Заблокируйте одну или более сетей от одноранговой соединения по протоколу BGP

Содержание

Введение

Фильтрация маршрутов – основа для реализации политик протокола граничного шлюза (BGP). Существует множество способов фильтрации одной или нескольких сетей с одноранговой стороны BGP, включая информацию о достижимости на сетевом уровне (NLRI) и атрибуты AS_Path и Community. В настоящем документе рассматривается только фильтрация на основе NLRI. Описание фильтрации на основе AS_Path см. в документе Использование регулярных выражений в BGP. Дополнительные сведения см. в разделе Фильтрация BGP документа Практические примеры BGP.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с базовой конфигурацией BGP. Дополнительные сведения см. в документах Практические примеры BGP и Настройка BGP.

Используемые компоненты

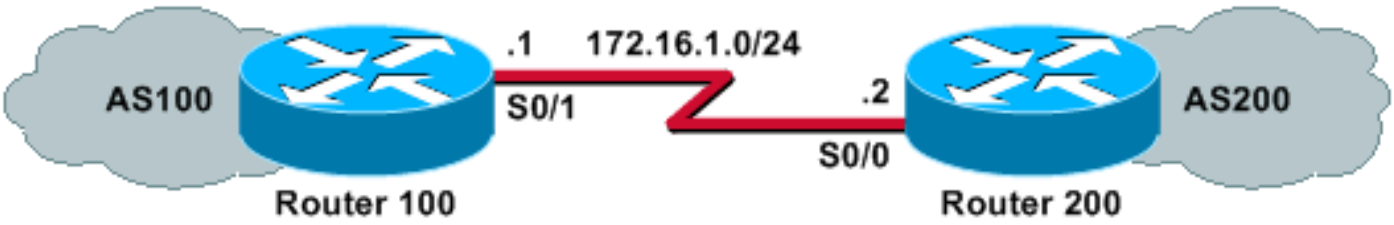
Сведения, содержащиеся в этом документе, относятся к выпуску ПО Cisco IOS® 12.2(28).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Идентификация и фильтрация маршрутов на основе NLRI

Чтобы свести к минимуму объем сведений о маршрутизации, которые маршрутизатор должен запоминать или объявлять, можно использовать фильтры на основе обновлений маршрутизации. Фильтры состоят из списка контроля доступа или списка префиксов, действующего для обновлений, адресованных соседним узлам и поступающих от соседних узлов. Эти варианты анализируются в контексте следующей схемы сети:

Схема сети



Фильтрация с ключевым словом distribute-list и стандартным списком контроля доступа

Маршрутизатор 200 объявляет эти сети связанному с ним маршрутизатору 100:

- 192.168.10.0/24
- 10.10.10.0/24

- 10.10.0.0/19

Этот пример конфигурации позволяет маршрутизатору 100 запретить обновление сети 10.10.10.0/24 и разрешить обновление сетей 192.168.10.0/24 и 10.10.0.0/19 в своей таблице BGP:

Маршрутизатор 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
```

Маршрутизатор 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
```

Выходные данные следующей команды show ip bgp подтверждают действия маршрутизатора 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
```

Фильтрация с ключевым словом distribute-list и расширенным списком контроля доступа

Применение стандартного списка контроля доступа для фильтрации суперсетей сталкивается с определенными сложностями. Предположим, что маршрутизатор 200 объявляет следующие сети:

- с 10.10.1.0/24 по 10.10.31.0/24
- 10.10.0.0/19 (объединение вышеуказанных сетей)

Маршрутизатор 100 заинтересован только в получении сведений об объединенной сети, 10.10.0.0/19. Информация, относящаяся к отдельным сетям, должна отфильтровываться.

Стандартный список контроля доступа вида access-list 1 permit 10.10.0.0 0.0.31.255 не подойдет, поскольку он разрешает больше сетей, чем нужно. Стандартный список контроля доступа контролирует адрес сети, но не сетевую маску. Этот стандартный список контроля доступа разрешает как объединенную сеть /19, так и отдельные сети /24.

Чтобы разрешать только суперсеть 10.10.0.0/19, используйте расширенный список контроля доступа вида access-list 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0. Формат команды access-list для расширенного списка контроля доступа описан в разделе access-list (расширенный список контроля доступа IP).

В нашем примере источник – 10.10.0.0. Для него настраивается точно соответствующий шаблон 0.0.0.0. Для точного соответствия с маской источника задаются маска 255.255.224.0 и шаблон маски 0.0.0.0. В случае неполного соответствия любому из этих значений (источнику или маске) список контроля доступа выдаст запрет.

Таким образом, расширенная команда access-list позволяет точно описать соответствие номеру сети источника 10.10.0.0 с маской 255.255.224.0 (и, как следствие, с 10.10.0.0/19). Другие, более узкие сети /24 будут фильтроваться.

> **Примечание:** При настройке подстановочных знаков **0** средств, что это - полное соответствие, укусили, и **1** do-not-care-bit.

Конфигурация маршрутизатора 100:

Маршрутизатор 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
```

Выходные данные команды show ip bgp с маршрутизатора 100 подтверждают, что список контроля доступа функционирует требуемым образом.

```
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
```

Как показано в этом разделе, расширенные списки контроля доступа более практичны в ситуациях, когда в пределах одной крупной сети нужно разрешить одни сети и запретить другие. Эти примеры в более полной мере иллюстрируют пользу расширенных списков контроля доступа в некоторых ситуациях:

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

  Этот список контроля доступа разрешает только суперсеть 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**

  Этот список контроля доступа разрешает все подсети 192.168.10.0/24. Иначе говоря, разрешаются подсети 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25, и т.д: *любая из подсетей 192.168.10.x с маской в диапазоне от 24 до 32.*

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

  Этот список контроля доступа разрешает любой префикс сети с маской от 24 до 32.

Фильтрация с использованием команды ip prefix-list

Маршрутизатор 200 объявляет эти сети связанному с ним маршрутизатору 100:

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

В примерах конфигурации, приведенных в этом разделе, применяется команда ip prefix-list, с которой маршрутизатор 100 будет выполнять сразу две функции:

- Разрешать обновления для любой сети с длиной маски префикса не более 19 разрядов.
- Запрещать обновления для всех сетей с длиной маски префикса более 19 разрядов.

Маршрутизатор 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
```

Маршрутизатор 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
```

Выходные данные команды show ip bgp с маршрутизатора 100 подтверждают, что список префиксов на нем функционирует требуемым образом.

```
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
```

Можно заключить, что применение списков префиксов – наиболее удобный способ фильтрации сетей в протоколе BGP. Но в некоторых случаях, например, когда нужно отфильтровать четные и нечетные сети одновременно с контролем длины маски, расширенные списки контроля доступа дают больше гибкости и управляемости по сравнению со списками префиксов.

Фильтрация маршрутов по умолчанию от других сторон BGP

Можно отфильтровать или заблокировать объявленный стороной BGP маршрут по умолчанию, например 0.0.0.0/32, используя команду prefix-list. Увидеть, что запись 0.0.0.0 доступна, можно при помощи команды 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
```

[Пример конфигурации, представленный в этом разделе, задан на маршрутизаторе Router 100 командой ip prefix-list.]

Маршрутизатор 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
```

Если после задания этой конфигурации выполнить команду show ip bgp, то запись 0.0.0.0, доступная ранее в выходных данных команды show ip bgp, видна не будет.

Дополнительные сведения

- Практические примеры BGP
- Страница поддержки BGP
- Cisco Systems – техническая поддержка и документация