某局点Portal认证设备拒绝请求问题处理经验案例

Portal 殷俊 2017-03-27 发表

某局点使用无线控制器WX5510E配置两款11AC款型AP进行无线覆盖，包括WA4320-ACN、WA4620i-ACN，以保证多种环境的用户使用。用户使用场景为办公场景无线接入，集中转发，无线接入采用无线PSK加密配合Portal无感知认证方式，无线加密方式为WPA2+CCMP模式，Portal认证起在AC上。现场AC版本为R2609P57（V200R006B09D050）。
客户反馈，部分用户在进行Portal认证时失败，在认证页面输入用户名密码信息后提示“设备拒绝请求”。之前Portal认证是起在核心105设备上，由于规格问题，将Portal认证迁移到AC上。出问题的用户在网络变更前是没有问题的，做了网络变更后引入的问题。
出现故障时针对故障终端账号进行多轮测试，包括反复踢出用户组重新认证与跟换不同账号在故障终端上进行测试，结果为故障终端账号（jlyu71）在不同手机终端上接入均报设备拒绝请求的故障，而其他账号在故障终端上认证结果正常。

先按照无线的云图之无线Portal（Web）认证排错，排除Portal基础配置、DNS配置问题、排除终端到Portal server路由问题、AC到Portal server路由问题，认证域，AC与AAA对接等基础配置问题。
认证失败属于个别终端问题，尝试将出问题的认证账号在不同终端上测试，均认证失败，尝试在出问题的终端上使用能认证过的账号，发现跟终端没关系。
稳定复现问题后，AC上打开debug调试开关，同时收集IMC UAM调试日志 Portal认证日志。
搜集debug信息：

```
<LWCO-N1-U19-WLC-5510-1> debugging radius packet
<LWCO-N1-U19-WLC-5510-1>debugging portal packet interface Vlan-interface 2032
<LWCO-N1-U19-WLC-5510-1>t m
<LWCO-N1-U19-WLC-5510-1>t d
```

通过日志分析发现有该用户在Filter-ID中下发了一条ACL，而AC上未配置该ACL。

```
*Jan 10 09:35:46:922 2017 LWCO-N1-U19-WLC-5510-1 RDS/7/DEBUG: Receive:IP=[10.210.2.2]Code=[2],Length=[154]
*Jan 10 09:35:46:922 2017 LWCO-N1-U19-WLC-5510-1 RDS/7/DEBUG:
[1  User-name                ] [11] [jlyu71]
[6  Service-Type             ] [6 ] [2]
[24 State                    ] [10] [3644473549777272]
[29 Termination-Action       ] [6 ] [0]
[11 Filter-ID                ] [6 ] [33303031]
[27 Session-TimeOut          ] [6 ] [86401]
*Jan 10 09:35:46:922 2017 LWCO-N1-U19-WLC-5510-1 RDS/7/DEBUG:
[85 Acct_Interim_Interval    ] [6 ] [600]
[H3C-26 Connect_ID           ] [6 ] [1681]
[H3C-61 Server_String        ] [65] []
```

同时在UAM日志中显示回应了AC认证设备的报文信息：

```
% 2017-01-10 08:22:53.544 ; [L_DEBUG (4)] ; [3000] ; LAN ; jlyu71 ; 1 ;
3f893ba860f740b6a1e02d6401576fb7 ; (NULL) ; RT[0]: Receive message from 172.20.1.36:
CODE = 1.
ID   = 104.
ATTRIBUTES:
    User-Name(1) = "...jlyu71".
    Password(2) = "$$$".
    NAS-IP-Address(4) = 2886992164.
    NAS-Identifier(32) = "LWCO-N1-U19-WLC-5510-1".
    NAS-Port(5) = 16820220.
    NAS-Port-Id(87) = "0100010000002044".
    NAS-Port-Type(61) = 19.
    Service-Type(6) = 2.
    Framed-Protocol(7) = 255.
    Calling-Station-Id(31) = "F0-99-BF-13-DB-62".
    Called-Station-Id(30) = "60-0B-03-57-14-40:YST".
    Acct-Session-Id(44) = "1170110082244120efe813b".
    Framed-IP-Address(8) = 180497781.
    hw_Connect_ID(26) = 315.
    hw_Product_ID(255) = "H3C WX5510E".
    hw_IP_Host_Addr(60) = "10.194.45.117 f0:99
```

AC上回应的错误报文为1

Info: Receive Acct username:jlyu71.
%Jan 10 09:35:45:491 2017 LWCO-N1-U19-WLC-5510-1 PORTAL/4/PORTAL_USER_LOGON_FAIL: -UserName=jlyu71-IPAddr=10.194.32.3-IfName=Vlan-interface2032-VlanID=2032-MACAddr=6C:72:E7:6B:65:DD-Reason=Rejected : 1; User failed to get online.
*Jan 10 09:35:45:492 2017 LWCO-N1-U19-WLC-5510-1 PORTAL/7/PORTAL_DEBUG:
Portal send to 10.210.2.2 packet length:52
  Portal packet head:
    Type:4   SN:11901 ReqId:0   AttrNum:3 ErrCode:1 UserIP:10.194.32.3
由于在终端账号认证时，终端由AC向IMC进行Portal认证，IMC通过认证后给AC回应通过的报文，并且携带下发ACL的请求回应给AC，AC收到IMC发来的报文后，检查自身ACL配置，但是由于本次配置业务上线无需用到终端ACL管控策略，则没有对AC进行ACL配置，因此AC未能找到ACL匹配策略于是拒绝了用户上网认证的申请。

方法一：
IMC上AAA服务器上将对应账号的ACL或user-profile策略删除，终端正常认证通过
方法二：
在AC上配置对应的ACL或user-profile策略，终端正常认证通过