BGP ピアからの 1 つまたは複数のネットワークをブロックする方法

目次

概要

ルート フィルタリングは、ボーダー ゲートウェイ プロトコル（BGP）のポリシーを設定するための基礎です。 ネットワーク層到達可能性情報（NLRI）、AS_Path およびコミュニティ アトリビュートなど、BGP ピアから 1 つ以上のネットワークをフィルタリングするさまざまな方法があります。 このドキュメントでは、NLRI だけに基づいたフィルタリングについて説明します。 AS_Path に基づいてフィルタリングする方法については、『BGP での正規表現の使用』を参照してください。 詳細については、「BGP ケース スタディ」の「BGP フィルタリング」を参照してください。

前提条件

要件

BGP 設定に関する基本的な知識があることをお勧めします。 詳細については、「BGP ケース スタディ」および「BGP の設定」を参照してください。

使用するコンポーネント

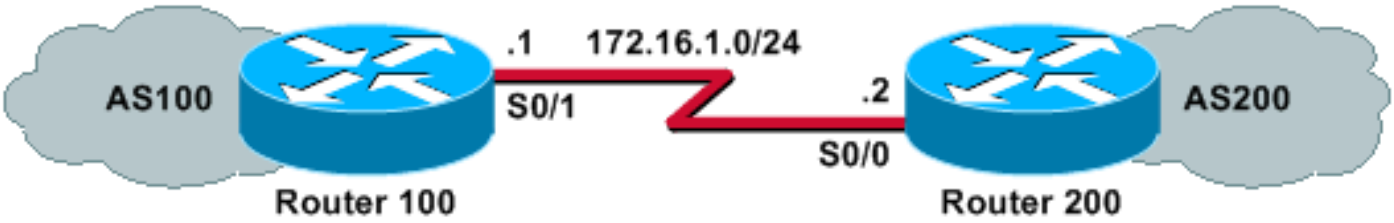
このドキュメントの情報は、Cisco IOS® ソフトウェア リリース 12.2(28) に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

NLRI ベースルートの識別とフィルタリング

ルータが学習またはアドバタイズするルーティング情報を制限するには、ルーティング更新に基づくフィルタを使用できます。 フィルタは、ネイバーへの更新およびネイバーからの更新に適用されるアクセス リストまたはプレフィックス リストで構成されます。 このドキュメントでは、次のネットワーク図で次のオプションを検討します。

ネットワーク図



標準アクセスリスト付きの配布リストを使用したフィルタリング

ルータ 200 は、次のネットワークをピアのルータ 100 に通知します。

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

この設定例では、ルータ 100 は BGP テーブルでネットワーク 10.10.10.0/24 用の更新を拒否し、ネットワーク 192.168.10.0/24 と 10.10.0.0/19 の更新を許可することができます。

ルータ 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
```

ルータ 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
```

次の **show ip bgp** コマンドの出力は、ルータ 100 の動作を示しています。

```
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
```

拡張アクセスリスト付きの配布リストを使用したフィルタリング

標準のアクセス リストを使用してスーパーネットをフィルタリングするのが難しい場合があります。 ルータ 200 が次のネットワークを通知するとします。

- 10.10.1.0/24 から 10.10.31.0/24 まで
- 10.10.0.0/19 (その集約)

ルータ 100 では集約ネットワーク 10.10.0.0/19 だけを受信し、他の個々のネットワークはすべてフィルタリングしたいとします。

access-list 1 permit 10.10.0.0 0.0.31.255 のような標準アクセス リストは、必要以上のネットワークを許可するため機能しません。 標準アクセス リストは、ネットワーク アドレスのみを調べ、ネットワーク マスクの長さをチェックできません。 この標準アクセス リストは、/19 の集約ネットワークだけでなく個々の /24 ネットワークも許可します。

スーパーネット 10.10.0.0/19 だけを許可するには、**access-list 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0** のような拡張アクセス リストを使用します。 拡張 access-list コマンドの書式については、「access-list (IP 拡張) 」を参照してください。

次の例では、送信元は 10.10.0.0 で、送信元を完全一致させるためにソース ワイルドカード 0.0.0.0 が設定されています。 送信元のマスクを完全に一致させるために、マスク 255.255.224.0 とマスク ワイルドカード 0.0.0.0 が設定されています。 これらのどちらか (発信元またはマスク) が完全に一致していない場合、アクセス リストは拒否します。

これで、拡張 access-list コマンドは、完全に一致した、マスク 255.255.224.0 の送信元のネットワーク番号 10.10.0.0 (したがって 10.10.0.0/19) を許可できます。 他の 24 の個々のネットワークはフィルタリングされます。

> **注:** ワイルドカードを設定する場合、**0** は完全一致のビットであることを、**1** は完全一致でなくてもかまわないビットであることを示します。

次にルータ 100 の設定を示します。

ルータ 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
```

次のルータ 100 からの **show ip bgp** コマンドの出力は、アクセス リストが期待どおりに動作していることを示しています。

```
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
```

このセクションで分かるように、同じ主ネットワーク内で許可するネットワークと拒否するネットワークがある場合は、拡張アクセス リストを使うと便利です。 次に、拡張アクセス リストが役立つ状況をいくつか紹介します。

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

  このアクセス リストは、スーパーネット 192.168.0.0/22 だけを許可します。

- **access-list 102 permit ip 192.168.10.0 0.0.0.255 255.255.255.0 0.0.0.255**

  このアクセス リストは、192.168.10.0/24 のすべてのサブネットを許可します。 つまり、192.168.10.0/24、192.168.10.0/25、192.168.10.128/25 など、 マスクが 24 ~ 32 の 192.168.10.x ネットワークすべてを許可します。

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

  このアクセス リストは、マスクが 24 ~ 32 の任意のネットワーク プレフィックスを許可します。

ip prefix-list コマンドを使用したフィルタリング

ルータ 200 は、次のネットワークをピアのルータ 100 に通知します。

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

このセクションの設定例では、ip prefix-list コマンドを使用して、ルータ 100 で次の 2 つのことを行えるようにします。

- プレフィックス マスクの長さが 19 以下のネットワークの更新を許可する。

- ネットワーク マスクの長さが 19 より長いすべてのネットワークの更新を拒否する。

ルータ 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
```

ルータ 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
```

次の **show ip bgp** コマンドの出力は、プレフィックス リストがルータ 100 で想定どおりに動作していることを示しています。

```
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
```

結論として、BGP でネットワークをフィルタリングするには、プレフィックス リストを使用するのが最も便利な方法です。 ただし、場合によっては、マスク長も制御しながら、奇数および偶数のネットワークをフィルタリングする場合などは、拡張アクセス リストのほうがプレフィックス リストより柔軟に制御できます。

BGP ピアからのデフォルト ルートのフィルタリング

prefix-list コマンドを使用して、BGP ピアによってアドバタイズされる 0.0.0.0/32 のようなデフォルト ルートをフィルタリングまたはブロックできます。 **show ip bgp** コマンドを使用すると、0.0.0.0 エントリを使用できることが分かります。

```
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
```

このセクションの設定例は ip prefix-list コマンドを使用して、ルータ 100 で実行されます。

ルータ 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
```

この設定後に **show ip bgp** を実行すると、前の **show ip bgp** 出力で使用できた 0.0.0.0 エントリは表示されません。

関連情報

- BGP ケース スタディ
- BGP に関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems