在安全防火牆上使用環回介面配置eBGP

目錄

簡介

本文檔介紹如何使用Cisco安全防火牆上的環回介面配置eBGP。

必要條件

需求

思科建議您瞭解以下主題：

- BGP通訊協定

7.4.0版引入了對BGP的環回介面支援，這是安全防火牆管理中心和Cisco Secure Firepower威脅防禦所需的最低版本。

採用元件

- 適用於VMware的安全防火牆管理中心版本7.4.1
- 2適用於VMware的Cisco安全Firepower威脅防禦7.4.1版

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

邊界閘道通訊協定(BGP)是一種外部閘道通訊協定(EGP)標準化路徑向量路由通訊協定，可提供擴充性、彈性及網路穩定性。具有相同自治系統(AS)的兩個對等體之間的BGP會話稱為內部BGP (iBGP)。具有不同自治系統(AS)的兩個對等體之間的BGP會話稱為外部BGP (eBGP)。

通常，對等體關係是使用最接近對等體的介面的IP地址建立的，但是，使用環回介面建立BGP會話很有用，因為當BGP對等體之間存在多個路徑時，它不會導致BGP會話關閉。

注意：此進程描述對eBGP對等體使用Loopkack的過程，但對iBGP對等體使用相同的進程，因此可以將其用作參考。

使用環回介面的eBGP配置

案例

在此配置中，防火牆SFTD-1具有IP地址為10.1.1.1/32的環回介面，而防火牆SFTD-2具有IP地址為10.2.2.2/32且AS64000為64001的環回介面。兩個防火牆均使用其外部介面到達另一個防火牆的環回介面（在本場景中，兩個防火牆上均預配置了外部介面）。

