Blocca una o più reti da un peer BGP

Sommario

Introduzione

Il filtro route è la base su cui vengono impostate le policy BGP (Border Gateway Protocol). Esistono diversi modi per filtrare una o più reti da un peer BGP, tra cui NLRI (Network Layer Reachability Information) e gli attributi AS_Path e Community. In questo documento viene descritto come filtrare i dati solo in base all'NLRI. Per informazioni su come filtrare in base a AS_Path, vedere Utilizzo delle espressioni regolari in BGP. Per ulteriori informazioni, fare riferimento alla sezione Filtraggio BGP di Case Study BGP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione BGP di base. Per ulteriori informazioni, fare riferimento ai casi di studio di BGP e alla configurazione di BGP.

Componenti usati

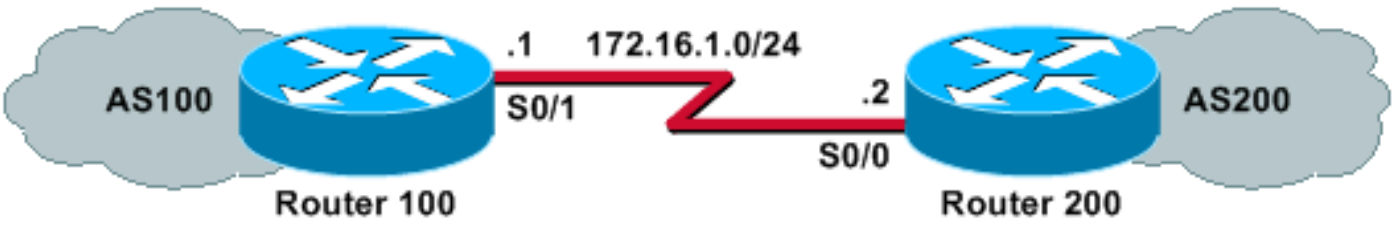
Il riferimento delle informazioni contenute in questo documento è il software Cisco IOS® versione 12.2(28).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Identificazione e filtro delle route in base all'NLRI

Per limitare le informazioni di routing che il router apprende o annuncia, è possibile utilizzare filtri basati sugli aggiornamenti di routing. I filtri sono costituiti da un elenco di accesso o da un elenco di prefissi, che viene applicato agli aggiornamenti dei computer adiacenti e dei computer adiacenti. In questo documento vengono esaminate le seguenti opzioni con il diagramma di rete:

Esempio di rete



Filtraggio tramite lista di distribuzione con un elenco degli accessi standard

Il router 200 annuncia queste reti al router peer 100:

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

Questa configurazione di esempio consente al router 100 di negare un aggiornamento per la rete 10.10.10.0/24 e di consentire gli aggiornamenti delle reti 192.168.10.0/24 e 10.10.0.0/19 nella relativa tabella 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
```

L'output del comando **show ip bgp** conferma le azioni 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
```

Filtraggio tramite lista di distribuzione con elenco degli accessi esteso

L'utilizzo di un elenco degli accessi standard per filtrare le superreti può risultare molto complesso. Si supponga che il router 200 annunci queste reti:

- da 10.10.1.0/24 a 10.10.31.0/24
- 10.10.0.0/19 (i suoi aggregati)

Il router 100 desidera ricevere solo la rete aggregata, ossia la rete 10.10.0.0/19, e filtrare tutte le reti specifiche.

Un elenco degli accessi standard, ad esempio **access-list 1 allow 10.10.0.0.0.31.255**, non funzionerà perché consente più reti di quante si desideri. L'elenco degli accessi standard controlla solo l'indirizzo di rete e non può controllare la lunghezza della network mask. L'elenco degli accessi standard consentirà l'aggregazione /19 e le reti /24 più specifiche.

Per autorizzare solo la supernet 10.10.0.0/19, usare un elenco degli accessi esteso, come **access-list 101 allow ip 10.10.0.0.0.0.0 255.255.224.0 0.0.0**. Fare riferimento all'elenco degli accessi (IP esteso) per il formato del comando **access-list** esteso.

