Configurazione di SNMP sulla VPN da sito a sito sull'interfaccia dati gestita da FDM

Sommario

Introduzione

Questo documento descrive la configurazione di SNMP su un'estremità remota tramite una VPN da sito a sito su un'interfaccia dati di un dispositivo FTD.

Prerequisiti

Prima di procedere con la configurazione, verificare che siano soddisfatti i seguenti prerequisiti:

- Conoscenza di base di questi argomenti:
  - Cisco Firepower Threat Defense (FTD) gestito da Firepower Device Manager (FDM).
  - Cisco Adaptive Security Appliance (ASA).
  - Protocollo SNMP (Simple Network Management Protocol).
  - VPN (Virtual Private Network).
- Accesso amministrativo ai dispositivi FTD e ASA.
- Verificare che la rete sia operativa e comprendere il potenziale impatto di qualsiasi comando.

Requisiti

- Cisco FTD gestito da FDM versione 7.2.7
- Cisco ASA versione 9.16
- Dettagli del server SNMP (incluso indirizzo IP, stringa della community)
- Dettagli della configurazione della VPN da sito a sito (inclusi IP peer, chiave precondivisa)
- Per utilizzare l'API REST per configurare SNMP, FTD deve essere almeno la versione 6.7.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firepower Threat Defense (FTD) gestito da Firepower Device Manager (FDM) versione 7.2.7.
- Cisco Adaptive Security Appliance (ASA) versione 9.16.
- Server SNMP (qualsiasi software per server SNMP standard)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

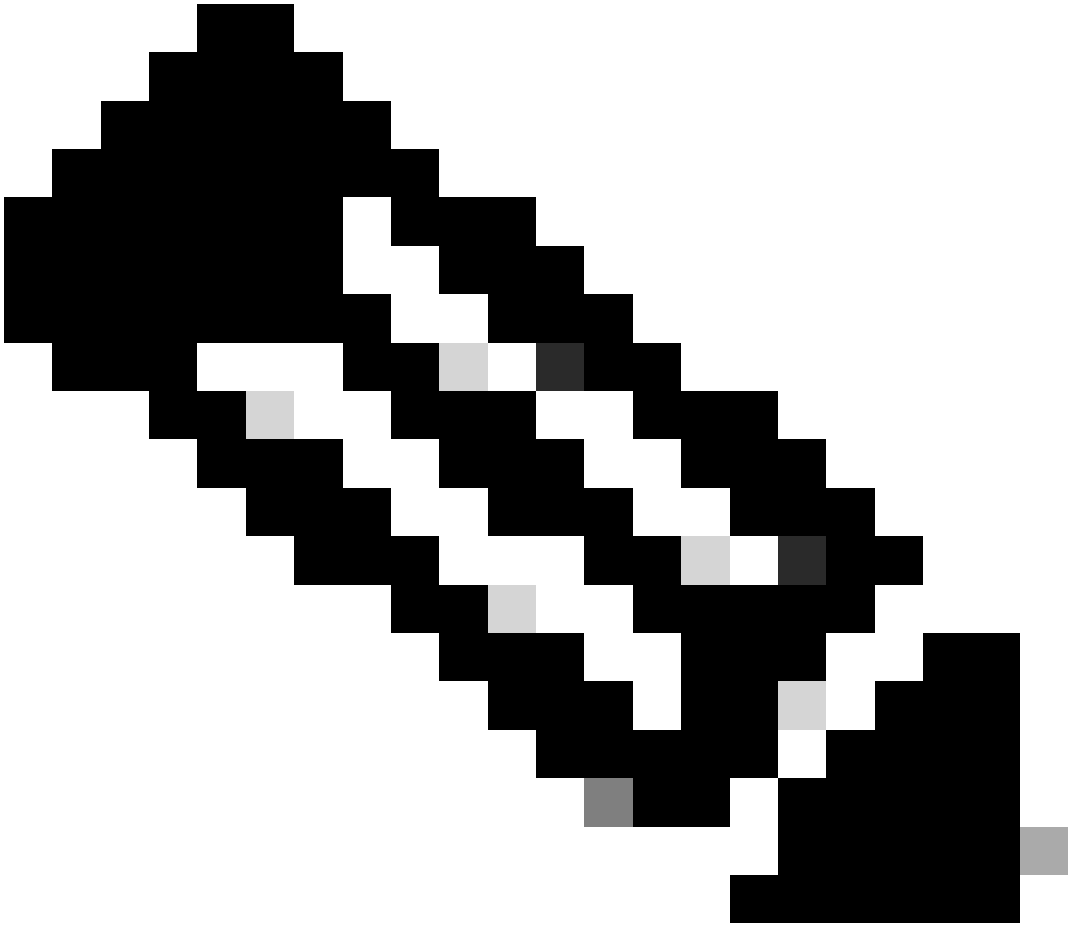
Premesse

In questa procedura gli amministratori di rete possono garantire il monitoraggio remoto dei dispositivi di rete.

L'SNMP (Simple Network Management Protocol) viene utilizzato per la gestione e il monitoraggio della rete. In questa configurazione, il traffico SNMP viene inviato dall'FTD a un server SNMP remoto tramite una VPN da sito a sito stabilita con un'ASA.

