Configuration du protocole SNMP sur le VPN site à site sur l'interface de données gérée par FDM

Table des matières

Introduction

Ce document décrit la configuration de SNMP à une extrémité distante via un VPN site à site sur une interface de données d'une interface de données de périphérique FTD.

Conditions préalables

Avant de poursuivre la configuration, assurez-vous que les conditions suivantes sont réunies :

- Compréhension de base de ces sujets :
  - Cisco Firepower Threat Defense (FTD) géré par Firepower Device Manager (FDM).
  - Appareil de sécurité adaptatif Cisco (ASA).
  - Protocole SNMP (Simple Network Management Protocol).
  - Réseau privé virtuel (VPN).
- Accès administratif aux périphériques FTD et ASA.
- Assurez-vous que votre réseau est actif et que vous comprenez l'impact potentiel de toute commande.

Exigences

- Cisco FTD géré par FDM version 7.2.7
- Cisco ASA version 9.16
- Détails du serveur SNMP (y compris l'adresse IP, la chaîne de communauté)
- Détails de la configuration VPN site à site (y compris IP homologue, clé pré-partagée)
- FTD doit être au moins la version 6.7 afin d'utiliser l'API REST pour configurer SNMP.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firepower Threat Defense (FTD) géré par Firepower Device Manager (FDM) version 7.2.7.
- Appareil de sécurité adaptatif Cisco (ASA) version 9.16.
- Serveur SNMP (tout logiciel serveur SNMP standard)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

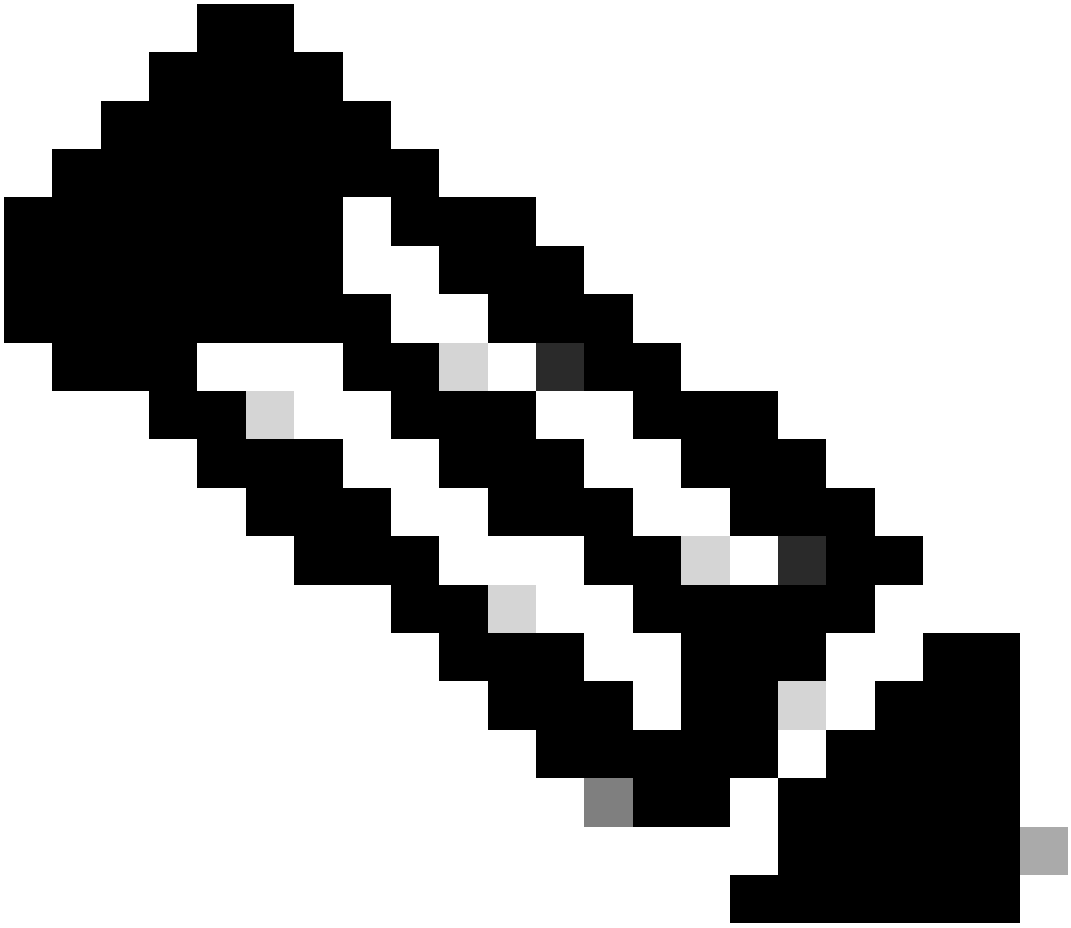
Informations générales

Comme indiqué ci-dessus, les administrateurs réseau peuvent assurer la surveillance à distance de leur périphérique réseau.

SNMP (Simple Network Management Protocol) est utilisé pour la gestion et la surveillance du réseau. Dans cette configuration, le trafic SNMP est envoyé du FTD à un serveur SNMP distant via un VPN de site à site établi avec un ASA.

