在安全防火墙上使用环回接口配置eBGP

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

使用环回接口的eBGP配置

- 场景
- 网络图
- 环回配置
- 静态路由配置
- BGP配置
- 验证
- 故障排除

简介

本文档介绍如何使用Cisco安全防火墙上的环回接口配置eBGP。

先决条件

要求

Cisco 建议您了解以下主题：

- BGP协议

7.4.0版中引入了BGP的环回接口支持，这是安全防火墙管理中心和思科安全Firepower威胁防御所需的最低版本。

使用的组件

- 适用于VMware 7.4.1版的安全防火墙管理中心
- 2适用于VMware 7.4.1版的Cisco Secure Firepower威胁防御

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

边界网关协议(BGP)是外部网关协议(EGP)标准化的路径矢量路由协议，可提供可扩展性、灵活性和网络稳定性。具有相同自治系统(AS)的两个对等体之间的BGP会话称为内部BGP (iBGP)。具有不同自治系统(AS)的两个对等体之间的BGP会话称为外部BGP (eBGP)。

通常，使用最接近对等体的接口的IP地址建立对等体关系，但是，使用环回接口建立BGP会话很有用，因为当BGP对等体之间存在多条路径时，它不会关闭BGP会话。

注意：此进程描述了eBGP对等体使用Loopkack的过程，但对于iBGP对等体使用的是同一进程，因此可将其用作参考。

使用环回接口的eBGP配置

场景

在此配置中，防火墙SFTD-1具有IP地址为10.1.1.1/32的环回接口，并且AS 64000，防火墙SFTD-2具有IP地址为10.2.2.2/32且AS 64001的环回接口。两个防火墙均使用其外部接口到达另一个防火墙的环回接口（在本场景中，两个防火墙上均预配置了外部接口）。

