Configuration de l'IPv6 Black-Holing via l'interface Null0

Contenu

Introduction

Ce document décrit comment configurer Black-Holing dans IPv6 via l'interface Null0. Le routage à trous noirs est une méthode qui permet à l'administrateur de bloquer le trafic indésirable, tel que le trafic provenant de sources illégales ou le trafic généré par une attaque par déni de service (DoS), en acheminant dynamiquement le trafic vers une interface indisponible ou vers un hôte conçu pour collecter des informations à des fins d'enquête, ce qui atténue l'impact de l'attaque sur le réseau.

Conditions préalables

Conditions requises

Assurez-vous de respecter ces conditions avant de tenter cette configuration :

- Comprendre le protocole de routage BGP et son fonctionnement
- Comprendre le schéma d'adressage IPv6

Components Used

Les informations de ce document sont basées sur le routeur de la gamme Cisco 7200 avec le logiciel Cisco IOS® version 15.0(1).

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

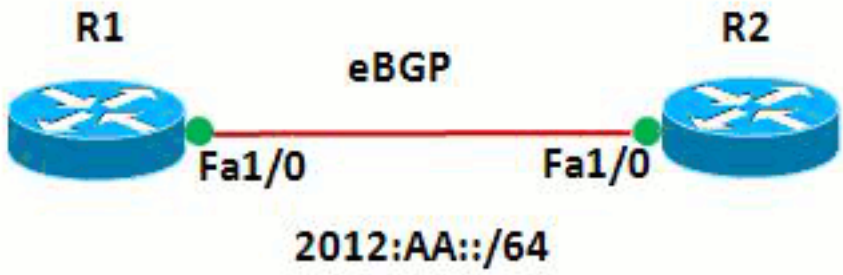
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin de trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans ce réseau, les routeurs et R1 et R2 forment une relation eBGP les uns avec les autres. Les routeurs utilisent OSPFv3 pour communiquer en interne. Dans le routeur R1, le Black-holing est obtenu par la configuration de Null0 de sorte que tous les paquets dont l'adresse source est 20:20::20/128 soient dirigés vers Null0. En d'autres termes, tout le trafic acheminé vers Null0 est abandonné.

Exemples de configuration

Ce document utilise les configurations suivantes :

- Routeur R1
- Routeur R2

Routeur R1

```
!
hostname R1
!
no ip domain lookup
ip cef
```

```
ipv6 unicast-routing
ipv6 cef
!
!
interface Loopback1
 no ip address
 ipv6 address AA::1/128
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Loopback10
 no ip address
 ipv6 address AA:10::10/128
 ipv6 enable
!
interface FastEthernet1/0
 no ip address
 speed auto
 duplex auto
 ipv6 address 2012:AA::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
router bgp 6501
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor BB::1 remote-as 6502
 neighbor BB::1 ebgp-multihop 2
 neighbor BB::1 update-source Loopback1
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
  redistribute static
  network AA:10::10/128
  neighbor BB::1 activate
 exit-address-family
!
ipv6 route 20:20::20/128 Null0
ipv6 router ospf 10
 router-id 1.1.1.1
!
end
```

Routeur R2

```
!
hostname R2
!
ipv6 unicast-routing
ipv6 cef
!
!
interface Loopback1
 no ip address
 ipv6 address BB::1/128
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface Loopback20
```

```
 no ip address
 ipv6 address 20:20::20/128
 ipv6 enable
!
interface FastEthernet1/0
 no ip address
 speed auto
 duplex auto
 ipv6 address 2012:AA::2/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
router bgp 6502
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor AA::1 remote-as 6501
 neighbor AA::1 ebgp-multihop 2
 neighbor AA::1 update-source Loopback1
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
  network 20:20::20/128
  neighbor AA::1 activate
 exit-address-family
!
ipv6 router ospf 10
 router-id 2.2.2.2
!
end
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Afin de vérifier la configuration eBGP, utilisez les commandes show ipv6 route bgp et show bgp ipv6 unicast dans le routeur R1.

Routeur R1

show ipv6 route

```
R1#show ipv6 route bgp
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-
user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R -
RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea,
IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor
Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext
1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
!--- The router R2 advertises the network 20:20::20/128,
```

```
!--- but still the routing table is empty.
```

Pour vérifier quelles sont les routes reçues par BGP, utilisez la commande **show bgp ipv6 unicast**.

```
R1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 1.1.1.1
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
*  20:20::20/128    BB::1                    0
0 6502 I
*>                  ::                       0
32768 ?
*> AA:10::10/128    ::                       0
32768 I
 !--- Note that the route 20:20::20/128 is received, !--
- but it is not installed in the routing table.
```

Utilisez la source comme interface de bouclage 20 afin d'essayer d'envoyer une requête ping au routeur R1 à partir du routeur R2.

```
R2#ping ipv6 AA:10::10 source lo20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to AA:10::10, timeout is 2 seconds:
Packet sent with a source address of 20:20::20
.....
Success rate is 0 percent (0/5)
!--- The reason is the ICMP packet reaches !--- router R1 with source address as !---
20:20::20/128 and therefore gets dropped.
```

Essayez d'envoyer une requête ping au routeur R1 à partir du routeur R2 sans utiliser l'interface de bouclage comme source.

```
R2#ping AA:10::10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to AA:10::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/61/180 ms
!--- In this case, the ICMP packet has !--- the source address as BB::1.
```

Si l'instruction **ipv6 route 20:20::20/128 Null0** est supprimée du routeur R1, la route 20:20::20/128 annoncée par le routeur R2 est installée dans la table de routage du routeur R1. Voici l'exemple de sortie :

Dans le routeur R1
R1(config)#no ipv6 route 20:20::20/128 Null0 *!--- The Null0 command in removed from router R1.* R1#show bgp ipv6 unicast BGP table version is 7, local router ID is 1.1.1.1 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 *>
20:20::20/128    ::                      0
32768 ?
*                  BB::1                   0
0 6502 I
*> AA:10::10/128    ::                     0
32768 I
 !--- After the removal of the statement, !--- the route
20:20::20/128 is shown as best route. R1#show ipv6 route
bgp
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-
user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R -
RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea,
IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor
Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext
1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   20:20::20/128 [20/0]
    via BB::1

!--- You can see that the route is displayed in routing
table.
```

Essayez maintenant d'envoyer une requête ping au routeur R1 à partir du routeur R2 avec la source comme interface de bouclage Lo 20.

```
R2#ping ipv6  AA:10::10 source lo20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to AA:10::10, timeout is 2 seconds:
Packet sent with a source address of 20:20::20
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/54/140 ms
!--- You can see that the ping is successful.
```

Informations connexes

- Filtrage des trous noirs déclenchés à distance
- Assistance technologique BGP
- Prise en charge de la technologie IP version 6
- Études de cas BGP
- Support et documentation techniques - Cisco Systems