Configurare il buco nero attivato da remoto IPV6 con IPv6 BGP

Sommario

Introduzione

In questo documento viene descritto il comportamento rilevato con il buco nero attivato da remoto (RTBH) di IPV6. Viene mostrato uno scenario in cui il traffico IPv6 è intenzionalmente bloccato dal nero utilizzando una mappa dei percorsi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- IPv6
- Border Gateway Protocol (BGP)

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco IOS versione 15.4.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il filtro RTBH è una tecnica generalmente utilizzata per prevenire gli attacchi DoS (Denial of Service). Un problema comune riscontrato negli attacchi DoS è che la rete è invasa da enormi volumi di traffico indesiderato/dannoso. Ciò provoca il blocco dei collegamenti e altri problemi come CPU elevata e così via. Questo diminuisce il traffico legittimo e ha gravi ripercussioni sulla rete.

In base alla RFC 2545, l'indirizzo locale del collegamento deve essere incluso nel campo Hop successivo se e solo se il diffusore BGP condivide una subnet comune con l'entità identificata dall'indirizzo IPv6 globale presente nel campo Indirizzo di rete dell'hop successivo e il peer a cui viene annunciato il percorso. In tutti gli altri casi, un altoparlante BGP deve annunciare al proprio peer nel campo Indirizzo di rete solo l'indirizzo IPv6 globale dell'hop successivo.

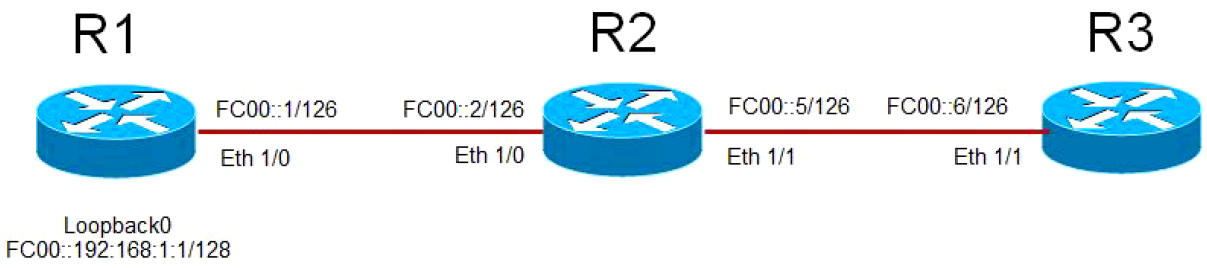
In pratica significa che se si dispone di una relazione adiacente EBGP IPv6 su una subnet a connessione diretta, come hop successivo vengono trasmessi l'indirizzo IP locale del collegamento e l'indirizzo IPv6 globale. Tuttavia, Request for Command (RFC) non specifica quale deve essere preferito. Cisco preferisce l'indirizzo locale del collegamento perché, mentre invia il pacchetto, è sempre la distanza più breve. Quando si utilizza il protocollo RTBH, potrebbe trattarsi di un problema e il presente documento spiega come gestirlo.

Configurazione

In questo documento viene illustrato uno Use Case per il funzionamento del protocollo RTBH.

Esempio di rete

Questa immagine viene utilizzata come topologia di esempio per il resto del documento.



- R1 ha una relazione di tipo adiacente EBGP con R2 e R2 ha una relazione di tipo adiacente EBGP con R3.
- Il router R1 annuncia il proprio loopback 0 (FC00::192:168:1:1/128) tramite BGP su R2, che viene pubblicizzato da R2 su R3.
- R3 utilizza una route-map per impostare l'hop successivo per il prefisso di loopback di R1 su un indirizzo IPv6 fittizio che punta a "NULL 0" nella tabella di routing.

Configurazione rilevante

Questa configurazione viene usata su router diversi per simulare una situazione in cui verrebbe usato il protocollo RTBH:

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
```

Verifica

Test case 1

Se in R3 non è configurato alcun routing basato su policy (PBR), nella tabella di routing instradare il loopback di R1 su R3 all'indirizzo locale del collegamento di 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
```

Test case 2

Quando il PBR è configurato utilizzando la route-map **BLACKHOLE-PBR** su R3, si noti che per **FC00::192:168:1:1/128** (loopback di R1), l'hop successivo nella tabella di routing punta ancora all'indirizzo locale del collegamento di R2 **FE80::A8BB:CCFF:FE00:A211**. Pertanto, il traffico non viene mai bloccato e instradato utilizzando gli indirizzi locali del collegamento.

```
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
```

Test case 3

Per risolvere questo problema, utilizzare il comando di configurazione dei router adiacenti BGP **disable-connected-check** su R3. Disable-connected-check viene utilizzato per presupporre che l'indirizzo IPv6 del router adiacente sia solo di un hop. Lo scenario più comune in cui viene utilizzato questo comando è quando la relazione tra nodi adiacenti EBGP viene stabilita sui loopback per i router connessi direttamente. In questo caso, il comando dà l'impressione che i router stiano costruendo una relazione tra nodi adiacenti EBGP e non si trovino su una subnet comune. È possibile che la vicinanza si trovi tra più loopback e, di conseguenza, router mentre annuncia il prefisso che non riporta l'indirizzo locale del collegamento ma solo l'indirizzo IPv6 globale.

Dopo aver aggiunto questo comando, è possibile visualizzare il percorso per il loopback di R1 **192:168:1:1/128** nella tabella di routing di R3, che punta all'hop successivo in base alla route-map **FC00:192:168:1:3**. Ora, poiché **FC00::192:168:1:3** ha una route che punta a Null 0, il traffico è bucato nero.

```
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)
```

> **Nota:** La nuova funzionalità avanzata CSCuv60686 modifica questo comportamento in modo che la route-map venga applicata senza utilizzare il comando **disable-connected-check**.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche sulla risoluzione dei problemi per questo documento.