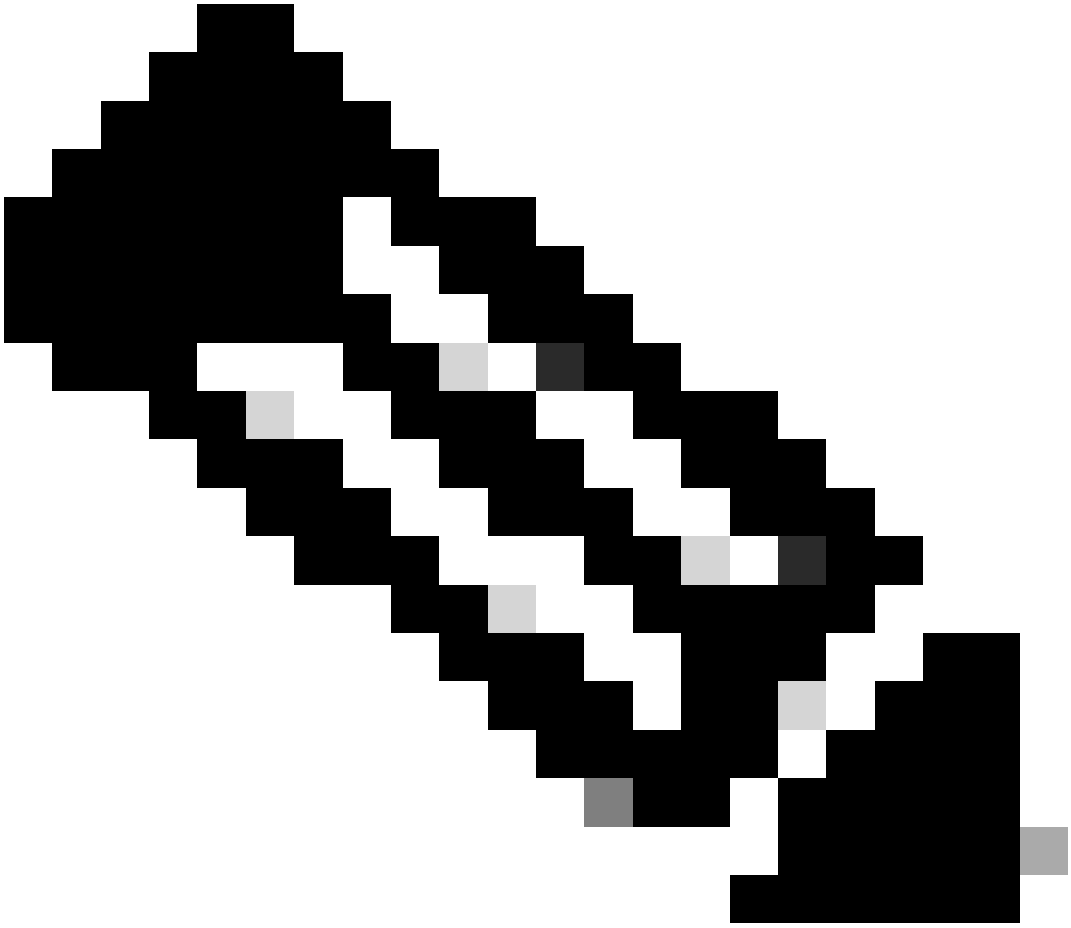
Ce guide vise à aider les administrateurs réseau à configurer le protocole SNMP à distance via un VPN site à site sur une interface de données d'un périphérique FTD. Cette configuration est utile pour la surveillance et la gestion à distance des périphériques réseau. Dans cette configuration, SNMP v2 est utilisé et le trafic SNMP est envoyé de l'interface de données FTD à un serveur SNMP distant via un VPN site à site établi avec un ASA.

L'interface utilisée est appelée « interne », mais cette configuration peut être appliquée à d'autres types de trafic « prêt à l'emploi » et peut utiliser n'importe quelle interface du pare-feu qui n'est pas celle où le VPN se termine.



Remarque : SNMP ne peut être configuré via l'API REST que lorsque FTD exécute la version 6.7 et les versions ultérieures, et est géré par FDM.

