网络卫士安全审计系统TA-W

用户手册

天融信

TOPSEC®

北京市海淀区上地东路 1 号华控大厦 4 层 100085

电话：+8610-82776666

传真：+8610-82776677

服务热线：+8610-8008105119

http://www.topsec.com.cn

版权声明

商标声明

信息反馈

http://www.topsec.com.cn

目　录

1 前言

本用户手册主要介绍了网络卫士安全审计系统 TA-W 的系统架构、配置、使用和管理。通过阅读本文档，用户可以了解网络卫士安全审计系统 TA-W 的基本设计思想，并根据实际应用环境安装和配置网络卫士安全审计系统。

本章内容主要包括：

- 文档目的
- 读者对象
- 文档基本内容
- 约定
- 相关文档
- 在线技术支持
- 技术服务体系

1.1 文档目的

本文档主要介绍如何配置和使用网络卫士安全审计系统 TA-W。通过阅读本文档，用户能够正确地部署和配置网络卫士安全审计系统，并综合运用安全审计系统提供的网络数据采集能力、强大的审计分析功能、智能的信息处理能力，实现对用户的网络行为监控、网络传输内容审计，实现网络传输信息的保密存储，从而实现网络行为后期取证，并对网络潜在威胁者予以威慑。

1.2 读者对象

本用户手册适用于具有基本网络知识的系统管理员和网络管理员阅读，通过阅读本文档，他们可以独自完成以下一些工作：

- 网络卫士安全审计系统的基本配置。
- 网络卫士安全审计系统的数据采集策略、报警策略、流量监控策略的配置与下发。
- 网络行为监控、内容审计、内容关键词中标检查。

- 综合分析网络数据，生成行为监控报表和流量监控报表。
- 网络卫士安全审计系统的实时监控与日志管理。
- 用户管理。

1.3 文档基本内容

本用户手册包含以下章节及附录：

- 第一章“前言”，介绍了本手册各章节的基本内容、文档约定和技术支持信息。
- 第二章“网络安全审计系统简介”，介绍了网络卫士安全审计系统的一些基本概念，如产品概述、系统架构、工作机制、基本概念等。
- 第三章“基本配置”，主要介绍用户在初次使用网络卫士安全审计系统时必须进行的初始配置和系统的基本管理。
- 第四章“审计策略配置”，介绍网络卫士安全审计系统的数据采集策略、报警响应策略、流量监控策略的配置与下发。
- 第五章“安全审计功能”，介绍了如何利用 WEBUI 管理中心，对被网络中预先设定的地址对象进行行为监控、内容审计、内容关键词中标检查。以及如何综合分析网络数据，生成行为监控报表和流量监控报表。
- 第六章“实时监控功能”，介绍如何进行应用监控、流量监控和报警信息监控。
- 第七章“系统日志管理”,介绍如何查看系统日志和导出系统日志。

1.4 约定

本文档遵循以下约定：

命令语法描述采用以下约定：

尖括号（<>）表示该命令参数为必选项。

方括号（[]）表示该命令参数是可选项。

竖线（|）隔开多个相互独立的备选参数。

黑体表示需要用户输入的命令或关键字，例如 **help** 命令。

*斜体*表示需要用户提供实际值的参数。

图形界面操作的描述采用以下约定：

“”表示按钮。

点击（选择）一个菜单项采用如下约定：

点击（选择） **高级管理 > 特殊对象 > 用户**。

为了叙述方便，本文档采用了大量网络拓扑图，图中的图标用于指明天融信安全设备和通用的网络设备、外设和其他设备，以下图标注释说明了这些图标代表的设备：

文档中出现的提示、警告、说明、示例等，是关于用户在安装和配置网络卫士安全审计系统过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。

 提示  说明  示例  警告

1.5 相关文档

网络卫士安全审计系统 TA-W 安装手册

网络卫士安全审计系统 TA-W 命令行手册

1.6 在线技术支持

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

http://www.topsec.com.cn/

www.topsec.com.cn 提供交互网络服务，用户及合作伙伴可以在世界的任何地方、任何时候访问 www.topsec.com.cn 技术支持中心，获取实时的网络安全解决方案、安全服务和各种安全资料。

在线技术支持

http://www.topsec.com.cn/bbs/

在线技术资料

http://www.topsec.com.cn/support/down.asp

安全解决方案

http://www.topsec.com.cn/solutions/qw.asp

技术支持中心

http://www.topsec.com.cn/support/support.asp

1.7 技术服务体系

天融信公司的技术服务体系由总公司、大区技术支持中心、各省分公司、办事处、集成商、代理商等多级机构共同组成。原则上，当地的服务由当地的集成商、代理商、办事处、分公司提供；如果当地分支机构人力不足或者技术支持难度很大时，各省所在的大区技术支持中心将派出工程师协助解决；北京总部则在大区技术支持中心人力不足或者解决问题困难较大时，直接对用户提供服务。

天融信全国安全服务热线：800-810-5119

获取技术支持中心最新联系方式，请访问：

http://www.topsec.com.cn/support/support.asp

2 网络卫士安全审计系统简介

本章对网络卫士安全审计系统 TA-W 的系统架构、工作机制以及所涉及的基本概念进行简单介绍。

本章内容主要包括：

- 产品概述：介绍产品的主要功能和适用对象。
- 系统架构：介绍系统的各组成部分及部署。
- 工作机制：介绍系统的基本工作流程。
- 基本概念：介绍本文档所涉及的基本概念。

2.1产品概述

网络卫士安全审计系统 TA-W 是由北京天融信公司自主研发的网络信息安全审计系统。TA-W 是面向企业级用户的集行为监控与内容审计为一体的产品，它以旁路的方式部署在网络中，不影响网络的性能。TA-W 具有即时的网络数据采集能力、强大的审计分析功能以及智能的信息处理能力。通过使用该系统，可以实现如下目标：

- 监控用户的网络行为、审计用户的网络传输内容 （如员工是否在工作时间上网冲浪、网上聊天、是否访问内容不健康的网站、员工是否通过网络泄漏了公司的机密信息等等）。
- 实现网络传输信息的保密存储。
- 实现网络行为后期取证。
- 通过与防火墙联动和对非法信息的阻断，对网络潜在威胁者予以威慑。

该产品适用于对信息保密、控制非法信息传播比较关心的单位或需要实施网络行为监控的单位和部门，如政府、军队机关的网络管理部门，公安、保密、司法等国家授权的网络安全监察部门，金融、电信、电力、保险、海关、商检、学校、军工等各行业网络管理中心，以及大中型企业网络管理中心等。

2.2 系统架构

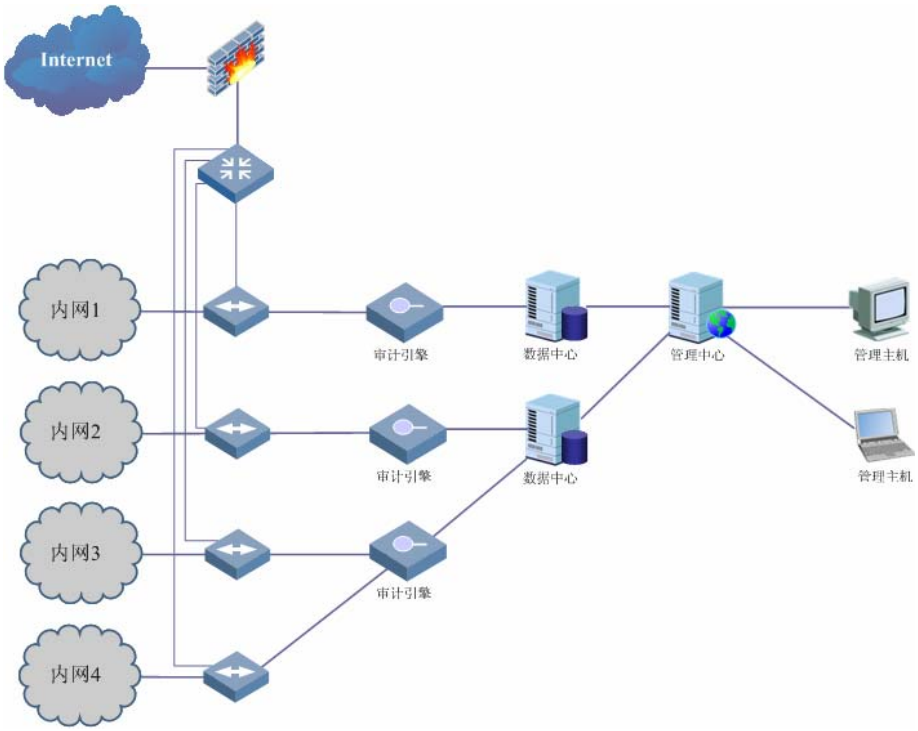


图 2-1 网络卫士安全审计系统部署示意图

网络卫士安全审计系统 TA-W 由审计引擎、数据中心和管理中心三部分组成。

审计引擎是硬件产品，通过旁路接入方式（交换机端口镜像或 HUB 接入）捕获网络中的数据；

数据中心是基于 Windows 平台的软件产品，负责对数据的分析和审计。数据中心需要安装 SQL Server 数据库来存储数据信息。一个数据中心可以存储管理多个审计引擎的数据。同时数据中心集成了数据还原模块，负责对收集到的数据包进行还原，从中获得原始的内容数据，同时还具有统计分析功能。

管理中心负责采集策略、报警策略、流量策略和关键词策略等的配置和下发，同时对一个或多个数据中心的数据进行审计；管理员通过 WEB 浏览器访问管理中心实现对数据中心和审计引擎的管理。

2.3 工作机制

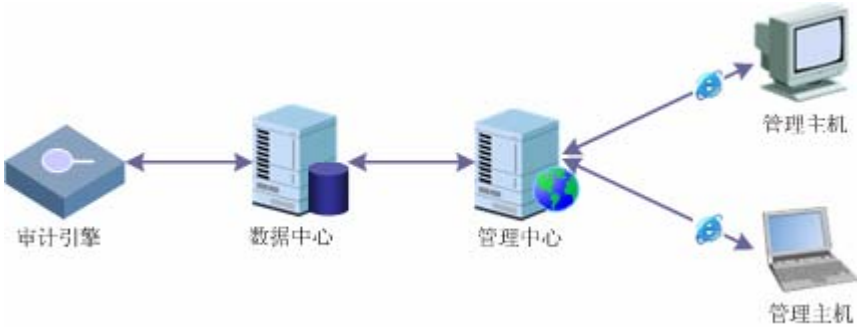


图 2-2 网络卫士安全审计系统工作机制示意图

在系统开始工作前，管理员需要根据实际应用需求在管理中心设置采集策略，并下发给数据中心，由数据中心转发到目的审计引擎。如果没有设置任何策略，则审计引擎将使用默认采集策略进行数据采集。但报警策略和流量监控策略功能在默认情况下不会启用，需要用户根据需要自行决定是否启用。

审计引擎主要负责数据采集，并根据已设置的策略进行过滤，初步分析后后将数据发送给数据中心。同时，审计引擎可以根据已设置的报警策略对异常行为做出反应，向数据中心发送报警信息。另外，审计引擎还可以根据流量分析策略对网络流量信息进行采集，并发送到数据中心。

数据中心负责存储来自审计引擎的数据流，同时响应来自管理中心的请求，对原始数据报文进行还原和分析，并将结果反馈给管理中心。另外数据中心还负责转发来自管理中心的数据采集策略、报警响应策略以及流量监控策略到审计引擎。

管理中心负责下发数据采集策略、报警响应策略以及流量监控策略，并对数据中心中的数据进行汇总显示。管理中心可以根据查询结果实时显示反馈信息，并生成图文报表，以供管理员查询，追踪。管理员通过浏览器访问管理中心，进行策略配置、查询审计结果和其他配置管理等操作。

2.4 基本概念

- 数据采集

网络卫士安全审计系统 TA-W 的审计引擎采用“零拷贝”技术来捕获网络中的数据包，从而避免了频繁的数据拷贝，有效地解决了由此引发的系统性能瓶颈。在对数据包进行过滤、重组和初步的协议分析后，直接把符合条件的数据传输到数据中心。

- 数据分析

网络卫士安全审计系统 TA-W 在捕获到数据包后，需要对数据包进行分析、还原供管理员审计和查询。网络卫士安全审计系统支持对基于 HTTP、FTP、SMTP、POP3、Webmail、TELNET、MSN、QQ、RTSP、MMS 等协议的数据包进行行为监控。另外，还可以对 HTTP、FTP、SMTP、POP3、Webmail、TELNET、MSN 协议进行完整的还原。

- 可分析的文件编码

网络卫士安全审计系统 TA-W 可分析采用 Base64、Quoted-Printable、UTF-7、UTF-8 等编码格式的文件。

- 可分析的压缩文件格式

网络卫士安全审计系统 TA-W 可分析 zip、rar、arj、gz、tar、cab 等压缩文件。

3 基本配置

本章主要介绍用户在初次使用网络卫士安全审计系统时，所需要进行的基本配置与管理，包括以下内容：

- 登录系统
- 系统资源管理
- 数据中心管理
- 审计引擎管理
- 数据库管理
- 用户管理

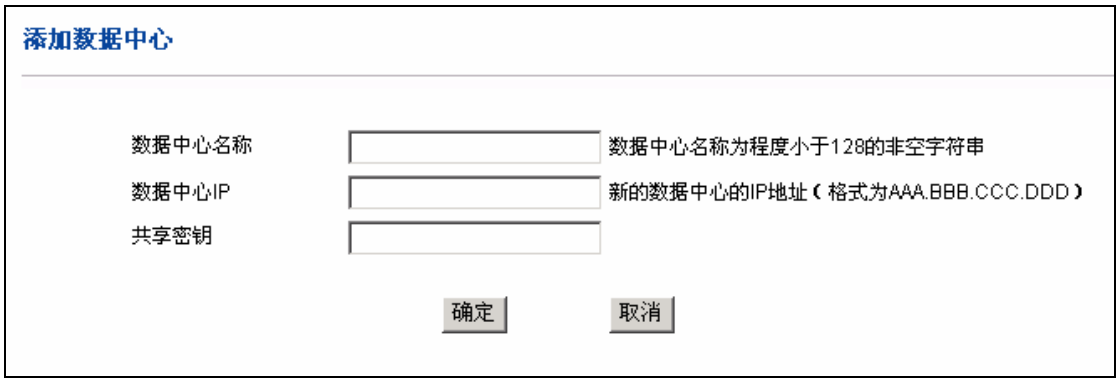
3.1 登录系统

管理员通过 WEB 浏览器可以登录网络卫士安全审计系统的管理中心，对系统的所有配置与管理工作都是在管理中心完成的。网络卫士安全审计系统支持 IE，MyIE，Firefox 等不同厂商的浏览器。

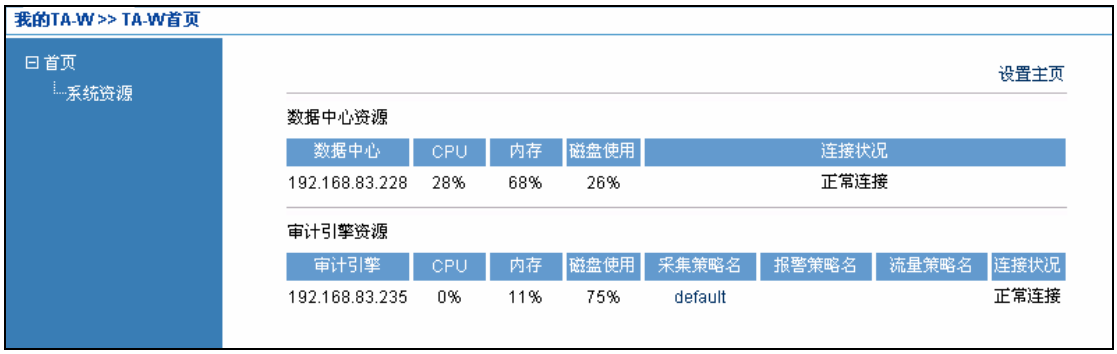
在登录时，管理员需要在管理主机的浏览器上输入网络卫士安全审计系统的管理 URL，例如：https://192.168.1.254，弹出如下的登录页面。

输入用户名密码后（网络卫士安全审计系统默认出厂用户名为：superman，密码为：talent），点击“登录”，就可以进入管理页面。

初次登录管理界面时，系统将自动进入“添加数据中心”的操作界面，要求用户输入数据中心的信息，如下图所示。



添加已经安装的数据中心的名称和 IP 地址，并输入共享密钥后（系统初始的共享密钥为“TOPSEC_2005”），点击“确定”，即可进入管理中心的首页。如下图，首页中显示了系统当前可用的数据中心资源和审计引擎资源信息。



提示

- TOPSEC安全审计系统支持http、https两种访问方式。例如，使用http://192.168.1.3和https://192.168.1.3均可以访问审计系统；
- TOPSEC 安全审计系统对于用户名、密码大小写敏感；
- 如果用户安装时修改了Apache服务的端口号(默认HTTP端口为 80，HTTPS 端口为 443)，在登录时需要在最后加上端口号，如http://192.168.1.254:8080。

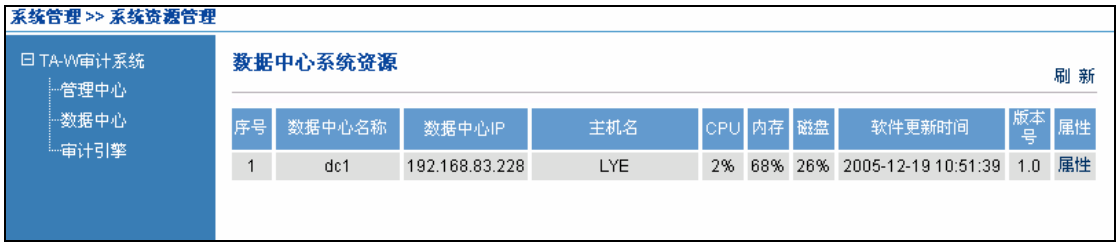
3.2 查看系统信息

选择 **系统管理**，进入“系统资源管理”页面，可以查看网络卫士安全审计系统的管理中心、数据中心和审计引擎的名称和IP地址。

3.3 数据中心管理

数据中心是网络卫士安全审计系统的重要组成部分。一个管理中心可以下设多个数据中心。管理员可以通过管理中心对数据中心进行统一管理。

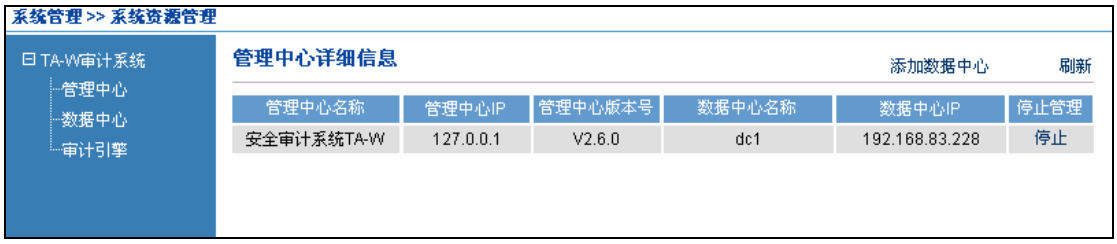
选择 **系统管理 > 系统资源管理 > 数据中心**，可以查看所有数据中心的信息，如图所示。



3.3.1 添加数据中心

对新的数据中心进行审计管理前，管理员需要添加审计管理的数据源，也就是添加数据中心。

1）选择 **系统管理 > 系统资源管理 > 管理中心**，进入管理中心详细信息页面，如下图所示。



该页面显示管理中心所在主机的相关信息，如主机IP地址和管理中心版本号，以及管理中心下属的数据中心信息。

2）点击页面右上方的“添加数据中心”，如下图所示。

逐项填入数据中心的名称、所在主机 IP 地址及数据中心与管理中心通信的共享密钥。

点击“添加”提交，或点击“重置”重新填写。添加成功后系统将显示提示信息。

说明

- ✧ 为了保证网络卫士安全审计系统各组成部分之间通信的安全性，不同部分之间的通信采用加密传输技术。管理中心到数据中心使用的是ssl通道加密技术，默认的共享密钥是“TOPSEC_2005”，共享密码可以在数据中心上进行修改。

3.3.2 维护数据中心

点击数据中心系统资源某数据中心的“属性”，可对该数据中心的部分属性进行修改，如图所示。

各属性的具体参数及含义如下：

1．网络属性

参数名	意义
数据中心名	安装数据中心时使用的名称，监控、审计时使用。
数据中心 IP	数据中心主机的 IP 地址。
数据中心 MAC	数据中心主机的 MAC 地址。
网关	数据中心主机所处网段网关的 IP 地址。
子网掩码	数据中心主机网段所使用的地址掩码。
DNS	数据中心主机所用 DNS 服务器的 IP 地址。

