某局点无线终端穿越NAT后AC本地portal认证失败问题处理经验案例

Portal NAT 殷俊 2023-04-24 发表

组网及说明

AP与AC之间穿越防火墙，无线终端业务地址段在防火墙上做NAT转换后可访问AC，AP与AC之间为三层路由互联，AC做本地portal认证

问题描述

设备本地配置portal 认证，客户如果终端和ac路由直通，能正常完成AC本地portal认证，但是中间的防火墙开了nat之后，客户端的认证可以弹出web，输入账号密码就没有反应，认证失败

过程分析

本地portal认证时，portal的交互不在capwap隧道封装内，因此终端与AC的portal交互在过NAT的情况下，终端的IP会被转换为NAT后的地址，这样AC回的时候无法回给实际无线终端。该方案不可行，建议还是通过路由互通方式实现

从收集的信息中可以看出：
正常情况下debug，AC上收到终端请求本地页面的信息中，userip是终端实际IP地址172.XX.XX.3
*Apr 13 16:53:19:097 2023 XXX PORTAL/7/EVENT: Request for /portal/logon.cgi.
*Apr 13 16:53:19:097 2023 XXX PORTAL/7/EVENT: Extend-auth: Parsed userip=0.0.0.0, usermac=0000-0000-0000. User IP=172.XX.XX.3.
穿越NAT认证失败时，AC上收到终端请求本地页面信息中，userip不是终端实际IP：
*Apr 13 16:09:01:147 2023 XXX PORTAL/7/EVENT: Request for /portal/logon.cgi.
*Apr 13 16:09:01:148 2023 XXX PORTAL/7/EVENT: Extend-auth: Parsed userip=0.0.0.0, usermac=0000-0000-0000. User IP=172.XX.XX.74. //这个应该是防火墙的地址

解决方法

终端做本地portal认证时，终端需要能访问AC，穿越NAT后AC回复的报文无法回复给终端，需要取消NAT改为路由互通可解决