

# 在FTD中通過路由協定通告遠端訪問VPN子網

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[通過FTD上的EIGRP重新分配遠端訪問VPN子網](#)

[網路圖表](#)

[使用network語句通過FTD上的EIGRP重新分發遠端訪問VPN子網](#)

[設定](#)

[驗證](#)

[使用redistribute static方法通過FTD上的EIGRP重新分發遠端訪問VPN子網](#)

[設定](#)

[驗證](#)

[EIGRP摘要地址配置](#)

[設定](#)

[驗證](#)

[通過FTD上的OSPF重新分發遠端訪問VPN子網](#)

[網路圖表](#)

[設定](#)

[驗證](#)

[OSPF摘要地址配置](#)

[設定](#)

[驗證](#)

[透過FTD上的eBGP重新分佈遠端存取VPN子網](#)

[網路圖表](#)

[設定](#)

[驗證](#)

[BGP彙總位址組態](#)

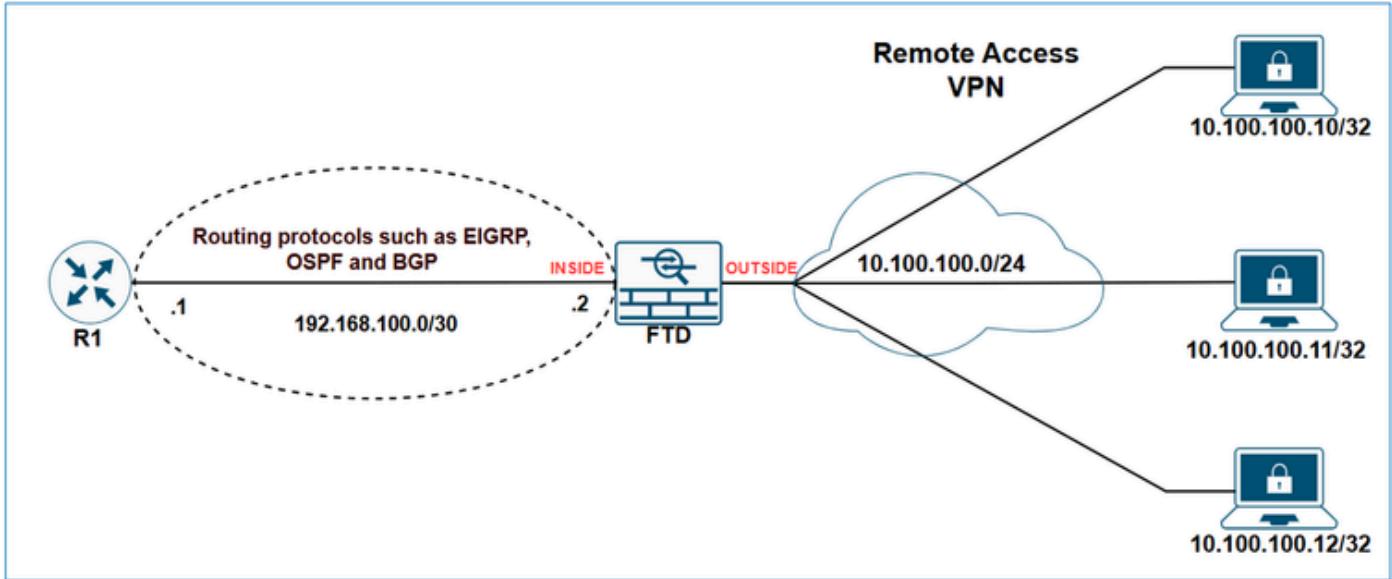
[設定](#)

[驗證](#)

