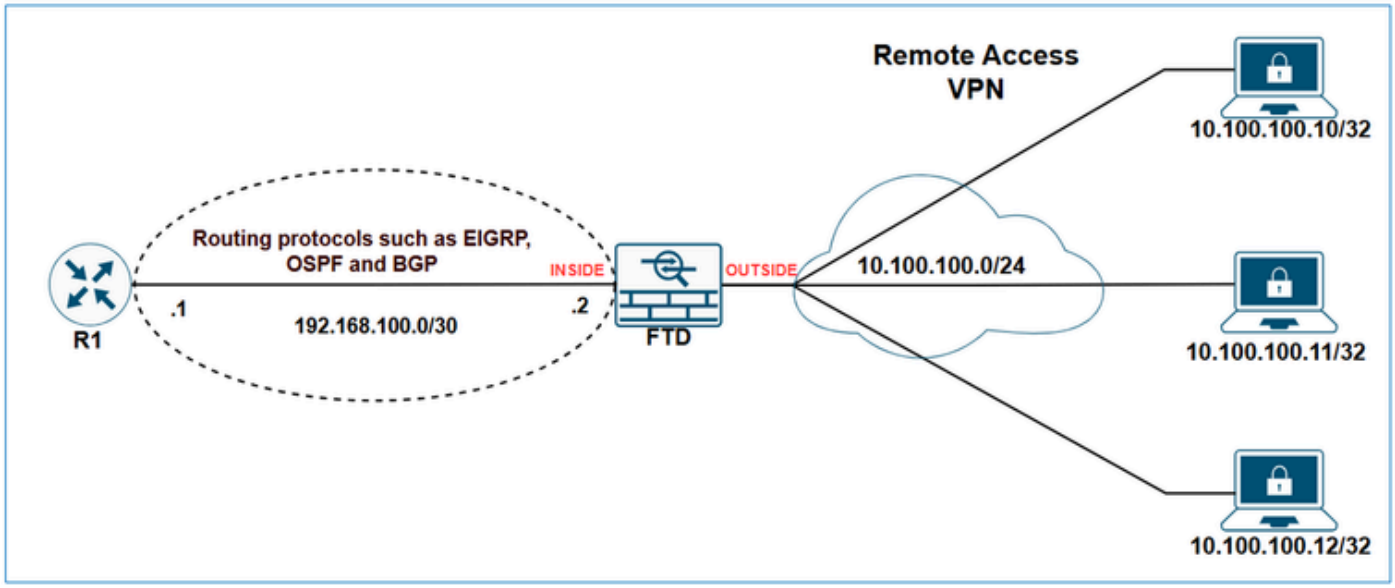
Pubblicizzare le subnet VPN ad accesso remoto tramite i protocolli di routing in FTD

Sommario

Introduzione

In questo documento vengono descritte le opzioni disponibili per la pubblicità delle subnet relative alla VPN con i protocolli di routing EIGRP, OSPF e BGP.



Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Nota: Questo documento descrive la configurazione per la ridistribuzione delle subnet VPN ad accesso remoto tramite EIGRP, OSPF e BGP tramite FMC. Per ulteriori informazioni sulla ridistribuzione dei percorsi con FDM, fare riferimento alla guida alla configurazione di FDM.

Premesse

La prima cosa da capire è come l'FTD classifica le subnet VPN nella sua tabella di routing. Sebbene queste subnet appaiano come connesse da VPN, non sono considerate subnet connesse direttamente; vengono invece trattati come route statiche.

Lo dimostrano i risultati dello show.

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
```

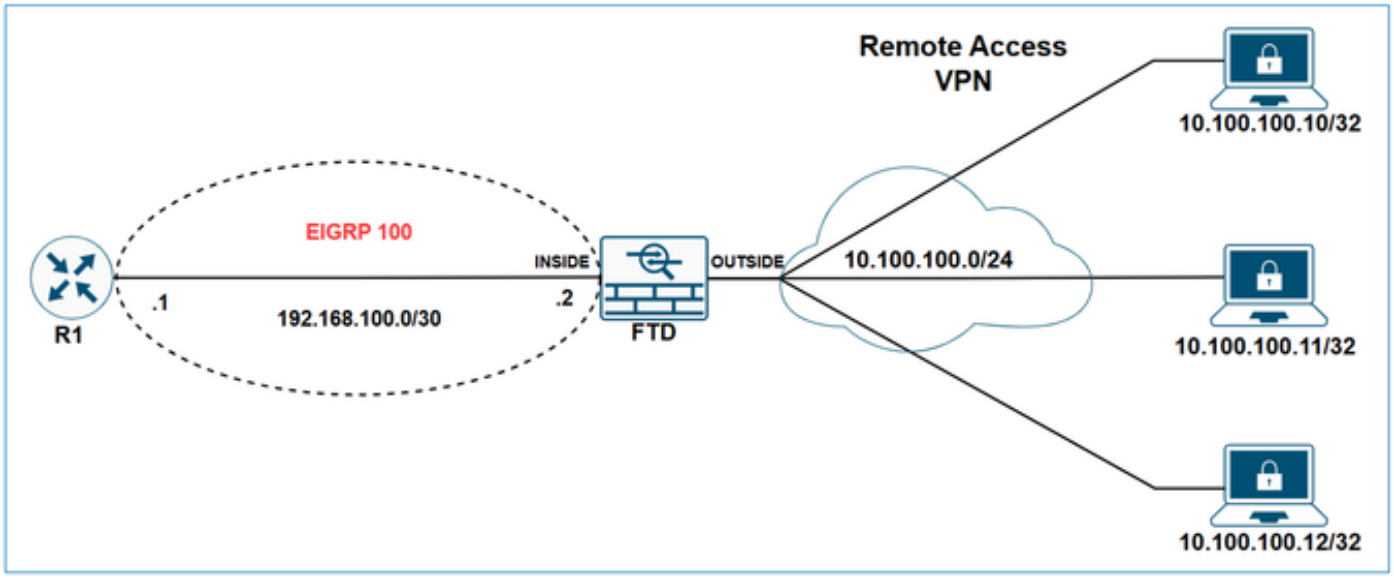
Output statico route FTD show:

```
<#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
```

Ora che è chiaro come vengono trattate le subnet VPN nella tabella di routing del firewall, il passaggio successivo è quello di esplorare come pubblicizzarle utilizzando vari protocolli di routing.

Ridistribuisci subnet VPN ad accesso remoto tramite EIGRP su FTD

Esempio di rete



Le rotte statiche che rientrano nell'ambito di applicazione di un prospetto informativo della rete

sono ridistribuite automaticamente all'EIGRP; non è necessario definire una regola di ridistribuzione per tali elementi. Tuttavia, quando si ridistribuiscono route statiche che puntano a interfacce VTI in EIGRP, è necessario specificare la metrica. Per le route statiche che puntano ad altri tipi di interfacce, non è necessario specificare la metrica.

A causa del comportamento dell'EIGRP di ridistribuire automaticamente le route statiche che rientrano nell'ambito dei rendiconti di rete, ci sono due opzioni per pubblicizzare le subnet VPN tramite EIGRP su FTD:

1. Utilizzo di un'istruzione di rete.
2. Utilizzando l'approccio statico di ridistribuzione.

In questo esempio l'obiettivo è quello di far sì che R1 apprenda la subnet VPN 10.100.100.0/24 tramite EIGRP.

Configurazione iniziale 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
```

Tabella di routing iniziale FTD:

<#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
```

Tabella topologia EIGRP iniziale 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
```

Tabella di routing iniziale R1:

