Configurar o SNMP na VPN Site a Site na Interface de Dados Gerenciados pelo FDM

Contents

Introdução

Este documento descreve a configuração do SNMP para uma extremidade remota através de uma VPN site a site em uma interface de dados de um dispositivo FTD interface de dados.

Pré-requisitos

Antes de prosseguir com a configuração, verifique se estes pré-requisitos estão em vigor:

- Noções básicas sobre estes tópicos:
  - Cisco Firepower Threat Defense (FTD) gerenciado pelo Firepower Device Manager (FDM).
  - Cisco Adaptive Security Appliance (ASA).
  - Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol).
  - Virtual Private Network (VPN).
- Acesso administrativo aos dispositivos FTD e ASA.
- Certifique-se de que sua rede esteja ativa e que você entenda o impacto potencial de qualquer comando.

Requisitos

- Cisco FTD gerenciado pelo FDM versão 7.2.7
- Cisco ASA versão 9.16
- Detalhes do servidor SNMP (incluindo endereço IP, série de comunidade)
- Detalhes de configuração da VPN site a site (incluindo IP de mesmo nível, chave pré-

compartilhada)
- O FTD deve ser pelo menos da versão 6.7 para usar a API REST para configurar o SNMP.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Firepower Threat Defense (FTD) gerenciado pelo Firepower Device Manager (FDM) versão 7.2.7.
- Cisco Adaptive Security Appliance (ASA) versão 9.16.
- Servidor SNMP (qualquer software de servidor SNMP padrão)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

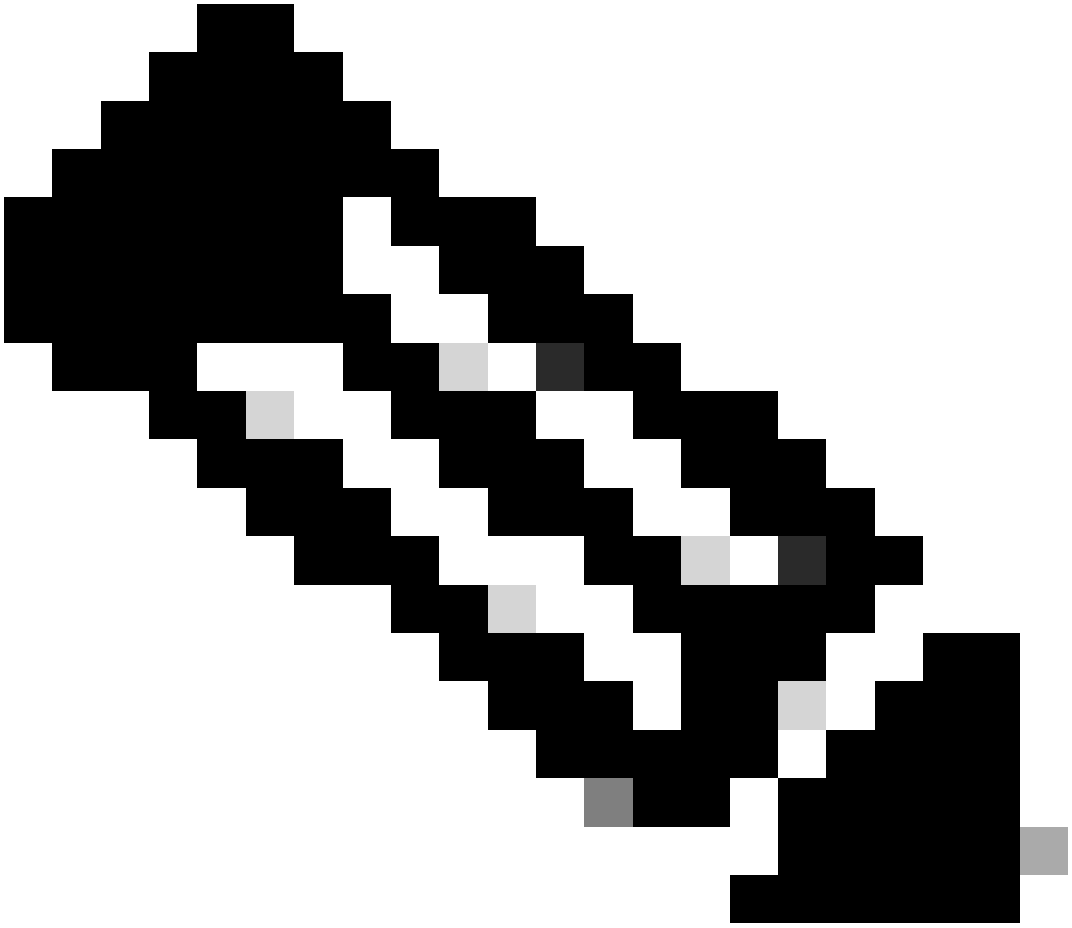
Informações de Apoio

Com essas etapas descritas, os administradores de rede podem garantir o monitoramento remoto de seus dispositivos de rede.

O SNMP (Simple Network Management Protocol) é usado para gerenciamento e monitoramento de rede. Nesta configuração, o tráfego SNMP é enviado do FTD para um servidor SNMP remoto através de uma VPN site a site estabelecida com um ASA.

