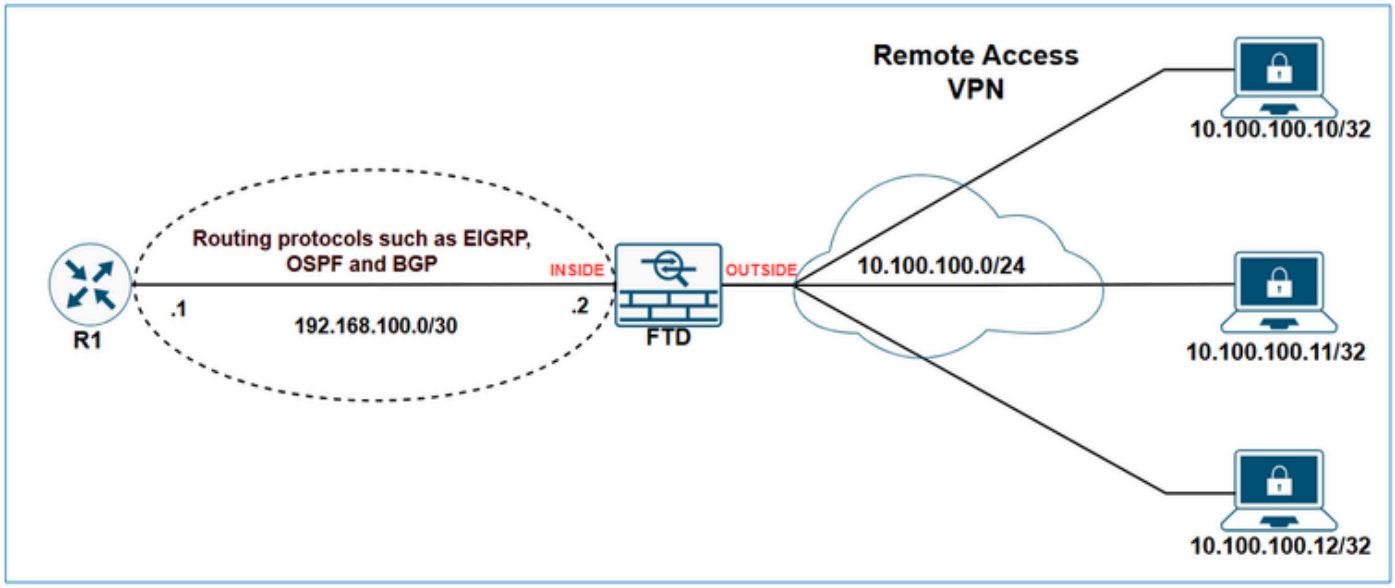
Anunciar subredes VPN de acceso remoto a través de protocolos de enrutamiento en FTD

Contenido

Introducción

Este documento describe las opciones disponibles para anunciar subredes relacionadas con VPN mediante los protocolos de ruteo EIGRP, OSPF y BGP.



Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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.

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

- Cisco Secure Firewall Management Center 7.6.0
- Cisco Secure Firewall 7.6.0

Nota: Este documento describe la configuración para redistribuir subredes VPN de acceso remoto a través de EIGRP, OSPF y BGP mediante FMC. Para obtener orientación sobre la redistribución de rutas con FDM, consulte la guía de configuración de FDM.

Antecedentes

Lo primero que hay que entender es cómo el FTD clasifica las subredes VPN en su tabla de ruteo. Aunque estas subredes aparecen como conectadas por VPN, no se consideran subredes conectadas directamente; en su lugar, se tratan como rutas estáticas.

Los resultados de show lo demuestran.

FTD show route output:

<#root>

```
FTD-1#
```

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 not set

C        10.10.20.0 255.255.255.0 is directly connected, outside
L        10.10.20.1 255.255.255.255 is directly connected, outside
C        192.168.100.0 255.255.255.252 is directly connected, inside
L        192.168.100.2 255.255.255.255 is directly connected, inside

V        10.100.100.10 255.255.255.255 connected by VPN (advertised), outside
```

FTD show route connected output:

<#root>

```
FTD-1#
```

show route connected

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

Gateway of last resort is not set

C        10.10.20.0 255.255.255.0 is directly connected, outside
L        10.10.20.1 255.255.255.255 is directly connected, outside
C        192.168.100.0 255.255.255.252 is directly connected, inside
L        192.168.100.2 255.255.255.255 is directly connected, inside
```

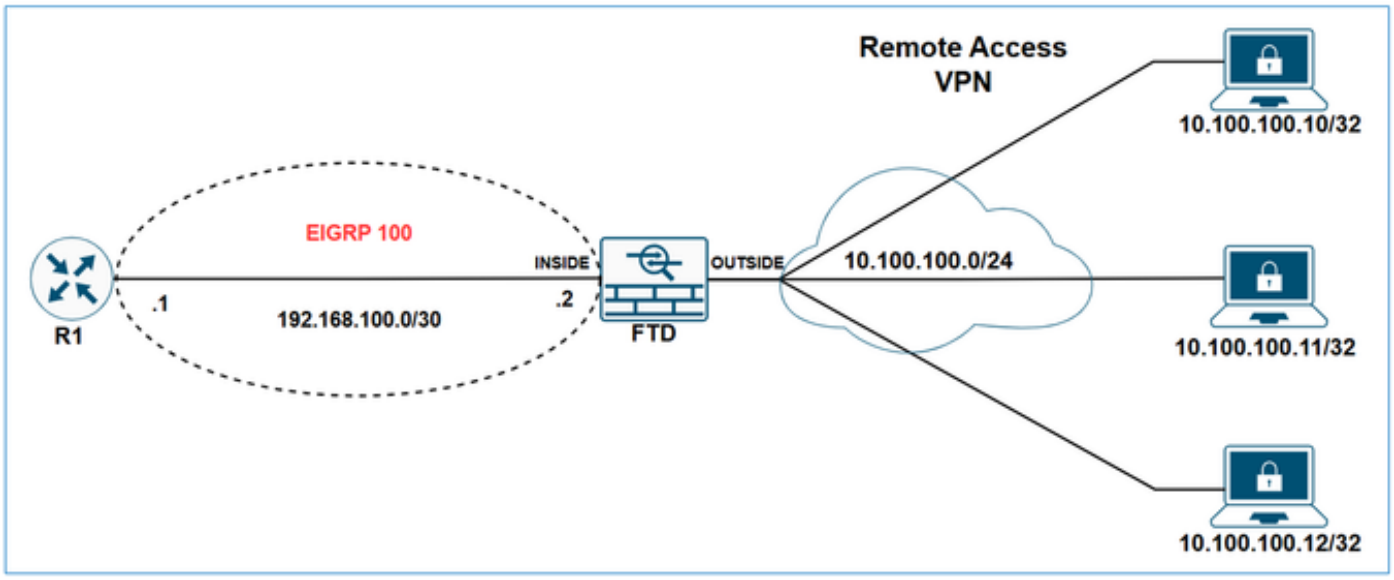
FTD show route static output:

```
<#root>

FTD-HQ-1#

show route static


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

Gateway of last resort is not set


V        10.100.100.10 255.255.255.255 connected by VPN (advertised), outside
```

Ahora que está claro cómo se tratan las subredes VPN en la tabla de ruteo del firewall, el siguiente paso es explorar cómo anunciarlas usando varios protocolos de ruteo.

Redistribución de subredes VPN de acceso remoto a través de EIGRP en FTD

Diagrama de la red



Las rutas estáticas que caen dentro del alcance de una sentencia de red se redistribuyen automáticamente a EIGRP; no es necesario definir una regla de redistribución para ellos. Sin embargo, al redistribuir rutas estáticas que apuntan a interfaces VTI en EIGRP, debe especificar la métrica. Para las rutas estáticas que apuntan a otros tipos de interfaces, no es necesario especificar la métrica.

Debido al comportamiento de EIGRP de redistribuir automáticamente las rutas estáticas que caen dentro del alcance de las sentencias de red, hay dos opciones para anunciar subredes VPN a través de EIGRP en FTD:

1. Uso de una instrucción de red.
2. Uso del enfoque estático de redistribución.

En este ejemplo, el objetivo es hacer que R1 aprenda la subred VPN 10.100.100.0/24 a través de EIGRP.

Configuración inicial de FTD:

```
<#root>

hostname FTD-1
!
ip local pool VPN-POOL1 10.100.100.10-10.100.100.254 mask 255.255.255.0


!
webvpn
...
  group-policy LAB_GROUP1 internal
group-policy LAB_GROUP1 attributes
...
  address-pools value VPN-POOL1
!
router eigrp 100


 no default-information in
 no default-information out
 no eigrp log-neighbor-warnings
 no eigrp log-neighbor-changes
network 192.168.100.0 255.255.255.252
```

FTD Tabla de routing inicial:

```
<#root>

FTD-1#
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 not set

C        10.10.20.0 255.255.255.0 is directly connected, outside
L        10.10.20.1 255.255.255.255 is directly connected, outside
C        192.168.100.0 255.255.255.252 is directly connected, inside
L        192.168.100.2 255.255.255.255 is directly connected, inside

V       10.100.100.10 255.255.255.255 connected by VPN (advertised), outside
```

Tabla de topología EIGRP inicial de FTD:

<#root>

```
FTD-1#

show eigrp topology



EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.100.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.100.0 255.255.255.252, 1 successors, FD is 512 via Connected, inside
```

Tabla de ruteo inicial R1:

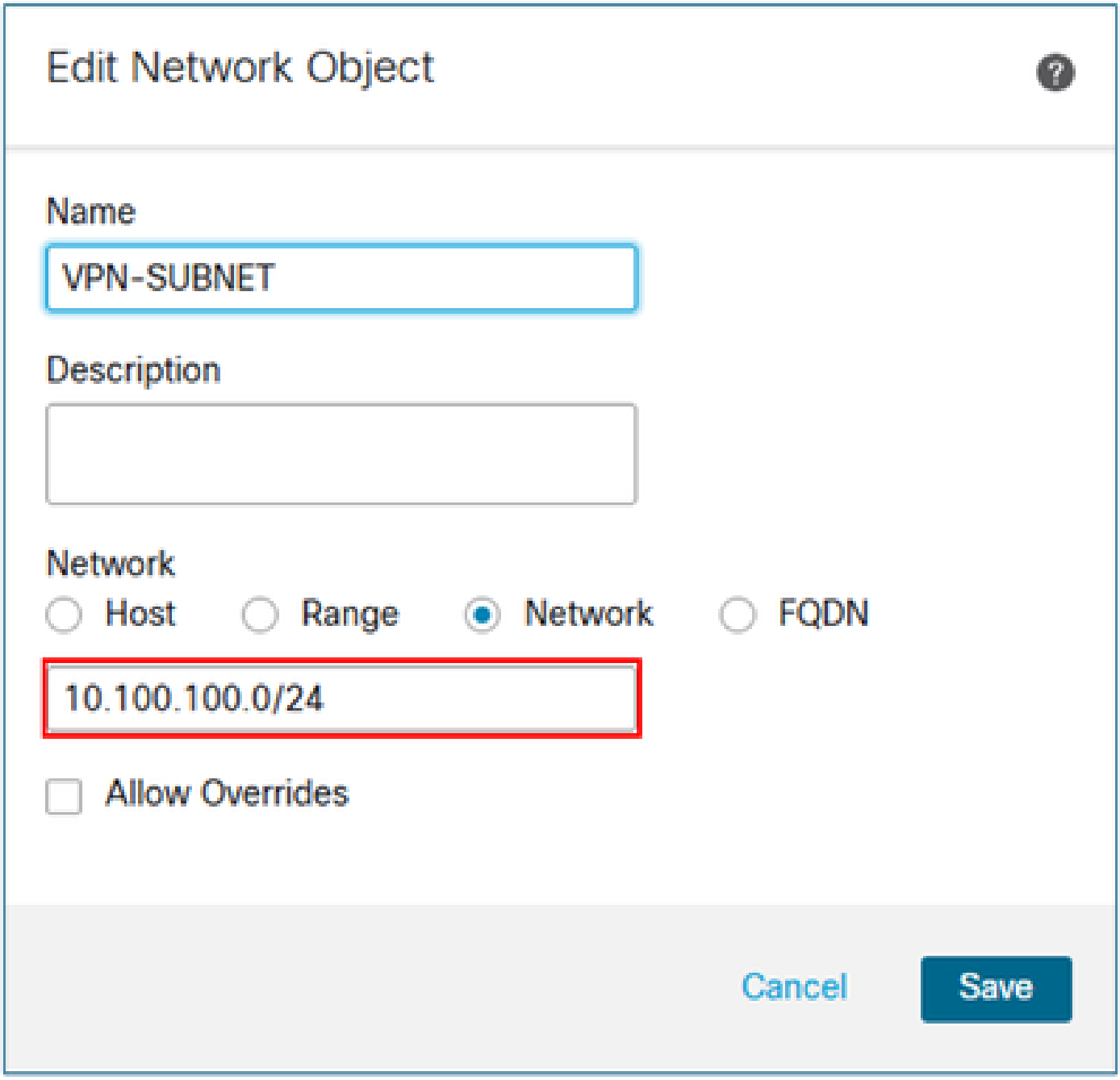
<#root>

```
R1#

show ip 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
```

