HIRSCHMANN IT

A BELDEN BRAND

参考手册

图形化用户界面

RAVEN4000 入侵检测与管理系统

图形化用户界面

发布 1.0 10/2020

技术支持

https:// www.belden.com.cn

即使没有特别说明，本手册中对版权商标的命名也不应该被认为是指这些名称在商标和商号保护 法的意义上被认为是免费的，因此也不得认为它们可以被任何人自由使用。

本文描述的性能特点只有在合同签订时已经明确商定时才具有约束力。本文件由 Belden 尽可能根据本公司所掌握的情况制作而成。Belden 保留更改本文件内容的权利，恕不另行通知。Belden 不保证本文件中信息的正确性或准确性。

对于因使用网络组件或相关操作软件而导致的损害，Belden 不承担任何责任。另外，我们还援引许可合同中规定的使用条件。

您可以通 Internet 在 Hirschmann IT 产品网站上获得本手册的最新版本

网址为 https://hirschmann-it.support.belden.com。

安全约定

安全管理

默认的，设备应当放置在安全、可靠的位置；所有的物理访问者都应是得到授权的操作员；使用的命令行脚本应当得到妥善的保管、更新和审核。

安全传输

Hirschmann IT 设备支持多种管理方式，包括 Telnet，SSH，HTTP，HTTPS 等，任何非加密的管理方式都是不推荐的。我们高度建议我们的用户仅使用 SSH 和 HTTPS 作为管理途径，以确保所有的管理流量都是加密的。

安全存储

登录设备使用的凭据、设备的配置和状态数据，应当被保管在合适的地方并定期更新，并且仅有有权限的人可以查阅和管理。

目录

第1章 首页介绍

1.1 概述

通过运行 Internet 浏览器的任何计算机使用 HTTP 或一个安全的 HTTPS 连接，便能够访问系统。推荐使用 IE11.0/Firefox3.x+/Google Chrome 或更高版本浏览器，屏幕最低显示分辨率要求 1366×768。

此产品需要 Adobe Flash Player 9.0.124 或更高版本，如果未安装或版本过低，系统中使用到该技术的功能将无法显示，系统会自动检测浏览器中此插件的安装情况，如果不符合要求，在登录页面会看到相关提示。

为了更好的用户体验，推荐使用 FireFox 或 Chrome 浏览器。


注意

系统推荐使用 Firefox3.x+/Google Chrome 或更高版本浏览器。在使用 IE11 浏览器时，如出现页面反应缓慢、数据展示不全等现象，请使用 Firefox、Google Chrome 浏览器访问。

1.2 登录系统

Web 登录：HTTP 登录端口使用 80 端口，HTTPS 登录端口使用 443 端口。

输入正确的用户名和密码，回车或点击**[登录]**按钮进入系统。

如果输入错误密码，连续重试一定次数（见用户管理一章，锁定解锁配置说明），系统会锁定试图登录的主机 IP 一段时间（时间可由用户管理员设定），这时，无论是否输入正确密码，都无法进入系统，直到锁定时间超时或用户管理员手动解锁才可以登录到系统的 Web 端。

1.3 界面布局和元素

RAVEN 入侵检测与管理系统界面由菜单、工具栏和工作显示区组成。点击菜单，可以展开下一级菜单，点击下一级菜单，进行工作页面切换。

图 1-2 系统主页

1.3.1 菜单

菜单提供了 RAVEN 入侵检测与管理系统的主要配置选项。大多数功能都需要通过选中菜单切换到相应的功能页面，页面菜单栏（如图 1-3）显示一级菜单。

图1-3 系统菜单

1.3.2 工具栏

工具栏提供一些功能的快捷链接。

图 1-4 快捷功能栏

1.3.3 列表

很多管理配置页面是以列表的形式显示，例如组件管理、特征检测配置等。

图形化用户界面

图1-5 以列表形式显示配置

列表中最右面的列一般为操作列，提供操作图标按钮，可对该条目进行对应的操作。通常列表上方会有针对整个列表的操作按钮，比如[**新建**]按钮，可以增加条目。

1.3.4 通用图标

页面中有很多图标帮助进行配置管理操作。当鼠标停留到图标上时，一般会显示提示信息。下表对页面中一些通用的图标进行说明。

图标	名称	说明
	编辑	编辑配置
	删除	删除一个条目
	下发	下发策略、内容
	导出	导出策略、内容

1.4 菜单分类介绍

主页：查看系统当前：内存、CPU、数据磁盘、授权状态等情况，显示当天整体、拒绝服务、端口扫描、蠕虫、木马病毒的统计，查看最近 24 小时内：特征检测 Top5、攻击类型统计、最近 24 小时流量曲线趋势图；

已知检测：

特征检测：查看特征检测日志、病毒检测日志、分析池结果；

文件检测：查看文件检测日志；

威胁情报：查看隐蔽信道日志、恶意 URL 日志；

WEB 防护：查看 WEB 防护日志；

安全审计：查看安全审计日志。

流量统计：

宏观流量：查看宏观流量分析结果，配置宏观流量报警参数；

微观流量：查看微观流量分析结果，配置微观流量报警参数、策略。

统计分析：

任务列表：制定各种数据报表，展现报表任务，查看、下载报表执行结果；

执行结果：查看下载执行报表，选择格式下载，删除报表；

检测配置：

特征检测配置：定制策略集、策略模板、自定义特征事件、二次事件、弱口令、事件合并规则；

资产配置：重点 WEB 服务器、IP-MAC 绑定；

组件管理：添加、编辑设备组件，包括动态引擎配置，查看上级连接状态；

文件检测配置：配置文件检测的黑/白名单；

病毒检测配置：配置入侵检测与管理系统的病毒检测协议及文件类型；

URL 信誉库：配置 URL 黑/白名单；

隐蔽信道库：配置隐蔽信道规则及特征。

系统管理：

响应方式：编辑 Syslog、SNMP、邮件、防火墙联动配置；

系统维护：升级管理进行各模块功能升级、存储维护进行数据维护及告警配置；

通用配置：包括时间、代理、关注度配置；

运行日志：运行日志展示及系统诊断日志导出。

用户管理：

仅用户管理员可见，添加、修改、删除配置管理员、受限管理员和用户自定义角色，对其账号进行锁定、修改密码等操作。

审计日志：

审计员可以查看、操作系统操作审计日志。

1.5 工具栏

由左至右分布表示：

菜单收缩、全屏切换、平铺菜单、更换皮肤、重要消息、个人信息（修改密码、关于我们、关机、退出）。

1.5.1 展示菜单

实现菜单整体收缩，使菜单栏占用页面比例减小。

图 1-6 菜单效果

1.5.2 全屏切换

实现全屏与退出全屏模式切换。

1.5.4 平铺菜单

实现菜单的平铺展示。

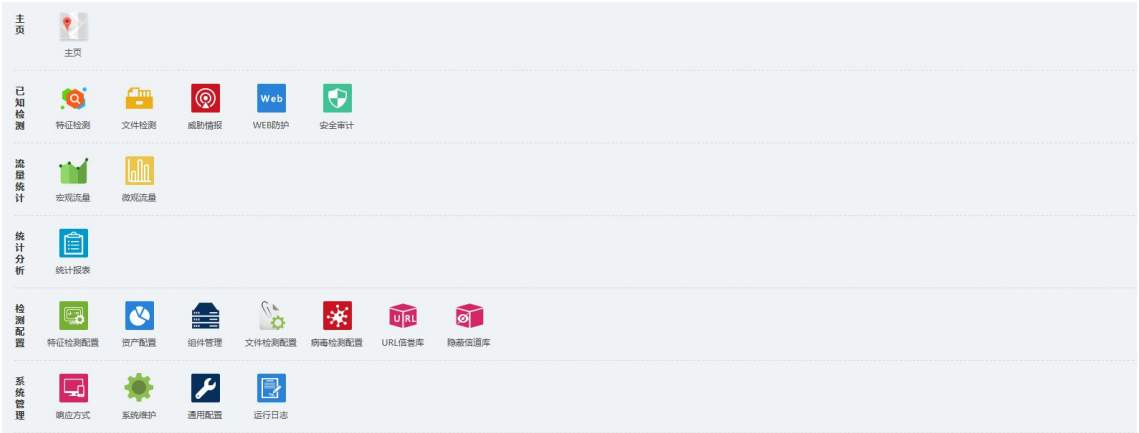

图 1-7 平铺菜单展示

1.5.5 更换皮肤

实现 Web 页面皮肤颜色的更换，可选颜色包括：清新绿、夜空、经典蓝色和典雅黑。

1.5.6 重要消息

在页面提供消息提示功能，有重要消息出现的时候，以消息数量的方式提示用户；重要消息确认之后，提示数字清零，点击图标进入新消息列表；同时可进入重要消息日志查询及导出结果日志查询，并提供查询、导出等功能。

重要消息提示位于页面右上角，包括资源告警、计划任务 2 种重要消息。如图所示。

图 1-8 通知消息

点击重要消息资源告警实时显示，进入到新消息界面。

图 1-9 资源告警信息

1.5.7 个人信息

个人消息包括修改密码、关于我们、关机和退出。

图 1-10 个人信息

修改密码：

当前登录用户通过此按钮，修改自身密码。用户管理员（admin）、审计管理员（audit）和配置管理员账号，只能通过此功能修改密码。

图 1-10 修改密码页面

原始密码：配置管理员的旧密码。

新密码：设置配置管理员的新密码。

再次输入密码：确认设置的新密码。

关于我们：

关于主要包括产品名称、版权所有、产品技术支持、产品和销售信息、版权信息。点

击相应的链接，可以浏览我公司产品技术支持、网址、分公司及办事处列表等相关信息，也可以给我公司发送邮件留下您的宝贵意见和建议。

关机：

系统关机。


注意

系统只能通过 web“关机”功能关机，拔电、背板按钮强制关机等视为异常操作，可能导致系统日志丢失、系统配置损坏等故障。

退出：

退出 Web 登录状态。

1.6 管理员默认账号

系统默认的用户管理员账号为 admin，密码为 Raven.private，可以使用这个账号添加、修改和删除配置管理员。

系统默认的审计员账号为 audit，密码为 Raven.audit，使用这个账号查看用户管理员和配置管理员的操作日志。

系统默认的配置管理员账号为 adm，密码为 Raven.public，配置管理员可以登录系统，进行各项安全业务上的操作配置。

第2章 主页

2.1 主页简要介绍

主页信息页面划分为五个区域显示：

系统资源状态：系统当前内存、CPU、数据磁盘占用的百分比图形呈现，设备状态评级、授权状态信息。

整体：对系统发生的所有事件进行统计。

拒绝服务：拒绝服务统计的是当天的拒绝服务以及分布式拒绝服务事件发生次数统计。

端口扫描：当天发生的安全扫描以及穷举探测事件统计。

蠕虫：当天发生的蠕虫病毒事件次数统计。

木马病毒：当天发生的木马后门事件统计。

攻击类型统计：最近 24 小时的威胁事件按照攻击类型进行统计。

特征检测 TOP5：最近 24 小时内排名前五的网络滥用或安全威胁事件统计。

流量曲线趋势：最近 24 小时引擎的总流量曲线、邮件流量曲线、web 流量曲线、数据库流量曲线、P2P 流量曲线、其他流量曲线。

2.2 系统资源状态

系统当前内存、CPU、数据磁盘占用的百分比图形呈现，设备状态评级、授权状态信息。

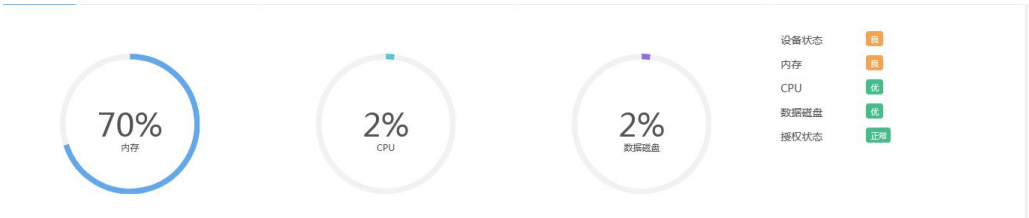

图2-1 系统资源状态

2.3 整体

对系统发生的所有事件进行统计。

2.4 拒绝服务

拒绝服务统计的是当天的拒绝服务以及分布式拒绝服务事件发生次数统计。

2.5 端口扫描

端口扫描统计的是当天安全扫描以及穷举探测事件。

2.6 蠕虫

当天发生的蠕虫病毒事件次数统计。

2.7 木马病毒

木马病毒统计的是当天发生的木马后门事件。

2.8 攻击类型统计

攻击类型统计记录最近 24 小时内，发生的威胁事件按照攻击类型进行的分类统计值，具体攻击类型包括：信息收集、获取权限、远程控制、数据盗取、系统破坏、隐藏攻击痕迹、有害程序、其他、安全审计、网络娱乐；将鼠标置于图顶端，会显示对应的攻击事件在最近 24 小时内发生的次数。

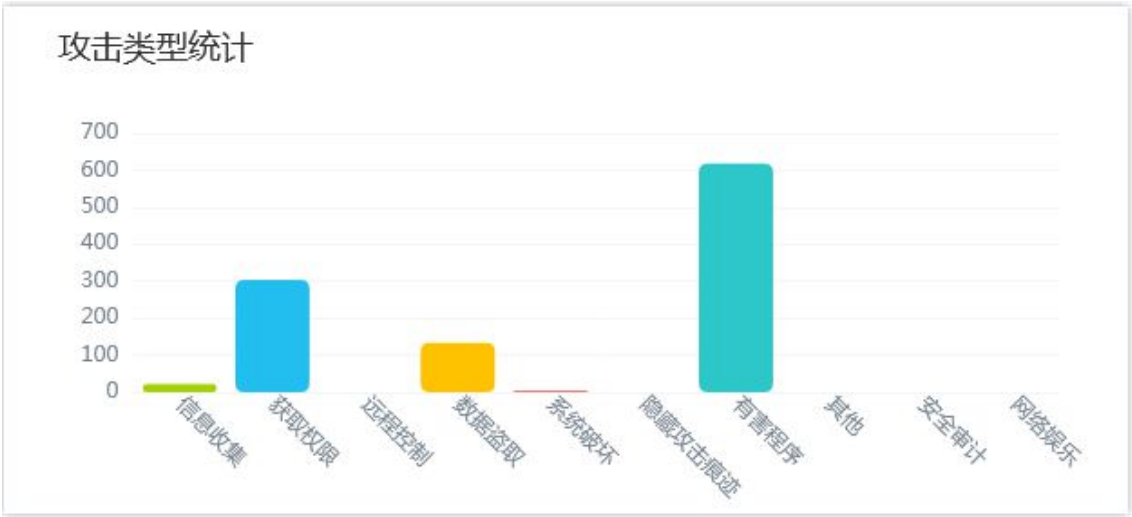

图2-2 攻击类型统计

点击图，会链接跳转到相应攻击类型事件的日志查询界面。

图2-3 事件列表展示

2.9 特征检测TOP5

系统在最近 24 小时内检测到的攻击事件，用柱状图显示发生次数最多的 5 个攻击事件。下图中，横坐标为 Top 排名，纵坐标为事件次数，鼠标移到柱状图形上，可以看到具体事件名称。如果某一种事件数量比平常大得多，说明需要进一步查看监控信息，以确定网络是否安全。

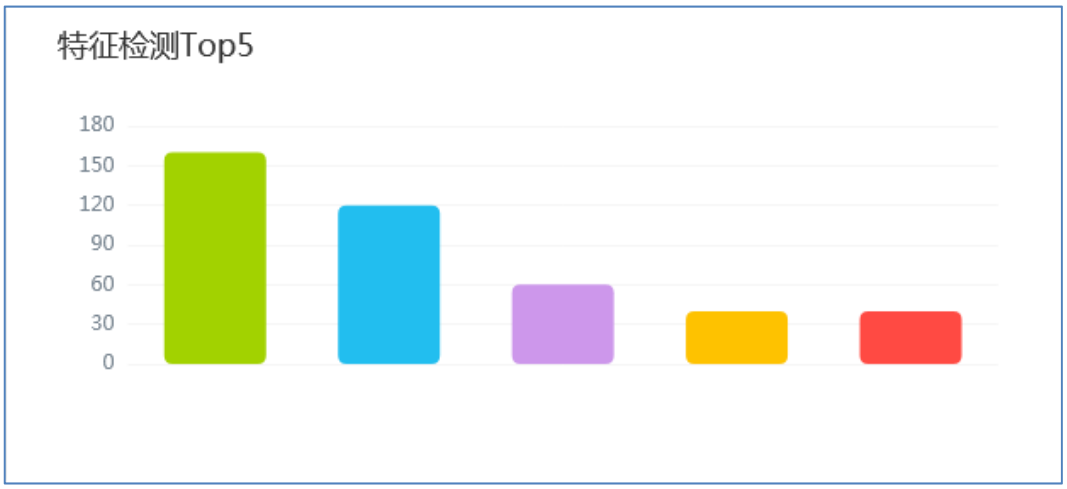

图2-4 特征检测 TOP5

2.10 流量曲线趋势

对引擎检测的流量进行统计，以曲线图显示。在总流量曲线中，显示最近 24 小时内网络总流量情况。

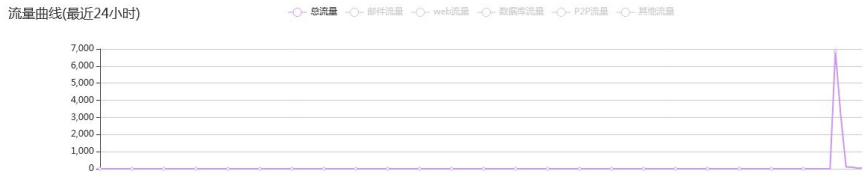

图 2-5 流量曲线图

第3章 已知检测

3.1 概述

已知检测用于展示匹配已知特征的特征检测、文件检测、威胁情报、WEB 防护、安全审计日志等信息。

3.2 特征检测

用来显示系统最近监测到的威胁事件、病毒日志及分析池结果。用于了解网络当前的威胁信息，保证在系统遭遇大规模攻击事件、病毒攻击时能及时的跟踪、定位和监控。匹配特征包括事件库中的特征事件及用户自定义的特征事件。

3.2.1 特征检测

特征检测日志展示内容包括：事件级别、安全类型、攻击类型、流行程度、事件名称、源 IP、目的 IP、引擎、发生时间、事件 ID、协议类型及操作。

图 3-1 特征检测

参数说明：

图形化用户界面

事件级别：高危、中危、低危、非攻击；

安全类型：按照安全类型进行分类，详细对应可以查看策略集；

攻击类型：按照攻击类型进行分类，详细对应可以查看策略集；

流行程度：流行、不流行、无威胁；

操作包括参数配置、查询、导出和分类统计。

参数配置：

用户可以根据实际需求自定义事件日志显示的数据列。配置项包括：事件级别、安全类型、攻击类型、流行程度、事件名称、源 IP、目的 IP、引擎、发生时间、事件 ID、协议类型及操作。

图 3-2 配置参数展示

查询：

点击**[查询]**按钮，可以根据实际需求进行日志列表筛选。查询配置项包括：

事件级别：非攻击、低危、中危、高危；

攻击类型：网络娱乐、信息收集、获取权限、安全审计、远程控制、数据盗取、系统破坏、隐藏攻击痕迹、有害程序、恶意网站、其他类攻击事件；

IP、IP 区间：根据 IP 或 IP 区间进行事件过滤查询；

事件名称：手动输入事件名称进行过滤查询；

引擎：全部引擎、单机引擎；

图 3-3 查询页面

导出：

点击**[导出]**按钮，会后台执行导出操作，成功导出后，重要消息会有提示，通过计划

任务进入导出结果日志查询模块，点击操作列中的**[下载]**按钮，实现日志导出功能。

图 3-4 事件导出

分类统计：

点击**[分类统计]**按钮，针对日志结果进行分类统计，统计成功后，重要消息会有提示，通过计划任务进入到消息日志，通过消息内容可以查看分类统计的结果，针对高危、中危、低危、非攻击及总数进行分类统计。

图 3-5 统计分析结果

3.2.2 事件详细信息

双击一条上报的事件或点击操作列**[详细]**按钮，可以弹出事件详细说明信息窗口，该窗口显示出该条事件的相关信息。

图3-6 事件详细信息

通过事件详细信息，可以快速查看事件基本信息、事件说明和事件返回参数；点击追溯分析中的目的 IP 分析（源 IP 分析），可查看相应目的 IP（源 IP）的特征事件日志。

3.2.3 回溯分析

点击事件日志操作列中的**[回溯分析]**按钮 ，进入回溯分析展示页面。

事件视角：展示此事件日志的详细信息；

攻击者视角：展示源 IP 地址所在资产的指纹信息、威胁情报信息、攻击态势统计信

息；

被攻击视角：展示目的 IP 地址所在资产的指纹信息、威胁情报信息、攻击态势统计信息；

资产指纹：未记录的资产信息展示为 N/A；要登记资产信息请到**检测配置>资产配置>资产管理**进行配置。

图 3-7 资产指纹结果

威胁情报：展示与此 IP 相关的隐蔽信道特征信息；无相关信息时展示“暂时无数据”。

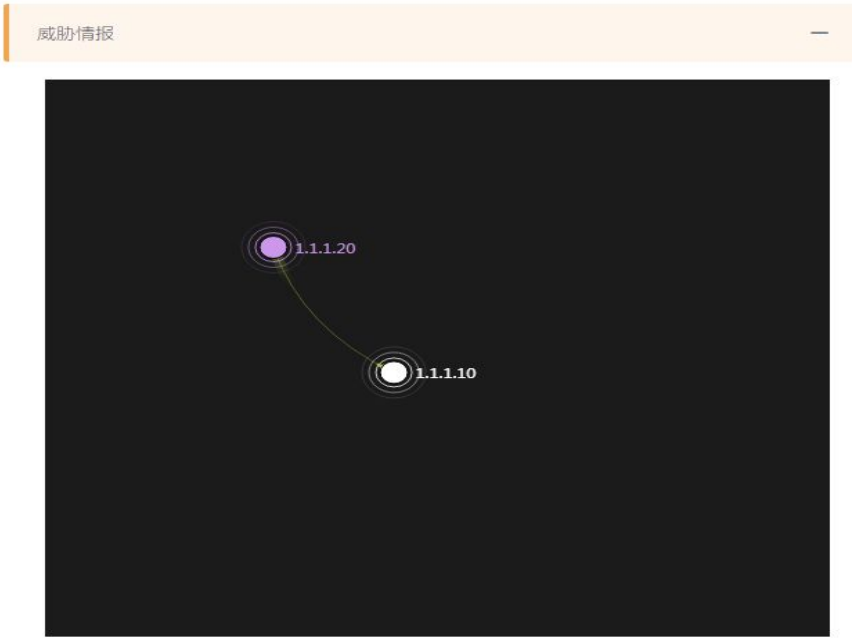

图 3-8 威胁情报展示

攻击态势：展示此 IP 最近 7 天各个攻击类型事件发生次数占比统计。

图 3-9 攻击态势展示

3.2.4 病毒检测

病毒检测日志展示内容包括：病毒名称、感染文件、协议类型、源 IP、目的 IP、引擎、发生时间。

查询：

点击**[查询]**按钮，可据实际需求进行日志列表筛选。查询配置项包括：源端口、目的端口、病毒名称、抓包口、引擎、源 IP、源 IP 区间、目的 IP、目的 IP 区间。

导出：

点击**[导出]**按钮，会后台执行导出操作，成功导出后，重要消息会有提示，通过计划任务进入导出结果日志查询模块，点击操作列中的**[下载]**按钮，实现日志导出功能。

