SNMP configureren op site-to-site VPN op FDM-beheerde data-interface

Inhoud

Inleiding

Dit document beschrijft het configureren van SNMP naar een extern einde via een site-to-site VPN op een data-interface van een FTD-interface voor apparaatgegevens.

Voorwaarden

Zorg ervoor dat u aan de volgende voorwaarden voldoet voordat u overgaat tot de configuratie:

- Basiskennis van deze onderwerpen:
  - Cisco Firepower Threat Defence (FTD), beheerd door Firepower Device Manager (FDM).
  - Cisco adaptieve security applicatie (ASA).
  - Simple Network Management Protocol (SNMP).
  - Virtual Private Network (VPN).
- Administratieve toegang tot de FTD- en ASA-apparatuur.
- Zorg ervoor dat uw netwerk live is en u begrijpt de mogelijke impact van elke opdracht.

Vereisten

- Cisco FTD beheerd door FDM versie 7.2.7
- Cisco ASA versie 9.16
- SNMP-servergegevens (inclusief IP-adres, community-string)
- Site-to-site VPN-configuratiegegevens (inclusief peer-IP, vooraf gedeelde sleutel)
- FTD moet ten minste versie 6.7 zijn om REST API te kunnen gebruiken om SNMP te configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firepower Threat Defence (FTD), beheerd door Firepower Device Manager (FDM), versie 7.2.7.
- Cisco adaptieve security applicatie (ASA) versie 9.16.
- SNMP-server (elke standaard SNMP-serversoftware)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

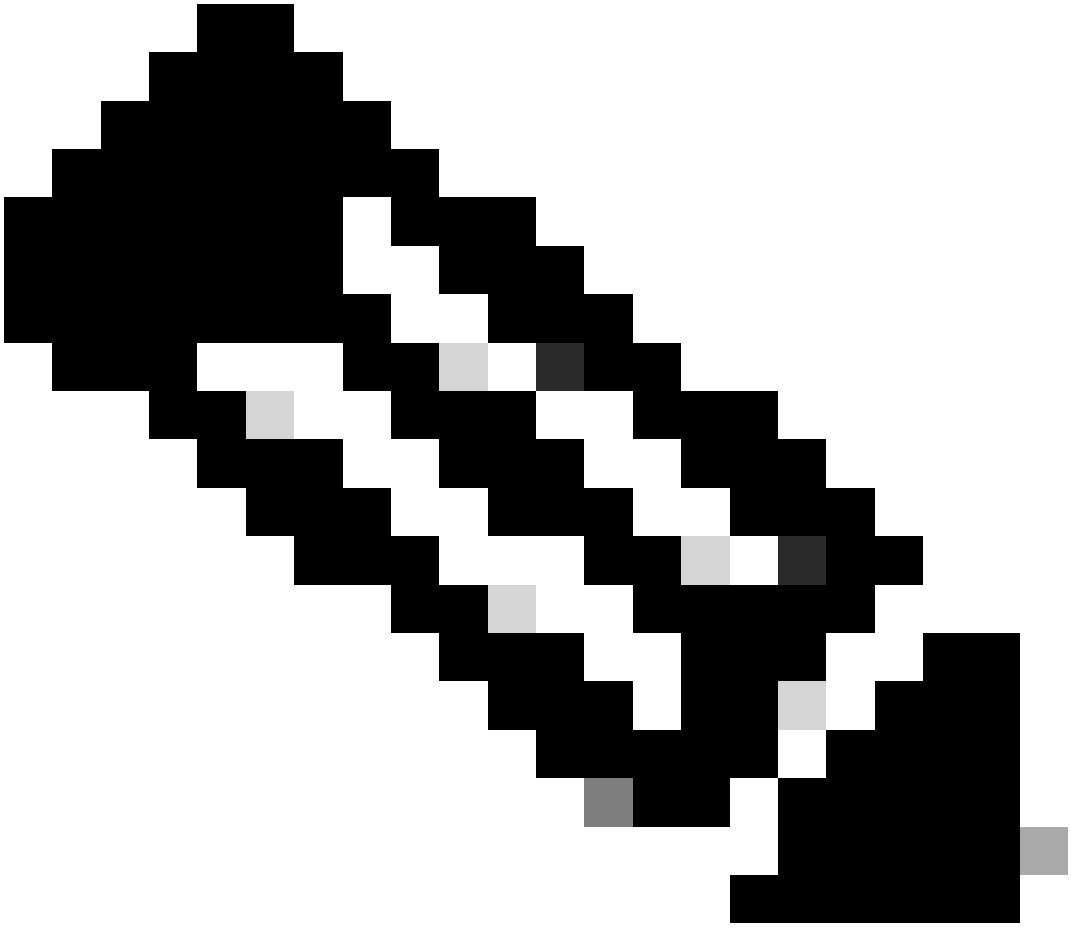
Achtergrondinformatie

Met deze stappen kunnen netwerkbeheerders de bewaking van hun netwerkapparaat op afstand garanderen.

SNMP (Simple Network Management Protocol) wordt gebruikt voor netwerkbeheer en -bewaking. In deze installatie wordt SNMP-verkeer vanaf de FTD naar een externe SNMP-server verzonden via een site-to-site VPN dat met een ASA is ingesteld.

