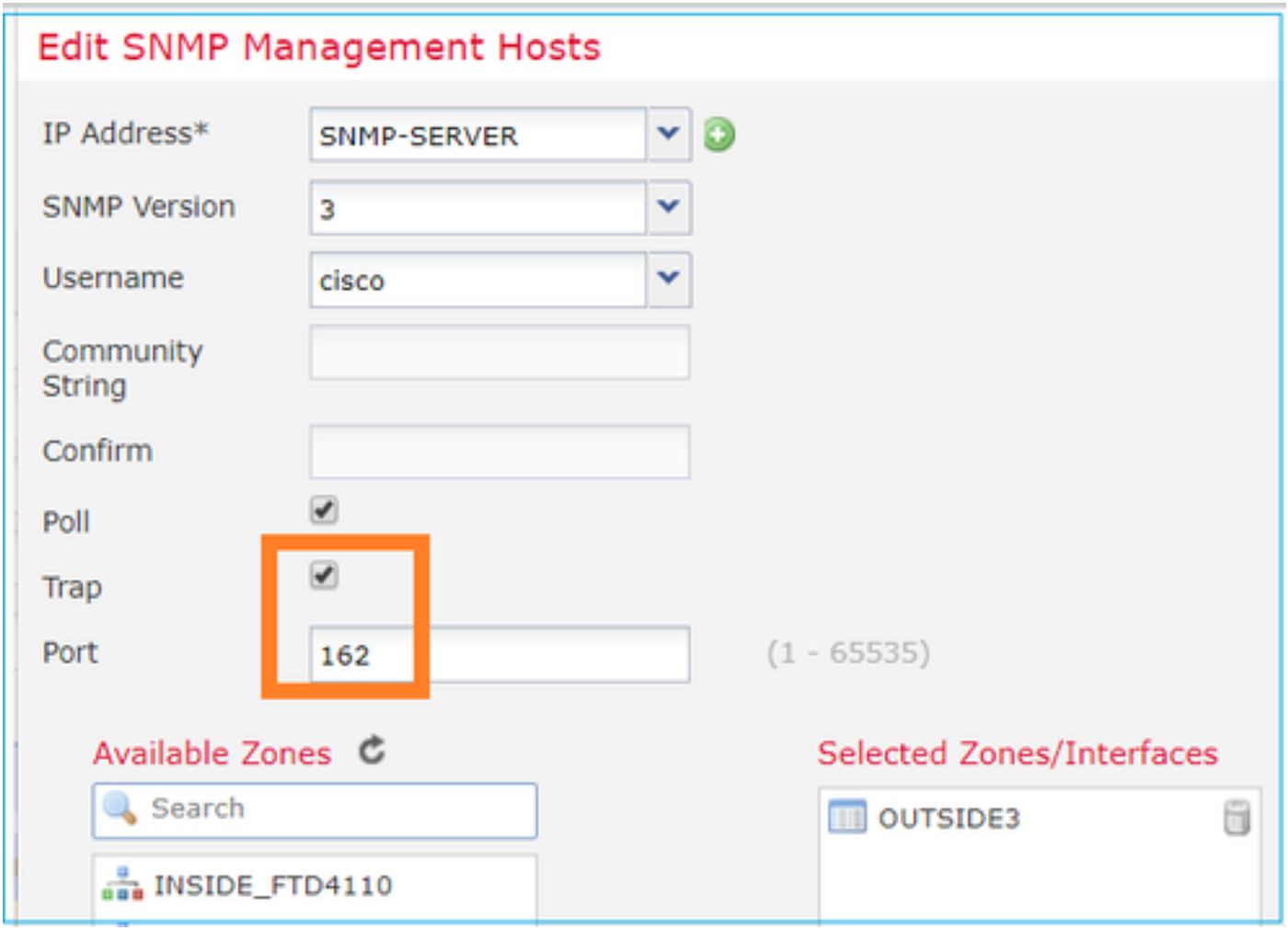
LINA SNMPv3 の構成

ステップ 1：FMC UIで、Devices > Platform Settings > SNMPの順に移動します。 Enable SNMP Serversオプションにチェックマークを入れて、SNMPv3のユーザとホストを設定します。

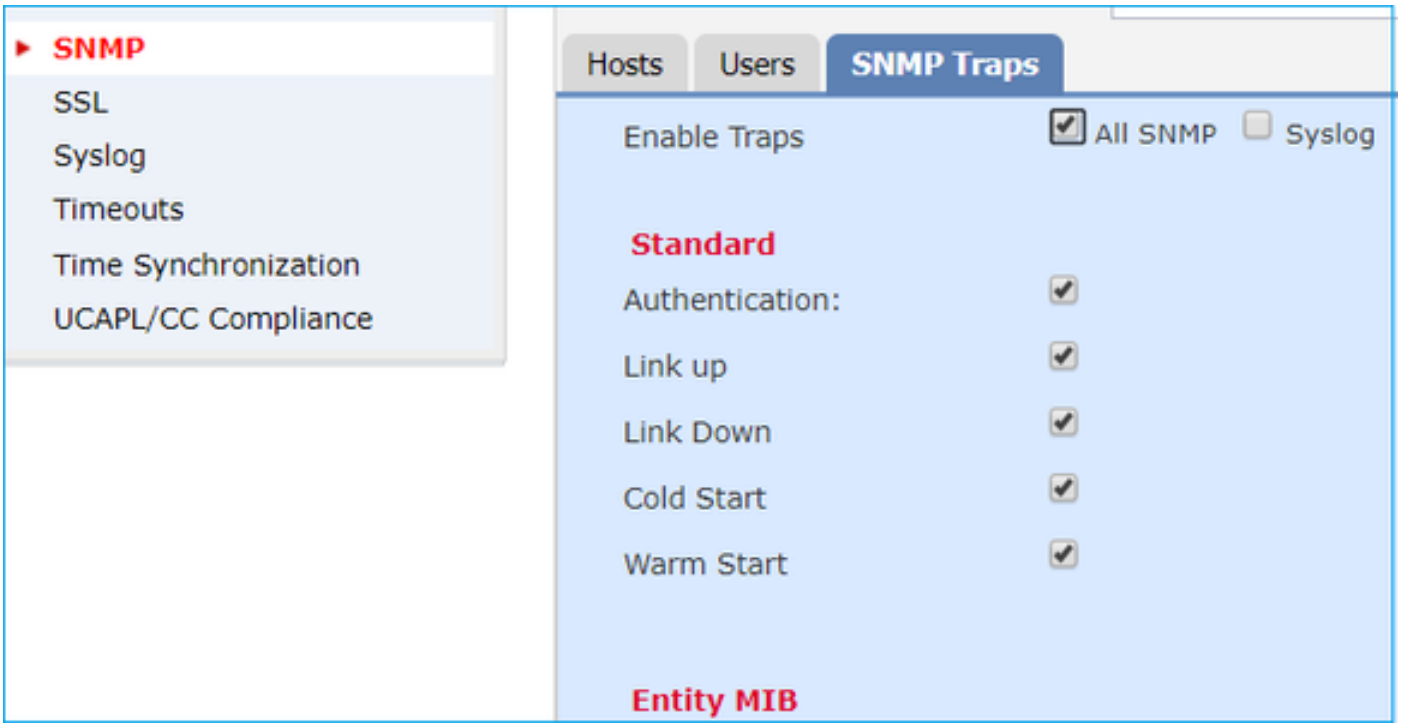




ステップ 2：トラップを受信するようにホストを設定します。



ステップ 3：受信するトラップは、SNMP Trapsセクションで選択できます。



MIOブレードSNMP統合(FXOS 2.12.1、FTD 7.2、ASA 9.18.1)

7.2より前の動作

- 9300および4100プラットフォームでは、シャーシ情報のSNMP MIBは、FTD/ASAアプリケーションで設定されたSNMPでは使用できません。MIOでは、シャーシマネージャを介して個別に設定し、個別にアクセスする必要があります。MIOは、管理およびI/O（スーパーバイザ）モジュールです。
- 2つの異なるSNMPポリシーを設定する必要があります。1つはBlade/App上に、もう1つはMIO上でSNMPモニタリング用に設定します。
- 別々のポートが使用され、1つはブレード用で、もう1つは同じデバイスのSNMPモニタリング用です。
- SNMPを使用して9300および4100のデバイスを設定および監視しようとすると、これが複雑になる可能性があります。

新しいリリース（FXOS 2.12.1、FTD 7.2、ASA 9.18.1以降）での動作のしくみ

- MIOブレードのSNMP統合により、ユーザはアプリケーション(ASA/FTD)インターフェイス経由でLINAおよびMIO MIBをポーリングできます。
- この機能は、新しいMIO CLIおよびFCM（シャーシマネージャ）UIを使用して有効または無効にできます。
- デフォルトのステータスはdisabledです。これは、MIO SNMPエージェントがスタンドアロンインスタンスとして実行されていることを意味します。シャーシ/DME MIBのポーリングには、MIOインターフェイスを使用する必要があります。この機能を有効にすると、アプリケーションインターフェイスを使用して同じMIBをポーリングできるようになります。
- この設定は、Chassis Manager UIのPlatform-settings > SNMP > Admin Instanceで使用できます。このFTDインスタンスは、NMSに提示するシャーシMIBを照合/収集するFTDインスタンスを指定できます
- ASA/FTDネイティブおよびMIアプリケーションがサポートされます。

- この機能は、MIOベースのプラットフォーム（FPR9300およびFPR4100）にのみ適用されます。

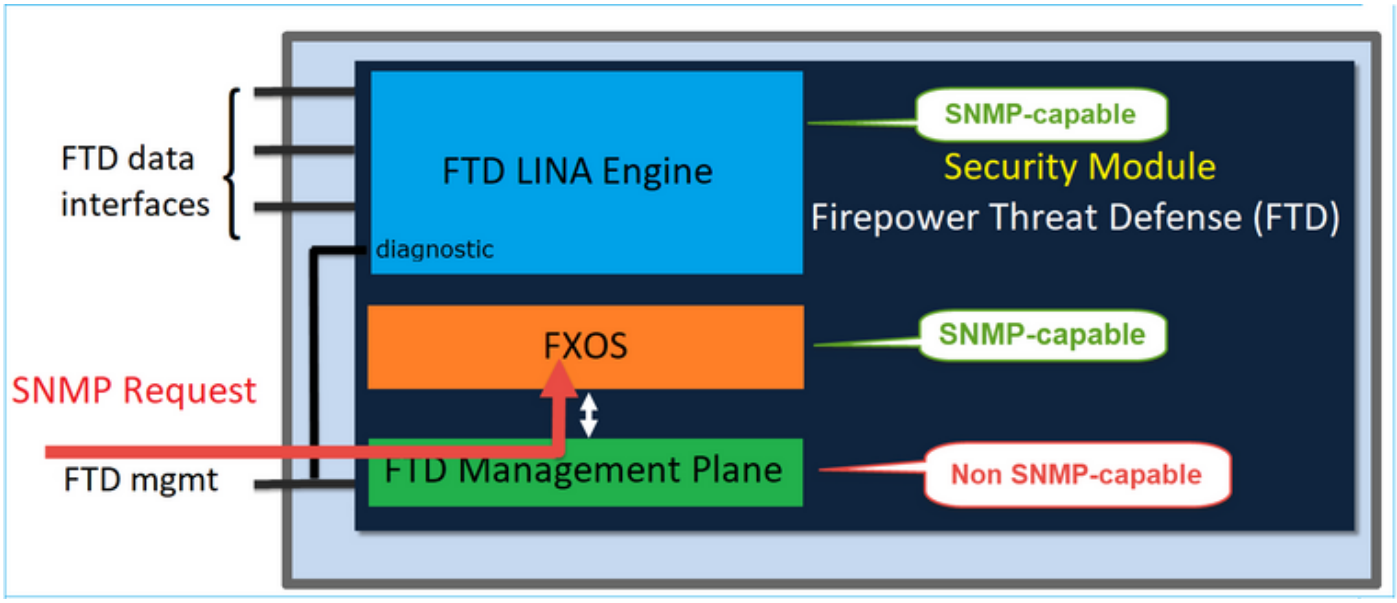
前提条件、サポートされるプラットフォーム

- サポートされるマネージャの最小バージョン：FCM 2.12.1
- マネージドデバイス：FPR9300/FP4100シリーズ
- サポートされる管理対象デバイスの最小バージョン：FXOS 2.12.1、FTD 7.2、またはASA 9.18.1

FPR2100 の SNMP

FPR2100 システムでは、FCM はありません。SNMP を構成する唯一の方法は、FMC 経由です。

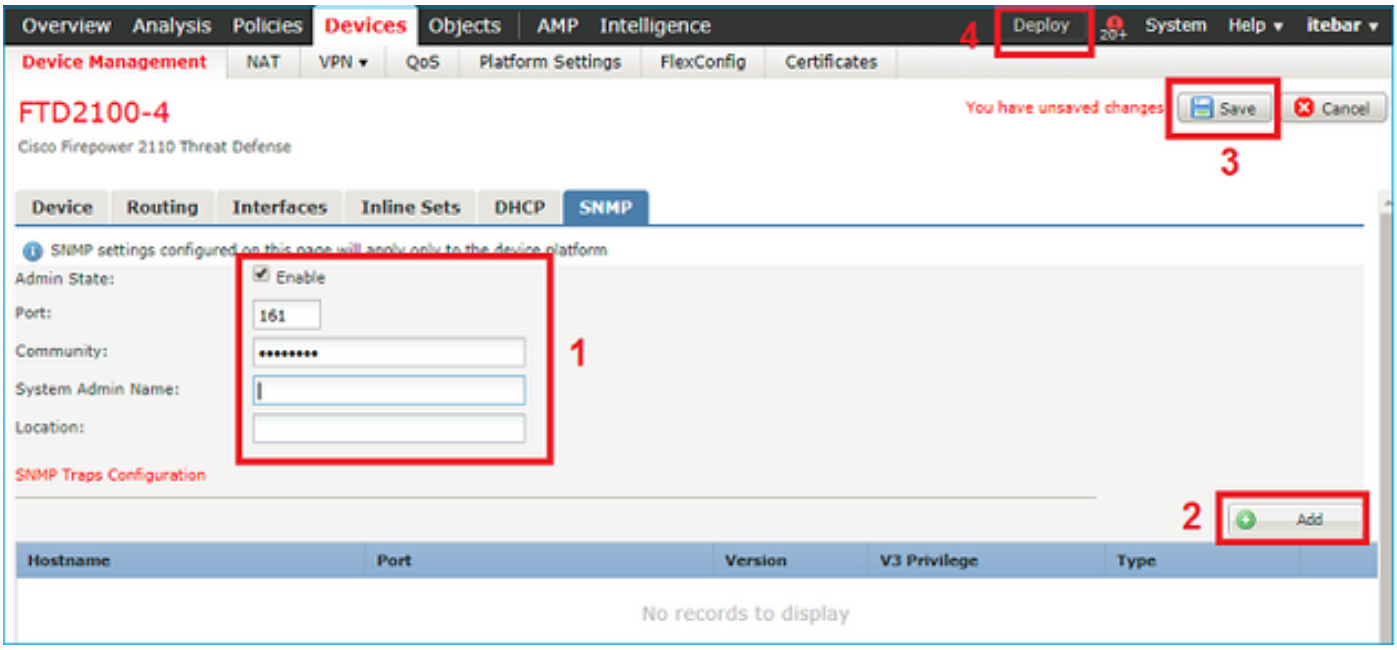
FPR2100 のシャーシ（FXOS）SNMP

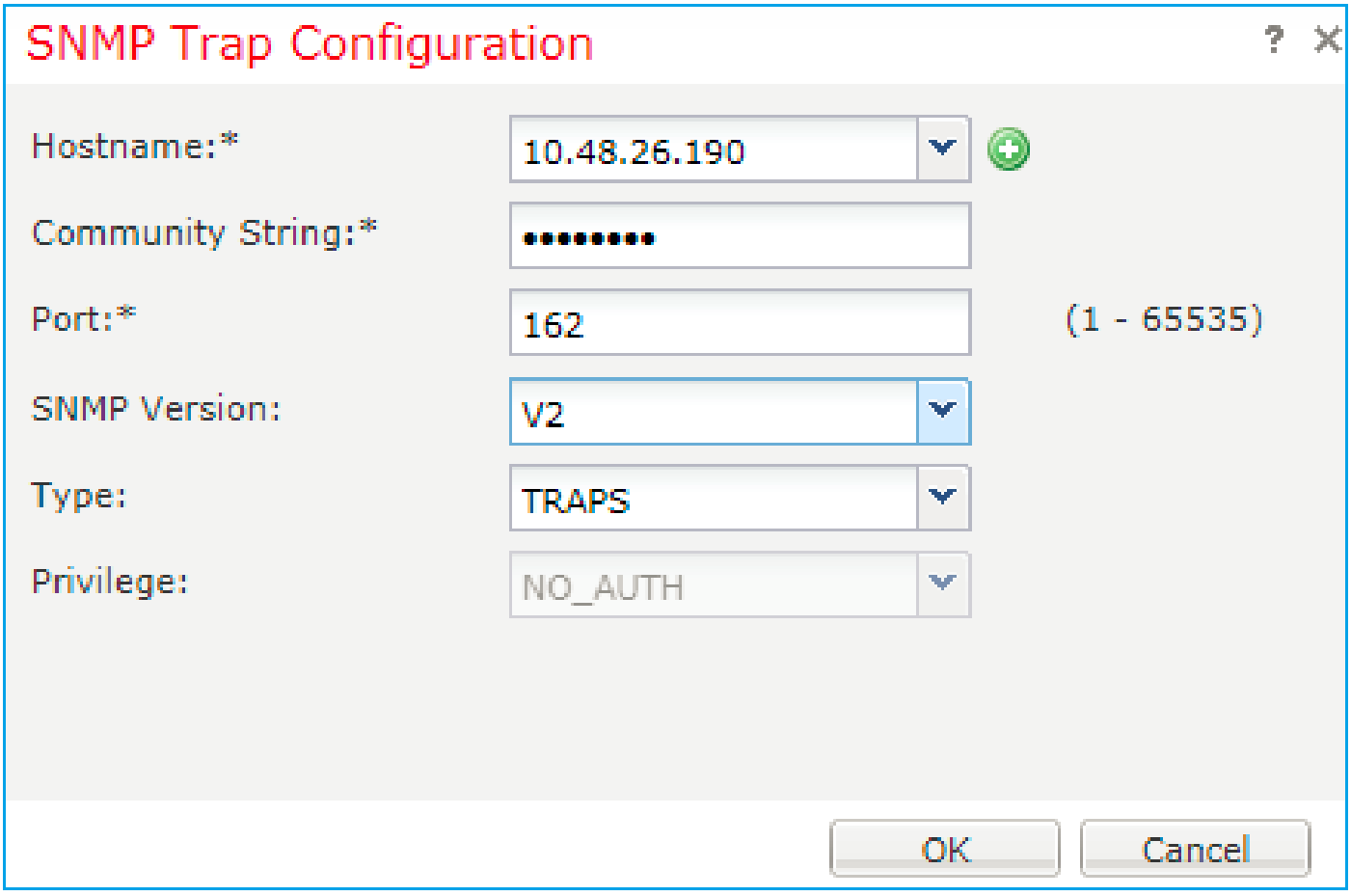


FTD 6.6 以降、SNMP に FTD 管理インターフェイスを使用するオプションもあります。この場合、FXOS と LINA SNMP 情報の両方が FTD 管理インターフェイスを介して転送されます。

FXOS SNMPv1/v2c の構成

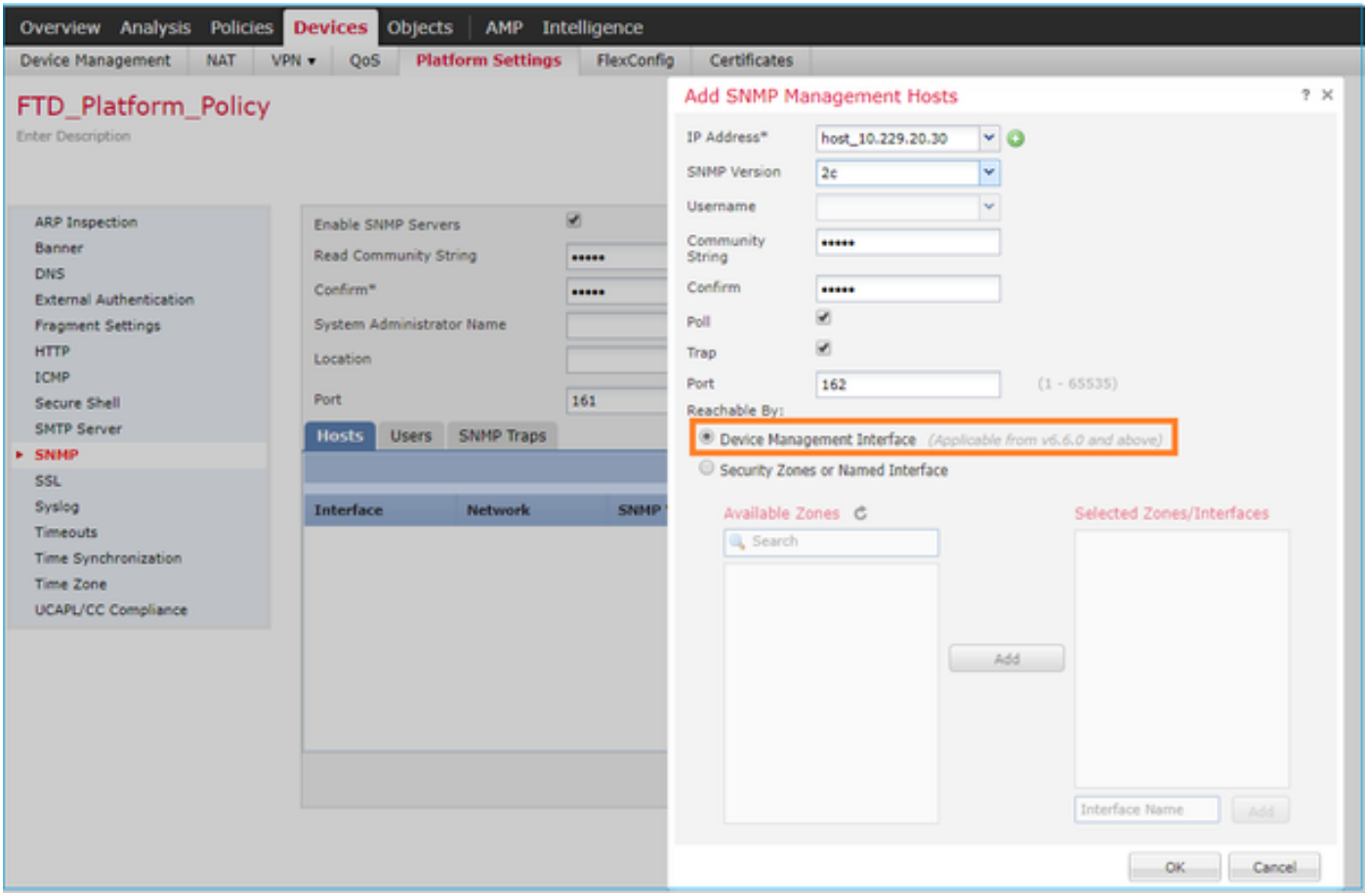
FMC UIを開き、Devices > Device Managementに移動します。 デバイスを選択し、SNMPを選択します。





FTD 6.6 以降での変更点

FTD 管理インターフェイスを指定できます。

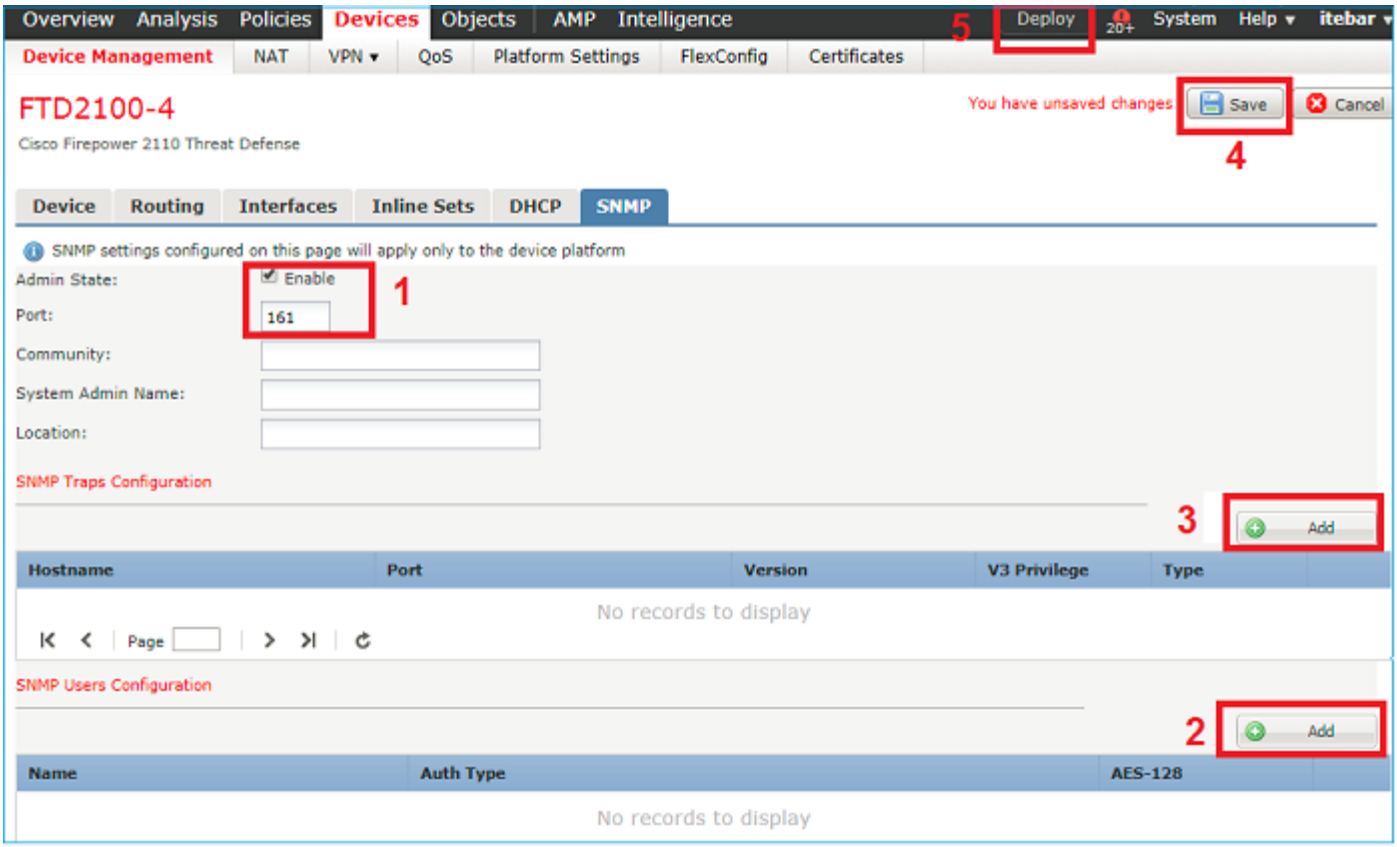


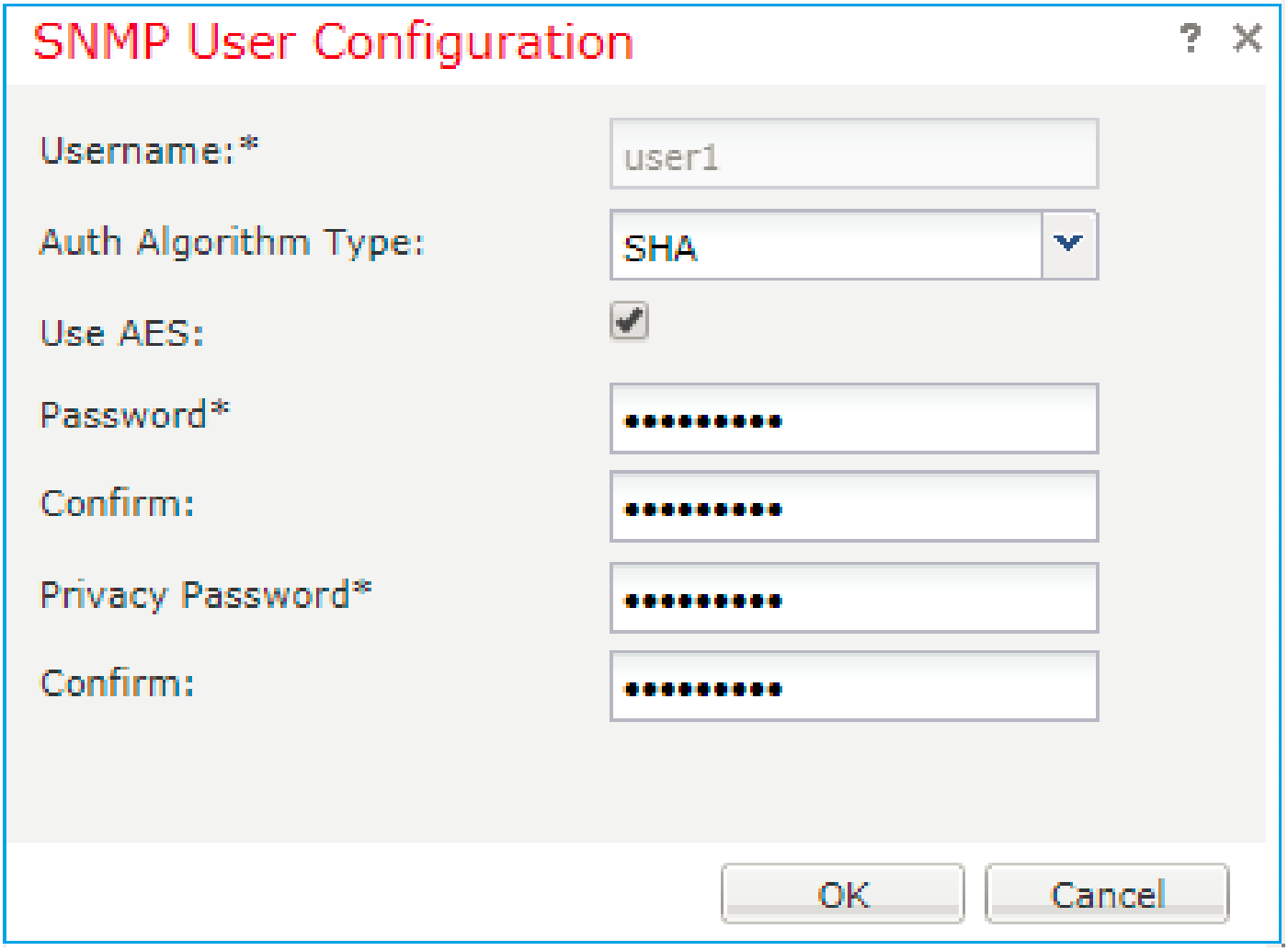
管理インターフェイスは SNMP にも構成できるため、このページには次の警告メッセージが表示されます。