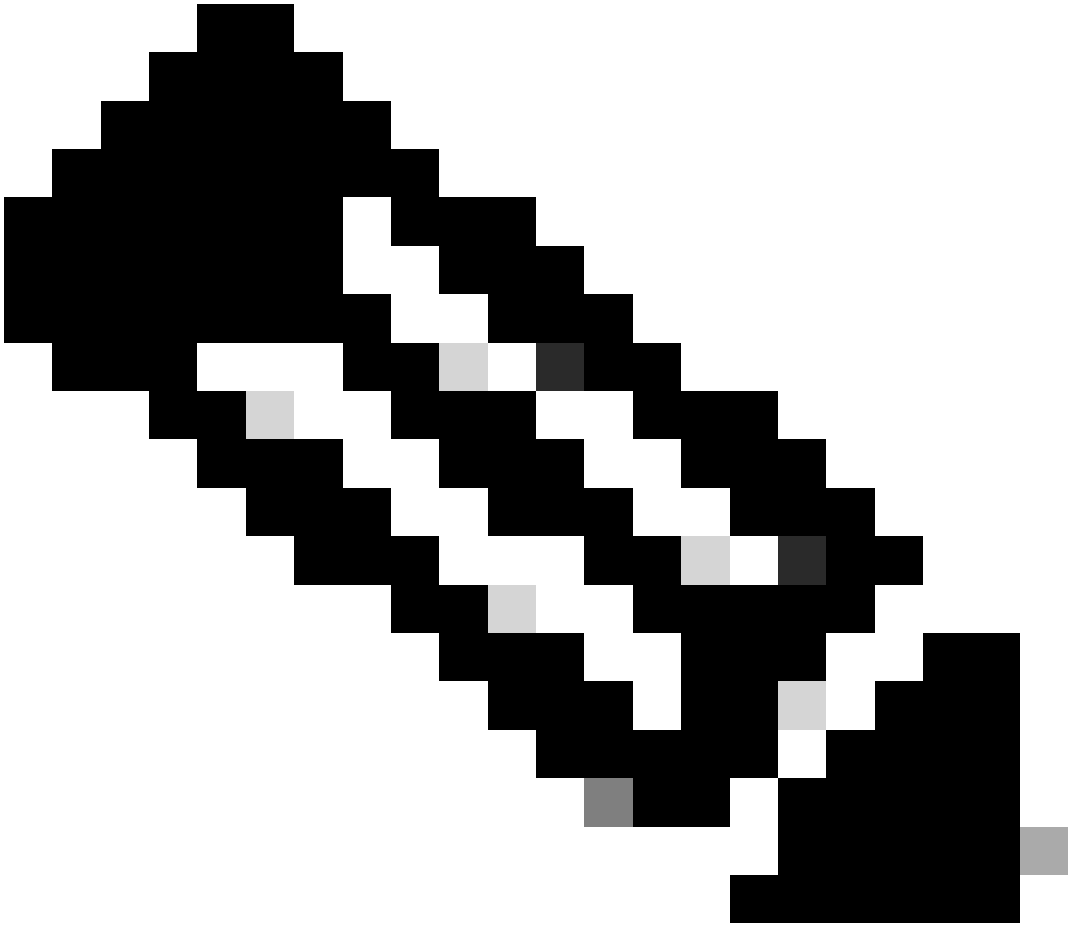
Questa guida ha lo scopo di aiutare gli amministratori di rete a configurare il protocollo SNMP su un'estremità remota tramite una VPN da sito a sito su un'interfaccia dati di un dispositivo FTD. Questa configurazione è utile per il monitoraggio e la gestione remota dei dispositivi di rete. In questa configurazione, viene usato il protocollo SNMP v2 e il traffico SNMP viene inviato dall'interfaccia dati FTD a un server SNMP remoto tramite una VPN da sito a sito stabilita con un'ASA.

L'interfaccia utilizzata è detta "interna", ma questa configurazione può essere applicata ad altri tipi di traffico "diretto" e può utilizzare qualsiasi interfaccia del firewall diversa da quella in cui la VPN termina.



Nota: il protocollo SNMP può essere configurato solo tramite l'API REST quando FTD esegue la versione 6.7 e successive ed è gestito da FDM.

