FDM 관리 데이터 인터페이스에서 사이트 간 VPN에 SNMP 구성

목차

소개

이 문서에서는 FTD 디바이스 데이터 인터페이스의 데이터 인터페이스에서 Site-to-Site VPN을 통해 원격 엔드로의 SNMP 구성에 대해 설명합니다.

사전 요구 사항

컨피그레이션을 진행하기 전에 다음 전제 조건을 갖추었는지 확인합니다.

- 다음 항목에 대한 기본 이해:
  - Cisco FTD(Firepower Threat Defense)는 FDM(Firepower Device Manager)에서 관리됩니다.
  - Cisco ASA(Adaptive Security Appliance).
  - SNMP(Simple Network Management Protocol).
  - VPN(Virtual Private Network)
- FTD 및 ASA 디바이스에 대한 관리 액세스.
- 네트워크가 가동 중인지 확인하고 모든 명령의 잠재적인 영향을 파악합니다.

요구 사항

- Cisco FTD managed by FDM 버전 7.2.7
- Cisco ASA 버전 9.16
- SNMP 서버 세부 정보(IP 주소, 커뮤니티 문자열 포함)
- Site-to-Site VPN 컨피그레이션 세부 정보(피어 IP, 사전 공유 키 포함)
- REST API를 사용하여 SNMP를 구성하려면 FTD가 버전 6.7 이상이어야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD(Firepower Threat Defense) - FDM(Firepower Device Manager) 버전 7.2.7에서 관리됨
- Cisco ASA(Adaptive Security Appliance) 버전 9.16
- SNMP 서버(모든 표준 SNMP 서버 소프트웨어)

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.

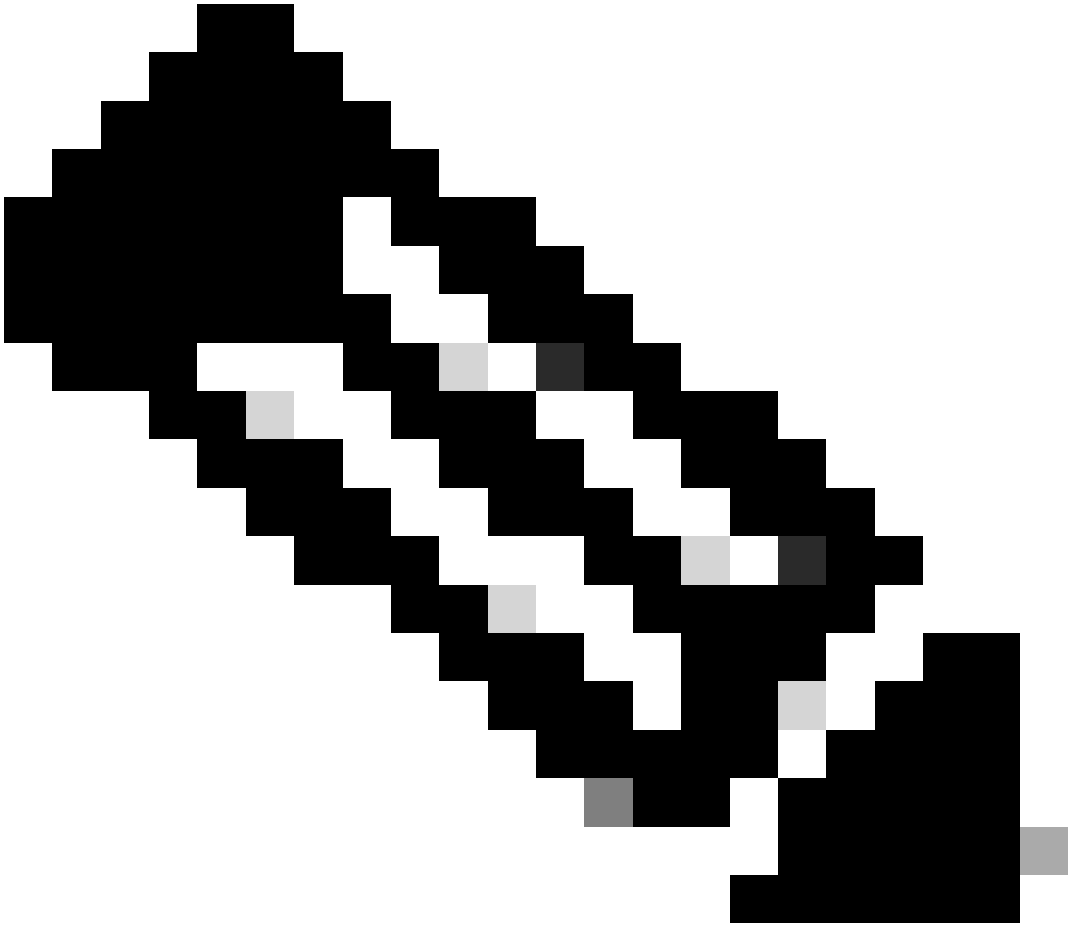
배경 정보

이러한 단계를 통해 네트워크 관리자는 네트워크 디바이스를 원격으로 모니터링할 수 있습니다.

SNMP(Simple Network Management Protocol)는 네트워크 관리 및 모니터링에 사용됩니다. 이 설정에서는 ASA와 함께 설정된 사이트 간 VPN을 통해 SNMP 트래픽이 FTD에서 원격 SNMP 서버로 전송됩니다.