Redistribución de subredes VPN de acceso remoto a través de EIGRP en FTD mediante una sentencia de red

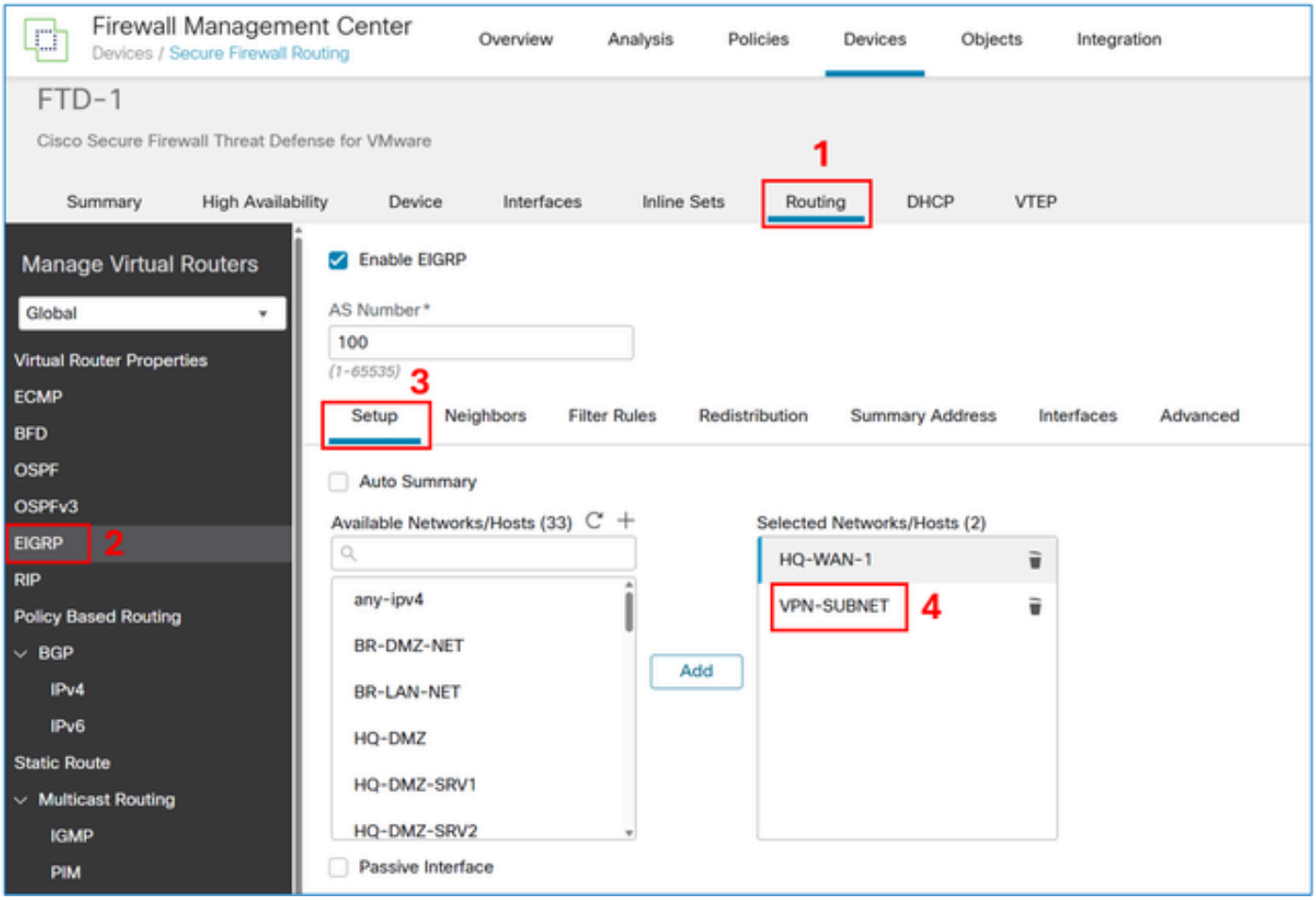
Configurar

Paso 1. Cree un objeto de red para la subred VPN.



Paso 2. Incluya el objeto de subred VPN en la instrucción de red.

En la IU de administración de dispositivos FMC, navegue hasta Routing > EIGRP > Setup e incluya la subred VPN en las redes/hosts seleccionados.



Guardar e implementar la configuración en el FTD.

Verificación

Configuración de FTD EIGRP:

<#root>

FTD-1#

show run router

```
router eigrp 100
 no default-information in
 no default-information out
 no eigrp log-neighbor-warnings
 no eigrp log-neighbor-changes
 network 10.100.100.0 255.255.255.0
 network 192.168.100.0 255.255.255.252
```

Tabla de topología FTD EIGRP:

<#root>

FTD-1#

show eigrp topology

EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.100.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.100.100.10 255.255.255.255, 1 successors, FD is 512

via Rstatic (512/0)

P 192.168.100.0 255.255.255.252, 1 successors, FD is 512
via Connected, inside

Tabla de ruteo R1:

<#root>

R1#

show ip 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C   192.168.100.0/30 is directly connected, GigabitEthernet1
L   192.168.100.1/32 is directly connected, GigabitEthernet1
      10.0.0.0/32 is subnetted, 1 subnets

D   10.100.100.10

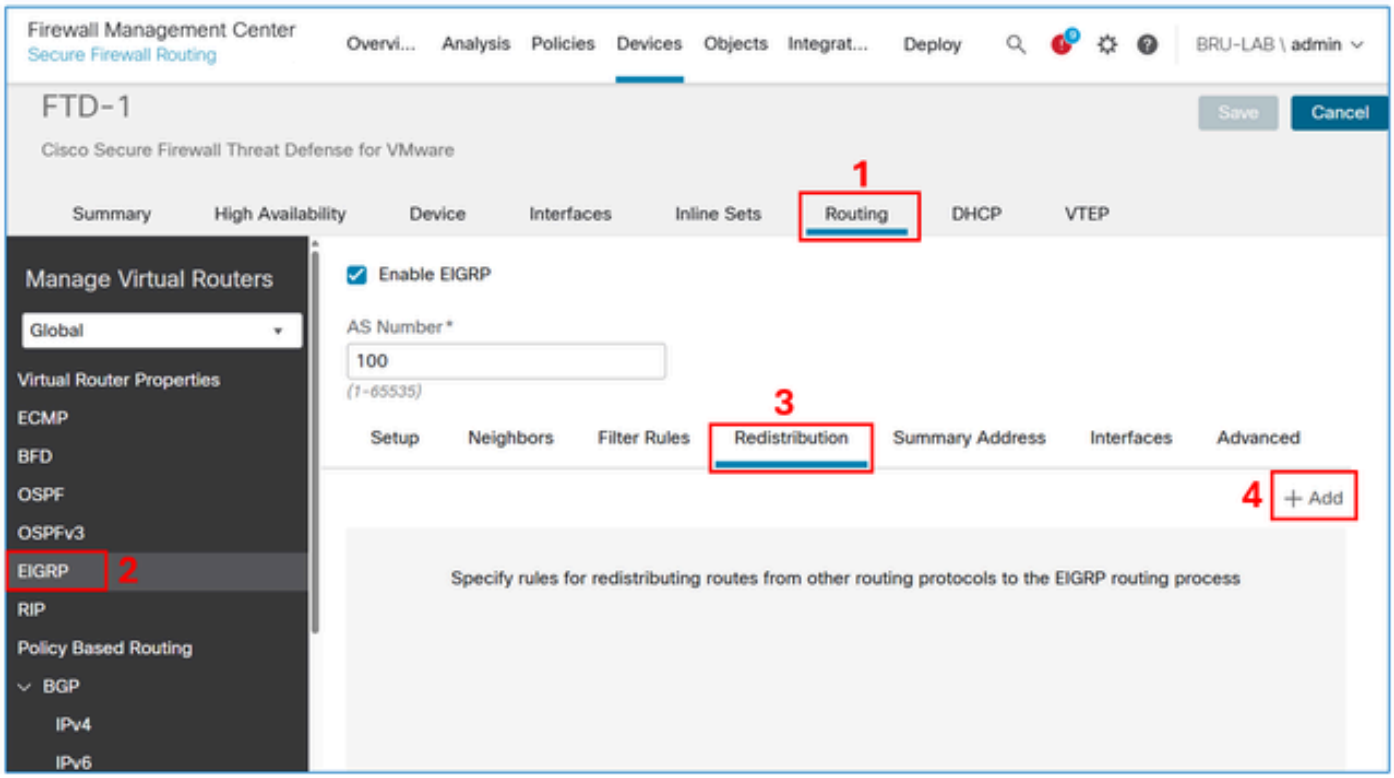
[90/3072] via 192.168.100.2, 00:02:17, GigabitEthernet1

Nota: Tenga en cuenta que aunque la sentencia de red era 10.100.100.0/24, el FTD redistribuye una subred /32 sobre EIGRP. Esto ocurre porque el FTD crea una ruta estática con un prefijo /32 para cada sesión VPN de acceso remoto. Para optimizar esto, puede utilizar la función EIGRP Summary Address .

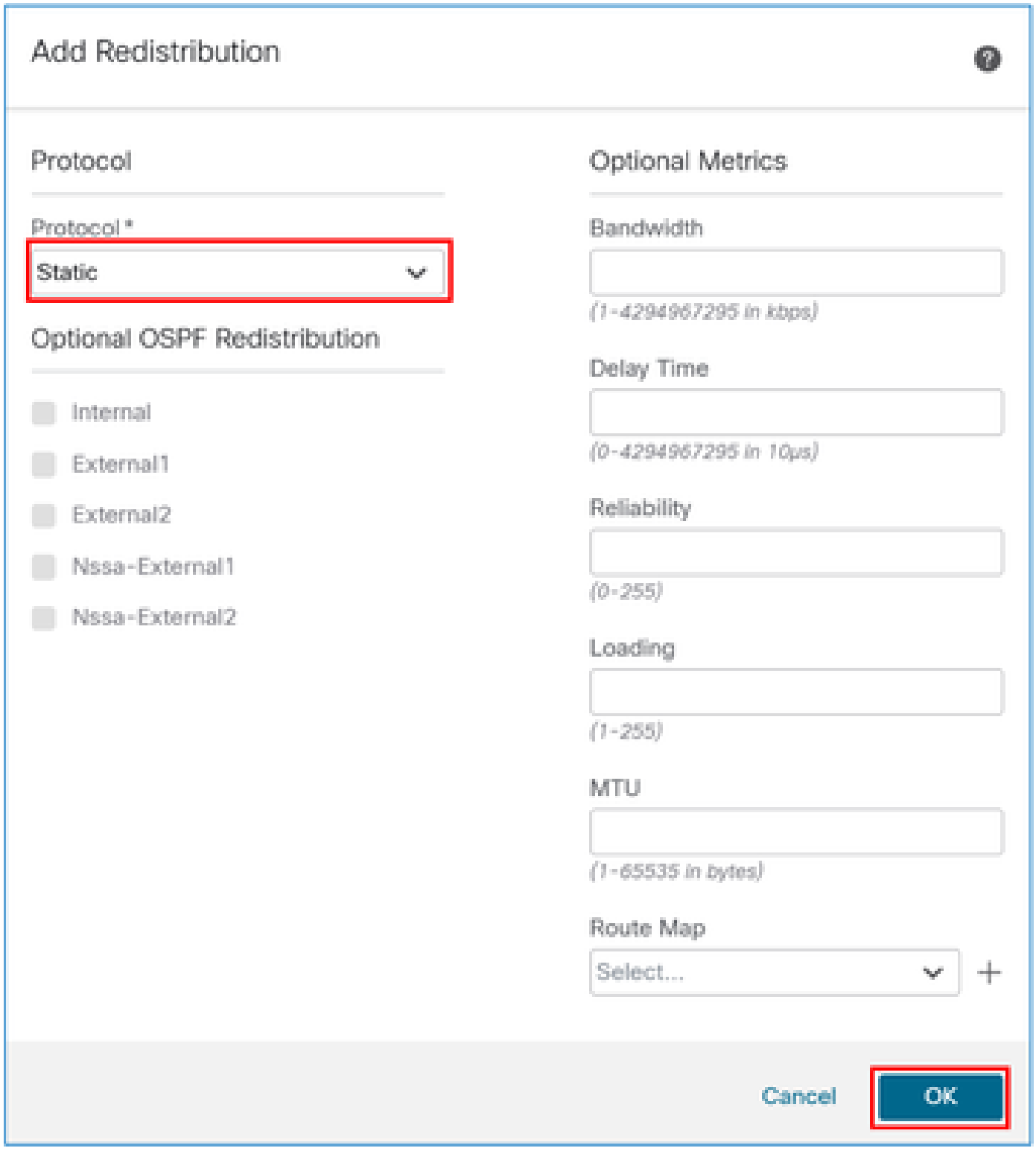
Redistribución de subredes VPN de acceso remoto a través de EIGRP en FTD mediante el enfoque estático de redistribución

Configurar

En la IU de administración de dispositivos FMC, navegue hasta Routing > EIGRP > Redistribution y luego seleccione el botón Add.

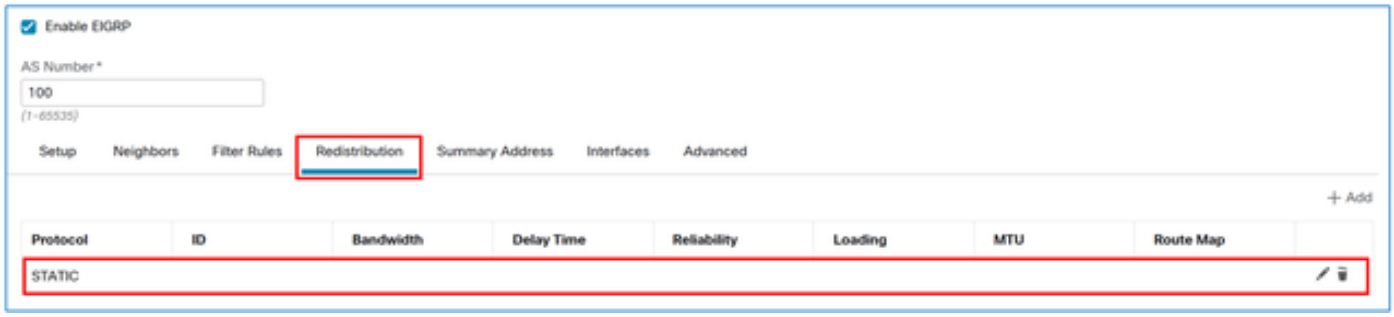


En el campo de protocolo, seleccione Estático y, a continuación, seleccione el botón Aceptar.



⚠ Precaución: Esto redistribuye todas las rutas estáticas en EIGRP. Si necesita anunciar solamente las subredes VPN, puede utilizar el enfoque de sentencia de red o aplicar un route map para filtrarlas.

El resultado:



Guardar e implementar la configuración en el FTD.

Verificación

Configuración de FTD EIGRP:

```
<#root>

FTD-HQ-1#

show run router


router eigrp 100
 no default-information in
 no default-information out
 no eigrp log-neighbor-warnings
 no eigrp log-neighbor-changes
 network 192.168.100.0 255.255.255.252

 redistribute static
```

Tabla de topología FTD EIGRP:

```
<#root>

FTD-1#

show eigrp topology


EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.100.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status


P 10.100.100.10 255.255.255.255, 1 successors, FD is 512


        via Rstatic (512/0)


P 192.168.100.0 255.255.255.252, 1 successors, FD is 512
        via Connected, inside
```

Tabla de ruteo R1:

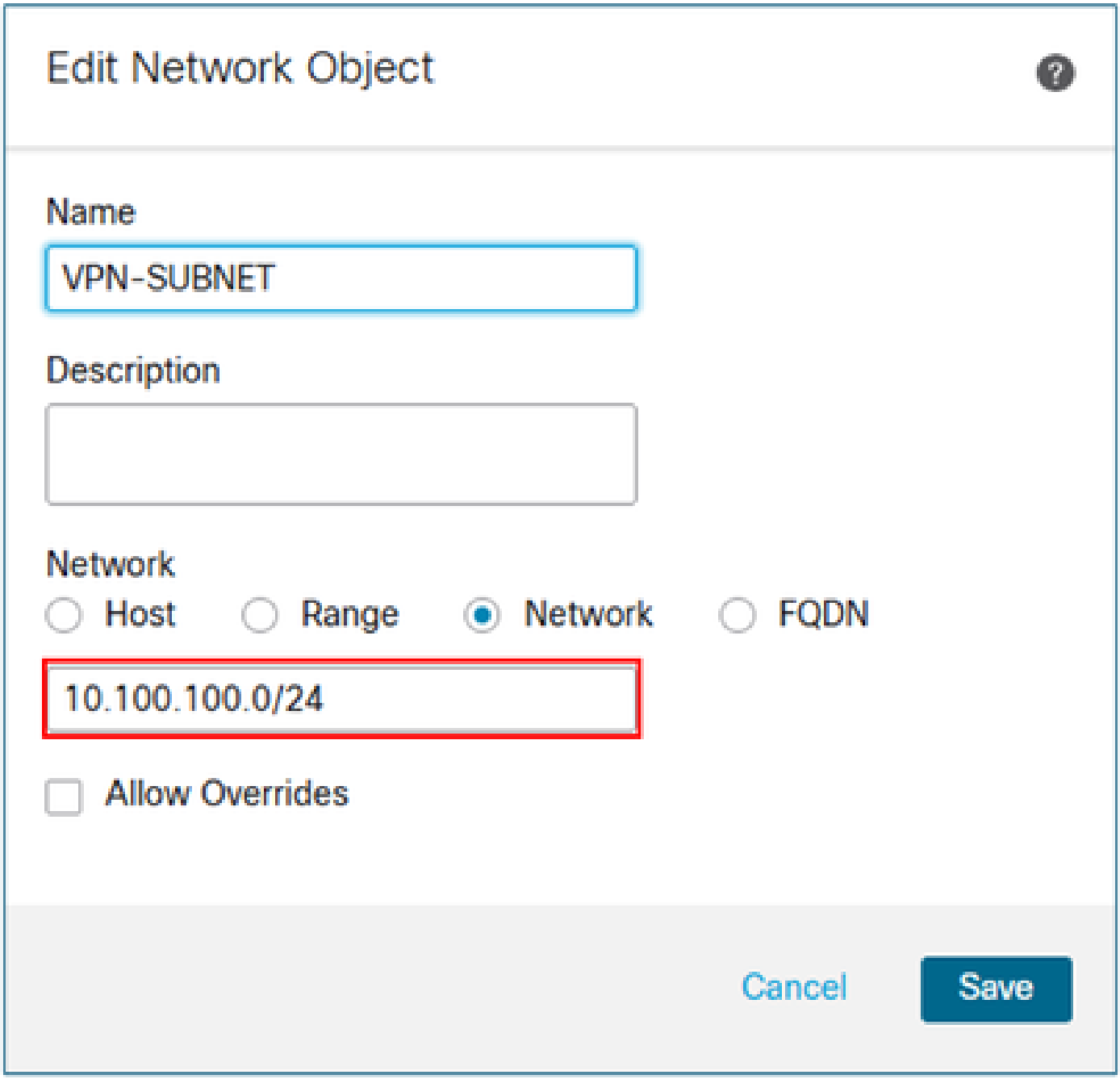
```
<#root>

R1#

show ip 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1

D EX     10.100.100.10


           [170/3072] via 192.168.100.2, 00:03:52, GigabitEthernet1
```

Consejo: Opcionalmente, puede utilizar la función de dirección de resumen EIGRP en FTD para optimizar el tamaño de la tabla de ruteo.

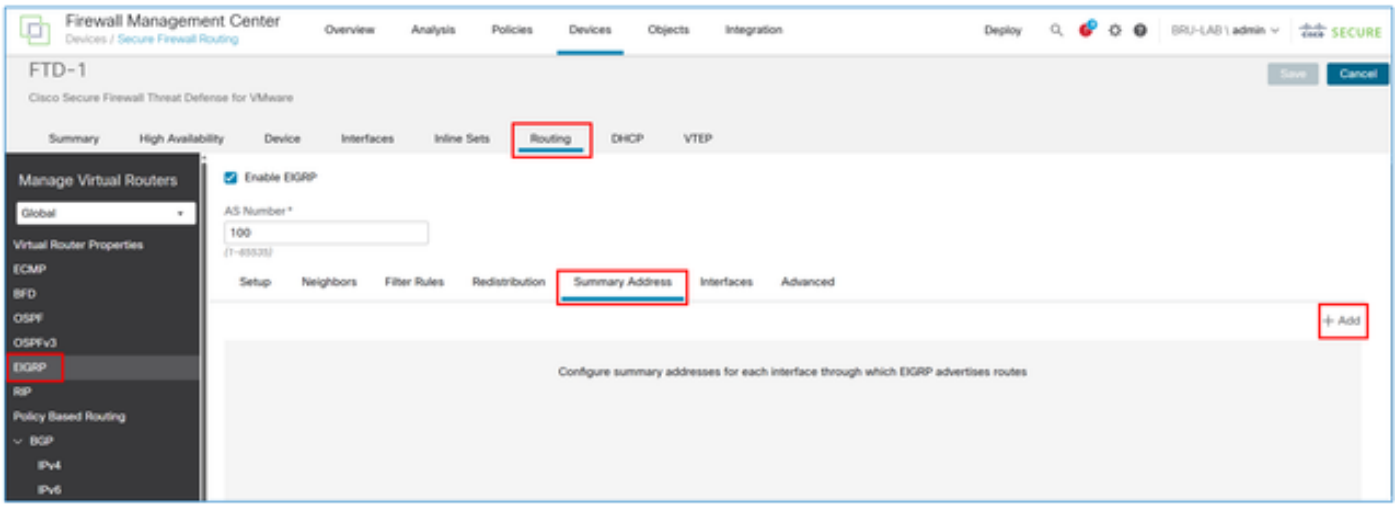
Configuración de dirección de resumen EIGRP

