Configurar interfaces VXLAN no FTD seguro com o FMC seguro

Contents

Introdução

Este documento descreve como configurar as interfaces VXLAN no Secure Firewall Threat Defense (FTD) com o Secure Firewall Management Center (FMC)

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Conceitos básicos de VLAN/VLAN.
- Conhecimento básico de rede.
- Experiência básica do Cisco Secure Management Center.
- Experiência básica do Cisco Secure Firewall Threat Defense.

Componentes Utilizados

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

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware executando a versão 7.2.4.
- Cisco Secure Firewall Threat Defense Virtual Appliance (FTDv) VMware executando a

versão 7.2.4.

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

A VLAN extensível virtual (VXLAN) fornece serviços de rede Ethernet de Camada 2 como a VLAN tradicional. Devido à alta demanda por segmentos de VLAN em ambientes virtuais, a VXLAN fornece maior extensibilidade, flexibilidade e também define um esquema de encapsulamento MAC-em-UDP em que o quadro original de Camada 2 tem um cabeçalho VXLAN adicionado e é então colocado em um pacote UDP-IP. Com esse encapsulamento MAC-em-UDP, a VXLAN faz o encapsulamento da rede de Camada 2 sobre a rede de Camada 3. A VXLAN oferece os próximos benefícios:

- Flexibilidade de VLAN em segmentos multilocatário:
- Maior escalabilidade para lidar com mais segmentos de Camada 2 (L2).
- Melhor utilização da rede.

O Cisco Secure Firewall Threat Defense (FTD) suporta dois tipos de encapsulamento VXLAN.

- VXLAN (usado para todos os modelos de defesa contra ameaças de firewall seguro)
- Geneve (usado para o dispositivo virtual Secure Firewall Threat Defense)

O encapsulamento Geneve é necessário para o roteamento transparente de pacotes entre o balanceador de carga do gateway do Amazon Web Services (AWS) e os dispositivos, e para o envio de informações extras.

O VXLAN usa o VTEP (VXLAN Tunnel Endpoint) para mapear os dispositivos finais dos locatários para segmentos VXLAN e para executar o encapsulamento e o desencapsulamento de VXLAN. Cada VTEP tem dois tipos de interface: uma ou mais interfaces virtuais chamadas interfaces VXLAN Network Identifier (VNI), onde a política de segurança pode ser aplicada, e uma interface regular chamada interface de origem VTEP, onde as interfaces VNI são encapsuladas entre VTEPs. A interface de origem VTEP é conectada à rede IP de transporte para comunicação VTEP-para-VTEP, as interfaces VNI são semelhantes às interfaces VLAN: elas são interfaces virtuais que mantêm o tráfego de rede separado em uma determinada interface física usando marcação. A política de segurança é aplicada a cada interface VNI. Uma interface VTEP pode ser adicionada e todas as interfaces VNI são associadas à mesma interface VTEP. Há uma exceção para clustering virtual de defesa contra ameaças no AWS.

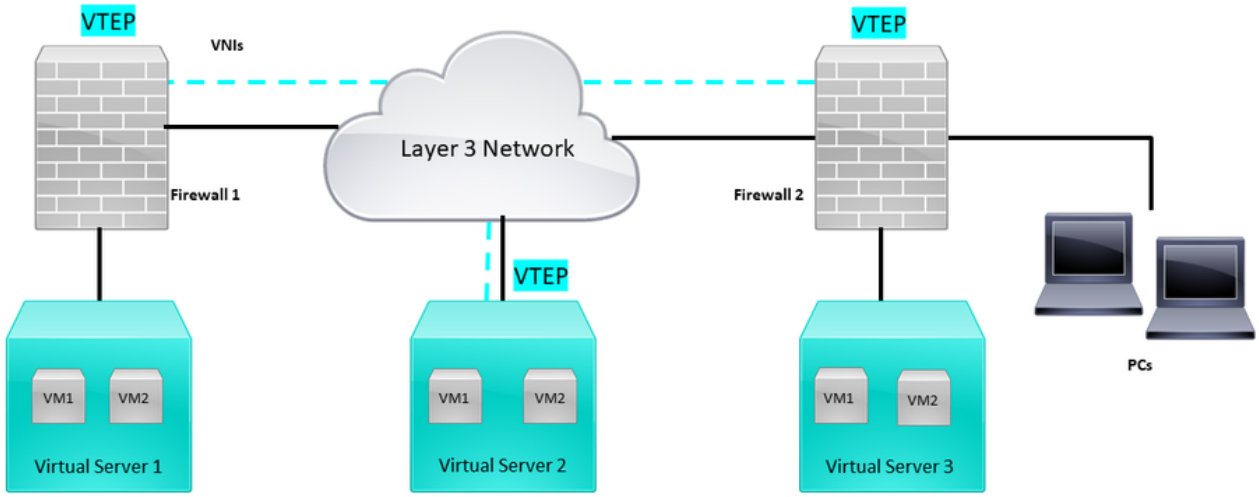
Há três maneiras pelas quais a defesa contra ameaças encapsula e desencapsula:

- Um único endereço IP VTEP de peer pode ser configurado estaticamente na defesa contra ameaças.
- Um grupo de endereços IP VTEP de peer pode ser configurado estaticamente na defesa contra ameaças.

- Um grupo multicast pode ser configurado em cada interface VNI.

Este documento se concentra nas interfaces VXLAN para o encapsulamento VXLAN com um grupo de 2 endereços IP VTEP de peer configurados estaticamente. Se você precisar configurar interfaces Geneve, verifique a documentação oficial para interfaces Geneve no AWS ou configure o VTEP com um único peer ou grupo multicast, verifique a interface VTEP com um único peer ou grupo multicast guia de configuração.

Diagrama de Rede



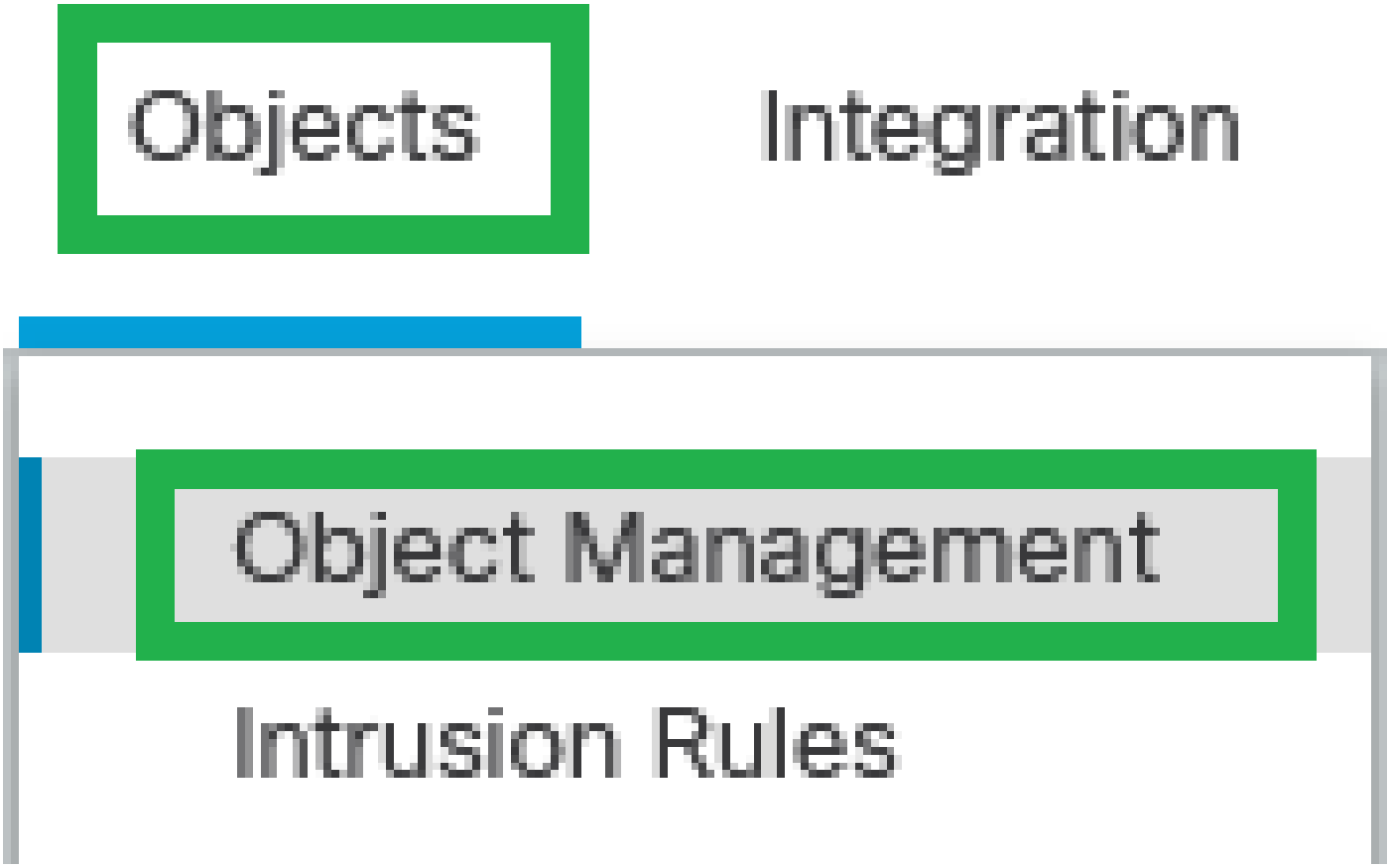
Topologia de rede

A seção configure pressupõe que a rede subjacente já esteja configurada na defesa contra ameaças através do Secure Firewall Management Center. Este documento concentra-se na configuração de rede de sobreposição.

