

在安全防火牆威脅防禦中配置BGP多路徑

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[圖表](#)

[BGP組態](#)

[BGP多重路徑組態](#)

[驗證](#)

[疑難排解](#)

[問答](#)

[相關資訊](#)

簡介

本檔案介紹如何在思科安全防火牆威脅防禦中設定邊界閘道通訊協定(BGP)多重路徑。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆威脅防禦(FTD)上的BGP配置
- 一般BGP
- 思科安全防火牆管理中心(FMC)

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- Cisco FTD版本7.6
- Cisco FMC版本7.6

免責聲明：本文檔中引用的網路和IP地址未與任何單個使用者、組或組織關聯。此配置專為實驗室環境而建立。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文描述當從同一AS（例如，同一ISP）中的不同路由器收到到達同一目標的路由時，如何在Firepower威脅防禦中配置BGP多重路徑負載共用。

BGP多重路徑允許將到達同一目的地首碼的多個等價的BGP路徑安裝到IP路由表中。到達目的地首碼的流量接著在所有已安裝的路徑上共用。

出於負載共用目的，這些路徑會與最佳路徑一起新增到路由表中。BGP多重路徑不會影響選擇最佳路徑的流程。例如，FTD仍會根據演算算法選擇一個路徑作為最佳路徑，並將此最佳路徑通告給其BGP對等路由器。

要有資格作為多重路徑的候選路徑，到達同一目標的路徑必須匹配以下特徵中的最佳路徑：

- 重量
- 本地優先使用程度
- AS-PATH 長度
- 原始代碼
- 多出口鑑別器(MED)

以下其中一項：

- 相鄰AS或子AS（在新增BGP多重路徑之前）
- AS-PATH（在新增BGP多重路徑之後）

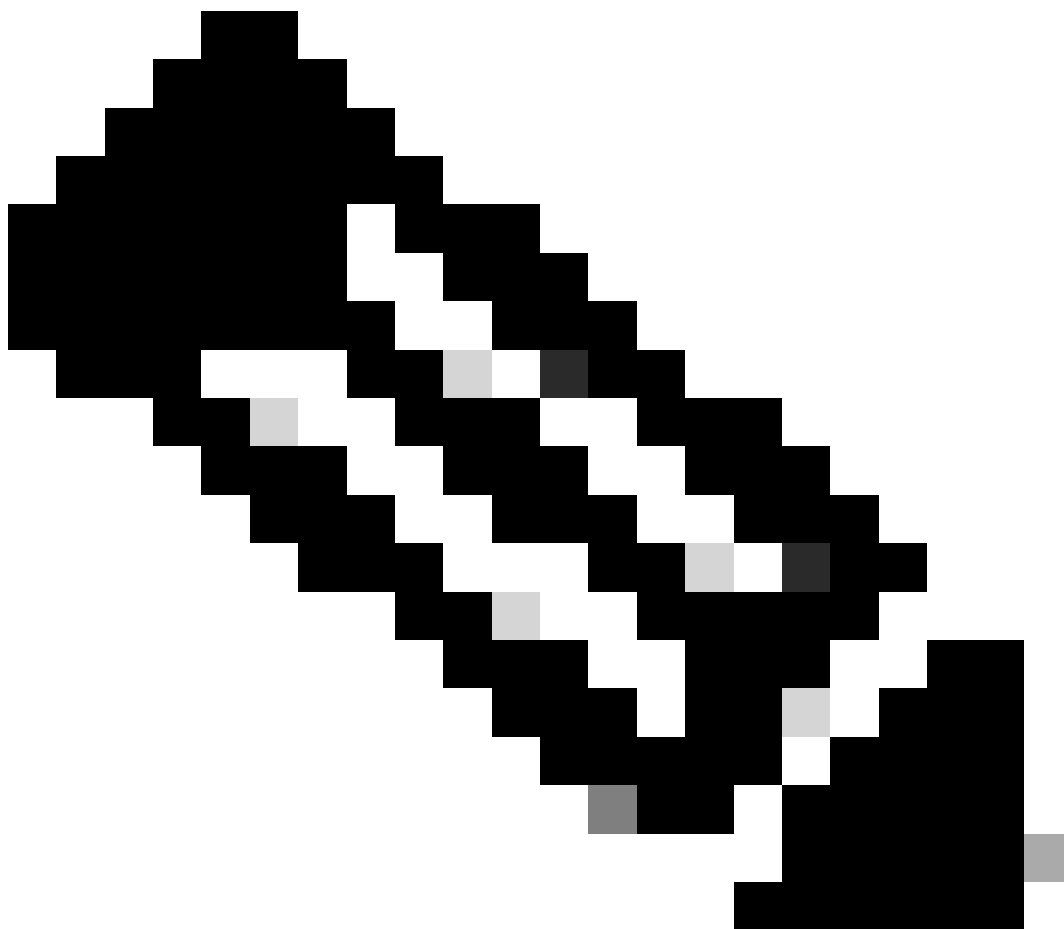
某些BGP多重路徑功能對多重路徑候選選項施加了進一步的需求：

- 路徑必須源自外部或聯盟外部鄰居(eBGP)。
- BGP下一躍點的IGP度量必須與最佳路徑的IGP度量匹配。

對於內部BGP(iBGP)多重路徑候選路徑，以下額外要求適用：

- 必須從內部鄰居(iBGP)得知該路徑。
- 除非路由器設定為不等價的iBGP多重路徑，否則BGP下一躍點的IGP指標必須與最佳路徑IGP指標相符。

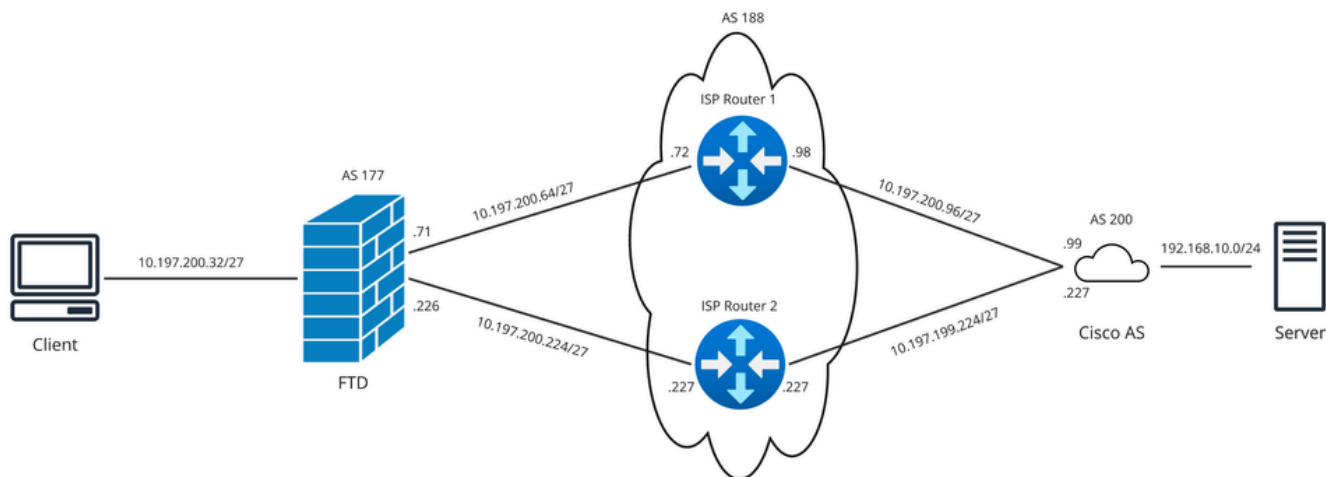
BGP最多可在IP路由表中插入n個最近從多重路徑候選路徑接收到的路徑，其中n是要安裝到路由表的路由數，這在配置BGP多重路徑時指定。FTD的n值範圍為1-8。當停用多重路徑時，預設值為1。