详细信息：

双击一条病毒检测日志，展示该病毒日志详细信息。

3.2.5 分析池

系统提供分析池功能，可将需要关注的事件加入分析池，并可按事件源/目的 IP 进行事件追溯，然后将相关联的事件加入分析池，建立案卷进行管理。

在**特征检测**、**WEB 防护**、**安全审计**页面，可在事件列表的操作列内点击**[加入分析池]** 按钮，可以把该事件加入分析池。

图 3-10 操作列表展示

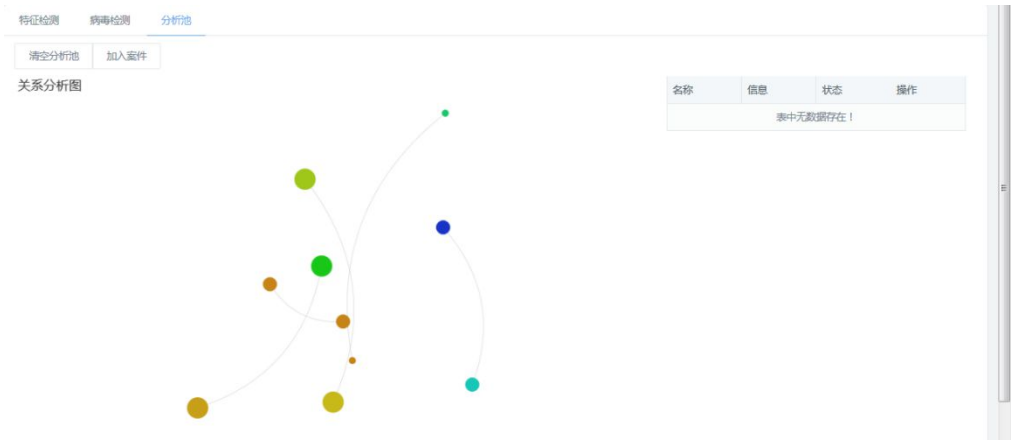

图 3-11 分析池展示

在**特征检测**、**WEB 防护**、**安全审计**页面，可双击一条事件或者在这条事件列表的操作列内点击**[详细]** 按钮，打开这条事件的详细框，可在框内点击**[源 IP 分析]**或者[**目的 IP 分析]**，展示出这条事件的关联事件，并可在该事件列表的操作列内点击**[加入分析池]** 按钮，可以把该事件加入分析池。

图 3-12 事件详细说明信息

在分析池页面可以点击**[加入案件]**按钮，将分析池内的数据加入案卷进行管理。

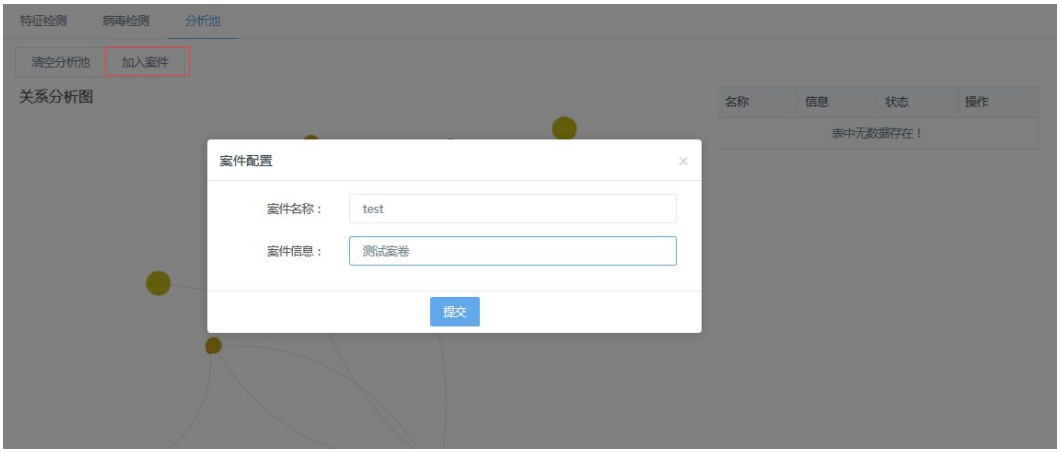

图 3-13 案件配置页面

在案卷列表可以对案卷进行操作，可以查看、归档、删除等。

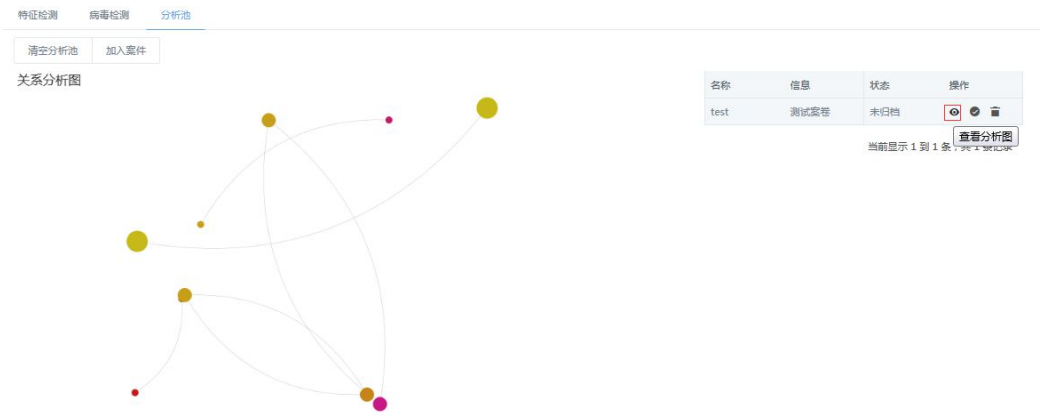

图 3-14 查看案件分析图

分析池内的数据不需要了时，可以点击**[清除分析池]**按钮，可以清空分析池内的数据。

图 3-15 清空分析池

3.3 文件检测

文件检测日志用于记录网络文件静态检测及动态检测的结果。恶意样本事件默认显示的数据列包括结果、时间、源 IP、目的 IP、样本名称、样本类型、检测方法、协议类型、捕获设备及操作列。

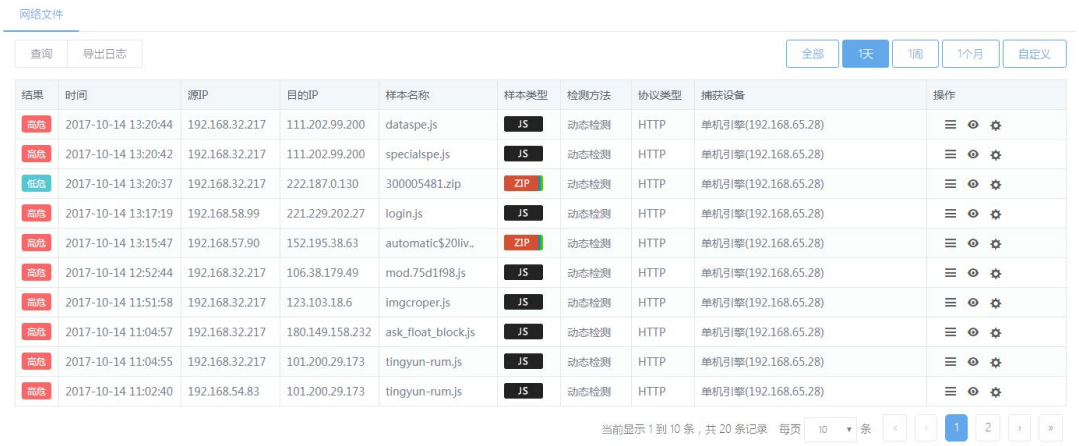

图 3-16 文件检测结果列表

查询：

点击**[查询]**按钮，可据实际需求进行日志列表筛选。查询配置项包括：样本名称、MD5、源 IP、目的 IP、协议、检测结果、样本类型、检测方法。

导出日志：

点击**[导出日志]**按钮，会直接导出下载网络样本检测日志的 xls 文件提供查看。

操作列：

详情：点击一条样本日志的**[详情]**按钮，展示该日志的详细信息，包括：样本信息、检测模式、协议信息；

查看报告：存在动态检测结果的日志才显示按钮。点击**[查看报告]**按钮，会展示样本动态检测报告；

更多：提供更多操作功能，包括：报告下载（动态检测日志才有）、文件下载、加入黑名单、加入白名单。

3.4 威胁情报

3.4.1 隐蔽信道

隐蔽信道日志记录匹配上隐蔽信道库特征的恶意行为。展示列包括：检测结果、检测时间、源 IP、源端口、目的 IP、目的端口、特征、类型、匹配来源、捕获设备及操作。

图 3-17 隐蔽信道结果列表

查询：

点击**[查询]**按钮，可据实际需求进行日志列表筛选。查询配置项包括：检测结果、类型、源 IP、目的 IP。

导出：

点击**[导出]**按钮，会直接导出下载隐蔽信道日志的 xls 文件提供查看。

操作列：

详情：点击一条隐蔽信道日志的**[详情]**按钮，展示该日志的详细信息；

移除隐蔽信道库：此按钮只有匹配自定义库特征的日志才有。点击此按钮，会将此条日志的隐蔽信道特征从自定义隐蔽信道库中移除；

3.4.2 恶意URL

恶意 URL 记录引擎检测到匹配自定义 URL 黑名单地址，或匹配 URL 信誉库中地址的 URL 日志。展示列包括：URL 地址、源 IP、目的 IP、恶意类型、协议类型、来源、发生时间、详细说明。

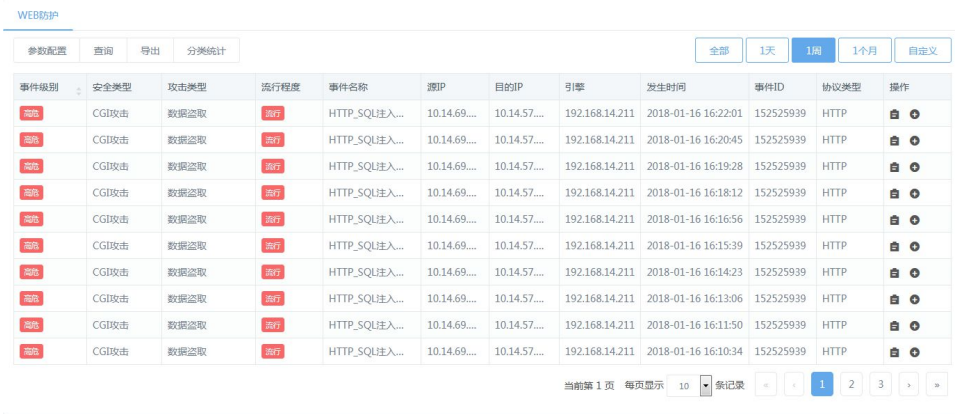

图 3-18 恶意 URL 检测结果列表

参数配置：

点击[**参数配置**]按钮，用户可以根据实际需求自定义恶意 URL 日志显示的数据列。配置项包括：URL 地址、源 IP、目的 IP、恶意类型、协议类型、来源、发生时间、详细说明。

查询：

点击**[查询]**按钮，可据实际需求进行日志列表筛选。查询配置项包括：URL 地址、恶意类型、源 IP、源 IP 区间、目的 IP、目的 IP 区间。

导出：

点击**[导出]**按钮，会后台执行导出操作，成功导出后，重要消息会有提示，通过计划任务进入导出结果日志查询模块，点击操作列中的**[下载]**按钮，实现日志导出功能。

分类统计：

点击**[分类统计]**按钮，针对日志结果进行分类统计，统计成功后，重要消息会有提示，通过计划任务进入到消息日志，通过消息内容可以查看分类统计的结果，针对恶意类型进行分类统计。

3.5 WEB防护

WEB 防护仅展示 WEB 攻击类特征事件日志，功能同特征检测，请参考 3.2.1 特征检测。展示列包括：事件级别、安全类型、攻击类型、流行程度、事件名称、源 IP、目的 IP、引擎、发生时间。

参数配置：

点击[**参数配置**]按钮，用户可以根据实际需求进行自定义 WEB 防护日志显示的数据列。配置包括：件级别、安全类型、攻击类型、流行程度、事件名称、源 IP、目的 IP、引擎、发生时间、事件 ID、协议类型、操作。

查询：

点击**[查询]**按钮，可据实际需求进行日志列表筛选。查询配置项包括：

事件级别：非攻击、低危、中危、高危。

攻击类型：网络娱乐、信息收集、获取权限、安全审计、远程控制、数据盗取、系统破坏、隐藏攻击痕迹、有害程序、恶意网站、其他类攻击事件。

IP、IP 区间、事件名称、引擎：全部引擎、单机引擎。

导出：

点击**[导出]**按钮，会后台执行导出操作，成功导出后，重要消息会有提示，通过计划任务进入导出结果日志查询模块，点击操作列中的**[下载]**按钮，实现日志导出功能。

分类统计：

点击**[分类统计]**按钮，针对日志结果进行分类统计，统计成功后，重要消息会有提示，通过计划任务进入到消息日志，通过消息内容可以查看分类统计的结果，针对恶意类型进行分类统计。

3.6 安全审计

安全审计仅展示安全审计类特征事件日志，功能同特征检测，请参考 3.2.1 特征检测。

展示列表包括：事件级别、安全类型、攻击类型、流行程度、事件名称、源 IP、目的 IP、引擎、发生时间。

参数配置：

点击[**参数配置**]按钮，用户可以根据实际需求进行自定义安全审计日志显示的数据列。配置包括：事件级别、安全类型、攻击类型、流行程度、事件名称、源 IP、目的 IP、引擎、发生时间、时间 ID、协议类型及操作。

查询：

点击**[查询]**按钮，可据实际需求进行日志列表筛选。查询配置项包括：

事件级别：非攻击、低危、中危、高危。

攻击类型：网络娱乐、信息收集、获取权限、安全审计、远程控制、数据盗取、系统破坏、隐藏攻击痕迹、有害程序、恶意网站、其他类攻击事件。

IP、IP 区间、事件名称、引擎：全部引擎、单机引擎。

导出：

点击**[导出]**按钮，会后台执行导出操作，成功导出后，重要消息会有提示，通过计划任务进入导出结果日志查询模块，点击操作列中的**[下载]**按钮，实现日志导出功能。

分类统计：

点击**[分类统计]**按钮，针对日志结果进行分类统计，统计成功后，重要消息会有提示，通过计划任务进入到消息日志，通过消息内容可以查看分类统计的结果，针对恶意类型进行分类统计。

第4章 流量统计

4.1 宏观流量

宏观流量模块主要是显示系统各个引擎的流量信息，包括宏观流量分析和宏观流量报警参数设置；其中，宏观流量分析主要针对最近 24 小时流量、最近 30 天流量、流量实时分布和报警信息列表。

流量的度量方式是以 10 分钟为单位，最小计量单位是 bps，也就是比特每秒。可以选择按照比特数或按照包数进行流量的显示。

流量报警可以根据用户配置的是阈值对比分析或机器自动分析，依据分析结果判断流量是偏低异常、轻度偏高异常、中度偏高异常、严重偏高异常。

4.1.1 分析

系统进入宏观流量统计的第一个界面就是系统中全部引擎的总流量信息，包含有 Web 流量、邮件流量、数据库流量、P2P 流量、其它流量和总流量六种分类显示情况，如下图所示。

图 4-1 宏观流量结果展示

界面左侧列出的是设备列表；包括本级控制中心以及该控制中心下面挂载的引擎，如下图所示。

图 4-2 设备列表展示

在设备列表下面的查询栏中输入引擎 IP，可以进行引擎定位，如下图所示。

图 4-3 查询引擎展示

界面右侧显示所选择引擎或者控制中心的宏观流量面积图（从 0 点到当前时间的流量变化面积图，每 10 分钟为一个点。）内容包括：Web 流量，邮件流量，数据库流量，p2p 流量、其他流量和总流量，当前流量值展示方式为按字节(bps)，如下图所示。

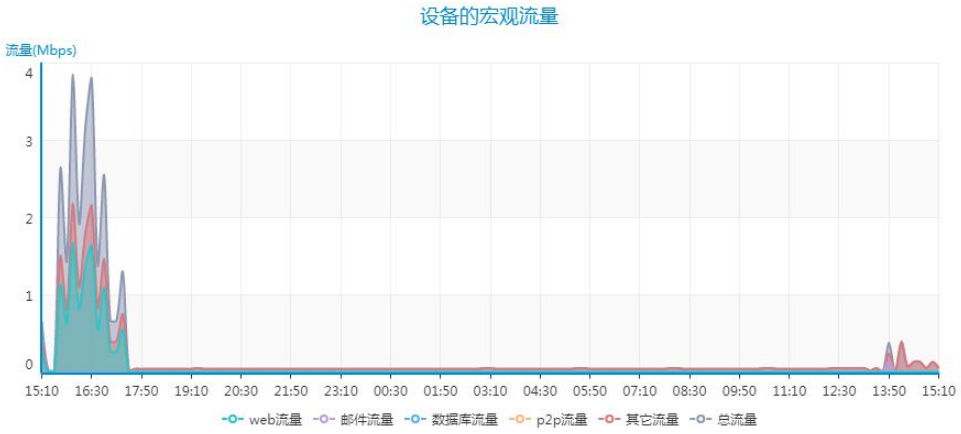

图 4-4 设备宏观流量

将鼠标放置于相应的时刻点的面积图上，可以看到相应流量的信息，如下图所示。

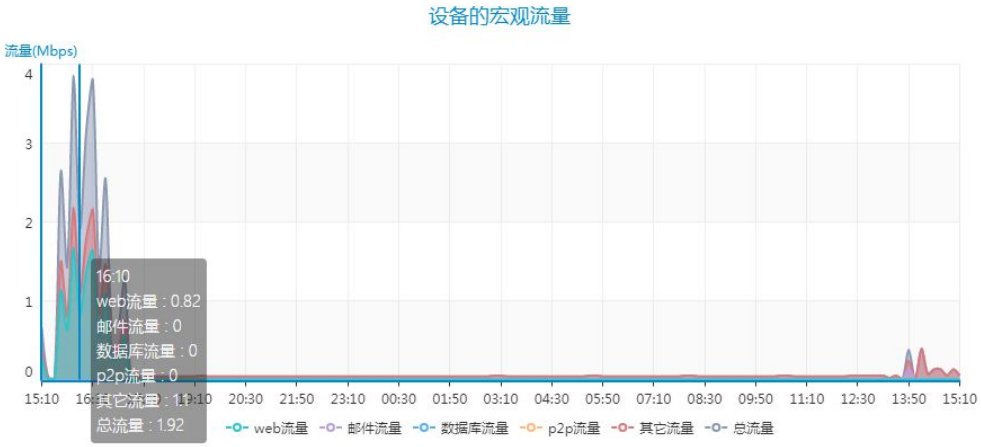

图 4-5 流量信息展示

点击界面上方的切换展示方式，可以选择各设备的当前流量按包数显示流量值（ppt）还是按比特显示流量值（bps），如下图所示。

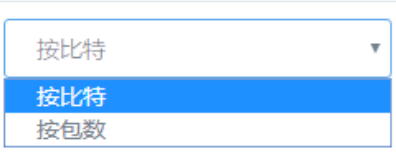

图 4-6 选择流量展示方式

在设备列表中点击所要查看的设备，即可在右侧界面展示该设备的宏观流量，假设要查看引擎 192.168.14.182 的宏观流量信息，点击设备列表 192.168.14.182 即可，如下图所示。

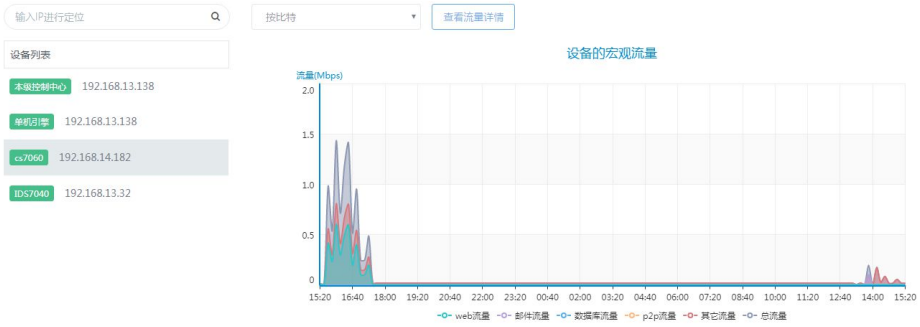

图 4-7 选择某一引擎查看宏观流量

点击界面上方的**[查看流量详情]**按钮，可以进入到宏观流量详细分析界面，如下图所示。

图 4-8 流量分析页面展示

在流量分析详细界面中点击**[返回]**按钮，即可返回到宏观流量分析界面。

宏观流量详细分析界面主要包括最近 24 小时流量、最近 30 天流量、流量实时分布和报警信息。

最近 24 小时流量：

最近 24 小时流量是展示的是最近 24 小时内的宏观流量统计信息，每 10 分钟统计一次，将鼠标置于对应的时刻点流量曲线时，会显示相应的流量信息，其中蓝色曲线代表当前的流量运行态势，紫色代表历史流量运行态势，如下图所示。

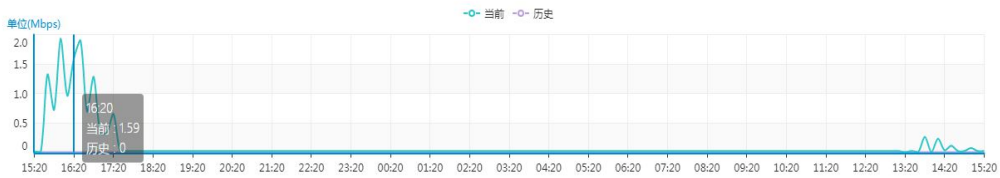

图 4-9 最近 24 小时流量展示

最近 30 天流量：

单击页面上的“最近 30 天”页签，展示当前设备的最近 30 天每天的平均流量。

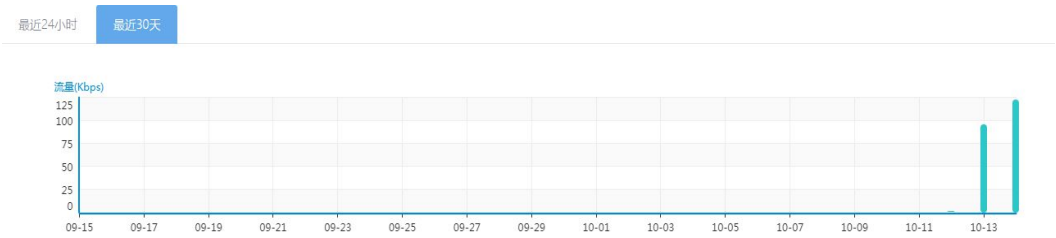

图 4-10 最近 30 天流量信息展示

将鼠标停置于某个时间点上，显示当天的流量信息，如下图所示。

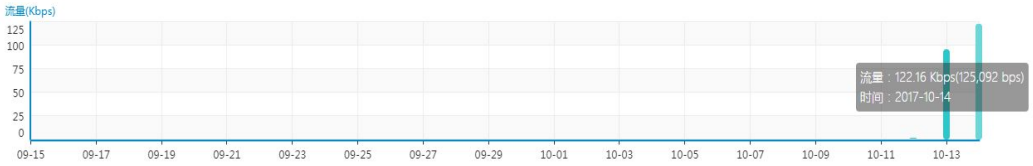

图 4-11 当天流量信息展示

流量实时分布：

该流量分布列表给出了流量类型、对应类型的流量值、流量压力以及运行态势，运行态势说明当前的运行状态；流量类型包括六种：总流量、Web 流量，邮件流量，数据库流量，P2P 流量和其他流量。

流量实时分布

类型	流量	压力 ?	态势
总流量	当前:23.37 Kbps 历史:N/A	0%	N/A
Web流量	当前:0 bps 历史:N/A	0%	N/A
邮件流量	当前:0 bps 历史:N/A	0%	N/A
数据库流量	当前:0 bps 历史:N/A	0%	N/A
P2P流量	当前:0 bps 历史:N/A	0%	N/A
其他流量	当前:23.37 Kbps 历史:N/A	0%	N/A

图 4-12 流量实时分布信息展示

点击不同的流量类型，其他展示模块也会随之切换为对应的流量展示，如点击流量实时分布中的**总流量**图标，最近 24 小时流量、最近 30 天流量和报警信息都会展示总流量的运行态势。

报警信息：

报警信息展示的是各种流量各时刻点与设定阈值或历史同期流量的对比，如下图所示。

图 4-13 总流量报警信息展示

点击界面上方的展示方式切换按钮，其他展示模块也会随之切换为对应的展示方式：按照比特或按照包数进行展示，如选择按包数进行展示，最近 24 小时流量、最近 30 天流量、流量实时分布和报警信息都会展示 Web 流量的运行态势，如下图所示。

