セキュアファイアウォール脅威対策におけるBGPマルチパスの設定

内容

はじめに

このドキュメントでは、Cisco Secure Firewall Threat DefenseでBorder Gateway Protocol(BGP)マルチパスを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Threat Defense(FTD)のBGP設定
- 一般的なBGP
- Cisco Secure Firewall Management Center(FMC)

使用するコンポーネント

このドキュメントの情報は、このソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FTDバージョン7.6
- Cisco FMCバージョン7.6

免責事項：このドキュメントで参照されているネットワークおよびIPアドレスは、個々のユーザ、グループ、または組織に関連付けられていません。この設定は、ラボ環境での使用のみを目的

として作成されています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、同じ宛先へのルートが同じAS内の異なるルータ（同じISPなど）から受信された場合に、Firepower Threat Defense(FTD)でBGPマルチパスロードシェアリングを設定する方法について説明します。

BGPマルチパスを使用すると、同じ宛先プレフィックスへの複数の等コストBGPパスをIPルーティングテーブルにインストールできます。宛先プレフィックスへのトラフィックは、インストールされたすべてのパスで共有されます。

これらのパスは、ロードシェアリング用のベストパスとともにルーティングテーブルに追加されます。BGPマルチパスは、ベストパスの選択プロセスに影響しません。たとえば、FTDはアルゴリズムに基づいて1つのパスをベストパスとして選択し、このベストパスをBGPピアにアドバタイズします。

マルチパスの候補として認定されるには、同じ宛先へのパスが次の特性のベストパスと一致する必要があります。

- 重量
- Local preference
- AS-PATH length
- 元のコード
- Multi Exit Discriminator(MED)

次のいずれか：

- ネイバーASまたはサブAS（BGPマルチパス追加前）
- AS-PATH（BGPマルチパスの追加後）

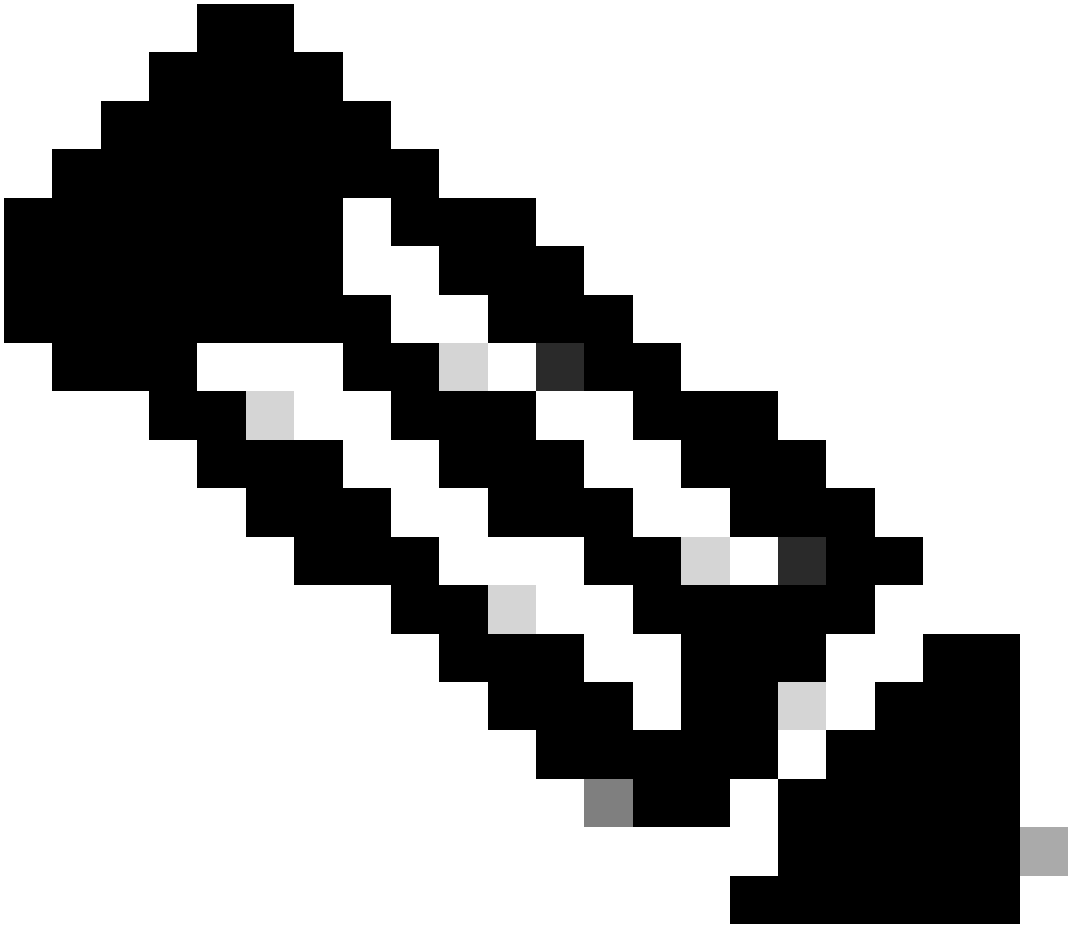
特定のBGPマルチパス機能により、マルチパス候補にさらに要件が課せられます。

- パスは、外部またはコンフェデレーション外部ネイバー(eBGP)から発信される必要があります。
- BGPネクストホップへのIGPメトリックは、ベストパスのIGPメトリックと一致する必要があります。