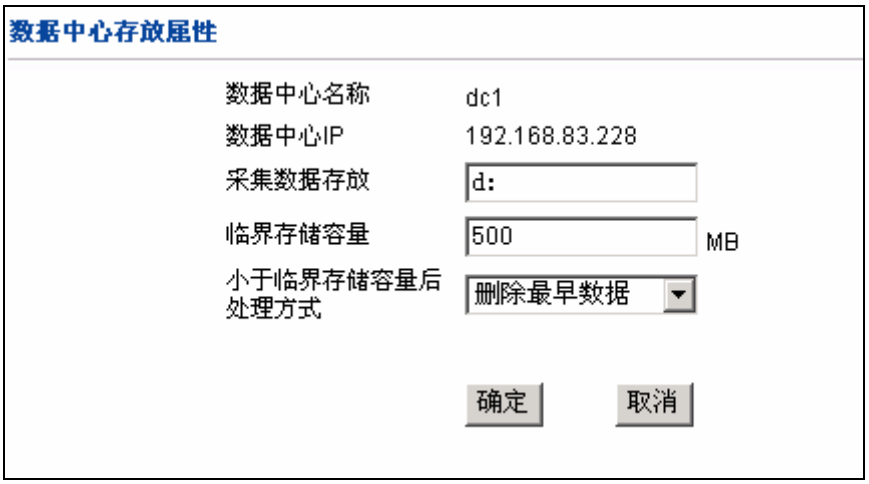
说明

✧ 网络属性部分的参数在添加数据中心时已经确定，不可修改。

2．采集数据存放属性

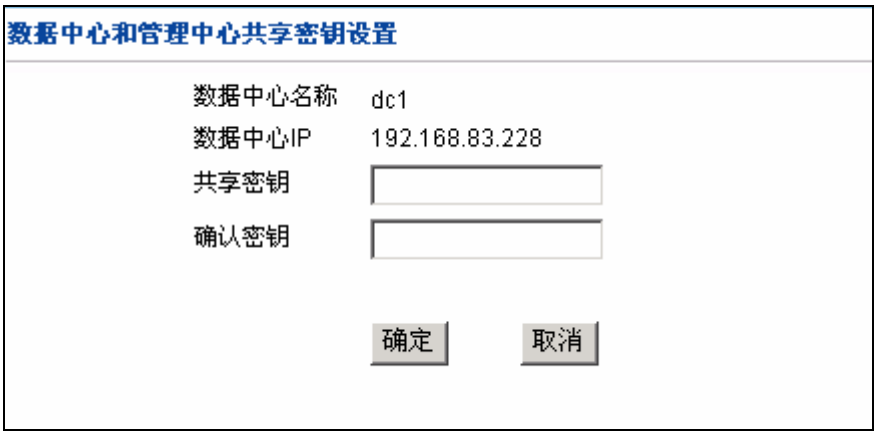
参数名	意义
采集数据存放	数据存放处磁盘的盘符。
剩余报警容量	存放数据的磁盘的剩余容量小于该值时将提示报警。
无剩余空间处理方式	存放数据的磁盘没有剩余空间时的处理方式。

点击旁边的“修改设置”按钮，可以修改相关参数，如下图。



3．与管理中心预共享密钥

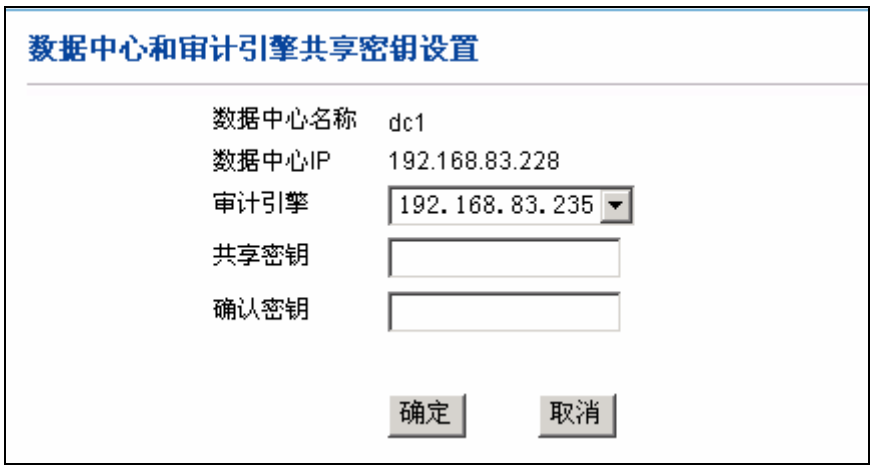
数据中心与管理中心通信的共享密钥设置，单击右侧的“修改设置”按钮，进行共享密钥的修改，如下图。



4．与审计引擎预共享密钥

数据中心与审计引擎通信的共享密钥设置。一个数据中心可以对应多个审计引擎，但是一个审计引擎只可以对应一个数据中心。在设置密钥时注意选择相应的审计引擎 IP 地址。

点击对应的“修改设置”按钮可以修改数据中心与审计引擎通讯的共享密钥和通讯时的加密方式，如下图 。



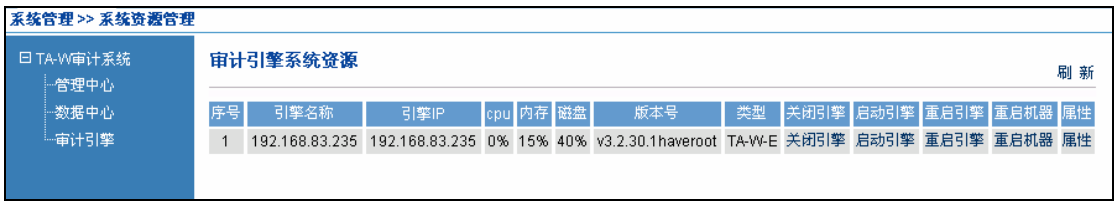
说明

- ✧ 数据中心与引擎的共享密钥、加密方式修改时，必须成对修改，否则审计引擎将无法与数据中心进行连接。

3.4 审计引擎管理

审计引擎主要根据审计策略来采集数据信息。管理员可以通过管理中心对审计引擎进行远程管理。

选择 **系统管理** > **系统资源管理** > **审计引擎**，可以查看所有审计引擎的信息，如图所示。



列表中显示的是当前正在通讯连接的审计引擎，审计引擎与数据中心通信配置请参见《网络卫士安全审计系统安装手册》。

管理员可以对审计引擎进行管理，如关闭引擎、启动引擎、重启引擎、重启机器

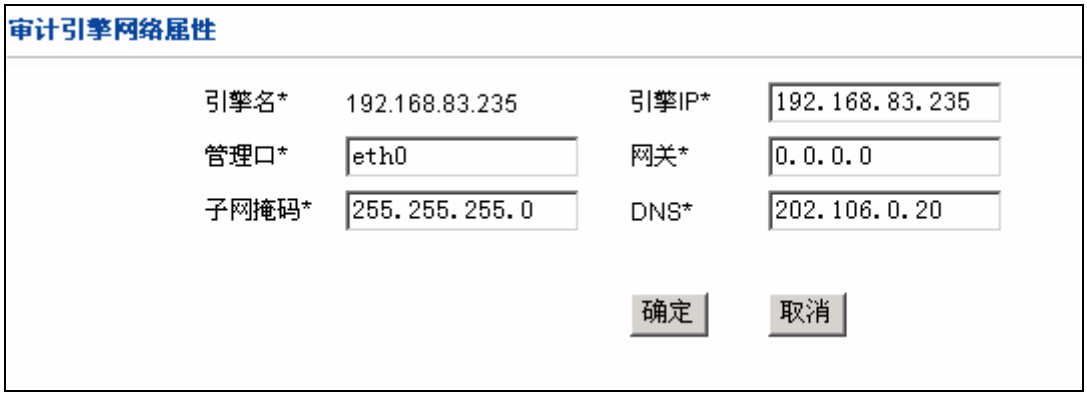
点击审计引擎对应的“属性”链接，可对该审计引擎的各属性信息进行修改，如图所示。

各属性的具体参数及含义如下：

1．网络属性

参数名	意义
引擎名	审计引擎的名称 。
引擎 IP	审计引擎管理口的 IP 地址。
引擎 MAC	审计引擎的 MAC 地址。
管理口	审计引擎的管理接口，默认为 Eth0，可以在审计引擎上更改管理口。
网关	审计引擎所在网段网关的 IP 地址。
子网掩码	审计引擎所在网段使用的地址掩码。
DNS	审计引擎所用 DNS 服务器的 IP 地址。

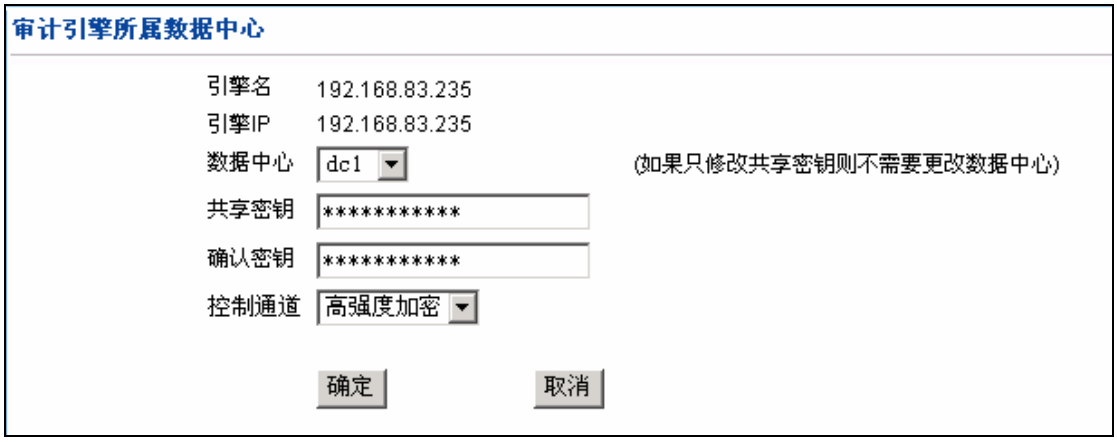
点击“修改设置“，可以修改审计引擎的网络属性，如下图所示。



2．数据中心

参数名	意义
所属数据中心	与审计引擎相连接的数据中心的 IP 地址。
共享密钥	审计引擎与数据中心的共享密钥。
通信加密方式	与数据中心之间通信的加密方式，默认为“高强度加密方式”。

点击“修改设置”，弹出如下对话框。管理员可以更改与审计引擎相连的数据中心，并修改与数据中心的共享密钥和加密方式。



3．引擎当前时间

调整引擎当前时间，保证数据采集的全面性，可以手动设置，也可以与时间服务器同步。

3.5 数据库管理

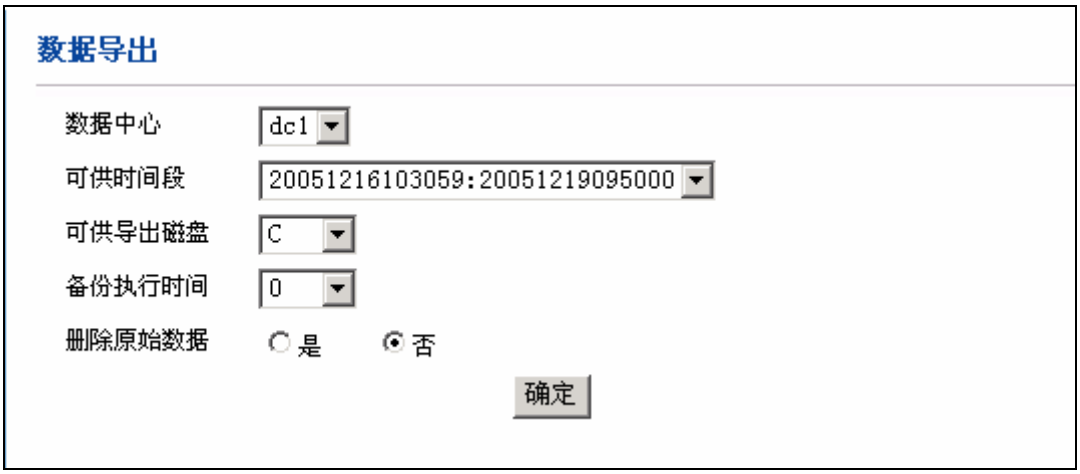
网络卫士安全审计系统支持数据的本地存储。存储内容包括了文件索引信息、流量、连接和应用监控信息等。管理员应根据实际情况及时对数据进行导出、导入、删除等操作。

说明

- ✧ 系统对当前正在读写的数据表不能执行导出操作，当数据表写满后，方可执行。

3.5.1 数据导出

选择 **系统管理** > **数据库管理** > **数据导出**，弹出如下对话框。



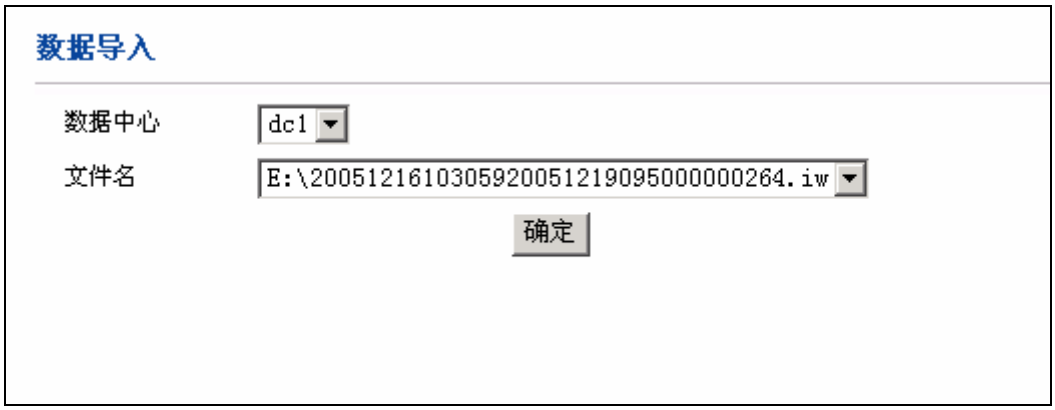
各属性的具体参数及含义如下：

参数名	意义
数据中心	选择希望备份的数据中心名称，设置备份数据的时间段。
可供时间段	下拉列表中显示可供导出数据的时间范围。
可供导出磁盘	选择要存放数据的磁盘盘符。
删除原始数据	导出后是否删除原数据中心的数据。

点击“确定”完成数据导出。

3.5.2 数据导入

选择 **系统管理** > **数据库管理** > **数据导入**，如图所示。



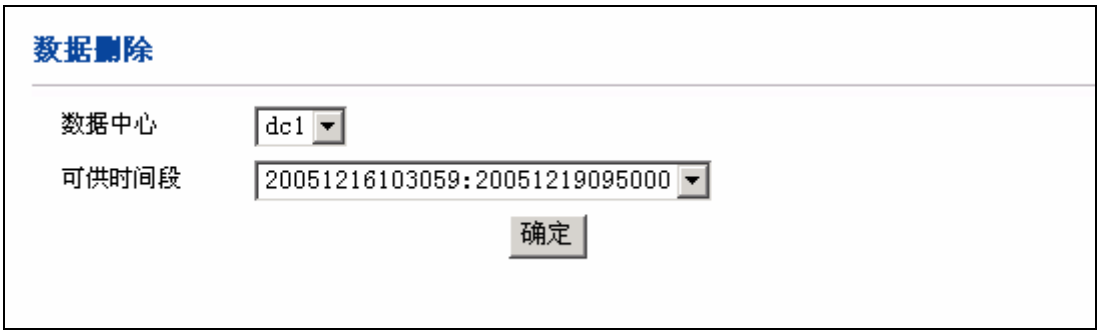
各属性的具体参数及含义如下：

参数名	意义
数据中心	选择希望导入数据的数据中心名称。
文件名	数据源的存储路径。

点击“确定”提交完成数据导入，系统将显示提示信息。

3.5.3 数据删除

选择 **系统管理** > **数据库管理** > **数据删除**，如图所示。



选择要删除的数据中心的数据表，点击“确定”按钮，完成删除。

3.6 审计引擎维护

网络卫士安全审计系统的管理中心还提供了审计引擎的高级配置和配置保存等功能。下面将具体介绍这些功能的使用和配置。

3.6.1 引擎高级配置

1）选择 **系统管理 > 其他设置 > 引擎高级配置**，如下图所示。

2）选择要配置的审计引擎。

3）设置会话大小，会话大小是系统支持的最大会话值，默认值为 4096KB。

4）设置在采集 HTTP 协议的数据时是否要采集图片数据，建议用户不采集图片。

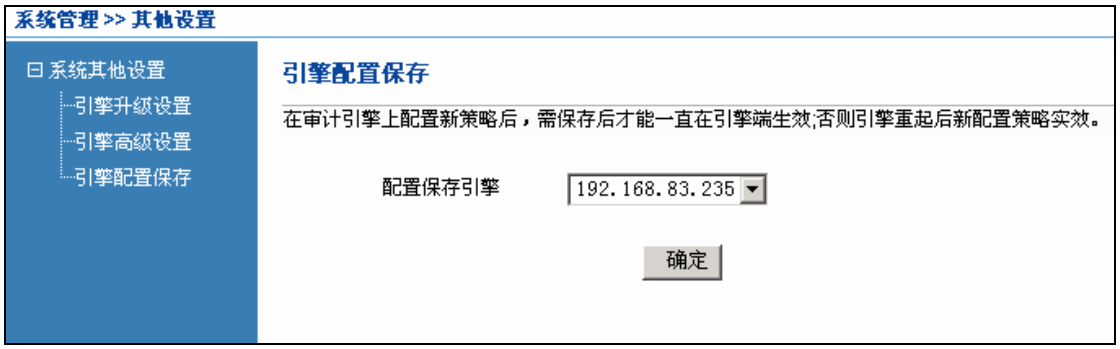
5）点击”确定”,完成配置。

3.6.2 引擎配置保存

在审计引擎上配置新策略后，策略只是暂时生效，在重新启动审计引擎后，原有的策略将会失效。因此需要在完成引擎的策略配置后，先保存引擎配置，才能保证引擎端策略的长期有效。

保存引擎配置的具体操作如下：

1）选择 **系统管理 > 其他设置 > 引擎配置保存**，如下图所示。



2）选择保存配置的审计引擎。

3）点击“确定”,保存配置。

3.7 用户管理

网络卫士安全审计系统是一个多用户系统，采用分级的用户管理和授权模式，并允许若干不同级别的用户同时操作和使用系统，在系统中定义了四种级别用户，各级用户的权限如下：

- 超级管理员：具有系统所有功能的权限，对所有的数据中心具有操作权限。
- 内容审计员：与指定的数据中心相对应，可以设置和下发关键词策略，查看采集策略、报警响应策略和流量监控策略，可以对各类行为的内容进行审计，内容审计员具有行为审计员的所有权限。
- 行为审计员：与指定的数据中心相对应，可以对网络行为进行监控，查看各类报表，查看各类策略，但对具体行为的内容不可查看。
- 日志管理员：仅可以对日志内容进行查看。

说明

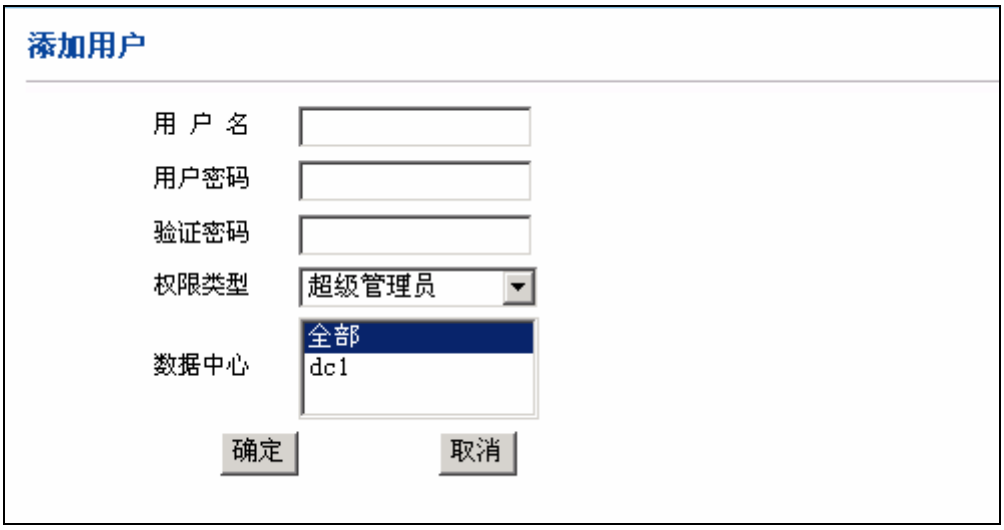
✧ 用户和数据中心是多对多的关系，即一个数据中心可以对应多个用户，一个用户也可以管理多个数据中心。

选择 **用户管理** > **用户权限管理**，进入用户管理页面，如图所示。

系统默认超级管理员“superman”，具有对所有数据中心的管理权限，不可删除。

➢ 添加用户

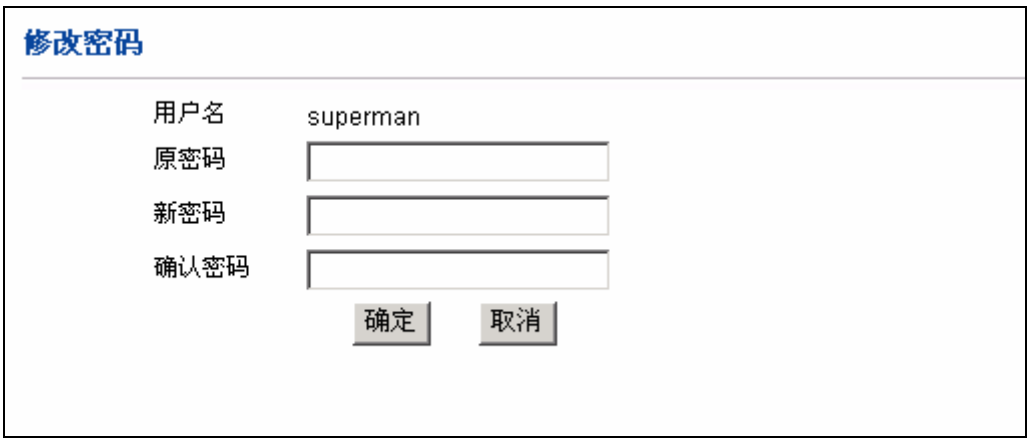
点击页面右上方“添加用户”按钮，弹出如下对话框。



输入“用户名”和“用户密码”，在“权限类型”中选择用户所具有的权限级别，在“数据中心”选择用户可管理的数据中心，可以是全部数据中心或某个数据中心。

➢ 修改用户信息

当前登录用户可以修改本身的密码信息，选择 **用户管理 > 修改用户信息**，点击列表右侧的“修改”，弹出“修改密码”对话框，如下图所示。



输入“原密码”并设置“新密码”，点击“确定”按钮，系统将显示“修改成功”的提示信息。

4 审计策略配置

超级管理员可以在管理中心为系统配置数据采集策略、报警响应策略和流量监控策略，并将已定义的策略通过数据中心下发到指定的审计引擎，审计引擎采集数据并根据采集策略对数据包进行过滤，还可根据报警响应策略做出实时的报警响应或发送报警日志到数据中心。

