某局点EWPXM2WCMD0F 无线V7的AC控制器板卡对接第三方的认证服务器做portal认证异常排查经验案例

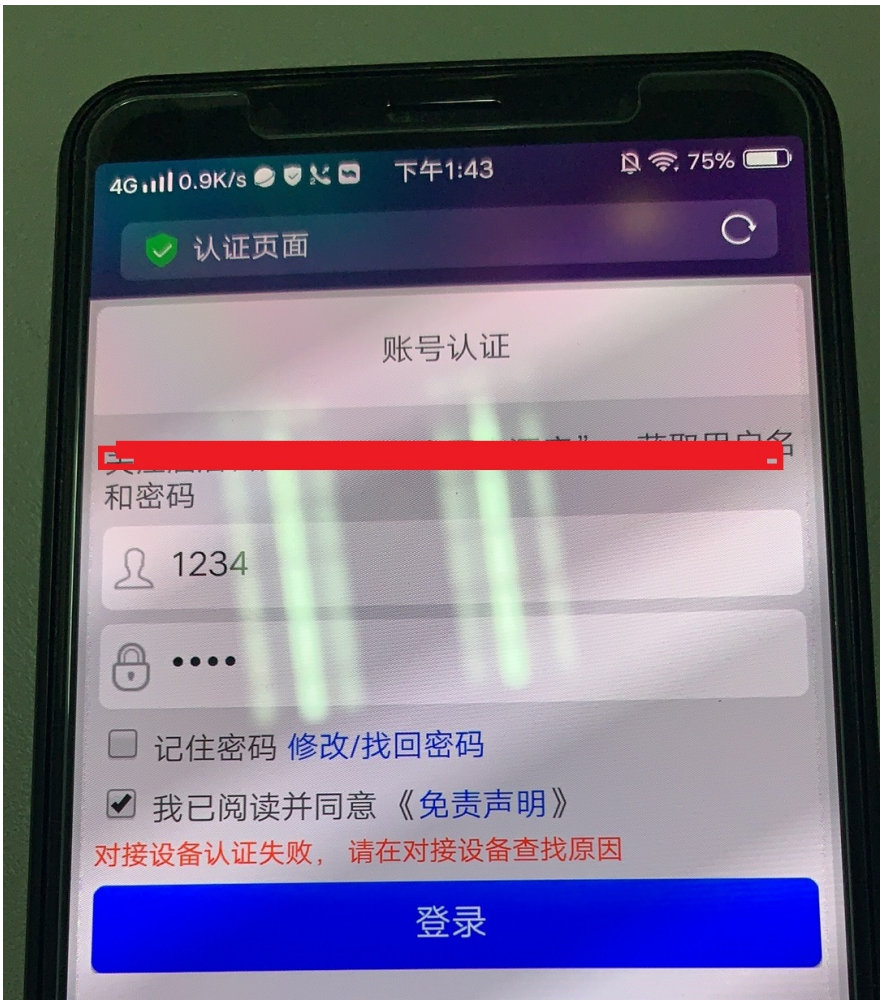
Portal 徐猛 2019-08-19 发表

组网及说明

普通企业网组网，无线控制器旁挂在核心交换机旁，终端的网关在核心交换机上，无线控制器上有和终端同网段的地址。portal服务器和AAA服务器为第三方服务器，也在该内网中部署。（为保护隐私，本案例对部分信息做了隐匿）

问题描述

现场配置完portal认证后，终端连接上无线信号，能正常弹出portal页面，但是在终端输入用户名和密码后，点击登录按钮，页面上提示对接设备认证失败。请在对接设备查找原因。