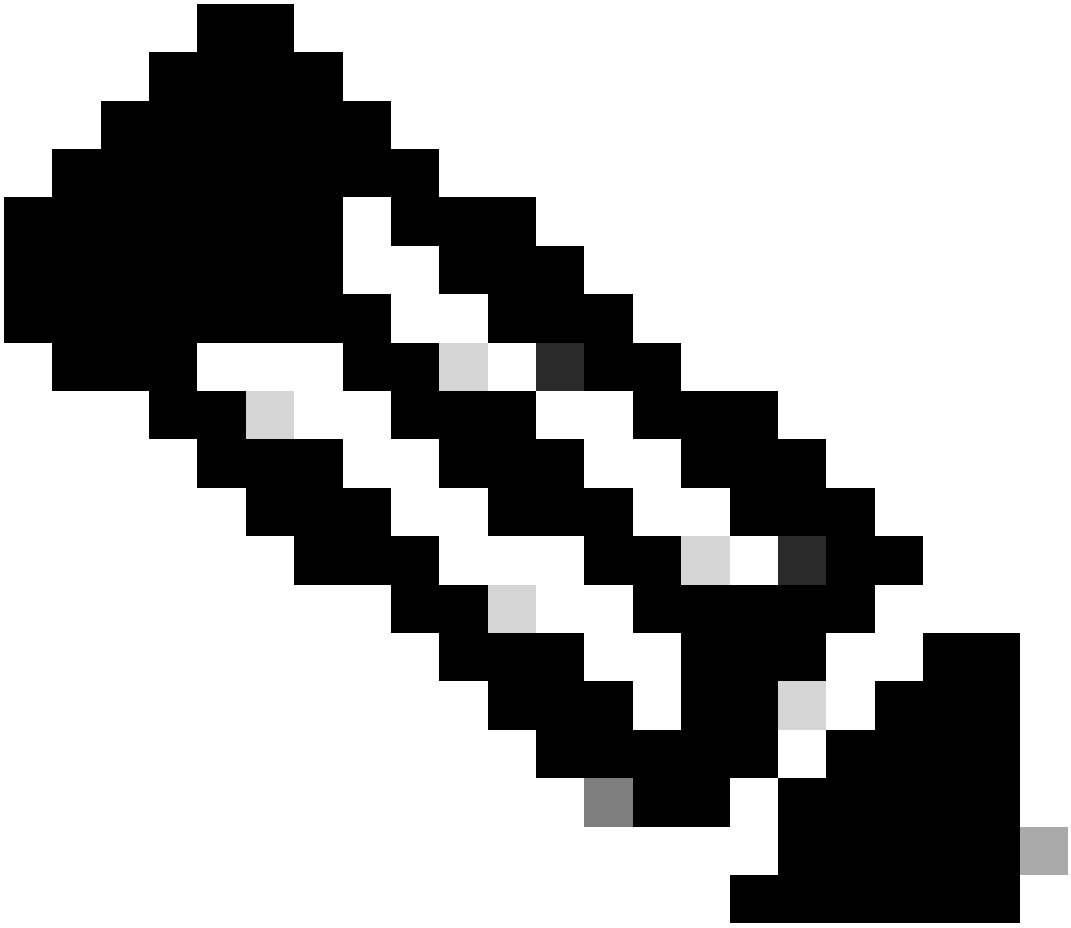
Deze handleiding is bedoeld om netwerkbeheerders te helpen SNMP te configureren naar een extern eindpunt via een site-to-site VPN op een data-interface van een FTD-apparaat. Deze instelling is handig om netwerkapparaten op afstand te bewaken en te beheren. In deze installatie wordt SNMP v2 gebruikt en wordt SNMP-verkeer vanuit de FTD-gegevensinterface naar een externe SNMP-server verzonden via een site-to-site VPN die met een ASA is ingesteld.

De gebruikte interface wordt "inside" genoemd, maar deze configuratie kan op andere typen "to-the-box" verkeer worden toegepast en kan elke interface van de firewall gebruiken die niet de interface is waar VPN eindigt.



Opmerking: SNMP kan alleen worden geconfigureerd via REST API als FTD versie 6.7 en hoger draait, en wordt beheerd door FDM.

