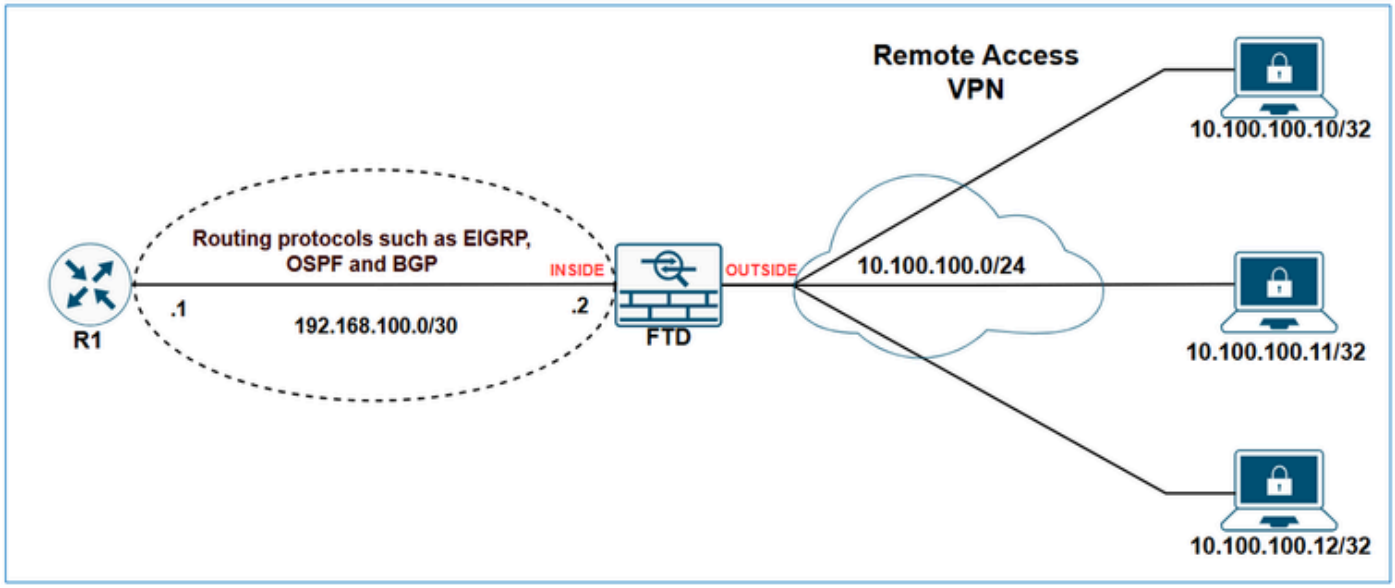
Annonce des sous-réseaux VPN d'accès distant via les protocoles de routage dans FTD

Table des matières

Introduction

Ce document décrit les options disponibles pour annoncer les sous-réseaux associés au VPN à l'aide des protocoles de routage EIGRP, OSPF et BGP.



Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

Remarque : Ce document décrit la configuration pour la redistribution des sous-réseaux VPN d'accès à distance via EIGRP, OSPF et BGP à l'aide du FMC. Pour obtenir des conseils sur la redistribution de route avec FDM, reportez-vous au guide de configuration FDM.

Informations générales

La première chose à comprendre est comment le FTD classe les sous-réseaux VPN dans sa table de routage. Bien que ces sous-réseaux apparaissent comme connectés par VPN, ils ne sont pas considérés comme des sous-réseaux connectés directement ; au lieu de cela, ils sont traités comme des routes statiques.

Les résultats de la commande show le démontrent.

Sortie FTD show route :

<#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
```

Sortie FTD show route connected :

<#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
```

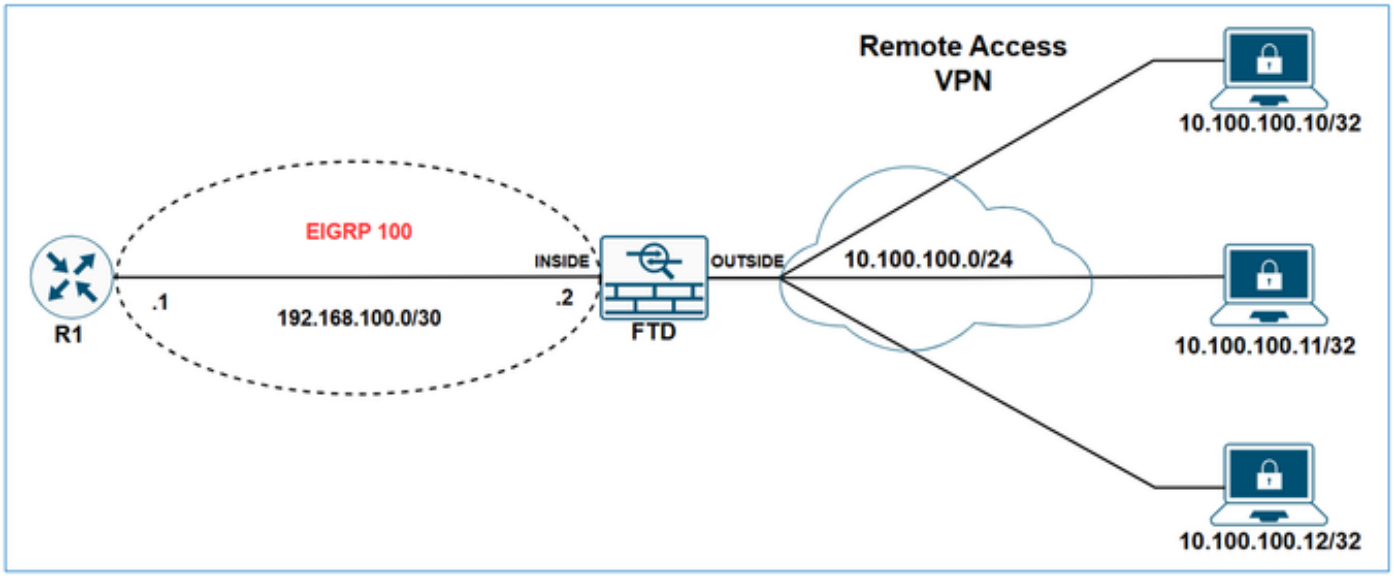
Sortie FTD show route static :

```
<#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
```

Maintenant que la manière dont les sous-réseaux VPN sont traités dans la table de routage du pare-feu est claire, l'étape suivante consiste à explorer comment les annoncer à l'aide de divers protocoles de routage.

Redistribution des sous-réseaux VPN d'accès à distance via EIGRP sur FTD

Diagramme du réseau



Les routes statiques qui entrent dans le cadre d'une instruction réseau sont automatiquement redistribuées au protocole EIGRP ; vous n'avez pas besoin de définir une règle de redistribution pour eux. Cependant, lors de la redistribution de routes statiques qui pointent vers des interfaces VTI dans EIGRP, vous devez spécifier la métrique. Pour les routes statiques pointant vers d'autres types d'interfaces, il n'est pas nécessaire de spécifier la métrique.

En raison du comportement du protocole EIGRP consistant à redistribuer automatiquement les routes statiques qui entrent dans le cadre des instructions réseau, il existe deux options pour annoncer les sous-réseaux VPN via le protocole EIGRP sur FTD :

1. Utilisation d'une instruction network.
2. Utilisation de l'approche statique redistribute.

Dans cet exemple, l'objectif est de faire apprendre à R1 le sous-réseau VPN 10.100.100.0/24 via EIGRP.

Configuration initiale 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 Table de routage initiale :

<#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
```

Table topologique EIGRP initiale 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
```

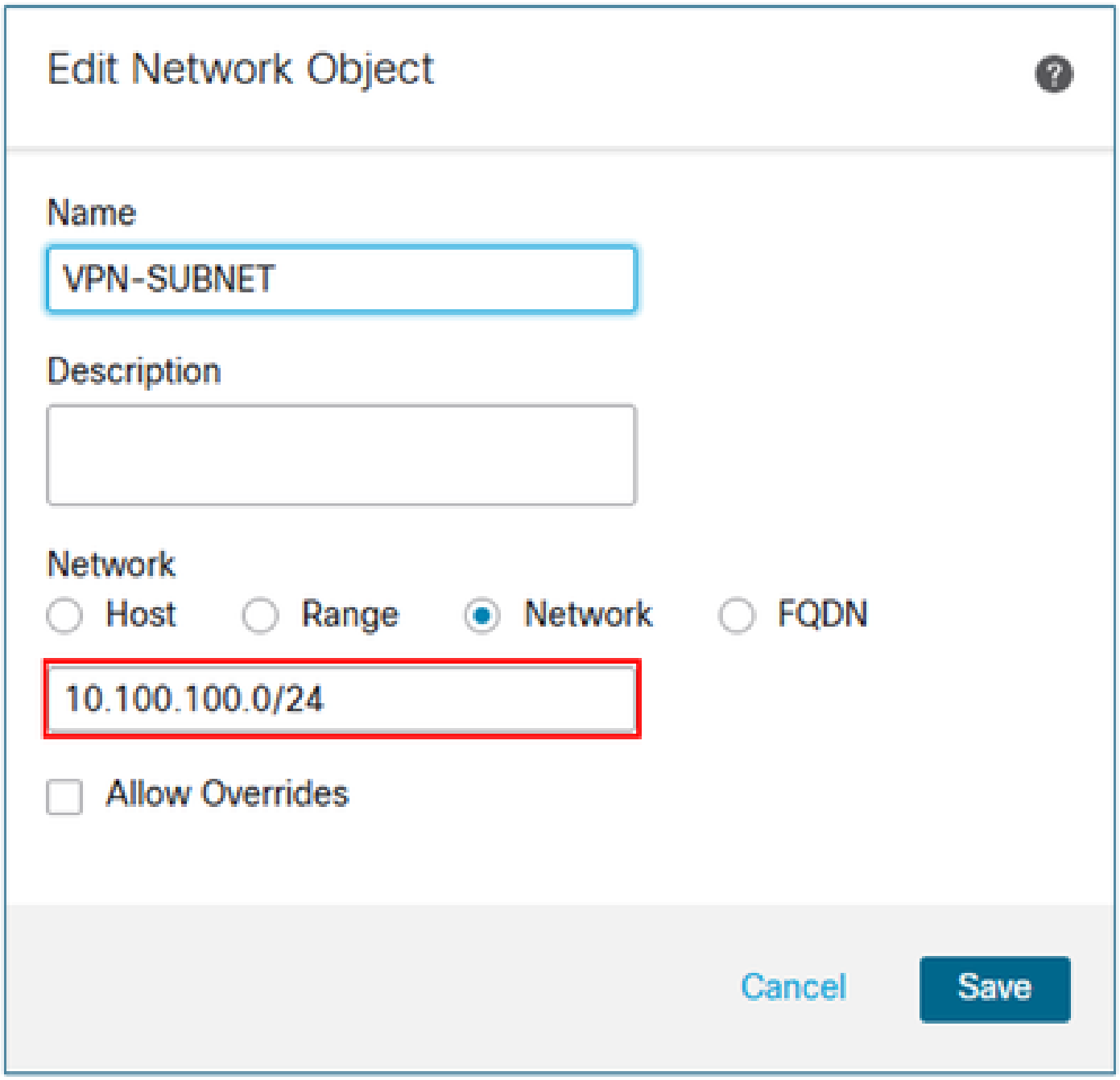
Table de routage initial de R1 :

```
<#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
```

