在FMC管理的FTD上使用IP SLA配置ECMP

目录

简介

先决条件

- 要求
- 使用的组件
- 背景信息

配置

- 网络图
- 配置
  - 步骤0.预配置接口/网络对象
  - 步骤1.配置ECMP区域
  - 步骤2.配置IP SLA对象
  - 步骤3.使用路由跟踪配置静态路由

验证

- 负载平衡
- 丢失的路由

故障排除

简介

本文档介绍如何在FMC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
- Cisco Secure Firewall Management Center (FMC)

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
- 思科FMC版本7.4.1

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 FMC管理的Cisco FTD上配置等价多路径(ECMP)和Internet协议服务级别协议(IP SLA)。ECMP允许您在FTD上将接口分组在一起，并跨多个接口对流量进行负载均衡。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。IP SLA可以与ECMP一起实施，以确保下一跳的可用性。在本示例中，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会跟踪连接情况，确保在发生故障时无缝转换到任何可用电路。

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

- Cisco Secure Firewall Management Center 7.1或更高版本

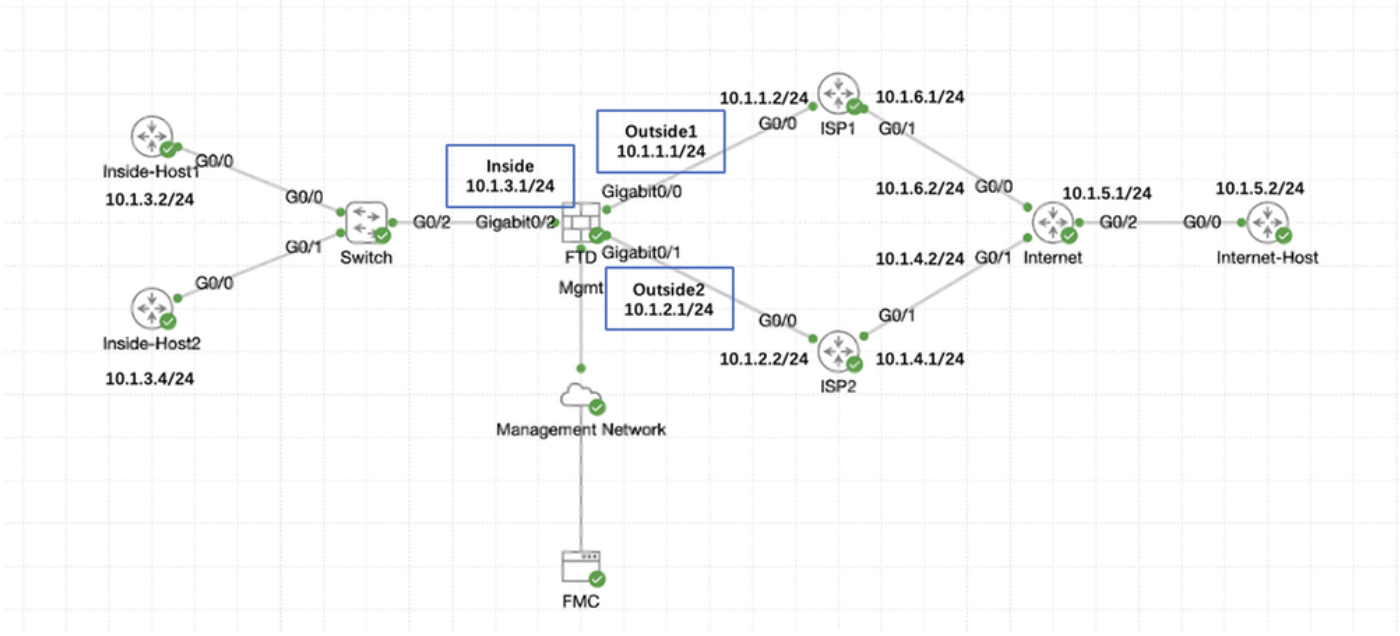
配置

网络图

在本示例中，Cisco FTD有两个外部接口：outside1和outside2。每个连接至ISP网关，outside1和outside2属于名为outside的相同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。如果任一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。

