Konfiguration von SNMP auf Site-to-Site-VPN über FDM-verwaltete Datenschnittstelle

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten
- Hintergrundinformationen

Konfigurieren

- Konfigurationen

Überprüfung

Fehlerbehebung

- Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration von SNMP für ein Remote-End über ein Site-to-Site-VPN an einer Datenschnittstelle eines FTD-Gerätes beschrieben.

Voraussetzungen

Bevor Sie mit der Konfiguration fortfahren, stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Grundlegendes Verständnis dieser Themen:
  - Cisco Firepower Threat Defense (FTD), verwaltet durch Firepower Device Manager (FDM).
  - Cisco Adaptive Security Appliance (ASA):
  - Simple Network Management Protocol (SNMP)
  - Virtual Private Network (VPN)
- Administratorzugriff auf FTD- und ASA-Geräte
- Stellen Sie sicher, dass Ihr Netzwerk in Betrieb ist, und verstehen Sie die möglichen Auswirkungen aller Befehle.

Anforderungen

- Cisco FTD verwaltet von FDM Version 7.2.7
- Cisco ASA Version 9.16
- SNMP-Serverdetails (einschließlich IP-Adresse, Community String)
- Standortübergreifende VPN-Konfigurationsdetails (einschließlich Peer-IP, Pre-Shared Key)

- FTD muss mindestens Version 6.7 sein, damit die REST-API für die Konfiguration von SNMP verwendet werden kann.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Firepower Threat Defense (FTD) verwaltet durch Firepower Device Manager (FDM) Version 7.2.7.
- Cisco Adaptive Security Appliance (ASA) Version 9.16.
- SNMP-Server (beliebige Standard-SNMP-Serversoftware)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

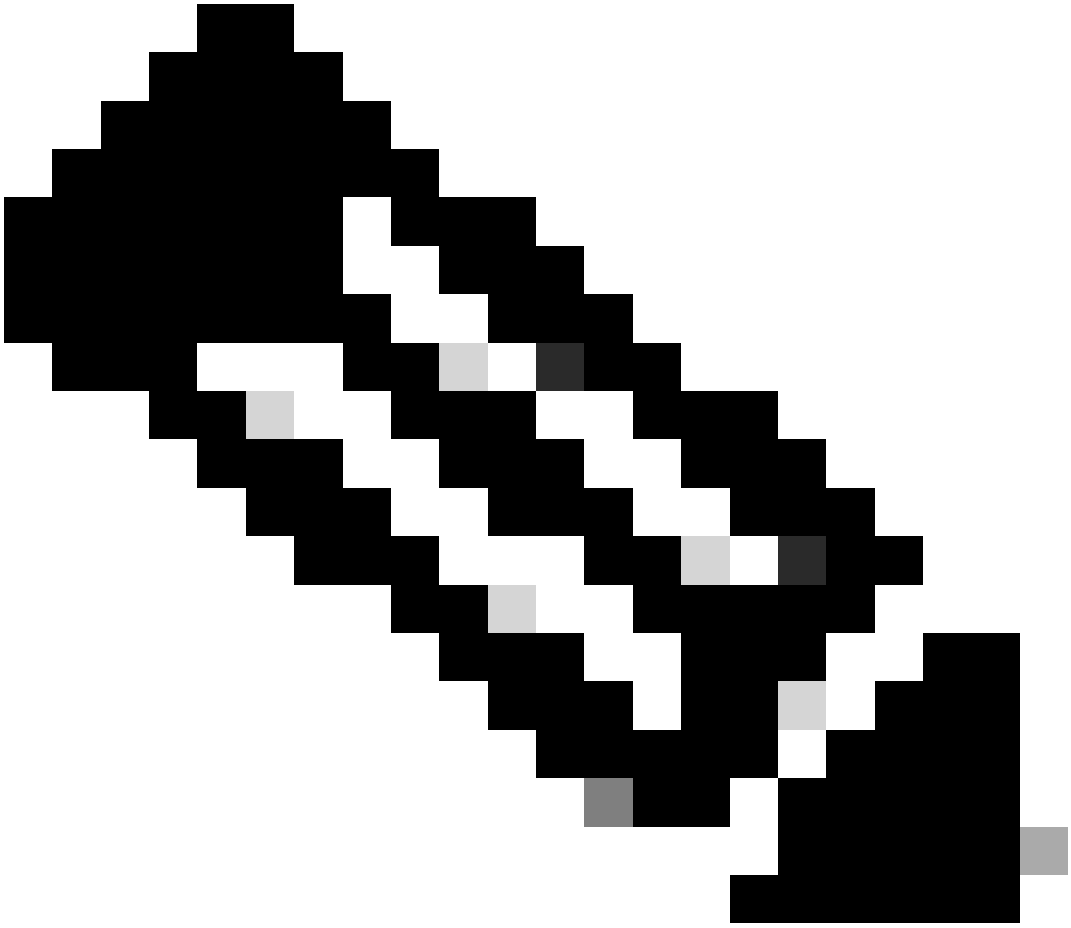
Hintergrundinformationen

Mit diesen Schritten können Netzwerkadministratoren die Remote-Überwachung ihrer Netzwerkgeräte sicherstellen.

SNMP (Simple Network Management Protocol) wird für die Netzwerkverwaltung und -überwachung verwendet. In dieser Konfiguration wird SNMP-Datenverkehr vom FTD über ein Site-to-Site-VPN, das mit einer ASA erstellt wurde, an einen Remote-SNMP-Server gesendet.

