在FMC上使用HTTP路徑監視器配置PBR

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

[設定](#)

- [網路圖表](#)
- [為HTTP路徑監控配置PBR](#)
- [設定等價多重路徑(ECMP)](#)
- [為安全FTD設定受信任DNS](#)
- [啟用路徑監控](#)
- [新增監控儀表板](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹如何在思科安全防火牆管理中心(FMC)上使用HTTP路徑監控來設定原則型路由(PBR)。

必要條件

需求

思科建議您瞭解以下主題：

- PBR基礎知識
- 基本Cisco Secure Management Center體驗
- 基本思科安全防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行7.4版本的Cisco Secure Firewall Management Center Virtual(FMCv)VMware
- 執行7.4版的Cisco安全防火牆威脅防禦虛擬裝置(FTDv)VMware

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。

背景資訊

在傳統路由中，資料包根據目的IP地址進行路由，但是在基於目的地的路由系統中很難更改指定流量的路由。PBR通過擴展和補充由路由協定提供的現有機制，使您能夠更好地控制路由。

PBR允許設定IP優先順序。它還允許為某些流量指定路徑，例如高成本鏈路上的優先順序流量。使用PBR時，路由基於目標網路以外的標準，例如源埠、目標地址、目標埠、協定應用程式或這些對象的組合。PBR可用於根據應用程式、使用者名稱、組成員身份和安全組關聯對網路流量進行分類。此路由方法適用於大型網路部署中大量裝置訪問應用程式和資料的情況。傳統上，大型部署採用在基於路由的VPN中將所有網路流量回傳到集線器的拓撲，將其作為加密流量。這些拓撲經常會導致資料包延遲、頻寬減少和資料包丟棄等問題。

PBR僅在路由防火牆模式下受支援，並且不適用於Embryonic連線。物理、埠通道、子介面和狀態隧道介面支援基於HTTP的應用程式。群集裝置不支援該功能。

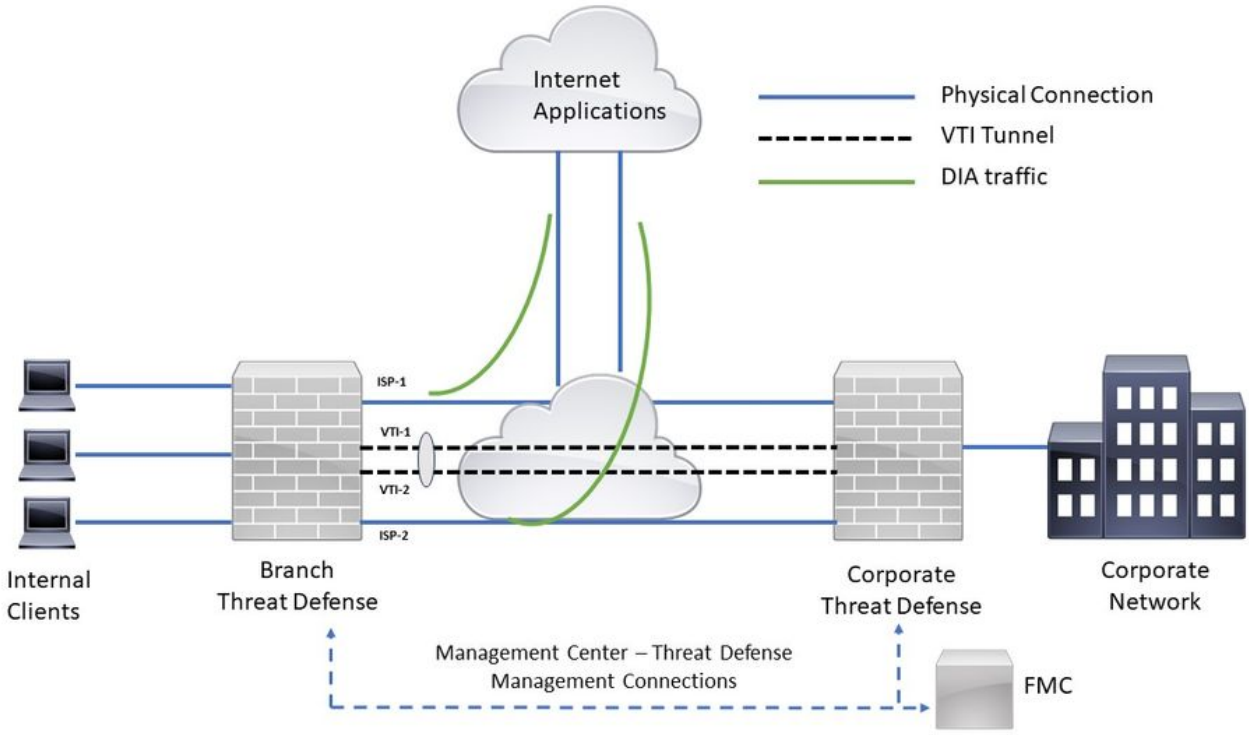
當配置的介面獲取諸如往返時間(RTT)、抖動、平均意見得分(MOS)和每個介面的資料包丟失等度量時，它們用於確定路由PBR流量的最佳路徑。路徑監控為每個介面計算多個遠端對等點的靈活度量。為了透過分支機構防火牆上的原則監控和判斷多個應用的最佳路徑，建議使用HTTP而不是ICMP，原因如下：

- HTTP-ping可以得出通向該伺服器的應用層（該應用位於該應用所在的位置）的路徑的效能度量。
- 每當更改應用伺服器IP地址時，更改防火牆配置的需要都會被刪除，因為會跟蹤應用域而非IP地址。

設定

網路圖表

考慮典型的企業網路場景，其中所有分支機構網路流量均通過企業網路的基於路由的VPN傳送，並在需要時分流到外網。下一個拓撲顯示了通過基於路由的VPN連線到公司網路的分支機構網路。傳統上，企業威脅防禦配置為同時處理分支機構的內部和外部流量。通過PBR策略，分支機構威脅防禦配置了一個策略，該策略將特定流量路由到WAN網路而不是虛擬隧道。其餘流量如往常一樣通過基於路由的VPN。



