從BGP對等體阻止一個或多個網路

目錄

簡介

路由過濾是設定邊界網關協定(BGP)策略的基礎。從BGP對等點過濾一個或多個網路的方法有多種，包括網路層可達性資訊(NLRI)和AS_Path以及社群屬性。本文檔僅討論基於NLRI的過濾。有關如何根據AS_Path進行過濾的資訊，請參閱在BGP中使用正規表示式。有關其他資訊，請參閱BGP案例研究的BGP過濾部分。

必要條件

需求

思科建議您瞭解基本的BGP配置。如需詳細資訊，請參閱BGP個案研究和設定BGP。

採用元件

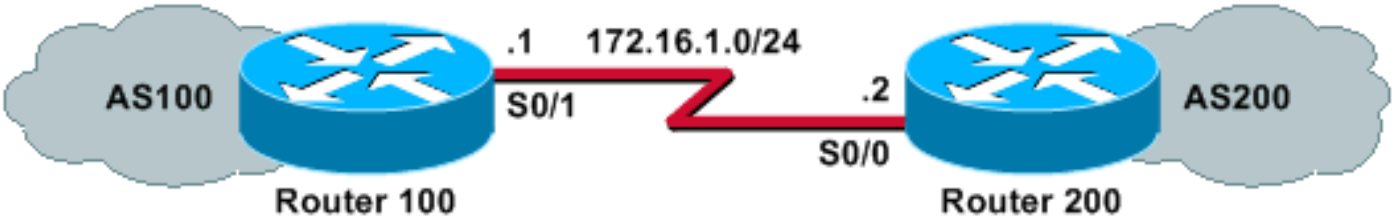
本檔案中的資訊是根據Cisco IOS®軟體版本12.2(28)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

基於NLRI的路由識別和過濾

要限制路由器獲知或通告的路由資訊，可以使用基於路由更新的過濾器。過濾器由訪問清單或字首清單組成，應用於鄰居和鄰居的更新。本檔案將透過此網路圖探討以下選項：

網路圖表



使用帶有標準訪問清單的分發清單進行過濾

Router 200向其對等路由器100通告這些網路：

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

此示例配置使路由器100能夠拒絕網路10.10.10.0/24的更新，並允許在其BGP表中更新網路192.168.10.0/24和10.10.0.0/19:

路由器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
```

路由器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
```

此**show ip bgp**命令輸出確認路由器100的動作：

```
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
```

使用帶有擴展訪問清單的分發清單進行過濾

使用標準訪問清單過濾超網可能會比較棘手。假設Router 200宣佈以下網路：

- 10.10.1.0/24 - 10.10.31.0/24
- 10.10.0.0/19（其總和）

路由器100希望僅接收聚合網路10.10.0.0/19，並過濾掉所有特定網路。

標準訪問清單(例如**access-list 1 permit 10.10.0.0 0.0.31.255**)無法工作，因為它允許的網路數超出了所需的數量。標準訪問清單僅檢視網路地址，無法檢查網路掩碼的長度。該標準訪問清單將允許/19聚合以及更具體的/24網路。

若要僅允許超級網路10.10.0.0/19，請使用延伸存取清單，例如**access-list 101 permit ip 10.10.0.0 0.0.0 255.255.224.0 0.0.0.0.0**。請參閱access-list（IP延伸），瞭解延伸型**access-list**命令的格式。

在本範例中，來源是10.10.0.0，且來源萬用字元0.0.0.0設定為來源的完全相符。遮罩255.255.224.0和mask-wildcard 0.0.0.0設定為與來源遮罩完全相符。如果其中任何一個（來源或遮罩）沒有完全相符專案，存取清單會拒絕此專案。

因此允許延伸型**access-list**命令允許來源網路編號10.10.0.0（遮罩為255.255.224.0）(因此是10.10.0.0/19)進行完全相符。 其他更具體的/24網路將被過濾掉。

附註：當設定萬用字元時，**0**表示它是一個完全匹配位元，**1**是一個不相關位元。

以下是Router 100上的組態：

路由器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
```

路由器100的**show ip bgp**命令輸出確認訪問清單是否按預期工作。

```
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
```

如本節所示，當同一個主網路中必須允許某些網路和禁止某些網路時，使用擴充存取清單會更方便。以下範例可深入瞭解延伸存取清單在某些情況下可如何提供幫助：

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

  此存取清單僅允許超級網路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**

  此訪問清單允許192.168.10.0/24的所有子網。換句話說，它將允許192.168.10.0/24、192.168.10.0/25、192.168.10.128/25等等：掩碼範圍從24到32的192.168.10.*x*網路。

- **access-list 103 permit ip 0.0.0.0 255.255.255.255.255.255.0 0.0.0.255**

  此存取清單允許遮罩範圍從24到32的任何網路首碼。

使用ip prefix-list命令進行過濾

Router 200向其對等路由器100通告這些網路：

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

本節中的示例配置使用ip prefix-list命令，該命令使路由器100能夠執行兩件事：

- 允許字首掩碼長度小於或等於19的任何網路的更新。
- 拒絕網路掩碼長度大於19的所有網路更新。

路由器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
```

路由器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
```

show ip bgp命令輸出確認字首清單在路由器100上是否按預期工作。

```
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
```

總之，在BGP中使用字首清單是最方便的網路過濾方式。但是，在某些情況下(例如，當您希望過濾奇數和偶數網路，同時還要控制掩碼長度時)，擴展訪問清單將為您提供比字首清單更大的靈活性和控制力。

從BGP對等點過濾預設路由

您可以使用prefix-list指令篩選或封鎖預設路由，例如由BGP對等點通告的0.0.0.0/32。可以使用show ip bgp命令看到0.0.0.0條目。

```
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
```

本部分中的示例配置使用ip prefix-list 命令在路由器100上執行。

路由器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
```

如果在此配置後執行**show ip bgp**，您將看不到0.0.0.0條目，該條目在之前的**show ip bgp**輸出中可用。

相關資訊

- BGP 個案研究
- BGP 支援頁面
- 技術支援與文件 - Cisco Systems