

在安全防火墙威胁防御中配置BGP多路径

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[图解](#)

[BGP配置](#)

[BGP多路径配置](#)

[验证](#)

[故障排除](#)

[问题解答](#)

[相关信息](#)

简介

本文档介绍如何在思科安全防火墙威胁防御中配置边界网关协议(BGP)多路径。

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BGP配置
- 常规BGP
- 思科安全防火墙管理中心(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7.6
- 思科FMC版本7.6

免责声明：本文档中引用的网络和IP地址未与任何单个用户、组或组织关联。此配置专为实验环境而创建。

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

本文档介绍当从同一AS（例如，同一ISP）中的不同路由器收到通往同一目标的路由时，如何在Firepower威胁防御中配置BGP多路径负载共享。

BGP多路径允许安装到IP路由表中指向同一目标前缀的多个等价的BGP路径。然后，到达目标前缀的流量在所有已安装的路径之间共享。

这些路径会与最佳路径一起添加到路由表中，以实现负载共享目的。BGP多路径不影响选择最佳路径的过程。例如，FTD仍会根据算法选择一个路径作为最佳路径，并将此最佳路径通告给其BGP对等体。

要符合多路径候选条件，到同一目标的路径必须匹配以下特征中的最佳路径：

- 权重
- 本地首选
- AS-PATH 长度
- 源代码
- 多出口鉴别器(MED)

