Configuración de BGP sobre VPN basada en ruta en FTD administrado por FDM

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Configurar

- Diagrama de la red
- Configuraciones en VPN
- Configuraciones en BGP

Verificación

Troubleshoot

Introducción

Este documento describe la configuración de BGP a través de VPN de sitio a sitio basada en ruta en FTDv administrado por FirePower Device Manager (FDM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de VPN
- Configuraciones BGP en FTDv
- Experiencia con FDM

Componentes Utilizados

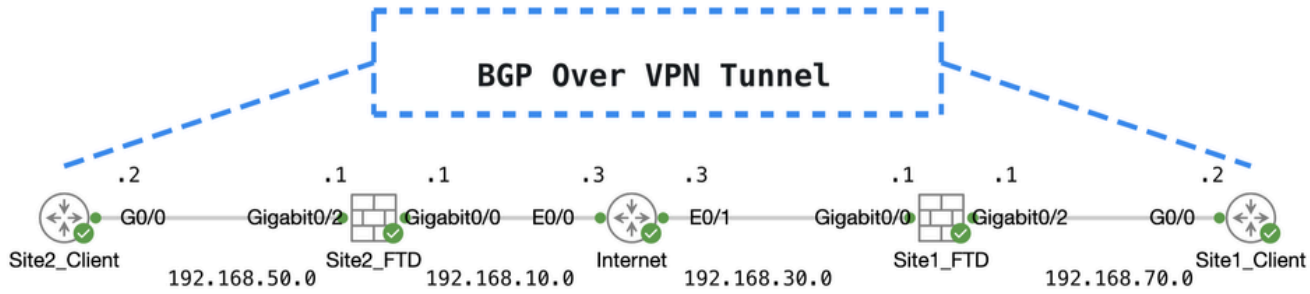
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 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.

Configurar

Diagrama de la red



Topo

Configuraciones en VPN

Paso 1. Asegúrese de que la interconectividad IP entre nodos esté lista y estable. La licencia inteligente de FDM se ha registrado correctamente con la cuenta inteligente.

Paso 2. La puerta de enlace del cliente Site1 se configura con la dirección IP interna del FTD Site1 (192.168.70.1). La puerta de enlace del cliente Site2 se configura con la dirección IP interior del FTD Site2 (192.168.50.1). Además, asegúrese de que la ruta predeterminada en ambos FTD esté configurada correctamente después de la inicialización de FDM.

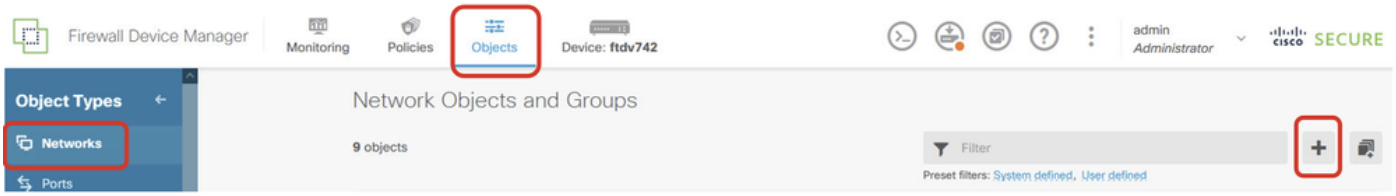
Inicie sesión en la GUI de cada FDM. Vaya a .Device > Routing Haga clic enView Configuration. Haga clic en la **Static Routing** pestaña para verificar la ruta estática predeterminada.

Site1_FTD_Gateway

Site2_FTD_Gateway

Paso 3. Configure la VPN de sitio a sitio basada en rutas. En este ejemplo, configure primero el FTD Site1.

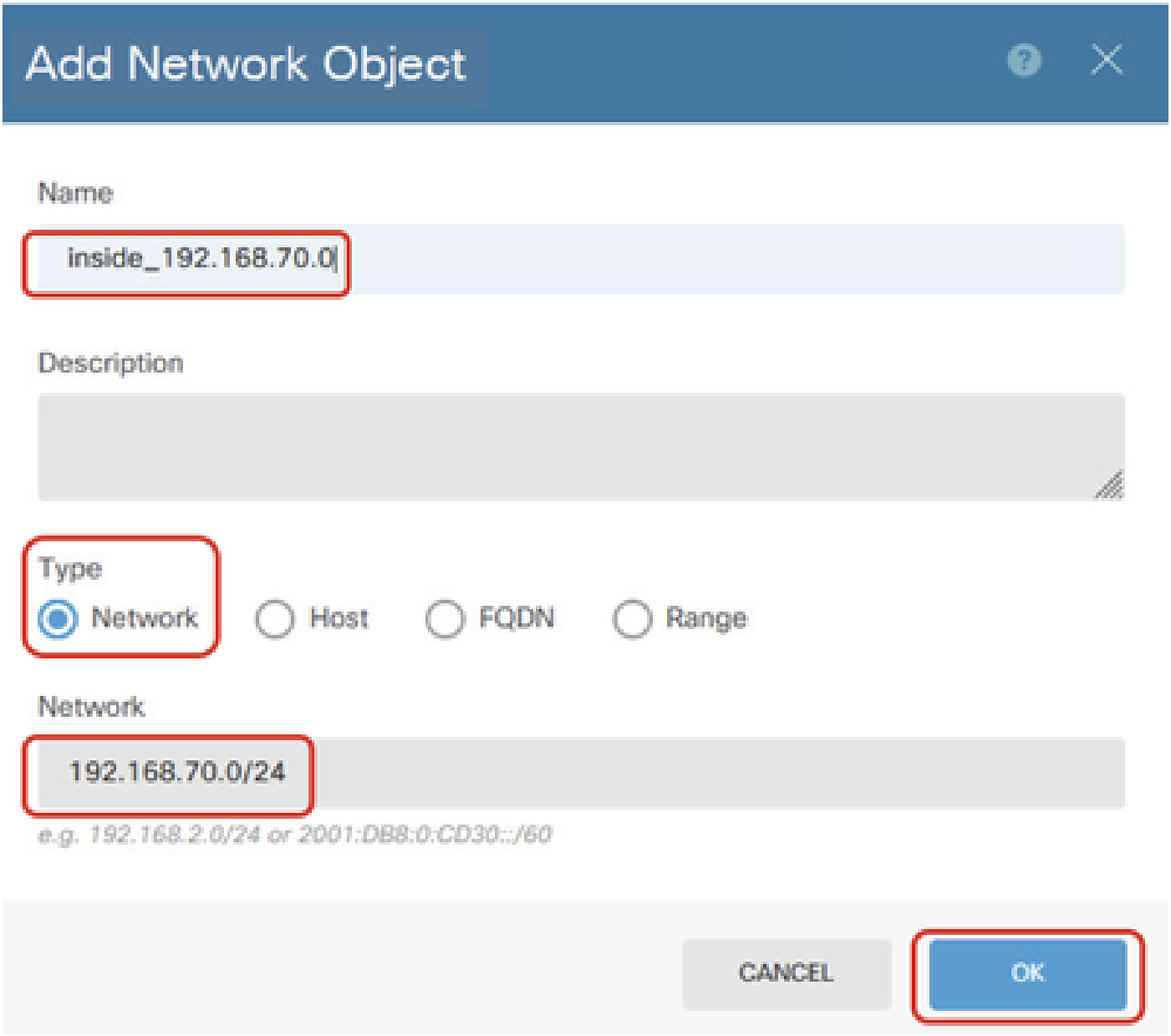
Paso 3.1. Inicie sesión en la GUI de FDM del FTD Site1. Cree un nuevo objeto de red para la red interna del FTD Site1. Desplácese hasta **Objects > Networks**, haga clic en el botón +.



Create_Network_Object

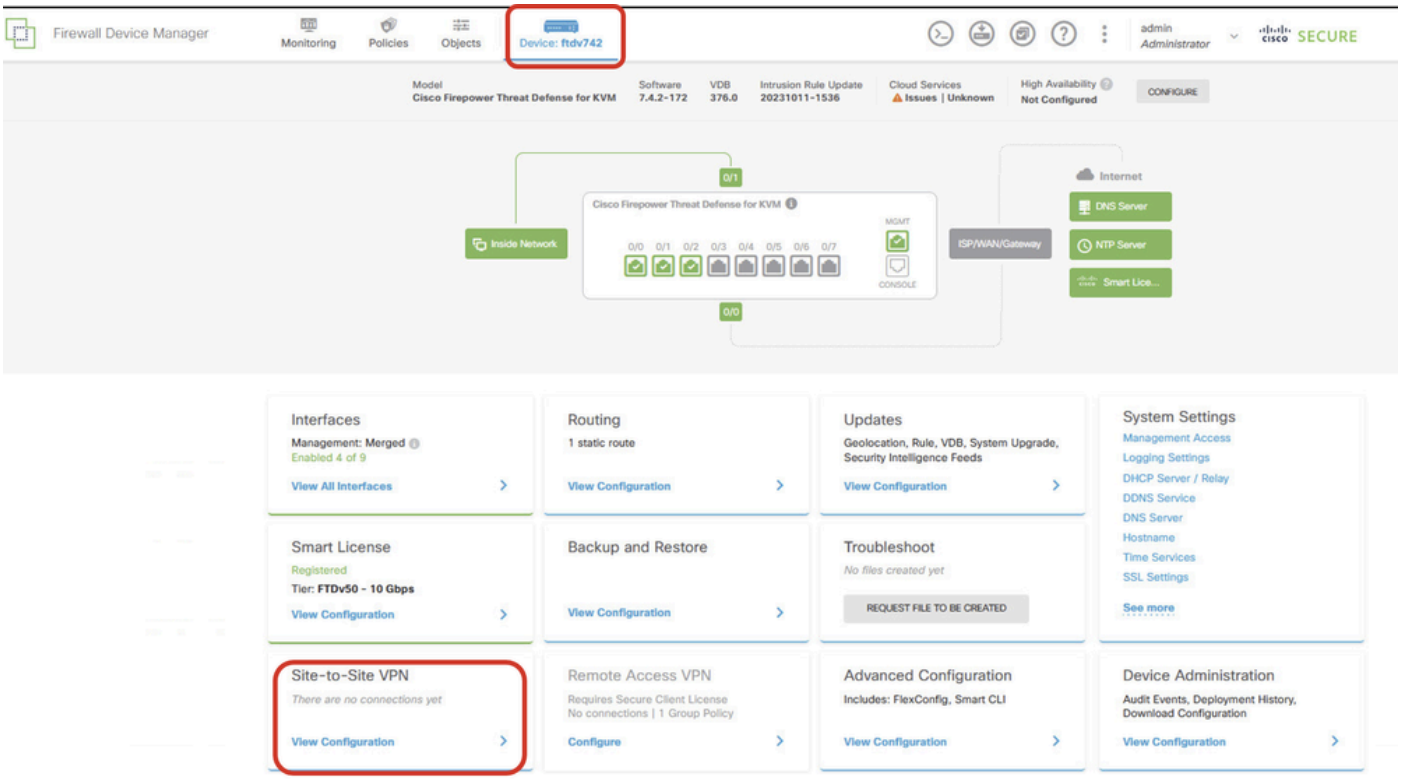
Paso 3.2. Proporcione la información necesaria. Haga clic en el**OK** botón.

- Nombre: inside_192.168.70.0
- Tipo: Red
- Red: 192.168.70.0/24



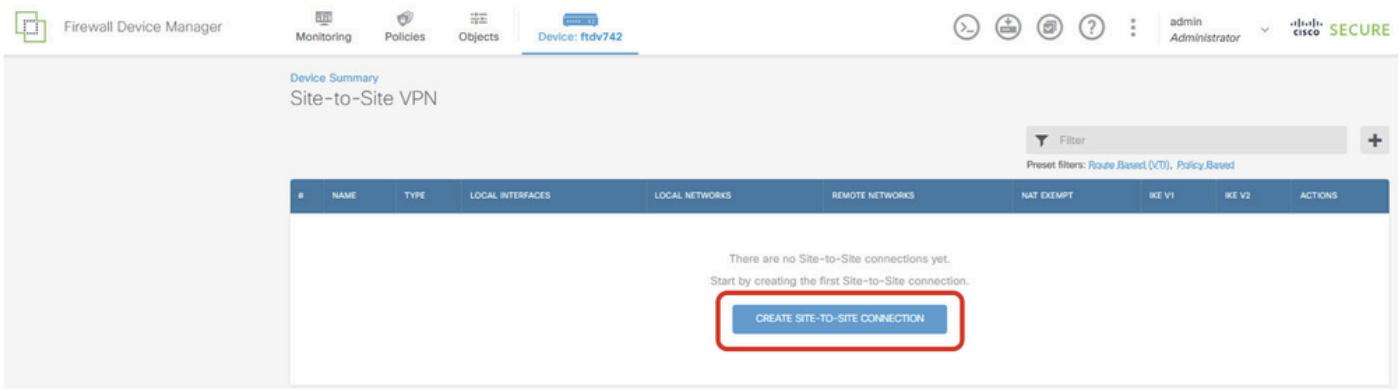
Sitio1_Red_interna

Paso 3.3. Vaya a **.Device > Site-to-Site VPN** Haga clic en **View Configuration .**



