403 Forbidden
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告
本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告

ACG1000实现对邮件内容审计配置举例

目录

1 配置需求或说明

1.1 适用的产品系列

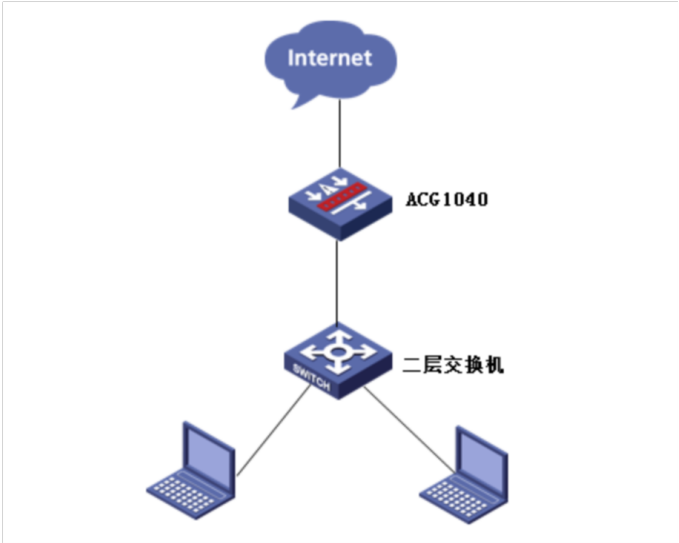
本案例适用于软件平台为ACG1000系列应用控制网关：ACG10X0、ACG1000-AKXXX等。

注：本案例是在ACG1040的Version 1.10, Release 6611版本上进行配置和验证的。

1.2 配置需求及实现的效果

用户网络中部署ACG1040应用审计，目前需要监控员工在上班时间是否发送违规邮件并对邮件内容进行记录，其中192.168.1.100、192.168.1.101为总裁电脑不做审计；

2 组网图



3 配置步骤

3.1 登录设备管理界面

设备管理口（ge0）的默认地址配置为192.168.1.1/24。默认允许对该接口进行PING，HTTPS操作。将终端与设备ge0端口互联，在终端打开浏览器输入https://192.168.1.1登录设备管理界面。默认用户名与密码均为admin。

3.2 检查设备应用识别特征库

#在“监控统计”>“设备信息”中检查应用识别特征库是否已经更换至最新版本，使用旧版本应用识别特征库可能导致应用识别效果差。

3.3 配置内网用户限制范围

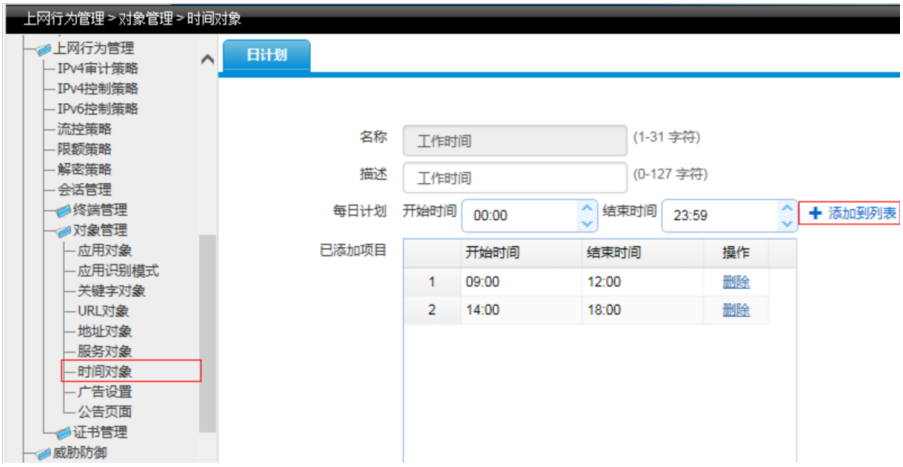
#在“上网行为管理”>“对象管理”>“地址对象”中新建IPV4地

址对象。

#名称设置为为“员工网络”、地址项目选择子网地址并配置192.168.1.0/24，设置完成后一定要点击添加到列表才能添加成功，排除地址中可以将不需要做控制的终端192.168.1.100、192.168.1.101排除；