以下之一：

- 相邻AS或子AS（在BGP多路径添加之前）
- AS-PATH（在BGP多路径添加之后）

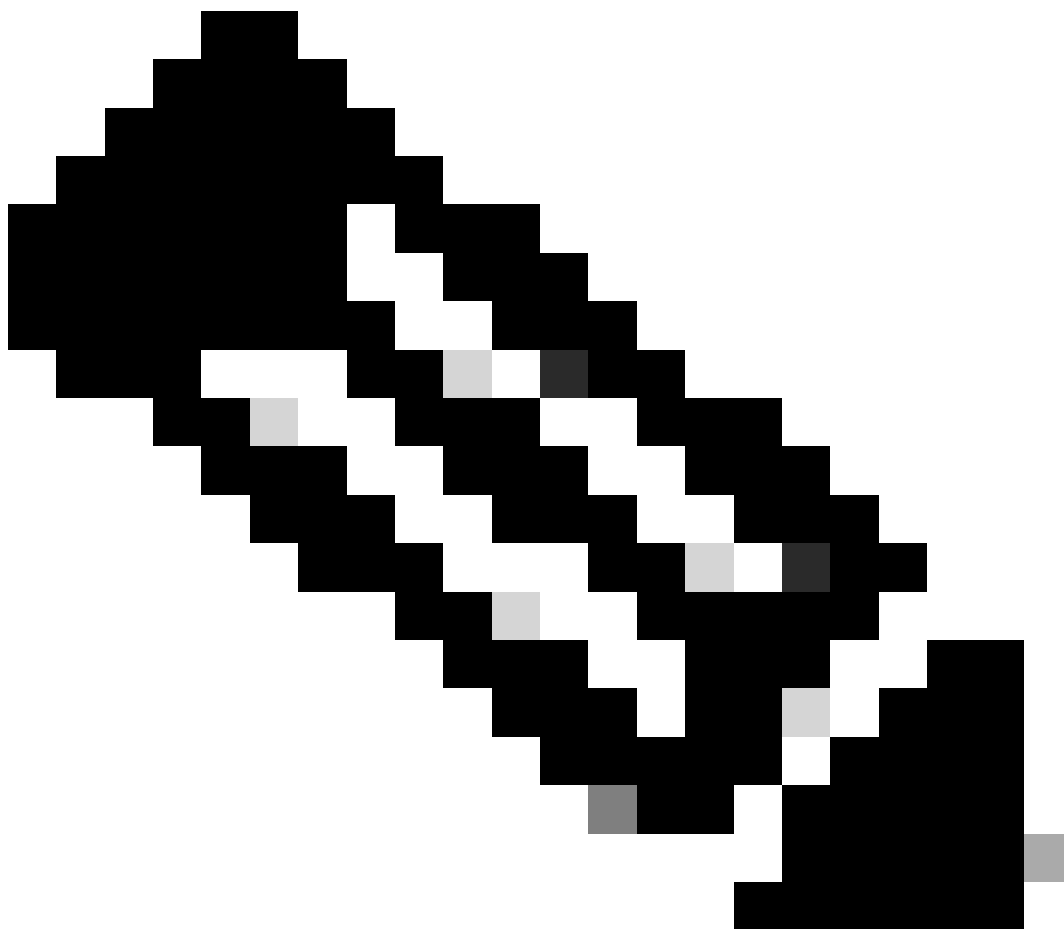
某些BGP多路径功能对多路径候选提出了进一步要求：

- 路径必须源自外部或联盟外部邻居(eBGP)。
- 到BGP下一跳的IGP度量必须与最佳路径的IGP度量匹配。

对于内部BGP(iBGP)多路径候选者，以下附加要求适用：

- 必须从内部邻居(iBGP)获知路径。
- 除非路由器设置为非等价的iBGP多路径，否则到BGP下一跳的IGP度量必须与最佳路径IGP度量匹配。

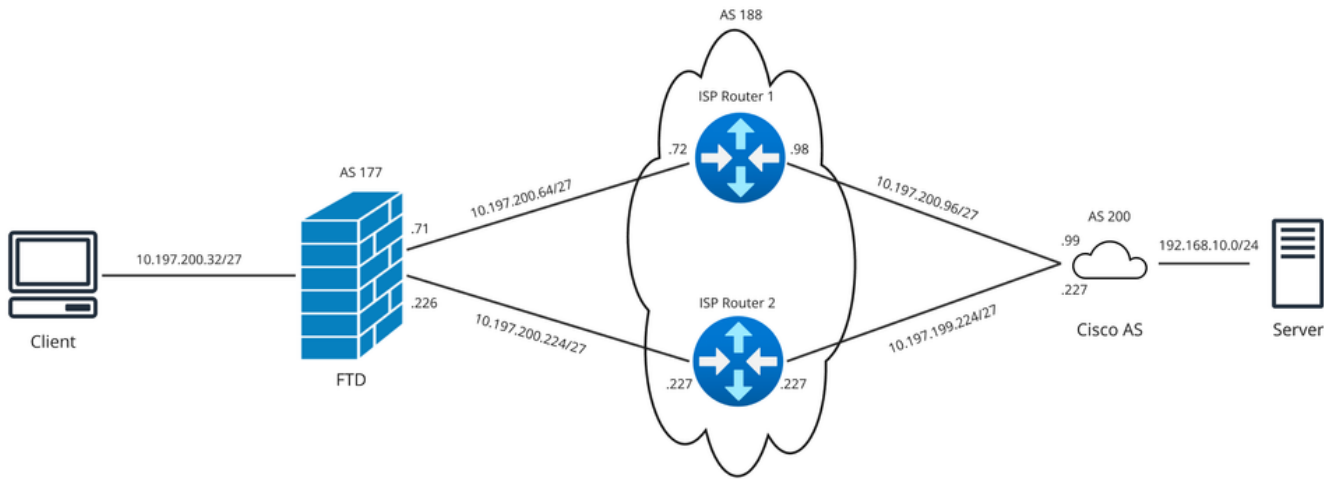
BGP最多将n条最近从多路径候选处接收的路径插入到IP路由表中，其中n是要安装到路由表中的路由数，如配置BGP多路径时指定。n的值范围为1-8（对于FTD）。当禁用多路径时，默认值为 1。