网络图

本文档使用以下网络设置：

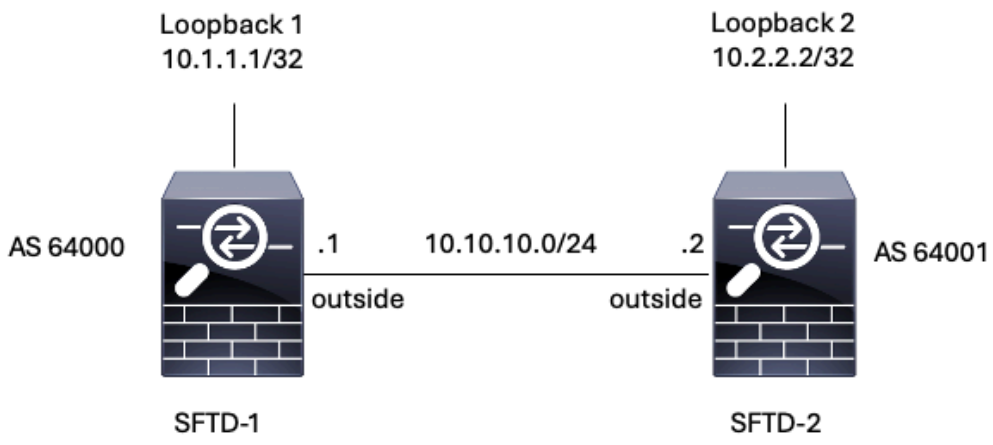

图 1.埃斯库纳里奥图

环回配置

步骤1:点击Devices > Device Management，然后选择要配置环回的设备。

第二步：单击Interfaces > All Interfaces。

第三步：单击Add Interface > Loopback Interface。

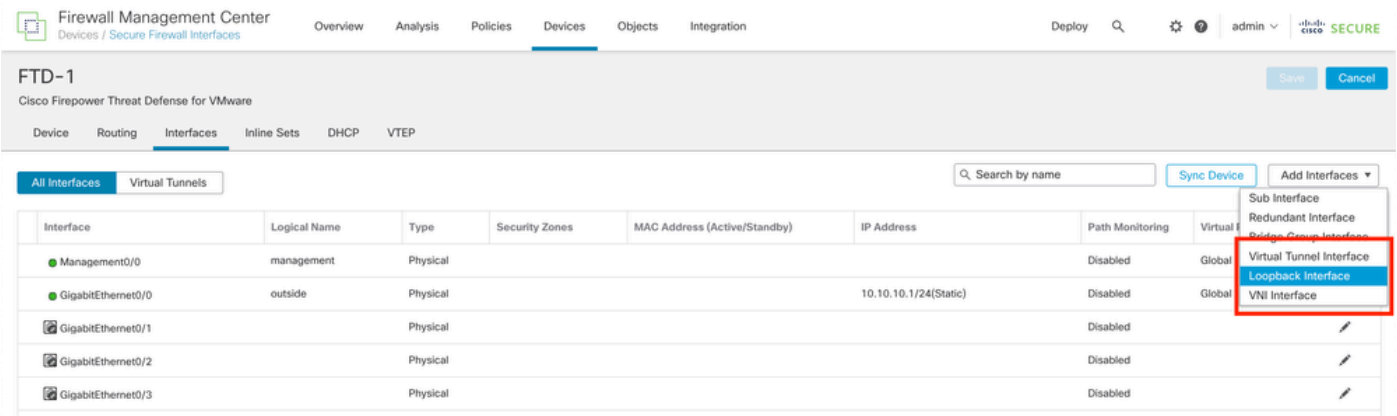

图 2.添加接口环回

第四步： 在常规部分中，配置环回接口的名称，选中已启用框，并配置环回ID。

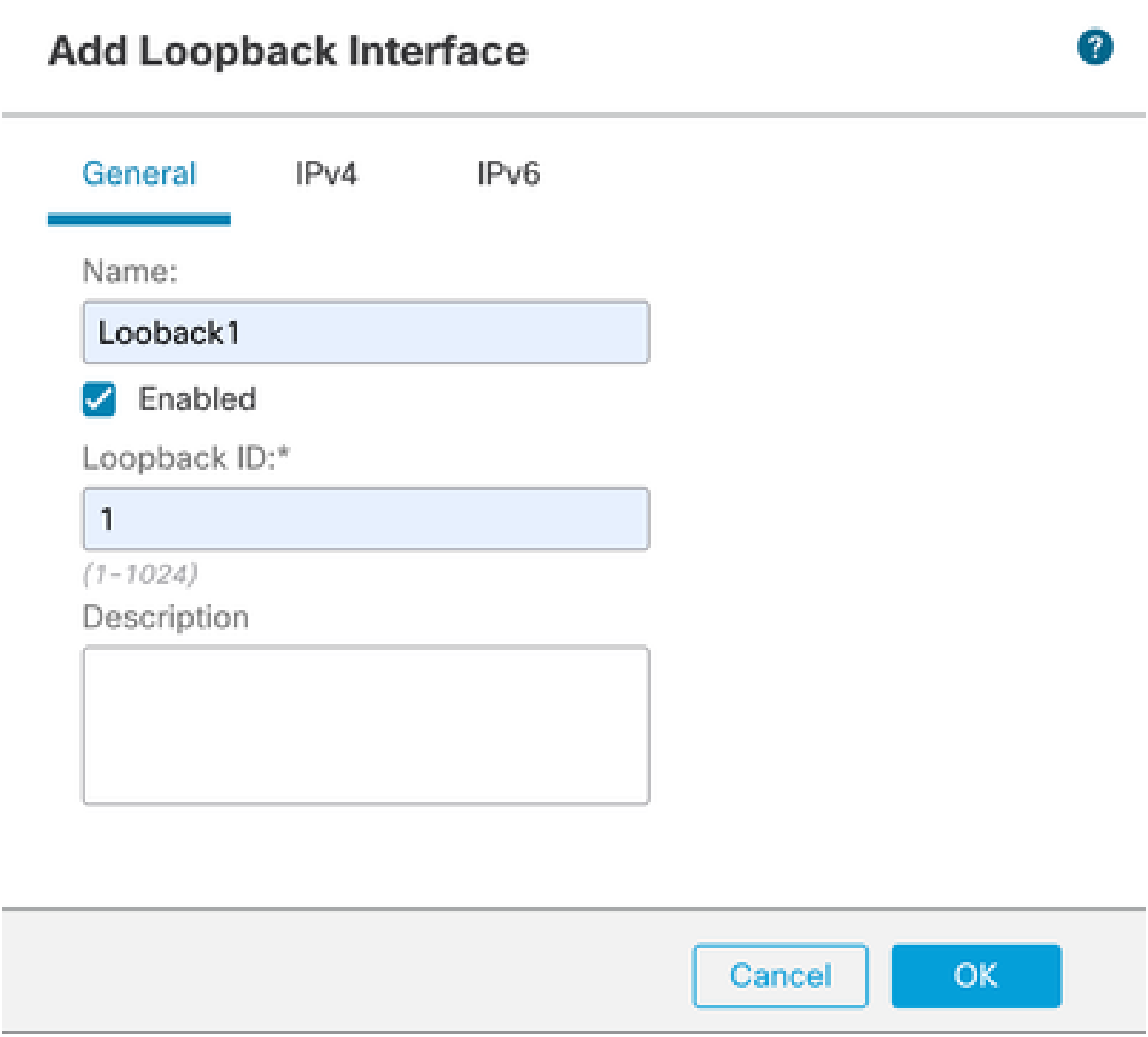

图 3.基本环回接口配置

第五步：在IPv4部分中，在IP Type部分中选择Use Static IP选项，配置环回IP，然后单击OK保存更改。

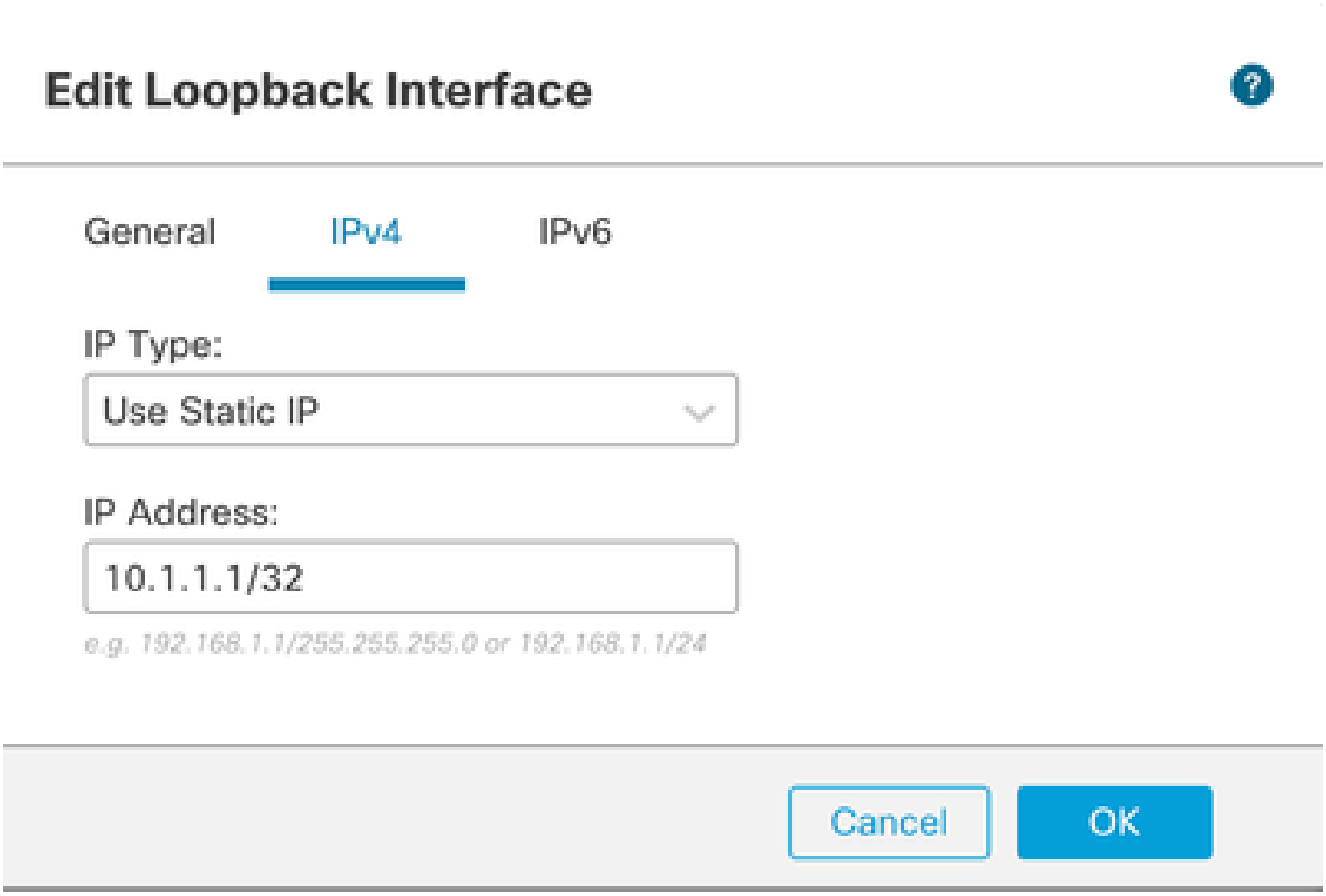

图 4.环回IP地址配置

第六步：Click Save.

