

外发文件告警的使用

本文介绍 AC1.96 能够根据文件的特征来识别一个文件的真实类型，对某些敏感的真实文件类型进行审计以及告警。基于特征的文件识别：存心泄密者通常通过 HTTP、FTP、Email 附件外发文件时会篡改、删除扩展名，压缩、加密再外发，AC 能识别并且报警；尝试解压压缩包后再识别文件类型，防止泄密。下面介绍详细的配置。

一. 外发文件告警的基本设置步骤：

首先，新建上网策略对象或者编辑已有的策略；

然后，在应用审计选项里开启[审计网页上传文件]、[审计邮件发送文件]和[审计 FTP 上传文件]；接着在外发文件告警添加需告警审计的文件类型；

最后，关联策略到用户或者用户组。（若用户或者组同时关联多条策略，并只有一条策略启用了外发文件告警，那么该策略没有位置先后要求；若用户或者组所关联多条策略里都启用了外发文件告警，那么会以第一条启用外发文件告警的策略为准，下面其他策略的外发文件告警规则都不会再匹配）

注意：

1.[外发文件告警]默认情况不可用，需要时可联系市场购买该授权，然后通过多功能序列号激活。

2.要启用[外发文件告警]功能，必须要开启[审计网页上传文件]、[审计邮件发送文件]和[审计 FTP 上传文件]。且只对 FTP、HTTP、SMTP 上传的文件进行检测告警。

3.对不需要告警的压缩包进行解压扫描其内部是否有审计告警文件，而且限制只扫描内部的 100 个文件，邮件告警时告警第一个需要邮件告警的信息，记录日志时，记录下最多一个文件的详细清单。设备只对小于 2M 的文件进行解压缩。

4.对 email 方式外发的文件，如果是 eml 格式的文件能够提取附件进行审计并告警。

5.有特征识别和加密识别的类型，在设置时是可以看到的，并且是文件本身进行加密。如果是第三方软件进行加密的话，设备识别不了类型。

6.告警文件类型中自定义类型优先于特征识别，例：如果特征识别 pdf 文件，自定义后缀识别 doc 文件，那么将一个 pdf 文件后缀改成 doc，则设备会以 doc 文件进行告警而不是 pdf 文件了。

二. 应用场景：

如某单位需要审计并告警内网通过 ftp、http 或者 email 的方式外发文本文件类型的所有文件、pdf 类型的加密文件、压缩文件，防止员工泄密。

设置步骤：

1. 登陆设备控制台，选择【上网行为管理】--【上网策略对象】，新增策略或者双击编辑需要设置的策略，下面以策略 lxf 为例。如图所示：

网关控制台 SINFOR 深信服科技
Sinfon-AC-1.9.6

当前用户: admin 注销

>> 上网策略对象 帮助

策略导入: 浏览... 导入 选择策略文件导入 下载策略模板

上网策略对象列表

选中	策略名称	描述	过期日期	状态	操作
<input type="checkbox"/>	_模板(基本上网审计)1	允许DNS, HTTP, HTTPS, FTP, 邮件, MSN, 并开启相关审计	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	_模板(封堵全部P2P)	封堵全部P2P等下载工具, 请注意作为最后一条策略的话是缺省拒绝。	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	_模板(监控IM聊天内容)	插件监控IM内容: QQ、MSN、ICQ、Skype、Yahoo通、UC、POPO、GTalk、飞信、阿里	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	_模板(防钓鱼网站)	阻止非法SSL协议证书欺骗, 需要控制https网站开启URL过滤相关域名即可。	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	_模板(开放全部上网权限并审计)	开放全部上网权限, 记录全部上网行为。	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	_模板(开放全部上网权限不审计)	开放全部上网权限, 不要记录任何上网行为。	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	_模板(防文件泄密)	对压缩包, 办公软件, 工程制造, 程序源代码等进行外发文件告警。	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	_模板(防木马)	对危险的网络行为进行识别, 对HTTP或者SMTP泄密行为告警。	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	_模板(基本上网审计)	允许DNS, HTTP, HTTPS, FTP, 邮件, MSN, 并开启相关审计	永久生效	启用	查看被使用情况 重命名
<input type="checkbox"/>	lxf	外发文件告警测试	永久生效	启用	查看被使用情况 重命名

首页 上一页 1/1 下一页 末页 跳转到 页 (每页显示 50 条记录)

