Configuración de VPN de sitio a sitio basada en ruta activa dual con PBR en FTD administrado por FDM

Contenido

Introducción

Este documento describe cómo configurar la VPN de sitio a sitio basada en ruta activa dual con PBR en FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de VPN
- Comprensión básica del routing basado en políticas (PBR)
- Comprensión básica del acuerdo de nivel de servicio del protocolo de Internet (IP SLA)
- 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

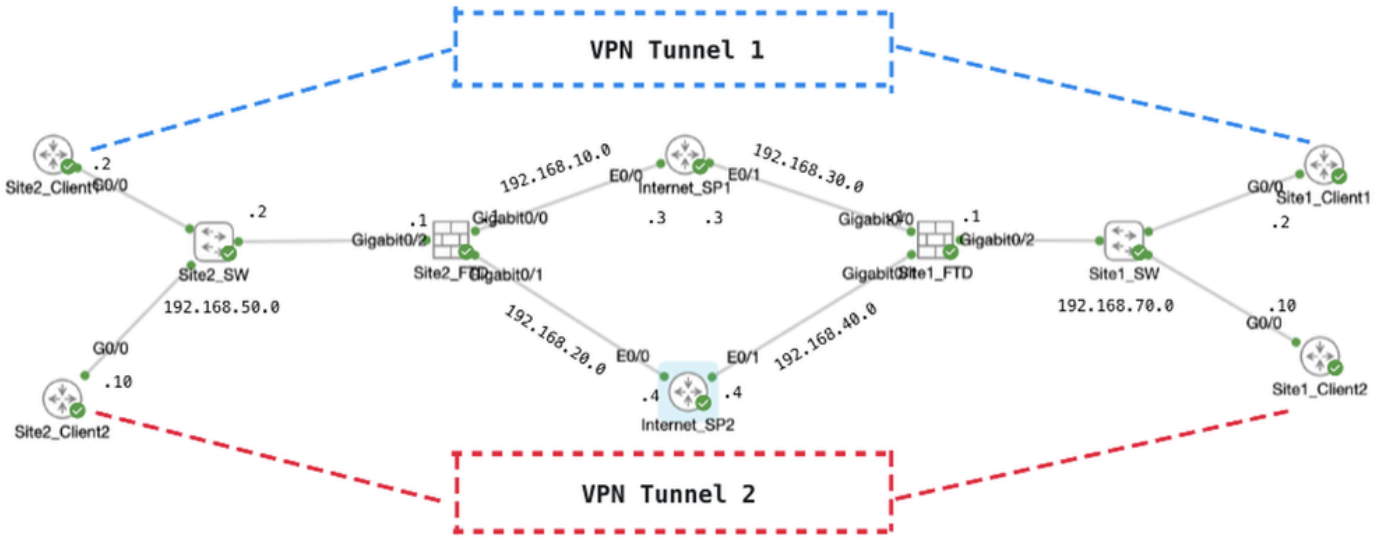
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Antecedentes

Este documento explica cómo configurar una VPN de sitio a sitio basada en ruta activa dual en FTD. En este ejemplo, los FTD en Site1 y Site2 tienen conexiones ISP activas duales que establecen la VPN de sitio a sitio con ambos ISP simultáneamente. De forma predeterminada, el tráfico VPN atraviesa el túnel 1 a través de ISP1 (línea azul). Para hosts específicos, el tráfico pasa por el túnel 2 a través de ISP2 (línea roja). Si el ISP1 experimenta una interrupción, el tráfico cambia al ISP2 como respaldo. Por el contrario, si el ISP2 experimenta una interrupción, el tráfico cambia al ISP1 como respaldo. En este ejemplo se utilizan el routing basado en políticas (PBR) y el acuerdo de nivel de servicio del protocolo de Internet (IP SLA) para cumplir estos requisitos.

Configurar

Diagrama de la red



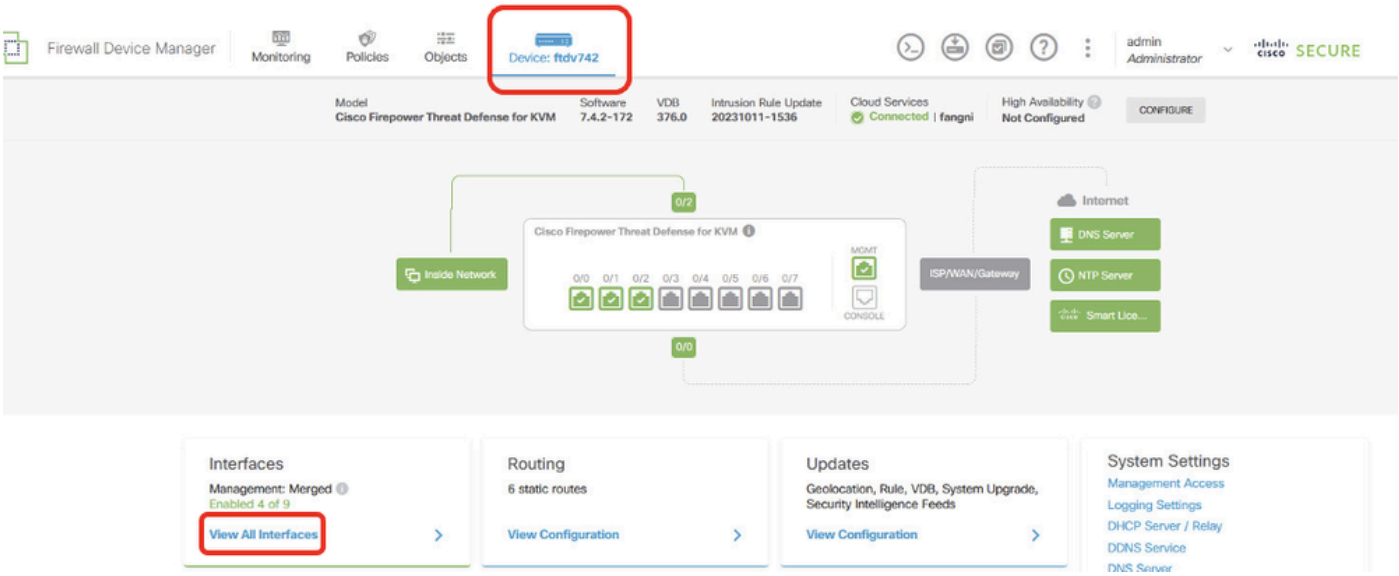
Topología

Configuraciones en VPN

Es esencial garantizar que la configuración preliminar de la interconectividad IP entre nodos se haya completado debidamente. Los clientes de Site1 y Site2 tienen la dirección IP interna de FTD como gateway.

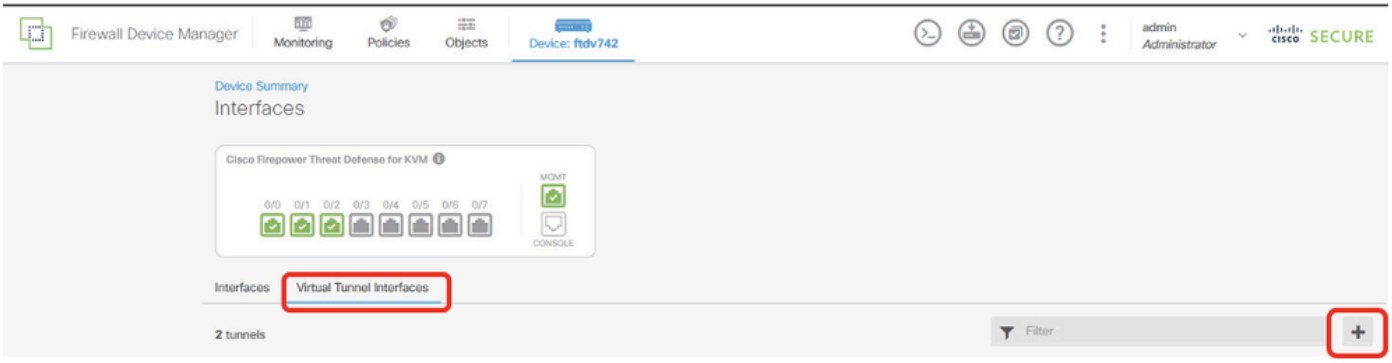
Configuración VPN FTD de Site1

Paso 1. Cree interfaces de túnel virtuales para ISP1 e ISP2. Inicie sesión en la GUI de FDM del FTD del sitio 1. Vaya a Dispositivo > Interfaces. Haga clic en Ver todas las interfaces.



Site1FTD_View_All_Interfaces

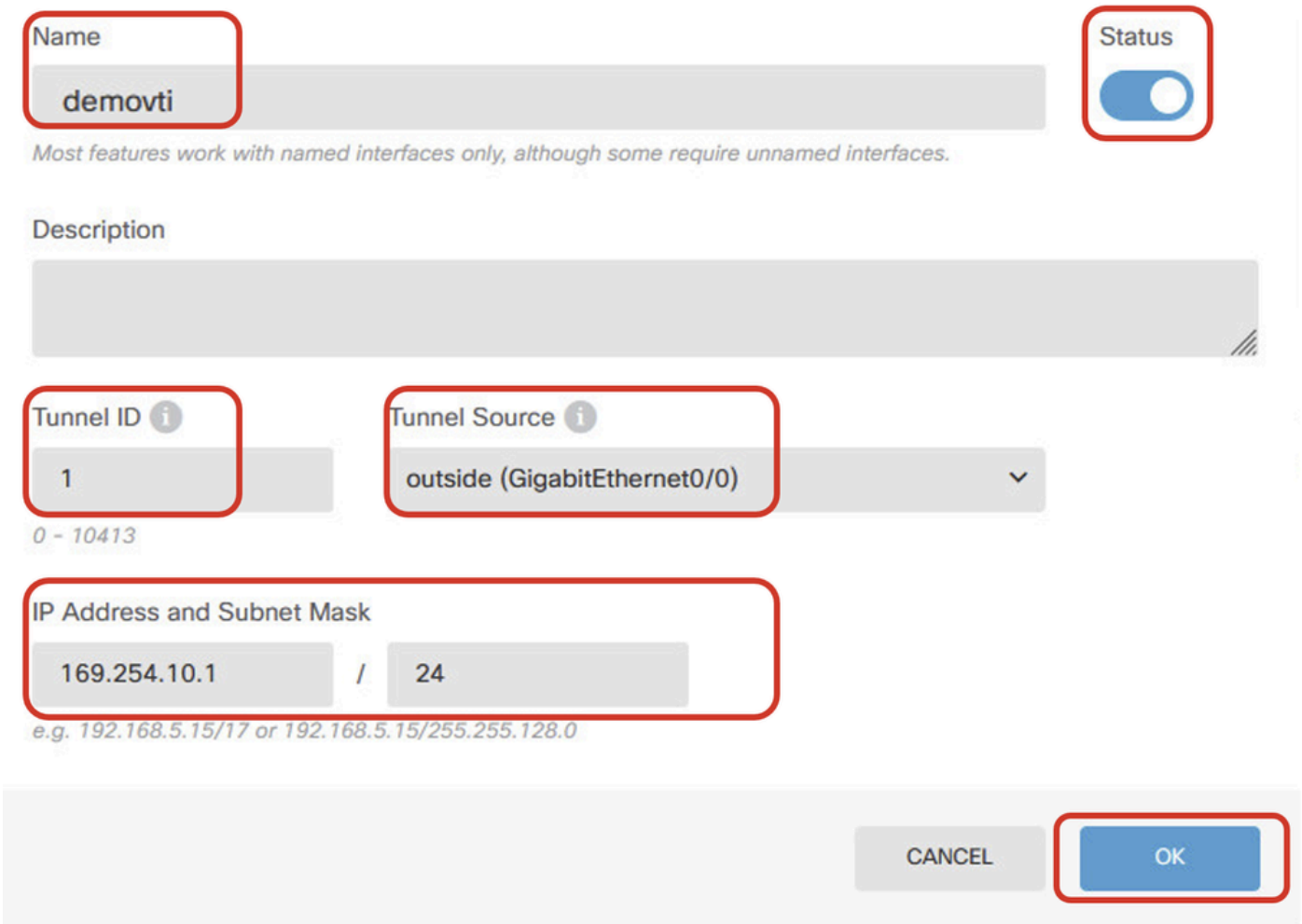
Paso 2. Haga clic en Interfaces de túnel virtual pestaña y luego el + botón.



Site1FTD_Create_VTI

Paso 3. Proporcione la información necesaria sobre los detalles de VTI. Haga clic en el botón Aceptar.

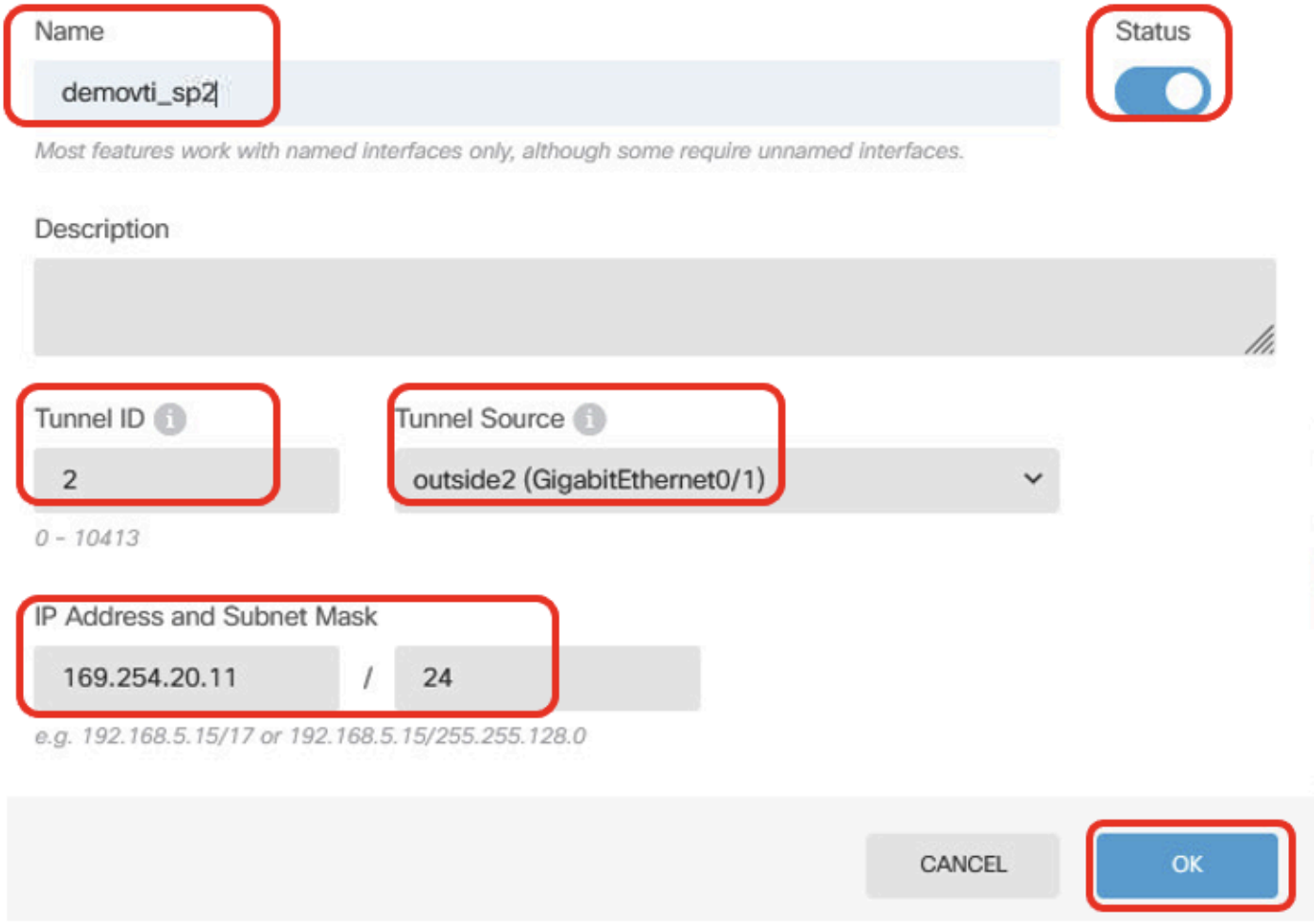
- Nombre: demovti
- ID de túnel: 1
- Origen del túnel: externa (GigabitEthernet0/0)
- Dirección IP y máscara de subred: 169.254.10.1/24
- Estado: haga clic en el control deslizante hasta la posición Activado



Site1FTD_VTI_Details_Tunnel1_ISP1

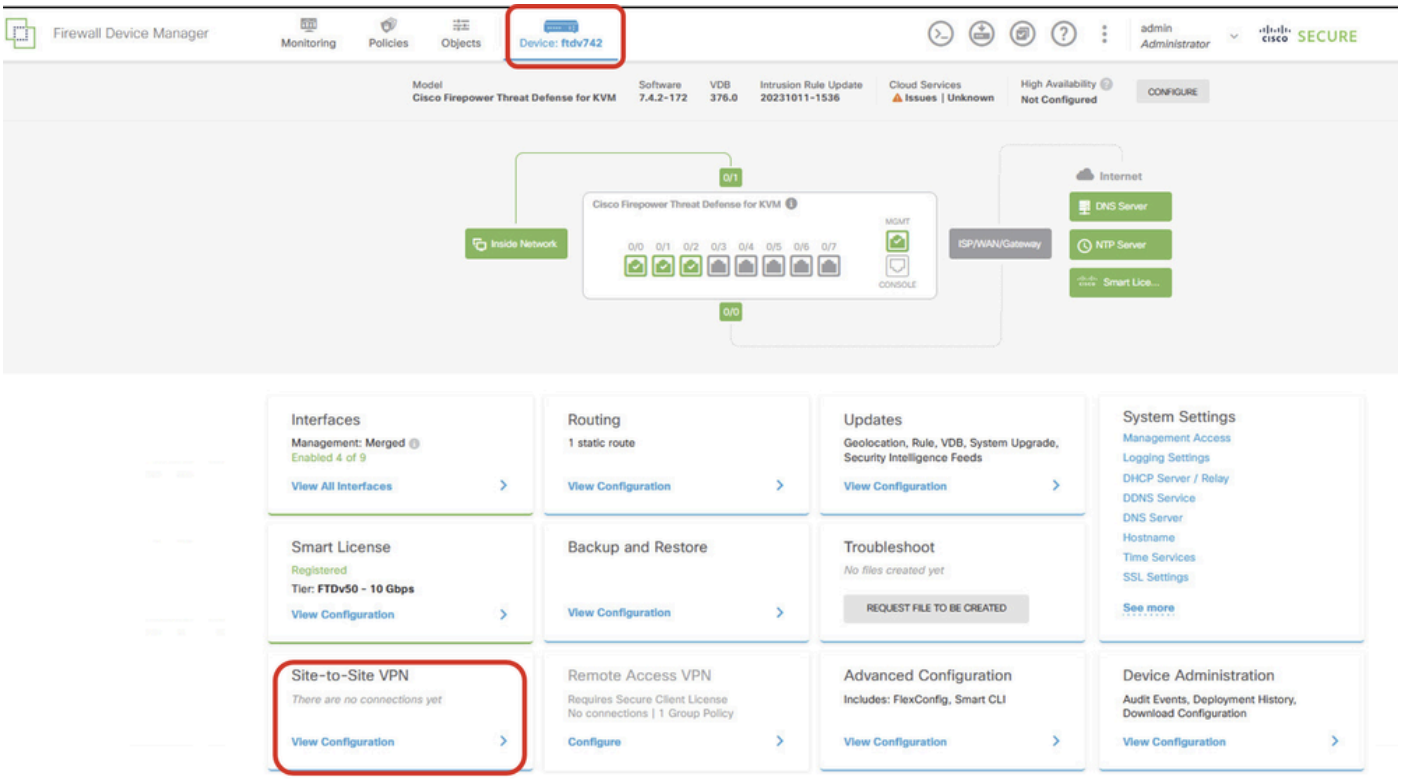
- Nombre: demovti_sp2

- ID de túnel: 2
- Origen del túnel: outside2 (GigabitEthernet0/1)
- Dirección IP y máscara de subred: 169.254.20.11/24
- Estado: haga clic en el control deslizante hasta la posición Activado



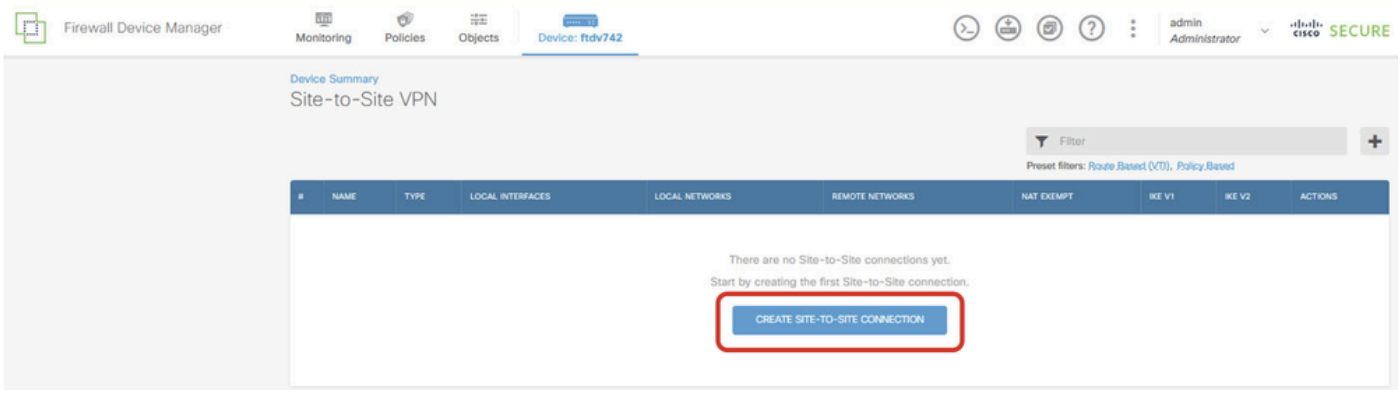
Site1FTD_VTI_Details_Tunnel2_ISP2

Paso 4. Navegue hasta Dispositivo > VPN de sitio a sitio. Haga clic en el botón View Configuration.



Site1FTD_View_Site2Site_VPN

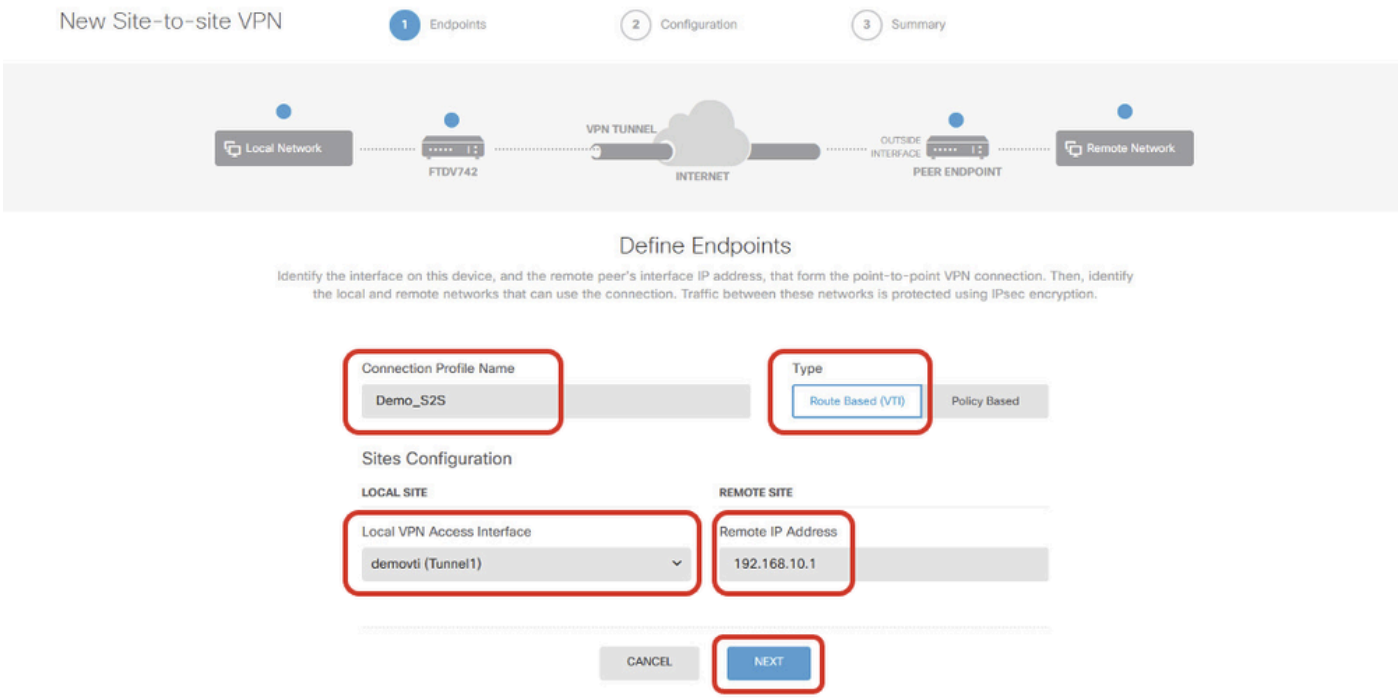
Paso 5. Comience a crear una nueva VPN de sitio a sitio a través de ISP1. Haga clic en el botón CREATE SITE-TO-SITE CONNECTION (CREAR CONEXIÓN DE SITIO A SITIO) o haga clic en el botón +.



Site1FTD_Create_Site-to-Site_Connection

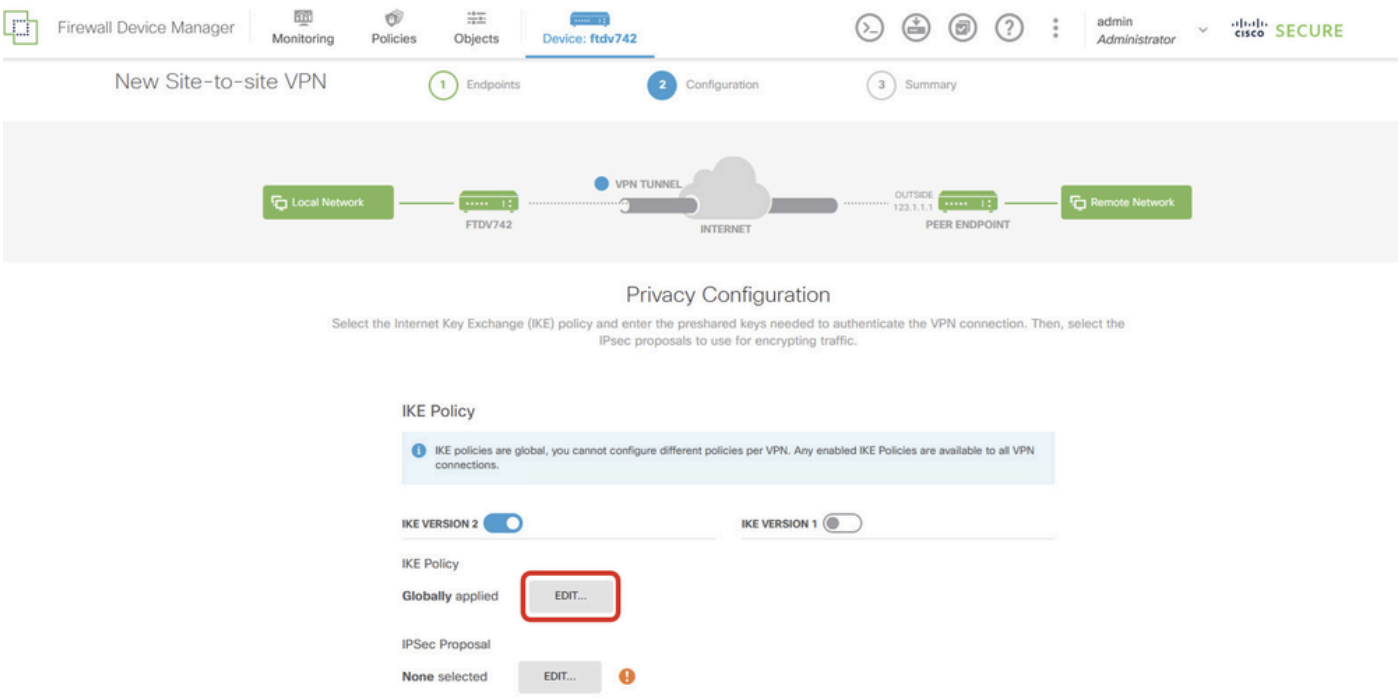
Paso 5.1. Proporcione la información necesaria de los terminales. Haga clic en el botón NEXT.

- Nombre del perfil de conexión: Demo_S2S
- Tipo: Basado en ruta (VTI)
- Interfaz de acceso VPN local: demovti (creado en el paso 3.0)
- Dirección IP remota: 192.168.10.1 (esta es la dirección IP ISP1 del FTD del sitio 2)



Site1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

Paso 5.2. Navegue hasta Política IKE. Haga clic en el botón EDIT.

