Bloquear uma ou mais redes de um peer BGP

Contents

Introduction

A filtragem de rota é a base pela qual as políticas do roteamento BGP são definidas. Há várias maneiras de filtrar uma ou várias redes de um peer BGP, incluindo a Network Layer Reachability Information (NLRI) e os atributos AS_Path e Community. Este documento discute a filtragem baseada em NLRI apenas. Para obter informações sobre como filtrar com base em AS_Path, consulte Usando expressões regulares em BGP. Para obter informações adicionais, consulte a seção Filtragem BGP de Estudos de Caso de BGP.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento da configuração BGP básica. Para obter mais informações, consulte Estudos de Caso BGP e Configuração do BGP.

Componentes Utilizados

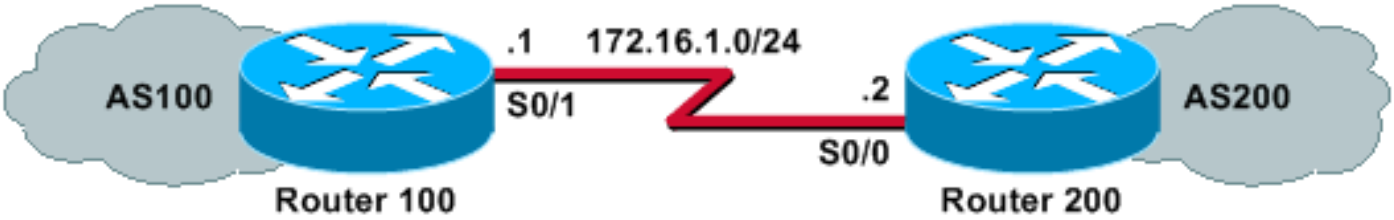
As informações neste documento são baseadas no Cisco IOS® Software Release 12.2(28).

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.

Identificando e filtrando rotas com base em NLRI

Para restringir as informações de roteamento que o roteador aprende ou anuncia, você pode usar filtros com base em atualizações de roteamento. Os filtros consistem em uma lista de acesso ou uma lista de prefixos, que é aplicada a atualizações de vizinhos e de vizinhos. Este documento explora estas opções com este diagrama de rede:

Diagrama de Rede



Filtragem usando lista de distribuição com uma lista de acesso padrão

O Roteador 200 anuncia essas redes ao seu peer Roteador 100:

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

Esta configuração de exemplo permite que o Roteador 100 negue uma atualização para a rede 10.10.10.0/24 e permita as atualizações das redes 192.168.10.0/24 e 10.10.0.0/19 na sua tabela BGP:

Roteador 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
```

Roteador 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 saída do comando **show ip bgp** confirma as ações do Roteador 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
```

Filtragem utilizando a lista de distribuição com uma lista de acesso estendido

Pode ser complicado usar uma lista de acesso padrão para filtrar super-redes. Suponha que o Roteador 200 anuncia estas redes:

- 10.10.1.0/24 até 10.10.31.0/24
- 10.10.0.0/19 (seu agregado)

O roteador 100 deseja receber apenas a rede agregada, 10.10.0.0/19, e filtrar todas as redes específicas.

Uma lista de acesso padrão, como **access-list 1 permit 10.10.0.0 0.0.31.255**, não funcionará porque permite mais redes do que o desejado. A lista de acesso padrão examina apenas o endereço de rede e não pode verificar o comprimento da máscara de rede. Essa lista de acesso padrão permitirá a agregação /19, bem como as redes /24 mais específicas.

Para permitir somente a super-rede 10.10.0.0/19, use uma lista de acesso estendida, como **access-list 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0**. Consulte a lista de acesso (IP estendido) para obter o formato do comando **access-list** estendido.

Em nosso exemplo, a origem é 10.10.0.0 e o curinga origem 0.0.0.0 está configurado para uma correspondência exata da origem. Uma máscara de 255.255.224.0 e um curinga de máscara de 0.0.0.0 estão configurados para uma correspondência exata da máscara de origem. Se algum deles (origem ou máscara) não tiver uma correspondência exata, a lista de acesso negará.

Isso permite que o comando **access-list** estendida permita uma correspondência exata do número de rede de origem 10.10.0.0 com a máscara 255.255.224.0 (e, portanto, 10.10.0.0/19). As outras redes /24 mais específicas serão filtradas.

> **Note**: Ao configurar curingas, **0** significa que é um bit de correspondência exato e **1** é um bit do tipo "não se importe".

Esta é a configuração no Roteador 100:

Roteador 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
```

A saída do comando **show ip bgp** do Roteador 100 confirma que a lista de acesso está funcionando conforme esperado.

```
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 visto nesta seção, as listas de acesso estendidas são mais convenientes para serem usadas quando algumas redes devem ser permitidas e algumas não permitidas, dentro da mesma rede principal. Estes exemplos fornecem mais informações sobre como uma lista de acesso estendida pode ajudar em algumas situações:

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

  Essa lista de acesso permite somente a super-rede 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**

  Essa lista de acesso permite todas as sub-redes de 192.168.10.0/24. Em outras palavras, permitirá 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25, e assim por diante: qualquer uma das redes 192.168.10.*x* com uma máscara que varia 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**

  Essa lista de acesso permite qualquer prefixo de rede com uma máscara que varia de 24 a 32.

Filtrando com o comando ip prefix-list

O Roteador 200 anuncia essas redes ao seu peer Roteador 100:

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

As configurações de exemplo nesta seção usam o comando **ip prefix-list**, que permite que o Roteador 100 faça duas coisas:

- Permitir atualizações para qualquer rede com um comprimento de máscara de prefixo inferior ou igual a 19.
- Negue todas as atualizações de rede com um comprimento de máscara de rede superior a 19.

Roteador 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
```

Roteador 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
```

A saída do comando **show ip bgp** confirma que a lista de prefixos está funcionando conforme esperado no Roteador 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
```

Em conclusão, o uso de listas de prefixos é a maneira mais conveniente de filtrar redes no BGP. Em alguns casos, no entanto — por exemplo, quando você quer filtrar redes ímpares e até mesmo quando você também controla o comprimento da máscara — as listas de acesso estendidas oferecerão maior flexibilidade e controle do que as listas de prefixos.

Filtrando rotas padrão dos peers BGP

Você pode filtrar ou bloquear uma rota padrão, como 0.0.0.0/32 sendo anunciado pelo peer BGP, usando o comando **prefix-list**. Você pode ver a entrada 0.0.0.0 disponível usando o 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
```

O exemplo de configuração nesta seção é executado no Roteador 100 usando o comando **ip prefix-list**.

Roteador 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
```

Se você executar **show ip bgp** após essa configuração, não verá a entrada 0.0.0.0, que estava disponível na saída **show ip bgp anterior**.

Informações Relacionadas

- Estudos de caso de BGP
- Página de suporte de BGP
- Suporte Técnico e Documentação - Cisco Systems