網路圖表

此文件使用以下網路設定：

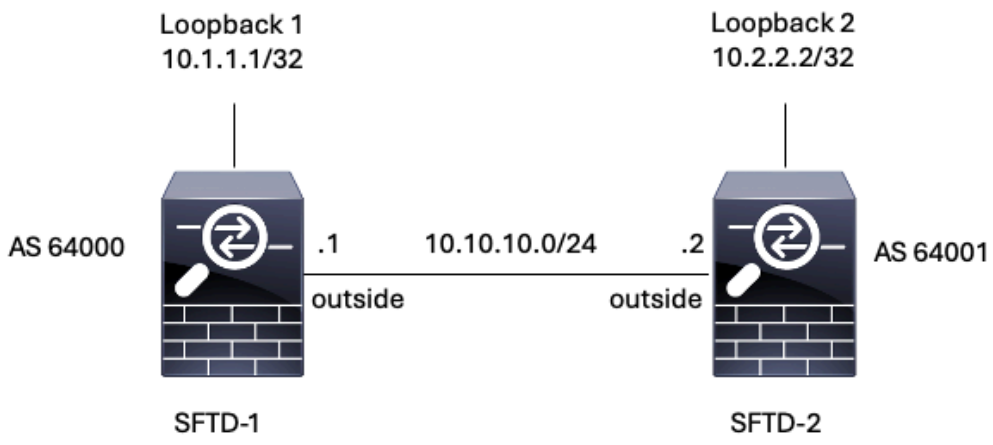

圖1.埃斯庫納里奧圖表

環回配置

步驟 1.按一下Devices > Device Management，然後選擇您要配置環回的裝置。

步驟 2.按一下Interfaces > All Interfaces。

步驟 3.按一下Add Interface > Loopback Interface。

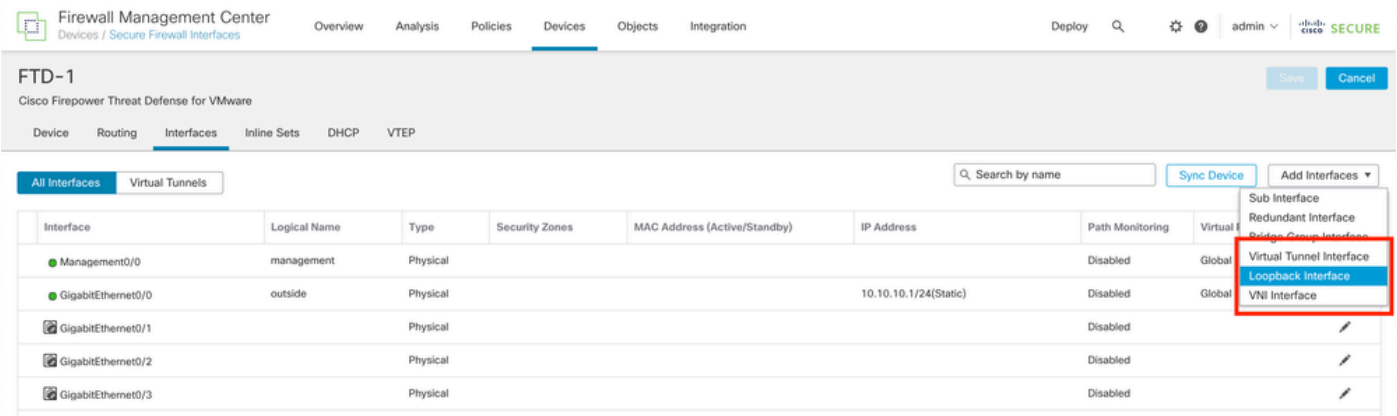

圖2.增加介面環回

步驟 4. 在常規部分中，配置環回的名稱，選中已啟用框，然後配置環回ID。

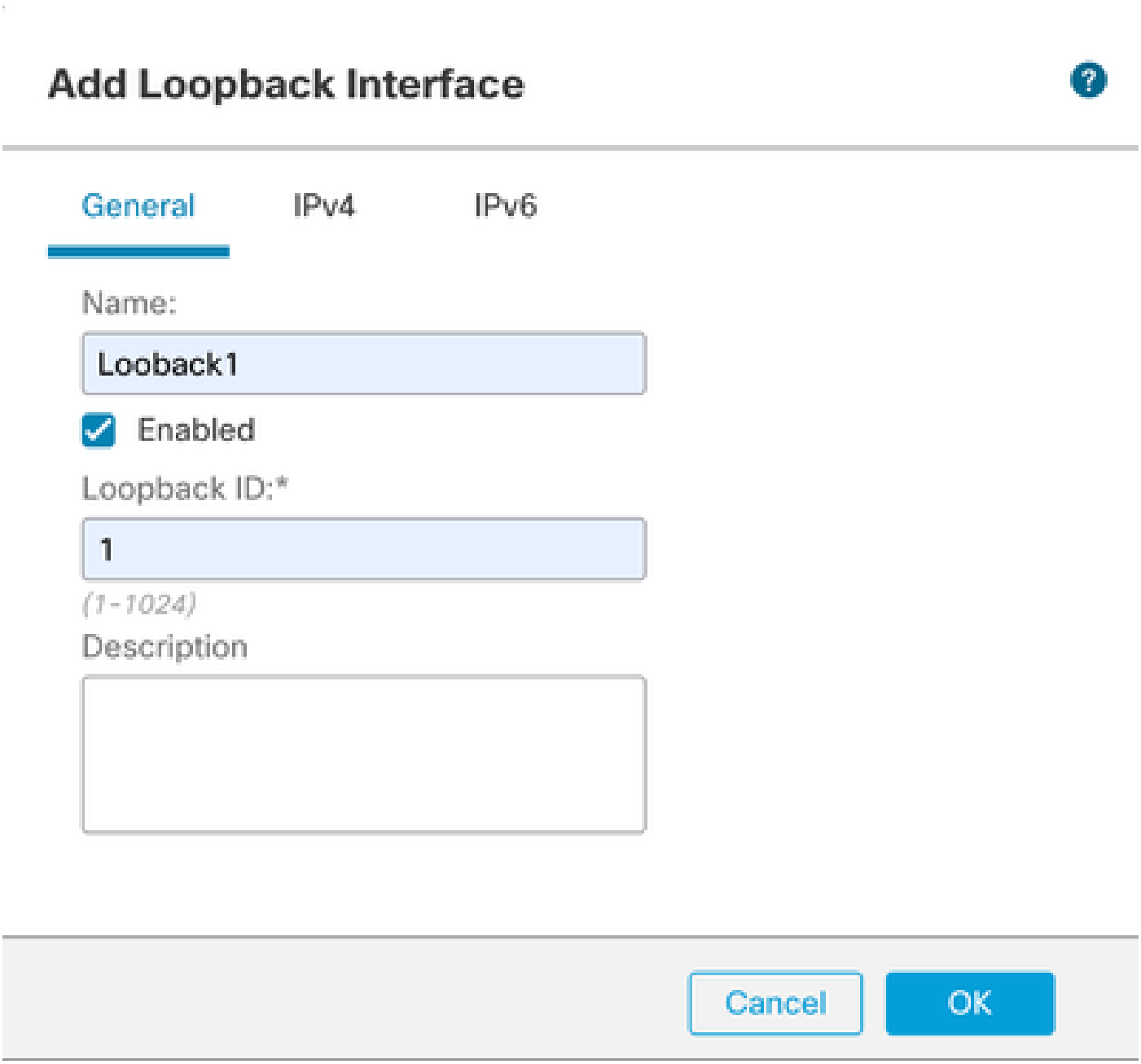

圖3.基本環回介面配置

步驟 5.在IPv4部分中，在IP Type部分選擇Use Static IP選項，配置環回IP，然後按一下OK儲存更改。

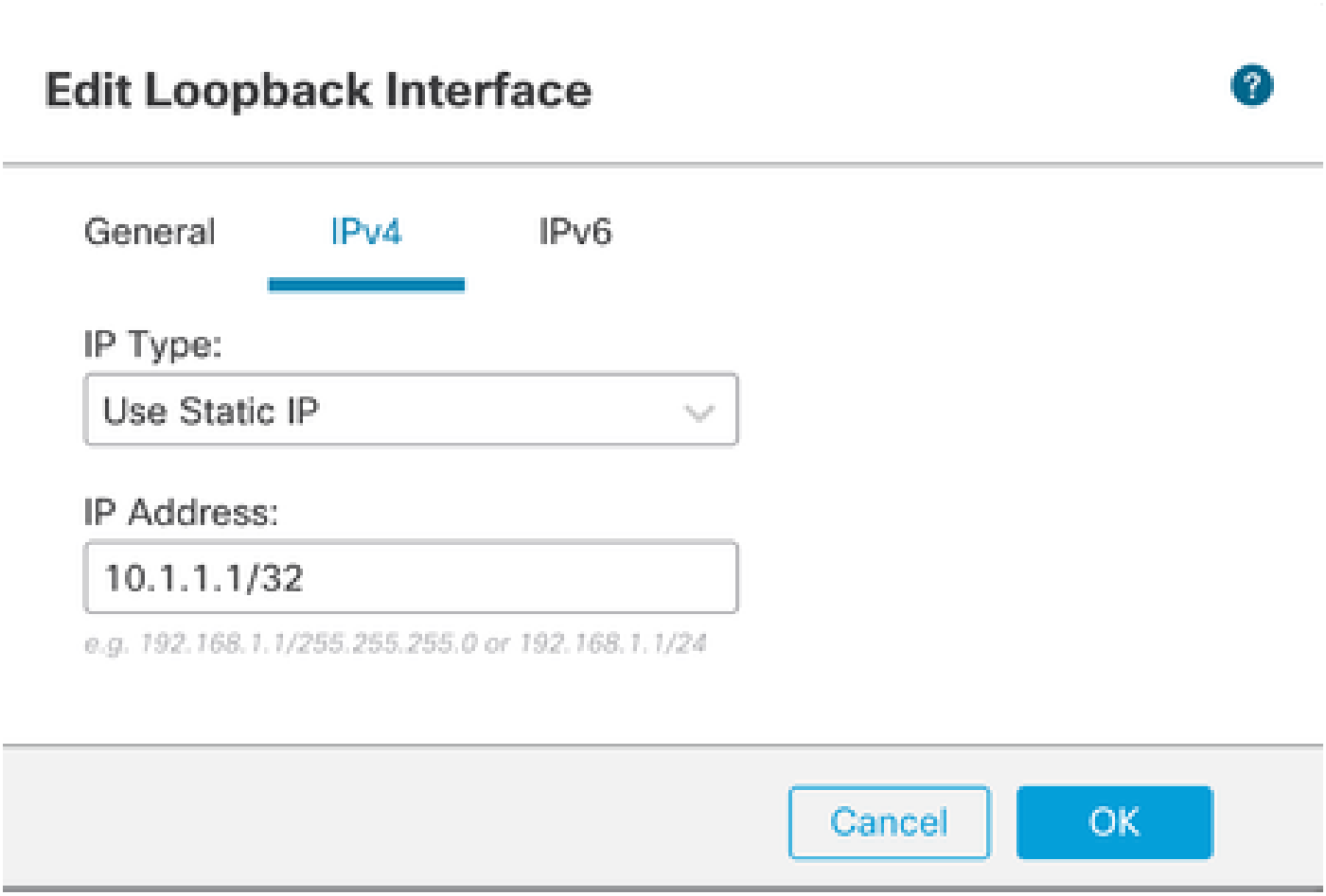