<#root>

```
R1#

show ip route
```

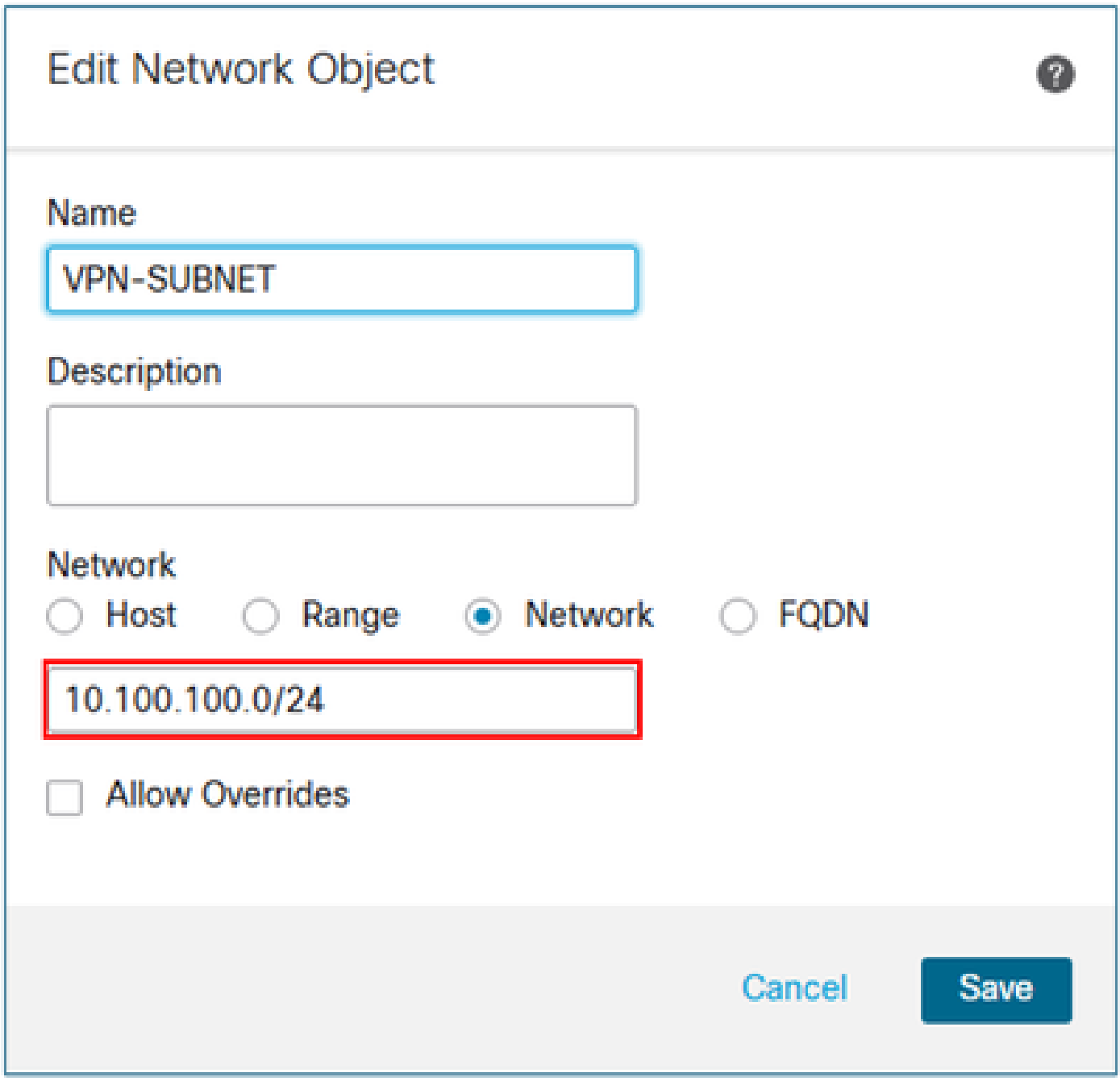
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, 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
```

Ridistribuisci subnet VPN ad accesso remoto tramite EIGRP su FTD tramite istruzione di rete

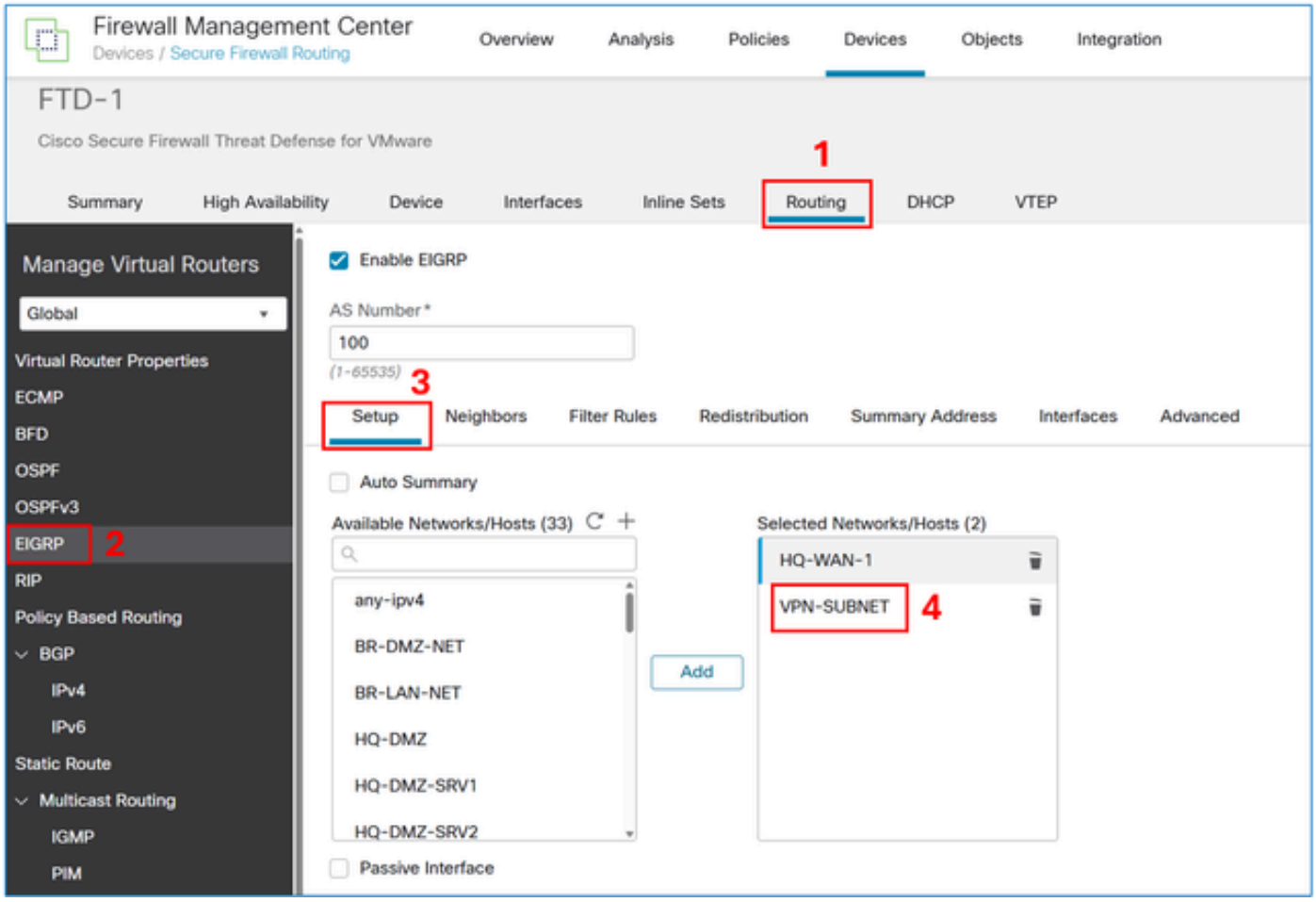
Configurazione

Passaggio 1. Creare un oggetto di rete per la subnet VPN.



Passaggio 2. Includere l'oggetto subnet VPN nel rendiconto della rete.

Nell'interfaccia utente di gestione dei dispositivi di FMC, selezionare Routing > EIGRP > Setup e includere la subnet VPN nelle reti/host selezionati.



Salvare e distribuire la configurazione sull'FTD.

Verifica

Configurazione EIGRP FTD:

<#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
```

Tabella topologia EIGRP 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 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
```

Tabella di routing 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

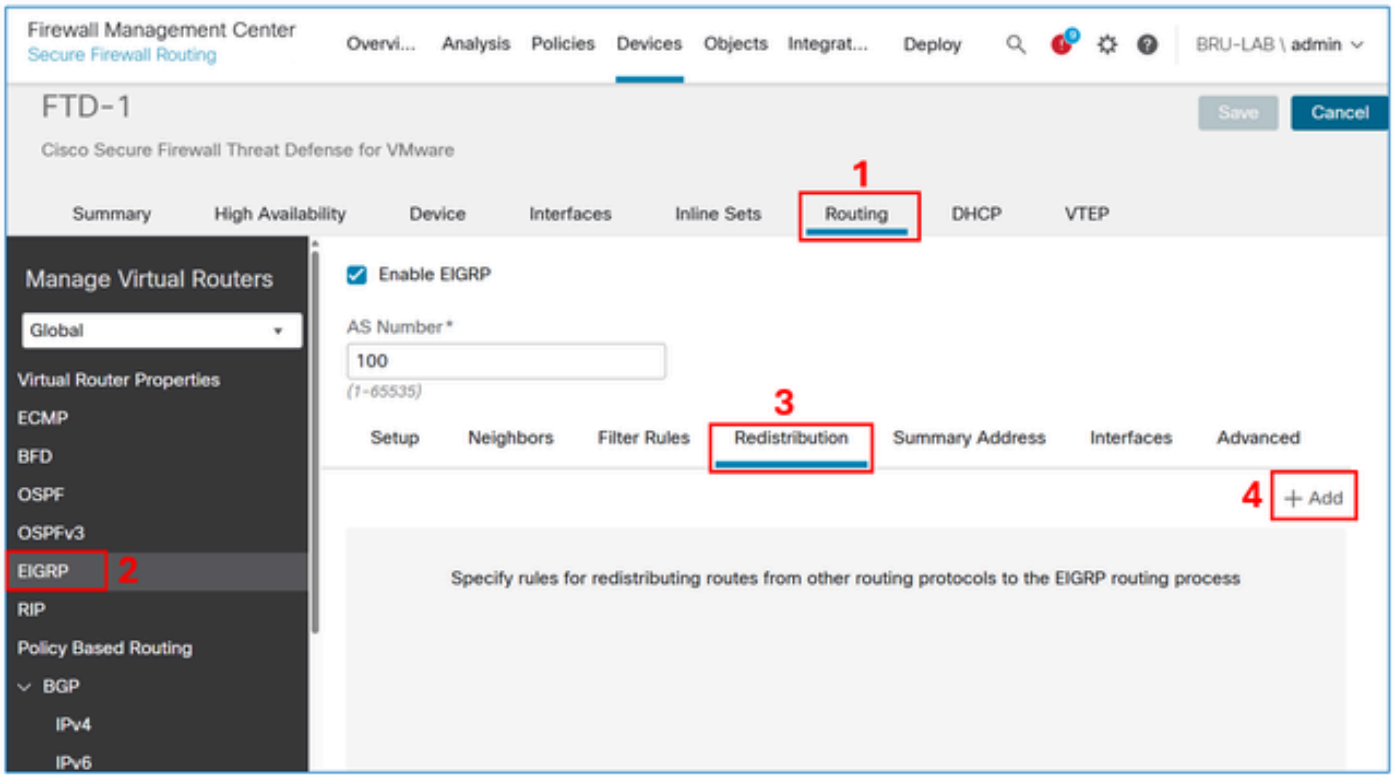
```
      [90/3072] via 192.168.100.2, 00:02:17, GigabitEthernet1
```

Nota: Sebbene l'istruzione network fosse 10.100.100.0/24, l'FTD ridistribuisce una subnet /32 su EIGRP. Questo si verifica perché l'FTD crea una route statica con un prefisso /32 per ogni sessione VPN di accesso remoto. Per ottimizzare questa operazione, è possibile utilizzare la funzione Indirizzo di riepilogo EIGRP.

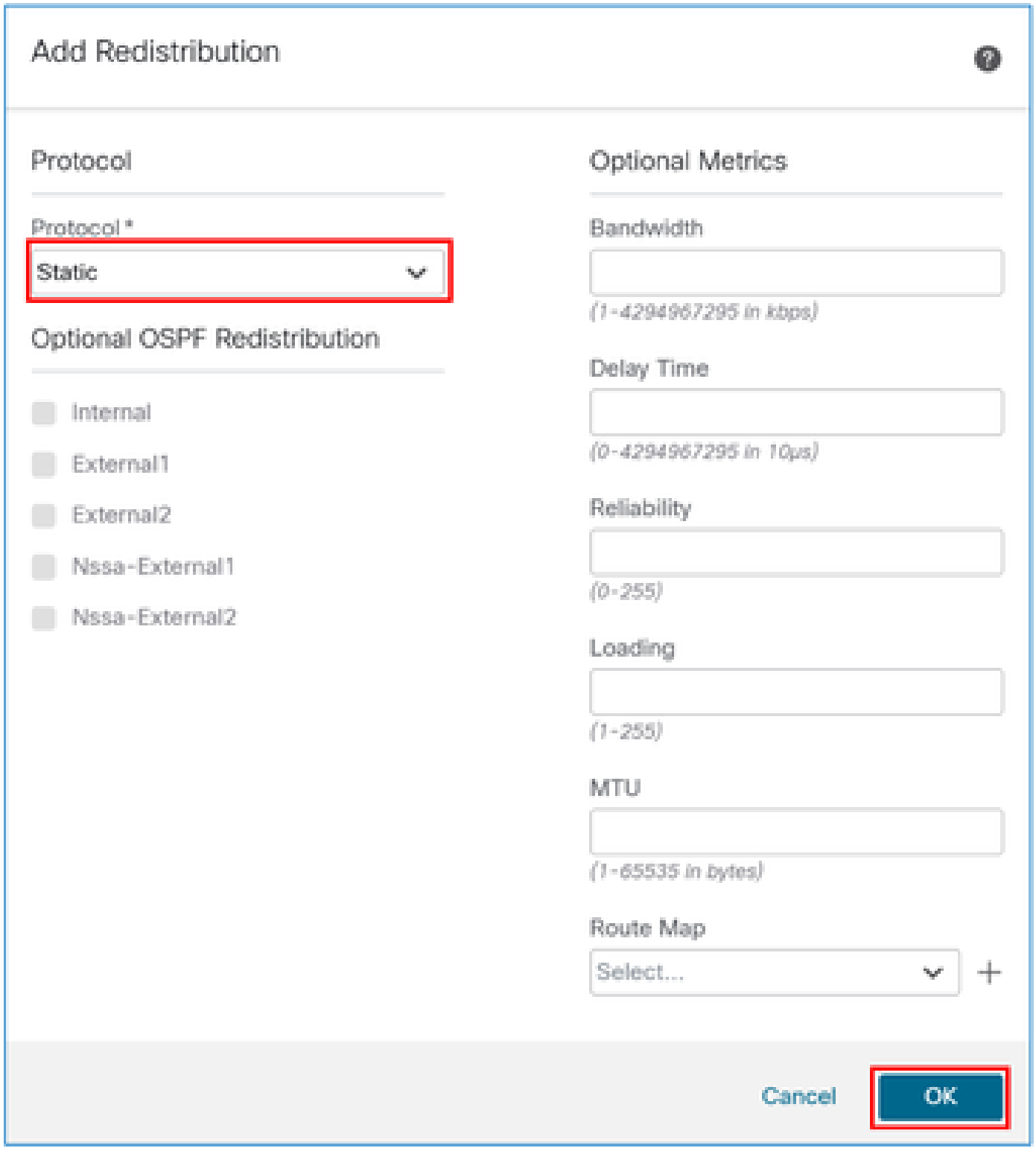
Ridistribuire le subnet VPN ad accesso remoto tramite EIGRP su FTD utilizzando l'approccio ridistribuisci statico

Configurazione

Nell'interfaccia utente di gestione dei dispositivi di FMC, selezionare Routing > EIGRP > Redistribution, quindi selezionare il pulsante Add.

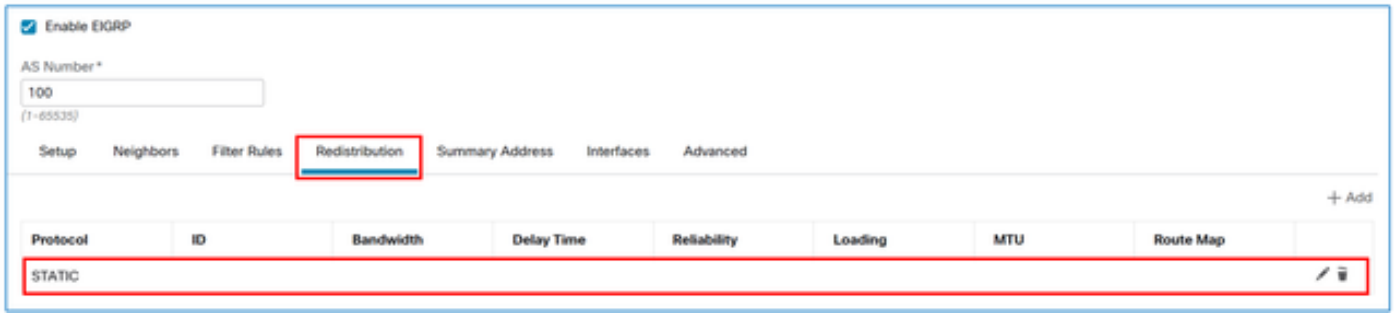


Nel campo del protocollo, selezionare Static, quindi selezionare il pulsante OK.



⚠ Attenzione: tutte le route statiche vengono ridistribuite in EIGRP. Se è necessario annunciare solo le subnet VPN, è possibile utilizzare l'istruzione network o applicare una mappa dei percorsi per filtrarle.

Il risultato:



Salvare e distribuire la configurazione sull'FTD.

Verifica

Configurazione EIGRP FTD:

```
<#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
```

Tabella topologia EIGRP 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 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
```

Tabella di routing R1:

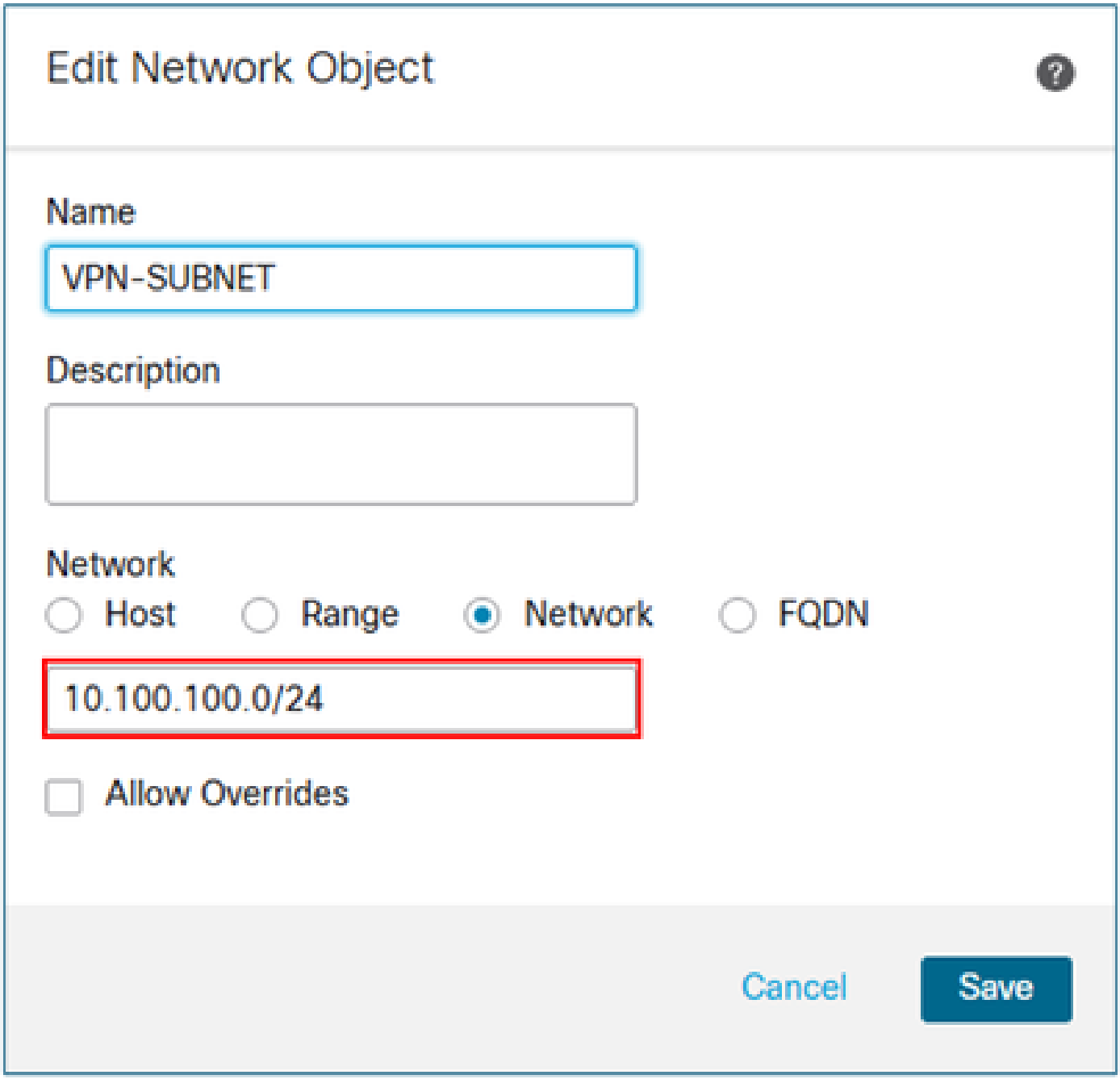
```
<#root>

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
```

Suggerimento: Facoltativamente, è possibile utilizzare la funzione di indirizzo di riepilogo EIGRP su FTD per ottimizzare le dimensioni della tabella di routing.

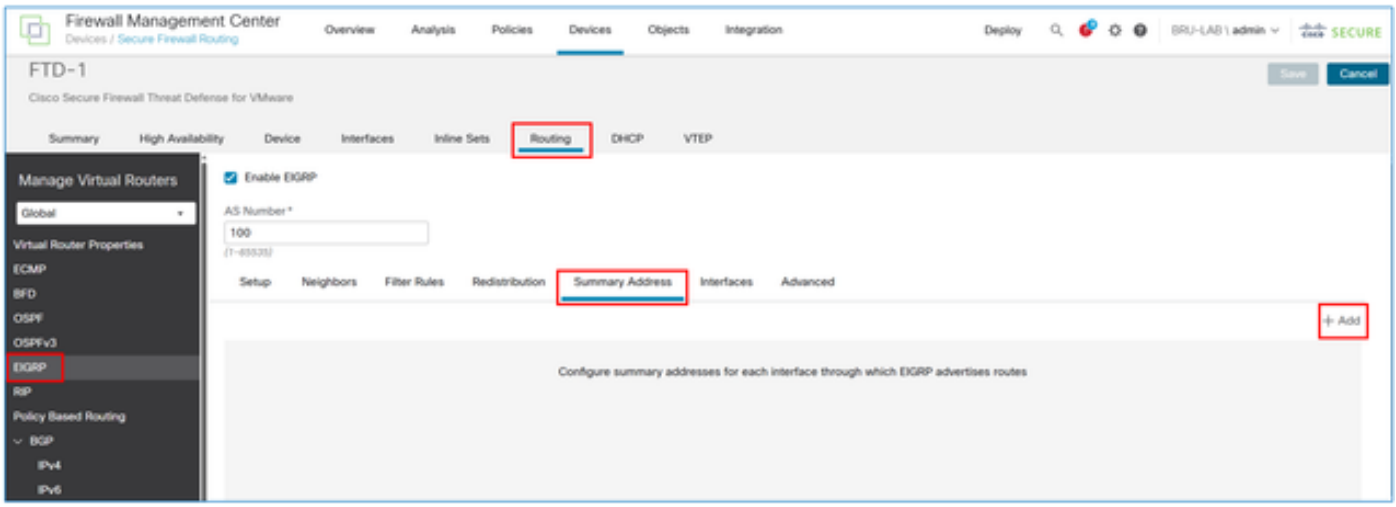
Configurazione indirizzo di riepilogo EIGRP

