在FDM管理的FTD上使用IP SLA配置ECMP

目录

简介

本文档介绍如何在由FDM管理的FTD上配置ECMP和IP SLA。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙威胁防御(FTD)上的ECMP配置
- 思科安全防火墙威胁防御(FTD)上的IP SLA配置
- 思科安全防火墙设备管理器(FDM)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD版本7.4.1（内部版本172）

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

本文档介绍如何在由Cisco FDM管理的Cisco FTD上配置等价多路径(ECMP)以及互联网协议服务级别协议(IP SLA)。 ECMP允许您在FTD上将接口分组到一起，并在多个接口之间均衡流量负载。 IP SLA是一种通过交换常规数据包来监控端到端连接的机制。与ECMP一起，可以实施IP SLA以确保下一跳的可用性。 在本例中，ECMP用于在两个Internet服务提供商(ISP)电路上平均分配数据包。同时，IP SLA会跟踪连通性，确保在发生故障时无缝过渡至任何可用电路。

本文档的具体要求包括：

- 使用具有管理员权限的用户帐户访问设备
- 思科安全防火墙威胁防御7.1版或更高版本

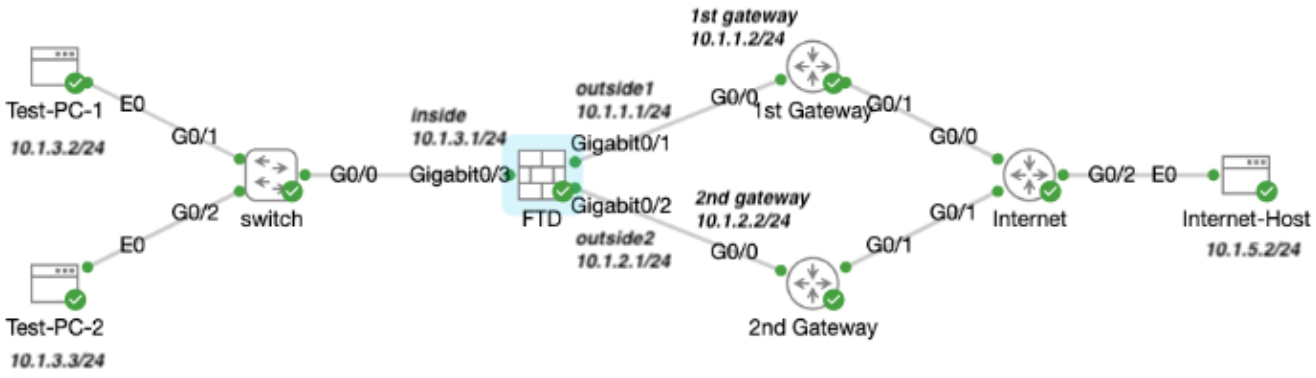
配置

网络图

在本例中，Cisco FTD有两个外部接口：outside1和outside2。每个都连接到ISP网关，outside1和outside2属于名为outside的同一个ECMP区域。

来自内部网络的流量通过FTD路由，并通过两个ISP实现到Internet的负载均衡。

同时，FTD使用IP SLA来监控与每个ISP网关的连接。如果任何ISP电路出现故障，FTD会故障切换到另一个ISP网关以保持业务连续性。

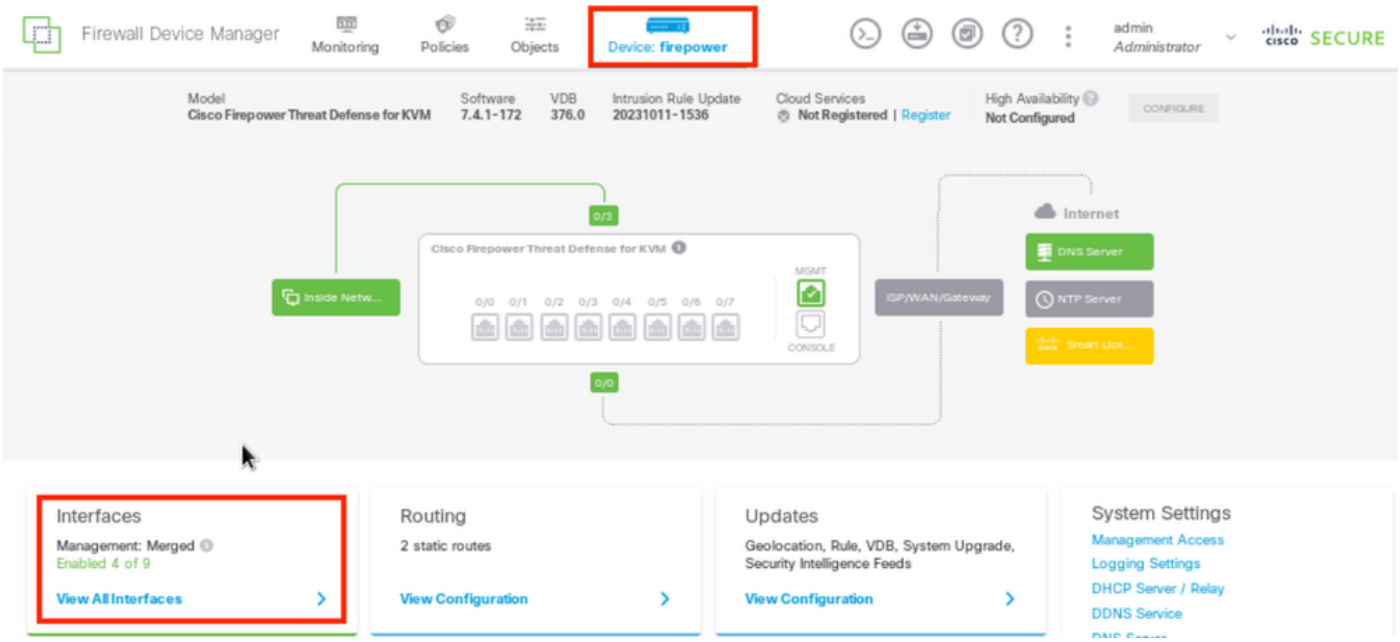


网络图

配置

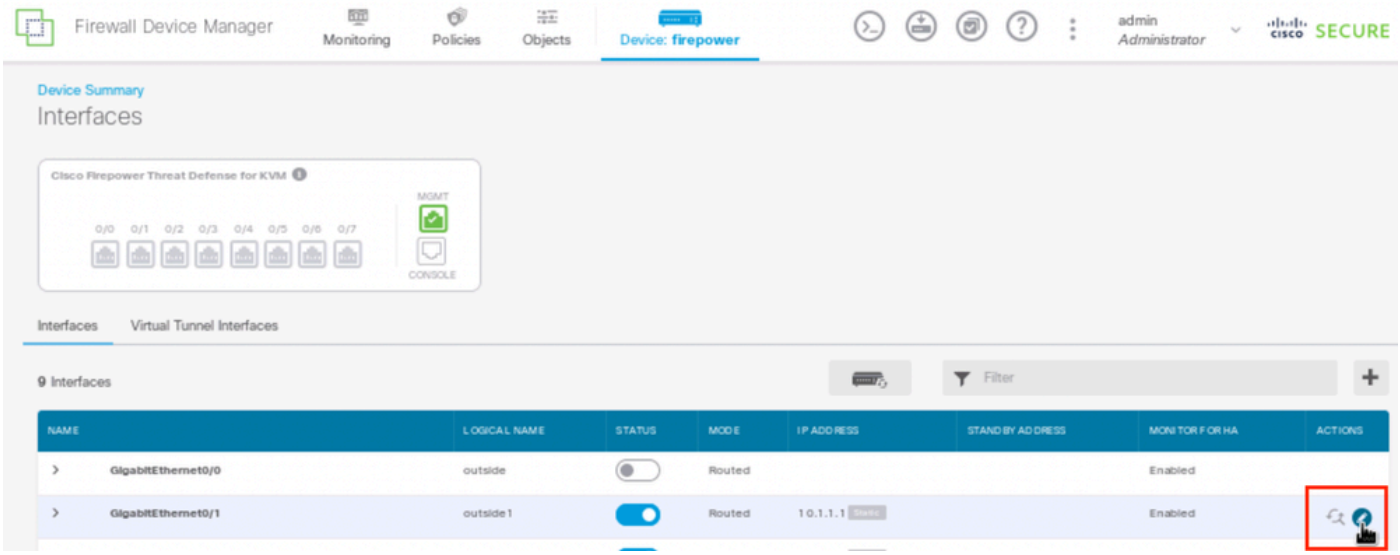
步骤 0预配置接口/对象

登录FDM Web GUI，单击Device，然后单击Interfaces摘要中的链接。 Interfaces 列表显示可用接口及其名称、地址和状态。



FDM设备接口

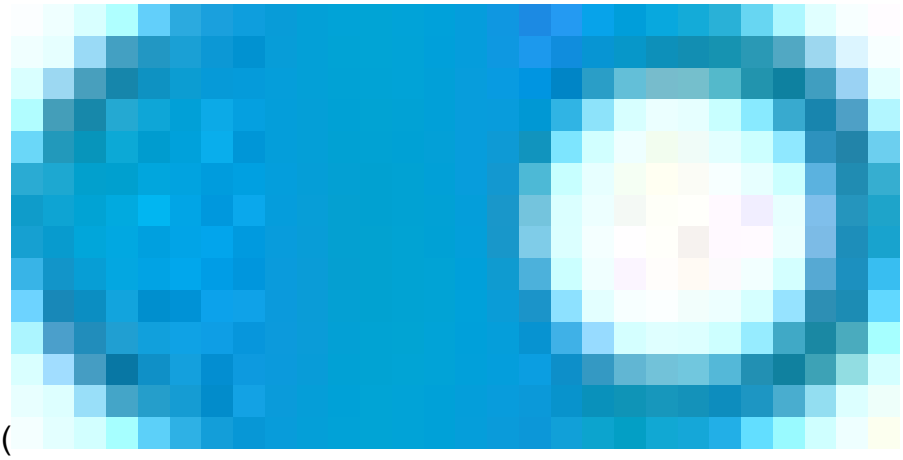
点击要编辑的物理接口的编辑图标(
)。 在本示例中，GigabitEthernet0/1。



