

知 某局点无线mac认证下发acl后终端无法连接无线

MAC地址认证 姜霁琛 2019-07-23 发表

组网及说明

终端网关在核心交换机

问题描述

现场结合imc做mac认证，通过imc下发acl，需求是要求内网10.0.0.0网段不能互访，只能上外网。在设备上创建acl 3050，通过imc下发acl3050，并放通imc服务器地址、dhcp服务器地址和dns地址，将内网网段10.0.0.0网段deny，配置完成后发现终端无法连上无线

```
# acl advanced 3050
```

```
rule 1 permit ip destination 10.159.0.1 0 //dhcp服务器
rule 2 permit ip destination 10.159.0.2 0 //dns服务器
rule 3 permit ip destination 10.159.0.3 0 //imc服务器
rule 4 permit ip destination 10.159.0.4 0 //imc服务器
rule 10 deny ip destination 10.0.0.0 0.255.255.255 //拒绝内网网段互访
rule 100 permit ip
```

过程分析

由于认证起在AC上，但是终端网关在核心交换机上，现场下发的acl中没有放通网关地址，虽然mac地址认证可以通过，但是下发acl后由于终端无法ping通网关，所以无法接入无线网络

解决方法

让现场在acl中加一条rule放通网关地址后终端可以正常接入无线