---

## 簡介

本文檔介紹使用路由協定EIGRP、OSPF和BGP通告VPN相關子網的可用選項。



## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆管理中心7.6.0
- 思科安全防火牆7.6.0

 附註：本文檔概述了使用FMC通過EIGRP、OSPF和BGP重新分配遠端接入VPN子網的配置。有關使用FDM重新分發路由的指導，請參閱[FDM配置指南](#)。

## 背景資訊

首先要瞭解的是FTD如何在其路由表中對VPN子網進行分類。雖然這些子網看起來是通過VPN連線的，但是它們不被視為直接連線的子網；相反，它們被視為靜態路由。

show輸出會顯示此情況。

FTD show route輸出：

```
<#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

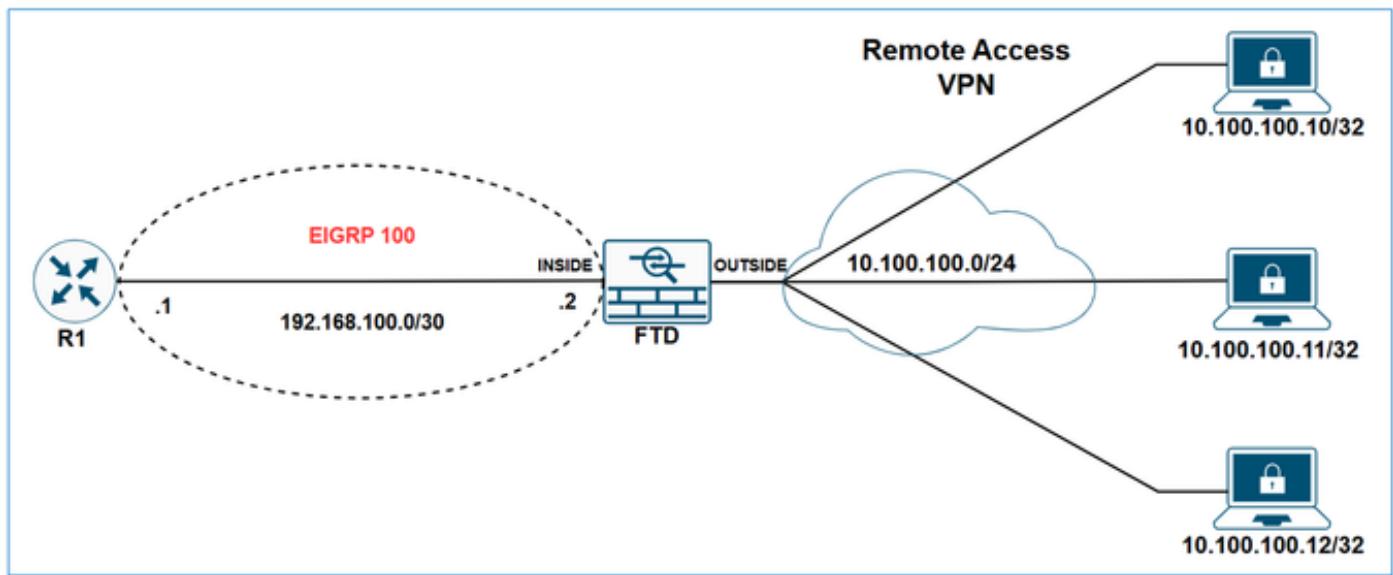
Gateway of last resort is not set

v 10.100.100.10 255.255.255.255 connected by VPN (advertised), outside

現在我們已經清楚如何在防火牆的路由表中處理VPN子網，下一步是探索如何使用各種路由協定來通告這些子網。

## 通過FTD上的EIGRP重新分配遠端訪問VPN子網

### 網路圖表



屬於network語句範圍的靜態路由會自動重新分發到EIGRP;您無需為其定義重分發規則。但是，重新分發指向EIGRP中VTI介面的靜態路由時，必須指定度量。對於指向其他型別介面的靜態路由，不需要指定度量。

由於EIGRP自動重分佈屬於network語句範圍的靜態路由的行為，因此在FTD上通過EIGRP通告VPN子網有兩個選項：

1. 使用network語句
2. 使用redistribute靜態方法。

在本示例中，目標是讓R1通過EIGRP瞭解VPN子網10.100.100.0/24。

FTD初始設定：