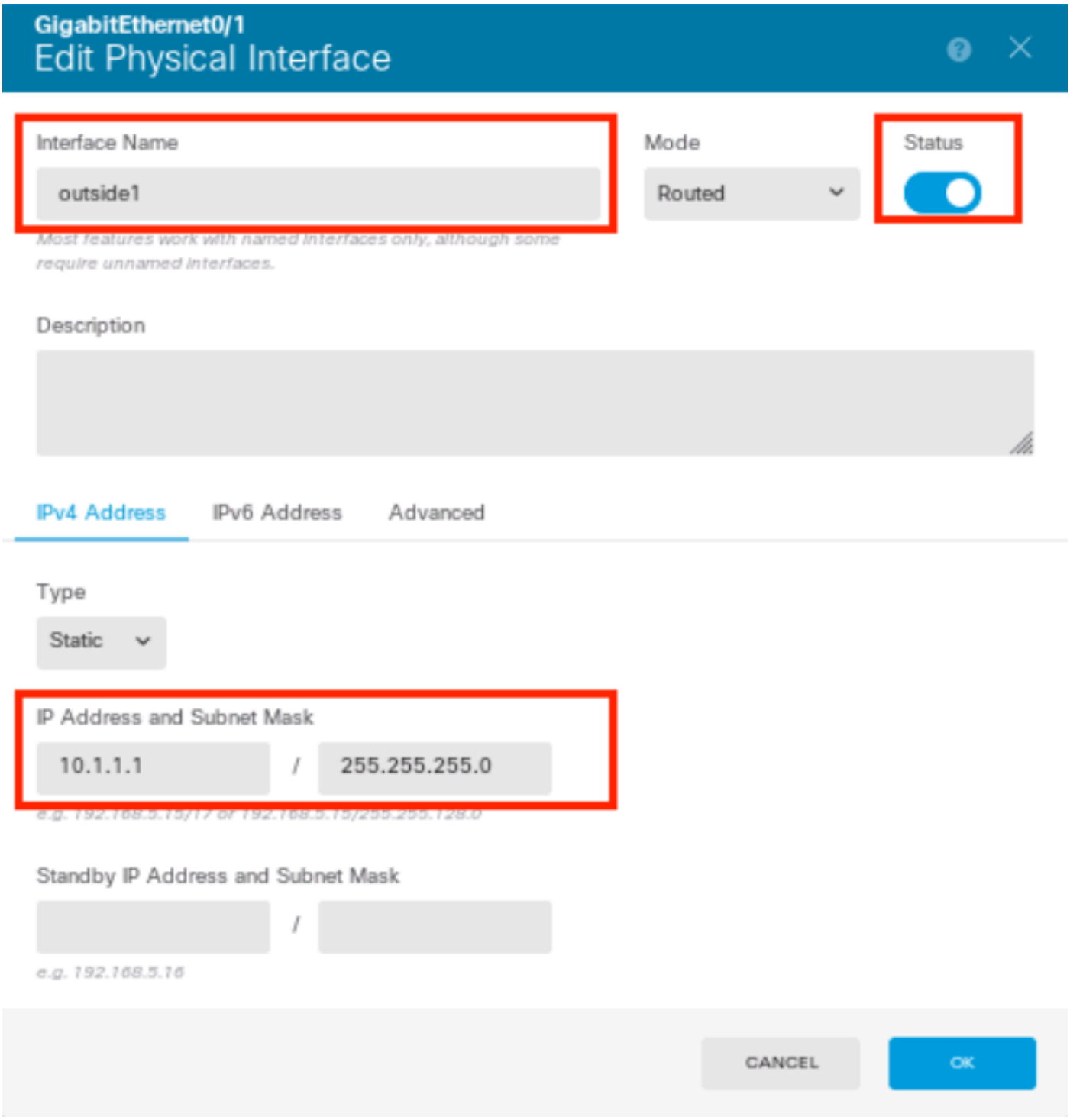
步骤0接口Gi0/1

在Edit Physical Interface窗口中：

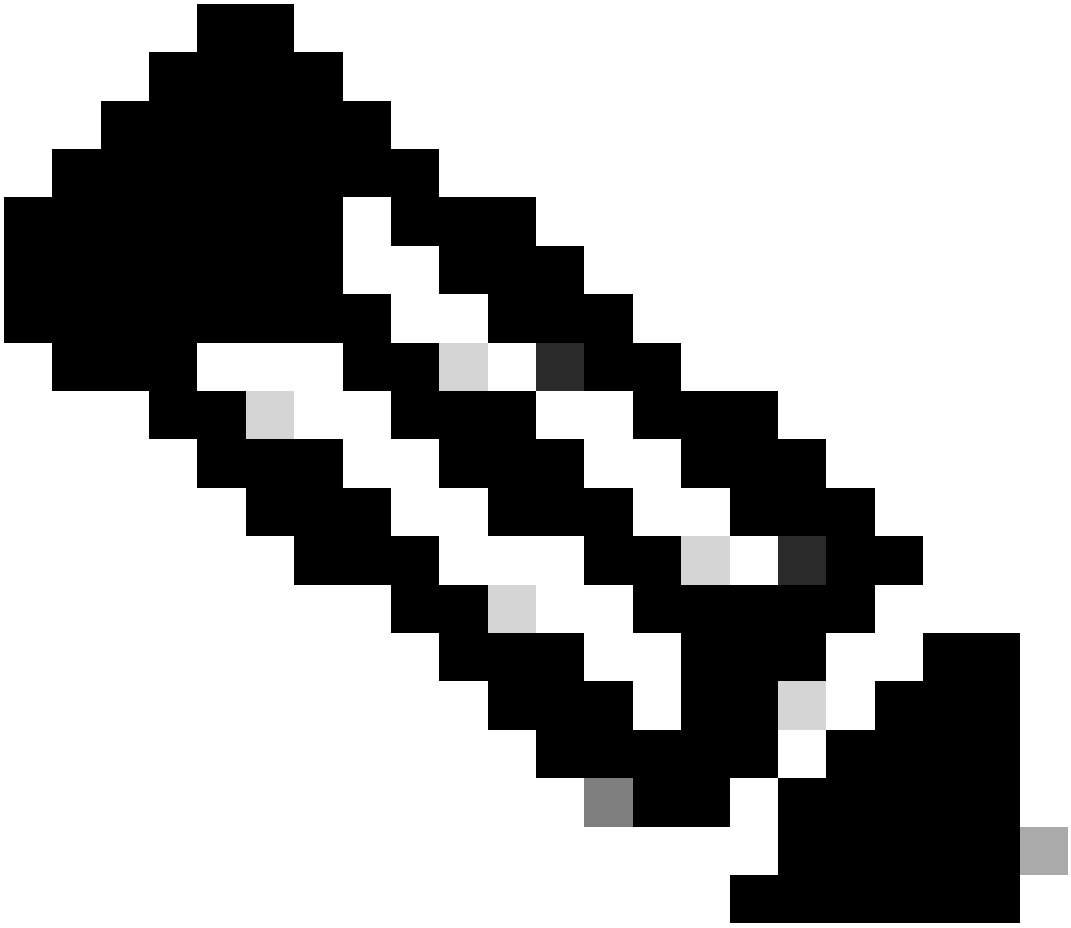
1. 设置Interface Name，在本例中为outside1。



2. 将状态滑块设置为已启用设置( )。
3. 单击IPv4 Address选项卡并配置IPv4地址(本例中为10.1.1.1/24)。
4. Click OK.



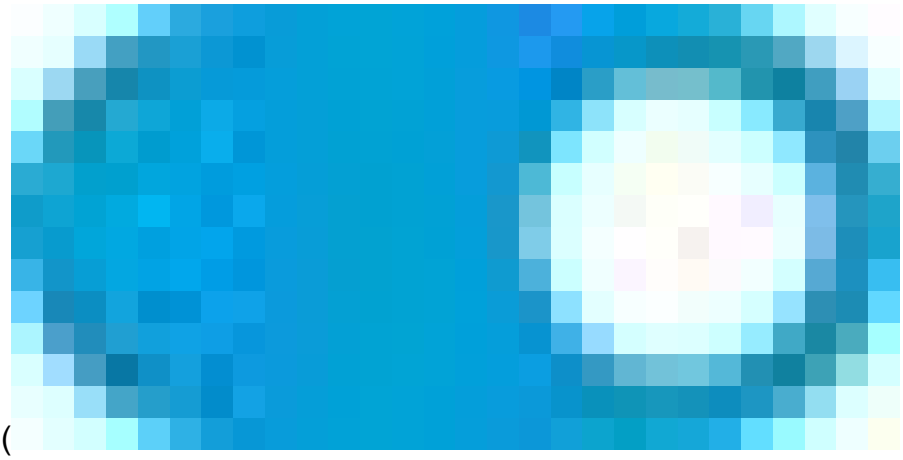
步骤0编辑接口Gi0/1



注意：只有路由接口可以与ECMP区域关联。

重复类似步骤，为辅助ISP连接配置接口，本示例中物理接口为GigabitEthernet0/2。在Edit Physical Interface窗口中：

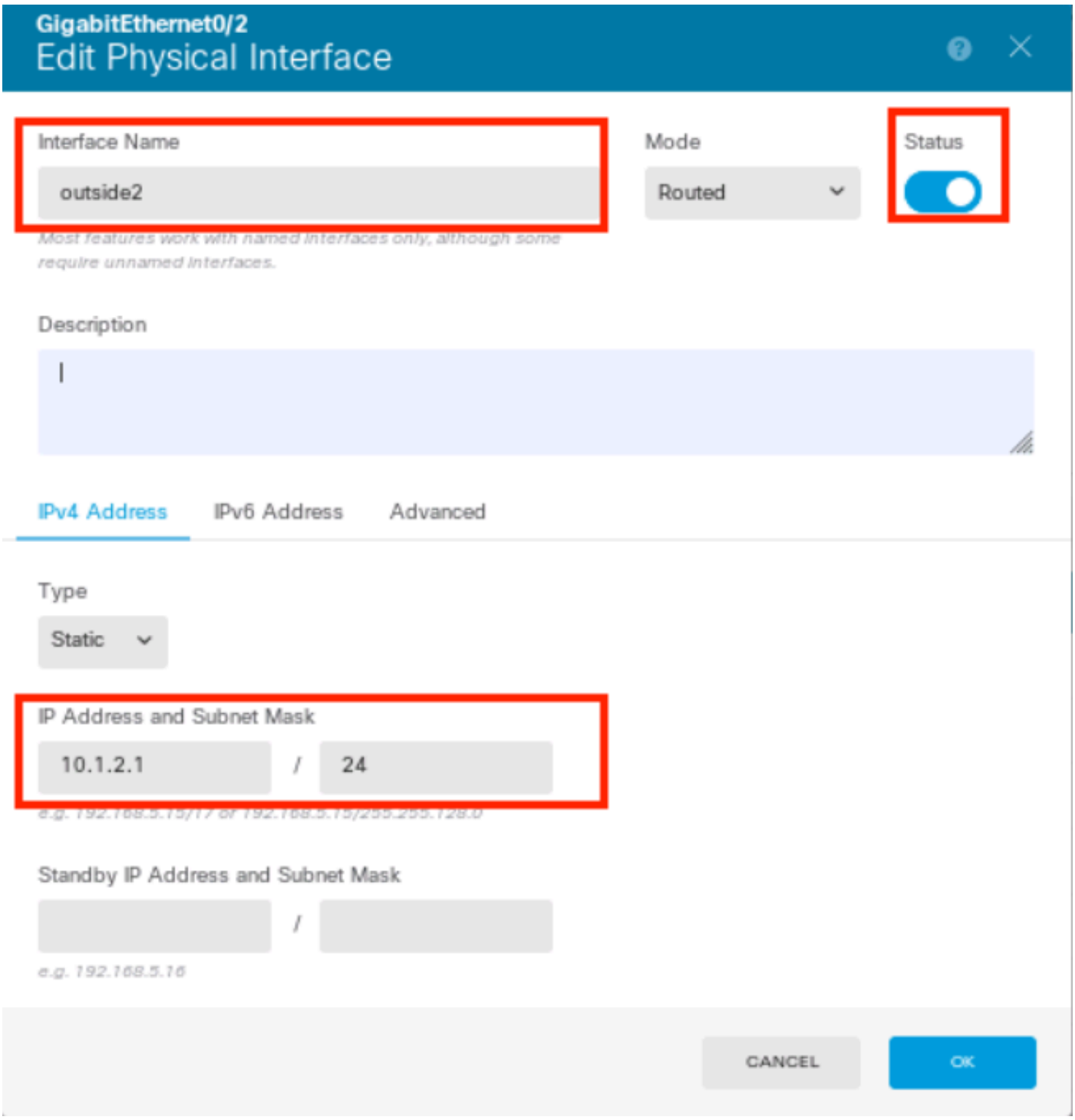
1. 设置Interface Name，在本例中为outside2。



2. 将状态滑块设置为已启用设置(

)。

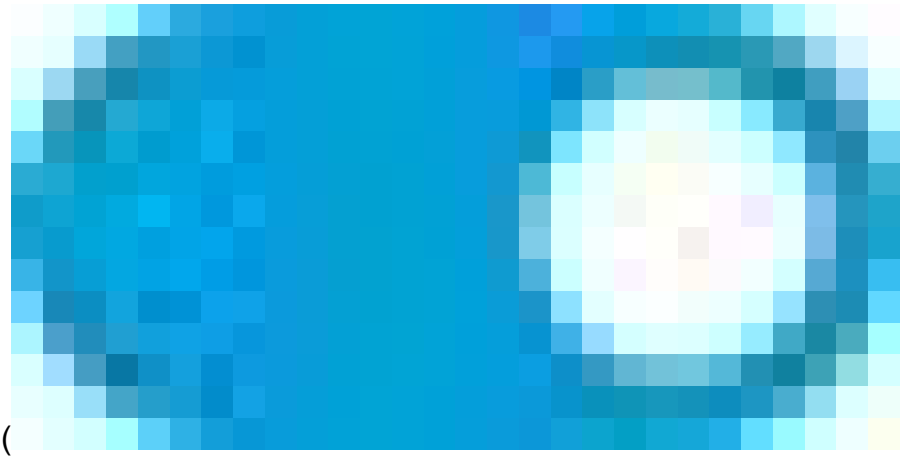
3. 单击IPv4 Address 选项卡并配置IPv4地址，在本例中为10.1.2.1/24。
4. Click OK.



