Changement de comportement pour l'annonce de route VPN dans BGP à partir de 7.1

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Informations générales](#)

[Changement De Comportement](#)

[Configuration](#)

[Scénario d'impact](#)

[Contourner](#)

Introduction

Ce document décrit le changement de comportement de l'injection de route VPN dans la table de routage BGP à partir de la version 7.1.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower
- Connaissances sur la configuration de BGP et l'annonce de route

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)

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

La condition requise est d'annoncer les routes VPN sur BGP.

Les routes VPN sont filtrées à l’aide de critères de correspondance de tronçon suivant.

La liste de contrôle d’accès standard est configurée pour correspondre à un tronçon suivant 0.0.0.0.

Changement De Comportement

Dans la version 6.6.5, les routes VPN sont injectées dans la table de routage BGP avec le saut suivant défini sur 0.0.0.0.

Dans la version 7.1, les routes VPN sont injectées dans la table de routage BGP avec le saut suivant défini comme adresse IP réseau du sous-réseau correspondant.

Configuration

Configuration BGP :

```
router bgp 12345
 bgp log-neighbor-changes
 bgp router-id vrf auto-assign
 address-family ipv4 unicast
  neighbor 172.30.0.21 remote-as 12346
  neighbor 172.30.0.21 description CISCO-FTD-B
  neighbor 172.30.0.21 transport path-mtu-discovery disable
  neighbor 172.30.0.21 timers 10 40
  neighbor 172.30.0.21 fall-over bfd
  neighbor 172.30.0.21 ha-mode graceful-restart
  neighbor 172.30.0.21 activate
  neighbor 172.30.0.21 send-community
  neighbor 172.30.0.21 route-map VPN_INSIDE_IN in
  neighbor 172.30.0.21 route-map VPN_INSIDE_OUT out
  redistribute static
  redustribute connected
  no auto-summary
  no synchronization
 exit-address-family
```

Configuration de la carte de routage :

```
firepower# sh run route-map VPN_INSIDE_OUT

route-map VPN_INSIDE_PRI_OUT permit 10
 match ip next-hop NextHopZeroes

firepower# sh run access-list NextHopZeroes
access-list NextHopZeroes standard permit host 0.0.0.0
```

Avec cette configuration, BGP annonce uniquement les routes pour lesquelles le saut suivant est défini comme 0.0.0.0.

Installation des routes VPN dans la table de routage :

```
firepower# sh route | inc 172.20.192
V 172.20.192.0 255.255.252.0 connected by VPN (advertised), VPN-OUTSIDE
```

Résultat de la commande show bgp :

Dans la version 6.6.5

```
show bgp :
*> 172.20.192.0/22 0.0.0.0 0 32768 ?
```

On peut voir que le sous-réseau 172.20.192.0/22 est installé dans la table BGP avec l'IP de tronçon suivant définie comme 0.0.0.0.

Dans la version 7.1

```
show bgp :
*> 172.20.192.0/22 172.20.192.0 0 32768 ?
```

On peut voir que le sous-réseau 172.20.192.0/22 est installé dans la table BGP avec l'IP de tronçon suivant définie comme l'IP de réseau de sous-réseau : 172.20.192.0 .

Scénario d'impact

Si la configuration inclut une route-map définie pour correspondre à une adresse IP de tronçon suivant de 0.0.0.0, le filtrage de route est affecté et les routes VPN ne sont pas annoncées.

Contourner

Deux solutions de contournement :

1. Créez une liste de tous les sous-réseaux VPN et configurez-les individuellement pour

l'annonce sur BGP. Remarque : Cette méthode n'est pas évolutive.

2. Configurez BGP pour annoncer les routes générées localement. Appliquez cette commande de configuration :

```
route-map <route-map-name> permit 10
match route-type local
```

En mettant en oeuvre l'une des solutions décrites précédemment, FTD annonce les routes injectées par VPN via 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.