Konfigurieren von IPV6 Remote Triggered Black Hole mit IPv6 BGP

Inhalt

Einführung

Dieses Dokument beschreibt das Verhalten, das mit dem IPV6 Remote Triggered Black Hole (RTBH) beobachtet wird. Es zeigt ein Szenario, in dem IPv6-Datenverkehr mithilfe einer Routenübersicht absichtlich schwarz gehalten wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- IPv6
- Border Gateway Protocol (BGP)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Version 15.4 der Cisco IOS-Software.

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.

Hintergrundinformationen

Die RTBH-Filterung ist eine Technik, die in der Regel eingesetzt wird, um DoS-Angriffe (Denial of Service) zu verhindern. Ein häufiges Problem bei DoS-Angriffen ist, dass das Netzwerk mit einem enormen Volumen an unerwünschtem/schädlichem Datenverkehr überflutet wird. Dies führt zu Engpässen und anderen Problemen wie hoher CPU-Auslastung. Dies führt zu einem Verlust von legitimem Datenverkehr und schwerwiegenden Auswirkungen auf das Netzwerk.

Gemäß RFC 2545 wird die lokale Adresse der Verbindung in das Next-Hop-Feld eingefügt, wenn und nur, wenn der BGP-Sprecher ein gemeinsames Subnetz mit der Entität teilt, die durch die globale IPv6-Adresse identifiziert wird, die im Feld "Network Address of Next Hop" (Netzwerkadresse des nächsten Hop) übertragen wird, und dem Peer, dem die Route angekündigt wird. In allen anderen Fällen gibt ein BGP-Sprecher seinem Peer im Feld "Network Address" (Netzwerkadresse) nur die globale IPv6-Adresse des nächsten Hop bekannt.

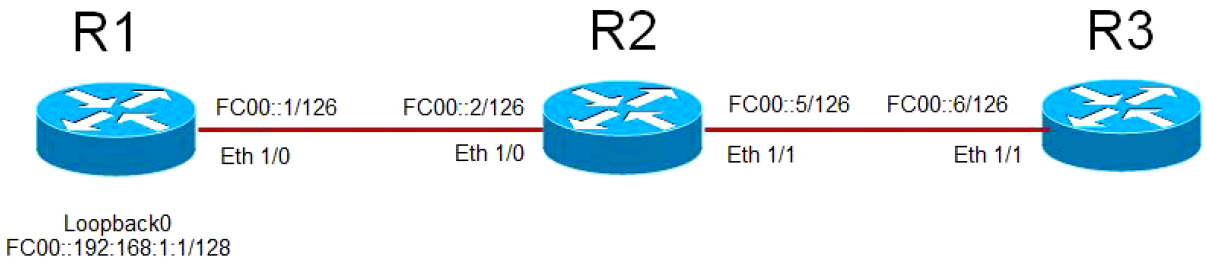
Im Grunde bedeutet dies, dass wenn Sie eine IPv6-EBGP-Nachbarbeziehung in einem direkt verbundenen Subnetz haben, dann die lokale IP-Adresse der Verbindung sowie die globale IPv6-Adresse als nächster Hop enthalten sind. Bei der Request for Command (RFC) wird jedoch nicht angegeben, welcher Befehl bevorzugt werden soll. Cisco bevorzugt lokale Link-Adressen, da sie das Paket zwar senden, aber immer die kürzeste Entfernung sind. Wenn Sie RTBH verwenden, kann es sich um ein Problem handeln, und in diesem Dokument wird erläutert, wie Sie damit umgehen.

Konfigurieren

In diesem Dokument wird anhand eines Anwendungsbeispiels das Verhalten und die Befehle erläutert, mit denen RTBH funktioniert.

Netzwerkdiagramm

Dieses Bild wird als Beispieltopologie für den Rest dieses Dokuments verwendet.



- R1 hat eine EBGP-Nachbarbeziehung zu R2, und R2 hat eine EBGP-Nachbarbeziehung zu R3.
- Router R1 kündigt sein Loopback 0 (FC00::192:168:1:1/128) via BGP an R2 und R2 an, es an R3 weiterzuleiten.
- R3 verwendet eine route-map, um den nächsten Hop für das Loopback-Präfix von R1 auf eine Dummy-IPv6-Adresse festzulegen, die in der Routing-Tabelle auf NULL verweist.

Relevante Konfiguration

Diese Konfiguration wird auf verschiedenen Routern verwendet, um eine Situation zu simulieren,

in der RTBH verwendet wird:

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
```

Überprüfen

Testfall 1

Wenn für R3 kein richtlinienbasiertes Routing (Policy-Based Routing, PBR) konfiguriert ist, wird in der Routing-Tabelle die Route zum R1-Loopback auf R3 auf die lokale Adresse der R2-Verbindung **FE80:A8BB:CCFF:FE00:A211** weitergeleitet.

```
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
```

Testfall 2

Wenn PBR mit route-map **BLACKHOLE-PBR** auf R3 konfiguriert ist, wird bei **FC00:192:168:1:1/128** (R1's Loopback) festgestellt, dass Next-Hop in der Routing-Tabelle weiterhin auf die lokale Adresse der R2 verweist **FE80::A8BB:CCFF:FE00:A211**. Daher wird der Datenverkehr niemals schwarz gespeichert und stattdessen über lokale Adressen weitergeleitet.

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
```

Testfall 3

Um dieses Verhalten zu überwinden, verwenden Sie den BGP-Nachbarkonfigurationsbefehl **disable-connected-check** auf R3. Disable-connected-check wird verwendet, um davon auszugehen, dass die IPv6-Adresse des Nachbarn nur eine Hop-Richtung ist. Das häufigste Szenario, in dem dieser Befehl verwendet wird, ist, wenn auf Loopbacks für direkt verbundene Router eine EBGP-Nachbarbeziehung hergestellt wird. In diesem Fall vermittelt der Befehl den Eindruck, dass Router eine EBGP-Nachbarbeziehung aufbauen und sich nicht im gemeinsamen Subnetz befinden. Die Nachbarschaft könnte sich über Loopbacks und damit Router befinden, während sie das Präfix ankündigt, das nicht die lokale Adresse der Verbindung, sondern nur die globale IPv6-Adresse enthält.

Nach dem Hinzufügen dieses Befehls sehen Sie, dass die Route für das Loopback von R1 **192:168:1:1/128** in der Routing-Tabelle von R3 in der Route-Map **FC00:192:168:1:3** auf den nächsten Hop verweist. Seit **FC00::192:168:1:3** hat **nun** eine Route, die auf Null 0 zeigt, daher ist der Datenverkehr schwarz verschwunden.

```
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)
```

> **Hinweis**: Eine neue Verbesserung CSCuv60686 ändert dieses Verhalten, sodass route-map ohne Verwendung des Befehls **disable-connected-check** wirksam wird.

Fehlerbehebung

Für dieses Dokument sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.