

Advertise Remote Access VPN Subnets Through Routing Protocols in FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Redistribute Remote Access VPN Subnets through EIGRP on FTD](#)

[Network Diagram](#)

[Redistribute Remote Access VPN Subnets through EIGRP on FTD using network statement](#)

[Configure](#)

[Verify](#)

[Redistribute Remote Access VPN Subnets through EIGRP on FTD using the redistribute static approach](#)

[Configure](#)

[Verify](#)

[EIGRP Summary Address Configuration](#)

[Configure](#)

[Verify](#)

[Redistribute Remote Access VPN Subnets through OSPF on FTD](#)

[Network Diagram](#)

[Configure](#)

[Verify](#)

[OSPF Summary Address Configuration](#)

[Configure](#)

[Verify](#)

[Redistribute Remote Access VPN Subnets through eBGP on FTD](#)

[Network Diagram](#)

[Configure](#)

[Verify](#)

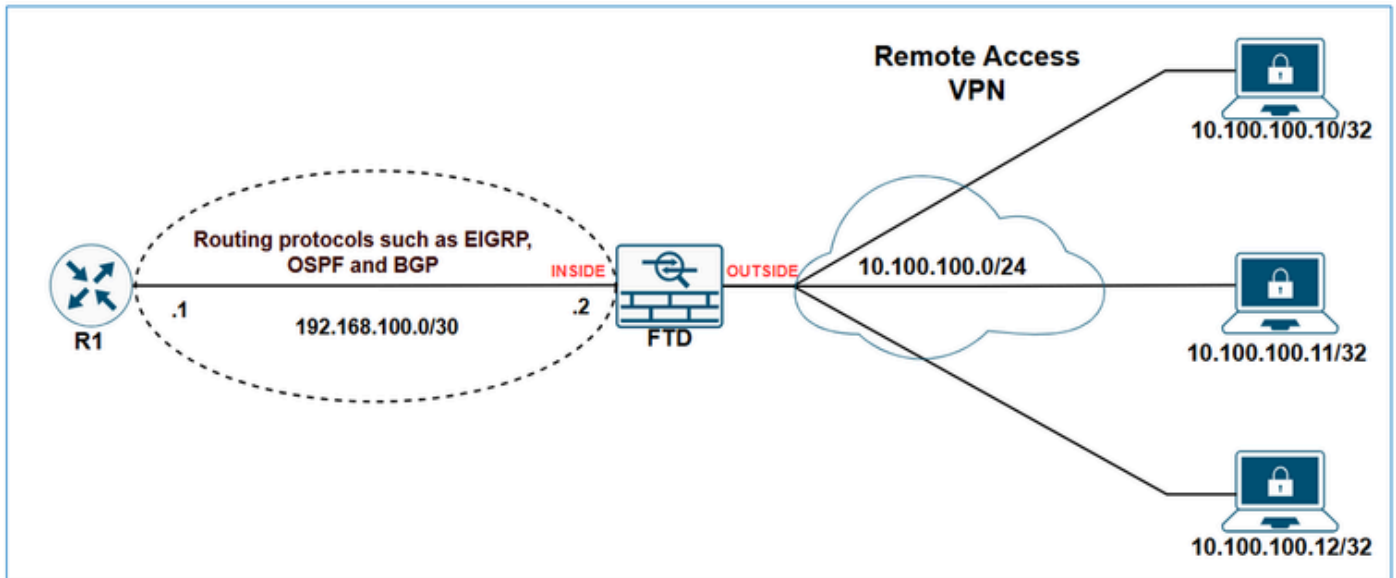
[BGP Aggregate Address Configuration](#)

[Configure](#)

[Verify](#)

Introduction

This document describes the options available for advertising VPN-related subnets using the routing protocols EIGRP, OSPF, and BGP.



Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

The information in this document is based on these software and hardware versions:

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

Note: This document outlines the configuration for redistributing Remote Access VPN subnets through EIGRP, OSPF, and BGP using the FMC. For guidance on route redistribution with FDM, please refer to the [FDM configuration guide](#).

Background Information

The first thing to understand is how the FTD classifies VPN subnets in its routing table. Although these subnets appear as **connected by VPN**, they are not considered directly connected subnets; instead, they are treated as static routes.

The show outputs demonstrate it.

