Configuración de interfaces VXLAN en FTD seguro con FMC seguro

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Diagrama de la red

Configurar

- Configuración del grupo de pares VTEP
- Configuración de la interfaz de origen de VTEP
- Configuración de la interfaz VTEP VNI

Verificación

Troubleshoot

Información Relacionada

Introducción

Este documento describe cómo configurar las interfaces VXLAN en Secure Firewall Threat Defence (FTD) con Secure Firewall Management Center (FMC)

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Conceptos básicos de VLAN/VXLAN.
- Conocimiento básico de la red.
- Experiencia básica de Cisco Secure Management Center.
- Experiencia básica de Cisco Secure Firewall Threat Defence.

Componentes Utilizados

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

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware con versión 7.2.4.
- Appliance virtual Cisco Secure Firewall Threat Defence (FTDv) VMware con versión 7.2.4.

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

La VLAN extensible virtual (VXLAN) proporciona servicios de red Ethernet de capa 2 como lo hace la VLAN tradicional. Debido a la alta demanda de segmentos de VLAN en entornos virtuales, VXLAN proporciona una mayor extensibilidad y flexibilidad, y también define un esquema de encapsulación MAC en UDP en el que la trama de capa 2 original tiene un encabezado VXLAN agregado y luego se coloca en un paquete UDP-IP. Con esta encapsulación MAC en UDP, VXLAN establece túneles para la red de capa 2 a través de la red de capa 3. VXLAN ofrece las siguientes ventajas:

- Flexibilidad de VLAN en segmentos de varios arrendatarios:
- Mayor escalabilidad para hacer frente a más segmentos de capa 2 (L2).
- Mejor utilización de la red.

Cisco Secure Firewall Threat Defence (FTD) admite dos tipos de encapsulación VXLAN.

- VXLAN (se utiliza para todos los modelos de protección frente a amenazas de firewall)
- Geneve (se utiliza para el appliance virtual Secure Firewall Threat Defence)

La encapsulación Geneve es necesaria para el enrutamiento transparente de paquetes entre el equilibrador de carga de gateway de Amazon Web Services (AWS) y los dispositivos, así como para el envío de información adicional.

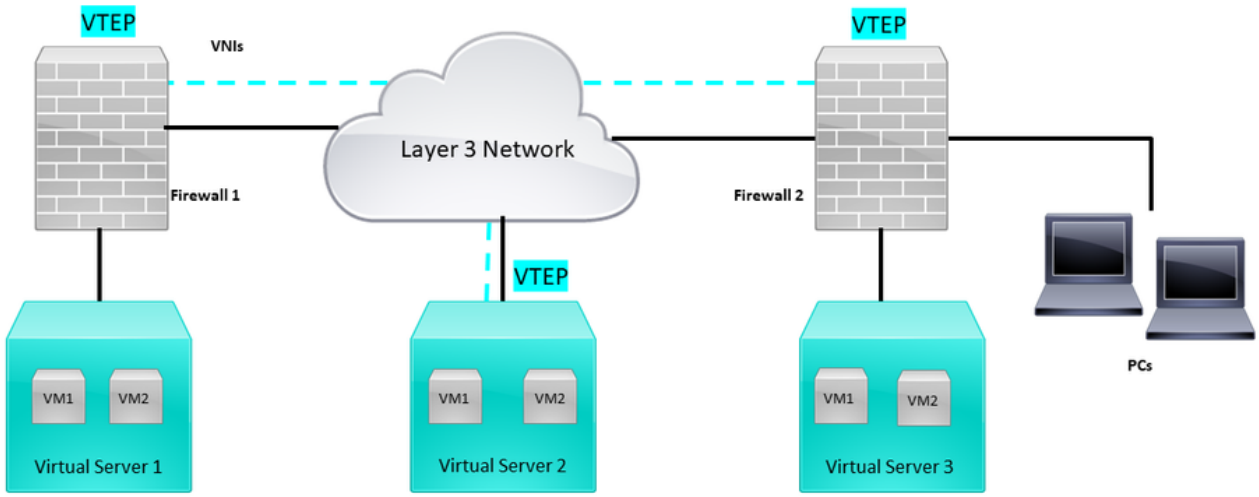
VXLAN utiliza el terminal de túnel VXLAN (VTEP) para asignar los dispositivos finales de los arrendatarios a segmentos VXLAN y para realizar la encapsulación y desencapsulación de VXLAN. Cada VTEP tiene dos tipos de interfaz: una o más interfaces virtuales denominadas interfaces VNI (VXLAN Network Identifier) en las que se puede aplicar la política de seguridad, y una interfaz normal denominada interfaz de origen VTEP en la que las interfaces VNI se tunelizan entre VTEP. La interfaz de origen VTEP está conectada a la red IP de transporte para la comunicación VTEP-a-VTEP, las interfaces VNI son similares a las interfaces VLAN: son interfaces virtuales que mantienen el tráfico de red separado en una interfaz física determinada mediante el uso de etiquetas. La política de seguridad se aplica a cada interfaz VNI. Se puede agregar una interfaz VTEP y todas las interfaces VNI están asociadas con la misma interfaz VTEP. Existe una excepción para el agrupamiento virtual de Threat Defence en AWS.

La defensa contra amenazas encapsula y desencapsula de tres formas:

- Se puede configurar de forma estática una única dirección IP VTEP del mismo nivel en la defensa contra amenazas.
- Se puede configurar estáticamente un grupo de direcciones IP de VTEP del mismo nivel en la defensa contra amenazas.
- Se puede configurar un grupo multicast en cada interfaz VNI.

Este documento se centra en las interfaces VXLAN para la encapsulación VXLAN con un grupo de direcciones IP VTEP de 2 pares configuradas estáticamente. Si necesita configurar las interfaces de Geneve, verifique la documentación oficial para las interfaces de Geneve en AWS o configure VTEP con un único peer o grupo multicast, verifique la interfaz VTEP con una guía de configuración de un peer o grupo multicast.

Diagrama de la red



Topología de red

La sección de configuración supone que la red subyacente ya está configurada en defensa contra amenazas a través de Secure Firewall Management Center. Este documento se centra en la configuración de red superpuesta.

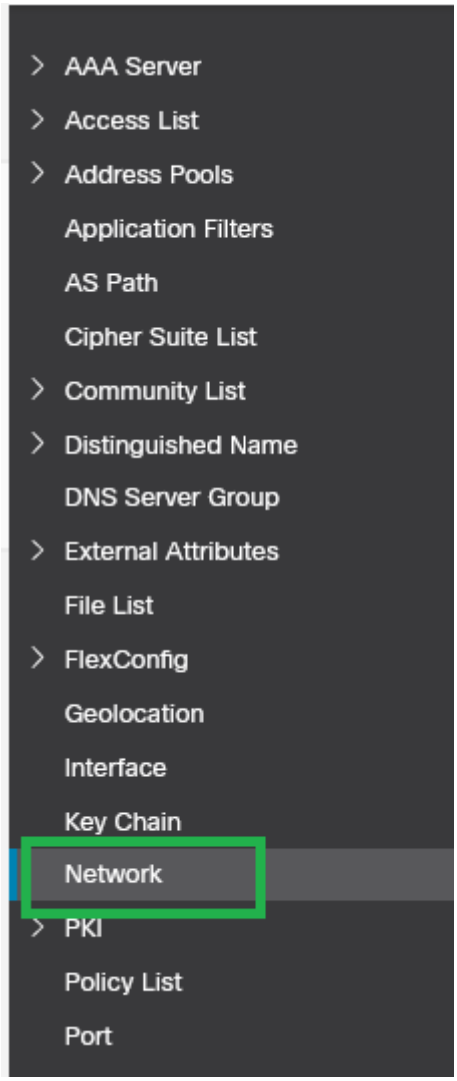
Configurar

Configuración del grupo de pares VTEP

Paso 1: Navegue hasta Objetos > Administración de objetos.

