在 FMC 上配置带有 HTTP 路径监控的 PBR

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- 为HTTP路径监控配置PBR
- 配置等价多路径(ECMP)
- 为安全FTD配置受信任DNS
- 启用路径监控
- 添加监控控制面板

验证

故障排除

相关信息

简介

本文档介绍如何使用HTTP路径监控在思科安全防火墙管理中心(FMC)上配置基于策略的路由(PBR)。

先决条件

要求

Cisco 建议您了解以下主题：

- PBR基础知识
- 基本的Cisco安全管理中心体验
- 基本思科安全防火墙威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行7.4版本的思科安全防火墙管理中心虚拟(FMCv)VMware
- 运行7.4版本的思科安全防火墙威胁防御虚拟设备(FTDv)VMware

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

在传统路由中，数据包根据目的IP地址进行路由，但在基于目标的路由系统中很难更改指定流量的路由。PBR通过扩展和补充路由协议提供的现有机制，使您能够更好地控制路由。

PBR允许设置IP优先级。它还允许为特定流量指定路径，例如高开销链路上的优先级流量。使用PBR时，路由基于目标网络以外的条件，例如源端口、目标地址、目标端口、协议应用程序或这些对象的组合。PBR可用于根据应用、用户名、组成员身份和安全组关联对网络流量进行分类。此路由方法适用于大型网络部署中大量设备访问应用和数据的情况。传统上，大型部署的拓扑会将所有网络流量回传到集线器，作为基于路由的VPN中的加密流量。这些拓扑经常会导致数据包延迟、带宽降低和丢包等问题。

PBR仅在路由防火墙模式上受支持，不应用于初期连接。物理、端口通道、子接口和状态隧道接口支持基于HTTP的应用。群集设备不支持该功能。

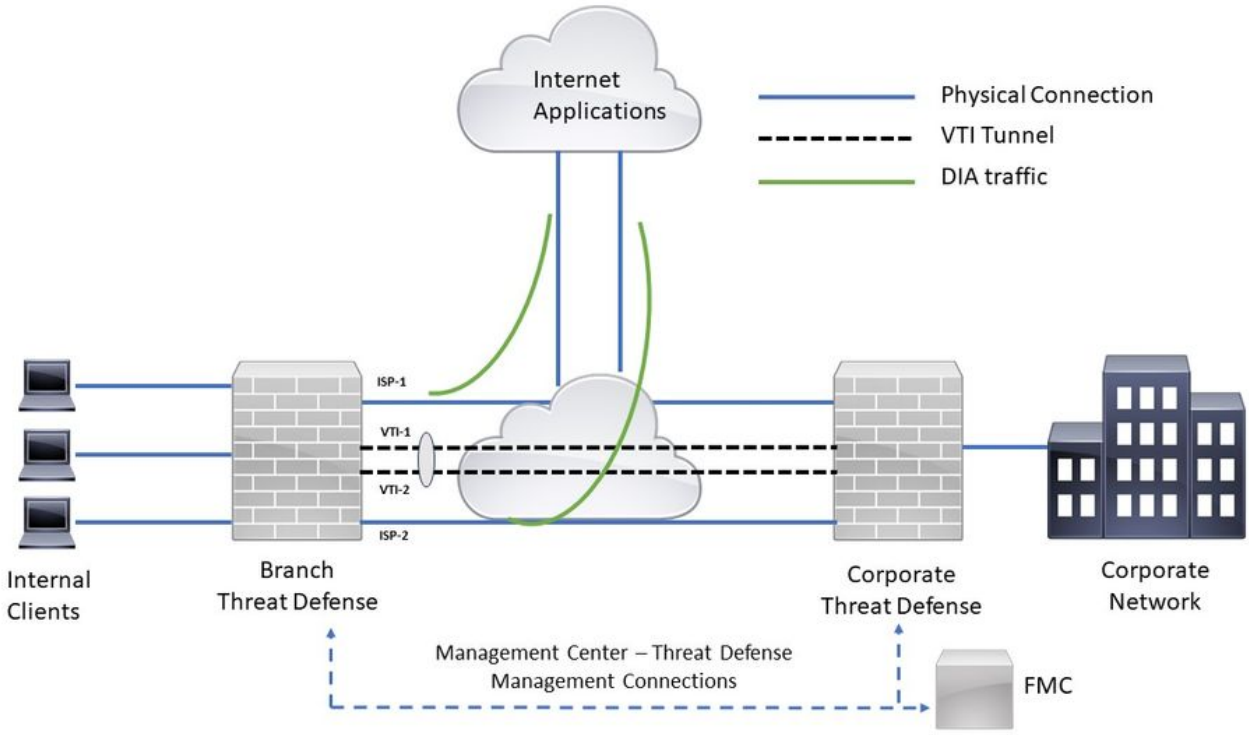
当配置的接口获得诸如往返时间(RTT)、抖动、平均意见评分(MOS)和每个接口丢包的度量时，它们用于确定路由PBR流量的最佳路径。路径监控为每个接口计算多个远程对等体的灵活度量。为了通过分支机构防火墙上的策略监控和确定多个应用的最佳路径，HTTP优先于ICMP，原因如下：

- HTTP-ping可以派生通往服务器应用层（应用所在层）的路径性能度量。
- 每当更改应用服务器IP地址时，更改防火墙配置的需要都会被删除，因为会跟踪应用域而不是IP地址。

配置

网络图

考虑典型的企业网络场景，其中所有分支机构网络流量均通过企业网络的基于路由的VPN发送，并在需要时分流到外网。下一个拓扑显示了通过基于路由的VPN连接到公司网络的分支机构网络。传统上，企业威胁防御配置为处理分支机构的内部和外部流量。使用PBR策略，分支机构威胁防御配置有将特定流量路由到WAN网络而不是虚拟隧道的策略。其余流量照常通过基于路由的VPN。