注意：等效的 next-hop-self 在转发到内部对等方之前，先在 eBGP 多路径中选择的最佳路径上执行。

配置

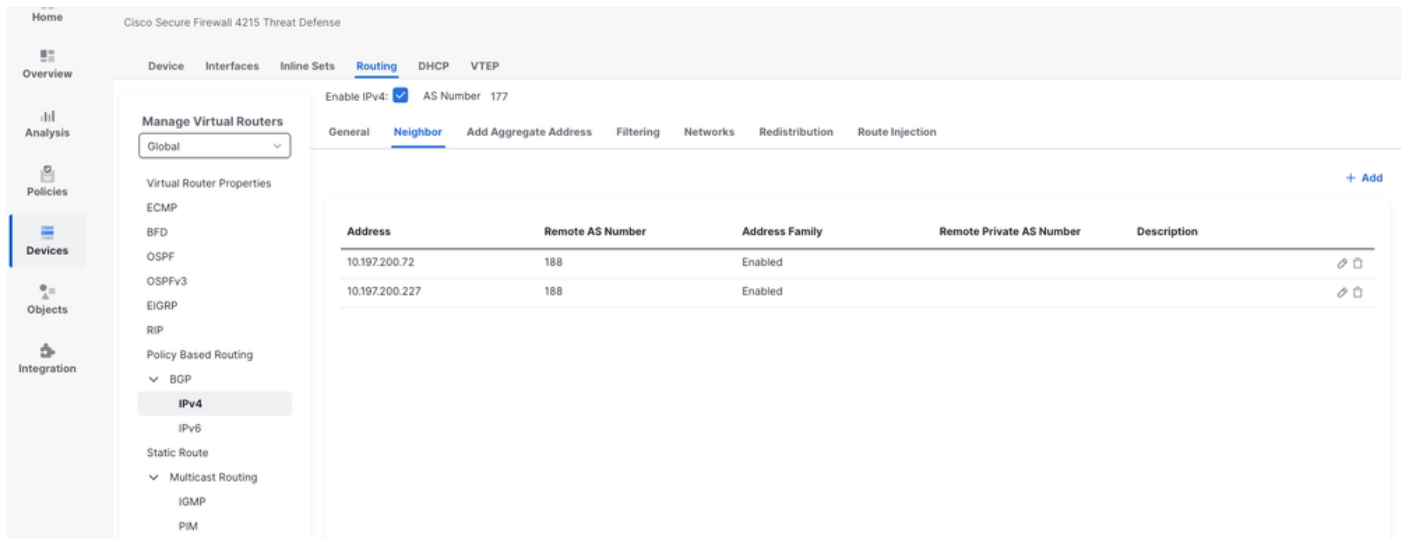
图解



网络图

BGP配置

启用后，导航到Devices > Device management > Edit Device > Routing > BGP > IPv4以配置BGP。



BGP配置

LINA中的BGP配置：

```
router bgp 177
  bgp log-neighbor-changes
  bgp router-id 1.1.x.x
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.197.200.72 remote-as 188
    neighbor 10.197.200.72 transport path-mtu-discovery disable
    neighbor 10.197.200.72 activate
    neighbor 10.197.200.227 remote-as 188
    neighbor 10.197.200.227 transport path-mtu-discovery disable
    neighbor 10.197.200.227 activate
  no auto-summary
```

```
no synchronization
exit-address-family
!
```

来自同一AS的两个BGP邻居：

```
ftd1# show bgp summary
BGP router identifier 1.1.x.x, local AS number 177
BGP table version is 9, main routing table version 9
2 network entries using 400 bytes of memory
4 path entries using 320 bytes of memory
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 40 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 968 total bytes of memory
BGP activity 4/2 prefixes, 10/6 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.197.200.72	4	188	67	66	9	0	0	01:10:15	1
10.197.200.227	4	188	60	60	9	0	0	01:00:56	1

请注意，同一目的网络收到两条有效路由，每条路由来自一个邻居。