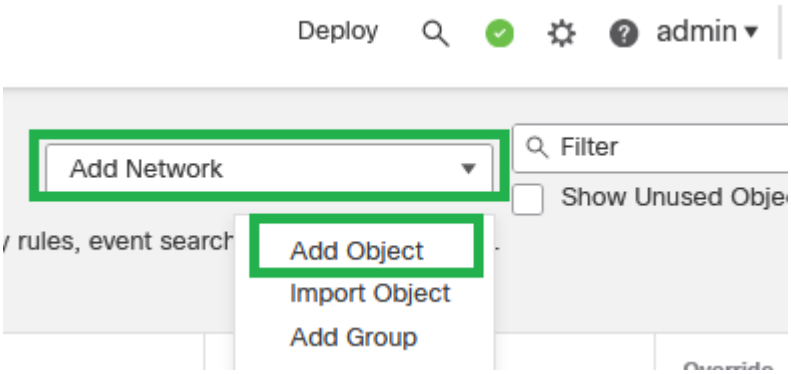
Objetos - Gestión de objetos

Paso 2: Haga clic en Network en el menú de la izquierda.



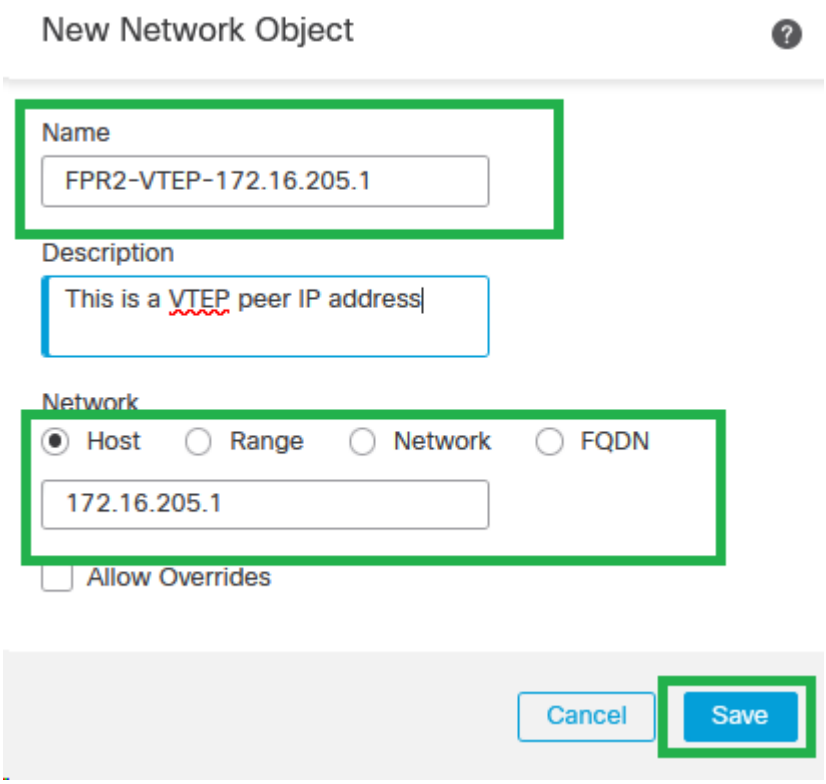
Red

Paso 3: Cree objetos de host de red para las direcciones IP del par VTEP. Haga clic en Add Network > Add Object.



Agregar red - Agregar objeto

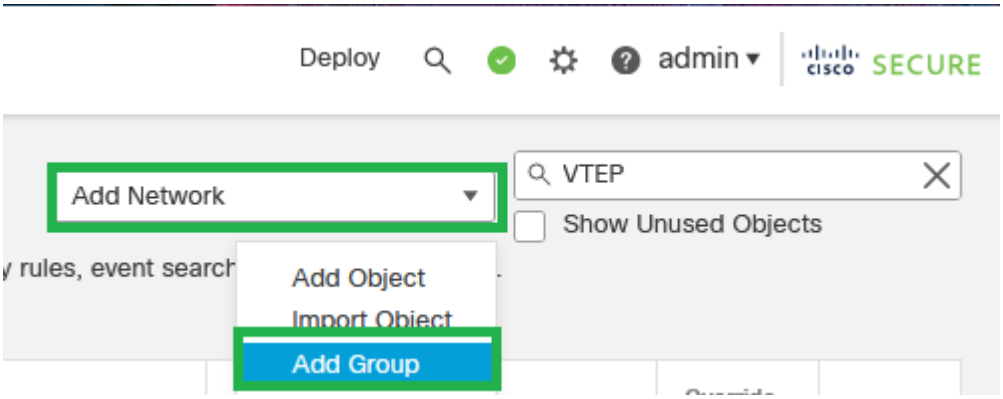
Paso 4: Cree un nuevo objeto de red host para el par VTEP. Configure un nombre de objeto y una dirección IP y, a continuación, haga clic en Guardar.