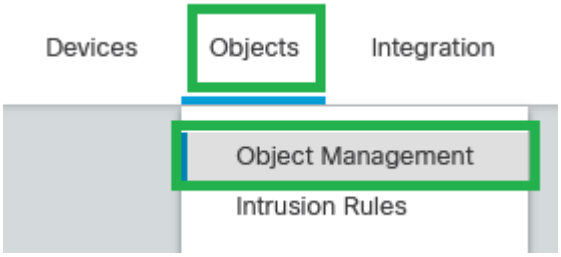
網路拓撲

「配置」部分假設ISP和VTI介面已在安全FMC中針對分支機構威脅防禦進行了配置。

為HTTP路徑監控配置PBR

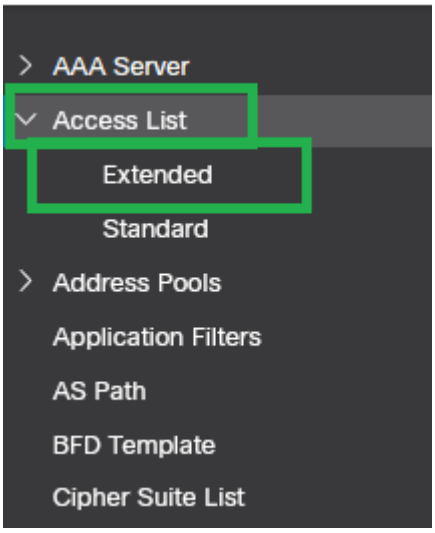
此配置部分顯示了ISP-1和ISP-2介面上的路徑監控配置。

步驟1.為受監控的應用程式建立擴展訪問清單。前往 。Objects > Object Management



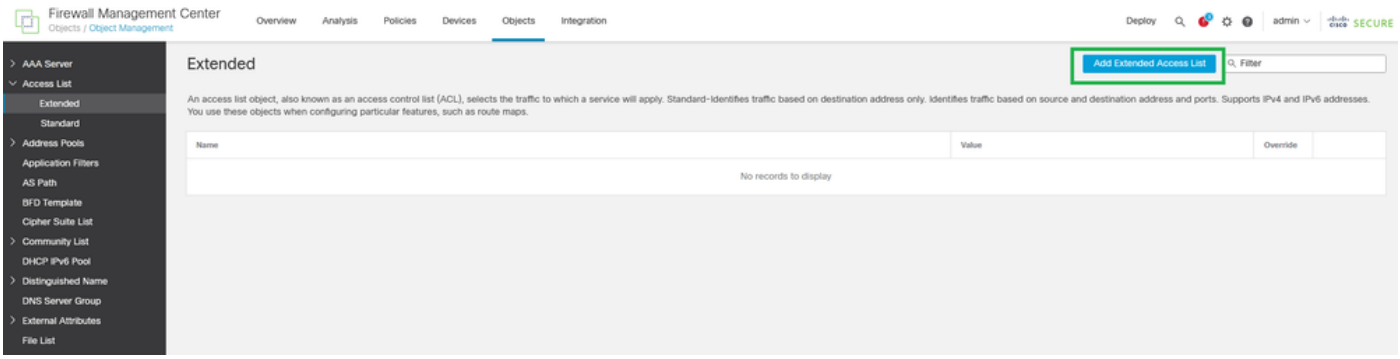
對象 — 對象管理

步驟2.導覽至Access-list > Extended左側選單上。



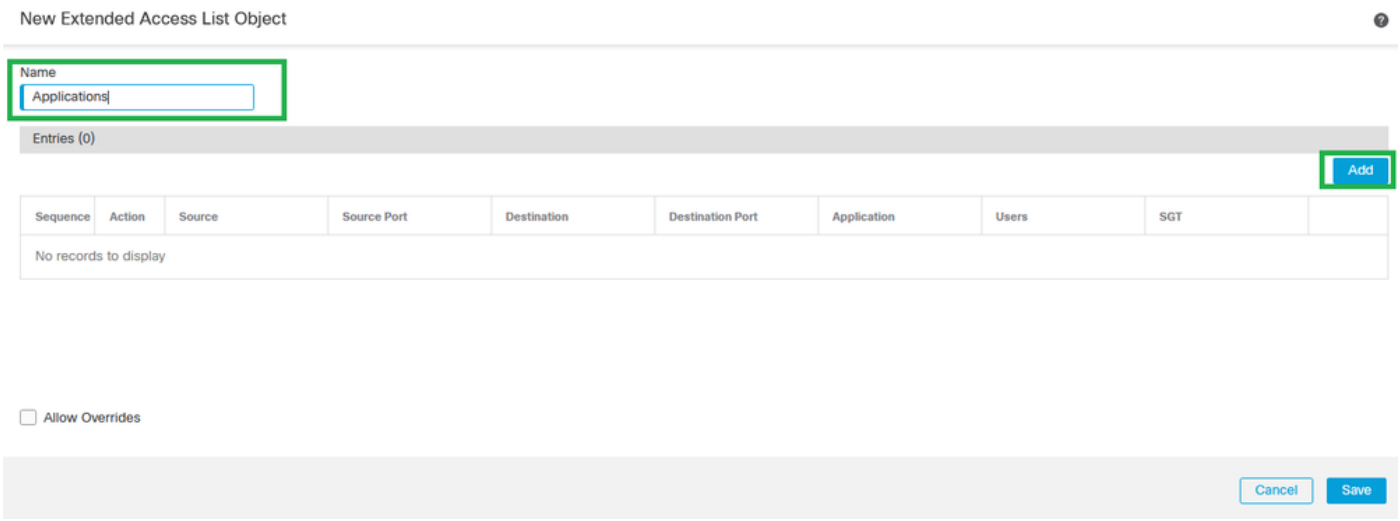
Access-list - Extended

步驟3.按一下Add Extended Access List。



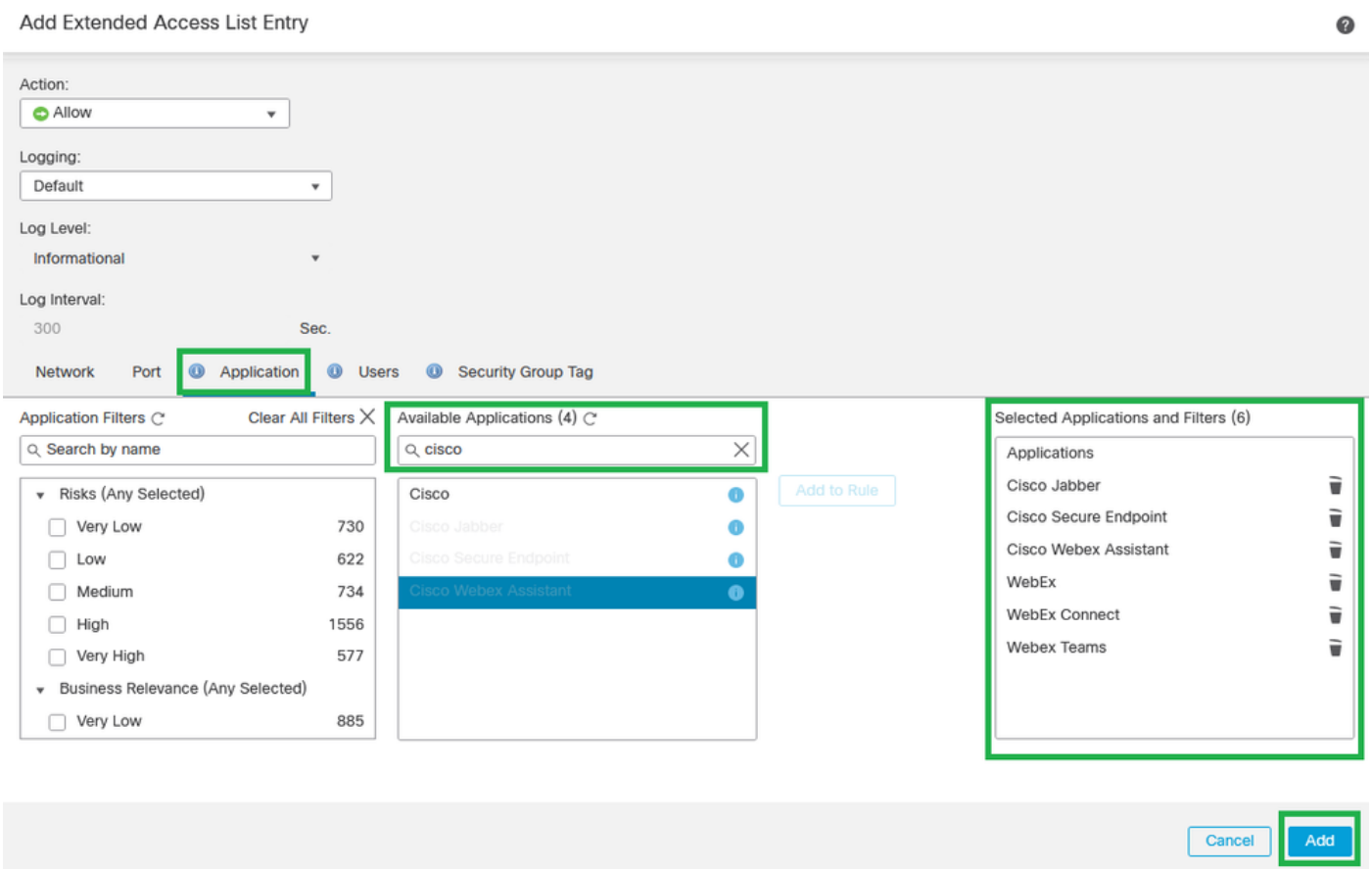
新增擴展訪問清單

步驟4.在Extended Access List中設定名稱並按一下Add。



新建擴展訪問清單對象

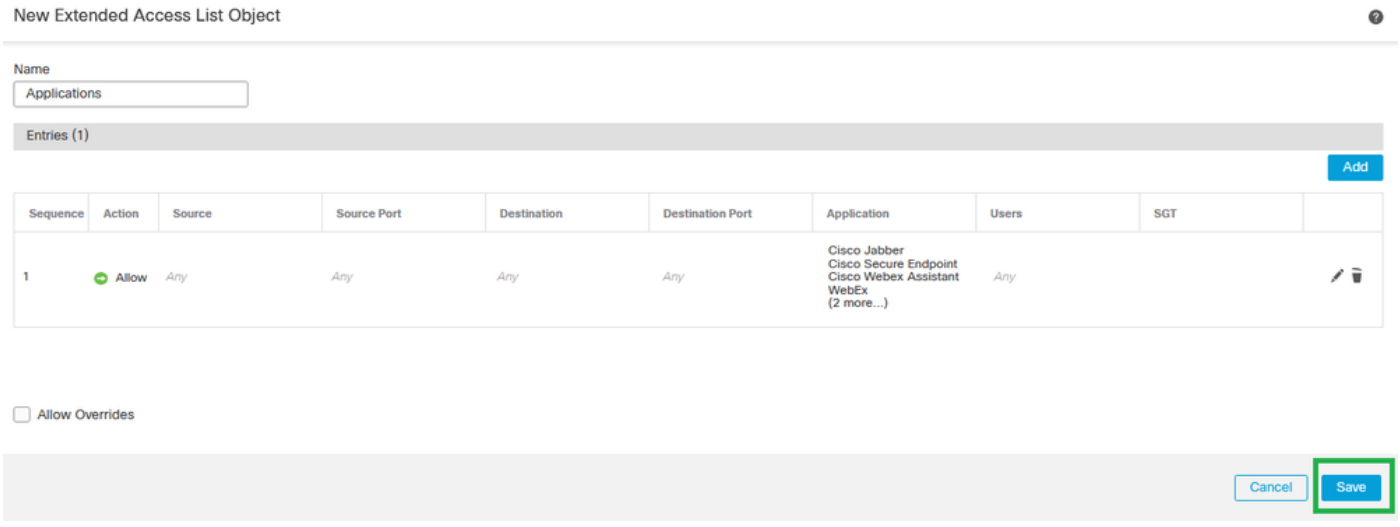
步驟5.按一下Application下並選擇所需的應用程式（本範例已選擇某些思科應用程式）。 然後按一下Add。



新增擴展訪問清單條目

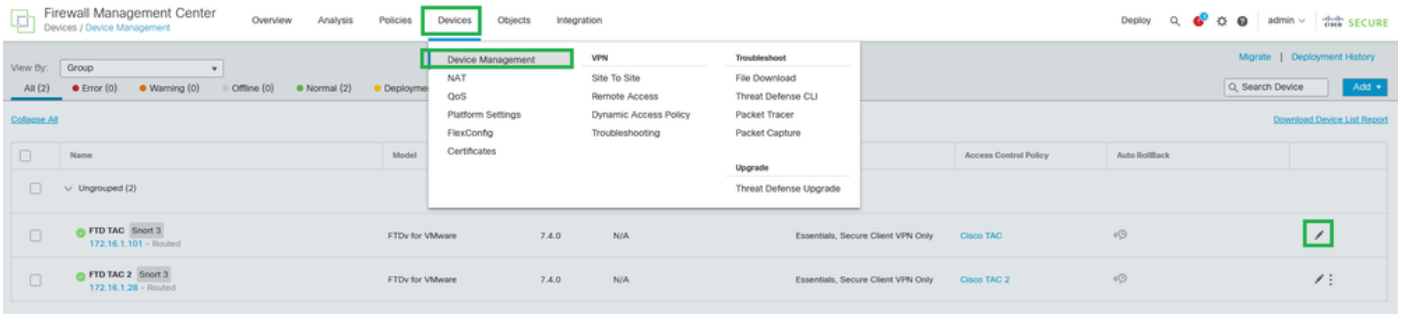
附註：可以使用源/目標IP和埠配置擴展訪問清單，以便將特定流量與所需應用相匹配。您可以建立多個擴展訪問控制清單以應用於PBR配置。

