

知 某局点S10508升级后IPS无法引流问题分析

林洪宇 2018-03-29 发表

某局点S10508在1框9槽位使用一块IPS安全插卡，作为主动式入侵防御系统，阻止各种针对系统漏洞的攻击，屏蔽蠕虫、病毒和间谍软件等，交换机采用手动MQC引流方式，将进入交换机的流量重定向到IPS插卡二层转发，经过匹配安全防护以及流量管理策略处理后回到交换机进行三层转发，转发至相应的出接口。在一次对交换机版本升级操作之后，发现IPS板上无法获取流量，业务中断。

查看接口的MQC引流配置：

```
traffic classifier all-address operator and
if-match acl 3001
#
traffic behavior redirect-to-ips
redirect interface Ten-GigabitEthernet1/9/0/1
#
qos policy up-stream
classifier all-address behavior redirect-to-ips
```

查看IPS插卡与交换机内联口配置：

```
#
interface Ten-GigabitEthernet1/9/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 2 to 4094
stp disable
packet-filter 4000 outbound
mac-address mac-learning disable
```

确认升级前后交换机配置没有变化，首先通过在MQC下发包计数，确认MQC已经匹配上流量重定向至内联接口，接下来检查内联口下过滤无关的二层报文,查看包过滤底层也下发成功：

```
acl number 4000
rule 9 permit type 0800 ffff dest-mac 3c8c-4005-50f7 ffff-ffff-ffff
rule 12 permit type 88a7 ffff
rule 100 deny
```

底层acl：

```
Acl-Type PktFilter Eth_Mac on PORT, Stage EFP, GroupPri 515, EntryID 192, Active Health 1,
PoolFree 0, PoolID 0, Prio_Mjr 264, Prio_Sub 6, Slice 3, SliceIdx 0 ACL GroupNo : 4000, RuleID : 9
Rule Match ----- Out Port: 24 L2Format: Any Dest mac: 3C8C-4005-50F7, FFFF-FFFF-FFFF
EtherType: 0x800, 0xffff Actions ----- Permit 最后通过对acl 4000的rule规则进行删减测试，
当将rule 100 的deny规则删除后，业务恢复正常，IPS可以检测到流量。
```

通过acl的rule增删确认引流的流量被包过滤过滤了，并没有匹配第一条rule放通的网关mac进入IPS插卡，在检查网关mac时发现，acl规则中放通的网关mac配置错误，但对比升级之前的交换机配置，配置并没有变化，通过对比设备桥mac，升级前后设备的桥mac发生了变化，导致acl没法正确匹配放通相应流量。

升级前设备桥mac：

```
=====debug sysm bridgemac read =====
=====
```

The Bridge Macs are as follows:

3c8c-4005-50f7

升级后设备桥mac：

```
=====debug sysm bridgemac read =====
=====
```

The Bridge Macs are as follows:

3c8c-4005-50bb

分析总结：

检查设备配置IRF的桥MAC地址保留时间为永久保留：irf mac-address persistent always

理论上升级导致堆叠发生主备倒换，设备的桥mac不会改变，不会对引流造成影响；

和现场确认升级过程，现场是将两台设备同时指定软件版本后重启升级，这种情况下，由于二框先启动完成，

选举为堆叠全局主设备，因此堆叠的桥mac变成二框的设备的自身mac地址，不在使用原来堆叠使用的一框的mac

地址作为堆叠桥mac。

建议之后在堆叠情况下使用MQC方式引流到IPS板卡，做过滤二层报文策略时，放通两框的设备自身桥mac地址，

用来防止由于设备掉电或其他原因造成设备桥mac地址改变导致业务中断情况发生。