

Adverteren voor VPN-subnetten met externe toegang via routeringsprotocollen in FTD

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Herdistributie van Remote Access VPN-subnetten via EIGRP op FTD](#)

[Netwerkdigram](#)

[Herdistributie van Remote Access VPN-subnetten via EIGRP op FTD met behulp van netwerkinstructie](#)

[Configureren](#)

[Verifiëren](#)

[Herdistributie van Remote Access VPN-subnetten via EIGRP op FTD met behulp van de statische benadering voor herverdeling](#)

[Configureren](#)

[Verifiëren](#)

[Configuratie EIGRP-overzichtsadres](#)

[Configureren](#)

[Verifiëren](#)

[Herdistributie van Remote Access VPN-subnetten via OSPF op FTD](#)

[Netwerkdigram](#)

[Configureren](#)

[Verifiëren](#)

[Adresconfiguratie OSPF-overzicht](#)

[Configureren](#)

[Verifiëren](#)

[Herdistributie van Remote Access VPN-subnetten via eBGP op FTD](#)

[Netwerkdigram](#)

[Configureren](#)

[Verifiëren](#)

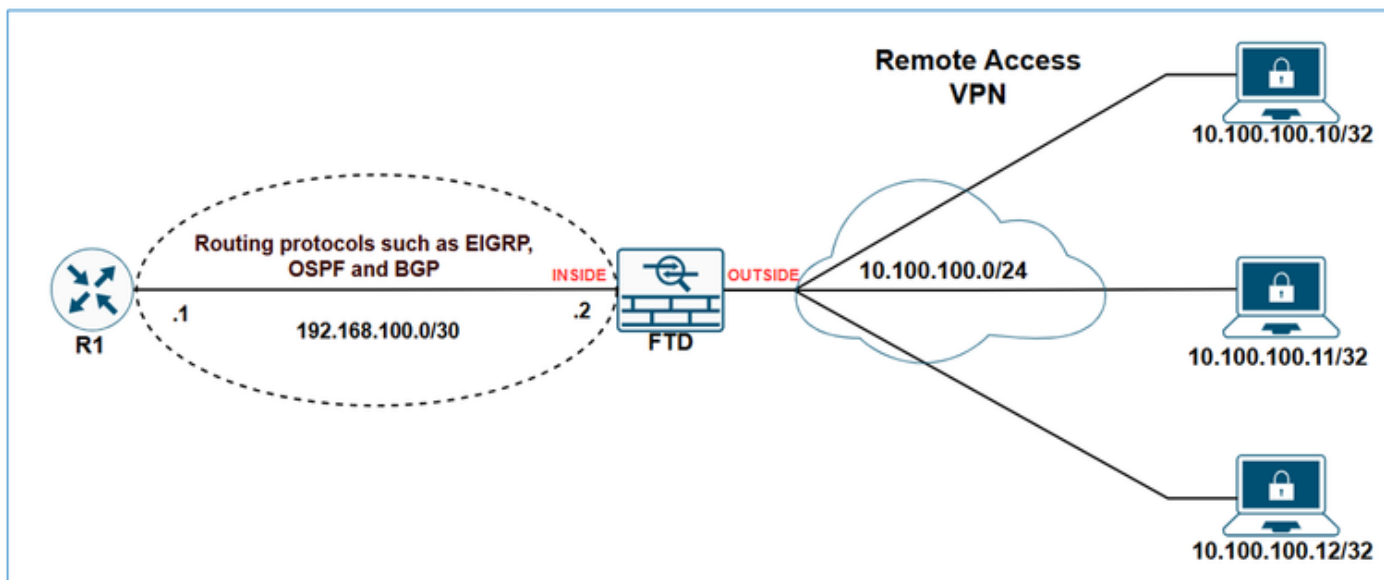
[BGP Aggregate Address Configuration](#)

[Configureren](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft de beschikbare opties voor het adverteren van VPN-gerelateerde subnetten met behulp van de routeringsprotocollen EIGRP, OSPF en BGP.



Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

 **Opmerking:** in dit document wordt de configuratie beschreven voor de herverdeling van VPN-subnetten voor externe toegang via EIGRP, OSPF en BGP met behulp van de FMC. Raadpleeg de FDM-[configuratiehandleiding voor](#) richtlijnen voor routeherverdeling met FDM.

Achtergrondinformatie

Het eerste dat u moet begrijpen, is hoe de FTD VPN-subnetten in zijn routingstabel classificeert. Hoewel deze subnetten worden weergegeven als verbonden door VPN, worden ze niet beschouwd als direct verbonden subnetten; in plaats daarvan worden ze behandeld als statische routes.

De output van de show laat dat zien.