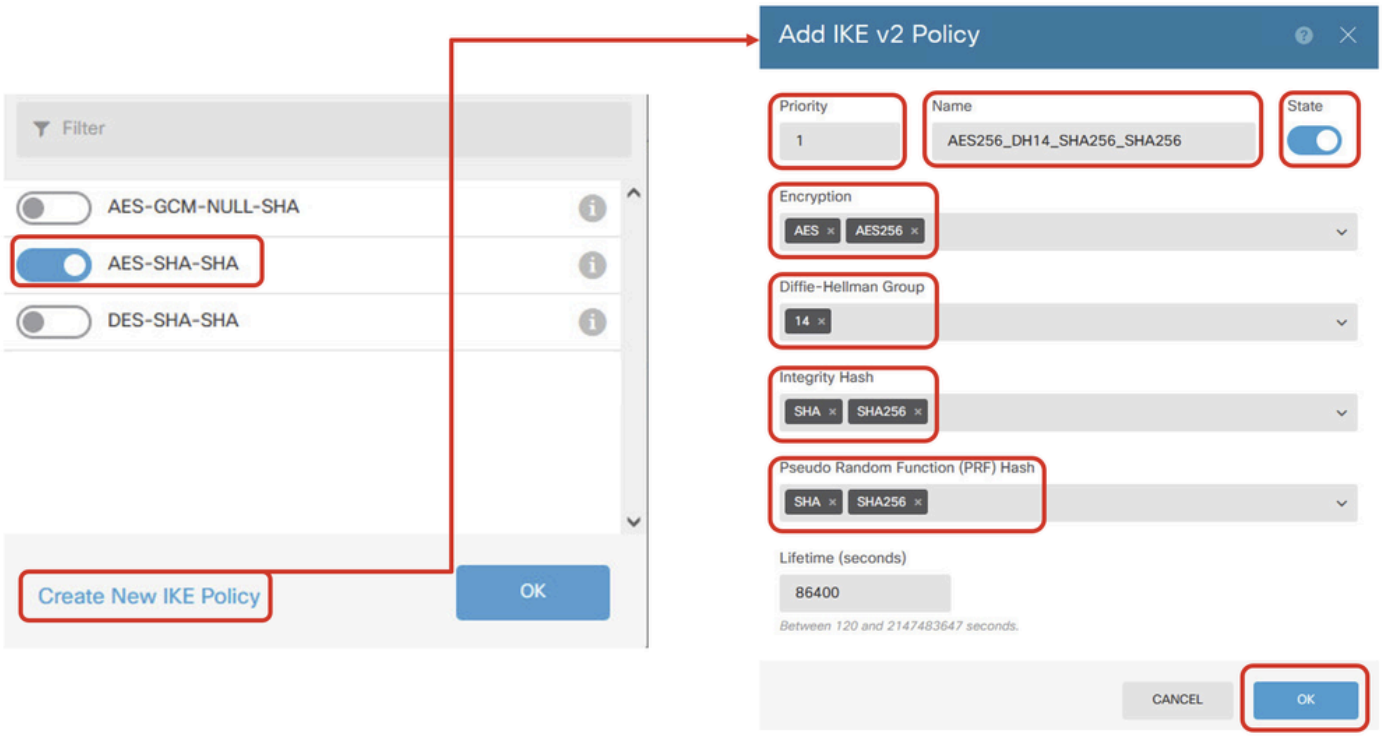


Site1FTD_Edit_IKE_Policy

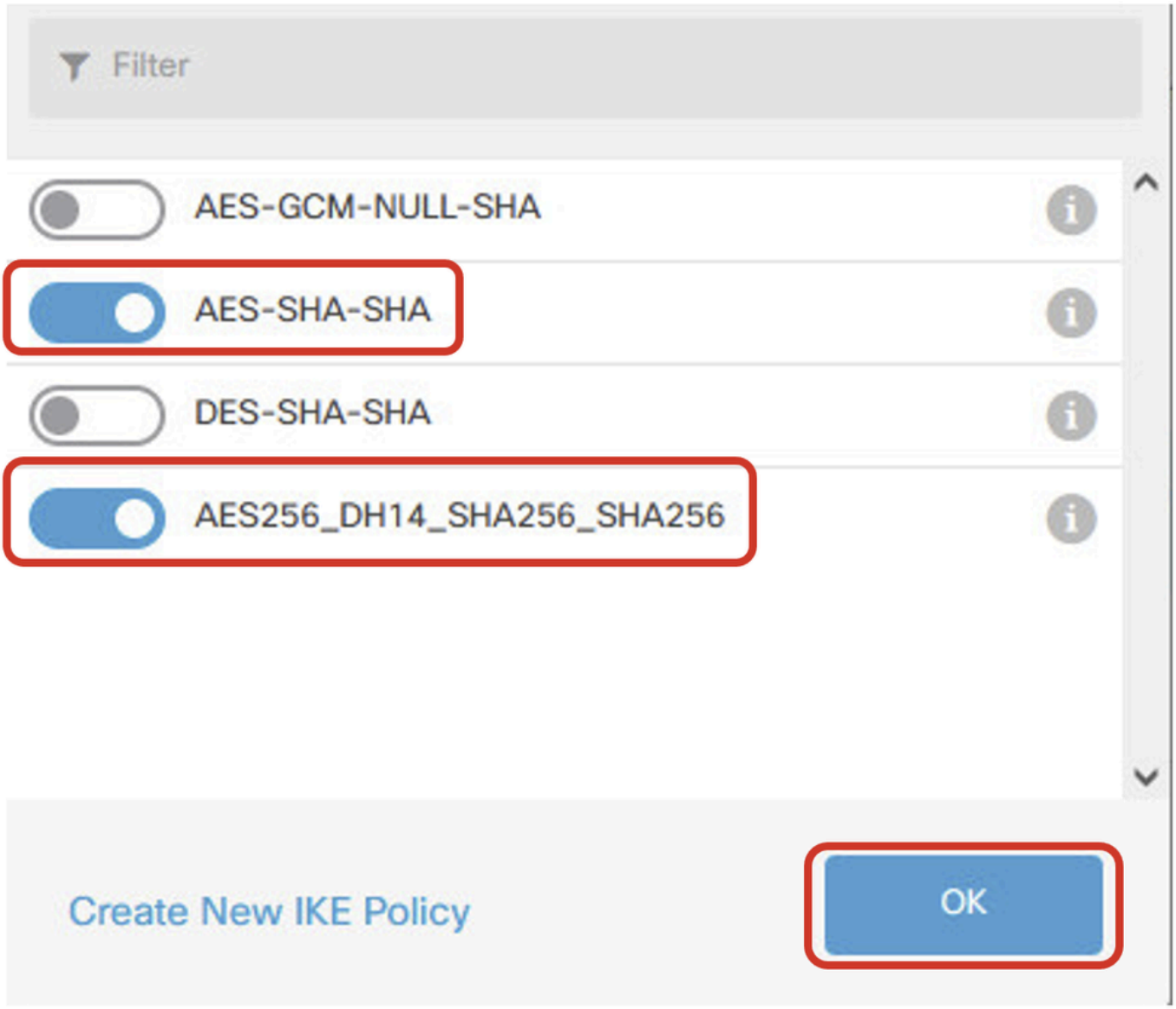
Paso 5.3. Para la política IKE, puede utilizar una predefinida o puede crear una nueva haciendo clic en Crear nueva política IKE.

En este ejemplo, alterne una política IKE existente AES-SHA-SHA y cree una nueva con fines de demostración. Haga clic en el botón OK para guardar.

- Nombre: AES256_DH14_SHA256_SHA256
- Cifrado: AES y AES256
- Grupo DH: 14
- Hash de integridad: SHA, SHA256
- Hash PRF: SHA, SHA256
- Vida útil: 86400 (default)

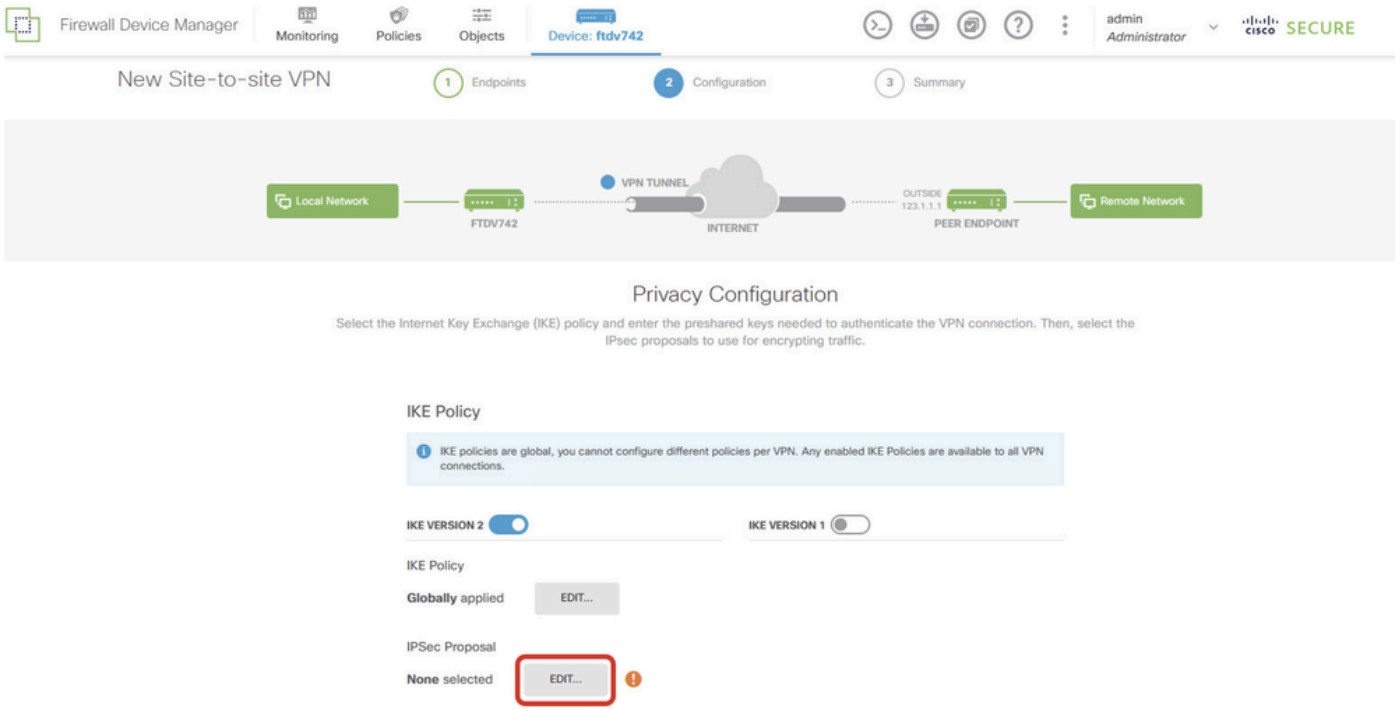


Site1FTD_Add_New_IKE_Policy



Site1FTD_Enable_New_IKE_Policy

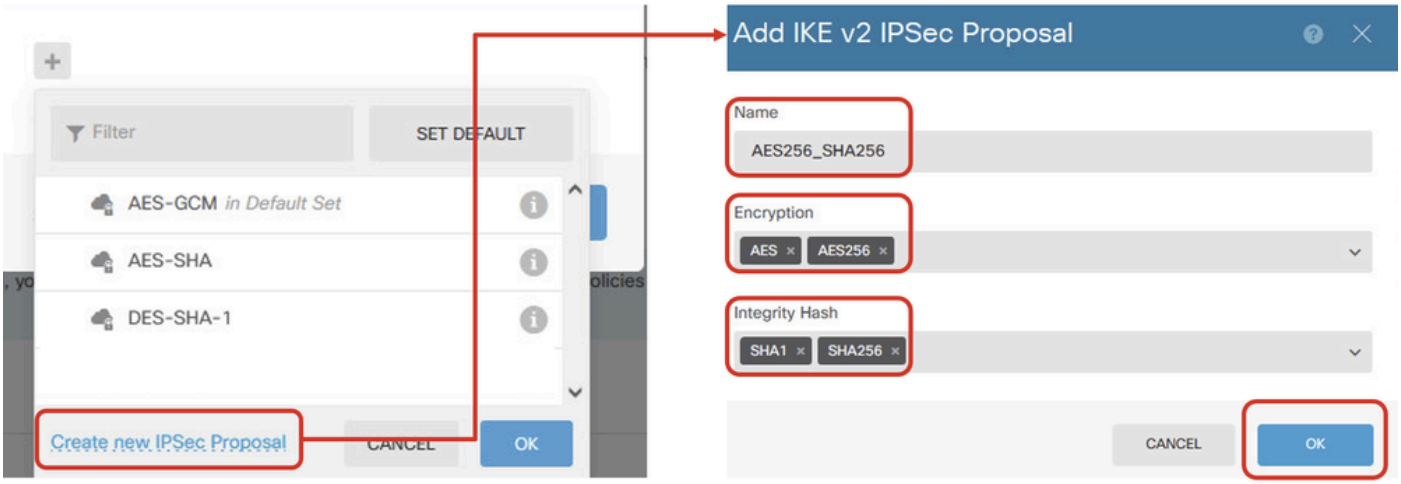
Paso 5.4. Vaya a Propuesta IPSec. Haga clic en el botón EDIT.



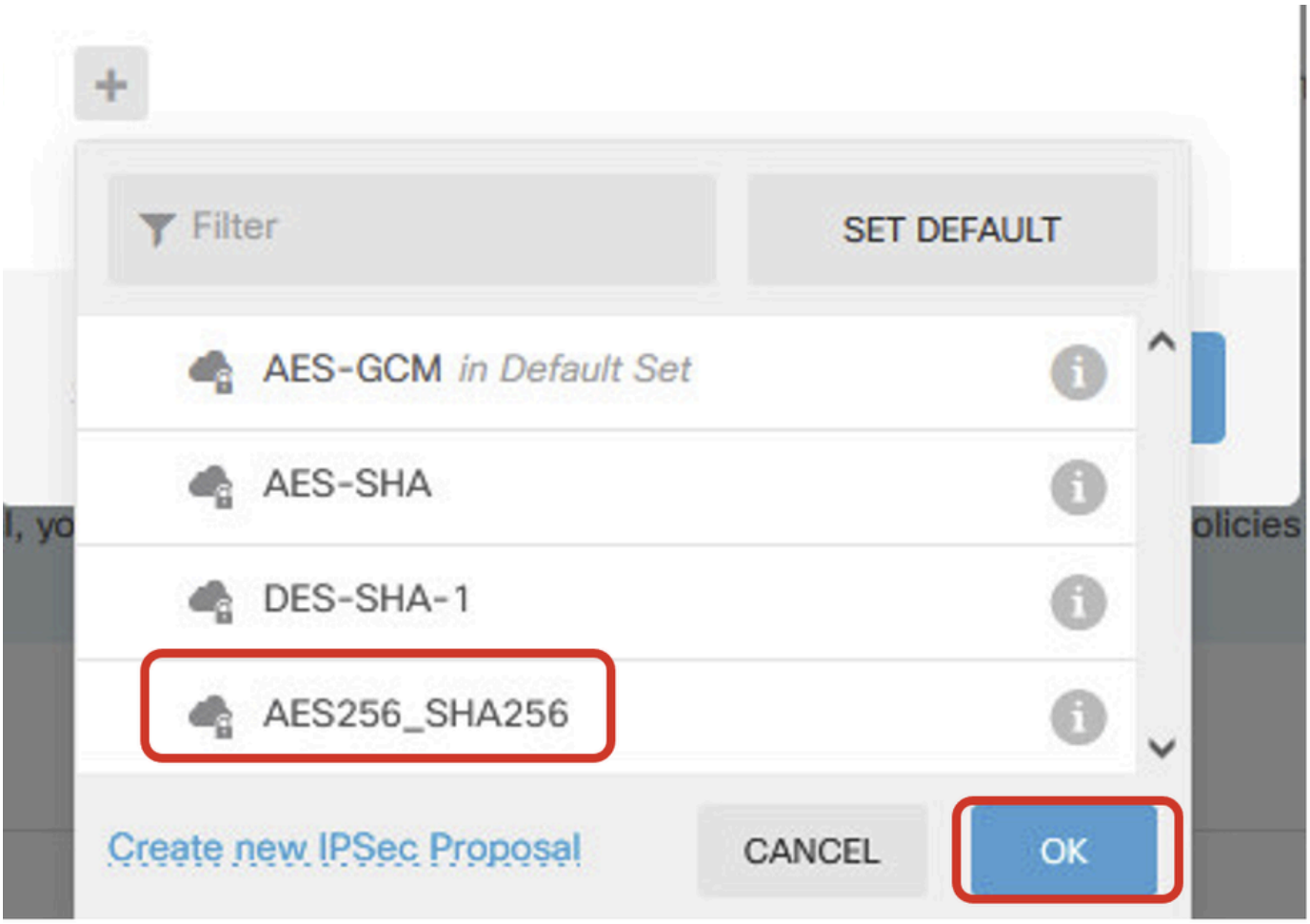
Site1FTD_Edit_IKE_Propuesta

Paso 5.5. 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, cree uno nuevo con fines de demostración. Haga clic en el botón OK para guardar.

- Nombre: AES256_SHA256
- Cifrado: AES y AES256
- Hash de integridad: SHA1, SHA256



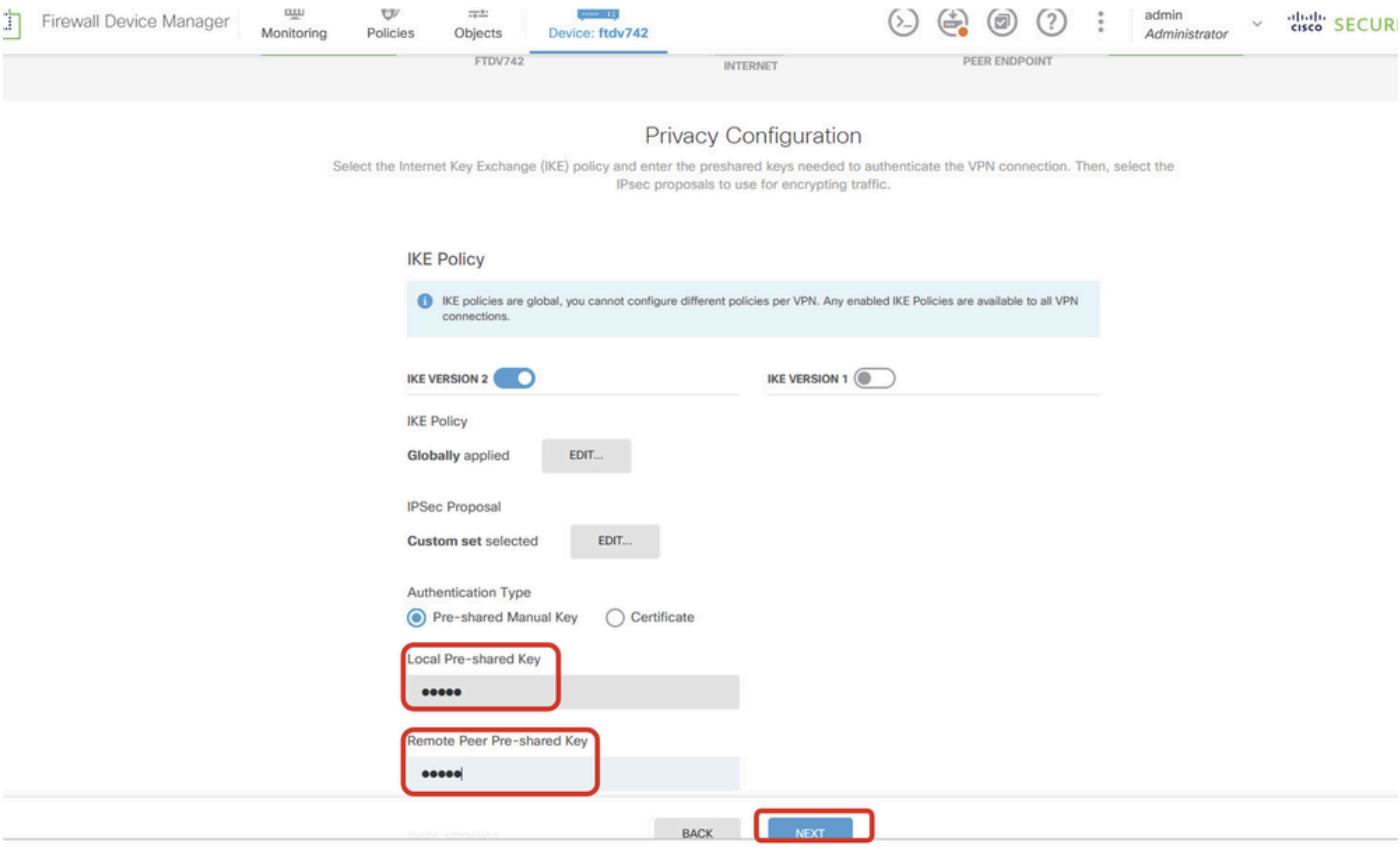
Site1FTD_Add_New_IKE_Propuesta



Site1FTD_Enable_New_IKE_Propuesta

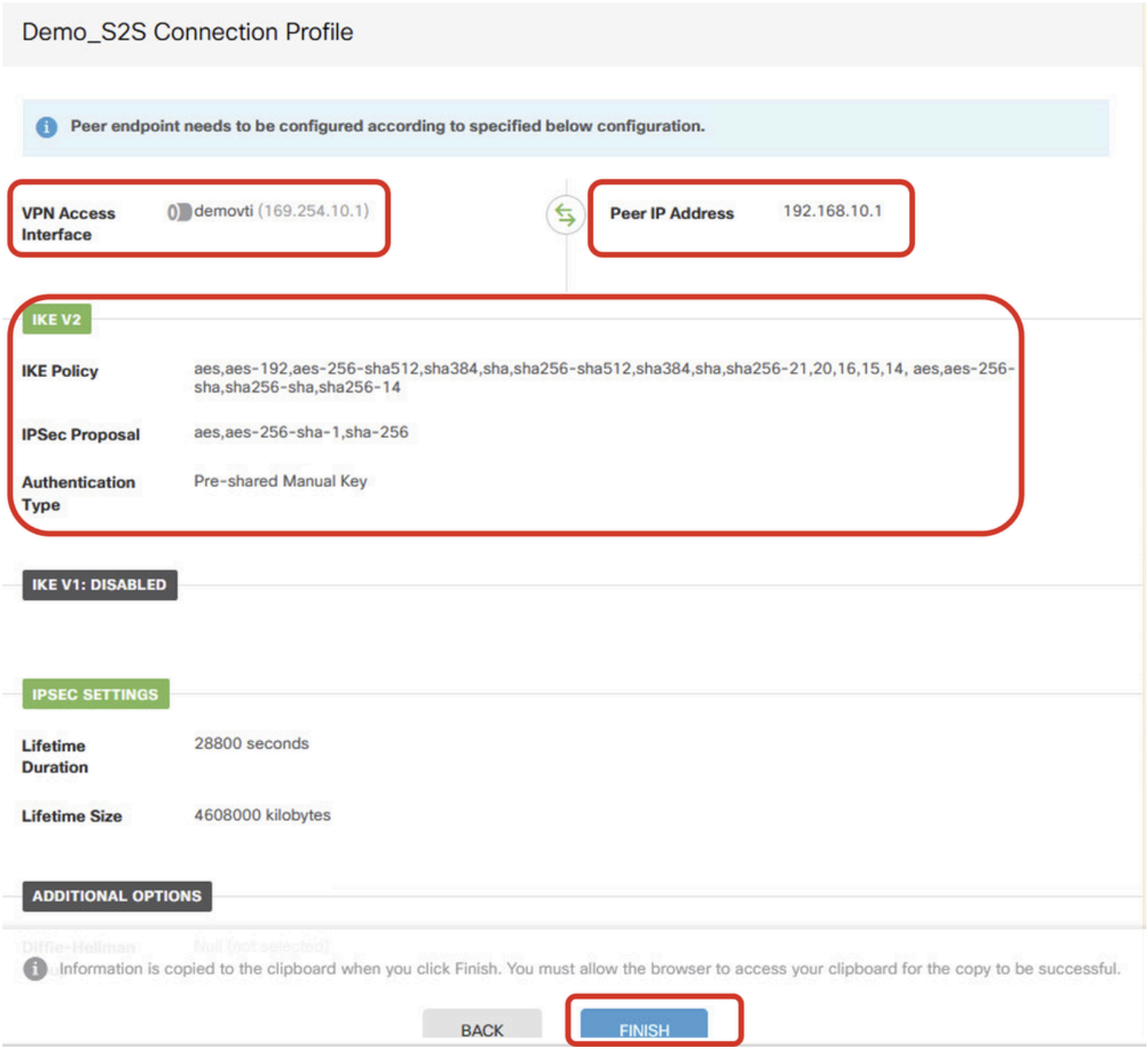
Paso 5.6. Desplácese por la página y configure la clave previamente compartida. Haga clic en el botónSIGUIENTE.

Anote esta clave precompartida y configúrela en el FTD Site2 más adelante.



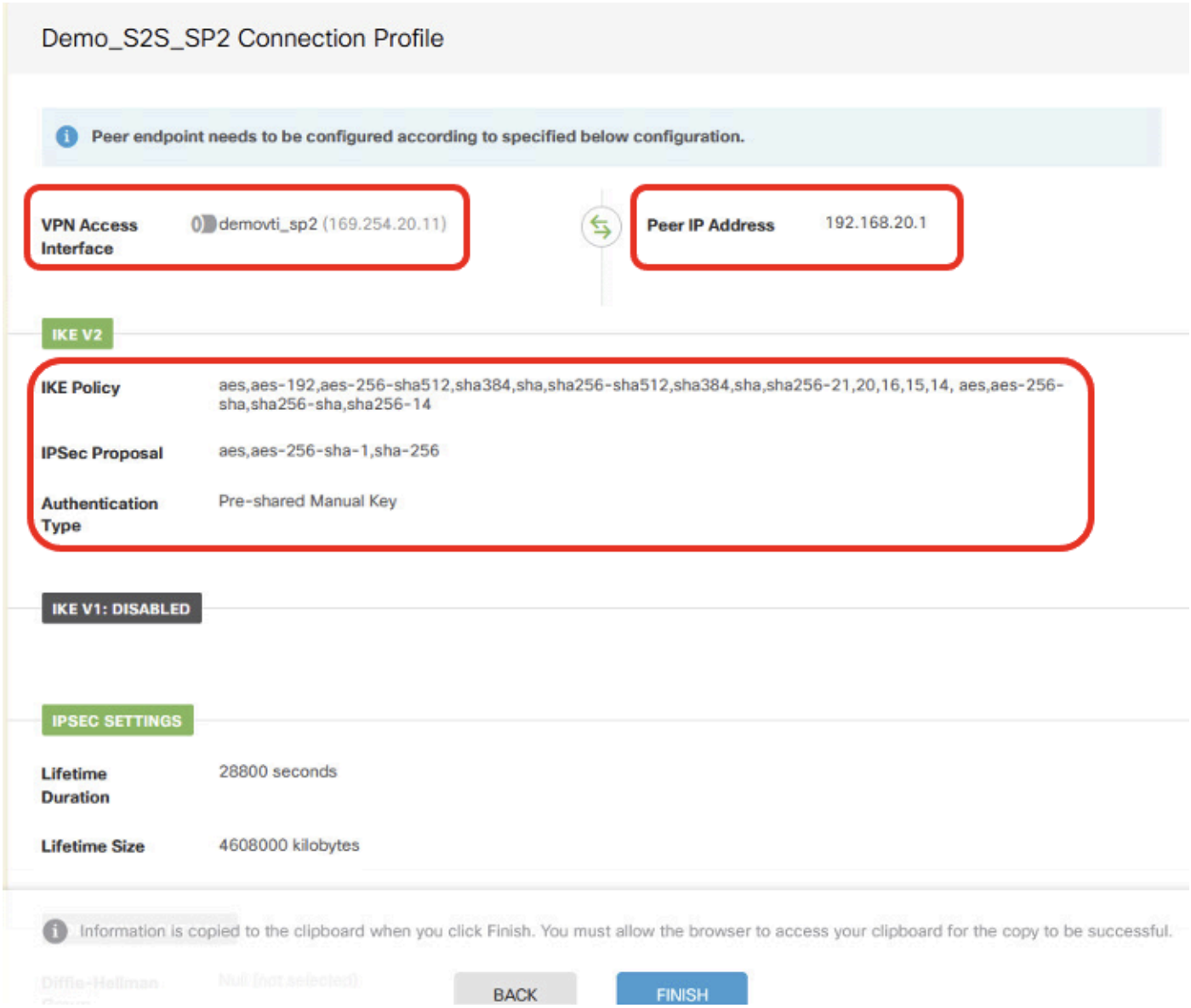
Site1FTD_Configure_Pre_Shared_Key

Paso 5.7. 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.



