排除FTD中的OSPF配置故障

目录

简介

本文档介绍如何使用FMC作为管理器对FTD设备上的OSPF配置进行验证和故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 开放最短路径优先(OSPF)的概念和功能
- 思科安全防火墙管理中心(FMC)
- 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：

- 虚拟FTD 7.2.5
- 虚拟FMC 7.2.5

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。

OSPF 背景

可以在FMC上配置OSPF，以在FTD设备与其他OSPF设备之间使用动态路由。

FMC允许同时为不同的一组接口运行两个OSPF进程。

每台设备都有一个路由器ID，类似于OSPF进程中的设备名称。默认情况下，此地址设置为较低接口IP，但可自定义为其他IP。

需要注意的是，这些参数必须在邻居上匹配才能形成OSPF邻接关系：

- 接口属于同一个IP网络
- 子网掩码
- 区域
- Hello 间隔和 dead 间隔
- MTU
- 区域类型（普通/NSSA/末节）
- 身份验证

基本配置

本部分显示为OSPF配置的基本参数，用于开始搜索与其邻居的邻接关系。

1. 导航到设备>设备管理>编辑设备

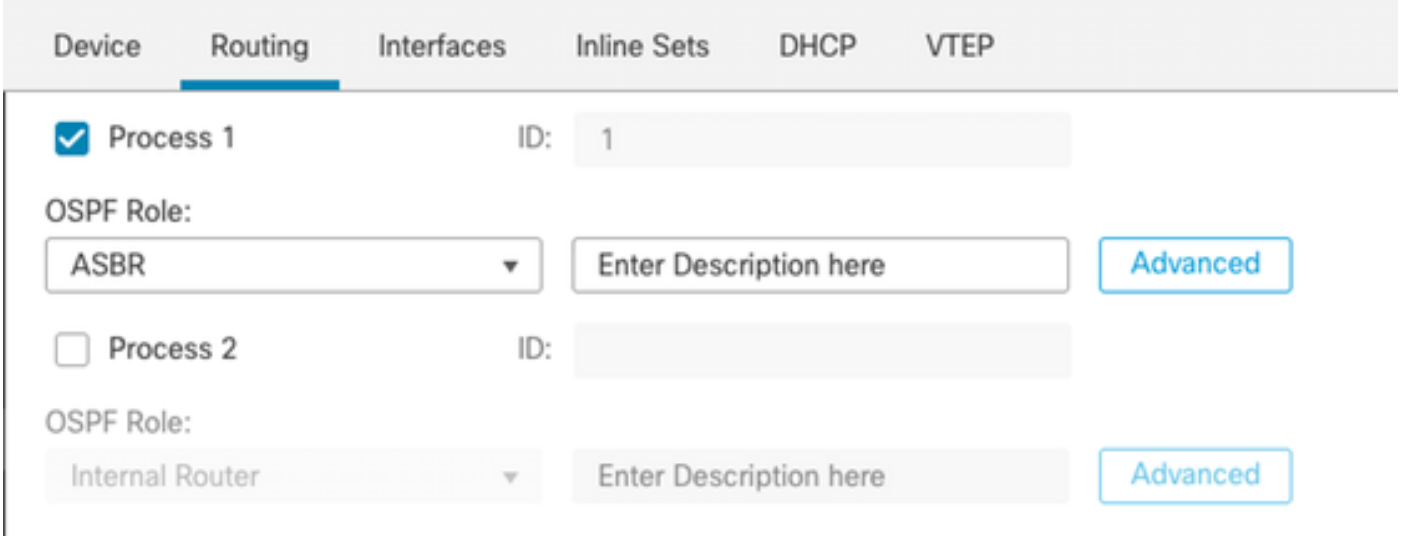
2. 单击Routing选项卡。

3. 单击左侧菜单栏上的OSPF。

4. 选择Process 1以启用OSPF配置。FTD可以在不同的接口集上同时运行两个进程。

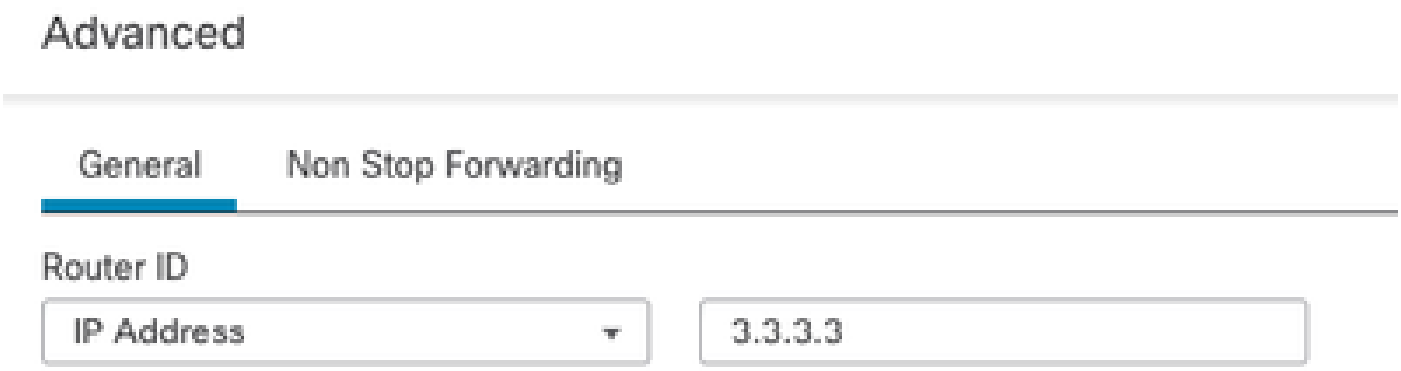
区域边界路由器(ABR)位于两个不同区域之间，而自治系统边界路由器(ASBR)位于使用其他路由协议的设备之间。