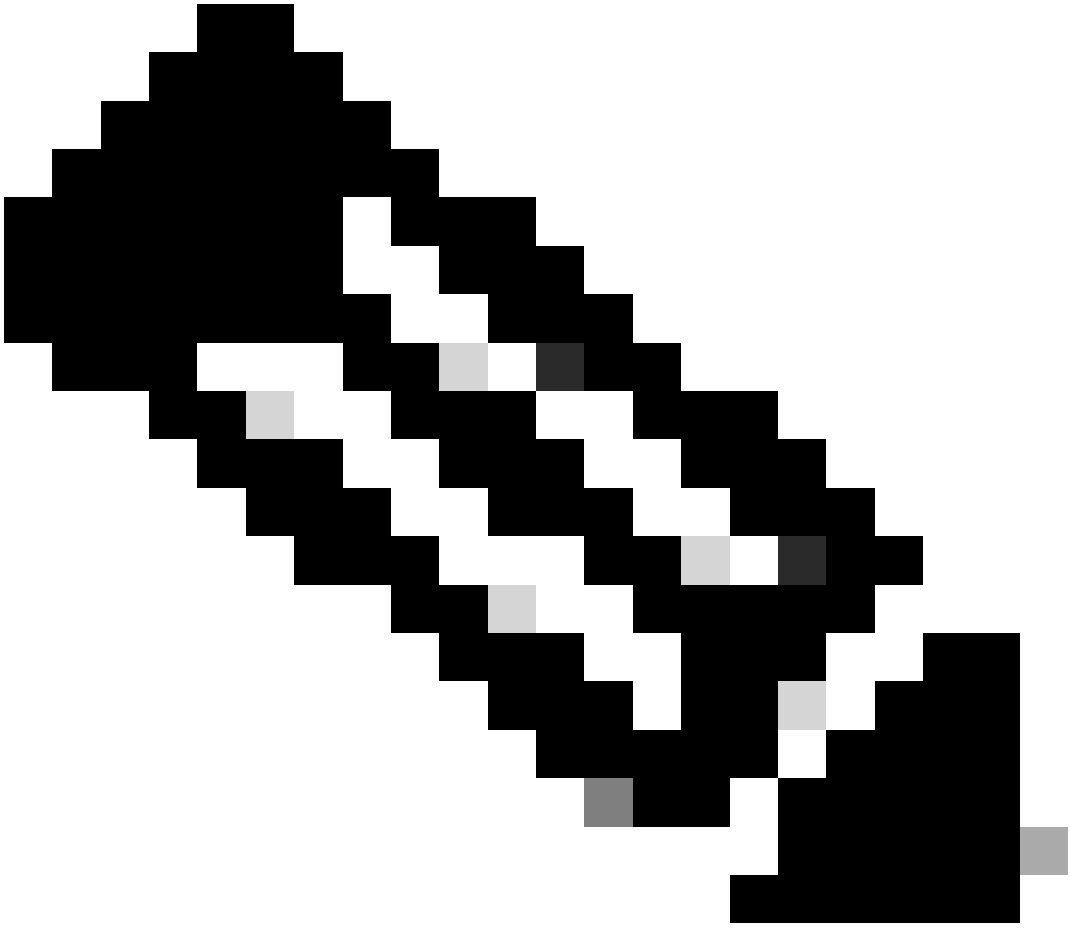
Este guia tem como objetivo ajudar os administradores de rede a configurar o SNMP para uma extremidade remota através de uma VPN site a site em uma interface de dados de um dispositivo FTD. Essa configuração é útil para monitorar e gerenciar dispositivos de rede remotamente. Nesta configuração, o SNMP v2 é usado e o tráfego SNMP é enviado da interface de dados FTD para um servidor SNMP remoto através de uma VPN site a site estabelecida com um ASA.

A interface usada é chamada de "interna", mas essa configuração pode ser aplicada a outros tipos de tráfego "para a caixa" e pode utilizar qualquer interface do firewall que não seja aquela em que a VPN termina.



Observação: o SNMP só pode ser configurado via API REST quando o FTD executa a versão 6.7 e posterior e é gerenciado pelo FDM.

