IPv6 Black-Holing über Schnittstelle konfigurieren Null0

Inhalt

Einführung

Dieses Dokument beschreibt, wie Black-Holing in IPv6 über die Schnittstelle Null0 konfiguriert wird. Black Hole Routing ist eine Methode, mit der der Administrator unerwünschten Datenverkehr blockieren kann, z. B. Datenverkehr aus illegalen Quellen oder Datenverkehr, der durch einen DoS-Angriff (Denial of Service) generiert wird, indem der Datenverkehr dynamisch an eine tote Schnittstelle oder an einen Host weitergeleitet wird, der Informationen für die Untersuchung erfasst, wodurch die Auswirkungen des Angriffs auf das Netzwerk verringert werden.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- BGP-Routing-Protokoll und dessen Betrieb verstehen
- Verständnis für das IPv6-Adressierungsschema

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Router der Serie 7200 mit Cisco IOS® Softwareversion 15.0(1).

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

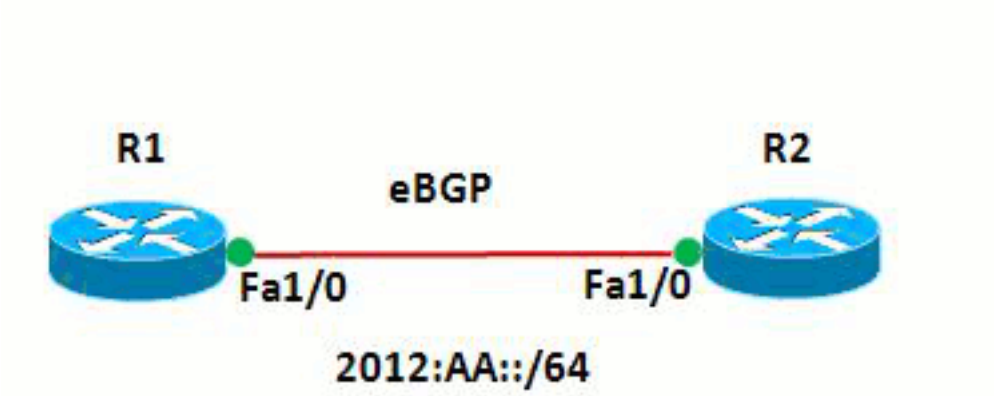
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Netzwerk bilden die Router sowie R1 und R2 eine eBGP-Beziehung zueinander. Die Router verwenden OSPFv3 für die interne Kommunikation. Beim Router R1 wird Blackholing durch die Konfiguration von Null0 so erreicht, dass alle Pakete mit der Quelladresse 20:20::20/128 an Null0 weitergeleitet werden. Mit anderen Worten, der gesamte Datenverkehr, der an Null0 weitergeleitet wird, wird verworfen.

Beispielkonfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Router R1
- Router R2

Router 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
```

Router 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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Um die eBGP-Konfiguration zu überprüfen, verwenden Sie die **Befehle show ipv6 route bgp** und **show bgp ipv6 unicast** in Router R1.

Router 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.
```

Um zu überprüfen, welche Routen vom BGP empfangen werden, verwenden Sie den Befehl **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.
```

Verwenden Sie die Quelle als Loopback-Schnittstelle 20, um einen Ping an Router R1 vom Router R2 zu senden.

```
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.
```

Versuchen Sie, Router R1 vom Router R2 zu pingen, ohne die Loopback-Schnittstelle als Quelle zu verwenden.

```
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.
```

Wenn die Anweisung **ipv6 route 20:20:20/128 Null0** vom Router R1 entfernt wird, wird die Route 20:20::20/128, die vom Router R2 angekündigt wurde, in der Routing-Tabelle des Routers R1 installiert. Dies ist die Beispielausgabe:

In Router 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.
```

Versuchen Sie jetzt, den Router R1 von Router R2 mit der Quelle als Loopback-Schnittstelle Lo 20 zu pingen.

```
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.
```

Zugehörige Informationen

- Remote ausgelöste Black Hole Filtering
- BGP-Technologie-Support
- Technischer Support für IP-Version 6
- BGP-Fallstudien
- Technischer Support und Dokumentation - Cisco Systems