5. 选择OSPF role作为Internal、ABR、ASBR和ABR and ASBR。



角色选择

6.（可选）更改自动路由器ID。选择OSPF role旁边的Advanced，然后选择Router ID作为IP address进行自定义。



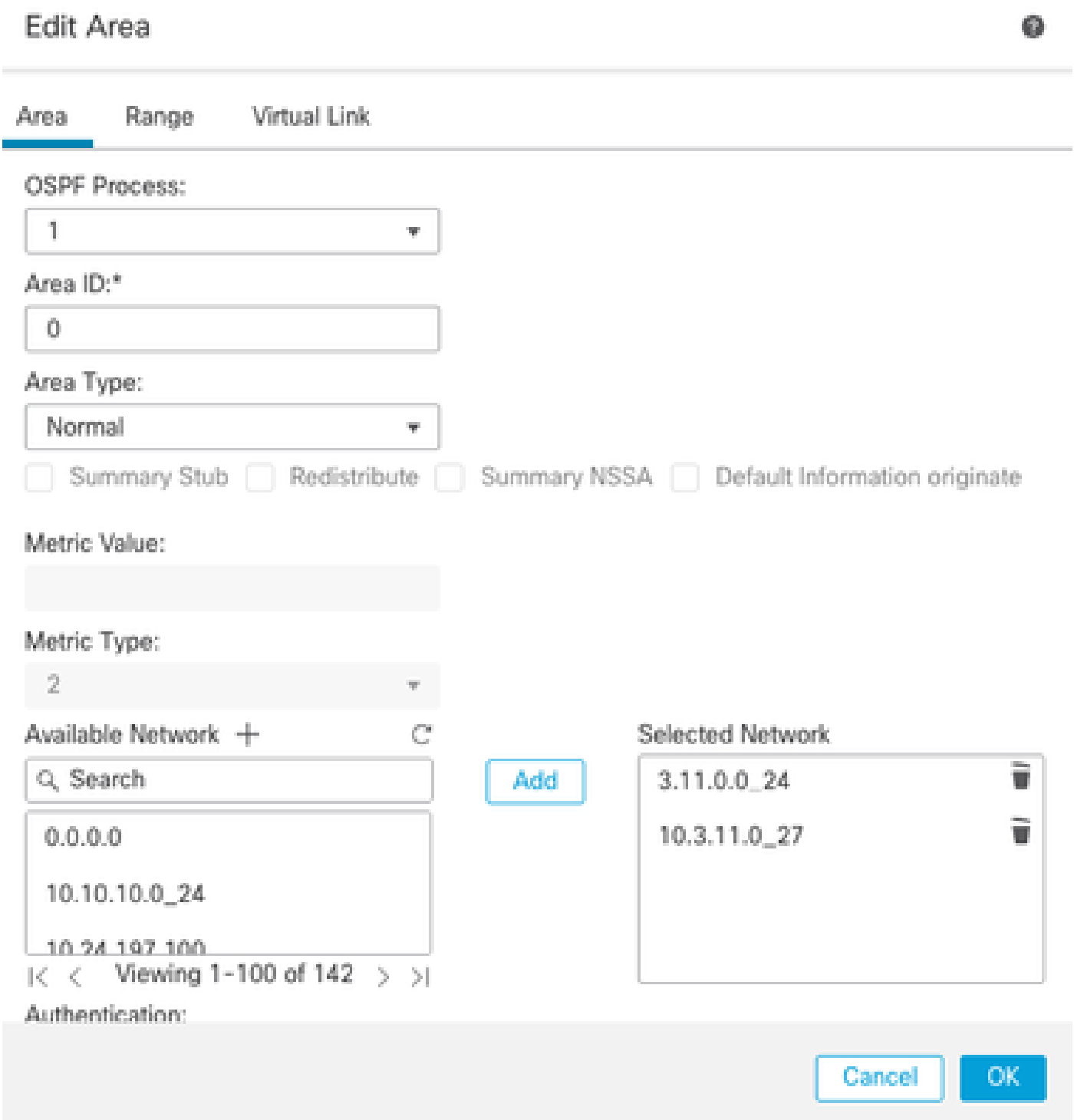
路由器ID选择

7. 选择区域>添加。

8. 输入区域信息：

- OSPF进程
- 区域 id
- 区域类型
- 可用网络

9. 单击确定保存配置。



区域选择

重分发

FTD可以将路由从一个OSPF进程重新分发到另一个OSPF进程。重分发也可以从RIP、BGP、EIGRP（7.2+版本）、静态路由和连接路由重分发到OSPF路由进程。

1. 要配置OSPF重分发，请导航到设备>设备管理>编辑设备。

2. 单击路由

3. 单击OSPF。

4. 选择Redistribution > Add。

5. 输入重分配字段：

- OSPF进程
- 路由类型（从重分发的位置）
  - 静态
  - 已连接
  - OSPF进程
  - 调试输出中显示“BGP
  - RIP
  - EIGRP

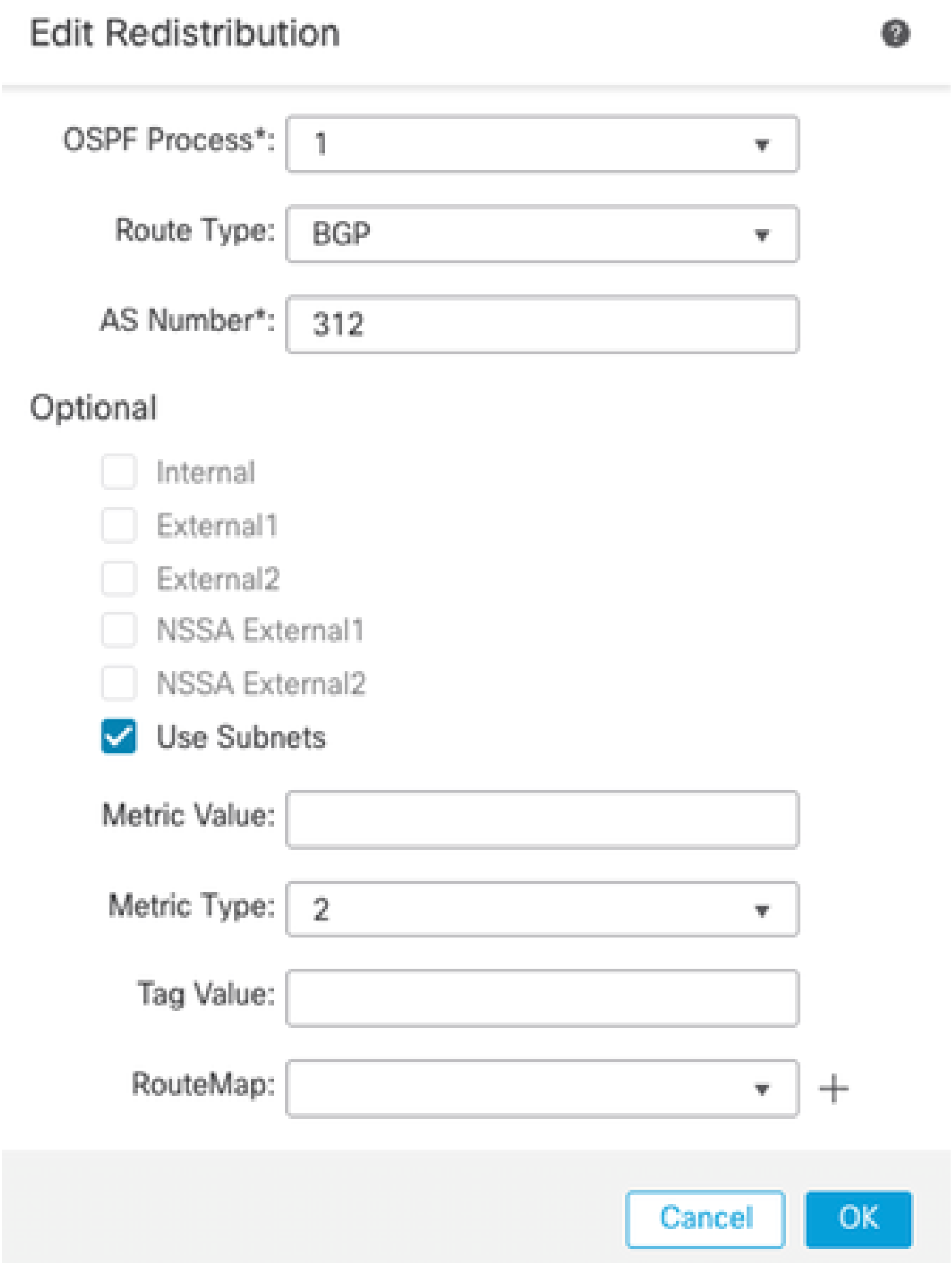
对于BGP和EIGRP，添加AS编号。

6.（可选）选择是否使用子网。

7. 选择指标类型。

- 第1类使用外部度量，并将通向ASBR的每一跳的内部开销相加。
- 第2类仅使用外部度量。

8. 单击确定保存更改。


Edit Redistribution
OSPF Process*:
1
Route Type:
BGP
AS Number*:
312
Optional
Internal
External1
External2
NSSA External1
NSSA External2
Use Subnets
Metric Value:
Metric Type:
2
Tag Value:
RouteMap:
Cancel
OK