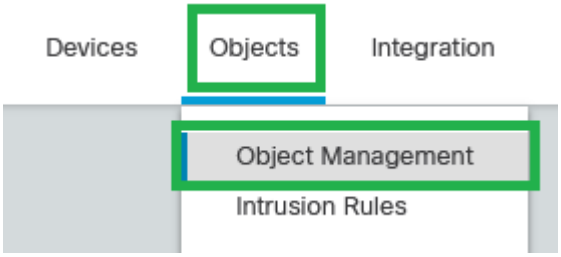
网络拓扑

“配置”部分假设ISP和VTI接口已配置用于安全FMC中的分支机构威胁防御。

为HTTP路径监控配置PBR

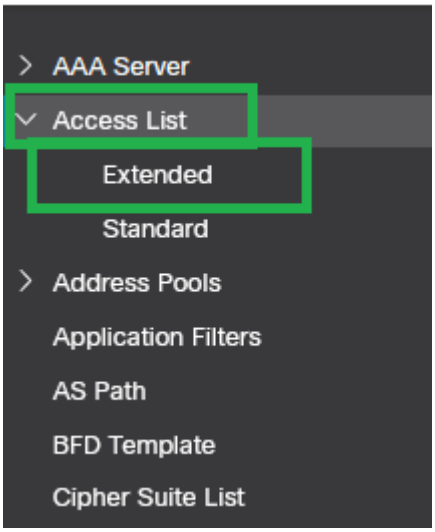
此配置部分显示了ISP-1和ISP-2接口上的路径监控配置。

步骤1.创建受监控应用的扩展访问列表。导航至。Objects > Object Management



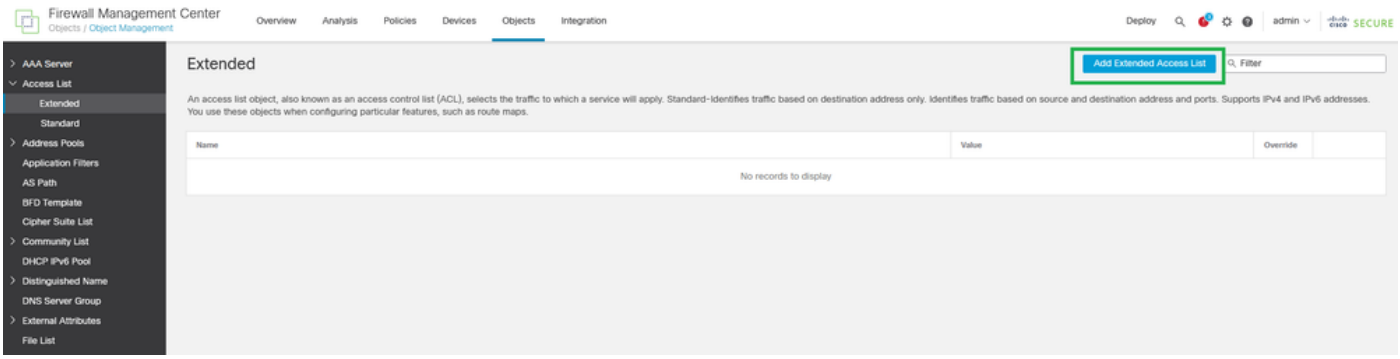
对象 — 对象管理

步骤2.导航Access-list > Extended到左侧菜单上。



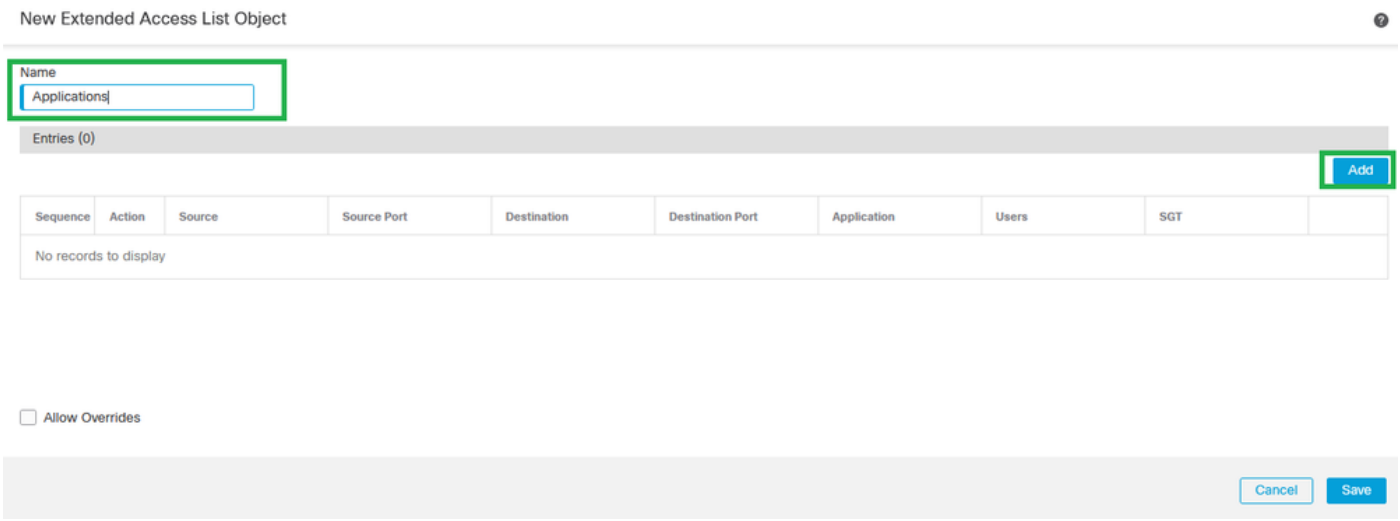
访问列表 — 扩展

步骤3.单击Add Extended Access List。



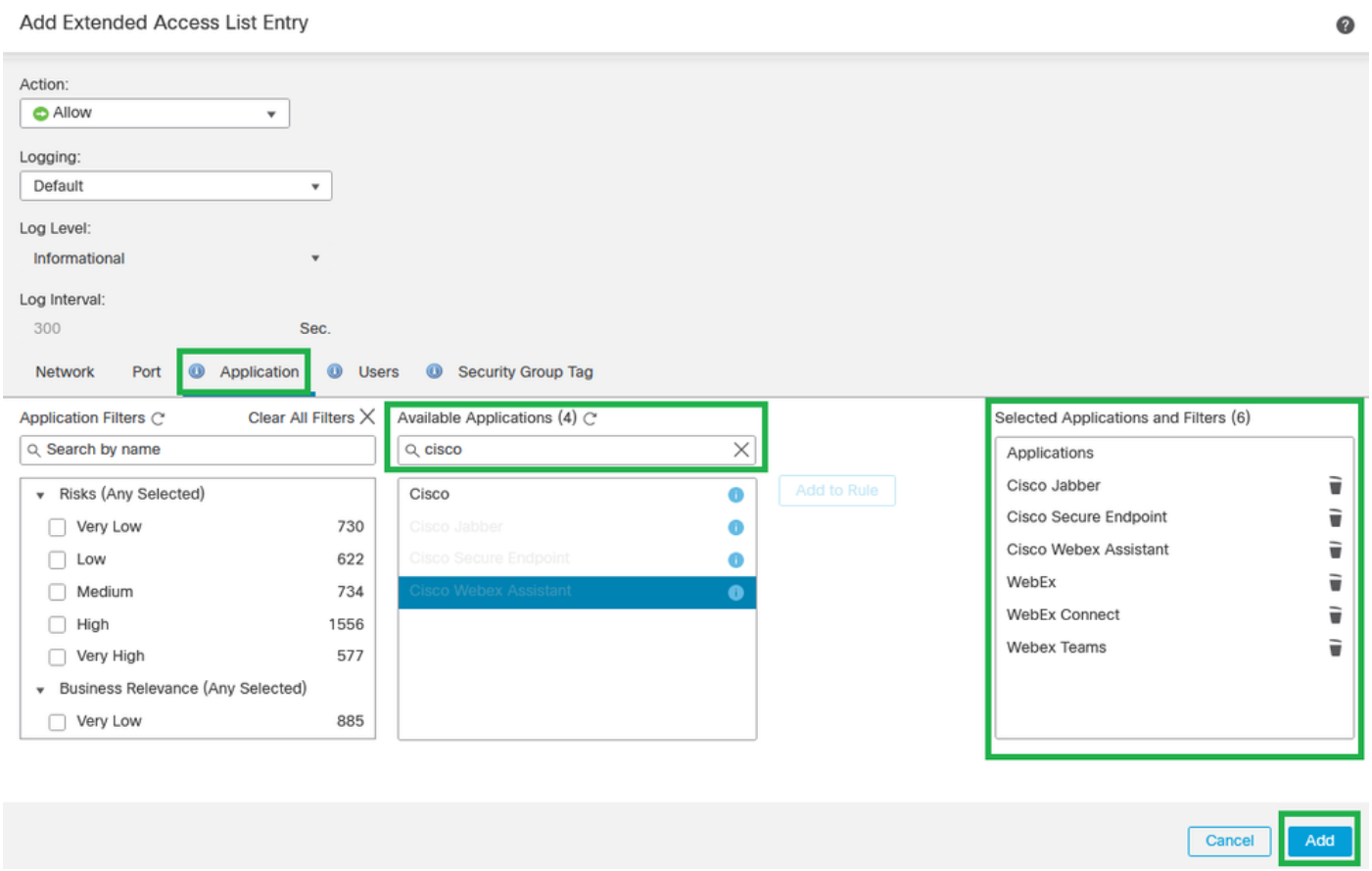
添加扩展访问列表

步骤4.在Extended Access List中设置名称并单击Add。



新建扩展访问列表对象

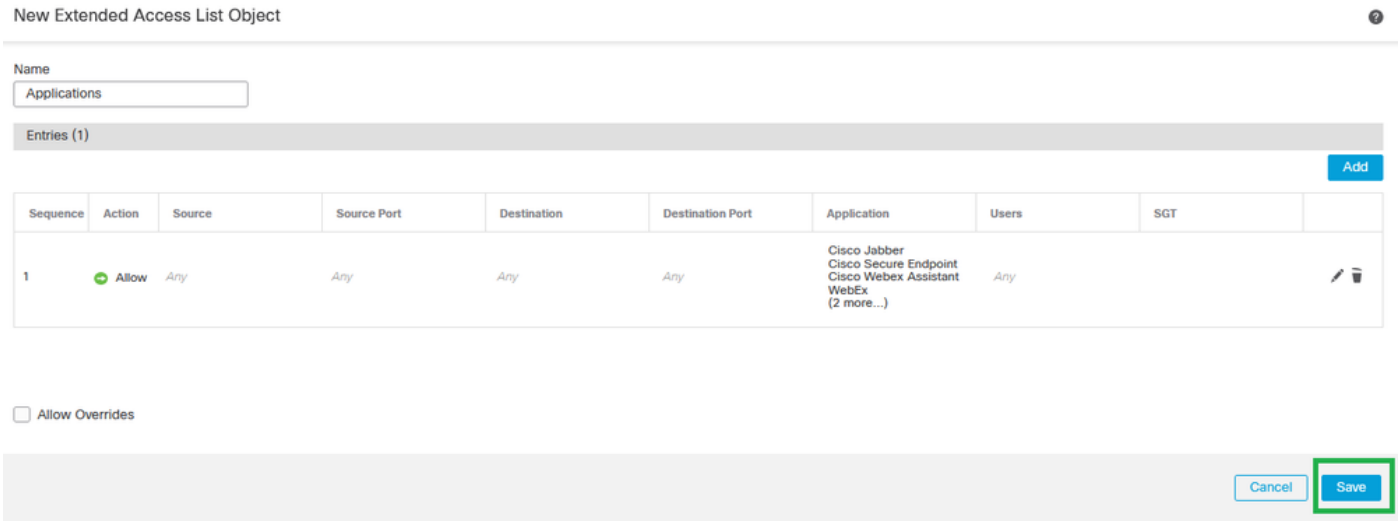
步骤5.点Application击并选择所需的应用（本示例已选择某些思科应用）。 ？？然后单击.Add



添加扩展访问列表条目

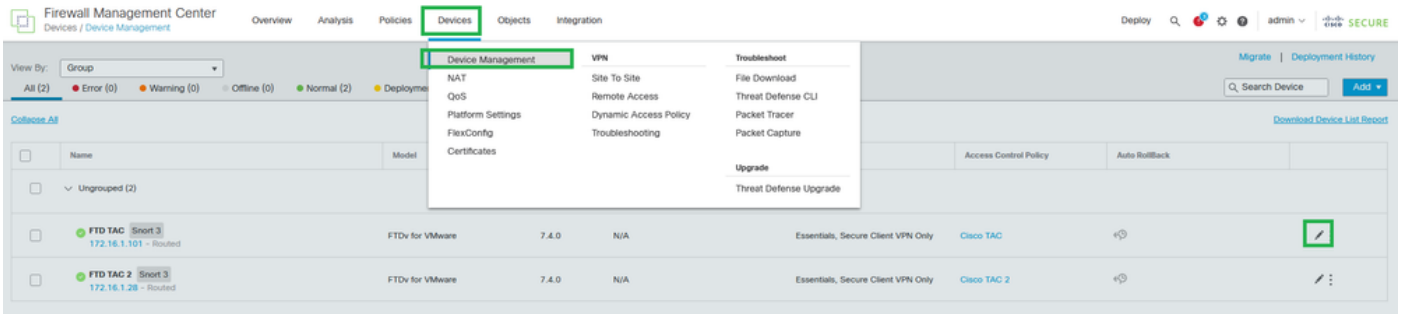
注意：可使用源/目标IP和端口配置扩展访问列表，以便将特定流量匹配到所需应用。您可以创建多个扩展访问控制列表以应用于PBR配置。

