Blockieren eines oder mehrerer Netzwerke von einem BGP-Peer

Inhalt

Einführung

Die Routenfilterung ist die Grundlage für die Festlegung von Border Gateway Protocol (BGP)-Richtlinien. Es gibt mehrere Möglichkeiten, ein oder mehrere Netzwerke von einem BGP-Peer zu filtern, einschließlich NLRI (Network Layer Reachability Information), AS_Path und Community-Attribute. In diesem Dokument wird die Filterung nur auf Basis von NLRI behandelt. Informationen zum Filtern auf Basis von AS_Path finden Sie unter Verwenden regulärer Ausdrücke im BGP. Weitere Informationen finden Sie im Abschnitt BGP-Filterung der BGP-Fallstudien.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der grundlegenden BGP-Konfiguration zu verfügen. Weitere Informationen finden Sie unter BGP-Anwenderberichte und BGP-Konfiguration.

Verwendete Komponenten

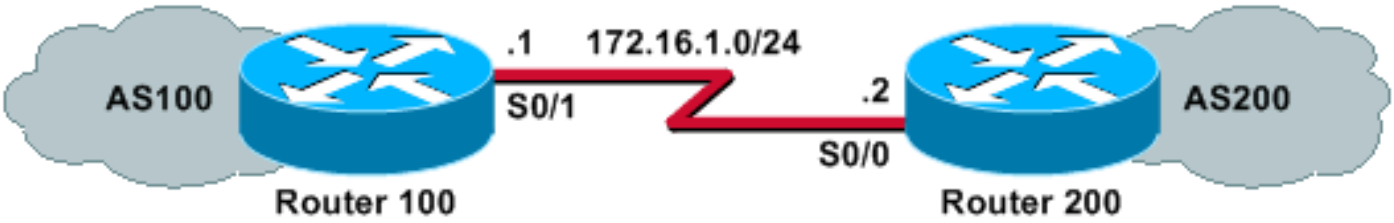
Die Informationen in diesem Dokument basieren auf der Cisco IOS® Softwareversion 12.2(28).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Identifizieren und Filtern von Routen basierend auf NLRI

Um Routing-Informationen einzuschränken, die der Router erfährt oder ankündigt, können Sie Filter basierend auf Routing-Updates verwenden. Die Filter bestehen aus einer Zugriffsliste oder einer Präfixliste, die auf Updates von Nachbarn und Nachbarn angewendet wird. In diesem Dokument werden die folgenden Optionen in diesem Netzwerkdiagramm behandelt:

Netzwerkdiagramm



Filtern mithilfe der Verteilerliste mit einer Standardzugriffsliste

Router 200 kündigt diese Netzwerke seinem Peer-Router 100 an:

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

Mithilfe dieser Beispielkonfiguration kann Router 100 ein Update für das Netzwerk 10.10.10.0/24 ablehnen und die Aktualisierungen der Netzwerke 192.168.10.0/24 und 10.10.0.0/19 in der BGP-Tabelle zulassen:

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
```

Diese **show ip bgp** command output bestätigt die Aktionen von 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
```

Filtern mithilfe der Verteilerliste mit erweiterter Zugriffsliste

Es kann schwierig sein, eine Standardzugriffsliste zum Filtern von Supernets zu verwenden.

Angenommen, Router 200 kündigt folgende Netzwerke an:

- 10.10.1.0/24 bis 10.10.31.0/24
- 10.10.0.0/19 (aggregiert)

Router 100 möchte nur das aggregierte Netzwerk 10.10.0.0/19 empfangen und alle spezifischen Netzwerke herausfiltern.

Eine Standard-Zugriffsliste, z. B. **Zugriffsliste 1 permit 10.10.0.0 0.31.255**, funktioniert nicht, da sie mehr Netzwerke zulässt, als gewünscht werden. Die Standardzugriffsliste betrachtet nur die Netzwerkadresse und kann die Länge der Netzwerkmaske nicht überprüfen. Diese Standard-Zugriffsliste erlaubt sowohl die /19-Aggregation als auch die spezifischeren /24-Netzwerke.

Verwenden Sie eine erweiterte Zugriffsliste, z. B. **Zugriffsliste 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0, um nur das Supernet 10.10.0.0/19 zuzulassen**. Das Format des erweiterten **Zugriffslisten-**Befehls finden Sie unter Zugriffsliste (IP erweitert).

