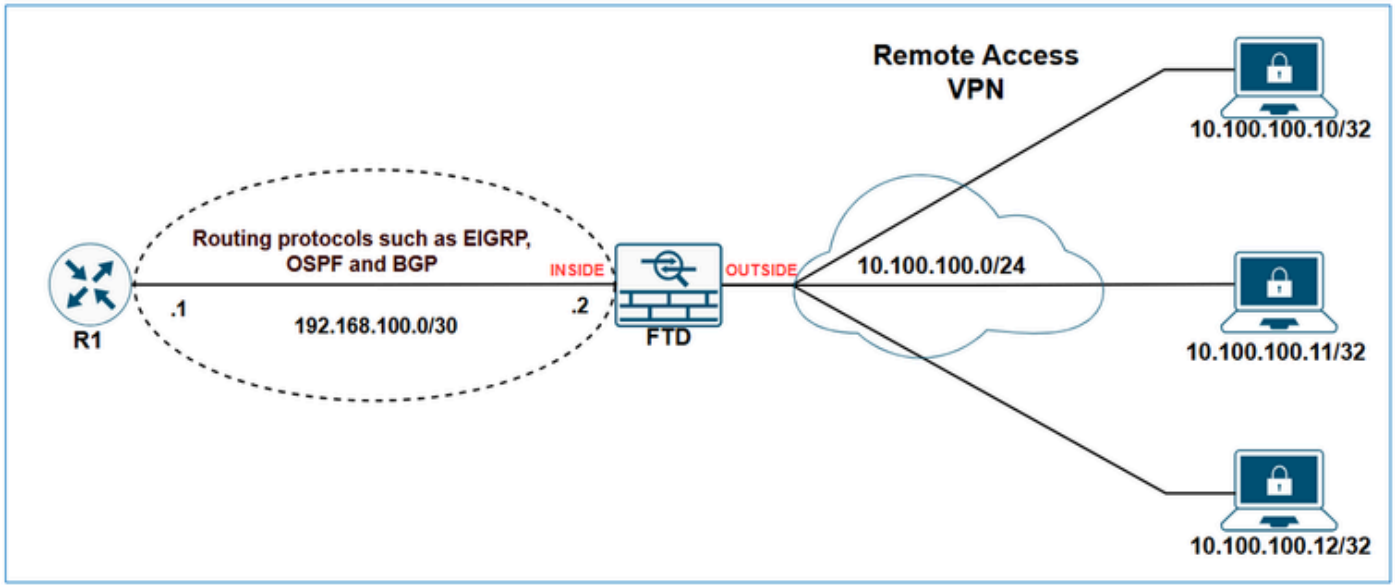
FTD의 라우팅 프로토콜을 통해 원격 액세스 VPN 서브넷 알림

목차

소개

이 문서에서는 라우팅 프로토콜 EIGRP, OSPF 및 BGP를 사용하여 VPN 관련 서브넷을 광고하는 데 사용할 수 있는 옵션에 대해 설명합니다.



사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

참고: 이 문서에서는 FMC를 사용하여 EIGRP, OSPF 및 BGP를 통해 원격 액세스 VPN 서브넷을 재배포하기 위한 컨피그레이션에 대해 간략하게 설명합니다. FDM을 사용한 경로 재배포에 대한 지침은 FDM 컨피그레이션 가이드를 참조하십시오.

배경 정보

가장 먼저 이해해야 할 사항은 FTD가 라우팅 테이블에서 VPN 서브넷을 분류하는 방법입니다. 이러한 서브넷은 VPN에 의해 연결된 것으로 표시되지만 직접 연결된 서브넷으로 간주되지 않습니다. 대신 고정 경로로 처리됩니다.

show 출력으로 확인할 수 있습니다.

FTD show route 출력:

<#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 출력:

<#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
```

FTD는 경로 고정 출력을 표시합니다.

<#root>

FTD-HQ-1#

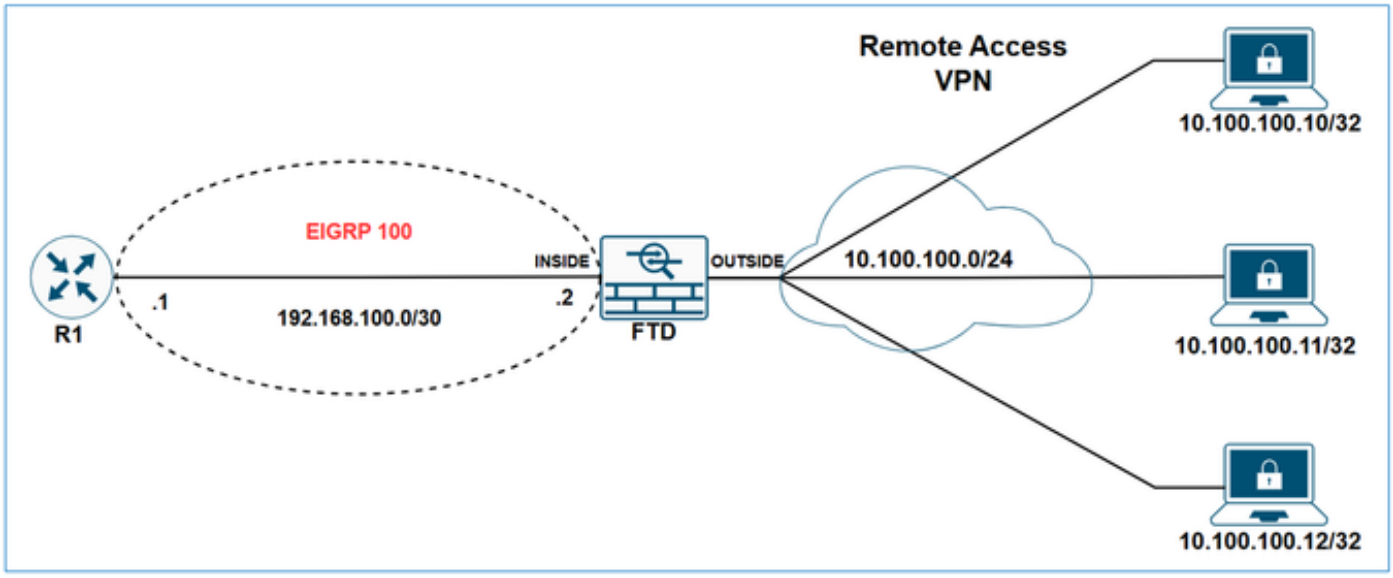
```
show route static
```

```
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
```

이제 VPN 서브넷이 방화벽의 라우팅 테이블에서 어떻게 처리되는지 분명하므로, 다음 단계는 다양한 라우팅 프로토콜을 사용하여 서브넷을 광고하는 방법을 탐색하는 것입니다.

FTD의 EIGRP를 통해 원격 액세스 VPN 서브넷 재배포

네트워크 다이어그램



network 문의 범위에 속하는 고정 경로는 EIGRP로 자동으로 재배포됩니다. 재배포 규칙을 정의할 필요가 없습니다. 그러나 EIGRP의 VTI 인터페이스를 가리키는 고정 경로를 재배포할 경우 메트릭을 지정해야 합니다. 다른 유형의 인터페이스를 가리키는 고정 경로의 경우 메트릭을 지정할 필요가 없습니다.

네트워크 명령문의 범위에 속하는 고정 경로를 자동으로 재배포하는 EIGRP의 동작으로 인해 FTD에서 EIGRP를 통해 VPN 서브넷을 광고하는 두 가지 옵션이 있습니다.

1. 네트워크 명령문 사용
2. Redistribute Static 접근 방식을 사용합니다.

이 예에서 목표는 R1이 EIGRP를 통해 VPN 서브넷 10.100.100.0/24을 학습하도록 하는 것입니다.

FTD 초기 구성:

<#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 초기 라우팅 테이블:

<#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 초기 EIGRP 토폴로지 테이블:

```
<#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
```

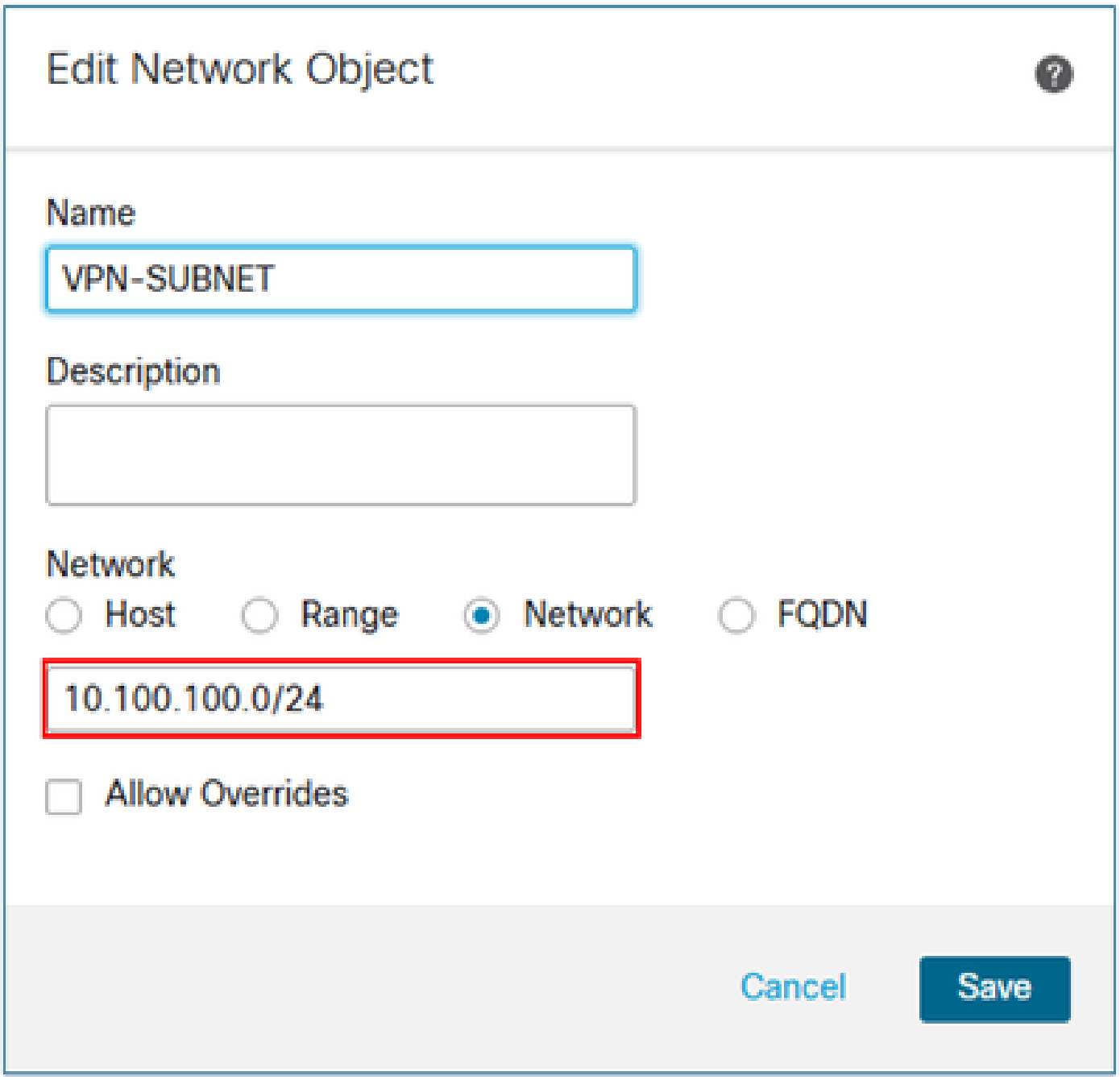
R1 초기 라우팅 테이블:

```
<#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
```

네트워크 명령문을 사용하여 FTD에서 EIGRP를 통해 원격 액세스 VPN 서브넷 재배포

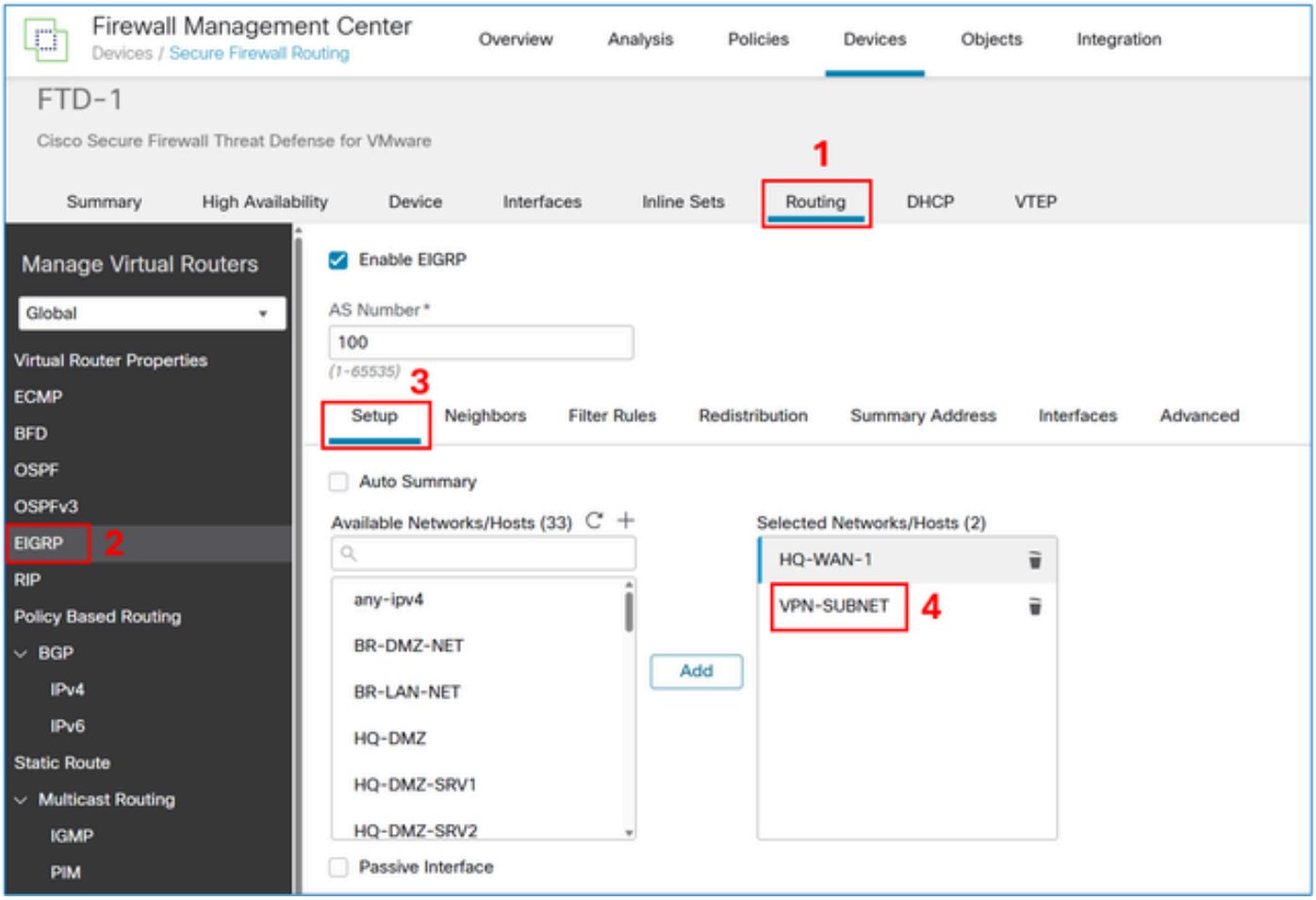
구성

1단계. VPN 서브넷에 대한 네트워크 개체를 만듭니다.



2단계. VPN 서브넷 개체를 network 문에 포함합니다.

FMC 디바이스 관리 UI에서 Routing(라우팅) > EIGRP > Setup(설정)으로 이동하고 선택한 네트워크/호스트에 VPN 서브넷을 포함합니다.



FTD에 컨피그레이션을 저장하고 구축합니다.

다음을 확인합니다.

FTD EIGRP 구성:

```
<#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
```

FTD EIGRP 토폴로지 테이블:

<#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

R1 라우팅 테이블:

<#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

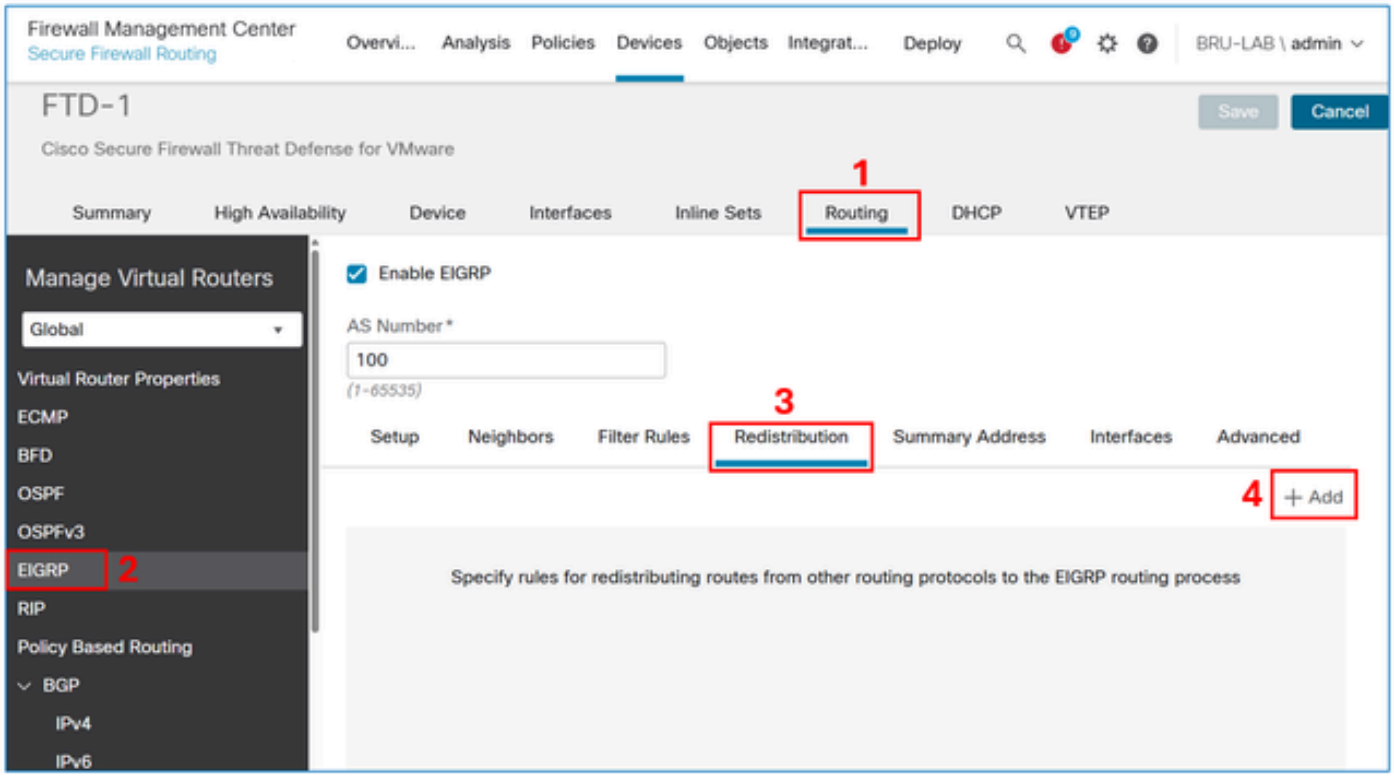
[90/3072] via 192.168.100.2, 00:02:17, GigabitEthernet1

참고: network 문은 10.100.100.0/24이지만 FTD는 EIGRP를 통해 /32 서브넷을 재배포합니다. 이는 FTD가 모든 원격 액세스 VPN 세션에 대해 /32 접두사를 사용하는 고정 경로를 생성하기 때문입니다. 이를 최적화하려면 EIGRP 요약 주소 기능을 사용할 수 있습니다.

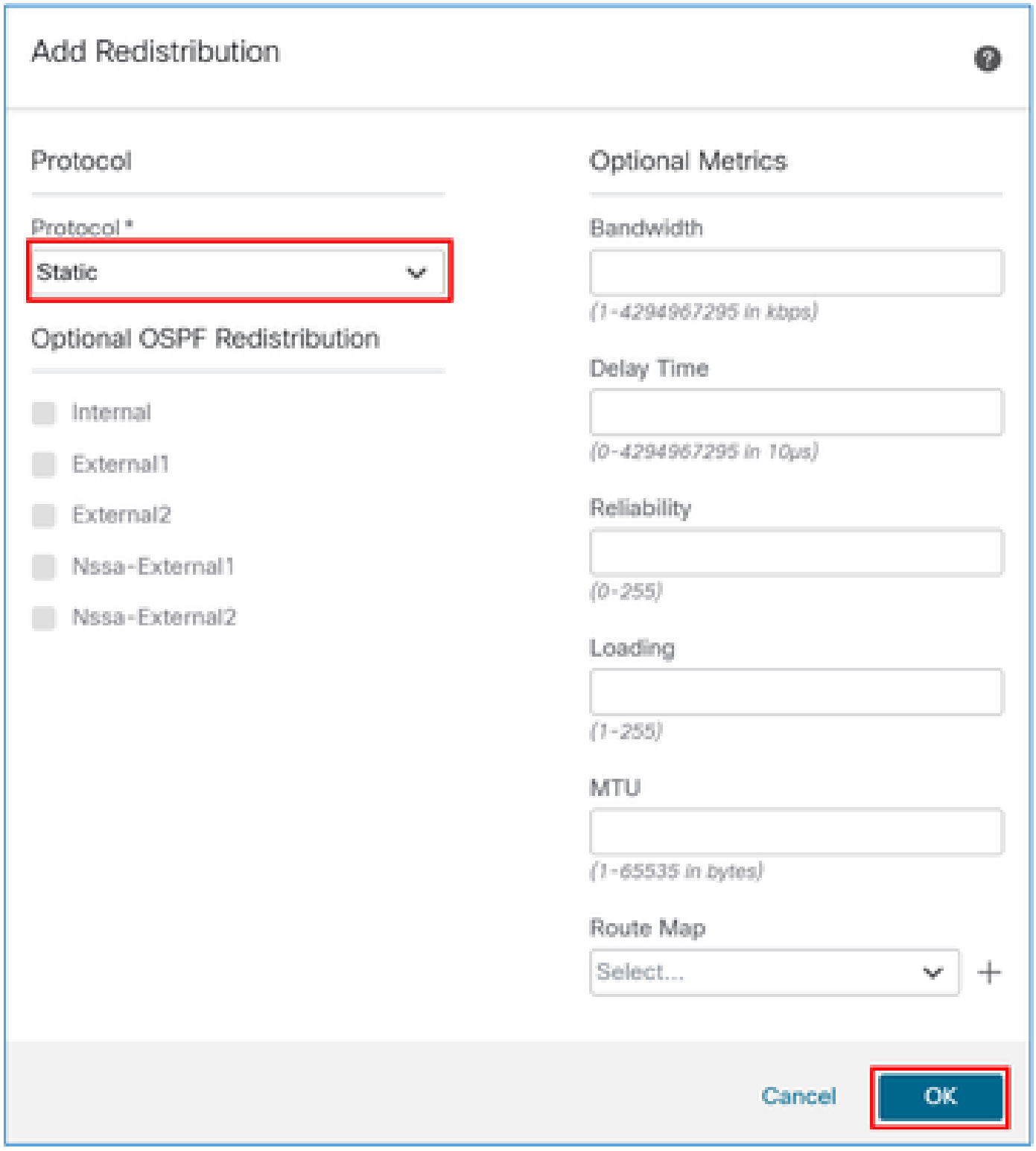
FTD에서 EIGRP를 통해 원격 액세스 VPN 서브넷을 재배포 고정 방식 사용

구성

FMC 디바이스 관리 UI에서 Routing(라우팅) > EIGRP > Redistribution(재배포)으로 이동한 다음 Add(추가) 버튼을 선택합니다.

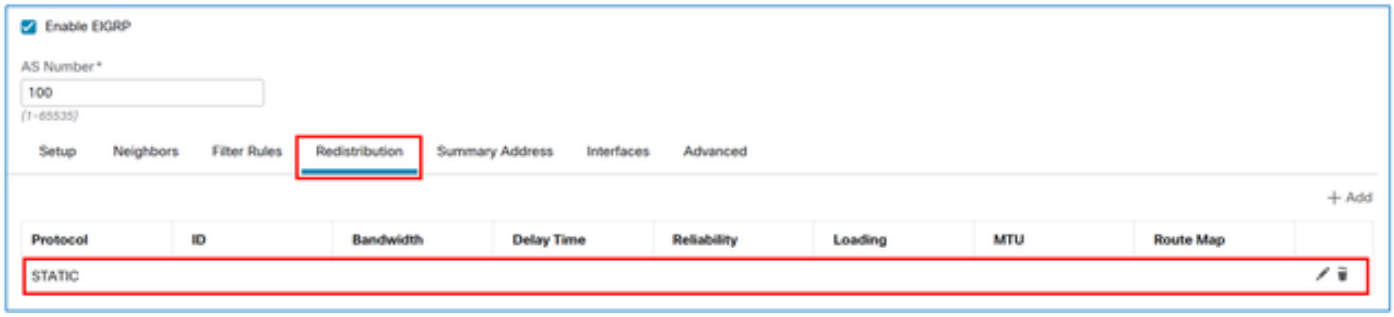


프로토콜 필드에서 Static을 선택한 다음 OK 버튼을 선택합니다.



⚠ 주의: 모든 고정 경로를 EIGRP로 재배포합니다. VPN 서브넷만 광고해야 하는 경우, network statement 접근 방식을 사용하거나 경로 맵을 적용하여 필터링할 수 있습니다.

결과:



FTD에 컨피그레이션을 저장하고 구축합니다.

다음을 확인합니다.

FTD EIGRP 구성:

<#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

FTD EIGRP 토폴로지 테이블:

<#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
```

R1 라우팅 테이블:

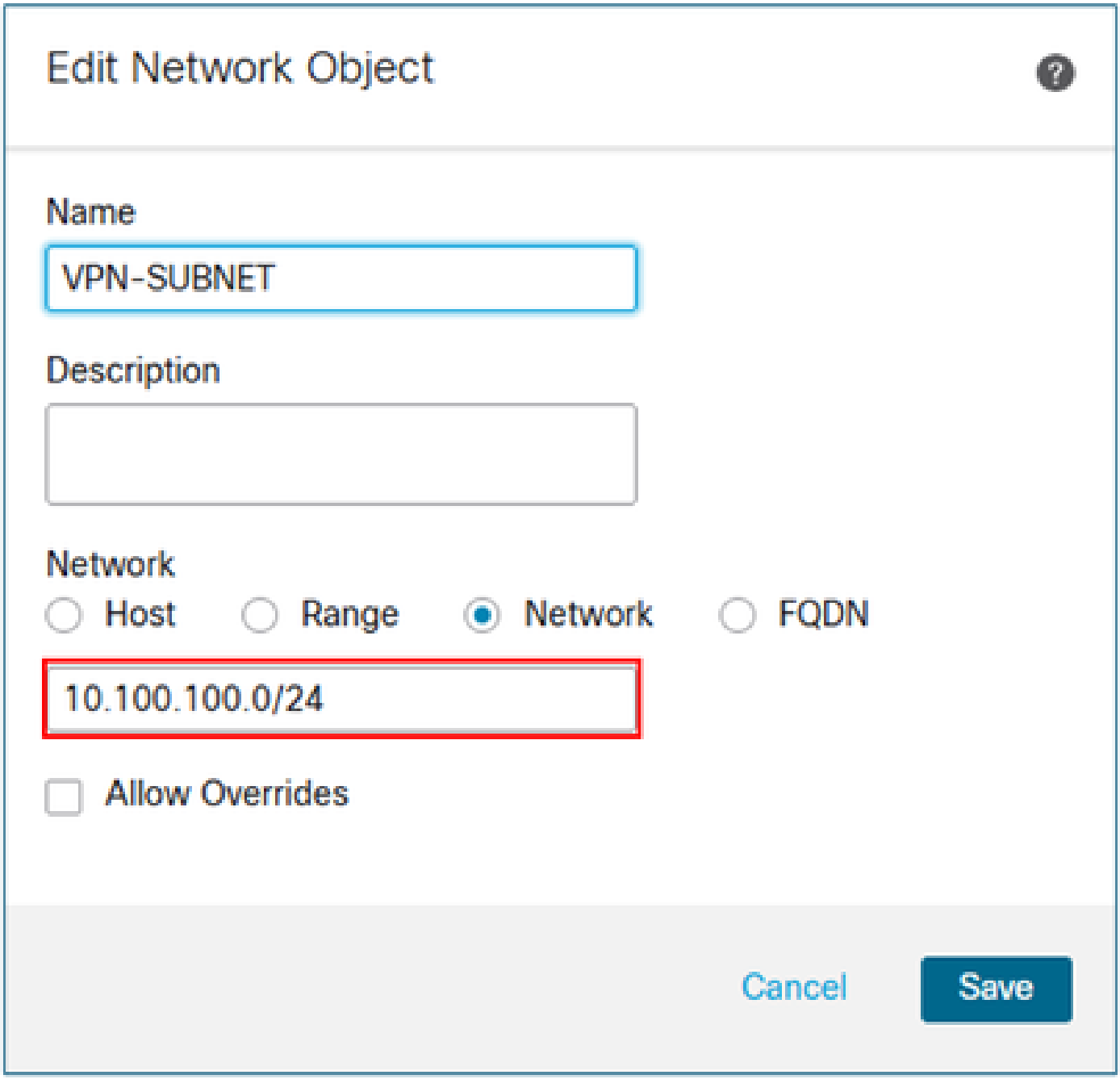
```
<#root>

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
```

팁: 선택적으로, FTD에서 EIGRP 요약 주소 기능을 사용하여 라우팅 테이블의 크기를 최적화할 수 있습니다.

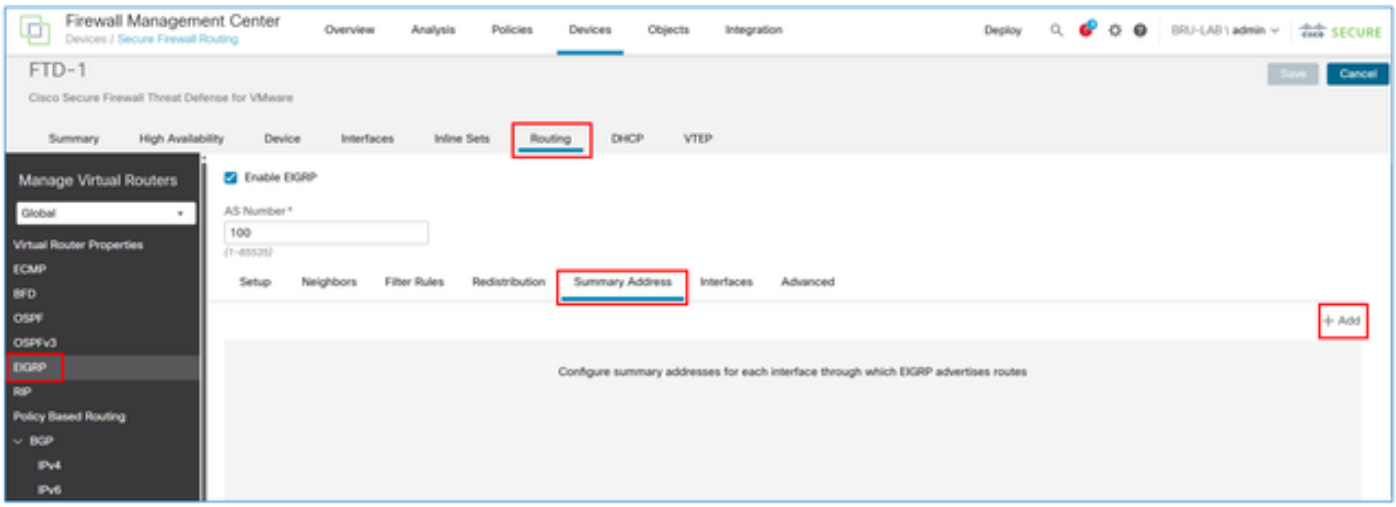
EIGRP 요약 주소 컨피그레이션

구성

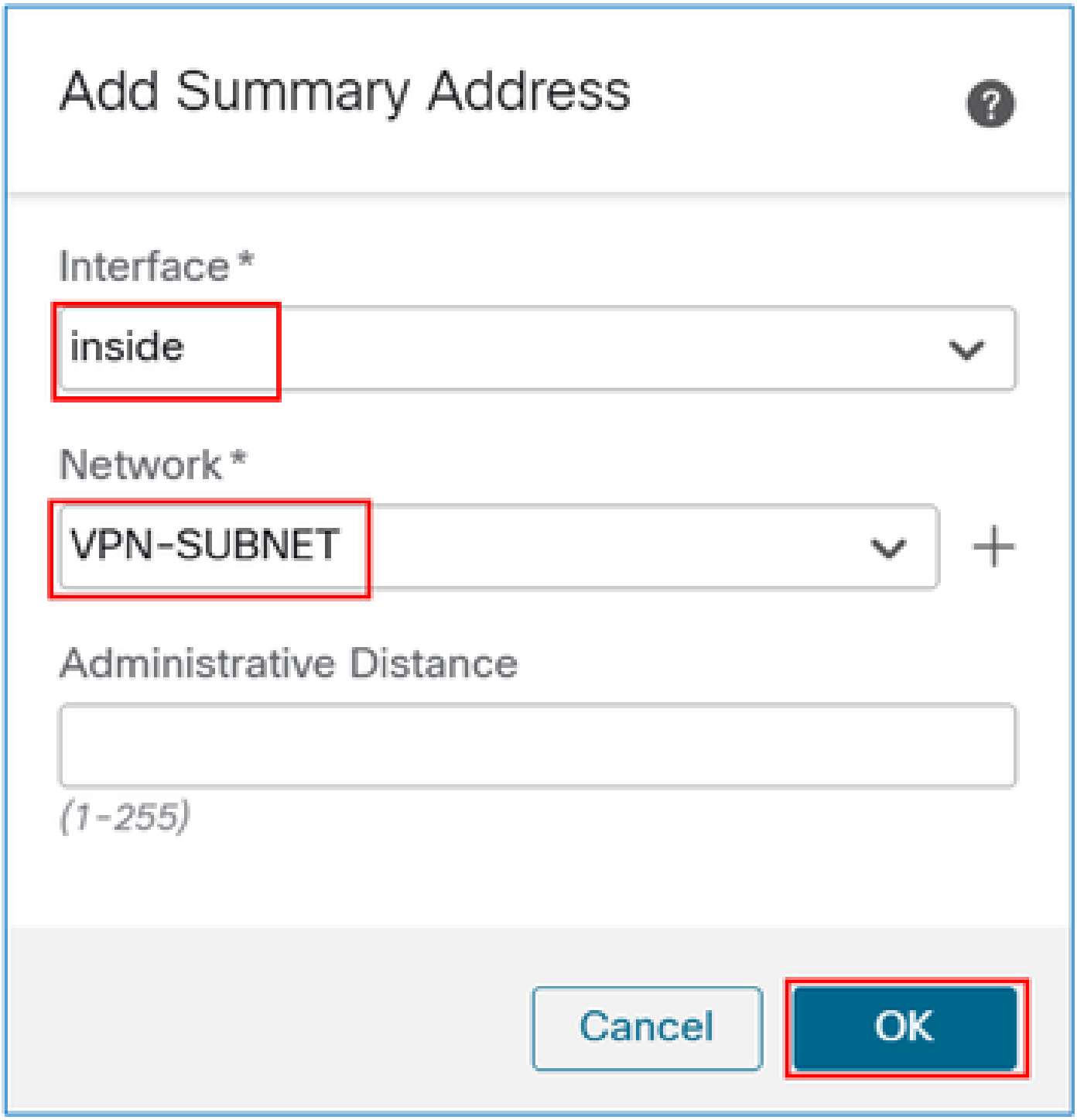
아직 생성하지 않은 경우 VPN 서브넷에 대한 네트워크 객체를 생성합니다.



