天清异常流量管理中心 ADM-Manager

Web 管理用户手册

北京启明星辰信息安全技术有限公司

Beijing Venustech Cybervision Co., Ltd

二零一二年五月

版 权 声 明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京启明星辰信息安全技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京启明星辰信息安全技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦　邮编：100193

电话：010-82779088

传真：010-82779000

您可以访问启明星辰网站：www.venustech.com.cn 获得最新技术和产品信息。

目　录

第一章 前言

1.1 导言

启明星辰的天清异常流量管理与抗拒绝服务系统(天清 ADM)由异常流量检测系统 ADM-Detector（简称 Detector)、异常流量清洗系统 ADM-Guard（简称 Guard）和异常流量管理中心 ADM-Manager（简称 Manager）三个模块组成，其中 Manager 可以对多台 Guard 和 Detector 设备进行统一管理，包括检测和清洗策略下发、状态监控、系统升级、日志集中等。

《天清异常流量管理中心 ADM-Manager Web 管理用户手册》是天清异常流量管理中心的管理员用户帮助文档。本手册详细介绍了异常流量管理中心的操作和使用方法。

1.2 适用对象

本手册适用于负责支持、维护管理中心的安全管理员，是对管理中心进行配置管理时的必备手册。使用本手册的读者，应当熟悉 Detector、Guard 等设备的使用，了解网络安全知识、TCP/IP 协议等基本知识。

1.3 适合产品

本手册适合异常流量管理中心 V3.6.3.1 版本。

第二章 如何开始

2.1 概述

产品特点

本设备为异常流量管理中心，通过集中的管理中心统一管理 Detector 与 Guard 设备，以及分布

在网络中的网络设备，提供用户一个完整的抗攻击解决方案，实现 Detector 与 Guard 以及各级联设备之间总体配置、统一调控、集中监控、简便的策略配置、智能策略下发、协调各安全设备互动等工作；达到流量清洗的智能化管理。

2.1.1 软件描述

管理中心使用 B/S 架构，用户通过 IE 登陆管理页面，可以对全系统的各项功能和配置进行管理。本系统仅支持 IE7 以上版本的浏览器。

使用本设备首先需要通过浏览器登录设备后在系统页面导入合法的 License 许可文件，同时需要将受管设备的集中管理主机和日志服务器的 IP 地址设置为管理中心服务器的 IP，用户就可以通过浏览器查看相关的设备信息和完成各项配置管理。

2.1.2 主要功能

管理中心主要包括系统主页、系统监控、集中管理、事件查询、统计报表、权限管理和系统管理等模块。

系统主页显示全局的安全状态，展示系统各个方面的安全信息，包括实时监控最近攻击事件、最近被攻击次数最多的目标 TOP N、流量告警事件、性能告警事件等。并可根据需要在系统-主页配置模块中，对主页的展示的项目、显示项目的数量、位置等进行自定义配置。

系统监控包括三部分：设备性能监控、流量监控和告警监控，监控对象包括 Detector 设备、Guard 设备、保护群组、网络设备和支持安装 SNMP 服务的主机等。

集中管理模块对用户关心的 Detector、Guard 设备与集群和普通网络设备、主机统一组织，以拓扑图和列表的方式，直观提供设备分布和连接情况。并在此基础上提供对设备的策略统一管理。

系统管理允许用户监控管理中心本身运行，以及系统配置和管理

2.1.3 License 控制

本系统的 License 控制分为激活控制类型和数量控制类型两大类。两种类型的 License 均与硬盘串号绑定，只能用于该 License 绑定的设备上。

本系统初始安装完毕之后，如果未导入激活控制型 License，则本系统默认可管理设备数量为 2 台，如果需要管理更多数量的设备需要登录系统，，进入 License 管理功能，导入激活和数量控制型 License 后，才能正常管理设备。

2.2 进入系统

2.2.1 登录

打开浏览器，输入管理中心主页 URL（如 https://ip:8889/LMSSiem），出现登录界面，如图所示：

图表 2-1

- 用户名：用户登录的名称。
- 密 码：分配给用户的密码（系统默认用户名为 admin，密码为 admin123）。

2.2.2 界面主框架

进入管理中心，包括三个部分：顶部菜单栏、左侧导航栏和中间主界面。

- 顶部菜单栏：包括：系统主页、系统监控、集中管理、事件查询、统计报表、权限管理和系统管理。
- 左侧导航栏：在不同的功能模块，左侧导航栏会出现不同的内容。如在主页菜单中，左侧显示安全等级、系统状态、服务状态、设备探测等内容。
- 中间主界面：系统各个功能的主要展示界面。

第三章 系统主页

3.1 概述

主页显示全局的安全态势，展示系统各个方面的安全信息，包括实时监控最近流量趋势、攻击报文速率趋势、流量告警 TOP10 攻击类型统计、性能告警按级别分布、最近入侵攻击事件、最近被攻击次数最多的主机 TOP10 设备告警事件、设备实际运行状态等。并可根据需要在系统-主页配置模块中，对主页的展示项的数量、位置等进行自定义配置。详细功能请参见 9.1.4 主页配置。

图表 3-1

3.1.1 安全等级

安全等级是系统分析全网安全数据得出的综合指标，代表全网的安全级别。展示的结果是最近 10 分钟的信息。

可以调整安全规则来自定义安全等级。具体可参考系统管理中的告警阈值配置。

图表 3-2

3.1.2 系统状态

系统状态展现了系统所在服务器的基本信息，包括 cpu，内存使用率，硬盘剩余空间，系统运行天数等。

图表 3-3

3.1.3 服务状态

服务状态展现了系统包括的各种服务的启停状态信息，包括 Web 服务、数据库服务、事件服务、设备发现服务、威胁响应服务。

图表 3-4

3.1.4 设备探测

设备探测是展示系统最新添加的 10 台设备。添加一天之内属于新设备，否则为已探测

图表 3-5

3.2 “全景”威胁管控

“全景”威胁管控实时监控最近 10 分钟的安全态势分析，以图形或表格形式展示。

图表 3-6

- 流量趋势：以折线图的形式显示了最近 10 分钟流入和流出流量的趋势。
- 攻击报文速率趋势：以折线图的形式显示了最近 10 分钟攻击报文速率的趋势。
- 流量告警 TOP10 攻击类型统计：以柱状图的形式显示了最近 10 分钟发生的流量告警次数最多的前 10 名攻击类型的告警次数统计。

- 性能告警按级别分布: 以饼图的形式显示了最近 10 分钟的性能告警按告警级别的分布情况。
- 入侵攻击事件趋势：以折线图的形式显示了最近 10 分钟入侵攻击事件总数的趋势。
- 主机被攻击次数统计排行 TOP10：以柱状图的形式显示了最近 10 分钟被攻击次数最多的前 10 名主机。
- 设备告警事件统计排行 TOP10：以柱状图的形式显示了最近 10 分钟告警次数最多的前 10 名设备。
- 设备实际运行状态：以分组表格的形式显示了最近 10 分钟各个管理域以及管理域下的所有设备的运行状态。包括管理域名称、设备名称、运行状态（连通、断开、未知）。

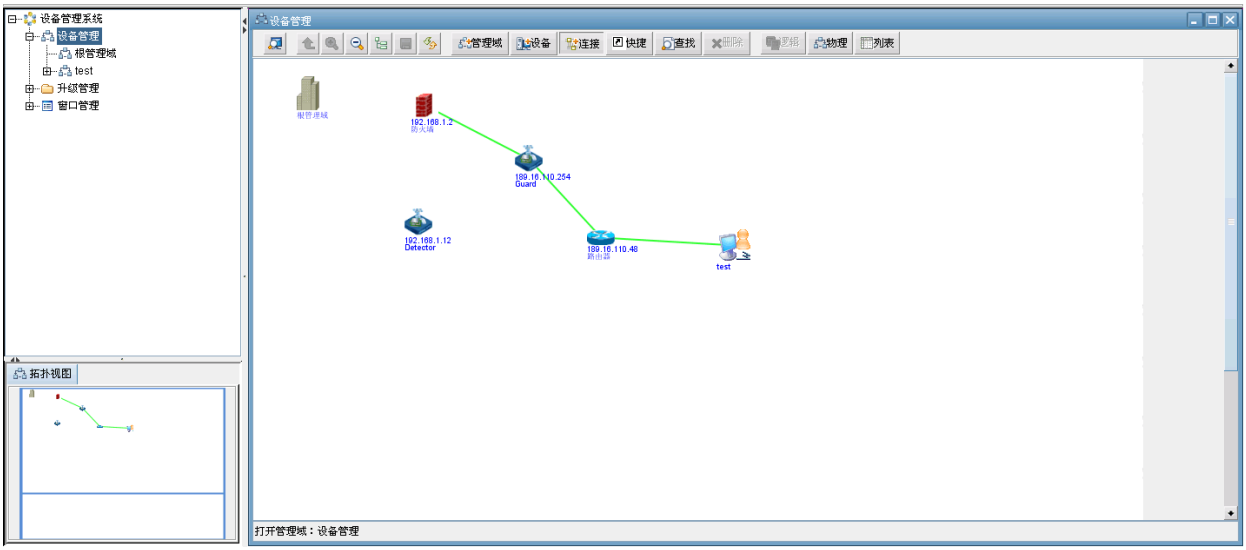
第四章 集中管理

在管理中心中，我们把设备、网络连接等归类为资产，统一在管理域中进行管理。

4.1 设备管理

设备管理拓扑图是对设备和网络的可视化管理。通过设备管理域拓扑图，可以从全局角度对网络系统、管理子网、设备等对象以及它们之间的归属关系和连接关系进行管理。

设备管理拓扑图中，管理对象主要是指：设备、管理域（子图）、网络连接，用户可以在系统中新建管理对象、修改对象属性以及删除管理对象，或通过对象的右键菜单进入对象管理的其它功能，如策略管理、位置转移等。

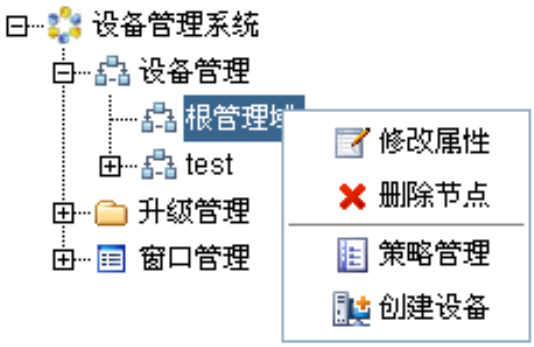


图表 4-1

4.1.1 网络拓扑管理

4.1.1.1管理域树

管理域功能树实现管理域的管理、浏览功能，通过管理域子图功能树可以清楚的查看系统内的管理域结构，通过鼠标点击可以快速打开管理域拓扑图，或通过右键弹出菜单完成对管理域的新建、属性修改和删除等工作，也可以进行创建设备、策略管理等各项功能操作。



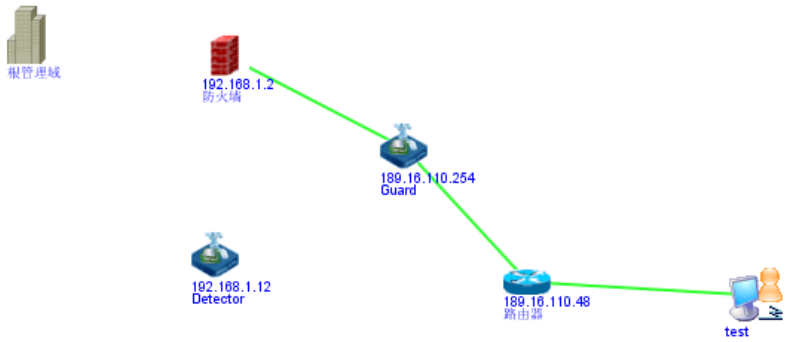
图表 4-2

用户可以展开、新建、修改、删除管理域。

在管理域拓扑图，用户可以看到设备当前的运行状态。当设备状态发生改变时，管理中心通过设备状态轮询，自动发现设备状态的改变，并在管理域拓扑图上更新设备状态的显示。

设备状态显示图标说明：设备正常运行状态； 设备无法连通。

4.1.1.2管理域拓扑图



图表 4-3

当用户通过鼠标单击设备管理树节点时，系统会在拓扑图面板上显示属于当前子图下的全部子图、设备以及网络连接。

设备管理域拓扑图全局直观的展现了当前打开的子图下定义的全部内容，用户可以通过鼠标双击设备对象或连接对象，查看或修改对象的属性；或双击拓扑图上的子图，展开该子图的拓扑视图。也可以通过鼠标拖拽的方式调整子图和设备在拓扑图上的布局。当调整了拓扑布局后，需要对修改进行保存，否则在用户关闭当前管理域（子图）后调整会丢失。

拓扑管理包括了物理拓扑和逻辑拓扑两种管理视图，列表选项可以列表显示两种不同视图的内容，用户点击逻辑拓扑后再点击列表按钮，列表显示逻辑拓扑视图的设备与连接等内容。同理，用户

点击物理拓扑后再点击列表按钮，列表显示物理拓扑视图中的各项信息。

4.1.1.3拓扑布局调整

拓扑布局调整分为手动和自动调整两种方式，用户可以通过鼠标拖拽的方式调整管理域和设备在拓扑图上的布局，展开将要操作的管理域拓扑图；且用户可以通过鼠标点击工具栏中的“布局”功能按钮，自动布局当前管理域子图。调整后请注意保存对拓扑图布局修改。

4.1.1.4设备管理工具栏

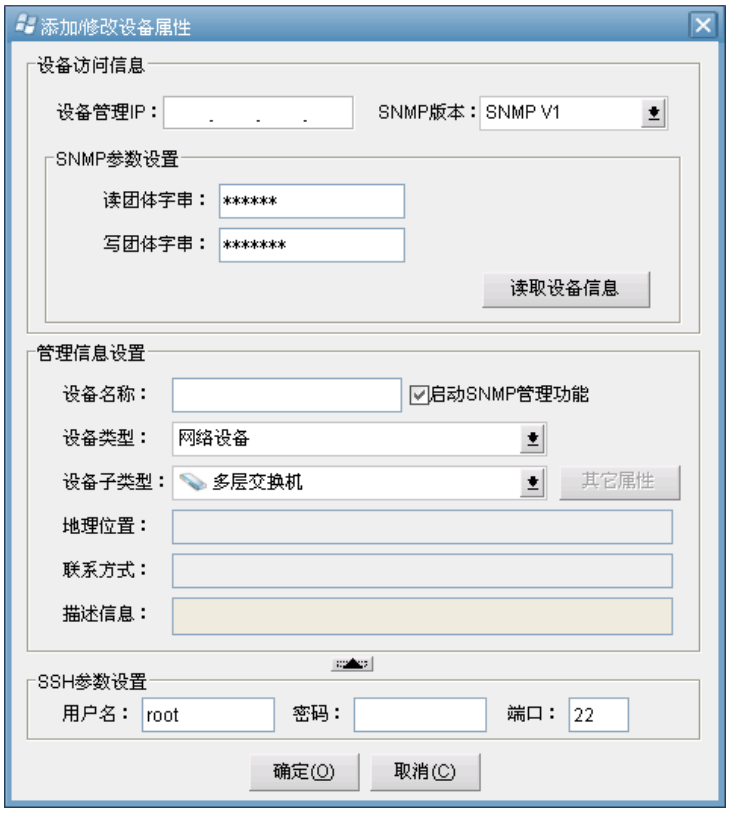
图表 4-4

4.1.1.5弹出菜单功能

鼠标右键点击拓扑对象（子网、设备、连接）或设备管理树图上的子网对象，可弹出对象弹出式菜单，用来执行选择对象的属性修改、对象删除、位置转移、策略管理等操作。对于不同类型的受管设备，弹出菜单会有所不同。

4.1.2 设备信息读取

设备管理功能包括新建、修改、删除、转移。点击拓扑图工具栏中的“设备”，即可弹出添加设备对话框。界面如图所示：



图表 4-5

用户需要输入合法的设备 IP 地址、SNMP 版本、SNMP 访问读团体字符串（默认为“public”）、SNMP 写团体字符串（默认为“private”），然后点击“读取设备信息”按钮，如果输入 IP 地址符合系统要求，并且 SNMP 方式能够连通设备，系统将得到设备类型、设备联系方式、设备名称、设备描述等基本信息，显示到新建设备界面中。

用户输入设备名称、类型、联系方式、描述等信息，按“确定”按钮添加设备。在添加设备窗口中，设备类型和设备型号以下拉框的形式选择。如果在添加设备或修改设备属性时没有将启用 SNMP 管理功能选中，则设备图标不显示连接状态。设备添加过程中，如果所选的设备类型及型号不是网御设备，则点击完成即可保存修改；如果是，则需要输入设备的其它属性。

设备如存在 SSH 接口，用户需要配置相应的 SSH 参数。

4.1.3 节点管理

4.1.3.1连接管理

用户可以新建、修改、删除连接。鼠标点击工具栏中的“新建连接”，系统进入画线状态。通过鼠标在要建立连接关系的两个对象（子图或设备）之间画连接，成功画线之后，点击工具栏中的“保存拓扑图”，保存对拓扑图修改。连接名称系统默认为“节点名称 -节点名称”的格式。

4.1.3.2快捷节点管理

系统提供节点快速定位的功能，用户可以为管理域或设备建立快捷节点，通过快捷节点可以方便的定位所连接的实际节点。具体操作步骤为：

1、选择要建立快捷节点的管理域或设备节点，点击鼠标右键，复制快捷节点。

2、打开将要建立快捷节点的管理域子图，在拓扑图空白处点击鼠标右键，粘贴快捷节点即可完成创建过程，快捷节点显示状态： 

3、用户通过鼠标双击管理域快捷节点，可以直接打开所关联的管理域；通过鼠标双击设备快捷节点，可以直接定位到所关联的设备节点。

4.1.3.3节点（管理域、设备、连接）查找

通过节点（管理域、设备、连接）对象查找功能，可以在系统中查找节点对象。输入对象名称，指定对象类型，点击“立即查找”按钮，查找结果会显示在查找结果列表中。查找结果中显示了节点名称、对象图标、对象所在管理域和对象类型描述信息。在查找列表中选择节点对象，鼠标双击或点击“定位节点”，即可打开选中节点所在的管理域拓扑图，并使焦点定位在选择的管理域、设备或连接对象上。

4.1.4 级联管理

级联管理功能可以实现管理中心多级级联，管理中心服务器可以管理中心网络、接收本地安全告警，同时可建立下级与分管理中心的级联应用；管理中心服务器通过网络，使用分管理中心的超级用户身份，访问分管理中心服务器，从而实现集中管理、集中监控、集中审计、分布部署等功能。其应用环境如图所示：

图表 4-7

在级联环境中，管理中心服务器通过超级用户身份登录分管理中心服务器后，通过远程调用，取得分管理中心服务器的拓扑数据、设备管理数据、设备监控数据等；分管理中心服务器同样可以再级联二级分管理中心服务器等，从而达到多级级联的功能。

在拓扑管理树上，可以通过菜单，在添加管理域窗口内添加下级级联管理中心；选择管理域为下级级联管理中心后，弹出属性配置窗口，用户需填入并确认相应下级管理中心属性数据；下级管理中心级联到本地管理后，下级管理中心拓扑图逻辑结构可以在本地拓扑树图和拓扑图中显示。如果操作节点为下级管理中心所管理内容，可以通过级联调用，显示下级管理中心拓扑图。

4.2 策略管理

策略管理用于为选定的子图或设备配置管理策略，根据用户的权限、选定的节点（子图或设备）所处的层级位置，执行预定义的业务逻辑，并将数据保存到数据库中。

用户在设备管理或拓扑管理界面中选择要管理的节点（子图或设备），从弹出菜单中选择策略管理，进入该节点的策略管理主界面。

策略管理支持情况如下表所示：

设备类型	支持的策略功能模块	策略管理方式
Detector	移动窗口基线、特征基线、周期性基线	下发
Guard	资源定义、清洗策略、牵引策略、回注策略、抓包策略	数据库存储并下发

图表 4-8

4.2.1 Detector 策略管理

4.2.1.1基线配置

类型	插件	检测模式	状态	启停	配置
SYN Flood攻击	IN_TimeWin	仅字节数检测	启用		
ACK Flood攻击	IN_TimeWin	仅字节数检测	启用		
ICMP Flood攻击	IN_TimeWin	仅字节数检测	启用		
HTTP Get Flood攻击	IN_TimeWin	仅字节数检测	启用		
LAND Flood攻击	IN_Features	仅字节数检测	启用		
IGMP Flood攻击	IN_TimeWin	仅字节数检测	启用		
TCP Flag NULL	IN_Features	仅字节数检测	启用		
TCP Flag 误用	IN_Features	仅字节数检测	启用		
Protocol NULL	IN_Features	仅字节数检测	启用		
UDP Flood攻击	IN_TimeWin	仅字节数检测	启用		
SYN-ACK Flood	IN_TimeWin	仅字节数检测	启用		

图表 4-9

4.2.1.2基线参数配置

类型	插件	检测模式	状态	配置
SYN Flood攻击	IN_TimeWin	仅字节数检测	启用	

保护域	分级阈值（字节）			分级阈值（包数）			平滑参数配置（字节）		平滑参数配置（包数）		状态	配置
	高级(k)	中级(k)	低级(k)	高级(k)	中级(k)	低级(k)	权重(%)	平滑常数	权重(%)	平滑常数		
缺省	200	100	50	200	100	50	20	0.4	0	0.4	不启用 / 启用	

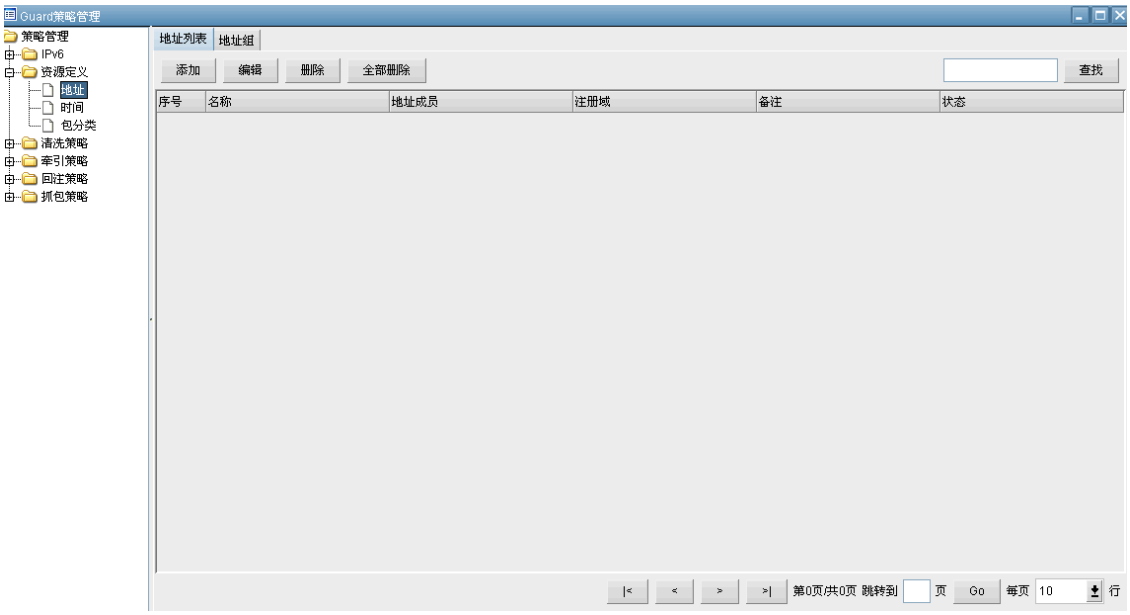
图表 4-10

4.2.2 Guard 策略管理

4.2.2.1资源定义

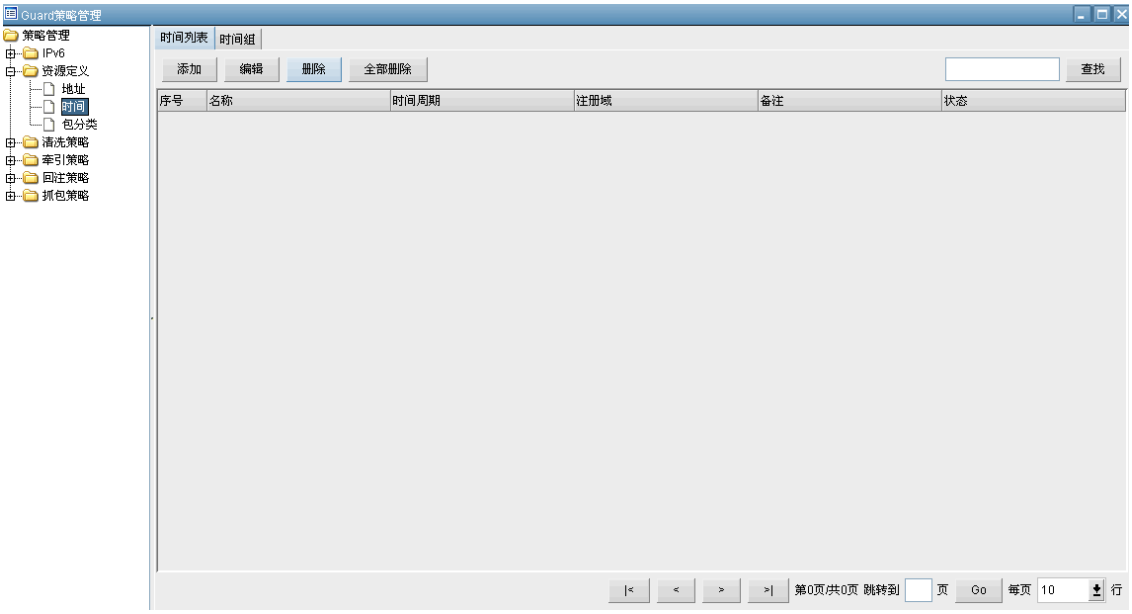
为了简化 Guard 清洗规则的配置和维护工作，引入了资源定义。可以定义以下资源

4.2.2.1.1 地址



图表 4-11

4.2.2.1.2 时间



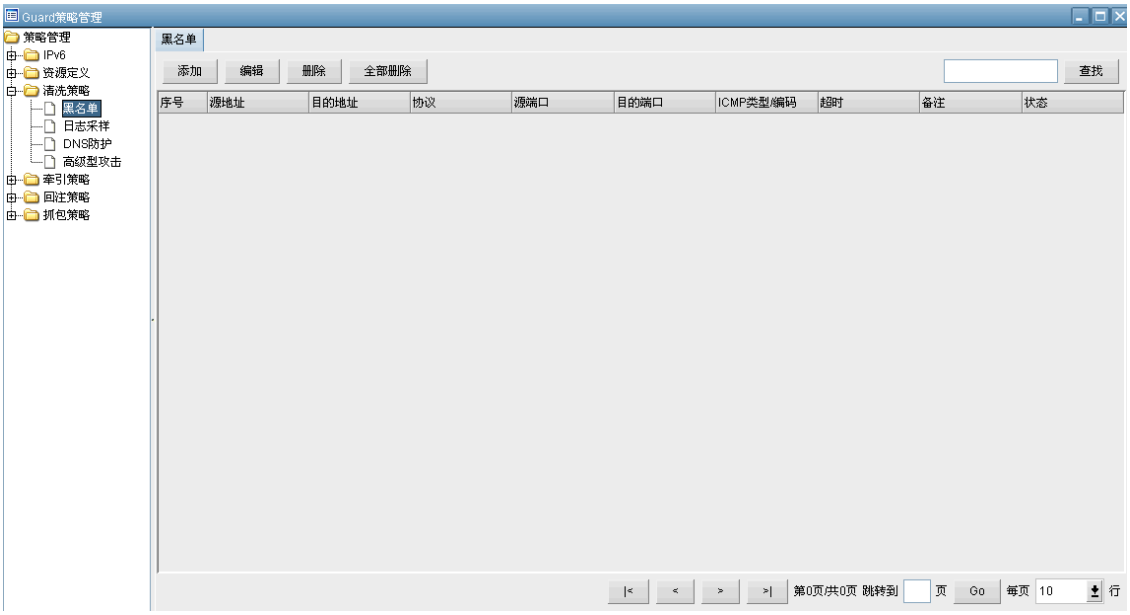
图表 4-12

4.2.2.1.3包分类

图表 4-13

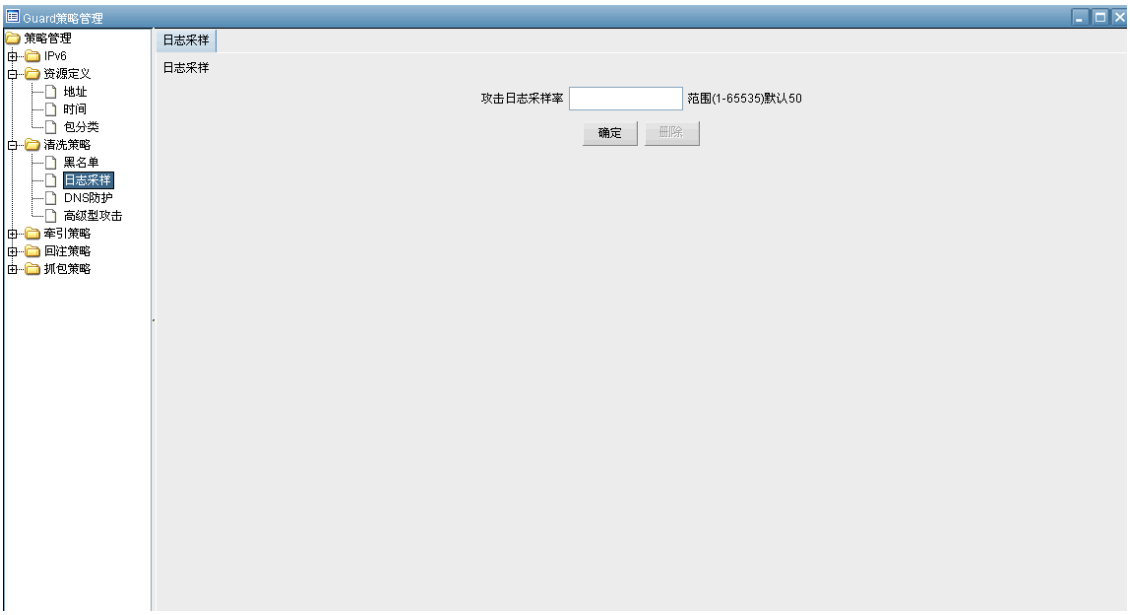
4.2.2.2清洗策略

4.2.2.2.1 黑名单



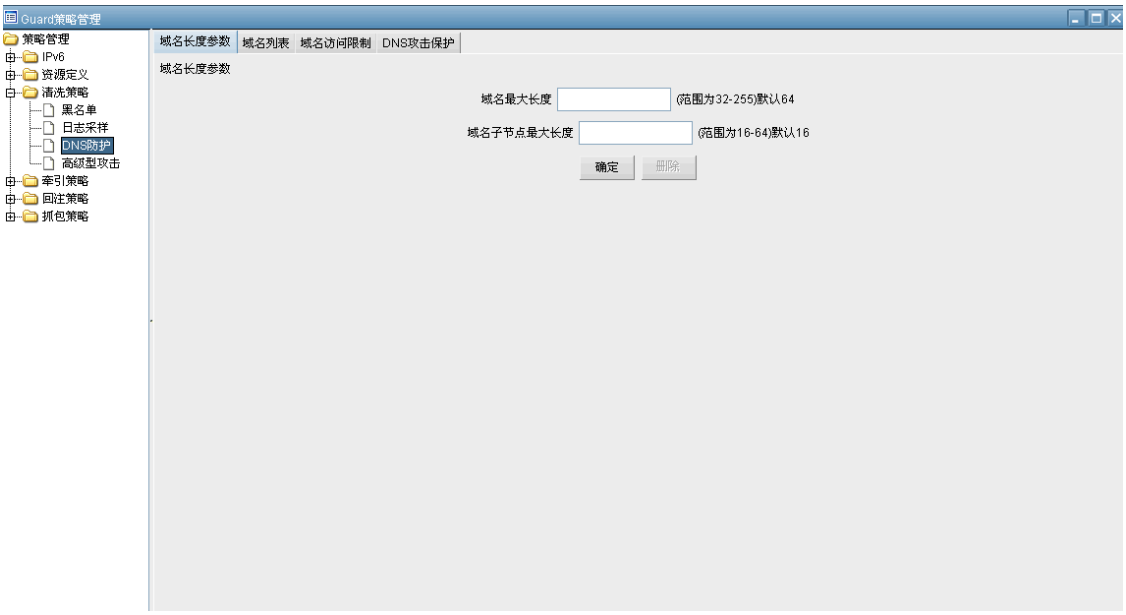
图表 4-14

4.2.2.2.2 日志采样



图表 4-15

4.2.2.2.3 DNS 防护



图表 4-16

4.2.2.2.4 高级型攻击

图表 4-17

4.2.2.3牵引策略

4.2.2.3.1 BGP 牵引

图表 4-18

4.2.2.3.2 OSPF 牵引

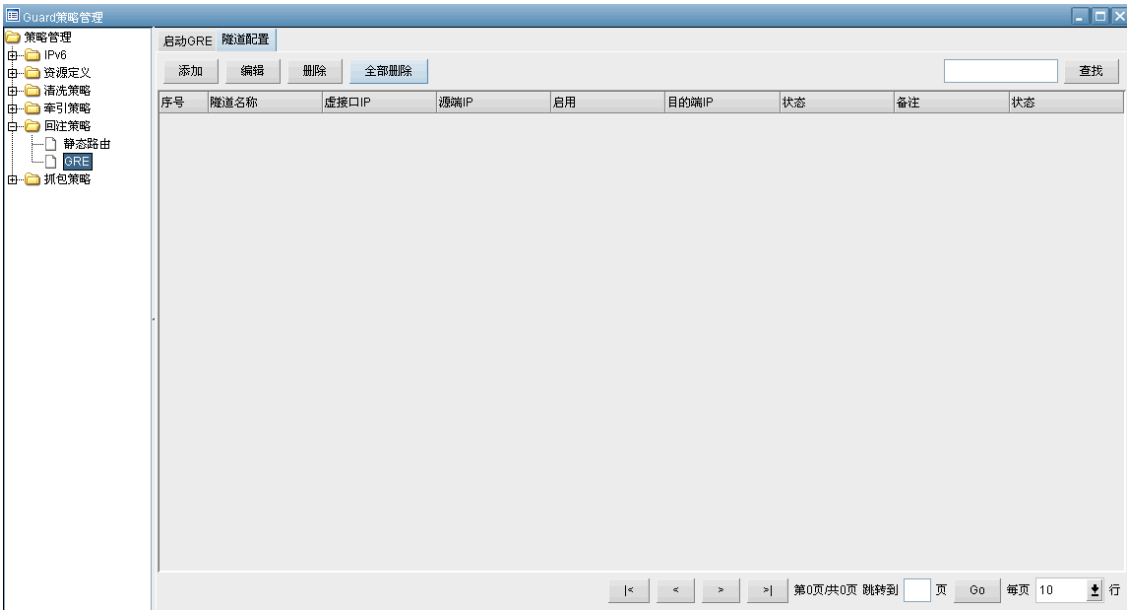
图表 4-19

4.2.2.4回注策略

4.2.2.4.1静态路由

图表 4-20

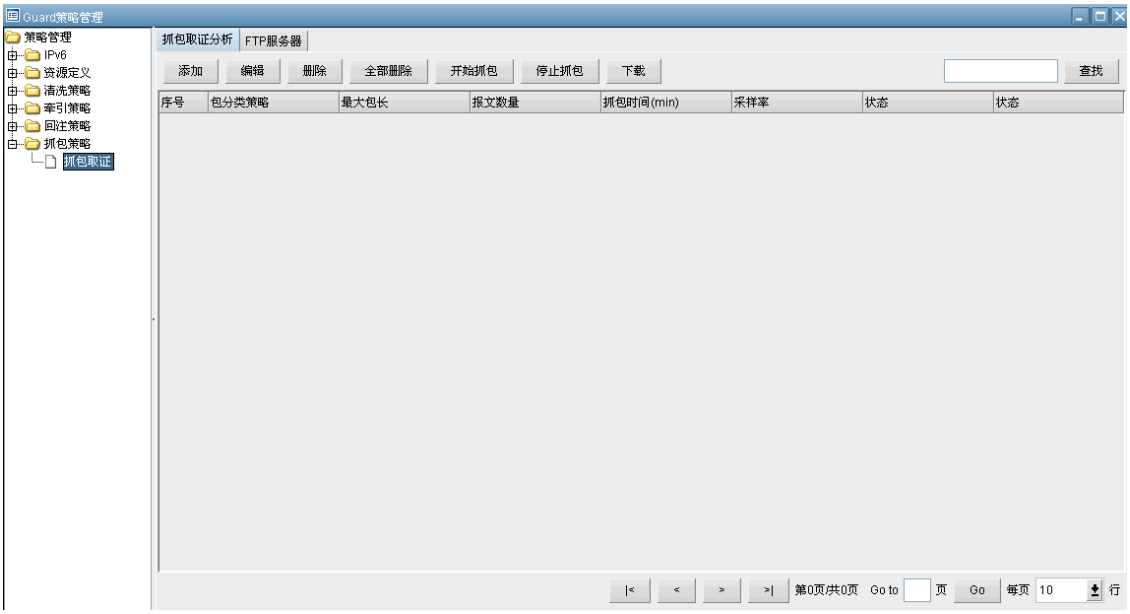
4.2.2.4.2GRE



图表 4-6

4.2.2.5抓包策略

抓包取证：



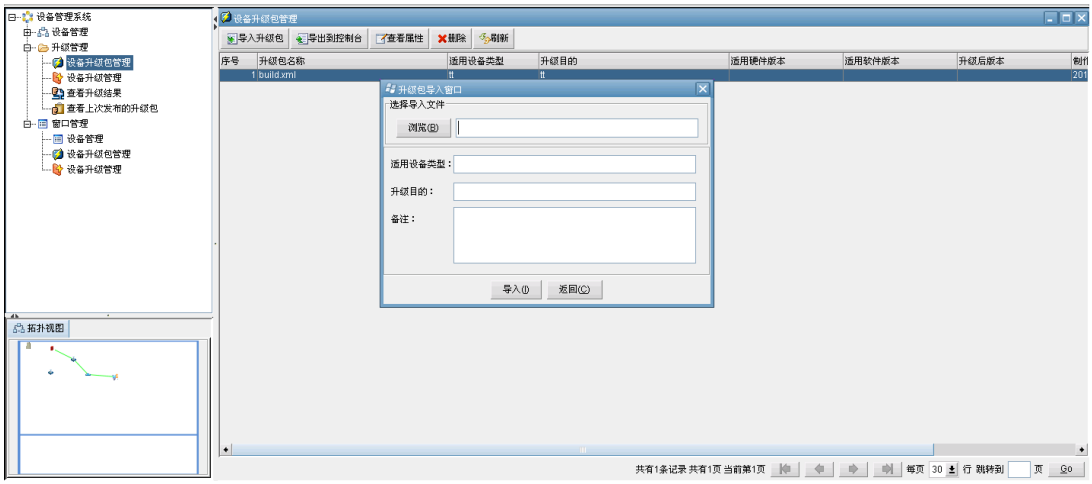
图表 4-22

4.3 升级管理

设备升级管理包括“升级包管理”和“设备升级”两部分。详细参见如下：

4.3.1 设备升级包管理

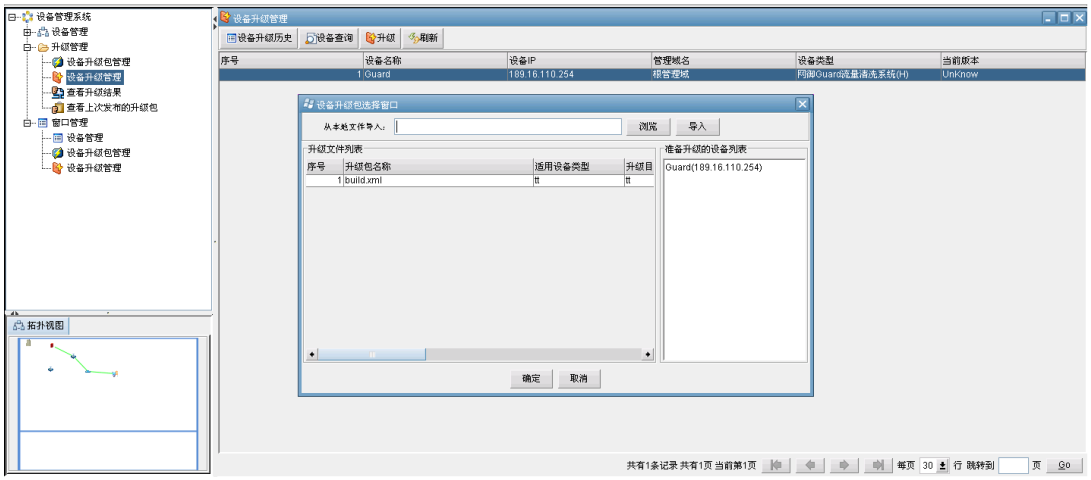
用户可以导入升级包、把升级包导出到控制台，查看升级包属性，删除升级包，获取最新的所有的设备升级包记录。导入升级包最好添加注释，便于以后查看。Guard 设备升级包的备注必须填写并且为英文。



图表 4-24

4.3.2 设备升级管理

本模块提供查看设备升级历史、查询设备、对设备进行升级、获取最新的所有的设备记录等功能。管理员确认升级后，系统显示升级过程窗口，显示当前设备的升级状态。通过点击“刷新”可以跟踪升级过程，升级完成后，系统会给出设备升级的结果。



图表 4-25

第五章 事件管理

管理中心 Web 应用程序通过浏览器，向用户提供安全事件管理功能。包括安全事件查询、安全事件监控、常用查询、定制查询等功能。

图表 5-1

5.1 实时监控

用来查看监控设备当天 24 小时的事件量趋势和最近一段时间内（30 秒）所产生的前 50 条日志信息（包括事件类型、告警级别、源地址、目的地址、发生次数、发生时间）。

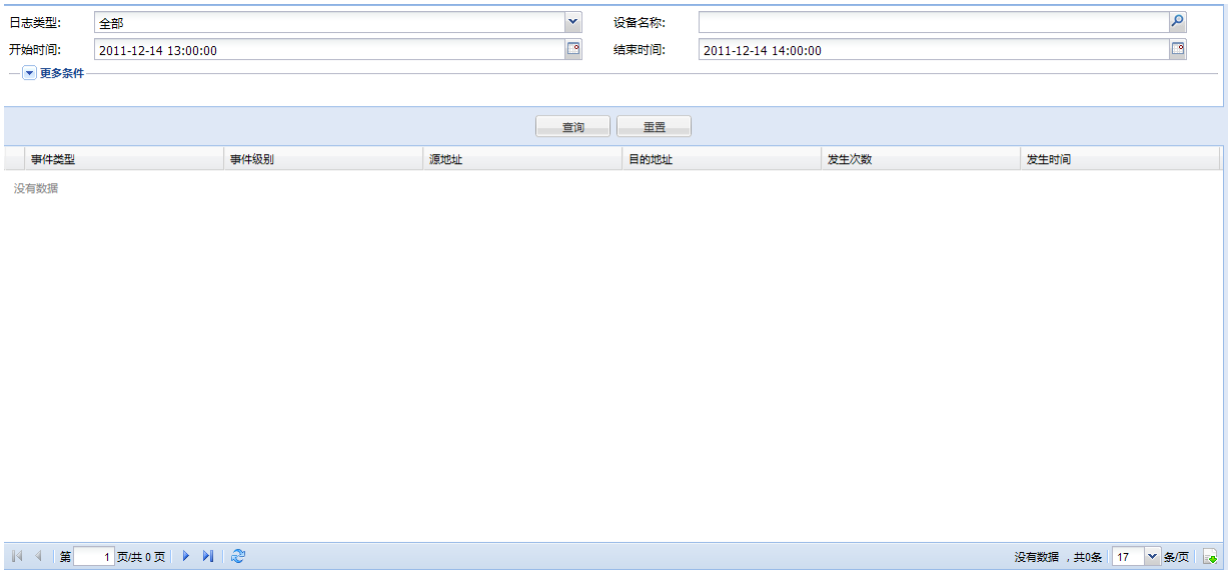
事件类型	告警级别	源地址	目的地址	发生次数	发生时间
一般代理日志事件	提示	0.0.0.0	0.0.0.0	1	2011-07-21 14:36:05
一般入侵检测事件	提示	192.168.93.1	10.1.1.1	1	2011-07-21 14:36:05
一般邮件过滤事件	出错	0.0.0.0	0.0.0.0	1	2011-07-21 14:36:05
一般代理日志事件	提示	0.0.0.0	0.0.0.0	1	2011-07-21 14:36:04
一般入侵检测事件	提示	192.168.93.1	10.1.1.1	1	2011-07-21 14:36:04
一般邮件过滤事件	出错	0.0.0.0	0.0.0.0	1	2011-07-21 14:36:04
一般代理日志事件	提示	0.0.0.0	0.0.0.0	1	2011-07-21 14:36:03
一般入侵检测事件	提示	192.168.93.1	10.1.1.1	1	2011-07-21 14:36:03
一般邮件过滤事件	出错	0.0.0.0	0.0.0.0	1	2011-07-21 14:36:03
一般代理日志事件	提示	0.0.0.0	0.0.0.0	1	2011-07-21 14:36:02
一般入侵检测事件	提示	192.168.93.1	10.1.1.1	1	2011-07-21 14:36:02
一般邮件过滤事件	出错	0.0.0.0	0.0.0.0	1	2011-07-21 14:36:02

图表 5-2

5.2 安全日志查询

安全事件查询使用户可以通过设定各种条件来查询管理中心收到、解析并保存事件日志。

查询条件包括基本查询条件和扩展查询条件，用户可以通过设定具体的条件查询到自己所关心的日志。对于扩展查询条件，可以通过点击文字前面的箭头来展开查询条件以供用户选择，有的是在文本框中直接输入，而有些条件需要在多个选项中选择。对于查询结果是以列表的形式进行显示，在列表的下面将显示查询到的总记录数和总页数，而且可以通过在多页的结果中进行浏览。



图表 5-3

- 基本查询条件**时间范围**：它是所有日志查询的必选条件。要求用户必须选择一个时间段，开始时间与结束时间间隔不能超过 7 天。注意：由于日志信息量很大所以在选择时间段时尽量选择较小的时间段，以避免由于数据量过大造成系统瘫痪。
- **设备名称**：点击“**设备名称**”后面的放大镜图标，将列出系统记录的所有设备列表信息，勾选需要查询的设备点击保存将其添加到选择设备列表中。如果勾选设备太多的话可以通过点击管理域名称前面的复选框来选择和取消选择设备列表中该管理域下的所有设备，然后点击保存确认选择。
- **日志类型**：管理中心分 11 种日志类型：抗攻击事件日志，抗攻击流量日志，设备管理日志，会话日志，性能日志，网络状态日志，牵引事件日志，应用识别日志，网络概览日志，设备告警日志，牵引流量日志。另外还可以选择全部来查询所有日志类型的数据。

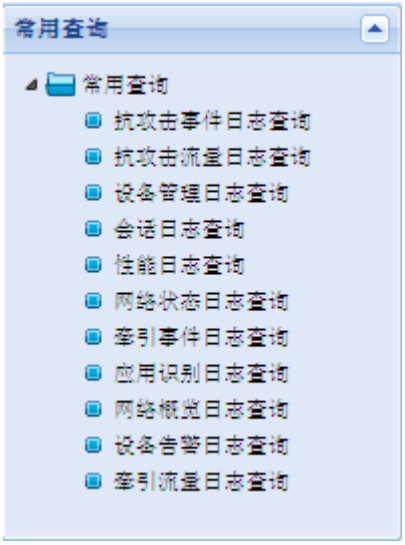
扩展查询条件

扩展查询条件是对基本查询条件的扩充，用户可根据需要进行填写和选择。其根据不同的日志类型产生不同的条件。主要包括：源地址、目的地址、端口、事件级别、源 MAC、目的 MAC、协议名称、应用名称、用户名查询条件。具体可选择不同的日志类型后展开更多条件即可查看。