圖4.環回IP地址配置

步驟 6.點選儲存。

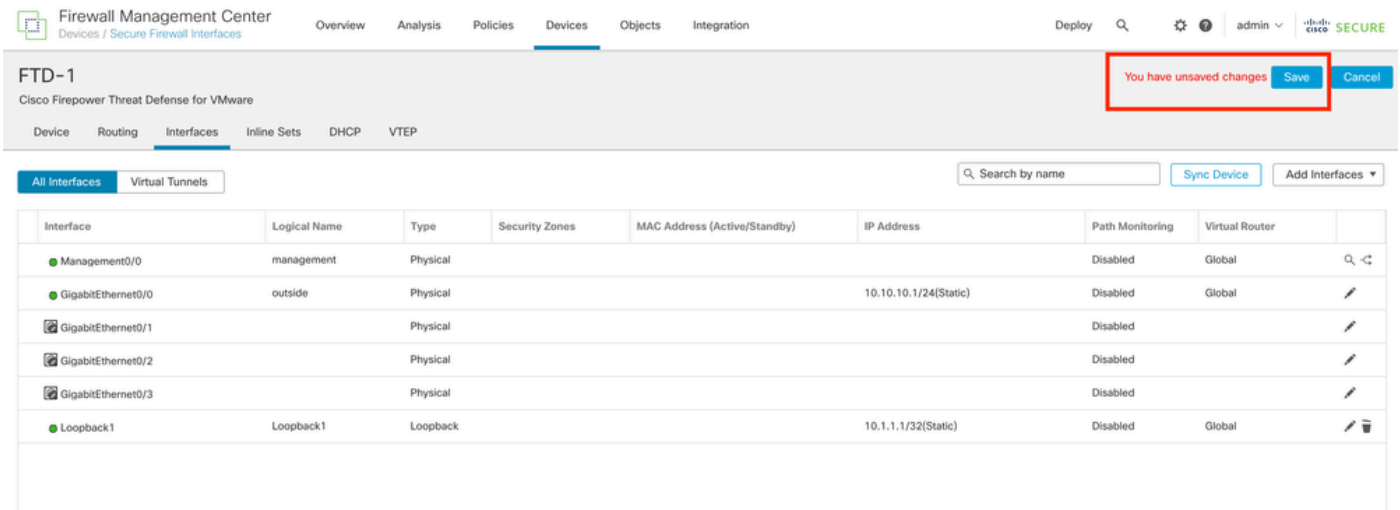

圖5.儲存環回介面配置

步驟 7.對第二個防火牆重複此過程。

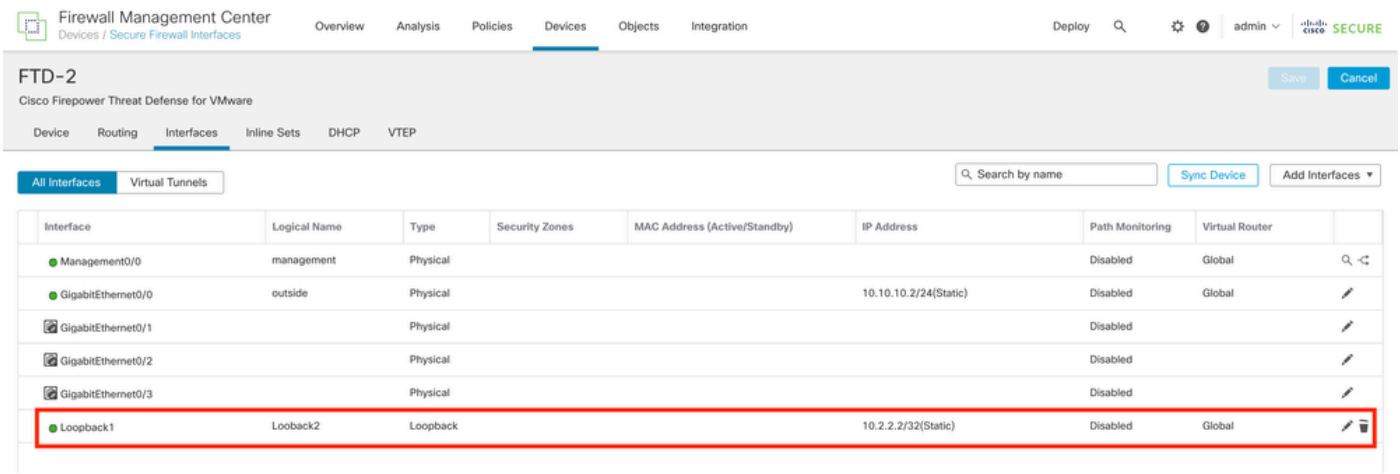

圖6.對等體上的環回介面配置

靜態路由配置

必須配置靜態路由，以確保用於對等操作的遠端對等體地址（環回）可透過所需介面訪問。

步驟 1.按一下Devices > Device Management，然後選擇您要配置靜態路由的裝置。

步驟 2.按一下Routing > Manage Virtual Routers > Static Route，然後按一下Add Route。

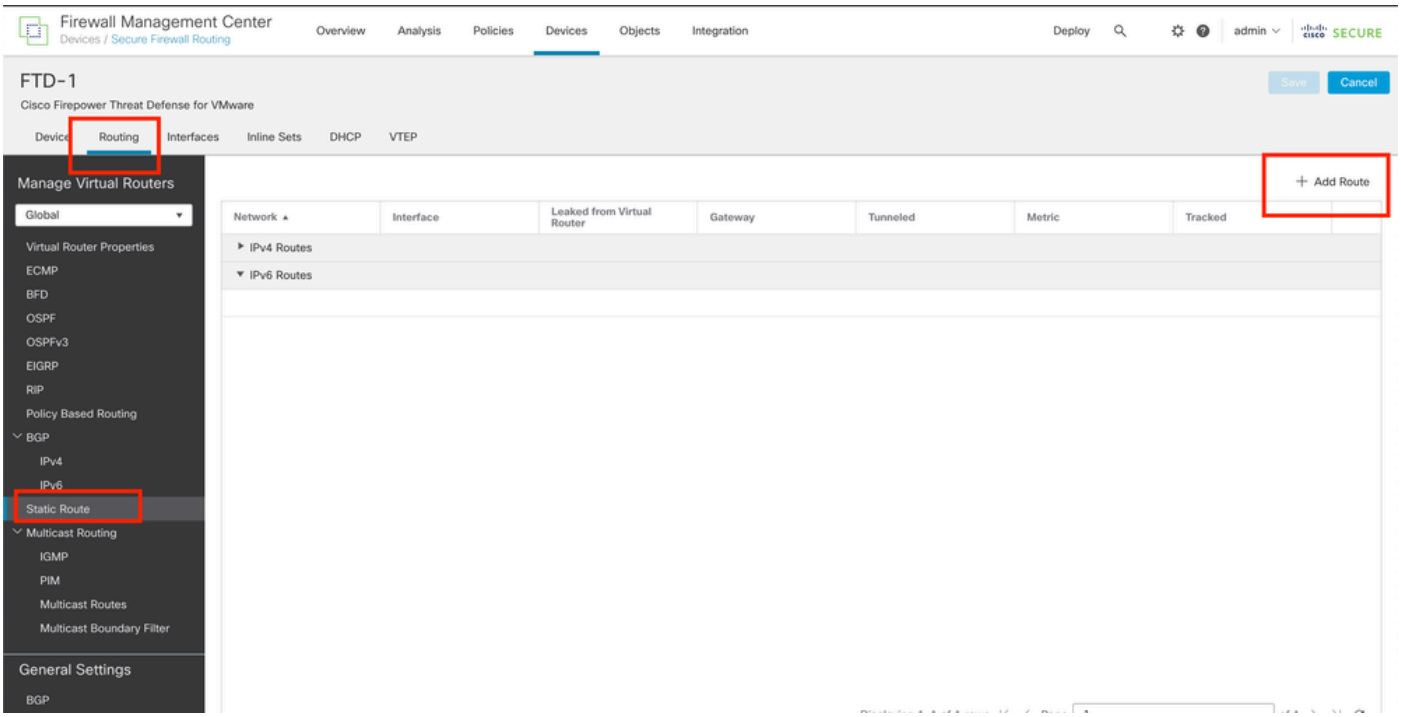

圖7.增加新的靜態路由

步驟 3.選中Type的IPv4選項。在Interface選項中選擇用於到達遠端對等體的環回的物理介面，然後指定用於到達Gateway部分的Loopback的下一跳。