步驟6.驗證Extended Access List配置並按一下Save。



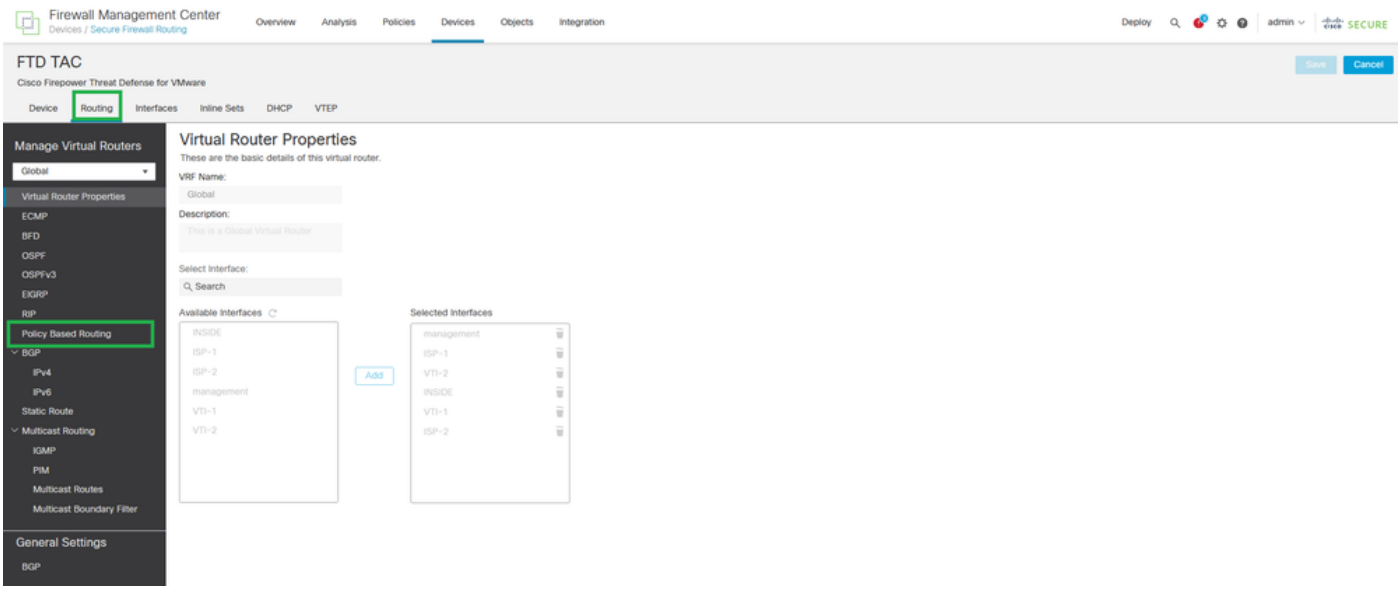
儲存擴展訪問清單對象

步驟 7. 導航到Devices > Device Management威脅防禦並對其進行編輯。



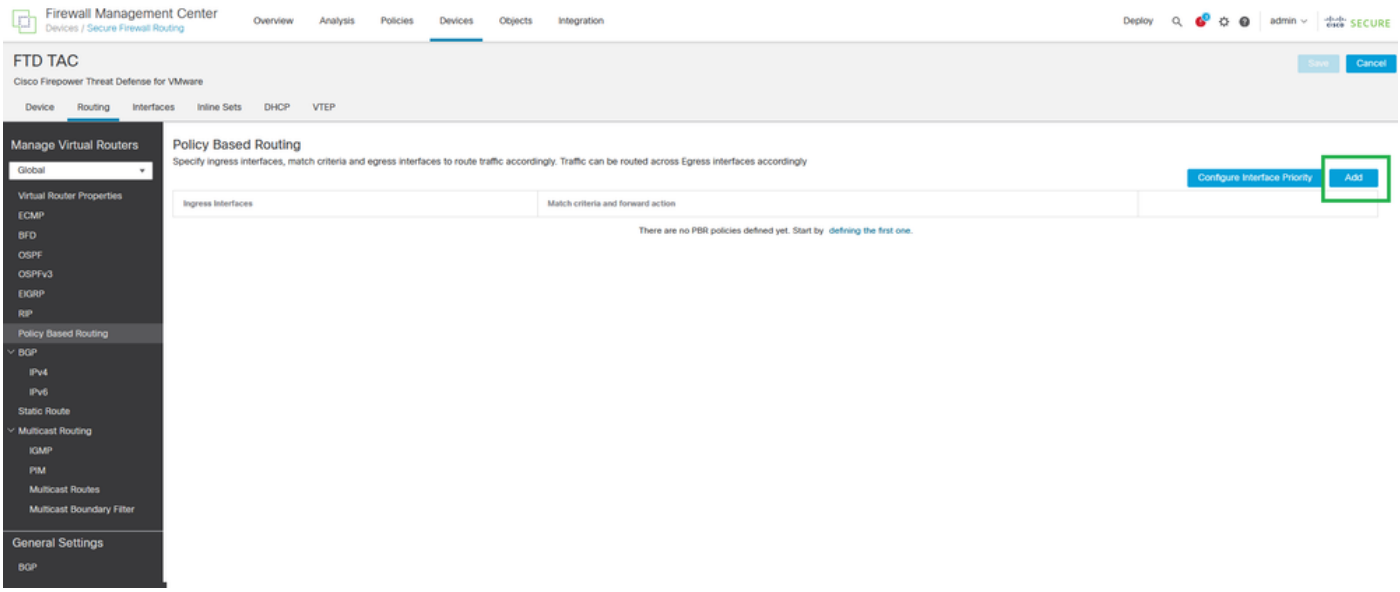
裝置 — 裝置管理

步驟8.導航到Routing > Policy-Based Routing中。



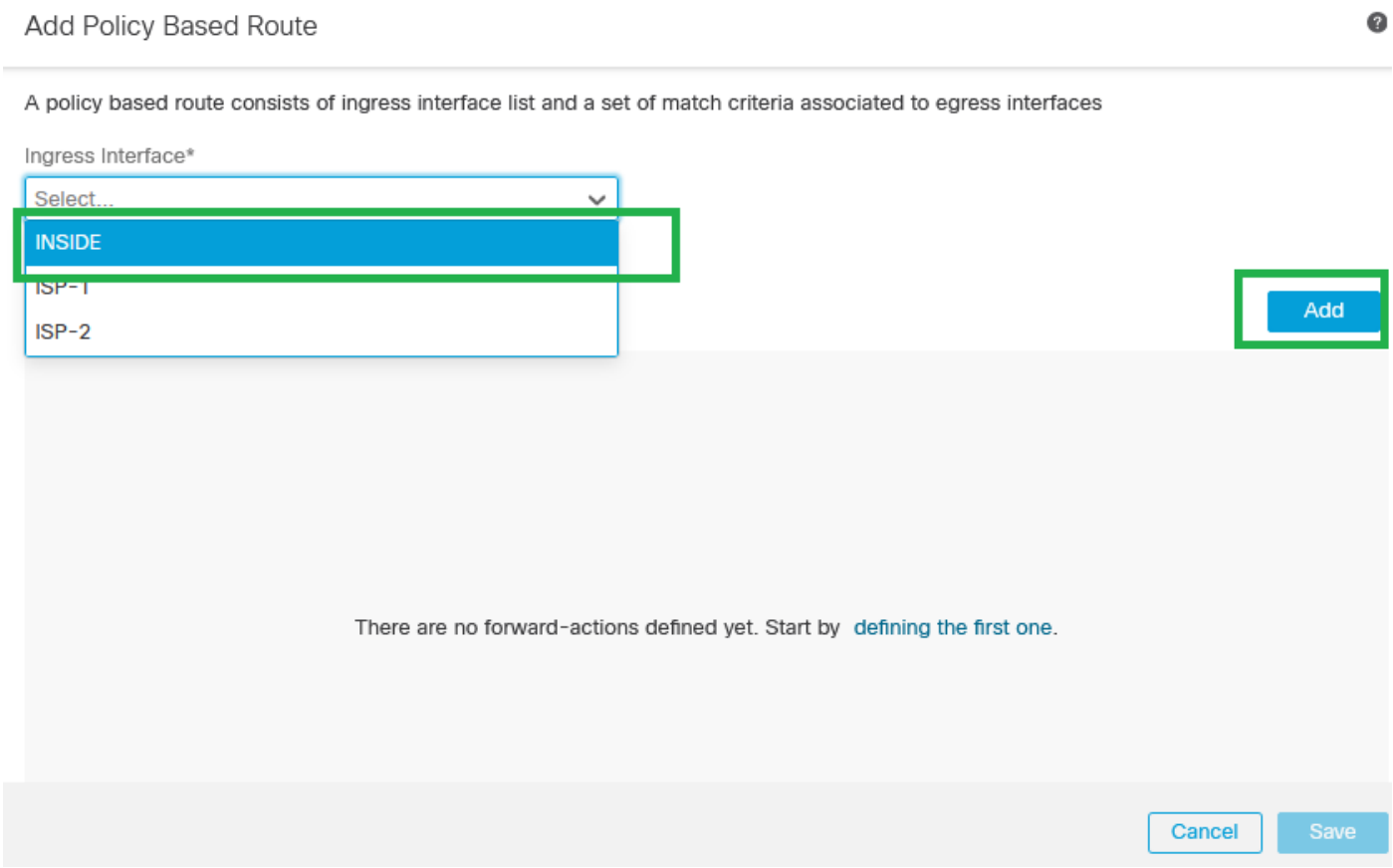
路由 — 基於原則的路由

步驟9.按一下Add。



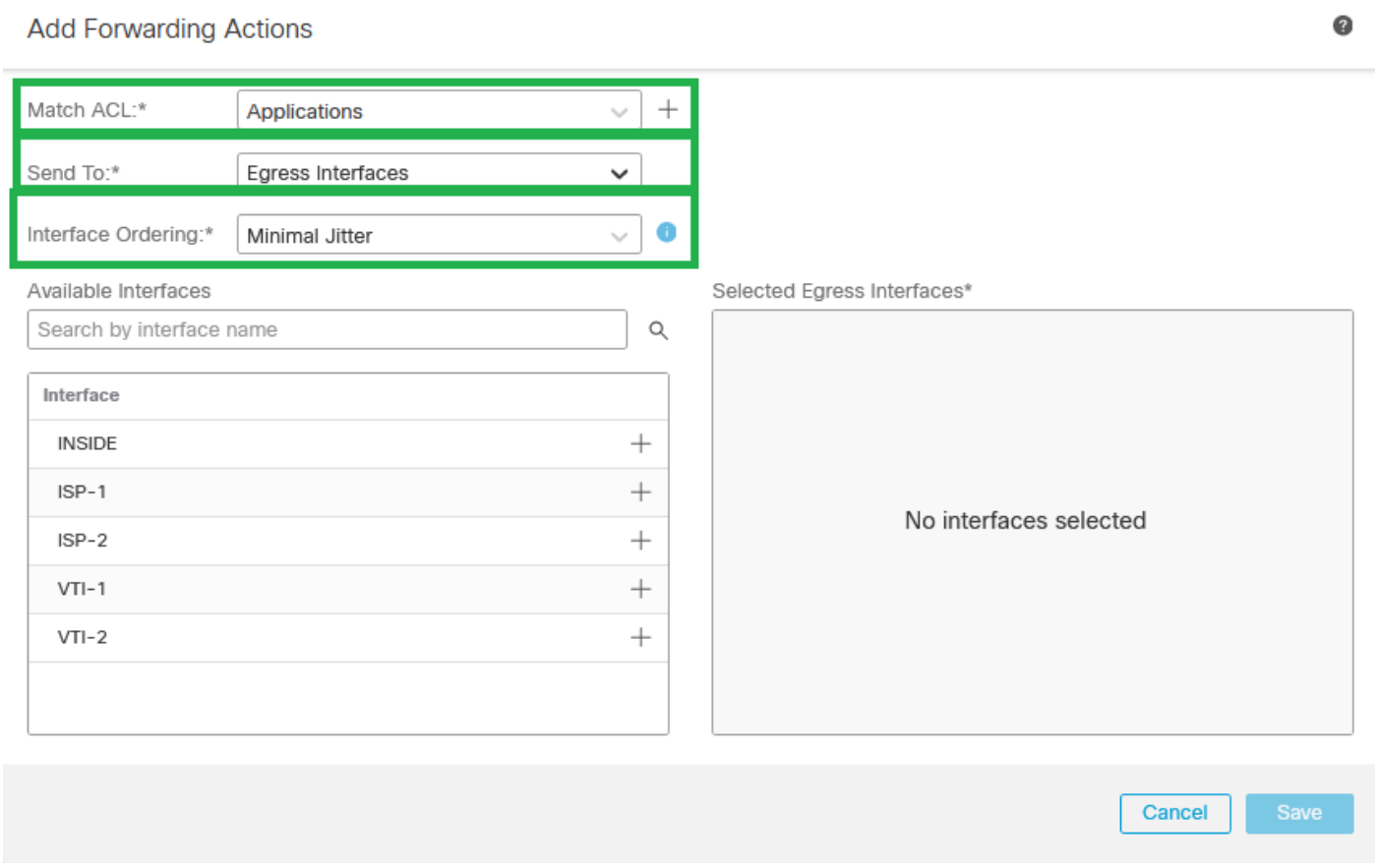
新增基於策略的路由

步驟10.為PBR配置新增入口介面(本例中為INSIDE)，然後按一下Add。



新增基於策略的路由

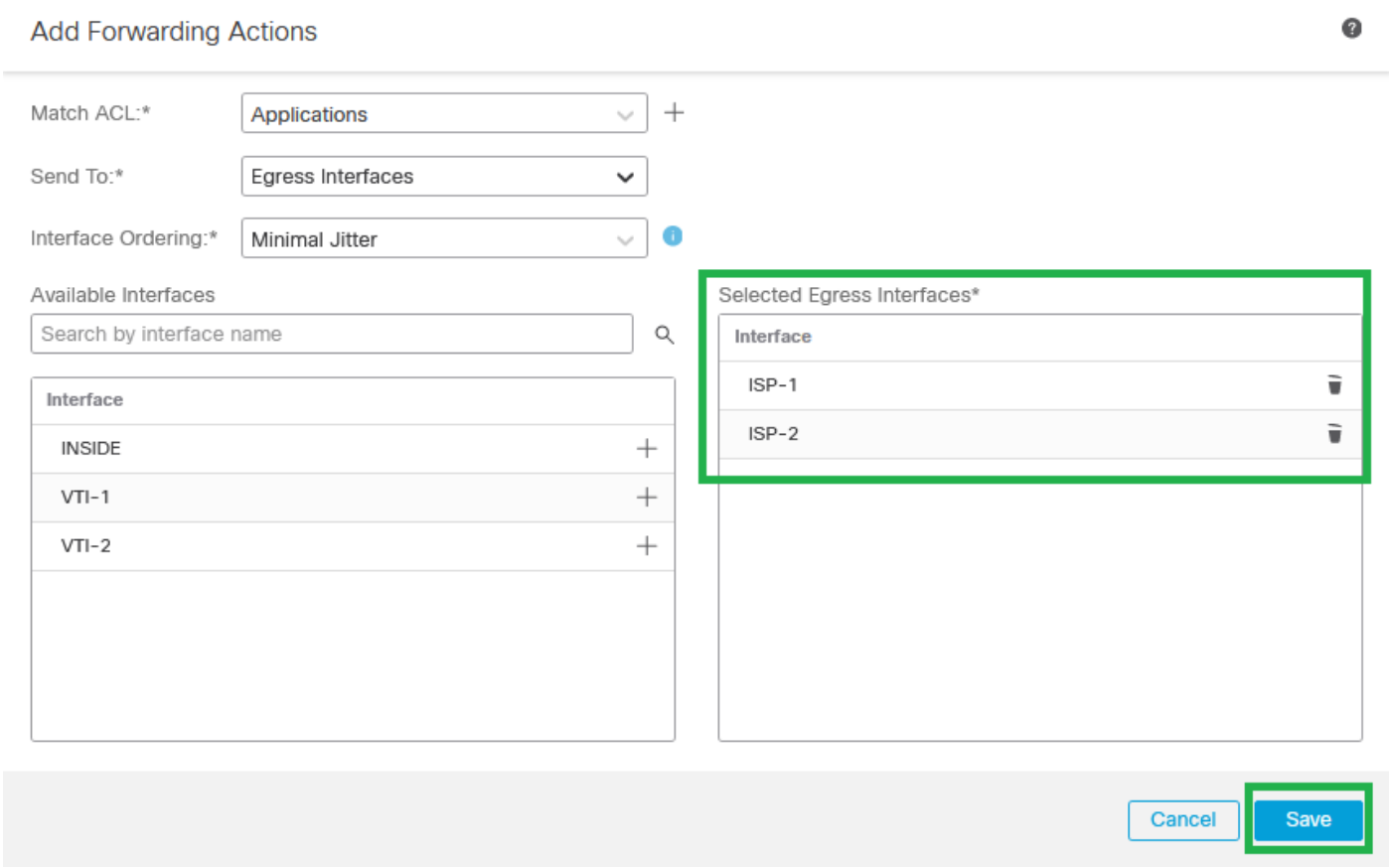
步驟11.定義匹配條件（使用前面步驟中建立的擴展訪問清單）、出口介面和介面排序。



