Configuración de SNMP en VPN de sitio a sitio en la interfaz de datos administrada por FDM

Contenido

Introducción

Este documento describe la configuración de SNMP a un extremo remoto a través de una VPN de sitio a sitio en una interfaz de datos de una interfaz de datos de dispositivo FTD.

Prerequisites

Antes de continuar con la configuración, asegúrese de que se cumplen estos requisitos previos:

- Comprensión básica de estos temas:
  - Cisco Firepower Threat Defence (FTD) gestionado por Firepower Device Manager (FDM).
  - Dispositivo de seguridad Cisco Adaptive Security Appliance (ASA).
  - Protocolo simple de administración de red (SNMP).
  - Red privada virtual (VPN).
- Acceso administrativo a los dispositivos FTD y ASA.
- Asegúrese de que la red está activa y de que comprende el impacto potencial de cualquier comando.

Requirements

- Cisco FTD administrado por FDM versión 7.2.7
- Cisco ASA versión 9.16
- Detalles del servidor SNMP (incluida la dirección IP y la cadena de comunidad)
- Detalles de la configuración VPN de sitio a sitio (incluida la IP del par y la clave precompartida)

- FTD debe ser al menos la versión 6.7 para poder utilizar la API REST para configurar SNMP.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Firepower Threat Defence (FTD) gestionado por Firepower Device Manager (FDM) versión 7.2.7.
- Cisco Adaptive Security Appliance (ASA) versión 9.16.
- Servidor SNMP (cualquier software de servidor SNMP estándar)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

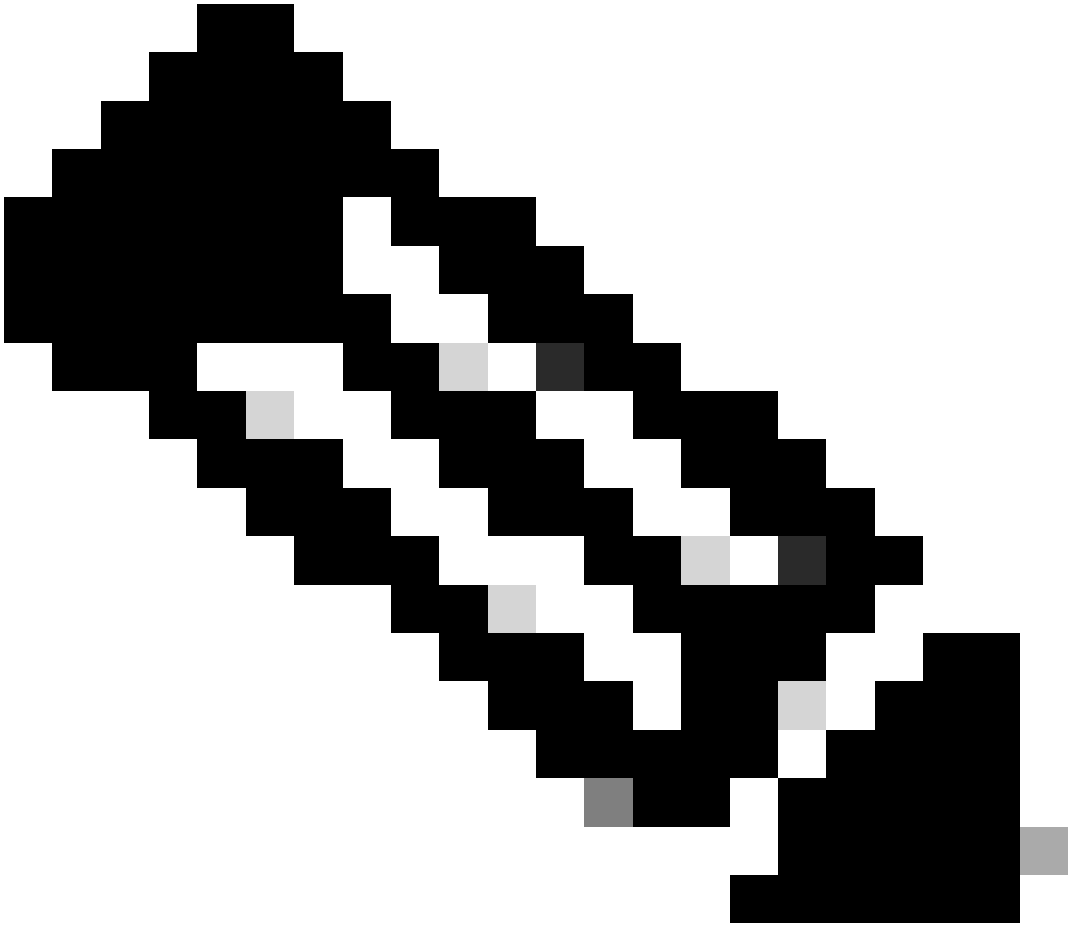
Antecedentes

Con estos pasos descritos, los administradores de red pueden garantizar la supervisión remota de sus dispositivos de red.

SNMP (protocolo simple de administración de red) se utiliza para la administración y supervisión de la red. En esta configuración, el tráfico SNMP se envía desde el FTD a un servidor SNMP remoto a través de una VPN de sitio a sitio establecida con un ASA.