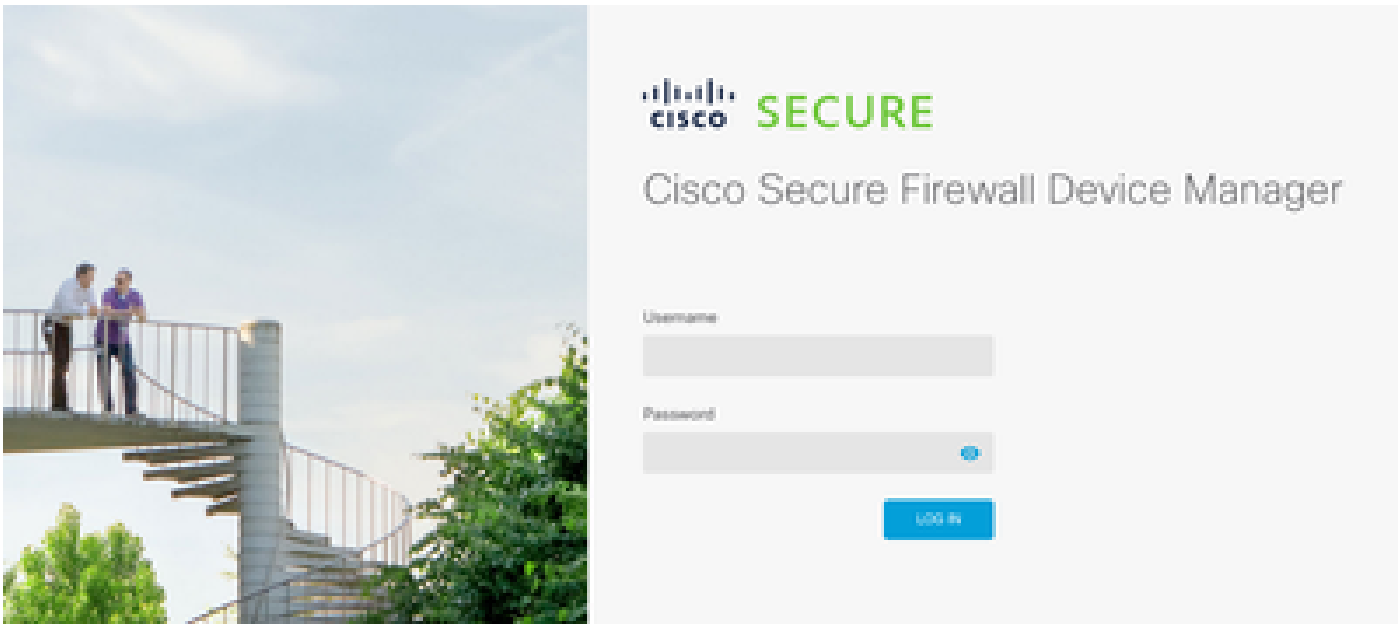
Configurar



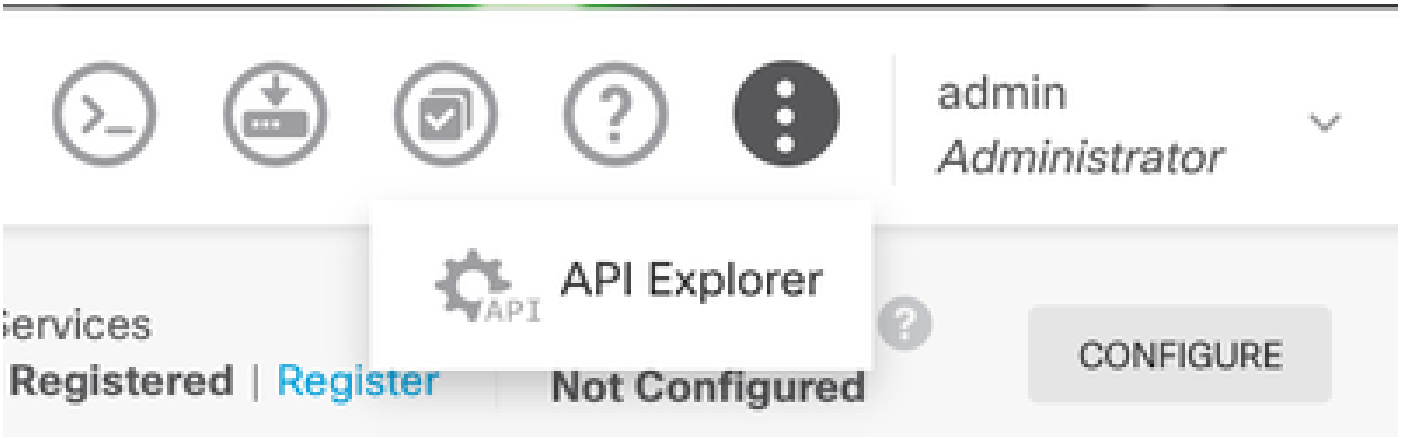
Observação: essa configuração considera que a VPN site a site já está configurada entre os dispositivos. Para obter detalhes adicionais sobre como configurar a VPN site a site, consulte o guia de configuração. Configurar VPN Site a Site no FTD gerenciado pelo FDM

Configurações

1. Efetue login no seu FTD.



2. Na visão geral do dispositivo, navegue até o explorador de API.



3. Configurar o SNMPv2 no FTD

- Obter informações de interface.

4. Role para baixo e selecione o botão Try it out! para fazer a chamada à API. Uma chamada bem-sucedida retorna o código de resposta 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