Ver VPN de sitio a sitio

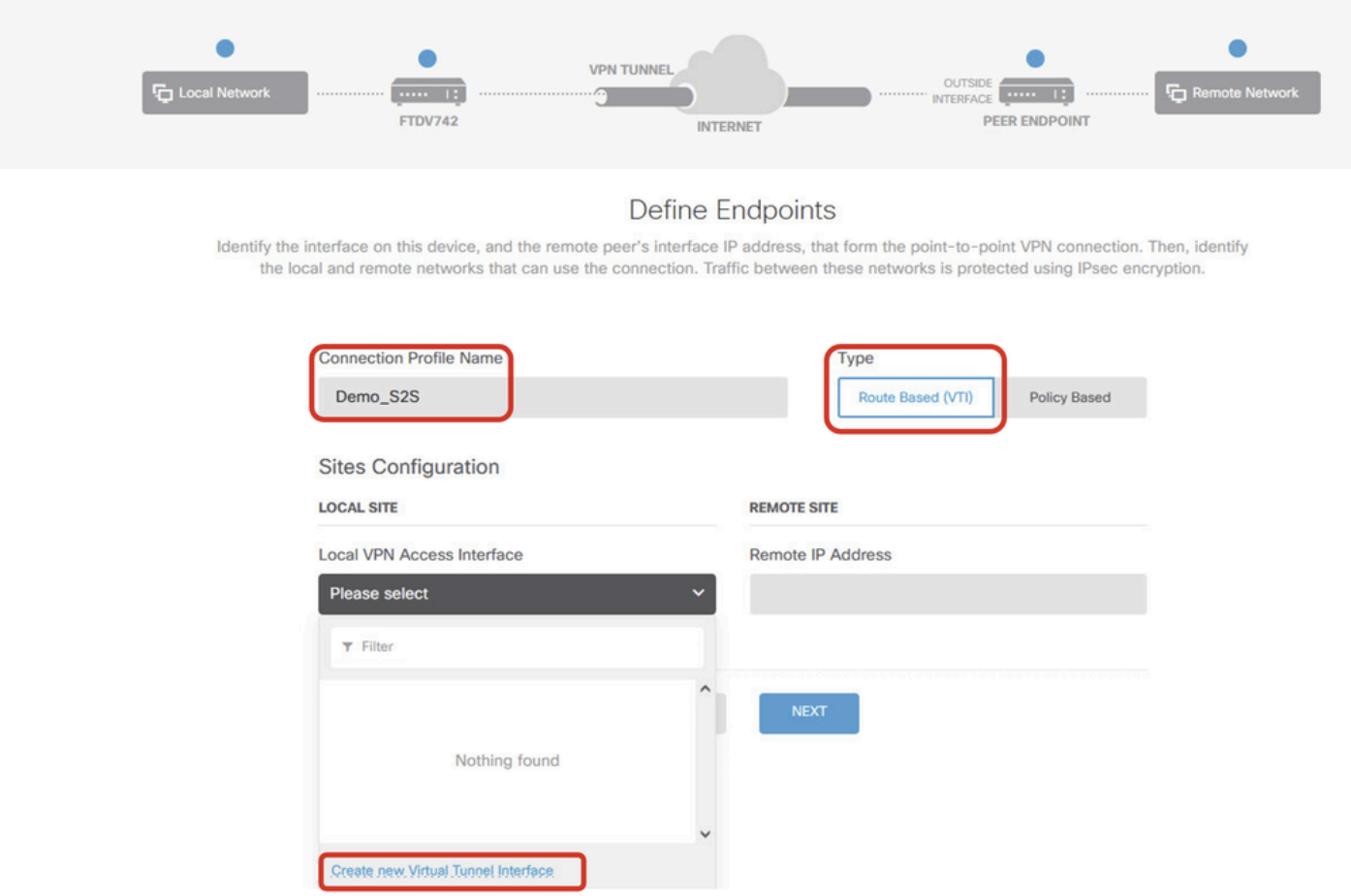
Paso 3.4. Comience a crear una nueva VPN de sitio a sitio. Haga clic en **CREATE SITE-TO-SITE CONNECTION** .



Create_Site-to-Site_Connection

Paso 3.5. Proporcione la información necesaria.

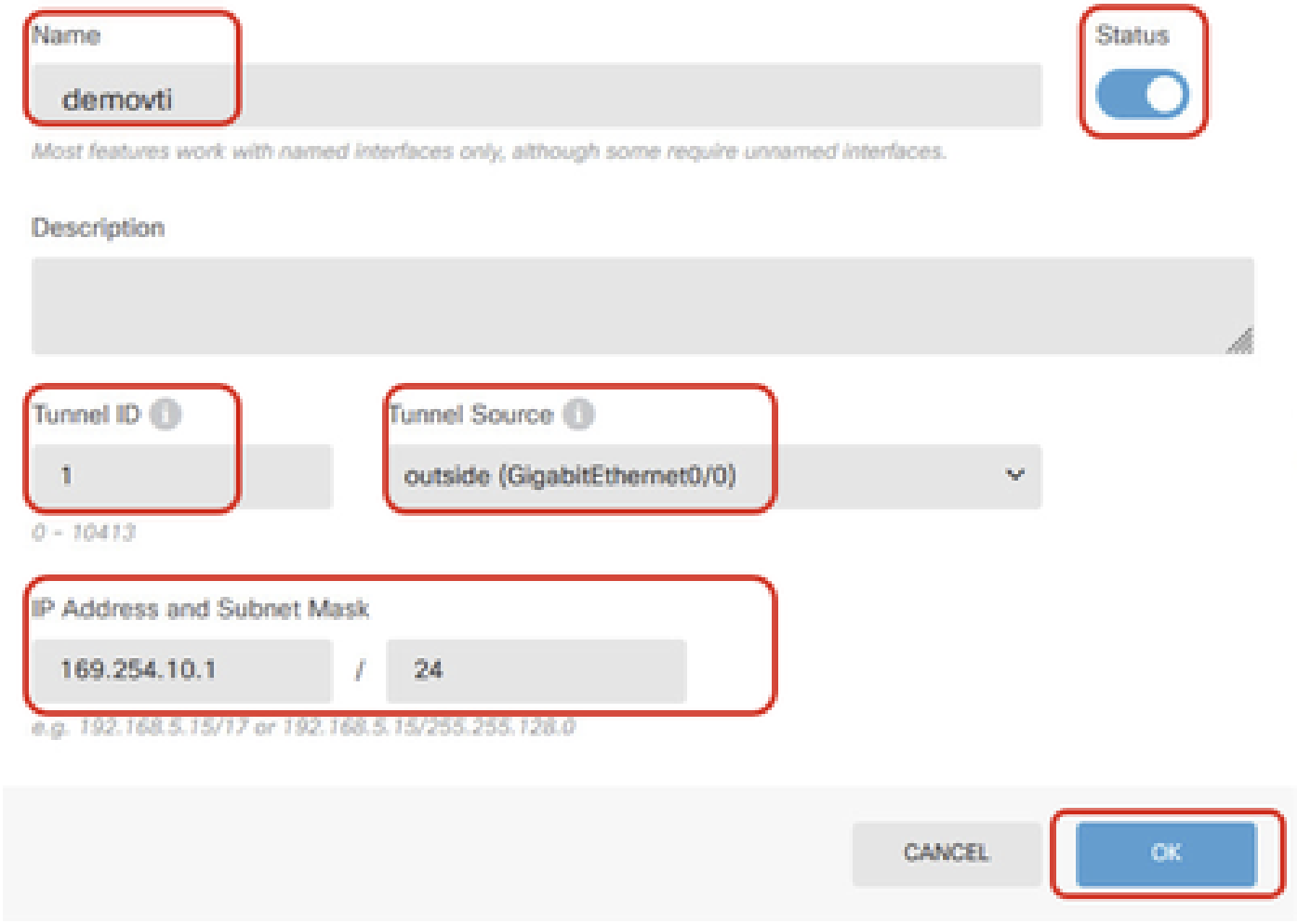
- Nombre del perfil de conexión: Demo_S2S
- Tipo: basado en ruta (VTI)
- Interfaz de acceso VPN local: haga clic en la lista desplegable y, a continuación, haga clic en **Create new Virtual Tunnel Interface** .



Create_VTI_in_VPN_Wizard

Paso 3.6. Proporcione la información necesaria para crear una nueva VTI. Haga clic en el botón OK (Aceptar)

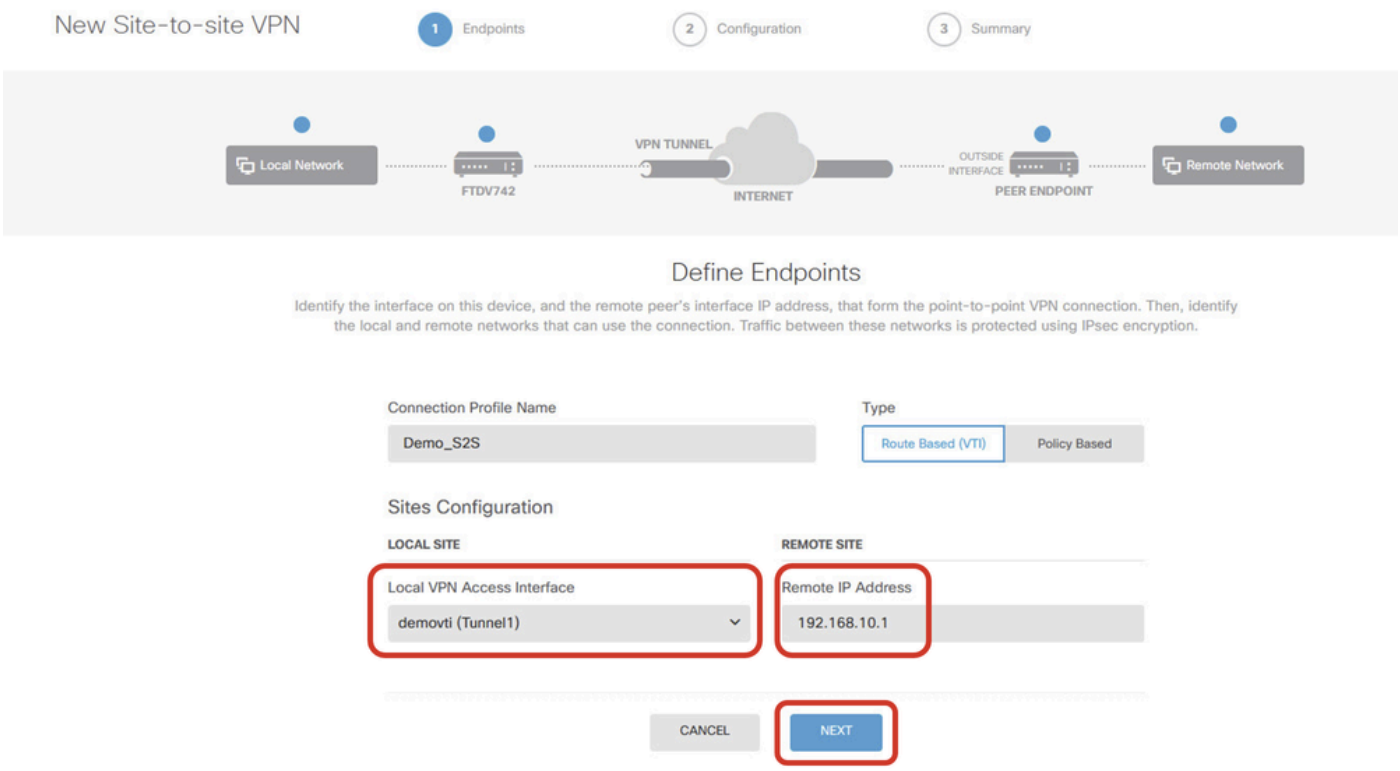
- Nombre: demovti
- ID de túnel: 1
- Fuente del túnel: exterior (GigabitEthernet0/0)
- Dirección IP Y Máscara De Subred: 169.254.10.1/24
- Estado: haga clic en el control deslizante hasta la posición Activado



Create_VTI_Details

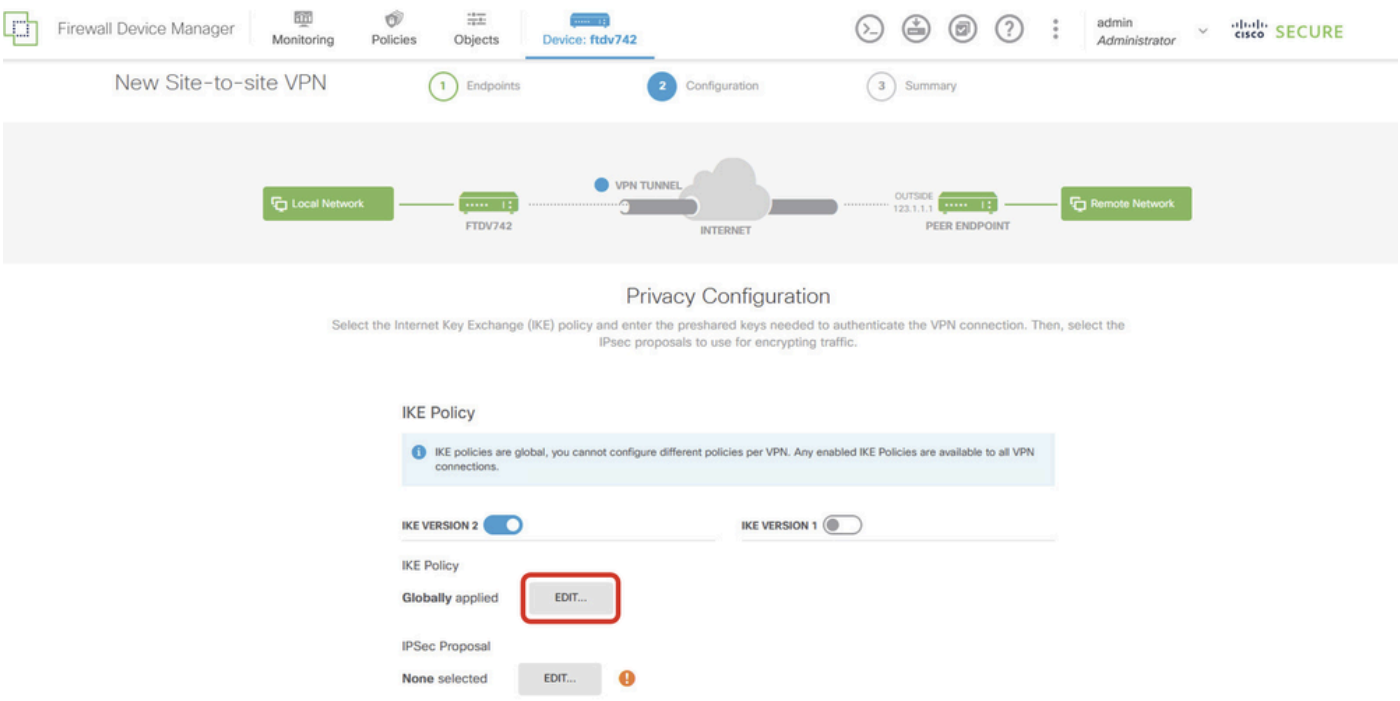
Paso 3.7. Continúe proporcionando la información necesaria. Haga clic en el botón NEXT.

- Interfaz de acceso VPN local: demovti (creada en el paso 3.6.1)
- Dirección IP remota: 192.168.10.1



VPN_Wizard_Endpoints_Step1

Paso 3.8. Vaya a Política IKE. Haga clic en el botón Editar.



