IPv6 BGP で IPV6 Remote Triggered Black Hole を設定する

内容

概要

このドキュメントでは、IPV6 Remote Triggered Black Hole(RTBH)で見られる動作について説明します。 ルート マップを使用して IPv6 トラフィックを意図的に廃棄するシナリオを示します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IPv6
- ボーダー ゲートウェイ プロトコル（BGP）

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15.4バージョンに基づくものです。

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

RTBH フィルタリングは、サービス妨害（DoS）攻撃を防ぐために一般的に採用される技術です。DoS 攻撃に見られる一般的な問題は、ネットワークが膨大な量の不要な/悪意のあるトラフィックでいっぱいにされることです。これにより、リンクが反応しなくなったり、CPU 使用率が高まったりするなどの問題が発生します。これは、正当なトラフィックを妨害し、ネットワークに重大な影響を及ぼします。

RFC 2545によると、BGPスピーカがネクストホップフィールドのネットワークアドレスに含まれるグローバルIPv6アドレスで識別されるエンティティと共通のサブネットを共有し、ルートがアドバタイズされるピアの場合にのみ、リンクローカルアドレスがネクストホップフィールドに含まれます。その他のケースでは、BGPスピーカはネクストホップのグローバルIPv6アドレスだけをNetwork Addressフィールドでピアにアドバタイズします。

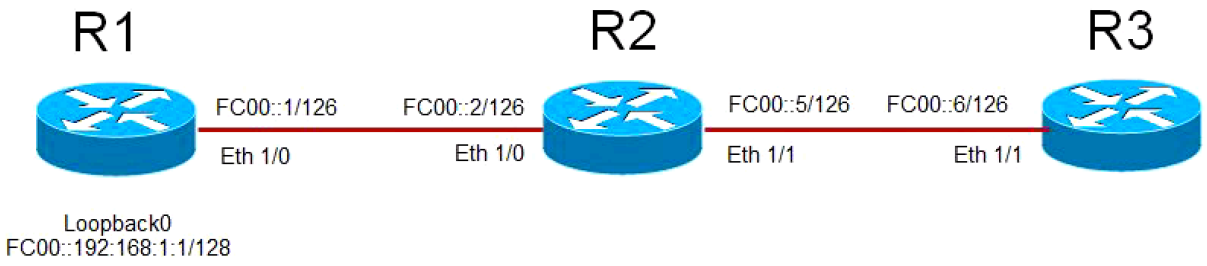
基本的に、直接接続されたサブネット(IPv6)にIPv6 EBGPネイバー関係がある場合、その関係はリンクローカルIPとグローバルIPv6アドレスをネクストホップとして伝送します。ただし、Request for Command(RFC)では、どちらのコマンドを使用するかを指定していません。シスコは、パケットを送信する間は常に最短距離であるため、リンクローカルアドレスを優先します。RTBHを使用する場合は、問題である可能性があります。このドキュメントでは、その対処方法について説明します。

設定

このドキュメントでは、RTBHを動作させるために使用される動作とコマンドについて説明するユースケースを取り上げています。

ネットワーク図

このイメージは、このドキュメントの残りの部分のサンプルトポロジとして使用されます。



- R1 には、R2 との EBGP ネイバー関係があります。R2 には、R3 との EBGP ネイバー関係があります。
- ルータ R1 は、BGP を介してループバック 0（FC00::192:168:1:1/128）を R2 にアドバタイズし、R2 はそれを R3 にアドバタイズします。
- R3 はルート マップを使用して、R1 のループバック プレフィクスのネクスト ホップを、ルーティング テーブルで「NULL 0」を指すダミーの IPv6 アドレスに設定します。

関連コンフィギュレーション

この設定は、RTBHが使用される状況をシミュレートするために、異なるルータで使用されます。

R1

```
interface Ethernet1/0
 no ip address
 ipv6 address FC00::1/126
end
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address FC00::192:168:1:1/128
 !
 router bgp 65500
 bgp router-id 192.168.1.1
 bgp log-neighbor-changes
 neighbor FC00::2 remote-as 65501
 !
 address-family ipv6
network FC00::/126
 network FC00::192:168:1:1/128
 neighbor FC00::2 activate
```

