Configuración de VPN de sitio a sitio basada en ruta con reconocimiento de VRF en FTD administrado por FDM

Contenido

Introducción

Este documento describe cómo configurar la VPN de sitio a sitio basada en rutas que reconoce VRF en el FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de VPN
- Comprensión básica del reenvío y routing virtuales (VRF)
- Experiencia con FDM

Componentes Utilizados

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

- Cisco FTDv versión 7.4.2
- Cisco FDM versión 7.4.2

- Cisco ASAv versión 9.20.3

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.

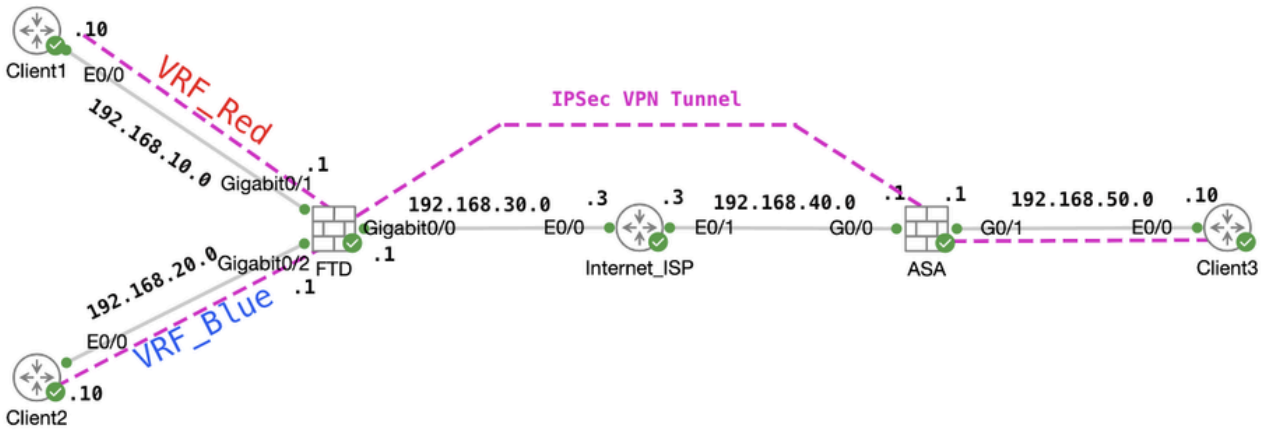
Antecedentes

El reenvío y routing virtuales (VRF) en Firepower Device Manager (FDM) permite crear varias instancias de routing aisladas en un único dispositivo Firepower Threat Defence (FTD). Cada instancia de VRF funciona como un router virtual independiente con su propia tabla de routing, lo que permite la separación lógica del tráfico de red y proporciona funciones mejoradas de seguridad y gestión del tráfico.

Este documento explica cómo configurar la VPN IPSec que reconoce VRF con VTI. La red VRF Red y la red VRF Blue están detrás del FTD. El cliente 1 en la red VRF roja y el cliente 2 en VRF azul se comunicarían con el cliente 3 detrás de ASA a través del túnel VPN IPSec.

Configurar

Diagrama de la red

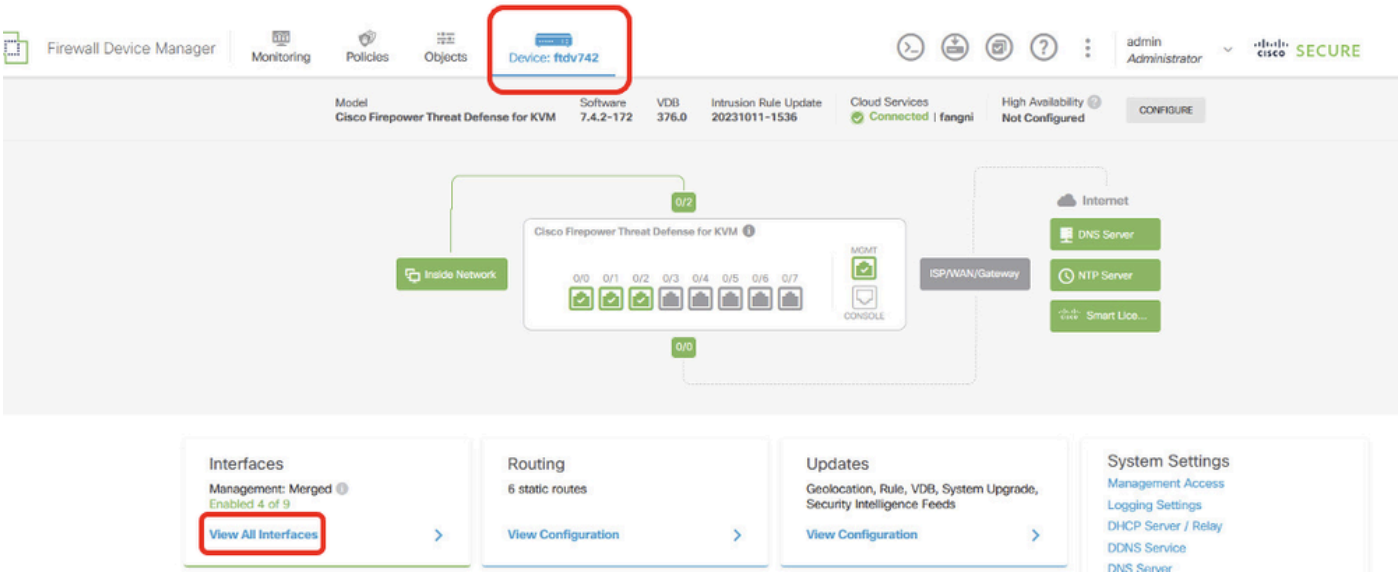


Topología

Configuración del FTD

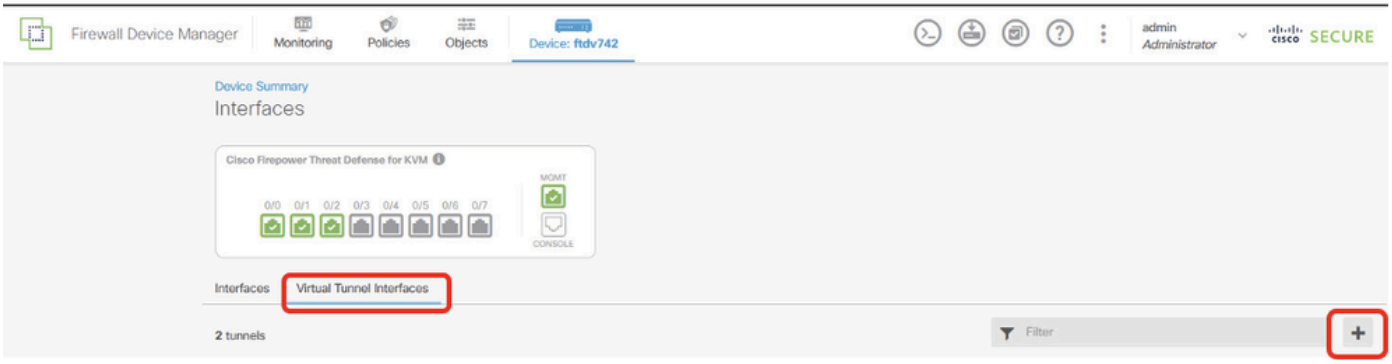
Paso 1. Es esencial asegurarse de que la configuración preliminar de la interconectividad IP entre nodos se haya completado debidamente. Client1 y Client2 tienen la dirección IP interna de FTD como gateway. El cliente 3 utiliza la dirección IP interna de ASA como gateway.

Paso 2. Crear interfaz de túnel virtual. Inicie sesión en la GUI de FDM de FTD. Vaya a Dispositivo > Interfaces . Haga clic en Ver todas las interfaces .



FTD_View_Interfaces

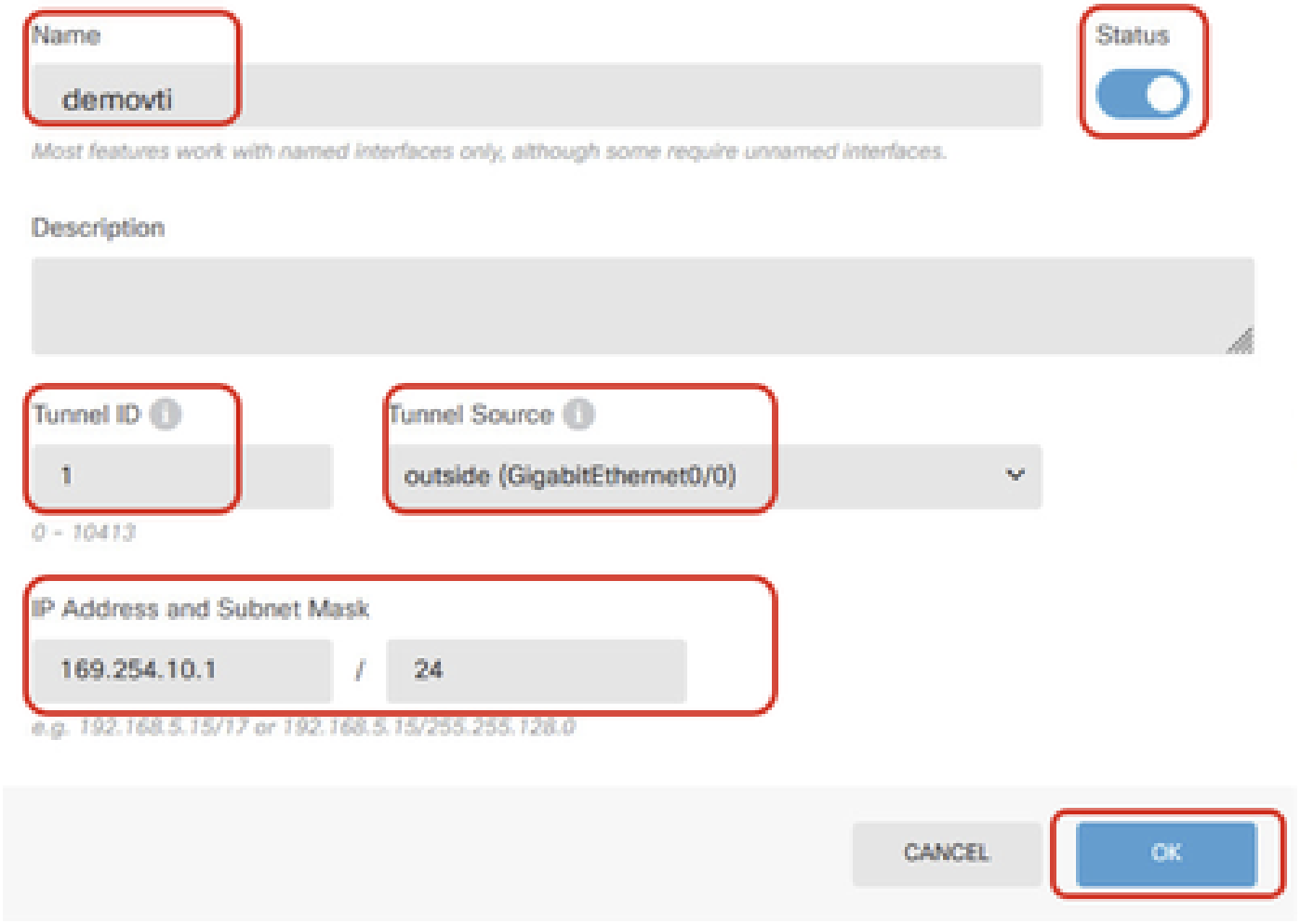
Paso 2.1. Haga clic en la pestaña Interfaces de Túnel Virtual. Haga clic en el botón +.



