

# firepower NGFW 어플라이언스에 SNMP 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[FPR4100/FPR9300의 새시\(FXOS\) SNMP](#)

[GUI를 통해 FXOS SNMPv1/v2c 구성](#)

[CLI\(명령줄 인터페이스\)를 통해 FXOS SNMPv1/v2c 구성](#)

[GUI를 통해 FXOS SNMPv3 구성](#)

[CLI를 통해 FXOS SNMPv3 구성](#)

[FPR4100/FPR9300의 FTD\(LINA\) SNMP](#)

[LINA SNMPv2c 구성](#)

[LINA SNMPv3 구성](#)

[MIO 블레이드 SNMP 통합\(FXOS 2.12.1, FTD 7.2, ASA 9.18.1\)](#)

[FPR2100의 SNMP](#)

[FPR2100의 새시\(FXOS\) SNMP](#)

[FXOS SNMPv1/v2c 구성](#)

[FXOS SNMPv3 구성](#)

[FPR2100의 FTD\(LINA\) SNMP](#)

[다음을 확인합니다.](#)

[FPR4100/FPR9300용 FXOS SNMP 확인](#)

[FXOS SNMPv2c 확인](#)

[FXOS SNMPv3 확인](#)

[FPR2100용 FXOS SNMP 확인](#)

[FXOS SNMPv2 확인](#)

[FXOS SNMPv3 확인](#)

[FTD SNMP 확인](#)

[FPR4100/FPR9300에서 FXOS에 대한 SNMP 트래픽 허용](#)

[GUI를 통해 전역 액세스 목록 구성](#)

[CLI를 통해 전역 액세스 목록 구성](#)

[확인](#)

[OID 개체 탐색기 사용](#)

[문제 해결](#)

[FTD LINA SNMP를 폴링할 수 없음](#)

[FXOS SNMP를 폴링할 수 없음](#)

[어떤 SNMP OID 값을 사용해야 하나요?](#)

[SNMP 트랩을 가져올 수 없음](#)

[SNMP를 통해 FMC를 모니터링할 수 없음](#)

[FDM\(Firepower Device Manager\)의 SNMP 구성](#)

[SNMP 문제 해결 치트 시트](#)

---

## 소개

이 문서에서는 NGFW(Next Generation Firewall) FTD 어플라이언스에서 SNMP(Simple Network Management Protocol)를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에는 SNMP 프로토콜에 대한 기본 지식이 필요합니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

Firepower NGFW 어플라이언스는 2개의 주요 하위 시스템으로 분할할 수 있습니다.

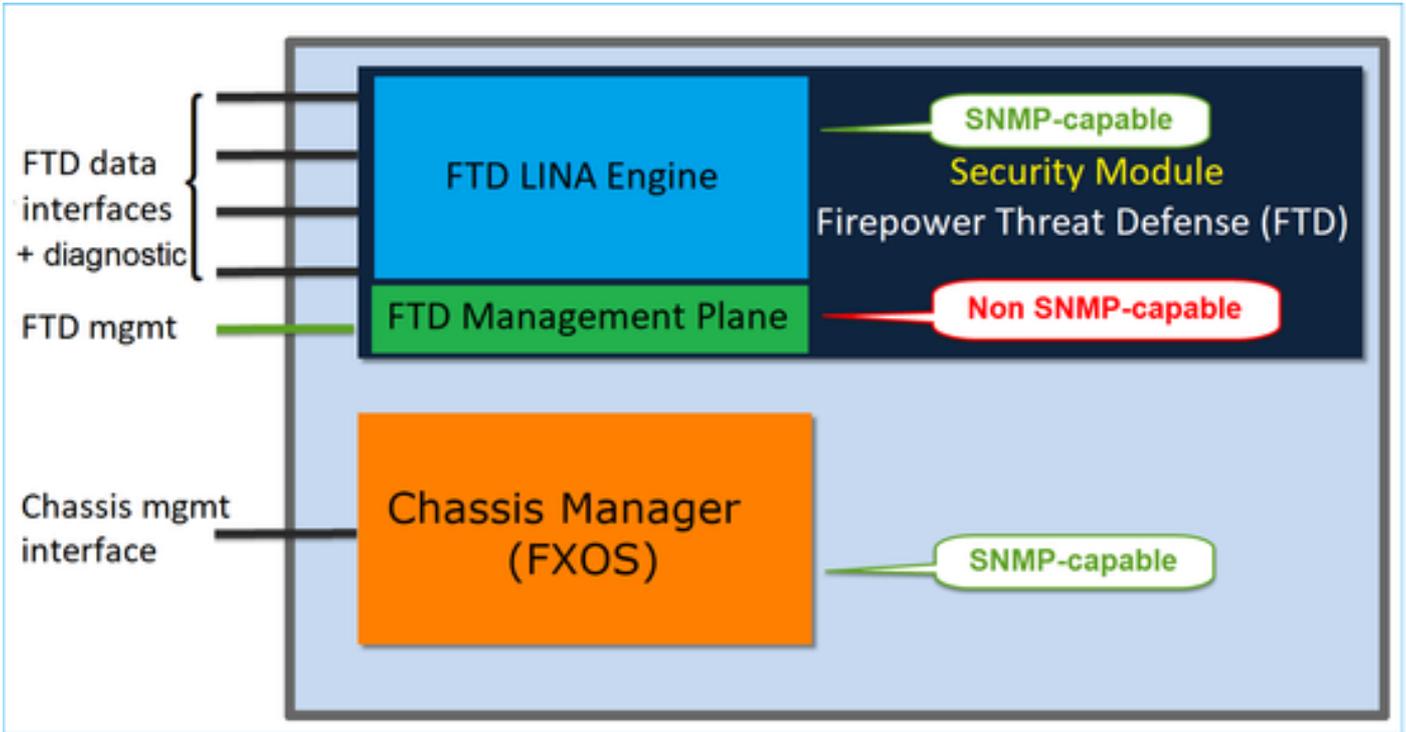
- FX-OS(Firepower Extensible Operative System)는 새시 하드웨어를 제어합니다.
- FTD(Firepower Threat Defense)는 모듈 내에서 실행됩니다.

FTD는 Snort 엔진 및 LINA 엔진의 2가지 주요 엔진으로 구성된 통합 소프트웨어입니다. FTD의 현재 SNMP 엔진은 기존 ASA에서 파생되며 LINA 관련 기능을 볼 수 있습니다.

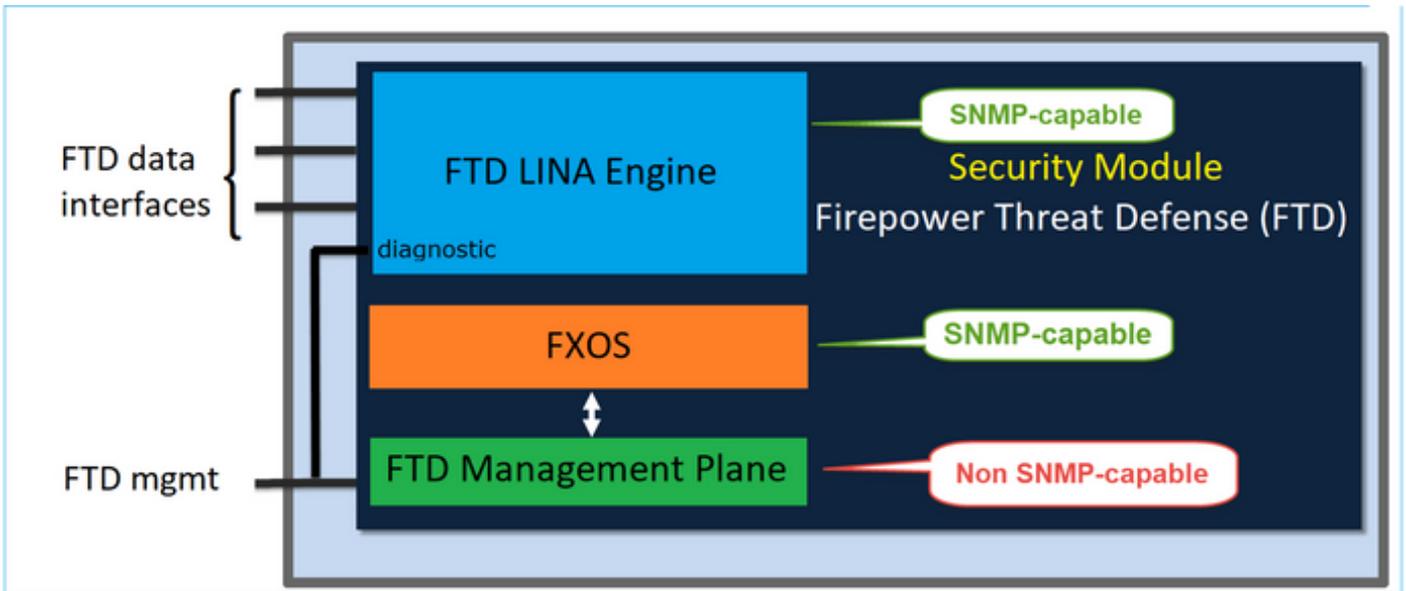
FX-OS와 FTD는 독립적인 컨트롤 플레인을 가지고 있으며, 모니터 목적으로 서로 다른 SNMP 엔진을 가지고 있습니다. 각 SNMP 엔진은 서로 다른 정보를 제공하며, 디바이스 상태를 좀 더 포괄적으로 보기 위해 둘 다 모니터링할 수 있습니다.

하드웨어 관점에서 Firepower NGFW 어플라이언스에는 현재 Firepower 2100 시리즈와 Firepower 4100/9300 시리즈라는 두 가지 주요 아키텍처가 있습니다.

Firepower 4100/9300 디바이스에는 디바이스 관리 전용 인터페이스가 있으며 이는 FXOS 하위 시스템으로 주소 지정된 SNMP 트래픽의 소스 및 대상입니다. 반면 FTD 애플리케이션은 LINA 인터페이스(데이터 및/또는 진단)를 사용합니다. 6.6 이후 FTD 릴리스에서는 SNMP 구성에 FTD 관리 인터페이스를 사용할 수 있습니다.



Firepower 2100 어플라이언스의 SNMP 엔진은 FTD 관리 인터페이스 및 IP를 사용합니다. 어플라이언스 자체는 이 인터페이스에서 수신되는 SNMP 트래픽을 브리지하고 FXOS 소프트웨어에 전달합니다.

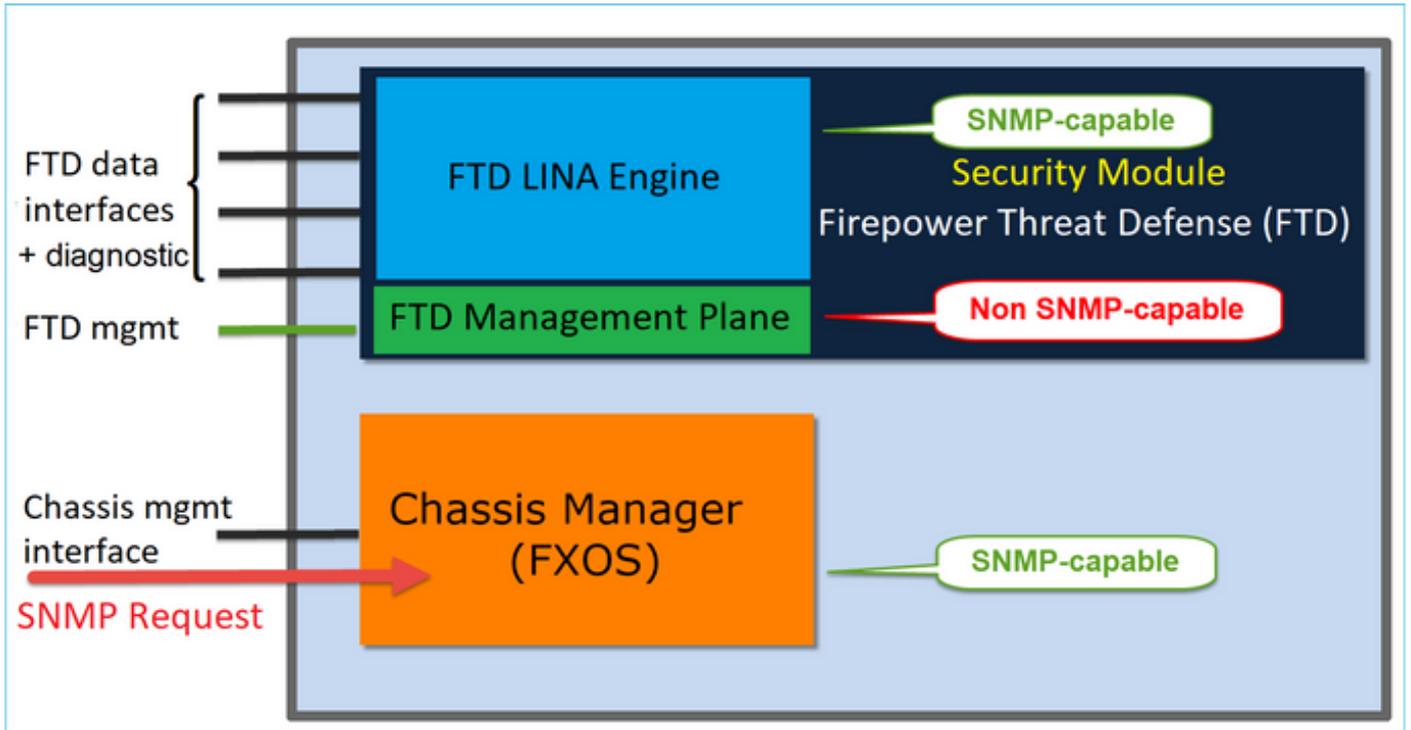


소프트웨어 릴리스 6.6 이후를 사용하는 FTD에는 다음과 같은 변경 사항이 도입되었습니다.

- 관리 인터페이스를 통한 SNMP.
- FPR1000 또는 FPR2100 시리즈 플랫폼에서는 이 단일 관리 인터페이스를 통해 LINA SNMP 및 FXOS SNMP를 모두 통합합니다. 또한 Platform settings(플랫폼 설정) > SNMP의 FMC에서 단일 구성 포인트를 제공합니다.

## 구성

## FPR4100/FPR9300의 새시(FXOS) SNMP



### GUI를 통해 FXOS SNMPv1/v2c 구성

1단계. FCM(Firepower Chassis Manager) UI를 열고 Platform Settings(플랫폼 설정) > SNMP 탭으로 이동합니다. SNMP 활성화 상자를 선택하고 SNMP 요청에 사용할 커뮤니티 문자열을 지정한 다음 Save(저장)를 선택합니다.

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

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

Admin State:  Enable **1**

Port: 161

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

System Administrator Name:

Location:

**SNMP Traps**

**4**

Name	Port	Version	V3 Privilege	Type

**SNMP Users**

Name	Auth Type	AES-128

**3**

 참고: Community/Username(커뮤니티/사용자 이름) 필드가 이미 설정되어 있는 경우 빈 필드의 오른쪽에 있는 텍스트는 Set: Yes(설정: 예)입니다. Community/Username(커뮤니티/사용자 이름) 필드에 값이 아직 입력되지 않은 경우, 빈 필드의 오른쪽에 있는 텍스트는 Set: No(설정: 아니요)입니다

2단계. SNMP 트랩 대상 서버를 구성합니다.

## Add SNMP Trap

Host Name:\*

Community/Username:\*

Port:\*

Version:  V1  V2  V3

Type:  Traps  Informs

V3 Privilege:  Auth  NoAuth  Priv

 참고: 쿼리 및 트랩 호스트에 대한 커뮤니티 값은 독립적이며 다를 수 있습니다

호스트는 IP 주소 또는 이름으로 정의할 수 있습니다. OK(확인)를 선택하면 SNMP 트랩 서버의 구성이 자동으로 저장됩니다. SNMP 기본 페이지에서 저장 버튼을 선택할 필요가 없습니다. 호스트를 삭제할 때도 마찬가지입니다.

CLI(명령줄 인터페이스)를 통해 FXOS SNMPv1/v2c 구성

```

<#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
```

## GUI를 통해 FXOS SNMPv3 구성

1단계. FCM을 열고 Platform Settings(플랫폼 설정) > SNMP 탭으로 이동합니다.

2단계. SNMP v3의 경우 상위 섹션에서 커뮤니티 문자열을 설정할 필요가 없습니다. 생성된 모든 사용자는 FXOS SNMP 엔진에 대한 쿼리를 성공적으로 실행할 수 있습니다. 첫 번째 단계는 플랫폼에서 SNMP를 활성화하는 것입니다. 완료되면 사용자 및 대상 트랩 호스트를 생성할 수 있습니다. SNMP 사용자 및 SNMP 트랩 호스트는 모두 자동으로 저장됩니다.

Admin State:  Enable **1**

Port: 161

Community/Username:  Set: No

System Administrator Name:

Location:

**SNMP Traps**

**4**

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

**SNMP Users**

**3**

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

**2**

3단계. 이미지에 표시된 대로 SNMP 사용자를 추가합니다. 인증 유형은 항상 SHA이지만 암호화에 AES 또는 DES를 사용할 수 있습니다.

### Add SNMP User

Name:\* user1

Auth Type: SHA

Use AES-128:

Password: .....

Confirm Password: .....

Privacy Password: .....

Confirm Privacy Password: .....

OK Cancel

4단계. 이미지에 표시된 대로 SNMP 트랩 호스트를 추가합니다.

## Add SNMP Trap

Host Name:\*

Community/Username:\*

Port:\*

Version:  V1  V2  V3

Type:  Traps  Informs

V3 Privilege:  Auth  NoAuth  Priv

CLI를 통해 FXOS SNMPv3 구성

```

<#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* #

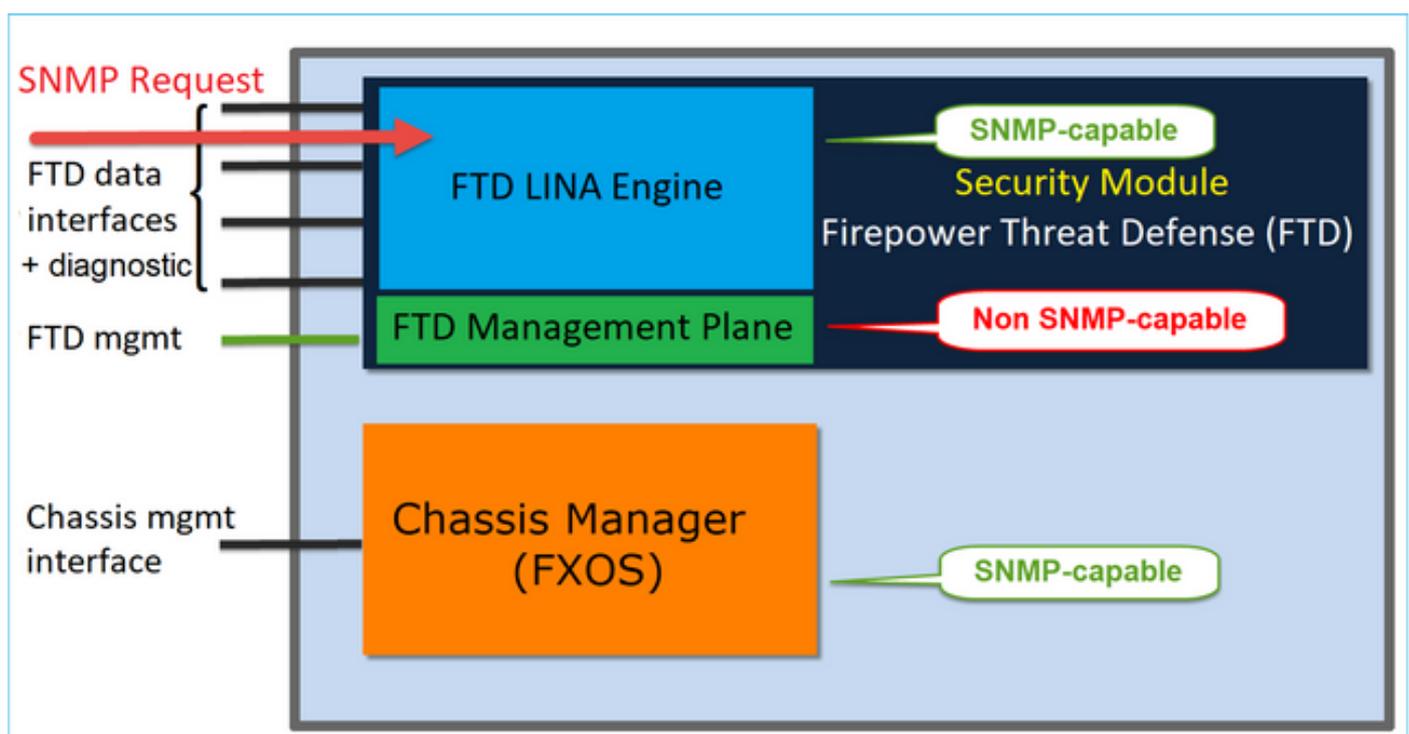
```

```

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

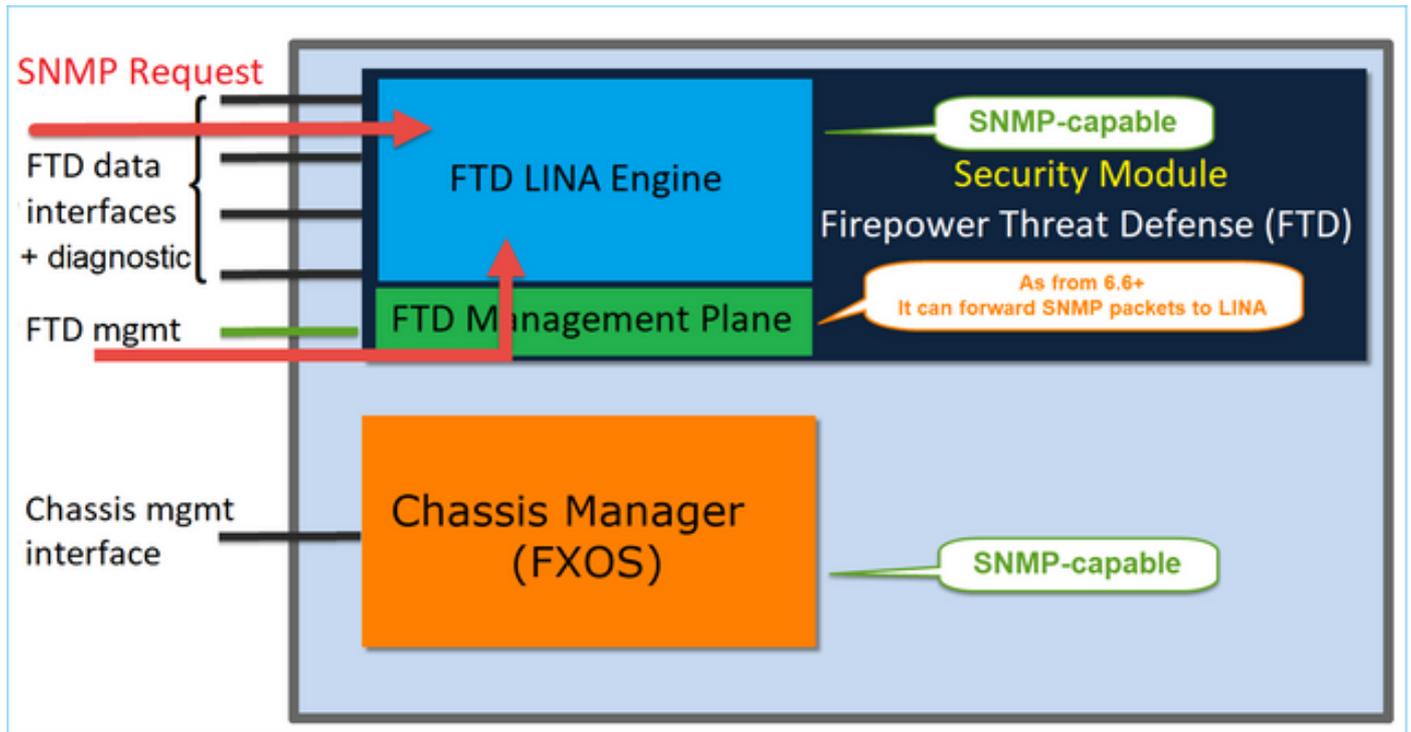
```

## FPR4100/FPR9300의 FTD(LINA) SNMP



## 6.6 이후 릴리스의 변경 사항

- 6.6 이후 릴리스에서는 폴링 및 트랩에 FTD 관리 인터페이스를 사용할 수도 있습니다.