Configurar

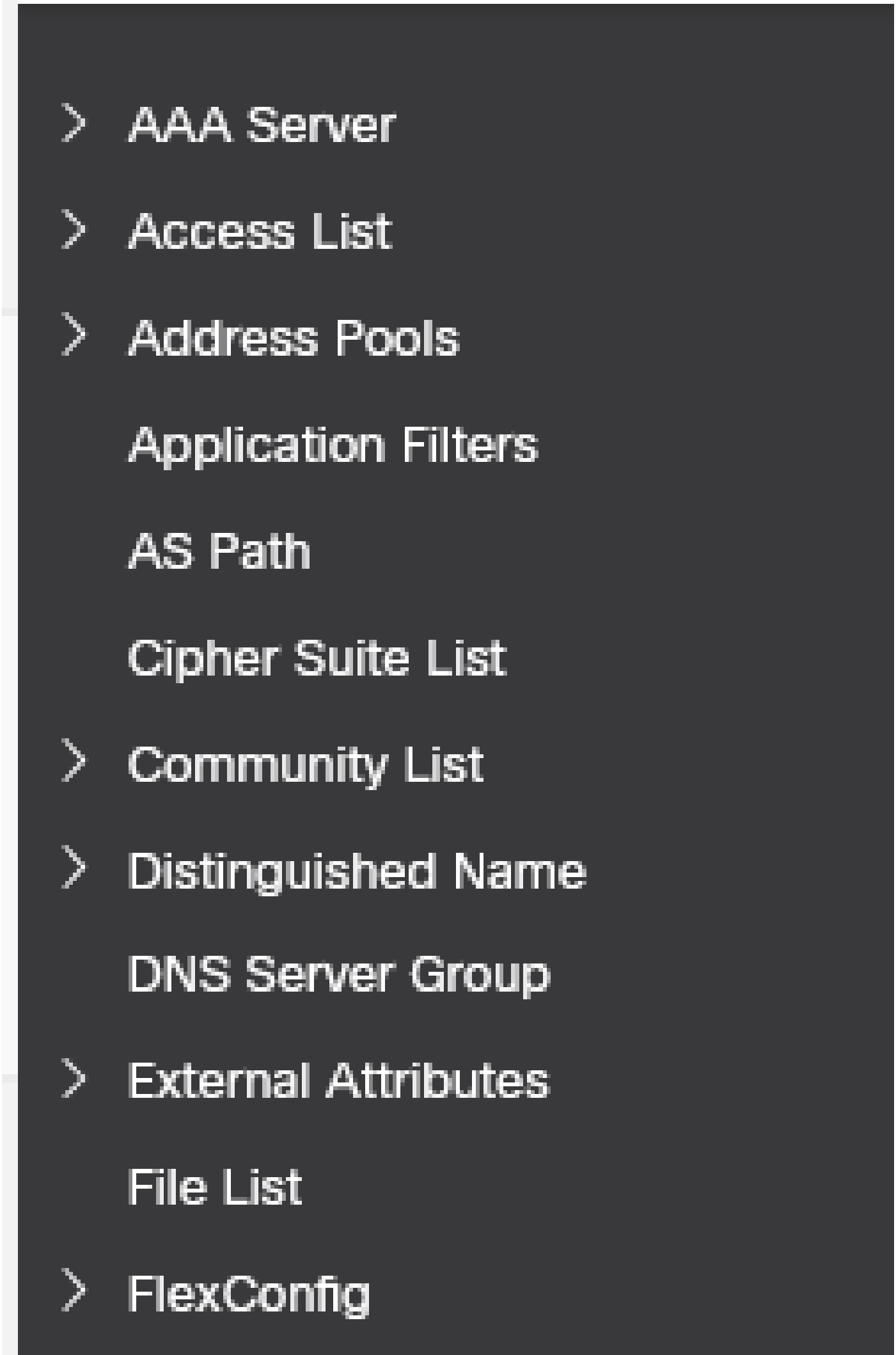
Configurar o grupo de correspondentes do VTEP

Etapa 1: Navegue até Objetos > Gerenciamento de Objetos.



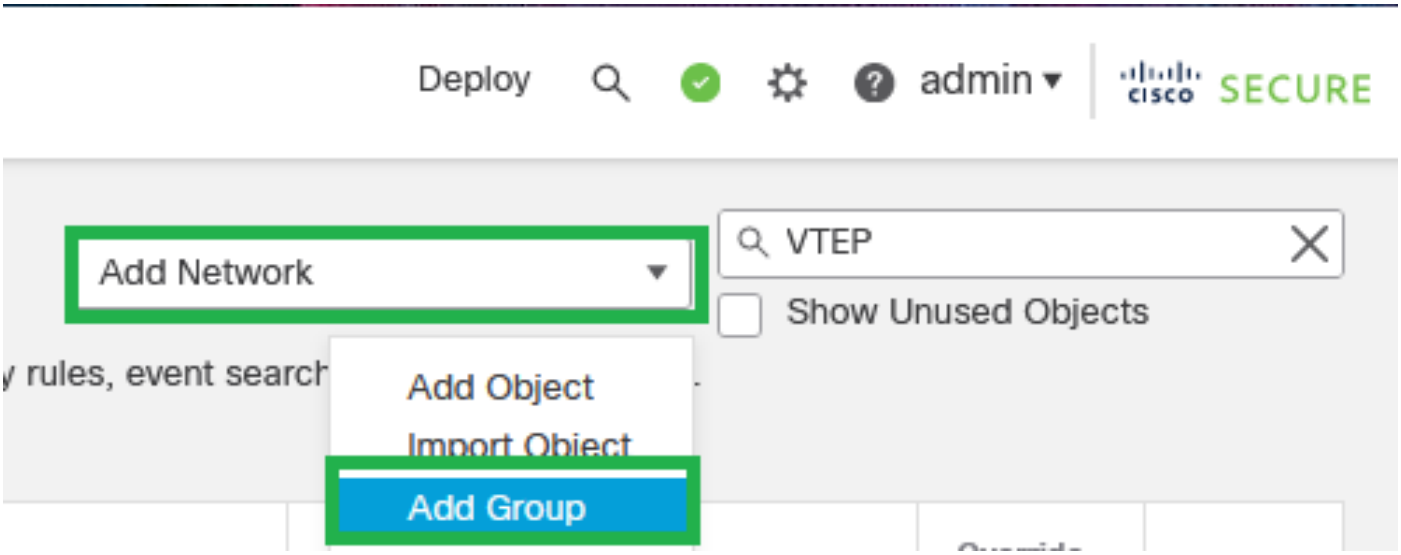
Objetos - Gerenciamento de Objetos

Etapa 2: Clique em Rede no menu esquerdo.


AAA Server
Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig

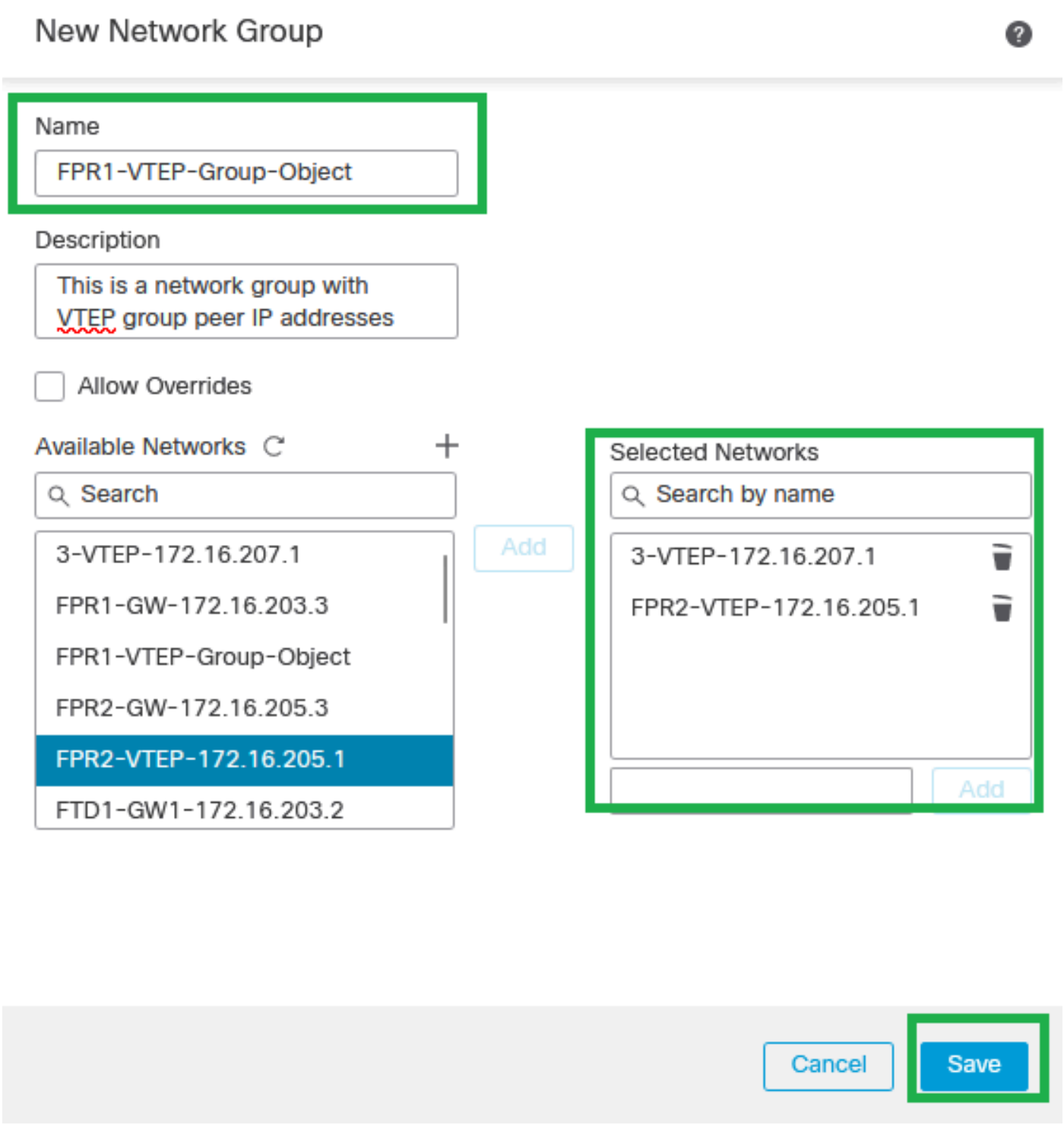
: Configure mais objetos de rede de host para cada endereço IP de peer VTEP que você tiver. Há dois objetos neste guia de configuração.

Etapa 5: Crie o Grupo de Objetos, clique em Adicionar Rede > Adicionar Grupo.



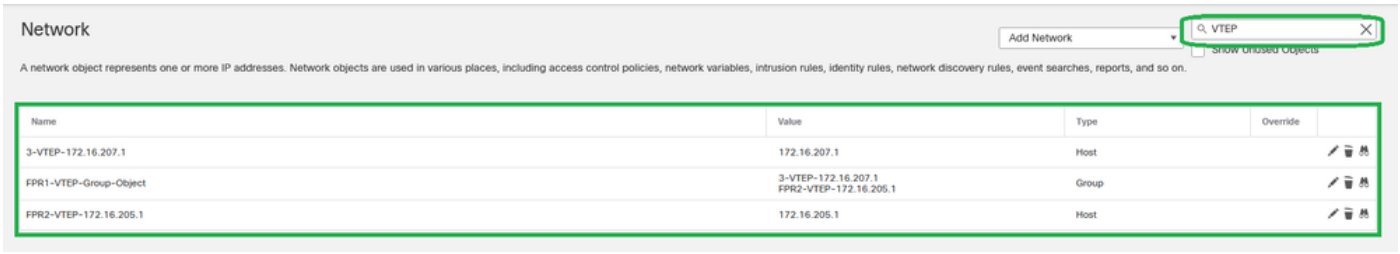
Adicionar rede - Adicionar grupo

Etapa 6: Crie o grupo de objetos de rede com todos os endereços IP do peer VTEP. Configure um nome de grupo de rede e selecione os grupos de objetos de rede necessários e clique em Salvar.