内部BGP(iBGP)マルチパス候補には、次の追加要件が適用されます。

- パスは内部ネイバー（iBGP）から学習される必要があります。
- ルータに不等コストiBGPマルチパスが設定されていない限り、BGPネクストホップへのIGPメトリックは、最適パスのIGPメトリックと一致している必要があります。

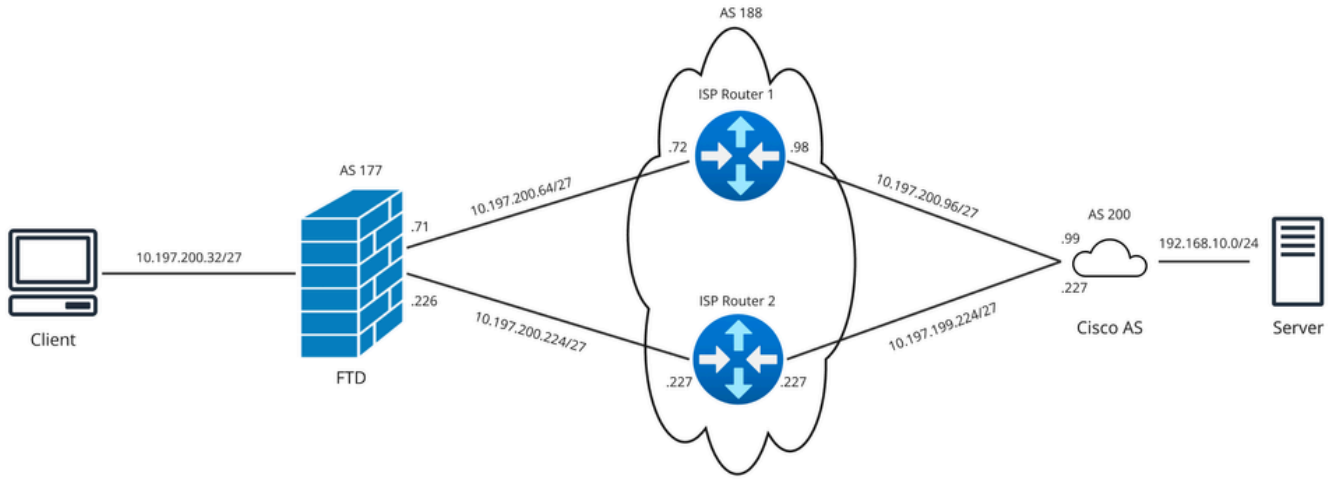
BGPは、マルチパス候補から最近受信した、最大n個のパスをIPルーティングテーブルに挿入します。ここで、nは、BGP Multipathの設定時に指定された、ルーティングテーブルにインストールされるルートの数です。nの値の範囲は、FTDでは1 ~ 8です。マルチパスがディセーブルになっている場合のデフォルト値は 1 です。



注：内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対して同等の next-hop-self が実行されます。