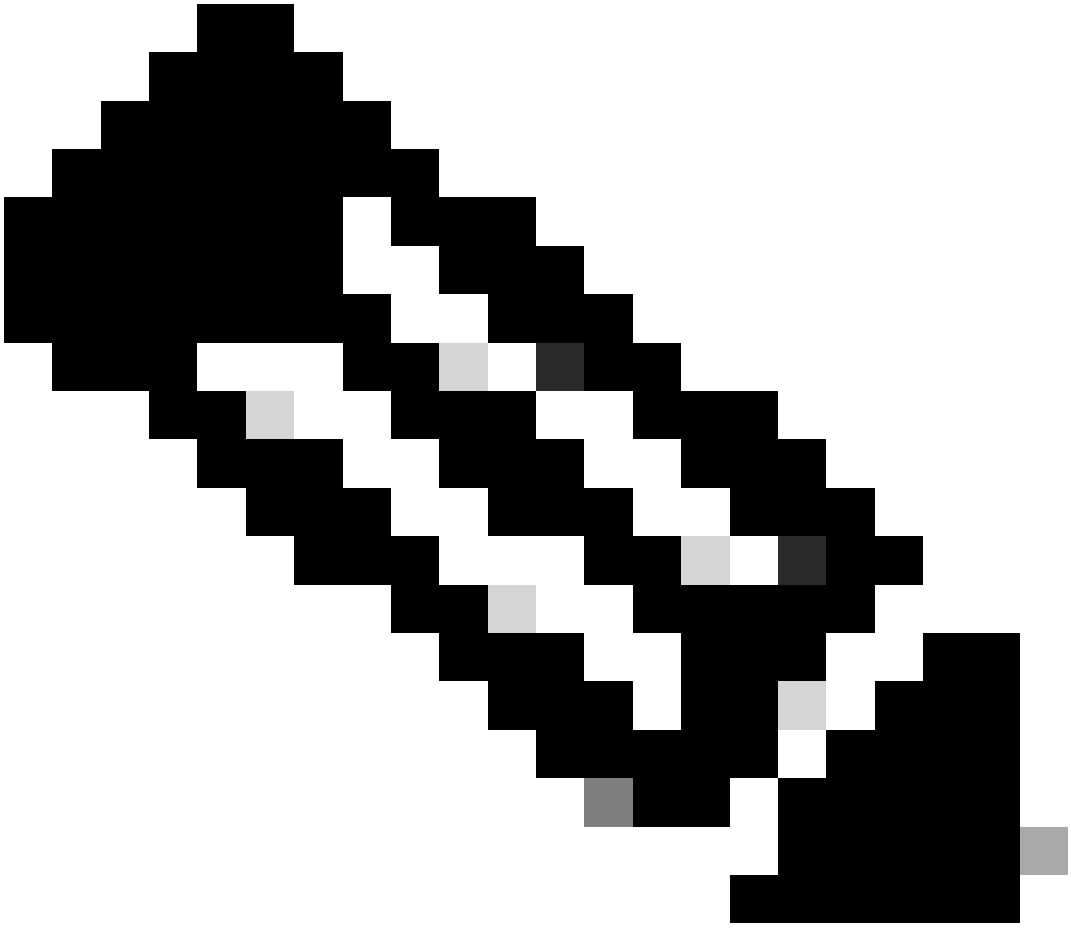
Esta guía tiene como objetivo ayudar a los administradores de red a configurar SNMP en un extremo remoto a través de una VPN de sitio a sitio en una interfaz de datos de un dispositivo FTD. Esta configuración resulta útil para supervisar y administrar dispositivos de red de forma remota. En esta configuración, se utiliza SNMP v2 y el tráfico SNMP se envía desde la interfaz de datos de FTD a un servidor SNMP remoto a través de una VPN de sitio a sitio establecida con un ASA.

La interfaz utilizada se denomina "interna", pero esta configuración se puede aplicar a otros tipos de tráfico "listo para usar" y puede utilizar cualquier interfaz del firewall que no sea aquella en la que termina la VPN.



Nota: SNMP sólo se puede configurar a través de la API REST cuando FTD ejecuta la versión 6.7 y posteriores, y FDM lo administra.