FTD toont routeoutput:

<#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 toont route-verbonden output:

<#root>

FTD-1#

show route connected

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

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

FTD toont statische routeoutput:

<#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

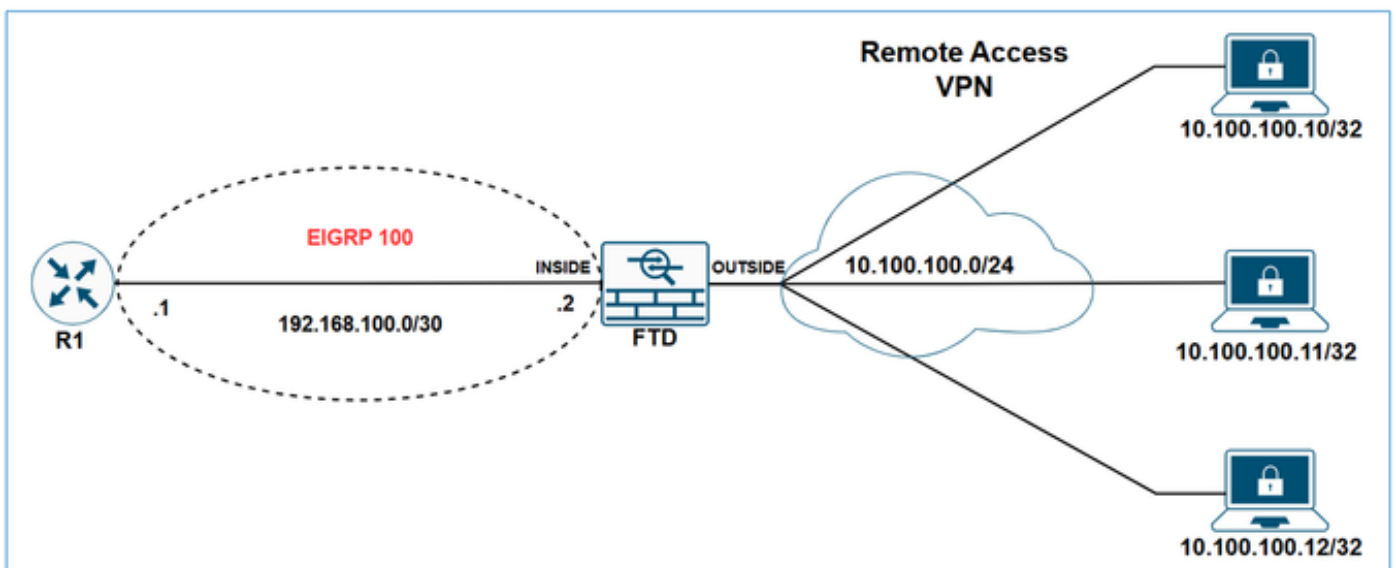
Gateway of last resort is not set

V 10.100.100.10 255.255.255.255 connected by VPN (advertised), outside

Nu duidelijk is hoe VPN-subnetten worden behandeld in de routingstabel van de firewall, is de volgende stap om te onderzoeken hoe u ze kunt adverteren met behulp van verschillende routeringsprotocollen.

Her distributie van Remote Access VPN-subnetten via EIGRP op FTD

Netwerkdigram



Statische routes die binnen het bereik van een netverklaring vallen, worden automatisch herverdeeld naar EIGRP; u hoeft hiervoor geen herverdelingsregel te definiëren. Bij het herverdelen van statische routes die naar VTI-interfaces in EIGRP wijzen, moet u echter de metriek opgeven. Voor statische routes die naar andere typen interfaces verwijzen, is het opgeven van de metriek niet vereist.

Vanwege het gedrag van EIGRP om statische routes die binnen het bereik van netwerkverklaringen vallen automatisch te herverdelen, zijn er twee opties voor het adverteren van VPN-subnetten via EIGRP op FTD:

1. Een netwerkinstructie gebruiken.
2. Gebruik de statische benadering voor herverdeling.

In dit voorbeeld is het doel om R1 het VPN-subnet 10.100.100.0/24 te laten leren via EIGRP.

Eerste FTD-configuratie:

```
<#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 Initiële routingstabel:

```
<#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 Eerste EIGRP-topologietabel:

<#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 Initiële routingstabel:

<#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
```

Her distributie van Remote Access VPN-subnetten via EIGRP op FTD met behulp van

netwerkinstructie

Configureren

Stap 1. Maak een netwerkobject voor het VPN-subnet.

Edit Network Object ?

Name

VPN-SUBNET

Description

Network

☐ Host

☐ Range

☒ Network

☐ FQDN

10.100.100.0/24

☐ Allow Overrides

Cancel

Save

Stap 2. Neem het VPN-subnetobject op in de netwerkinstructie.

Navigeer in de gebruikersinterface voor apparaatbeheer van de FMC naar Routing > EIGRP > Setup, en neem het VPN-subnet op in de geselecteerde netwerken/hosts.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

FTD-1
Cisco Secure Firewall Threat Defense for VMware

Summary High Availability Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM

☒ Enable EIGRP
AS Number *
100
(1-65535)

Setup Neighbors Filter Rules Redistribution Summary Address Interfaces Advanced

☐ Auto Summary

Available Networks/Hosts (33) C +
any-ipv4
BR-DMZ-NET
BR-LAN-NET
HQ-DMZ
HQ-DMZ-SRV1
HQ-DMZ-SRV2

Selected Networks/Hosts (2)
HQ-WAN-1
VPN-SUBNET

Add

☐ Passive Interface

Bewaar en implementeer de configuratie op de FTD.

Verifiëren

FTD EIGRP-configuratie:

<#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 topoloty tabel:

<#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-routingstabel:

<#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

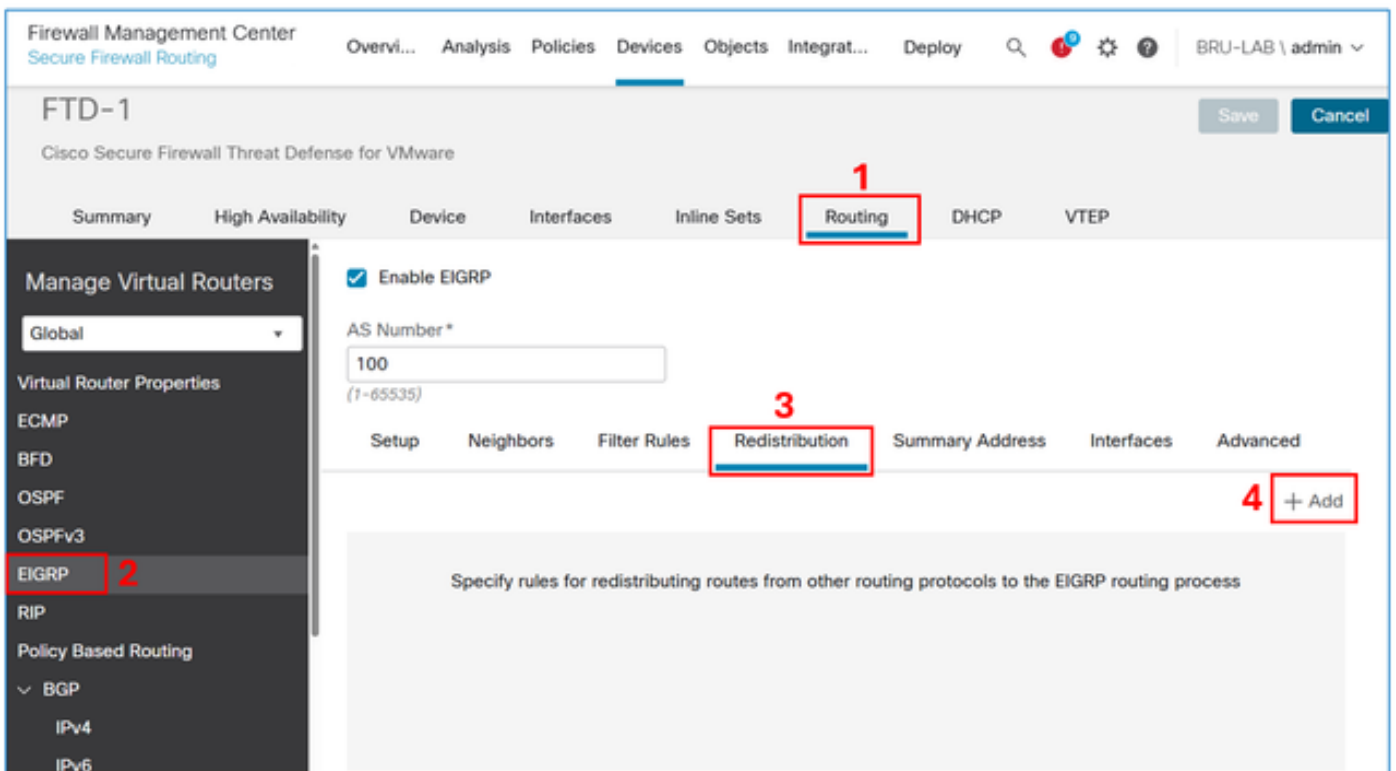
[90/3072] via 192.168.100.2, 00:02:17, GigabitEthernet1

 Opmerking: hoewel de netverklaring 10.100.100.0/24 was, herverdeelt de FTD een /32-subnet over EIGRP. Dit gebeurt omdat de FTD een statische route creëert met een /32 voorvoegsel voor elke VPN-sessie voor externe toegang. Om dit te optimaliseren, kunt u de functie EIGRP-overzichtsadres gebruiken.

Her distributie van Remote Access VPN-subnetten via EIGRP op FTD met behulp van de statische benadering voor herverdeling

Configureren

Navigeer in de gebruikersinterface voor FMC-apparaatbeheer naar Routing > EIGRP > Redistribution en selecteer vervolgens de knop Toevoegen.



Selecteer in het veld Protocol de optie Statisch en selecteer vervolgens de knop OK.

Add Redistribution

Protocol