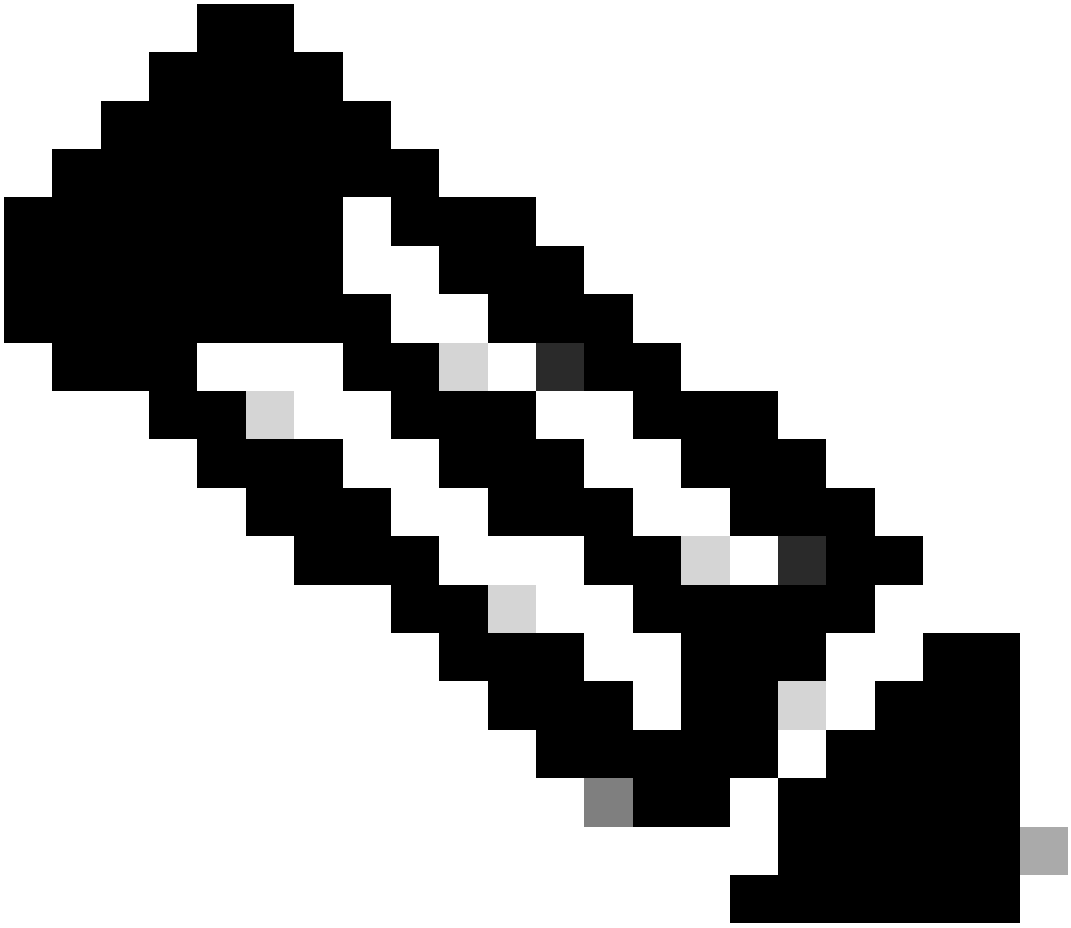
이 가이드는 네트워크 관리자가 FTD 디바이스의 데이터 인터페이스에서 사이트 간 VPN을 통해 원격 엔드로의 SNMP를 구성하는 데 도움이 됩니다. 이 설정은 네트워크 장치를 원격으로 모니터링하고 관리하는 데 유용합니다. 이 설정에서는 SNMP v2가 사용되고 ASA와 함께 설정된 사이트 간 VPN을 통해 FTD 데이터 인터페이스에서 원격 SNMP 서버로 SNMP 트래픽이 전송됩니다.

사용되는 인터페이스를 "inside"라고 하지만 이 컨피그레이션은 다른 유형의 "to-the-box" 트래픽에 적용할 수 있으며 VPN이 종료되는 인터페이스가 아닌 방화벽의 모든 인터페이스를 사용할 수 있습니다.



참고: FTD에서 버전 6.7 이상을 실행하고 FDM에서 관리되는 경우 SNMP는 REST API를 통해서만 구성할 수 있습니다.