Nuevo objeto de red

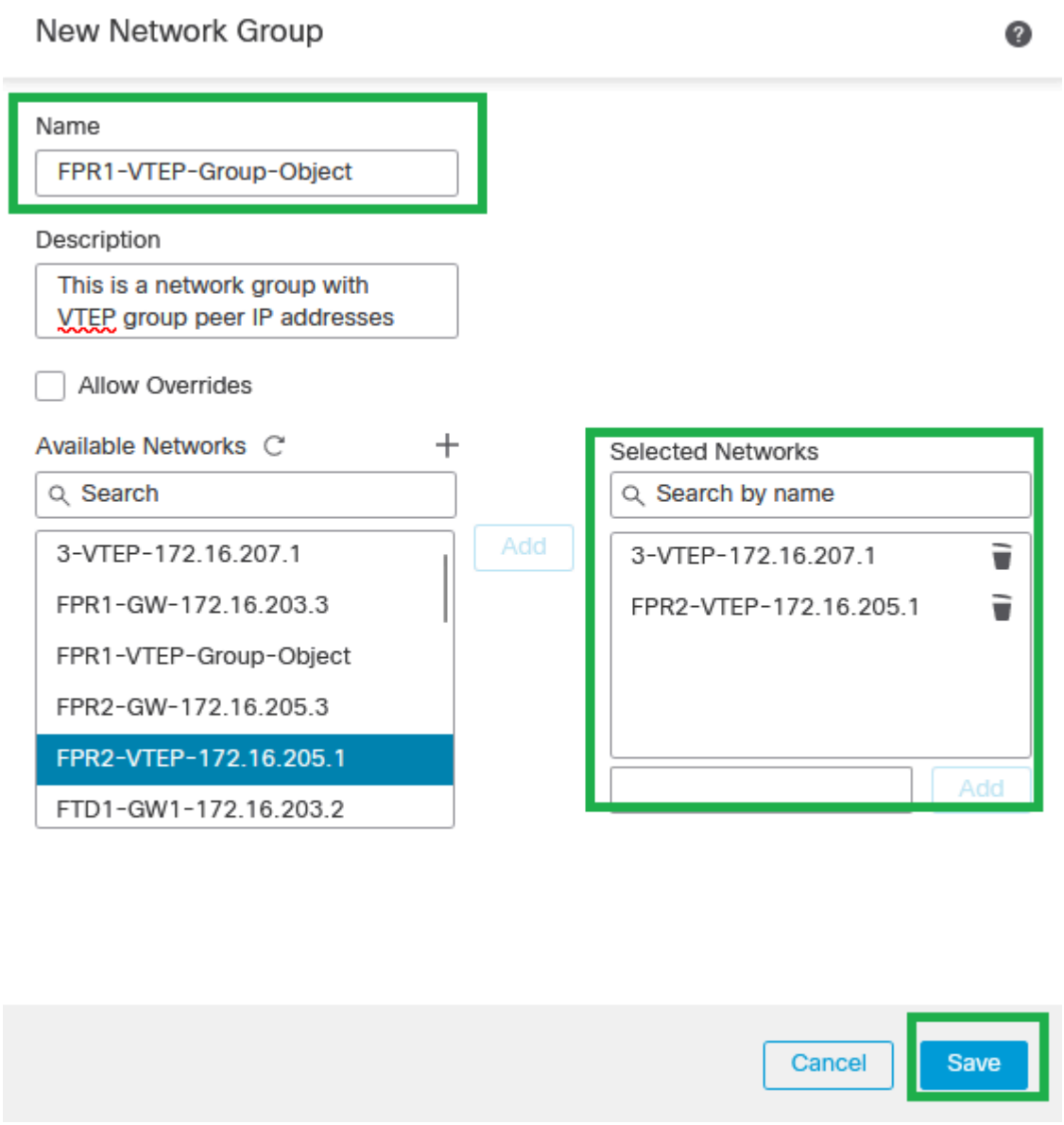
Nota: Configure más objetos de red de host para cada dirección IP de par VTEP que tenga. Hay dos objetos en esta guía de configuración.

Paso 5: Crear grupo de objetos, haga clic en Agregar red > Agregar grupo.



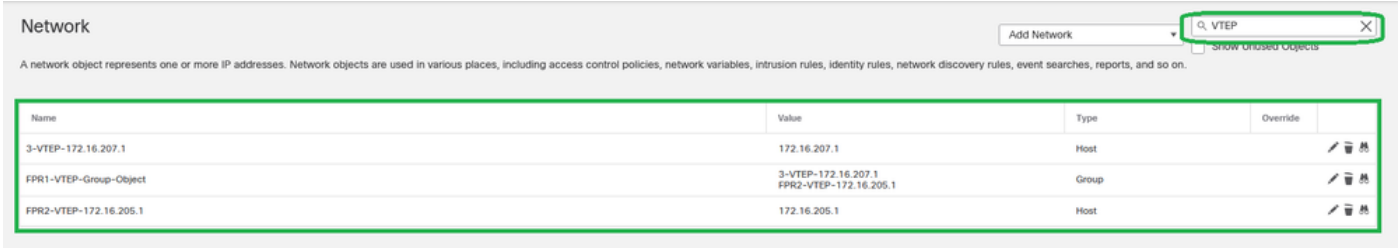
Agregar red - Agregar grupo

Paso 6: Cree el grupo de objetos de red con todas las direcciones IP de peer VTEP. Configure un nombre de grupo de red, seleccione los grupos de objetos de red necesarios y haga clic en Save.



Crear grupo de objetos de red

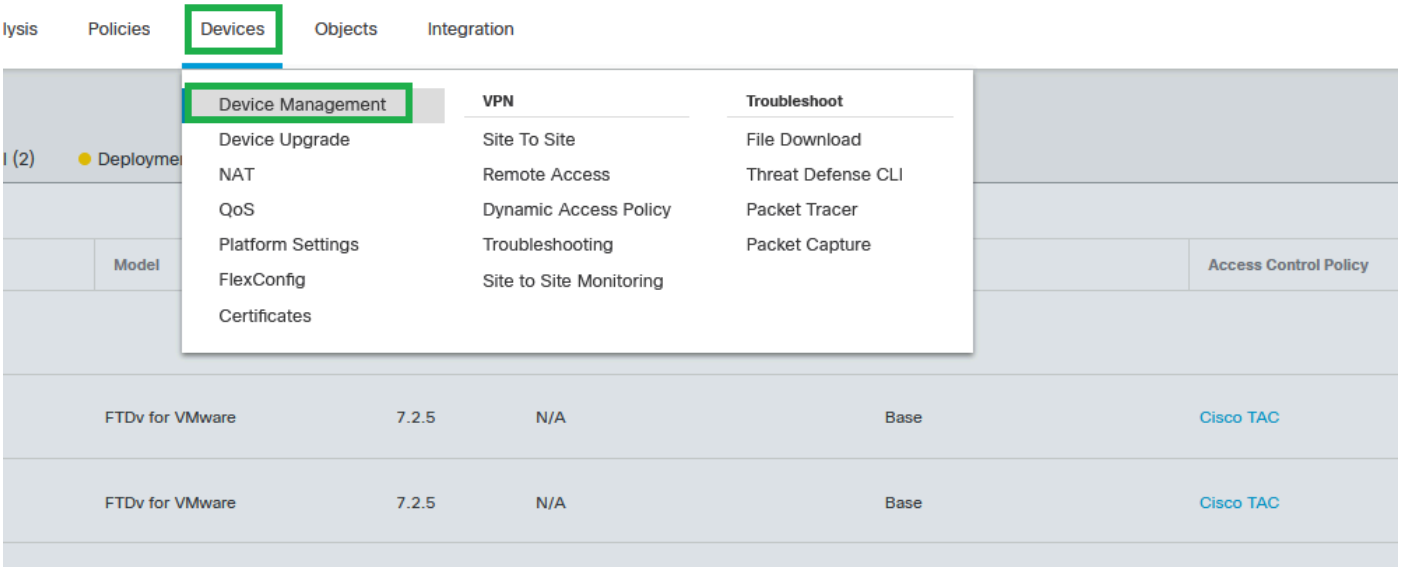
Paso 7: Valide el objeto de red y el grupo de objetos de red desde el filtro Objeto de red.