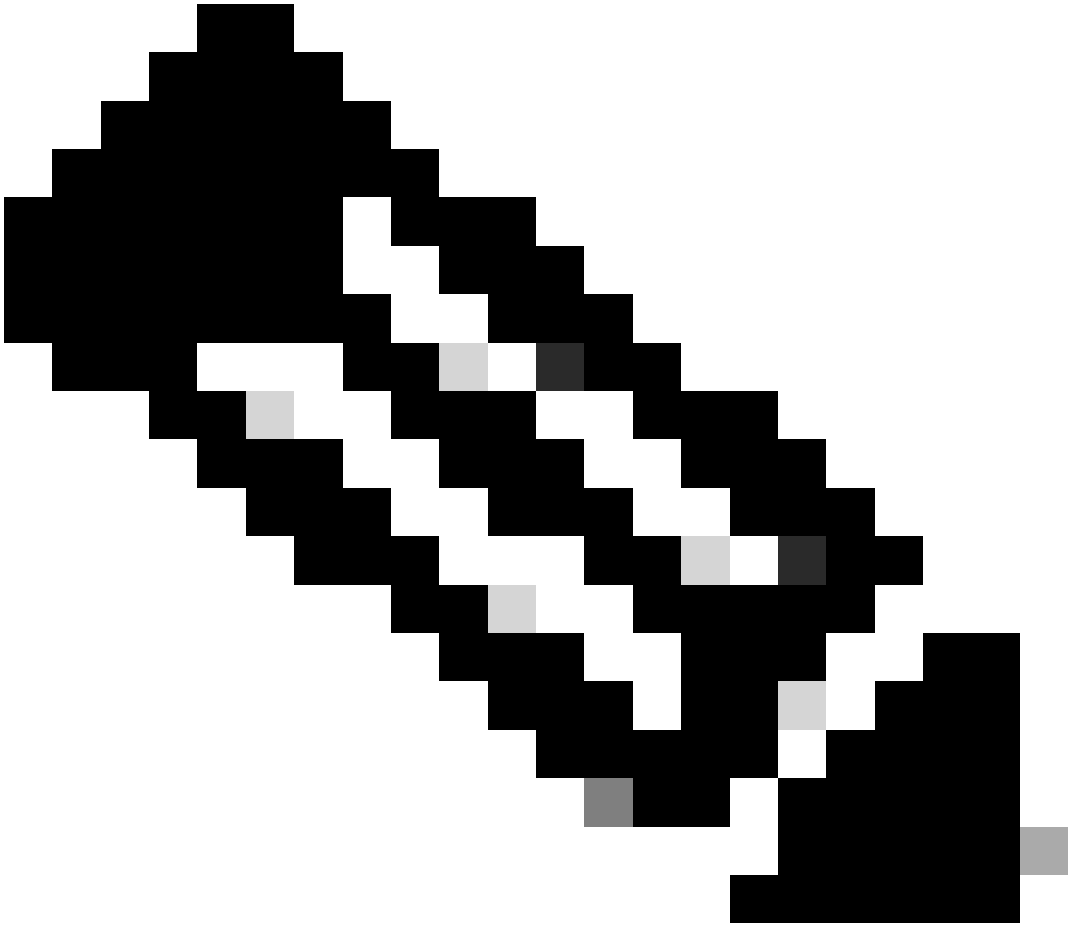
Dieses Handbuch soll Netzwerkadministratoren helfen, SNMP über ein Site-to-Site-VPN auf einer Datenschnittstelle eines FTD-Geräts für ein Remote-End zu konfigurieren. Diese Konfiguration ist für die Remote-Überwachung und -Verwaltung von Netzwerkgeräten nützlich. In dieser Konfiguration wird SNMP v2 verwendet, und SNMP-Datenverkehr wird von der FTD-Datenschnittstelle über ein Site-to-Site-VPN, das mit einer ASA erstellt wurde, an einen Remote-SNMP-Server gesendet.

Die verwendete Schnittstelle wird "inside" genannt, diese Konfiguration kann jedoch auf andere Arten von einsatzbereitem Datenverkehr angewendet werden und kann jede Schnittstelle der Firewall nutzen, die nicht die Schnittstelle ist, an der das VPN endet.



Hinweis: SNMP kann nur über die REST-API konfiguriert werden, wenn FTD Version 6.7 oder höher ausführt und von FDM verwaltet wird.