Redistribution des sous-réseaux VPN d'accès distant via EIGRP sur FTD à l'aide de l'instruction network

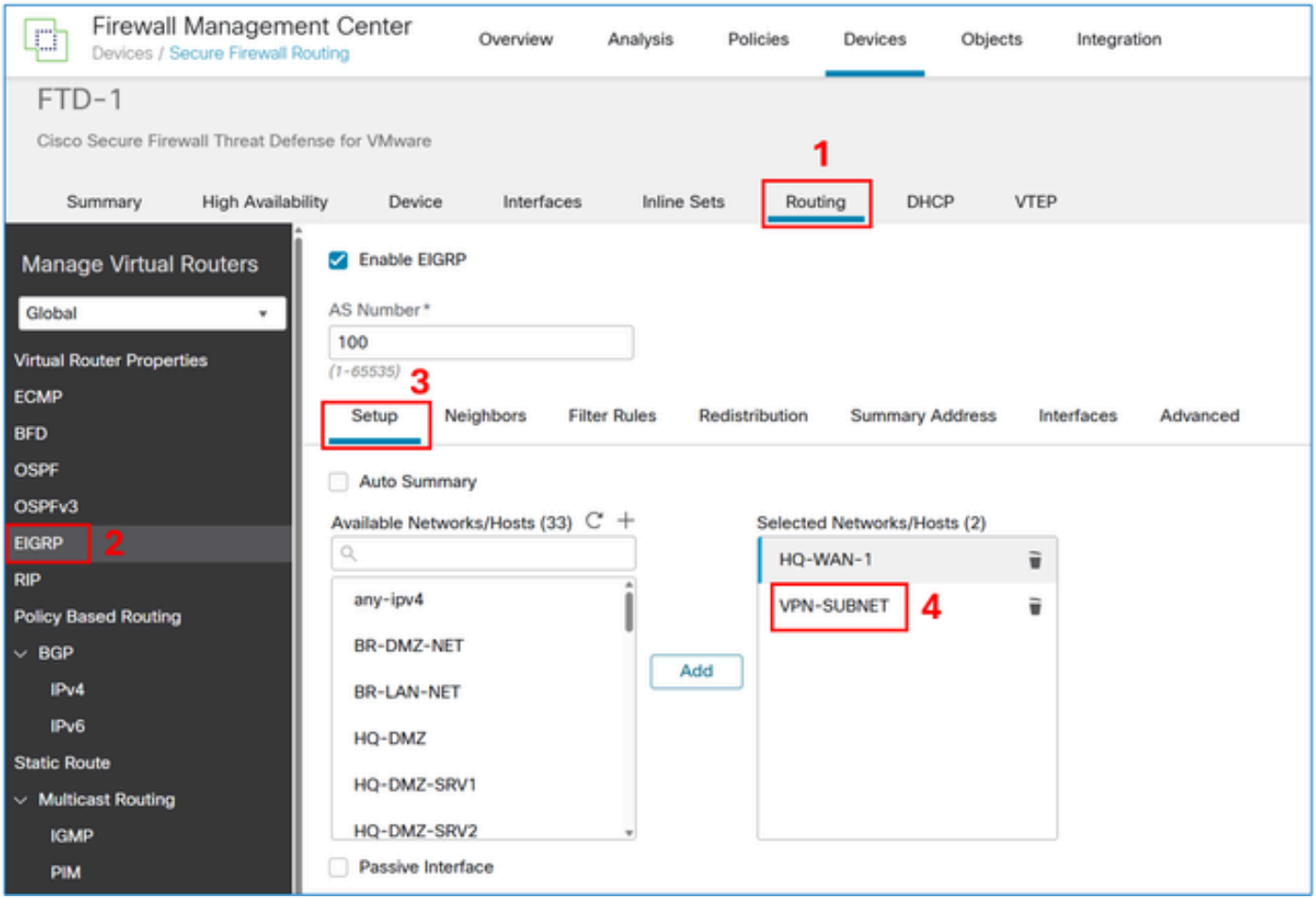
Configurer

Étape 1 : création d’un objet réseau pour le sous-réseau VPN



Étape 2 : inclusion de l’objet de sous-réseau VPN dans l’instruction network

Dans l'interface utilisateur de gestion des périphériques FMC, accédez à Routing > EIGRP > Setup, et incluez le sous-réseau VPN dans les réseaux/hôtes sélectionnés.



Enregistrez et déployez la configuration sur le FTD.

Vérifier

Configuration 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
```

Table topologique 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

Table de routage 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

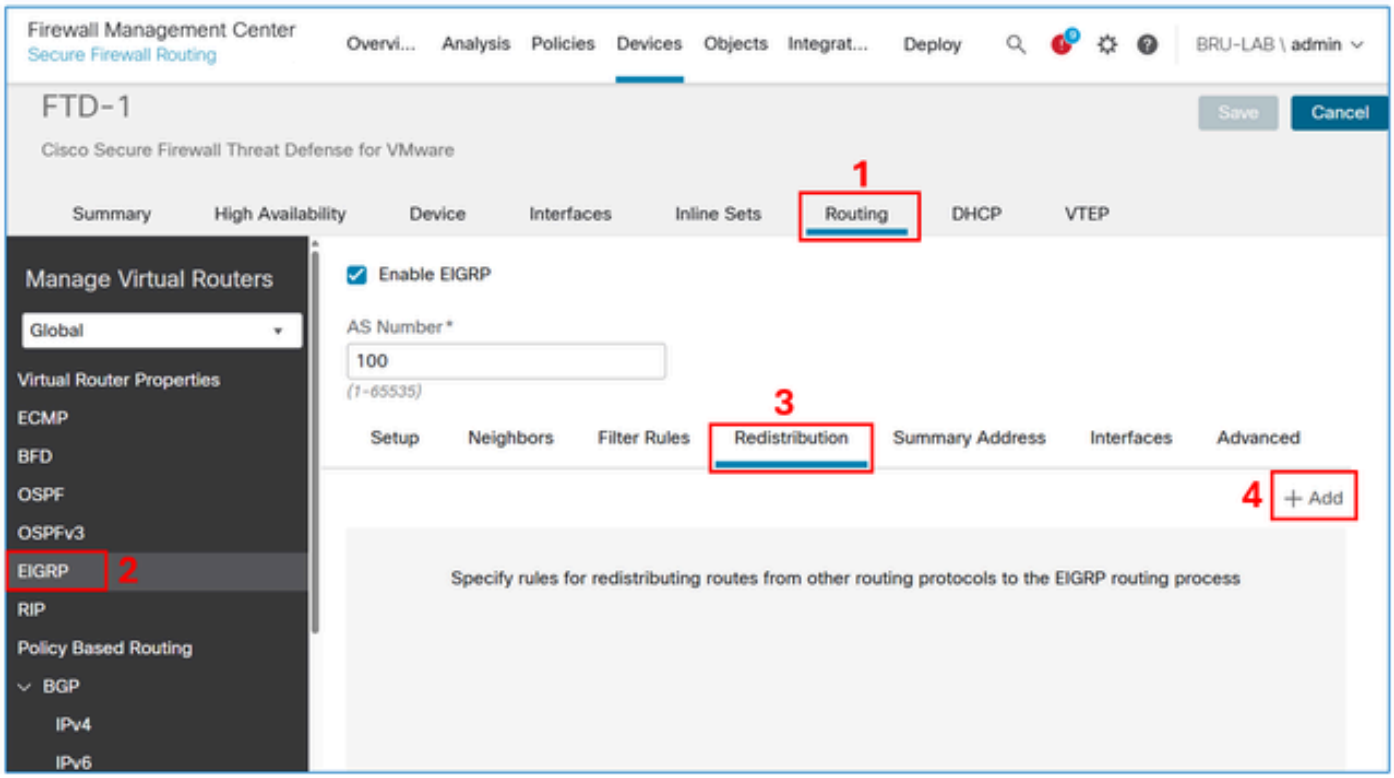
[90/3072] via 192.168.100.2, 00:02:17, GigabitEthernet1

Remarque : Notez que bien que l'instruction network ait été 10.100.100.0/24, le FTD redistribue un sous-réseau /32 sur EIGRP. Cela se produit parce que le FTD crée une route statique avec un préfixe /32 pour chaque session VPN d'accès à distance. Pour optimiser cela, vous pouvez utiliser la fonctionnalité d'adresse récapitulative EIGRP.

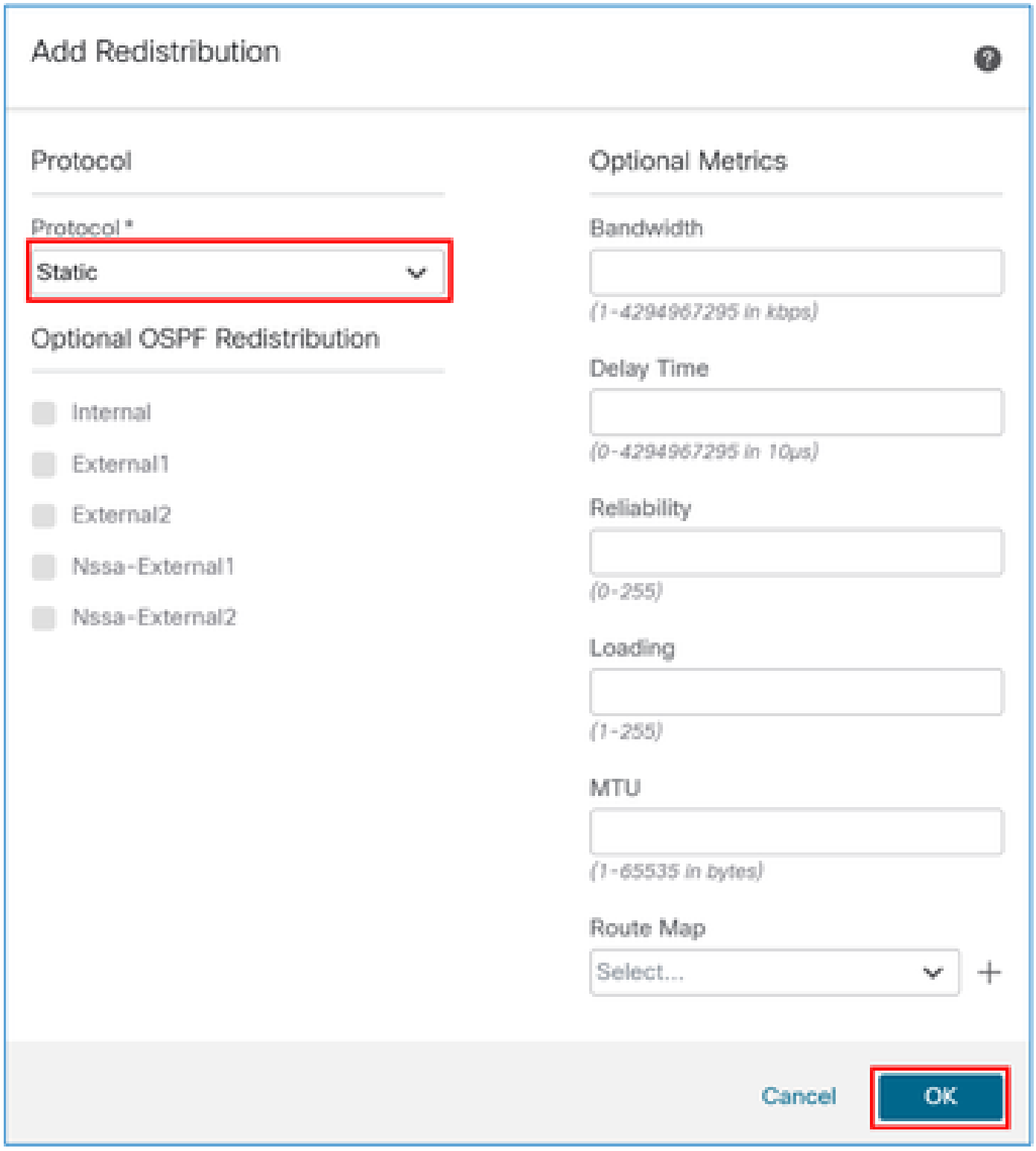
Redistribuez les sous-réseaux VPN d'accès à distance via EIGRP sur FTD en utilisant l'approche statique redistribute

Configurer

Dans l'interface utilisateur de gestion des périphériques FMC, accédez à Routing > EIGRP > Redistribution, puis sélectionnez le bouton Add.

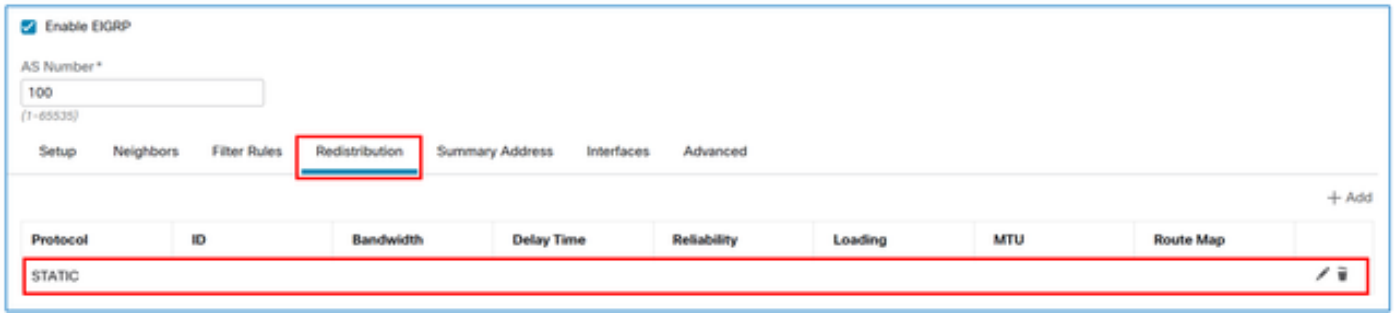


Dans le champ de protocole, sélectionnez Static, puis cliquez sur le bouton OK.



⚠ Attention : toutes les routes statiques sont redistribuées dans EIGRP. Si vous devez annoncer uniquement les sous-réseaux VPN, vous pouvez soit utiliser l'approche d'instruction réseau, soit appliquer une carte de routage pour les filtrer.

Le résultat :



Enregistrez et déployez la configuration sur le FTD.

Vérifier

Configuration 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

Table topologique 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
```