FTD_Create_VTI

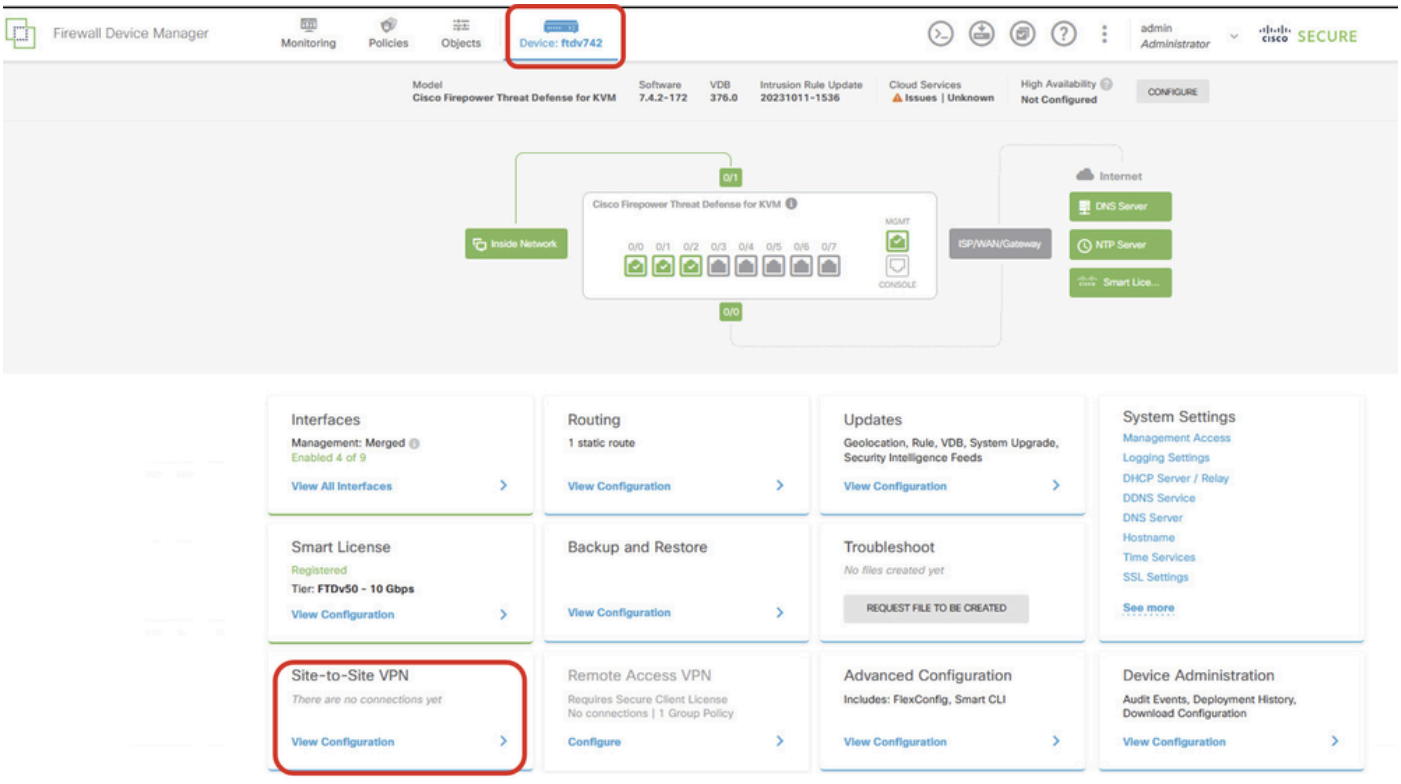
Paso 2.2. Proporcionar la información necesaria. Haga clic en el botón Aceptar.

- Nombre: demovti
- ID de túnel: 1
- Origen del túnel: externa (GigabitEthernet0/0)
- Dirección IP y máscara de subred: 169.254.10.1/24
- Estado: haga clic en el control deslizante hasta la posición Activado



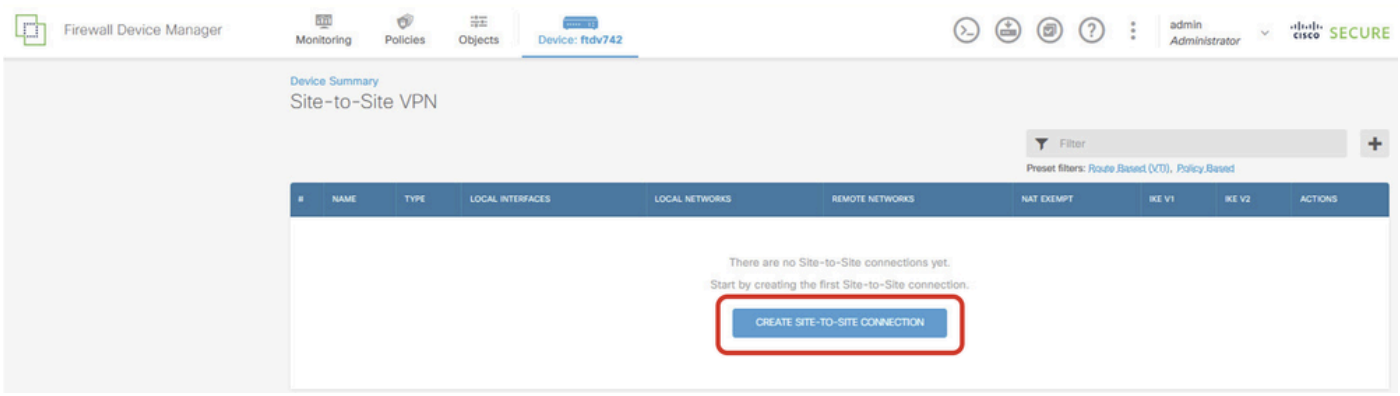
FTD_Create_VTI_Details

Paso 3. Vaya a Device > Site-to-Site VPN . Haga clic en el botón View Configuration.



FTD_Site-to-Site_VPN_View_Configurations

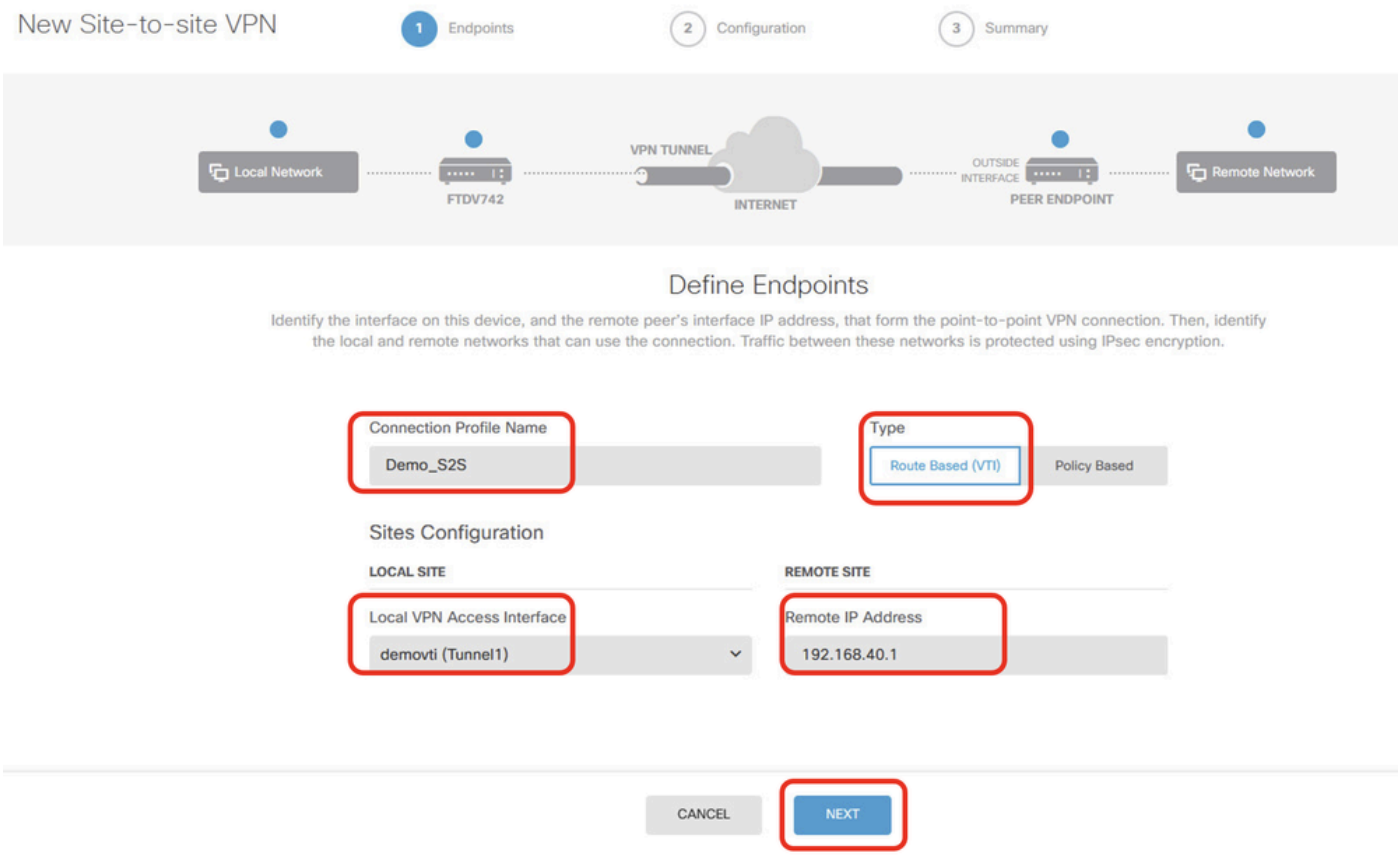
Paso 3.1. Comience a crear una nueva VPN de sitio a sitio. Haga clic en el botón CREATE SITE-TO-SITE CONNECTION. O haga clic en el botón +.



FTD_Create_Site2Site_Connection

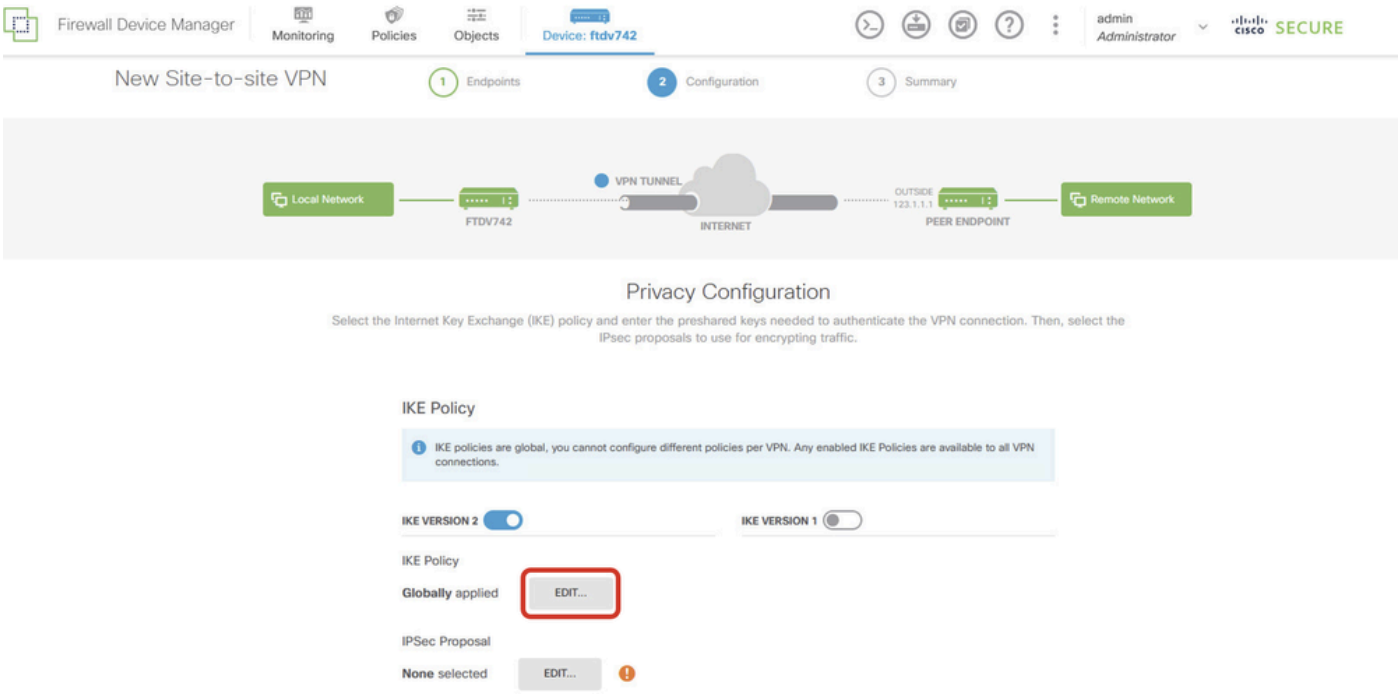
Paso 3.2. Proporcionar información necesaria. Haga clic en el botón NEXT.