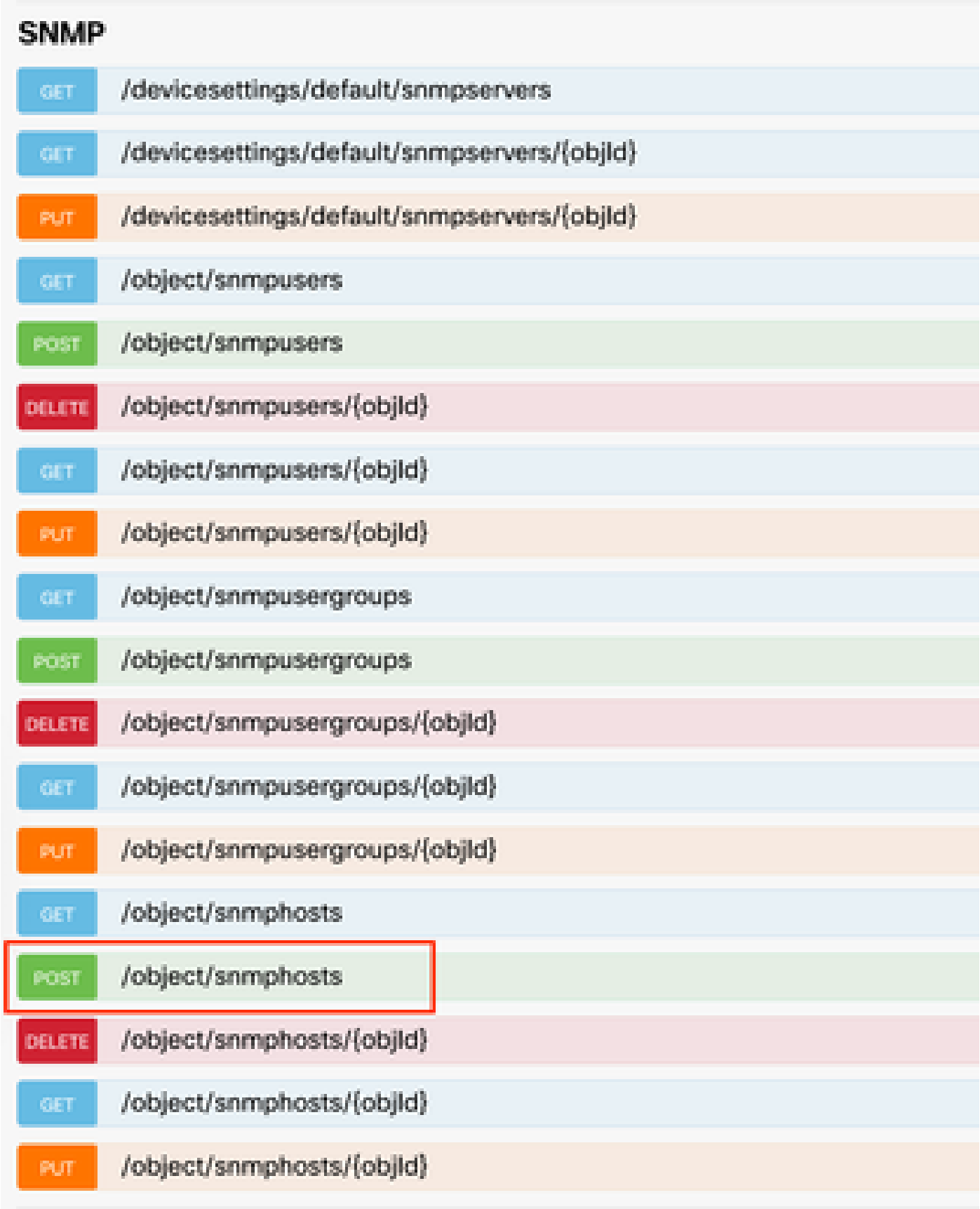

```
    },
    {
      "version": "mqjiipiswsgsx",
      "name": "inside",
      "description": null,
      "hardwareName": "GigabitEthernet0/1",
      "monitorInterface": false,
      "ipv4": {
        "ipType": "STATIC",
        "defaultRouteUsingDHCP": false,
        "dhcpRouteMetric": null,
    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


Response Code

