某局点无线控制器Portal认证对集中转发不生效经验案例

Portal wlan安全 尹灵康 2018-03-09 发表

某局点在服务模板下配置了Portal无感知认证，采用MAC+Portal的认证方式。使用中发现用户第一次可以正常关联上网，断开WiFi，再将服务器上的在线表项、MAC表项、设备上的在线表项删除后，用户再次关联可以直接上网，不用再次进行认证。

服务模板及AP下的配置如下：

```
wlan service-template aaa
 description 所有区域SSID
 ssid ABCD
 client forwarding-location ap vlan 601
 client-security authentication-mode mac
 client-security ignore-Authentication
 mac-authentication domain drcom
 portal enable method direct
 portal domain drcom
 portal bas-ip 10.1.1.250
 portal apply web-server drcom
 service-template enable

wlan ap-group hy
vlan 1
ap-model WA4320-ACN-B
  map-configuration cfa0:/MAP-BB.txt
  radio 1
   radio enable
   channel band-width 40
   service-template aaa vlan 501
  radio 2
   rate mandatory 11
   rate supported 12 18 24 36 48 54
   rate disabled 1 2 5.5 6 9
   radio enable
   service-template aaa vlan 501
```

用户在服务模板下配置了基于VLAN的本地转发方式，在AP组下绑定绑定服务模板时，绑定了另外一个VLAN作集中转发，即用户在同一服务模板下同时配置了集中转发和本地转发，起了Portal认证和MAC认证，认证流程为：终端接入后先进行MAC认证，若服务器上查不到终端的MAC表项，则进行Portal认证，Portal认证通过后，设备会记录终端的MAC表项，下次在进行关联时，通过MAC认证后，直接访问网络。

```
%Jan 10 14:24:02:350 2018 IRF-AC STAMGR/5/STAMGR_MACA_LOGIN_FAILURE : -Username=7862566bf643-UserMAC=7862-566b-f643-BSSID=9428-2e97-d6c1-SSID=ABCD-VLANID=501-UsernameFormat=MAC address; A user failed MAC authentication.   //用户MAC
%Jan 10 14:24:02:360 2018 IRF-AC STAMGR/6/STAMGR_CLIENT_ONLINE: Client 7862-566b-f643 went online from BSS 9428-2e97-d6c1 with SSID ABCD on AP tsg-4f-1. State changed to Run. //只有上线信息，没有mac或者Portal认证信息。
<IRF-AC>display wlan client mac-address  7862-566b-f643 //查看用户在线信息
Total number of clients: 1
MAC address    User name  AP name       RID IP address      IPv6 address   VLAN
7862-566b-f643 N/A        tsg-4f-1      2   10.11.3.12                     501

<IRF-AC>display mac-authentication connection user-mac 7862-566b-f643 //查看用户Portal表项
Total connections: 0

<IRF-AC>display portal user all | include 7862-566b-f643 //查看用户MAC表项
<IRF-AC>
```

收集现网的debug信息，发现终端再次连接时，没有进行MAC认证，也没有进行Portal。在设备上查看终端的在线表项，在Portal表项和MAC表项中，均看不到终端的信息。服务器上也显示终端处于离线状态。另外找多个终端来测试，均是没有经过认证便直接访问网络，从这些现象可以看出，在服务模板下开启的Portal认证没有生效，用户访问网络时没有进行Portal认证直接上网。

经分析，当在同一服务模板下同时配置了集中转发和本地转发，并起了Portal认证时，由于实现机制上的限制，Portal认证只对本地转发生效，对集中转发的情况不生效。客户测试时是在集中转发的区域，因此出现了上述现象。将本地转发方式去掉即可。

建议客户合理规划网络，将集中转发和本地转发配置在不同服务模板下，一个服务模板只配置一种转发方式。