某局点S7003X包过滤无法过滤访问本机地址问题

ACL packet-filter **苏亚东** 2023-03-27 发表

问题描述

现场设备三层转发，通过包过滤来隔离网段时间的访问，但是目前发现访问设备本身的流量没法被包过滤限制。

PC（192.168.4.11）----（vlan-int40 192.168.4.1）S7003X（vlan-int50 192.168.5.1）----- 192.168.5.55

过程分析

（1）首先检查设备上包过滤配置，访问本机的流量确实可以匹配到对应rule 60中的，并且流量从PC访问192.168.5.55时报文能够过滤，说明acl已经成功下发并生效。

```
#
acl advanced 3000
rule 10 deny ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 20 deny ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
rule 30 deny ip source 192.168.4.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
rule 40 deny ip source 192.168.4.0 0.0.0.255 destination 192.168.5.0 0.0.0.255
rule 50 deny ip source 192.168.4.0 0.0.0.255 destination 192.168.6.0 0.0.0.255
rule 60 deny ip source 192.168.4.0 0.0.0.255 destination 192.168.4.0 0.0.0.255
rule 100 permit ip
#
interface Vlan-interface40
ip address 192.168.4.1 255.255.255.0
packet-filter filter all
packet-filter 3000 inbound
packet-filter 3000 outbound
#
```

（2）经过内部分析确认，该设备在当前版本中，访问本机的报文可以通过协议acl直接上送CPU处理，该流程的优先级高于包过滤的优先级，因此包过滤无法过滤到访问本机地址的报文：

（3）目前硬件acl禁不了上送cpu的协议报文，已实测过。可以1.使用本地pbr（软转）禁用回程报文，该方式需要升级到R7748P01; 2.出端口非路由口时，也可以使用出方向包过滤禁用掉回程报文

本地pbnr相关参考配置如下：

```
#
acl number 3201
rule 0 permit ip source 192.168.4.1 0 destination 192.168.4.11 0          #<-----禁用的是回程报文
#
#
policy-based-route 1 permit node 1
if-match acl 3201
apply output-interface NULL0
#
ip local policy-based-route 1
```

解决方法

1、使用本地pbr（软转）禁用回程报文，该方式需要升级到R7748P01;

2、出端口非路由口时，也可以使用出方向包过滤禁用掉回程报文