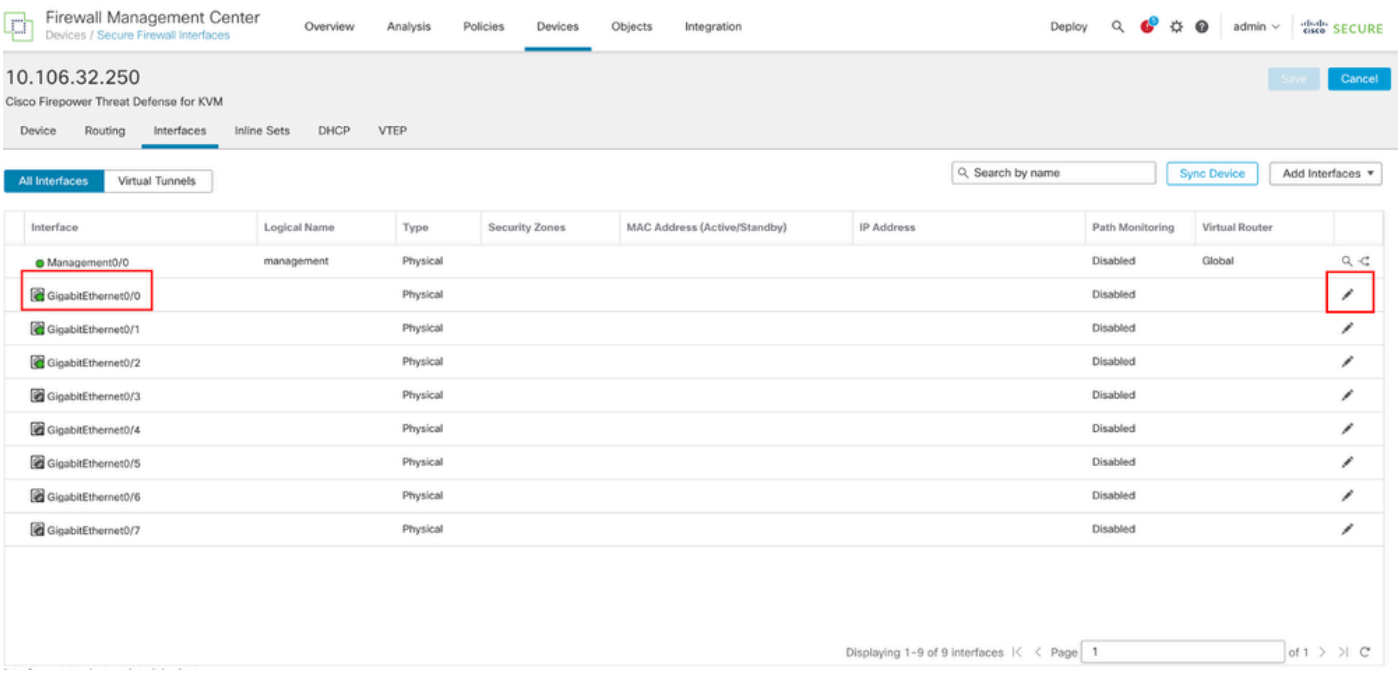


网络图

配置

步骤0.预配置接口/网络对象

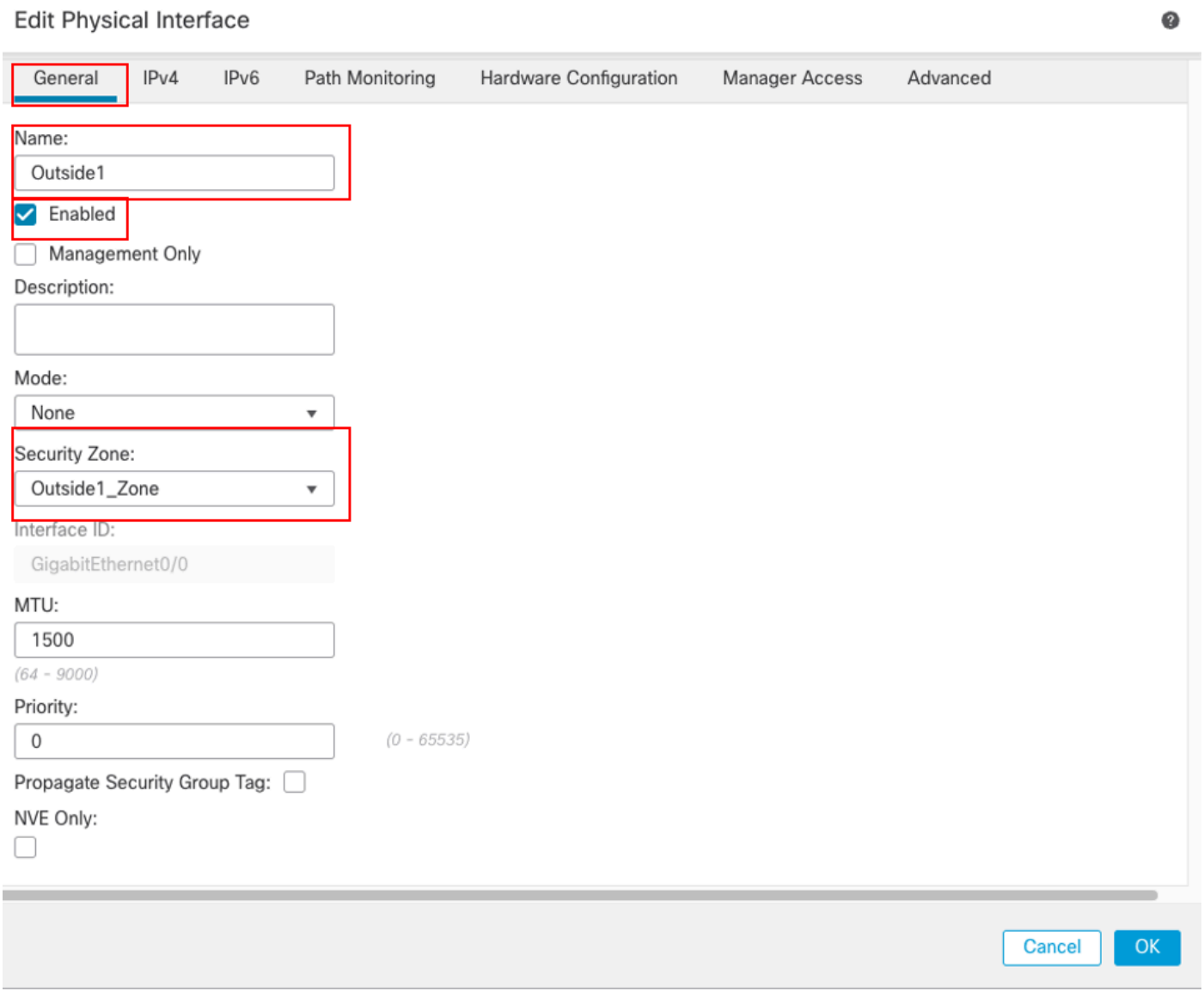
登录FMC Web GUI，选择Devices > Device Management，然后点击威胁防御设备的Edit按钮。默认情况下会选择Interfaces页面。单击要编辑的接口的Edit按钮，在本例中为GigabitEthernet0/0。



编辑接口Gi0/0

在Edit Physical Interface窗口的General选项卡下：

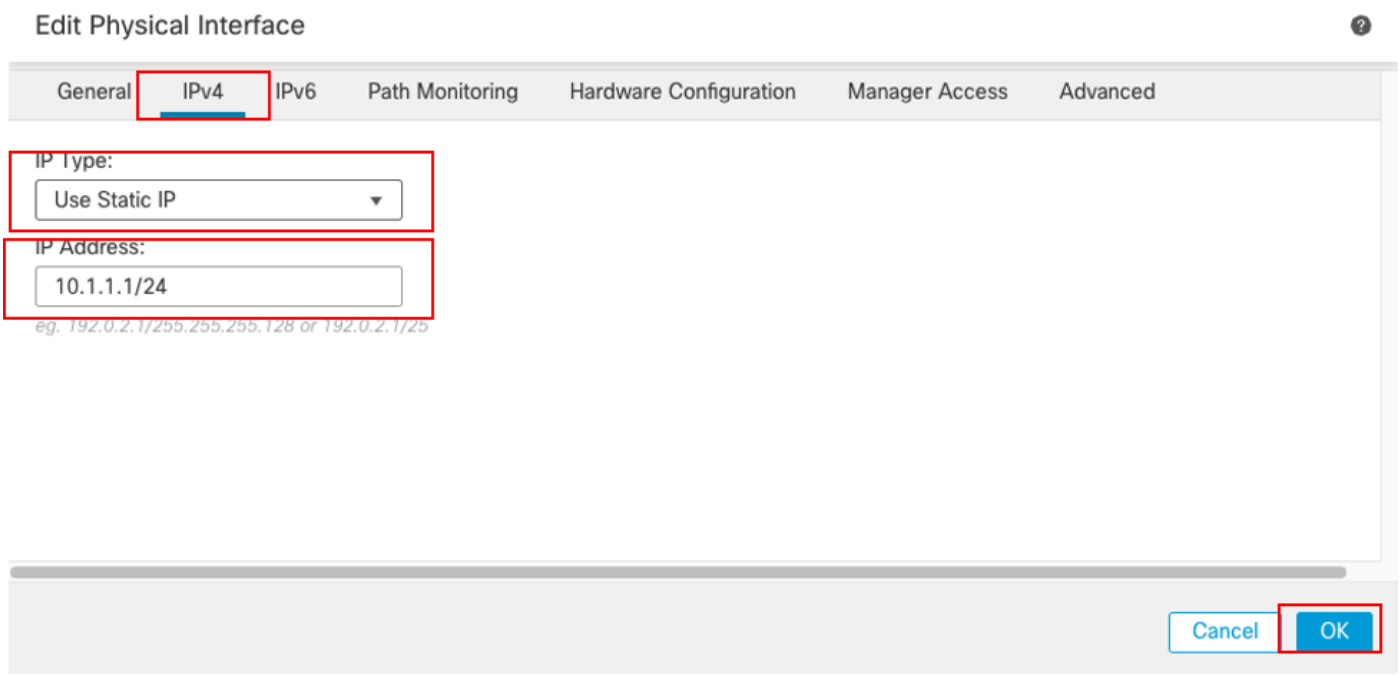
a. 设置Name，在本例中为Outside1。
b. 通过选中Enabled复选框启用接口。
c. 在Security Zone下拉列表中，选择现有安全区域或创建新安全区域，在本示例中为Outside1_Zone。