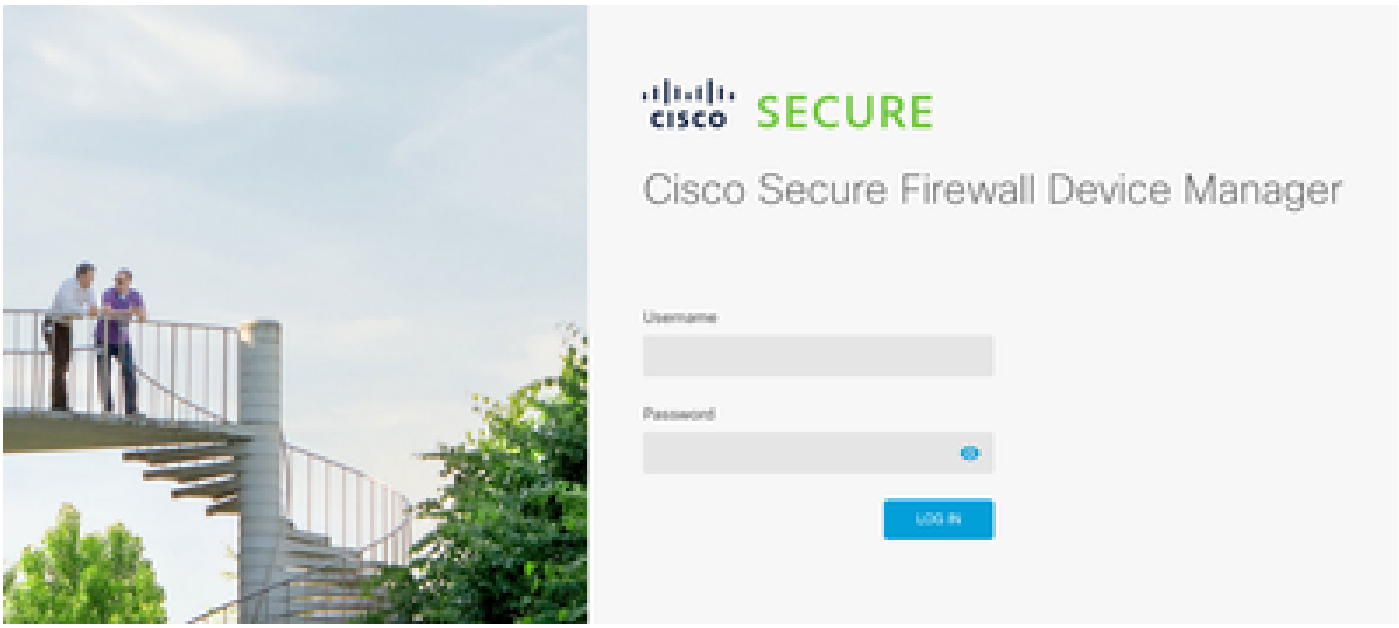
Konfigurieren



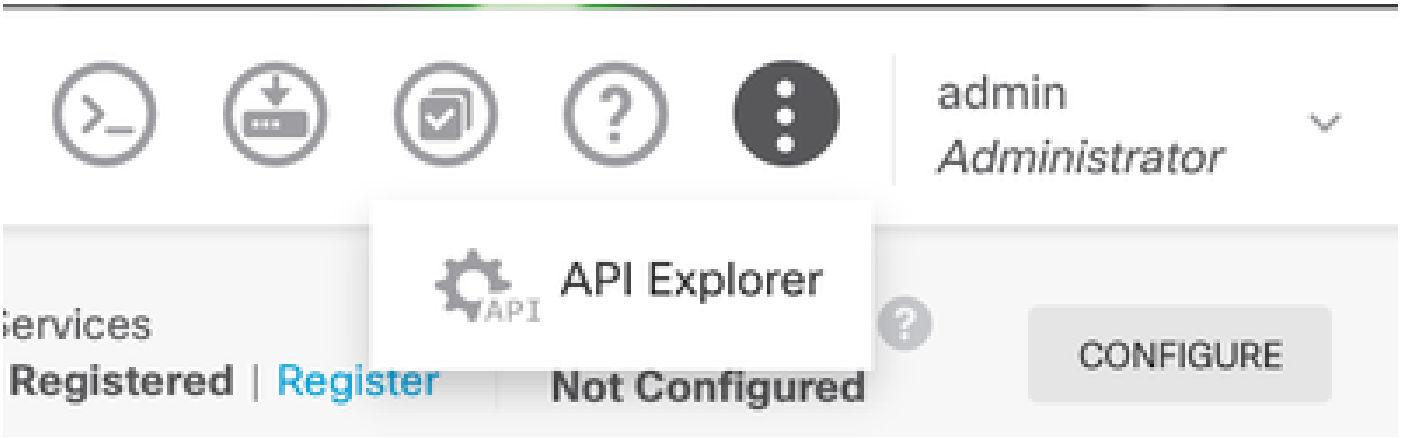
Hinweis: Bei dieser Konfiguration wird berücksichtigt, dass das standortübergreifende VPN bereits zwischen den Geräten konfiguriert ist. Weitere Informationen zum Konfigurieren des standortübergreifenden VPN finden Sie im Konfigurationsleitfaden. Konfiguration eines Site-to-Site-VPN auf von FDM verwaltetem FTD

Konfigurationen

1. Melden Sie sich bei Ihrem FTD an.



2. Navigieren Sie unter der Geräteübersicht zum API-Explorer.



3. SNMPv2 auf FTD konfigurieren

- Schnittstelleninformationen abrufen.

4. Scrollen Sie nach unten und wählen Sie die Schaltfläche Try it out!, um den API-Aufruf zu starten. Bei einem erfolgreichen Anruf wird der Antwortcode 200 zurückgegeben.

TRY IT OUT! Hide Response

Curl

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

Request URL

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

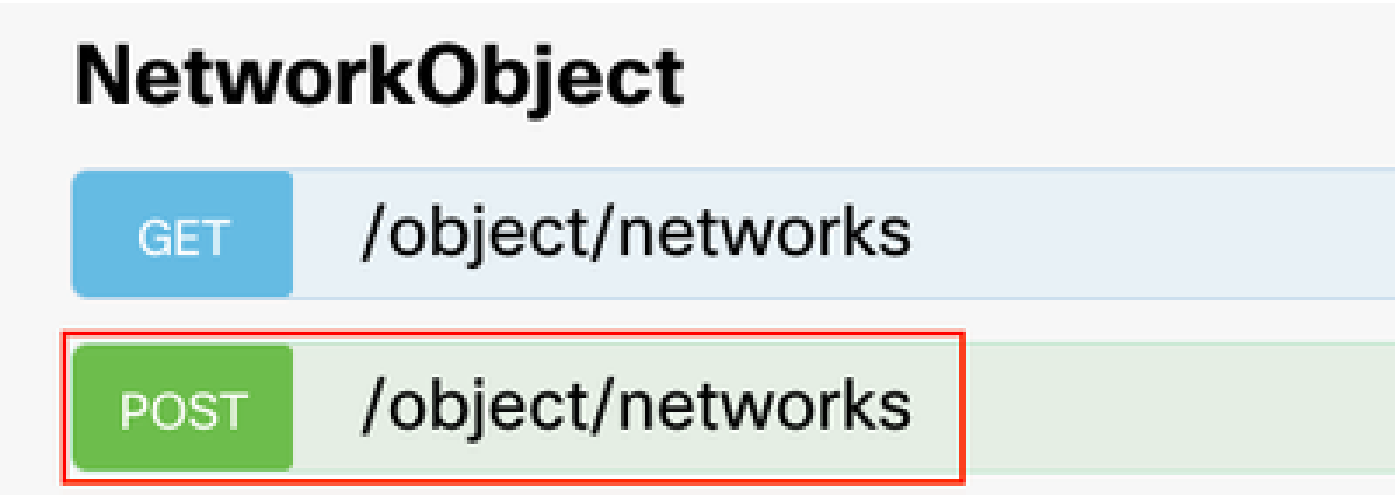
Response Body


```
    },
    {
      "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"
      },
```