FTD **show route** output:

```
<#root>
```

```
FTD-1#
```

show route

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

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

V      10.100.100.10 255.255.255.255 connected by VPN (advertised), outside
```

FTD show route connected output:

<#root>

FTD-1#

show route connected

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

Gateway of last resort is not set

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

FTD show route static output:

<#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

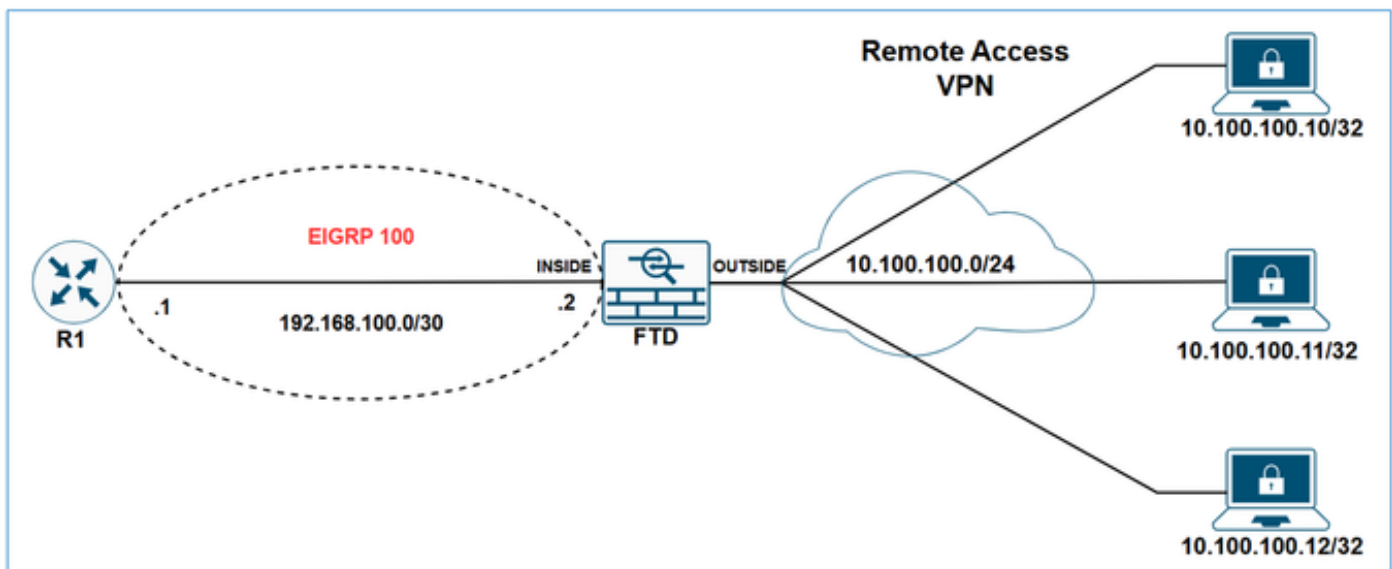
Gateway of last resort is not set

V 10.100.100.10 255.255.255.255 connected by VPN (advertised), outside

Now that it is clear how VPN subnets are treated in the firewall's routing table, the next step is to explore how to advertise them using various routing protocols.

Redistribute Remote Access VPN Subnets through EIGRP on FTD

Network Diagram



Static routes that fall within the scope of a network statement are automatically redistributed to EIGRP; you do not need to define a redistribution rule for them. However, when redistributing static routes that point to VTI interfaces in EIGRP, you must specify the metric. For static routes pointing to other types of interfaces, specifying the metric is not required.

Due to EIGRP's behavior of automatically redistributing static routes that fall within the scope of network statements, there are two options for advertising VPN subnets via EIGRP on FTD:

1. Using a network statement.
2. Using the redistribute static approach.

In this example the goal is to make R1 learn the VPN subnet 10.100.100.0/24 via EIGRP.

FTD initial configuration:

<#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 topology table:

<#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 Initial Routing table:

<#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

Redistribute Remote Access VPN Subnets through EIGRP on FTD using network statement

Configure

Step 1. Create a network object for the VPN subnet.

Edit Network Object

Name

VPN-SUBNET

Description

Network

☐ Host

☐ Range

☒ Network

☐ FQDN

10.100.100.0/24

☐ Allow Overrides

Cancel

Save

Step 2. Include the VPN subnet object in the network statement.

In the FMC device management UI, navigate to **Routing > EIGRP > Setup**, and include the VPN subnet in the **selected networks/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) +

- any-ipv4
- BR-DMZ-NET
- BR-LAN-NET
- HQ-DMZ
- HQ-DMZ-SRV1
- HQ-DMZ-SRV2

Add

Selected Networks/Hosts (2)

- HQ-WAN-1
- VPN-SUBNET**

☐ Passive Interface

Save and **deploy** the configuration on the FTD.

Verify

FTD EIGRP configuration:

```
<#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 topology table:

```
<#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 table:

<#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



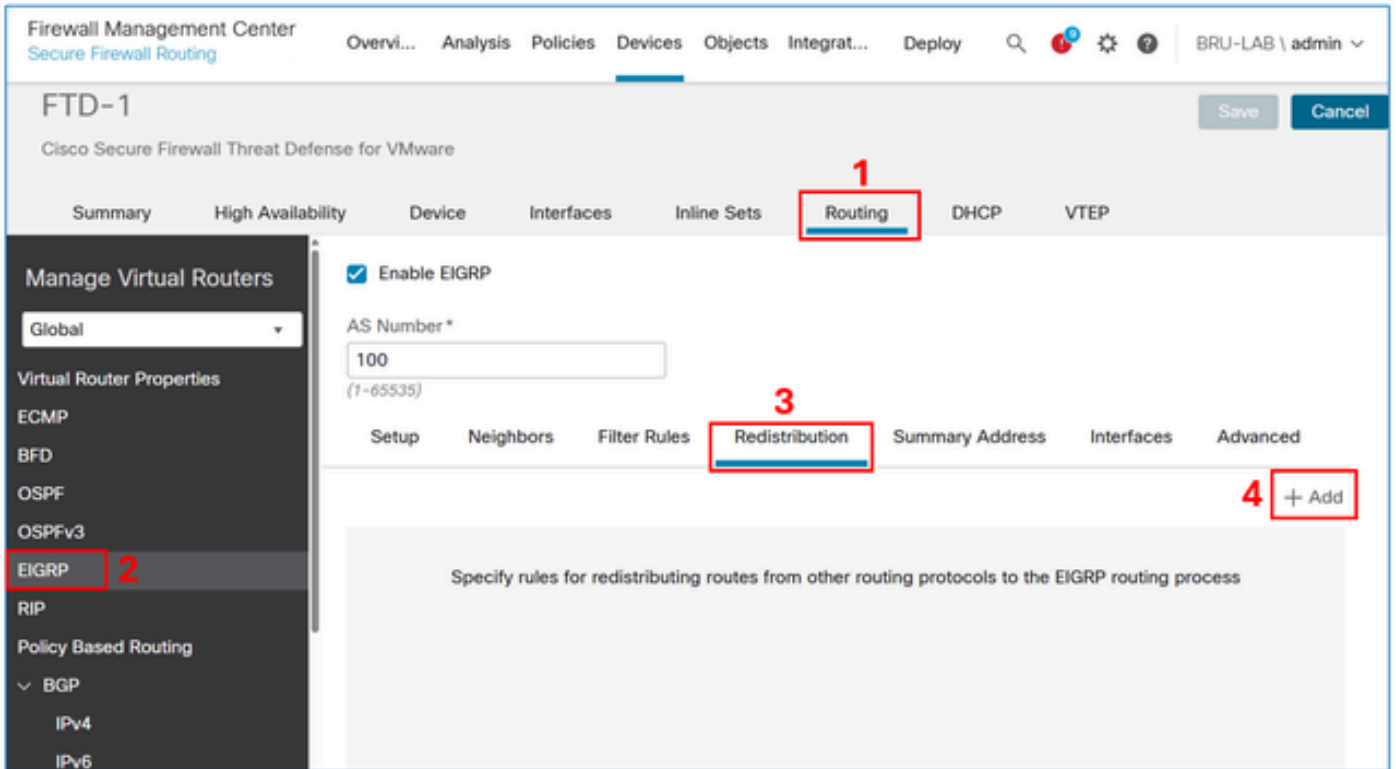
Note: Note that although the network statement was 10.100.100.0/24, the FTD redistributes a /32

 subnet over EIGRP. This occurs because the FTD creates a static route with a /32 prefix for every remote access VPN session. To optimize this, you can use the EIGRP Summary Address feature.

Redistribute Remote Access VPN Subnets through EIGRP on FTD using the redistribute static approach

Configure

In the FMC device management UI, navigate to **Routing > EIGRP > Redistribution**, and then select the **Add** button.



The screenshot displays the Firewall Management Center (FMC) interface for device FTD-1. The navigation path is highlighted with red boxes and numbers: 1. The 'Routing' tab in the top navigation bar. 2. The 'EIGRP' option in the left-hand 'Manage Virtual Routers' sidebar. 3. The 'Redistribution' sub-tab within the EIGRP configuration area. 4. The '+ Add' button in the bottom right corner of the configuration area. The main configuration area shows 'Enable EIGRP' checked and 'AS Number' set to 100. Below the sub-tabs, a message states: 'Specify rules for redistributing routes from other routing protocols to the EIGRP routing process'.

In the protocol field, select **Static**, and then select the **OK** button.

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

 **Caution:** This redistributes all static routes into EIGRP. If you need to advertise only the VPN subnets, you can either use the network statement approach or apply a route map to filter them.

The result:

☒ 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							

Save and **deploy** the configuration on the FTD.

Verify

FTD EIGRP configuration:

<#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 table:

<#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 table:

<#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:** Optionally, you can use the EIGRP summary address feature on FTD to optimize the size of the routing table.

EIGRP Summary Address Configuration

Configure

If it has not been created yet, create a network object for the VPN subnets.

Edit Network Object ?

Name

VPN-SUBNET

Description

Network

☐ Host ☐ Range ☒ Network ☐ FQDN