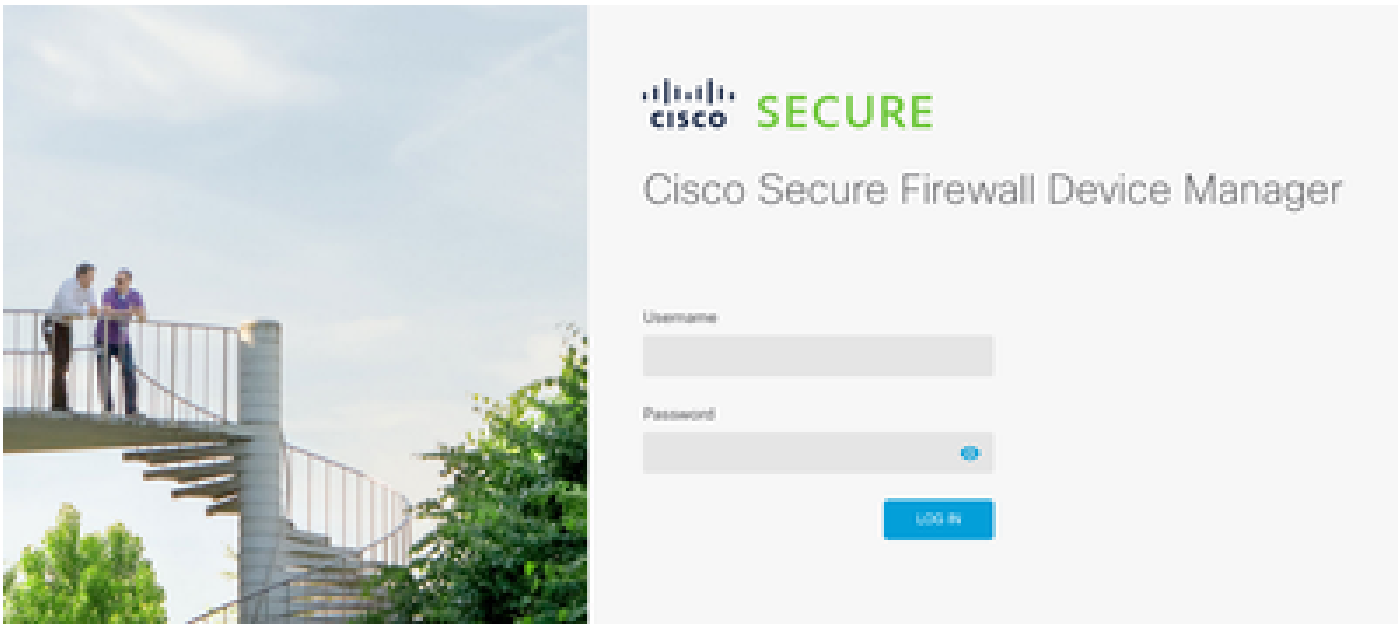
Configurar



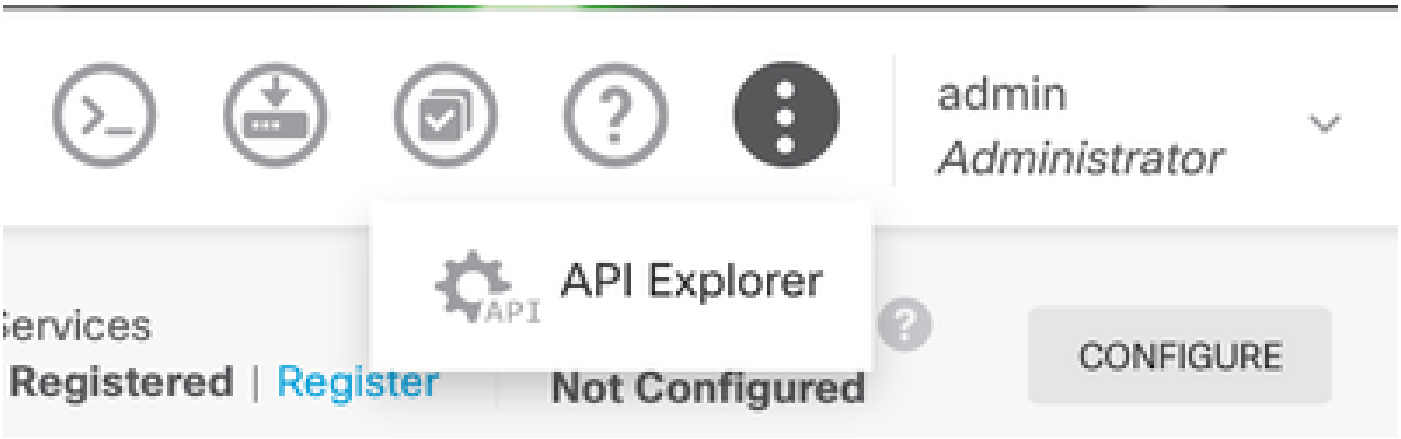
Nota: Esta configuración considera que la VPN de sitio a sitio ya está configurada entre los dispositivos. Para obtener más información sobre cómo configurar la VPN sitio a sitio, consulte la guía de configuración. Configuración de VPN de sitio a sitio en FTD gestionado por FDM

Configuraciones

1. Inicie sesión en el FTD.



2. En la descripción general de Device, navegue hasta el explorador de API.



3. Configure SNMPv2 en FTD

- Obtener información de la interfaz.

4. Desplácese hacia abajo y seleccione el botón Try it out! para realizar la llamada a la API. Una llamada correcta devuelve el código de respuesta 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