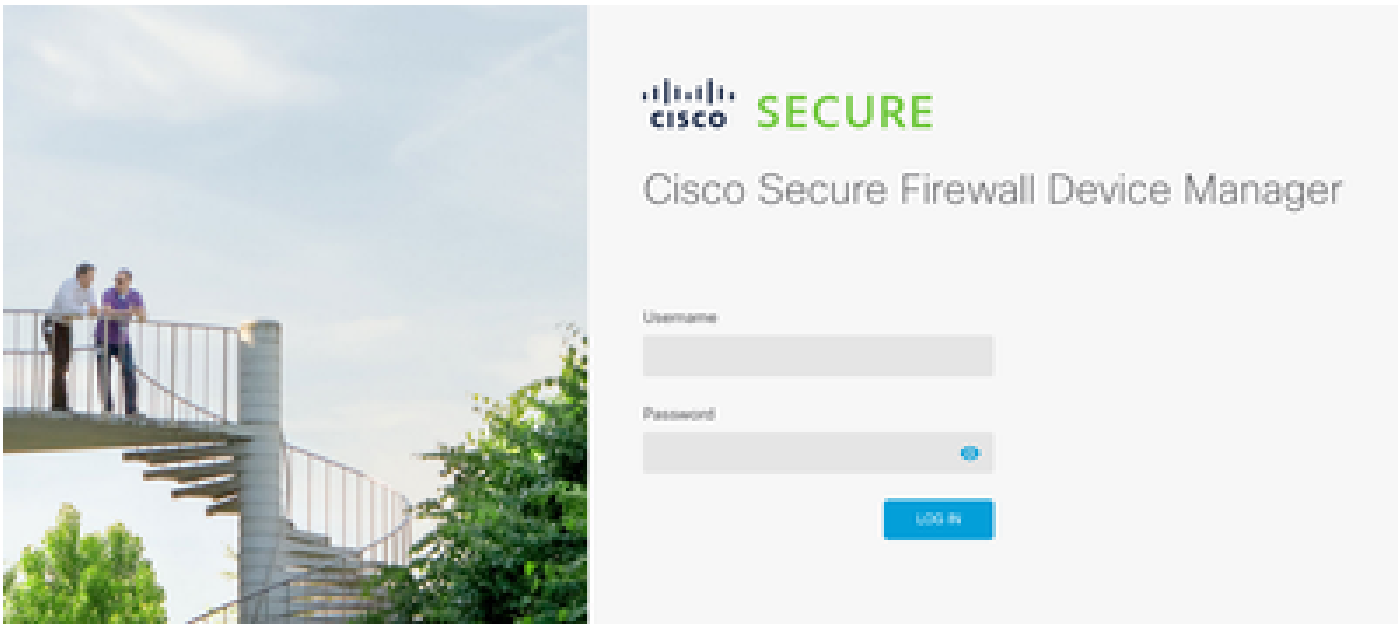
Configurer



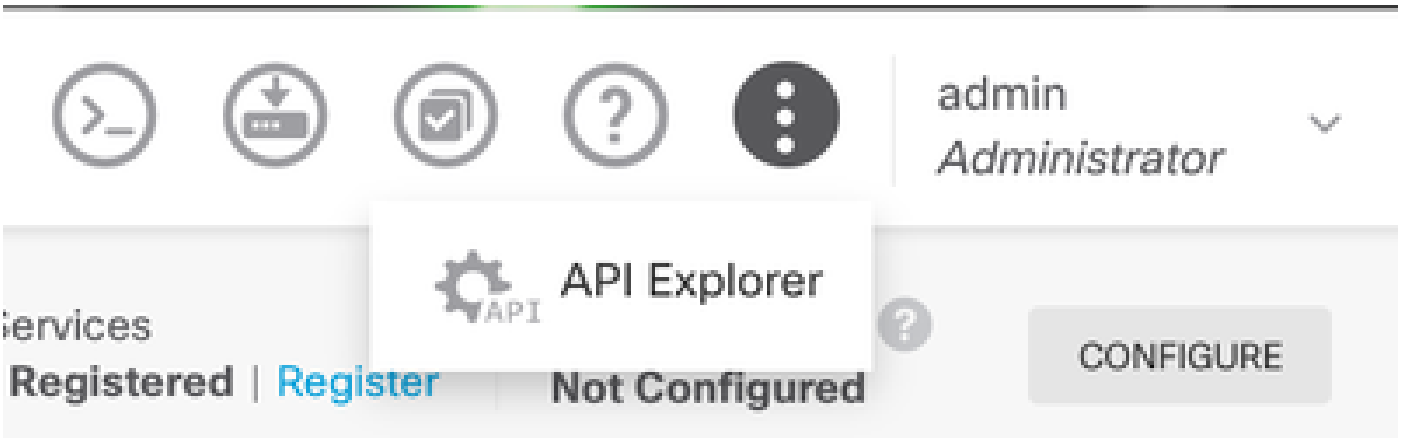
Remarque : cette configuration considère que le VPN site à site est déjà configuré entre les périphériques. Pour plus d'informations sur la configuration du VPN site à site, consultez le guide de configuration. Configurer un VPN site à site sur FTD géré par FDM

Configurations

1. Connectez-vous à votre FTD.



2. Dans la vue d'ensemble Device, accédez à l'explorateur API.



3. Configurez SNMPv2 sur FTD

- Obtenir les informations d'interface.

4. Faites défiler l'affichage vers le bas et sélectionnez le bouton Try it out ! pour passer l'appel API. Un appel réussi renvoie le code de réponse 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

