ACG1000本地web认证，所有用户用一个手机号上网，只有第一个用户能弹窗做认证

安全监测中心 Portal认证 王听宇 2023-06-26 发表

组网及说明

出口---acg（桥模式部署）---核心（网关）----pc

告警信息

无

问题描述

web上看到虽有认证用户用一个手机号

过程分析

现场使用管理口弹portal，管理口可以弹portal

pc和acg跨三层要开snmp用户同步

用户名 向下箭头看对应mac，发现所有用户都是相同的mac，此mac是网关上联口mac

pc和acg跨三层要开snmp用户同步，没有snmp配置用户同步导致

snmp同步的接口不能配置vpn实例，不支持snmp同步的地址在vpn实例中

有无感知需求

无感知是终端下线后在设定时间内再次上线不需要认证。

超时时间是终端静默超过设定时间系统给予下线

注销账号，无感知表项就注销，要测试无感知，只能等过了客户端超时时间 最少是10分钟

第一次认证显示本地认证，下线后无感知上来就显示 本地认证-无感知

认证方式	终
本地认证-无感知	正
本地认证-无感知	正
本地认证-无感知	移
本地认证	正

解决方法

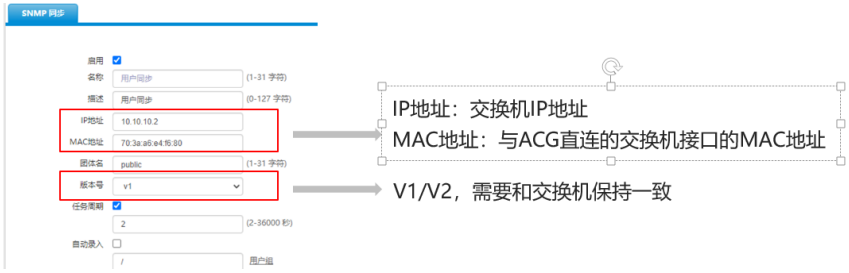
pc和acg跨三层要开snmp用户同步

SNMP同步也叫做跨三层MAC地址学习，跨三层MAC地址学习是指在ACG1000与上网终端之间存在三层设备，无法直接获取终端MAC地址，因此，通过该功能来获取上网终端MAC地址信息。将获取到的终端MAC地址信息，与IP地址在ACG1000上进行绑定，可实现对跨三层的接入终端实现上网控制，同时也可以实现用户名、ip、MAC三者信息绑定实现实名审计需求

数据包经过三层设备时，源目MAC地址会重新封装，当ACG部署在三层设备上游时无法直接从数据包中获取到终端的MAC信息。此时在线用户中用户MAC地址显示为三层设备接口的MAC。

若获取终端真实MAC，需要借助SNMP协议。三层设备上开启SNMP服务，ACG设备上配置交换机信息后，ACG会定时调用snmpwalk进程向三层交换机mib库节点中ip/mac对应关系信息获取终端真实的mac地址。由于内置脚本定期执行，因此终端MAC地址学习有一定的延迟性。

通过菜单“用户管理 > 用户同步 > SNMP同步”可配置SNMP同步参数。



web上看用户的mac是什么，snmp同步里就配置什么

无感知需要配置mac地址敏感

H3C> en

H3C# configure terminal

H3C(config)#

【举例】

配置用户MAC敏感

(config)# user mac-sensitive enable 开启用户MAC敏感