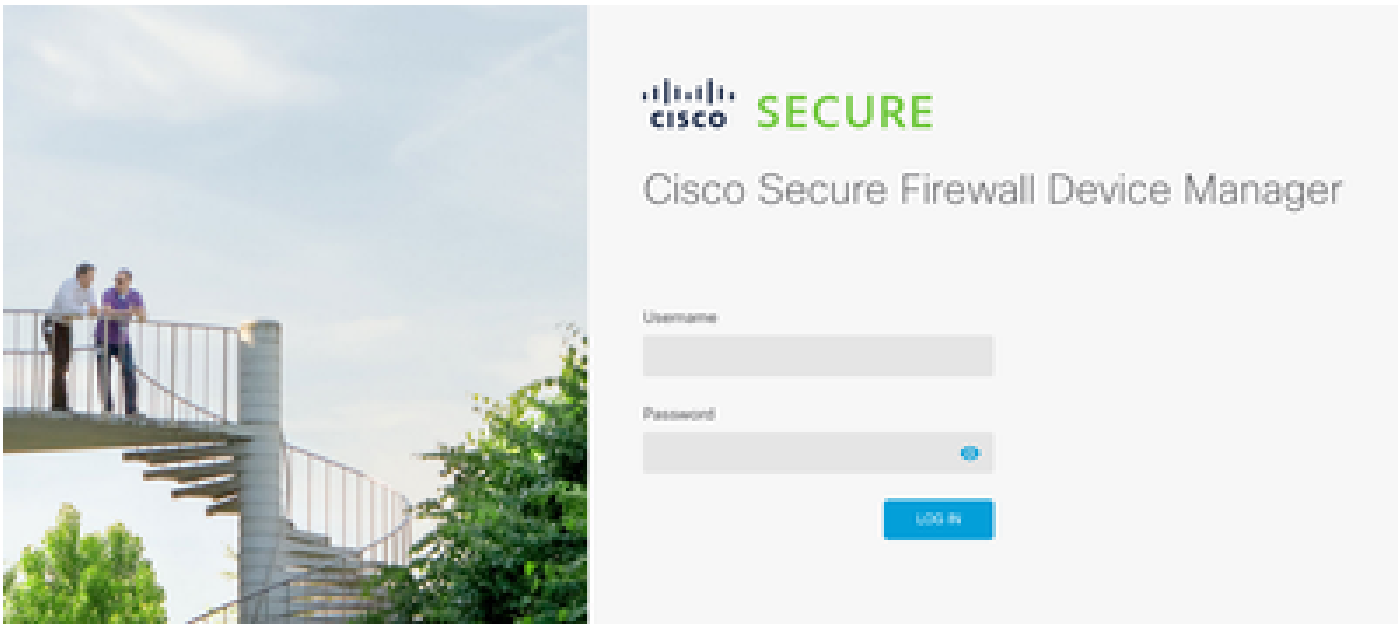
Configureren



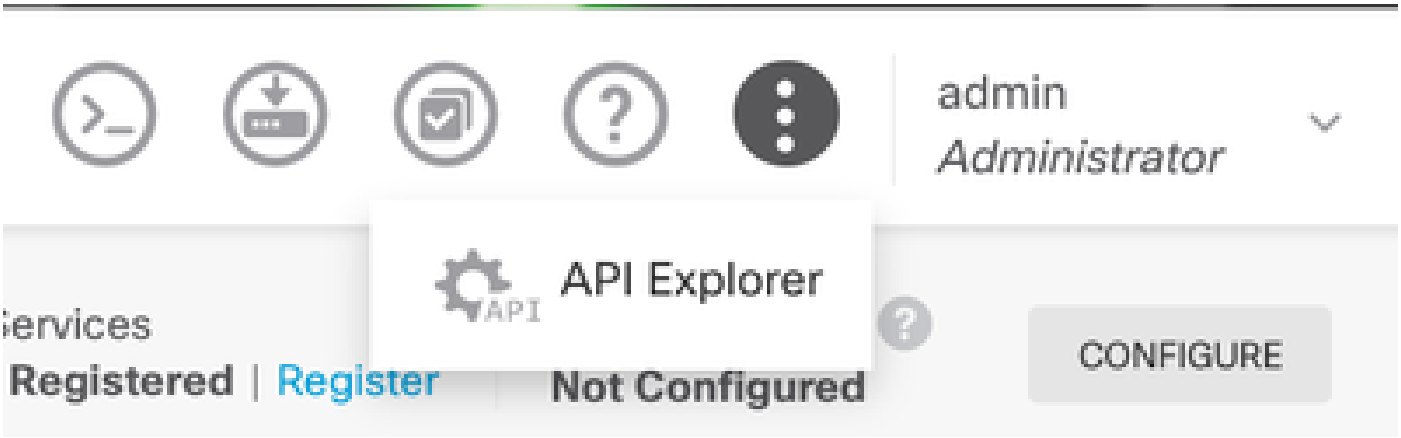
Opmerking: deze configuratie beschouwt de site-to-site VPN al tussen de apparaten geconfigureerd. Voor extra details hoe u de site aan site VPN kunt configureren, raadpleegt u de configuratiehandleiding. Site-to-site VPN configureren op FTD beheerd door FDM

Configuraties

1. Log in op uw FTD.



2. Ga onder het Apparaatoverzicht naar de API-verkenner.



3. SNMPv2 op FTD configureren

- Krijg interfaceinformatie.

4. Scroll naar beneden en selecteer de knop Try it out! om de API te bellen. Een succesvolle oproep retourneert 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

