某局点WX2510H做微信认证异常问题处理经验案例

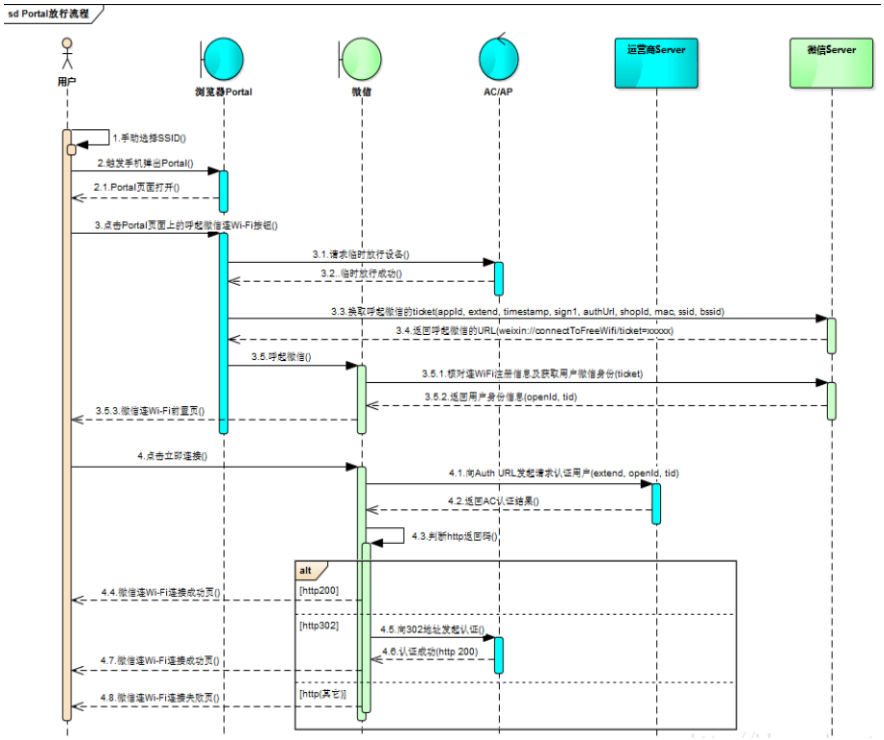
Portal 孟普 2019-06-30 发表

组网及说明

某局点做无线的微信认证，认证端是云端的服务器。

问题描述

做普通微信认证正常通过，但是客户希望提高网络的监控和安全度，希望在微信认证的时候添加TID（加密后的用户手机）属性，发现添加该属性后认证就异常。认证过程如下：



8. 连接Wi-Fi

用户点立即连接 按钮，微信自动向authUrl（JSAPI的传入参数）发起请求，提交认证所需的用户微信身份信息参数，包括extend、openId、tid。

```
http://www.fangbei.org/wifigw/
auth.xhtml?httpCode=200&extend=fangbei&
openId=oiPuduCHIBb2aHvZoqSm1t7KbXtw&
tid=010002d1eb4ee298934a7d44c1ece599ed5
7c4c010119bb23028b8
```

