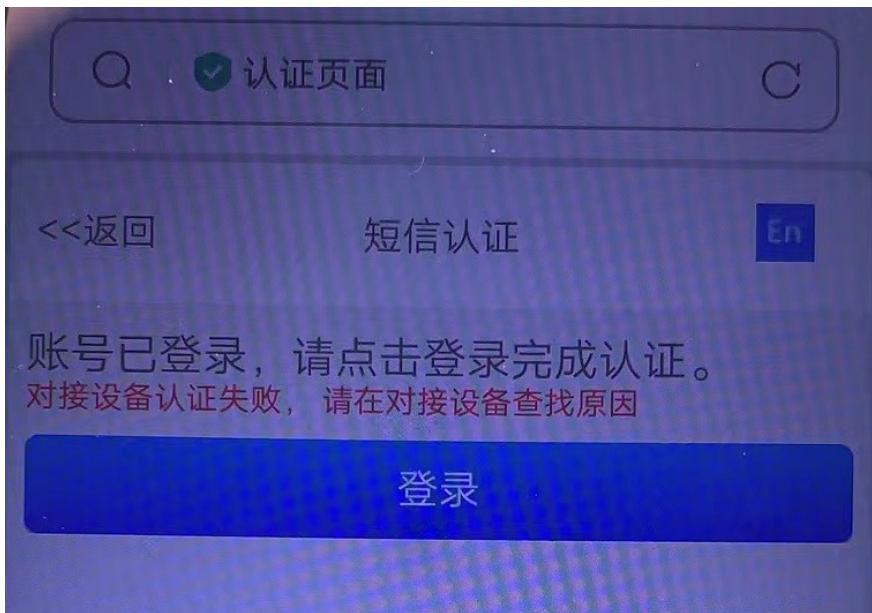


知 某局点 WX2540X-LI 对接信锐Portal短信认证失败

Portal 付军 2023-10-31 发表

问题描述

现场反馈对接信锐Portal短信认证失败



过程分析

在AC开启debug, 然后过一遍认证收集debug信息分析

<AC>debugging portal all

<AC>debugging radius all

【第一次抓包】：

*Sep 19 11:45:41:745 2023 AC PORTAL/7/PACKET:

Portal received 63 bytes of packet: **Type=req_auth(3)**, ErrCode=0, IP=192.168.10.x //设备收到服务器发来的req_auth报文, 获取用户名密码

*Sep 19 11:45:41:745 2023 AC PORTAL/7/PACKET:

[1 USERNAME] [13] [18xxxxxx]

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

*Sep 19 11:45:41:745 2023 AC PORTAL/7/PACKET:

02 03 01 00 03 67 00 00 c0 a8 0a 52 00 00 00 02

48 29 91 97 b3 79 a8 83 ad fb 9c 07 9e 75 ef a3

*Sep 19 11:45:41:745 2023 AC PORTAL/7/ERROR: **Failed to obtain user physical information when create user.UserIP=192.168.10.x //获取用户信息失败**

*Sep 19 11:45:41:745 2023 AC PORTAL/7/ERROR: **Portal is disabled on the interface.**

*Sep 19 11:45:41:745 2023 AC PORTAL/7/ERROR: **User mac is invalid.**

*Sep 19 11:45:41:745 2023 AC PORTAL/7/ERROR: Failed to get get ssid by user mac,UserMac is Zero.

*Sep 19 11:45:41:746 2023 AC PORTAL/7/PACKET:

Portal sent 38 bytes of packet: **Type=ack_auth(4)**, **ErrCode=1**, IP=192.168.10.x //设备回了ErrCode=1表示3A认证失败

*Sep 19 11:45:41:746 2023 AC PORTAL/7/PACKET:

[10 BASIP] [6] [192.168.9.xxx]

【第二次抓包】：

*Sep 19 17:54:48:732 2023 AC PORTAL/7/EVENT: Success to get info from wlan snooping, vlan:10. mac:xxxx-xxxx-xxxx,userip:192.168.10.x

*Sep 19 17:54:48:732 2023 AC PORTAL/7/EVENT: Success to get ifindex(262) and vlan(10) from IP CIM, user IP=192.168.10.x,MAC=xxxx-xxxx-xxxx

*Sep 19 17:54:48:732 2023 AC PORTAL/7/EVENT: Success to get ifindex(262) and vlan(10) from IP CIM, user IP=192.168.10.x,MAC=xxxx-xxxx-xxxx

*Sep 19 17:54:48:732 2023 AC PORTAL/7/PACKET:

Portal received 63 bytes of packet: Type=req_auth(3), ErrCode=0, IP=192.168.10.x

*Sep 19 17:54:48:732 2023 AC PORTAL/7/PACKET:

[1 USERNAME] [13] [18xxxxxxx]

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

*Sep 19 17:54:48:747 2023 AC RADIUS/7/EVENT:

Found request context, dstIP: xxx.xxx.xxx.xxx, dstPort: 1812, VPN instance: --(public), socketFd: 116, pktID: 135.

*Sep 19 17:54:48:747 2023 AC RADIUS/7/EVENT:

The reply packet is valid.

*Sep 19 17:54:48:747 2023 AC RADIUS/7/EVENT:

Decoded reply packet successfully.

*Sep 19 17:54:48:747 2023 AC RADIUS/7/PACKET: //服务器回消息: 认证被拒绝

User-Name="18xxx@radius"

Reply-Message="authen reject"

*Sep 19 17:54:48:747 2023 AC RADIUS/7/PACKET:

03 87 00 37 de a9 e0 f9 09 0d d3 29 1c 71 43 94

88 9b c9 b7 01 14 31 38 31 30 35 31 31 38 31 39

*Sep 19 17:54:48:747 2023 AC RADIUS/7/EVENT:

Sent reply message successfully.

*Sep 19 17:54:48:747 2023 AC RADIUS/7/EVENT:

PAM_RADIUS: Processing RADIUS authentication.

*Sep 19 17:54:48:747 2023 AC RADIUS/7/EVENT:

PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 1

解决方法
*Sep 19 17:54:48:747 2023 AC PORTAL/7/EVENT: User-SM[192.168.10.82]: Received authentication response, resultCode=26.

第一次抓包的问题
AC没有拿到终端的MAC地址，需要在AC上配置portal-hsm-check-enable。

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。
Portal send by Portal packet: Type=ack_auth(4), ErrCode=1, IP=192.168.10.x

*Sep 19 17:54:48:747 2023 AC PORTAL/7/PACKET:

第二次抓包的问题: [[8] [xxxx-xxx-xxxx]

第一次EXTINFO-check失败，可以看到AC通过wlan snooping拿到了终端的MAC地址，但是从debug信息中看到服务器拒绝了认证。检查AC和服务器两端的配置，发现发给服务器的用户名带了domain域的名称，在AC上配置不带域名：

```
radius scheme 1
```

```
user-name-format without-domain
```

配置之后终端Portal认证成功

注意事项

业务空窗期排查