Configurazione

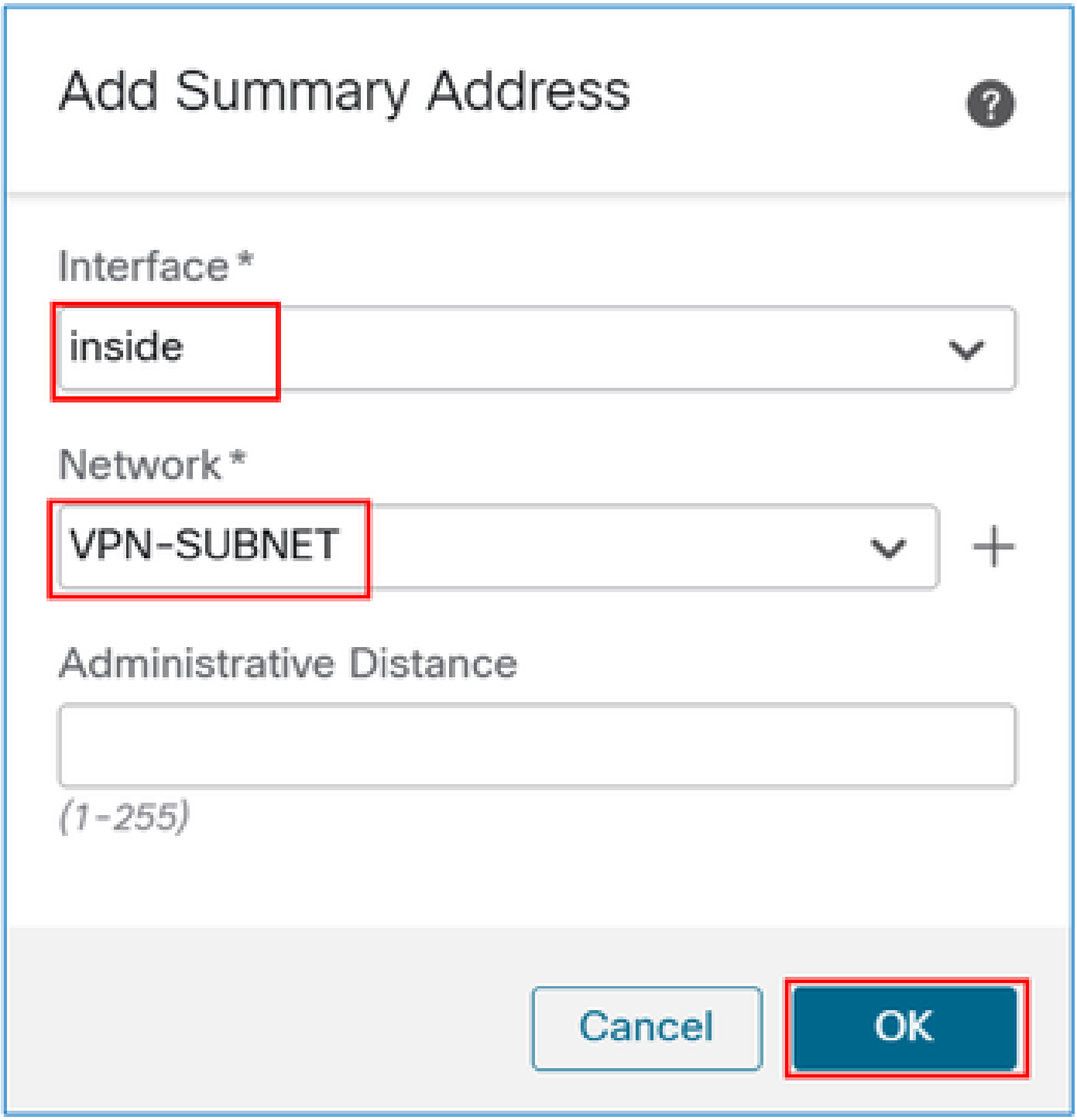
Se non è ancora stato creato, creare un oggetto di rete per le subnet VPN.



Nell'interfaccia utente di gestione dei dispositivi di FMC, selezionare Routing > EIGRP > Summary Address, quindi selezionare il pulsante Add.



Nel campo interface (interfaccia), immettere quello rivolto al router adiacente EIGRP, quindi nel campo network (rete), immettere l'oggetto creato per la subnet VPN.



Il risultato:

Verifica

Configurazione indirizzo di riepilogo EIGRP 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

Tabella topologia EIGRP 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 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
```

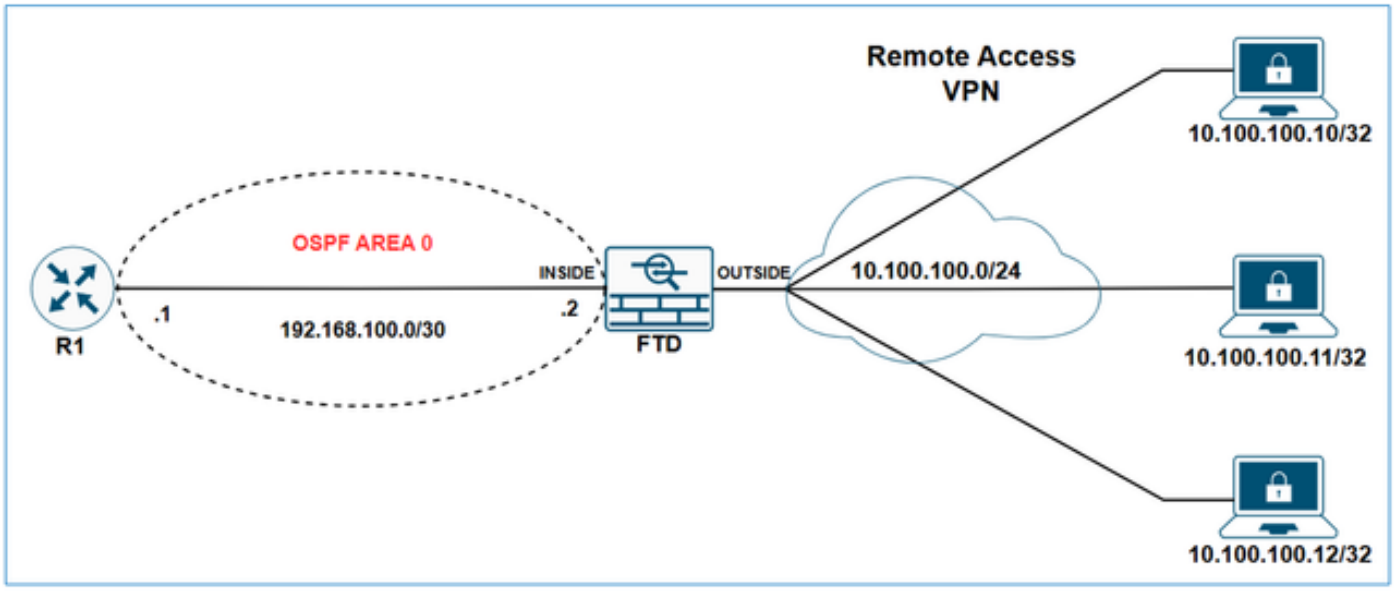
Tabella di routing R1:

<#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
```

Ridistribuisci subnet VPN di accesso remoto tramite OSPF su FTD

Esempio di rete



Configurazioni iniziali

<#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
```

Output FTD show ospf neighbors:

<#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 output router adiacente:

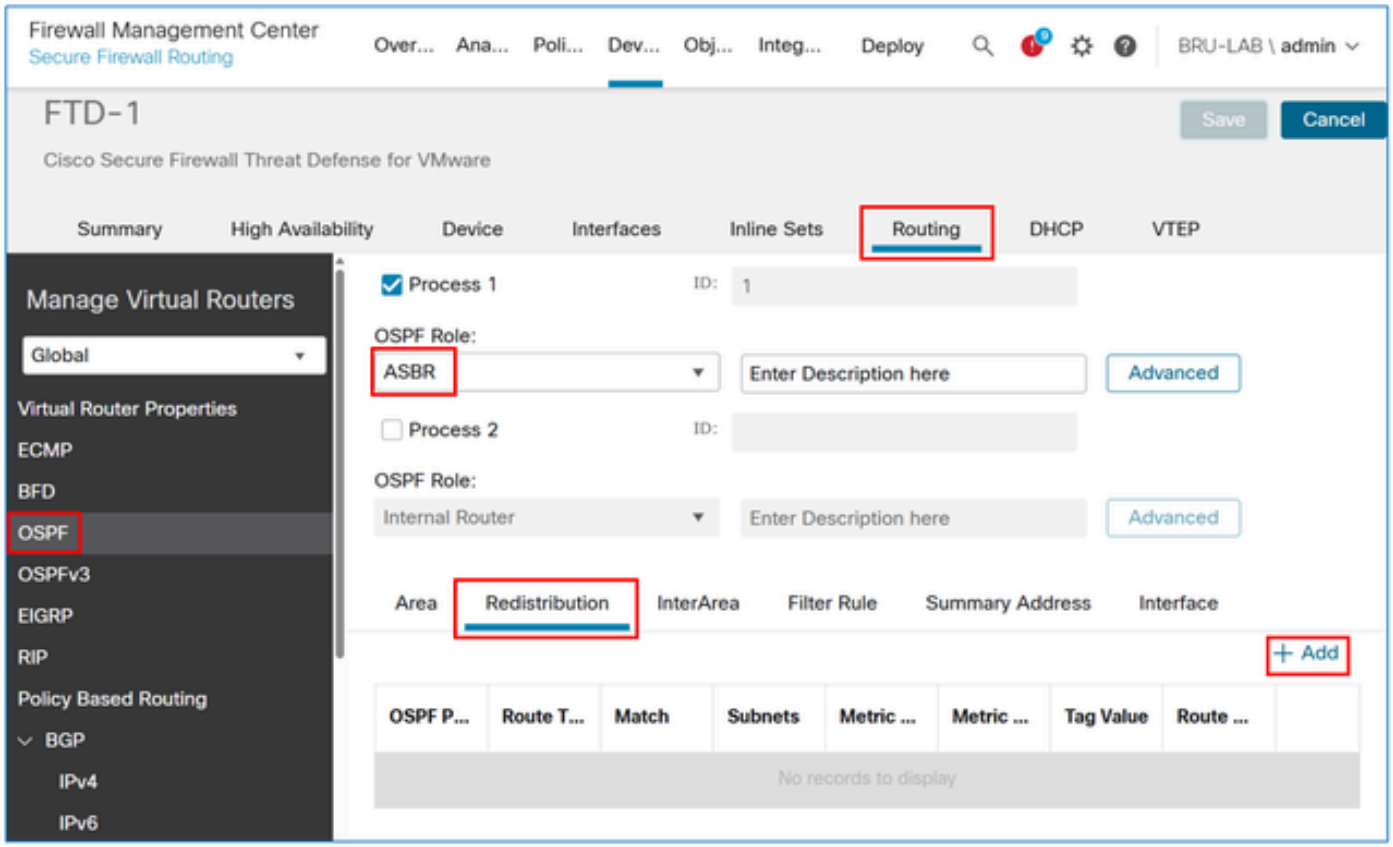
```
<#root>

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
```

Tabella di routing 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
```