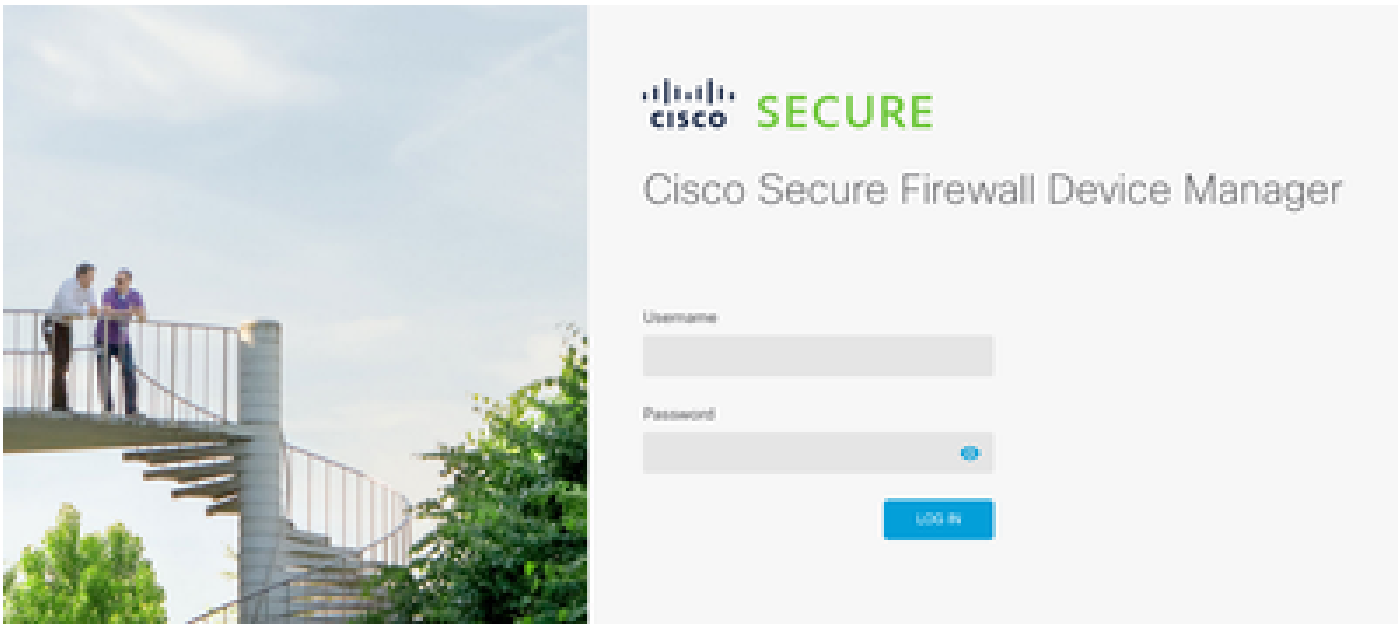
Configurazione



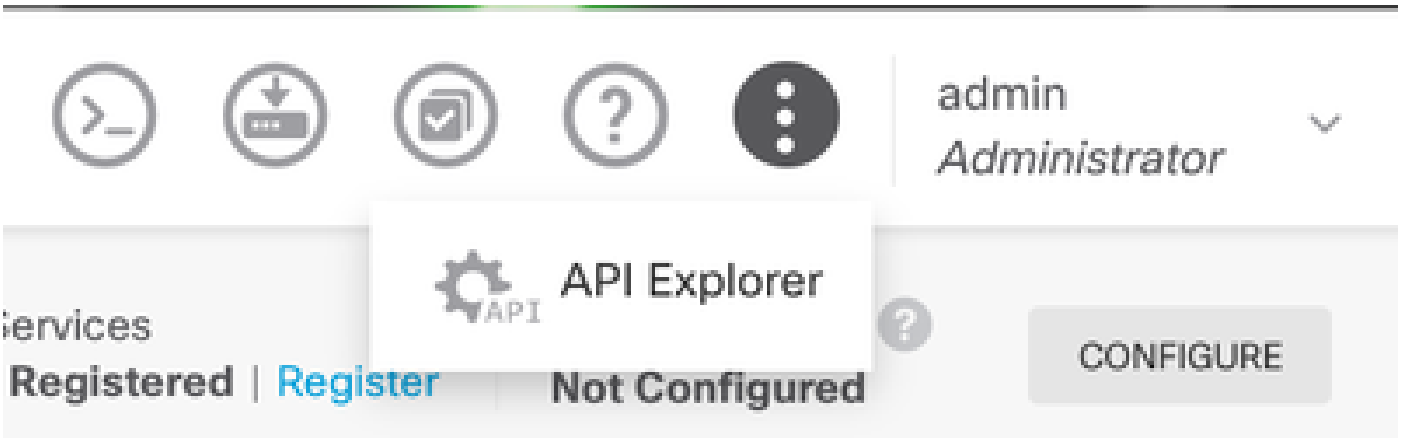
Nota: questa configurazione considera che la VPN da sito a sito è già configurata tra i dispositivi. Per ulteriori informazioni su come configurare la VPN da sito a sito, vedere la guida alla configurazione. Configura VPN da sito a sito su FTD gestito da FDM

Configurazioni

1. Accedere al proprio FTD.



2. In Cenni preliminari sul dispositivo passare a Gestione API.



3. Configurare SNMPv2 su FTD

- Ottiene le informazioni sull'interfaccia.

4. Scorrere verso il basso e selezionare il pulsante Prova! per effettuare la chiamata API. Una chiamata riuscita restituisce il codice di risposta 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