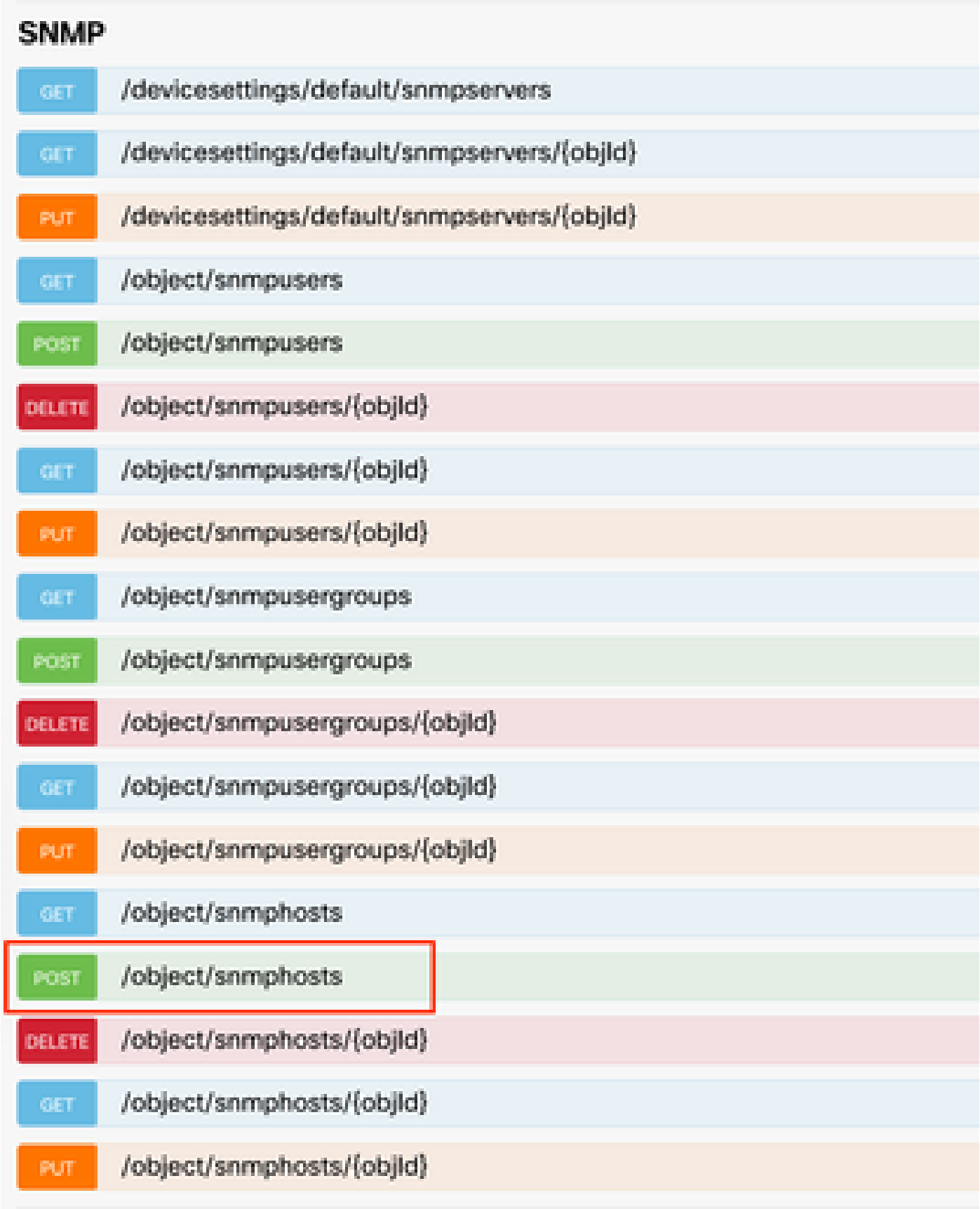

```
    },
    {
      "version": "mqjiipiswsgsx",
      "name": "inside",
      "description": null,
      "hardwareName": "GigabitEthernet0/1",
      "monitorInterface": false,
      "ipv4": {
        "ipType": "STATIC",
        "defaultRouteUsingDHCP": false,
        "dhcpRouteMetric": null,
    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


Response Code