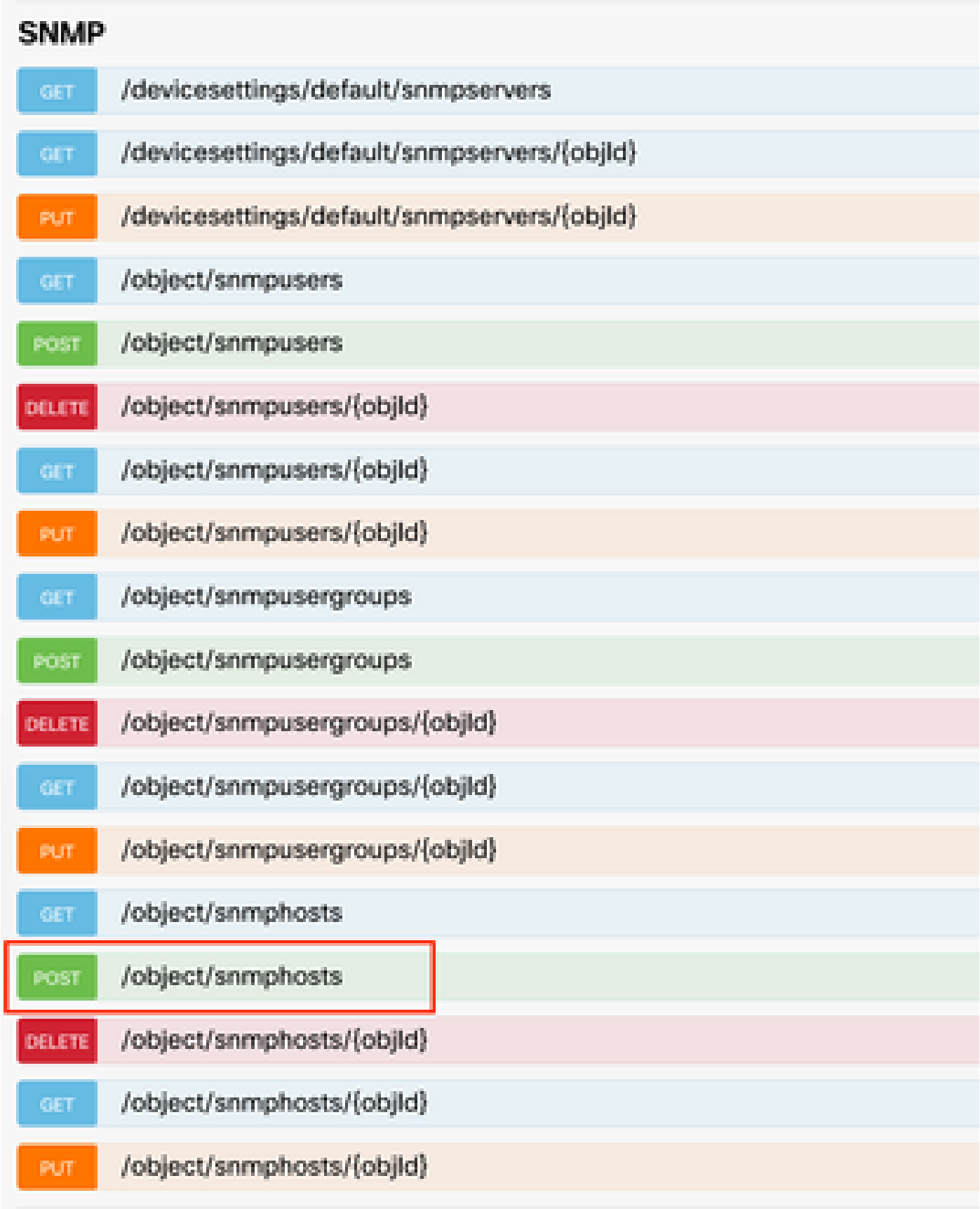

Response Code

```
200
```

- Erstellen einer Netzwerkobjektkonfiguration für den SNMP-Host

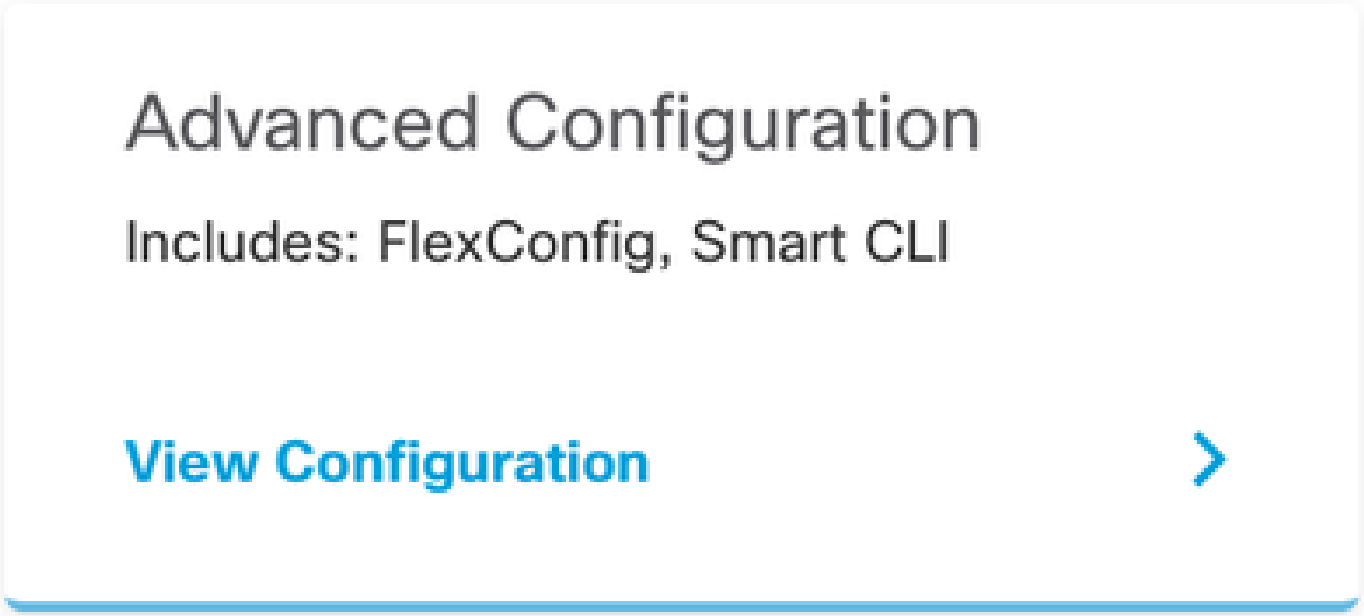


- Erstellen Sie ein neues SNMPv2c-Hostobjekt.