- Nombre del perfil de conexión: Demo_S2S
- Tipo: Basado en ruta (VTI)
- Interfaz de acceso VPN local: demovti (creado en el paso 2)
- Dirección IP remota: 192.168.40.1 (se trata de una dirección IP externa de ASA par)



FTD_Site-to-Site_VPN_Endpoints

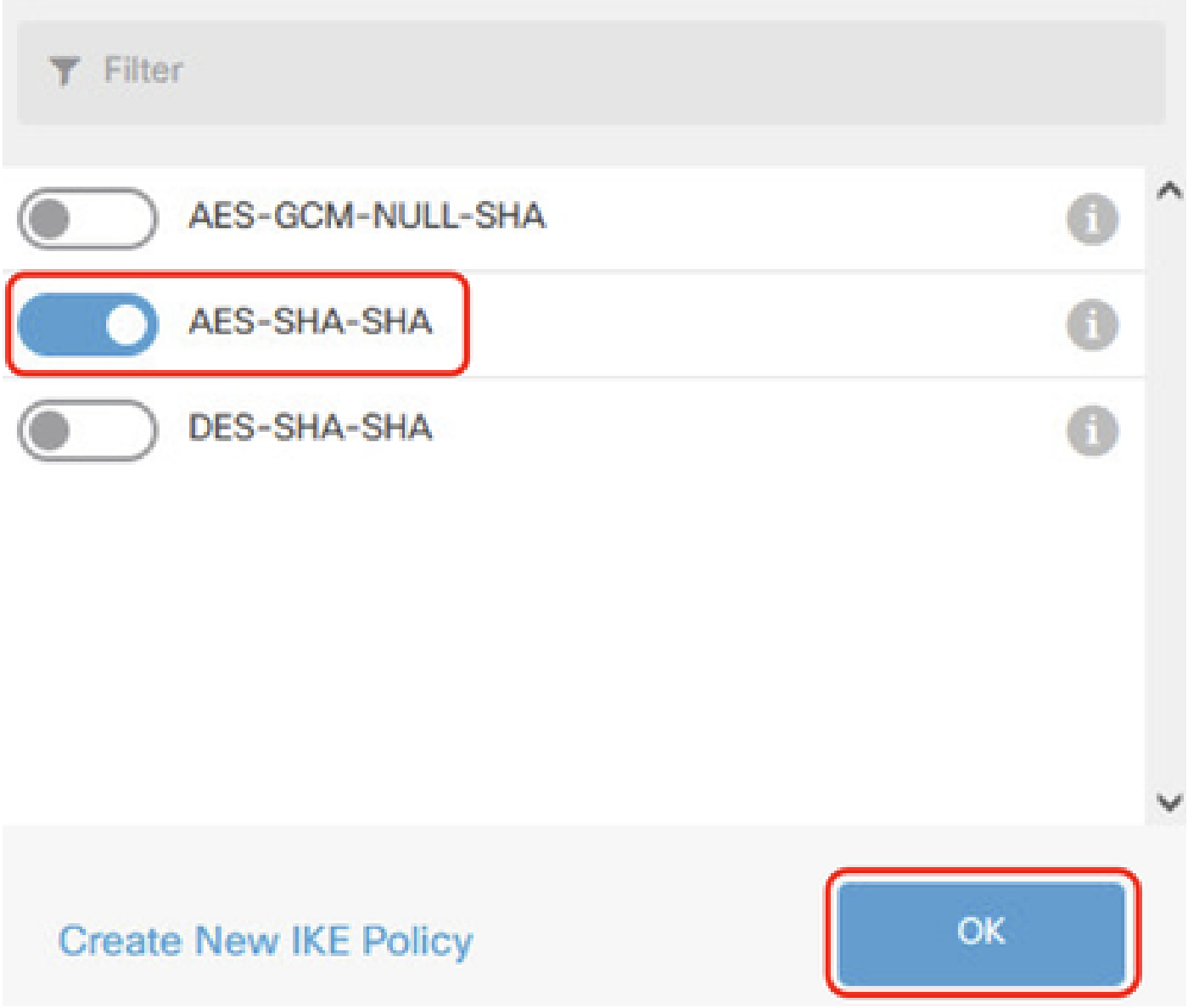
Paso 3.3. Vaya a Política IKE. Haga clic en el botón EDIT.



FTD_Edit_IKE_Policy

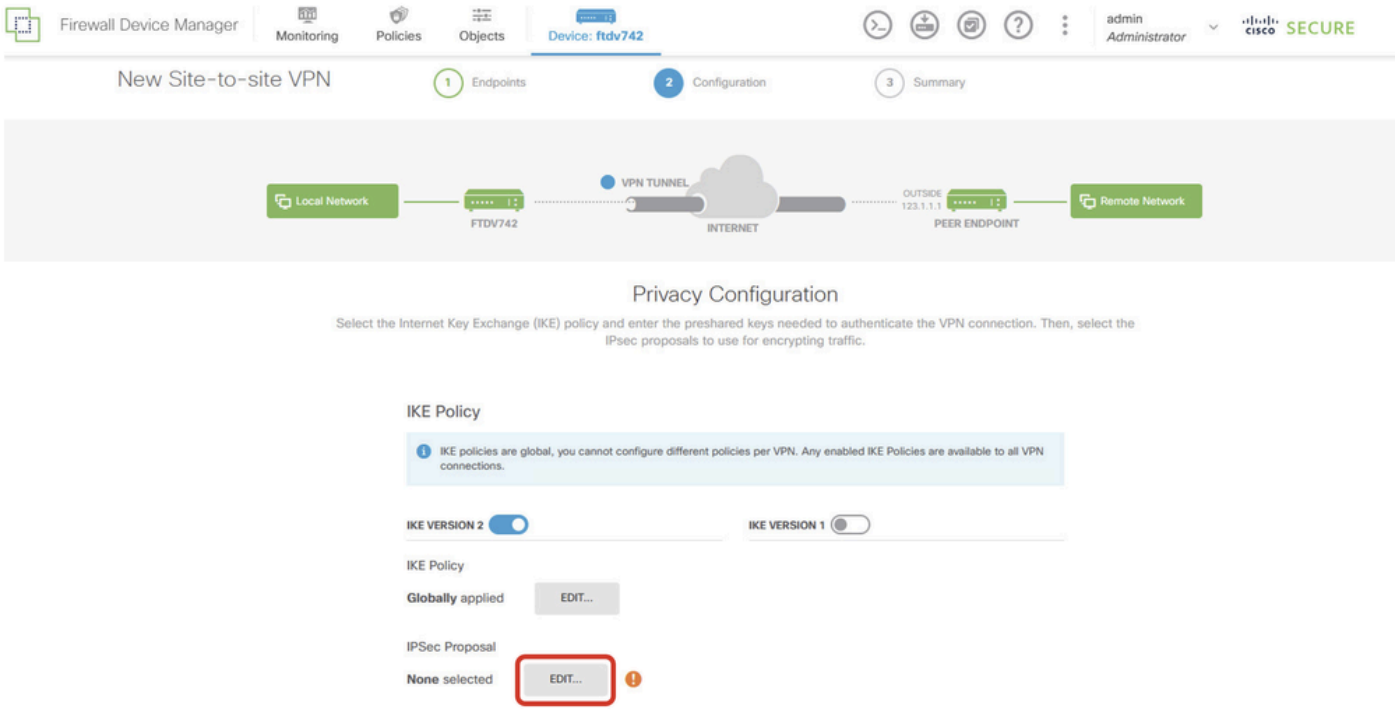
Paso 3.4. Para la política IKE, puede utilizar una predefinida o puede crear una nueva haciendo clic en Crear nueva política IKE .

En este ejemplo, alterne un nombre de política IKE existente AES-SHA-SHA . Haga clic en el botón Aceptar para guardar.



FTD_Enable_IKE_Policy

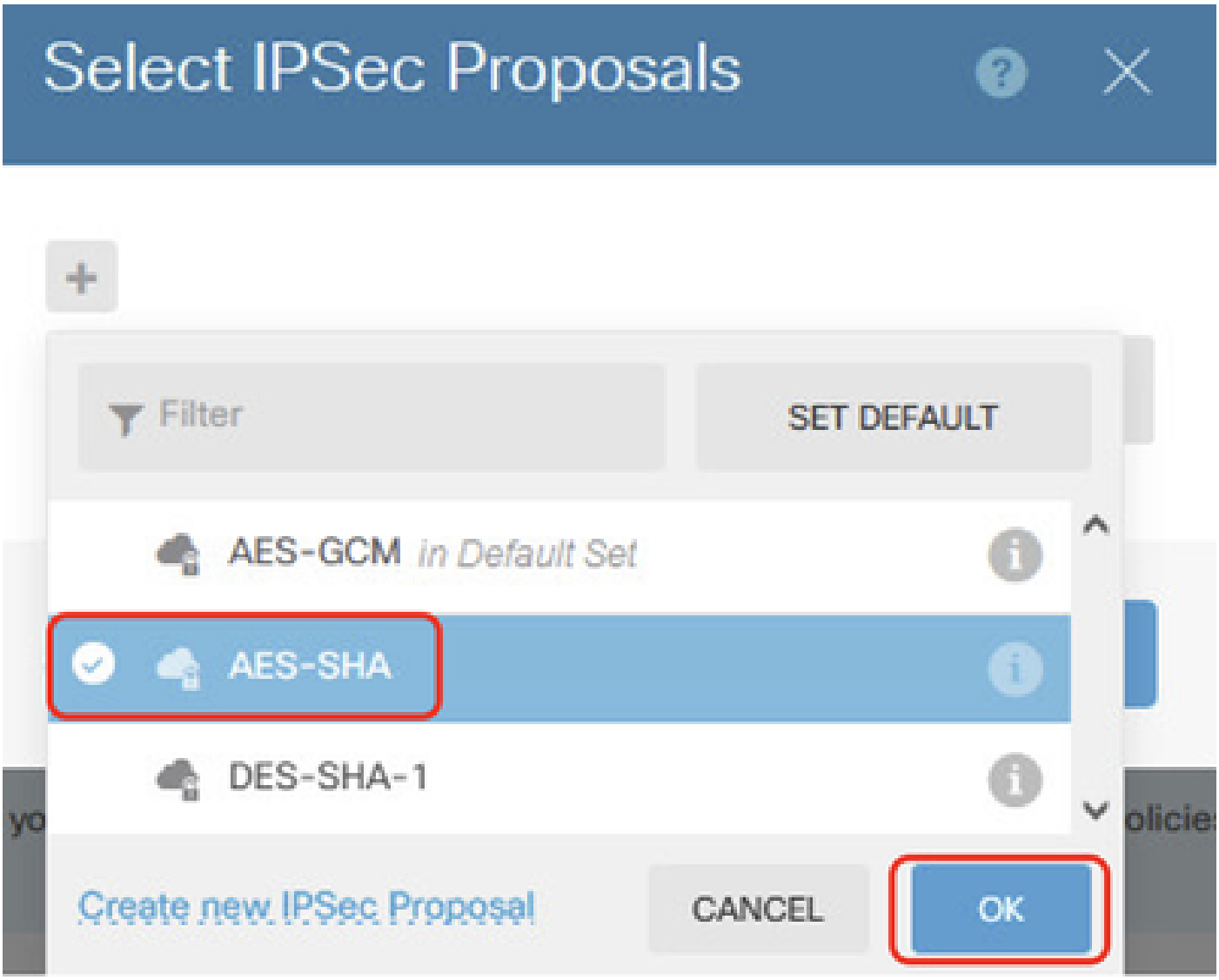
Paso 3.5. Vaya a Propuesta IPSec. Haga clic en el botón EDIT.



FTD_Edit_IPSec_Propuesta

Paso 3.6. Para la propuesta de IPSec, puede utilizar una predefinida o puede crear una nueva haciendo clic en Crear nueva propuesta de IPSec.

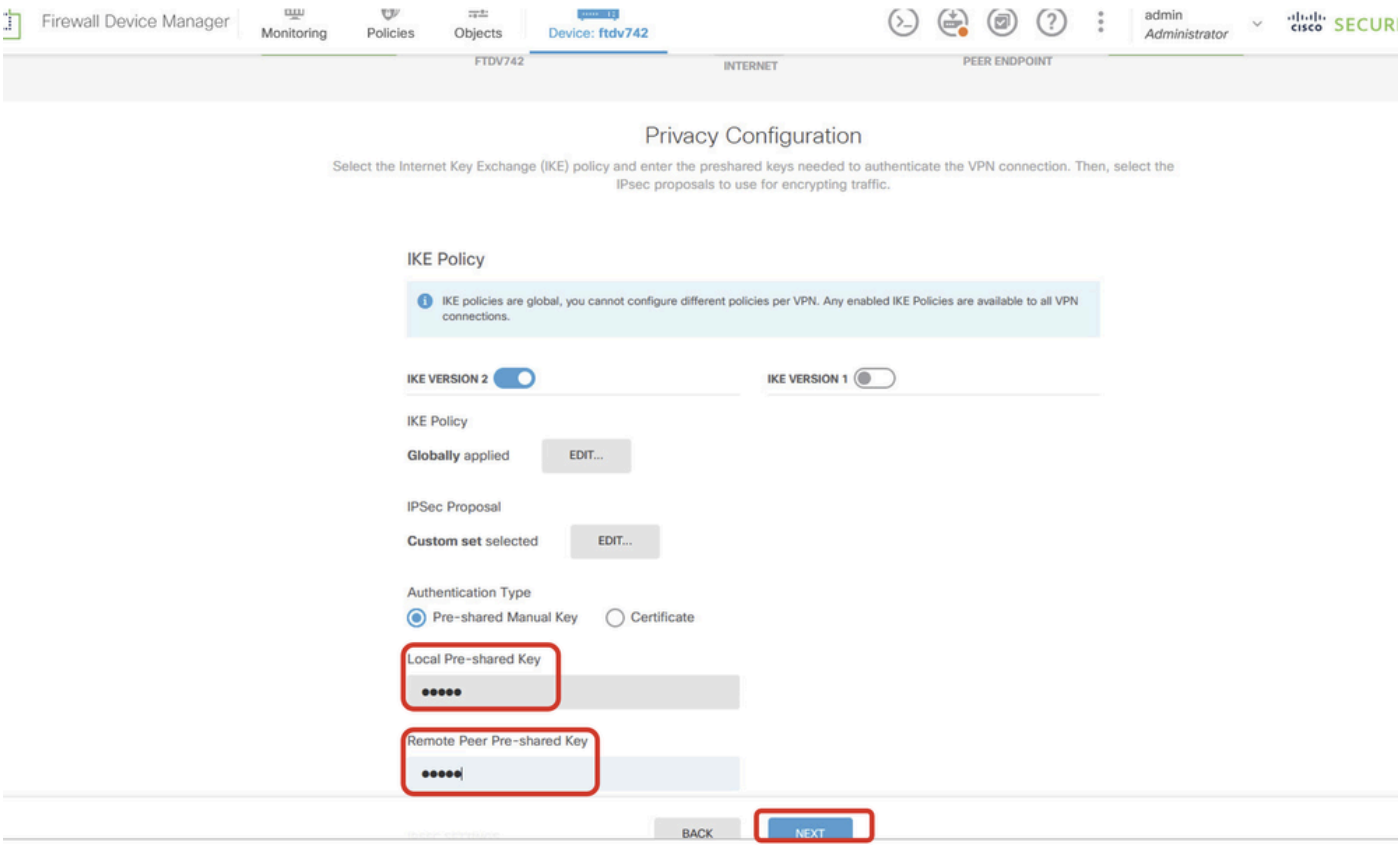
En este ejemplo, alterne un nombre de propuesta IPSec existente AES-SHA . Haga clic en OK para guardar.