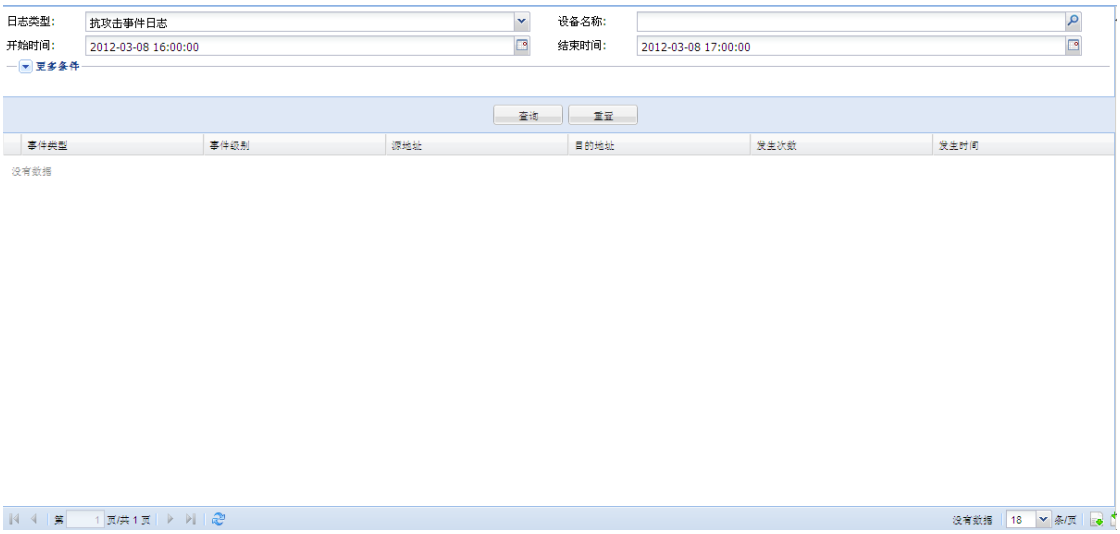
图表 5-4

5.3 常用查询

为方便用户的查询，系统默认提供了全部日志类型的常用查询：

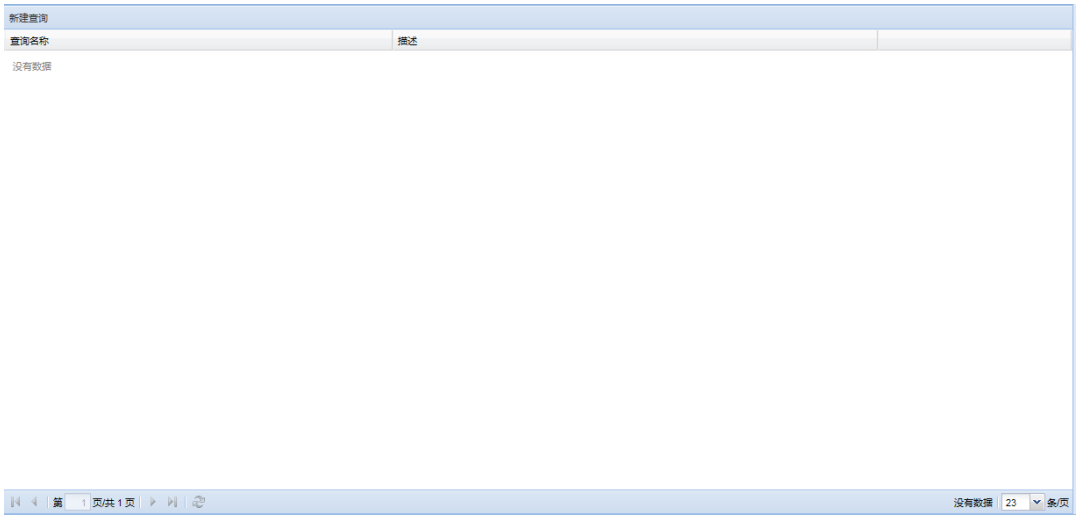


其功能和事件查询的功能一致。如下图：



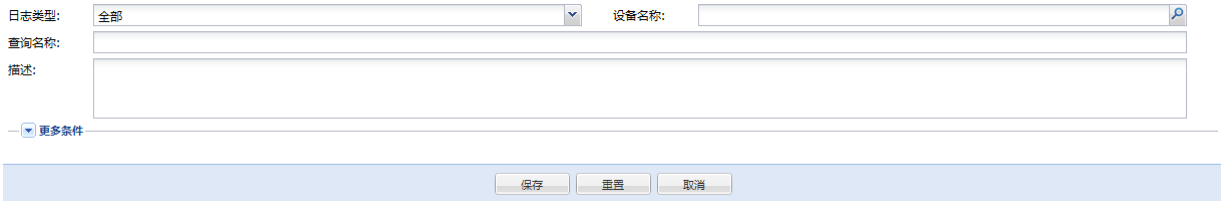
5.4 定制查询

根据用户的需要，可以对关心的内容设置不同的查询条件（包括基本查询条件和扩展查询条件），并填写一个查询名称，点击保存按钮，之后会在左侧栏生成一个永久性的菜单结点，作为一个自定义查询存在，便于用户使用。用户还可以对已经生成的自定义查询菜单进行编辑和删除操作。如下图所示：



图表 5-5

点击新建查询即可新增自定制查询：



图表 5-6

第六章 报表管理

6.1 概述

6.1.1 功能简介

管理中心报表功能可以对已收集到的日志进行统计分析，并以报表的形式呈现给用户。用户可以设定不同的查询条件，对相应的报表功能进行精确查询，系统会将查询到的结果以图形加表单的形式呈现给用户，同时提供报表的 PDF、Excel、Word、XML 等格式的导出功能，方便用户进行备份及查询。

6.1.2 功能分类

管理中心报表功能可分为常用报表、定制查询、定时报表、定制报表四类功能。

1. 常用报表：

系统预先根据设备接收的日志类型，设定了六大类的基本报表功能，包括：流量概览、安全报表、流量深度分析、抗攻击报表、设备信息统计报表和综合报表。其中流量概览、安全报表、流量深度分析、抗攻击报表都有各自的子报表功能，供用户进行更详细，更精确的审计查询。

2. 定制查询：

用户可以选择一个常用报表，设定不同的查询条件、时间粒度和报表名称，系统会将查询结果以图形和表格的形式展示给用户。方便用户对所关心的设备、IP 地址、端口、协议等进行审计查询。

3. 定时报表：

系统为每种常用报表都提供了定时报表的功能，用户可以预先配置好审计查询参数后，设定生成此报表的定时任务，当到达对应时刻，系统会自动的进行报表的生成，用户可以对已生成的报表进行查询和下载，同时，系统还提供定时任务的管理功能，用户可以对已添加的定时任务进行开始（暂停）、恢复和删除等操作，方便管理使用。

4. 定制报表：

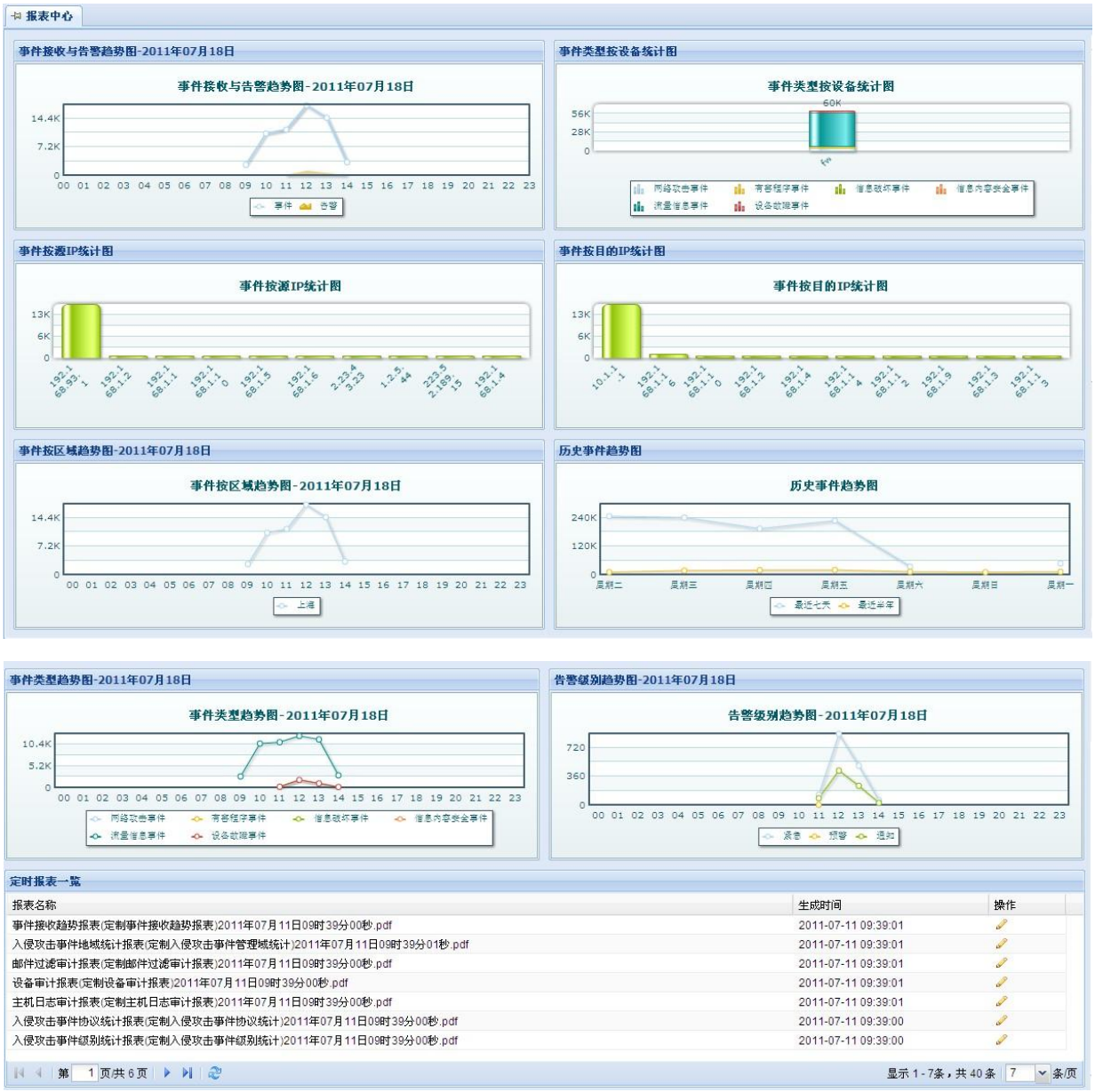
系统提供给用户一个自定义报表的功能，用户可以选择一个常用报表，设置不同的查询条件和时间粒度，系统会根据条件生成一个菜单项，方便用户直接查看，并可以对已生成的菜单进行编辑和删

除操作。

6.2 功能介绍

6.2.1 功能首页

管理中心报表功能的首页展示的是当前系统所管理设备的基本情况，包括事件接收与告警趋势图、事件类型按设备统计图、事件按源 IP 统计图、事件按目的 IP 统计图、事件按区域趋势图、历史事件趋势图、事件类型趋势图、告警级别趋势图以及定时报表一览。

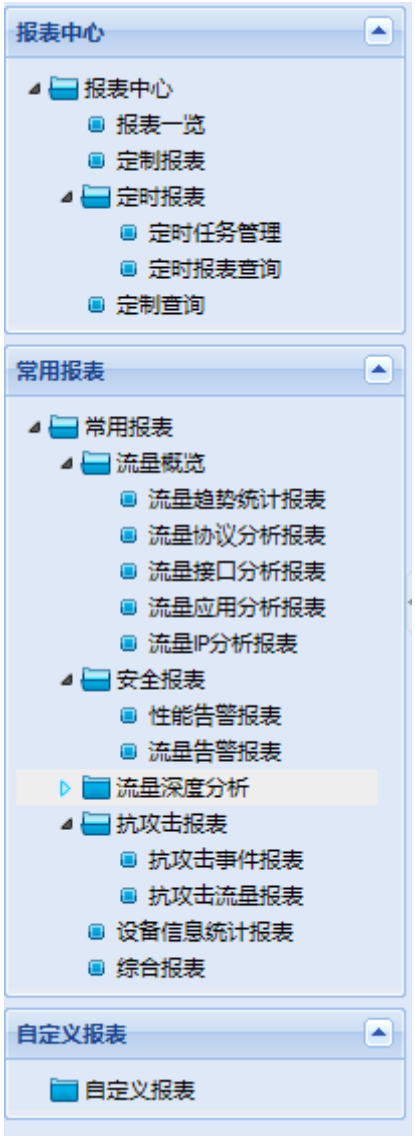


图表 6-1

- 事件接收与告警趋势图：以折线和区域混合的形式显示了当天事件与告警的趋势。

- 事件类型按设备统计图：以堆积图的形式显示了当天事件量最多的前 10 名设备，堆积序列为事件类型。
- 事件按源 IP 统计图：以柱状图的形式显示了当天事件量最多的前 10 名源 IP。
- 事件按目的 IP 统计图：以柱状图的形式显示了当天事件量最多的前 10 名目的 IP。
- 事件按区域趋势图：以多序列折线图的形式显示了当天系统所有管理域的事件量趋势。
- 历史事件趋势图：以多序列折线图的形式显示了最近七天和最近半年同比的事件量趋势。
- 事件类型趋势图：以多序列折线图的形式显示了当天所有事件类型的事件量趋势。
- 告警级别趋势图：以多序列折线图的形式显示了当天所有告警级别的告警量趋势。

左侧边栏是报表功能的全部四大类功能，常用报表及各自所包含的子报表功能、定制报表、定时报表、定制查询。



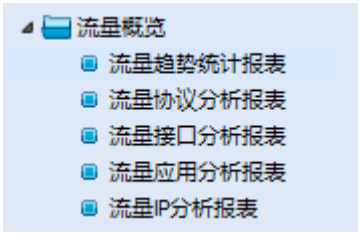
图表 6-2

6.2.2 常用报表

流量概览、安全报表、流量深度分析、抗攻击报表、设备信息统计报表和综合报表。

6.2.2.1 流量概览

流量概览主要分析 Detector 设备发出的流量日志，反映用户当前的网络状况。流量概览功能分为五个子报表，包括流量趋势统计报表、流量接口分析报表、流量协议分析报表、流量应用分析报表、流量 IP 分析报表，各个子报表都分别有侧重的审计了设备的网络流量以及其他情况。默认显示的是当天的流量情况。用户可以点击页面上部的“导出报表”下拉框，保存 PDF、Excel 等报表文件。

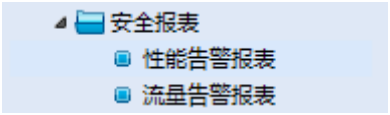


图表 6-3

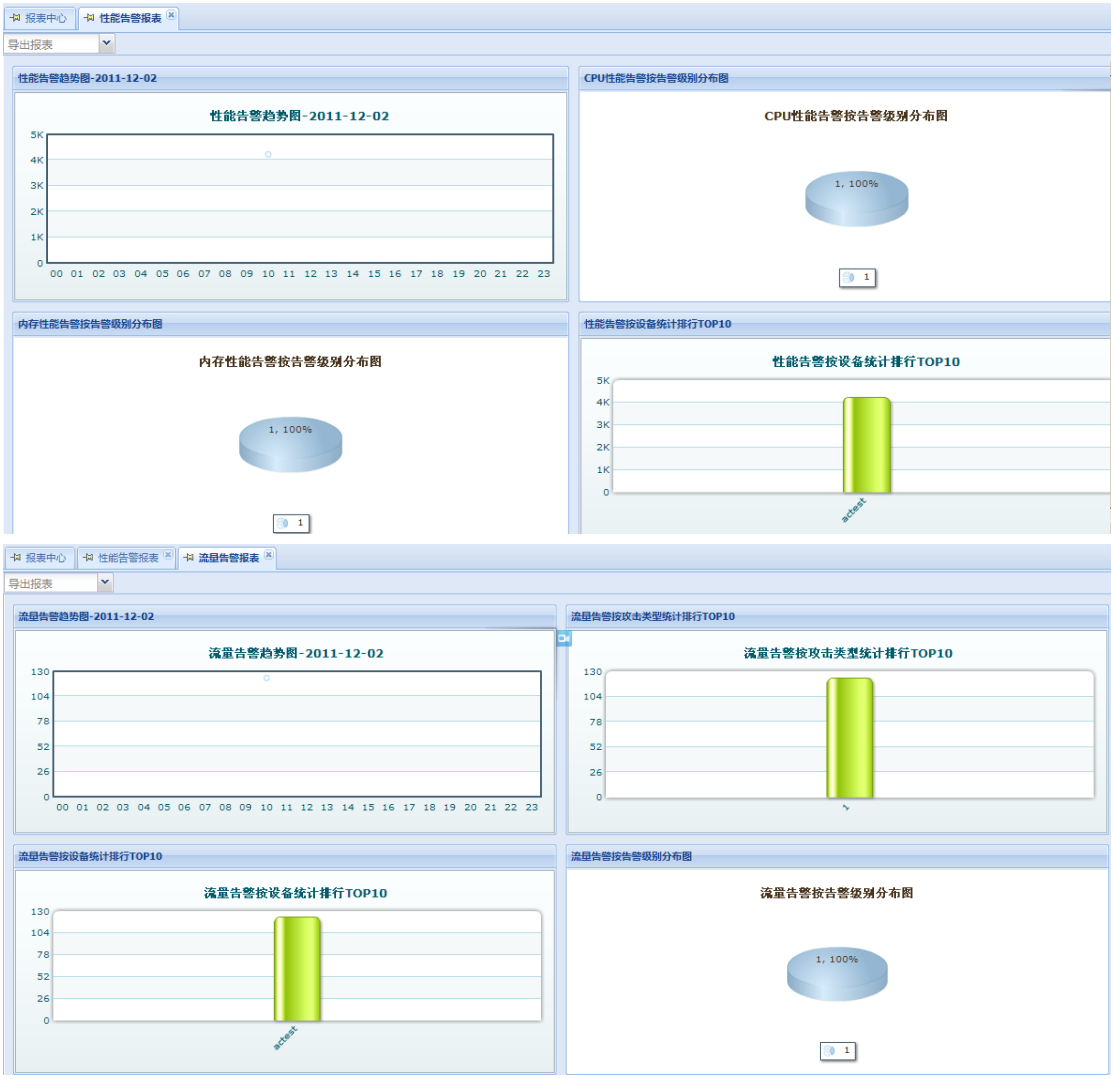
图表 6-4

6.2.2.2 安全报表

安全报表是审计设备本身信息的统计报表。具体包括如下子报表：性能告警报表和流量告警报表。点击报表功能的左侧边栏“安全报表”即可列出上述子报表，用户可以点击任意一个子报表功能，进入对应的子报表功能页面。用户可以点击页面上部的“导出报表”下拉框，保存 PDF、Excel 等报表文件。