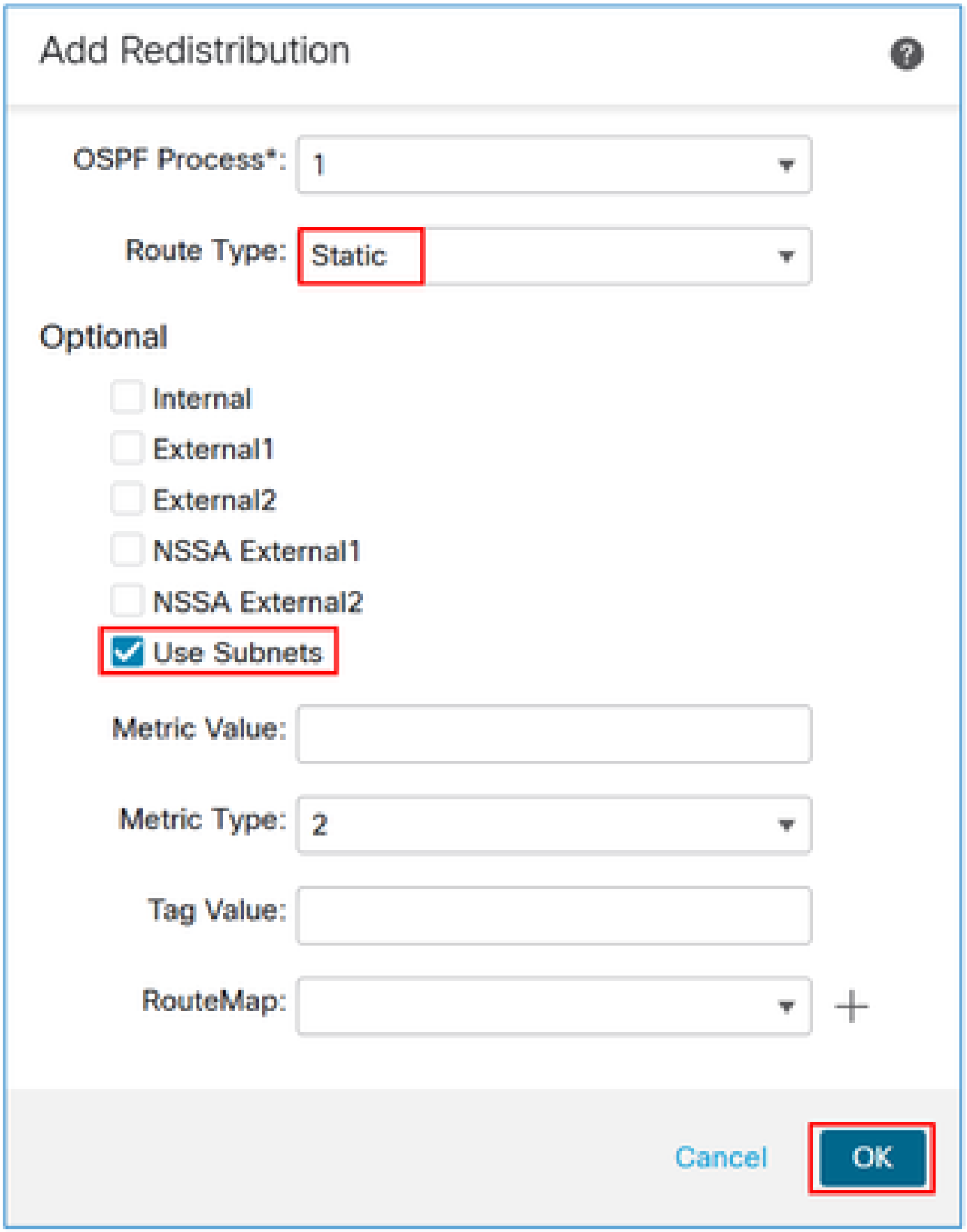
Configurazione

Nell'interfaccia utente di gestione dei dispositivi di FMC passare a Routing > OSPF > Redistribution, quindi selezionare il pulsante Add.



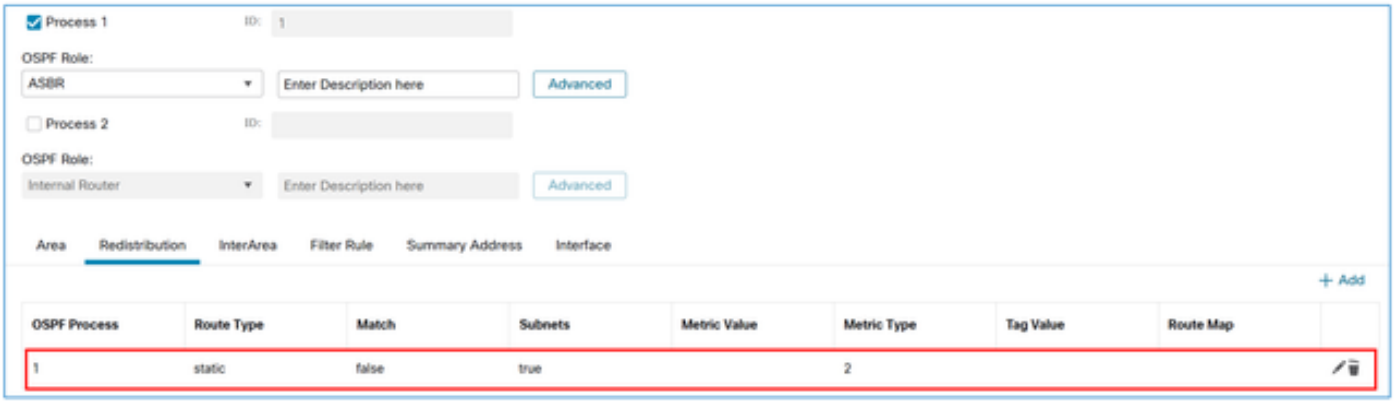
Nota: Per abilitare la ridistribuzione, il ruolo OSPF deve essere impostato come ASBR o ABR & ASBR.

Nel campo Tipo di instradamento selezionare Statico, quindi selezionare la casella di controllo Usa subnet.



⚠ Attenzione: tutte le route statiche vengono ridistribuite in OSPF. Se è necessario annunciare solo le subnet VPN, è possibile applicare una mappa dei percorsi per filtrarle.

Il risultato:



Verifica

Configurazione ridistribuzione 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
```

Tabella di routing 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
```

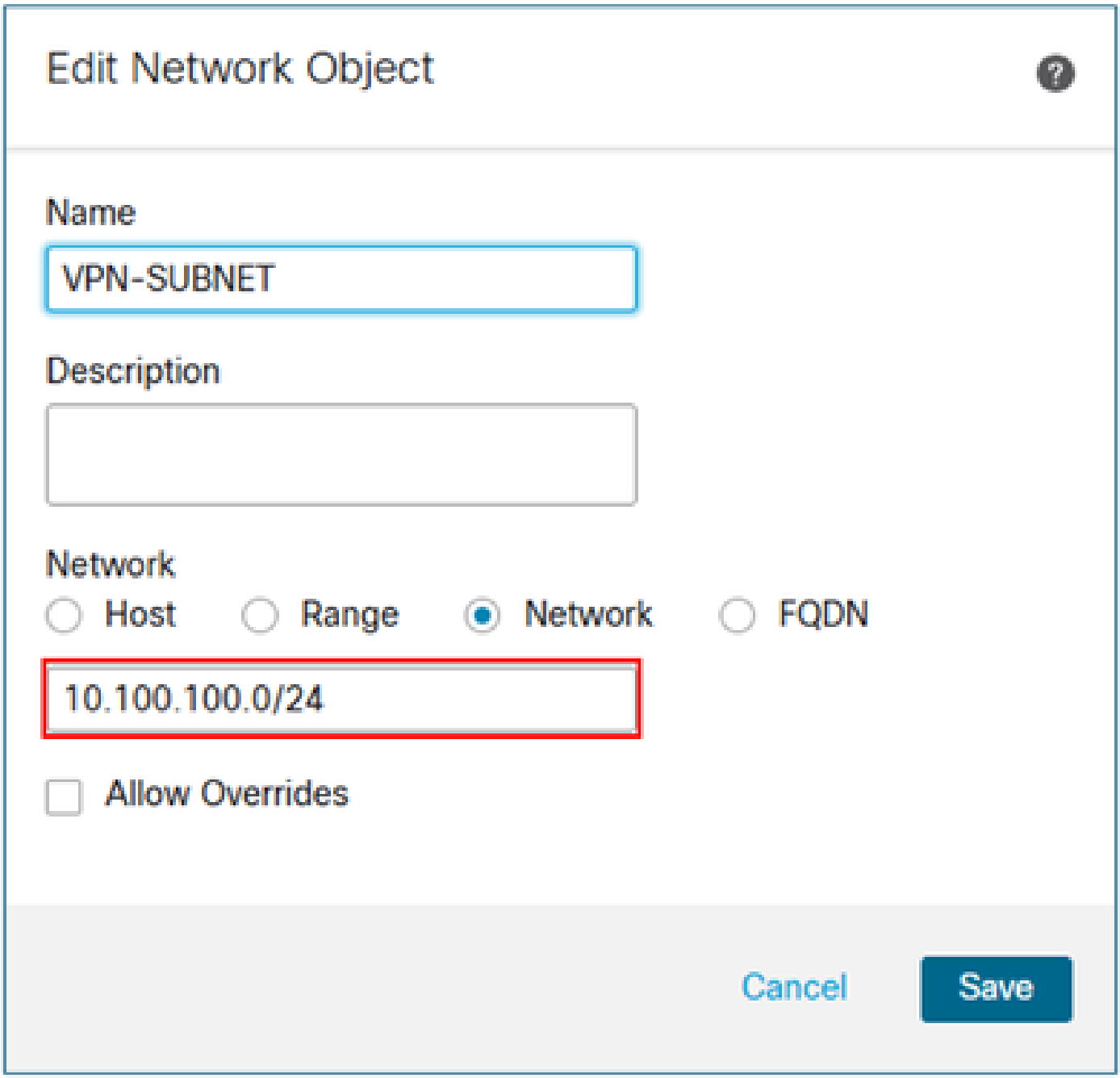
`O E2     10.100.100.10 [110/20] via 192.168.100.2, 00:08:01, GigabitEthernet1`

Suggerimento: Sebbene il pool VPN sia 10.100.100.0/24, l'FTD ridistribuisce una subnet /32 su OSPF. Questo si verifica perché l'FTD crea una route statica con un prefisso /32 per ogni sessione VPN di accesso remoto. Per ottimizzare questa operazione, è possibile utilizzare la funzionalità Indirizzo di riepilogo OSPF.