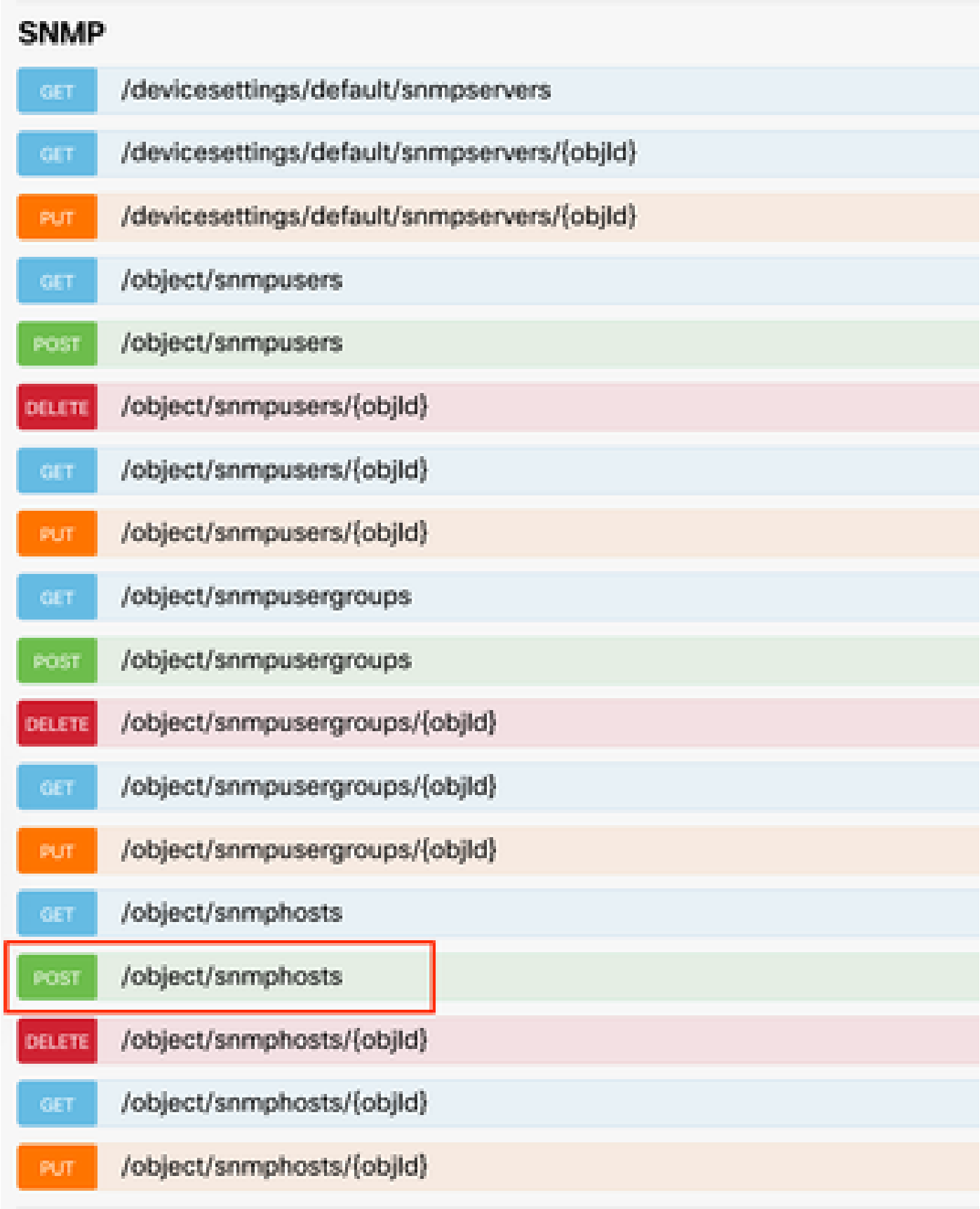

```
    },
    {
      "version": "mqjiipiswsgsx",
      "name": "inside",
      "description": null,
      "hardwareName": "GigabitEthernet0/1",
      "monitorInterface": false,
      "ipv4": {
        "ipType": "STATIC",
        "defaultRouteUsingDHCP": false,
        "dhcpRouteMetric": null,
    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


Response Code