R2

```
interface Ethernet1/0
 no ip address
 ipv6 address FC00::2/126
end
!
interface Ethernet1/1
 no ip address
 ipv6 address FC00::5/126
!
router bgp 65501
 bgp router-id 192.168.1.2
 bgp log-neighbor-changes
 neighbor FC00::1 remote-as 65500
 neighbor FC00::6 remote-as 65502
 !
 address-family ipv6
 network FC00::/126
 network FC00::4/126
 neighbor FC00::1 activate
 neighbor FC00::6 activate
```

R3

```
interface Ethernet1/1
 no ip address
 ipv6 address FC00::6/126
end
!
ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
 match ipv6 address prefix-list BLACKHOLE-PREFIX
 set ipv6 next-hop FC00::192:168:1:3
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
 bgp router-id 192.168.1.3
 bgp log-neighbor-changes
 neighbor FC00::5 remote-as 65501
```

```
!
 address-family ipv6
 network FC00::4/126
 neighbor FC00::5 activate
 neighbor FC00::5 route-map BLACKHOLE-PBR in
```

確認

テスト ケース 1

R3 に設定されたポリシーベース ルーティング（PBR）がない場合、ルーティング テーブルで、R3 での R1 のループバックへのルートは、R2 のリンク ローカル アドレス FE80::A8BB:CCFF:FE00:A211 を指します。

```
BGP Configuration

router bgp 65502
 bgp router-id 192.168.1.3
 bgp log-neighbor-changes
 neighbor FC00::5 remote-as 65501
 !
 address-family ipv6
 network FC00::4/126
 neighbor FC00::5 activate


BGP has both next-hops.

R3#show bgp ipv6 unicast FC00::192:168:1:1/128
BGP routing table entry for FC00::192:168:1:1/128, version 4
Paths: (1 available, best #1, table default)
 Not advertised to any peer
 Refresh Epoch 1
 65501 65500
   FC00::5 (FE80::A8BB:CCFF:FE00:A211) from FC00::5 (192.168.1.2)
     Origin IGP, localpref 100, valid, external, best
     rx pathid: 0, tx pathid: 0x0


Routing Table has Link Local address as the next-hop.

R3#show ipv6 route FC00::192:168:1:1
Routing entry for FC00::192:168:1:1/128
 Known via "bgp 65502", distance 20, metric 0, type external
 Route count is 1/1, share count 0
 Routing paths:
   FE80::A8BB:CCFF:FE00:A211, Ethernet1/1
     MPLS label: nolabel
     Last updated 00:02:45 ago


Destination is reachable

R3#ping ipv6 FC00::192:168:1:1
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

テスト ケース 2

R3でルートマップ**BLACKHOLE-PBR**を使用してPBRが設定されている場合、**FC00::192:168:1:1/128（R1のループバック）**（R1のループバック）のネクストホップが引き続きR2のリンクローカルアドレス**FE 8BB 80::FE 80::A8FE CCFF:FE00:A211**。そのため、トラフィックはブラックホール化されず、リンクローカルアドレスを使用してルーティングされます。

```
BGP Configuration

ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
 match ipv6 address prefix-list BLACKHOLE-PREFIX
 set ipv6 next-hop FC00::192:168:1:3
!
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
 bgp router-id 192.168.1.3
 bgp log-neighbor-changes
 neighbor FC00::5 remote-as 65501
 !
 address-family ipv4
 no neighbor FC00::5 activate
 exit-address-family
 !
 address-family ipv6
 network FC00::4/126
 neighbor FC00::5 activate
 neighbor FC00::5 route-map BLACKHOLE-PBR in


Next-hop in BGP changes to the one defined in route-map.