步骤6.验证扩展访问列表配置并点击Save。



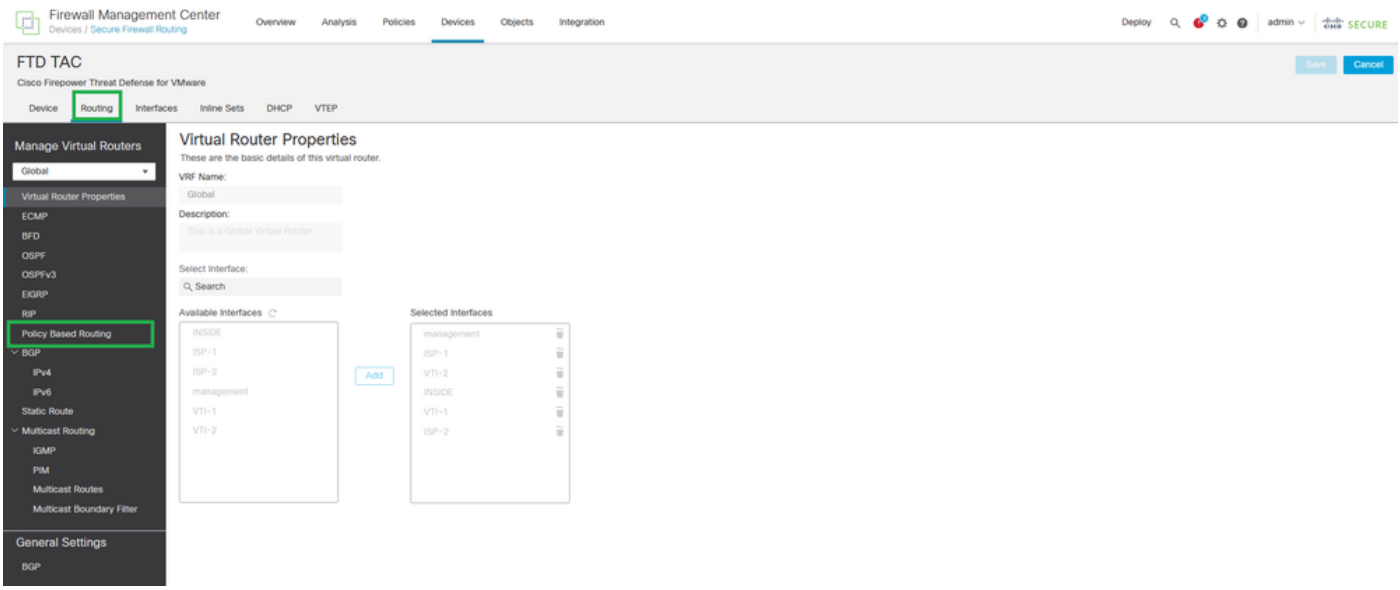
保存扩展访问列表对象

第 7 步： 导航到Devices > Device Management威胁防御并对其进行编辑。



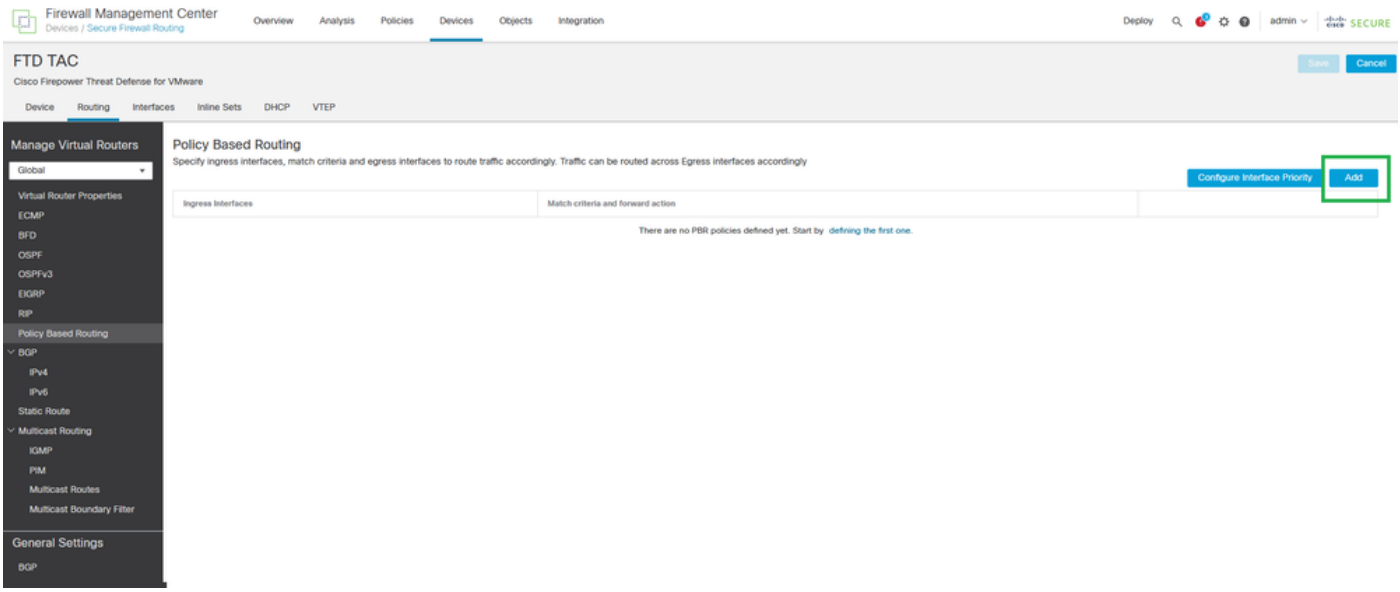
设备 — 设备管理

第 8 步： 导航至 。 Routing > Policy-Based Routing



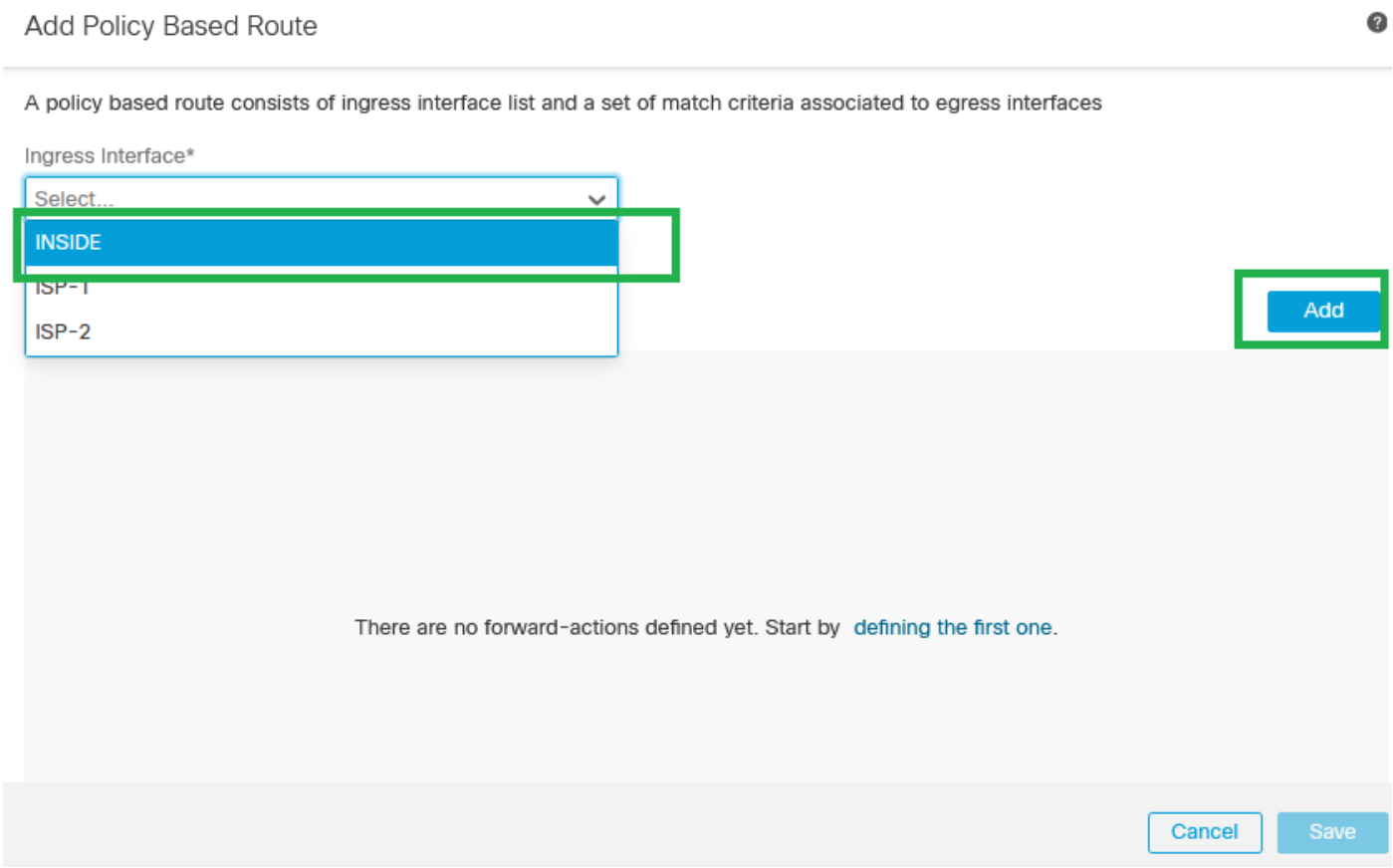
路由 — 基于策略的路由

步骤9.单击Add。



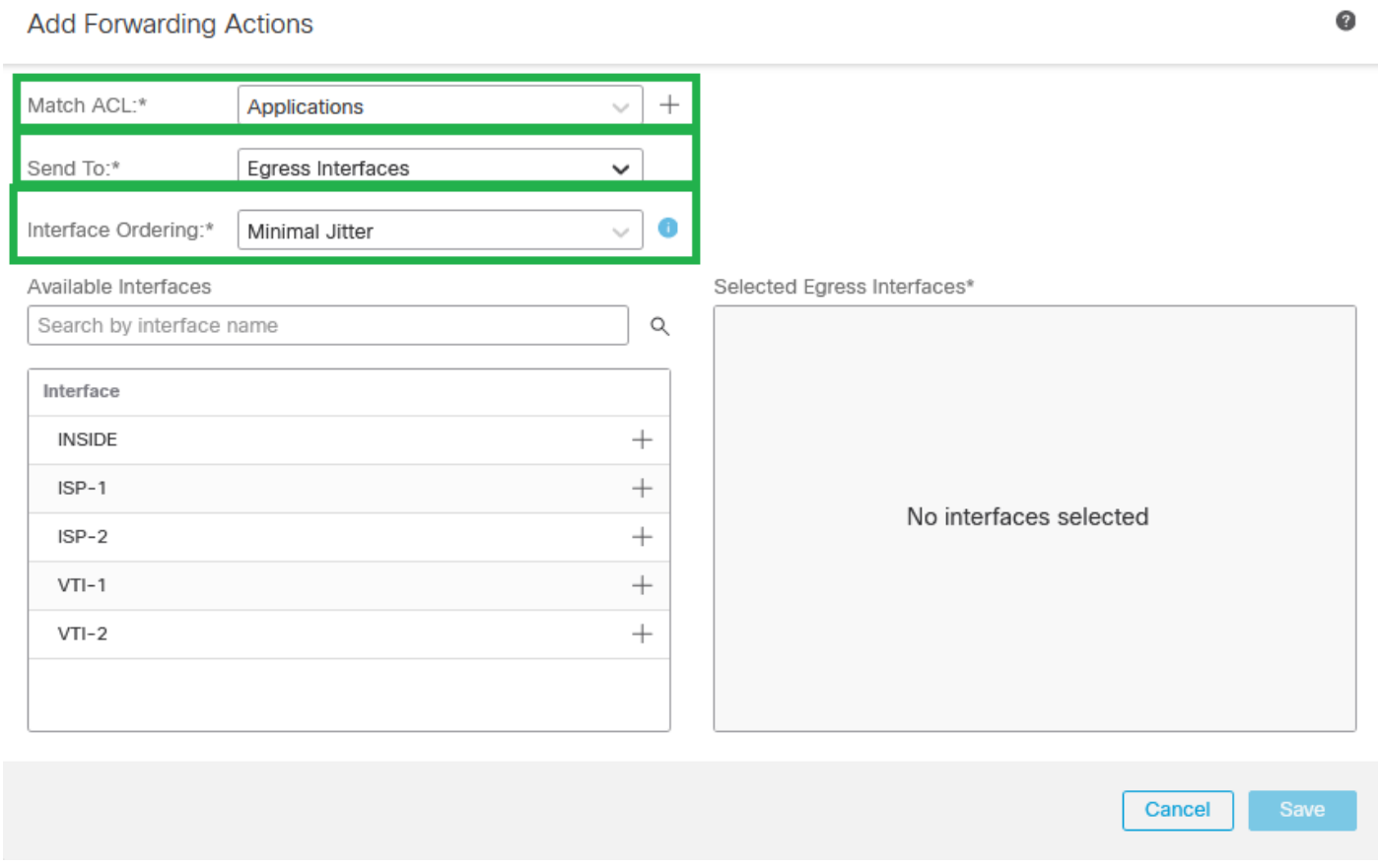
添加基于策略的路由

步骤10.为PBR配置添加入口接口（本示例中为INSIDE），然后单击Add。



添加基于策略的路由

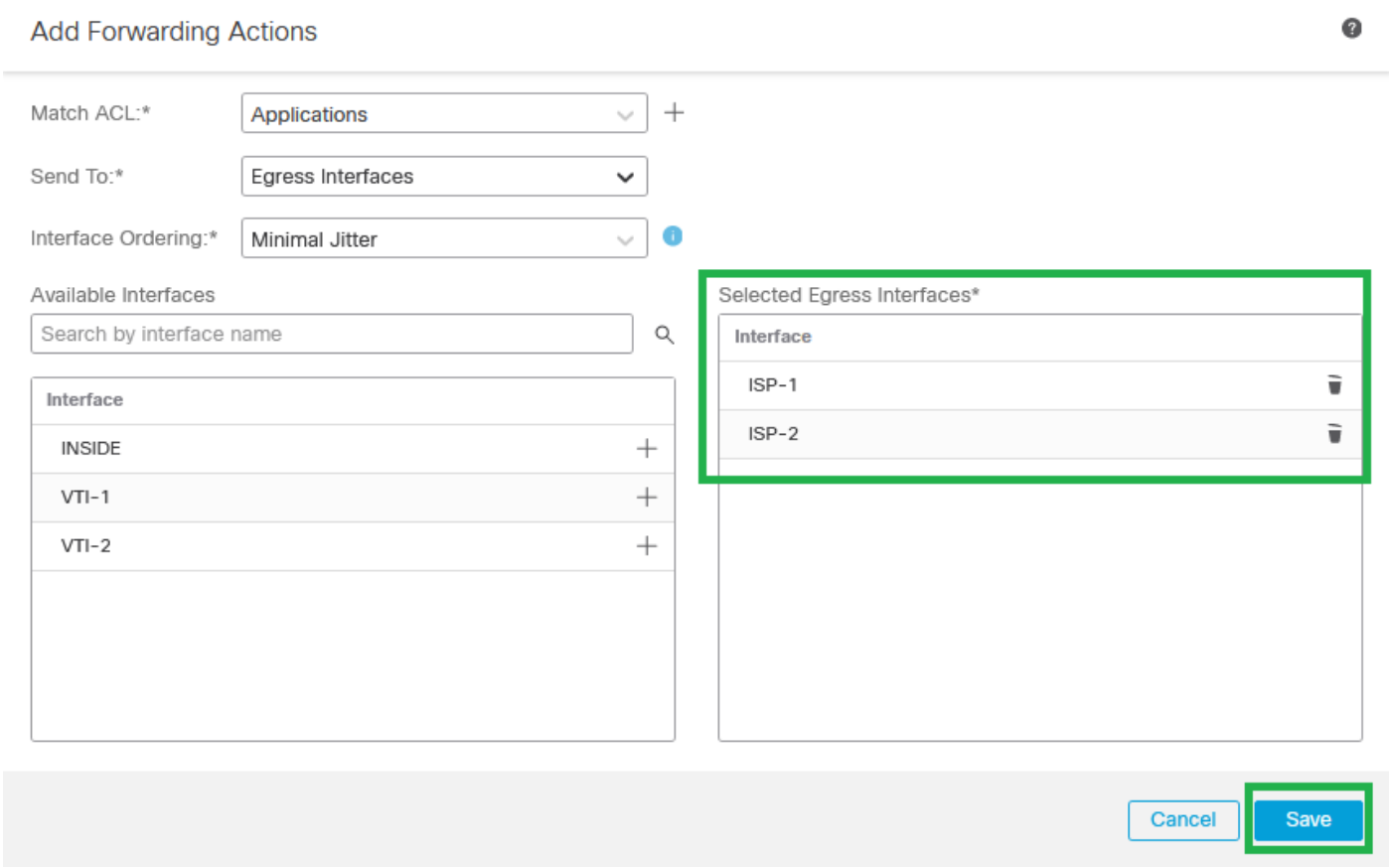
步骤11.定义匹配条件（使用之前步骤中创建的扩展访问列表）、出口接口和接口排序。