```
200
```

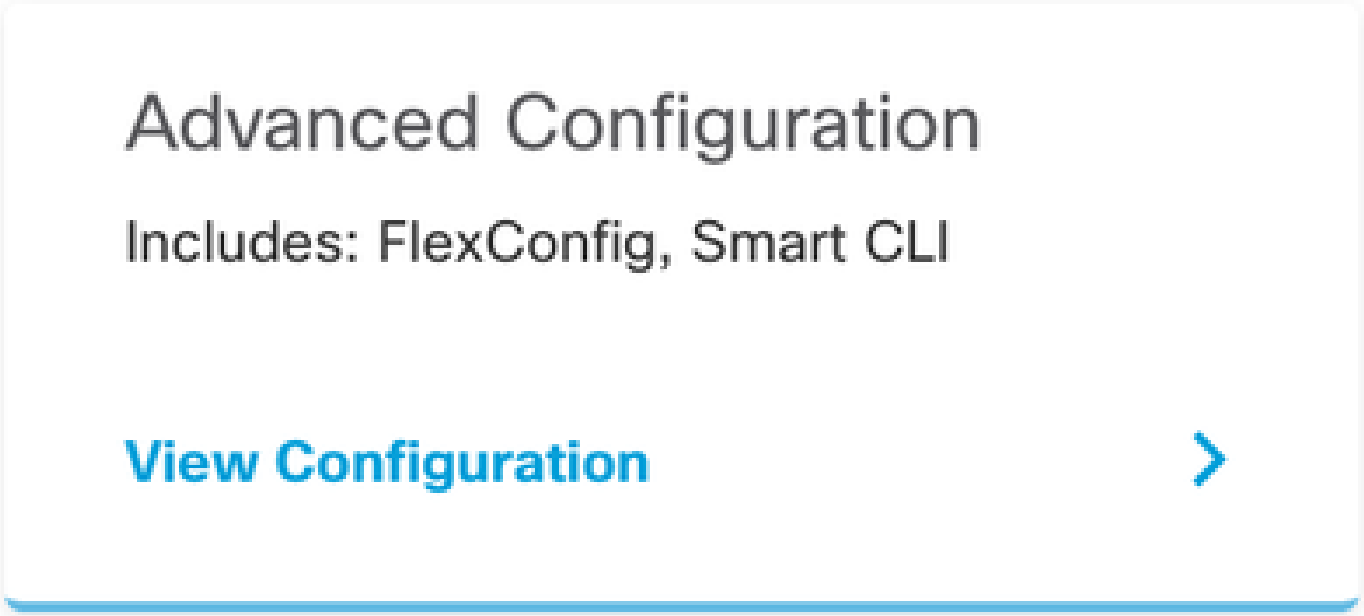
- Crie uma configuração de objeto de rede para o host SNMP.

- Crie um novo objeto de host SNMPv2c.

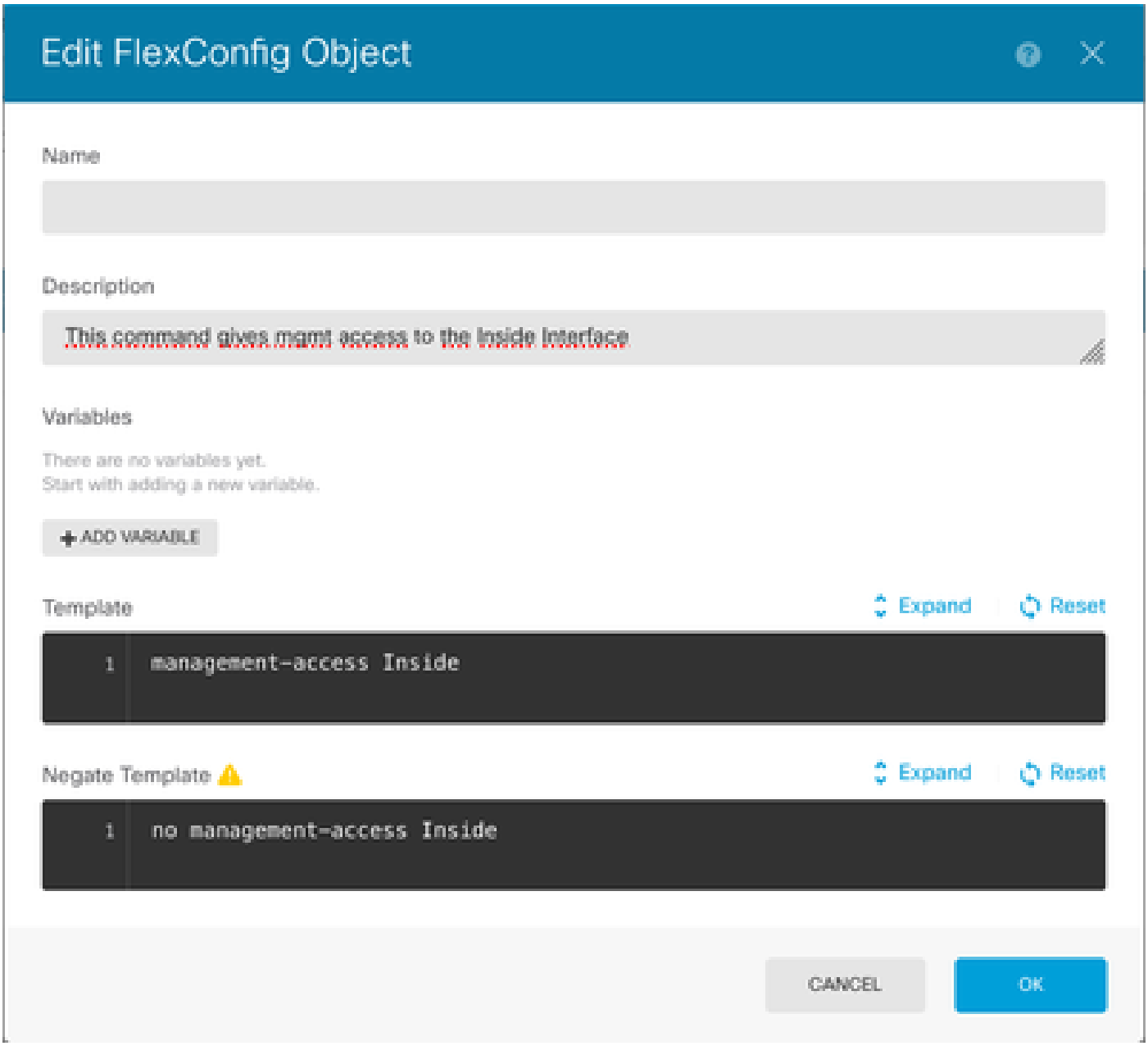


Para obter detalhes adicionais, consulte o Guia de configuração, [Configurar e solucionar problemas de SNMP no Firepower FDM]

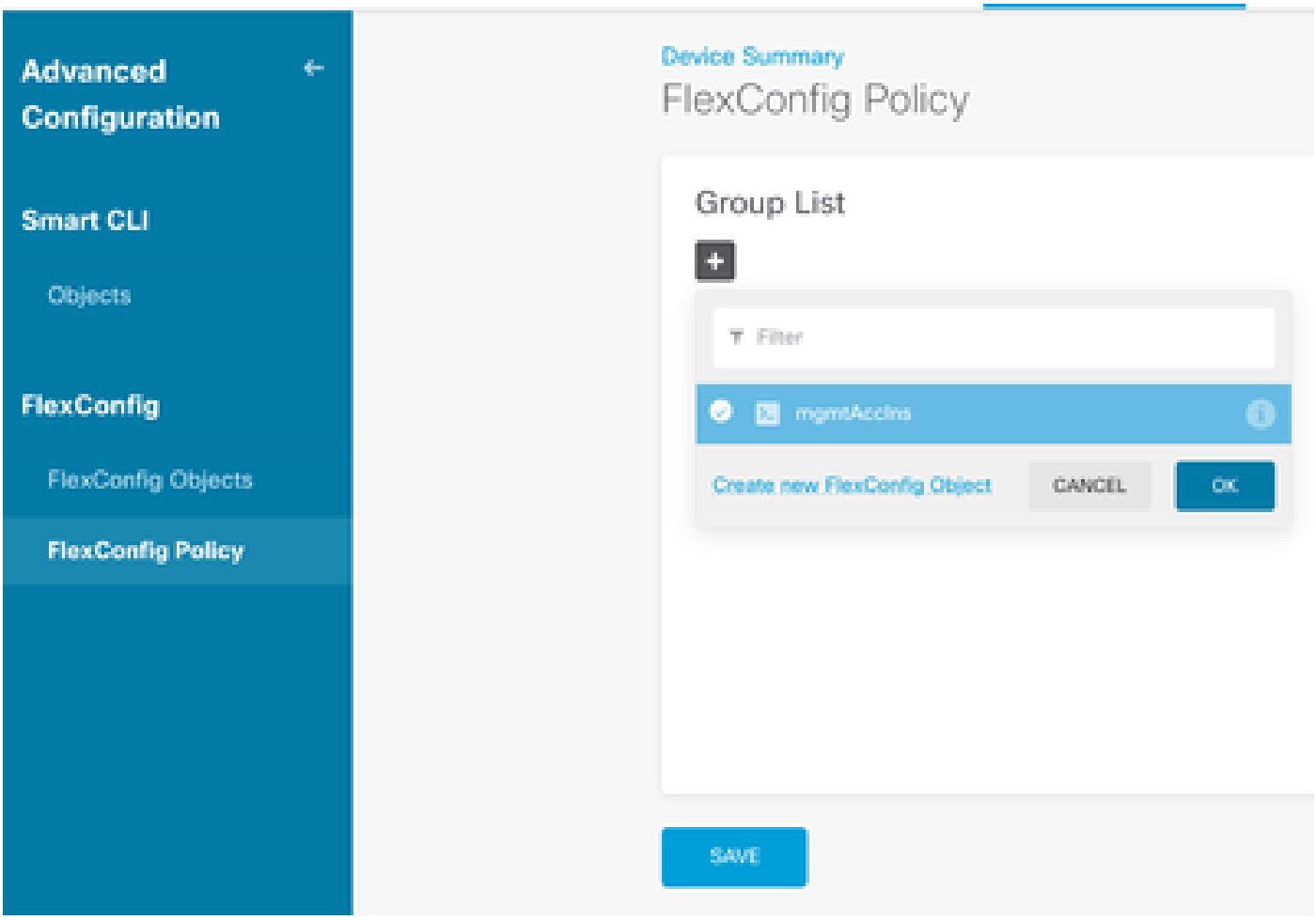
5. Depois que o SNMP estiver configurado no dispositivo, navegue até Device na seção Advanced Configuration e selecione View Configuration.



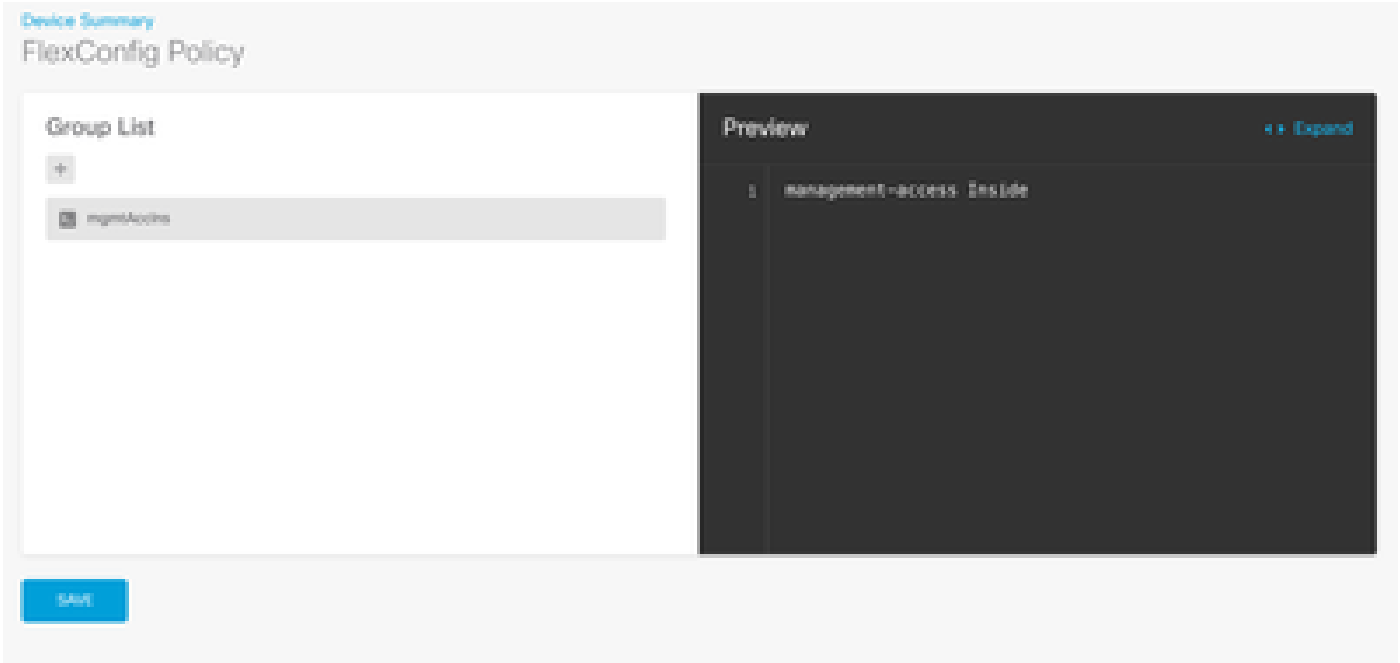