SNMP 단일 IP 관리 기능은 모든 FTD 플랫폼에서 6.6 이후 릴리스에서 지원됩니다.

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- FTD를 실행하는 ASA5500
- FTDv

### LINA SNMPv2c 구성

1단계. FMC UI에서 Devices(디바이스) > Platform Settings(플랫폼 설정) > SNMP로 이동합니다.  
. 'SNMP 서버 활성화' 옵션을 선택하고 다음과 같이 SNMPv2 설정을 구성합니다.

2단계. Hosts(호스트) 탭에서 Add(추가) 버튼을 선택하고 SNMP 서버 설정을 지정합니다.

### Edit SNMP Management Hosts

IP Address\*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port  (1 - 65535)

#### Available Zones

- INSIDE\_FTD4110
- OUTSIDE1\_FTD4110
- OUTSIDE2\_FTD4110
- NET1\_4100-3
- NET2\_4100-3
- NET3\_4100-3

#### Selected Zones/Interfaces

OUTSIDE3

진단 인터페이스를 SNMP 메시지의 소스로 지정할 수도 있습니다. 진단 인터페이스는 박스를 통과하는 트래픽만 허용하는 데이터 인터페이스입니다(관리 전용).

## 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

이 이미지는 6.6 릴리스의 이미지이며 밝은 색 테마를 사용합니다.

추가로 6.6 이후 FTD 릴리스에서는 관리 인터페이스를 선택할 수도 있습니다.

## Add SNMP Management Hosts

IP Address\*

SNMP-SERVER



SNMP Version

2c

Username

Community String

Confirm

Poll

Trap

Trap Port

162

(1 - 65535)

Reachable By:

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

Security Zones or Named Interface

Available Zones



Search

Add

2100\_inside  
2100\_outside  
cluster\_dmz  
cluster\_inside  
cluster\_outside

Selected Zones/Interfaces

diagnostic



Interface Name

Add

Cancel

OK

새 관리 인터페이스를 선택하면 관리 인터페이스를 통해 LINA SNMP를 사용할 수 있습니다.

결과:

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

### LINA SNMPv3 구성

1단계. FMC UI에서 Devices(디바이스) > Platform Settings(플랫폼 설정) > SNMP로 이동합니다 . Enable SNMP Servers(SNMP 서버 활성화) 옵션을 선택하고 SNMPv3 User and Host(SNMPv3 사용자 및 호스트)를 구성합니다.

**Add Username**

Security Level: Priv

Username\*: cisco

Encryption Password Type: Clear Text

Auth Algorithm Type: SHA

Authentication Password\*: .....

Confirm\*: .....

Encryption Type: AES128

Encryption Password\*: .....

Confirm\*: .....

OK Cancel

Overview Analysis Policies **Devices** Objects AMP Intelligence

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

### mzafeiro\_FTD4110-HA

Enter Description

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

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Port  (1 - 65535)

**Hosts** Users SNMP Traps

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

2단계. 트랩을 수신하도록 호스트도 구성합니다.

### Edit SNMP Management Hosts

IP Address\*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Port  (1 - 65535)

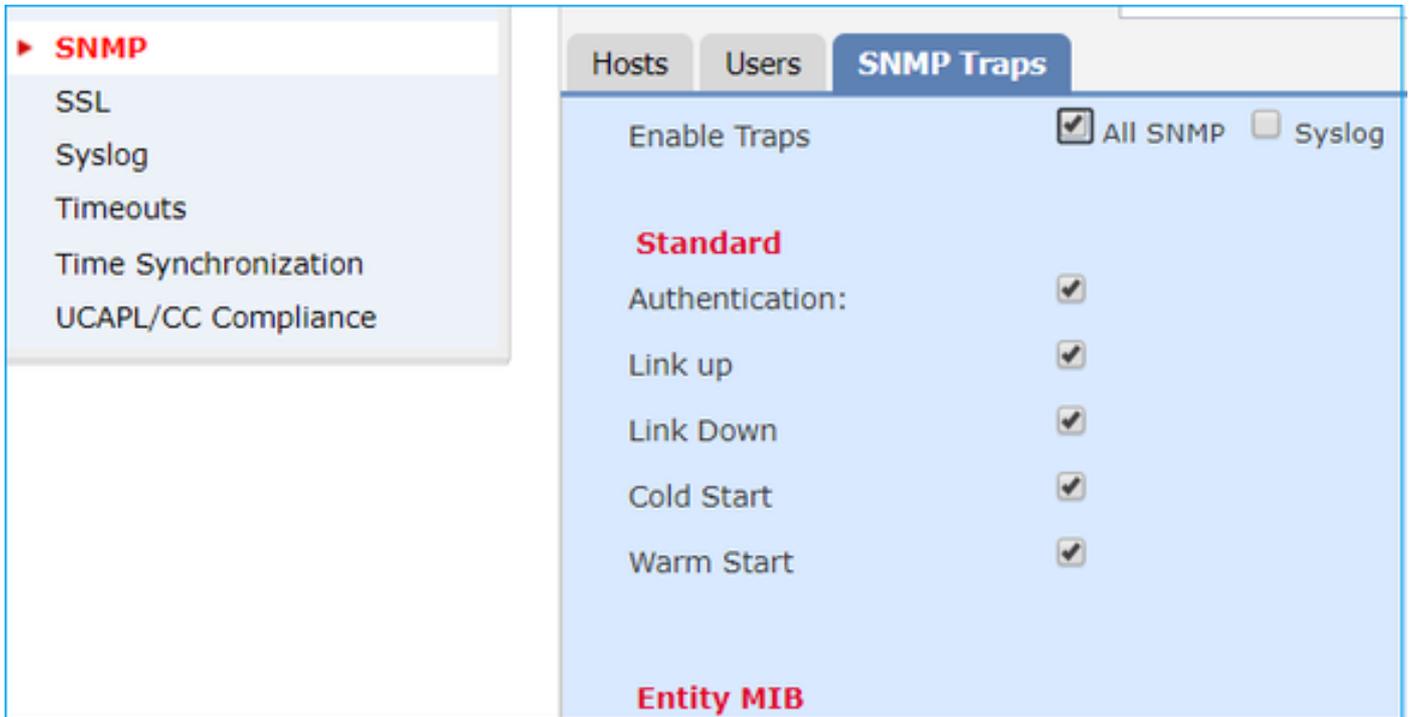
**Available Zones**

INSIDE\_FTD4110

**Selected Zones/Interfaces**

OUTSIDE3

3단계. 수신할 트랩은 SNMP Traps(SNMP 트랩) 섹션에서 선택할 수 있습니다.



MIO 블레이드 SNMP 통합(FXOS 2.12.1, FTD 7.2, ASA 9.18.1)

## 7.2 이전 동작

- 9300 및 4100 플랫폼에서는 FTD/ASA 애플리케이션에 구성된 SNMP에서 쉐시 정보에 대한 SNMP MIB를 사용할 수 없습니다. 쉐시 관리자를 통해 MIO에서 별도로 구성하고 별도로 액세스해야 합니다. MIO는 관리 및 I/O(수퍼바이저) 모듈입니다.
- 두 개의 개별 SNMP 정책을 구성해야 합니다. 하나는 블레이드/엡에, 다른 하나는 SNMP 모니터링을 위한 MIO에 각각 구성해야 합니다.
- 동일한 디바이스의 SNMP 모니터링을 위해 블레이드와 MIO에 각각 하나씩 별도의 포트가 사용됩니다.
- 따라서 SNMP를 통해 9300 및 4100 디바이스를 구성하고 모니터링하려고 할 때 복잡성이 발생할 수 있습니다.

최신 릴리스(FXOS 2.12.1, FTD 7.2, ASA 9.18.1 이상)에서 작동하는 방식

- MIO 블레이드 SNMP 통합을 통해 사용자는 애플리케이션(ASA/FTD) 인터페이스를 통해 LINA 및 MIO MIB를 폴링할 수 있습니다.
- 이 기능은 새로운 MIO CLI 및 FCM(Chassis Mgr) UI를 통해 활성화 또는 비활성화할 수 있습니다.
- 기본 상태는 disabled입니다. 이는 MIO SNMP 에이전트가 독립형 인스턴스로 실행 중임을 의미합니다. 쉐시/DME MIB를 폴링하는 데 MIO 인터페이스를 사용해야 합니다. 이 기능이 활성화되면 애플리케이션 인터페이스를 사용하여 동일한 MIB를 폴링할 수 있습니다.
- 이 컨피그레이션은 Chassis Manager UI의 Platform-settings(플랫폼 설정) > SNMP > Admin Instance(관리 인스턴스)에서 사용할 수 있습니다. 여기서 사용자는 쉐시 MIB를 수집/수집하여 NMS에 제공할 FTD 인스턴스를 지정할 수 있습니다
- ASA/FTD 네이티브 및 MI 애플리케이션이 지원됩니다.
- 이 기능은 MIO 기반 플랫폼(FPR9300 및 FPR4100)에만 적용됩니다.

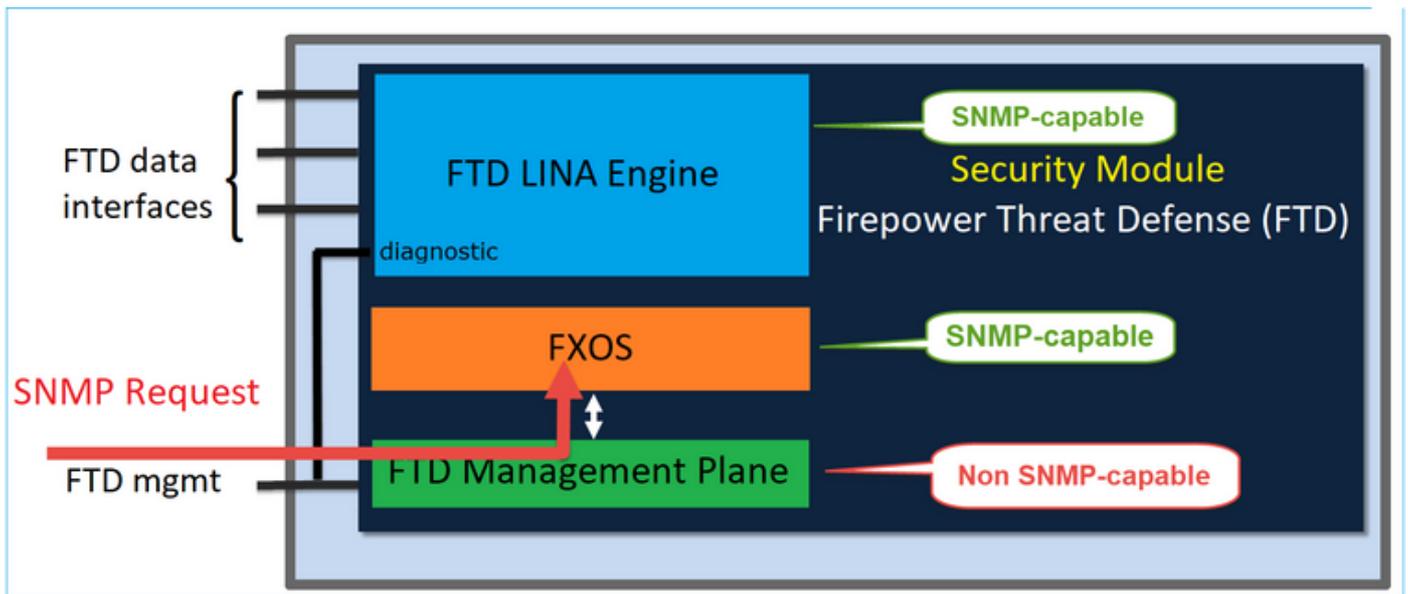
사전 요구 사항, 지원되는 플랫폼

- 지원되는 최소 관리자 버전: FCM 2.12.1
- 관리되는 디바이스: FPR9300/FP4100 Series
- 최소 지원 관리되는 디바이스 버전 필요: FXOS 2.12.1, FTD 7.2 또는 ASA 9.18.1

## FPR2100의 SNMP

FPR2100 시스템에는 FCM이 없습니다. SNMP를 구성하는 유일한 방법은 FMC를 사용하는 것입니다.

## FPR2100의 새시(FXOS) SNMP



FTD 6.6 이후 릴리스에서는 SNMP용 FTD 관리 인터페이스를 사용할 수도 있습니다. 이 경우 FXOS 및 LINA SNMP 정보가 FTD 관리 인터페이스를 통해 전송됩니다.

## FXOS SNMPv1/v2c 구성

FMC UI를 열고 Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다. 디바이스를 선택하고 SNMP를 선택합니다.

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

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

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

Device Routing Interfaces Inline Sets DHCP **SNMP**

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

Admin State:  Enable

Port: 161

Community: \*\*\*\*\*

System Admin Name: |

Location:

SNMP Traps Configuration

Hostname	Port	Version	V3 Privilege	Type
No records to display				

2 Add

## SNMP Trap Configuration

Hostname:\* 10.48.26.190 +

Community String:\* \*\*\*\*\*

Port:\* 162 (1 - 65535)

SNMP Version: V2

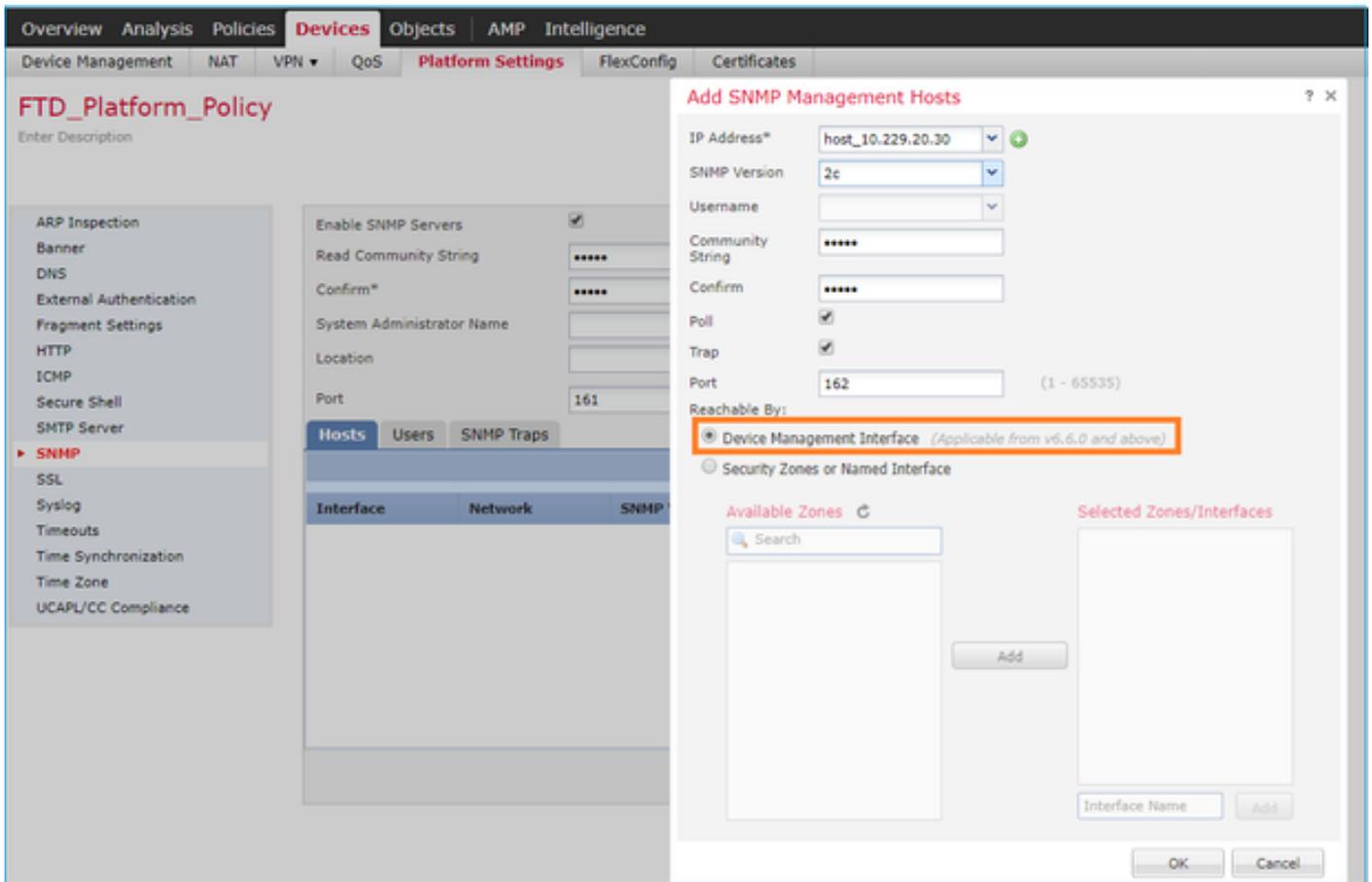
Type: TRAPS

Privilege: NO\_AUTH

OK Cancel

FTD 6.6 이후 릴리스의 변경 사항

FTD 관리 인터페이스를 지정할 수 있습니다.



SNMP에 대한 관리 인터페이스도 구성할 수 있으므로 페이지에 다음 경고 메시지가 표시됩니다.

Device(디바이스) > Platform Settings(Threat Defense) > SNMP > Hosts(호스트)를 통해 Device Management Interface(디바이스 관리 인터페이스)로 SNMP 설정을 구성한 경우 이 페이지에서 디바이스 플랫폼 SNMP 컨피그레이션을 사용할 수 없습니다.

### FXOS SNMPv3 구성

FMC UI를 열고 Choose Devices(디바이스 선택) > Device Management(디바이스 관리)로 이동합니다. 디바이스를 선택하고 SNMP를 선택합니다.

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\*:

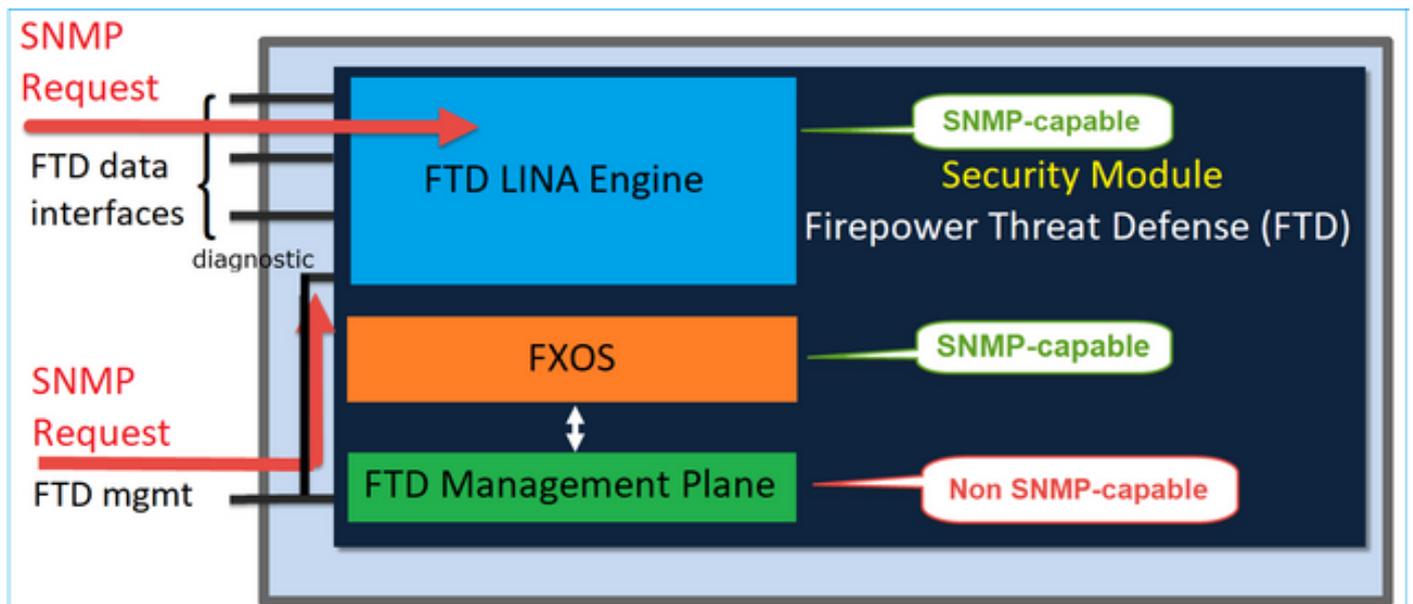
Confirm:

## SNMP Trap Configuration

Hostname:\*  +  
 Community String:\*   
 Port:\*  (1 - 65535)  
 SNMP Version:   
 Type:   
 Privilege:

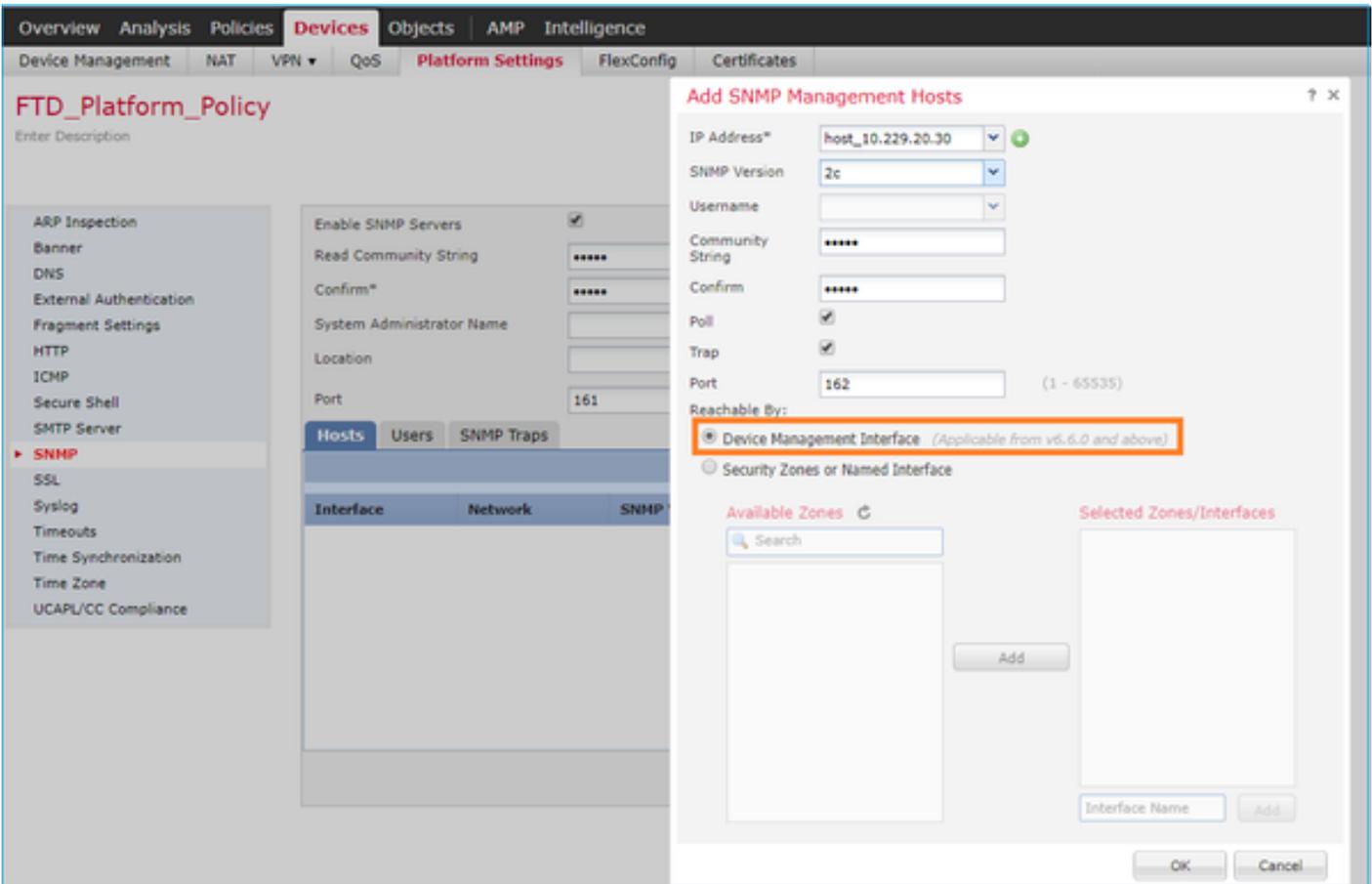
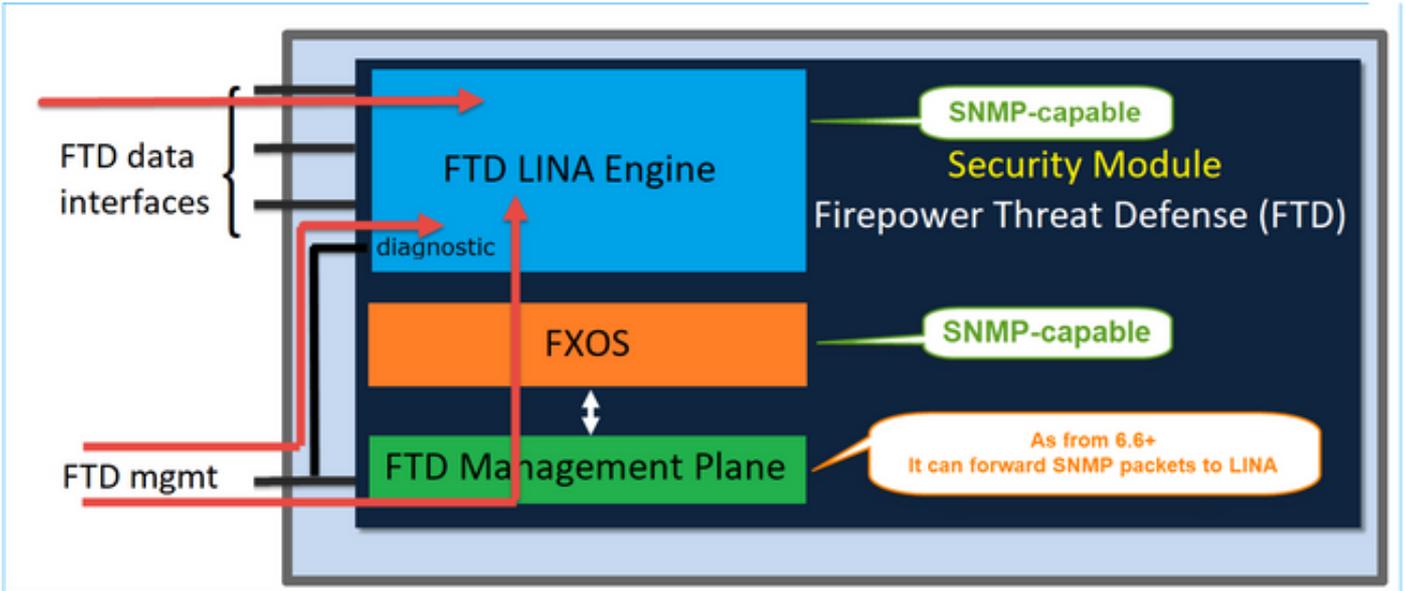
### FPR2100의 FTD(LINA) SNMP

- 6.6 이전 릴리스의 경우 FTD FP1xxx/FP21xx 어플라이언스의 LINA FTD SNMP 구성은 Firepower 4100 또는 9300 어플라이언스의 FTD와 동일합니다.