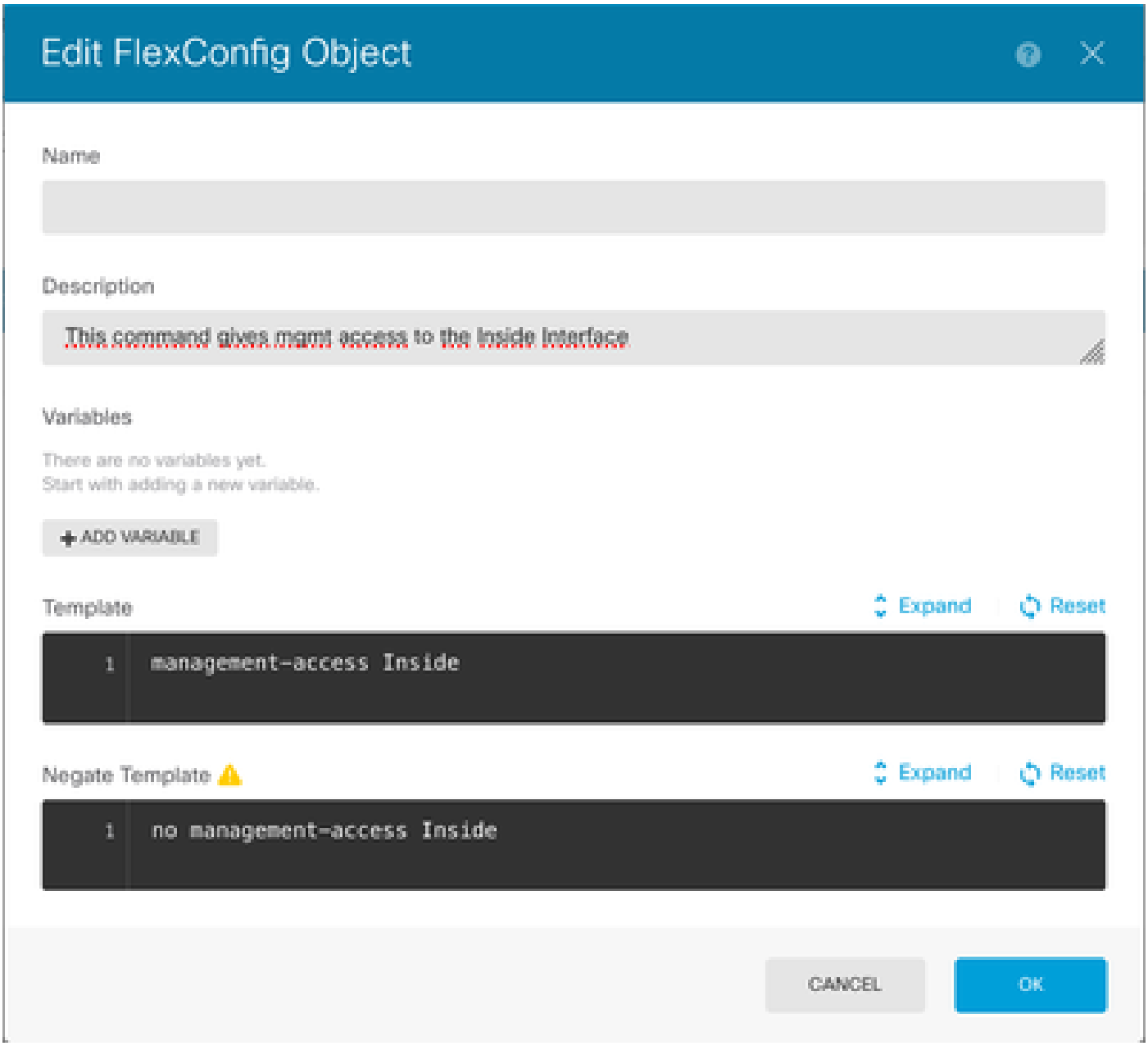


Weitere Informationen finden Sie im Konfigurationsleitfaden, SNMP konfigurieren und Fehlerbehebung für FirePOWER FDM durchführen.