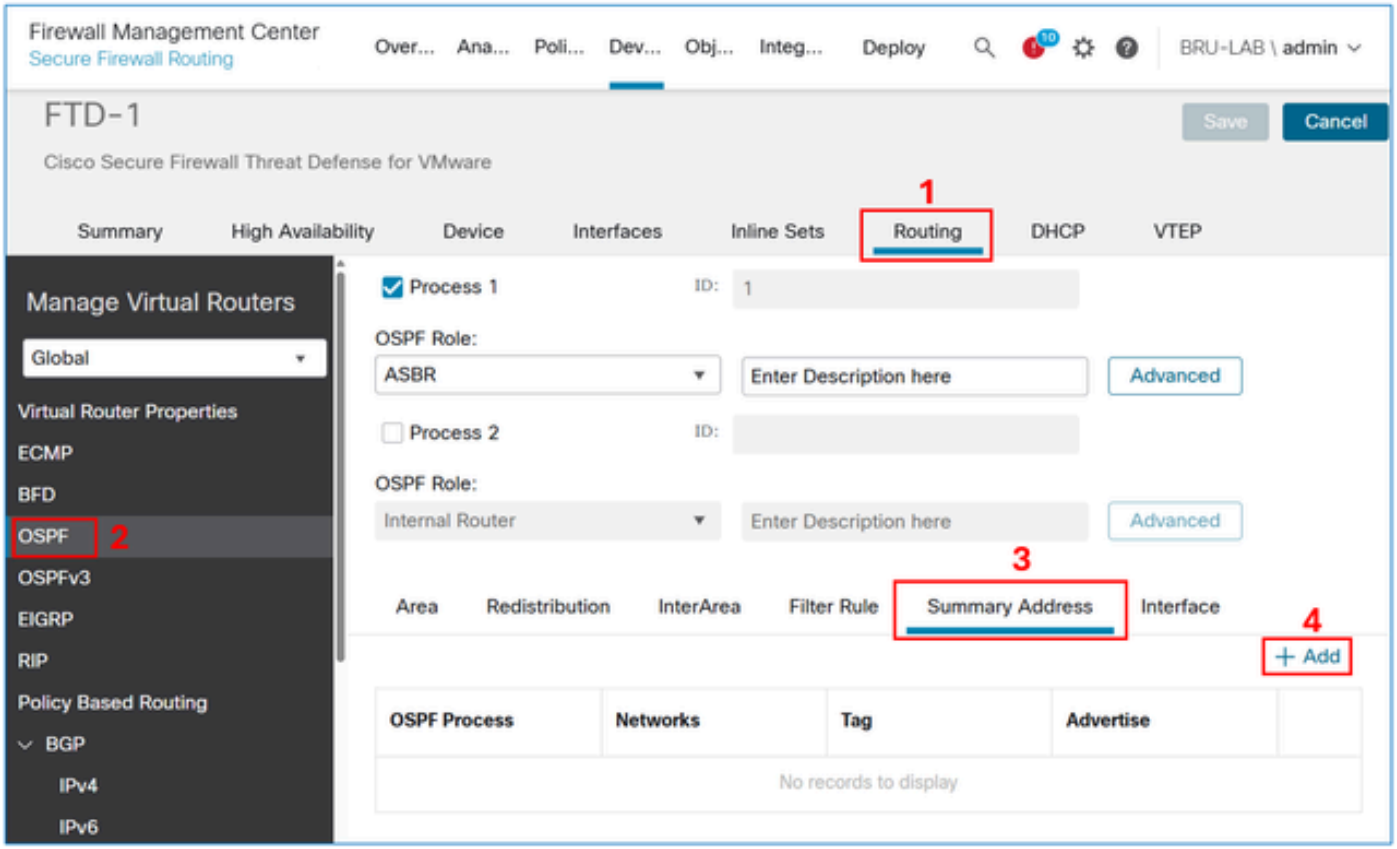
Configurazione indirizzo di riepilogo OSPF

Configurazione

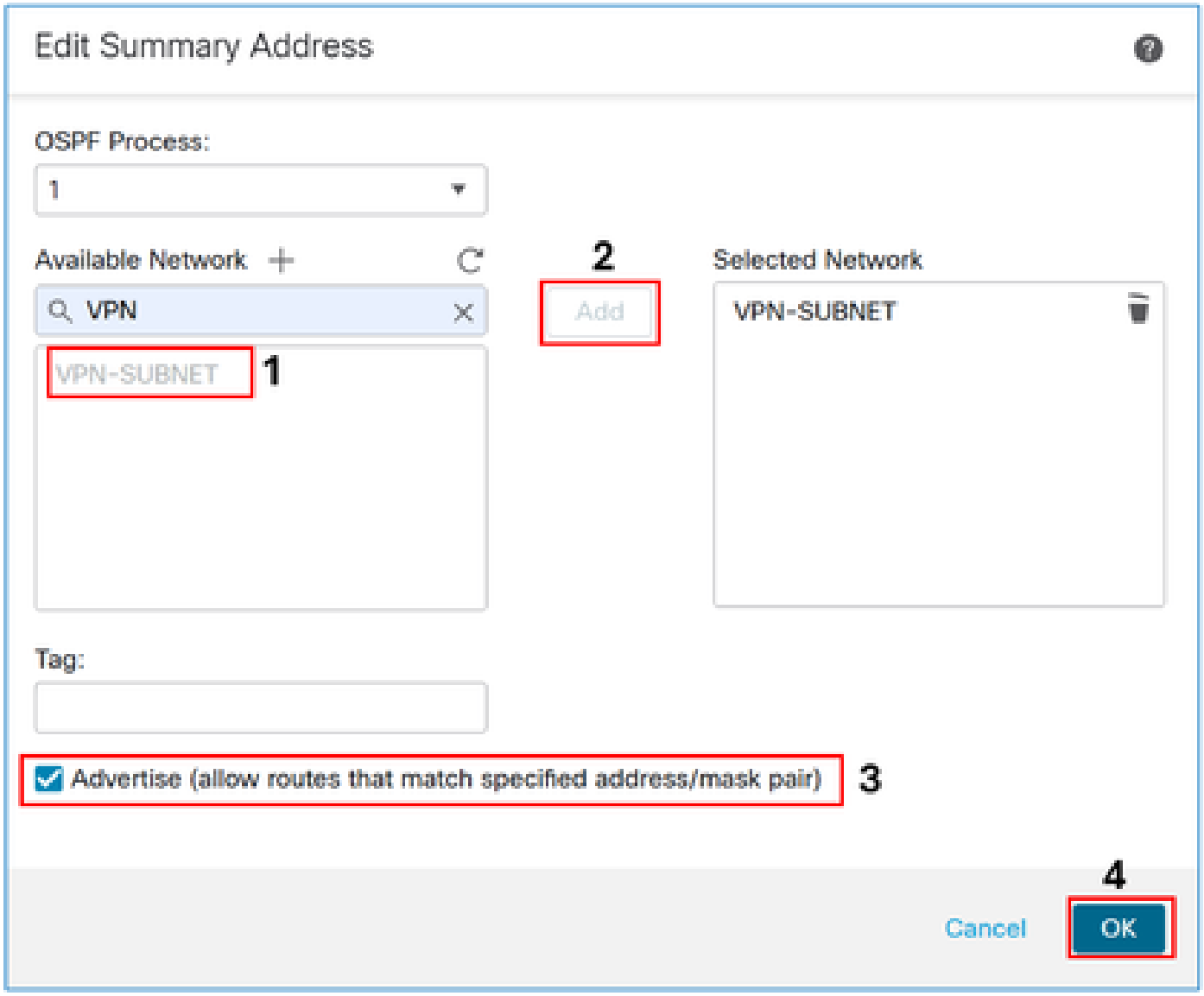
Se non è ancora stato creato, creare un oggetto di rete per le subnet VPN.



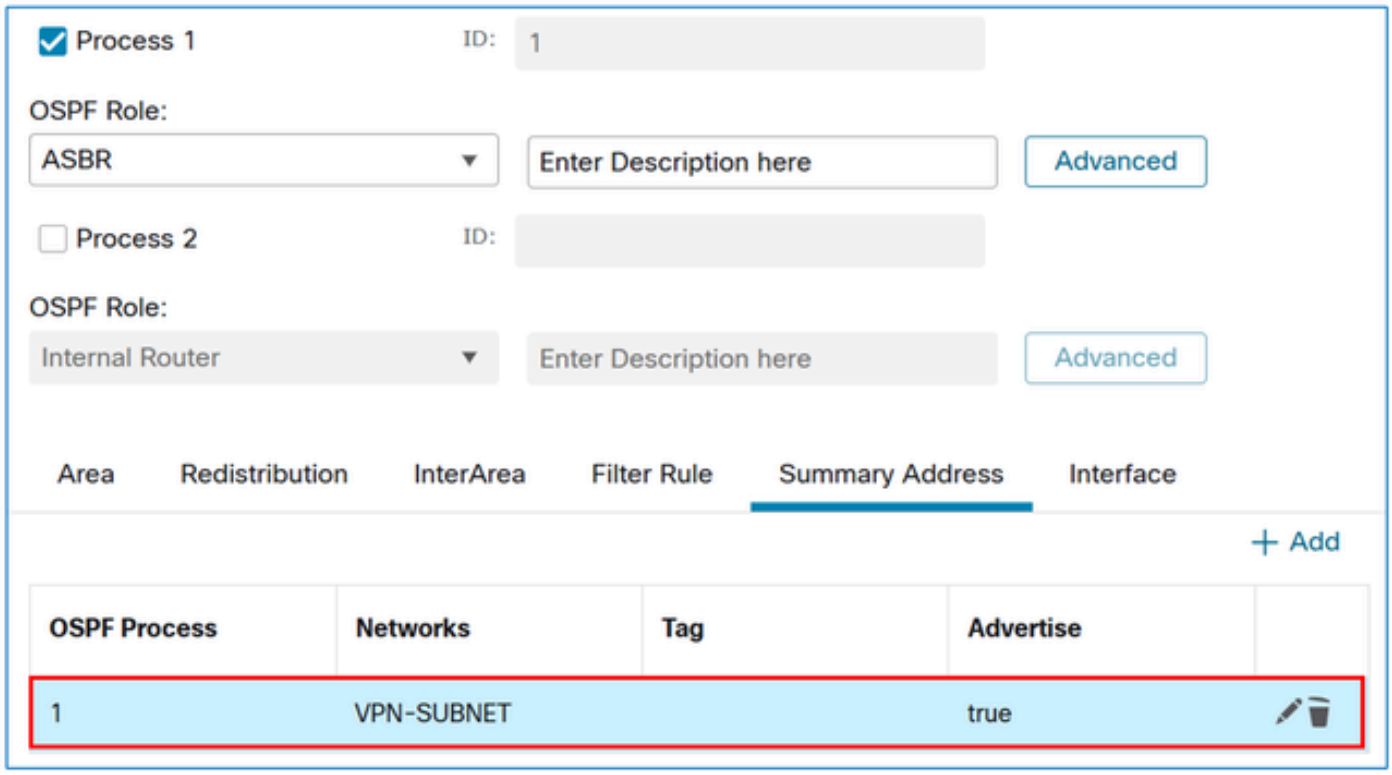
Nell'interfaccia utente di gestione dei dispositivi di FMC passare a Routing > OSPF> Summary Address, quindi selezionare il pulsante Add.



Aggiungere l'oggetto subnet VPN e selezionare la casella di controllo Annuncia.