3.4 配置时间策略

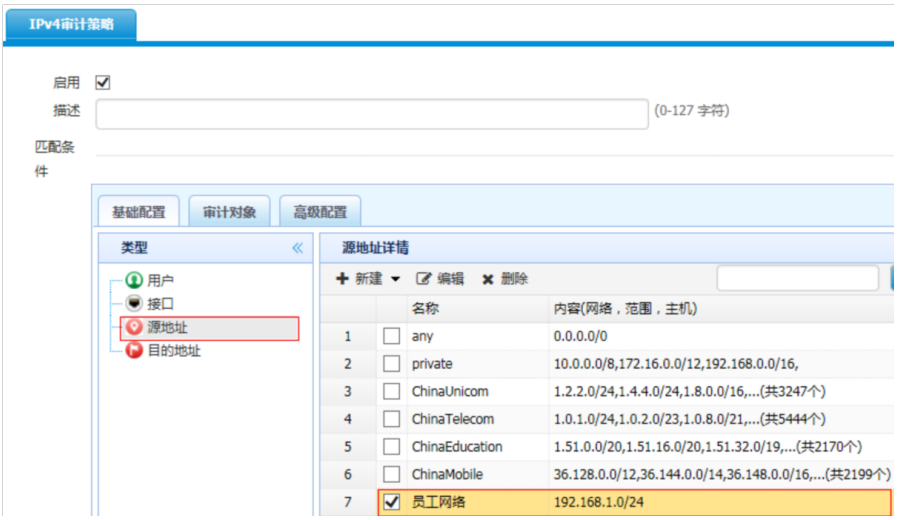
#在“上网行为管理”>“对象管理”>“时间对象”中新建时间对象，创建日计划9:00-12:00和14:00-18:00的时间管理计划；