FMC 디바이스 관리 UI에서 Routing(라우팅) > EIGRP > Summary Address(요약 주소)로 이동한 다음 Add(추가) 버튼을 선택합니다.



interface 필드에 EIGRP 인접 디바이스와 마주하는 를 입력하고 network 필드에 VPN 서브넷을 위해 생성된 객체를 입력합니다.


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

결과:

다음을 확인합니다.

FTD EIGRP 요약 주소 구성:

<#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

FTD EIGRP 토폴로지 테이블:

<#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

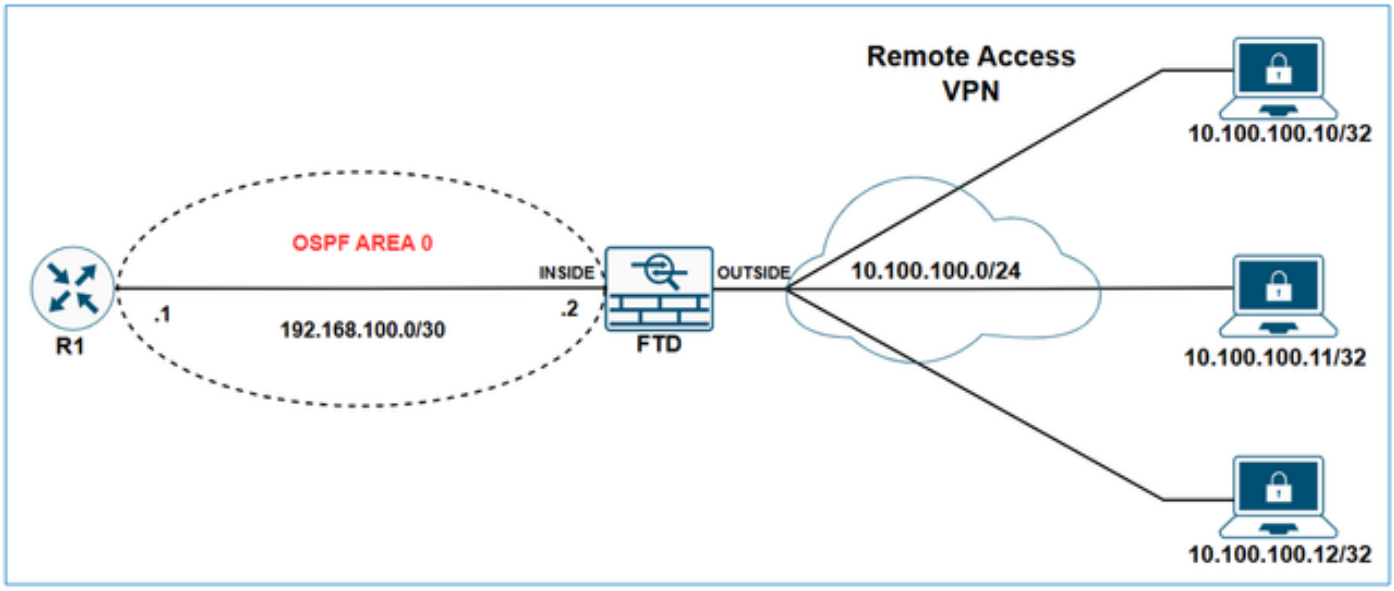
```
        via Summary (512/0), Null0


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

R1 라우팅 테이블:

```
<#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
```

FTD의 OSPF를 통해 원격 액세스 VPN 서브넷 재배포

네트워크 다이어그램



초기 컨피그레이션

<#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 출력:

<#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 출력:

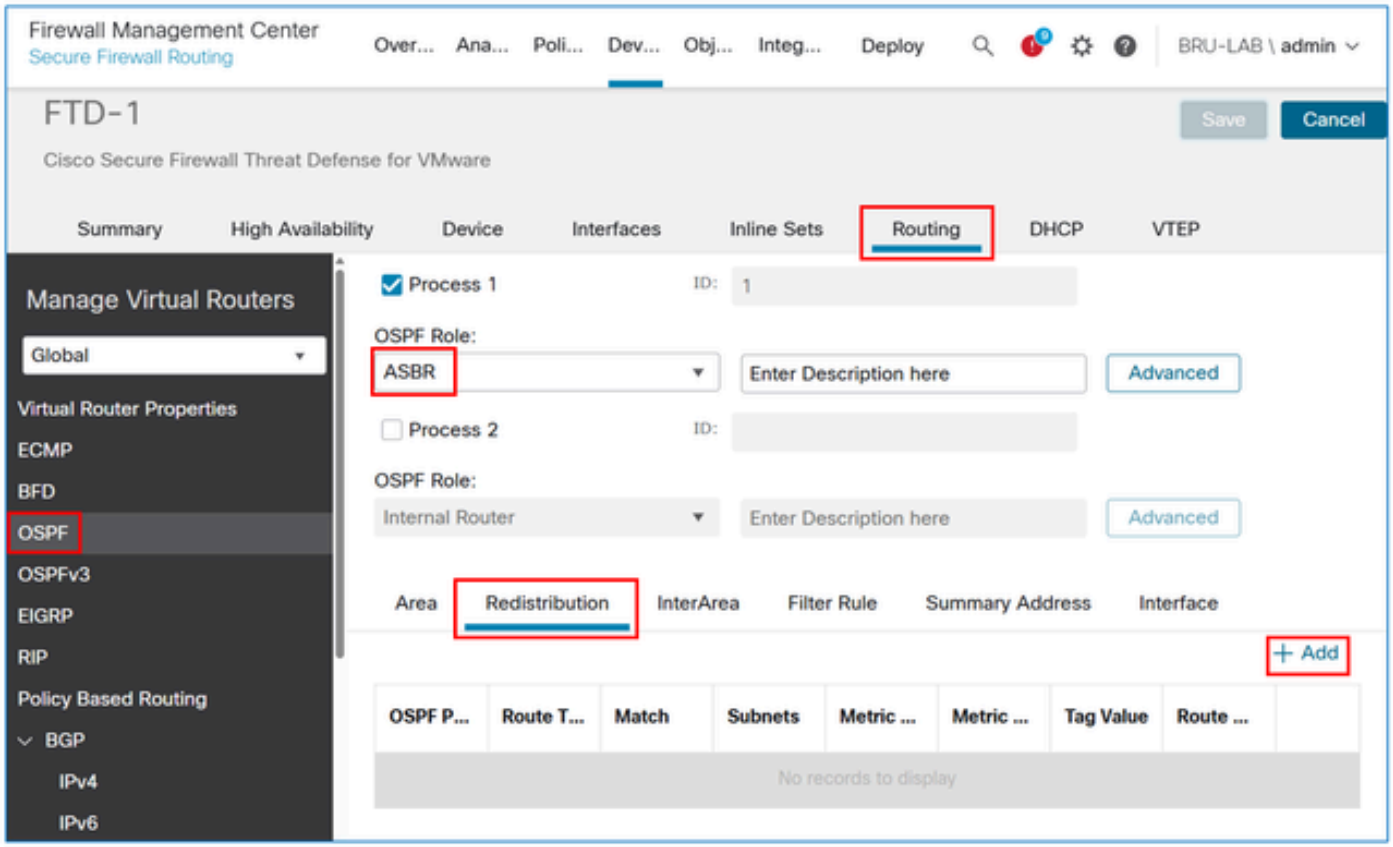
```
<#root>

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
```

R1 라우팅 테이블:

```
<#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
```

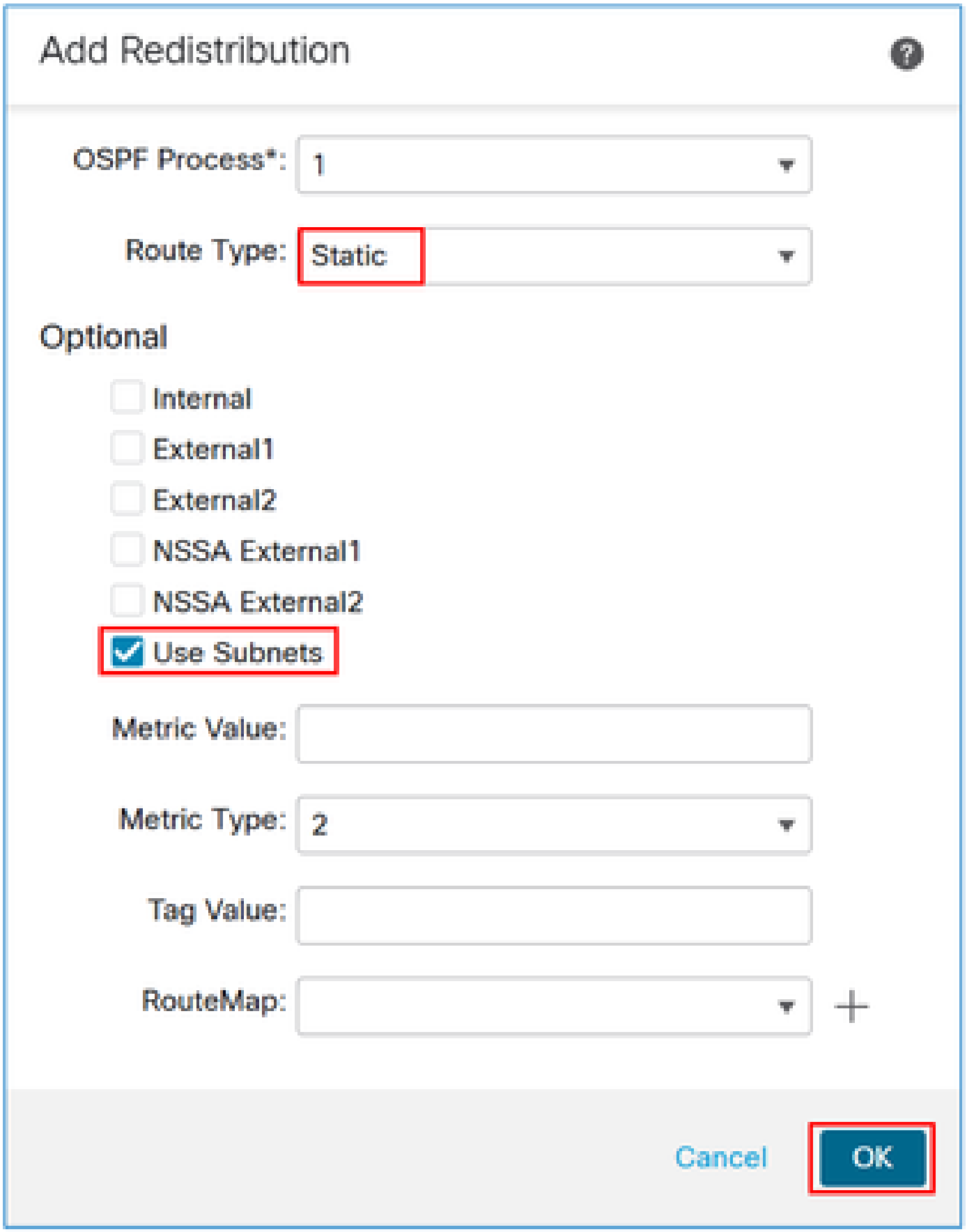
구성

FMC 디바이스 관리 UI에서 Routing(라우팅) > OSPF > Redistribution(재배포)으로 이동한 다음 Add(추가) 버튼을 선택합니다.



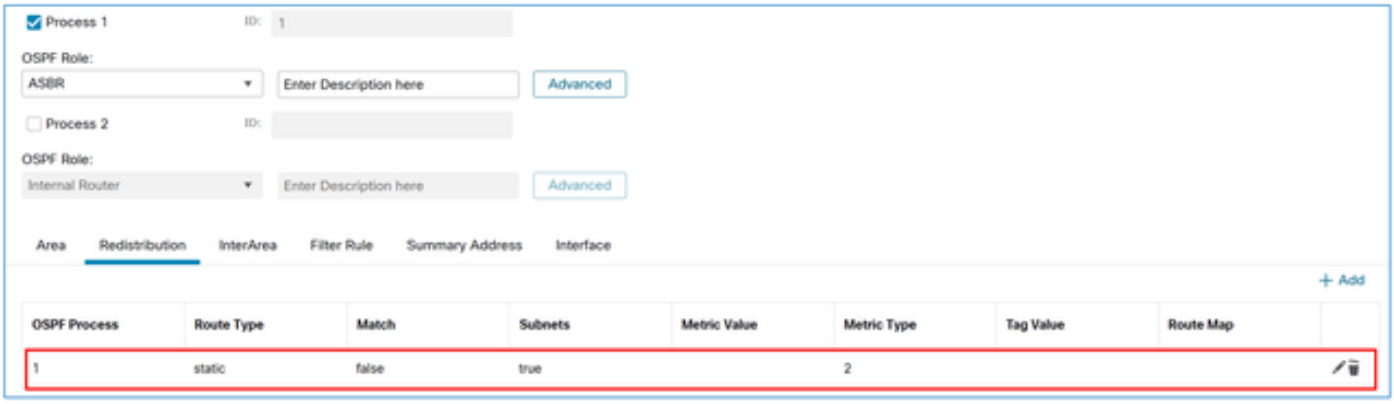
참고: 재배포를 활성화하려면 OSPF 역할을 ASBR 또는 ABR & ASBR로 설정해야 합니다.

Route Type(경로 유형) 필드에서 Static(정적)을 선택한 다음 Use Subnets(서브넷 사용) 상자를 선택합니다.



⚠ 주의: 모든 고정 경로를 OSPF에 재배포합니다. VPN 서브넷만 광고해야 하는 경우 경로 맵을 적용하여 필터링할 수 있습니다.

결과:



다음을 확인합니다.

FTD OSPF 재배포 구성:

```
<#root>

FTD-1#

sh run router


router ospf 1
 network 192.168.100.0 255.255.255.252 area 0

 redistribute static subnets
```

R1 라우팅 테이블:

```
<#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
```

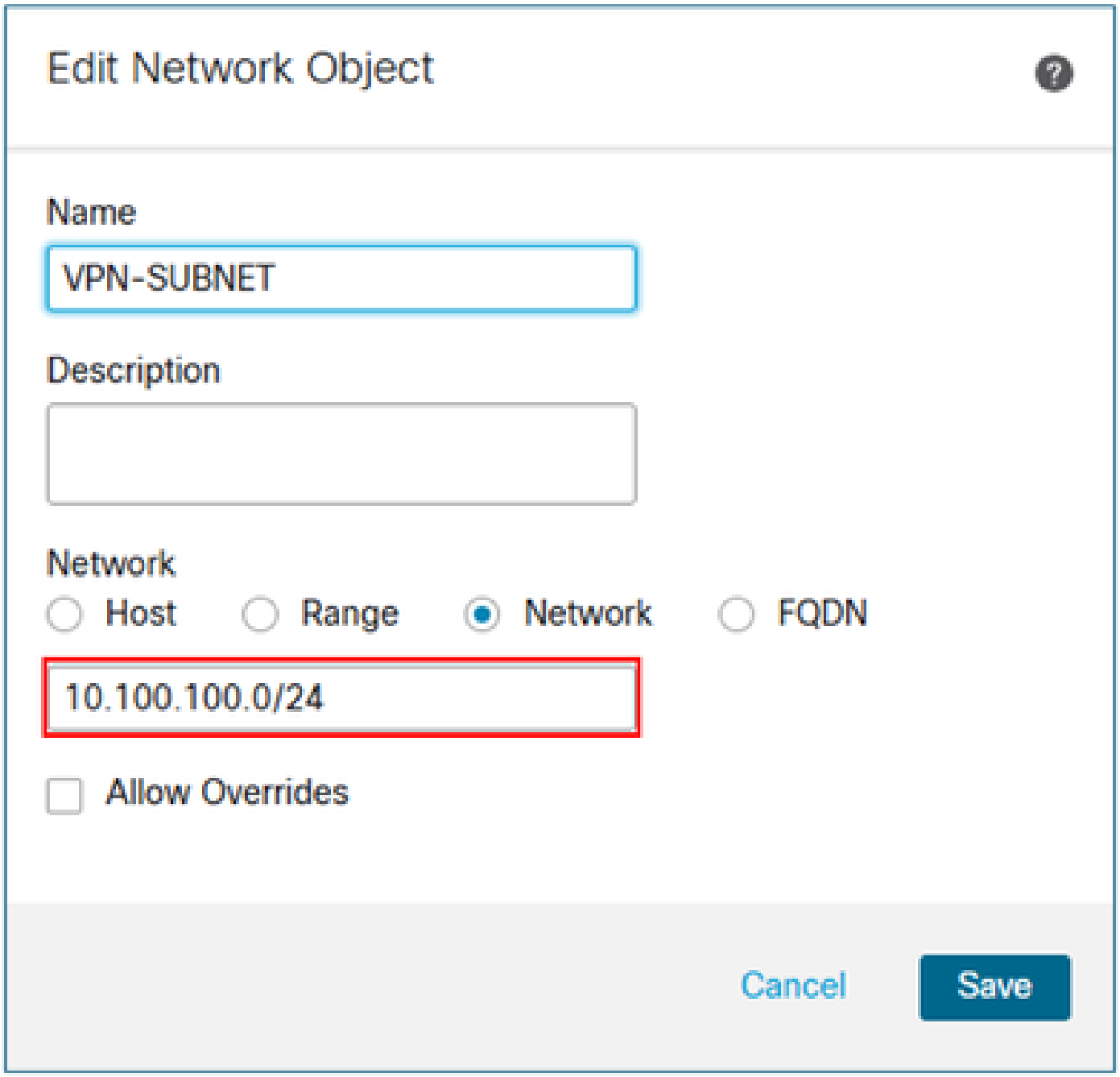
`O E2     10.100.100.10 [110/20] via 192.168.100.2, 00:08:01, GigabitEthernet1`

팁: VPN 풀이 10.100.100.0/24이지만 FTD는 OSPF를 통해 /32 서브넷을 재배포합니다. 이는 FTD가 모든 원격 액세스 VPN 세션에 대해 /32 접두사를 사용하는 고정 경로를 생성하기 때문입니다. 이를 최적화하려면 OSPF Summary Address 기능을 사용할 수 있습니다.

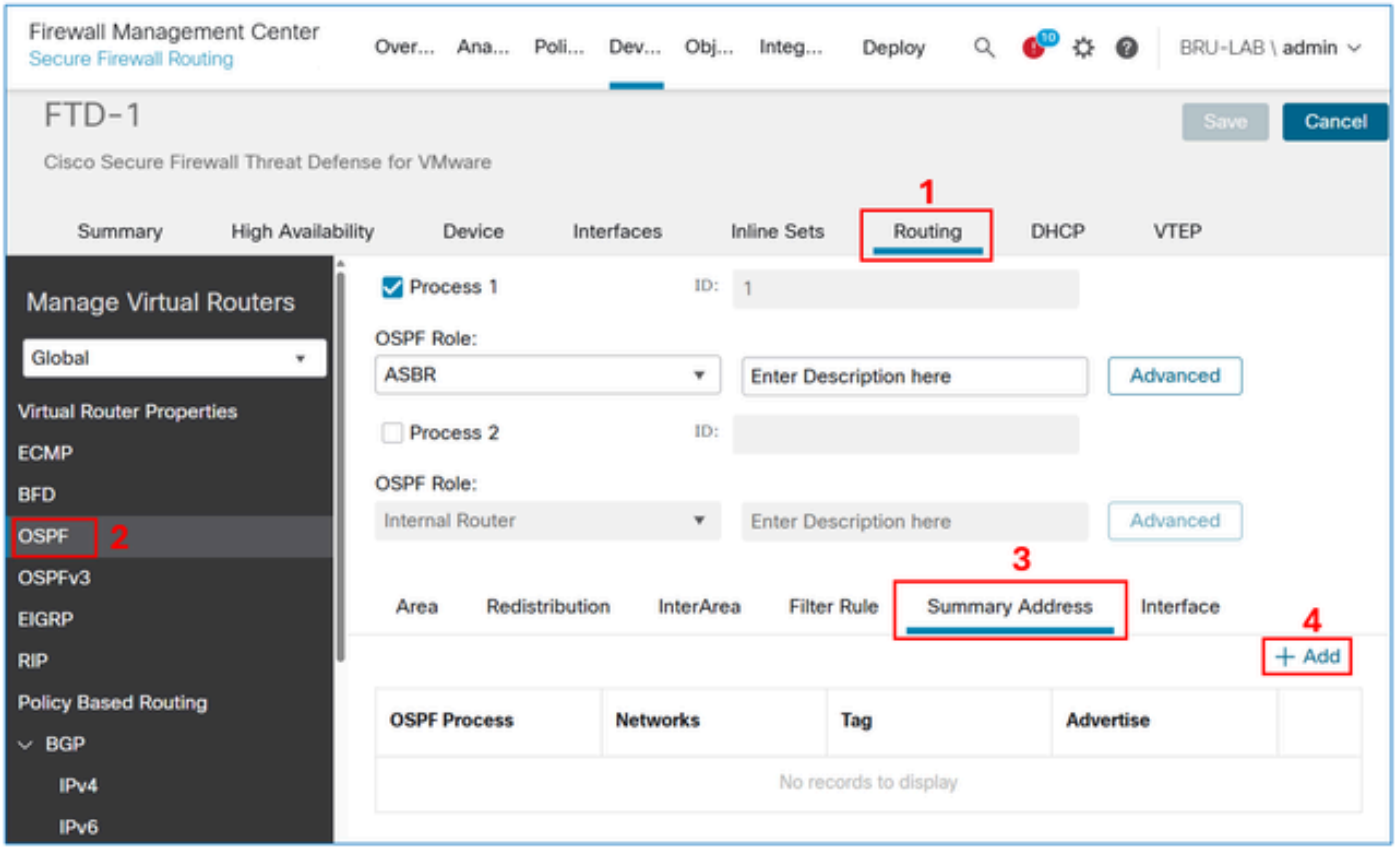
OSPF 요약 주소 컨피그레이션

구성

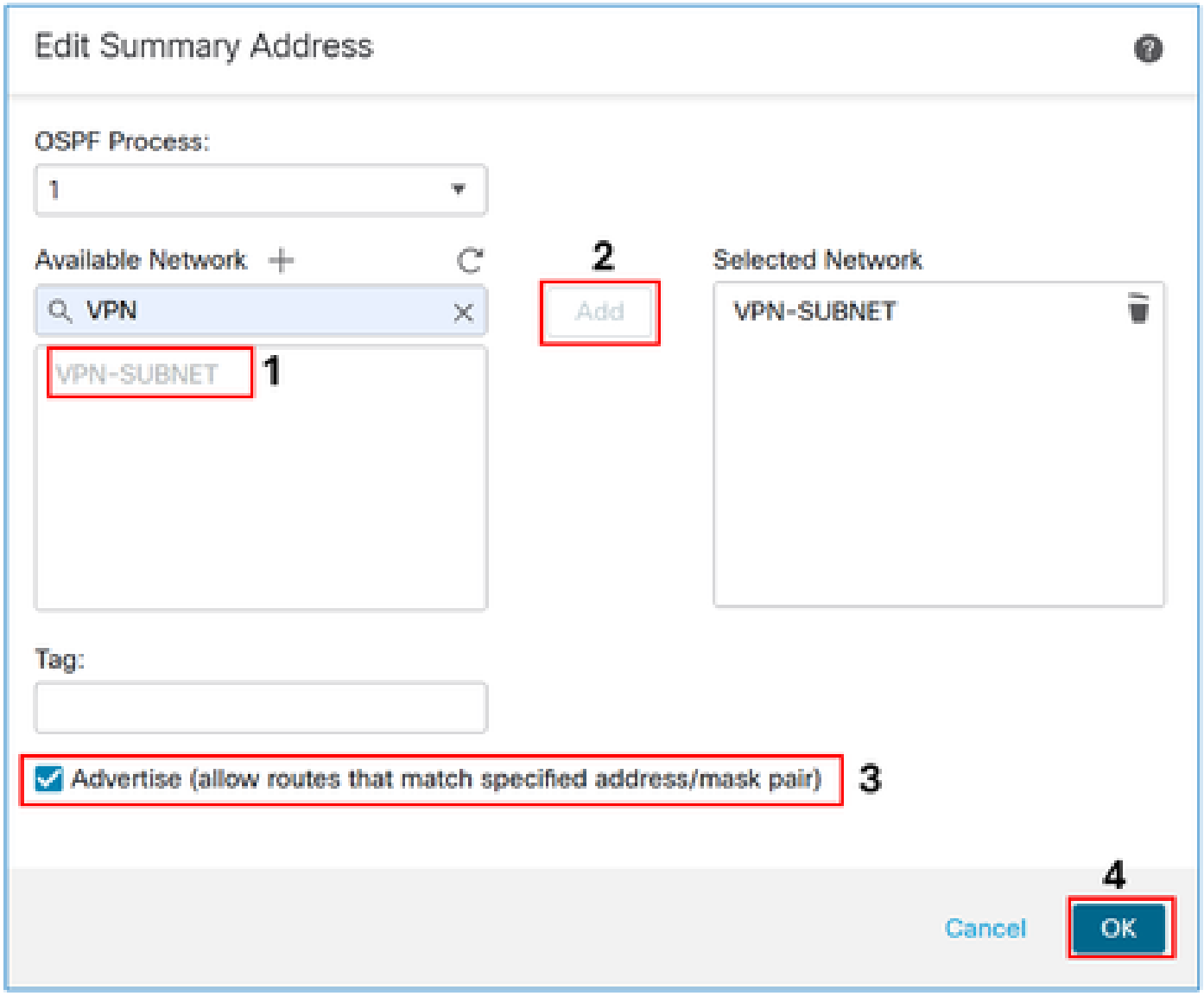
아직 생성하지 않은 경우 VPN 서브넷에 대한 네트워크 객체를 생성합니다.



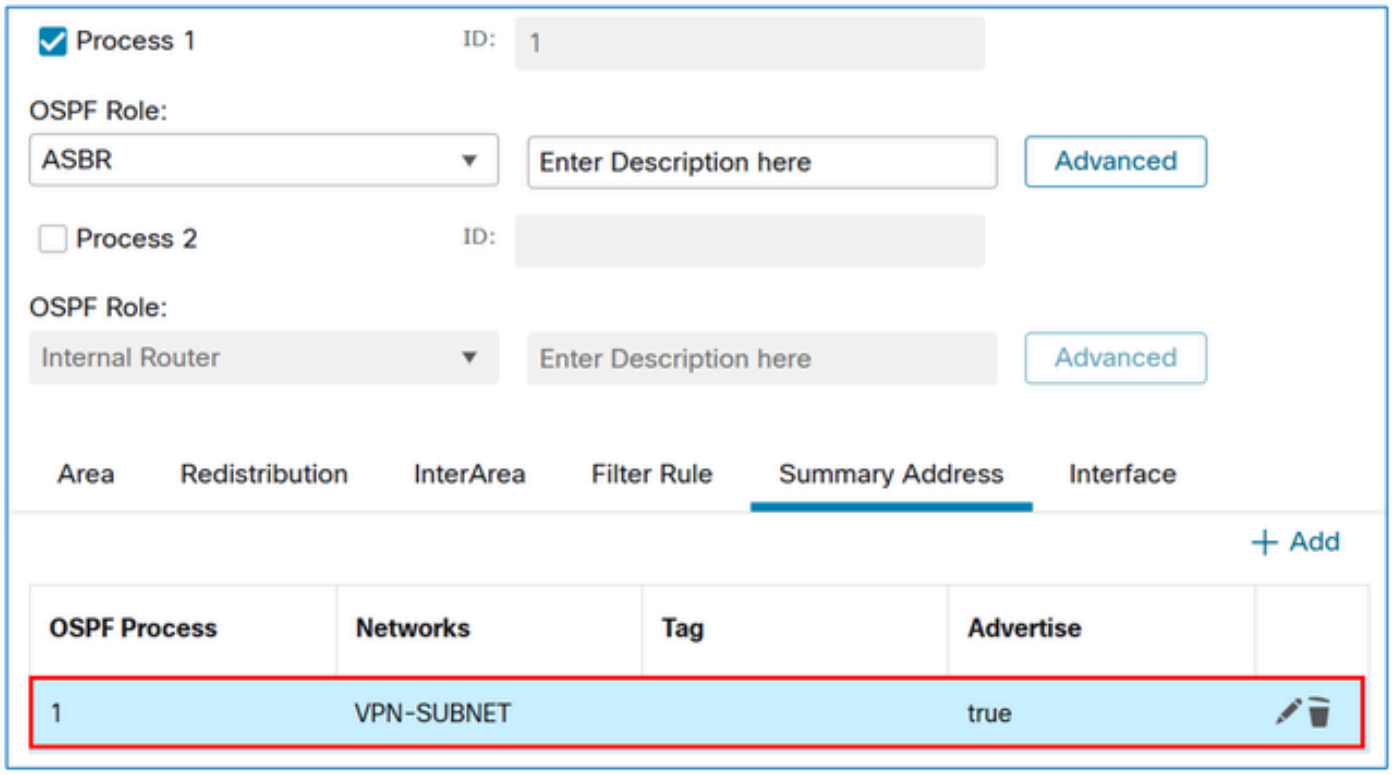
FMC 디바이스 관리 UI에서 Routing(라우팅) > OSPF > Summary Address(요약 주소)로 이동한 다음 Add(추가) 버튼을 선택합니다.



VPN 서브넷 개체를 추가하고 Advertise(알림) 확인란을 선택합니다.


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

결과:



다음을 확인합니다.

FTD OSPF 구성:

<#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

R1 라우팅 테이블:

<#root>

R1#

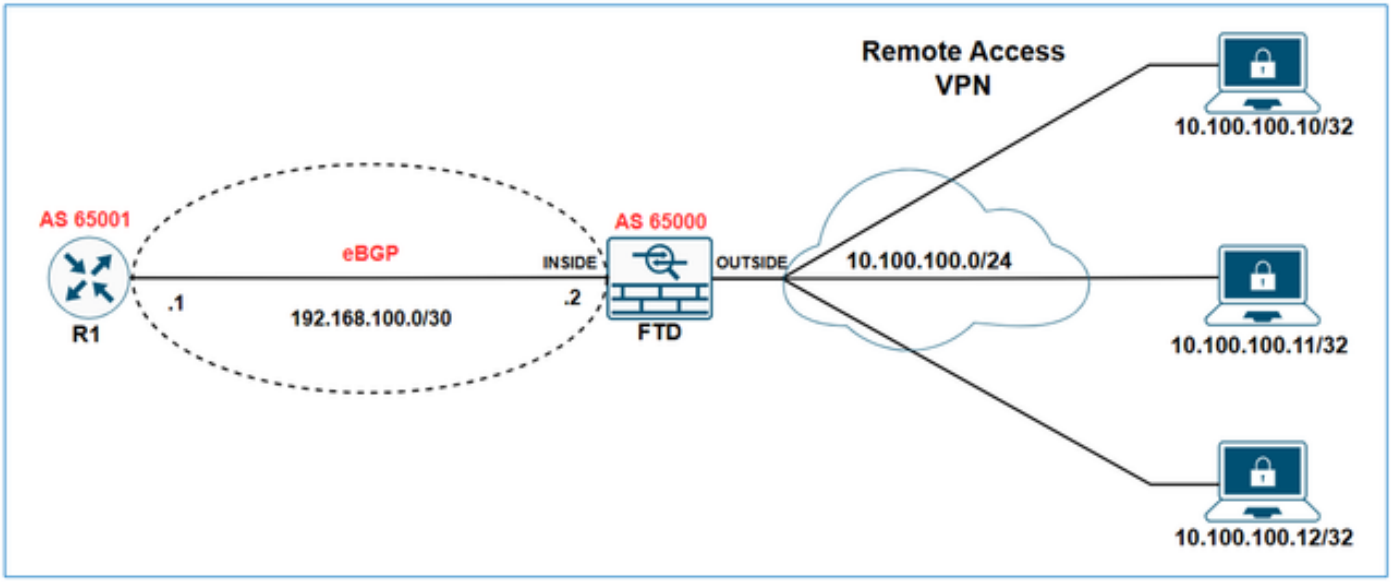
sh ip route