FTD 6.6 이후 릴리스

- 6.6 이후 릴리스에서는 LINA 폴링 및 트랩에 FTD 관리 인터페이스를 사용할 수도 있습니다.

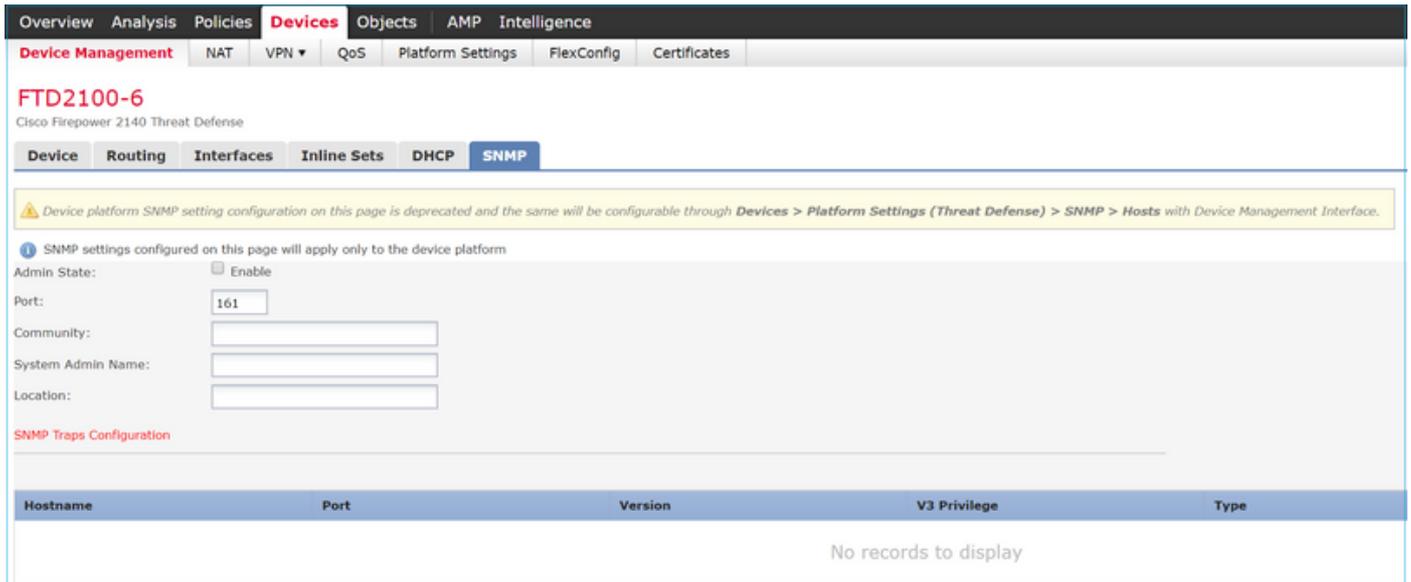


새 관리 인터페이스가 선택된 경우:

- LINA SNMP는 관리 인터페이스를 통해 사용할 수 있습니다.
- Devices(디바이스) > Device Management(디바이스 관리)에서 SNMP 탭은 더 이상 필요하지 않으므로 비활성화됩니다. 알림 배너가 표시됩니다. SNMP 디바이스 탭은 2100/1100 플랫폼에서만 표시되었습니다. 이 페이지는 FPR9300/FPR4100 및 FTD55xx 플랫폼에 없습니다.

구성이 완료되면 (FP1xxx/FP2xxx의) 결합된 LFP SNMP + FXOS SNMP 폴링/트랩 정보가 FTD 관

리 인터페이스를 통해 전송됩니다.



SNMP 단일 IP 관리 기능은 모든 FTD 플랫폼에서 6.6 이후 릴리스에서 지원됩니다.

- FPR2100
- FPR1000
- FPR4100
- FPR9300
- FTD를 실행하는 ASA5500
- FTDv

자세한 내용은 Threat Defense에 대한 SNMP 설정 참조

다음을 확인합니다.

FPR4100/FPR9300용 FXOS SNMP 확인

FXOS SNMPv2c 확인

CLI 구성 확인:

```
<#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 모드에서:

<#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

```

추가 확인:

<#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 요청 테스트.

유효한 호스트에서 SNMP 요청 수행.

트랩 생성 확인.

EthAnalyzer가 활성화된 상태에서 인터페이스 플랩을 사용하여 SNMP 트랩이 생성되어 정의된 트랩 호스트로 전송되는지 확인할 수 있습니다.

```
<#root>
```

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

```
ethalyzer 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
```

---

 경고: 인터페이스 플랩은 트래픽 중단을 일으킬 수 있습니다. 이 테스트는 랩 환경 또는 유지 보수 기간에만 수행하십시오.

---

## FXOS SNMPv3 확인

1단계. Open FCM UI Platform Settings(FCM UI 플랫폼 설정) > SNMP > User(사용자)는 구성된 비밀번호 및 프라이버시 비밀번호가 있는지 표시합니다.

## Edit user1

Name:\*

Auth Type: SHA

Use AES-128:

Password:  Set:Yes

Confirm Password:

Privacy Password:  Set:Yes

Confirm Privacy Password:

OK Cancel

2단계. CLI에서 범위 모니터링에서 SNMP 컨피그레이션을 확인할 수 있습니다.

<#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

3단계. FXOS 모드에서 SNMP 컨피그레이션 및 세부 정보를 확장할 수 있습니다.

```
<#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

SNMP 요청 테스트.

컨피그레이션을 확인하고 SNMP 기능이 있는 모든 디바이스에서 SNMP 요청을 수행할 수 있습니다.

SNMP 요청이 처리되는 방식을 확인하기 위해 SNMP 디버그를 사용할 수 있습니다.

```
<#root>
```

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

```
debug snmp pkt-dump
```

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

---

 주의: 디버그는 디바이스 성능에 영향을 줄 수 있습니다.

---

## FPR2100용 FXOS SNMP 확인

### FXOS SNMPv2 확인

CLI를 통해 구성 확인:

```
<#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 동작 확인.

FXOS를 폴링하고 호스트 또는 SNMP 기능이 있는 디바이스에서 SNMP 요청을 전송할 수 있는지 확인할 수 있습니다.

capture-traffic 명령을 사용하여 SNMP 요청 및 응답을 확인합니다.

```
<#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
```

## FXOS SNMPv3 확인

CLI를 통해 구성 확인:

```
<#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 동작 확인.

FXOS를 폴링할 수 있는지 확인하기 위해 SNMP 요청 보내기.

추가로 요청을 캡처할 수 있습니다.

```
<#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 확인

FTD LINA SNMP 구성 확인:

```
<#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 이후 FTD에서는 SNMP용 FTD 관리 인터페이스를 구성하고 사용할 수 있습니다.

```
<#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
```

추가 확인:

```
<#root>
```

```
Firepower-module1#
```

```
show snmp-server host
```

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

SNMP 서버 CLI에서 snmpwalk 실행:

<#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 트래픽 통계를 확인합니다.

<#root>

Firepower-module1#

show snmp-server statistics

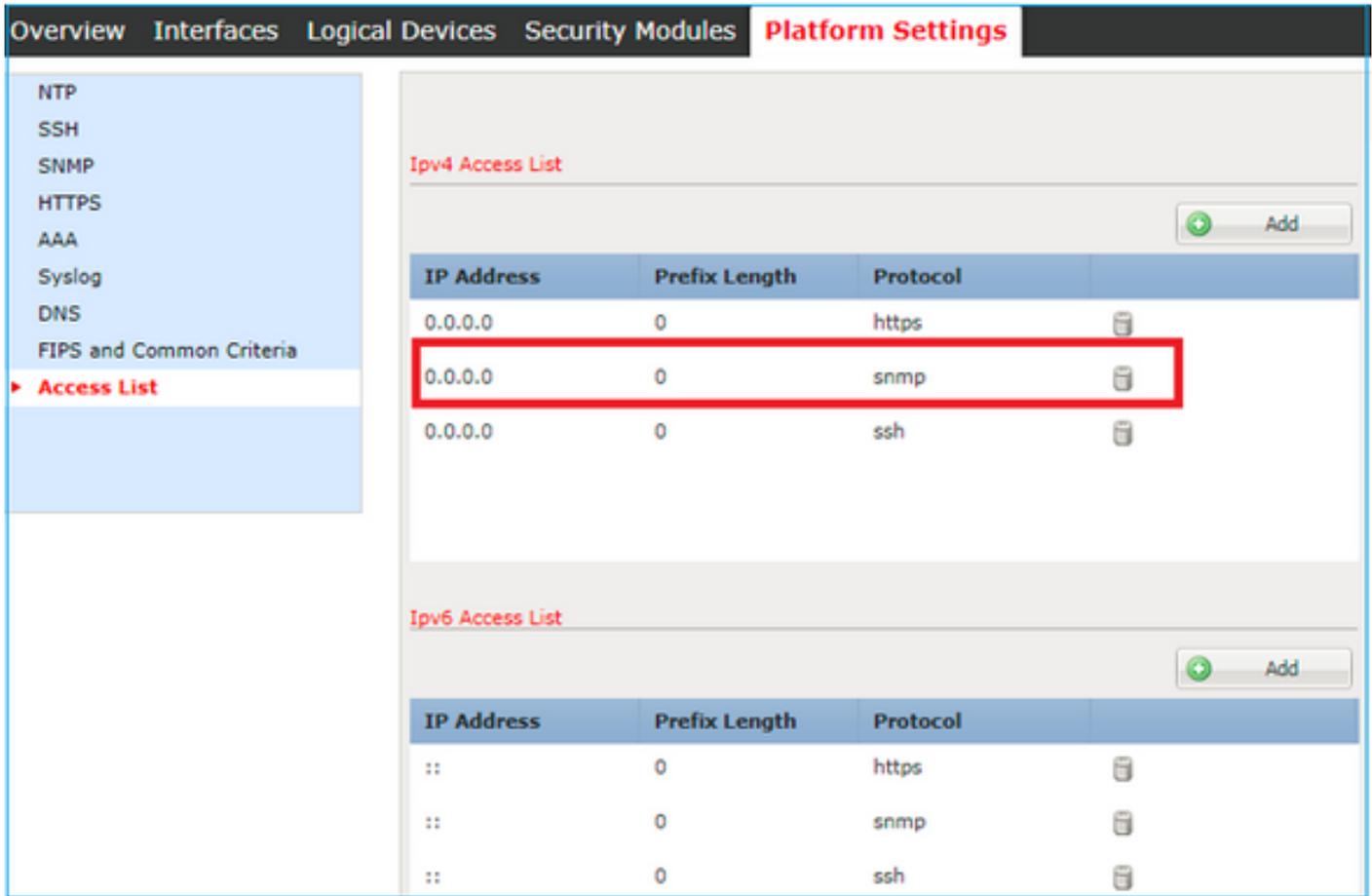
```
1899 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  1899 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  1899 Get-next PDUs
  0 Get-bulk PDUs
  0 Set-request PDUs (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/FPR9300에서 FXOS에 대한 SNMP 트래픽 허용

FPR4100/9300의 FXOS 구성은 소스 IP 주소별로 SNMP 액세스를 제한할 수 있습니다. 액세스 목록 구성 섹션에서는 SSH, HTTPS 또는 SNMP를 통해 디바이스에 연결할 수 있는 네트워크/호스트

를 정의합니다. SNMP 서버의 SNMP 쿼리가 허용되는지 확인해야 합니다.

GUI를 통해 전역 액세스 목록 구성



CLI를 통해 전역 액세스 목록 구성

```
<#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
```

확인

<#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 개체 탐색기 사용

[Cisco SNMP 개체 탐색기](#)는 여러 OID를 변환하고 간단한 설명을 얻을 수 있는 온라인 툴입니다.

Tools & Resources

# SNMP Object Navigator

HOME  
SUPPORT  
TOOLS & RESOURCES  
SNMP Object Navigator

TRANSLATE/BROWSE SEARCH DOWNLOAD MIBS MIB SUPPORT - SW

Translate | Browse The Object Tree

Translate OID into object name or object name into OID to receive object details

Enter OID or object name:  examples -  
OID: 1.3.6.1.4.1.9.9.27  
Object Name: ifIndex

Translate

Object Information

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; - <a href="#">View Supporting Images</a>
Description	A table of overall CPU statistics.

FTD LINA CLI에서 show snmp-server oid 명령을 사용하여 폴링할 수 있는 LINA OID의 전체 목록을 검색합니다.

<#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#
```

 참고: 이 명령은 숨겨집니다.

## 문제 해결

Cisco TAC에서 볼 수 있는 가장 일반적인 SNMP 케이스 생성 원인은 다음과 같습니다.

1. FTD LINA SNMP를 폴링할 수 없음
2. FXOS SNMP를 폴링할 수 없음
3. 어떤 SNMP OID 값을 사용해야 합니까?
4. SNMP 트랩을 가져올 수 없음
5. SNMP를 통해 FMC를 모니터링할 수 없음
6. SNMP를 구성할 수 없음
7. Firepower Device Manager의 SNMP 구성

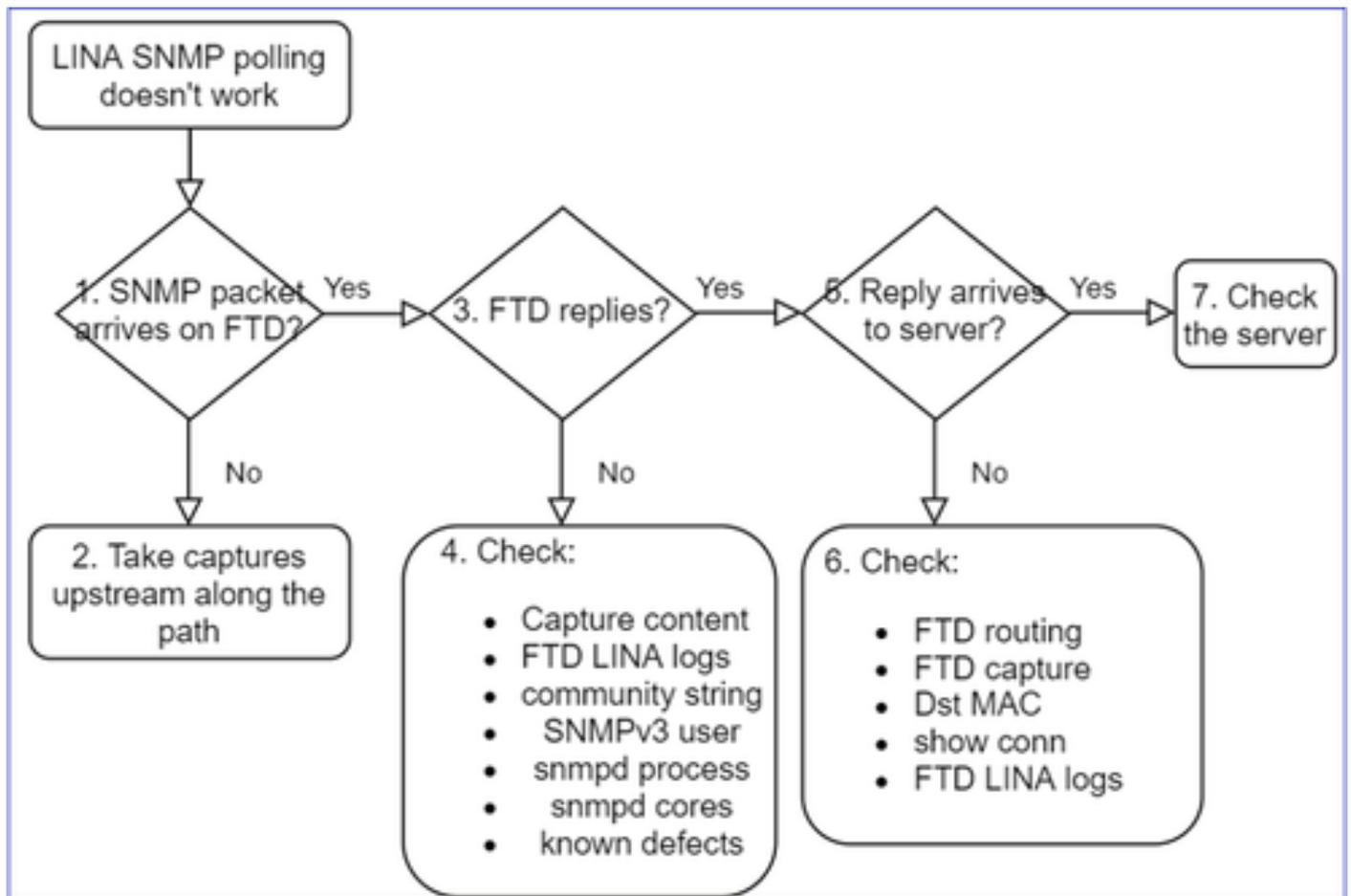
### FTD LINA SNMP를 폴링할 수 없음

문제 설명(실제 Cisco TAC 케이스의 샘플):

- "SNMP를 통해 데이터를 가져올 수 없습니다."
- "SNMPv2를 통해 디바이스를 폴링할 수 없습니다."
- "SNMP가 작동하지 않습니다. SNMP를 사용하여 방화벽을 모니터링하려고 하지만 구성 이후 문제가 발생합니다."
- "SNMP v2c 또는 3을 통해 FTD를 모니터링할 수 없는 두 개의 모니터링 시스템이 있습니다."
- "SNMP walk가 방화벽에서 작동하지 않습니다."

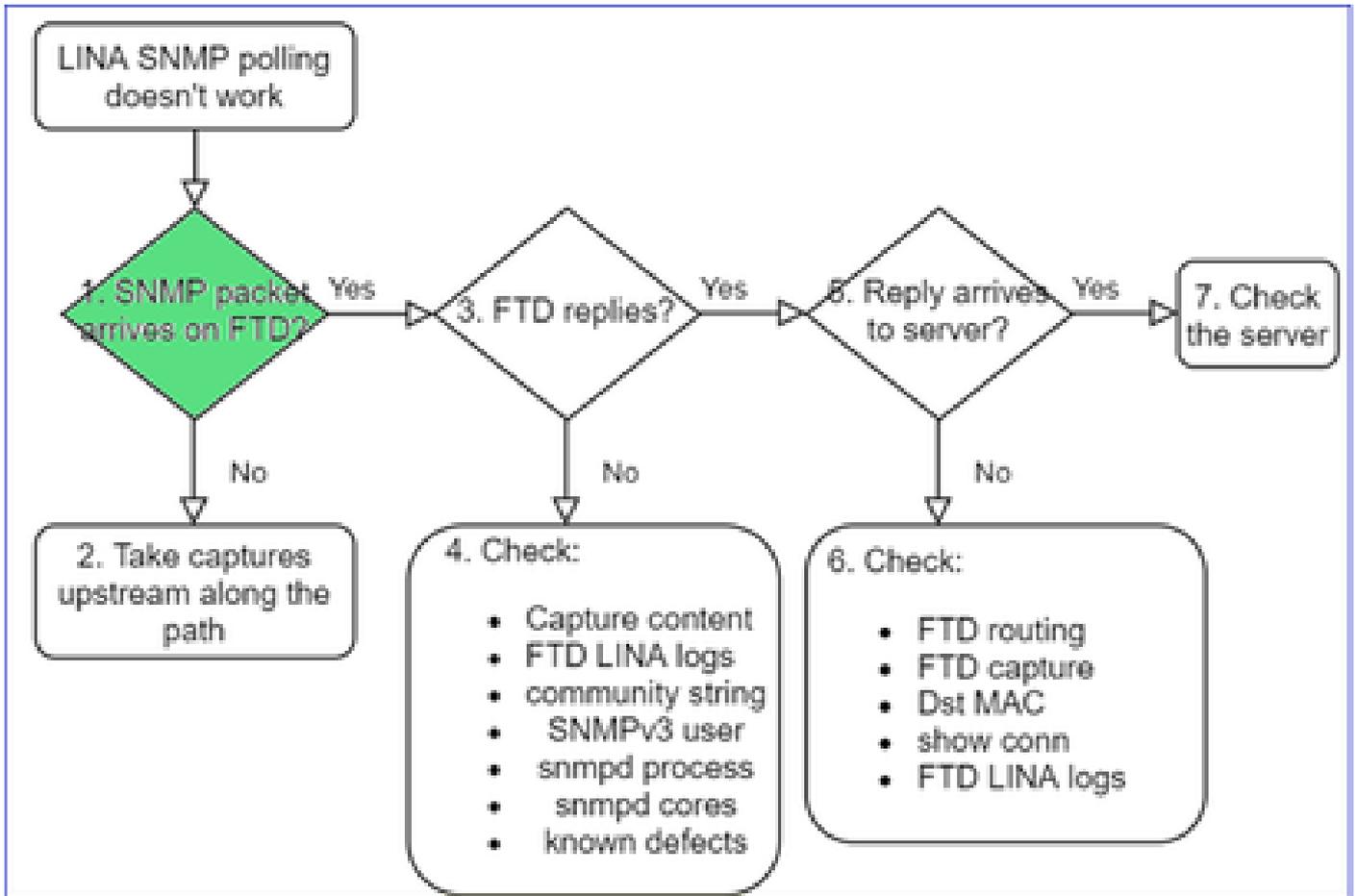
문제 해결 방법에 대한 권장 사항

다음은 LINA SNMP 폴링 문제에 대한 순서도 문제를 해결하는 권장 프로세스입니다.



### 심층 분석

1. SNMP 패킷이 FTD에 도착합니까?



- 캡처를 활성화하여 SNMP 패킷 도착 확인.

FTD 관리 인터페이스(post-6.6 릴리스)의 SNMP는 다음과 같이 management 키워드를 사용합니다

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

FTD 데이터 인터페이스의 SNMP는 인터페이스의 이름을 사용합니다.

