

Configurer le protocole BGP par trajets multiples dans Secure Firewall Threat Defense

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme](#)

[Configuration BGP](#)

[Configuration multichemin BGP](#)

[Vérifier](#)

[Dépannage](#)

[Q&R](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer le protocole BGP (Border Gateway Protocol) Multipath dans Cisco Secure Firewall Threat Defense.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration BGP sur Cisco Secure Firewall Threat Defense (FTD)
- BGP général
- Cisco Secure Firewall Management Center (FMC)

Composants utilisés

Les informations contenues dans ce document sont basées sur la version logicielle et matérielle suivante :

- Cisco FTD version 7.6
- Cisco FMC version 7.6

Avertissement : Les réseaux et les adresses IP référencés dans ce document ne sont associés à

aucun utilisateur, groupe ou organisation individuel. Cette configuration a été créée exclusivement pour une utilisation dans un environnement de travaux pratiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit comment configurer le partage de charge multichemin BGP dans Firepower Threat Defense quand une route vers la même destination est reçue de différents routeurs dans le même AS (Par exemple, le même FAI).

BGP Multipath permet l'installation dans la table de routage IP de plusieurs chemins BGP à coût égal vers le même préfixe de destination. Le trafic vers le préfixe de destination est ensuite partagé entre tous les chemins installés.

Ces chemins sont ajoutés à la table de routage en même temps que le meilleur chemin à des fins de partage de charge. BGP Multipath n'influence pas le processus de sélection du meilleur chemin. Par exemple, un FTD sélectionne toujours un chemin comme le meilleur en fonction de l'algorithme et annonce ce meilleur chemin à ses homologues BGP.

Pour être admissibles en tant que candidats pour le multichemin, les chemins vers la même destination doivent correspondre au meilleur chemin dans les caractéristiques suivantes :

- Poids
- Préférence locale
- Longueur AS-PATH (CHEMIN-AS)
- Code origine
- Discriminateur de sortie multiple (MED)

L'un des éléments suivants :

- AS ou sous-AS voisin (avant l'ajout de trajets multiples BGP)
- AS-PATH (suite à l'ajout de trajets multiples BGP)

Certaines fonctionnalités BGP Multipath imposent des exigences supplémentaires aux candidats multipath :

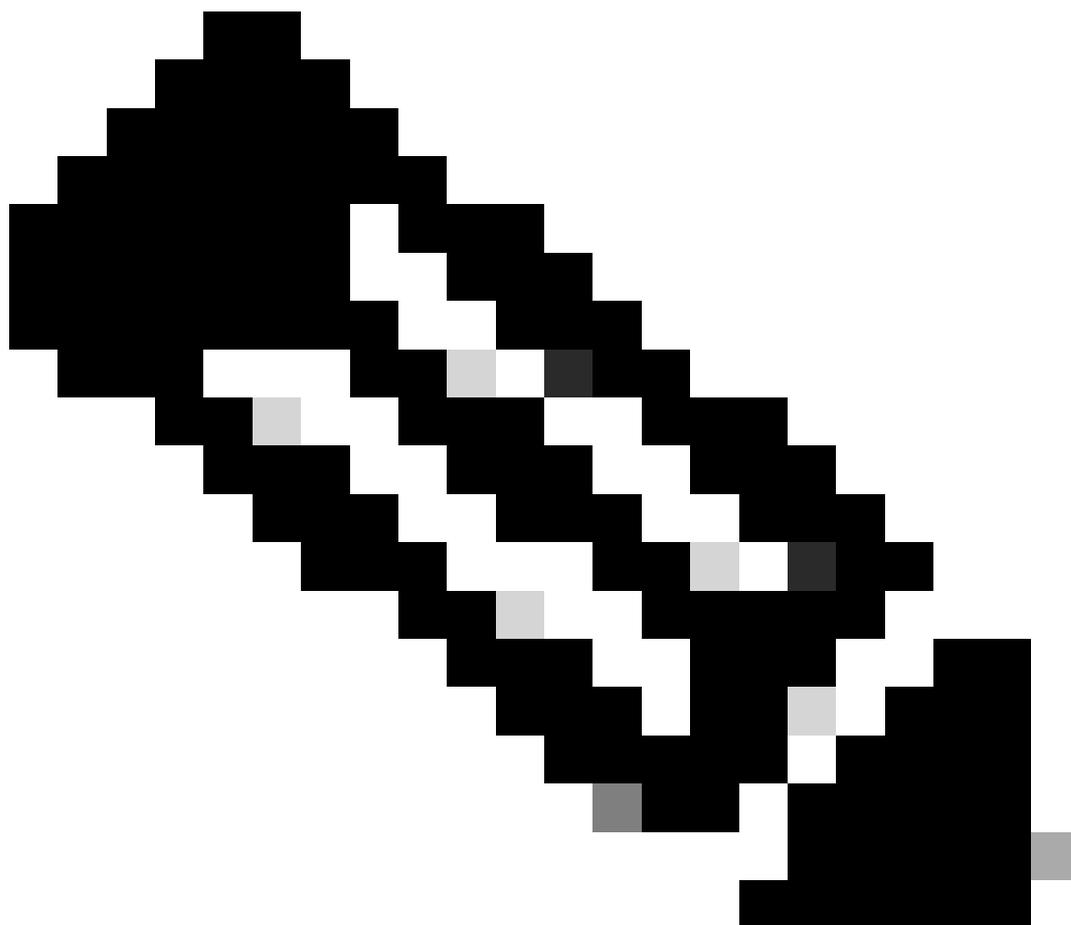
- Le chemin doit provenir d'un voisin externe ou d'un voisin externe de confédération (eBGP).
- La métrique IGP vers le tronçon suivant BGP doit correspondre à la métrique IGP du meilleur chemin.

