Bloquer un ou plusieurs réseaux d'un homologue 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 vous recommande de connaître la configuration BGP de base. Pour plus d'informations, référez-vous à Études de cas BGP et Configuration de BGP.

Components Used

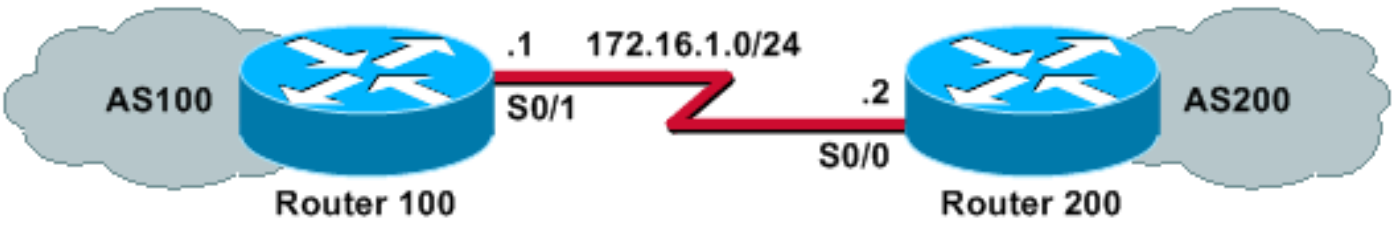
Les informations de ce document sont basées sur le logiciel Cisco IOS® Version 12.2(28).

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. If your network is live, make sure that you understand the potential impact of any command.

Identification et filtrage des routes basées sur NLRI

Pour limiter les informations de routage que le routeur apprend ou annonce, vous pouvez utiliser des filtres basés sur les 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 des voisins et des voisins. Ce document explore ces options avec ce schéma de réseau :

Diagramme du réseau



Filtrage à l'aide de distribute-list avec une liste d'accès standard

Router 200 annonce ces réseaux à son homologue Router 100 :

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

Cet exemple de configuration permet au routeur 100 de refuser une mise à jour pour le réseau 10.10.10.0/24 et d'autoriser 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 **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 à l'aide de distribute-list avec une liste d'accès étendue

Il peut être difficile d’utiliser une liste d’accès standard pour filtrer les super-réseaux. Supposons que le routeur 200 annonce les réseaux suivants :

- 10.10.1.0/24 à 10.10.31.0/24
- 10.10.0.0/19 (son agrégat)

Le routeur 100 souhaite recevoir uniquement le réseau agrégé 10.10.0.0/19 et filtrer tous les réseaux spécifiques.

Une liste d'accès standard, telle que **access-list 1 permit 10.10.0.0 0.0.31.255**, ne fonctionnera pas car elle autorise plus de réseaux que prévu. La liste de contrôle d'accès standard examine uniquement l'adresse réseau et ne peut pas vérifier la longueur du masque réseau. Cette liste d'accès standard permettra l'agrégation /19 ainsi que les réseaux /24 plus spécifiques.

Pour autoriser uniquement le super-réseau 10.10.0.0/19, utilisez une liste d'accès étendue, telle que **access-list 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0**. Référez-vous à access-list (IP extended) pour le format de la commande extended **access-list**.

Dans notre exemple, la source est 10.10.0.0 et le masque générique source 0.0.0.0 est configuré pour une correspondance exacte de la source. Un masque de 255.255.224.0 et un masque générique de 0.0.0.0 sont configurés pour une correspondance exacte du masque source. Si l'une d'elles (source ou masque) ne possède pas de correspondance exacte, la liste d'accès la refuse.

Cela permet à la commande extended **access-list** d'autoriser une correspondance exacte du numéro de réseau source 10.10.0.0 avec le masque 255.255.224.0 (et donc, 10.10.0.0/19). Les autres réseaux /24 plus spécifiques seront filtrés.

> **Note**: Lors de la configuration des caractères génériques, **0** signifie qu'il s'agit d'un bit de correspondance exact et **1** est un bit de ne pas se soucier.

Voici la configuration du 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
```

Le résultat de la commande **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 le montre cette section, les listes d'accès étendues sont plus pratiques à utiliser lorsque certains réseaux doivent être autorisés et d'autres non autorisés, au sein du même réseau principal. Ces exemples fournissent plus d'informations sur la manière dont une liste de contrôle d'accès étendue peut aider dans certaines situations :

- **access-list 101 permit ip 192.168.0.0 0.0.0.0 255.255.252.0 0.0.0.0**

  Cette liste d'accès autorise uniquement le super-réseau 192.168.0.0/22.

- **access-list 102 permit ip 192.168.10.0 0.0.0.255 255.255.255.0 0.0.0.255**

  Cette liste d'accès autorise tous les sous-réseaux de 192.168.10.0/24. En d'autres termes, il autorise 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25, et ainsi de suite : tous les réseaux 192.168.10.*x* avec un masque compris entre 24 et 32.

- **access-list 103 permit ip 0.0.0.0 255.255.255.255 255.255.255.255.0 0.0.0.255**

  Cette liste d'accès autorise tout préfixe réseau avec un masque compris entre 24 et 32.

Filtrage à l'aide de la commande ip prefix-list

Router 200 annonce ces réseaux à son homologue Router 100 :

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

Les exemples de configuration de cette section utilisent la commande ip prefix-list, qui permet au routeur 100 d'effectuer deux opérations :

- Autoriser les mises à jour pour tout réseau dont la longueur de masque de préfixe est inférieure ou égale à 19.
- Refuser toutes les mises à jour réseau avec une longueur de masque de réseau supérieure à 19.

Routeur 100

```
hostname Router 100
  !
  router bgp 100
   neighbor 172.16.1.2 remote-as 200
   neighbor 172.16.1.2 prefix-list cisco in
  !

ip prefix-list cisco seq 10 permit 0.0.0.0/0 le 19
```

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
```

La sortie de la commande **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 de listes de préfixes est la méthode la plus pratique pour filtrer les réseaux dans BGP. Dans certains cas, cependant— par exemple, lorsque vous voulez filtrer des réseaux impairs et pairs tout en contrôlant la longueur du masque—les listes d'accès étendues vous offrent une plus grande flexibilité et un meilleur contrôle que les listes de préfixes.

Filtrage des routes par défaut des homologues BGP

Vous pouvez filtrer ou bloquer une route par défaut, telle que 0.0.0.0/32 annoncée par l'homologue BGP, à l'aide de la commande **prefix-list**. Vous pouvez voir l'entrée 0.0.0.0 disponible à l'aide de la commande **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
```

L'exemple de configuration de cette section est exécuté sur le routeur 100 à l'aide de la commande ip prefix-list.

Routeur 100

```
hostname Router 100
  !
  router bgp 100
   neighbor 172.16.1.2 remote-as 200
   neighbor 172.16.1.2 prefix-list deny-route in
  !

ip prefix-list deny-route seq 5 deny 0.0.0.0/0
ip prefix-list deny-route seq 10 permit 0.0.0.0/0 le 32
```

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

Informations connexes

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