某无线portal用户部分区域不用认证直接上网问题分析

wlan接入 Portal 陈铮 2019-03-20 发表

组网及说明

不涉及

问题描述

某用户无线网络出现S楼覆盖的WIFI能够正常认证上网，N号楼的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不同vlan和网关。

过程分析

1、现场工程在N楼区域连接SSID：A或者B，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 guest
 ssid A
 client forwarding-location ap
 client cache aging-time 0
 client vlan-alloc static
 preshared-key pass-phrase cipher $c$3$pjyIFJGkFA3p2k4OFCbHajCuHXsCdniQ+Ym+
 portal enable method direct
 portal domain portal
 portal bas-ip 10.255.4.52
 portal apply web-server zb
 portal apply mac-trigger-server zb
 portal fail-permit web-server
 service-template enable
#
wlan service-template wlan
 ssid B
 client forwarding-location ap
 client cache aging-time 0
 client vlan-alloc static
 portal enable method direct
 portal domain portal
 portal bas-ip 10.255.4.52
 portal apply web-server XX
 portal apply mac-trigger-server XX
 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N号楼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N楼单一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 cache aging-time 0
 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
```

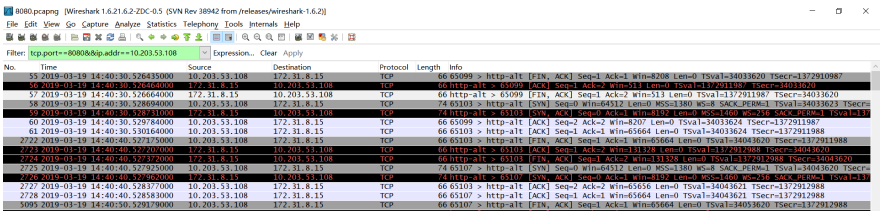
```
portal web-server 123
 url http://172.31.8.15:8080/portal
#
portal web-server zb
 url http://172.31.8.15:8080/portal
 server-detect interval 10 log trap
 if-match original-url http://captive.apple.com/hotspot-detect.html user-agent Mozilla temp-pass redire
ct-url http://172.31.8.15:8080/portal
 if-match original-url http://www.apple.com user-agent Mozilla temp-pass redirect-url
http://172.31.8.15:8080/portal
```

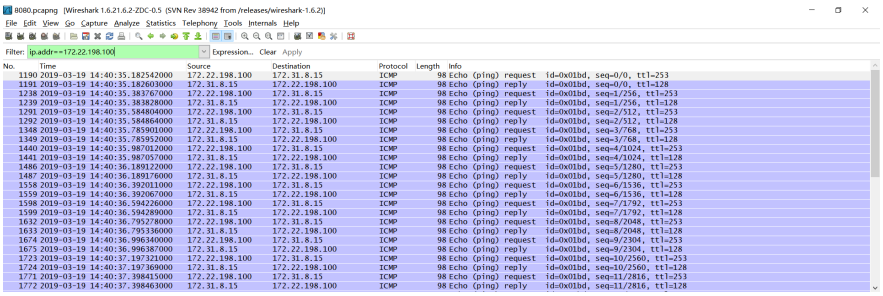
4、根据以上测试，明确与逃生有关，在N楼的AP上ping服务器并不丢包，但探测的tcp无法建立。
这里选择N楼AP g13和S楼1f-1进行对比，发现N楼ap无法探测到服务器逃生生效，S楼探测服务器正常。