FTD_Enable_IPSec_Propuesta

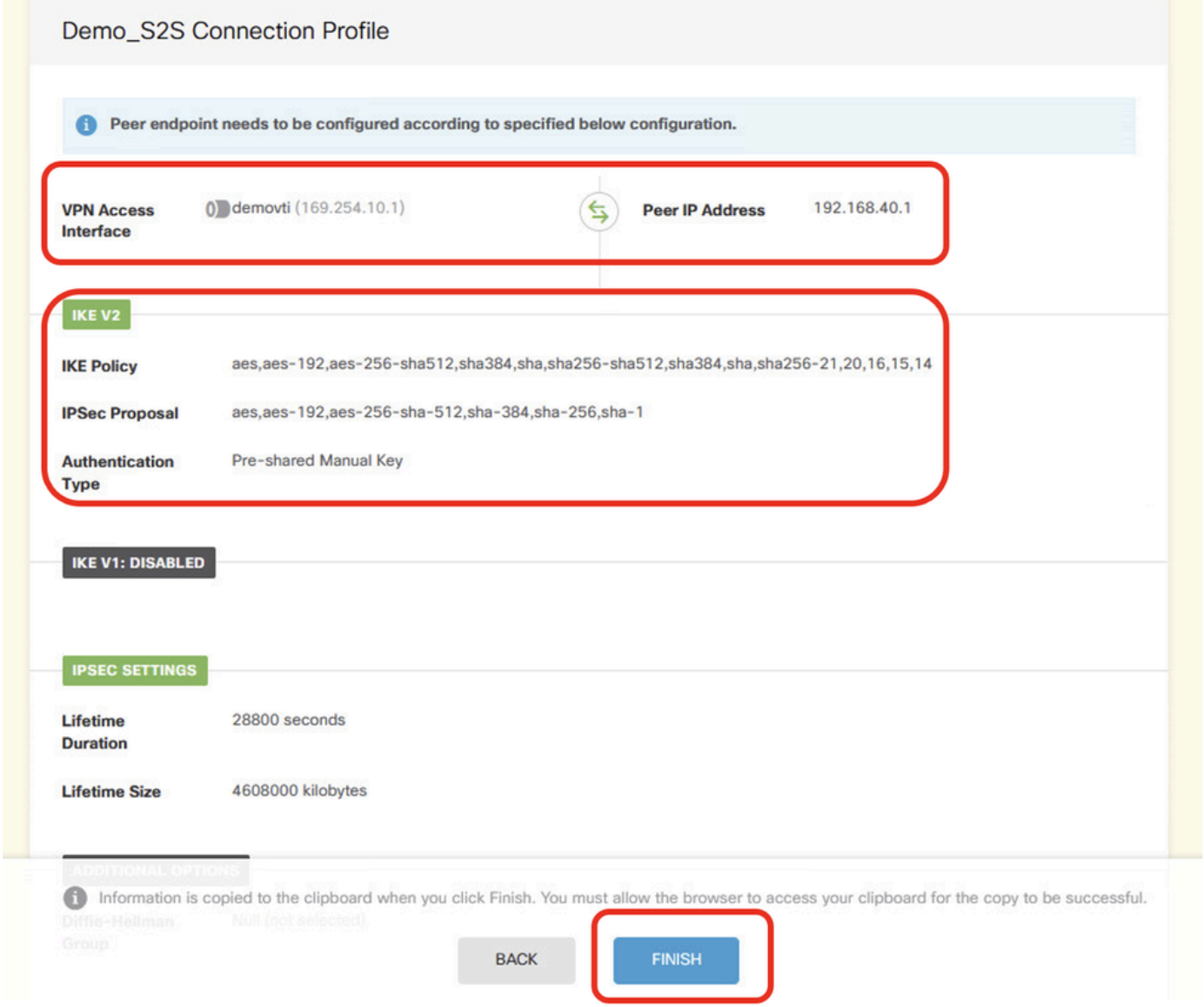
Paso 3.7. Desplácese por la página y configure la clave previamente compartida. Haga clic en el botón NEXT.

Anote esta clave previamente compartida y configúrela en ASA más tarde.



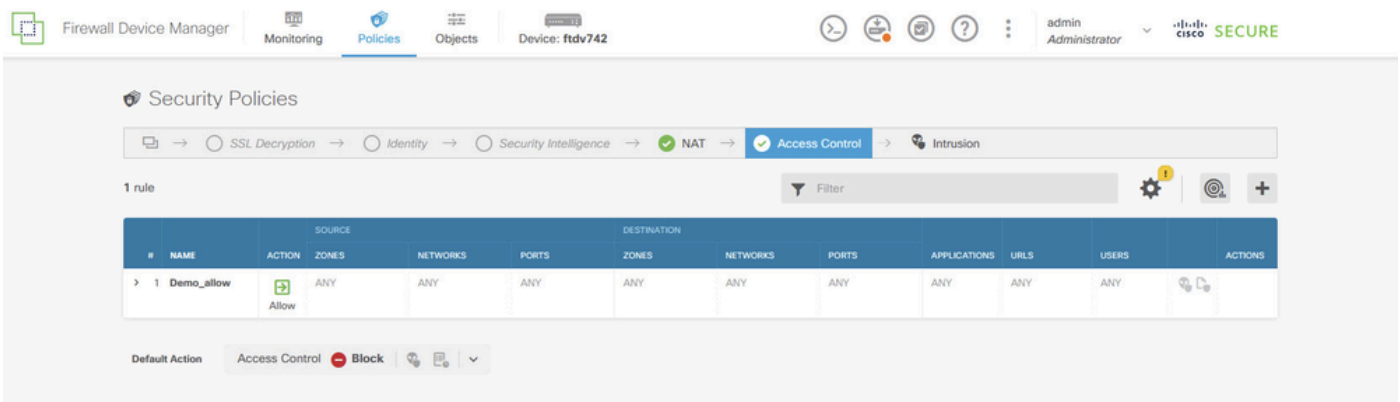
FTD_Configure_Pre_Shared_Key

Paso 3.8. Revise la configuración de VPN. Si necesita modificar algo, haga clic en el botón BACK. Si todo está bien, haga clic en el botón FINISH.



FTD_Review_VPN_Configuration

Paso 3.9. Crear regla de control de acceso para permitir que el tráfico pase a través del FTD. En este ejemplo, permita todas las demostraciones. Modifique su política en función de sus necesidades reales.

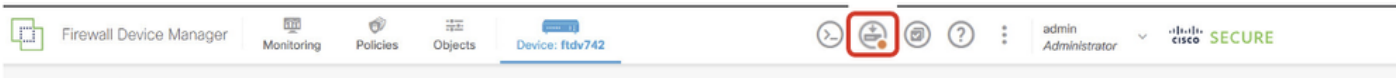


Ejemplo_FTD_ACP

Paso 3.10. (Opcional) Configure la regla de exención de NAT para el tráfico del cliente en FTD si

hay NAT dinámica configurada para que el cliente acceda a Internet. En este ejemplo, no hay necesidad de configurar una regla de exención de NAT porque no hay NAT dinámica configurada en FTD.

Paso 3.11. Implemente los cambios de configuración.



FTD_Deployment_Changes

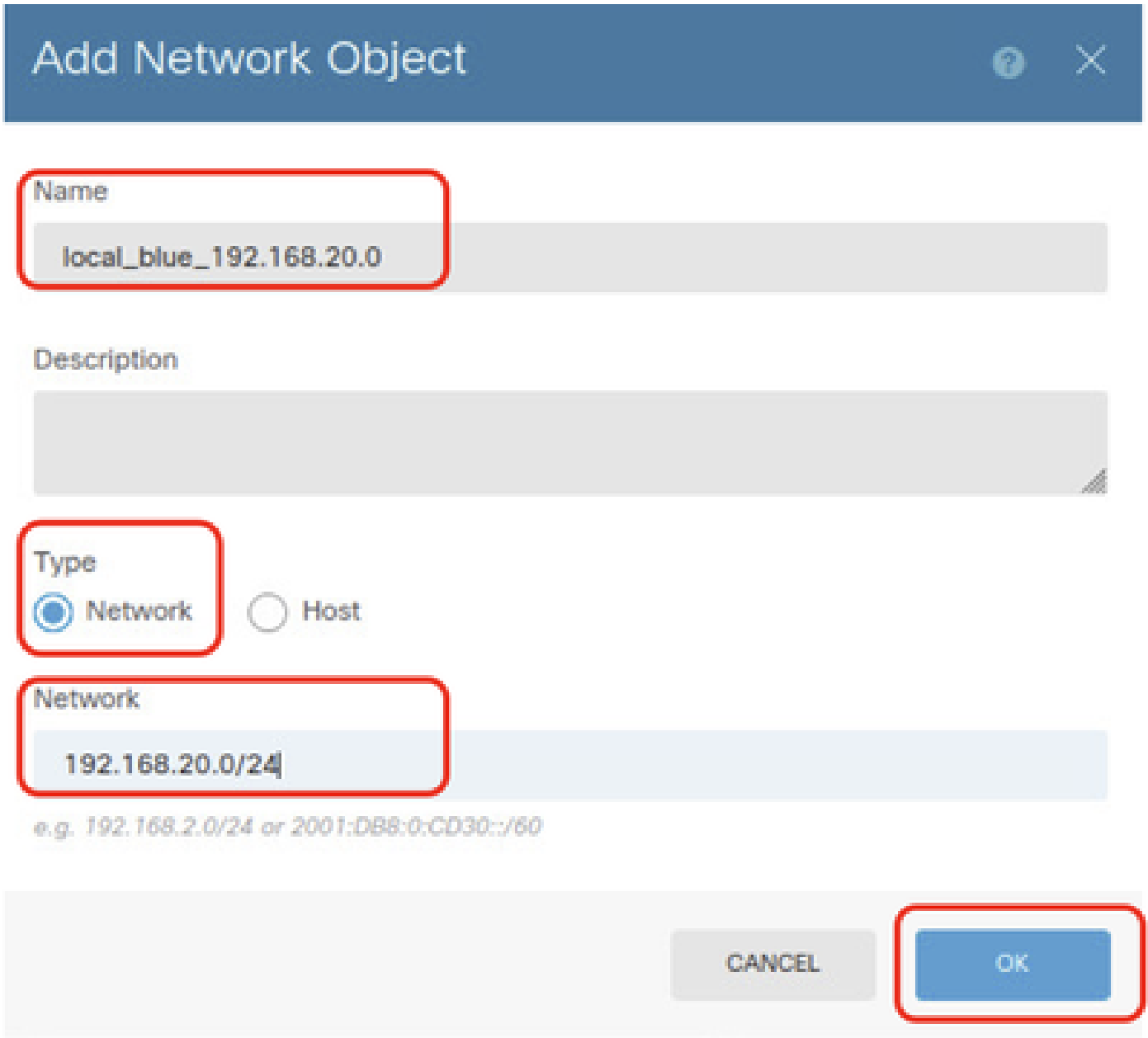
Paso 4. Configure los routers virtuales.

Paso 4.1. Cree objetos de red para la ruta estática. Navegue hasta Objetos > Redes , haga clic en el botón +.