在数据采集过程中，系统对采集的数据做以下处理：

对于匹配采集策略的数据将保留数据包并发往数据中心存储，管理员可在管理中心通过设定审计条件对用户的操作行为和内容进行审计，并可根据设定产生各种行为统计报表，具体操作请参见节5.1行为审计、5.2内容审计、5.3行为统计报表查看。

对于匹配报警策略的数据包将向数据中心发送报警信息并根据设定的响应方式响应，管理员可在管理中心查看所需的报警日志，具体操作请参见节6.3报警信息监控。

对于匹配流量监控策略的数据包将实时监控数据流量并将统计数据发往数据中心。管理员可在管理中心查看指定对象范围的实时流量信息并按设定的条件生成各种流量统计报表，具体操作请参见节6.1应用监控、6.2流量监控 和5.4流量统计报表查看。

本章详细说明在管理中心中如何定义和下发各种审计策略，包括：

- 对象定义
- 采集策略配置
- 关键词策略配置
- 报警策略的配置
- 流量监控策略的配置

4.1 对象定义

在配置各审计策略前，管理员需要预先定义全局的时间对象和 IP 地址对象，用于设置各种审计策略的时间范围和 IP 地址范围。管理员可以使用自定义和预定义两种方式定义对象，使用预定义对象需要提前进行设置。

系统中用到的对象包括：

- IP 对象：IP 地址段，可以是不在一个 IP 段的地址。

- IP 组对象：最多包括 32 个 IP 对象。
- 时间对：24 小时之内。
- 时间组对象：最多包括 8 个时间对象。

系统提供了几个常用对象的默认出厂配置，如下表所示。

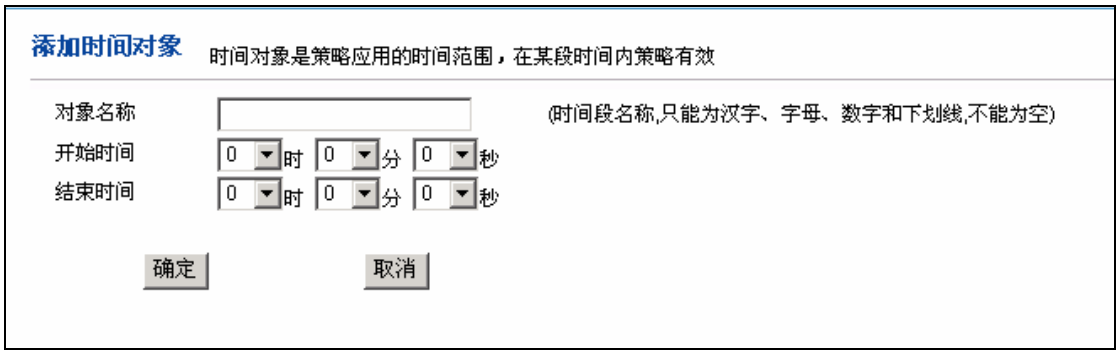
对象	出厂配置
时间对象	凌晨：00：00：00－09：00：00 上午：09：00：00－12：00：00 中午：12：00：00－13：00：00 下午：13：00：00－18：00：00 晚上：18：00：00－23：59：59
时间组对象	上班时间：上午、下午 全天：凌晨、上午、中午、下午、晚上
IP 对象	any：0.0.0.0－255.255.255.255
IP 组对象	any

下面将分别介绍每种对象的定义方法。

4.1.1 时间段设置

1）选择 **审计策略 > 采集策略 > 时间对象**，如图所示。

2）点击页面右侧“添加时间对象”，弹出如下对话框。

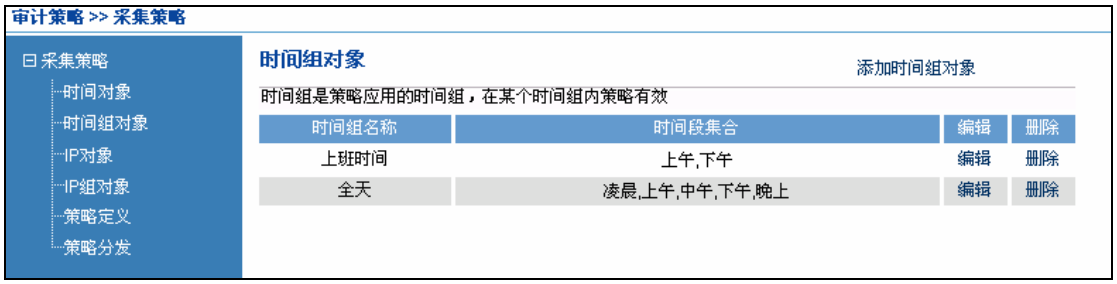


3）输入时间对象的名称，设置开始时间和结束时间，点击“确定”按钮，该对象将被添加到时间对象列表中。

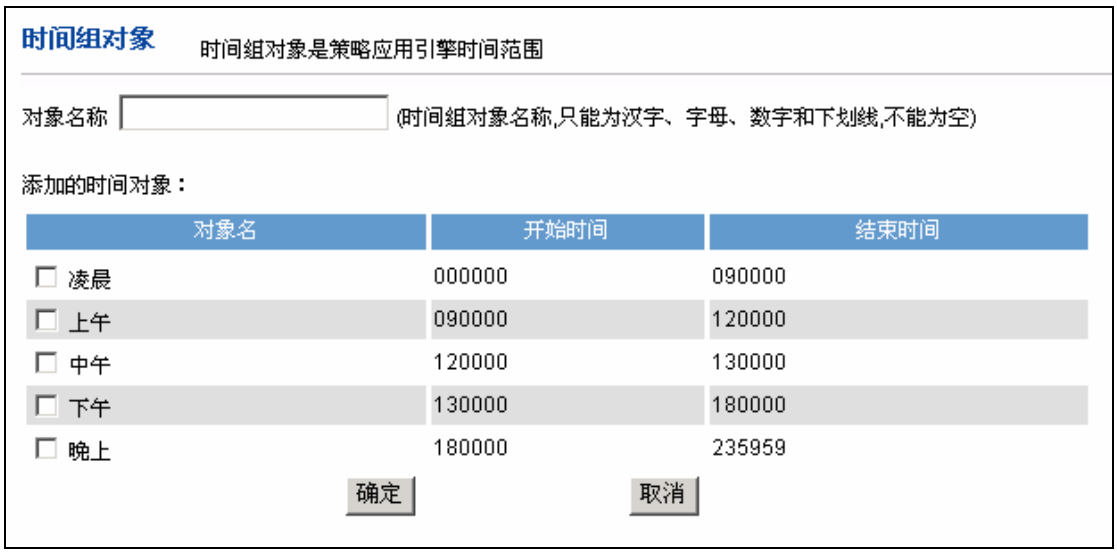
4）添加对象后可以对其进行修改和删除，点击对象右侧“编辑”和“删除”即可。

4.1.2 时间组设置

1）选择 **审计策略 > 采集策略 > 时间组对象**，如图所示。



2）点击页面右侧“添加时间组对象”，弹出如下对话框。

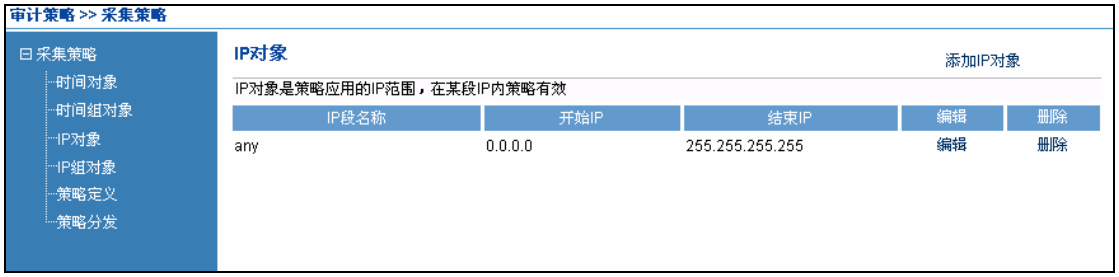


3）添加对象名称，选择已定义的时间对象，点击“确定”提交。

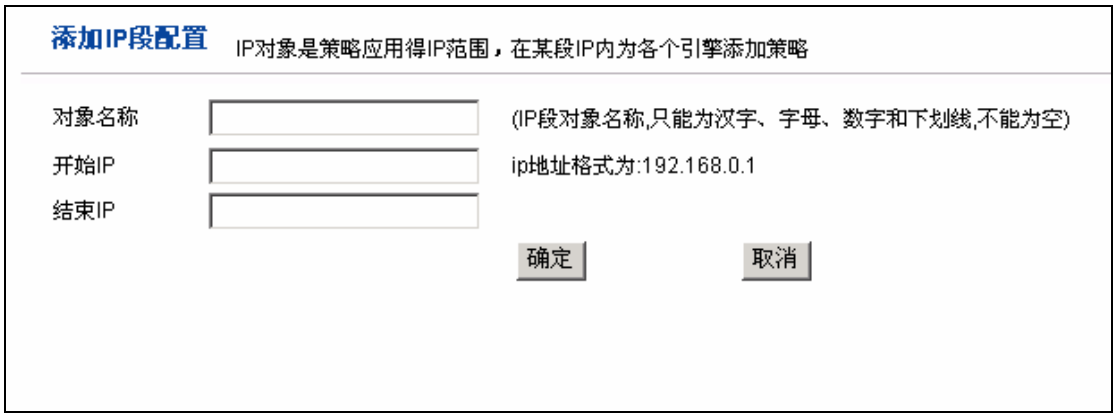
4）添加对象后可以对其进行修改和删除，点击对象右侧“编辑”和“删除”即可。

4.1.3 IP 对象设置

1）选择 **审计策略 > 采集策略 > IP对象**，如图所示。



2）点击页面右侧“添加 IP 对象”，弹出如下对话框。



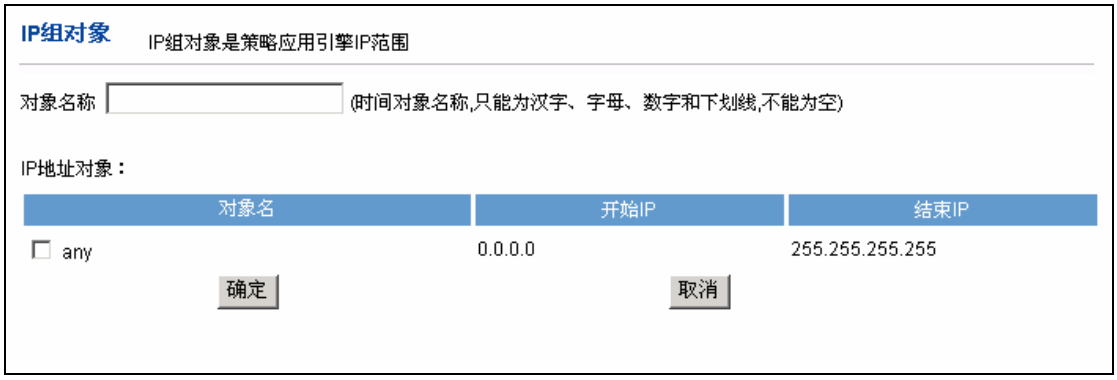
3）添加对象名称和开始、结束 IP 后，点击“确定”提交，IP 对象可以是源 IP, 也可以是目标 IP。

4）添加对象后可以对其进行修改和删除，点击对象右侧“编辑”和“删除”即可。

4.1.4 IP 组设置

1）选择 **审计策略 > 采集策略 > IP组对象**，如图所示。

2）点击页面右侧“添加 IP 组对象”，弹出如下对话框。



3）添加对象名称，选择已定义的 IP 对象，点击“确定”提交。

4）添加对象后可以对其进行修改和删除，点击对象右侧“编辑”和“删除”即可。

说明

- ✧ 已经使用的对象无法进行删除。

4.2 采集策略配置

数据采集策略定义了审计引擎需要采集的数据包的范围，通过应用协议类型来过滤需要采集的数据，系统支持对多种应用的采集过滤，包括：

HTTP：超文本传输协议，用于从 WWW 服务器传输 WEB 超文本到本地浏览器，是最常用的 internet 服务。

FTP ：文件传输协议，用于将文件从远程计算机上拷贝到本地计算机，或者把本地计算机上的文件传送到远程计算机上。

SMTP：简单邮件传输协议，用于发送电子邮件。

POP3：邮局协议（第 3 版），用于接收电子邮件。

Webmail：一些网站提供的网页形式的邮件系统，目前没有标准的协议，网络卫士安全审计系统支持对 sina、hotmail、yahoo、163、sohu 发邮件的单独提取处理。

TELNET：远程登录协议，用于与远程的计算机建立通信。

MSN：微软的即时通信服务，主要使用 MSN 协议通信。

QQ：腾讯的网上聊天服务，在数据通信中主要使用 TCPF（文字聊天协议簇）等协议。

RTSP；Real-Time Streaming Protocol，实时流协议，一般用于传输 Real 服务器发布的媒体文件，如.rm、.ram 文件。

MMS：Microsoft Media Server，微软媒体服务器，通过 MMS 协议可以访问并接收 Windows Media 服务器中的媒体文件，如.asf、.wmv 等。

系统可以对采用以上协议传输数据的行为进行监控，同时，可以对采用 HTTP、FTP、SMTP、POP3、Webmail、TELNET 和 MSN 协议传输的数据内容进行还原，并支持对多重压缩文件的解压还原，支持的压缩文件格式包括 zip、rar、arj、gz、tar 和 cab。

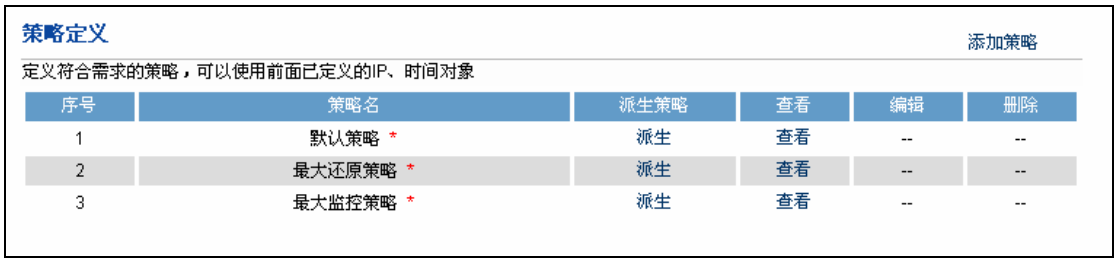
4.2.1 定义采集策略

采集策略的配置是对系统进行的最基本策略配置，审计引擎根据系统下发的采集策略分析和过滤数据包，在管理中心可以定义多种采集策略下发给不同的审计引擎。

超级管理员具有定义数据采集策略的权限，默认情况下，系统已定义了以下三种采集策略：

- 最大还原策略：系统预先设定的默认策略，可以对审计系统所支持的所有还原协议的数据内容进行还原。
- 最大监控策略：系统预先设定的默认策略，可以对审计系统所支持的所有协议的数据和网络行为进行监控。
- 默认策略：系统预先设定的默认策略，可以实现对 POP3、SMTP 和 WEBMAIL 的还原，还可以实现对其他系统所支持协议的监控。

默认采集策略的策略名后以“*”号标记，如下图所示。



说明

✧ 系统已定义的默认策略无法删除、编辑，只能查看和派生。

管理员可以根据需要添加新的采集策略，并查看或修改已有的策略，具体操作如下：

➢ 添加采集策略

1）选择 **审计策略** > **采集策略** > **策略定义**，点击右侧的“添加策略”按钮，进入“新建策略”页面，如下图所示。

2）输入“策略名”，选择需要采集的数据所采用的协议类型，界面中显示了各协议默认的端口号，可以设置这些协议的其他常用端口号，在“时间组名”和“IP 组名”

中选择需要采集数据的时间范围和地址范围，字段的下拉列表中显示了用户在对象定义中已定义的时间组对象和 IP 组对象。

如果仅需要对数据访问的操作行为进行监控，则选中“监控”按钮。

如果需要对访问的数据内容进行还原，则选中“还原”按钮。

3）设置完成后，点击“确定”按钮，系统提示“添加策略成功”，该采集策略将被添加到策略列表中。

- 派生采集策略

管理员也可以选择派生采集策略，即在已定义策略上的基础上进行简单的修改生成新的采集策略，这种方法能快速定义采集策略，同时也适用于初次定义采集策略的管理员。

- 查看/修改/删除采集策略

管理员可以查看策略的详细信息，或者修改和删除策略，在相应的策略后点击“查看”、“编辑”和“删除”按钮。

- 导入/导出采集策略

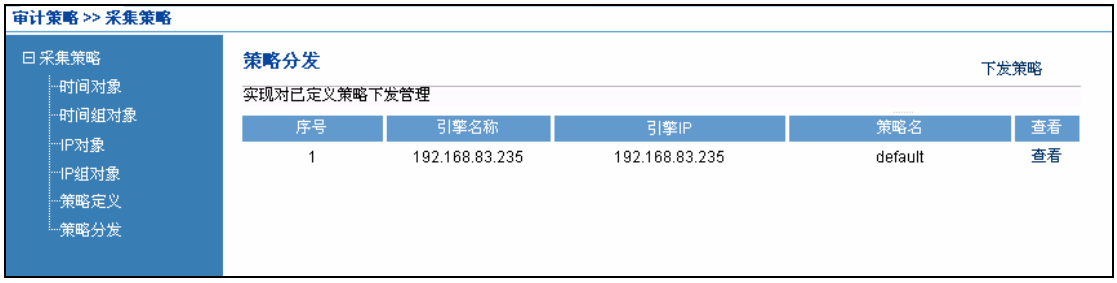
可以对已配置好的采集策略进行导出操作，当管理中心重新安装后，将已导出的采集策略直接导入系统，而不必再重新配置策略。具体的操作请参见4.6策略管理。

4.2.2 下发采集策略

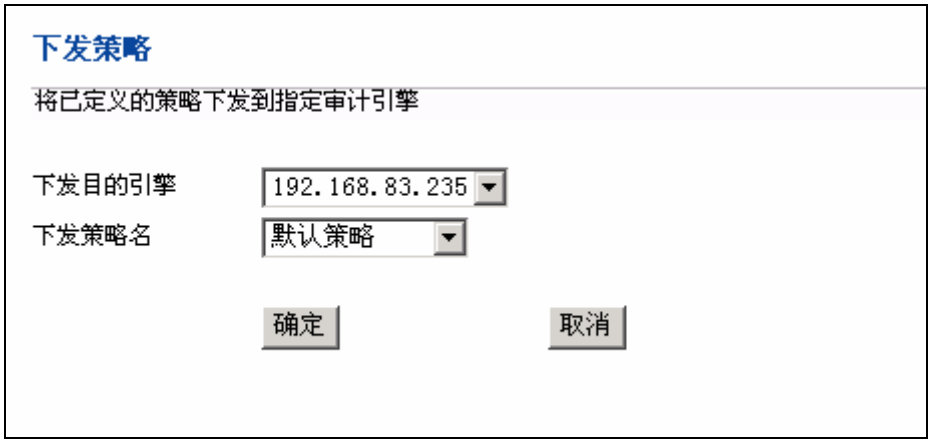
管理员可以为不同的审计引擎下发不同的采集策略，同一审计引擎只匹配一条采集策略，当修改采集策略后，管理员需要重新下发策略，新的采集策略将取代原策略生效。

策略下发的操作如下：

1）选择 **审计策略 > 采集策略 > 策略分发**，进入“策略分发”界面，显示已下发到审计引擎的策略，如下图。



2）点击右侧的“下发策略”按钮，弹出如下界面。



3）选择“目的引擎”和“策略名”，在下拉列表中显示了在系统中已定义的引擎名和策略名。

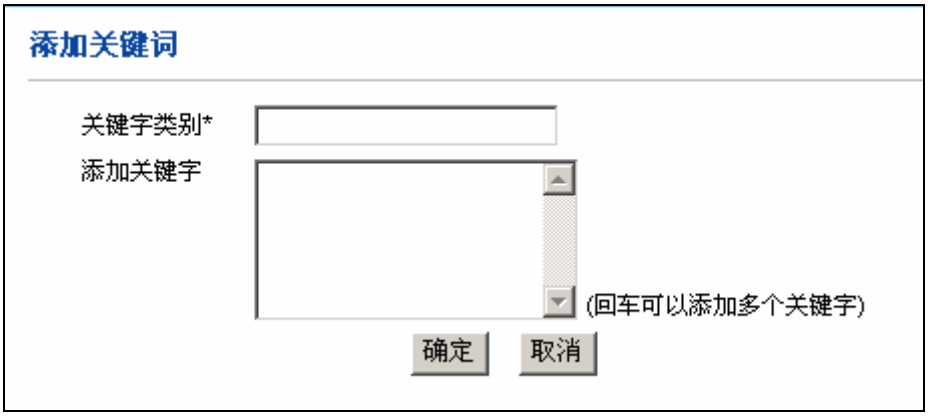
4）点击“确定”，系统将提示重启引擎，选择 **系统管理 > 重启引擎**，在对应的引擎项中点击“重启引擎“后，采集策略将在审计引擎中生效。