重分发配置

过滤

您可以执行区域间过滤，从而限制从一个区域发送到另一个区域的入站或出站路由。此操作仅在ABR上执行。

使用前缀列表配置过滤，这些前缀列表随后会链接到OSPF配置。这是一项可选功能，OSPF不需要它就能工作。

1. 要配置OSPF区域间过滤，请导航到Devices > Device Management > Edit device。

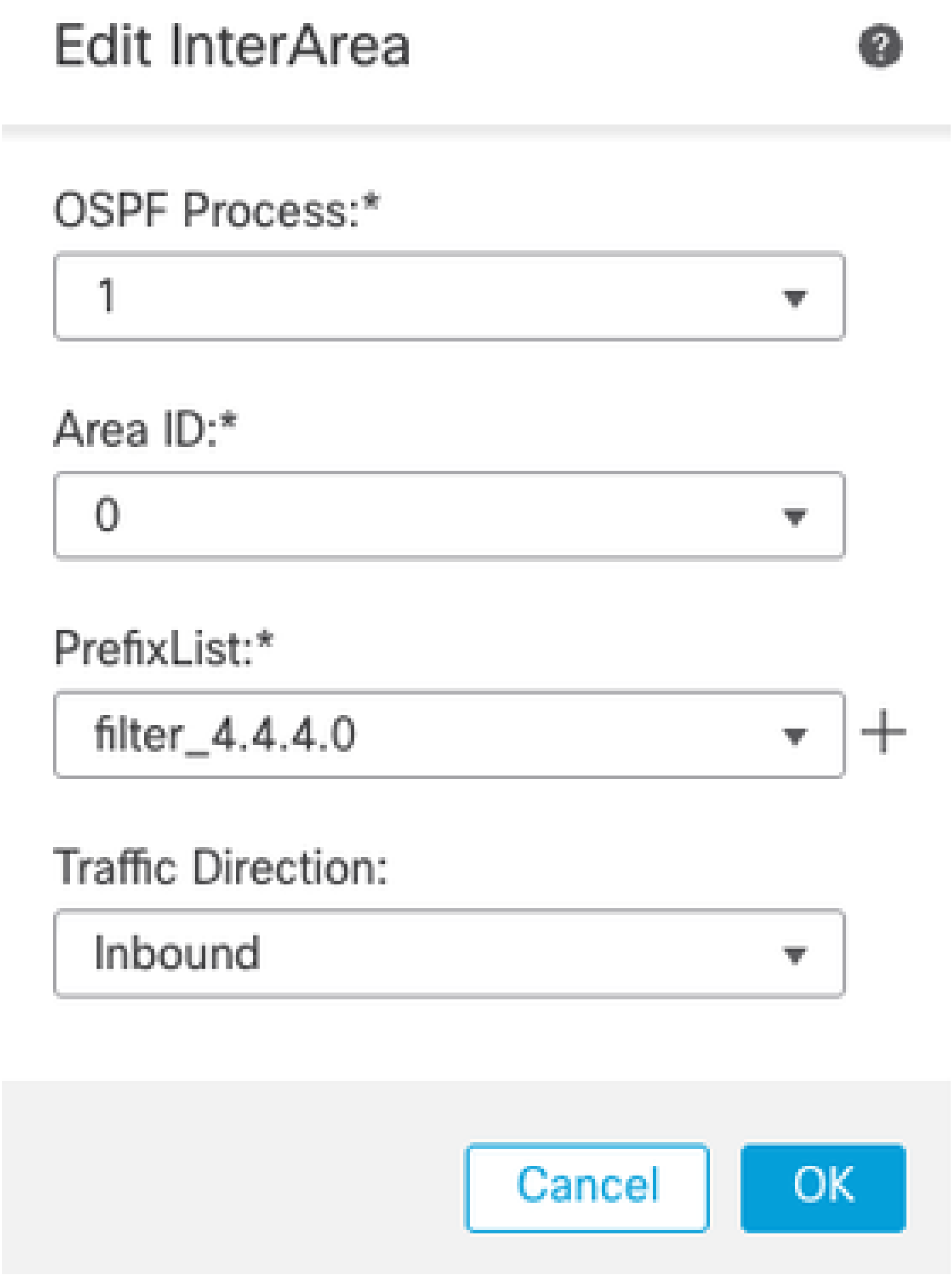
2. 单击路由

3. 单击OSPF。

4. 选择区域间>添加。

5. 配置过滤字段：

- OSPF进程
- 区域 id
- 前缀列表
- 流量方向-入站或出站


Edit InterArea
OSPF Process:*
1
Area ID:*
0
PrefixList:*
filter_4.4.4.0
Traffic Direction:
Inbound
Cancel
OK