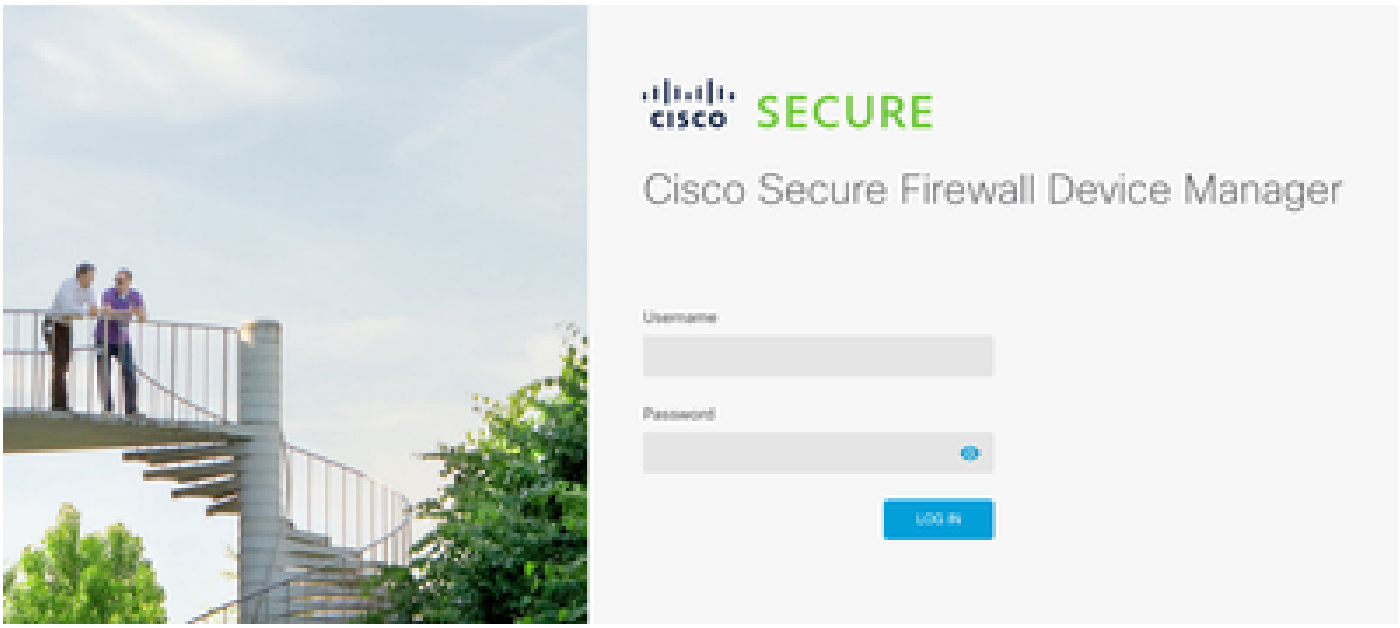
구성



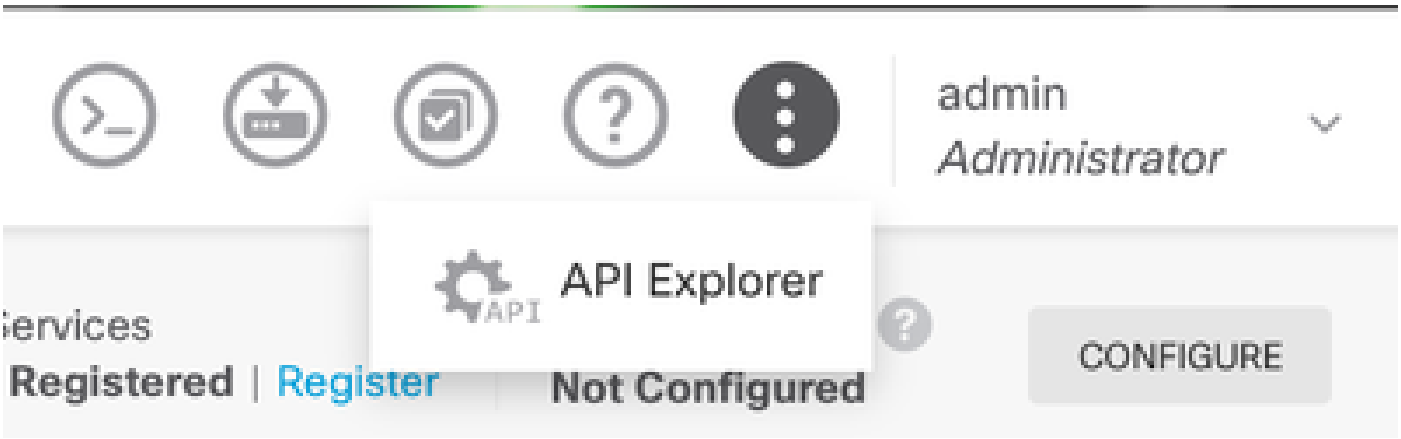
참고: 이 컨피그레이션에서는 디바이스 간에 사이트 대 사이트 VPN이 이미 구성된 것으로 간주합니다. 사이트 대 사이트 VPN을 구성하는 방법에 대한 자세한 내용은 컨피그레이션 가이드를 참조하십시오. FDM에서 관리하는 FTD에 사이트 대 사이트 VPN 구성

설정

1. FTD에 로그인합니다.



2. 장치 개요 아래에서 API 탐색기로 이동합니다.



3. FTD에서 SNMPv2를 구성합니다

- 인터페이스 정보를 가져옵니다.

4. 아래로 스크롤하여 API 호출을 수행하려면 Try it out! 버튼을 선택합니다. 호출이 성공하면 응답 코드 200이 반환됩니다.

TRY IT OUT! Hide Response

Curl

```
curl -X GET --header 'Accept: application/json' 'https:.
```

Request URL

```
https://                34/api/fdm/v6/devices/default/interfaces
```

Response Body

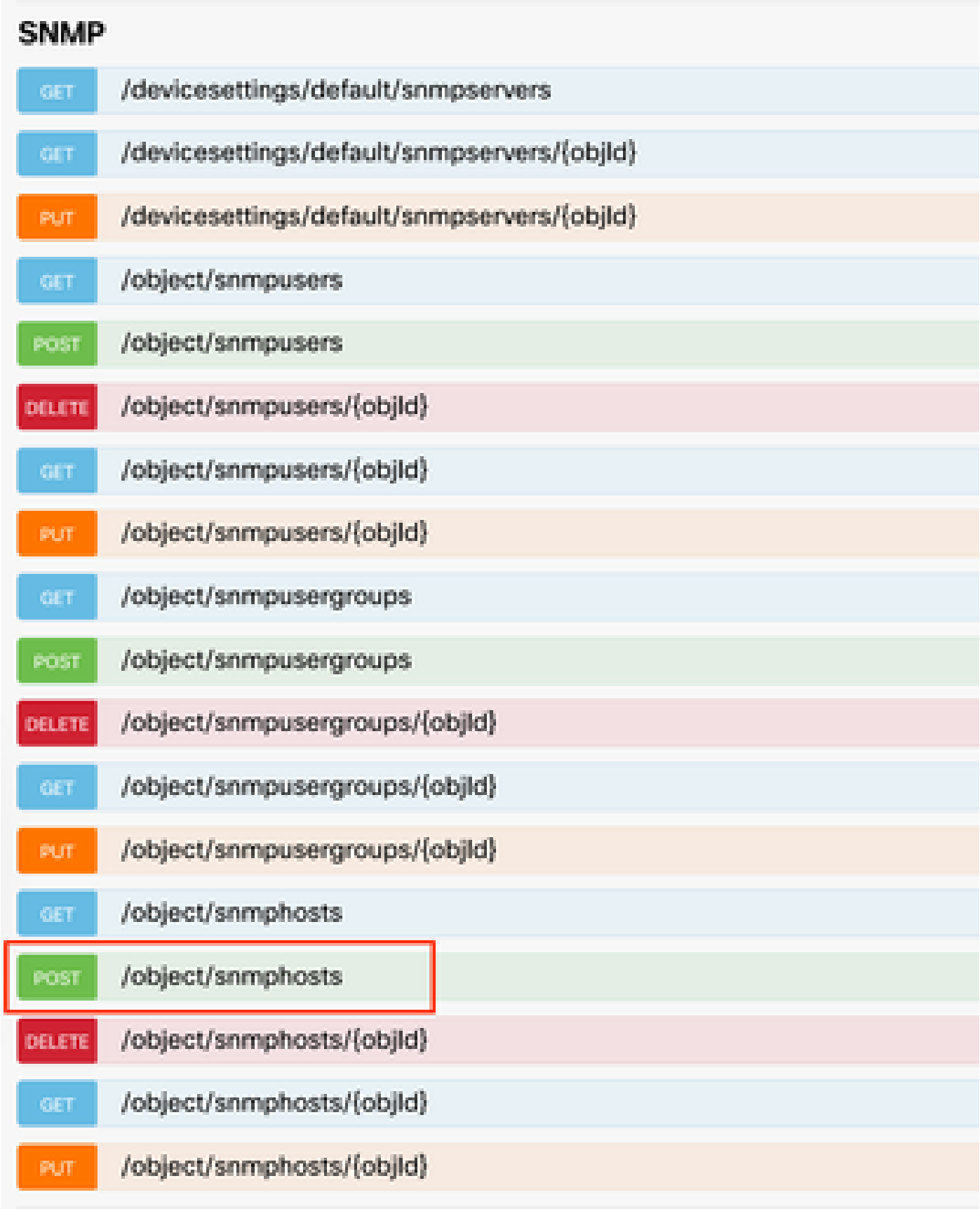

```
    },
    {
      "version": "mqjiipiswsgsx",
      "name": "inside",
      "description": null,
      "hardwareName": "GigabitEthernet0/1",
      "monitorInterface": false,
      "ipv4": {
        "ipType": "STATIC",
        "defaultRouteUsingDHCP": false,
        "dhcpRouteMetric": null,
        "ipAddress": {
          "ipAddress": "10.57.58.1",
          "netmask": "255.255.255.0",
          "standbyIpAddress": null,
          "type": "haipv4address"
        },
        "dhcp": false,
        "addressNull": false,
        "type": "interfaceipv4"
      },
```