4.3 关键词策略配置

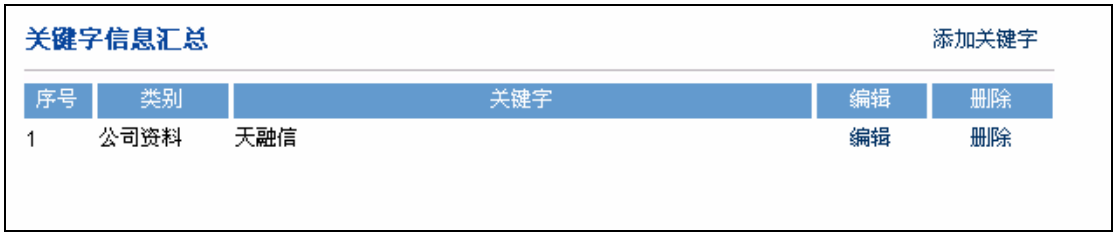
关键词审计首先需要管理员预先设定关键词库，并将关键词策略下发到数据中心，数据中心将根据用户定义的时间范围和关键词对数据库和硬盘中存储的数据信息进行分析和查找。

设置关键词策略的具体步骤描述如下：

1）设置关键词。选择 **审计策略 >关键词策略 >关键词管理**，并在右侧界面中点击“添加关键词”，进入添加关键词页面，如下图所示。



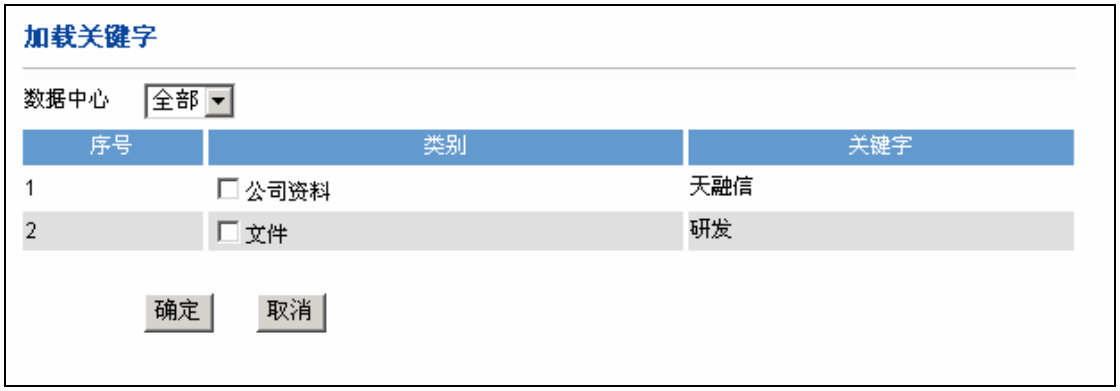
设置关键词的类别，并输入关键词，可以输入一个或多个关键词（利用回车符分隔多个关键词），点击“确定”即可看到新的关键词已添加到关键词的列表中，如下图所示。



如果要修改或删除已有的关键词，点击该条关键词对应的“修改”或“删除”即可。

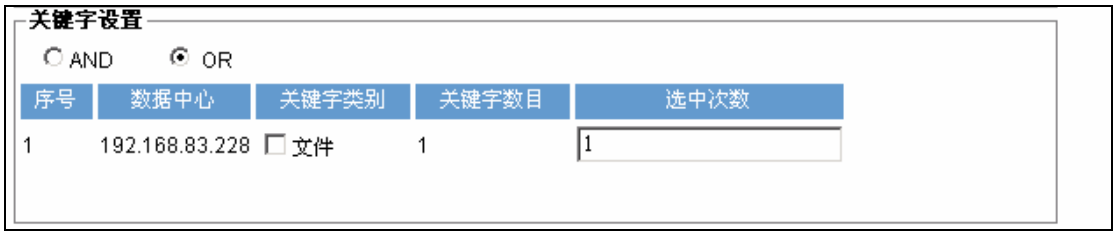
2）关键词策略分发。选择 **审计策略 > 关键词策略 > 关键词分发，**右侧界面显示已下发的关键词，如下图所示。

点击“下发关键字”可以下发关键词策略，弹出如下界面。



选择要下发关键字的数据中心，并选择要下发的关键字。点击“确定“，系统将提示“下发成功”。

3）下发成功后，选择 **安全审计 >内容审计 >关键字审计**,在右侧界面中可以查看到所有已经下发的关键词策略。



网络卫士安全审计系统还提供了关键词的导入、导出功能，只需在“策略管理”部分设置导入、导出策略为“关键词策略”便可，具体的操作请参见4.6策略管理。

4.4 报警策略配置

网络卫士安全审计系统定义了不同的报警策略，对于匹配报警策略的操作按照设定的响应方式报警，并向数据中心发送报警日志，管理员可在管理中心按照设定的条件查看实时报警日志。

用户在下发报警策略前，必须先配置和下发响应方式，如果报警策略中包含未下发的响应方式，该策略将无法下发。

4.4.1 定义响应方式

管理员可以设定阻断、邮件和联动的报警响应方式，根据需要可以设置其中的一种或多种，在报警策略定义中选择已下发的响应方式，审计引擎将根据策略中的方式响应，同时记录报警响应日志。

网络卫士安全审计系统通过自身阻断以及与防火墙联动的方式，可以及时阻止敏感信息的泄漏和非法的网络访问，同时支持邮件报警方式，各响应方式的工作机制如下：

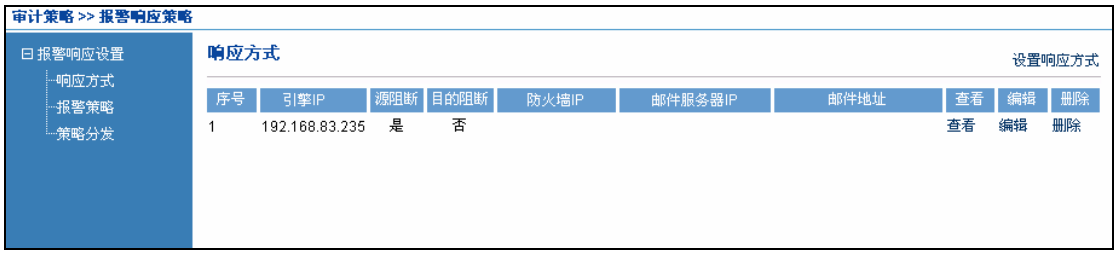
阻断：当信息在网上传输时，如果与管理员设定的报警策略匹配时，系统会自动阻断该信息的传输，导致非法信息发送失败。分为源阻断和目的阻断。

联动：联动实现了安全产品之间的信息互通，网络卫士安全审计系统支持基于TOPSEC 协议的联动功能，当匹配报警策略时，向指定防火墙发出通知报文，防火墙生成动态规则实现对非法行为的控制和阻断。

邮件：当产生报警事件时，将通知信息发往指定邮件服务器的指定邮箱，管理员可以据此监控非法行为。

设置响应方式的操作如下：

1）选择 **审计策略 > 报警响应策略 > 响应方式**，进入“响应方式”界面，界面中将显示已经配置的响应方式。



2）点击右侧的“设置响应方式”，弹出如下对话框。

3）设置阻断、联动和邮件响应方式的参数，各参数的说明如下表所示。

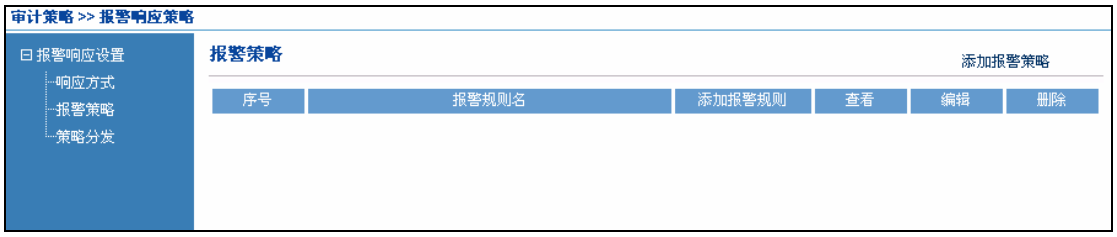
参数	说明
引擎	发起响应的审计引擎的 IP 地址。
阻断设置	指触发响应后，采取的阻断方式，可选“源阻断”和“目的阻断”。
联动设置	当响应方式为联动时，需要设置防火墙联动响应参数，包括防火墙 IP 地址、密钥和认证方式。
邮件响应设置	当响应方式为邮件响应时，需要设置邮件响应的参数，包括邮件服务器 IP、端口号、email 地址、主题。
邮件认证	如果邮件需要认证，输入认证的用户名和密码信息。

4.4.2 定义报警策略

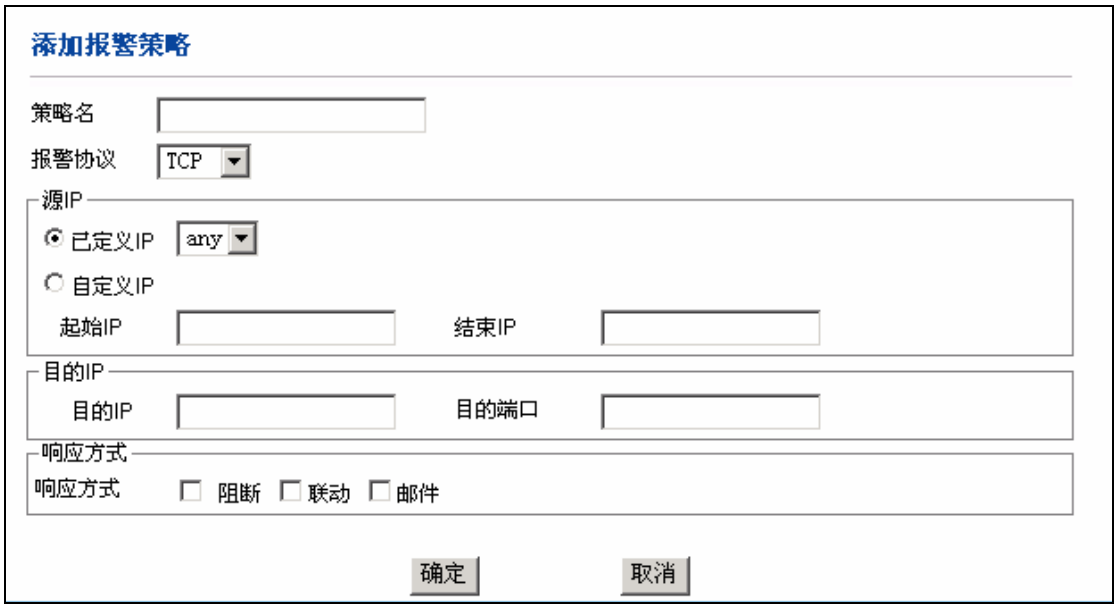
报警策略定义了当数据匹配哪些规则时将触发报警，并定义了报警响应的方式，管理员可以定义不同的报警策略，并将报警策略下发到审计引擎，审计引擎收到匹配策略的数据时将按照设定的响应方式做出响应。

定义报警策略的步骤如下：

1）选择 **审计策略 > 报警响应策略 > 报警策略**，进入“报警策略”界面，如下图所示。



2）点击“添加报警策略”按钮，进入“添加报警策略”界面，如下图所示，可以定义一条新的报警策略。



3）输入策略名，定义响应方式、源、目的地址和端口号，各参数的说明如下表。

参数	说明
策略名	报警策略的名称。
报警协议	设置报警消息采用的协议，可选 TCP、UDP 和 ICMP。
源 IP	定义触发报警策略的源IP，在此用户可选择已经定义的IP对象组，也

	可以自定义IP地址段。关于IP对象组的定义请参见4.1.4 IP组设置
目的 IP	定义触发报警策略的目的 IP 地址。
目的端口	定义触发报警策略的目的端口。
响应方式	触发响应时选择的响应方式，包括阻断、联动和邮件。每种响应方式对应的参数都在定义响应方式时设定，具体设置请参见“4.4.1定义响应方式”。

4) 点击“确定”，新添加的报警策略将显示在报警策略列表中。

如果需要为某个报警策略添加多条报警规则，在该条策略后点击“添加”按钮，可以定义不同的报警规则。

管理员可以对已定义的报警策略进行查看、修改和删除操作。

说明

- ✧ 每个报警策略包含多个报警规则，用户可以在一个策略中定义多个报警规则。

4.4.3 下发报警策略

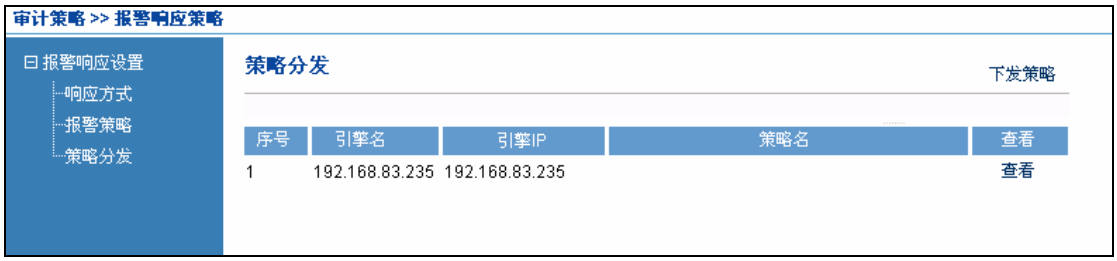
管理员可以为不同的审计引擎下发不同的报警策略，每个审计引擎匹配一条报警策略。如果需要修改策略，管理员需要重新下发策略，新的报警策略将取代原策略生效。

说明

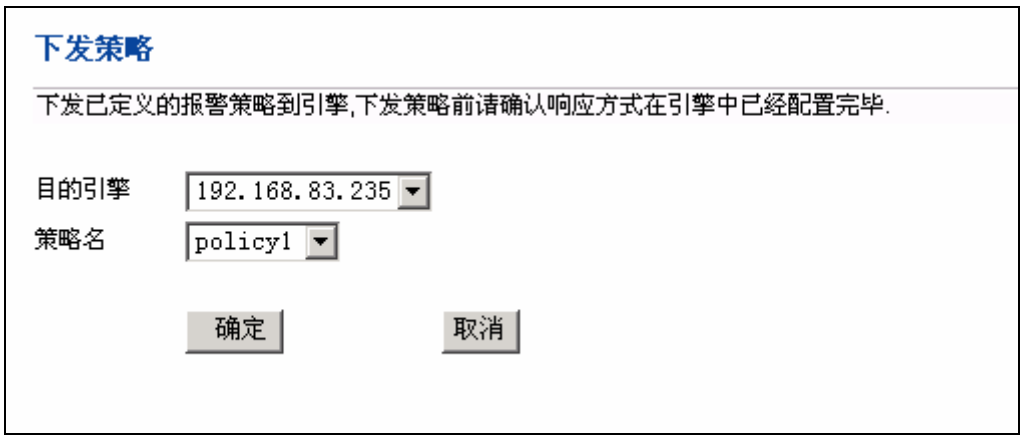
- ✧ 下发报警策略前，用户需要确定该策略对应的响应方式已在引擎上配置，否则无法下发该策略。

下发报警策略的步骤如下：

1）选择菜单 **审计引擎 > 报警响应策略 > 策略分发**，进入“策略分发”界面，显示已经下发报警策略的审计引擎。



2）点击右侧的下发策略按钮，进入“下发策略”界面，如下图所示。



3）选择“目的引擎”和“策略名”，下拉列表中显示了已定义的引擎和策略名。

4）点击“确定”按钮，系统提示需要重启审计引擎，重启后策略将生效。

4.5 流量监控策略配置

流量监控策略定义了系统监控流量的 IP 地址范围和采样间隔，审计引擎将按照采样间隔对策略定义范围内的 IP 的数据流量进行统计，并将统计数据传入数据中心，为管理中心提供实时的流量监控信息。

提示

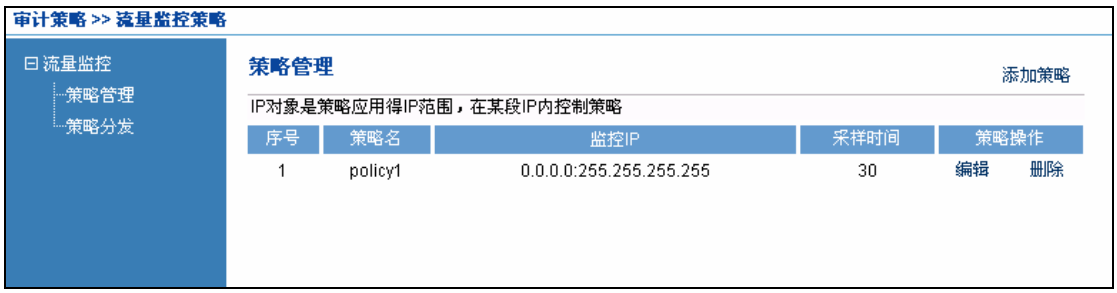
- ✧ 流量监控策略需要数据库支持大容量的数据存储，在定义策略前，请先确认数据库的存储性能。

4.5.1 定义流量监控策略

管理员可以在流量监控策略中定义需要监控的审计引擎采集口的流量或某机器的进出数据流量，也可以定义监控某地址段范围内所有设备的数据流量。

定义流量监控策略的步骤如下：

1）选择 **审计策略 > 流量监控策略 > 策略管理**，进入策略管理页面，显示系统已经设置的流量监控策略。



2）点击右侧的“添加策略”按钮，进入“监控设置”页面，可以定义一条新的流量监控策略，如下图所示。

3）输入策略名称，定义采样时间和 IP 地址段。

4）点击“提交”按钮，则新定义的流量监控策略将被添加到策略列表中，管理员可以修改和删除策略。

4.5.2 下发流量监控策略

不同的审计引擎可以下发不同的流量监控策略，审计引擎将对匹配策略的设备的数据流量进行采样，并将统计数据发送的数据中心。

下发流量监控策略的操作如下：

1）选择 **审计策略 > 流量监控策略 > 策略分发**，进入策略分发页面。

2）点击右侧的“下发策略”按钮，弹出如下对话框。

3）在“引擎”和“策略名”中选择要下发策略的引擎名和策略名，参数的下拉列表中显示了系统中已定义的引擎名和策略名。

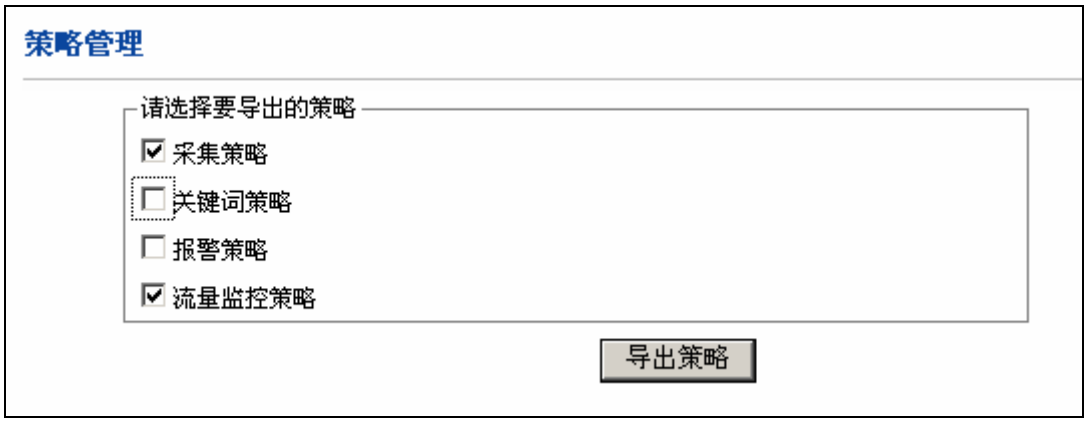
4）点击“下发策略”，系统提示需要重启审计引擎，重启后策略将生效。

4.6 策略管理

策略管理主要提供了策略导入、导出的功能，帮助用户在系统故障时可以快速的维护和恢复网络卫士安全审计系统。

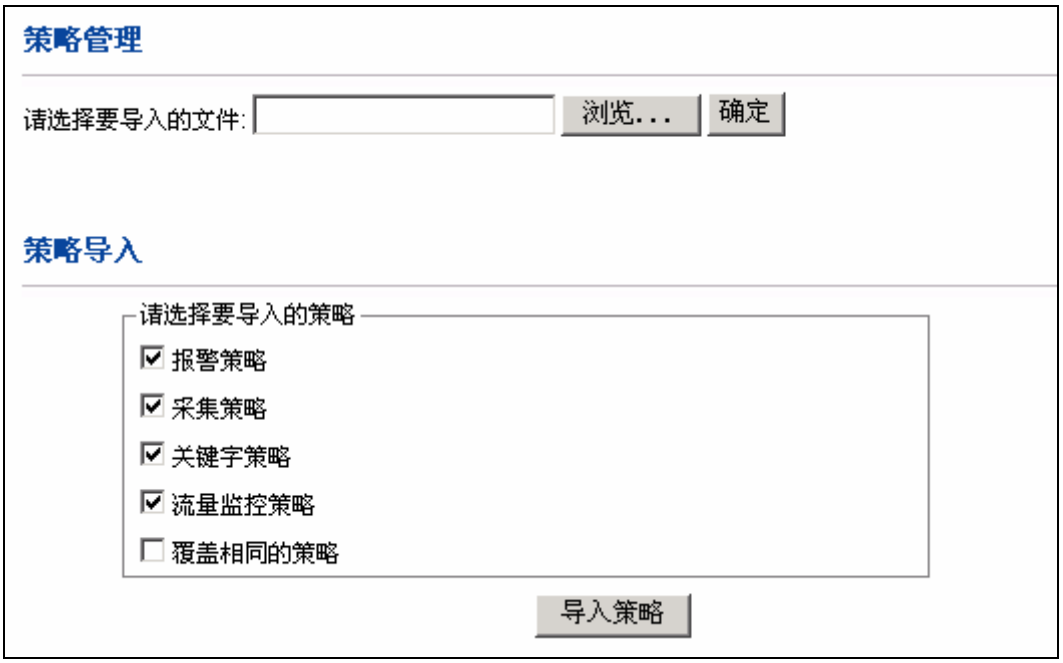
导入/导出策略的具体操作如下：

1）策略导出。选择 **审计策略 > 策略管理 > 策略导出**，进入导出策略页面，如下图所示。



选择要导出的策略的类别，并单击“导出策略”按钮，选择导出文件的路径，输入文件名称，系统将保存策略的配置文件。

2）策略导入。选择 **审计策略 > 策略管理 > 策略导入**，进入策略导入页面，如下图所示。



点击“浏览…”按钮选择要导入的策略文件，选择完成后点击“确定”，将显示要导入的策略类别，如果选择“覆盖相同的策略”，将覆盖系统当前的同类型的策略，点击“导入策略”，完成策略导入操作。