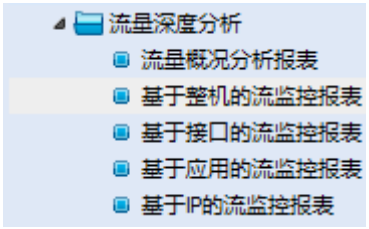
图表 6-5



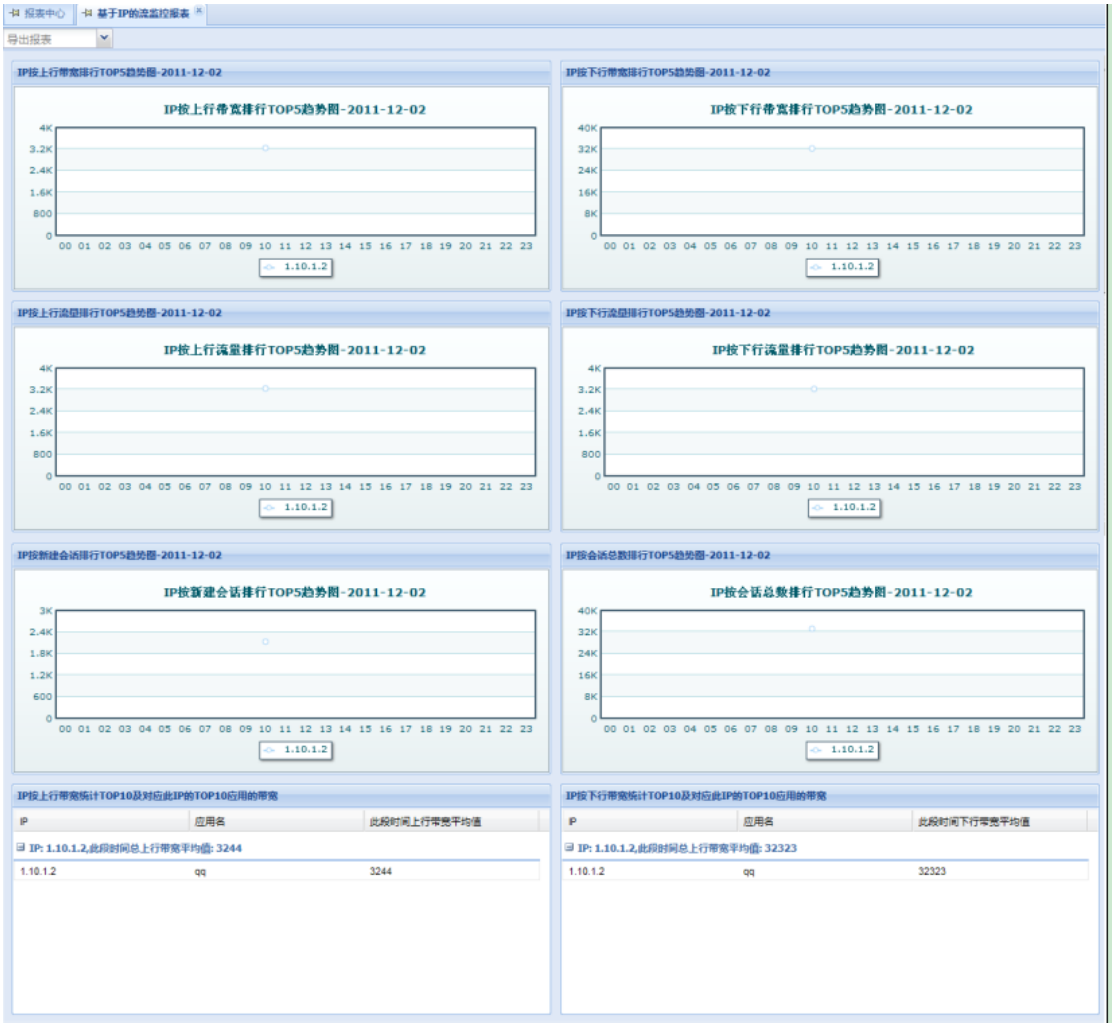
图表 6-6

6.2.2.3 流量深度分析

流量深度分析是分析 Guard 设备上的流量，带宽和会话数的相关日志信息。具体包括如下子报表：流量概况分析报表及基于整机、接口、应用、IP 的流监控报表。点击报表功能的左侧边栏“流量深度分析”即可列出上述子报表，用户可以点击任意一个子报表功能，进入对应的子报表功能页面。用户可以点击页面上部的“导出报表” 下拉框，保存 PDF、Excel 等报表文件。



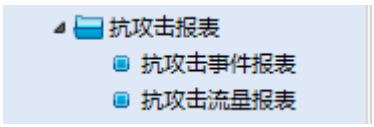
图表 6-7



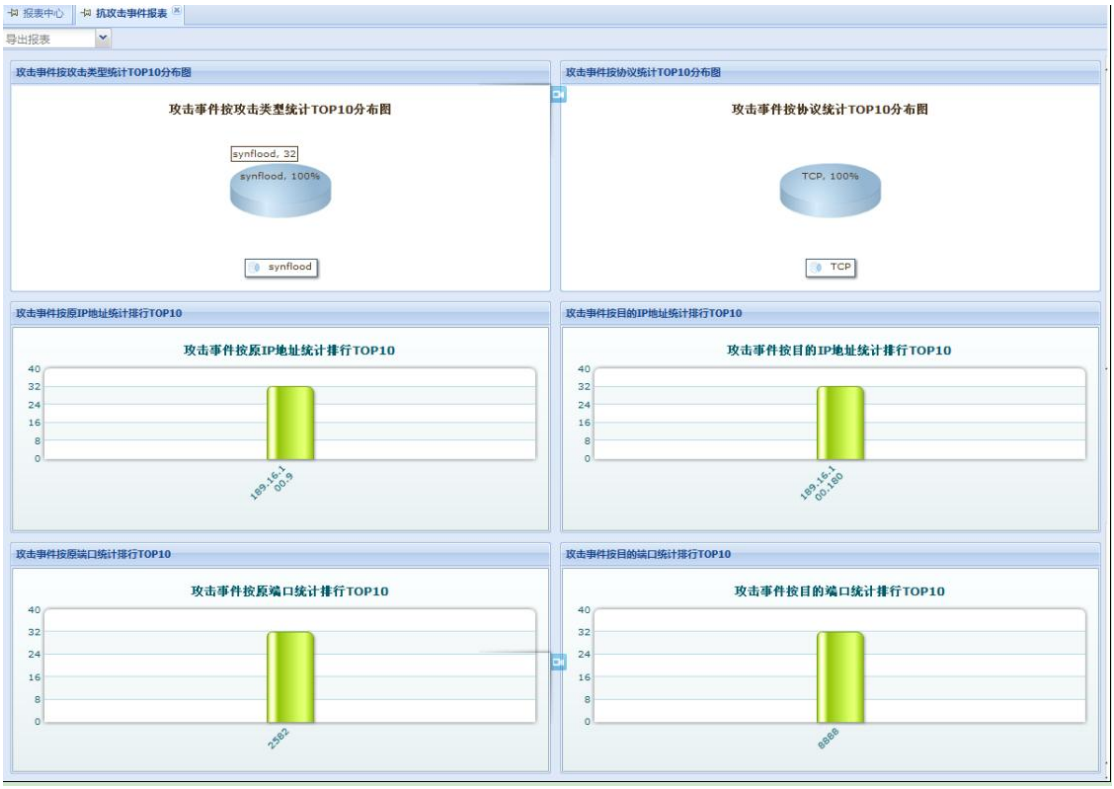
图表 6-8

6.2.2.4 抗攻击报表

抗攻击报表是审计设备攻击事件和攻击流量的相关日志信息。具体包括抗攻击事件报表和抗攻击流量报表两个子报表。点击报表功能的左侧边栏“抗攻击报表”即可列出上述子报表，用户可以点击任意一个子报表功能，进入对应的子报表功能页面。用户可以点击页面上部的“导出报表” 下拉框，保存 PDF、Excel 等报表文件。



图表 6-9



图表 6-10

图表 6-11

6.2.2.5 设备信息统计报表

设备信息统计报表是审计设备运行产生的相关日志信息。具体包括：TOP5 设备 CPU 使用率趋势图、TOP5 设备内存使用率趋势图、TOP5 设备流入流量使用率趋势图、TOP5 设备流出流量使用率趋势图。用户可以点击页面上部的“导出报表”下拉框，保存 PDF、Excel 等报表文件。

图表 6-12

6.2.2.6 综合报表

综合分析报表是对当前设备的日志分析的一个综合展示,包括流量趋势图、TOP10 攻击类型的攻击报文速率分布图、性能告警按规则分布图和 TOP10 攻击类型流量告警的统计图。用户可以点击页面上部的“导出报表”下拉框，保存 PDF、Excel 等报表文件。

图表 6-13

6.2.3 定制查询

6.2.3.1功能概述

定制查询方便用户以所关心的设备、IP 地址、端口、协议、时间等为条件进行一次性的审计查询。用户首先从报表下拉框中选择一个常用报表，之后可以自定义报表名称，选择查询条件以及时间粒度等等。查询后的审计结果与常用报表的审计结果一样，只是条件是由用户自定义的。定制查询与常用报表相同，可以将审计结果导出成 PDF、EXCEL 等格式的报表文件。

图表 6-14

6.2.4 定时报表

6.2.4.1功能概述

系统为每种常用报表都提供了定时报表的功能，用户可以预先配置好审计查询参数后，设定生成此报表的定时任务，当到达对应时刻，系统会自动的进行报表的生成，用户可以对已生成的报表进行查询和下载，同时，系统还提供定时任务的管理功能，用户可以对已添加的定时任务进行开始（暂停）、恢复和删除等操作，方便管理使用。定时报表功能在左侧边栏处。

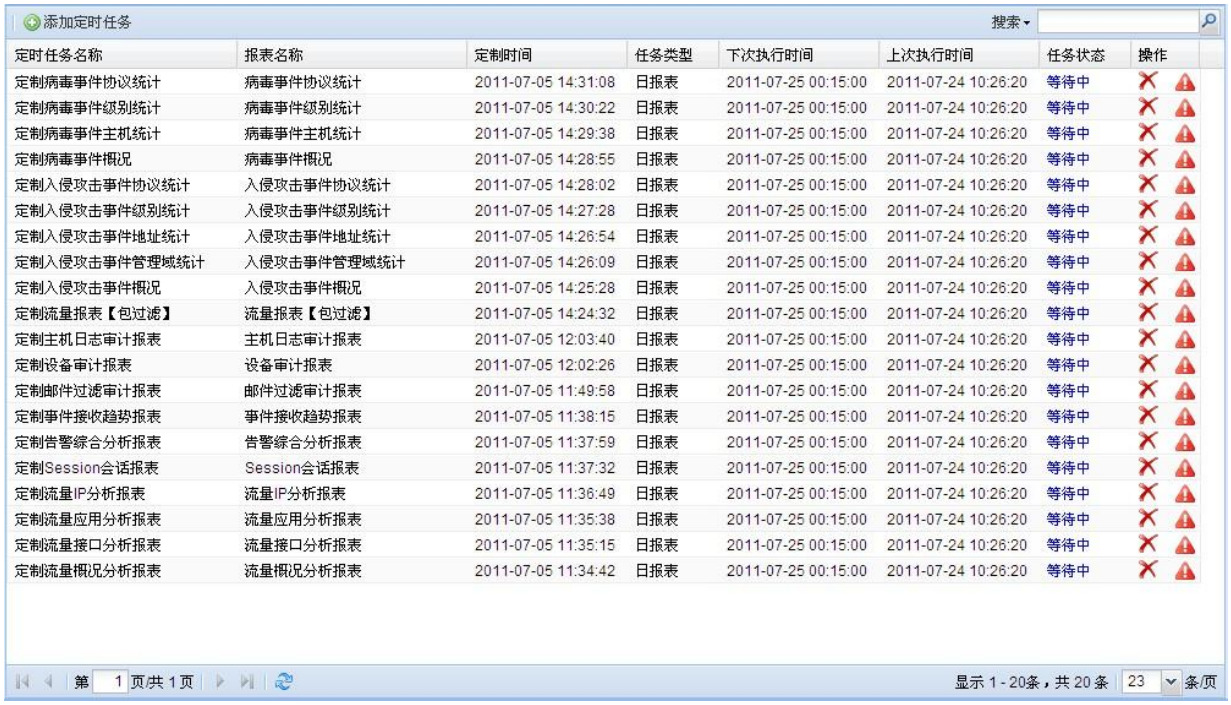
定时任务，是用户指定一个时间频率，系统会按照用户指定的时间频率，比如“每天生成一次”、“每月生成一次”、“每年生成一次”等，系统会自动的在到达时间的时候生成报表。

6.2.4.2定时任务管理

在定时任务管理模块中，系统为每个常用报表统一提供了定时任务的配置和浏览用户定义的所有定时任务的功能。用户可以从报表下拉框中选择一个常用报表，之后可以设置定时任务名称、生成频率（天、月、年）、任务描述、选择关心的设备名称、IP 地址、端口、协议等等自定义条件。

图表 6-15

当用户配置好定时任务后，点击“提交”按钮，系统即开始任务的计时，当到达任务点时，会自动的开始执行定时任务。用户可以在定时报表功能的“定时任务管理”模块下看到已经定时的任务，同时可以进行管理操作。

