

## 问题描述

现场AC型号是WX2580X，版本是R5630，现场的认证方式是 AC结合友商的ClearPass服务器进行portal认证，现场已有其他AC结合相同服务器认证成功。

报错异常为：可以正常弹出输入短信和验证码的页面，但是点击登陆之后要等一会，之后跳转到AC本地的页面报错。

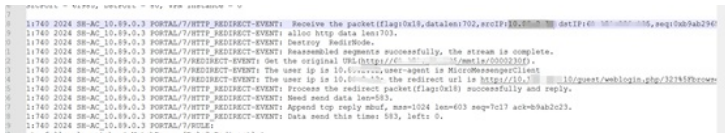


## 过程分析

1、首先检查AC配置，发现与另一台认证成功的AC设备配置基本一样，没有什么问题：

```
wlan service-template XX-guest
ssid XX-GUEST
vlan 20
user-isolation enable
portal enable method direct
portal domain XX-guest
portal bas-ip 10.Y.Y.3
portal apply web-server XX-guest
service-template enable
#
domain XX-guest
authorization-attribute idle-cut 120 1
nas-id XX-GUEST
authentication portal radius-scheme XX-guest
authorization portal radius-scheme XX-guest
accounting portal radius-scheme XX-guest
#
radius scheme XX-guest
primary authentication 10.X.X 10
primary accounting 10.X.X 10
key authentication cipher $c$3$dPpcfNeF8QXbPwA+xm9O2axudOnJZI7RnQ==
key accounting cipher $c$3$AuWwWojbWwEQ5TikHQPMEsYlr22aZM7oJaw==
user-name-format without-domain
nas-ip 10.Y.Y.3
#
portal web-server XX-guest
url http://10.X.X.10/guest/weblogin.php/32?_browser=1
server-type cmcc
#
portal server XX-guest
ip 10.Y.Y.3 key cipher $c$3$vh+7qjCDSOUH1Cl2zTfjbb1zh5umvkQiKg==
server-type cmcc
#
portal local-web-server http
default-logon-page defaultfile.zip
#
portal local-web-server https
default-logon-page defaultfile.zip
```

2、在AP的上行接口进行端口镜像抓包，同时在AC上debug portal all和debug radius all。Debug显示重定向没有问题，这个和能正常弹出portal页面的现象也能对应上。

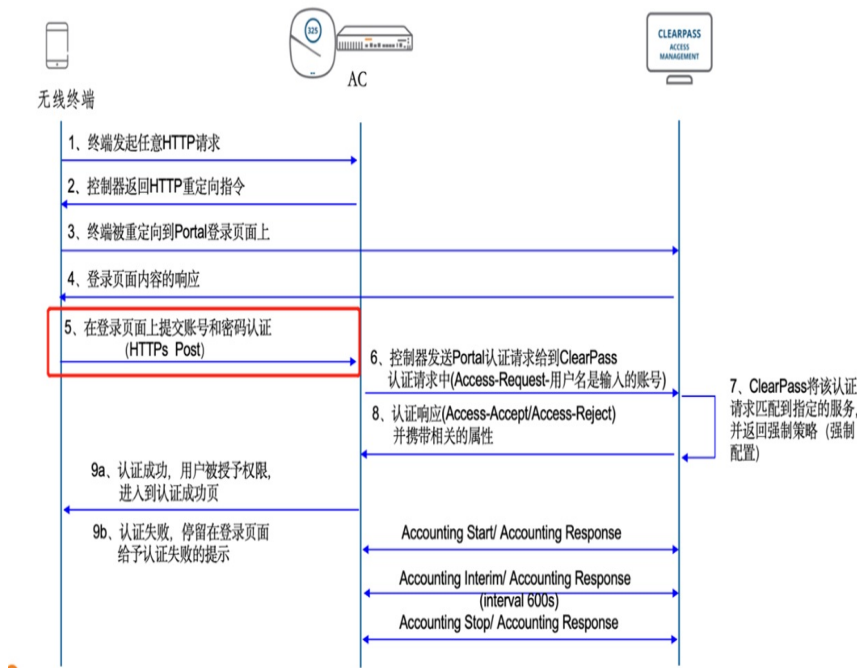


抓包显示终端和AC的TCP连接建立失败，也就是说中间网络通信有问题。

```

Time      Source          Destination      Protocol  Length  Info
-----
2713.2824-09-09 12:46:19.138648 10.47.10.12 10.47.10.12    TCP      60      [RST] Seq=1083716844 Win=0 Len=0
4497.2824-09-09 12:46:22.22555 10.47.10.12 10.47.10.12    TCP      60      [RST] Seq=1083716844 Win=0 Len=0
5412.2824-09-09 12:46:24.872451 10.47.10.12 10.47.10.12    TCP      60      [RST] Seq=1083716844 Win=0 Len=0
    
```

抓包分析和debug分析也是一样的，如下为结合ClearPass的认证流程，也就是第5步：终端给AC发的提交账号和密码的https报文没有到AC上，导致后续流程出现异常。



3、之后让现场排查终端和AC的通信问题，发现是中间网络设备做了策略，放开对应的策略之后终端正常认证成功。

### 解决方法

中间设备网络策略导致终端无法与AC建立TCP通信，放开对应策略就可以正常认证成功。