Pour les candidats à trajets multiples BGP internes (iBGP), ces exigences supplémentaires s'appliquent :

- Le chemin doit être appris d'un voisin interne (iBGP).
- La métrique IGP vers le prochain saut BGP doit correspondre aux meilleurs chemins de la

métrique IGP, sauf si le routeur est défini pour le multichemin iBGP à coût inégal.

Le protocole BGP insère jusqu'à n chemins récemment reçus des candidats à chemins multiples dans la table de routage IP, où n est le nombre de routes à installer dans la table de routage, comme spécifié lorsque vous configurez le protocole BGP à chemins multiples. La plage de valeurs pour n est comprise entre 1 et 8 pour FTD. La valeur par défaut, si les trajets multiples sont désactivés, est de 1.



Remarque : Le prochain auto-saut équivalent est exécuté sur le meilleur chemin qui est sélectionné parmi des trajets multiples d'eBGP avant qu'il soit expédié aux partenaires internes.

Configurer

Diagramme

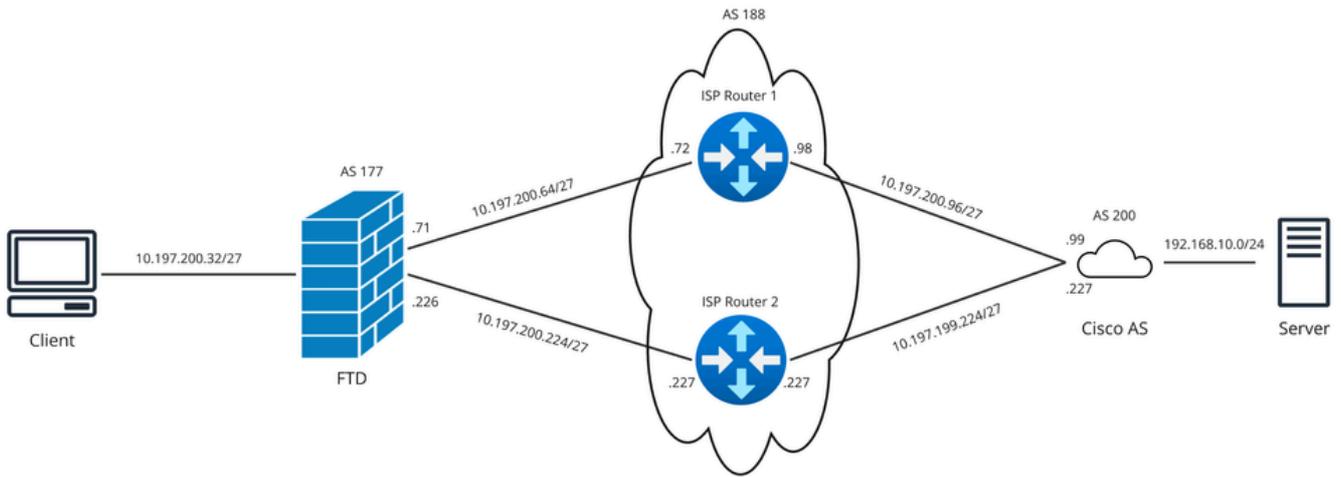


Diagramme du réseau

Configuration BGP

Accédez à **Devices > Device management > Edit Device > Routing > BGP > IPv4** pour configurer BGP après l'avoir activé.

The screenshot shows the configuration page for BGP IPv4 on a Cisco Secure Firewall 4215 Threat Defense. The interface includes a sidebar with navigation options and a main configuration area.

Virtual Router Properties:

- ECMP
- BFD
- OSPF
- OSPFv3
- EIGRP
- RIP
- Policy Based Routing
- BGP (selected)
- IPv4 (selected)
- IPv6
- Static Route
- Multicast Routing
- IGMP
- PIM

Neighbor Configuration Table:

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
10.197.200.72	188	Enabled		
10.197.200.227	188	Enabled		

Configuration BGP

Configuration BGP à partir de LINA :

```
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
!
```

Deux voisins BGP du même AS :

```
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

Notez qu'il existe deux routes valides reçues pour le même réseau de destination, une de chaque voisin.

```
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
```

Vous pouvez voir que le meilleur chemin sélectionné et installé dans la table de routage est celui qui est reçu du voisin 10.197.200.72.

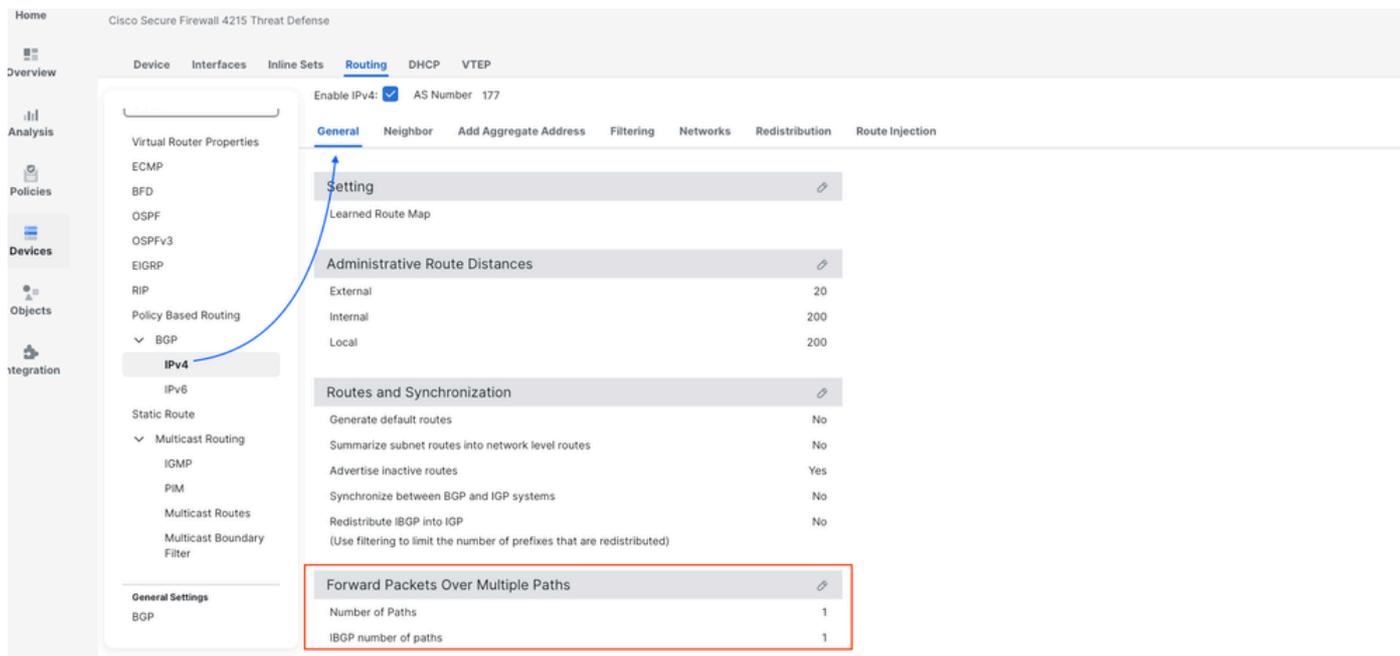
```
ftd1# show route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - 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