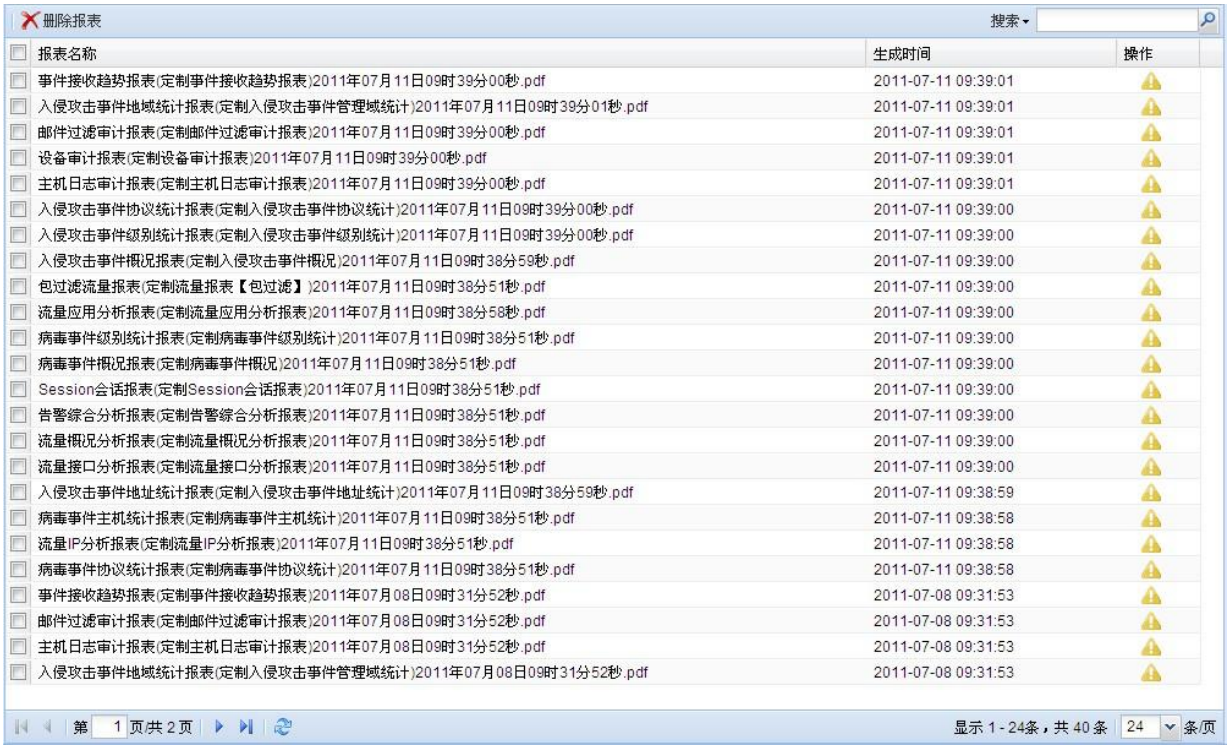


图表 6-16

在定时任务管理页面，用户可以查看到当前系统已经添加的定时任务及任务的类型和状态，每个任务都有一组操作按钮：“暂停”（“恢复”）、“删除”，方便用户对定时任务进行相应的管理操作。

6.2.4.3定时报表查询

当系统定时生成好报表后，用户可以在“定时报表查询”功能处，对已生成的定时报表进行管理操作。



图表 6-17

用户可以对已生成的定时报表进行“下载”和“删除”操作。

6.2.5 定制报表

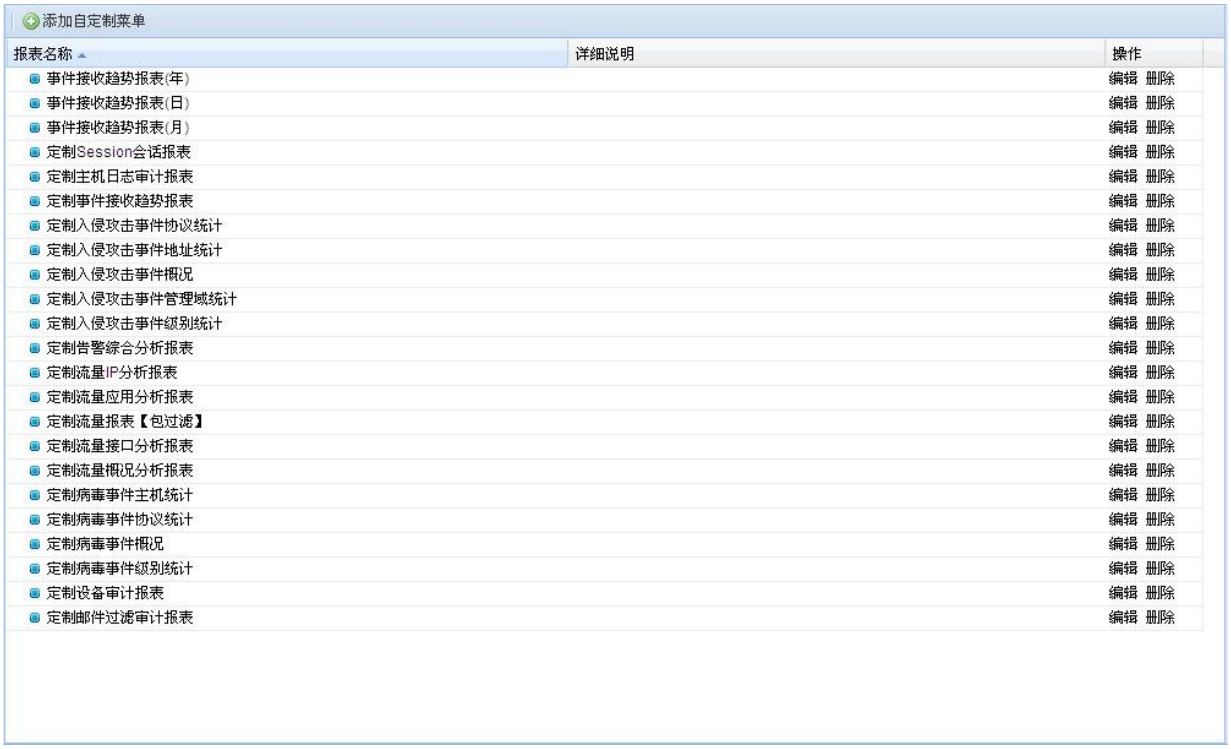
6.2.5.1功能概述

系统提供给用户一个定制报表的功能，让用户可以根据自己的需要，以所关心的设备、IP 地址、端口、协议、接口等为条件，在左侧栏生成一个报表菜单，以供用户随时查看。

用户可以从报表下拉框中选择一个常用报表，之后可以设置菜单名称、时间（本天、本月、本年）、描述、自定义条件。点击“提交”按钮后，系统便会为用户生成一个对应的报表菜单。

图表 6-18

用户可以对已经生成的报表菜单进行编辑和删除操作，以满足各种需要。



图表 6-19

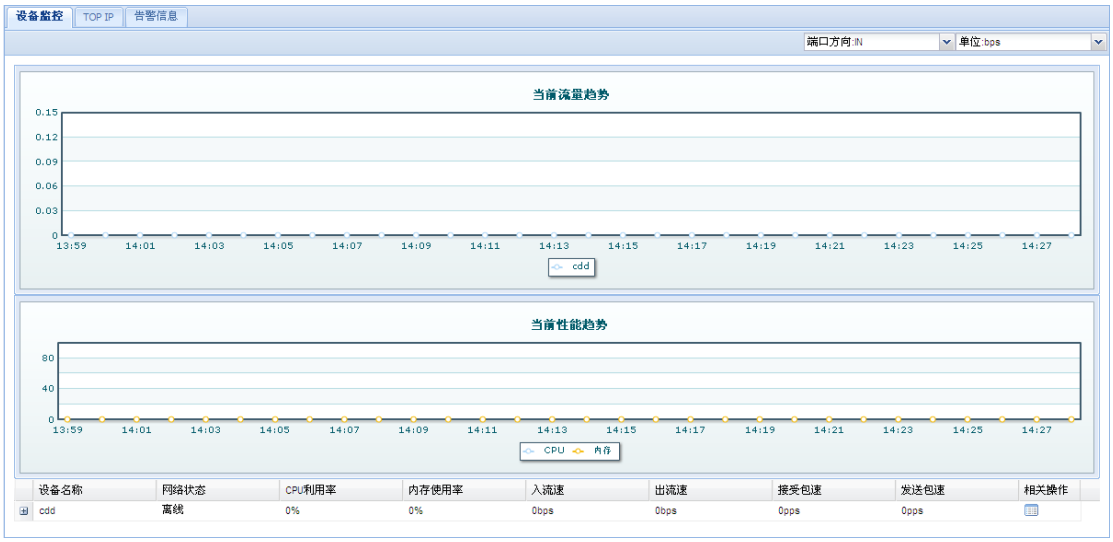
第七章 设备监控

7.1 设备监控

实时监控模块，向用户展示该设备的流量实时情况。包括设备的总流量、TCP 协议流量、UDP 协议流量、STACK 协议流量趋势。以及设备的总攻击流量趋势，同时也展示 TCP 协议攻击流量趋势、UDP 协议攻击流量趋势、STACK 协议流量趋势等等。

点击【端口方向】可以选择流入/流出端口

点击【单位】按钮可以选择曲线图中显示图例的单位



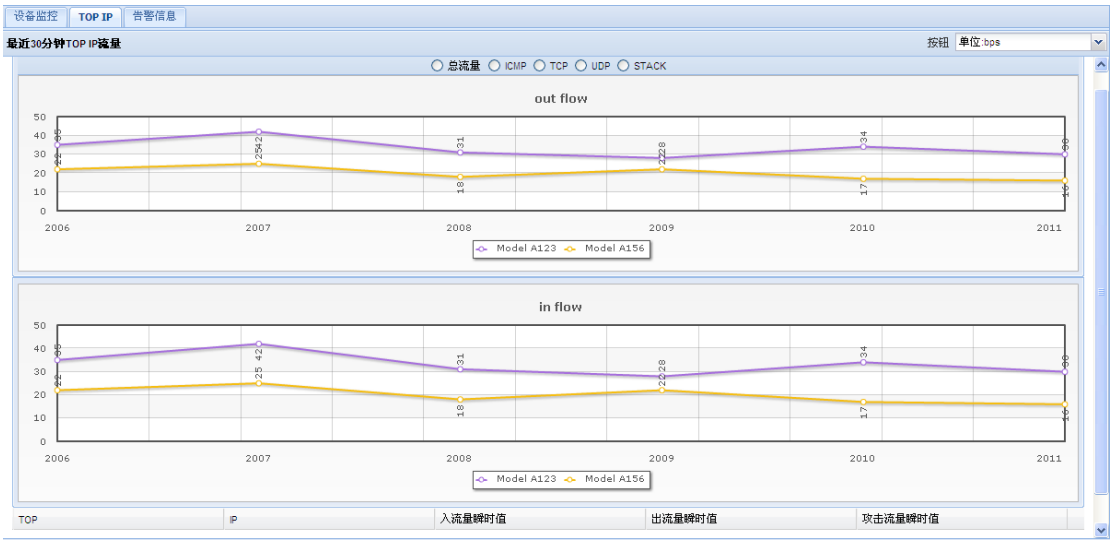
图表 7-1

7.2 TOP IP

TOPIP 监控展示节点下流量最大十个防护设备的瞬时出入端口流量、攻击流量。并展示最近一小时内牵引流量和攻击流量的趋势(可以根据 ICMP、TCP、UDP 等协议以及不同流量单位查看)。

点击界面顶端的单选按钮【总流量】【ICMP】【TCP】【UDP】【STACK】选择流量曲线图显示的内容。

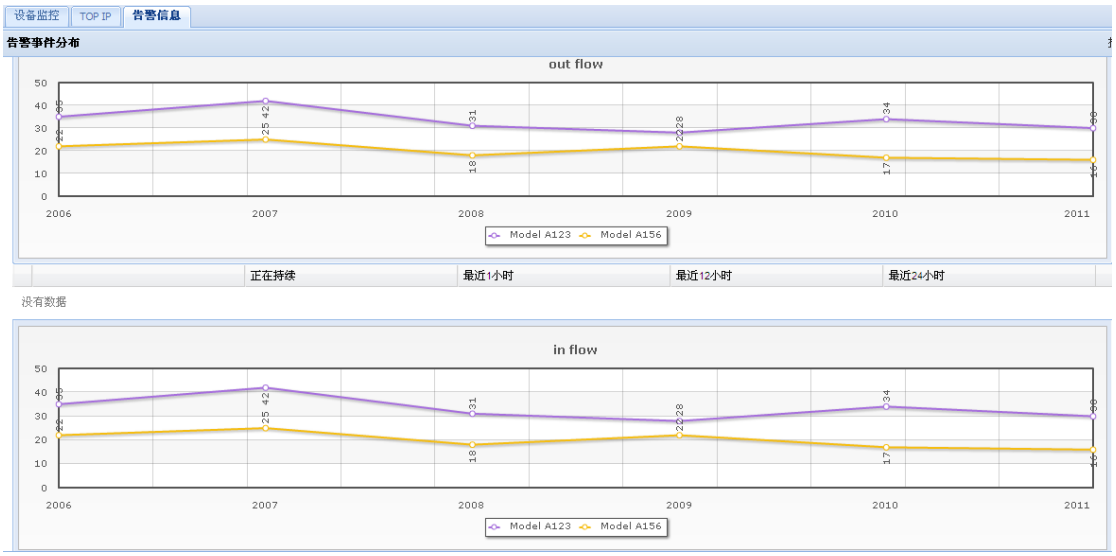
点击【单位】下拉菜单可以选择显示流量曲线的单位。



图表 7-2

7.3 告警信息

告警信息监控，对管理中心管理的 Detector 和 Guard 系列产品所检测到的流量异常告警事件（一般指各类 DOS 攻击事件）进行统计和展示。对管理中心管理的 Detector 和 Guard 系列产品的性能（主要指 CPU 和内存）超出阈值的告警进行统计和展示。同时对流量告警和性能告警均需按照正在持续、最近 1 小时、最近 12 小时和最近 24 小时的时间粒度统计不同告警级别的事件数。并按不同时间粒度展示其实时告警趋势。

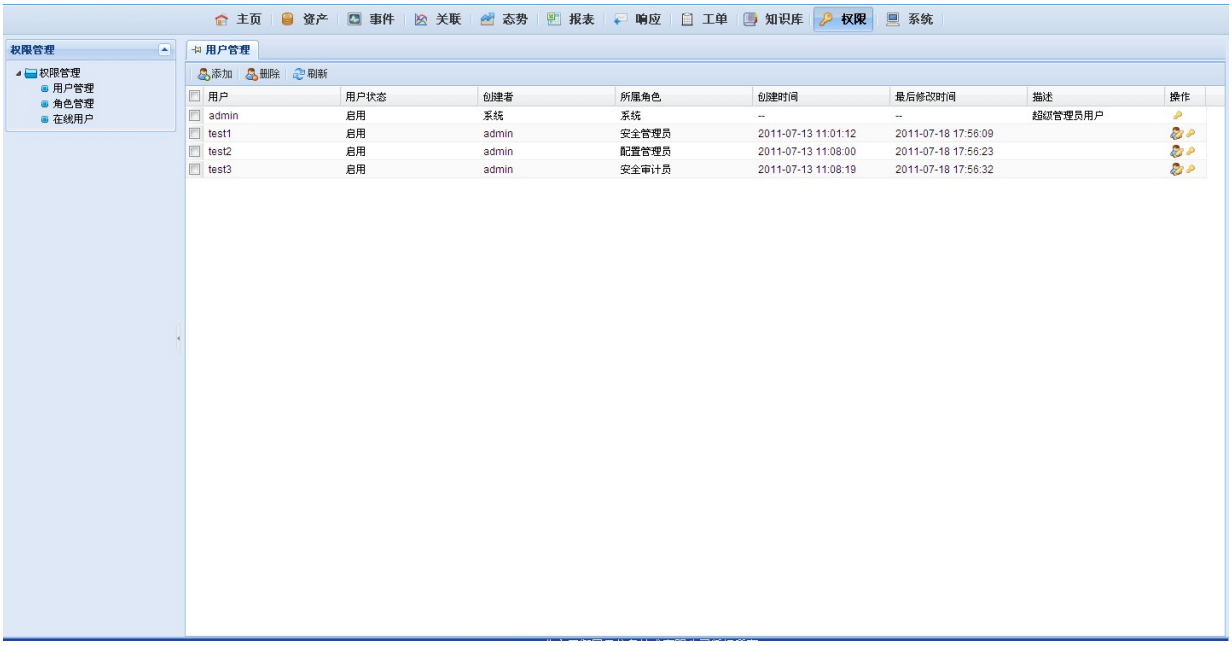


图表 7-3

第八章 权限管理

权限管理包含用户管理和角色管理、在线用户三个功能。

进入到权限管理操作界面，如图所示：



图表 8-1

8.1 用户管理

点击【用户管理】，进入用户管理操作页面

8.1.1 添加用户

点击【添加】按钮，则进入添加用户操作界面，如图所示：

图表 8-2

在相应的输入框输入信息，“所属角色”为用户所具有的权限，密码必须由八位以上数字、字母组合。注意：带红色星号标识的为必填项。填写完成后点击【提交】按钮，则返回用户操作界面，并显示新添加的用户。点击【重置】按钮，则清空填写内容。点击【返回】按钮，返回用户操作界面。