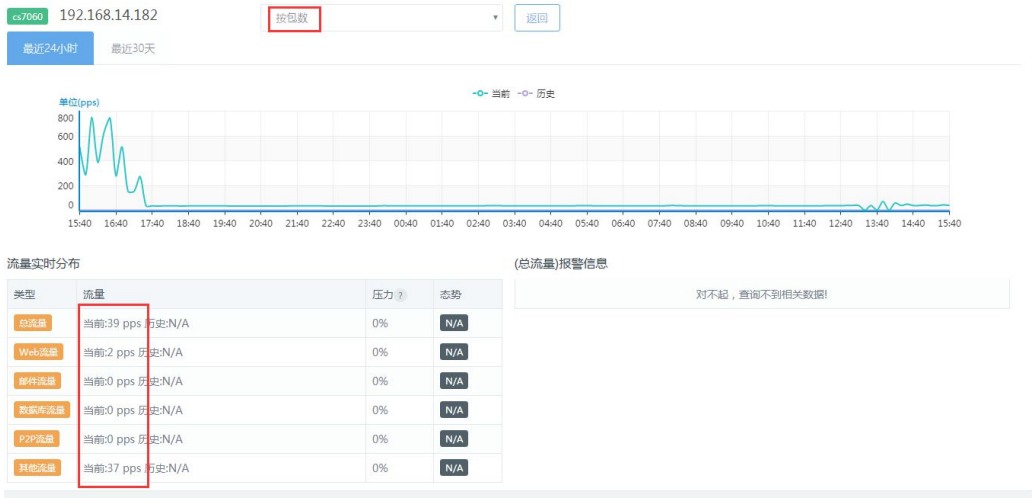

图 4-14 流量信息分析图

4.1.2 报警参数配置

点击**流量统计>宏观流量>报警参数配置**，可以看到 6 种类型的宏观流量分析参数，系

统默认状态是历史同期对比方式，系统会采用默认（机器自动分析）进行报警分析。系统默认参数（偏低系数 50，轻度偏高系数 150，中度偏高系数 200，严重偏高系数是大于 200），如下图所示。

图 4-15 报警参数配置信息展示

点击操作列[**编辑**]按钮相应的流量类型，可以进入到该类型流量报警参数的设置，假设要设置 Web 流量的报警参数，如下图所示。

图 4-16 报警参数配置展示

若要采用自定义配置模式，点击配置类型设置切换按钮，进入到自定义配置模式，如下图所示。

图 4-17 自定义参数配置展示

流量异常分析方法包括同期对比分析和阈值对比分析两种分析方法。

同期对比分析：

当配置是默认配置时，系统默认为同期对比分析配置，系统会根据当前 10 分点的引擎流量数据的 bps 值与配置的自动分析系数进行对比，如果发现异常进行报警。为用户自定义配置，会根据当前 10 分点的引擎的流量数据包（pps）的值跟用户配置的自动分析参数对比，如果发现异常进行报警。

“同期对比分析”时，修改流量分析参数，具体报警级别分为四种：偏低、轻度偏高、中度偏高和严重偏高；如下图所示。

图 4-18 同期对比参数展示

用户可以根据实际情况进行响应方式的配置，是否产生报警日志，是否产生报警，报警级别具体开放或关闭哪个级别，是否利用邮件进行报警信息的发送，如下图所示。

图 4-19 响应方式配置展示

当控制中心未配置邮件时，会有提示“无可用邮件列表，若开启邮件报警，请先到“系统管理->响应方式->邮件配置”下配置”，如下图所示。

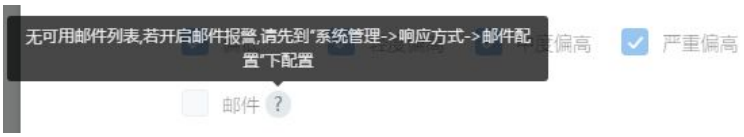

图 4-20 未配置邮件提示展示

若控制中心进行了邮件配置，则此处会出现收件人信息列表，可以根据实际情况进行收件人的选择，配置收件人后，产生的报警信息就会发送给相关人员，以便实时关注流量状态。

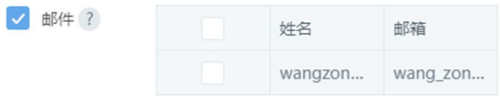

图 4-21 已配置邮件展示

阈值对比分析：

如果用户配置的是阈值对比分析，系统会根据当前 10 分点引擎流量数据跟用户配置的阈值进行对比。如果发现异常进行报警。

点击流量异常分析方法切换按钮切换到阈值对比分析配置模式，如下图所示。

图 4-22 异常分析功能展示

“阈值对比分析”时，修改流量分析参数，具体报警级别分为四种：偏低、轻度偏高、中度偏高和严重偏高；如下图所示。

图 4-23 阀值对比参数展示

流量的默认单位是 bps，可能通过参数设置流量的单位。展开单位下拉框，进入参数设置界面，选择流量单位，就可以设置流量的单位，并且在以后登录后，会一直使用这个单位，直到下一次改变。

图 4-24 单位参数设置

展开数量级下拉框，可以进行数量级的设置，设置完成后，相应报警级别后的区间范围会自动乘以该数量级，如下图所示。

图 4-25 数量级参数设置

用户可以根据实际情况进行响应方式的配置，是否产生报警日志，是否产生报警，报警级别具体开放或关闭哪个级别，是否利用邮件进行报警信息的发送，如下图所示。

图 4-26 响应方式配置展示

当控制中心未配置邮件时，会有提示“无可用邮件列表，若开启邮件报警，请先到“系统管理->响应方式->邮件配置”下配置”，如下图所示。

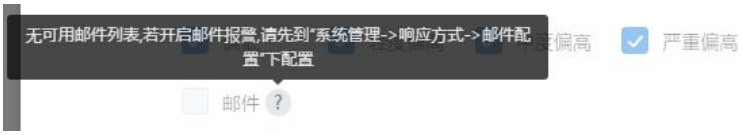

图 4-27 未配置邮件提示展示

若控制中心进行了邮件配置，则此处会出现收件人信息列表，可以根据实际情况进行收件人的选择，配置收件人后，产生的报警信息就会发送给相关人员，以便实时进行流量

的分析。

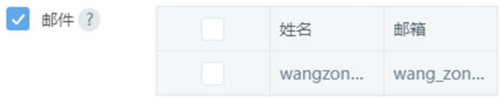

图 4-28 已配置邮件展示

用户根据需要进行报警参数的自定义配置后，保存相应配置后，在宏观流量报警参数设置列表中会有所表现，如下图所示。

图 4-29 自定义后配置展示

4.2 微观流量

微观流量统计模块主要是显示系统各个引擎的微观流量信息，包括微观流量分析，微观流量报警参数设置和微观流量策略配置；其中，微观流量分析主要针对 P2P、DNS、IP/端口、重点协议、关键运维、关键 Web 行为 6 种微观流量实时分布和报警信息列表；

流量的度量方式是以 10 分钟为单位，最小计量单位是 bps，也就是比特每秒。引擎会通过检测的流量，自适应显示流量单位，流量的单位为按比特数 bps，Kbps，Mbps，Gbps 或按照包数 pps。

流量报警可以根据用户配置的是阈值对比分析或机器自动分析，依据分析结果判断流量是偏低异常、轻度偏高异常、中度偏高异常、严重偏高异常。

4.2.1 分析

系统进入微观流量统计的第一个界面就是系统中全部引擎的流量信息，包含有 P2P、DNS、IP/端口、重点协议、关键运维、关键 Web 行为六种分类显示情况，（其中 P2P 流量类型中包括 16 种协议，重点协议类型包括 27 种协议，关键运维 3 种报文，关键 Web 运维 3 种请求方式，以上在新建策略模块下介绍）如下图所示。

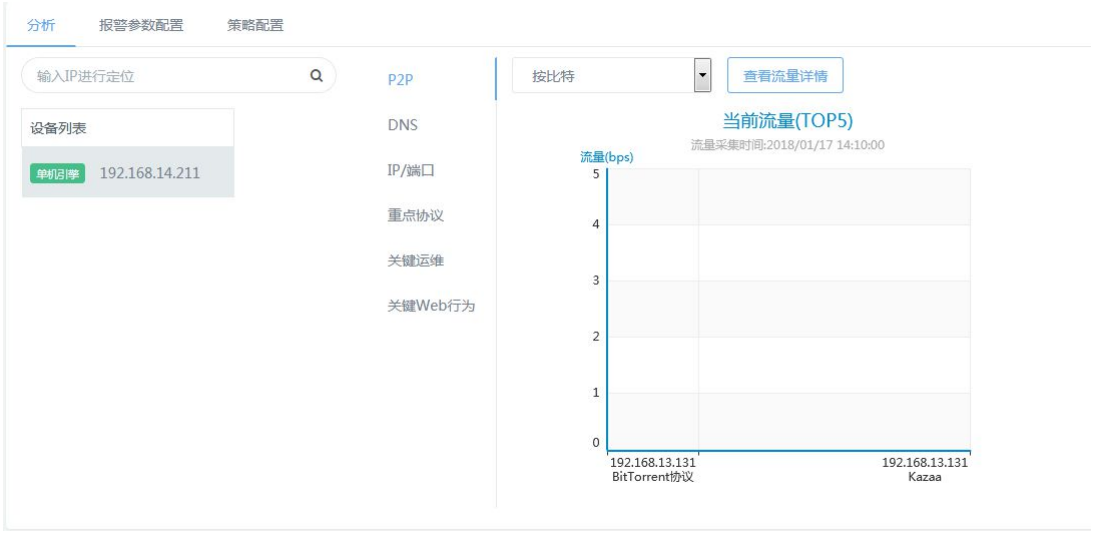

图 4-30 分析页面

界面左侧列出的是设备列表；主要是控制中心下面挂载的引擎，如下图所示。

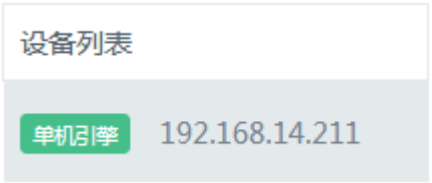

图 4-31 设备列表信息

在设备列表下面的查询栏中输入引擎 IP，可以进行引擎定位，如下图所示。

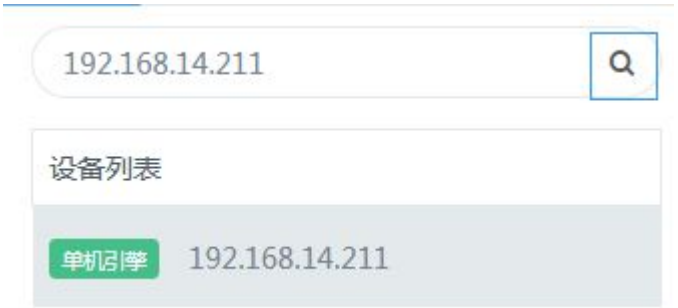

图 4-32 查询列表页面

界面右侧显示所选择引擎的微观流量柱形图（当前时间的流量变化柱形图，每 10 分钟为一个点的流量 TOP5 排序）内容包括：P2P、DNS、IP/端口、重点协议、关键运维、关键 Web 行为，当前流量值展示方式为按字节(bps)，如下图所示。

图 4-33 引擎流量信息展示

点击**[重点协议]**，可查看微观流量中重点协议当前 Top5 流量。

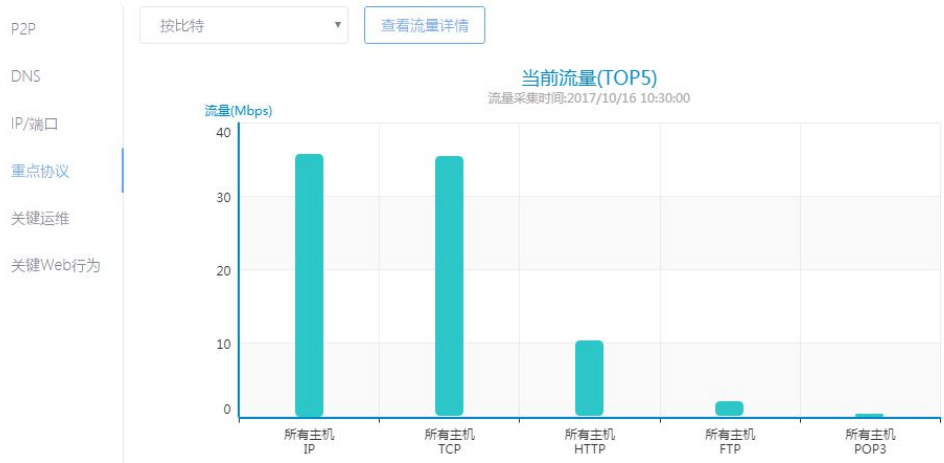

图 4-34 重点协议流量信息展示

将鼠标放置于相应的时刻点的柱形积图上，可以看到相应流量的信息，如下图所示。

图 4-35 重点协议相信流量展示

点击界面上的切换展示方式，可以选择各设备的当前流量按包数显示流量值（pps）还是按照比特显示流量值（bps），如下图所示。

图 4-36 选择流量显示方式

图 4-37 按包数显示流量展示

在设备列表中点击所要查看的设备，即可在右侧界面展示该设备的微观流量，假设要查看引擎-IDS 的微观流量中的**重点协议**信息，点击 192.168.13.89 设备即可，如下图所示。

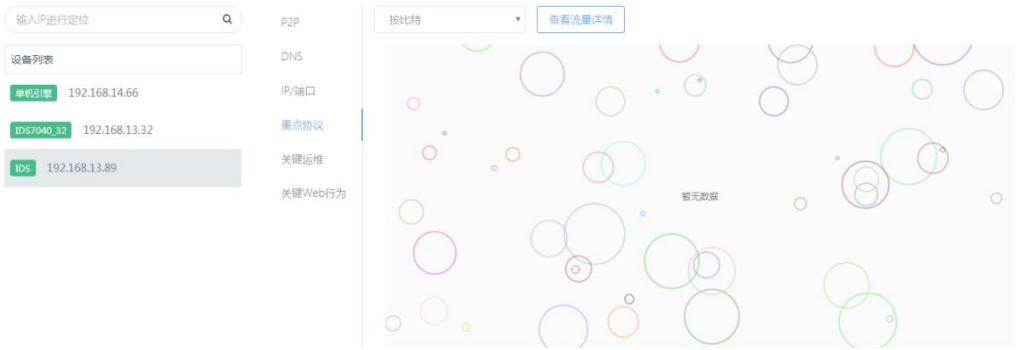

图 4-38 指定引擎流量信息展示

点击界面上方的**[查看流量详情]**按钮，可以进入到微观流量中 P2P 流量详细分析界面，如下图所示。

图 4-39 查看详细流量展示

在流量分析详细界面中点击**[返回]**按钮，即可返回到微观流量分析界面，如下图所示。

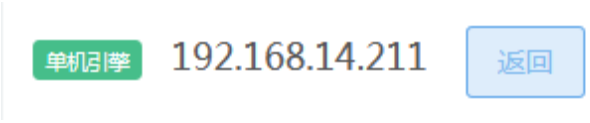

图 4-40 返回分析界面

微观流量详细分析界面主要包括最近 24 小时流量、流量实时分布和报警信息。

最近 24 小时流量：

最近 24 小时流量是展示的是当前时间之前的最近 24 小时微观流量统计信息，每 10 分钟统计一次，将鼠标置于对应的时刻点流量曲线时，会显示相应的流量信息，其中蓝色

曲线代表当前的流量运行态势，紫色色代表历史流量运行态势，如下图所示。

图 4-41 最近 24 小时流量展示

流量实时分布：

该流量分布列表给出了分析目标、协议类型、流量、流量压力、及运行态势，运行态势说明当前的运行状态；P2P 协议类型包括：Maze、迅雷流量、百度下吧流量，POCO 流量，Kamun 流量，酷狗流量等，协议类型后续在“微观流量配置策略模块”说明。

流量实时分布

分析目标	协议类型	流量	压力	运行态势
所有主机	Maze	当前:0 bps 历史:N/A	0%	N/A
所有主机	迅雷	当前:0 bps 历史:N/A	0%	N/A
所有主机	百度下吧	当前:0 bps 历史:N/A	0%	N/A
所有主机	BitTorrent...	当前:1.84 Kbps 历史:N/A	0%	N/A
所有主机	FlashGet	当前:0 bps 历史:N/A	0%	N/A
所有主机	百宝	当前:0 bps 历史:N/A	0%	N/A
所有主机	eMule协议	当前:0 bps 历史:N/A	0%	N/A

图 4-42 流量实时分布展示

点击不同的流量类型，其他展示模块也会随之切换为对应的流量展示，如点击流量实时分布中的 BitTorrent 流量，今日流量、报警信息都会展示 P2P 流量中 BitTorrent 流量的运行态势，如下图所示。

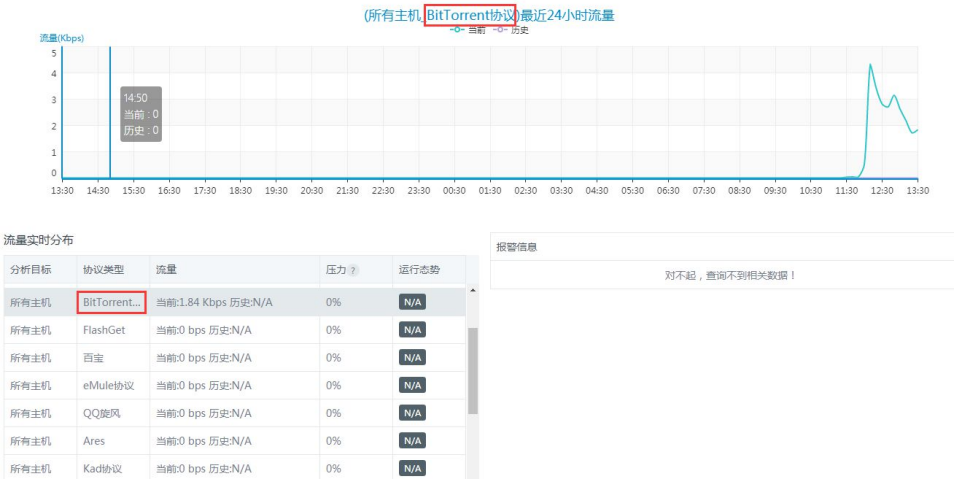

图 4-43 流量实时分布指定信息展示

报警信息：

报警信息展示的是各种流量各时刻点与设定阈值或历史同期流量的对比。

4.2.2 报警参数配置

点击**流量统计>微观流量>报警参数配置**，可以看到 6 种类型的微观流量分析参数，系统默认状态是历史同期对比方式，系统会采用默认（机器自动分析）进行报警分析。系统默认参数(偏低系数 0-50，正常系数 50-100，轻度偏高系数 100-150，中度偏高系数 150-200，严重偏高系数是 200-∞)，如下图所示。

图 4-44 报警参数配置展示

点击相应流量类型的**[编辑]**按钮，可以进入到该类型流量报警参数的设置，假设要设置重点协议流量的报警参数，如下图所示。

图 4-45 报警参数配置展示

若要采用自定义配置模式，点击配置类型设置切换按钮，进入到自定义配置模式，如下图所示。

图 4-46 配置类型选择展示

图 4-47 自定义配置展示

流量异常分析方法包括同期对比分析和阈值对比分析两种分析方法。

同期对比分析：

当配置是默认配置时，系统默认为同期对比分析配置，系统会根据当前 10 分点的引擎流量数据的 bps 值与配置的自动分析系数进行对比，如果发现异常进行报警。为用户自定义配置，会根据当前 10 分点的引擎的流量数据包（pps）的值跟用户配置的自动分析参数对比，如果发现异常进行报警。

“同期对比”时，修改流量分析参数，具体报警级别分为四种：偏低、轻度偏高、中度偏高和严重偏高；如下图所示。

图 4-48 同期对比参数展示

用户可以根据实际情况进行响应方式的配置，是否产生报警日志，是否产生报警，报警级别具体开放或关闭哪个级别，是否利用邮件进行报警信息的发送，如下图所示。

图 4-49 响应方式配置展示

当控制中心未配置邮件时，会有提示“无可用邮件列表，若开启邮件报警，请先到“系统管理->响应方式->邮件配置”下配置”，如下图所示。

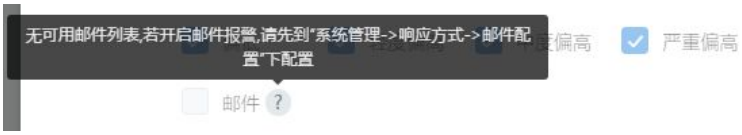

图 4-50 未配置邮件展示

若控制中心进行了邮件配置，则此处会出现收件人信息列表，可以根据实际情况进行收件人的选择，配置收件人后，产生的报警信息就会发送给相关人员，以便实时进行流量的分析。

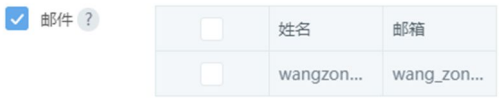

图 4-51 已配置邮件展示

阈值对比分析：

如果用户配置的是阈值对比分析，系统会根据当前 10 分点引擎流量数据跟用户配置的流量数据进行对比。如果发现异常进行报警。

点击流量异常分析方法切换按钮切换到阈值对比分析配置模式，如下图所示。

图 4-52 流量异常分析选择展示

“阈值对比分析”时，修改流量分析参数，具体报警级别分为四种：偏低、轻度偏高、中度偏高和严重偏高；如下图所示。

图 4-53 阈值对比参数展示

流量的默认单位是 bps，可以通过参数设置流量的单位。展开单位下拉框，进入参数设置界面，选择流量单位，就可以设置流量的单位，并且在以后登录后，会一直使用这个单位，直到下一次改变。

图 4-54 单位选择页面

展开数量级下拉框，可以进行数量级的设置，设置完成后，相应报警级别后的区间范围会自动乘以该数量级，如下图所示。

图 4-55 数量级参数展示

用户可以根据实际情况进行响应方式的配置，是否产生报警日志，是否产生报警，报警级别具体开放或关闭哪个级别，是否利用邮件进行报警信息的发送，如下图所示。

图 4-56 响应方式配置展示

当控制中心未配置邮件时，会有提示“无可用邮件列表，若开启邮件报警，请先到“系统管理->响应方式->邮件配置”下配置”，如下图所示。

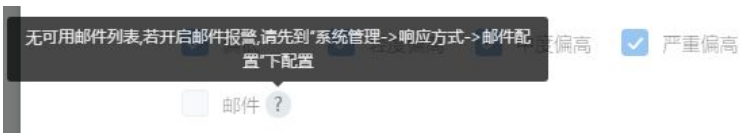

图 4-57 未配置邮件展示

若控制中心进行了邮件配置，则此处会出现收件人信息列表，可以根据实际情况进行收件人的选择，配置收件人后，产生的报警信息就会发送给相关人员，以便实时进行流量的分析。

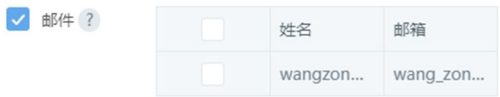

图 4-58 已配置邮件展示

用户根据需要进行报警参数的自定义配置后，保存相应配置后，在微观流量报警参数设置列表中会有所表现，如下图所示。

图 4-59 自定义配置展示

4.2.3 策略配置

点击**流量统计>微观流量>策略配置**，默认打开策略列表界面如图：

图 4-60 策略配置界面展示

策略列表：

点击右上角**[新建]**按钮，弹出新建策略界面，在新建策略界面展开流量类型下拉框，可以新建 6 种协议类型，包括 P2P、DNS、IP/端口、重点协议、关键运维、关键 Web 行为。如图所示：

图 4-61　新建策略展示

P2P 流量类型如图所示：

图 4-62 P2P 流量类型选择展示

DNS 流量类型如图所示：

图 4-63 DNS 流量类型展示

IP/端口流量类型如图所示：

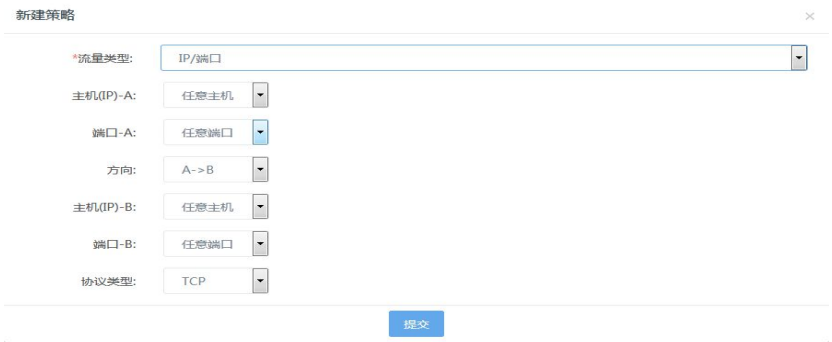

图 4-64 IP/端口流量类型展示

重点协议流量类型如图所示：

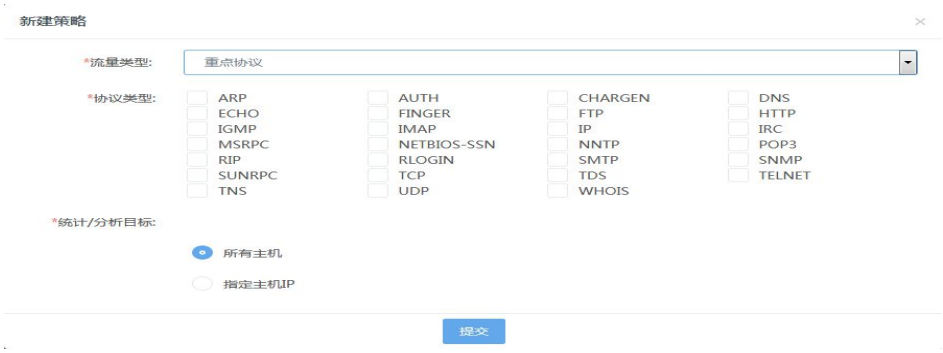

图 4-65 重点协议流量类型展示

关键运维流量类型如图所示：

图 4-66 关键运维流量展示

关键 Web 行为流量类型如图所示：

图 4-67 关键 Web 行为流量展示

假设用户配置 P2P 流量类型，配置 16 种协议，统计/分析目标为所有主机。（其中 P2P 流量类型有 16 种协议，可以选择单个协议或者选择多个协议）。如图所示：

图 4-68 P2P 流量参数展示

针对 P2P 流量类型中的协议类型，鼠标放置协议类型上，系统会弹出相关协议说明，如图所示：

图 4-69 P2P 流量协议说明展示

统计/分析目标可以配置所有主机或者指定主机 IP，（所有主机引擎会统计所有主机的配置流量统计，指定主机引擎会根据用户输入 IP 地址进行流量统计）例如输入 192.168.1.1，如图所示：

图 4-70 统计分析配置展示

用户输入错误 IP 数据格式时，页面上方系统会出现提示，如图所示：

图 4-71 错误提示页面

将用户配置好的 P2P 流量类型然后保存，关闭。在策略列表界面会显示出刚才配置的策略，如图所示：

图 4-72 策略配置成功展示

在创建好的策略集列表，点击策略项的**[编辑]**按钮进行编辑，系统会弹出修改策略界面，用户可以进行策略修改提交，关闭即可。

可以进行单个策略删除，系统弹出删除策略，确定即可对策略删除。如图所示：

图 4-73 删除策略页面

策略集列表：

点击**[策略集列表]**按钮，进入策略列表界面，如图所示：

图 4-74 策略集列表展示

策略集列表右上角**[新建]**按钮，可以新建策略集，弹出新建策略集界面如图所示：

图 4-75 新建策略集展示

在新建策略集界面，输入必填策略集名称，（名称不能为空，字符不超过 50，不能输入特殊符号，在说明栏内可以为空，可以输入数字，字母以及符号，字符不能超过 100）如图所示：

图 4-76 新建策略集参数展示

在新建策略集对话框中，可以添加策略，左边是选择策略复选框添加策略（这里的策略是策略列表界面新建的策略）将选择的策略添加到右边已选择的策略复选框中，可以用单击某条策略添加，也可以用全部按钮（ ➔➔ ）添加，进行保存。可对引擎进行策略下发。反之可以将右边添加好的策略进行单击移除，或全部移除按钮（ ←← ）全部移除。

选择添加策略，如下图所示：

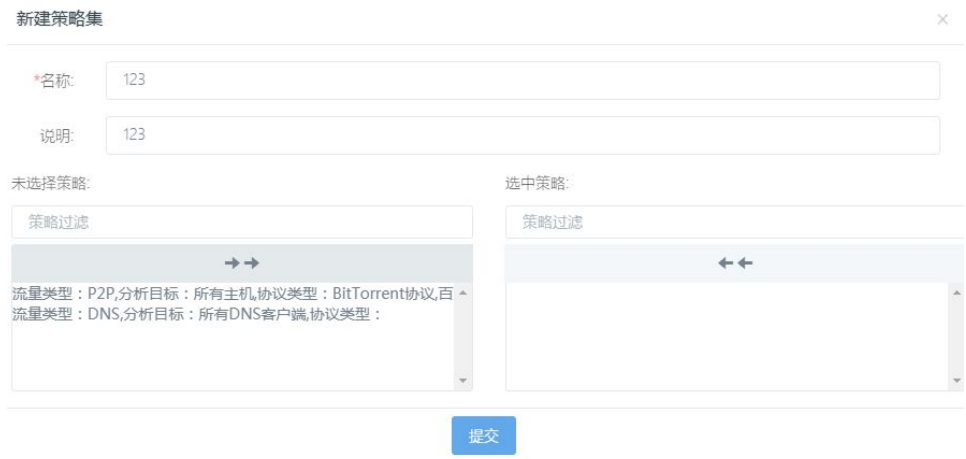

图 4-77 选择添加策略展示

单击单个策略添加，如图所示：

图 4-78 单个策略添加展示

全部策略添加，全部添加后，可选策略为空，如图所示：

图 4-79 全选策略添加展示

可以对策略进行过滤，在可选择策略过滤复选框中输入需要的内容进行过滤，（过滤内容有流量类型，分析目标，以及协议类型）如图所示：

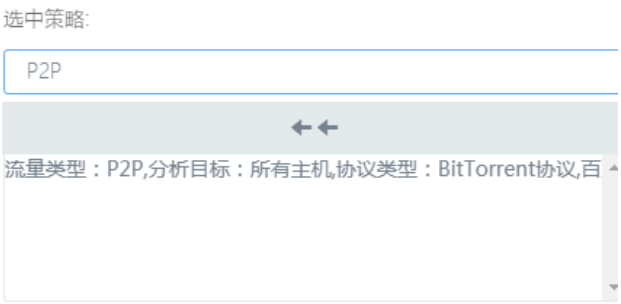

图 4-80 过滤策略展示

将添加好的策略，保存，退出后，在新建策略集列表界面可以看到策略集，如图所示：

图 4-81 成功新建策略集展示

新建好的策略集列表可以进行修改，点击操作列**[编辑]**按钮，弹出策略集列表修改界面。

可以对策略集进行删除，使用**[删除]**按钮，系统弹出删除策略集对话框，点击**[确定]**按钮即可如图所示：

图 4-82 删除策略集页面展示

将创建好的策略集进行下发，选择**[下发]**按钮，弹出下发策略界面，如图所示：

图 4-83 下发策略集页面展示

在过滤在线引擎列表复选框中，输入过滤条件。（检索内容为引擎名称以及引擎 IP）如图所示：

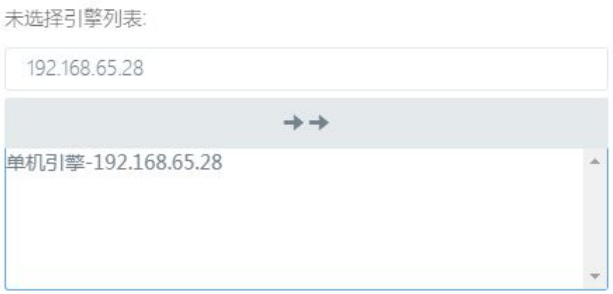

图 4-84 过滤引擎列表展示

在线引擎列表中选择要下发的引擎，点击引擎进行选择，也可以使用全选按钮（ ）多选下发，一个策略集可以下发多个引擎，但是一个引擎只能接受一个策略集。如图所示：

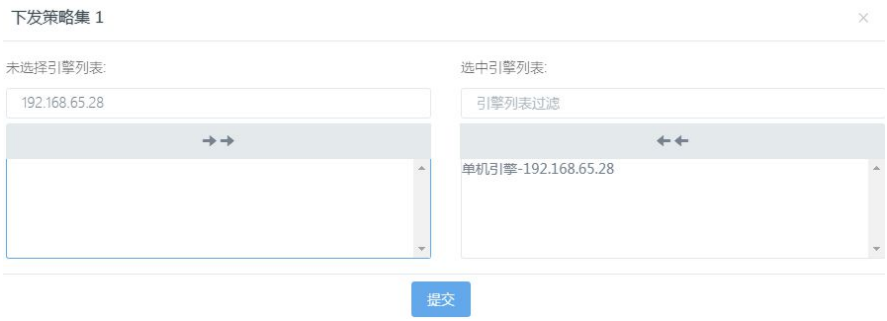

图 4-85 选择引擎页面展示

点击**[提交]**按钮，系统会提示下发成功。

图 4-86 下发策略成功页面展示

第5章 统计分析

统计分析由统计报表、任务列表和执行结果组成。

统计报表由任务列表及执行结果 2 个模块组成。任务列表包括报表基本信息，如报表名称、提交人、提交单位、描述等，报表模板类型的选择，如分析报表、基础统计报表、高级统计报表及详细事件报表，报表查询的时间范围、报表相关条件设置及报表是循环执行的任务还是手动执行的任务。

任务列表是用于导入或导出报表任务列表，新建分析报表、基础统计报表、高级统计报表及详细事件报表。如下图所示：

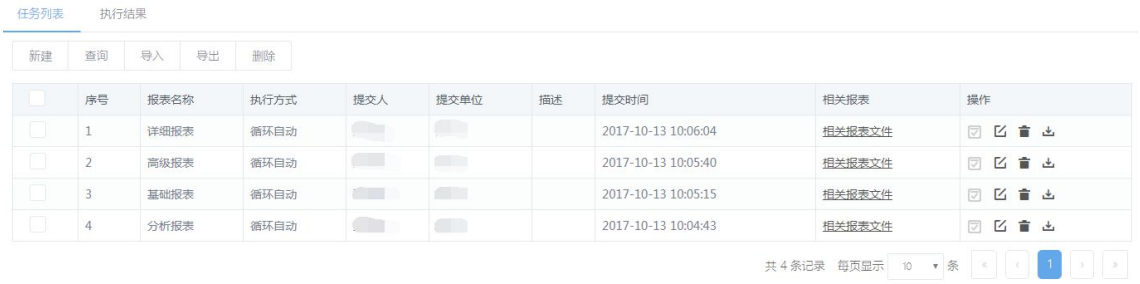

图 5-1 任务列表信息页面展示

报表执行结果是展示已经生成的报表文件。如下图所示：

图 5-2 报表执行结果展示

5.1 报表任务配置

5.1.1 新建报表任务

新增分析报表：

点击任务列表**[新建]**按钮，新增报表任务，进入配置报表页面如下图：

图 5-3 新建报表页面展示

新建报表任务时，必须填写报表名称、提交人、提交单位，描述可以根据实际需求进行填写，并且报表名称不能重复；输入相关信息。如下图：

图 5-4 新建报表参数展示

报表类型选择分析报表点击[下一步]按钮，进入选择分析报表模板页面。如下图：

图 5-5 报表类型选择展示

分析报表模板中，可以根据实际情况进行分析类型的选择，从 8 种类型中选择所需要的。时间周期有两种方式：基础时间周期和高级时间周期，基础时间周期中勾选所需要统计的事件发生的时间周期进行分析报表的生成；如果勾选高级时间周期，会出现相应的下拉菜单。如下图：

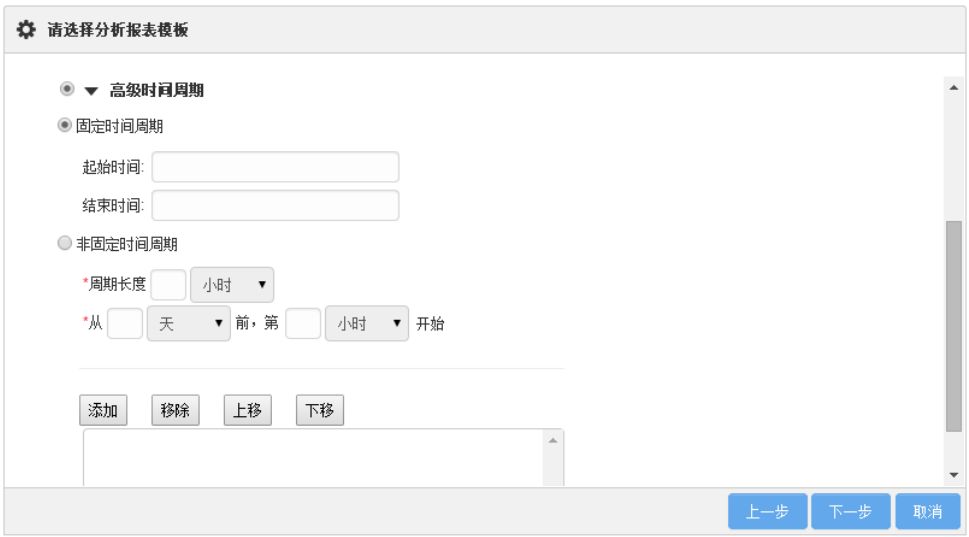

图 5-6 报表时间设置页面展示

在高级时间周期中，如果勾选固定时间周期，可以根据实际需求选择起始时间和结束时间进行分析报表的生成，如果勾选非固定时间周期，例如：我们添加一个时间周期“从 1 天前，第 3 小时开始，5 个小时为周期”，以今天是 2012-07-18 为基准，则按照周期统计的日志报表是 2012-07-17 的 3:00-8:00 的事件。

选择报表模板完成，点击**[下一步]**按钮，进入查询条件配置界面。查询条件配置完成后，点击**[下一步]**按钮，进入任务执行周期配置页面如下图：

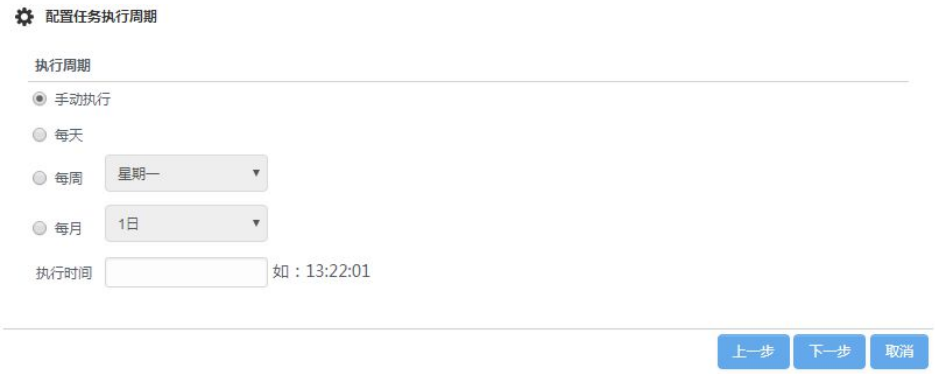

图 5-7 报表执行周期设置展示

任务执行周期具体可以分为两类：手动执行和自动执行；手动执行必须人工进行点击**[执行]**按钮方可以进行报表的生成，自动执行可以根据实际需求按照每天几时几分几秒、每周周几几时几分几秒和每月几日几时几分几秒进行定时自动执行。

任务执行周期配置结束后，点击**[下一步]**按钮，进入报表任务输出格式配置界面，该模块可以进行生成报表文件格式的选择和定义用户邮件组。可以根据实际情况勾选 HTML、PDF、EXCEL 和 WORD 格式的选择。如下图：

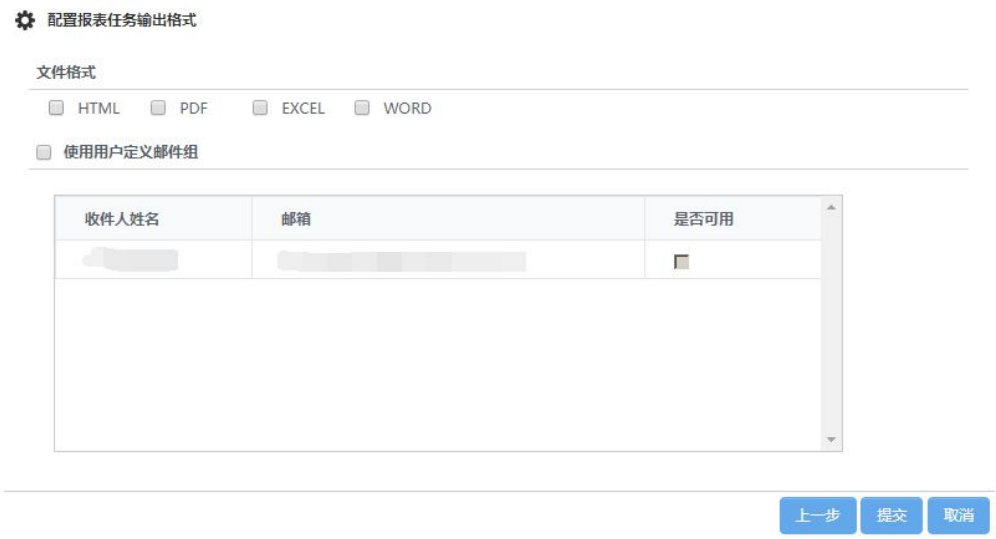

图 5-8 设置报表输出格式展示

如果勾选使用用户定义邮件组，会展开下拉框，如下图所示。

（用户定义邮件组配置见 7.1.3 邮件配置）

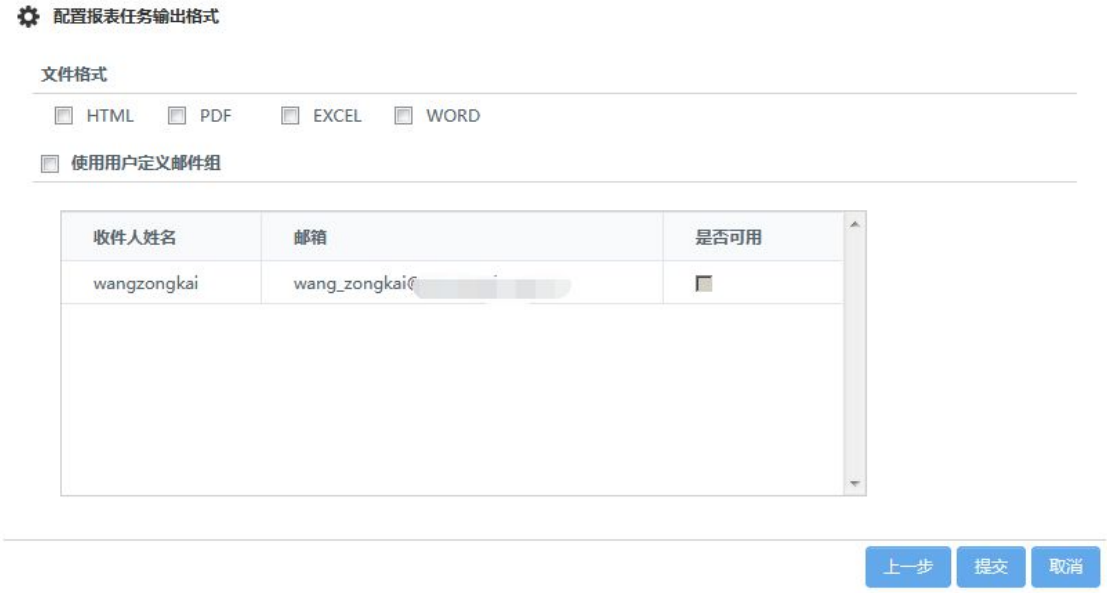

图 5-9 设置邮箱展示

可以将相应要生成的报表，生成后直接转发到相应用户的邮箱中。

进行完所有配置后，点击**[提交]**按钮，完成任务配置。相应配置的分析报表就出现在

报表任务列表中。

新增基础统计报表

点击**[新建]**按钮，新增报表任务，进入配置报表页面如下图：

图 5-10 新建基础统计报表展示

新建报表任务时，在报表类型中勾选“基础统计报表”，必须填写报表名称、提交人、提交单位，并且报表名称不能重复；进行基础统计报表生成时，可以进行 TopN 值的选择，N 值的范围在 5 到 100 之间，该值代表生成报表时每类统计事件最多统计的数量。点击**[下一步]**按钮，则进入基础统计报表模板选择页面如下图：

图 5-11 新建基础统计报表设置展示

可以根据实际需求进行事件基础统计的类别选择以及是否报表存在摘要，配置完成后；

点击**[下一步]**按钮，进入查询条件配置界面，如下图：

图 5-12 基础统计报表查询展示

查询条件配置后是配置任务执行周期和报表任务输出格式，具体的操作方法与新建分析报表一模一样，此处不再描述。

新增高级统计报表：

点击**[新建]**按钮，新增报表任务，进入配置报表页面如下图：

图 5-13 新建高级统计报表展示

新建报表任务时，在报表类型中勾选“高级统计报表”，必须填写报表名称、提交人、提交单位，并且报表名称不能重复；进行高级统计报表生成时，可以进行 TopN 值的选择，N 值的范围在 5 到 100 之间，该值代表生成报表时每类统计事件最多统计的数量。点击**[下一步]**按钮，则进入高级统计报表模板选择页面如下图：

图 5-14 高级统计报表设置展示

根据实际需求进行引擎、事件名称、事件级别、源 IP 地址、目的 IP 地址、处理状态、受影响的系统、受影响的设备和隐蔽信道的配置，配置完成后，接下来会相应的进行配置查询条件、任务执行周期和报表任务输出格式，具体的操作方法与新建分析报表一模一样，

此处不再描述。

新增详细事件报表：

点击**[新建]**按钮，新增报表任务，进入配置报表页面如下图：

图 5-15 新建详细事件报表展示

新建报表任务时，在报表类型中勾选“详细事件报表”，必须填写报表名称、提交人、提交单位，并且报表名称不能重复。点击**[下一步]**按钮，进行配置查询条件、任务执行周期和报表任务输出格式，具体的操作方法与新建分析报表一模一样，此处不再描述。

5.1.2 导入报表任务

点击**[导入]**按钮，导入报表任务，弹出导入报表任务对话框，浏览选择文件所在位置，如下图所示：

图 5-16 导入报表展示

点击**[提交]按钮**后，成功导入会提示如下信息。

导入错误扩展名的文件，会提示如下错误。

图 5-17 导入不支持类型提示页面

导入错误数据的文件，会提示如下错误。

图 5-18 导入错误数据提示页面

5.1.3 导出报表任务

报表任务配置可以批量导出，也可以单条导出。

如果执行批量导出操作，点击**[导出]**按钮，导出报表任务，弹出导出报表任务对话框，如下图所示，导出任务列表的格式为 xls，可以用 Excel 打开。如下图：

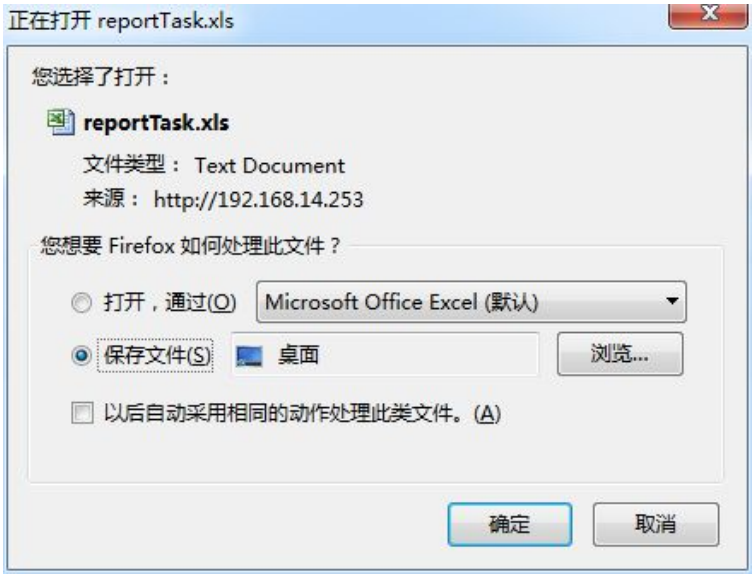

图 5-19 导出报表页面展示

如果执行单条导出操作，点击**[导出]**按钮，导出相应报表任务，弹出导出报表任务对话框，导出任务列表的格式为 xls，可以用 Excel 打开。

注意

导出 xls 文件时，由于个人机器环境不同，有可能无法弹出确认对话框，而是 IE 直接调用已安装的 EXCEL 软件把需要下载的文件打开 ,这时只能通过 IE 的后退功能返回到报表文件列表页面。