Configurar

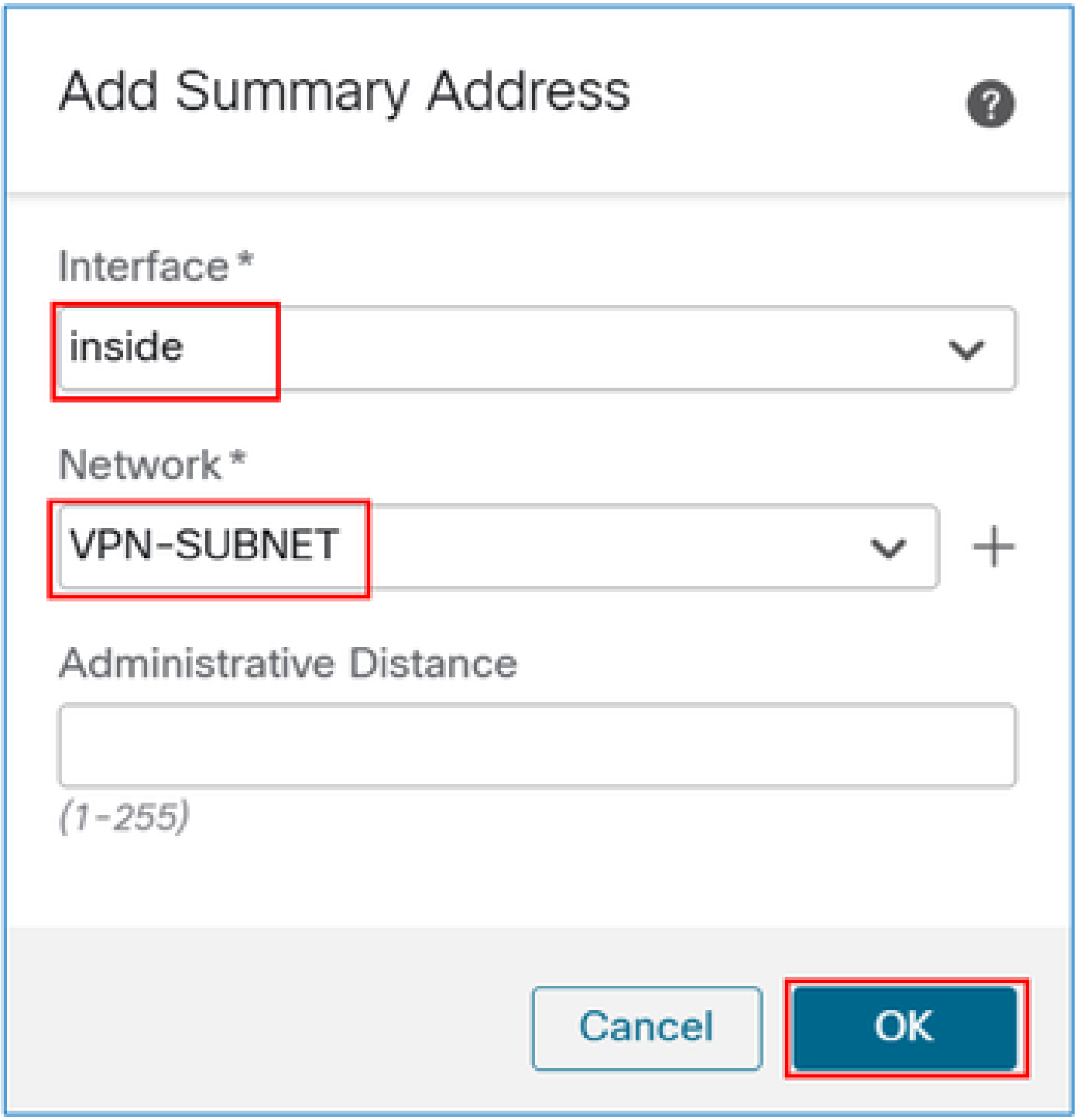
Si aún no se ha creado, cree un objeto de red para las subredes VPN.



En la UI de administración de dispositivos FMC, navegue hasta Routing > EIGRP > Summary Address y luego seleccione el botón Add.



En el campo interface, ingrese el que está frente al vecino EIGRP, y en el campo network, ingrese el objeto creado para la subred VPN.



El resultado:

Verificación

Configuración de la dirección de resumen EIGRP de FTD:

<#root>

FTD-1#

sh run interface

```
interface GigabitEthernet0/0
 nameif inside
 security-level 0
 zone-member inside
 ip address 192.168.100.2 255.255.255.252
```

summary-address eigrp 100 10.100.100.0 255.255.255.0

Tabla de topología FTD EIGRP:

<#root>

FTD-1#

show eigrp topology

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.100.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.100.100.10 255.255.255.255, 1 successors, FD is 512
        via Rstatic (512/0)
```

P 10.100.100.0 255.255.255.0, 1 successors, FD is 512

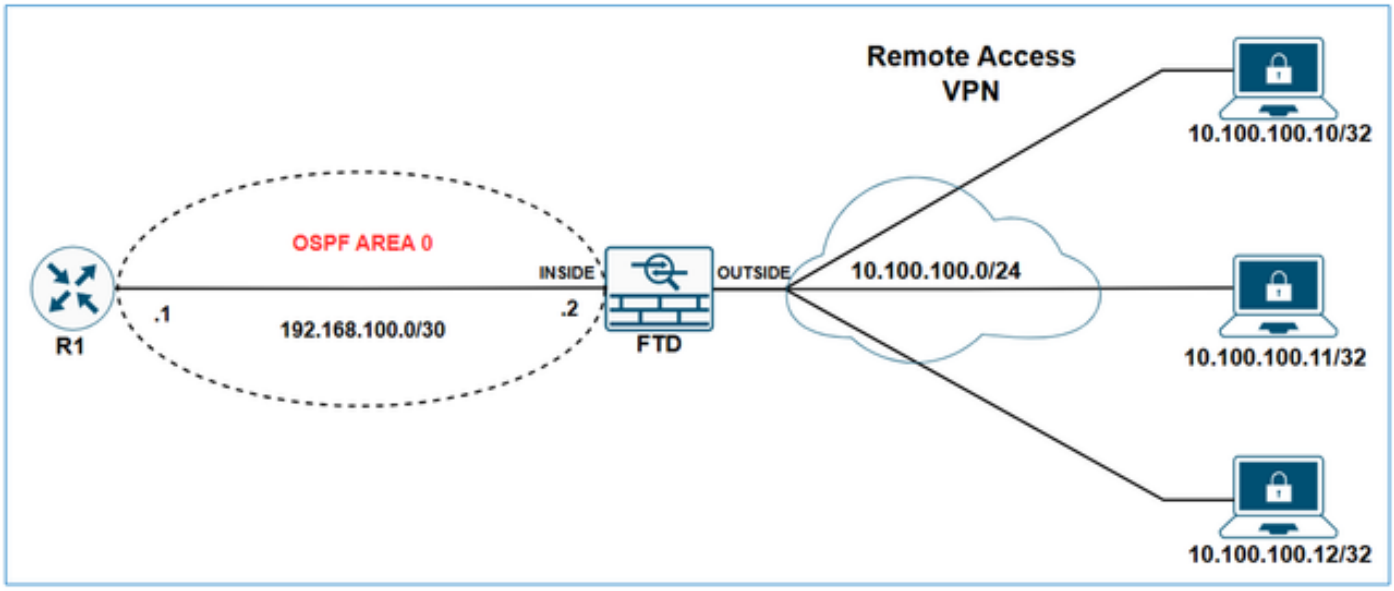
```
        via Summary (512/0), Null0


P 192.168.100.0 255.255.255.0, 1 successors, FD is 512
        via Connected, inside
```

Tabla de ruteo R1:

```
<#root>

R1#

show ip 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
      10.0.0.0/24 is subnetted, 1 subnets

D        10.100.100.0 [90/3072] via 192.168.100.2, 00:01:54, GigabitEthernet1
```

Redistribución de subredes VPN de acceso remoto a través de OSPF en FTD

Diagrama de la red



Configuraciones iniciales

<#root>

```
ip local pool VPN-POOL1 10.100.100.10-10.100.100.254 mask 255.255.255.0
```

```
!
webvpn
  group-policy LAB_GROUP1 internal
...
group-policy LAB_GROUP1 attributes
...
```

```
address-pools value VPN-POOL1
```

```
!
router ospf 1
```

```
network 192.168.100.0 255.255.255.252 area 0
```

FTD show ospf neighbor output:

<#root>

```
FTD-1#
```

```
show ospf neighbor
```

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.100.1     1   FULL/DR         0:00:39     192.168.100.1   inside
```

R1 show ip ospf neighbor output:

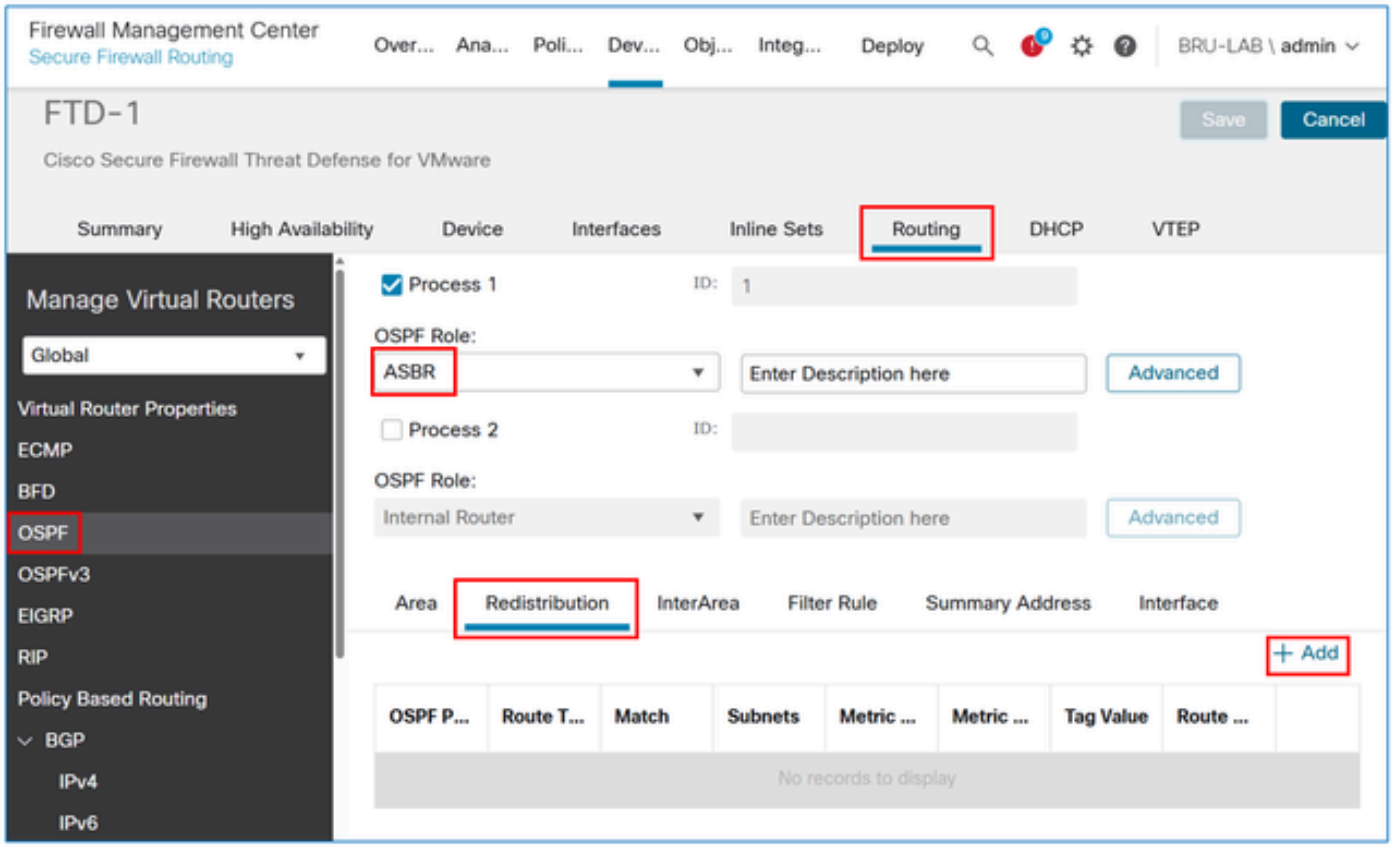
```
<#root>

R1#

show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.100.2     1   FULL/BDR        00:00:37    192.168.100.2   GigabitEthernet1
```

Tabla de ruteo R1:

```
<#root>

R1#

show ip 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
```

