某局点V7无线控制器802.1X认证通过iMC服务器下发ACL失败的经验案例

802.1X ACL 叶靖 2020-06-29 发表

组网及说明

某局点购买了一台V7无线插卡以实现对无线AP的管理，无线插卡为LSUM1WCMX20RT ，现场设备版本为Version 7.1.064, Release 5426P02。

现场配置了802.1x认证，认证服务器为IMC服务器，IMC作为远程radius服务器，现场想通过IMC服务器给802.1x认证用户下发ACL，以实现对802.1x用户的控制。

问题描述

现场配置完1x认证，并在IMC服务器上下发ACL之后，现场测试发现ACL下发不生效。

现场下发的ACL为ACL 3020:

```
#
acl number 3020
rule 0 permit ip destination 192.168.1.5 0
rule 5 deny ip
#
```

但是终端测试ping不通acl中 3020中的192.168.1.5这个地址，替换其他终端也一样

过程分析

我们查看到现场终端已经成功通过了802.1x认证，已经正常上线。通过查看display wlan client mac-address aaaa-aaaa-aaaa verbose命令结果如下:

```
<AC>dis wlan client mac-address 184f-32a9-975d verbose
Total number of clients: 1

 MAC address                  : 184f-32a9-975d
 IPv4 address                 : 192.172.0.45
 IPv6 address                 : N/A
 Username                     : test
 AID                        : 4
 AP ID                       : 60
 AP name                      : ap1
 Radio ID                     : 2
 SSID                       : inode
 BSSID                       : 74ea-c8a0-cb77
 VLAN ID                      : 700
 Sleep count                  : 71
 Wireless mode                  : 802.11gn
 Channel bandwidth              : 20MHz
 20/40 BSS Coexistence Management  : Not supported
 SM power save                : Disabled
 Short GI for 20MHz             : Supported
 Short GI for 40MHz             : Not supported
 STBC RX capability             : Not supported
 STBC TX capability             : Not supported
 LDPC RX capability             : Not supported
 Block Ack                    : TID 0  Both
                              TID 1  Out
 Supported HT MCS set           : 0, 1, 2, 3, 4, 5, 6, 7
 Supported rates              : 1, 2, 5.5, 6, 9, 11,
                              12, 18, 24, 36, 48, 54 Mbps
 QoS mode                     : WMM
 Listen interval              : 1
 RSSI                       : 35
 Rx/Tx rate                   : 72.2/72.2 Mbps
 Speed                      : 0.000/0.016Kbps
```

Authentication method : Open system
Security mode : RSN
AKM mode : 802.1X
Cipher suite : CCMP
User authentication mode : 802.1X
WPA3 status : Disabled
Authorization CAR : N/A
Authorization ACL ID : 3020//可以看到终端已经成功下发了ACL3020
Authorization user profile : N/A
Roam status : N/A
Key derivation : SHA1
PMF status : N/A
Forwarding policy name : Not configured
Online time : 0days 0hours 40minutes 42seconds
FT status : Inactive

从终端上线信息看，终端已经成功下发了acl 3020。

后续我们在192.168.1.5这个终端上抓包发现，收到了来自测试802.1x终端的ICMP请求，也发出了ICMP的回应报文。

最后我们测试发现，为802.1x用户下发ACL的时候，ACL会对双向的报文都做限制。所以在之前的ACL 3020中，我们只放通了802.1x用户到192.168.1.5的报文，但是没有放通192.168.1.5的回包。也就是说，需要修改ACL3020放通双向的报文。

解决方法

为802.1x用户下发ACL的时候，ACL会对双向的报文都做限制。所以我们可以通过修改ACL放通双向的报文即可。

修改ACL3020如下：
#
acl number 3020
rule 0 permit ip destination 192.168.1.5 0//放通802.1x终端到192.168.1.5
rule 5 permit ip source 192.168.1.5 0//放通192.168.1.5到802.1x终端
rule 10 deny ip
#
修改ACL放通双向报文之后测试正常。