Response Code

```
200
```

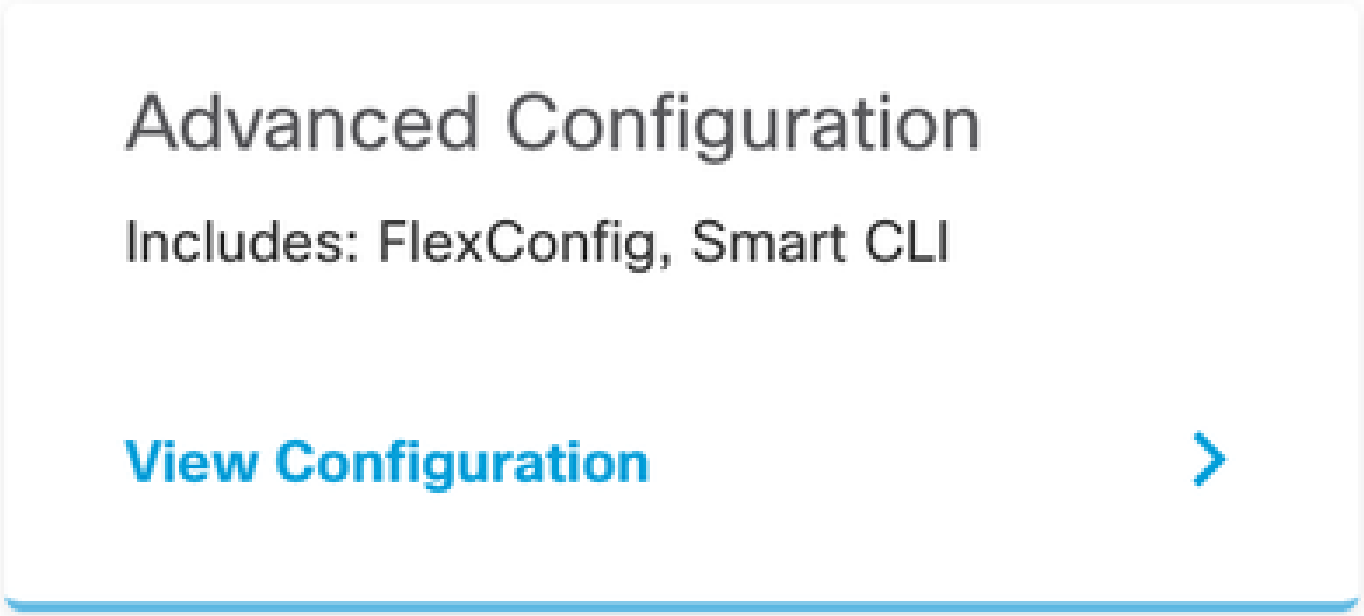
- SNMP 호스트에 대한 네트워크 개체 컨피그레이션을 생성합니다.

- 새 SNMPv2c 호스트 개체를 만듭니다.

