某局点portal用户不需要认证直接上网问题分析

Portal 朱恺 2019-12-12 发表

组网及说明

问题描述

某局点网络出现A区域覆盖的WIFI能够正常认证上网，B区域的WIFI不用认证即可上网，两个区域的WIFI均是本地转发采用相同的SSID，除了不同的vlan和网关。

过程分析

1、现场工程师在B区域连接SSID：XXXX-GUEST或者XXXX-WLAN，从配置上看，两者除名称外并无区别，问题现象依旧是不用认证可以上网不能，设备上也看不到认证表项。

```
wlan service-template scal-guest
 ssid XXXX-GUEST
 client forwarding-location ap
 client vlan-alloc static
 portal enable method direct
 portal domain portal
 portal bas-ip 1.1.1.2
 portal apply web-server AAA
 portal apply mac-trigger-server AAA
 portal fail-permit web-server
 service-template enable
#
wlan service-template scal-wlan
 ssid XXXX-WLAN
 client forwarding-location ap
 client vlan-alloc static
 portal enable method direct
 portal domain portal
 portal bas-ip 1.1.1.2
 portal apply web-server AAA
 portal apply mac-trigger-server AAA
 portal fail-permit web-server
 service-template enable
```

2、通常设备开启portal后会拒绝任意未通过认证的流量，且终端在B区域上网过程中也没有触发无感知生成表项，所以问题疑点只能是开启了逃生功能。

portal fail-permit web-server//开启Portal Web服务器不可达时的Portal用户逃生功能，即设备探测到Portal Web服务器不可达时暂停Portal认证功能，允许用户不经过Portal认证即可自由访问网络。
server-detect interval 10 log trap//每10s发tcp包尝试与服务器建立连接，如不能建立则认为服务器故障，逃生生效不会对接入用户进行认证

3、新建测试SSID绑定B区域单一AP测试，
发现规律：
配置“portal fail-permit web-server”现象与之前一致；
删除“portal fail-permit web-server”无法自动弹出页面，手工输入url后认证成功；
新建测试web server 123，不采用特殊重定向，终端能够自动弹出页面认证成功。

```
 wlan service-template 123
 ssid 123
 client forwarding-location ap
 client vlan-alloc static
 portal enable method direct
 portal domain portal
 portal bas-ip 10.255.4.52
 portal apply web-server 123
 service-template enable

portal web-server 123
```

```
 url http:// 1.1.1.2 :8080/portal
#
portal web-server AAAA
 url http:// 1.1.1.2:8080/portal
 server-detect interval 10 log trap
 if-match original-url http://captive.apple.com/hotspot-detect.html user-agent Mozilla temp-pass redire
ct-url http://1.1.1.2:8080/portal
 if-match original-url http://www.apple.com user-agent Mozilla temp-pass redirect-url http://1.1.1.2:808
0/portal
```

4、根据以上测试，明确与逃生有关，在B区域的AP上ping服务器并不丢包，但探测的tcp无法建立。
这里选择B区域AP和A区域AP进行对比，发现B区域 ap无法探测到服务器逃生生效，A区域探测服务器正常。
同时在服务器进行抓包与现象一致，探测报文无法抵达服务器端，从ap ping服务器时，能够抓取icmp包。

解决方法

1、如果逃生功能不用，可以取消逃生功能和web-server的if-match重定向策略；
2、如果逃生功能必要，需要找出中间网络限制tcp的原因，确保AP能够与服务器探测正常