Table de routage R1:

<#root>

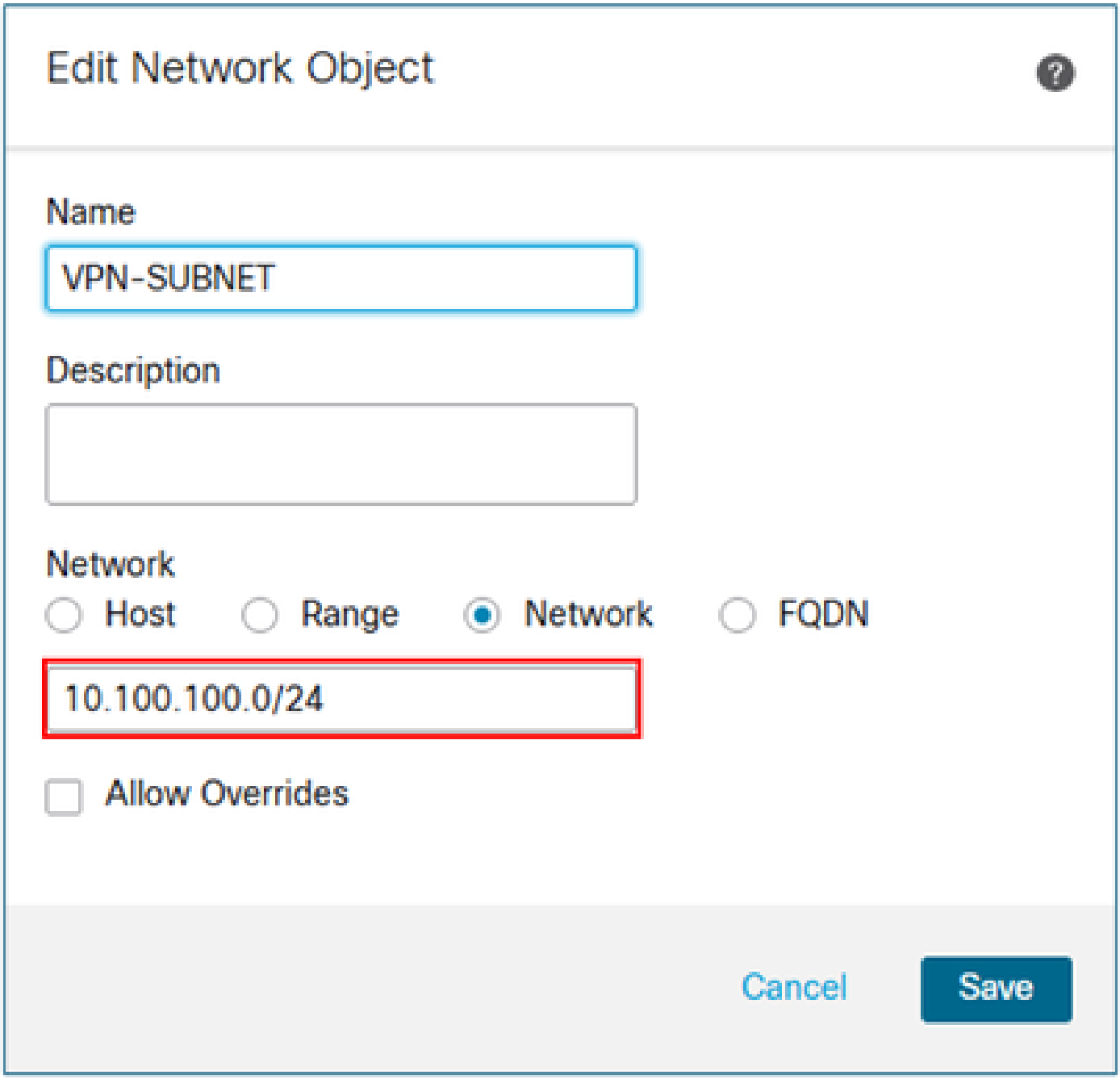
```
R1#
show ip route


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
```

Conseil : Vous pouvez éventuellement utiliser la fonctionnalité d'adresse récapitulative EIGRP sur FTD pour optimiser la taille de la table de routage.

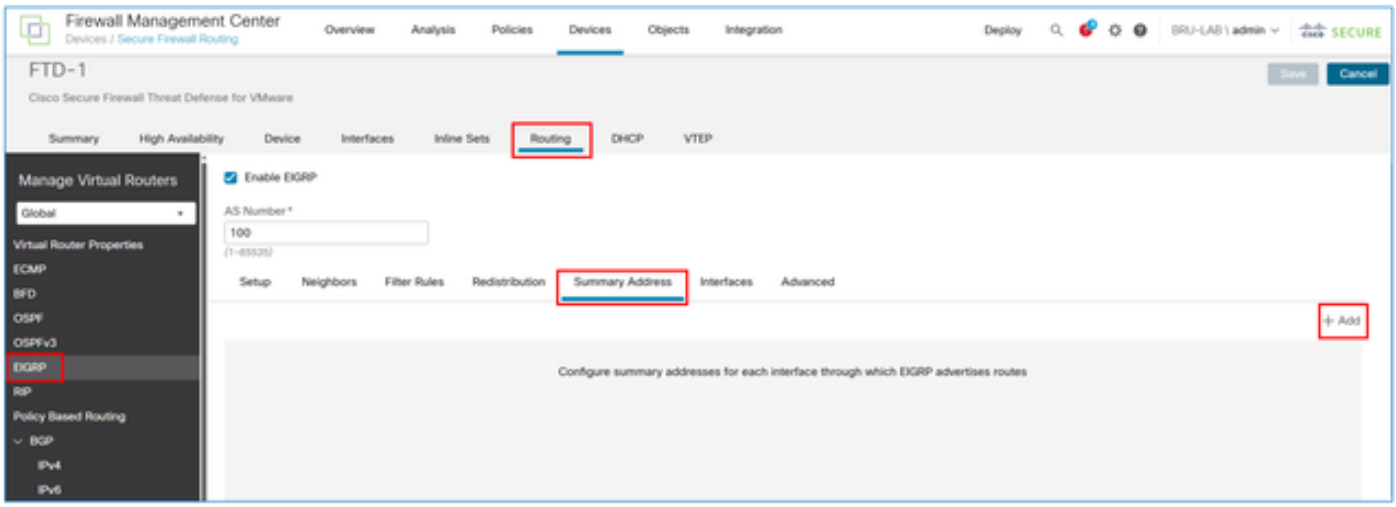
Configuration des adresses récapitulatives EIGRP

