

知 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  0xffffffff9d
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 0xffffffff9f
172.22.198.100:64769  10.255.4.52:6633  ESTABLISHED 0xfffffffffa0
*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  0xffffffff9d
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 0xfffffffffad
10.203.53.108:49615  10.255.4.52:6633  ESTABLISHED 0xfffffffffae
*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。

Wireshark 1.6.21.6.2-ZDC-0.5 (SVN Rev 38942 from /releases/wireshark-1.6.21) - 8080.pcapng

Filter: ip.addr==10.203.53.108

No.	Time	Source	Destination	Protocol	Length	Info
55	2019-03-19 14:40:30.526435000	10.203.53.108	172.31.8.15	TCP	66	65099 > http-alt [FIN, ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033620 TSecr=137291987
57	2019-03-19 14:40:30.526640000	172.31.8.15	10.203.53.108	TCP	66	http-alt > 65099 [FIN, ACK] Seq=1 Ack=2 Win=513 Len=0 Tsv1=137291987 TSecr=34033620
58	2019-03-19 14:40:30.526845000	10.203.53.108	172.31.8.15	TCP	66	65103 > http-alt [FIN, ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033620 TSecr=137291988
59	2019-03-19 14:40:30.527050000	10.203.53.108	172.31.8.15	TCP	66	65107 > http-alt [ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033620 TSecr=137291988
60	2019-03-19 14:40:30.529780000	10.203.53.108	172.31.8.15	TCP	66	65099 > http-alt [ACK] Seq=2 Ack=2 Win=8207 Len=0 Tsv1=134033624 TSecr=137291987
61	2019-03-19 14:40:30.530690000	10.203.53.108	172.31.8.15	TCP	66	65103 > http-alt [ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033624 TSecr=137291988
2722	2019-03-19 14:40:40.527175000	10.203.53.108	172.31.8.15	TCP	66	65103 > http-alt [FIN, ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033620 TSecr=137291988
2723	2019-03-19 14:40:40.527380000	10.203.53.108	172.31.8.15	TCP	66	65107 > http-alt [ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033620 TSecr=137291988
2724	2019-03-19 14:40:40.527590000	10.203.53.108	172.31.8.15	TCP	66	http-alt > 65103 [FIN, ACK] Seq=1 Ack=2 Win=513 Len=0 Tsv1=137291988 TSecr=34033620
2725	2019-03-19 14:40:40.527800000	10.203.53.108	172.31.8.15	TCP	66	65107 > http-alt [FIN, ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033620 TSecr=137291988
2726	2019-03-19 14:40:40.528010000	10.203.53.108	172.31.8.15	TCP	66	65103 > http-alt [ACK] Seq=2 Ack=2 Win=8207 Len=0 Tsv1=134033624 TSecr=137291987
2727	2019-03-19 14:40:40.528220000	10.203.53.108	172.31.8.15	TCP	66	65107 > http-alt [ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033624 TSecr=137291988
2728	2019-03-19 14:40:40.528430000	10.203.53.108	172.31.8.15	TCP	66	65107 > http-alt [ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033624 TSecr=137291988
3093	2019-03-19 14:40:30.529170000	10.203.53.108	172.31.8.15	TCP	66	65107 > http-alt [FIN, ACK] Seq=1 Ack=1 Win=8208 Len=0 Tsv1=134033620 TSecr=137291988

Wireshark 1.6.21.6.2-ZDC-0.5 (SVN Rev 38942 from /releases/wireshark-1.6.21) - 8080.pcapng

Filter: ip.addr==172.22.198.100

No.	Time	Source	Destination	Protocol	Length	Info
1150	2019-03-19 14:40:35.182540000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=0/0, ttl=253
1191	2019-03-19 14:40:35.182690000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=0/0, ttl=128
1238	2019-03-19 14:40:35.183760000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=1/256, ttl=253
1239	2019-03-19 14:40:35.183820000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=1/256, ttl=128
1292	2019-03-19 14:40:35.184800000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=2/512, ttl=253
1292	2019-03-19 14:40:35.184860000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=2/512, ttl=128
1348	2019-03-19 14:40:35.185910000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=3/768, ttl=253
1349	2019-03-19 14:40:35.185970000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=3/768, ttl=128
1440	2019-03-19 14:40:35.187020000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=4/1024, ttl=253
1441	2019-03-19 14:40:35.187080000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=4/1024, ttl=128
1480	2019-03-19 14:40:36.189120000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=5/1280, ttl=253
1481	2019-03-19 14:40:36.189180000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=5/1280, ttl=128
1538	2019-03-19 14:40:36.192010000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=6/1536, ttl=253
1539	2019-03-19 14:40:36.192070000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=6/1536, ttl=128
1598	2019-03-19 14:40:36.194260000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=7/1792, ttl=253
1599	2019-03-19 14:40:36.194320000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=7/1792, ttl=128
1632	2019-03-19 14:40:36.195270000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=8/2048, ttl=253
1633	2019-03-19 14:40:36.195330000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=8/2048, ttl=128
1673	2019-03-19 14:40:36.196380000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) request id=0x01bd, seq=9/2304, ttl=253
1674	2019-03-19 14:40:36.196440000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=9/2304, ttl=128
1724	2019-03-19 14:40:37.197320000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=10/2560, ttl=253
1725	2019-03-19 14:40:37.197380000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=10/2560, ttl=128
1774	2019-03-19 14:40:37.198430000	172.22.198.100	172.31.8.15	ICMP	98	Echo (ping) request id=0x01bd, seq=11/2816, ttl=253
1775	2019-03-19 14:40:37.198490000	172.31.8.15	172.22.198.100	ICMP	98	Echo (ping) reply id=0x01bd, seq=11/2816, ttl=128

解决方法

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