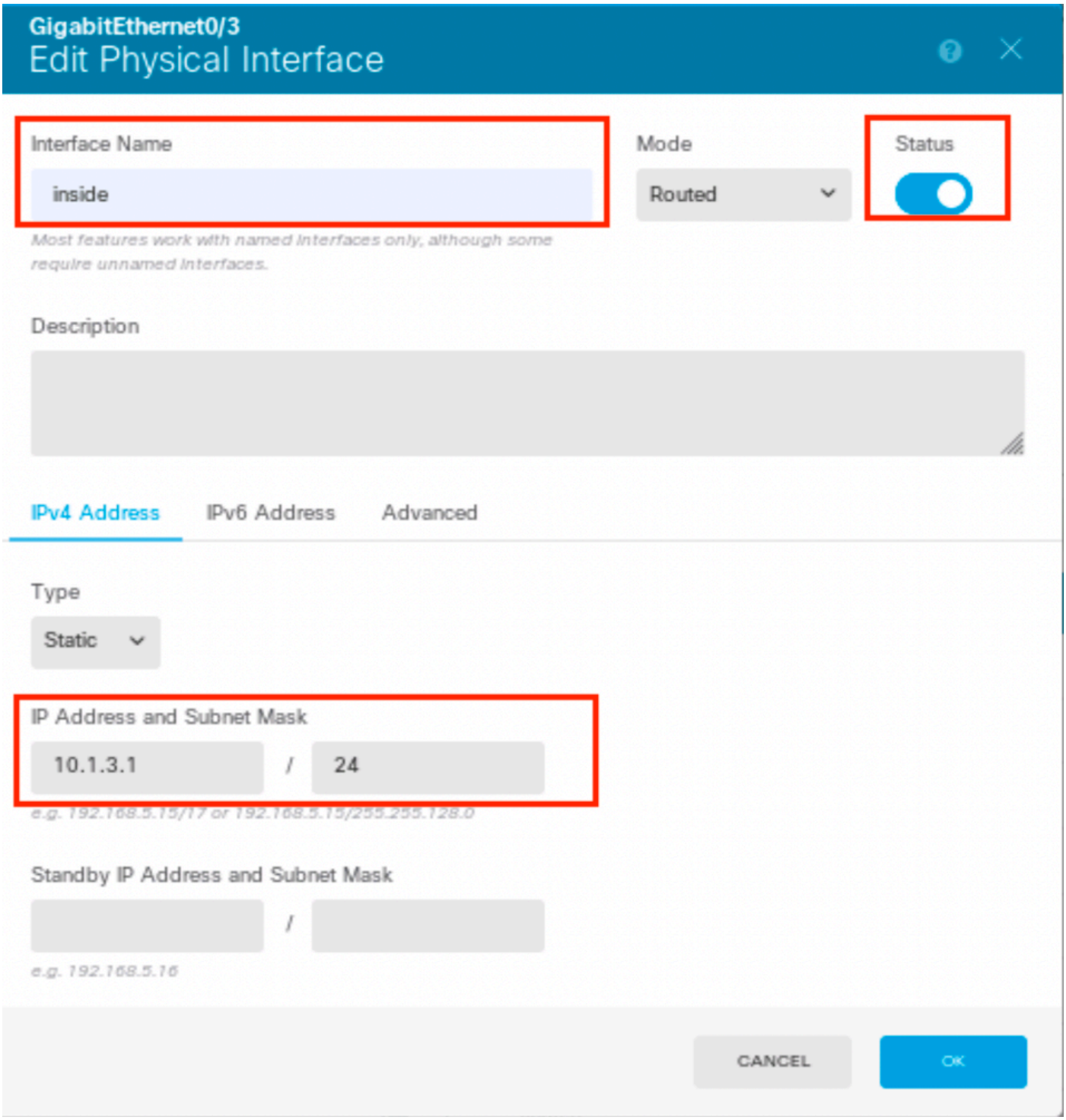
步骤0编辑接口Gi0/2

重复类似步骤，为内部连接配置接口，在本示例中，物理接口为GigabitEthernet0/3。在Edit Physical Interface窗口中：

1. 设置Interface Name，在此示例中为inside。

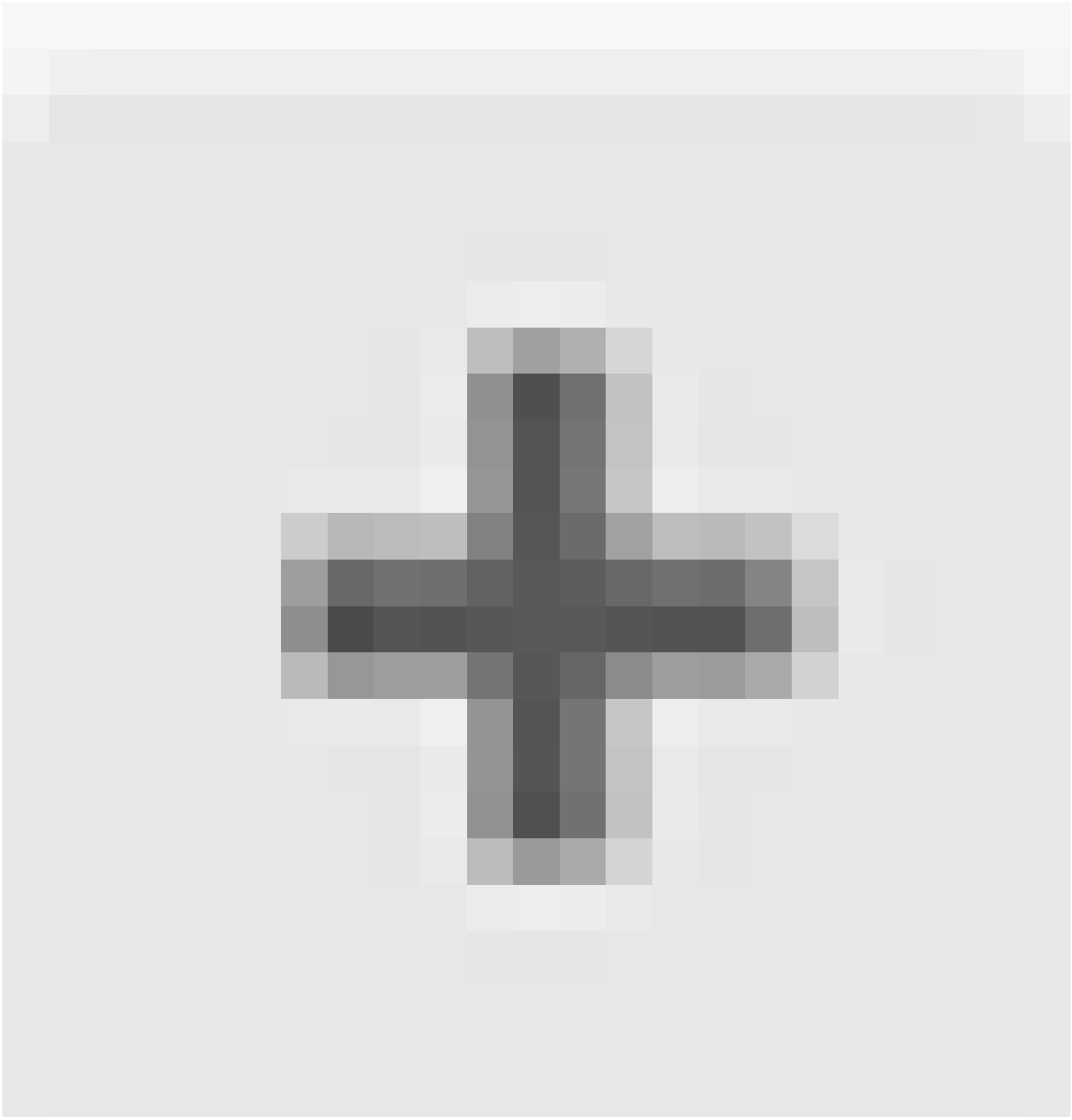


2. 将状态滑块设置为已启用设置(
)。
3. 点击IPv4 Address选项卡并配置IPv4地址，在本例中为10.1.3.1/24。
4. Click OK.

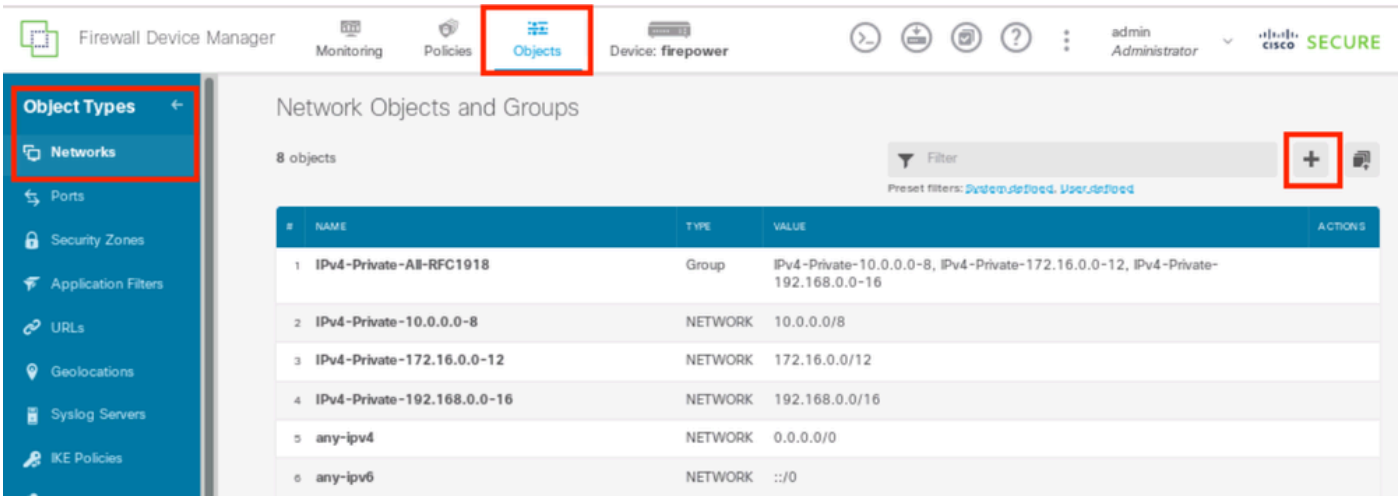


步骤0编辑接口Gi0/3

导航到对象>对象类型>网络，点击添加图标(



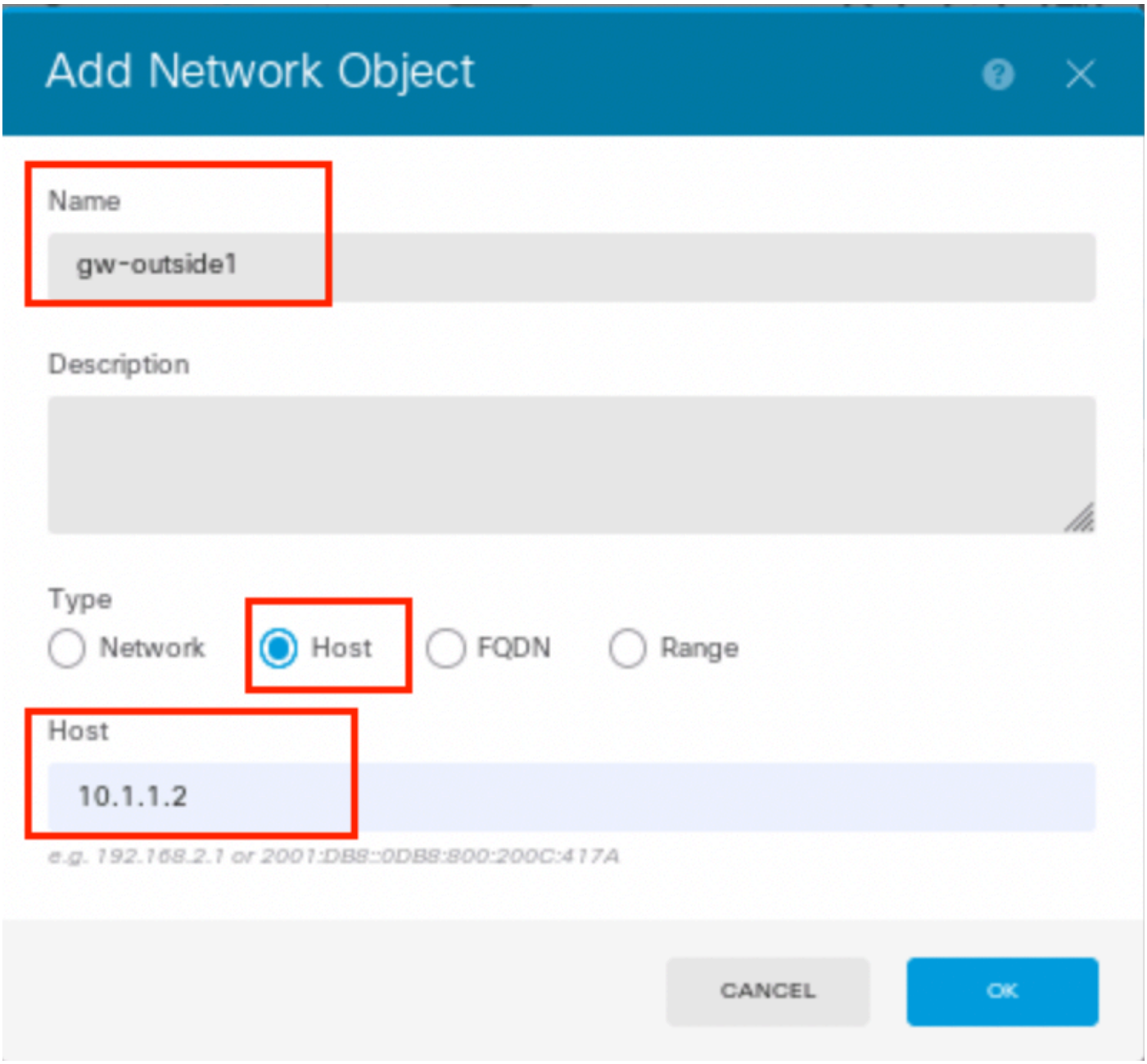
)添加新对象。



第0步对象1

在Add Network Object 窗口中，配置第一个ISP网关：

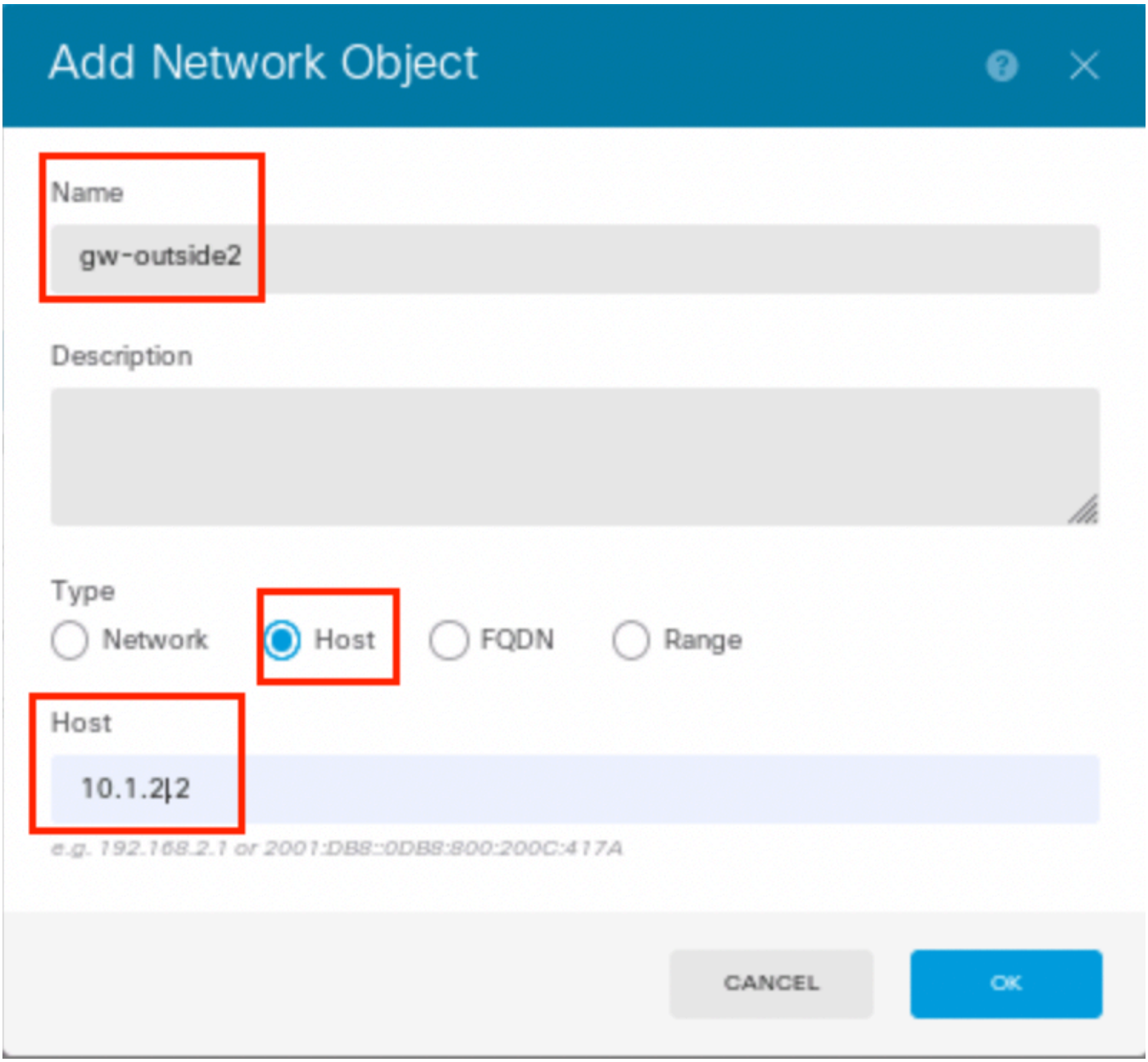
1. 设置对象的Name，在本例中为gw-outside1。
2. 选择对象的类型，在本例中为主机。
3. 设置主机的IP地址，在本例中为10.1.1.2。
4. Click OK.



