ACG1000-M关于IPV4策略默认拒绝后的通信问题

ACG1000 Trust 2017-11-20 发表

组网及说明

问题是如何解决匹配了源地址和源mac的策略后，所有其他规矩拒绝后，还能让策略匹配，通过把snmp学习过来的交换机mac做白名单后会导致共享上网阻断的冲突。有什么办法解决。

问题描述

该局点目前做了基于源地址源用户（静态mac绑定）的ipv4策略，目前出现的问题是，当把所有策略都做完后，配置默认规则为拒绝时，所有网络都无法通过策略放行流量，（我认为是SNMP三层学习mac时，需要把核心源MAC也一并加入到放通队列才能让acg正常学习到终端用户mac），后来通过匹配第一策略：放通源为所有地址，用户为三层交换机mac地址（取名为三层），此时所有策略中的用户和mac都正常匹配命中了策略。

问题就来了

因为acg并未对所有用户经过mac绑定，有些mac还未统计，此时在线用户中那些没绑定过mac的用户名都变为了（三层），mac还是各个终端的mac，移动用户管理中，用户名也都变成了（三层），IP地址为各个终端地址。这个导致了共享上网监控在执行了自动阻断后，会把所有用户都屏蔽掉，可能原因是共享上网认为终端所有mac都是三层交换机的mac学习过来的，共享这个功能认准所有用户都是的三层交换机mac学习来的，导致共享阻断一开全部断网。

解决方法

目前跨三层取mac主要是针对日志信息可以体现mac来实现的，基于mac的策略目前不建议使用

答案来自于 **不科学君**