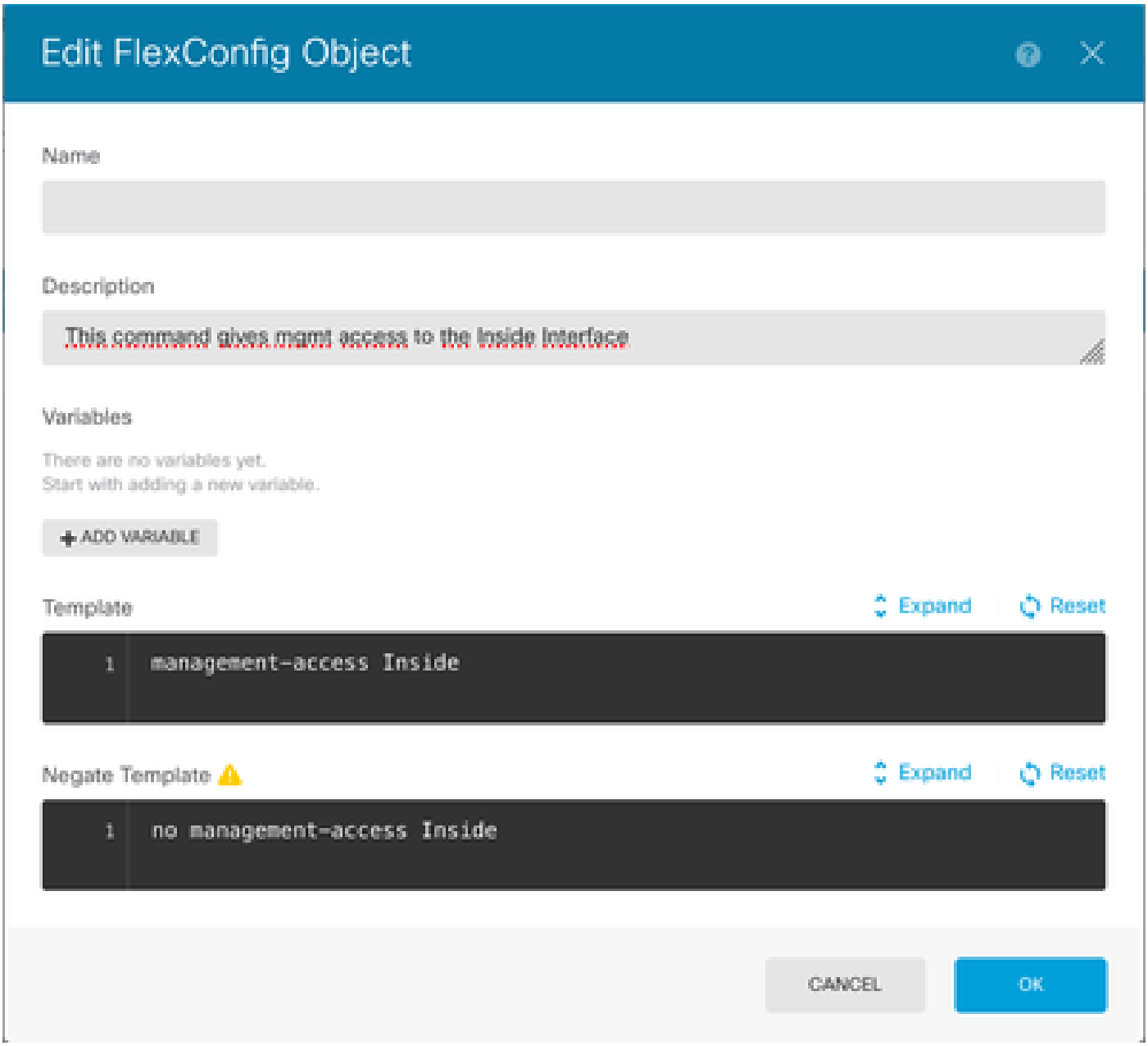


자세한 내용은 Configuration(컨피그레이션) 가이드를 확인하고 Firepower FDM에서 SNMP 구성 및 문제 해결

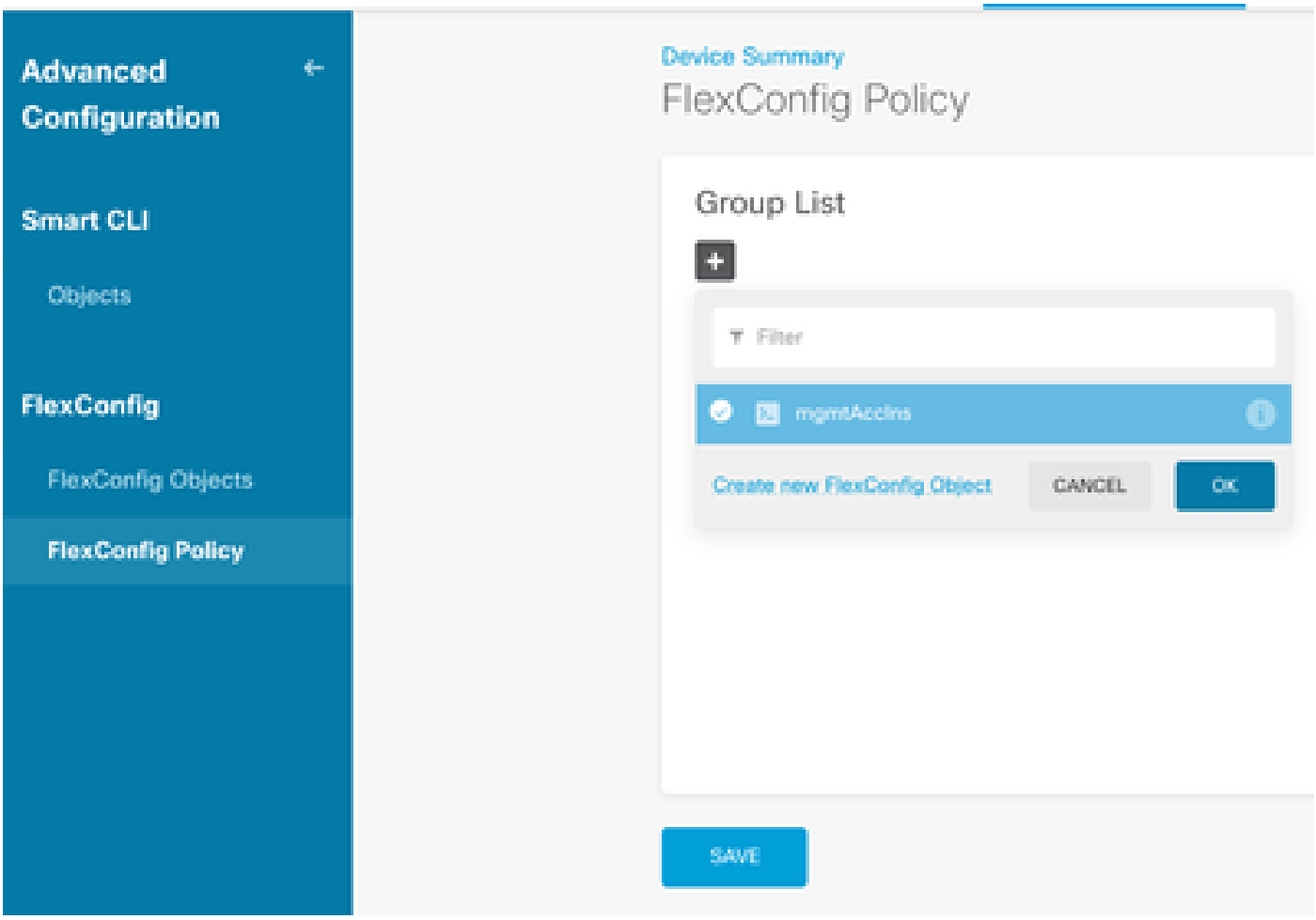
5. 디바이스에 SNMP가 구성되면 고급 컨피그레이션 섹션에서 디바이스로 이동하여 컨피그레이션 보기를 선택합니다.