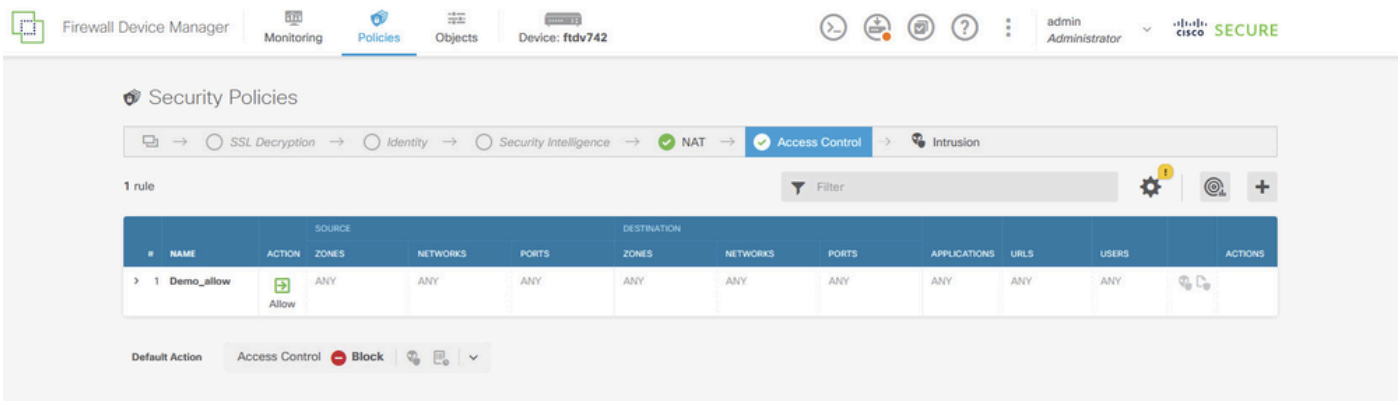
Site1FTD_ISP1_Review_VPN_Config_Summary

Paso 6. Repita el Paso 5. para crear una nueva VPN de sitio a sitio a través de ISP2.



Site1FTD_ISP2_Review_VPN_Config_Summary

Paso 7. Cree una 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 de Site1FTD_Allow_Access_Control_Rule_Example

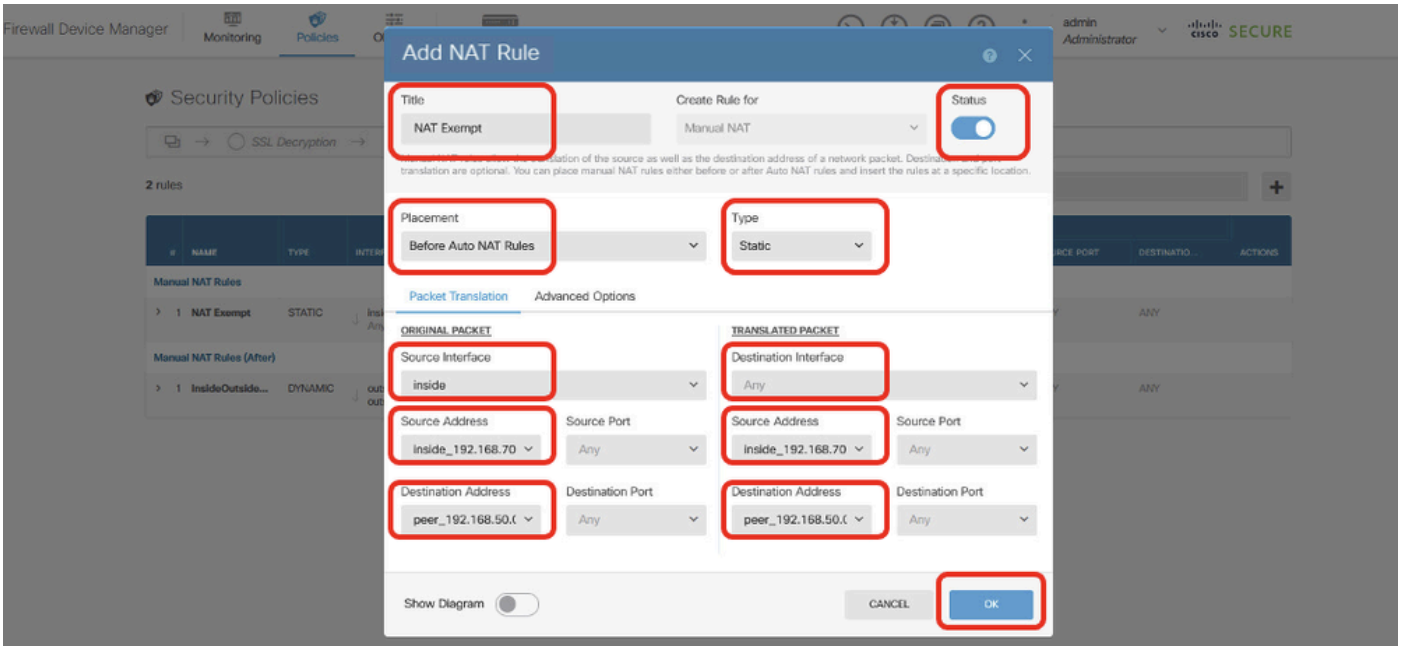
Paso 8. (Opcional) Configure la regla de exención de NAT para el tráfico del cliente en FTD si hay

NAT dinámica configurada para el cliente para acceder a Internet.

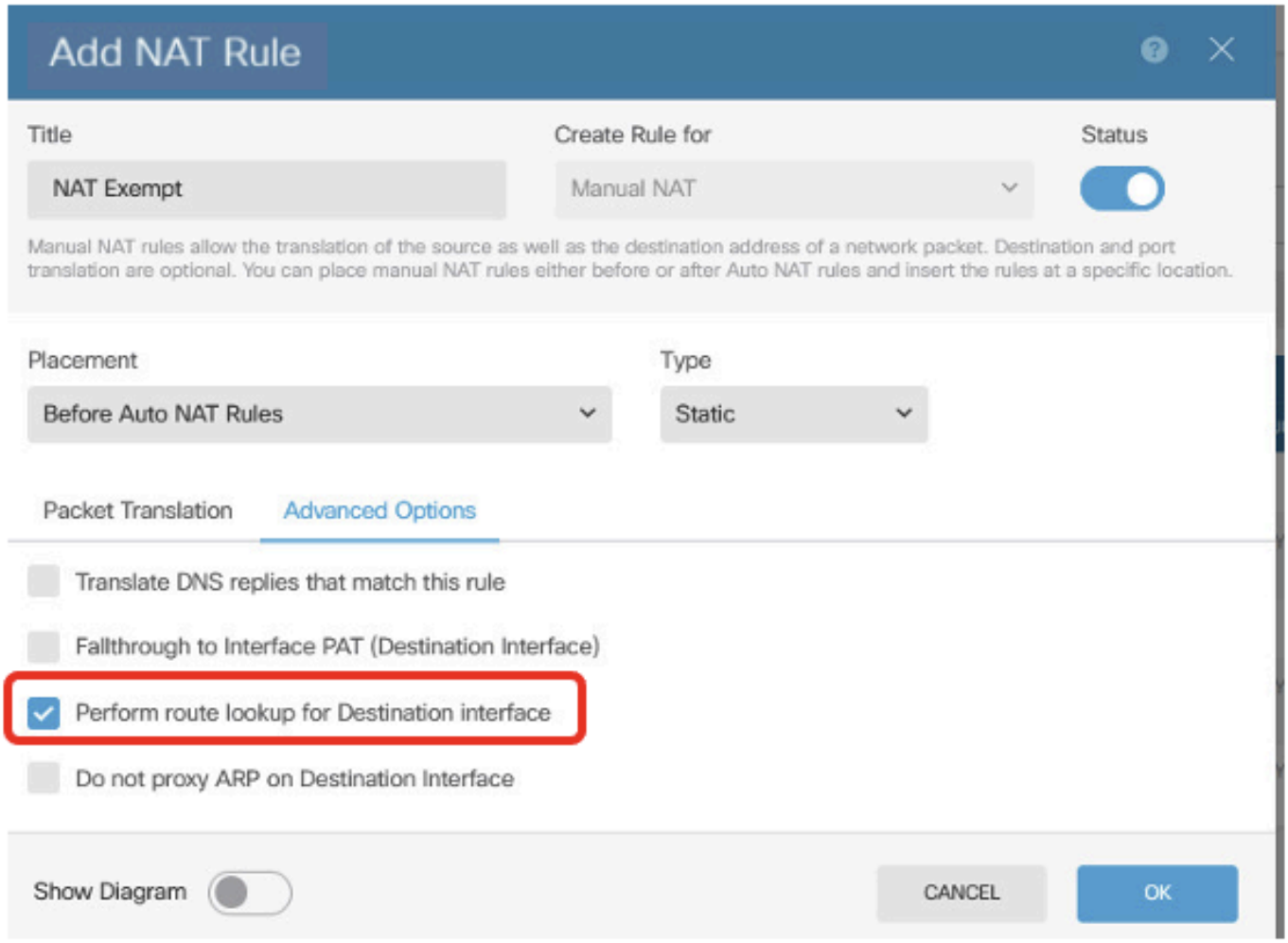
Para la demostración, la NAT dinámica se configura para los clientes para acceder a Internet en este ejemplo. Por lo tanto, se necesita la regla de exención de NAT.

Vaya a Políticas > NAT. Haga clic en el botón +. Proporcione los detalles y haga clic en Aceptar.

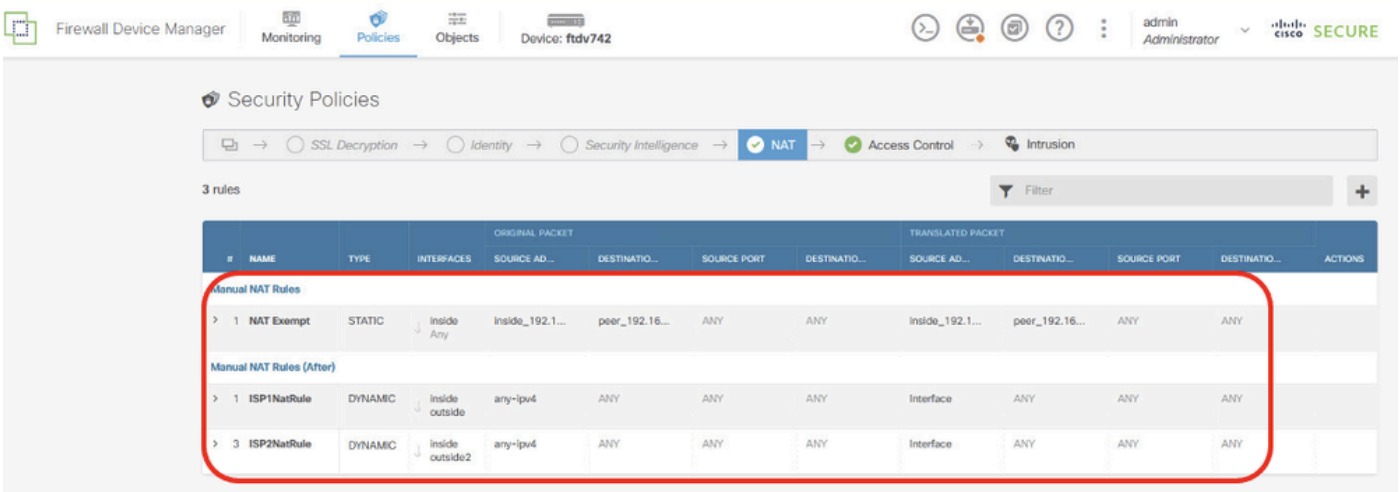
- TÍTULO: Exención de NAT
- Ubicación: Antes de las reglas NAT automáticas
- Tipo: Estática
- Interfaz de origen: Dentro
- Destino: cualquiera
- Dirección de origen original: 192.168.70.0/24
- Dirección de origen traducida: 192.168.70.0/24
- Dirección de destino original: 192.168.50.0/24
- Dirección de destino traducida: 192.168.50.0/24
- Con Route-Lookup habilitado



Site1FTD_Nat_Exempt_Rule



Site1FTD_Nat_Exempt_Rule_2



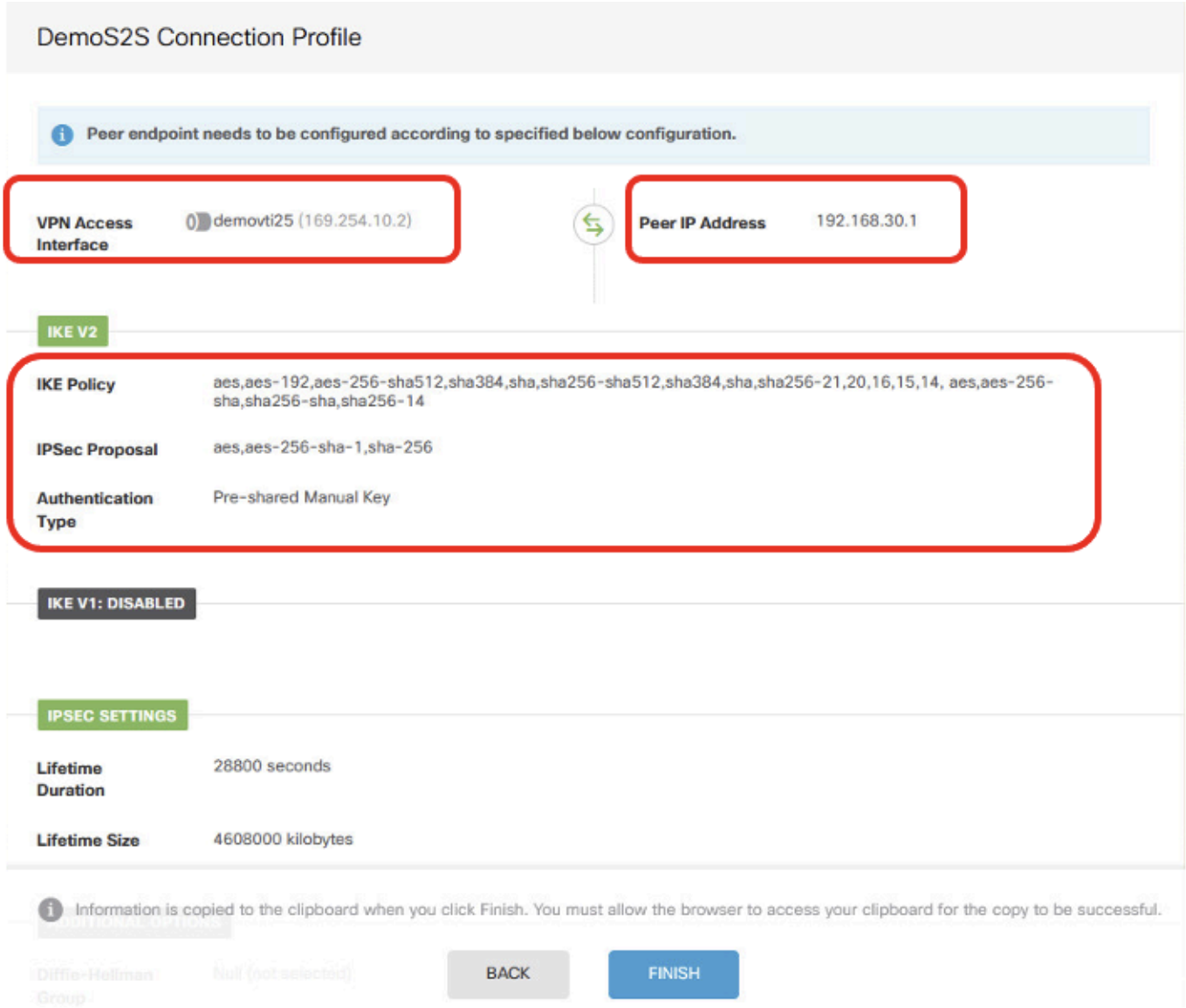
Site1FTD_Nat_Rule_Overview

Paso 9. Implemente los cambios de configuración.

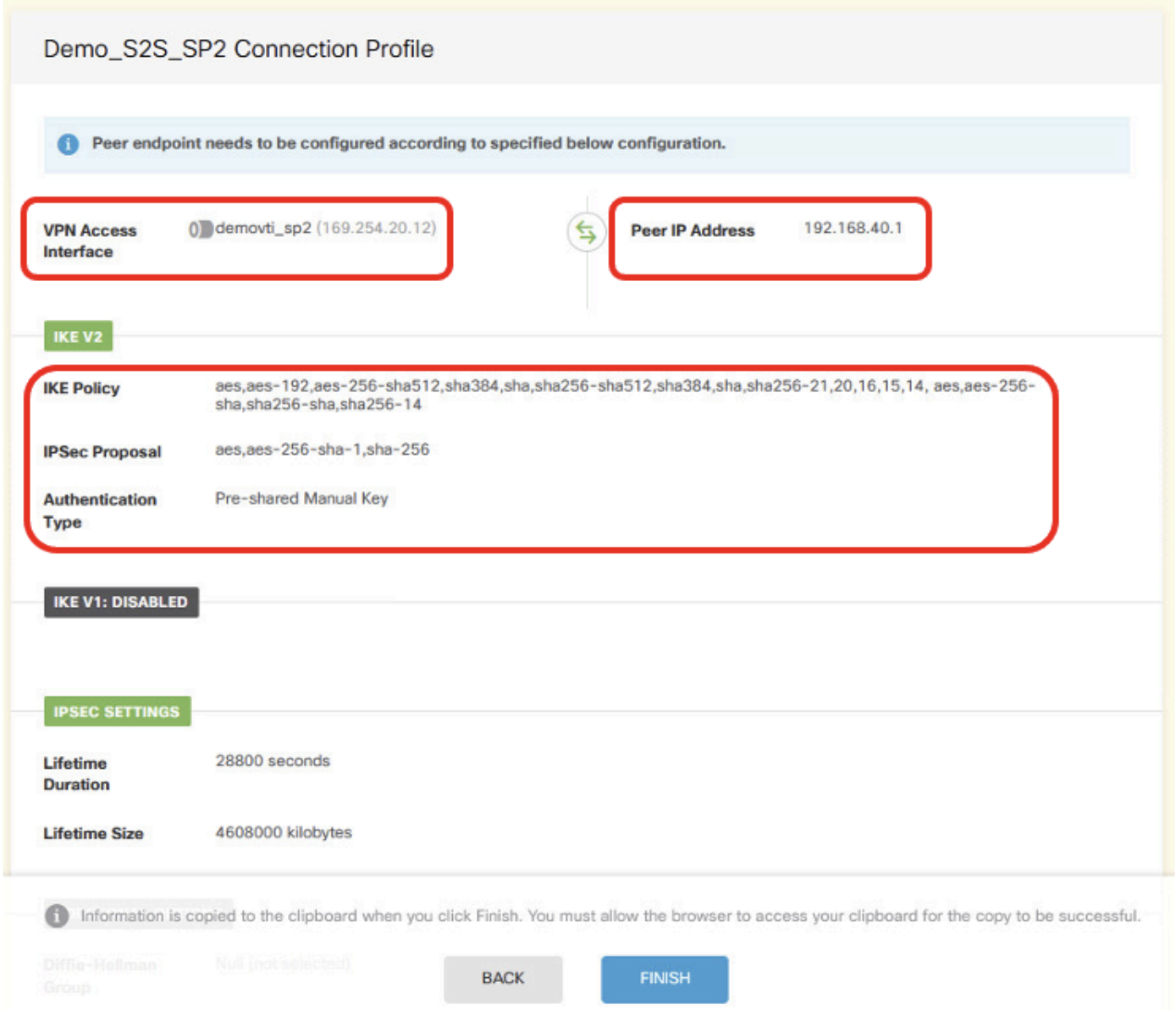
Site1FTD_Deployment_Changes

Configuración VPN FTD de Site2

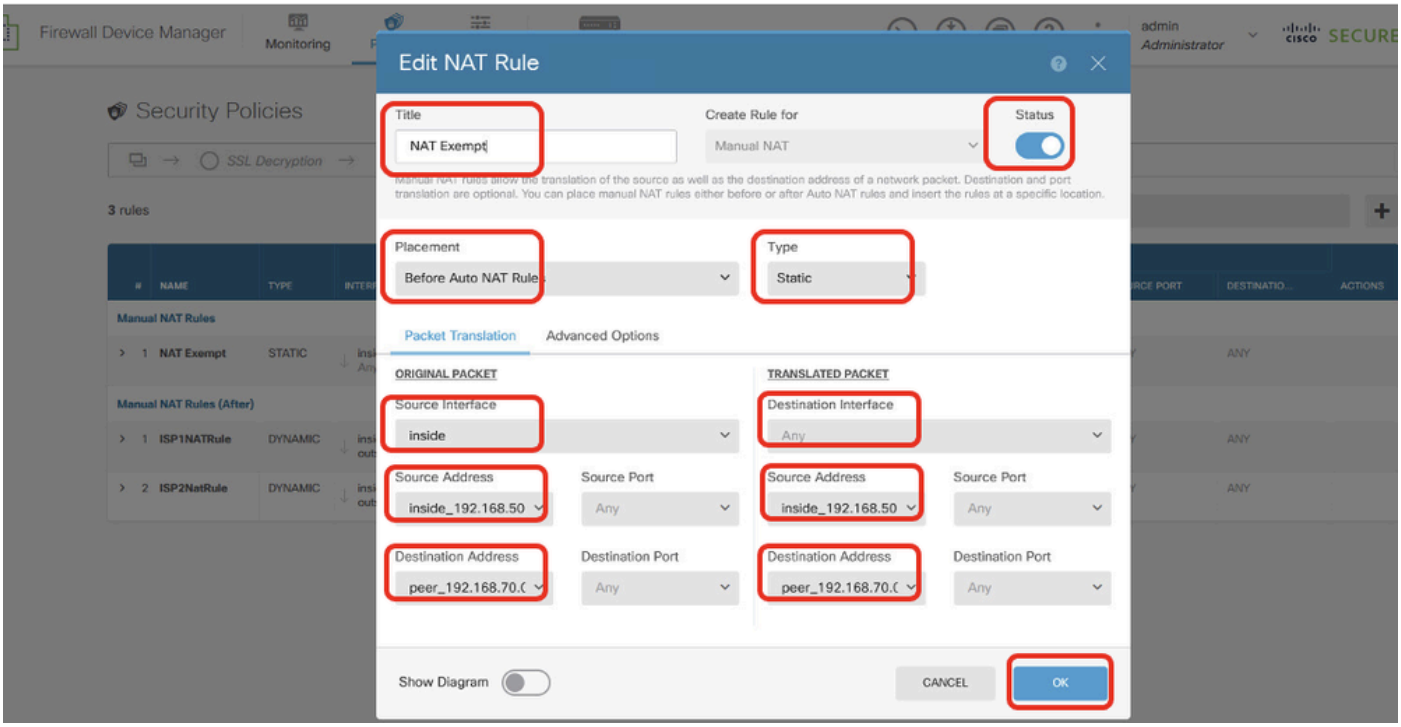
Paso 10. Repita los pasos 1 a 9 con los parámetros correspondientes para FTD de Sitio2.



Site2FTD_ISP1_Review_VPN_Config_Summary



Site2FTD_ISP2_Review_VPN_Config_Summary

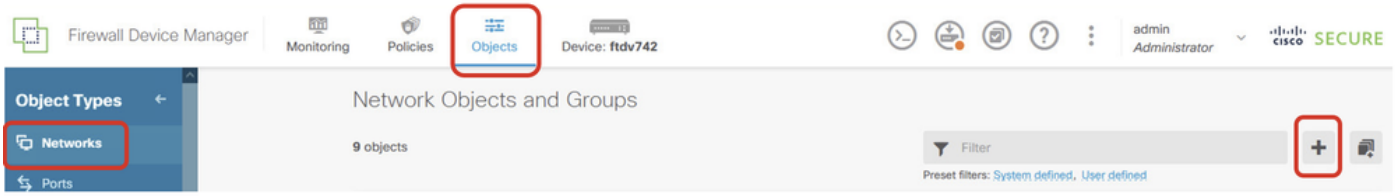


Site2FTD_Nat_Exempt_Rule

Configuraciones en PBR

Configuración PBR de FTD de Site1

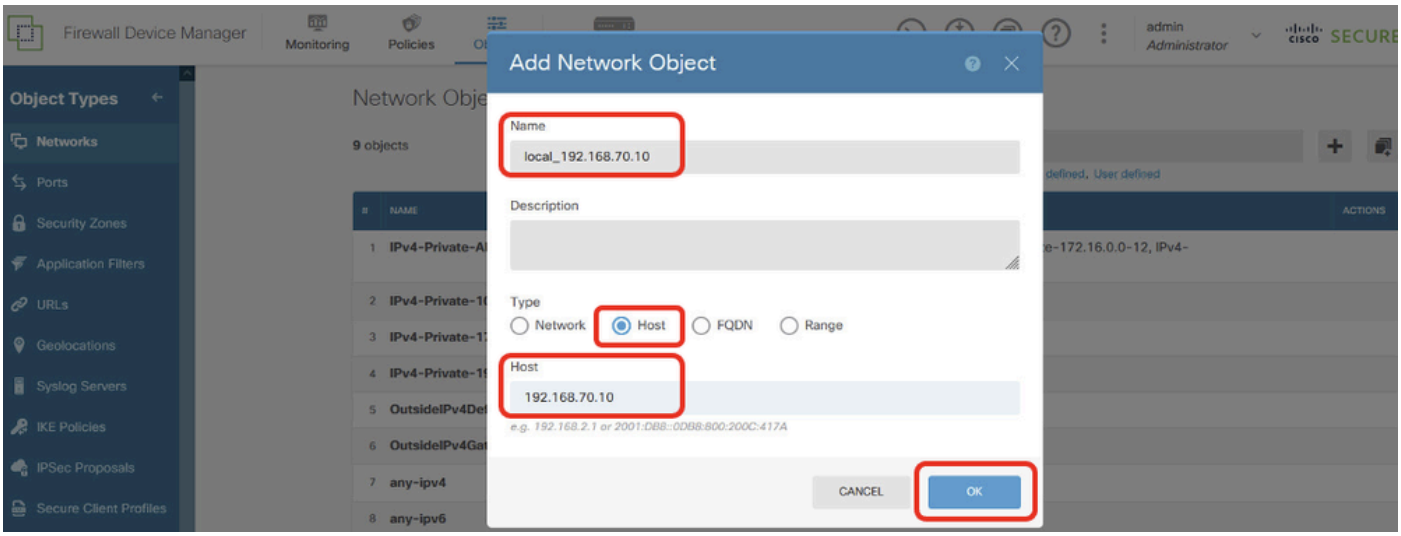
Paso 11. Cree nuevos objetos de red para que los utilice la lista de acceso PBR para el FTD Site1. Navegue hasta Objetos > Redes y haga clic en el botón +.



