ASR 9000 brongebaseerde externe getriggerde Blackhole filtering met RPL Next-hop Discard Configuration Voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u op afstand getriggerde Blackhole (RTBH) kunt configureren op de Aggregation Services Router (ASR) 9000.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Deze informatie in dit document is gebaseerd op Cisco IOS-XR® en ASR 9000.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

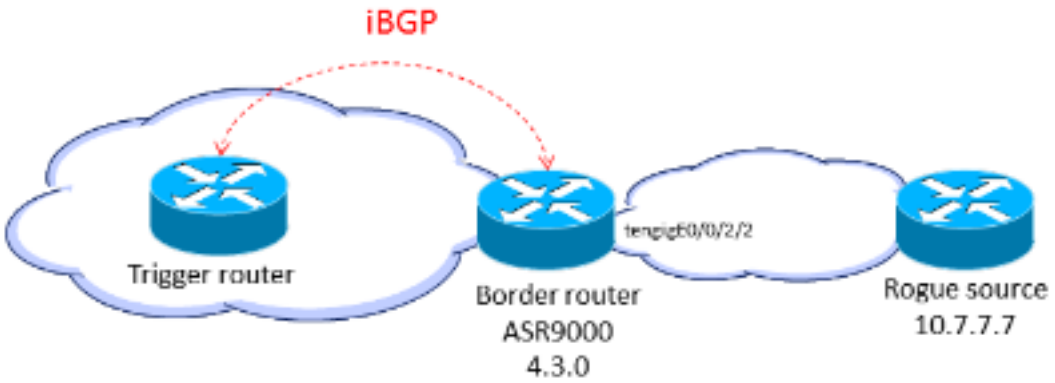
Achtergrondinformatie

Wanneer u de oorsprong van een aanval kent (bijvoorbeeld door een analyse van NetFlow-gegevens), kunt u insluitingsmechanismen toepassen, zoals toegangscontrolelijsten (ACL's). Wanneer aanvalsverkeer wordt gedetecteerd en geclassificeerd, kunt u geschikte ACL's maken en implementeren op de benodigde routers. Omdat dit handmatige proces tijdrovend en complex kan zijn, gebruiken veel mensen Border Gateway Protocol (BGP) om drop-informatie snel en efficiënt naar alle routers te verspreiden. Deze techniek, RTBH, stelt de volgende hop van het IP-adres van het slachtoffer in op de null interface. Het verkeer dat voor het slachtoffer bestemd is, wordt bij het betreden van het netwerk gedropt.

Een andere optie is om verkeer uit een bepaalde bron te laten vallen. Deze methode is vergelijkbaar met de eerder beschreven drop, maar is afhankelijk van de vorige implementatie van Unicast Reverse Path Forwarding (uRPF), die een pakket laat vallen als de bron "ongeldig" is, waaronder routes naar null0. Met hetzelfde mechanisme van de op bestemming gebaseerde drop wordt een BGP-update verzonden, en deze update stelt de volgende hop voor een bron in op null0. Nu laat al verkeer dat een interface met uRPF ingaat verkeer uit die bron vallen.

Op bron gebaseerde RTBH-filtering op de ASR 9000

Wanneer de functie uRPF is ingeschakeld op de ASR9000, kan de router geen recursieve lookup tot null0 uitvoeren. Dit betekent dat de op bron gebaseerde RTBH-filtering die door Cisco IOS wordt gebruikt, niet rechtstreeks door Cisco IOS-XR op de ASR 9000 kan worden gebruikt. Als alternatief wordt de Routing Policy Language (RPL) **set next-hop discard** optie (geïntroduceerd in Cisco IOS XR versie 4.3.0) gebruikt.



Configureren

Configuratie op de triggerrouter

Configureer een beleid voor statische routeherverdeling dat een community instelt op statische routes die gemarkeerd zijn met een speciale tag en pas dit toe in BGP:

```
route-policy RTBH-trigger
```

```
if tag is 777 then
set community (1234:4321, no-export) additive
pass
else
pass
endif
end-policy

router bgp 65001
address-family ipv4 unicast
redistribute static route-policy RTBH-trigger
!
neighbor 192.168.102.1
remote-as 65001
address-family ipv4 unicast
route-policy bgp_all in
route-policy bgp_all out
```

Configureer een statische route met de speciale tag voor het bronprefix dat zwart moet worden gehold:

```
router static
address-family ipv4 unicast
10.7.7.7/32 Null0 tag 777
```

Configuratie op de grensrouter

Configureer een routebeleid dat overeenkomt met de community die op de trigger-router is ingesteld en stel de **volgende-hop-verwerping in**:

```
route-policy RTBH
if community matches-any (1234:4321) then
set next-hop discard
else
pass
endif
end-policy
```

Pas het routebeleid op de iBGP-peers toe:

```
router bgp 65001
address-family ipv4 unicast
!
neighbor 192.168.102.2
remote-as 65001
address-family ipv4 unicast
route-policy RTBH in
route-policy bgp_all out
```

Voor de grensinterfaces, vorm losse wijze uRPF:

```
interface TenGigE0/0/2/2
cdp

ipv4 address 192.168.101.2 255.255.255.0
ipv4 verify unicast source reachable-via any
```

Opmerking: deze uRPF-configuratie is van toepassing op al het verkeer op deze interface.

Verifiëren

Op de border-router wordt het prefix **10.7.7.7/32** gemarkeerd als **Nexthop-discard**:

```
RP/0/RSP0/CPU0:router#show bgp
BGP router identifier 10.210.0.5, local AS number 65001
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000 RD version: 12
BGP main routing table version 12
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
N>i10.7.7.7/32        192.168.102.2            0    100      0 ?

RP/0/RSP0/CPU0:router#show bgp 10.7.7.7/32
BGP routing table entry for 10.7.7.7/32
Versions:
Process bRIB/RIB SendTblVer
Speaker 12 12
Last Modified: Jul 4 14:37:29.048 for 00:20:52
Paths: (1 available, best #1, not advertised to EBGP peer)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
192.168.102.2 (discarded) from 192.168.102.2 (10.210.0.2)
Origin incomplete, metric 0, localpref 100, valid, internal best, group-best
Received Path ID 0, Local Path ID 1, version 12
Community: 1234:4321 no-export

RP/0/RSP0/CPU0:router#show route 10.7.7.7/32

Routing entry for 10.7.7.7/32
 Known via "bgp 65001", distance 200, metric 0, type internal
 Installed Jul 4 14:37:29.394 for 01:47:02
 Routing Descriptor Blocks
   directly connected, via Null0
     Route metric is 0
 No advertising protos.
```

U kunt op de ingangslijnkaarten controleren dat RPF-druppels optreden:

```
RP/0/RSP0/CPU0:router#show cef drop location 0/0/CPU0
CEF Drop Statistics
Node: 0/0/CPU0
Unresolved drops packets : 0
Unsupported drops packets : 0
Null0 drops packets : 10
No route drops packets : 17
No Adjacency drops packets : 0
Checksum error drops packets : 0
RPF drops             packets :           48505   <=====
RPF suppressed drops packets : 0
RP destined drops packets : 0
Discard drops packets : 37
```

```
GRE lookup drops packets : 0
GRE processing drops packets : 0
LISP punt drops packets : 0
LISP encap err drops packets : 0
LISP decap err drops packets :
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- OP AFSTAND GEACTIVEERD FILTEREN VAN ZWARTE GATEN - OP BESTEMMING GEBASEERD EN BRONGEBASEERD
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.