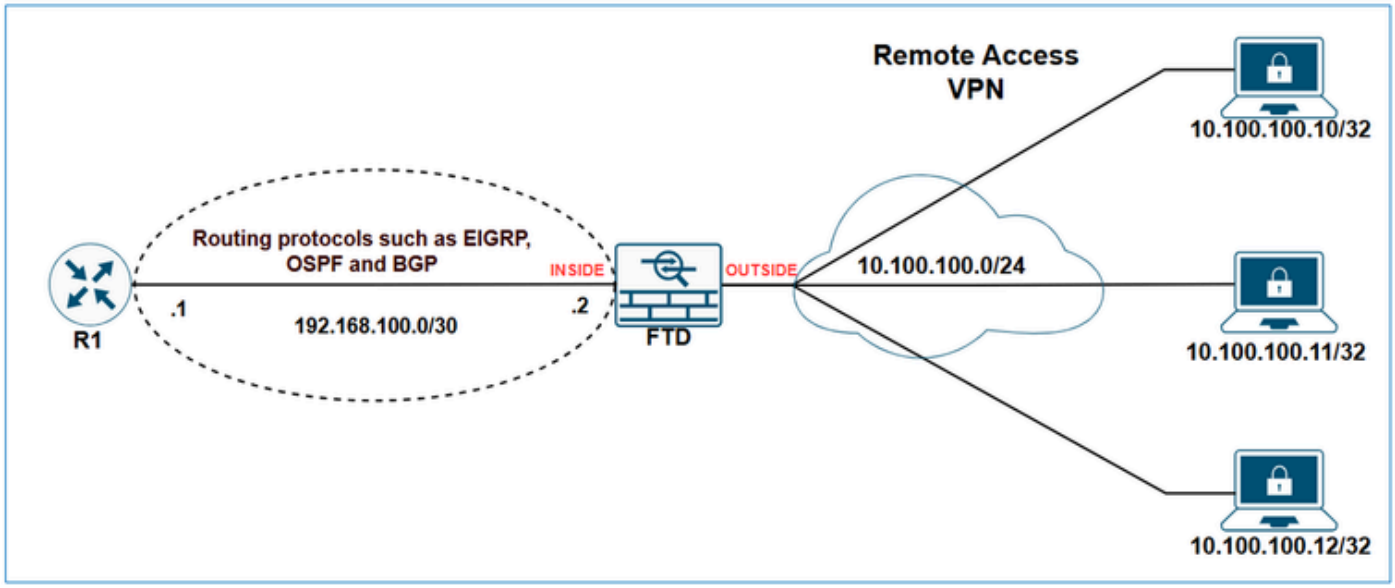
Ankündigung von VPN-Subnetzen für Remote-Zugriff über Routing-Protokolle in FTD

Inhalt

Einleitung

In diesem Dokument werden die verfügbaren Optionen für die Ankündigung VPN-bezogener Subnetze unter Verwendung der Routing-Protokolle EIGRP, OSPF und BGP beschrieben.



Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Anmerkung: In diesem Dokument wird die Konfiguration für die Neuverteilung von Remote Access-VPN-Subnetzen über EIGRP, OSPF und BGP mithilfe des FMC beschrieben. Hinweise zur Routen-Neuverteilung mit FDM finden Sie im FDM-Konfigurationsleitfaden.

Hintergrundinformationen

Zunächst muss ermittelt werden, wie die FTD VPN-Subnetze in ihrer Routing-Tabelle klassifiziert. Obwohl diese Subnetze durch VPN verbunden erscheinen, gelten sie nicht als direkt verbundene Subnetze; Stattdessen werden sie als statische Routen behandelt.

Die Ausgabe von show veranschaulicht dies.

FTD Routen-Ausgabe anzeigen:

<#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 zeigt die Ausgabe für verbundene Routen an:

<#root>

```
FTD-1#
```

show route connected

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

Gateway of last resort is not set

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

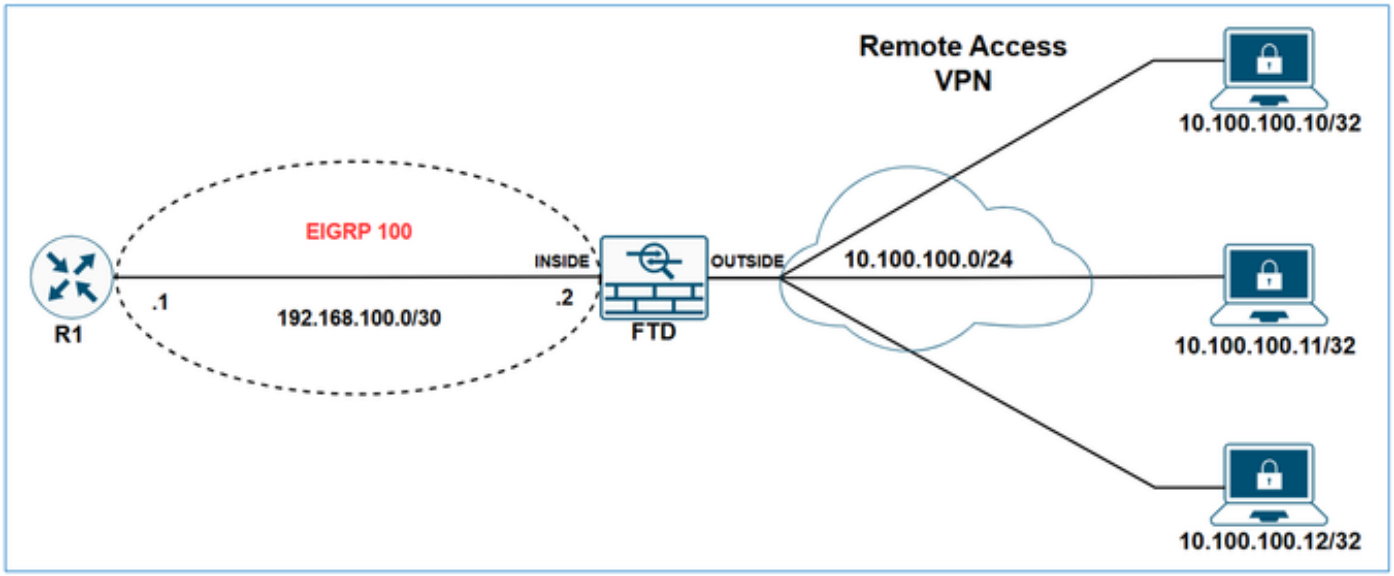
FTD zeigt statische Routenausgabe an:

```
<#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
```

Nachdem nun klar ist, wie VPN-Subnetze in der Routing-Tabelle der Firewall behandelt werden, besteht der nächste Schritt darin, zu prüfen, wie sie mithilfe verschiedener Routing-Protokolle angekündigt werden können.

Verteilung von Remote Access-VPN-Subnetzen über EIGRP auf FTD

Netzwerkdiagramm



Statische Routen, die in den Anwendungsbereich einer Netzwerkanweisung fallen, werden automatisch an EIGRP weitergeleitet. müssen Sie für diese keine Umverteilungsregel definieren. Wenn Sie jedoch statische Routen, die auf VTI-Schnittstellen in EIGRP verweisen, neu verteilen, müssen Sie die Kennzahl angeben. Bei statischen Routen, die auf andere Schnittstellentypen verweisen, ist die Angabe der Metrik nicht erforderlich.

Aufgrund des Verhaltens von EIGRP, statische Routen, die in den Anwendungsbereich der Netzwerkanweisungen fallen, automatisch neu zu verteilen, gibt es zwei Möglichkeiten, VPN-Subnetze über EIGRP auf FTD anzukündigen:

1. Verwenden einer Netzwerkanweisung.
2. Verwenden des statischen Redistribution-Ansatzes.

In diesem Beispiel soll R1 dazu gebracht werden, das VPN-Subnetz 10.100.100.0/24 über EIGRP zu erlernen.

FTD-Erstkonfiguration:

<#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 Initial Routing Table:

<#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 Initial EIGRP Topologietabelle:

<#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 Erstroutingtabelle:

<#root>

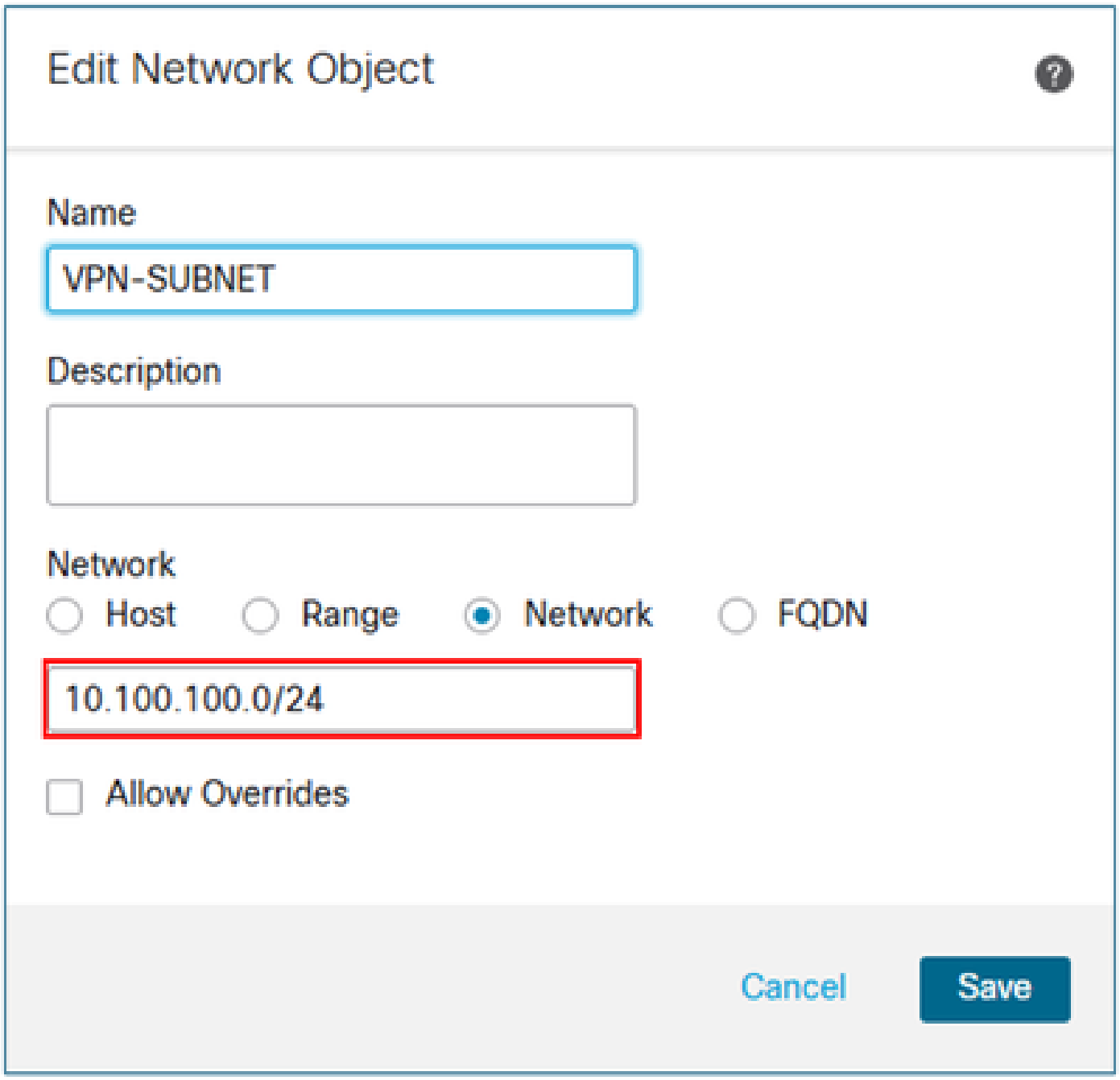
```
R1#

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
```