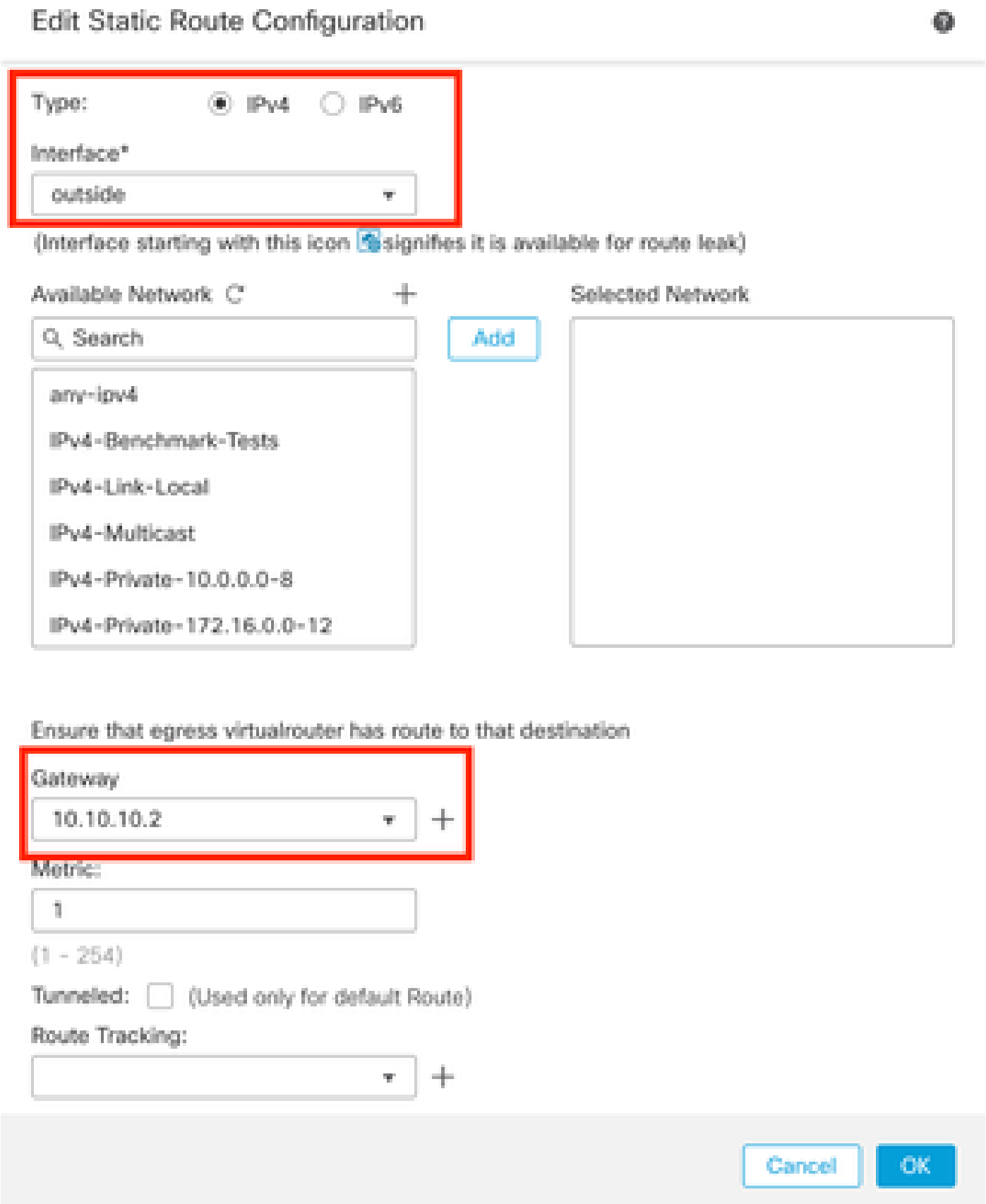

圖8.靜態路由配置

步驟 4. 點選可用網路部分旁邊的圖示(+)。

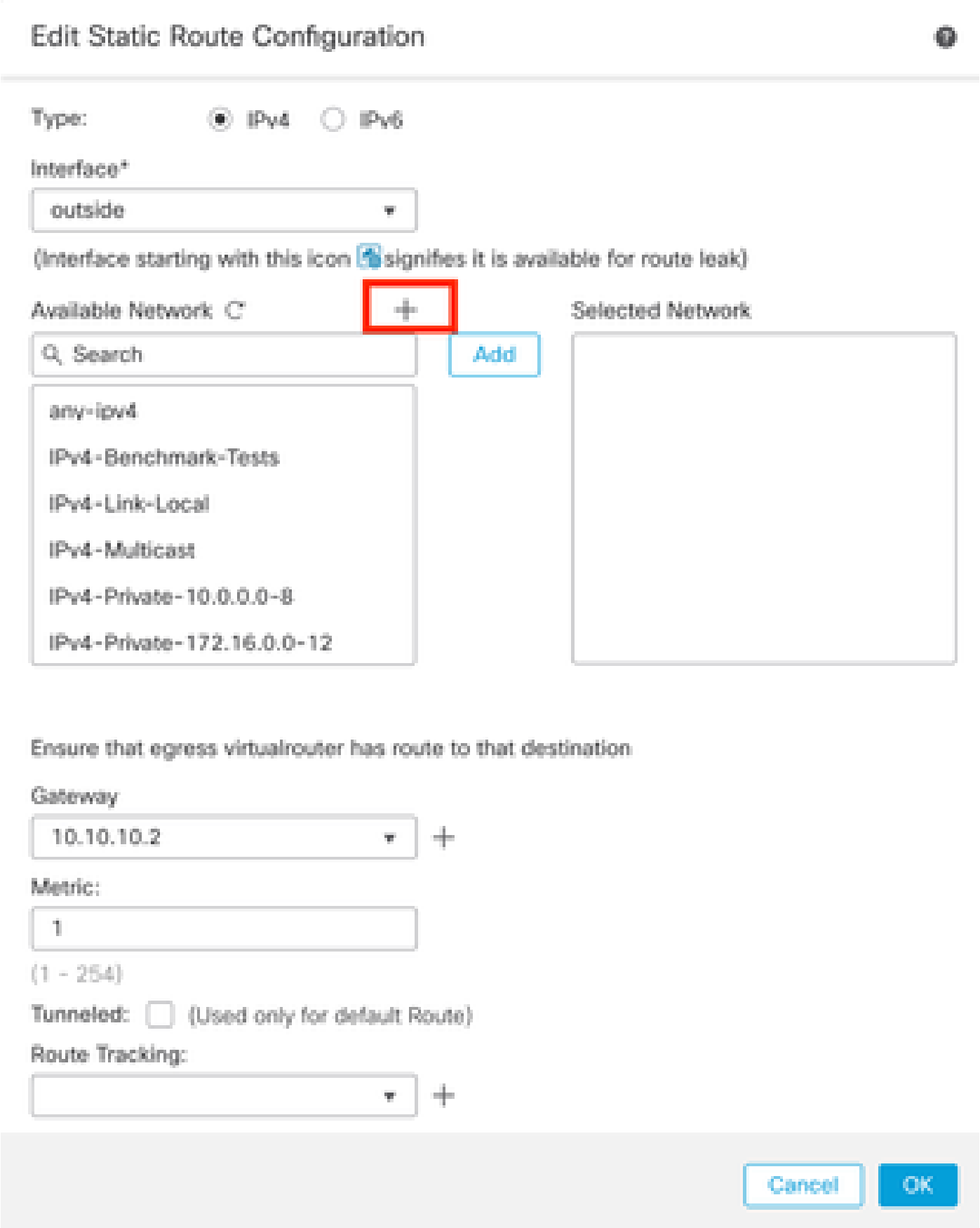

圖9.新增網路物件

步驟 5.配置供參考的名稱以及遠端對等體的Looback的IP，然後按一下Save。

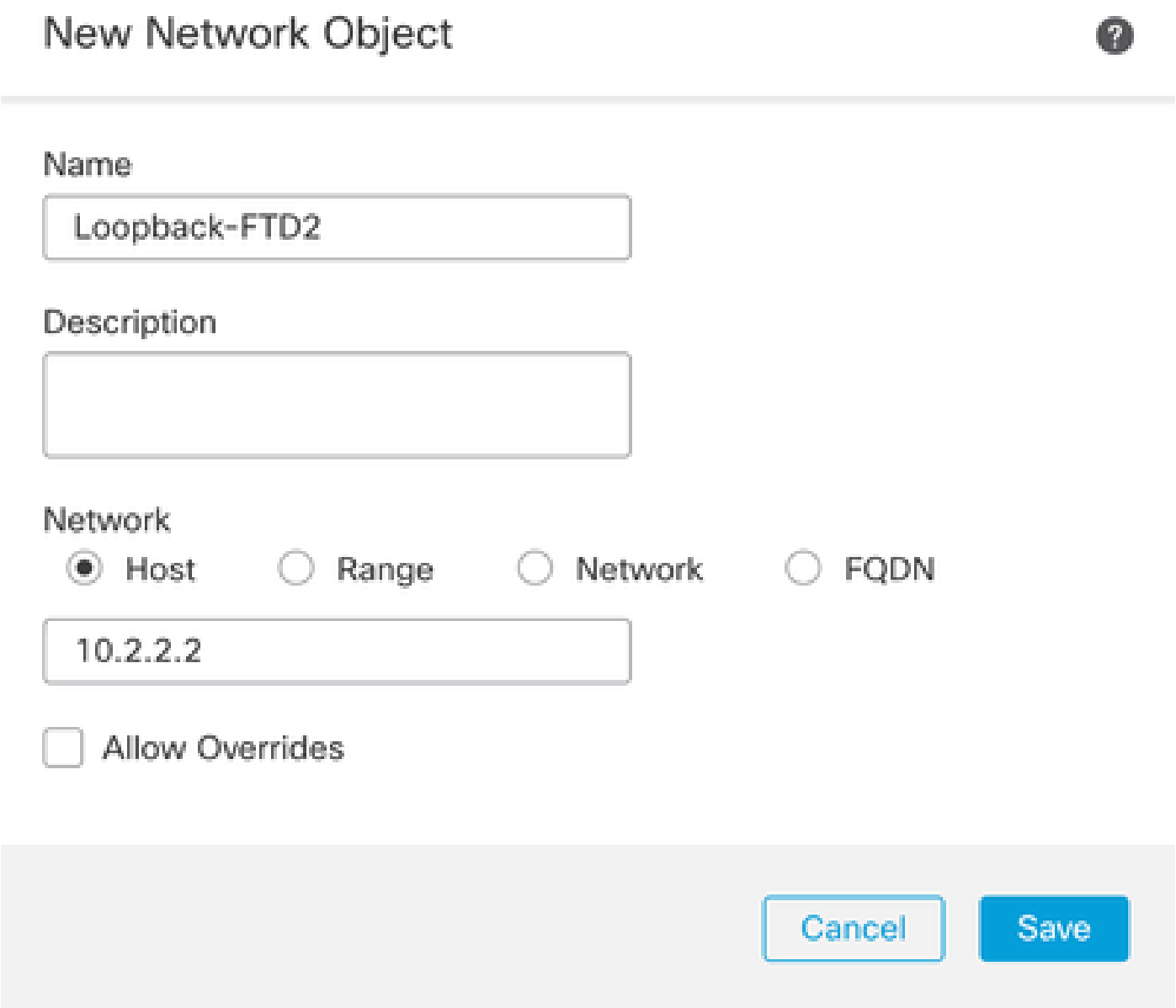

圖10.在靜態路由中配置網路目標

步驟 6.搜尋在搜尋欄中建立的新對象，選擇該對象，然後按一下Add，再按一下OK。

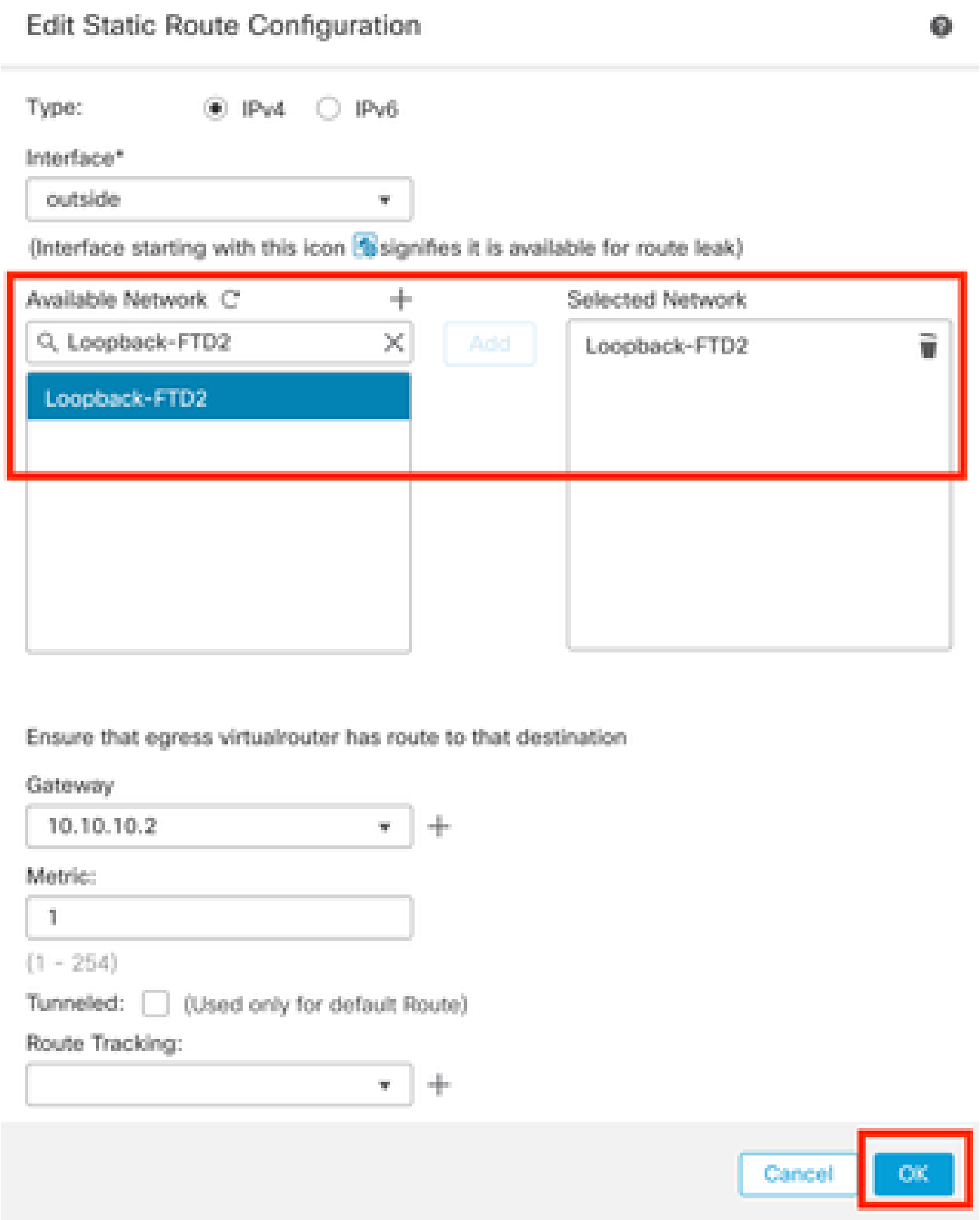

圖11.配置靜態路由中的下一跳

步驟 7.點選儲存。

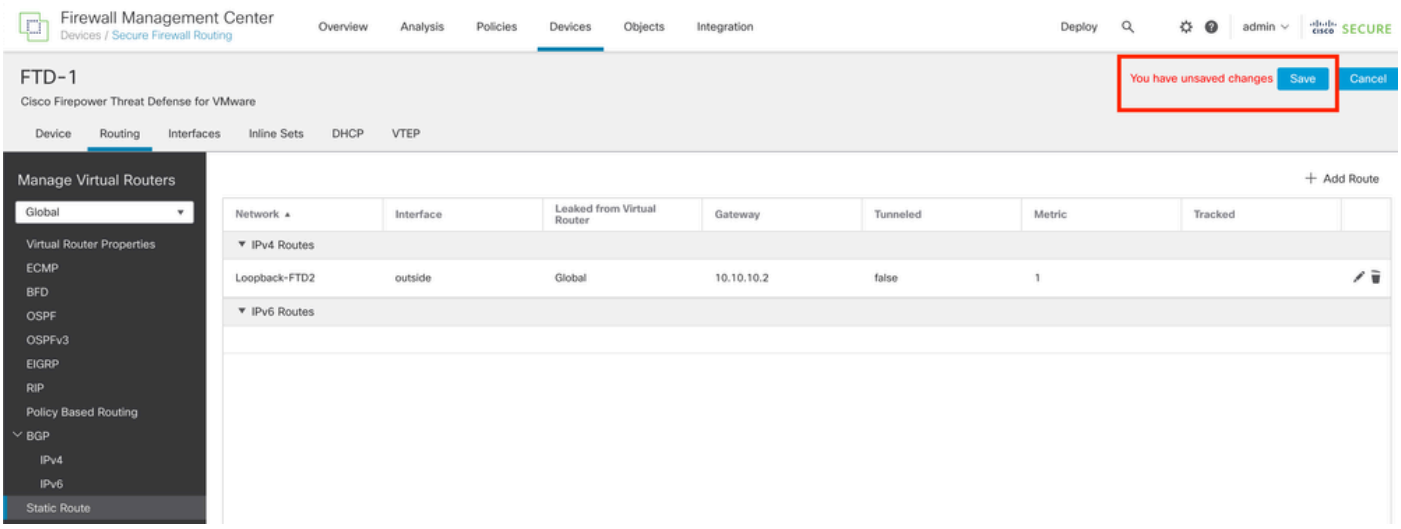

圖12.儲存靜態路由介面配置

步驟 8.對第二個防火牆重複此過程。

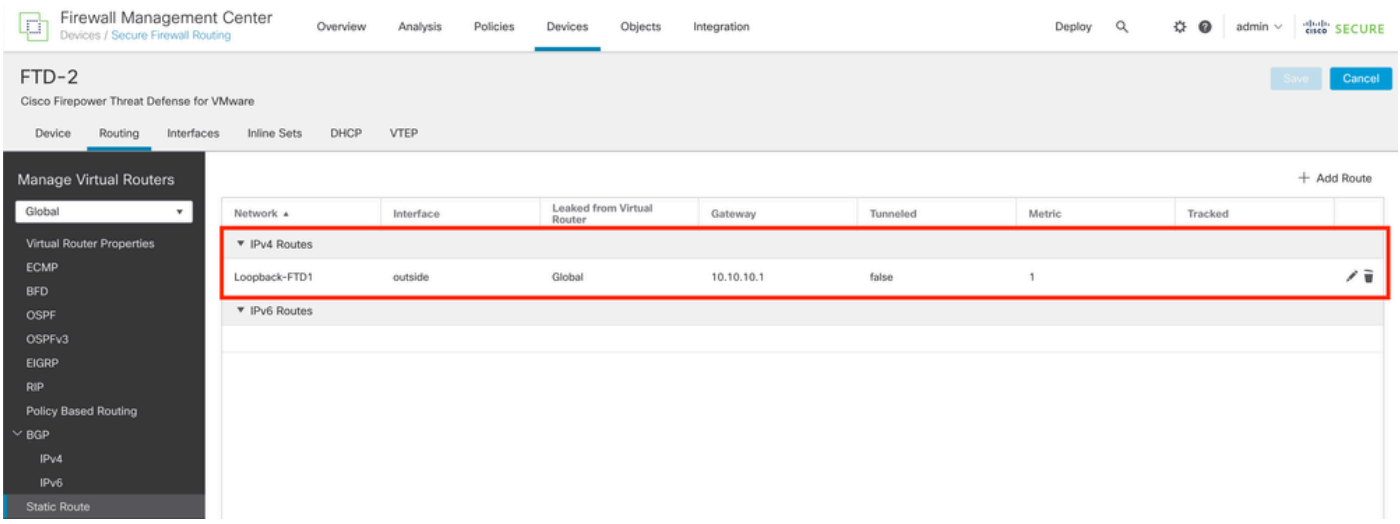

圖13.配置對等體上的靜態路由

BGP配置

步驟 1.按一下Devices > Device Management，然後選擇您要啟用BGP的裝置。

步驟 2. 按一下Routing > Manage Virtual Routers > General Settings，然後按一下BGP。

步驟 3.選中Enable BGP框，然後在AS Number部分配置防火牆的本地AS。

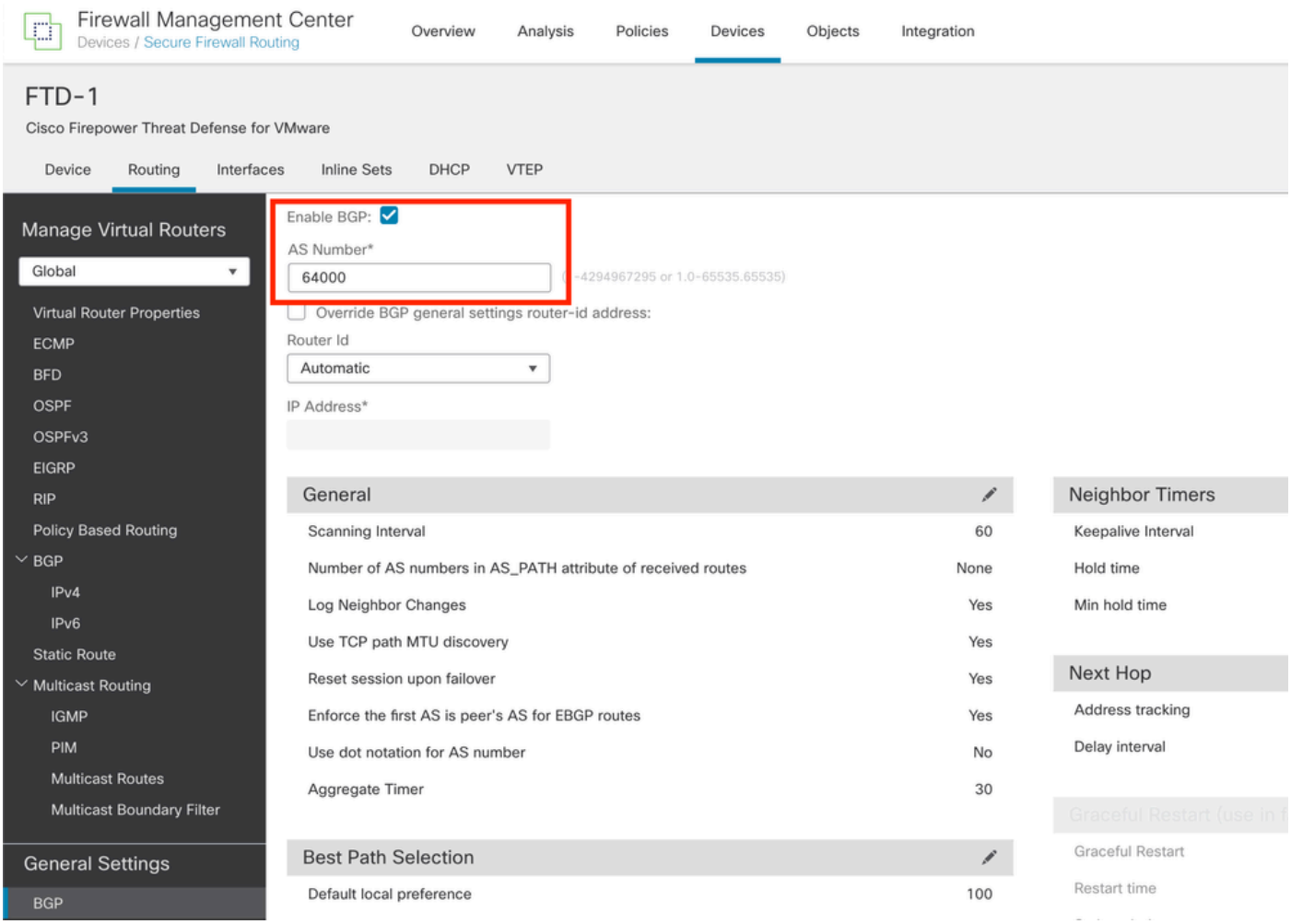

圖14.全局啟用BGP

步驟 4.按一下Save按鈕儲存更改。