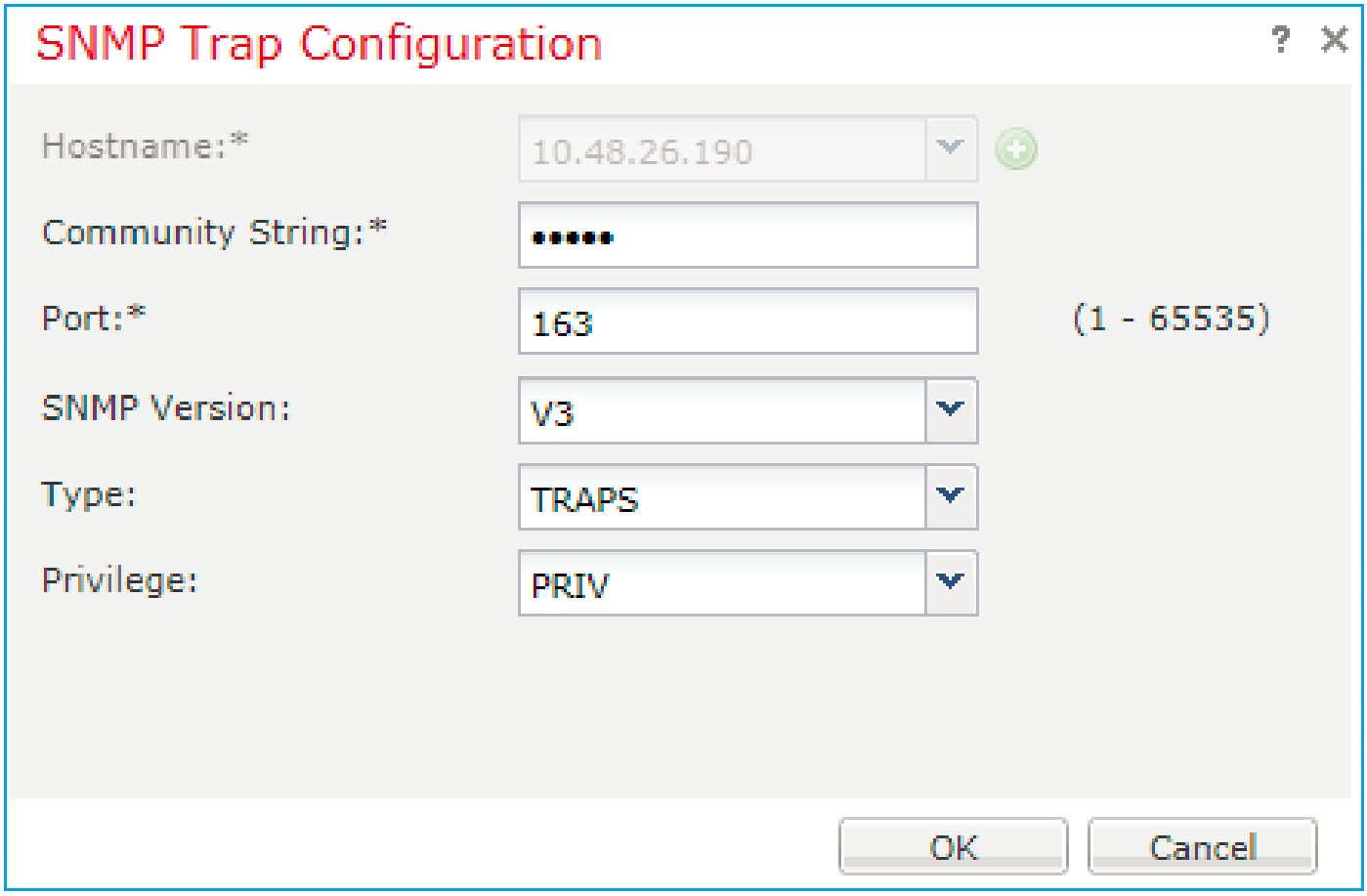
デバイス>プラットフォーム設定（脅威対策）> SNMP >ホストを使用してデバイス管理インターフェイスでSNMP設定を設定している場合、このページのデバイスプラットフォームのSNMP設定は無効になります。

FXOS SNMPv3 の構成

FMC UIを開き、Devices > Device Managementの順に選択します。デバイスを選択し、SNMPを選択します。

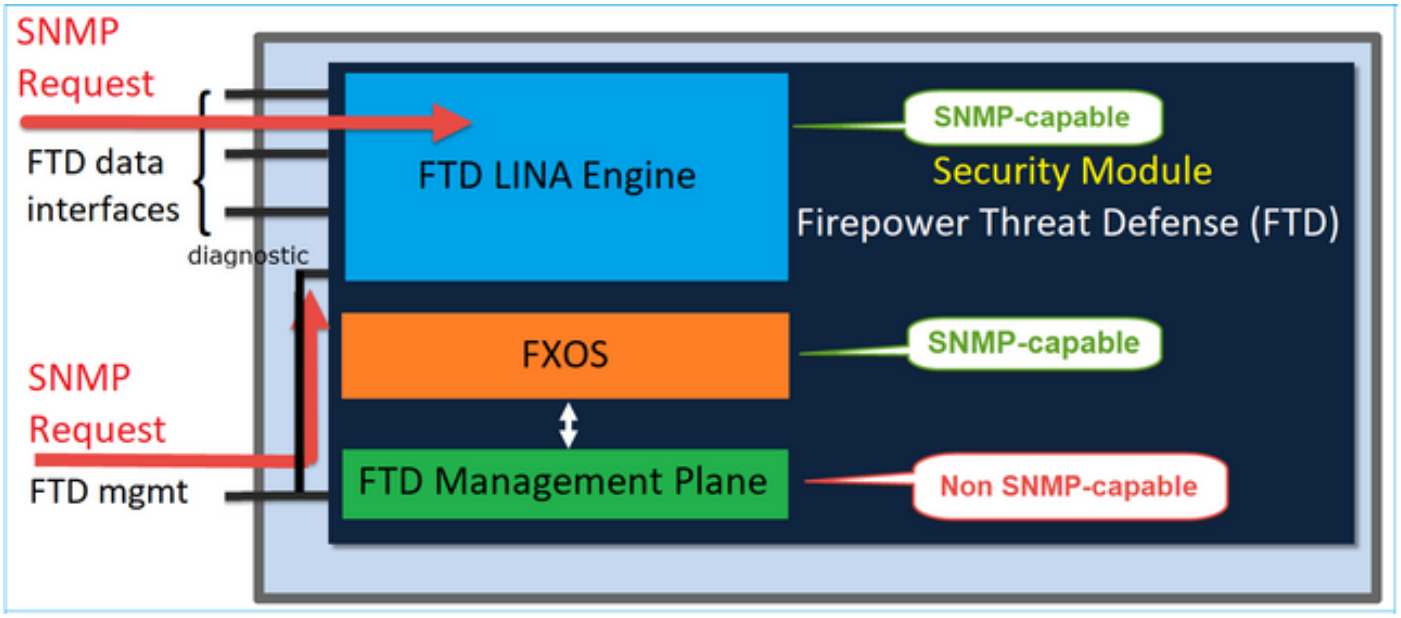

Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
5
Deploy
System
Help
itebar
Device Management
NAT
VPN
QoS
Platform Settings
FlexConfig
Certificates
FTD2100-4
Cisco Firepower 2110 Threat Defense
You have unsaved changes
Save
Cancel
4
Device
Routing
Interfaces
Inline Sets
DHCP
SNMP
SNMP settings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


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



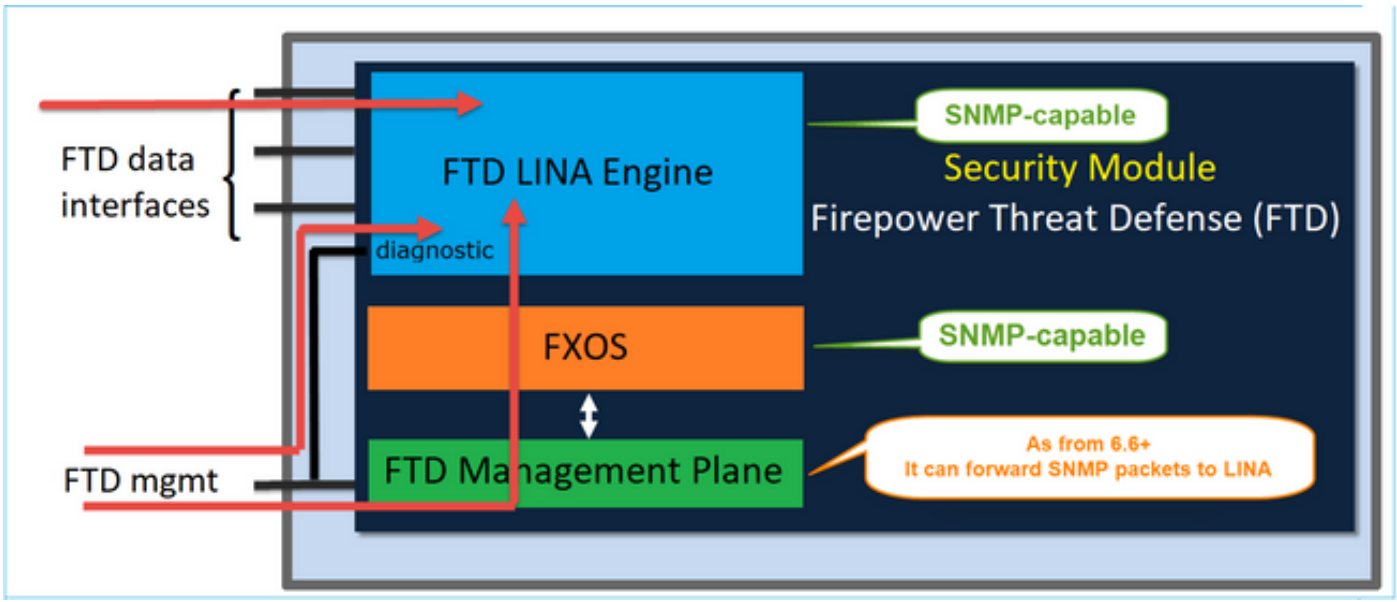
FPR2100 の FTD (LINA) SNMP

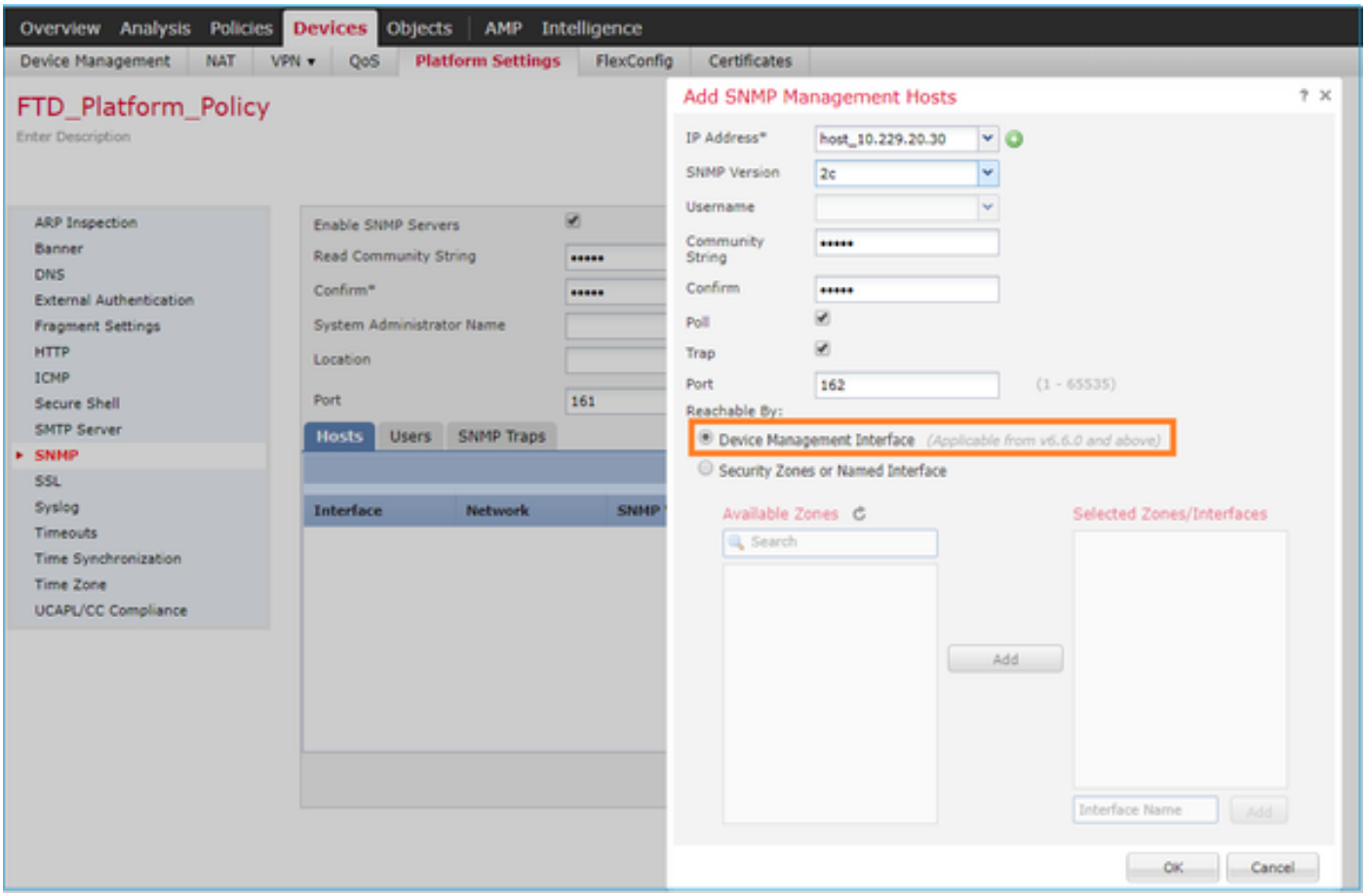
- 6.6 より前のリリースでは、FTD FP1xxx/FP21xx アプライアンスの LINA FTD SNMP 構成は、Firepower 4100 または 9300 アプライアンスの FTD と同じです。



FTD 6.6 以降のリリース

- 6.6 以降のリリースでは、LINA ポーリングとトラップに FTD 管理インターフェイスを使用するオプションもあります。



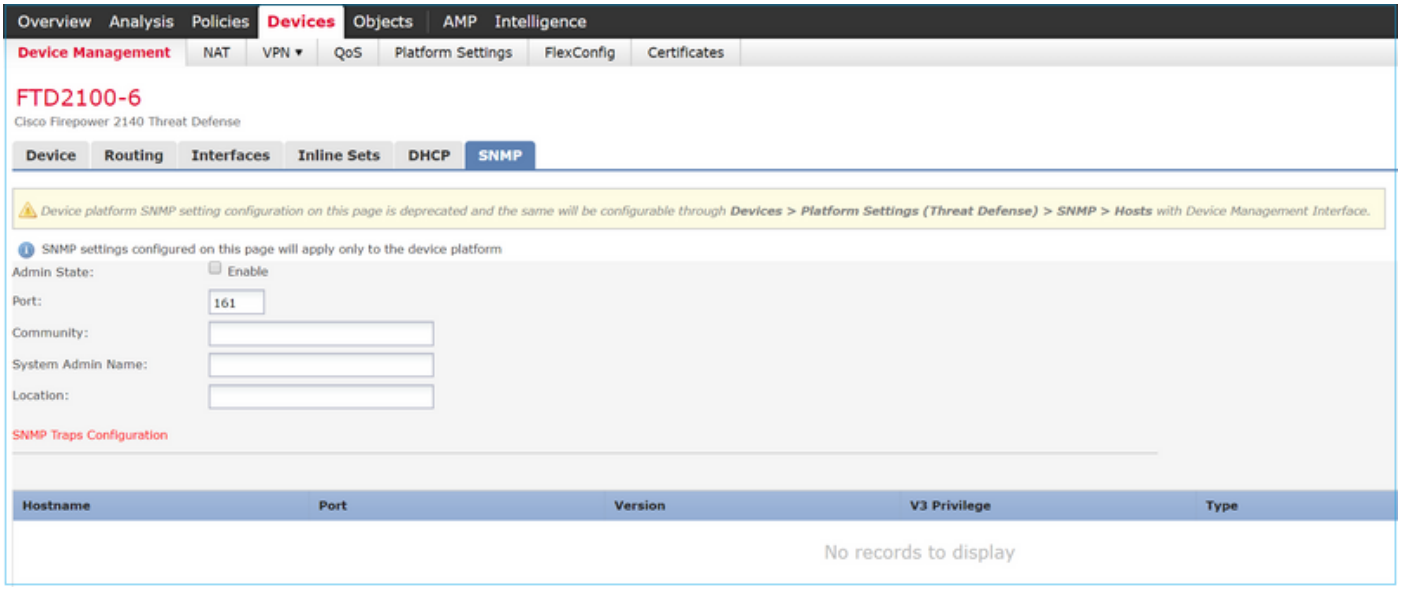


新しい管理インターフェイスが選択されている場合：

- LINA SNMP は、管理インターフェイス経由で使用できます。
- [Devices] > [Device Management] の下にあった [SNMP] タブは不要になったため無効になっています。通知バナーが表示されます。[SNMP device] タブは、2100/1100 プラットフォームでのみ表示されていました。このページは、FPR9300/FPR4100 および FTD55xx プラ

ットフォームには存在しません。

構成されると、（FP1xxx/FP2xxx 上の）結合された LINA SNMP + FXOS SNMP ポーリング/トラップ情報は、FTD 管理インターフェイスを介して送信されます。



SNMP シングル IP 管理機能は、すべての FTD プラットフォームで 6.6 以降サポートされています。

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- FTD を実行する ASA5500
- FTDv

詳細については、「Configure SNMP for Threat Defense」を参照してください。

確認

FPR4100/FPR9300 の FXOS SNMP の検証

FXOS SNMPv2c の検証

CLI 構成の検証：

```
<#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
```

FXOS モードから：

<#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
```

追加の検証：

<#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

...
```

SNMP 要求のテスト.

有効なホストからSNMP要求を実行します。

トラップ生成の確認.

Ethanalyzer が有効になっているインターフェイスでフラップを使用して、SNMP トラップが生成され、定義されたトラップホストに送信されることを確認できます。

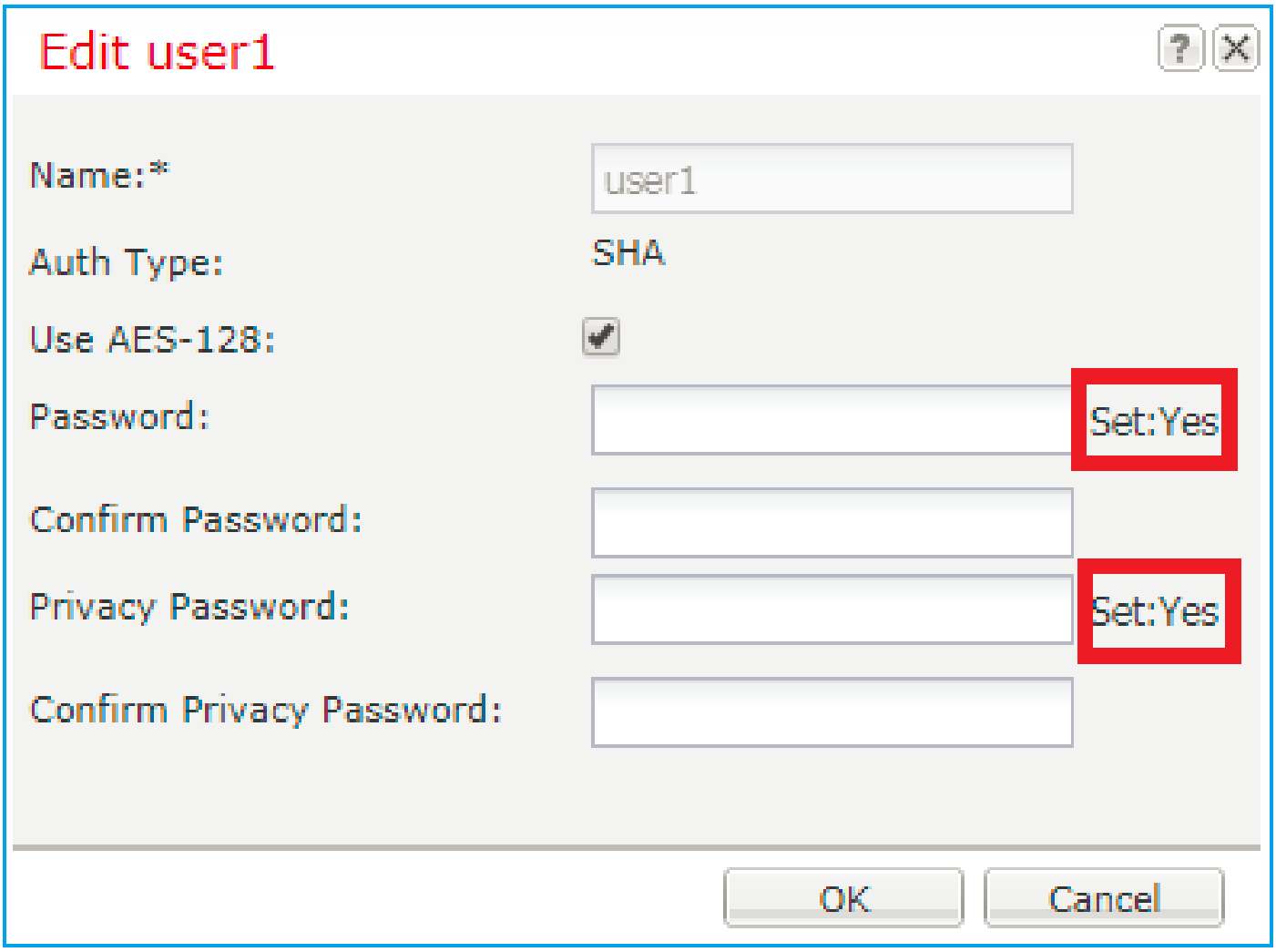
<#root>

```
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
```

⚠ 警告：インターフェイスフラップにより、トラフィックが停止する可能性があります。このテストは、ラボ環境またはメンテナンスウィンドウでのみ実行してください。

FXOS SNMPv3 の検証

ステップ 1：FCM UI Platform Settings > SNMP > User を開くと、パスワードとプライバシーパスワードが設定されているかどうかが表示されます。



ステップ 2：CLIでは、スコープmonitoringでSNMP設定を確認できます。

<#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
```

ステップ 3：FXOSモードで、SNMP設定と詳細を展開できます。

<#root>

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

show running-config snmp all

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

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

show snmp user

```
_____________________________________________________________
                  SNMP USERS
_____________________________________________________________

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

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

User                          Auth  Priv
____                          ____  ____

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

show snmp host

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

SNMP 要求のテスト.

設定を確認し、SNMP機能を持つ任意のデバイスからSNMP要求を実行できます。

SNMP 要求の処理方法を確認するには、SNMP デバッグを使用します。

<#root>

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

debug snmp pkt-dump

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

⚠ 注意：デバッグはデバイスのパフォーマンスに影響を与える可能性があります。

FPR2100 の FXOS SNMP の検証

FXOS SNMPv2 の検証

CLI 経由で構成を確認します。

<#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
```

SNMP 動作の確認.

FXOSをポーリングし、ホストまたはSNMP機能を持つ任意のデバイスからSNMP要求を送信できることを確認できます。

capture-traffic コマンドを使用して、SNMP 要求と応答を確認します。

<#root>

>

capture-traffic

Please choose domain to capture traffic from:
  0 - management0

Selection?

0

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

udp port 161

HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on management0, link-type EN10MB (Ethernet), capture size 96 bytes
13:50:50.521383 IP *10.48.26.190*.42224 > FP2110-4.snmp: C=cisco123 GetNextRequest(29) interfaces.ifTab
13:50:50.521533 IP FP2110-4.snmp > *10.48.26.190*.42224: C=cisco123 GetResponse(32) interfaces.ifTable.
^C
Caught interrupt signal

Exiting.

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

FXOS SNMPv3 の検証

CLI 経由で構成を確認します。

<#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
```

SNMP 動作の確認.

