某局点WX3520H 基于SSID的包过滤不生效

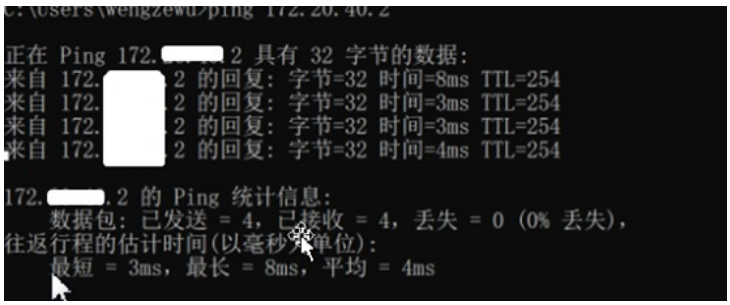
wlan安全 刘文粟 2021-08-12 发表

组网及说明

无

问题描述

在ssid上配置了包过滤没有生效，仍能访问为允许的网段



过程分析

因为所有用户都在同一个vlan上，无法在三层接口上去调用acl，因此想到针对不同的ssid去调用acl来控制访问内网权限；
目前做法是，建了一个wlan service-template 1，绑定了 ssid lab，调用了

```
 packet-filter 3000 outbound
 packet-filter 3000 inbound,
acl:
acl number 3000
 rule 10 permit ip source 172.22.0.0 0.0.255.255 destination 172.x.x.128 0.0.0.127
 rule 20 permit ip source 172.22.0.0 0.0.255.255 destination 172.22.0.1 0
 rule 1000 deny ip


#
wlan service-template 1
ssid lab
vlan 1007
 packet-filter 3000 outbound
packet-filter 3000 inbound
 akm mode psk
preshared-key pass-phrase cipher $c$3$WuKNSAGrx+HWEakzPhkEVorMcQ1Dc7Tb0OMF
cipher-suite ccmp
cipher-suite tkip
security-ie rsn
security-ie wpa
service-template enable
#
```

配置完了不生效，测试源地址172.x.x.4，目的172.x.x.2，仍能访问

```
address                  : xxxx-xxxx-3229
 IPv4 address                : 172.xx.4
IPv6 address                : N/A
Username                    : N/A
AID                       : 1
AP ID                      : 83
AP name                      : xxx
Radio ID                   : 2
Channel                    : 149
SSID                      : lab
BSSID                      : xxxxxxxx-6a60
VLAN ID                    : 1007
Sleep count                : 56
```

解决方法

服务模板下应用包过滤，需要将acl的配置配在ap上，可以通过map文件下发

acl number 3000

rule 10 permit ip source 172.22.0.0 0.0.255.255 destination 172.x.x.128 0.0.0.127

rule 20 permit ip source 172.22.0.0 0.0.255.255 destination 172.x.x.1 0

rule 500 permit udp destination-port eq bootps

rule 501 permit udp destination-port eq bootpc　　如果最后一条规则默认为deny，需要额外增加两条规则，否则终端上线无法获取ip地址

rule 1000 deny ip