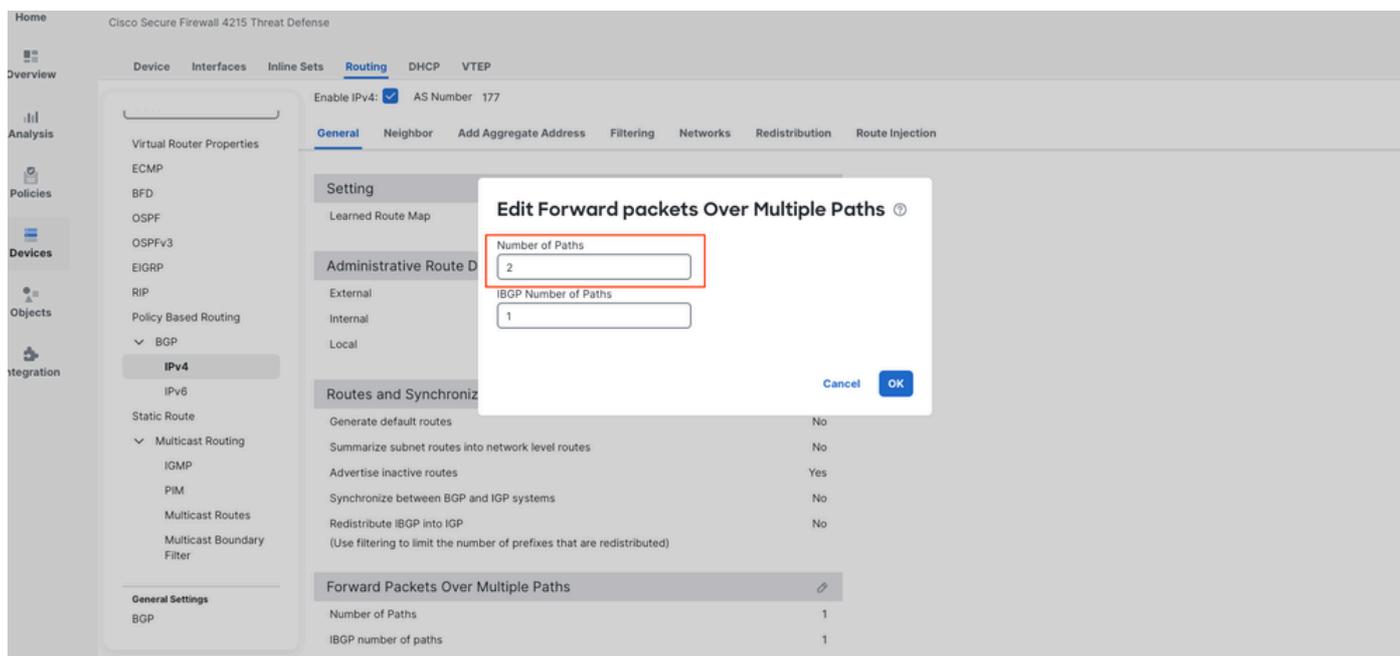
B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.72, 00:01:55

Configuration multichemin BGP

Configurez le multichemin BGP sous Périphériques > Gestion des périphériques > Modifier le périphérique > Routage > BGP > IPv4 > Modifier Transférer les paquets sur plusieurs chemins.



Multichemin BGP dans FMC



Multichemin BGP dans FMC

Enregistrez les modifications et déployez.

Vérifier

Configuration BGP à partir de LINA après l'activation de multipath :

```
<#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
```

Remarquez le m avant l'une des routes indiquant le multichemin

```
<#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
```

Notez que, maintenant, deux routes vers la même destination sont installées dans la table de routage après l'activation du multichemin BGP.

<#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
```

Dépannage

1. Vérifiez la configuration BGP :

Utilisez la commande `show bgp` pour vérifier la table BGP et vous assurer que plusieurs chemins sont marqués comme multichemins.

Vérifiez que Nombre de chemins est configuré pour autoriser plusieurs chemins.

2. Vérifier les attributs de chemin :

Assurez-vous que les chemins ont les mêmes attributs BGP requis pour le multichemin ; comme le poids, la préférence locale, la longueur du chemin AS, etc.

3. Vérification du partage de charge :

Utilisez la commande `show route` pour vérifier que les chemins sont utilisés pour le partage de charge. Le résultat doit indiquer plusieurs chemins pour la même destination.

Q&R

1. La commande `bgp bestpath as-path multipath-relax` est-elle prise en charge dans FTD via FlexConfig pour le partage de charge ?

Non, une amélioration est déjà en place pour cette prise en charge dans FTD/ASA. ID de bogue Cisco [CSCvw16654](#)

Informations connexes

[Dépannage des problèmes courants du protocole BGP](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.