SNMP要求を送信して、FXOSをポーリングできることを確認します。

さらに、要求をキャプチャできます。

<#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
```

FTD SNMP の検証

FTD LINA SNMP 構成を確認するには：

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

6.6 以降の FTD では、SNMP の FTD 管理インターフェイスを構成して使用できます。

```
<#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
```

その他の検証:

```
<#root>

Firepower-module1#

show snmp-server host

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

SNMP サーバー CLI から、snmpwalk を実行します。

<#root>

root@host:/Volume/home/admin#

snmpwalk -v2c -c cisco -OS *10.62.148.48*

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

SNMP トラフィック統計の検証。

<#root>

Firepower-module1#

show snmp-server statistics

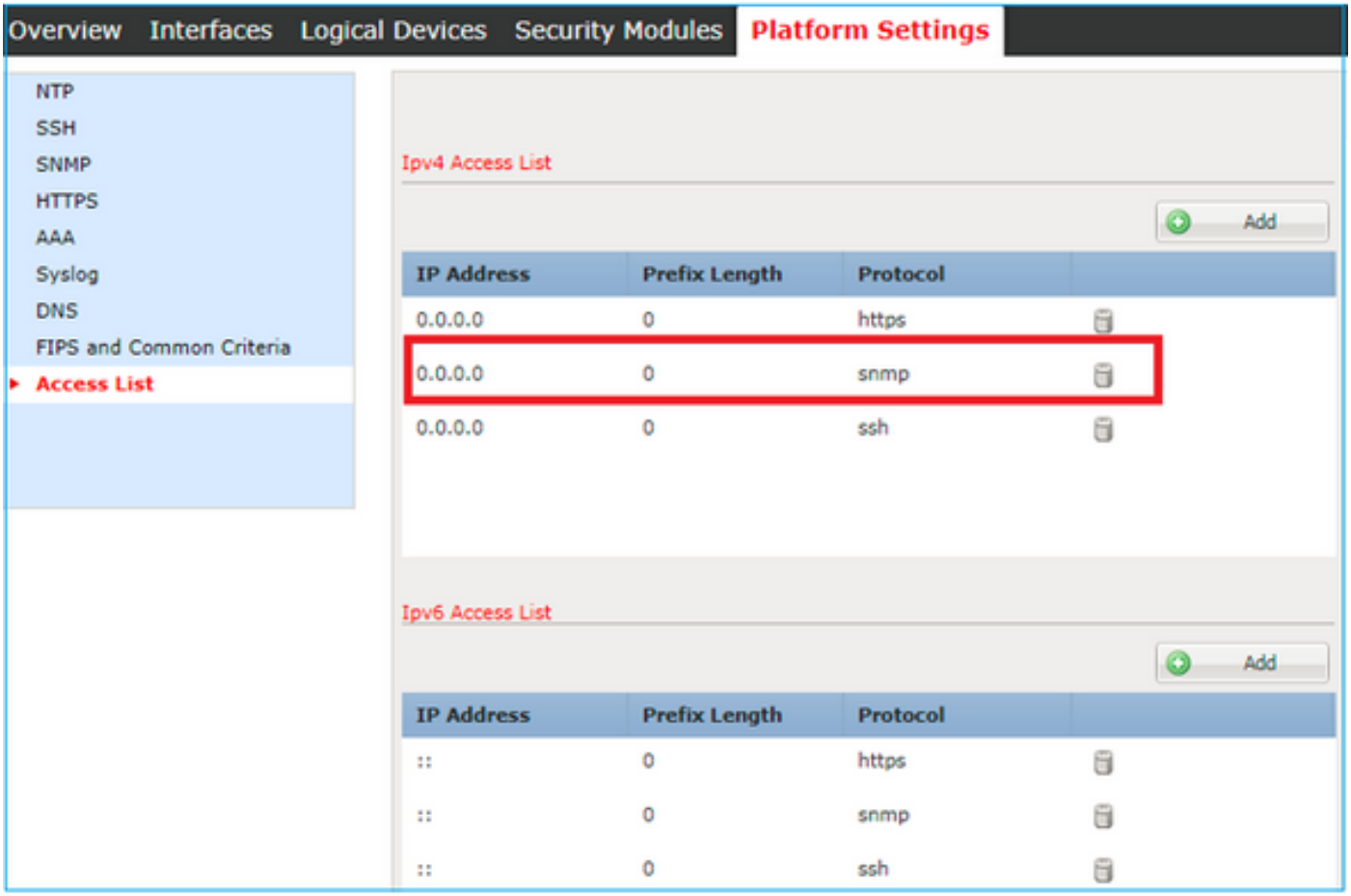
1899 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    1899 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    1899 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
1904 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    1899 Response PDUs
    5 Trap PDUs

FPR4100/FPR9300 での FXOS への SNMP トラフィック許可

FPR4100/9300 の FXOS 構成では、ソース IP アドレスごとに SNMP アクセスを制限できます。アクセスリスト構成セクションでは、SSH、HTTPS、または SNMP 経由でデバイスに到達できるネットワーク/ホストを定義します。SNMP サーバーからの SNMP クエリが許可されているこ

とを確認する必要があります。

GUI によるグローバルアクセスリストの構成



CLI によるグローバルアクセスリストの構成

<#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
```

検証

<#root>

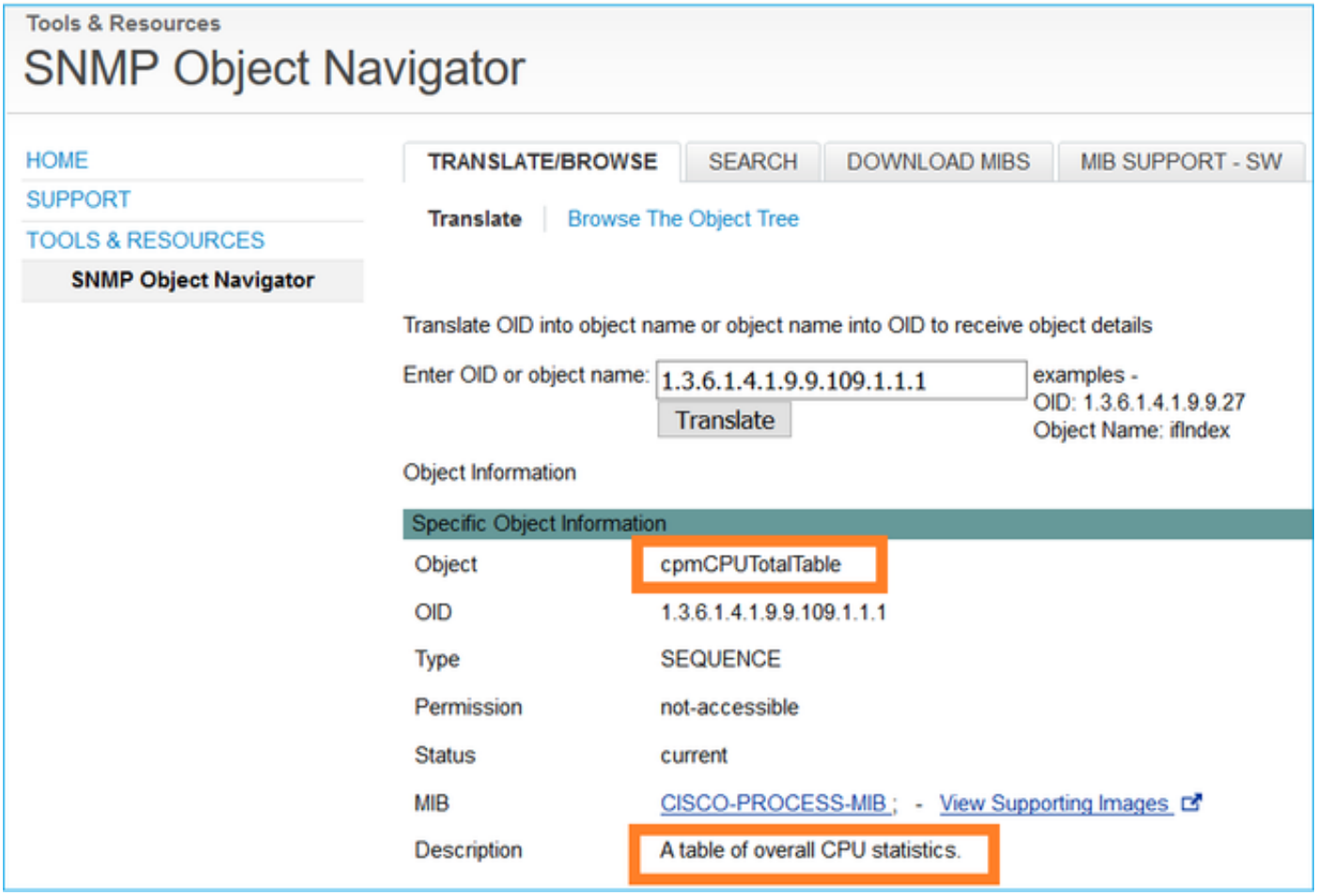
```
ksec-fpr9k-1-A /system/services #
```

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
```

OID オブジェクトナビゲータの使用

Cisco SNMP オブジェクトナビゲータは、さまざまな OID を変換して簡単な説明を取得できるオンラインツールです。



FTD LINA CLI からコマンド show snmp-server oid を使用して、ポーリングできる LINA OID のリスト全体を取得します。

<#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#
```

注：このコマンドは隠しコマンドです。

トラブルシュート

Cisco TAC によって確認された最も一般的な SNMP ケースジェネレータを以下に示します。

1. FTD LINA SNMP をポーリングできない
2. FXOS SNMP をポーリングできない
3. 使用する SNMP OID の値
4. SNMP トラップを取得できない
5. SNMP 経由で FMC を監視できない
6. SNMP を構成できない
7. Firepower Device Manager 上の SNMP 構成

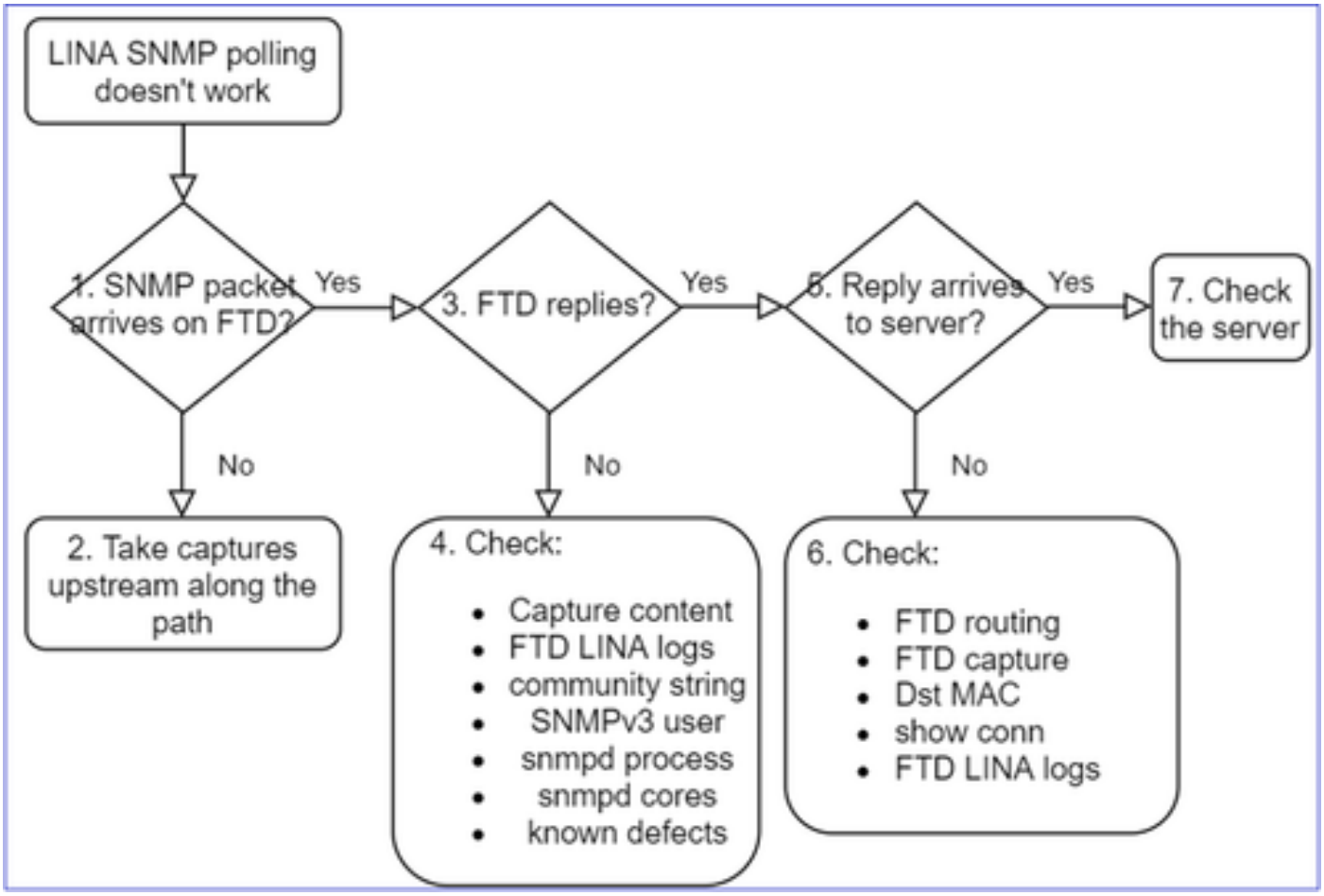
FTD LINA SNMP をポーリングできない

問題の説明（実際の Cisco TAC ケースからのサンプル）：

- 「SNMP 経由でデータを取得できません。」
- 「SNMPv2 経由でデバイスをポーリングできません。」
- 「SNMP が機能しません。SNMP でファイアウォールを監視したいのですが、構成後に問題が発生しました。」
- 「2 つの監視システムがありますが、SNMP v2c または 3 を介して FTD を監視できません。」
- 「SNMP walk がファイアウォールで機能しません。」

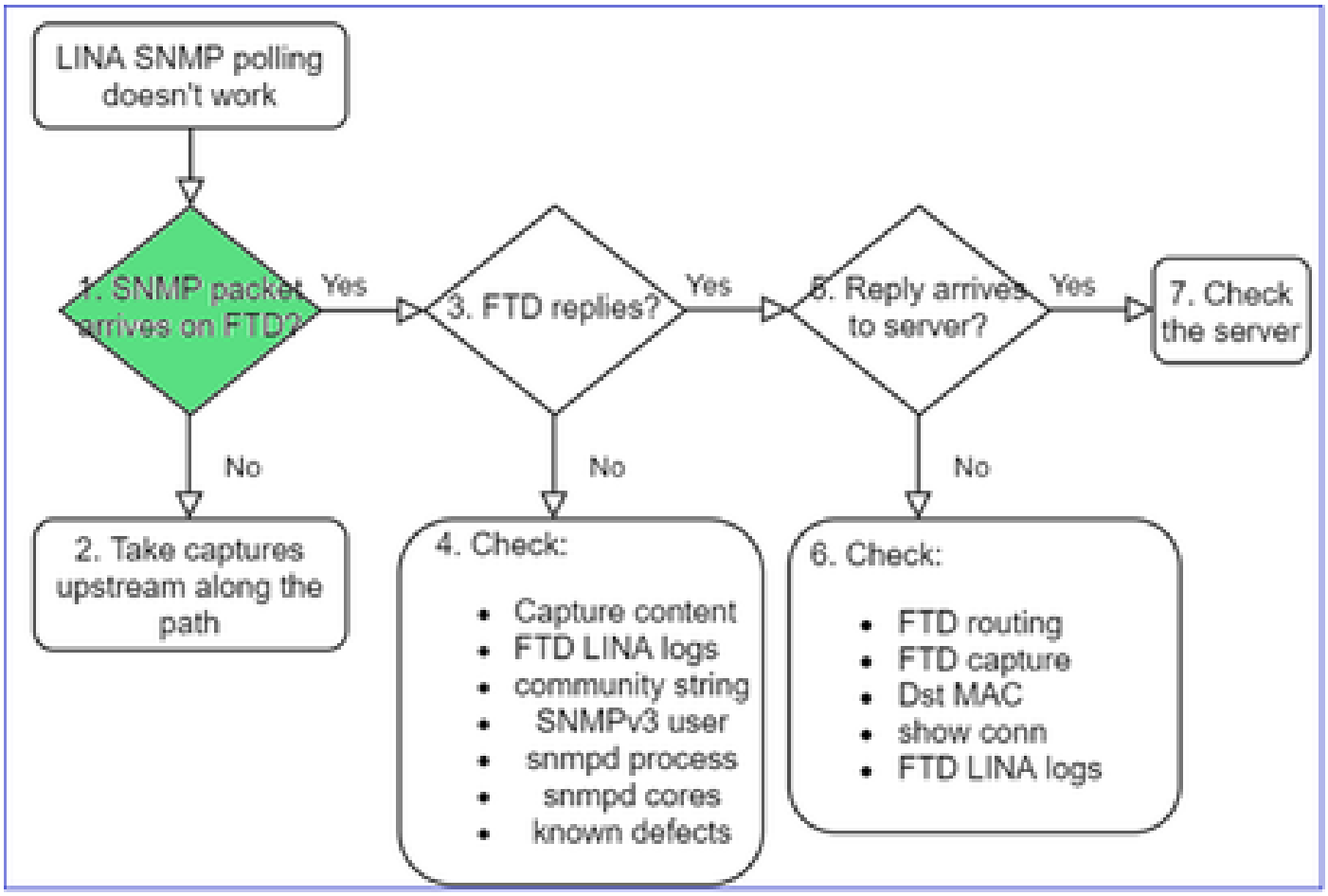
トラブルシューティング方法に関する推奨事項

LINA SNMPポーリングの問題に関するフローチャートのトラブルシューティングには、次のプロセスが推奨されます。



分析 [英語]

1. SNMPパケットはFTDに到着しますか。



- SNMPパケットの着信を確認するためにキャプチャを有効にします。

FTD管理インターフェイス（6.6以降のリリース）のSNMPでは、managementキーワードを使用します。

```
<#root>

firepower#

show run snmp-server

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

FTD データインターフェイス上の SNMP では、インターフェイスの名前を使用します。

```
<#root>

firepower#

show run snmp-server

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

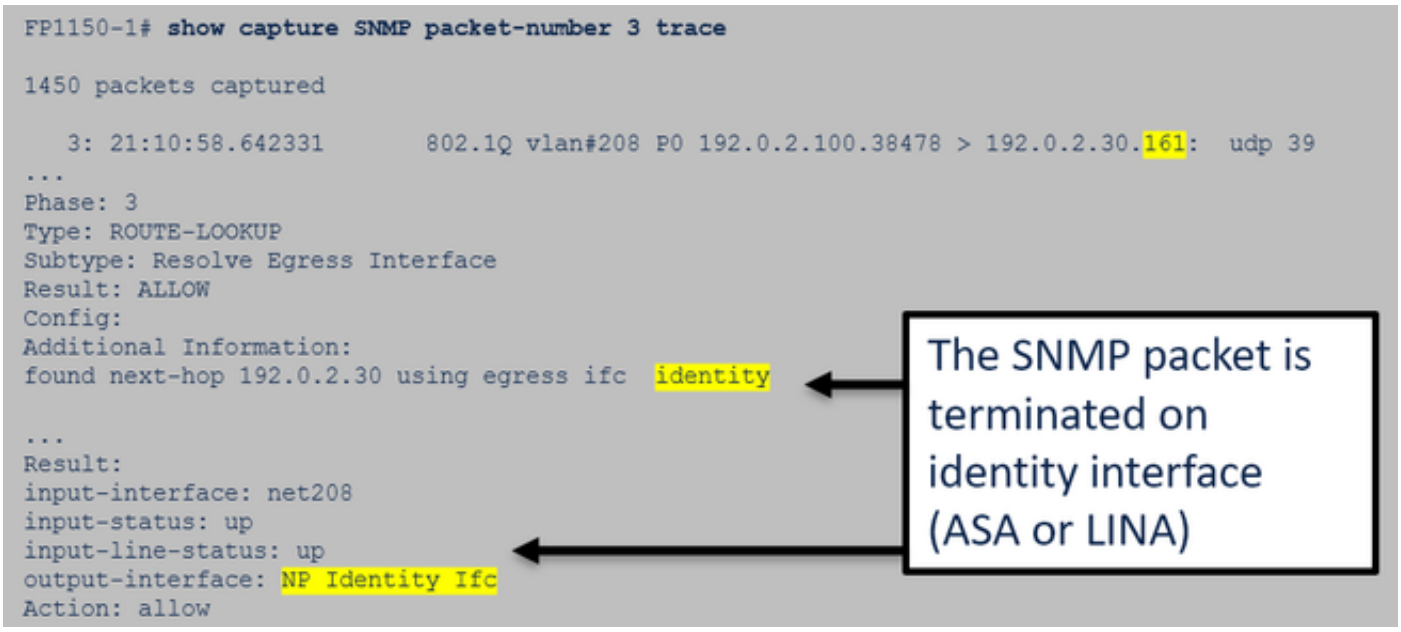
FTD 管理インターフェイスでキャプチャします。

```
<#root>

>

capture-traffic


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

1
```

FTD データインターフェイスでキャプチャします。

```
<#root>

firepower#

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

FTDデータインターフェイスのパケットトレース (6.6/9.14.1よりも前) :



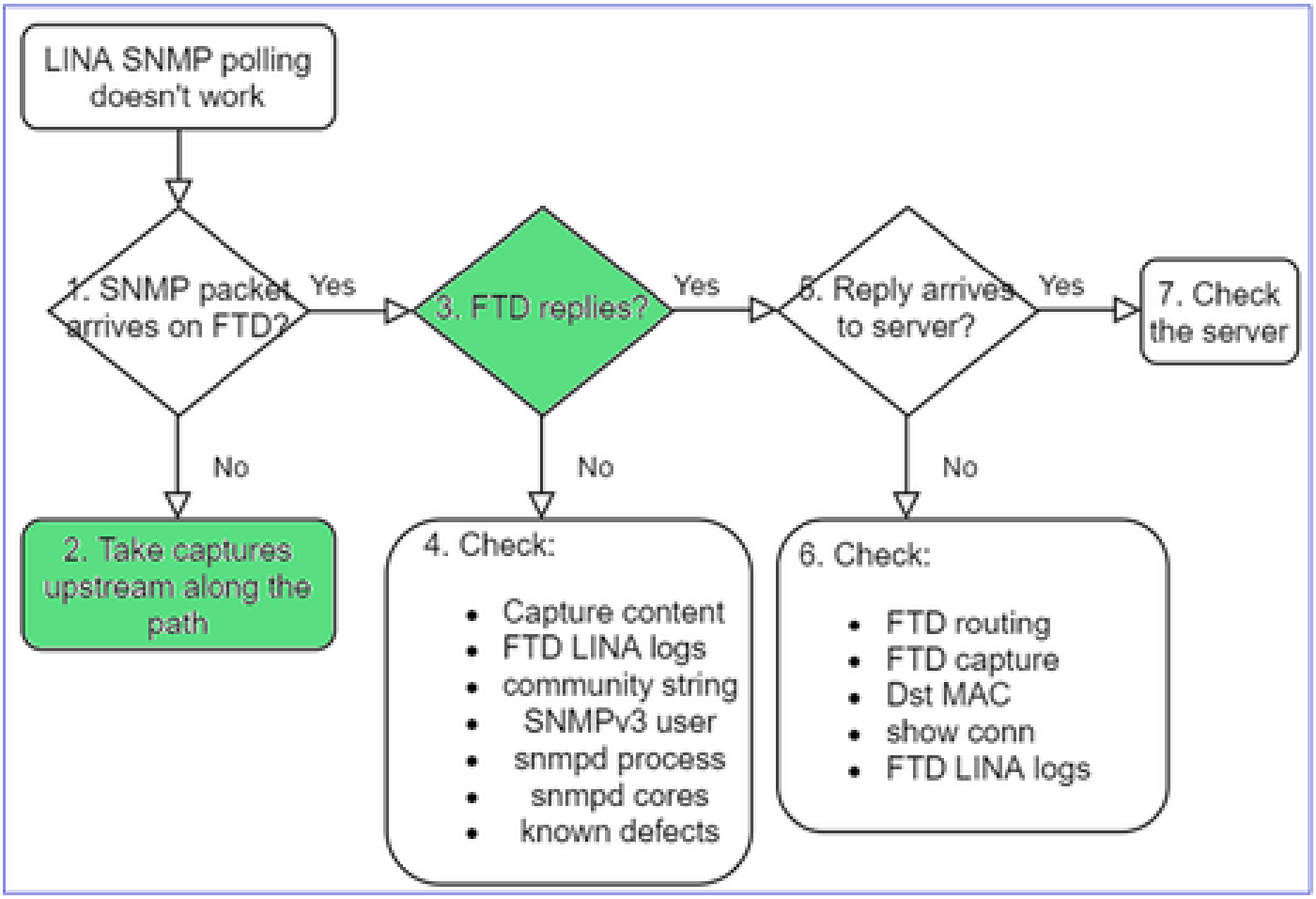
FTDデータインターフェイスパケットトレース (6.6/9.14.1以降) :

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

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

2. FTDの入力キャプチャにSNMPパケットが表示されない場合：

- パスに沿ったアップストリームのキャプチャを取得します。
- SNMPサーバが適切なFTD IPを使用していることを確認します。
- FTDインターフェイスに面するスイッチポートから開始し、アップストリームに移動します。



3. FTD SNMP 応答を確認できるか。

チェックした FTD が応答するかどうかを検証するには：

1. FTD 出力キャプチャ（LINA または管理インターフェイス）

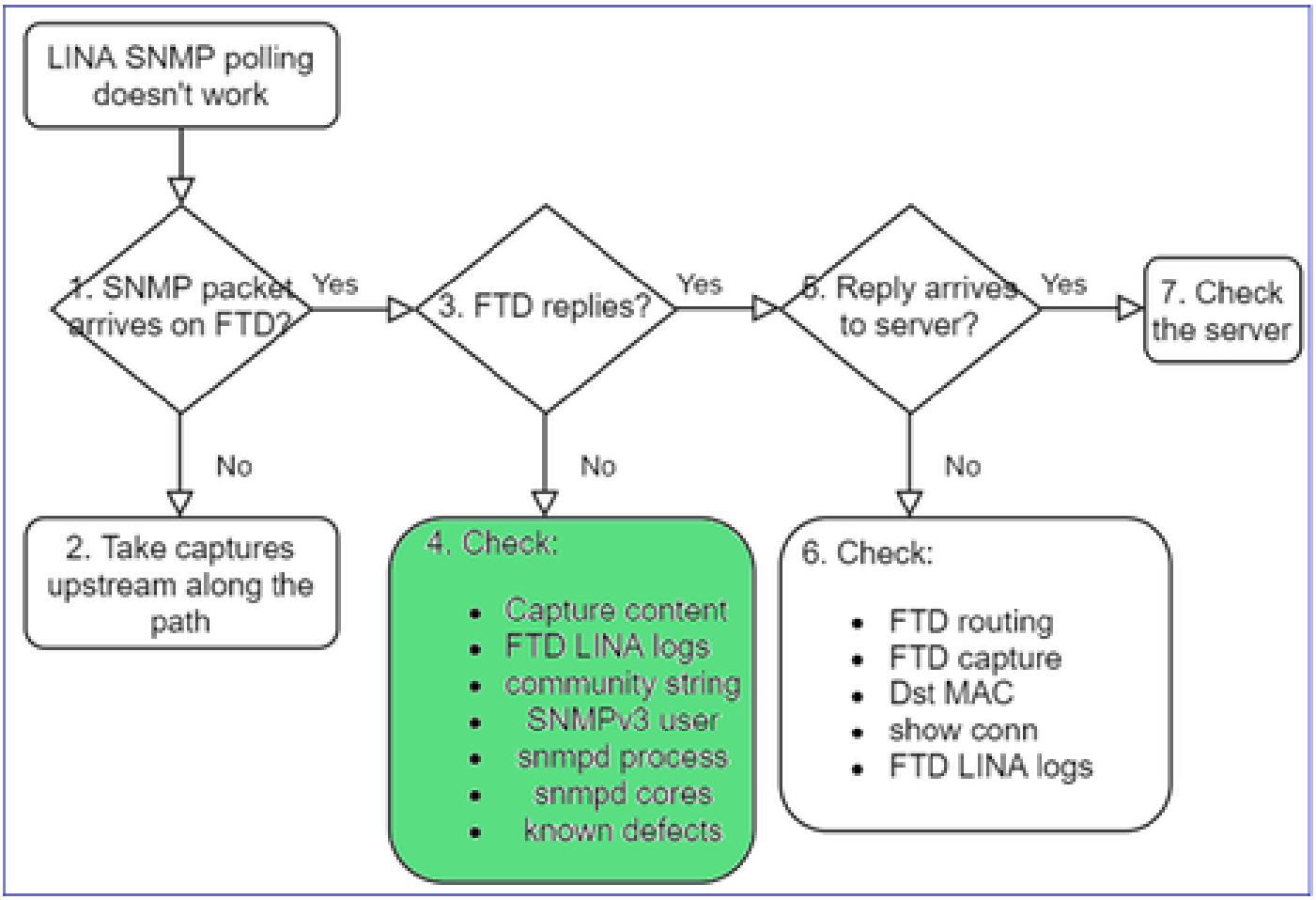
送信元ポート 161 で SNMP パケットを確認します。

```
<#root>

firepower#

show capture SNMP


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

6.6/9.14.1以降のリリースには、もう1つのキャプチャポイントがあります。それは、NLPタップインターフェイスでのキャプチャです。NAT変換されたIPアドレスは162.254.x.xの範囲です。

```
<#root>

admin@firepower:~$

sudo tcpdump -i tap_nlp


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

4.追加確認



a. Firepower4100/9300デバイスの場合は、FXOS互換表を確認してください。

Firepower 4100/9300 Compatibility with ASA and Threat Defense

The following table lists compatibility between the ASA or threat defense applications with the Firepower 4100/9300.
The FXOS versions with (EoL) appended have reached their end of life (EoL), or end of support.