Criar Grupo de Objetos de Rede

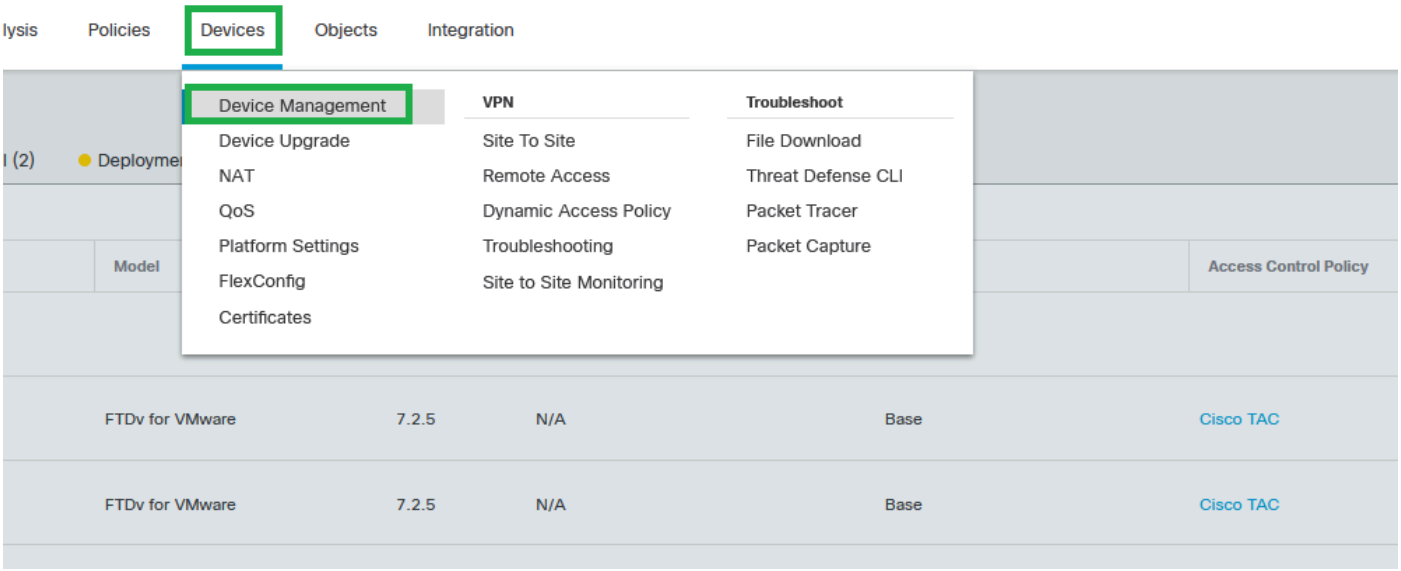
Etapa 7: Valide o objeto de rede e o grupo de objetos de rede a partir do filtro Objeto de rede.



Validar o grupo de objetos VTEP

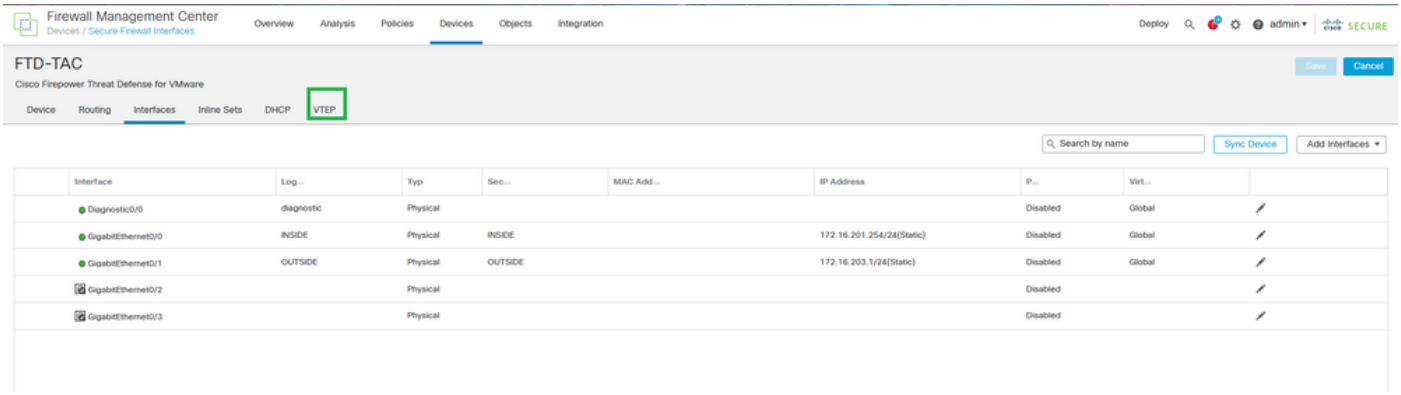
Configurar a interface de origem do VTEP

Etapa 1: navegue até Devices > Device Management e edite a defesa contra ameaças.



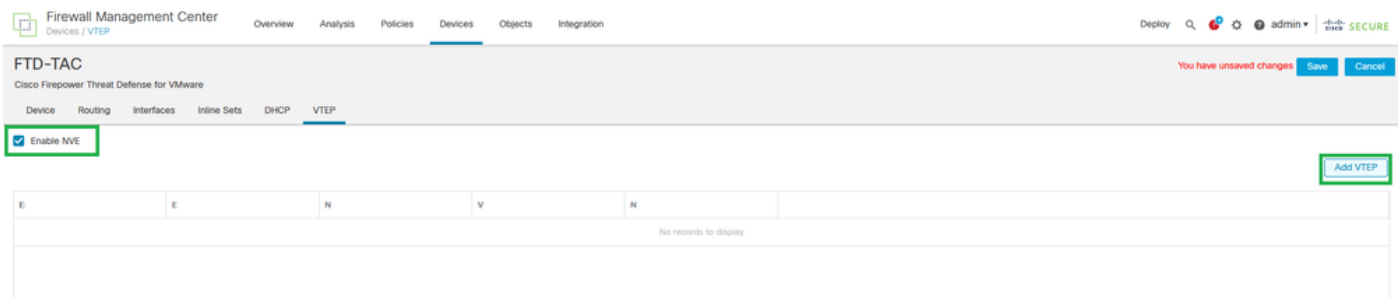
Dispositivos - Gerenciamento de dispositivos

Etapa 2: vá até a seção VTEP.



seção VTEP

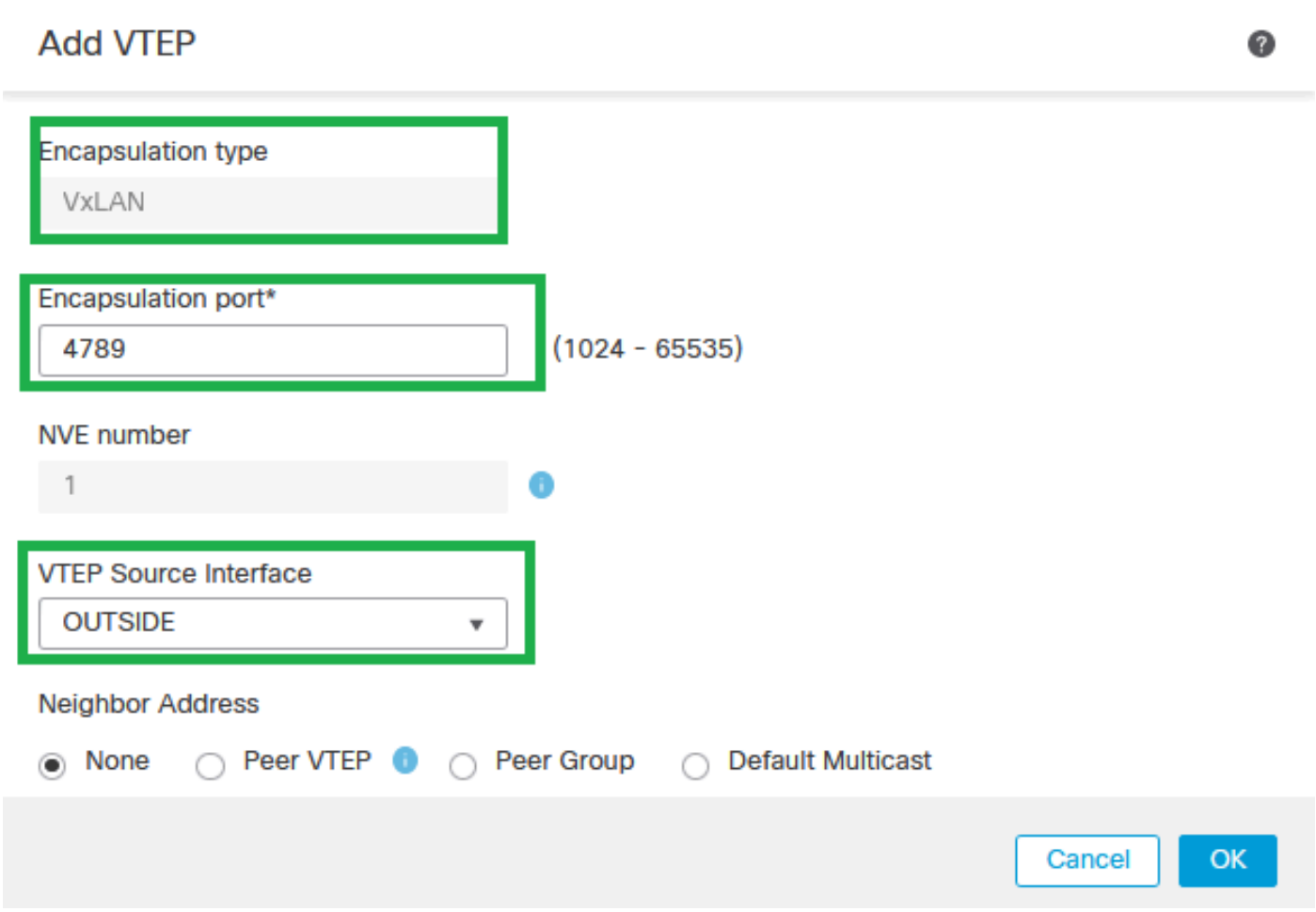
Etapa 3: Marque a caixa de seleção Enable VNE e clique em Add VTEP.



Habilitar NVE e Adicionar VTEP

Etapa 4: selecione VxLAN como o tipo de encapsulamento, insira o valor Encapsulation Port e escolha a interface usada para a origem VTEP nesta defesa contra ameaças (Interface externa

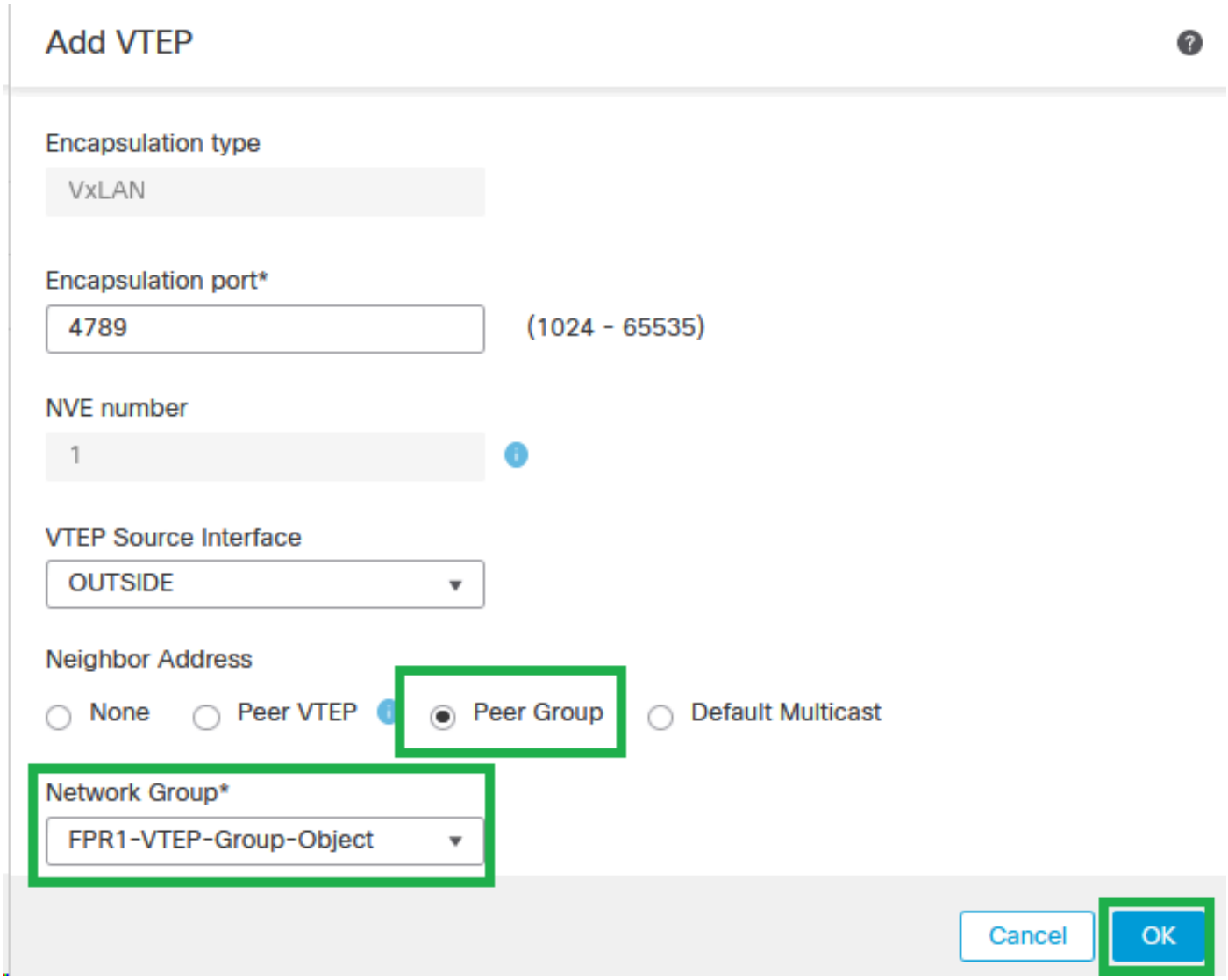
para este guia de configuração)