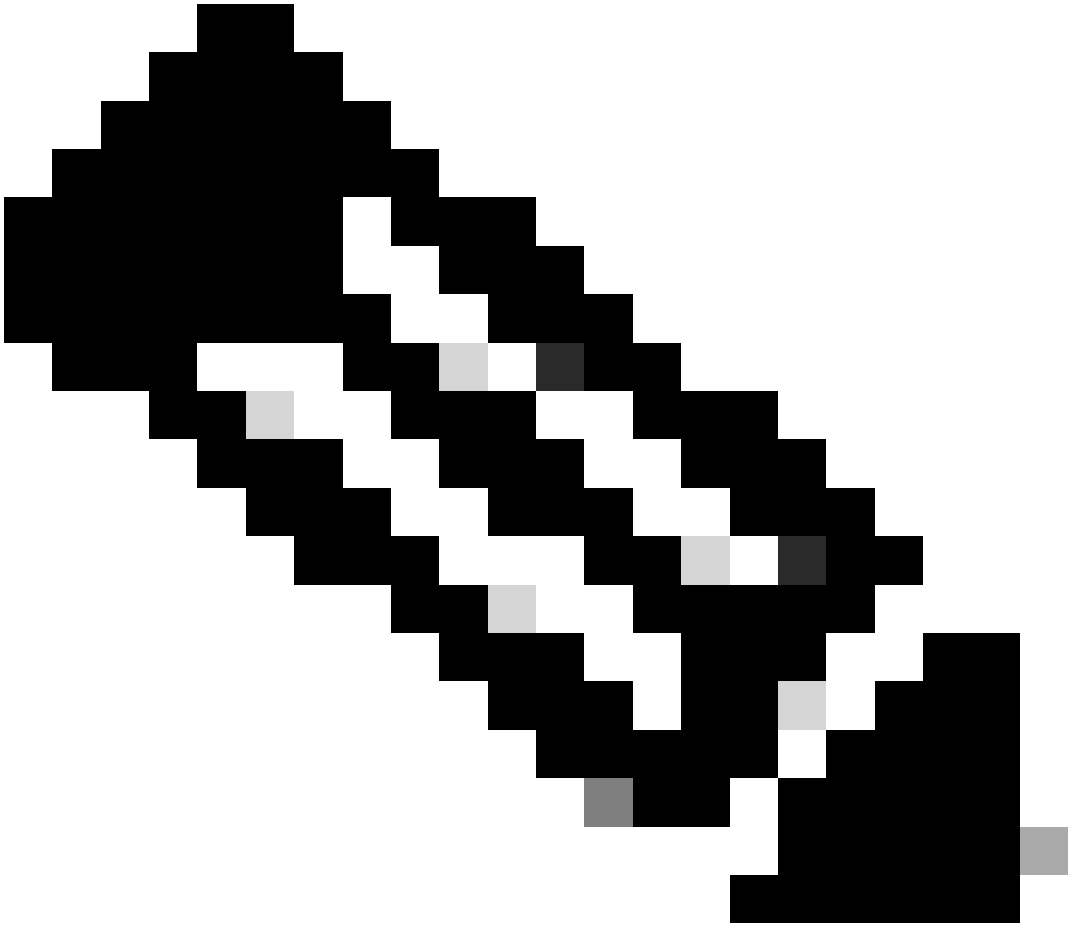
第0步对象2

重复类似步骤，为第二个ISP网关配置另一个网络对象：

1. 设置对象的Name，在本例中为gw-outside2。
2. 选择对象的类型，在本例中为主机。
3. 设置主机的IP地址，在本例中为10.1.2.2。
4. Click OK.


Add Network Object
Name
gw-outside2
Description
Type
Network
Host
FQDN
Range
Host
10.1.2.2
e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A
CANCEL
OK

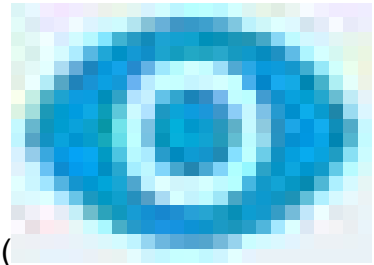
第0步对象3



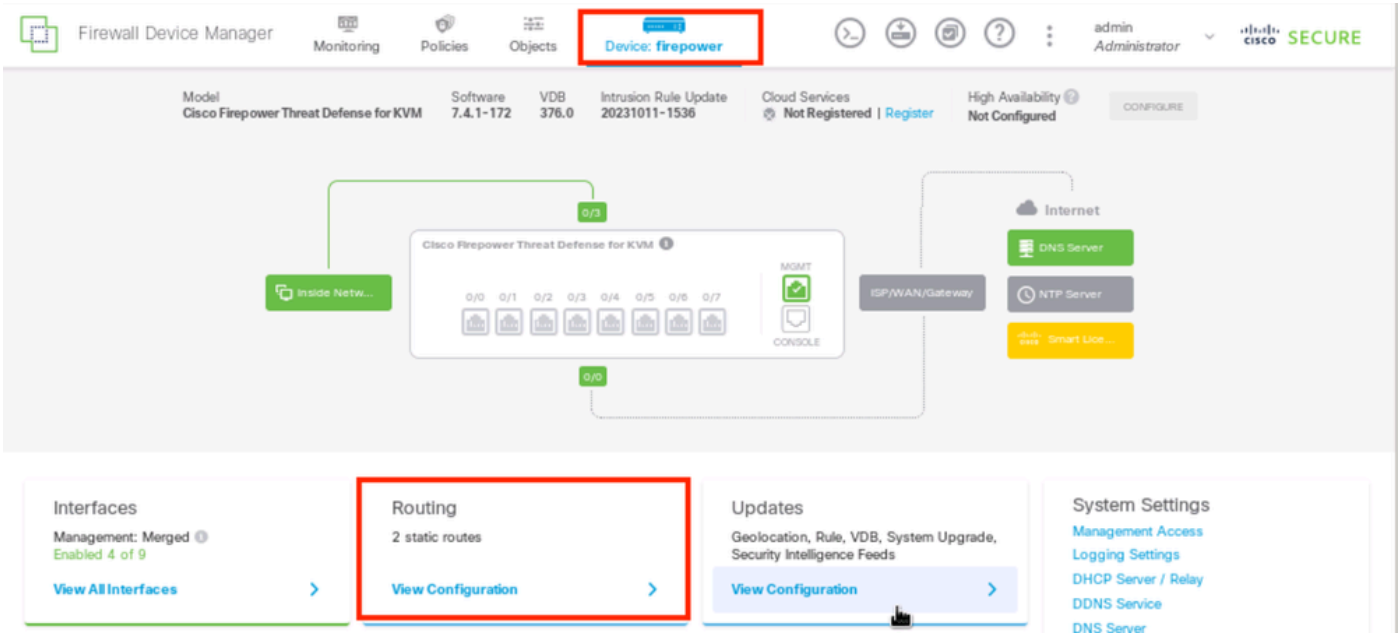
注意：必须在FTD上配置访问控制策略才能允许该流量，本文档中不包含此部分。

步骤1:配置ECMP区域

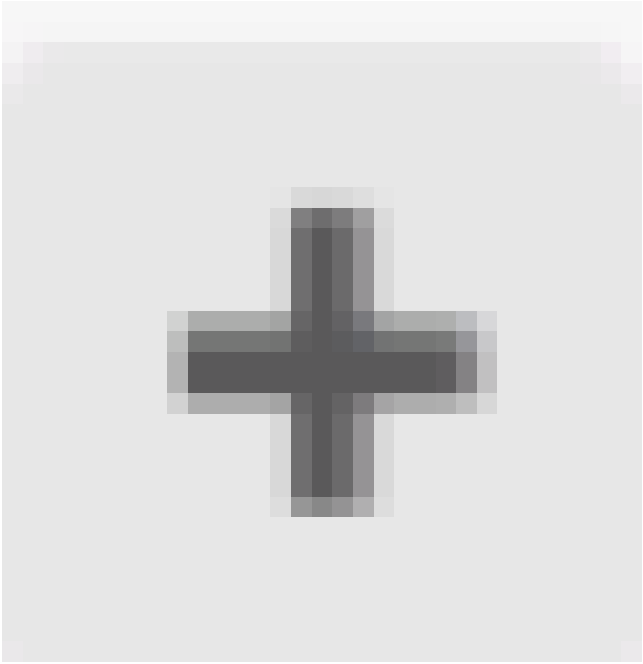
导航到设备，然后点击路由摘要中的链接。



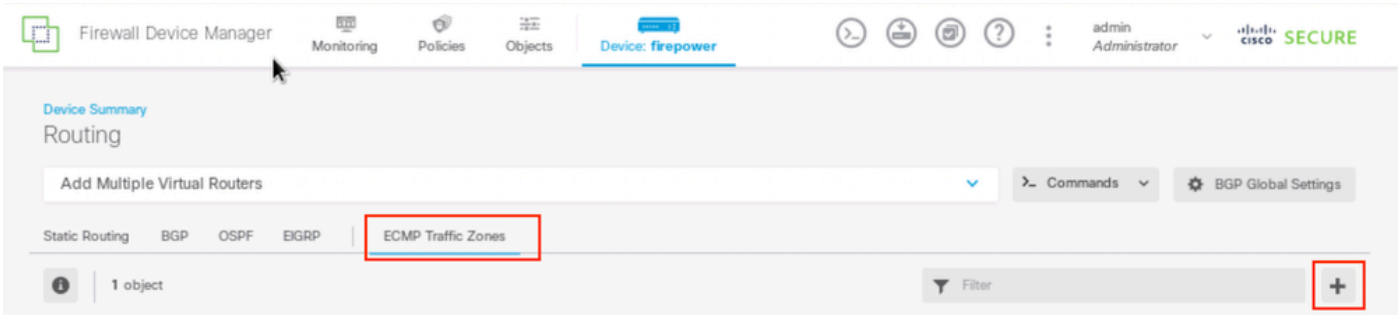
如果启用了虚拟路由器，请点击在其中配置静态路由的路由器的查看图标( )。在这种情况下，虚拟路由器未启用。