```

<#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初始路由表：

```

<#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初始EIGRP拓撲表：

```
<#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初始路由表：

```
<#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 - LISPs
       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
```

## 使用network語句通過FTD上的EIGRP重新分發遠端訪問VPN子網

設定

步驟1.為VPN子網建立網路對象。

## Edit Network Object



Name

Description

Network

Host     Range     Network     FQDN

Allow Overrides

[Cancel](#)

[Save](#)

步驟2.在network語句中包含VPN子網對象。

在FMC裝置管理UI中，導航到Routing > EIGRP > Setup，並將VPN子網包含在選定的網絡/主機中。

The screenshot shows the Firewall Management Center interface for FTD-1. The top navigation bar includes Overview, Analysis, Policies, Devices (selected), Objects, and Integration. Below the navigation is a sub-header for Cisco Secure Firewall Threat Defense for VMware. The main content area has tabs for Summary, High Availability, Device, Interfaces, Inline Sets, **Routing** (selected and highlighted with a red box), DHCP, and VTEP. On the left, a sidebar titled 'Manage Virtual Routers' shows a dropdown set to 'Global' and lists protocols: ECMP, BFD, OSPF, OSPFv3, **EIGRP** (highlighted with a red box), RIP, Policy Based Routing, BGP (IPv4 and IPv6), Static Route, Multicast Routing, IGMP, and PIM. The 'EIGRP' section is expanded, showing the AS Number (100) and other options like Auto Summary, Available Networks/Hosts (any-ipv4, BR-DMZ-NET, BR-LAN-NET, HQ-DMZ, HQ-DMZ-SRV1, HQ-DMZ-SRV2), Selected Networks/Hosts (HQ-WAN-1, VPN-SUBNET), and Passive Interface. A red box labeled '1' highlights the 'Routing' tab, '2' highlights the 'EIGRP' entry in the sidebar, '3' highlights the AS Number input field, and '4' highlights the 'VPN-SUBNET' entry in the selected networks list.

