SecCenter与iMC配合对ACG基于用户组下发策略的典型配置

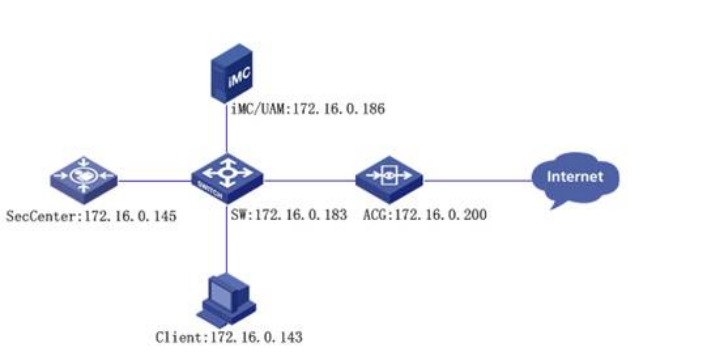
Seccenter A1000 刘思 2014-08-20 发表

SecCenter与iMC配合对ACG基于用户组下发策略的典型配置

一、 组网需求

ACG设备可以基于IP地址组做带宽策略。但在实际组网应用中，客户可能会有针对不同认证用户来给ACG配置不同带宽策略的需求。实现该需求可以通过SecCenter、iMC和ACG进行联动实现。主要原理为SecCenter定时向iMC获取相关用户名对应的IP地址信息，然后针对获取到的IP信息想ACG下发预先配置好的带宽策略。

二、 组网图



三、 功能简介

该功能主要实现原理为：

1）seccenter上创建一用户组，iMC将用户上下线信息通过radius报文发送给seccenter，报文中包含一用户组属性，该用户组名称必须与seccenter上配置的用户组名称一致。

2）seccenter以该用户组名称为基础，给ACG设备推送8个IP地址组。

3）seccenter在接收到由iMC　EIA发送给某一用户组的用户名之后，定期向EIA获取该用户名对应的IP地址。

4）seccenter将获取到IP地址推送到ACG的地址组。

5）seccenter将带宽策略推送ACG，并调用前期已经下发给ACG的地址组信息。

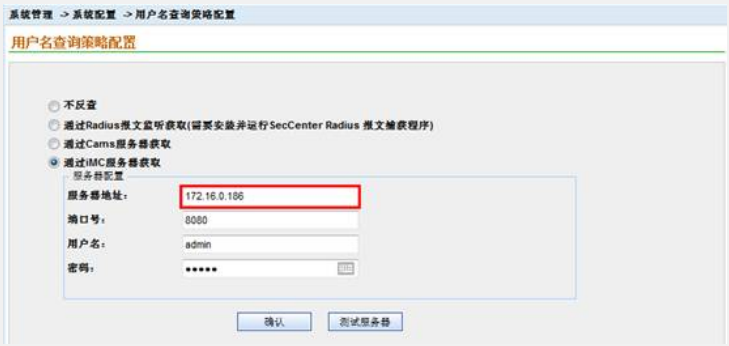
四、　　配置步骤

1、SecCenter上添加用户组以及用户名。

在SecCenter　web页面依次点击带宽策略》资源管理》用户组管理》添加用户组，并在添加的用户组中添加用户名，见下图：

2、配置SecCenter用户名查询策略

在SecCenter web界面依次打开系统管理 》 系统配置 》用户名查询策略配置，做如下截图中配置：



3、在SecCenter配置用户自动同步用户组IP的间隔时间，时间间隔默认为60s，用户可根据需要自行调节，见下图：

4、在iMC配置用户上下线通知策略

依次在iMC web页面点击业务 >> 用户接入管理 >> 业务参数配置 >> 系统配置 >> 用户上下线通知参数配置，其中服务器ip为SecCenter服务器ip，端口号为1812，密钥任意，见下图：

5、在iMC接入策略中配置需要下发的用户组名称

依次在iMC web页面点击业务 >> 用户接入管理 >> 接入规则管理 >> 修改接入规则，见下图：

6、在SecCenter中根据用户需求添加带宽策略，本例中要求当用户test1认证通过时，SecCenter自动向ACG下发阻断策略，阻止该用户访问internet。

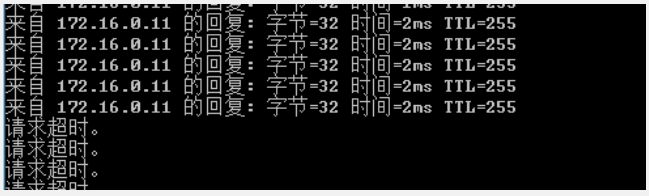
7、在SecCenter中配置带宽策略policy1下发到ACG设备，策略应用选择生效，具体配置见下图：

8、在ACG设备查看相关段策略，可见段策略已经成功下发，见下图：

9、在ACG查看ip地址组信息，可见SecCenter已经向ACG下发了8个ip地址组。由于目前暂无用户认证上线，所以ip地址组中暂无ip地址信息，见下图：

10、PC客户端通过用户名test1进行认证上线测试，从iMC所有在线用户中可查询到该用户在线信息，见下图：

PC客户端进行连续ping测试，可见上线后不久出现ping失败的现象，见下图：



在ACG设备查看ip地址组信息，可见相关ACG已经获取相关ip地址信息，阻断策略在ACG上生效，见下图：

五、 配置关键点

1、如果客户端认证协议为802.1x且网卡已经提前配置好IP地址，则必须使用inode进行认证且须做如下截图配置：

2、SecCenter中系统管理》系统配置》用户名查询策略处iMC服务器ip地址必须为iMC平台所在服务器ip地址，与UAM组件是否分布式部署无关。

3、SecCenter向ACG下发带宽策略时主要通过http或者https方式进行下发，所以须保证SecCenter与ACG设备之间http或https协议可达并正确配置了相关的访问参数。

4、MAC地址认证方式客户端无法向iMC/UAM服务器端上送自身ip地址，所以原理上无法实现本文档中描述的功能。