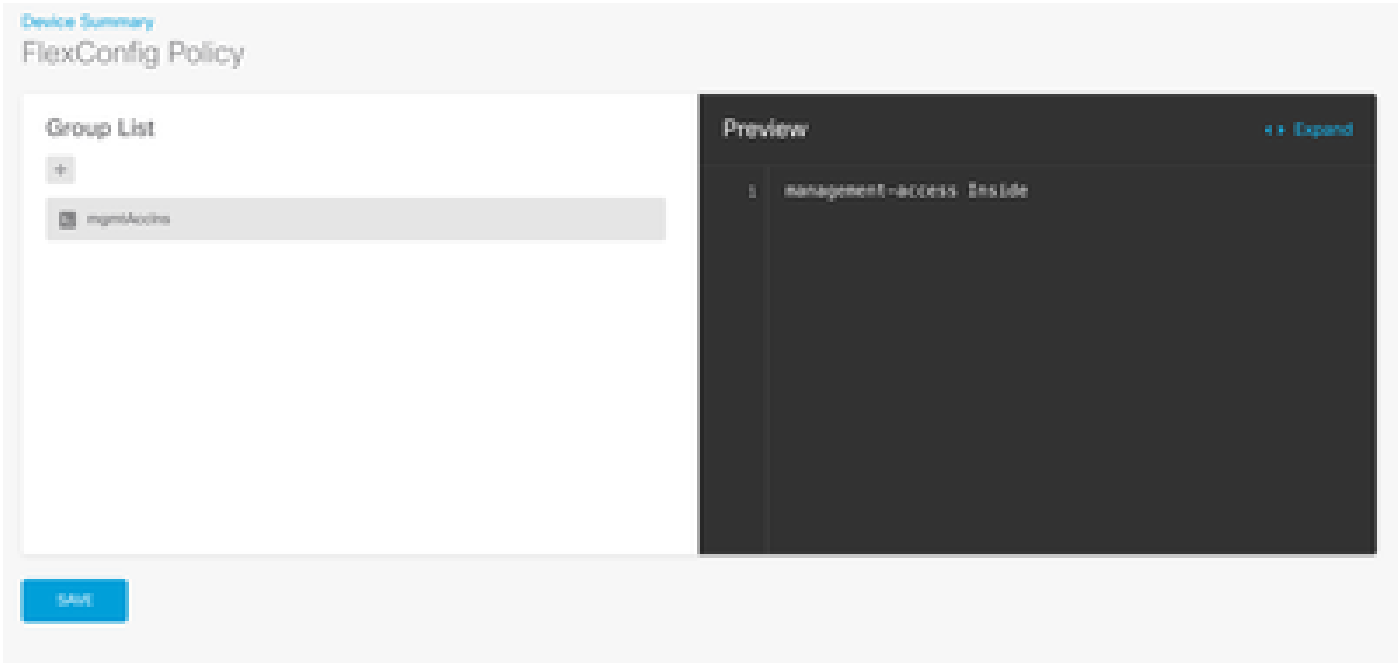
6. FlexConfig 섹션에서 FlexConfig 객체를 선택하고 새 객체를 생성한 다음 이름을 지정하고 템플릿 섹션에 management-access 명령을 추가하고, 인터페이스를 지정하고 템플릿 부정 부분에 명령 부정을 추가합니다.



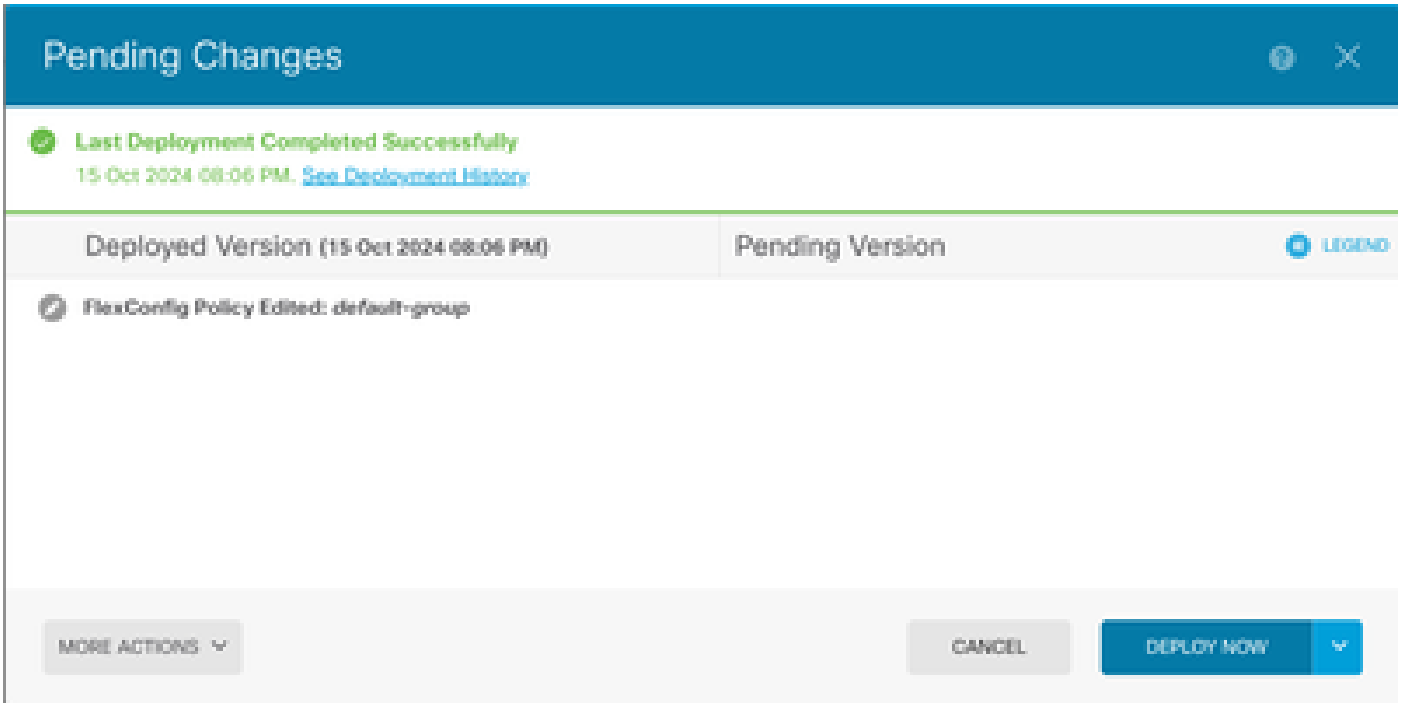
7. FlexConfig 섹션에서 FlexConfig Policy를 선택하고 추가 아이콘을 클릭한 다음 이전 단계에서 생성한 flexConfig 개체를 선택하고 OK를 선택합니다.