Verteilung von Remote Access-VPN-Subnetzen über EIGRP auf FTD unter Verwendung der Netzwerkanweisung

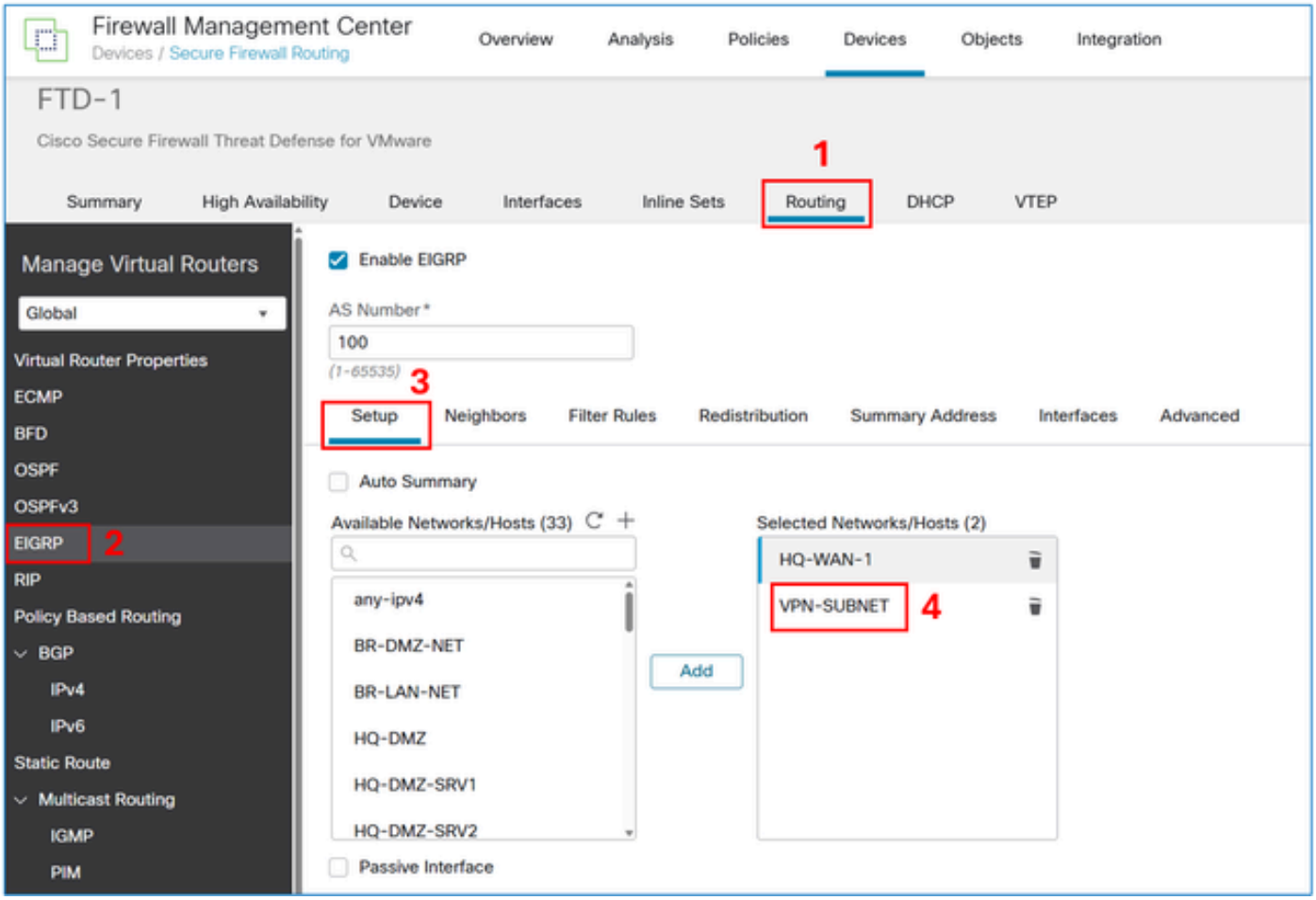
Konfigurieren

Schritt 1: Erstellen Sie ein Netzwerkobjekt für das VPN-Subnetz.



Schritt 2: Integrieren Sie das VPN-Subnetzobjekt in der Netzwerkanweisung.

Navigieren Sie in der Benutzeroberfläche für das FMC-Gerätemanagement zu Routing > EIGRP > Setup, und fügen Sie das VPN-Subnetz in die ausgewählten Netzwerke/Hosts ein.



Speichern und Bereitstellen der Konfiguration auf dem FTD

Überprüfung

FTD EIGRP-Konfiguration:

<#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-Topologietabelle:

<#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-Routing-Tabelle:

<#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

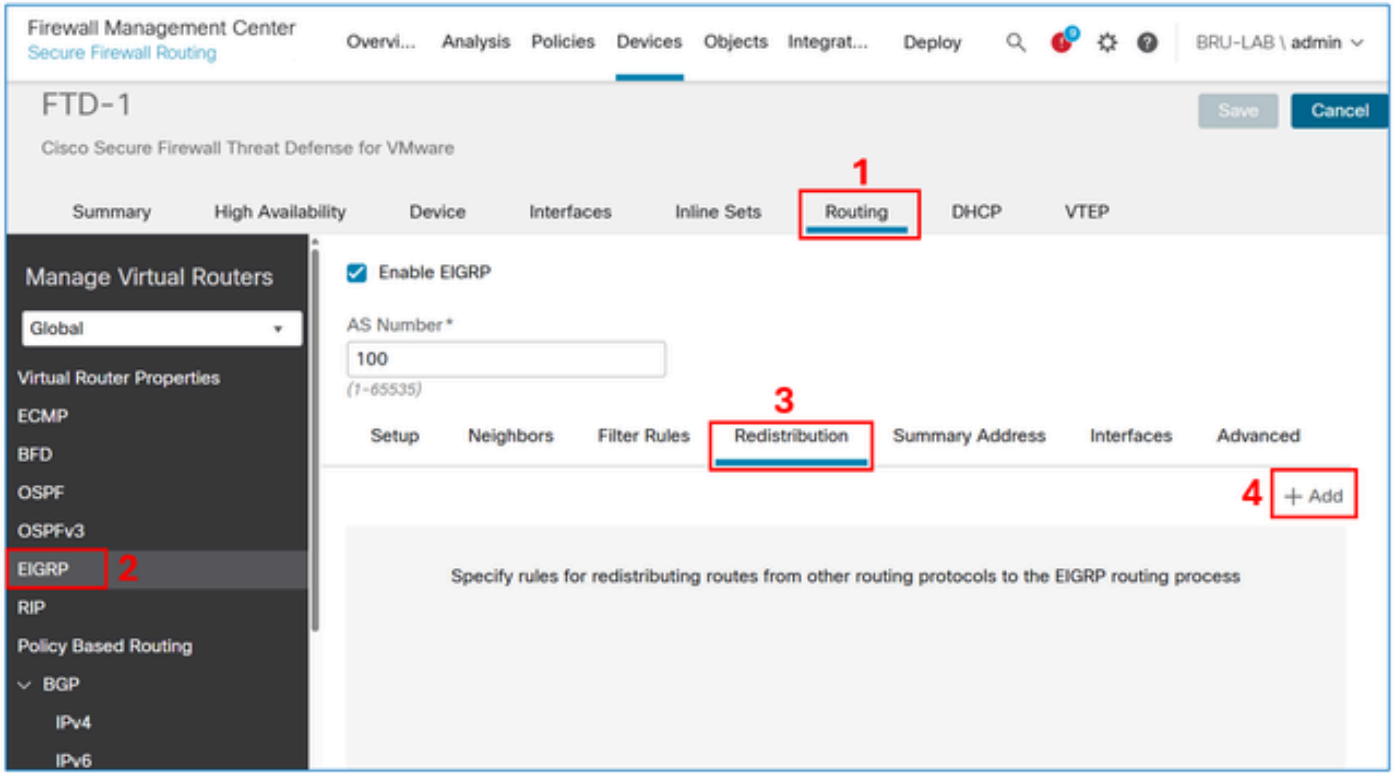
[90/3072] via 192.168.100.2, 00:02:17, GigabitEthernet1

Anmerkung: Beachten Sie, dass die FTD ein /32-Subnetz über EIGRP verteilt, obwohl die Netzwerk-Anweisung 10.100.100.0/24 lautete. Dies liegt daran, dass die FTD für jede Remotezugriff-VPN-Sitzung eine statische Route mit einem /32-Präfix erstellt. Um dies zu optimieren, können Sie die Funktion "EIGRP Summary Address" (EIGRP-Zusammenfassungsadresse) verwenden.

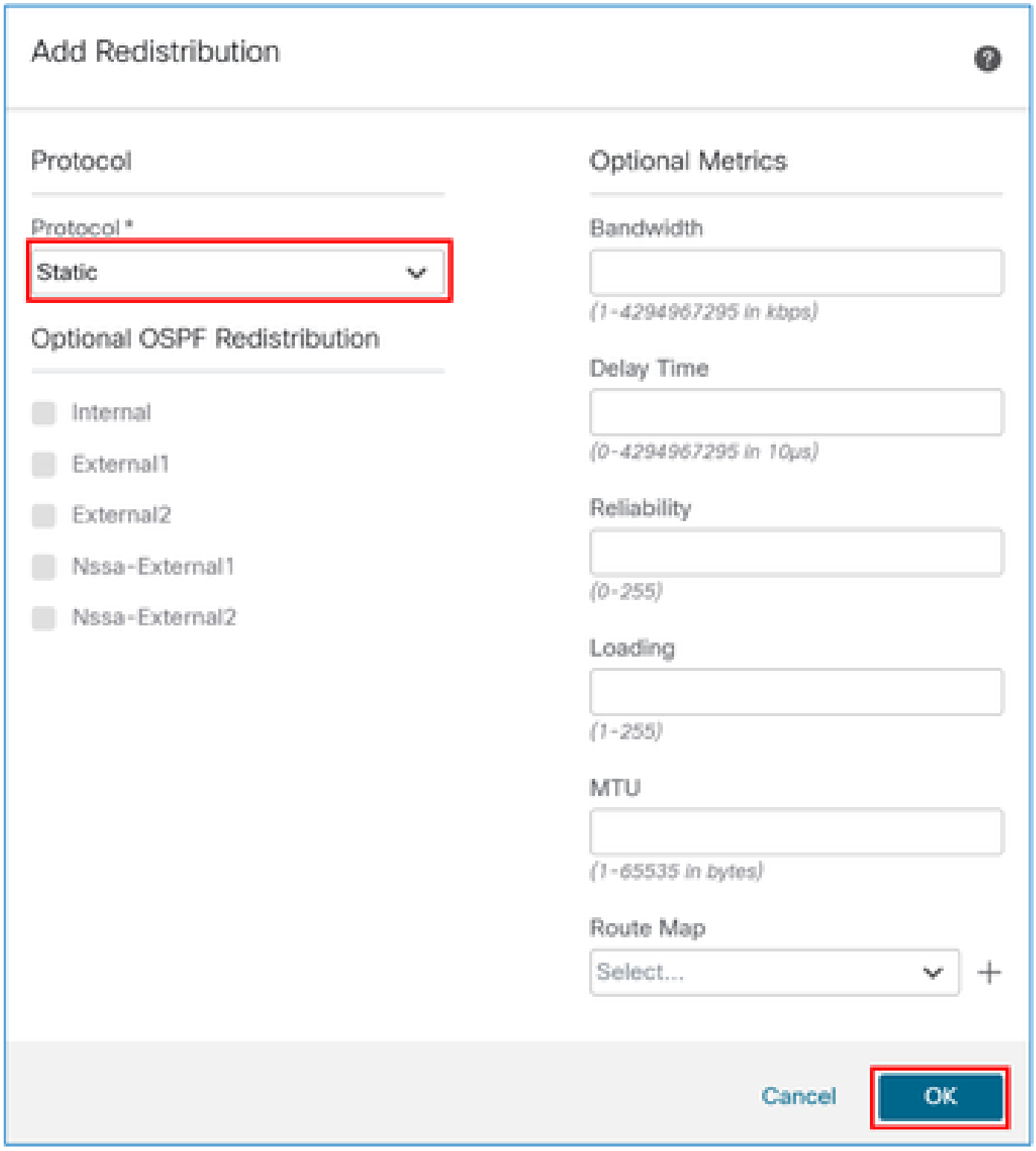
Neuverteilung von Remote Access-VPN-Subnetzen über EIGRP auf FTD mithilfe des statischen Neuverteilungsansatzes