Adicionar VTEP

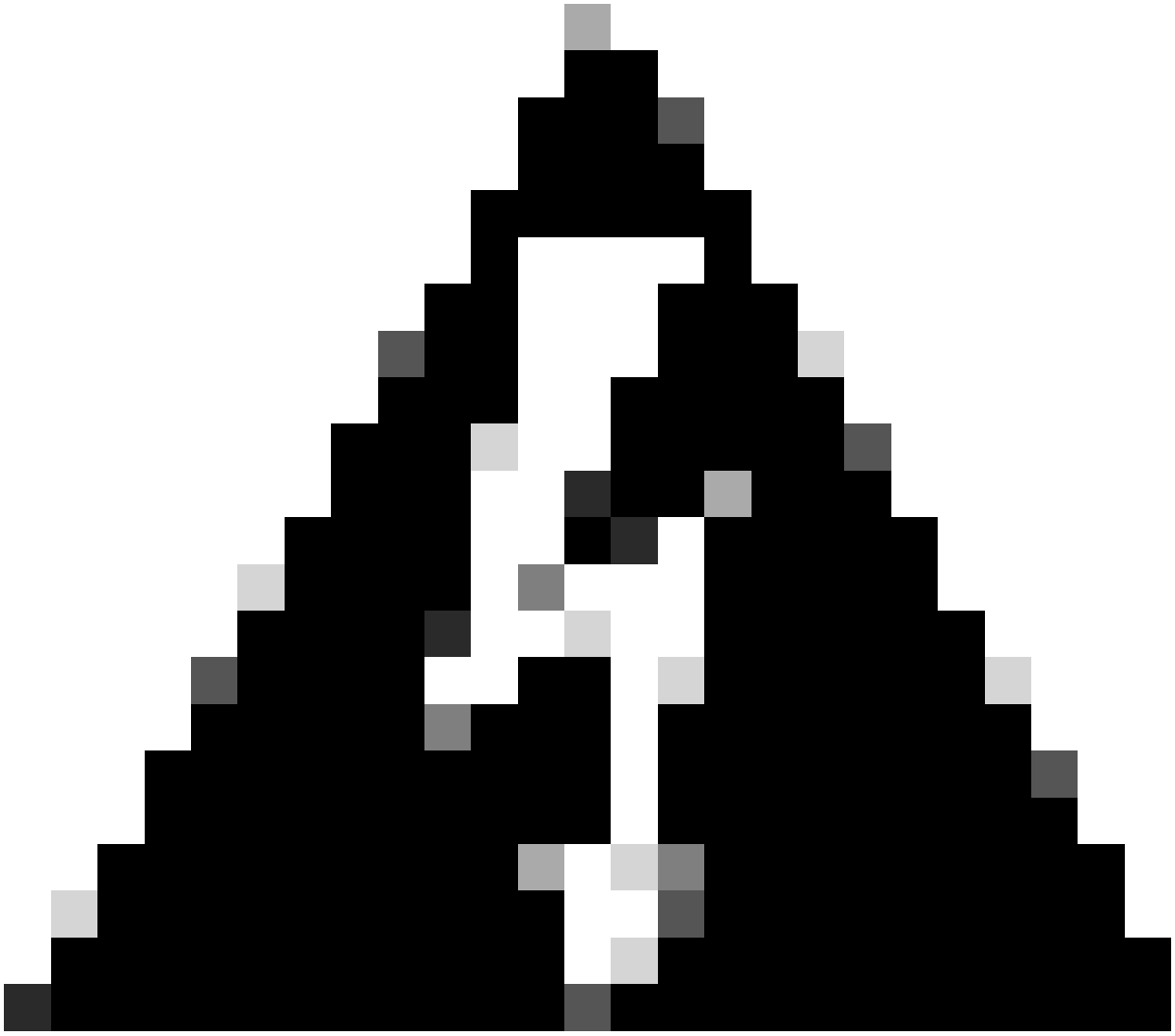
Observação: o encapsulamento VxLAN é o padrão. Para AWS, você pode escolher entre VxLAN e Geneve. O valor padrão é 4789, Qualquer porta de encapsulamento pode ser escolhida entre 1024 - 65535 intervalo de acordo com o projeto.

Etapa 5: Selecione Grupo de Pares e escolha o Grupo de Objetos de Rede criado na seção de configuração anterior. Em seguida, clique em OK.



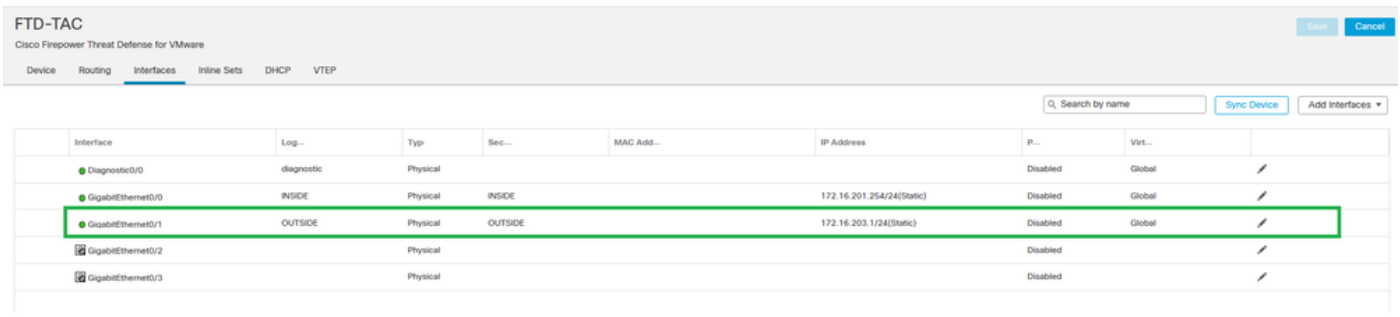
Grupo de Pares - Grupo de Objetos de Rede

Etapa 6: salve as alterações.



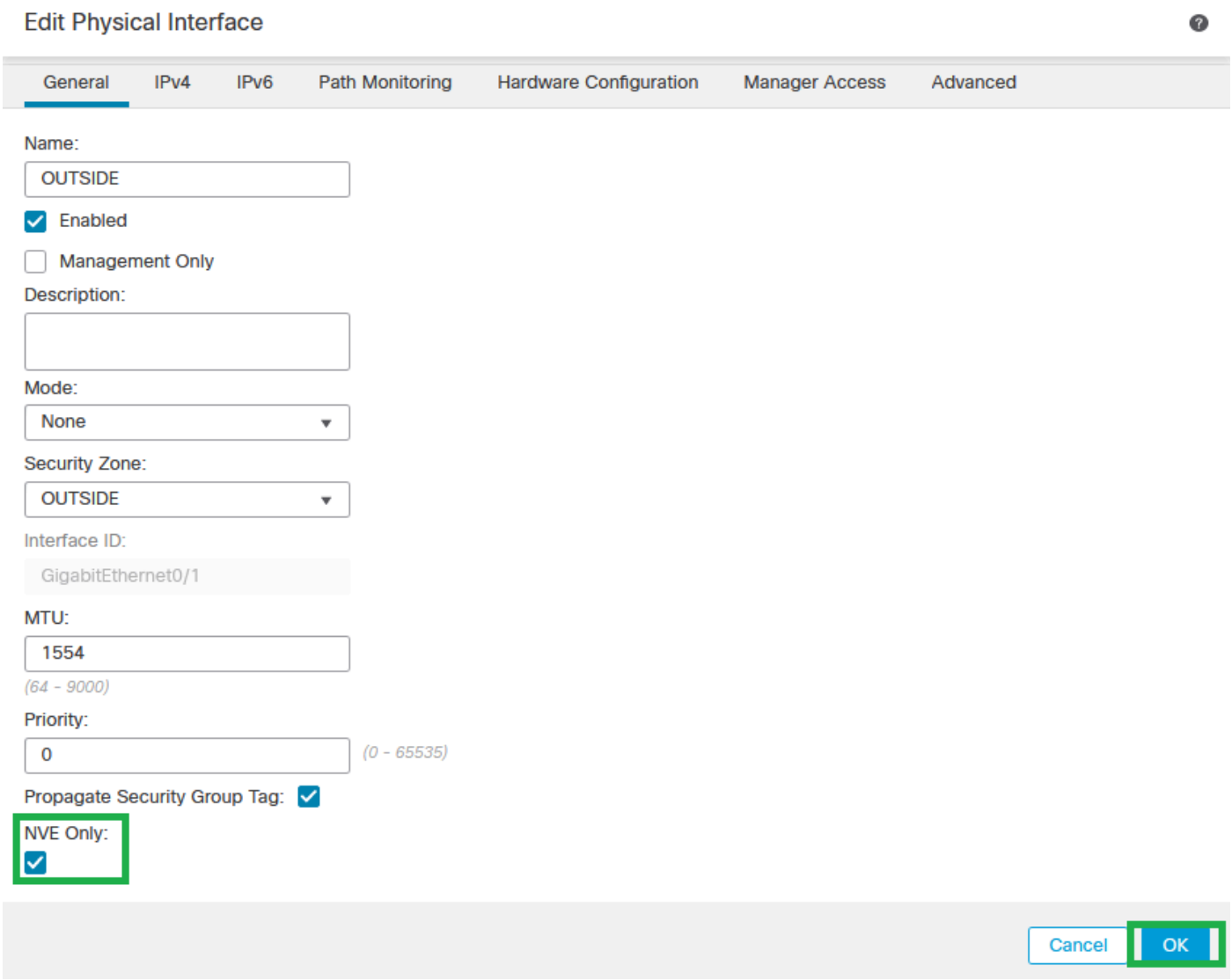
Aviso: Depois que as alterações forem salvas, uma mensagem de alteração de quadro jumbo será exibida, o MTU será alterado na interface atribuída como VTEP para 1554, certifique-se de usar o mesmo MTU na rede subjacente.

