Configure SNMP on Site-to-Site VPN on FDM-Managed Data Interface

Contents

Introduction

This document describes configuring SNMP to a remote end through a site-to-site VPN on a data interface of an FTD device data interface.

Prerequisites

Before proceeding with the configuration, ensure that you have these prerequisites in place:

- Basic understanding of these topics:
  - Cisco Firepower Threat Defense (FTD) managed by Firepower Device Manager (FDM).
  - Cisco Adaptive Security Appliance (ASA).
  - Simple Network Management Protocol (SNMP).
  - Virtual Private Network (VPN).
- Administrative access to the FTD and ASA devices.
- Ensure that your network is live and you understand the potential impact of any command.

Requirements

- Cisco FTD managed by FDM version 7.2.7
- Cisco ASA version 9.16
- SNMP server details (including IP address, community string)
- Site-to-site VPN configuration details (including peer IP, pre-shared key)
- FTD must be at least version 6.7 in order to use REST API to configure SNMP.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Firepower Threat Defense (FTD) managed by Firepower Device Manager (FDM) version 7.2.7.
- Cisco Adaptive Security Appliance (ASA) version 9.16.

- SNMP Server (any standard SNMP server software)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

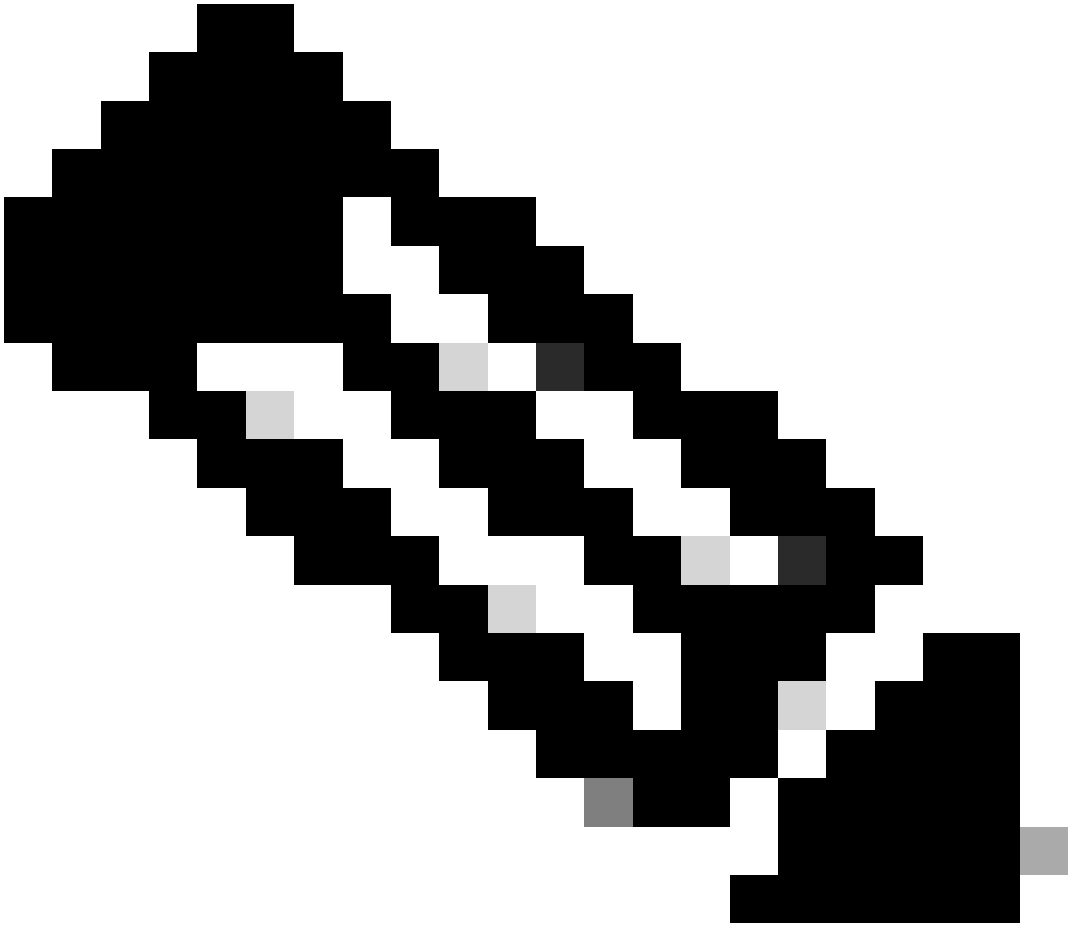
Background information

These steps outlined, network administrators can ensure monitoring of their network device remotely.

SNMP (Simple Network Management Protocol) is used for network management and monitoring. In this setup, SNMP traffic are sent from the FTD to a remote SNMP server through a site-to-site VPN established with an ASA.

