无线服务模板下应用包过滤策略不生效经验案例

ACL packet-filter 范书珩 2021-08-20 发表

组网及说明

不涉及

问题描述

无线服务模板下应用包过滤策略，AC上相关配置：

```
wlan service-template 1
ssid lab
vlan 1007
packet-filter 3000 outbound
packet-filter 3000 inbound
service-template enable

acl number 3000
 rule 10 permit ip source 172.22.0.0 0.0.255.255 destination 172.20.40.128 0.0.0.127
 rule 1000 deny ip
```

匹配rule 10的地址可以ping通，其余地址deny。

配置完成后使用终端连接无线，测试依然能ping通不在rule 10放通规则中的ip地址

过程分析

基于无线服务模板的包过滤需要将ACL策略配置在AP上才能生效

解决方法

基于无线服务模板的包过滤需要将ACL规则配置到AP上，不论使用的是集中转发还是本地转发，可以通过map文件下发配置

```
acl number 3000
 rule 10 permit ip source 172.22.0.0 0.0.255.255 destination 172.20.40.128 0.0.0.127
 rule 500 permit udp destination-port eq bootps
 rule 501 permit udp destination-port eq bootpc
 rule 1000 deny ip
```

如果最后一条规则默认为deny，需要额外增加两条规则rule 500、rule501，目的是放通DHCP交互使用的udp端口，否则终端上线无法获取ip地址