新增策略时以 为模板

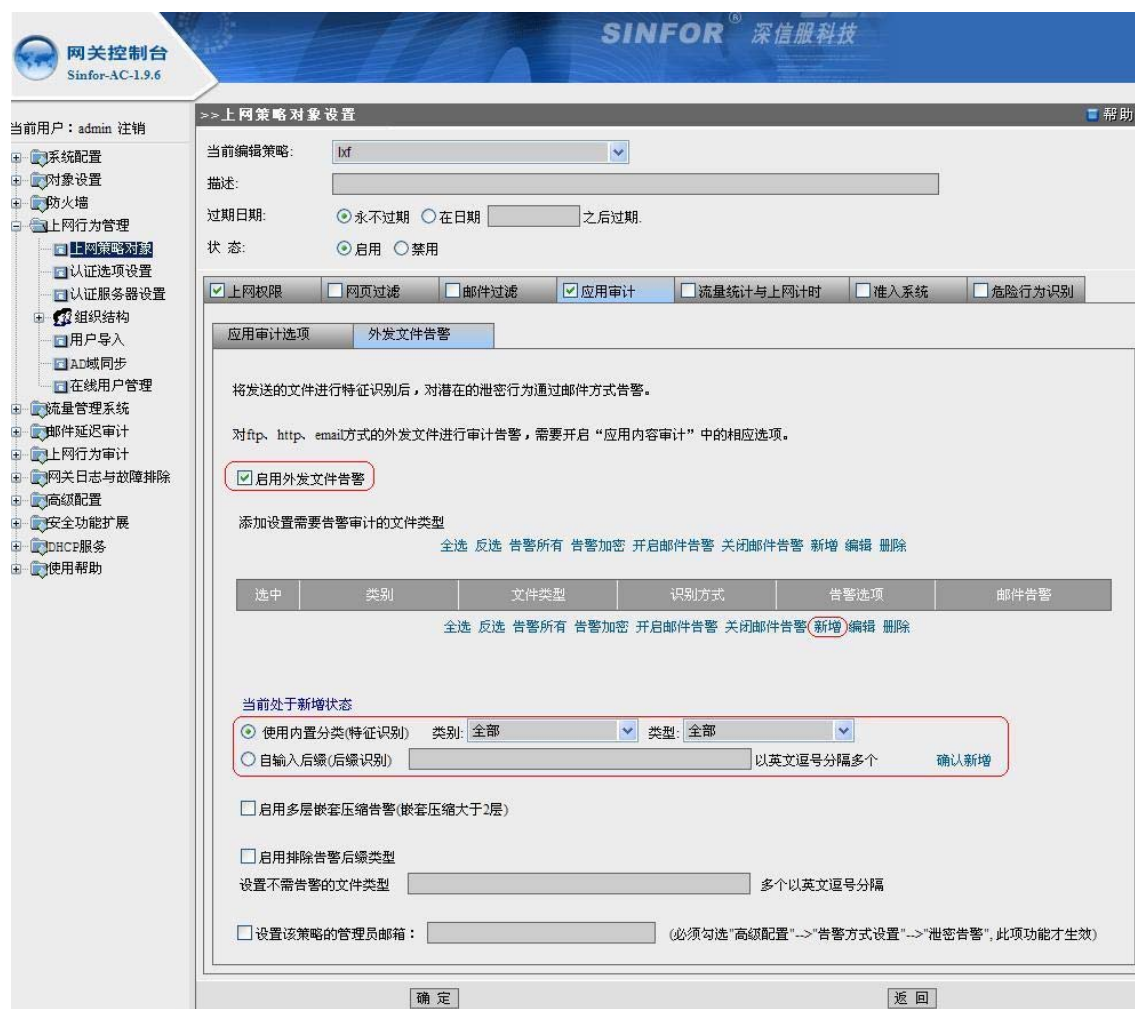
2. 勾选【应用审计】，在【应用审计选项】页面勾选【网页上传审计】、【邮件审计】和【审计FTP】相应的选项。如图所示：