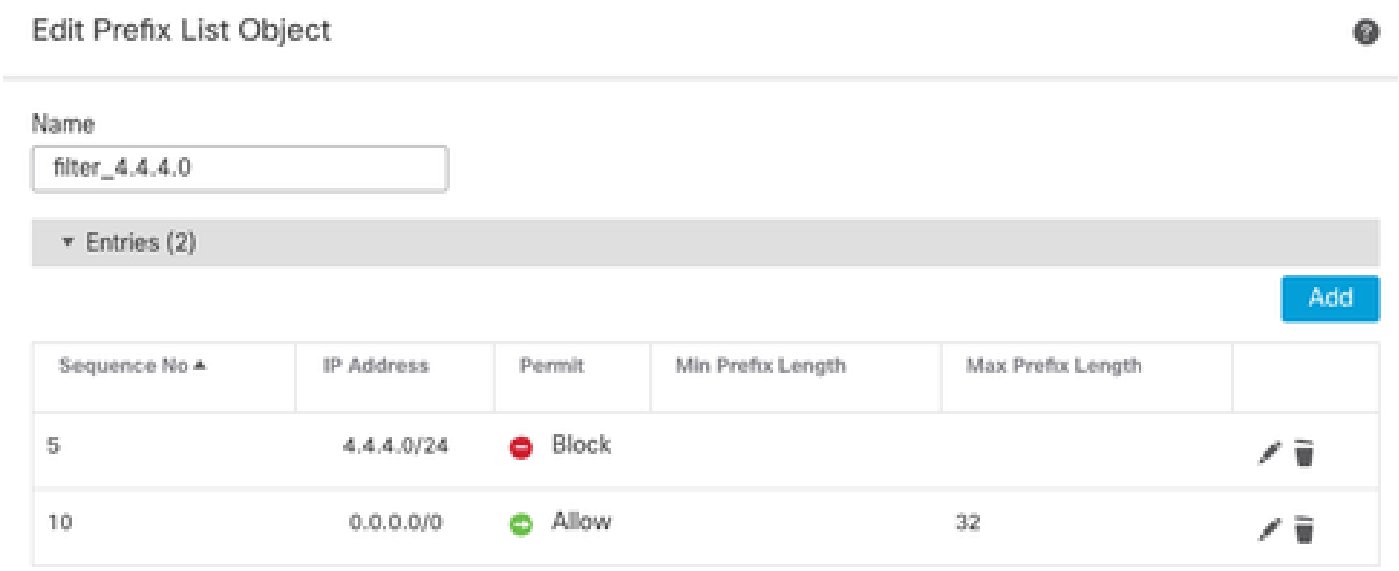
区域间过滤配置

6. 如果已配置前缀列表，请移至步骤10。如果需要创建一个新加号，您可以选择它或从Objects > Object Management > Prefix Lists > IPv4 prefix list > Add中创建它。

7. 单击Add条目。

8. 使用以下字段配置前缀列表：

- 序列号
- IP Address
- 操作
- 最小/最大前缀长度（可选）



前缀列表对象编辑

9. 单击确定保存前缀列表。

10. 单击确定保存区域间配置。

接口参数

对于参与OSPF的每个接口，可以修改某些参数。

1. 要配置OSPF接口参数，请导航到设备>设备管理>编辑设备。

2. 单击路由

3. 单击OSPF。

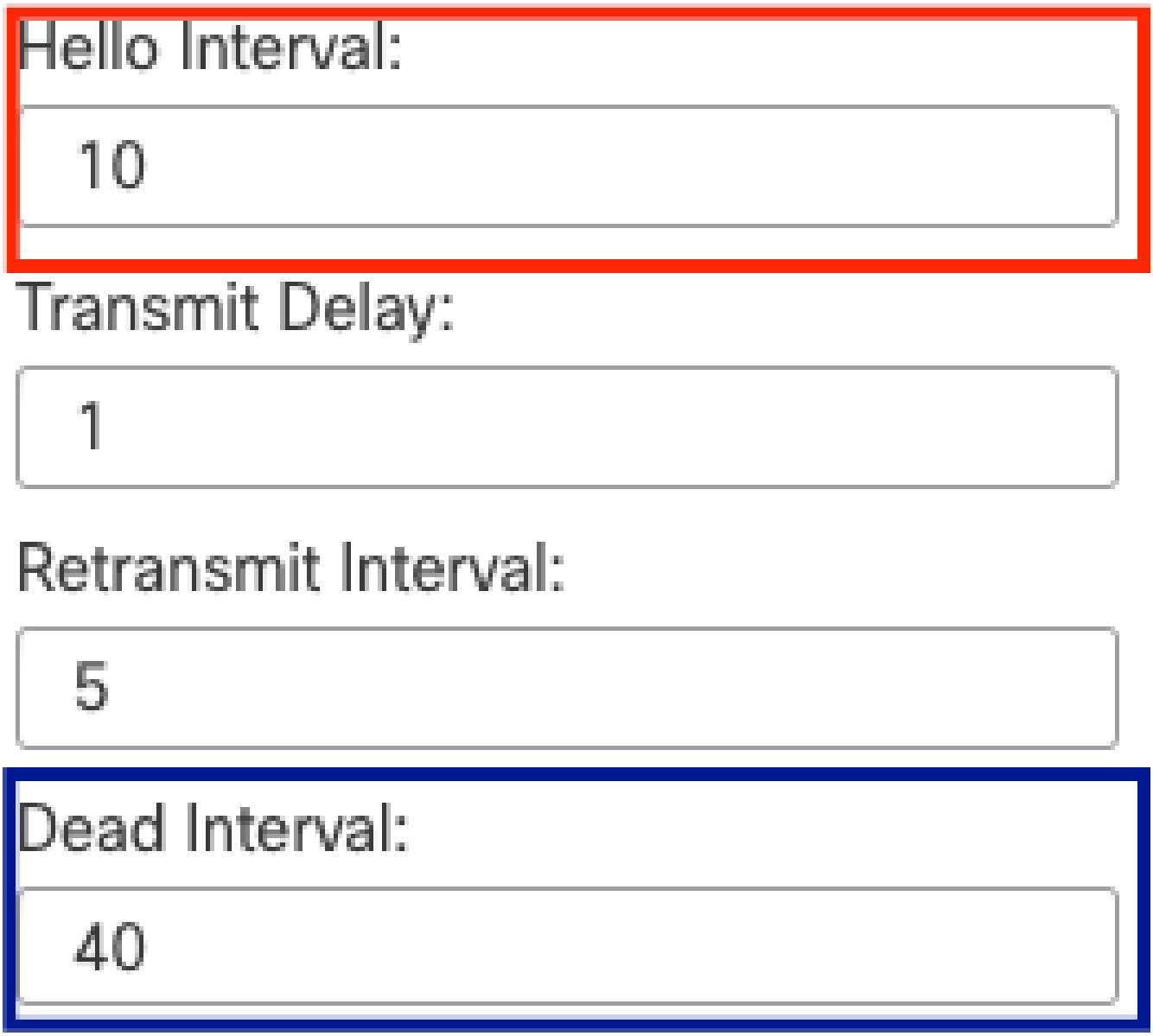
4. 选择Interface > Add。

5. 选择要修改的参数

Hello和Dead计时器

发送OSPF Hello数据包以维护设备之间的邻接。这些数据包以可配置的间隔发送。如果设备在dead间隔（也可配置）内未收到来自邻居的hello数据包，则邻居会变为down状态。