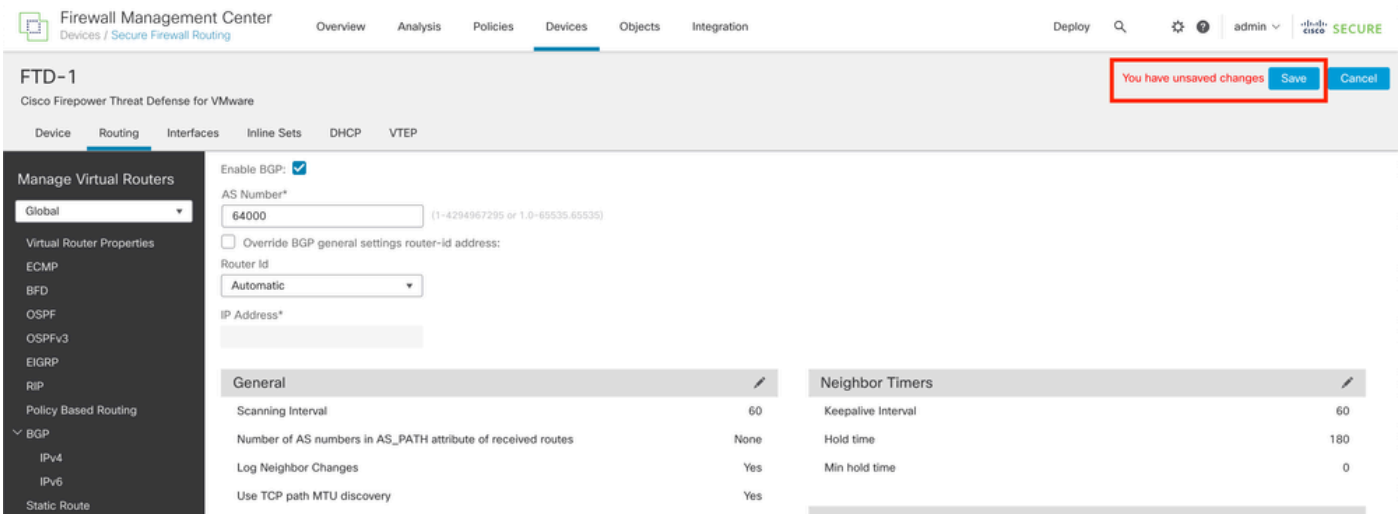

圖15.儲存BGP啟用更改

步驟 5.在管理虛擬路由器部分中，轉到BGP 選項，然後按一下IPv4。

步驟 6.選中Enable IPv4框，然後按一下Neighbor，然後按一下+ Add。

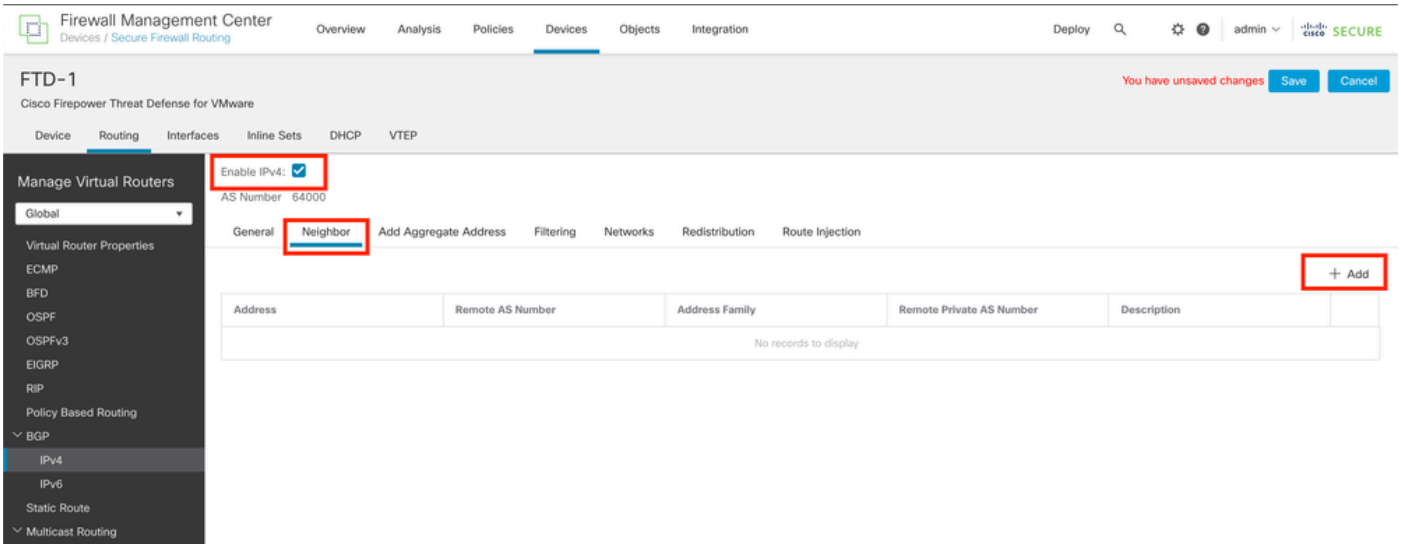

圖16.增加新的BGP對等體

步驟 7.在IP Address 部分中配置遠端對等體的IP地址，然後在Remote AS 部分中配置遠端對等體的AS，並選中Enable address 框。

步驟 8.在Update Source部分中選擇本地介面Loopback。

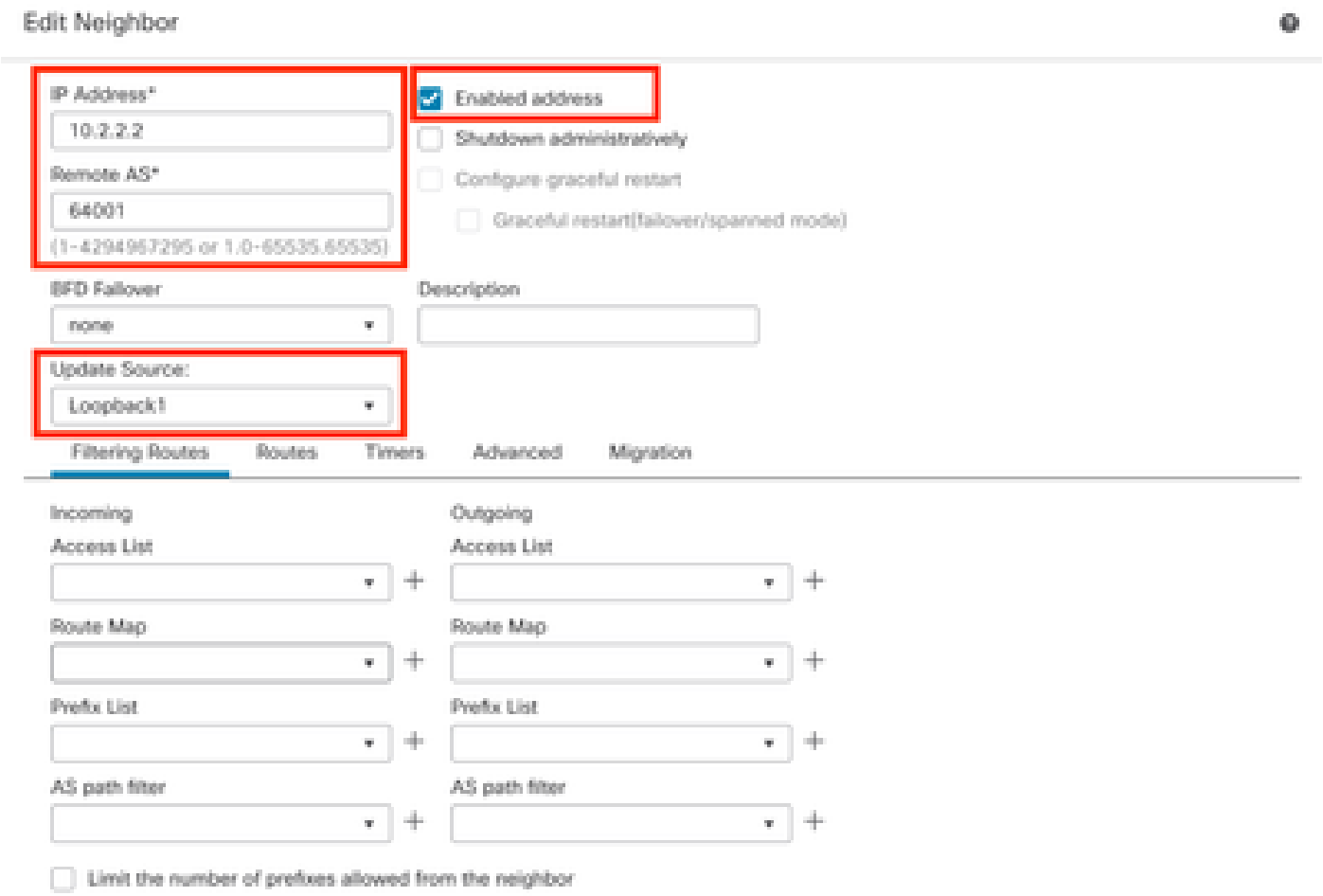

圖17.基本BGP對等體引數

注意：Update Source 選項用於啟用neighbor update-source 命令，該命令用於允許任何工作

介面（包括環回）。可以指定此命令以建立TCP連線。

步驟 9.按一下Advanced，然後在TTL Hops 選項中配置數字2，然後按一下OK。

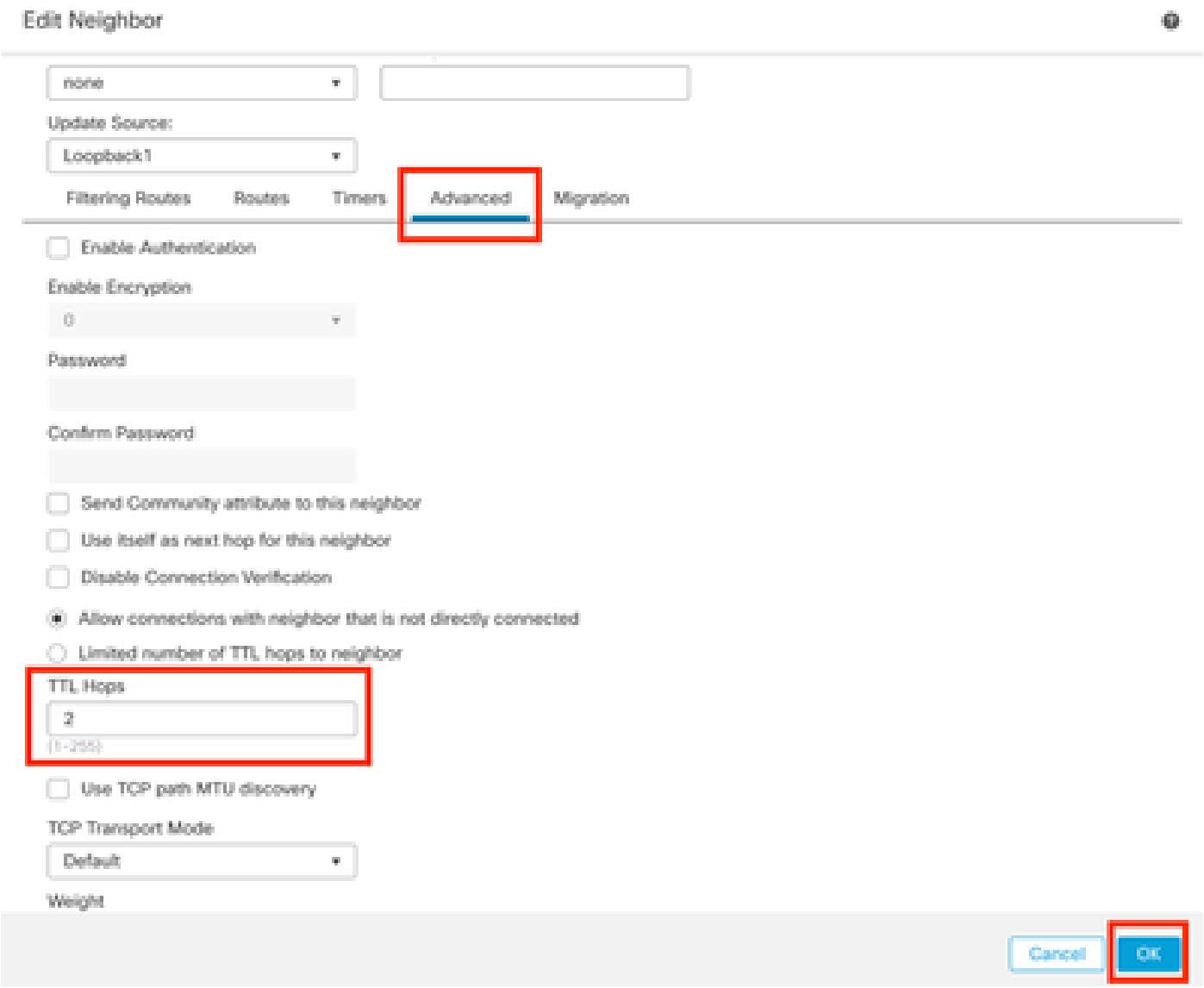

圖18.配置TTL跳數

注意：TTL Hops 選項用於啟用ebgp-multihop 命令，該命令用於更改TTL值，以允許資料包到達非直連的外部BGP對等體或具有直連介面以外的介面。

步驟 10.點選儲存並部署更改。

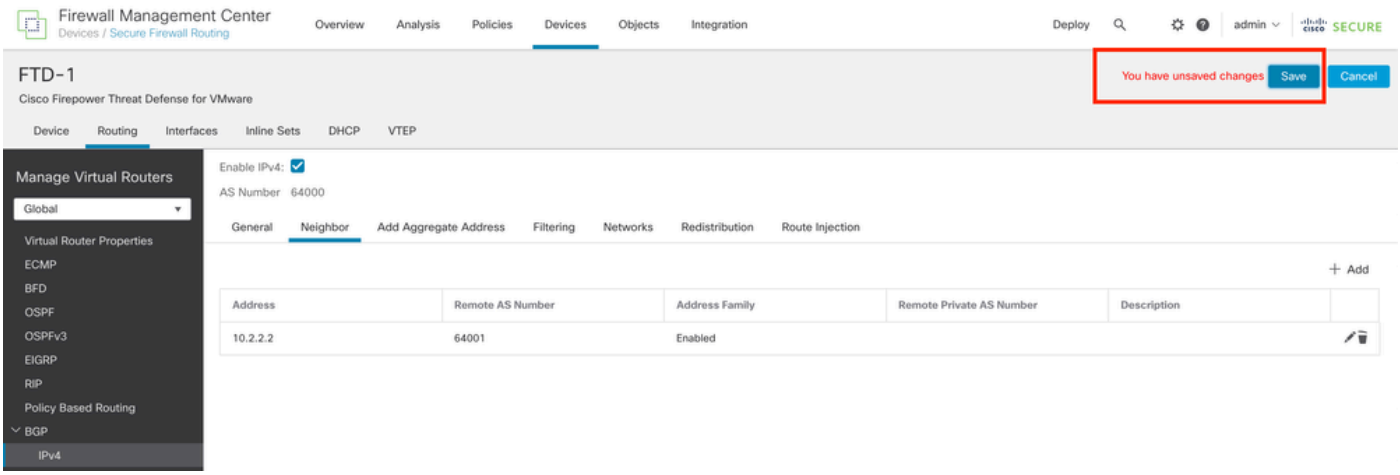

圖19.儲存BGP配置

步驟 11.對第二個防火牆重複此過程。

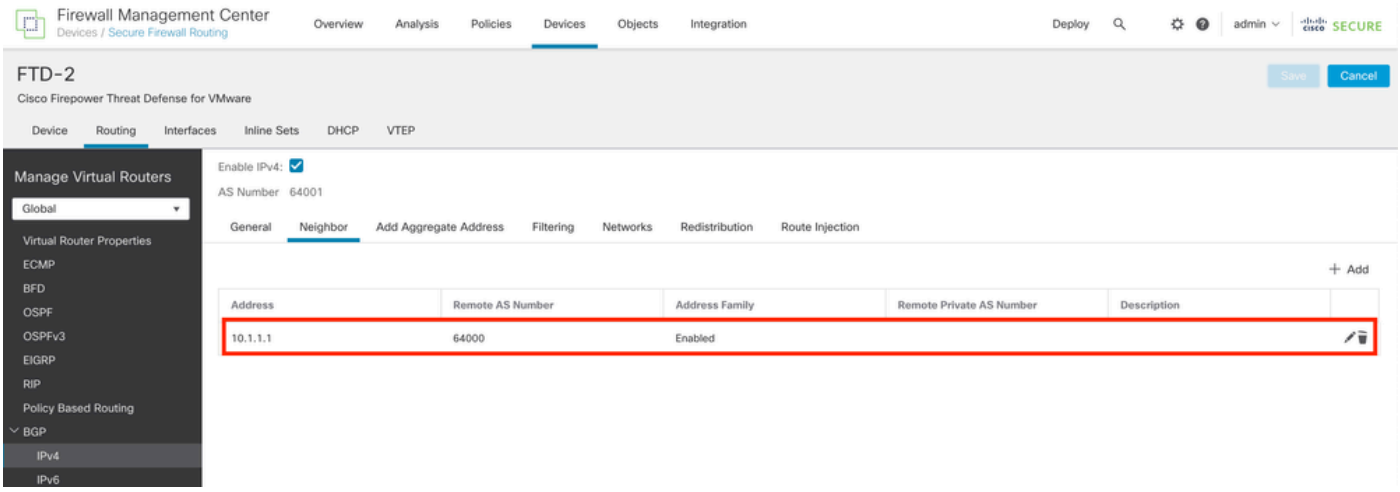

