H3C iMC EIA组件对接深信服SG设备

王奕超 2018-03-19 发表

客户当前部署环境下已经购买了我司的IMC平台以及EIA组件并配有服务器，另外也同时购买了深信服的SG设备，当前需求是客户希望首先通过EIA组件对接入用户进行身份认证，在认证结束后将用户在线情况从IMC平台中同步到深信服的SG设备上。

深信服设备与我司IMC服务器都与交换机直连，网络可达
版本：

智能管理平台	iMC PLAT 7.3 (E0506)
终端智能接入管理	iMC EIA 7.3 (E0508)

深信服SG测

第一步：首先需要在深信服测配置单点登录。
操作步骤：用户与策略管理->用户认证->认证选项->单点登陆选项->第三方设备，勾选H3C IMC并配置IMC服务器地址，点击提交即可。
如下图所示：

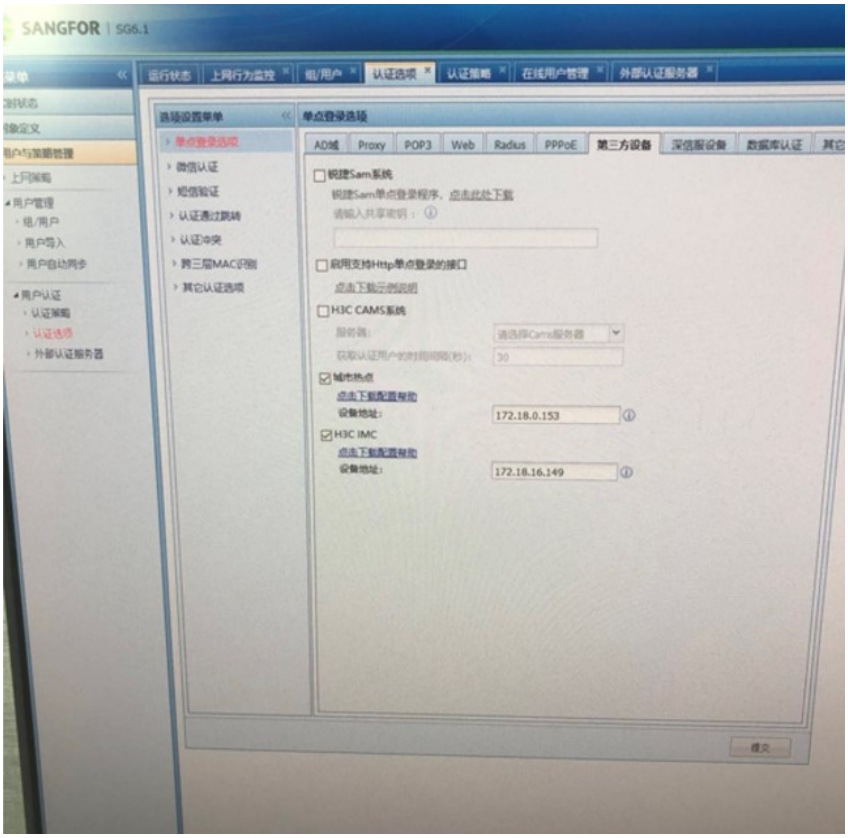

图1

第二步：在深信服设备上配置认证策略，如下图所示：
操作步骤：用户与策略管理->用户认证->认证策略->新增，点击提交即可。
如下图所示：（适用范围中填入需要单点登录的业务地址范围，其余不用改动）