新增轉發操作

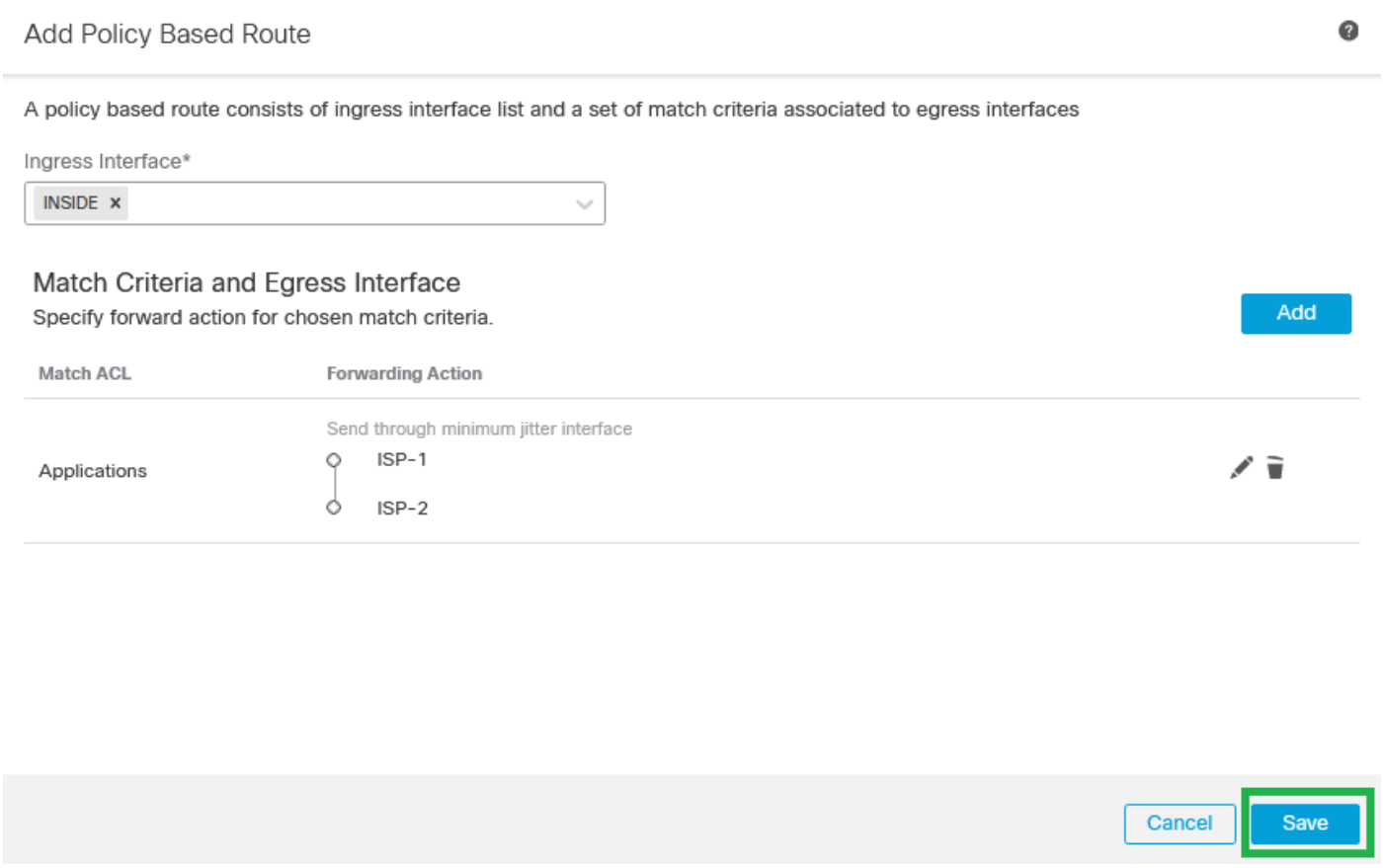
注意:Egress Interfaces和Minimal Jitter，已選擇用於此配置指南。請檢視官方PBR文檔，以瞭解更多有關其他選項的資訊。

步驟12.選擇輸出介面（本例中為ISP-1和ISP-2），然後按一下Save。



選定的輸出介面

步驟13.驗證PBR配置並按一下Save。



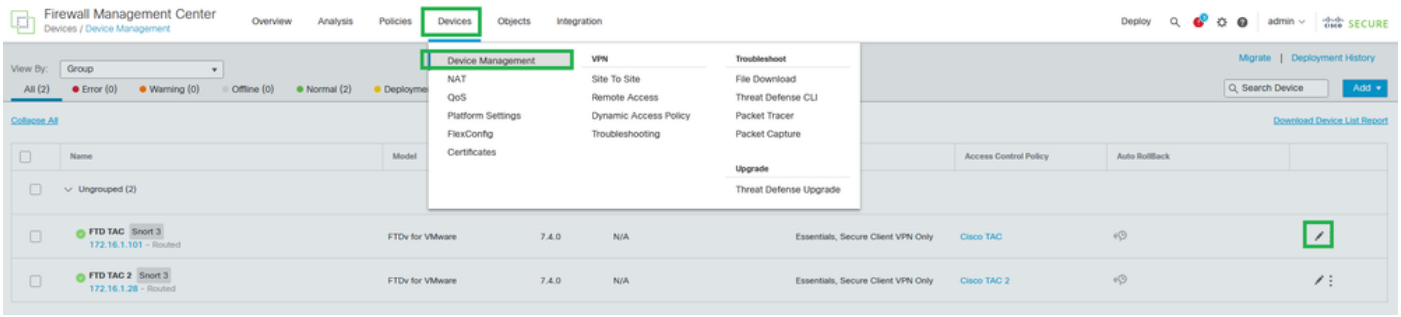
基於策略的路由驗證

步驟14.（可選）如果建立了更多的擴展訪問控制清單，或者存在更多必須應用PBR配置的源介面，請重複步驟9、10、11、12和13。

步驟15.儲存並部署FMC中的更改。

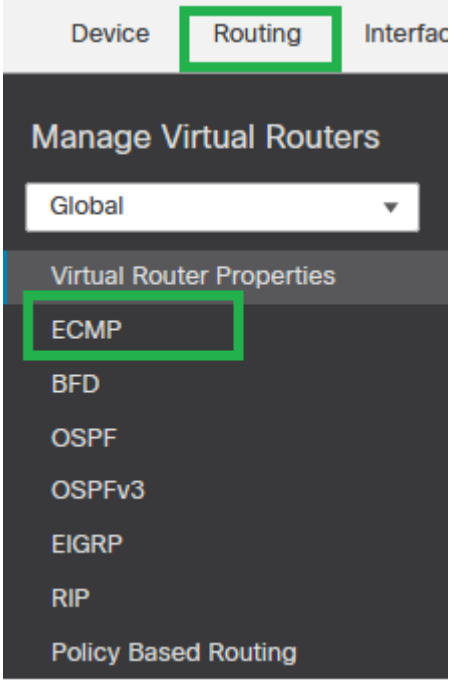
設定等價多重路徑(ECMP)