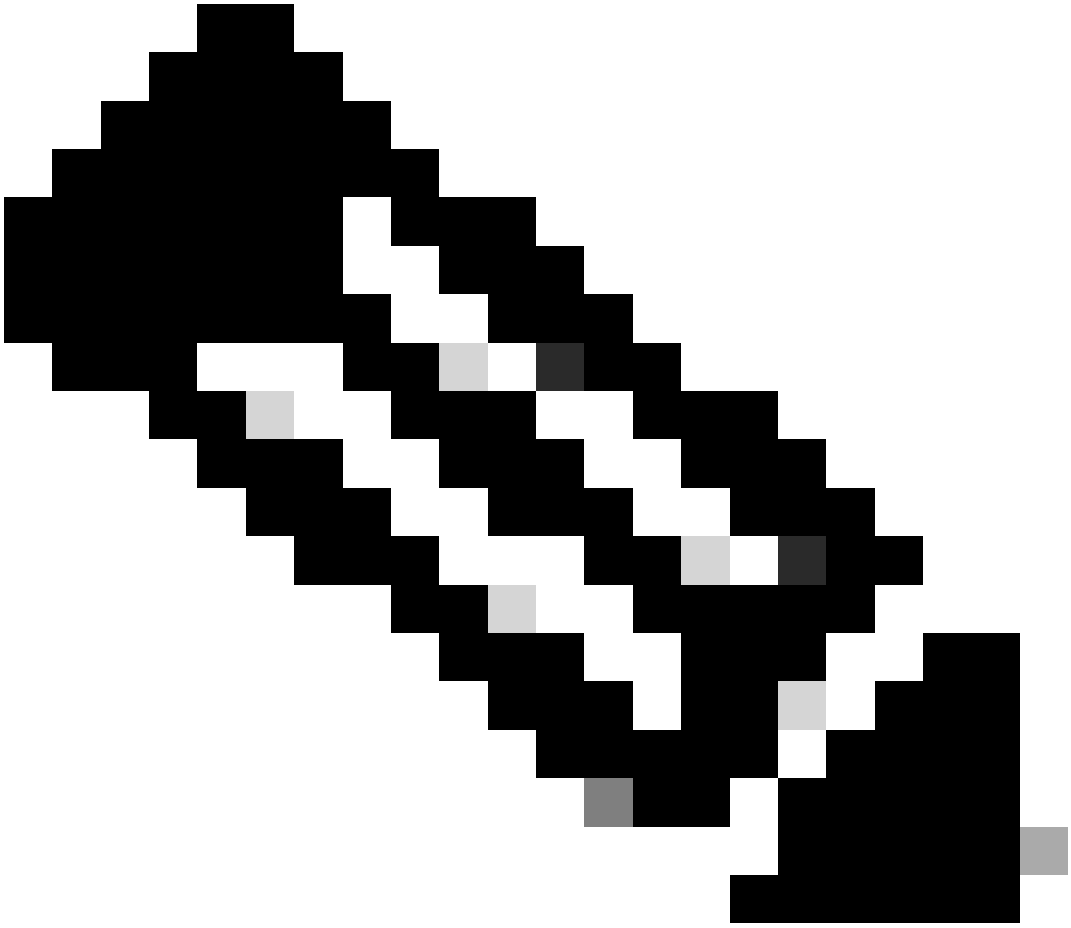
This guide aims to help network administrators configure SNMP to a remote end through a site-to-site VPN on a data interface of an FTD device. This setup is useful for monitoring and managing network devices remotely. In this setup, SNMP v2 is used and SNMP traffic are sent from the FTD data interface to a remote SNMP server through a site-to-site VPN established with an ASA.

The interface used is called "inside," but this configuration can be applied to other types of "to-the-box" traffic and can utilize any interface of the firewall that is not the one where the VPN terminates.



Note: SNMP can only be configured via REST API when FTD runs version 6.7 and later, and is managed by FDM.