設定

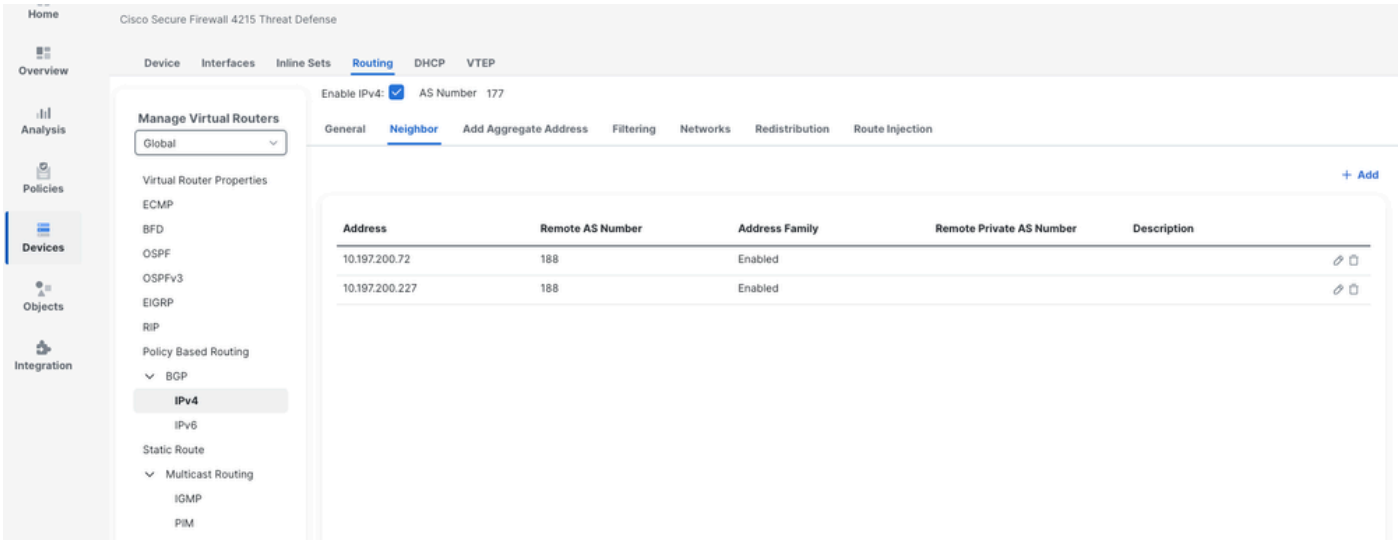
図



ネットワーク図

BGPの設定

イネーブルにした後でBGPを設定するには、Devices > Device management > Edit Device > Routing > BGP > IPv4の順に選択します。



BGPの設定

LINAからのBGP設定：

```
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
!
```

同じASからの2つのBGPネイバー：

```
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
```

同じ宛先ネットワークに対して受信した2つの有効なルートが各ネイバーから1つずつあることに注意してください。

```
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
```

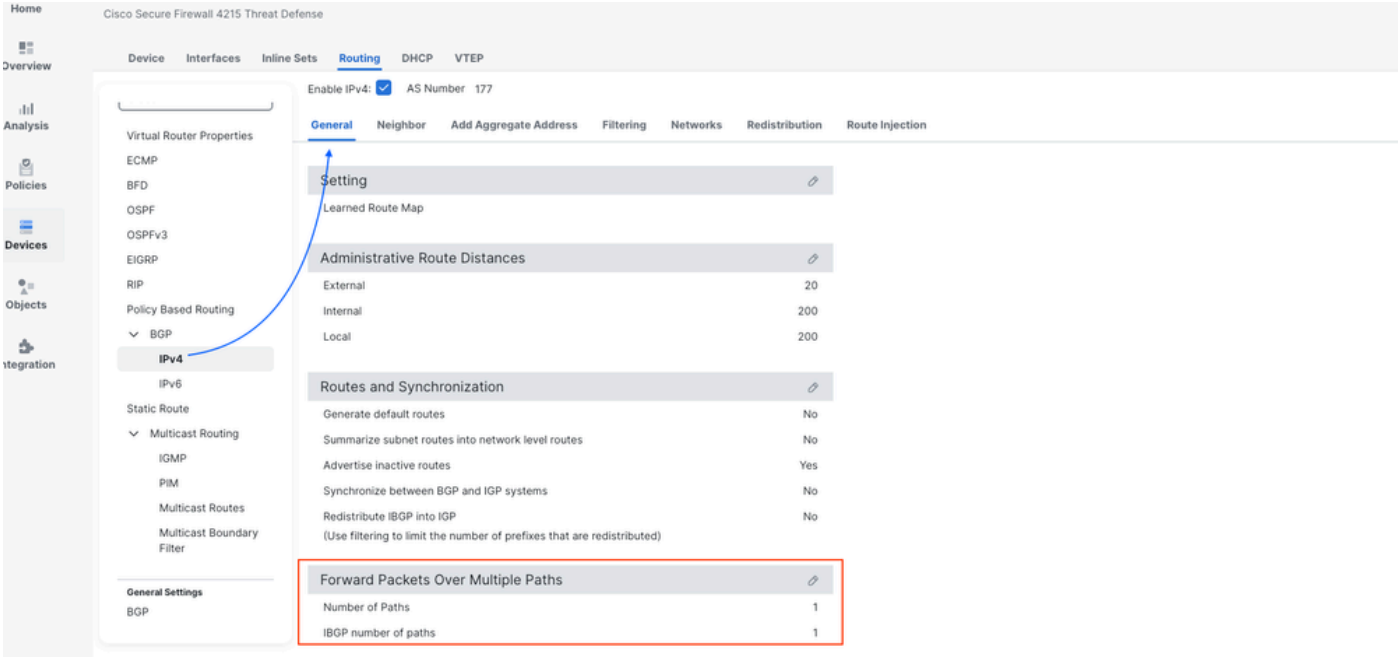
ルーティングテーブルで選択されてインストールされたベストパスは、ネイバー10.197.200.72から受信したパスであることがわかります。

```
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
```