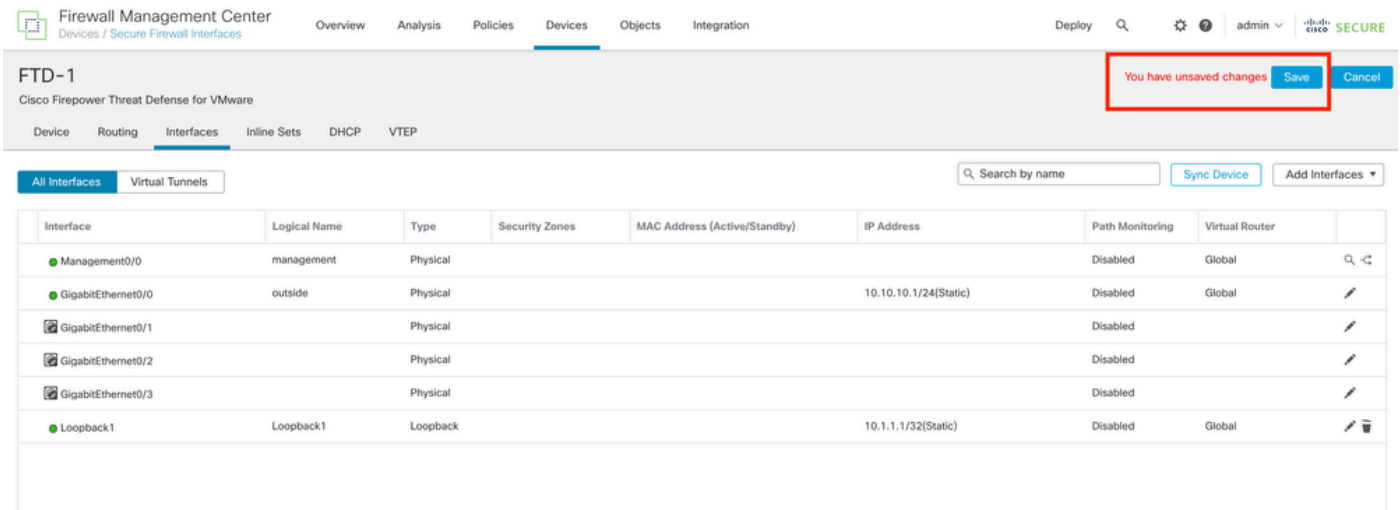

图 5.保存环回接口配置

步骤 7.对第二个防火墙重复此过程。

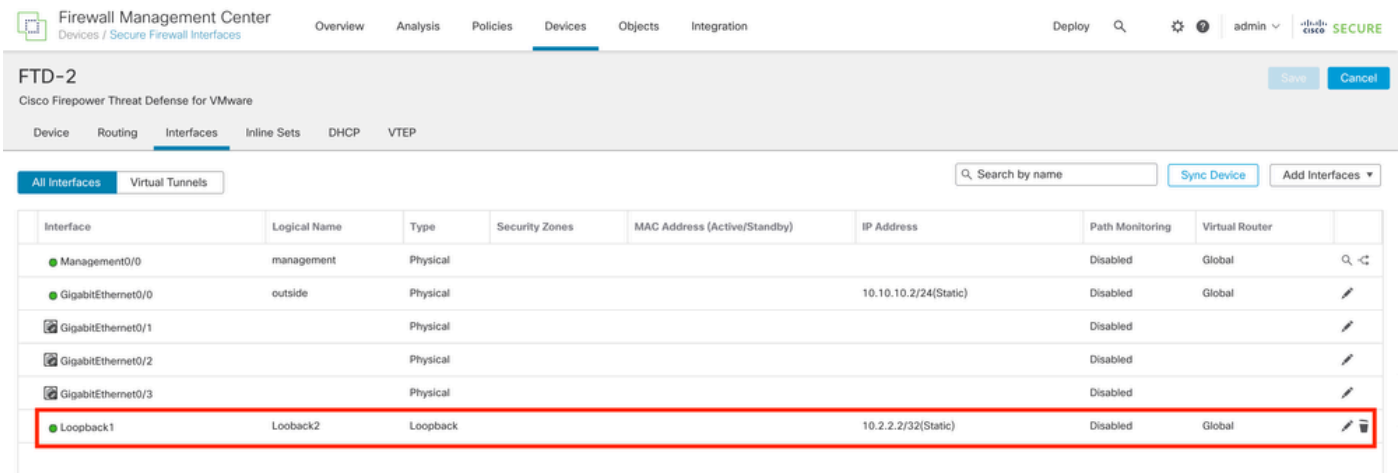

图 6.对等体上的环回接口配置

静态路由配置

必须配置静态路由，以确保用于对等连接的远程对等体地址（环回）可通过所需接口访问。

步骤1:点击Devices > Device Management，然后选择要配置静态路由的设备。