R3#show bgp ipv6 unicast FC00::192:168:1:1/128
BGP routing table entry for FC00::192:168:1:1/128, version 4
Paths: (1 available, best #1, table default)
 Not advertised to any peer
 Refresh Epoch 1
 65501 65500
   FC00::192:168:1:3 (FE80::A8BB:CCFF:FE00:A211) from FC00::5 (192.168.1.2)
     Origin IGP, localpref 100, valid, external, best
     rx pathid: 0, tx pathid: 0x0


New next-hop is not reachable and points to Null 0

R3#show ipv6 route FC00::192:168:1:3
Routing entry for FC00::192:168:1:3/128
 Known via "static", distance 1, metric 0
 Route count is 1/1, share count 0
 Routing paths:
   directly connected via Null0
     Last updated 00:19:23 ago
```

```
Routing table still uses Link Local address as next-hop.

R3#show ipv6 route FC00::192:168:1:1
Routing entry for FC00::192:168:1:1/128
 Known via "bgp 65502", distance 20, metric 0, type external
 Route count is 1/1, share count 0
 Routing paths:
FE80::A8BB:CCFF:FE00:A211, Ethernet1/1
     MPLS label: nolabel
     Last updated 00:00:41 ago


Destination is still reachable.

R3#ping ipv6 FC00::192:168:1:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

テスト ケース 3

この動作を克服するには、R3でBGPネイバー設定コマンドdisable-connected-checkを使用します。Disable-connected-checkは、ネイバーのIPv6アドレスが1つのホップ方法(IPv6)のみであると仮定するために使用します。このコマンドが使用される最も一般的なシナリオは、直接接続されたルータのループバックに EBGP ネイバー関係が確立されている場合です。この場合、このコマンドは、ルータがEBGPネイバー関係を構築していて、共通のサブネット上にないことを示しています。ネイバーシップはループバック全体に存在する可能性があるため、ルータはリンクローカルアドレスではなく、グローバルIPv6アドレス(IPv6)だけを伝送するプレフィクスをアドバタイズします。

このコマンドを追加すると、R3 のルーティング テーブルにおける R1 のループバック 192:168:1:1/128 のルートは、FC00::192:168:1:3 であるルート マップに従ってネクスト ホップを指すようになります。 FC00::192:168:1:3にはNull 0を指すルートがあるため、トラフィックはブラックホール化されます。

```
BGP Configuration

ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
 match ipv6 address prefix-list BLACKHOLE-PREFIX
 set ipv6 next-hop FC00::192:168:1:3
!
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
 bgp router-id 192.168.1.3
 bgp log-neighbor-changes
 neighbor FC00::5 remote-as 65501
neighbor FC00::5 disable-connected-check
 !
```

```
 address-family ipv4
 no neighbor FC00::5 activate
 exit-address-family
 !
 address-family ipv6
 network FC00::4/126
 neighbor FC00::5 activate
 neighbor FC00::5 route-map BLACKHOLE-PBR in
```

Next-hop in BGP changes to the one defined in route-map. There is no Link Local Address.

```
R3#show bgp ipv6 unicast FC00::192:168:1:1/128
BGP routing table entry for FC00::192:168:1:1/128, version 4
Paths: (1 available, best #1, table default)
 Not advertised to any peer
 Refresh Epoch 1
 65501 65500
   FC00::192:168:1:3 from FC00::5 (192.168.1.2)
     Origin IGP, localpref 100, valid, external, best
     rx pathid: 0, tx pathid: 0x0
```

Routing table uses the new next-hop.

```
R3#show ipv6 route FC00::192:168:1:1
Routing entry for FC00::192:168:1:1/128
 Known via "bgp 65502", distance 20, metric 0, type external
 Route count is 1/1, share count 0
 Routing paths:
FC00::192:168:1:3
     MPLS label: nolabel
     Last updated 00:00:37 ago
```

New next-hop is pointed to Null 0. Traffic will be dropped.

```
R3#show ipv6 route FC00::192:168:1:3
Routing entry for FC00::192:168:1:3/128
 Known via "static", distance 1, metric 0
 Route count is 1/1, share count 0
 Routing paths:
   directly connected via Null 0
     Last updated 02:18:03 ago
```

Destination is not reachable

```
R3#ping ipv6 FC00::192:168:1:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

注： CSCuv60686**disable-connected-check**

トラブルシュート

現在のところ、このドキュメントに関する特定のトラブルシューティング情報はありません。