Note: The **bold** versions listed below are specially-qualified companion releases. You should use these software combinations whenever possible because Cisco performs enhanced testing for these combinations.

Note: Firepower 1000/2100 appliances utilize FXOS only as an underlying operating system that is included in the ASA and threat defense unified image bundles.

Note: FXOS 2.12/ASA 9.18/Threat Defense 7.2 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.

Table 2. ASA or Threat Defense, and Firepower 4100/9300 Compatibility

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

b. FTD LINA snmp-server statisticsをチェックします。

<#root>

```
firepower#

clear snmp-server statistics


firepower#

show snmp-server statistics


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

c. FTD LINA接続テーブル

このチェックは、FTD入力インターフェイスのキャプチャにパケットが表示されない場合に非常に役立ちます。これは、データインターフェイス上のSNMPに対してのみ有効な検証であることに注意してください。SNMPが管理インターフェイス上にある場合（6.6/9.14.1以降）、connは作成されません。

<#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. FTD LINA syslog

これも、データインターフェイスの SNMP に対してのみ有効な検証です。SNMP が管理インターフェイス上にある場合、ログは作成されません。

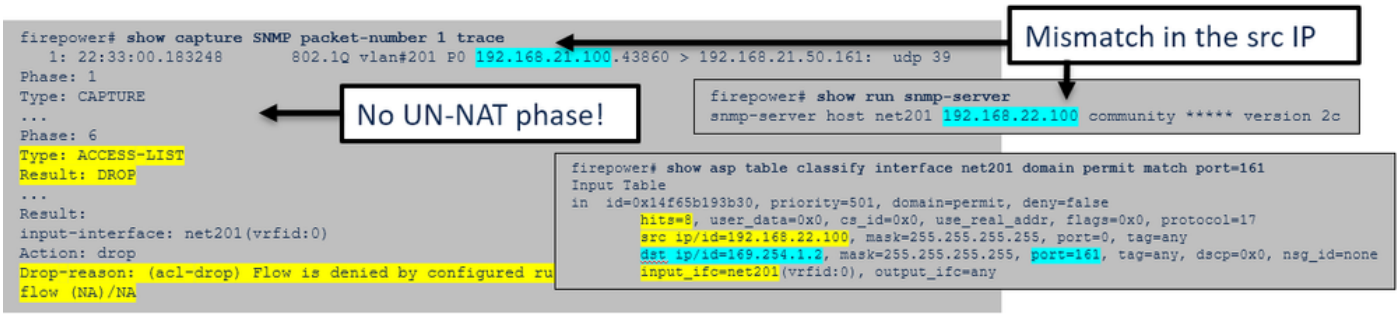
<#root>

firepower#

show log | i 302015.*161

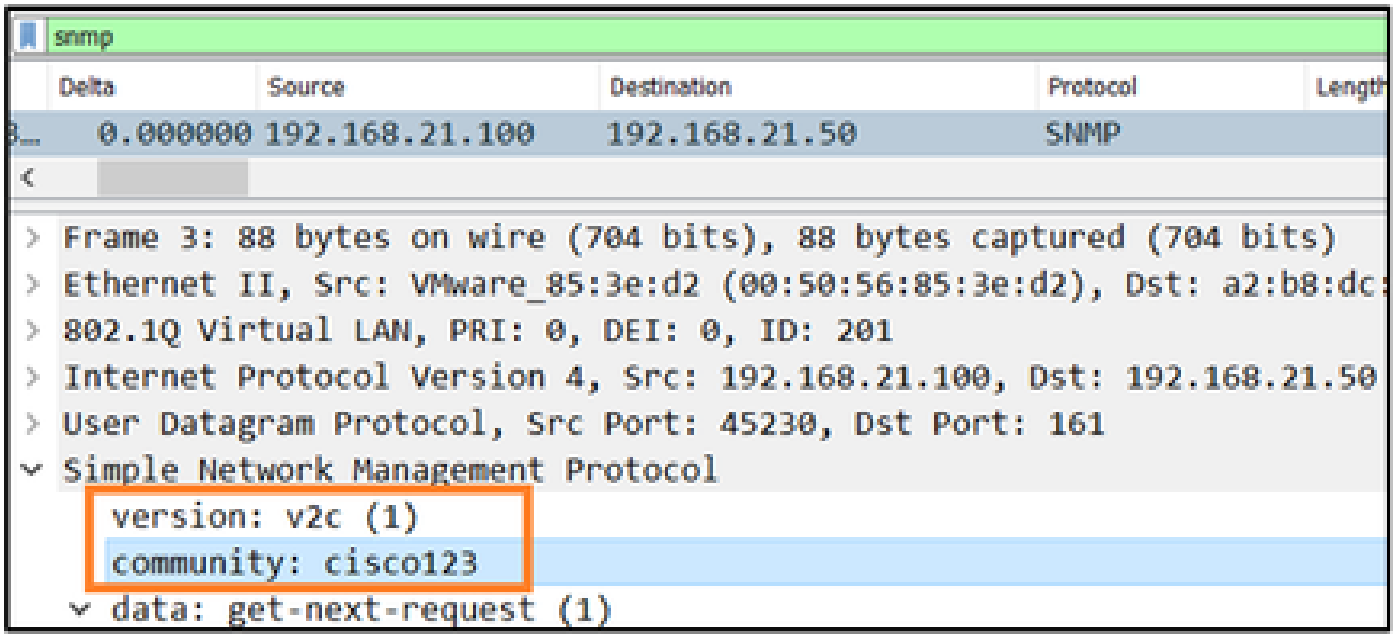
Jul 13 2021 21:24:45: %FTD-6-302015: Built inbound UDP connection 5292 for net201:192.0.2.100/42909 (19

e.ホストの送信元IPが正しくないために、FTDがSNMPパケットをドロップしていないかどうかを確認します



f.クレデンシャルが正しくない（SNMPコミュニティ）

キャプチャの内容で、コミュニティ値を確認できます（SNMP v1 および 2c）。



g.設定が正しくない（SNMPバージョン、コミュニティストリングなど）

デバイスの SNMP 設定とコミュニティストリングを確認するには、いくつかの方法があります。

<#root>

firepower#

more system:running-config | i community

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

別の方法：

```
<#root>

firepower#

debug menu netsnmp 4
```

h. FTD LINA/ASA ASPドロップ

これは、SNMP パケットが FTD によってドロップされたかどうかを確認するための便利なチェックです。まず、カウンタをクリアして（clear asp drop）、次にテストします。

```
<#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. ASPキャプチャ

ASP キャプチャは、ドロップされたパケット（たとえば、ACL や隣接関係（アジャセンシー））を可視化します。

```
<#root>

firepower#

capture ASP type asp-drop all
```

テストして、キャプチャの内容を確認します。

```
<#root>
firepower#
show capture

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

j. SNMPコア（トレースバック）：検証方法1

このチェックは、システムの安定性の問題が疑われる場合に役立ちます。

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

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

SNMP コア（トレースバック）：検証方法 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
```

SNMP コアファイルが見つかった場合は、次の項目を収集して、Cisco TAC に連絡してください。

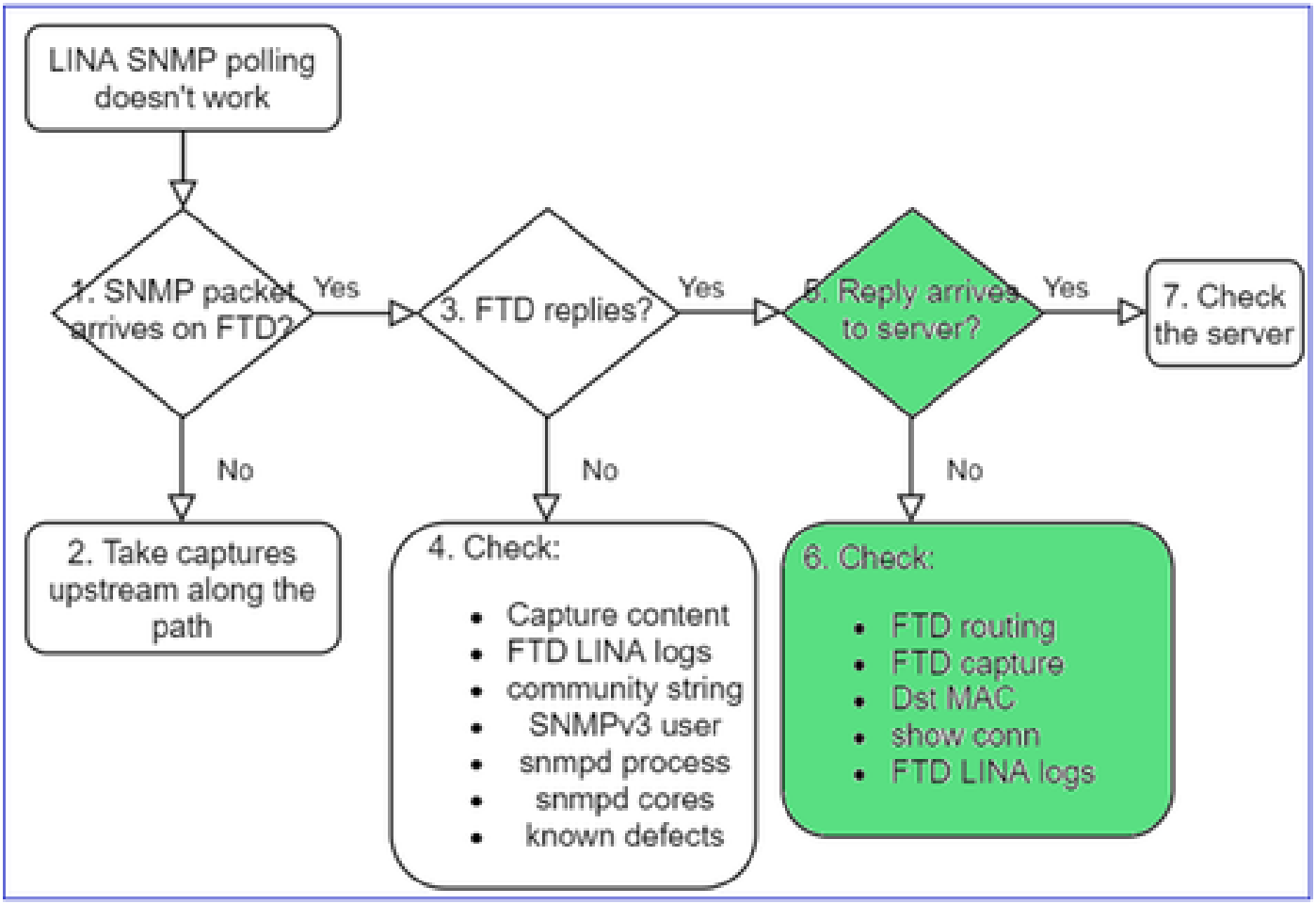
- FTD TS ファイル（または ASA show tech）
- snmpd コアファイル

SNMP デバッグ（これらは隠しコマンドであり、新しいバージョンでのみ使用可能）：

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

```
firepower#
debug snmp verbose [255]

firepower#
debug snmp error [255]

firepower#
debug snmp packet [255]
```

ファイアウォールの SNMP 応答はサーバーに到達するか。



FTD が応答したが、応答がサーバーに到達しない場合は、次のようにチェックします。

a. FTDルーティング

FTD 管理インターフェイスのルーティングの場合：

```
<#root>

>

show network
```

FTD LINA データインターフェイスのルーティングの場合：

```
<#root>

firepower#

show route
```

b.宛先MACの確認

FTD 管理インターフェイスの宛先 MAC 検証：

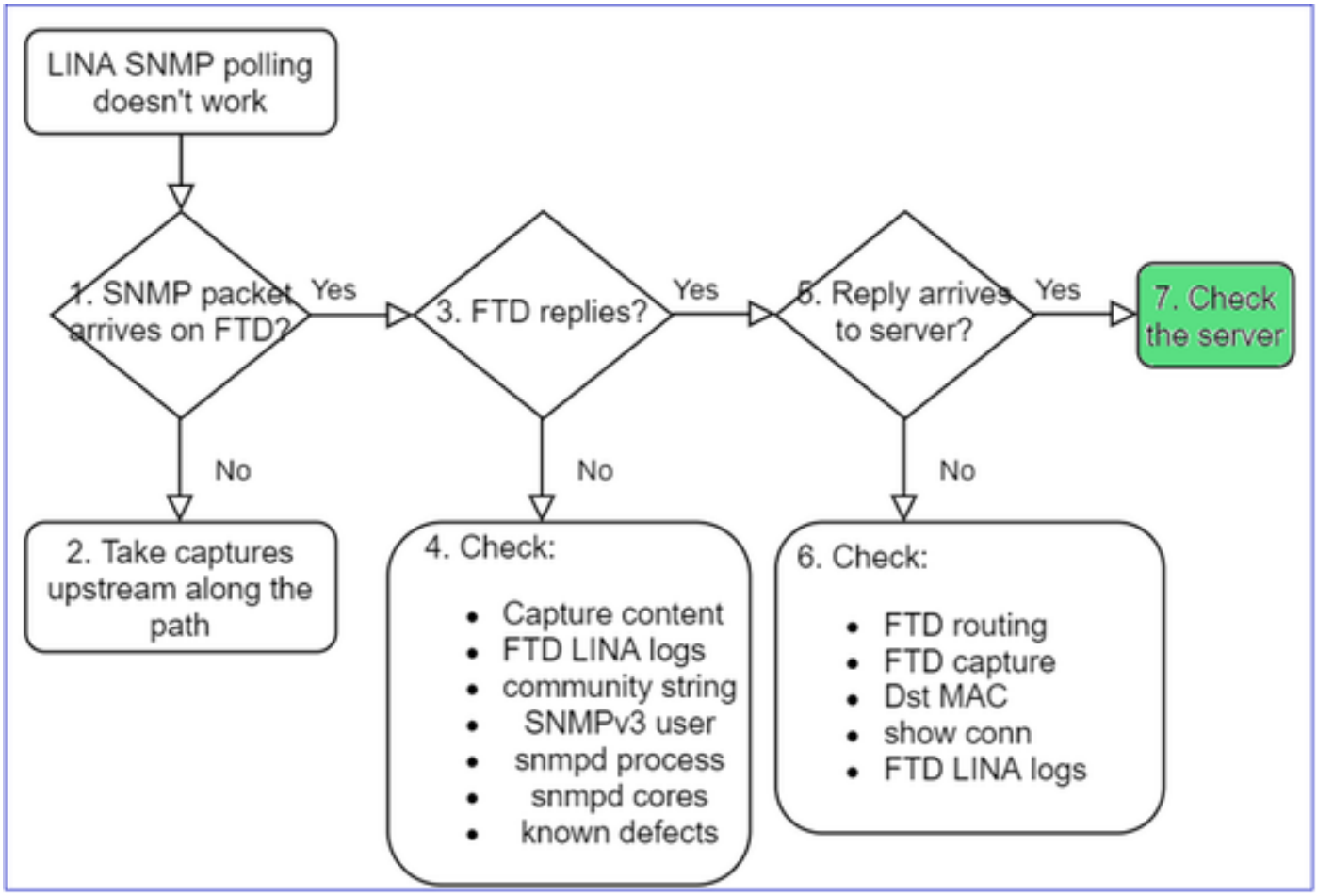
```
<#root>

>

capture-traffic


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

1


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

-n -e udp port 161


01:00:59.553385 a2:b8:dc:00:00:02 > 5c:fc:66:36:50:ce, ethertype IPv4 (0x0800), length 161: 10.62.148.1
```

FTD LINA データインターフェイスの宛先 MAC 検証：

```
<#root>

firepower#

show capture SNMP detail


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

c. SNMP パケットをドロップ/ブロックする可能性のあるパス上のデバイスを確認します。

SNMP サーバーの確認



a.設定を確認するには、キャプチャの内容を確認します。

b.サーバ設定を確認します。

c. SNMPコミュニティ名を変更してみます（たとえば、特殊文字を使用しません）。

次の2つの条件が満たされている限り、エンドホストまたはFMCを使用してポーリングをテストできます。

1. SNMP 接続が確立されている.
2. 送信元 IP がデバイスのポーリングを許可されている.

<#root>

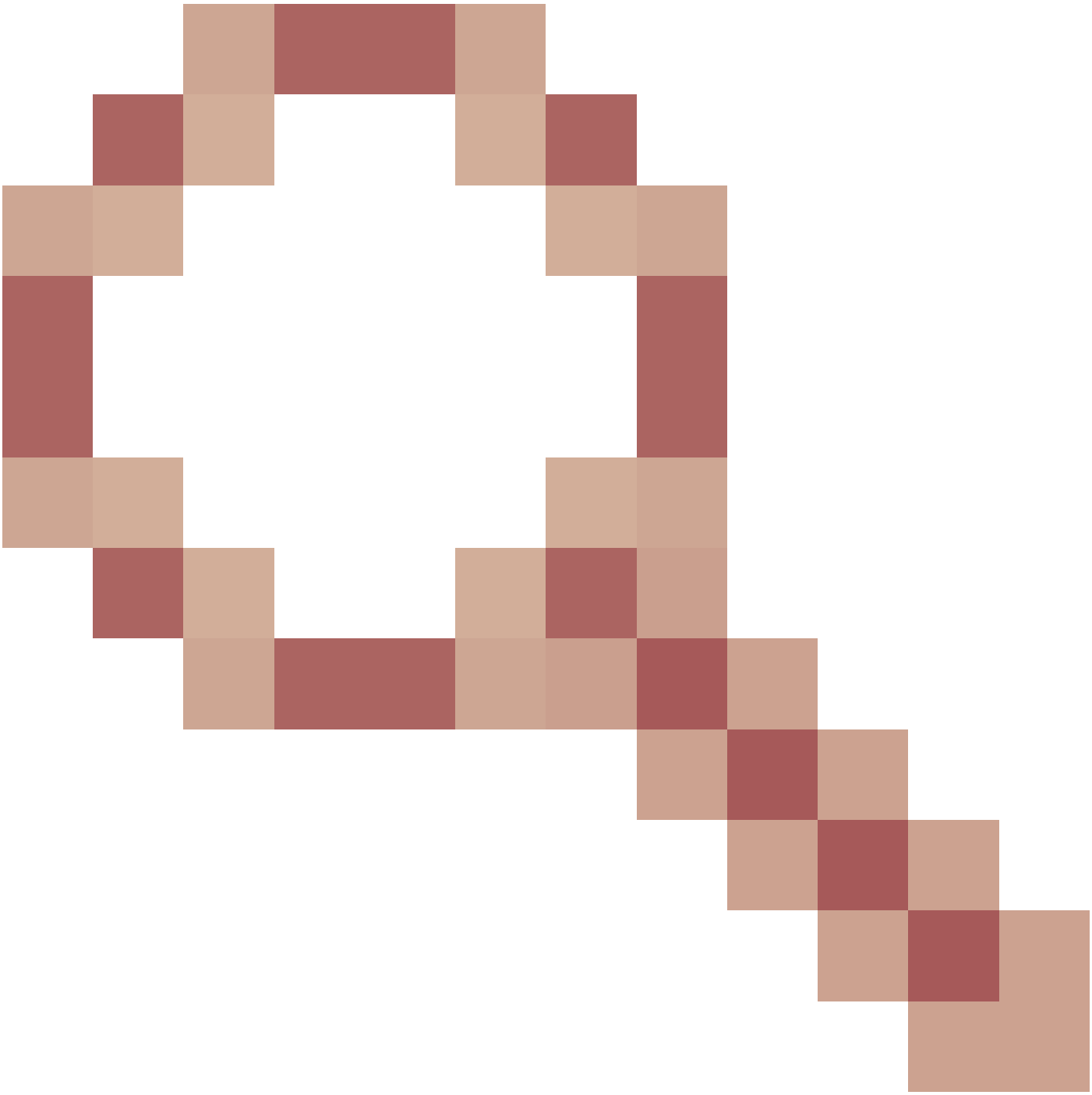
```
admin@FS2600-2:~$
```

```
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
```

SNMPv3ポーリングの考慮事項

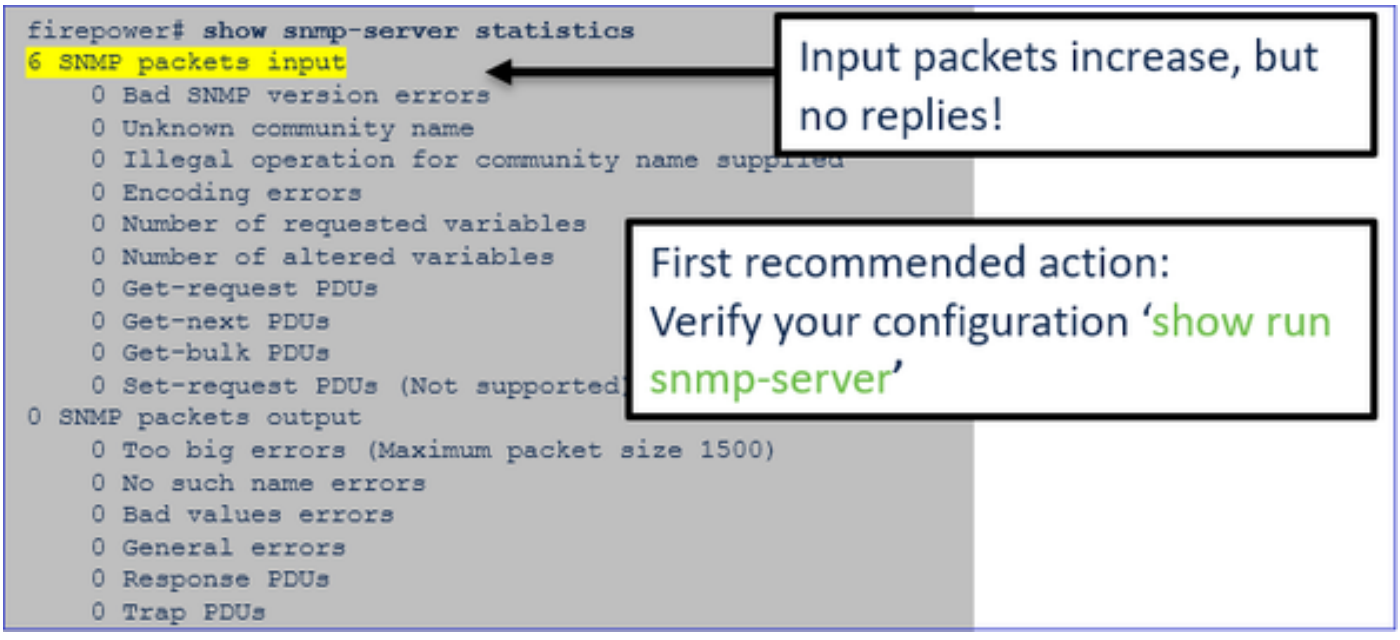
- ライセンス：SNMPv3には強力な暗号化ライセンスが必要です。スマートライセンスポータルで輸出規制機能が有効になっていることを確認します。
- トラブルシューティングを行うには、新しいユーザ/クレデンシャルを試すことができます
- 暗号化を使用する場合は、https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59で説明されているように、SNMPv3トラフィックを復号化し、ペイロードを確認できます。
- ソフトウェアが次のような不具合の影響を受ける場合は、暗号化に AES128 を検討してください。
- Cisco Bug ID CSCvy27283



ASA/FTD SNMPv3のポーリングが、プライバシーアルゴリズムAES192/AES256を使用して失敗する可能性がある

Cisco Bug ID CSCvx45604
auth shaおよびpriv aes 192を使用するユーザでsnmpv3ウォークが失敗する

注：アルゴリズムの不一致が原因でSNMPv3に障害が発生した場合は、showの出力に何も表示されず、ログに明白な情報は何も表示されません



SNMPv3 ポーリングに関する考慮事項 - ケーススタディ

1. SNMPv3 snmpwalk - 機能シナリオ

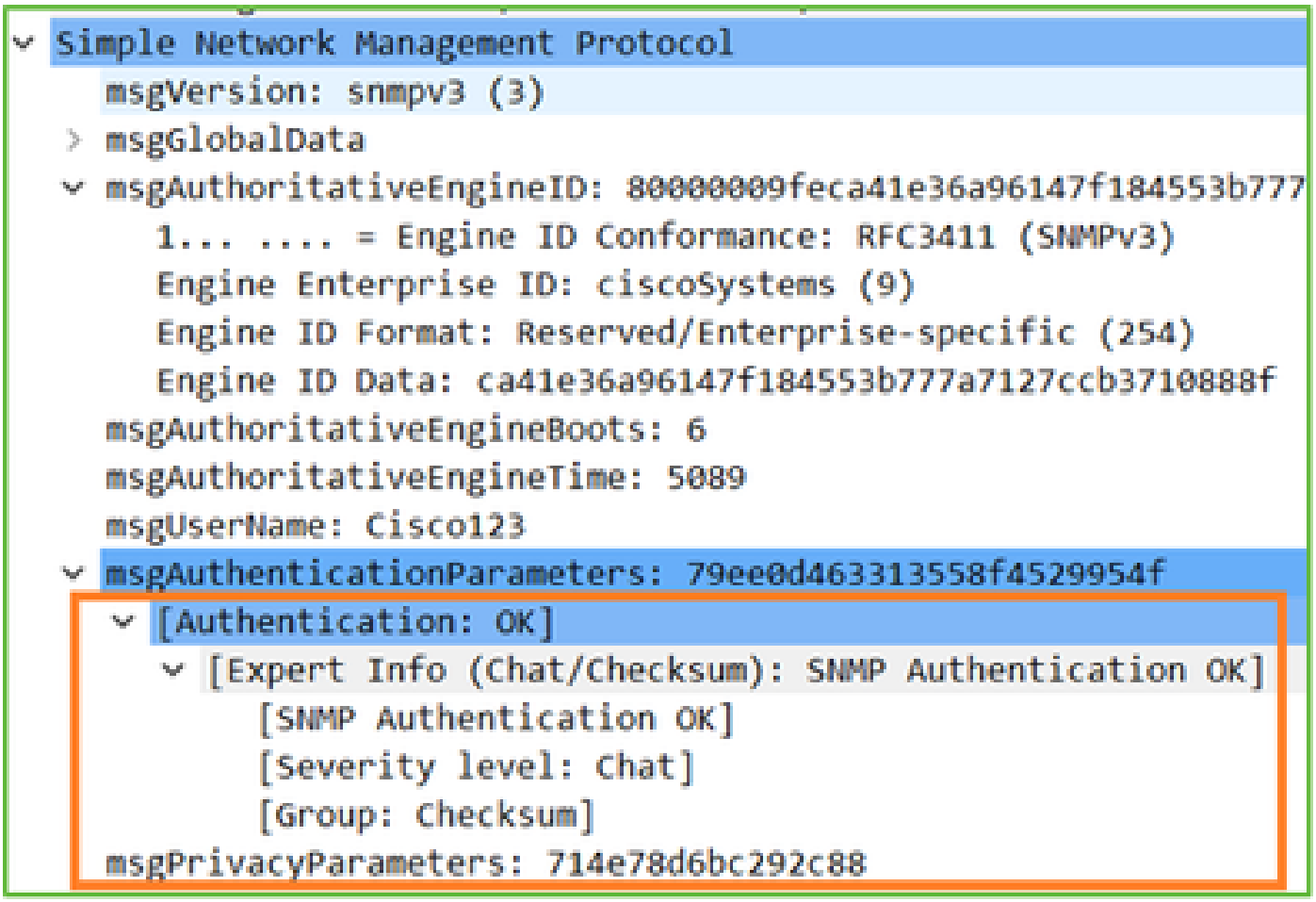
<#root>

