ASR9000 source basado Blackhole remotamente accionado que filtra con el ejemplo de configuración del descarte del Next-Hop RPL

Contenido

Introducción

Este documento describe cómo configurar Blackhole remotamente accionado (RTBH) en el router de los servicios de la agregación (ASR) 9000.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Esta información en este documento se basa en el ® y ASR 9000 del Cisco IOS XR.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Cuando usted conoce el origen de un ataque (por ejemplo, por un análisis de los datos de NetFlow), usted puede aplicar los mecanismos de la contención, tales como Listas de control de acceso (ACL). Cuando se detecta y se clasifica el tráfico del ataque, usted puede crear y desplegar los ACL apropiados al Routers necesario. Porque este Proceso manual puede ser largo y complejo, mucha gente utiliza el Border Gateway Protocol (BGP) para propagar la información del descenso a todo el Routers de manera rápida y eficiente. Esta técnica, RTBH, fija el salto siguiente de la dirección IP de la víctima a la interfaz nula. El tráfico destinado a la víctima se cae en el ingreso en la red.

Otra opción es caer el tráfico de una fuente particular. Este método es similar al descenso descrito previamente pero confía en el despliegue anterior del Unicast Reverse Path Forwarding (uRPF), que cae un paquete si su fuente es “inválida,” que incluye las rutas al null0. Con el mismo mecanismo del descenso basado en el destino, se envía una actualización de BGP, y esta actualización fija el salto siguiente para una fuente al null0. Ahora todo el tráfico que ingresa una interfaz con el uRPF habilitó los descensos trafica de esa fuente.

Source basado RTBH que filtra en el ASR9000

Cuando el uRPF de la característica se habilita en el ASR9000, el router no puede hacer las operaciones de búsqueda recurrentes al null0. Esto significa que la configuración de filtración del source basado RTBH usada por el Cisco IOS no se puede utilizar directamente por el Cisco IOS XR en el ASR9000. Como alternativa, se utiliza el lenguaje del política de ruteo (RPL) **fijó la** opción del **descarte del Next-Hop** (introducida en la versión 4.3.0 del Cisco IOS XR).

Configurar

Configuración en el router del activador

Configure una política de redistribución de la Static ruta que fije a una comunidad en las Static rutas marcadas con una etiqueta especial, y apliqúela en el 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
```

Configure una Static ruta con la etiqueta especial para el prefijo de la fuente que necesita negro-ser agujereado:

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

Configuración en el Router del borde

Configure una directiva de la ruta que haga juego al conjunto de comunidades en el router del activador y configure el **descarte determinado del Next-Hop**:

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

Aplique la directiva de la ruta en los pares del iBGP:

```
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
```

En las interfaces de la frontera, configure el modo flexible del uRPF:

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

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

> Nota: Esta configuración del uRPF se aplica a todo el tráfico en esta interfaz.

Verificación

En el Router del borde, el prefijo **10.7.7.7/32** se señala por medio de una bandera como Nexthop-**descarte**:

```
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.
```

Usted puede verificar en el linecards del ingreso que ocurran los descensos RPF:

```
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 :
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- FILTRACIÓN REMOTAMENTE ACCIONADA DEL AGUJERO NEGRO - DESTINO BASADO Y FUENTE BASADA
- Soporte Técnico y Documentación - Cisco Systems