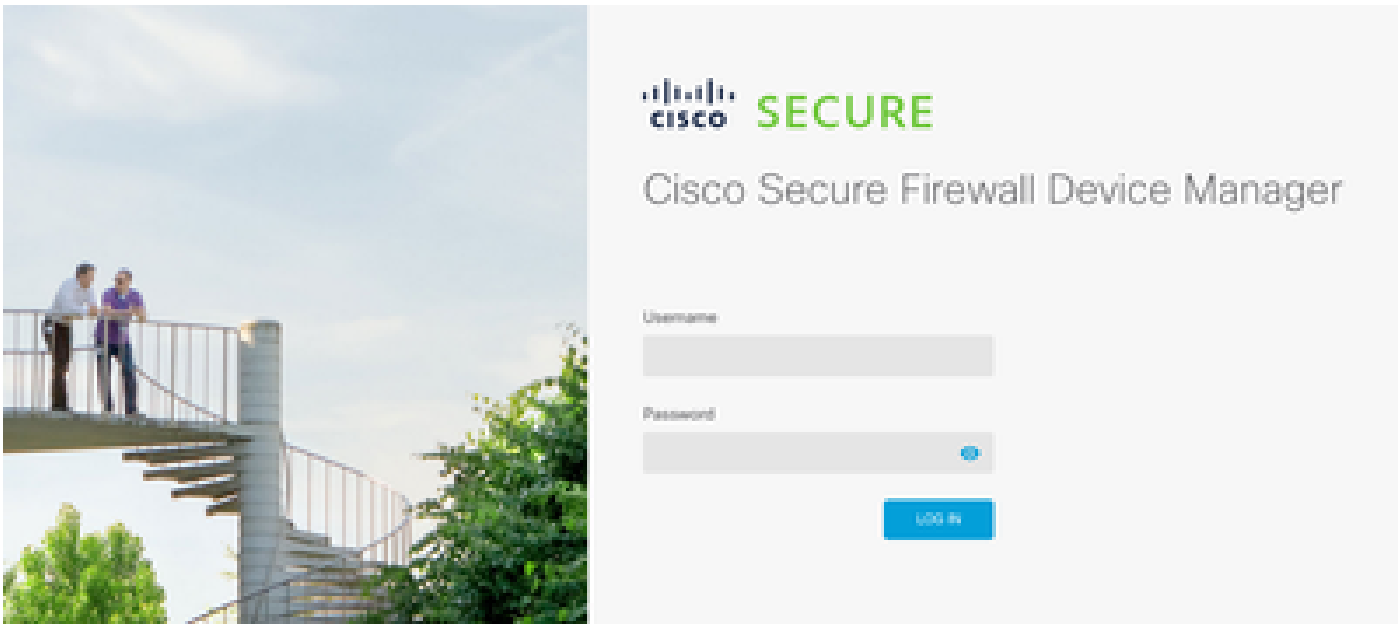
Configure



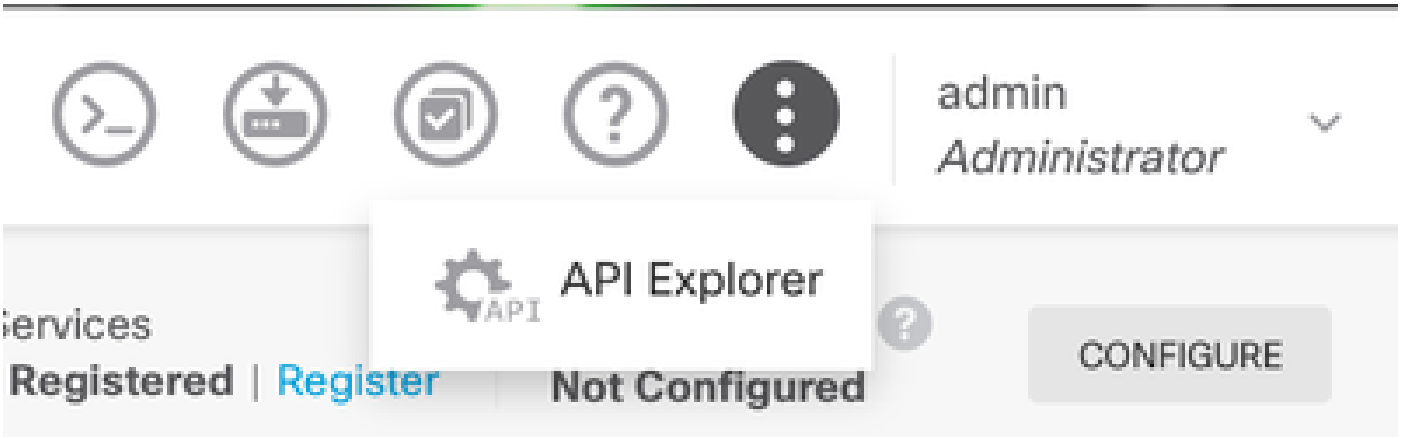
Note: This configuration considers that the site to site VPN is already configured between the devices. For additional details on how to configure the site to site VPN check the configuration guide. Configure Site-to-site VPN on FTD managed by FDM

Configurations

1. Log in to your FTD.



2. Under the **Device** overview navigate to the **API explorer**.



3. Configure SNMPv2 on FTD

- Get interface information.