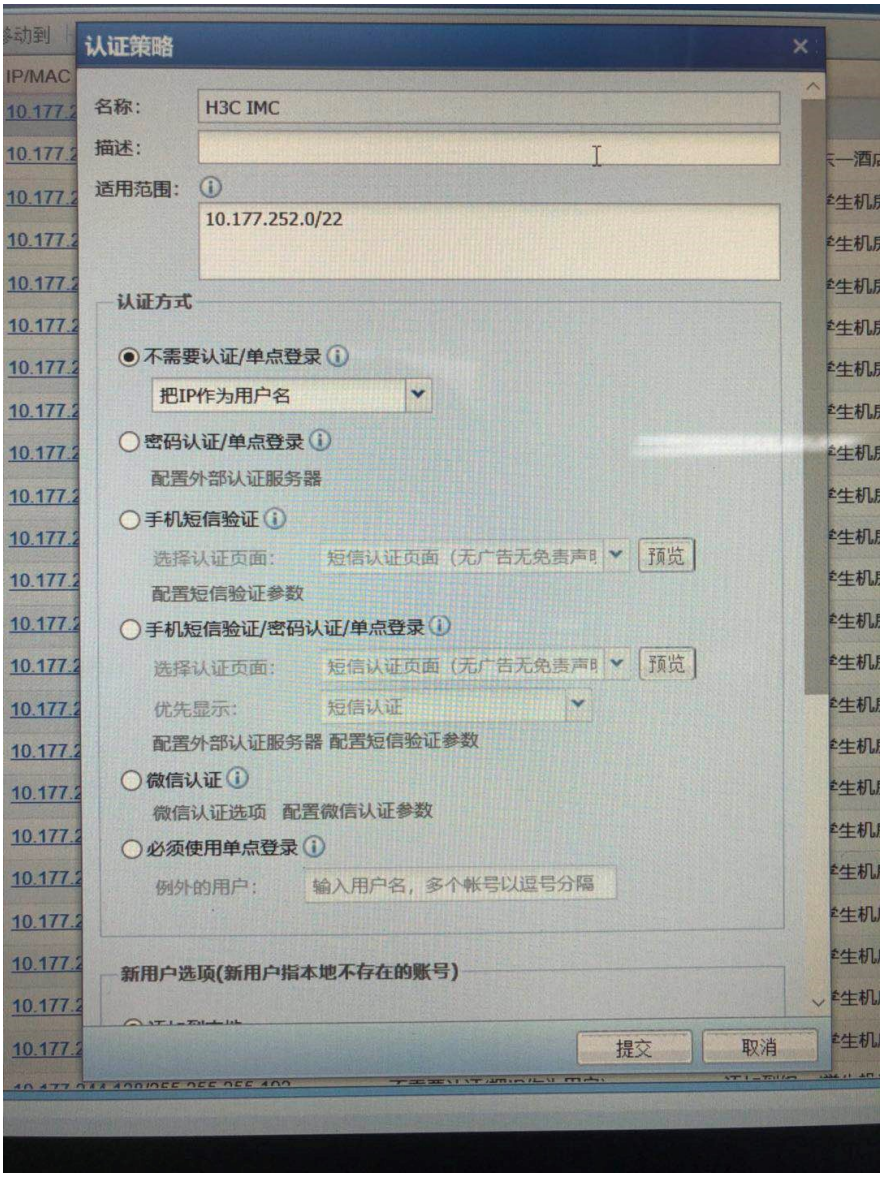

图2

第三步：在深信服设备上配置认证策略，如下图所示：
操作步骤：用户与策略管理->用户认证->认证选项->单点登录选项->AD域，勾选“启用域单点登录”和“通过域自动下发”，并在下面输入共享秘钥（自己配置一个即可，后面要用到）
如下图所示：（适用范围中填入需要单点登录的业务地址范围，其余不用改动）