Protocol *

Static

Optional OSPF Redistribution

☐ Internal

☐ External1

☐ External2

☐ Nssa-External1

☐ Nssa-External2

Optional Metrics

Bandwidth

(1-4294967295 in kbps)

Delay Time

(0-4294967295 in 10µs)

Reliability

(0-255)

Loading

(1-255)

MTU

(1-65535 in bytes)

Route Map

Select...

Cancel

OK

 Let op: Dit herverdeelt alle statische routes in EIGRP. Als u alleen de VPN-subnetten wilt adverteren, kunt u de netwerkinstructiebenadering gebruiken of een routekaart toepassen om ze te filteren.

Het resultaat:

☒ Enable EIGRP

AS Number *

100
(1-65535)

Setup Neighbors Filter Rules **Redistribution** Summary Address Interfaces Advanced

+ Add

Protocol	ID	Bandwidth	Delay Time	Reliability	Loading	MTU	Route Map
STATIC							

Bewaar en implementeer de configuratie op de FTD.

Verifiëren

FTD EIGRP-configuratie:

<#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 topology tabel:

<#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-routingstabel:

<#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



Tip: Optioneel kunt u de functie EIGRP-overzichtsadres op FTD gebruiken om de grootte van de routingstabel te optimaliseren.

Configuratie EIGRP-overzichtsadres

Configureren

Als het nog niet is gemaakt, maakt u een netwerkobject voor de VPN-subnetten.

Edit Network Object

Name

VPN-SUBNET

Description

Network

☐ Host

☐ Range

☒ Network

☐ FQDN

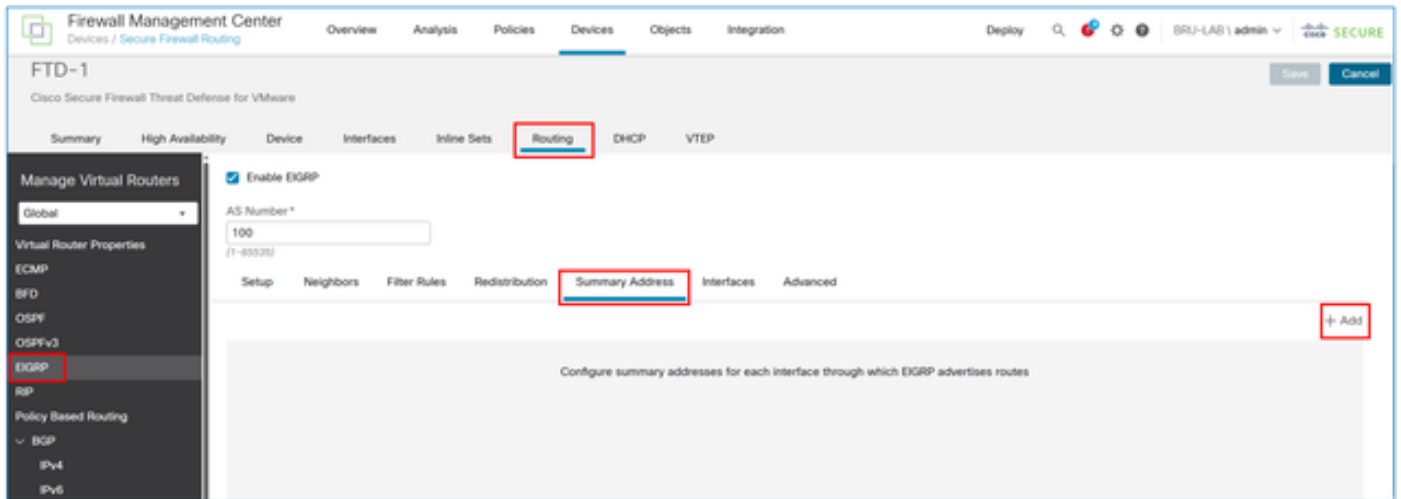
10.100.100.0/24

☐ Allow Overrides

Cancel

Save

Navigeer in de gebruikersinterface voor apparaatbeheer van de FMC naar Routing > EIGRP > Summary Address (Overzichtsadres) en selecteer vervolgens de knop Add (Toevoegen).



Voer in het veld Interface degene in die naar de EIGRP-buur kijkt en voer in het netwerkveld het object in dat is gemaakt voor het VPN-subnet.

Add Summary Address



Interface *

inside



Network *

VPN-SUBNET



Administrative Distance

(1-255)

Cancel

OK

Het resultaat:

☒ Enable EIGRP

AS Number*

 (1-65535)

Setup Neighbors Filter Rules Redistribution **Summary Address** Interfaces Advanced

+ Add

Interface	Network	Administrative Distance
inside	VPN-SUBNET	

Verifiëren

FTD EIGRP Samenvatting Adresconfiguratie:

```
<#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 topoloty tabel:

```
<#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-routingstabel:

<#root>

R1#

show ip route

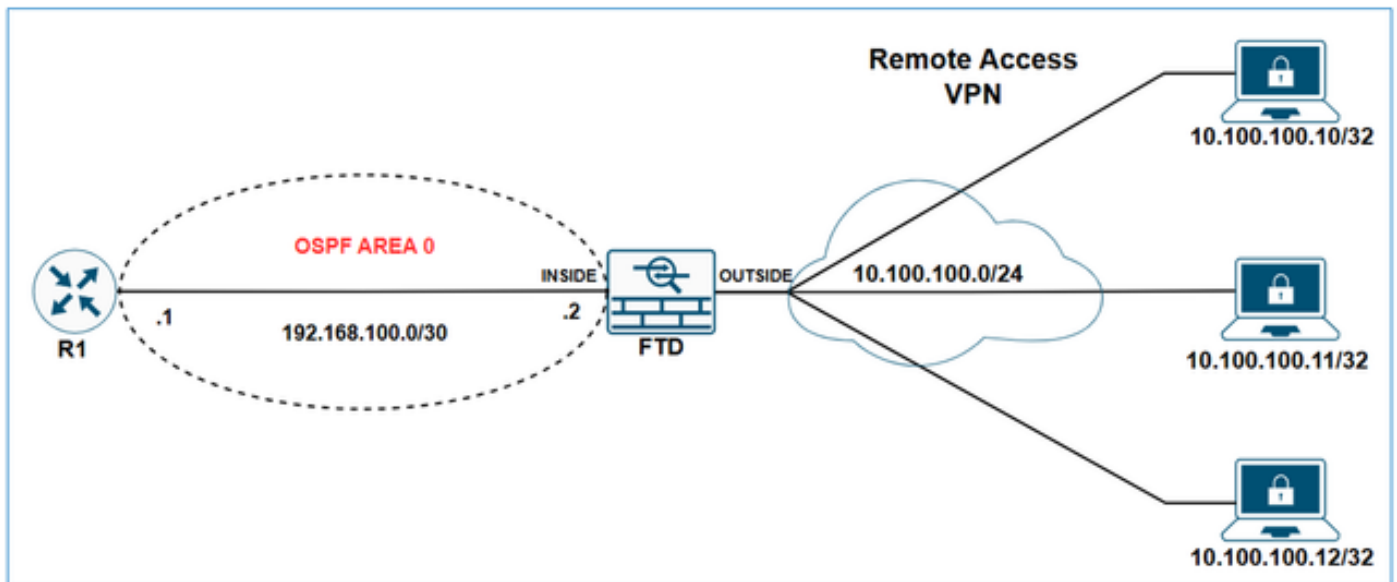
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, 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

Her distributie van Remote Access VPN-subnetten via OSPF op FTD

Netwerkdigram



Initiële configuraties

<#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 toont de output van de ospf-buren:

<#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 toon ip ospf buur uitgang:

<#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-routingstabel:

<#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

Configureren

Navigeer in de gebruikersinterface voor FMC-apparaatbeheer naar Routing > OSPF > Redistribution en selecteer vervolgens de knop Toevoegen.

Firewall Management Center
Secure Firewall Routing

Over... Ana... Poli... Dev... Obj... Integ... Deploy 🔍 ⚙️ ? BRU-LAB \ admin

FTD-1

Cisco Secure Firewall Threat Defense for VMware

Save Cancel

Summary High Availability Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global ▾

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

☒ Process 1 ID: 1

OSPF Role:
ASBR Enter Description here Advanced

☐ Process 2 ID:

OSPF Role:
Internal Router Enter Description here Advanced

Area **Redistribution** InterArea Filter Rule Summary Address Interface

+ Add

OSPF P...	Route T...	Match	Subnets	Metric ...	Metric ...	Tag Value	Route ...
No records to display							

✎ Opmerking: De OSPF-rol moet worden ingesteld als ASBR of ABR & ASBR om herverdeling mogelijk te maken.

Selecteer in het veld Routetype de optie Statisch en schakel vervolgens het vak Subnetten gebruiken in.

Add Redistribution



OSPF Process*: 1

Route Type: Static

Optional

- ☐ Internal
- ☐ External1
- ☐ External2
- ☐ NSSA External1
- ☐ NSSA External2
- ☒ Use Subnets

Metric Value:

Metric Type: 2

Tag Value:

RouteMap: +

Cancel

OK

 Let op: Dit herverdeelt alle statische routes in OSPF. Als u alleen de VPN-subnetten wilt adverteren, kunt u een routekaart toepassen om ze te filteren.

Het resultaat:

OSPF Process	Route Type	Match	Subnets	Metric Value	Metric Type	Tag Value	Route Map
1	static	false	true	2			

Verifiëren

FTD OSPF-herverdelingsconfiguratie:

```
<#root>
```

```
FTD-1#
```

```
sh run router
```

```
router ospf 1
network 192.168.100.0 255.255.255.252 area 0
redistribute static subnets
```

R1-routeringstabel:

```
<#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
```

 Tip: Merk op dat hoewel de VPN-pool 10.100.100.0/24 is, de FTD een /32-subnet herverdeelt over OSPF. Dit gebeurt omdat de FTD een statische route creëert met een /32 voorvoegsel voor elke VPN-sessie voor externe toegang. Om dit te optimaliseren, kunt u de OSPF-overzichtsadresfunctie gebruiken.

Adresconfiguratie OSPF-overzicht

Configureren

Als het nog niet is gemaakt, maakt u een netwerkobject voor de VPN-subnetten.

Edit Network Object

Name

VPN-SUBNET

Description

Network

☐ Host

☐ Range

☒ Network

☐ FQDN

10.100.100.0/24

☐ Allow Overrides

Cancel

Save

Navigeer in de gebruikersinterface voor apparaatbeheer van de FMC naar Routing > OSPF> Summary Address en selecteer vervolgens de knop Add.

Firewall Management Center
Secure Firewall Routing

Over... Ana... Poli... Dev... Obj... Integ... Deploy 🔍 10 ⚙️ ? BRU-LAB \ admin ▾

FTD-1 Save Cancel

Cisco Secure Firewall Threat Defense for VMware

Summary High Availability Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global ▾

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

☒ Process 1 ID: 1

OSPF Role: ASBR ▾ Advanced

☐ Process 2 ID:

OSPF Role: Internal Router ▾ Advanced

Area Redistribution InterArea Filter Rule **Summary Address** Interface

+ Add

OSPF Process	Networks	Tag	Advertise	
No records to display				

Voeg het VPN-subnetobject toe en selecteer het selectievakje Adverteren.

Edit Summary Address

?

OSPF Process:

1

Available Network

+

Q VPN

X

VPN-SUBNET

1

Tag:

☒ Advertise (allow routes that match specified address/mask pair)

3

2

Add

Selected Network

VPN-SUBNET

4

Cancel

OK

The image shows a 'Edit Summary Address' dialog box with several components. At the top, there's a title bar with a question mark icon. Below it, the 'OSPF Process' is set to '1'. The 'Available Network' section has a search bar with 'VPN' and a list containing 'VPN-SUBNET', which is highlighted with a red box and labeled '1'. An 'Add' button, also highlighted with a red box and labeled '2', is positioned between the 'Available Network' and 'Selected Network' lists. The 'Selected Network' list contains 'VPN-SUBNET'. Below these lists is a 'Tag' input field. At the bottom, there's a checkbox labeled 'Advertise (allow routes that match specified address/mask pair)' which is checked, highlighted with a red box, and labeled '3'. The bottom right corner features 'Cancel' and 'OK' buttons, with the 'OK' button highlighted with a red box and labeled '4'.

Het resultaat:

☒ Process 1
 ID: 1

OSPF Role:

ASBR

Enter Description here

Advanced

☐ Process 2
 ID:

OSPF Role:

Internal Router

Enter Description here

Advanced

Area
 Redistribution
 InterArea
 Filter Rule
 Summary Address
 Interface

+ Add

OSPF Process	Networks	Tag	Advertise	
1	VPN-SUBNET		true	 

Verifiëren

FTD OSPF-configuratie:

<#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-routingstabel:

<#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

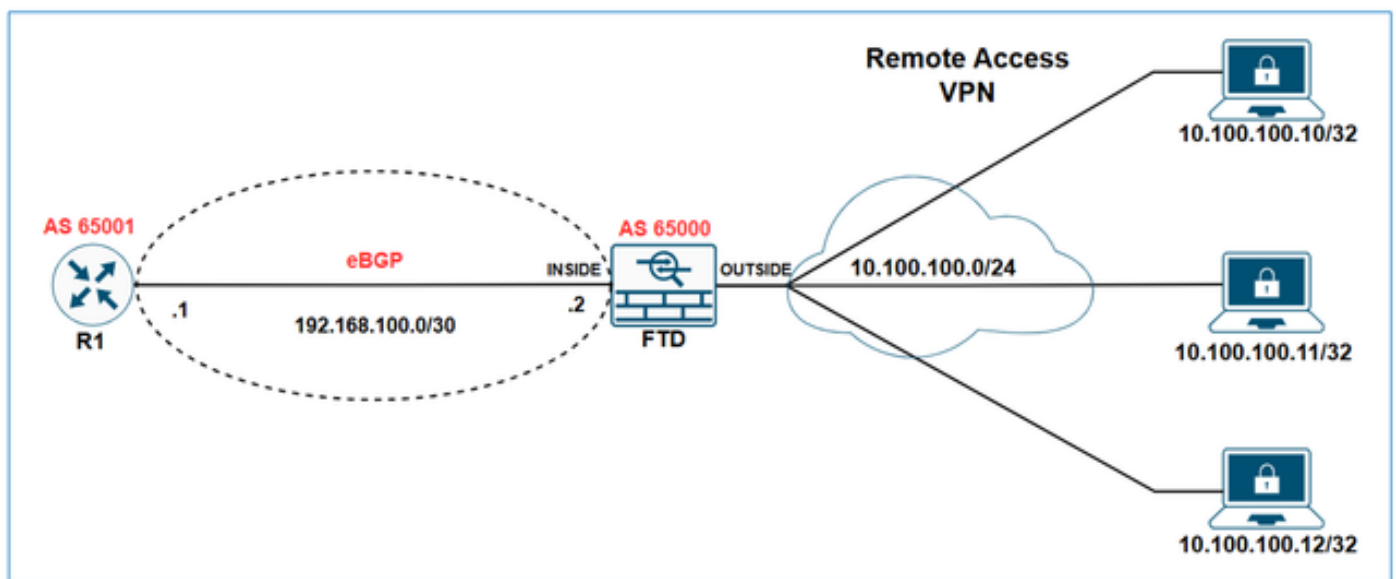
L 192.168.100.1/32 is directly connected, GigabitEthernet1

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

Herdistributie van Remote Access VPN-subnetten via eBGP op FTD

Netwerkdigram



In dit voorbeeld is het doel om R1 het VPN-subnet 10.100.100.0/24 te laten leren via eBGP.

Initiële configuraties

FTD Initiële configuratie:

```
<#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-tabeluitvoer:

```
<#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 toont bgp samenvatting output:

```
<#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 toon ip bgp samenvatting 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

R1 bgp tabeluitvoer:

<#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-routingstabel:

<#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

Configureren

Navigeer in de gebruikersinterface voor apparaatbeheer van de FMC naar Routing > BGP > IPv4 > Redistribution en selecteer vervolgens de knop Toevoegen.

The screenshot shows the Cisco FTD-1 configuration interface for BGP IPv4 Redistribution. The interface is titled "FTD-1" and "Cisco Secure Firewall Threat Defense for VMware". The "Routing" tab is selected, and the "Redistribution" sub-tab is also selected. The "Enable IPv4" checkbox is checked, and the "AS Number" is set to 65000. The "General" sub-tab is selected, and the "Route Injection" section is visible. A table with columns "Source Protocol", "AS Number/Process ID", "Metric", "RouteMap", and "Match" is shown, with a message "No records to display". A red box highlights the "+ Add" button in the top right corner of the table. The left sidebar shows the "Manage Virtual Routers" section, with "Global" selected. The "Virtual Router Properties" section is expanded, showing "ECMP", "BFD", "OSPF", "OSPFv3", "EIGRP", "RIP", and "Policy Based Routing". The "BGP" section is expanded, showing "IPv4" and "IPv6".

Kies in het veld Bronprotocol de optie Statisch en selecteer vervolgens de knop OK.