```
200
```

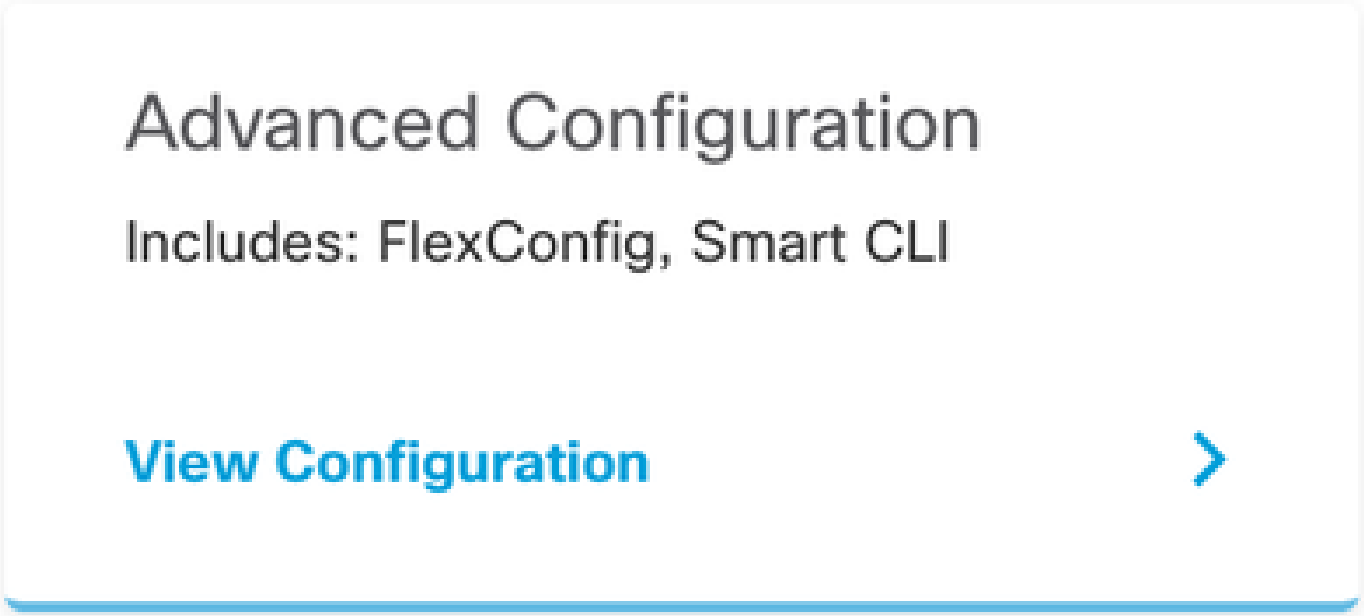
- Cree una configuración de objeto de red para el host SNMP.

- Cree un nuevo objeto de host SNMPv2c.

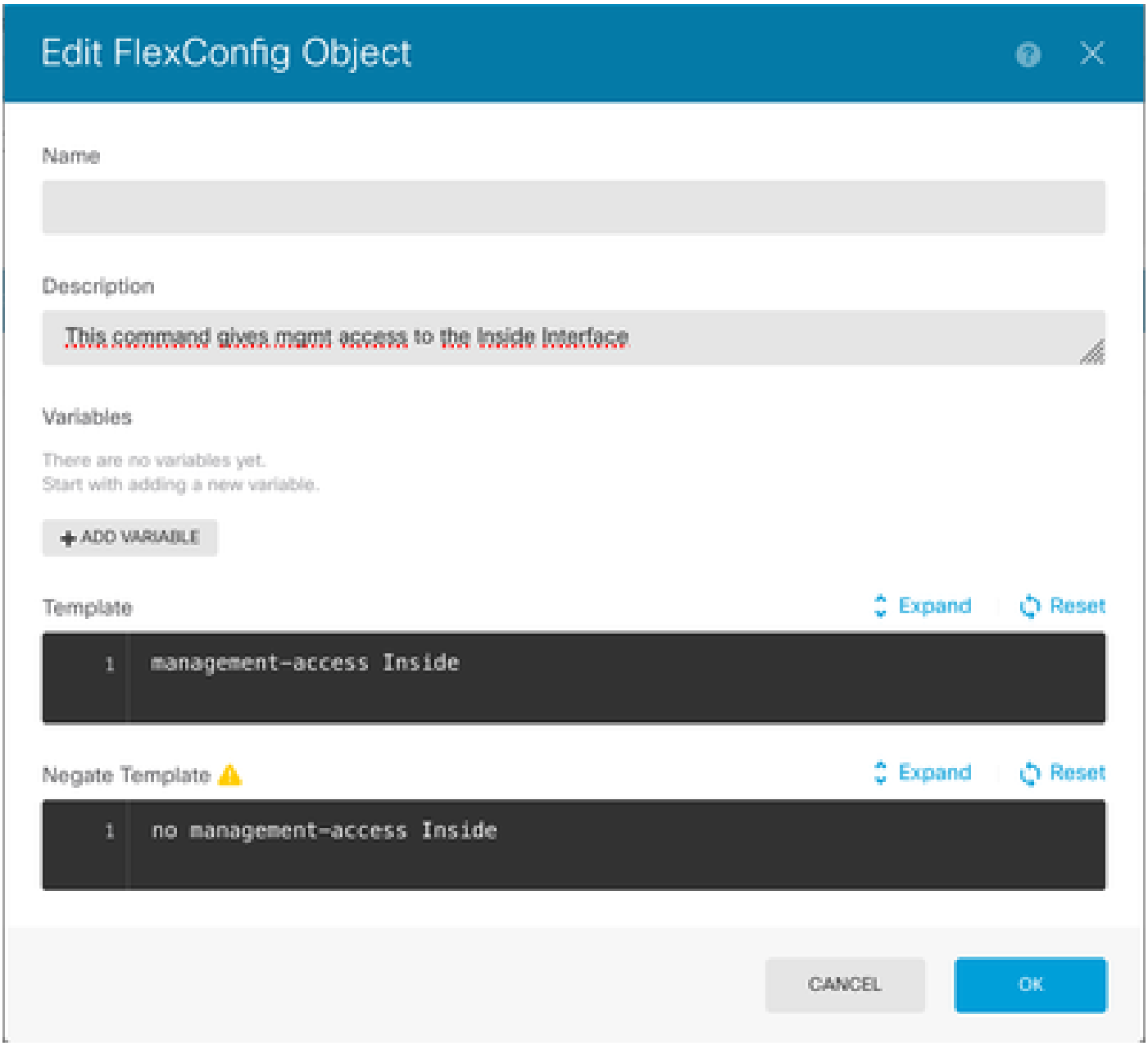


Para obtener más información, consulte la guía de configuración y configure y solucione los problemas de SNMP en Firepower FDM

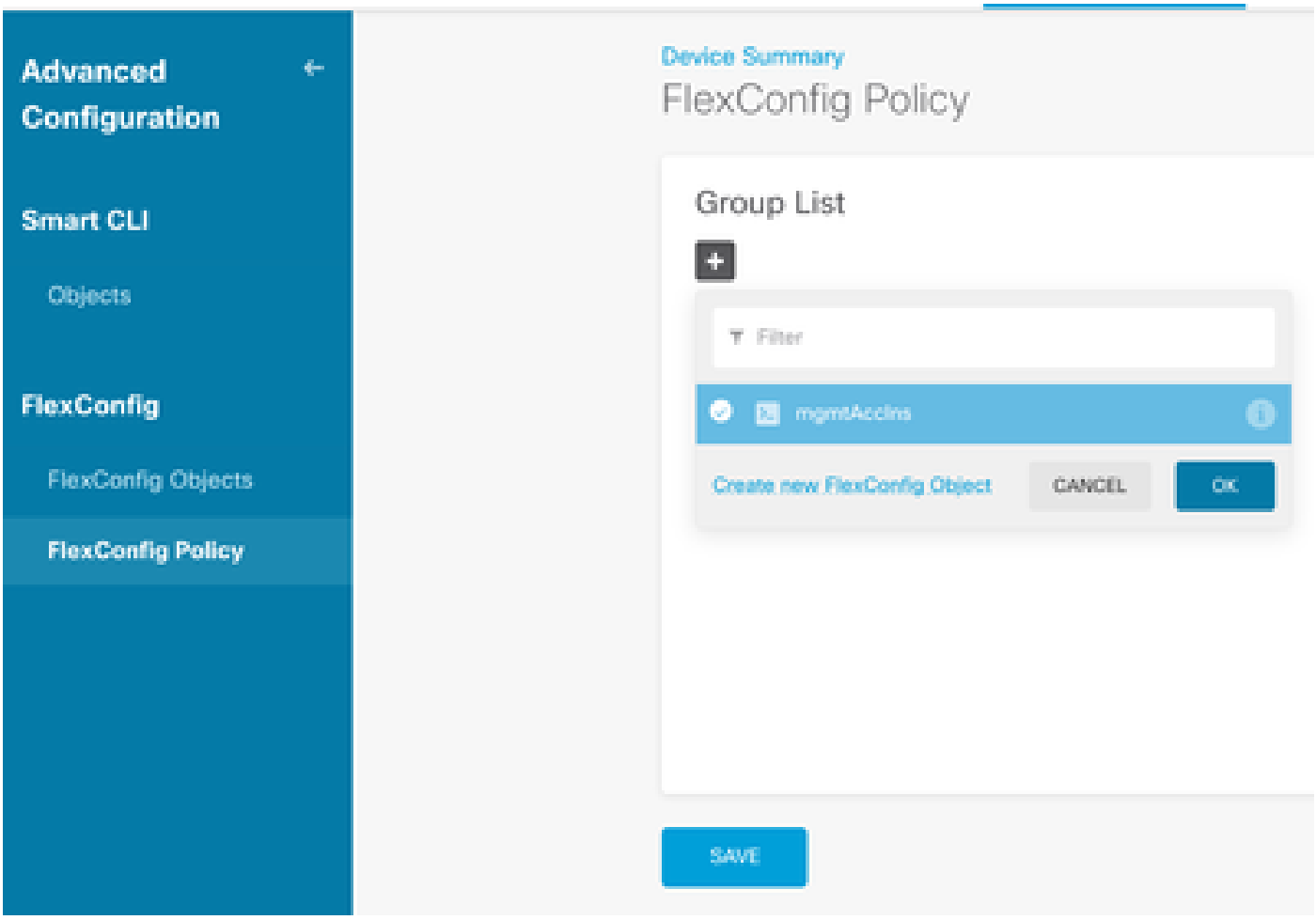
5. Una vez que SNMP esté configurado en el dispositivo, navegue hasta Device en la sección Advanced Configuration y seleccione View Configuration.



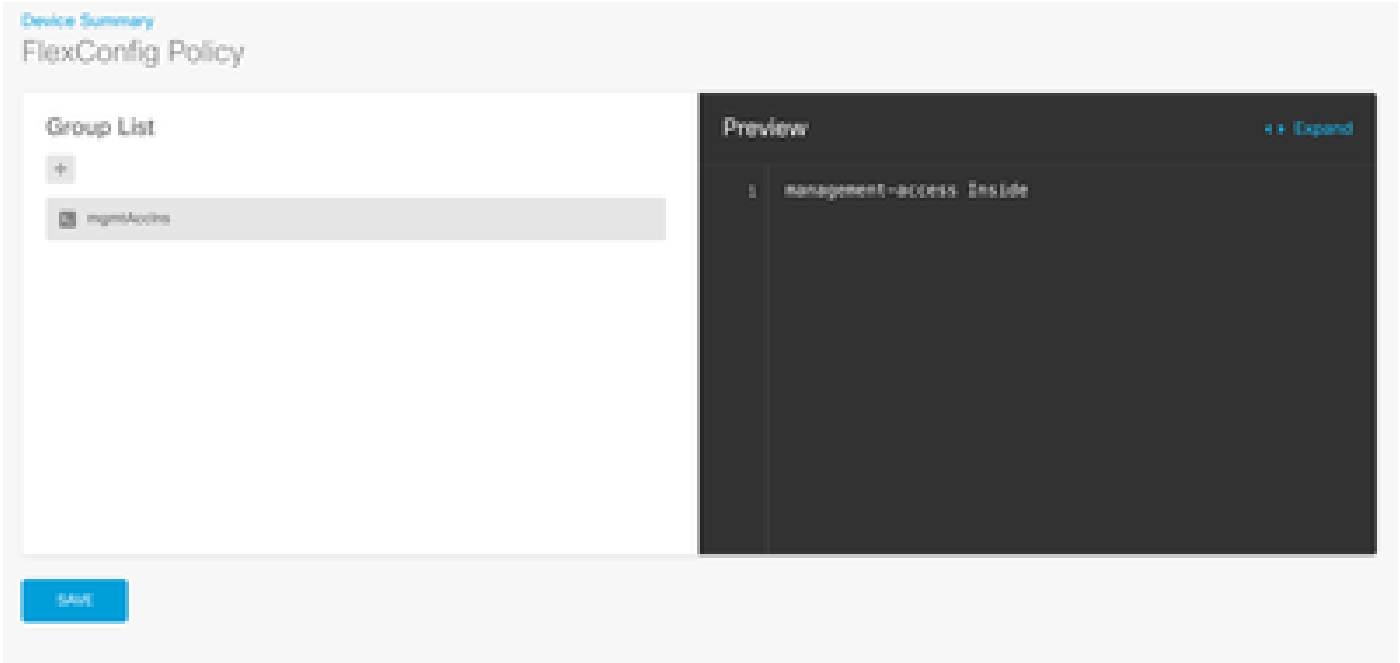