步骤 2依次单击Routing > Manage Virtual Routers > Static Route，然后单击Add Route。

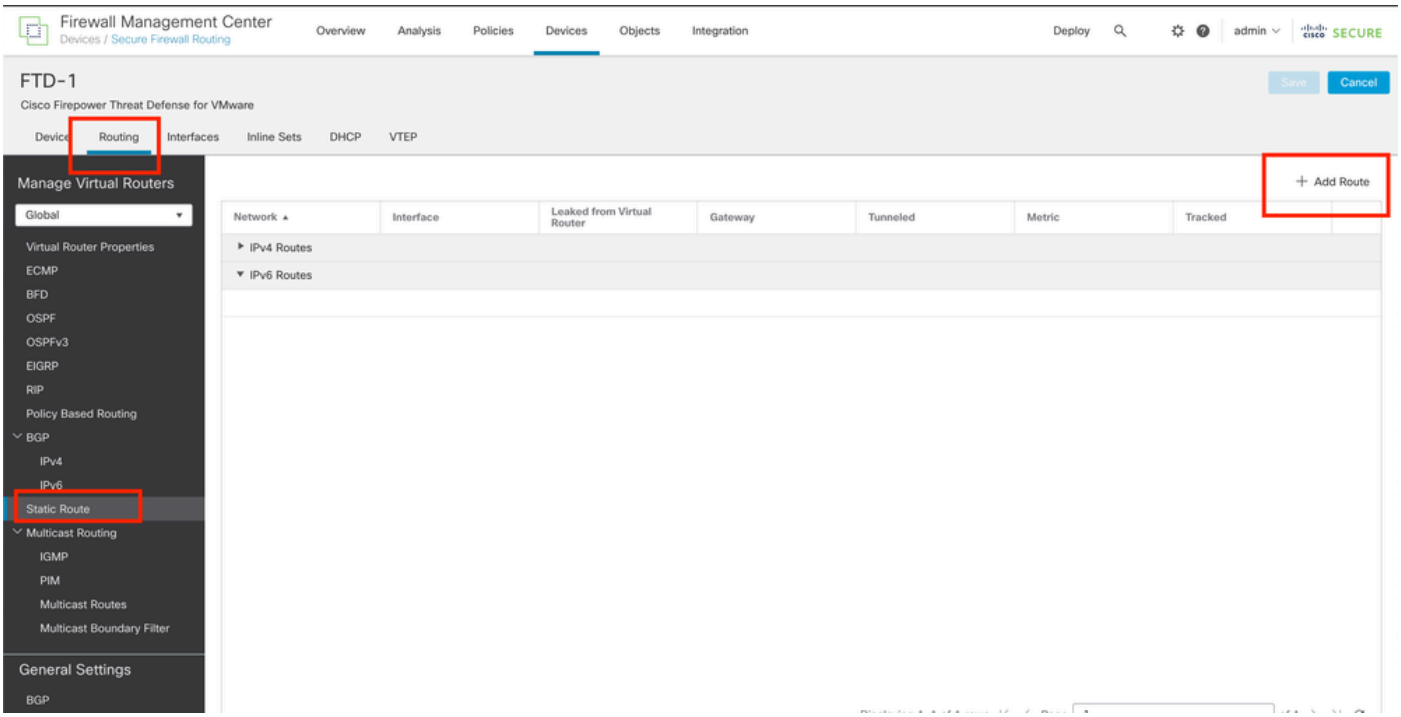

图 7.添加新的静态路由

第 3 步：选中Type的IPv4选项。在Interface选项中选择用于到达远程对等体的环回接口的物理接口，然后指定到达网关上环回接口的下一跳。

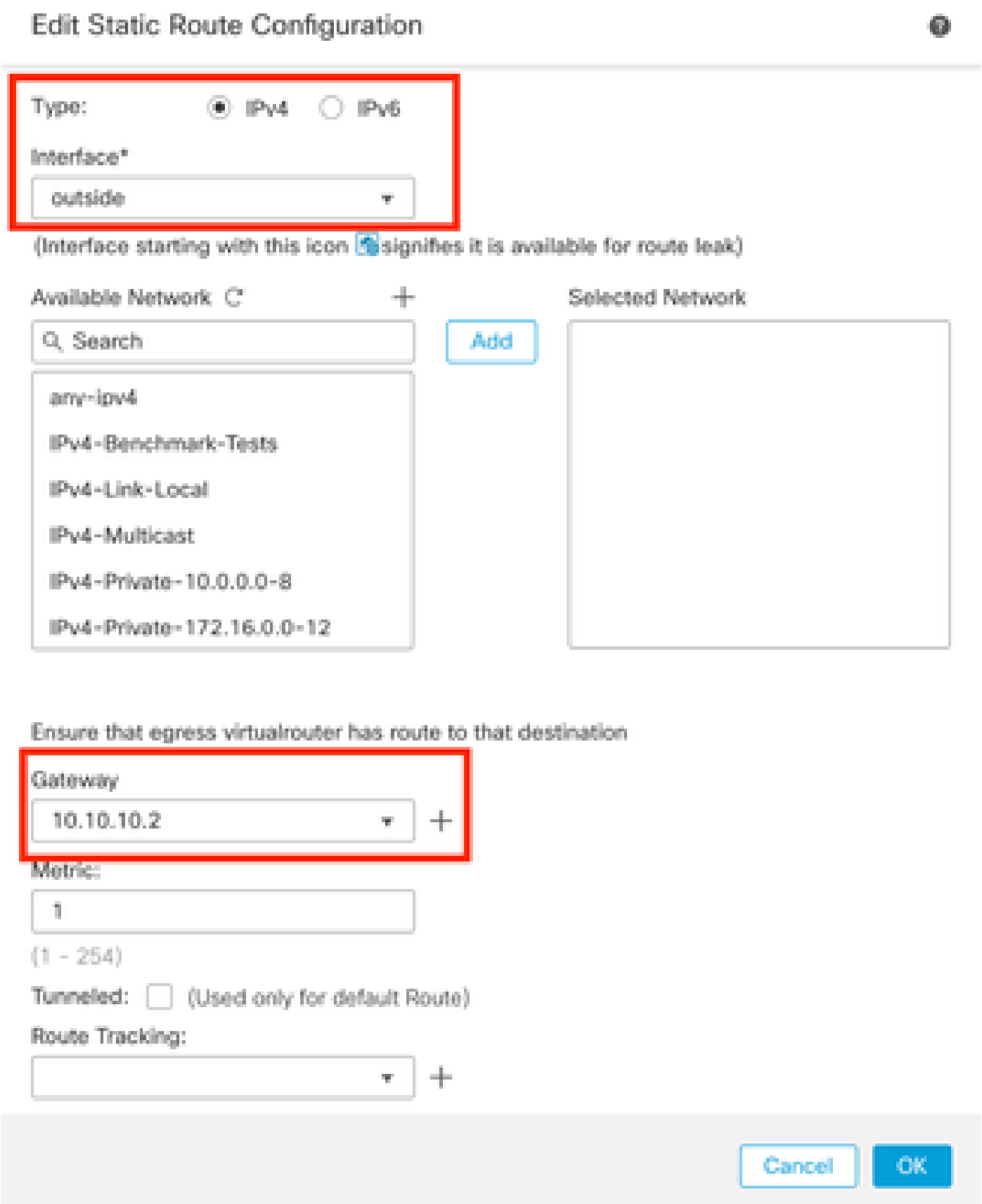

图 8.静态路由配置

第 4 步： 点击可用网络部分旁边的图标(+)。