5.1.4 编辑报表任务

点击报表任务列表中的**[编辑]**按钮，可以修改报表任务。如下图：

图 5-20 编辑报表页面展示

此处需要注意的是进行四种日志报表的修改时，开始配置的报表名称和报表类型是不允许修改的，其他的配置条件可以根据实际需求的变化进行修改配置，相应的配置方法与新建报表任务时相应的操作一样。

5.1.5 删除报表任务

点击报表任务所在行的**[删除]**图标，会弹出一个询问对话框。如下图：

图 5-21 删除报表页面

点击**[确定]**按钮，相应的报表即被删除。

也可以通过多选统一进行报表任务删除。

5.1.6 手动执行报表任务

只有一次性任务才能手动执行报表任务，周期性任务无法手动执行。点击报表任务所在行的**[执行]**图标，报表任务即被手动执行。如下图所示：

图 5-22 执行报表页面展示

5.1.7 相关报表文件

点击报表任务所在行的**[相关报表文件]**的链接，进入该报表文件相关的报表文件列表页面，如下图所示，选择的报表名称会作为下拉过滤框的查询条件。如下图：

图 5-23 相关报表展示

5.1.8 使用邮件方式发送报表

在新建报表时，配置报表任务输出格式模板里，可以配置使用用户定义邮件组进行报表发送，如图所示：（用户定义邮件组配置见 7.1.3 邮件配置）如下图：

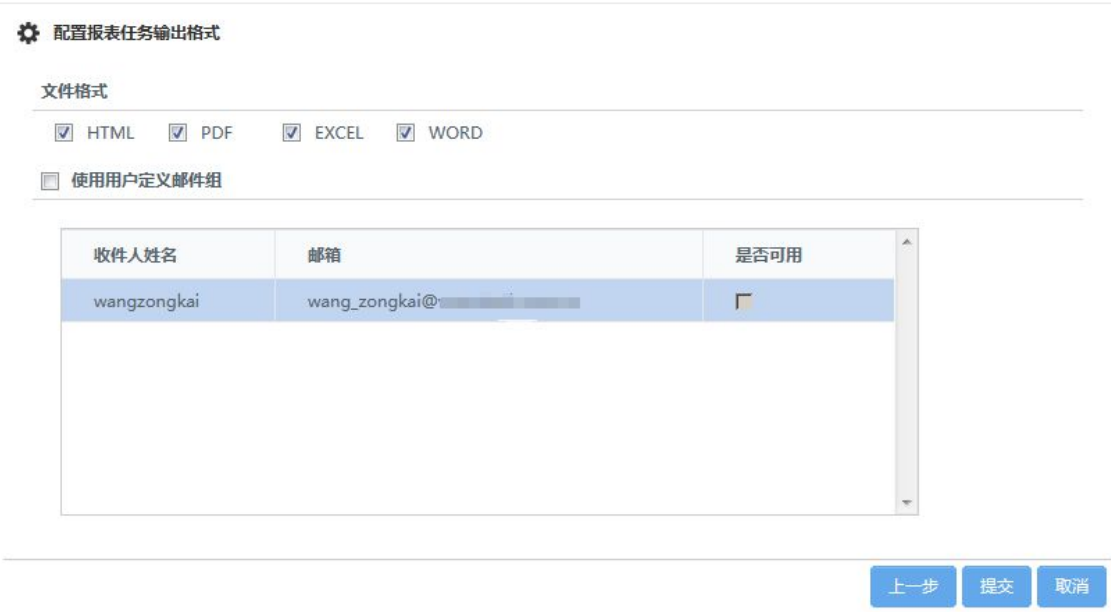

图 5-24 邮件发报表设置

勾选“使用用户定义邮件组”前的选项框，在下拉列表中，选择收件人。如下图：

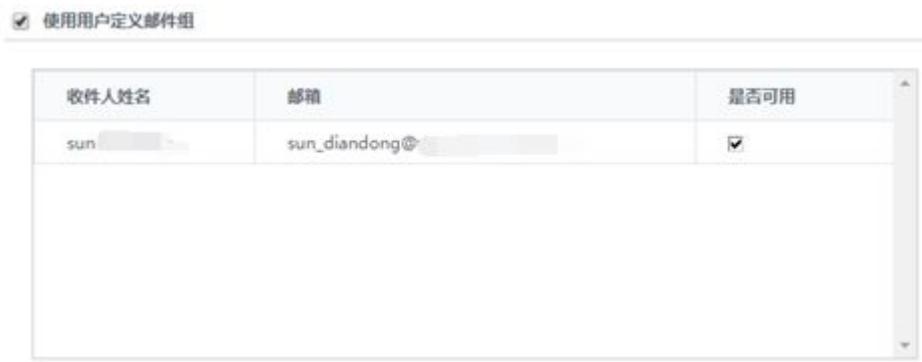

图 5-25 选择自定义收件人

选择自定义收件人，勾选相应收件人栏中“是否可用”选项框，（默认收件人栏中“是否可用”选项框是不勾选的），配置收件人完毕后，点击**[提交]**按钮，新建报表任务成功。

5.2 报表执行结果

可以根据报表名称及相应报表生成时间的范围进行日志报表的查询、删除、查看、下载等操作。

5.2.1 查询报表结果

选择报表名称、开始日期、结束日期查询报表结果文件列表，查询条件如下图：

图 5-26 查询报表页面展示

注意

如果通过设置查询时间来查询报表结果时，开始时间和结束时间必须均有值才可以查询，只输入单一时间值，不可以查询，并且结束时间必须大于开始时间。

按照配置的查询条件进行查询，查询结果如下图：

图 5-27 查询报表配置条件展示

5.2.2 删除报表目录

点击报表文件列表所在行的**[删除]**按钮，会弹出相应的询问窗口。

图 5-28 删除报表页面

点击**[确认]**按钮，该报表文件及其目录即被删除。

5.2.3 查看HTML文件

点击报表文件列表所在行的报表文件超链接，即可以打开 HTML 文件。如下图：

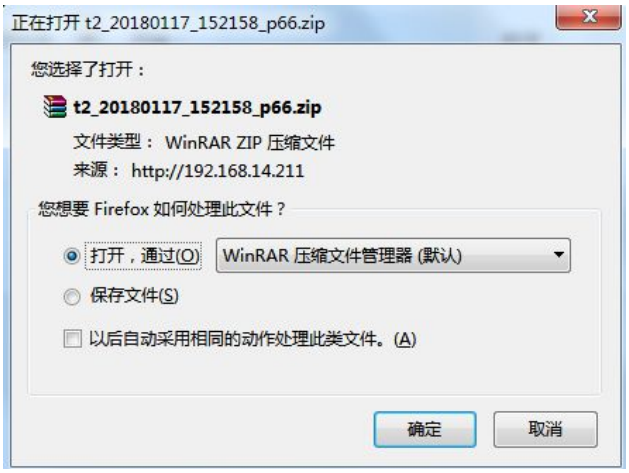

图 5-29 下载 HTML 文件展示

5.2.4 下载PDF文件

点击报表文件列表所在行的**下载 PDF** 图标，弹出下载确认对话框，询问是否保存，点击**[保存]**按钮之后，PDF 文件下载到用户本机。如下图：

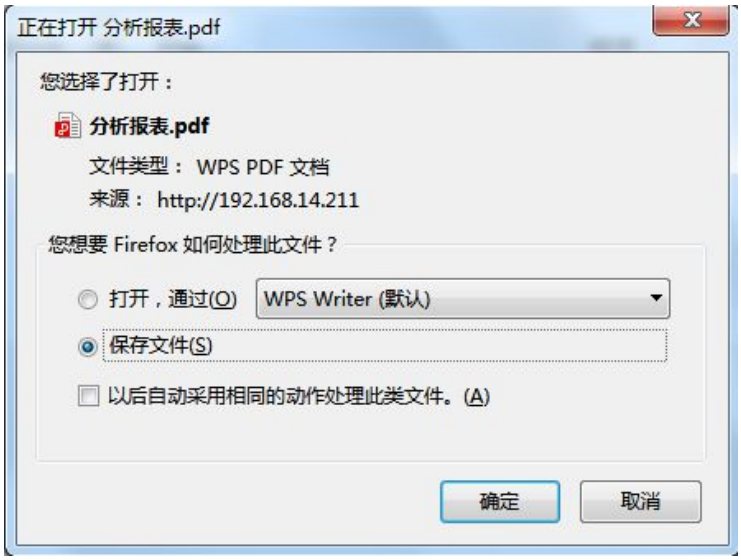

图 5-30 下载 PDF 文件展示

注意

下载 PDF 文件时，由于个人机器环境不同，有可能无法弹出确认对话框，而是 IE 直接调用已安装的 PDF 阅读软件把需要下载的文件打开，这时只能通过 IE 的后退功能返回到报表文件列表页面。

5.2.5 下载WORD文件

点击报表文件列表所在行的**下载 WORD** 图标，弹出下载确认对话框，询问是否保存，点击**[保存]**按钮之后，WORD 文件下载到用户本机。

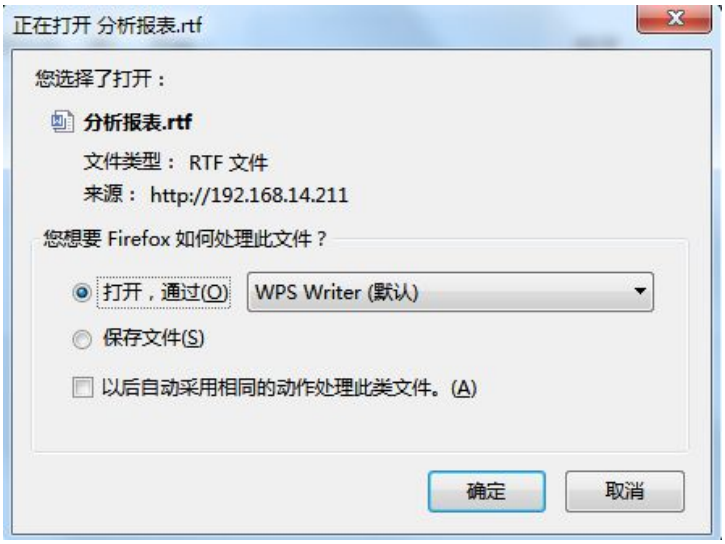

图 5-31 下载 WORD 文件展示

注意

下载 WORD 文件时，由于个人机器环境不同，有可能无法弹出确认对话框，而是 IE 直接调用已安装的 WORD 软件把需要下载的文件打开，这时只能通过 IE 的后退功能返回

到报表文件列表页面。

5.2.6 下载EXCEL文件

点击报表文件列表所在行的**下载 EXCEL** 图标，弹出下载确认对话框，询问是否保存，点击**[保存]**按钮之后，EXCEL 文件下载到用户本机。如下图：

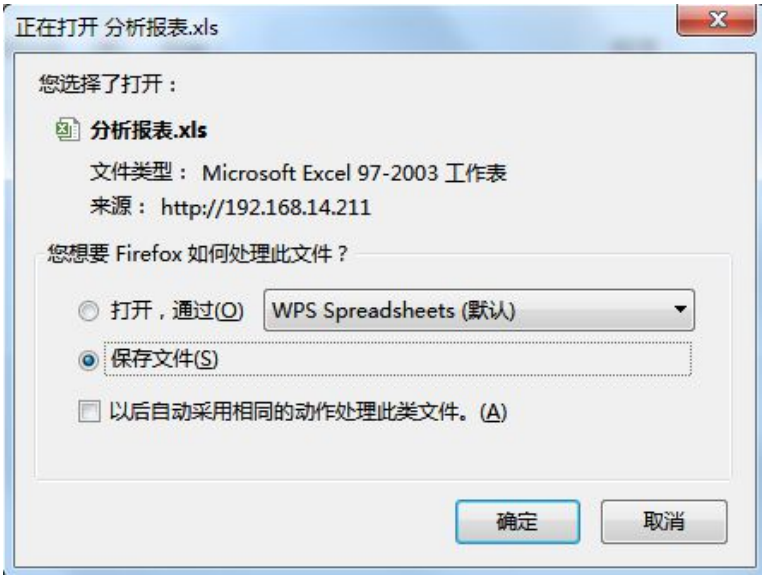

图 5-32 下载 EXCEL 文件展示

注意

下载 EXCEL 文件时，由于个人机器环境不同，有可能无法弹出确认对话框，而是 IE 直接调用已安装的 EXCEL 软件把需要下载的文件打开，这时只能通过 IE 的后退功能返回到报表文件列表页面。

5.2.7 更改IE直接在页面打开下载文件设置

如果需要修改 IE 直接在页面打开下载文件的方式，可以通过以下步骤实现：

打开我的电脑，选择菜单>工具>文件夹选项，选择文件类型选项，在已注册的文件类型中选择需要更改的文件类型如：XLS，选择高级按钮，勾选下载后确认打开，不勾选在同一窗口中浏览，点击[确定]按钮，设置完毕。重新启动 IE，看是否会弹出确认对话框。

第6章 检测配置

检测配置模块由管理人员对特征检测、资产、组件、文件检测、病毒检测、URL 检测、隐蔽信道检测模块根据客户本身的需要进行配置。

特征检测配置模块包括：策略集、策略模板、特征事件、二次事件和拒绝服务与扫描类、弱口令配置、事件合并。

资产配置模块包括：重点 web 服务器、IP-MAC 绑定。

设备管理模块包括：组件管理、引擎配置、上级状态。

文件检测配置模块包括：黑名单、白名单。

病毒检测配置模块包括：病毒检测配置。

URL 信誉库模块包括：黑名单、白名单。

隐蔽信道库模块包括：隐蔽信道库。

6.1 特征检测配置

6.1.1 概述

建立并管理系统 Web 端的策略集，系统默认的策略集允许查看、衍生、导出操作但不允许删除操作。新建的策略集主要提供以下功能：新增、编辑、设置有效性、应用模板和删除五个功能。策略集中还允许策略集合并、导入、导出和衍生操作。

6.1.2 策略集操作

策略集编辑界面由命令按钮和一个列表组成。如下图：

图形化用户界面

图 6-1 策略集信息展示

命令按钮：

命令按钮提供了对策略集的新建、合并、导入和刷新操作。

新建：新建一个策略集。

合并：将多个策略集进行合并生成一个新的策略集。

导入：将导出的策略集文件导入。

刷新：刷新策略集列表。

列表如下图：

图 6-2 策略集列表信息展示

列表中的条目为显示项信息。列表中最右面的列一般为图标按钮列，可对该条目进行操作。

图标：

页面中有很多图标帮助进行配置管理操作。当鼠标停留到图标上时，会出现提示信息，以帮助理解图标的含义。下表对页面中的图标进行说明。

图标	名称	说明
	查看	打开系统默认的策略集
	下发策略	将当前策略集下发给引擎
	编辑	编辑某个用户自定义的策略集
	衍生	从当前策略集衍生出一个新的策略集
	导出	将当前策略集导出到本地指定位置
	删除	将对应的自定义策略集删除

6.1.3 新建策略集

功能介绍：新建一个策略集。

操作步骤：

进入策略集列表界面；

点击右上方列表中的**[新建]**按钮；随后弹出对话框，如下图：

图 6-3 新建策略集页面

在对话框中输入名称和描述，点击**[下一步]**，进入事件选择对话框。如下图：

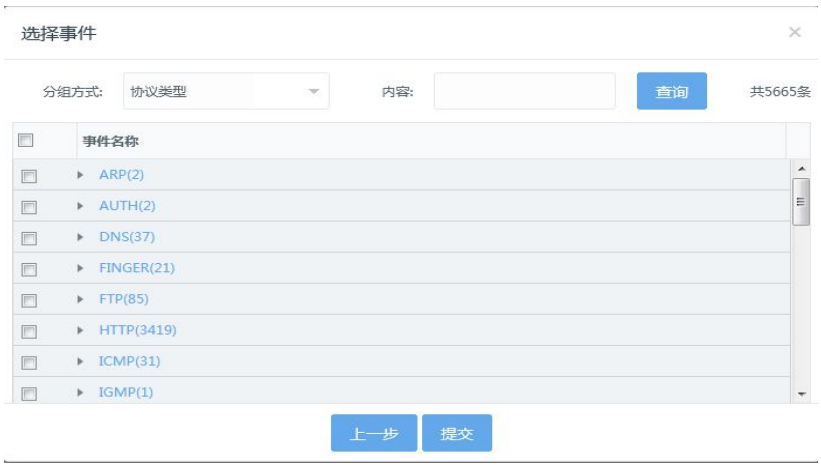

图 6-4 策略集事件设置展示

选择要添加的事件或者通过模糊查询找到目标事件，然后点击**[确定]**按钮进行提交，添加完成；点击**[上一步]**返回前一操作，点击 **X** 按钮取消操作。

注意

策略集的名称不能为空，描述可以为空；策略集的名称和描述不允许输入某些特殊字符（如：~!@#$%^&*等）。

6.1.4 导入策略集

功能介绍：将从已导出的策略集文件导入到当前系统策略集列表中。

操作步骤：

进入策略集列表界面；

点击右上方的**[导入]**按钮，随后弹出对话框，如下图：

图 6-5 导入策略集文件

选择要导入策略集文件，文件后缀为**.**policy；

然后点击**[提交]**按钮进行提交或者 **X** 按钮取消操作；

提交完成后，返回策略集列表界面，可以通过刷新查看策略集是否导入完成。

注意

如果选择不合法的文件会出现错误提示。

6.1.5 打开策略集

功能介绍：打开系统默认的策略集，查看里面的策略项。

操作步骤：

进入策略集列表界面；

点击列表中的**查看**（用户自定义策略集是**[编辑]**按钮），进入策略项列表界面。

备注：系统默认策略集不能编辑，只能查看。如下图：

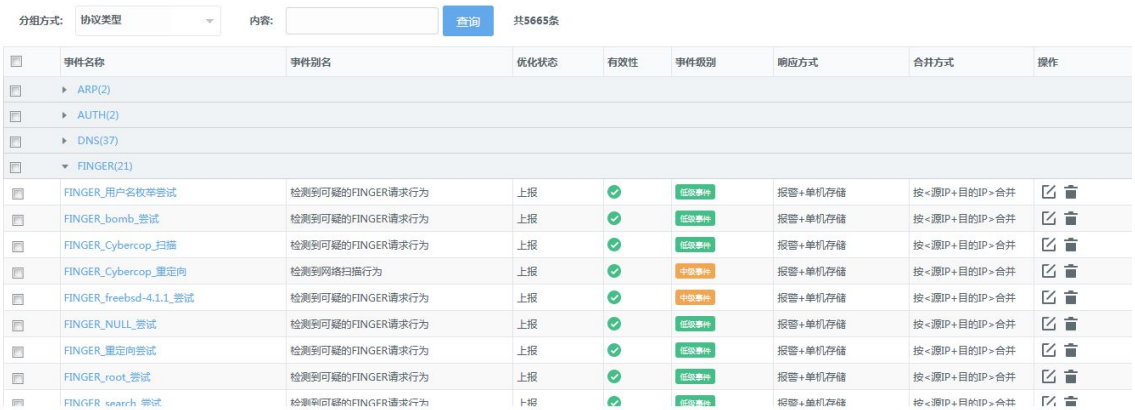

图 6-6 查看事件信息展示

6.1.6 编辑策略集

功能介绍：打开用户自定义的策略集，对里面的策略项进行编辑。

操作步骤：

进入策略集列表界面；

点击列表中的**[编辑]**按钮，进入策略项列表界面。

策略集修改完成后，只有重新下发到引擎后才能生效。

策略项列表如下图所示：

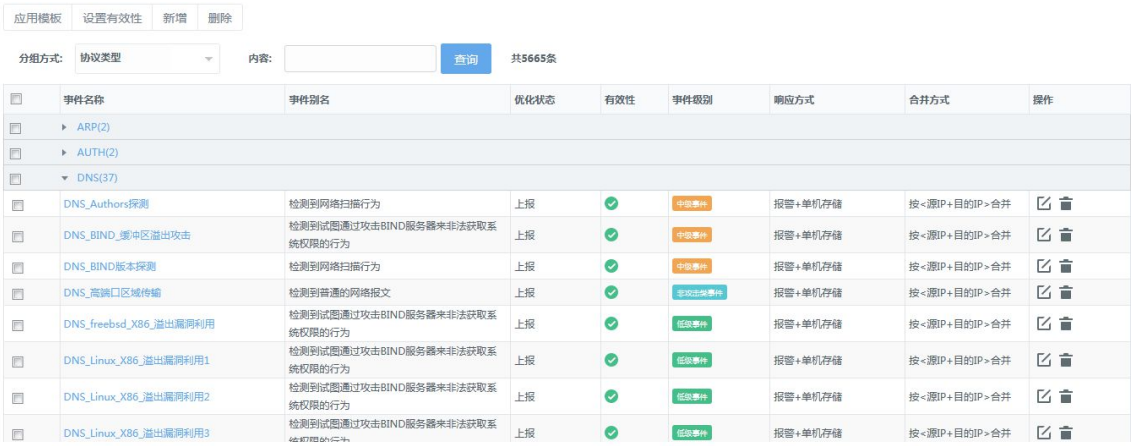

图 6-7 自定义策略集事件展示

说明：只有用户定义策略集才可以进行新增、删除、修改、应用模板、设置有效性、批量删除操作。

分组方式：

点击策略列表工具栏中的分组方式列表可以根据按协议类型、攻击类型、安全类型、流行程度、事件级别、影响设备、影响系统分组显示。

查询：

在名称输入框里输入关键字点击**[查询]**按钮或回车进行查询，显示要查询的结果，查询为模糊查询，例如输入“IP”，则名称包含关键字 IP 的都显示出来，不区分大小写。

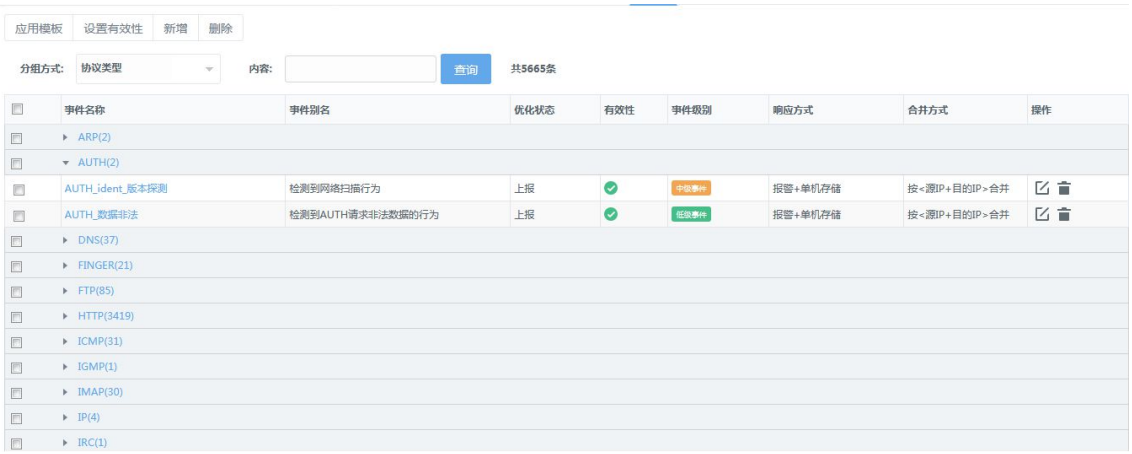

图 6-8 查询事件展示

新增策略项：

在所编辑的策略集中增加新的策略项，点击**[新增]**按钮打开新增策略项对话框如下图

所示：

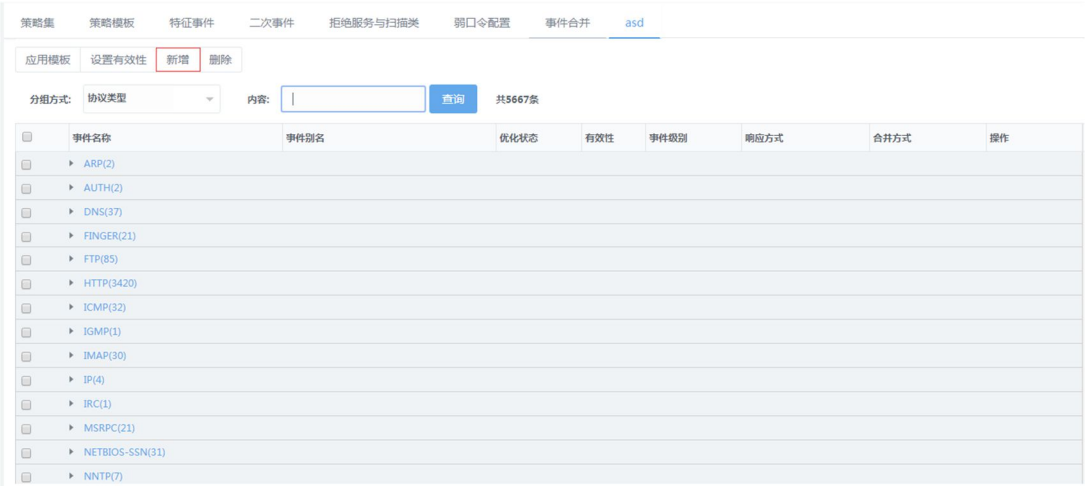

图 6-9 新增策略项页面展示

分组方式可以按协议类型、安全类型、流行情况、事件级别、影响设备、影响系统进行分组，打开默认按协议类型分组；点击**[事件名称]**按钮弹出事件的详细信息如下图。在表头事件名称下面的输入框中输入关键字点击**[查询]**按钮可以根据事件名称检索事件。

图 6-10 详细事件信息展示

点击事件列表前面的复选按钮可以选中要添加的事件，可以进行多组事件中的多个事件的选中和取消，选中事件后点击**[确定]**按钮，把选中的事件添加到策略中，返回策略项列表，刷新显示。

批量删除：

选中要删除的策略项，点击**[删除]**按钮，打开确定对话框，如果没有选中任何策略项，则提示“请选择策略项”。确定对话框如下图：

图 6-11 删除策略项页面

点击**[确定]**按钮删除所有选中的策略项，返回策略项列表，刷新显示。

批量设置有效性：

选中要设置的策略项，点击**[设置有效性]**按钮，打开设置有效性对话框，如果没有选中任何策略项，则提示“请选择策略项”。设置有效性对话框如下图：

图 6-12 批量有效性设置

选择有效或无效，点击**[确定]**按钮完成，返回策略项列表，刷新显示。

应用模板：

选中要应用模板的策略项，点击**[应用模板]**按钮，打开应用模板对话框。如果没有选中任何策略项，则提示“请选择策略项”。应用模板对话框如下图：

图 6-13 应用模板设置页面

选择要应用的模板，点击**[提交]**按钮完成，返回策略项列表，刷新显示。

备注：如果没有策略模板则提示“策略模板为空，请添加。”。

编辑策略项：

点击**[编辑]**图标，打开编辑策略项对话框如下图所示：

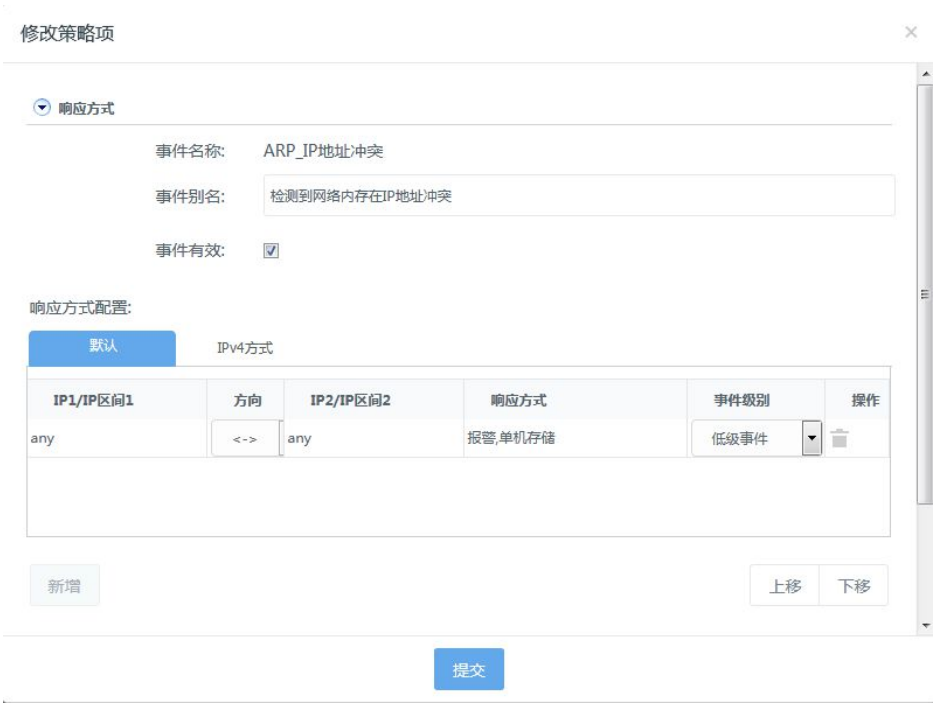

图 6-14 编辑策略项展示

响应方式：

响应方式里面包括：事件是否有效、事件级别、响应方式子项，响应方式子项又包括：日志、报警、单机存储、RST 阻断、防火墙联动、Syslog、SNMP、邮件报警、提取原始报

文选项。单机响应方式可以打开响应方式选择列表，如下图所示。默认的响应方式的 IP/IP 区间为 any，方向为双方向<->，事件级别为系统默认的级别，表示该事件是任意源 IP、目的 IP 时使用的响应方式和事件级别。默认的响应方式中 IP/IP 区间与方向是不允许修改的，且不可以删除，响应方式和事件级别允许修改。如下图：

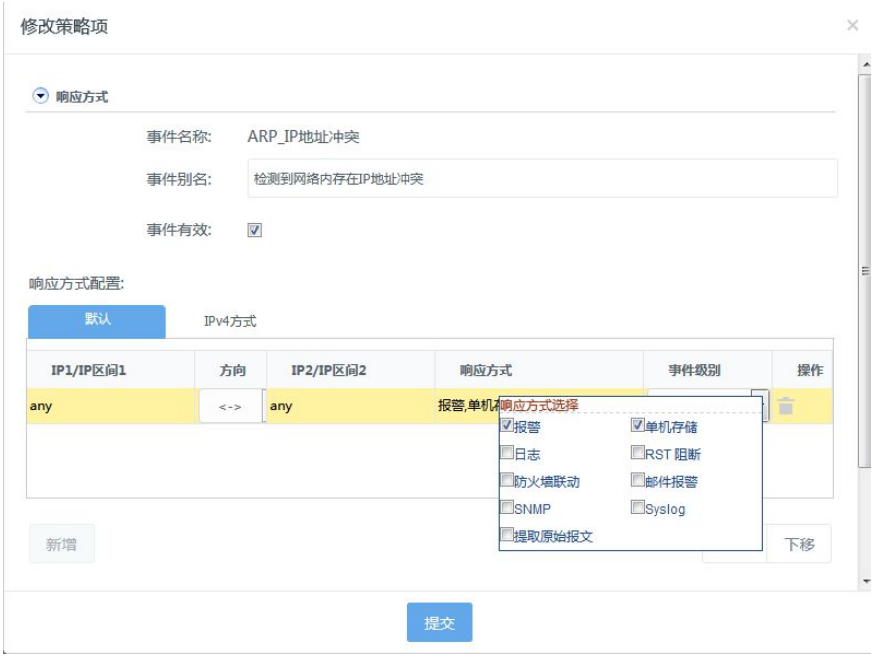

图 6-15 响应方式设置展示

针对指定的 IPv4 点击响应方式配置下方的**[新增]**按钮，可以增加 IP/IP 区间响应方式，如下图所示。

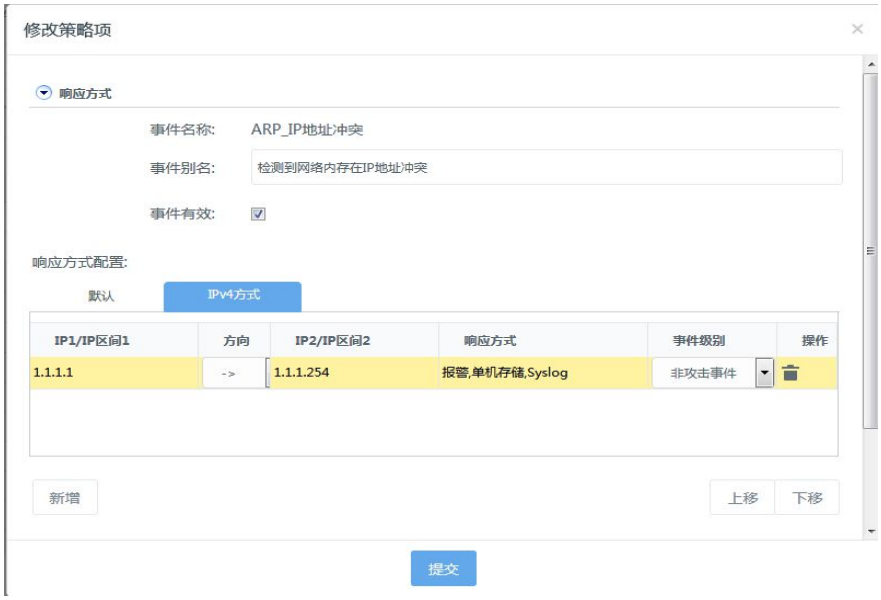

图 6-16 新增响应方式展示

针对 IPv4 方式，单击 IP/IP 区间进入编辑模式，输入 IP 或 IP 区间，IP 区间使用“-”分隔。方向“->”表示 IP1/IP1 区间为源 IP/IP 区间，IP2/IP2 区间为目的 IP/IP 区间；方向“<-”表示 IP2/IP2 区间为源 IP/IP 区间，IP1/IP1 区间为目的 IP/IP 区间；方向“<->”表示 IP1/IP1 区间为源或目的 IP/IP 区间，IP2/IP2 区间为源或目的 IP/IP 区间。如下图：

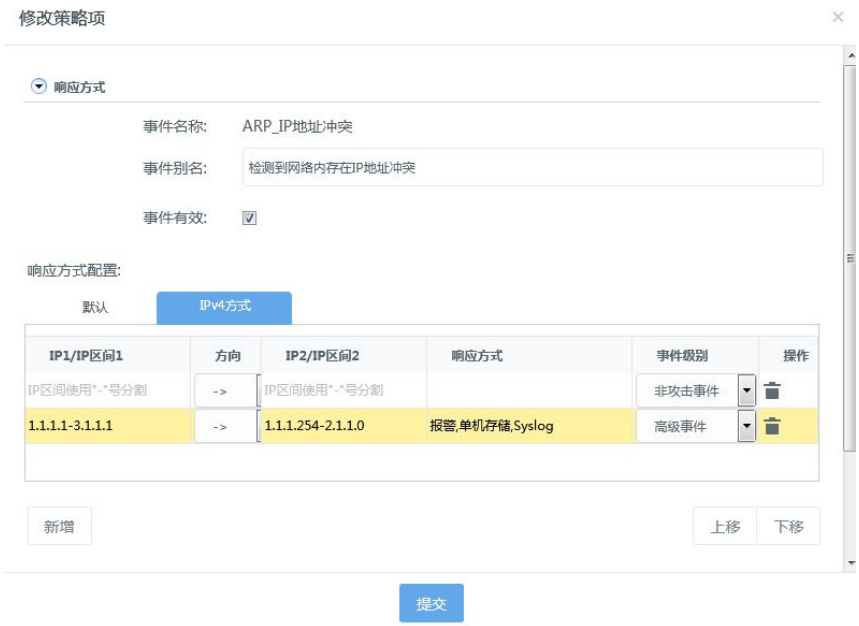

图 6-17 新增响应方式展示

点击**[响应方式]**按钮，可以勾选满足此 IP 配置时启用的响应方式，事件级别的下拉框中可以选择此事件的级别。如下图：

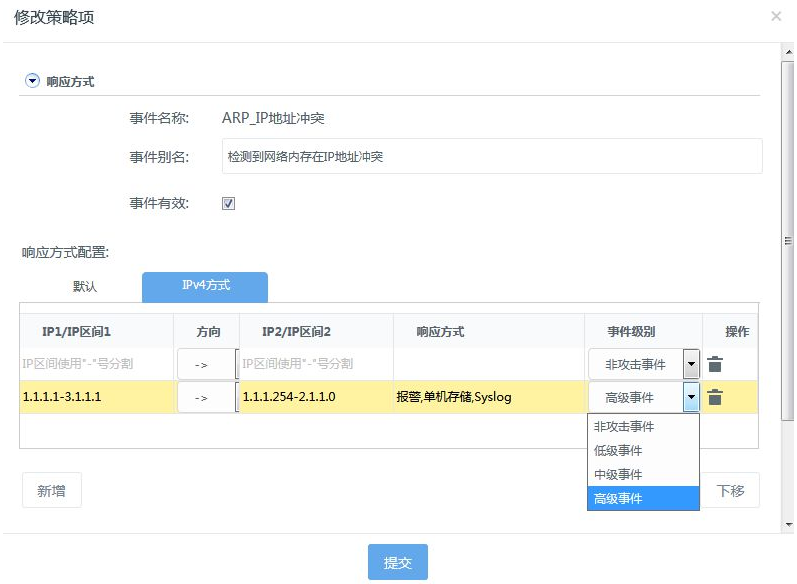

图 6-18 事件级别参数展示

点击操作列的**[删除]**按钮，可以对相应配置进行删除操作。

按照如上操作步骤即可完成 IP/IP 区间响应配置，如下图所示的配置表示当“ARP_IP 地址冲突”事件的源 IP 为 1.1.1.1，目的 IP 属于 10.0.0.1-20.0.0.1 时，响应方式启用：日志、报警，该事件的上报级别为中级事件。若此事件 IP 不满足第一条的配置，则启用 any<->any 的响应方式：日志、报警，该事件的上报级别为低危事件。如下图：

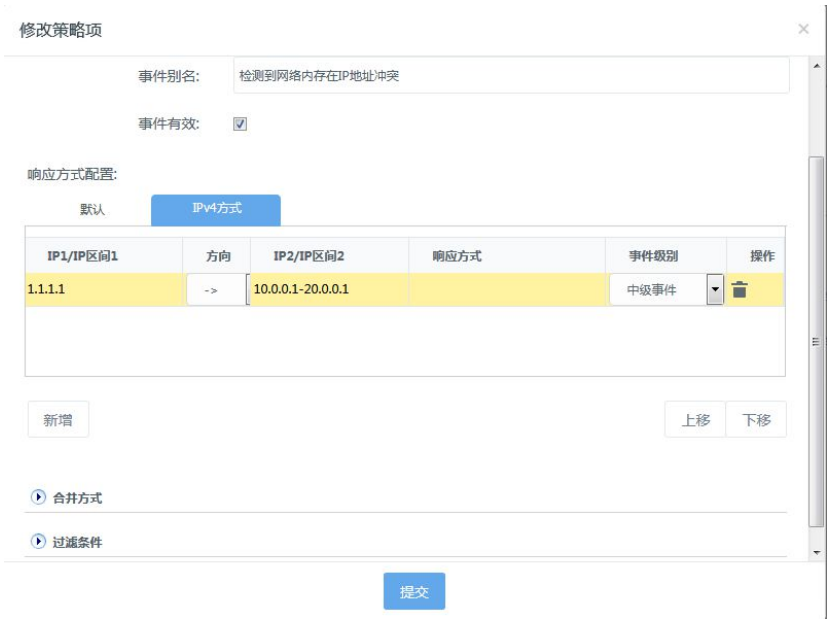

图 6-19 设置 IP/IP 区间展示

该功能支持 IP 的排序功能，排序在前的配置优先。同时，我们可以对所有条目移动进行上下移动，来调整匹配顺序。选中某个条目，然后点击**[上移]**、**[下移]**按钮，即可以提高相应条目的优先级别。

合并方式：

点击合并方式表头展开如下图所示页面：

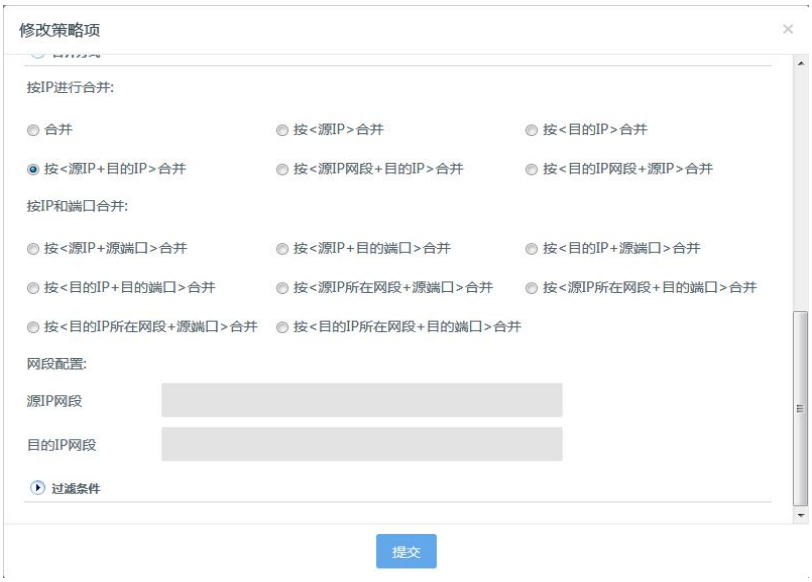

图 6-20 合并方式参数展示

合并方式包括：按 IP 进行合并和按 IP 和端口合并两种方式，如果选中按带有网段合并方式则在网段设置里面输入相应的网段，网段默认为：255.255.255.255。

过滤条件：

点击过滤条件表头展开如下图所示页面：

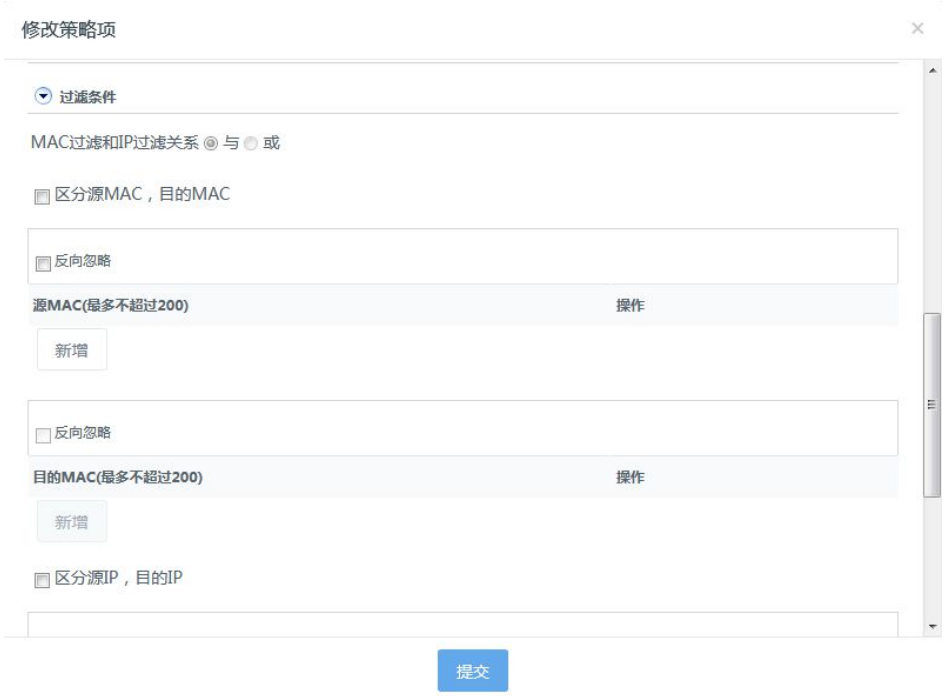

图 6-21 过滤条件展示

过滤条件包括： IP、MAC 以及它们之间的关系；IP 过滤条件和 MAC 过滤条件包括与，或两种逻辑关系。

MAC 过滤条件设置，点击**[新增]**按钮弹出添加 MAC 对话框如下图：

图 6-22 新增 MAC 地址展示

MAC 地址格式为：XX:XX:XX:XX:XX:XX，请正确填写，如不正确则提示“错误的 MAC 地址”，点击**[确定]**按钮，增加 MAC 地址，并返回到修改策略项对话框。

IP 过滤条件设置，点击**[新增]**按钮弹出新增 IP 对话框如下图：

图 6-23 新增 IP 地址展示

IP 格式分为：单 IP、IP 范围，这两种格式应该正确填写，如果填写不正确，则提示“错误的 IP 地址”点击**[确定]**按钮，增加 IP 地址，并返回到修改策略项对话框。

策略项修改完成后，点击**[提交]**按钮完成，返回策略项列表，刷新显示。

查看事件详细信息：

点击策略项列表中的**事件名称**，则显示当前事件的详细信息，例如点击“DNS_Authors 探测 ”，则显示下图所示详细信息。

图 6-24 详细事件信息展示

详细信息包括：事件名称，事件别名，事件说明，危险级别，事件类型，流行情况，漏洞发现时间，影响系统，影响设备，事件处理方法，影响的软件版本。点击**[关闭]**按钮

关闭事件详细信息对话框。

6.1.7 衍生策略集

功能介绍：从存在的策略集衍生一个新的策略集。

操作步骤：

进入策略集列表界面；

点击列表中的**[衍生]**按钮，随后弹出对话框，如下图所示：

图 6-25 策略集衍生页面展示

在对话框中输入名称和说明信息；

然后，点击**[提交]**按钮进行衍生，衍生完成返回策略集列表界面，或者点击**[取消]**按钮取消操作。

注意

策略集的名称不能为空字符 ,且不可以超过 50 个字符长度，说明内容可以为空，如果输入则不能超过 120 字符。策略集的名称不允许输入 `~!@#$%^&*+\\;'\/{}|:\"<>? 等特殊字符。

6.1.8 导出策略集

功能介绍：将当前策略集导出到本地指定位置。

操作步骤：

进入策略集列表界面；

点击列表中的**[导出]**按钮，随后弹出对话框，如下图：

图 6-26 导出策略集展示

选择要保存的本地路径后进行保存。

6.1.9 删除策略集

功能介绍：将当前策略集删除。

操作步骤：

进入策略集列表界面；

点击列表中的**[删除]**图标后弹出消息提示框，如下图：

图 6-27 删除策略集页面

点击**[确定]**按钮，删除策略集，返回策略集列表。

备注：系统策略集不能删除。

6.1.10 策略模板

策略模板提供了用户定制事件处理和响应方式的一种方法。用来调整策略集默认的处理方法和响应方式。策略模板列表如下图：

序号	名称	说明	最后修改时间	操作
1	单机存储		2016-08-31 17:24:33	
2	单机存储+报警		2016-08-31 17:24:33	
3	单机存储+日志+报警		2016-08-31 17:24:33	
4	邮件报警		2016-08-31 17:24:33	
5	SNMP		2016-08-31 17:24:33	
6	syslog		2016-08-31 17:24:33	

图 6-28 策略集模板列表

新建策略模板：

新建一个策略响应模板；点击**[新建]**按钮弹出“新建模板”对话框如下图：

图 6-29 新建策略模板展示

对话框中输入名称和说明信息，点击**[下一步]**按钮进入模板内容对话框如下：

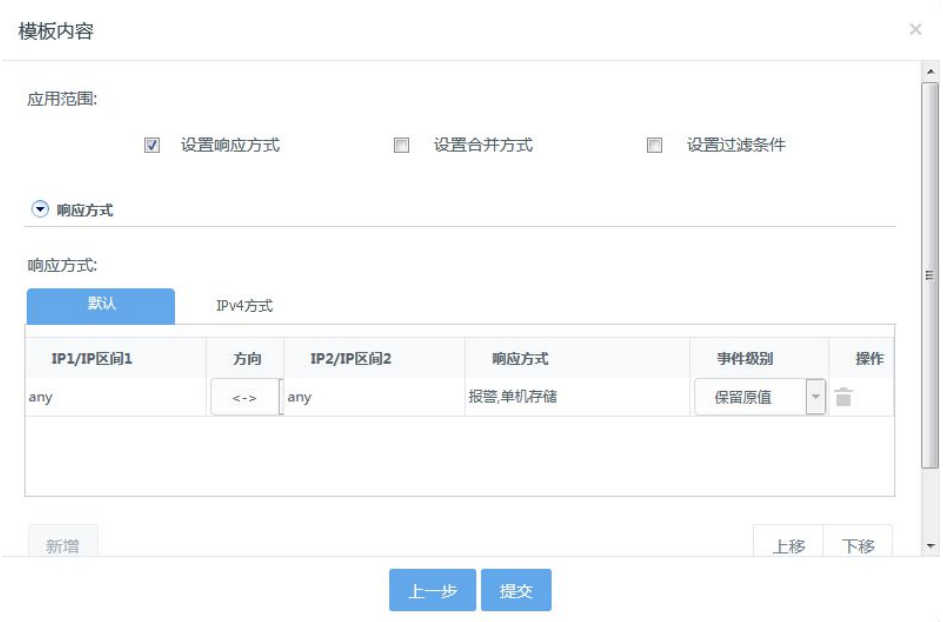

图 6-30 模板内容页面展示

编辑好模板内容，点击**[提交]**按钮添加策略模板，添加完成返回策略模板列表页面。

导入策略模板：

策略模板导入，可以将已备份的策略模板导入到现有系统。

点击**[导入]**按钮打开导入策略模板对话框如下图：

图 6-31 导入模板页面展示

选择要导入的文件，点击**[提交]**按钮，执行导入，导入成功跳转到策略模板列表页面。

导出策略模板：

将当前所有策略模板导出到本地指定位置。

点击列表中的**[导出]**图标，随后弹出文件下载对话框，如下图：

图 6-32 导出模板展示

选择你要保存的本地路径后进行保存。

删除策略模板：

删除现有的一条策略模板。

打开策略模板列表；

点击**[删除]**图标，弹出消息对话框，如下图：

图 6-33 删除模板页面

点击**[确定]**按钮，删除所选策略模板，返回策略集列表，否则点击 按钮取消操作。

编辑策略模板：

新建一个策略模板后，需要根据情况修改配置。

打开策略模板列表；

点击**[编辑]**按钮，弹出修改模板对话框，如下图：

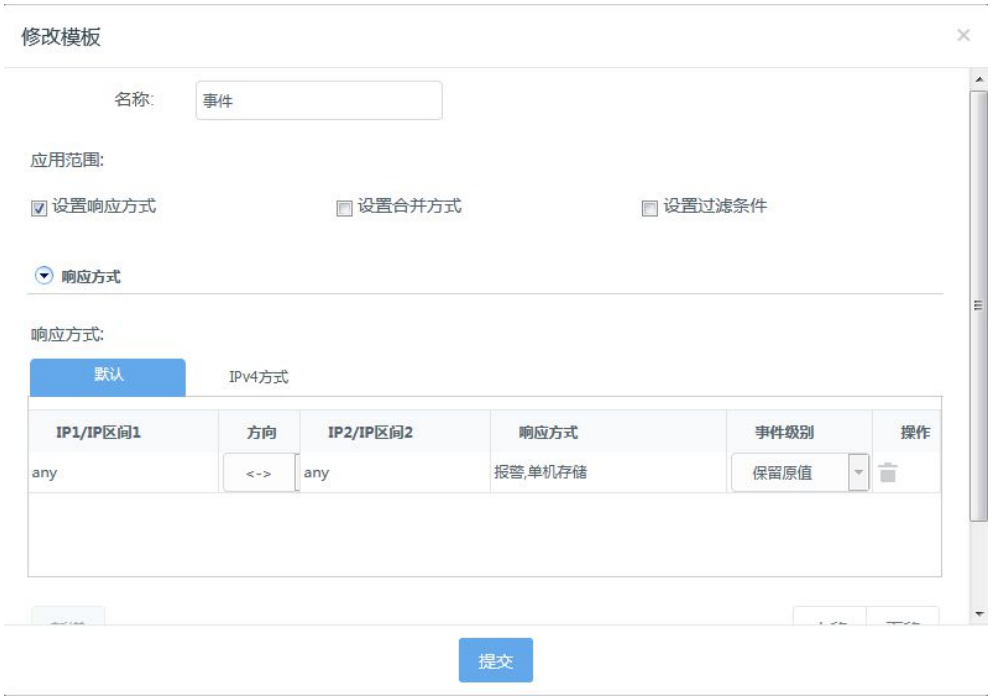

图 6-34 编辑策略模板页面展示

策略模板包括：应用范围、响应方式、合并方式、过滤条件；选择不同的应用范围出现相应的设置。

响应方式：

IP/IP 区间响应方式里面包括：日志、报警、单机存储、Syslog、SNMP、邮件报警选项等；

合并方式：

在应用范围中选择设置合并方式，展开如下图所示页面：

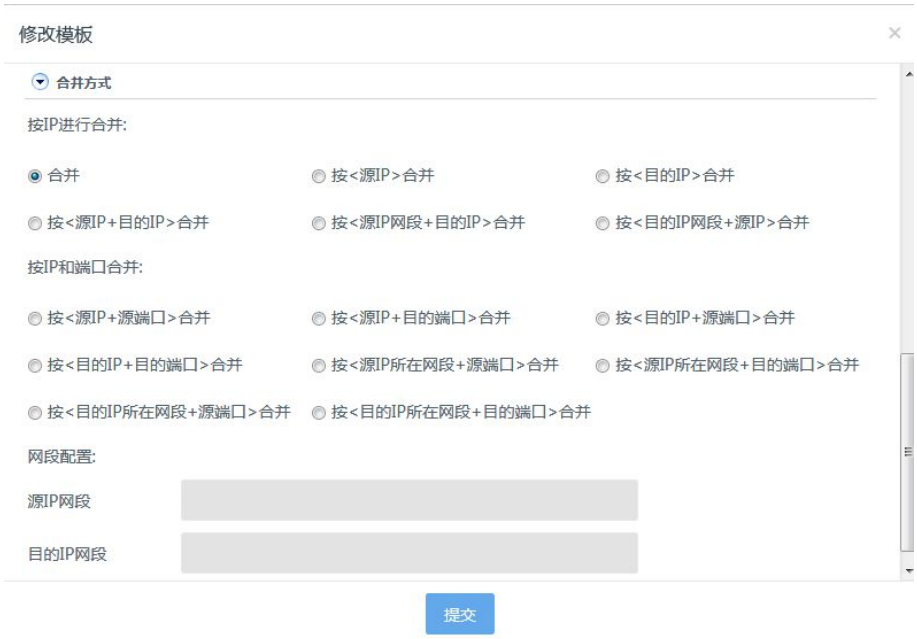

图 6-35 合并方式设置

合并方式包括：按 IP 进行合并和按 IP 和端口合并两种方式，如果选中按带有网段合并方式则在网段设置里面输入相应的网段，网段默认为：255.255.255.255。

过滤条件：

在应用范围中选择设置过滤条件，展开如下图所示页面：

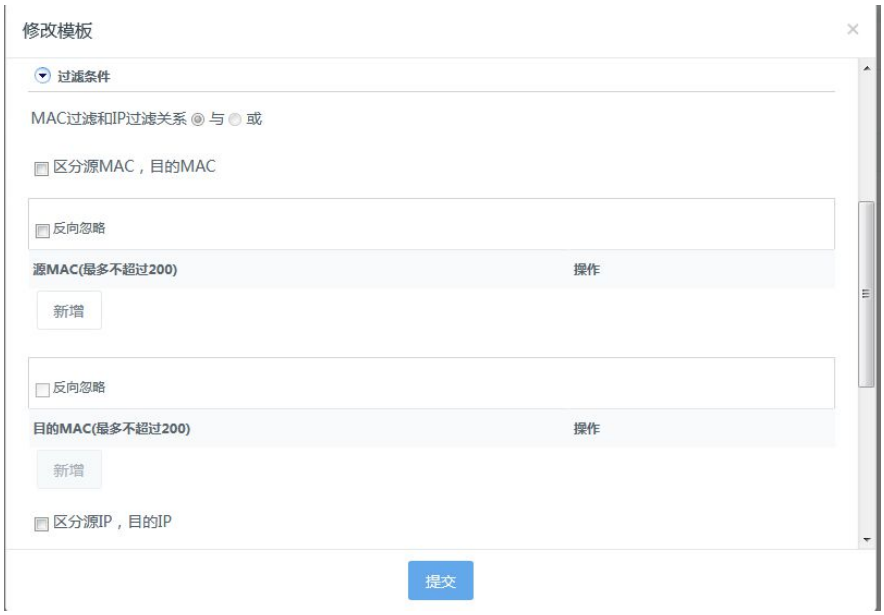

图 6-36 过滤条件设置

过滤条件包括： IP、MAC 以及它们之间的关系；IP 过滤条件和 MAC 过滤条件包括与，或。

MAC 过滤条件设置，点击**[新增]**按钮弹出添加 MAC 对话框如下图：

图 6-37 新增 MAC 地址页面展示

MAC 地址格式为：XX:XX:XX:XX:XX:XX，请正确填写，如不正确则提示“错误的 MAC 地址”，点击**[确定]**按钮，增加 MAC 地址，返回编辑策略项对话框。

IP 过滤条件设置，点击**[新增]**按钮弹出新增 IP 对话框如下图：

图 6-38 新增 IP 地址页面展示

IP 格式分为：单 IP、IP 范围；这两种格式应该正确填写，如果填写不正确，则提示“错误的 IP 地址”点击**[确定]**，增加 IP 地址，返回编辑策略项对话框。

策略模板修改完成后，点击**[确定]**完成，返回策略模板列表。

6.1.11 特征事件自定义

特征事件自定义是向用户提供一种自定义事件的功能，特征事件就是指网络流量中存在着可匹配规则的一类事件，通过匹配这些特征，我们可以分析出具有某些攻击的行为。特征事件是现今主流入侵检测所采用的一种成熟的模式匹配技术，这种检测技术以协议分析为核心，在协议分析的基础上采用模式匹配的方法对网络流量进行特征过滤。

检测配置>特征检测配置>特征事件进入特征事件自定义页面，如下图：

图 6-39 事件特征列表展示

新建基础特征事件：

点击**[新建]**按钮在新窗口中打开新增事件窗口，添加一条特征事件。如下图：

配置步骤：

图 6-40 新建特征事件页面展示

参数说明：

事件名称：事件的名称，名称必须以所属的协议开头，该项不能为空；

事件别名：便于记忆的事件别称；

事件说明：事件的相关说明，说明长度不能大于 120 个字节，该项可以为空；

危险级别：事件所属的级别，有四种级别可供选择：非攻击事件、低级事件、中级事件和高级事件，默认为非攻击事件；

协议类型：事件所属的协议类型；

安全类型：事件所属的安全类型；

影响系统：事件影响的关键系统；

影响设备：事件影响的关键设备；

流行程度：事件的流行情况；

是否源/目的 IP 反向：设置是否将事件的源 IP 与目的 IP 进行交换；

特征定义：事件的特征定义字符串，建议通过**特征定义向导**进行定义，并可使用“语法检查”进行校验。该项不能为空；

返回参数定义：事件的返回参数定义字符串，建议通过**返回参数向导**进行定义，并可使用“语法检查”进行校验。返回参数字符串须小于 128 个字符，该项可以为空；

定义策略集：选择特征事件对应的响应方式，添加到用户自定义的策略集中，在新增特征事件时，可以暂时不指定所属的策略集，之后可在**特征检测配置>策略集**中进行添加，修改。

配置案例

我们想监控网段内所有访问 www.sina.com.cn 网站的用户，并且要对该用户是否访问了文件名为 index.php 的行为进行监控。

点击**[新建]**按钮在新窗口中打开新增事件窗口；

输入事件名称：名称应该清晰地表达出事件的含义，这样定义出来的事件一目了然、清晰易懂，也易于管理。因此这里我们输入“HTTP_selfdefine_001”；

输入事件别名：这里我们输入便于以后查找的名称，“新浪访问监控”；

输入事件说明：我们可以根据自己的需要输入适当的事件描述说明，这里我们输入“特征事件定义演示”；

选择事件所属的事件级别：此处我们可以根据自己的需要做合适的选择，不妨暂时选为“高级事件”；

选择事件所属的协议类型，因为要监控网段内所有访问 www.sina.com.cn 网站的用户，所以在协议类型之中选择“HTTP”；

选择事件所属的安全类型：由于我们属于对网段内的流量进行监控审计行为，所以安全类型较为合理的选择是“安全审计”；

选择影响系统：结合实际情况选择，这里选择“MySQL”；

选择影响设备：结合实际情况选择，这里选择“多种网络设备”；

选择流行程度：结合实际情况选择，这里选择“流行”；

源/目的 IP 反向：否。

图 6-41 自定义事件特征演示

事件特征定义：建议通过“特征定义向导”进行定义。点击**[特征定义向导]**链接，在新窗口中打开特征定义向导窗口：如下图：

图 6-42 事件特征定义向导演示

由于要监控的网站是 www.sina.com.cn，所以在左侧的协议变量目录树中选择“http_host”，在右侧的详细信息中，选择操作符为“^ - 包含”，在数据值中输入”www.sina.com.cn”。如下图：

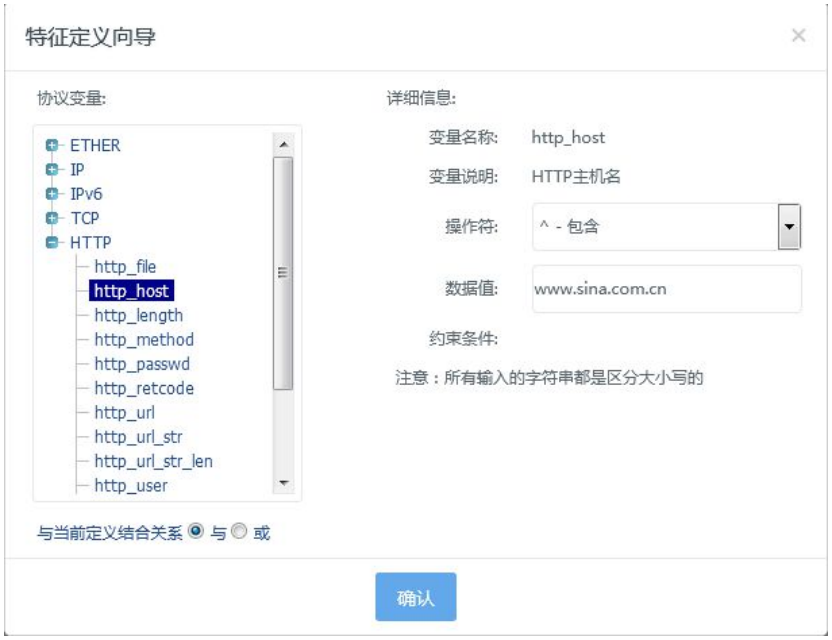

图 6-43 事件特征定义演示

完成后点击**[确认]**按钮，在特征定义输入框中将生成对应的特征定义字符串“http_host^www.sina.com.cn”。如下图：

图 6-44 新建事件特征演示

再点击**[特征定义向导]**链接，进行另一条特征定义。由于监控访问的文件名称为index.php，所以在左侧的协议变量目录树中选择“http_url”，在右侧的详细信息中，选择操作符为“^ - 包含”，在数据值中输入“index.php”。在点击**[确认]**按钮之前，需要确定这两条特征定义的结合关系，这里我们使用“与”的关系。如下图：

图 6-45 自定义特征演示

点击**[确认]**按钮后，在特征定义输入框中将生成对应的特征定义字符串“http_host^www.sina.com.cn&http_url^index.php”。如下图：

图 6-46 自定义特征演示

为了检查特征定义字符串的正确性，可以使用特征定义的语法检查功能。点击**[语法检查]**按钮，将弹出新窗口提示检查的结果。

如果特征定义字符串通过语法检查，将提示：如下图：

图 6-47 语法检查页面

如果特征定义字符串没通过语法检查，将根据错误的不同提示相应的错误信息。

返回参数定义：建议通过“返回参数向导”进行定义。点击**[返回参数向导]**链接，在新窗口中打开返回参数向导窗口。如下图：

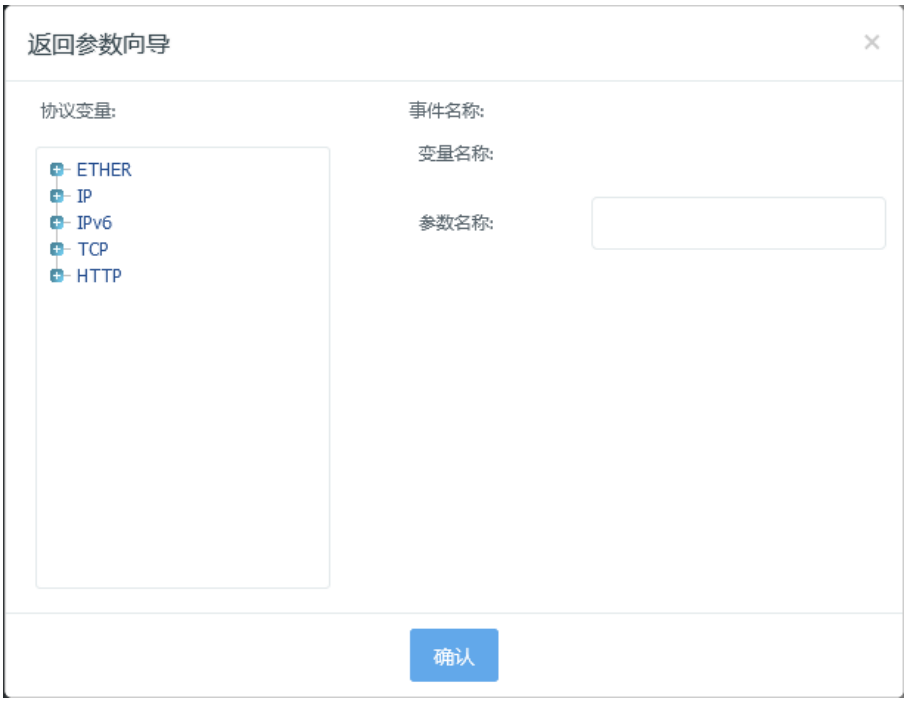

图 6-48 返回参数导向页面

由于我们需要把检测出来的 http_url 作为返回的变量，所以在左侧的协议变量目录树中选择“http_url”，在右侧的详细信息中，在返回提示符中输入“URL”。如下图：

图 6-49 自定义事件特征演示

点击**[确认]**按钮后，在返回参数定义输入框中将生成对应的返回参数定义字符串“URL=http_url”。如下图：

图 6-50 自定义事件特征演示

为了检查返回参数定义字符串的正确性，可以使用返回参数定义的语法检查功能。点击**[语法检查]**按钮，将弹出新窗口提示检查的结果。

如果返回参数定义字符串通过语法检查，将提示：如下图：

图 6-51 语法查询页面

如果返回参数定义字符串没通过语法检查，将根据错误的不同提示相应的错误信息。

选择策略集：点击**[定义策略集]**链接，出现如下对话框，可选择特征事件对应的响应方式，所属的自定义策略集。如下图：

图 6-52 响应方式设置页面

当特征事件的各项信息都按照需要输入后，可以点击**[提交]**按钮完成新增。

如果事件的各项信息均按要求输入、验证无误，则可在事件列表中看到刚才新增的事件。如下图：

图 6-53 成功新建事件特征页面展示

如果检查到当前某项信息输入不正确时，将会出现错误提示，不允许新增，直到用户按要求输入对应信息后，才能完成新增。

编辑特征事件定义：

点击**[编辑]**图标在新窗口中打开编辑事件窗口，编辑一条已有的特征事件。如下图：

配置步骤：

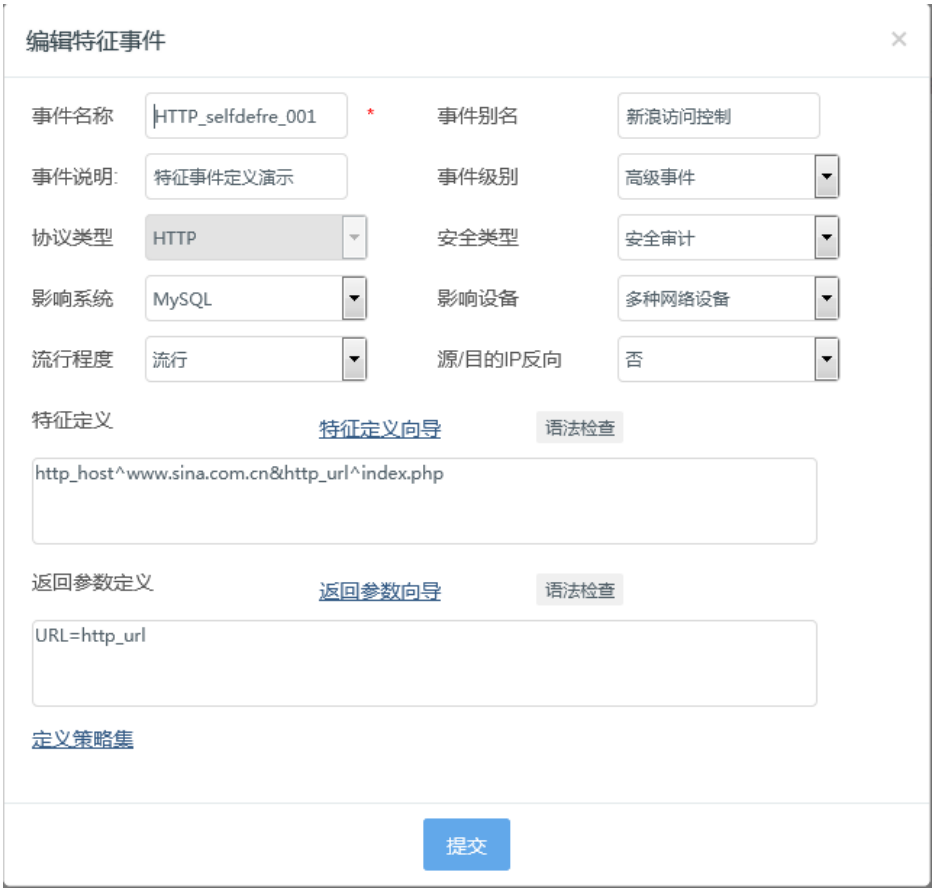

图 6-54 编辑事件特征页面

参数说明：

事件名称：事件的名称，名称必须以所属的协议开头，该项不能为空；

事件别名：便于记忆的事件别称；

事件说明：事件的相关说明，说明长度不能大于 120 个字节，该项可以为空；

危险级别：事件所属的级别，有四种级别可供选择：连接事件、低级事件、中级事件和高级事件，默认为连接事件；

协议类型：事件所属的协议类型；

安全类型：事件所属的安全类型；

影响系统：事件影响的关键系统；

影响设备：事件影响的关键设备；

流行程度：事件的流行情况；

是否源/目的 IP 反向：设置是否将事件的源 IP 与目的 IP 进行交换。

特征定义：事件的特征定义字符串，建议通过“特征定义帮助”进行定义，并可使用“语法检查”进行校验。该项不能为空。

返回参数定义：事件的返回参数定义字符串，建议通过“返回参数帮助”进行定义，并可使用“语法检查”进行校验。返回参数字符串须小于 128 个字符，该项可以为空。

定义策略集：选择特征事件对应的响应方式，添加到用户自定义的策略集中，在新增特征事件时，可以暂时不指定所属的策略集，之后可在**特征检测配置>策略集**中进行添加，修改。