步驟1.導航至Devices > Device Management，然後編輯威脅防禦。



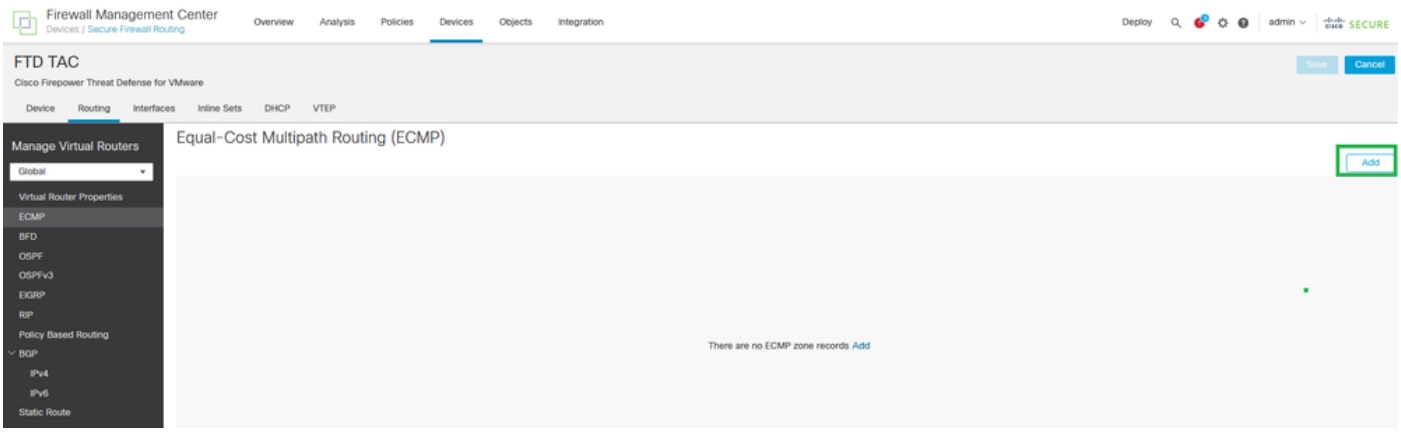
裝置 — 裝置管理

步驟2.導航至Routing > ECMP。



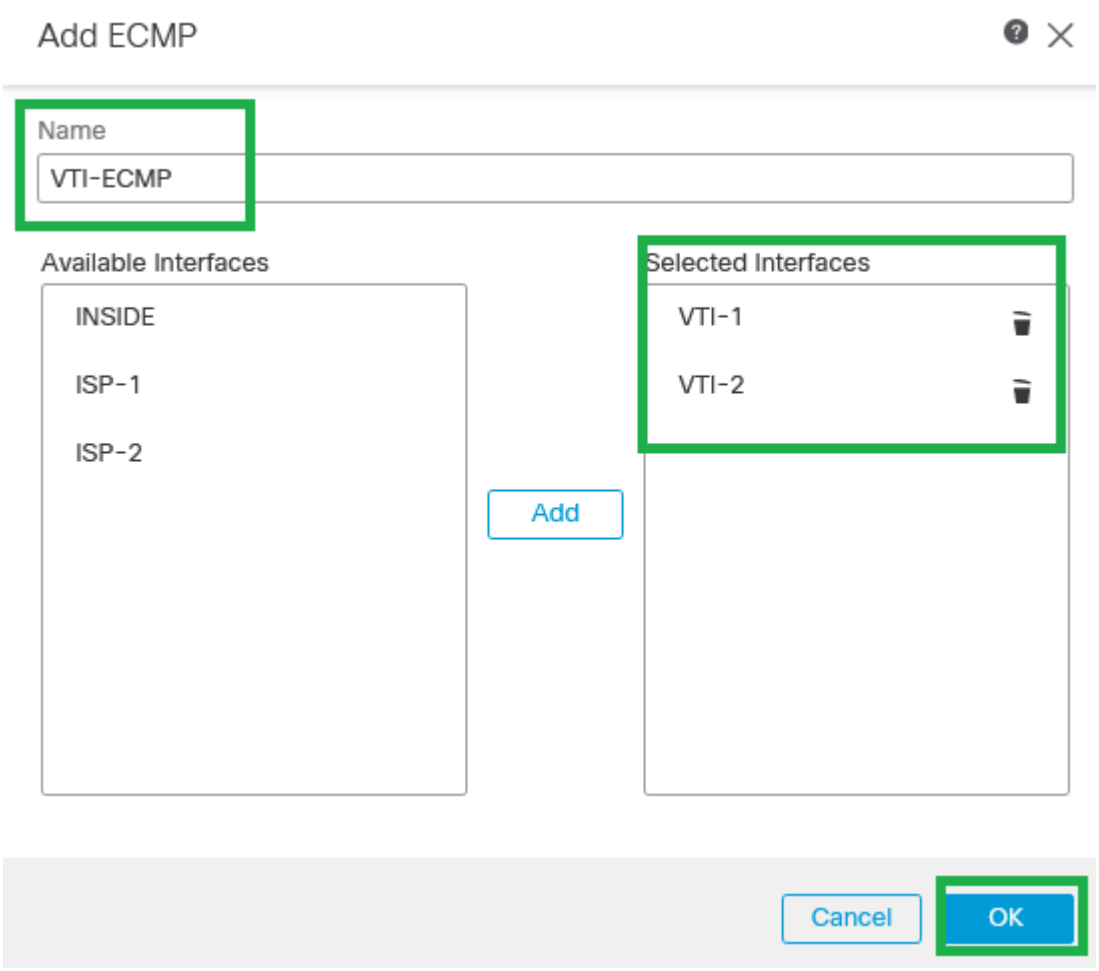
路由 — ECMP

步驟3.按一下Add，在VTI和WAN介面（本配置指南為ISP-1和ISP-2）之間建立ECMP。



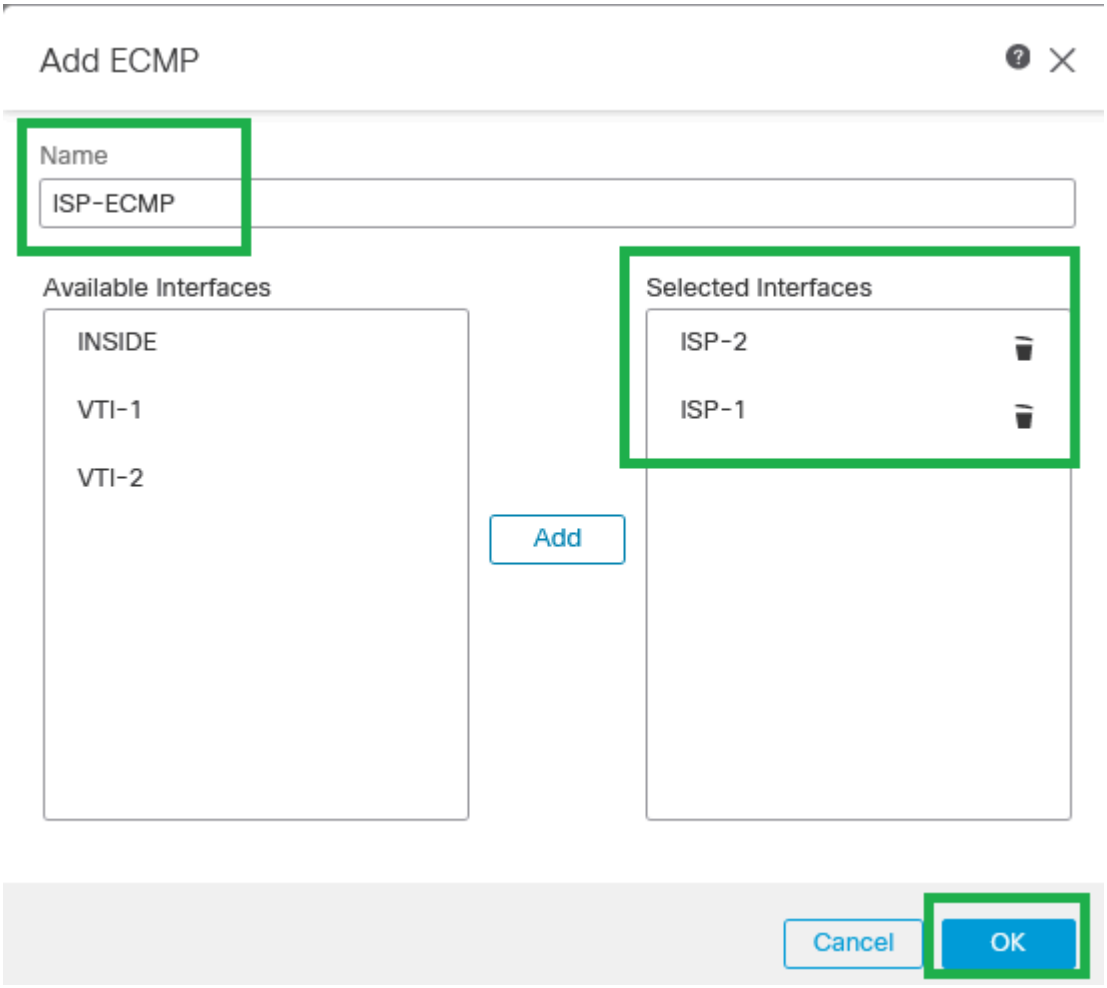
等價多重路徑路由(ECMP)

步驟4.設定ECMP名稱並選擇所有VTI介面，然後按一下Add。



適用於VTI的ECMP

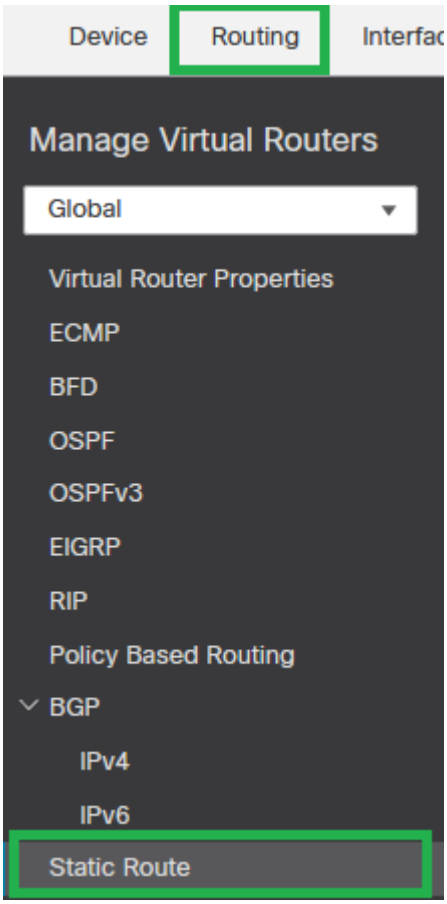
步驟5.重複步驟3和4，以便在WAN介面（本配置指南中的ISP-1和ISP-2）之間建立ECMP。



適用於ISP介面的ECMP

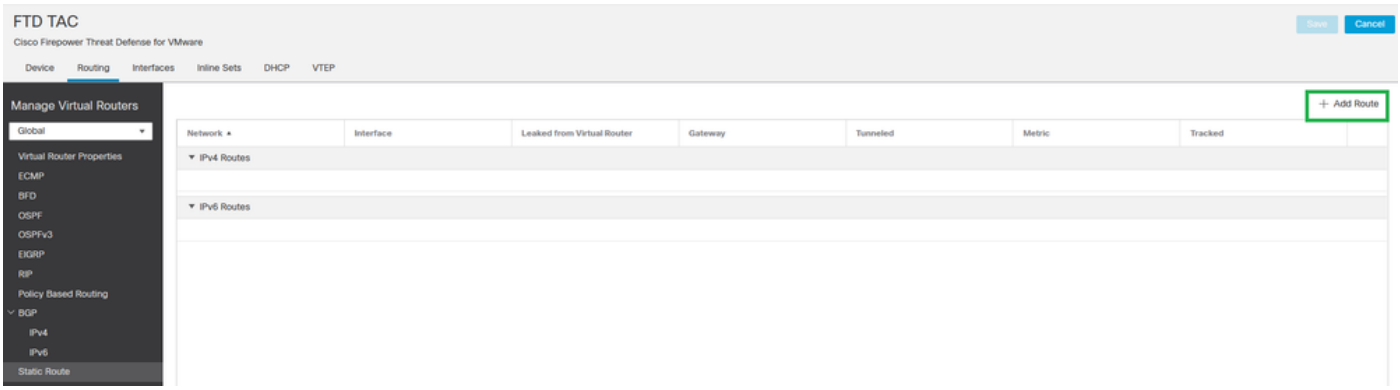
步驟6.儲存ECMP配置。

步驟7.為區域介面配置靜態路由以實現負載均衡。導航至 Routing > Static Route.



