Configuration du trou noir déclenché à distance IPV6 avec IPv6 BGP

Contenu

Introduction

Ce document décrit le comportement observé avec le RTBH (Remote Triggered Black Hole) IPV6. Il montre un scénario où le trafic IPv6 est intentionnellement en trou noir à l'aide d'une carte de route.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IPv6
- BGP (Border Gateway Protocol)

Components Used

Les informations de ce document sont basées sur la version 15.4 du logiciel Cisco IOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Le filtrage RTBH est une technique généralement utilisée pour empêcher les attaques par déni de service (DoS). Un problème courant observé avec les attaques DoS est que le réseau est inondé d'énormes volumes de trafic indésirable/malveillant. Cela entraîne un blocage des liaisons et d'autres problèmes tels qu'un CPU élevé, etc. Cela étouffe le trafic légitime et entraîne de graves conséquences sur le réseau.

Conformément à la RFC 2545, l'adresse link-local doit être incluse dans le champ Next Hop si et uniquement si le haut-parleur BGP partage un sous-réseau commun avec l'entité identifiée par l'adresse IPv6 globale figurant dans le champ Network Address of Next Hop et l'homologue auquel la route est annoncée. Dans tous les autres cas, un haut-parleur BGP doit annoncer à son homologue dans le champ Network Address (Adresse réseau) uniquement l'adresse IPv6 globale du saut suivant.

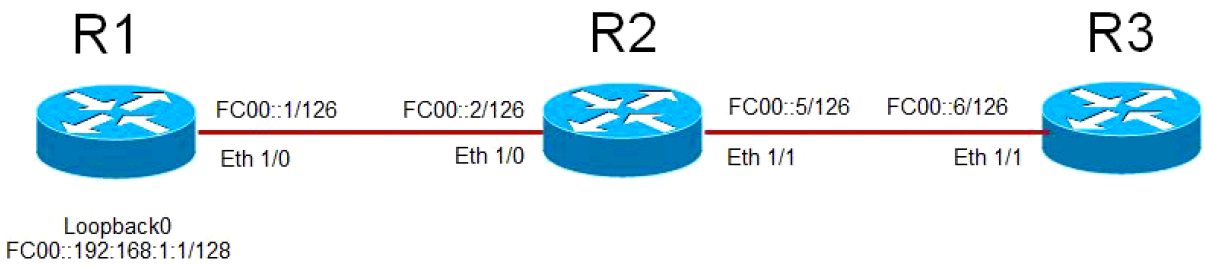
Cela signifie en gros que si vous avez une relation de voisinage EBGP IPv6 sur un sous-réseau directement connecté , alors il transporte l'adresse IP locale de liaison ainsi que l'adresse IPv6 globale comme saut suivant. Cependant, Request for Command (RFC) ne spécifie pas lequel doit être préféré. Cisco préfère l'adresse link-local, car lorsqu'il envoie le paquet, il s'agit toujours de la distance la plus courte. Lorsque vous utilisez RTBH, il peut s'agir d'un problème et ce document explique comment le traiter.

Configuration

Ce document prend un exemple d'utilisation pour expliquer le comportement et les commandes utilisées pour faire fonctionner RTBH.

Diagramme du réseau

Cette image est utilisée comme exemple de topologie pour le reste de ce document.



- R1 a une relation de voisinage EBGP avec R2 et R2 a une relation de voisinage EBGP avec R3.
- Le routeur R1 annonce son bouclage 0 (FC00::192:168:1:1/128) via BGP à R2 et R2 l'annonce à R3.
- R3 utilise une route-map pour définir le tronçon suivant du préfixe de bouclage de R1 sur une adresse IPv6 factice qui pointe sur « NULL 0 » dans la table de routage.

Configuration pertinente

Cette configuration est utilisée sur différents routeurs pour simuler une situation dans laquelle RTBH serait utilisé :

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
```

Vérification

Cas d'essai 1

Lorsqu'aucun routage basé sur des stratégies (PBR) n'est configuré sur R3, dans la table de routage, la route vers le bouclage de R1 sur R3 pointe vers l'adresse link-local de R2 FE80::A8BB:CCFF:FE00:A211.

```
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
```

Cas d'essai 2

Lorsqu'un PBR est configuré à l'aide de la route-map **BLACKHOLE-PBR** sur R3, il est observé que pour **FC00::192:168:1:1/128** (bouclage de R1), le tronçon suivant de la table de routage pointe toujours vers l'adresse locale de liaison de R2 **FE88880:0::: A8BB:CCFF:FE00:A211**. Par conséquent, le trafic n'est jamais en trou noir et est routé à la place à l'aide d'adresses link-local.

```
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
```

Cas d'essai 3

Afin de surmonter ce comportement, utilisez la commande de configuration de voisin BGP **disable-connected-check** sur R3. Disable-connected-check est utilisé pour présumer que l'adresse IPv6 du voisin n'est qu'un seul chemin de saut . Le scénario le plus courant dans lequel cette commande est utilisée est lorsque la relation de voisinage EBGP est établie sur les bouclages pour les routeurs connectés directement. Dans ce cas, la commande donne l'impression que les routeurs établissent une relation de voisinage EBGP et ne se trouvent pas sur un sous-réseau commun. Le voisinage peut être à travers des boucles et donc, le routeur pendant qu'il annonce le préfixe qui ne porte pas l'adresse link-local mais seulement l'adresse IPv6 globale .

Une fois cette commande ajoutée, vous pouvez voir que la route pour le bouclage de R1 **192:168:1:1/128** dans la table de routage de R3, pointe vers le tronçon suivant conformément à route-map qui est **FC00::192:168:1:3**. Maintenant, depuis **FC00::192:168:1:3** a une route pointant vers Null 0, par conséquent, le trafic est en trou noir.

```
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)
```

> **Note**: Une nouvelle amélioration CSCuv60686 modifie ce comportement de sorte que route-map prenne effet sans utiliser la commande **disable-connected-check**.

Dépannage

Ce document ne contient actuellement aucune information de dépannage spécifique.