Site1FTD_Create_Network_Object

Paso 11.1. Cree el objeto de la dirección IP del cliente 1 del sitio 2. Proporcione la información necesaria. Haga clic en el botón OK (Aceptar)

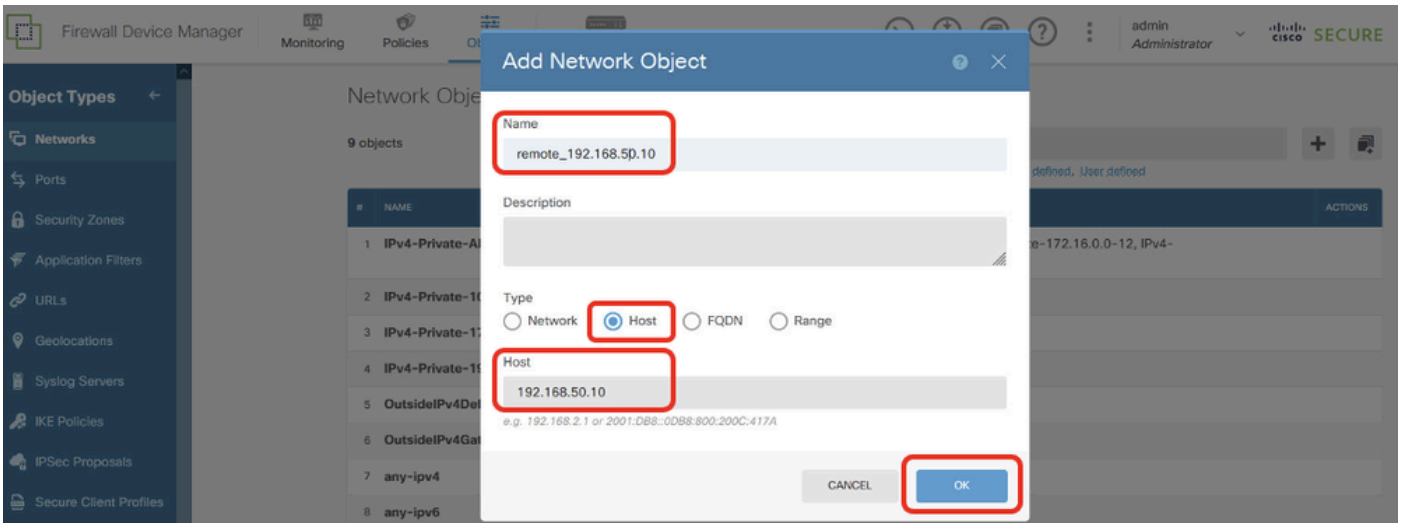
- Nombre: local_192.168.70.10
- Tipo: Anfitrión
- Host: 192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

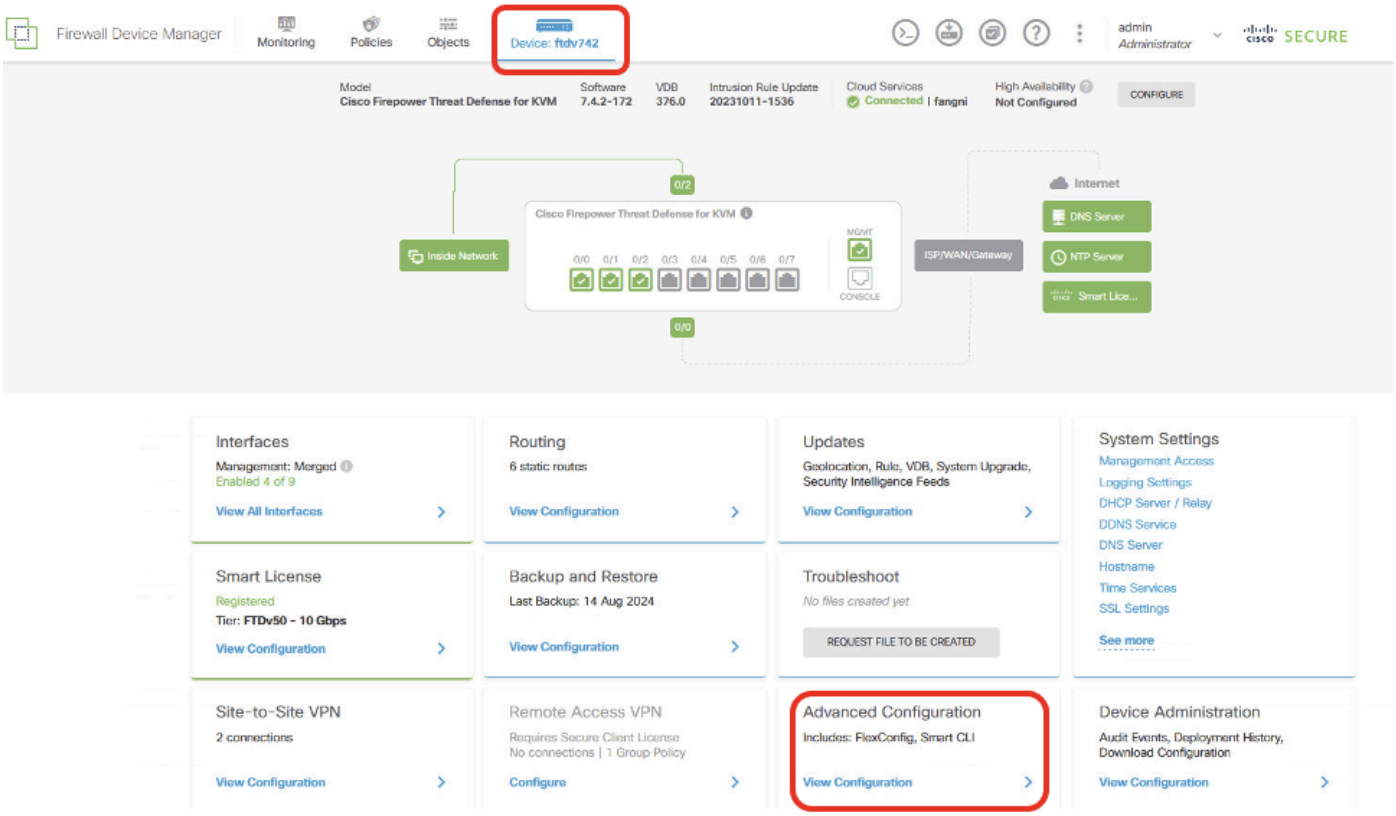
Paso 11.2. Crear objeto de la dirección IP del cliente 2 del sitio 2. Proporcionar la información necesaria. Haga clic en el botón Aceptar.

- Nombre: remote_192.168.50.10
- Tipo: Anfitrión
- Host: 192.168.50.10



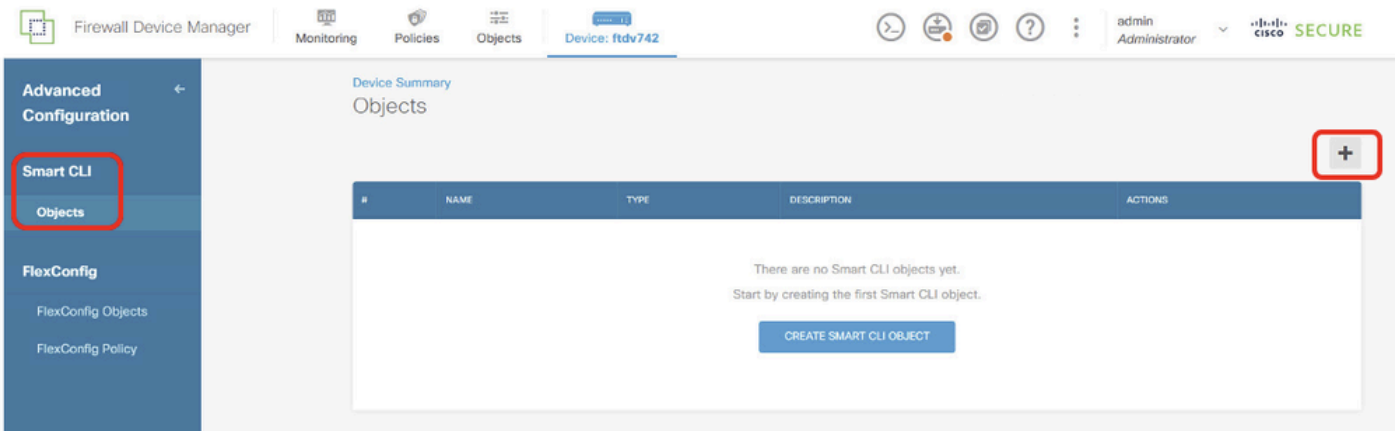
Site1FTD_PBR_RemoteObject

Paso 12. Crear una lista de acceso ampliada para PBR. Vaya a Device > Advanced Configuration. Haga clic en Ver configuración.



Site1FTD_View_Advanced_Configuration

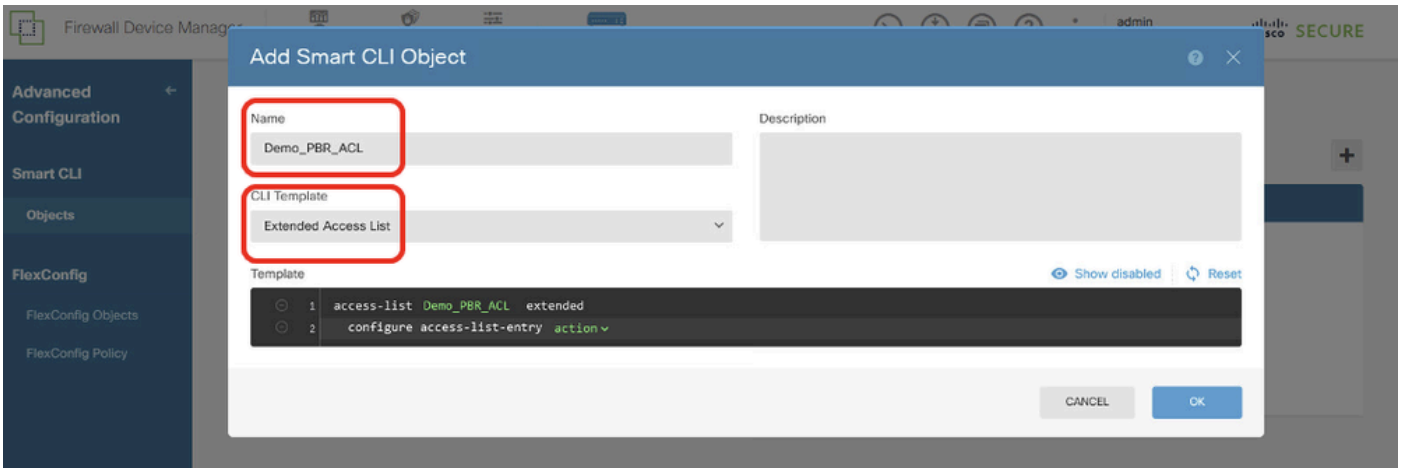
Paso 12.1. Navegue hasta CLI inteligente > Objetos. Haga clic en el botón +.



Site1FTD_Add_SmartCLI_Object

Paso 12.2. Introduzca un nombre para el objeto y elija la plantilla CLI.

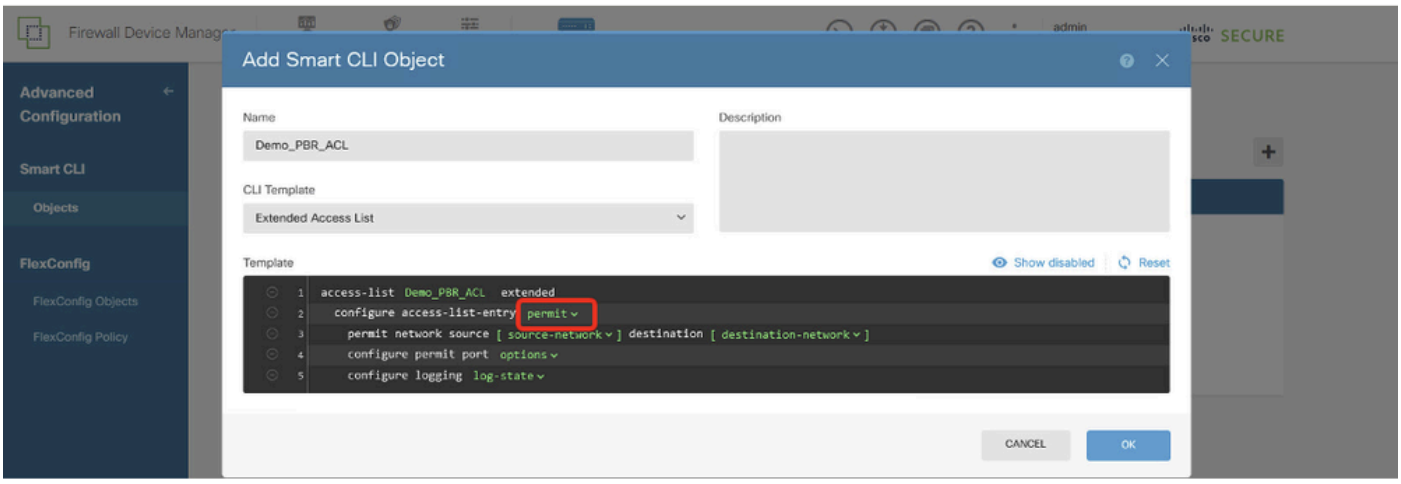
- Nombre: Demo_PBR_ACL
- Plantilla de CLI: Lista de acceso ampliada



Site1FTD_Create_PBR_ACL_1

Paso 12.3. Navegue hasta Plantilla y configure. Haga clic en el botón OK para guardar.

Línea 2, haga clic en action. Seleccione Permit (Permitir).

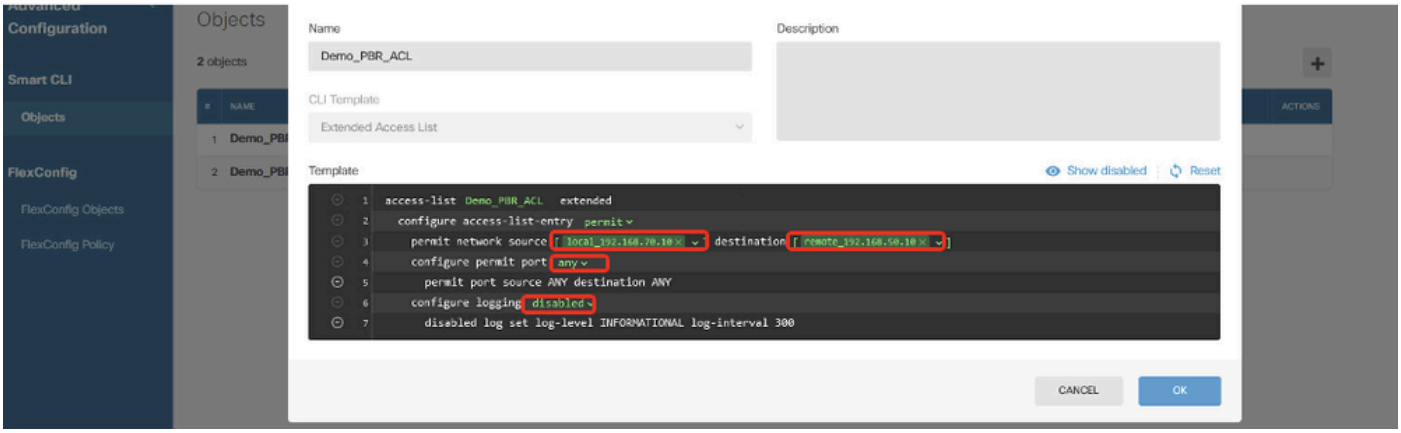


Site1FTD_Create_PBR_ACL_2

Línea 3, haga clic en source-network. Elija local_192.168.70.10. Haga clic en destination-network. Elija remote_192.168.50.10.

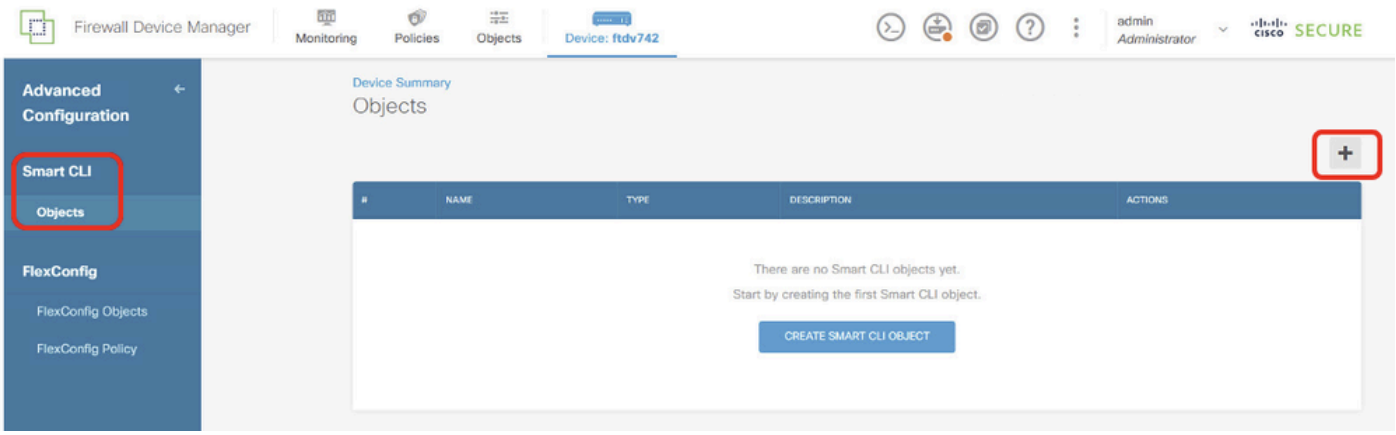
Línea 4, haga clic en options y elija any.

En la línea 6, haga clic en log-state y elija disabled.



Site1FTD_Create_PBR_ACL_3

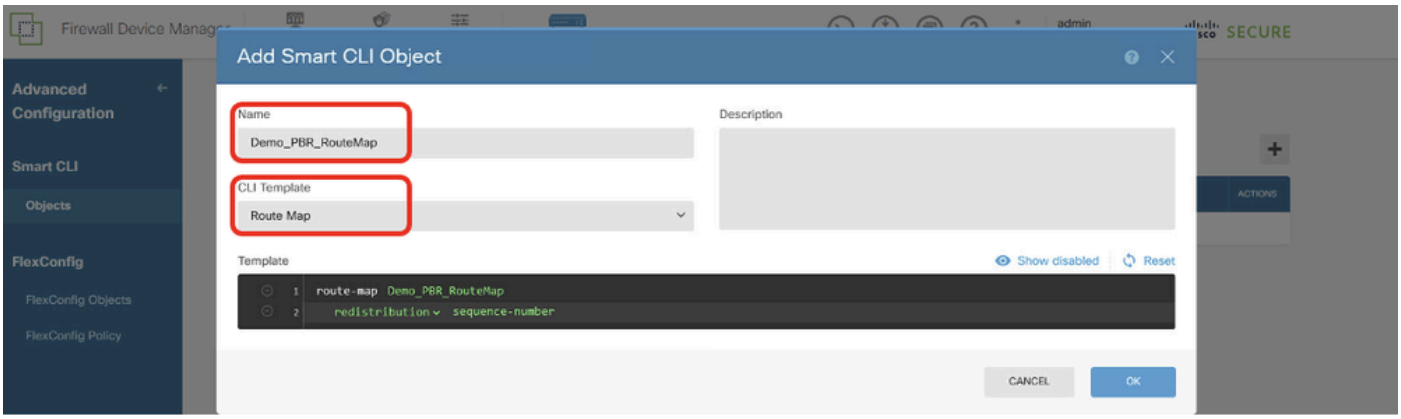
Paso 13. Crear mapa de rutas para PBR. Vaya a Dispositivo > Configuración avanzada > CLI inteligente > Objetos. Haga clic en el botón +.



Site1FTD_Add_SmartCLI_Object

Paso 13.1. Introduzca un nombre para el objeto y elija la plantilla CLI.

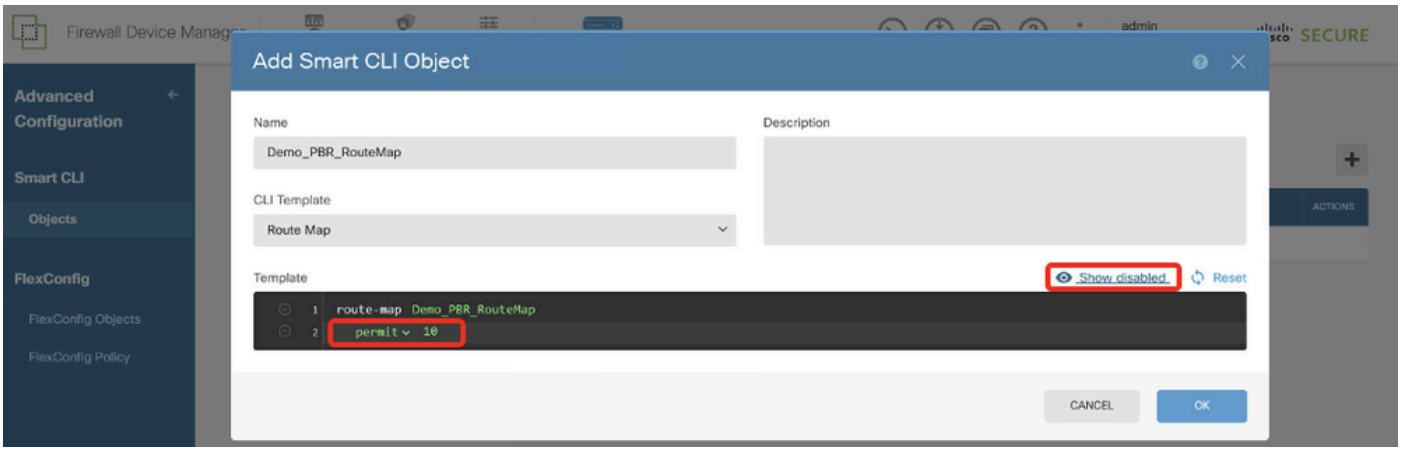
- Nombre: Demo_PBR_RouteMap
- Plantilla de CLI: Route Map



Site1FTD_Create_PBR_RouteMap_1

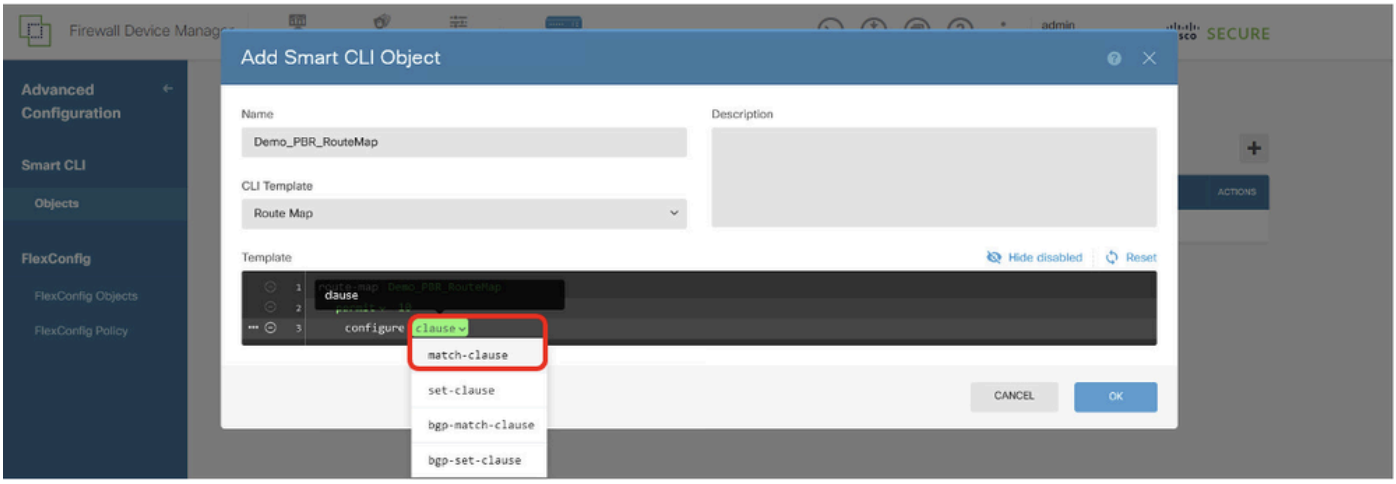
Paso 13.2. Navegue hasta Plantilla y configure. Haga clic en el botón OK para guardar.

Línea 2, haga clic en redistribution. Seleccione Permit (Permitir). Haga clic en sequence-number, entrada manual 10. Haga clic en Show disabled.



Site1FTD_Create_PBR_RouteMap_2

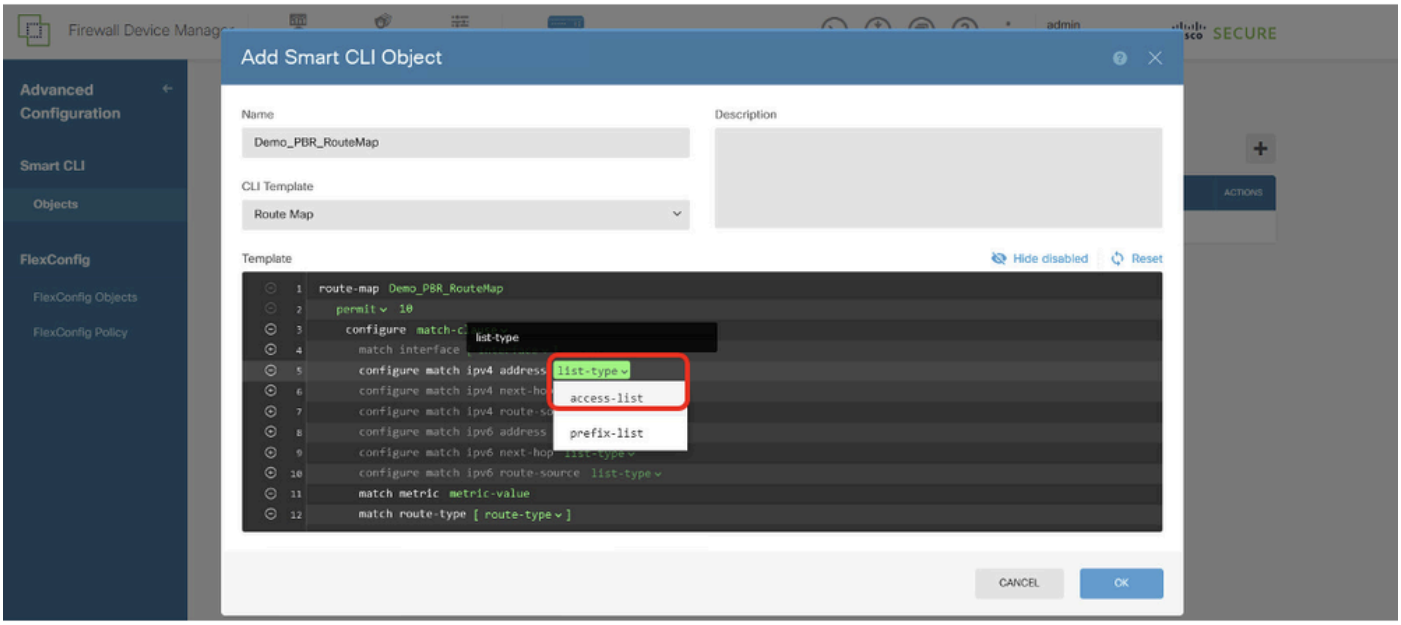
Línea 3, haga clic en + para habilitar la línea. Haga clic en cláusula. Elija la cláusula de coincidencia.



Site1FTD_Create_PBR_RouteMap_3

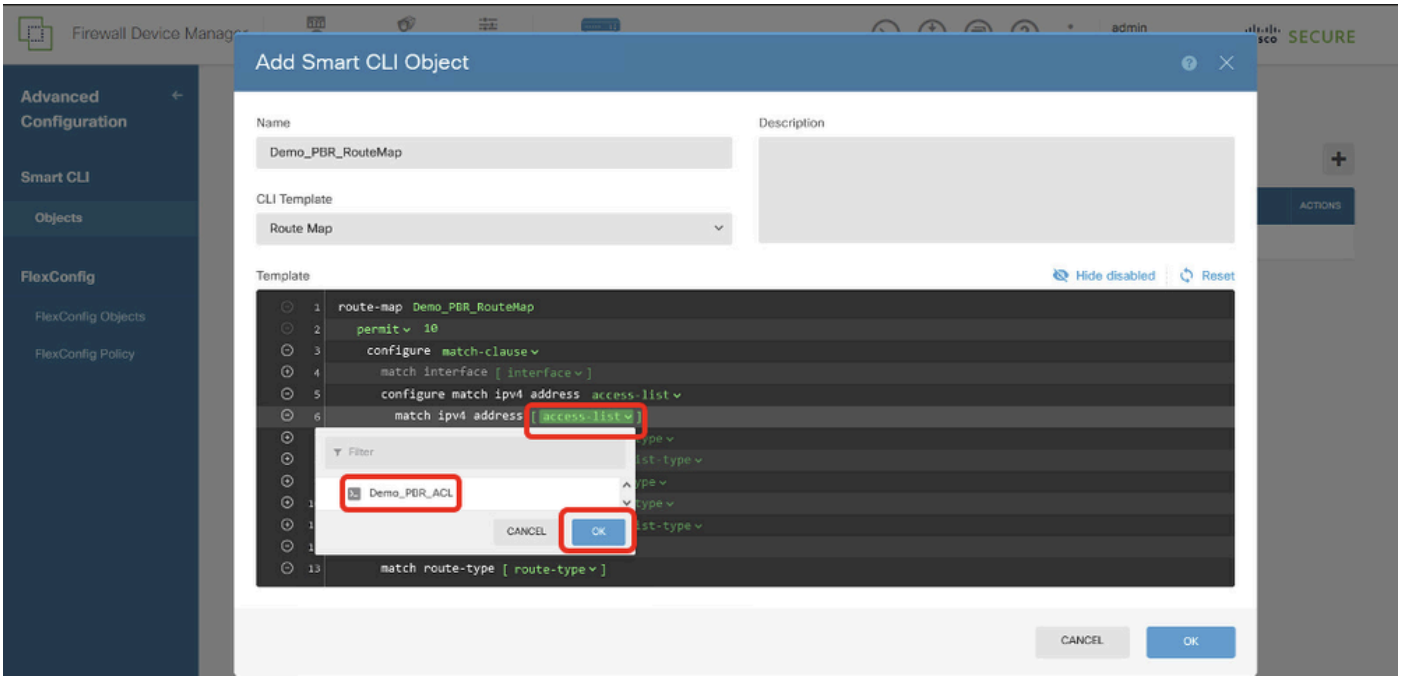
Línea 4, haga clic en - para desactivar la línea.

Línea 5, haga clic en + para habilitar la línea. Haga clic en list-type. Elija access-list.