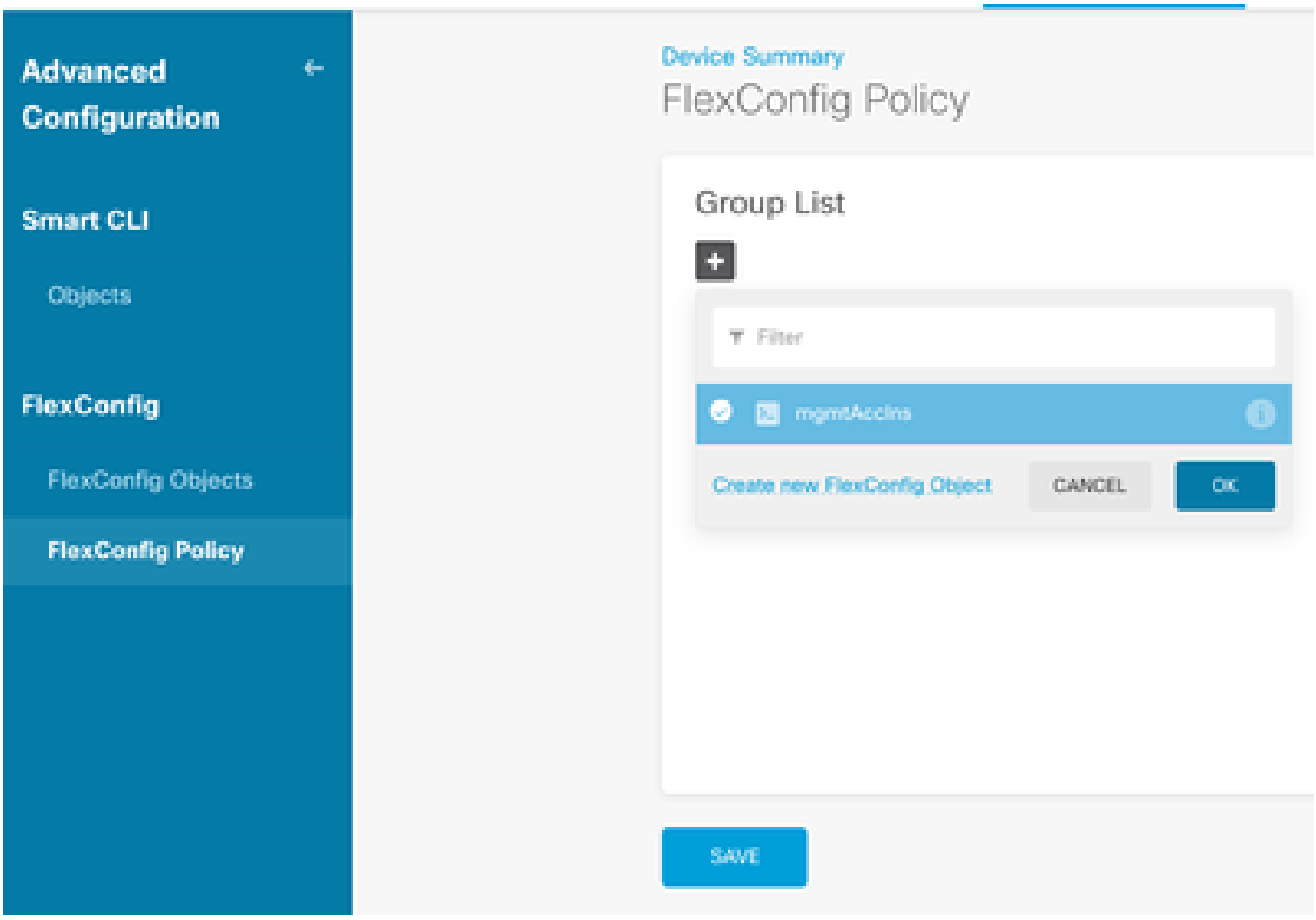
5. Sobald SNMP auf dem Gerät konfiguriert ist, navigieren Sie zu Gerät im Abschnitt Erweiterte Konfiguration und wählen Konfiguration anzeigen.



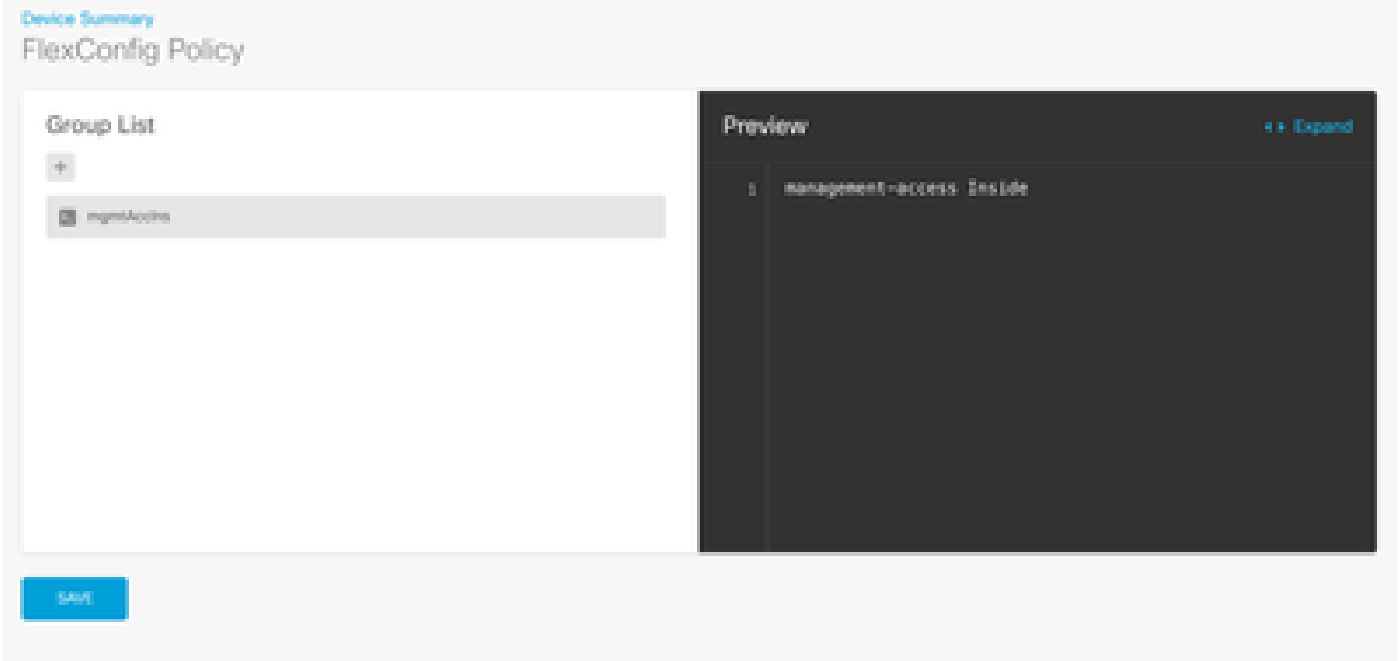
6. Wählen Sie im Abschnitt FlexConfig die Option FlexConfig-Objekte, und erstellen Sie ein neues Objekt, benennen Sie es, und fügen Sie den Befehl management-access im Vorlagenabschnitt hinzu, geben Sie die Schnittstelle an, und fügen Sie den Befehl negation im Vorlagennegationsteil hinzu.