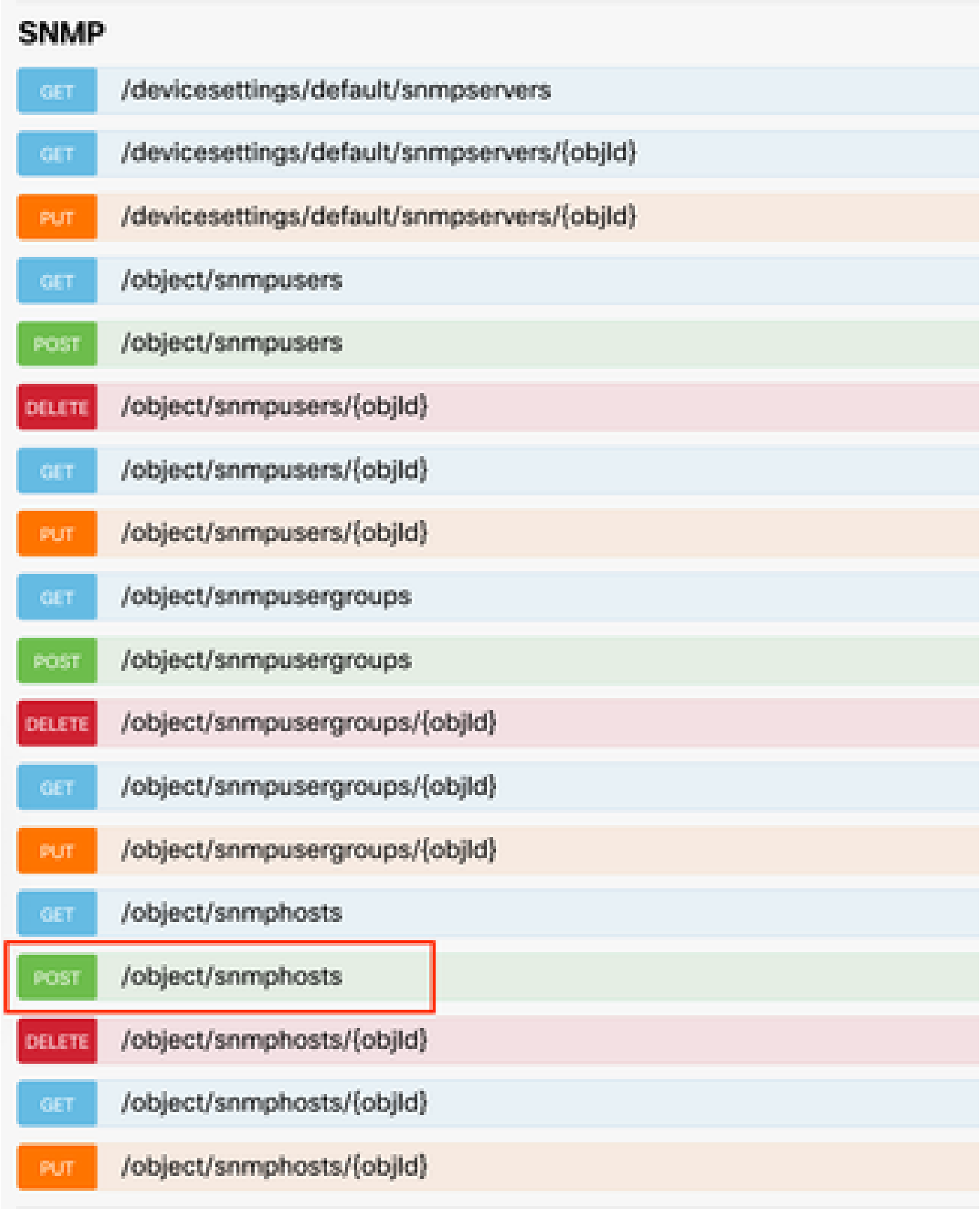

```
    },
    {
      "version": "mqjiipiswsgsx",
      "name": "inside",
      "description": null,
      "hardwareName": "GigabitEthernet0/1",
      "monitorInterface": false,
      "ipv4": {
        "ipType": "STATIC",
        "defaultRouteUsingDHCP": false,
        "dhcpRouteMetric": null,
    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


Response Code