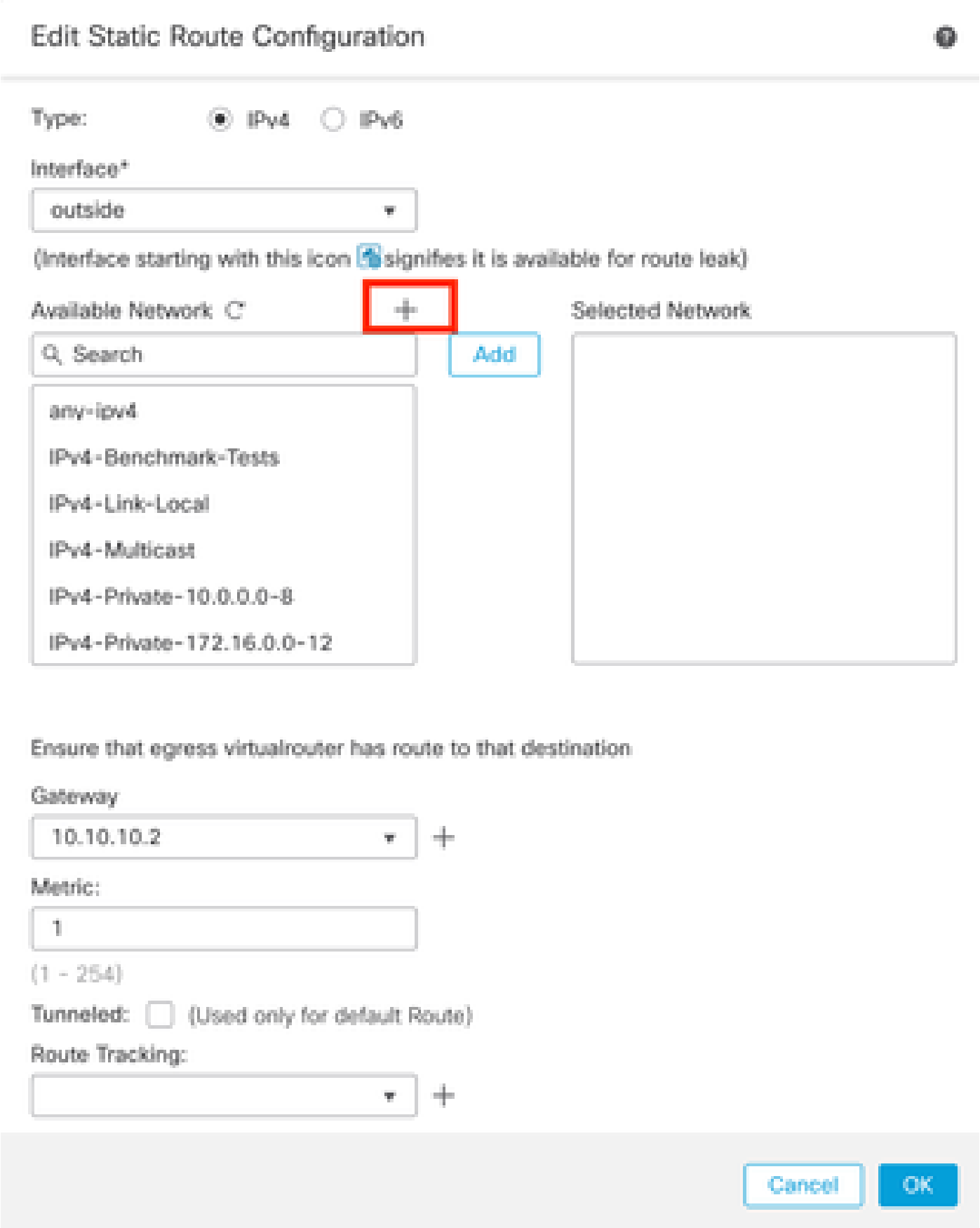

图 9.添加新网络对象

第 5 步：配置供参考的名称和远程对等体的Looback的IP地址，然后使用Save。

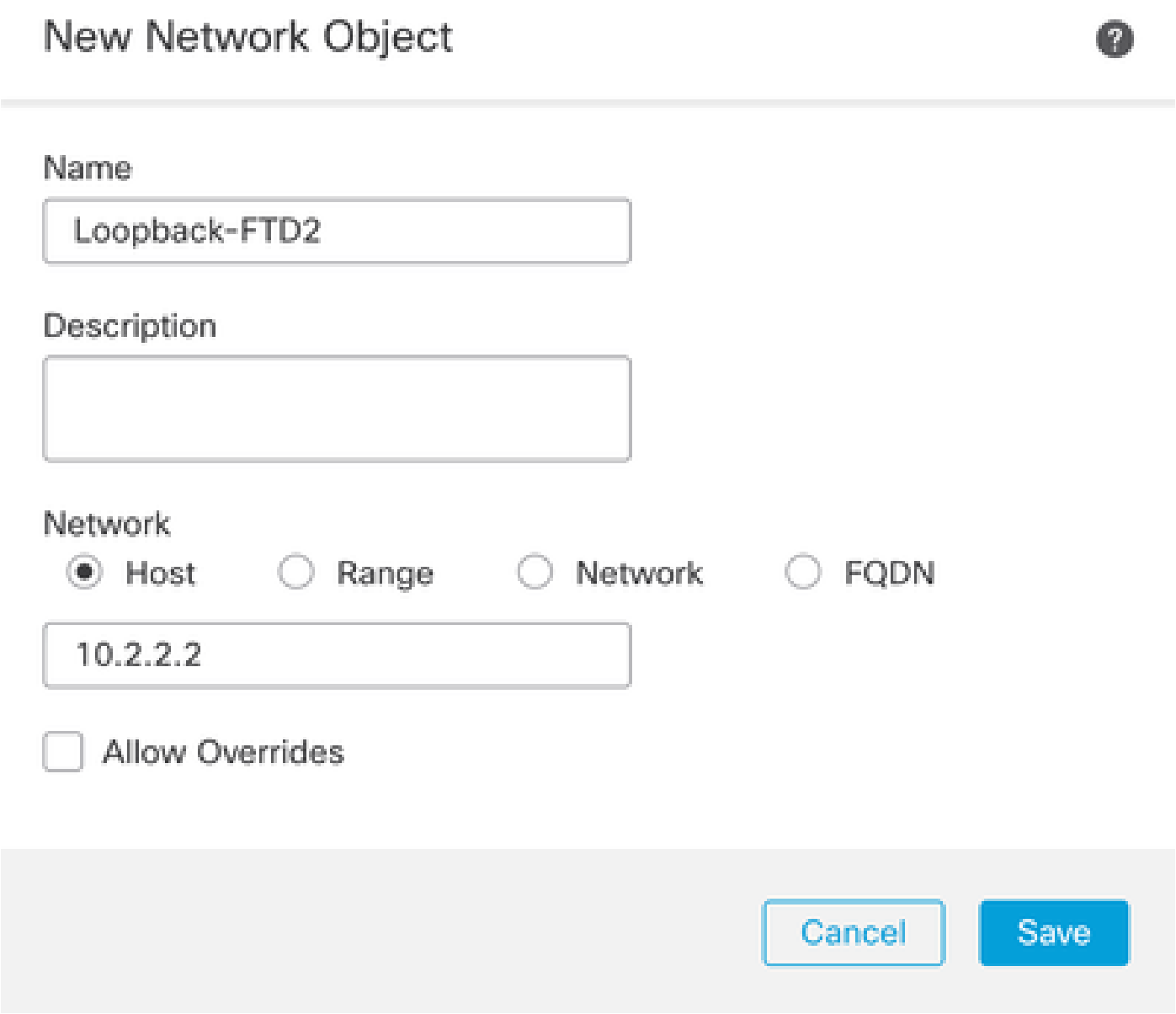

图 10.在静态路由中配置网络目标

步骤 6 搜索在搜索栏中创建的新对象，选择它，然后单击Add，再单击OK。

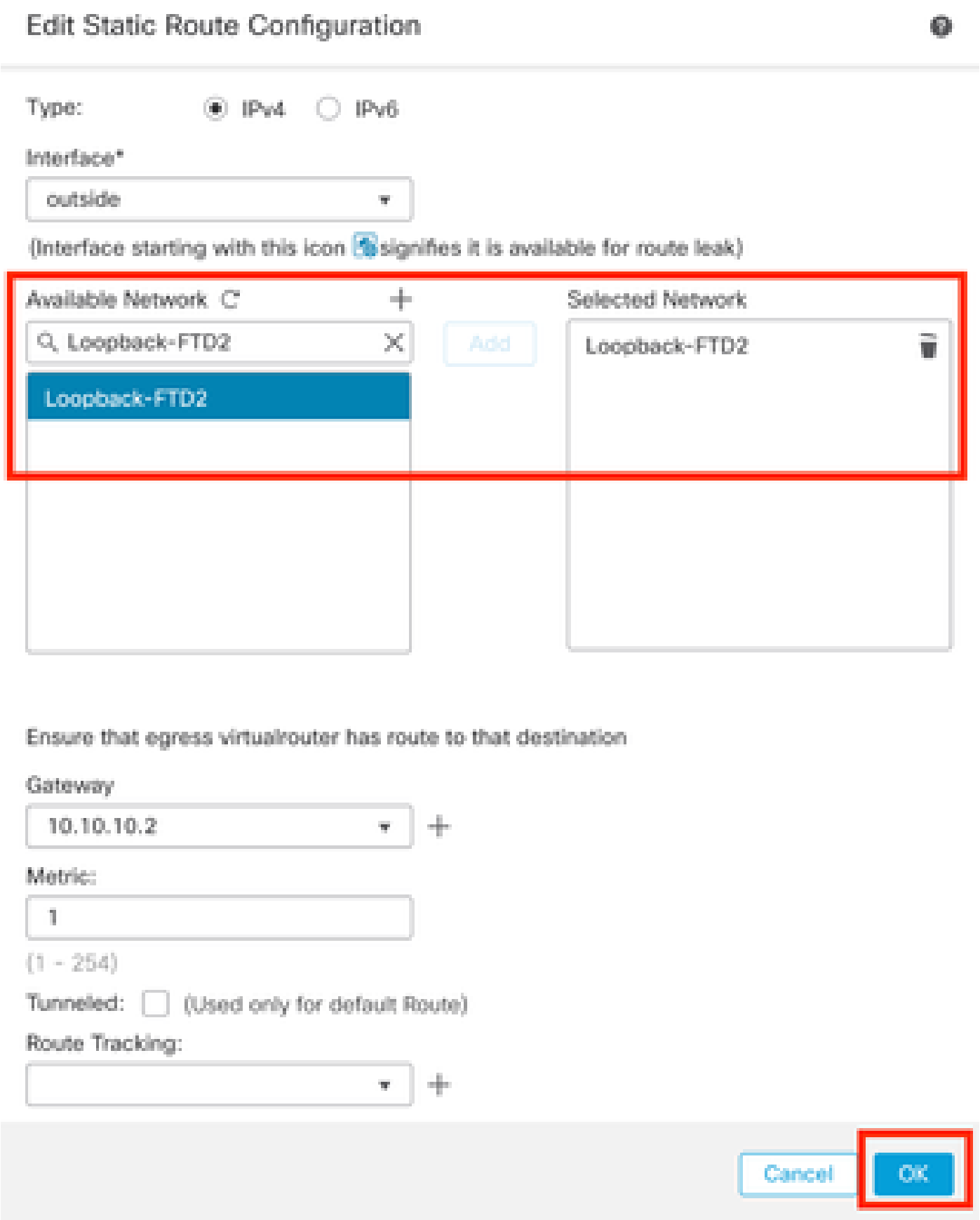

图 11.配置静态路由中的下一跳

步骤 7.Click Save.