6. Na seção FlexConfig, selecione objetos FlexConfig e crie um novo objeto, nomeie-o e adicione o comando management-access na seção de modelo, especifique a interface e adicione a negação de comando na parte de negação de modelo.



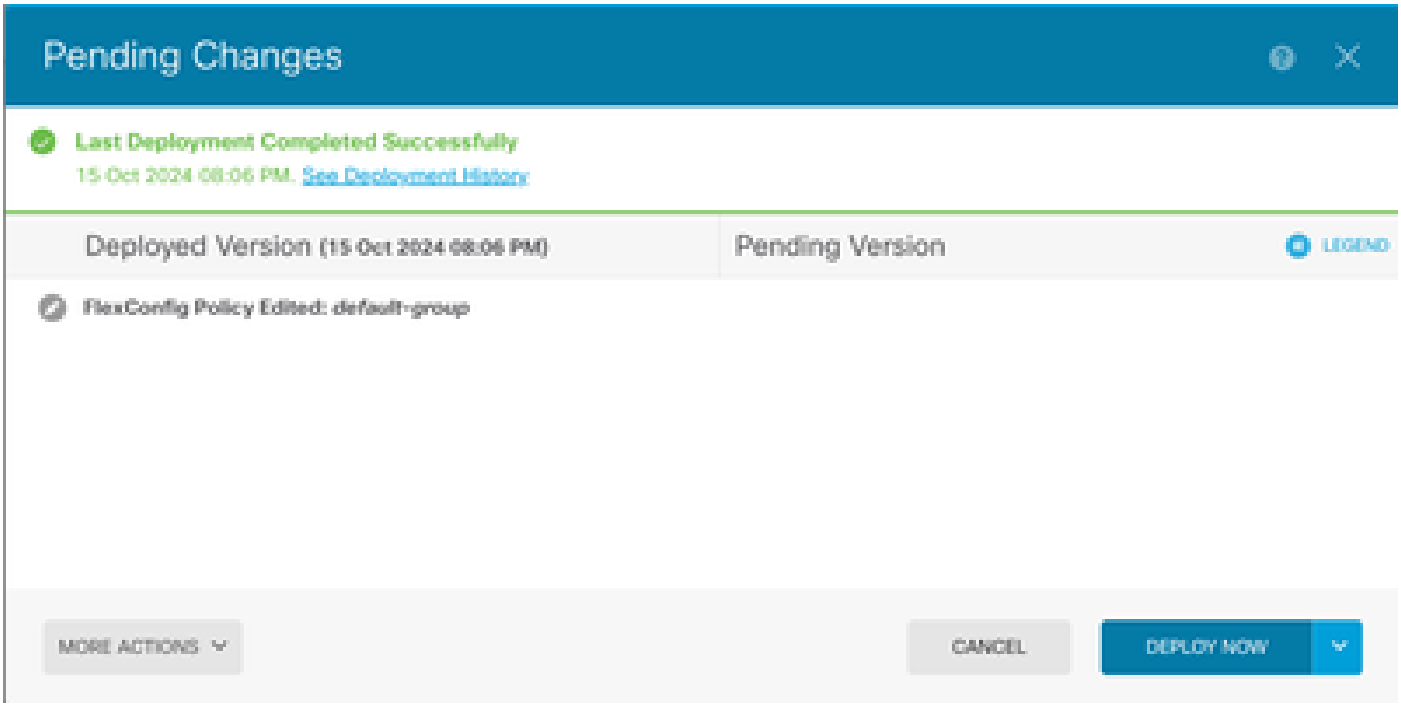
7. Na seção FlexConfig, selecione FlexConfig Policy, clique no ícone add e selecione o objeto flexConfig que criamos na etapa anterior e selecione OK.

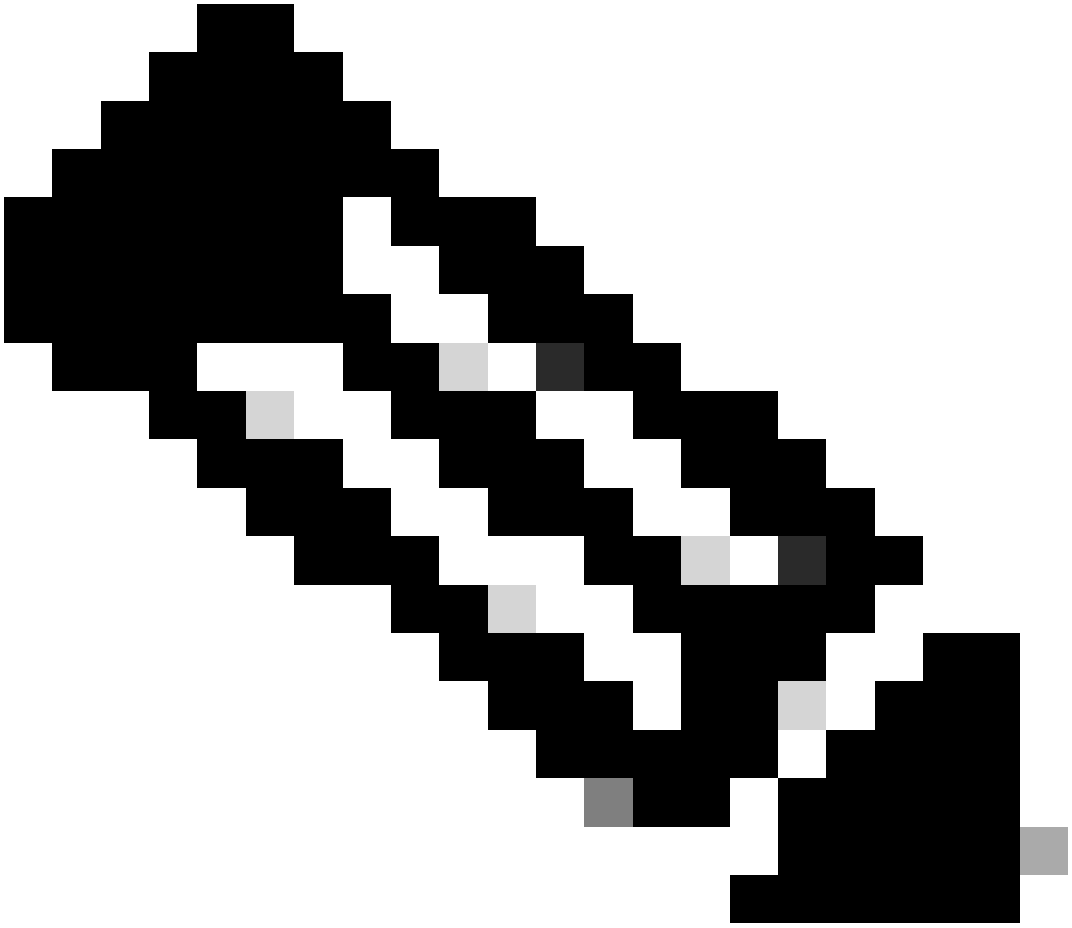


8. Em seguida, uma visualização dos comandos a serem aplicados ao dispositivo é exibida. Selecione Save.



9. Disponibilize a configuração, selecione o ícone de disponibilização e clique em disponibilizar agora.


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



Observação: certifique-se de que ela esteja concluída de forma satisfatória; você pode verificar a lista de tarefas para confirmá-la.

Verificar

Para verificar a configuração, execute estas verificações, efetue login no FTD via SSH ou console e execute estes comandos:

- Verifique se a configuração atual do dispositivo contém as alterações que fizemos.