Il risultato:



Verifica

Configurazione 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

summary-address 10.100.100.0 255.255.255.0

Tabella di routing R1:

<#root>

R1#

sh ip route

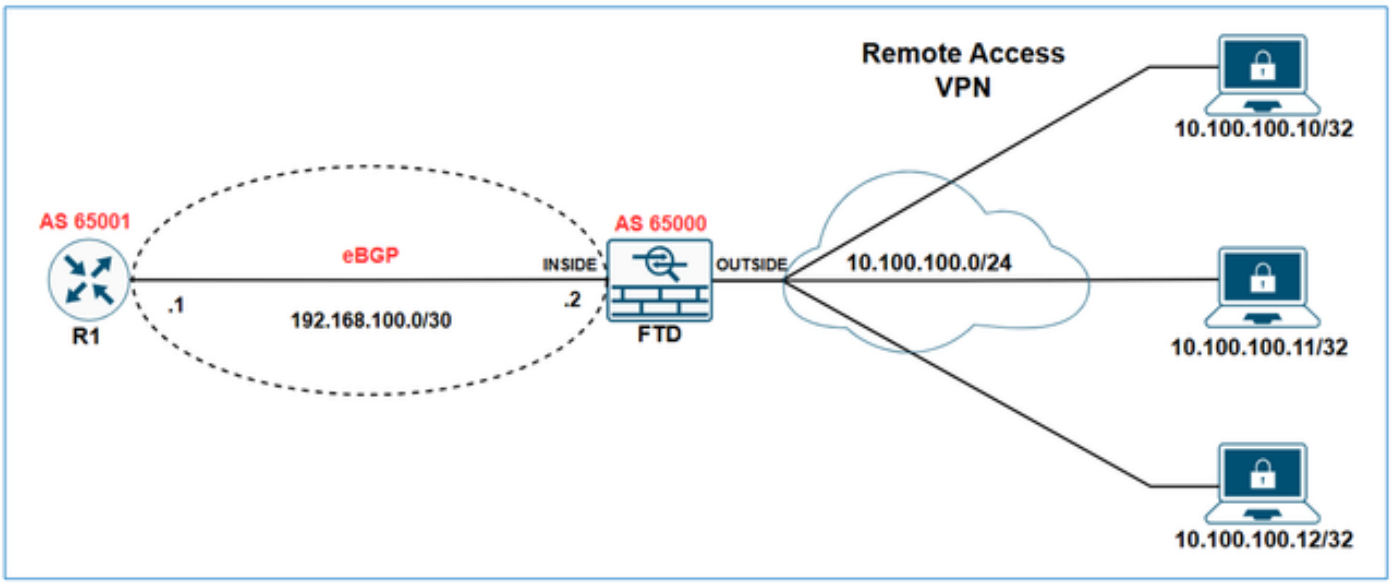
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

```
       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`

Ridistribuzione delle subnet VPN di accesso remoto tramite eBGP su FTD

Esempio di rete



In questo esempio l'obiettivo è quello di far sì che R1 apprenda la subnet VPN 10.100.100.0/24 tramite eBGP.

Configurazioni iniziali

Configurazione iniziale 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 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
```

Output tabella bgp 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 ?

Output di riepilogo 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
```

Output tabella bgp R1:

<#root>

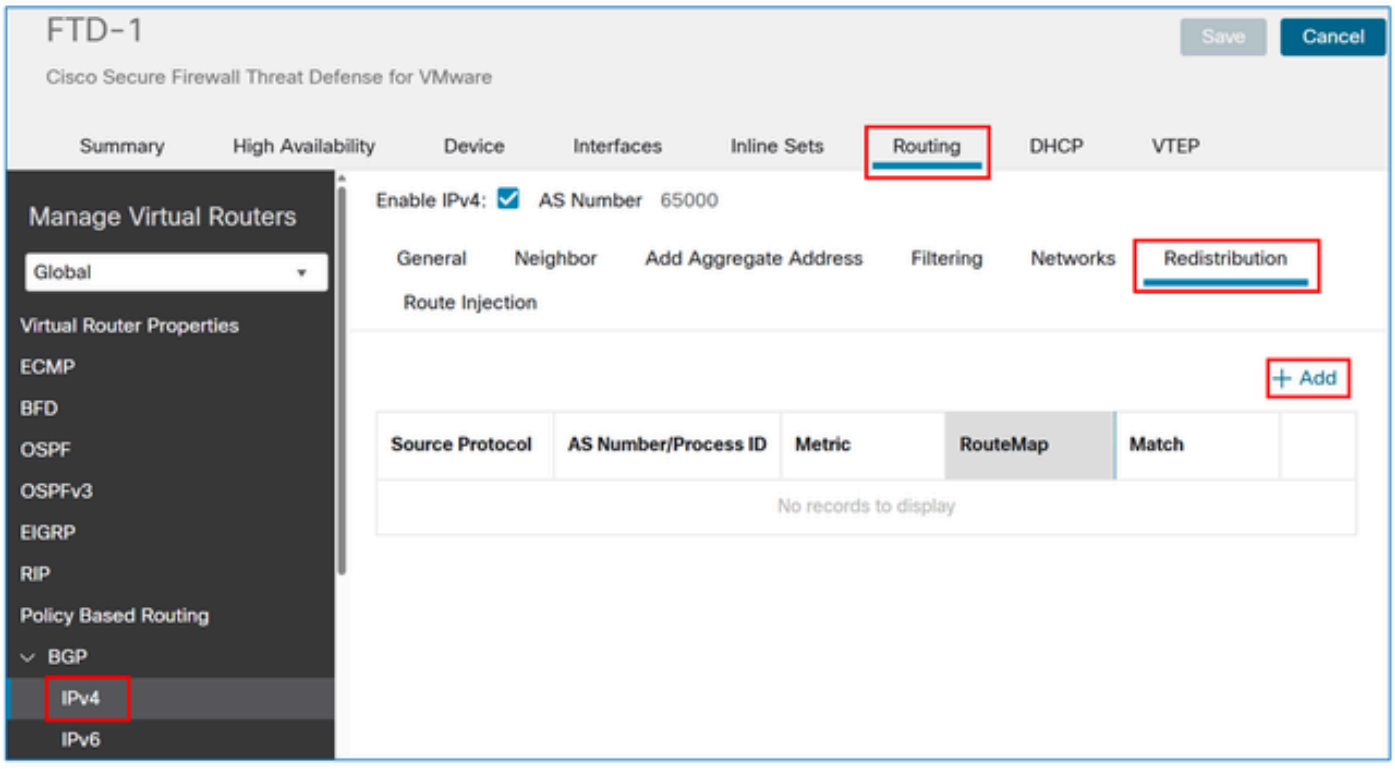
```
R1#

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 ?
```

Tabella di routing 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
```

Configurazione

Nell'interfaccia utente di gestione dei dispositivi di FMC, selezionare Routing > BGP > IPv4 > Redistribution, quindi selezionare il pulsante Add.



Nel campo Source Protocol (Protocollo di origine), scegliere Static, quindi selezionare il pulsante OK.

Add Redistribution

Source Protocol

Static

Process ID*

Metric

(0-4294967295)

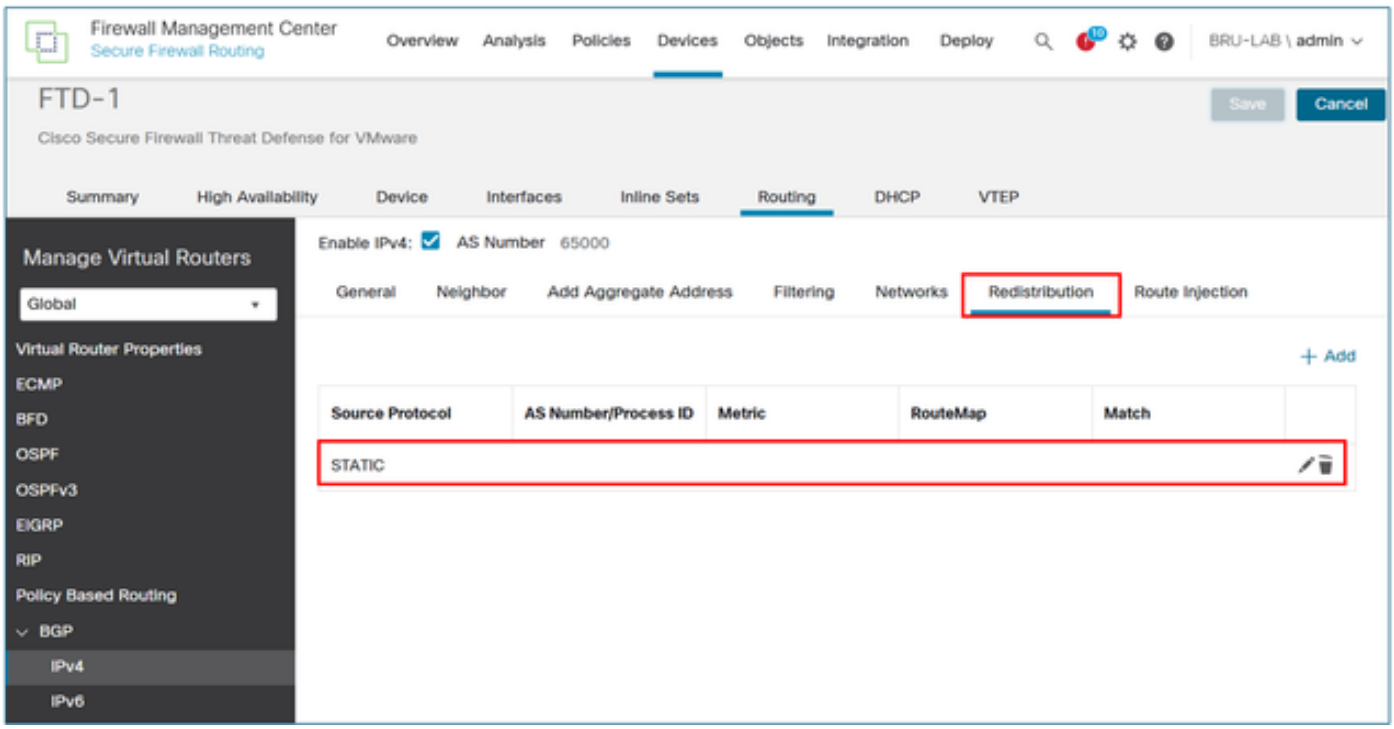
Route Map

Match

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

⚠ : in questo modo vengono ridistribuite tutte le route statiche in BGP. Se è necessario annunciare solo le subnet VPN, è possibile applicare una mappa dei percorsi per filtrarle.

Il risultato:



Salvare e distribuire la configurazione sull'FTD.