```
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
```

キャプチャ（snmpwalk）では、各パケットの応答が表示されます。

```
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
```

キャプチャファイルには異常は何も表示されません。



2. SNMPv3 snmpwalk - 暗号化の失敗

ヒント#1：タイムアウトがあります：

<#root>

admin@FS2600-2:~$

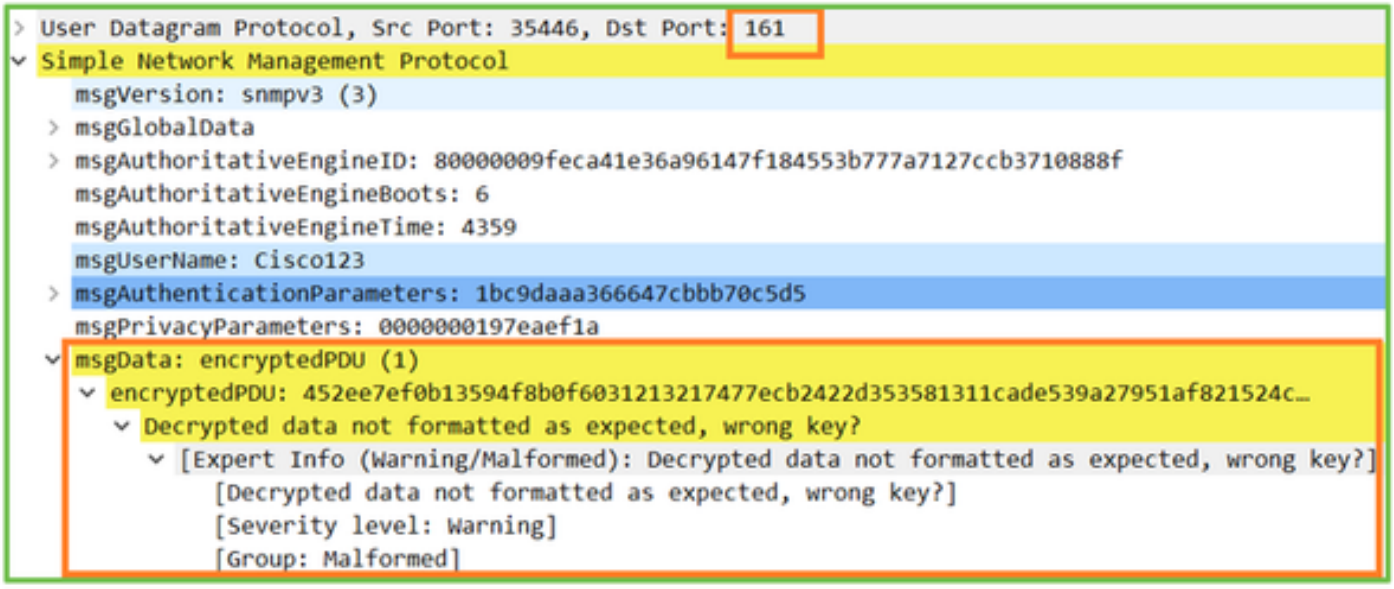
snmpwalk -v 3 -u Cisco123 -l authPriv -a SHA -A Cisco123 -x DES -X Cisco123 192.168.21.50

Timeout: No Response from 192.168.2.1

ヒント#2：多くの要求と1つの応答があります：

```
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
```

ヒント#3: Wiresharkの暗号化解除が失敗しました：



ヒント#4ma_ctx2000.logファイルで「error parsing ScopedPDU」メッセージを確認します。

<#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
```

ScopedPDUの解析エラーは、暗号化エラーの強力なヒントです。ma_ctx2000.logファイルには、SNMPv3！のイベントだけが表示されます。

3. SNMPv3 snmpwalk - 認証の失敗

ヒント#1：認証の失敗

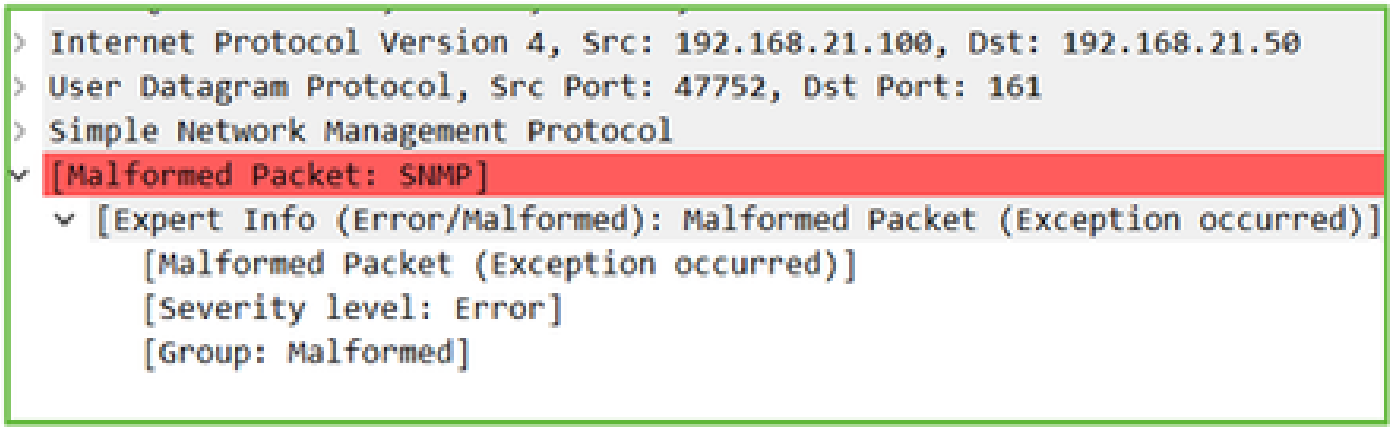
<#root>

```
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)
```

ヒント#2：多くの要求と多くの応答があります

```
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
```

ヒント#3:Wiresharkの不正なパケット



ヒント#4ma_ctx2000.logファイルで「Authentication failed」メッセージを確認します。

```
<#root>

>

expert


admin@firepower:~$

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


Authentication failed for Cisco123
Authentication failed for Cisco123
```

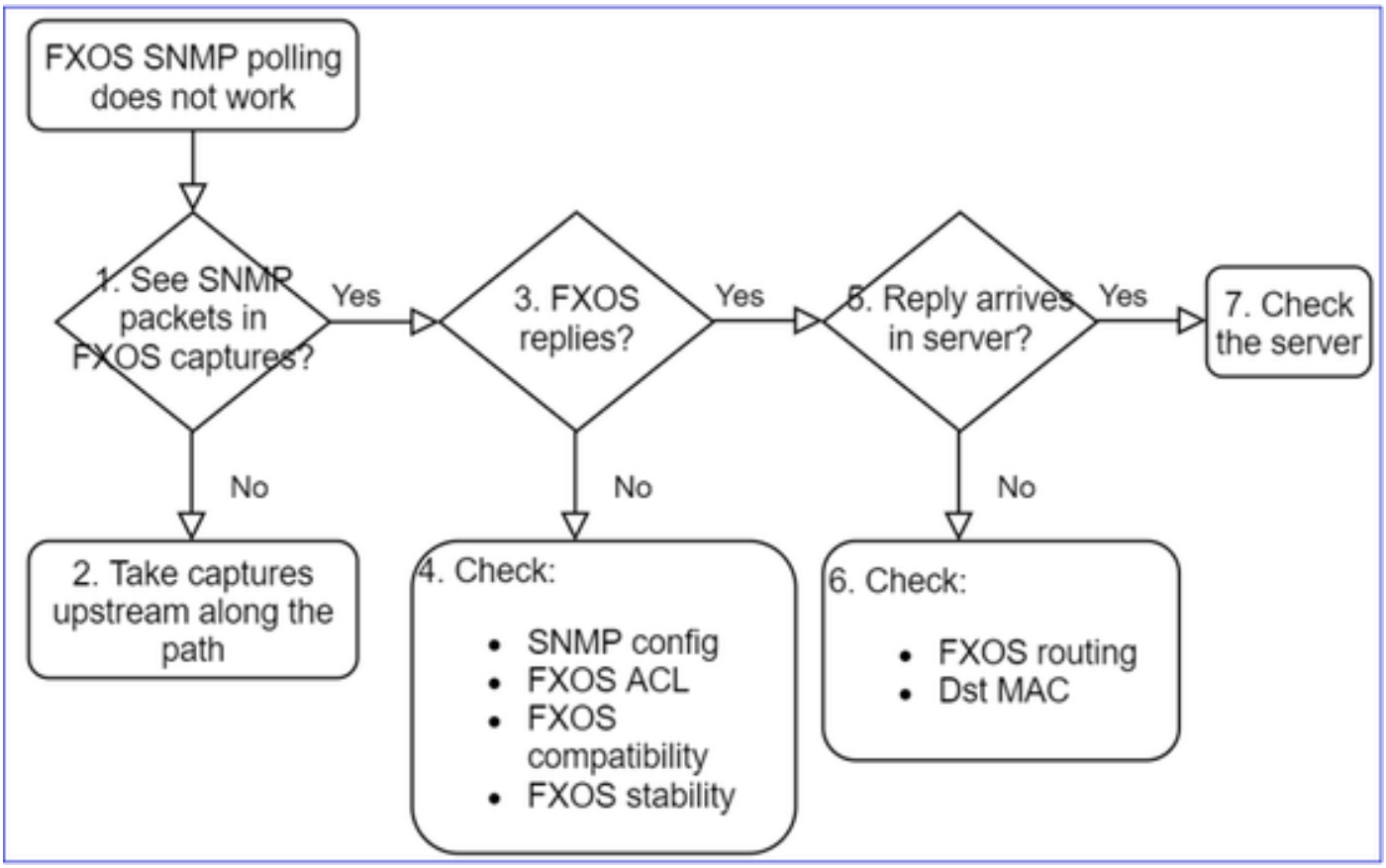
FXOS SNMP をポーリングできない

問題の説明（実際の Cisco TAC ケースからのサンプル）：

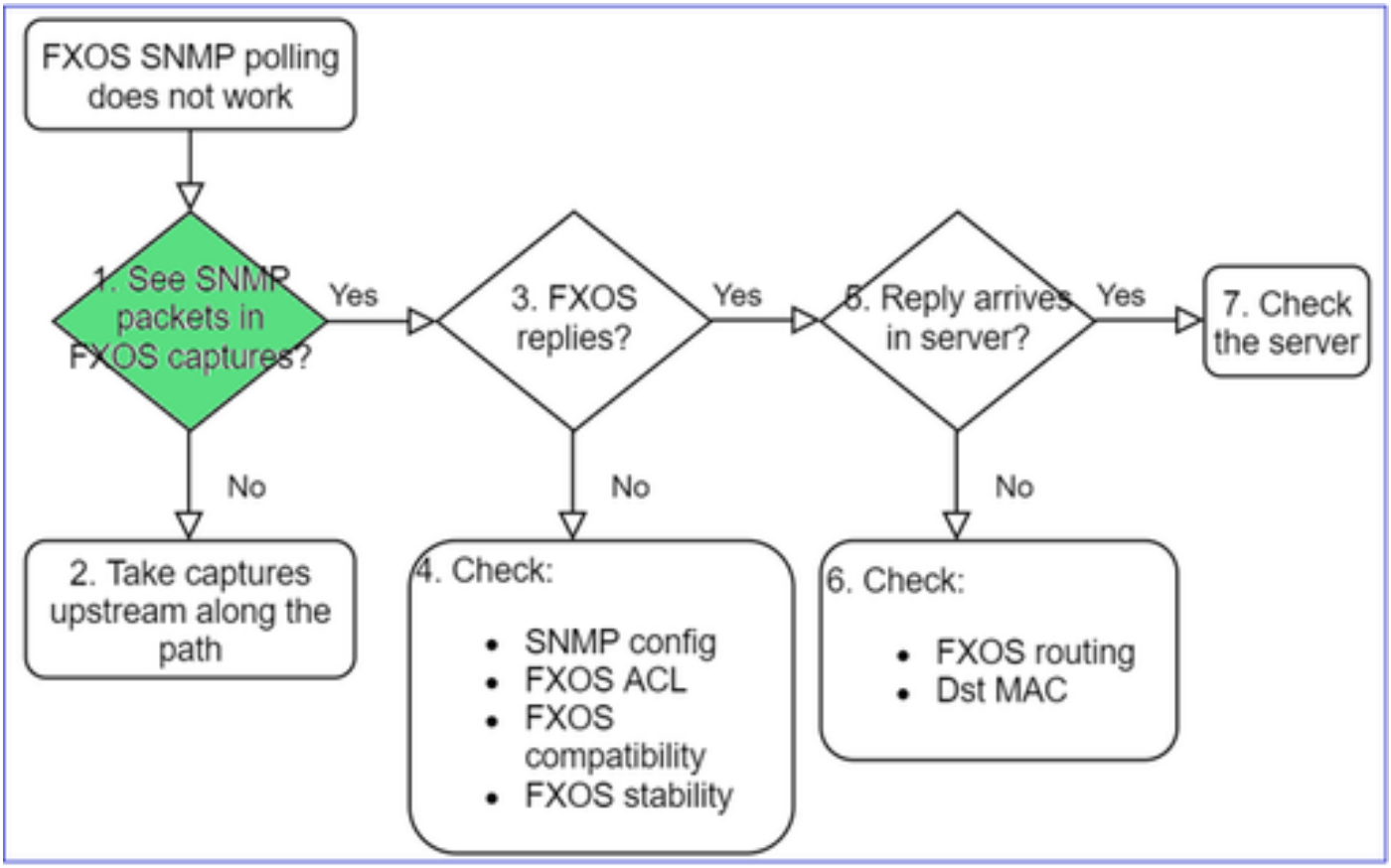
- 「SNMP は FXOS の間違ったバージョンを提供します。FXOS のバージョンについて SNMP でポーリングする場合、出力を理解するのが困難です。」
- 「FXOS FTD4115 で snmp コミュニティをセットアップできません。」
- 「スタンバイファイアウォールで FXOS を 2.8 から 2.9 にアップグレードした後、SNMP 経由で情報を受信しようとするとタイムアウトが発生します。」
- 「snmpwalk は 9300 fxos では失敗しますが、同じバージョンの 4140 fxos では機能します。到達可能性とコミュニティは問題ではありません。」
- 「FPR4K FXOS に 25 の SNMP サーバーを追加したいのですが、できません。」

推奨されるトラブルシューティング

これは、FXOS SNMPポーリングの問題に関するフローチャートをトラブルシューティングするプロセスです。



1. FXOS キャプチャに SNMP パケットが表示されるか。



FPR1xxx/21xx

- FPR1xxx/21xxでは、シャーシマネージャ（アプライアンスモード）はありません。
- 管理インターフェイスからFXOSソフトウェアをポーリングできます。

```
<#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
```

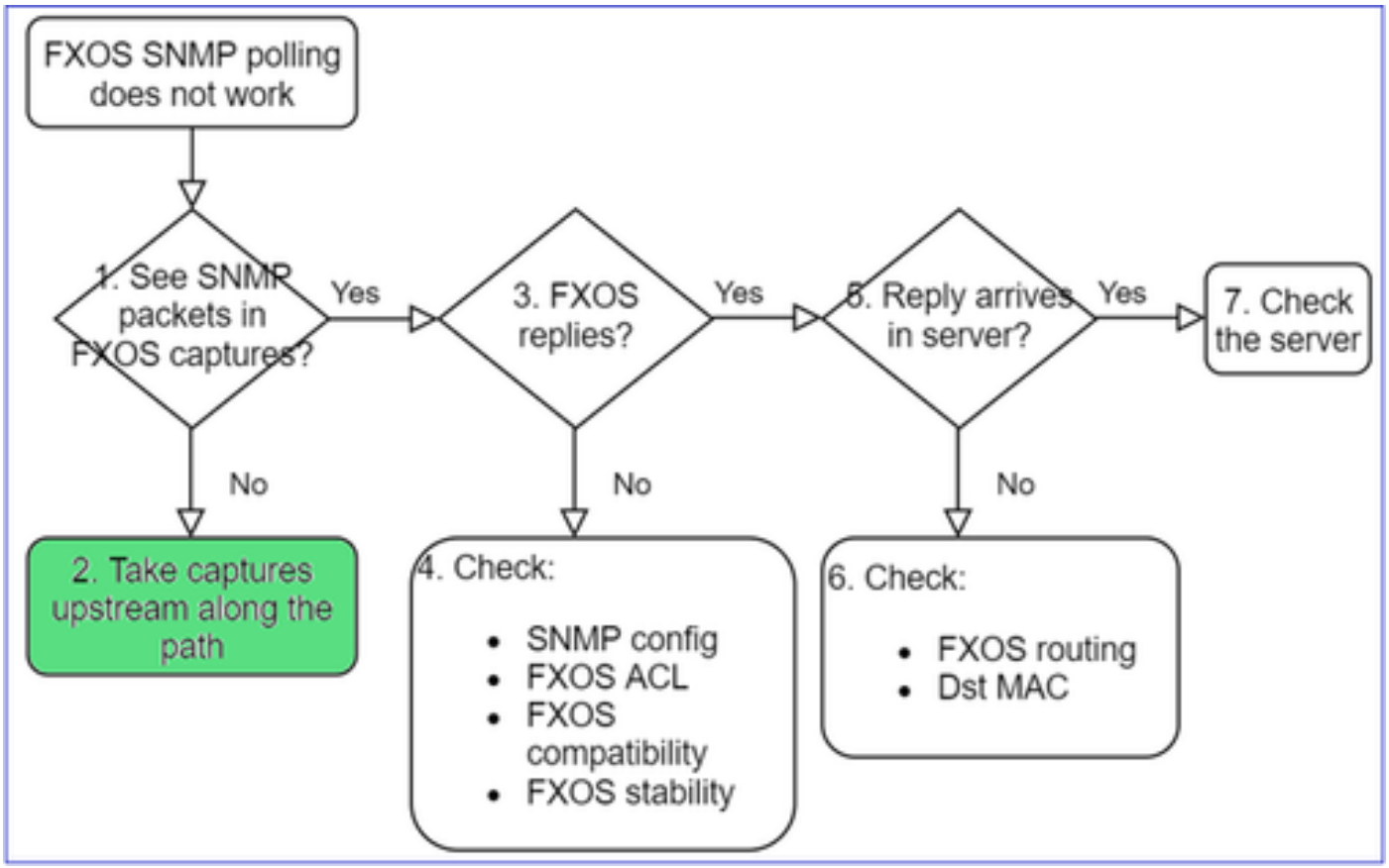
41xx/9300

- Firepower 41xx/93xx では、Ethanalyzer CLI ツールを使用してシャーシキャプチャを取得します。

<#root>

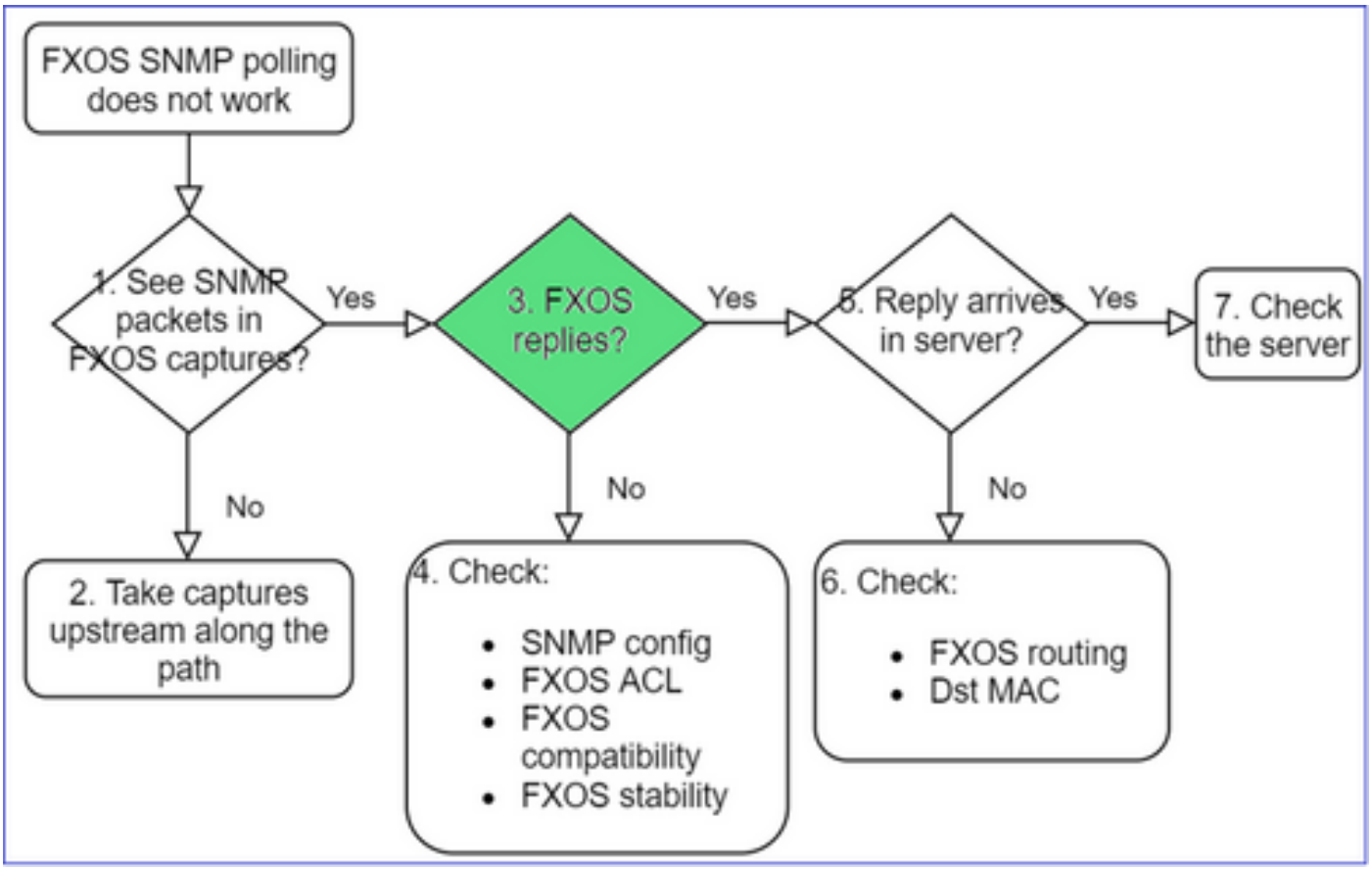
```
firepower#
connect fxos

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

firepower(fxos)#
exit

firepower#
connect local-mgmt

firepower(local-mgmt)#
dir


1
 11152 Jul 26 09:42:12 2021 SNMP.pcap
firepower(local-mgmt)#
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. FXOS キャプチャにパケットがないか。



- パスに沿ってアップストリームでキャプチャします。

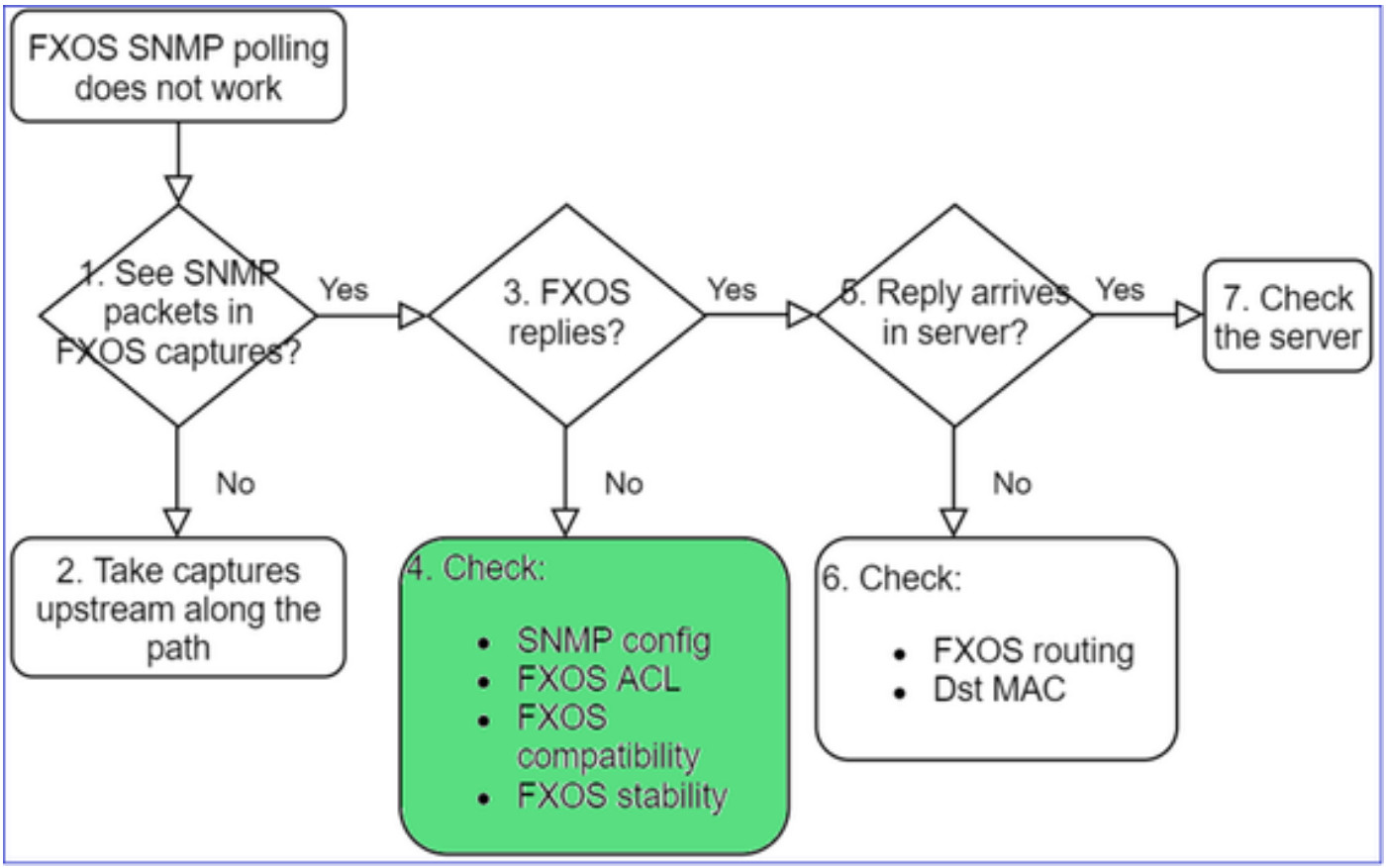
3. FXOS 応答はあるか。



- 機能シナリオ：

```
<#root>

>

capture-traffic


...
Options:

-n host 192.0.2.23 and udp port 161


HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on management0, link-type EN10MB (Ethernet), capture size 262144 bytes
08:17:25.952457 IP 192.168.2.23.36501 > 192.168.2.28.161:  C="Cisco123" GetNextRequest(25)  .10.3.1.1.2
08:17:25.952651 IP 192.168.2.28.161 > 192.168.2.23.36501:  C="Cisco123" GetResponse(97)  .1.10.1.1.1.1.
```

4. FXOS が応答しません。



その他の確認事項

- SNMP 構成を検証します（UI または CLI から）。

```
<#root>
```

```
firepower#
scope monitoring

firepower /monitoring #
show snmp

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

- 特殊文字 (「$」など) に注意してください。

<#root>

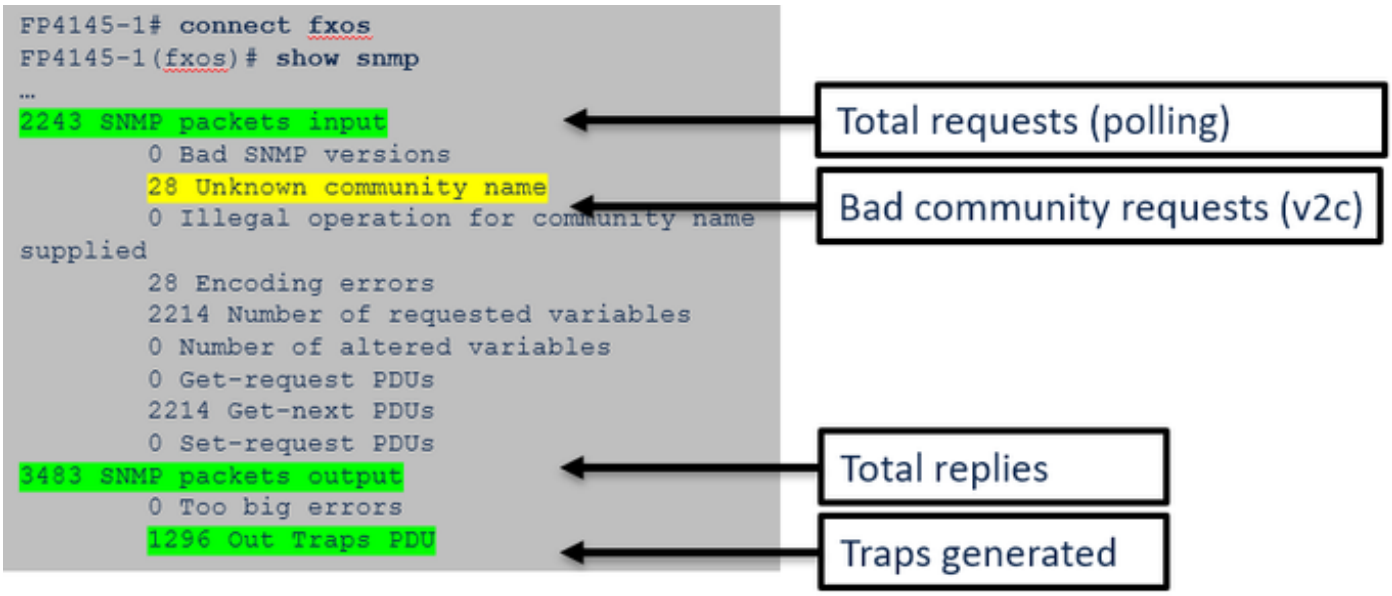
```
FP4145-1#
connect fxos

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

FP4145-1(fxos)#
show snmp community

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

- SNMP v3 の場合は、show snmp-user [detail] を使用します。
- FXOS の互換性を検証します。

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

4. FXOS が応答しない場合

FXOS SNMP カウンタを確認します。



- FXOS アクセス制御リスト（ACL）を確認します。これは、FPR41xx/9300 プラットフォームにのみ適用されます。

トラフィックがFXOS ACLによってブロックされている場合、要求は表示されますが、応答は表示されません。

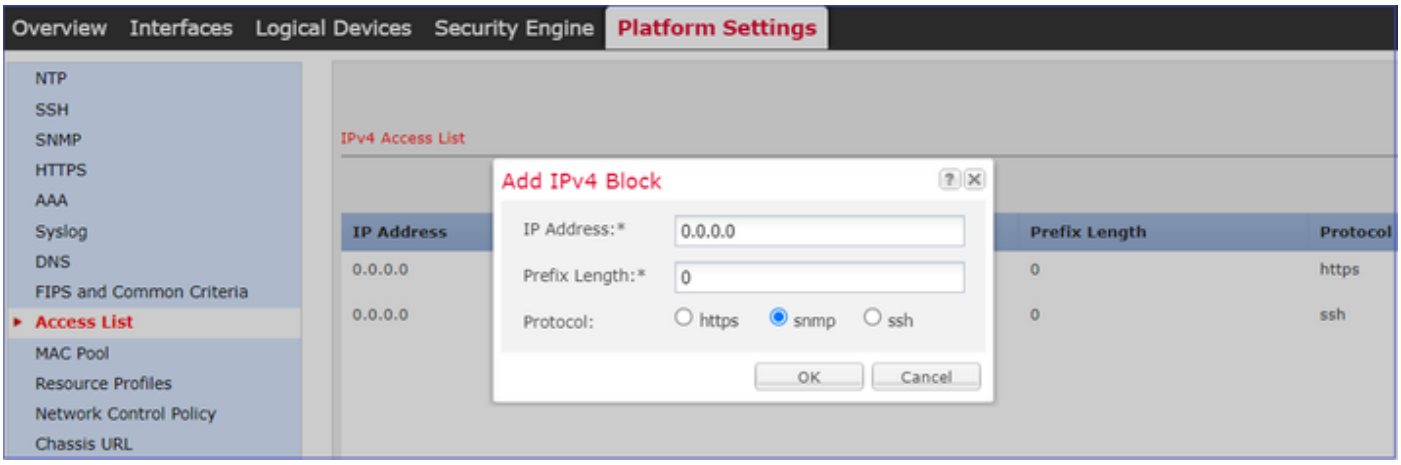
<#root>

firepower(fxos)#

ethanalyzer local interface mgmt capture-filter

"udp port 161" limit-captured-frames 50 write workspace:///SNMP.pcap
Capturing on 'eth0'
    1 2021-07-26 11:56:53.376536964 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1
    2 2021-07-26 11:56:54.377572596 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.10.1.10.1.1
    3 2021-07-26 11:56:55.378602241 192.0.2.23 → 192.168.2.37 SNMP 84 get-next-request 10.3.1.10.2.1

ユーザーインターフェイス（UI）から FXOS ACL を確認できます。



CLI から FXOS ACL を確認することもできます。

```
<#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
```

- SNMP をデバッグします（パケットのみ）。FPR41xx/9300 のみに適用されます。

```
<#root>

FP4145-1#

connect fxos

FP4145-1(fxos)#

 terminal monitor

FP4145-1(fxos)#

debug snmp pkt-dump

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

- Debug SNMP(all)：このデバッグ出力は非常に冗長です。

```
<#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
```

- SNMP 関連の FXOS 障害があるかどうかを確認します。

<#root>

FXOS#

show fault

```
Severity Code Last Transition Time ID Description
--------- -------- ----------------------- -------- -----------
Warning F78672 2020-04-01T21:48:55.182 1451792 [FSM:STAGE:REMOTE-ERROR]: Result: resource-unavailable C
```

- snmpd コアがあるかどうかを確認します。

FPR41xx/FPR9300 の場合：

<#root>

firepower#

connect local-mgmt

firepower(local-mgmt)#

dir cores

```
1 1983847 Apr 01 17:26:40 2021 core.snmpd.10012.1585762000.gz
1 1984340 Apr 01 16:53:09 2021 core.snmpd.10018.1585759989.gz
```

FPR1xxx/21xx の場合：

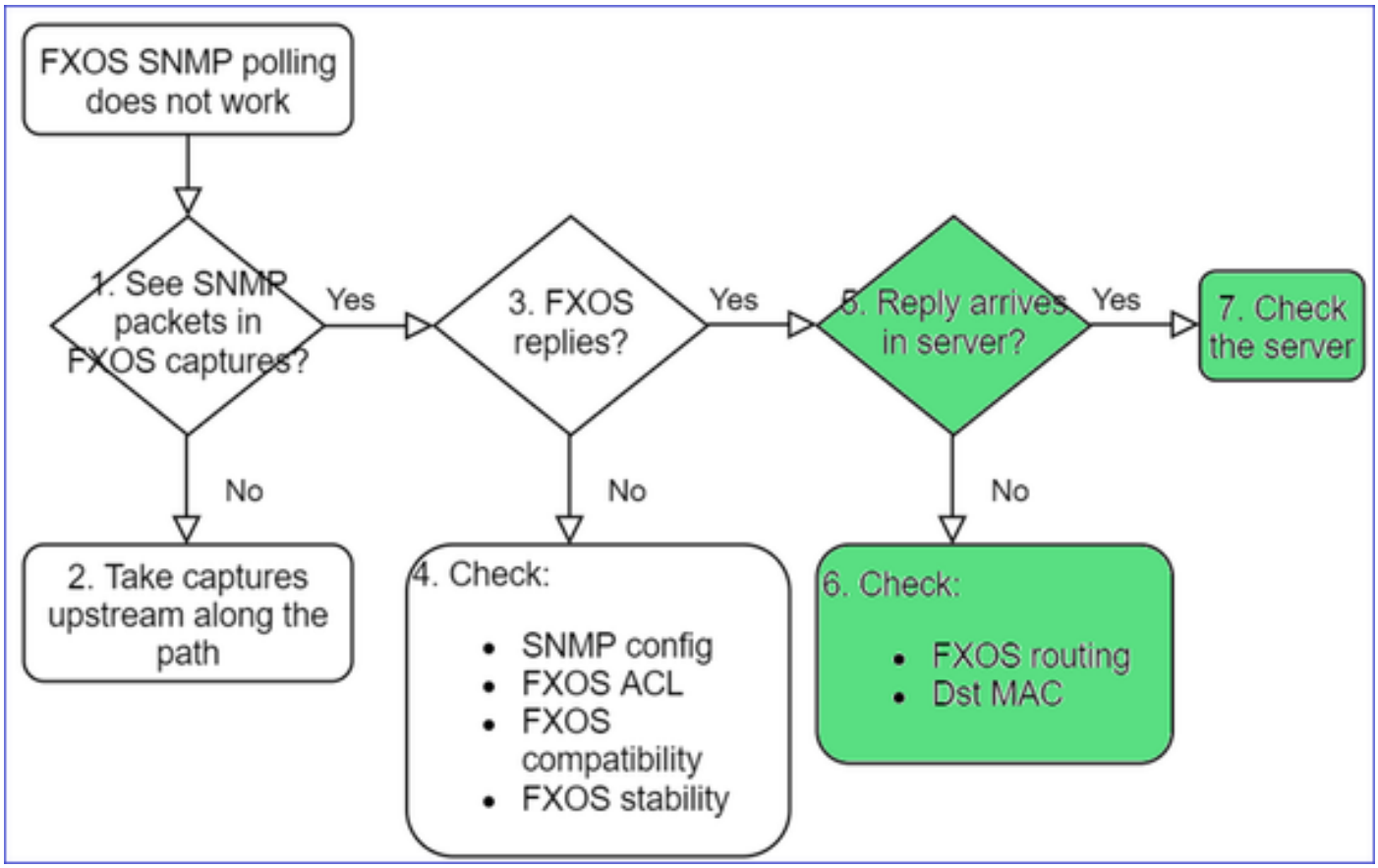
<#root>

firepower(local-mgmt)#

dir cores_fxos

snmpd コアが見つかった場合は、コアを FXOS トラブルシュートバンドルとともに収集し、Cisco TAC に連絡してください。

5. SNMP 応答は SNMP サーバーに到達するか。



- FXOS ルーティングを確認します。

この出力は FPR41xx/9300 からのものです。

<#root>

```
firepower#
```

show fabric-interconnect

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

- キャプチャを取得し、pcap をエクスポートして、応答の宛先 MAC を確認します。
- 最後に、SNMP サーバー（キャプチャ、構成、アプリケーションなど）を確認します。

使用する SNMP OID の値

問題の説明（実際の Cisco TAC ケースからのサンプル）：

- 「シスコの Firepower 機器を監視したい。コア CPU、メモリ、ディスクごとに SNMP OID を提供してください。」
- 「ASA 5555 デバイスの電源ステータスを監視するために使用できる OID はありますか。

」

- 「FPR 2K および FPR 4K でシャーシの SNMP OID を取得したい。」
- 「ASA ARP キャッシュをポーリングしたい。」
- 「BGP ピアダウンの SNMP OID を知る必要があります。」

SNMP OID 値を見つける方法

以下のドキュメントでは、Firepower デバイスの SNMP OID に関する情報を提供します。

- 「Cisco Firepower Threat Defense (FTD) SNMP Monitoring White Paper」：

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

- 「Cisco Firepower 4100/9300 FXOS MIB Reference Guide」：

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

- 「How to Search for a Specific OID on FXOS Platforms」：

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

- CLI からの SNMP OID を確認します（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
```

- OID の詳細については、SNMP オブジェクトナビゲータを確認してください。

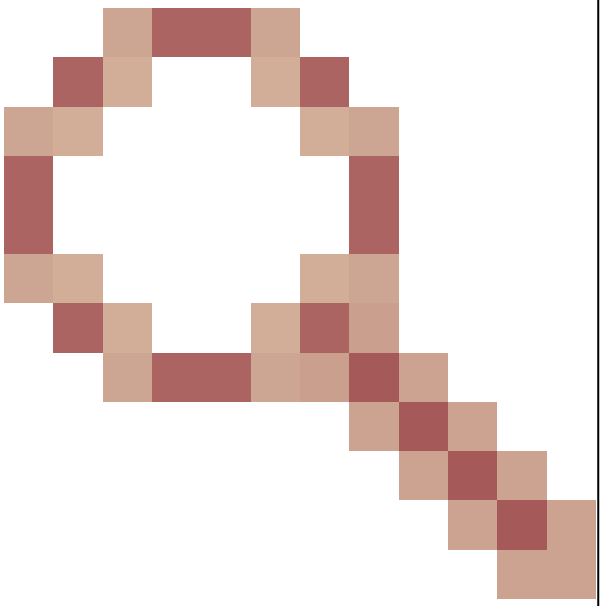
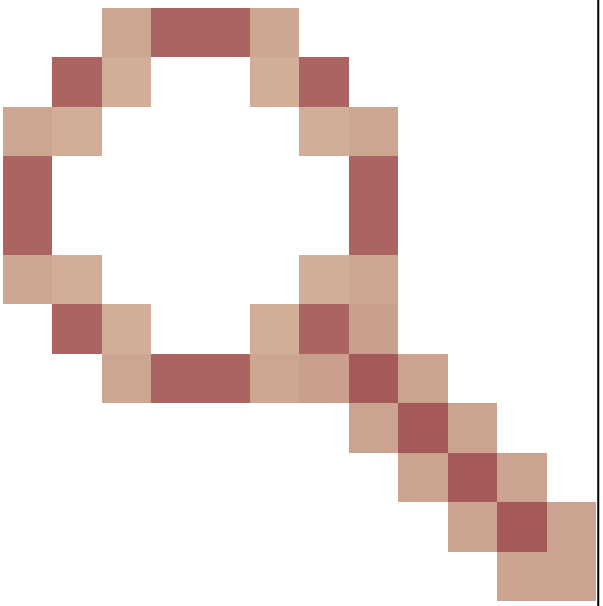
https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

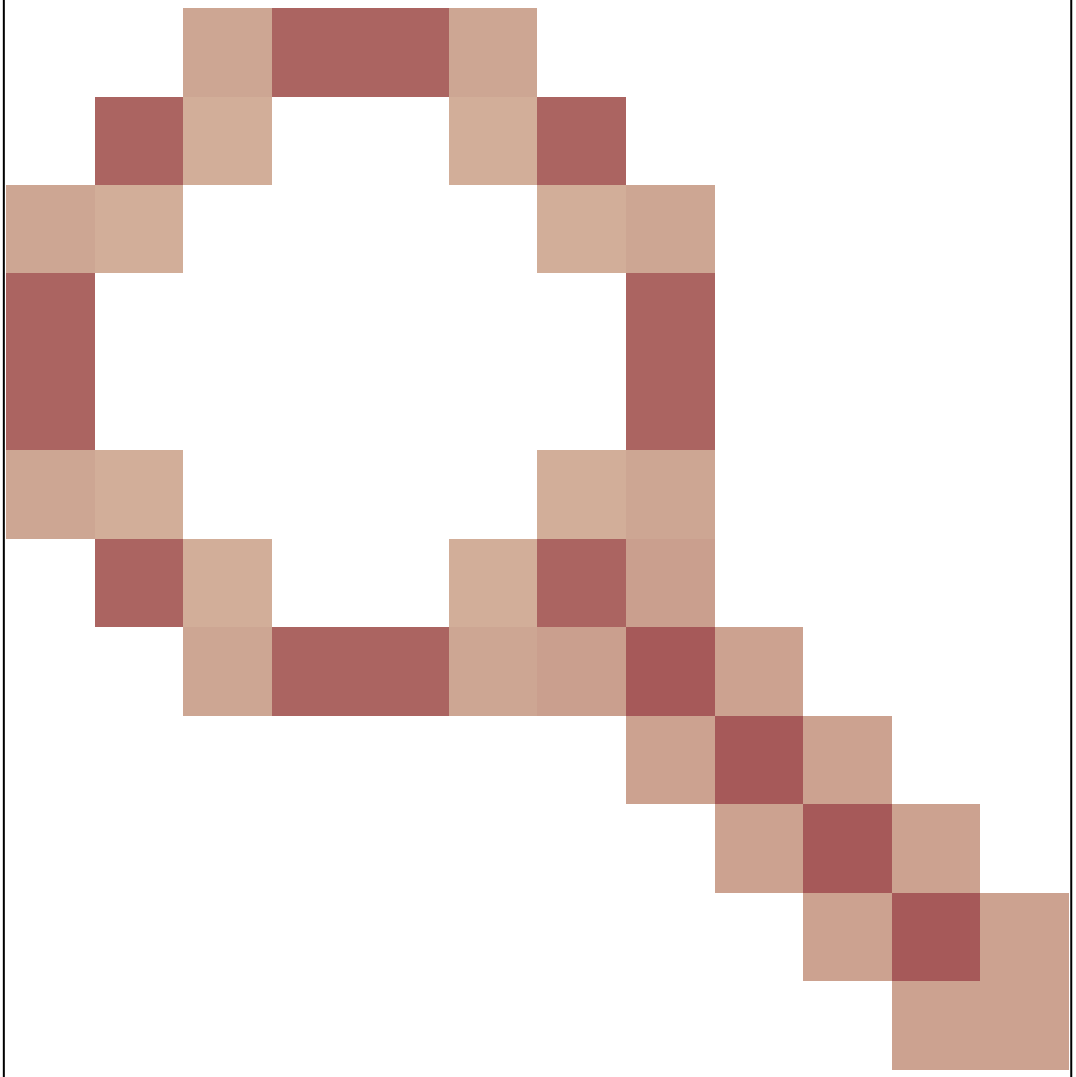
- FXOS（41xx/9300）では、FXOS CLI から次の 2 つのコマンドを実行します。

```
<#root>

FP4145-1#

connect fxos


FP4145-1(fxos)#

show snmp internal oids supported create


FP4145-1(fxos)#

show snmp internal oids supported


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

一般的な OID クイックリファレンス

Requirement	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)
メモリ（LINA）	1.3.6.1.4.1.9.9.221.1.1
メモリ （Linux/FMC）	1.3.6.1.1.4.1.2021.4
HA 情報	1.3.6.1.4.1.9.9.491.1.4.2
クラスタ情報	1.3.6.1.4.1.9.9.491.1.8.1
VPN 情報	RA-VPNセッション数：1.3.6.1 .4.1.9.9.392.1.3.1(7.x) RA-VPNユーザ数：1.3.6.1 .4.1.9.9.392.1.3.3(7.x) RA-VPNピークセッション数：1.3.6.1.4.1.9.9.392.1.3.41(7.x)

	S2S VPNセッション数：1.3.6.1.4.1.9.9.392.1.3.29 S2S VPNピークセッション数：1.3.6.1.4.1.9.9.392.1.3.31 – ヒント：firepower# show snmp-server oid | アイク
BGP ステータス	 ENH Cisco Bug ID CSCux13512 :SNMP ポーリング用の BGP MIB を追加
FPR1K/2K ASA/ASAv スマートライセンス	 ENH Cisco Bug ID CSCvv83590 :FPR1k/2kでのASAv/ASA：スマートライセンスのステータスを追跡するにはSNMP OIDが必要
FXOS レベルのポートチャネルの LINA SNMP OID	ENH Cisco Bug ID CSCvu91544

	 :FXOS レベルのポートチャネル インターフェイス統計のために LINA SNMP OID のサポート

FMC 7.3の追加（FMC 1600/2600/4600以降）

Requirement	OID
ファンステータストラップ	トラップOID:1.3.6.1.4.1.9.9.117.2.0.6 値OID: 1.3.6.1 .4.1.9.9.117.1.4.1.1.1.<index> 0 – ファンが動作していない 1 – ファンが動作している
CPU/PSU温度トラップ	トラップOID:1.3.6.1.4.1.9.9.91.2.0.1 しきい値OID: 1.3.6.1 .4.1.9.9.91.1.2.1.1.4.<index>.1 値OID: 1.3.6.1 .4.1.9.9.91.1.1.1.1.4.<index>

PSUステータストラップ	トラップOID:1.3.6.1.4.1.9.9.117.2.0.2 OperStatus OID: 1.3.6.1 .4.1.9.9.117.1.1.2.1.2.<index> AdminStatus OID: 1.3.6.1 .4.1.9.9.117.1.1.2.1.1.<index> 0 – 電源装置の存在が検出されない 1 – 電源装置の存在が検出されました、ok