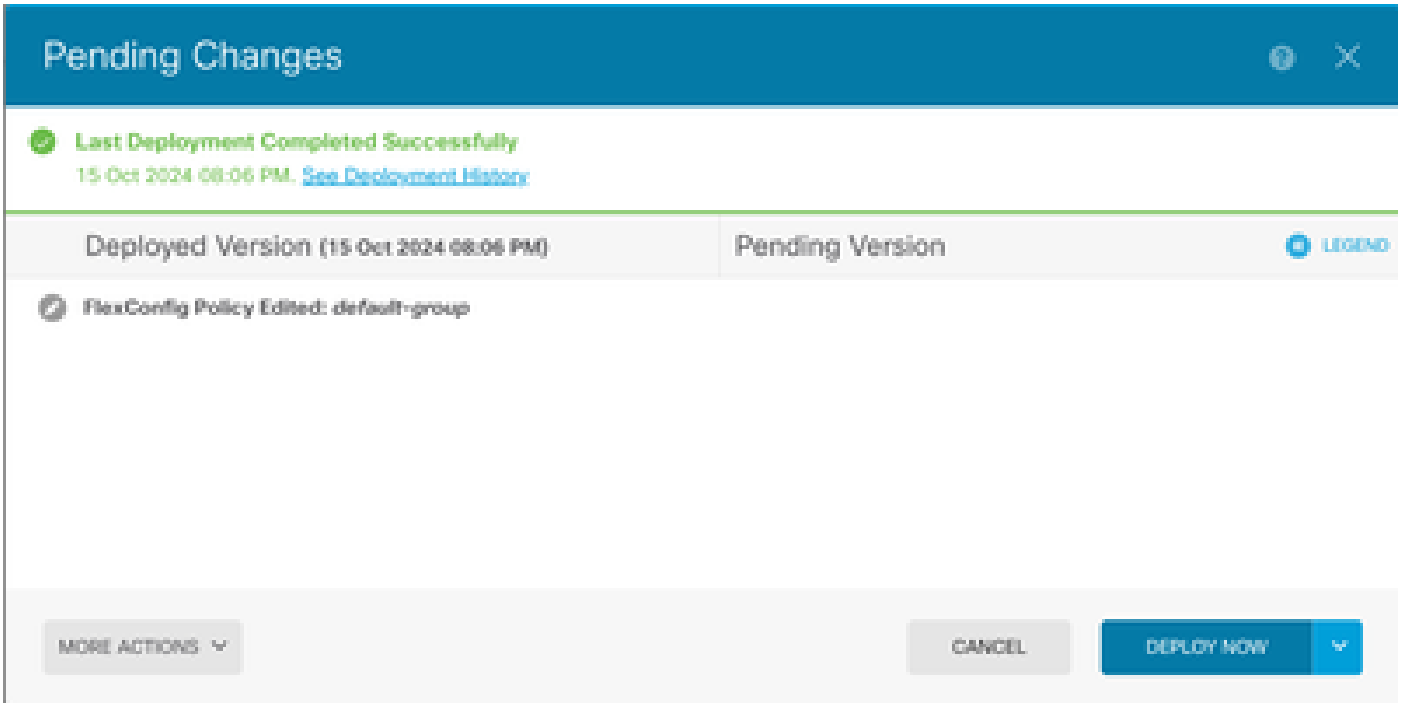
7. Wählen Sie im Abschnitt FlexConfig die Option FlexConfig Policy (FlexConfig-Richtlinie) aus, klicken Sie auf das Symbol zum Hinzufügen, wählen Sie das im vorherigen Schritt erstellte flexConfig-Objekt aus, und wählen Sie OK aus.