```
ftd1# show bgp 192.168.10.0 255.255.255.0
BGP routing table entry for 192.168.10.0/24, version 9
Paths: (2 available, best #2, table default)
  Advertised to update-groups: 3
  188 200
    10.197.200.227 from 10.197.200.227 (3.3.x.x)
      Origin incomplete, localpref 100, valid, external
  188 200
    10.197.200.72 from 10.197.200.72 (2.2.x.x)
      Origin incomplete, localpref 100, valid, external, best
```

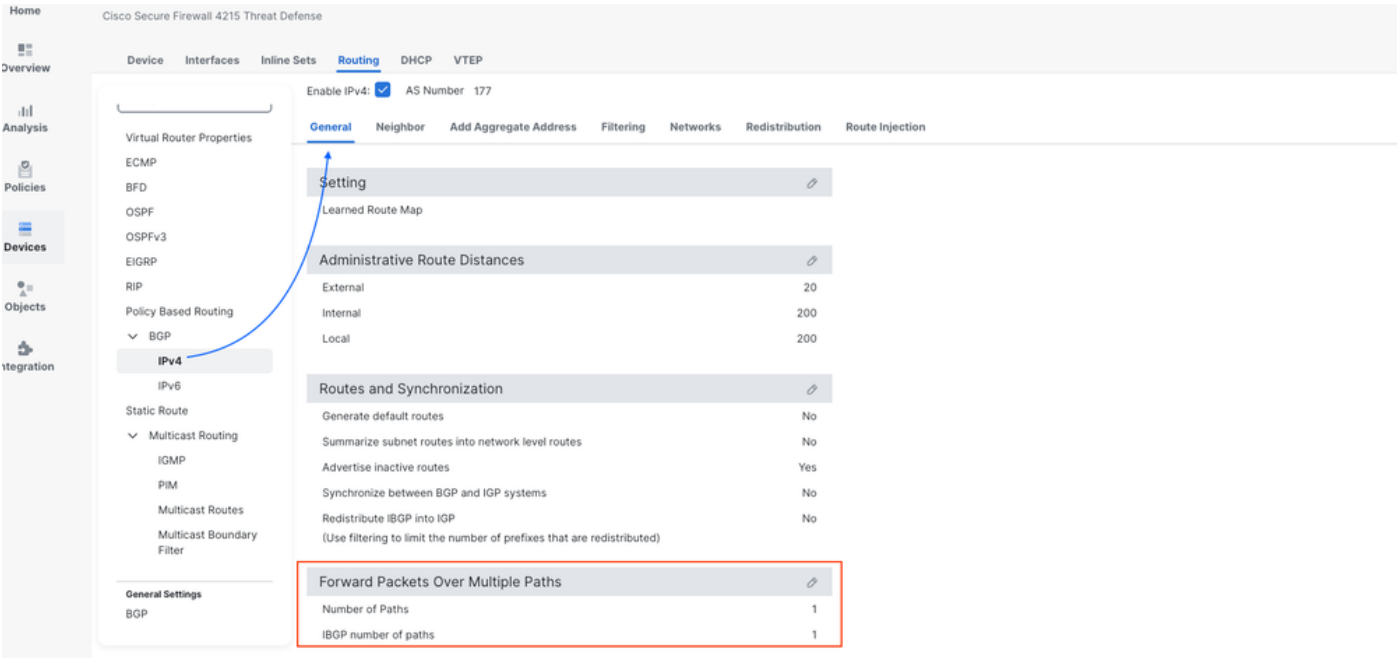
您可以看到，路由表中选定并安装的最佳路径是从邻居10.197.200.72接收的最佳路径。