提示

- ✧ 策略下发后，在引擎上生效但没有保存在引擎上，引擎重起后，该配置失效，需要用户手动保存策略配置才能够永久生效。关于保存策略配置的具体操作请参见3.6.2引擎配置保存。
- ✧ 如果在配置策略成功但还没有保存策略配置时发现策略错误，可以重新启动审计引擎返回上次的配置状态。

5 安全审计功能

网络卫士安全审计系统支持多种典型应用的全面审计，并支持多种审计方式，还可以根据用户设定的条件生成行为统计报表和流量统计报表。网络卫士安全审计系统还提供同类产品中少有的网络内容还原功能，能针对常用的多种应用协议，比如HTTP、FTP、SMTP、POP3、Telnet、Webmail、QQ、MSN 等进行内容恢复，能完全真实地记录通信的全部过程与内容，并将其进行回放。此功能对于了解攻击者的攻击过程、监控内部网络中的用户是否滥用网络资源、发现未知的攻击具有重要和积极的作用。

本章描述如何进行网络应用的安全审计，包括如下几种审计方式：

- 行为审计——记录用户的网络行为，但不能记录用户网络行为所涉及的内容，例如用户访问http://www.sina.com网站时，行为审计只能记录用户曾经访问过此网站，但是并不记录用户访问的网页内容。
- 内容审计——记录用户与网络行为相关的所有数据内容，内容审计支持网络数据的完全还原，后期可以进行内容审计、取证，包括内容回放和关键词审计。
- 流量统计报表——通过对历史流量统计分析，对重要 IP 进行流量监测，并绘制出直观的流量曲线图，有效发现网上出现的异常流量。
- 行为统计报表——通过行为统计分析，发现网络中潜在的危险。支持多种条件的统计分析。

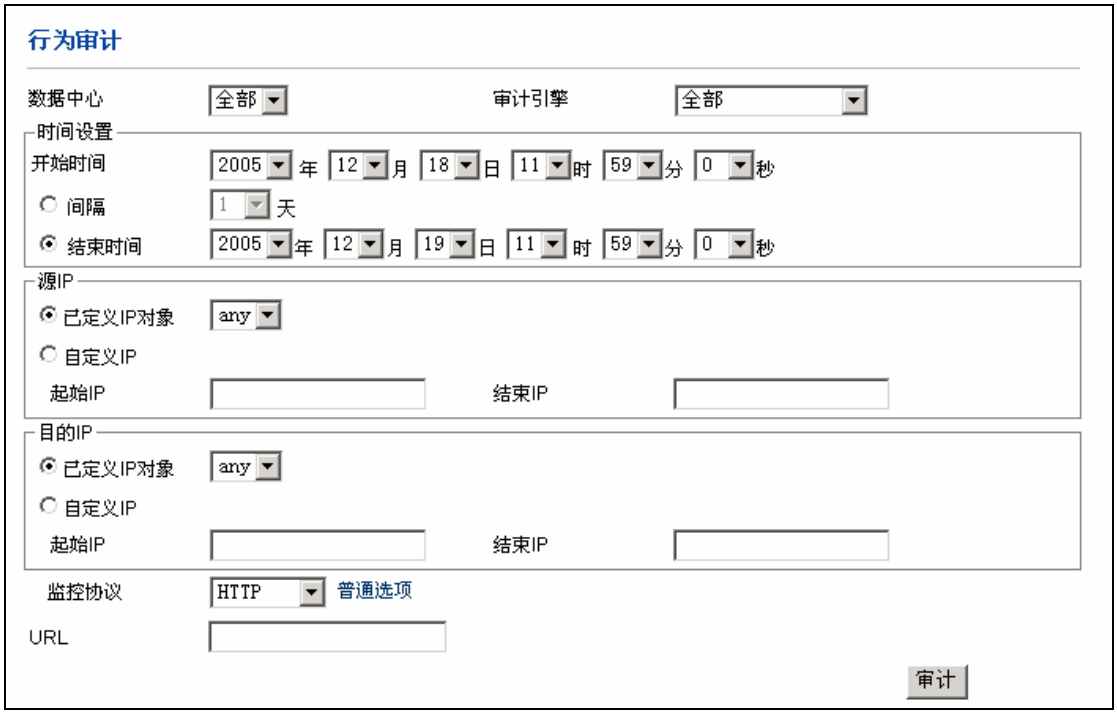
5.1 行为审计

行为审计用于对用户的网络行为进行记录和分析，包括用户网络行为数据的采集和分析。行为审计技术不仅是简单的数据记录和查询，而且可以在广泛采集网络信息的基础上对数据进行过滤、聚合、统计与分析，并以直观的形态展示数据，是网络管理者得力的决策助手。

网络卫士安全审计系统支持对以下协议进行行为审计：HTTP、FTP、SMTP、POP3、WEBMAIL、TELNET、MSN、QQ、MMS、RTSP。

行为审计的具体设置和操作如下：

1）选择 **安全审计 > 行为审计**，进入行为审计页面，如下图所示。



2）通过下拉框选择数据中心和审计引擎。

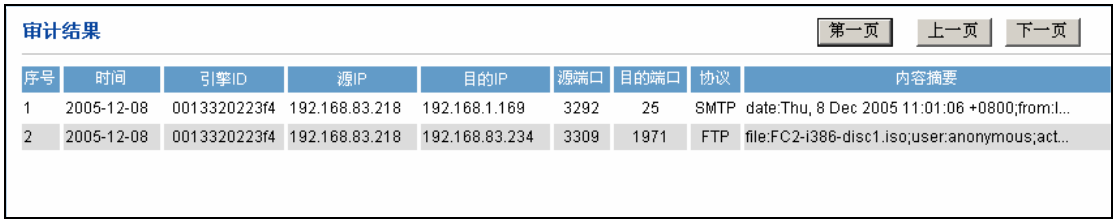
3）设置要审计哪个时间段的网络行为，即设置开始时间和结束时间。也可以通过设置开始时间和间隔来确定时间段，例如开始时间为 2005 年 1 月 1 日 0 时 0 分 0 秒，间隔为 1 天，表示审计从 2005 年 1 月 1 日 0 时 0 分 0 秒到 2005 年 1 月 2 日 0 时 0 分 0 秒这段时间内的网络行为。

4）设置网络行为的源IP。IP可以从下拉框中选择已经定义的IP对象，也可以自定义起始IP和结束IP，关于IP对象的定义请参见4.1.3 IP对象设置。

5）设置网络行为的目的 IP。

6）设置行为审计的协议类型，选择某一具体协议，点击“还原协议”右边的“高级选项”可以更详细的设置还原协议的相关参数。

7）设置完成后，点击“审计”将会显示详细的审计结果，如下图所示。



序号	时间	引擎ID	源IP	目的IP	源端口	目的端口	协议	内容摘要
1	2005-12-08	0013320223f4	192.168.83.218	192.168.1.169	3292	25	SMTP	date:Thu, 8 Dec 2005 11:01:06 +0800;from:l...
2	2005-12-08	0013320223f4	192.168.83.218	192.168.83.234	3309	1971	FTP	file:FC2-i386-disc1.iso;user:anonymous;act...

审计结果中包含了行为时间、源 IP、目的 IP、协议、审计引擎、内容摘要等详细信息。

8）点击上图中的“第一页”、“上一页”、“下一页”可以翻页显示审计结果。

5.2 内容审计

网络卫士安全审计系统支持对以下协议进行内容为审计：HTTP、FTP、SMTP、POP3、WEBMAIL、TELNET、MSN。管理员可以通过设置关键词、时间范围等条件，使得审计系统可以自动快速的进行全文检索。匹配成功的内容将以醒目字体颜色显示。

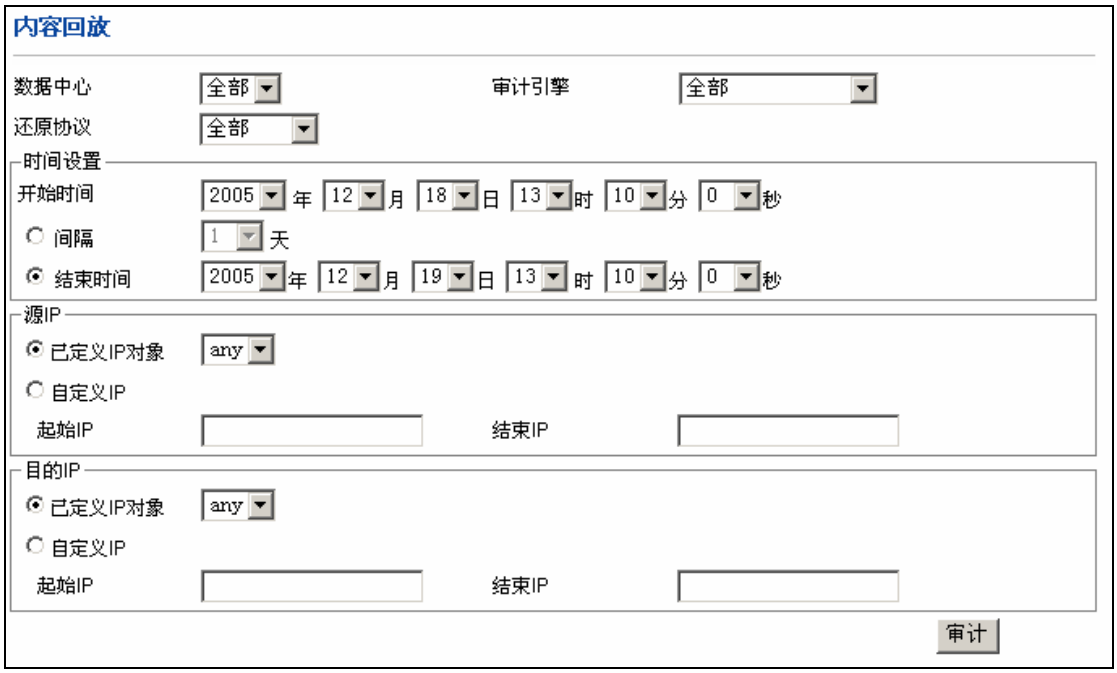
网络卫士安全审计系统的内容审计主要包含两部分的功能：内容回放和关键词审计，下面将分别介绍二者的具体设置和使用。

5.2.1 内容回放

在网络卫士安全审计系统中，由审计引擎发送过来的经过协议分析后的数据流以文件的形式存储在磁盘上，内容回放负责对这些文件进行还原，从应用协议数据中获得真正的内容数据。内容回放支持对 HTTP、FTP、SMTP、POP3、TELNET、WEBMAIL、MSN 等协议的还原，对于 SMTP、POP3、WEBMAIL 等邮件收发协议，支持多种编码方式（Base64、Quoted-Printable、UTF-7、UTF-8 等）、多种压缩格式（Zip、Rar、Arj、Gz 等；支持多达十四层的压缩）的附件内容的回放。

内容回放的具体设置方法如下：

1）选择 **安全审计 > 内容审计 > 内容回放**，右侧弹出如下界面，用于设定内容审计的条件。



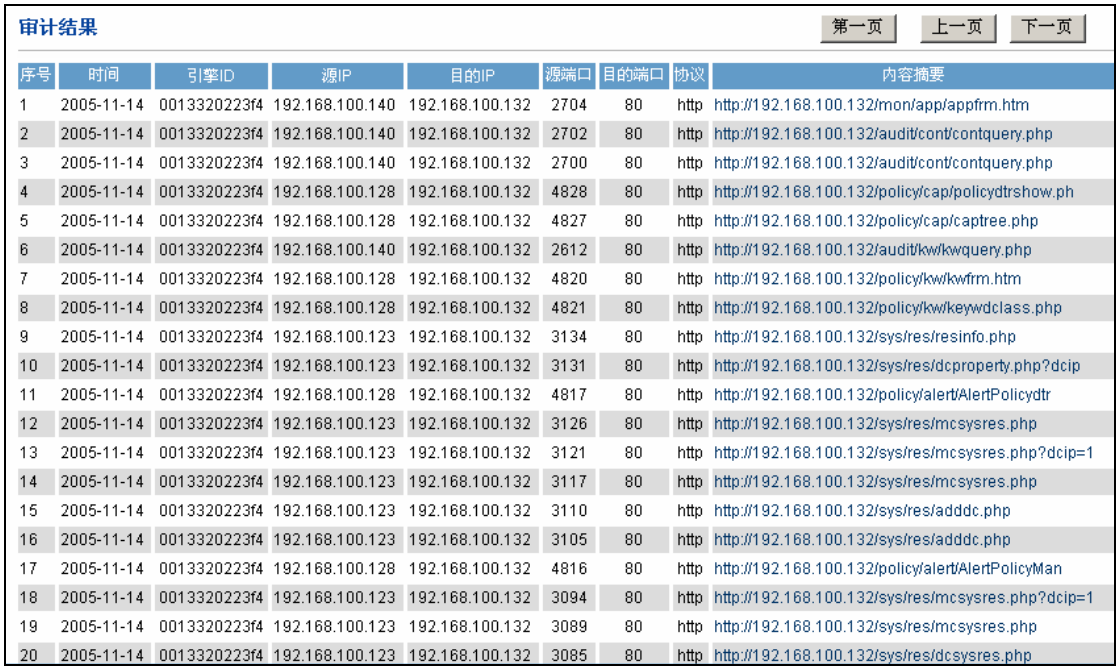
2）选择数据中心和审计引擎。由于一个管理中心可以管理多个数据中心，一个数据中心又存储多个审计引擎的数据，所以需要选择对哪个数据中心所存储的哪个审计引擎采集的数据文件进行内容审计。

3）设置对哪个协议的数据进行内容审计。

4）设置对哪个时间段的数据进行内容审计。“开始时间”表示时间段的起始值；“间隔”表示开始时间后几天；“结束时间”表示时间段的终止值。

5）设置源 IP 和目的 IP 地址应满足何种约束条件时对网络传输数据包进行内容审计。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）点击“审计”，则在窗口显示审计结果，包括时间、引擎 ID、源 IP、源端口、目的 IP、目的端口、使用的协议、内容摘要信息，如下图所示。



审计结果

第一页 上一页 下一页

序号	时间	引擎ID	源IP	目的IP	源端口	目的端口	协议	内容摘要
1	2005-11-14	0013320223f4	192.168.100.140	192.168.100.132	2704	80	http	http://192.168.100.132/mon/app/appfrm.htm
2	2005-11-14	0013320223f4	192.168.100.140	192.168.100.132	2702	80	http	http://192.168.100.132/audit/cont/contquery.php
3	2005-11-14	0013320223f4	192.168.100.140	192.168.100.132	2700	80	http	http://192.168.100.132/audit/cont/contquery.php
4	2005-11-14	0013320223f4	192.168.100.128	192.168.100.132	4828	80	http	http://192.168.100.132/policy/cap/policydtrshow.ph
5	2005-11-14	0013320223f4	192.168.100.128	192.168.100.132	4827	80	http	http://192.168.100.132/policy/cap/captree.php
6	2005-11-14	0013320223f4	192.168.100.140	192.168.100.132	2612	80	http	http://192.168.100.132/audit/kw/kwquery.php
7	2005-11-14	0013320223f4	192.168.100.128	192.168.100.132	4820	80	http	http://192.168.100.132/policy/kw/kwfrm.htm
8	2005-11-14	0013320223f4	192.168.100.128	192.168.100.132	4821	80	http	http://192.168.100.132/policy/kw/keywdclass.php
9	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3134	80	http	http://192.168.100.132/sys/res/resinfo.php
10	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3131	80	http	http://192.168.100.132/sys/res/dcproperty.php?dcip
11	2005-11-14	0013320223f4	192.168.100.128	192.168.100.132	4817	80	http	http://192.168.100.132/policy/alert/AlertPolicydtr
12	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3126	80	http	http://192.168.100.132/sys/res/mcsysres.php
13	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3121	80	http	http://192.168.100.132/sys/res/mcsysres.php?dcip=1
14	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3117	80	http	http://192.168.100.132/sys/res/mcsysres.php
15	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3110	80	http	http://192.168.100.132/sys/res/adddc.php
16	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3105	80	http	http://192.168.100.132/sys/res/adddc.php
17	2005-11-14	0013320223f4	192.168.100.128	192.168.100.132	4816	80	http	http://192.168.100.132/policy/alert/AlertPolicyMan
18	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3094	80	http	http://192.168.100.132/sys/res/mcsysres.php?dcip=1
19	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3089	80	http	http://192.168.100.132/sys/res/mcsysres.php
20	2005-11-14	0013320223f4	192.168.100.123	192.168.100.132	3085	80	http	http://192.168.100.132/sys/res/dcsysres.php

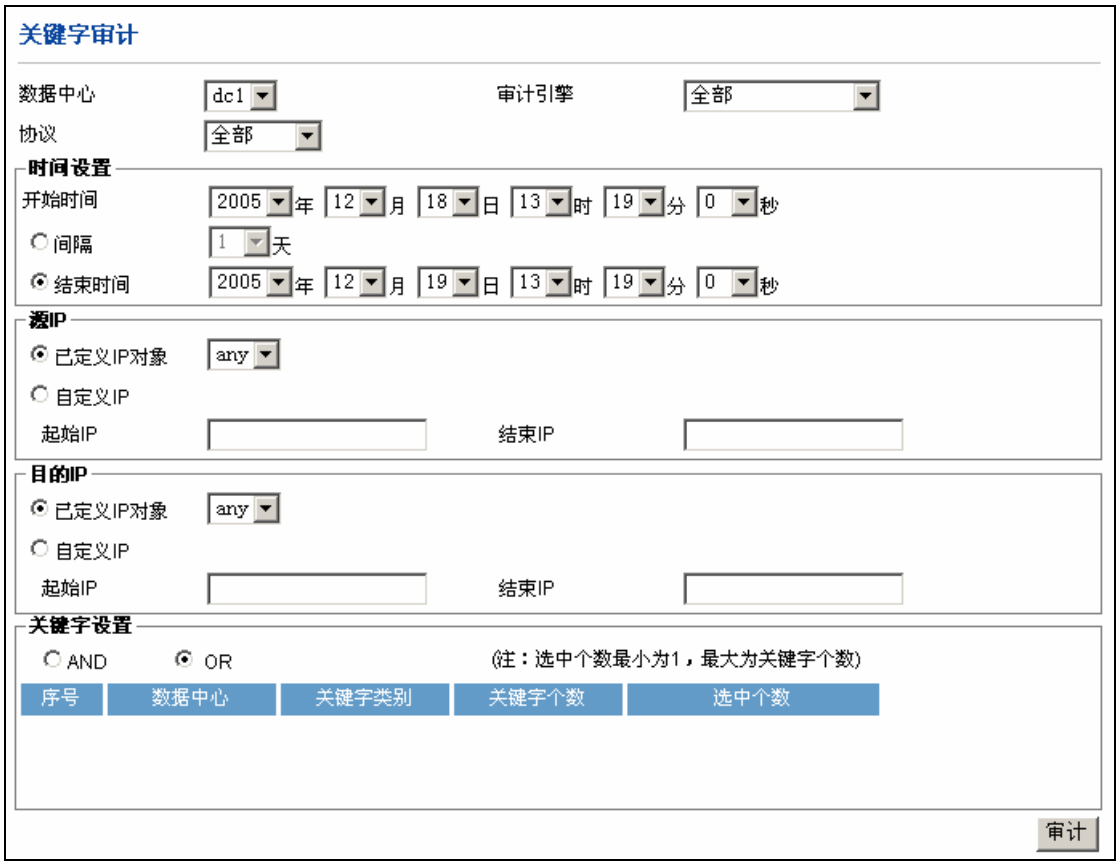
点击“第一页”、“上一页”、“下一页”可以翻页显示审计结果。点击某条内容摘要，则可以在新的窗口显示内容的详细信息，如下图所示为还原的用户登录的网页。