FTD_Create_NetObjects

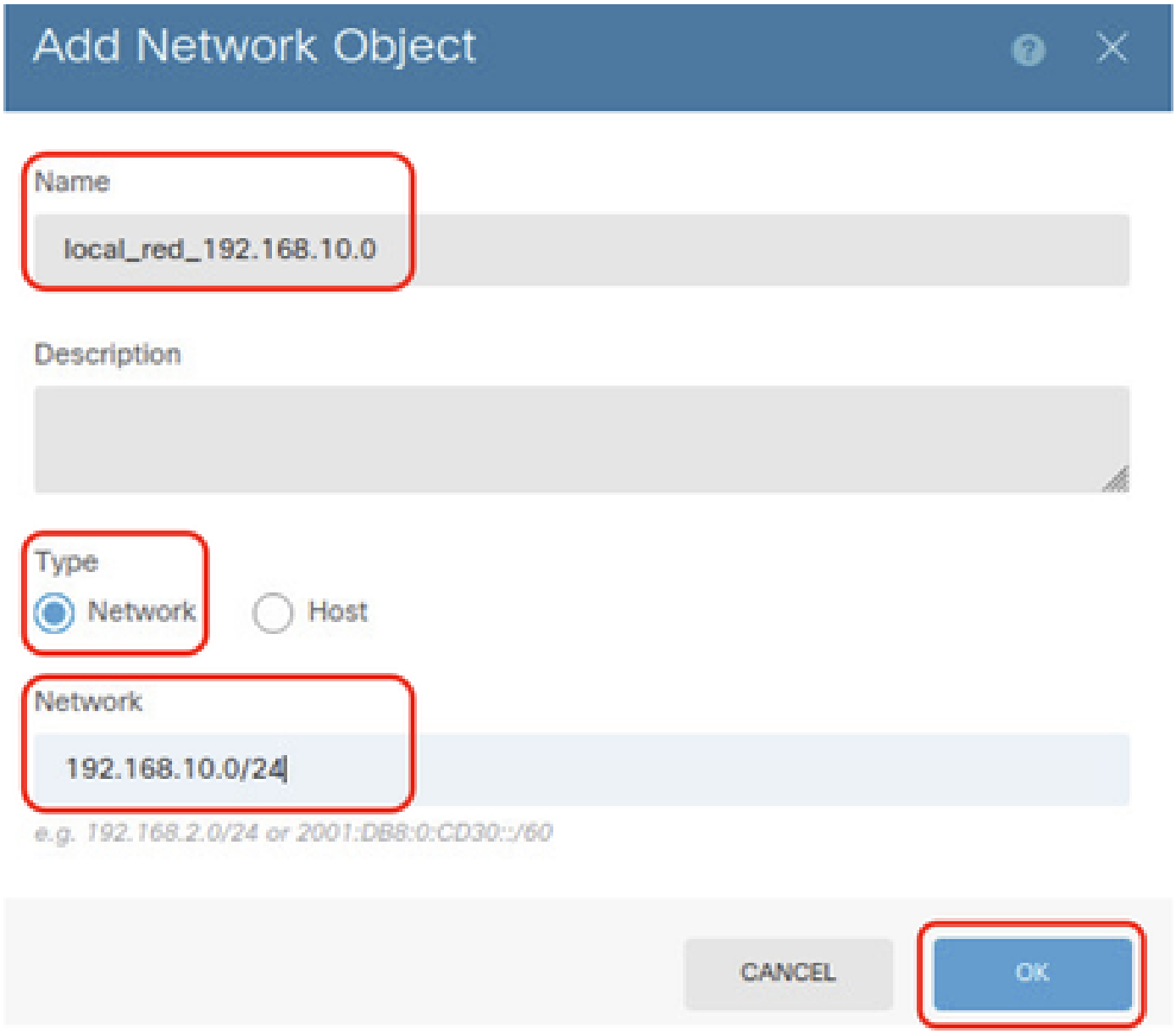
Paso 4.2. Proporcionar la información necesaria de cada objeto de red. Haga clic en el botón Aceptar.

- Nombre: local_blue_192.168.20.0
- Tipo: Red
- Red: 192.168.20.0/24



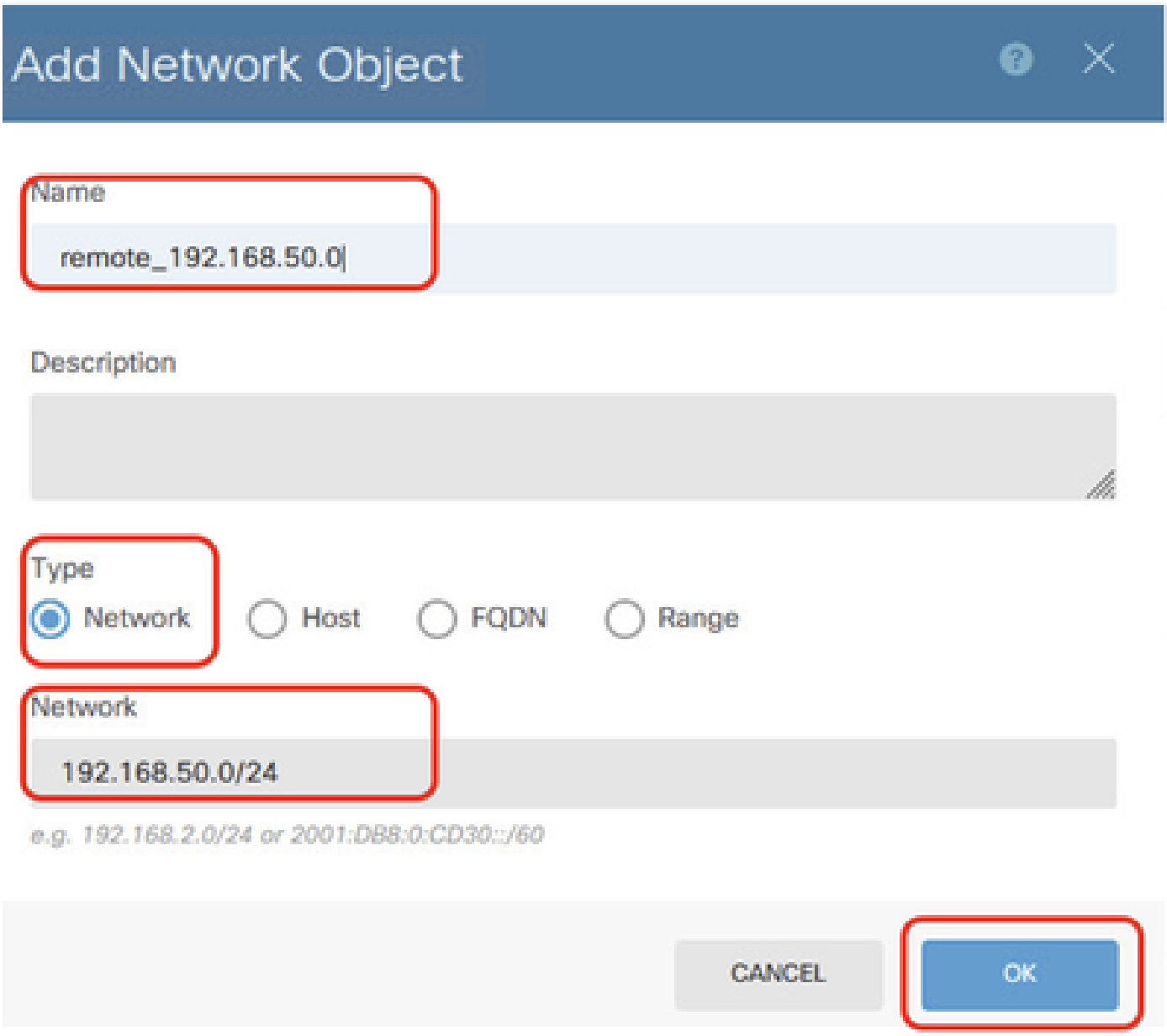
FTD_VRF_Blue_Network

- Nombre: local_red_192.168.10.0
- Tipo: Red
- Red: 192.168.10.0/24



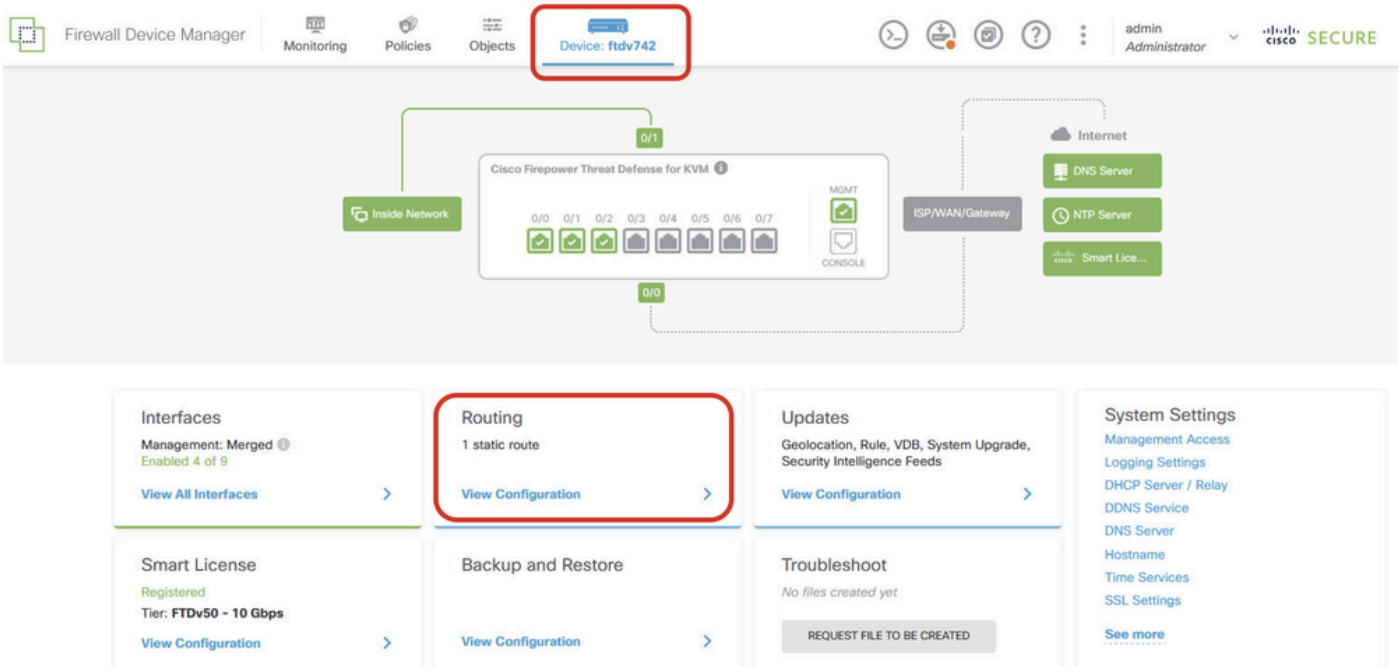
FTD_VRF_Red_Network

- Nombre: remote_192.168.50.0
- Tipo: Red
- Red: 192.168.50.0/24



FTD_Red_remota

Paso 4.3. Crear el primer router virtual. Vaya a Device > Routing . Haga clic en Ver configuración .



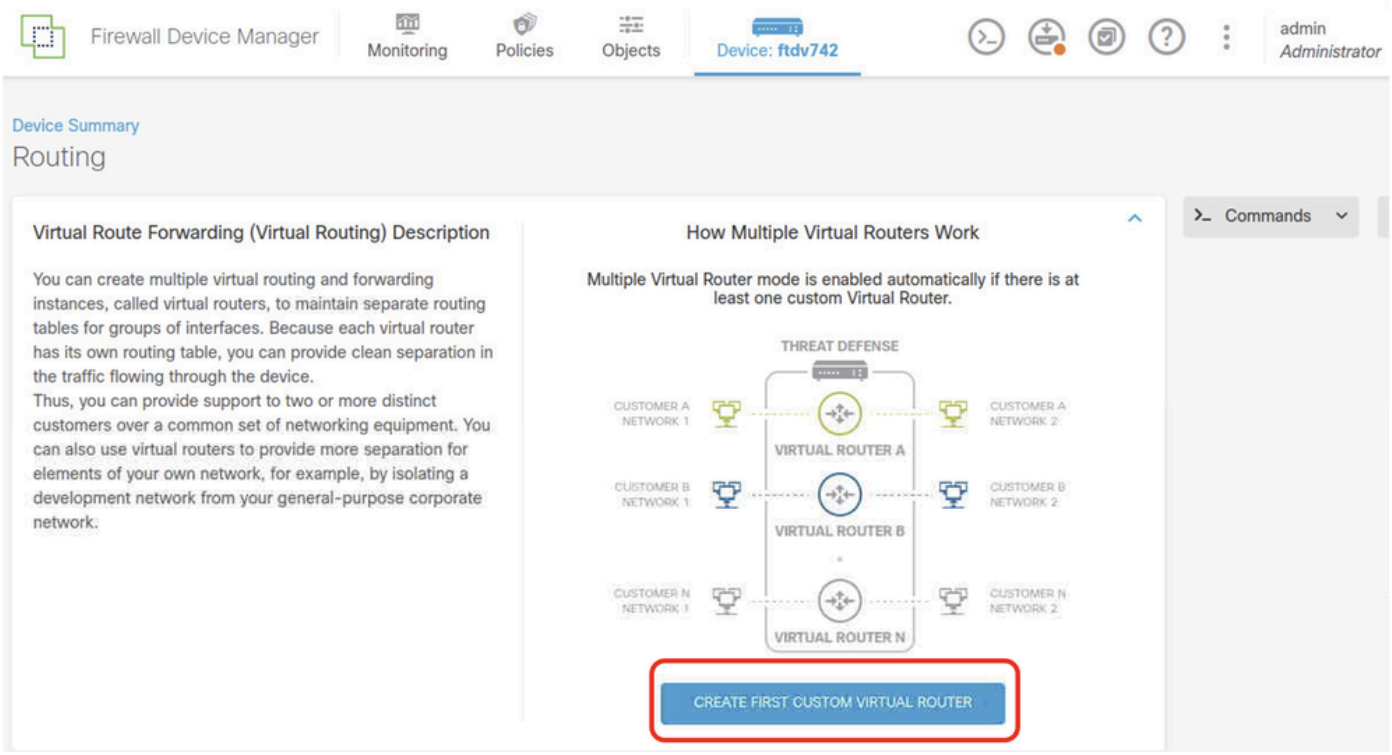
FTD_View_Routing_Configuration

Paso 4.4. Haga clic en Add Multiple Virtual Routers .