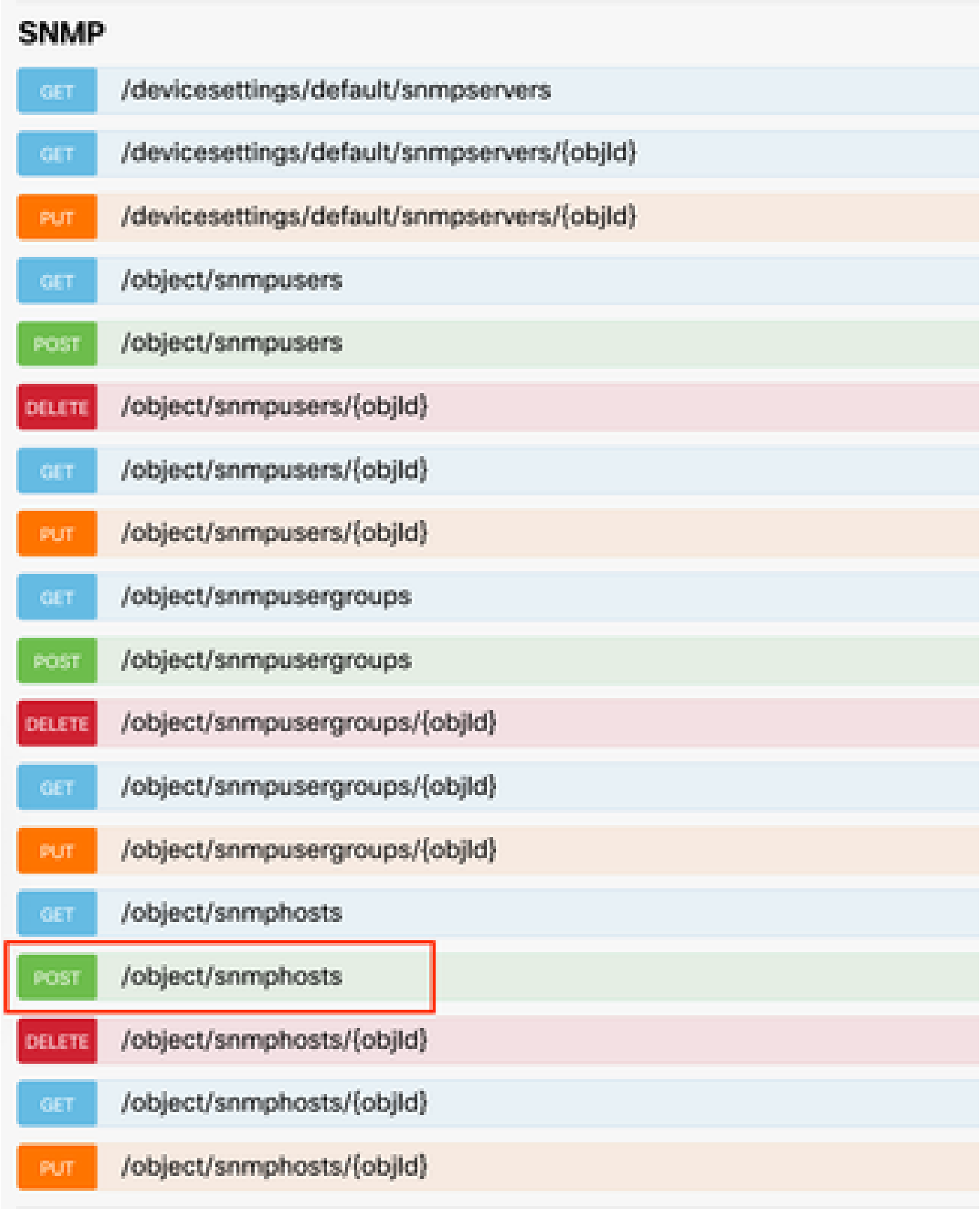

```
    },
    {
      "version": "mqjiipiswsgsx",
      "name": "inside",
      "description": null,
      "hardwareName": "GigabitEthernet0/1",
      "monitorInterface": false,
      "ipv4": {
        "ipType": "STATIC",
        "defaultRouteUsingDHCP": false,
        "dhcpRouteMetric": null,
    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


Response Code