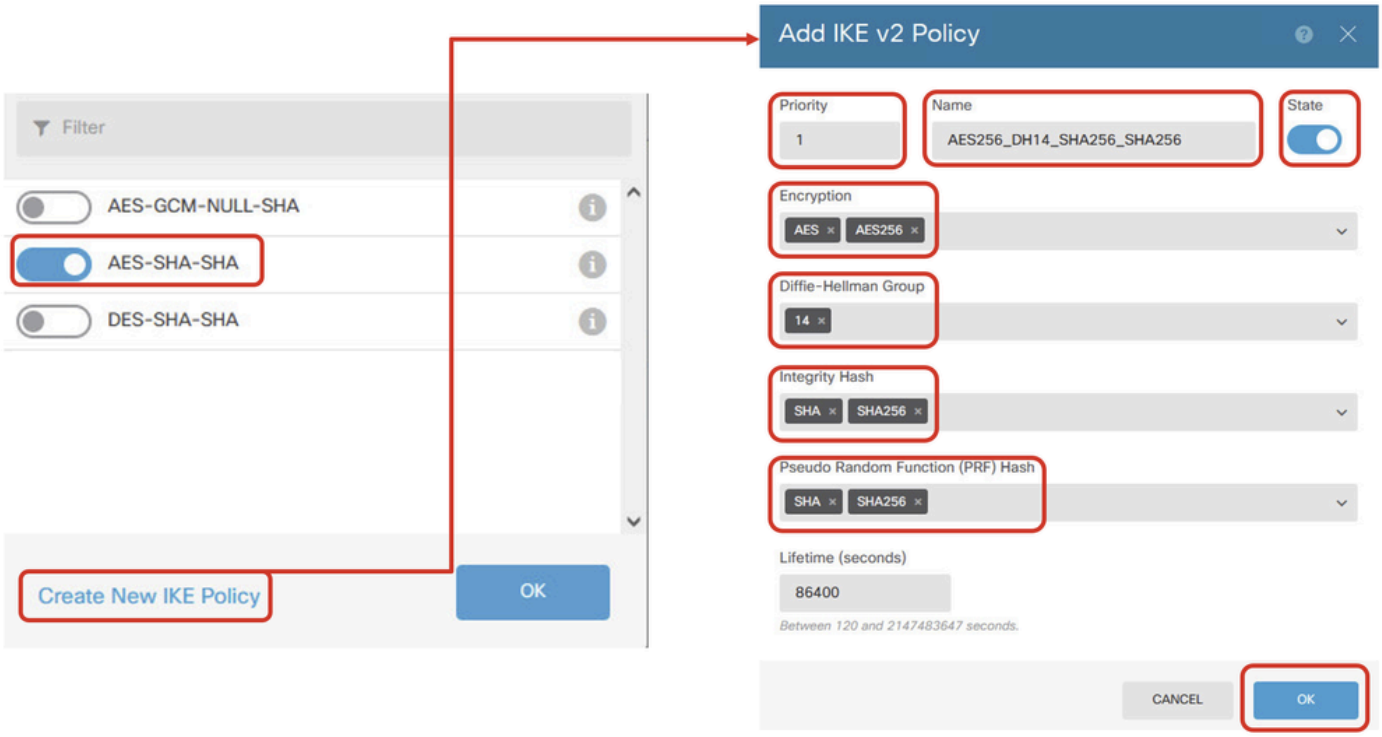
Edit_IKE_Policy

Paso 3.9. Para la política IKE, puede utilizar una predefinida o crear una nueva haciendo clic en Create New IKE Policy.

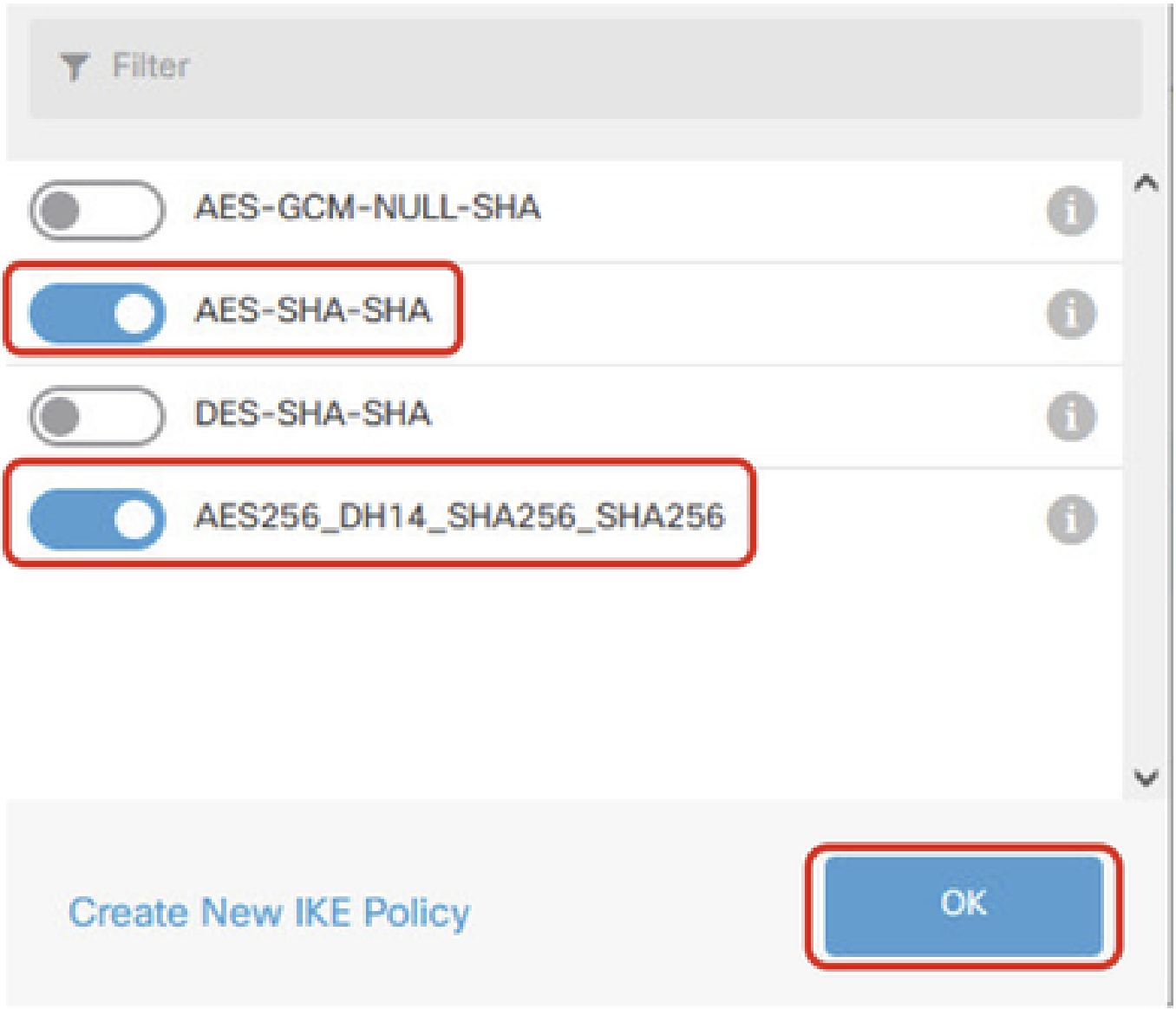
En este ejemplo, alterne una política IKE existente AES-SHA-SHA y cree una nueva para fines de

demostración. Haga clic en el botón OK para guardar.

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

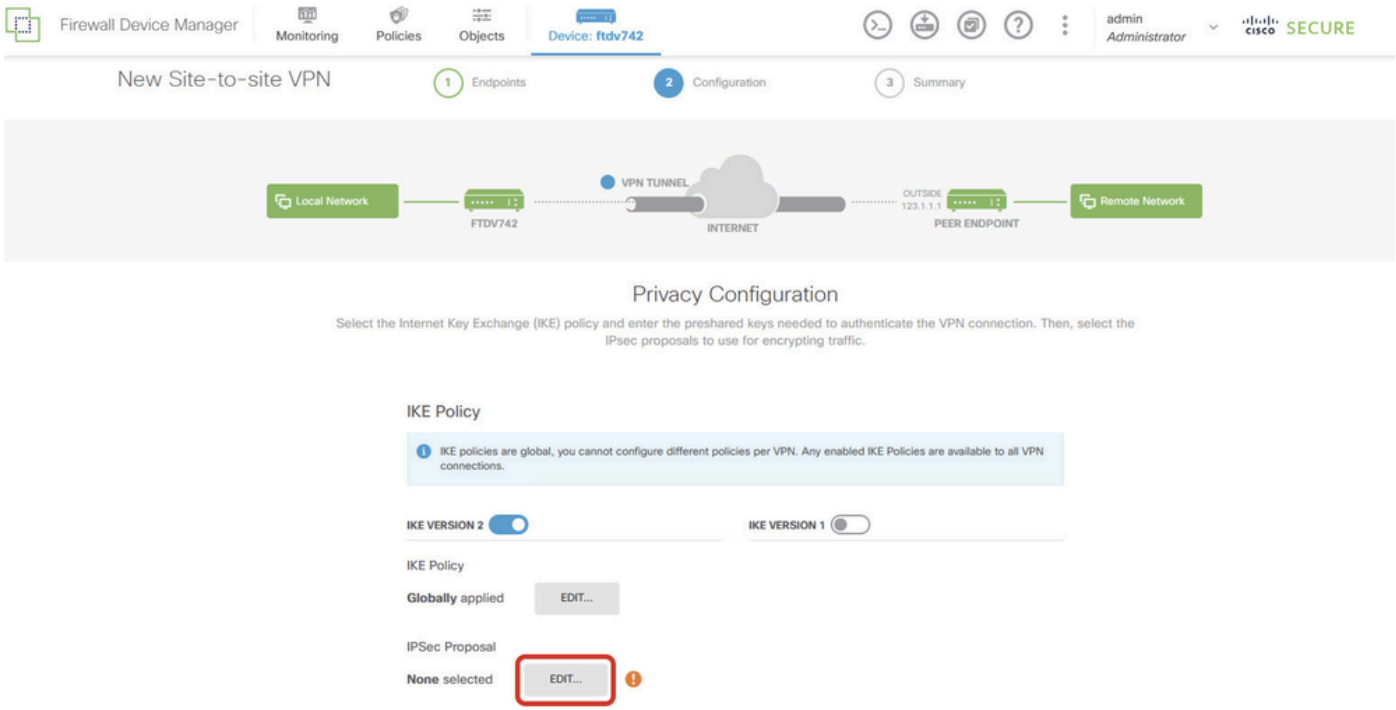


Add_New_IKE_Policy



Enable_New_IKE_Policy

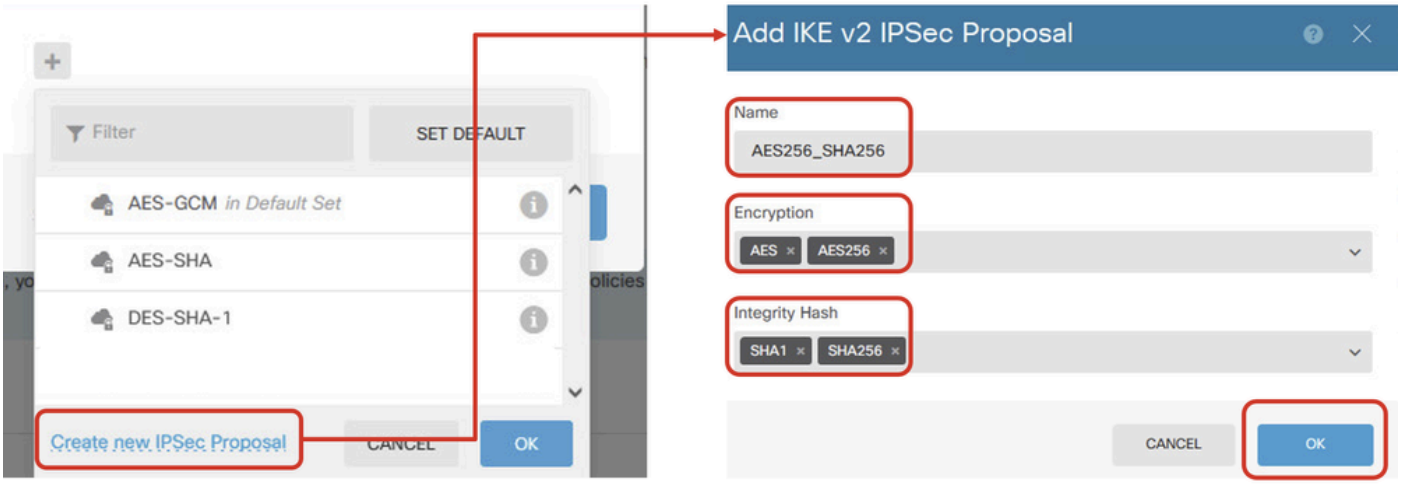
Paso 3.10. Vaya a la propuesta IPSec. Haga clic en el botón Editar.



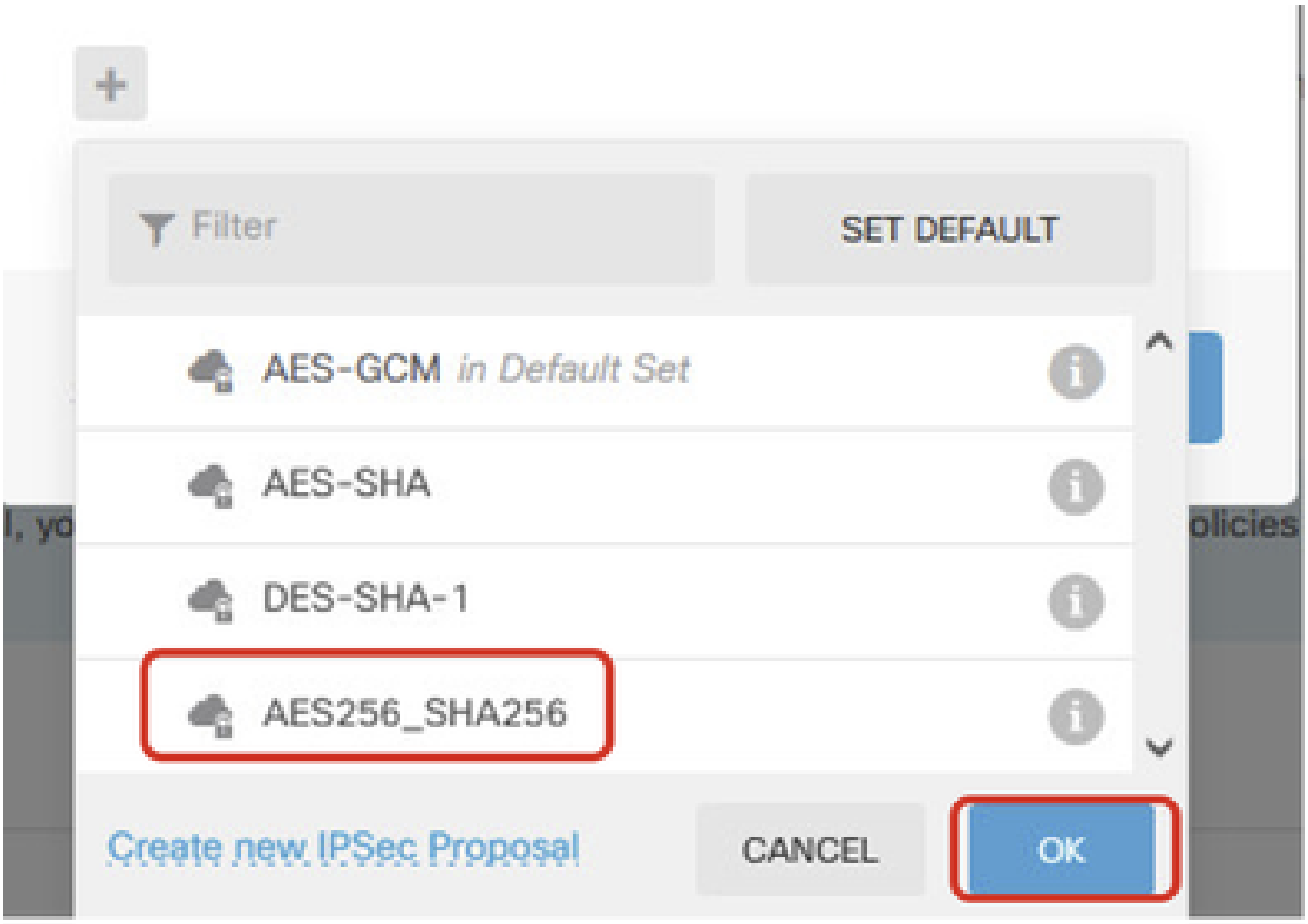
Editar_IKE_Propuesta

Paso 3.11. Para la propuesta IPSec, puede utilizar una propuesta predefinida o puede crear una nueva haciendo clic en Create new IPSec posed. En este ejemplo, cree uno nuevo con fines de demostración. Proporcione la información necesaria. Haga clic en el botón OK para guardar.

