Block One or More Networks from a BGP Peer

Contenido

Introducción

El filtrado de Routes es la base por la cual se establecen las políticas BGP (Border Gateway Protocol). Hay número de maneras de filtrar una o más redes de un peer BGP, incluida la Información de alcance de la capa de red (NLRI) y los atributos de comunidad AS_Path. Este documento solamente trata el filtrado basado en la NLRI. Para obtener información sobre el filtro basado en AS_Path, consulte Uso de Expresiones Normales en BGP. Para obtener información adicional, consulte la sección Filtrado de BGP de Casos Prácticos de BGP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de la configuración básica de BGP. Para obtener más información, consulte Casos Prácticos de BGP y Configuración de BGP.

Componentes Utilizados

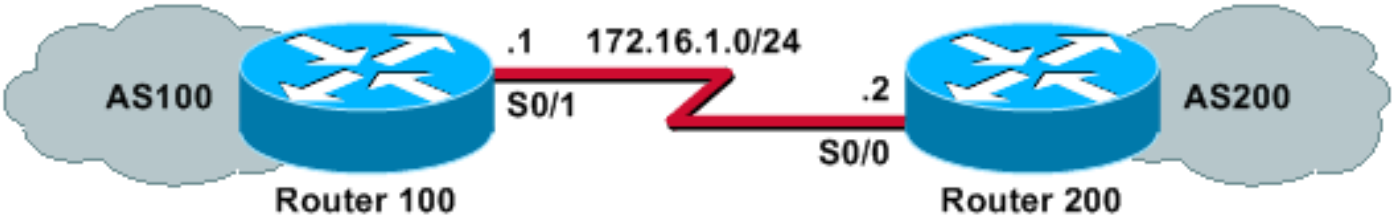
La información en este documento se basa en Cisco IOS® Software Release 12.2(28).

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.

Identificación y filtro de rutas en función del NLRI

Para restringir la información de ruteo que el router detecta o anuncia, puede utilizar filtros basados en actualizaciones de ruteo. Los filtros consisten en una lista de acceso o una lista de prefijos, que se aplica a las actualizaciones de vecinos y de vecinos. Este documento explora estas opciones con este diagrama de red:

Diagrama de la red



Filtrado utilizando una distribute list con una lista de acceso estándar

El Router 200 anuncia estas redes a su Router 100 de peer:

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

Esta configuración de ejemplo permite que el Router 100 niegue una actualización para la red 10.10.10.0/24 y permita las actualizaciones de las redes 192.168.10.0/24 y 10.10.0.0/19 en su tabla BGP:

Router 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
```

Router 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
```

Esta salida del comando **show ip bgp** confirma las acciones del Router 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
```

Filtrado utilizando una lista de distribución con una Lista de acceso ampliado

Puede resultar complicado utilizar una lista de acceso estándar para filtrar superredes. Suponga que el Router 200 anuncia estas redes:

- 10.10.1.0/24 a 10.10.31.0/24
- 10.10.0.0/19 (su agregado)

El router 100 desea recibir solamente la red agregada, 10.10.0.0/19, y filtrar todas las redes específicas.

Una lista de acceso estándar, como **access-list 1 permit 10.10.0.0 0.0.31.255**, no funcionará porque permite más redes de las deseadas. La lista de acceso estándar sólo mira la dirección de red y no puede verificar la longitud de la máscara de red. Esa lista de acceso estándar permitirá el agregado /19 así como las redes /24 más específicas.

Para permitir solamente la superred 10.10.0.0/19, utilice una lista de acceso extendida, como **access-list 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0**. Consulte access-list (IP extended) para ver el formato del **comando** de lista de acceso extendido.

En nuestro ejemplo, el origen es 10.10.0.0 y el comodín de origen 0.0.0.0 se configura para una coincidencia exacta del origen. Se configura una máscara de 255.255.224.0 y un comodín de máscara de 0.0.0.0 para una coincidencia exacta de la máscara de origen. Si alguno de ellos (origen o máscara) no tiene una coincidencia exacta, la lista de acceso lo niega.

Esto permite que el comando **access-list** extendido permita una coincidencia exacta del número de red de origen 10.10.0.0 con la máscara 255.255.224.0 (y por lo tanto, 10.10.0.0/19). Las otras redes /24 más específicas se filtrarán.

> **Nota:** Al configurar comodines, **0** significa que es un bit de coincidencia exacta y **1** es un bit de no importa.

Esta es la configuración en el Router 100:

Router 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
```

El resultado del comando **show ip bgp** del Router 100 confirma que la lista de acceso funciona como se esperaba.

```
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
```

Como se puede ver en esta sección, las listas de acceso ampliadas son más cómodas cuando se deben permitir algunas redes y algunas no se permiten, dentro de la misma red principal. Estos ejemplos proporcionan más información sobre cómo una lista de acceso ampliada puede ayudar en algunas situaciones:

- **access-list 101 permit ip 192.168.0.0 0.0.0.0 255.255.252.0 0.0.0**

  Esta lista de acceso sólo permite la superred 192.168.0.0/22.

- **access-list 102 permit ip 192.168.10.0 0.0.0.255 255.255.0 0.0.0.255**

  Esta lista de acceso permite todas las subredes de 192.168.10.0/24. En otras palabras, permitirá 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25 y así sucesivamente: cualquiera de las redes 192.168.10.*x* con una máscara que va de 24 a 32.

- **access-list 103 permit ip 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255**

  Esta lista de acceso permite cualquier prefijo de red con una máscara que va de 24 a 32.

Aplicación de filtro con el comando ip prefix-list

El Router 200 anuncia estas redes a su Router 100 de peer:

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

Las configuraciones de ejemplo de esta sección utilizan el comando ip prefix-list, que permite al Router 100 hacer dos cosas:

- Permitir actualizaciones para cualquier red con una longitud de máscara de prefijo inferior o igual a 19.
- Denegar todas las actualizaciones de red con una longitud de máscara de red superior a 19.

Router 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
```

Router 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
```

El resultado del comando **show ip bgp** confirma que la lista de prefijos funciona como se esperaba en el Router 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 conclusión, el uso de listas de prefijos es la manera más conveniente de filtrar redes en BGP. Sin embargo, en algunos casos, por ejemplo, cuando desea filtrar redes impares e impares mientras también controla la longitud de la máscara, las listas de acceso ampliadas le ofrecerán mayor flexibilidad y control que las listas de prefijos.

Filtrado de Rutas Predeterminadas de Peers BGP

Puede filtrar o bloquear una ruta predeterminada, como 0.0.0.0/32 que anuncia el peer BGP, usando el comando **prefix-list**. Puede ver la entrada 0.0.0.0 disponible usando el comando **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 configuración de ejemplo de esta sección se realiza en el Router 100 mediante el comando [ip prefix-list](#).

Router 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 realiza **show ip bgp** después de esta configuración, no verá la entrada 0.0.0.0, que estaba

disponible en la salida anterior de **show ip bgp**.

Información Relacionada

- Casos Prácticos de BGP
- Página de Soporte de BGP
- Soporte Técnico y Documentación - Cisco Systems