接口Gi0/0常规

在IPv4选项卡下：

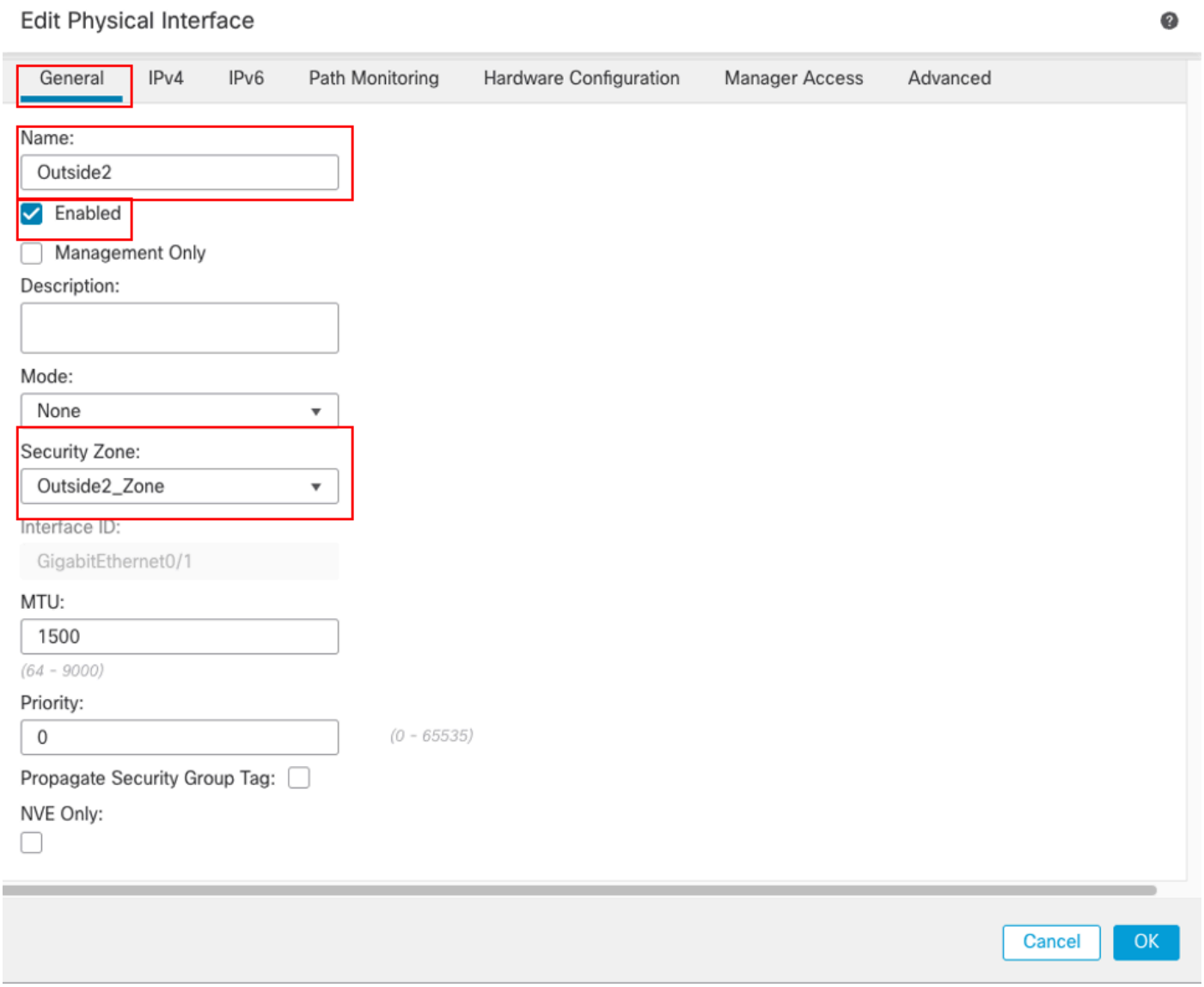
a. 从IP Type下拉列表中选择其中一个选项，在本示例中为Use Static IP。
b. 设置IP地址，在本例中为10.1.1.1/24。
c. Click OK.



接口Gi0/0 IPv4

在Edit Physical Interface窗口的General选项卡下，重复类似步骤配置接口GigabitEthernet0/1:

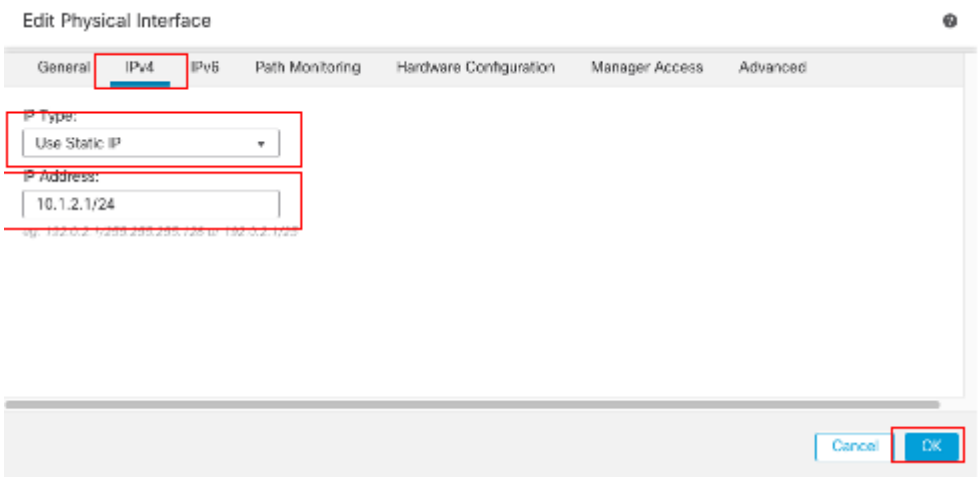
a. 设置Name，在本例中为Outside2。
b. 通过选中Enabled复选框启用接口。
c. 在Security Zone下拉列表中，选择现有安全区域或创建新安全区域，在本示例中为Outside2_Zone。



