ADCampus环境无法弹出web界面经验案例

ADCampus方案 孙兆强 2020-02-29 发表

组网及说明

ADCampus标准三层组网

问题描述

Byod认证通过，无法弹出web页面，pc能ping通DR2000

过程分析

在leaf上查看认证结果，byod账号已经认证通过，已经授权了url

[leaf-1.1]display mac-authentication connection

Total connections: 1

Slot ID: 1

User MAC address: 1458-d0b7-2407

Access interface: GigabitEthernet1/0/1

Username: 1458d0b72407

User access state: Successful

Authentication domain: test

IPv4 address: 192.168.10.3

IPv6 address: FE80::F4C1:6D34:27B5:7165

Initial VLAN: 111

Authorization untagged VLAN: N/A

Authorization tagged VLAN: N/A

Authorization VSI: vsi3501

Authorization ACL ID: 3001

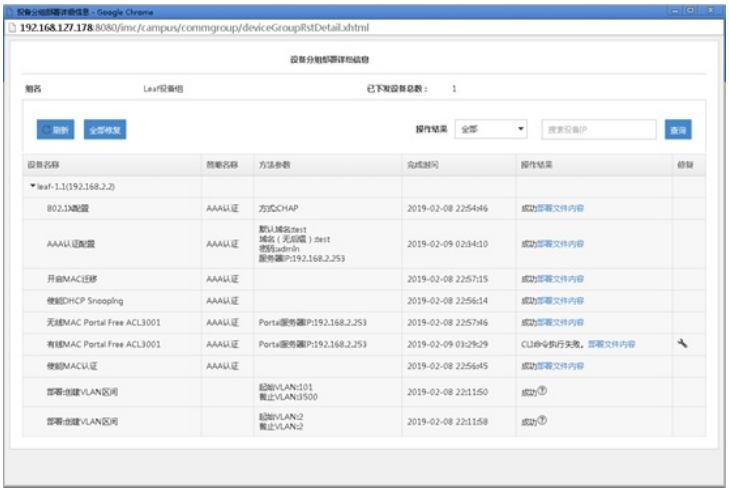
Authorization URL: http://192.168.10.12:8080/portal

Authorization user profile: N/A

Authorization CAR: N/A

在pc的浏览器地址栏查看http没有重定向，抓包看也没有重定向。从pc上ping服务器能ping通。

在leaf上和DR2000上查看配置情况发现同时下发了无线和有线的ACL。



acl advanced 3001

rule 1 permit udp destination-port eq bootps

rule 2 permit udp destination-port eq bootpc

rule 3 permit udp destination-port eq dns

rule 4 permit udp source-port eq dns

rule 5 permit ip destination 192.168.2.253 0

rule 6 permit ip source 192.168.2.253 0

rule 100 deny ip

因为先下发了无线的acl3001导致有线的acl3001下发失败。无线的acl里方通了到服务器的地址所以pc能ping通服务器。但是无线的acl最后有一个rule 100 deny ip过滤了所有流量。所以http流量直接被过滤，授权url无法重定向。

解决方法

DR2000里将无线的acl下发去掉