儲存並部署FTD上的組態。

## 驗證

FTD EIGRP配置：

```
<#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拓撲表：

```
<#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路由表：

```
<#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

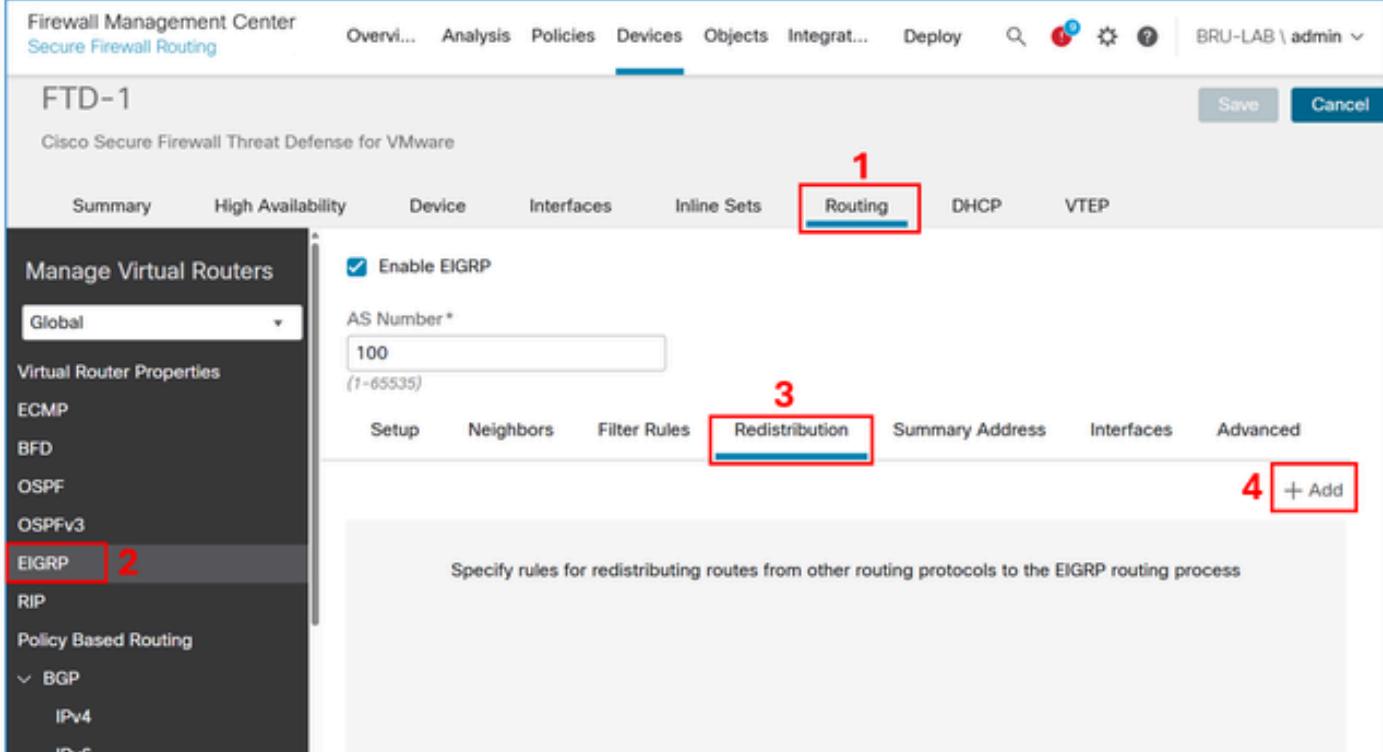
[90/3072] via 192.168.100.2, 00:02:17, GigabitEthernet1
```

 附註：請注意，雖然network語句是10.100.100.0/24，但FTD會通過EIGRP重新分配/32子網。發生這種情況的原因是FTD為每個遠端訪問VPN會話建立字首為/32的靜態路由。要最佳化此功能，您可以使用EIGRP摘要地址功能。

## 使用redistribute static方法通過FTD上的EIGRP重新分發遠端訪問VPN子網

### 設定

在FMC裝置管理UI中，導航到Routing > EIGRP > Redistribution，然後選擇Add按鈕。



The screenshot shows the FMC (Firewall Management Center) interface for configuring EIGRP routing. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, Integration, Deploy, and several icons. The current device is 'FTD-1' (Cisco Secure Firewall Threat Defense for VMware). The main content area is titled 'Manage Virtual Routers' and shows 'Global' selected under 'Virtual Router Properties'. On the left sidebar, 'EIGRP' is highlighted with a red box and the number '2'. The main configuration area has a 'Enable EIGRP' checkbox checked and an 'AS Number' field set to '100'. Below these, there are tabs for Setup, Neighbors, Filter Rules, **Redistribution** (which is highlighted with a red box and the number '3'), Summary Address, Interfaces, and Advanced. A large red box labeled '4' surrounds the '+ Add' button at the bottom right of the redistribution configuration area.

在協定欄位中，選擇Static，然後選擇OK按鈕。

## Add Redistribution



### Protocol

Protocol \*

### Optional OSPF Redistribution

- Internal
- External1
- External2
- Nssa-External1
- Nssa-External2

### Optional Metrics

Bandwidth

(1-4294967295 in kbps)

Delay Time

(0-4294967295 in 10<sup>-6</sup>s)

Reliability

(0-255)

Loading

(1-255)

MTU

(1-65535 in Bytes)

Route Map



Cancel

OK

**⚠ 注意：**這會將所有靜態路由重分發到EIGRP。如果您只需要通告VPN子網，則可以使用 network語句方法或應用路由對映來過濾它們。

結果是：

The screenshot shows the FTD EIGRP configuration interface. At the top, there is a checkbox labeled 'Enable EIGRP'. Below it, the 'AS Number' is set to '100'. The 'Redistribution' tab is selected, indicated by a red border around the tab name. Under the 'Redistribution' tab, there is a table with columns: Protocol, ID, Bandwidth, Delay Time, Reliability, Loading, MTU, and Route Map. A single row is present in the table, labeled 'STATIC'. A red box highlights both the 'Redistribution' tab and the 'STATIC' row.