```
<#root>
```

```
firepower#
```

```
show run snmp-server
```

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

FTD 관리 인터페이스에서 캡처:

```
<#root>
```

```
>
```

```
capture-traffic
```

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

```
0 - management1
```

```
1 - management0
```

```
2 - Global
```

```
Selection?
```

```
1
```

FTD 데이터 인터페이스에서 캡처:

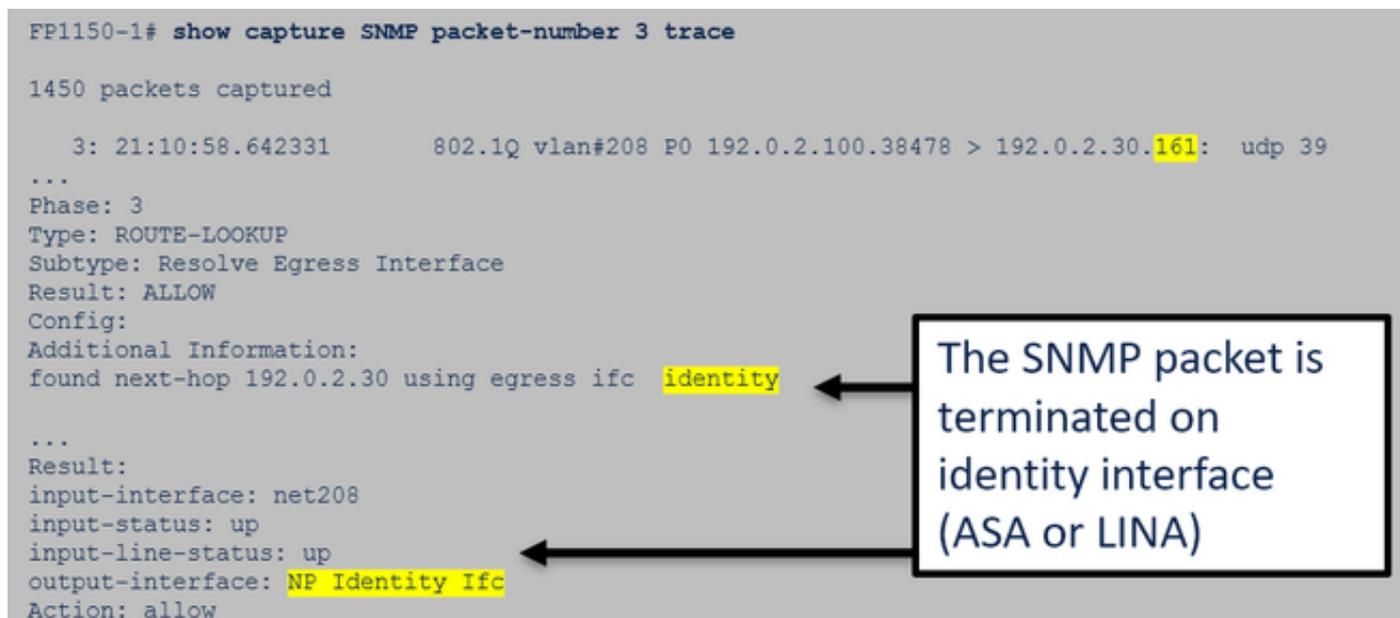
```
<#root>
```

```
firepower#
```

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

FTD 데이터 인터페이스 패킷 추적(6.6/9.14.1 이전):

```
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
```



FTD 데이터 인터페이스 패킷 추적(6.6/9.14.1 이후):

```

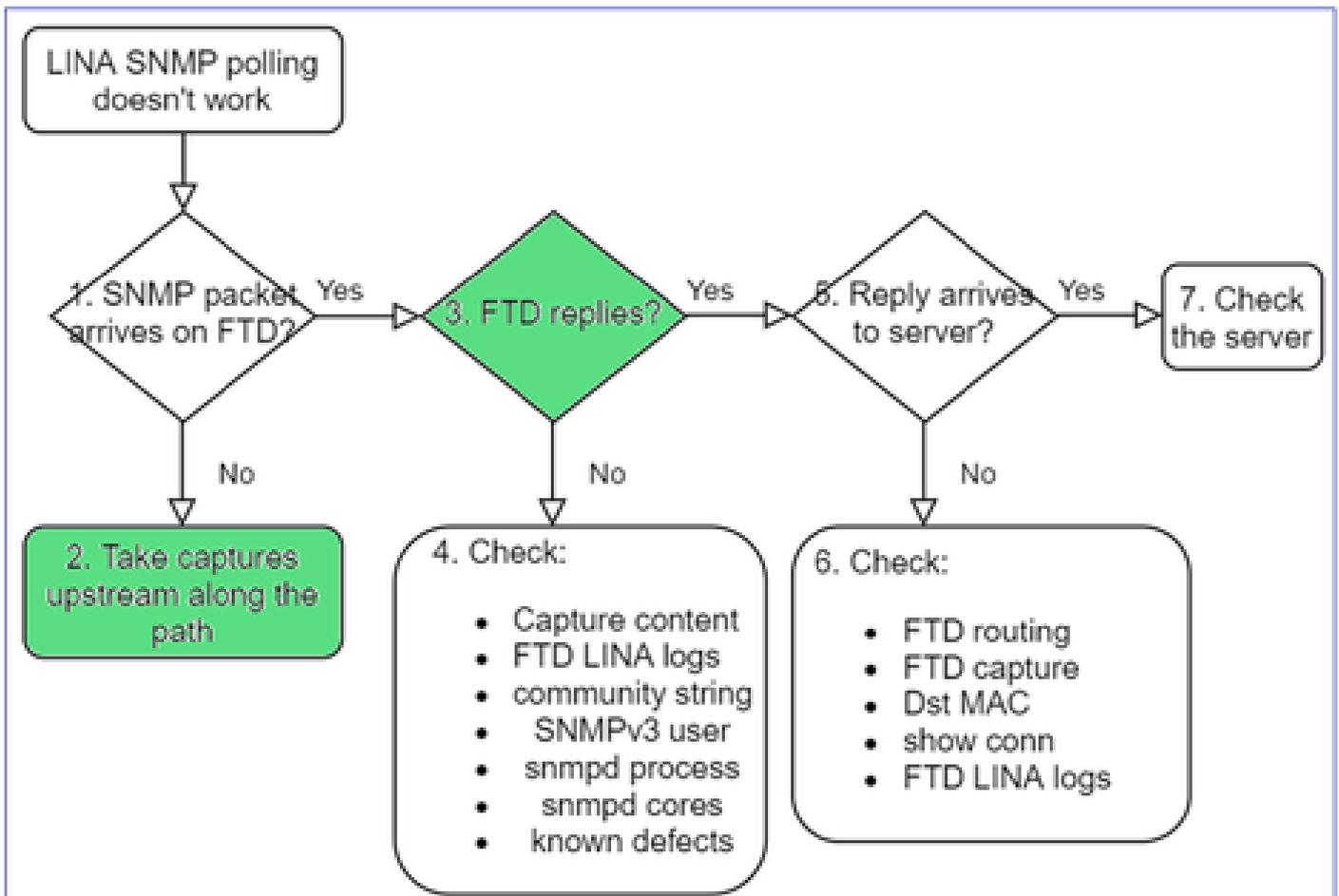
firepower# show capture SNMP packet-number 1 trace
1: 22:43:39.568101      802.1Q vlan#201 P0 192.168.21.100.58255 > 192.168.21.50.161:  udp 39
...
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 9
Config:
nat (nlp_int_tap,net201) source static nlp_server__snmp_192.168.21.100_intf4 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. FTD 인그레스 캡처에 SNMP 패킷이 표시되지 않는 경우:

- 경로를 따라 업스트림 캡처 수행.
- SNMP 서버가 적절한 FTD IP를 사용하는지 확인.
- FTD 인터페이스를 향하는 스위치 포트에서 시작하여 업스트림으로 이동.



3. FTD SNMP 회신이 표시됩니까?

다음을 확인하여 FTD가 응답하는지 확인:

1. FTD 이그레스 캡처(LINA 또는 관리 인터페이스)

소스 포트 161을 사용하는 SNMP 패킷 확인:

```
<#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 이후 릴리스에서는 NLP 탭 인터페이스에서 캡처라는 하나의 추가 캡처 포인트가 있습니다. NATed IP는 162.254.x.x 범위의 IP입니다.

```
<#root>
```

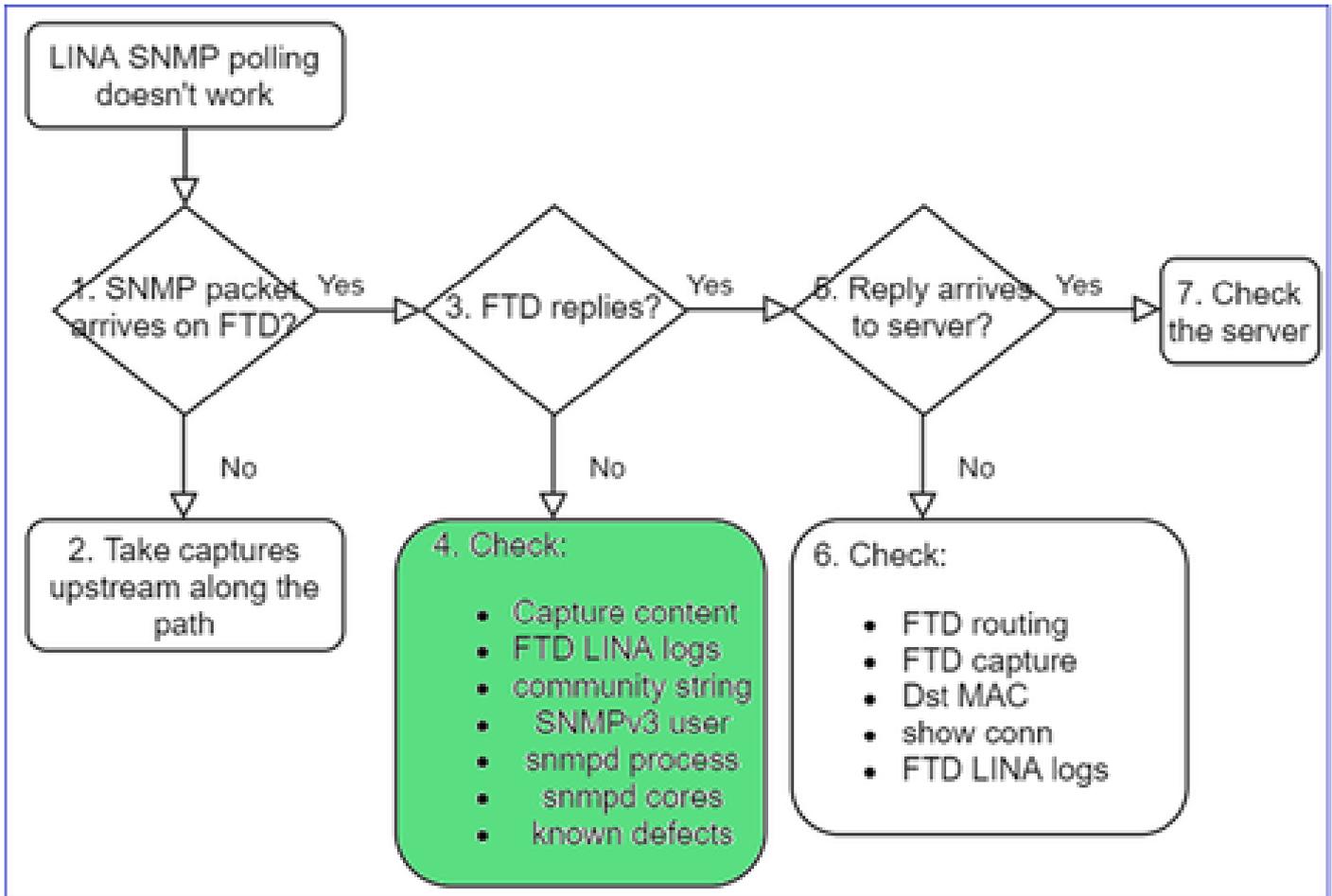
```
admin@firepower:~$
```

```
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. 추가 검사



a. Firepower 4100/9300 디바이스의 경우 FXOS 호환성 테이블을 확인합니다.

**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		
<b>2.13(0.198)+</b> <b>Note</b> 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	<b>9.19(x)</b> (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.3.0</b> (recommended) 7.2.0 7.1.0 7.0.0 6.7.0 6.6.x		
	Firepower 4145 Firepower 4125 Firepower 4115	<b>9.19(x)</b> (recommended) 9.18(x) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.3.0</b> (recommended) 7.2.0 7.1.0 7.0.0 6.7.0 6.6.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)	7.0.0 6.7.0 6.5.0 6.4.0		
	<b>2.12(0.31)+</b> <b>Note</b> 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	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0 6.7.0 6.6.x	
		Firepower 4145 Firepower 4125 Firepower 4115	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0 6.7.0 6.6.x	
		Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.14(x) 9.13(1) 9.12(x)	6.6.x 6.5.0 6.4.0	
		Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	<b>9.18(x)</b> (recommended) 9.17(x) 9.16(x) 9.15(1) 9.14(x) 9.13(x) 9.12(x)	<b>7.2.0</b> (recommended) 7.1.0 7.0.0 6.7.0 6.6.x 6.5.0 6.4.0 6.3.0	
		Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.10(x) 9.9(x) 9.8(x)	6.4.0 6.3.0	
		<b>2.11(1.154)+</b> <b>Note</b> 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	<b>9.17(x)</b> (recommended) 9.16(x) 9.15(1) 9.14(x)	<b>7.1.0</b> (recommended) 7.0.0 6.7.0 6.6.x

b. FTD LINA snmp-server 통계를 확인합니다.

```
<#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 연결 테이블

이 검사는 FTD 인그레스 인터페이스의 캡처에 패킷이 표시되지 않는 경우에 매우 유용합니다. 이 확인은 데이터 인터페이스의 SNMP에 대해서만 유효합니다. SNMP가 관리 인터페이스(post-6.6/9.14.1)에 있으면 연결이 생성되지 않습니다.

```
<#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

데이터 인터페이스의 SNMP에 대해서만 유효한 확인입니다. SNMP가 관리 인터페이스에 있는 경우 로그가 생성되지 않습니다.

```
<#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. 잘못된 호스트 소스 IP로 인해 FTD에서 SNMP 패킷을 삭제하는지 확인합니다.

The screenshot shows a CLI session with the following commands and outputs:

```

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(vrfd:0)
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
flow (NA)/NA

firepower# show run snmp-server
snmp-server host net201 192.168.22.100 community **** version 2c

firepower# show asp table classify interface net201 domain permit match port=161
Input Table
in id=0x14f65b193b30, priority=501, domain=permit, deny=false
hits=8, user_data=0x0, cs_id=0x0, use_real_addr, flags=0x0, protocol=17
src ip/id=192.168.22.100, mask=255.255.255.255, port=0, tag=any
dst ip/id=169.254.1.2, mask=255.255.255.255, port=161, tag=any, dscp=0x0, nsg_id=none
input_ifc=net201(vrfd:0), output_ifc=any

```

Annotations in the image:

- Mismatch in the src IP**: Points to the source IP 192.168.22.100 in the configuration and the destination IP 192.168.21.50 in the capture trace.
- No UN-NAT phase!**: Points to the capture trace output, indicating that the source IP was not translated.

f. 잘못된 자격 증명(SNMP 커뮤니티)

캡처 콘텐츠에서 커뮤니티 값(SNMP v1 및 2c)을 확인할 수 있습니다.

The screenshot shows a network capture window with the following details:

Delta	Source	Destination	Protocol	Length
0.000000	192.168.21.100	192.168.21.50	SNMP	

Packet details:

- Frame 3: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
- Ethernet II, Src: VMware\_85:3e:d2 (00:50:56:85:3e:d2), Dst: a2:b8:dc:
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 201
- Internet Protocol Version 4, Src: 192.168.21.100, Dst: 192.168.21.50
- User Datagram Protocol, Src Port: 45230, Dst Port: 161
- Simple Network Management Protocol
  - version: v2c (1)
  - community: cisco123
  - data: get-next-request (1)

g. 잘못된 컨피그레이션(예: SNMP 버전 또는 커뮤니티 문자열)

디바이스 SNMP 구성 및 커뮤니티 문자열을 확인하는 몇 가지 방법이 있습니다.

<#root>

firepower#

more system:running-config | i community

snmp-server host net201 192.168.2.100 community CISC0123 version 2c

다른 방법:

```
<#root>
```

```
firepower#
```

```
debug menu netsnmp 4
```

#### h. FTD LINA/ASA ASP 삭제

FTD에서 SNMP 패킷이 삭제되었는지를 확인하는 데 유용합니다. 먼저, 카운터를 지우고(clear asp drop) 테스트합니다.

```
<#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 캡처

ASP 캡처는 삭제된 패킷에 대한 가시성을 제공합니다(예: ACL 또는 인접성).

```
<#root>
```

```
firepower#
```

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

테스트하고 캡처 콘텐츠 확인:

```
<#root>
```

```
firepower#
```

```
show capture
```

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

## j. SNMP 코어(역추적) - 확인 방법 1

시스템 안정성 문제가 의심되는 경우에 유용합니다.

```
<#root>
```

```
firepower#
```

```
show disk0: | i core
```

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

## SNMP core(역추적) - 확인 방법 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 core 파일이 표시되면 다음 항목을 수집하고 Cisco TAC에 문의합니다.

- FTD TS 파일(또는 ASA show tech)
- snmpd core 파일

SNMP debug(숨겨진 명령이며 최신 버전에서만 사용 가능):

```
<#root>
```

```
firepower#
```

```
debug snmp trace [255]
```

```
firepower#
```

```
debug snmp verbose [255]
```

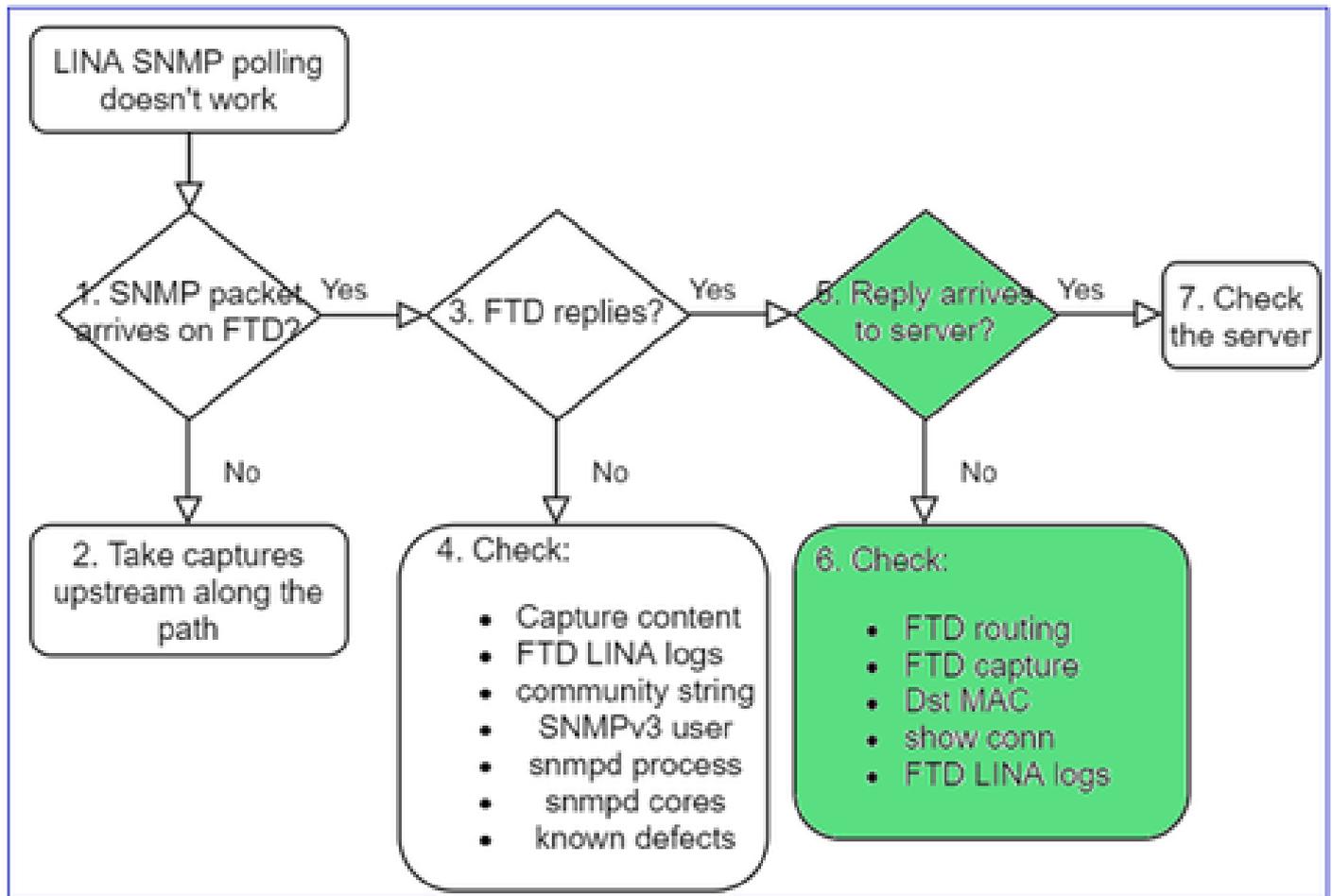
```
firepower#
```

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

```
firepower#
```

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

방화벽 SNMP 응답이 서버에 도착합니까?



FTD가 응답하지만 응답이 서버에 도달하지 않는 경우:

a. FTD 라우팅

FTD 관리 인터페이스 라우팅의 경우:

```
<#root>
```

```
>
```

```
show network
```

FTD LINA 데이터 인터페이스 라우팅의 경우:

```
<#root>
```

```
firepower#
```

```
show route
```

## b. 대상 MAC 확인

FTD 관리 대상 MAC 확인:

```
<#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 데이터 인터페이스 대상 MAC 확인:

```
<#root>
```

```
firepower#
```

```
show capture SNMP detail
```

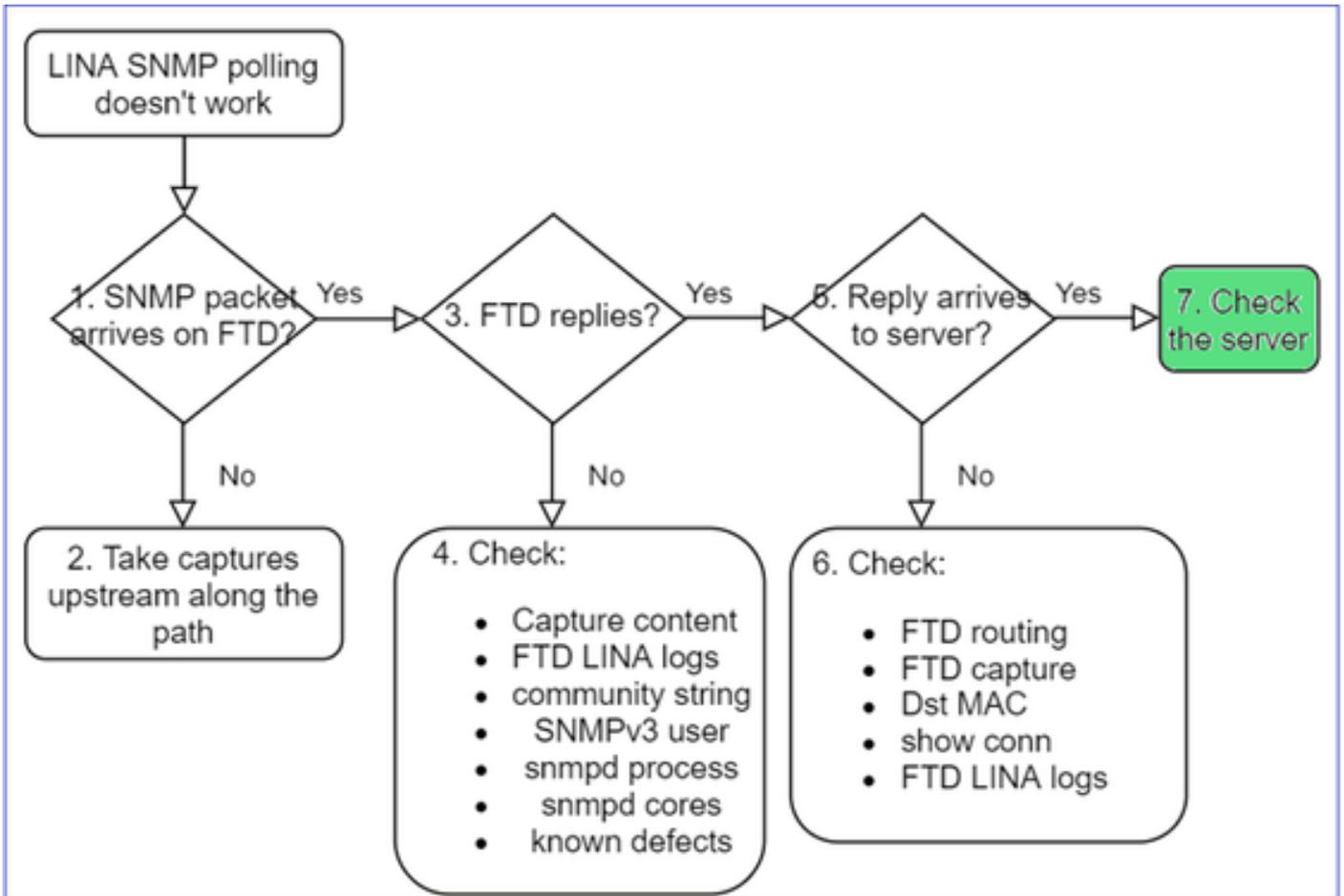
```
...
```

```
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 패킷을 삭제/차단할 가능성이 있는 경로를 따라 디바이스를 확인합니다.

