

# 知 iMC-EIA进行Portal无感知时WEB页面提示“设备拒绝请求”的处理方法

Portal 罗孝晨 2016-06-05 发表

某局点使用iMC-EIA组件配合我司WX5540E设备进行Portal无感知认证，用户终端页面输入完成用户名和密码之后提示“设备拒绝请求”，但是iMC侧能看到在线用户问题。

设备拒绝请求



一、根据故障现象及截图，首先收集UAM和Portal调试级别日志。分析Portal调试日志，如下图所示  
2016-06-05 20:52:59.767[Portal服务器][调试(0)][24][ProxyResponseDeviceHandler::run]172.17.0.3 ; REQ\_AUTH(3) ; 74 ; 10.0.0.13:2000 ; 报文处理成功

```
Packet Type:REQ_AUTH(3)
SerialNo:74
Address:10.0.0.11
Port:50300
Remotep:10.0.0.13
RemotePort:2000
Version:portal 2.0
Auth Type:CHAP
ErrorID:0
UserIP:172.17.0.3
UserPort:0
ReqID:72
Rsvd:0
attriNum:4
```

```
User Name:access1
Challenge Password:***
Challenge Type:CHAP
Device Ip:10.0.0.13
```

2016-06-05 20:52:59.767[Portal服务器][调试(0)][23][TimerSendTask::run]packet insert into response DeviceQueue, send count = 1

2016-06-05 20:52:59.774[Portal服务器][调试(0)][21][ProxyRequestHandler::run]172.17.0.3 ; ACK\_AUTH(4) ; 74 ; 10.0.0.13:2000 ; 设备拒绝请求(1)

```
Packet Type:ACK_AUTH(4)
SerialNo:74
Address:10.0.0.11
Port:50908
Remotep:10.0.0.13
RemotePort:2000
Version:portal 2.0
```

Auth Type:CHAP  
ErrorID:1  
UserIP:172.17.0.3  
UserPort:0  
ReqID:72  
Rsvd:0  
attriNum:3

Device Ip:10.0.0.13  
Session Id:14 f6 5a d5 63 cd  
Device Time Stamp:1465152328

发现在设备回应给iMC服务器的ACK\_AUTH报文里携带了ErrorID:1的错误值，由于该值的存在，才会导致WEB页面提示“设备拒绝请求”。在ACK\_AUTH和REQ\_AUTH之间，设备和iMC服务器之间传递的是RADIUS报文，所以此时需要分析UAM调试日志。

## 二、查看UAM调试日志

```
% 2016-06-05 20:52:59.769 ; [L_DEBUG (4)] ; [7908] ; LAN ; access1 ; 1 ;  
b01b284a8e054ca09cc57d4d2c5a74f1 ; (NULL) ; Received message from 10.0.0.13:  
CODE = 1.  
ID = 72.  
ATTRIBUTES:  
  User-Name(1) = "...access1"\\用户名: access1  
  CHAP-Password(3) = "48f90db839a15ae015450e54a5d255506e".  
  CHAP-Challenge(60) = "6313c57d42f2254976ab77a1eae307f3".  
  NAS-IP-Address(4) = 167772173.\\设备ip: 10.0.0.13  
  NAS-Identifier(32) = "AC".  
  NAS-Port(5) = 16793900.  
  NAS-Port-Id(87) = "0100004000000300".  
  NAS-Port-Type(61) = 19.  
  Service-Type(6) = 2.  
  Framed-Protocol(7) = 255.  
  Calling-Station-Id(31) = "14-F6-5A-D5-63-CD"\\用户MAC地址  
  Called-Station-Id(30) = "38-97-D6-25-2B-20;portal-mac"\\设备MAC地址  
  Acct-Session-Id(44) = "11606052052070ff17c649".  
  Framed-IP-Address(8) = 2886795267.\\用户IP: 172.17.0.3  
  hw_Connect_ID(26) = 80.\\此值用来表示连接id, 每次认证该值唯一  
  hw_Product_ID(255) = "H3C WX3510E".  
  hw_IP_Host_Addr(60) = "172.17.0.3 14:f6:5a:d5:63:cd".  
  hw_Nas_Startup_Timestamp(59) = 1465152323.  
% 2016-06-05 20:52:59.769 ; [L_DEBUG (4)] ; [7908] ; radDispatcher ; ; (NULL) ; (NULL) ; (NULL) ; p  
rsRawPkt: chk-sum 1912785739.  
% 2016-06-05 20:52:59.770 ; [L_DEBUG (4)] ; [7908] ; LAN ; ; (NULL) ; (NULL) ; (NULL) ;  
Code = 2  
ID = 72  
ATTRIBUTES:  
  User-Name(1) = access1\\用户名access1  
  Service_Type(6) = 2  
  State(24) = BLJh8TFk  
  Class(25) = BLJh8TFk  
  Termination-Action(29) = 0  
  Filter_Id(11) = 3000\\隔离ACL, 由RADIUS 2号报文下发给设备  
  hw-Input-Peak-Rate(1) = 2560000  
  hw-Input-Average-Rate(2) = 512000  
  hw-Input-Basic-Rate(3) = 512000  
  hw-Output-Peak-Rate(4) = 1536000  
  hw-Output-Average-Rate(5) = 307200  
  hw-Output-Basic-Rate(6) = 307200  
  Session-Timeout(27) = 86400\\会话时长86400s  
  Acct-Interim-Interval(85) = 600\\计费更新间隔600s  
  hw-Connect-Id(26) = 80\\此值与刚才code=1中的connect id相同  
  hw_User_Notify(61) =  
  IF_PROXY = 0
```

```
IF_DOUBLE_NETCARD = 0
IF_IE_PROXY = 0
FRAMED_IP_SET_MODE = 0
IF_CHECK_MODIFY_MAC = 0
IF_CHECK_SAME_MAC = 0
EIA_DETAIL_VERSION = V700R003B04D009
EAD_EVENT_SEQ_ID = BLJh8TFk
```