10.100.100.0/24

☐ Allow Overrides

Cancel Save

In the FMC device management UI, navigate to **Routing > EIGRP > Summary Address**, and then select the **Add** button.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ BRJ-LAB1 admin 🔒 **SECURE**

FTD-1 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

☒ Enable EIGRP

AS Number*
100
(1-65535)

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

+ Add

Configure summary addresses for each interface through which EIGRP advertises routes

In the **interface** field, enter the one facing the EIGRP neighbor, and in the **network** field, enter the object created for the VPN subnet.

Add Summary Address ?

Interface *

inside ▼

Network *

VPN-SUBNET ▼ +

Administrative Distance

(1-255)

Cancel

OK

The result:

☒ Enable EIGRP

AS Number*

100

(1-65535)

Setup Neighbors Filter Rules Redistribution Summary Address Interfaces Advanced

+ Add

Interface	Network	Administrative Distance
inside	VPN-SUBNET	

Verify

FTD EIGRP Summary Address configuration:

<#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 topology table:

<#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 table:

<#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

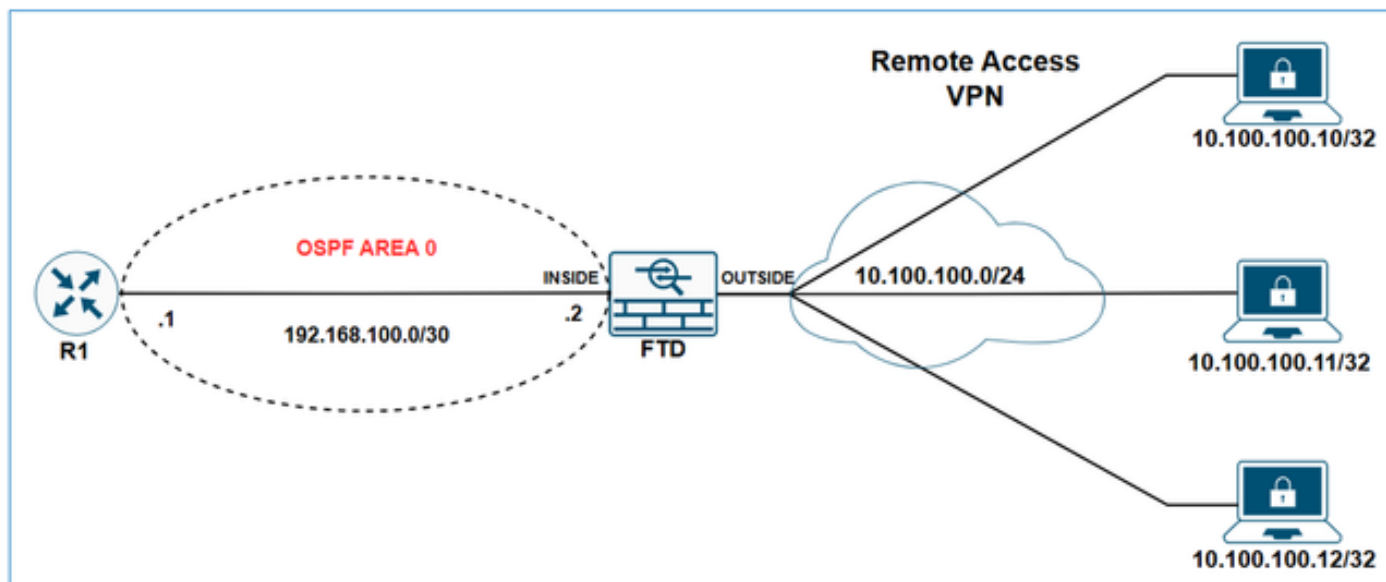
C 192.168.100.0/30 is directly connected, GigabitEthernet1

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

Redistribute Remote Access VPN Subnets through OSPF on FTD

Network Diagram



Initial configurations

<#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** output:

<#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 table:

<#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

Configure

In the FMC device management UI, navigate to **Routing > OSPF > Redistribution**, and then select the **Add** button.

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							



Note: The OSPF role must be set as ASBR or ABR & ASBR to enable redistribution.

In the **Route Type** field, select **Static**, and then check the **Use Subnets** box.

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

 **Caution:** This redistributes all static routes into OSPF. If you need to advertise only the VPN subnets, you can apply a route map to filter them.

The result:

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

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

Verify

FTD OSPF redistribution configuration:

```
<#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 table:

```
<#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:** Note that although the VPN pool is 10.100.100.0/24, the FTD redistributes a /32 subnet over OSPF. This occurs because the FTD creates a static route with a /32 prefix for every remote access VPN session. To optimize this, you can use the OSPF Summary Address feature.

OSPF Summary Address Configuration

Configure

If it has not been created yet, create a network object for the VPN subnets.

Edit Network Object

Name

Description

Network

☐ Host ☐ Range ☒ Network ☐ FQDN

☐ Allow Overrides

Cancel

In the FMC device management UI, navigate to **Routing > OSPF > Summary Address**, and then select the **Add** button.

The screenshot shows the Cisco Firewall Management Center (FMC) interface for device FTD-1. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, Integrations, and Deployment. The left sidebar shows the 'Manage Virtual Routers' section with a dropdown menu set to 'Global'. Under 'Virtual Router Properties', the 'OSPF' option is selected and highlighted with a red box and the number 2. The main content area is titled 'Routing' (highlighted with a red box and the number 1) and contains configuration for two OSPF processes. Process 1 is selected, with its role set to 'ASBR'. Below this, the 'Summary Address' sub-tab is highlighted with a red box and the number 3. At the bottom right of the configuration area, a '+ Add' button is highlighted with a red box and the number 4. The bottom section of the page shows a table with columns for 'OSPF Process', 'Networks', 'Tag', and 'Advertise', currently displaying 'No records to display'.

Add the VPN subnet object and select the **Advertise** checkbox.

Edit Summary Address?

OSPF Process:
1

Available Network +
VPN
VPN-SUBNET 1

Tag:

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

2
Add

Selected Network
VPN-SUBNET

4
Cancel OK

The Result:

☒ 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	 

Verify

FTD OSPF configuration:

```
<#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 table:

```
<#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

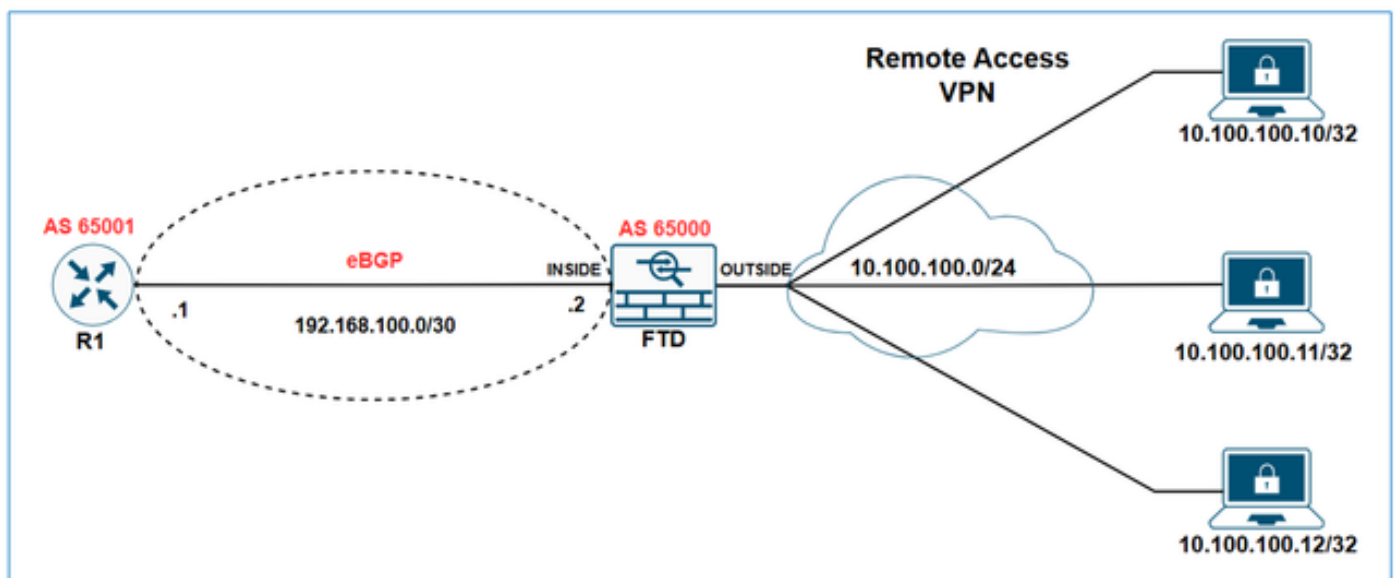
L 192.168.100.1/32 is directly connected, GigabitEthernet1

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

Redistribute Remote Access VPN Subnets through eBGP on FTD

Network Diagram



In this example the goal is to make R1 learn the VPN subnet 10.100.100.0/24 via eBGP.

Initial configurations

FTD Initial configuration:

```
<#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 table output:

```
<#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 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 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

R1 bgp table output:

<#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 table:

<#root>

R1#

show ip route

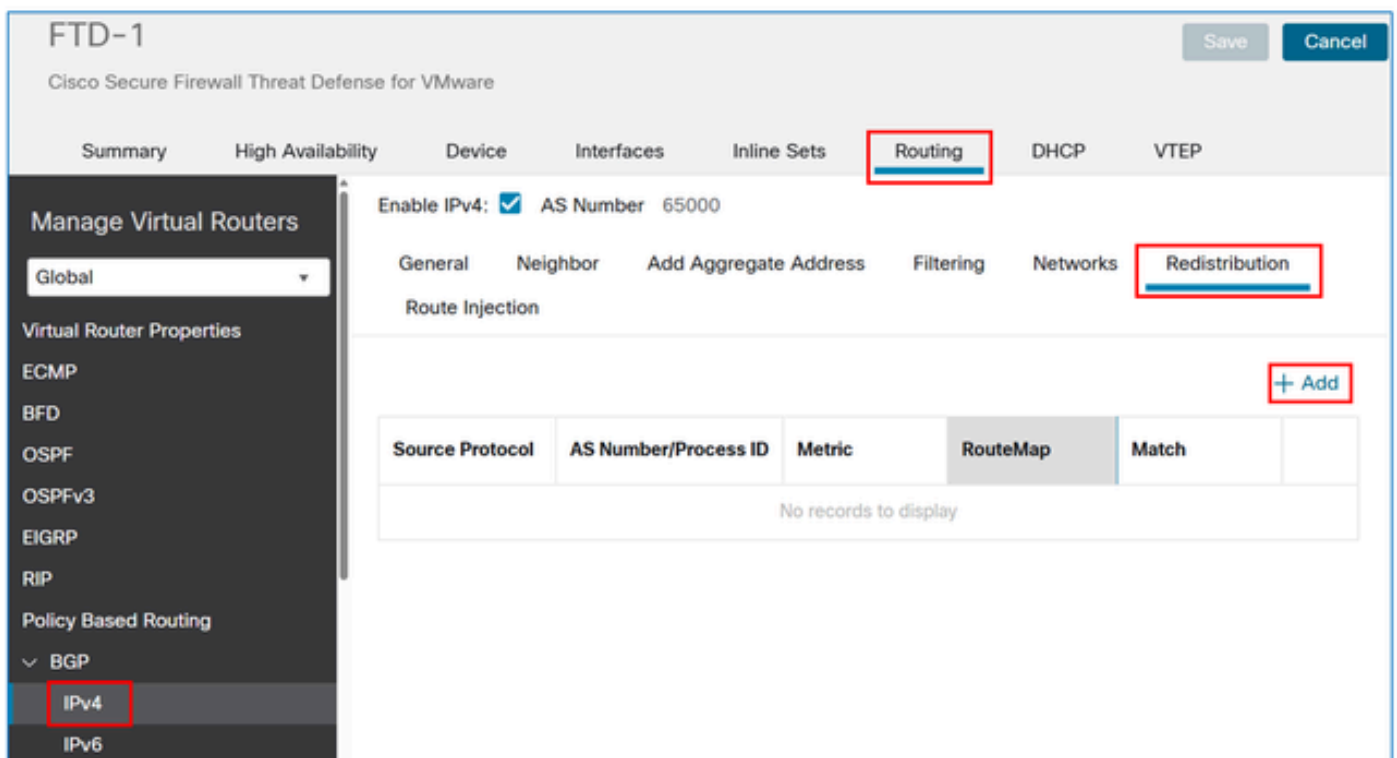
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside,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

Configure

In the FMC device management UI, navigate to **Routing > BGP > IPv4 > Redistribution**, and then select the **Add** button.



In the **Source Protocol** field, choose **Static**, and then select the **OK** button.

Add Redistribution



Source Protocol

Static



Process ID*



Metric

(0-4294967295)

Route Map



Match

☐

Internal

☐

External 1

☐

External 2

☐

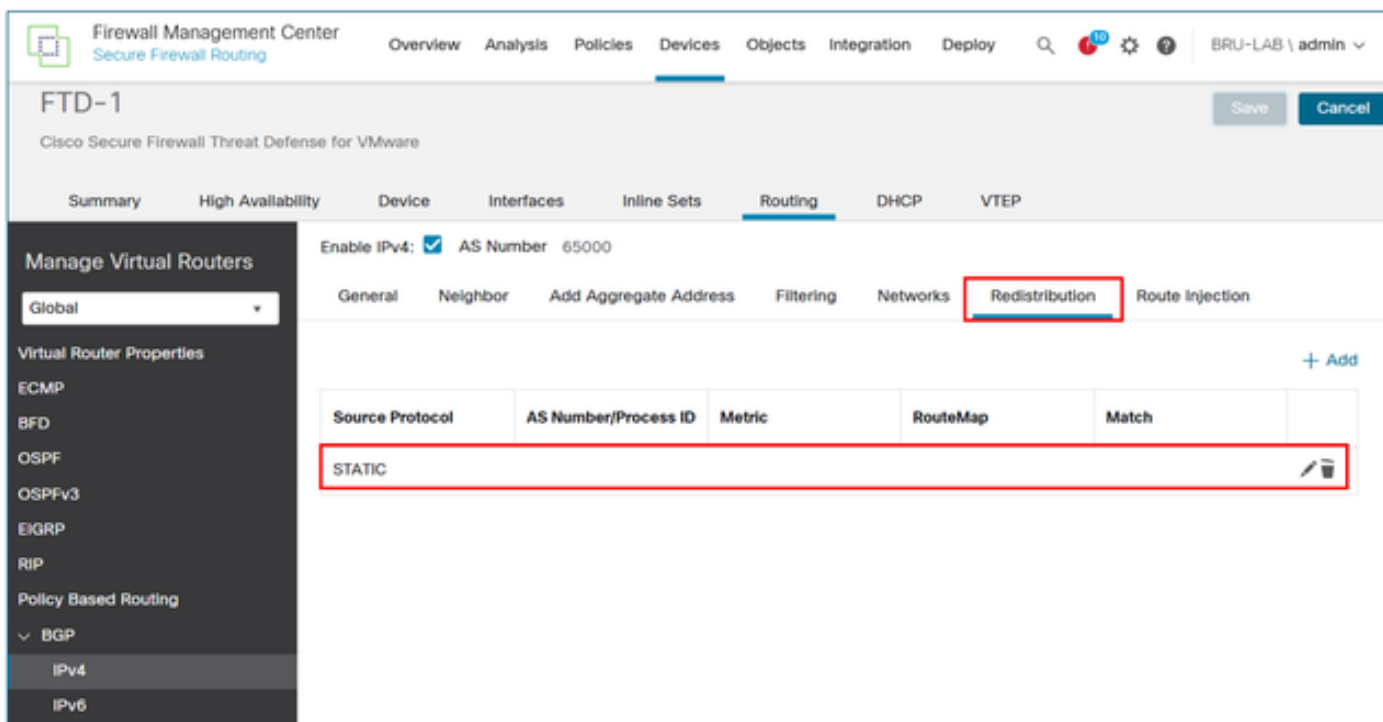
NSSAExternal 1

☐

NSSAExternal 2

 This redistributes all static routes into BGP. If you need to advertise only the VPN subnets, you can apply a route map to filter them.

The result:



Firewall Management Center
Secure Firewall Routing

Overview Analysis Policies Devices Objects Integration Deploy

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

Source Protocol	AS Number/Process ID	Metric	RouteMap	Match
STATIC				

Save and **deploy** the configuration on the FTD.

Verify

FTD BGP configuration:

<#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 table output:

<#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 table output:

<#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	?

R1 routing table output:

<#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: Note that although the VPN pool is 10.100.100.0/24, the FTD redistributes a /32 subnet over BGP. This occurs because the FTD creates a static route with a /32 prefix for every remote access VPN session. To optimize this, you can use the BGP Aggregate Address feature.