6. En la sección FlexConfig, seleccione objetos FlexConfig y cree un nuevo objeto, asígnele un nombre y agregue el comando management-access en la sección de plantilla, especifique la interfaz y agregue el comando negation en la parte de negación de plantilla.



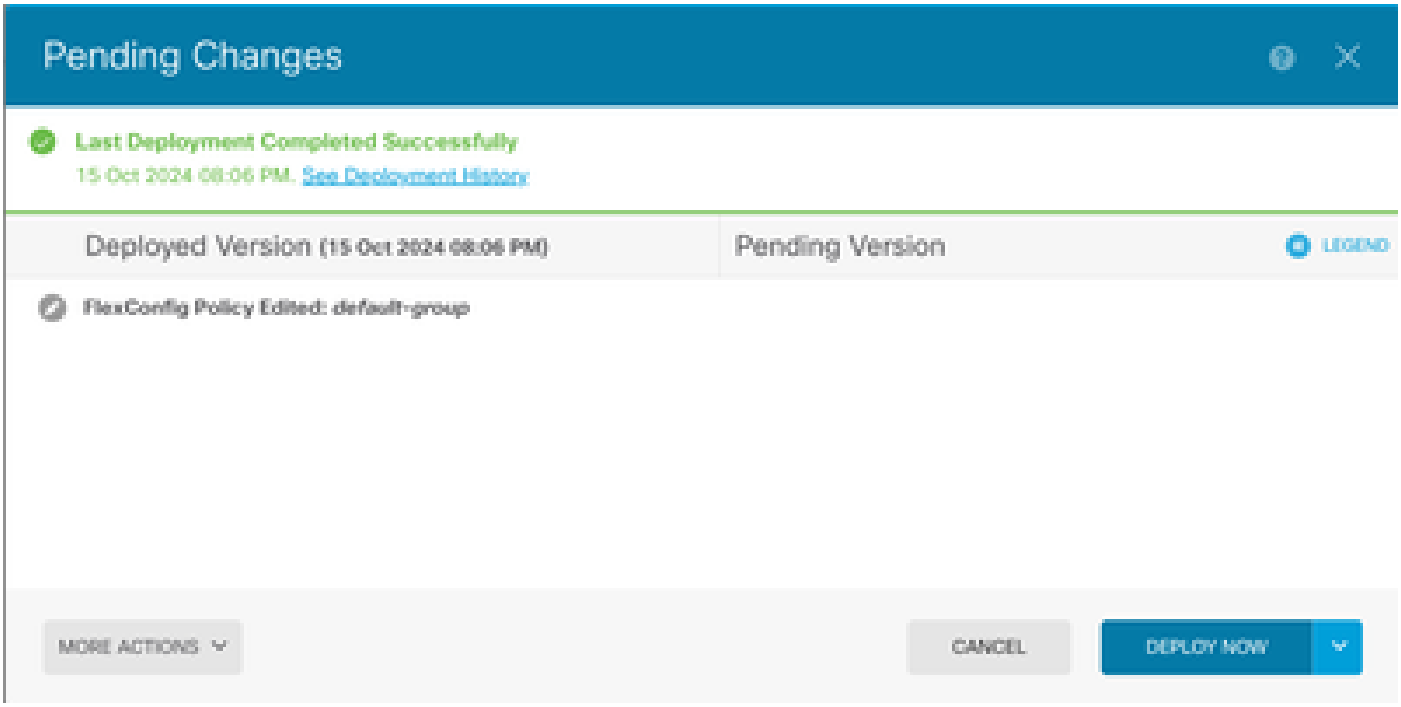
7. En la sección FlexConfig, seleccione FlexConfig Policy, haga clic en el icono Add (Agregar) y seleccione el objeto FlexConfig que creamos en el paso anterior. A continuación, seleccione OK (Aceptar).

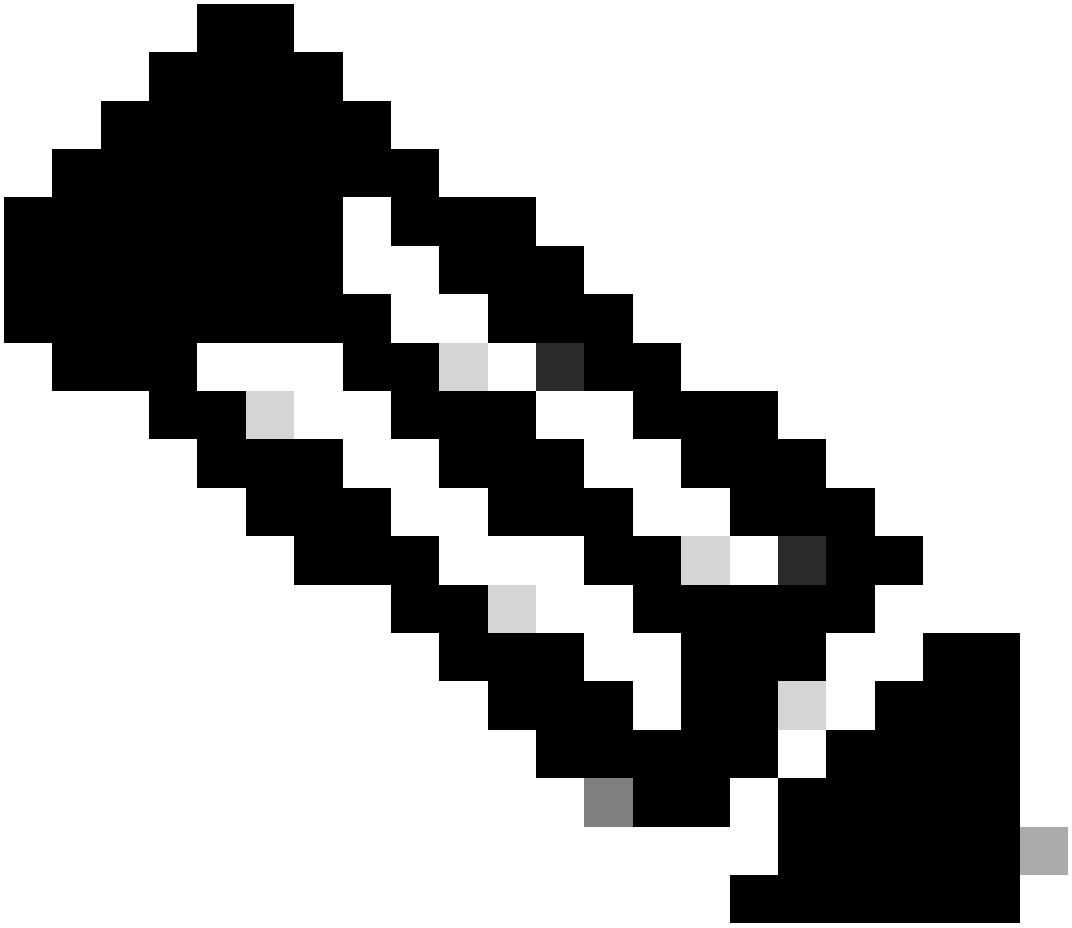


8. A continuación, aparece una vista previa de los comandos que se aplicarán al dispositivo. Seleccione Guardar.



9. Despliegue la configuración, seleccione el icono de despliegue y haga clic en Desplegar ahora.


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: Asegúrese de que se ha completado de forma satisfactoria. Puede comprobar la lista de tareas para confirmarla.

Verificación

Para verificar la configuración, realice estas comprobaciones, inicie sesión en el FTD a través de SSH o la consola y ejecute estos comandos:

- Verifique que la configuración en ejecución del dispositivo contenga los cambios que hicimos.