```
200
```

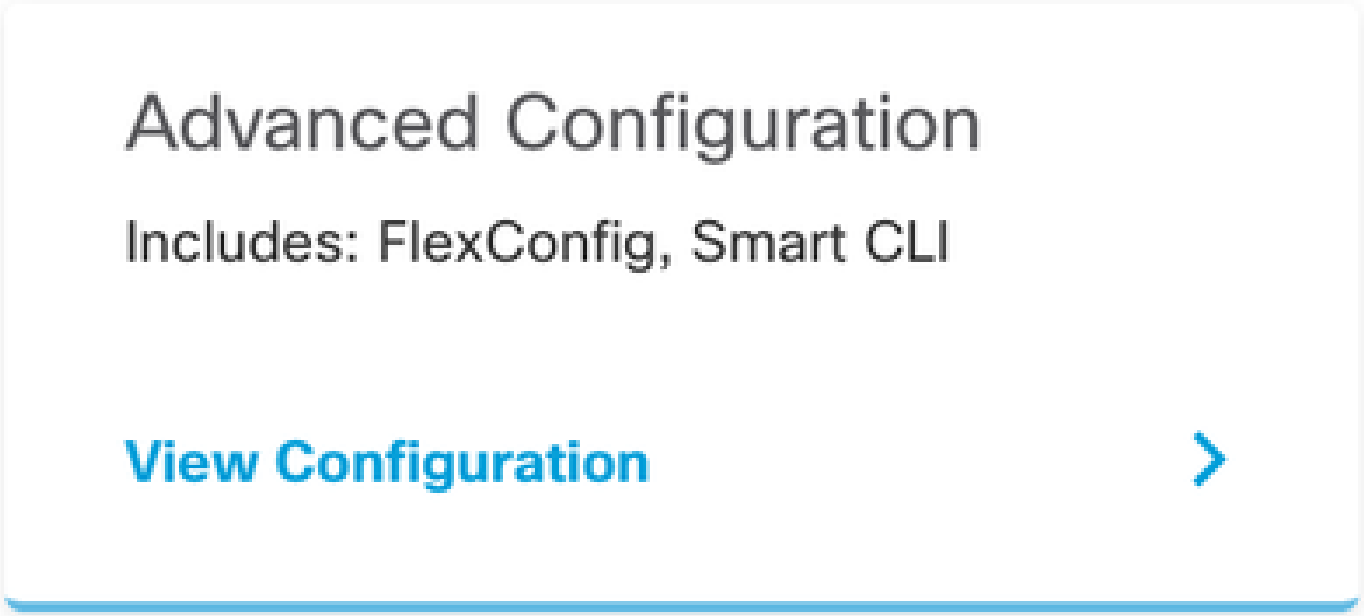
- Maak een Network Object Config voor de SNMP-host.

- Maak een nieuw SNMPv2c-hostobject.

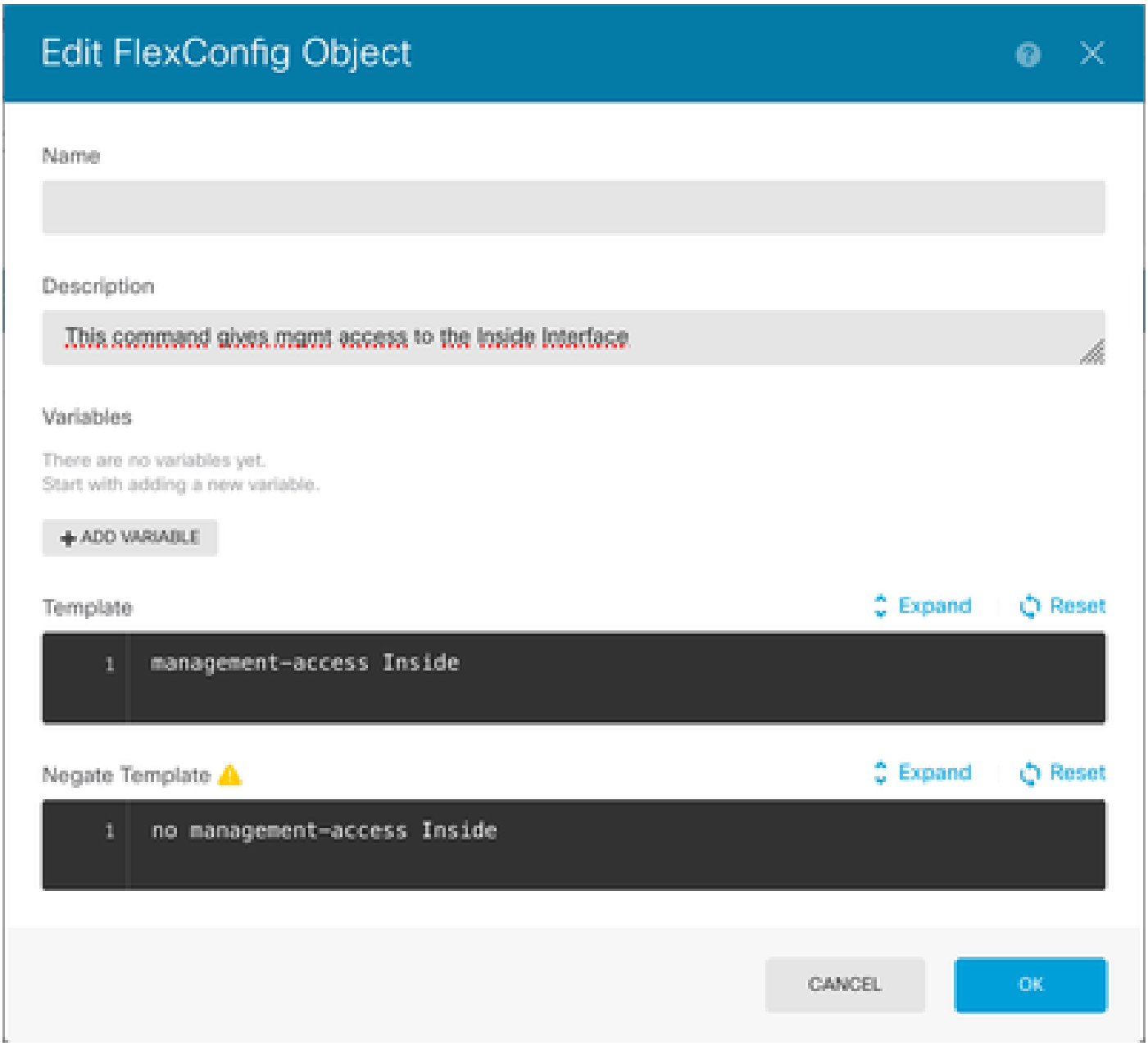


Controleer voor meer informatie de Configuratiehandleiding, configureer en probleemoplossing SNMP op Firepower FDM

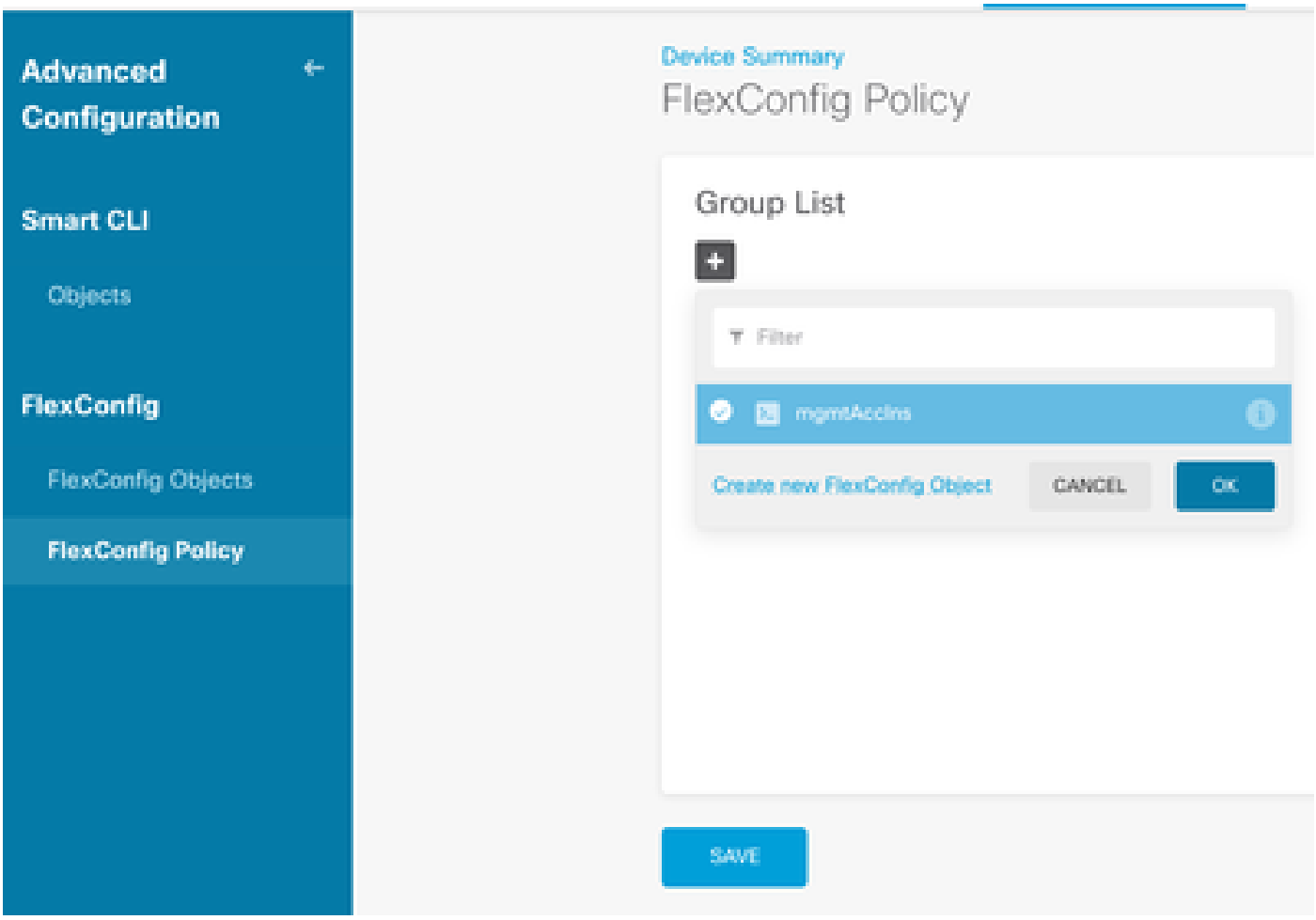
5. Nadat SNMP op het apparaat is geconfigureerd, navigeer dan naar apparaat in het gedeelte Advanced Configuration en selecteer View Configuration.



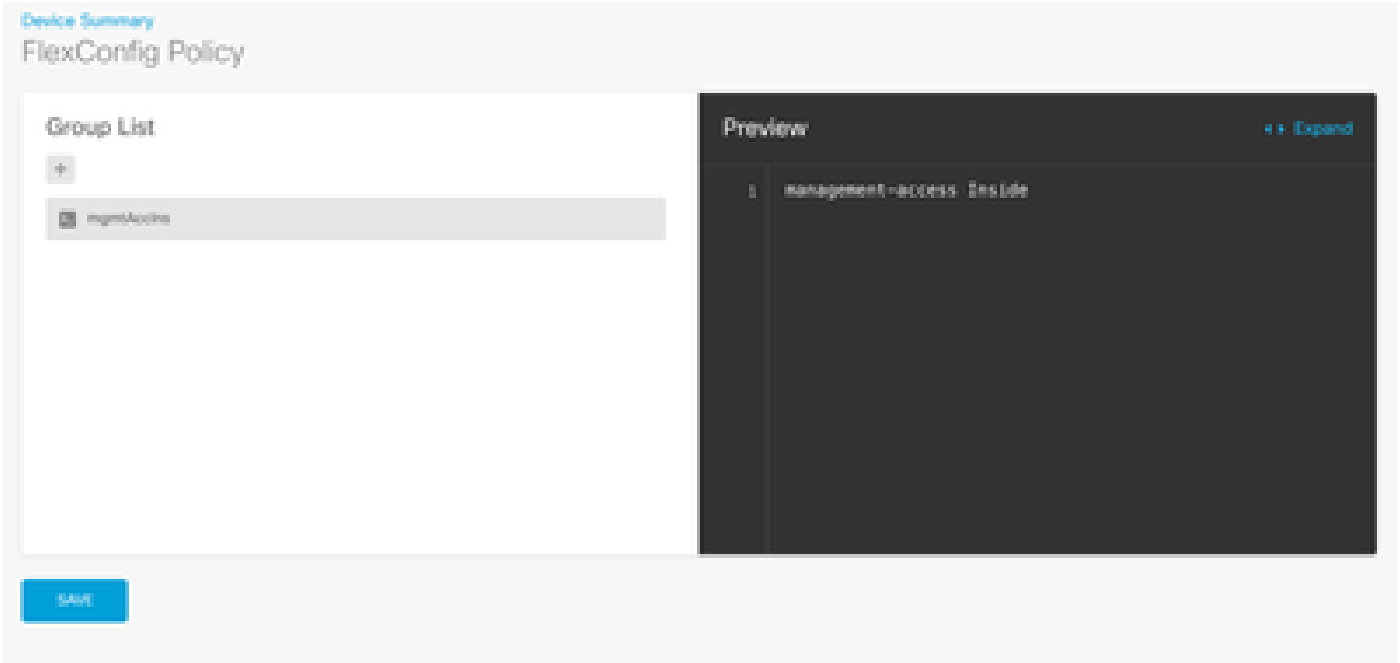