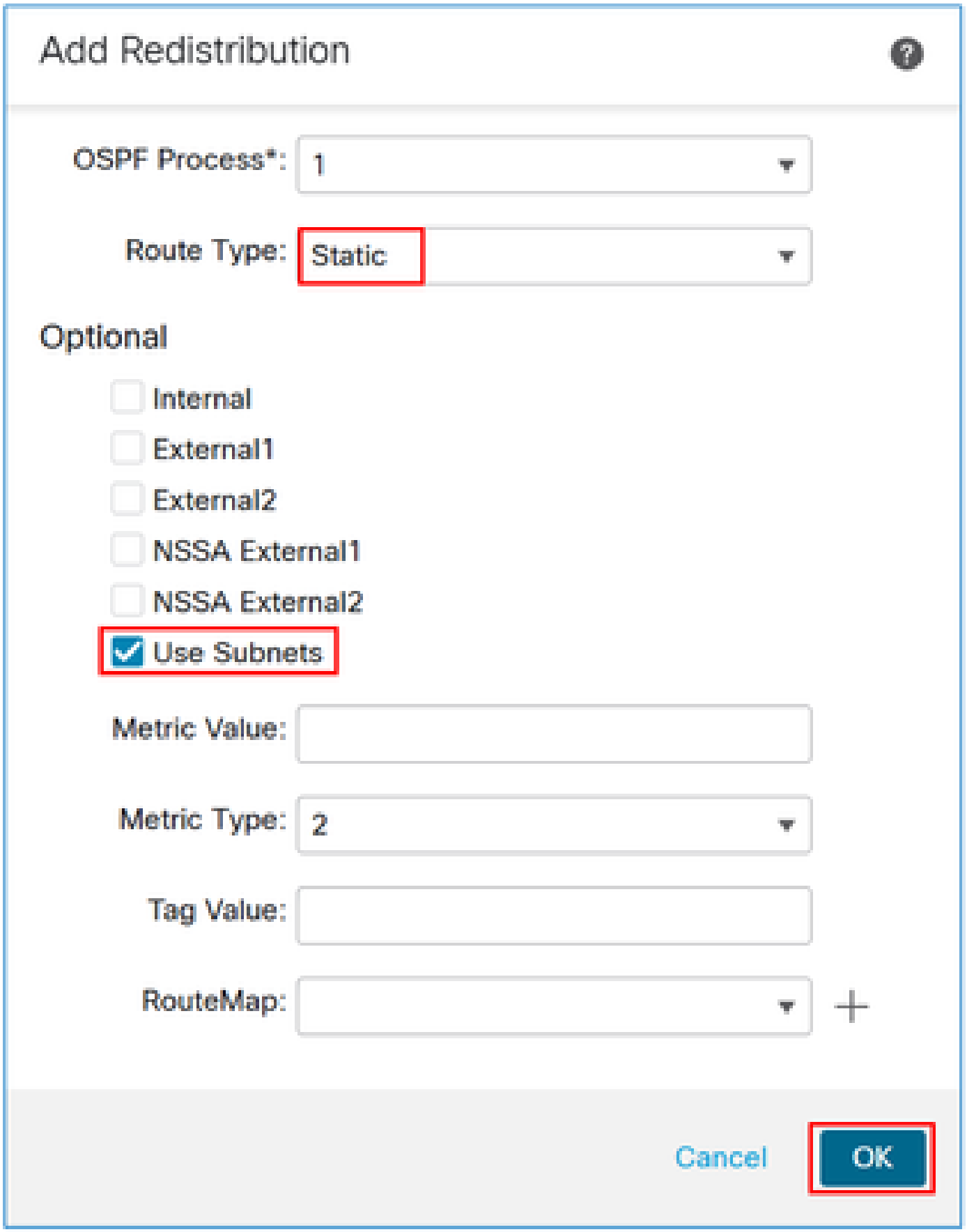
Configurar

En la IU de administración de dispositivos FMC, navegue hasta Routing > OSPF > Redistribución, y luego seleccione el botón Add.



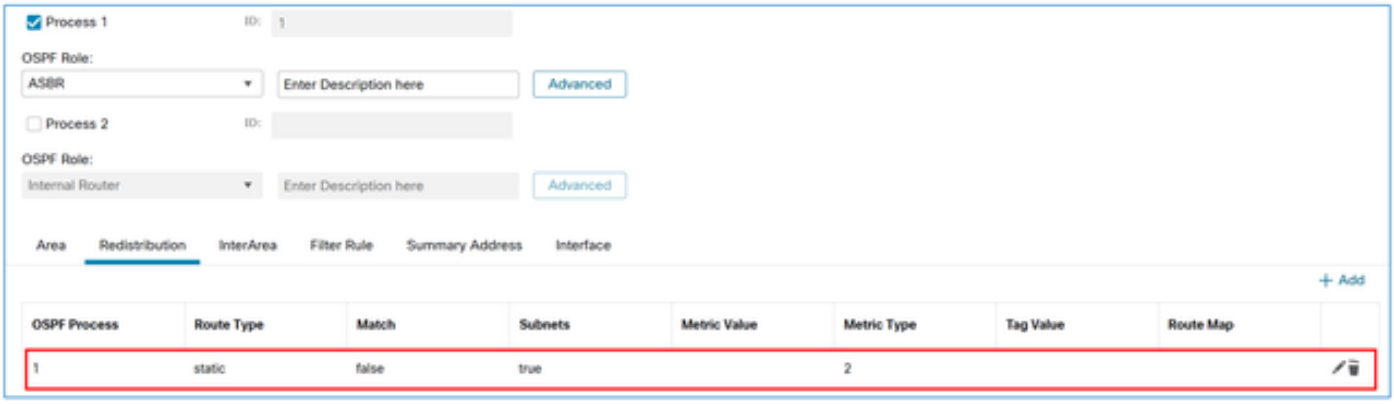
Nota: El rol OSPF debe configurarse como ASBR o ABR & ASBR para habilitar la redistribución.

En el campo Route Type, seleccione Static y, a continuación, marque la casilla Use Subnets.



⚠ Precaución: Esto redistribuye todas las rutas estáticas en OSPF. Si necesita anunciar solamente las subredes VPN, puede aplicar un route map para filtrarlas.

El resultado:



Verificación

Configuración de redistribución OSPF FTD:

```
<#root>

FTD-1#

sh run router


router ospf 1
 network 192.168.100.0 255.255.255.252 area 0

 redistribute static subnets
```

Tabla de ruteo R1:

```
<#root>

R1#

show ip 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set
```

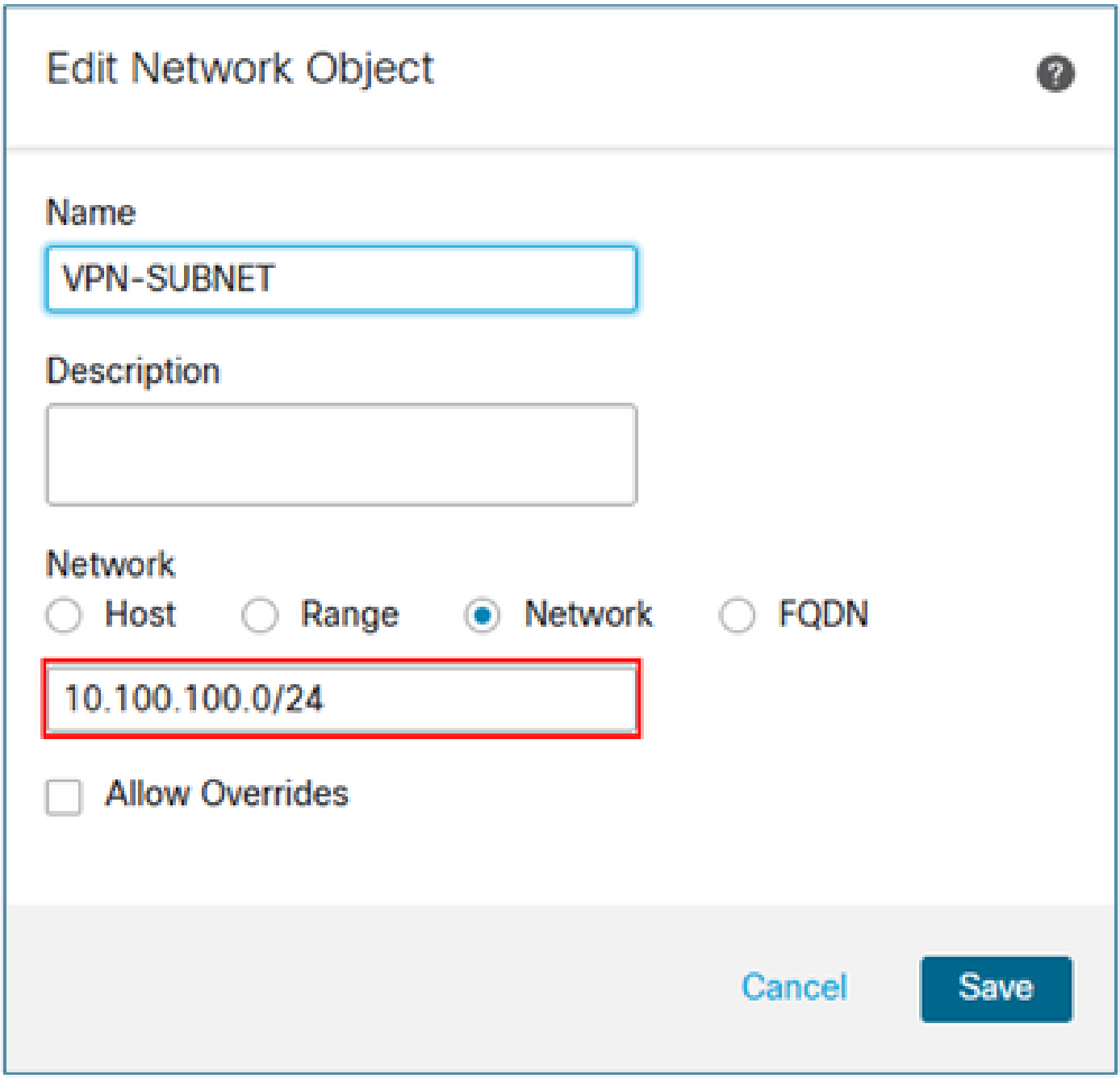
```
C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
      10.0.0.0/32 is subnetted, 1 subnets
O E2     10.100.100.10 [110/20] via 192.168.100.2, 00:08:01, GigabitEthernet1
```

Consejo: Tenga en cuenta que aunque el grupo VPN es 10.100.100.0/24, el FTD redistribuye una subred /32 sobre OSPF. Esto ocurre porque el FTD crea una ruta estática con un prefijo /32 para cada sesión VPN de acceso remoto. Para optimizar esto, puede utilizar la función OSPF Summary Address .

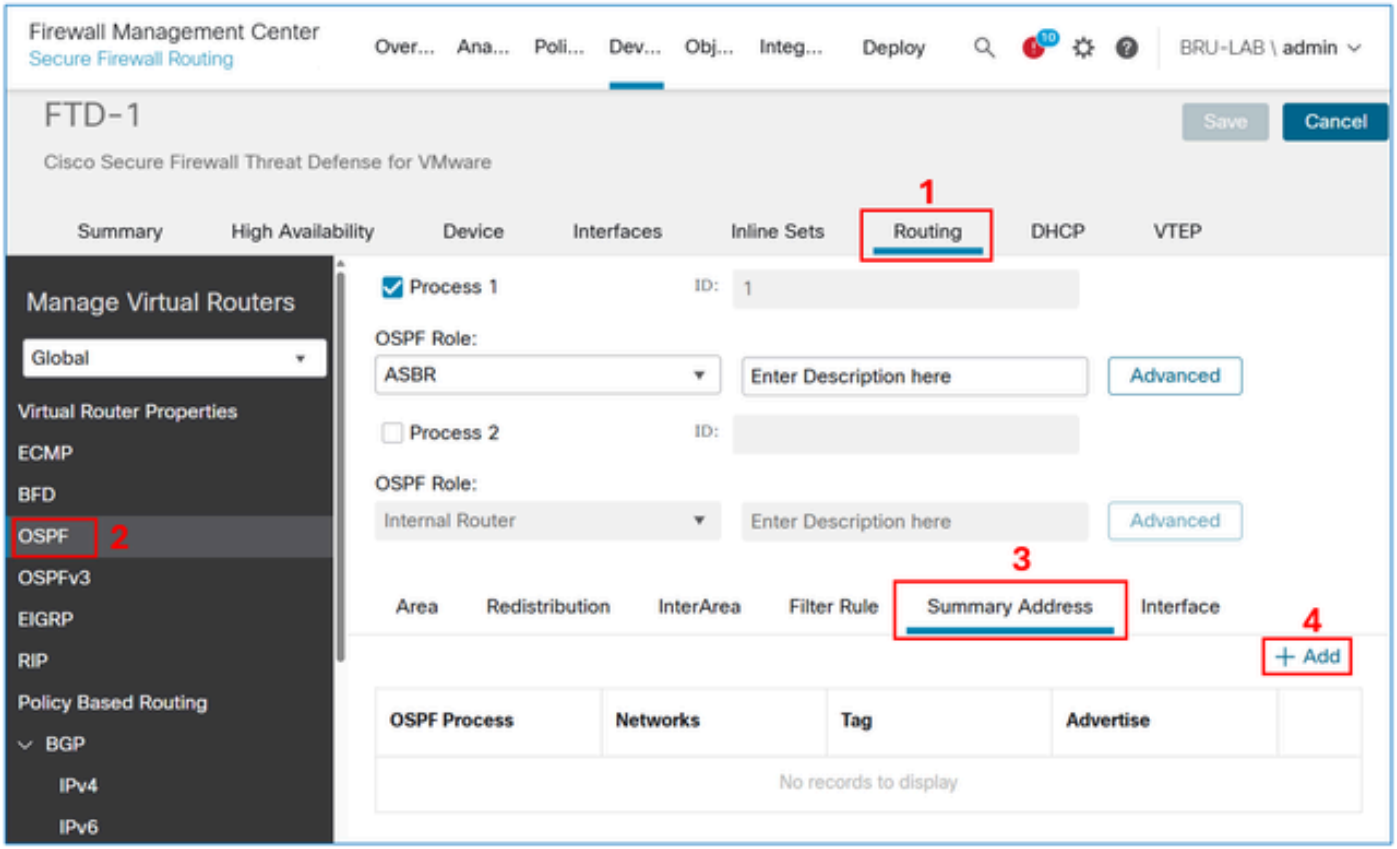
Configuración de dirección de resumen OSPF