Add Redistribution



Source Protocol

Static



Process ID*



Metric

(0-4294967295)

Route Map



Match

☐

Internal

☐

External 1

☐

External 2

☐

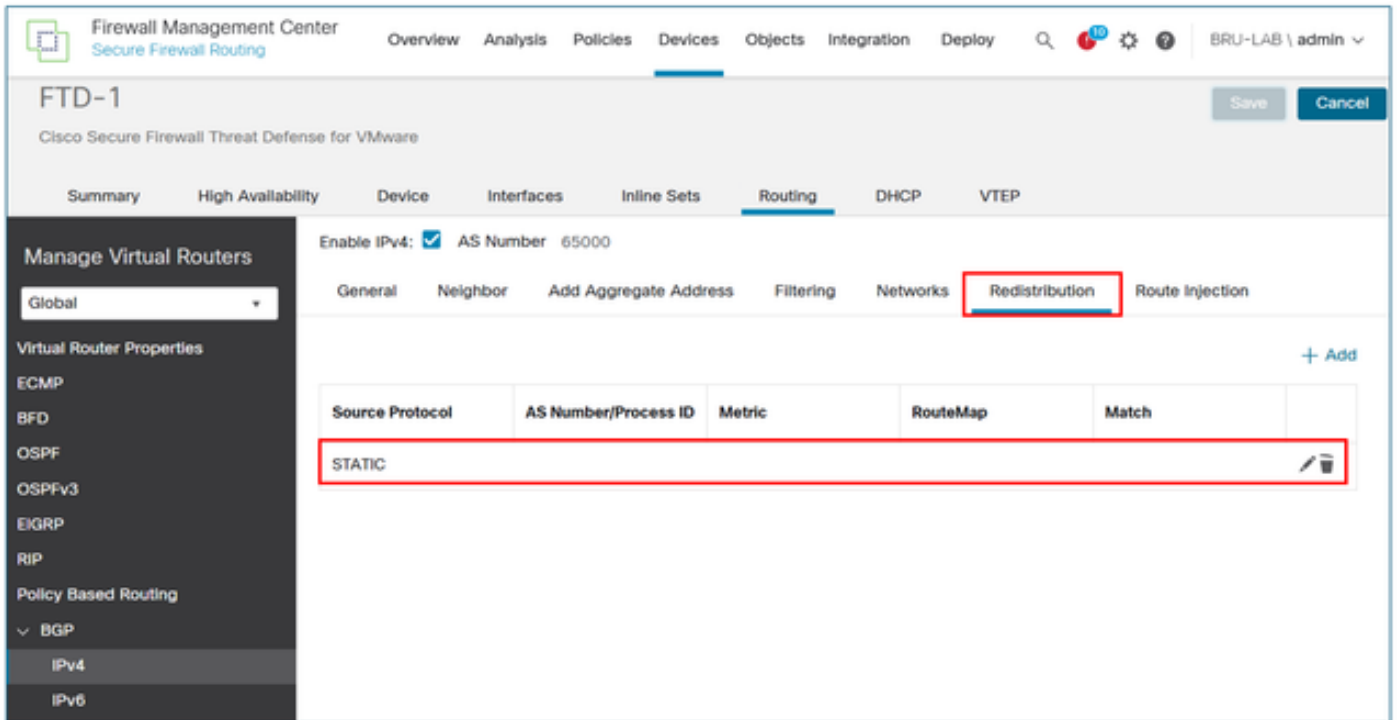
NSSAExternal 1

☐

NSSAExternal 2

 : Dit herverdeelt alle statische routes in BGP. Als u alleen de VPN-subnetten wilt adverteren, kunt u een routekaart toepassen om ze te filteren.

Het resultaat:



The screenshot shows the Firewall Management Center (FMC) interface for FTD-1. The 'Routing' tab is selected, and the 'Redistribution' sub-tab is highlighted with a red box. The 'Source Protocol' is set to 'STATIC', also highlighted with a red box. The 'AS Number' is 65000. The interface includes a sidebar with 'Manage Virtual Routers' and 'Virtual Router Properties' sections. The 'Routing' section has tabs for General, Neighbor, Add Aggregate Address, Filtering, Networks, Redistribution, and Route Injection. The 'Redistribution' tab shows a table with columns for Source Protocol, AS Number/Process ID, Metric, RouteMap, and Match. A single row is visible with 'STATIC' in the Source Protocol column.

Bewaar en implementeer de configuratie op de FTD.

Verifiëren

FTD BGP-configuratie:

<#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
```

FTD bgp-tabeluitvoer:

<#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 ?
---------------------	---------------	---	--	---	---------

R1 bgp tabeluitvoer:

<#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	?

Uitgang routingstabel 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
```

 Tip: Merk op dat hoewel de VPN-pool 10.100.100.0/24 is, de FTD een /32-subnet herverdeelt over BGP. Dit gebeurt omdat de FTD een statische route creëert met een /32 voorvoegsel voor elke VPN-sessie voor externe toegang. Om dit te optimaliseren, kunt u de functie BGP Aggregate Address gebruiken.

BGP Aggregate Address Configuration

Configureren

Als het nog niet is gemaakt, maakt u een netwerkobject voor de VPN-subnetten.