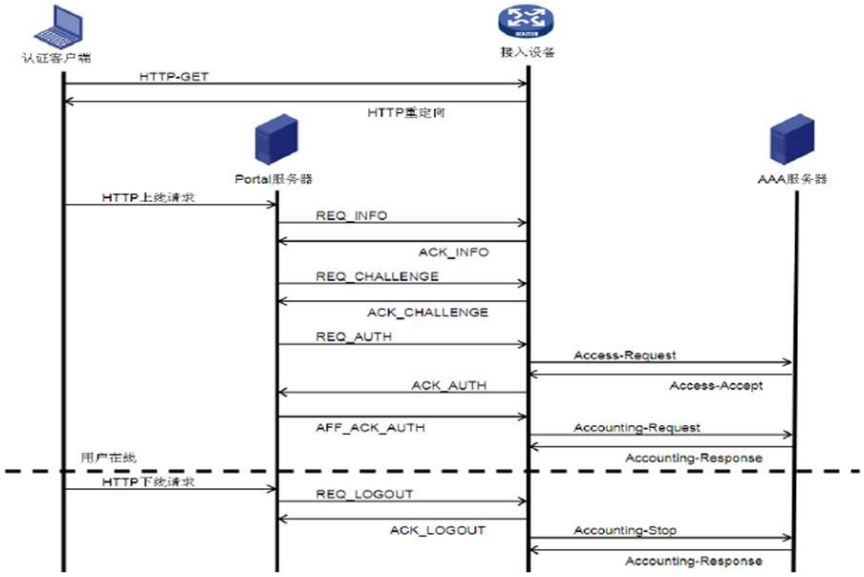


过程分析

1.根据现场的情况看，我们设备侧，对于终端上网的流量，进行重定向是正常的。检查设备portal认证相关配置，现场是采用的集中转发方式，相关portal配置也都正常：

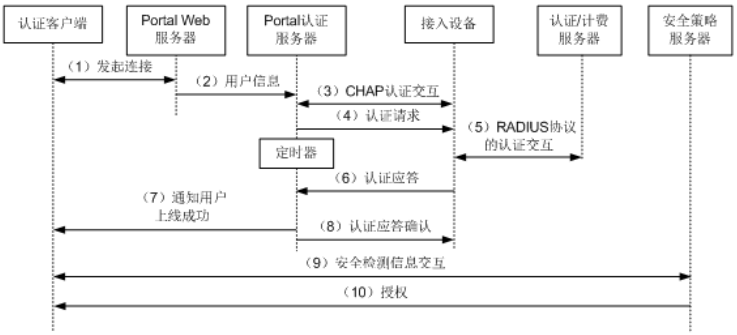
2.现场收集设备debug portal all 以及debug radius all的信息，发现设备portal认证过程，到portal重定向完成后，就没有后续内容了，设备的重定向记录如下：
*Aug 17 13:43:31:016 2019 AC PORTAL/7/REDIRECT-EVENT: The user ip is 192.168.2.135; the redirect url is http://10.0.0.3/?url_id=1564379&userip=192.168.2.135&usermac=D4-50-3F-**-**-47&ssid=GuoBinHotel

3. 通常我们设备会用来对接IMC服务器使用，对接portal服务器时，我们设备侧和服务器侧的常见报文交互流程如下，根据现场现象，以及debug出的情况，服务器侧未反馈REQ_INFO报文给设备，故开始认为是portal服务器的问题，后续由第三方厂家portal服务器工程师定位，发现他们的服务器直接回复了REQ_AUTH报文，而跳过了RER_INFO以及REQ_Challenge过程。



根据现场第三方portal服务器抓包的情况，后续跟第三方厂家确认了下，他们使用的认证方式为PAP，而通常对接我们IMC使用的是CHAP，根据Portal原理，如果是PAP的方式，服务器直接回复REQ_Auth，是正常的流程。详细可以看下下面流程分析PAP和CHAP的区别说明：

流程图如下：



认证流程：

(1)　Portal用户通过HTTP/HTTPS协议访问外部网络。HTTP/HTTPS报文经过接入设备时，对于访问Portal Web服务器或设定的免认证地址的HTTP/HTTPS报文，接入设备允许其通过；对于访问其它地址的HTTP/HTTPS报文，接入设备将其重定向到Portal Web服务器。Portal Web服务器提供Web页面供用户输入用户名和密码。