```
> 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
```

- Execute um teste do testador SNMP e certifique-se de que ele seja concluído com êxito.

Troubleshooting

Se você encontrar algum problema, considere estas etapas:

- Certifique-se de que o túnel VPN esteja ativo e em execução, você pode executar estes comandos para verificar o 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
```

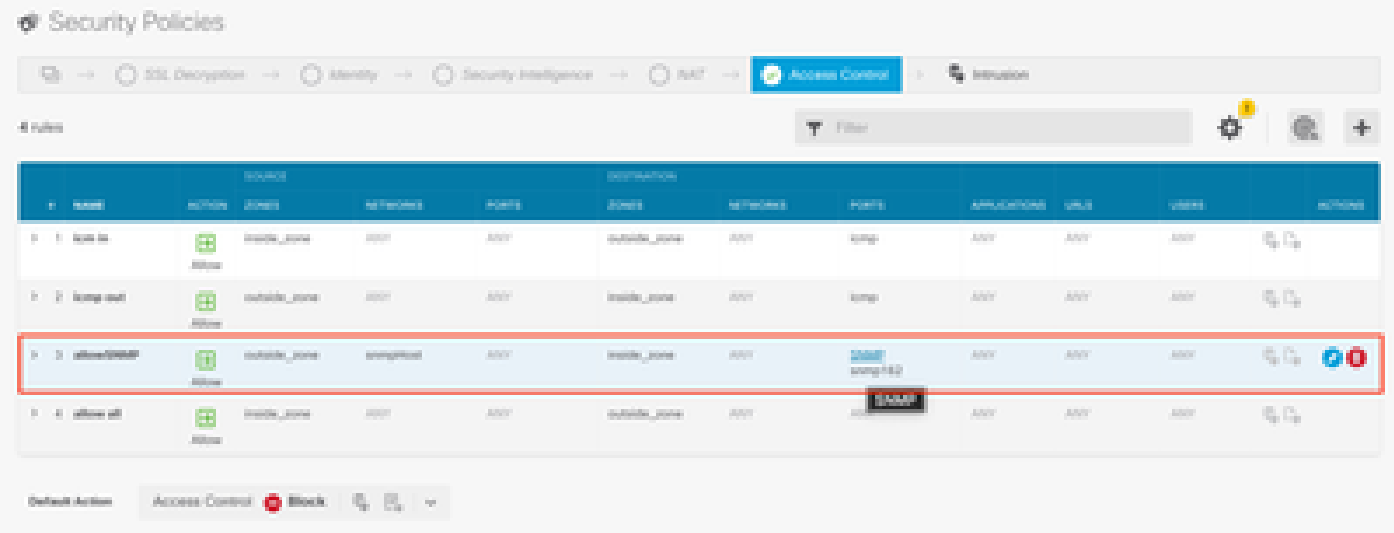
Um guia detalhado sobre como depurar túneis IKEv2 pode ser encontrado aqui: Como depurar VPNs IKEv2

- Verifique a configuração do SNMP e certifique-se de que a sequência de caracteres da comunidade e as configurações de controle de acesso estejam corretas em ambas as extremidades.

firepower# sh run snmp-server
snmp-server host dentro da comunidade 10.56.58.10 ***** versão 2c
snmp-server location null
snmp-server contact null
snmp-server community *****

- Certifique-se de que o tráfego SNMP esteja sendo permitido através do FTD.

Navegue para Policies > Access Control e verifique se você tem uma regra que permita o tráfego SNMP.



- Use a captura de pacotes para monitorar o tráfego SNMP e identificar quaisquer problemas.

Habilitar captura com rastreamento no 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 obter detalhes adicionais, consulte o Guia de configuração de SNMP, Configurar e solucionar problemas de SNMP no Firepower FDM

Informações Relacionadas

- Guia de configuração do Cisco Secure Firepower Device Manager
- Guia de configurações do Cisco ASA
- Configuração de SNMP em dispositivos Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.