通过UAM日志，我们能够看出在iMC已经给设备侧回应了认证成功报文，而对于7.2版本的EIA组件，只要iMC回应了认证成功报文，就会创建在线用户，这也就解释了为什么WEB页面上虽然提示了“设备拒绝请求”，但是服务器上仍然有在线用户。

刚刚在Portal日志中已经分析了ACK\_AUTH中携带了ERROR ID=1的值，按照之前处理此类问题的经验，应该是iMC给设备回应的报文中携带了特殊的报文内容，而此内容没有被设备所解析出来，从而导致设备回应的报文中携带错误值。在UAM调试日志中，我们看到有这样一条报文Filter\_Id(11) = 3000。这条报文是隔离ACL报文，是iMC服务器通过认证接受2号报文下发给接入设备的。而根据现场设备上的配置，发现并没有此条ACL配置。所以导致iMC下发的报文设备无法解析。

通过iMC服务器上的抓包更加验证了我们的推测，抓包如下图所示：

```
694 2016-06-05 20:52:59.76254000 10.0.0.13 10.0.0.11 RADIUS 303 Access-Request(1) (Id=11, L=253)
695 2016-06-05 20:52:59.76925000 10.0.0.11 10.0.0.13 RADIUS 279 Access-Accept(2) (Id=72, L=279)
710 2016-06-05 20:53:01.32163000 10.0.0.13 10.0.0.11 RADIUS 303 Access-Request(1) (Id=73, L=261)
711 2016-06-05 20:53:01.32693000 10.0.0.11 10.0.0.13 RADIUS 249 Access-Accept(2) (Id=74, L=239)

# User Datagram Protocol, Src Port: radius (1812), Dst Port: 4204 (4204)
# Radius Protocol
Code: Access-Accept (2)
Packet Identifier: 0x48 (72)
Length: 237
Authenticator: 8540ec28690c3bc8d584f22edc1908c
[This is a response to a request in frame 694]
[Time from request: 0.002741000 seconds]
# Attribute Value Pairs
# AVP: 1=12 t=User-Name(1): \025\002\021access1
# AVP: 1=4 t=Service-Type(0): Framed(3)
# AVP: 1=10 t=State(24): 424ca683854466b
# AVP: 1=10 t=Class(25): 424ca683854466b
# AVP: 1=6 t=Termination-Action(29): Default(0)
# AVP: 1=6 t=Filter-Id(11): 3000
# AVP: 1=12 t=vendor-specific(26) v=Huawei(2011)
# AVP: 1=12 t=vendor-specific(26) v=Huawei(2011)
# AVP: 1=12 t=vendor-specific(26) v=Huawei(2011)
```

- 1、若在iMC的接入策略管理里配置了ACL，则必须要保证此条ACL和设备侧配置保持一致
- 2、处理此类问题，我们需要学会分析UAM和Portal调试日志，必要时结合服务器抓包和设备DEBUG信息同步进行分析。