In unserem Beispiel ist die Quelle 10.10.0.0, und der Source-Platzhalter 0.0.0.0 ist für eine exakte Übereinstimmung der Quelle konfiguriert. Die Maske 255.255.224.0 und der MaskenPlatzhalter 0.0.0.0 werden für die exakte Übereinstimmung der Quellmaske konfiguriert. Wenn eine der Access Points (Quelle oder Maske) nicht exakt übereinstimmt, wird sie von der Zugriffsliste abgelehnt.

Dadurch kann der Befehl **access-list** eine genaue Übereinstimmung der Quellnetznummer 10.10.0.0 mit der Maske 255.255.224.0 (und damit 10.10.0.0/19) zulassen. Die anderen spezifischeren /24-Netzwerke werden herausgefiltert.

> **Hinweis**: Bei der Konfiguration von Platzhalterkarten bedeutet **0**, dass es sich um ein exaktes Match-Bit und **1** um ein Do-Not-Care-Bit handelt.

Dies ist die Konfiguration auf 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
```

Die Ausgabe des Befehls **show ip bgp** von Router 100 bestätigt, dass die Zugriffsliste wie erwartet funktioniert.

```
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
```

Wie in diesem Abschnitt gezeigt, sind erweiterte Zugriffslisten benutzerfreundlicher, wenn einige Netzwerke im selben großen Netzwerk zugelassen und einige gesperrt werden müssen. In diesen Beispielen erfahren Sie mehr darüber, wie eine erweiterte Zugriffsliste in bestimmten Situationen hilfreich sein kann:

- **access-list 101 permit ip 192.168.0.0 0.0.0 255.255.252.0 0.0.0.0**

  Diese Zugriffsliste erlaubt nur das Supernet 192.168.0.0/22.

- **access-list 102 permit ip 192.168.10.0 0.0.0.255 255.255.0 0.0.0.0.255**

  Diese Zugriffsliste erlaubt alle Subnetze von 192.168.10.0/24. Mit anderen Worten, sie ermöglicht 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25 usw.: eines der Netzwerke 192.168.10.*x* mit einer Maske zwischen 24 und 32.

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

  Diese Zugriffsliste erlaubt jedes Netzwerkpräfix mit einer Maske zwischen 24 und 32.

Filtern mit dem Befehl ip prefix-list

Router 200 kündigt diese Netzwerke seinem Peer-Router 100 an:

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

Die Beispielkonfigurationen in diesem Abschnitt verwenden den Befehl **ip prefix-list**, mit dem Router 100 zwei Aufgaben ausführen kann:

- Zulassen von Updates für jedes Netzwerk mit einer Präfixmasklänge von maximal 19.
- Verweigern Sie alle Netzwerkaktualisierungen mit einer Netzwerkmaske von mehr als 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
```

Die Ausgabe des Befehls **show ip bgp** bestätigt, dass die Präfixliste auf Router 100 wie erwartet funktioniert.

```
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
```

Zusammenfassend lässt sich sagen, dass die Verwendung von Präfixlisten die einfachste Methode ist, Netzwerke im BGP zu filtern. In einigen Fällen - z. B. wenn Sie ungerade und sogar Netzwerke filtern möchten, während Sie gleichzeitig die Maskenlänge steuern - bieten erweiterte Zugriffslisten mehr Flexibilität und Kontrolle als Präfixlisten.

Filtern von Standard-Routen von BGP-Peers

Mit dem Befehl **prefix-list** können Sie eine Standardroute filtern oder blockieren, z. B. 0.0.0.0/32, die vom BGP-Peer angekündigt wird. Der verfügbare Eintrag 0.0.0.0 wird mit dem Befehl **show ip bgp** angezeigt.

```
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
```

Die Beispielkonfiguration in diesem Abschnitt wird mit dem Befehl **ip prefix-list** auf Router 100 durchgeführt.

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
```

Wenn Sie **show ip bgp** nach dieser Konfiguration ausführen, wird der Eintrag 0.0.0.0 nicht angezeigt, der in der vorherigen **show ip bgp-**Ausgabe verfügbar war.

Zugehörige Informationen

- BGP-Fallstudien
- BGP-Support-Seite
- Technischer Support und Dokumentation - Cisco Systems