

知 某局点ACG1000-AK270设备ipv4策略不生效的案例

透明模式 张子衡 2022-06-29 发表

组网及说明

正常透明部署在核心上行监控所有用户的行为

问题描述

acg在升级版本配置完ipv4策略后正常，过一天后发现都不可以上网，只有重新配置策略，重新导入用户然后重启设备后，设备才可以正常上网，但过一天时间用户又都不能上网了。还需要重复以上操作才能上网。

策略ID	策略名称	策略行为	策略用户	源接口域	目的接口域	源地址	目的地址	应用	服务	策略	策略生效时间	策略生效日期	策略生效时间	策略生效日期
2	策略名称	允许	default	any	any	any	any	全部	any	策略	策略生效时间	策略生效日期	策略生效时间	策略生效日期
3	策略名称	允许	default	any	any	any	any	全部	any	策略	策略生效时间	策略生效日期	策略生效时间	策略生效日期
8	策略名称	允许	default	any	any	any	any	全部	any	策略	策略生效时间	策略生效日期	策略生效时间	策略生效日期
1	策略名称	允许	default	any	any	any	any	全部	any	策略	策略生效时间	策略生效日期	策略生效时间	策略生效日期
6	策略名称	策略行为	策略用户	any	any	any	any	全部	any	策略	策略生效时间	策略生效日期	策略生效时间	策略生效日期

过程分析

查看控制策略可以发现，最后一条拒绝策略计数很多，怀疑是匹配上最后一条拒绝的策略导致不能正常上网。

使用终端测试发现计数有所增长。

看策略都是有做用户组的，怀疑为未能正常识别导致的，于是查看用户



序号	名称	描述	用户类型	用户策略	自动加入	用户状态	状态	操作
1	匿名用户	172.30.110.10	单认证	正在同步	2022/03/29 11:17	8 分钟	正常	操作
2	匿名用户	80.0.0.4	单认证	正在同步	2022/03/29 11:16	19 分钟	正常	操作
3	匿名用户	172.30.123.3	单认证	正在同步	2022/03/29 11:11	19 分钟	正常	操作
4	匿名用户	172.30.110.7	单认证	正在同步	2022/03/29 11:07	19 分钟	正常	操作
5	匿名用户	172.30.125.195	单认证	正在同步	2022/03/29 11:06	20 分钟	正常	操作
6	匿名用户	172.30.123.104	单认证	策略转换失败(策略组200失败)	2022/03/29 10:59	27 分钟	正常	操作
7	匿名用户	172.30.110.8	单认证	正在同步	2022/03/29 10:56	22 分钟	正常	操作
8	匿名用户	172.30.128.73	单认证	PCWeb-based	2022/03/29 10:11	35 分钟	正常	操作

当未进行认证的用户上到acg的时候会归类为匿名用户，如果是创建的用户，绑定了ip或者mac地址的用户，上来到acg后会匹配ip地址与mac地址，然后归类为静态绑定用户，但现场全为匿名用户 acg是在防火墙和华为交换机之间做透传，部署透明模式，但是业务报文上到acg的时候是跨三层上来的

如果三层转发的话，acg要识别真实的用户的mac地址的话，必须在acg上配置snmp跨三层mac学习，检查现场配置，发现现场也是有做跨三层mac学习，但查看用户同步也是正常的，时间也是最短的两秒，但是就是不能成功识别用户



名称	描述	用户类型	用户策略	自动加入	用户状态	状态	操作
1	匿名用户	SNMP 跨3	2秒	否	同步成功	正常	操作

解决方法

排查发现现场并没有开启mac地址敏感，将用户管理>高级选项>全局配置下的用户mac感知勾选上之后正常。

或者配置user mac-sensitive enable。