Konfigurieren

Navigieren Sie in der Benutzeroberfläche für das FMC-Gerätemanagement zu Routing > EIGRP > Redistribution, und wählen Sie dann die Schaltfläche Hinzufügen aus.

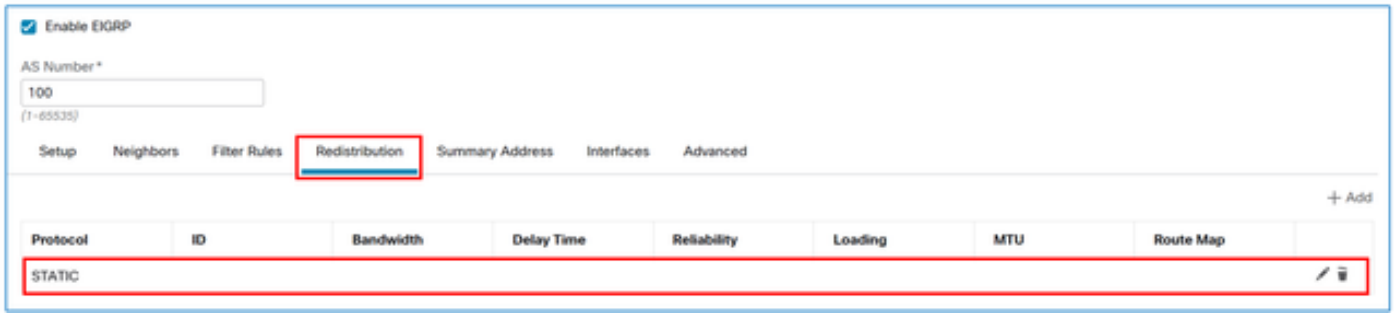


Wählen Sie im Protokollfeld die Option Statisch aus, und klicken Sie dann auf die Schaltfläche OK.



⚠ Vorsicht: Dadurch werden alle statischen Routen auf EIGRP umverteilt. Wenn Sie nur die VPN-Subnetze ankündigen müssen, können Sie entweder den Network Statement-Ansatz verwenden oder eine Routing-Map anwenden, um sie zu filtern.

Ergebnis:



Speichern und Bereitstellen der Konfiguration auf dem FTD

Überprüfung

FTD EIGRP-Konfiguration:

<#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-Topologietabelle:

<#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-Routing-Tabelle:

<#root>

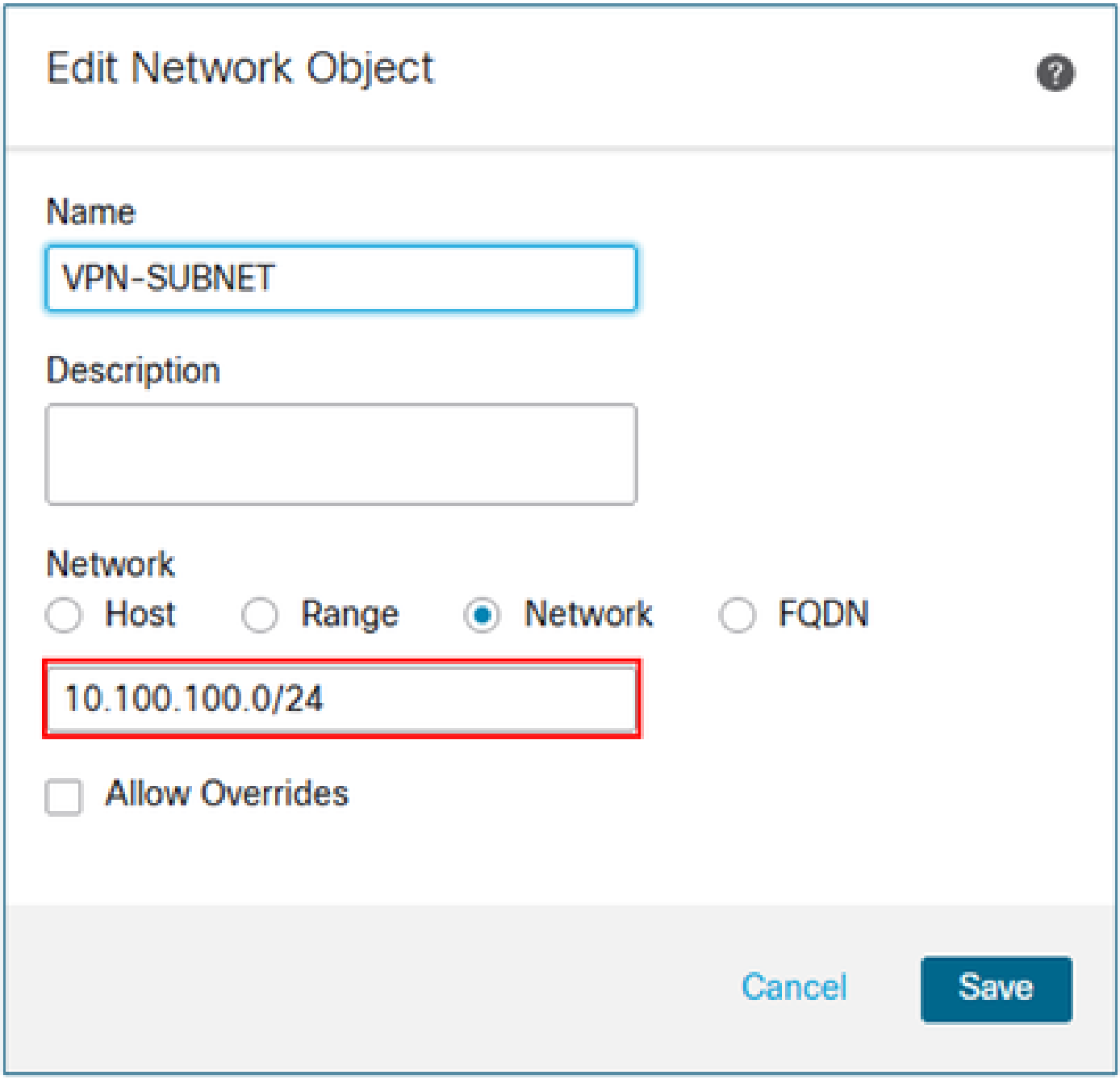
```
R1#
show ip route


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
```

Tipp: Optional können Sie die EIGRP-Summary-Address-Funktion auf FTD verwenden, um die Größe der Routing-Tabelle zu optimieren.