Configurer

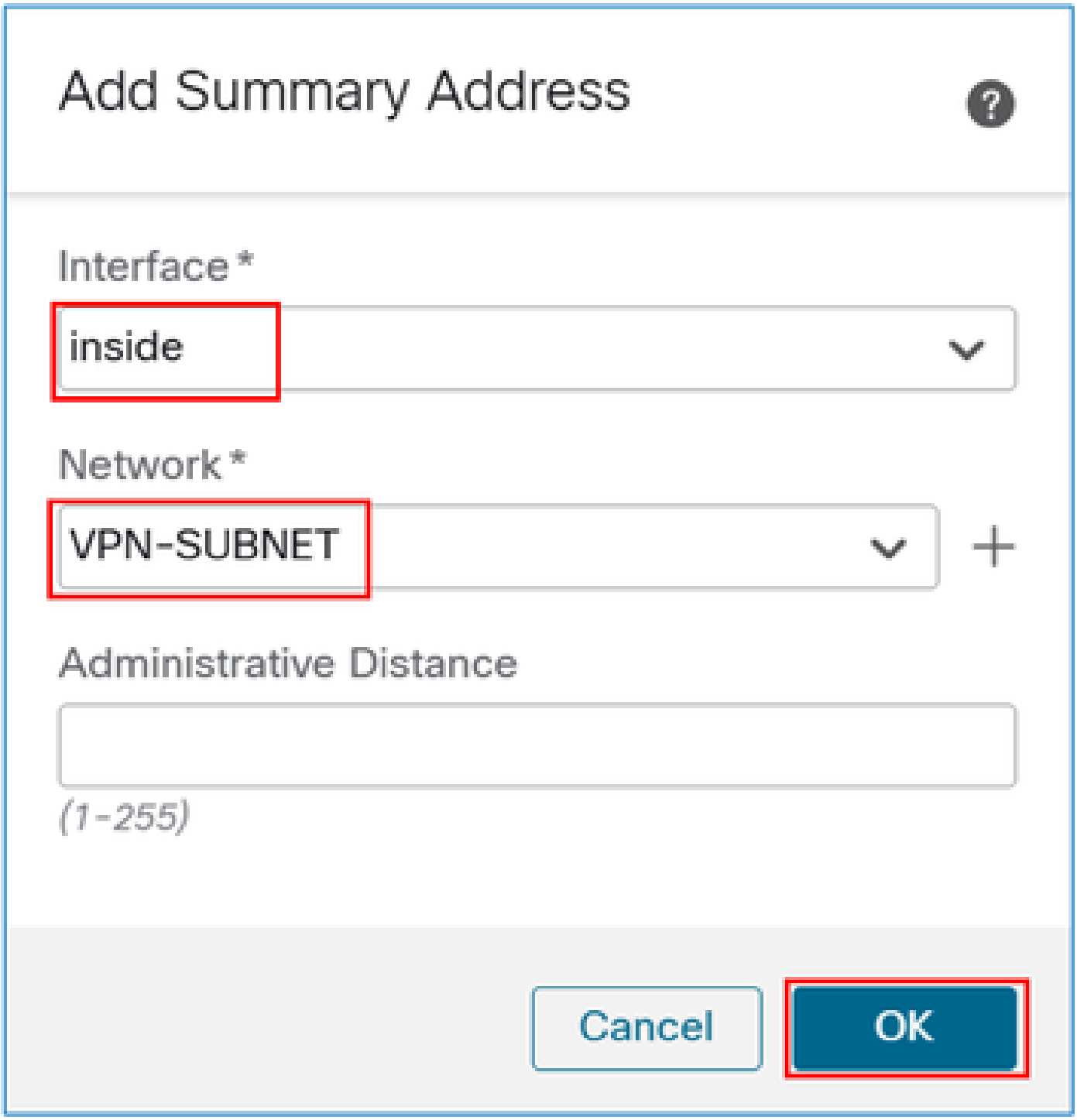
S'il n'a pas encore été créé, créez un objet réseau pour les sous-réseaux VPN.



Dans l'interface utilisateur de gestion des périphériques FMC, accédez à Routing > EIGRP > Summary Address, puis sélectionnez le bouton Add.



Dans le champ interface, saisissez celui qui fait face au voisin EIGRP, et dans le champ network, saisissez l'objet créé pour le sous-réseau VPN.


Add Summary Address
Interface *
inside
Network *
VPN-SUBNET
Administrative Distance
(1-255)
Cancel
OK

Le résultat :

Vérifier

Configuration de l'adresse récapitulative 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

Table topologique 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
```

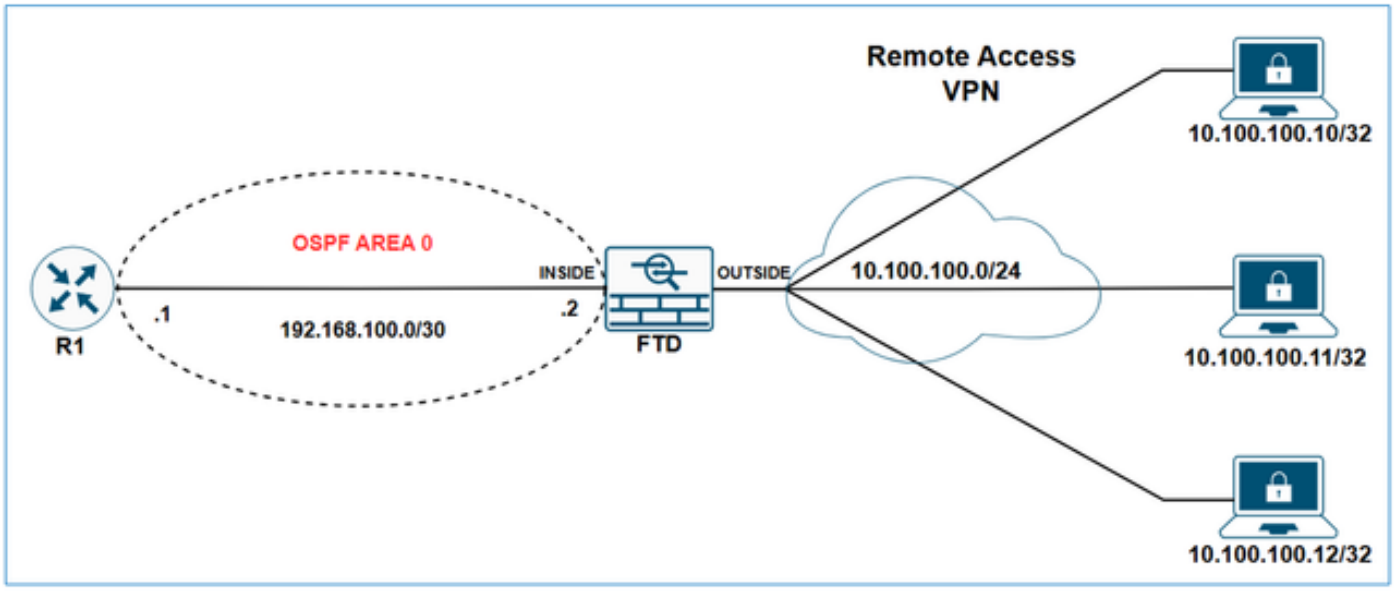
Table de routage R1:

<#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
```

Redistribution des sous-réseaux VPN d'accès à distance via OSPF sur FTD

Diagramme du réseau



Paramètres de configuration initiaux

<#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
```

Sortie de la commande FTD show ospf neighbor :

<#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
```

Résultat de la commande show ip ospf neighbor de R1 :

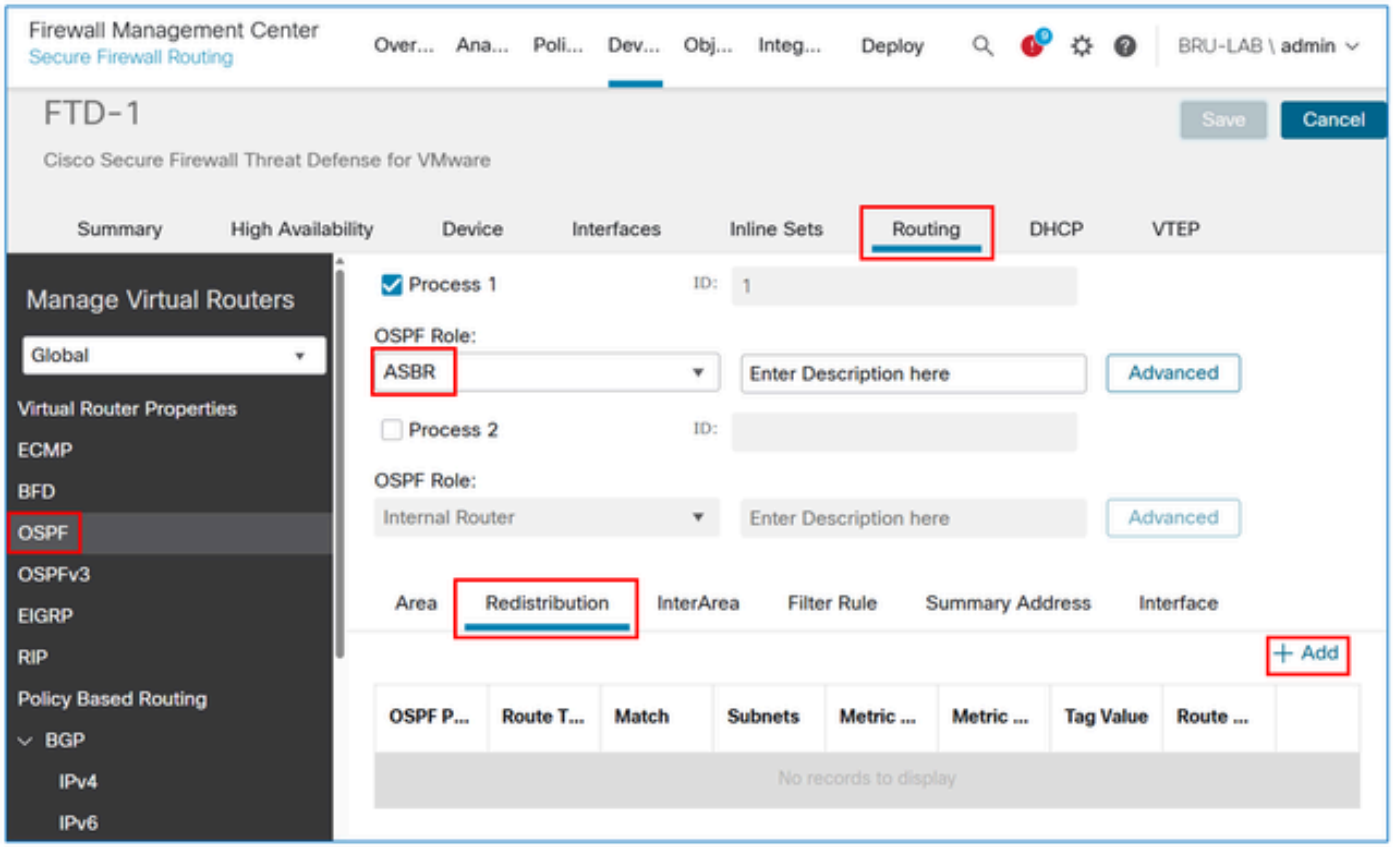
```
<#root>

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
```