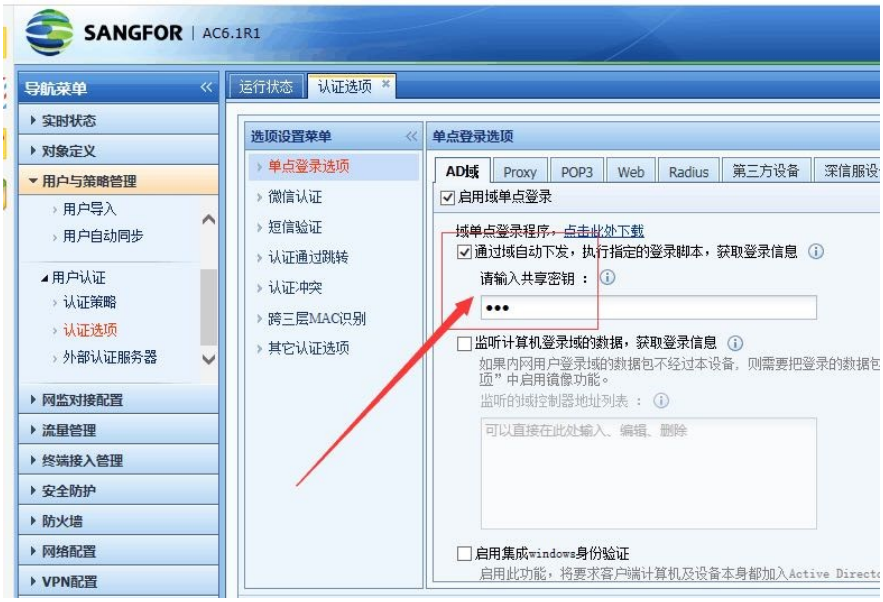

图3

第4步：在“用户与策略管理”中选择“上网策略”，并将图2添加到本地对应的组添加到“适用用户”中。

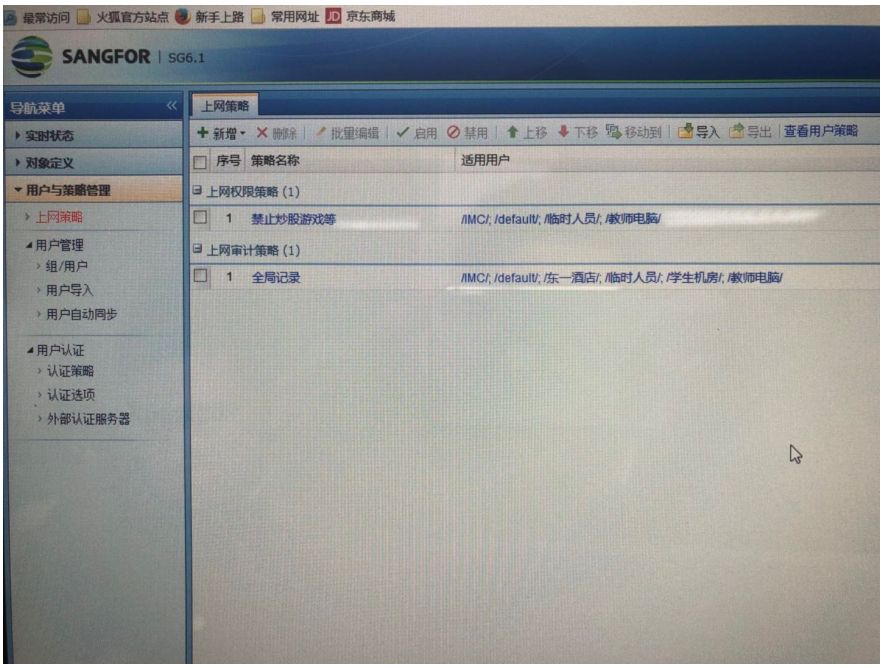

图4

iMC测

在配置完深信服的SG设备后，在我司H3C IMC平台上作如下操作：

操作步骤：用户->接入策略管理->业务参数配置->系统配置->用户通知参数配置->修改用户通知

选择私有报文，配置好深信服SG设备的IP地址和UDP端口号（默认为61442），这里输入之前在SG上配置好的共享秘钥，点击下方保存。

如下图所示：

图5

（1） 配置第三方接收用户上下线通知报文的服务器IP。

（2） 配置第三方接收用户上下线通知报文服务器端口，和第三方服务器规定的端口一致即可。

（3） 配置第三方接收用户上下线通知报文的服务器的共享密钥，和第三方服务器规定的一致即可。

此时登陆SG设备“实时状态，在线用户”，就能看到结果了：

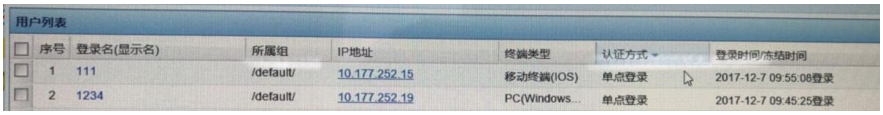

图6

实现原理

上下线通知报文通知报文格式为Radius协议格式的私有报文，上线报文通过Radius code[252]发送，下线报文通过Radius code[253]发送，通知报文内容如下：

1号属性：用户登录帐号名

2号属性：用户姓名

3号属性：用户上线、下线时间（上线通知报文是上线时间，下线通知报文是下线时间）

8号属性：用户IP地址

31号属性：用户MAC地址

iMC UAM/EIA发送用户上线报文的时间：EIA V7之前版本只要收到设备侧的计费开始报文就发给第三方系统，EIA V7（包含V7）及之后版本，收到设备侧的计费开始报文后先判断有没有用户的IP地址，如果有，则立即发送，如果没有，则等第一个计费更新报文再发用户上线报文。

注意事项

（1） 需求不同，第三方系统需提取的数值可能不同，而iMC UAM/EIA侧的用户上下线报文属性都是接入设备上传的，所以在评估需求的时候一定要评估认证方式。比如：如果第三方系统需要提取认证用户的MAC地址，那么就不能使用三层网页Portal认证，因为三层网页Portal认证场景，设备侧无法携带终端的MAC地址，而如果需要提取认证用户的IP地址，则必须要求接入设备携带终端的IP地址。

（2） iMC UAM/EIA通过UDP报文发送用户上下线报文，如果中间有防火墙设备，请放通报文。