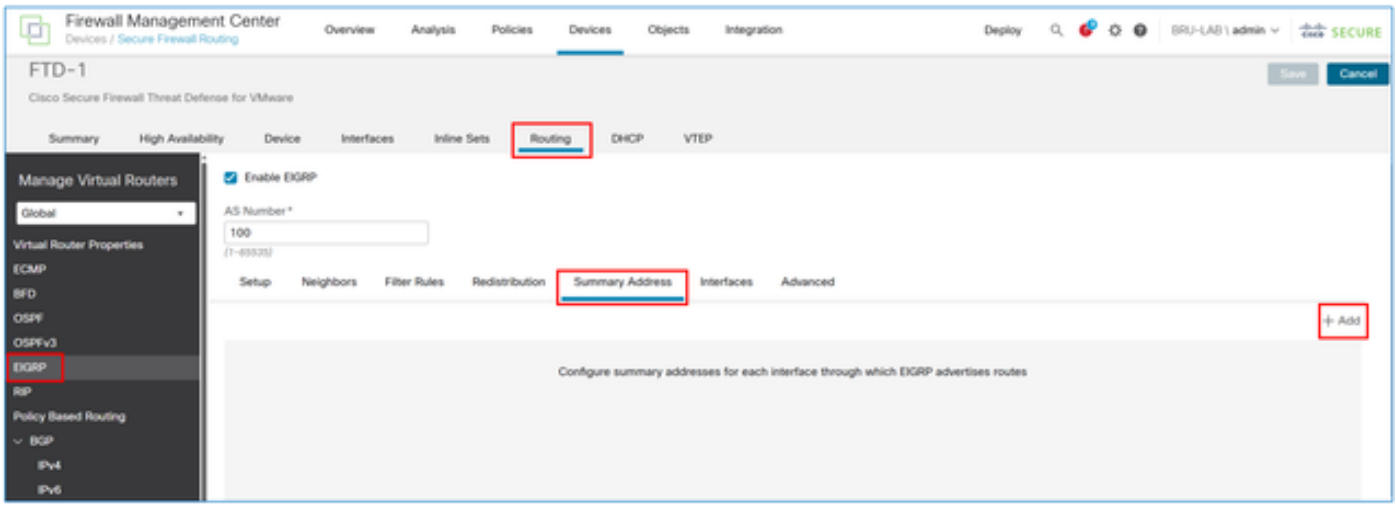
Konfiguration der EIGRP-Summary-Adresse

Konfigurieren

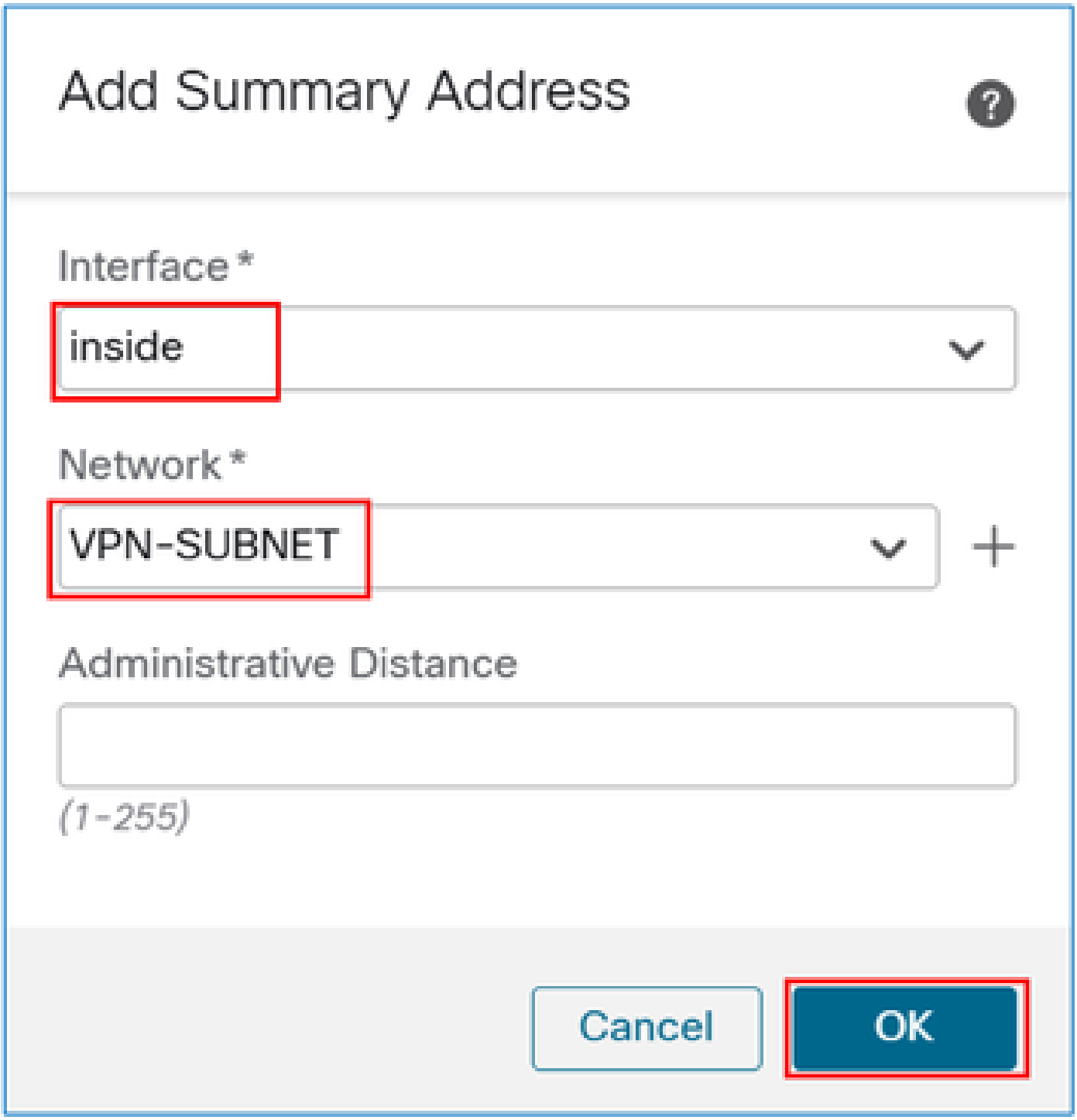
Falls noch nicht erstellt, erstellen Sie ein Netzwerkobjekt für die VPN-Subnetze.



Navigieren Sie in der Benutzeroberfläche für das FMC-Gerätemanagement zu Routing > EIGRP > Summary Address, und wählen Sie dann die Schaltfläche Add (Hinzufügen).



Geben Sie im Feld interface (Schnittstelle) das Objekt ein, das dem EIGRP-Nachbarn zugewandt ist, und im Feld network (Netzwerk) das Objekt, das für das VPN-Subnetz erstellt wurde.


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

Ergebnis:

Überprüfung

FTD EIGRP Summary-Adresskonfiguration:

```
<#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-Topologietabelle:

```
<#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
```

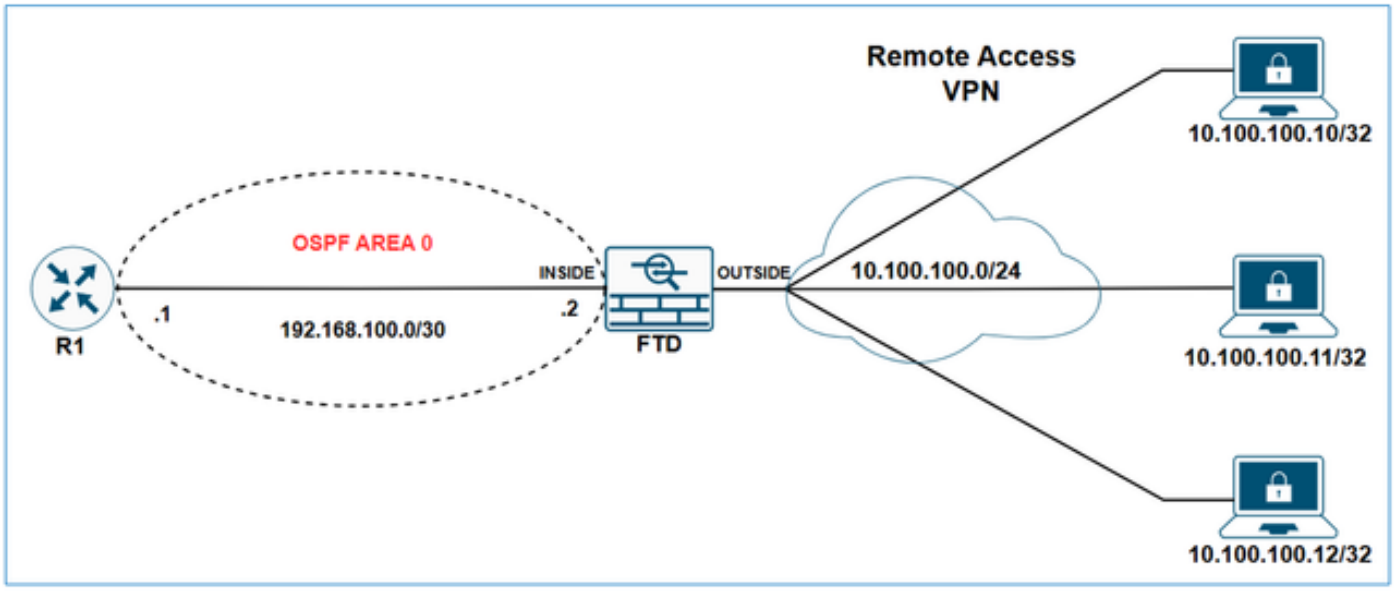
R1-Routing-Tabelle:

<#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
```

Neuverteilung von Remote Access-VPN-Subnetzen über OSPF auf FTD

Netzwerkdiagramm



Startkonfigurationen

<#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 zeigt ospf Neighbor-Ausgabe an:

<#root>

```
FTD-1#
```

```
show ospf neighbor
```

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

R1 show ip ospf neighbor output:

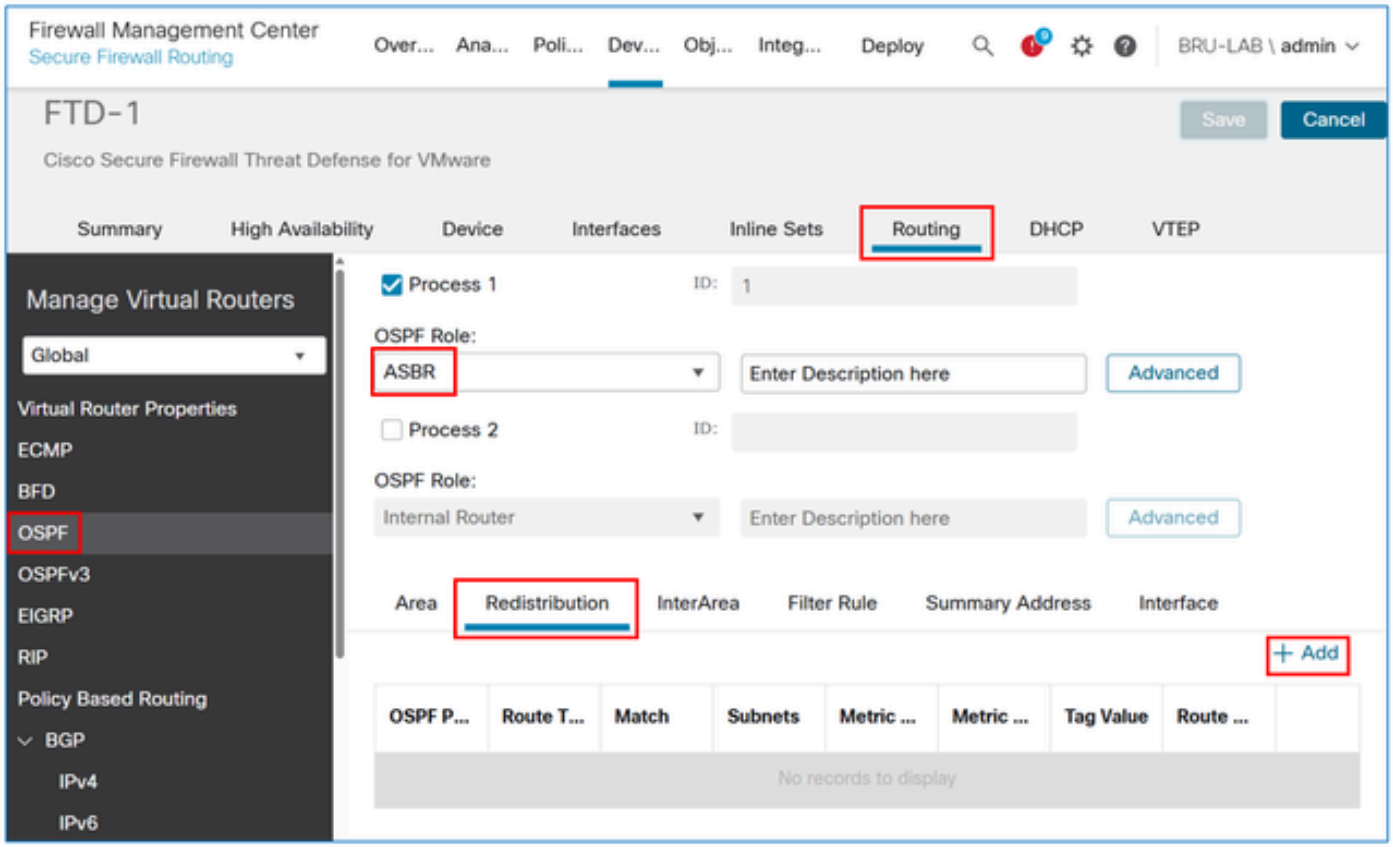
```
<#root>

R1#

show ip ospf neighbor


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

R1-Routing-Tabelle:

```
<#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
```

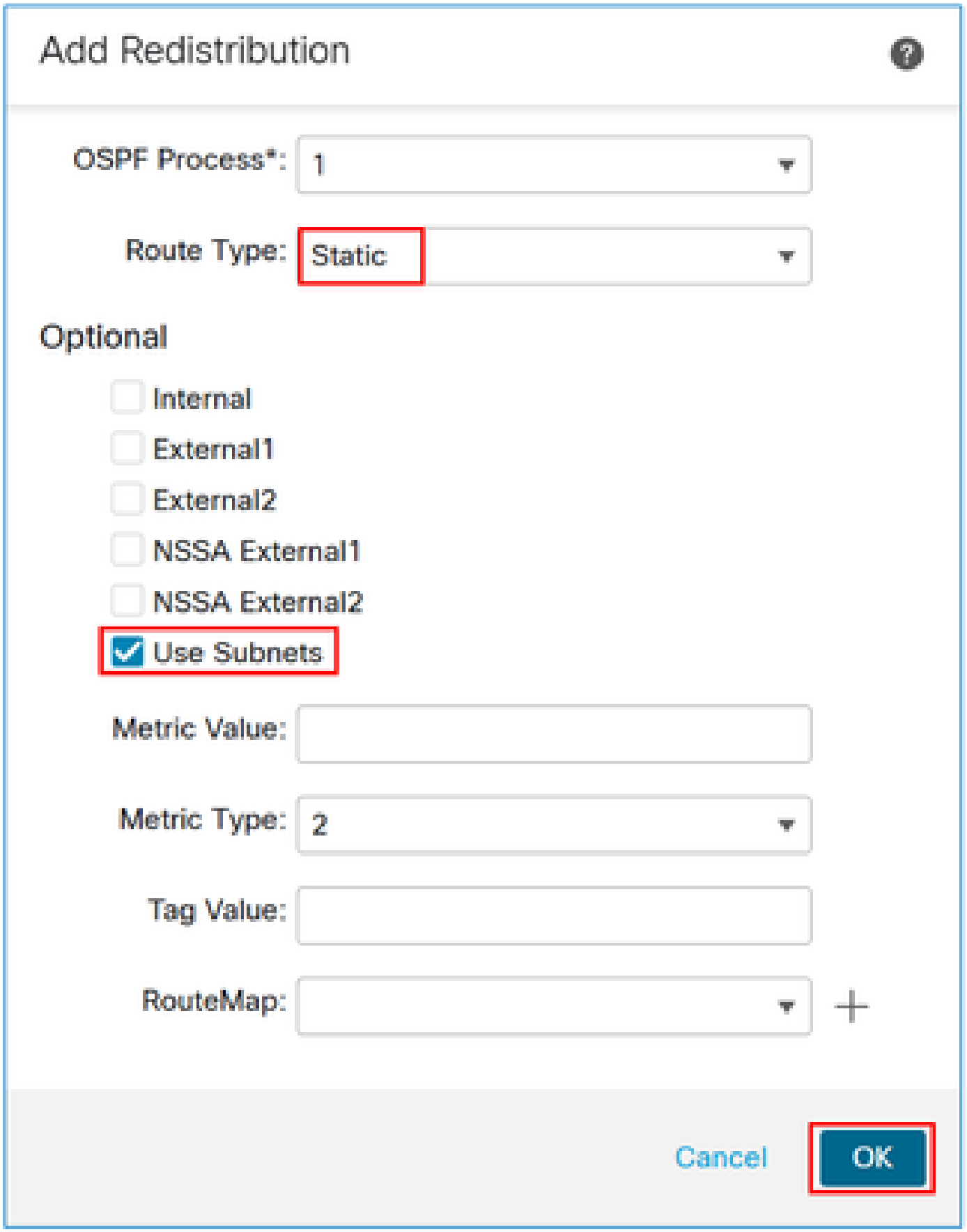
Konfigurieren

Navigieren Sie in der Benutzeroberfläche für das FMC-Gerätemanagement zu Routing > OSPF > Redistribution, und wählen Sie dann die Schaltfläche Hinzufügen.



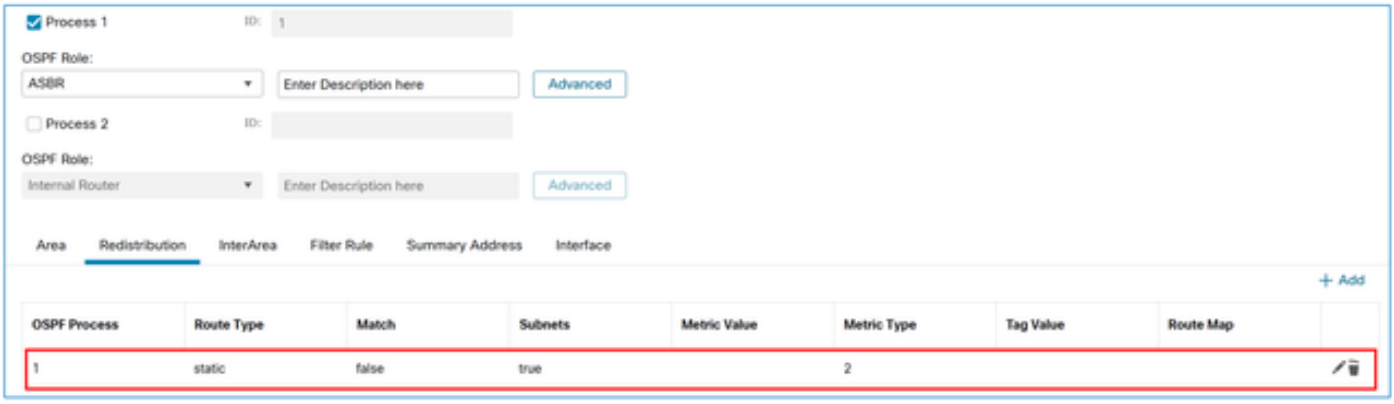
Anmerkung: Die OSPF-Rolle muss als ASBR oder ABR und ASBR festgelegt werden, um die Neuverteilung zu ermöglichen.

Wählen Sie im Feld "Route Type" die Option Static (Statisch) aus, und aktivieren Sie dann das Kontrollkästchen Use Subnets (Subnetze verwenden).



⚠ Achtung: Dadurch werden alle statischen Routen in OSPF umverteilt. Wenn Sie nur die VPN-Subnetze ankündigen müssen, können Sie eine Routenübersicht anwenden, um sie zu filtern.

Ergebnis:



Überprüfung

FTD OSPF-Neuverteilungskonfiguration:

```
<#root>

FTD-1#

sh run router


router ospf 1
 network 192.168.100.0 255.255.255.252 area 0

 redistribute static subnets
```

R1-Routing-Tabelle:

```
<#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
```

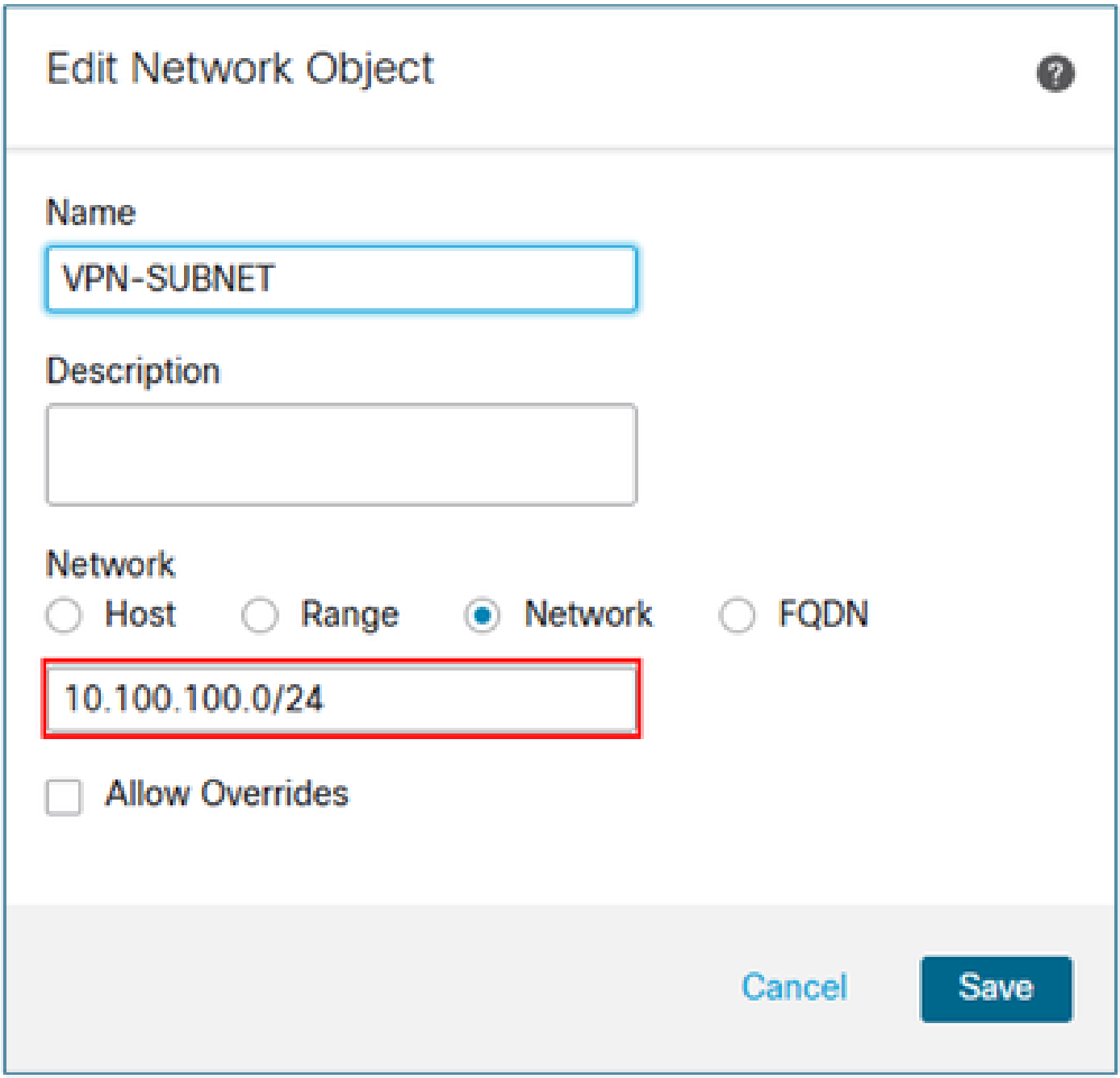
```
C        192.168.100.0/30 is directly connected, GigabitEthernet1
L        192.168.100.1/32 is directly connected, GigabitEthernet1
      10.0.0.0/32 is subnetted, 1 subnets
O E2     10.100.100.10 [110/20] via 192.168.100.2, 00:08:01, GigabitEthernet1
```

Tipp: Beachten Sie, dass der VPN-Pool zwar 10.100.100.0/24 lautet, die FTD jedoch ein /32-Subnetz über OSPF verteilt. Dies liegt daran, dass die FTD für jede Remotezugriff-VPN-Sitzung eine statische Route mit einem /32-Präfix erstellt. Um dies zu optimieren, können Sie die Funktion "OSPF Summary Address" (OSPF-Summary-Adresse) verwenden.

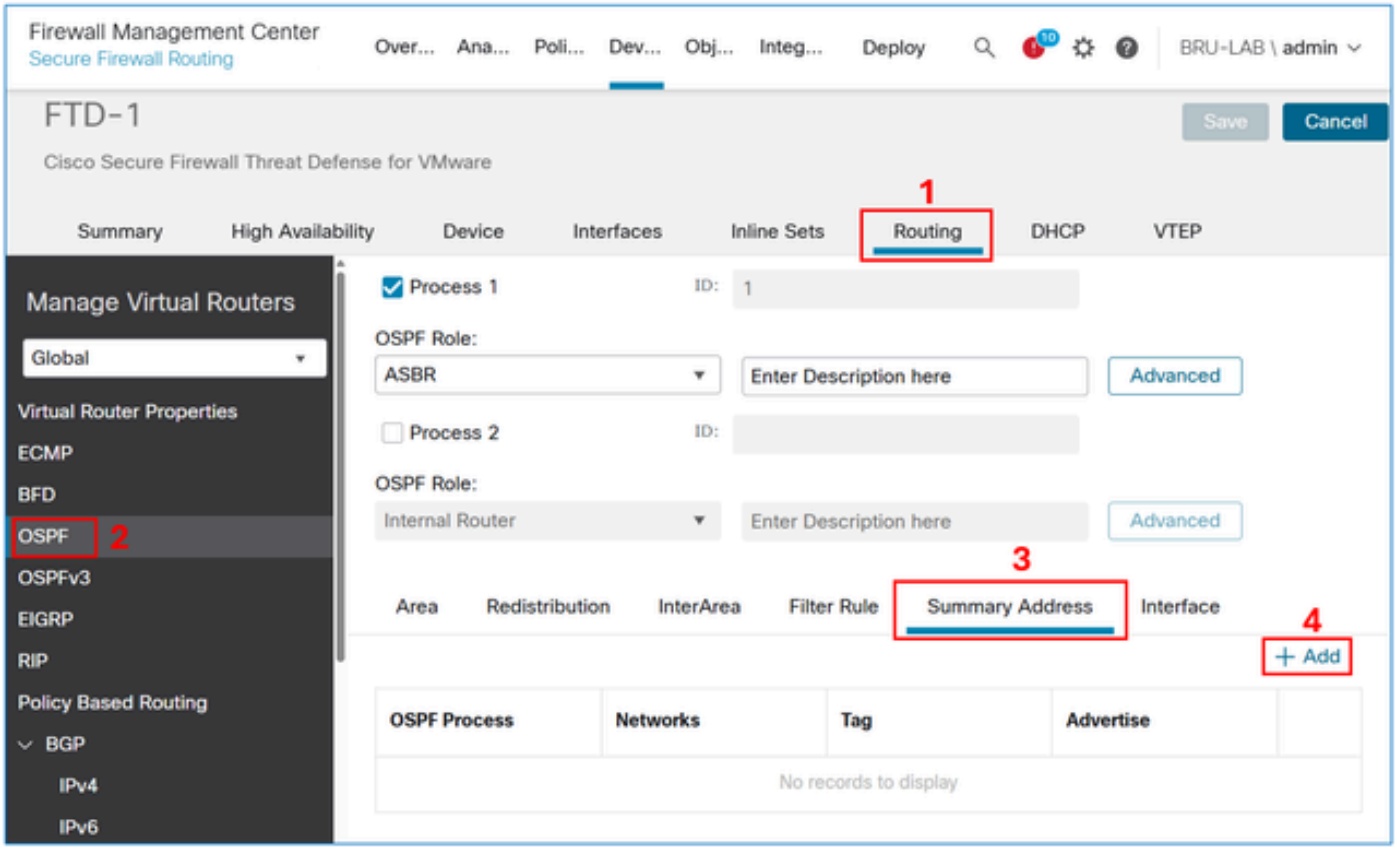
Konfiguration der OSPF-Summary-Adresse

Konfigurieren

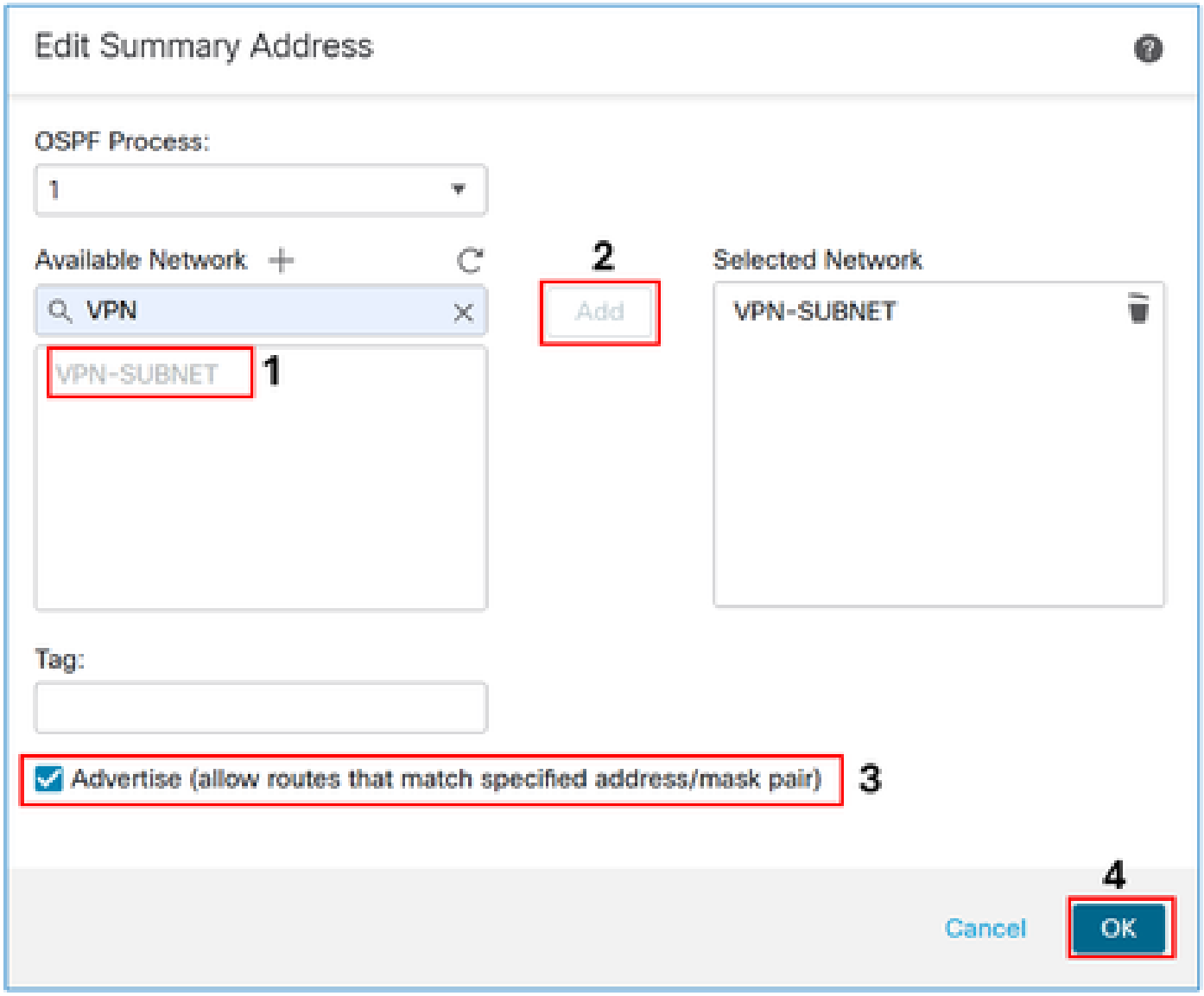
Falls noch nicht erstellt, erstellen Sie ein Netzwerkobjekt für die VPN-Subnetze.



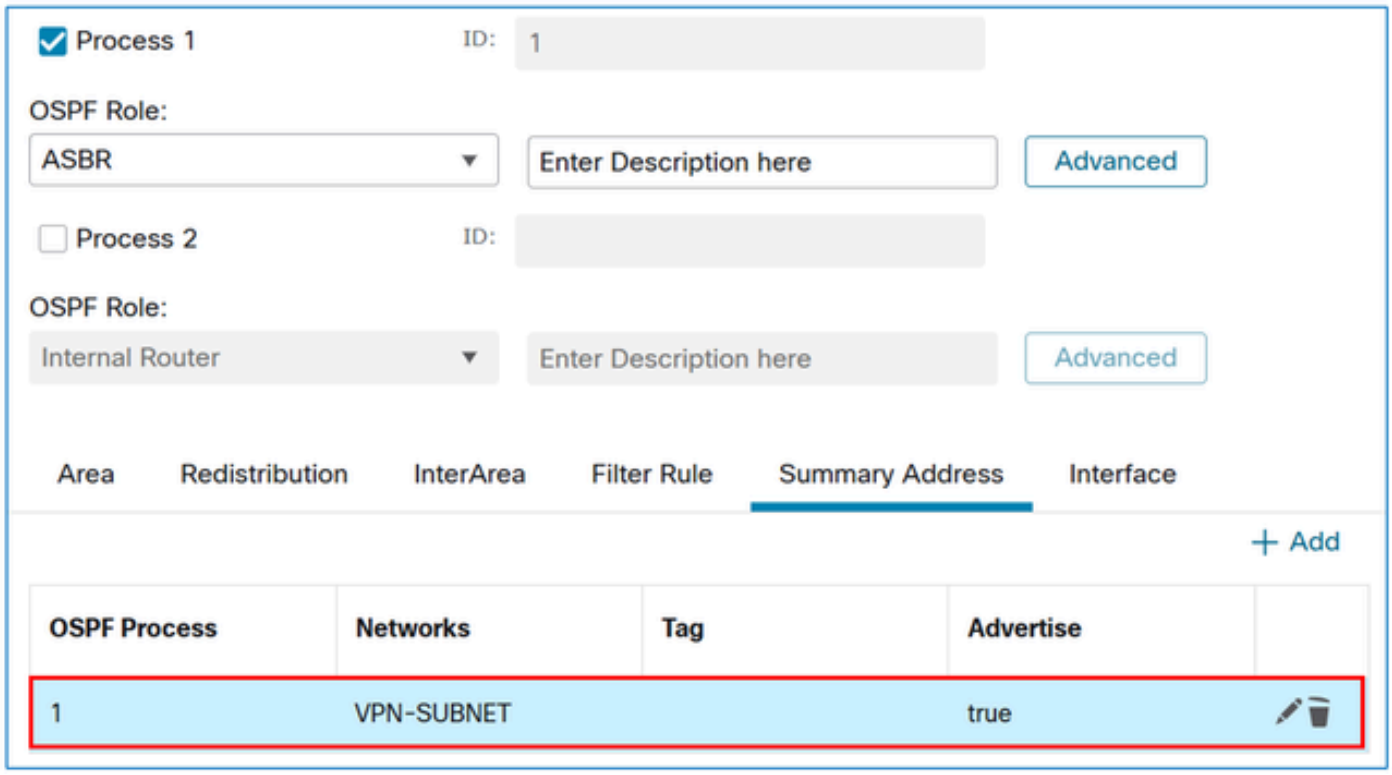
Navigieren Sie in der Benutzeroberfläche für das FMC-Gerätemanagement zu Routing > OSPF > Summary Address, und wählen Sie dann die Schaltfläche Add (Hinzufügen).



Fügen Sie das VPN-Subnetzobjekt hinzu, und aktivieren Sie das Kontrollkästchen Anzeigen.


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

Ergebnis:



Überprüfung

FTD-OSPF-Konfiguration:

<#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-Routing-Tabelle:

<#root>

R1#

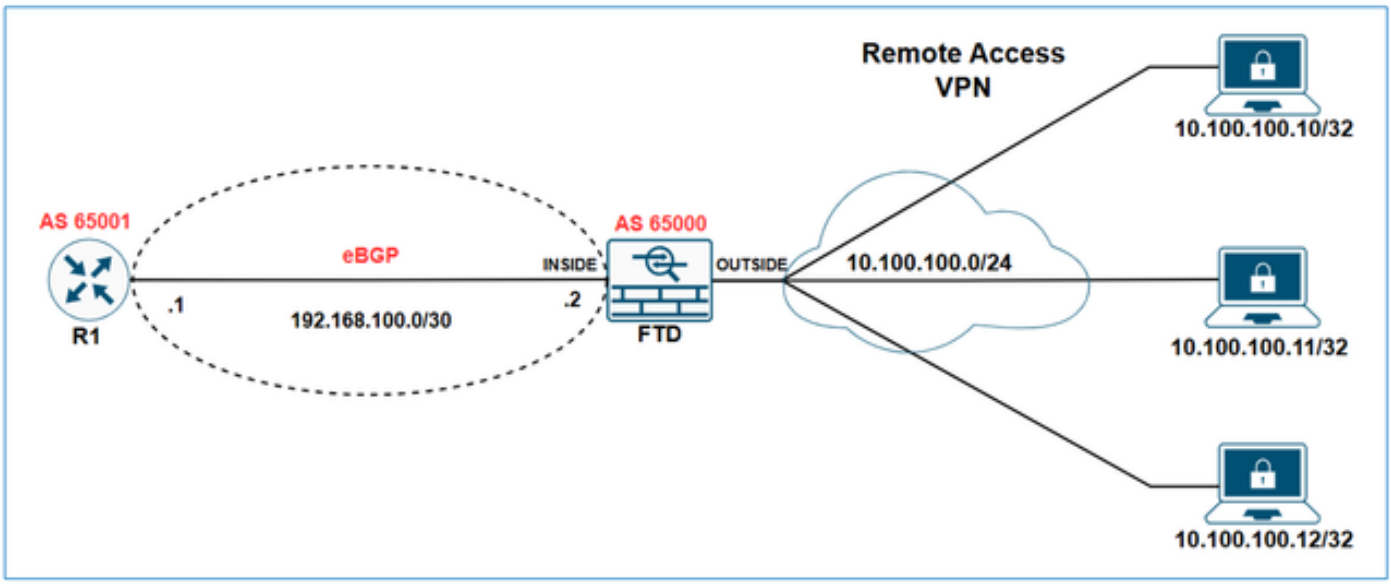
sh ip route