Table de routage 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
```

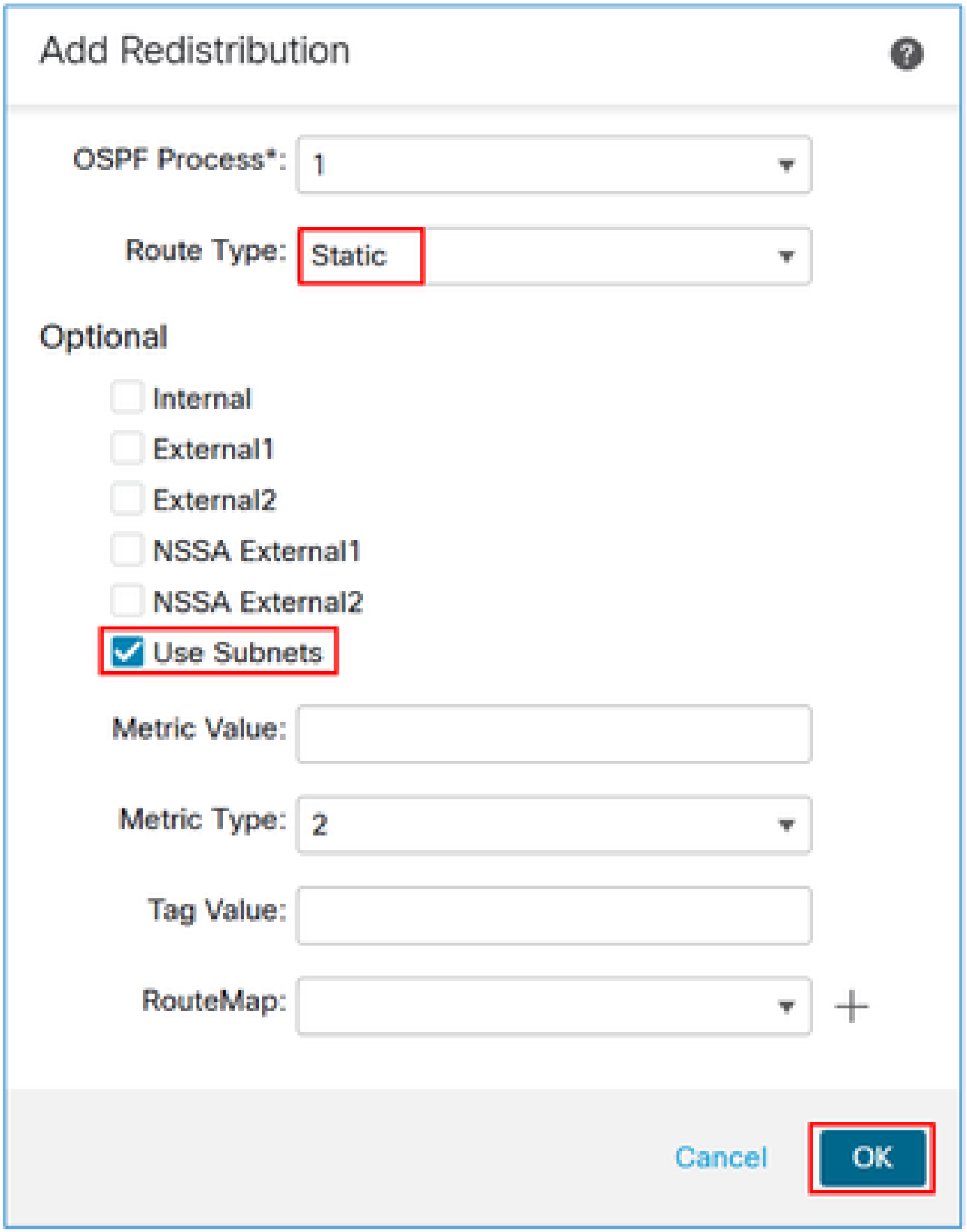
Configurer

Dans l'interface utilisateur de gestion des périphériques FMC, accédez à Routing > OSPF > Redistribution, puis sélectionnez le bouton Add.



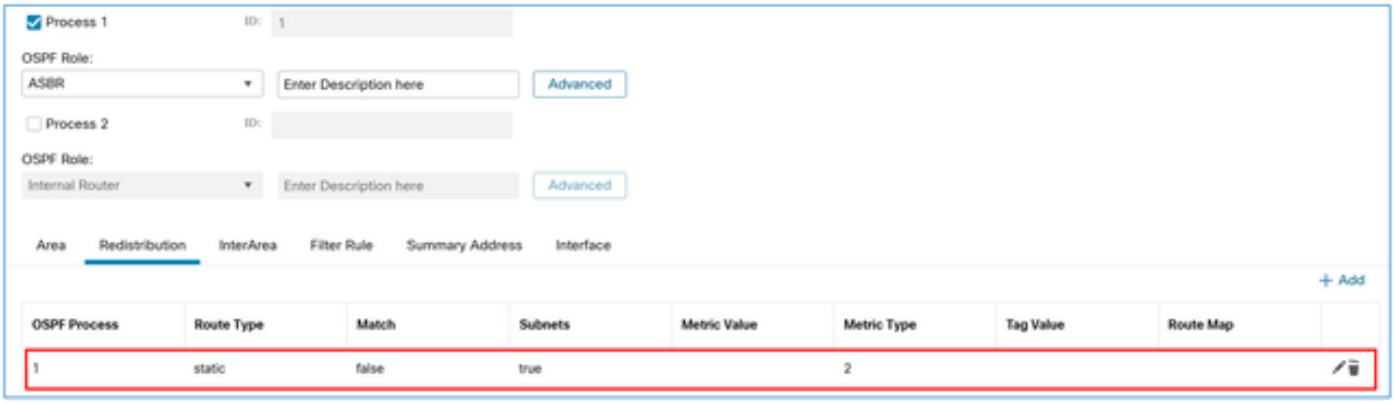
Remarque : Le rôle OSPF doit être défini sur ASBR ou ABR & ASBR pour activer la redistribution.

Dans le champ Type de route, sélectionnez Static, puis cochez la case Use Subnets.



⚠ Attention : toutes les routes statiques sont redistribuées dans OSPF. Si vous devez annoncer uniquement les sous-réseaux VPN, vous pouvez appliquer une carte de routage pour les filtrer.

Le résultat :



Vérifier

Configuration de redistribution 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

Table de routage 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
```

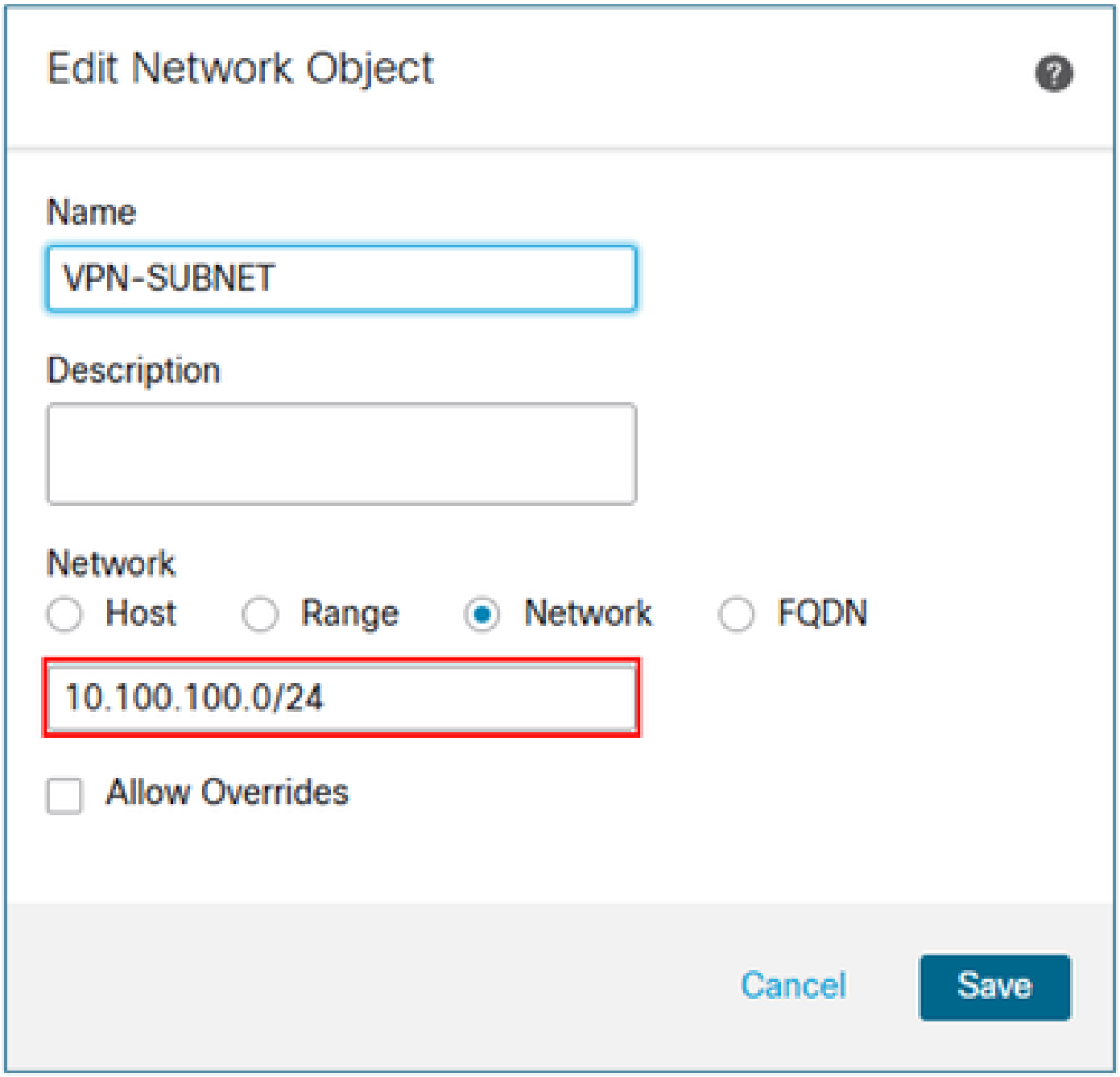
```
C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
      10.0.0.0/32 is subnetted, 1 subnets
O E2     10.100.100.10 [110/20] via 192.168.100.2, 00:08:01, GigabitEthernet1
```

Conseil : Notez que bien que le pool VPN soit 10.100.100.0/24, le FTD redistribue un sous-réseau /32 sur OSPF. Cela se produit parce que le FTD crée une route statique avec un préfixe /32 pour chaque session VPN d'accès à distance. Pour optimiser cela, vous pouvez utiliser la fonctionnalité OSPF Summary Address.

