S5560-56C-HI 包过滤不生效问题

packet-filter 翁青山 2018-06-30 发表

组网及说明

设备型号及版本：S5560-56C-HI V7 R7116P01
组网：PC1----- （1/0/47）S5560-56C-HI （1/0/7）----PC2

问题描述

客户想要针对某个固定终端过滤该终端的所有报文，于是在二层物理接口1/0/47做了包过滤（packet-filter），调用二层acl，在 1/0/7 口虚机上抓包发现还是能收到源MAC为7427-eab1-e750的PC发出的ARP报文；
但是实际上两台PC间无法ping通，属于同一网段；

```
#
interface GigabitEthernet1/0/47
port link-mode bridge
packet-filter 4000 inbound
acl number 4000
rule 20 deny source-mac 7427-eab1-e750 ffff-ffff-ffff
#
```

过程分析

1、从测试结果并结合抓包看，在物理接口上下发包过滤实际上只过滤的icmp报文，但是没有过滤掉arp报文；
2、收集底层acl，查看包过滤acl下发情况：
先debug port mapping slot 1看下1/0/47是属于哪个芯片的（unit列如果是0就是chip 0，unit 列是1就是chip 1），

```
Probe
debug qacl show acl-resc slot 1 chip 0    1-->Slot number 0-->Chip number（根据上述看到的chip号对应收集。）
debug qacl show slot 1 chip 0 verbose 0    1-->Slot number 0-->Chip number
debug qacl show slot 1 chip 0 verbose 20
debug qacl show slot 1 chip 0 verbose 40
debug qacl show slot 1 chip 0 verbose 60
..... （每20一个步长，一直收集到没有显示内容为止）
```

3、设备上终端的mac表和arp表：

```
7427-eab1-e750   6         Learned         GE1/0/47              Y
10.6.11.211     7427-eab1-e750 6         GE1/0/47              20    D
```

底层acl信息：

```
========
Acl-Type PktFilter Eth_Mac on PORT, Stage IFP, SinglePort, Installed, Active
Prio Mjr/Sub 520/18, Group 3 [3], Slice/Idx 10/4, Entry 94, Double: 5124/5636
ACL GroupNo : 4000, RuleID : 20
Rule Match --------
        Ports: 0x0000800000014000; 0x3fffffffffffffff
        Lookup: STP forwarding, 0x18, 0x18
        Source mac: 7427-EAB1-E750, FFFF-FFFF-FFFF
Actions --------
        Deny
========
Acl-Type RX IPv4 High, Stage IFP, Global, Installed, Active
Prio Mjr/Sub 523/24, Group 1 [1], Slice/Idx 12/8, Entry 31, Double: 6152/6664
Rule Match --------
        Ports: 0x03fffffffffffffe; 0x3fffffffffffffff
        Lookup: VLAN ID valid[y], STP forwarding, 0x1c, 0x1c
        Dest mac: FFFF-FFFF-FFFF, FFFF-FFFF-FFFF
        EtherType: 0x806, 0xffff
        SysmRule Index : 29
        Vlan Class id: 0x2    Mask: 0x2
Actions --------
        CAR cir 0x100, cbs 0x800, pir 0x100, pbs 0x800, mode srTCM color blind
```

Account mode packets, green and non-green
Copy_to_cpu : Yes
Change CPU pkt COS 8
Permit
Red_Copy_to_cpu : No
Yel_Copy_to_cpu : No
MatchedName:29, ARP
Accounting: Hi 29, LO 0
========
4、看了下，终端是接在设备vlan 6下面的，本地也配置了vlan-interface 6且接口是up的，所以，设备会下发一个匹配arp的acl到底层，5560HI这条系统下发的acl规则比包过滤规则优先级高， 这时候执行动作copy一份到cpu，原始的报文也正常硬件转发出去了，此时不会再匹配低优先的包过滤acl，所以，配置包过滤没有过滤掉arp广播报文。

解决方法

1、 用户配这个包过滤的目的如果是限制下行用户上网，那没问题，因为只有下行用户发送的广播arp请求报文能转发，其他报文都会被deny。
2、若客户确实也想过滤掉arp报文，可以在设备上undo int vlan（对应设备收到该arp报文对应的vlan tag）来解决。