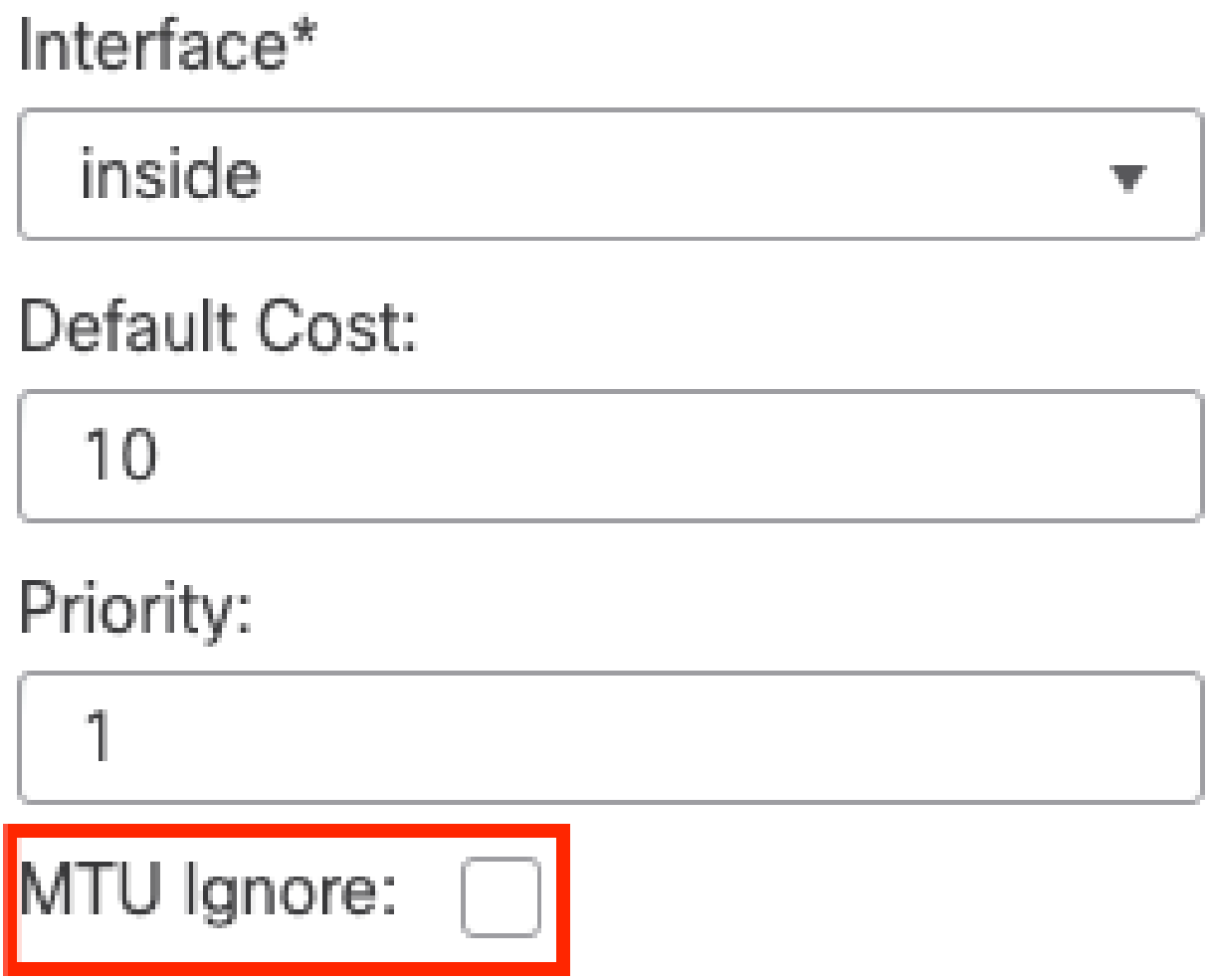
默认情况下，hello间隔为10秒，dead间隔是hello间隔的四倍，即40秒。这些间隔在邻居之间必须匹配。



计时器配置

MTU Ignore-OSPF

使用MTU ignore复选框可避免由于邻居接口之间的MTU不匹配而导致OSPF邻接停滞在EXSTART状态。MTU匹配已验证，因为在该状态下，DBD在邻居之间发送，大小差异可能会引起问题。但是，最佳做法是取消选中此选项。



MTU忽略检查配置

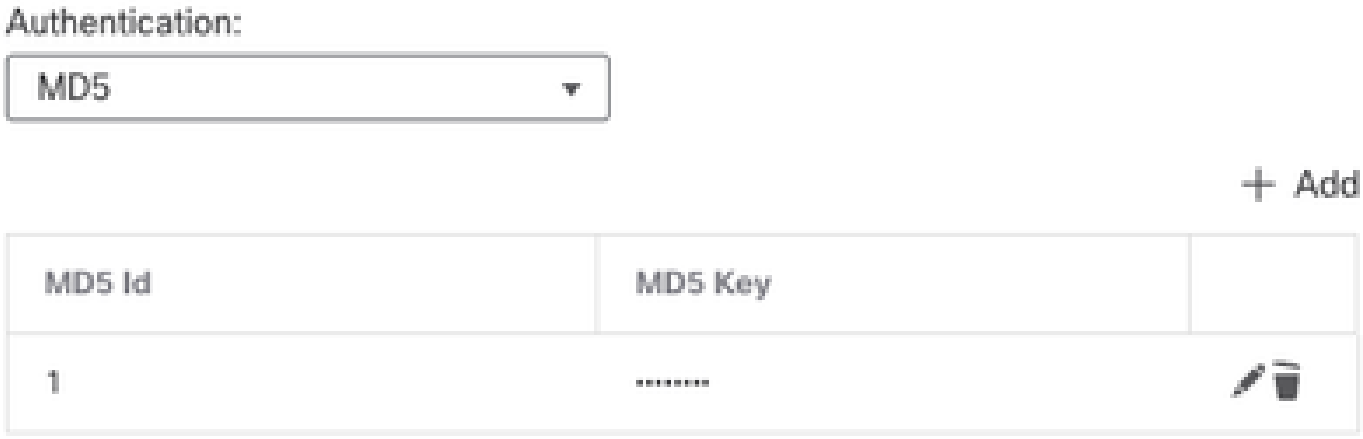
身份验证

您可以选择三种不同类型的接口OSPF身份验证。默认情况下，身份验证未启用。

- 无
- Password -明文密码
- MD5 -使用MD5散列

建议使用MD5作为身份验证，因为它是提供安全性的散列算法。

配置MD5 ID和MD5密钥，然后单击OK进行保存。



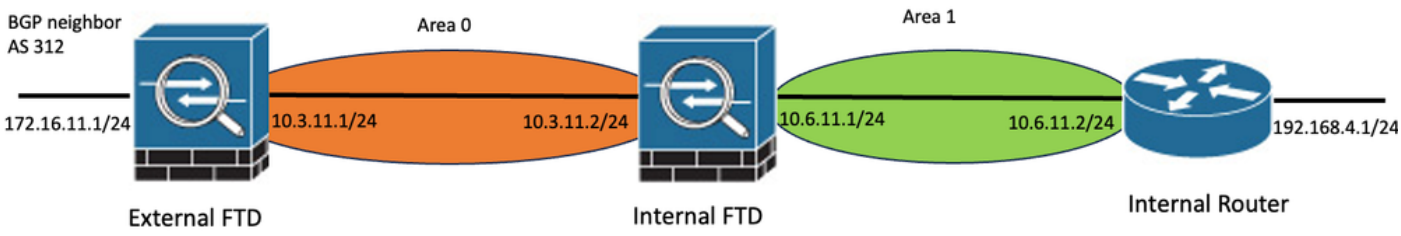
MD5密钥配置

MD5密钥或密码在经过身份验证的邻居的接口参数上必须匹配。

常规CLI验证

示例拓扑

考虑将此网络拓扑作为示例：



网络拓扑示例

请考虑以下因素：

- OSPF在外部FTD、内部FTD和内部路由器上配置。
- 选择外部FTD作为ASBR角色，选择内部FTD作为ABR，选择内部路由器作为内部角色。
- 区域0创建于外部和内部FTD之间，而区域1创建于内部FTD和内部路由器之间。
- 外部FTD还与其他设备执行BGP邻居关系。
- 自治系统312获知的BGP路由会重分配到OSPF中。
- MTU和间隔使用默认值进行配置。
- 内部FTD过滤从内部路由器获知的区域0的入站区域间路由。
- 在参与OSPF的所有设备上，接口身份验证配置为MD5。