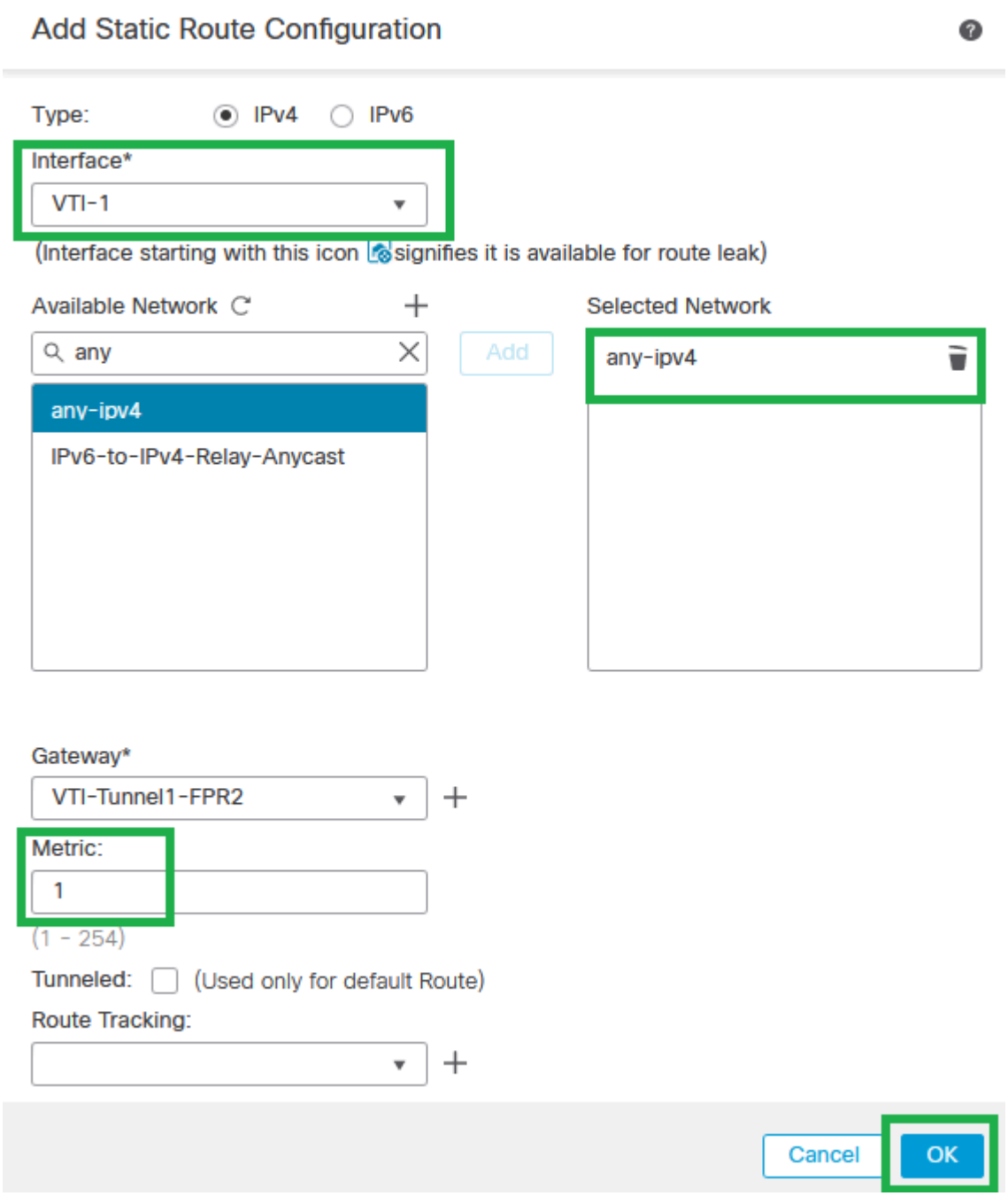
路由 — 靜態路由

步驟8.按一下+ Add Route。



+新增路由

步驟9.為VTI介面建立預設靜態路由（本配置指南為VTI-1），將1作為度量值，然後按一下OK。

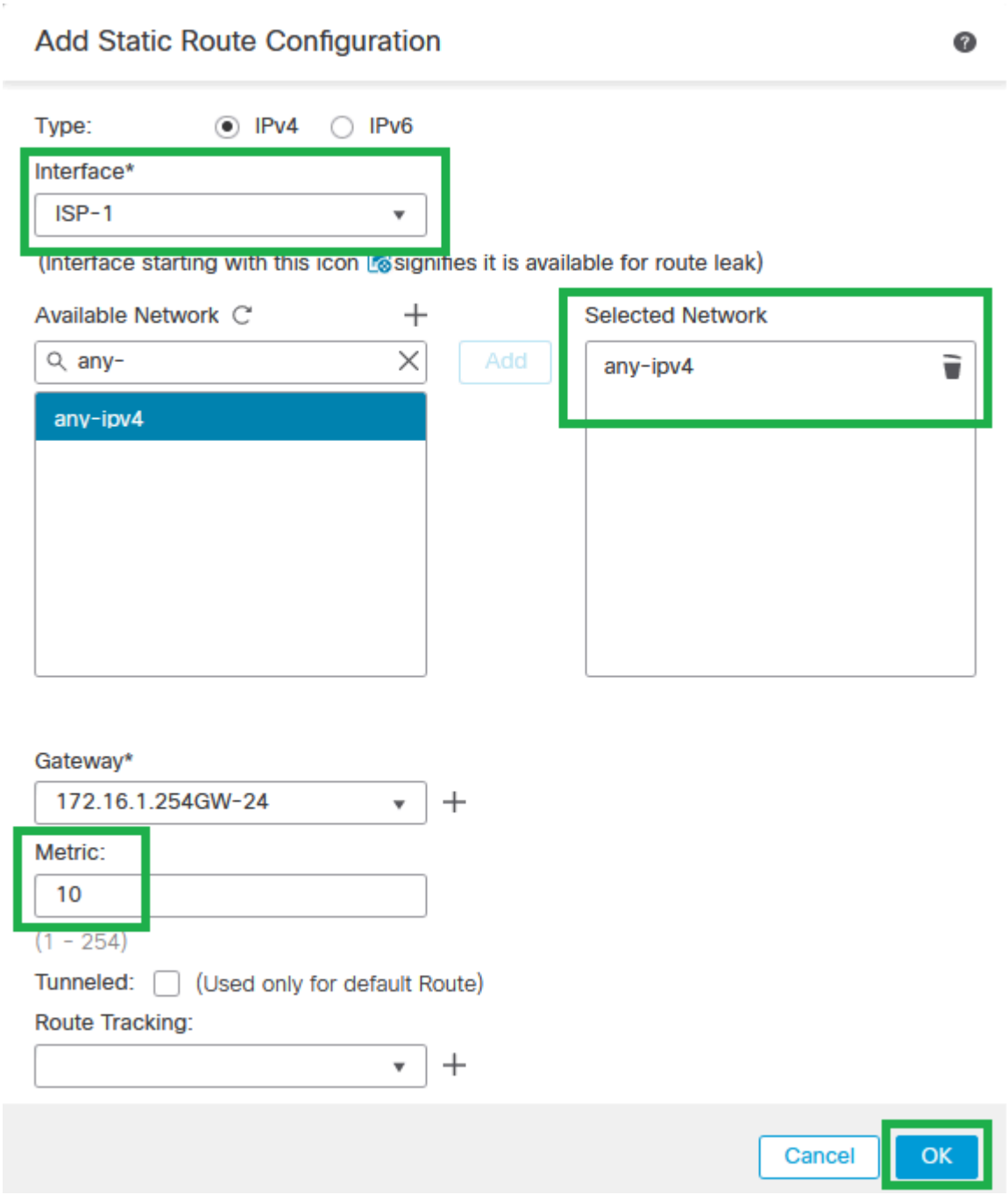


VTI-1的預設靜態路由

步驟10.重複步驟8。如果配置了更多VTI介面。

附註：為配置的每個VTI介面建立預設路由。

步驟11.為WAN/ISP介面（本配置指南為ISP-1）建立度量值大於VTI的預設靜態路由，然後按一下OK。

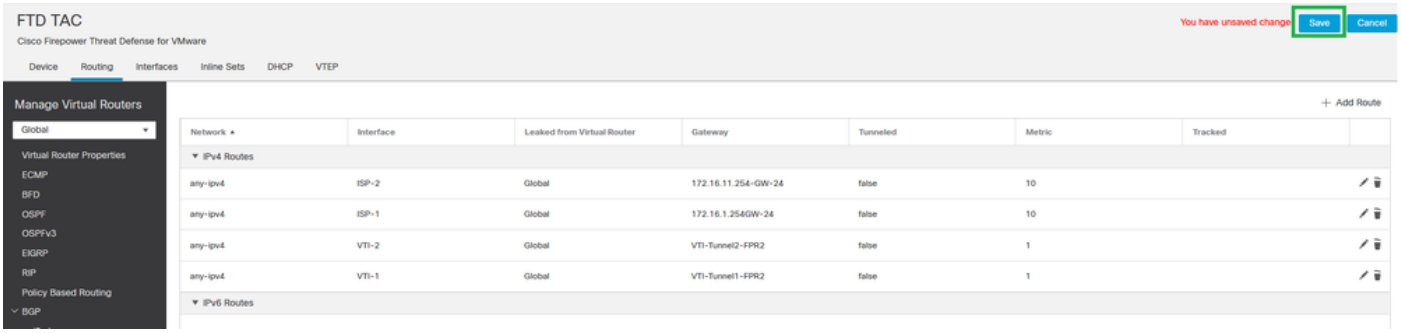


ISP-1的預設靜態路由

步驟12.重複步驟10。如果配置了更多WAN/ISP介面。

附註：為配置的每個WAN/ISP介面建立預設路由。

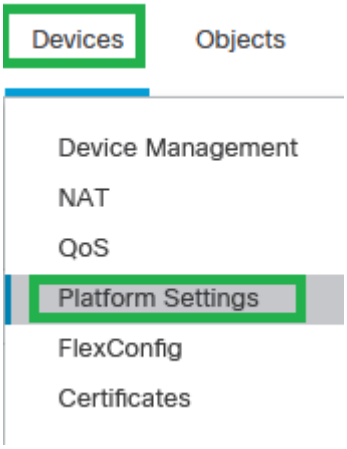
步驟13.驗證預設路由配置，然後按一下OK。



靜態路由配置

為安全FTD設定受信任DNS

步驟1。導覽至 Devices > Platform Settings**。**

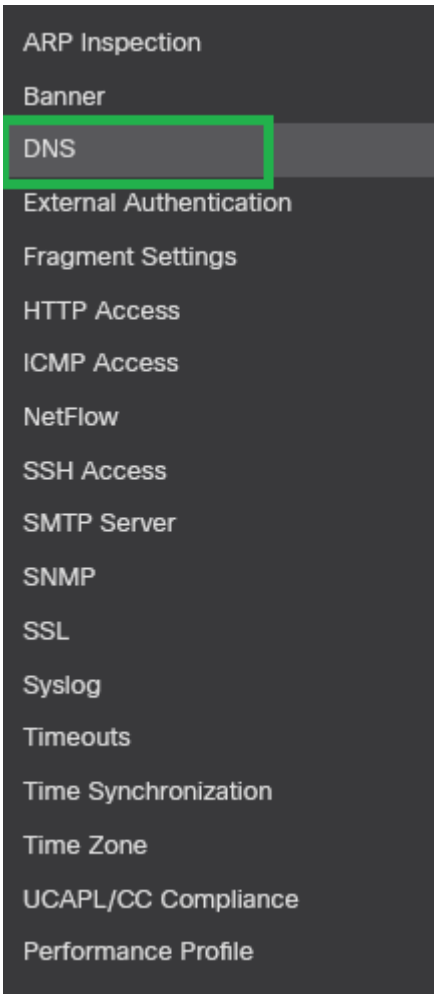


裝置 — 平台設定

步驟2.建立或編輯現有平台設定策略。

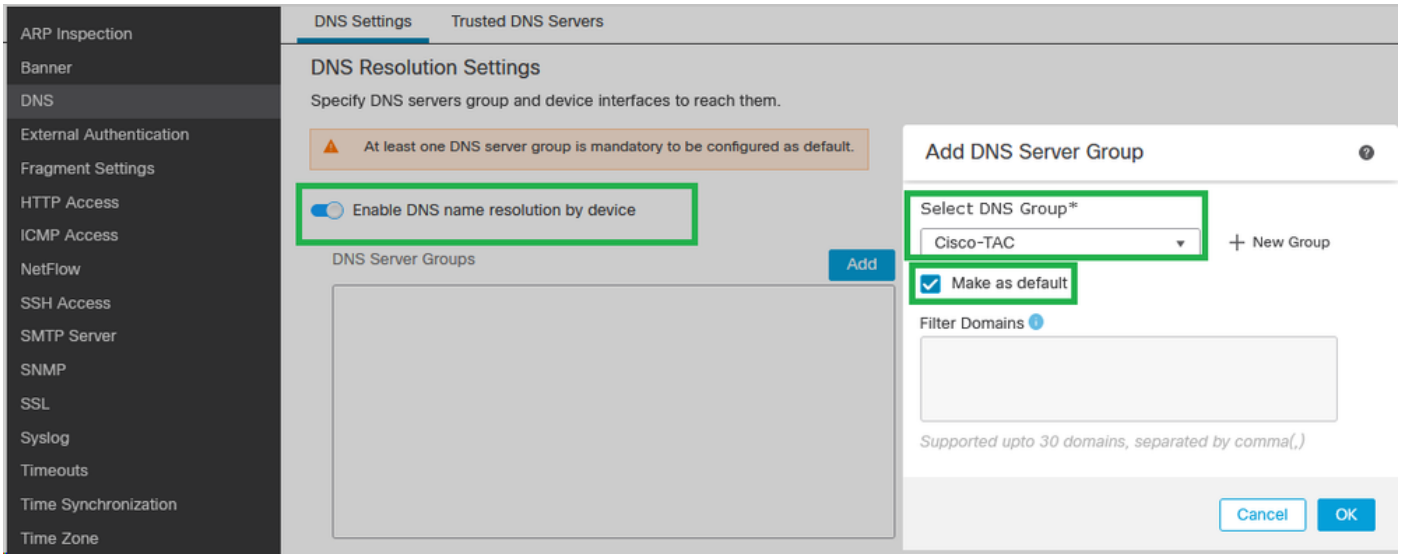
附註：確保「平台設定策略」已應用於安全威脅防禦裝置。

步驟3.按一下DNS**。**



DNS平台設定

