

## 某运营商局点ADCampus终端mac portal认证登陆页面无法弹出问题处理经典案例

wlan安全 wlan接入 陈少华 2017-03-09 发表

某运营商局点ADCampus园区组网，有线无线一体化认证。按认证方案设计，无感知状态“无效”账户，终端上线需要出现mac portal登陆页面，重新输入用户名密码认证。接到客户反馈多个终端连接获取地址后，输入域名不进行重定向（包括http或https），输入1.1.1.1可以重定向页面出来。看输入域名的情况，浏览器地址栏没有发生变化。软件开发分析从UAM日志和设备debug信息看，在下发ACL3001是也同时会下发重定向URL，EIA侧处理没有问题，不能重定向的问题需要AC配合定位。

### 1. 故障复现终端抓包分析

通过现场故障复现手机终端测试，PC终端抓包看，PC打开的是www.qq.com，抓包能看到往114.114.14.114 发送DNS 报文解析这个域名，但是没有看到114.114.114.114的回复。

下面这个报文是DNS 请求：

```
*Mar 3 11:42:09:730 2017 bmh-ap-b-8f-ap4 WLANFW/7/PACKET:
```

```
interface = WLAN-Radio1/0/1 payload =
```

```
00 00 00 00 01 60 57 18 33 39 8E 08 00 45 00
```

```
00 38 0F A6 00 00 40 11 7A ED 0A 57 00 E7 72 72
```

```
72 72 DA 85 00 35 00 24 71 91 03 62 01 00 00 01
```

```
00 00 00 00 00 03 77 77 77 02 71 71 03 63 6F
```

```
6D 00 00 01 00 01
```

```
prompt: Received a frame from a radio.
```

### 2. 故障现象分析

怀疑网络中的DNS不通，从客户反馈得知，认证界面无法弹出问题主要集中在两类：

1) HTTPS无法跳转，AD Campus方案无线AC在授权下发重定向URL的场景下，尚未支持https重定向。----已提出产品需求，待研发规划实施；

2) HTTP无法跳转问题，经过现场确认，新用户第一次接入正常页面正常弹出，IE输入IP地址或HTTP网址均能正常跳转。问题集中在IMC平台显示的“失效用户”再次关联会出现该类问题，复现条件逐步清晰：

A.复现终端集中在“失效用户”，即初次认证已通过，间隔多日网管账号处于失效用户列表状态，再次接入会触发；

B.“失效用户”在多个AP下测试能复现，判断为AP位置关系不大；

C.通过远程AP下配置查看，各AP下发的free-rule 配置一致，测试过程没有发现因rule规格导致重定向失败；

D. PC打开www.qq.com 测试，抓包能看到往114.114.114.114 发送DNS 报文解析这个域名，但是没有看到114.114.114.114的回复。怀疑网络DNS不通，涉及到账户权限区分，还需要进一步分析排查。故障复现跟用户终端账户状态强相关---“失效用户”。

### 3. 检查AC/AP上acl 配置如下

10.88.200.155 ---portal服务器地址（从机）

10.88.200.153---director平台地址（之前主机上部署了EIP服务器和从机重定向是负载的）

1) AP上的ACL 3001配置：（除了200.155和153，其他都是DNS地址，AP上本身也没有做deny规则）

```
#
acl advanced 3001
rule 0 permit ip destination 10.88.200.155 0
rule 1 permit ip destination 10.88.200.153 0
rule 2 permit ip source 10.88.200.155 0
rule 3 permit ip source 10.88.200.153 0
rule 20 permit ip destination 218.108.248.200 0
rule 25 permit ip destination 218.108.248.228 0
rule 30 permit ip source 218.108.248.200 0
rule 35 permit ip source 218.108.248.228 0
rule 40 permit ip destination 10.0.97.20 0
rule 41 permit ip source 10.0.97.20 0
rule 45 permit ip destination 10.0.97.87 0
rule 46 permit ip source 10.0.97.87 0
rule 50 permit ip destination 114.114.114.114 0
rule 55 permit ip destination 8.8.8.8 0
#
domain system
#
domain default enable system
#
user-group system
#
return
<bmh-ap-b-8f-ap4>
<bmh-ap-b-8f-ap4>
```

2) AC上的ACL 3001配置: (UDP方通的那两个端口是DHCP的), 配置参照ADCAM最佳实践手册

```
<BMH-HX-H-B1F-WX6103E-AC-IRF>dis acl 3001
Advanced IPv4 ACL 3001, 14 rules,
ACL's step is 5
rule 0 permit ip destination 10.88.200.155 0
rule 1 permit ip destination 10.88.200.153 0
rule 5 permit ip source 10.88.200.155 0
rule 6 permit ip source 10.88.200.153 0
rule 10 permit udp destination-port eq bootpc (182 times matched)
rule 15 permit udp destination-port eq bootps (771160 times matched)
rule 20 permit ip destination 218.108.248.200 0 (326 times matched)
rule 25 permit ip destination 218.108.248.228 0 (33 times matched)
rule 30 permit ip source 218.108.248.200 0
rule 40 permit ip destination 8.8.8.8 0
rule 45 permit ip destination 10.0.97.20 0
rule 50 permit ip destination 10.0.97.87 0
rule 55 permit ip destination 114.114.114.114 0
rule 100 deny ip (19314 times matched)
```

#### 4. 故障原因分析:

- 1) 由于AP是本地转发, 查看重定向ACL 3001 rule规则DNS source和destination全部放通的, 原理上是不存在到DNS不通的现象。在AC侧ACL 3001 rule规则放通了byod VLAN DNS的source和destination, 业务VLAN的DNS destination放通了但source未放通, 所以导致账号失效后的终端在业务VLAN进行URL重定向 DNS解析失败, 输入IP可以弹出认证的问题, 解决方法在AC上添加rule规则放通业务VLAN对应的DNS source地址。
- 2) 问题现象是从ADCAM平台升级到7.3版本后出现的, 由于版本未升级时, 终端认证都是在byod VLAN处理, 认证成功后EIA会下发一个业务VLAN, 无感知认证失效后, 终端再次上线还会到byod VLAN进行认证。7.3 MAC Portal Plus版本处理认证机制变了, 新终端首次接入没有问题, 当无感知认证账号状态失效后, 此时终端不会到byod进行认证, 而是直接在本业务VLAN进行认证 (EIA会下发重定向URL), 原则上认证也是没有问题的, 但是DHCP服务器侧, byod VLAN对应的DNS设置和业务VLAN DNS设置不相同。
- 3) 另外现场反馈一个新问题, 华为手机认证成功后, 无感知未过期, 终端漫游每天都需要重新认证几次, 在Director查看终端认证失败日志提示: "应用场景阻止"导致的, 原因是客户自己在应用场景添加禁止第三方路由接入策略, 策略内容是基于厂商MAC其中包含了华为、中兴、小米等。删除华为策略后终端重新认证, 测试切换漫游来回走动上网正常, 问题解决。

解决方法在AC上添加rule规则放通业务VLAN对应的DNS source地址。导致此问题的最终原因还是由ADCAM平台升级认证机制变化导致, 升级方案评估未考虑到此问题, 所以希望研发在这种应用场景下实验室也要充分验证, 建议日后添加到开局手册中避免其他局点升级遇到相同问题。