SNMP 서버 확인



a. 캡처 내용을 확인하여 설정을 확인합니다.

b. 서버 컨피그레이션을 확인합니다.

c. SNMP 커뮤니티 이름을 수정해 봅니다(예: 특수 문자 제외).

두 가지 조건이 충족되는 한 엔드 호스트 또는 FMC를 사용하여 폴링을 테스트할 수 있습니다.

1. SNMP 연결이 설정됨.
2. 소스 IP는 디바이스를 폴링할 수 있음.

<#root>

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

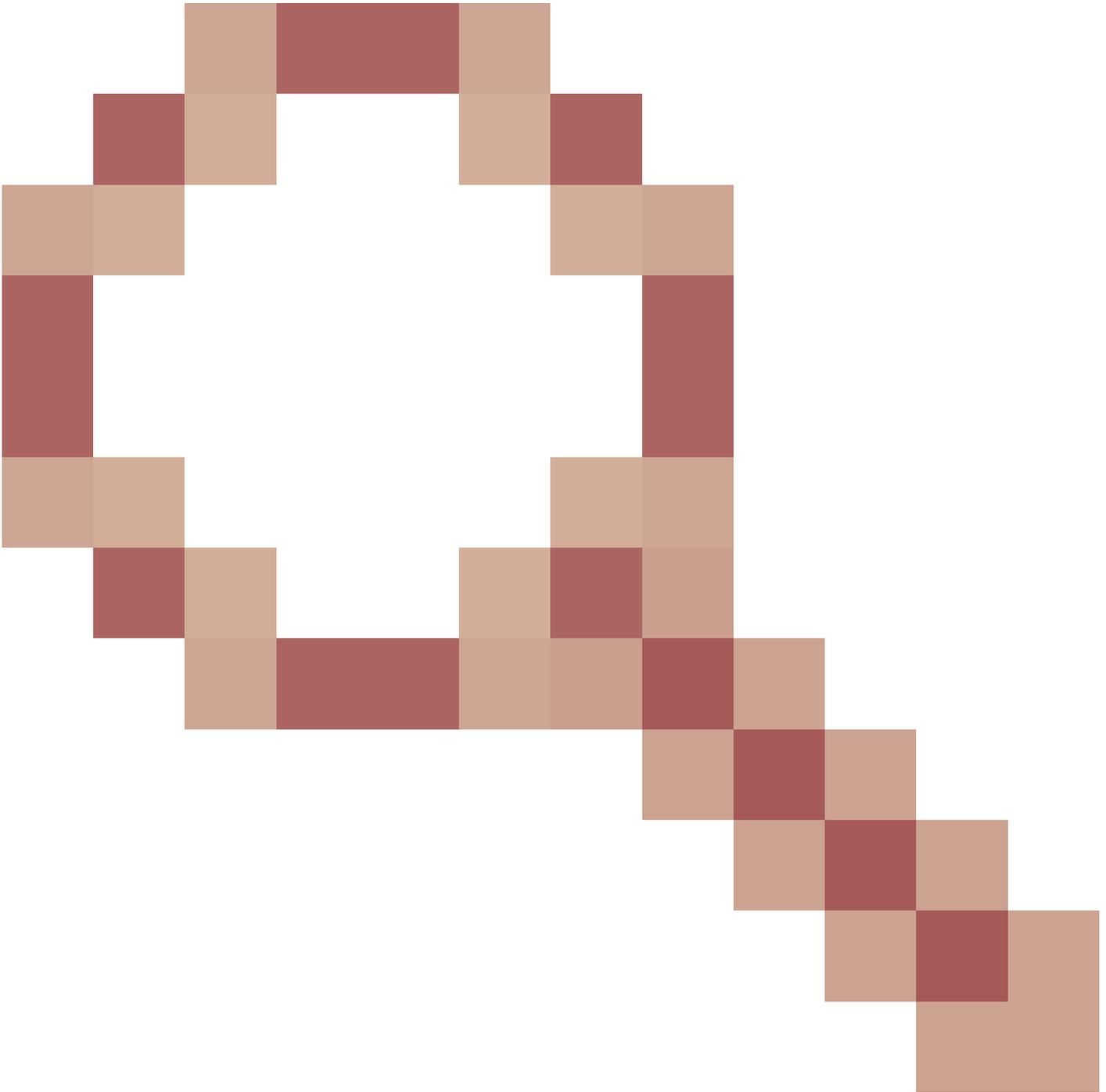
```
snmpwalk -c cisco -v2c 192.0.2.197
```

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

### SNMPv3 폴링 고려 사항

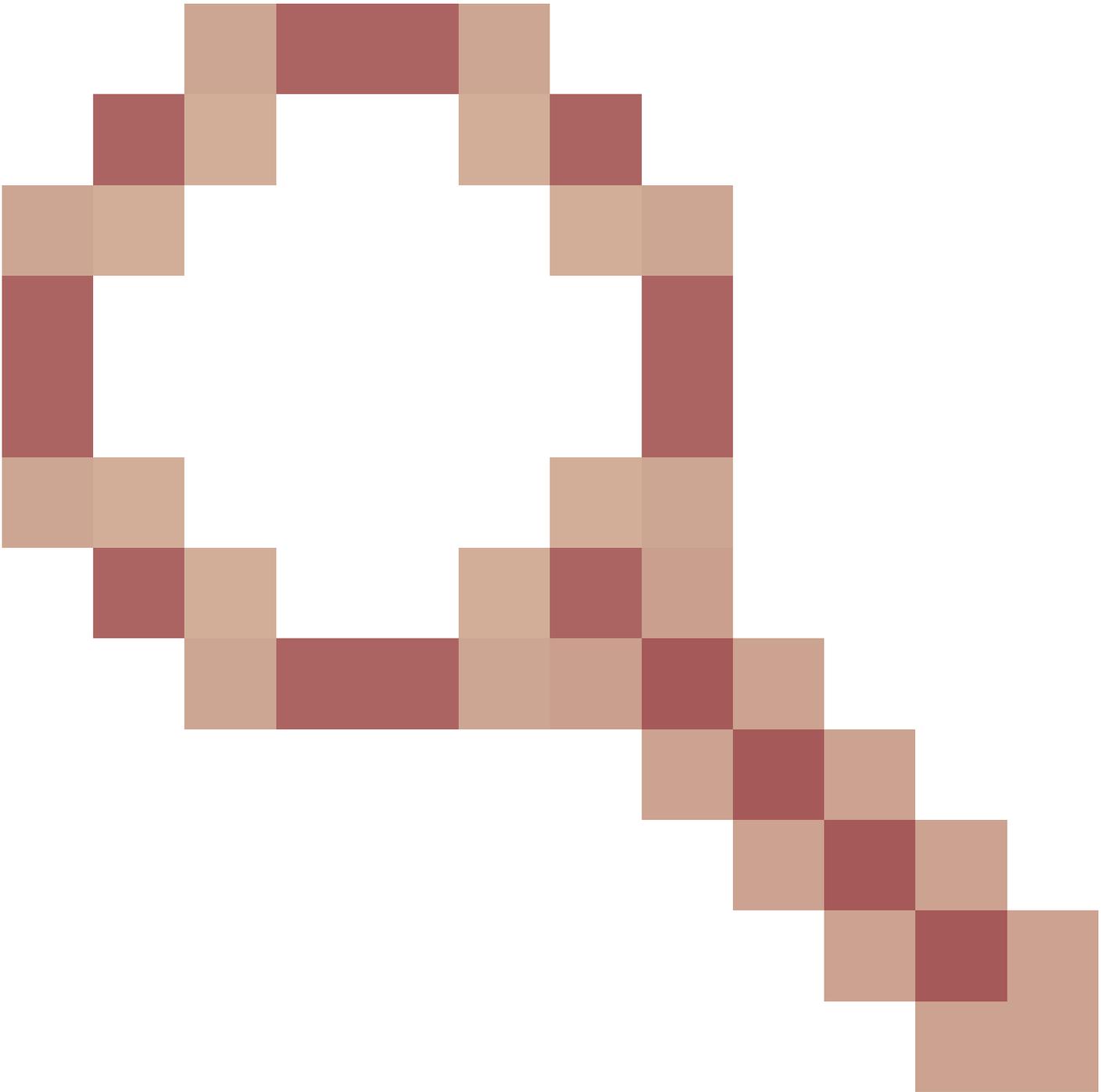
- 라이선스: SNMPv3에는 Strong Encryption 라이선스가 필요합니다. 스마트 라이선싱 포털에서 내보내기 제어 기능이 활성화되어 있는지 확인
- 문제를 해결하려면 새 사용자/자격 증명으로 시도할 수 있습니다

- 암호화를 사용하는 경우 <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html#anc59>에 설명된 대로 SNMPv3 트래픽의 암호를 해독하고 페이로드를 확인할 수 있습니다.
- 소프트웨어가 다음과 같은 결함의 영향을 받는 경우 암호화에 AES128을 고려해 보십시오.
- Cisco 버그 ID [CSCvy27283](#)



ASA/FTD SNMPv3 폴링은 프라이버시 알고리즘 AES192/AES256을 사용하여 실패할 수 있습니다.

Cisco 버그 ID [CSCvx45604](#)



인증 sha 및 priv aes 192를 사용하는 사용자의 Snmpv3 walk 실패

---

 참고: 알고리즘 불일치로 인해 SNMPv3가 실패할 경우 show 출력이 표시되고 로그에 명확한 내용이 표시되지 않습니다

---

```

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'

### SNMPv3 폴링 고려 사항 - 고객 사례

#### 1. SNMPv3 snmpwalk - 작동 시나리오

<#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

캡처(snmpwalk)에는 각 패킷에 대한 응답이 표시됩니다.

```

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

```

캡처 파일에는 비정상적인 내용이 표시되지 않음:

```

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

```

## 2. SNMPv3 snmpwalk - 암호화 실패

힌트 #1: 시간 초과가 있습니다.

<#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

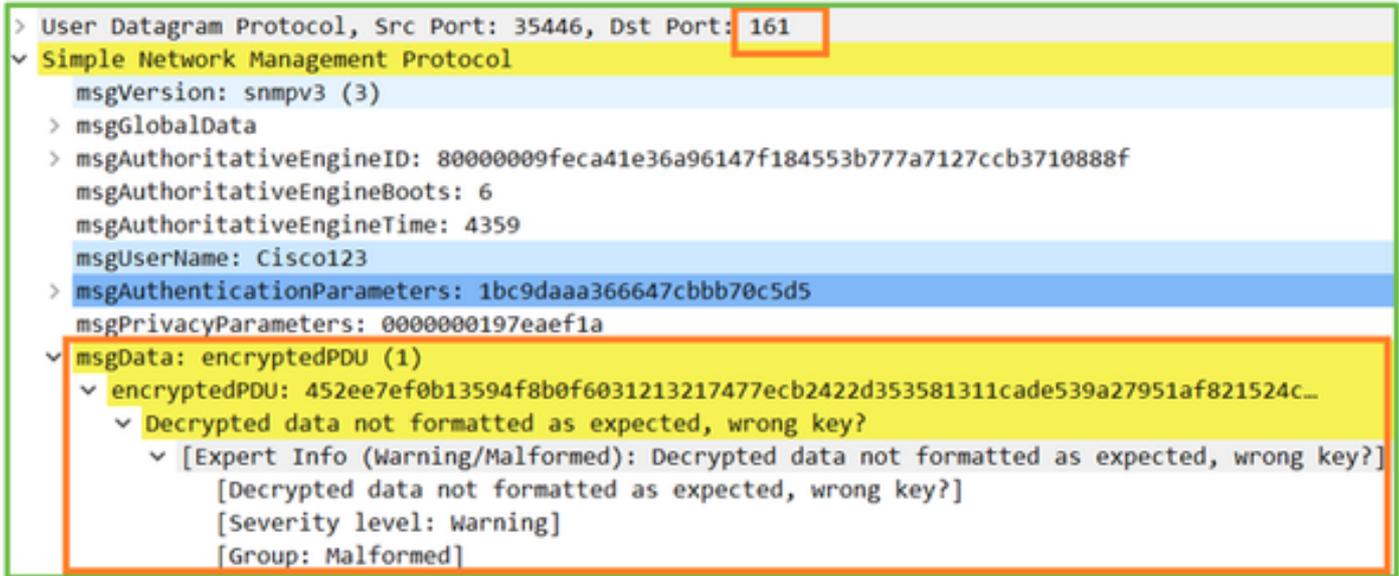
힌트 #2: 많은 요청과 1개의 응답이 있습니다.

```

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

```

힌트 #3: Wireshark 암호 해독 실패:



힌트 #4. ma\_ctx2000.log 파일에서 'error parsing ScopedPDU' 메시지를 확인합니다.

<#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
```

ScopedPDU를 구문 분석하는 오류는 암호화 오류에 대한 강력한 힌트입니다. ma\_ctx2000.log 파일은 SNMPv3에 대한 이벤트만 표시합니다.

### 3. SNMPv3 snmpwalk – 인증 실패

힌트 #1: 인증 실패

<#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)
```

힌트 #2: 많은 요청과 응답이 있습니다.

```
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
```

힌트 #3: Wireshark 형식이 잘못된 패킷

```
> 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]
```

힌트 #4. ma\_ctx2000.log 파일에서 'Authentication failed'(인증 실패) 메시지를 확인합니다.

```
<#root>
```

```
>
```

```
expert
```

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

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

```
Authentication failed for Cisco123
Authentication failed for Cisco123
```

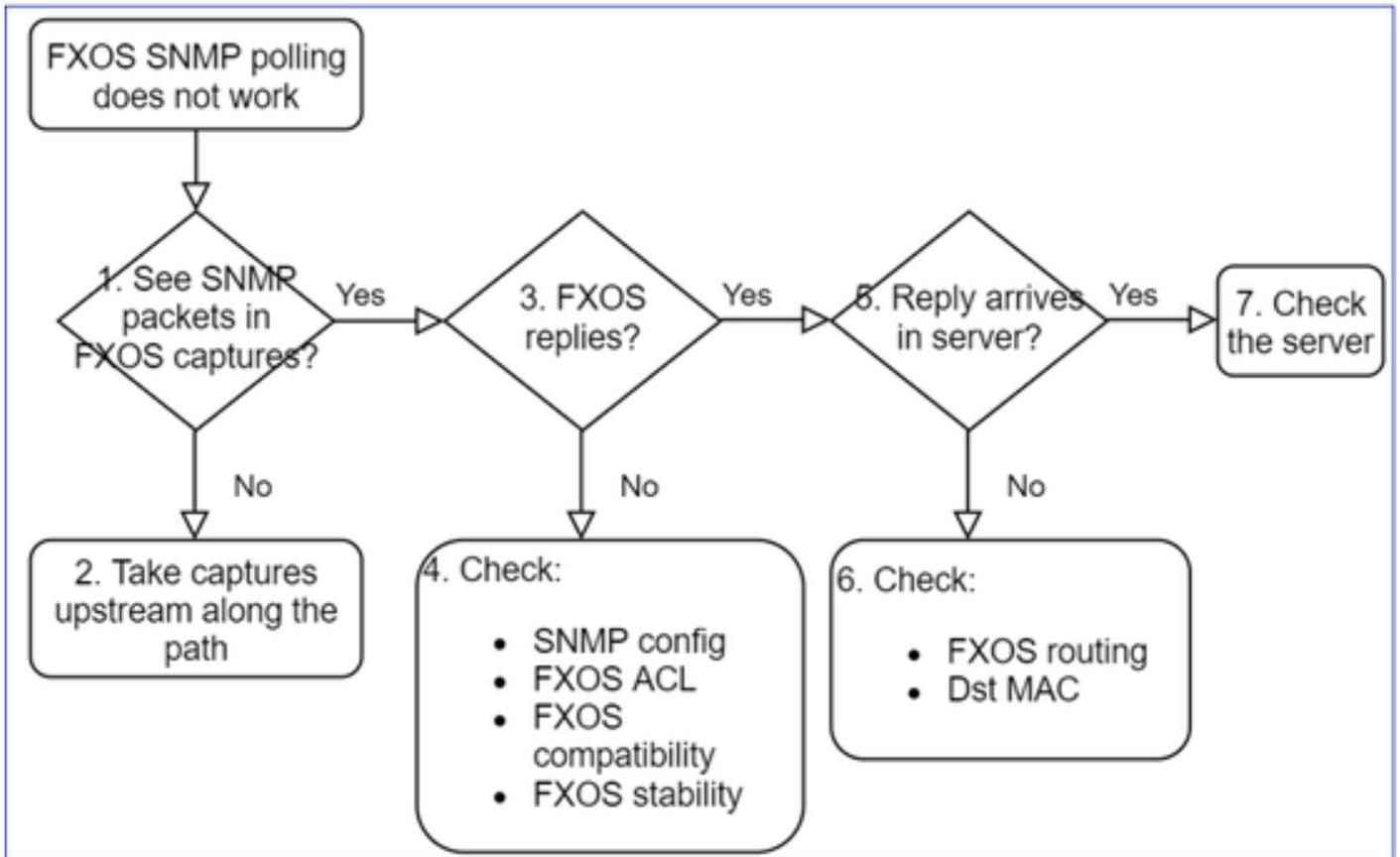
## FXOS SNMP를 폴링할 수 없음

문제 설명(실제 Cisco TAC 케이스의 샘플):

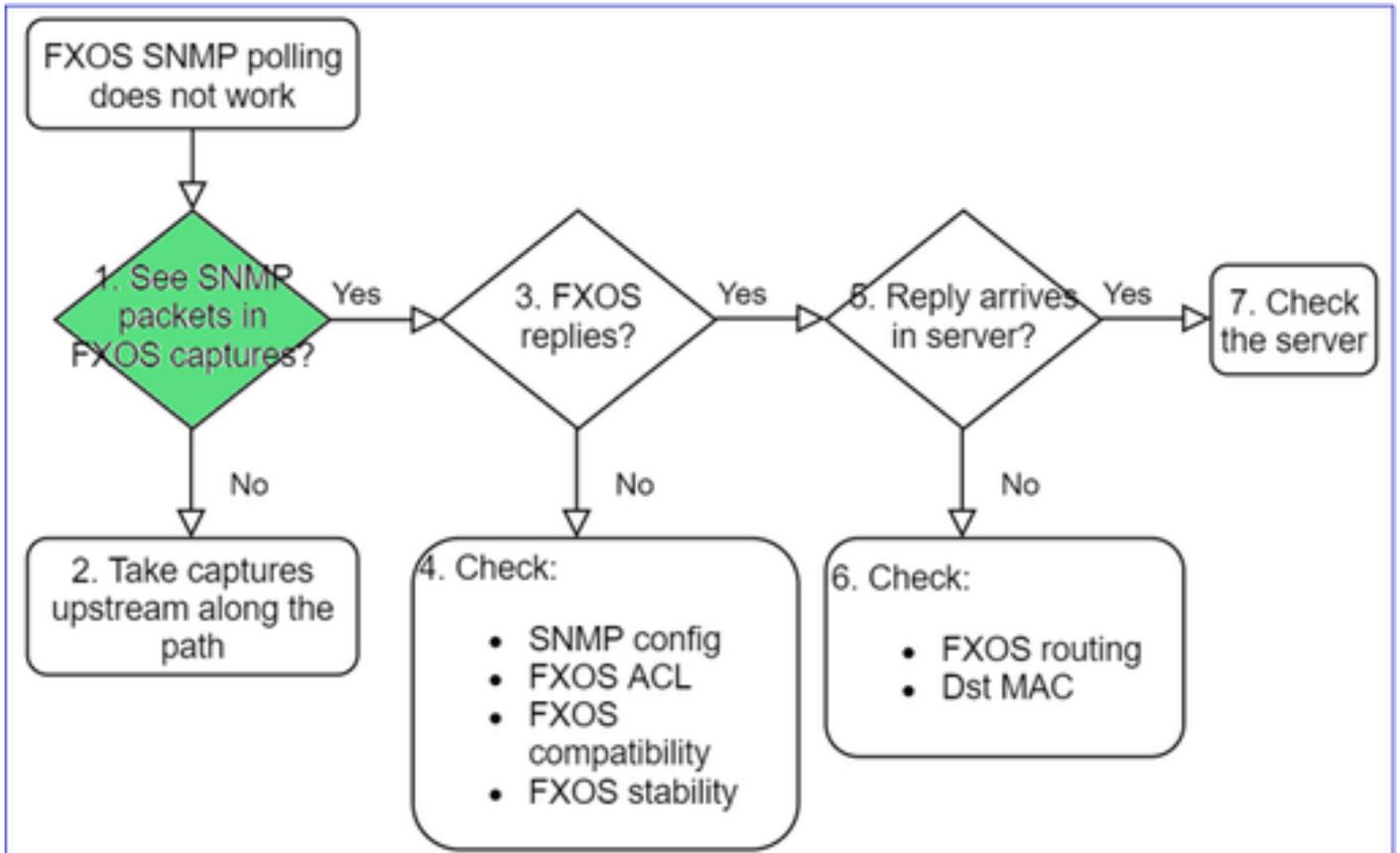
- "SNMP에서 FXOS에 대해 잘못된 버전을 제공합니다. FXOS 버전용 SNMP로 폴링할 경우 출력을 이해하기가 어렵습니다."
- "FXOS FTD4115에서 SNMP 커뮤니티를 설정할 수 없습니다."
- "대기 방화벽에서 FXOS를 2.8에서 2.9로 업그레이드한 후 SNMP를 통해 정보를 수신하려고 하면 시간 초과가 발생합니다."
- "snmpwalk는 9300 FXOS에서 실패하지만 동일한 버전의 4140 FXOS에서 작동합니다. 연결성 및 커뮤니티는 문제가 되지 않습니다."
- "FPR4K FXOS에 25개의 SNMP 서버를 추가하려고 하지만 그렇게 할 수 없습니다."

## 권장 문제 해결

FXOS SNMP 폴링 문제에 대한 순서도 문제를 해결하기 위한 프로세스입니다.



1. FXOS 캡처에 SNMP 패킷이 표시됩니까?



FPR1xxx/21xx

- FPR1xxx/21xx에는 새시 관리자(어플라이언스 모드)가 없습니다.
- 관리 인터페이스에서 FXOS 소프트웨어를 폴링할 수 있습니다.

<#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/93xx의 경우에는 EthAnalyzer CLI 툴을 사용하여 새시를 캡처합니다.