6. Selecteer in het gedeelte FlexConfig de optie FlexConfig-objecten en maak een nieuw object, geef het een naam en voeg de opdracht voor de toegang tot het beheer in het gedeelte over de sjabloon toe, specificeer de interface en voeg de opdrachtnegatie toe in het gedeelte over de negatie van de sjabloon.



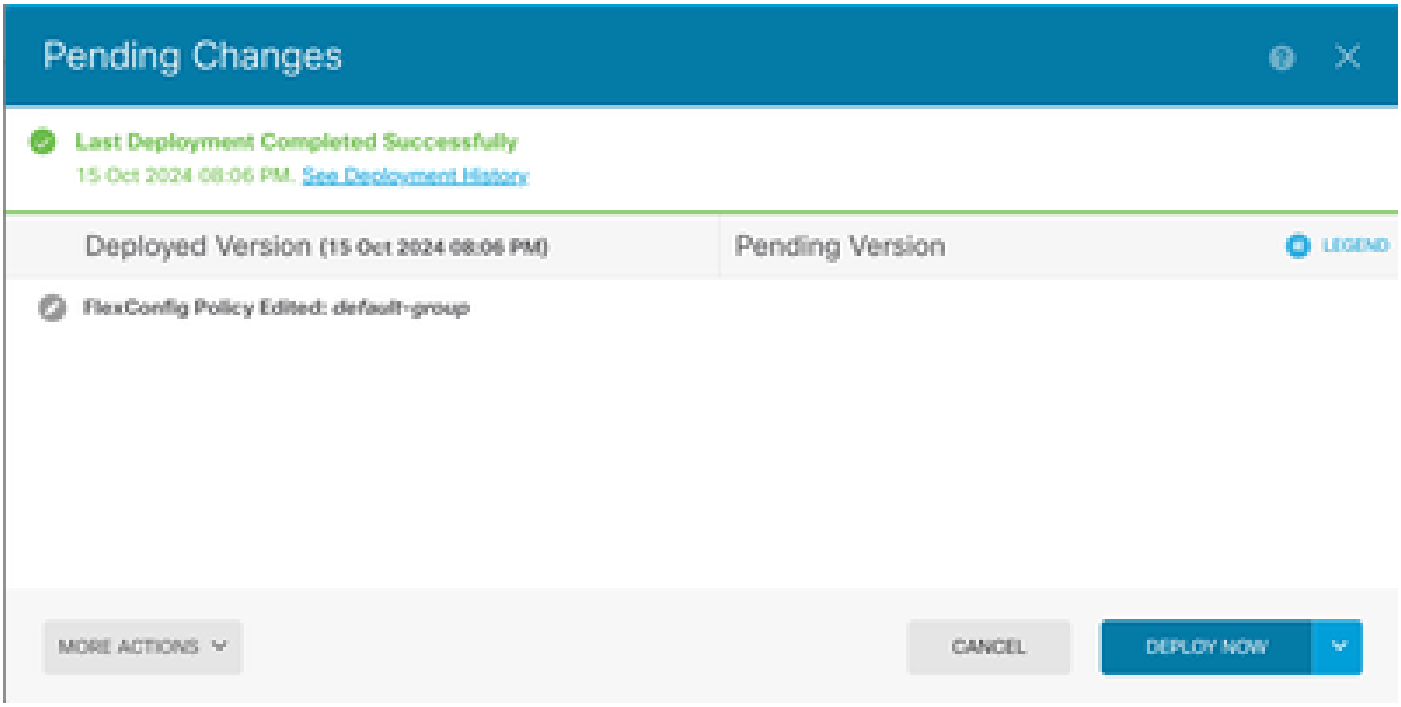
7. Selecteer in het gedeelte FlexConfig de optie FlexConfig-beleid, klik op het pictogram Add en selecteer het object flexConfig dat we in de vorige stap hebben gemaakt, en selecteer OK.

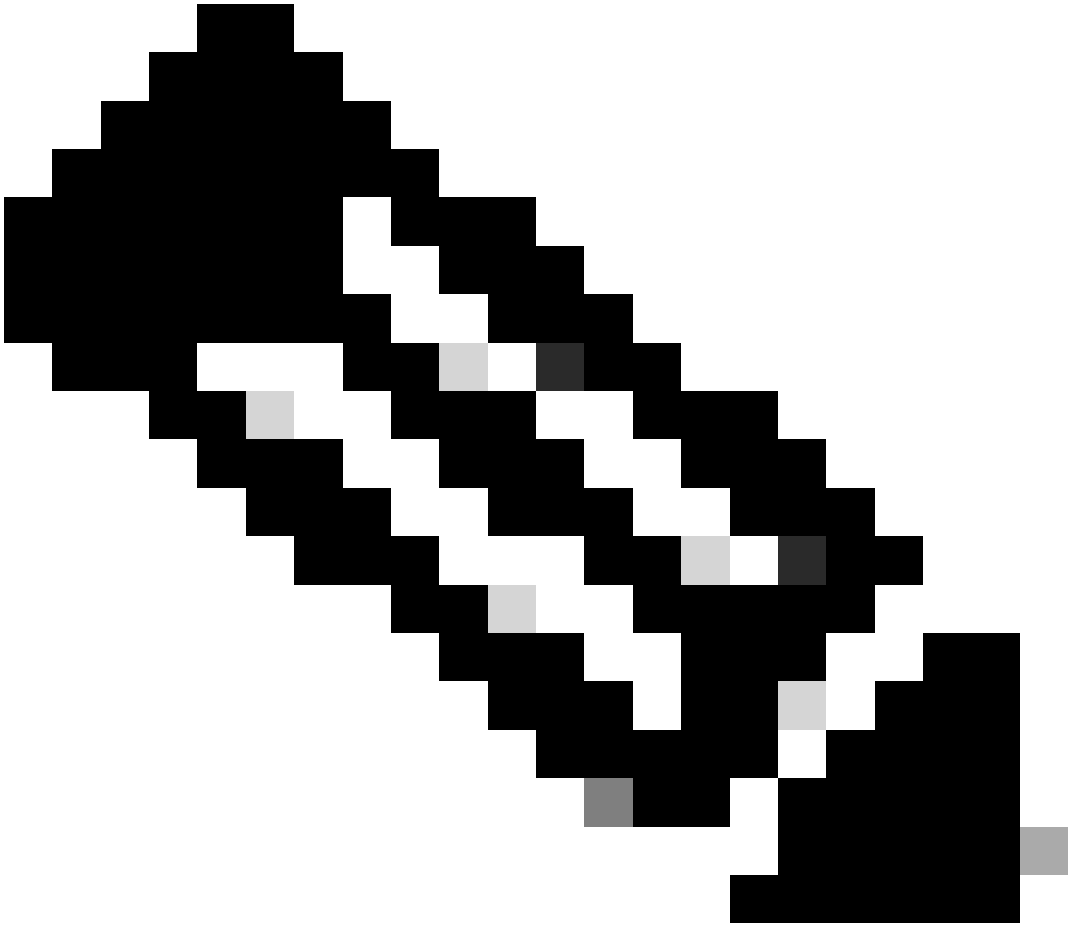


8. Vervolgens wordt een voorbeeld weergegeven van de opdrachten die op het apparaat moeten worden toegepast. Selecteer Opslaan.



9. Stel de configuratie op, selecteer het implementatiepictogram en klik op nu implementeren.


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



Opmerking: controleer of de taak naar tevredenheid is voltooid en controleer de taaklijst om deze te bevestigen.

Verifiëren

Om de configuratie te verifiëren, voer deze controles uit, log in aan de FTD via SSH of console, en voer deze opdrachten uit:

- Controleer dat de lopende configuratie van het apparaat de wijzigingen bevat die wij hebben aangebracht.

