Ejemplo de Configuración de ASR9000 Basada en Origen y Activada Remotamente de Blackhole Filtering con RPL Next-hop Discard

Contenido

Introducción

Este documento describe cómo configurar el agujero negro activado de forma remota (RTBH) en el router de servicios de agregación (ASR) 9000.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Esta información de este documento se basa en Cisco IOS-XR® y ASR 9000.

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). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Cuando conoce el origen de un ataque (por ejemplo, mediante un análisis de los datos de NetFlow), puede aplicar mecanismos de contención, como listas de control de acceso (ACL). Cuando se detecta y clasifica el tráfico de ataque, puede crear e implementar las ACL adecuadas en los routers necesarios. Debido a que este proceso manual puede ser lento y complejo, muchas personas utilizan el Protocolo de gateway fronterizo (BGP) para propagar la información de caídas a todos los routers de manera rápida y eficiente. Esta técnica, RTBH, establece el siguiente salto de la dirección IP de la víctima en la interfaz nula. El tráfico destinado a la víctima se descarta al entrar en la red.

Otra opción es descartar el tráfico de un origen determinado. Este método es similar al descarte descrito anteriormente, pero se basa en la implementación previa de Unicast Reverse Path Forwarding (uRPF), que descarta un paquete si su origen es "no válido", que incluye rutas a null0. Con el mismo mecanismo del descarte basado en el destino, se envía una actualización de BGP y esta actualización establece el siguiente salto para un origen en null0. Ahora todo el tráfico que ingresa a una interfaz con uRPF habilitado descarta tráfico de esa fuente.

Filtrado RTBH basado en el origen en ASR9000

Cuando la función uRPF está habilitada en el ASR9000, el router no puede realizar la búsqueda recursiva en null0. Esto significa que Cisco IOS-XR no puede utilizar directamente la configuración de filtrado RTBH basada en origen utilizada por Cisco IOS en ASR9000. Como alternativa, se utiliza la opción **set next-hop discard del** lenguaje de política de routing (RPL) (introducida en Cisco IOS XR versión 4.3.0).

Configurar

Configuración en el router desencadenador

Configure una política de redistribución de rutas estáticas que establezca una comunidad en rutas estáticas marcadas con una etiqueta especial y aplíquela en 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 ruta estática con la etiqueta especial para el prefijo de origen que debe ser de agujeros negros:

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

Configuración en el router de borde

Configure una política de ruta que coincida con el conjunto de comunidad en el router del disparador y configure **set next-hop discard**:

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

Aplique la política de ruta en los peers 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 borde, configure el modo flexible 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 uRPF se aplica a todo el tráfico en esta interfaz.

Verificación

En el router de borde, el prefijo **10.7.7.7/32** se marca como **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.
```

Puede verificar en las tarjetas de línea de ingreso que se producen caídas de 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 :
```

Troubleshoot

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

Información Relacionada

- FILTRADO DE AGUJEROS NEGROS ACTIVADO DE FORMA REMOTA: BASADO EN DESTINO Y BASADO EN ORIGEN
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).