BGP Aggregate Address Configuration

Configure

If it has not been created yet, create a network object for the VPN subnets.

Edit Network Object

Name

VPN-SUBNET

Description

Network

☐ Host

☐ Range

☒ Network

☐ FQDN

10.100.100.0/24

☐ Allow Overrides

Cancel

Save

In the FMC device management UI, navigate to **Routing > BGP > IPv4 > Add Aggregate Address**, and then select the **Add** button.

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					

In the network field, add the object for the VPN subnet, and then select the **Filter all routes from updates** checkbox.

Add Aggregate Address



Network*

VPN-SUBNET



Attribute Map



Advertise Map



Suppress Map



☐ Generate AS set path information

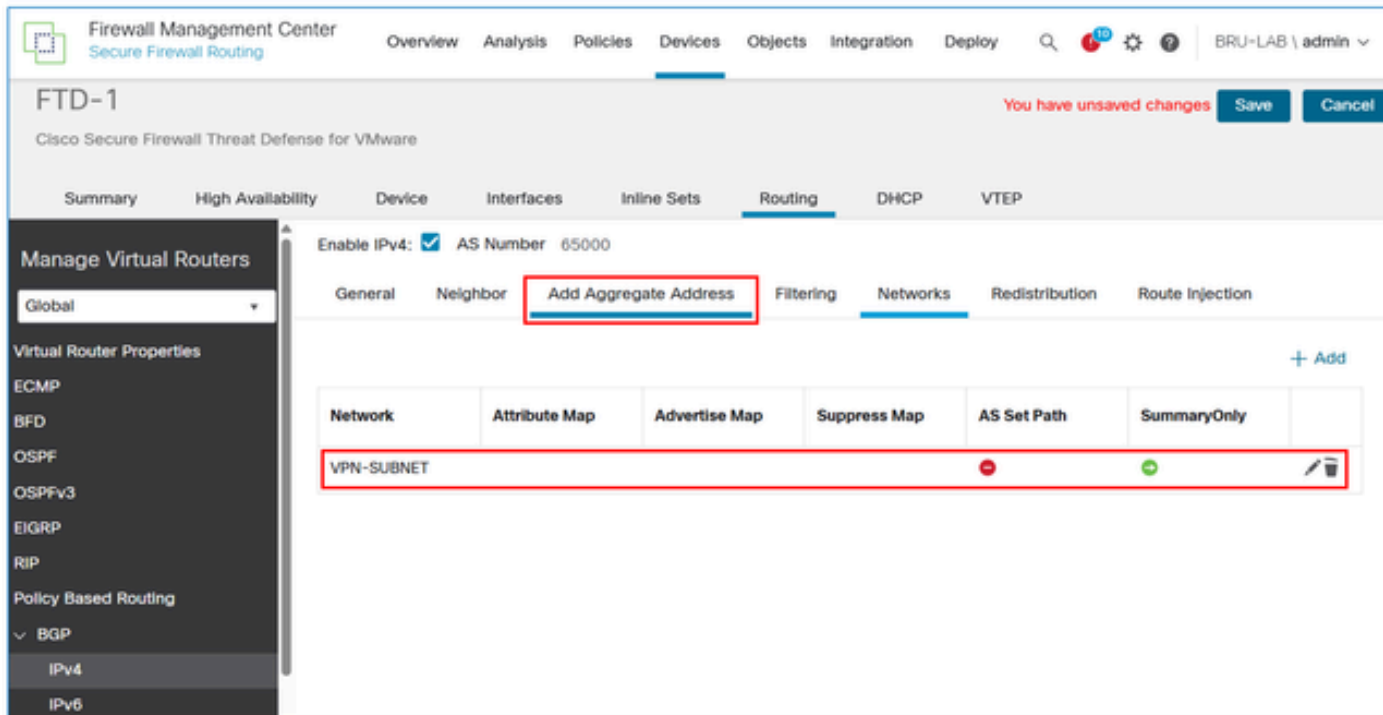
☒ Filter all routes from updates

Cancel

OK

 **Note:** If the **Filter all routes from updates** checkbox is unchecked, the FTD advertise both the summary address and the specific /32 VPN routes over BGP. When the checkbox is enabled, the FMC pushes the command **aggregate-address summary-only** to the FTD LINA configuration, ensuring that only the summary address is advertised.

The result:



The screenshot shows the FMC interface for FTD-1. The 'Routing' tab is active, and the 'Add Aggregate Address' sub-tab is highlighted. A table below shows the configuration for 'VPN-SUBNET' with 'SummaryOnly' checked.

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

Save and **deploy** the configuration on the FTD.

Verify

FTD BGP configuration:

```
<#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 table output:

```
<#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 table output:

```
<#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	?

R1 routing table output:

<#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