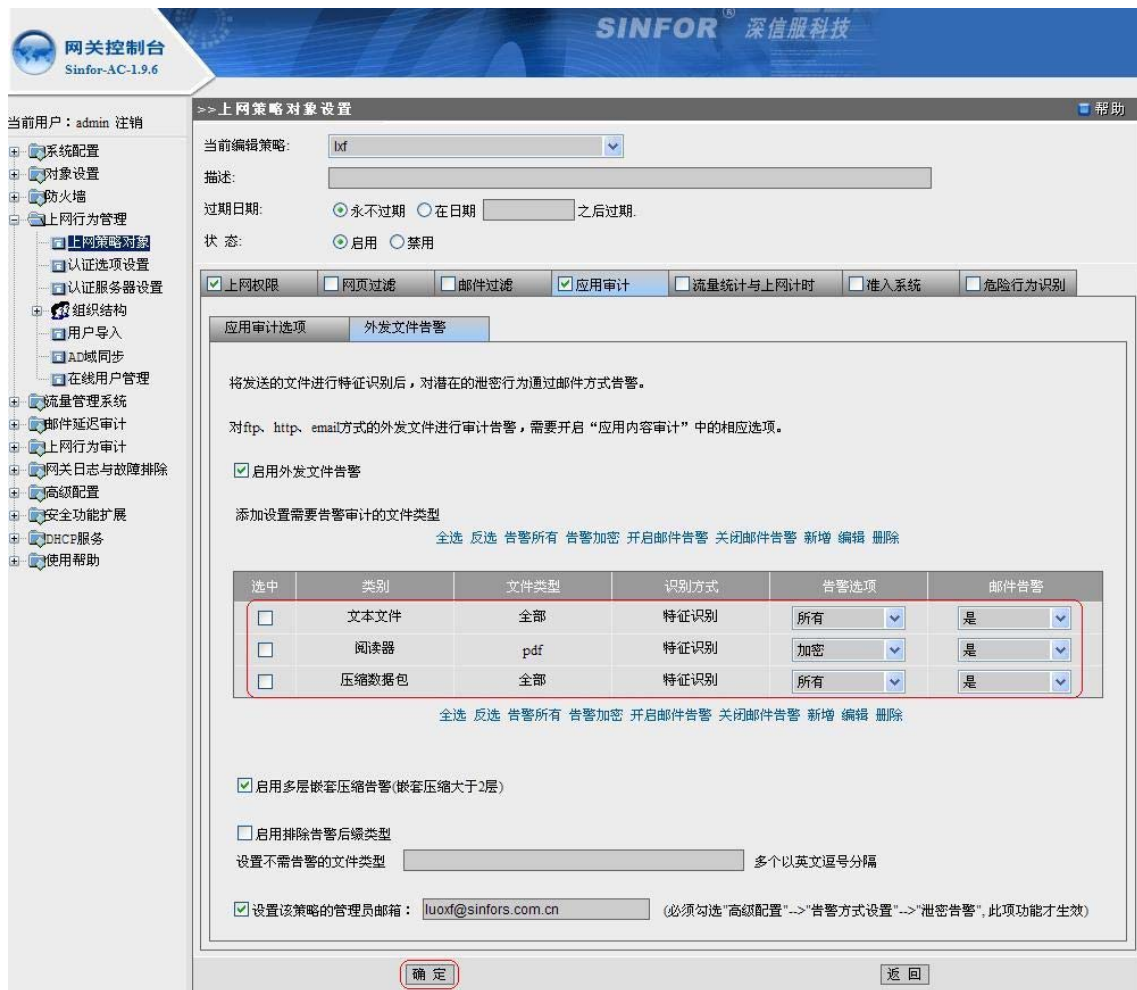
3. 然后选择【外发文件告警】，点击【新增】，如图所示：

注意：使用内置分类（特征识别）：是添加内置库中已经存在的文件类型，根据文件特征进

行识别；自定义后缀（后缀识别）：是由用户自定义需要审计告警的文件类型，根据文件后缀进行识别，支持添加多个后缀名，每个后缀名以英文逗号分隔。



接着选择“使用内置分类（特征识别）”添加三条规则，分别是：第一条类别为“文本文件”、类型为“全部”，然后点击【确认新增】；第二条类别为“阅读器”、类型为“加密”，然后点击【确认新增】；第三条类别为“压缩包”、类型为“全部”，然后点击【确认新增】；然后点击【确定】进行保存策略。如需要告警审计其他文件类型继续添加即可，根据实际情况设置。如图所示：



注意：【启用多层嵌套压缩告警（嵌套压缩大于2层）】、【启用排除告警后缀类型】和【设置该策略的管理员邮箱】可以根据实际需求进行配置；如果没有该功能需求，可以不做设置。

启用多层嵌套压缩告警（嵌套压缩大于2层）：对嵌套压缩文件进行告警；

启用排除告警后缀类型：设置不需要告警的文件类型，支持填写多个后缀，以英文逗号隔开；

设置该策略的管理员邮箱：填写告警邮件的接收人。要使告警邮件发送到管理员邮箱，通知管理员，还必须勾选"高级配置"-->"告警方式设置"-->"泄密告警"，此项功能才生效。

配置界面如图所示：



4. 设置好策略后，接下来就需要把用户或者组和策略关联起来。
 操作步骤：选择【上网行为管理】--【组织结构】，选择需要绑定的用户或者用户组（如“lxf”组），然后选择【上网策略列表】，点击【添加策略】，选择策略对象为“lxf”再点击【添加】，最后点击【确定】按钮进行保存。