添加转发操作

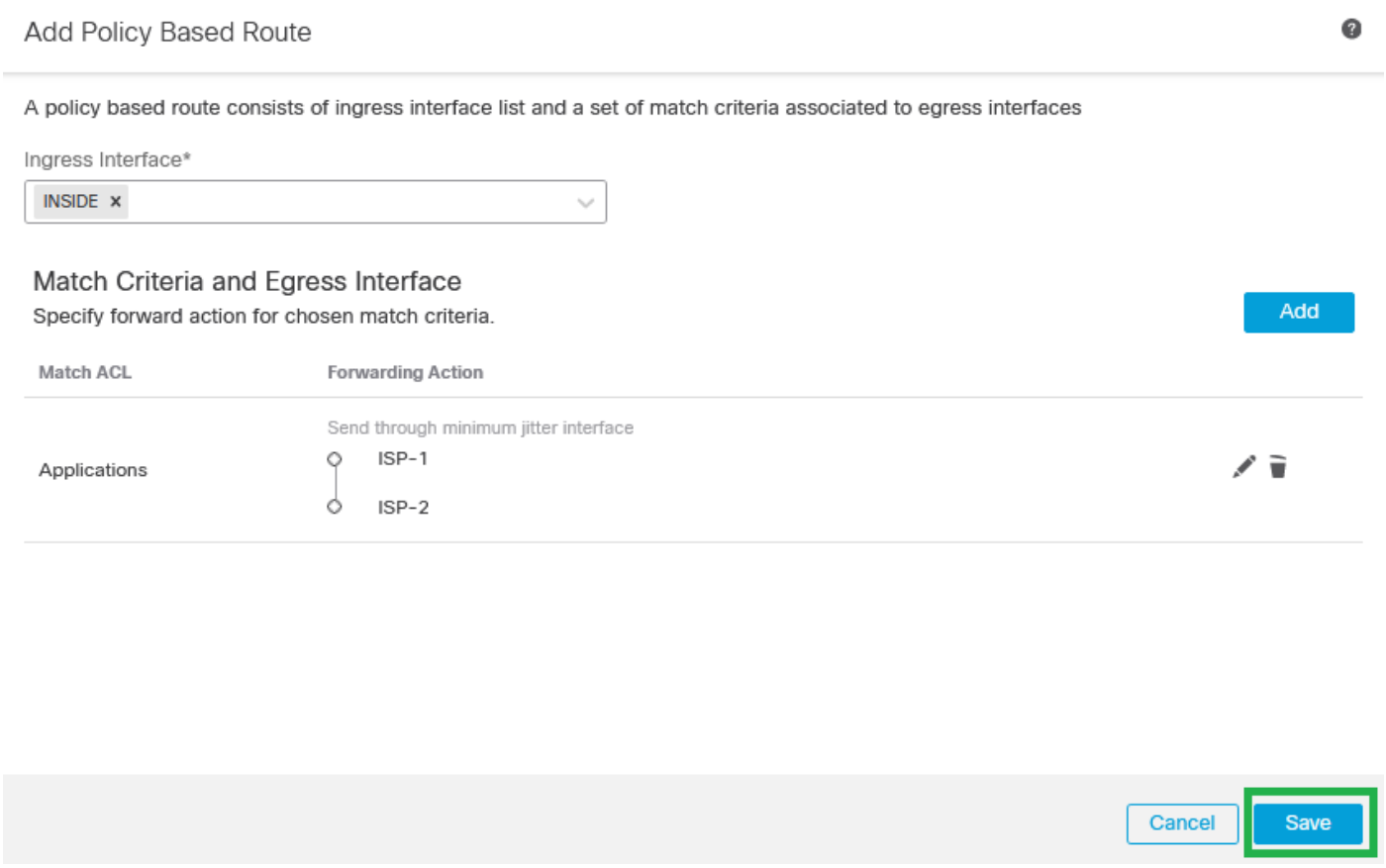
注意:Egress Interfaces为Minimal Jitter此配置指南选择了和。请查看官方PBR文档以了解有关其他选项的详细信息。

步骤12.选择出口接口（本例中为ISP-1和ISP-2），然后单击Save。



选定的出口接口

步骤13.验证PBR配置并点击Save。



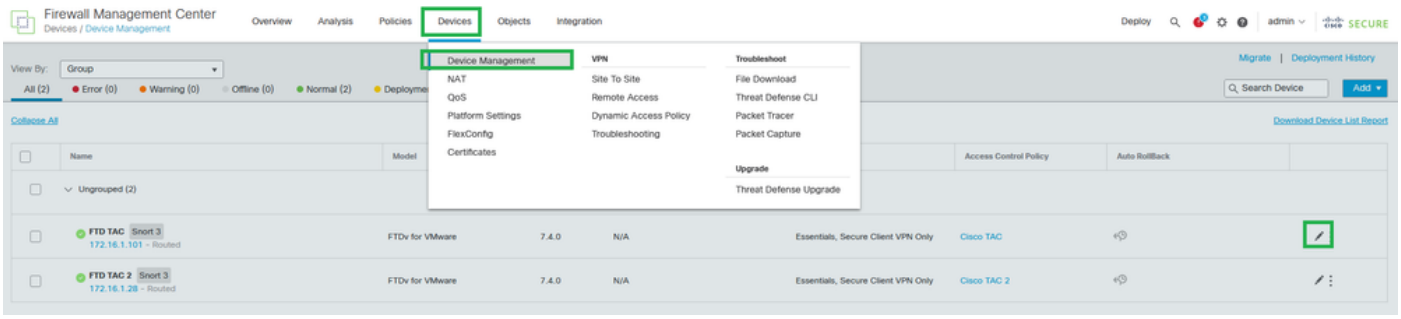
基于策略的路由验证

步骤14.（可选）如果创建了更多的扩展访问控制列表，或者如果有更多的源接口必须应用PBR配置，请重复步骤9、10、11、12和13。

步骤15.保存并部署FMC中的更改。

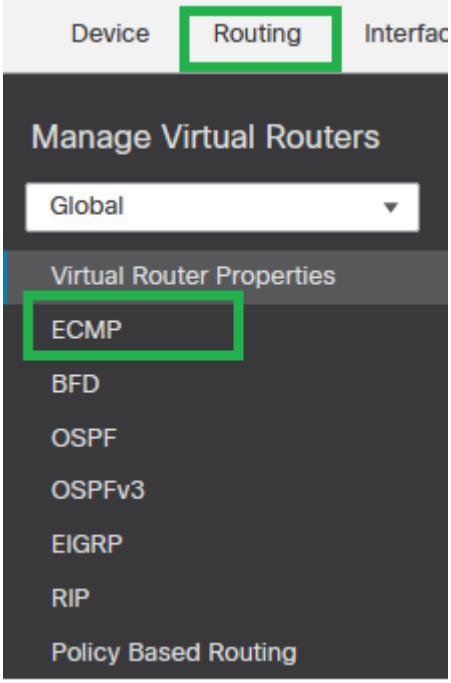
配置等价多路径(ECMP)