```
> 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
```

- Voer een test uit op de SNMP-tester en controleer of deze met succes is voltooid.

Problemen oplossen

Als u problemen ondervindt, moet u deze stappen overwegen:

- Zorg dat de VPN-tunnel actief is, u kunt deze opdracht uitvoeren om de VPN-tunnel te verifiëren.

```
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
```

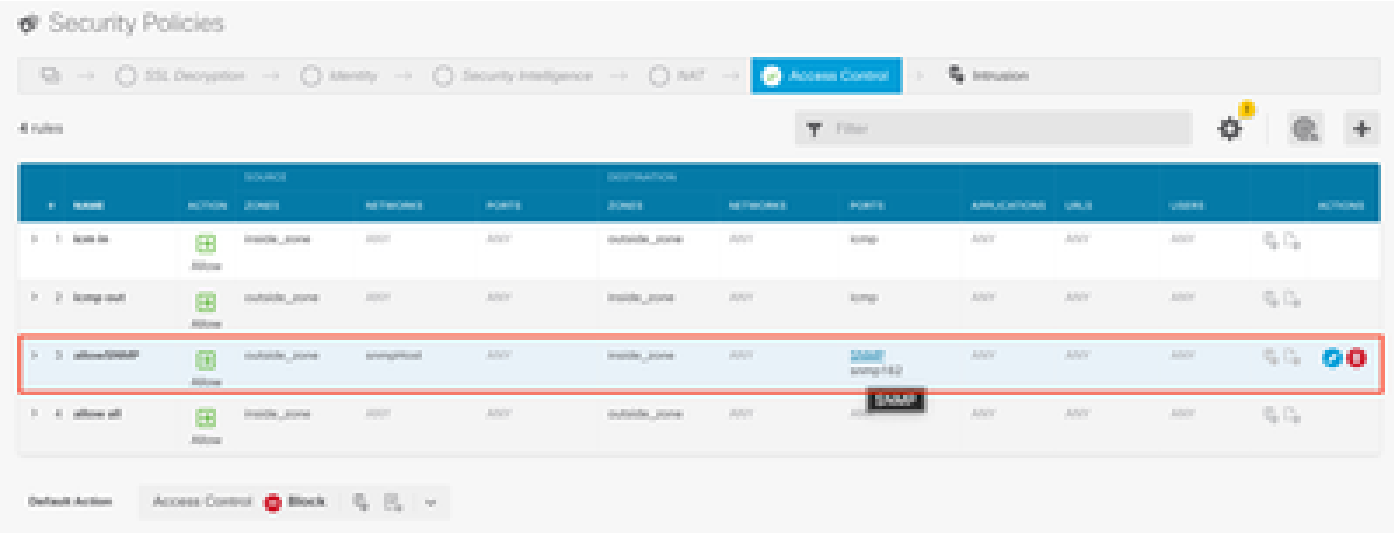
Hier vindt u een gedetailleerde handleiding over het debuggen van IKEv2-tunnels: Hoe IKEv2 VPN's te debuggen

- Controleer de SNMP-configuratie en zorg ervoor dat de community-string en toegangscontrole instellingen aan beide uiteinden correct zijn.

FirePOWER# sh SNMP-server uitvoeren
SNMP-server host binnen 10.56.58.10 community ***** versie 2c
Locatie van SNMP-server ongeldig
contact null voor snmp-server
SNMP-server *****

- Zorg ervoor dat SNMP-verkeer via de FTD is toegestaan.

Navigeer naar Beleid > Toegangsbeheer en controleer of u een regel hebt die SNMP-verkeer toestaat.



- Gebruik pakketopname om SNMP-verkeer te controleren en eventuele problemen te identificeren.

Opname met overtrekken op de firewall inschakelen:

```
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
```

Voor meer informatie kunt u de SNMP-configuratiehandleiding raadplegen [en SNMP op Firepower FDM configureren en problemen oplossen]

Gerelateerde informatie

- Configuratiehandleiding voor Cisco Secure Firepower Device Manager
- Cisco ASA-configuratiegids
- SNMP-configuratie op Cisco-apparaten

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.