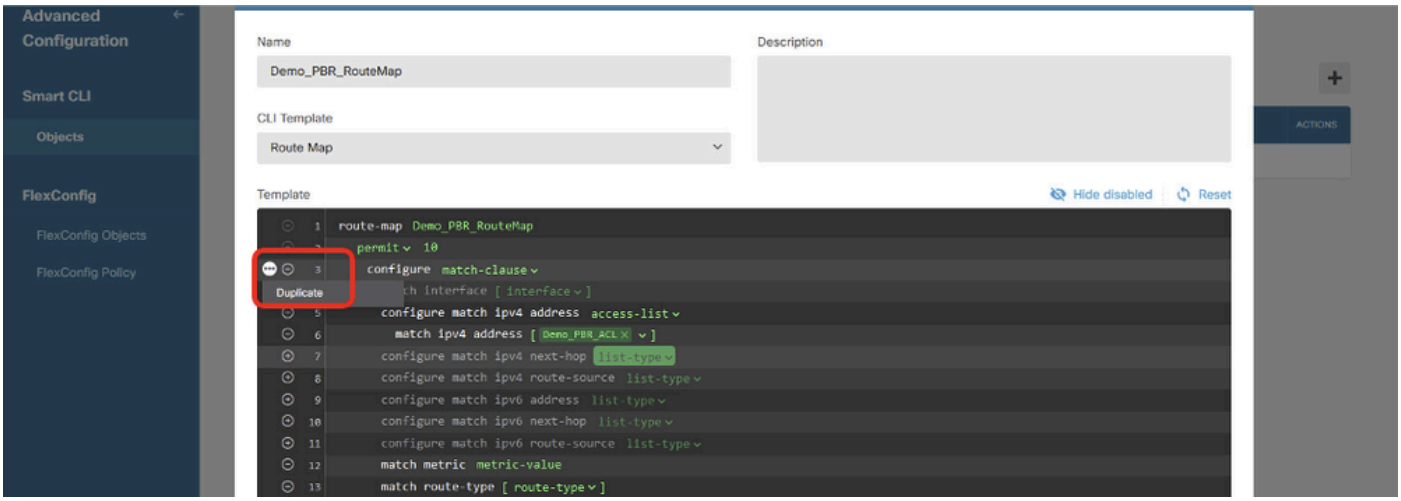
Site1FTD_Create_PBR_RouteMap_4

En la línea 6, haga clic en access-list. Elija el nombre de ACL que se crea en el paso 12. En este ejemplo, es Demo_PBR_ACL.



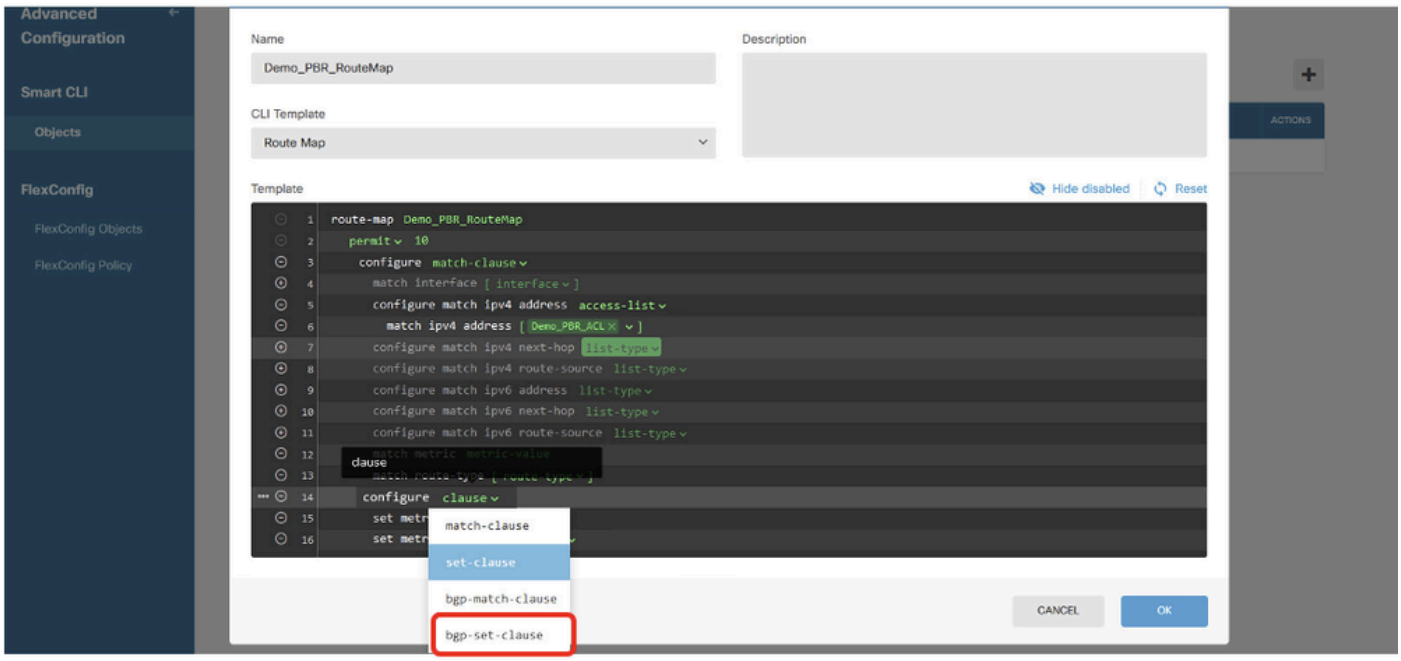
Site1FTD_Create_PBR_RouteMap_5

Vuelva a la línea 3. Haga clic en las opciones ... y seleccione Duplicar.



Site1FTD_Create_PBR_RouteMap_6

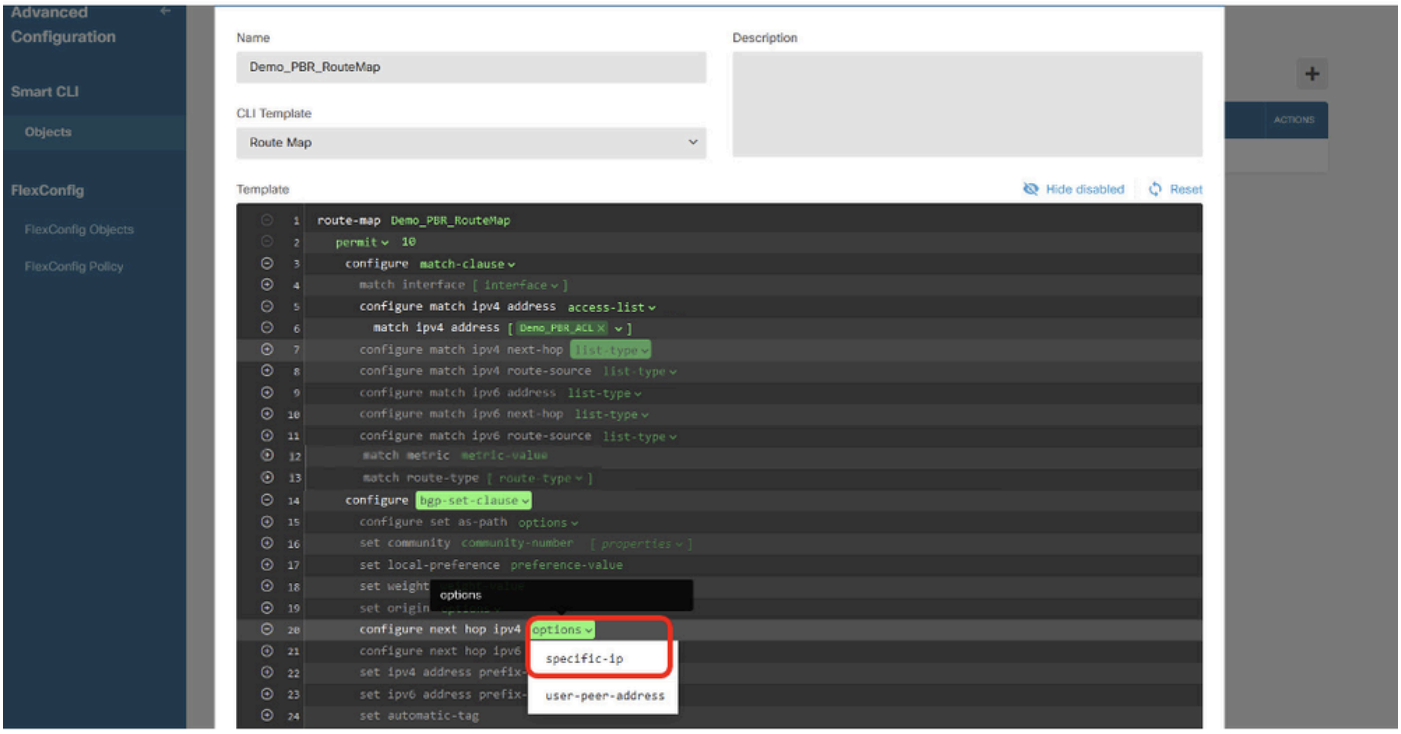
En la línea 14, haga clic en cláusula y elija bgp-set-cláusula.



Site1FTD_Create_PBR_RouteMap_7

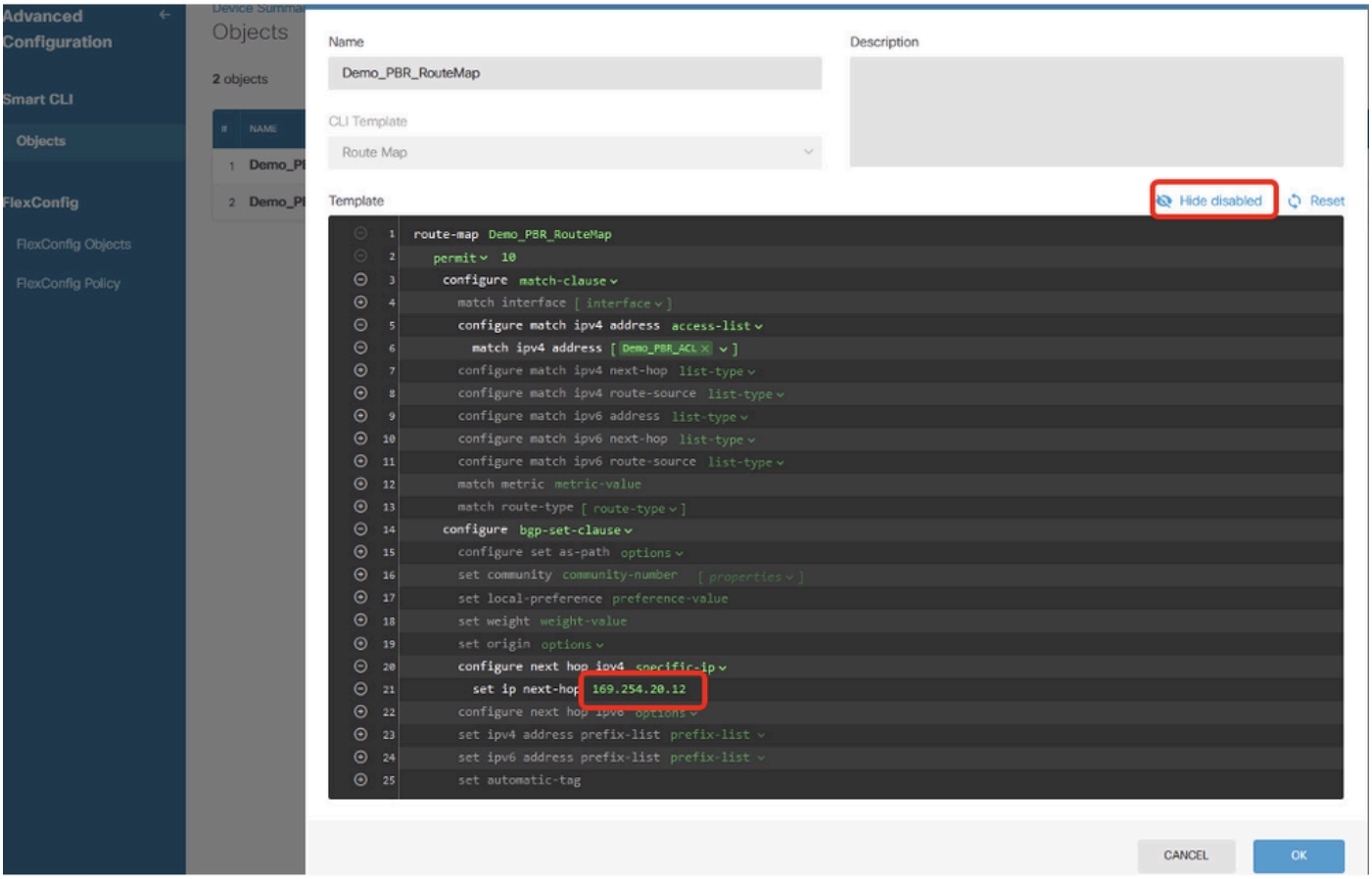
En las líneas 12, 13, 15, 16, 17, 18, 19, 21, 22, 23, 24, haga clic en - botón para desactivar.

Línea 20, haga clic en options y elija specific-ip.



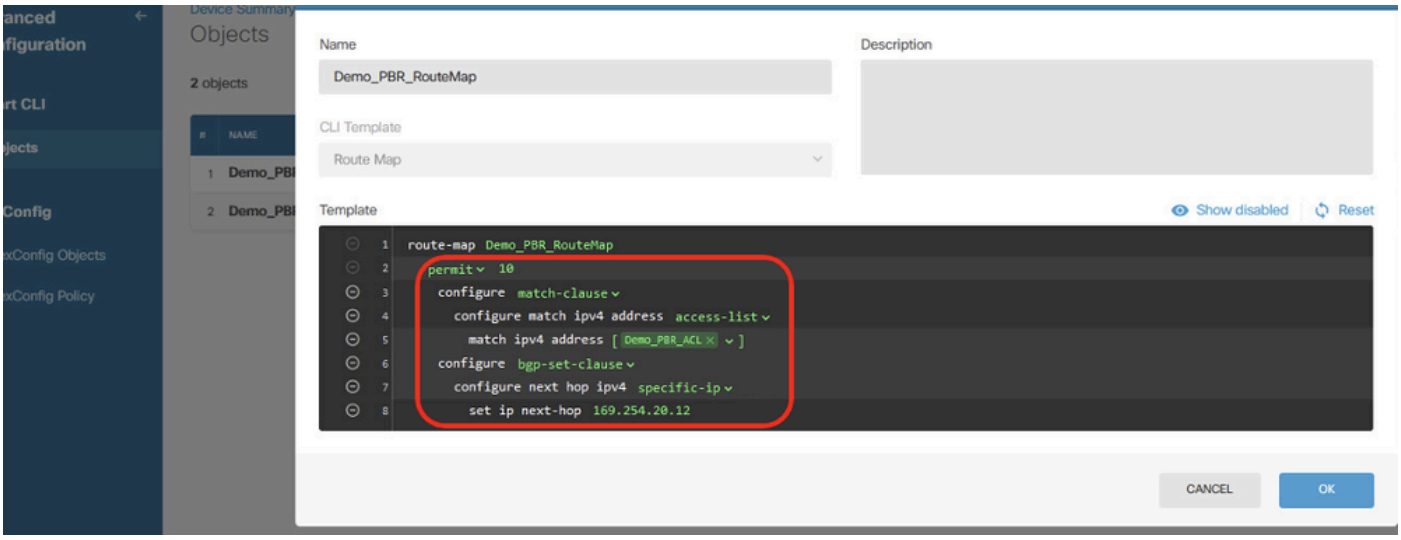
Site1FTD_Create_PBR_RouteMap_8

Línea 21, haga clic en ip-address. Dirección IP de próximo salto de entrada manual. En este ejemplo, es la dirección IP del par Site2 FTD VTI tunnel2 (169.254.20.12). Haga clic en Ocultar desactivado.



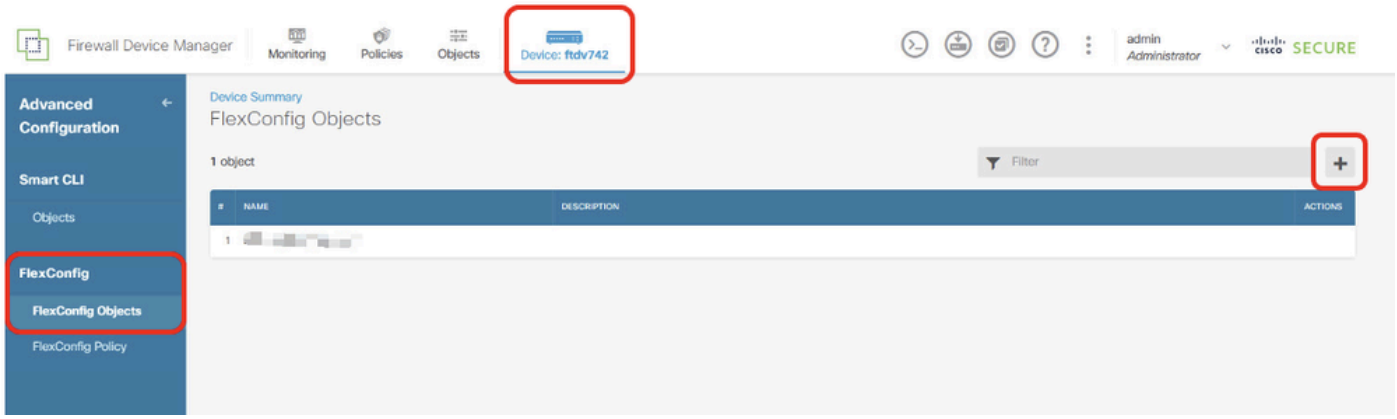
Site1FTD_Create_PBR_RouteMap_9

Revise la configuración del mapa de ruta.



Site1FTD_Create_PBR_RouteMap_10

Paso 14. Crear objeto FlexConfig para PBR. Navegue hasta Device > Advanced Configuration > FlexConfig Objects y haga clic en el botón +.



Site1FTD_Create_PBR_FlexObj_1

Paso 14.1. Introduzca un nombre para el objeto. En este ejemplo, Demo_PBR_FlexObj. En el editor Template y Negate Template, ingrese las líneas de comandos.

- Plantilla:

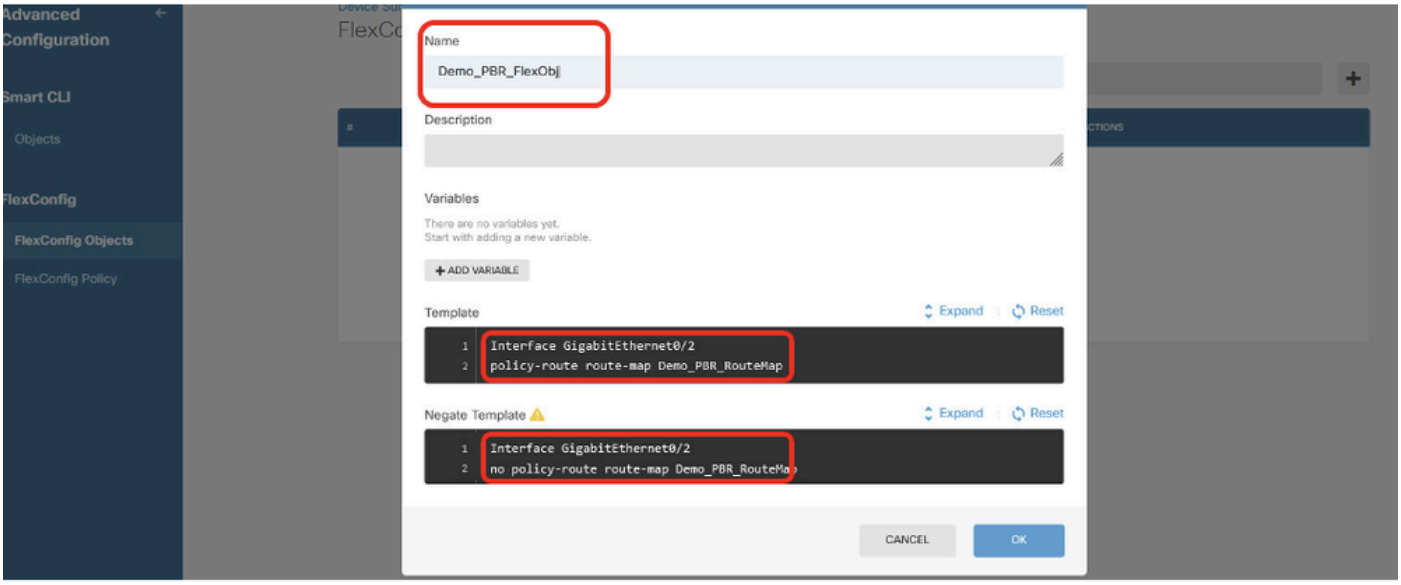
interface GigabitEthernet0/2

policy-route route-map Demo_PBR_RouteMap_Site2

- Negar plantilla:

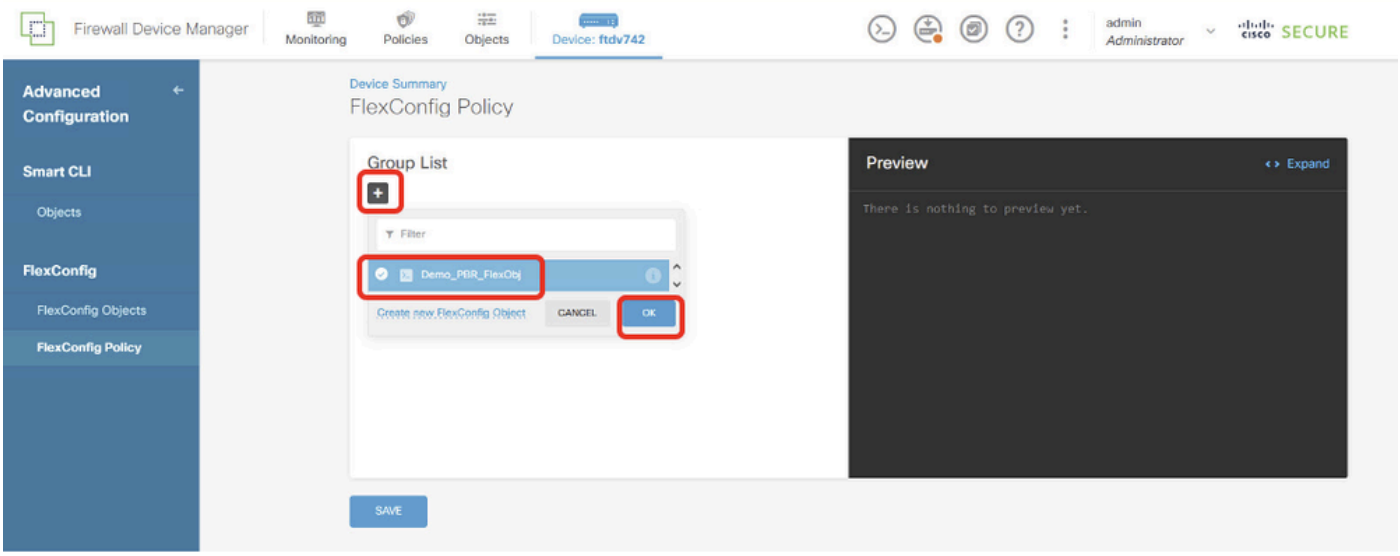
interface GigabitEthernet0/2

no policy-route route-map Demo_PBR_RouteMap_Site2



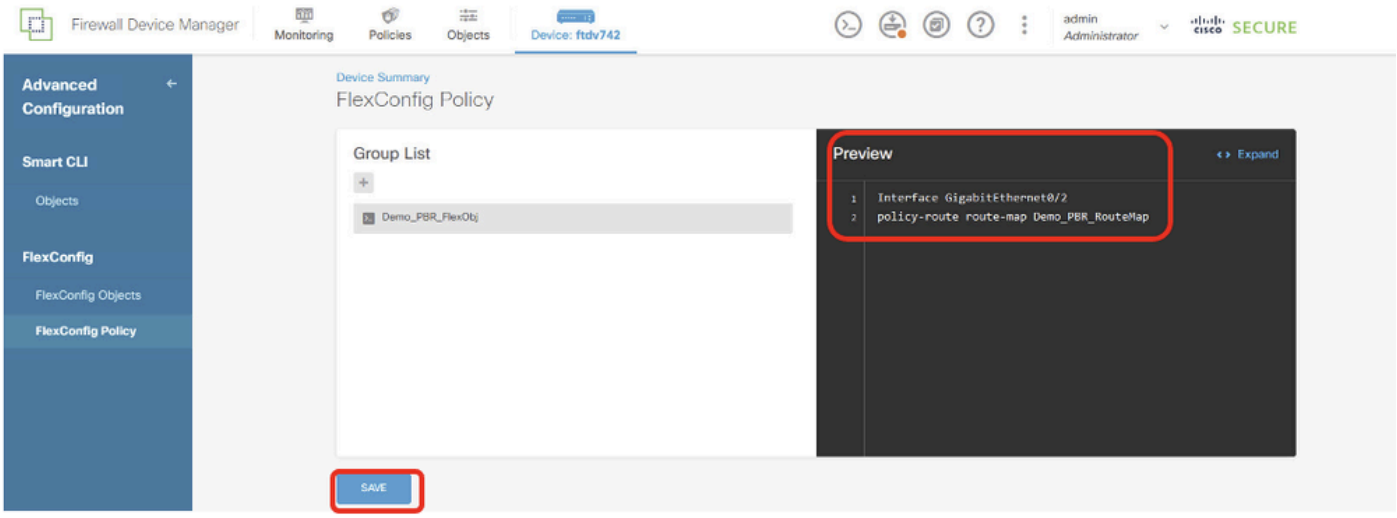
Site1FTD_Create_PBR_FlexObj_2

Paso 15. Crear política FlexConfig para PBR. Vaya a Dispositivo > Configuración avanzada > Política FlexConfig. Haga clic en el botón +. Elija el nombre del objeto FlexConfig creado en el paso 14. Haga clic en el botón Aceptar.



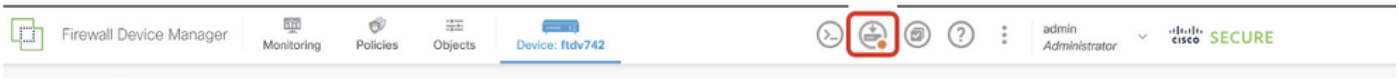
Site1FTD_Create_PBR_FlexPolicy_1

Paso 15.1. Verifique el comando en la ventana Preview. Si está correcto, haga clic en Guardar.



Site1FTD_Create_PBR_FlexPolicy_2

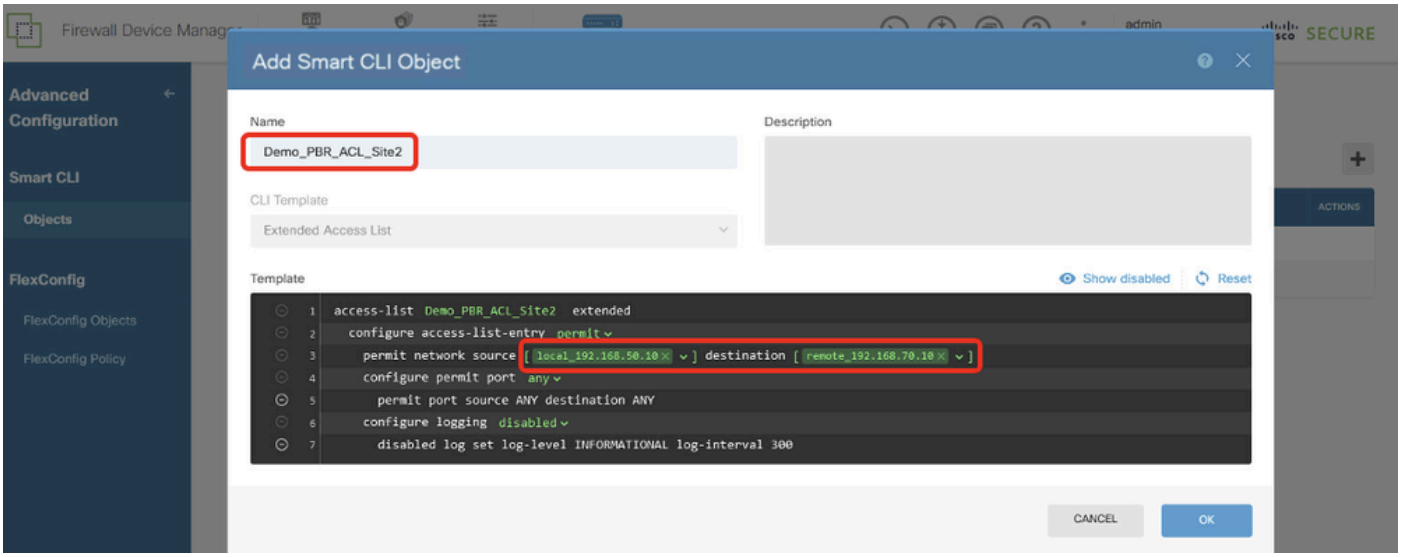
Paso 16. Implemente los cambios de configuración.



