

## 知 下发授权ACL成功但是不生效

Portal 田卓 2020-09-22 发表

### 问题描述

结合我司IMC做portal认证, 认证无问题, 但是下发授权ACL一直未生效, 从设备上, 已经是下发成功了, debug来看授权也是下发给了设备。但是一直能ping通172.16.1.1

```
display portal user username 123
```

```
Username: 123
```

```
AP name: 1-3-4
```

```
Radio ID: 1
```

```
SSID: H3C
```

```
Portal server: imc
```

```
State: Online
```

```
VPN instance: N/A
```

```
MAC          IP          VLAN  Interface
1234-5678-aaaa 192.168.1.1 88    WLAN-BSS1/0/12018
```

```
Authorization information:
```

```
DHCP IP pool: N/A
```

```
User profile: N/A
```

```
Session group profile: N/A
```

```
ACL number: 3499 (active)
```

```
Inbound CAR: N/A
```

```
Outbound CAR: N/A
```

部分debug信息如下:

```
*Sep 14 16:50:38:882 2020 H3C RADIUS/7/EVENT:PAM_RADIUS: RADIUS Authorization successfully.
```

```
*Sep 14 16:50:38:882 2020 H3C PORTAL/7/EVENT: User-SM[192.168.1.1]: AAA processed authorization request and returned success.
```

```
*Sep 14 16:50:38:883 2020 H3C PORTAL/7/EVENT: User-SM[ 192.168.1.1 ]: Received session-timeout is 86400 sec.
```

```
*Sep 14 16:50:38:883 2020 H3C PORTAL/7/FSM: User-SM [ 192.168.1.1 ]: State changed from Waiting_Author to Waiting_Rule_OK.
```

```
*Sep 14 16:50:38:884 2020 H3C PORTAL/7/RULE:
```

```
DRV_USER_RULE:
```

```
L2 Interface = WLAN-BSS1/0/12018
```

```
L3 Interface = WLAN-BSS1/0/12018
```

```
VLAN = 88
```

```
SrcIP = 192.168.1.1
```

```
SrcMAC = 1234-5678-aaaa
```

```
AuthorACL = 3499
```

```
Operation = 0
```

```
SetDrvFlag = 1
```

```
TrafficLevelNum = 0
```

```
TrafficLevelMap = 0x0
```

```
TrafficActiOnMap= 0x0
```

```
UserID = 268446310
```

```
vrfIndex = 0
```

```
AcIMismatchAction= 0
```

ACL配置如下:

```
#
```

```
acl advanced 3499
```

```
rule 5 permit tcp destination 172.16.1.1 0 destination-port eq 8080
```

```
rule 10 permit tcp destination 172.16.1.1 0 destination-port eq 8443
```

```
rule 15 permit tcp destination 172.16.1.2 0 destination-port eq 8080
```

```
rule 20 permit tcp destination 172.16.1.2 0 destination-port eq 8443
```

```
rule 55 deny ip destination 172.16.1.1 0
```

```
rule 60 deny ip destination 172.16.1.2 0
```

```
rule 100 permit ip
```

```
#
```

portal-free规则配置如下:

```
#
portal host-check enable
portal packet log enable
portal free-rule 1 destination ip 172.16.1.1 255.255.255.255 tcp 8080
portal free-rule 2 destination ip 172.16.1.1 255.255.255.255 tcp 8443
portal free-rule 6 destination ip any tcp 53
portal free-rule 7 destination ip any udp 53
#
```

#### 解决方法

portal-free里面的规则都是地址+端口, 不存在放通的情况。且测试访问172.16.1.2是无法访问成功的, 说明ACL其实已正常下发给用户  
后经确认因为webserver也是这个地址, 而webserver的地址是直接放行的, 不区分端口号, 所以172.16.1.1直接放行

```
#
portal web-server portal
url http://172.16.1.1:8080/portal
#
```