第1步ECMP Zone1

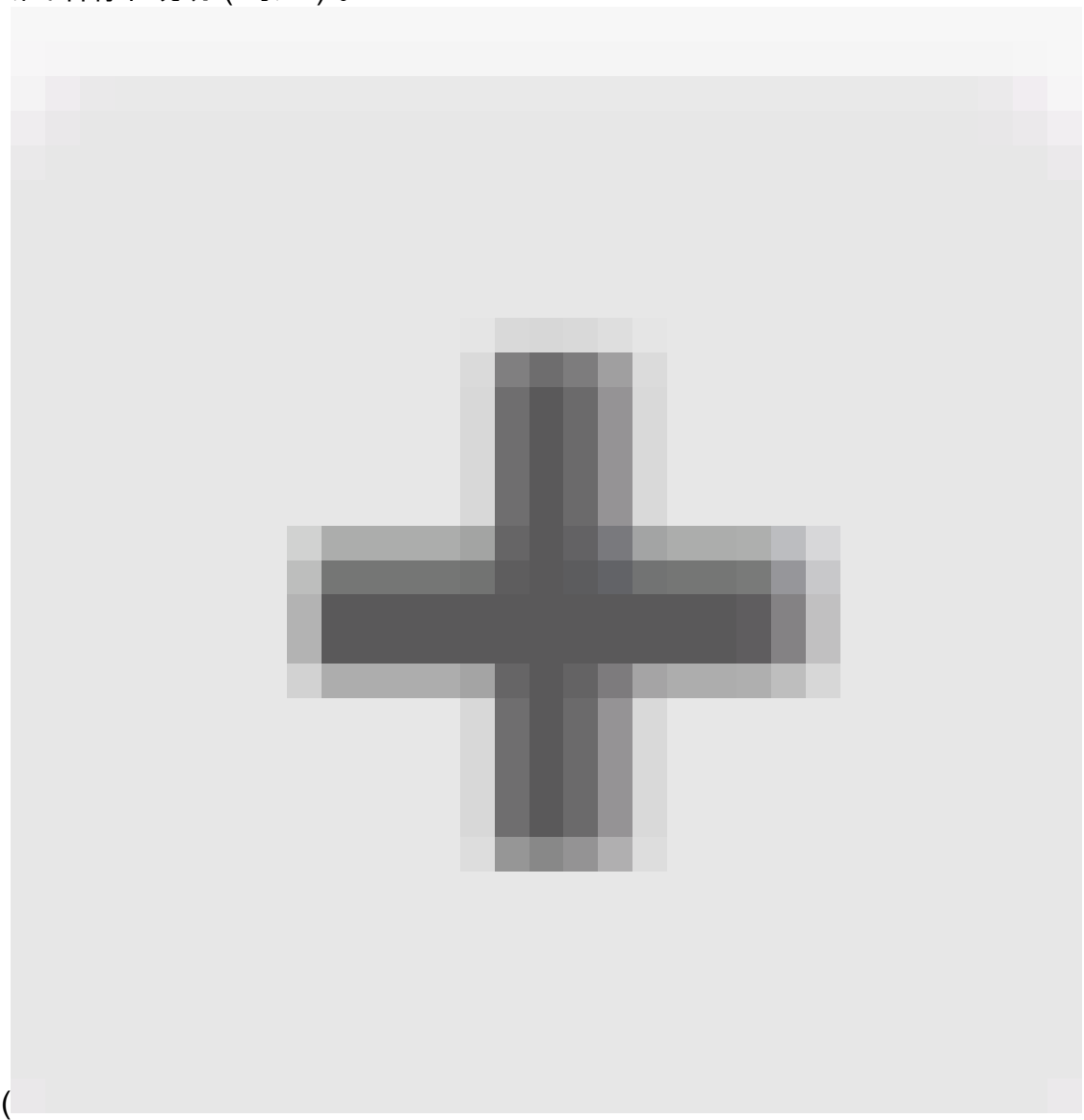


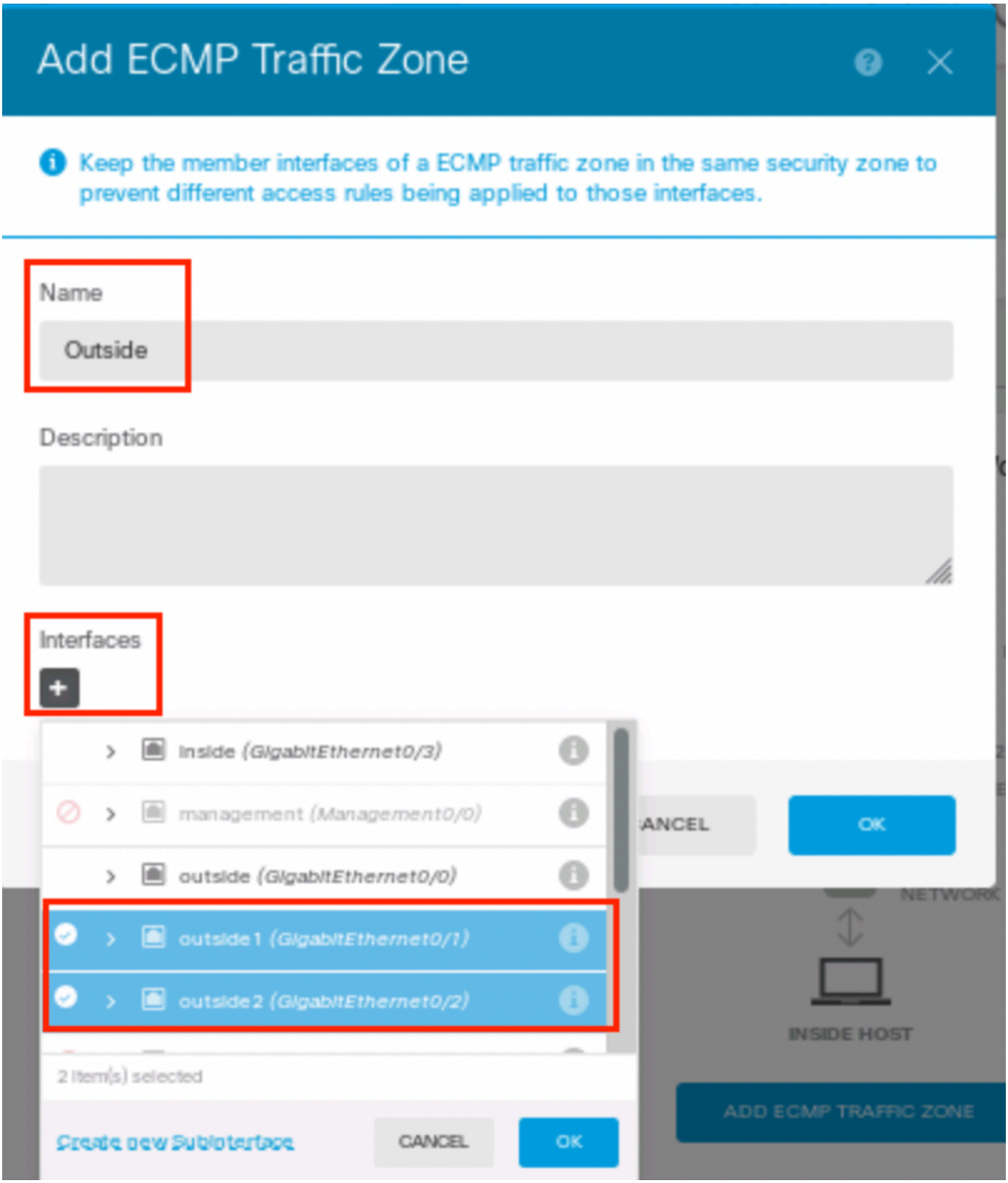
点击ECMP Traffic Zones选项卡，然后点击添加图标( )添加新区域。



第1步ECMP Zone2

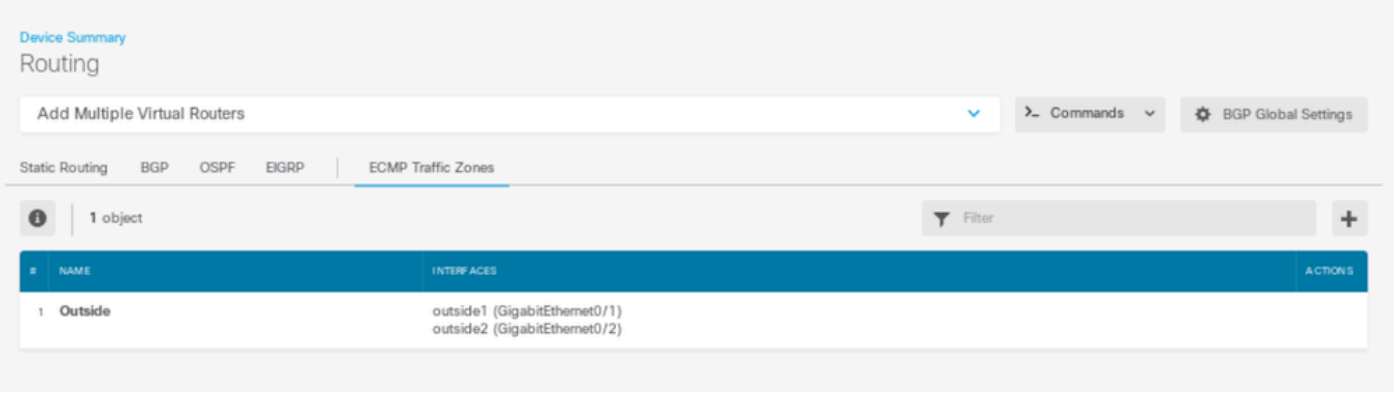
在Add ECMP Traffic Zone窗口中：

1. 设置ECMP区域的名称和说明（可选）。
2. 点击添加图标()可选择最多8个接口以包含在区域中。在本示例中，ECMP名称为Outside，接口outside1和outside2将添加到此区域。
3. Click OK.