步骤1.导航到Devices > Device Management，然后编辑威胁防御。



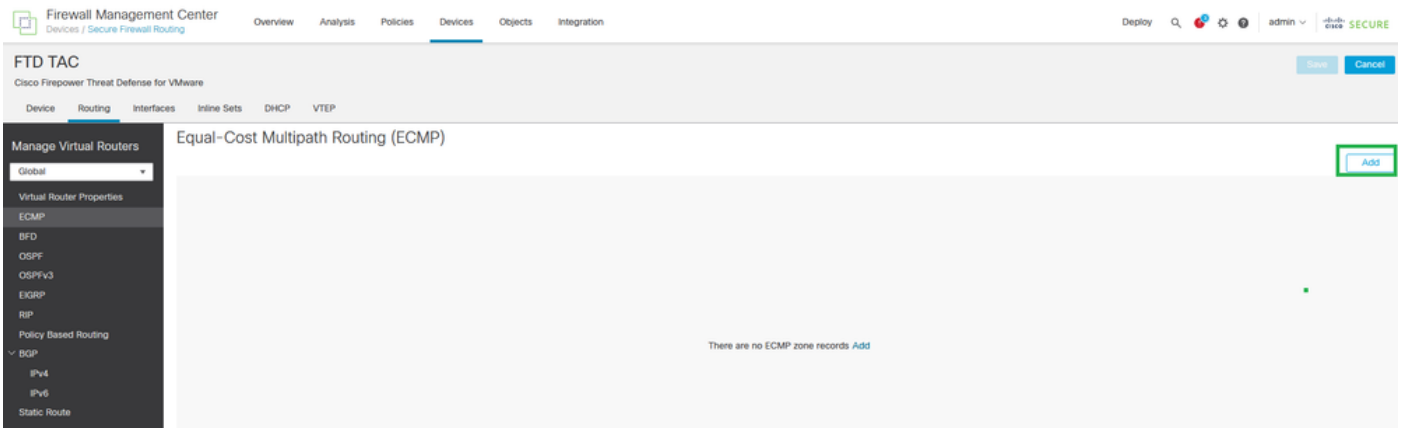
设备 — 设备管理

第 2 步： 导航至 。Routing > ECMP



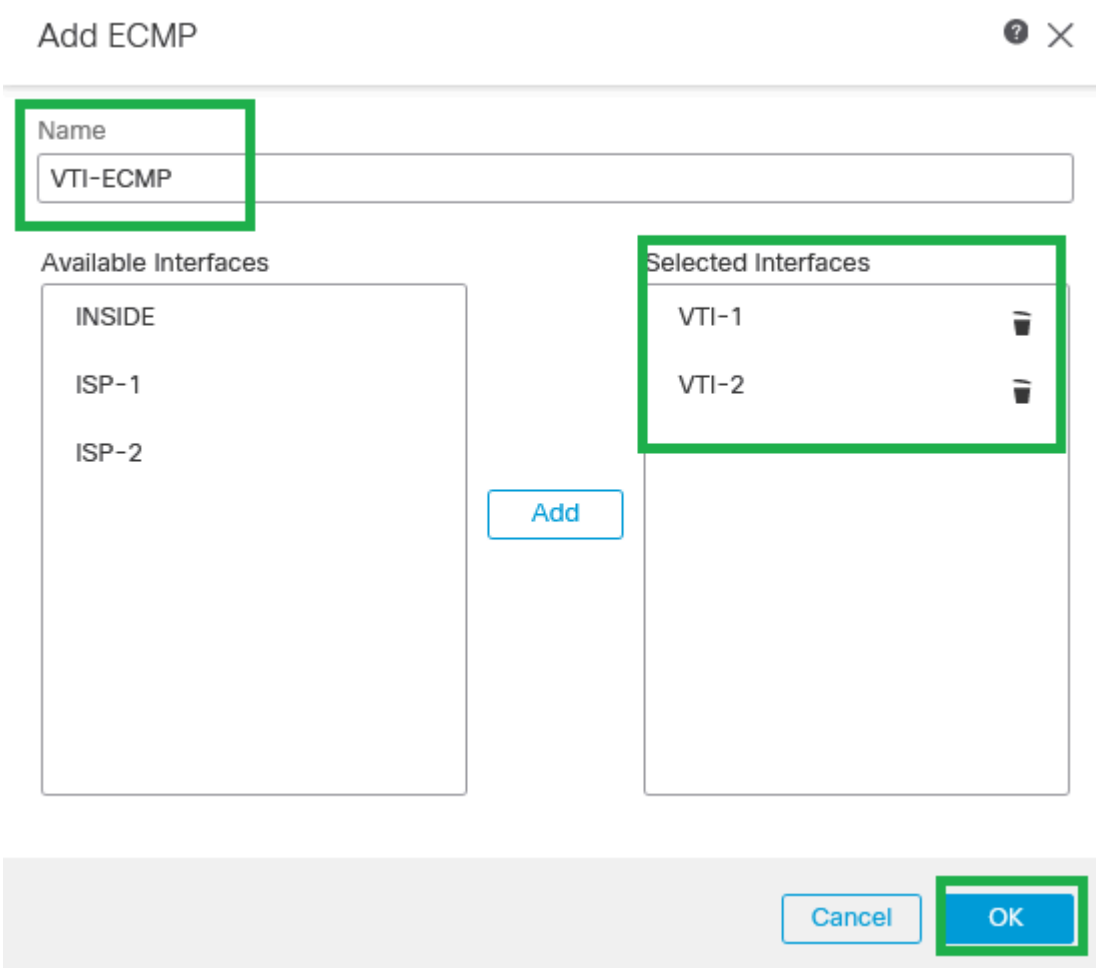
路由 — ECMP

步骤3.单击Add，以便在VTI和WAN接口（本配置指南中为ISP-1和ISP-2）之间创建ECMP。



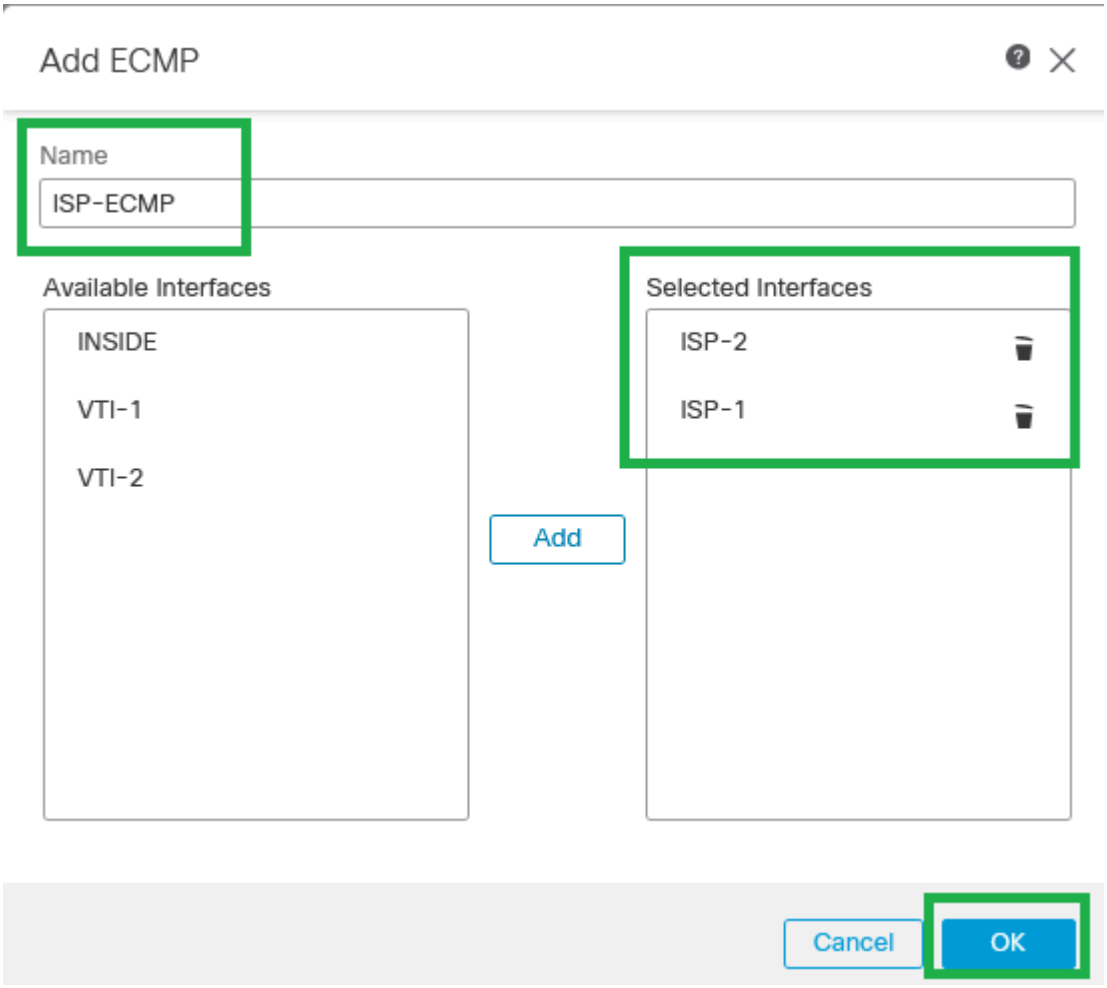
等价多路径路由(ECMP)

步骤4.设置ECMP名称并选择所有VTI接口，然后单击Add。



用于VTI的ECMP

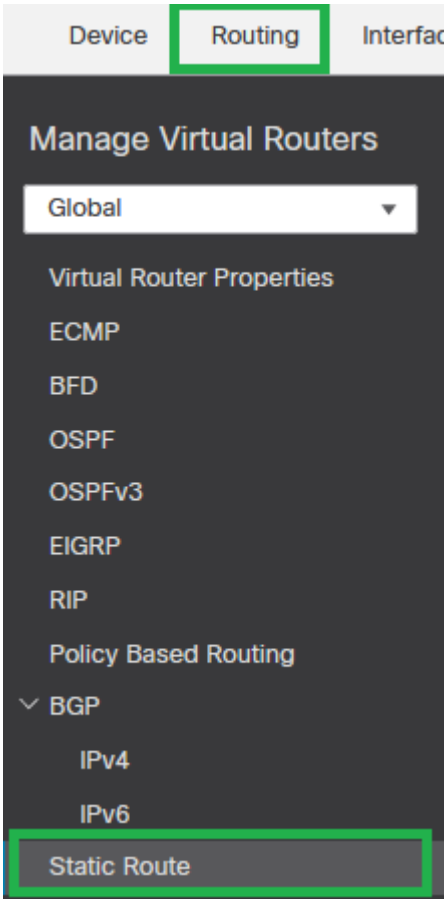
步骤5.重复步骤3和4，以便在WAN接口（本配置指南中为ISP-1和ISP-2）之间创建ECMP。



用于ISP接口的ECMP

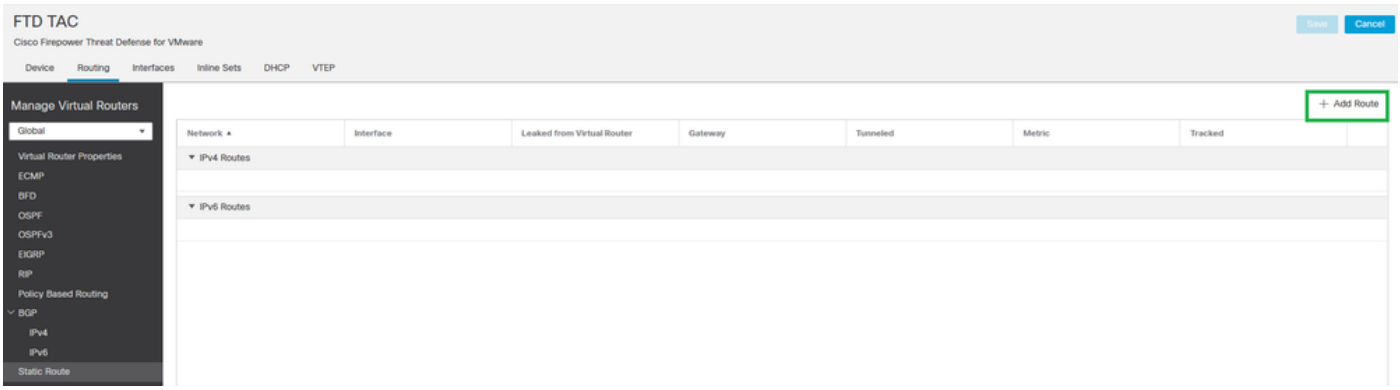
步骤6.保存ECMP配置。

步骤7.为区域接口配置静态路由以实现负载均衡。依次导航至 Routing > Static Route.