内部FTD

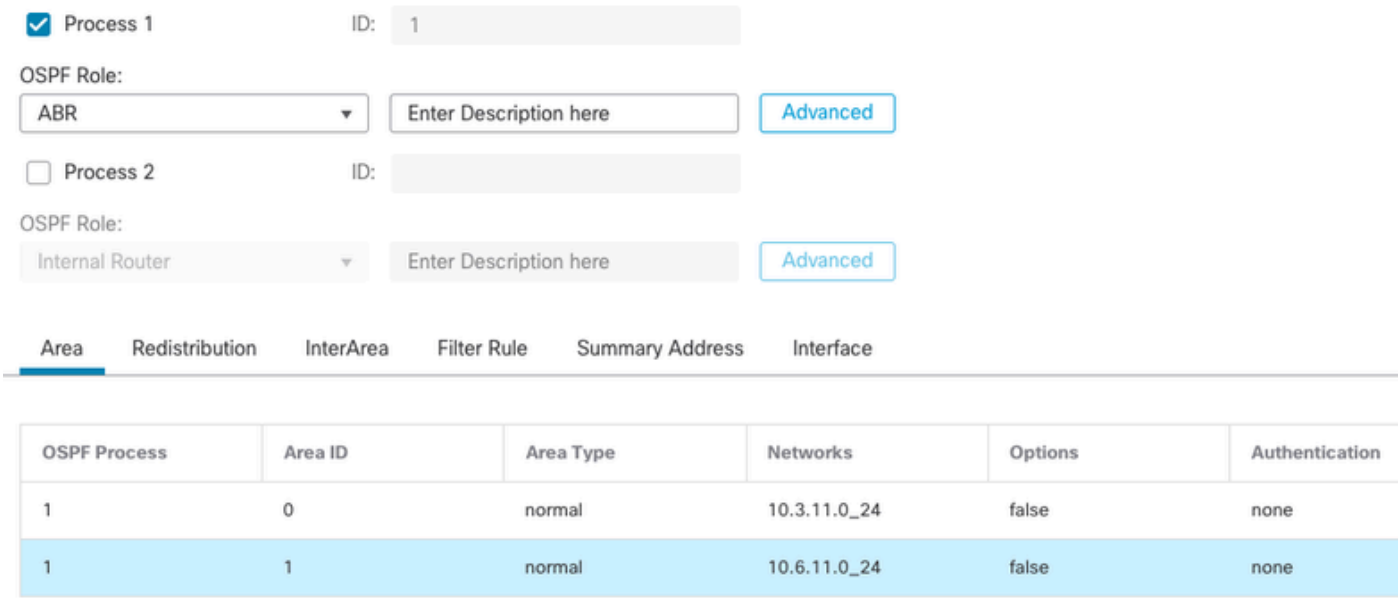
内部FTD的配置如下所示：

使用MD5身份验证的接口配置

```
interface GigabitEthernet0/0
nameif inside
security-level 0
ip address 10.6.11.1 255.255.255.0
ospf message-digest-key 1 md5 *****
ospf authentication message-digest
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.3.11.2 255.255.255.0
ospf message-digest-key 1 md5 *****
ospf authentication message-digest
!
```

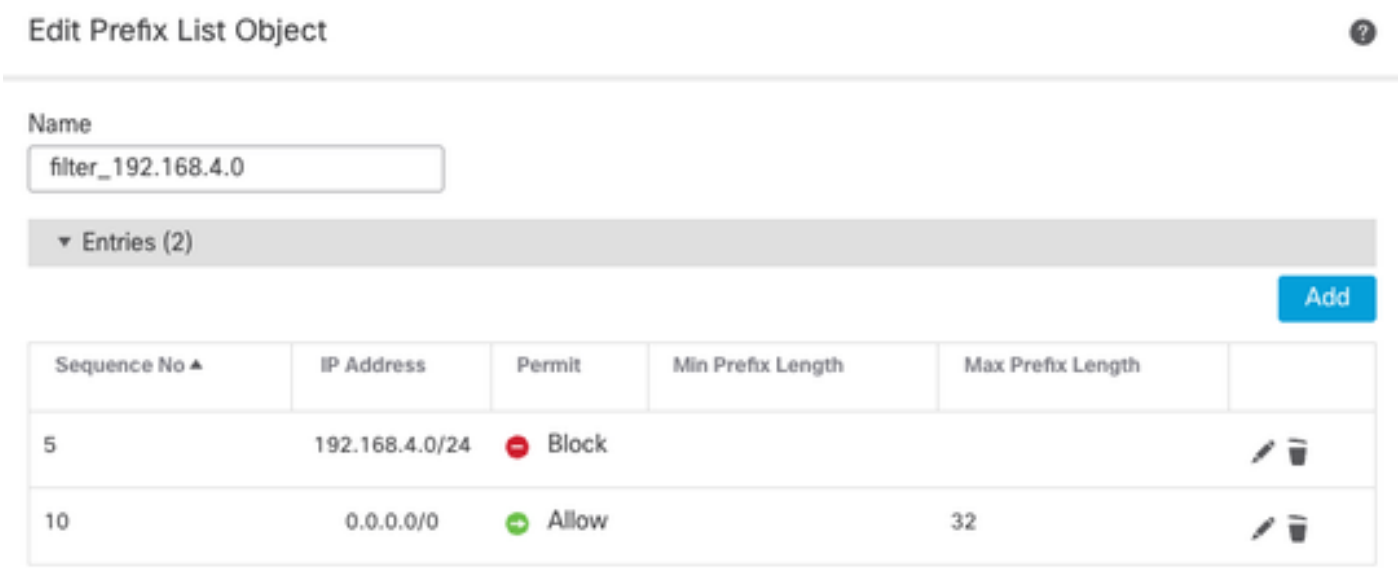
OSPF配置表明，网络10.3.11.0/24通告给区域0，网络10.6.11.0/24通告给区域1上的邻居。

区域间过滤将前缀列表应用到进入区域0的入站路由。在此前缀列表中，来自内部路由器的网络192.168.4.0被拒绝，并且所有其他内容均被允许。



内部FTD区域配置

内部FTD过滤配置



内部FTD前缀列表

```
router ospf 1
network 10.3.11.0 255.255.255.0 area 0
network 10.6.11.0 255.255.255.0 area 1
area 0 filter-list prefix filter_192.168.4.0 in
log-adj-changes

prefix-list filter_192.168.4.0 seq 5 deny 192.168.4.0/24
prefix-list filter_192.168.4.0 seq 10 permit 0.0.0.0/0 le 32
```