接口Gi0/1常规

在IPv4选项卡下：

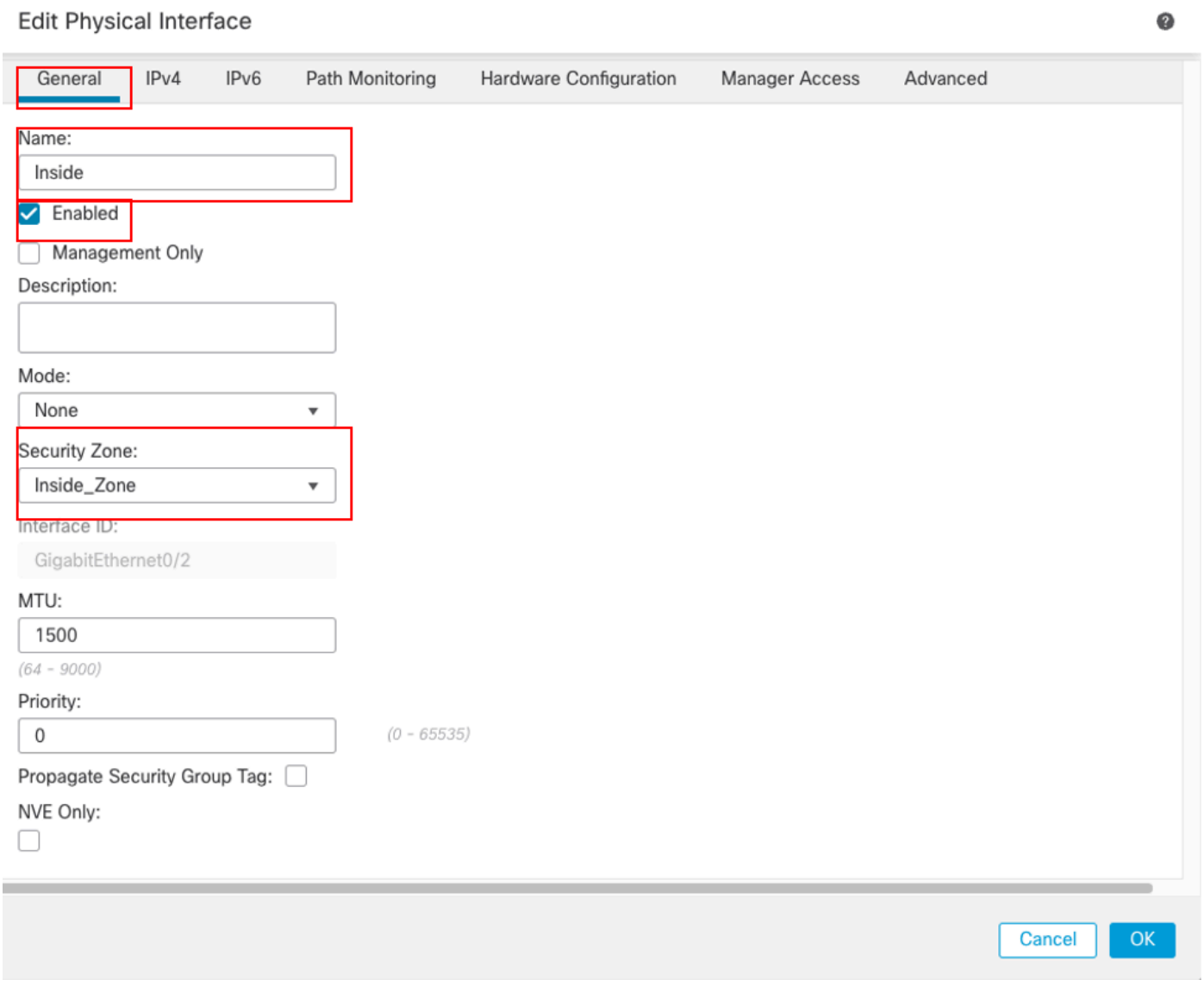
a. 从IP Type下拉列表中选择其中一个选项，在本示例中为Use Static IP。
b. 设置IP地址，在本例中为10.1.2.1/24。
c. Click OK.



接口Gi0/1 IPv4

在Edit Physical Interface窗口的General选项卡下，重复类似步骤配置接口GigabitEthernet0/2:

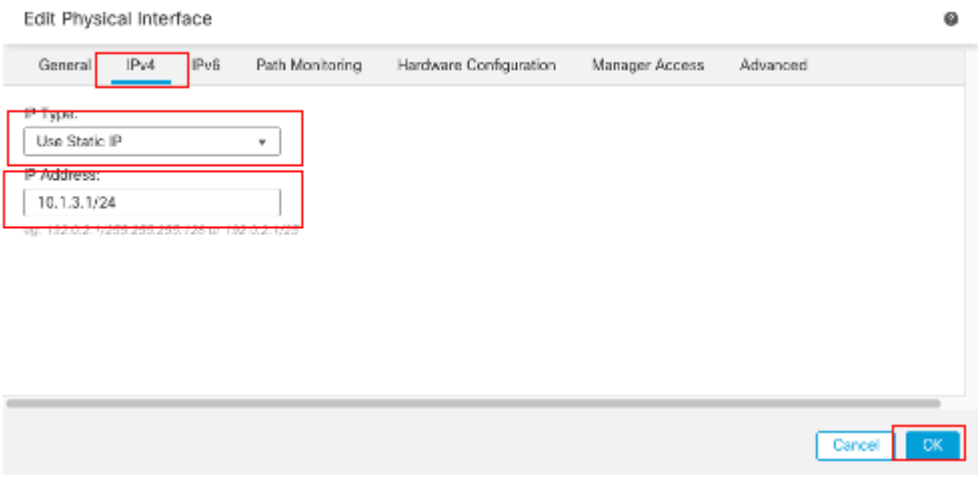
a. 设置Name，在本例中为Inside。
b. 通过选中Enabled复选框启用接口。
c. 在Security Zone下拉列表中，选择现有安全区域或创建新安全区域，在本示例中为Inside_Zone。



接口Gi0/2常规

在IPv4选项卡下：

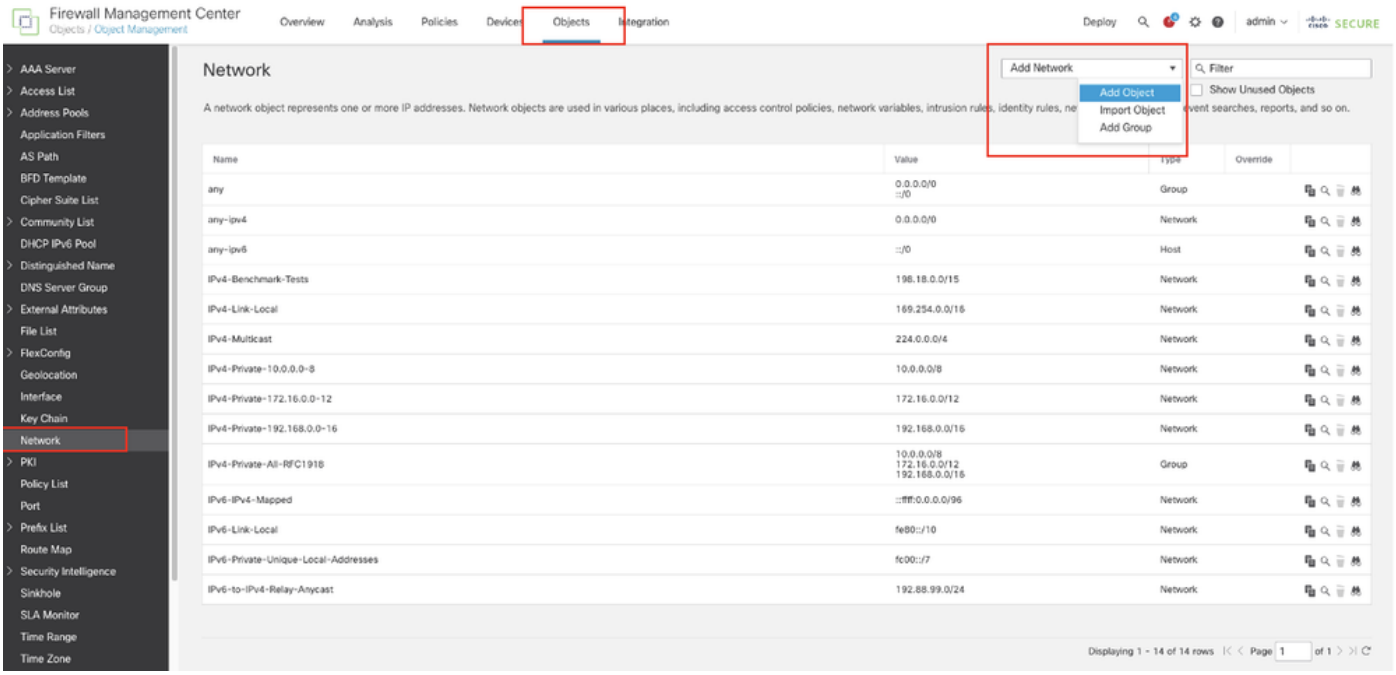
a. 从IP Type下拉列表中选择其中一个选项，在本示例中为Use Static IP。
b. 设置IP地址，在本例中为10.1.3.1/24。
c. Click OK.