Validar el grupo de objetos VTEP

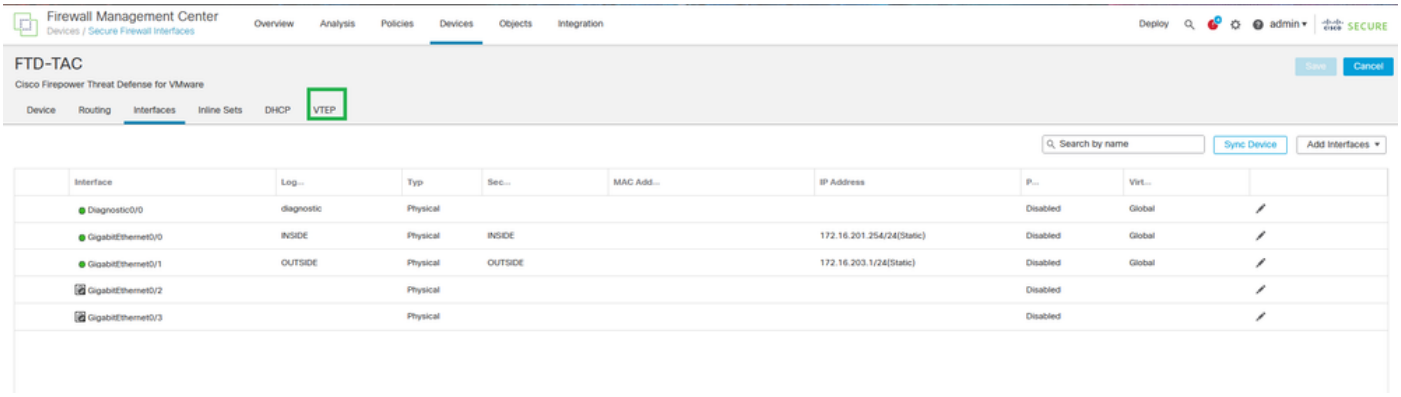
Configuración de la interfaz de origen de VTEP

Paso 1: Navegue hasta Devices > Device Management, y edite la defensa contra amenazas.



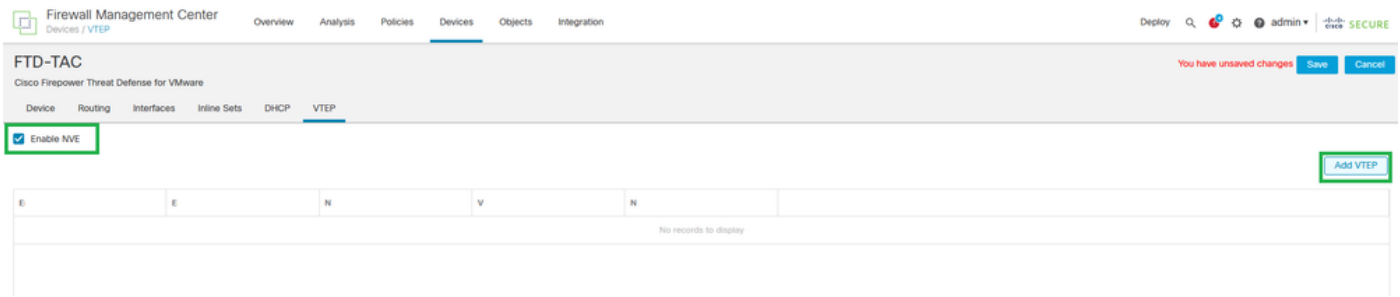
Dispositivos: gestión de dispositivos

Paso 2: Vaya a la sección VTEP.



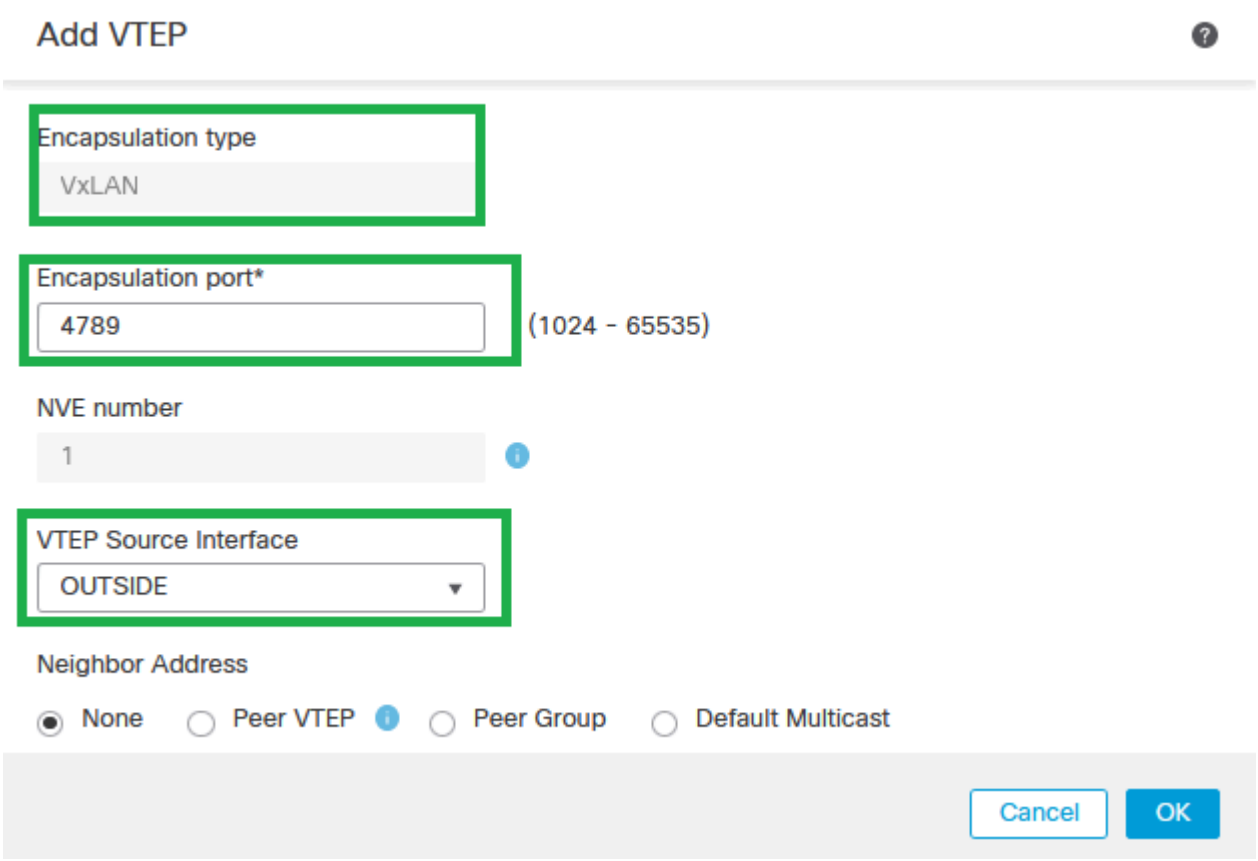
sección VTEP

Paso 3: Seleccione la casilla de verificación Enable VNE y haga clic en Add VTEP.