外部FTD

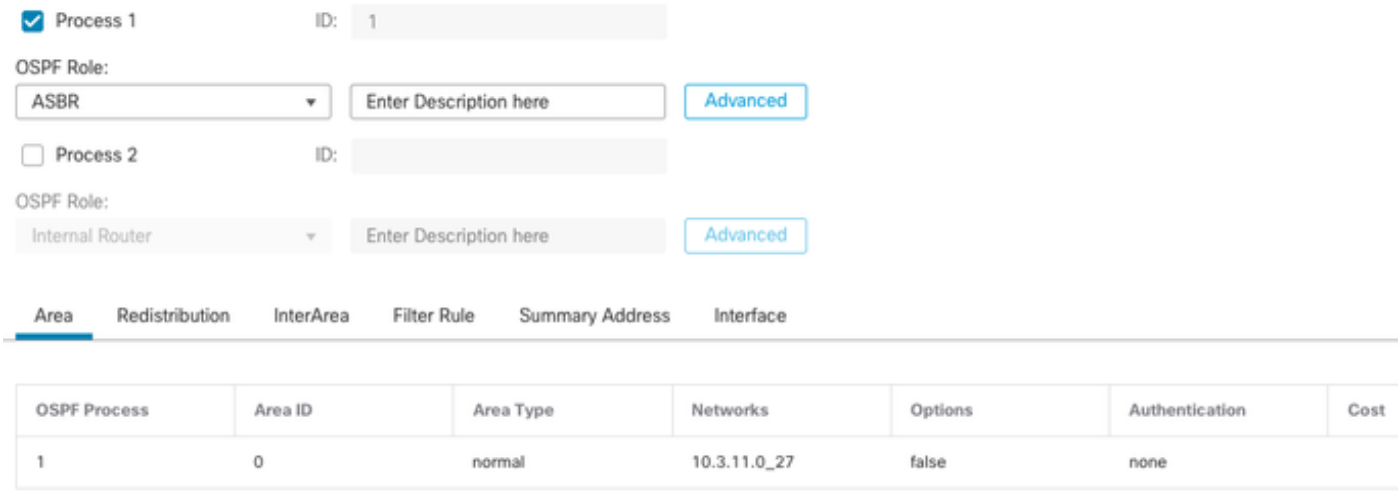
外部FTD的配置在CLI中显示如下：

使用MD5身份验证配置接口。

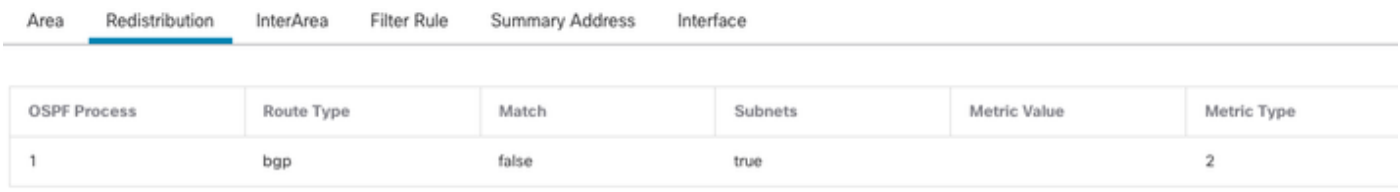
```
interface GigabitEthernet0/0
nameif inside
security-level 0
ip address 10.3.11.1 255.255.255.0
ospf message-digest-key 1 md5 *****
ospf authentication message-digest
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 172.16.11.1 255.255.255.0
!
```

OSPF配置显示路由10.3.11.0/24通告给区域0中的内部FTD。

还可以观察到BGP重分发到OSPF的过程。



外部FTD区域配置

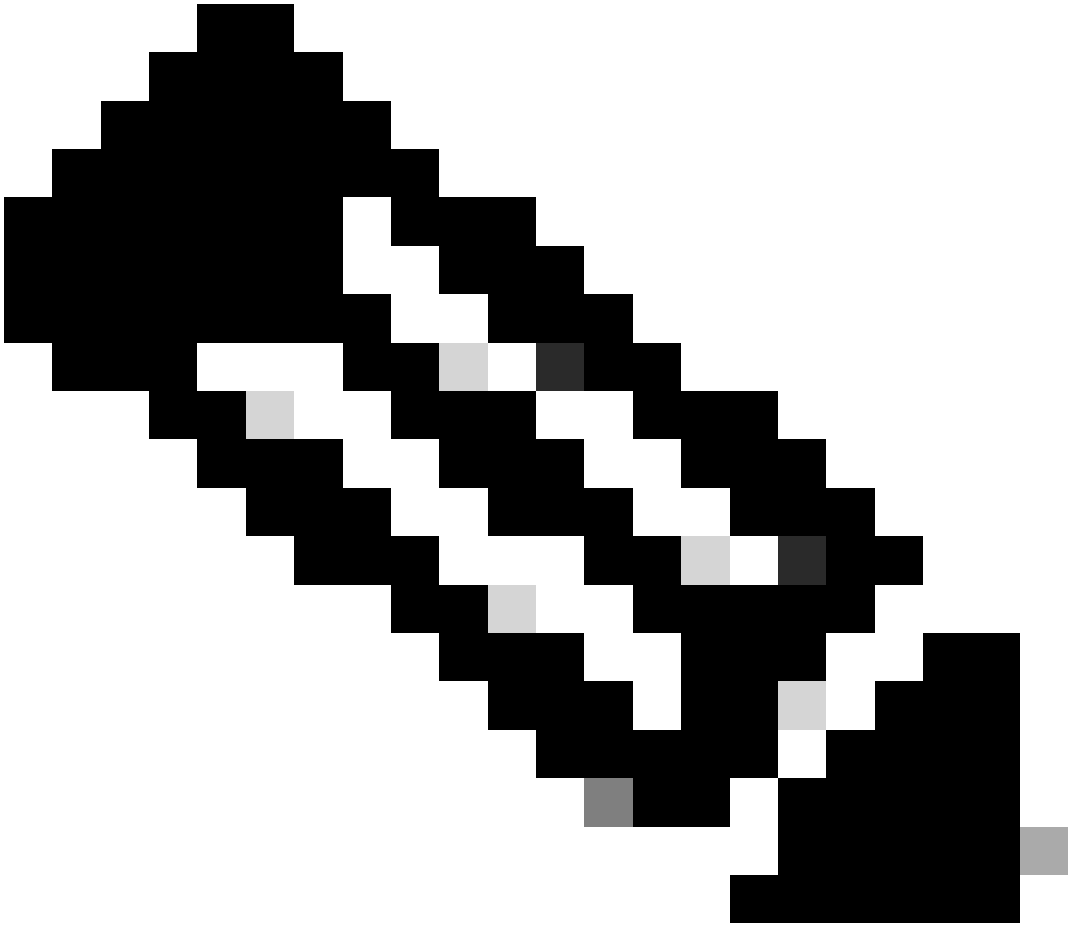


外部FTD重分发配置

```
router ospf 1
network 10.3.11.0 255.255.255.0 area 0
log-adj-changes
redistribute bgp 312 subnets
```

故障排除命令

有几个命令可用于确定OSPF是否按预期工作。



注意：当FTD故障排除文件是除OSPF配置之外生成的，并且需要从FTD CLI手动输入时，show tech files上不会显示这些命令。

show running-config router

此命令不仅显示OSPF，还显示动态路由协议的配置。

在CLI中检查OSPF相关配置时非常有用。

show route

show route输出说明了有关当前可用路由的重要信息。

- 通过OSPF获取的路由以字母O显示。
- 区域间路由以字母O IA显示。
- 通过重分发从其他路由协议获取的路由根据所选的度量类型显示字母O E1或O E2。