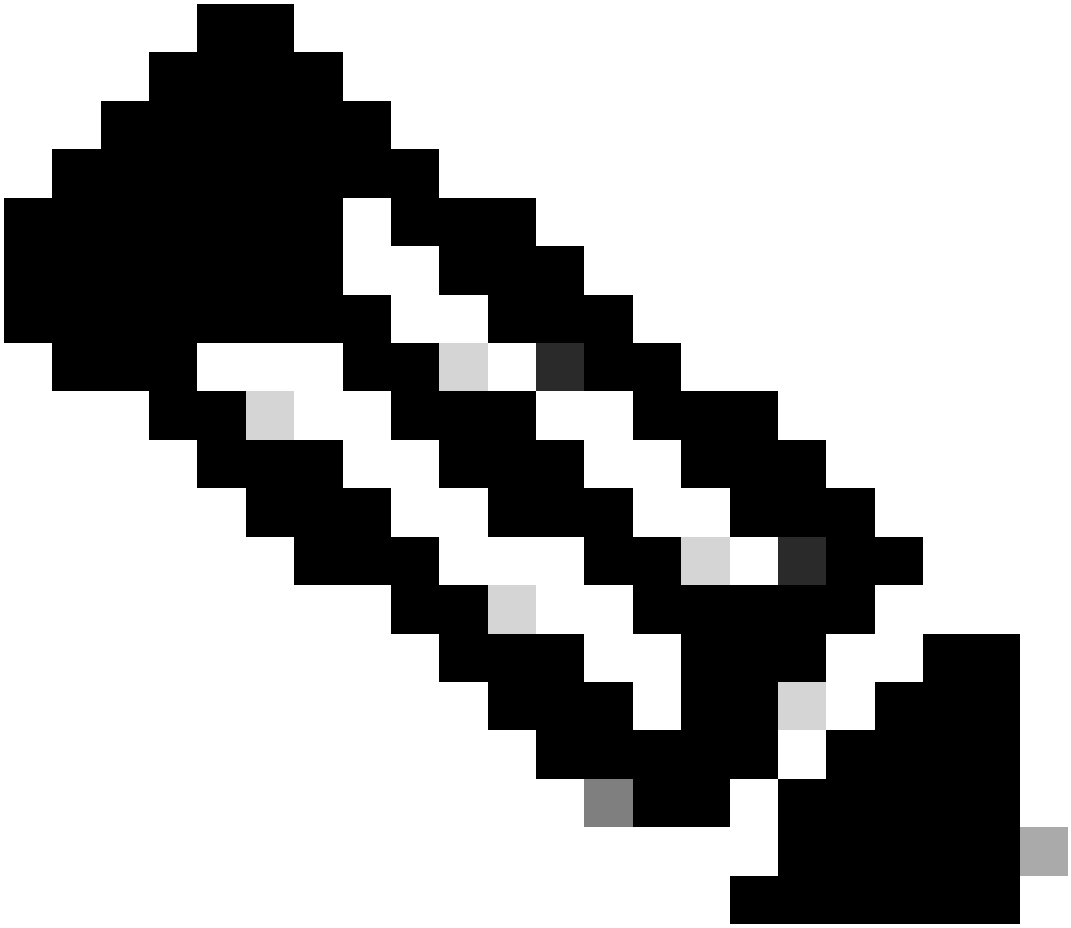


第1步ECMP区域3

接口outside1和outside2均已成功添加到ECMP区域outside。



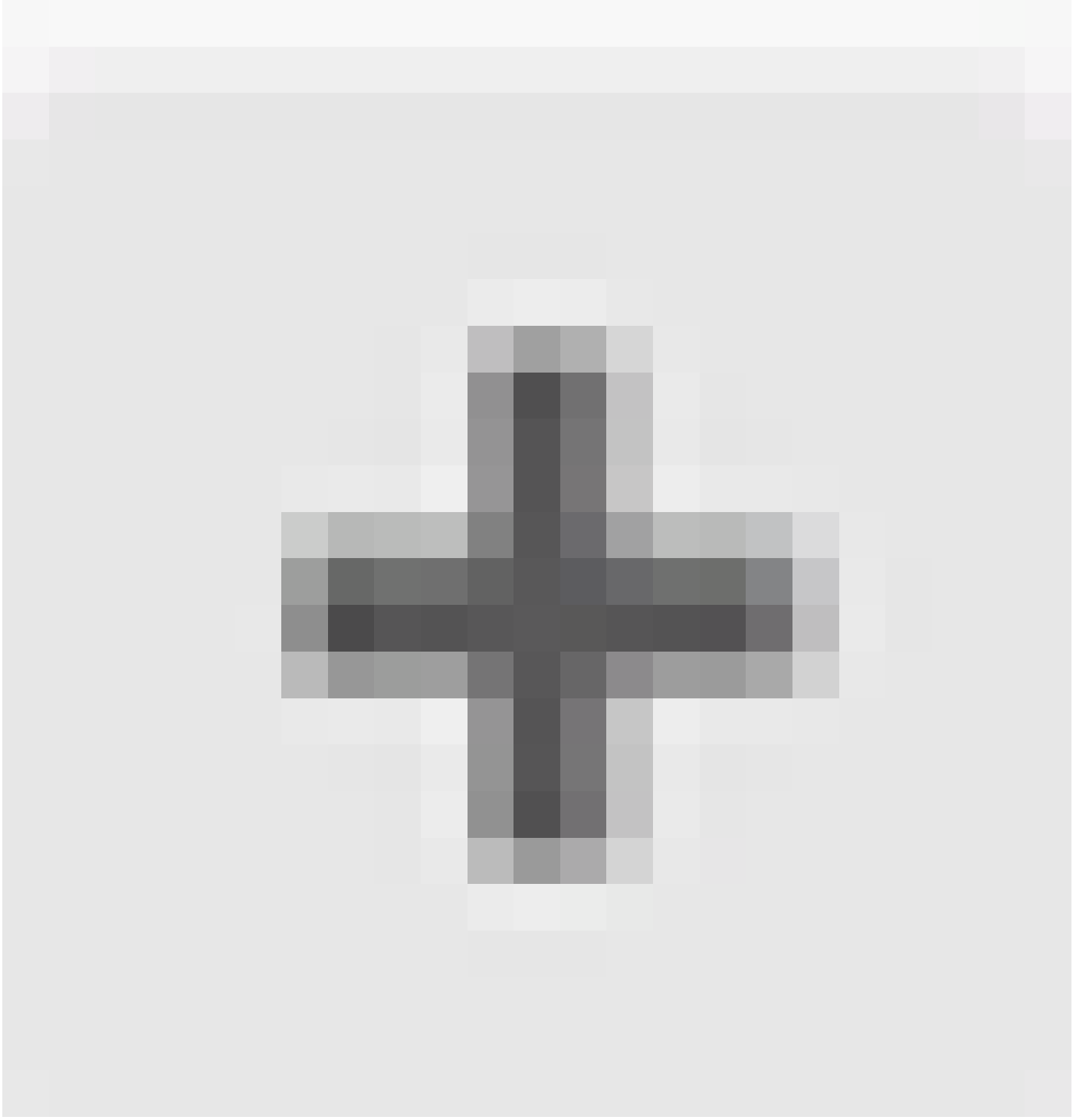
第1步ECMP Zone4



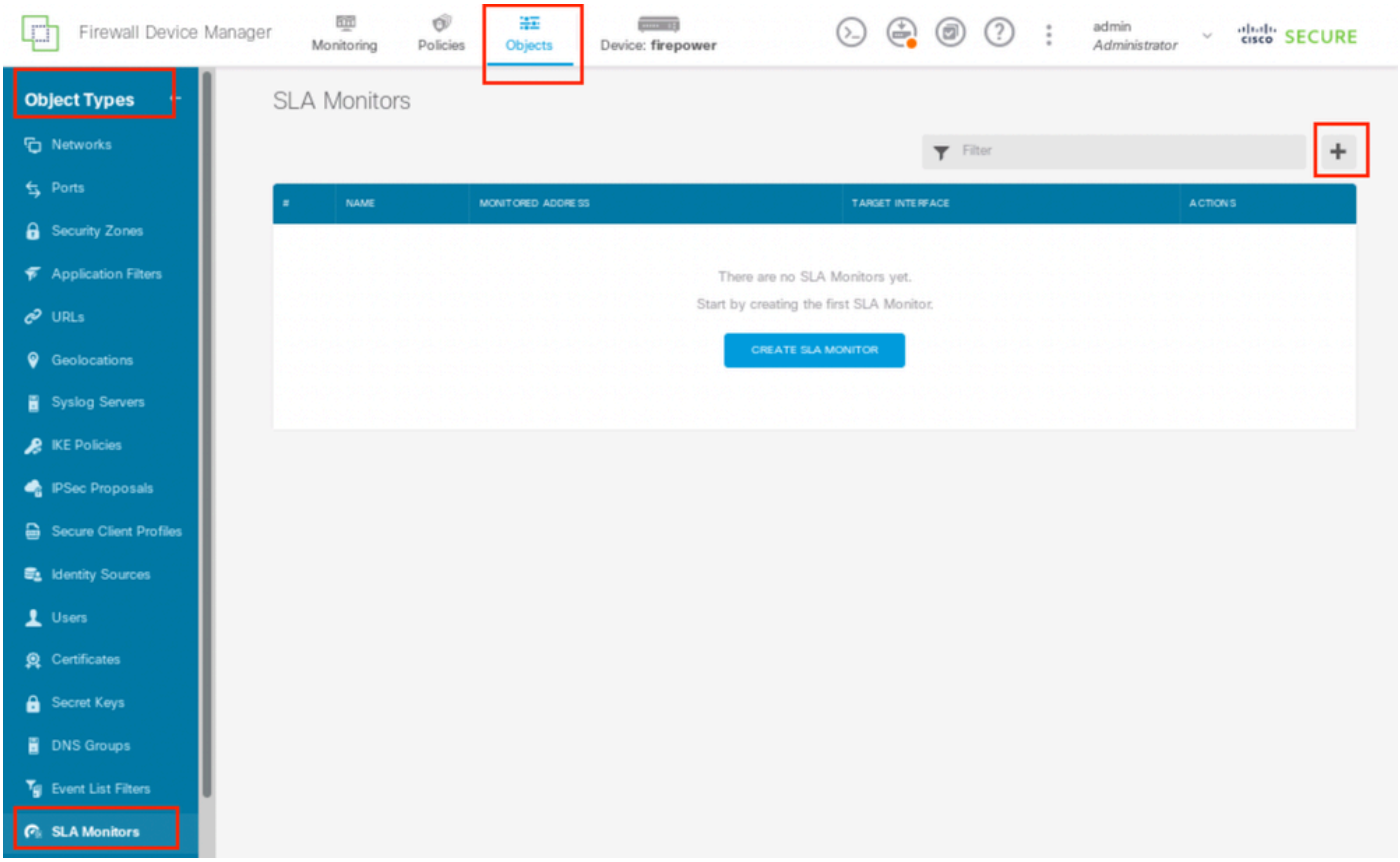
注意：ECMP路由流量区域与安全区域无关。创建包含outside1和outside2接口的安全区域不会为ECMP路由实现流量区域。

第二步：配置IP SLA对象

要定义用于监控到每个网关连接的SLA对象，请导航到对象>对象类型> SLA监控器，点击添加图标(



)为第一个ISP连接添加新的SLA监控器。



第2步IP SLA1

在Add SLA Monitor Object 窗口中：

1. 为SLA监控器对象设置Name，也可以设置说明(本例中为sla-outside1)。
2. 设置Monitor Address，在本例中为gw-outside1（第一个ISP网关）。
3. 设置用于到达监控器地址的目标接口，在本例中为outside1。
4. 此外，还可以调整超时和阈值。Click OK.

Add SLA Monitor Object

Name

sla-outside1

Description

Monitor Address

gw-outside1

Target Interface

outside1 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000 milliseconds

0 - 2147483647

Timeout

5000 milliseconds

0 - 604800000

Frequency

60000 milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

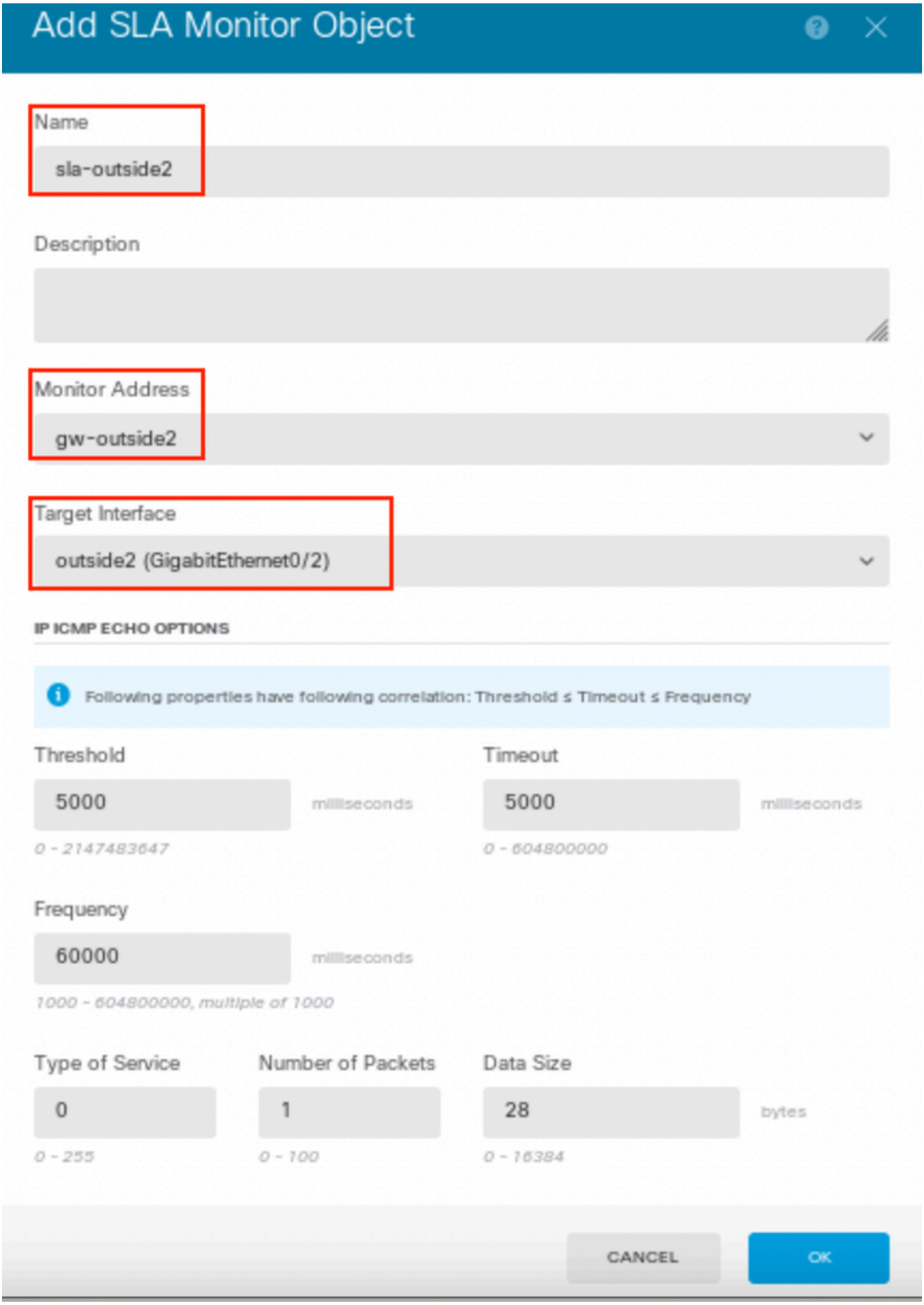
28 bytes

0 - 16384

CANCEL OK

重复类似步骤，在Add SLA Monitor Object 窗口中为第二个ISP连接配置另一个SLA Monitor对象：

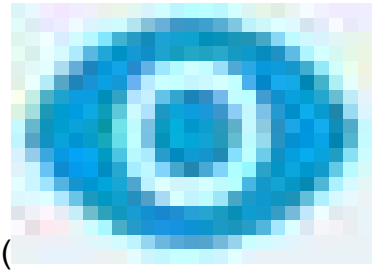
1. 为SLA监控器对象设置Name，也可以设置说明(本例中为sla-outside2)。
2. 设置Monitor Address，在本例中为gw-outside2（第二个ISP网关）。
3. 设置可到达监控器地址的目标接口，此例中为outside2。
4. 此外，还可以调整超时和阈值。Click OK.


Add SLA Monitor Object
Name
sla-outside2
Description
Monitor Address
gw-outside2
Target Interface
outside2 (GigabitEthernet0/2)
IP ICMP ECHO OPTIONS
Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency
Threshold
5000
milliseconds
0 - 2147483647
Timeout
5000
milliseconds
0 - 604800000
Frequency
60000
milliseconds
1000 - 604800000, multiple of 1000
Type of Service
0
0 - 255
Number of Packets
1
0 - 100
Data Size
28
bytes
0 - 16384
CANCEL
OK