5.2.2 关键词审计

关键词策略成功下发后，通过审计引擎根据关键词策略对网络中的数据包进行采集和分析，将分析后的数据流发送给数据中心以文件的形式存储在磁盘上，由数据中心负

责对这些文件进行还原，之后进行基于还原内容的关键词审计。关于关键词策略的设置和下发请参见4.3关键词策略配置。

1）选择 **安全审计 > 内容审计 > 关键字审计**，右侧弹出如下界面，用于设定关键字查询的条件。



2）选择数据中心和审计引擎。由于一个管理中心可以管理多个数据中心，一个数据中心又存储多个审计引擎的数据，所以需要选择对哪个数据中心所存储的哪个审计引擎采集的数据文件进行内容关键字审计。

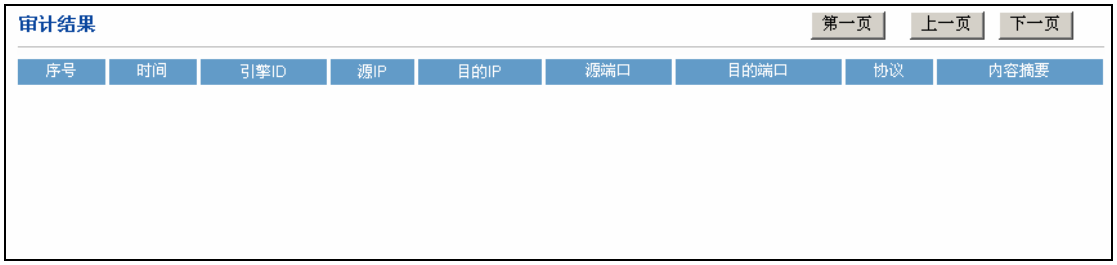
3）选择对哪个协议的内容进行关键词审计。可以选择对 HTTP、FTP、SMTP、POP3、TELNET、WEBMAIL、MSN 其中一种或所有协议的内容进行关键词审计。

4）设置对哪个时间段的存储内容进行审计。“开始时间”表示时间段的起始值，“间隔”表示开始时间后几天，“结束时间”表示时间段的终止值。

5）设置数据包的源 IP 地址和目的 IP 地址应满足的条件。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）设置关键词匹配条件。在“关键字设置”一栏显示了管理中心下发给当前数据中心的关键词策略，可以选择一条或多条关键词策略作为该次查询的匹配条件。如果设置了多个关键词类别，“AND”表示只有选择的关键词类别均匹配时才认为该还原内容中标，“OR”表示只要所选择的关键词类别中有一类匹配就认为该还原内容中标。关键词定义，请参见**错误！未找到引用源。错误！未找到引用源。**。

7）点击“审计”，则在窗口显示审计结果，包括时间、引擎 ID、源 IP、源端口、目的 IP、目的端口、使用的协议、内容摘要信息，如下图所示。



5.3 行为统计报表查看

网络卫士安全审计系统支持对 HTTP、FTP、SMTP、POP3、WebMail、MMS、RTSP、MSN、QQ、TELNET 协议的行为进行综合分析统计和每种协议的单独分析统计功能。根据管理员指定组合条件，如时间、协议、IP 地址或 IP 地址网段等，网络卫士安全审计系统可以生成用户需要的行为统计报表，管理员可以在此统计查看网络中各协议操作统计数据，也可以针对 IP 地址，对某台主机的操作进行某段时间的全程监控，如一天、一个星期、一月等，查看关于该主机上网情况、收发邮件统计、网络聊天内容、上传和下载数据、访问其他主机情况等等。还向管理员提供报表打印功能，可以将报表在纸介质上打印或打印为 pdf 文件以备日后查看。

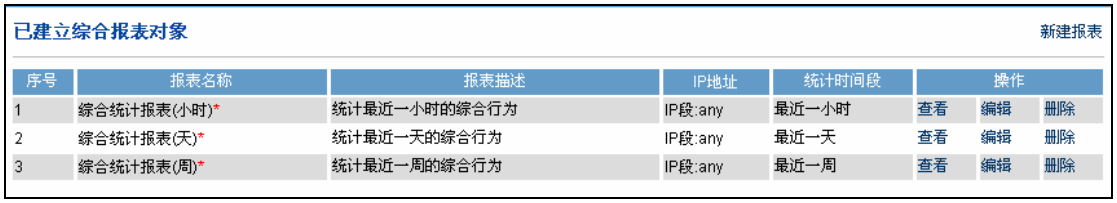
- 综合统计分析：统计和查看指定时间段内的指定 IP 地址（段）某种协议的综合使用情况。
- Web 浏览统计分析（HTTP）：统计和查看被监测网络中所有用户浏览的 WEB 页面情况。
- 文件下载(FTP)：统计和查看用户利用 FTP 协议在服务器上的操作情况
- 远程登录（TELNET）：统计和查看用户使用 TELNET 协议情况。

- 电子邮件（POP3、SMTP、WEB MAIL）：统计和查看被监测网络中所有用户收发的电子邮件情况。
- 即时聊天（MSN、QQ 等）：统计和查看用户利用 MSN、QQ 进行网上聊天情况。
- 流媒体（MMS、RTSP）：统计和查看用户访问的流媒体情况。

5.3.1 综合统计分析

综合统计分析用于全面地统计和分析网络中审计系统所支持的所有协议的网络行为和数据状况。具体设置方法如下：

1）选择 **安全审计 > 行为统计报表 > 综合统计分析**，右侧页面中显示了已建立的综合报表对象的列表。



2）点击“新建报表”，弹出如下界面。

3）选择从哪个数据中心读取数据以形成统计报表和欲统计行为的协议类型。

4）设置生成报表的时间间隔：如果选择“最近”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、天报表、周报表、月报表、季度报表。如果选择“某一时间”，则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

5）设置参与行为统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）选择 IP 方式：设置选定的地址段作为源 IP 还是目的 IP。

7）指定在报表中显示 IP 还是 IP 段。

8）如果只是想查看报表信息，则点击“生成报表”按钮即可。

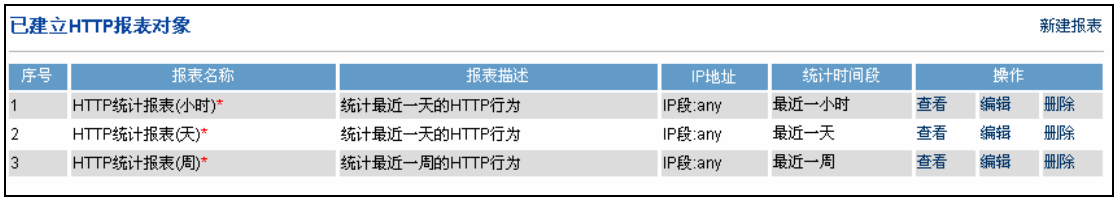
9）如果要保存生成的报表对象，则必须填写报表名称和报表描述信息，然后点击“保存条件并生成报表”按钮可以保存生成报表的条件，并同时生成报表。保存后会在已建立的综合报表对象中显示该报表对象。

10）点击“查看”可以查看已经生成的报表。点击“编辑”可以对生成报表的条件进行编辑修改。点击“删除”则可以删除该报表。

5.3.2 HTTP 统计分析

HTTP 统计分析用于统计和分析被监测网络网段中所有用户浏览 WEB 页的行为，包括：各种文件，如 HTML 文件、图像文件、文本文件等，并能根据用户指定条件，生成报表。设置方法如下。

1）选择 **安全审计 > 行为统计报表 > HTTP统计分析**，右侧显示已生成的HTTP报表对象。



2）点击“新建报表”，弹出如下界面。

3）选择从哪个数据中心读取数据以形成统计报表。

4）设置生成报表的时间间隔： 如果选择“最近”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、天报表、周报表、月报表、季度报表。如果选择“某一时间”，则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

5）设置参与行为统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）选择 IP 方式：设置选定的地址段作为源 IP 还是目的 IP。

7）指定在报表中显示 IP 还是 IP 段。

8）设定URL：设置要生成报表的URL，例如设置为http://www.sina.com时，报表的内容将只是与此URL相关的网络行为和数据。当高级统计设置的项目不做设置时，系统将会统计所有行为。

9）如果只是想查看 WEB 页面的访问信息，则点击“生成报表”按钮即可。点击“保存条件并生成报表”按钮可以在保存生成报表的条件的同时生成报表，保存后会在已建立的 HTTP 报表对象中显示该报表对象。

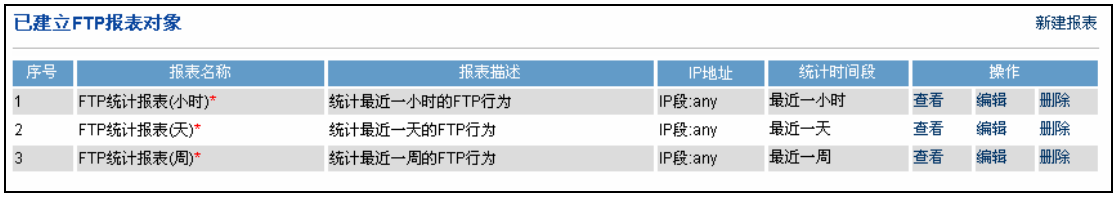
10）点击“查看”可以查看已经生成的报表。点击“编辑”可以对生成报表的条件进行编辑修改。点击“删除”则会删除该报表。

5.3.3 FTP 统计分析

FTP 统计分析用于统计和分析被监测网络中所有用户访问 FTP 的行为，包括访问 FTP 服务器的用户名、口令等信息。并能根据指定条件，生成报表。

具体的设置方法如下：

1）选择 **安全审计 > 行为统计报表 > FTP统计分析**，右侧显示已建立的FTP报表列表。



2）点击“新建报表”，弹出如下界面。

3）选择从哪个数据中心读取数据以形成统计报表。

4）设置生成报表的时间间隔：如果选择“最近”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、天报表、周报表、月报表、季度报表。如果选择“某一时间”，则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

5）设置参与行为统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）选择 IP 方式：设置选定的地址段作为源 IP 还是目的 IP

7）指定在报表中显示 IP 还是 IP 段。

8）设定用户名和文件名：设置用户名和文件名为网络行为的过滤条件。例如设置用户名和文件名分别为 user 和 file 时，报表中将只会显示同时和二者有关的网络行为数据。当高级统计设置的项目不做设置时，系统将会统计所有行为。

9）如果只是想查看 FTP 协议的操作统计信息，则点击“生成报表”按钮即可。点击“保存条件并生成报表”按钮可以在保存生成报表的条件的同时生成报表。保存成功后可以在已建立的 FTP 报表对象中显示该报表对象。

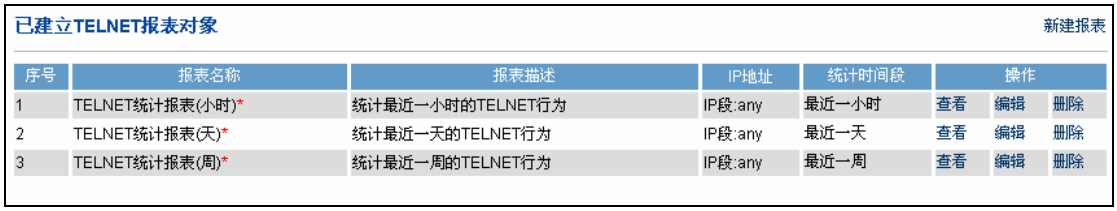
10）点击“查看”可以查看已经生成的报表。点击“编辑”可以对生成报表的条件进行编辑修改。点击“删除”则会删除该报表。

5.3.4 TELNET 统计分析

TELNET 统计分析用于统计和分析被监测网络中所有用户使用 TELNET 协议的行为，包括访问 TELNET 服务器的用户名、口令等信息。并能根据指定条件，生成报表。

具体的设置方法如下：

1）选择 **安全审计 > 行为统计报表 > TELNET统计分析**，右侧显示已建立的TELNET报表列表。



2）点击“新建报表”，弹出如下界面。

3）选择从哪个数据中心读取数据以形成统计报表。

4）设置生成报表的时间间隔： 如果选择“最近”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、天报表、周报表、月报表、季度报表。如果选择“某一时间”，则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

5）设置参与行为统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）选择 IP 方式：设置选定的地址段作为源 IP 还是目的 IP

7）指定在报表中显示 IP 还是 IP 段。

8）设定用户名：设置用户名为网络行为的过滤条件。例如设置用户名为 user 时，报表中将只会显示和 user 有关的网络行为数据。当高级统计设置的项目不做设置时，系统将会统计所有行为。

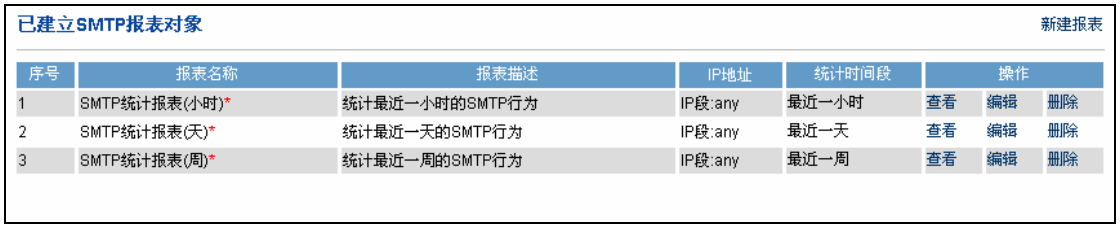
9）如果只是想查看 TELNET 协议的操作统计信息，则点击“生成报表”按钮即可。点击“保存条件并生成报表”按钮可以在保存生成报表的条件的同时生成报表。保存成功后可以在已建立的 TELNET 报表对象中显示该报表对象。

10）点击“查看”可以查看已经生成的报表。点击“编辑”可以对生成报表的条件进行编辑修改。点击“删除”则会删除该报表

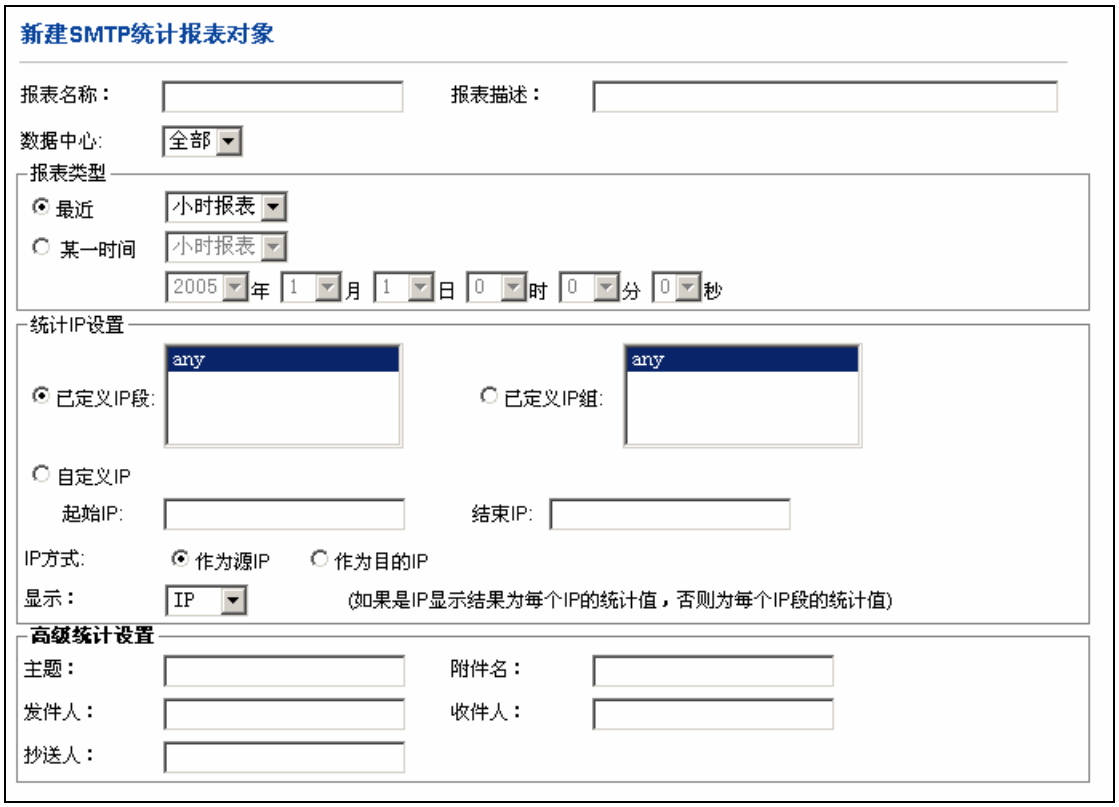
5.3.5 SMTP/POP3/WebMail 统计分析

电子邮件收发行为统计分析，主要包括 SMTP/POP3/WebMail 统计分析。能够完全统计和分析被监测网络中所有用户收发电子邮件的行为。其内容包括：收件人和发件人各自的邮件地址、收件人和发件人各自的 IP 地址、电子邮件的主题、电子邮件的内容等。下面以 SMTP 统计分析为例，具体说明设置方法。

1）选择 **安全审计 > 行为统计报表 > SMTP统计分析**，右侧显示已建立的SMTP报表对象的列表。



2）点击“新建报表”，弹出如下界面。



3）选择从哪个数据中心读取数据以形成统计报表。

4）设置生成报表的时间间隔：如果选择“最近”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、天报表、周报表、月报表、季度报表。如果选择“某一时间”，则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

5）设置参与行为统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）选择 IP 方式：设置已选定的地址段作为源 IP 还是目的 IP

7）指定在报表中显示 IP 还是 IP 段。

8）设定邮件主题、附件名、发件人、收件人、抄送人。当高级统计设置的项目不做设置时，系统将会统计所有行为。

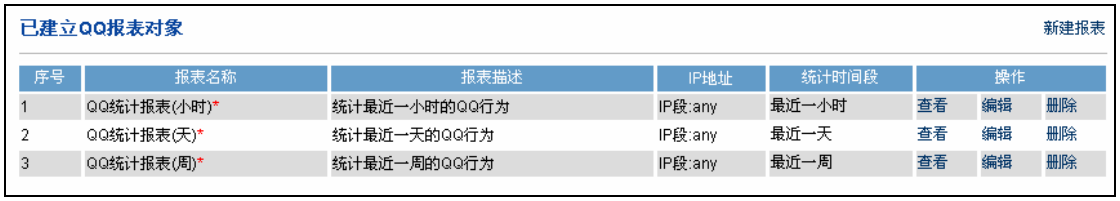
9）如果只是想查看 SMTP 的操作统计信息，则点击“生成报表”按钮即可。点击“保存条件并生成报表”按钮可以在保存生成报表的条件的同时生成报表。保存成功后可以在已建立的 SMTP 报表对象中显示该报表对象。

10）点击“查看”可以查看已经生成的报表。点击“编辑”可以对生成报表的条件进行编辑修改。点击“删除”则会删除该报表。

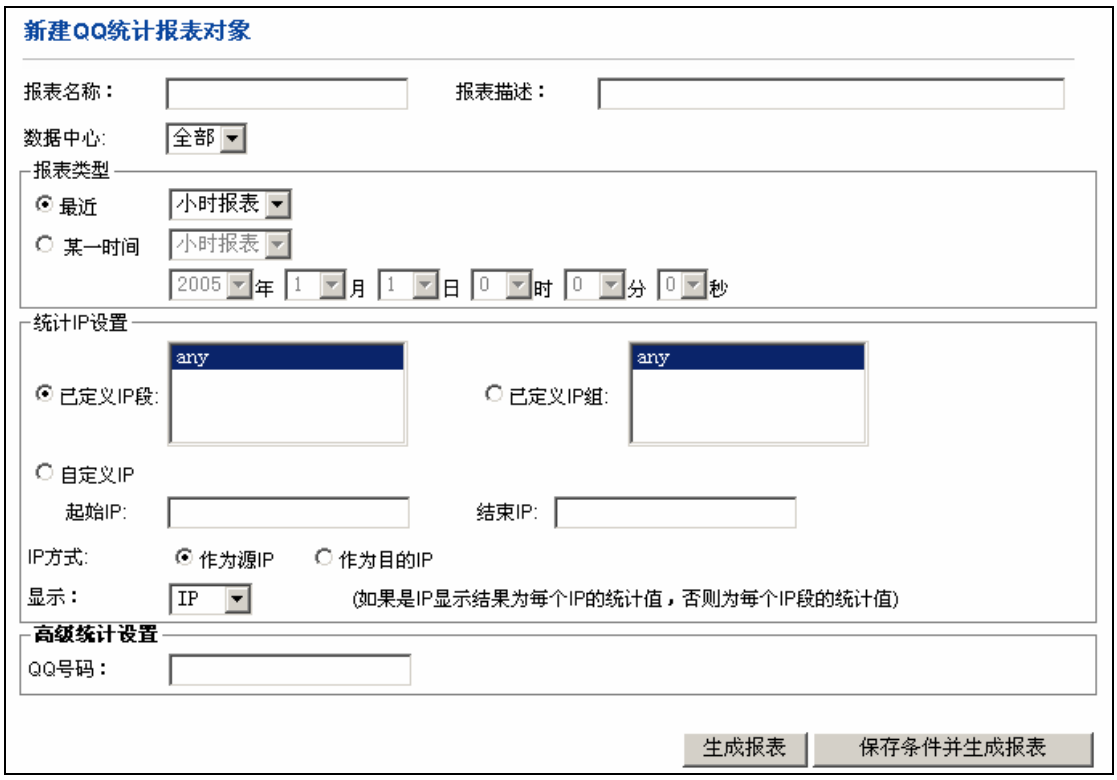
5.3.6 MSN/QQ 统计分析

内部员工在工作时间上网聊天可能违反规章制度，同时也是泄密的重要渠道。网络卫士安全审计系统支持对多种即时网络聊天协议内容的截获、记录、回放、归档。利用行为统计可以统计员工利用 MSN、QQ 聊天开始时间、结束时间、聊天对象，进而根据用户指定条件，生成报表。下面以 QQ 统计分析为例，具体说明设置方法。

1）选择 **安全审计 > 行为统计报表 > QQ统计分析**，右侧显示已建立的QQ报表对象的列表。



2）点击“新建报表”，弹出如下界面。



3）选择从哪个数据中心读取数据以形成统计报表。

4）设置生成报表的时间间隔： 如果选择“最近”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、天报表、周报表、月报表、季度报表。如果选择“某一时间”，则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

5）设置参与行为统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）选择 IP 方式：设置已选定的地址段作为源 IP 还是目的 IP.

7）指定在报表中显示 IP 还是 IP 段。

8）设定 QQ 的用户名作为过滤网络行为的条件。当高级统计设置的项目不做设置时，系统将会统计所有行为。

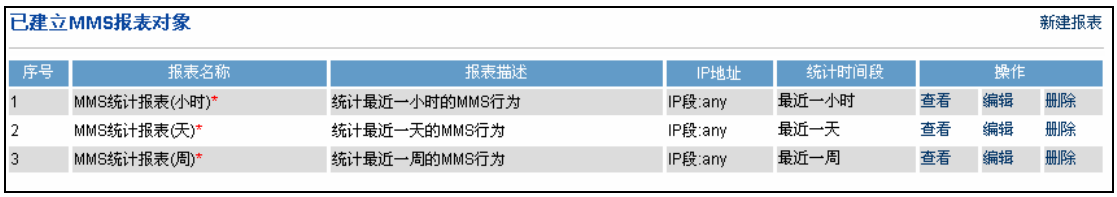
9）如果只是想查看 QQ 的操作统计信息，则点击“生成报表”按钮即可。点击“保存条件并生成报表”按钮可以在保存生成报表的条件的同时生成报表。保存成功后可以在已建立的 QQ 报表对象中显示该报表对象。

10）点击“查看”可以查看已经生成的报表。点击“编辑”可以对生成报表的条件进行编辑修改。点击“删除”则会删除该报表。

5.3.7 MMS/RTSP 统计分析

在网络上利用 RTSP (Realtime Streaming Protocol)或 MMS (Microsoft Media Server)协议实时流式传输音、视频等多媒体信息会占用大量的网络带宽，网络卫士安全审计系统支持对实时流媒体传输数据的行为进行统计分析，并可以根据设定条件生成报表，从而有利于管理人员及时快速了解网络带宽的使用情况。下面以 MMS 统计分析为例，具体说明设置方法。

1）选择 **安全审计 > 行为统计报表 > MMS统计分析RTSP统计分析**，右侧显示已建立的MMS报表对象的列表。



2）点击“新建报表”，弹出如下界面。

3）选择从哪个数据中心读取数据以形成统计报表。

4）设置生成报表的时间间隔：如果选择“最近”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的行为统计报表。如小时报表、天报表、周报表、月报表、季度报表。如果选择“某一时间”，则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行行为统计，开始时间可以精确到分钟。

5）设置参与行为统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。自定义时如果起始 IP 地址和结束 IP 地址相同，则认为是具体的主机 IP 地址。

6）选择 IP 方式：设置已选定的地址段作为源 IP 还是目的 IP。

7）指定在报表中显示 IP 还是 IP 段。

8）设定文件名作为过滤网络行为的条件。当高级统计设置的项目不做设置时，系统将会统计所有行为。

9）如果只是想查看 MMS 的操作统计信息，则点击“生成报表”按钮即可。点击“保存条件并生成报表”按钮可以在保存生成报表的条件的同时生成报表。保存成功后可以在已建立的 MMS 报表对象中显示该报表对象。

10）点击“查看”可以查看已经生成的报表。点击“编辑”可以对生成报表的条件进行编辑修改。点击“删除”则会删除该报表。

说明

- ✧ 网络卫士安全审计系统向管理员提供报表打印功能，可以将报表在纸介质上打印或打印为 pdf 文件以备日后查看。

5.4 流量统计报表查看

网络卫士安全审计系统不但能实时监控网络的数据流量，还能根据用户要求，统计历史流量信息，即统计网络中某一时间段（如一天，一周，一个月等）的总体流量和某一时间段的流量曲线图。而且，管理员可以选择查看哪一层的数据流量：总体流量、传输层流量或应用层流量。本功能有助于网络管理员即时了解网络连接和通信数据流量状

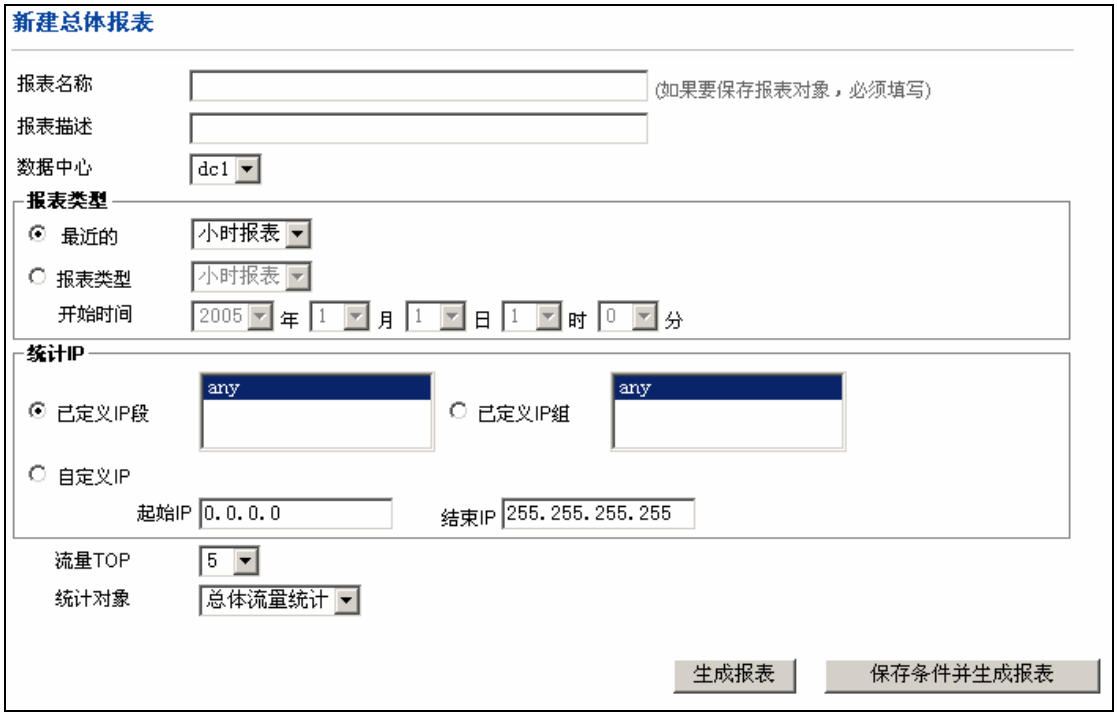
况，便于管理员监控和调节。系统还向管理员提供报表打印功能，可以将报表在纸介质上打印或打印为 pdf 文件以备日后查看。

5.4.1 总体流量统计

总体流量统计用于全面地统计和分析网络流量状况，显示网络中不同流量信息的变化、分布趋势。设置方法如下。

选择 **安全审计 > 流量统计报表 > 总体流量统计**，右侧显示已有的总体流量报表对象。

1）点击“新建报表”，弹出如下界面。



2）选择生成报表的时间间隔：如果选择“最近的”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、日报表、周报表、月报表、季度报表。否则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

说明

✧ 生成报表的开始时间只能从整点或半点开始。

3）设置从哪个数据中心读取数据以形成统计报表。

4）设置参与流量统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。

5）流量 TOP：显示审计引擎采集口采集到的排名前 5 位、10 位、20 位的流量。

6）指定统计对象：是统计总体流量、还是只统计进流量或出流量。

7）如果要保存生成的报表对象，则必须填写报表名称和报表描述信息。点击“生成报表”按钮即可查看报表内容。

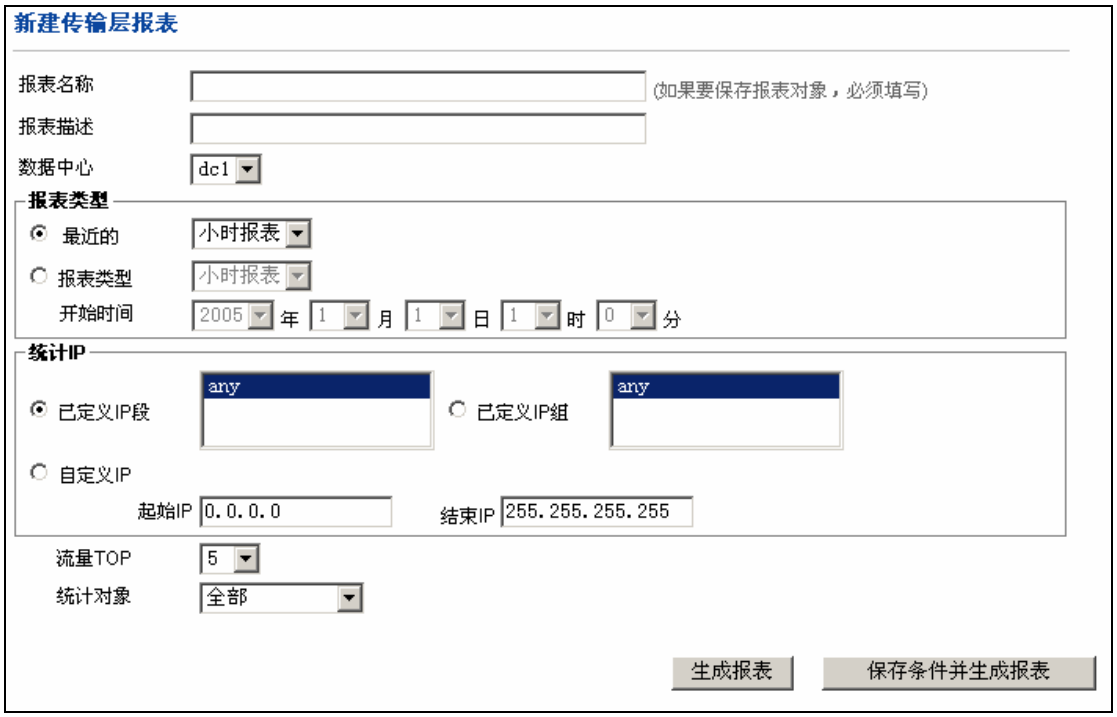
8）点击“保存条件并生成报表”按钮可以保存流量统计设定的条件，并同时生成报表。如图所示。

5.4.2 传输层流量统计

传输层流量统计用于统计和分析网络传输层的数据流量状况，显示网络中不同流量信息的变化、分布趋势。设置方法如下。

选择 **安全审计 > 流量统计报表 > 传输层流量统计**，右侧显示已有的传输层流量报表对象。

1）点击“新建报表”，弹出如下界面。



2）选择生成报表的时间间隔：如果选择“最近的”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、日天报表、周报表、月报表、季度报表。否则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

3）设置从哪个数据中心读取数据以形成统计报表。

4）设置参与流量统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。

5）设置流量 TOP：显示审计引擎采集口采集到的排名前 5 位、10 位、20 位的流量。

6）指定统计对象：是统计 TCP 流量、UDP 流量、ICMP 流量或其他流量。

7）如果要保存生成的报表对象，则必须填写报表名称和报表描述信息。如果只是想查看传输层流量信息，则点击“生成报表”按钮即可。

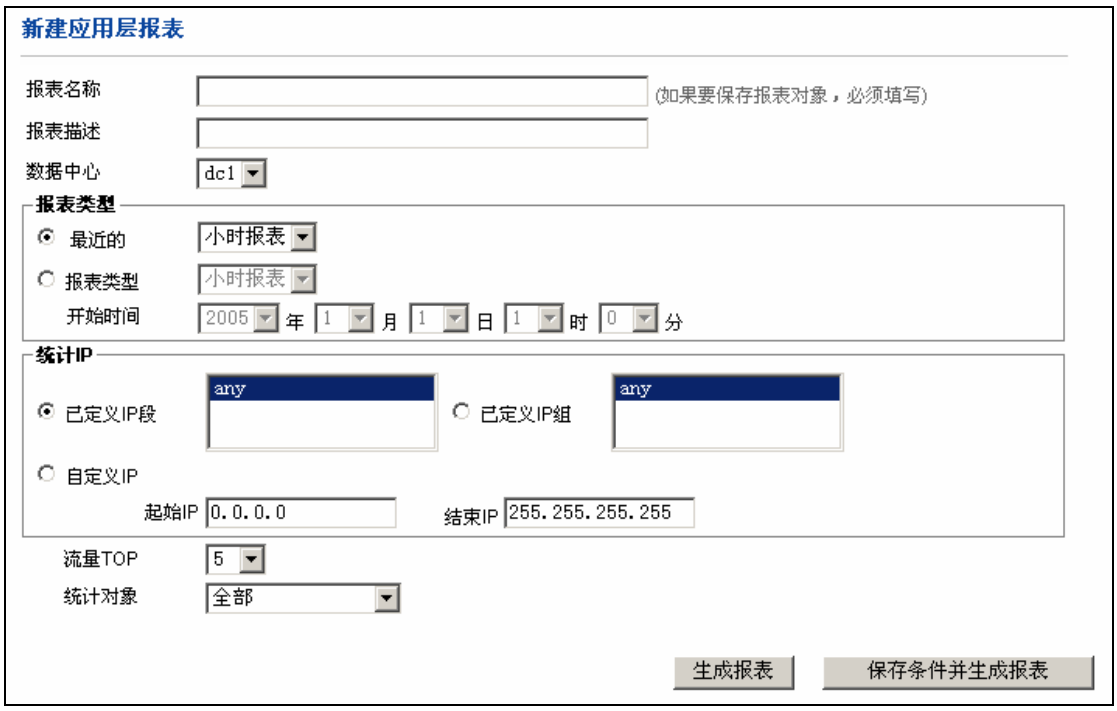
8）点击“保存条件并生成报表”按钮可以保存流量统计设定的条件，并同时生成报表。

5.4.3 应用层流量统计

应用层流量统计用于统计和分析网络应用层的数据流量状况，显示网络中不同流量信息的变化、分布趋势。设置方法如下。

选择 **安全审计 > 流量统计报表 > 应用层流量统计**，右侧显示已有的应用层流量报表对象。

1）点击“新建报表”，弹出如下界面。



2）选择生成报表的时间间隔：如果选择“最近的”选项，则以当前数据中心的时间为基点，根据设定时间间隔生成当前时间前一个小时、前一天、前一周、前一月或前一季度的流量统计报表。如小时报表、日报表、周报表、月报表、季度报表。否则需要设置生成该报表的具体开始时间，以设定的开始时间作为基准时间进行流量统计，开始时间可以精确到分钟。

3）设置从哪个数据中心读取数据以形成统计报表。

4）设置参与流量统计的地址段。可以选择已经定义的 IP 地址段或 IP 地址组，也可以自定义地址对象。

5）设置流量 TOP：显示审计引擎采集口采集到的排名前 5 位/10 位/20 位的流量。

6）指定统计对象：是统计 HTTP 流量、FTP 流量、TELNET 流量、SMTP 流量、POP3 流量、MSN 流量、NETBIOS 流量、WEBMIL 流量、MMS 流量、RTSP 流量或其它流量。

7）如果要保存生成的报表对象，则必须填写报表名称和报表描述信息。如果只是想查看总体流量信息，则点击“生成报表”按钮即可。

8）点击“保存条件并生成报表”按钮可以保存流量统计设定的条件并同时生成报表

说明

- ✧ 网络卫士安全审计系统向管理员提供报表打印和保存功能，可以将报表在纸介质上打印或保存为 pdf 文件以备日后查看。

6 实时监控功能

网络卫士安全审计系统为用户提供了实时、动态的监控功能，管理员可以根据需要，及时地了解网络中的各种动态信息。包括：

应用信息：通过应用监控，及时了解被监控网络中各种应用的访问情况，如：用户使用 MSN 通信的情况，或者用户使用 MMS 媒体服务的情况等，从而及时发现网络中不同应用的访问情况。

流量信息：通过流量监控，掌握整个网络中数据的流量趋势，并通过明细表查看的流量排位在前列的用户 IP。

报警信息：通过查看报警日志，了解哪些用户进行了非法访问。

在网络安全审计系统中，实时信息的查看是通过以下机制实现的：审计引擎与数据中心之间建立了实时通信，审计引擎定时主动向数据中心传送信息，包括实时报警信息、实时连接监控信息、和实时流量统计信息。管理员在管理中心按照设定的条件查看数据中心的保存的实时信息，并按照设定的刷新频率更新。

本章主要介绍了如何对各种信息进行实时监控，包括：

- 应用监控
- 流量监控
- 报警日志查询

6.1 应用监控

应用监控为用户提供了各种不同应用使用情况的实时信息，用户可以定义需要监控的协议类型，系统提供对常用的 10 种应用协议的监控，包括：HTTP、FTP、SMTP、POP3、TELENT、MSN、QQ、WEBMAIL、MMS 和 RTSP.

进行实时应用监控的操作如下：

1）选择 **实时监控 > 应用监控**，进入“应用监控”页面，如下图所示。

2)设置监控条件。

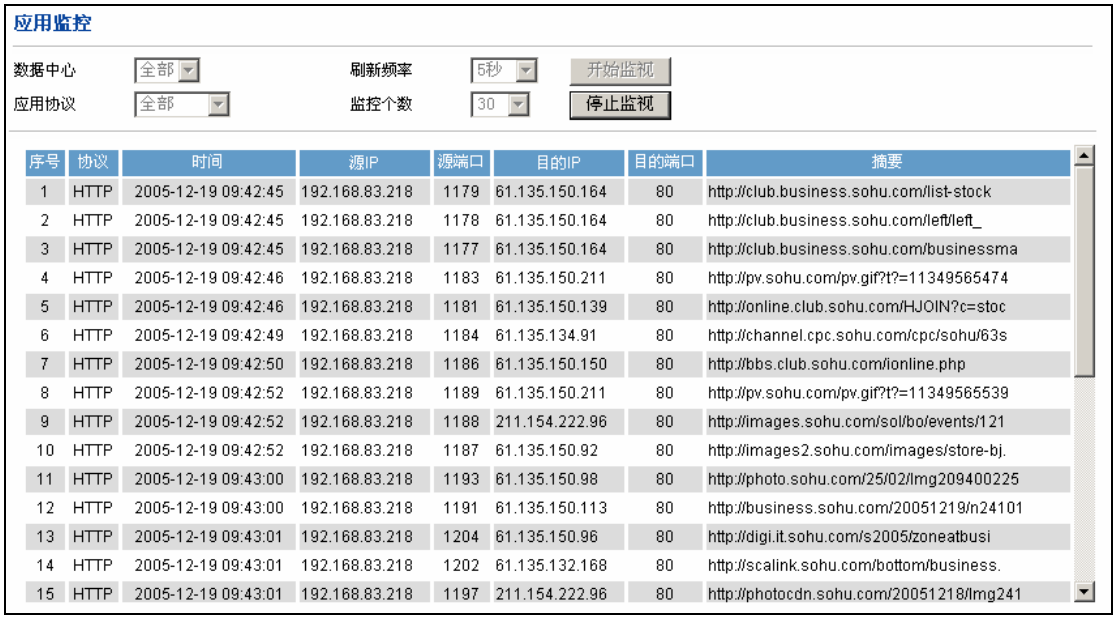
选择要监控的数据中心：每个管理中心可以监控多个数据中心，可以选择监控某个数据中心或者监控全部数据中心；