Configurar

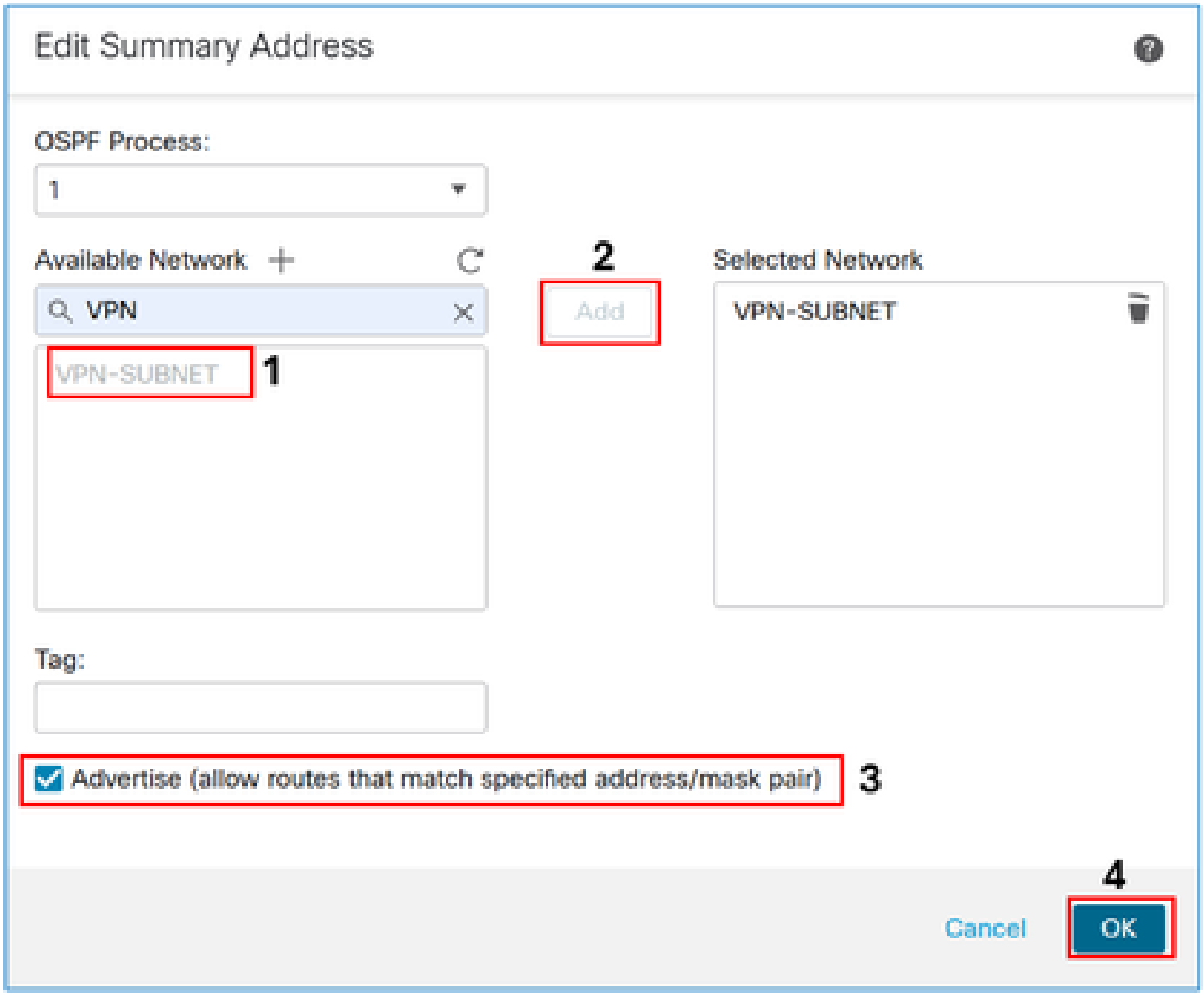
Si aún no se ha creado, cree un objeto de red para las subredes VPN.



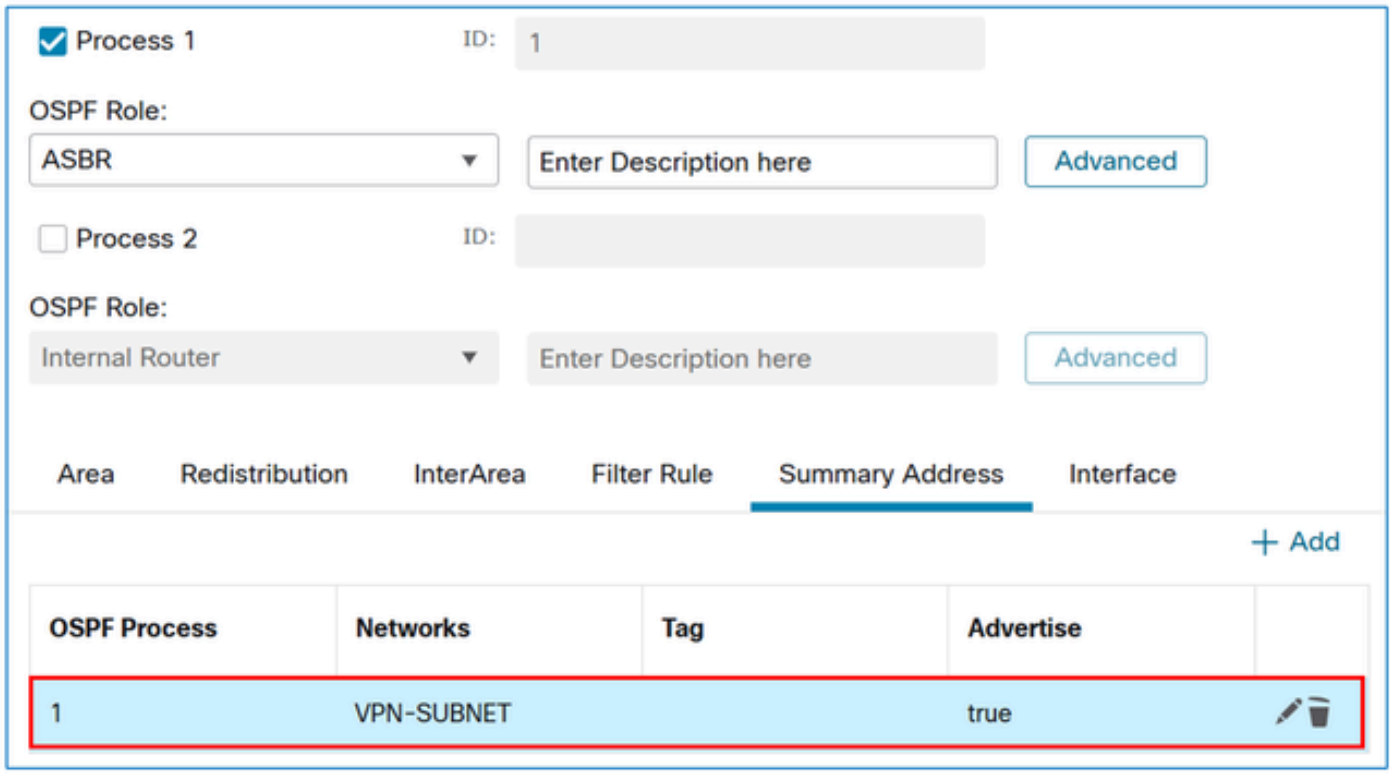
En la IU de administración de dispositivos FMC, navegue hasta Routing > OSPF> Summary Address y, a continuación, seleccione el botón Add.



Agregue el objeto de subred VPN y seleccione la casilla de verificación Advertise.



El resultado:



Verificación

Configuración OSPF de FTD:

<#root>

FTD-1#

sh run router

router ospf 1
 network 192.168.100.0 255.255.255.252 area 0

redistribute static subnets

summary-address 10.100.100.0 255.255.255.0

Tabla de ruteo R1:

<#root>

R1#

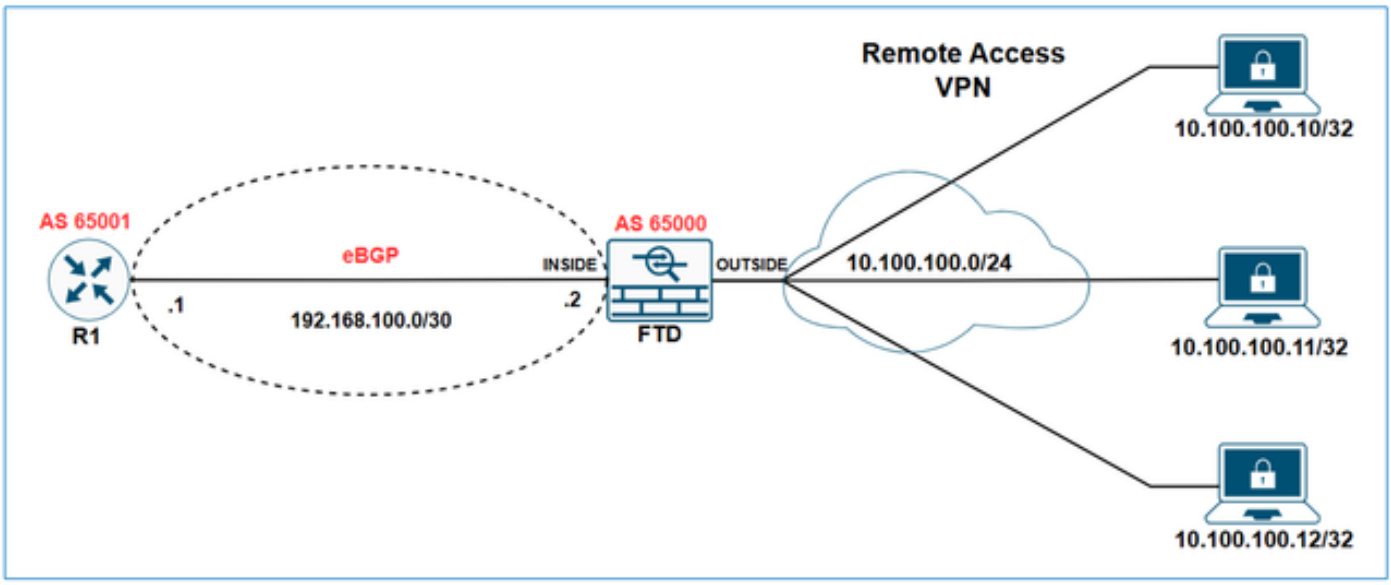
sh ip route

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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
      10.0.0.0/24 is subnetted, 1 subnets
O E2     10.100.100.0 [110/20] via 192.168.100.2, 00:00:26, GigabitEthernet1
```

Redistribución de subredes VPN de acceso remoto a través de eBGP en FTD

Diagrama de la red



En este ejemplo, el objetivo es hacer que R1 aprenda la subred VPN 10.100.100.0/24 vía eBGP.

Configuraciones iniciales

FTD Configuración inicial:

<#root>