步驟4.啟用DNS name resolution by device並點選Add，或選擇現有的DNS組。選擇Make as default，然後按一下OK。

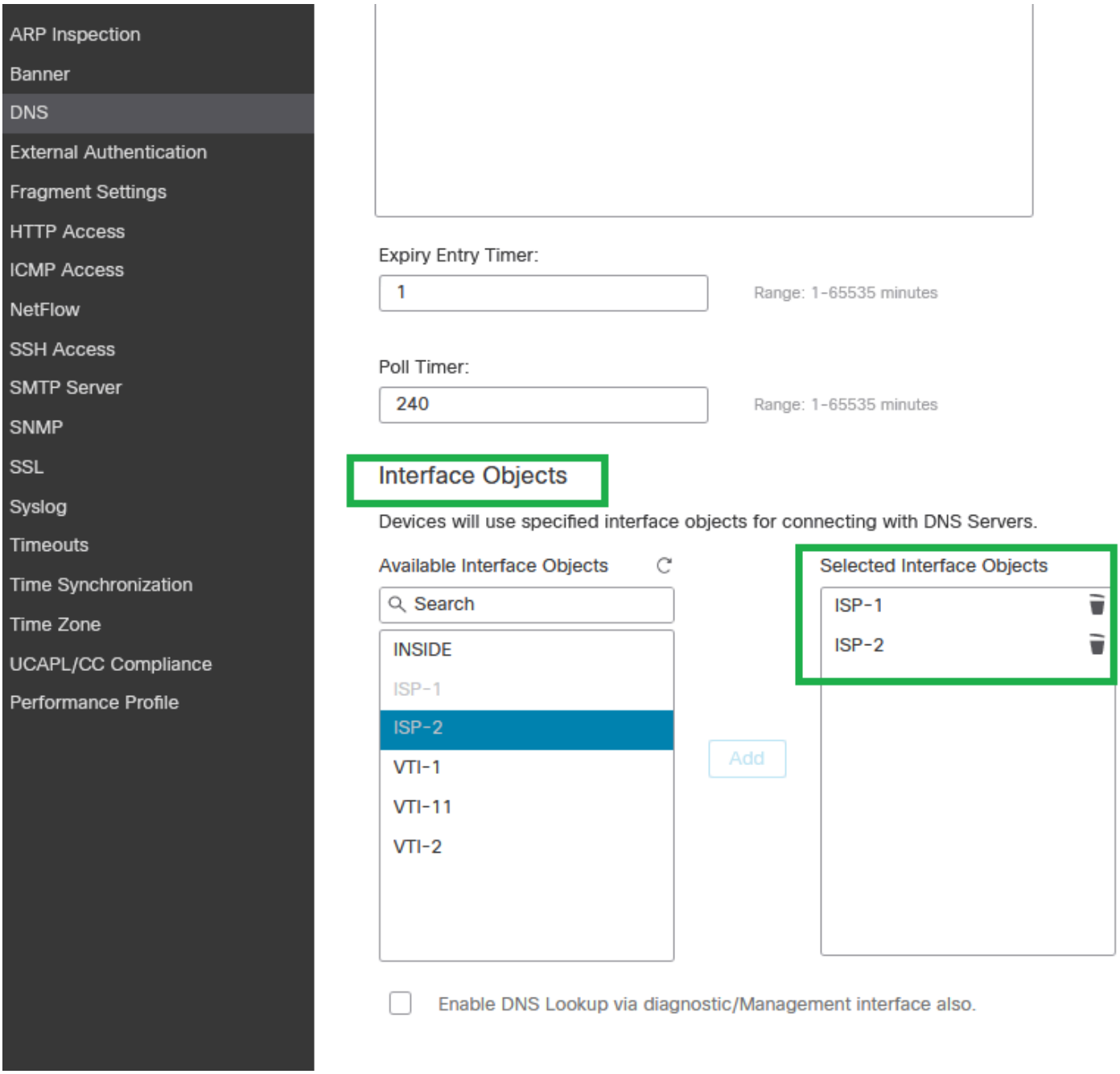


新增DNS伺服器組

附註：如果要瞭解有關平台設定策略上的DNS配置的詳細資訊，請檢視正式平台設定文檔

。

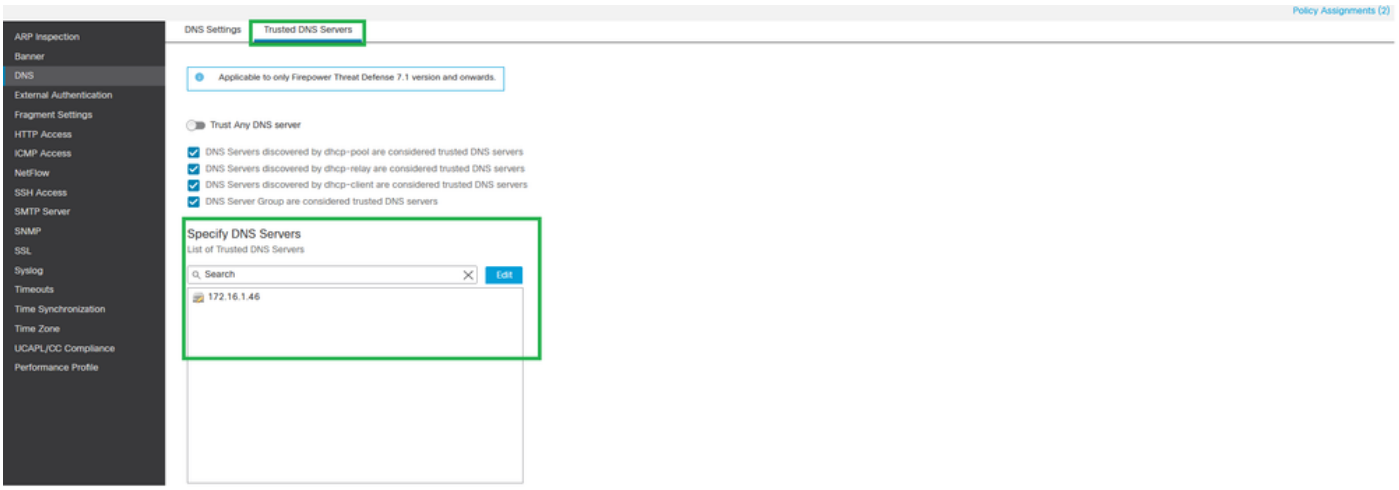
步驟5.選擇Interface Objects部分下的WAN/ISP介面。



DNS介面配置

步驟6. 儲存變更。

步驟7.導航到並指Trusted DNS Servers定受信任的DNS伺服器。

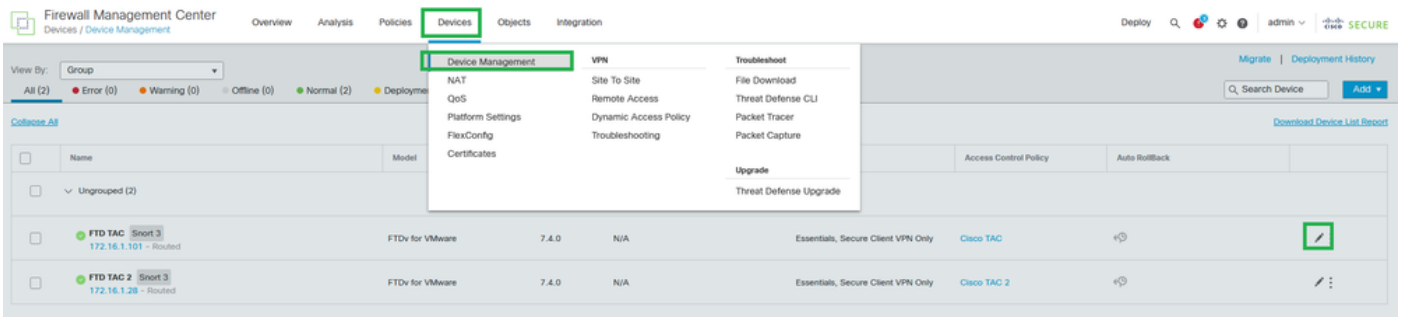


受信任的DNS伺服器

步驟8.單擊Save，然後部署更改。

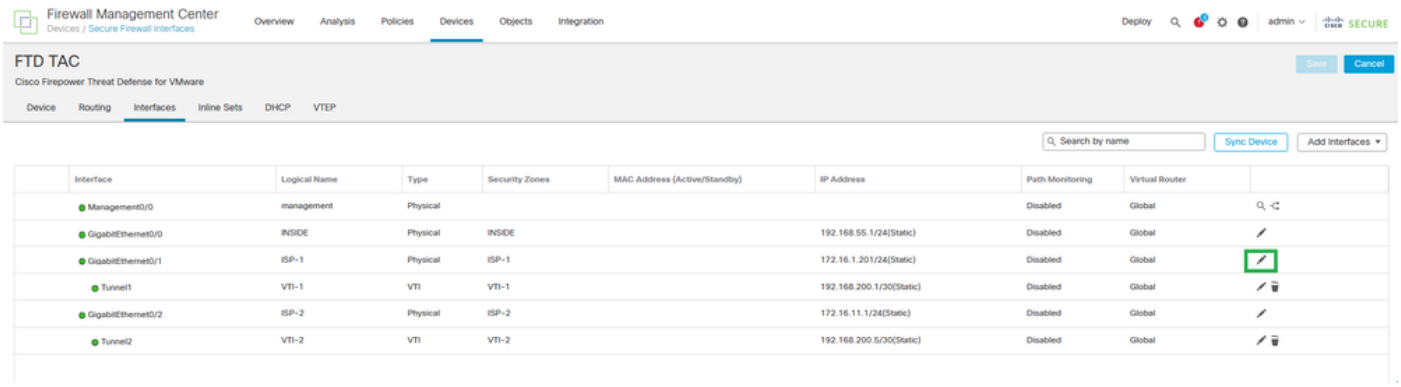
啟用路徑監控

步驟1.導航至Devices > Device Management，然後編輯威脅防禦。



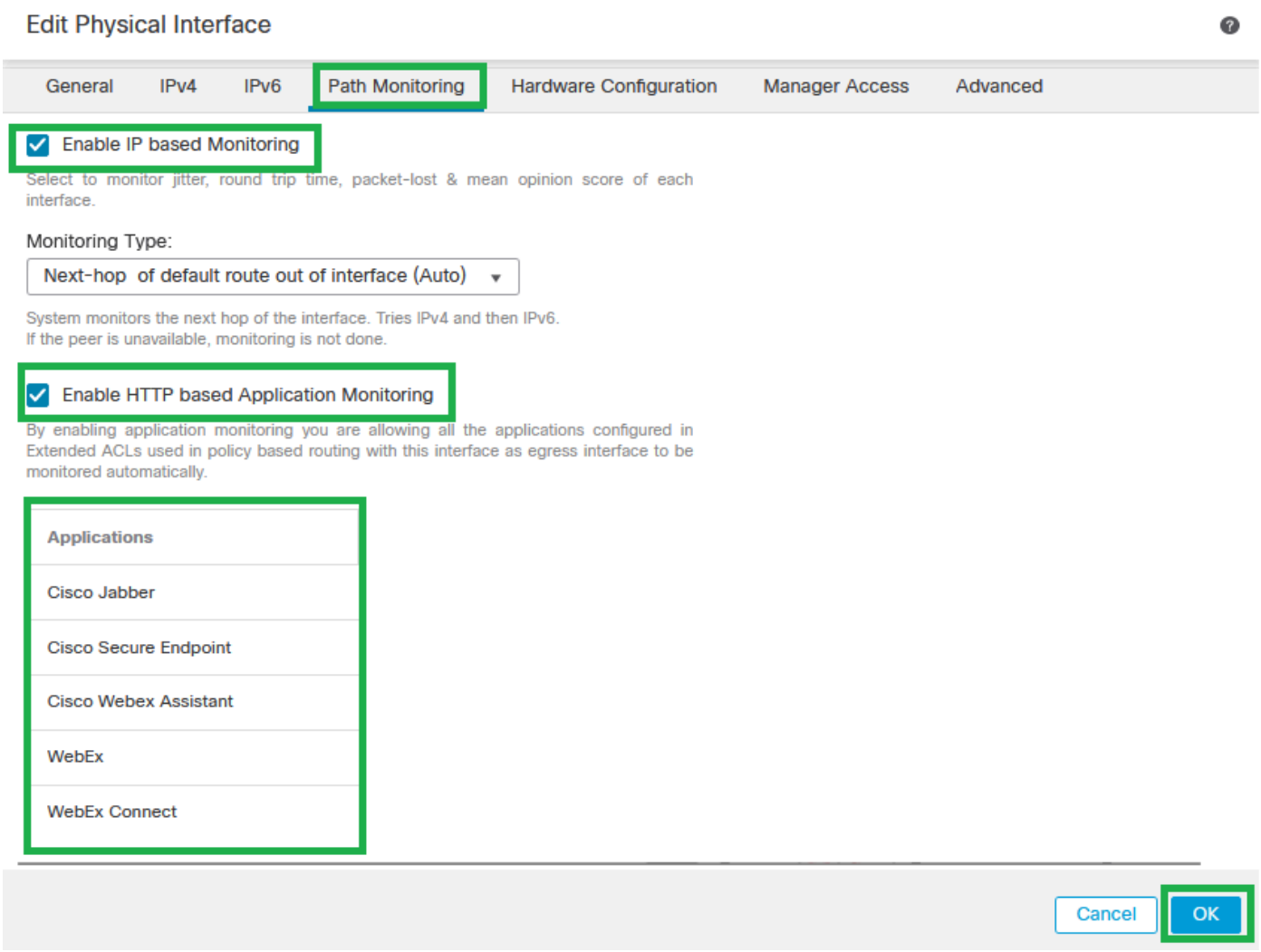
裝置 — 裝置管理

步驟2.在Interfaces頁籤下，編輯介面WAN/ISP介面（本配置指南中為ISP-1和ISP-2）。



介面配置

步驟3.按一下該選Path Monitoring項卡，選擇Enable IP Monitoring，並啟用復HTTP-based Application Monitoring選框。然後按一下Save。