Etapa 7:Clique em Interfaces e edite a interface usada para a interface de origem VTEP. (Interface externa neste guia de configuração)

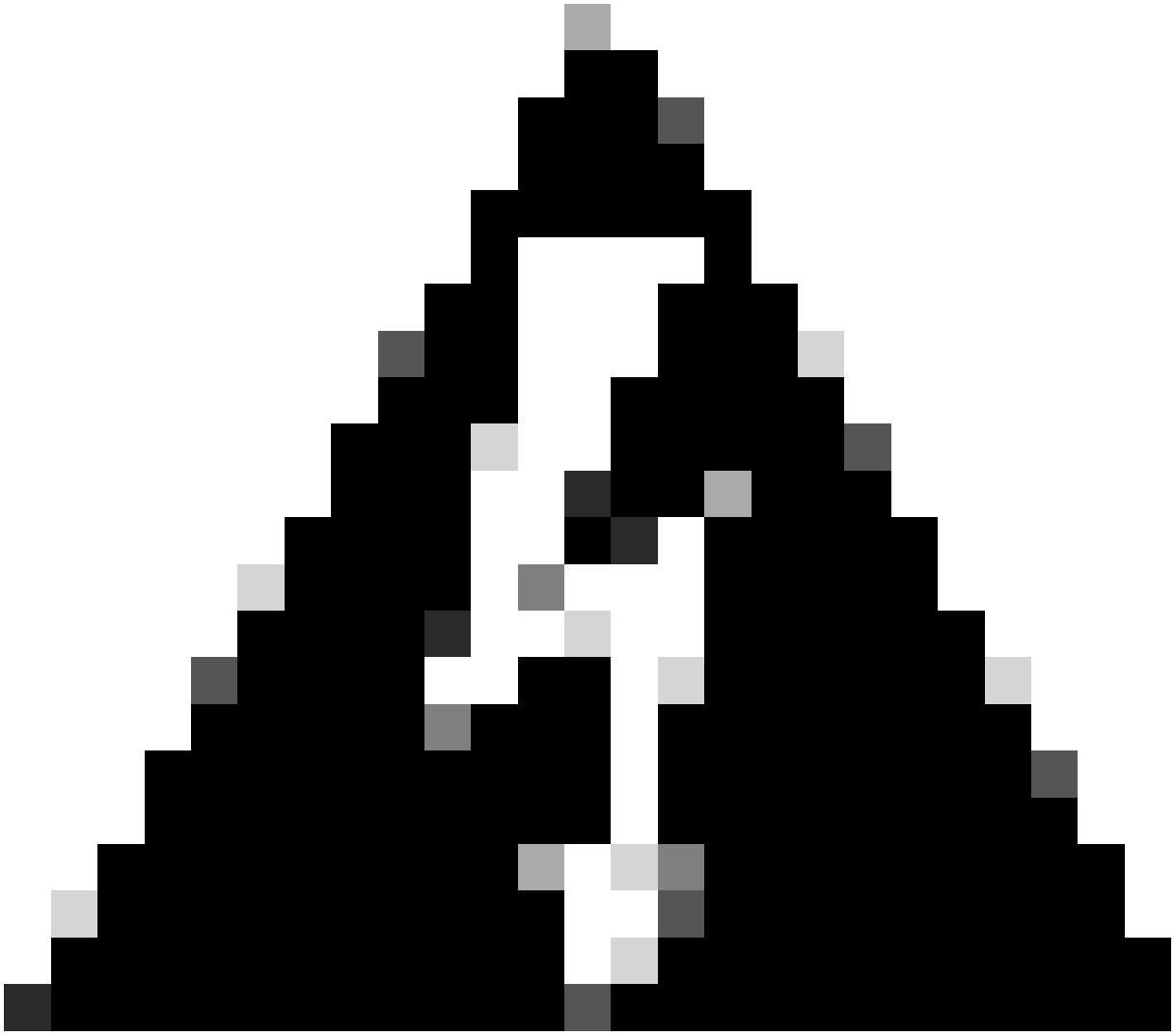


Externo como interface de origem VTEP

Etapa 8 (Opcional):Na página Geral, marque a caixa de seleção Somente NVE e clique em OK.



Configuração Somente NVE

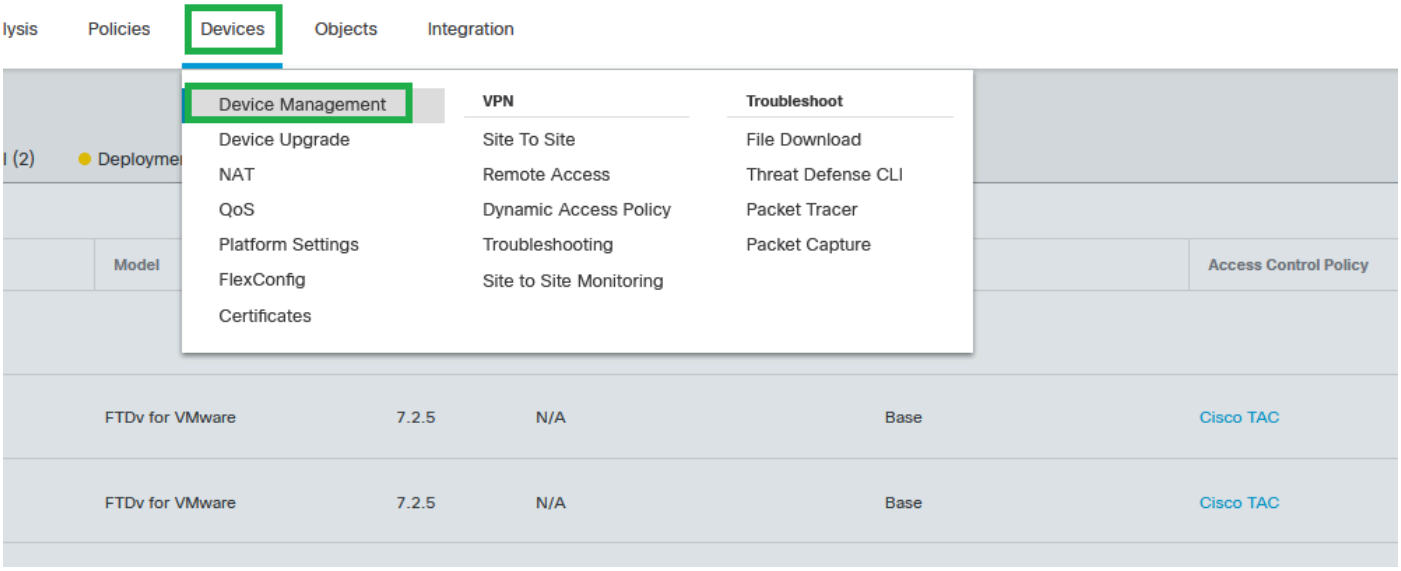


Aviso: esta configuração é opcional para o modo roteado, em que esta configuração restringe o tráfego para VXLAN e o tráfego de gerenciamento comum somente nesta interface. Essa configuração é automaticamente habilitada para o modo de firewall transparente.

Etapa 9: salve as alterações.

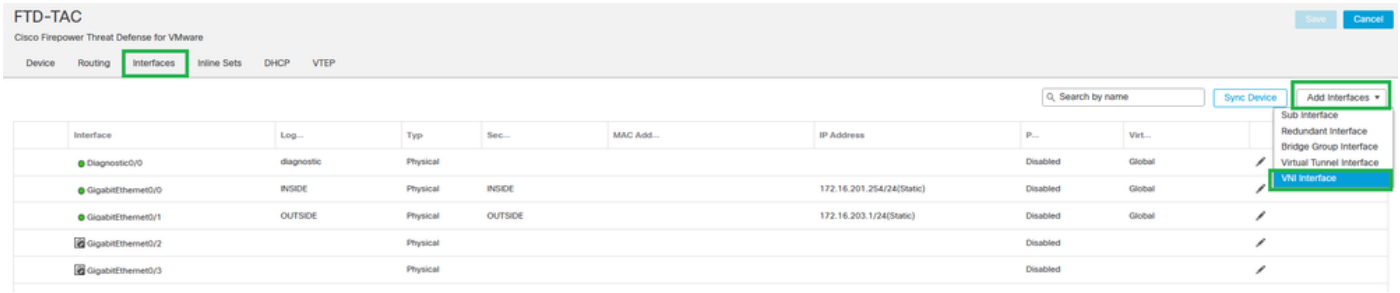
Configurar a interface VTEP VNI

Etapa 1: Navegue em Devices > Device Management e edite a defesa contra ameaças.



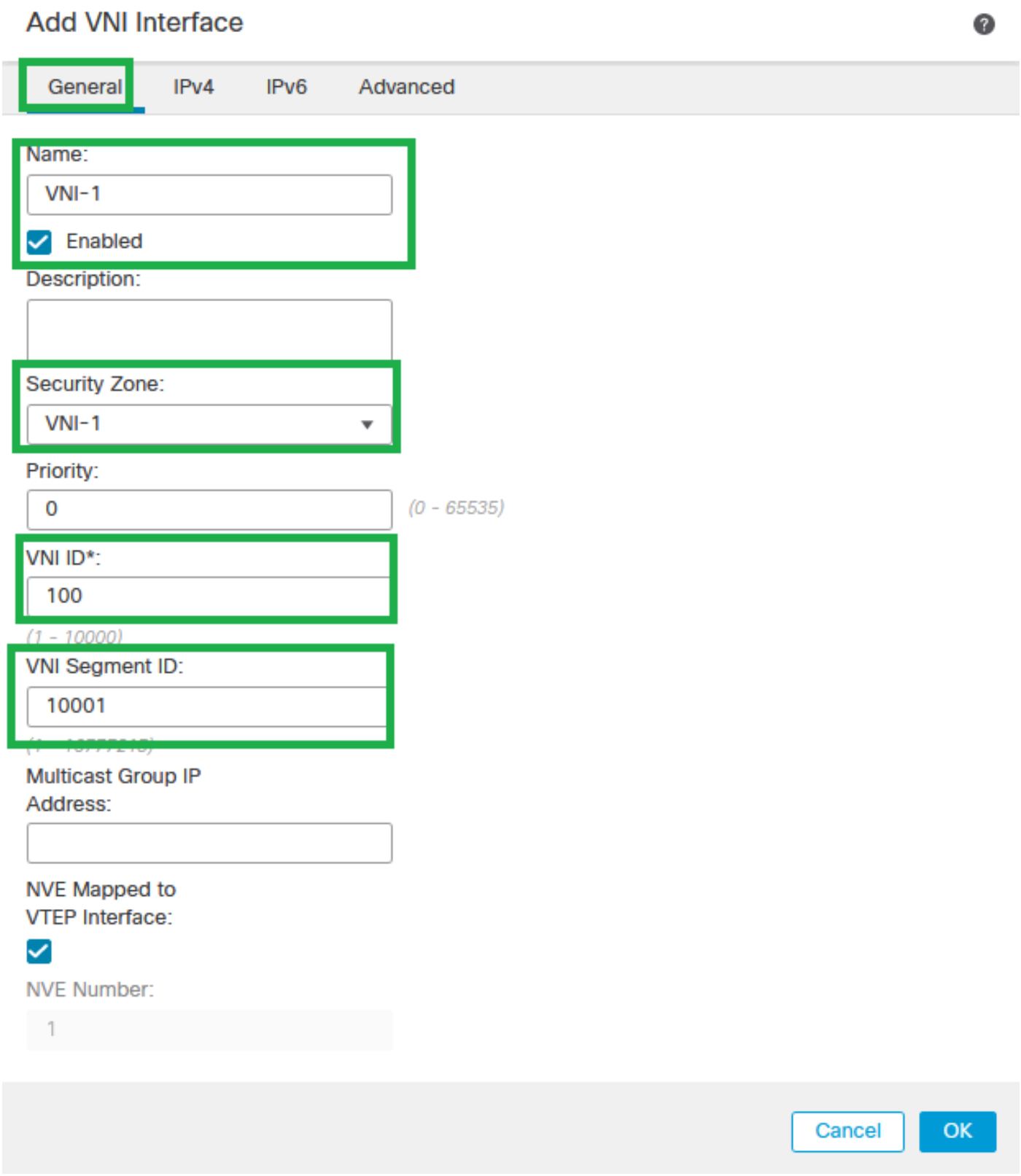
Dispositivos - Gerenciamento de dispositivos

Etapa 2: Na seção Interfaces, clique em Add Interfaces > VNI Interfaces.