到这里，设置已基本完成。

5. 如所设置的组（如“lxf”组）有使用 ftp、http 或者 email 方式的外发文件，那么可以登陆到内置数据中心查看日志。

查看方法：在设置控制台选择【上网行为审计】--【数据中心入口】，点击【进入内置数据中心】，然后选择【查询内容】--【上网行为查询】--【外发文件告警查询】。

以下是用 foxmail 客户端外发邮件的方式进行测试的效果。在数据中心的外发文件告警查询页面，点击右上角的【查询选项】设置查询的条件，如图所示：

SINFOR 深信服科技
Sinfor-DC-1.9.6

登录 注销 当前登录用户名: admin 当前语言: 简体中文(CHS)

当前网关: aalog 刷新 自动刷新 1分钟 查询选项 收藏 导出日志

0条记录 组名: / | 日期: 2009-07-03 - 2009-07-03 | 时间: 00:00:00 - 23:59:59 | 包含子组: 是 | 上网应用: 所有类型: 所有应用 | 动作: 拒...

外发文件告警查询

查询对象: 组名 用户名 主机IP地址 包含子组

排除对象: 组名 用户名 主机IP地址 多个对象间用分号间隔
选择需要查看的组或用户

应用类型: 所有类型 可选择所有类型或者指定类型查询

文件类型: 所有类型

时间: 时间范围: 00:00:00 - 23:59:59
 时间对象: 全天

日期范围: 2009-07-02 - 2009-07-03 选择要查看的日志时间

动作: 拒绝 被记录 发现病毒

详细查询

外发文件告警查询结果

↓ → 首页 上一页 1/1 下一页 末页 按最近时间排序 每页显示20条记录

点击列表 [按J 键查看下一条记录, 按K 键查看上一条记录], 按<-或->键向前或后翻页

点击这里选择您想查看的列

序号	用户名	组名	主机IP地址	应...	文件类型	告警状态	文件清单	日期与时间	详细
首页 上一页 1/1 下一页 末页 每页显示20条记录									

点击【开始查询】，在外发文件告警查询结果下可以查看相应的日志记录。点击记录的最后一列【详细】即可查看详细的日志信息。如图所示：

SINFOR® 深信服科技
Sinfor-DC-1.9.6

登录 注销 当前登录用户名: admin 当前语言: 简体中文(CHS)

当前网关: aalog 刷新 自动刷新 1分钟 查询选项 收藏 导出日志

3条记录 组名:/ | 日期:2009-07-02 - 2009-07-03 | 时间:00:00:00 - 23:59:59 | 包含子组:是 | 上网应用:所有类型:所有应用 | 动作:拒...

外发文件告警查询结果

↓ → 首页 上一页 1/1 下一页 末页 [按最近时间排序] 每页显示20条记录

点击列表[按J键查看下一条记录,按K键查看上一条记录],按<-或->键向前或后翻页

☺ 点击这里选择您想查看的列

序号	用户名	组名	主机IP地址	应...	文件类型	告警状态	文件清单	日期与时间	详细
1	lxf2	/lxf/	192.168.1.104	邮件	压缩数...	常规文件	压缩文件.7z(7z压缩包格式)1.JP...	2009-07-02 14:...	
2	lxf2	/lxf/	192.168.1.104	邮件	阅读器	加密文件	外发文件告警加密文件测试.pdf(pd...	2009-07-02 13:...	
3	lxf2	/lxf/	192.168.1.104	邮件	文本文件	常规文件	外发文件告警测试.txt(txt,文本文件)	2009-07-02 10:...	

首页 上一页 1/1 下一页 详细内容 [按J键查看下一条记录,按K键查看上一条记录]

用户名:	lxf2
组名:	/lxf/
IP地址:	192.168.1.104
目标IP:	202.108.3.190
应用类型:	邮件
时间:	2009-07-02 10:57:01
动作:	被记录
文件类型:	文本文件
告警状态:	常规文件
邮件标题:	外发文件告警测试
邮件附件:	1
下载邮件:	查看
邮件大小(B):	1803
策略:	lxf
发送地址:	sinfors_kf@sina.com
收件地址:	271852682@qq.com
邮件状态:	正常发送或接收
文件清单:	外发文件告警测试.txt(txt,文本文件)
文件名:	外发文件告警测试.txt
DNS:	smtp.sina.com.cn

点击【查看】即可打开或保存相关发送文件

另外,如果是外置的数据中心,需要在IE中输入安装数据中心服务的那台服务器的IP地址,如果默认的80端口被改掉,那么的输入应该是: http://数据中心服务器IP:更改后的端口。进入后的界面跟内置数据中心界面一致,查询方法也一致。