```
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
```

Verteilung von Remote Access-VPN-Subnetzen über eBGP auf FTD

Netzwerkdiagramm



In diesem Beispiel soll erreicht werden, dass R1 das VPN-Subnetz 10.100.100.0/24 via eBGP erlernt.

Startkonfigurationen

FTD Erstkonfiguration:

<#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
```

Ausgabe der FTD-BGP-Tabelle:

```
<#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 zeigt BGP-Übersichtsausgabe an:

```
<#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
```

Ausgabe der R1-BGP-Tabelle:

<#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-Routing-Tabelle:

<#root>

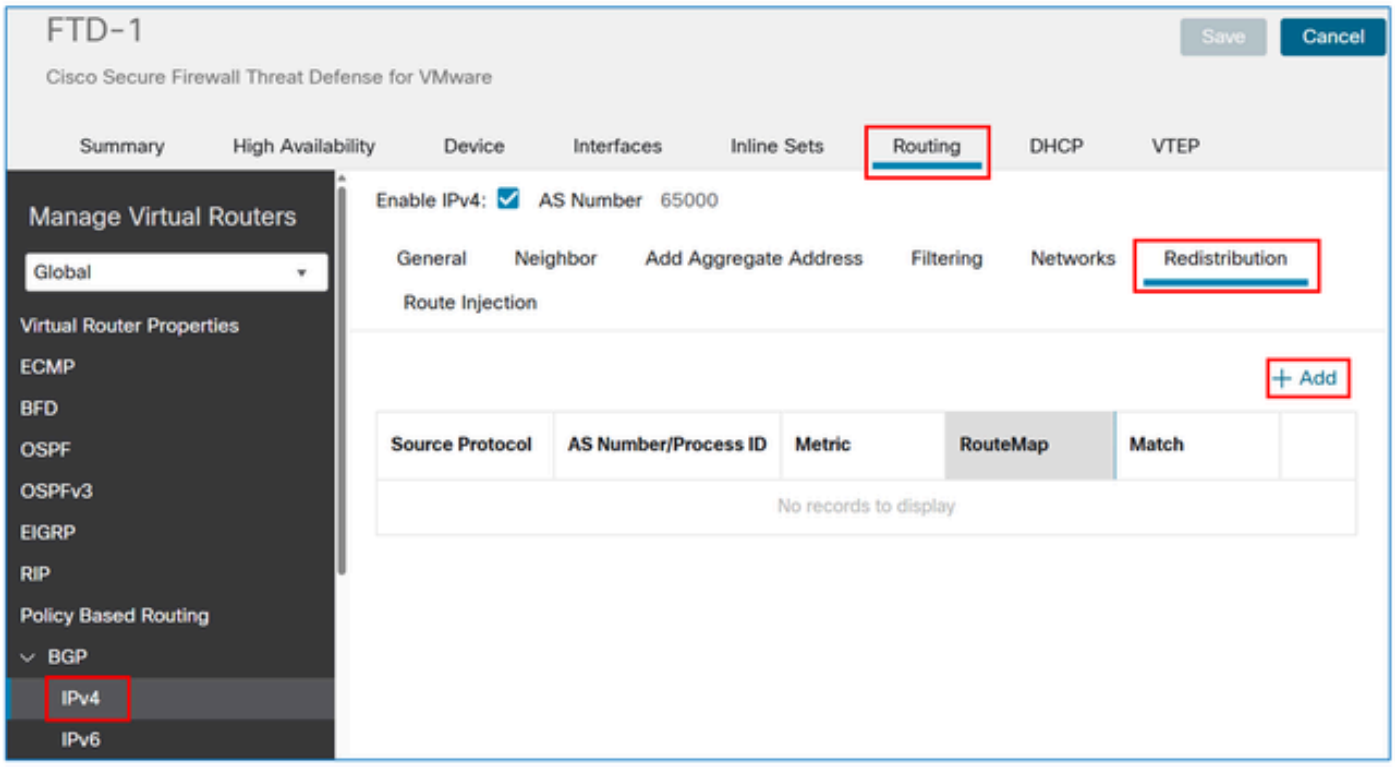
R1#

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
```

Konfigurieren

Navigieren Sie in der Benutzeroberfläche für das FMC-Gerätemanagement zu Routing > BGP > IPv4 > Redistribution, und wählen Sie dann die Schaltfläche Hinzufügen.



Wählen Sie im Feld Source Protocol (Quellprotokoll) die Option Static (Statisch) aus, und klicken Sie dann auf die Schaltfläche OK.

Add Redistribution

Source Protocol

Static

Process ID*

Metric

(0-4294967295)

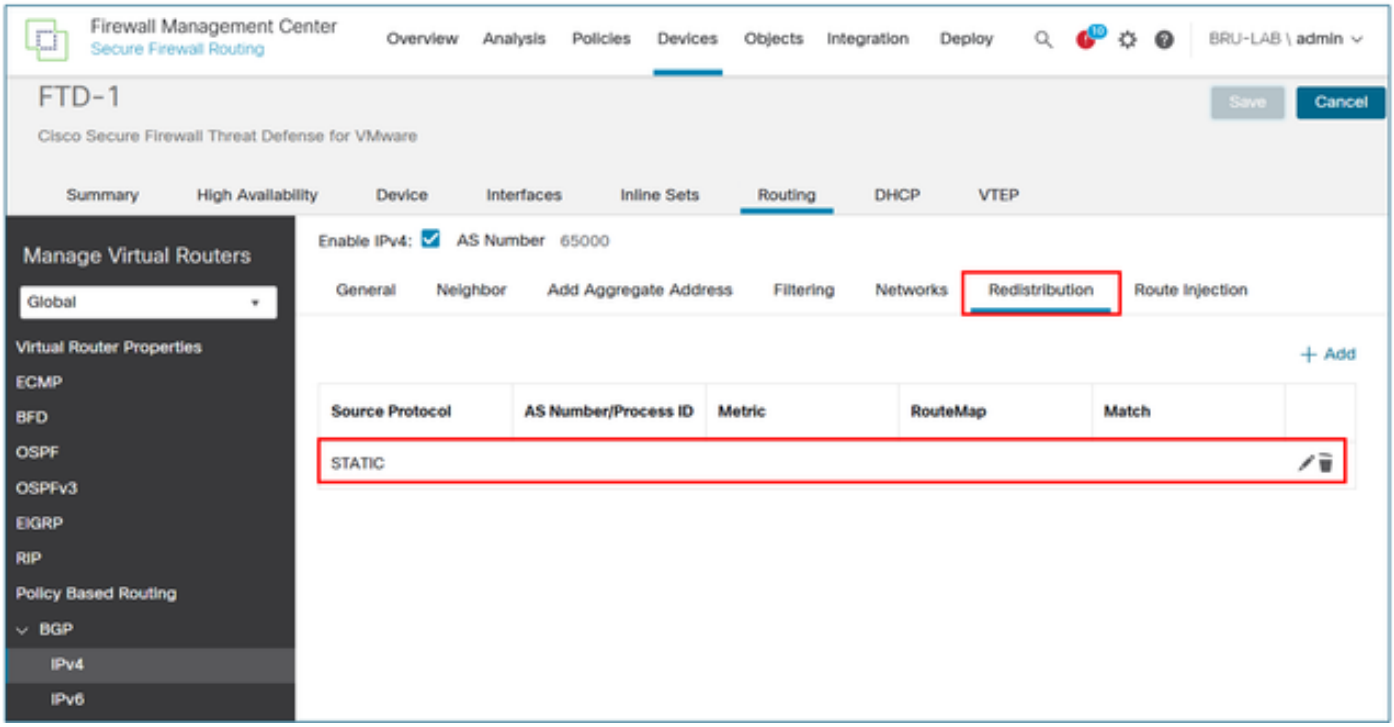
Route Map

Match

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

⚠ : Dadurch werden alle statischen Routen über das BGP neu verteilt. Wenn Sie nur die VPN-Subnetze ankündigen müssen, können Sie eine Routenübersicht anwenden, um sie zu filtern.

