交换机ACL不生效

ACL 雒小强 2023-01-30 发表

问题描述

现场需求，其他vlan下地址不能访问vlan11，以vlan2为例；配置了acl包过滤，ping不通，但是可以telnet成功，如下：

过程分析

检查相关配置：

#

interface Vlan-interface2

ip address 10.2.2.1 255.255.255.0

packet-filter 3000 inbound

#

interface Vlan-interface11

ip address 10.2.11.1 255.255.255.0

packet-filter 3001 inbound

#

acl number 3000

rule 5 deny ip destination 10.2.6.0 0.0.0.255

rule 10 deny ip destination 10.2.7.0 0.0.0.255

rule 15 deny ip destination 10.2.11.0 0.0.0.255

#

acl advanced 3001

rule 5 deny ip destination 10.0.0.0 0.255.255.255

#

另外查看ACL资源也是足够的；

测试终端：10.2.2.17，未配置ACL，包过滤之前是可以通的，配置之后ping不通，但是可以telnet上去；

流统信息收集：

1.ping测试的流统正常，但是telnet时在物理接口下做流统没有看到报文；

ssh默认端口号22，telnet默认端口号23，设备根据入方向tcp报文的L4端口号匹配报文上送cpu，动作为copy+redirect,即上送CPU一份也硬转一份。当前telnet流量为tcp目的端口号22的报文，匹配规则上送cpu且硬转的优先级高，所以流统不到

2。配置包过滤之后ping不通，但是telnet能通

Ping不通是正常现象；

之所以telnet能通，正如1解释，该telnet流量除了上送cpu一份，也会硬转一份，导致包过滤不生效。

解决方法

规避手段：

该问题的触发是由于设备对入方向目的端口号为22/23的tcp报文上送cpu+硬转处理，所以可以修改目的端口号为其他非协议默认端口号规避，比如24；

也可以在vlan-int11出方向下发包过滤，端口出方向报文不会上送cpu+硬转