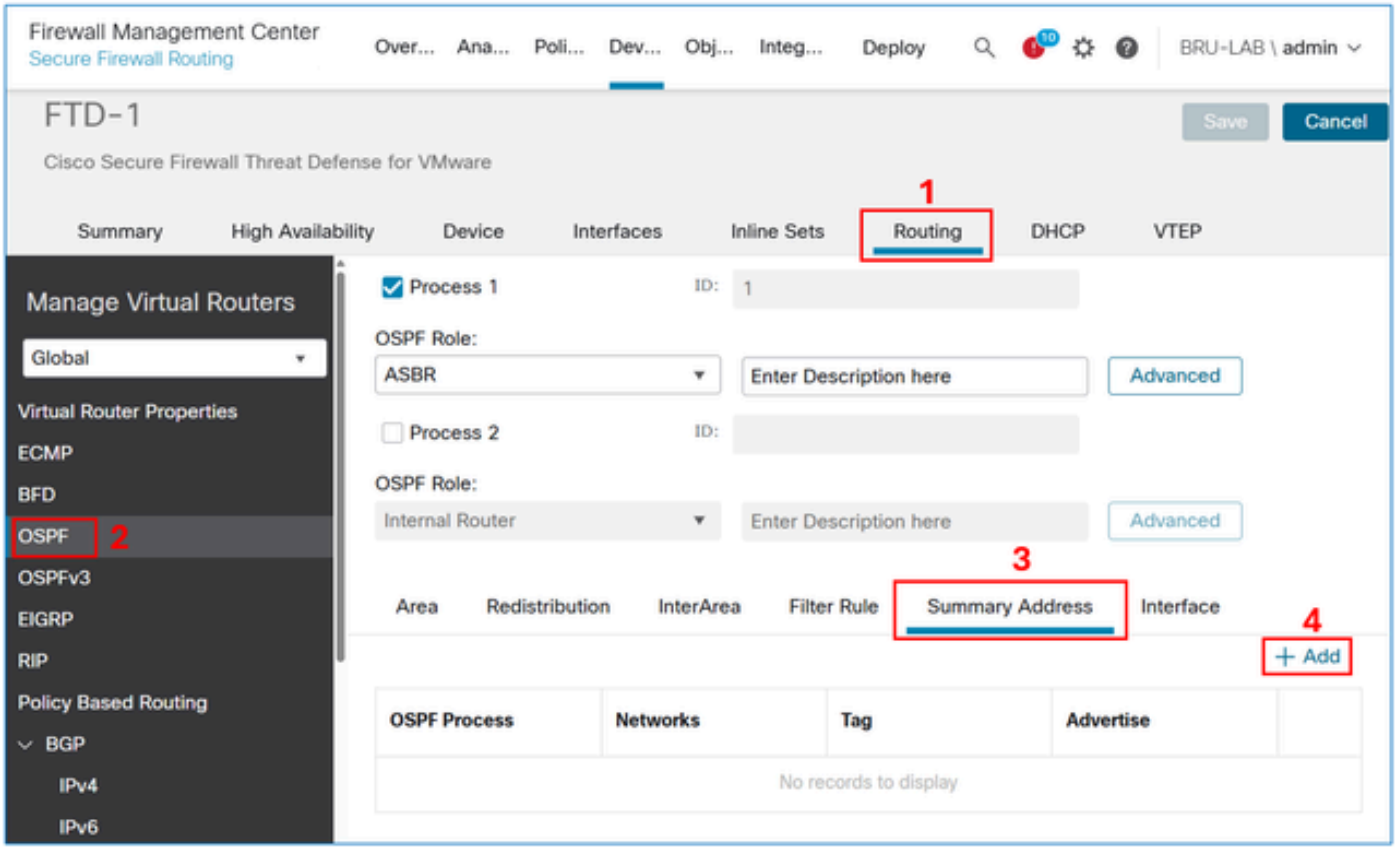
Configuration des adresses récapitulatives OSPF

Configurer

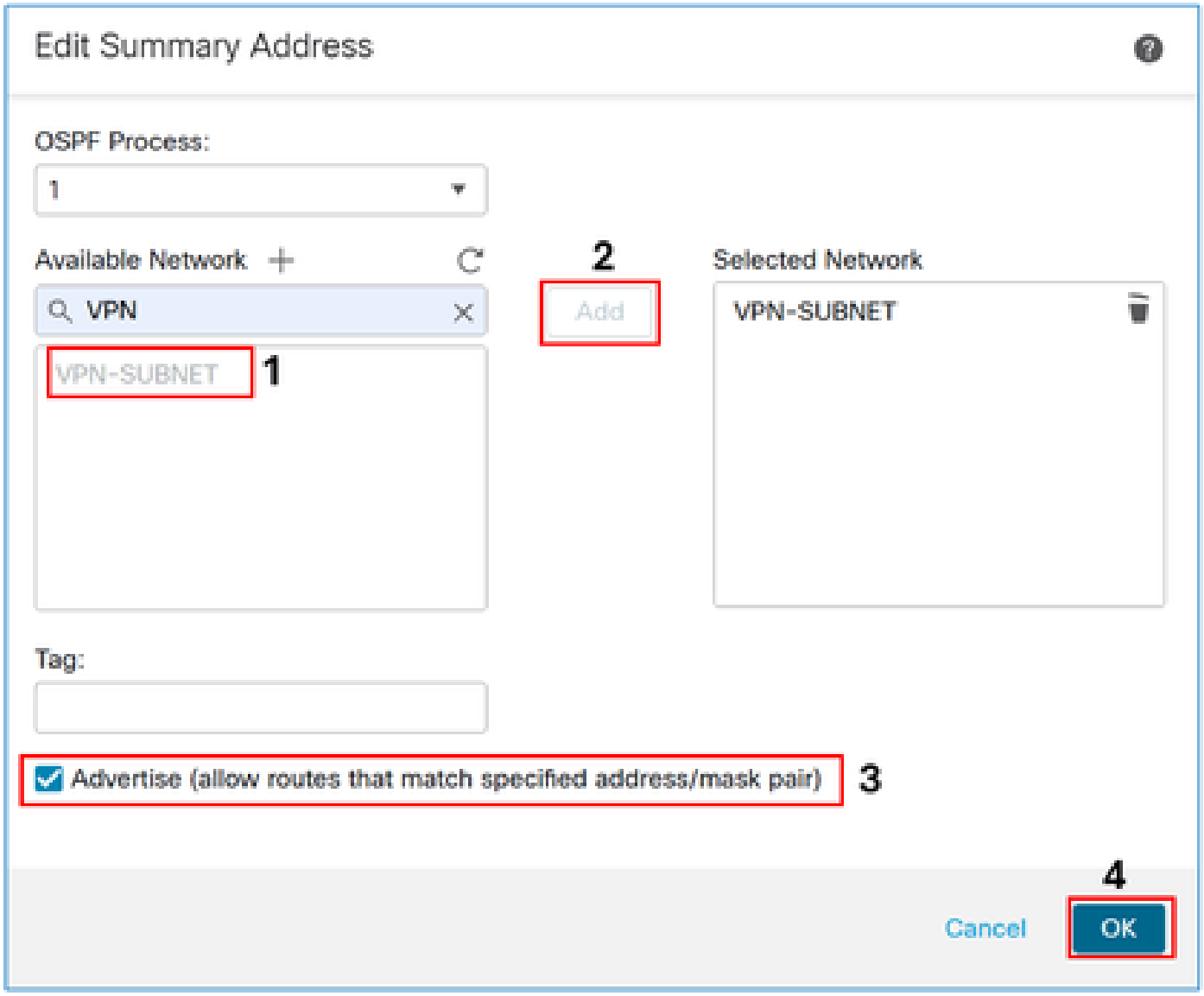
S'il n'a pas encore été créé, créez un objet réseau pour les sous-réseaux VPN.



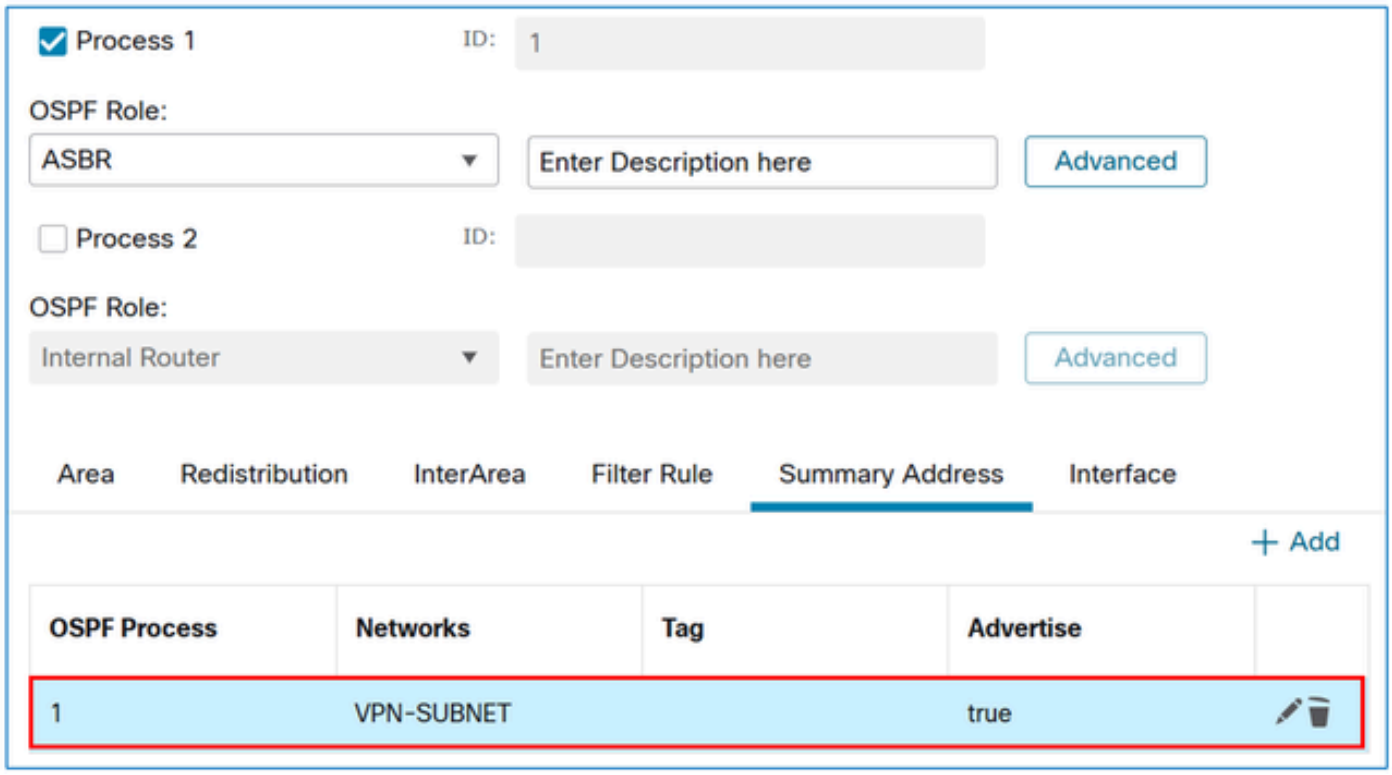
Dans l'interface utilisateur de gestion des périphériques FMC, accédez à Routing > OSPF> Summary Address, puis sélectionnez le bouton Add.



Ajoutez l'objet de sous-réseau VPN et cochez la case Annoncer.