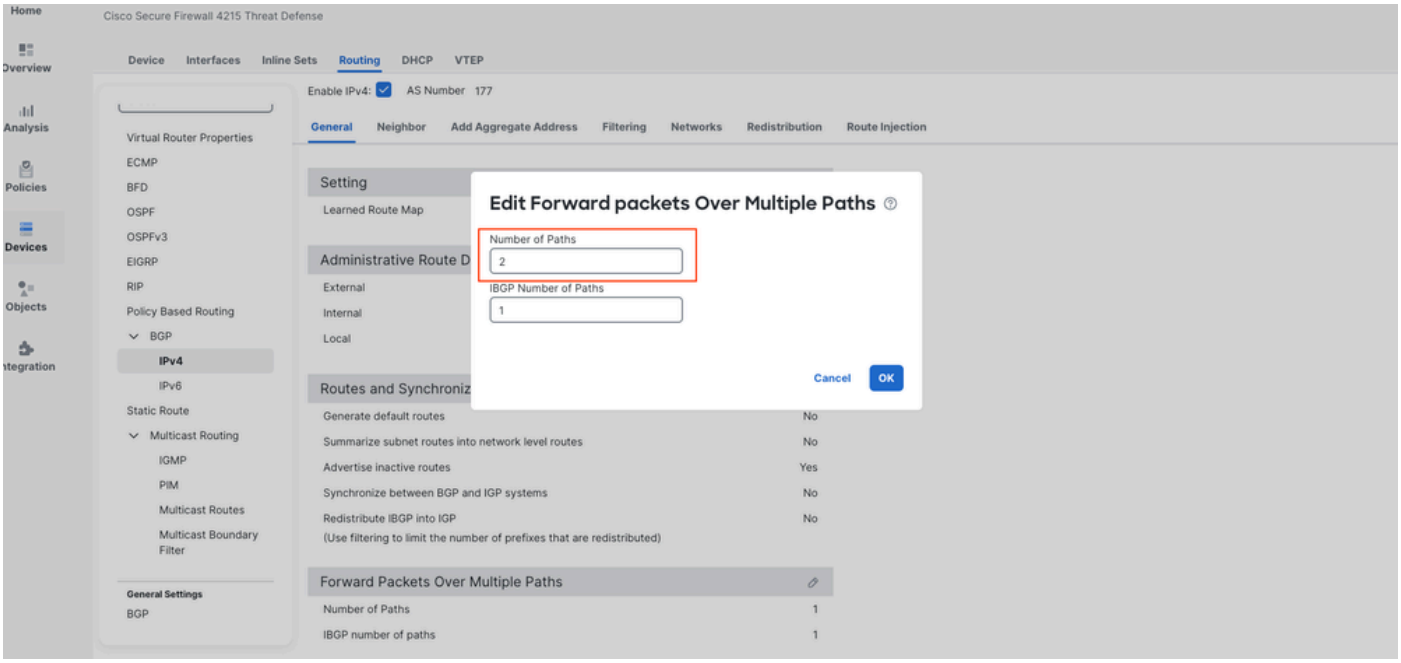
```
Gateway of last resort is not set

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

BGPマルチパス設定

Devices > Device management > Edit Device > Routing > BGP > IPv4 > Edit Forward Packets Over Multiple Pathsの順に選択して、BGPマルチパスを設定します。



FMCでのBGPマルチパス



FMCでのBGPマルチパス

変更を保存して展開します。

確認

マルチパスを有効にした後のLINAからのBGP設定：

<#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
```

ルートの1つの前にあるmは、マルチパスを示しています

<#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
```

BGPマルチパスを有効にした後、同じ宛先への2つのルートがルーティングテーブルにインストールされていることに注意してください。

<#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

トラブルシュート

1. BGP設定を確認します。

show bgpコマンドを使用してBGPテーブルをチェックし、複数のパスがマルチパスとしてマーキングされていることを確認します。

Number of Pathsがマルチパスを許可するように設定されていることを確認します。

2. パス属性の確認：

マルチパスに必要な等しいBGPアトリビュート（weight、local preference、AS Path Lengthなど）がパスにあることを確認します。

3. ロードシェアリングの検証：

show routeコマンドを使用して、パスがロードシェアリングに使用されていることを確認します。出力には、同じ宛先に対する複数のパスが表示されるはずです。

Q&A

1. ロードシェアリング用のFlex Config経由のFTDでは、コマンドbgp bestpath as-path multipath-relaxがサポートされていますか。

いいえ、FTD/ASAでこれをサポートするための機能拡張がすでに行われています。Cisco Bug ID CSCvw16654

関連情報

一般的なBGP問題のトラブルシューティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。