ASR9000与RPL下个跳越丢弃配置示例的基于来源的远程被触发的黑洞过滤

目录

简介

本文描述如何配置远程被触发的黑洞(RTBH)在聚合服务路由器(ASR) 9000。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

此本文档中的信息根据Cisco IOS XR ®和ASR 9000。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

当您认识攻击的始发地(例如，由NetFlow数据分析)，您能应用遏制机制，例如访问控制列表(ACL)。当攻击流量检测并且分类时，您能创建和部署适当的ACL到必要的路由器。由于此手动程序可以费时和复杂，许多人使用边界网关协议(BGP)为了传播丢弃信息到所有路由器迅速和高效。此技术， RTBH，设置受害者的IP地址的下一跳为NULL接口。流量被注定对受害者在入口丢弃到网络。

另一个选项是从特定来源降低流量。此方法类似于以前描述的丢弃，但是依靠单播逆向路径转发(URPF)先前配置，丢弃数据包，如果其来源"无效"，包括路由对null0。使用基于目的地丢弃的同一机制， BGP更新被发送，并且此更新设置来源的下一跳为null0。现在进入与uRPF的一个接口的所有流量启用从该来源的丢包流量。

在ASR9000的基于来源的RTBH过滤

当功能uRPF在ASR9000时启用，路由器无法执行递归查找到null0。这意味着Cisco IOS使用的基于来源的RTBH过滤器配置不可能由在ASR9000的Cisco IOS XR直接地使用。作为替代方案， (介绍在Cisco IOS XR版本4.3.0)使用路由策略语言(RPL) **set next-hop丢弃**选项。

配置

在触发路由器的配置

配置设置静态路由的一个社区标记用一特殊标记的一项静态路由再分配策略，并且应用它在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
```
配置有特殊标记的静态路由需要黑洞的来源前缀的：

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

在边界路由器的配置

配置匹配在触发路由器的属性集合的路由策略并且配置**set next-hop丢弃**：

```
route-policy RTBH
if community matches-any (1234:4321) then
set next-hop discard
else
pass
endif
end-policy
```
运用在iBGP对等体的路由策略：

```
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
```
在边界接口，请配置uRPF松散模式：

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

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

注意：此uRPF配置适用对在此接口的所有流量。

验证

在边界路由器上，前缀**10.7.7.7/32**被标记作为Nexthop**丢弃**：

```
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.
```

您在RPF丢包发生的进入线路卡能验证：

```
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 :
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 远程被触发的黑洞过滤-基于的目的地基于的和来源
- 技术支持和文档 - Cisco Systems