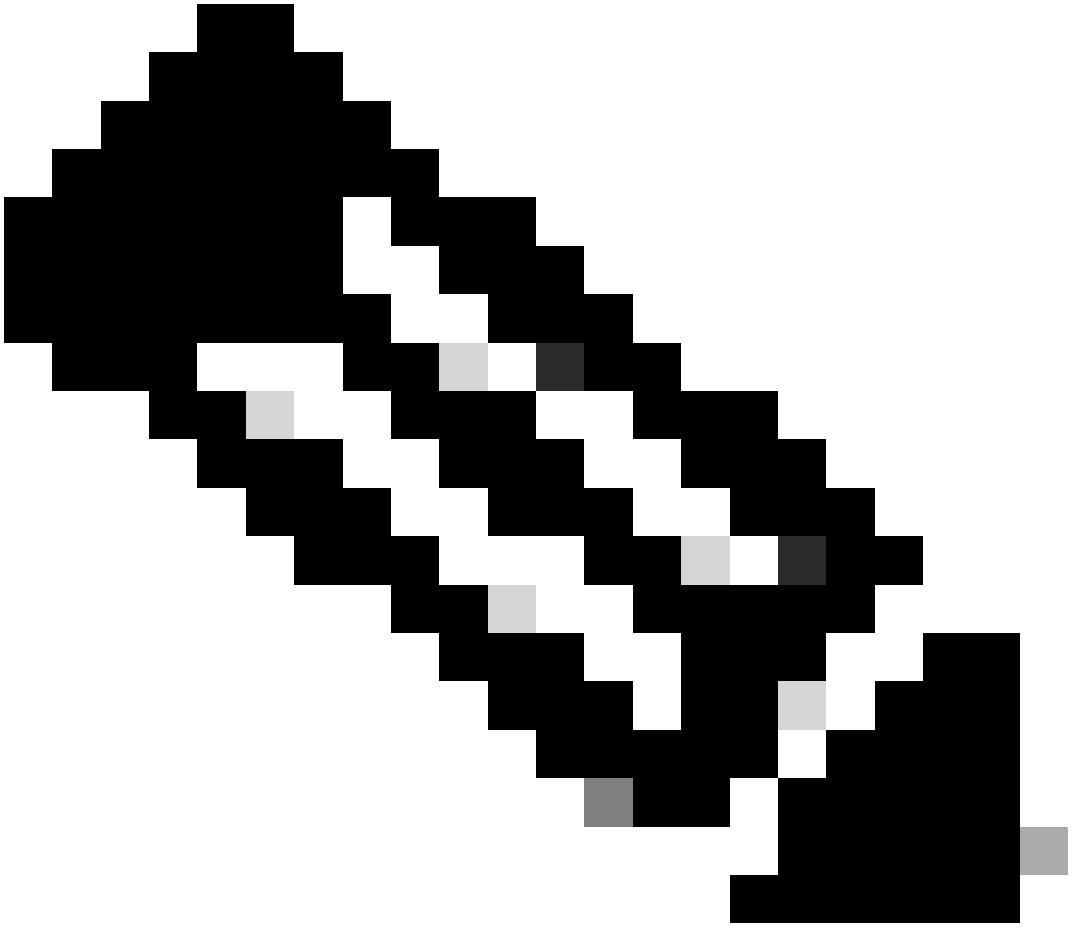


Interfaces - Adicionar interfaces - Interfaces VNI

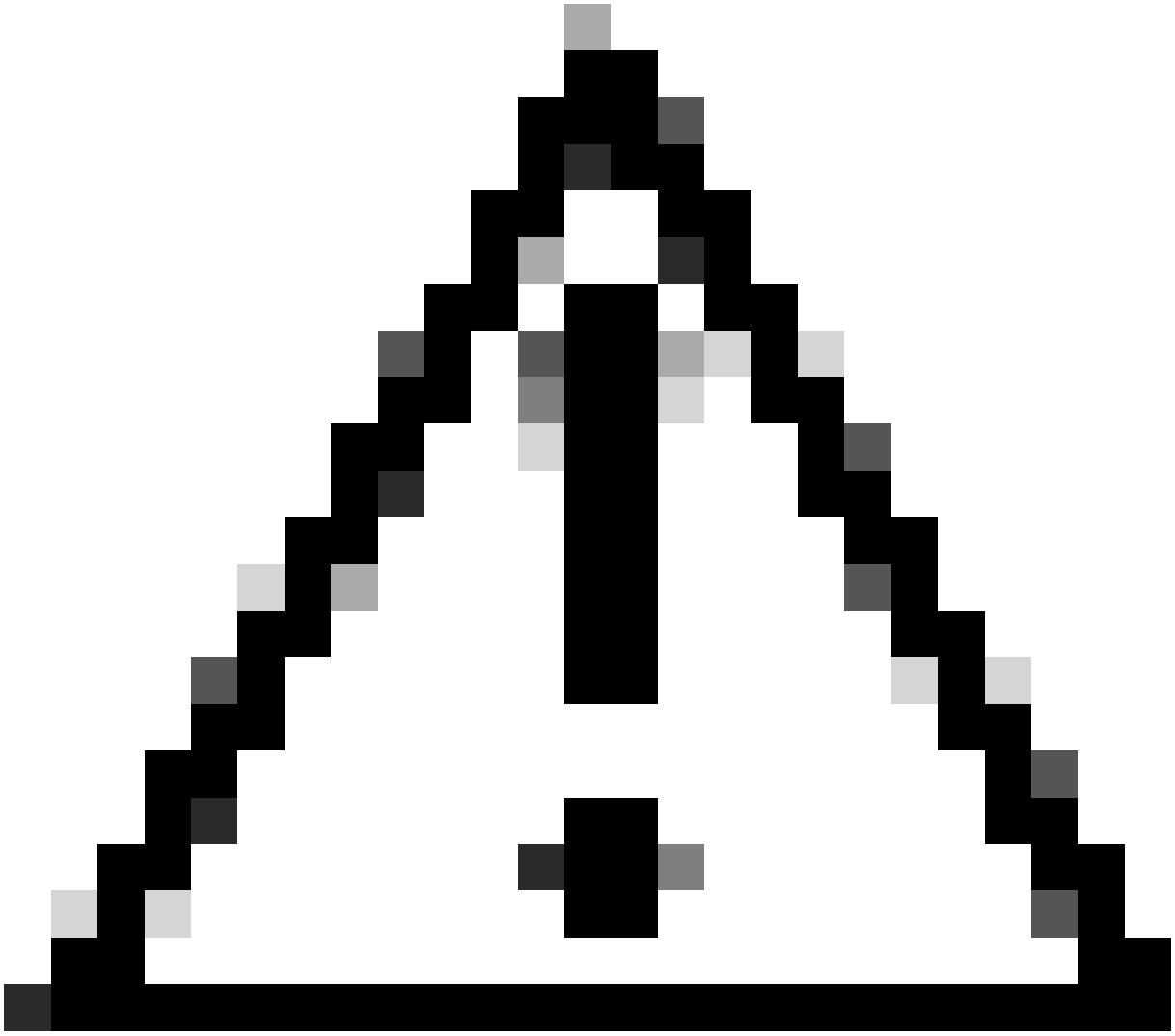
Etapa 3: Na seção Geral, configure a interface do VNI com nome, descrição, Zona de segurança, ID do VNI e ID do segmento do VNI.



Adicionar interface VNI

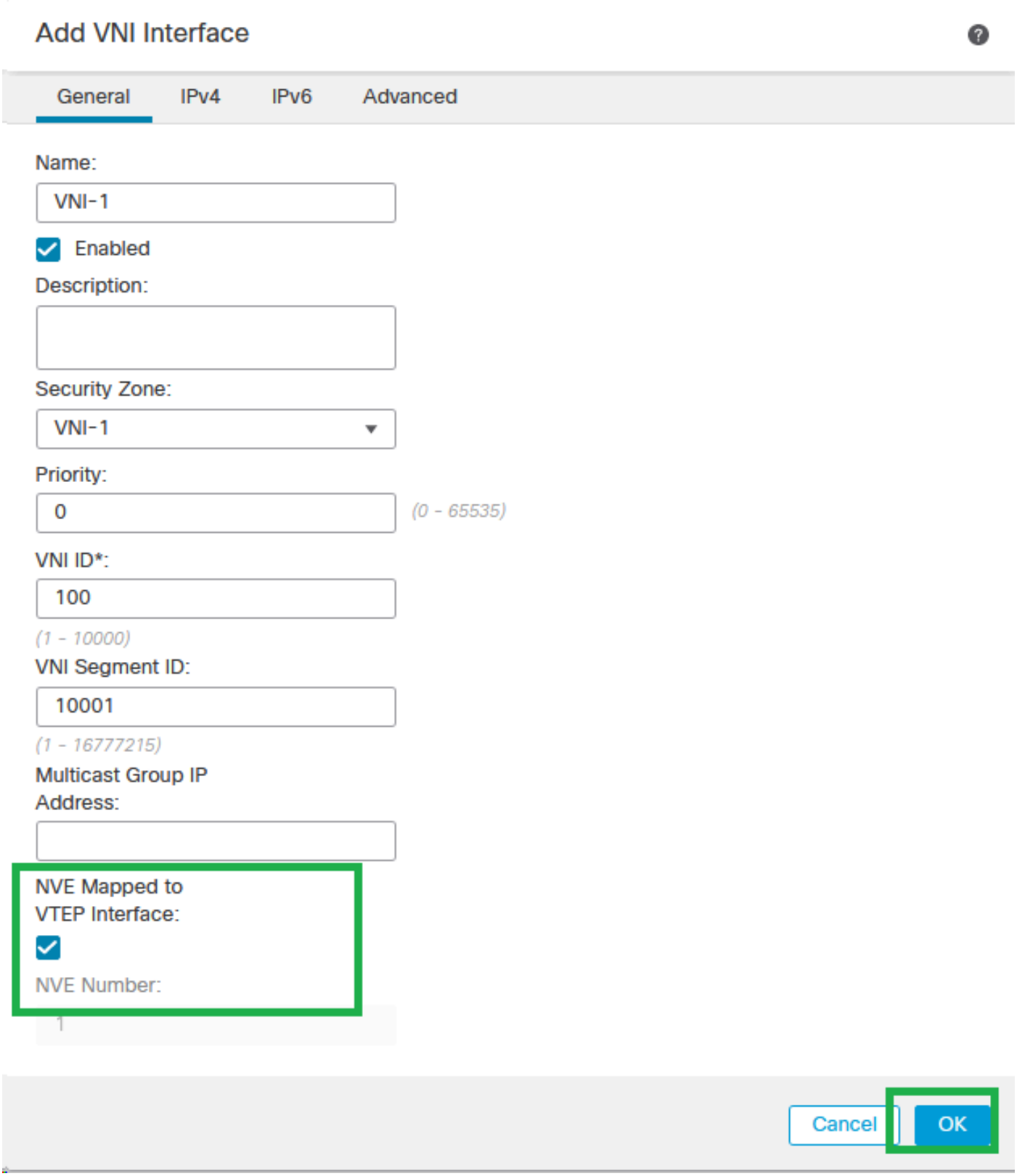


Observação: o ID do VNI é configurado entre 1 e 10000, e o ID do segmento VNI é configurado entre 1 e 16777215 (o ID do segmento é usado para marcação VXLAN).