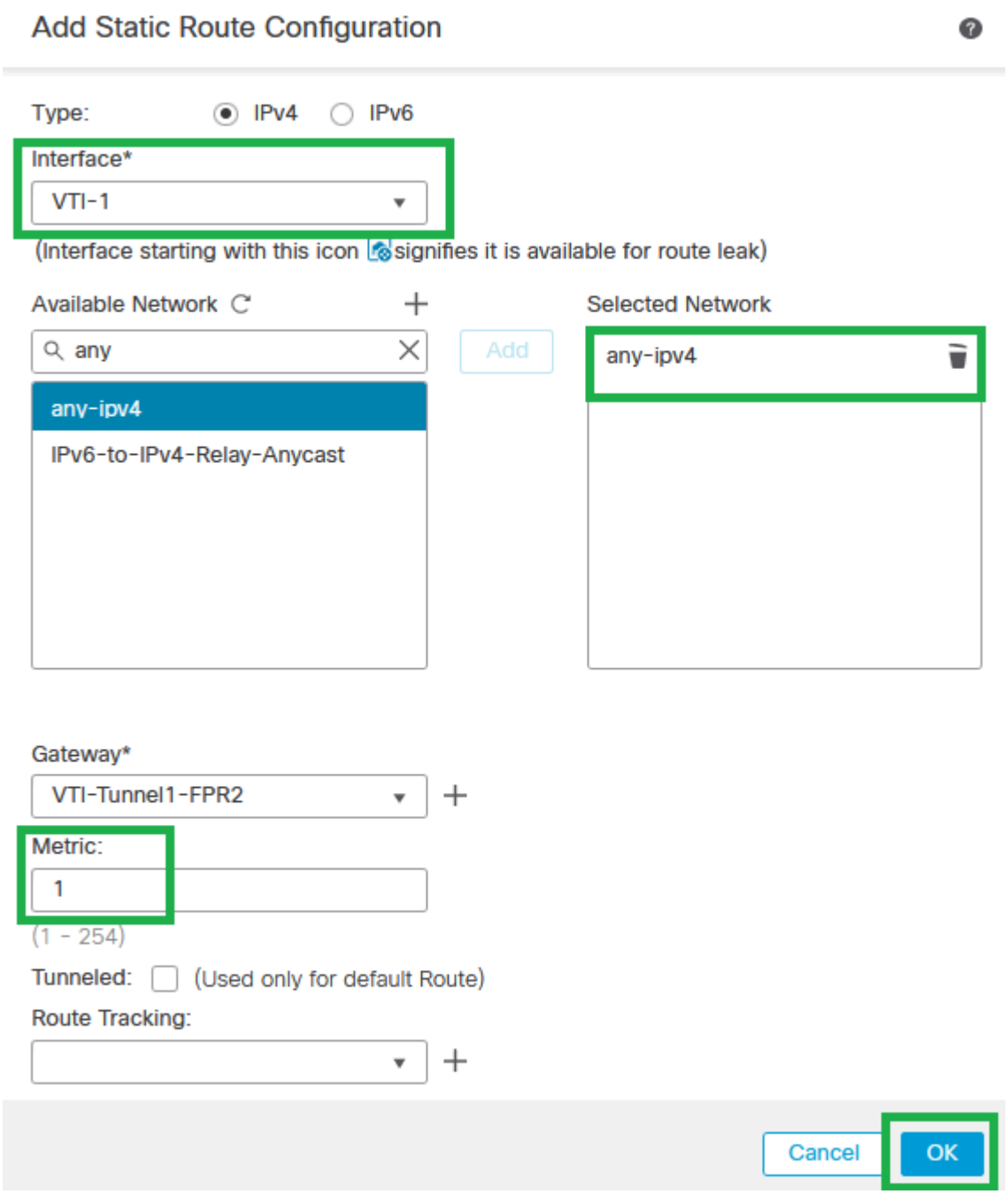
路由 — 静态路由

步骤8.单击+ Add Route。



+添加路由

步骤9.为VTI接口创建默认静态路由（本配置指南为VTI-1），将1作为度量值，然后单击OK。

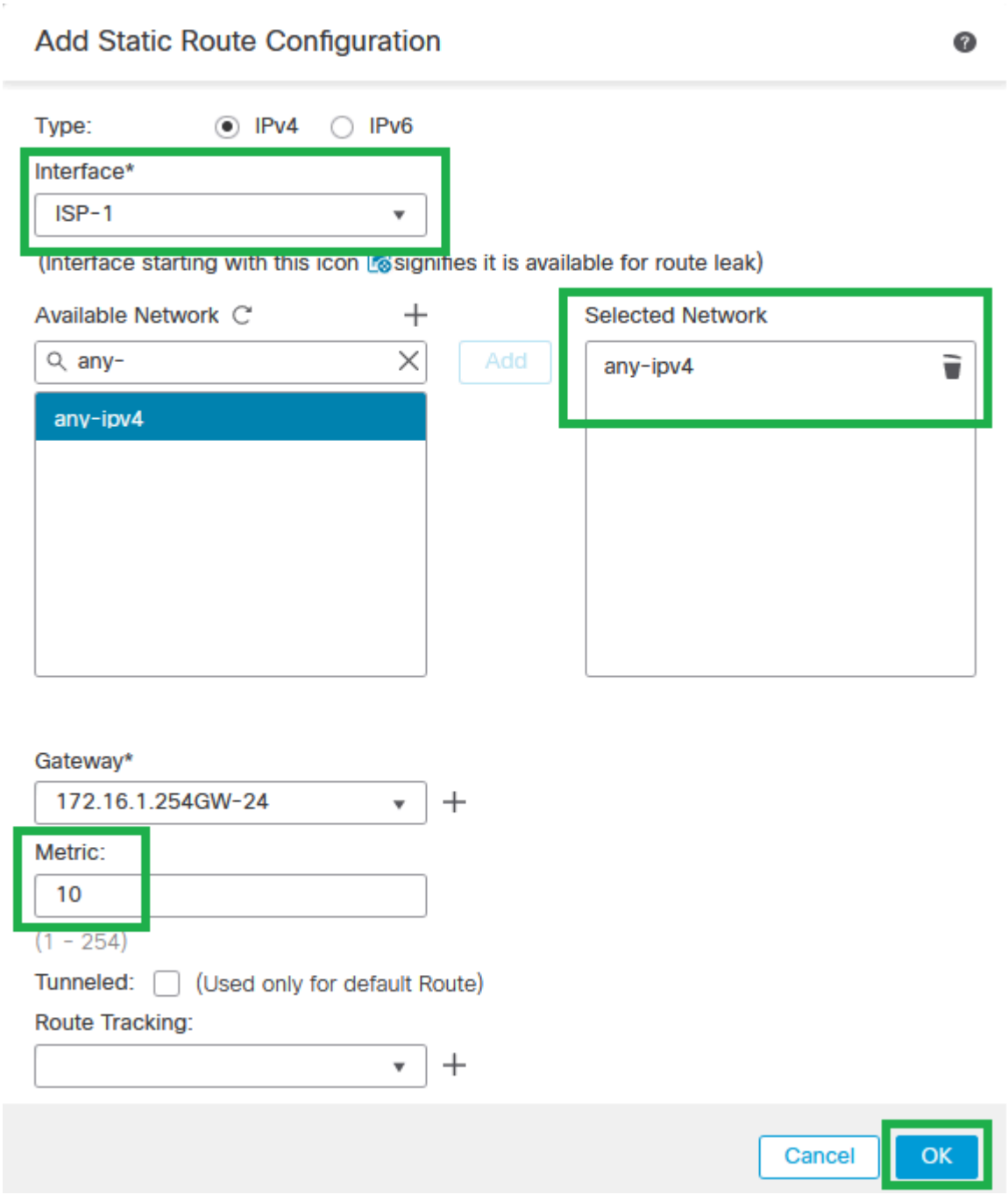


VTI-1的默认静态路由

步骤10.重复步骤8。如果配置了多个VTI接口。

注意：为配置的每个VTI接口创建默认路由。

步骤11.为WAN/ISP接口（本配置指南中的ISP-1）创建度量值大于VTI的默认静态路由，然后单击OK。

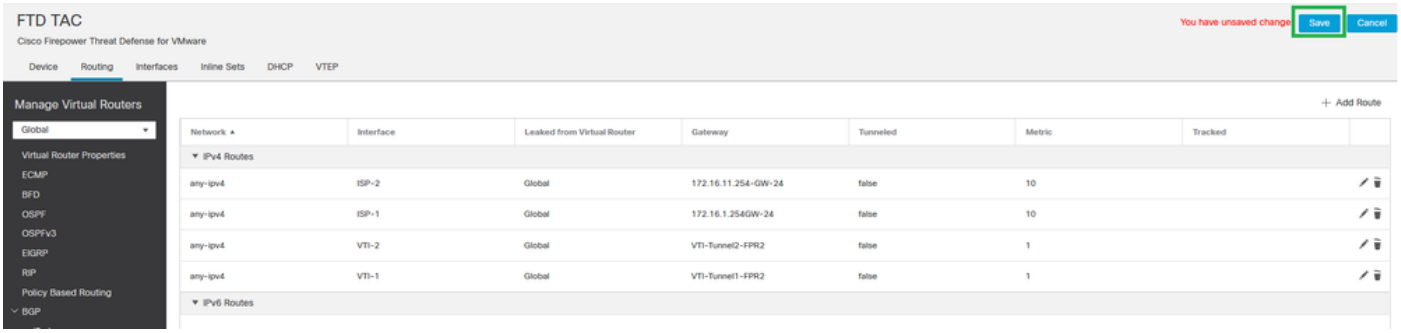


ISP-1的默认静态路由

步骤12.重复步骤10。如果配置了更多WAN/ISP接口。

注意：为配置的每个WAN/ISP接口创建默认路由。

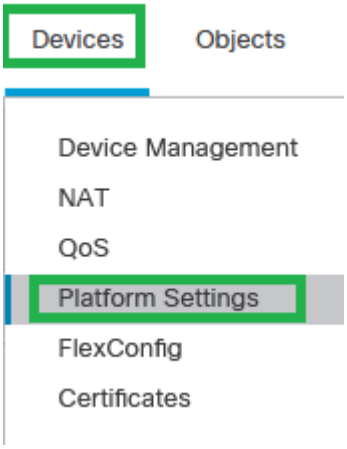
步骤13.验证默认路由配置并点击OK。



静态路由配置

为安全FTD配置受信任DNS

第 1 步： 导航至 。Devices > Platform Settings

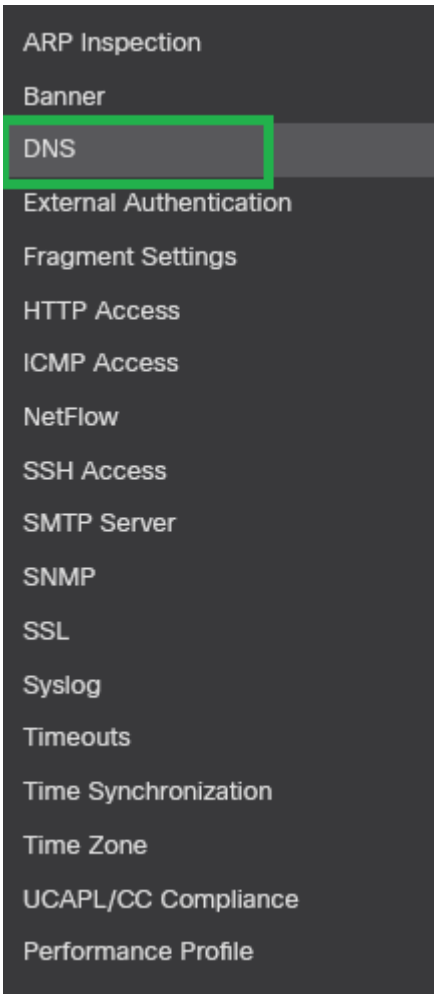


设备 — 平台设置

步骤2.创建或编辑现有平台设置策略。

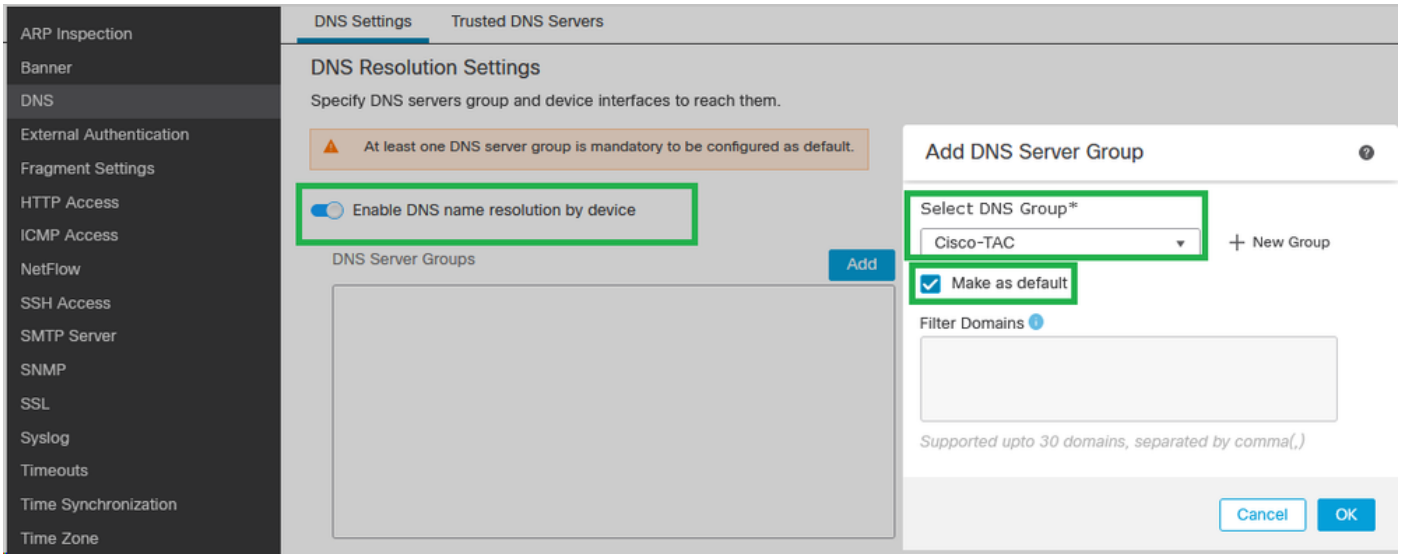
注意：确保平台设置策略应用于安全威胁防御设备。

步骤3.单击DNS。



DNS平台设置

步骤4.启用DNS name resolution by device并点击Add，或选择现有的DNS组。选择Make as default，然后单击OK。

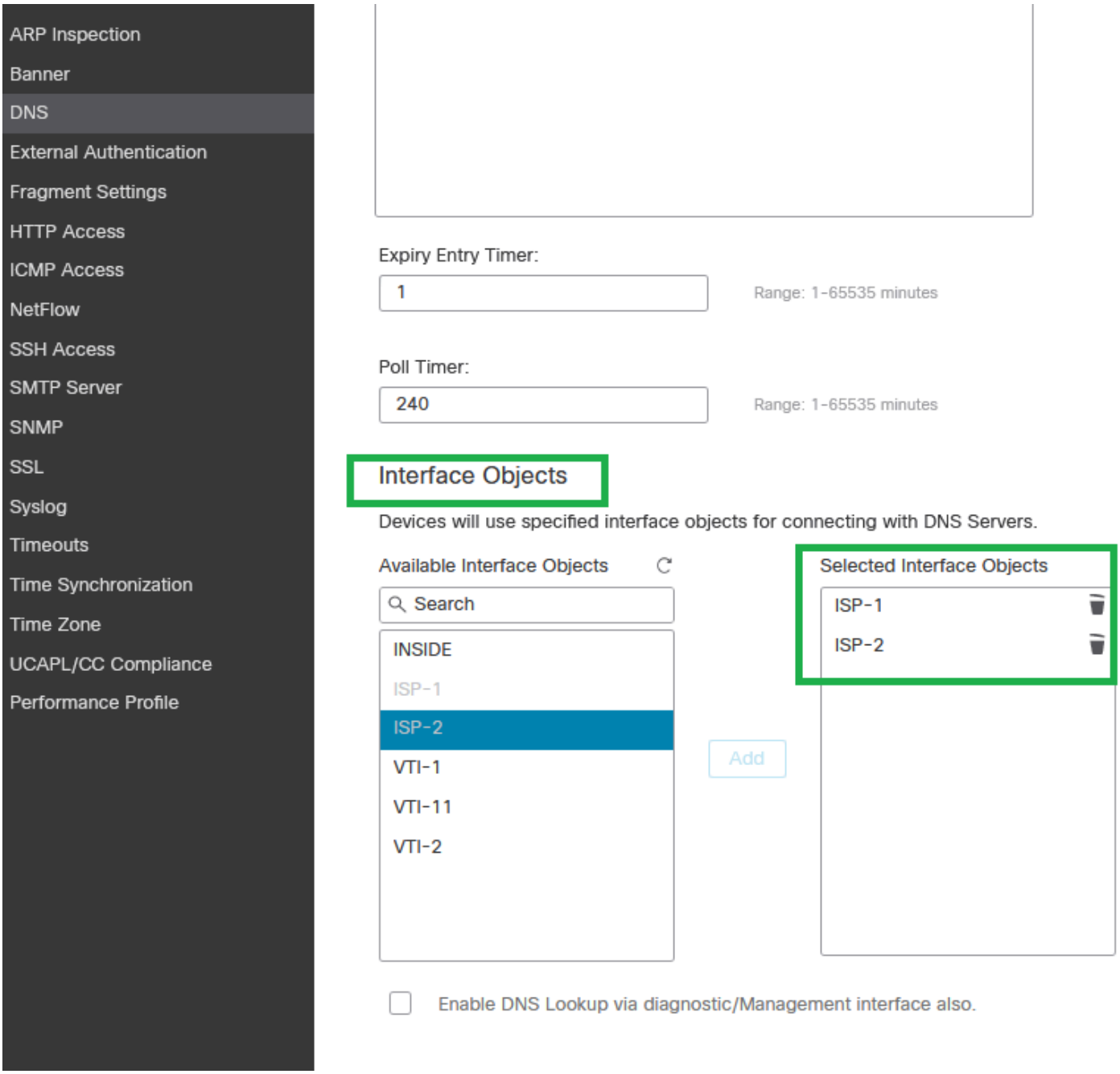


添加DNS服务器组

注意：如果您想了解有关平台设置策略上的DNS配置的详细信息，请查阅官方的平台设置

文档。

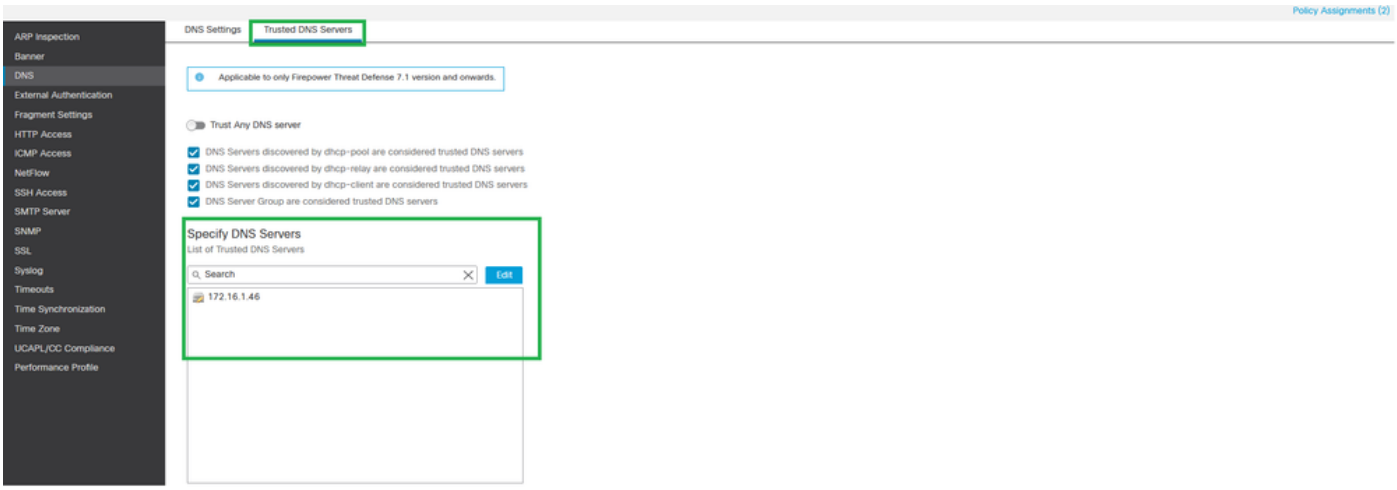
步骤5.选择部分下的WAN/ISP接Interface Objects口。



DNS接口配置

步骤6.保存更改。

步骤7.导航到并指Trusted DNS Servers定受信任DNS服务器。

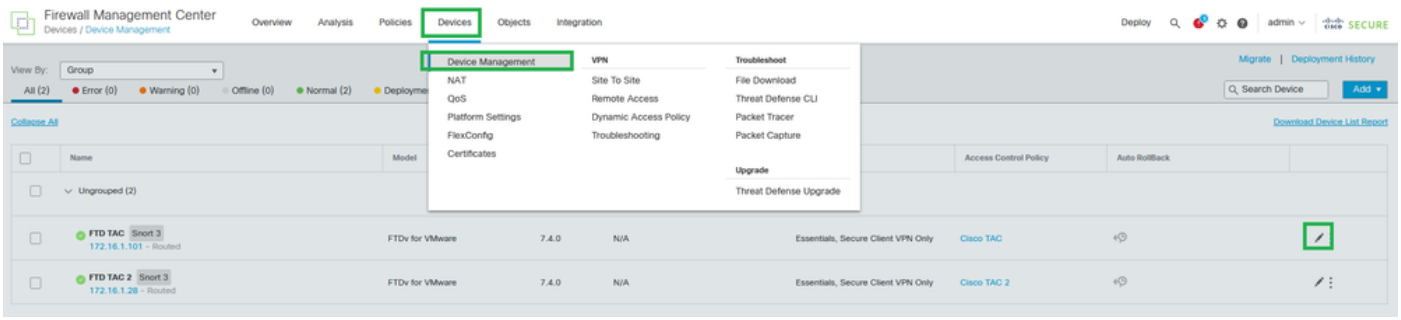


受信任的DNS服务器

步骤8.单击Save，然后部署更改。

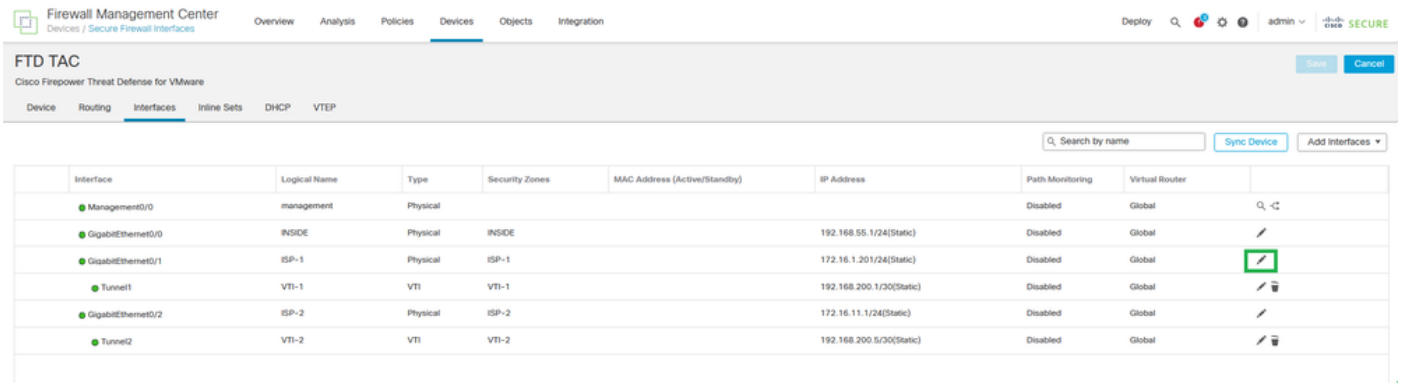
启用路径监控

步骤1.导航到Devices > Device Management，然后编辑威胁防御。