```
<#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)#
```

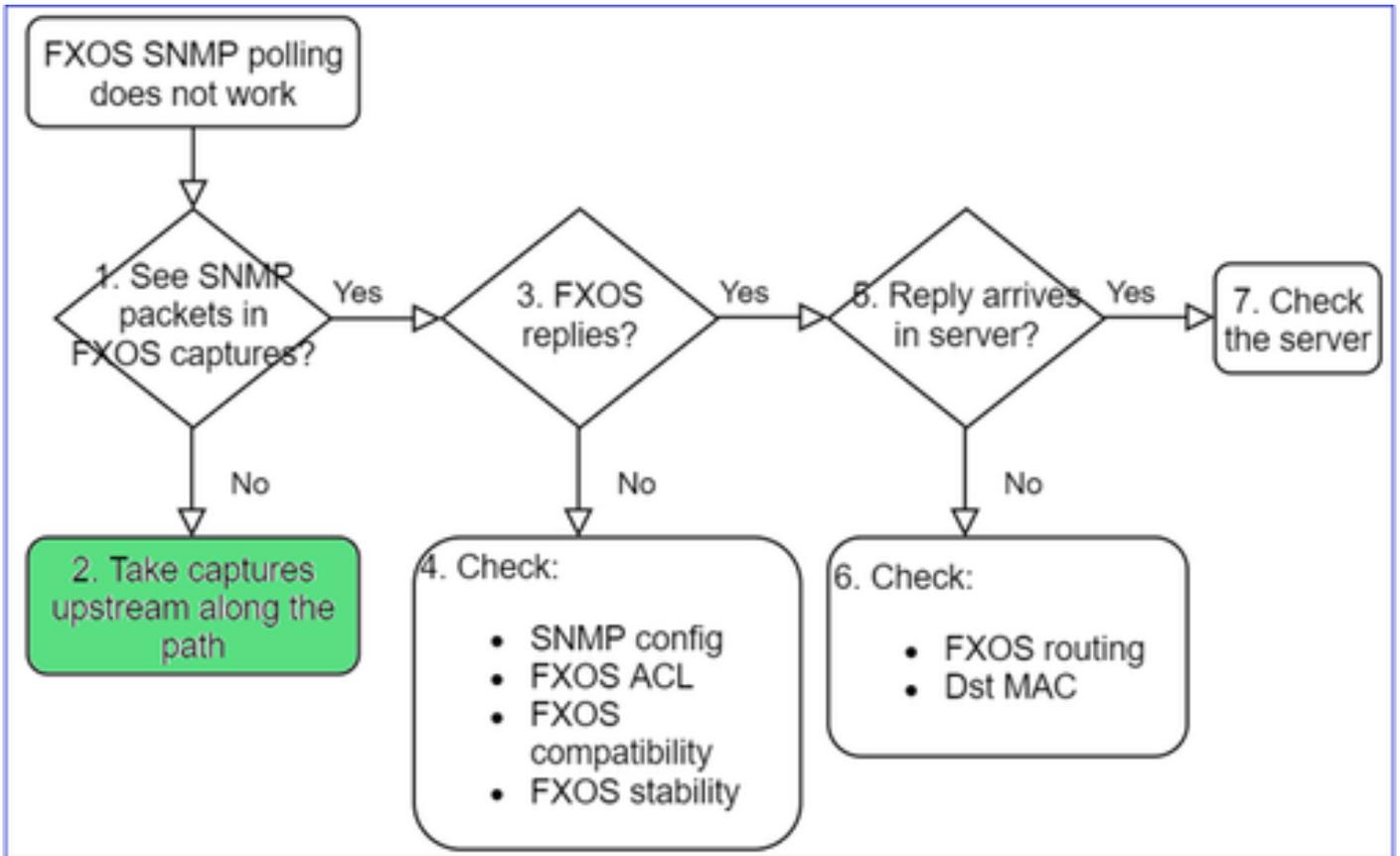
```
dir
```

```
1
```

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

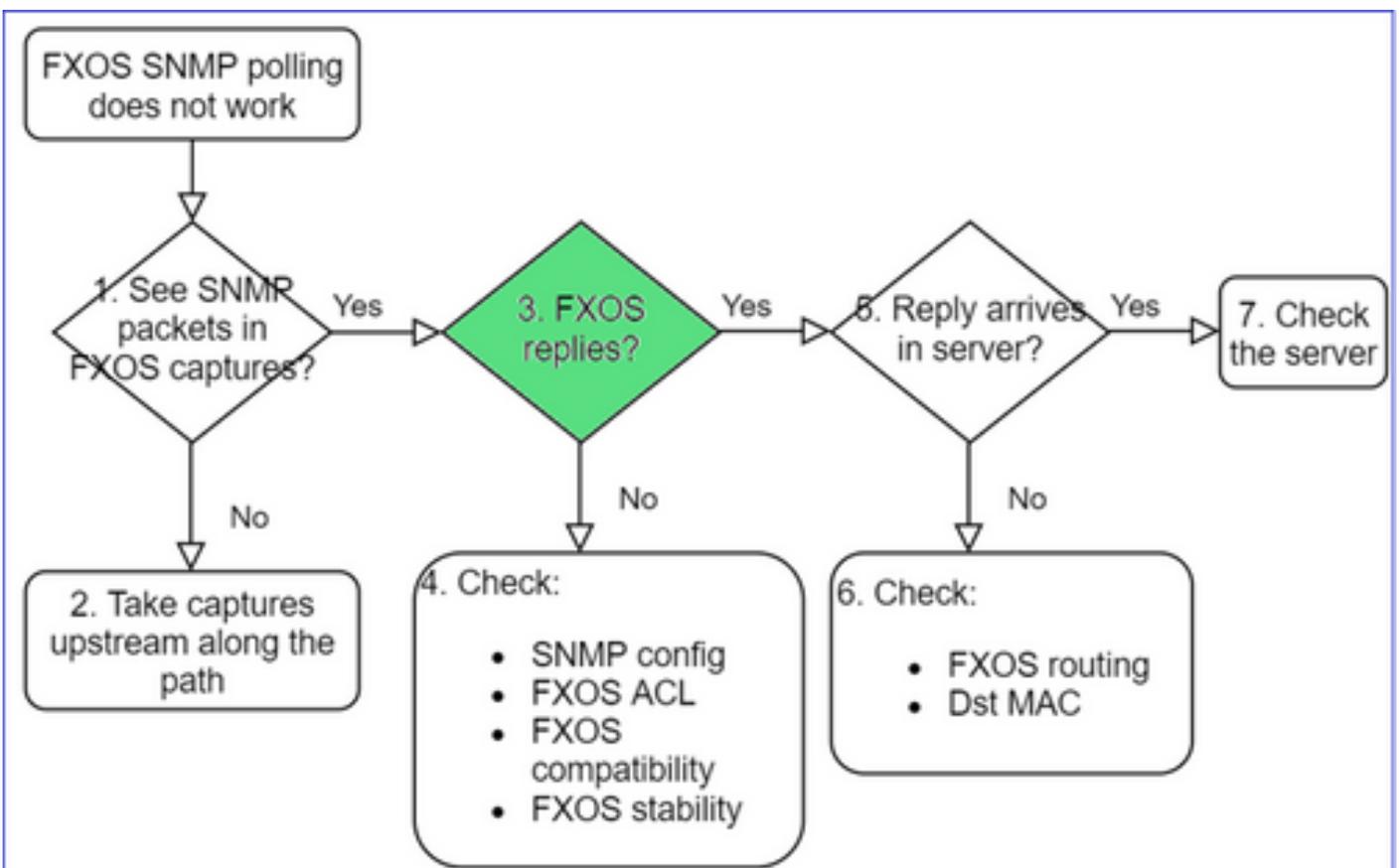
```
copy workspace:///SNMP.pcap ftp://ftp@192.0.2.100/SNMP.pcap
```

2. FXOS 캡처에 패킷이 없습니까?



- 경로를 따라 업스트림 캡처 수행

### 3. FXOS 응답?



- 작동 시나리오:

<#root>

>

capture-traffic

...

Options:

-n host 192.0.2.23 and udp port 161

HS\_PACKET\_BUFFER\_SIZE is set to 4.

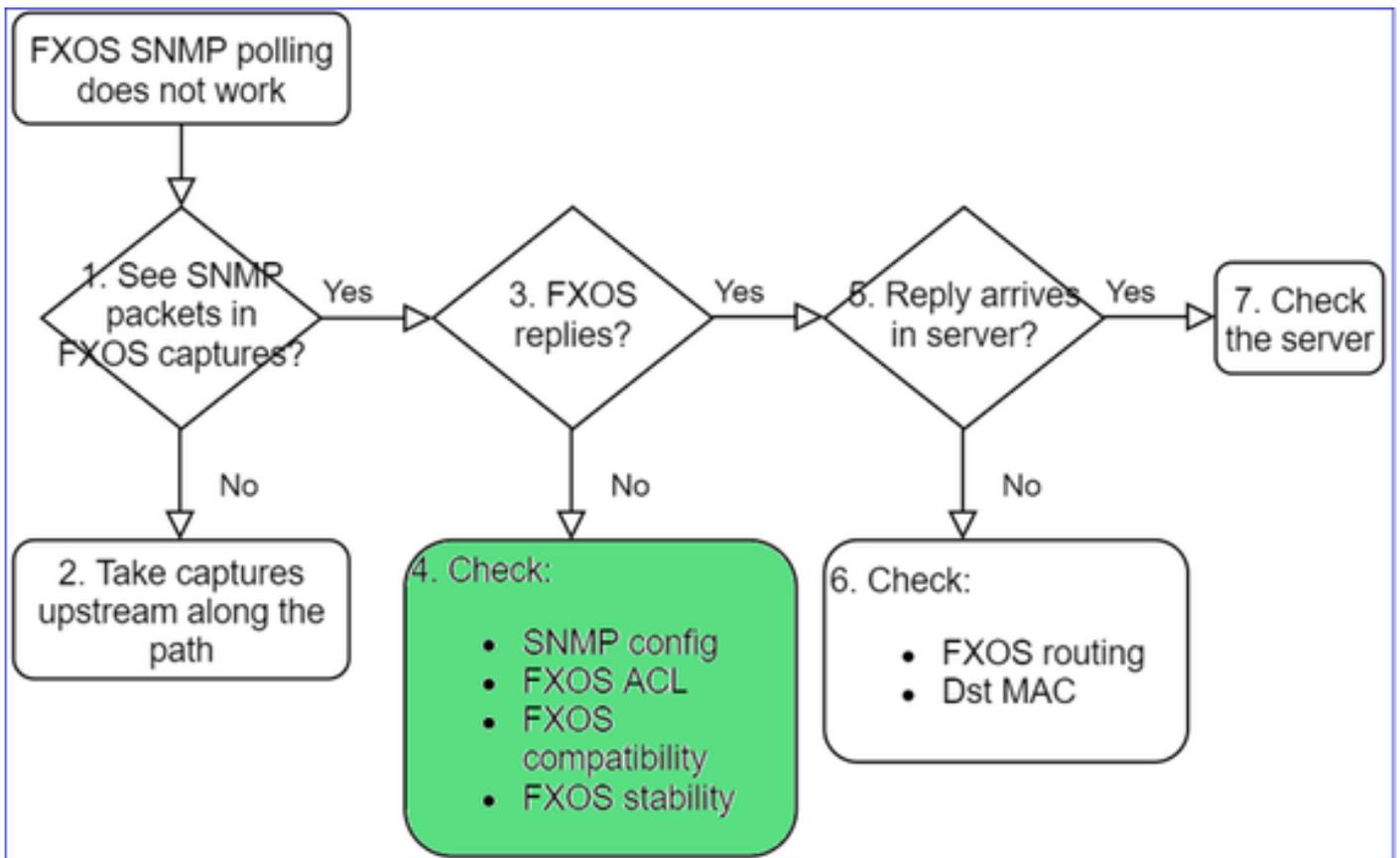
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

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. FXOS가 응답하지 않음



추가 확인

- UI 또는 CLI에서 SNMP 구성 확인:

<#root>

```
firepower#
scope monitoring

firepower /monitoring #
show snmp

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

- 특수 문자(예: '\$')에 주의:

```
<#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		

- SNMPv3의 경우 show snmp-user [detail] 사용
- FXOS 호환성 확인

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id\\_59069](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#id_59069)

#### 4. FXOS가 응답하지 않는 경우

FXOS SNMP 카운터 확인:

```

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

```

• FXOS ACL(Access Control List)을 확인합니다. 이는 FPR41xx/9300 플랫폼에만 적용됩니다. 트래픽이 FXOS ACL에 의해 차단된 경우, 요청이 표시되지만 회신은 표시되지 않습니다.

<#root>

firepower(fxos)#

ethalyzer local interface mgmt capture-filter

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

Capturing on 'eth0'

```

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

```

UI(User Interface)에서 FXOS ACL을 확인할 수 있음:

CLI에서 FXOS ACL을 확인할 수도 있습니다.

```
<#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 디버그(패킷만). FPR41xx/9300에만 해당:

```
<#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)(디버그 SNMP(모두)) - 이 디버그 출력은 매우 자세한 정보입니다.

```
<#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 관련 FXOS 결함이 있는지 확인:

```
<#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 core가 있는지 확인:

```
FPR41xx/FPR9300:
```

```
<#root>
```

```
firepower#
```

```
connect local-mgmt
```

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

```
dir cores
```

```
1 1983847 Apr 01 17:26:40 2021 core.snmpd.10012.1585762000.gz
```

```
1 1984340 Apr 01 16:53:09 2021 core.snmpd.10018.1585759989.gz
```

```
FPR1xxx/21xx:
```

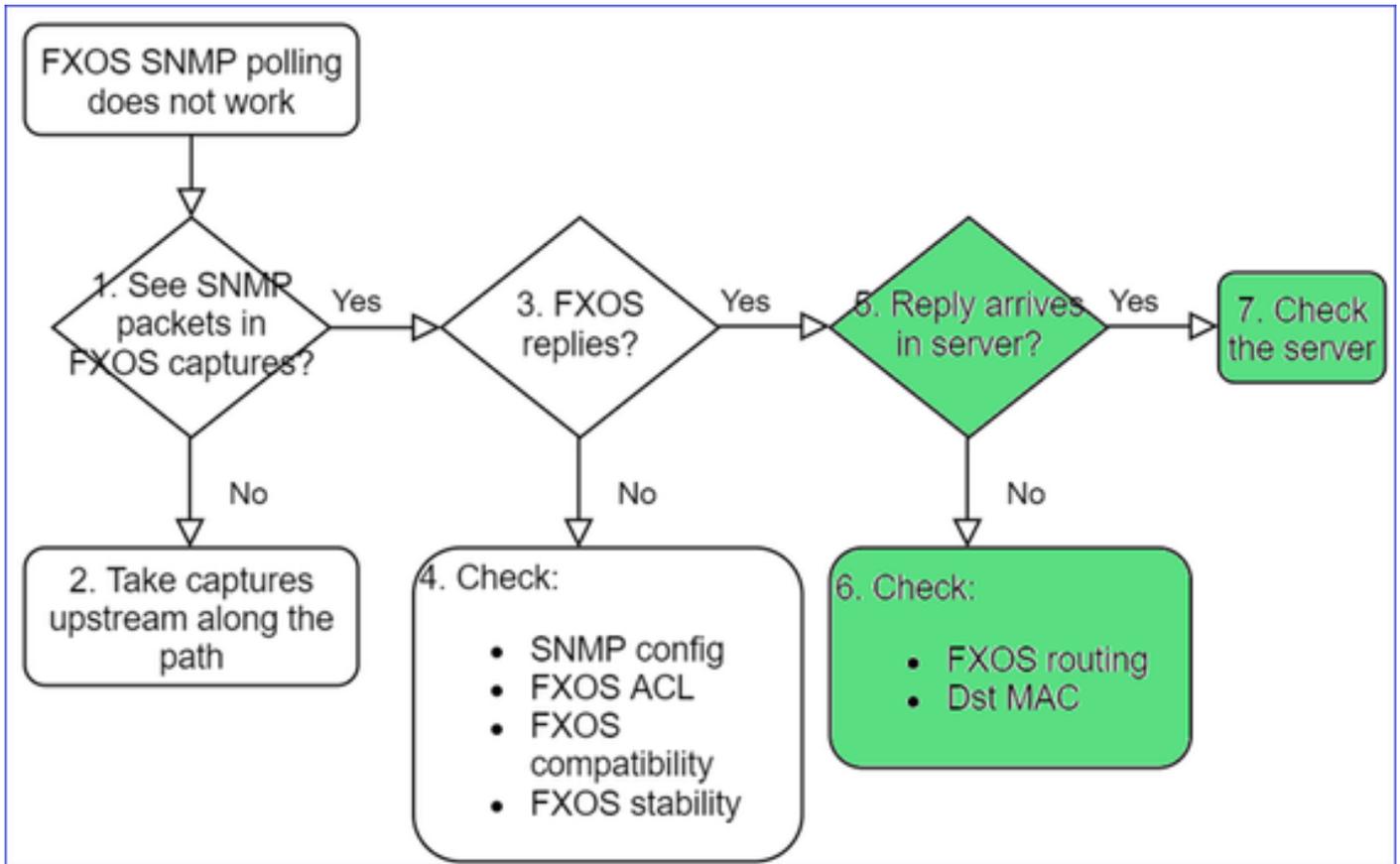
```
<#root>
```

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

```
dir cores_fxos
```

snmpd core가 보이면 FXOS 문제 해결 번들과 함께 core를 수집하고 Cisco TAC에 문의하십시오.

5. SNMP 응답이 SNMP 서버에 도착합니까?



- FXOS 라우팅 확인

이 출력은 FPR41xx/9300의 출력입니다.

<#root>

firepower#

show fabric-interconnect

Fabric Interconnect:

ID	OOB IP Addr	OOB Gateway	OOB Netmask	OOB IPv6 Address	OOB IPv6 Gateway	Prefix	Operational
A	192.168.2.37	192.168.2.1	10.255.255.128 ::	::		64	Operable

- 캡처를 수행하고 pcap을 내보내고 회신의 대상 MAC을 확인합니다.
- 마지막으로 SNMP 서버(캡처, 구성, 애플리케이션 등)를 확인합니다.

어떤 SNMP OID 값을 사용해야 합니까?

문제 설명(실제 Cisco TAC 케이스의 샘플):

- "Cisco Firepower 장비를 모니터링해야 합니다. 각 코어 CPU, 메모리, 디스크에 대한 SNMP OID를 제공하십시오."
- "ASA 5555 디바이스에서 전력 공급 장치의 상태를 모니터링하는 데 사용할 수 있는 OID가 있

습니까?"

- "FPR 2K 및 FPR 4K에서 새시 SNMP OID를 가져오려고 합니다."
- "ASA ARP 캐시를 폴링하려고 합니다."
- "BGP 피어 중단에 대한 SNMP OID를 알아야 합니다."

## SNMP OID 값을 찾는 방법

이 문서에서는 Firepower 디바이스의 SNMP OID에 대한 정보를 제공합니다.

- Cisco FTD(Firepower Threat Defense) SNMP 모니터링 백서:

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

- Cisco Firepower 4100/9300 FXOS MIB 참조 가이드:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b\\_FXOS\\_4100\\_9300\\_MIBRef.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/mib/b_FXOS_4100_9300_MIBRef.html)

- FXOS 플랫폼에서 특정 OID를 검색하는 방법:

<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(ASA/LINA)에서 SNMP OID 확인