Habilitar NVE y agregar VTEP

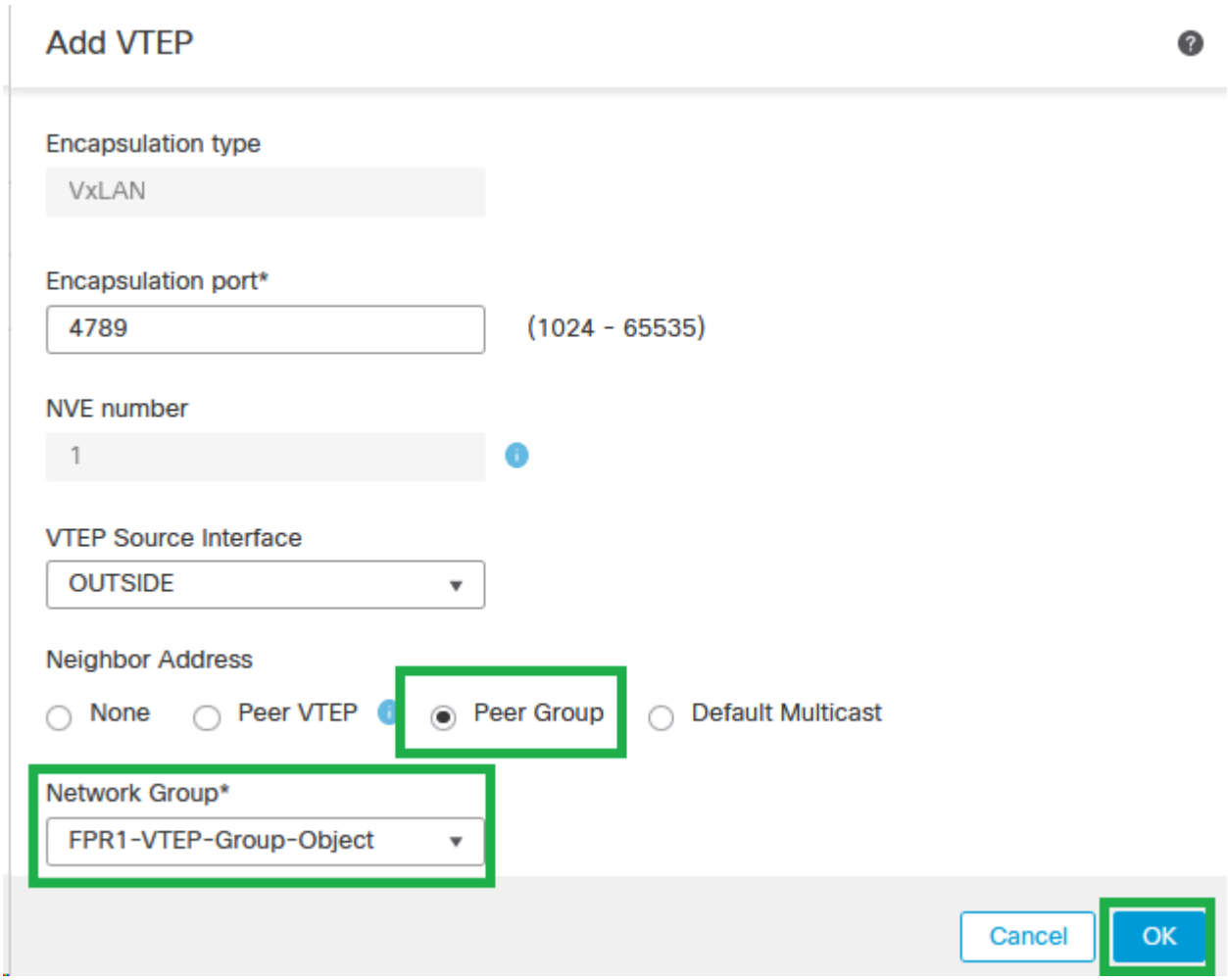
Paso 4: Elija VxLAN como tipo de encapsulación, ingrese el valor de Puerto de encapsulación y elija la interfaz utilizada para el origen VTEP en esta defensa contra amenazas (Interfaz externa para esta guía de configuración)



Agregar VTEP

Nota: La encapsulación VxLAN es la predeterminada. Para AWS, puede elegir entre VxLAN y Geneve. El valor predeterminado es 4789, cualquier puerto de encapsulación se puede elegir entre el rango de 1024 a 65535 según el diseño.

Paso 5: Seleccione Peer Group y elija el Network Object Group creado en la sección de configuración anterior, luego haga clic en OK.

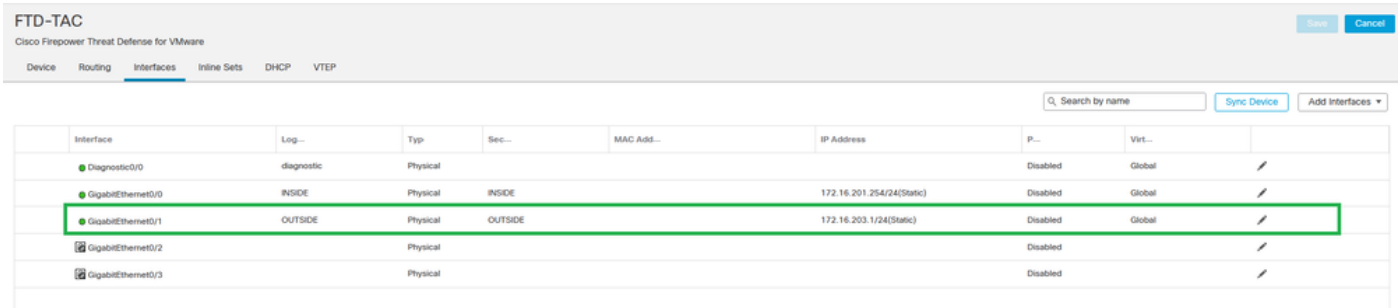


Grupo de pares: grupo de objetos de red

Paso 6: Guarde los cambios.

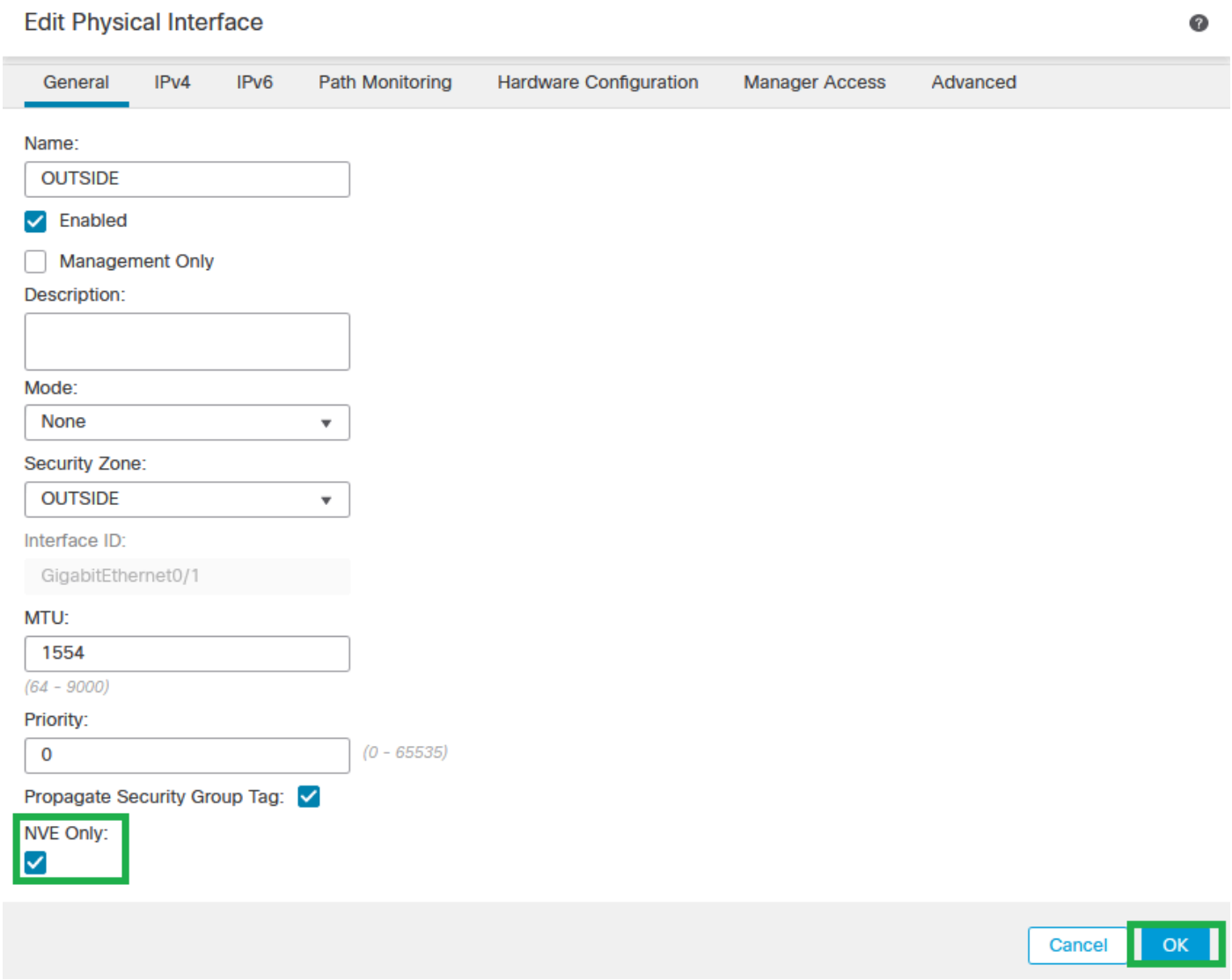
Advertencia: Después de guardar los cambios, aparece un mensaje de cambio de trama jumbo, se cambia la MTU en la interfaz asignada como VTEP a 1554, asegúrese de utilizar la misma MTU en la red subyacente.