```
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
```

FTD의 eBGP를 통해 원격 액세스 VPN 서브넷 재배포

네트워크 다이어그램



이 예에서 목표는 R1이 eBGP를 통해 VPN 서브넷 10.100.100.0/24을 학습하도록 하는 것입니다.

초기 컨피그레이션

FTD 초기 구성:

```
<#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
```

FTD bgp 테이블 출력:

<#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 출력:

<#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 출력:

<#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
```

R1 bgp 테이블 출력:

<#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 ?
```

R1 라우팅 테이블:

<#root>

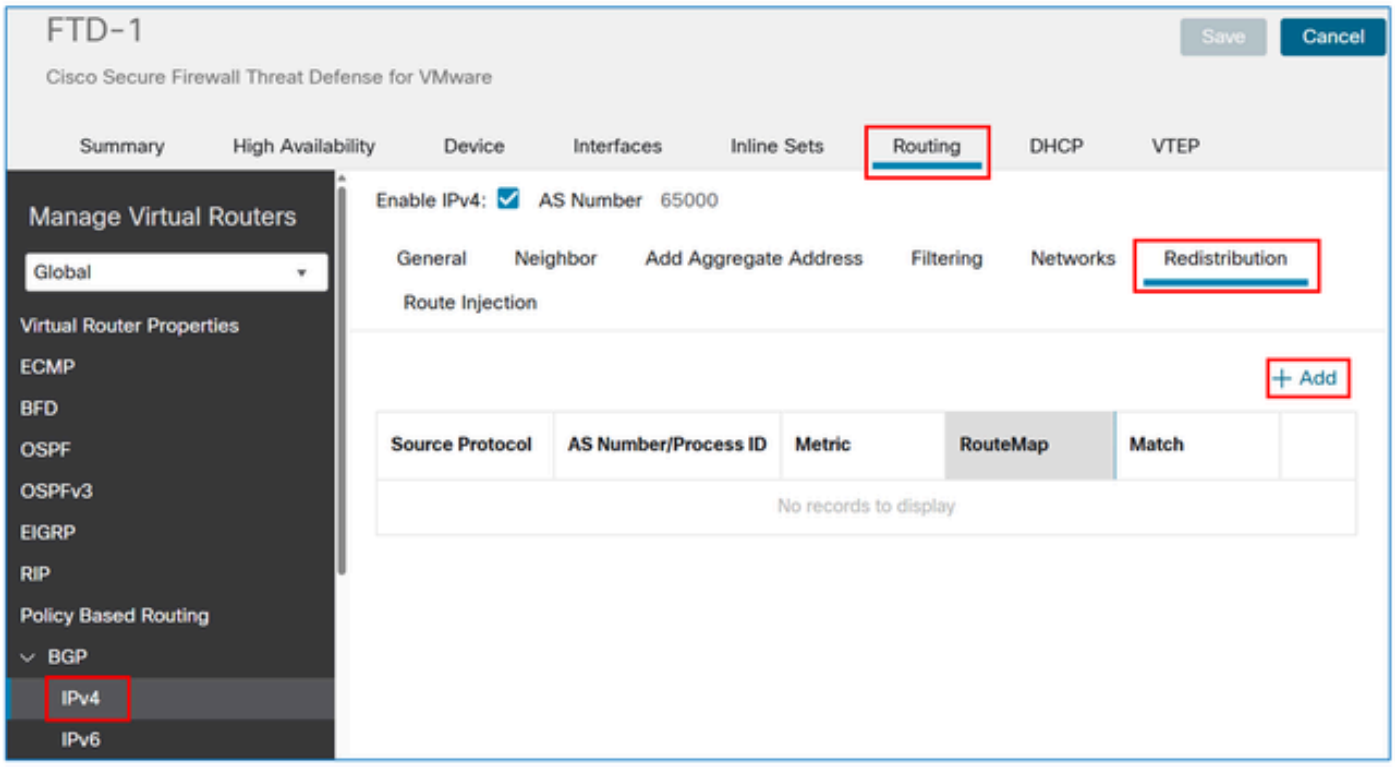
R1#

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
```

구성

FMC 디바이스 관리 UI에서 Routing(라우팅) > BGP > IPv4 > Redistribution(재배포)으로 이동한 다음 Add(추가) 버튼을 선택합니다.



Source Protocol 필드에서 Static을 선택한 다음 OK 버튼을 선택합니다.

Add Redistribution

Source Protocol

Static

Process ID*

Metric

(0-4294967295)

Route Map

Match

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.