```
<#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
```

- OID에 대한 자세한 내용은 SNMP 개체 탐색기를 확인하십시오.

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

- FXOS(41xx/9300) CLI에서 다음 2개의 명령을 실행:

<#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

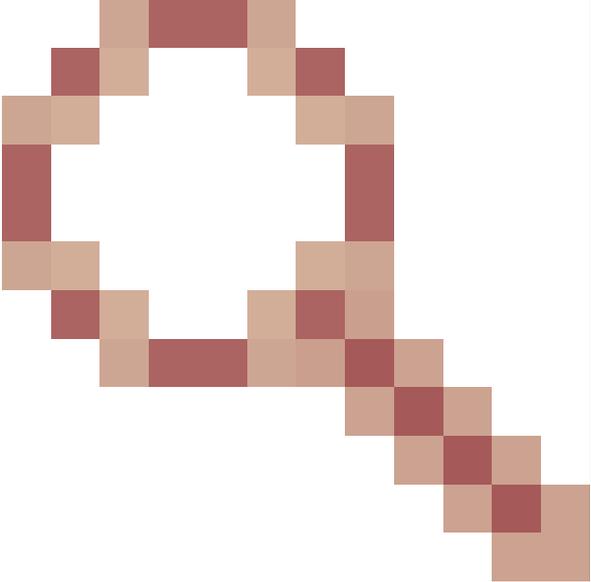
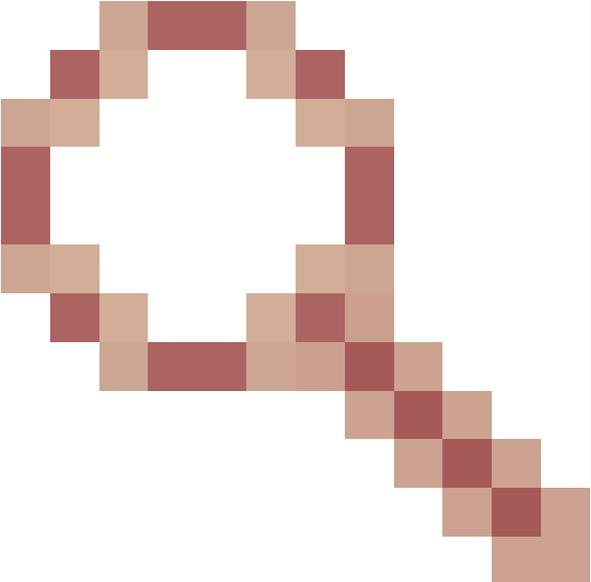
1.0.88010.1.1.1.1.1.1.1 ieee8021paeMIB

1.0.88010.1.1.1.1.1.1.2

...

## 공통 OID 빠른 참조

요건	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)
메모리(LINA)	1.3.6.1.4.1.9.9.221.1.1
메모리(Linux/FMC)	1.3.6.1.1.4.1.2021.4
HA 정보	1.3.6.1.4.1.9.9.491.1.4.2
클러스터 정보	1.3.6.1.4.1.9.9.491.1.8.1
VPN 정보	RA-VPN Num 세션: 1.3.6.1.4.1.9.9.392.1.3.1(7.x) RA-VPN 번호 사용자: 1.3.6.1.4.1.9.9.392.1.3.3(7.x) RA-VPN Num Peak 세션: 1.3.6.1.4.1.9.9.392.1.3.41(7.x)

	<p>S2S VPN 번호 세션: 1.3.6.1.4.1.9.9.392.1.3.29</p> <p>S2S VPN Num Peak 세션: 1.3.6.1.4.1.9.9.392.1.3.31</p> <p>- 팁: firepower# show snmp-server oid   아이케</p>
<p>BGP 상태</p>	 <p>ENH Cisco 버그 ID <a href="#">CSCux13512</a> :SNMP 폴링을 위한 BGP MIB 추가</p>
<p>FPR1K/2K ASA/ASAv 스마트 라이선싱</p>	 <p>ENH Cisco 버그 ID <a href="#">CSCvv83590</a> : FPR1k/2k의 ASAv/ASA: Smart Licensing 상태 추적을 위한 SNMP OID 필 요</p>
<p>FXOS 레벨 포트 채 널용 Lina SNMP OID</p>	<p>ENH Cisco 버그 ID <a href="#">CSCvu91544</a></p>

:FXOS 레벨 포트 채널 인터페이스 통계를 위한 Lina SNMP OID 지원

FMC 7.3 추가(FMC 1600/2600/4600 이상)

요건	OID
팬 상태 트랩	트랩 OID: 1.3.6.1.4.1.9.9.117.2.0.6 값 OID: 1.3.6.1.4.1.9.9.117.1.4.1.1.<index> 0 - 팬이 실행되지 않음 1 - 팬이 실행 중입니다.
CPU/PSU 온도 트랩	트랩 OID: 1.3.6.1.4.1.9.9.91.2.0.1 임계값 OID: 1.3.6.1.4.1.9.9.91.1.2.1.1.4.<index>.1 값 OID: 1.3.6.1.4.1.9.9.91.1.1.1.4.<index>

PSU 상태 트랩	트랩 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.<인덱스> AdminStatus OID: 1.3.6.1.4.1.9.9.117.1.1.2.1.1.<인덱스>  0 - 전원 공급 장치 프레즌스가 감지되지 않음  1 - 전원 공급 장치 프레즌스 감지, 확인
-----------	--

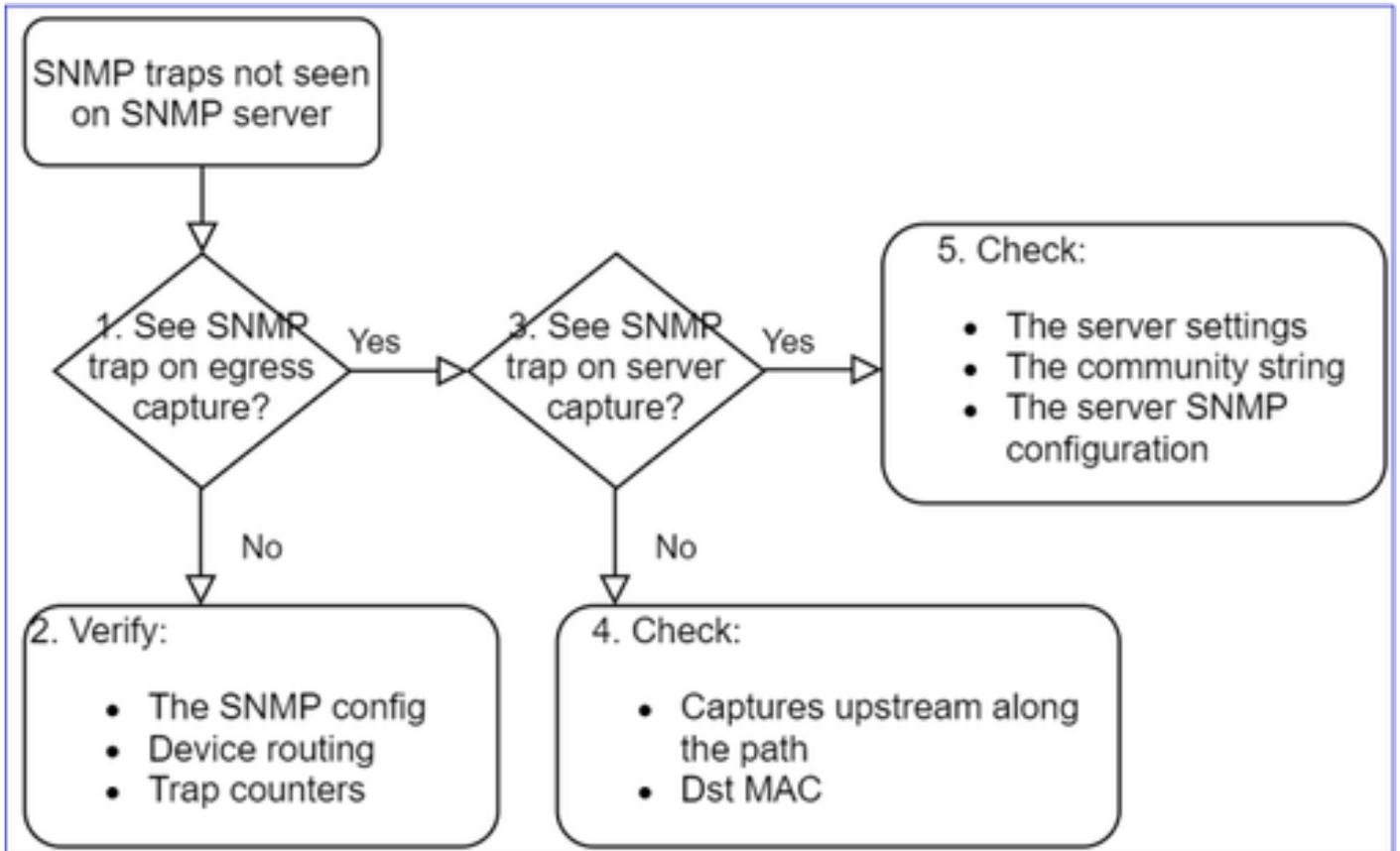
## SNMP 트랩을 가져올 수 없음

문제 설명(실제 Cisco TAC 케이스의 샘플):

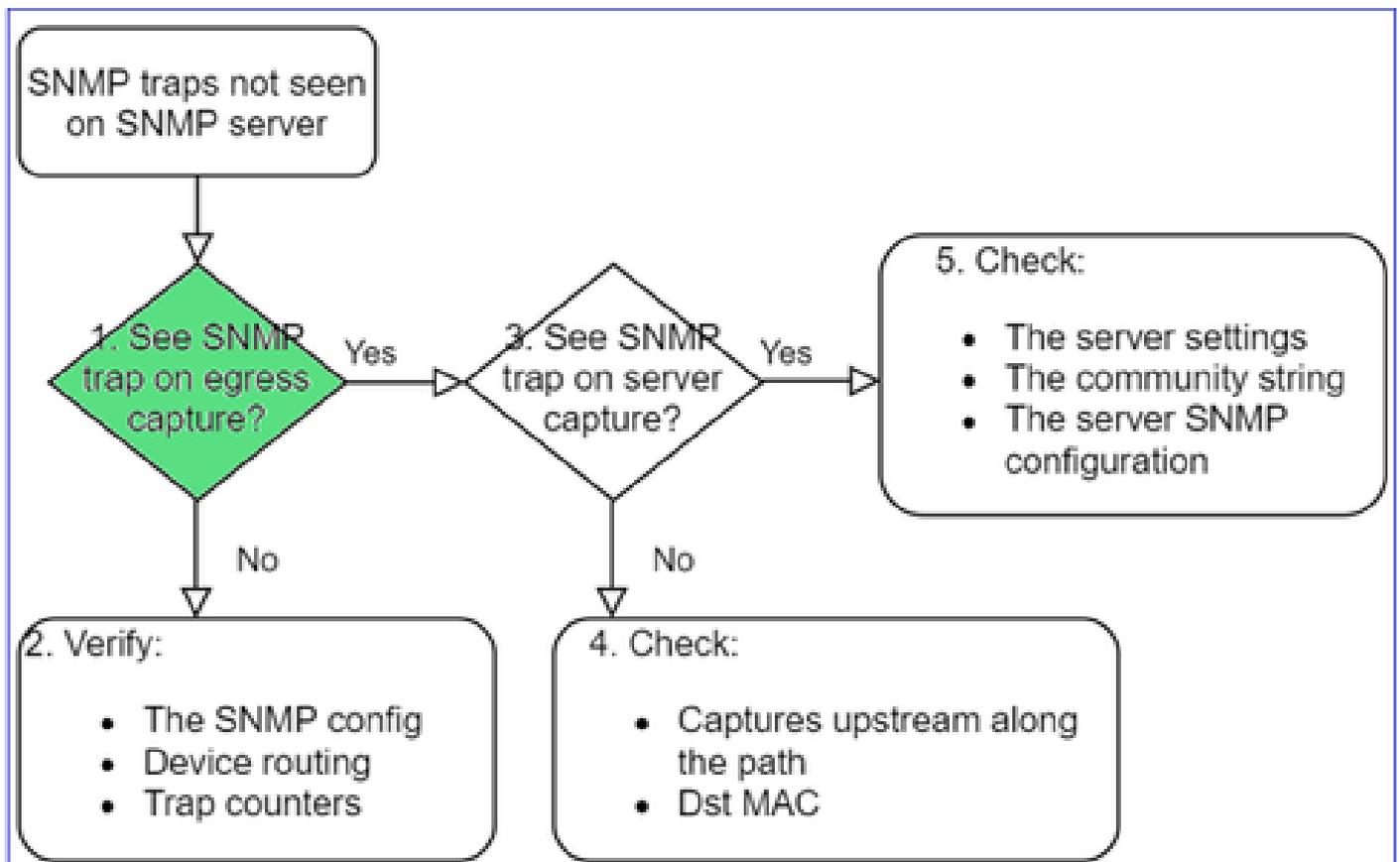
- "FTD의 SNMPv3가 SNMP 서버에 트랩을 보내지 않습니다."
- "FMC 및 FTD가 SNMP 트랩 메시지를 보내지 않습니다."
- "FXOS용 FTD 4100에서 SNMP를 구성했으며 SNMPv3 및 SNMPv2를 시도했지만 둘 다 트랩을 보낼 수 없습니다."
- "Firepower SNMP가 트랩을 모니터링 톨에 보내지 않습니다."
- "Firewall FTD는 SNMP 트랩을 NMS로 보내지 않습니다."
- "SNMP 서버 트랩이 작동하지 않습니다."
- "FXOS용 FTD 4100에서 SNMP를 구성했으며 SNMPv3 및 SNMPv2를 시도했지만 둘 다 트랩을 보낼 수 없습니다."

## 권장 문제 해결

firepower SNMP 트랩 문제에 대한 순서도를 트러블슈팅하기 위한 프로세스입니다.



1. 이그레스 캡처에 SNMP 트랩이 표시됩니까?



관리 인터페이스에서 LINA/ASA 트랩을 캡처:

<#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

데이터 인터페이스에서 LINA/ASA 트랩을 캡처:

<#root>

firepower#

capture SNMP interface net208 match udp any any eq 162

FXOS 트랩(41xx/9300)을 캡처:

<#root>

firepower#

connect fxos

firepower(fxos)#

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

1 2021-08-02 11:22:23.661436002 10.62.184.9 → 10.62.184.23 SNMP 160 snmpV2-trap 10.3.1.1.2.1.1.3.0 10.3.1.1.1.2.1.1.3.0

firepower(fxos)#

exit

firepower#

connect local-mgmt

firepower(local-mgmt)#

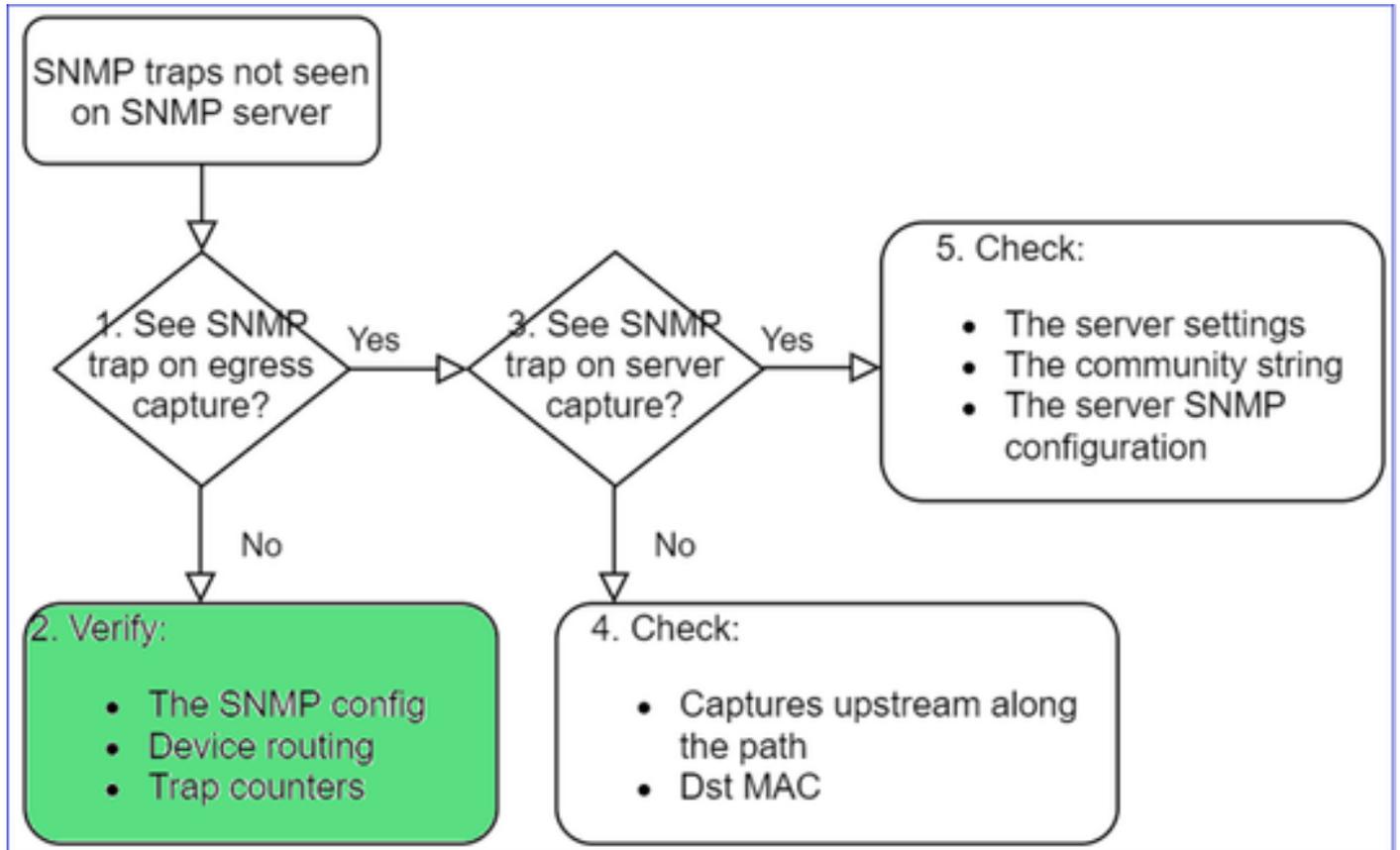
dir

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. 이그레스 인터페이스에 패킷이 표시되지 않는 경우



<#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 트랩 구성:

<#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

참고: 1xxx/21xx에서는 Devices(디바이스) > Device Management(디바이스 관리) > SNMP config(SNMP 컨피그레이션)의 경우에만 이러한 설정이 표시됩니다.

- 관리 인터페이스를 통한 트랩에 대한 LINA/ASA 라우팅:

```
<#root>
```

```
>
```

```
show network
```

- 데이터 인터페이스를 통한 트랩에 대한 LINA/ASA 라우팅:

```
<#root>
```

```
firepower#
```

```
show route
```

- FXOS 라우팅(41xx/9300):

```
<#root>
```

```
FP4145-1#
```

```
show fabric-interconnect
```

- 트랩 카운터(LINA/ASA):

```
<#root>
```

```
firepower#
```

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

```
20 Trap PDUs
```

FXOS:

```
<#root>
```

```
FP4145-1#
```

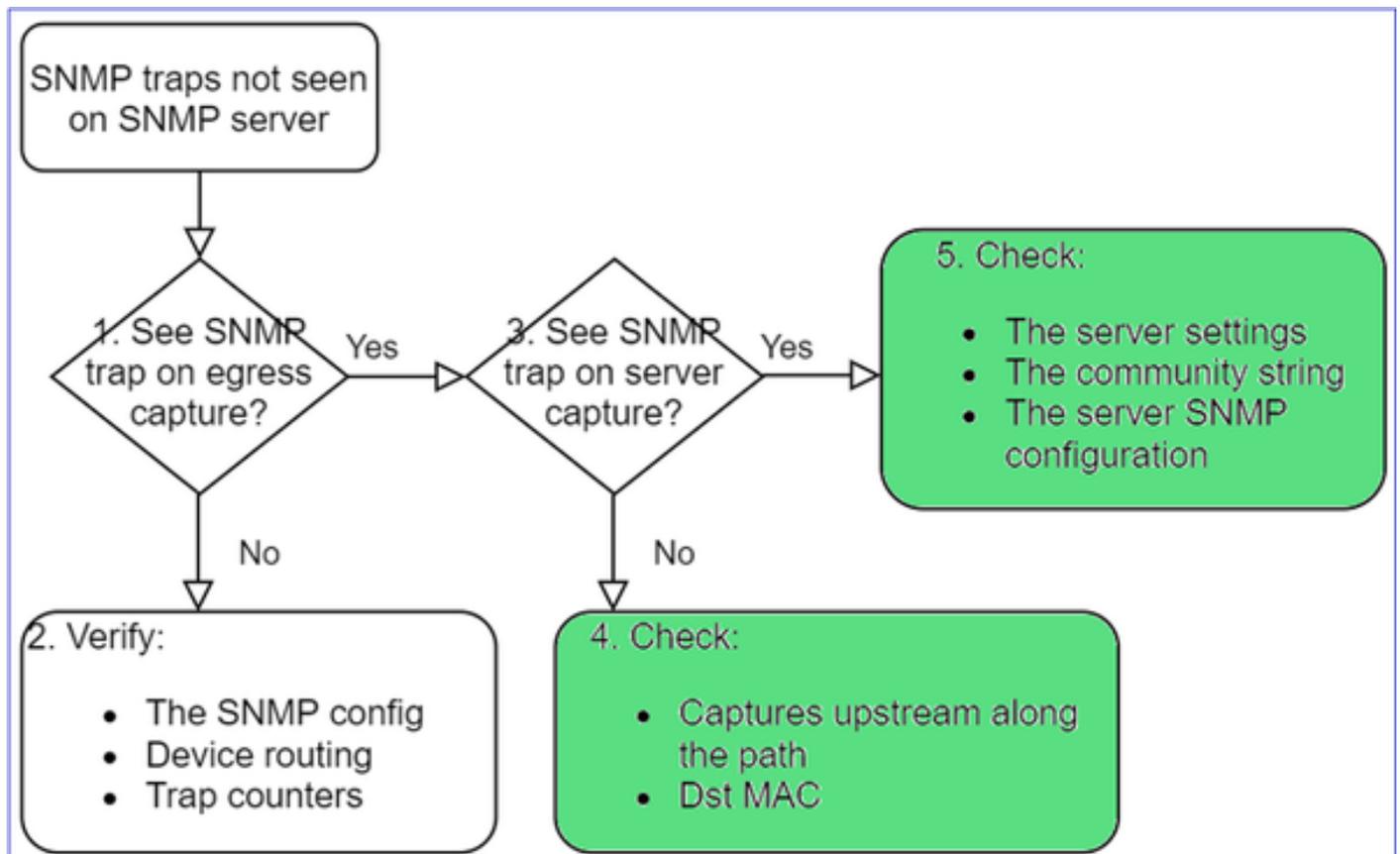
```
connect fxos
```

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

```
show snmp | grep Trap
```

```
1296 Out Traps PDU
```

추가 확인



- 대상 SNMP 서버에서 캡처 수행.

기타 확인 사항:

- 경로를 따라 캡처.
- SNMP 트랩 패킷의 대상 MAC 주소.
- SNMP 서버 설정 및 상태(예: 방화벽, 열린 포트 등).
- SNMP 커뮤니티 문자열.
- SNMP 서버 구성.

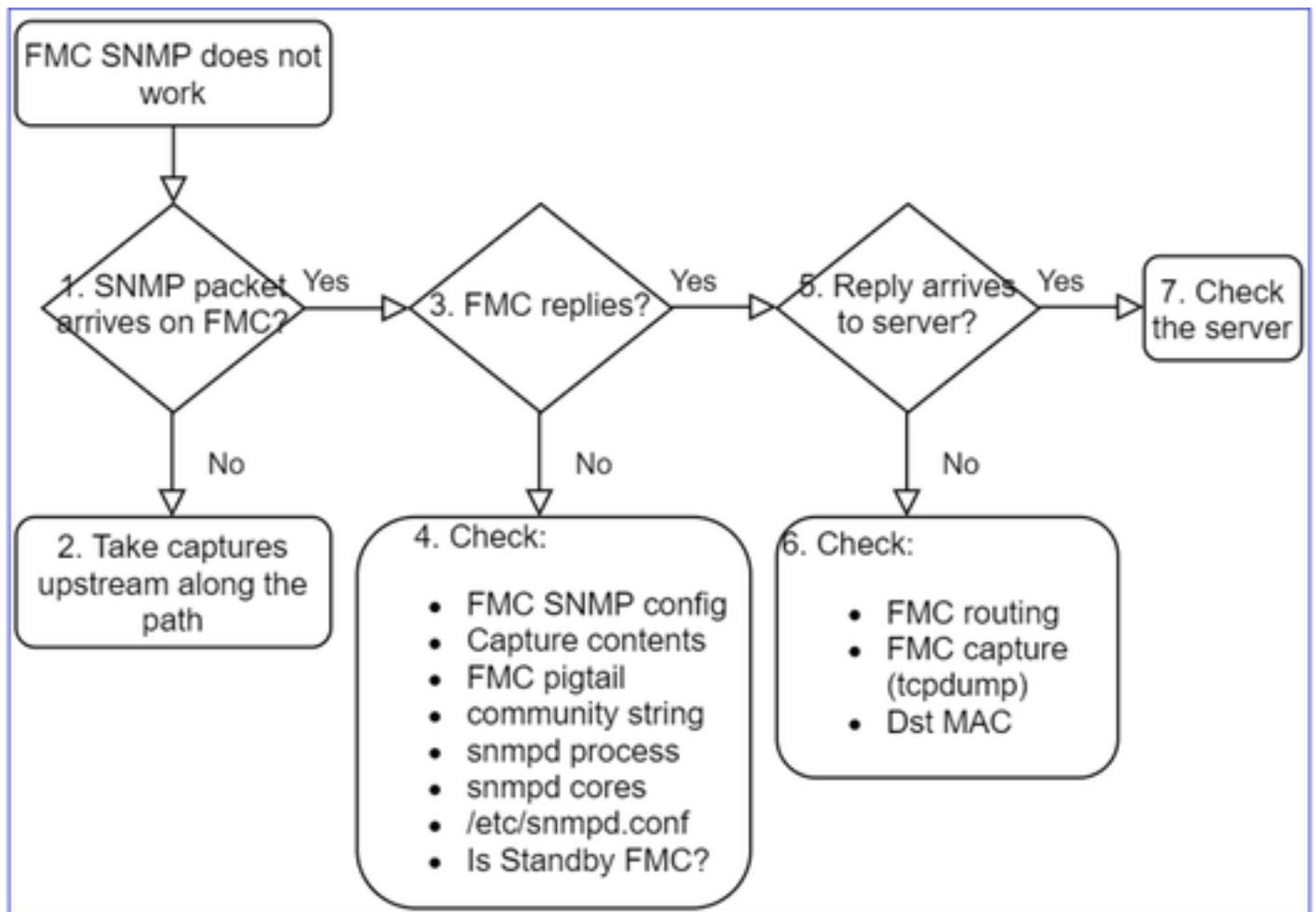
## SNMP를 통해 FMC를 모니터링할 수 없음

문제 설명(실제 Cisco TAC 케이스의 샘플):

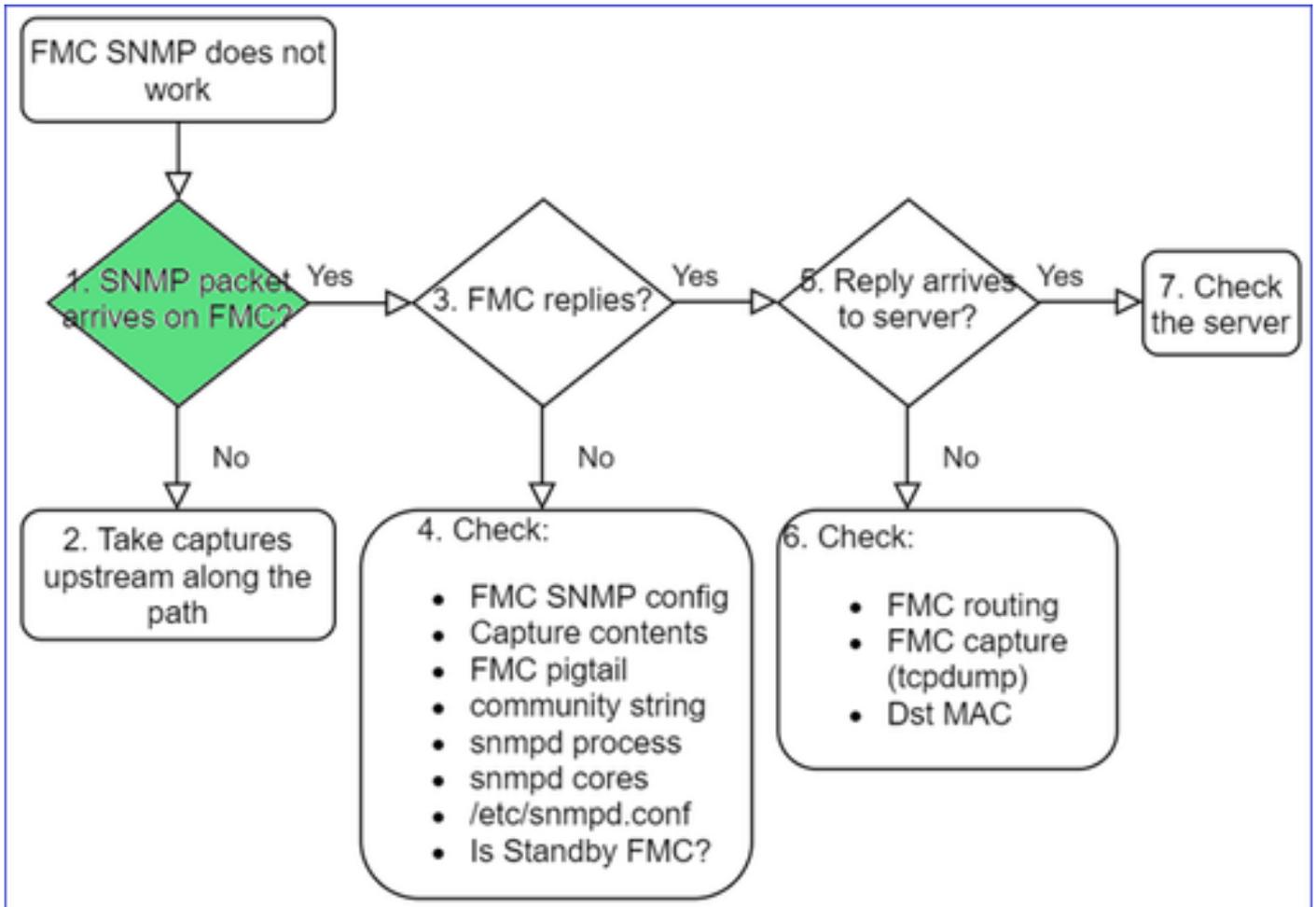
- "SNMP가 대기 FMC에서 작동하지 않습니다."
- "FMC 메모리를 모니터링해야 합니다."
- "대기 192.168.4.0.8 FMC에서 SNMP가 작동해야 합니까?"
- "CPU, 메모리 등의 리소스를 모니터링하도록 FMC를 구성해야 합니다."

문제 해결 방법

FMC SNMP 문제에 대한 순서도를 트러블슈팅하는 프로세스입니다.



1. SNMP 패킷이 FMC에 도착합니까?



- FMC 관리 인터페이스에서 캡처:

```
<#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
```



팁: FMC /var/common/ 디렉토리에 캡처를 저장하고 FMC UI에서 다운로드합니다.