儲存並部署FTD上的組態。

## 驗證

FTD EIGRP配置：

```
<#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拓撲表：

```
<#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路由表：

```
<#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
```

---

 提示：或者，可以使用FTD上的EIGRP摘要地址功能來最佳化路由表的大小。

---

## EIGRP摘要地址配置

### 設定

如果尚未建立，請為VPN子網建立網路對象。

## Edit Network Object



### Name

### Description

### Network

 Host     Range     Network     FQDN Allow Overrides

在FMC裝置管理UI中，導航到Routing > EIGRP > Summary Address，然後選擇Add按鈕。

The screenshot shows the Cisco FMC Device Management interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices (selected), Objects, and Integration. On the right, there are buttons for Deploy, Save, and Cancel.

The main content area is titled "FTD-1" and "Cisco Secure Firewall Threat Defense for VMware". It features a sidebar with options like Summary, High Availability, Device, Interfaces, Inline Sets, Routing (selected), DHCP, and VTEP. The "Virtual Router Properties" section is expanded, showing "ECMP", "BFD", "OSPF", "OSPFv3", "EIGRP" (selected), "IGP", and "Policy Based Routing" (with "BGP", "IPv4", and "IPv6" sub-options). Under "EIGRP", the "Enable EIGRP" checkbox is checked, and the "AS Number" is set to 100. The "Summary Address" tab is selected in the "Setup" sub-section, which contains a note: "Configure summary addresses for each interface through which EIGRP advertises routes". A red box highlights the "Summary Address" tab, and another red box highlights the "+ Add" button at the bottom right of the configuration area.

在interface欄位中輸入面向EIGRP鄰居的對象，在network欄位中輸入為VPN子網建立的對象。

## Add Summary Address

Interface \*

inside

Network \*

VPN-SUBNET

Administrative Distance

(1-255)

Cancel

OK

結果是：

Enable EIGRP

AS Number \*

100  
(1-65535)

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

+ Add

Interface	Network	Administrative Distance
inside	VPN-SUBNET	

## 驗證

FTD EIGRP摘要地址配置：

```
<#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拓撲表：

```
<#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路由表：

```
<#root>

R1#
show ip route

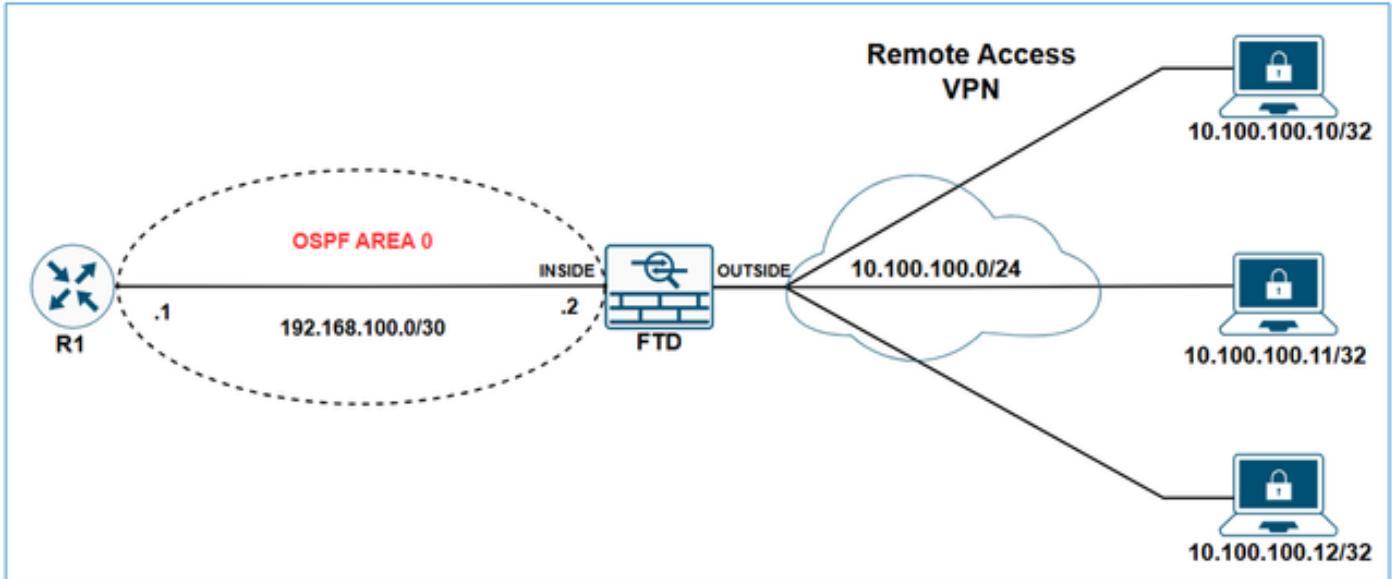
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
      n - NAT, Ni - NAT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

通過FTD上的OSPF重新分發遠端訪問VPN子網

網路圖表



## 初始配置

