使用RPL下一跳丢弃的ASR9000基于源的远程触发黑洞过滤配置示例

目录

简介

本文档介绍如何在聚合服务路由器(ASR)9000上配置远程触发黑洞(RTBH)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于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

当您了解攻击的来源（例如，通过分析NetFlow数据）时，可以应用包含机制，例如访问控制列表(ACL)。当检测到攻击流量并进行分类时，您可以创建相应的ACL并将其部署到所需的路由器。由于此手动过程可能既耗时又复杂，因此许多人使用边界网关协议(BGP)来快速高效地向所有路由器传播丢弃信息。此技术RTBH将受害者IP地址的下一跳设置为空接口。流向受害者的流量会在进入网络的入口处丢弃。

另一种方法是丢弃来自特定源的流量。此方法类似于前面介绍的丢弃，但依赖于之前的单播逆向路径转发(uRPF)部署，如果数据包的源“无效”（包括指向null0的路由），则丢弃数据包。使用相同的基于目标的丢弃机制，将发送BGP更新，并且此更新将源的下一跳设置为null0。现在，所有进入启用了uRPF的接口的流量都会丢弃来自该源的流量。

ASR9000上基于源的RTBH过滤

在ASR9000上启用功能uRPF时，路由器无法对null0执行递归查找。这意味着Cisco IOS使用的基于源的RTBH过滤配置不能直接由ASR9000上的Cisco IOS-XR使用。作为替代方案，使用路由策略语言(RPL)**set next-hop discard**选项（在Cisco IOS XR版本4.3.0中引入）。

配置

触发路由器上的配置

配置静态路由重分发策略，该策略在标记有特殊标记的静态路由上设置社区，并将其应用于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
```

为需要黑洞的源前缀配置带有特殊标记的静态路由：

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

边界路由器上的配置

配置与触发路由器上设置的团体匹配的路由策略，并配置set next-hop discard:

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

在iBGP对等体上应用路由策略：

```
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
```

在边界接口上，配置uRPF松动模式：

```
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配置适用于此接口上的所有流量。

验证

在边界路由器上，前缀10.7.7.7/32标记为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.
```

您可以在入口线卡上验证RPF丢弃是否发生：

```
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

- 远程触发的黑洞过滤 — 基于目的地和基于源
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。