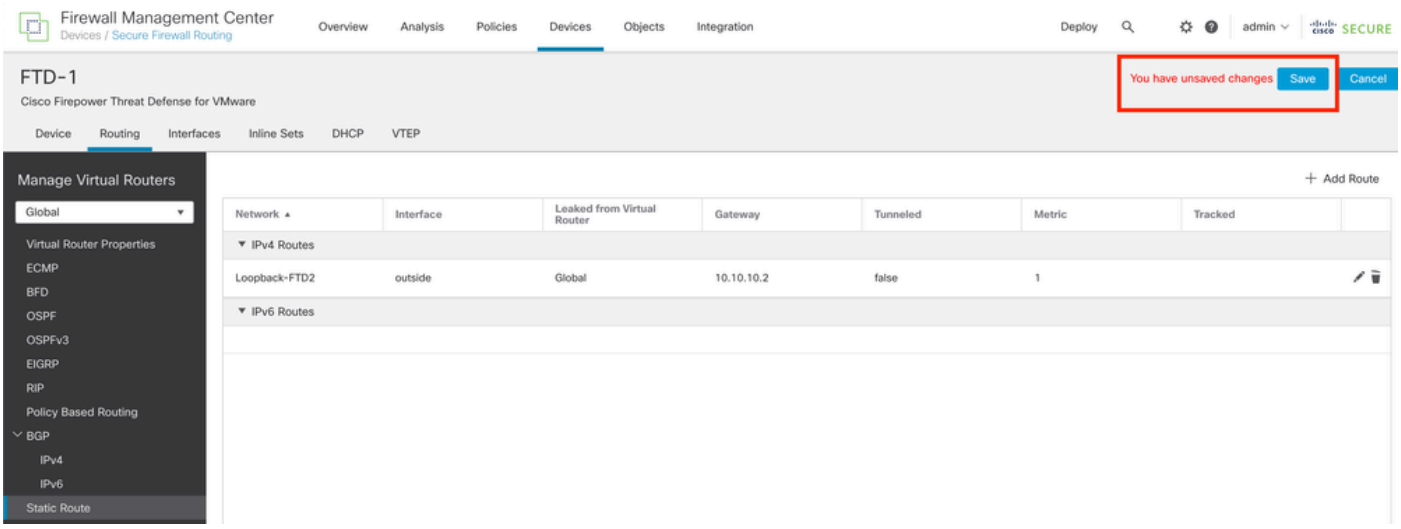

图 12.保存静态路由接口配置

步骤 8对第二个防火墙重复此过程。

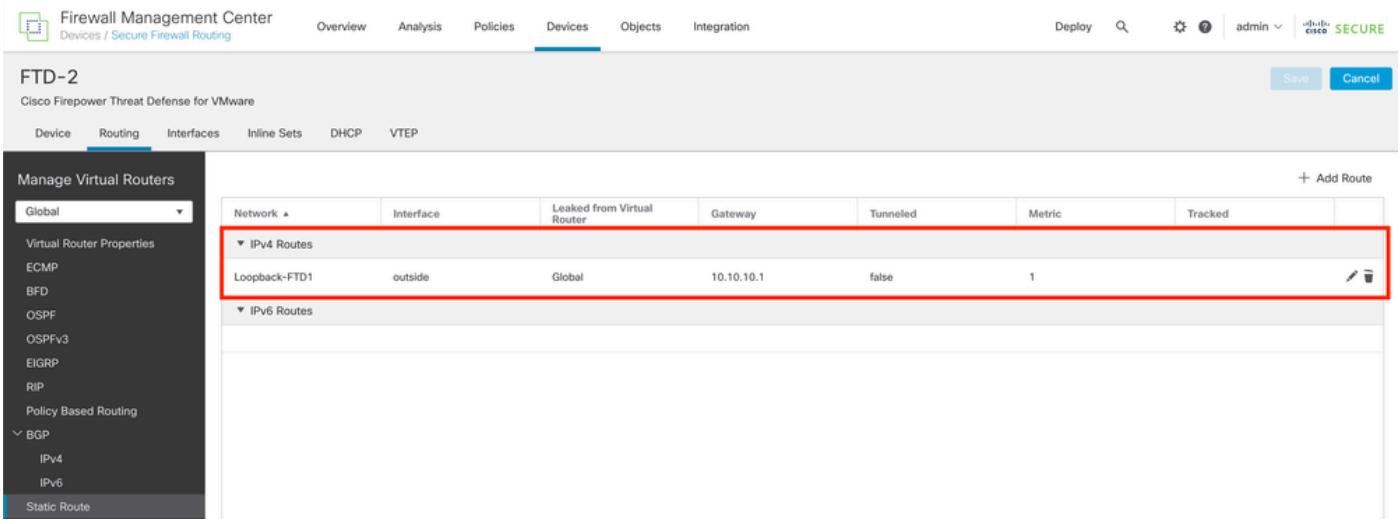

图 13.配置对等体上的静态路由

BGP配置

步骤1:单击Devices > Device Management，然后选择要启用BGP的设备。

步骤 2 单击Routing > Manage Virtual Routers > General Settings，然后单击BGP。

第 3 步：选中Enable BGP框，然后在AS Number部分中配置防火墙的本地AS。

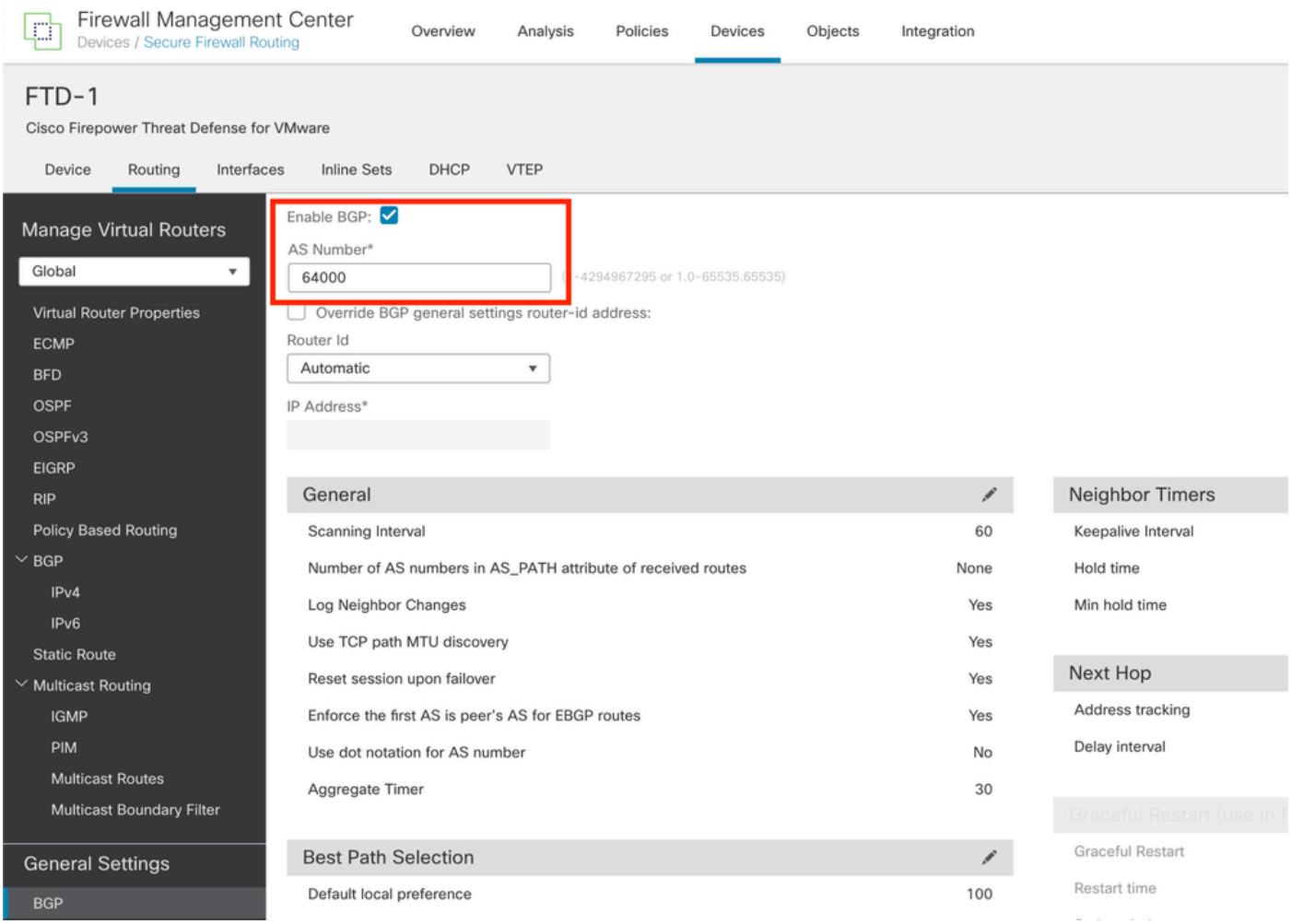

图 14.全局启用BGP

第 4 步：单击Save按钮保存更改。

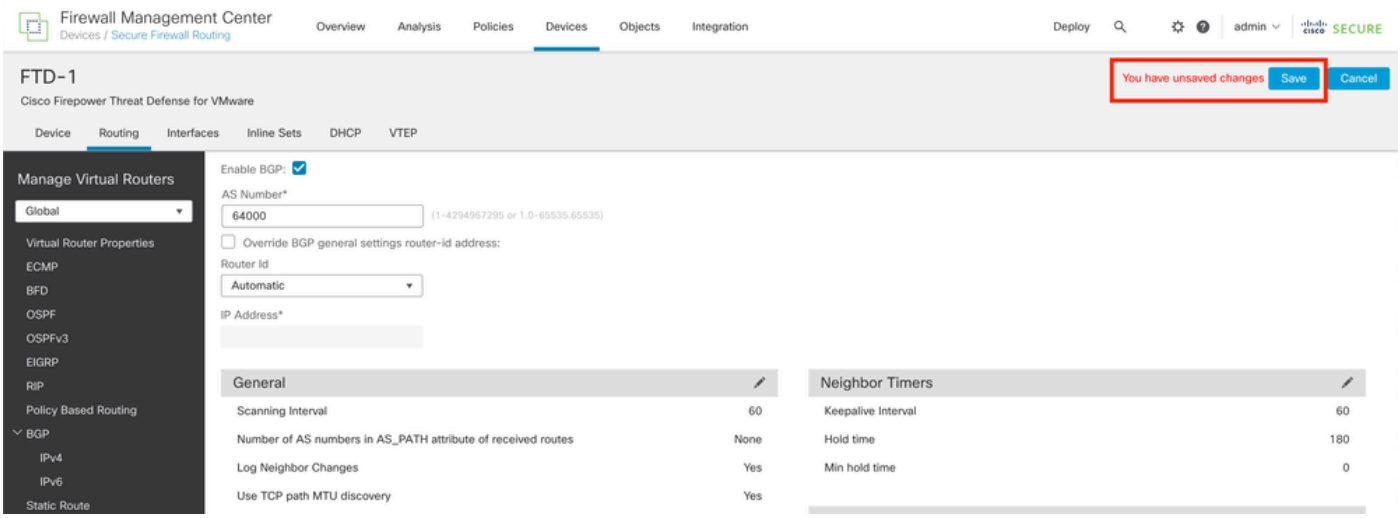

图 15.保存BGP启用更改

第五步：在管理虚拟路由器部分中，转到BGP 选项，然后单击IPv4。

第六步：选中Enable IPv4框，然后单击Neighbor，再单击+ Add。

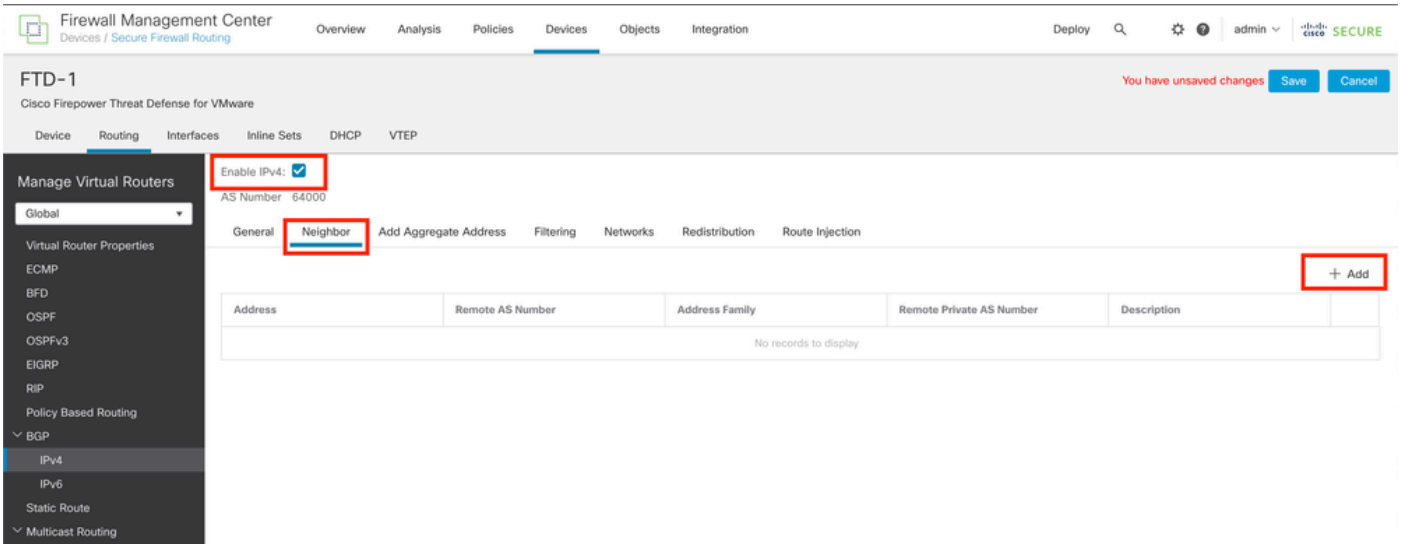

图 16.添加新的BGP对等体

步骤 7.在IP Address部分中配置远程对等体的IP地址，然后在Remote AS部分中配置远程对等体的AS，并选中Enable address框。

步骤 8在更新源部分中选择本地接口环回。

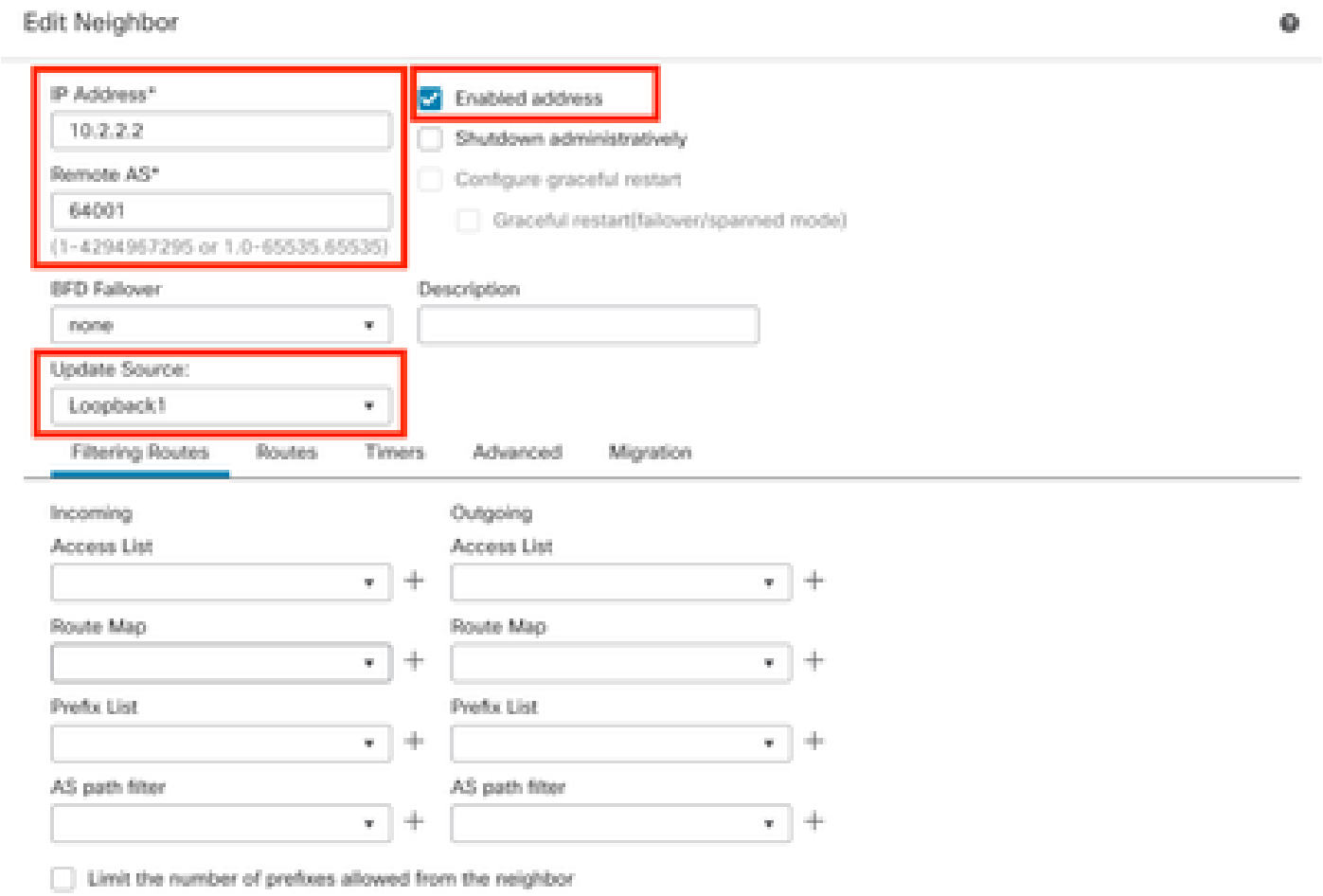

图 17.基本BGP对等体参数

注意：Update Source 选项启用neighbor update-source 命令，用于允许任何工作接口（包括

环回）。可以指定此命令来建立TCP连接。

步骤 9单击Advanced，然后在TTL Hops 选项中配置数字2，然后单击OK。

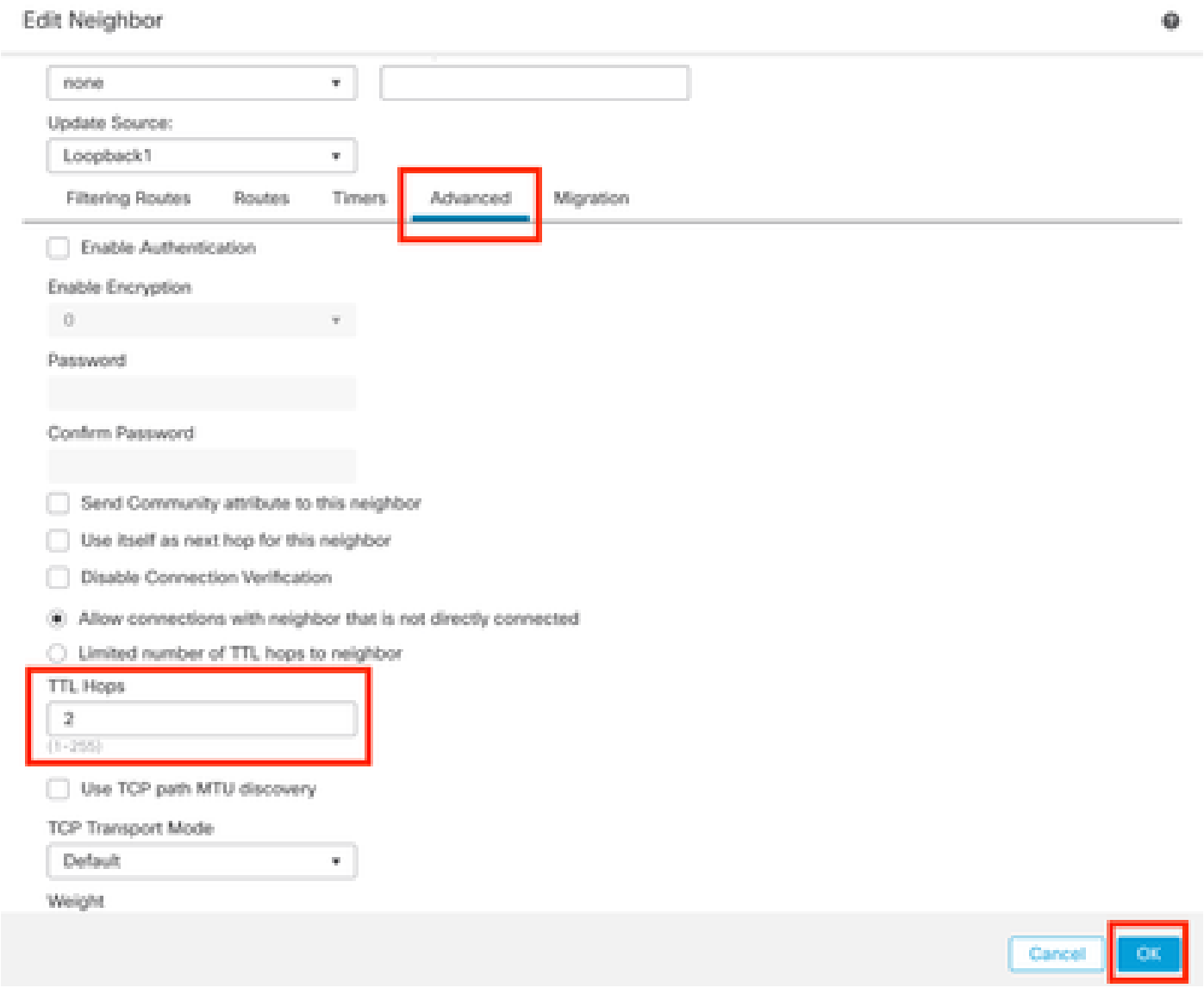

图 18.配置TTL跳数