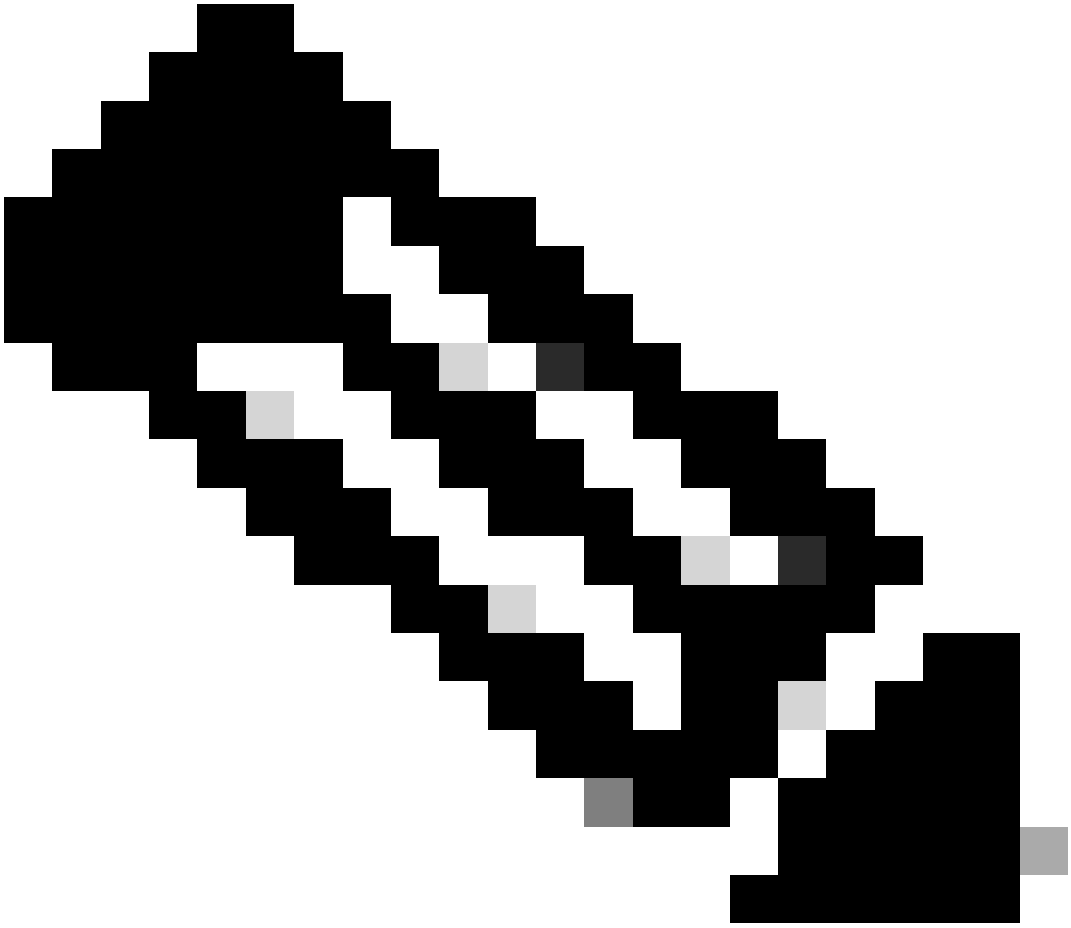


8. 그러면 장치에 적용할 명령의 미리 보기가 나타납니다. 저장을 선택합니다.



9. 구성을 배포하고 배포 아이콘을 선택한 후 지금 배포를 누릅니다.


Pending Changes
Last Deployment Completed Successfully
15 Oct 2024 08:06 PM. See Deployment History
Deployed Version (15 Oct 2024 08:06 PM)
Pending Version
LEGEND
FlexConfig Policy Edited: default-group
MORE ACTIONS
CANCEL
DEPLOY NOW



참고: 만족스럽게 완료되었는지 확인합니다. 작업 목록을 확인하여 확인할 수 있습니다.

다음을 확인합니다.

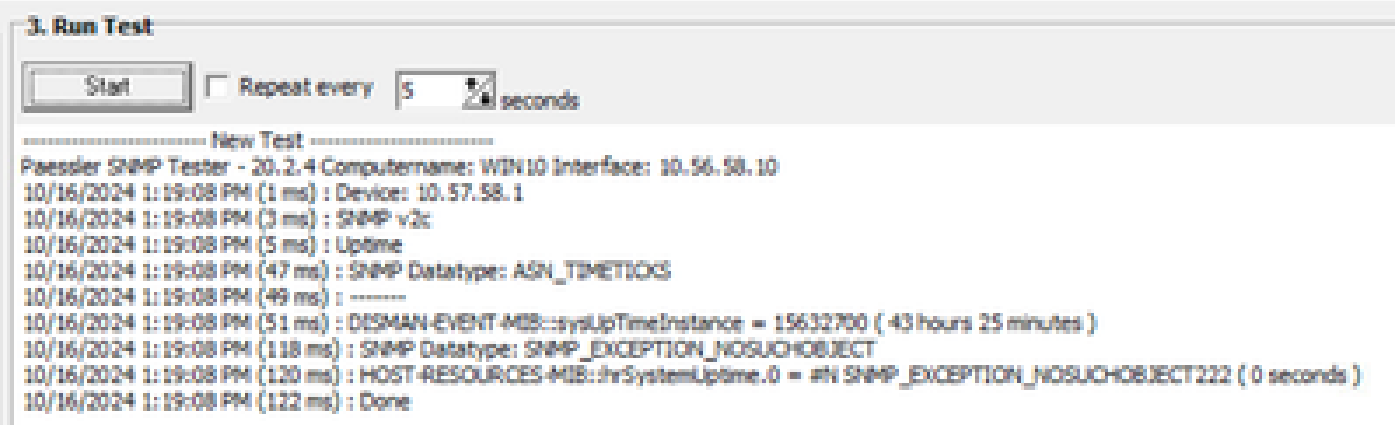
컨피그레이션을 확인하려면 다음 검사를 수행하고, SSH 또는 콘솔을 통해 FTD에 로그인하고 다음 명령을 실행합니다.