接口Gi0/2 IPv4

单击Save和Deploy配置。

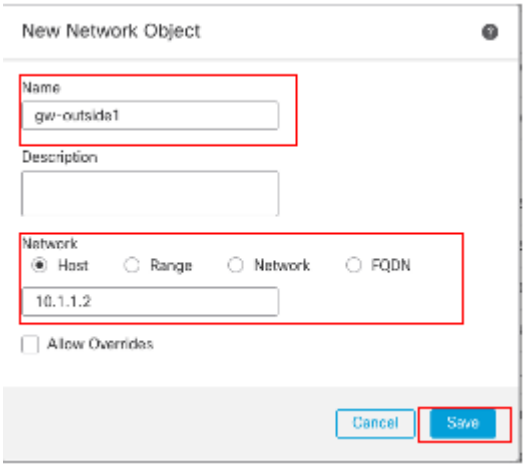
导航到Objects > Object Management，从对象类型列表中选择Network，从Add Network下拉菜单中选择Add Object，为第一个ISP网关创建对象。



网络对象

在New Network Object窗口中：

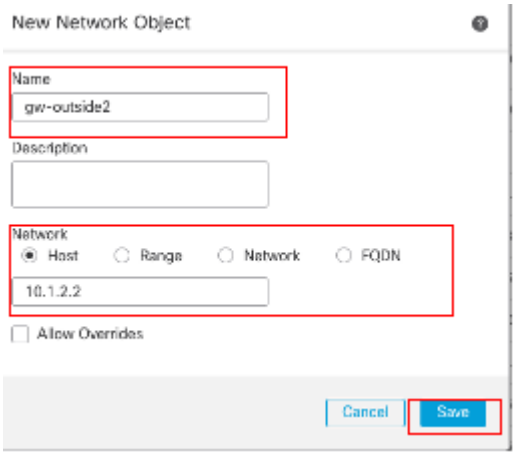
a. 设置Name，在本例中为gw-outside1。
b. 在Network字段中，选择所需的选项并输入适当的值，在本示例中为Host和10.1.1.2。
c. Click Save.



对象Gw-outside1

重复类似步骤，为第二个ISP网关创建另一个对象。在New Network Object窗口中：

a. 设置Name，在本例中为gw-outside2。
b. 在Network字段中，选择所需的选项并输入适当的值，在本示例中为Host和10.1.2.2。
c. Click Save.

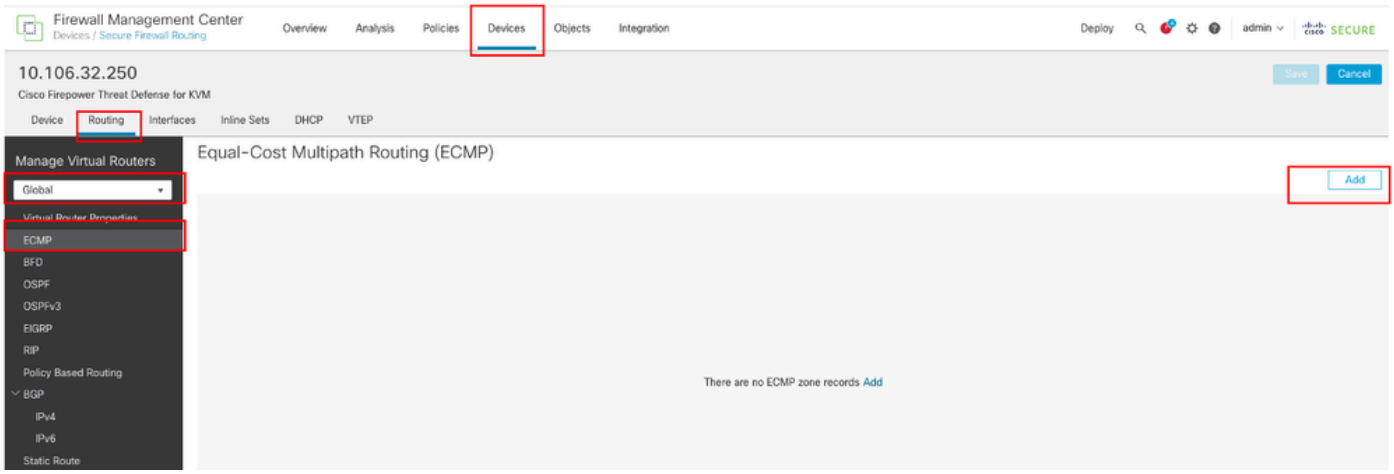


对象Gw-outside2

步骤1.配置ECMP区域

导航到设备 > 设备管理并编辑威胁防御设备，然后单击路由。从virtual router下拉列表中，选择要在其中创建ECMP区域的虚拟路由器。您可以在全局虚拟路由器和用户定义的虚拟路由器中创建ECMP区域。在本例中，选择Global。