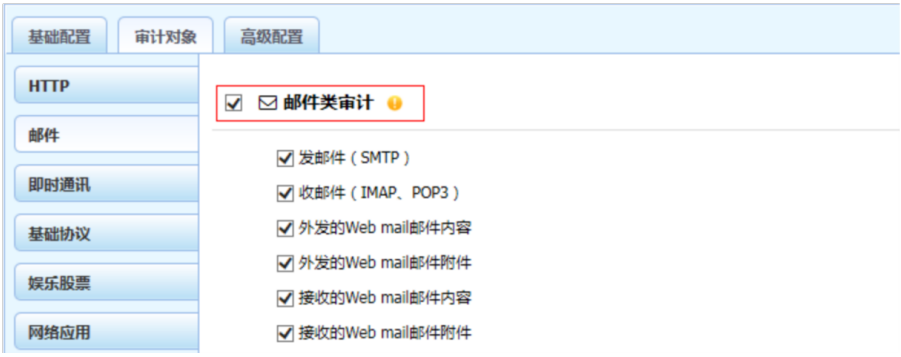
3.5 配置上网行为管理

#在“上网行为管理”>“IPV4审计策略”中选择新建。

#策略需要为启用状态、匹配条件选择源地址中的员工网络。

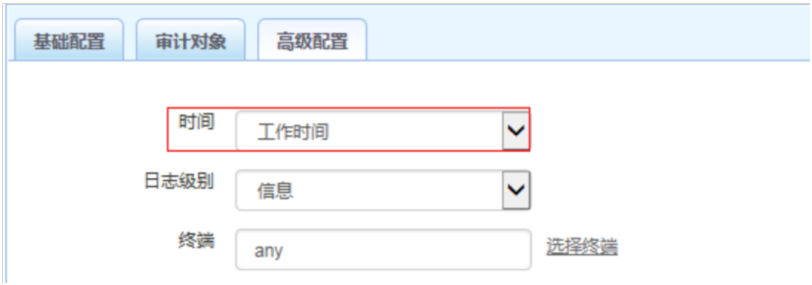


#在“审计对象”中勾选对邮件类审计。



#在“即时通信”中勾选即时通信类审计。

#在高级配置中选择时间为工作时间。



3.6 配置HTTPS解密策略

#在“网络管理”>“DNS服务”中创建DNS服务用于ACG1000设备域名解析。

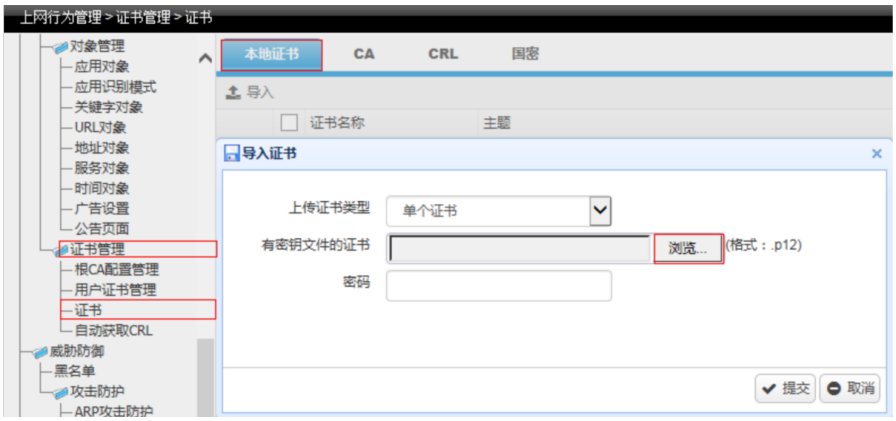
#在“上网行为管理”> “对象管理”>“URL对象”>“HTTPS对象”中新建策略，域名分类选择所有；

#在“上网行为管理”> “证书管理”> “根CA配置管理”中生成

CA根证书。

#将已经生成的证书以PKCS12格式导出至电脑保存。

#在“上网行为管理”>“证书管理”>“证书”中将导出的证书文件上传至本地证书中，密码根据生成证书时有无加密配置，如生成证书时没有加密则此处密码可以为空。



#在“系统管理”>“管理设定”中间HTTPS端口修改为1443端口，因为HTTPS界面端口为443端口与HTTPS登录界面端口冲突。

#配置完成后设备管理界面卡死，需要重新使用https://192.168.1.1:1443登录WEB界面配置。

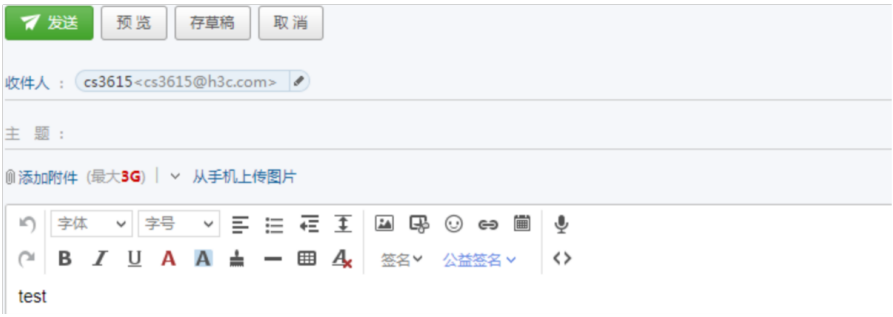
#在“上网行为管理”>“解密策略”在证书列表中选择生成的证书并新建解密策略。

3.7 配置保存

#在设备管理界面右上角点击配置保存，保存当前配置。

3.8 上网行为策略验证

#终端发送邮件测试



#在终端已经可以监控到邮件记录：

点击插卡内容后可以看到邮件发送时间及内容等信息。

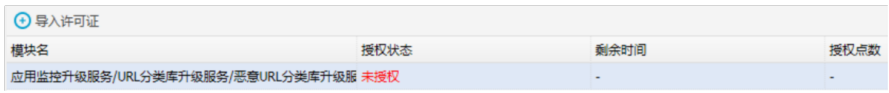
3.9 注意事项

1、 邮件审计中只能审计到发送邮件的内容，收邮件内容在云端因

此无法审计。

2、 应用审计功能需要购买特征库激活文件并激活后才能使用，如果特征库授权未激活或者特征库授权过期则无法保证应用审计功能正常使用。

#在“系统管理”>“授权管理”中可查看授权是否为已授权状态。



注：出现上图中“未授权”字样则表示没有授权，无法使用应用识别功能。