

Configurer le routage BGP avec des limitations de reconfiguration logicielle sur FTD

Table des matières

[Problème](#)

[Environnement](#)

[Résolution](#)

[Limites des fonctionnalités](#)

[Approche alternative \(fonctionnalité d'actualisation de route\)](#)

[Motif](#)

[Autres informations utiles](#)

- [Problème](#)
 - [Environnement](#)
 - [Résolution](#)
 - [Limites des fonctionnalités](#)
 - [Approche alternative \(fonctionnalité d'actualisation de route\)](#)
 - [Motif](#)
 - [Autres informations utiles](#)
-

Problème

Lorsqu'un utilisateur tente de configurer la reconfiguration logicielle BGP (Border Gateway Protocol) sur un homologue BGP dans Firewall Threat Defense (FTD) à l'aide de Firewall Management Center (FMC), la configuration ne peut pas être effectuée via l'interface BGP FMC standard. En outre, les tentatives d'implémentation de cette fonctionnalité à l'aide d'objets FlexConfig entraînent des erreurs lors de la saisie de texte pour diverses parties de la commande de reconfiguration logicielle BGP neighbor. La condition spécifique est d'activer la reconfiguration logicielle entrante sur les voisins BGP pour stocker les routes reçues à des fins d'évaluation de la politique et de dépannage.

Environnement

- Matériel : Secure Firewall 3100. D'autres plates-formes matérielles sont également

concernées.

- le logiciel Cisco IOS: FTD (cette limitation s'applique également aux appareils de sécurité adaptatifs (ASA)).
- FMC version 7.4.6. D'autres versions logicielles sont également affectées.
- FTD version 7.4.6. Les autres versions logicielles sont également affectées.
- FTD a une configuration de protocole de routage BGP.

Résolution

Au moment de cet écriture, la reconfiguration logicielle entrante de voisin BGP classique (commande BGP neighbor x.x.x.x soft-reconfiguration inbound) n'est pas prise en charge sur les périphériques FTD, soit par l'interface utilisateur BGP FMC, soit comme méthode FlexConfig prise en charge.

Limites des fonctionnalités

Ces fonctionnalités de reconfiguration logicielle BGP ne sont pas disponibles :

- La configuration BGP FMC ne fournit pas d'option de configuration pour la reconfiguration logicielle entrante du voisin.
- La tentative de configuration de l'interface de ligne de commande équivalente via FlexConfig échoue car il ne s'agit pas d'un élément de configuration BGP géré par FTD/FMC pris en charge.

Approche alternative (fonctionnalité d'actualisation de route)

FTD ne prend pas en charge la fonctionnalité d'actualisation de route BGP lorsqu'elle est négociée avec des homologues BGP. Cela fournit le mécanisme pris en charge pour le comportement de réinitialisation logicielle dynamique après des modifications de stratégie, bien qu'il diffère de la fonctionnalité entrante de reconfiguration logicielle classique.

L'approche recommandée inclut :

- Poursuivez la configuration des voisins BGP, des listes de préfixes, des mappages de route et du filtrage via le workflow de configuration BGP pris en charge par FMC.
- Confirmez que les homologues BGP négocient la capacité d'actualisation de route :

<#root>

device#

show bgp neighbors 192.0.2.2

```
BGP neighbor is 192.0.2.2, context single_vf, remote AS 65535, internal link
BGP version 4, remote router ID 192.0.2.2
BGP state = Established, up for 00:17:39
Last read 00:00:31, last write 00:00:31, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
  1 active, is not multisession capable (disabled)
Neighbor capabilities:
```

Route refresh: advertised and received(new)

```
<----- BGP Route Refresh capability is enabled on both peers
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Multisession Capability:
Message statistics:
  InQ depth is 0
  OutQ depth is 0
```

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	3
Keepalives:	17	20

Route Refresh: 1 0

```
<----- The neighbor sent 1 BGP Route Refresh message
Total:                      20                      24
```

- Utilisez le comportement Actualisation de route pour la réévaluation des stratégies au lieu d'essayer d'activer la reconfiguration logicielle entrante, par exemple :

<#root>

device#

`clear bgp 192.0.2.2 in`

- Pour les exigences opérationnelles pour auditer toutes les routes reçues et rejetées, vérifiez du côté de l'homologue/routeur BGP.

Comparaison

Fonctionnalité	Fonctionnalité d'actualisation de route BGP	Reconfiguration logicielle entrante
Pris en charge sur FTD/ASA	Oui	Non
Comment ça fonctionne	Le routeur envoie un message de demande d'actualisation de route BGP explicite au voisin, lui demandant d'annoncer à nouveau sa table de routage.	Le routeur alloue de la mémoire vive supplémentaire pour enregistrer une copie brute non filtrée de la table BGP du voisin dans la mémoire locale.
Configuration requise	Aucune. Activé automatiquement par défaut sur FTD et ASA.	Configuration manuelle requise (voisin x.x.x.x soft-reconfiguration inbound), mais la commande n'est pas prise en charge sur FTD/ASA.
Consommation de mémoire	Extrêmement faible. Aucune table de routage supplémentaire n'est stockée dans la mémoire vive.	Très haut. Consomme beaucoup plus de mémoire pour les chemins de ce voisin.
Commande Trigger	<code># clear bgp x.x.x.x in</code>	Non pris en charge sur ASA/FTD.
Dépendance du voisin	Oui. L'homologue BGP distant doit également prendre en charge et accepter la fonctionnalité d'actualisation de route.	Non. Il est complètement local au pare-feu ; le voisin homologue ne sait pas qu'il est activé.
commande : <code>show bgp neighbor x.x.x.x received-routes</code>	Non pris en charge / Échec. Le routeur ne stocke pas de copie locale. L'exécution de cette commande renvoie	Pris en charge. Affiche instantanément les routes brutes et non filtrées actuellement mises en

	une erreur (% reconfiguration logicielle entrante non activée sur x.x.x.x).	cache dans la mémoire vive du routeur avant l'application des stratégies.
--	---	---

Motif

Il s'agit d'une limitation de fonctionnalité sur les périphériques FTD et ASA. La fonctionnalité de reconfiguration logicielle entrante du voisin BGP n'a pas été implémentée dans l'interface de configuration BGP du FMC ou en tant qu'option FlexConfig prise en charge pour les périphériques FTD. Cette limitation est suivie comme une amélioration logicielle Cisco bug ID [CSCvy97220](#).

Autres informations utiles

- [Guide de configuration BGP FMC \(10.x\)](#)
- [Référence des commandes FTD pour le voisin BGP et visibilité résumée](#)
- [ID de bogue Cisco CSCvy97220 - Demande d'amélioration pour la prise en charge de la reconfiguration logicielle entrante du voisin BGP](#)
- [Assistance technique de Cisco et téléchargements](#)

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.