介面路徑監控組態

注意：必須列出在早期配置部分中配置的應用程式。

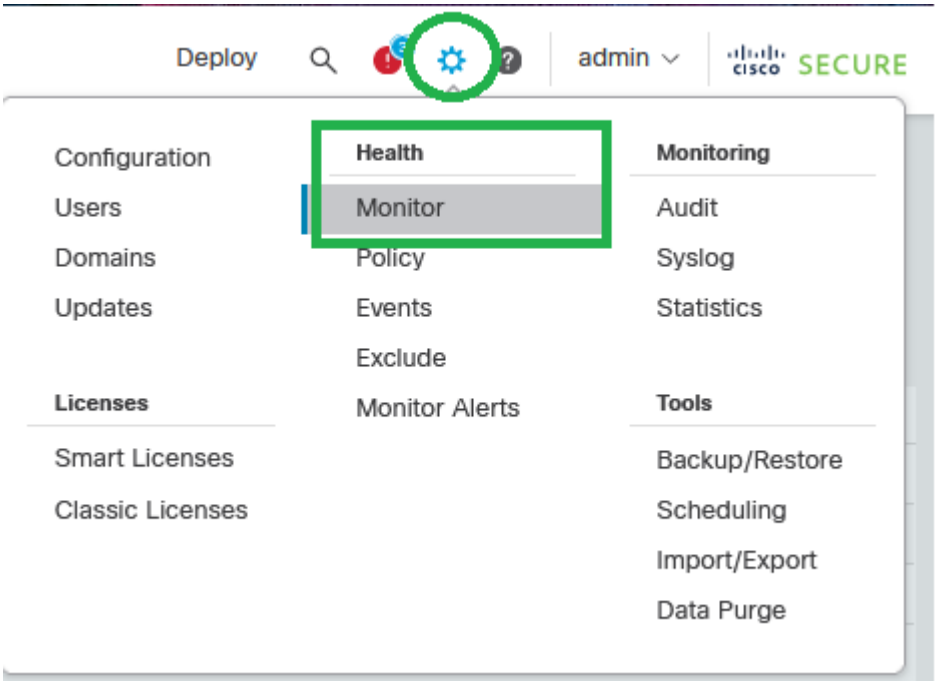
附註：已為此配置指南選擇「監控型別」。檢查官方配置指南上的路徑監視設定，以瞭解有關其他選項的詳細資訊。

步驟4.對已配置的所有WAN/ISP介面重複步驟2和步驟3。

步驟5.按一下Save，然後部署變更。

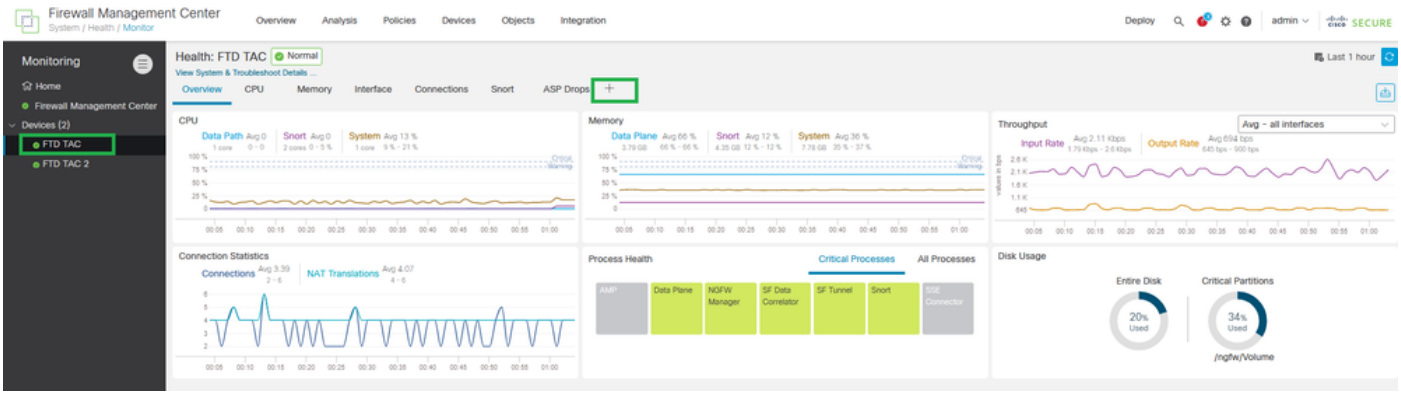
新增監控儀表板

步驟1。導覽至System > Health > Monitor。



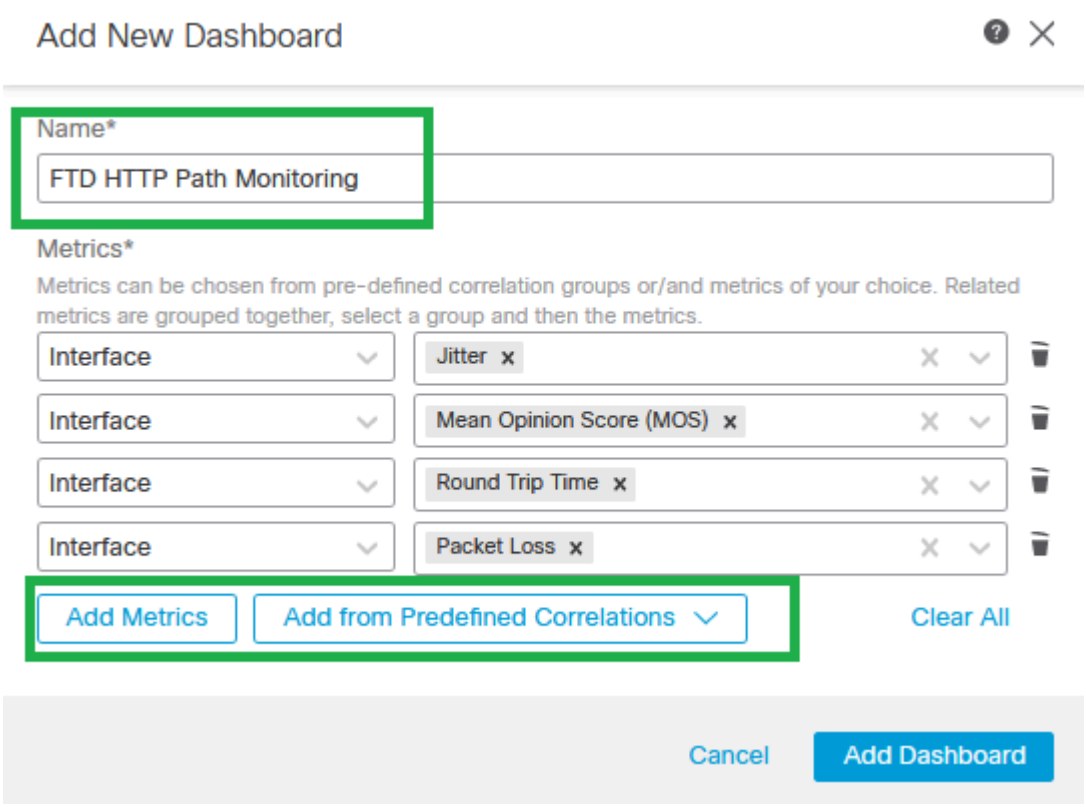
系統 — 運行狀況 — 監控

步驟2.選擇Secure FTD裝置，然後點選Add New Dashboard。



新增新儀表板

步驟3.設定儀表板名稱，Correlate Metrics在對話方塊的下拉選單中選擇Interface - Path Metrics。然後按一下Add Dashboard。



新增具有路徑度量的新儀表板

驗證

本節介紹如何驗證浮動靜態路由、ECMP、包含應用程式的對象組和PBR配置。

檢驗預設路由和浮動靜態路由配置：

```
firepower# show run route
route VTI-1 0.0.0.0 0.0.0.0 192.168.200.1 1
route VTI-2 0.0.0.0 0.0.0.0 192.168.200.5 1
route ISP-1 0.0.0.0 0.0.0.0 172.16.1.254 10
route ISP-2 0.0.0.0 0.0.0.0 172.16.11.254 10
```

驗證ECMP配置：

```
firepower# sh run | i ecmp
zone ECMP-VTI ecmp
zone ECMP-ISP ecmp
```

驗證路由表上的ECMP是否正在平衡流量。路由表必須在安全FTD路由表上安裝兩條路由。

```
firepower# 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 172.16.11.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.200.5, VTI-2
[1/0] via 192.168.200.1, VTI-1
```

驗證PBR路由對映配置：

```
firepower# show run route-map
!
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set adaptive-interface cost ISP-1 ISP-2
!
```

驗證分配給PBR配置的ACL（檢查路由對映配置上的ACL名稱）：

```
firepower# show run access-list | i Applications
access-list Applications extended permit ip any object-group-network-service FMC_NSG_639950173988
```

檢驗Object Group with Applications assigned to the access list（使用ACL配置中的應用程式檢查對象組名稱）：

```
firepower# show run object-group
object-group network-service FMC_NSG_639950173988
network-service-member "Cisco Jabber"
network-service-member "Cisco Secure Endpoint"
network-service-member "Cisco Webex Assistant"
network-service-member "WebEx"
network-service-member "WebEx Connect"
network-service-member "Webex Teams"
```

驗證分配給PBR配置中使用的資料介面的策略路由：

```
interface GigabitEthernet0/0
```

```
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.35.1 255.255.255.0
policy-route route-map FMC_GENERATED_PBR_1694885402369
!
interface GigabitEthernet0/1
nameif ISP-1
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
zone-member ECMP-ISP
ip address 172.16.1.202 255.255.255.0
policy-route path-monitoring auto
!
interface GigabitEthernet0/2
nameif ISP-2
security-level 0
zone-member ECMP-ISP
ip address 172.16.11.2 255.255.255.0
policy-route path-monitoring auto
!
```

從HTTP路徑監控控制面板資訊驗證並檢查抖動、MOS、往返時間和丟包統計資訊。

驗證HTTP路徑監視儀表板

疑難排解

如果路徑監控失敗，啟用基於IP的監控後，WAN/ISP介面配置為將ICMP探測資料包傳送到在靜態路由上配置的網關。在WAN/ISP介面上配置輸入/輸出捕獲，以檢查ICMP是否正常工作。

輸入和輸出擷取：

```
firepower# cap in interface ISP-1 trace match icmp any any
firepower# cap in2 interface isP-2 trace match icmp any any
```

入口捕獲：

```
firepower# show cap in

12 packets captured
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
12 packets shown
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
12 packets shown
```

輸出捕獲：

```
firepower# show cap in2

12 packets captured

1: 00:08:28.073543 172.16.11.2 > 172.16.11.254 icmp: echo request
2: 00:08:28.074764 172.16.11.254 > 172.16.11.2 icmp: echo reply
3: 00:08:29.150810 172.16.11.2 > 172.16.11.254 icmp: echo request
4: 00:08:29.151954 172.16.11.254 > 172.16.11.2 icmp: echo reply
5: 00:08:30.217640 172.16.11.2 > 172.16.11.254 icmp: echo request
6: 00:08:30.218799 172.16.11.254 > 172.16.11.2 icmp: echo reply
7: 00:08:31.247667 172.16.11.2 > 172.16.11.254 icmp: echo request
8: 00:08:31.248888 172.16.11.254 > 172.16.11.2 icmp: echo reply
9: 00:08:32.308913 172.16.11.2 > 172.16.11.254 icmp: echo request
10: 00:08:32.310012 172.16.11.254 > 172.16.11.2 icmp: echo reply
11: 00:08:33.386576 172.16.11.2 > 172.16.11.254 icmp: echo request
12: 00:08:33.387888 172.16.11.254 > 172.16.11.2 icmp: echo reply
```

```
12 packets captured
```

注意：確保使用源IP地址和目標IP地址配置捕獲，因為捕獲可以顯著提高裝置效能。

提示：如果Ping不起作用，請排查與預設網關的直接連線故障，檢查ARP表，或聯絡Cisco TAC。

為了檢查PBR是否工作，您可以使用Packet Tracer工具確保通過PBR路由應用流量。

```
firepower# packet-tracer input insIDE tcp 172.16.35.2 54352 'PUBLIC-IP-ADDRESS-FOR-WEBEX' $
---
[Output omitted]
---
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set ip next-hop 172.16.1.254
Additional Information:
Matched route-map FMC_GENERATED_PBR_1694885402369, sequence 5, permit
Found next-hop 172.16.1.254 using egress ifc ISP-1
---
[Output omitted]
---
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: ISP-1
output-status: up
output-line-status: up
Action: allow
```

附註：要瞭解在對象組上配置的網路服務的應用程式IP地址，請使用命**show object-group network-service detail**令。

相關資訊

有關具有HTTP路徑監控的PBR的其他文檔，請訪問以下網站：

- 安全防火牆管理中心裝置配置指南上的基於策略的路由配置
- 《Secure Firewall Management Center裝置配置指南》中基於策略的路由配置上的路徑監控
- 配置基於策略的路由策略
- 基於策略的路由的配置示例
- 配置PBR路徑監控示例
- 新增路徑監控儀表板
- 安全防火牆管理中心裝置配置指南上的DNS平台設定配置
- 思科技術支援與下載

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）。