内部FTD的show route输出显示，存在三个已知来自ASBR邻居10.3.11.1的外部路由。

它还显示从同一区域的邻居10.6.11.2获知的网络192.168.4.0/24。

```
<#root>

Internal-FTD#

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
Gateway of last resort is not set

C        10.3.11.0 255.255.255.0 is directly connected, outside
L        10.3.11.2 255.255.255.255 is directly connected, outside
O E2     10.5.11.0 255.255.255.224 [110/1] via 10.3.11.1, 6w5d, outside
O E2     10.5.11.32 255.255.255.224 [110/1] via 10.3.11.1, 6w5d, outside
O E2     10.5.11.64 255.255.255.224 [110/1] via 10.3.11.1, 6w5d, outside
C        10.6.11.0 255.255.255.0 is directly connected, inside
L        10.6.11.1 255.255.255.255 is directly connected, inside
O        192.168.4.0 255.255.255.0 [110/20] via 10.6.11.2, 02:19:24, inside
```

从外部FTD可以观察到，路由10.6.11.0/24已知自邻居10.3.11.2，它属于另一个区域。

此输出中未观察到路由192.168.4.0/24，因为它已在内部FTD中过滤。

此外，从另一设备获取的三个BGP路由作为外部类型2路由重分发到OSPF，如内部FTD所示。

```
<#root>

External-FTD#

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 not set

C        10.3.11.0 255.255.255.0 is directly connected, inside
L        10.3.11.1 255.255.255.255 is directly connected, inside
```

```
B        10.5.11.0 255.255.255.224 [20/0] via 172.16.11.2, 6w5d
B        10.5.11.32 255.255.255.224 [20/0] via 172.16.11.2, 6w5d
B        10.5.11.64 255.255.255.224 [20/0] via 172.16.11.2, 6w5d
O IA     10.6.11.0 255.255.255.0 [110/20] via 10.3.11.2, 02:03:27, inside
C        172.16.11.0 255.255.255.0 is directly connected, outside
L        172.16.11.1 255.255.255.255 is directly connected, outside
```

show ospf neighbor

此命令有助于验证OSPF邻接的状态是什么，以及该邻居是否为指定路由器(DR)、备用指定路由器(BDR)或其他(DROTHER)。

DR是指在网络发生变化时更新同一子网中其余设备的设备。如果不再提供，BDR将承担DR角色。

这也很有用，因为它显示邻居的路由器ID以及IP地址和已知邻居的接口。

还会观察停顿时间倒计时。如果您有默认计时器，在发送新的hello数据包和重新启动计时器之前，您可以看到时间从00:40下降到00:30。

如果此时间一直为零，则邻接关系将丢失。

在本例中，内部FTD输出显示，此设备是一个BDR处于FULL状态，并且其两个邻居中的每一个都可从每个接口访问DR。它们的路由器ID分别为10.3.11.1和192.168.4.1。

```
<#root>

Internal-FTD#

show ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.11.1         1   FULL/DR         0:00:38    10.3.11.1       outside
192.168.4.1       1   FULL/DR         0:00:33    10.6.11.2       inside
```

show ospf interface

show ospf interface输出显示详细信息，并提供每个已配置接口上OSPF进程的更广阔视图。

以下是此输出中可见的一些参数：

- OSPF 进程 ID
- 路由器 ID
- 度量（开销）
- 状态- DR、BDR或DROTHER
- 谁是DR和BDR。
- Hello和Dead计时器间隔
- 邻居汇总

- 身份验证详细信息

在内部FTD的下一个输出中，可以观察到此设备实际上是两个接口上的BDR，且该邻居与来自show ospf neighbors的信息匹配。

```
<#root>

Internal-FTD#

show ospf interface



outside is up, line protocol is up
Internet Address 10.3.11.2 mask 255.255.255.0, Area 0
Process ID 1, Router ID 10.6.11.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 10.3.11.1, Interface address 10.3.11.1
Backup Designated router (ID) 10.6.11.1, Interface address 10.3.11.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 0:00:04
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 10.3.11.1 (Designated Router)
Suppress hello for 0 neighbor(s)
Cryptographic authentication enabled
Youngest key id is 1

inside is up, line protocol is up
Internet Address 10.6.11.1 mask 255.255.255.0, Area 1
Process ID 1, Router ID 10.6.11.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.4.1, Interface address 10.6.11.2
Backup Designated router (ID) 10.6.11.1, Interface address 10.6.11.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 0:00:03
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.4.1 (Designated Router)
Suppress hello for 0 neighbor(s)
Cryptographic authentication enabled
Youngest key id is 1
```

show ospf database

此命令具有有关OSPF的链路状态通告(LSA)类型的详细信息。输出非常复杂，仅有助于进行更深入的故障排除。

LSA是OSPF在设备之间交换信息和更新，而不是发送完整路由表的方式。

最常见的LSA类型包括：

第1类-路由器链路状态- 通告路由器的路由器ID

第2类-网络链路状态 -与指定路由器连接在同一链路中的接口。

第3类-汇总网络链路状态- 区域边界路由器(ABR)注入此区域的区域间路由。

第4类-汇总ASB链路状态- 自治系统边界路由器(ASBR)的路由器ID。

第5类- AS外部链路状态- 从ASBR获知的外部路由。

记住这一点后，可以从Internal FTD示例解释此命令的输出。

- 数据库按区域显示。
- 链接ID列包含要注意的重要信息。
- 如前所述，类型1显示区域中每台设备的路由器ID，类型2显示每个子网链路的DR。在本例中，区域0为10.3.11.1，区域1为10.6.11.2。
- 类型3显示区域0的ABR 10.6.11.0和区域1的10.3.11.0插入到各自区域的区域间路由。
- 第4类显示ASBR的路由器ID。区域1认为10.3.11.1设备是进程的ASBR。
- 第5类显示ASBR重分发的路由。在本例中，有三个外部路由：10.5.11.0、10.5.11.32和10.5.11.64。

```
<#root>

Internal-FTD#

show ospf database



            OSPF Router with ID (10.6.11.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.3.11.1       10.3.11.1       234         0x8000002b 0x4c4d 1
10.6.11.1       10.6.11.1       187         0x8000002e 0x157b 1

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.3.11.1       10.3.11.1       234         0x80000029 0x7f2b

                Summary Net Link States (Area 0)
```

```
Link ID         ADV Router      Age         Seq#       Checksum
10.6.11.0       10.6.11.1       187         0x8000002a 0x7959

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.6.11.1       10.6.11.1       187         0x8000002c 0x513b 1
192.168.4.1     192.168.4.1     1758        0x8000002a 0x70f1 2

                Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
10.6.11.2       192.168.4.1     1759        0x80000028 0xd725

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
10.3.11.0       10.6.11.1       189         0x80000029 0x9f37

                Summary ASB Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
10.3.11.1       10.6.11.1       189         0x80000029 0x874d

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
10.5.11.0       10.3.11.1       1726        0x80000028 0x152b 311
10.5.11.32      10.3.11.1       1726        0x80000028 0xd34c 311
10.5.11.64      10.3.11.1       1726        0x80000028 0x926d 311
```

相关信息

- 思科技术支持和下载
- 了解开放最短路径优先 (OSPF) - 设计指南

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）。