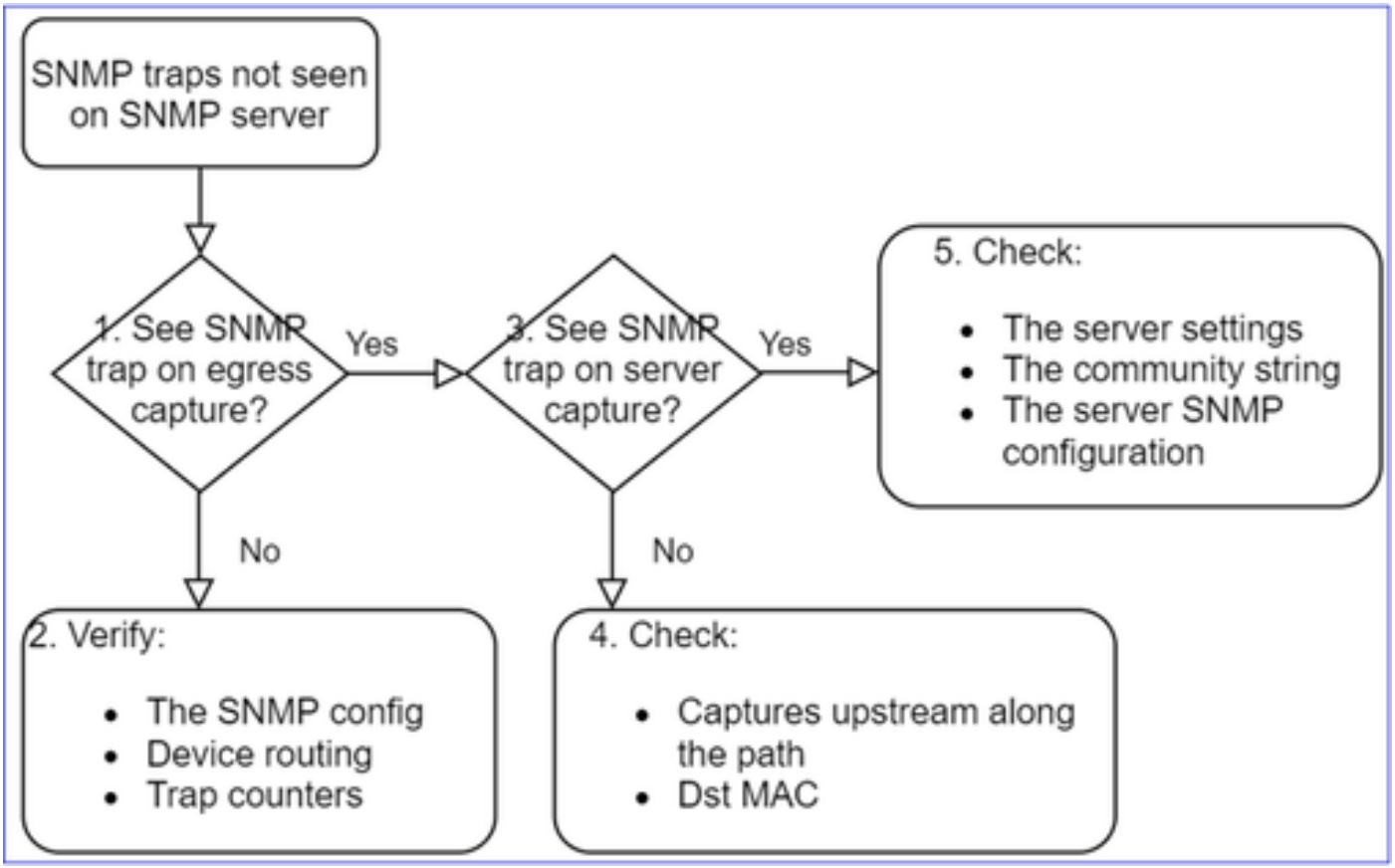
SNMP トラップを取得できない

問題の説明（実際の Cisco TAC ケースからのサンプル）：

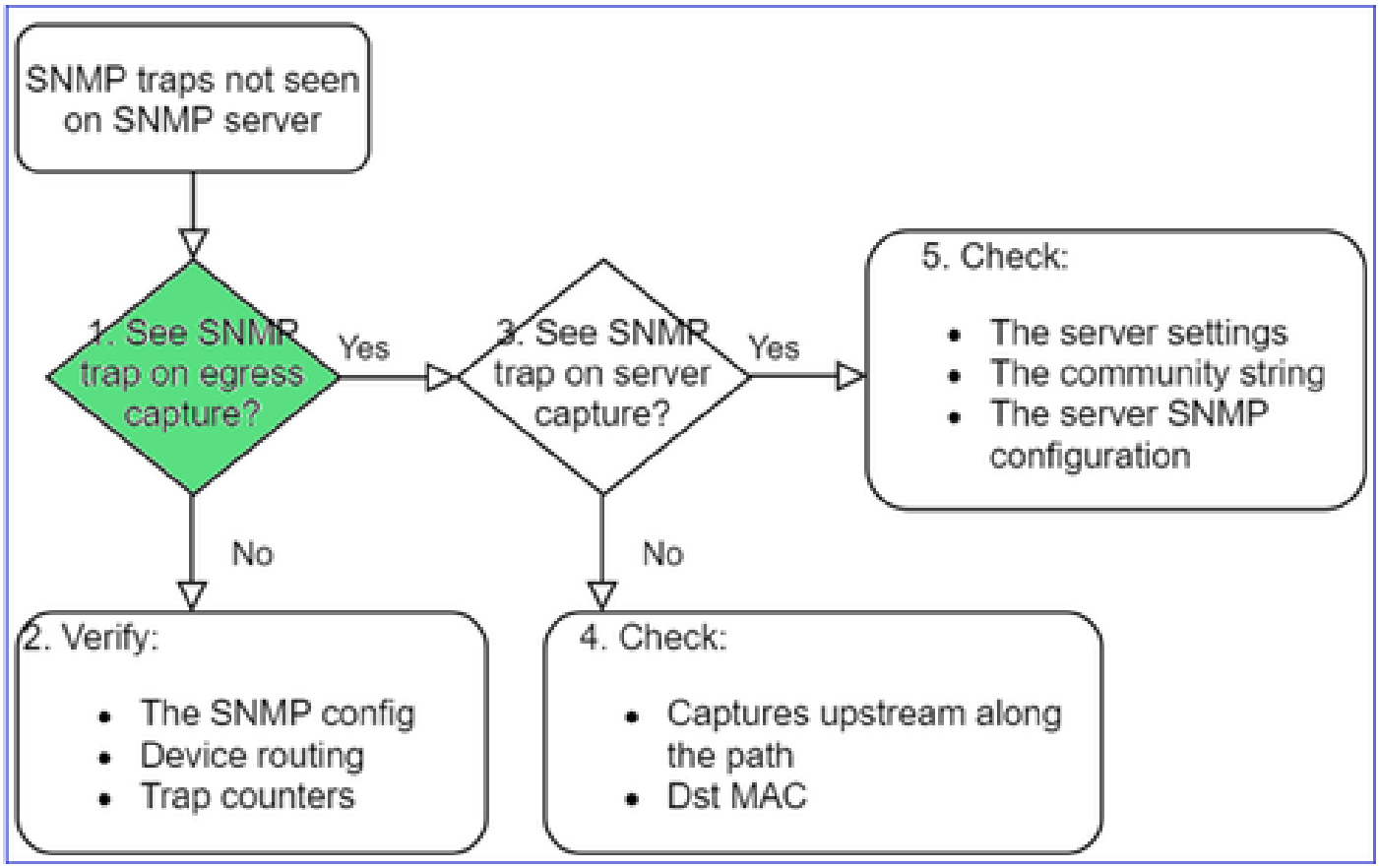
- 「FTD の SNMPv3 が SNMP サーバーにトラップを送信しません。」
- 「FMC と FTD が SNMP トラップメッセージを送信しません。」
- 「FXOS 用に FTD 4100 で SNMP を構成し、SNMPv3 と SNMPv2 を試しましたが、どちらもトラップを送信できません。」
- 「Firepower SNMP が監視ツールにトラップを送信しません。」
- 「ファイアウォール FTD が SNMP トラップを NMS に送信しません。」
- 「SNMP サーバートラップが機能しません。」
- 「FXOS 用に FTD 4100 で SNMP を構成し、SNMPv3 と SNMPv2 を試しましたが、どちらもトラップを送信できません。」

推奨されるトラブルシューティング

次に、FirepowerSNMPトラップの問題に関するフローチャートをトラブルシューティングするプロセスを示します。



1. 出力キャプチャで SNMP トラップが表示されるか。



管理インターフェイスで LINA/ASA トラップをキャプチャするには：

<#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

データインターフェイスで LINA /ASA トラップをキャプチャするには：

<#root>

firepower#

capture SNMP interface net208 match udp any any eq 162

FXOS トラップをキャプチャするには（41xx/9300）：

<#root>

firepower#

connect fxos

firepower(fxos)#

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

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

exit

firepower#

connect local-mgmt

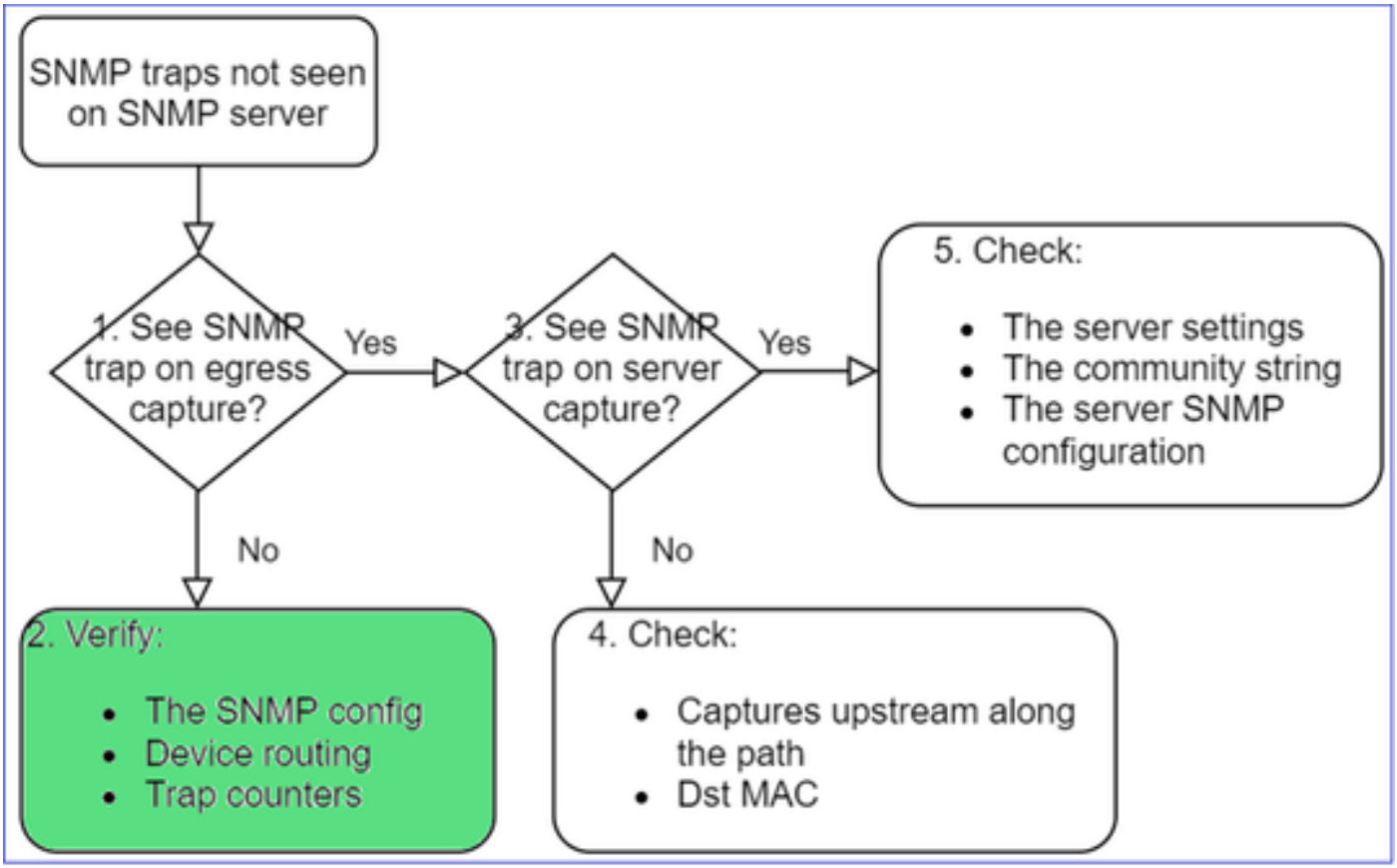
firepower(local-mgmt)#

dir

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

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

2. 出力インターフェイスでパケットが表示されない場合



<#root>

firepower#

show run all snmp-server

```
snmp-server host ngfw-management 10.62.184.23 version 3 Cisco123 udp-port 162
snmp-server host net208 192.168.208.100 community ***** version 2c udp-port 162
snmp-server enable traps failover-state
```

FXOS SNMP トラップ構成：

<#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
```

注：1xxx/21xxでは、これらの設定はDevices > Device Management > SNMP config！の場合にのみ表示されます。

- 管理インターフェイスを介したトラップの LINA/ASA ルーティング：

```
<#root>

>

show network
```

- データインターフェイスを介したトラップの LINA/ASA ルーティング：

```
<#root>

firepower#

show route
```

- FXOS ルーティング（41xx/9300）：

```
<#root>

FP4145-1#

show fabric-interconnect
```

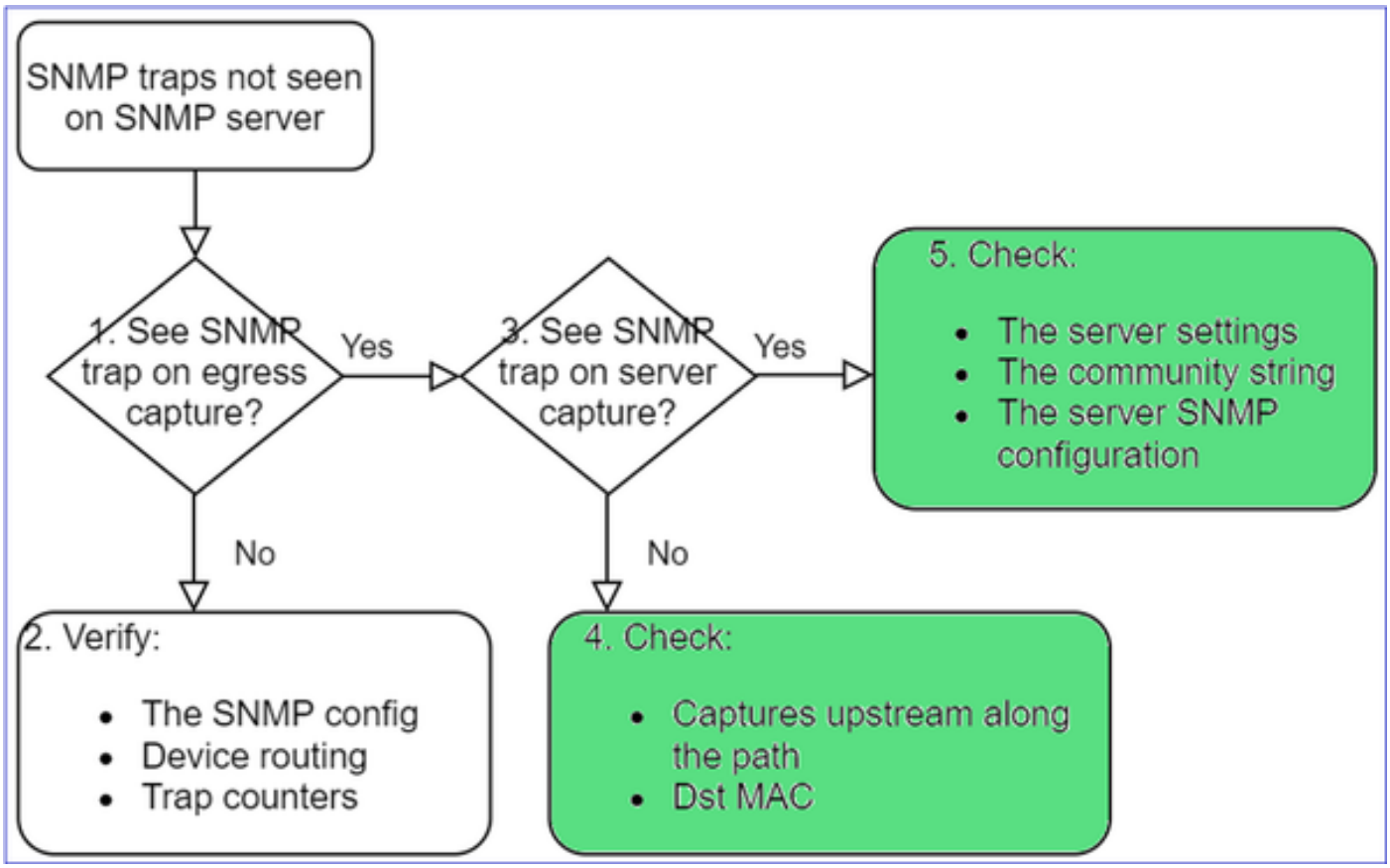
- トラップカウンタ（LINA/ASA）：

```
<#root>

firepower#

show snmp-server statistics | i Trap

    20 Trap PDUs
```

FXOS の場合：

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

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

        1296 Out Traps PDU
```

その他の確認事項



- 宛先SNMPサーバでキャプチャを取得します。

チェックするべきその他の項目：

- パスに沿ったキャプチャ.
- SNMP トラップパケットの宛先 MAC アドレス.
- SNMPサーバの設定とステータス（ファイアウォール、オープンポートなど）。
- SNMP コミュニティストリング.
- SNMP サーバー構成.

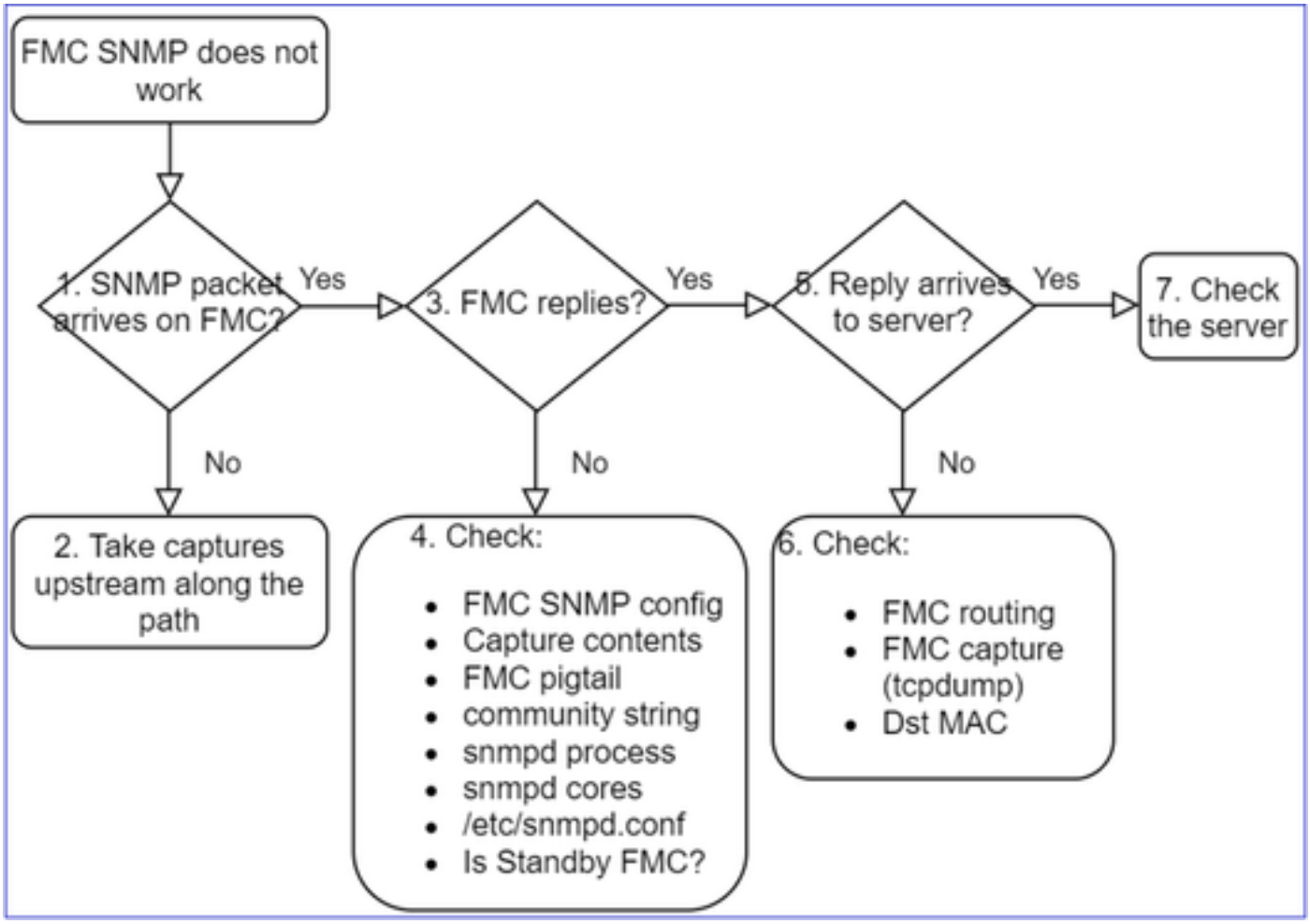
SNMP 経由で FMC を監視できない

問題の説明（実際の Cisco TAC ケースからのサンプル）：

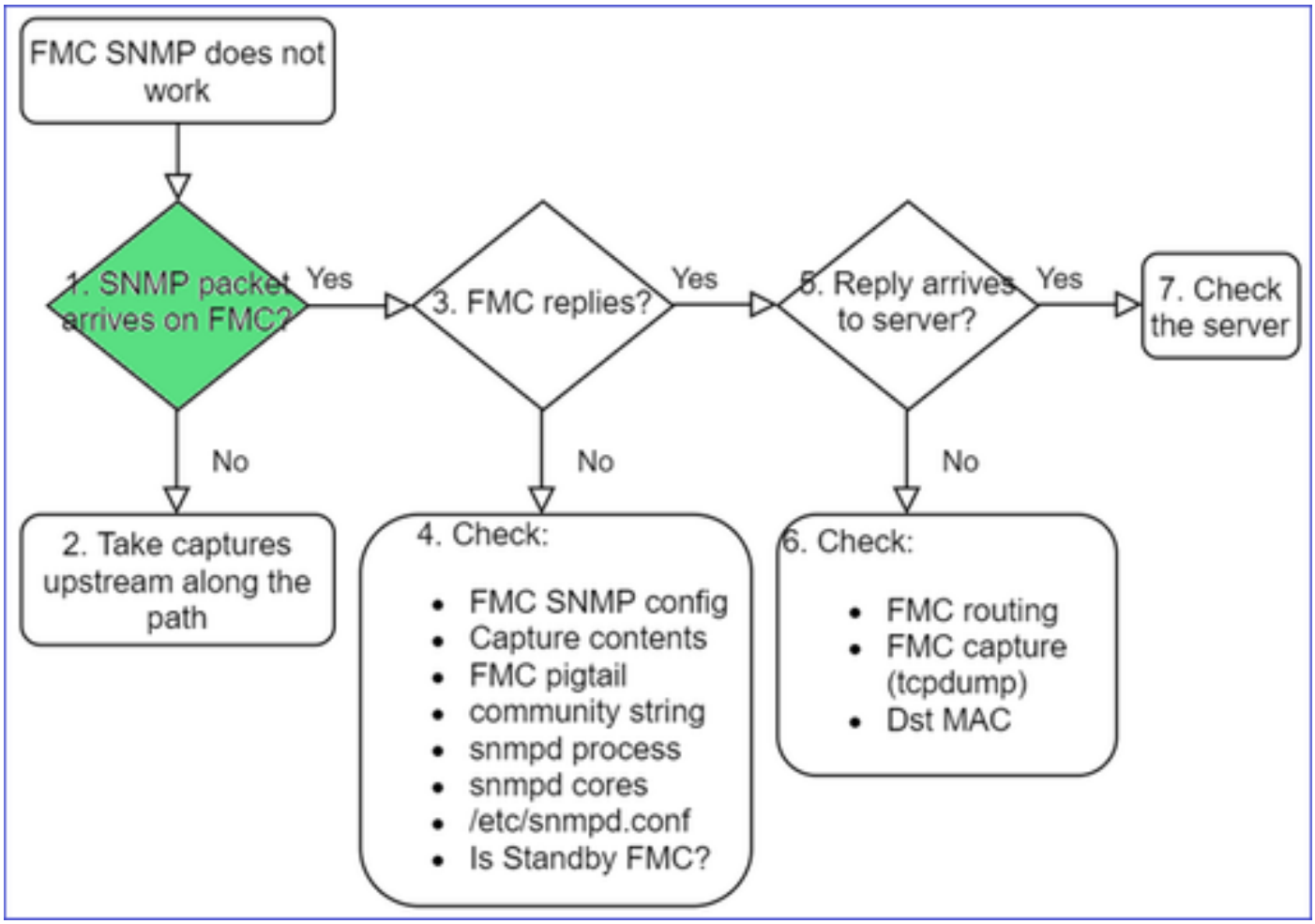
- 「SNMP がスタンバイ FMC で機能しません。」
- 「FMC メモリを監視する必要があります。」
- 「SNMP はスタンバイ 192.168.4.0.8 FMC で機能する必要がありますか。」
- 「CPUやメモリなどのリソースをモニタするようにFMCを設定する必要があります」

トラブルシューティング方法

これは、FMC SNMPの問題のフローチャートをトラブルシューティングするプロセスです。



1. SNMP パケットが FMC に到着するか。



- FMC 管理インターフェイスでのキャプチャ：

<#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
```

ヒント：キャプチャをFMCの/var/common/ディレクトリに保存し、FMC UIからダウンロードします

<#root>

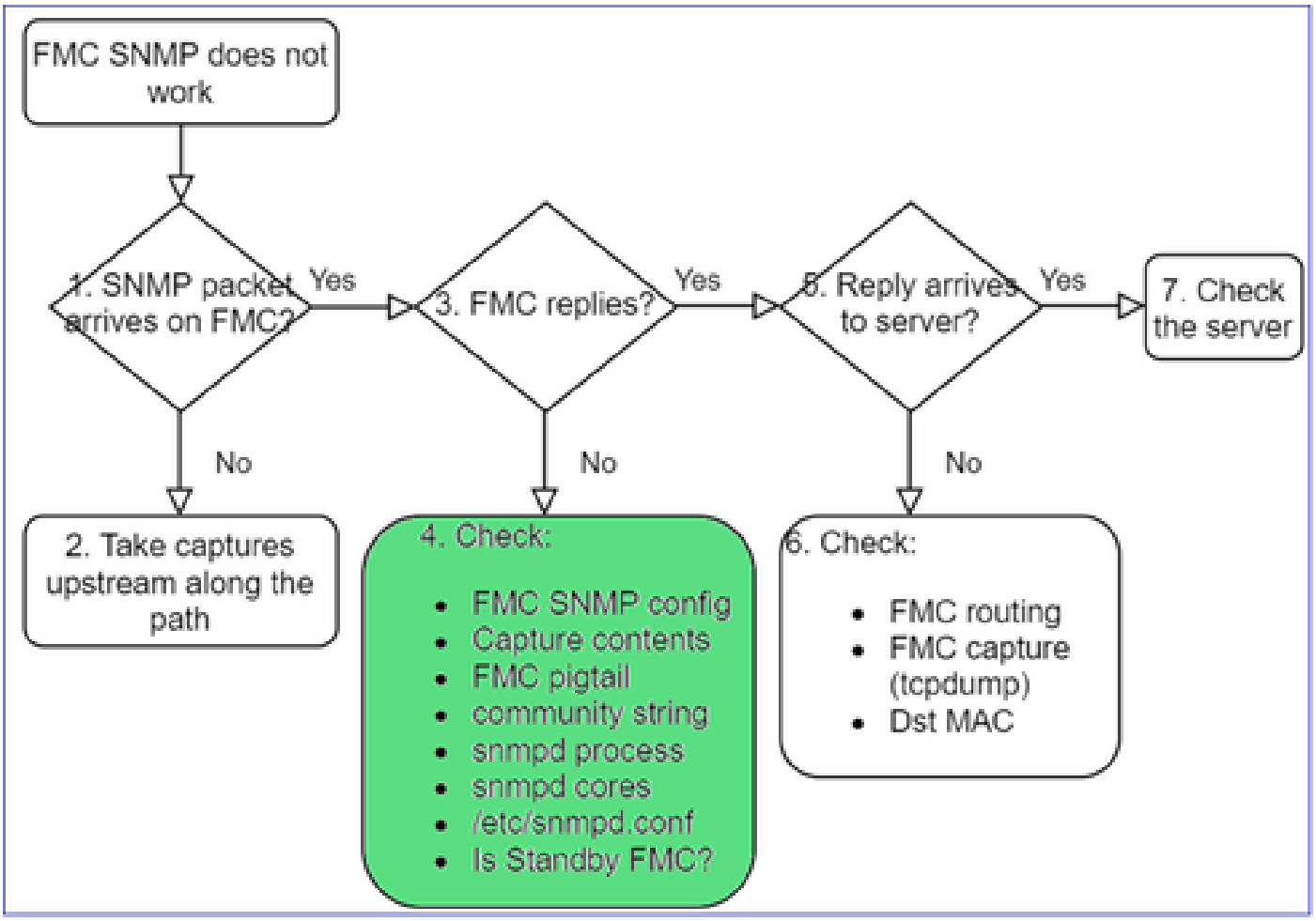
```
admin@FS2600-2:~$
```

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

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

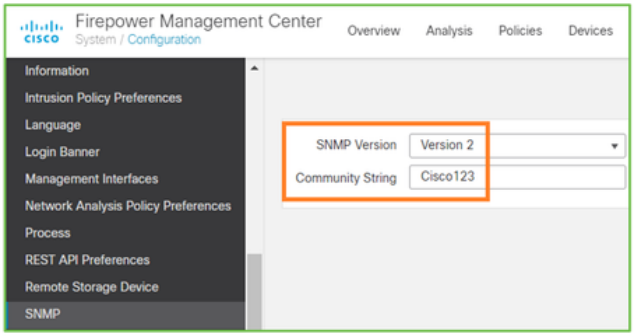
```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C46 packets captured
46 packets received by filter
```

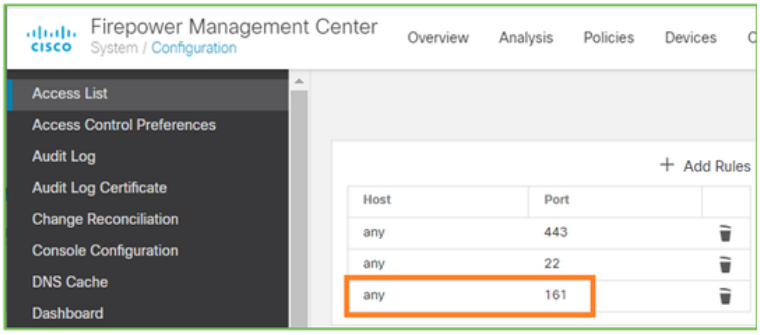
FMC は応答するか。



FMC が応答しない場合は、次の点を確認します。

- FMC SNMP 構成（ [System] > [Configuration] ）
  1. [SNMP] セクション
  2. [Access List] セクション





FMC が応答しない場合は、次の点を確認します。

- キャプチャ（pcap）の内容
- コミュニティストリング（これはキャプチャで確認できます）
- FMC pigtail 出力（エラー、失敗、トレースを探す）と /var/log/snmpd.log の内容
- snmpd プロセス

<#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 コア

<#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
```