8.1.2 修改用户信息

点击【修改属性】按钮，进入修改用户信息界面，如图所示：

图表 8-3

在相应的输入框输入需要修改的属性内容，【启用】代表该用户可以使用；【禁用】表示该用户不能使用，须编辑启用后才能进行使用，带红色星号为必填项，填写完成后，点击【提交】按钮，则返回用户操作表，用户操作表会显示最新修改结果。点击【重置】按钮，则回复修改前状态（注意：admin 用户不能进行编辑）。点击【返回】按钮，返回用户操作界面。

8.1.3 修改密码

点击【修改密码】按钮，则进入修改密码界面，如图所示：

图表 8-4

修改密码时，不需要输入旧密码，直接输入新密码即可，要求两次输入的密码必须相同并且密码必须由八位及以上数字和字母组合而成，确认后点击【提交】按钮，则返回用户操作表，修改完成。点击【重置】按钮则清空填写的新密码。（注意：admin 用户不能进行密码修改）。点击【返回】按钮，返回用户操作界面。

8.1.4 删除用户

选择要删除的用户，点击【删除】按钮，则弹出确认删除对话框，点击【是】按钮，则删除该用户，点击【否】按钮则不删除用户。（注意：admin 用户不能进行删除）

8.2 角色管理

点击【角色管理】管理链接，则进入角色管理操作页，如图所示：

图表 8-5

8.2.1 添加角色

点击【添加】按钮，弹出如下添加角色界面：

图表 8-6

在相应的输入框添加信息，带红色星号的为必填项，角色分为三种类型：安全管理员、配置管理员、安全审计员。

角色类型	角色权限
安全管理员	可操作菜单：系统主页、集中管理、设备监控、系统管理。
配置管理员	可操作菜单：系统主页、权限管理。
安全审计员	可操作菜单：系统主页、事件查询、统计报表

填写完成后，点击【提交】按钮，则添加角色，并返回角色操作表。在角色操作表中显示新添加的角色。点击【重置】按钮，则清空用户填写内容。点击【返回】按钮，返回角色操作界面。

8.2.2 修改角色

点击角色表中【修改】按钮，则弹出修改角色页面，如图所示：

图表 8-7

操作过程与添加角色过程相同，请参照添加角色过程。

8.2.3 删除角色

点击角色列表【删除】按钮，则弹出确认删除对话框，如果点击【是】按钮，则删除角色，点击【否】按钮，则不删除角色。

8.3 在线用户列表

点击【在线用户】链接按钮，则页面进入，如图所示：

图表 8-8

如果想看到当前在线用户最新信息，点击【刷新】按钮，则显示当前最新在线用户列表。

第九章 系统管理

系统设置模块主要用来查看系统总体状态、设置系统参数、维护日志、管理事件服务器等。

图表 9-1

9.1 系统管理

9.1.1 系统参数配置

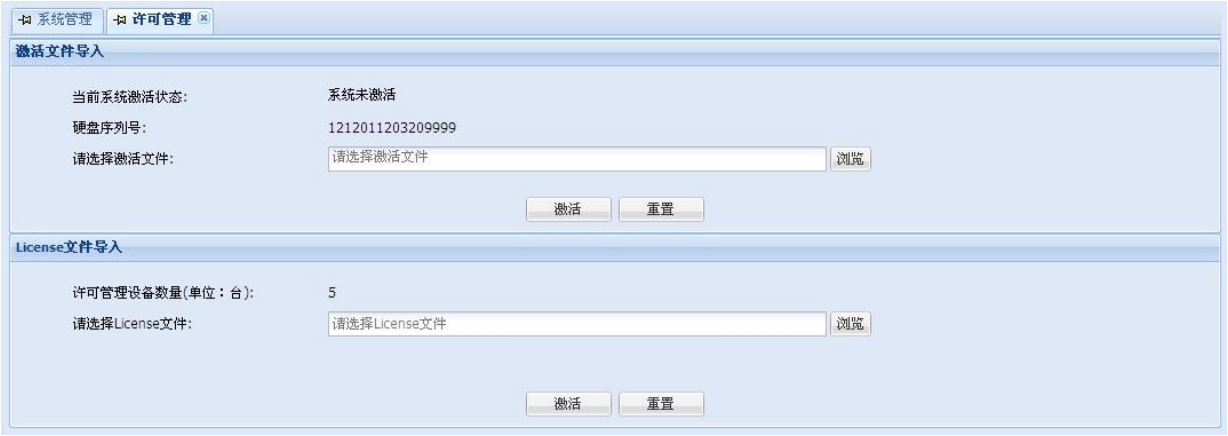
该功能用来配置服务器相关的一些参数，包括系统超时登录时间，系统日志自动删除时间，SNMP 字符串等。

图表 9-2

9.1.2 许可管理

本功能用于显示当前许可证可以管理和审计设备数量， 以及导入数量控制型许可证文件。界面

如图所示：



图表 9-3

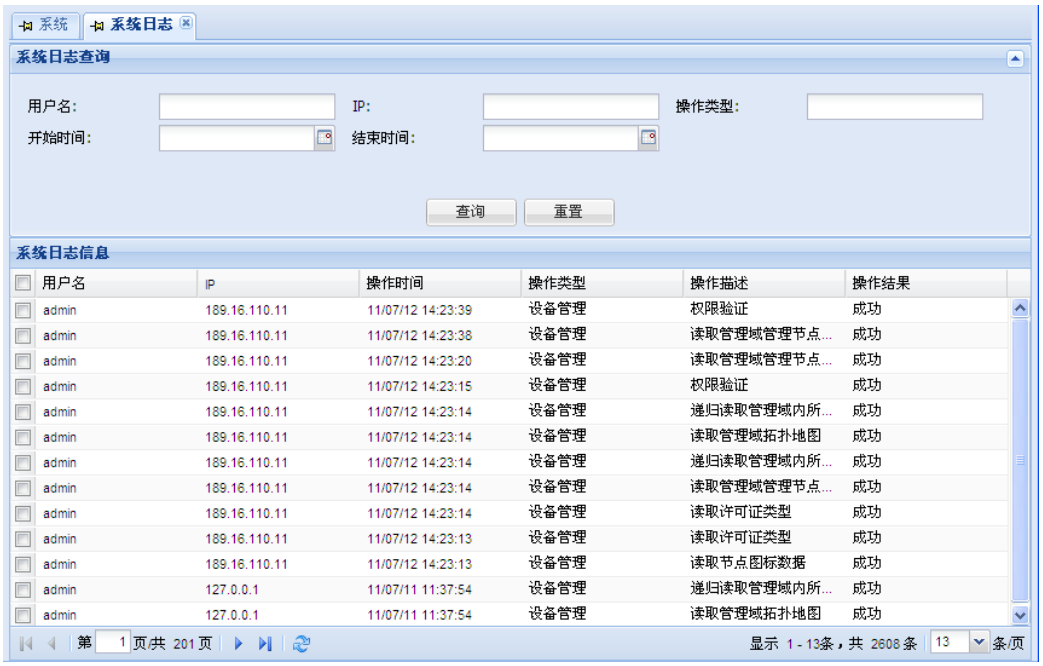
登录时间超时设置；该项目设置登录之后多长时间不操作，系统超时自动注销。取值范围是 1~120 分钟，默认值为 60 分钟。

系统日志自动删除时间设置；该项目设置系统自动删除多少天之前的用户操作日志。取值范围是 1~180 天，默认值为 90 天。

SNMP Trap 团体字符串设置；该项目默认值为“public”。

9.1.3 系统日志

可以查看系统操作日志，并可按用户名、操作类型、IP、开始时间、结束时间等条件组合查询相应的操作日志，并可设置每页显示的记录数量。界面如图所示：

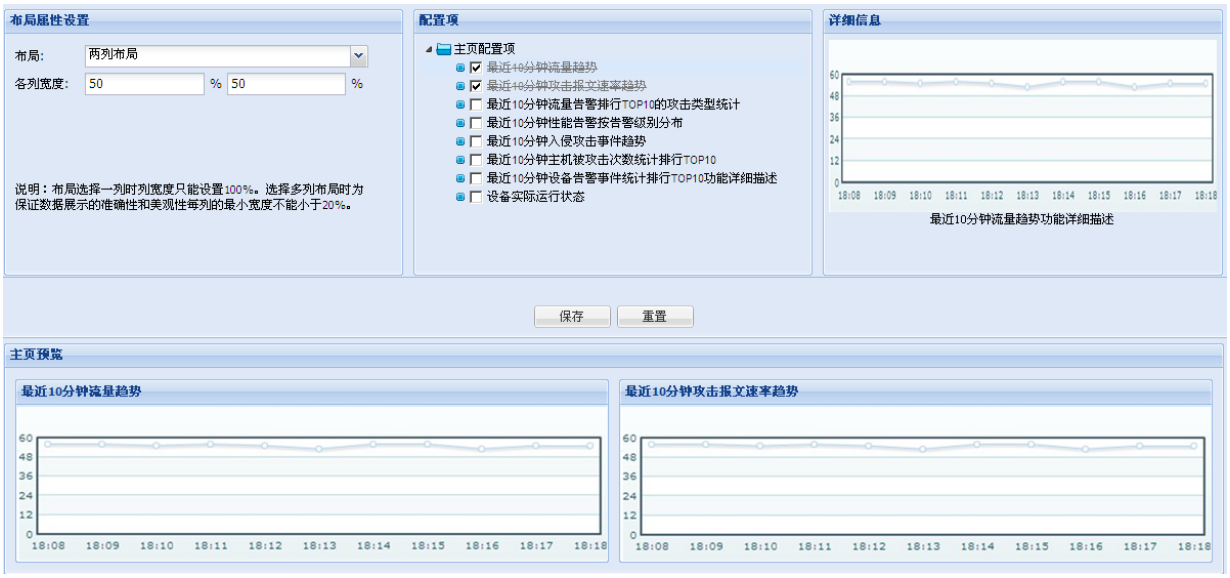


图表 9-4

进入该功能后，默认分页显示所有操作日志。输入查询条件后，可过滤显示指定条件的日志。例如，输入用户名 admin，点击“查询”，则会显示用户 admin 的所有操作记录。

9.1.4 主页配置

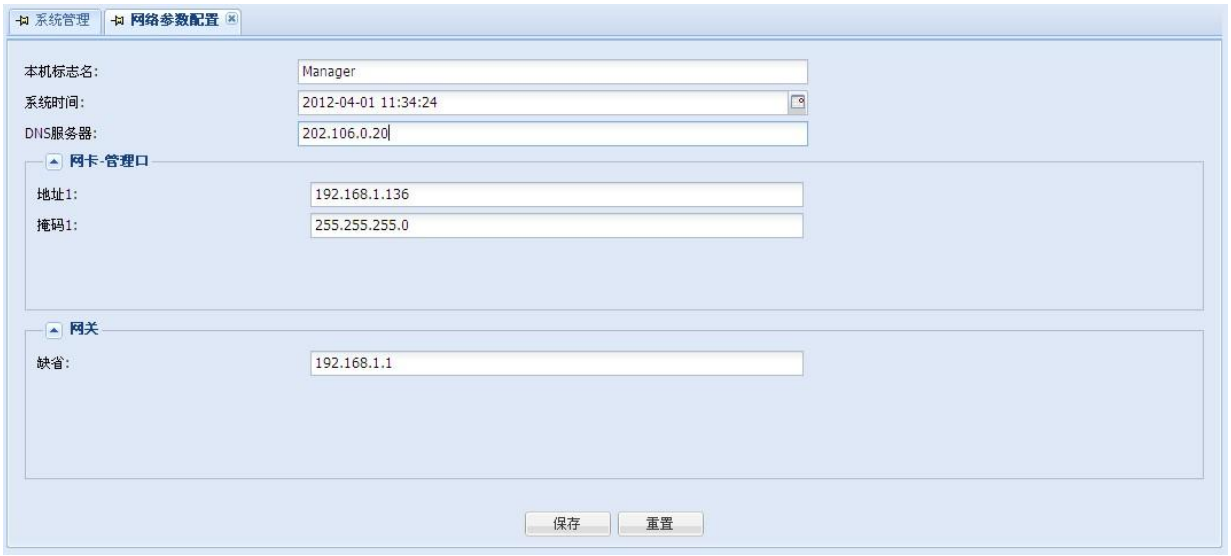
该功能用来对主页显示的项目属性进行配置。主要包括布局列数（一列、两列、三列、四列）、各列宽度百分比、各功能项是否展示、各功能项的位置（以鼠标拖动的方式来设置项目的位置关系）以及功能项的详细说明。点击保存按钮后，再次进入主页时便会呈现出配置好的项目。



图表 9-5

9.1.5 网络参数

该功能用来对系统的网络参数进行配置，包括主机名、系统时间、DNS 服务器、网卡地址、掩码、网关等。



图表 9-6

9.2 日志维护

9.2.1 日志备份管理

通过设定条件，进行日志的备份。默认的导出路径为：（系统安装路径）/resource/backupdata。在系统设置页面中，点击“日志备份”，进入日志备份页面

图表 9-7

该页面分为 4 部分：

- 操作状态：显示系统现在的状态，有两种情况：其一，当前无操作，此时系统处于空闲状态，可以进行日志的导出，并且状态栏中会显示上次操作的信息（操作用户，操作时间，操作类型，操作结果），初次使用则各种状态显示为“0”；其二，操作中，此时系统处于忙碌状态，不能进行日志的导出，并且状态栏中会显示当前操作的信息（操作用户，操作时间，操作类型，操作结果）；上次备份时间，显示上次备份日志的时间；磁盘总空间，系统安装盘符的总空间；磁盘剩余空间，系统安装盘剩余的空间，点击“刷新”按钮可以进行页面的刷新
- 备份路径：显示日志导出到服务器的路径，点击“保存”按钮，可以进行保存
- 自动备份：设置自动备份的选项，启用复选框选中，日志会进行自动备份，反之，不进行自动备份，默认为启用；备份周期为日志自动备份的周期长度，默认为按天备份，可根据实际情况修改，点击“保存”按钮，进行备份设置保存，点击“重置”按钮，可以初始化为原始值。
- 手动备份：可以随时手动备份日志，开始时间和结束时间均不可为空，指定设备为可选项，作用是进一步细化导出条件。默认（不选）情况下，系统将导出指定时间范围内的所有设备和所有日志类型的日志，点击“备份”按钮，系统开始进行备份操作，点击“重置”按钮，可以初始化时间及设备文本框。