- 디바이스의 실행 중인 컨피그레이션에 변경 사항이 포함되어 있는지 확인합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password:
firepower# show running-config
<some outouts are ommitted>
object network snmpHost
host 10.56.58.10
```

```
<some outputs are ommitted>
snmp-server host inside 10.56.58.10 community ***** version 2c
snmp-server location null
snmp-server contact null
snmp-server community *****
<some outputs are omitted>
management-access inside
```

- SNMP 테스터에서 테스트를 수행하고 정상적으로 완료되는지 확인합니다.



문제 해결

문제가 발생하는 경우 다음 단계를 고려하십시오.

- VPN 터널이 작동 및 실행 중인지 확인합니다. 이 명령을 실행하여 VPN 터널을 확인할 수 있습니다.

```
firepower# show crypto ikev2 sa

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf Status Role
442665449 10.197.225.82/500 10.197.225.81/500 READY RESPONDER
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/10 sec
Child sa: local selector 10.57.58.0/0 - 10.57.58.255/65535
remote selector 10.56.58.0/0 - 10.56.58.255/65535
ESP spi in/out: 0x3c8ba92b/0xf79c95a9

firepower# show crypto ikev2 stats

Global IKEv2 Statistics
Active Tunnels: 1
Previous Tunnels: 2
```

IKEv2 터널을 디버그하는 방법에 대한 자세한 설명서는 [How to Debug IKEv2 VPNs(IKEv2 VPN을

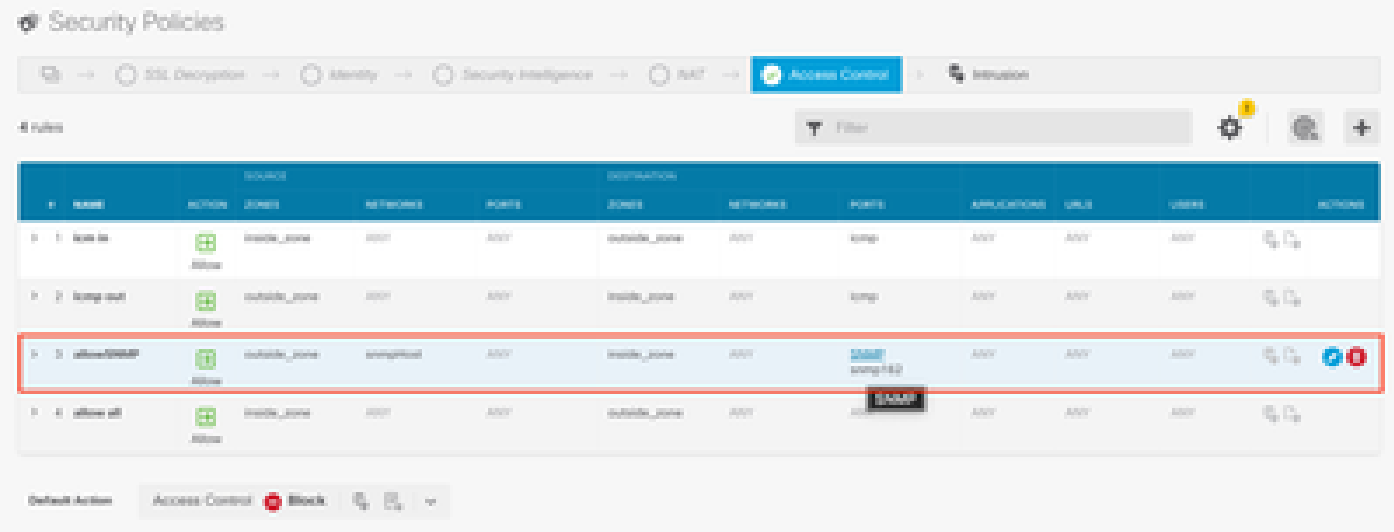
[디버깅하는 방법)을 참조하십시오.](#)

- SNMP 컨피그레이션을 확인하고 양쪽 끝에서 커뮤니티 문자열 및 액세스 제어 설정이 올바른지 확인합니다.

firepower# sh snmp-server 실행
10.56.58.10 커뮤니티 ***** 버전 2c 내부의 snmp-server 호스트
snmp-server 위치 null
snmp-server 연락처 null
snmp-server 커뮤니티 *****

- SNMP 트래픽이 FTD를 통해 허용되는지 확인합니다.

Policies(정책) > Access Control(액세스 제어)로 이동하고 SNMP 트래픽을 허용하는 규칙이 있는지 확인합니다.



- 패킷 캡처를 사용하여 SNMP 트래픽을 모니터링하고 문제를 식별합니다.

방화벽에서 추적을 통한 캡처 활성화:

```
capture snmp interface inside trace detail match udp any any eq snmp
```

```
firepower# show capture
capture snmp type raw-data trace detail interface inside include-decrypted [Capturing - 405 bytes]
match udp host 10.57.58.10 host 10.56.58.1 eq snmp
```

```
firepower# sh capture snmp
4 packets captured

1: 17:50:42.271806 10.56.58.10.49830 > 10.57.58.1.161: udp 43
2: 17:50:42.276551 10.56.58.10.49831 > 10.57.58.1.161: udp 43
```

```
3: 17:50:42.336118 10.56.58.10.49832 > 10.57.58.1.161: udp 44
4: 17:50:42.338803 10.56.58.10.49833 > 10.57.58.1.161: udp 43
4 packets shown
```

자세한 내용은 SNMP 컨피그레이션 가이드를 확인하고 Firepower FDM에서 SNMP 구성 및 문제 해결

관련 정보

- Cisco Secure Firepower Device Manager 컨피그레이션 가이드
- Cisco ASA 컨피그레이션 가이드
- Cisco 디바이스의 SNMP 컨피그레이션

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.