```
<#root>
```

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

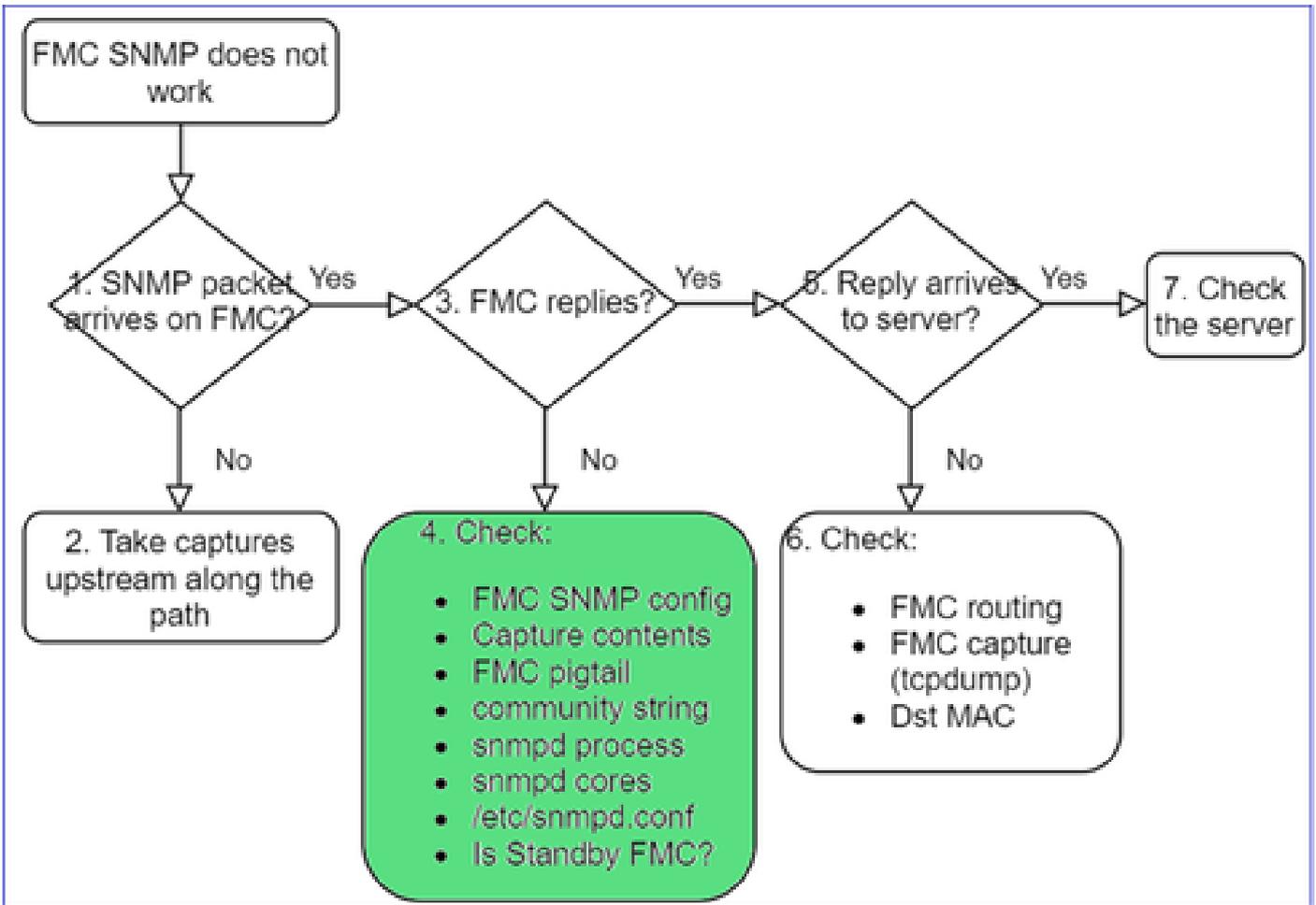
```
sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap
```

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

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

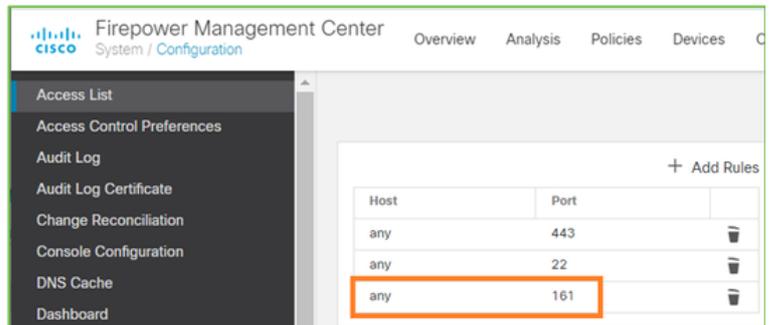
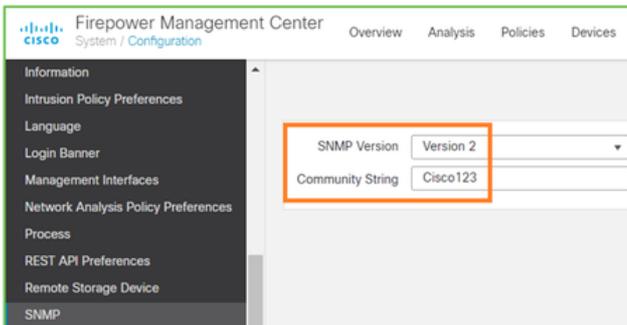
^C46 packets captured  
46 packets received by filter

FMC가 응답합니까?



FMC가 응답하지 않는 경우 확인:

- FMC SNMP 구성(시스템 > 구성)
  1. SNMP 섹션
  2. 액세스 목록 섹션



FMC가 응답하지 않는 경우 확인:

- 캡처(pcap) 콘텐츠

- 커뮤니티 문자열(캡처에서 확인할 수 있음)
- FMC pigtail 출력(오류, 실패, 추적 확인) 및 /var/log/snmpd.log의 콘텐츠
- snmpd 프로세스

<#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 core

<#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.conf의 백엔드 구성 파일:

<#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
```

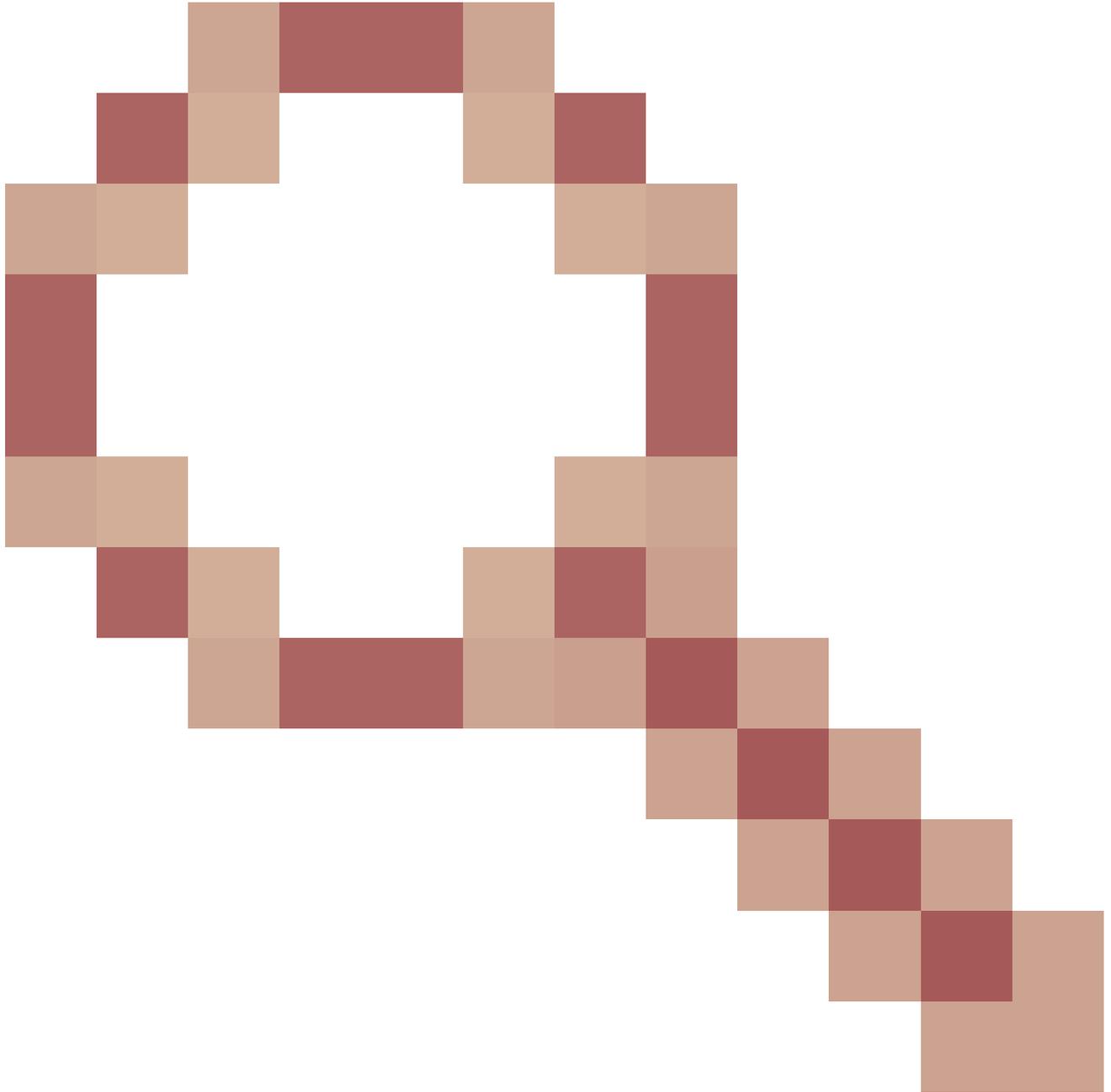


참고: SNMP를 비활성화하면 snmpd.conf 파일이 존재하지 않습니다

---

- 대기 FMC입니까?

6.4.0-9 이전 및 6.0.6.0 이전 버전에서는 대기 FMC가 SNMP 데이터를 전송하지 않습니다 (snmpd가 대기 상태임). 이는 정상적인 동작입니다. 개선 사항 Cisco 버그 ID CSCvs를 [선택합니다](#)



[32303](#)

SNMP를 구성할 수 없음

문제 설명(실제 Cisco TAC 케이스의 샘플):

- "Cisco Firepower Management Center 및 Firepower 4115 Threat Defense에 대해 SNMP를 구성하려고 합니다."
- "FTD에서 SNMP 컨피그레이션 지원"
- "FTD 어플라이언스에서 SNMP 모니터링을 활성화하려고 합니다."
- "FXOS에서 SNMP 서비스를 구성하려고 시도하지만 시스템에서 결국 commit-buffer를 허용하지 않습니다. 오류: 변경이 허용되지 않습니다. 변경하려면 'ftd 연결'을 사용하십시오."
- "FTD 어플라이언스에서 SNMP 모니터링을 활성화하려고 합니다."
- "FTD에서 SNMP를 구성하고 모니터링 중인 디바이스를 검색할 수 없습니다."

SNMP 구성 문제에 접근하는 방법

첫 번째 사항: 문서!

- 최신 설명서를 읽어보십시오!
- FMC 구성 가이드:

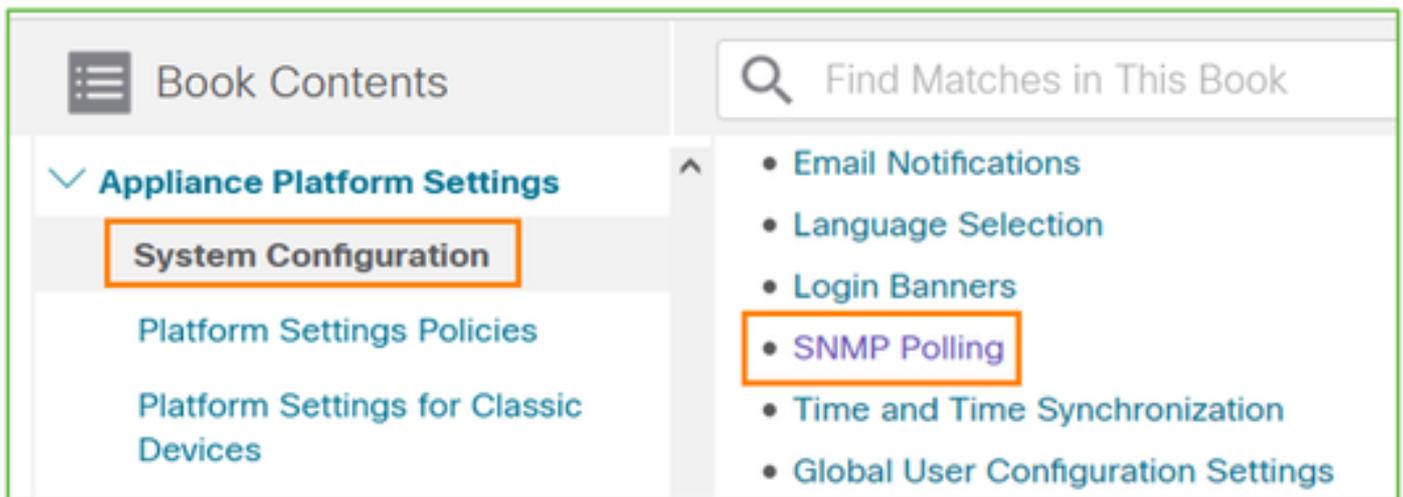
<https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70.html>

- FXOS 구성 가이드:

[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](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)

다양한 SNMP 설명서에 유의하십시오.

FMC SNMP:



FXOS SNMP:

# Cisco Firepower 4100/9300 FXOS Firepower

Book Contents

Find Matches in This Book

Book Title Page

Introduction to the Firepower Security Appliance

Getting Started

License Management for the ASA

User Management

Image Management

Security Certifications Compliance

System Administration

**Platform Settings**

Chapter: Platform Settings

> Chapter Contents

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

Firepower 41xx/9300 SNMP 구성:

✓ Appliance Platform Settings

System Configuration

Platform Settings Policies

Platform Settings for Classic Devices

**Platform Settings for Firepower Threat Defense**

Firepower 1xxx/21xx SNMP 구성:

## Firepower Threat Defense Interfaces and Device Settings

### Interface Overview for Firepower Threat Defense

### Regular Firewall Interfaces for Firepower Threat Defense

### Inline Sets and Passive Interfaces for Firepower Threat Defense

### DHCP and DDNS Services for Threat Defense

### SNMP for the Firepower 1000/2100

## FDM(Firepower Device Manager)의 SNMP 구성

문제 설명(실제 Cisco TAC 케이스의 샘플):

- "FDM을 사용하는 디바이스 Firepower의 SNMPv3에 대한 지침이 필요합니다."
- "SNMP 구성이 FDM의 FPR 2100 디바이스에서 작동하지 않습니다."
- "FDM에서 작동하도록 SNMP v3 구성을 가져올 수 없습니다."
- "FDM 6.7 SNMP 구성 지원."
- "Firepower FDM에서 SNMP v3를 활성화하십시오."

SNMP FDM 구성 문제에 접근하는 방법

- 6.7 이전 버전의 경우 FlexConfig를 사용하여 SNMP 구성을 수행할 수 있습니다.

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

- Firepower 버전 6.7에서와 같이 SNMP 구성은 더 이상 FlexConfig가 아닌 REST API로 구성됩니다.

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

## SNMP 문제 해결 치트 시트

1xxx/21xx/41xx/9300(LINA / ASA) – Cisco TAC에서 케이스를 열기 전에 수집할 사항

명령을 사용합니다	설명
firepower# show run snmp-server	ASA/FTD LINA SNMP 구성 확인.
firepower# show snmp-server statistics	ASA/FTD LINA에서 SNMP 통계를 확인합니다.

	SNMP 패킷 입력 및 SNMP 패킷 출력 카운터에 집중합니다.
> capture-traffic	관리 인터페이스에서 트래픽 캡처.
firepower# capture SNMP-POLL interface net201 trace match udp any any eq 161	UDP 161(SNMP 폴링)에 대한 데이터 인터페이스 (nameif 'net201')에서 트래픽을 캡처합니다.
firepower# capture SNMP-TRAP interface net208 match udp any any eq 162	UDP 162(SNMP 트랩)의 데이터 인터페이스 ('net208'이라고 함)에서 트래픽을 캡처합니다.
firepower# show capture SNMP-POLL packet-number 1 trace	ASA/FTD LINA 데이터 인터페이스에 도착하는 인그레스 SNMP 패킷을 추적합니다.
admin@firepower:~\$ sudo tcpdump -i tap_nlp	NLP(Non-Lina Process) 내부 탭 인터페이스에서 캡처.
firepower# show conn all protocol udp port 161	UDP 161(SNMP 폴링)에서 모든 ASA/FTD LINA 연결을 확인합니다.
firepower# show log   i 302015.*161	SNMP 폴링에 대해 ASA/FTD LINA 로그 302015 확인.
firepower# more system:running-config   i 커뮤니티	SNMP 커뮤니티 문자열 확인.
firepower# debug menu netsnmp 4	SNMP 구성 및 프로세스 ID 확인.
firepower# show asp table classify interface net201 domain permit match port=161	이름이 'net201'인 인터페이스의 SNMP ACL에서 hitcount를 확인합니다.
firepower# show disk0:   i 코어	SNMP core가 있는지 확인.
admin@firepower:~\$ ls -l /var/data/cores	SNMP core가 있는지 확인. FTD에만 적용 가능.
firepower# show route	ASA/FTD LINA 라우팅 테이블 확인.

> show network	FTD 관리 플레인 라우팅 테이블 확인.
admin@firepower:~\$ tail -f /mnt/disk0/log/ma_ctx2000.log	FTD에서 SNMPv3 확인/문제 해결
firepower# debug snmp trace [255] firepower# debug snmp verbose [255] firepower# debug snmp error [255] firepower# debug snmp packet [255]	최신 릴리스에서 숨겨진 명령. 내부 디버그는 Cisco TAC를 사용하여 SNMP 문제를 해결하는 데 유용함.

41xx/9300(FXOS) – Cisco TAC에서 케이스를 열기 전에 수집할 사항

명령을 사용합니다	설명
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 폴링을 위한 FXOS 캡처(UDP 161) 원격 FTP 서버에 업로드 FTP IP: 192.0.2.100 FTP 사용자 이름: 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 트랩을 위한 FXOS 캡처(UDP 162)
firepower# scope system firepower /system # scope services	FXOS ACL 확인

firepower /system/services # show ip-block detail	
firepower# show fault	FXOS 결함 확인
firepower# show fabric-interconnect	FXOS 인터페이스 구성 및 기본 게이트웨이 설정 확인
firepower# connect fxos firepower(fxos)# show running-config snmp all	FXOS SNMP 구성 확인
firepower# connect fxos firepower(fxos)# show snmp internal oids supported create firepower(fxos)# show snmp internal oids supported	FXOS SNMP OID 확인
firepower# connect fxos firepower(fxos)# show snmp	FXOS SNMP 설정 및 카운터 확인
firepower# connect fxos firepower(fxos)# terminal monitor firepower(fxos)# debug snmp pkt-dump firepower(fxos)# debug snmp all	FXOS SNMP 디버그('packets' 또는 'all') 중지하려면 'terminal no monitor' 및 'undebug all' 사용

1xxx/21xx(FXOS) – Cisco TAC에서 케이스를 열기 전에 수집할 사항

명령을 사용합니다	설명
> capture-traffic	관리 인터페이스에서 트래픽 캡처
> show network	FTD 관리 플레인 라우팅 테이블 확인
firepower# scope monitoring firepower /monitoring # show snmp [host]	FXOS SNMP 구성 확인

firepower /monitoring # show snmp-user [detail]	
firepower /monitoring # show snmp-trap	
firepower# show fault	FXOS 결함 확인
firepower# connect local-mgmt	
firepower(local-mgmt)# dir cores_fxos	FXOS core 파일(traceback) 확인
firepower(local-mgmt)# dir cores	

FMC – Cisco TAC에서 케이스를 열기 전에 수집할 사항

명령을 사용합니다	설명
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n	SNMP 폴링에 대해 관리 인터페이스에서 트래픽 캡처
admin@FS2600-2:~\$ sudo tcpdump -i eth0 udp port 161 -n -w /var/common/FMC_SNMP.pcap	SNMP 폴링에 대해 관리 인터페이스에서 트래픽을 캡처하고 파일에 저장
admin@FS2600-2:~\$ sudo pmtool status   grep snmpd	SNMP 프로세스 상태 확인
admin@FS2600-2:~\$ ls -al /var/common   grep snmpd	SNMP core 파일(traceback) 확인
admin@FS2600-2:~\$ sudo cat /etc/snmpd.conf	SNMP 구성 파일의 콘텐츠 확인

snmpwalk 예시

이러한 명령은 확인 및 문제 해결에 사용할 수 있습니다.

명령을 사용합니다	설명
# snmpwalk -c Cisco123 -v2c 192.0.2.1	SNMP v2c를 사용하여 원격 호스트에서 모든 OID를 가져옵니다.

	Cisco123 = 커뮤니티 문자열 192.0.2.1 = 대상 호스트
<pre># snmpwalk -v2c -c Cisco123 -OS 192.0.2.1 10.3.1.1.4.1.9.109.1.1.1.3 iso.3.6.1.4.1.9.9.109.1.1.1.3.1 = 게이지32: 0</pre>	SNMP v2c를 사용하여 원격 호스트에서 특정 OID를 가져옵니다.
<pre># snmpwalk -c Cisco123 -v2c 192.0.2.1 .10.3.1.4.1.9.9.109.1.1.1.1 -켜짐 .10.3.1.1.4.1.9.9.109.1.1.1.6.1 = 게이지32: 0</pre>	가져온 OID를 숫자 형식으로 표시
<pre># snmpwalk -v3 -l authPriv -u cisco -a SHA -A Cisco123 - x AES -X Cisco123 192.0.2.1</pre>	SNMP v3를 사용하여 원격 호스트에서 모든 OID를 가져옵니다. SNMPv3 사용자 = Cisco SNMPv3 인증 = SHA. SNMPv3 권한 부여 = AES
<pre># snmpwalk -v3 -l authPriv -u cisco -a MD5 -A Cisco123 - x AES -X Cisco123 192.0.2.1</pre>	SNMP v3를 사용하여 원격 호스트에서 모든 OID 가져오기(MD5 및 AES128)
<pre># snmpwalk -v3 -l auth -u cisco -a SHA -A Cisco123 192.0.2.1</pre>	인증을 사용하는 SNMPv3만

## SNMP 결함 검색 방법

1. <https://bst.cloudapps.cisco.com/bugsearch/search?kw=snmp&pf=prdNm&sb=anfr&bt=custV로 이동>
2. 키워드 snmp를 입력하고 목록에서 선택을 선택합니다.

Tools & Resources

# Bug Search Tool

Save Search Load Saved Search Clear Search Email Current Search

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

Product:

Releases:

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

Save Search Load Saved Search Clear Search Email Current Search

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

Product:

Releases:

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

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)

가장 일반적인 제품:

- Cisco Adaptive Security Appliance(ASA) 소프트웨어
- Cisco Firepower 9300 Series
- Cisco Firepower Management Center 가상 어플라이언스
- Cisco Firepower NGFW

## 관련 정보

- [Threat Defense에 대한 SNMP 설정](#)
- [FXOS\(UI\)에서 SNMP 구성](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.