```
> 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
```

- Realice una prueba desde el probador SNMP y asegúrese de que se completa con éxito.

Troubleshoot

Si tiene algún problema, siga estos pasos:

- Asegúrese de que el túnel VPN esté activo y en funcionamiento; puede ejecutar estos comandos para verificar el túnel 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
```

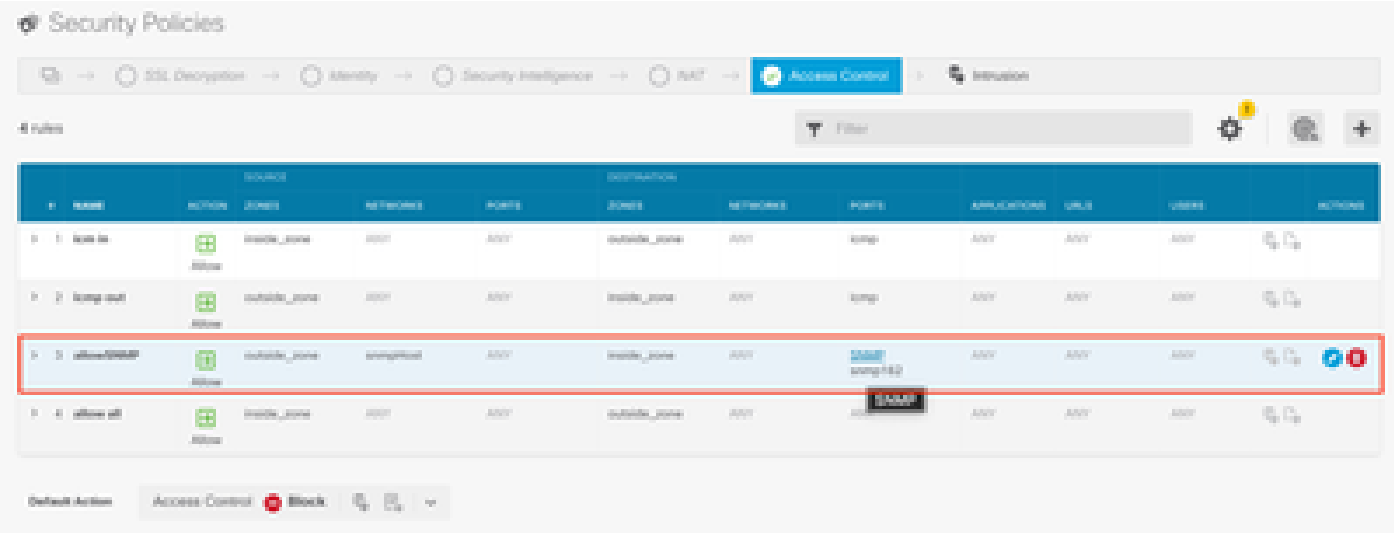
Una guía detallada sobre cómo depurar túneles IKEv2 se puede encontrar aquí: Cómo depurar VPN IKEv2

- Verifique la configuración de SNMP y asegúrese de que la cadena de comunidad y la configuración de control de acceso sean correctas en ambos extremos.

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 *****

- Asegúrese de que se permite el tráfico SNMP a través del FTD.

Navegue hasta Políticas > Control de acceso y verifique que tenga una regla que permita el tráfico SNMP.



- Utilice la captura de paquetes para monitorear el tráfico SNMP e identificar cualquier problema.

Habilite la captura con seguimiento en el 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
```

Para obtener más información, consulte la guía de configuración de SNMP, configure y solucione problemas de SNMP en Firepower FDM

Información Relacionada

- Guía de configuración de Cisco Secure Firepower Device Manager
- Guía de configuración de Cisco ASA
- Configuración SNMP en dispositivos Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).