4. Scroll down and select the **Try it out!** button to make the API call. A successful call returns Response code 200

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

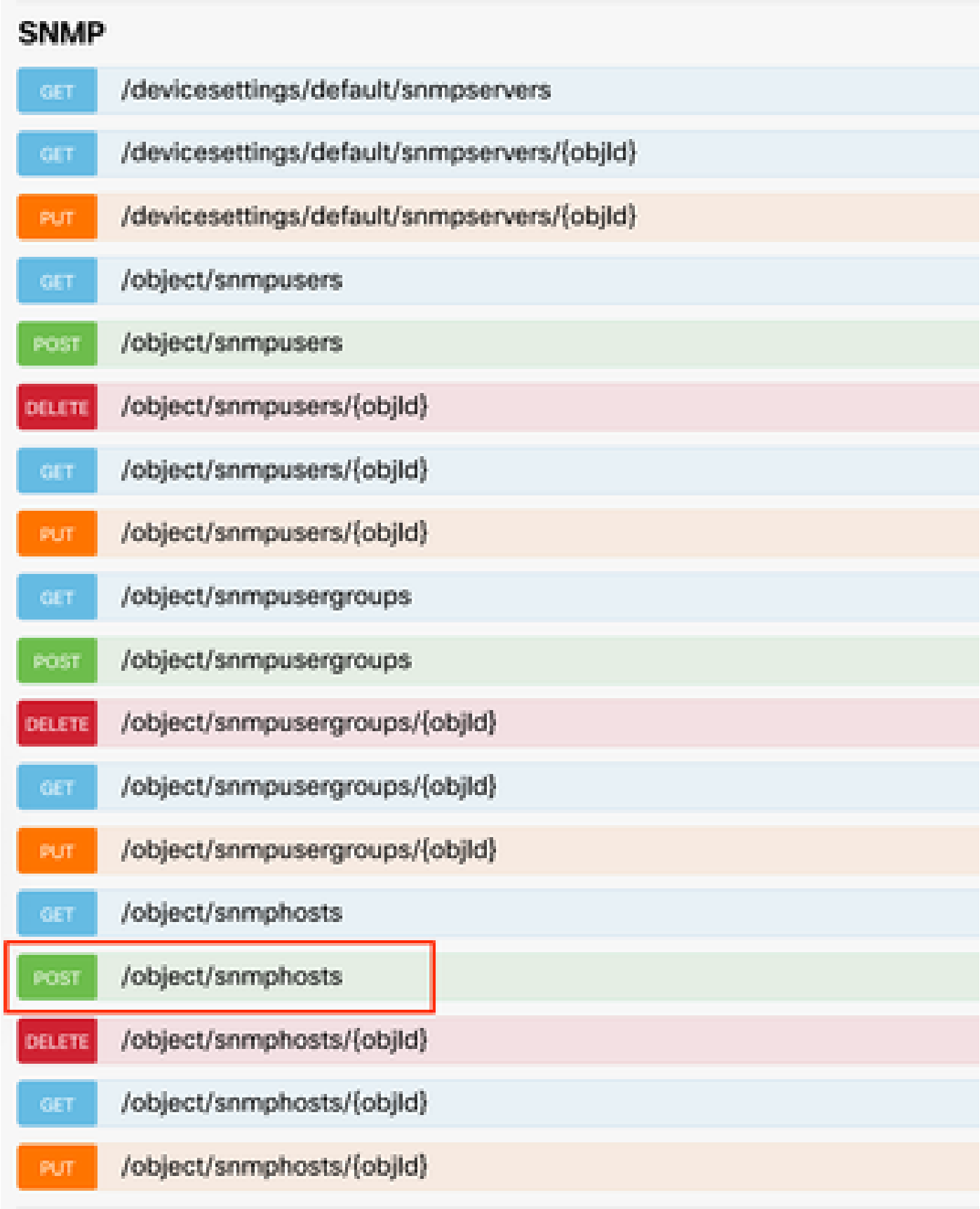

```
    },
    {
      "version": "mqjiipiswsgsx",
      "name": "inside",
      "description": null,
      "hardwareName": "GigabitEthernet0/1",
      "monitorInterface": false,
      "ipv4": {
        "ipType": "STATIC",
        "defaultRouteUsingDHCP": false,
        "dhcpRouteMetric": null,
    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


Response Code