参数说明如下

参数	说明
extend	为上文中调用呼起微信JSAPI时传递的ext
openId	用户的微信openId
tid	为加密后的用户手机号码（仅作网监部门

云端Auth URL 返回AC认证结果

authUrl所对应的后台认证服务器必须能识别这些参数信息，并向微信客户端返回AC认证结果，微信客户端将根据http返回码，提示用户连网成功与否。

过程分析

1.查看配置，发现正常：

```
#
 version 7.1.064, Release 5221
#

#
 dns server 114.114.114.114
```

```
#
vlan 800
 description i-guangdong-wifi
#
vlan 810
 description i-guangdong-wifi-user
#
wlan service-template 1
 ssid i-Guangdong
 vlan 810
 user-isolation enable
 client-rate-limit enable
 client-rate-limit inbound mode static cir 512
 client-rate-limit outbound mode static cir 6144
 portal enable method direct
 portal domain i-guangdong
 portal bas-ip 10.65.4.163
 portal apply web-server portal
 service-template enable
#
wlan service-template 2
 ssid cl-office
 akm mode psk
 preshared-key pass-phrase cipher $c$3$ojfOHtlQFJZNcmtndKhszuVO9iAVY0GXG0+lcw==
 cipher-suite ccmp
 security-ie rsn
 client-rate-limit enable
 client-rate-limit inbound mode static cir 512
 client-rate-limit outbound mode static cir 12288
 service-template enable
#
wlan service-template 3
 ssid iGT
 vlan 810
 user-isolation enable
 portal enable method direct
 portal domain i-guangdong-portal3
 portal bas-ip 10.65.4.163
 portal apply web-server portal3
 service-template enable
#
interface NULL0
#
interface Vlan-interface800
 ip address 10.65.4.163 255.255.255.224
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 800
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 810
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 810
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 description link-to-route
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 800 810
```

```
#
 ip route-static 0.0.0.0 0 10.65.4.161
#
 radius session-control enable
#
radius scheme i-guangdong
 primary authentication 10.64.1.201 key cipher $c$3$qXeFEBd8VF8Kk1ySRmVh9cQfUP8ka5PgbMlF
gz0aCFQAEG8=
 primary accounting 10.64.1.201 key cipher $c$3$tbG57h1SD566zp5SxXAHaO4WQhKJD5fqx+9rStx
WqKhZY30=
 key authentication cipher $c$3$4WE02rHwjgHV4jT4bh3nRIeakKkbCuw3nYV3MwCA97ndUP0=
 key accounting cipher $c$3$/2jhhSOpqE5AoHJiOBLISYxtjPsI+8EuIMl4WjPyfS8pWrA=
 user-name-format keep-original
 nas-ip 10.65.4.163
#
radius scheme i-guangdong-portal3
 primary authentication 10.64.2.104 key cipher
$c$3$A7hfmQ1Il5PMT6Y2qt2qrt4DwkWmzGuTSIJRC/LCA++PxwI=
 primary accounting 10.64.2.104 key cipher
$c$3$/vq/m668j7ZoRMlVHFLlAQBenmFs5P4uH32aKmkqnjjwfqg=
 key authentication cipher $c$3$DWsVsgeUUj7UYKF4FvfsOkJNSvtR9xHZOafIpup4dVLT8xs=
 key accounting cipher $c$3$sUftC5uX84n8j59qJVER3BjQZsiv4unajDyBUtkMsHt1oig=
 user-name-format keep-original
 nas-ip 10.65.4.163
#
domain i-guangdong
 authorization-attribute idle-cut 120 10240
 session-time include-idle-time
 authentication portal radius-scheme i-guangdong
 authorization portal radius-scheme i-guangdong
 accounting portal radius-scheme i-guangdong
#
domain i-guangdong-portal3
 authorization-attribute idle-cut 120 10240
 session-time include-idle-time
 authentication portal radius-scheme i-guangdong-portal3
 authorization portal radius-scheme i-guangdong-portal3
 accounting portal radius-scheme i-guangdong-portal3
#
 portal host-check enable
 portal device-id IGD_H3C_CJRJYPX
 portal auth-fail-record enable
 portal auth-error-record enable
 portal free-rule 1 source ip any destination ip 114.67.*.0 255.255.255.240
 portal free-rule 2 source ip 114.67.*.0 255.255.255.240 destination ip any
 portal free-rule 3 source ip any destination ip 202.96.*.86 255.255.255.255
 portal free-rule 4 source ip any destination ip 202.96.*.166 255.255.255.255
 portal free-rule 5 source ip any destination ip 10.64.1.0 255.255.255.0
 portal free-rule 6 source ip 10.64.1.0 255.255.255.0 destination ip any
 portal free-rule 7 source ip any destination ip 114.114.114.114 255.255.255.255
 portal free-rule 8 source ip any destination ip 10.64.2.0 255.255.255.0
 portal free-rule 9 source ip 10.64.2.0 255.255.255.0 destination ip any
 portal free-rule 10 source interface GigabitEthernet1/0/5
#
portal web-server portal
 url https://i-guangdong.windfindtech.com/portal/login
 server-type cmcc
 url-parameter apmac ap-mac
 url-parameter nasid nas-id
 url-parameter userip source-address
 url-parameter usermac source-mac
 url-parameter wlanacip value 10.65.4.163
 url-parameter wlanacname value IGD_H3C_CJRJYPX
#
```

```
portal web-server portal3
 url https://i-guangdong.windfindtech.com/portal2/login
 server-type cmcc
 url-parameter apmac ap-mac
 url-parameter nasid nas-id
 url-parameter userip source-address
 url-parameter usermac source-mac
 url-parameter wlanacip value 10.65.4.163
 url-parameter wlanacname value IGD_H3C_CJRJYPX
#
portal server portal
 ip 10.64.1.3
 server-type cmcc
#
portal server portal2
 ip 10.64.1.4
 server-type cmcc
#
portal server portal3
 ip 10.64.1.234
 server-type cmcc
#
portal server portal4
 ip 10.64.2.104
 server-type cmcc
#
wlan global-configuration
 control-address enable
 nas-id 767017
#
wlan ap-group default-group
 vlan 1
 ap-model WA4320-ACN-SI
  radio 1
   radio enable
   service-template 1 vlan 810
   service-template 2 vlan 810
   service-template 3 vlan 810
  radio 2
   radio enable
   service-template 1 vlan 810
   service-template 2 vlan 810
   service-template 3 vlan 810
#
wlan ap 2f-01 model WA4320-ACN-SI
 serial-id 219801A0T78171E08716
 radio 1
  radio enable
  channel band-width 40
 radio 2
  radio enable
#
wlan ap 2f-02 model WA4320-ACN-SI
 serial-id 219801A0T78171E05524
 radio 1
  radio enable
  channel band-width 40
 radio 2
  radio enable
#
wlan ap 2f-03 model WA4320-ACN-SI
 serial-id 219801A0T78171E08761
 radio 1
  channel band-width 40
```

```
 radio 2
  radio enable
#
wlan ap 3f-04 model WA4320-ACN-SI
 serial-id 219801A0T78171E06080
 radio 1
  radio enable
  channel band-width 40
 radio 2
  radio enable
#
wlan ap 3f-05 model WA4320-ACN-SI
 serial-id 219801A0T78171E08346
 radio 1
  radio enable
  channel band-width 40
 radio 2
  radio enable
#
wlan ap 3f-06 model WA4320-ACN-SI
 serial-id 219801A0T78171E05550
 radio 1
  radio enable
  channel band-width 40
 radio 2
  radio enable
#
 cloud-management server domain oasis.h3c.com
#
```