```
200
```

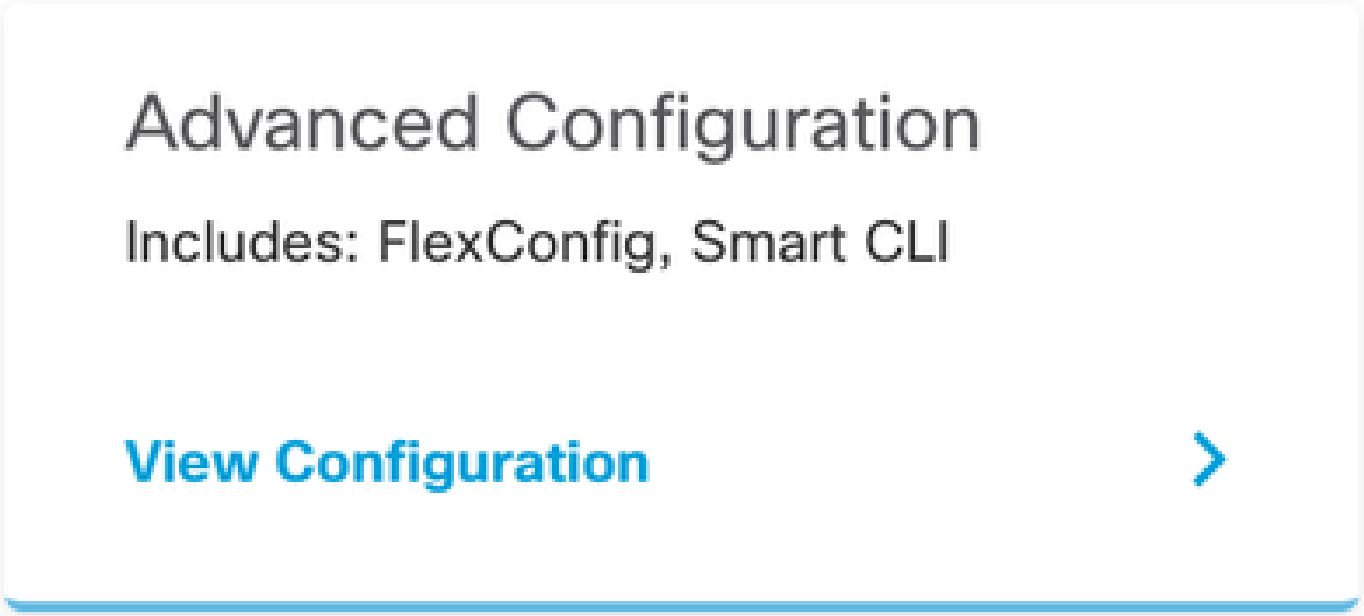
- Créez une configuration d'objet réseau pour l'hôte SNMP.

- Créez un nouvel objet hôte SNMPv2c.

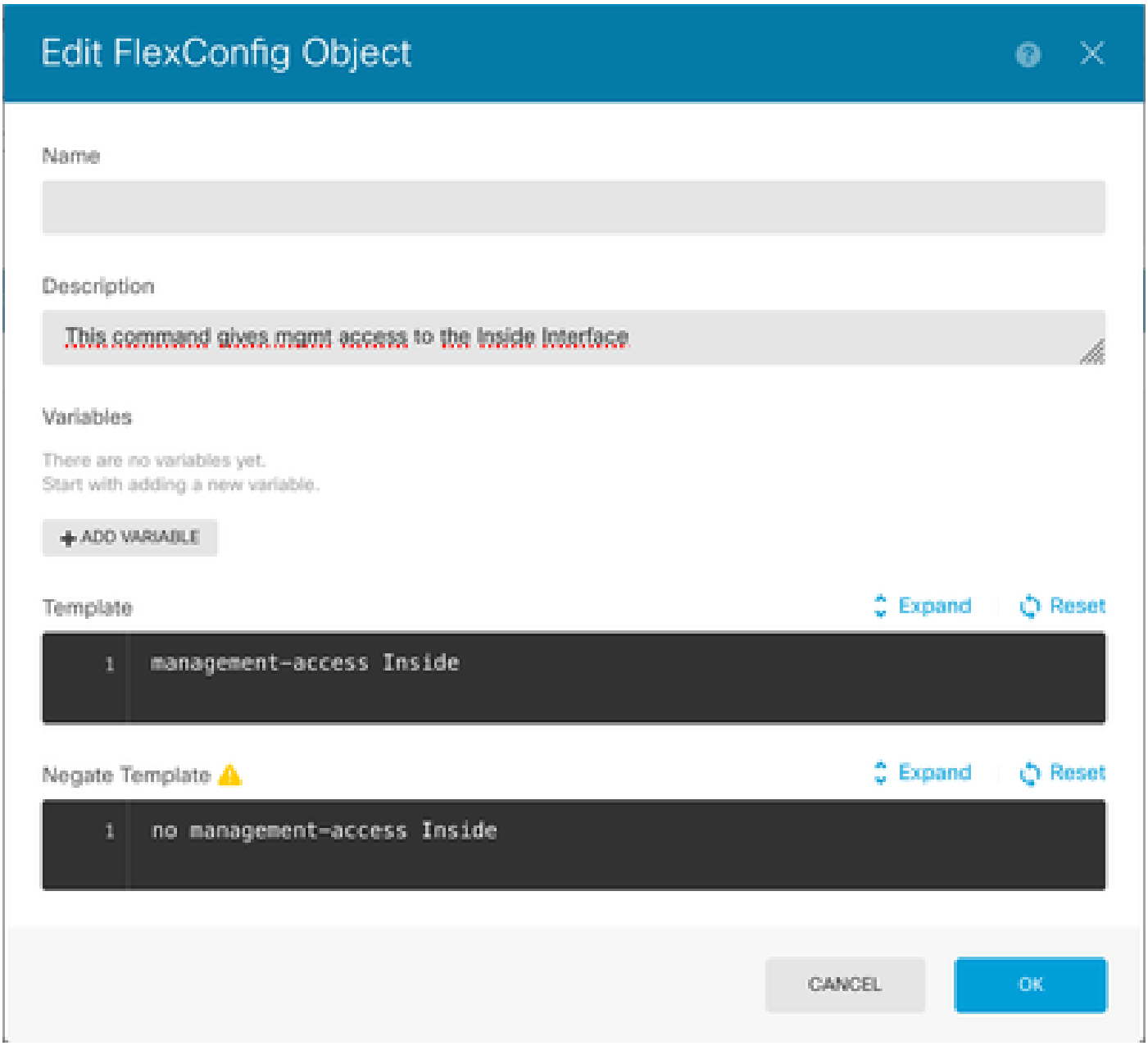


Pour plus de détails, consultez le guide de configuration, Configurer et dépanner SNMP sur Firepower FDM

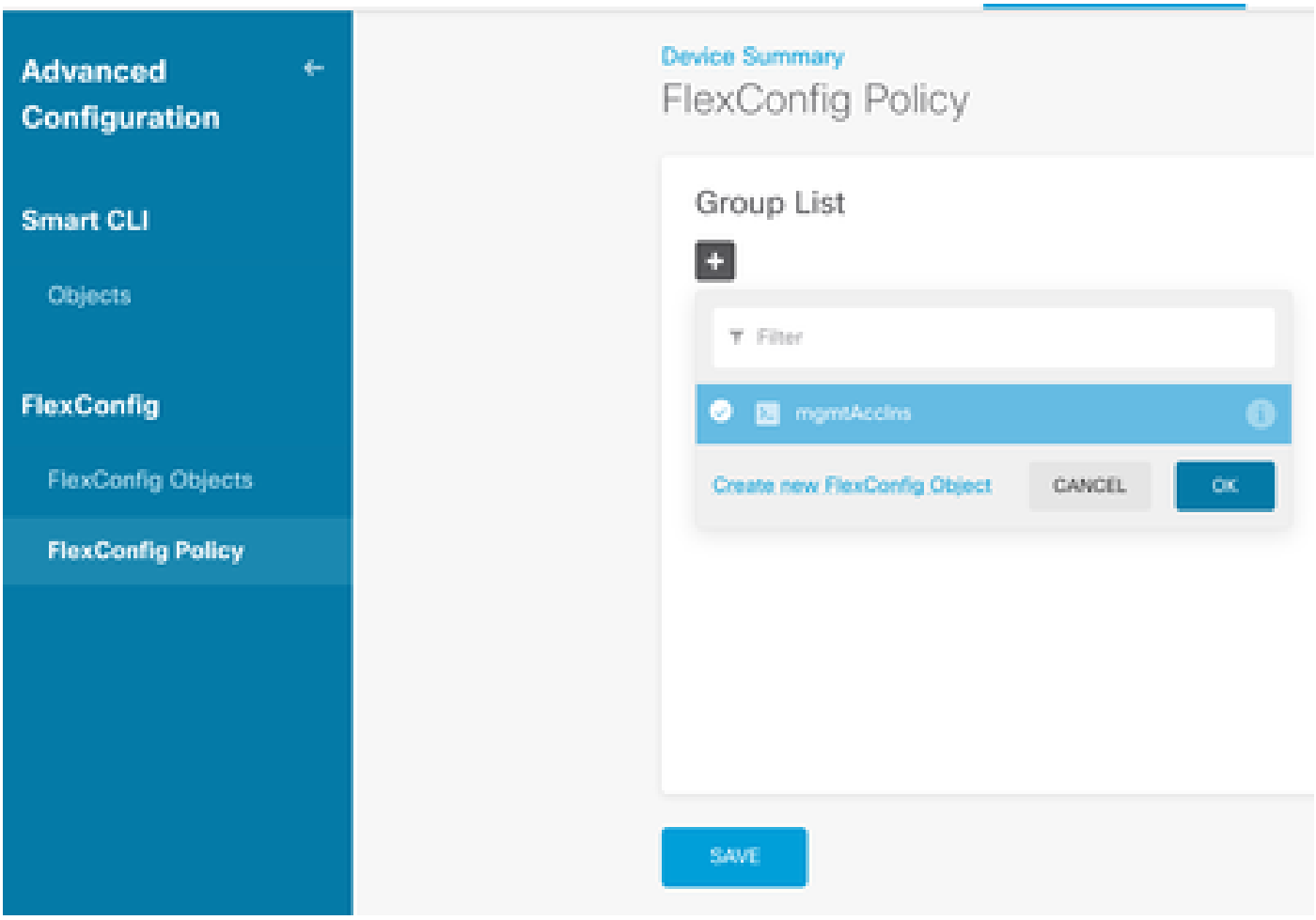
5. Une fois que le protocole SNMP est configuré sur le périphérique, accédez à Device dans la section Advanced Configuration et sélectionnez View Configuration.



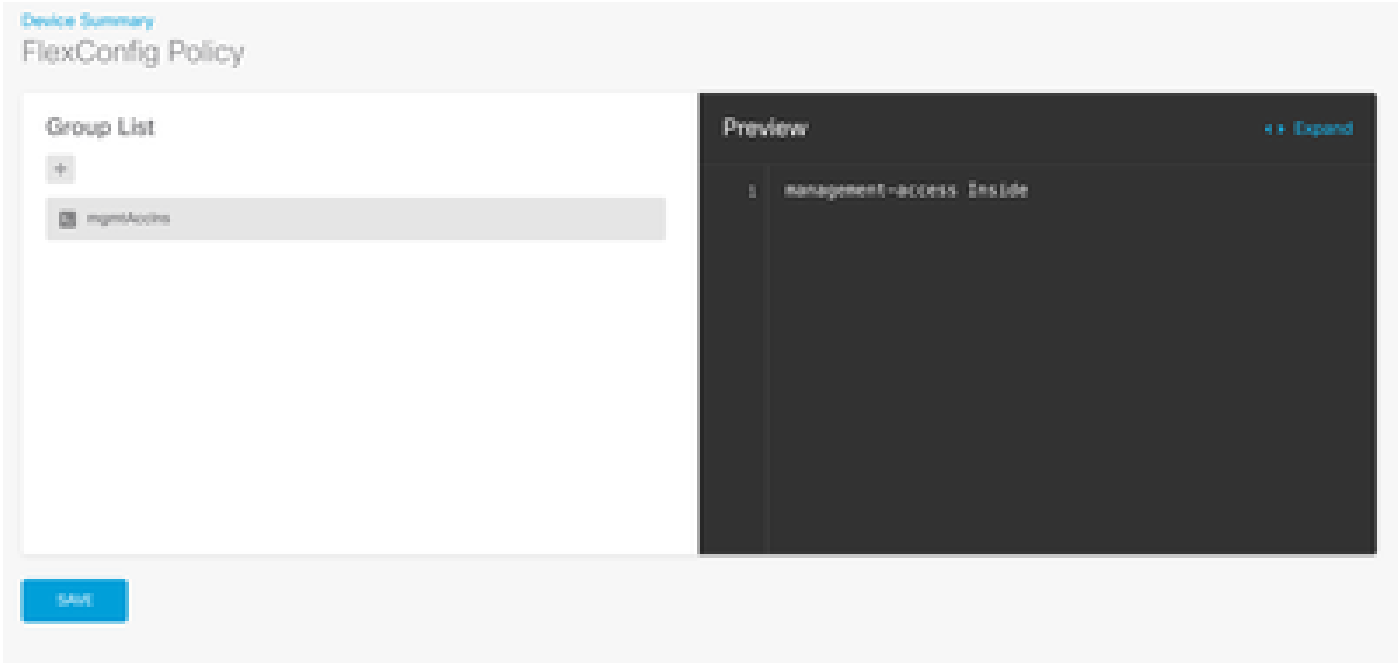