```
200
```

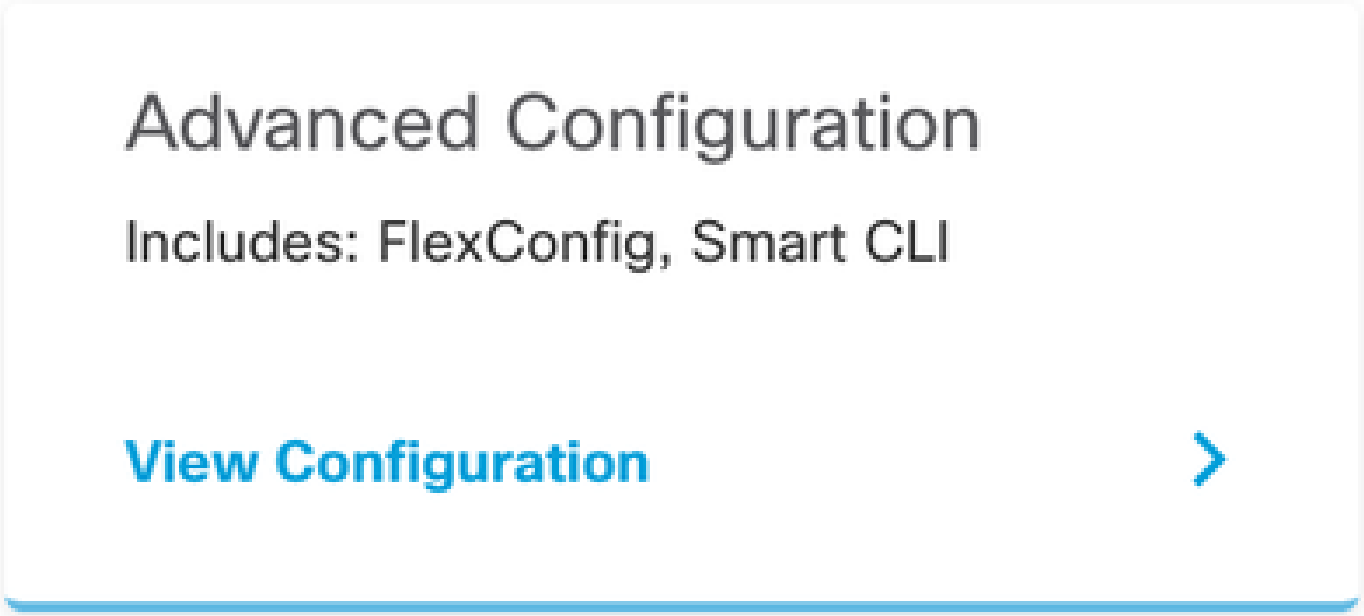
- Create a Network Object Config for the SNMP host.

- Create a new SNMPv2c host object.

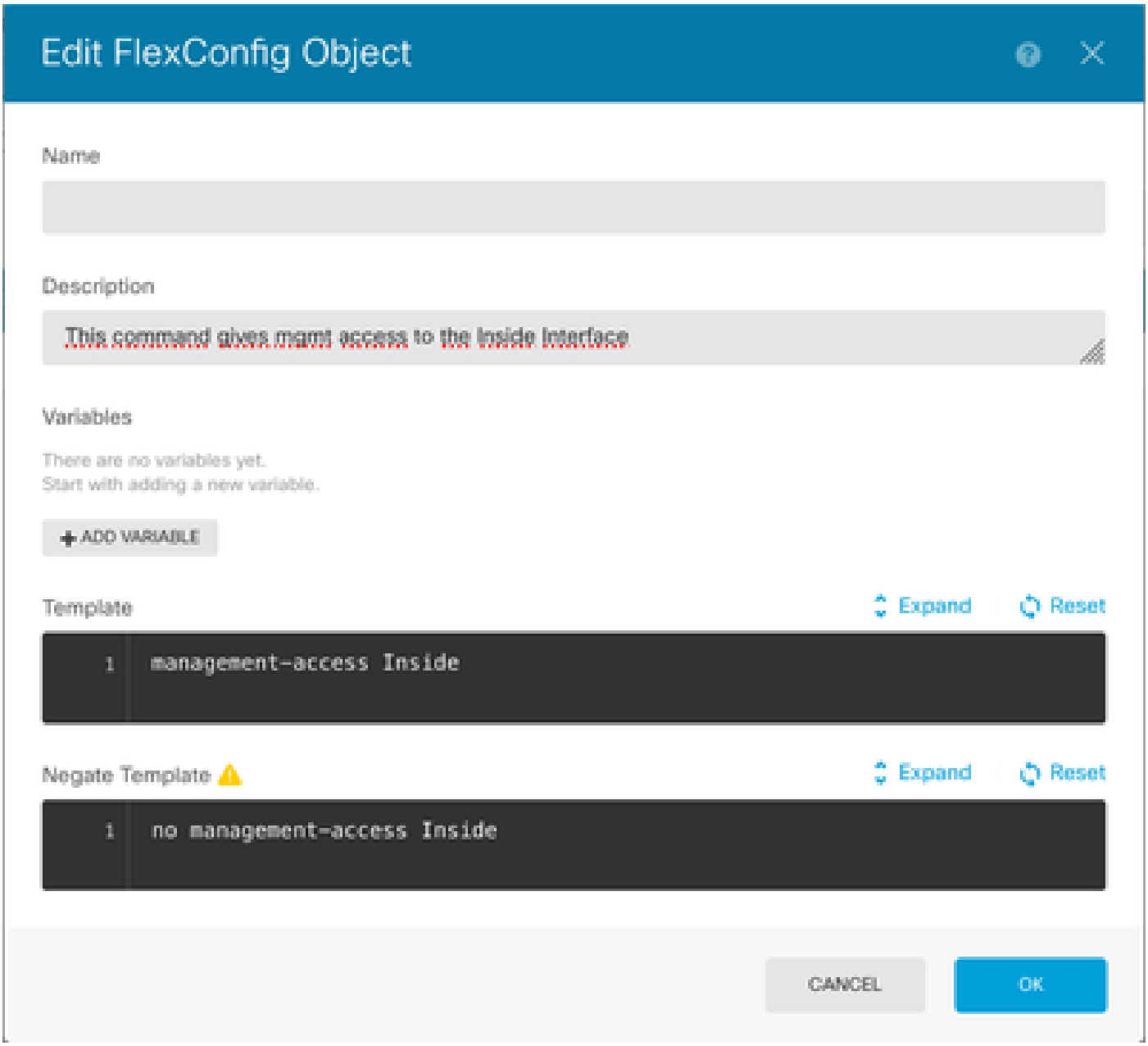


For additional details check the Configuration guide, [Configure and troubleshoot SNMP on Firepower FDM]

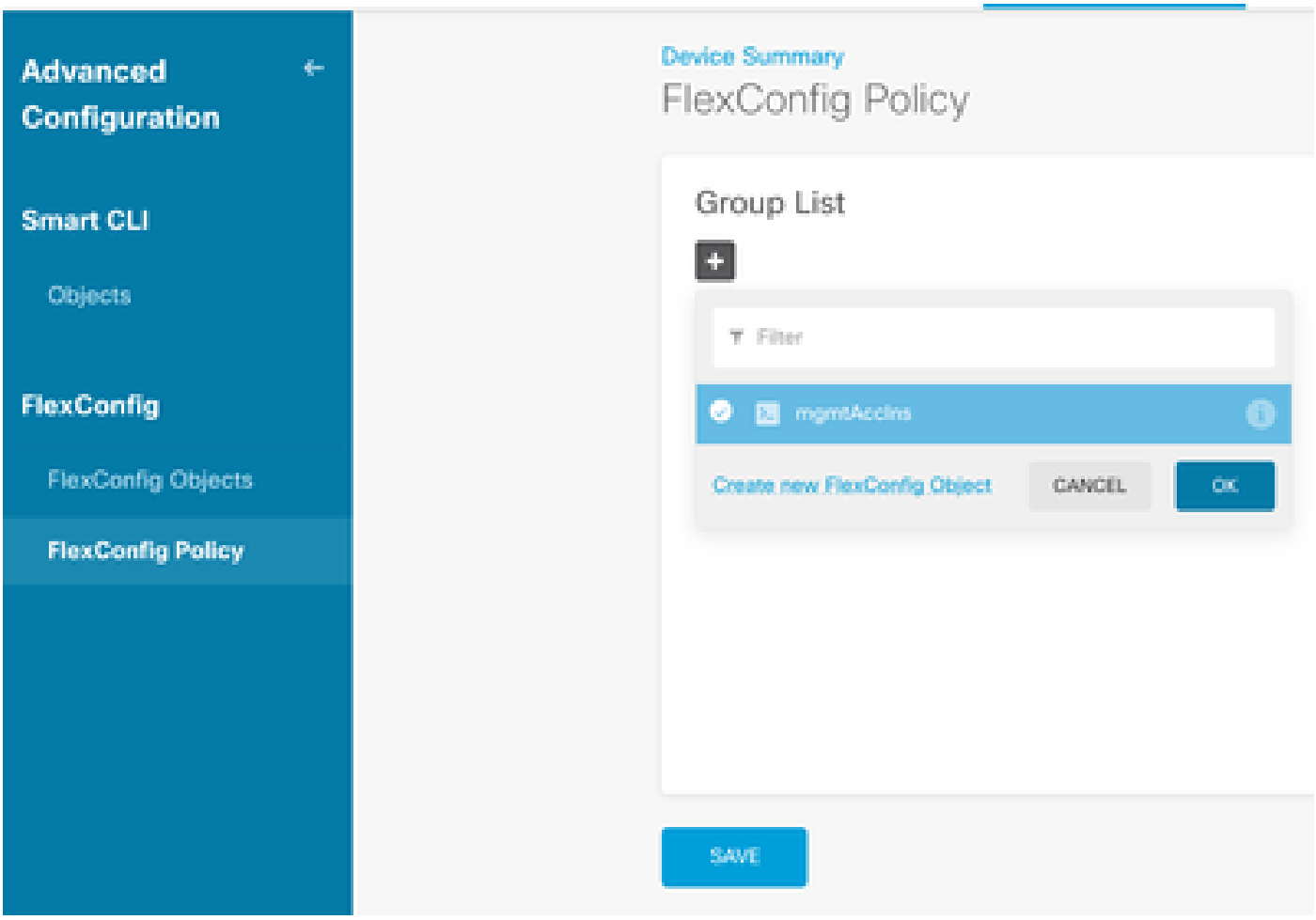
5. Once SNMP is configured on the device, navigate to **Device** in the **Advanced Configuration** section and select **View Configuration**.



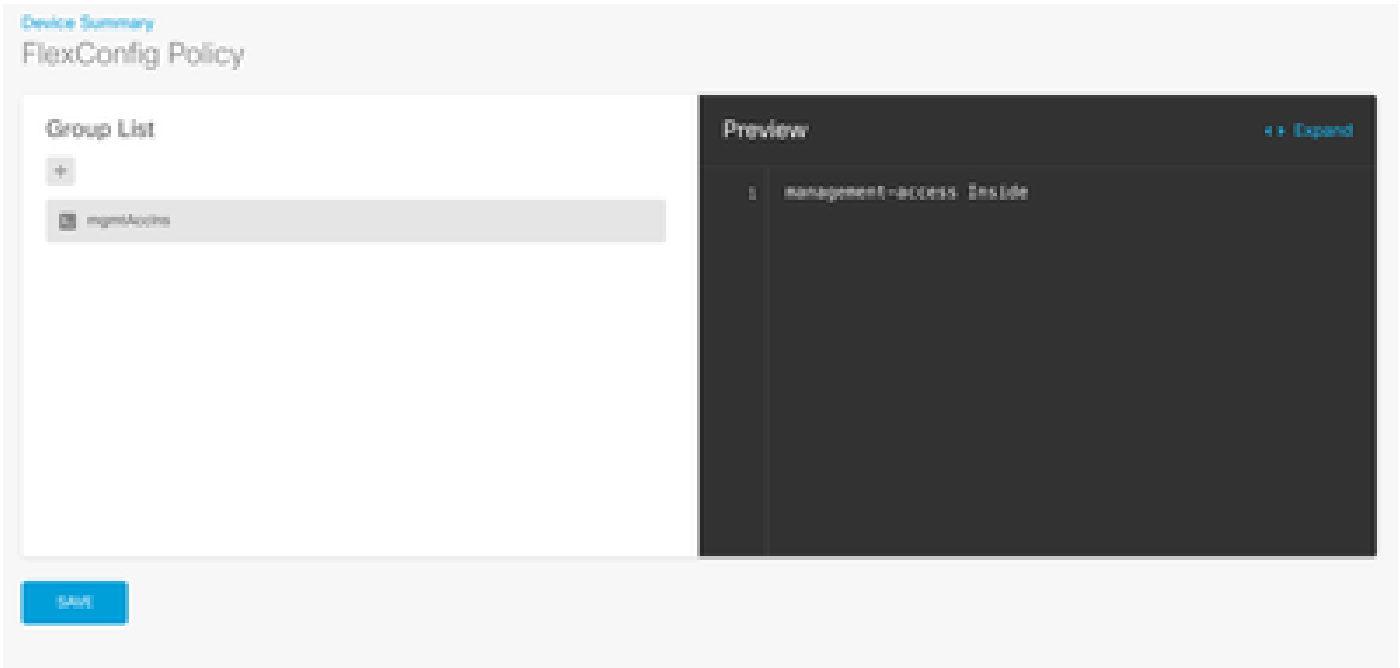
6. In the FlexConfig section, select **FlexConfig objects** and create a new object, name it and add the **management-access** command in the template section, specify the interface and add the command negation in the template negation part.



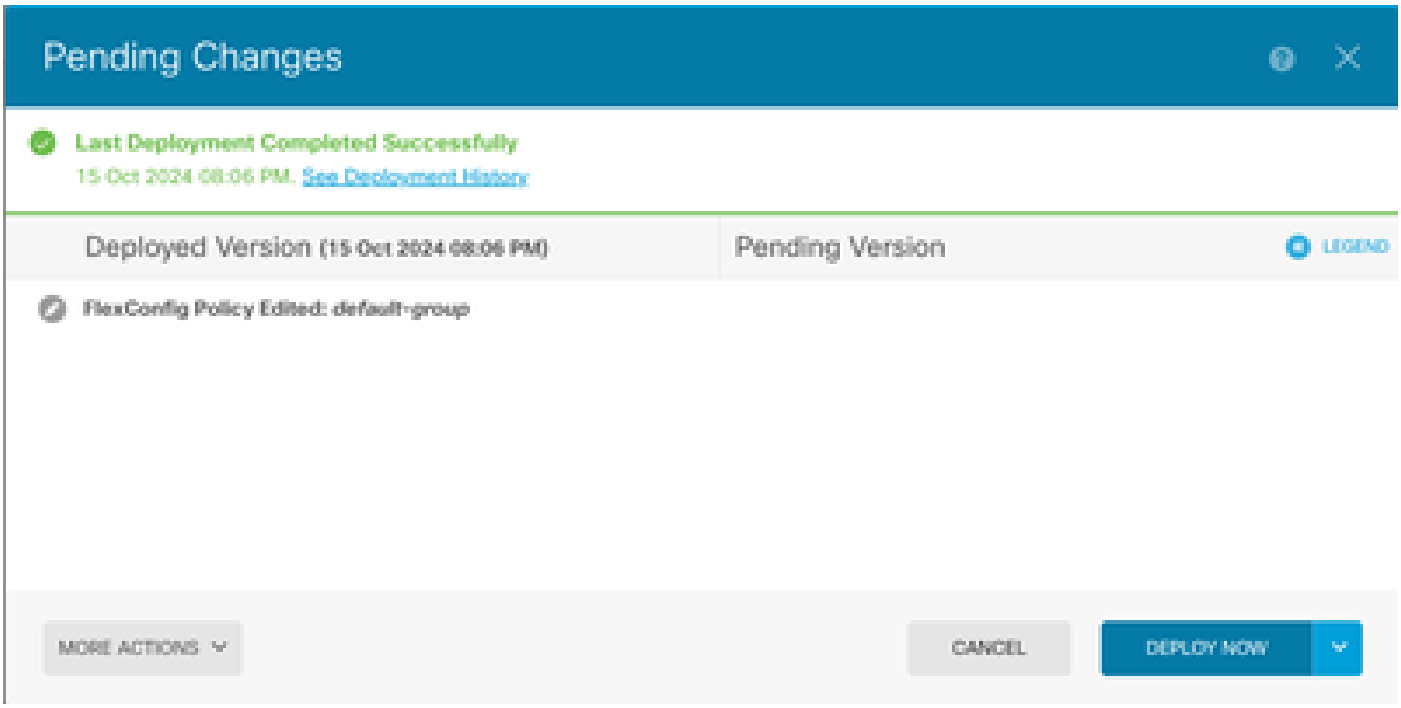
7. In the FlexConfig section, select **FlexConfig Policy**, click on the add icon and select the flexConfig object we created in the previous step and select OK.

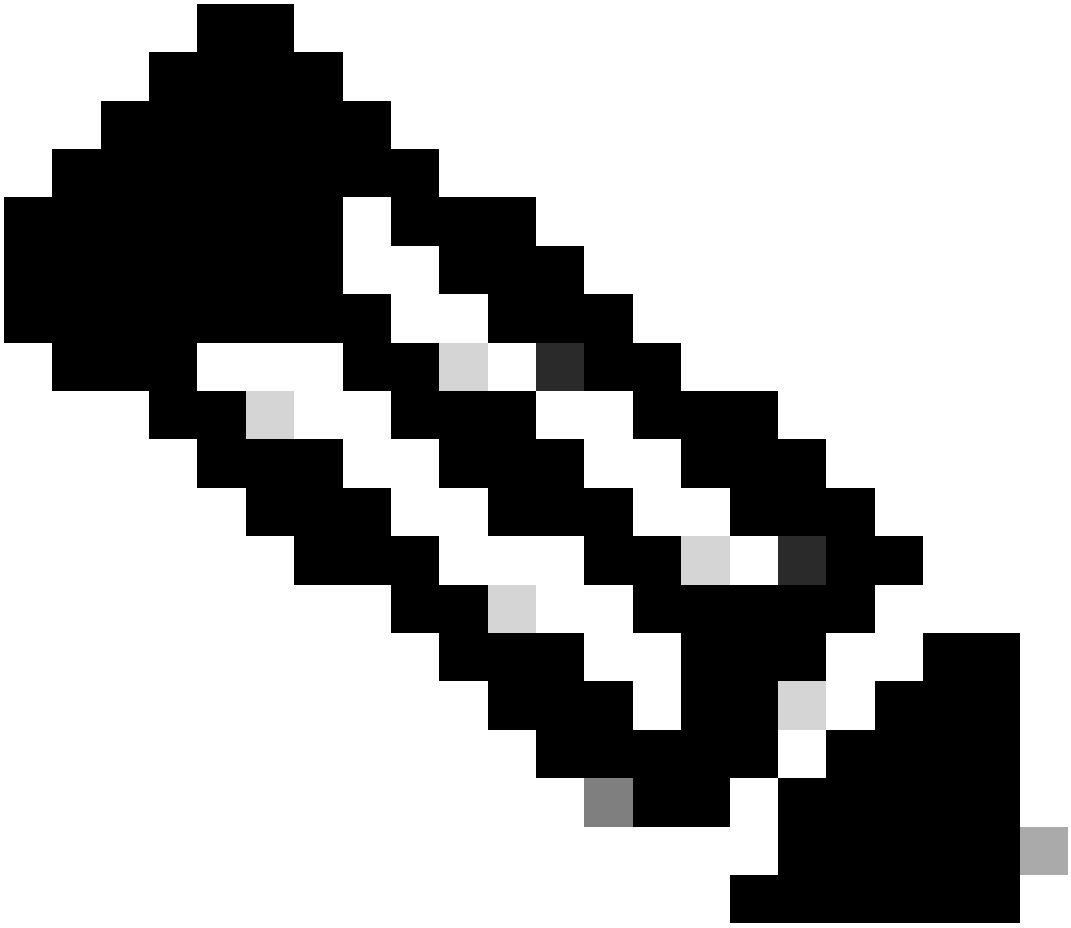


8. Then, a preview of the commands to be applied to the device appears. Select **Save**.



9. Deploy the configuration, select the deploy icon and click deploy now.


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



Note: Make sure it is completed satisfactorily, you can check the task list to confirm it.

Verify

To verify the configuration, perform these checks, log in to the FTD via SSH or console, and run these commands:

- Verify that the running config of the device contains the changes we made.