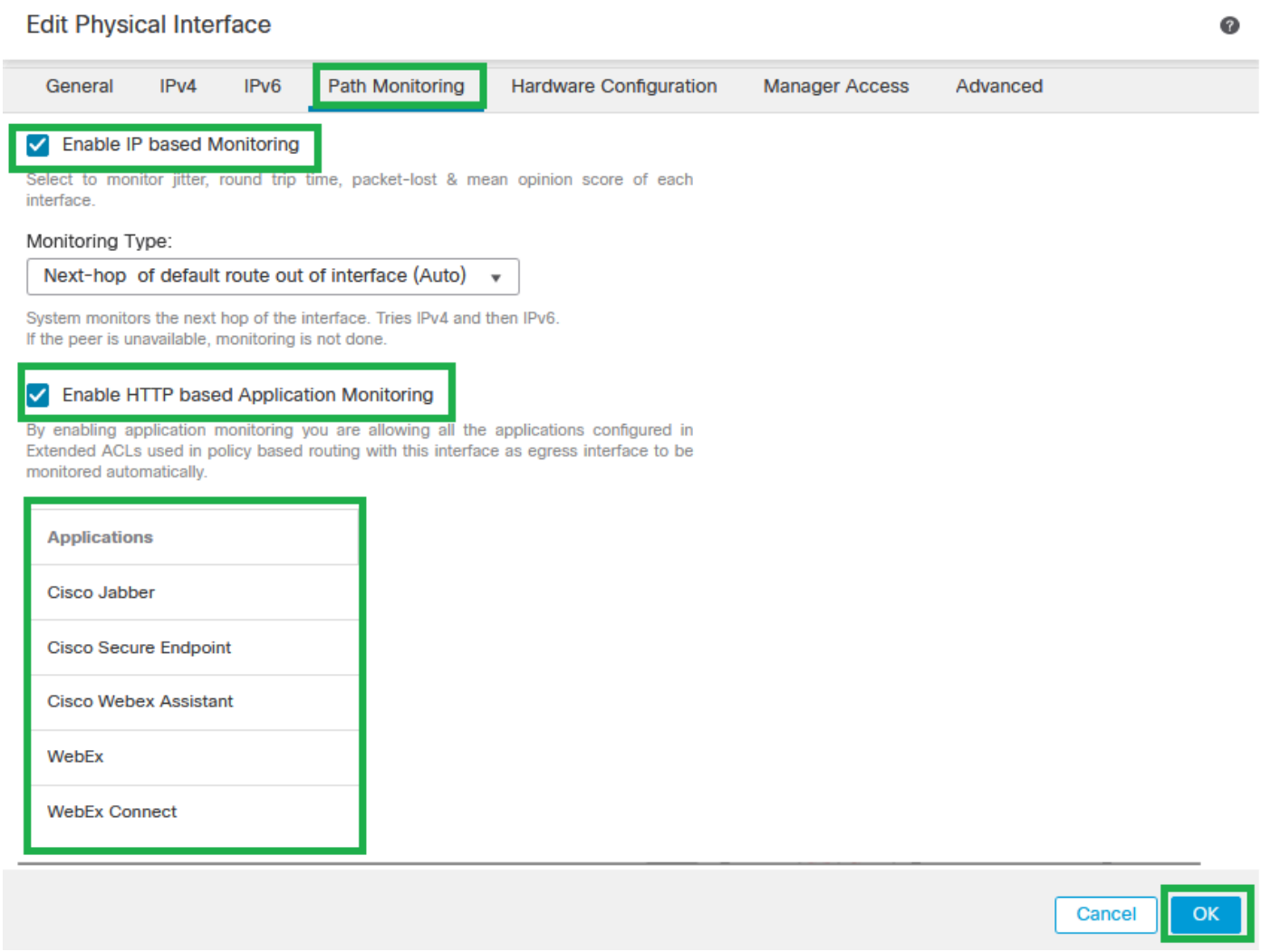
设备 — 设备管理

步骤2.在Interfaces选项卡下，编辑接口WAN/ISP接口（本配置指南中为ISP-1和ISP-2）。



接口配置

步骤3.点击该选Path Monitoring项卡，选择并启Enable IP Monitoring用该复选HTTP-based Application Monitoring框。？？然后单击.Save



接口路径监控配置

警告：必须列出在早期配置部分中配置的应用。

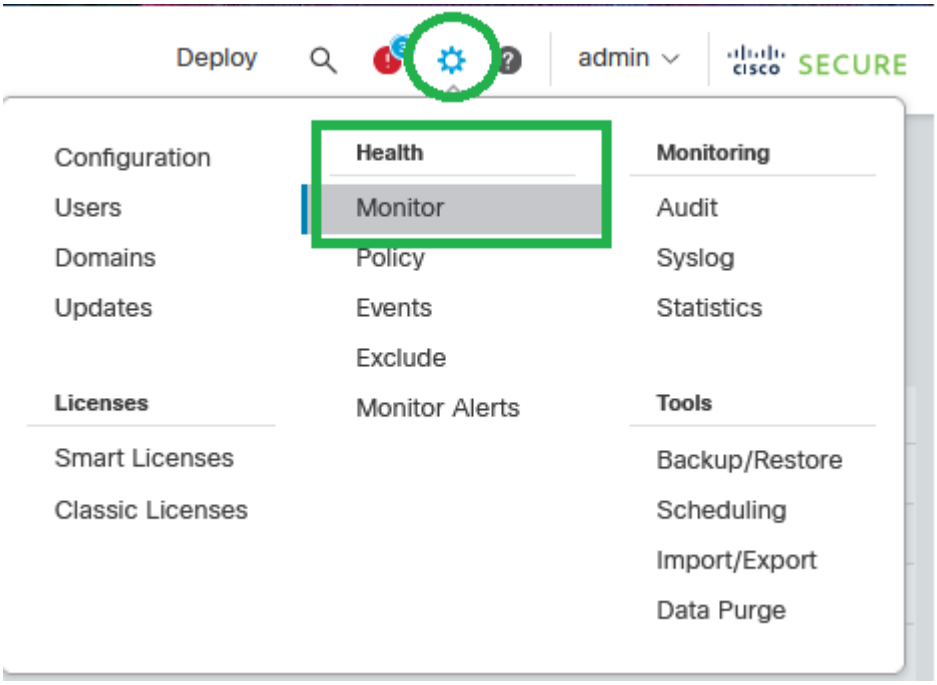
注意：已为此配置指南选择“监控类型”。查看官方配置指南上的Path Monitoring Settings以了解有关其他选项的详细信息。

步骤4.对配置的所有WAN/ISP接口重复步骤2和步骤3。

步骤5.单击Save，然后部署更改。

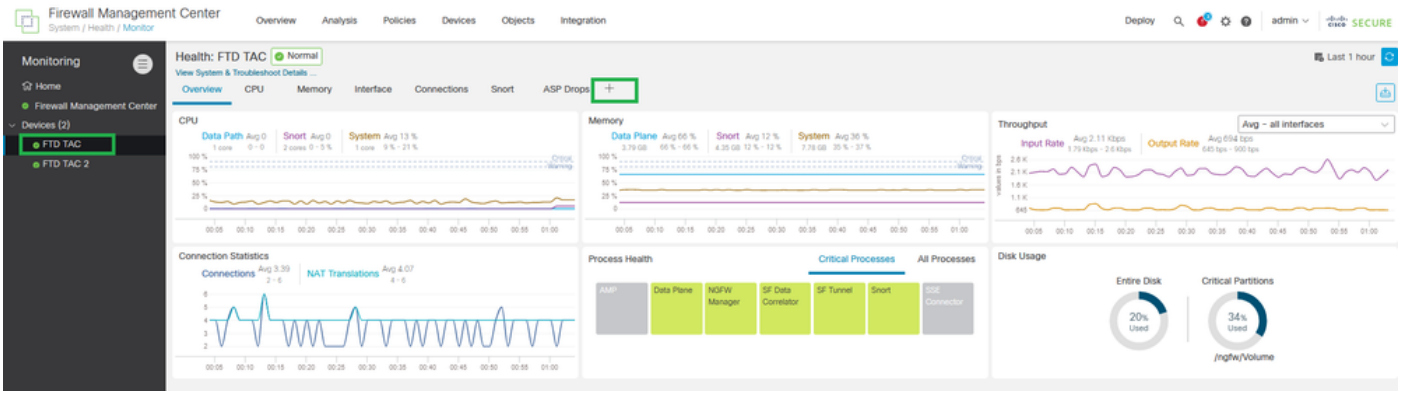
添加监控控制面板

第 1 步： 导航至 。System > Health > Monitor



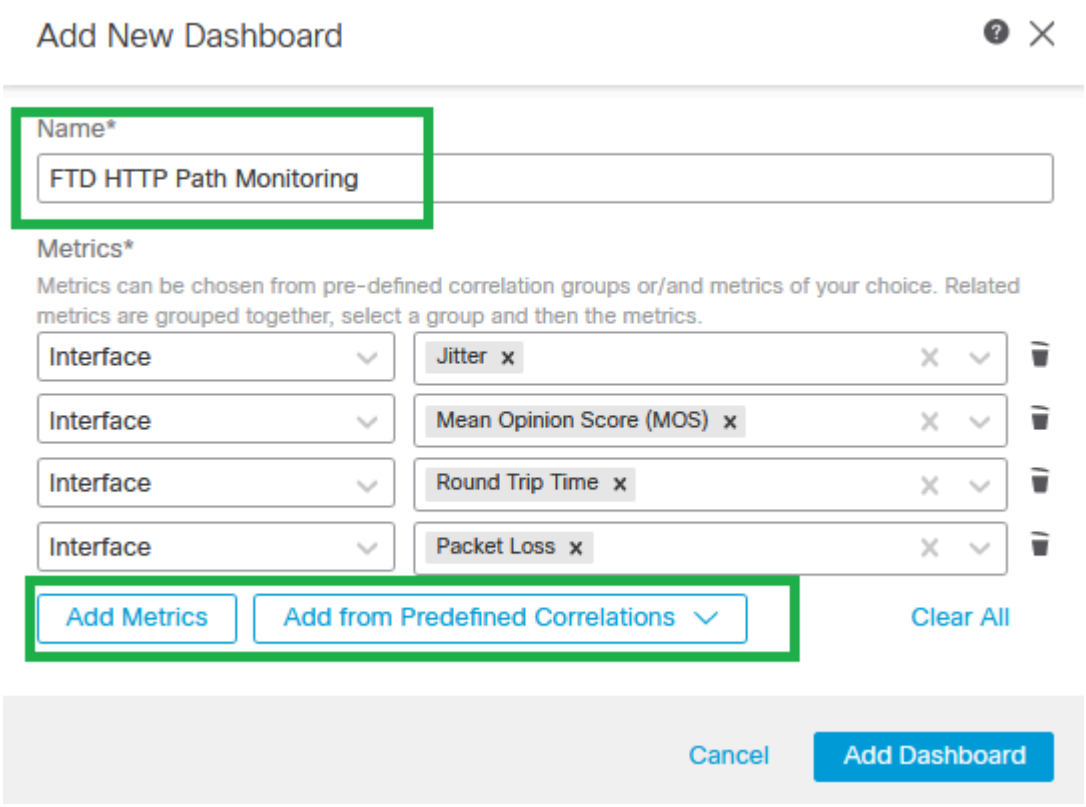
系统 — 运行状况 — 监控

步骤2.选择安全FTD设备，然后点击Add New Dashboard。



添加新控制面板

步骤3.设置仪表板名称，Correlate Metrics在对话框中，从下拉列表中选择Interface - Path Metrics。 ？？然后单击.Add Dashboard



添加具有路径度量的新控制面板

验证

本节介绍如何验证浮动静态路由、ECMP、包含应用程序的对象组和PBR配置。

检验默认路由和浮动静态路由配置：

```
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
```

验证ECMP配置：

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

验证路由表上的ECMP是否正在平衡流量。路由表必须在安全FTD路由表中安装两条路由。

```
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
```

验证PBR路由映射配置：

```
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
!
```

检验分配给PBR配置的ACL（检查路由映射配置上的ACL名称）：

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