Edit Summary Address
OSPF Process:
1
Available Network
VPN
VPN-SUBNET
1
2
Add
Selected Network
VPN-SUBNET
Tag:
Advertise (allow routes that match specified address/mask pair)
3
4
Cancel
OK

Le résultat :



Vérifier

Configuration FTD OSPF :

<#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

Table de routage R1:

<#root>

R1#

sh ip route

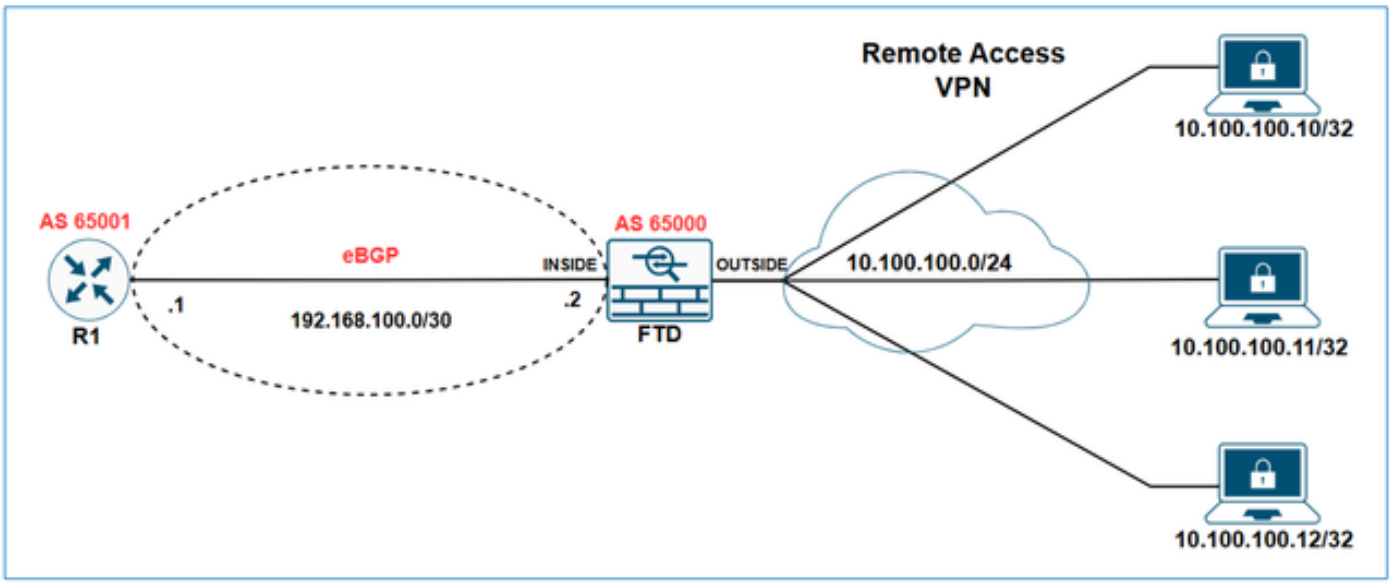
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       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`

Redistribuer les sous-réseaux VPN d'accès à distance via eBGP sur FTD

Diagramme du réseau



Dans cet exemple, l'objectif est de faire apprendre à R1 le sous-réseau VPN 10.100.100.0/24 via eBGP.

Paramètres de configuration initiaux

FTD Configuration initiale :

<#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
```

Sortie de la table FTD bgp :

<#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 ?

FTD show bgp summary sortie :

<#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
```

Sortie show ip bgp summary de R1 :

```
<#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
```

Sortie de la table bgp de R1 :

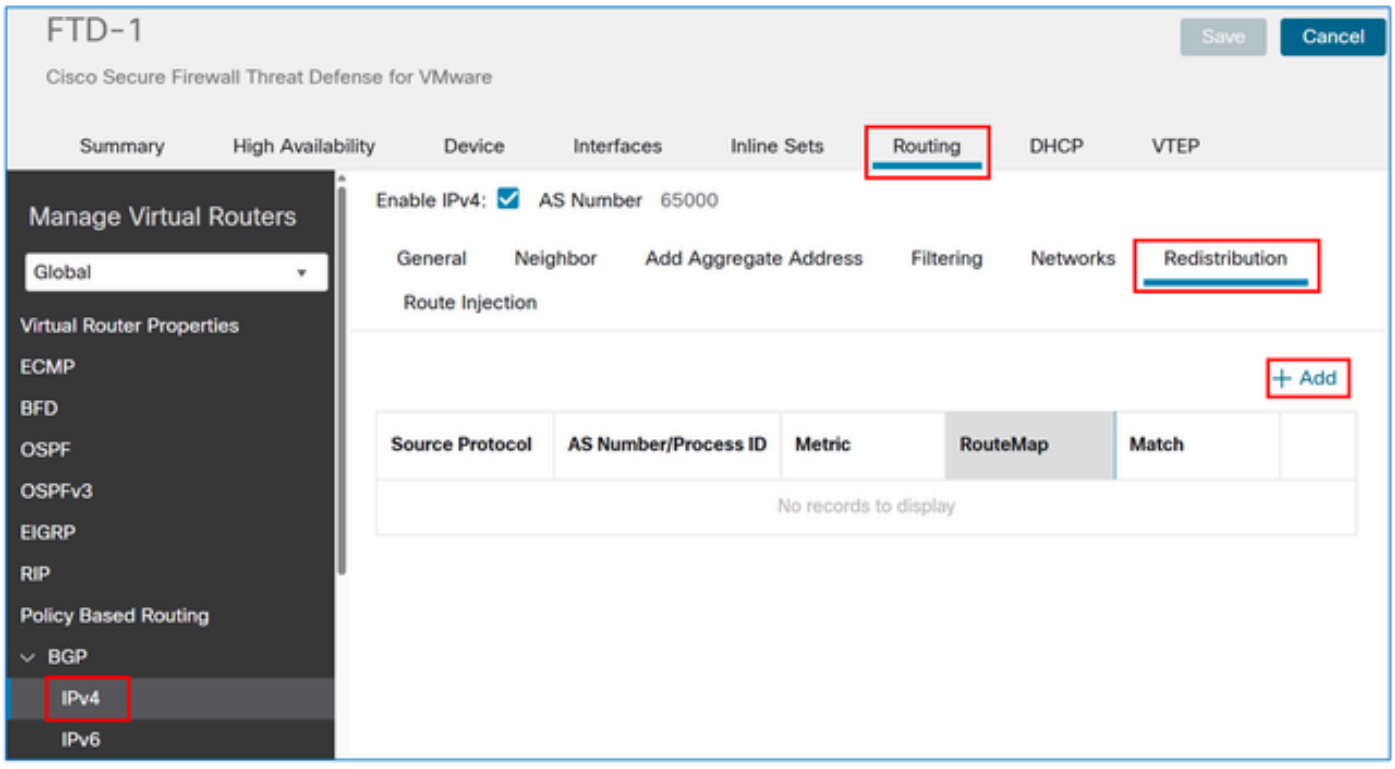
```
<#root>

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 ?
```

Table de routage 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
```

Configurer

Dans l'interface utilisateur de gestion des périphériques FMC, accédez à Routing > BGP > IPv4 > Redistribution, puis sélectionnez le bouton Add.



Dans le champ Source Protocol, choisissez Static, puis sélectionnez le bouton OK.

Add Redistribution

Source Protocol

Static

Process ID*

Metric

(0-4294967295)

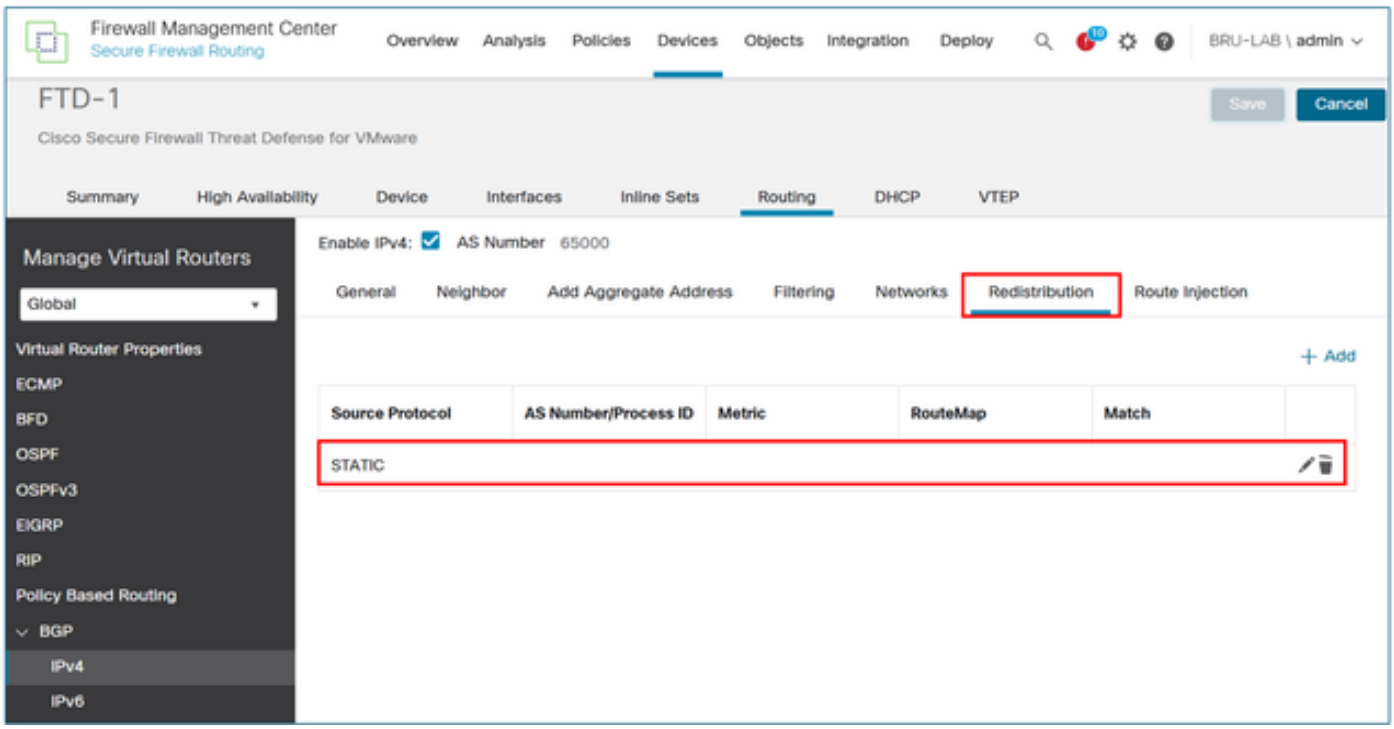
Route Map

Match

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

⚠ : cela redistribue toutes les routes statiques dans BGP. Si vous devez annoncer uniquement les sous-réseaux VPN, vous pouvez appliquer une carte de routage pour les filtrer.

Le résultat :



Enregistrez et déployez la configuration sur le FTD.

Vérifier

Configuration 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
```

Sortie de la table FTD bgp :

```
<#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 ?
```

Sortie de la table bgp de 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 ?
```

Sortie de la table de routage R1 :