Ergebnis:



Speichern und Bereitstellen der Konfiguration auf dem FTD

Überprüfung

FTD-BGP-Konfiguration:

<#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
```

Ausgabe der FTD-BGP-Tabelle:

```
<#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 ?
```

Ausgabe der R1-BGP-Tabelle:

```
<#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 ?
```

Ausgabe der R1-Routing-Tabelle:

```
<#root>

R1#

show ip route
```

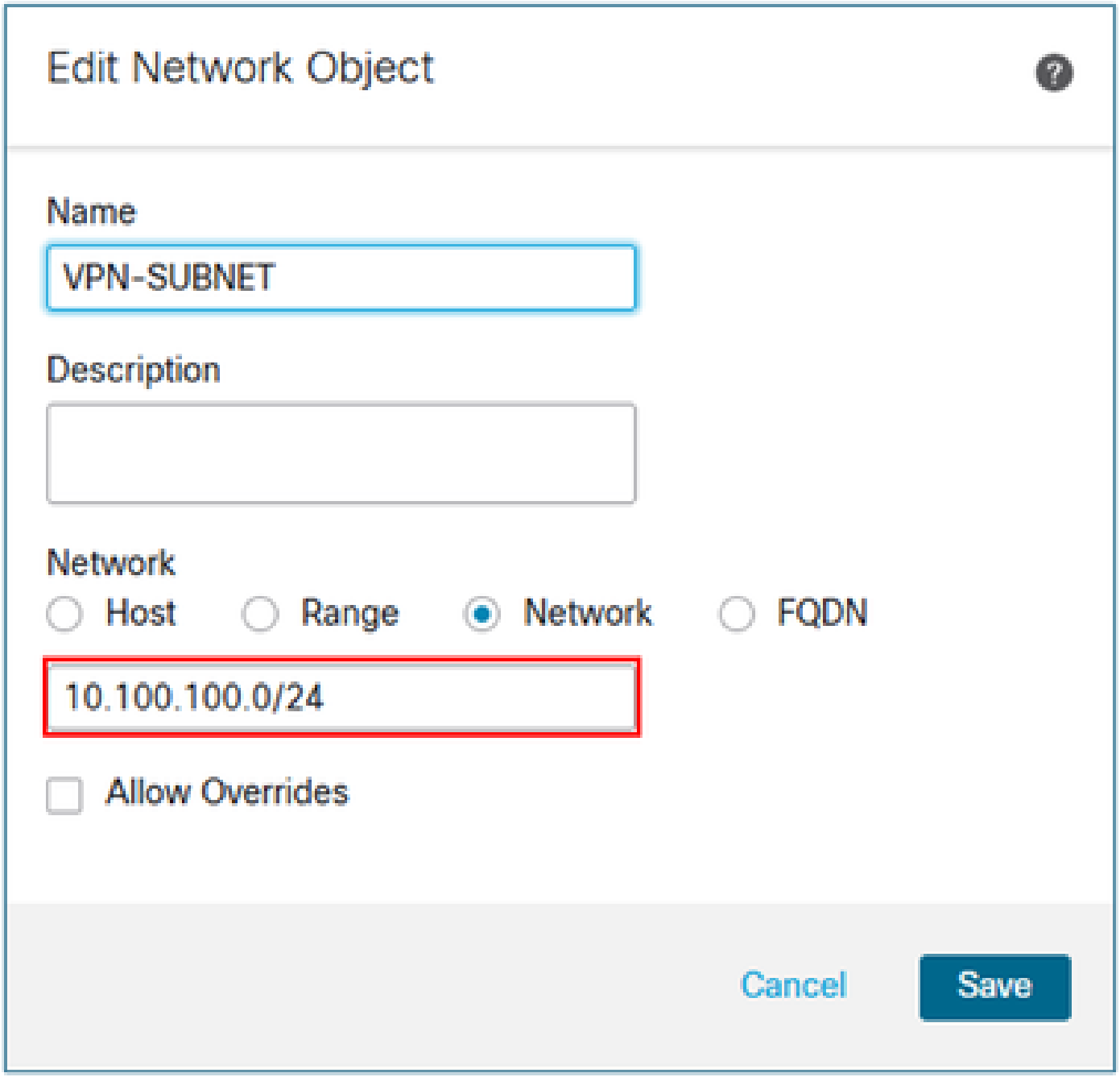
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT,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

Tipp: Beachten Sie, dass der VPN-Pool zwar 10.100.100.0/24 lautet, die FTD jedoch ein /32-Subnetz über BGP verteilt. Dies liegt daran, dass die FTD für jede Remotezugriff-VPN-Sitzung eine statische Route mit einem /32-Präfix erstellt. Um dies zu optimieren, können Sie die Funktion "BGP Aggregate Address" verwenden.

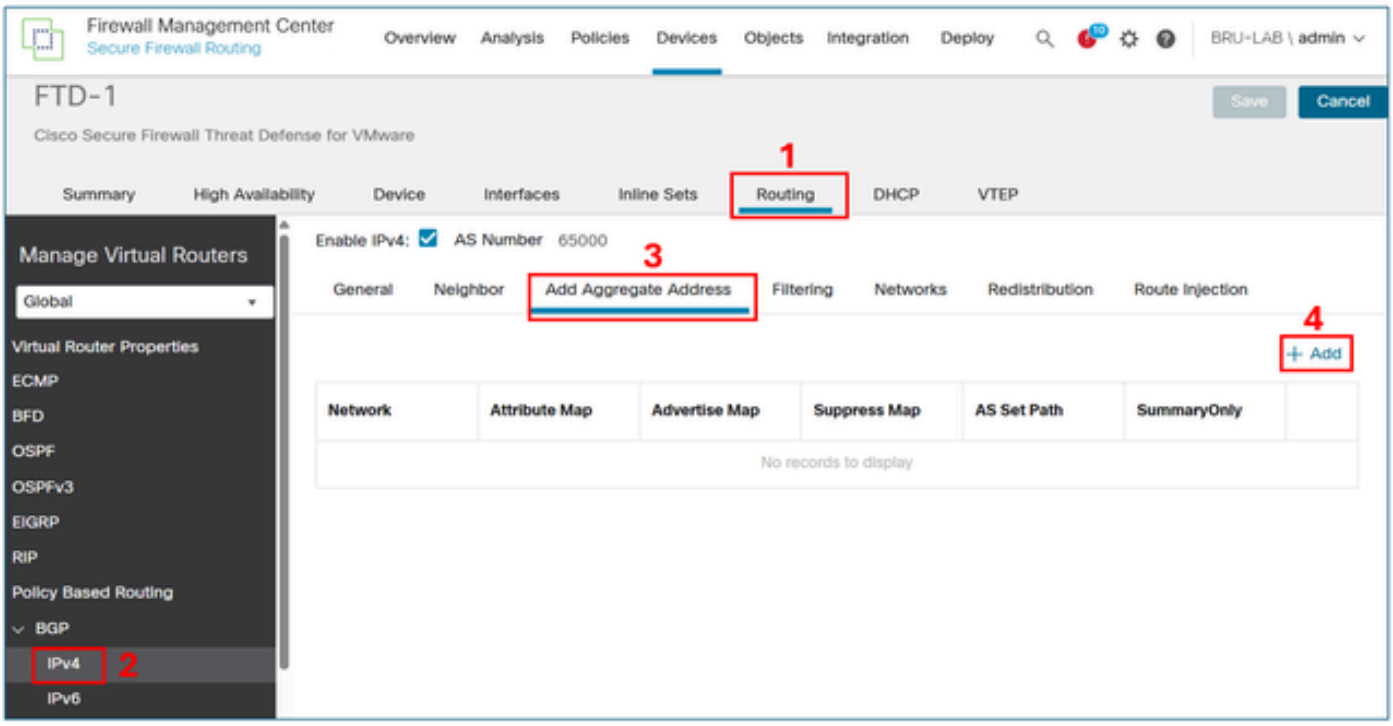
Konfiguration der aggregierten BGP-Adresse

Konfigurieren

Falls noch nicht erstellt, erstellen Sie ein Netzwerkobjekt für die VPN-Subnetze.



Navigieren Sie in der Benutzeroberfläche für das FMC-Gerätemanagement zu Routing > BGP> IPv4 > Add Aggregate Address, und wählen Sie dann die Schaltfläche Add (Hinzufügen).



Fügen Sie im Feld "Network" (Netzwerk) das Objekt für das VPN-Subnetz hinzu, und aktivieren Sie dann das Kontrollkästchen Filter all route from updates (Alle Routen aus Updates filtern).

Add Aggregate Address

Network*

VPN-SUBNET

Attribute Map

Advertise Map

Suppress Map

Generate AS set path information

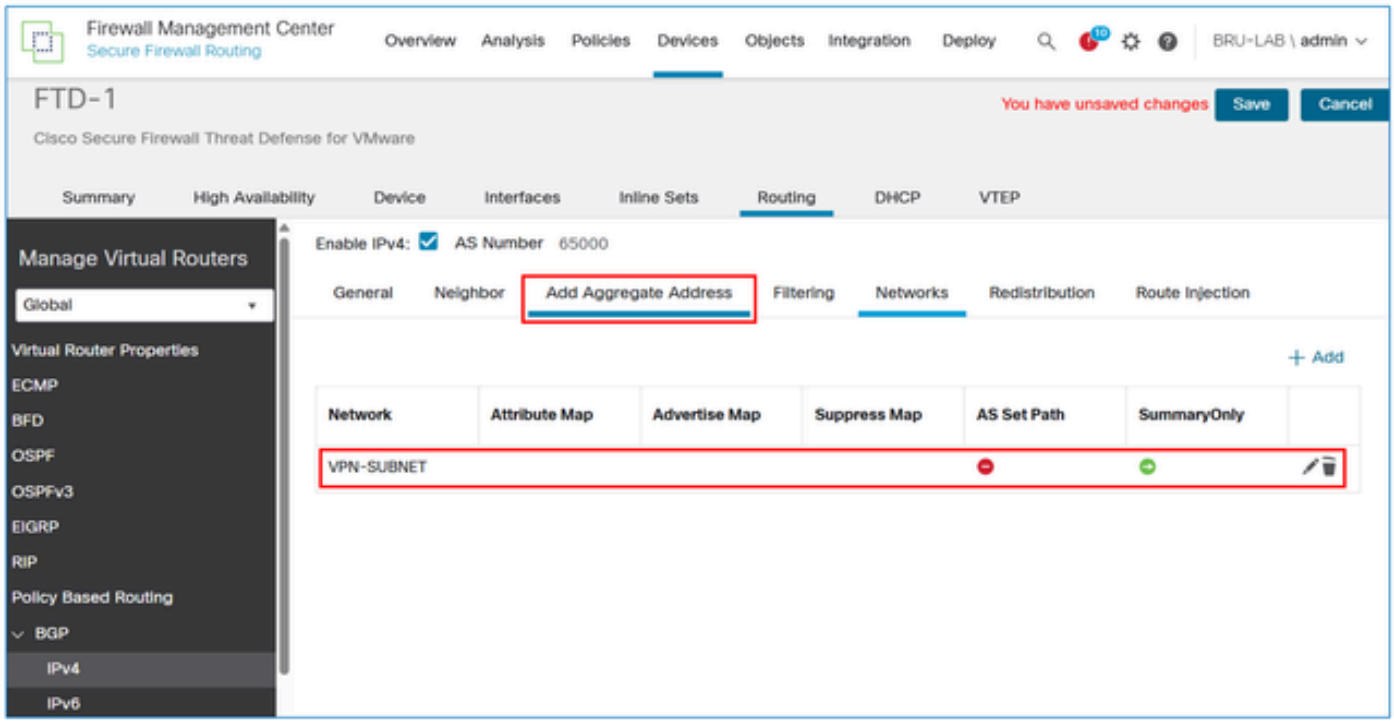
Filter all routes from updates

Cancel

OK

Anmerkung: Wenn das Kontrollkästchen Alle Routen von Updates filtern deaktiviert ist, kündigt das FTD die zusammengefasste Adresse und die spezifischen /32 VPN-Routen über BGP an. Wenn das Kontrollkästchen aktiviert ist, überträgt das FMC den Befehl aggregate-address summary-only an die FTD-LINA-Konfiguration und stellt sicher, dass nur die zusammengefasste Adresse angekündigt wird.

Ergebnis:



Speichern und Bereitstellen der Konfiguration auf dem FTD

Überprüfung

FTD-BGP-Konfiguration:

<#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
```

Ausgabe der FTD-BGP-Tabelle:

<#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 ?
```

Ausgabe der R1-BGP-Tabelle:

<#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 ?
```

Ausgabe der R1-Routing-Tabelle:

<#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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.