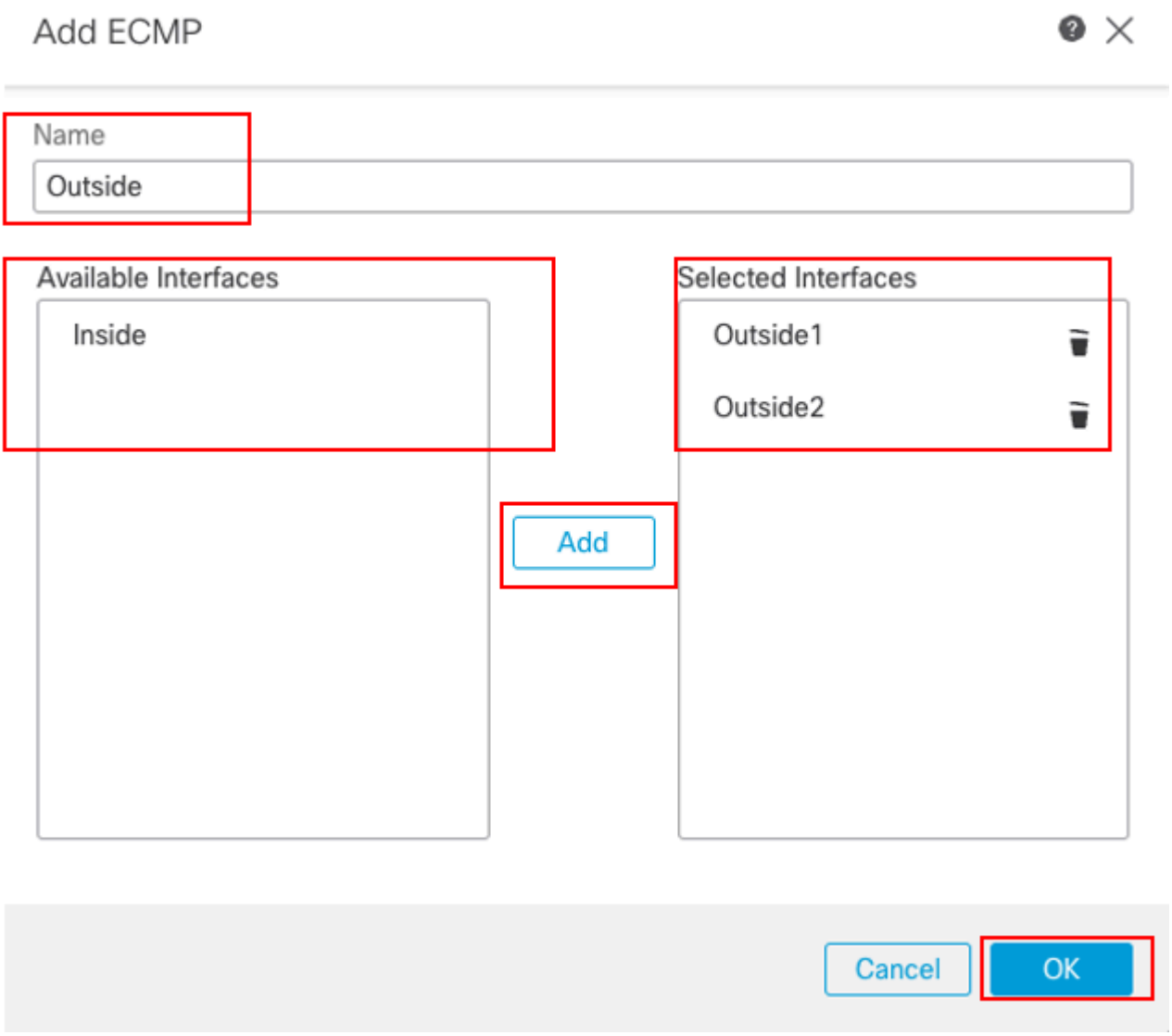
单击ECMP，然后单击Add。



配置ECMP区域

在Add ECMP窗口中：

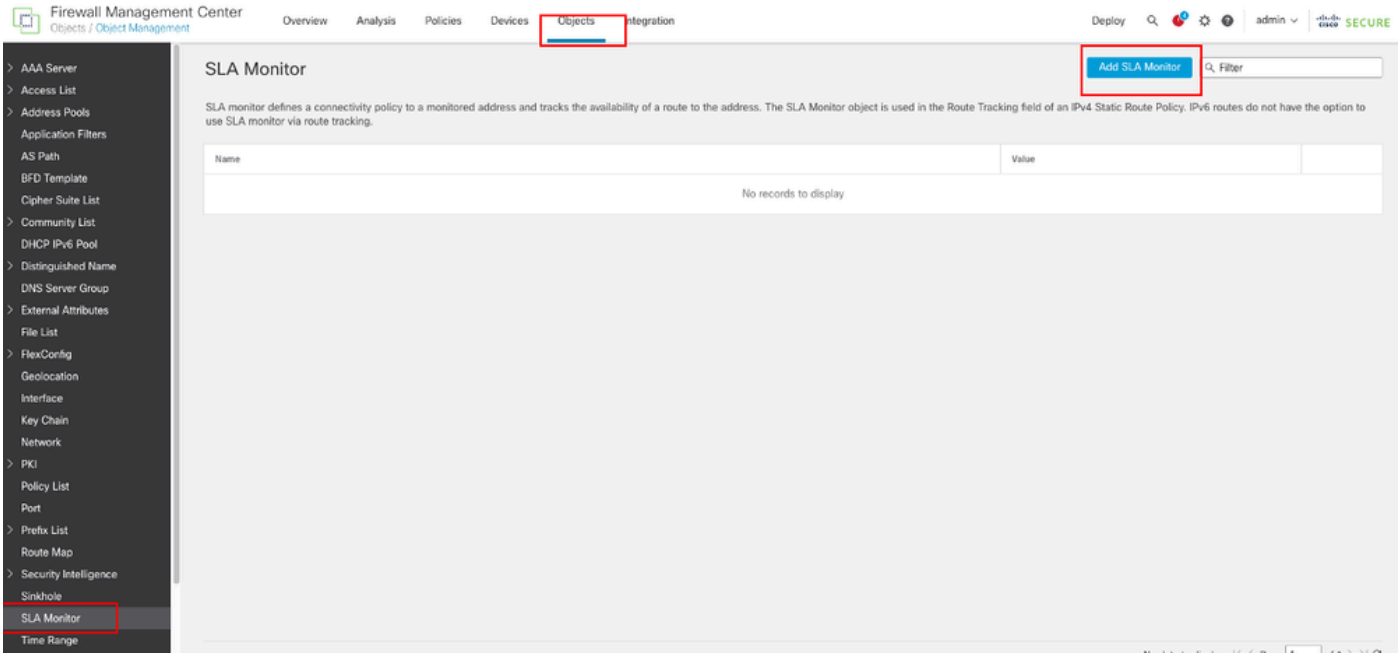
a. 为ECMP区域设置Name，在本示例中为Outside。
b. 要关联接口，请在Available Interfaces框下选择接口，然后单击Add。在本示例中Outside1和Outside2。
c. Click OK.



单击Save和Deploy配置。

步骤2.配置IP SLA对象

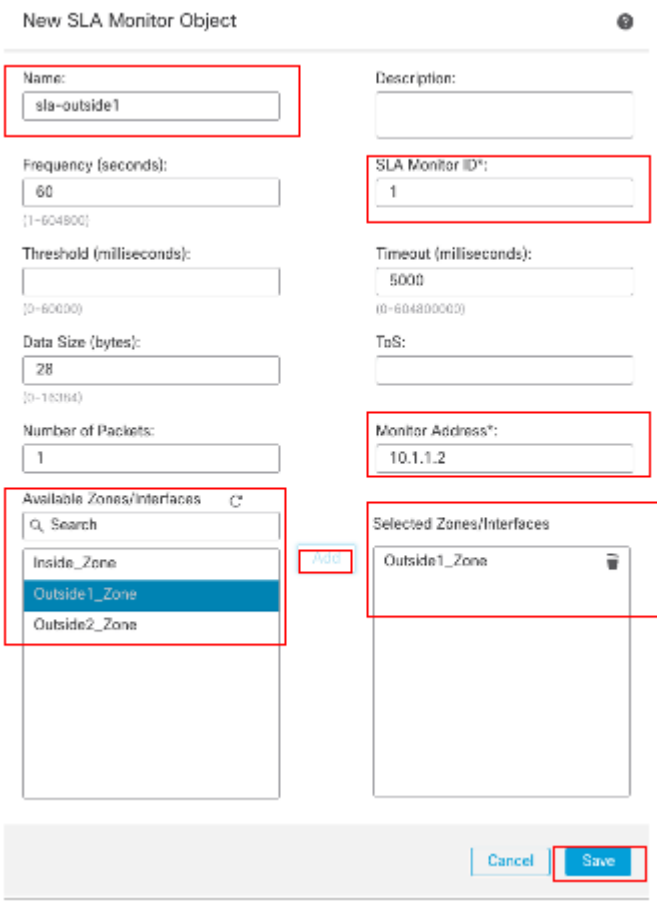
导航到Objects > Object Management，从对象类型列表中选择SLA Monitor，然后单击Add SLA Monitor为第一个ISP网关添加新的SLA监控器。



创建SLA监控器

在New SLA Monitor Object窗口中：

a. 为SLA监控器对象设置Name，在本例中为sla-outside1。
b. 在SLA Monitor ID字段中输入SLA操作的ID号。值范围为1至2147483647。您最多可在设备上创建2000个SLA操作。每个ID号对于策略和设备配置必须是唯一的。在本示例1中。
c. 在Monitored Address字段中输入由SLA操作监控的IP地址。在本例中为10.1.1.2。
d. Available Zones/Interfaces列表显示区域和接口组。在Zones/Interfaces列表中，添加包含设备通过哪些接口与管理站进行通信的区域或接口组。要指定单个接口，需要为该接口创建区域或接口组。在本示例中Outside1_Zone。
e. Click Save.