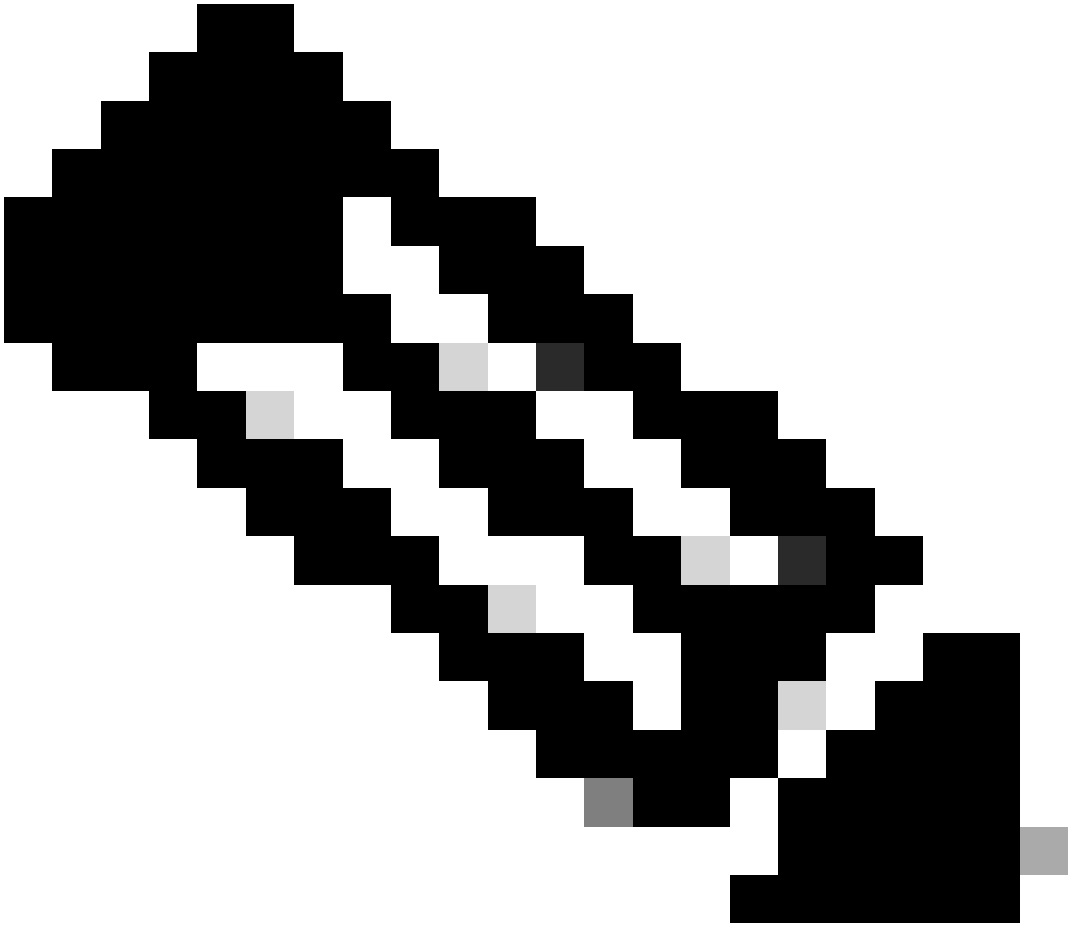


8. Dann wird eine Vorschau der auf das Gerät anzuwendenden Befehle angezeigt. Wählen Sie Speichern aus.



9. Stellen Sie die Konfiguration bereit, wählen Sie das Bereitstellungssymbol aus, und klicken Sie auf Jetzt bereitstellen.


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



Hinweis: Stellen Sie sicher, dass die Aufgabe zufriedenstellend abgeschlossen wurde. Überprüfen Sie die Aufgabenliste, um sie zu bestätigen.

Überprüfung

Um die Konfiguration zu überprüfen, führen Sie diese Prüfungen durch, melden Sie sich über SSH oder die Konsole beim FTD an, und führen Sie die folgenden Befehle aus:

- Überprüfen Sie, ob die aktuelle Konfiguration des Geräts die vorgenommenen Änderungen enthält.

```
> 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
```

- Führen Sie einen Test vom SNMP-Tester aus, und stellen Sie sicher, dass er erfolgreich abgeschlossen wurde.

Fehlerbehebung

Wenn Probleme auftreten, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass der VPN-Tunnel betriebsbereit ist. Mit dem folgenden Befehl können Sie den VPN-Tunnel überprüfen.

```
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
```

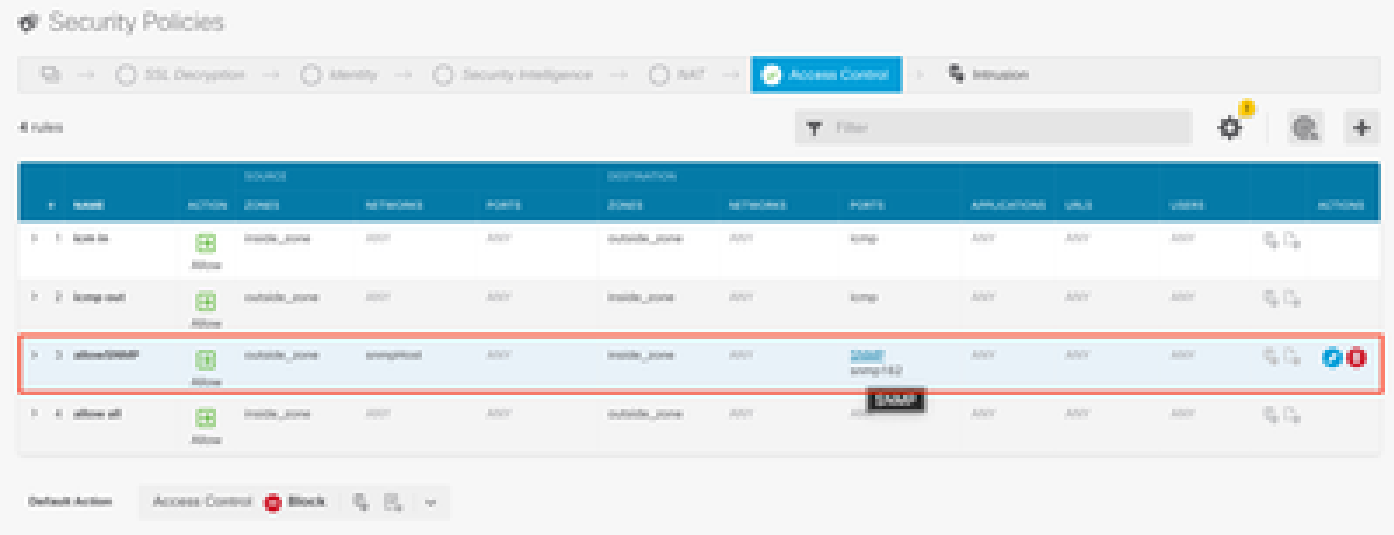
Eine detaillierte Anleitung zum Debuggen von IKEv2-Tunneln finden Sie hier: [So debuggen Sie IKEv2-VPNs]

- Überprüfen Sie die SNMP-Konfiguration, und stellen Sie sicher, dass der Community-String und die Einstellungen für die Zugriffskontrolle auf beiden Seiten korrekt sind.

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

- Stellen Sie sicher, dass SNMP-Datenverkehr über die FTD zugelassen wird.

Navigieren Sie zu Richtlinien > Zugriffskontrolle, und stellen Sie sicher, dass Sie über eine Regel verfügen, die SNMP-Datenverkehr zulässt.



- Verwenden Sie die Paketerfassung, um den SNMP-Datenverkehr zu überwachen und etwaige Probleme zu identifizieren.

Erfassung mit Ablaufverfolgung auf der Firewall aktivieren:

```
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
```

Weitere Informationen finden Sie im SNMP-Konfigurationsleitfaden, SNMP konfigurieren und Fehlerbehebung für FirePOWER FDM durchführen.

Zugehörige Informationen

- Konfigurationsleitfaden für Cisco Secure FirePOWER Device Manager
- Cisco ASA - Konfigurationsleitfaden
- SNMP-Konfiguration auf Cisco Geräten

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.