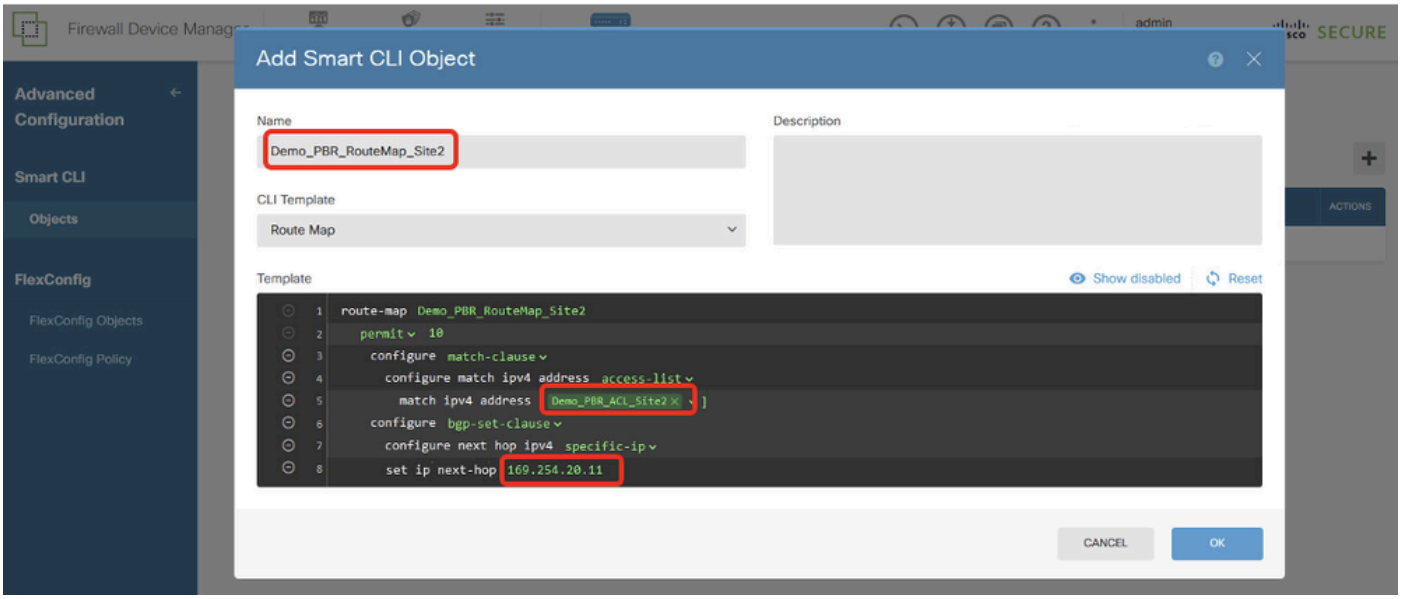
Site1FTD_Deployment_Changes

Configuración PBR de FTD de Site2

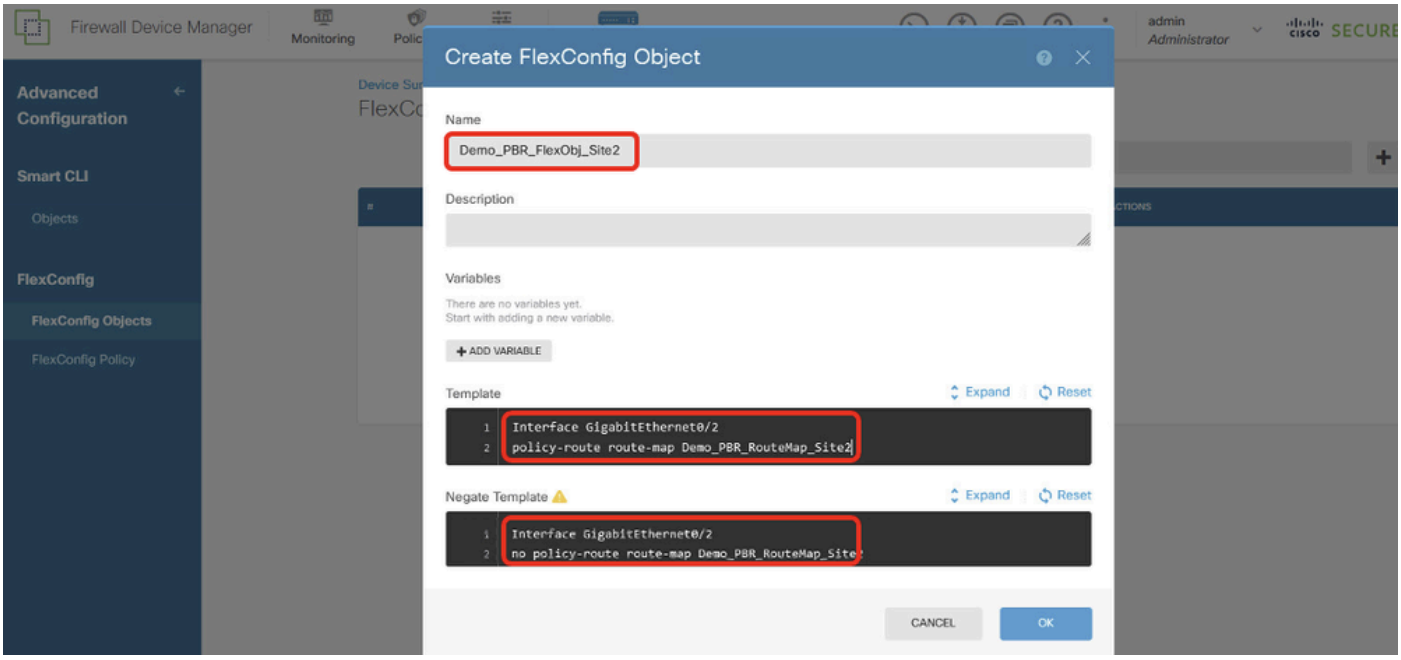
Paso 17. Repita el Paso 11. al Paso 16. para crear PBR con los parámetros correspondientes para FTD Site2.



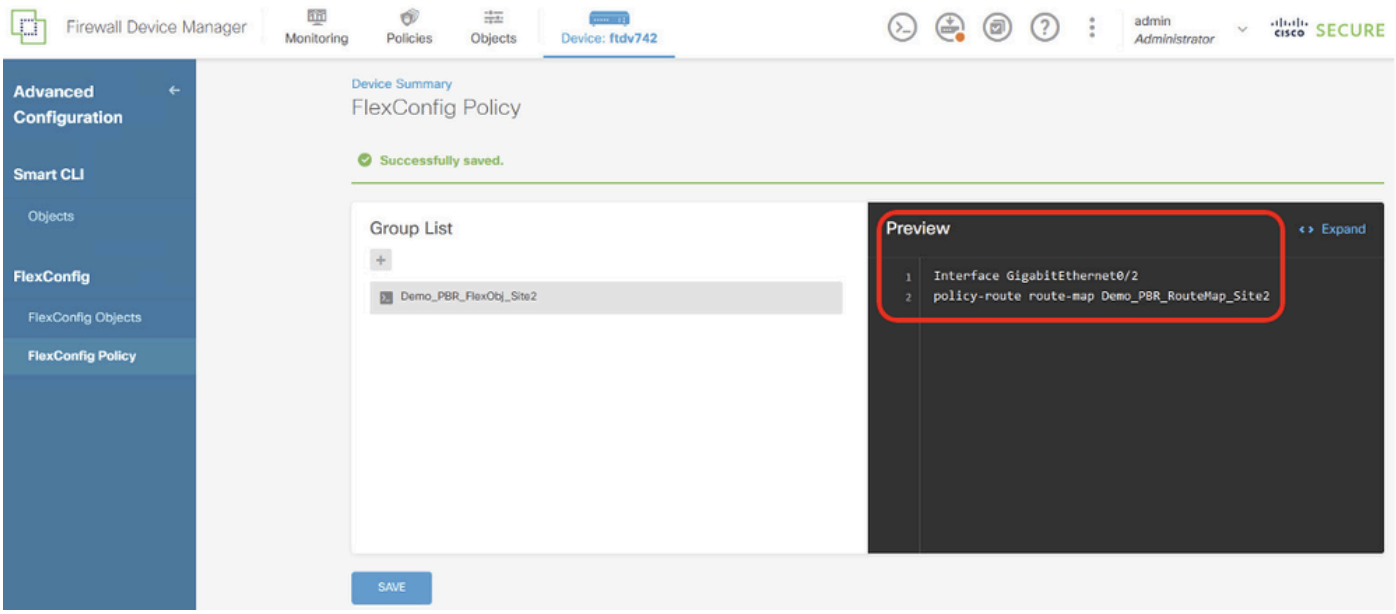
Site2FTD_Create_PBR_ACL



Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

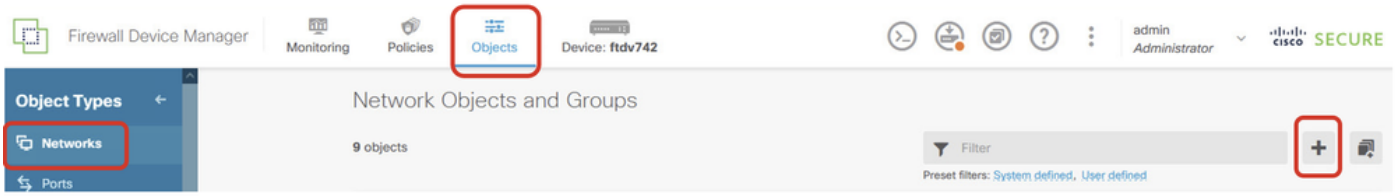


Site2FTD_Create_PBR_FlexPolicy

Configuraciones en el Monitor SLA

Configuración del monitor de FTD SLA del sitio 1

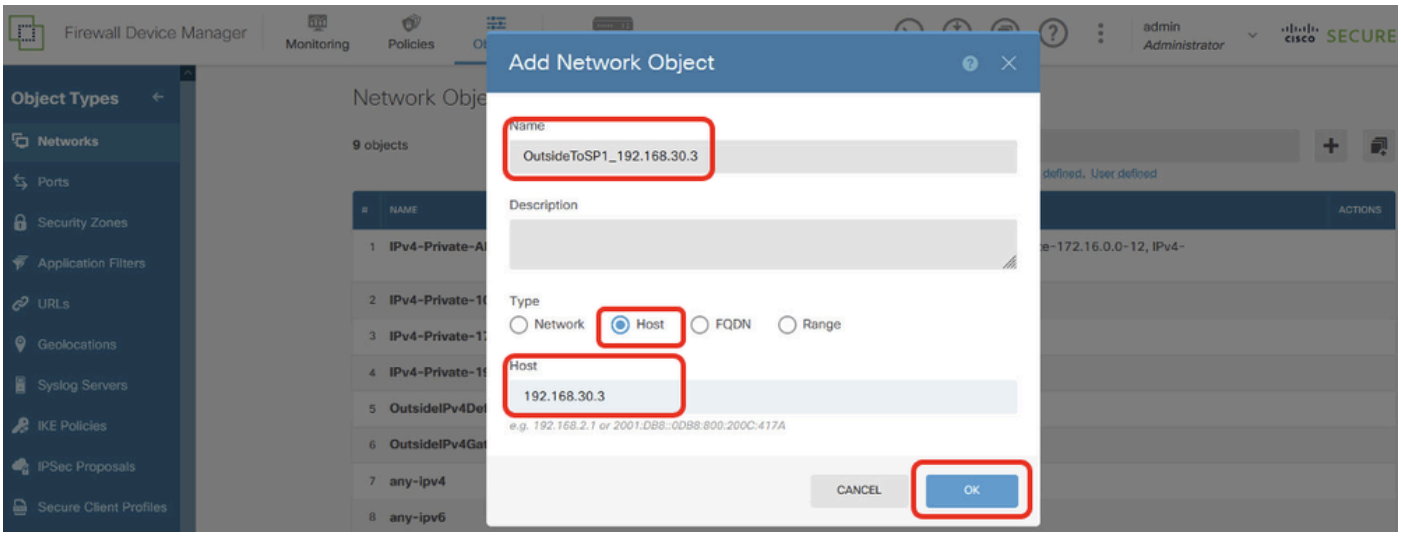
Paso 18. Cree nuevos objetos de red para que los supervisores de SLA los utilicen para el FTD del sitio 1. Navegue hasta Objetos > Redes, haga clic en el botón +.



Site1FTD_Create_Network_Object

Paso 18.1. Crear objeto para la dirección IP de la puerta de enlace ISP1. Proporcione la información necesaria. Haga clic en el botón Aceptar.

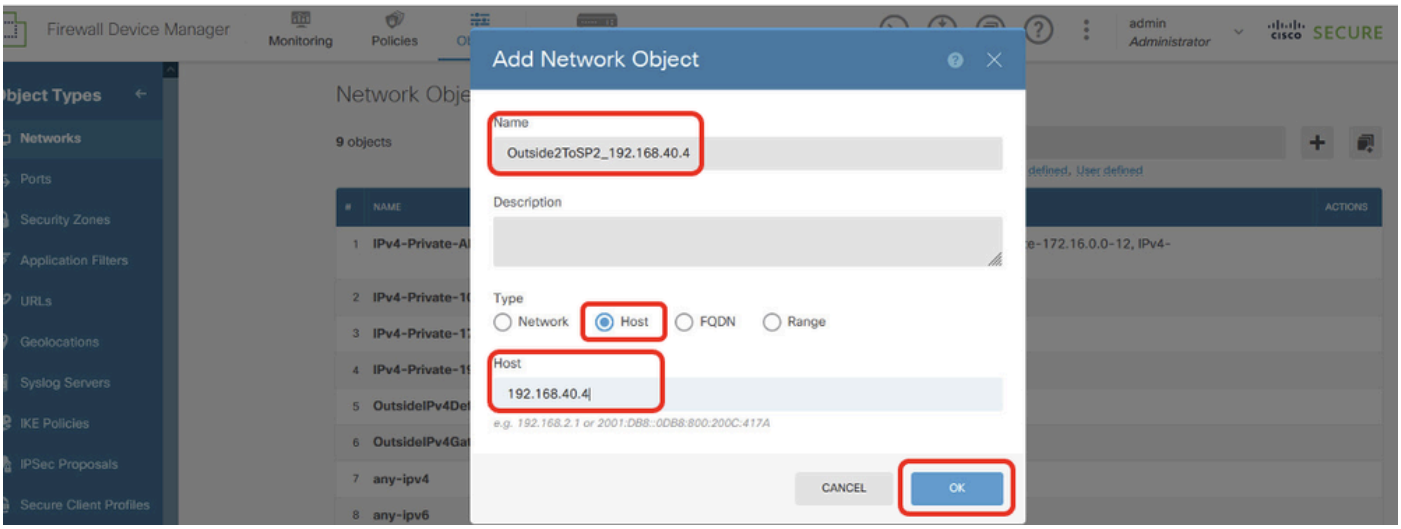
- Nombre: OutsideToSP1_192.168.30.3
- Tipo: Anfitrión
- Host: 192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

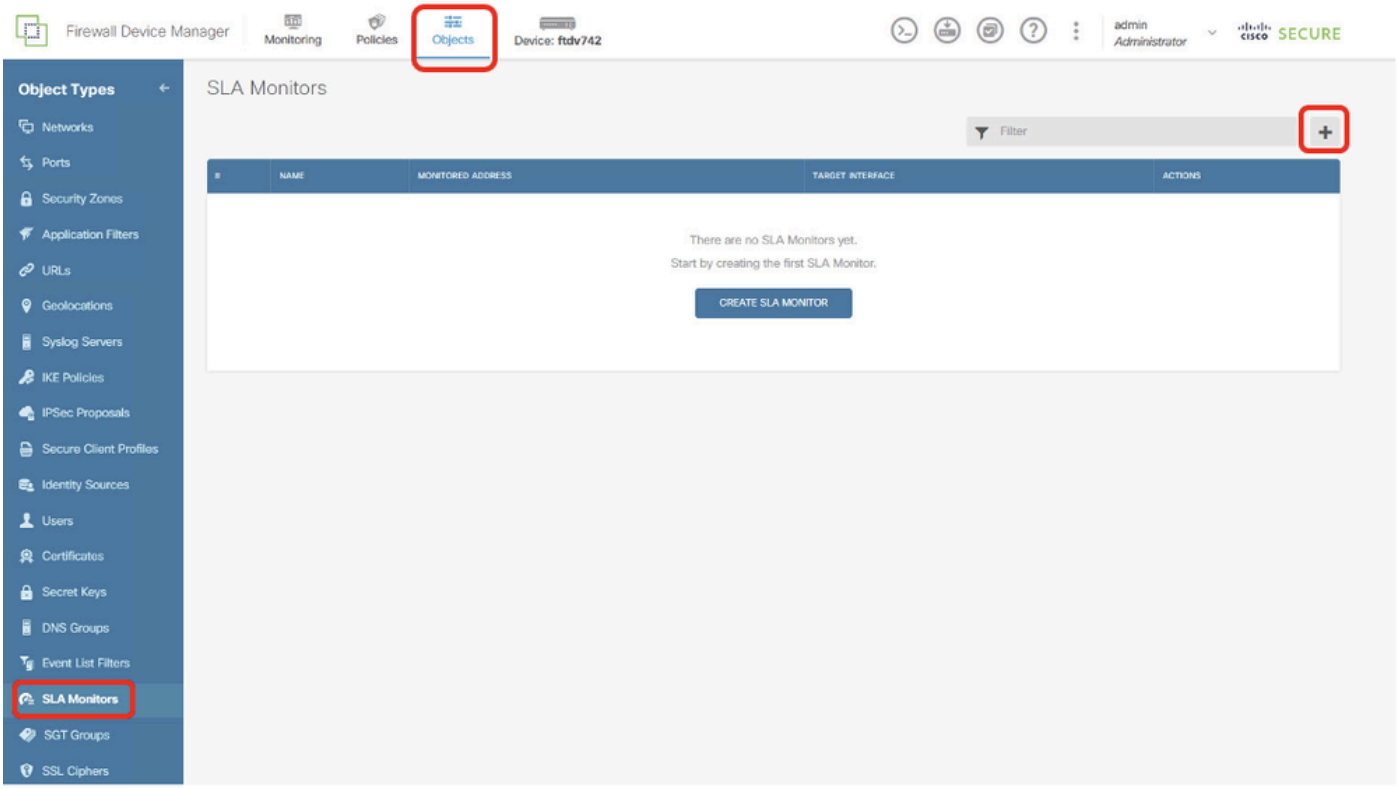
Paso 18.2. Crear objeto para la dirección IP de la puerta de enlace ISP2. Proporcione la información necesaria. Haga clic en el botón Aceptar.

- Nombre: Outside2ToSP2_192.168.40.4
- Tipo: Anfitrión
- Host: 192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

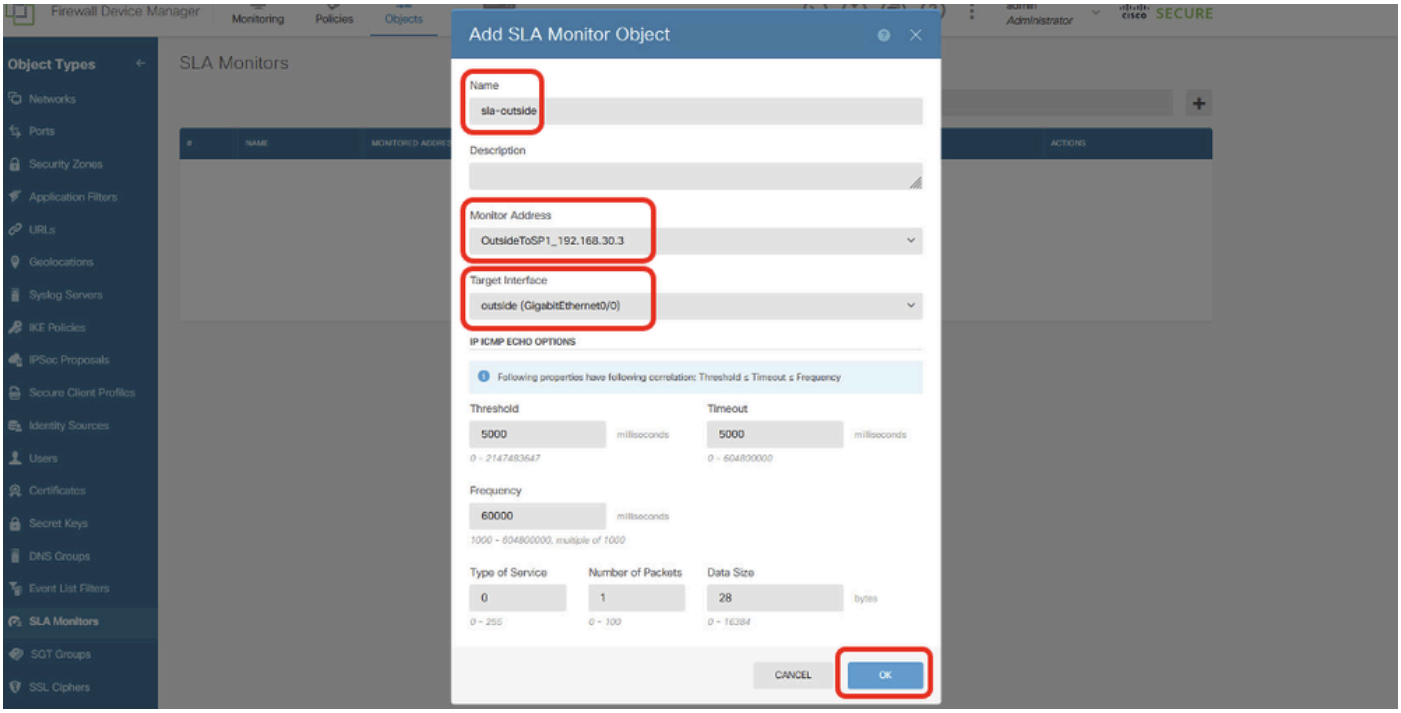
Paso 19. Creación de un monitor de SLA. Navegue hasta Objetos > Tipos de Objeto > Monitores de SLA. Haga clic en el botón + para crear un nuevo monitor SLA.



Site1FTD_Create_SLAMonitor

Paso 19.1. En la ventana Add SLA Monitor Object, proporcione la información necesaria para el gateway ISP1. Haga clic en el botón OK para guardar.

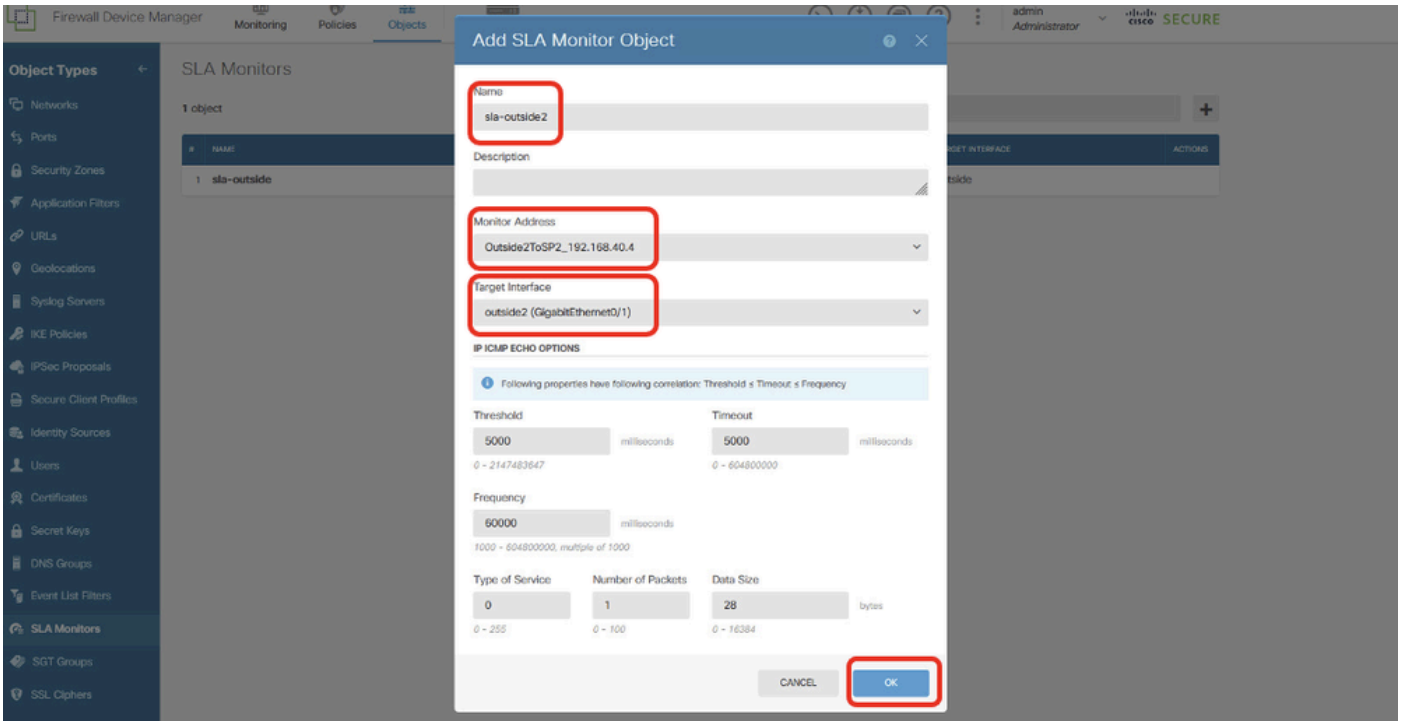
- Nombre: sla-outside
- Dirección del monitor: OutsideToSP1_192.168.30.3
- Interfaz de destino: outside(GigabitEthernet0/0)
- OPCIONES DE ECO ICMP IP: predeterminado



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

Paso 19.2. Continúe haciendo clic en el botón + para crear un nuevo monitor de SLA para el gateway ISP2. En la ventana Add SLA Monitor Object, proporcione la información necesaria para el gateway ISP2. Haga clic en el botón OK para guardar.

- Nombre: sla-outside2
- Dirección del monitor: Outside2ToSP2_192.168.40.4
- Interfaz de destino: outside2(GigabitEthernet0/1)
- OPCIONES DE ECO ICMP IP: predeterminado



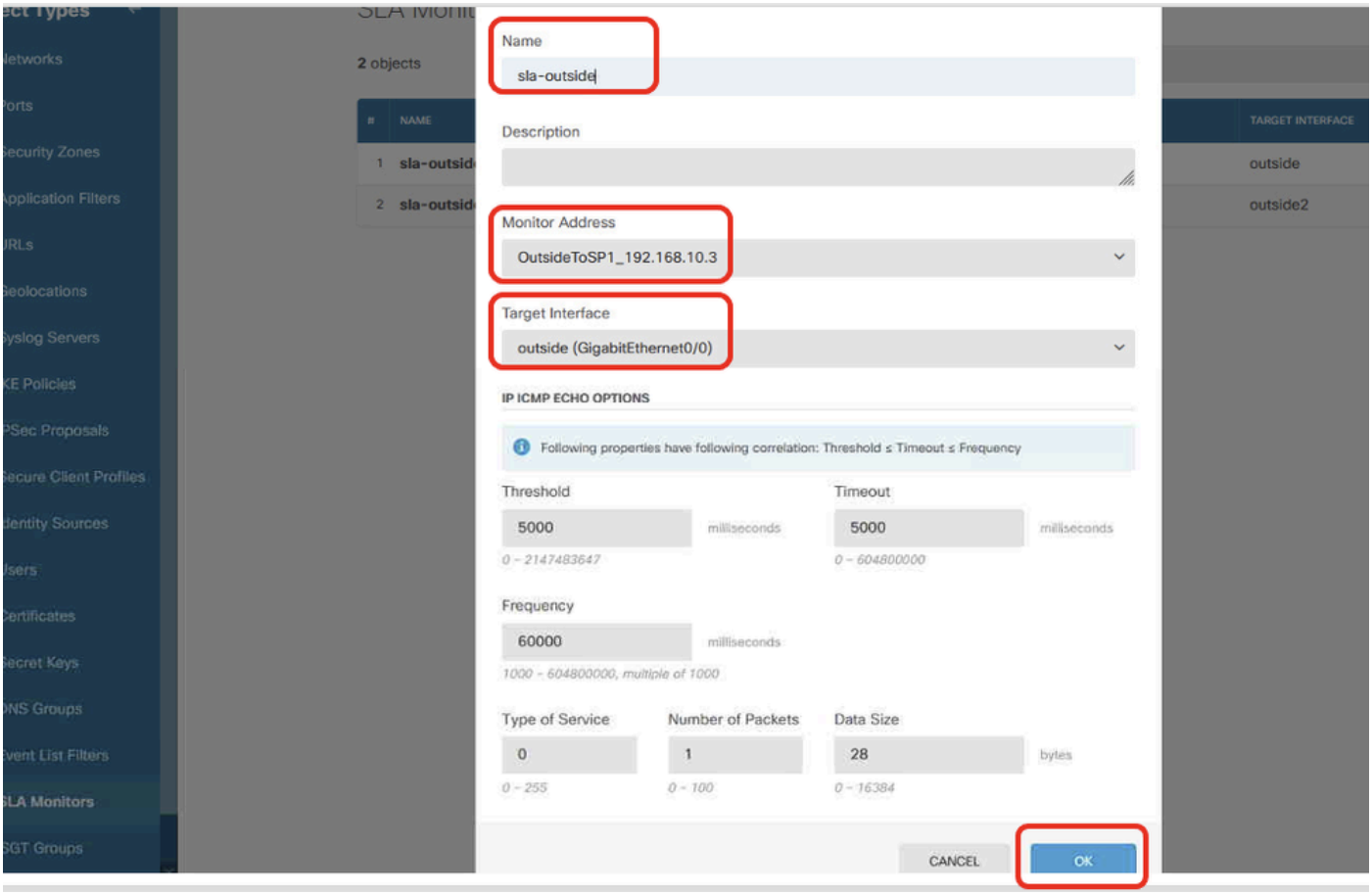
Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

Paso 20. Implemente los cambios de configuración.