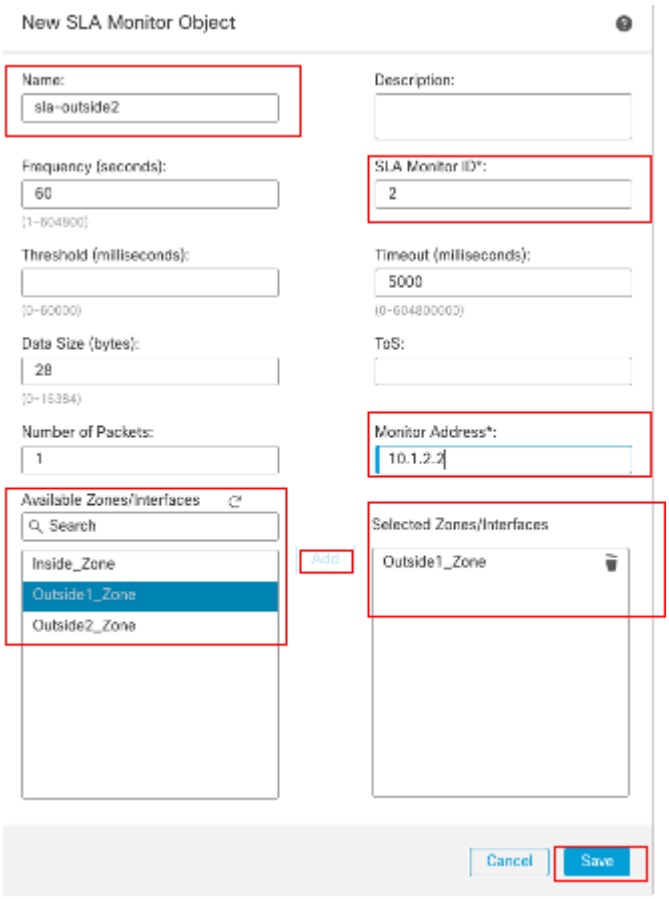


SLA对象Sla-outside1

重复类似步骤，为第二个ISP网关创建另一个SLA监控器。

在New SLA Monitor Object窗口中：

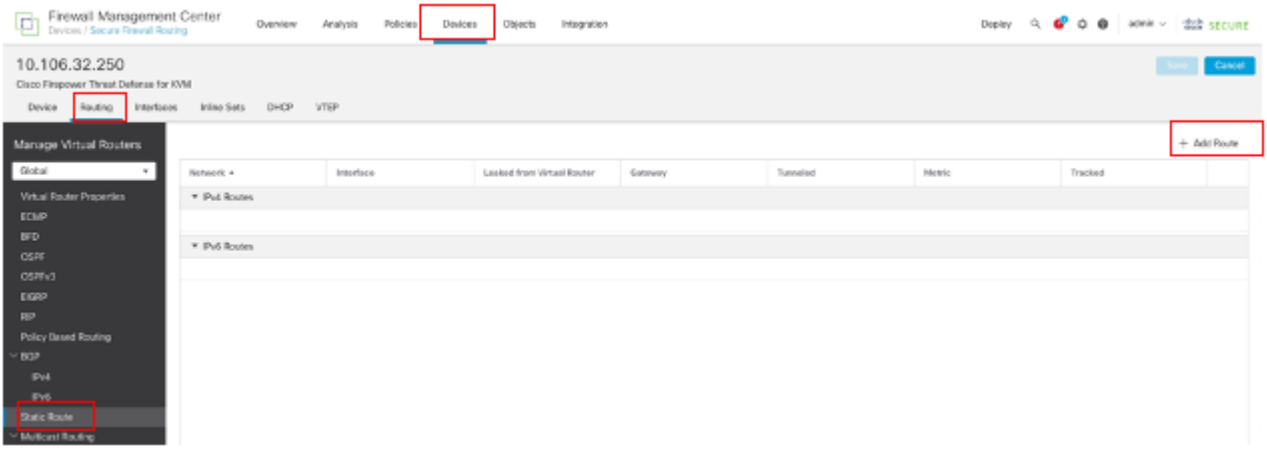
a. 为SLA监控器对象设置Name，在本例中为sla-outside2。
b. 在SLA Monitor ID字段中输入SLA操作的ID号。值范围为1至2147483647。您最多可在设备上创建2000个SLA操作。每个ID号对于策略和设备配置必须是唯一的。在本示例2中。
c. 在Monitored Address字段中输入由SLA操作监控的IP地址。在本例中为10.1.2.2。
d. Available Zones/Interfaces列表显示区域和接口组。在Zones/Interfaces列表中，添加包含设备通过哪些接口与管理站进行通信的区域或接口组。要指定单个接口，需要为该接口创建区域或接口组。在本示例中Outside2_Zone。
e. Click Save.



SLA对象Sla-outside2

步骤3.使用路由跟踪配置静态路由

导航到Devices > Device Management，编辑威胁防御设备，单击Routing，从虚拟路由器下拉列表中选择要为其配置静态路由的虚拟路由器。在本示例全局中。选择静态路由，然后单击添加路由将默认路由添加到第一个ISP网关。