附註：從 eBGP 多重路徑中選取的最佳路徑會先執行等價的 next-hop-self，才會轉送到內部同儕節點。

設定

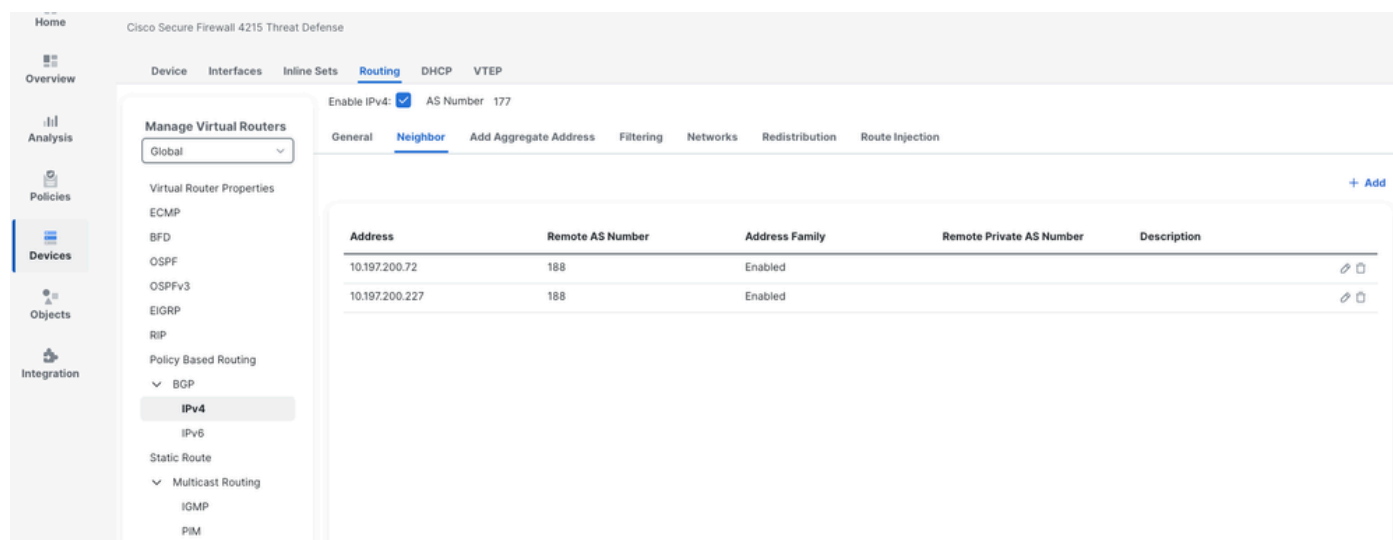
圖表



網路圖表

BGP組態

啟用後，導覽至Devices > Device management > Edit Device > Routing > BGP > IPv4以設定BGP。



BGP組態

來自LINA的BGP組態：

```

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
!
```

來自同一AS的兩個BGP鄰居：

```
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

請注意，同一目的網路收到兩條有效路由，每條路由來自一個鄰居。

```
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
```

您可以看到在路由表中選取並安裝的最佳路徑是從鄰居10.197.200.72接收的路徑。

```
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多重路徑組態

在Devices > Device management > Edit Device > Routing > BGP > IPv4 > Edit Forward Packets Over Multiple Paths下配置BGP多重路徑。

The screenshot shows the Cisco Secure Firewall 4215 Threat Defense configuration page. The left sidebar contains navigation options: Overview, Analysis, Policies, Devices, Objects, and Integration. The main content area is titled 'Cisco Secure Firewall 4215 Threat Defense' and includes tabs for Device, Interfaces, Inline Sets, Routing, DHCP, and VTEP. Under the 'Routing' tab, there are sub-tabs for General, Neighbor, Add Aggregate Address, Filtering, Networks, Redistribution, and Route Injection. The 'General' sub-tab is selected, and the 'BGP' section is expanded. The 'Forward Packets Over Multiple Paths' section is highlighted with a red box, showing the following configuration:

Setting	Value
Number of Paths	1
IBGP number of paths	1

FMC中的BGP多重路徑

The screenshot shows the Cisco Secure Firewall 4215 Threat Defense configuration page. The left sidebar contains navigation options: Overview, Analysis, Policies, Devices, Objects, and Integration. The main content area is titled 'Cisco Secure Firewall 4215 Threat Defense' and includes tabs for Device, Interfaces, Inline Sets, Routing, DHCP, and VTEP. Under the 'Routing' tab, there are sub-tabs for General, Neighbor, Add Aggregate Address, Filtering, Networks, Redistribution, and Route Injection. The 'General' sub-tab is selected, and the 'BGP' section is expanded. The 'Forward Packets Over Multiple Paths' section is highlighted with a red box, showing the following configuration:

Setting	Value
Number of Paths	2
IBGP Number of Paths	1

FMC中的BGP多重路徑

儲存變更並進行部署。

驗證

啟用多重路徑後來自LINA的BGP組態：

<#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
```

請注意其中一個路由前的m以指示多重路徑

<#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

請注意，啟用BGP多重路徑後，現在路由表中安裝有兩個通往同一目標的路由。

<#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
```

疑難排解

1.驗證BGP配置：

使用show bgp命令檢查BGP表，並確保將多個路徑標籤為多重路徑。

確認Number of Paths已設定為允許多個路徑。

2.檢查路徑屬性：

確保路徑具有多重路徑所需的相等BGP屬性；如權重、區域性優先選擇、AS路徑長度等。

3.負載共用驗證：

使用show route命令驗證路徑是否用於負載共用。輸出應顯示同一目標的多個路徑。

問答

1.透過Flex config在FTD中支援用於負載共用的bgp bestpath as-path multipath-relax命令嗎？

否，FTD/ASA中已存在支援此功能的增強功能。思科錯誤ID [CSCvw16654](#)

相關資訊

[解決常見BGP問題](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。