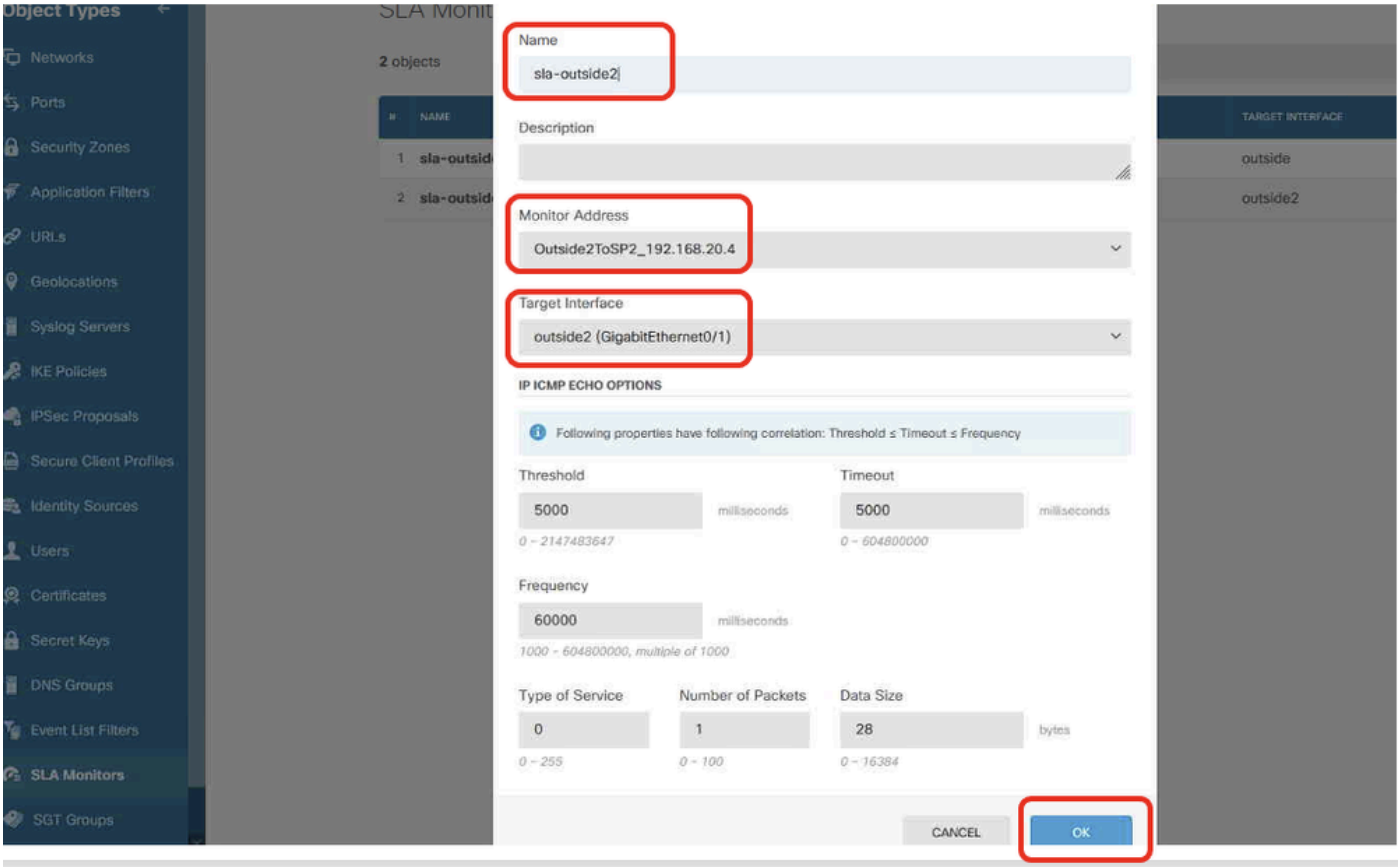
Site1FTD_Deployment_Changes

Configuración del Monitor FTD SLA de Site2

Paso 21. Repita el Paso 18. al Paso 20. cree el Monitor de SLA con los parámetros correspondientes en el FTD del Sitio 2.



Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

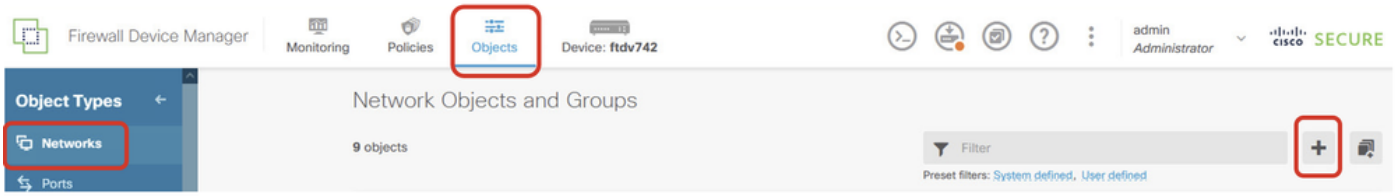


Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

Configuraciones en ruta estática

Configuración de la Ruta Estática FTD Site1

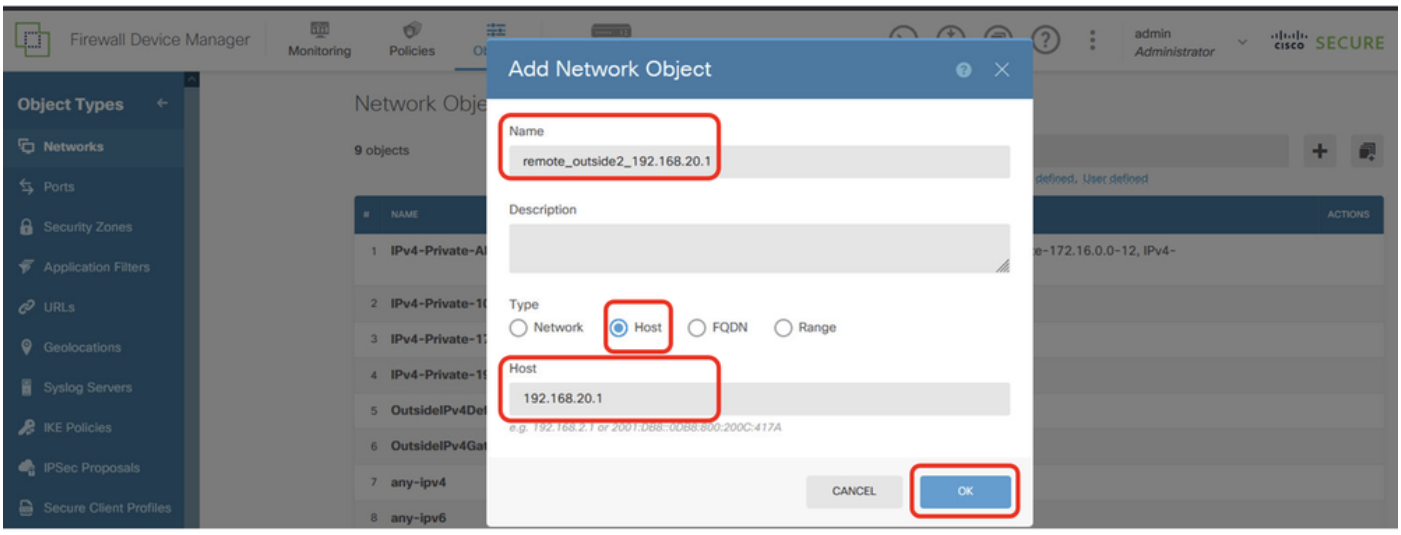
Paso 22. Cree nuevos objetos de red para que los utilice la ruta estática del FTD de Site1. Navegue hasta Objetos > Redes, haga clic en el botón +.



Site1FTD_Create_Obj

Paso 2.1. Crear objeto para la dirección IP outside2 del FTD Site2 del par. Proporcionar la información necesaria. Haga clic en el botón Aceptar.

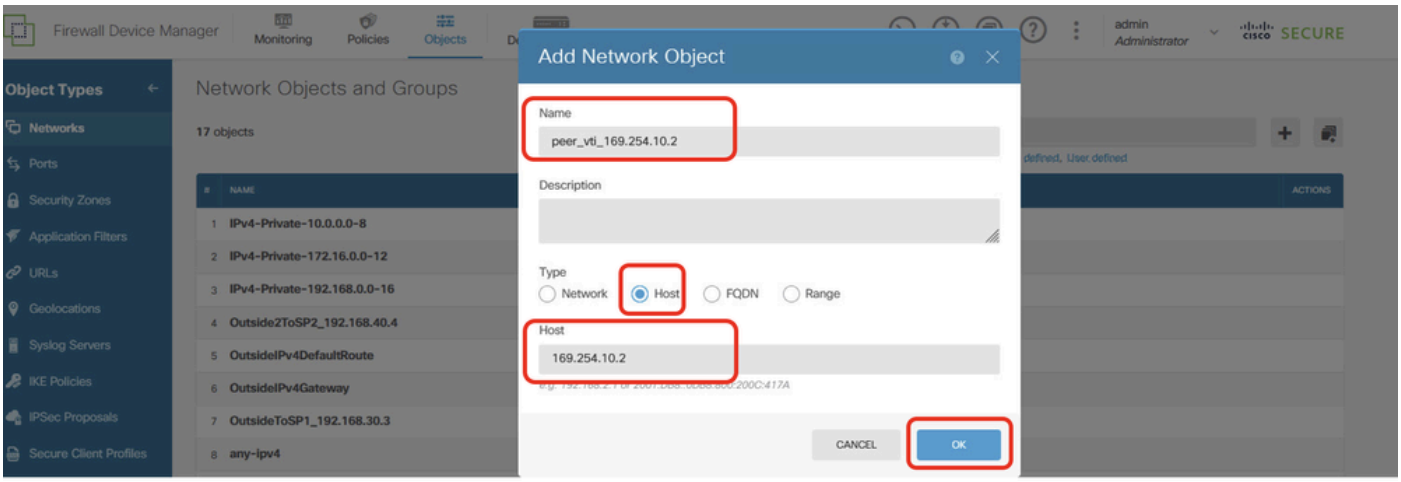
- Nombre: remote_outside2_192.168.20.1
- Tipo: ANFITRIÓN
- Red: 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

Paso 2.2. Crear objeto para la dirección IP del túnel VTI1 del FTD del sitio 2 del par. Proporcionar la información necesaria. Haga clic en el botón Aceptar.

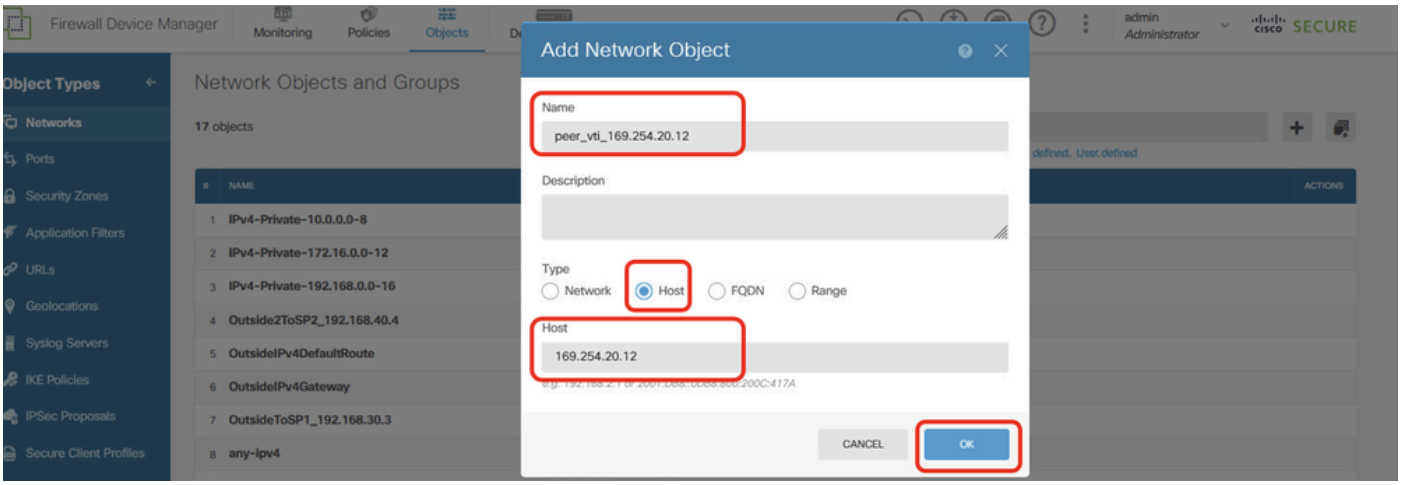
- Nombre: peer_vti_169.254.10.2
- Tipo: ANFITRIÓN
- Red:169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

Paso 2.3. Crear objeto para la dirección IP del túnel VTI2 del FTD del sitio 2 del par. Proporcionar la información necesaria. Haga clic en el botón Aceptar.

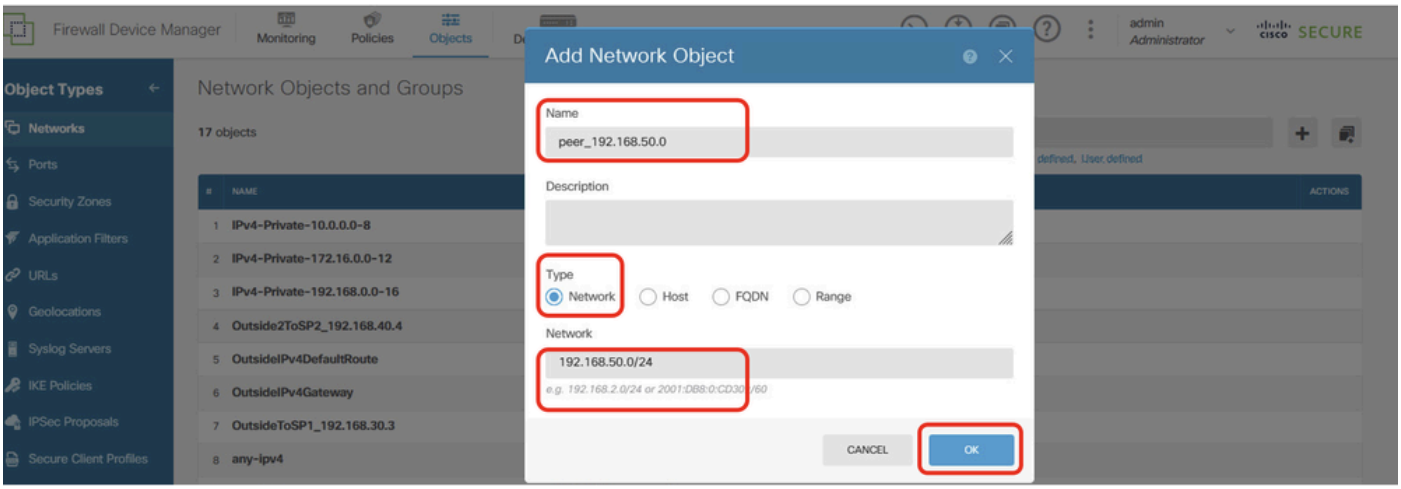
- Nombre: peer_vti_169.254.20.12
- Tipo: ANFITRIÓN
- Red:169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

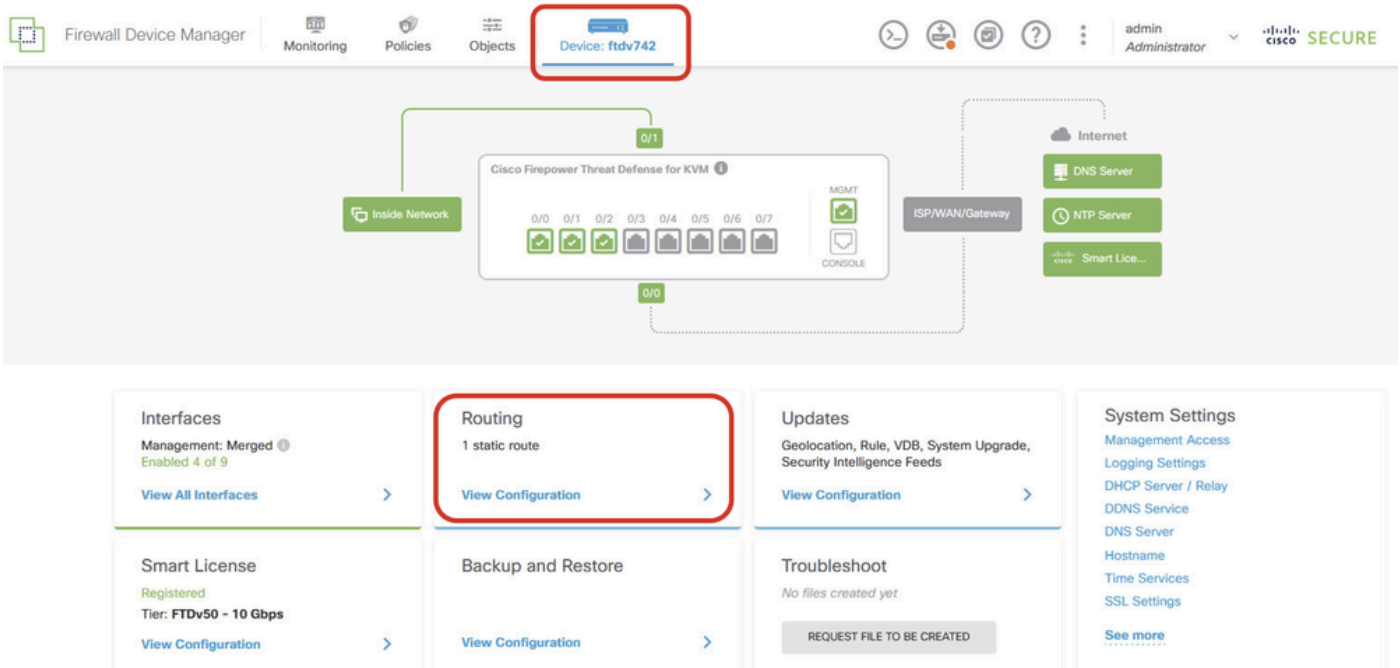
Paso 22.4. Crear objeto para la red interna del FTD del sitio 2 del par. Proporcionar la información necesaria. Haga clic en el botón Aceptar.

- Nombre: peer_192.168.50.0
- Tipo: RED
- Red:192.168.50.0/24

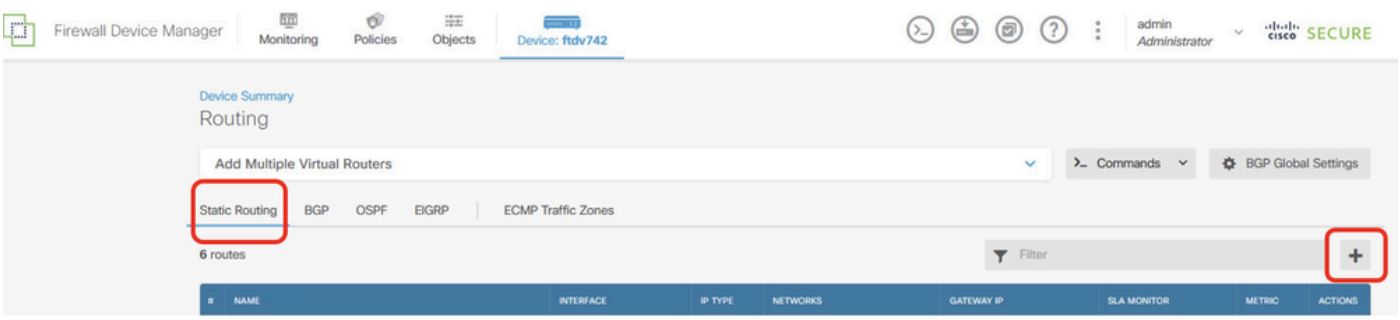


Site1FTD_Create_NetObj_StaticRoute_4

Paso 23. Navegue hasta Dispositivo > Ruteo. Haga clic en Ver configuración. Haga clic en la pestaña Static Routing. Haga clic en el botón + para agregar una nueva ruta estática.



Site1FTD_View_Route_Configuration

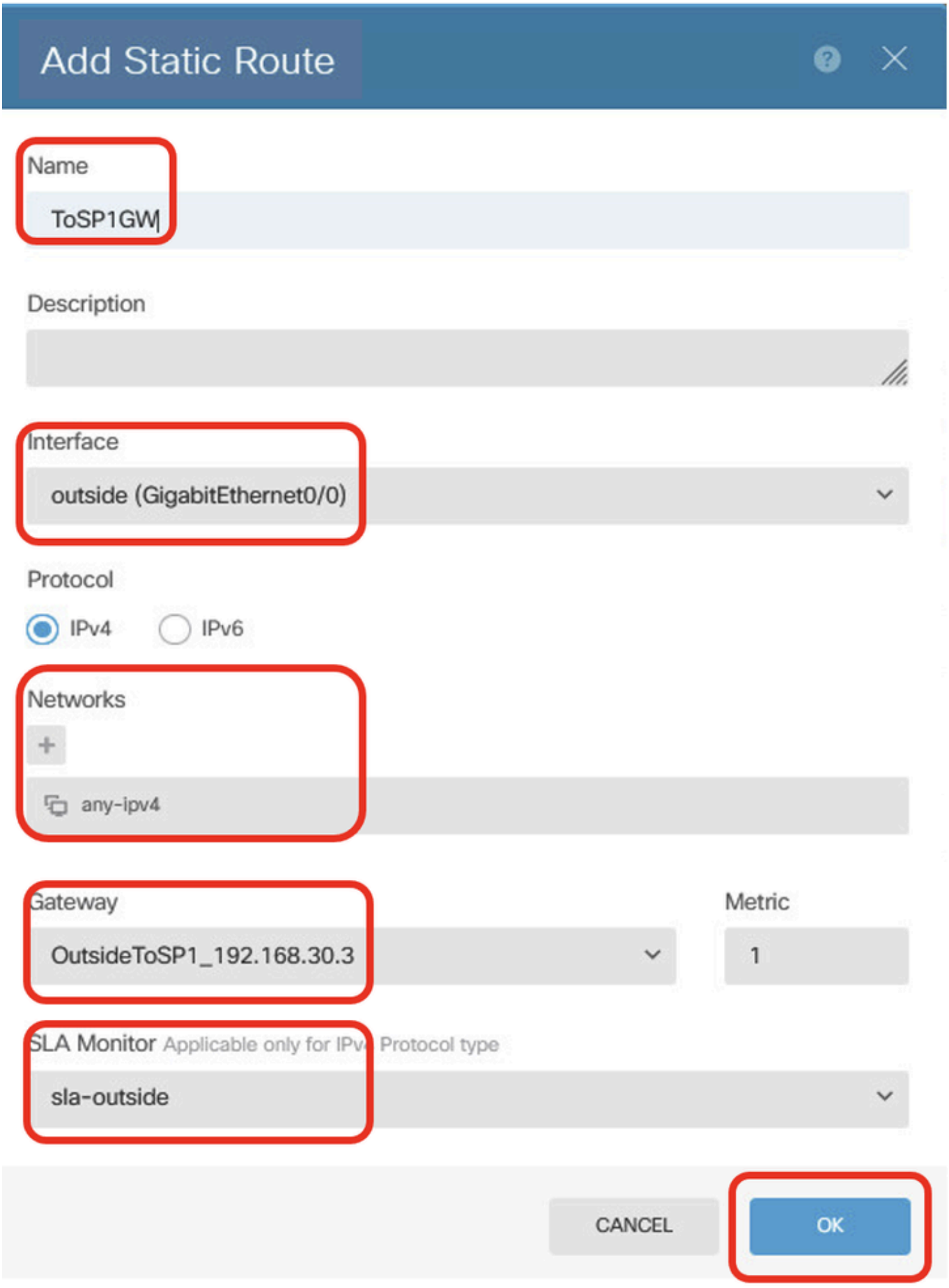


Site1FTD_Add_Static_Route

Paso 23.1. Cree una ruta predeterminada utilizando el gateway ISP1 con monitoreo SLA. Si el gateway ISP1 experimenta una interrupción, el tráfico cambia a la ruta predeterminada de copia

de seguridad a través de ISP2. Una vez que ISP1 se recupera, el tráfico vuelve a utilizar ISP1. Proporcione la información necesaria. Haga clic en el botón OK para guardar.

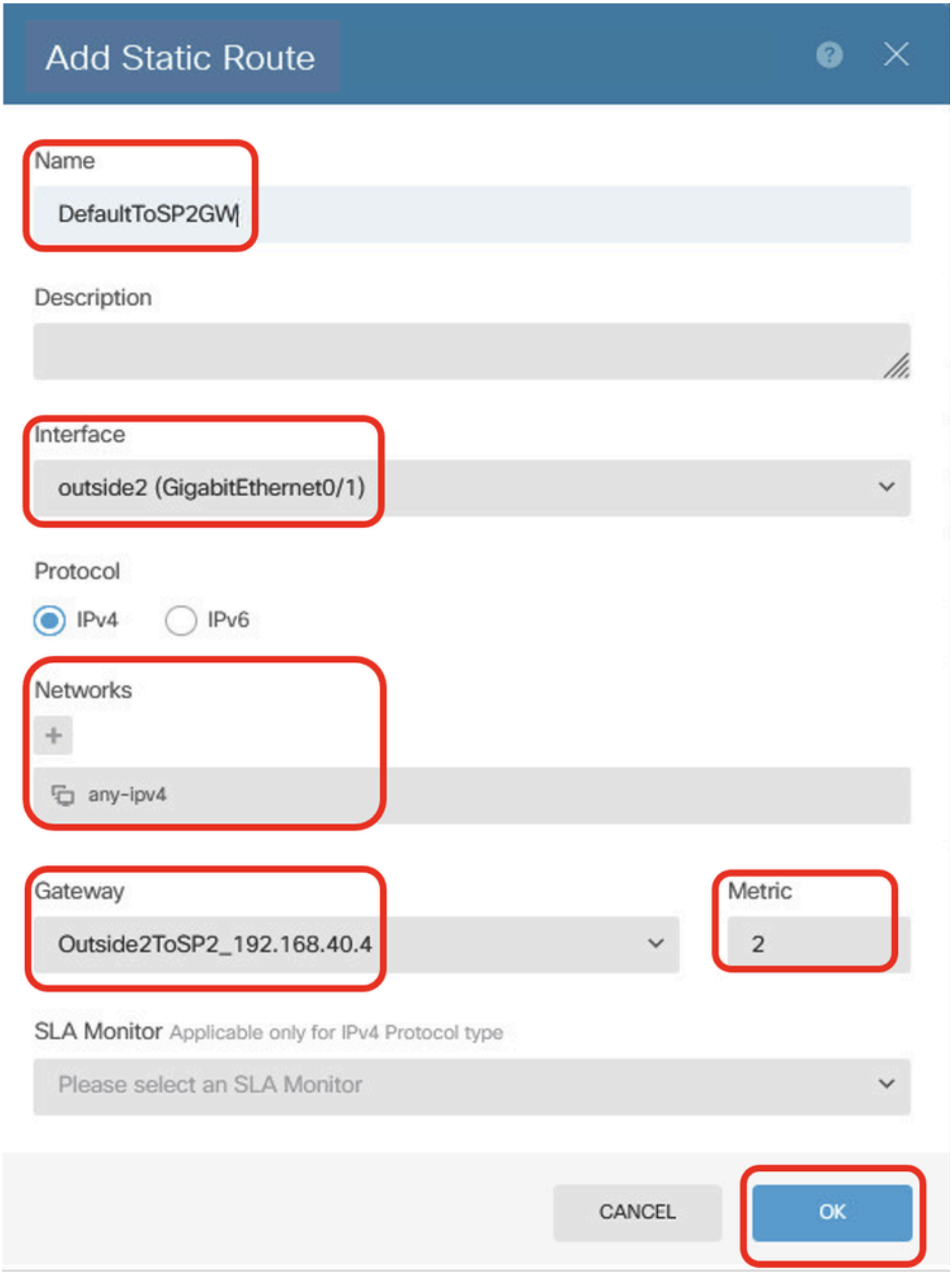
- Nombre: ToSP1GW
- Interfaz: outside(GigabitEthernet0/0)
- Protocolo: IPv4
- Redes: any-ipv4
- Gateway: OutsideToSP1_192.168.30.3
- Métrico: 1
- Supervisión de SLA: sla-outside



Site1FTD_Create_StaticRoute_1

Paso 23.2. Crear una ruta predeterminada de respaldo a través del gateway ISP2 gateway. La métrica debe ser mayor que 1. En este ejemplo, la métrica es 2. Proporcione la información necesaria. Haga clic en el botón OK para guardar.