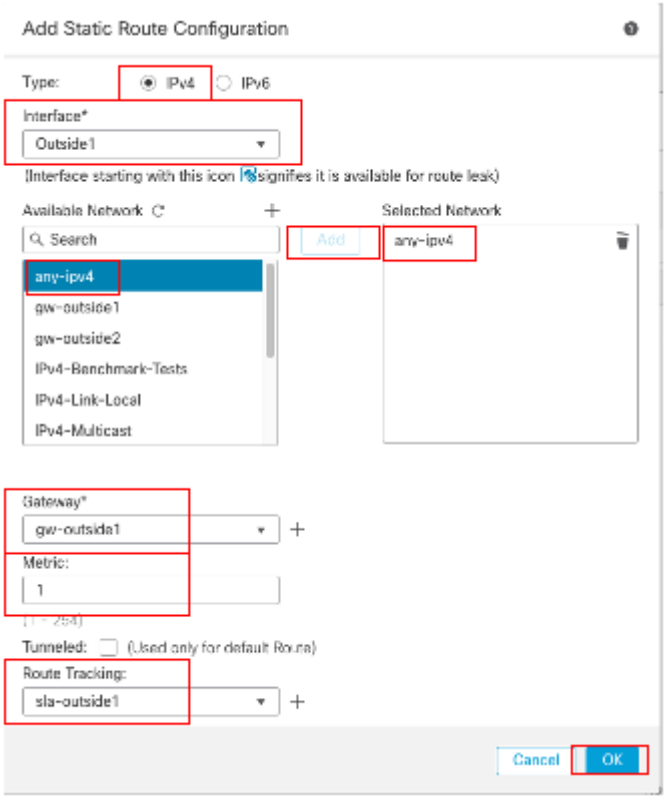


配置静态路由

在Add Static Route Configuration窗口中：

a. 根据要添加的静态路由的类型，单击IPv4或IPv6。在本示例中IPv4。
b. 选择此静态路由应用的Interface。在本示例中Outside1。

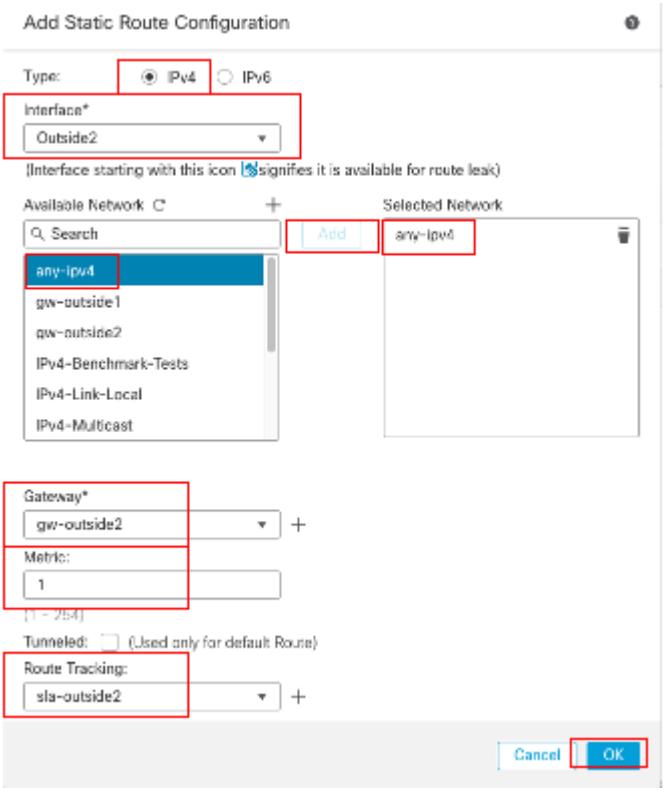
c. 在Available Network列表中，选择目标网络。在本示例中any-ipv4。
d. 在Gateway或IPv6 Gateway字段中，输入或选择作为此路由下一跳的网关路由器。可以提供IP地址或网络/主机对象。在本示例中gw-outside1。
e. 在度量字段中，输入到目标网络的跳数。有效值范围为1至255;默认值为1。在本例中为1。
f. 要监控路由可用性，请在Route Tracking字段中输入或选择定义监控策略的SLA监控对象的名称。在本示例中sla-outside1。
g. Click OK.



首先添加静态路由ISP

重复类似步骤，将默认路由添加到第二个ISP网关。在Add Static Route Configuration窗口中：

a. 根据要添加的静态路由类型，单击IPv4或IPv6。在本示例中IPv4。
b. 选择此静态路由应用的Interface。在本例中，Outside2。
c. 在Available Network列表中，选择目标网络。在本示例中any-ipv4。
d. 在Gateway或IPv6 Gateway字段中，输入或选择作为此路由下一跳的网关路由器。可以提供IP地址或网络/主机对象。在本示例中gw-outside2。
e. 在度量字段中，输入到目标网络的跳数。有效值范围为1至255;默认值为1。请确保指定与第一个路由相同的度量，在本例中为1。
f. 要监控路由可用性，请在Route Tracking字段中输入或选择定义监控策略的SLA监控对象的名称。在本示例中sla-outside2。
g. Click OK.



添加第二个ISP静态路由

单击Save和Deploy配置。

验证

登录FTD的CLI，运行命令以检查有关ECMP流量区域的信**show zone** 息，包括属于每个区域的接口。

<#root>

```
> show zone
Zone: Outside ecmp
Security-level: 0
```

Zone member(s): 2

Outside2 GigabitEthernet0/1

Outside1 GigabitEthernet0/0

运行命令show running-config route检查路由配置的运行配置，在这种情况下，有两条静态路由带有路由路径。

<#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
```

运行命令show route，检查路由表。如果有两个默认路由通过接口outside1和outside2，开销相等，流量可以在两个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: 1
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: 2
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，确认SLA监控器的状态。在这种情况下，您可以找到“超时：FALSE”，表示网关的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安装在路由表中。

<#root>

```
> show sla monitor operational-state
Entry number: 1
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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: 10:52:28.785 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

Entry number: 2
Modification time: 09:31:28.785 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 82
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: 10:52:28.785 UTC Thu Feb 15 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，以验证ECMP是否在ECMP区域中的网关之间对流量进行负载均衡。**show conn**在这种情况下，从Inside-Host1(10.1.3.2)和Inside-Host2(10.1.3.4)发起telnet连接以访问Internet-Host(10.1.5.2)，运行命令确认流量在两个ISP链路之间实现了负载均衡，Inside-Host1(10.1.3.2)通过interface outside1,Inside-Host2(10.1.3.4)通过interface outside2。

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:24, bytes 1329, flags UIO N1
TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:04, bytes 1329, flags UIO N1
```



注意：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。当您运行测试时，由于哈希算法，您模拟的流量可以路由到同一网关，这是预期的，它会更改6个元组（源IP、目标IP、传入接口、协议、源端口、目标端口）中的任何值以更改哈希结果。

丢失的路由

如果通向第一个ISP网关的链路已关闭（在本例中），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，则认为主机不可达，并标记为关闭。到达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，确认SLA监控器的当前状态。在这种情况下，您可以找到“Timeout occurred:如果命令输出中为true，则表示发往第一个ISP网关的ICMP回应没有响应。

<#root>

```
> show sla monitor operational-state
Entry number: 1
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
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: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 2
Modification time: 09:31:28.783 UTC Thu Feb 15 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 104
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: 11:14:28.813 UTC Thu Feb 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 1 RTTMin: 1 RTTMax: 1
```

```
NumOfRTT: 1 RTTSum: 1 RTTSum2: 1
```

运行命令检查当前路由表，删除了通过interface outside1到第一个ISP网关的路由，只有一条通过interface outside2到第二个ISP网关的活动默认路由**show route**。

<#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，您会发现两个连接仍处于运行状态。telnet会话在Inside-Host1(10.1.3.2)和Inside-Host2(10.1.3.4)上也处于活动状态，不会出现任何中断。

<#root>

```
> show conn
2 in use, 3 most used
Inspect Snort:
preserve-connection: 2 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP Inside 10.1.3.2:46069 Outside1 10.1.5.2:23, idle 0:00:22, bytes 1329, flags UIO N1


TCP Inside 10.1.3.4:61915 Outside2 10.1.5.2:23, idle 0:00:02, bytes 1329, flags UIO N1
```

注意：show conn 您可以看到，在的输出中，虽然通过接口outside1的默认路由已从路由表中删除，但来自Inside-Host1(10.1.3.2)的telnet会话仍通过接口outside1。这是预期结果，而

且根据设计，实际流量流经接口outside2。如果您启动从Inside-Host1(10.1.3.2)到Internet-Host(10.1.5.2)的新连接，则可以查找所有流量流经接口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
```

运行命令show route，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网关的链路重新打开时，通过接口outside1的路由将添加回路由表中。

<#root>

```
> debug ip routing
IP routing debugging is on

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
```

运行命令show route，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


                   [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
```

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）。