验证Object Group with Applications assigned to the access list（使用分配给访问列表的应用程序，检查ACL配置中的Object group name）：

```
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"
```

验证分配给PBR配置中使用的数据接口的策略路由：

```
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
!
```

从HTTP路径监控控制面板信息验证并检查抖动、MOS、往返时间和丢包统计信息。



验证HTTP路径监控仪表板

故障排除

如果路径监控失败，在启用基于IP的监控时，WAN/ISP接口配置为向静态路由上配置的网关发送ICMP探测数据包。在WAN/ISP接口上配置入口/出口捕获，以检查ICMP是否工作。

入口和出口捕获：

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

入口捕获：

```
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
```

出口捕获：

```
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
```



警告：确保使用源IP地址和目标IP地址配置捕获，因为捕获可以显着提高设备性能。



提示：如果ping不起作用，请排除与默认网关的直接连接故障，检查ARP表或与思科TAC联系。

为了检查PBR是否工作，您可以使用Packet Tracer工具确保通过PBR路由应用流量。

```
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
```



注意：要了解在对象组上配置的网络服务的应用IP地址，请使用命**show object-group network-service detail**令。

相关信息

有关带有HTTP路径监控的PBR的其他文档，请访问以下网站：

- 《Secure Firewall Management Center设备配置指南上的基于策略的路由配置》
- 《Secure Firewall Management Center设备配置指南》中基于策略的路由配置的路径监控
- 配置基于策略的路由策略
- 基于策略的路由的配置示例
- 配置PBR路径监控示例
- 添加路径监控仪表板
- 安全防火墙管理中心设备上的DNS平台设置配置指南
- 思科技术支持和下载

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）。