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



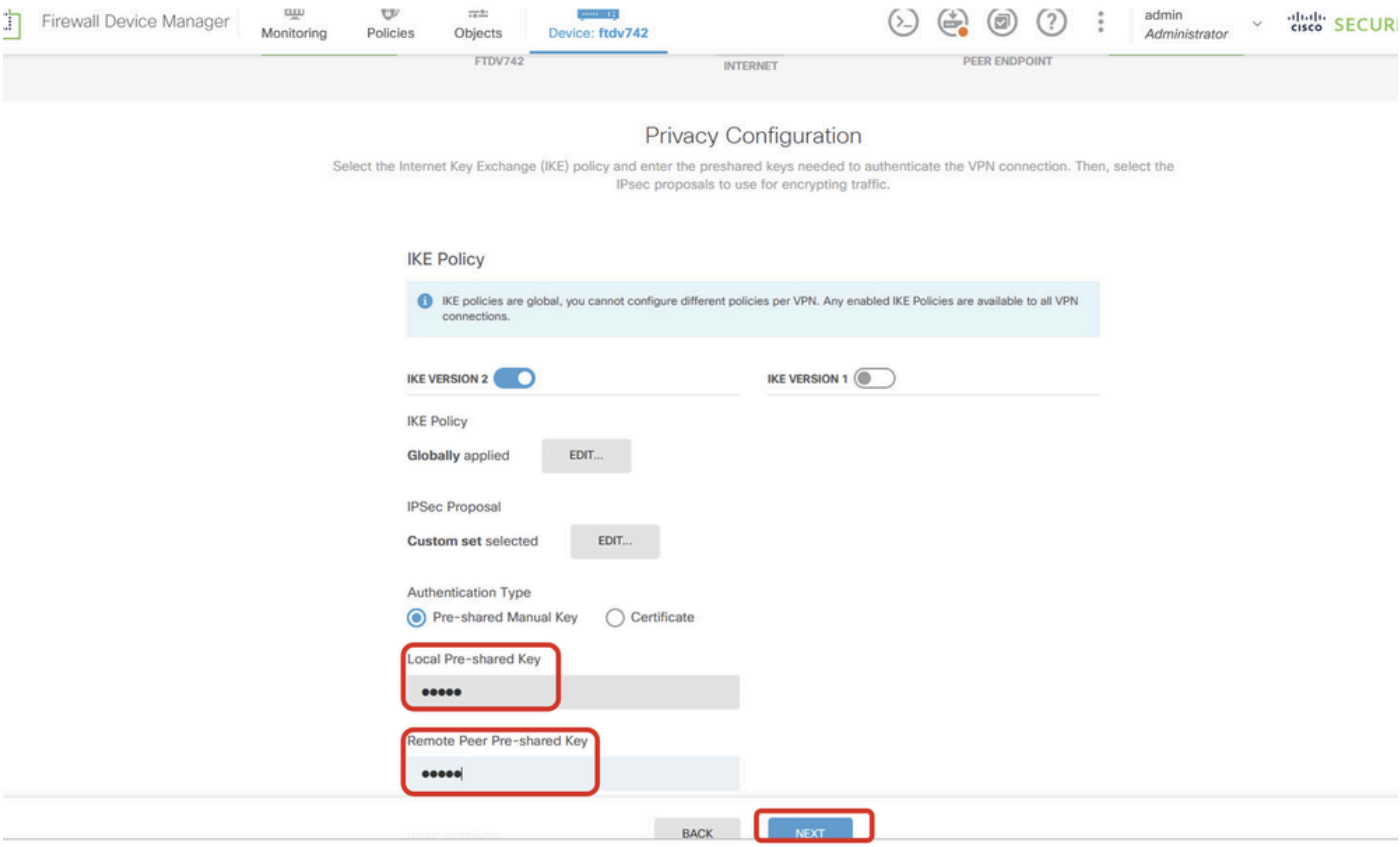
Agregar_nueva_propuesta_IPSec



Habilitar_Nueva_propuesta_IPSec

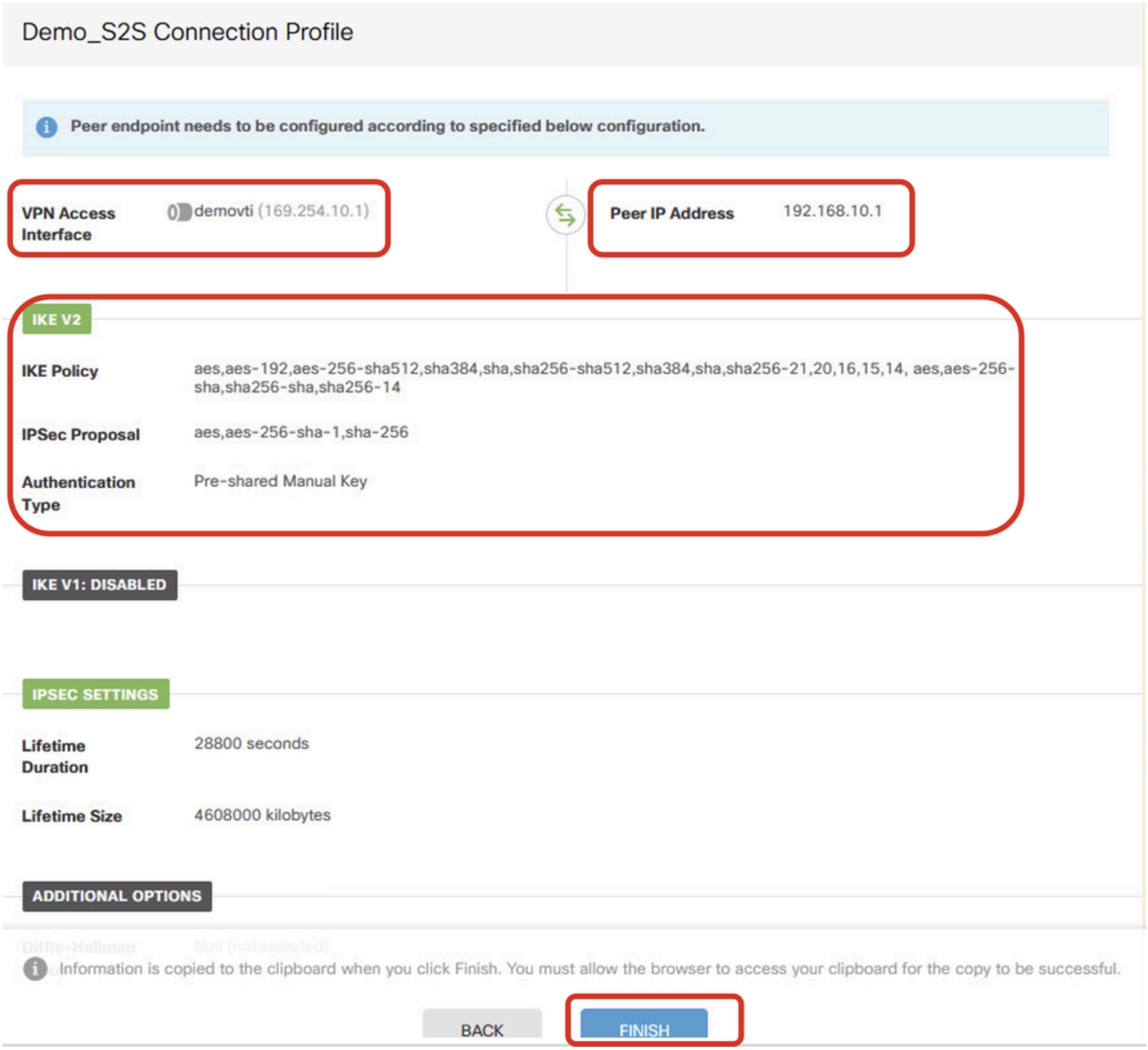
Paso 3.12. Configure la clave previamente compartida. Haga clic en el botón NEXT.

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



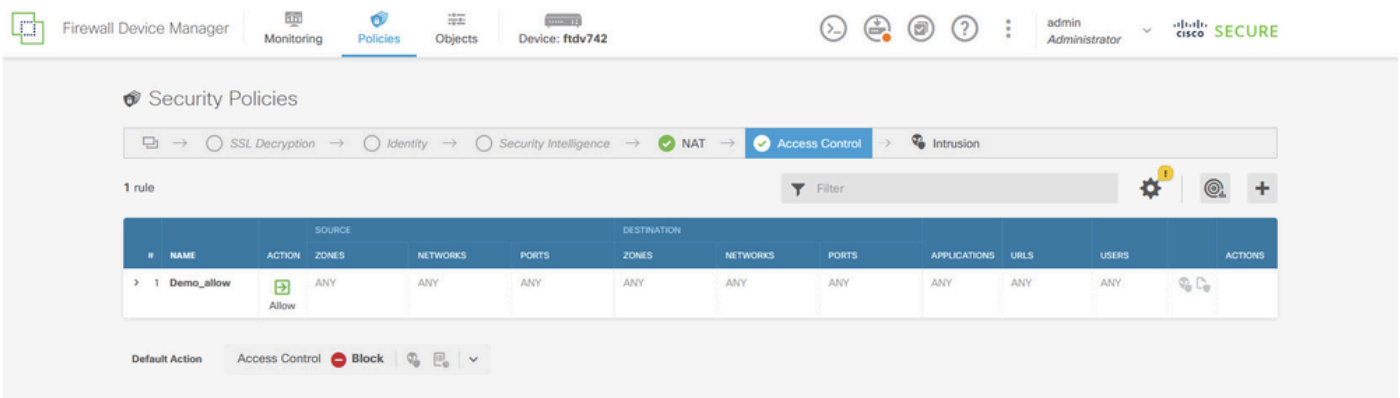
Configure_Pre_Shared_Key

Paso 3.13. 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.



VPN_Wizard_Complete

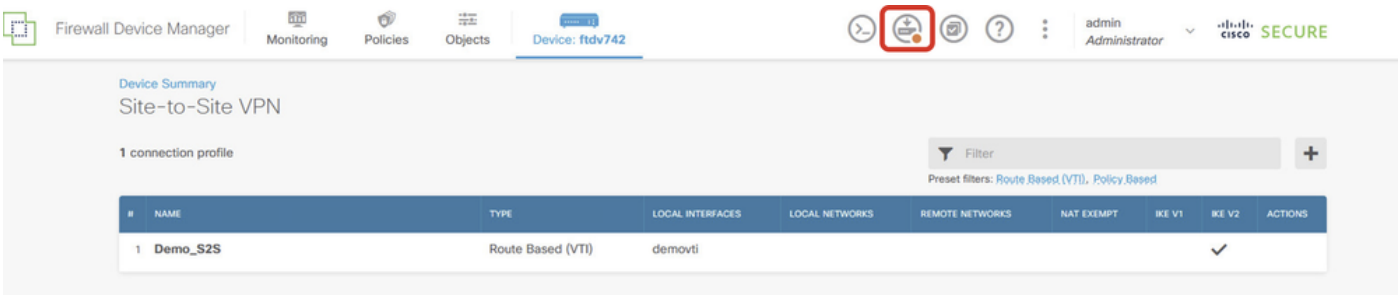
Paso 3.14. Cree una regla de control de acceso para permitir que el tráfico pase a través del FTD. En este ejemplo, permitir todos con fines de demostración. Modifique su política en función de sus necesidades reales.



Ejemplo_de_regla_de_control de acceso

Paso 3.15. (Opcional) Configure la regla de exención de NAT para el tráfico del cliente en FTD si se configura NAT dinámica para el cliente para acceder a Internet. En este ejemplo, no es necesario configurar una regla exenta de NAT porque no se configura ninguna NAT dinámica en cada FTD.

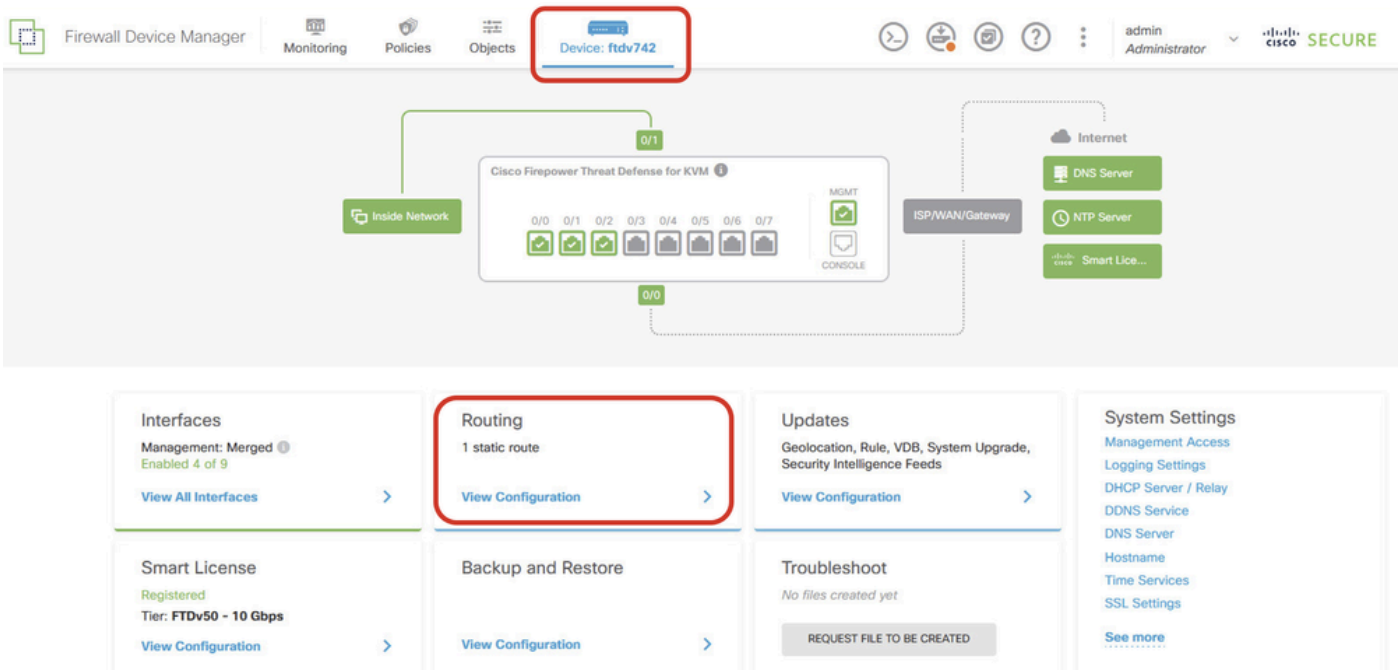
Paso 3.16. Implemente los cambios de configuración.



