Blokkeer een of meer netwerken van een BGP-peer

Inhoud

Inleiding

Routefiltering is de basis waarop het BGP-beleid (Border Gateway Protocol) wordt ingesteld. Er zijn een aantal manieren om een of meer netwerken te filteren van een BGP-peer, waaronder Network Layer Reachability Information (NLRI) en AS_Path en Community-kenmerken. In dit document wordt filtering alleen op basis van NLRI besproken. Zie Reguliere expressies in BGP gebruiken voor informatie over het filteren op basis van AS_Path. Raadpleeg het gedeelte BGP-filtering van BGP-casestudy's voor extra informatie.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de basis-BGP-configuratie. Raadpleeg BGP-casestudy's en BGP-configuratie voor meer informatie.

Gebruikte componenten

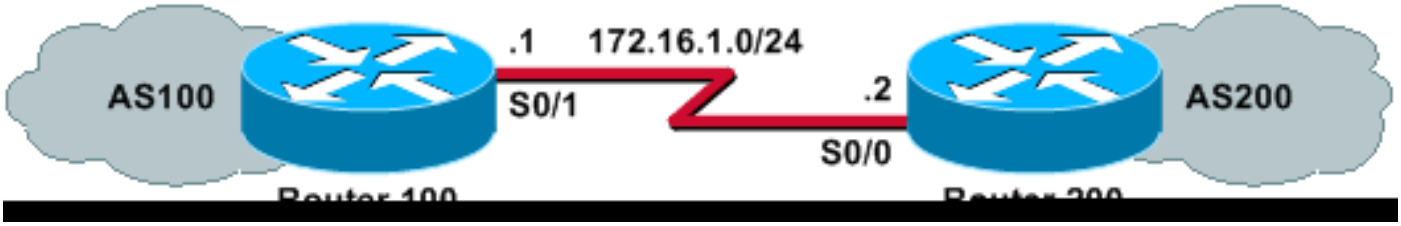
De informatie in dit document is gebaseerd op Cisco IOS®-softwarerelease 12.2(28).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Identificatie en filtering van routers op basis van NLRI

Om het routing-informatie die de router leert of adverteert te beperken, kunt u filters gebruiken op basis van routing-updates. De filters bestaan uit een toegangslijst of een prefixlijst, die wordt toegepast op updates van buren en van buren. Dit document verkent deze opties met dit netwerkdiagram:

Netwerkdiagram



Filtering met distributielijst met een standaard toegangslijst

Router 2000 kondigt deze netwerken aan op zijn peer router 100:

- 192.168.10.0/24

- 10.10.10.0/24
- 10.10.0.0/19

Deze voorbeeldconfiguratie stelt router 100 in staat om een update voor netwerk 10.10.10.0/24 te ontkennen en de updates van netwerken 192.168.10.0/24 en 10.10.0.0/19 in zijn BGP-tabel toe te staan:

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 2000

```
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
```

Deze opdrachtoutput van ip bgp bevestigt de acties van router 100:

<#root>

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
```

Filtering met distributielijst met uitgebreide toegangslijst

Het kan lastig zijn om een standaard toegangslijst te gebruiken om supernets te filteren. Veronderstel dat router 200 deze netwerken aankondigt:

- 10.10.1.0/24 t/m 10.10.31.0/24
- 10.10.0.0/19 (het totaal ervan)

Router 100 wil alleen het geaggregeerde netwerk, 10.10.0.0/19, ontvangen en alle specifieke netwerken uitfilteren.

Een standaard toegangslijst, zoals toegangslijst 1 vergunning 10.10.0.0 0.0.0.31.255, zal niet werken omdat het meer netwerken toelaat dan gewenst. De standaard toegangslijst bekijkt alleen het netwerkadres en kan niet de lengte van het netwerkmasker controleren. Die standaard toegangslijst maakt zowel de /19 aggregaat als de specifiekere /24 netwerken mogelijk.

Als u alleen de supernet 10.10.0.0/19 wilt toestaan, gebruikt u een uitgebreide toegangslijst, zoals de toegangslijst 101-toegangslijst ip 10.10.0.0.0.0 255.255.224.0 0.0.0.0. Raadpleeg de toegangslijst (IP Extended) voor het formaat van de opdracht uitgebreide toegangslijst.

In ons voorbeeld, is de bron 10.10.0.0 en de bron-vervanging van 0.0.0.0 wordt gevormd voor een nauwkeurige gelijke van bron. Een masker van 255.255.224.0, en een masker-vervanging van 0.0.0.0 wordt gevormd voor een nauwkeurige gelijke van bronmasker. Als een van hen (bron of masker) geen exacte overeenkomst heeft, ontkent de toegangslijst het.

Dit staat het uitgebreide access-list bevel toe om een nauwkeurige gelijke van bronnetwerknummer 10.10.0.0 met masker 255.255.224.0 (en zo, 10.10.0.0/19) toe te staan. De andere meer specifieke /24 netwerken zullen worden weggefilterd.

Opmerking: Bij het configureren van wild cards betekent 0 dat het een exact match bit is en 1 een do-not-care-bit.

Dit is de configuratie op router 100:

Router 100
<#root> 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

De opdrachtoutput van de show ip bgp van router 100 bevestigt dat de toegangslijst werkt zoals verwacht.

<#root>

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
```

Zoals in deze sectie wordt getoond, zijn uitgebreide toegangslijsten handiger om te gebruiken wanneer sommige netwerken moeten worden toegestaan en sommige worden verboden, binnen hetzelfde grote netwerk. Deze voorbeelden bieden meer inzicht in hoe een uitgebreide toegangslijst in bepaalde situaties kan helpen:

- toegangslijst 101 vergunning ip 192.168.0.0 0.0.0 255.255.252.0 0.0.0.0

  Deze toegangslijst maakt alleen de supernet 192.168.0.0/22 mogelijk.

- toegangslijst 102 vergunning ip 192.168.10.0 0.0.0.255 255.255.255.0 0.0.0.255

  Deze toegangslijst staat alle subnetten van 192.168.10.0/24 toe. Met andere woorden, het staat 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25, enzovoort toe: een van de 192.168.10.x-netwerken met een masker dat varieert van 24 tot 32.

- toegangslijst 103 vergunning ip 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255

  Deze toegangslijst staat elk netwerkprefix toe met een masker dat varieert van 24 tot 32.

Filteren met de opdracht IP-prefixlijst

Router 2000 kondigt deze netwerken aan op zijn peer router 100:

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

De voorbeeldconfiguraties in deze sectie gebruiken de opdracht IP-voorvoegsel-lijst, waarmee router 100 twee dingen kan doen:

- Laat updates toe voor elk netwerk met een prefixmasker met een lengte kleiner dan of gelijk

aan 19.

- Ontken alle netwerkupdates met een netwerkmaskerlengte groter dan 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 2000

```
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
```

De opdrachtoutput van de show ip bgp bevestigt dat de prefixlijst werkt zoals verwacht op router 100.

<#root>

```
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
```

Samenvattend, het gebruik van prefixlijsten is de gemakkelijkste manier om netwerken in BGP te filteren. In sommige gevallen echter—bijvoorbeeld als u oneven en even netwerken wilt filteren terwijl u ook de maskerlengte controleert—bieden uitgebreide toegangslijsten u een grotere flexibiliteit en controle dan prefixlijsten.

Standaardroutes van BGP-peers filteren

U kunt een standaardroute filteren of blokkeren, zoals 0.0.0.0/32 die door de BGP-peer wordt geadverteerd, met behulp van de opdracht prefix-lijst. U kunt de beschikbare ingang van 0.0.0.0 zien met de opdracht show ip bgp.

<#root>

```
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
```

De voorbeeldconfiguratie in deze sectie wordt op router 100 uitgevoerd met behulp van de opdracht IP-prefix-lijst.

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
```

Als u ip bgp na deze configuratie toont, zult u niet de 0.0.0.0 ingang zien, die in de vorige show ip bgp output beschikbaar was.

Gerelateerde informatie

- Casestudy's van BGP
- Ondersteuningspagina voor BGP
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.