注意：TTL Hops 选项用于启用ebgp-multihop 命令，该命令用于更改TTL值，以允许数据包到达非直连的外部BGP对等体或者具有直连接口以外的接口。

步骤 10点击保存并部署更改。

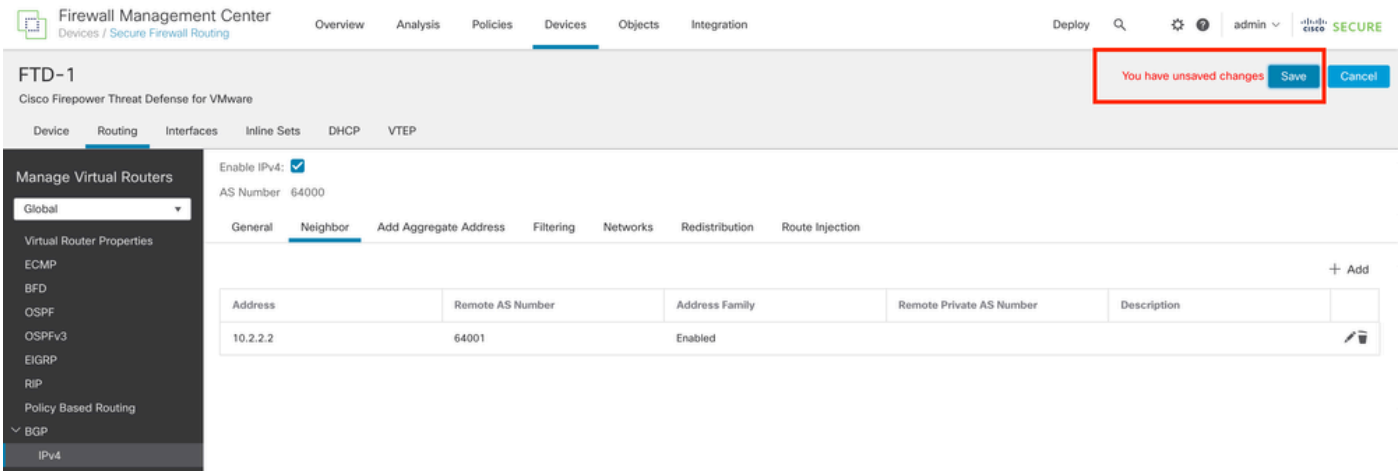

图 19.保存BGP配置

步骤 11对第二个防火墙重复此过程。

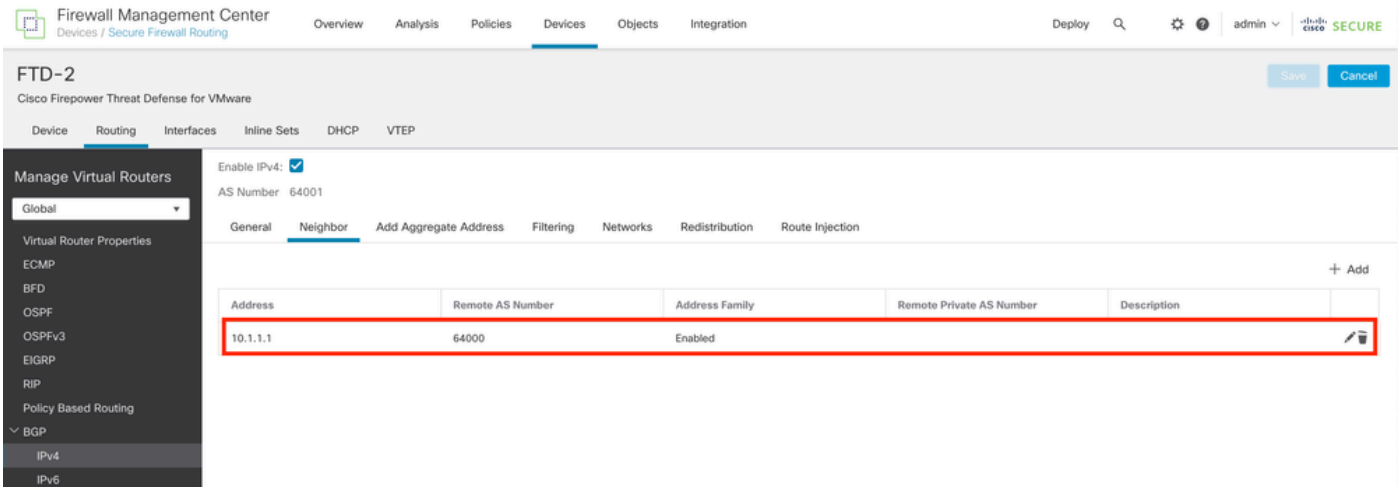

图 20.配置对等体上的BGP

验证

步骤1:验证环回和静态路由配置，然后使用ping测试检查BGP对等体之间的连接。

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 nameif Looback2

ip address 10.1.1.1 255.255.255.255 show running-config route outside 10.2.2.2 255.255.255.255 10.10.10.2 1 ping 10.2.2.2 Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms	ip address 10.2.2.2 255.255.255.255 show running-config route outside 10.1.1.1 255.255.255.255 10.10.10.1 1 ping 10.1.1.1 Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

第二步：验证BGP配置，然后确保BGP对等已建立。

show running-config router bgp

show bgp neighbors

show bgp summary

SFTD-1	SFTD-2

show running-config router bgp
 	
router 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
 	
  邻居10.2.2.2激活
 	