```
200
```

- Creare una configurazione oggetto di rete per l'host SNMP.

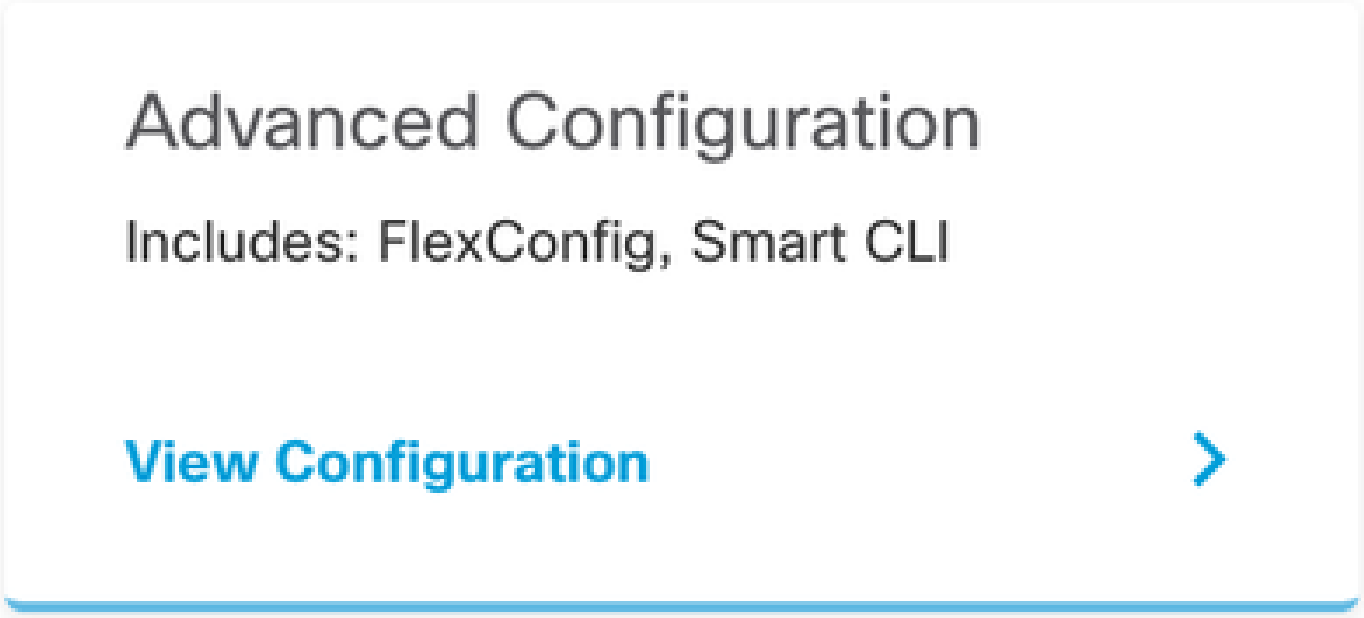
- Creare un nuovo oggetto host SNMPv2c.



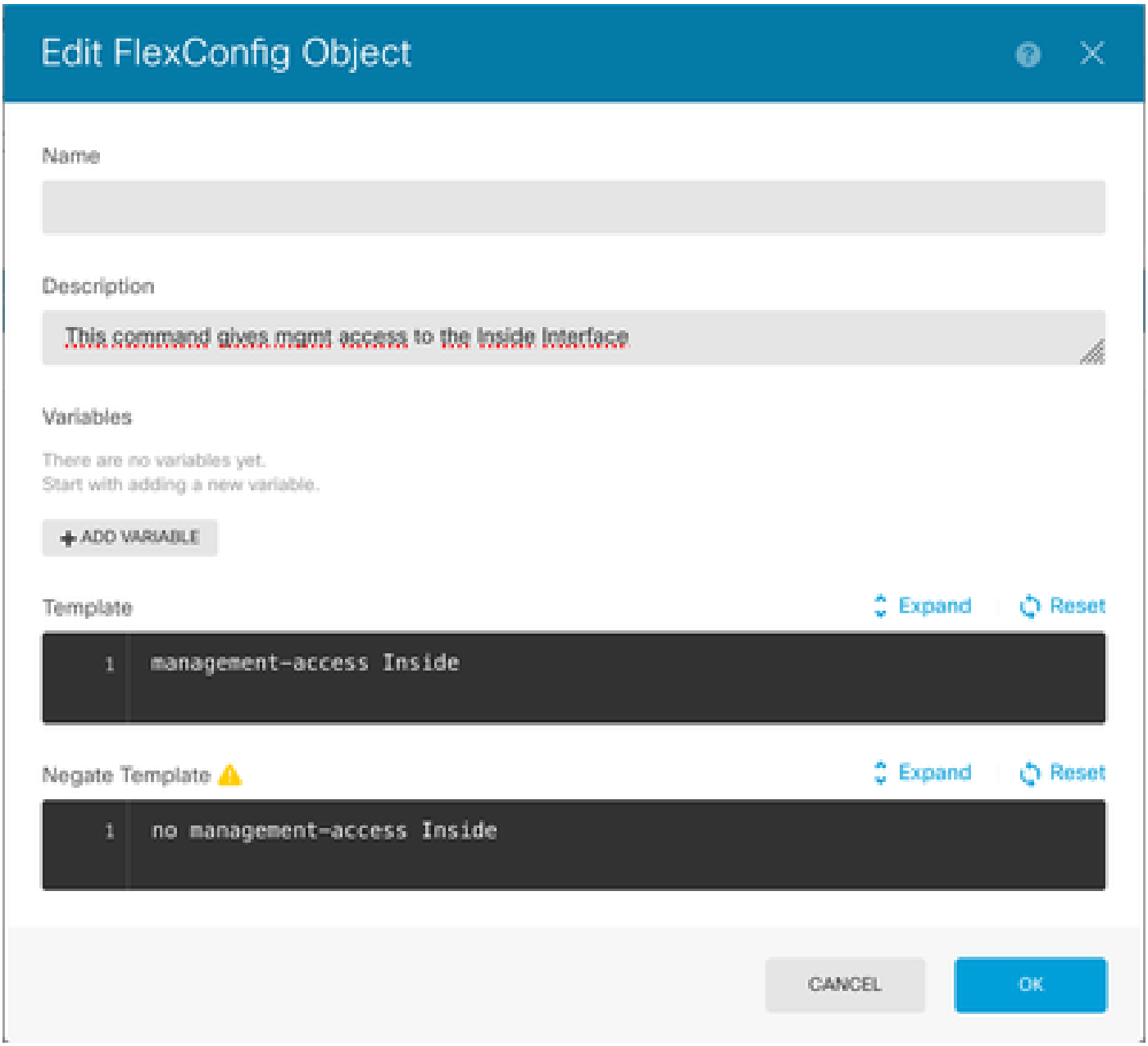
Per ulteriori informazioni, consultare la guida alla configurazione, [configurare e risolvere i problemi relativi al protocollo SNMP su Firepower FDM]

5. Una volta configurato il protocollo SNMP sul dispositivo, spostarsi su Device nella sezione Advanced Configuration (Configurazione avanzata) e selezionare View Configuration (Visualizza

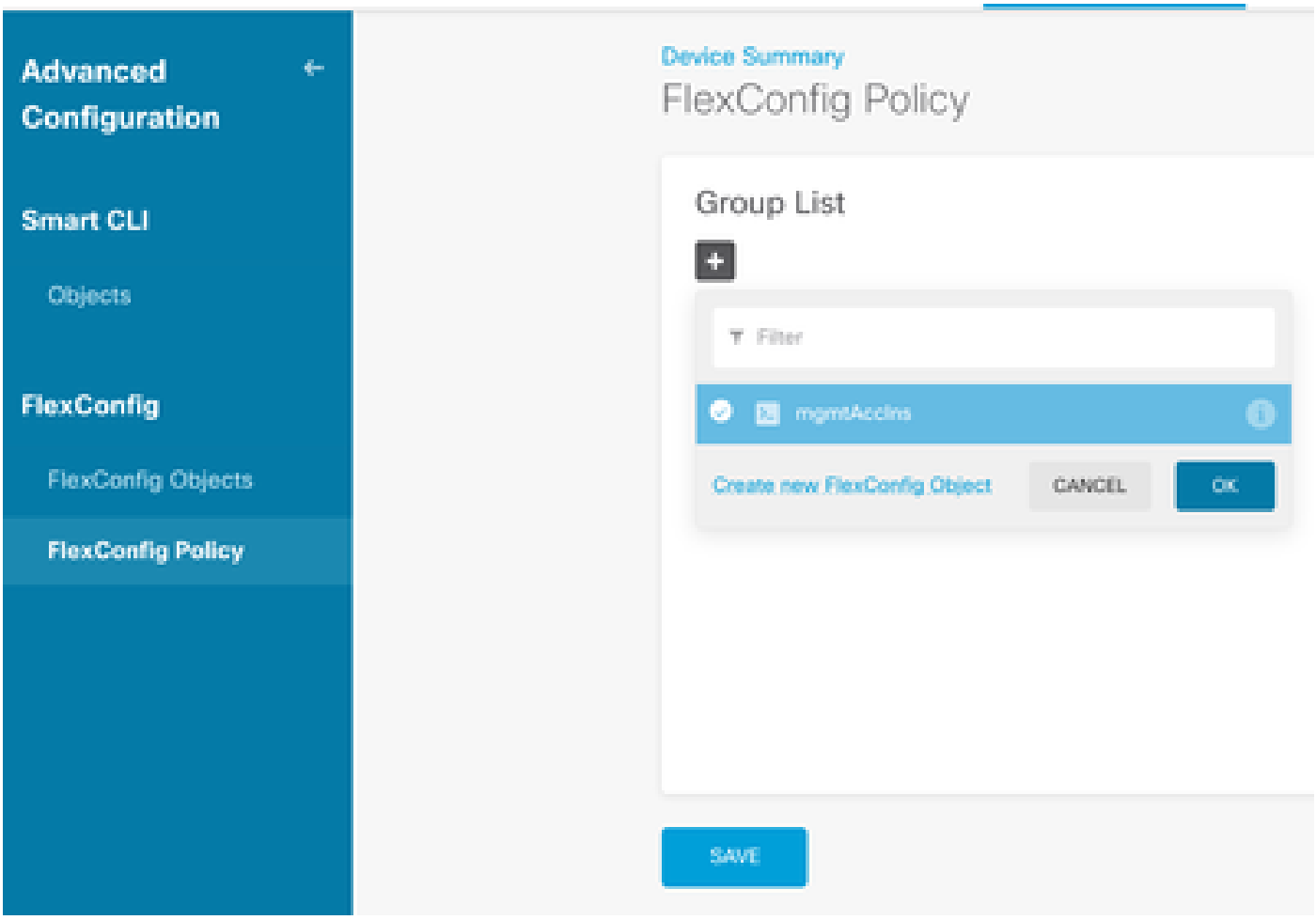
configurazione).