```
<#root>

R1#

show ip route
```

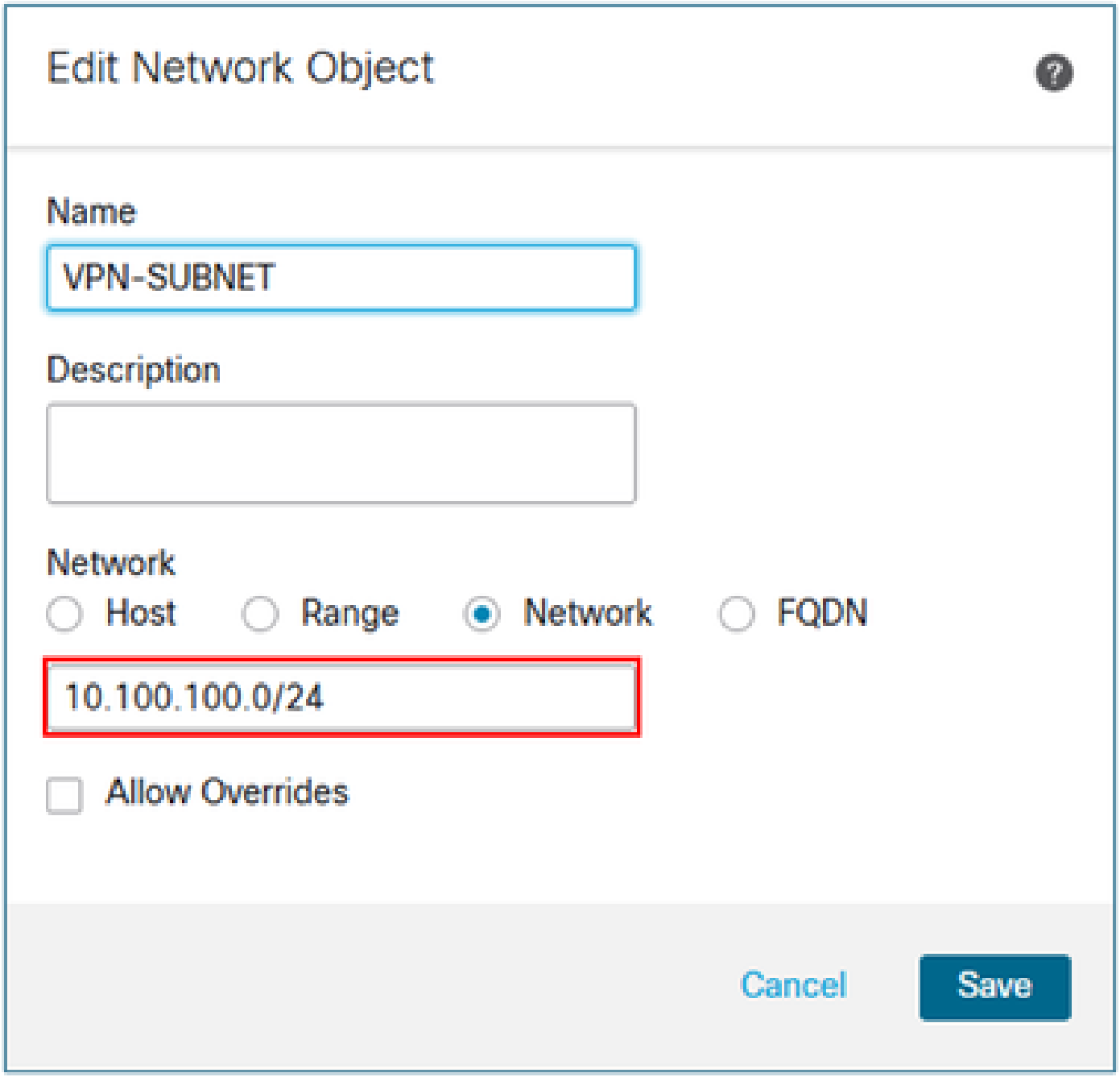
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT,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

Conseil : Notez que bien que le pool VPN soit 10.100.100.0/24, le FTD redistribue un sous-réseau /32 sur BGP. Cela se produit parce que le FTD crée une route statique avec un préfixe /32 pour chaque session VPN d'accès à distance. Pour optimiser cela, vous pouvez utiliser la fonctionnalité d'adresse d'agrégation BGP.

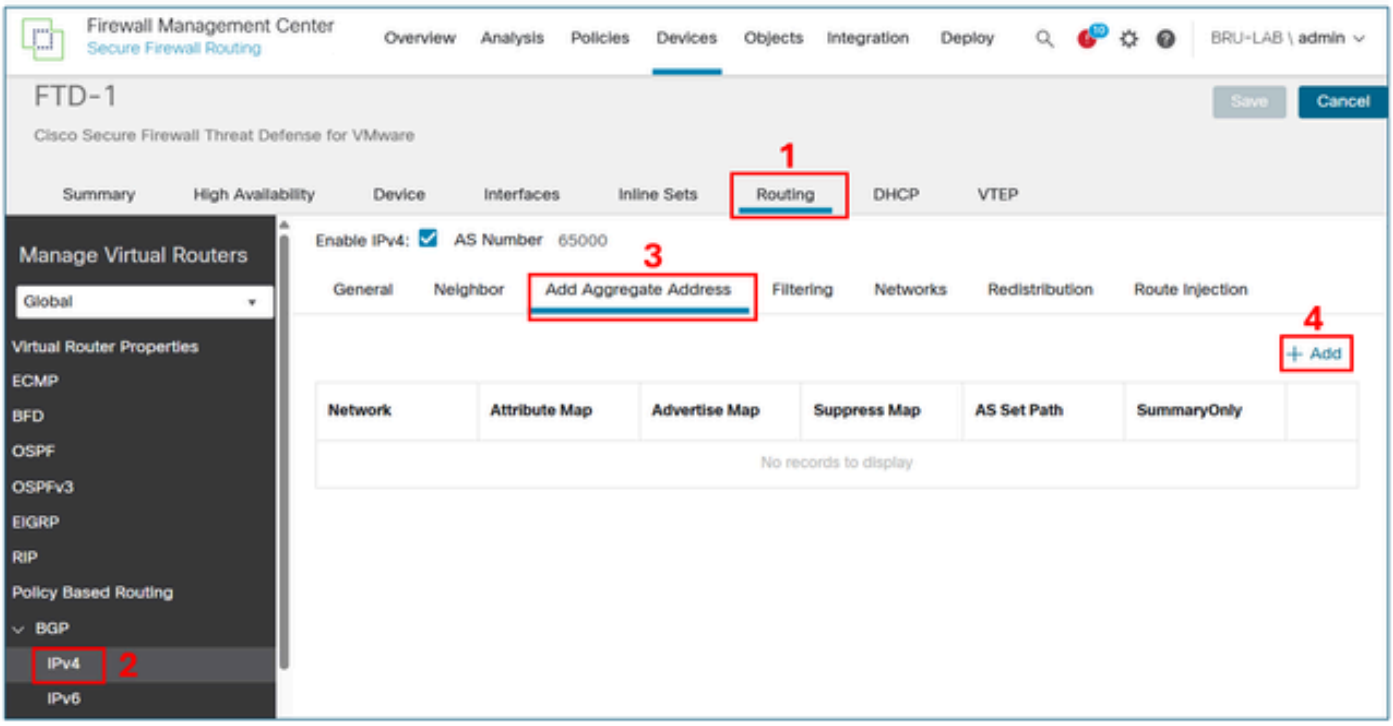
Configuration des adresses d'agrégation BGP

Configurer

S'il n'a pas encore été créé, créez un objet réseau pour les sous-réseaux VPN.



Dans l'interface utilisateur de gestion des périphériques FMC, accédez à Routing > BGP > IPv4 > Add Aggregate Address, puis sélectionnez le bouton Add.



Dans le champ réseau, ajoutez l'objet pour le sous-réseau VPN, puis activez la case à cocher Filtrer toutes les routes à partir des mises à jour.

Add Aggregate Address

Network*

VPN-SUBNET

Attribute Map

Advertise Map

Suppress Map

Generate AS set path information

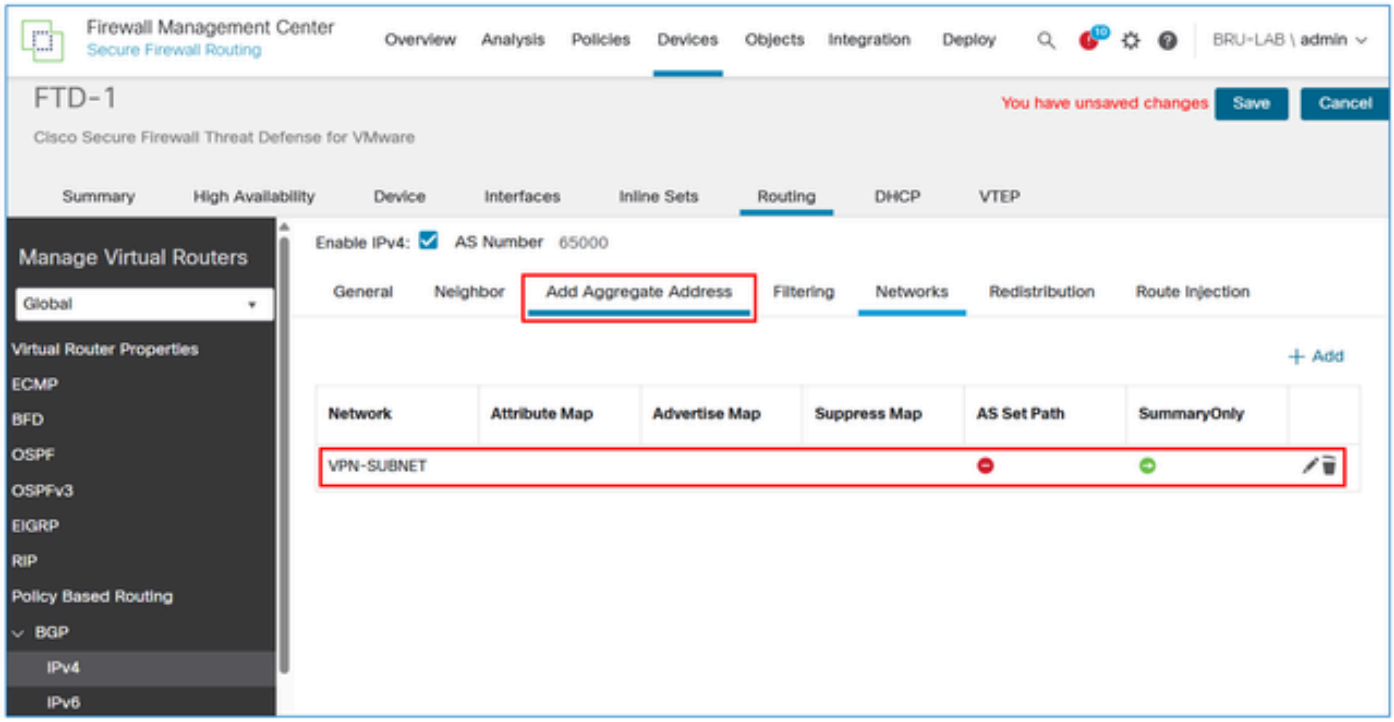
Filter all routes from updates

Cancel

OK

Remarque : Si la case Filter all routes from updates est décochée, le FTD annonce à la fois l'adresse récapitulative et les routes VPN /32 spécifiques sur BGP. Lorsque la case est cochée, le FMC pousse la commande aggregate-address summary-only vers la configuration FTD LINA, en s'assurant que seule l'adresse récapitulative est annoncée.

Le résultat :



Enregistrez et déployez la configuration sur le FTD.

Vérifier

Configuration 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
```

Sortie de la table 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 ?
```

Sortie de la table BGP de 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 ?
```

Sortie de la table de routage 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.