```
> 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
```

- Perform a test from the SNMP tester and make sure it completes successfully.

Troubleshoot

If you encounter any issues, consider these steps:

- Make sure that the VPN tunnel is up and running, you can run these command to verify the VPN tunnel.

```
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
```

A detailed guide on how to debug IKEv2 tunnels can be found here: [How to Debug IKEv2 VPNs]

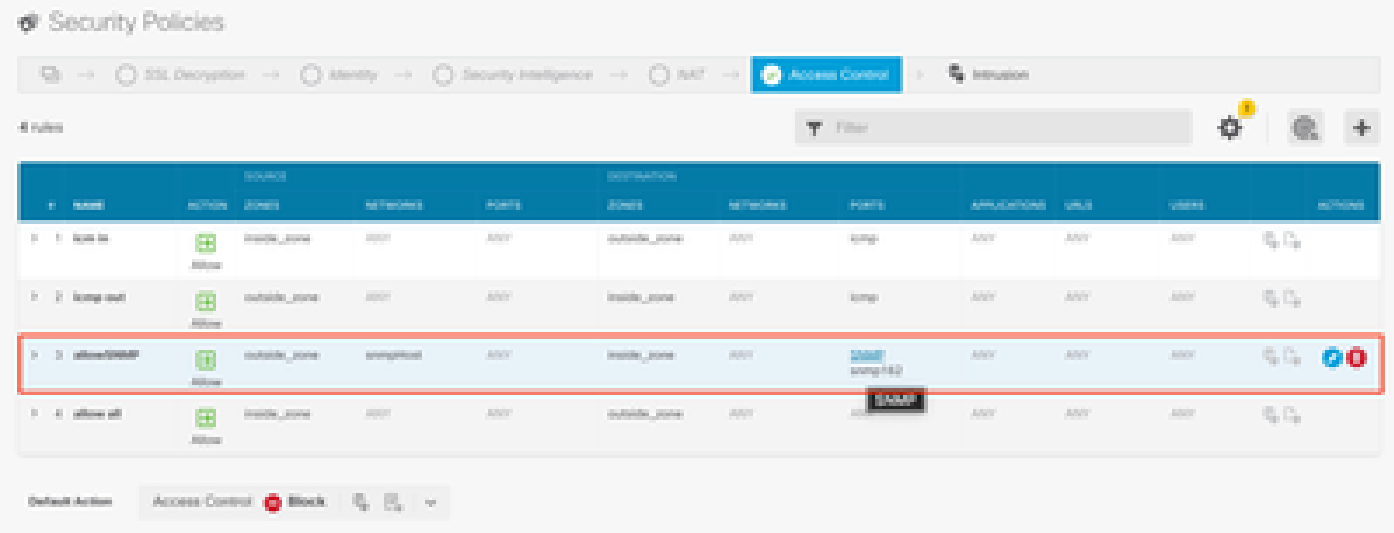
- Verify the SNMP configuration and ensure that the community string and access control settings are

correct on both ends.

```
firepower# sh run snmp-server
snmp-server host inside 10.56.58.10 community ***** version 2c
snmp-server location null
snmp-server contact null
snmp-server community *****
```

- Make sure that SNMP traffic is being allowed through the FTD.

Navigate to Policies > Access Control and verify that you have a rule that allows SNMP traffic.



- Use packet capture to monitor SNMP traffic and identify any issues.

Enable capture with trace on the firewall:

```
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
```

For additional details check the SNMP Configuration Guide, [Configure and troubleshoot SNMP on Firepower FDM]

Related information

- Cisco Secure Firepower Device Manager Configuration Guide
- Cisco ASA Configurations Guide
- SNMP Configuration on Cisco Devices