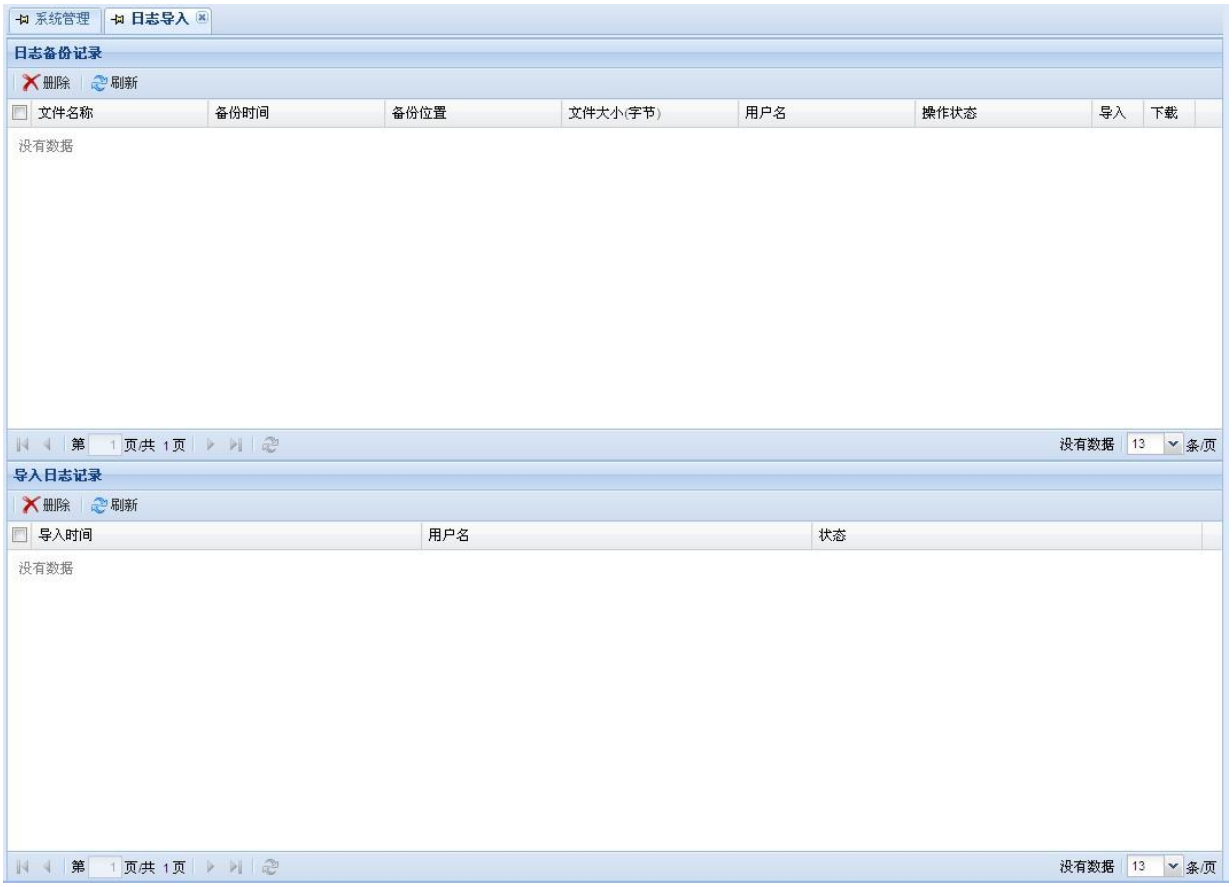
9.2.2 日志导入管理

导入日志到数据库，以便查询。

该页面分为

注意：用于导入的数据包必须为系统导出的数据包，并且未做过修改，且只能在服务器上操作

系统设置页面中， 点击“日志导入”，进入日志导入页面



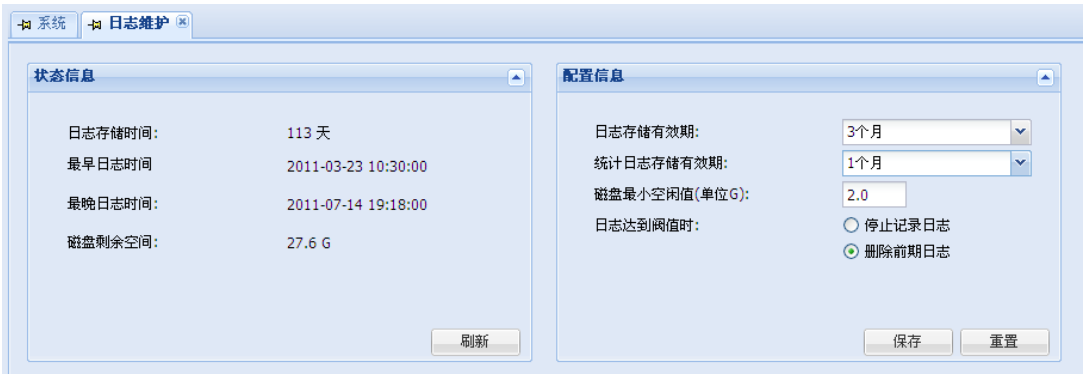
图表 9-8

该页面分为 2 个部分：

- 导入安全日志：输入要导入数据完整路径，点击“导入”便可进行日志的导入。
- 导入日志信息：显示导入日志记录，顺序从最近的开始，分页显示

9.2.3 日志维护

显示当前的日志状态信息及日志自动维护配置设置。



图表 9-9

该页面分为 2 个部分

- 状态信息：日志存储时间，指的是日志最早日志到最晚日志的时间；日志最早时间，最早日志的时间；日志最晚时间，最晚日志的时间；磁盘剩余空间，系统所在磁盘的可用大小/总大小
- 配置信息

【日志存储有效期】：日志存在的有效期，单位为月 ，超过有效期的日志将被自动删除，为了您的日志完整，该值的设置请大于备份周期，默认为 3 个月。

【统计日志有效期】：统计日志存在的有效期，单位为月 ，超过有效期的统计日志将被自动删除，默认为 1 个月。

【磁盘最小空闲值】：保证系统正常运行，系统所在磁盘的最大空闲值。不满足最小空闲值时，系统将进行自动维护，停止记录日志，或者删除前期日志。

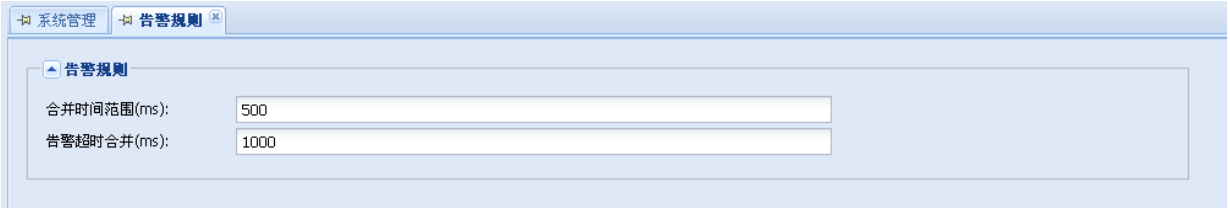
【日志达到阈值时】：确定系统所在磁盘空间报警时所采取的操作，“停止记录日志”：保存日志的前期数据，不存储现有的日志信息；“删除前期日志”：保存日志的现在数据，删除前期数据。

- “保存”和“重置”按钮

9.3 告警管理

9.3.1 告警规则

该功能主要用来配置响应告警的时间与范围，单位为毫秒，页面如下图所示：



图表 9-12

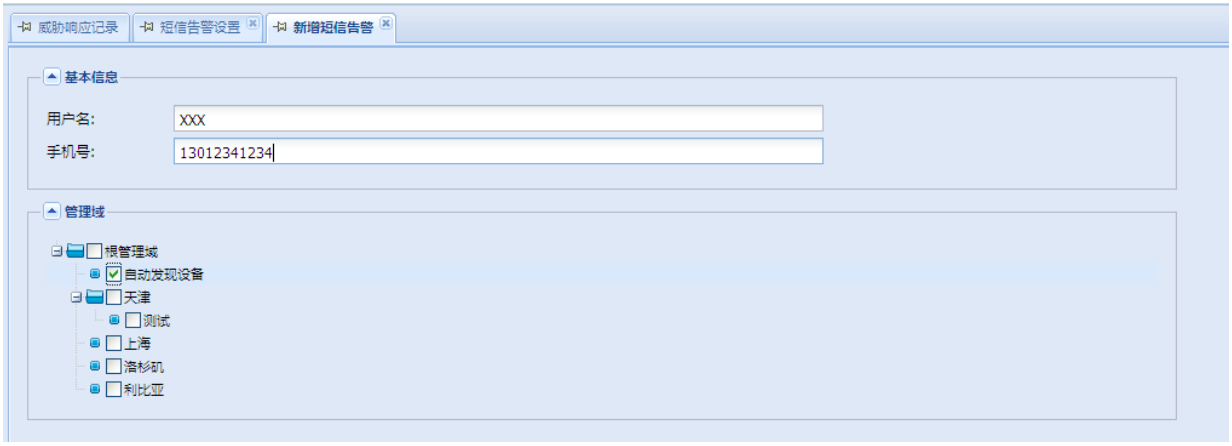
9.3.2 告警阈值

该功能主要用来配置 CUP 告警、内存告警的响应范围，以百分比来衡量，页面如下图所示：

图表 9-13

9.3.3 短信告警

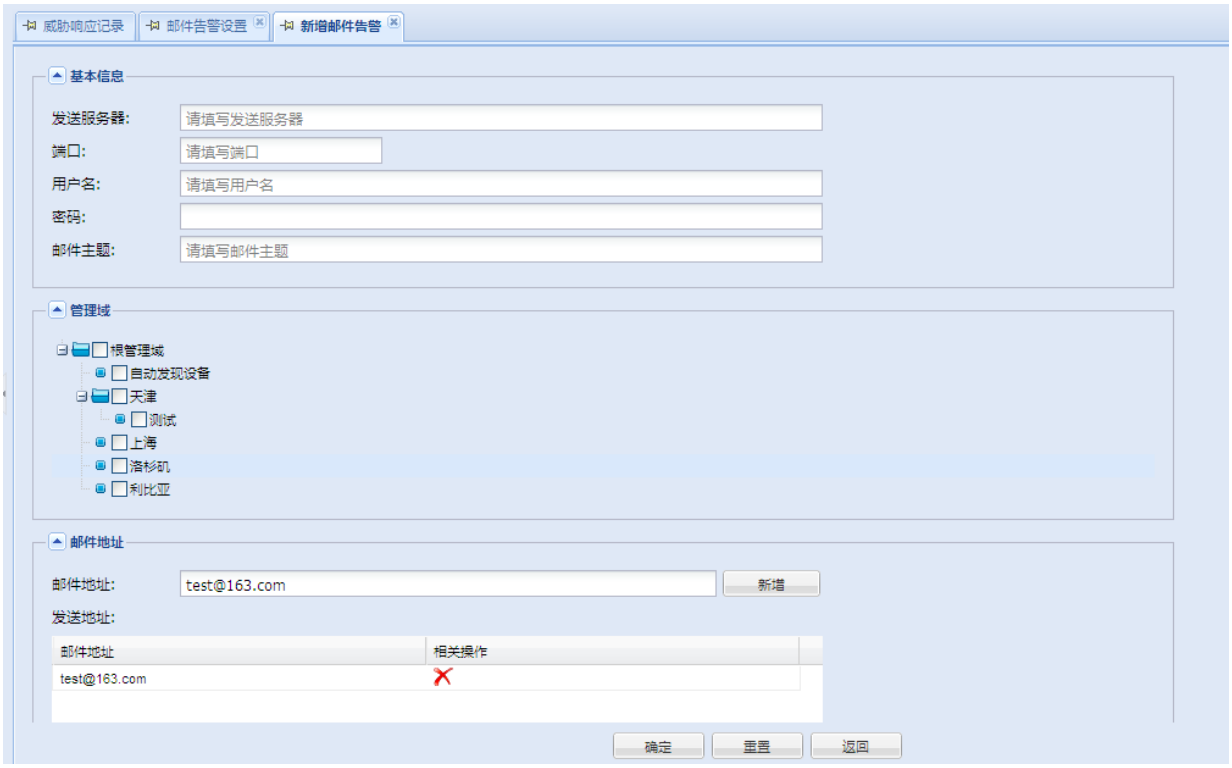
在短信告警设置中可以按域添加需要收到短信的手机号，当该域的设备发生告警，会发送短信给属于该域的手机号。根管理域的手机号会收到所有管理域的告警短信。新增短信告警配置的效果，如图 9-14 所示



图表 9-14 新增短信告警图

9.3.4 邮件告警

邮件告警用于设置发送邮件的服务器配置以及接收告警的邮件列表。每个域上配置的邮箱会收到该域的设备告警邮件，根管理域的邮箱会收到所有域的告警邮件。效果如图 9-17 所示



图表 9-17 新增邮件告警图

9.4 服务器管理

9.4.1 系统服务器信息

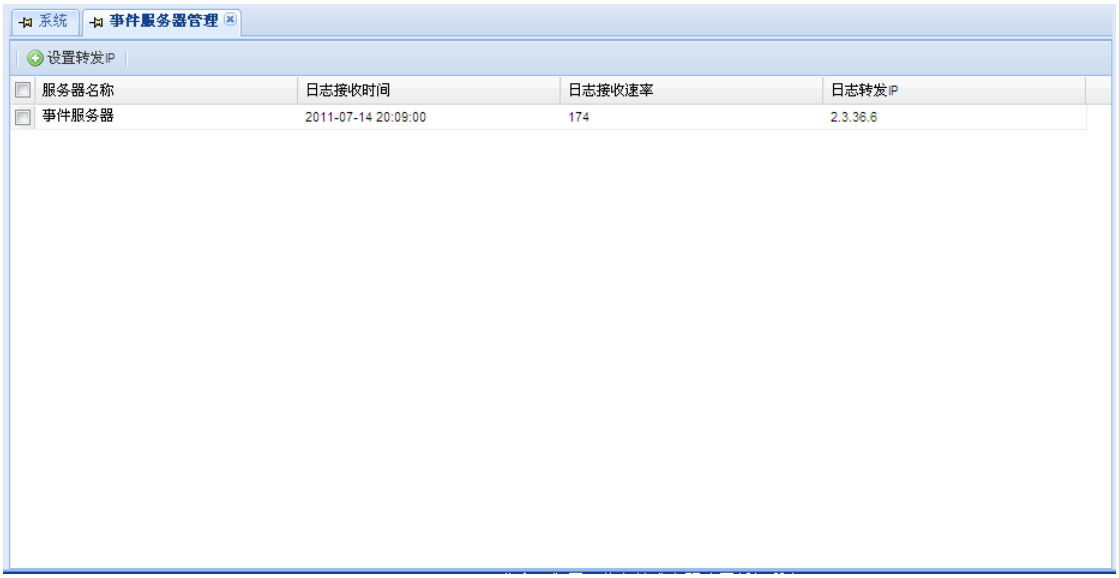
系统服务器用来展示系统的内存状态，产品信息等，包括物理内存总数，物理内存空闲值、JVM 空闲内存、JVM 最大内存、CPU 使用率、产品名称、产品版本及许可数量等，页面如下图所示：

图表 9-18

9.4.2 事件服务器管理

此功能可以将管理中心收到的 Syslog 日志转发给第三方 Syslog 服务器。

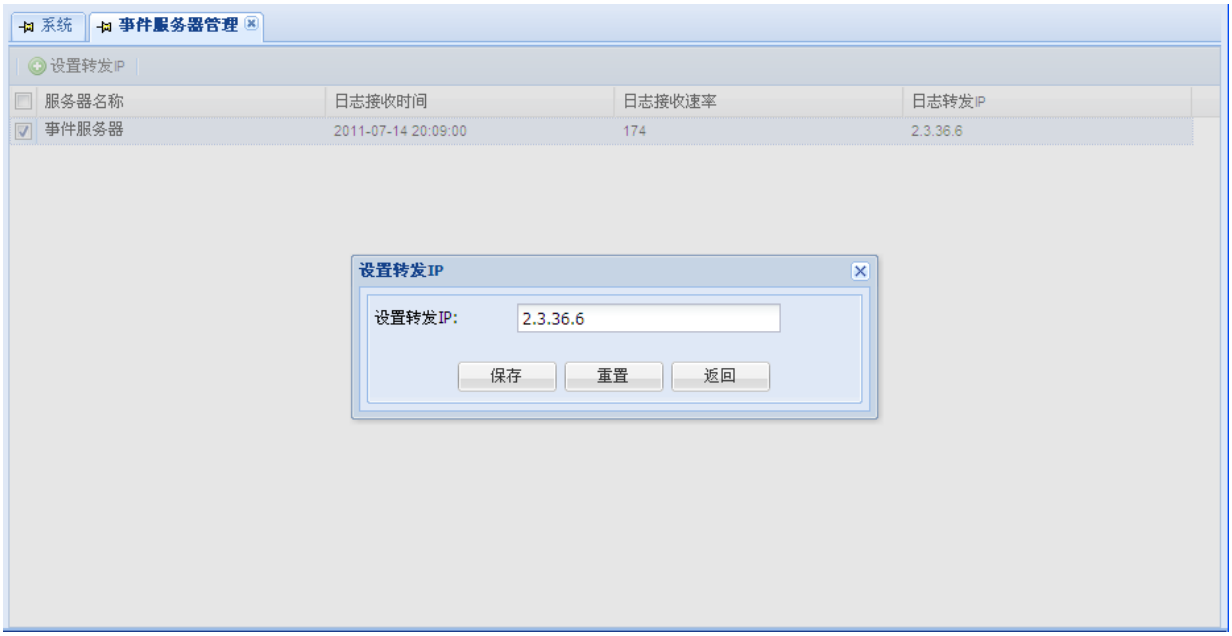
事件服务器管理界面如图所示：



图表 9-19

在本页面列出了事件服务器名称、运行状态、最近日志接收时间、日志接收速率、日志转发 IP 等内容。

在【操作】栏位中，有“设置转发 IP”功能。进入之后，可以设置事件服务器日志转发 IP，如图所示：



图表 9-20

输入想要转发的 IP 地址后点击确定，即可保存转发 IP 设置。

9.5 帮助

9.5.1 帮助文档

点击【帮助文档】链接，将打开系统帮助文档。帮助文档为 PDF 格式，因此需要客户端 PC 预先安装支持查看 PDF 文件格式的工具。