```
<#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路由表：

```
<#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
```

## 設定

在FMC裝置管理UI中，導航到Routing > OSPF > Redistribution，然後選擇Add按鈕。

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**

No records to display

附註：必須將OSPF角色設定為ASBR或ABR和ASBR才能啟用重分發。

在Route Type欄位中，選擇Static，然後選中Use Subnets框。

## 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

**⚠ 注意：**這會將所有靜態路由重分發到OSPF。如果您只需要通告VPN子網，則可以應用路由對映來過濾這些子網。

結果是：

The screenshot shows a configuration interface for OSPF processes. At the top, there are two sections for Process 1 and Process 2. Process 1 is selected, with its ID set to 1 and OSPF Role set to ASBR. An 'Advanced' button is available for this section. Process 2 is unselected. Below this, there is another section for OSPF Role, with Internal Router selected and an 'Advanced' button.

Below the process sections, there is a navigation bar with tabs: Area, Redistribution, InterArea, Filter Rule, Summary Address, and Interface. The 'Redistribution' tab is currently active. To the right of the tabs is a '+ Add' button.

The main area displays a table for redistribution rules. The columns are labeled: OSPF Process, Route Type, Match, Subnets, Metric Value, Metric Type, Tag Value, and Route Map. A single row is present in the table:

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

## 驗證

FTD OSPF重分發配置：

```
<#root>
FTD-1#
sh run router

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

R1路由表：

```
<#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
```

---

 提示：請注意，雖然VPN池是10.100.100.0/24，但FTD會通過OSPF重新分配/32子網。發生這種情況的原因是FTD為每個遠端訪問VPN會話建立字首為/32的靜態路由。要最佳化此功能，您可以使用OSPF摘要地址功能。

---

## OSPF摘要地址配置

### 設定

如果尚未建立，請為VPN子網建立網路對象。

## Edit Network Object



Name

Description

Network

Host     Range     Network     FQDN

Allow Overrides

[Cancel](#)

[Save](#)

在FMC裝置管理UI中，導航到Routing > OSPF> Summary Address，然後選擇Add按鈕。

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** (1) DHCP VTEP

Manage Virtual Routers

Global (2)

Virtual Router Properties

ECMP

BFD

OSPF (3)

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	<b>Summary Address</b>	Interface
No records to display					

+ Add (4)

新增VPN子網對象並選中Advertise覈取方塊。

## Edit Summary Address



OSPF Process:

1

Available Network + C

Q VPN X

VPN-SUBNET 1

2

Add

Selected Network

VPN-SUBNET



Tag:

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

3

4

Cancel

OK

結果：

Process 1      ID: 1

OSPF Role:

Process 2      ID:

OSPF Role:

Area	Redistribution	InterArea	Filter Rule	Summary Address	Interface
<a href="#">+ Add</a>					
OSPF Process	Networks	Tag	Advertise		
1	VPN-SUBNET	true			

## 驗證

FTD OSPF配置：