6. Dans la section FlexConfig, sélectionnez des objets FlexConfig et créez un nouvel objet, nommez-le et ajoutez la commande management-access dans la section template, spécifiez l'interface et ajoutez la commande négation dans la partie négation template.



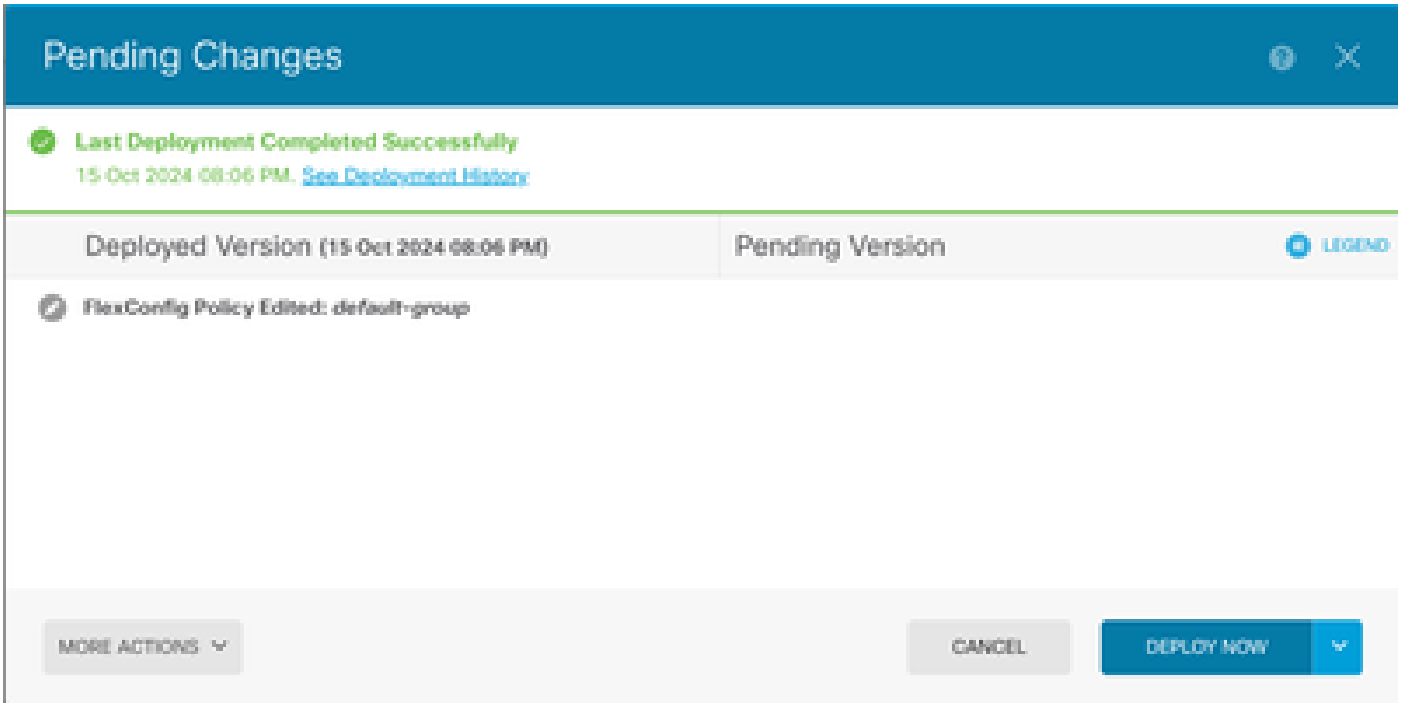
7. Dans la section FlexConfig, sélectionnez FlexConfig Policy, cliquez sur l'icône d'ajout et sélectionnez l'objet flexConfig que nous avons créé à l'étape précédente et sélectionnez OK.

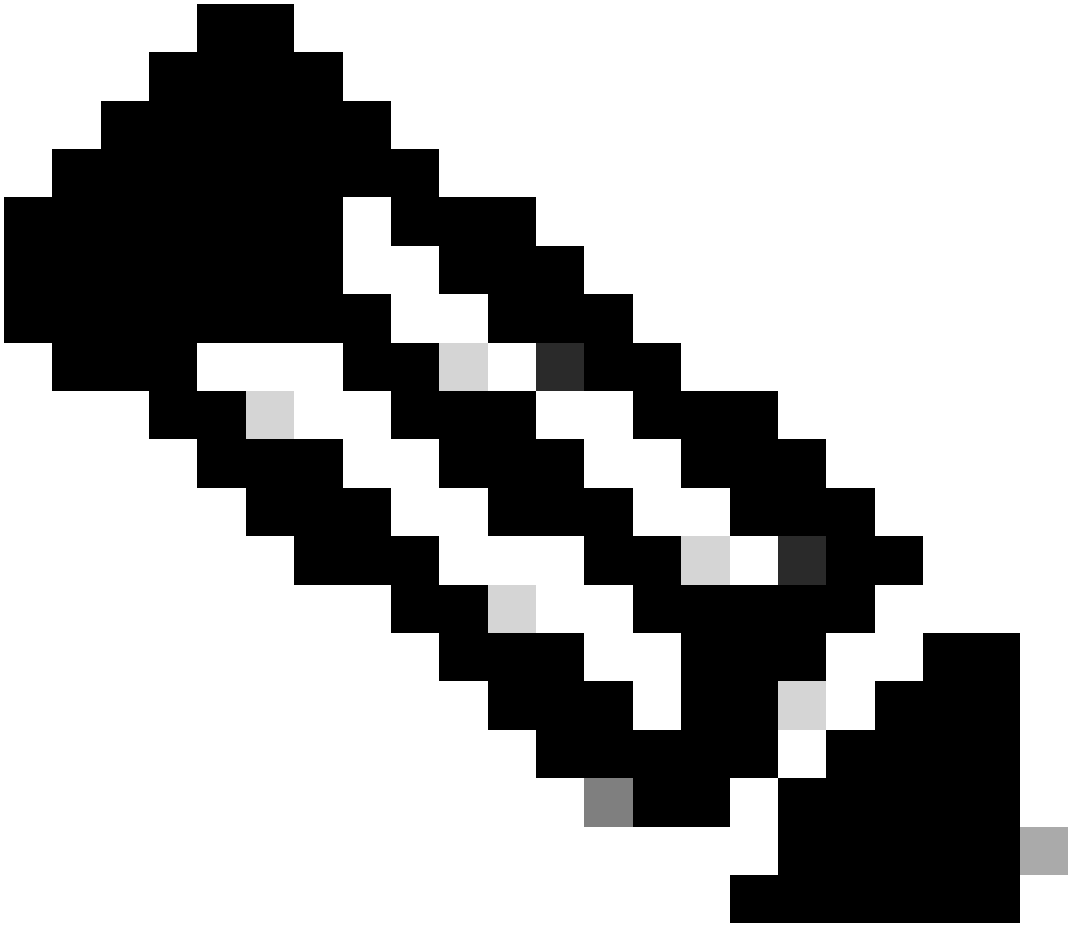


8. Un aperçu des commandes à appliquer au périphérique s’affiche ensuite. Sélectionnez Enregistrer.



9. Déployez la configuration, sélectionnez l'icône de déploiement et cliquez sur déployer maintenant.


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



Remarque : assurez-vous qu'elle est terminée de manière satisfaisante. Vous pouvez consulter la liste des tâches pour la confirmer.

Vérifier

Pour vérifier la configuration, effectuez les vérifications suivantes, connectez-vous au FTD via SSH ou la console, puis exécutez les commandes suivantes :

- Vérifiez que la configuration en cours du périphérique contient les modifications que nous avons apportées.