Deploy_VPN_Configuration

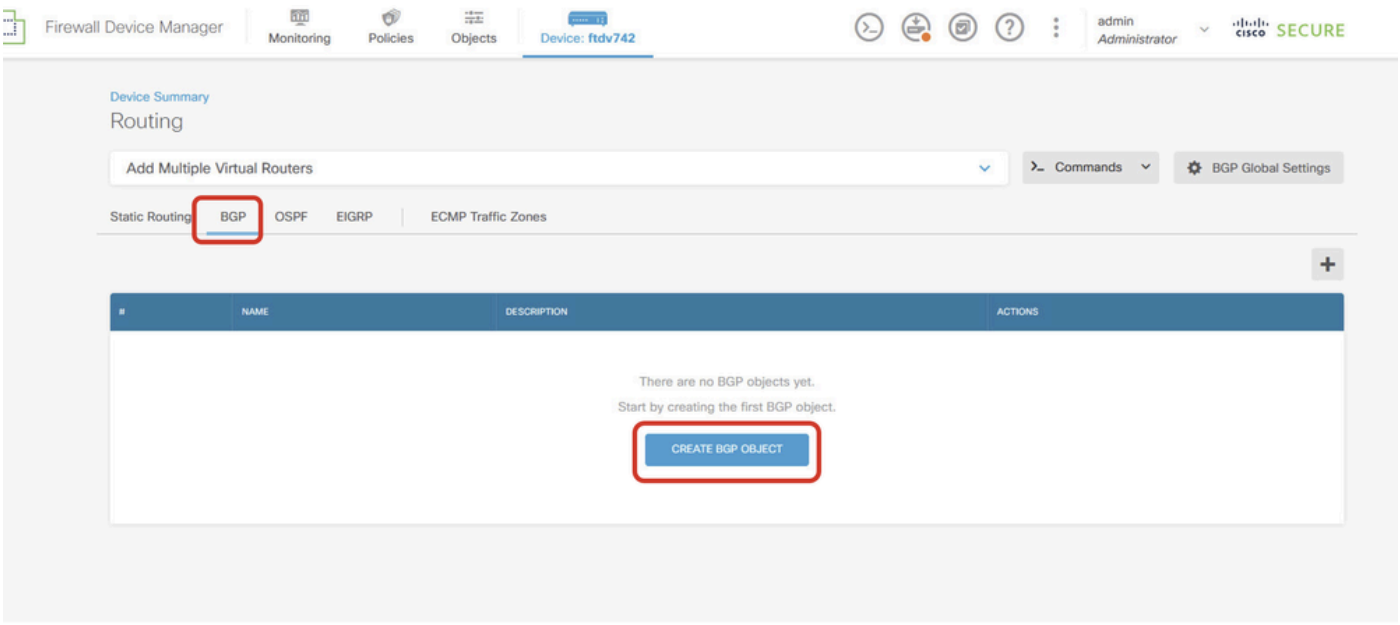
Configuraciones en BGP

Paso 4. Vaya a Device > Routing. Haga clic en Ver configuración.



View_Routing_Configuration

Paso 5. Haga clic en la pestaña BGP y luego haga clic en CREATE BGP OBJECT.



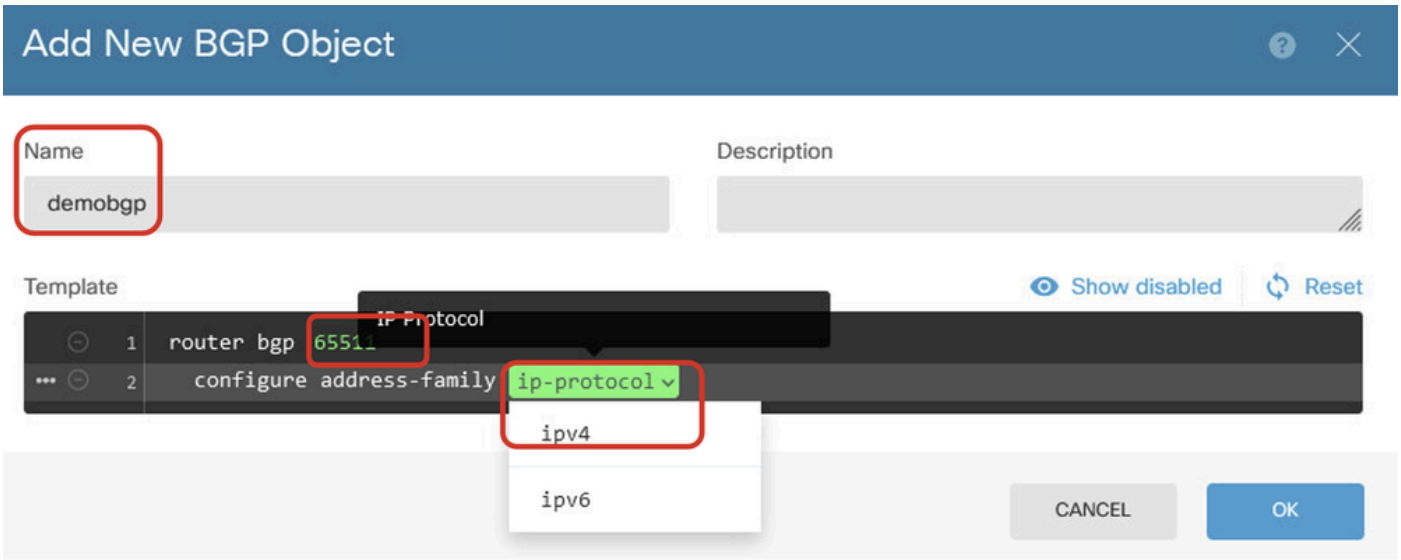
Create_BGP_Object

Paso 6. Proporcione el nombre del objeto. Navegue hasta Plantilla y configure. Haga clic en el botón OK para guardar.

Nombre: demobgp

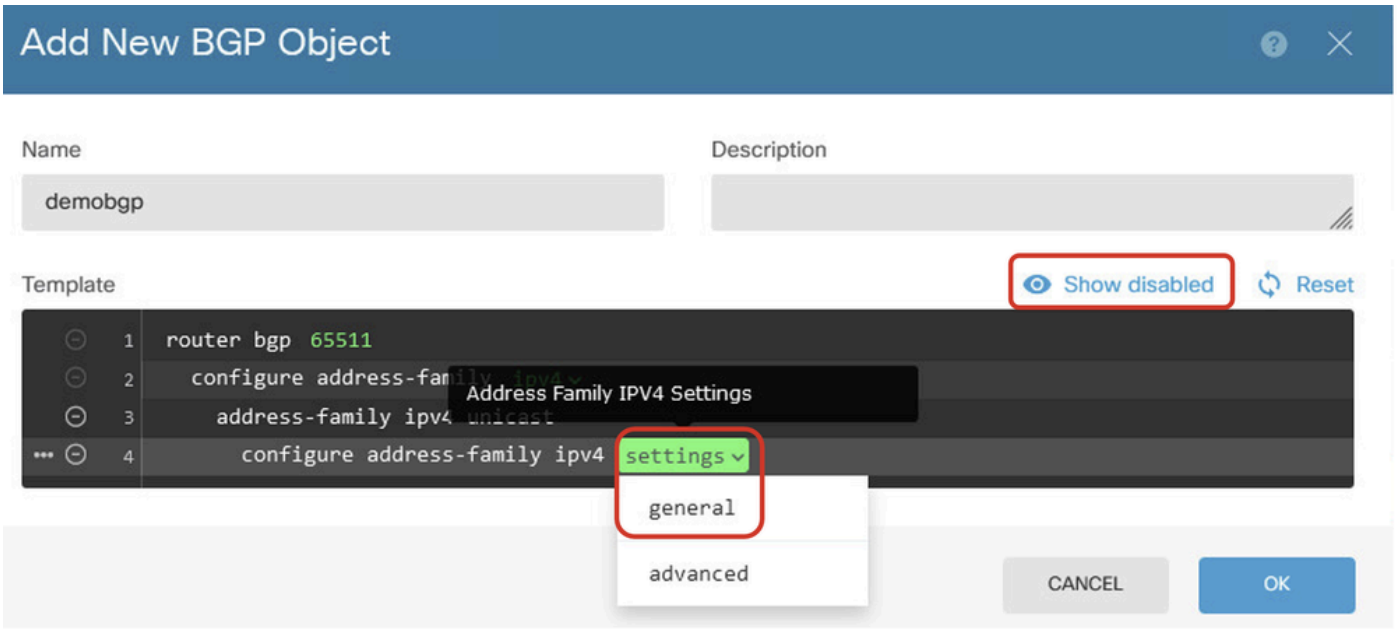
Línea 1: Configure el número AS. Haga clic en as-number. Entrada manual del número AS local. En este ejemplo, el número AS 65511 para el FTD Site1.

Línea 2: Configure el protocolo IP. Haga clic en ip-protocol. Seleccione ipv4.



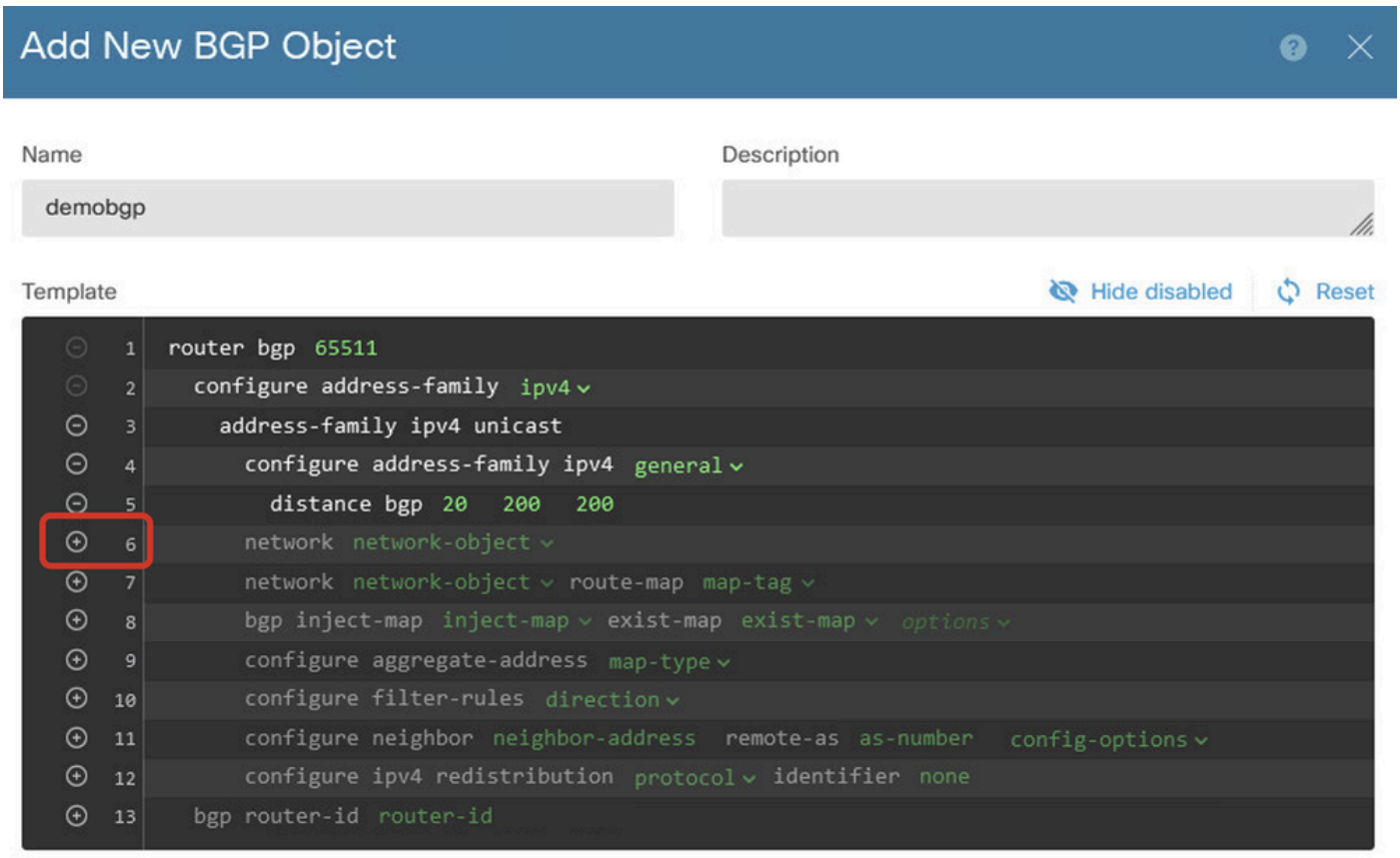
Create_BGP_Object_ASNumber_Protocol

Línea 4: Configure más parámetros. Haga clic en settings, elija general, y luego haga clic en Show disabled.