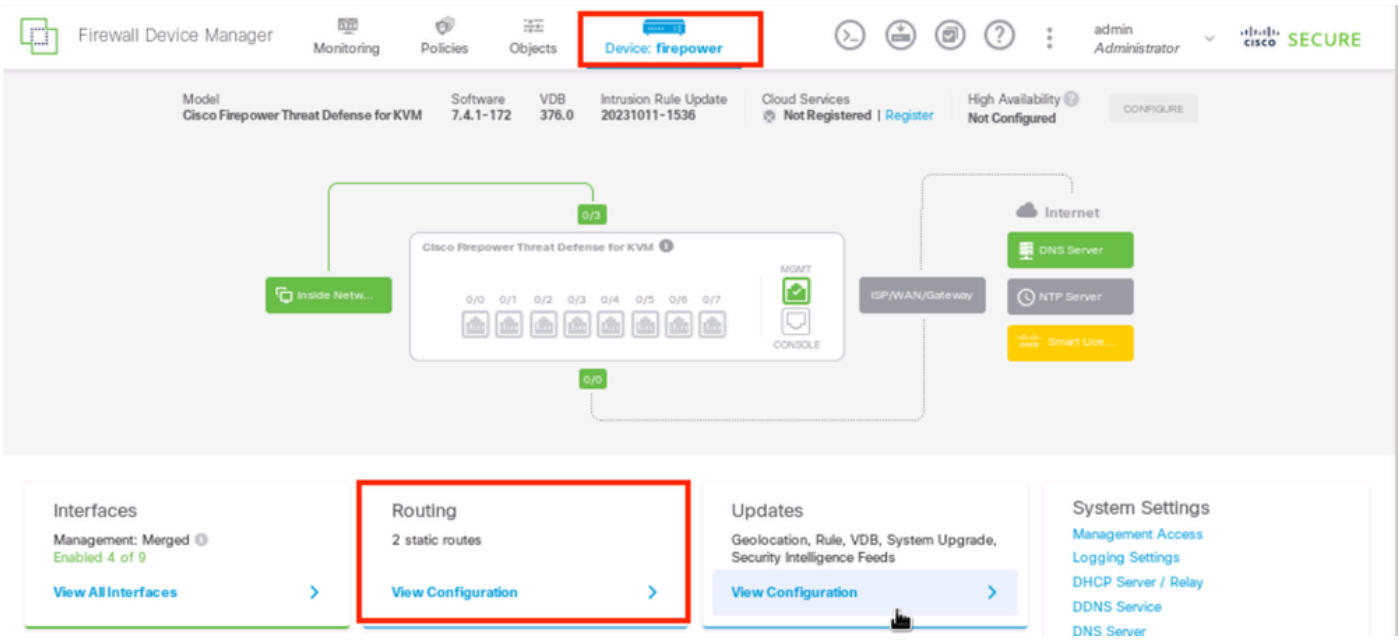
第2步IP SLA3

第三步：使用路由跟踪配置静态路由

导航到设备，然后点击路由摘要中的链接。

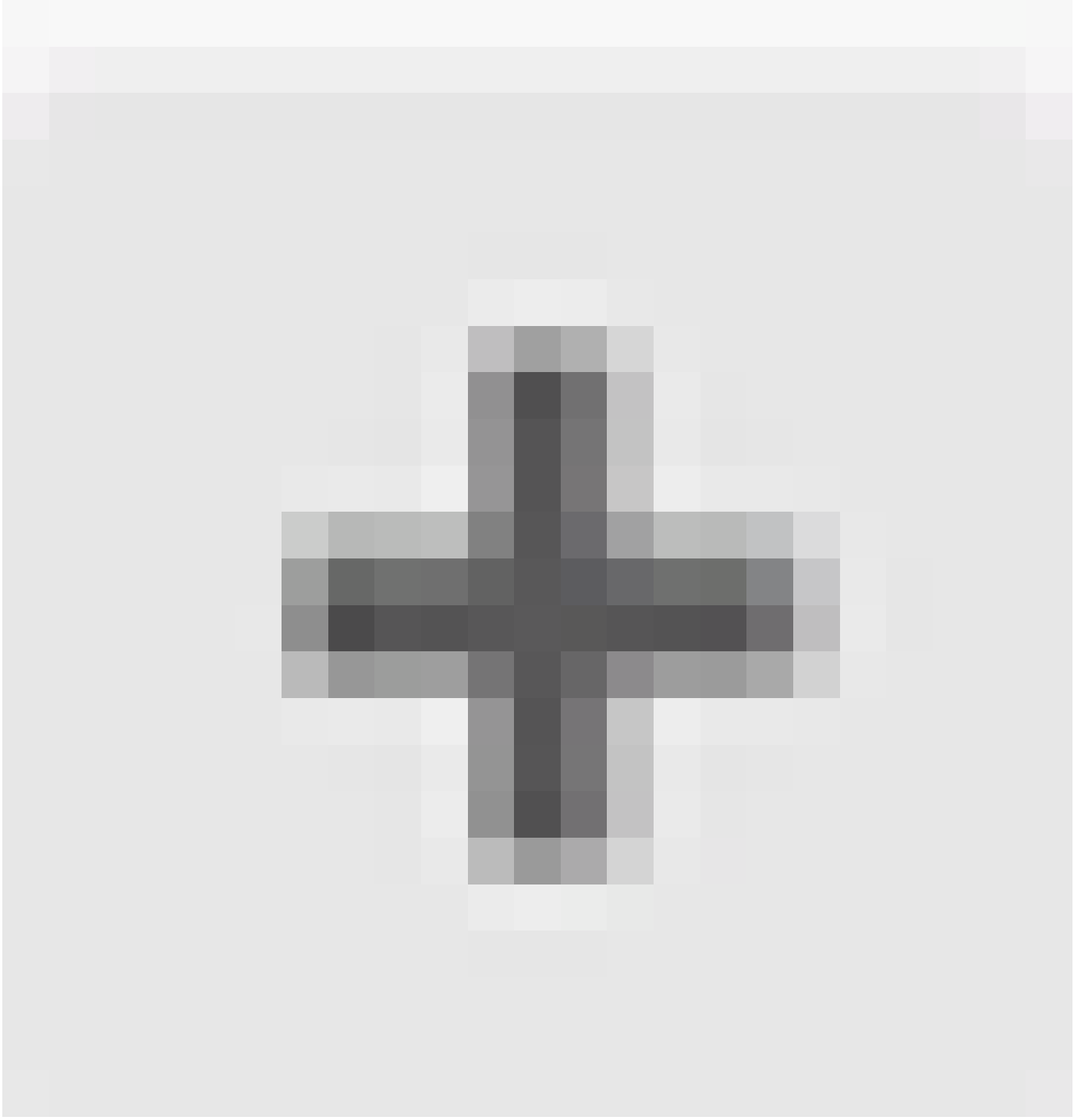


如果启用了虚拟路由器，请点击在其中配置静态路由的路由器的查看图标( )。在这种情况下，虚拟路由器未启用。



第3步Route1

在静态路由页面上，点击添加图标(

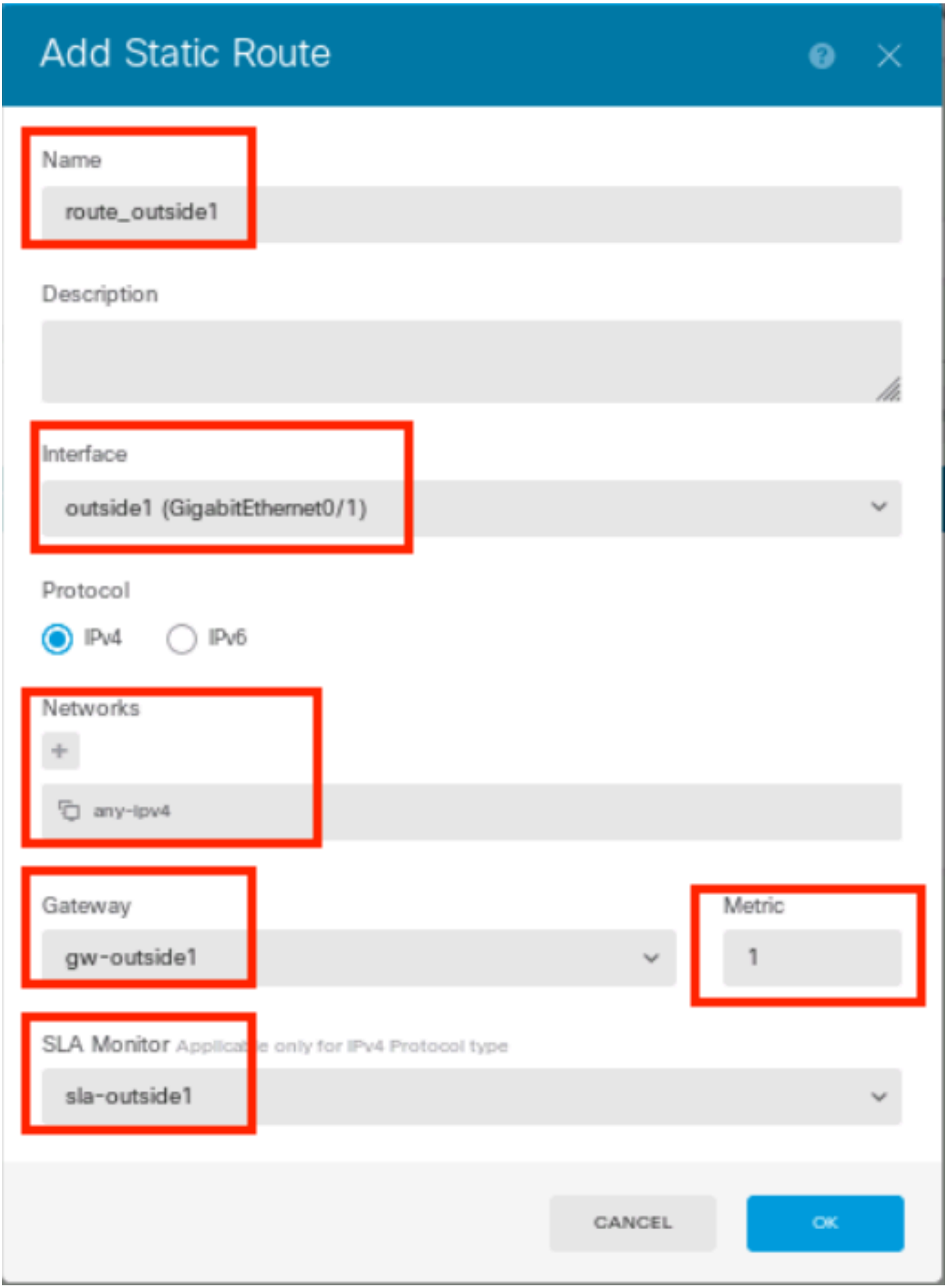


)为第一个ISP链路添加新静态路由。

在Add Static Route 窗口中：

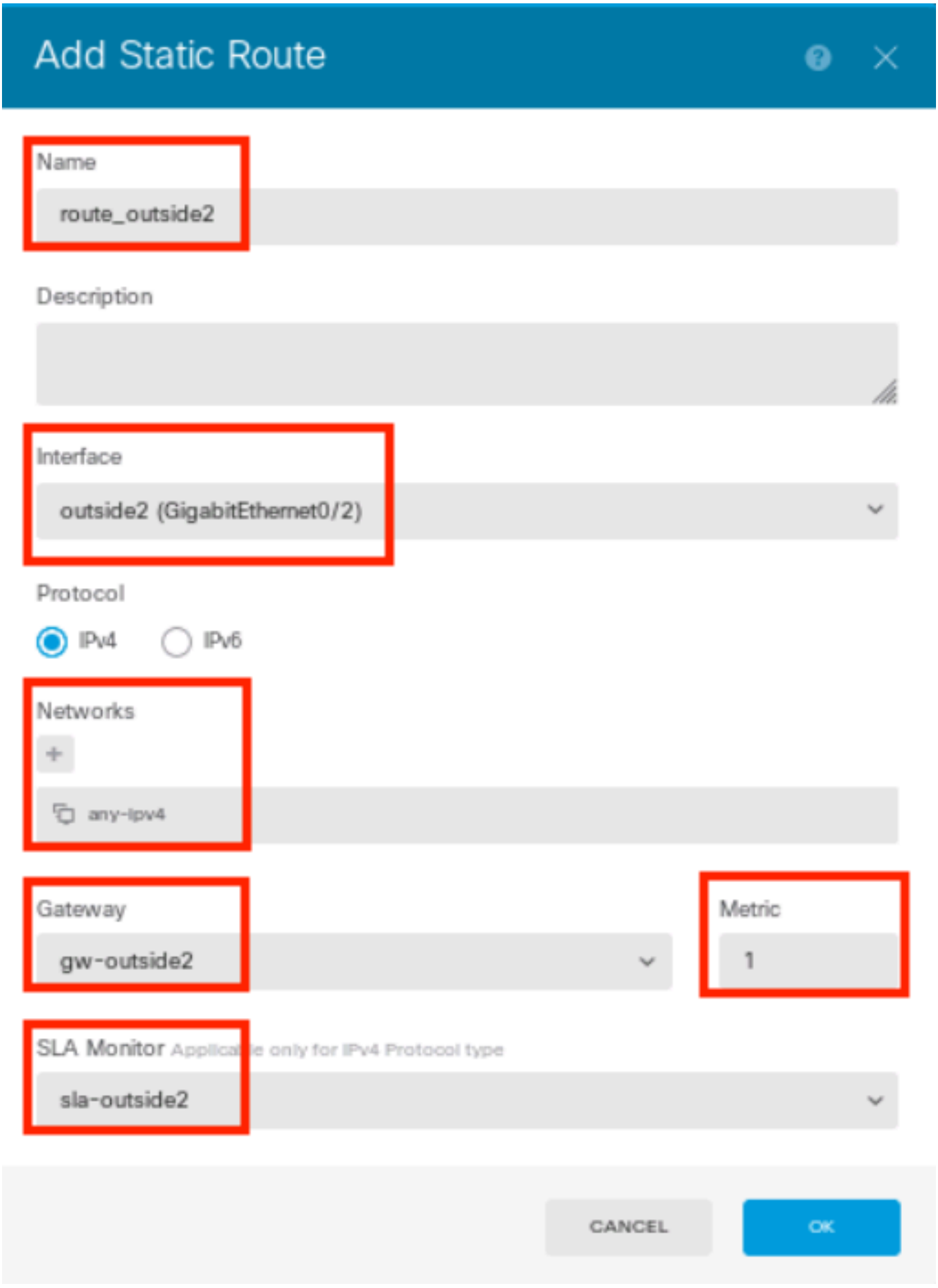
1. 设置路由的名称和说明（可选）。在本示例中，route_outside1。
2. 从Interface 下拉列表中，选择要通过其发送流量的接口，网关地址需要通过该接口可访问。在本示例中，outside1 (GigabitEthernet0/1)。
3. 选择Networks 以标识使用此路由中网关的目标网络或主机。在本示例中，预定义any-ipv4。
4. 从Gateway 下拉列表中，选择用于识别网关IP地址的网络对象，Traffic is sent to this address。在本示例中，gw-outside1（第一个ISP网关）。
5. 设置路由的Metric，介于1和254之间。在本示例1中。
6. 从SLA Monitor下拉列表中选择SLA监控器对象。在本例中，sla-outside1。

7. Click OK.


Add Static Route
Name
route_outside1
Description
Interface
outside1 (GigabitEthernet0/1)
Protocol
IPv4
IPv6
Networks
any-ipv4
Gateway
gw-outside1
Metric
1
SLA Monitor
sla-outside1
CANCEL
OK

在Add Static Route 窗口中重复类似步骤，为第二个ISP连接配置另一个静态路由：

1. 设置路由的名称和说明（可选）。在本示例中，route_outside2。
2. 从Interface 下拉列表中，选择要通过其发送流量的接口，网关地址需要通过该接口可访问。在本示例中，outside2 (GigabitEthernet0/2)。
3. 选择Networks 以标识使用此路由中网关的目标网络或主机。在本示例中，预定义any-ipv4。
4. 从Gateway 下拉列表中，选择识别网关IP地址的网络对象，流量将发送到此地址。 在本示例中，gw-outside2（第二个ISP网关）。
5. 设置路由的Metric，介于1和254之间。在本示例1中。
6. 从SLA Monitor下拉列表中选择SLA监控器对象。在本场景中，为sla-outside2。
7. Click OK.