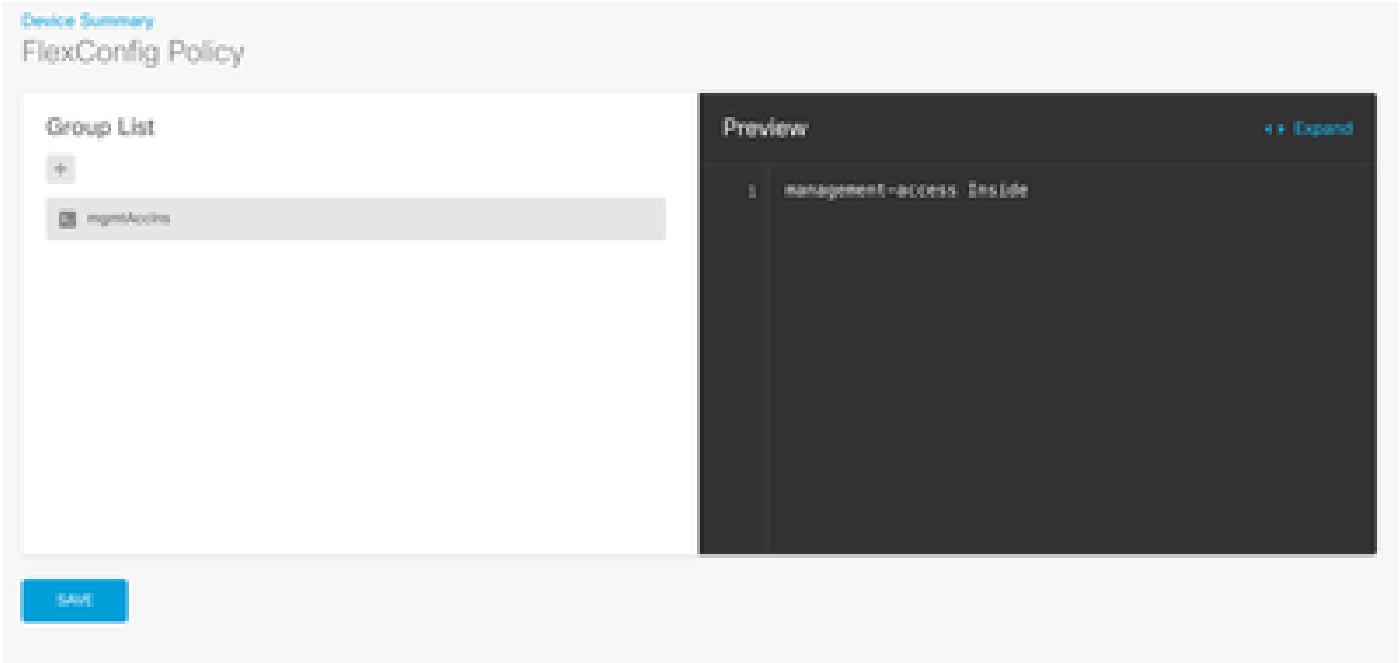
6. Nella sezione FlexConfig, selezionare gli oggetti FlexConfig e creare un nuovo oggetto, assegnargli un nome e aggiungere il comando management-access nella sezione template, specificare l'interfaccia e aggiungere la negazione del comando nella parte di negoziazione del modello.



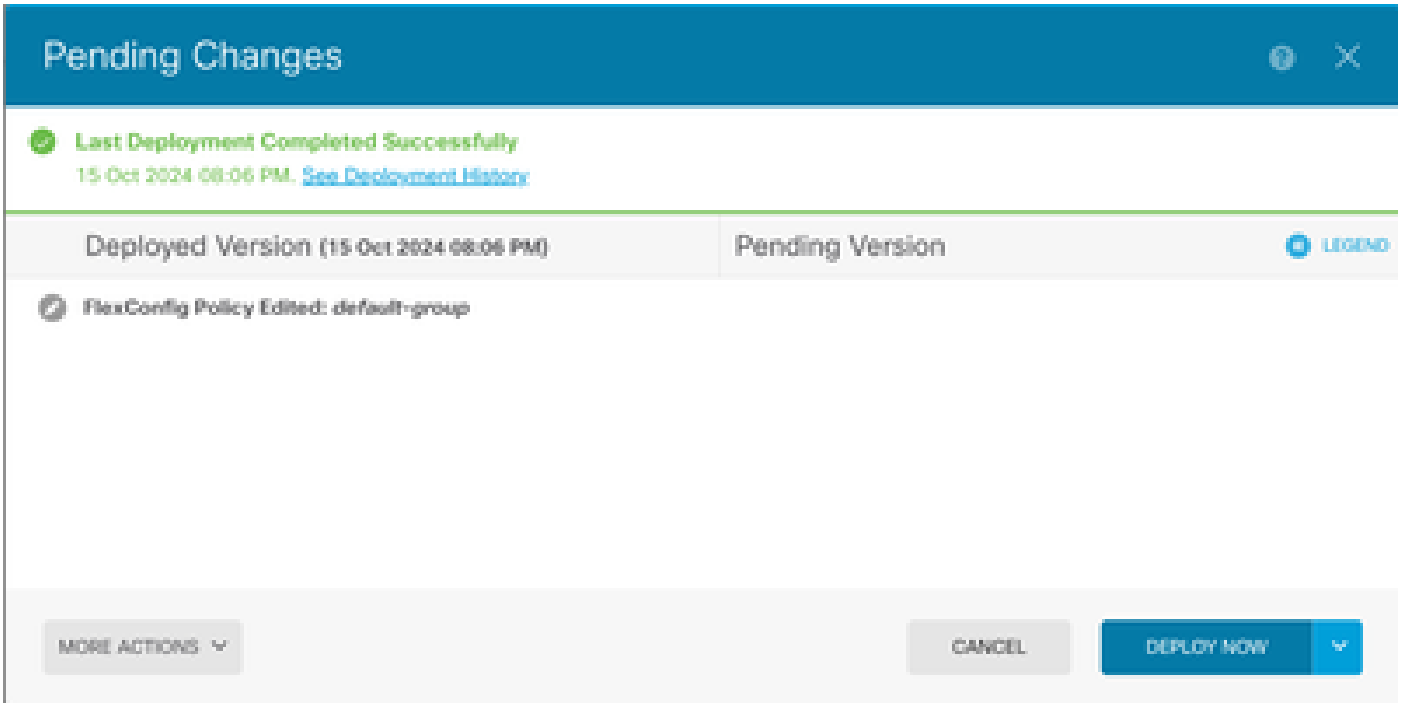
7. Nella sezione FlexConfig, selezionare FlexConfig Policy, fare clic sull'icona di aggiunta e selezionare l'oggetto flexConfig creato nel passaggio precedente, quindi selezionare OK.

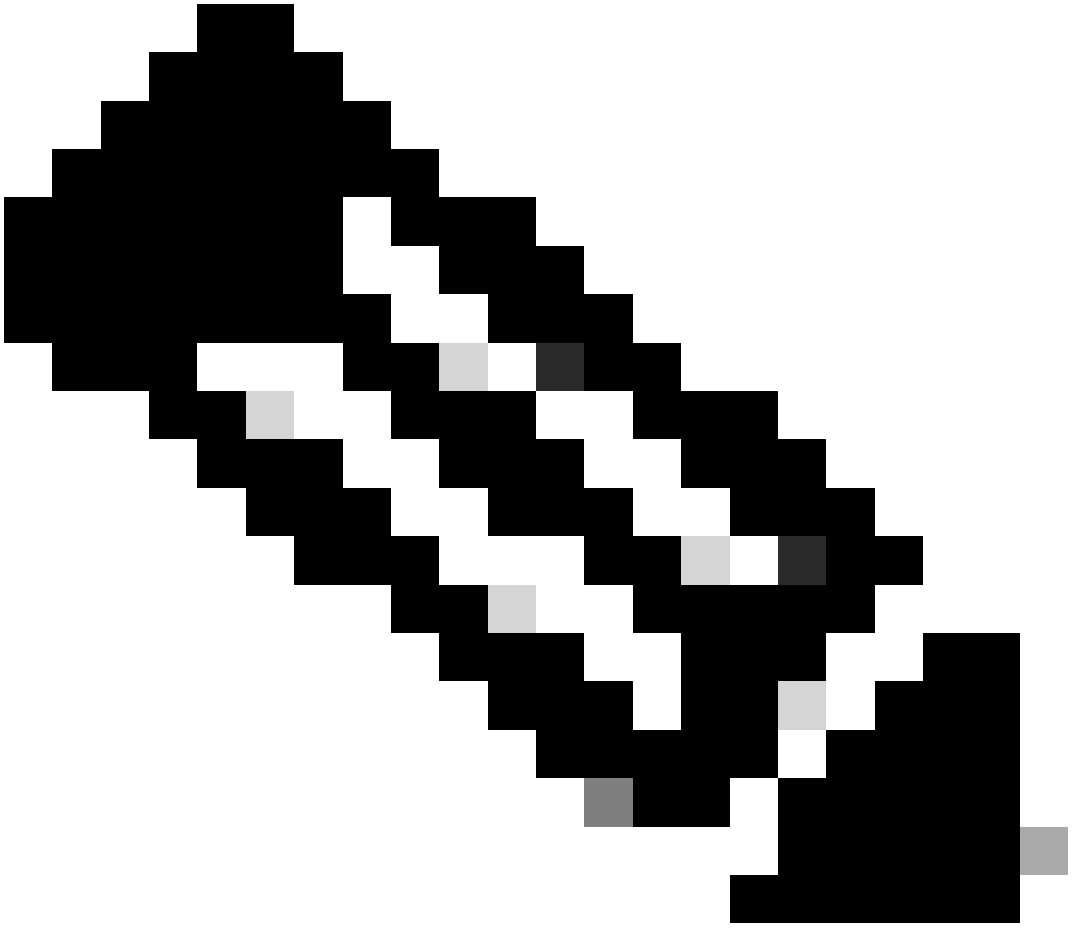


8. Quindi, viene visualizzata un'anteprima dei comandi da applicare al dispositivo. Selezionare Salva.



9. Distribuire la configurazione, selezionare l'icona di distribuzione e fare clic su distribuisci ora.


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



Nota: assicurarsi che sia stato completato in modo soddisfacente, è possibile controllare l'elenco di task per confermarlo.

Verifica

Per verificare la configurazione, eseguire questi controlli, accedere all'FTD tramite SSH o la console ed eseguire questi comandi:

- Verificare che la configurazione corrente del dispositivo contenga le modifiche apportate.