```
ftd1# show route bgp
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

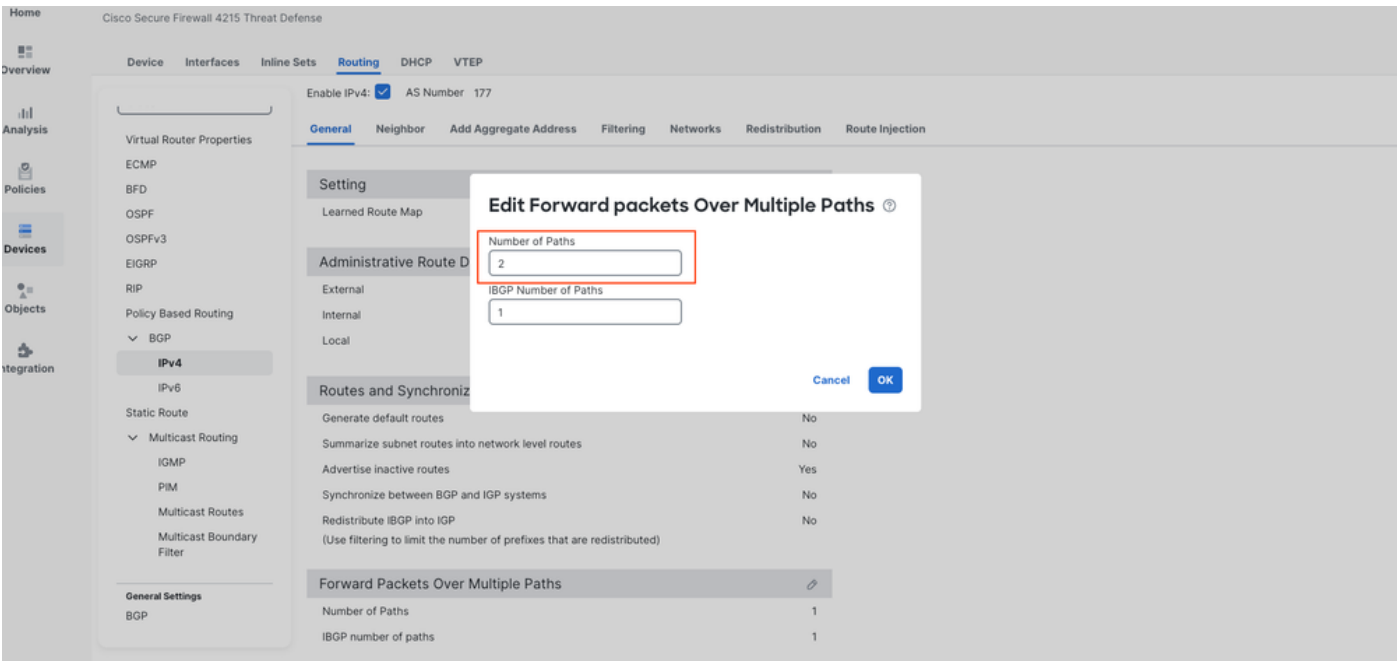
B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.72, 00:01:55
```

BGP多路径配置

在Devices > Device management > Edit Device > Routing > BGP > IPv4 > Edit Forward Packets Over Multiple Paths下配置BGP多路径。



FMC中的BGP多路径



FMC中的BGP多路径

保存更改并部署。

验证

启用多路径后来自LINA的BGP配置：

<#root>

```
ftd1# sh run router
router bgp 177
bgp log-neighbor-changes
bgp router-id 1.1.x.x
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 10.197.200.72 remote-as 188
neighbor 10.197.200.72 transport path-mtu-discovery disable
neighbor 10.197.200.72 activate
neighbor 10.197.200.227 remote-as 188
neighbor 10.197.200.227 transport path-mtu-discovery disable
neighbor 10.197.200.227 activate

maximum-paths 2
```

```
no auto-summary
no synchronization
exit-address-family
```

注意其中一个路由前的m，该路由表示多路径

<#root>

```
ftd1# show bgp

BGP table version is 11, local router ID is 1.1.x.x
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*m 192.168.10.0 10.197.200.227 0 188 200 ?

*> 10.197.200.72 0 188 200 ?

ftd1# show bgp 192.168.10.0 255.255.255.0
BGP routing table entry for 192.168.10.0/24, version 11
Paths: (2 available, best #2, table default)
Multipath: eBGP
Advertised to update-groups: 3
188 200
10.197.200.227 from 10.197.200.227 (3.3.x.x)
Origin incomplete, localpref 100, valid, external,

multipath

188 200
10.197.200.72 from 10.197.200.72 (2.2.x.x)
Origin incomplete, localpref 100, valid, external,
```

multipath

, best

请注意，启用BGP多路径后，路由表中现在安装有两个通往同一目标的路由。

<#root>

```
ftd1# show route bgp
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
```

B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.227, 00:01:17

[20/0] via 10.197.200.72, 00:01:17

故障排除

1.验证BGP配置：

使用show bgp命令检查BGP表并确保将多个路径标记为多路径。

确认Number of Paths已配置为允许多个路径。

2.检查路径属性：

确保路径具有多路径所需的相等的BGP属性；如权重、本地优先级、AS路径长度等。

3.负载共享验证：

使用show route命令验证路径是否用于负载共享。输出应显示同一目的地的多条路径。

问题解答

1.FTD中是否通过Flex config支持用于负载共享的bgp bestpath as-path multipath-relax命令？

否，FTD/ASA中支持此功能的增强功能已就绪。Cisco Bug ID [CSCvw16654](#)

相关信息

常见BGP问题故障排除

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）。