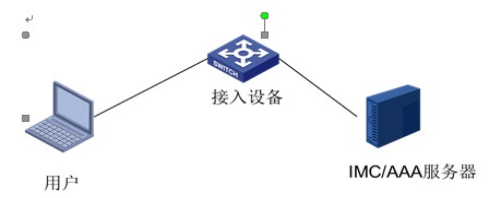
S5800与IMC配合做portal认证下发ACL失败

Portal ACL 孔天娇 2014-07-28 发表

S5800与IMC配合做portal认证下发ACL失败

一、 组网：



二、 问题描述：

代理商反馈使用UAM规则给设备下发acl，终端认证成功之后访问网页时还会再次弹出认证界面，去掉下发acl后就正常了。

三、 过程分析：

收集下发失败时的debug radius信息，发现提示ACL_FAILURE: The input parameters are wrong，但[11 Filter-ID] [6] [33303030]字段正确，IMC上配置下发的ACL为3000。

*May 28 04:18:08:536 2014 L1-Aggregation-First-EAST RDS/7/DEBUG: Receive:IP=[172.17.111.35],Code=[2],Length=[150]
*May 28 04:18:08:536 2014 L1-Aggregation-First-EAST RDS/7/DEBUG:
[1 User-name] [13] [test@portal]
[6 Service-Type] [6] [2]
[24 State] [10] [50344631664D5A54]
[29 Termination-Action] [6] [0]
[11 Filter-ID] [6] [33303030]
[27 Session-TimeOut] [6] [86401]
*May 28 04:18:08:537 2014 L1-Aggregation-First-EAST RDS/7/DEBUG:
[85 Acct_Interim_Interval] [6] [600]
[H3C-26 Connect_ID] [6] [3932161]
[H3C-61 Server_String] [59] []
*May 28 04:18:08:537 2014 L1-Aggregation-First-EAST RDS/7/DEBUG: Acl-Group = 3000, Inter-Group=
%May 28 04:18:08:541 2014 L1-Aggregation-First-EAST PORTAL/5/PORTAL_ACL_FAILURE: The input parameters are wrong.

进而查看ACL的配置如下：

acl number 3000
rule 0 deny ip source 10.200.0.0 0.0.255.255 destination 10.2.5.0 0.0.0.255
rule 1 permit ip

ACL的编号没有问题，为3000，但rule 0中包含了对源IP的匹配。

设备在结合IMC给认证成功的用户下发ACL时，会对ACL的内容进行检查，当前实现机制无法匹配源IP，配置了源IP会导致设备无法识别此ACL。

ACL规则中是否匹配源IP对没有任何影响，因该ACL针对认证成功的用户下发，限制其认证成功后对某些特定网段的访问，匹配目的网段即可。

四、 解决方法：

去掉匹配源IP的配置，更改配置如下：

rule 0 deny ip destination 10.2.5.0 0.0.0.255
rule 1 permit ip