```
[g13]dis tcp
 *: TCP MD5 Connection
 Local Addr:port       Foreign Addr:port     State       PCB
 0.0.0.0:23            0.0.0.0:0             LISTEN      0xffffffffffffff9d
 172.22.198.100:23     10.255.4.52:16749     ESTABLISHED 0x0000000000004077
 172.22.198.100:24593  172.31.8.15:8080      SYN_SENT    0x0000000000004079
 172.22.198.100:0      15.15.15.15:8080      SYN_SENT    0x000000000000407b
 172.22.198.100:64768  10.255.4.52:6633      ESTABLISHED 0xffffffffffffff9f
 172.22.198.100:64769  10.255.4.52:6633      ESTABLISHED 0xffffffffffffffa0
*Mar 19 15:07:46:284 2019 g13 SOCKET/7/TCP:
TCP Output(vrf = 0, state = SYN_SENT):
 TCP packet: src = 172.22.198.100/9537, dst = 172.31.8.15/8080
            seq = 936325537, ack = 0, flag = SYN
            window = 64512, checksum = 0x7a93, datalen = 0, headlen = 40

*Mar 19 15:07:49:283 2019 g13 SOCKET/7/TCP:
TCP Output(vrf = 0, state = SYN_SENT):
 TCP packet: src = 172.22.198.100/9537, dst = 172.31.8.15/8080
            seq = 936325537, ack = 0, flag = SYN
            window = 64512, checksum = 0x6edb, datalen = 0, headlen = 40

*Mar 19 15:07:52:483 2019 g13 SOCKET/7/TCP:
TCP Output(vrf = 0, state = SYN_SENT):
 TCP packet: src = 172.22.198.100/9537, dst = 172.31.8.15/8080
            seq = 936325537, ack = 0, flag = SYN
            window = 64512, checksum = 0x625b, datalen = 0, headlen = 40
<1f-1>dis tcp
 *: TCP MD5 Connection
 Local Addr:port       Foreign Addr:port     State       PCB
 0.0.0.0:23            0.0.0.0:0             LISTEN      0xffffffffffffff9d
 10.203.53.108:23      10.255.4.52:65044     ESTABLISHED 0x00000000000023de
 10.203.53.108:7235    172.31.8.15:8080      TIME_WAIT   0x00000000000023e4
 10.203.53.108:7239    172.31.8.15:8080      TIME_WAIT   0x00000000000023e8
 10.203.53.108:7243    172.31.8.15:8080      TIME_WAIT   0x00000000000023ec
 10.203.53.108:7247    172.31.8.15:8080      ESTABLISHED 0x00000000000023f0
 10.203.53.108:0       15.15.15.15:8080      SYN_SENT    0x00000000000023f2
 10.203.53.108:16823   172.31.8.15:8080      TIME_WAIT   0x00000000000023d7
 10.203.53.108:16827   172.31.8.15:8080      TIME_WAIT   0x00000000000023db
 10.203.53.108:16831   172.31.8.15:8080      TIME_WAIT   0x00000000000023e0
 10.203.53.108:49614   10.255.4.52:6633      ESTABLISHED 0xffffffffffffffad
 10.203.53.108:49615   10.255.4.52:6633      ESTABLISHED 0xffffffffffffffae

*Mar 19 15:05:13:601 2019 1f-1 SOCKET/7/TCP:
TCP Output(vrf = 0, state = SYN_SENT):
 TCP packet: src = 10.203.53.108/5643, dst = 172.31.8.15/8080
            seq = 3253741230, ack = 0, flag = SYN
            window = 64512, checksum = 0xd98c, datalen = 0, headlen = 40
```

*Mar 19 15:05:13:602 2019 1f-1 SOCKET/7/TCP:
TCP Output(vrf = 0, state = TIME_WAIT):
TCP packet: src = 10.203.53.108/5639, dst = 172.31.8.15/8080
seq = 3514846174, ack = 3973675138, flag = ACK
window = 8207, checksum = 0xca2d, datalen = 0, headlen = 32

*Mar 19 15:05:13:602 2019 1f-1 SOCKET/7/TCP:
TCP Output(vrf = 0, state = ESTABLISHED):
TCP packet: src = 10.203.53.108/5643, dst = 172.31.8.15/8080
seq = 3253741231, ack = 3787810994, flag = ACK
window = 8208, checksum = 0x19cc, datalen = 0, headlen = 32
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

排查中间网络，发现防火墙限制了tcp报文，放通以后逃生能够正常探测，portal认证业务正常。