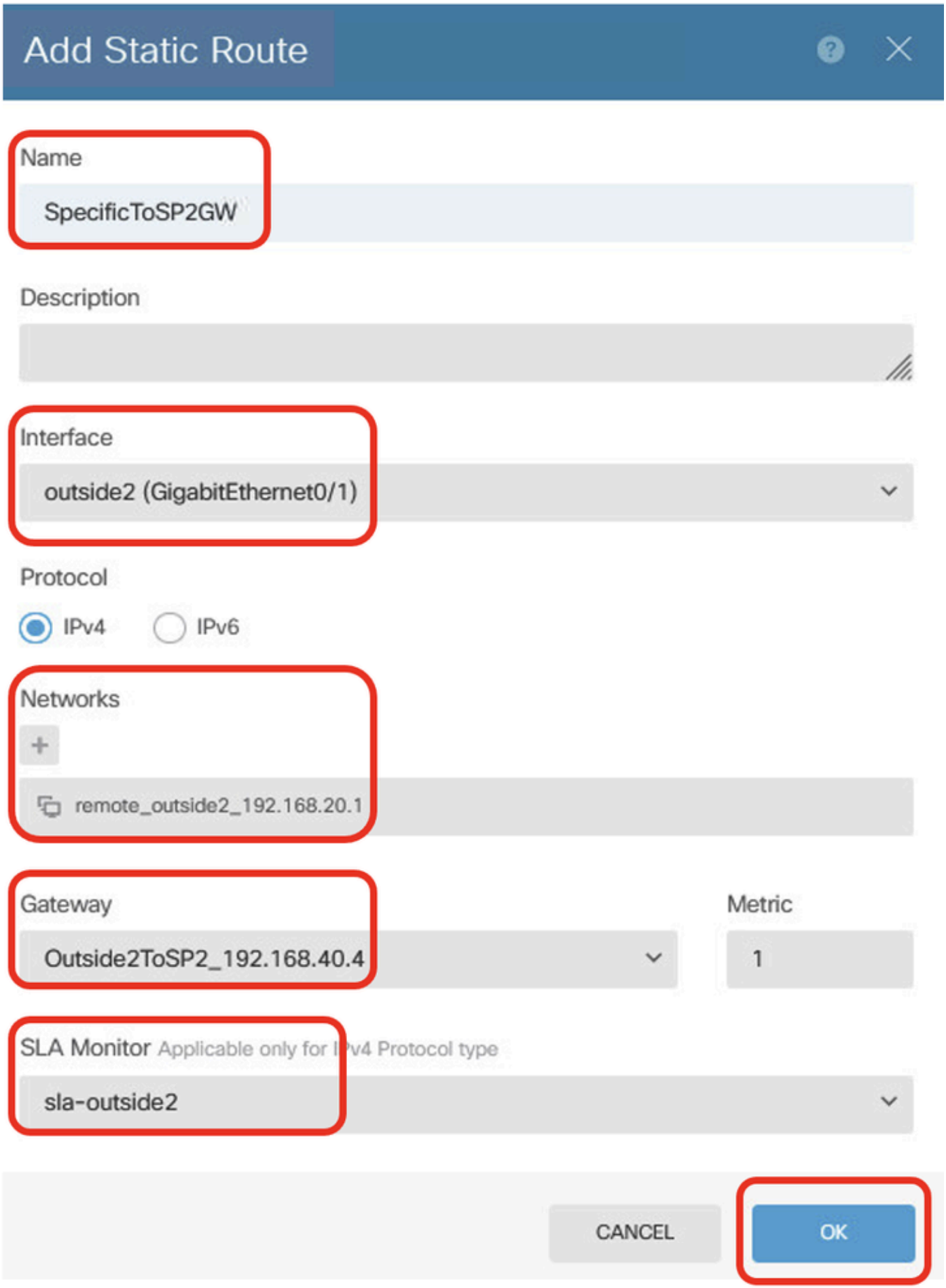
- Nombre: DefaultToSP2GW
- Interfaz: outside2(GigabitEthernet0/1)
- Protocolo: IPv4
- Redes: any-ipv4
- Gateway: Outside2ToSP2_192.168.40.4
- Métrico: 2



Site1FTD_Create_StaticRoute_2

Paso 23.3. Crear una ruta estática para el tráfico de destino a la dirección IP outside2 del FTD del sitio2 a través del gateway ISP2, con supervisión de SLA, utilizada para establecer VPN con outside2 del FTD del sitio2. Proporcionar la información necesaria. Haga clic en el botón OK para guardar.

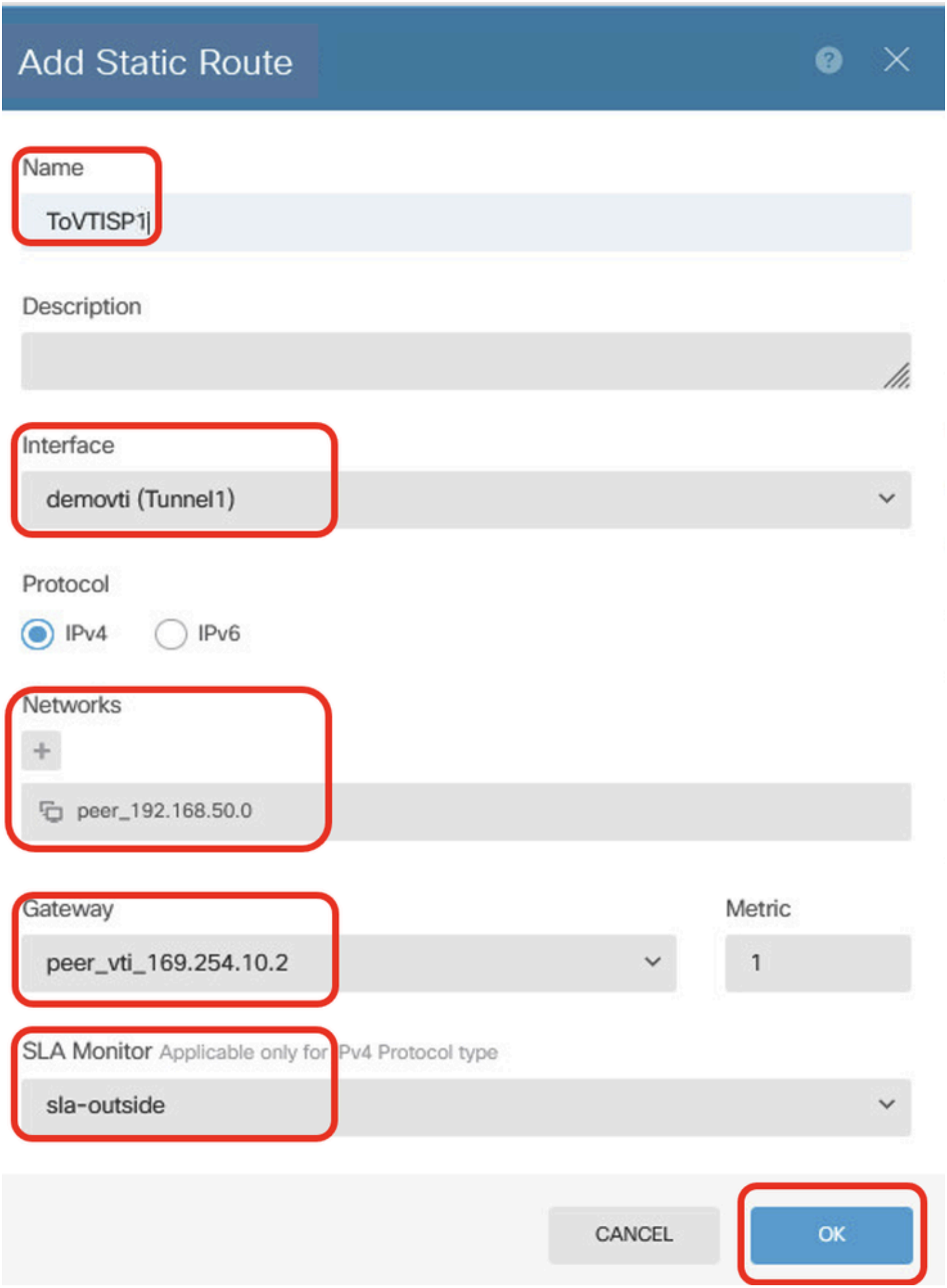
- Nombre: SpecificToSP2GW
- Interfaz: outside2(GigabitEthernet0/1)
- Protocolo: IPv4
- Redes: remote_outside2_192.168.20.1
- Gateway: Outside2ToSP2_192.168.40.4
- Métrico: 1
- Supervisión de SLA: sla-outside2



Site1FTD_Create_StaticRoute_3

Paso 23.4. Cree una ruta estática para el tráfico de destino a la red interna del FTD del sitio 2 a través del túnel VTI 1 del FTD del sitio 2 como gateway, con monitoreo SLA para cifrar el tráfico del cliente a través del túnel 1. Si el gateway ISP1 experimenta una interrupción, el tráfico VPN cambia al túnel VTI 2 del ISP2. Una vez que se recupera el ISP1, el tráfico vuelve al túnel VTI 1 del ISP1. Proporcione la información necesaria. Haga clic en el botón OK para guardar.

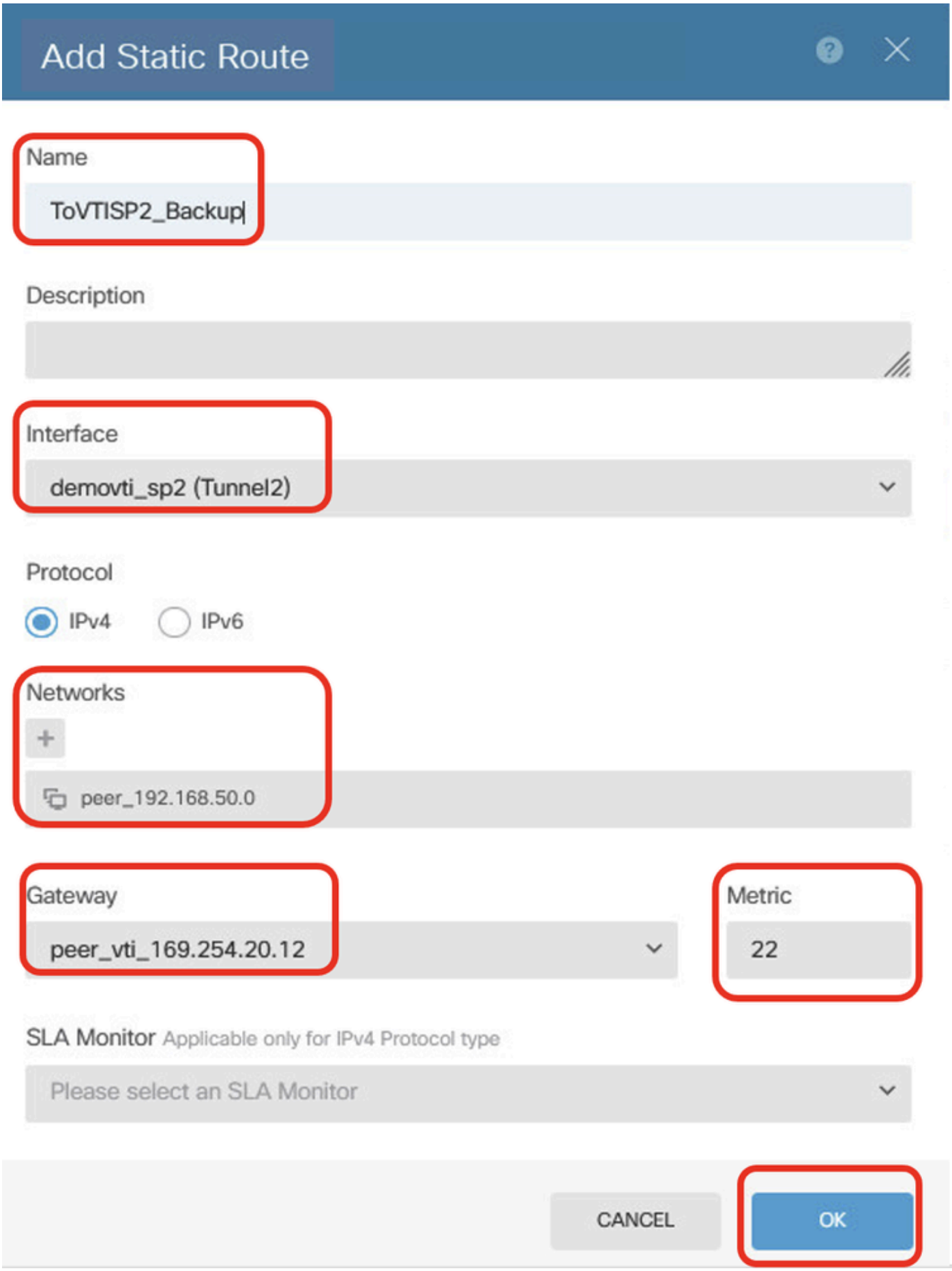
- Nombre: ToVTISP1
- Interfaz: demovti(Túnel1)
- Protocolo: IPv4
- Redes: peer_192.168.50.0
- Gateway: peer_vti_169.254.10.2
- Métrico: 1
- Supervisión de SLA: sla-outside



Site1FTD_Create_StaticRoute_4

Paso 23.5. Cree una ruta estática de reserva para el tráfico de destino a la red interna del FTD de sitio2 a través del túnel VTI 2 del FTD de sitio2 como gateway, utilizado para cifrar el tráfico del cliente a través del túnel 2. Establezca la métrica en un valor superior a 1. En este ejemplo, la métrica es 22. Proporcione la información necesaria. Haga clic en el botón OK para guardar.

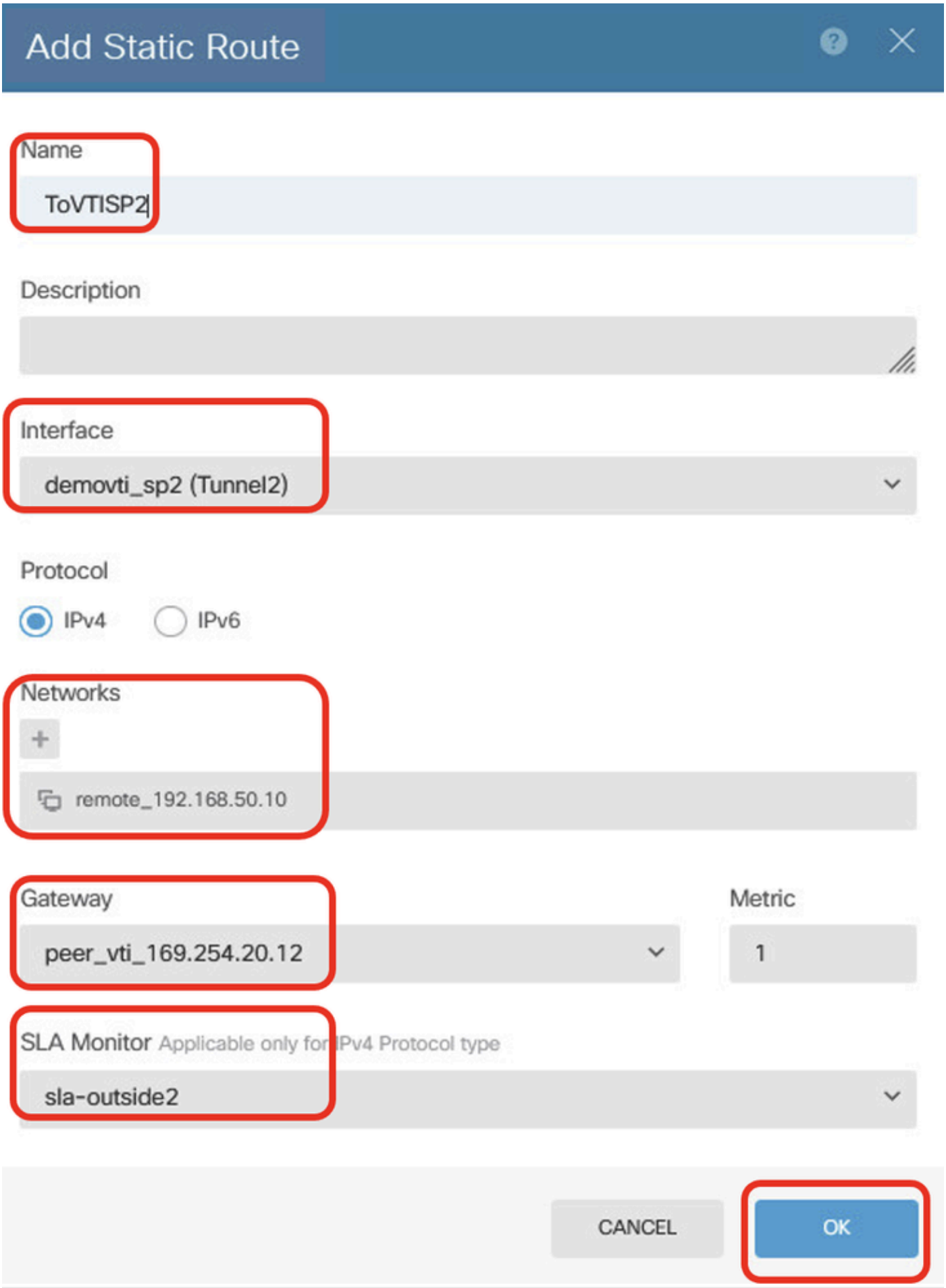
- Nombre: ToVTISP2_Backup
- Interfaz: demovti_sp2(Túnel2)
- Protocolo: IPv4
- Redes: peer_192.168.50.0
- Gateway: peer_vti_169.254.20.12
- Métrico: 22



Site1FTD_Create_StaticRoute_5

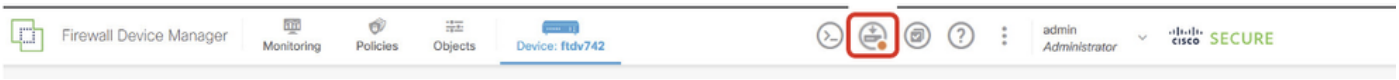
Paso 23.6. Crear una ruta estática para el tráfico PBR. Tráfico de destino al cliente 2 del sitio 2 a través del túnel 2 VTI del FTD del sitio 2 como gateway, con supervisión de SLA. Proporcione la información necesaria. Haga clic en el botón OK para guardar.

- Nombre: ToVTISP2
- Interfaz: demovti_sp2(Túnel2)
- Protocolo: IPv4
- Redes: remote_192.168.50.10
- Gateway: peer_vti_169.254.20.12
- Métrico: 1
- Supervisión de SLA: sla-outside2



Site1FTD_Create_StaticRoute_6

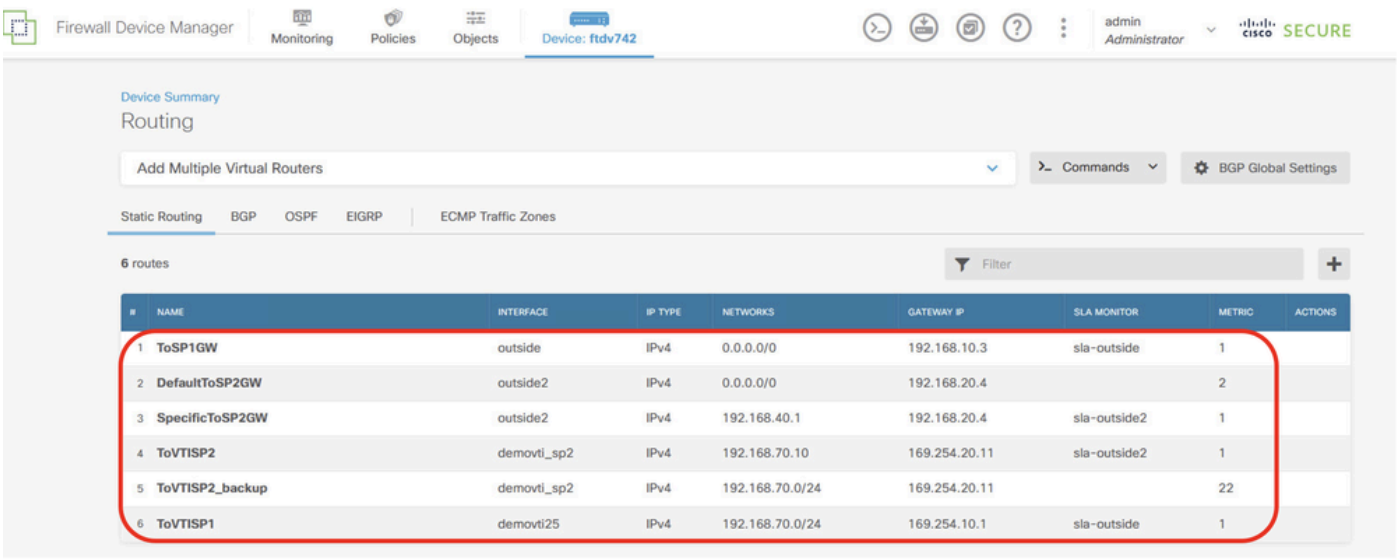
Paso 24. Implemente los cambios de configuración.



Site1FTD_Deployment_Changes

Configuración de la Ruta Estática FTD Site2

Paso 25. Repita los pasos 22 a 24 para crear una ruta estática con los parámetros correspondientes para FTD Site2.



Site2FTD_Create_StaticRoute

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente. Navegue hasta la CLI de FTD de Sitio1 y FTD de Sitio2 a través de la consola o SSH.

Tanto ISP1 como ISP2 funcionan correctamente

VPN

```
//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1072332533 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1045734377 192.168.40.1/500                               192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d
```

```
// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
499259237 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607
```

Ruta

```
// Site1 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
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside
```

```
// Site2 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

Monitor SLA

```
// Site1 FTD:
```

```
ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:


ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

```
Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

// Site2 FTD:

```
ftdv742#  show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
```

```
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100

Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

Prueba de ping

Situación 1. Cliente del sitio 1: ping del sitio 2 Cliente 1.

Antes de hacer ping, verifique los contadores de show crypto ipsec sa | inc interface:|encap|decap en FTD Site1.

En este ejemplo, Tunnel1 muestra 1497 paquetes para encapsulación y 1498 paquetes para desencapsulación.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
```

```
      #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
      #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 correctamente.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/97/227 ms
```

Verifique los contadores de show crypto ipsec sa | inc interface:|encap|decap en FTD Site1 después de realizar un ping correctamente.

En este ejemplo, el Túnel 1 muestra 1502 paquetes para encapsulación y 1503 paquetes para desencapsulación, con ambos contadores aumentando en 5 paquetes, coincidiendo con las 5 solicitudes de eco de ping. Esto indica que los pings del Cliente1 del Sitio1 al Cliente1 del Sitio2 se enrutan a través del Túnel 1 del ISP1. El Túnel 2 no muestra ningún aumento en los contadores de encapsulación o desencapsulación, lo que confirma que no se está utilizando para este tráfico.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
      #pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Escenario 2. Cliente del sitio12 ping Cliente2 del sitio2.

Antes de hacer ping, verifique los contadores de show crypto ipsec sa | inc interface:|encap|decap en FTD Site1.

En este ejemplo, Tunnel2 muestra 21 paquetes para encapsulación y 20 paquetes para desencapsulación.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2 ping Site2 Client2 correctamente.

```
Site1_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 = 4/39/87 ms
```

Verifique los contadores de show crypto ipsec sa | inc interface:|encap|decap en FTD Site1 después de realizar un ping correctamente.

En este ejemplo, el Túnel 2 muestra 26 paquetes para encapsulación y 25 paquetes para desencapsulación, con ambos contadores aumentando en 5 paquetes, coincidiendo con las 5 solicitudes de eco de ping. Esto indica que los pings del Cliente2 del Sitio1 al Cliente2 del Sitio2 se enrutan a través del Túnel 2 del ISP2. El Túnel 1 no muestra ningún aumento en los contadores de encapsulación o desencapsulación, lo que confirma que no se está utilizando para este tráfico.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP1 experimenta una interrupción mientras que ISP2 funciona bien

En este ejemplo, cierre manual de la interfaz E0/1 en ISP1 para simular que el ISP1 experimenta una interrupción.

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
Internet_SP1(config)#
```

VPN

El Túnel 1 se desactivó. Solo el túnel 2 está activo con IKEV2 SA.

```
// Site1 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.1, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.30.1
    Destination IP address: 192.168.10.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d


ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
1045734377 192.168.40.1/500                                      192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d




// Site2 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.2, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.10.1
    Destination IP address: 192.168.30.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
ftdv742#

ftdv742# show crypto ikev2 sa
```

```
IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500                      G
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

Ruta

En la tabla de rutas, las rutas de respaldo tienen efecto.

```
// Site1 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
Gateway of last resort is 192.168.40.4 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

Monitor SLA

En el FTD Site1, el monitor SLA muestra el tiempo de espera 855903900 (la dirección de destino es 192.168.30.3) para ISP1.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000

Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
```

```
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

ftdv742# show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Down
  7 changes, last change 00:11:03
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Up
  4 changes, last change 13:15:11
  Latest operation return code: OK
  Latest RTT (millisecs) 140
  Tracked by:
    STATIC-IP-ROUTING 0
```

Prueba de ping

Antes de hacer ping, verifique los contadores de show crypto ipsec sa | inc interface:|encap|decap en FTD Site1.

En este ejemplo, Tunnel2 muestra 36 paquetes para encapsulación y 35 paquetes para desencapsulación.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
      #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 correctamente.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/133/253 ms
```

Site1 Client2 ping Site2 Client2 correctamente.

```
Site1_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 = 34/56/87 ms
```

Verifique los contadores de show crypto ipsec sa | inc interface:|encap|decap en FTD Site1 después de realizar un ping correctamente.

En este ejemplo, el Túnel 2 muestra 46 paquetes para encapsulación y 45 paquetes para desencapsulación, con ambos contadores aumentando en 10 paquetes, coincidiendo con las 10 solicitudes de eco de ping. Esto indica que los paquetes ping se rutean a través del túnel 2 ISP2.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
      #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP2 experimenta una interrupción mientras que ISP1 funciona bien

En este ejemplo, cierre manual de la interfaz E0/1 en ISP2 para simular que el ISP2 experimenta una interrupción.

```
Internet_SP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

El Túnel 2 se cayó. Sólo el túnel 1 está activo con IKEV2 SA.

```
// Site1 FTD:

ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.11, subnet mask 255.255.255.0
  Tunnel Interface Information:
```

```
    Source interface: outside2    IP address: 192.168.40.1
    Destination IP address: 192.168.20.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1375077093 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc




// Site2 FTD:

ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.12, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.20.1
    Destination IP address: 192.168.40.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1025640731 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

Ruta

En la tabla de rutas, la ruta relacionada con ISP2 desapareció para el tráfico PBR.

```
// Site1 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
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

Monitor SLA

En el FTD Site1, el monitor SLA muestra el tiempo de espera 188426425 (la dirección de destino es 192.168.40.4) para ISP2.

```
// Site1 FTD:
```

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100


ftdv742#  show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Up
  8 changes, last change 00:14:37
  Latest operation return code: OK
  Latest RTT (millisecs) 60
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Down
  5 changes, last change 00:09:30
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

Prueba de ping

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

en FTD Site1.

En este ejemplo, el Túnel 1 muestra 74 paquetes para encapsulación y 73 paquetes para desencapsulación.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
      #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 correctamente.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/158/255 ms
```

Site1 Client2 ping Site2 Client2 correctamente.

```
Site1_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 = 6/58/143 ms
```

Verifique los contadores de show crypto ipsec sa | inc interface:|encap|decap en FTD Site1 después de realizar un ping correctamente.

En este ejemplo, el Túnel 1 muestra 84 paquetes para encapsulación y 83 paquetes para desencapsulación, con ambos contadores aumentando en 10 paquetes, coincidiendo con las 10 solicitudes de eco de ping. Esto indica que los paquetes ping se rutean a través del Túnel 1 ISP1.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
      #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
      #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 estos 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 estos comandos debug para resolver problemas de la sección PBR.

```
debug policy-route
```

Puede utilizar estos comandos debug para resolver problemas de la sección Monitor SLA.

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

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).