Nota: ya se ha configurado una ruta estática a través de la interfaz externa durante la inicialización de FDM. Si no lo tiene, configúrelo manualmente.

FTD_Add_First_Virtual_Router1

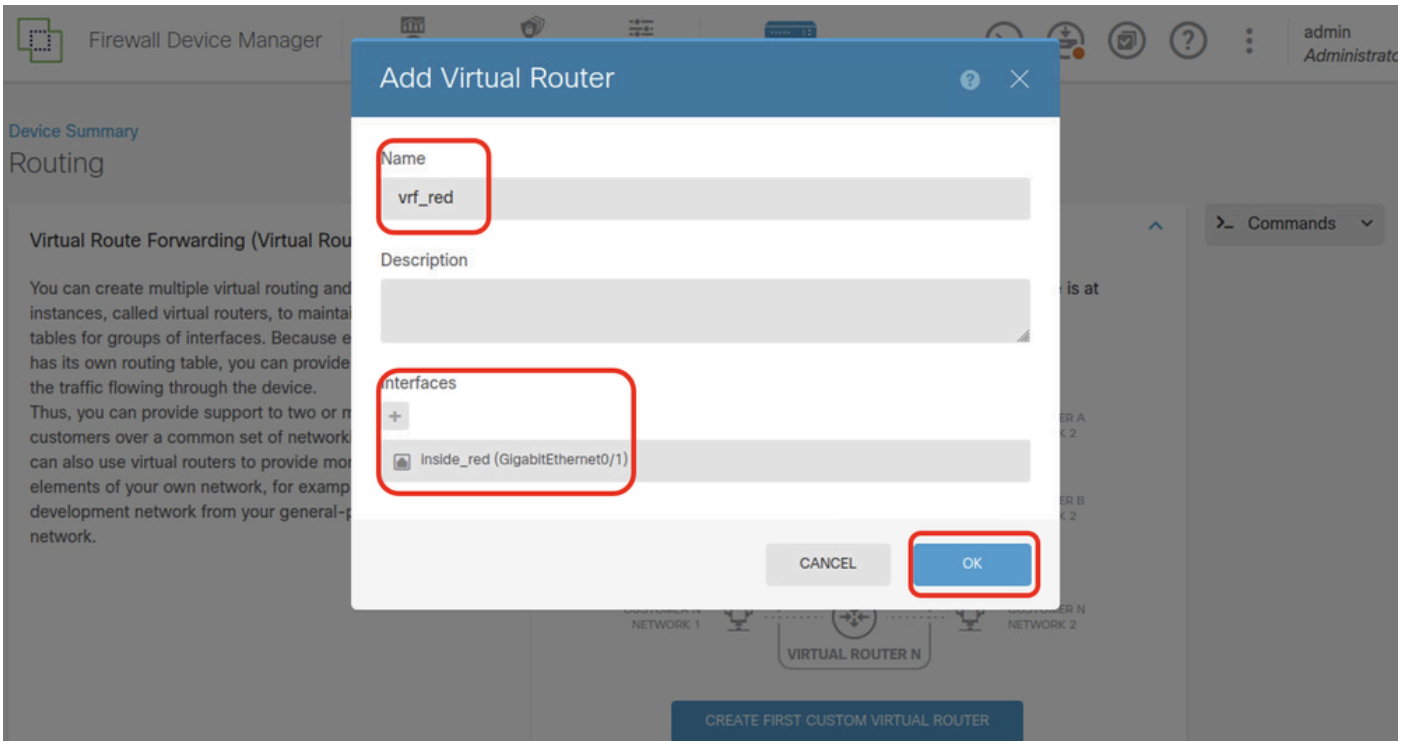
Paso 4.5. Haga clic en CREATE FIRST CUSTOM VIRTUAL ROUTER .



FTD_Add_First_Virtual_Router2

Paso 4.6. Proporcione la información necesaria del primer router virtual. Haga clic en el botón Aceptar. Después de la primera creación del router virtual, se mostrará automáticamente un nombre de vrf Global.

- Nombre: vrf_red
- Interfaces: inside_red (GigabitEthernet0/1)



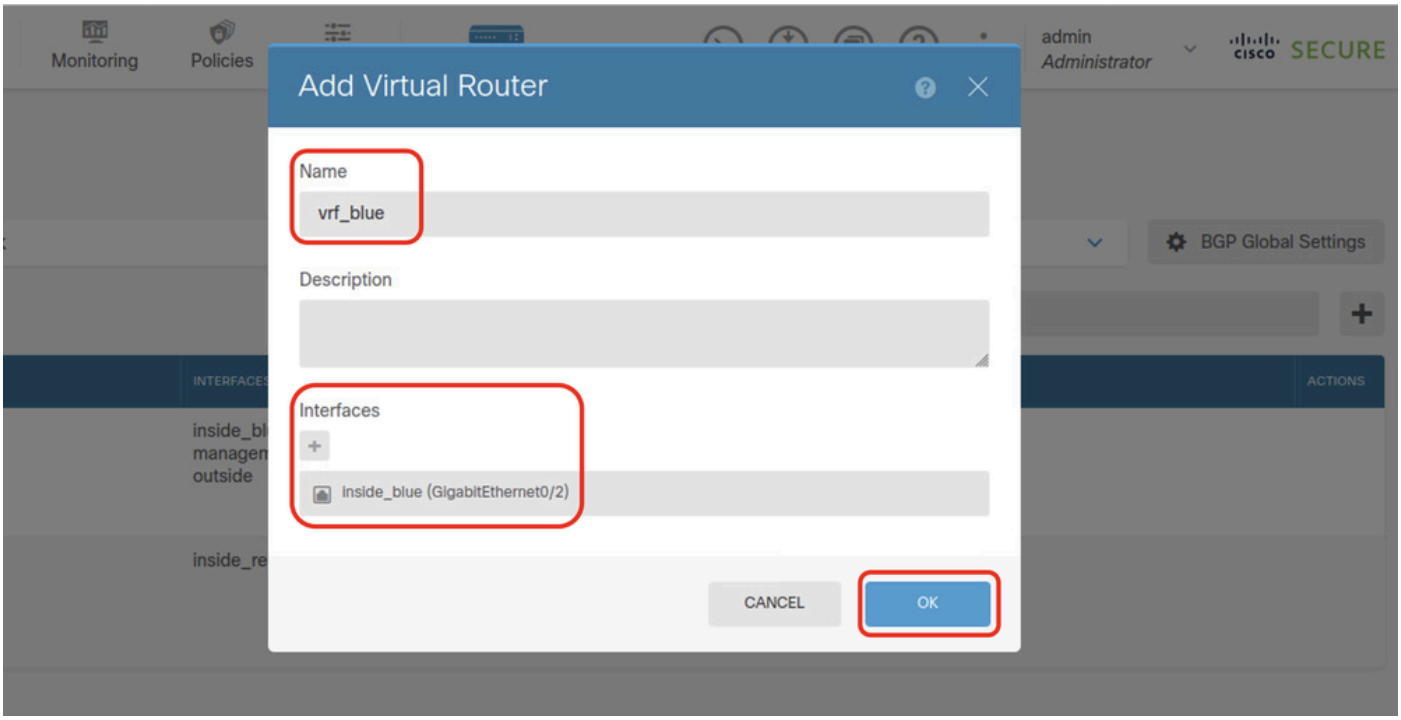
FTD_Add_First_Virtual_Router3

Paso 4.7. Cree un segundo router virtual. Navegue hasta Dispositivo > Enrutamiento. Haga clic en Ver configuración . Haga clic en el botón +.

FTD_Add_Second_Virtual_Router

Paso 4.8. Proporcione la información necesaria del segundo router virtual. Haga clic en el botón Aceptar

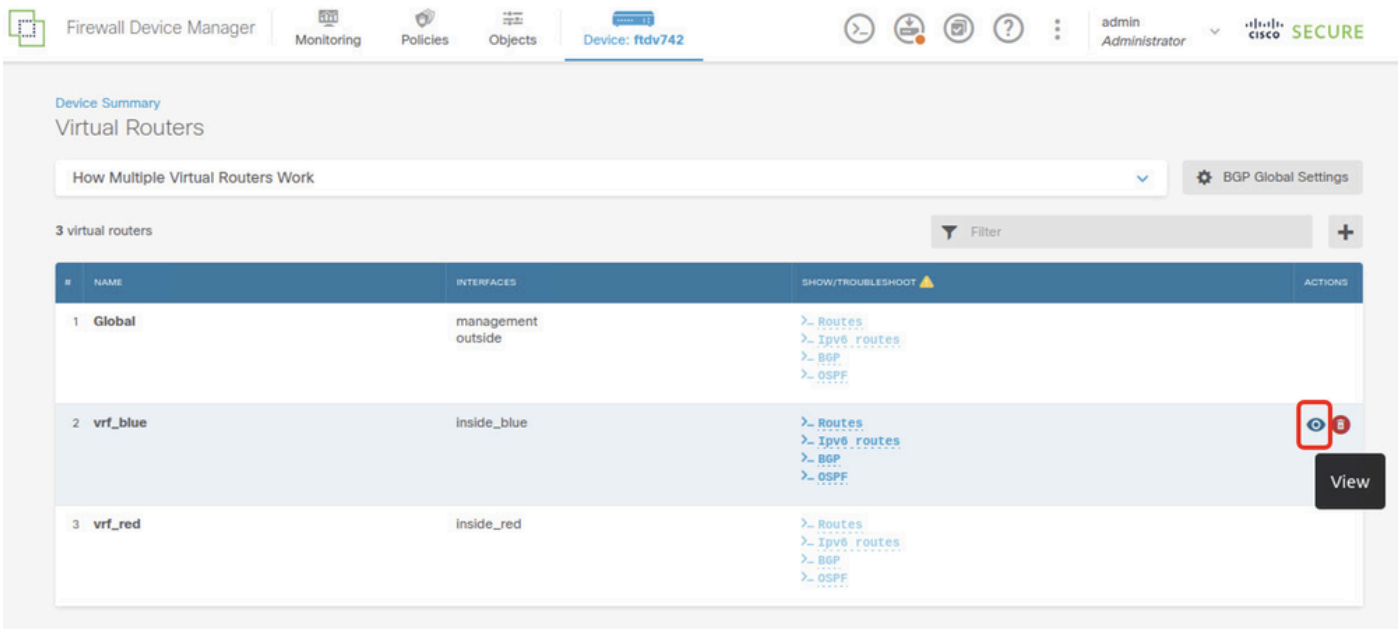
- Nombre: vrf_blue
- Interfaces: inside_blue (GigabitEthernet0/2)



FTD_Add_Second_Virtual_Router2

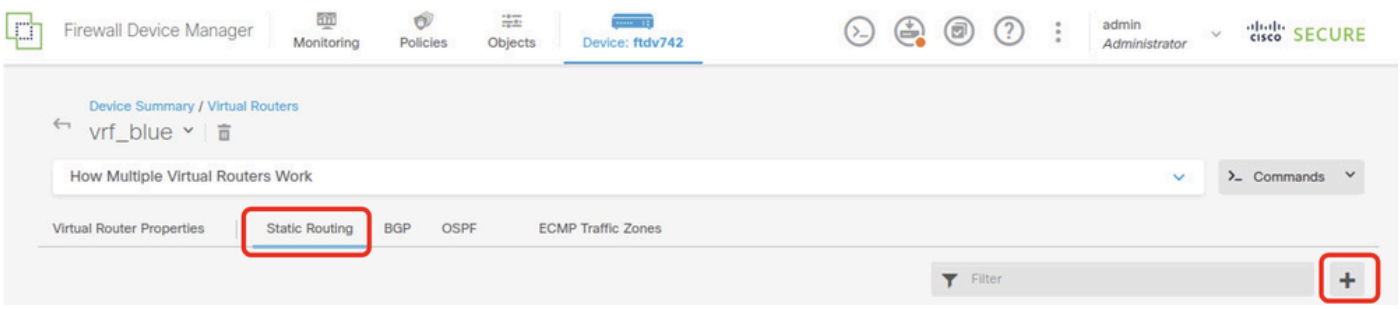
Paso 5. Cree una fuga de ruta de vrf_blue a Global. Esta ruta permite que los terminales de la red 192.168.20.0/24 inicien conexiones que atravesarían el túnel VPN de sitio a sitio. En este ejemplo, el extremo remoto protege la red 192.168.50.0/24.

