

知 某局点 ACG1000针对用户做上网限制不生效

ACG1000 卯静 2020-06-08 发表

组网及说明

ACG透明部署，下行为核心交换机

问题描述

现场配了SNMP跨三层学MAC，将学到的IP和MAC地址同步到用户组里。然后针对该用户组做控制策略，只放通这个用户组到外网的流量，测试发现不行。只要选择该用户组以后内网用户就无法访问外网

ID	名称	动作	用户	源端口	目的端口	源地址	目的地址	应用	策略	策略	策略	匹配次数	应用策略	时间	日志	统计时间	操作
1	内网	放行	内网	any	any	any	any	any	any	any	any	79112	always	-	0	0	操作
2	外网	放行	外网	any	any	any	any	any	any	any	any	0	always	总是	0	0	操作

过程分析

查看测试电脑的IP和MAC，确认SNMP同步的用户没有问题，又新建了一条放通any的策略，发现每次测试any这条策略的匹配次数都会增加，怀疑还有其他流量没有放通，查看测试电脑的DNS服务器发现客户将电脑的DNS设置在了核心交换机上，交换机上开了DNS代理，此时DNS请求的源地址是交换机的地址，限制了用户组以后，访问外网的DNS请求报文会被阻止，导致访问外网不通。

解决方法

将客户电脑的DNS服务器换为公网DNS后正常，由于客户内网所有电脑的DNS服务器都是核心交换机的地址，直接把交换机的地址加到这个用户组解决。