Verifica

Configurazione BGP 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
```

Output tabella bgp 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 ?
```

Output tabella 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 ?
```

Output tabella di routing R1:

<#root>

```
R1#
```

show ip route

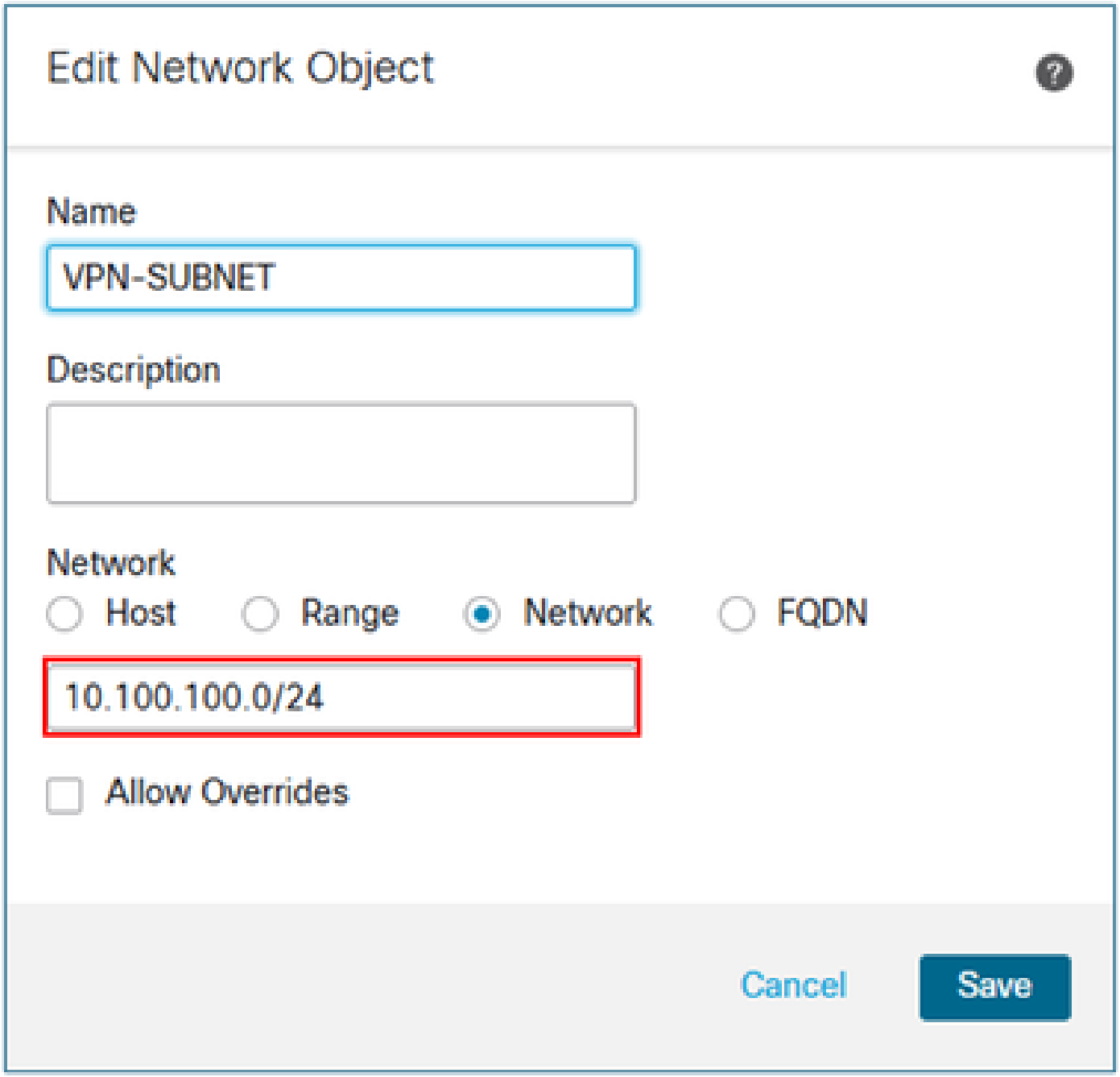
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, 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
```

Suggerimento: Sebbene il pool VPN sia 10.100.100.0/24, l'FTD ridistribuisce una subnet /32 su BGP. Questo si verifica perché l'FTD crea una route statica con un prefisso /32 per ogni sessione VPN di accesso remoto. Per ottimizzare questa operazione, è possibile utilizzare la funzionalità Indirizzo aggregato BGP.

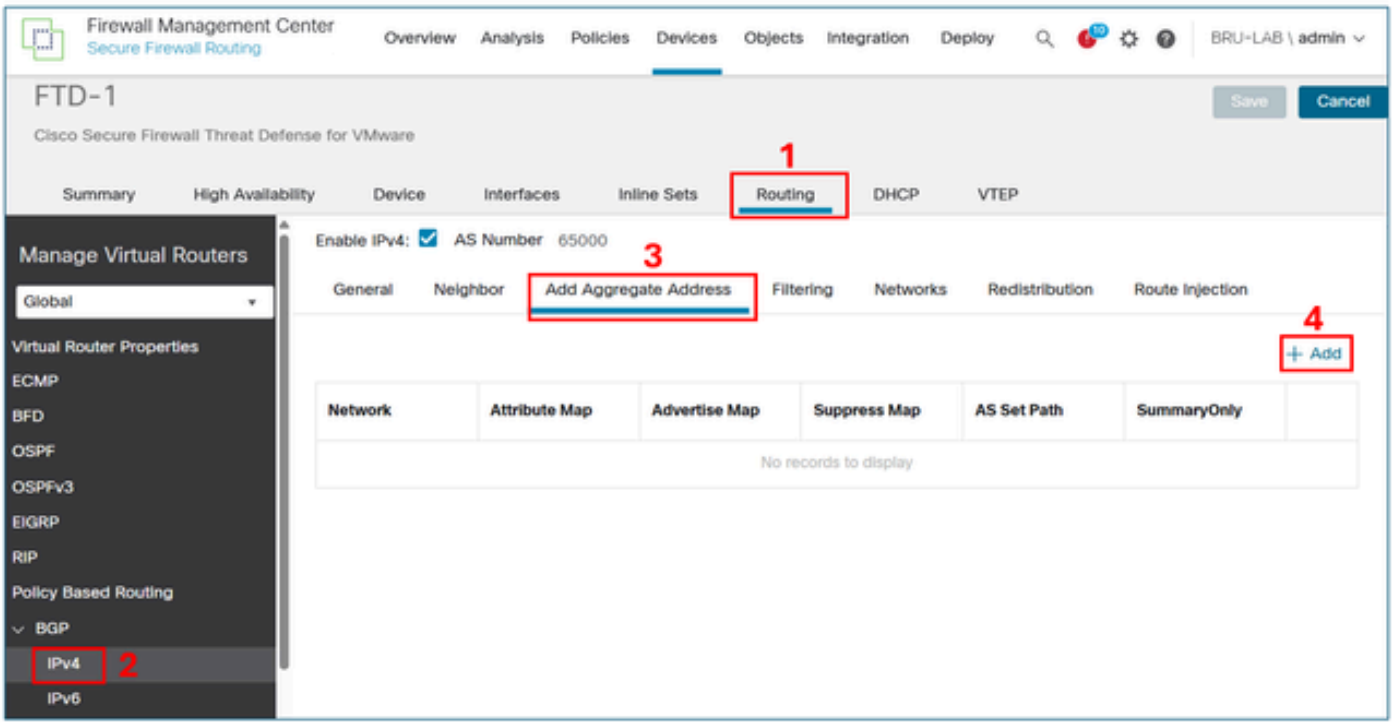
Configurazione indirizzo aggregato BGP

Configurazione

Se non è ancora stato creato, creare un oggetto di rete per le subnet VPN.



Nell'interfaccia utente di gestione dei dispositivi di FMC, selezionare Routing > BGP> IPv4 > Add Aggregate Address, quindi selezionare il pulsante Add.



Nel campo Rete aggiungere l'oggetto per la subnet VPN e quindi selezionare la casella di controllo Filtra tutte le route dagli aggiornamenti.

Add Aggregate Address

Network*

VPN-SUBNET

Attribute Map

Advertise Map

Suppress Map

Generate AS set path information

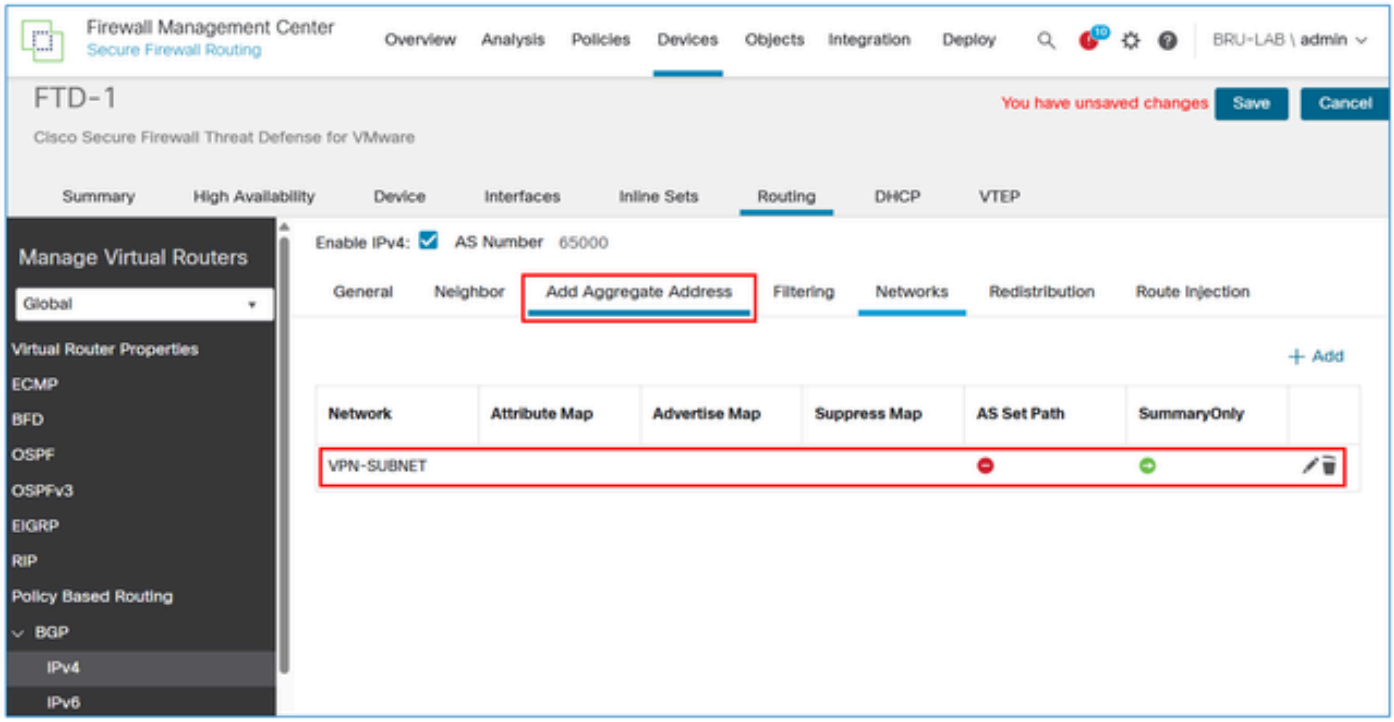
Filter all routes from updates

Cancel

OK

Nota: Se la casella di controllo Filtra tutte le route dagli aggiornamenti è deselezionata, l'FTD annuncia sia l'indirizzo di riepilogo che le route VPN /32 specifiche su BGP. Quando la casella di controllo è attivata, il FMC invia il comando aggregate-address summary-only alla configurazione LINA FTD, assicurandosi che venga annunciato solo l'indirizzo di riepilogo.

Il risultato:



Salvare e distribuire la configurazione sull'FTD.

Verifica

Configurazione BGP 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
```

Output tabella FTD BGP:

<#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 ?
```

Output tabella BGP R1:

<#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 ?
```

Output tabella di routing 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).