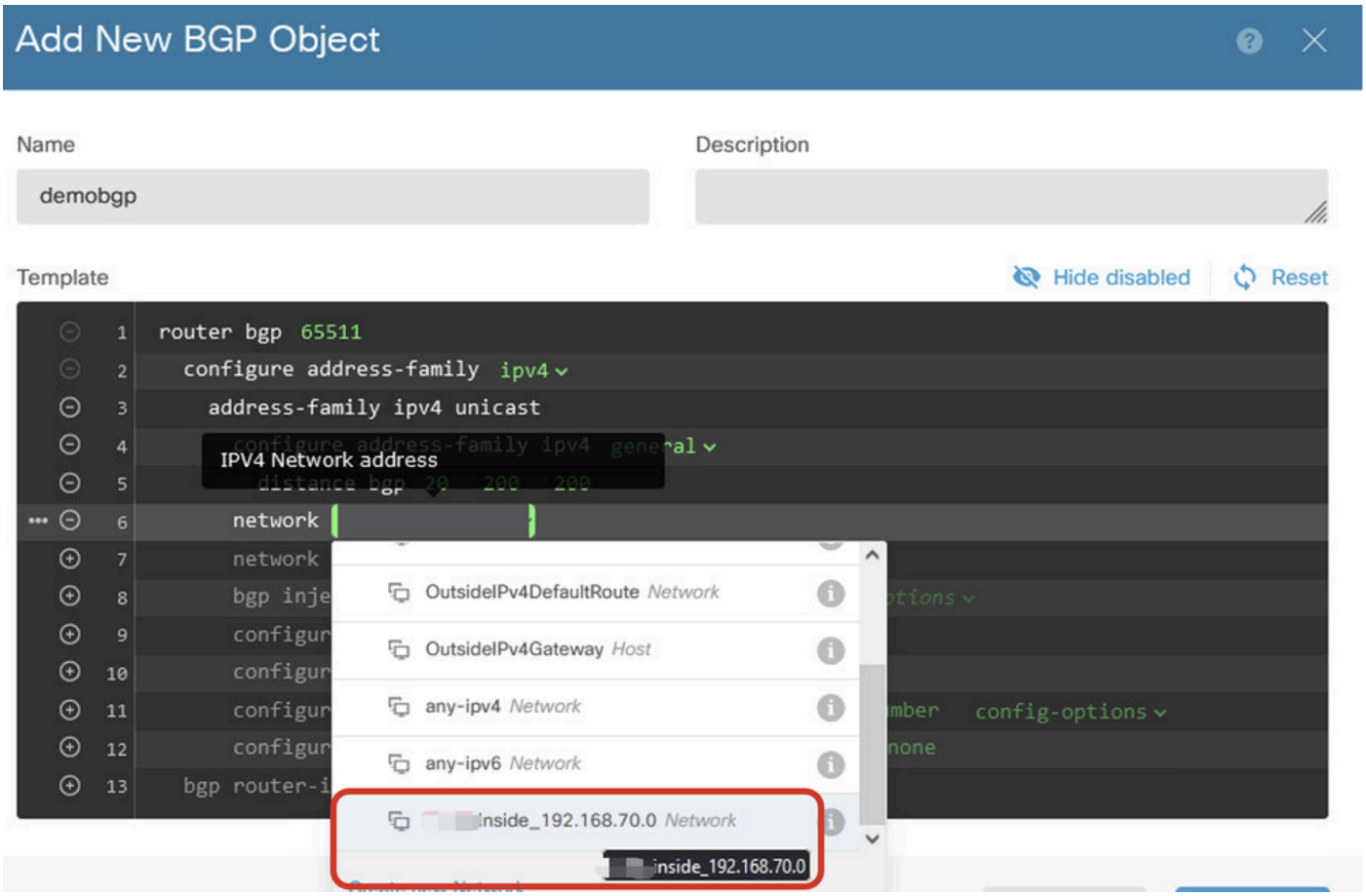


Create_BGP_Object_AddressSetting

Línea 6: Haga clic en el icono + para habilitar la línea para configurar la red BGP. Haga clic en network-object. Puede ver los objetos disponibles existentes y elegir uno. En este ejemplo, elija el nombre de objeto inside_192.168.70.0 (creado en el paso 3.2.).

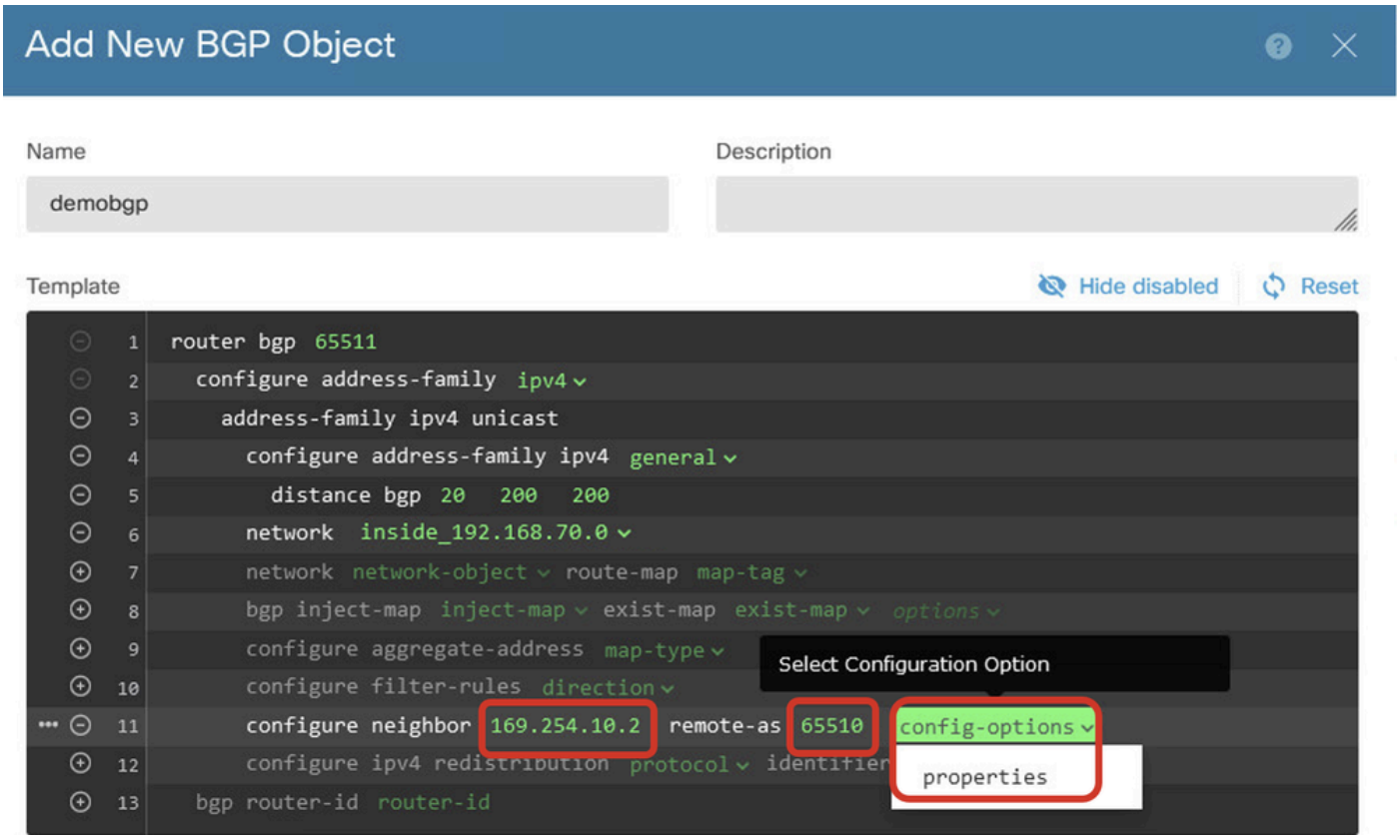


Create_BGP_Object_Add_Network



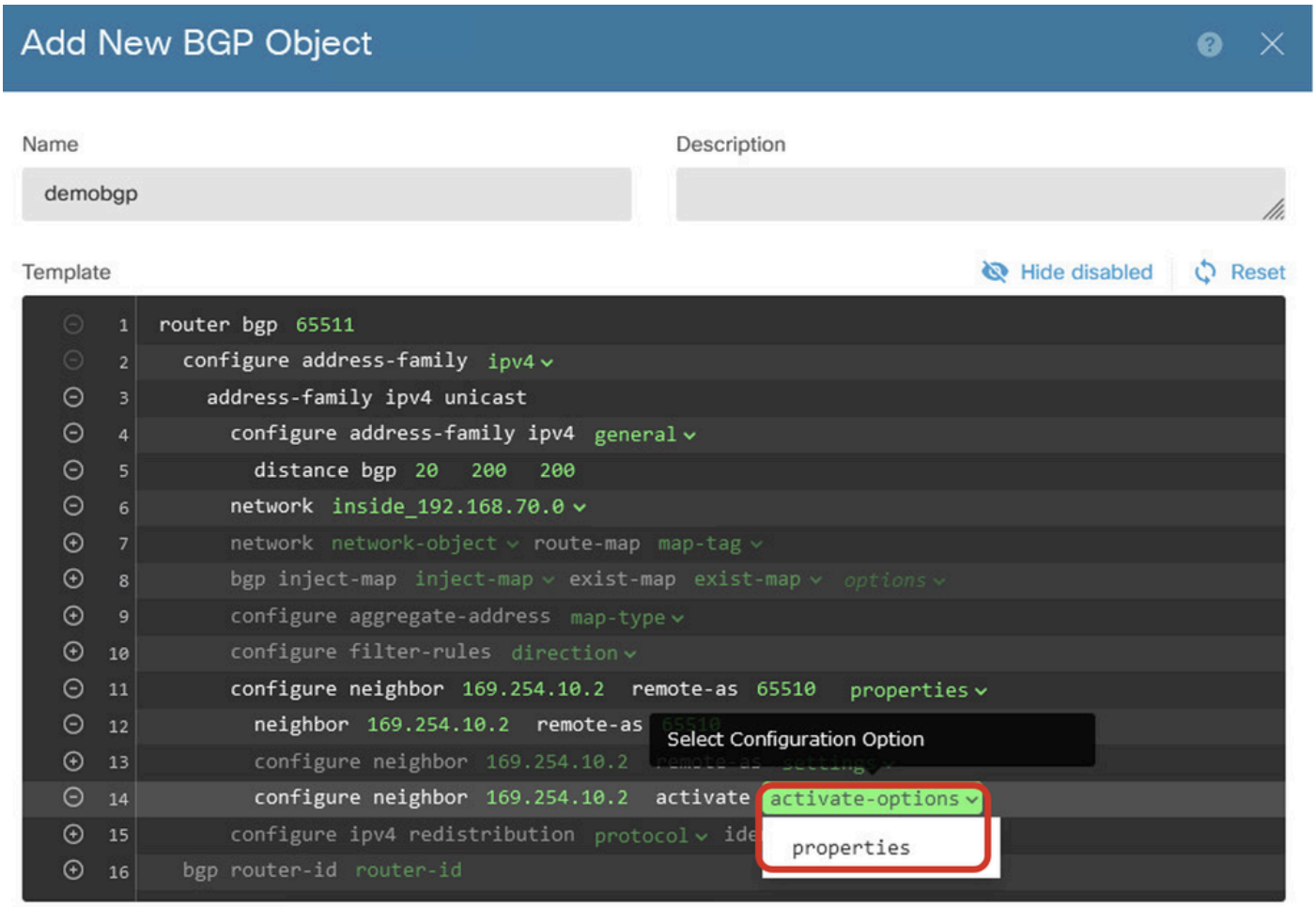
Create_BGP_Object_Add_Network2

Línea 11: Haga clic en el icono + para habilitar la línea para configurar la información relacionada con el vecino BGP. Haga clic en neighbor-address, e ingrese manualmente la dirección de vecino BGP de peer. En este ejemplo, es 169.254.10.2 (dirección IP VTI del FTD Site2). Haga clic en as-number, e ingrese manualmente el número AS de peer. En este ejemplo, 65510 es para FTD Site2. Haga clic en config-options y elija properties.



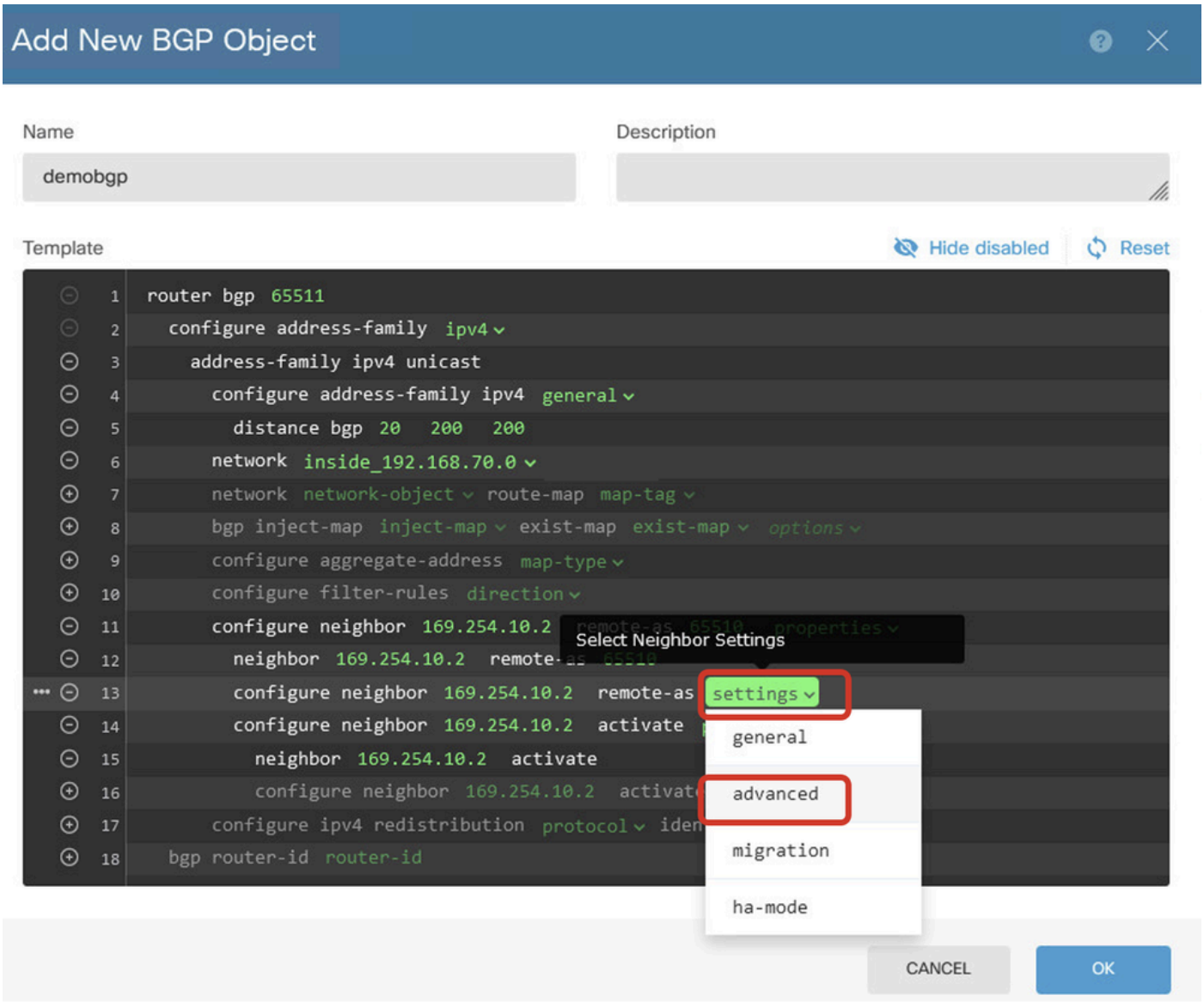
Create_BGP_Object_NeighborSetting

Línea 14: Haga clic en el icono + para habilitar la línea para configurar algunas propiedades del vecino. Haga clic en activate-options y elija properties.