```
hostname FTD-1
!
ip local pool VPN-POOL1 10.100.100.10-10.100.100.254 mask 255.255.255.0

!
```

```
webvpn
...
  group-policy LAB_GROUP1 internal
group-policy LAB_GROUP1 attributes
...
```

address-pools value VPN-POOL1

```
!
router bgp 65000
 bgp log-neighbor-changes
 bgp router-id vrf auto-assign
 address-family ipv4 unicast
  neighbor 192.168.100.1 remote-as 65001
  neighbor 192.168.100.1 transport path-mtu-discovery disable
  neighbor 192.168.100.1 activate
  no auto-summary
  no synchronization
 exit-address-family
```

Resultado de la tabla bgp de FTD:

<#root>

FTD-1#

show bgp

```
BGP table version is 25, local router ID is 192.168.100.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network               Next Hop        Metric LocPrf Weight  Path
```

r> 192.168.100.0/30 192.168.100.1   1   0 65001 ?

Resultado del resumen de FTD show bgp:

<#root>

FTD-1#

show bgp summary

```
BGP router identifier 192.168.100.2, local AS number 65000
BGP table version is 25, main routing table version 25
1 network entries using 2000 bytes of memory
17 path entries using 1360 bytes of memory
3/3 BGP path/bestpath attribute entries using 624 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
```

```
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4032 total bytes of memory
BGP activity 176/166 prefixes, 257/240 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

192.168.100.1  4        65001 4589    3769          25    0    0 2d21h  8
```

R1 show ip bgp summary output:

<#root>

```
R1#

sh ip bgp summary


BGP router identifier 192.168.100.1, local AS number 65001
BGP table version is 258, main routing table version 258
1 network entries using 2480 bytes of memory
1 path entries using 2312 bytes of memory
1/1 BGP path/bestpath attribute entries using 864 bytes of memory
1 BGP AS-PATH entries using 64 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 5720 total bytes of memory
BGP activity 85/75 prefixes, 244/227 paths, scan interval 60 secs
12 networks peaked at 11:10:00 Apr 17 2025 UTC (00:06:27.485 ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.100.2  4        65000    3770    4590      258    0    0 2d21h           9
```

Resultado de la tabla bgp R1:

<#root>

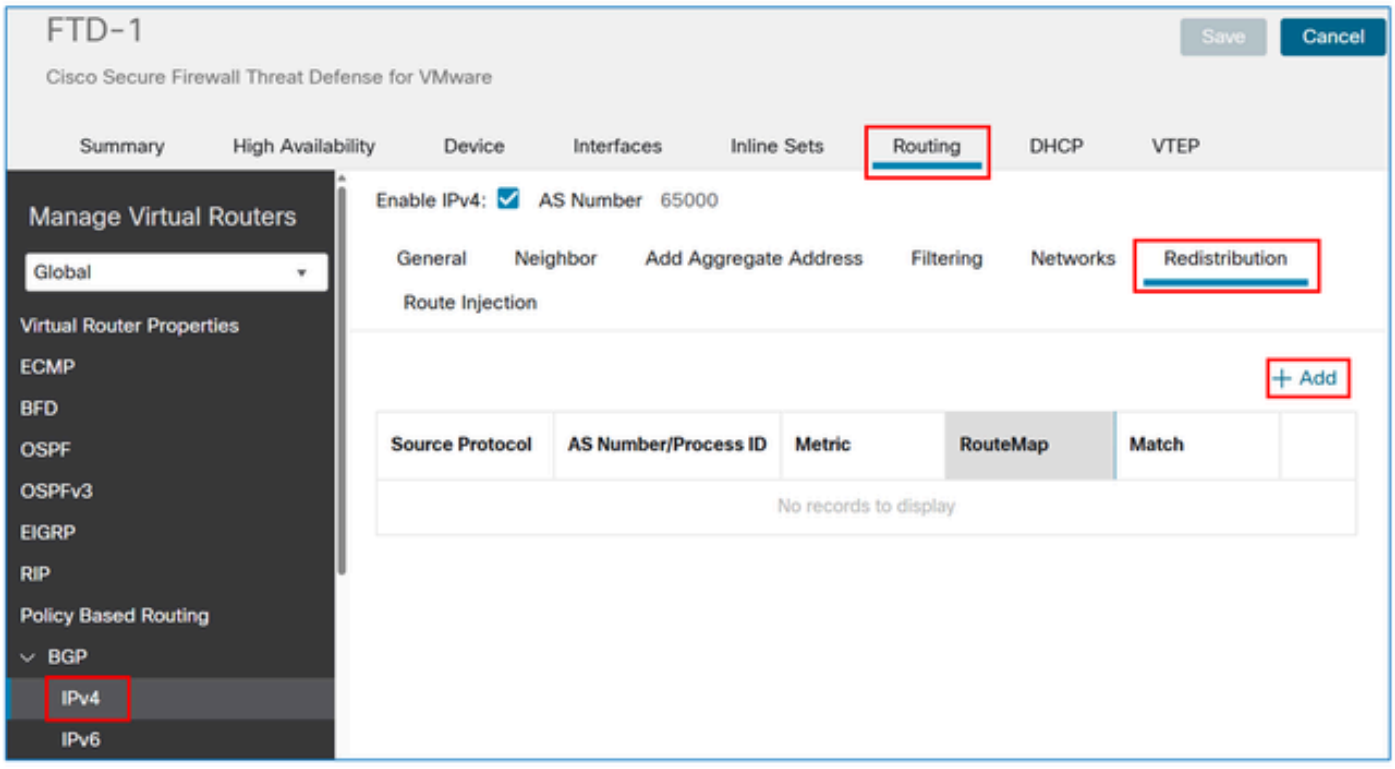
```
R1#

show ip bgp


BGP table version is 258, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
               t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
       Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.100.0/30                      0.0.0.0                  1         32768 ?
```

Tabla de ruteo R1:

```
<#root>

R1#

show ip 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
```

Configurar

En la interfaz de usuario de administración de dispositivos FMC, navegue hasta Routing > BGP > IPv4 > Redistribución y, a continuación, seleccione el botón Add.



En el campo Source Protocol, elija Static, y luego seleccione el botón OK.

Add Redistribution

Source Protocol

Static

Process ID*

Metric

(0-4294967295)

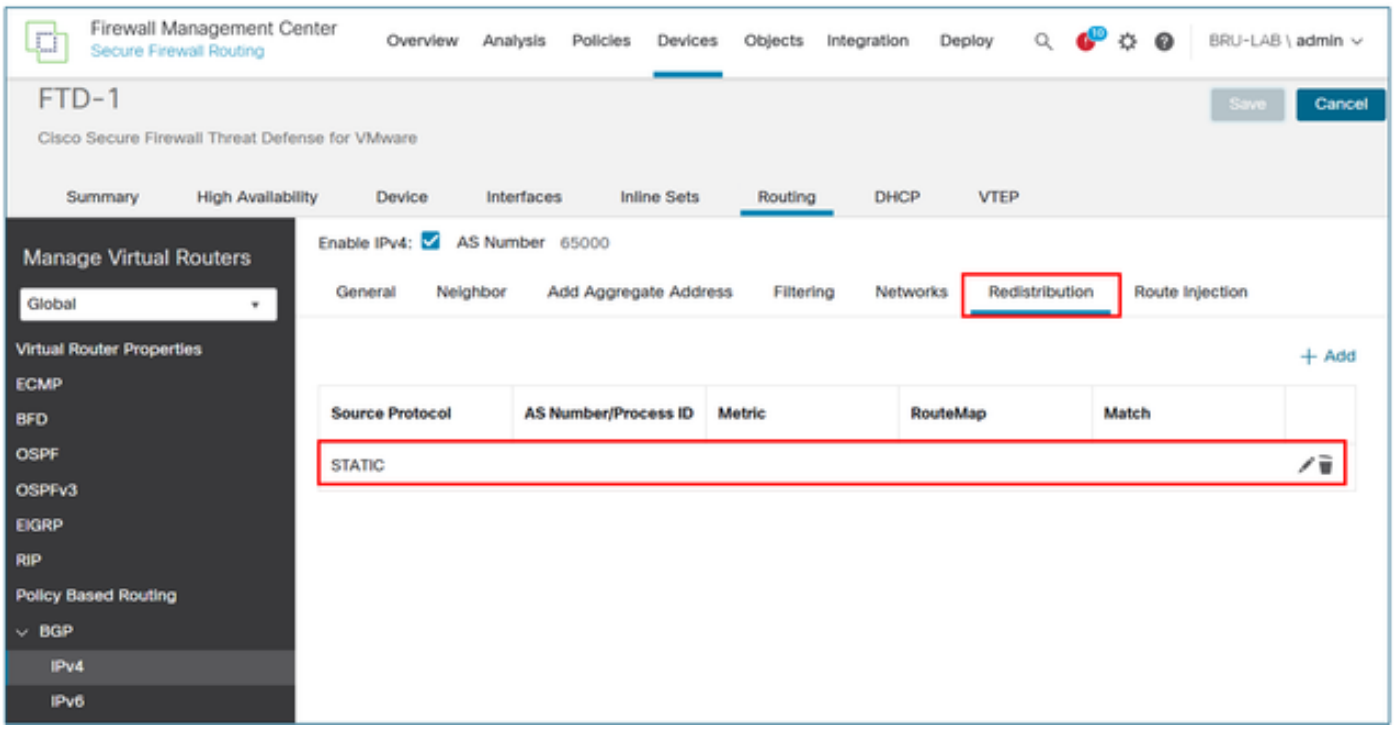
Route Map

Match

- Internal
- External 1
- External 2
- NSSAExternal 1
- NSSAExternal 2

⚠ : Esto redistribuye todas las rutas estáticas en BGP. Si necesita anunciar solamente las subredes VPN, puede aplicar un route map para filtrarlas.

El resultado:



Guardar e implementar la configuración en el FTD.

Verificación

Configuración BGP de FTD:

```
<#root>

FTD-HQ-1#

show run router


router bgp 65000
 bgp log-neighbor-changes
 bgp router-id vrf auto-assign
 address-family ipv4 unicast
  neighbor 192.168.100.1 remote-as 65001
  neighbor 192.168.100.1 transport path-mtu-discovery disable
  neighbor 192.168.100.1 activate

  redistribute static


  no auto-summary
  no synchronization
 exit-address-family
```

Resultado de la tabla bgp de FTD:

```
<#root>

FTD-1#

show bgp



BGP table version is 26, local router ID is 192.168.100.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop        Metric LocPrf Weight  Path

*> 10.100.100.10/32 10.100.100.10        0         32768  ?


r> 192.168.100.0/30 192.168.100.1      1             0  65001 ?
```

Resultado de la tabla bgp R1:

```
<#root>

R1#

show ip bgp



BGP table version is 259, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path

 *>   10.100.100.10/32 192.168.100.2           0             0 65000 ?