Paso 7:Haga clic en Interfaces y edite la Interfaz utilizada para la Interfaz de origen VTEP. (Interfaz externa en esta guía de configuración)



Fuera como interfaz de origen de VTEP

Paso 8 (opcional):En la página General, marque la casilla de verificación de Sólo NVE, Luego haga clic en OK (Aceptar).



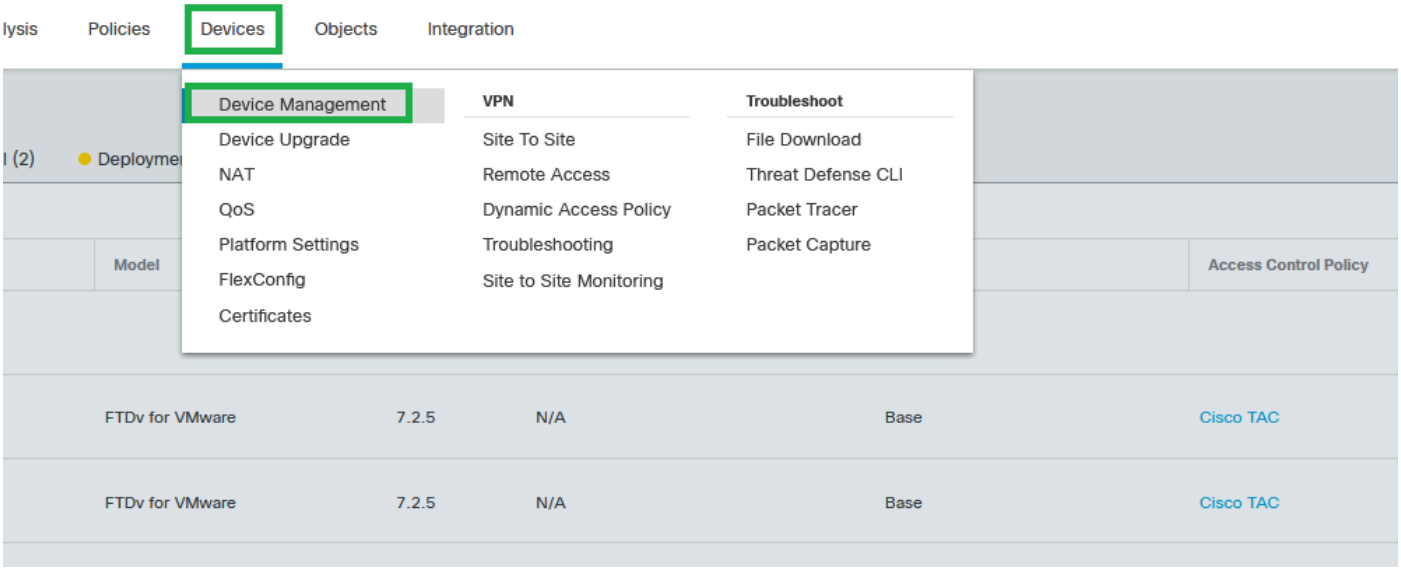
Configuración NVE Only

Advertencia: Esta configuración es opcional para el modo ruteado, donde restringe el tráfico a VXLAN y el tráfico de administración común sólo en esta interfaz. Esta configuración se habilita automáticamente para el modo de firewall transparente.

Paso 9: Guarde los cambios.

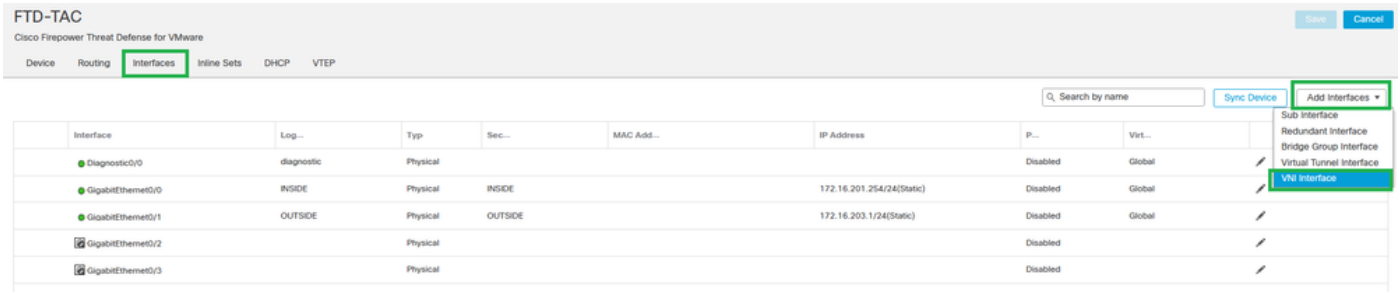
Configuración de la interfaz VTEP VNI

Paso 1: Navegue Devices > Device Management, y edite la defensa contra amenazas.