Edit Network Object

Name

VPN-SUBNET

Description

Network

☐ Host

☐ Range

☒ Network

☐ FQDN

10.100.100.0/24

☐ Allow Overrides

Cancel

Save

Navigeer in de gebruikersinterface voor apparaatbeheer van de FMC naar Routing > BGP> IPv4 > Add Aggregate Address (Samengevoegde adressen toevoegen) en selecteer vervolgens de knop Add (Toevoegen).

Firewall Management Center
Secure Firewall Routing

Overview Analysis Policies Devices Objects Integration Deploy BRU-LAB \ admin

FTD-1
Cisco Secure Firewall Threat Defense for VMware

Summary High Availability Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6

Enable IPv4: ☒ AS Number 65000

General Neighbor **Add Aggregate Address** Filtering Networks Redistribution Route Injection

+ Add

Network	Attribute Map	Advertise Map	Suppress Map	AS Set Path	SummaryOnly
No records to display					

Voeg in het veld Netwerk het object voor het VPN-subnet toe en selecteer vervolgens het selectievakje Alle routes filteren uit updates.

Add Aggregate Address



Network*

VPN-SUBNET



Attribute Map



Advertise Map



Suppress Map



☐ Generate AS set path information

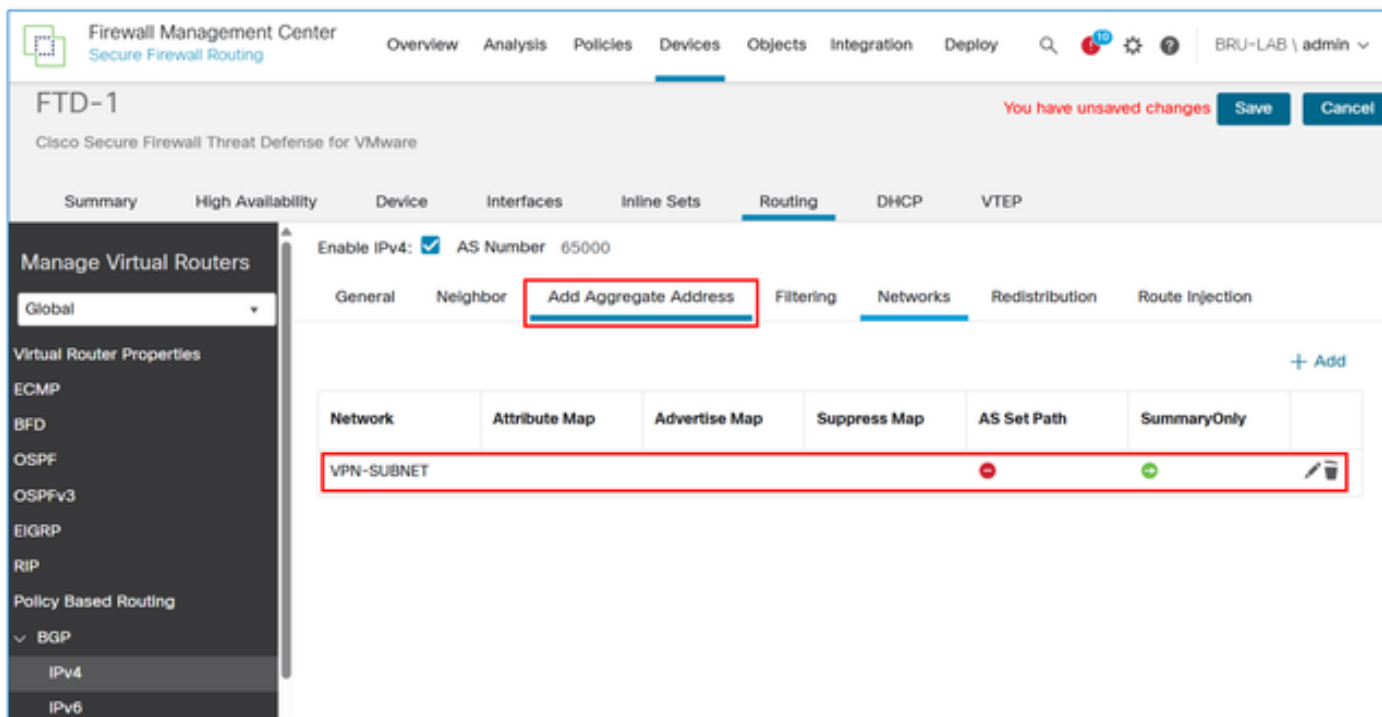
☒ Filter all routes from updates

Cancel

OK

 **Opmerking:** Als het selectievakje Filter alle routes van updates is uitgeschakeld, adverteert de FTD zowel het overzichtsadres als de specifieke /32 VPN-routes via BGP. Wanneer het selectievakje ingeschakeld is, duwt de FMC de opdracht aggregaten-adres samenvatting-only naar de FTD LINA configuratie, zodat alleen het samenvatting adres wordt geadverteerd.

Het resultaat:



The screenshot shows the FMC interface for FTD-1. The 'Routing' tab is active, and the 'Add Aggregate Address' sub-tab is selected. The table below shows the configuration for the aggregate address 'VPN-SUBNET'.

Network	Attribute Map	Advertise Map	Suppress Map	AS Set Path	SummaryOnly
VPN-SUBNET					

Bewaar en implementeer de configuratie op de FTD.

Verifiëren

FTD BGP-configuratie:

<#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
```

FTD BGP-tabeluitvoer:

<#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 ?

R1 BGP-tabeluitvoer:

<#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 ?

Uitgang routeringstabel 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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.