圖20.配置對等體上的BGP

驗證

步驟 1.驗證環回和靜態路由配置，然後使用ping測試檢查BGP對等體之間的連線。

show running-config interface interface_name

show running-config route

show destination_ip

SFTD-1	SFTD-2
show running-config interface Loopback1 interface Loopback1 nameif Loopback1	show running-config interface Loopback1 interface Loopback1 名稱Looback2

IP 網址 10.1.1.1 255.255.255.255 show running-config route 10.2.2.2 255.255.255.255 10.10.10.2外部的路由1 ping 10.2.2.2 向10.2.2.2傳送5,100位元組ICMP響應，超時為2秒： !!!!! 成功率為100% (5/5)，往返最小/平均/最大= 1/1/1毫秒	IP 網址 10.2.2.2 255.255.255.255 show running-config route 10.1.1.1 255.255.255.255 10.10.10.1外部的路由1 ping 10.1.1.1 向10.1.1.1傳送5,100位元組ICMP響應，超時為2秒： !!!!! 成功率為100% (5/5)，往返最小/平均/最大= 1/1/1毫秒

步驟 2.驗證BGP配置，然後確保BGP對等已建立。

show running-config router bgp

show bgp neighbors

show bgp summary

SFTD-1	SFTD-2

show running-config router bgp
 	
路由器bgp 64000
 	
bgp log-neighbor-changes
 	
bgp router-id vrf auto-assign
 	
address-family ipv4 unicast
 	
  neighbor 10.2.2.2 remote-as 64001
 	
  neighbor 10.2.2.2 ebgp-multihop 2
 	
  neighbor 10.2.2.2 transport path-mtu-discovery disable
 	
  neighbor 10.2.2.2 update-source Loopback1
 	
  鄰居10.2.2.2啟用
 	
  no auto-summary
	show running-config router bgp
	
	路由器bgp 64001
	
	bgp log-neighbor-changes
	
	bgp router-id vrf auto-assign
	
	address-family ipv4 unicast
	
	  neighbor 10.1.1.1 remote-as 64000
	
	  neighbor 10.1.1.1 ebgp-multihop 2
	
	  neighbor 10.1.1.1 transport path-mtu-discovery disable
	
	  neighbor 10.1.1.1 update-source Looback2
	
	  鄰居10.1.1.1啟用
	
