Bloquez un ou plusieurs réseaux d'un pair BGP

Contenu

Introduction

Le filtrage de route est la base par laquelle les stratégies de Border Gateway Protocol (BGP) sont définies. Il y a nombre de manières de filtrer un ou plusieurs réseaux d'un pair BGP, y compris les informations d'accessibilité des couches réseau (NLRI) et AS_Path et attributs de Community. Ce document discute du filtrage basé sur NLRI seulement. Pour les informations sur la façon de filtrer basé sur AS_Path, référez-vous à l'utilisation des expressions régulières dans BGP. Pour des informations complémentaires, référez-vous à la section de filtrage BGP sur les études de cas de BGP.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la configuration BGP de base. Le pour en savoir plus, se rapportent à des études de cas de BGP et BGP de configurer.

Composants utilisés

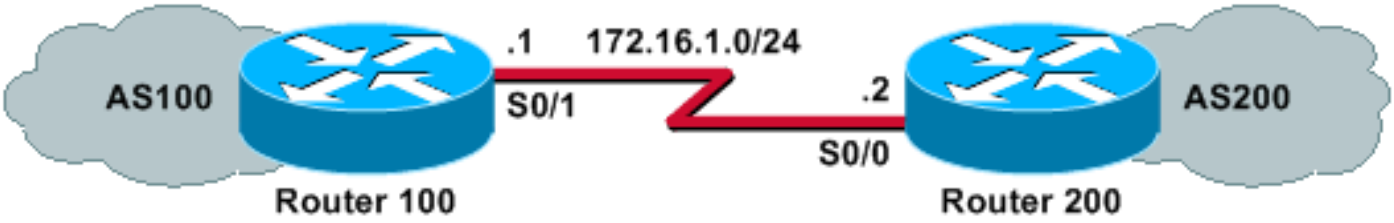
Les informations dans ce document sont basées sur la version de logiciel 12.2(28) de Cisco IOS®.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Artères les identifiant et de filtrages basées sur NLRI

Pour limiter les informations de routage que le routeur apprend ou annonce, vous pouvez utiliser des filtres basés sur des mises à jour de routage. Les filtres se composent d'une liste d'accès ou d'une liste de préfixes, qui est appliquée aux mises à jour aux voisins et des voisins. Ce document explore ces options avec ce schéma de réseau :

Diagramme du réseau



Filtrage utilisant la distribute-list avec une liste d'accès standard

Le routeur 200 annonce ces réseaux à son routeur 100 de pair :

- 192.168.10.0/24
- 10.10.10.0/24
- 10.10.0.0/19

Ce routeur 100 d'enables de configuration d'échantillon pour refuser une mise à jour pour le réseau 10.10.10.0/24 et pour permettre les mises à jour des réseaux 192.168.10.0/24 et 10.10.0.0/19 dans sa table BGP :

Routeur 100

```
hostname Router 100
!
router bgp 100
neighbor 172.16.1.2 remote-as 200
neighbor 172.16.1.2 distribute-list 1 in
!
access-list 1 deny 10.10.10.0 0.0.0.255
access-list 1 permit any
```

Routeur 200

```
hostname Router 200
!
router bgp 200
no synchronization
network 192.168.10.0
network 10.10.10.0 mask 255.255.255.0
network 10.10.0.0 mask 255.255.224.0
no auto-summary
neighbor 172.16.1.1 remote-as 100
```

Cette sortie de commande de **show ip bgp** confirme les actions du routeur 100 :

```
Router 100# show ip bgp

BGP table version is 3, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.0.0/19     172.16.1.2               0             0 200 i
*> 192.168.10.0/24  172.16.1.2               0             0 200 i
```

Filtrage utilisant la distribute-list avec une liste d'accès étendue

Il peut être délicat pour employer une liste d'accès standard pour filtrer des supernets. Supposez que le routeur 200 annonce ces réseaux :

- 10.10.1.0/24 à 10.10.31.0/24

- 10.10.0.0/19 (son agrégat)

Souhaits du routeur 100 à uniquement récepteur le réseau agrégé, 10.10.0.0/19, et pour filtrer tous les réseaux spécifiques.

Une liste d'accès standard, telle que l'**autorisation 10.10.0.0 0.0.31.255 de la liste d'accès 1**, ne fonctionnera pas parce qu'elle laisse plus de réseaux que désirés. La liste d'accès standard regarde l'adresse réseau seulement et ne peut pas vérifier la longueur du masque de réseau. Cette liste d'accès standard permettra l'agrégat de /19 aussi bien que les réseaux plus spécifiques de /24.

Pour permettre seulement les super-réseaux 10.10.0.0/19, utilisez une liste d'accès étendue, telle que l'**IP 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0 d'autorisation de la liste d'accès 101**. Référez-vous à l'access-list (IP extended) pour le format de la commande de liste d'accès étendue.

Dans notre exemple, la source est 10.10.0.0 et le source-wildcard de 0.0.0.0 est configuré pour un précis - correspondance de source. Un masque de 255.255.224.0, et un masque-masque de 0.0.0.0 est configuré pour un précis - correspondance de masque de source. Si des aucuns d'entre eux (source ou masque) n'ont un précis - appariez, la liste d'accès la refuse.

Ceci permet la commande de liste d'accès étendue de permettre un précis - correspondance de network number 10.10.0.0 de source avec le masque 255.255.224.0 (et ainsi, 10.10.0.0/19). Les autres réseaux plus spécifiques de /24 seront filtrés.

> Remarque: En configurant des caractères génériques, **0** signifie qu'il est un précis - apparient le bit et **1** est un faire-non-soin-bit.

C'est la configuration sur le routeur 100 :

Routeur 100

```
hostname Router 100
  !
  router bgp 100
!--- Output suppressed.

   neighbor 172.16.1.2 remote-as 200
   neighbor 172.17.1.2 distribute-list 101 in
```

```
!
!
access-list 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0
```

La sortie de commande de **show ip bgp du** routeur 100 confirme que la liste d'accès fonctionne comme prévu.

```
Router 100# show ip bgp

BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.0.0/19     172.16.1.2               0             0 200 i
```

Comme vu dans cette section, il est plus commode l'utiliser les Listes d'accès étendues quand on doit permettre quelques réseaux et certains rejetés, dans le même principal réseau. Ces exemples fournissent plus de vue sur la façon dont une liste d'accès étendue peut aider dans certaines situations :

- **IP 192.168.0.0 0.0.0.0 255.255.252.0 0.0.0.0 d'autorisation de la liste d'accès 101**

  Cette liste d'accès permet seulement les super-réseaux 192.168.0.0/22.

- **IP 192.168.10.0 0.0.0.255 255.255.255.0 0.0.0.255 d'autorisation de la liste d'accès 102**

  Cette liste d'accès permet tous les sous-réseaux de 192.168.10.0/24. En d'autres termes, il permettra 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25, et ainsi de suite : réseaux 192.168.10.x l'uns des avec un masque qui s'étend de 24 à 32.

- **IP 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255 d'autorisation de la liste d'accès 103**

  Cette liste d'accès permet n'importe quel préfixe réseau avec un masque qui s'étend de 24 à 32.

Filtrage utilisant la commande d'ip prefix-list

Le routeur 200 annonce ces réseaux à son routeur 100 de pair :

- 192.168.10.0/24
- 10.10.10.0/24
- 10.10.0.0/19

Les configurations d'échantillon dans cette section utilisent la commande d'ip prefix-list, qui permet au routeur 100 de faire deux choses :

- Les mises à jour d'autorisation pour n'importe quel réseau avec un préfixe masquent la longueur inférieur ou égal à 19.
- Refusez toutes les mises à jour de réseau avec une longueur de masque de réseau plus grand que 19.

Routeur 100

```
Router 100# show ip bgp

BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.0.0/19     172.16.1.2               0             0 200 i
```

Routeur 200

```
Router 100# show ip bgp

BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.0.0/19     172.16.1.2               0             0 200 i
```

La sortie de commande de **show ip bgp** confirme que la liste de préfixes fonctionne comme prévu sur le routeur 100.

```
Router 100# show ip bgp

BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.0.0/19     172.16.1.2               0             0 200 i
```

En conclusion, l'utilisation des listes de préfixes est la plupart de moyen pratique de filtrer des réseaux dans le BGP. Dans certains cas, toutefois — par exemple, quand vous voulez filtrer impair et même des réseaux tandis que vous contrôlez également la longueur de masque — les Listes d'accès étendues t'offriront la meilleure flexibilité et la contrôleront que des listes de préfixes.

Default route de filtrage des pairs BGP

Vous pouvez filtrer ou bloquer un default route, tel que 0.0.0.0/32 annoncé par le pair BGP, utilisant la commande de **prefix-list**. Vous pouvez voir l'entrée de 0.0.0.0 disponible utilisant la commande de **show ip bgp**.

```
Router 100#show ip bgp
BGP table version is 5, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          172.16.1.2               0             0 200 i
```

La configuration d'échantillon dans cette section est exécutée sur le routeur 100 utilisant la commande d'[ip prefix-list](#).

Routeur 100

```
Router 100#show ip bgp
BGP table version is 5, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          172.16.1.2               0             0 200 i
```

Si vous **show ip bgp de** perfom après cette configuration, vous ne verrez pas l'entrée de 0.0.0.0, qui était disponible dans la sortie précédente de **show ip bgp**.

Informations connexes

- Études de cas BGP
- Page de support BGP
- Support et documentation techniques - Cisco Systems