Nell'esempio, l'origine è 10.10.0.0 e il valore 0.0.0.0 per source-wildcard è configurato per una corrispondenza esatta di origine. Per una corrispondenza esatta della maschera di origine, vengono configurati una maschera di 255.255.224.0 e un carattere jolly di 0.0.0.0. Se uno dei due (origine o maschera) non ha una corrispondenza esatta, l'elenco degli accessi lo nega.

In questo modo, il comando **access-list** esteso permette di trovare una corrispondenza esatta tra il numero di rete 10.10.0.0 e la maschera 255.255.224.0 (e quindi 10.10.0.0/19). Le altre reti /24 più specifiche saranno escluse dal filtro.

> **Nota:** Quando si configurano i caratteri jolly, il valore **0** indica che si tratta di un bit di corrispondenza esatta e il valore **1** indica che il bit non è rilevante.

Questa è la configurazione sul 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
```

L'output del comando **show ip bgp** restituito dal router 100 conferma che l'elenco degli accessi funziona come previsto.

```
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
```

Come mostrato in questa sezione, gli elenchi degli accessi estesi sono più comodi da utilizzare quando alcune reti devono essere consentite e altre no, all'interno della stessa rete principale. Gli esempi riportati di seguito forniscono ulteriori informazioni sul modo in cui un elenco degli accessi esteso può essere utile in alcune situazioni:

- **access-list 101 allow ip 192.168.0.0 0.0.0 255.255.252.0 0.0.0**

  Questo elenco degli accessi consente solo la supernet 192.168.0.0/22.

- **access-list 102 allow ip 192.168.10.0.0.0.255.255.255.255.0 0.0.0.255**

  Questo elenco degli accessi consente tutte le subnet di 192.168.10.0/24. In altre parole, consente 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25 e così via: una delle reti 192.168.10.*x* con una maschera che va da 24 a 32.

- **access-list 103 allow ip 0.0.0.0 255.255.255.255.255.255.255.0 0.0.255**

  Questo elenco degli accessi consente di usare qualsiasi prefisso di rete con una maschera che va da 24 a 32.

Filtraggio con il comando ip prefix-list

Il router 200 annuncia queste reti al router peer 100:

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

Nelle configurazioni di esempio in questa sezione viene usato il comando **ip prefix-list** , che permette al router 100 di eseguire due operazioni:

- Permettere gli aggiornamenti per tutte le reti con una lunghezza della maschera del prefisso inferiore o uguale a 19.
- Nega tutti gli aggiornamenti di rete con una lunghezza della maschera di rete maggiore di 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
```

L'output del comando **show ip bgp** conferma che l'elenco dei prefissi funziona come previsto sul 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
```

In conclusione, l'uso degli elenchi di prefissi è il modo più conveniente per filtrare le reti in BGP. In alcuni casi, tuttavia—ad esempio, quando si desidera filtrare le reti pari e dispari e contemporaneamente controllare la lunghezza della maschera—gli elenchi degli accessi estesi offrono una maggiore flessibilità e un maggiore controllo rispetto agli elenchi dei prefissi.

Filtraggio delle route predefinite dai peer BGP

Èpossibile filtrare o bloccare una route predefinita, ad esempio 0.0.0.0/32 annunciata dal peer BGP, utilizzando il comando **prefix-list**. la voce 0.0.0.0 è disponibile con il 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
```

L'esempio di configurazione illustrato in questa sezione viene eseguito sul router 100 con il 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
```

se si esegue **show ip bgp** dopo questa configurazione, la voce 0.0.0.0 non verrà visualizzata, come era possibile verificare nell'output **show ip bgp** precedente.

Informazioni correlate

- Case study del protocollo BGP
- Pagina di supporto BGP
- Documentazione e supporto tecnico – Cisco Systems