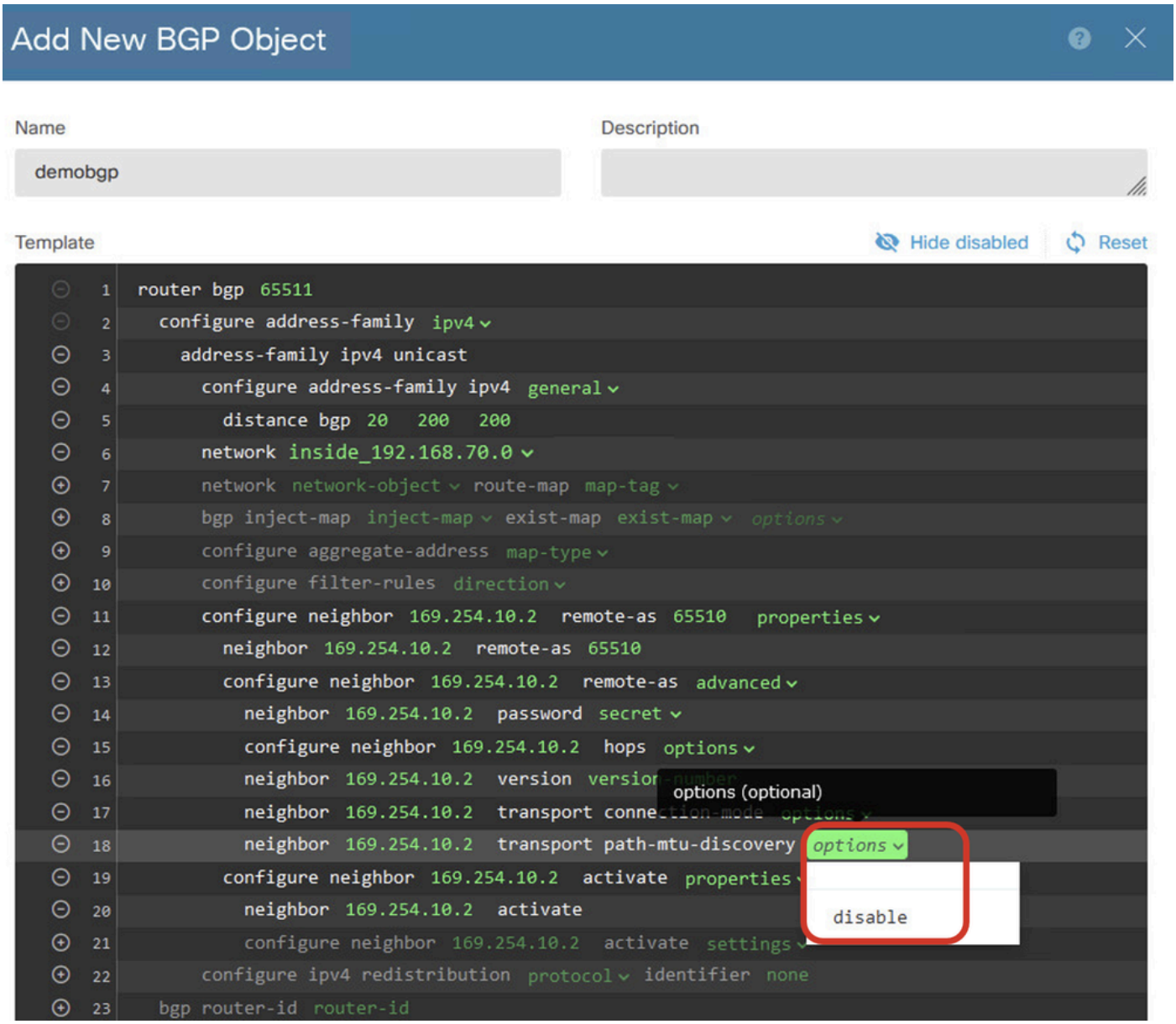
Create_BGP_Object_NeighborSetting_Properties

Línea 13: Haga clic en el icono + para habilitar la línea para mostrar las opciones avanzadas. Haga clic en Settings y elija advanced.



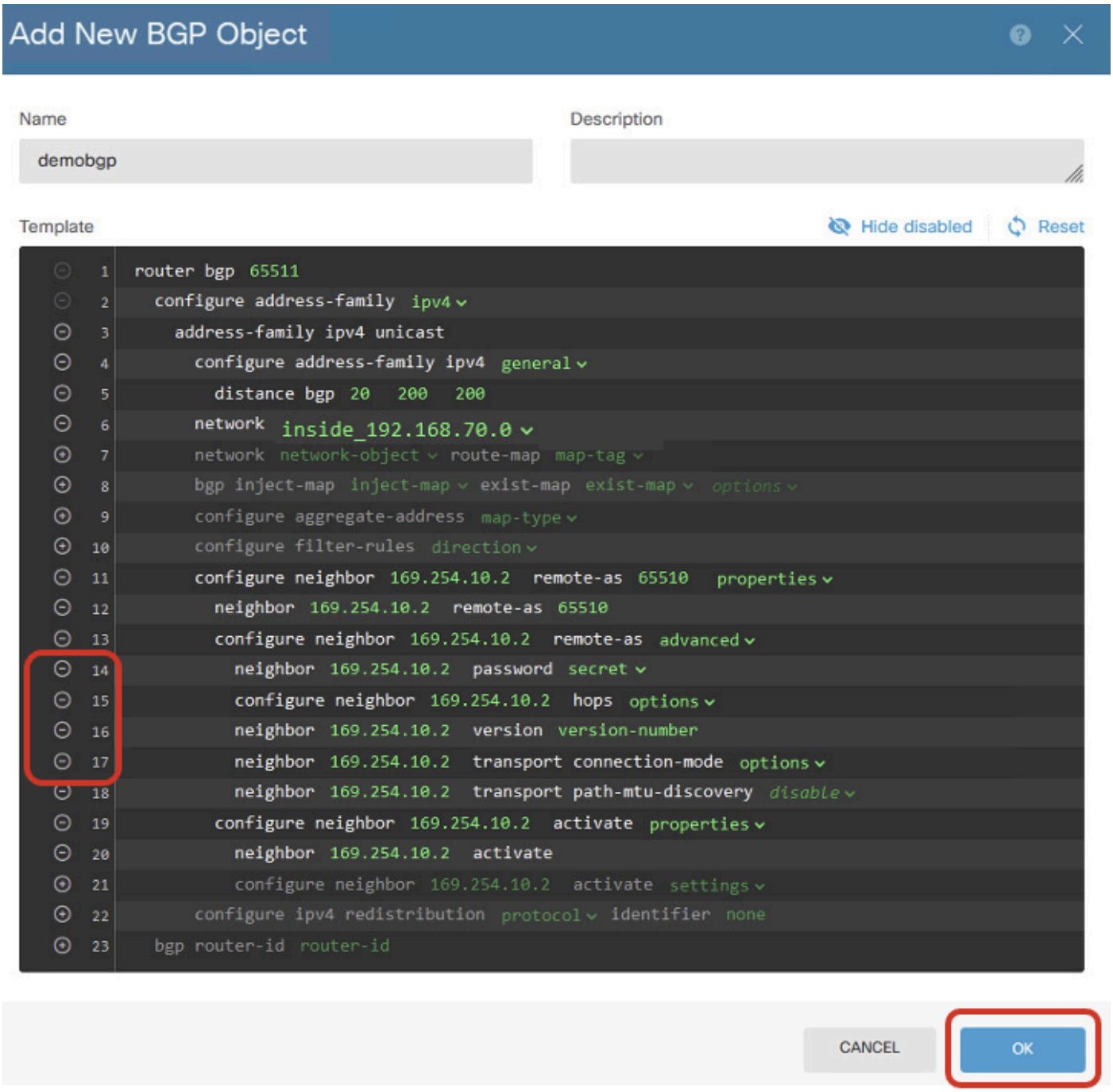
Create_BGP_Object_NeighborSetting_Properties_Advanced

Línea 18: Haga clic en options y elija disable para inhabilitar la detección de MTU de trayectoria.



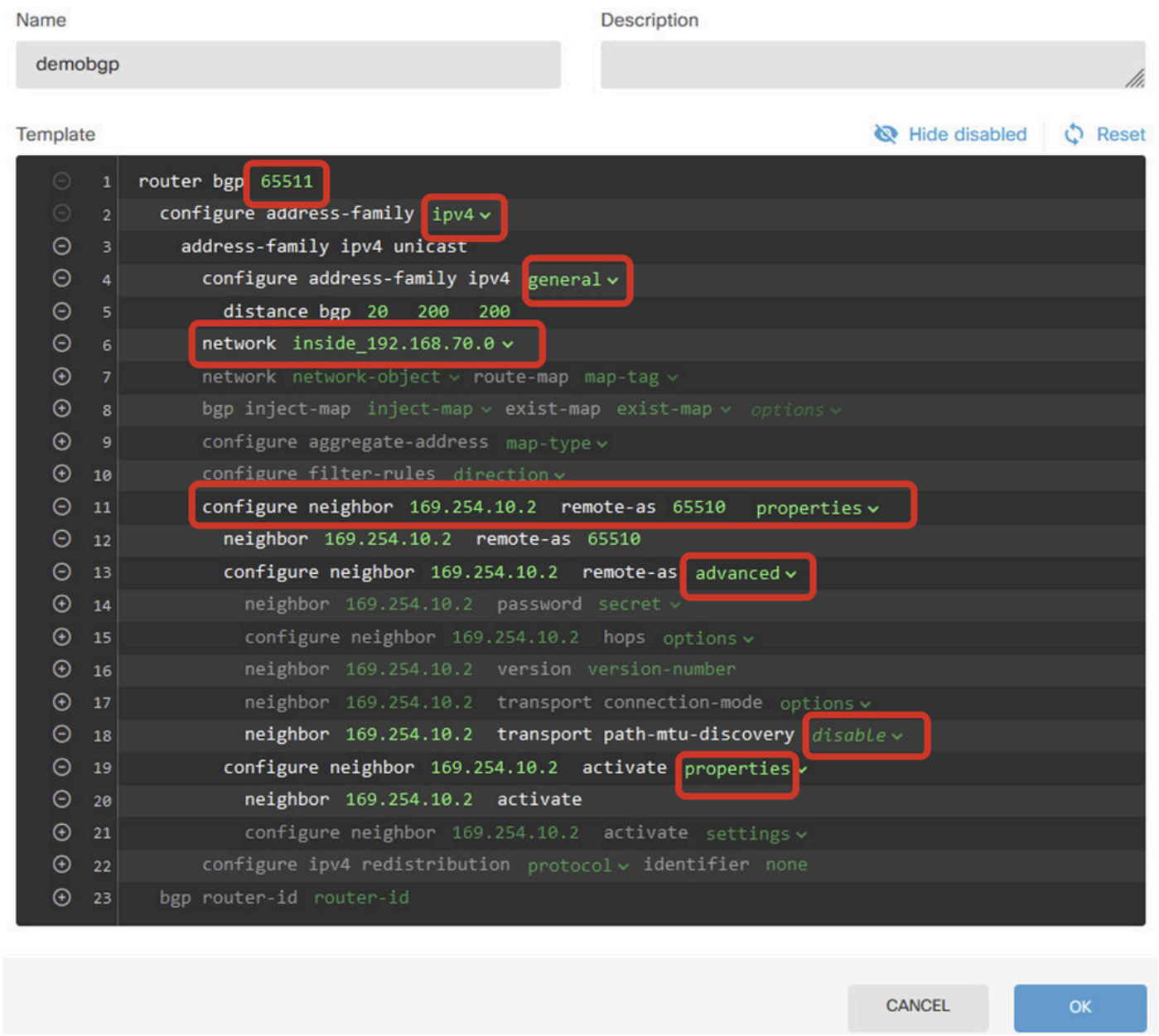
Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

Línea 14, 15, 16, 17: Haga clic en el - botón para desactivar las líneas. A continuación, haga clic en el botón OK para guardar el objeto BGP.



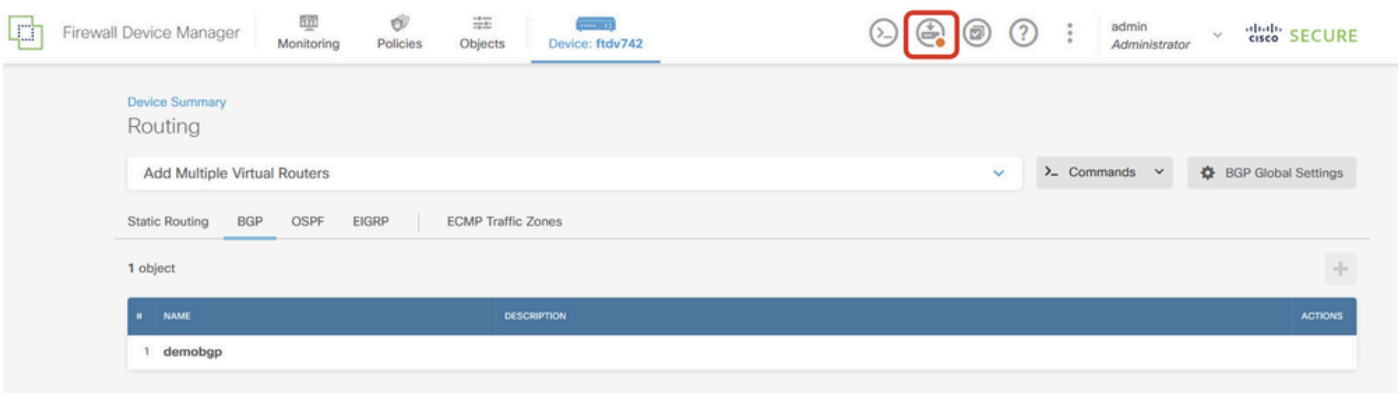
Create_BGP_Object_DisableLines

Esta es una descripción general de la configuración de BGP en este ejemplo. Puede configurar los otros parámetros de BGP en función de sus necesidades reales.



Create_BGP_Object_Final_Overview

Paso 7. Implemente los cambios de configuración de BGP.



Deploy_BGP_Configuration

Paso 8. Ahora se ha completado la configuración del FTD Site1.

Para configurar Site2 FTD VPN y BGP, repita los pasos 3 a 7 con los parámetros correspondientes de Site2 FTD.

Descripción general de la configuración del FTD del sitio 1 y del FTD del sitio 2 en CLI.

