Bloquee una o más redes de un peer BGP

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.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene configuración BGP del conocimietno básico. Para más información, refiera a los casos prácticos de BGP y BGP el configurar.

Componentes Utilizados

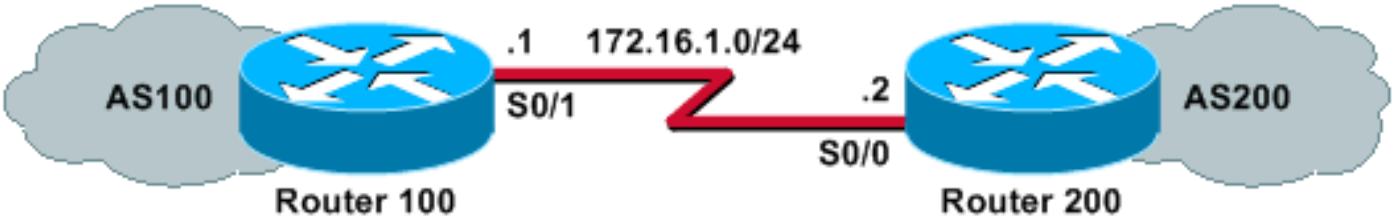
La información en este documento se basa en la versión del Cisco IOS ® Software 12.2(28).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Identificación y filtro de rutas en función del NLRI

Para restringir la información de ruteo de que el router aprende o hace publicidad, usted puede utilizar los filtros basados en las actualizaciones de ruteo. Los filtros consisten en una lista de acceso o una lista de prefijos, que se aplica a las actualizaciones a los vecinos y de los vecinos. Este documento explora estas opciones con este diagrama de la 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 del par:

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

Esta configuración de muestra permite al router 100 para negar una actualización para la red 10.10.10.0/24 y para permitir 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 ser difícil utilizar una lista de acceso estándar para filtrar el supernets. Asuma 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)

Deseos del router 100 a RO la red agregada, 10.10.0.0/19, y filtrar hacia fuera todas las redes específicas.

Una lista de acceso estándar, tal como **permiso 10.10.0.0 0.0.31.255 de la lista de acceso 1**, no trabajará porque permite más redes que deseadas. Las miradas de la lista de acceso estándar en la dirección de red solamente y no pueden marcar la longitud de la máscara de la red. Esa lista de acceso estándar permitirá el agregado de /19 así como las redes más específicas de /24.

Para permitir solamente el supernet 10.10.0.0/19, utilice una lista de acceso ampliada, tal como **IP 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0 del permiso del access-list 101**. Refiera a la lista de acceso (IP extendido) para el formato del comando de la lista de acceso ampliada.

En nuestro ejemplo, la fuente es 10.10.0.0 y el source comodín de 0.0.0.0 se configura para un exacto - coincidencia de la fuente. Configuran una máscara de 255.255.224.0, y a un máscara-comodín de 0.0.0.0 para un exacto - coincidencia de la máscara de la fuente. Si ningún de ella (fuente o máscara) no tiene un exacto - haga juego, la lista de acceso la niega.

Esto permite el comando de la lista de acceso ampliada de permitir un exacto - coincidencia del network number 10.10.0.0 de la fuente con la máscara 255.255.224.0 (y así, 10.10.0.0/19). Las otras redes más específicas de /24 serán filtradas hacia fuera.

> Nota: Al configurar las placas comodín, **0** significa que es un exacto - hace juego el bit y **1** es un hacer-no-cuidado-bit.

Ésta 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
```

La salida del **comando show ip bgp del** router 100 confirma que la lista de acceso está trabajando 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 ve en esta sección, las listas de acceso ampliadas son más convenientes de utilizar cuando algunas redes se deben permitir y algunos rechazadas, dentro de la misma red principal. Estos ejemplos proporcionan más penetración en cómo una lista de acceso ampliada puede ayudar en algunas situaciones:

- **IP 192.168.0.0 0.0.0.0 255.255.252.0 0.0.0.0 del permiso del access-list 101**

  Esta lista de acceso permite solamente el supernet 192.168.0.0/22.

- **IP 192.168.10.0 0.0.0.255 255.255.255.0 0.0.0.255 del permiso de la lista de acceso 102**

  Esta lista de acceso permite todas las subredes de 192.168.10.0/24. Es decir permitirá 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25, y así sucesivamente: redes unas de los 192.168.10.x con una máscara que se extiende a partir de la 24 a 32.

- **IP 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255 del permiso de la lista de acceso 103**

  Esta lista de acceso permite cualquier Prefijo de red con una máscara que se extienda a partir de la 24 a 32.

Aplicación de filtro con el comando ip prefix-list

El router 200 anuncia estas redes a su router 100 del par:

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

Las configuraciones de muestra en esta sección utilizan el comando ip prefix-list, que permite al router 100 para hacer dos cosas:

- Permita las actualizaciones para cualquier red con una longitud de la máscara del prefijo inferior o igual 19.
- Niegue todas las actualizaciones de la red con una longitud de la máscara de la red mayor de 19.

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
```

Router 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 salida del comando show ip bgp confirma que la lista de prefijos está trabajando 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 las listas de prefijos es la mayoría de la manera conveniente de filtrar las redes en el BGP. En algunos casos, no obstante — por ejemplo, cuando usted quiere filtrar impar e incluso las redes mientras que usted también controla la longitud de la máscara — las listas de acceso ampliadas le ofrecerán la mayor flexibilidad y la controlarán que las listas de prefijos.

Rutas predeterminado de filtración de los peeres BGP

Usted puede filtrar o bloquear una ruta predeterminado, tal como 0.0.0.0/32 que es hecho publicidad por el peer BGP, usando el comando de la **lista de prefijo**. Usted puede ver la entrada de 0.0.0.0 disponible con 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 muestra en esta sección se realiza en el router 100 usando el [comando ip prefix-list](#).

Router 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 usted **BGP del IP de la demostración del** perfom después de esta configuración, usted no ve la entrada de 0.0.0.0, que estaba disponible en la **demostración** anterior **resultado de ip bgp**.

Información Relacionada

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