  no auto-summary
	show running-config router bgp
	
	router 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
	
	  邻居10.1.1.1激活
	
	  no auto-summary

无同步 exit-address-family ! show bgp neighbors	i BGP BGP邻居为10.2.2.2，vrf single_vf，远程AS 64001，外部链路 BGP版本4，远程路由器ID 10.2.2.2 BGP状态= Established，持续了1d15h BGP表版本7，邻居版本7/0 外部BGP邻居的距离可能高达2跳。 show bgp summary BGP路由器标识符10.1.1.1，本地AS编号64000 BGP表版本为7，主路由表版本为7 Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.2.2.2 4 64001 2167 2162 7 0 1d15h 0	无同步 exit-address-family ! show bgp neighbors	i BGP BGP邻居为10.1.1.1，vrf single_vf，远程AS 64000，外部链路 BGP版本4，远程路由器ID 10.1.1.1 BGP状态= Established，持续了1d16h BGP表版本1，邻居版本1/0 外部BGP邻居的距离可能高达2跳。 show bgp summary BGP路由器标识符10.2.2.2，本地AS编号64001 BGP表版本为1，主路由表版本为1 Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.1.1.1 4 64000 2168 2173 1 0 1d16h 0

故障排除

如果在此过程中遇到任何问题，请阅读本文：

· 边界网关协议(BGP)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。