Vaya a Device > Routing . Haga clic en Ver configuración. haga clic en el icono Ver en la celda Action del router virtual vrf_blue.



FTD_View_VRF_Blue

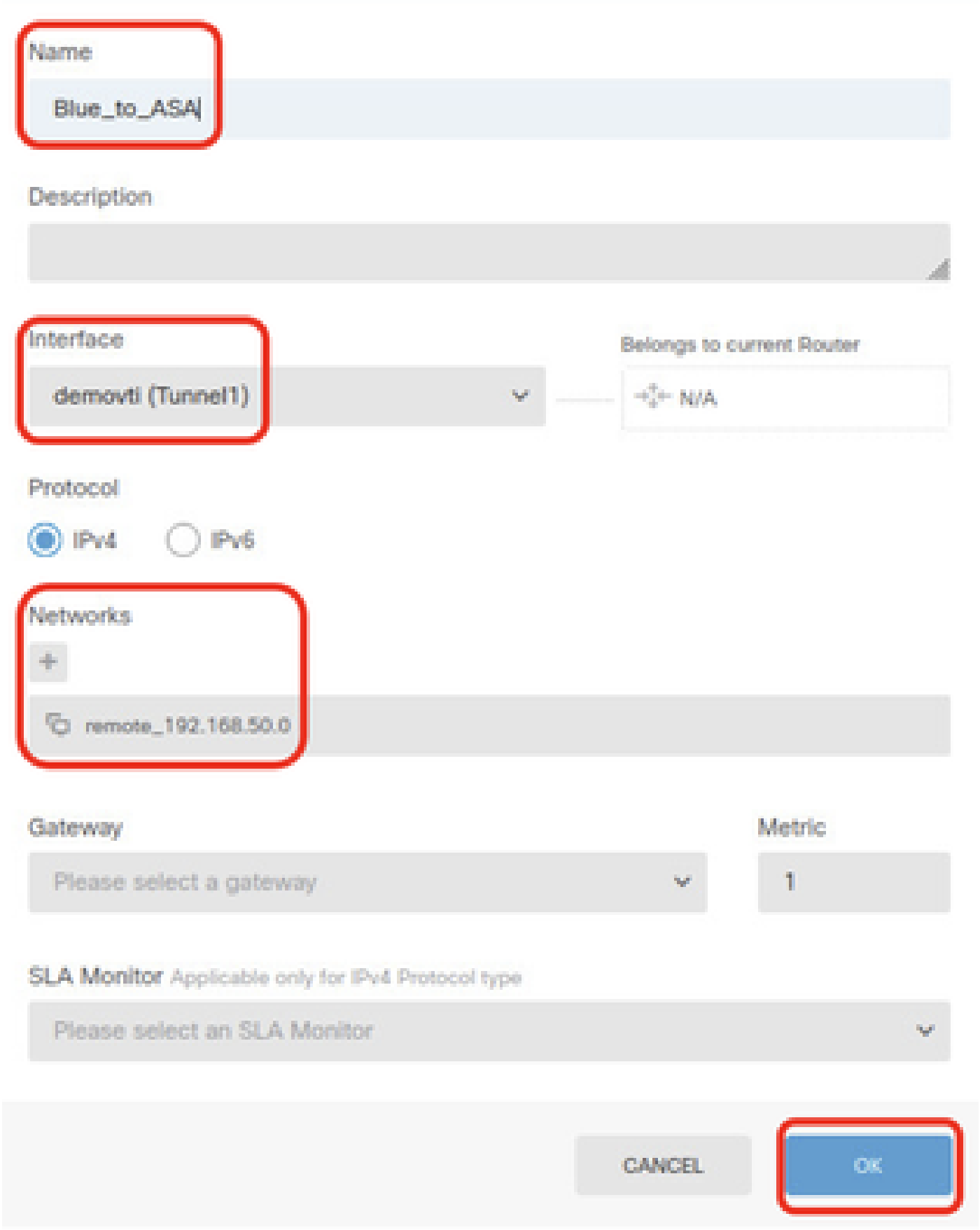
Paso 5.1. Haga clic en la pestaña Static Routing . Haga clic en el botón +.



FTD_Create_Static_Route_VRF_Blue

Paso 5.2. Proporcione la información necesaria. Haga clic en el botón Aceptar.

- Nombre: Azul_a_ASA
- Interfaz: demovti (Túnel1)
- Redes: remote_192.168.50.0
- Gateway: deje este elemento en blanco.

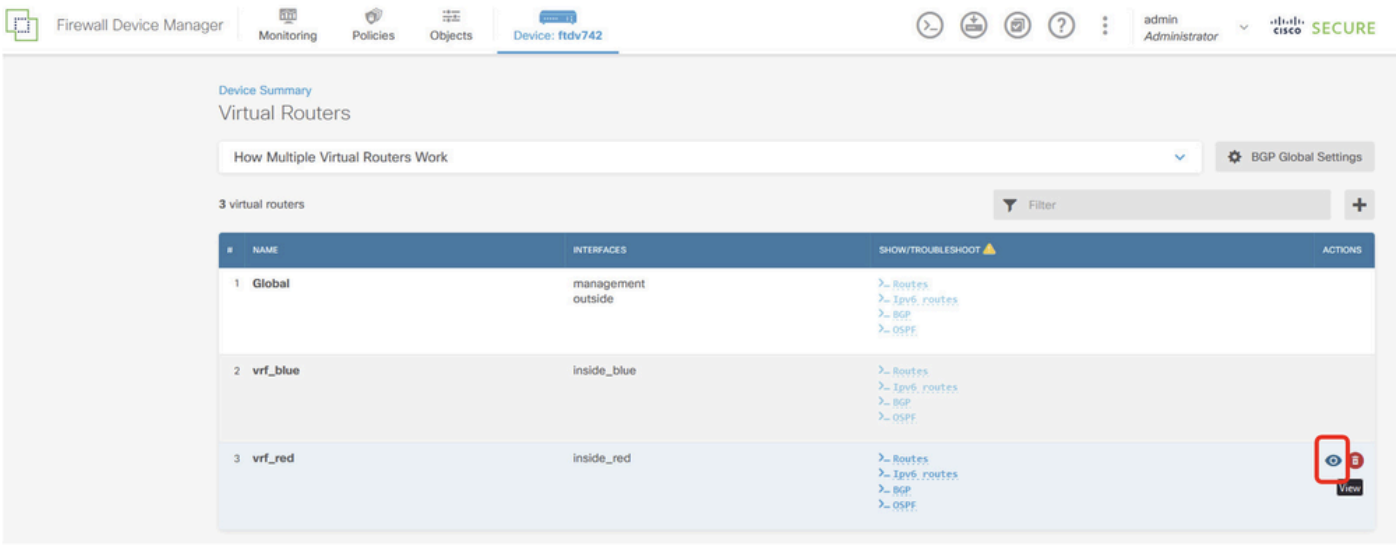


FTD_Create_Static_Route_VRF_Blue_Details

Paso 6. Cree una fuga de ruta de vrf_red a Global. Esta ruta permite que los terminales de la red 192.168.10.0/24 inicien conexiones que atravesarían el túnel VPN de sitio a sitio. En este

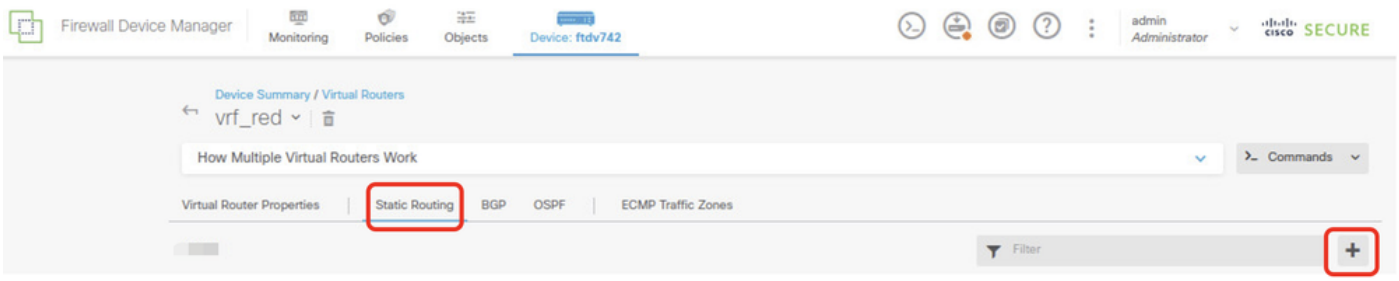
ejemplo, el extremo remoto protege la red 192.168.50.0/24.

Vaya a Device > Routing . Haga clic en Ver configuración. haga clic en el icono Ver en la celda Action del router virtual vrf_red.



FTD_View_VRF_Red

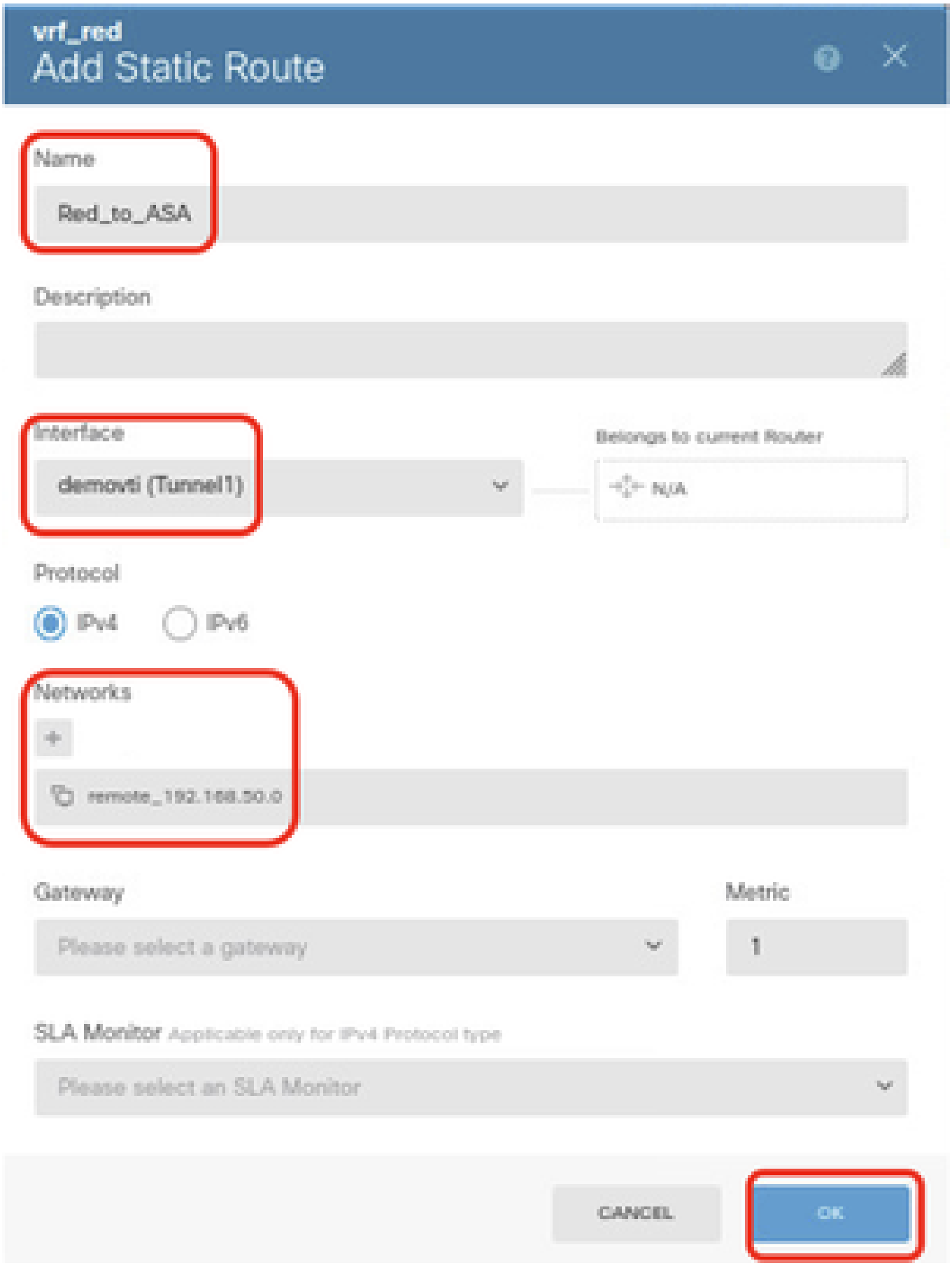
Paso 6.1. Haga clic en la pestaña Static Routing. Haga clic en el botón +.