- /etc/snmpd.conf のバックエンド構成ファイル：

<#root>

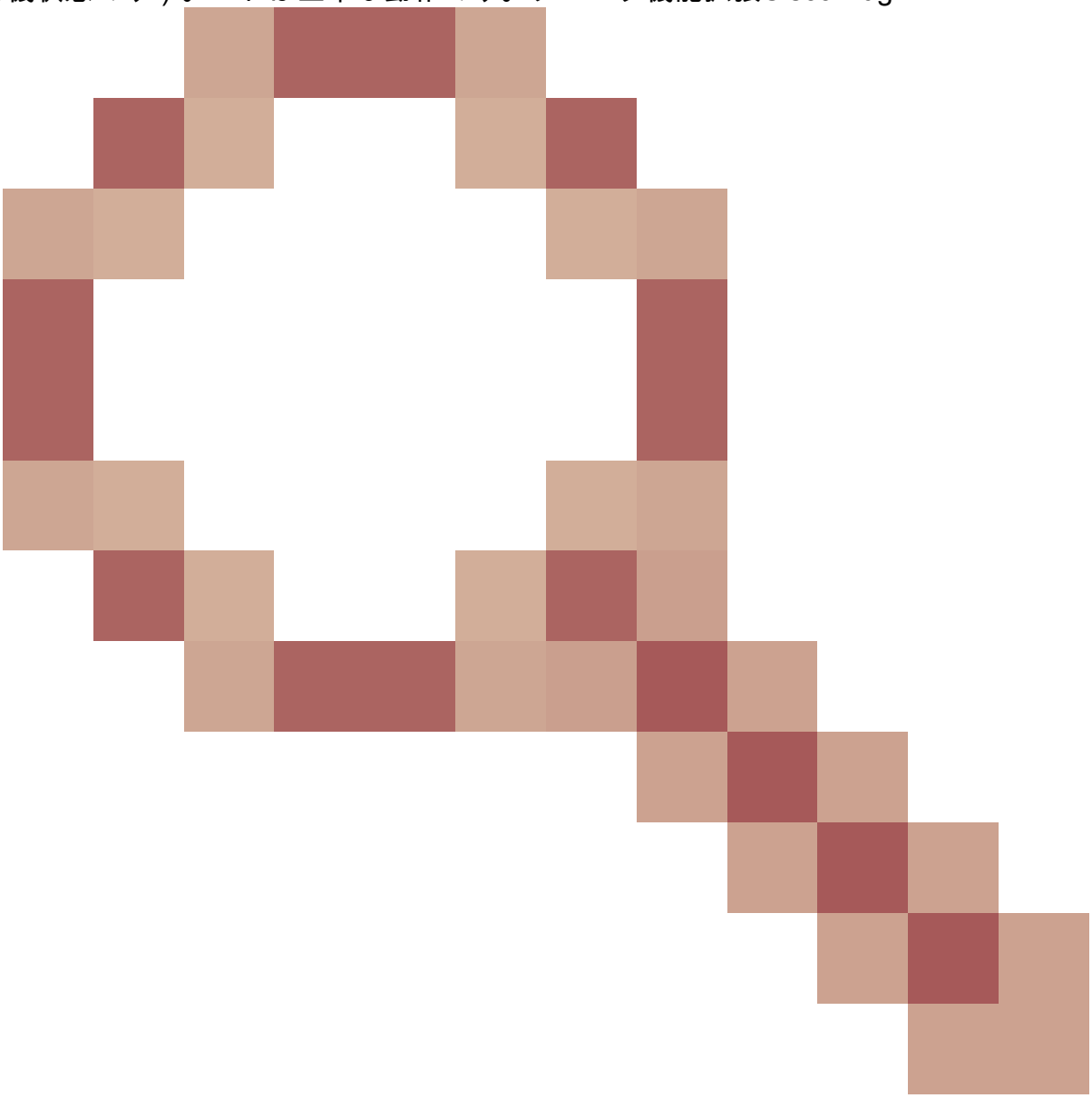
```
admin@FS2600-2:~$

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
```

注:SNMPが無効になっている場合、snmpd.confファイルは存在しません

- スタンバイ FMC か

6.4.0-9 より前および 6.6.0 より前では、スタンバイ FMC は SNMP データを送信しません

（snmpd は待機状態です）。これは正常な動作です。チェック機能拡張Cisco Bug ID



CSCvs32303

SNMP を構成できない

問題の説明（実際の Cisco TAC ケースからのサンプル）：

- 「Cisco Firepower Management Center および Firepower 4115 Threat Defense 用に SNMP を設定したいと考えています。」
- 「FTDでのSNMP設定のサポート」
- 「FTD アプライアンスで SNMP モニタリングを有効にしたいと考えています。」
- 「FXOS で SNMP サービスを設定しようとしましたが、システムが最終的に commit-buffer を許可しません。「Error: Changes not allowed. use 'Connect ftd' to make changes.」というメッセージが表示されます。
- 「FTD アプライアンスで SNMP モニタリングを有効にしたいと考えています。」
- 「FTD で SNMP を構成できず、モニタリングでデバイスを検出できません。」

SNMP 構成の問題にアプローチする方法

最初のポイント：ドキュメント

- 現在のドキュメントを読みます。
- FMC の構成ガイド：

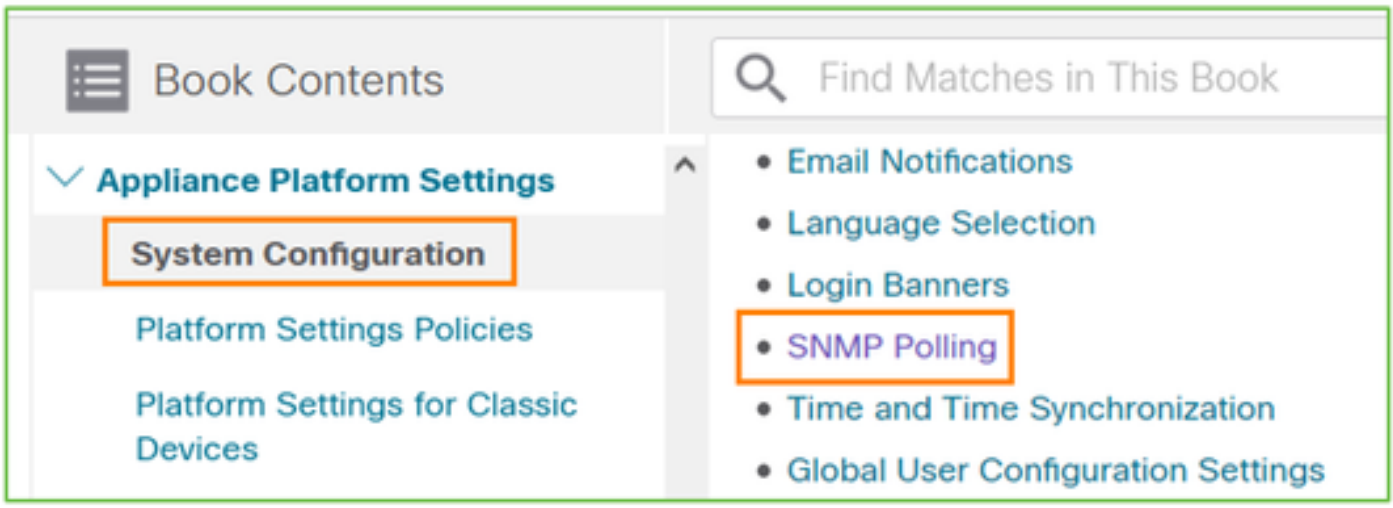
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html

- FXOS の構成ガイド：

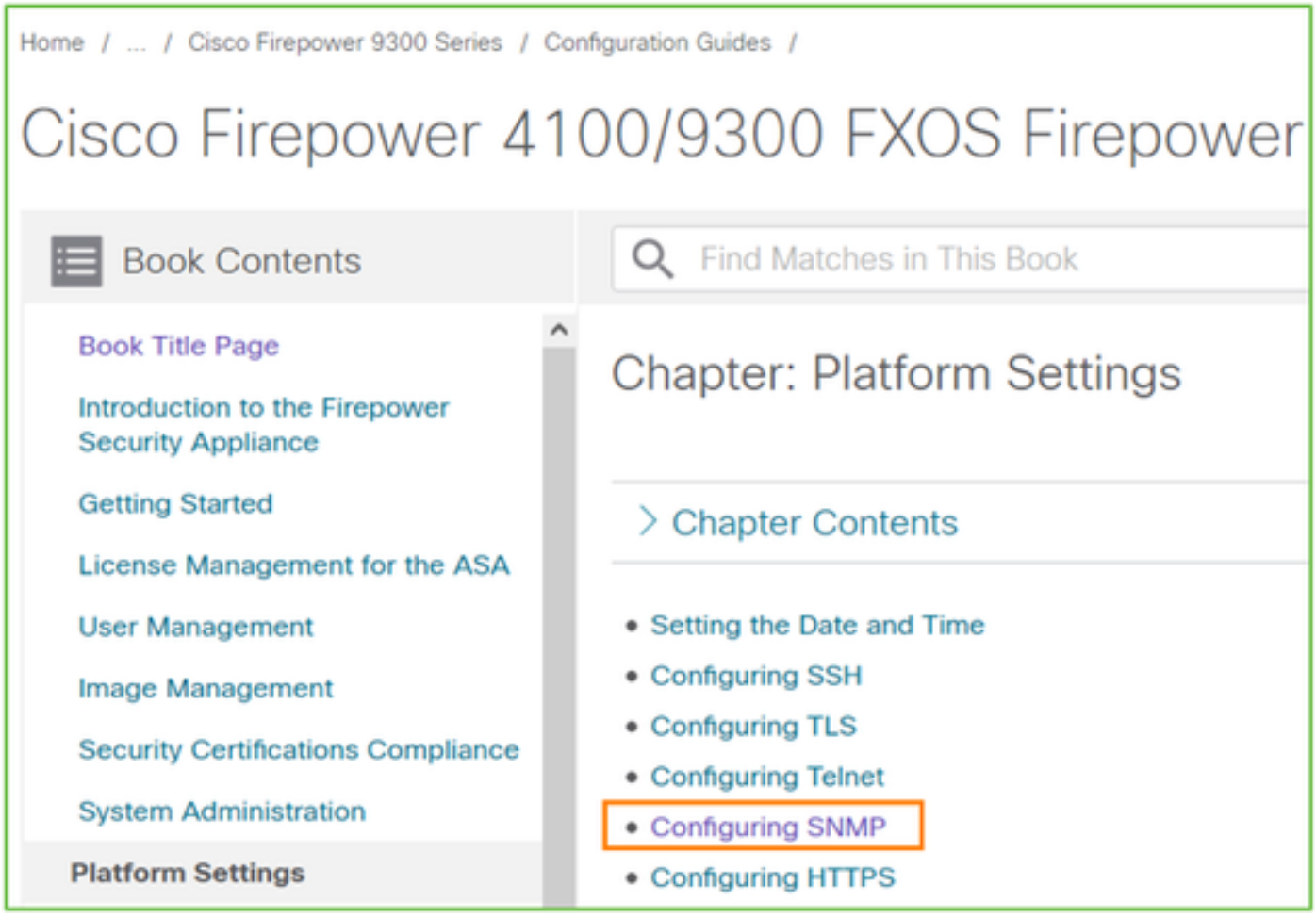
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos2101/web-guide/b_GUI_FXOS_ConfigGuide_2101/platform_settings.html#topic_6C6725BBF4BC4333BA207BE9DB

さまざまな SNMP ドキュメントに注意してください。

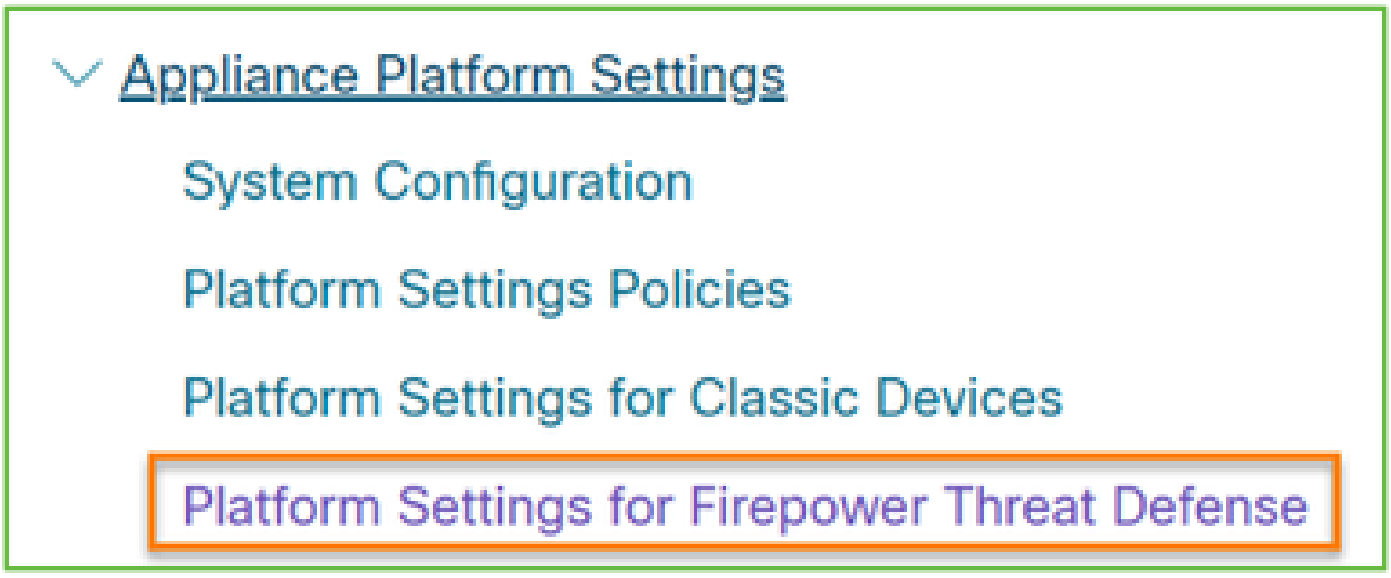
FMC SNMP：



FXOS SNMP：



Firepower 41xx/9300 SNMP 構成：



Firepower 1xxx/21xx SNMP 構成：

Firepower Device Manager（FDM）上の SNMP 構成

問題の説明（実際の Cisco TAC ケースからのサンプル）：

- 「FDM を使用した Firepower デバイスの SNMPv3 に関するガイダンスが必要です。」
- 「SNMP 構成は、FDM から FPR 2100 デバイスでは機能しません。」
- 「FDM で機能する SNMP v3 構成を取得できません。」
- 「FDM 6.7 SNMP 構成の支援。」
- 「Firepower FDM で SNMP v3 を有効にしてください。」

SNMP FDM 構成の問題にアプローチする方法

- 6.7 より前のバージョンでは、FlexConfig を使用して SNMP 構成を行うことができます。

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

- Firepower バージョン 6.7 以降、SNMP 構成は FlexConfig ではなく、REST API を使用して行われます。

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

SNMP トラブルシューティングのチートシート

1xxx/21xx/41xx/9300（LINA/ASA）- Cisco TAC でケースを開く前に収集するもの

コマンド	説明
firepower# show run snmp-server	ASA/FTD LINA SNMP設定を確認します。
firepower# show snmp-server statistics	ASA/FTD LINA の SNMP 統計を確認します。

	SNMP パケット入力と SNMP パケット出力のカウンタに注目してください。
> capture-traffic	管理インターフェイスでトラフィックをキャプチャします。
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	UDP 161（SNMPポーリング）のデータインターフェイス(nameif 'net201')上のトラフィックをキャプチャします。
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	UDP 162（SNMPトラップ）のデータインターフェイス(nameif 'net208')でトラフィックをキャプチャします。
firepower# show capture SNMP-POLL packet-number 1 trace	ASA/FTD LINAデータインターフェイスに到達する入力SNMPパケットをトレースします。
admin@firepower:~$ sudo tcpdump -i tap_nlp	NLP(Non-Lina Process)内部タップインターフェイスでキャプチャします。
firepower# show conn all protocol udp port 161	UDP 161ですべてのASA/FTD LINA接続をチェックします（SNMPポーリング）。
firepower# show log | i 302015.*161	ASA/FTD LINAログ302015でSNMPポーリングを確認します。
firepower# more system:running-config | iコミュニティ	SNMPコミュニティストリングを確認します。
firepower# debug menu netsnmp 4	SNMPの設定とプロセスIDを確認します。
firepower# show asp table classify interface net201 domain permit match port=161	「net201」という名前のインターフェイスのSNMP ACLのヒットカウントをチェックします。
firepower# show disk0: | iコア	SNMP コアがあるかどうかを確認します。
admin@firepower:~$ ls -l /var/data/cores	SNMP コアがあるかどうかを確認します。FTDにのみ適用されます。

firepower# show route	ASA/FTD LINAルーティングテーブルを確認します。
> show network	FTD mgmtプレーンのルーティングテーブルを確認します。
admin@firepower:~$ tail -f /mnt/disk0/log/ma_ctx2000.log	FTDでSNMPv3の確認とトラブルシューティングを行います。
firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	新しいリリースの隠しコマンドです。内部デバッグ。Cisco TACでSNMPをトラブルシューティングする際に役立ちます。

41xx/9300（FXOS）- Cisco TAC でケースを開く前に収集するもの

コマンド	説明
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	SNMP ポーリング（UDP 161）の FXOS キャプチャ。 リモート FTP サーバーにアップロードします。 FTP IP:192.0.2.100 FTPユーザ名：ftp
firepower# connect fxos firepower(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 162" limit-captured-frames 50 write workspace:///SNMP-TRAP.pcap	SNMP トラップ（UDP 162）の FXOS キャプチャ。

firepower# scope system firepower /system # scope services firepower /system/services # show ip-block detail	FXOS ACL を確認します。
firepower# show fault	FXOS 障害を確認します。
firepower# show fabric-interconnect	FXOS インターフェイス構成とデフォルトゲートウェイ設定を確認します。
firepower# connect fxos firepower(fxos)# show running-config snmp all	FXOS SNMP 構成を確認します。
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	FXOS SNMP OID を確認します。
firepower# connect fxos firepower(fxos)# show snmp	FXOS SNMP 設定とカウンタを確認します。
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	FXOS SNMP をデバッグします（「パケット」または「すべて」）。 停止するには、「terminal no monitor」と「undebug all」を使用します。

1xxx/21xx（FXOS）- Cisco TAC でケースを開く前に収集するもの

コマンド	説明
> capture-traffic	管理インターフェイスでトラフィックをキャプチャします。
> show network	FTD 管理プレーンのルーティングテーブルを確認します。

firepower# scope monitoring firepower /monitoring # show snmp [host] firepower /monitoring # show snmp-user [detail] firepower /monitoring # show snmp-trap	FXOS SNMP 構成を確認します。
firepower# show fault	FXOS 障害を確認します。
firepower# connect local-mgmt firepower(local-mgmt)# dir cores_fxos firepower(local-mgmt)# dir cores	FXOS コアファイル（トレースバック）を確認します。

FMC - Cisco TAC でケースを開く前に収集するもの

コマンド	説明
admin@FS2600-2:~$ sudo tcpdump -i eth0 udp port 161 -n	SNMP ポーリングについて管理インターフェイスでトラフィックをキャプチャします。
admin@FS2600-2: ~ $ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	SNMP ポーリングについて管理インターフェイスでトラフィックをキャプチャし、ファイルに保存します。
admin@FS2600-2:~$ sudo pmtool status | grep snmpd	SNMP プロセスの状態をチェックします。
admin@FS2600-2:~$ ls -al /var/common | grep snmpd	SNMP コアファイル（トレースバック）を確認します。
admin@FS2600-2:~$ sudo cat /etc/snmpd.conf	SNMP 構成ファイルの内容を確認します。

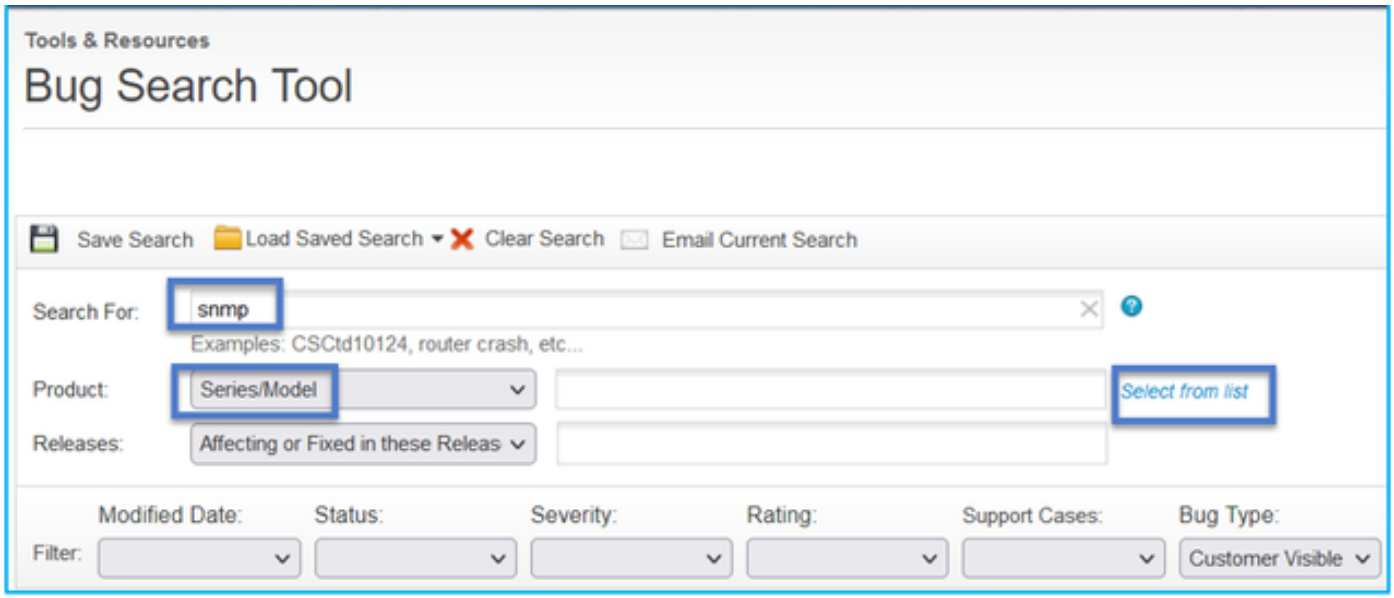
snmpwalk の例

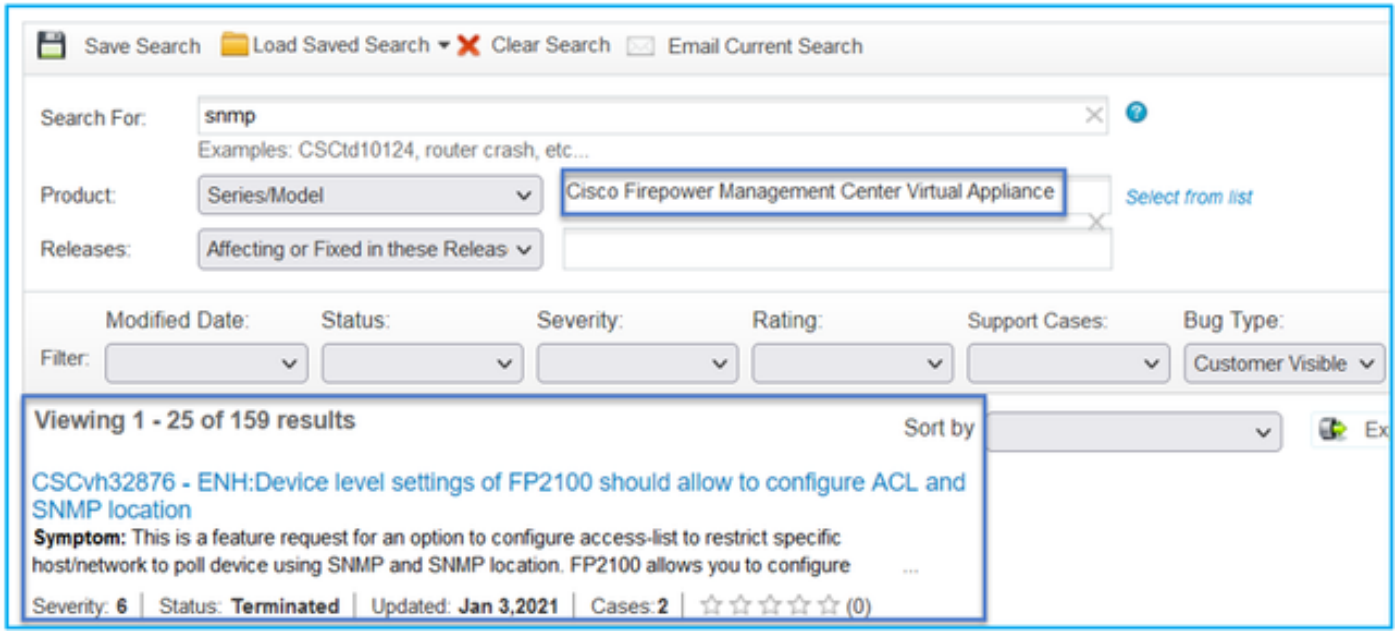
これらのコマンドは、検証とトラブルシューティングに使用できます。

コマンド	説明
# snmpwalk -c Cisco123 -v2c 192.0.2.1	SNMP v2c を使用して、リモートホストからすべての OID を取得します。 Cisco123 = コミュニティストリング 192.0.2.1 = 宛先ホスト
# snmpwalk -v2c -c Cisco123 -OS 192.0.2.1 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 =ゲージ32: 0	SNMP v2c を使用して、リモートホストから特定の OID を取得します。
# snmpwalk -c Cisco123 -v2c 192.0.2.1 .10.3.1.4.1.9.9.109.1.1.1.1 -On .10.3.1.1.4.1.9.9.109.1.1.1.1.6.1 =ゲージ32: 0	取得した OID を数値形式で表示します。
# snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 -x AES -X Cisco123 192.0.2.1	SNMP v3 を使用して、リモートホストからすべての OID を取得します。 SNMPv3 ユーザー = cisco SNMPv3 認証 = SHA SNMPv3 承認 = AES
# snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 -x AES -X Cisco123 192.0.2.1	SNMP v3（MD5 および AES128）を使用して、リモートホストからすべての OID を取得します。
# snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1	認証のみの SNMPv3。

SNMP の不具合を検索する方法

1. https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV に移動します。
2. キーワードsnmpを入力し、Select from listを選択します。





最も一般的な製品：

- Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Cisco Firepower 9300 シリーズ
- Cisco Firepower Management Center 仮想アプライアンス
- Cisco Firepower NGFW

関連情報

- SNMP の脅威に対する防御の設定
- FXOS(UI)でのSNMPの設定
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。