某局点IMC漫游中继对接第三方服务器时终端802.1x认证失败

802.1X AAA 王媛媛 2017-12-25 发表

某局点反馈，采用IMC漫游中继对接第三方服务器组网时，终端进行802.1x认证失败。该局点组网比较特殊，Client ----AC---IMC服务器(Radius漫游中继)—Radius第三方认证服务器。IMC服务器 只做Radius漫游中继，Radius的认证实际由第三方的服务器来完成。整个认证流程为：AC 只与IMC服务器进行Radius通信， IMC接收到AC 发送的Radius报文后再转送给第三方服务器。同样，IMC也将第三方服务器返回的认证报文转送给AC。
AC 上配置的Radius服务器的地址是IMC的IP地址。对于AC 来说是感知不到第三方服务器的存在的。
radius scheme 1x
 primary authentication 10.160.5.18 //IMC服务器的地址
 primary accounting 10.160.5.18 //IMC服务器的地址
但是在整个认证过程中，IMC只扮演中继的角色，并不对Radius的报文做实质性的处理。
现场进行802.1x认证测试时发现终端无法接入网络。服务器上看到的信息就是终端在认证成功被AC 强制下线。Inode客户端显示用户认证成功之后依旧无法接入。

无

首先需要确认AC 上的802.1x认证的配置没有问题。建议现场测试AC分别和IMC、第三方服务器直接对接，不采用漫游中继的组网时，对接是可以成功的，说明AC 上的基本配置没有问题。
在AC 上进行Debug，收集802.1x认证过程的交互过程信息可以看到：
*Dec 4 08:52:30:237 2017 AC-A1 RADIUS/7/PACKET:
    MS-MPPE-Receive-Key=******
    MS-MPPE-Send-Key=******
    EAP-Message=0x030a0004
    Message-Authenticator=0x33e1af6b24dbe0ec11800a53af3ef07e
    User-Name="320227196901230438"
*Dec 4 08:52:30:237 2017 AC-A1 RADIUS/7/PACKET:
 02 79 00 b4 31 ee 27 85 39 62 09 26 20 16 88 90
 39 a0 e6 91 1a 3a 00 00 01 37 11 34 90 87 3f 74
 1c 33 a9 ff 14 37 7d 9e e4 af 18 90 67 f1 74 26
 ba 9d 00 ed 25 78 c4 98 93 96 e8 38 ca f4 5e 02
 44 01 ec f9 95 cd 9c 00 02 82 e5 89 7e eb 1a 3a
 00 00 01 37 10 34 98 67 04 c8 86 01 f4 81 ba 4a
 bb c2 5f e4 3d 09 32 18 f5 fd c3 42 55 bd 9e b2
 39 13 0c 11 21 9f 7c b6 fb 3d 7f 6f 76 56 cd b0
 33 b8 9c 2a e9 68 22 02 4f 06 03 0a 00 04 50 12
 33 e1 af 6b 24 db e0 ec 11 80 0a 53 af 3e f0 7e
 01 14 33 32 30 32 32 37 31 39 36 39 30 31 32 33
 30 34 33 38
*Dec 4 11:44:04:863 2017 AC-A1 STAMGR/7/Event: [MAC: b88a-608c-66c1, BSSID: 60da-83a3-e0c1]Received authorization information, VLAN 16.
    *Dec 4 11:44:04:864 2017 AC-A1 STAMGR/7/Event: [MAC: b88a-608c-66c1, BSSID: 60da-83a3-e0c1]Started processing L2 authentication: Result=0, Authentication status=1.
    *Dec 4 11:44:04:864 2017 AC-A1 STAMGR/7/Error: [MAC: b88a-608c-66c1, BSSID: 60da-83a3-e0c1]Invalid sent session key length 39 or invalid received session key length 129.
    *Dec 4 11:44:04:864 2017 AC-A1 STAMGR/7/Event: [MAC: b88a-608c-66c1, BSSID: 60da-83a3-e0c1]Finished user authentication: Result=failed with reasoncode 23.
此处报错表示Dot1x客户端接入时，设备端使用秘钥解密后，Receive key/ Send Key的长度不符合无线Dot1x客户端的预期。
分析：AC 显示用秘钥解析出来的报文Session key（Receive key/ Send Key）的长度不合法。Session-key由IMC 侧配置的秘钥衍生。AC 和IMC 通信时，有一个AC 和IMC之间通信所用的Session-key1。而IMC和第三方服务器通信时，有一个IMC和和第三方服务器通信所用的Session-key2。而IMC 在做Radius漫游中继时只是简单地将Radius报文（包括Session-key）原封不动的转送，不做任何处理。如果两个Session-key不一致，就会出现AC 用和IMC通信的Session-key1去解析第三方服务器返回的用Session-key2加密的报文，导致解析结果出错，报文不合法，所以Radius认证失败。

修改IMC侧的秘钥配置。将IMC上AC 和第三方服务器对接的秘钥修改一致，同时也将AC 上配置的秘钥修改得与IMC上的一致。
radius scheme 1x
    key authentication simple 123

key accounting simple 123
修改相关配置后，终端测试802.1x认证成功。

1. IMC漫游中继对接第三方服务器的组网比较少见。如果采用这种特殊组网时，可以先进行常规组网的对接，确保配置无问题，明确问题出在组网的特殊性上。
2. 终端认证失败时，需要在AC 上进行Debug，结合服务器抓包，明确终端认证失败的原因，再给出相应的解决方案。