某局点Apple iOS终端进行EAP-TLS认证失败案例

iMC　陈冰洁　2020-02-07 发表

组网及说明

无

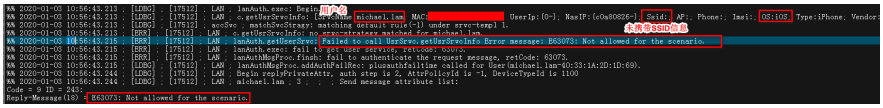
问题描述

某局点使用EAP-TLS证书认证方式进行认证，使用的是终端自带的EAP-TLS客户端。其中，Android终端可以成功认证上线，而Apple iOS终端认证失败，具体表现为Apple iOS终端在进行认证证书安装过程中，停留在输入账号密码这一步，如下图所示，即Apple iOS终端证书认证失败，导致其无法成功认证上线。

过程分析

1、收集uam的debug日志信息及测试的用户名信息。

2、分析uam日志，发现该测试的iOS终端提示：Error message: E63073: Not allowed for the scenario，即用户在对应的场景中不允许接入。



3、在iMC上查看对应的接入服务信息，发现接入场景是根据终端的SSID进行匹配的，而接入服务的缺省接入策略为禁止接入。从日志可以看出，iOS终端在进行证书认证时，输入账号密码后，将对应的信息发送给imc，而此时的报文并未携带相应的SSID信息，因此未匹配到接入场景，反而匹配了缺省策略（缺省策略为禁止接入）。

详细过程分析：该Apple iOS终端认证方案，需要设置两个SSID，一个是下载认证证书用的SSID，一个是业务SSID。 Apple iOS终端第一次下载证书的时候，连的是CA的SSID，在输入账号密码的时候，此时发到imc的报文只携带了账号密码，并未携带SSID信息，所以匹配到了缺省策略。只有将缺省策略设置为允许接入，Apple iOS终端的证书认证过程才能完成，从而进行下一步的用户认证上线。

备注：

Apple iOS终端是通过网页配置的， Android终端是通过app配置的。两者进行认证的时候处理逻辑不同，所以有时才会出现Android终端认证成功，而Apple iOS终端认证失败的现象。

解决方法

解决方案：将缺省接入策略配置为非禁止接入，即可以配置一个权限低的接入策略，通过下发acl或者v

lan之类来限制该策略下的访问权限。