 *>   192.168.100.0/30  0.0.0.0                 1         32768 ?
```

Resultado de la tabla de ruteo R1:

```
<#root>

R1#

show ip route
```

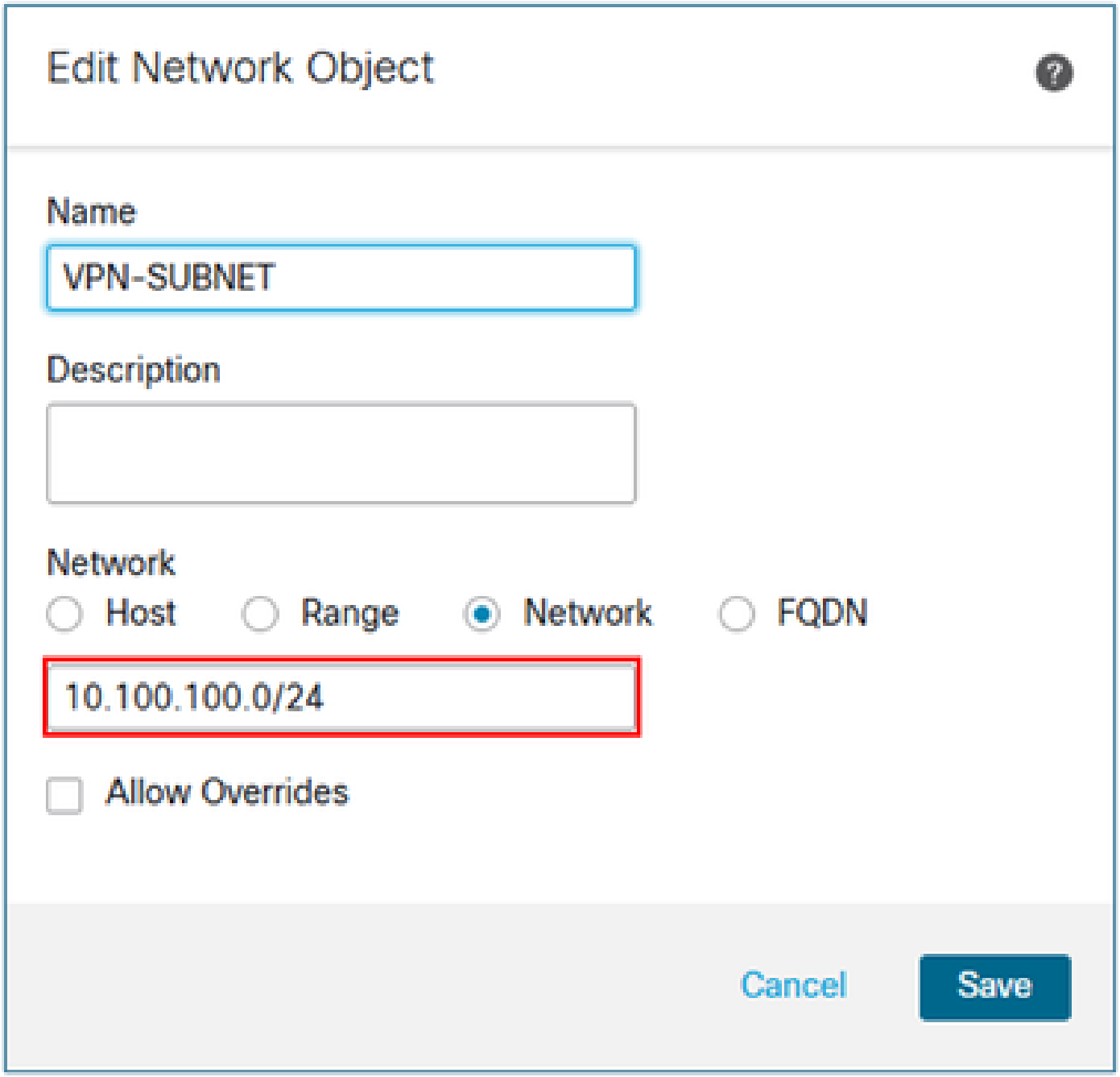
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
      10.0.0.0/32 is subnetted, 1 subnets
B        10.100.100.10 [20/0] via 192.168.100.2, 00:02:00
```

Consejo: Tenga en cuenta que aunque el grupo VPN es 10.100.100.0/24, el FTD redistribuye una subred /32 sobre BGP. Esto ocurre porque el FTD crea una ruta estática con un prefijo /32 para cada sesión VPN de acceso remoto. Para optimizar esto, puede utilizar la función BGP Aggregate Address .

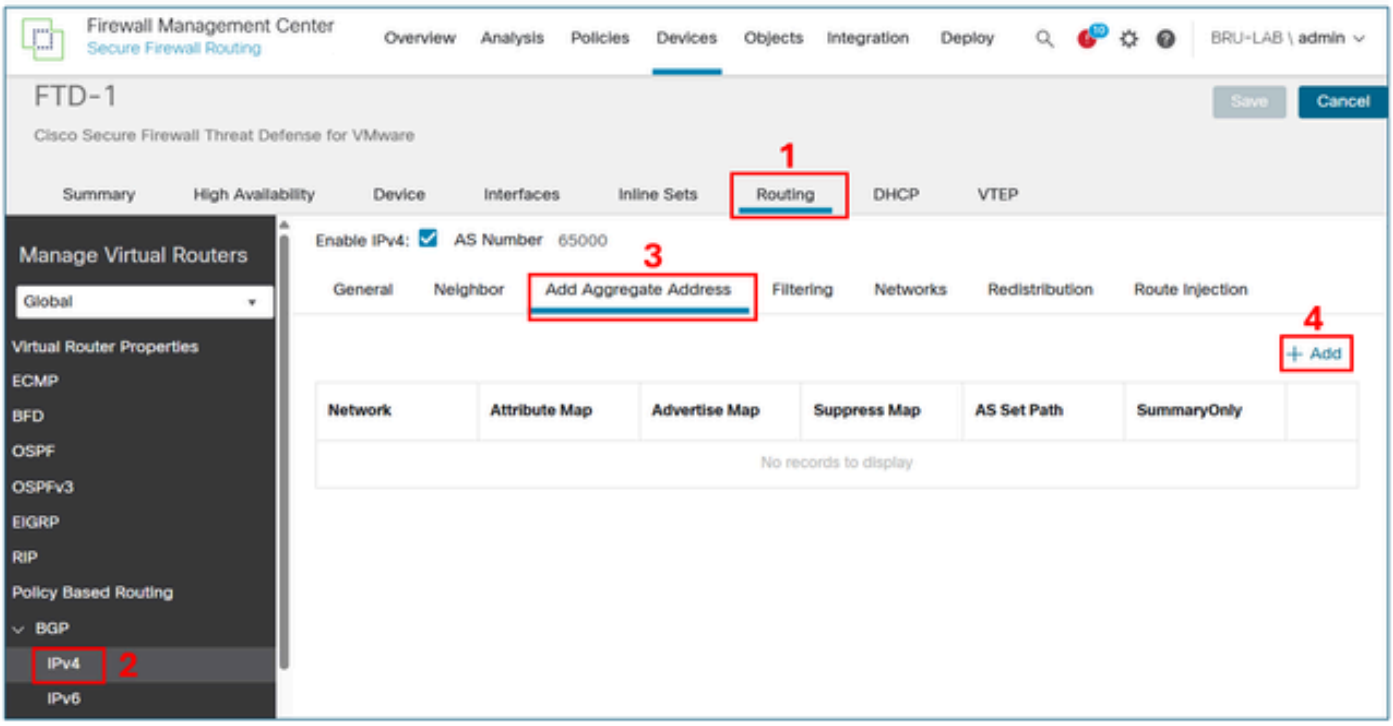
Configuración de Dirección Agregada BGP

Configurar

Si aún no se ha creado, cree un objeto de red para las subredes VPN.



En la IU de administración de dispositivos FMC, navegue hasta Routing > BGP > IPv4 > Add Aggregate Address y, a continuación, seleccione el botón Add.



En el campo de red, agregue el objeto para la subred VPN y, a continuación, active la casilla de verificación Filtrar todas las rutas de las actualizaciones.

Add Aggregate Address

Network*

VPN-SUBNET

Attribute Map

Advertise Map

Suppress Map

Generate AS set path information

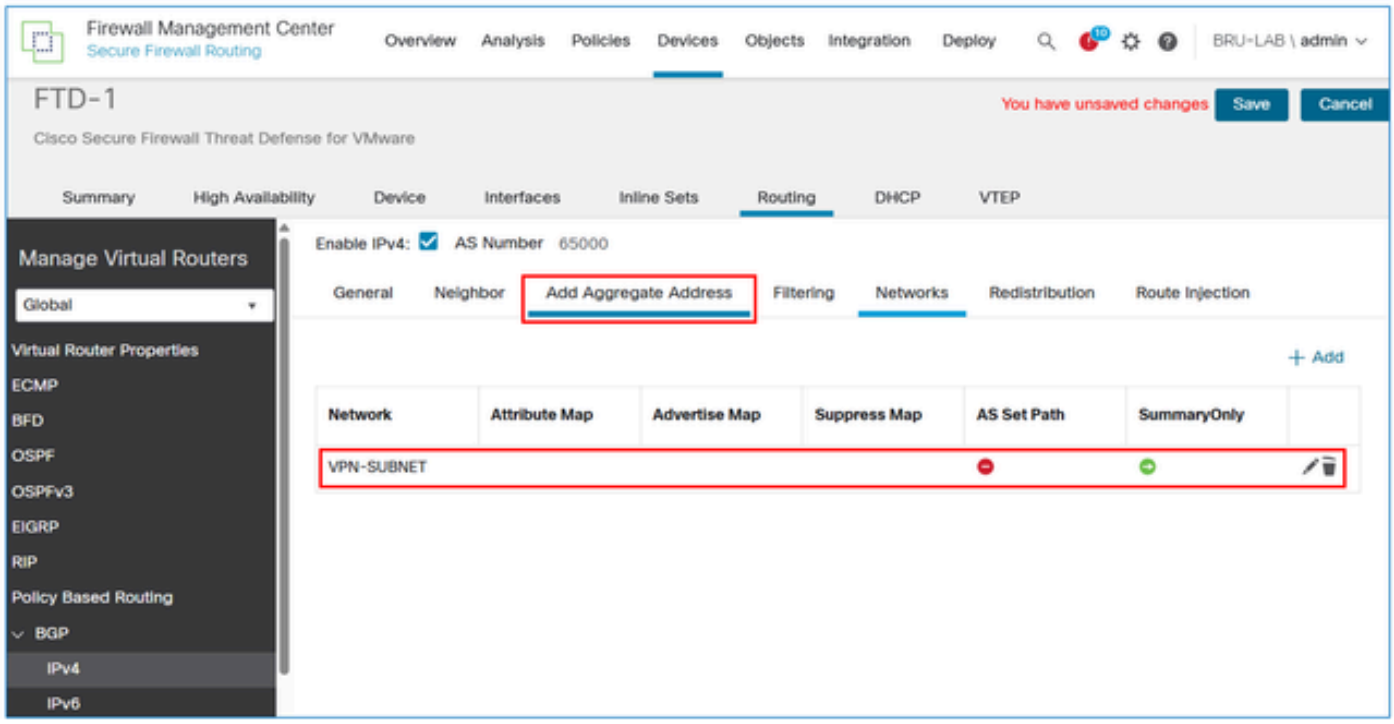
Filter all routes from updates

Cancel

OK

Nota: Si la casilla de verificación Filter all routes from updates no está marcada, el FTD anuncia la dirección de resumen y las rutas VPN /32 específicas sobre BGP. Cuando la casilla de verificación está habilitada, el FMC envía el comando aggregate-address summary-only a la configuración LINA del FTD, asegurándose de que solo se anuncia la dirección de resumen.

El resultado:



Guardar e implementar la configuración en el FTD.

Verificación

Configuración BGP de FTD:

<#root>

FTD-1#

sh run router

```
router bgp 65000
 bgp log-neighbor-changes
 bgp router-id vrf auto-assign
 address-family ipv4 unicast
  neighbor 192.168.100.1 remote-as 65001
  neighbor 192.168.100.1 transport path-mtu-discovery disable
  neighbor 192.168.100.1 activate
```

redistribute static

aggregate-address 10.100.100.0 255.255.255.0 summary-only

```
  no auto-summary
  no synchronization
 exit-address-family
```

Resultado de la tabla BGP de FTD:

<#root>

FTD-1#

sh bgp

```
BGP table version is 28, local router ID is 192.168.100.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path

*> 10.100.100.0/24  0.0.0.0                          32768  i

s> 10.100.100.10/32 10.100.100.10        0         32768  ?

r> 192.168.100.0/30 192.168.100.1       1             0  65001 ?
```

Resultado de la tabla R1 BGP:

<#root>

R1#

show ip bgp

```
BGP table version is 261, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path

*>   10.100.100.0/24  192.168.100.2          0             0 65000 i

 *>   192.168.100.0/30  0.0.0.0                  1         32768 ?
```

Resultado de la tabla de ruteo R1:

<#root>

R1#

show ip 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
      10.0.0.0/24 is subnetted, 1 subnets
```

B   10.100.100.0 [20/0] via 192.168.100.2, 00:02:04

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).