```
> 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
```

- Eseguire un test dal tester SNMP e verificare che venga completato correttamente.

Risoluzione dei problemi

In caso di problemi, considerare i seguenti passaggi:

- Verificare che il tunnel VPN sia attivo e in esecuzione, è possibile eseguire questi comandi per verificare il 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
```

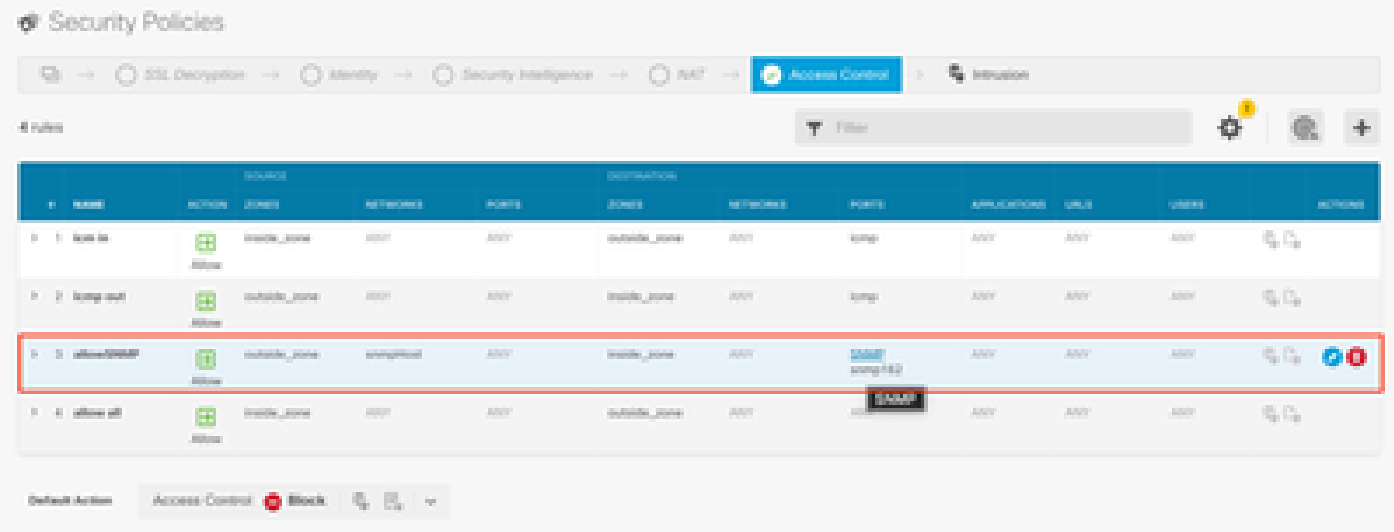
Per una guida dettagliata su come eseguire il debug dei tunnel IKEv2, fare riferimento a:

- Verificare la configurazione SNMP e accertarsi che la stringa della community e le impostazioni di controllo dell'accesso siano corrette su entrambe le estremità.

firepower# sh esegui snmp-server
host snmp-server all'interno della community 10.56.58.10 **** versione 2c
percorso snmp-server null
contatto snmp-server null
community snmp-server *****

- Verificare che il traffico SNMP sia autorizzato tramite l'FTD.

Passare a Criteri > Controllo di accesso e verificare di disporre di una regola che consenta il traffico SNMP.



- Usare l'acquisizione dei pacchetti per monitorare il traffico SNMP e identificare eventuali problemi.

Abilita acquisizione con traccia nel 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
```

Per ulteriori informazioni, consultare la guida alla configurazione di SNMP, configurare e risolvere i problemi relativi a SNMP su Firepower FDM

Informazioni correlate

- Guida alla configurazione di Cisco Secure Firepower Device Manager
- Guida alle configurazioni di Cisco ASA
- Configurazione SNMP sui dispositivi Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).