FTD_Create_Static_Route_VRF_Red

Paso 6.2. Proporcione la información necesaria. Haga clic en el botón Aceptar.

- Nombre: Red_a_ASA
- Interfaz: demovti (Túnel1)
- Redes: remote_192.168.50.0
- Gateway: deje este elemento en blanco.

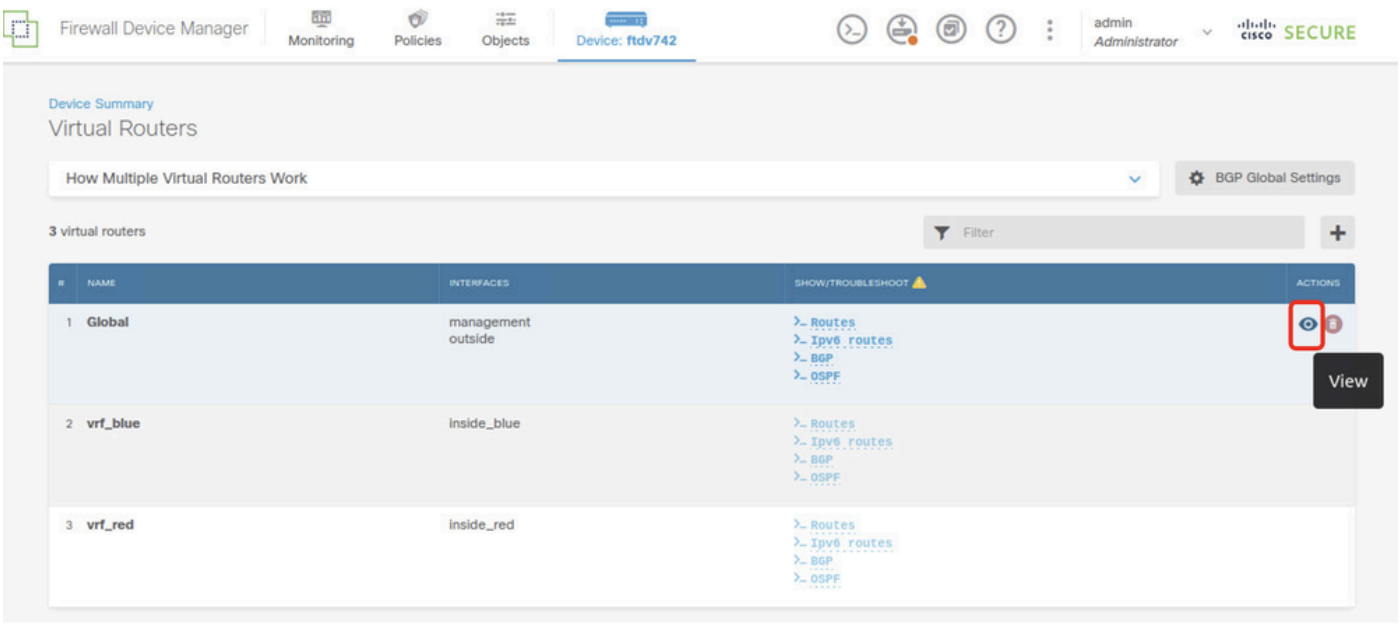


FTD_Create_Static_Route_VRF_Red_Details

Paso 7. Crear fuga de ruta de Global a routers virtuales. Las rutas permiten que los terminales protegidos por el extremo remoto de la VPN de sitio a sitio accedan a la red 192.168.10.0/24 en el

router virtual vrf_red y a la red 192.168.20.0/24 en el router virtual vrf_blue.

Vaya a Device > Routing . Haga clic en Ver configuración . haga clic en el icono Ver en la celda Acción del router virtual global.



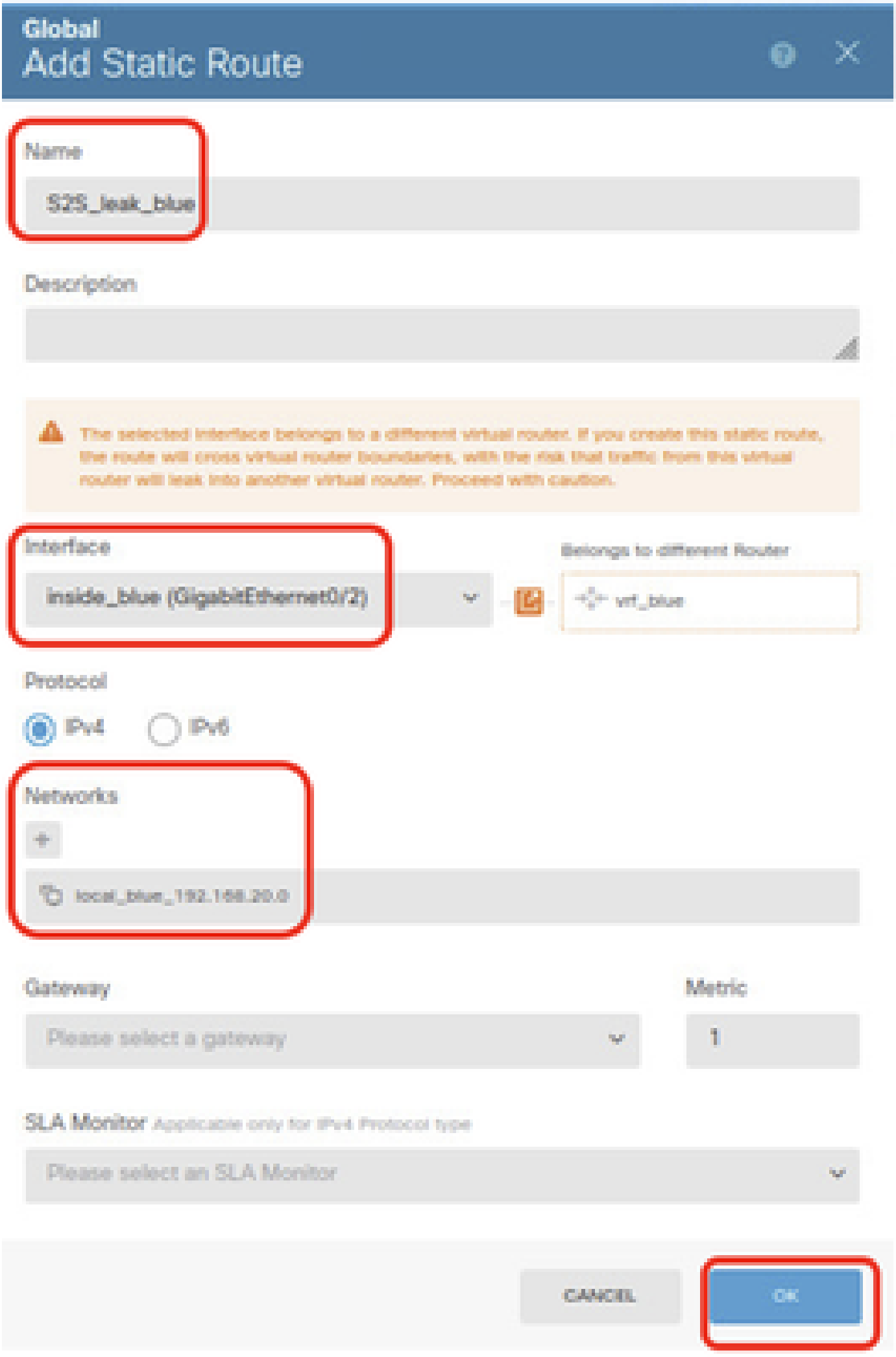
FTD_View_VRF_Global

Paso 7.1. Haga clic en la pestaña Static Routing. Haga clic en el botón +.

FTD_Create_Static_Route_VRF_Global

Paso 7.2. Proporcione la información necesaria. Haga clic en el botón Aceptar.

- Nombre: S2S_leak_blue
- Interfaz: inside_blue (GigabitEthernet0/2)
- Redes: local_blue_192.168.20.0
- Gateway: deje este elemento en blanco.


Global
Add Static Route
Name
S2S_leak_blue
Description
The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.
Interface
inside_blue (GigabitEthernet0/2)
Belongs to different Router
vrf_blue
Protocol
IPv4
IPv6
Networks
local_blue_192.168.20.0
Gateway
Please select a gateway
Metric
1
SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor
CANCEL
OK

```
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 21 20 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

Paso 10. Cree una propuesta IKEv2 ipsec que defina los mismos parámetros configurados en el FTD.

<#root>

```
crypto ipsec ikev2 ipsec-proposal
```

AES-SHA

```
 protocol esp encryption aes-256 aes-192 aes
 protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

Paso 11. Crear un perfil IPSec, referencia propuesta de IPSec creada en el paso 10.

<#root>

```
crypto ipsec profile
```

demo_ipsec_profile

```
 set ikev2 ipsec-proposal
```

AES-SHA

```
 set security-association lifetime kilobytes 4608000
 set security-association lifetime seconds 28800
```

Paso 12. Cree una política de grupo que permita el protocolo IKEv2.

<#root>

```
group-policy
```

demo_gp_192.168.30.1

```
 internal
group-policy demo_gp_192.168.30.1 attributes
 vpn-tunnel-protocol ikev2
```

Paso 13. Cree un grupo de túnel para la dirección IP externa de FTD de peer, haciendo referencia

a la política de grupo creada en el Paso 12 y configuración de la misma clave previamente compartida con FTD (creada en el paso 3.7).

<#root>

```
tunnel-group 192.168.30.1 type ipsec-l2l
tunnel-group 192.168.30.1 general-attributes
 default-group-policy
```

demo_gp_192.168.30.1

```
tunnel-group 192.168.30.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

Paso 14. Habilite IKEv2 en la interfaz externa.

```
crypto ikev2 enable outside
```

Paso 15. Crear túnel virtual.

<#root>

```
interface Tunnel1
 nameif demovti_asa
 ip address 169.254.10.2 255.255.255.0
 tunnel source interface outside
 tunnel destination 192.168.30.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile
```

demo_ipsec_profile

Paso 16. Crear ruta estática.

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Navegue hasta la CLI de FTD y ASA a través de la consola o SSH para verificar el estado de VPN de la fase 1 y la fase 2 a través de los comandos show crypto ikev2 sa y show crypto ipsec sa .

FTD:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv742#
ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
 32157565 192.168.30.1/500                               192.168.40.1/500                        G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/67986 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x4cf55637/0xa493cc83

ftdv742# show crypto ipsec sa
interface: demovti
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 192.168.40.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: A493CC83
      current inbound spi : 4CF55637

    inbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16867)
```

```
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
    outbound esp sas:
      spi: 0xA493CC83 (2761149571)
        SA State: active
        transform: esp-aes-256 esp-sha-512-hmac no compression
        in use settings ={L2L, Tunnel, IKEv2, VTI, }
        slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
        sa timing: remaining key lifetime (kB/sec): (4285440/16867)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

ASA:

```
ASA9203# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
 26025779 192.168.40.1/500                                192.168.30.1/500                        G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/68112 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xa493cc83/0x4cf55637
ASA9203#
ASA9203# show cry
ASA9203# show crypto ipsec sa
interface: demovti_asa
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 192.168.30.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 4CF55637
```

```
      current inbound spi : A493CC83

    inbound esp sas:
      spi: 0xA493CC83 (2761149571)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4101120/16804)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16804)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Paso 2. Verifique la ruta de VRF y Global en FTD.

```
ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
SI       192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI       192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside


ftdv742# show route vrf vrf_blue


Routing Table: vrf_blue
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        192.168.20.0 255.255.255.0 is directly connected, inside_blue
L        192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti


ftdv742# show route vrf vrf_red


Routing Table: vrf_red
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        192.168.10.0 255.255.255.0 is directly connected, inside_red
L        192.168.10.1 255.255.255.255 is directly connected, inside_red
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

Paso 3. Verifique la prueba de ping.

Antes de hacer ping, verifique los contadores de show crypto ipsec sa | inc interface:|encap|decap on FTD.

En este ejemplo, Tunnel1 muestra 30 paquetes tanto para encapsulación como para desencapsulación.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

El ping Cliente1 al Cliente3 se realizó correctamente.

```
Client1#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms
```

El ping Cliente2 al Cliente3 se realizó correctamente.

```
Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms
```

Compruebe los contadores de show crypto ipsec sa | inc interface:|encap|decap en FTD después de realizar un ping correctamente.

En este ejemplo, Tunnel1 muestra 40 paquetes para encapsulación y desencapsulación después de un ping exitoso. Además, ambos contadores aumentaron en 10 paquetes, coincidiendo con las solicitudes de eco de 10 ping, lo que indica que el tráfico de ping pasó correctamente a través del túnel IPSec.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
      #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Puede utilizar esos comandos debug para resolver problemas de la sección VPN.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

Puede utilizar esos comandos debug para resolver problemas de la sección route.

```
debug ip routing
```

Referencia

Guía de configuración de Cisco Secure Firewall Device Manager, versión 7.4

Guía de configuración CLI de VPN ASA de Cisco Secure Firewall, 9.20

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).