(2)　Portal Web服务器将用户输入的信息提交给Portal认证服务器进行认证。

//**此处第（3）部过程为重点区别点说明：**

(3)　Portal认证服务器与接入设备之间进行CHAP（Challenge Handshake Authentication Protocol，质询握手认证协议）认证交互。若采用**PAP（Password Authentication Protocol，密码认证协议）认证则直接进入下一步骤。采用哪种认证交互方式由Portal认证服务器决定。**

(4)　Portal认证服务器将用户输入的用户名和密码组装成认证请求报文发往接入设备，同时开启定时器等待认证应答报文。

(5)　接入设备与RADIUS服务器之间进行RADIUS协议报文的交互。

(6)　接入设备向Portal认证服务器发送认证应答报文，表示认证成功或者认证失败。

(7)　Portal认证服务器向客户端发送认证成功或认证失败报文，通知客户端认证成功（上线）或失败。

(8)　若认证成功，Portal认证服务器还会向接入设备发送认证应答确认。若是iNode客户端，则还需要进行以下安全扩展功能的步骤，否则Portal认证过程结束，用户上线。

(9)　客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测客户端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

(10)　安全策略服务器根据安全检查结果授权用户访问指定的网络资源，授权信息保存到接入设备中，接入设备将使用该信息控制用户的访问。

步骤(9)、(10)为Portal认证安全扩展功能的交互过程。

4.根据上述分析，由于第三方portal服务器使用的是PAP方式，那么直接回应REQ_AUTH报文给设备就是正常的，于是我们继续分析下设备侧是否有什么问题，查看设备侧的debug过程：

*Aug 17 13:43:35:853 2019 AC PORTAL/7/PACKET:

Portal received 56 bytes of packet: **Type=req_auth(3)**, ErrCode=0, IP=192.168.3.37

*Aug 17 13:43:35:853 2019 AC PORTAL/7/PACKET:

[1 USERNAME] [6] [1234]

[2 PASSWORD] [18] [******]

*Aug 17 13:43:35:853 2019 AC PORTAL/7/PACKET:
02 03 01 00 c6 33 00 00 c0 a8 03 25 00 00 00 02
62 19 04 0d 7b 82 02 17 59 80 2f 53 83 a0 07 3a
01 06 31 32 33 34 02 12 38 64 34 32 31 65 38 39
32 61 34 37 64 66 66 35

*Aug 17 13:43:35:853 2019 AC PORTAL/7/ERROR: **Failed to obtain user physical information when create user**.UserIP=192.168.3.37
*Aug 17 13:43:35:854 2019 AC PORTAL/7/ERROR: Portal is disabled on the interface.
*Aug 17 13:43:35:854 2019 AC PORTAL/7/PACKET:
Portal sent 38 bytes of packet: **Type=ack_auth(4), ErrCode=1**, IP=192.168.3.37

发现，设备侧对服务器侧发送的REQ_AUTH报文给回应了errCode=1的非正常响应，这也是代表着设备拒绝了认证请求，查看debug报错显示：**Failed to obtain user physical information when create user，意思是设备在新建portal用户时，无法正常的获取用户的物理信息。默认情况下，设备会根据自身ARP表项是否包含该用户的ARP物理信息，来检查认证的终端是否合法。合法则通过认证。非法则拒绝认证通过。后来经过确认，终端的网关并不在AC上，终端正常情况下也不会发ARP请求等给AC，所以AC上没有终端的ARP表项，后来让现场在设备上开启**portal host-check enable 命令使用后，现场认证业务实现正常。

解决方法

由于我们设备进行portal认证的时候，会对终端的合法性进行检查，默认情况下，AC只是通过ARP表项来检查终端的合法性，当终端网关不在AC上时，AC可能不会有终端的ARP表项信息，故需要使用portal host-check enable命令开启允许使用WLAN Snooping表、DHCP Snooping表和ARP表对其进行合法性检查的功能 本功能开启后，当设备收到未认证Portal用户的认证报文后，将使用WLAN Snooping表、DHCP Snooping表和ARP表对其进行合法性检查。如果在这三个表中查询到该Portal客户端信息，则认为其合法并允许进行Portal认证。