	  no auto-summary

無同步 exit-address-family ! show bgp neighbors | i BGP BGP鄰居是10.2.2.2，vrf single_vf，遠端AS 64001，外部鏈路 BGP版本4，遠端路由器ID 10.2.2.2 BGP狀態= Established，持續1d15h BGP表版本7，鄰居版本7/0 外部BGP鄰居可能距離最多2跳。 show bgp summary BGP路由器識別符號10.1.1.1，本地AS編號 64000 BGP表版本為7，主路由表版本為7 鄰居V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.2.2.2 4 64001 2167 2162 7 0 0 1d15h 0	無同步 exit-address-family ! show bgp neighbors | i BGP BGP鄰居是10.1.1.1，vrf single_vf，遠端AS 64000，外部鏈路 BGP版本4，遠端路由器ID 10.1.1.1 BGP狀態= Established，持續1d16h BGP表版本1，鄰居版本1/0 外部BGP鄰居可能距離最多2跳。 show bgp summary BGP路由器識別符號10.2.2.2，本地AS編號 64001 BGP表版本為1，主路由表版本為1 鄰居V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.1.1.1 4 64000 2168 2173 1 0 0 1d16h 0

疑難排解

如果在此過程中遇到任何問題，請檢視以下文章：

·邊界閘道通訊協定(BGP)