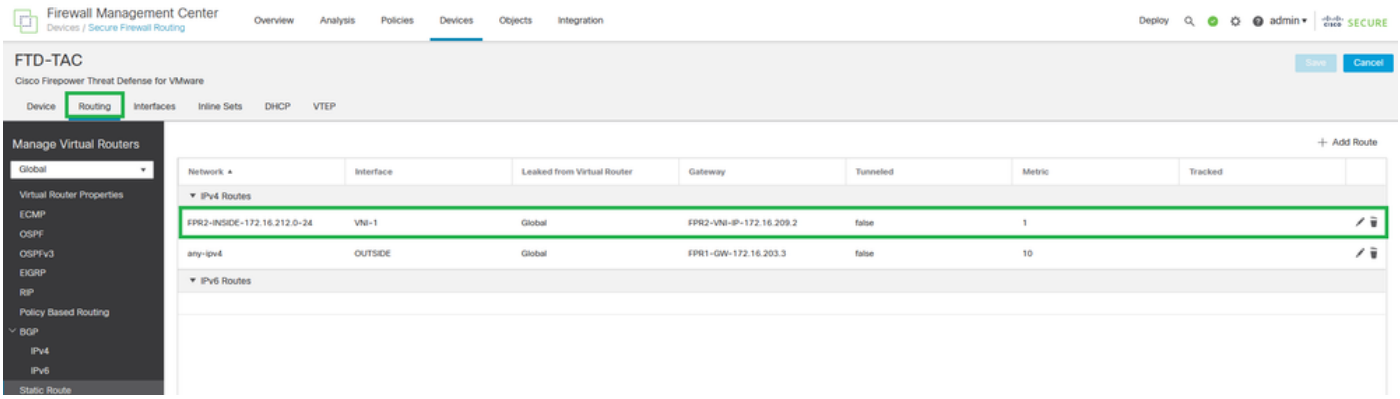
Cuidado: se o grupo multicast não estiver configurado na interface VNI, o grupo padrão da configuração da interface de origem VTEP será usado, se estiver disponível. Se você definir manualmente um IP de peer VTEP para a interface de origem VTEP, não poderá especificar um grupo multicast para a interface VNI.

Etapa 3: Marque a caixa de seleção NVE Mapped to VTEP Interface e clique em OK.

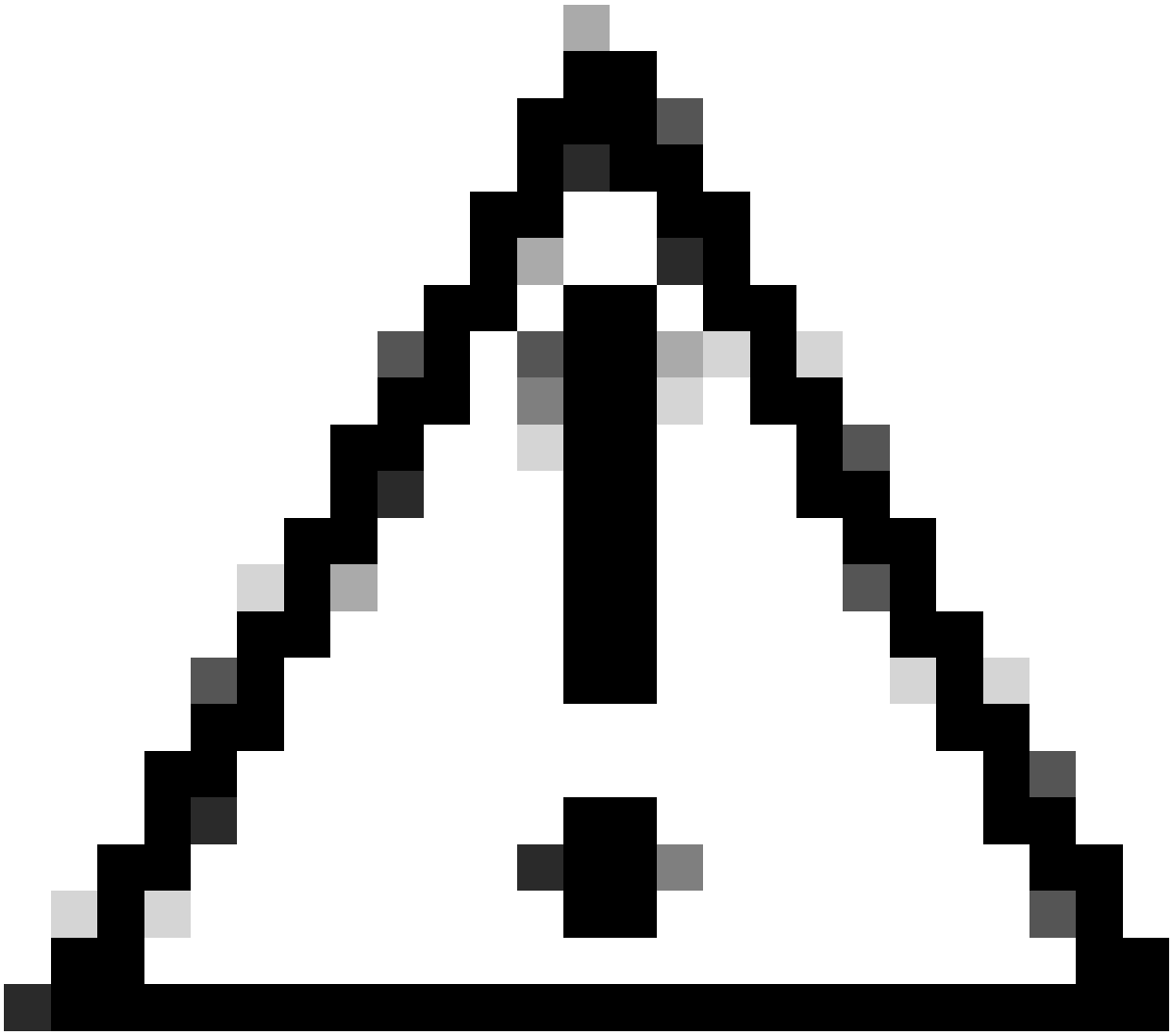


NVE mapeado para interface VTEP

Etapa 4: Configure uma rota estática para anunciar as redes de destino para VXLAN à interface do peer VNI. Navegue até Roteamento > Rota estática.

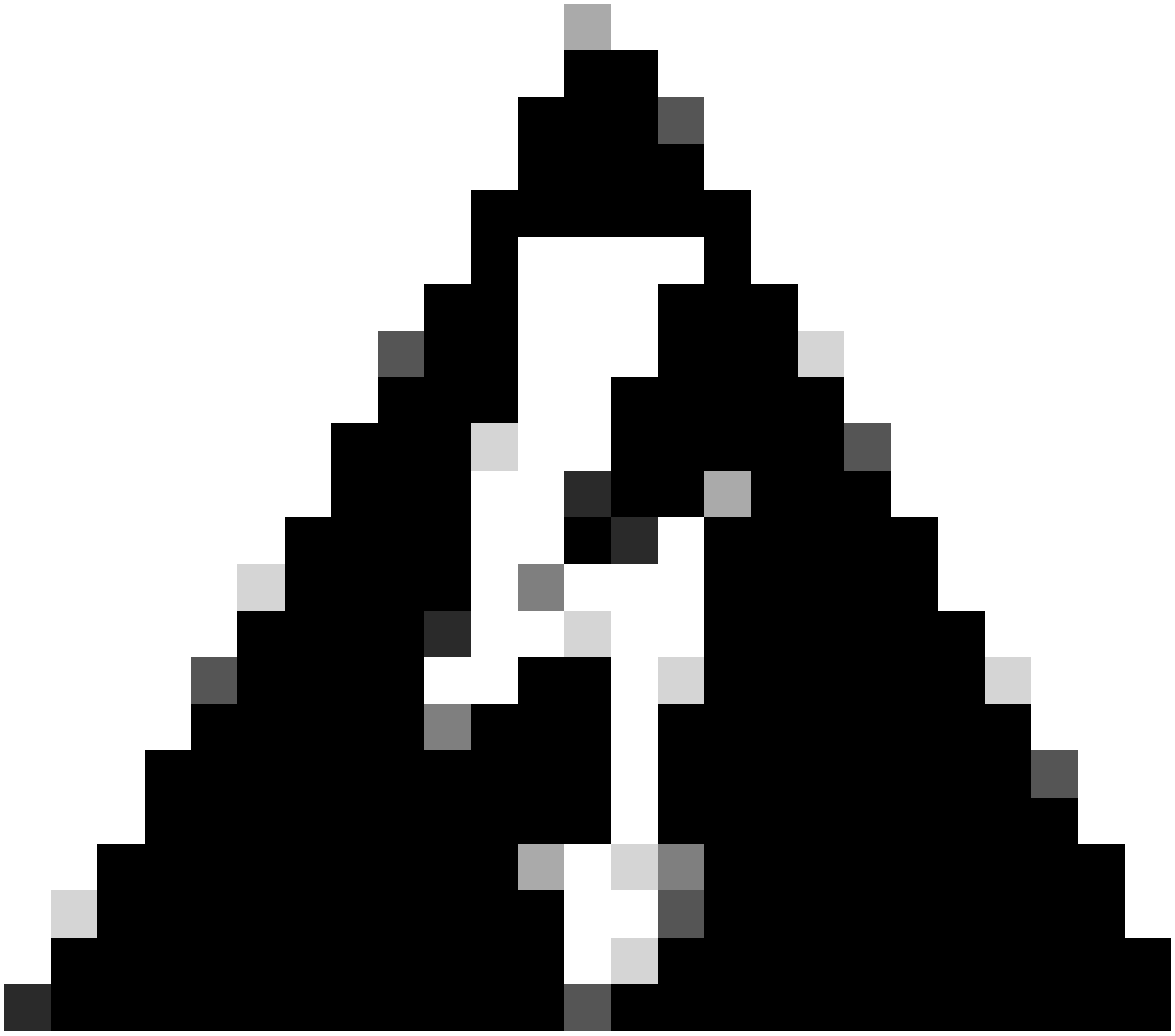


Configuração de rota estática



Cuidado: as redes de destino para VXLAN devem ser enviadas através da interface VNI de mesmo nível. Todas as interfaces VNI devem estar no mesmo domínio de broadcast (segmento lógico).

Etapa 5: salvar e implantar as alterações.



Aviso: os avisos de validação podem ser vistos antes da implantação, certifique-se de que os endereços IP do peer VTEP estejam acessíveis na interface de origem VTEP física.