选择数据的实时刷新频率：系统设定了 5 秒、10 秒、20 秒和 30 秒的刷新频率。

选择应用协议：可以监控全部协议或某一指定的协议。

选择监控个数：指界面滚屏中最多显示的监控对象的个数，30、50、100。

3）点击“开始监控”，界面中将按照以上设置的监控条件显示被监控对象的信息，包括源 IP、源端口、目的 IP、目的端口和访问地址的摘要信息，如下图所示。



序号	协议	时间	源IP	源端口	目的IP	目的端口	摘要
1	HTTP	2005-12-19 09:42:45	192.168.83.218	1179	61.135.150.164	80	http://club.business.sohu.com/list-stock
2	HTTP	2005-12-19 09:42:45	192.168.83.218	1178	61.135.150.164	80	http://club.business.sohu.com/left/left_
3	HTTP	2005-12-19 09:42:45	192.168.83.218	1177	61.135.150.164	80	http://club.business.sohu.com/businessma
4	HTTP	2005-12-19 09:42:46	192.168.83.218	1183	61.135.150.211	80	http://pv.sohu.com/pv.gif?t?=11349565474
5	HTTP	2005-12-19 09:42:46	192.168.83.218	1181	61.135.150.139	80	http://online.club.sohu.com/HJOIN?c=stoc
6	HTTP	2005-12-19 09:42:49	192.168.83.218	1184	61.135.134.91	80	http://channel.cpc.sohu.com/cpc/sohu/63s
7	HTTP	2005-12-19 09:42:50	192.168.83.218	1186	61.135.150.150	80	http://bbs.club.sohu.com/ionline.php
8	HTTP	2005-12-19 09:42:52	192.168.83.218	1189	61.135.150.211	80	http://pv.sohu.com/pv.gif?t?=11349565539
9	HTTP	2005-12-19 09:42:52	192.168.83.218	1188	211.154.222.96	80	http://images.sohu.com/sol/bo/events/121
10	HTTP	2005-12-19 09:42:52	192.168.83.218	1187	61.135.150.92	80	http://images2.sohu.com/images/store-bj.
11	HTTP	2005-12-19 09:43:00	192.168.83.218	1193	61.135.150.98	80	http://photo.sohu.com/25/02/img209400225
12	HTTP	2005-12-19 09:43:00	192.168.83.218	1191	61.135.150.113	80	http://business.sohu.com/20051219/n24101
13	HTTP	2005-12-19 09:43:01	192.168.83.218	1204	61.135.150.96	80	http://digi.it.sohu.com/s2005/zoneatbusi
14	HTTP	2005-12-19 09:43:01	192.168.83.218	1202	61.135.132.168	80	http://scalink.sohu.com/bottom/business.
15	HTTP	2005-12-19 09:43:01	192.168.83.218	1197	211.154.222.96	80	http://photocdn.sohu.com/20051218/img241

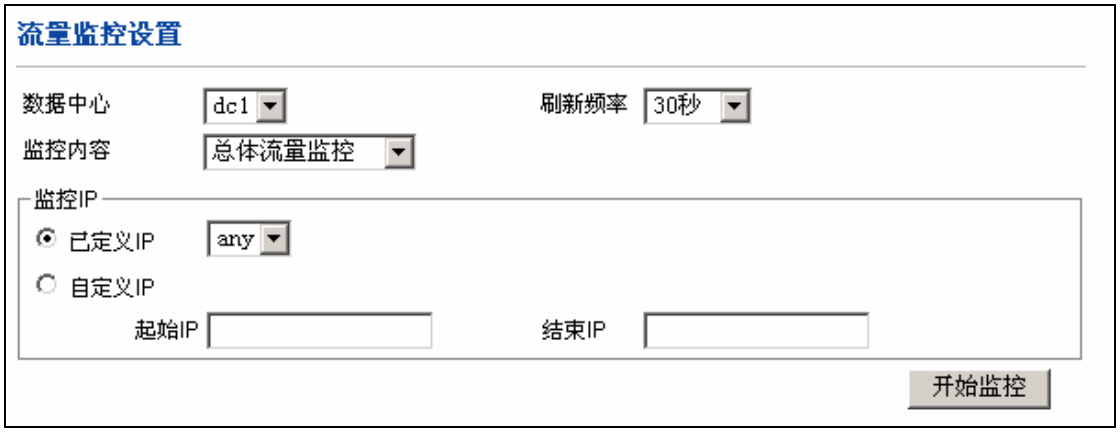
4）点击“停止监控”按钮，界面将停止在当前的监控状态，即不再进行实时刷新。

6.2 流量监控

流量监控提供了被监控 IP 地址范围内所有对象的进出数据的流量统计信息，系统可以分别对总体流量、传输层流量和应用层流量进行监控，并以直观的流量趋势图显示了系统的总体数据流量状况。

进行流量监控的操作如下：

1）选择 **实时监控** > **流量监控**，进入“流量监控”设置页面，如下图所示。

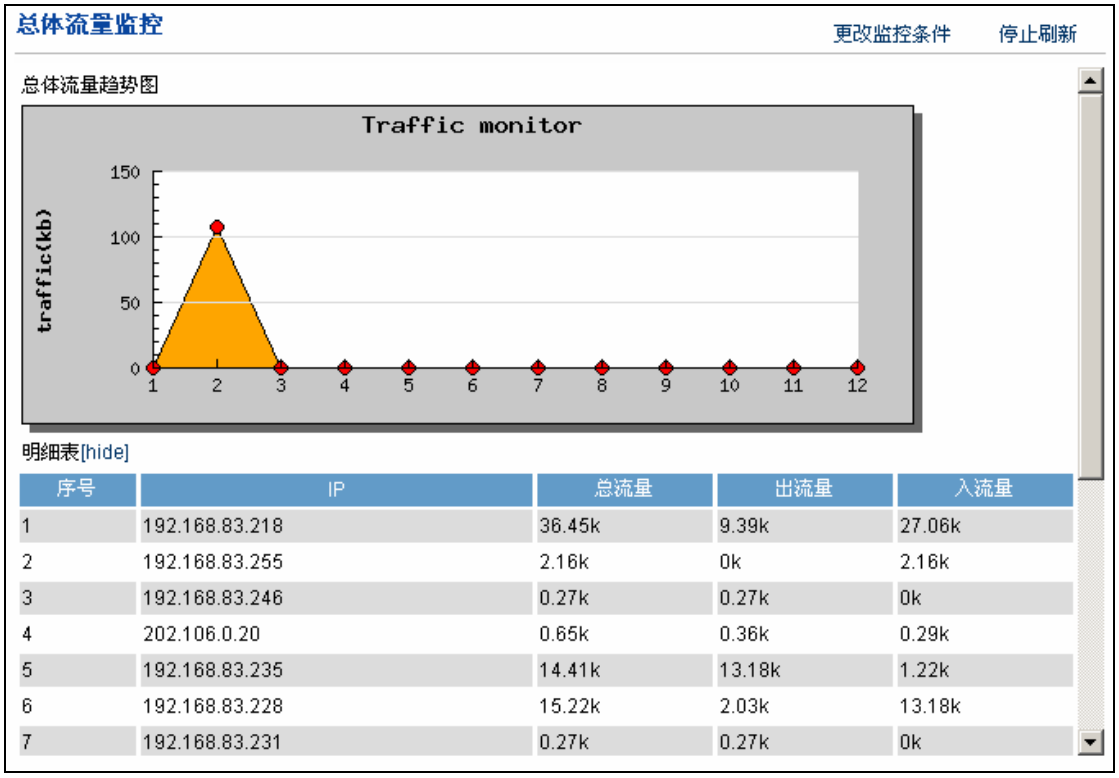


2）设置监控范围和刷新频率。

选择要监控的数据中心和实时刷新频率，并设定被监控的 IP 地址范围，可以选择系统中已设定的地址段或自定义 IP 地址范围，所选择的 IP 地址范围要与数据中心象对应，即该 IP 段中对象的信息要存储在指定的数据中心中。

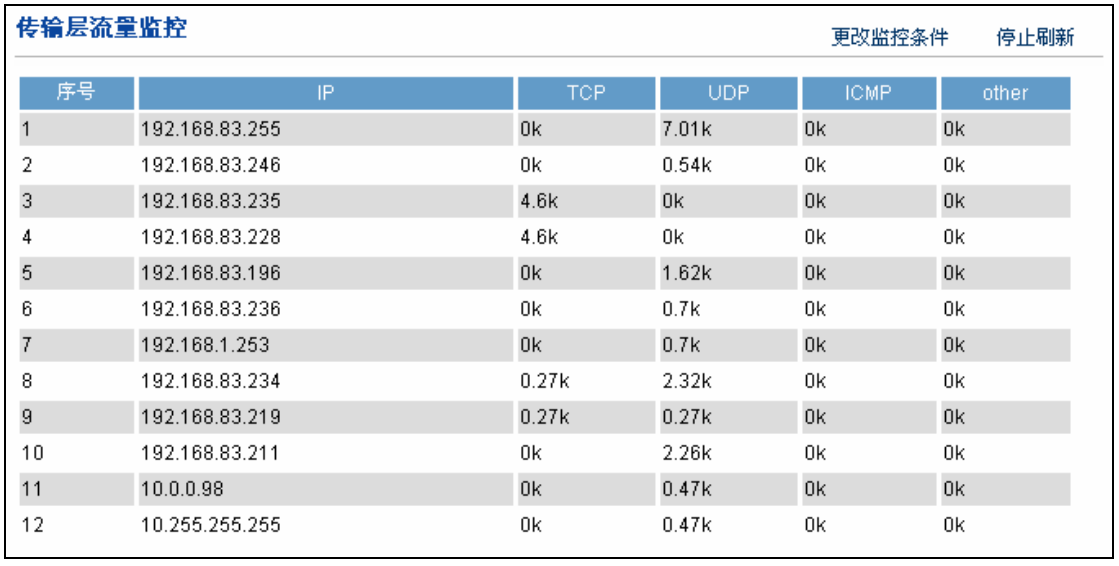
3）设置监控内容。

在“监控内容”下拉列表中，选择“总体流量监控”，点击“开始监控”，出现实时监控界面。点击趋势图下的“Hide”按钮，将隐藏每个被监控 IP 进、出流量及总流量的详细信息，如下图所示。



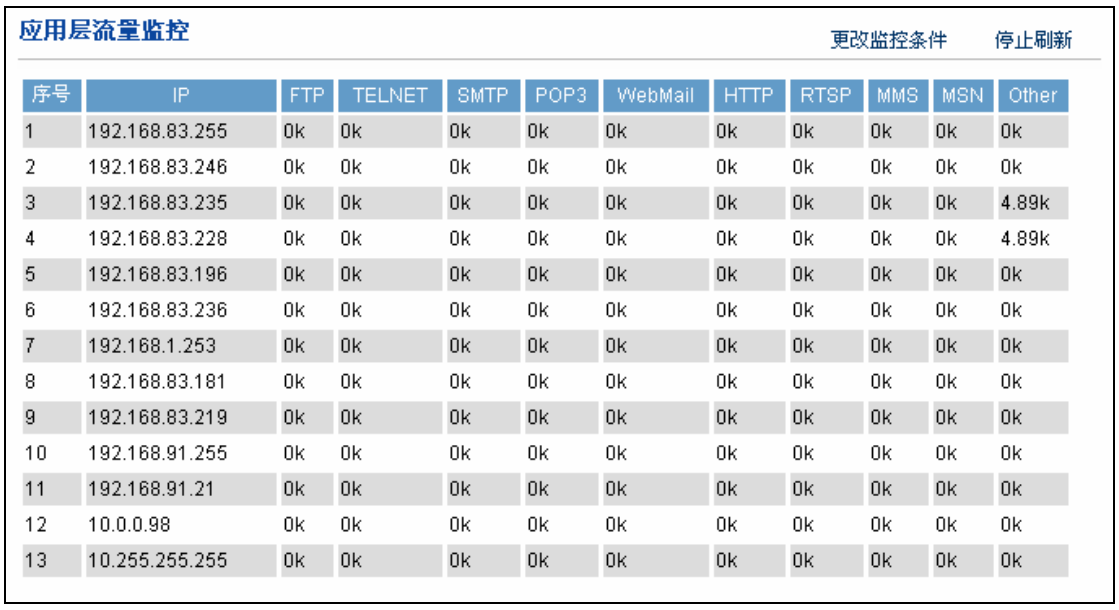
序号	IP	总流量	出流量	入流量
1	192.168.83.218	36.45k	9.39k	27.06k
2	192.168.83.255	2.16k	0k	2.16k
3	192.168.83.246	0.27k	0.27k	0k
4	202.106.0.20	0.65k	0.36k	0.29k
5	192.168.83.235	14.41k	13.18k	1.22k
6	192.168.83.228	15.22k	2.03k	13.18k
7	192.168.83.231	0.27k	0.27k	0k

选择“传输层流量监控”，点击“开始监控”按钮，界面中将分别列出在传输层采用 TCP、UDP、ICMP 和其他协议传输数据的流量值，“0k”即零 K，表示无该协议的流量，如下图所示。



序号	IP	TCP	UDP	ICMP	other
1	192.168.83.255	0k	7.01k	0k	0k
2	192.168.83.246	0k	0.54k	0k	0k
3	192.168.83.235	4.6k	0k	0k	0k
4	192.168.83.228	4.6k	0k	0k	0k
5	192.168.83.196	0k	1.62k	0k	0k
6	192.168.83.236	0k	0.7k	0k	0k
7	192.168.1.253	0k	0.7k	0k	0k
8	192.168.83.234	0.27k	2.32k	0k	0k
9	192.168.83.219	0.27k	0.27k	0k	0k
10	192.168.83.211	0k	2.26k	0k	0k
11	10.0.0.98	0k	0.47k	0k	0k
12	10.255.255.255	0k	0.47k	0k	0k

选择“应用层流量监控”，点击“开始监控”按钮，界面中将列出采用各种应用层协议传输数据的流量值，如下图所示。



序号	IP	FTP	TELNET	SMTP	POP3	WebMail	HTTP	RTSP	MMS	MSN	Other
1	192.168.83.255	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
2	192.168.83.246	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
3	192.168.83.235	0k	0k	0k	0k	0k	0k	0k	0k	0k	4.89k
4	192.168.83.228	0k	0k	0k	0k	0k	0k	0k	0k	0k	4.89k
5	192.168.83.196	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
6	192.168.83.236	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
7	192.168.1.253	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
8	192.168.83.181	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
9	192.168.83.219	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
10	192.168.91.255	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
11	192.168.91.21	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
12	10.0.0.98	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k
13	10.255.255.255	0k	0k	0k	0k	0k	0k	0k	0k	0k	0k

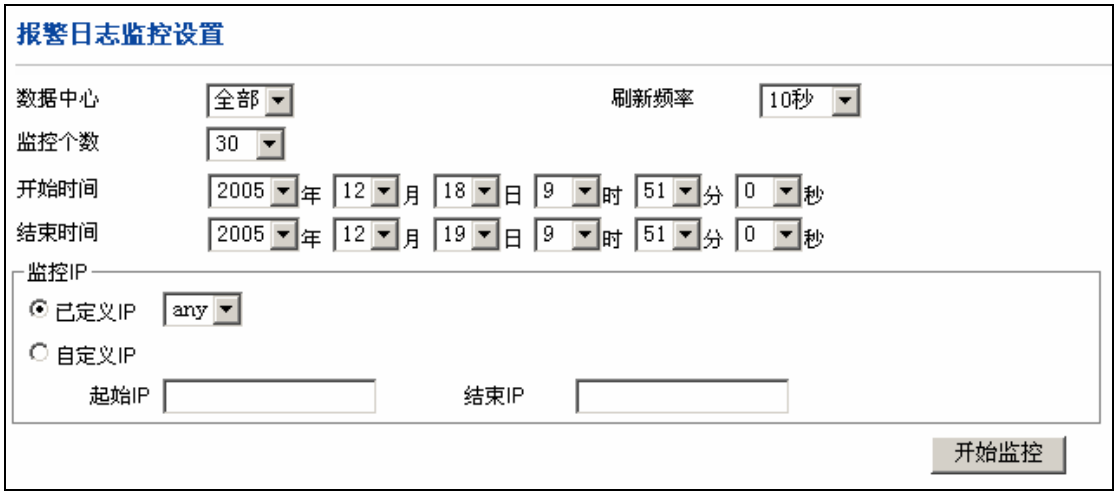
用户可以根据需要在上述界面中停止监控和更改监控条件。

6.3 报警信息监控

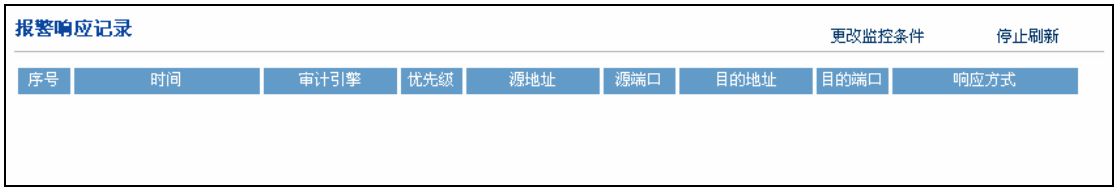
当审计引擎匹配报警策略后，在产生报警响应的同时将向数据中心发送报警信息，数据中心将报警信息存入数据库，管理员可以随时在管理中心中根据设定的条件查看数据库中的报警记录。

查看报警日志的操作如下：

1）选择 **实时监控 > 报警日志**，进入“报警日志监控设置”界面，如下图所示。



2）设置日志监控条件。选择要监控的数据中心和显示记录的个数，设定监控的范围，包括地址范围和时间范围，点击“开始监控”按钮，系统将按照时间顺序显示离当前时间最近的报警响应记录，如下图所示。



用户可以随时更改监控条件和停止监控。

7 系统日志管理

网络卫士安全审计系统提供完整的操作日志、系统日志记录，管理员可以对日志可以进行方便的查看、导入导出。

7.1 系统日志查看

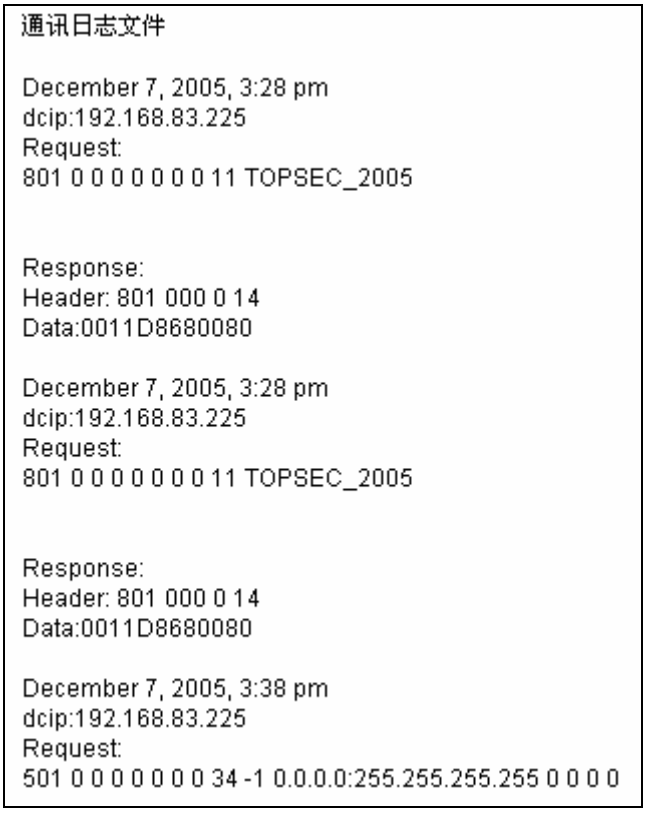
选择 **系统日志**，进入系统日志页面，如同图所示。

日志信息按照时间逆序排列，记录了所有用户登录网络卫士安全审计系统后的一切活动，包含行为目标、使用命令及获得结果等。

7.2 查看通讯日志

网络卫士安全审计系统提供了查看通讯日志的功能。

点击系统日志页面右上角的“查看通讯日志”，如下图所示。

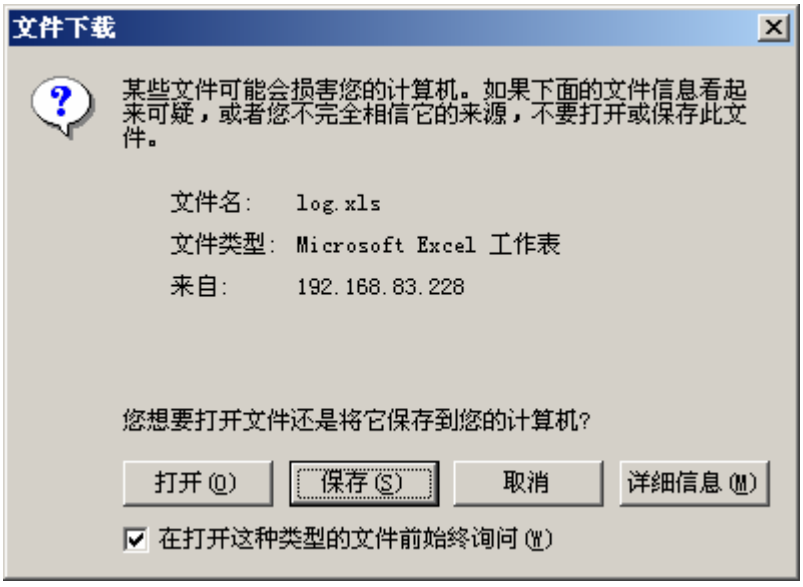


如图所示，网络卫士安全审计系统保存了所有的通讯日志。

7.3 系统日志导出

网络卫士安全审计系统提供了日志导出的功能。具体操作如下：

点击系统日志页面右上角的“日志导出”，弹出如下图的界面。

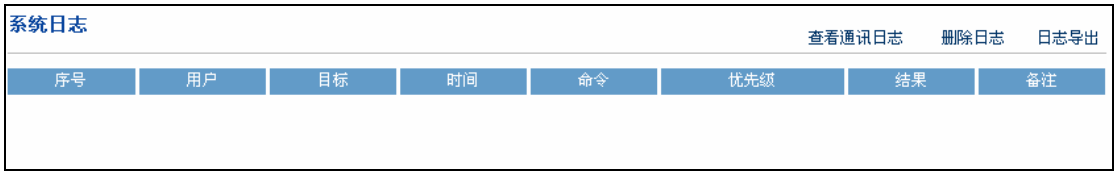


点击“保存”选择存放的位置，便可将日志导出。

7.4 系统日志删除

网络卫士安全审计系统提供了删除日志的功能。

点击系统日志页面右上角的“删除日志”，将清空选定数据中心的所有日志。如图所示。



建议用户慎重选用此操作，以免日志丢失。