```
> 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
```

- Effectuez un test à partir du testeur SNMP et assurez-vous qu'il se termine correctement.

Dépannage

Si vous rencontrez des problèmes, procédez comme suit :

- Assurez-vous que le tunnel VPN est opérationnel et que vous pouvez exécuter ces commandes pour vérifier le tunnel VPN.

```
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
```

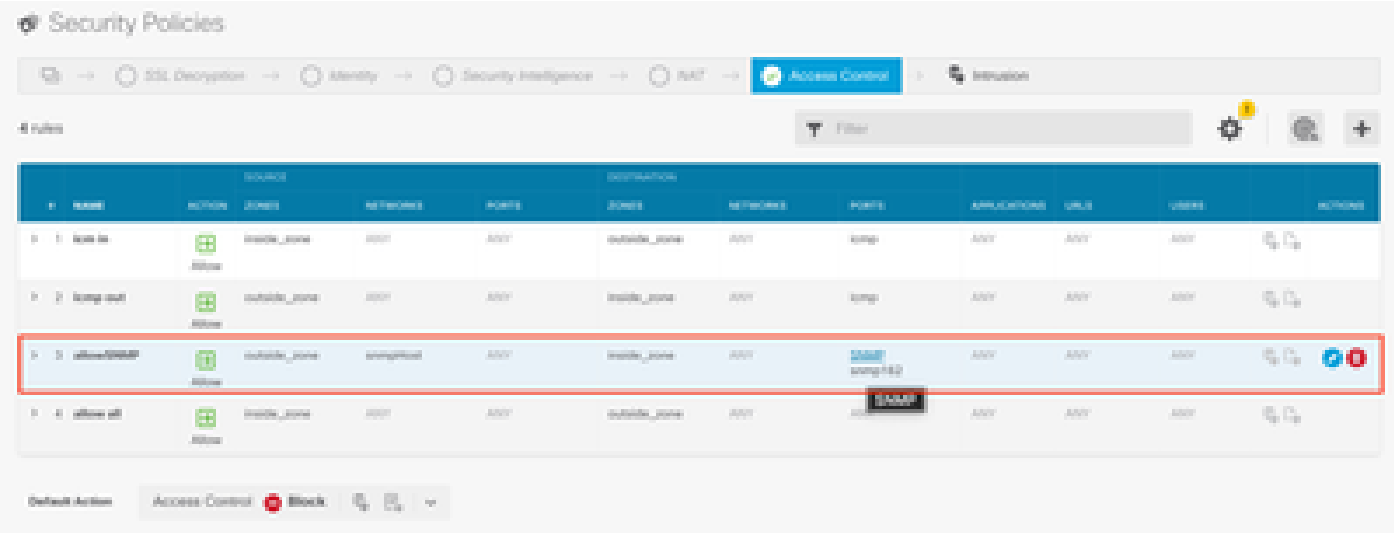
Un guide détaillé sur la façon de déboguer les tunnels IKEv2 peut être trouvé ici : Comment déboguer les VPN IKEv2

- Vérifiez la configuration SNMP et assurez-vous que la chaîne de communauté et les paramètres de contrôle d'accès sont corrects aux deux extrémités.

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 *****

- Assurez-vous que le trafic SNMP est autorisé via le FTD.

Accédez à Policies > Access Control et vérifiez que vous disposez d'une règle autorisant le trafic SNMP.



- Utilisez la capture de paquets pour surveiller le trafic SNMP et identifier les problèmes éventuels.

Activez la capture avec trace sur le pare-feu :

```
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
```

Pour plus de détails, consultez le Guide de configuration SNMP, Configurer et dépanner SNMP sur Firepower FDM

Informations connexes

- Guide de configuration de Cisco Secure Firepower Device Manager
- Guide de configuration de Cisco ASA
- Configuration SNMP sur les périphériques Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.