2.看了一下故障的debug，如下：

```
*May 27 15:44:00:386 2019 IGD_H3C_CJRJYPX PORTAL/7/EVENT: User-SM[172.18.0.107]: Notified Auth-SM to process the REQ_AUTH packet.
*May 27 15:44:00:386 2019 IGD_H3C_CJRJYPX PORTAL/7/FSM: Auth-SM: Started to run.
*May 27 15:44:00:387 2019 IGD_H3C_CJRJYPX PORTAL/7/FSM: Auth-SM [172.18.0.107]: Entered state Authenticating.
*May 27 15:44:00:387 2019 IGD_H3C_CJRJYPX PORTAL/7/EVENT: User-SM[172.18.0.107]: AAA processed authentication request and returned processing.
*May 27 15:44:00:387 2019 IGD_H3C_CJRJYPX PORTAL/7/FSM: User-SM[172.18.0.107]: Begin to run.
*May 27 15:44:00:387 2019 IGD_H3C_CJRJYPX PORTAL/7/EVENT: User-SM[172.18.0.107]: Received authentication response, RespCode=26.
*May 27 15:44:00:387 2019 IGD_H3C_CJRJYPX PORTAL/7/FSM: Auth-SM: Started to run.
*May 27 15:44:00:387 2019 IGD_H3C_CJRJYPX PORTAL/7/PACKET:
Portal sent 16 bytes of packet: Type=ack_auth(4), ErrCode=1, IP=172.18.0.107
```

正常portal过程，AC收到portal服务器发送的REQ-AUTH（type=3）的报文之后，应该会和AAA服务器交互认证报文，AAA服务器回复通过之后，AC才会回复ACK-AUTH（type=4），errorcode=0 的报文给portal服务器。

而上面这个不正常的认证过程，可以发现AAA服务器回复的RespCode=26代表信息交互不正常，正常应该是：

```
*May 27 16:18:12:190 2019 IGD_H3C_CJRJYPX PORTAL/7/EVENT: User-SM[172.18.0.107]: Received authentication response, RespCode=0.
```

即AAA服务器不通过这个认证，导致后续AC给portal服务器回复的ACK-AUTH（type=4）报文的errorcode=1，所以这就应该排查服务器为什么回复的是RespCode=26。

解决方法

通过排查服务器端解决问题。对于跟第三方对接的问题，要根据实际情况判断是我司设备问题还是第三方设备问题。