Verificar

Verifique a configuração do NVE.

```
firepower# show running-config nve
nve 1
encapsulation vxlan
source-interface OUTSIDE
peer-group FPR1-VTEP-Group-Object
```

```
firepower# show nve 1
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
IP address 172.16.203.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
1309 packets input, 128170 bytes
2009 packets output, 230006 bytes
142 packets dropped
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Configured static peer group VTEPs:
IP address 172.16.205.1 MAC address 0050.56b3.c30a (learned)
IP address 172.16.207.1 MAC address 0050.56b3.c30a (learned)
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 172.16.205.1
IP address 172.16.207.1
Number of VNIs attached to nve 1: 1
VNIs attached:
vni 100: proxy off, segment-id 10001, mcast-group none
NVE proxy single-arm channel is off.
```

```
firepower# show nve 1 summary
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Number of discovered peer VTEPs: 2
Number of VNIs attached to nve 1: 1
NVE proxy single-arm channel is off.
```

Verifique a configuração da interface VNI.

```
firepower# show run interface
interface vni100
segment-id 10001
nameif VNI-1
security-level 0
ip address 172.16.209.1 255.255.255.0
vtep-nve 1
```

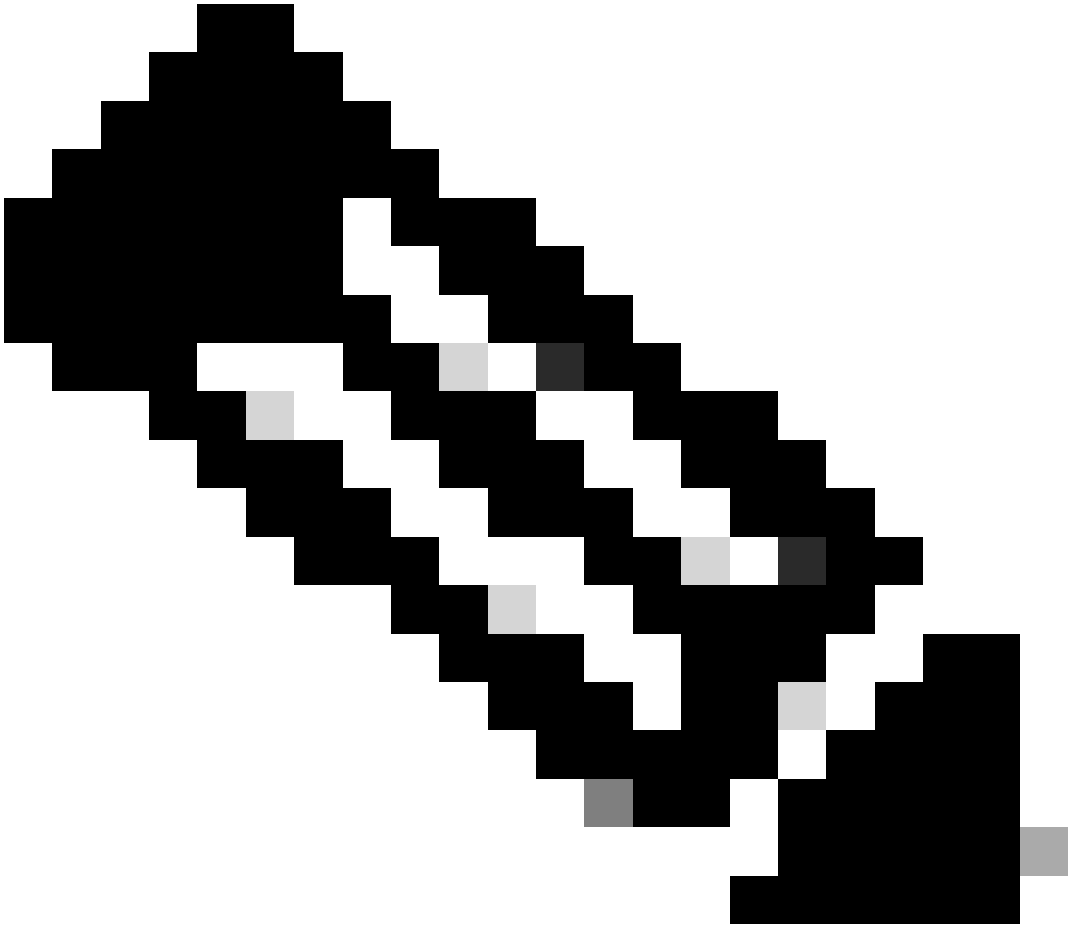
Verifique a configuração de MTU na interface VTEP.

```
firepower# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up
Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0050.56b3.26b8, MTU 1554
IP address 172.16.203.1, subnet mask 255.255.255.0
```

```
---
[Output omitted]
---
```

Verifique a configuração da rota estática para as redes de destino.

```
firepower# show run route
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.203.3 10
route VNI-1 172.16.212.0 255.255.255.0 172.16.209.2 1
route VNI-1 172.16.215.0 255.255.255.0 172.16.209.3 1
```



Observação: verifique se as interfaces VNI em todos os pares estão configuradas no mesmo domínio de broadcast.

Troubleshooting

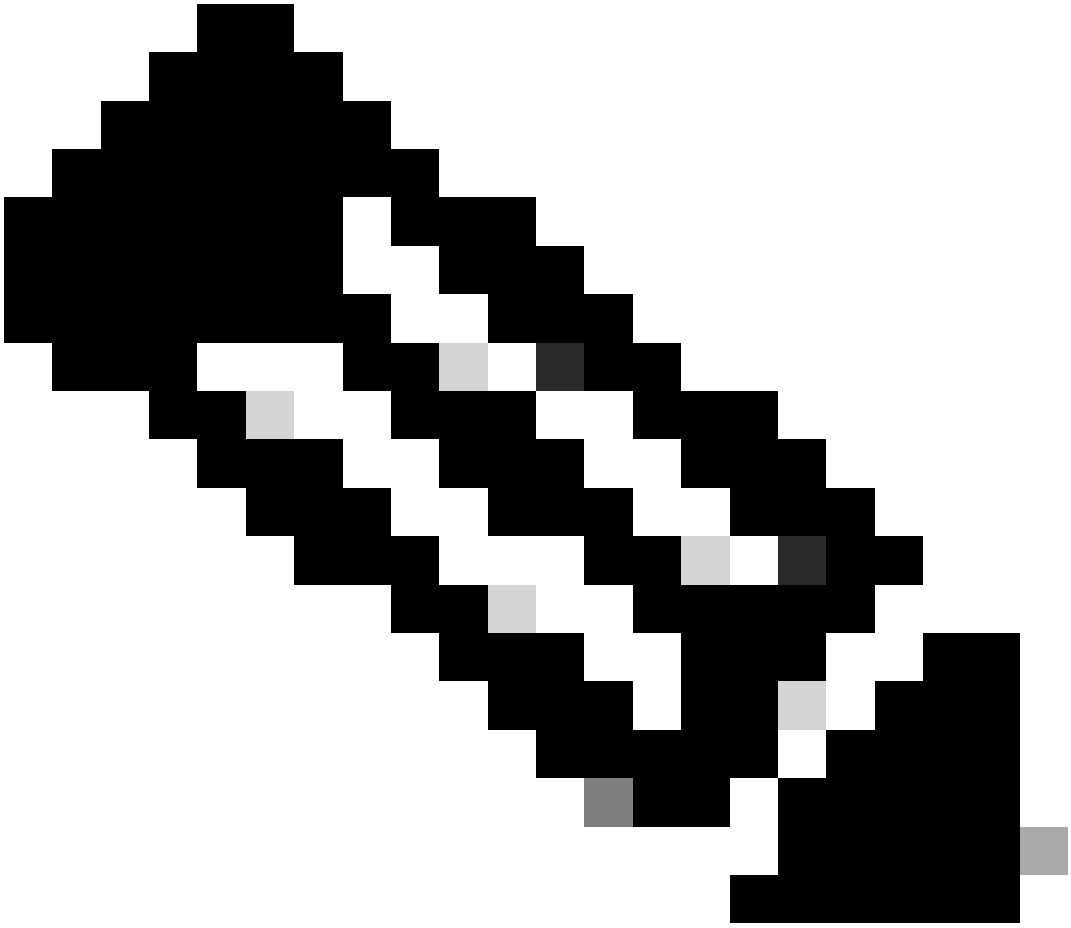
Verifique a conectividade com os pares VTEP.

Par 1:

```
firepower# ping 172.16.205.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.205.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Par 2:

```
firepower# ping 172.16.207.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.207.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```



Observação: um problema de conectividade de peer VTEP pode gerar falhas de implantação no FMC seguro. Certifique-se de manter a conectividade com todas as suas configurações de pares VTEP.

Verifique a conectividade com os pares VNI.

.

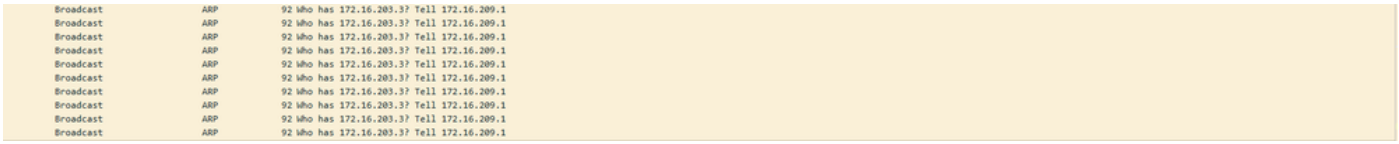
Par 1:

```
firepower# ping 172.16.209.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Par 2:

```
firepower# ping 172.16.209.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Às vezes, uma rota estática errada configurada pode gerar saídas ARP incompletas. Configure uma captura na interface VTEP para pacotes VXLAN e faça o download em um formato pcap, qualquer ferramenta de análise de pacotes ajuda a confirmar se há algum problema com as rotas. Certifique-se de usar o endereço IP do peer do VNI como um gateway.



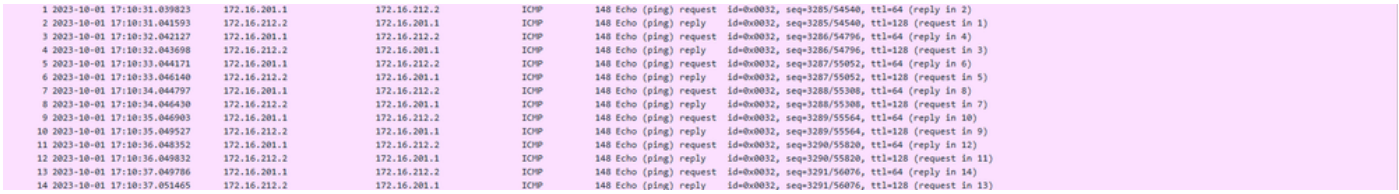
Problema de Roteamento

Configure as capturas de queda do ASP no FTD seguro em caso de qualquer queda do Firewall, verifique o contador de queda do ASP com o comando show asp drop. Entre em contato com o TAC da Cisco para análise.

Certifique-se de configurar as regras de política de controle de acesso para permitir o tráfego VXLAN UDP na interface VNI/VTEP.

Às vezes, os pacotes VXLAN podem ser fragmentados, certifique-se de alterar o MTU para quadros jumbo na rede subjacente para evitar a fragmentação.

Configure a captura na interface Ingress/VTEP e baixe as capturas no formato .pcap para análise. Os pacotes devem incluir o cabeçalho VXLAN na interface VTEP,



Ping capturado com cabeçalho VXLAN

Informações Relacionadas

- Configurar interfaces VXLAN
- Casos de uso de VXLAN
- Processamento de pacotes VXLAN
- Configurar a interface de origem do VTEP
- Configurar a interface VNI
- Suporte técnico e downloads da 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.