Add Static Route
Name
route_outside2
Description
Interface
outside2 (GigabitEthernet0/2)
Protocol
IPv4
IPv6
Networks
any-ipv4
Gateway
gw-outside2
Metric
1
SLA Monitor
sla-outside2
CANCEL
OK

第3步Route3

您有2条通过具有路由路径的outside1和outside2接口的路由。

第3步Route4

将更改部署到FTD。

验证

登录FTD的CLI，运行命令 show zone 以检查有关ECMP流量区域的信息，包括作为每个区域一部分的接口。

<#root>

> show zone
Zone:

Outside

ecmp
Security-level: 0

Zone member(s): 2

outside2 GigabitEthernet0/2

outside1 GigabitEthernet0/1

运行 show running-config route 命令检查正在运行的路由配置是否正确，在这种情况下，有两条带路由跟踪的静态路由。

<#root>

> show running-config route

route outside1 0.0.0.0 0.0.0.0 10.1.1.2 1 track 1

route outside2 0.0.0.0 0.0.0.0 10.1.2.2 1 track 2

运行 show route 命令检查路由表，如果有两个默认路由是通过接口outside1和outside2以等价方式路由，数据流可以在两个ISP电路之间分配。

<#root>

> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

[1/0] via 10.1.1.2, outside1

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

运行命令 show sla monitor configuration 以检查SLA监控器的配置。

<#root>

> show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 1037119999
Owner:
Tag:

Type of operation to perform: echo

Target address: 10.1.1.2

Interface: outside1

Number of packets: 1

```
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 1631063762
Owner:
Tag:

Type of operation to perform: echo


Target address: 10.1.2.2


Interface: outside2


Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

运行命令 show sla monitor operational-state 以确认SLA监控器的状态。在这种情况下，您可以在命令输出中找到“Timeout occurred：FALSE”，它表示发往网关的ICMP回应正在应答，因此通过目标接口的默认路由处于活动状态并已安装在路由表中。

<#root>

```
> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE
```

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 05:32:32.791 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 1631063762
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 79
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
```

Timeout occurred: FALSE

```
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 05:32:32.791 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

负载平衡

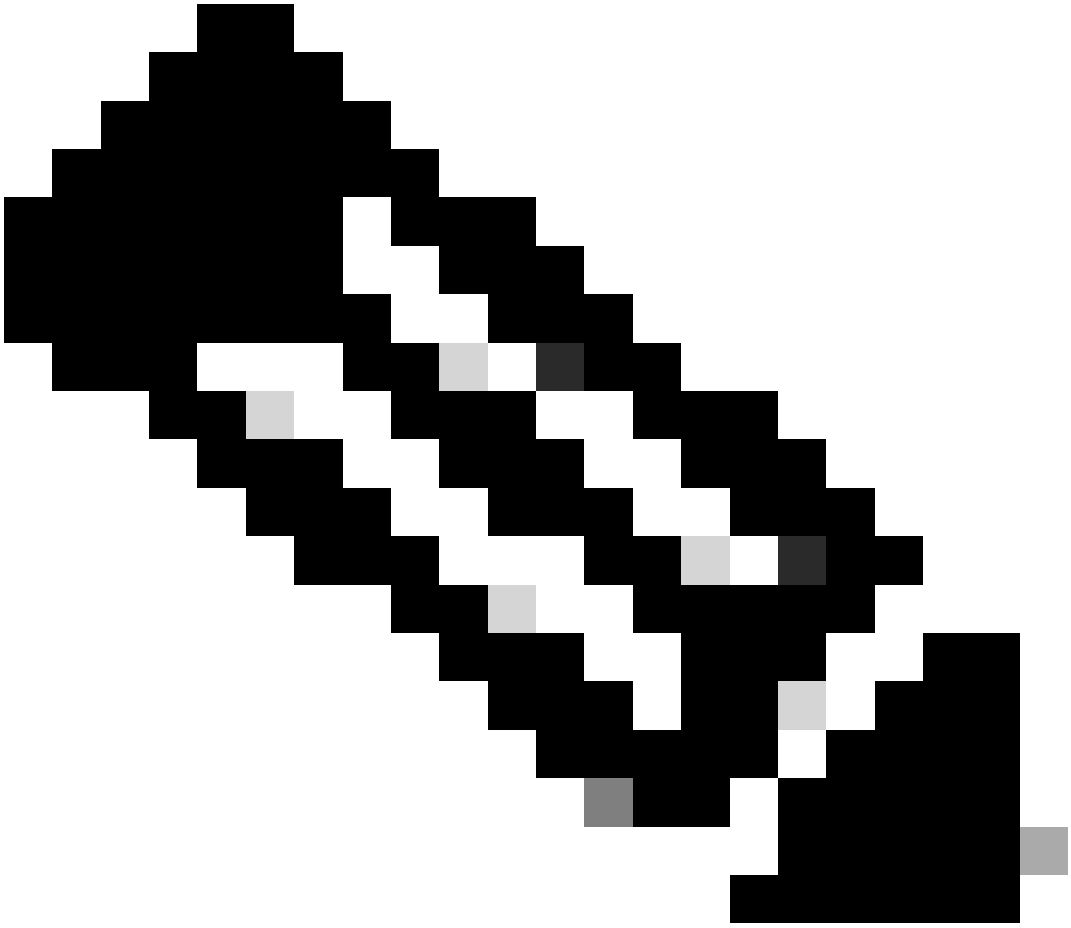
通过FTD的初始流量，用于检验ECMP是否在ECMP区域中的网关之间对流量进行负载均衡。在这种情况下，从Test-PC-1 (10.1.3.2)和Test-PC-2 (10.1.3.4)到Internet主机(10.1.5.2)启动SSH连接，运行 show conn 命令确认流量在两个ISP链路之间实现负载均衡，Test-PC-1 (10.1.3.2)通过interface outside1，Test-PC-2 (10.1.3.4)通过interface outside2。

<#root>

> show conn
4 in use, 14 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:02:10, bytes 5276, flags UIO N1

TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:00:04, bytes 5276, flags UIO N1



注：根据散列源和目标IP地址、传入接口、协议、源和目标端口的算法，在指定网关之间对流量进行负载均衡。运行测试时，由于使用散列算法，可以模拟的流量路由到同一网关，这是预期的，更改6个元组（源IP、目标IP、传入接口、协议、源端口、目标端口）中的任何值，以更改散列结果。

丢失的路由

在这种情况下，如果通向第一个ISP网关的链路关闭，请关闭第一个网关路由器进行模拟。 如果FTD在SLA监控器对象中指定的阈值计时器内没有收到来自第一个ISP网关的回应应答，则认为主机无法访问，并标记为关闭。通向第一个网关的跟踪路由也会从路由表中删除。

运行命令 show sla monitor operational-state 以确认SLA监控器的当前状态。在这种情况下，您可以在命令输出中找到“Timeout occurred： True”，这表示发往第一个ISP网关的ICMP回应没有响应。

<#root>

> show sla monitor operational-state
Entry number: 1037119999
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 121
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: TRUE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 06:14:32.801 UTC Tue Jan 30 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 1631063762
Modification time: 04:14:32.771 UTC Tue Jan 30 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 121
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE

Timeout occurred: FALSE

Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 06:14:32.802 UTC Tue Jan 30 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

运行 **show route** 命令以检查当前路由表，通过接口outside1到第一个ISP网关的路由被删除，通过接口outside2到第二个ISP网关只有一个活动默认路由。

<#root>

> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

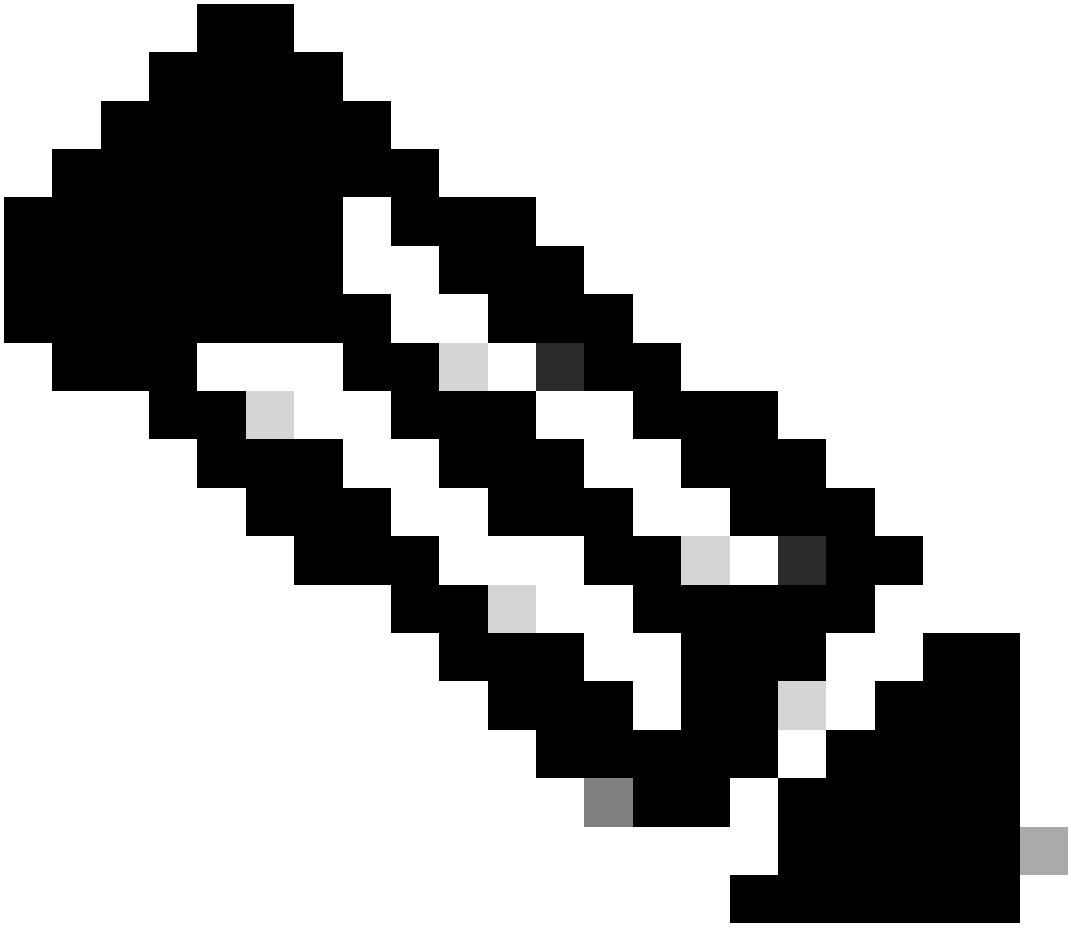
运行命令 show conn（PIM稀疏或PIM密集模式），您会发现两个连接仍为up状态。SSH会话在Test-PC-1 (10.1.3.2)和Test-PC-2 (10.1.3.4)上也处于活动状态，不会出现任何中断。

<#root>

> show conn
4 in use, 14 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 12 most enabled, 0 most in effect

TCP inside 10.1.3.4:41652 outside2 10.1.5.2:22, idle 0:19:29, bytes 5276, flags UIO N1

TCP inside 10.1.3.2:57484 outside1 10.1.5.2:22, idle 0:17:22, bytes 5276, flags UIO N1



注意：在show conn的输出中，您会注意到，虽然通过接口outside1的默认路由已从路由表中删除，但来自Test-PC-1 (10.1.3.2)的SSH会话仍通过接口outside1。这是预期的，而且根据设计，实际流量流经接口outside2。如果从Test-PC-1 (10.1.3.2)到Internet主机(10.1.5.2)发起新连接，则可以发现所有流量都通过接口outside2。

故障排除

要验证路由表更改，请运行命令 debug ip routing。

在本例中，当通向第一个ISP网关的链路断开时，通过接口outside1的路由将从路由表中删除。

<#root>

> debug ip routing
IP routing debugging is on

RT:

ip_route_delete 0.0.0.0 0.0.0.0 via 10.1.1.2, outside1

ha_cluster_synced 0 routetype 0

RT: del 0.0.0.0 via 10.1.1.2, static metric [1/0]NP-route: Delete-Output 0.0.0.0/0 hop_count:1 , via 0.0

RT(mgmt-only):

NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, outside2

NP-route: Update-Input 0.0.0.0/0 hop_count:1 Distance:1 Flags:0X0 , via 10.1.2.2, outside2

运行 show route 命令以确认当前路由表。

<#root>

> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2

C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

当通向第一个ISP网关的链路重新接通时，通过接口outside1的路由将添加回路由表。

<#root>

> debug ip routing
IP routing debugging is on

RT(mgmt-only):

NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.2.2, outside2

NP-route: Update-Output 0.0.0.0/0 hop_count:1 , via 10.1.1.2, outside2

NP-route: Update-Input 0.0.0.0/0 hop_count:2 Distance:1 Flags:0X0 , via 10.1.2.2, outside2
via 10.1.1.2, outside1

运行 show route 命令以确认当前路由表。

> 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 10.1.2.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.1.2.2, outside2
[1/0] via 10.1.1.2, outside1
C 10.1.1.0 255.255.255.0 is directly connected, outside1
L 10.1.1.1 255.255.255.255 is directly connected, outside1
C 10.1.2.0 255.255.255.0 is directly connected, outside2
L 10.1.2.1 255.255.255.255 is directly connected, outside2
C 10.1.3.0 255.255.255.0 is directly connected, inside
L 10.1.3.1 255.255.255.255 is directly connected, inside

相关信息

- 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）。