```
<#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路由表：

```
<#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

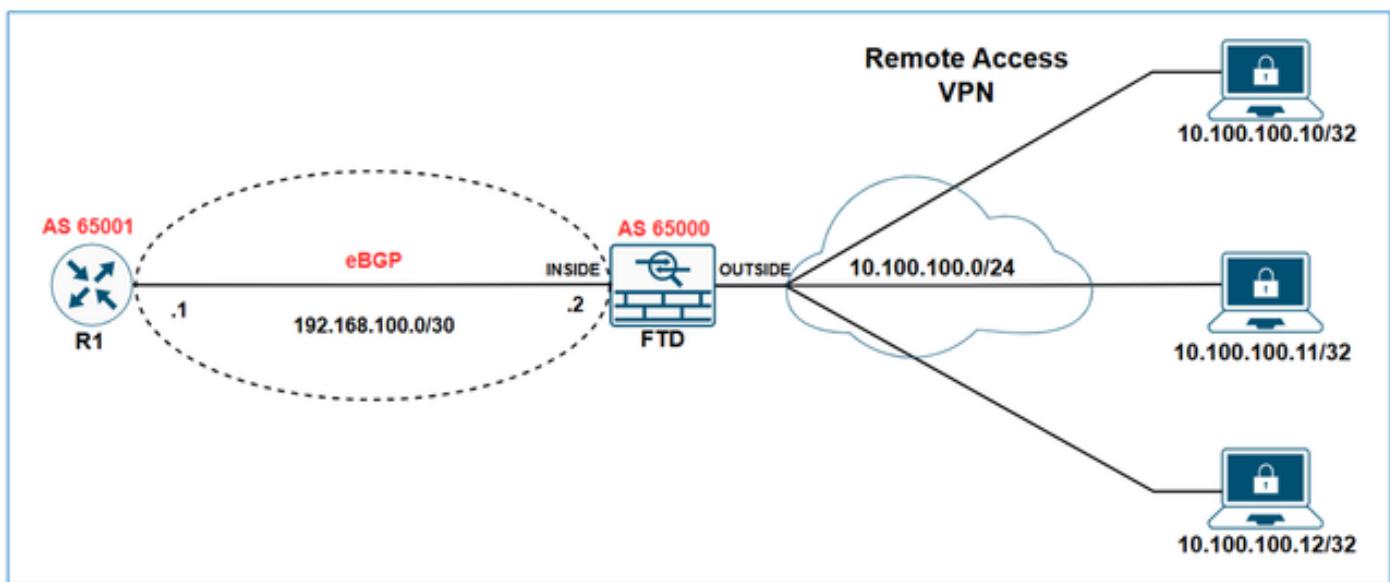
Gateway of last resort is not set

```

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
  
```

## 透過FTD上的eBGP重新分佈遠端存取VPN子網

### 網路圖表



在本示例中，目標是讓R1通過eBGP學習VPN子網10.100.100.0/24。

### 初始配置

FTD初始設定：

```

<#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表輸出：

```
<#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輸出：

```
<#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表輸出：

```
<#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路由表：

```
<#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
```

## 設定

在FMC裝置管理UI中，導航到Routing > BGP > IPv4 > Redistribution，然後選擇Add按鈕。

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

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
No records to display				

在「Source Protocol」欄位中，選擇「Static」，然後選擇「OK」按鈕。

# Add Redistribution



## Source Protocol

Static

## Process ID\*

## Metric

(0-4294967295)

## Route Map

 +

## Match

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

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。