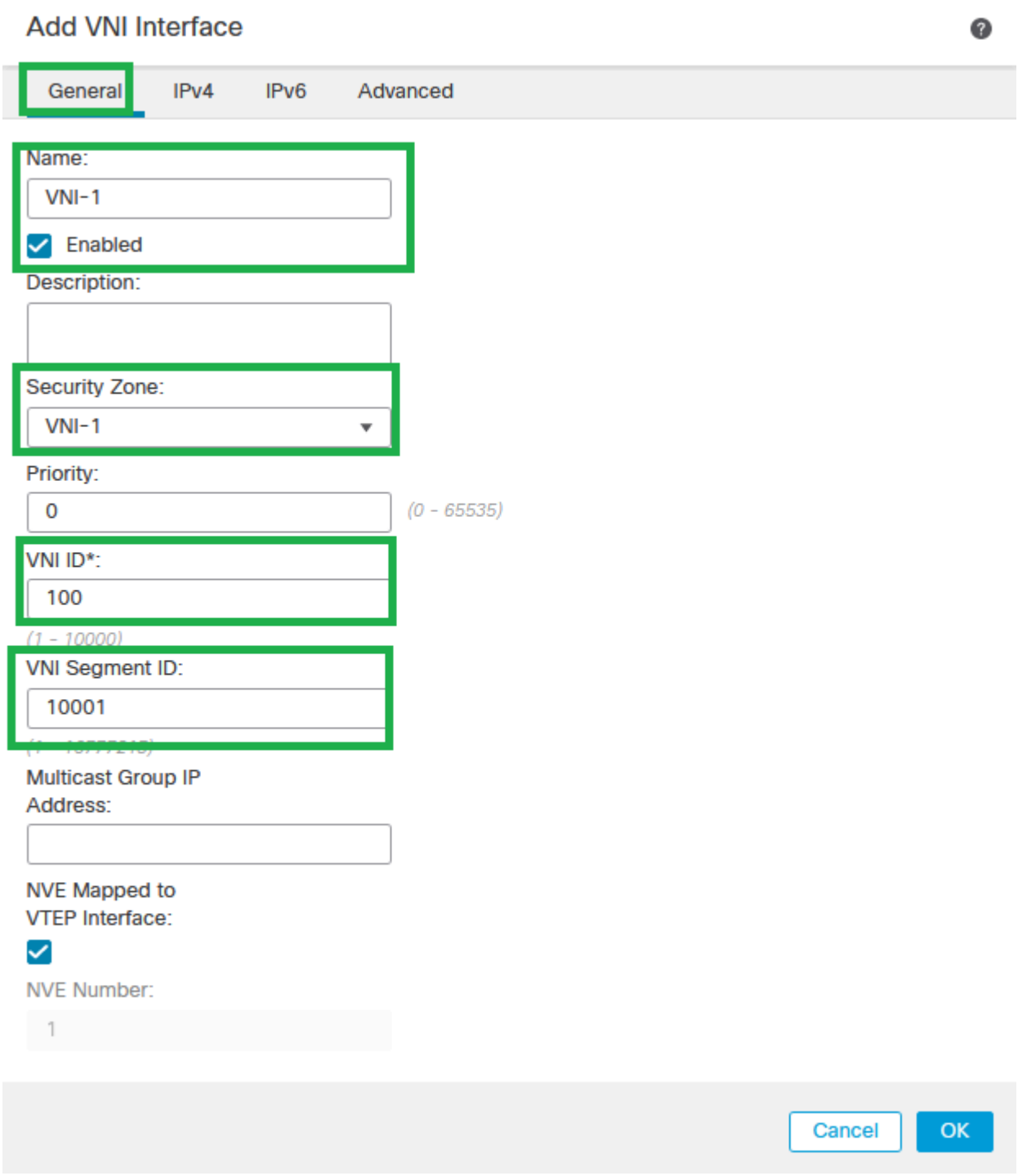
Dispositivos: gestión de dispositivos

Paso 2: En la sección Interfaces, haga clic en Add Interfaces > VNI Interfaces.



Interfaces - Agregar interfaces - Interfaces VNI

Paso 3: En la sección General, configure la interfaz VNI con nombre, descripción, zona de seguridad, ID de VNI e ID de segmento de VNI.



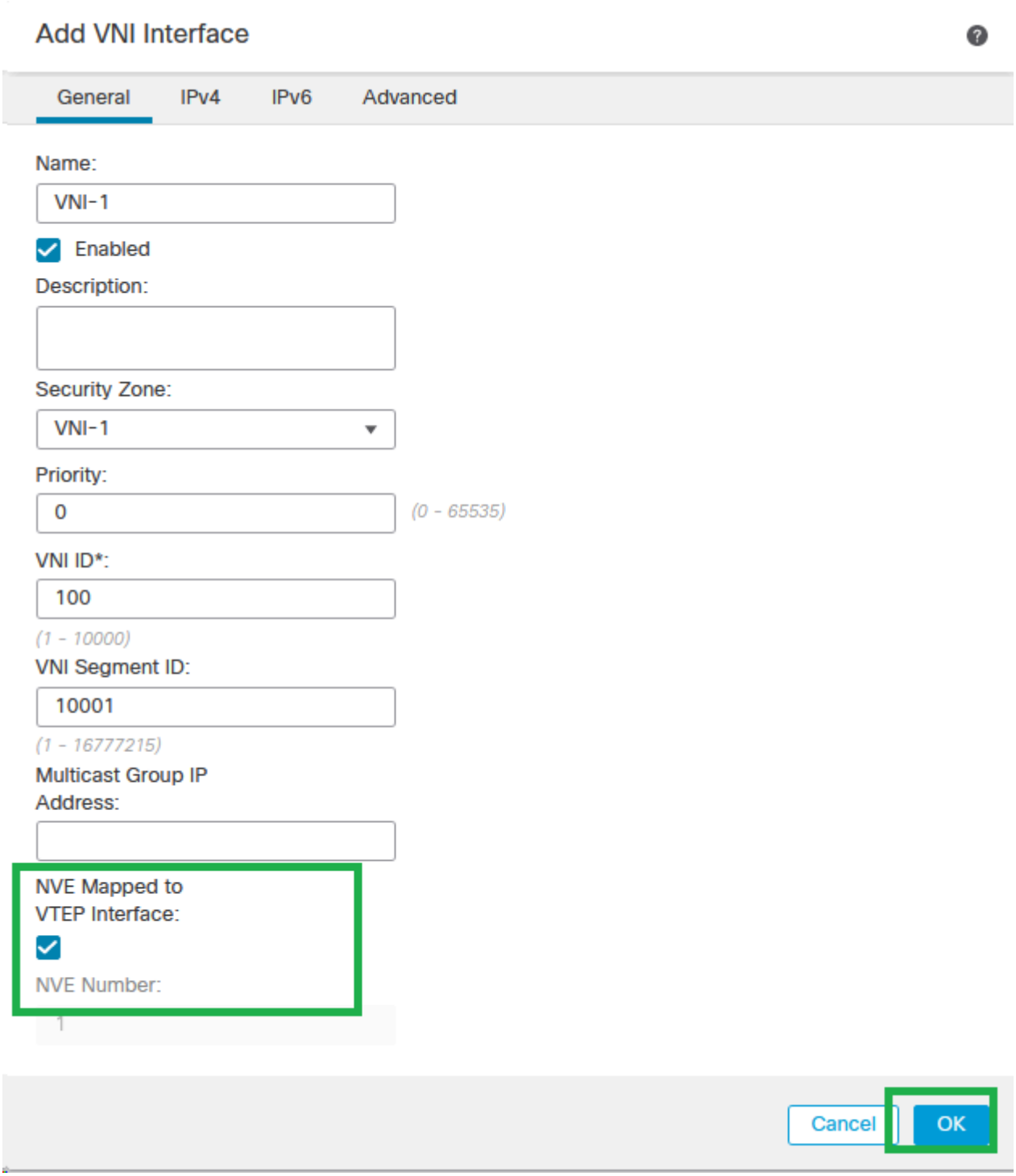
Agregar interfaz VNI

Nota: La ID de VNI se configura entre 1 y 10000, y la ID de segmento de VNI se configura entre 1 y 16777215 (la ID de segmento se utiliza para el etiquetado de VXLAN).