FTD del sitio 1	FTD del sitio 2
NGFW versión 7.4.2 interface GigabitEthernet0/0 nameif outside manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 IP address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside security-level 0 IP address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti IP address 169.254.10.1 255.255.255.0 tunnel source interface outside tunnel destination 192.168.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec_profile|e4084d322d Red de objetos OutsideIPv4Gateway host 192.168.30.3 Red de objetos inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc dentro de cualquier ifc fuera de cualquier rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458:	NGFW versión 7.4.2 interface GigabitEthernet0/0 nameif outside manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 IP address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside security-level 0 IP address 192.168.50.1 255.255.255.0 interface Tunnel1 nameif demovti25 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 ipsec_profile|e4084d322d Red de objetos OutsideIPv4Gateway host 192.168.10.3 Red de objetos inside_192.168.50.0 subnet 192.168.50.0 255.255.255.0 access-group NGFW_ONBOX_ACL global access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc dentro de cualquier ifc fuera de cualquier rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458: ACCESS POLICY: NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458: L5 RULE: Demo_allow

L5 RULE: Demo_allow	
access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435458 any any rule-id 268435458 event-log both	access-list NGFW_ONBOX_ACL advanced permit object-group |acSvcg-268435458 any any rule-id 268435458 event-log both
access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy	access-list NGFW_ONBOX_ACL remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule	access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule
access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1	access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1
router bgp 65511	router bgp 65510
bgp log-neighbor-changes	bgp log-neighbor-changes
bgp router-id vrf auto-assign	bgp router-id vrf auto-assign
address-family ipv4 unicast	address-family ipv4 unicast
neighbor 169.254.10.2 remote-as 65510	neighbor 169.254.10.1 remote-as 65511
neighbor 169.254.10.2 transport path-mtu-discovery disable	neighbor 169.254.10.1 transport path-mtu-discovery disable
neighbor 169.254.10.2 activate	neighbor 169.254.10.1 activate
network 192.168.70.0	network 192.168.50.0
no auto-summary	no auto-summary
sin sincronización	sin sincronización
exit-address-family	exit-address-family
route outside 0.0.0.0 0.0.0.0 192.168.30.3 1	route outside 0.0.0.0 0.0.0.0 192.168.10.3 1
crypto ipsec ikev2 ipsec-offer AES256_SHA256	crypto ipsec ikev2 ipsec-offer AES256_SHA256
protocol esp encryption aes-256 aes	protocol esp encryption aes-256 aes
protocol esp integration sha-256 sha-1	protocol esp integration sha-256 sha-1
crypto ipsec profile ipsec_profile|e4084d322d	crypto ipsec profile ipsec_profile|e4084d322d
set ikev2 ipsec-offer AES256_SHA256	set ikev2 ipsec-offer AES256_SHA256
set security-association lifetime kilobytes 4608000	set security-association lifetime kilobytes 4608000
set security-association lifetime seconds 28800	set security-association lifetime seconds 28800
crypto ipsec security-association pmtu-aging infinite	crypto ipsec security-association pmtu-aging infinite
crypto ikev2 policy 1	crypto ikev2 policy 1
encryption aes-256 aes	encryption aes-256 aes
Integrity sha256 sha	Integrity sha256 sha
grupo 14	grupo 14
prf sha256 sha	prf sha256 sha
lifetime seconds 86400	lifetime seconds 86400
crypto ikev2 policy 20	crypto ikev2 policy 20
encryption aes-256 aes-192 aes	encryption aes-256 aes-192 aes
integridad sha512 sha384 sha256 sha	integridad sha512 sha384 sha256 sha
grupo 21 20 16 15 14	grupo 21 20 16 15 14

prf sha512 sha384 sha256 sha lifetime seconds 86400 crypto ikev2 enable outside política de grupo |s2sGP|192.168.10.1 internal política de grupo Atributos |s2sGP|192.168.10.1 vpn-tunnel-protocol ikev2 tunnel-group 192.168.10.1 type ipsec-l2l tunnel-group 192.168.10.1 general-attributes default-group-policy |s2sGP|192.168.10.1 tunnel-group 192.168.10.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****	prf sha512 sha384 sha256 sha lifetime seconds 86400 crypto ikev2 enable outside política de grupo |s2sGP|192.168.30.1 internal política de grupo Atributos |s2sGP|192.168.30.1 vpn-tunnel-protocol ikev2 tunnel-group 192.168.30.1 type ipsec-l2l tunnel-group 192.168.30.1 general-attributes default-group-policy |s2sGP|192.168.30.1 tunnel-group 192.168.30.1 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Navegue hasta la CLI de cada FTD 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 del sitio 1	FTD del sitio 2
ftdv742# show crypto ikev2 sa SA IKEv2: Session-id:134, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Función de estado de FVRF/IVRF remoto local de ID de túnel 563984431 192.168.30.1/500 192.168.10.1/500 Global/Global READY RESPONDER Encr: AES-CBC, tamaño de clave: 256, hash: SHA256, DH Grp:14, signo de autenticación: PSK, verificación de autenticación: PSK Vida/Tiempo activo: 86400/5145 s Child sa: selector local 0.0.0.0/0 - 255.255.255.255/65535	ftdv742# show crypto ikev2 sa SA IKEv2: Id. de sesión:13, Estado:ACTIVO-ASCENDENTE, recuento IKE:1, recuento HIJO:1 Función de estado de FVRF/IVRF remoto local de ID de túnel 339797985 192.168.10.1/500 192.168.30.1/500 INICIADOR DE PREPARACIÓN global/global Encr: AES-CBC, tamaño de clave: 256, hash: SHA256, DH Grp:14, signo de autenticación: PSK, verificación de autenticación: PSK Vida/Tiempo activo: 86400/74099 s Child sa: selector local 0.0.0.0/0 - 255.255.255.255/65535 remote selector 0.0.0.0/0 - 255.255.255.255/65535 Entrada/salida SPI ESP:

remote selector 0.0.0.0/0 - 255.255.255.255/65535 Entrada/salida SPI ESP: 0xf0c4239d/0xb7b5b38b	0xb7b5b38b/0xf0c4239d
ftdv742# show crypto ipsec sa interfaz: demovti Etiqueta de mapa criptográfico: __vti-crypto-map-Tunnel1-0-1, número de secuencia: 65280, dirección local: 192.168.30.1 vrf protegido (ivrf): global ident local (addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) ident remoto (addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.10.1 #pkts encaps: 5720, #pkts encrypt: 5720, #pkts digest: 5720 #pkts decaps: 5717, #pkts decrypt: 5717, #pkts verify: 5717 #pkts comprimido: 0, #pkts descomprimido: 0 #pkts sin comprimir: 5720, error en la compilación de #pkts: 0, error en la descomposición de #pkts: 0 #pre-frag éxitos: 0, #pre-frag fracasos: 0, #fragments creado: 0 #PMTUs enviado: 0, #PMTUs recibido: 0, #decapsulated frgs que necesitan reensamblado: 0 #TFC recibido: 0, #TFC enviado: 0 #Valid Errores ICMP recibidos: 0, #Invalid Errores ICMP recibidos: 0 #send errores: 0, #recv errores: 0 local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.10.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 Tiempo restante de PMTU (s): 0, directiva DF: copy-df Validación de error ICMP: deshabilitada, paquetes TFC: deshabilitados	ftdv742# show crypto ipsec sa interfaz: demovti25 Etiqueta de mapa criptográfico: __vti-crypto-map-Tunnel1-0-1, número de secuencia: 65280, dirección local: 192.168.10.1 vrf protegido (ivrf): global ident local (addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) ident remoto (addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1 #pkts encaps: 5721, #pkts encrypt: 5721, #pkts digest: 5721 #pkts decaps: 5721, #pkts decrypt: 5721, #pkts verify: 5721 #pkts comprimido: 0, #pkts descomprimido: 0 #pkts sin comprimir: 5721, error de comp #pkts: 0, error de descomp #pkts: 0 #pre-frag éxitos: 0, #pre-frag fracasos: 0, #fragments creado: 0 #PMTUs enviado: 0, #PMTUs recibido: 0, #decapsulated frgs que necesitan reensamblado: 0 #TFC recibido: 0, #TFC enviado: 0 #Valid Errores ICMP recibidos: 0, #Invalid Errores ICMP recibidos: 0 #send errores: 0, #recv errores: 0 local crypto endpt.: 192.168.10.1/500, remote crypto endpt.: 192.168.30.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 Tiempo restante de PMTU (s): 0, directiva DF: copy-df Validación de error ICMP: deshabilitada, paquetes TFC: deshabilitados spi de salida actual: F0C4239D

spi saliente actual: B7B5B38B spi de entrada actual: F0C4239D sas esp de entrada: spi: 0xF0C4239D (4039386013) Estado de SA: activo transform: esp-aes-256 esp-sha-256-hmac no compression configuración en uso ={L2L, Túnel, IKEv2, VTI, } slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 tiempo de sa: duración restante de la clave (kB/s): (4285389/3722) Tamaño IV: 16 bytes compatibilidad con detección de repetición: S Anti replay bitmap: 0xFFFFFFFF 0xFFFFFFFF sas esp salientes: spi: 0xB7B5B38B (3082138507) Estado de SA: activo transform: esp-aes-256 esp-sha-256-hmac no compression configuración en uso ={L2L, Túnel, IKEv2, VTI, } slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 tiempo de sa: duración restante de la clave (kB/s): (4147149/3722) Tamaño IV: 16 bytes compatibilidad con detección de repetición: S Anti replay bitmap: 0x00000000 0x00000001	spi entrante actual: B7B5B38B sas esp de entrada: spi: 0xB7B5B38B (3082138507) Estado de SA: activo transform: esp-aes-256 esp-sha-256-hmac no compression configuración en uso ={L2L, Túnel, IKEv2, VTI, } slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 tiempo de sa: duración restante de la clave (kB/s): (3962829/3626) Tamaño IV: 16 bytes compatibilidad con detección de repetición: S Anti replay bitmap: 0xFFFFFFFF 0xFFFFFFFF sas esp salientes: spi: 0xF0C4239D (4039386013) Estado de SA: activo transform: esp-aes-256 esp-sha-256-hmac no compression configuración en uso ={L2L, Túnel, IKEv2, VTI, } slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 tiempo de sa: duración restante de la clave (kB/s): (4101069/3626) Tamaño IV: 16 bytes compatibilidad con detección de repetición: S Anti replay bitmap: 0x00000000 0x00000001

Paso 2. Navegue hasta la CLI de cada FTD a través de la consola o SSH para verificar el estado de BGP mediante los comandos show bgp neighbors y show route bgp.

FTD del sitio 1	FTD del sitio 2
ftdv742# show bgp neighbors El vecino BGP es 169.254.10.2, vrf single_vf, AS 65510 remoto, link externo BGP versión 4, ID de router remoto 192.168.50.1 Estado BGP = Establecido, hasta 1d20h Última lectura 00:00:25, última escritura 00:00:45, tiempo de espera es 180, intervalo de	ftdv742# show bgp neighbors El vecino BGP es 169.254.10.1, vrf single_vf, AS 65511 remoto, link externo BGP versión 4, ID de router remoto 192.168.70.1 Estado BGP = Establecido, hasta 1d20h Última lectura 00:00:11, última escritura 00:00:52, tiempo de espera es 180, intervalo de

keepalive es 60 segundos Sesiones de vecino: 1 activo, no admite multisesión (deshabilitado) Capacidades del vecino: Actualización de ruta: anunciada y recibida (nueva) Capacidad de ASN de cuatro octetos: anunciada y recibida Unidifusión IPv4 de la familia de direcciones: anunciada y recibida Capacidad multisesión: Estadísticas de mensajes: La profundidad de InQ es 0 La profundidad de salida es 0 Enviados y recibidos Aperturas: 1 1 Notificaciones: 0 0 Actualizaciones: 2 2 Keepalives: 2423 2427 Actualización de ruta: 0 0 Total: 2426 2430 El tiempo mínimo predeterminado entre ejecuciones de anuncios es de 30 segundos Para la familia de direcciones: unidifusión IPv4 Sesión: 169.254.10.2 Tabla BGP versión 3, versión vecina 3/0 Tamaño de la cola de salida: 0 Índice 1 1 miembro del grupo de actualización Enviados y recibidos Actividad de prefijo: ---- ---- Prefijos actuales: 1 1 (consume 80 bytes) Prefijos totales: 1 1 Retirada implícita: 0 0 Retirada explícita: 0 0 Se utiliza como bestpath: n/a 1 Se utiliza como ruta múltiple: n/a 0 Saliente entrante Prefijos denegados de directiva local: -------- ---------- Mejor trayectoria desde este par: 1 n/a Total: 1 0 Número de NLRI en la actualización enviada:	keepalive es 60 segundos Sesiones de vecino: 1 activo, no admite multisesión (deshabilitado) Capacidades del vecino: Actualización de ruta: anunciada y recibida (nueva) Capacidad de ASN de cuatro octetos: anunciada y recibida Unidifusión IPv4 de la familia de direcciones: anunciada y recibida Capacidad multisesión: Estadísticas de mensajes: La profundidad de InQ es 0 La profundidad de salida es 0 Enviados y recibidos Aperturas: 1 1 Notificaciones: 0 0 Actualizaciones: 2 2 Keepalives: 2424 a 2421 Actualización de ruta: 0 0 Total: 2427 2424 El tiempo mínimo predeterminado entre ejecuciones de anuncios es de 30 segundos Para la familia de direcciones: unidifusión IPv4 Sesión: 169.254.10.1 tabla BGP versión 9, versión vecina 9/0 Tamaño de la cola de salida: 0 Índice 4 4 miembro del grupo de actualización Enviados y recibidos Actividad de prefijo: ---- ---- Prefijos actuales: 1 1 (consume 80 bytes) Prefijos totales: 1 1 Retirada implícita: 0 0 Retirada explícita: 0 0 Se utiliza como bestpath: n/a 1 Se utiliza como ruta múltiple: n/a 0 Saliente entrante Prefijos denegados de directiva local: -------- ---------- Mejor trayectoria desde este par: 1 n/a Total: 1 0 Número de NLRI en la actualización enviada:

máx. 1, mín. 0 El rastreo de direcciones está habilitado, el RIB tiene una ruta a 169.254.10.2 Conexiones establecidas 1; descartadas 0 Último restablecimiento nunca Transport(tcp) path-mtu-discovery is disabled Graceful-Restart está desactivado	máx. 1, mín. 0 El rastreo de direcciones está habilitado, el RIB tiene una ruta a 169.254.10.1 Conexiones establecidas 4; descartadas 3 Último reinicio 1d21h, debido a la inestabilidad de la interfaz de la sesión 1 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart está desactivado
ftdv742# show route bgp Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2 E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 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 - ruta estática descargada periódicamente, + - ruta replicada SI - InterVRF estático, BI - InterVRF BGP El gateway de último recurso es 192.168.30.3 para la red 0.0.0.0 B 192.168.50.0 255.255.255.0 [20/0] vía 169.254.10.2, 1d20h	ftdv742# show route bgp Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2 E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 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 - ruta estática descargada periódicamente, + - ruta replicada SI - InterVRF estático, BI - InterVRF BGP El gateway de último recurso es 192.168.10.3 para la red 0.0.0.0 B 192.168.70.0 255.255.255.0 [20/0] vía 169.254.10.1, 1d20h

Paso 3. El cliente Site1 y el cliente Site2 se hacen ping entre sí correctamente.

Cliente del sitio 1:

```
Site1_Client#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 = 31/56/90 ms
```

Cliente de Site2:

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

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 BGP.

```
ftdv742# debug ip bgp ?

A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range      BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpnv4      Address family
vpnv6      Address family
vrf        VRF scope
<cr>
```

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).