Precaución: Si el grupo multicast no está configurado en la interfaz VNI, se utiliza el grupo predeterminado de la configuración de la interfaz de origen VTEP si está disponible. Si configura manualmente una IP de peer VTEP para la interfaz de origen VTEP, no puede

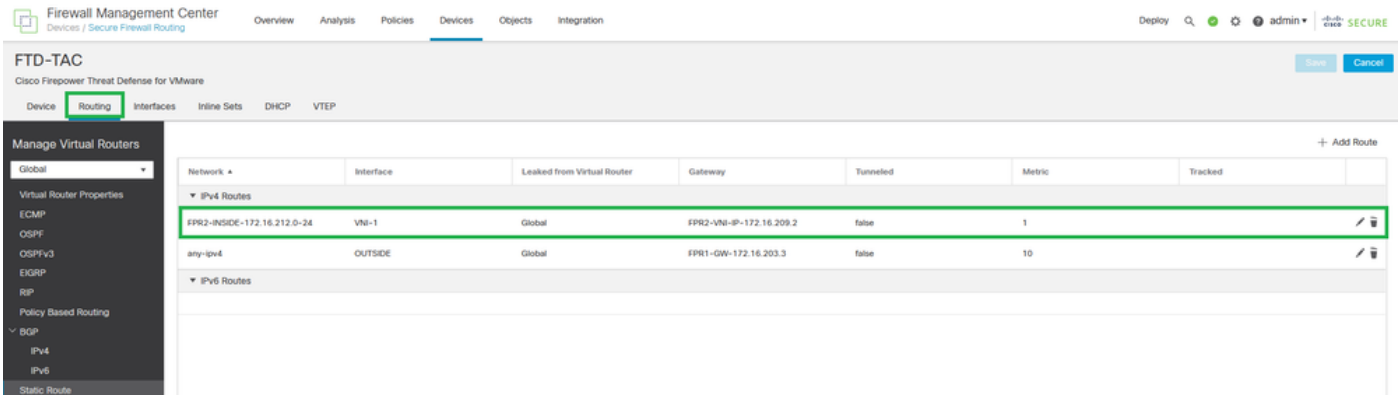
especificar un grupo multicast para la interfaz VNI.

Paso 3: Seleccione la casilla de verificación NVE Mapped to VTEP Interface y haga clic en OK.



NVE asignada a la interfaz VTEP

Paso 4: Configure una ruta estática para anunciar las redes de destino para VXLAN a la interfaz de par VNI. Vaya a Routing > Static Route.



Configuración de ruta estática

Precaución: Las redes de destino para VXLAN se deben enviar a través de la interfaz VNI par. Todas las interfaces VNI deben estar en el mismo dominio de difusión (segmento lógico).

Paso 5: Guardar e implementar los cambios.

Advertencia: Las advertencias de validación se pueden ver antes de la implementación, asegúrese de que las direcciones IP del par VTEP sean accesibles desde la interfaz de origen VTEP física.

Verificación

Verifique la configuración de 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 la configuración de la interfaz 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 la configuración de MTU en la interfaz 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 la configuración de la ruta estática para las 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
```

Nota: Valide las interfaces VNI en todos los pares configurados en el mismo dominio de broadcast.

Troubleshoot

Compruebe la conectividad con los pares VTEP.

Peer 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
```

Peer 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
```

Nota: Un problema de conectividad entre pares VTEP puede generar errores de implementación en FMC seguro. Asegúrese de mantener la conectividad en todas las configuraciones de pares VTEP.

Compruebe la conectividad con los pares VNI.

.

Peer 1:

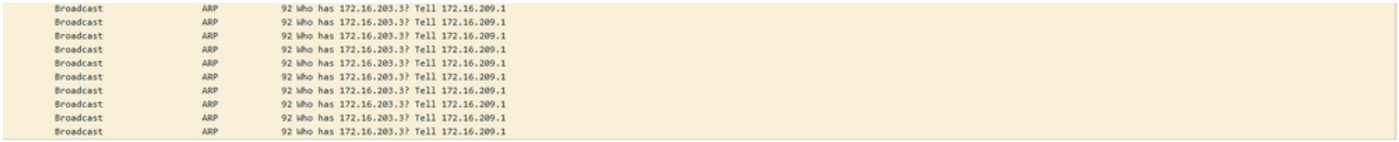
```
firepower# ping 172.16.209.2
```

```
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
```

Peer 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
```

A veces, una ruta estática incorrecta configurada puede generar salidas ARP incompletas. Configure una captura en la interfaz VTEP para paquetes VXLAN y descárguela en un formato pcap. Cualquier herramienta de análisis de paquetes ayuda a confirmar si hay algún problema con las rutas. Asegúrese de utilizar la dirección IP del par VNI como gateway.



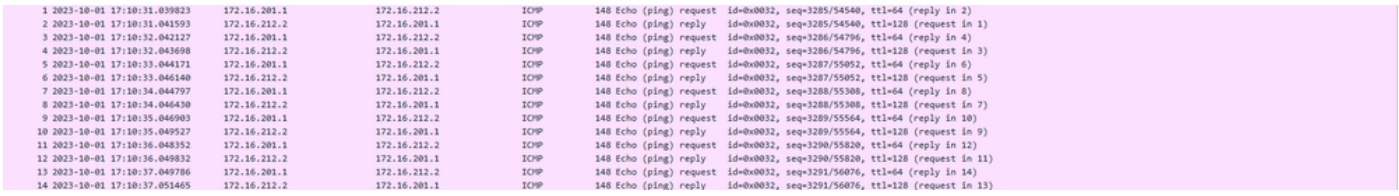
Problema de ruteo

Configure las capturas de caídas de ASP en FTD seguro en caso de que se produzca alguna caída de Firewall, verifique el contador de caídas de ASP con el comando show asp drop. Póngase en contacto con Cisco TAC para realizar análisis.

Asegúrese de configurar las reglas de la política de control de acceso para permitir el tráfico UDP de VXLAN en la interfaz VNI/VTEP.

A veces los paquetes VXLAN se pueden fragmentar, asegúrese de cambiar la MTU a tramas jumbo en la red subyacente para evitar la fragmentación.

Configure la captura en la interfaz de Ingress/VTEP y descargue las capturas en formato .pcap para su análisis. Los paquetes deben incluir el encabezado VXLAN en la interfaz VTEP,



Ping capturado con encabezado VXLAN

encabezado VXLAN

Información Relacionada

- Configuración de interfaces VXLAN
- Casos prácticos de VXLAN
- Procesamiento de paquetes VXLAN
- Configuración de la interfaz de origen de VTEP
- Configuración de la interfaz VNI
- Soporte técnico y descargas de 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).

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).