删除特征事件定义：

点击**[删除]**图标弹出新窗口询问是否删除当前的自定义事件。如下图：

配置步骤：

图 6-55 删除事件特征页面

事件定义文件导出：

点击**[导出]**按钮弹出新窗口询问打开或保存事件定义文件。如下图：

配置步骤：

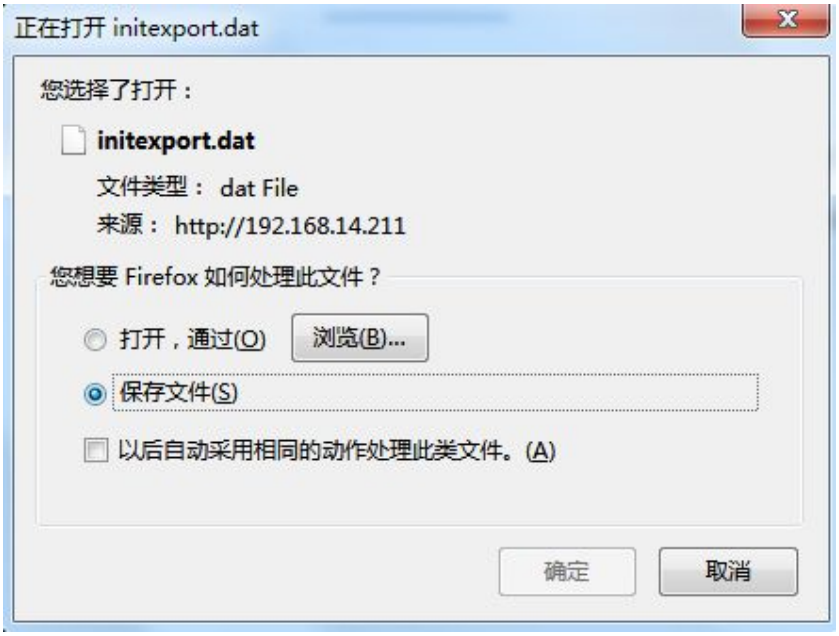

图 6-56 导出事件特征展示

选择本地目录进行保存。

事件定义文件导入：

配置步骤：

点击**[导入]**按钮弹出新窗口事件定义文件导入窗口。如下图：

图 6-57 导入事件特征展示

点击**[选择文件]**按钮弹出新窗口选择要导入的事件定义文件，按**[提交]**按钮进行导入。

如果选择的不是 dat 类型事件定义文件，则显示：如下图：

图 6-58 导入事件特征文件提示页面

导入成功后，导入的特征事件定义将显示在事件列表中：如下图：

图 6-59 导入事件成功列表展示

6.1.12 二次事件自定义

与特征事件不同，二次事件的检测基础不是特征匹配，而是对事件发生次数的统计，因为网络中存在着很多难以找到其特征的攻击与探测行为，在无法提取特征的情况下进行入侵防御，这在基于误用的入侵检测系统之中几乎是不可能的。概括来说，二次事件就是在特征事件的基础上引入统计函数 num()，在受控的时间段内判断是否做出响应的机制。与特征事件相似，二次事件也可以由用户来自定义。如下图：

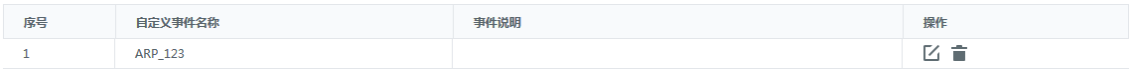

图 6-60 二次事件自定义页面

新建二次事件定义：

点击**[新建]**按钮在新窗口中打开新建二次事件窗口，添加一条二次事件。如下图：

配置步骤：

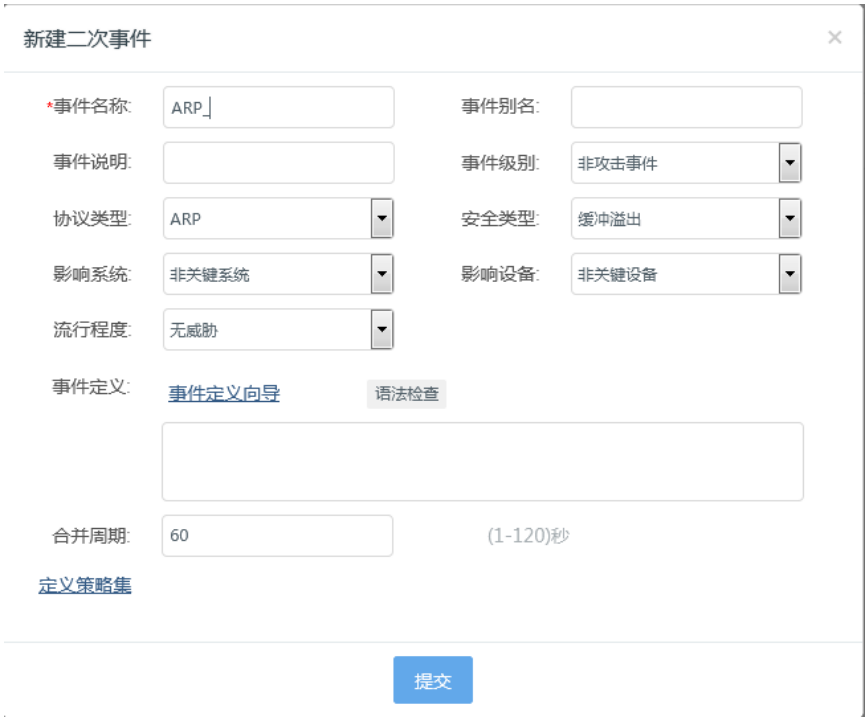

图 6-61 二次事件自定义演示

参数说明：

事件名称：事件的名称，名称必须以所属的协议开头。该项不能为空；

事件别名：便于记忆的事件别称；

事件说明：事件的相关说明，说明的长度不能大于 120 个字节，该项可以为空；

事件级别：事件所属的级别，有四种级别可供选择：非攻击事件、低级事件、中级事件和高级事件，默认为非攻击事件；

协议类型：事件所属的协议类型；

安全类型：事件所属的安全类型；

影响系统：事件影响的关键系统；

影响设备：事件影响的关键设备；

流行程度：事件的流行情况；

事件定义：事件定义字符串，建议通过**事件定义向导**进行定义，并可使用**语法检查**进行校验。该项不能为空；

合并周期：定义二次事件的合并周期阈值；

定义策略集：选择二次事件对应的响应方式，添加到用户自定义的策略集中，在新建二次事件时，可以暂时不指定所属的策略集，之后可在**特征检测配置>策略集**中进行添加，修改。

配置案例：

我们想监控网络内可视的所有主机对所要保护的目的主机 192.168.1.187，在受控的时间段，累计发生“ICMP_PING_事件”的次数。这里我们将次数阈值设置为 10。

点击**[新建]**按钮在新窗口中打开新建二次事件窗口。

输入事件名称：名称应该清晰地表达出事件的含义，这样定义出来的事件一目了然、清晰易懂，也易于管理。因此这里我们输入“ICMP_selfdefine_001”；

输入事件别名：这里我们输入便于以后查找的名称，“ICMP_PING_事件监控”；

输入事件说明：我们可以根据自己的需要输入适当的事件描述说明，这里我们输入“二次事件定义演示”；

选择事件所属的事件级别：此处我们可以根据自己的需要做合适的选择，暂时选为“中级事件”；

选择事件所属的协议类型：因为要监控所基于的特征事件是“ICMP_PING_事件”，所以在协议类型之中选择“ICMP”；

选择事件所属的安全类型：由于网络内过分频繁“ICMP_PING_事件”将产生 DDoS Ping 攻击，所以安全类型选择为“分布式拒绝服务”；

选择影响系统：结合实际情况选择，这里选择“Web 服务器”；

选择影响设备：结合实际情况选择，这里选择“UNIX OS”；

选择流行程度：结合实际情况选择，这里选择“流行”；

合并周期：阈值 60 秒。

如下图：

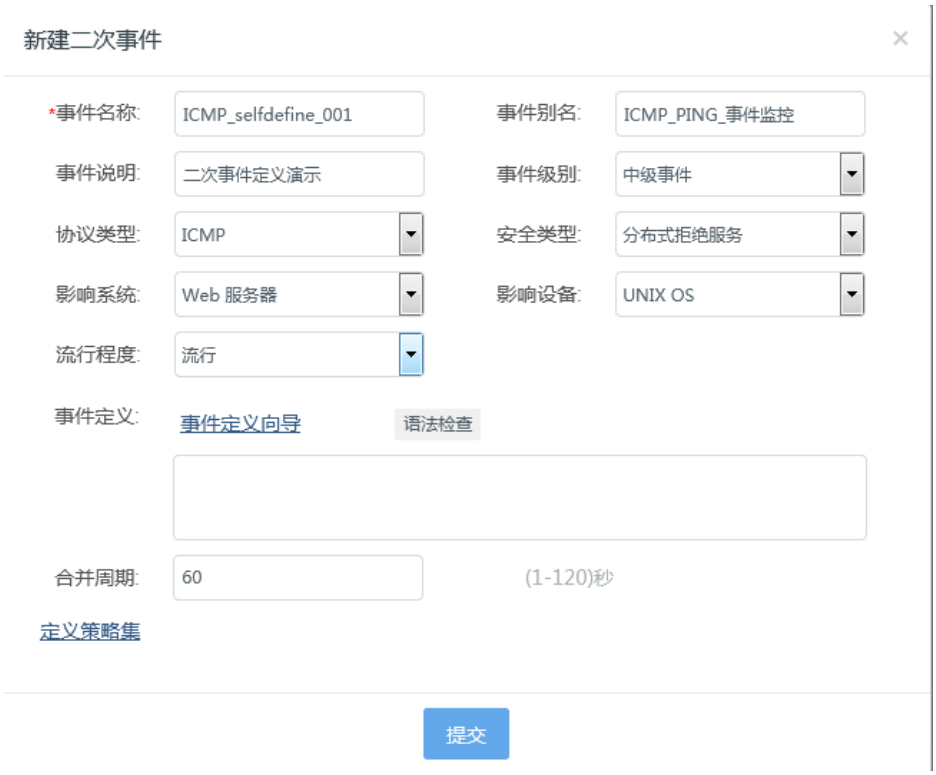

图 6-62 自定义二次事件特征演示

事件定义：建议通过“事件定义向导”进行定义。点击**[事件定义向导]**链接，在新窗口中打开事件定义向导窗口。如下图：

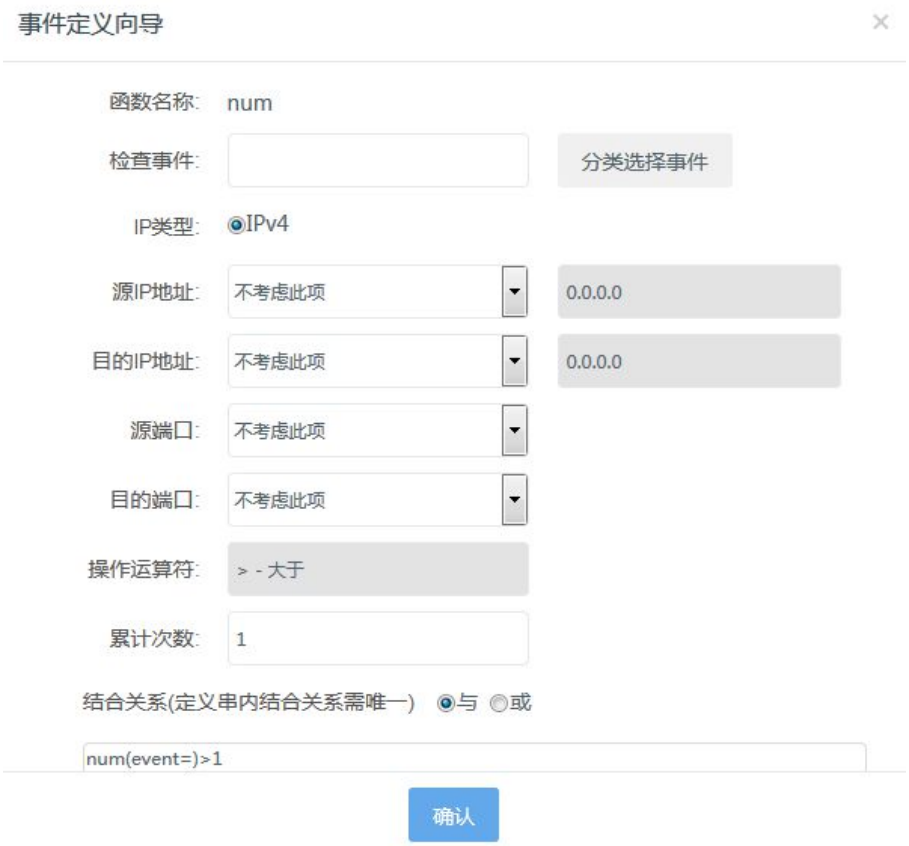

图 6-63 事件定义向导设置页面

参数说明：

检查事件：该二次事件所基于的特征事件，通过**分类选择事件**进行选择，不允许用户手工输入。

IP 类型：依照需求以及事件发生的场景，进行 IPv4 或 IPv6 的选择。

源 IP 地址：所要监控的源主机 IP 地址，下拉列表框中有四个选项：“指定 IP”、“各次均相同”、”各次均不同”、“不考虑此项”，默认为“不考虑此项”。当选择“指定 IP”时，可在后面的输入框中输入指定的 IP 地址。

目的 IP 地址：所要保护的目的主机 IP 地址，下拉列表框中有四个选项：“指定 IP”、“各次均相同”、“各次均不同”、“不考虑此项”，默认为“不考虑此项”。当选择“指定 IP”时，可在后面的输入框中输入指定的 IP 地址。

源端口：所要监控的源主机端口，下拉列表框中有三个选项：“各次均相同”、“各次均不同”、“不考虑此项”，默认为“不考虑此项”。

目的端口：所要保护的目的主机端口，下拉列表框中有三个选项：“各次均相同”、“各次均不同”、“不考虑此项”，默认为“不考虑此项”。

操作运算符：事件统计次数与累计次数阈值的比较关系，默认为“> - 大于”，不能修改，只能为此值。

累计次数：监控所基于的特征事件在事件合并周期内的统计次数，这个阈值是二次事件最主要的一项参数，阈值的设定是根据用户的需求所不同的。

选择基于的特征事件，分类选择事件，在新窗口中打开事件选择窗口。窗口的顶部是协议类型的下拉选择框，事件名称列表显示了相应协议类型下的所有特征事件。我们所要选择的特征事件是“ICMP_PING_事件”，因此在协议类型下拉选择框中选择“ICMP”，之后在右侧列表中选择“ICMP_PING_事件”。如下图：

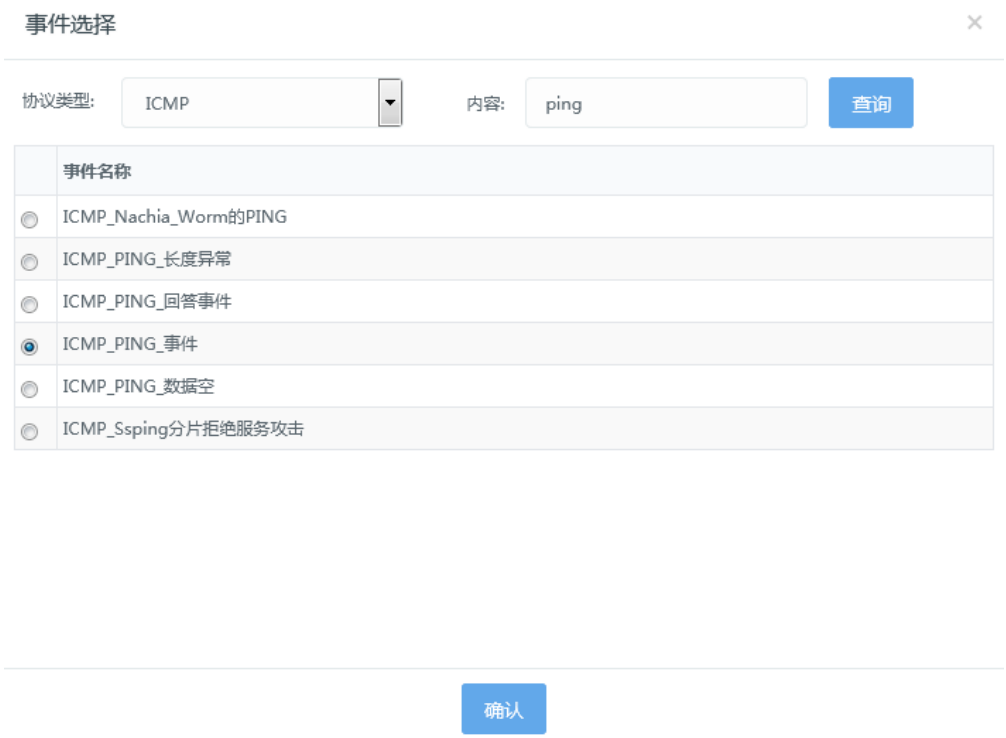

图 6-64 事件选择设置页面

点击**[确定]**按钮完成特征事件选择，在事件定义向导的检查事件输入框中将出现“ICMP_PING_事件”。如下图：

图 6-65 事件定义设置页面

完成事件定义帮助窗口中余下参数的设置。

源 IP 地址使用默认选项“不考虑此项”。

我们所要保护的目的主机为 192.168.1.187，因此对目的 IP 地址选择“指定 IP”，在后面的输入框中填入”192.168.1.187”。

源端口使用默认选项“不考虑此项”。

目的端口使用默认选项“不考虑此项”。

操作运算符默认“> - 大于”。

累计计数的设定是根据用户的需求所不同，这里我们暂时定义为 10，之后可根据使用的效果再做调整。

如果之前已经定义了其他的事件定义单元，则还需要确定与之前定义的结合关系，可选择“与”或者“或”。如下图：

图 6-66 事件定义设置演示

完成事件定义向导的参数设置后，点击**[确定]**按钮，在事件定义输入框中将生成对应的事件定义字符串“num(event=ICMP_PING_事件,dip=192.168.1.187)>10”。如下图：

图 6-67 自定义二次事件演示

为了检查事件定义字符串的正确性，可以使用事件定义的语法检查功能。点击**[语法检查]**按钮，将弹出新窗口提示检查的结果。

如果特征定义字符串通过语法检查，将提示：

图 6-68 语法检查页面

如果事件定义字符串没通过语法检查，将根据错误的不同提示相应的错误信息。

合并周期用来控制在对应时间内累计发生次数达到配置的阈值上报一次该二次事件，时间阈值范围 1-120s。

选择策略集：点击**[选择策略集]**链接，出现如下对话框，可选择特征事件对应的响应

方式，所属的自定义策略集。如下图：

图 6-69 设置策略集展示

当二次事件的各项信息都按照需要输入后，可以点击**[提交]**按钮完成新建。

如果事件的各项信息均按要求输入、验证无误，则可在事件列表中看到刚才新建的事件。如下图：

图 6-70 成功新建二次事件列表展示

如果检查到当前某项信息输入不正确时，将会出现错误提示，不允许新增，直到用户按要求输入对应信息后，才能完成新增。

编辑二次事件定义：

点击**[编辑]**图标在新窗口中打开编辑事件窗口，编辑一条已有的二次事件。如下图：

配置步骤：

图 6-71 编辑二次事件页面

参数说明：

事件名称：事件的名称，名称必须以所属的协议开头。该项不能为空；

事件别名：便于记忆的事件别称；

事件说明：事件的相关说明，说明的长度不能大于 120 个字节，该项可以为空；

事件级别：事件所属的级别，有四种级别可供选择：非攻击事件、低级事件、中级事件和高级事件，默认为非攻击事件；

协议类型：事件所属的协议类型；

安全类型：事件所属的安全类型；

影响系统：事件影响的关键系统；

影响设备：事件影响的关键设备；

流行程度：事件的流行情况；

事件定义：事件定义字符串，建议通过“事件定义向导”进行定义，并可使用“语法检查”进行校验。该项不能为空。

删除二次事件定义：

点击**[删除]**图标弹出新窗口询问是否删除当前的二次事件。如下图：

配置步骤：

图 6-72 删除二次事件页面

事件定义文件导出：

点击**[导出]**按钮弹出新窗口询问打开或保存事件定义文件。如下图：

配置步骤：

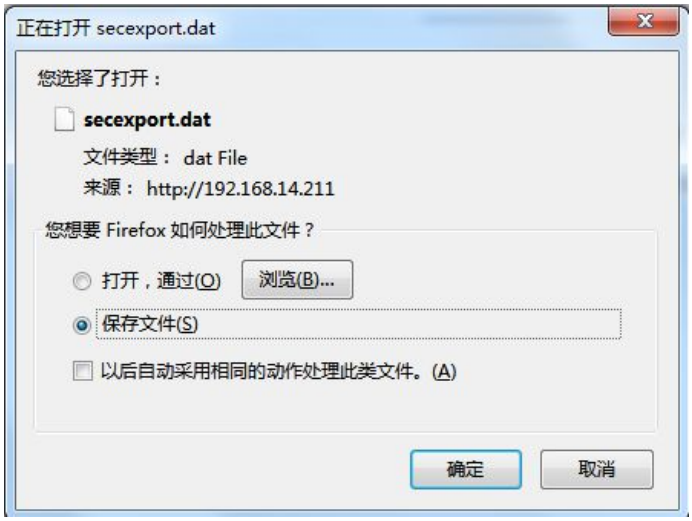

图 6-73 导出特征文件展示

选择本地目录进行保存。

事件定义文件导入：

配置步骤：

点击**[导入]**按钮弹出新窗口事件定义文件导入窗口。如下图：

图 6-74 导入二次事件特征文件展示

点击**[选择文件]**按钮弹出新窗口选择要导入的事件定义文件，按**[提交]**按钮进行导入。

如果选择的不是事件定义文件，则显示：

图 6-75 导入事件文件错误提示页面

导入成功后，导入的特征事件定义将显示在事件列表中：

注意

二次事件添加成功后，会自动在“重点关注”模块中被分配到“需要关注”类型。

6.1.13 拒绝服务与扫描类

对于拒绝服务与扫描类事件，由于其海量性，需要设定阈值，减少误报。进入**特征检测配置>拒绝服务与扫描类**，即可看到拒绝服务与扫描类事件阈值设定的界面，如下图：

图 6-76 拒绝服务与扫描类信息展示

该模块是和事件库相关的，如果事件库中没有拒绝服务与扫描类的事件，那么该模块，将不会显示任何事件。

该模块可以进行的操作只有编辑，点击某条事件后面的**[编辑]**按钮，进入编辑事件阈值的界面。以 SCAN_SYNONLY_TCP 端口扫描事件为例，事件阈值编辑界面如下图：

图 6-77 事件编辑页面

输入时间和阈值的数值，选择时间的单位，点击**[确定]**按钮完成事件阈值的编辑操作。如下图：

事件名称	事件类型	事件(秒)	数量	操作
SCAN_ICMP扫描探测	scan	1	10	
SCAN_UDP端口扫描	scan	1	20	
SCAN_SYNONLY_TCP端口扫描	scan	1	4096	
DOS_TCP_FLOOD_拒绝服务[STREAM]	flood	1	2048	
DOS_TCP_FLOOD_拒绝服务[HALFSESSION]	flood	1	4096	
DOS_TCP_FLOOD_拒绝服务[SYNRST]	flood	1	4096	
DOS_SYN_FLOOD_拒绝服务[SYNONLY]	flood	1	4096	
DOS_UDP_FLOOD_拒绝服务	flood	1	4096	
DOS_ICMP_FLOOD_拒绝服务	flood	1	4096	

数据表中共为 9 条记录

图 6-78 成功新建事件列表展示

每条事件都有其默认的配置，时间和阈值都是可以编辑的。时间单位有四个：秒、分、时、日。可以任意选择所需的时间单位，如下图选择的时间单位是分，配置的阈值是 100。如下图：

图 6-79 编辑事件页面展示

提交后，时间一项会自动转化为以秒为单位的时间，如下图：

图 6-80 编辑事件页面展示

点击**[编辑]**按钮，界面上的时间会显示为以秒为单位：

图 6-81 时间单位显示页面

如果选择时间的单位为时、日，提交之后，时间也同样会转化为以秒为单位，提交后再点编辑，时间单位也变换为秒。

备注：该模块的事件的条数与事件库相关，如果事件库中删除了某条拒绝服务与扫描事件，这里同样会删除。

6.1.14 弱口令配置

弱口令配置模块，主要针对一些简单数字和字母的口令，例如“123”、“abc”等，在用户访问服务器的时候进行检测，并上报检测结果。

进入弱口令配置界面，根据用户需求，可以选择相应的配置项。如下图：

图 6-82 弱口令配置参数页面

点击**[提交]**按钮，弹窗“选择引擎”，在列表中勾选要下发配置的引擎，如下图：

图 6-83 选择引擎页面

点击**[确定]**，提示“配置弱口令成功”。

图 6-84 配置成功提示

注意

弱口令配置通过 web 页面下发到不同引擎，因此页面上不回显配置状态，页面默认展示为下图：

图 6-85 弱口令配置页面

6.1.15 事件合并

事件合并可以配置引擎事件的合并周期和最多合并次数。

进入**特征检测配置>事件合并**菜单。如下图：

图 6-86 事件合并页面

合并周期：配置事件合并的周期，以秒为单位，范围是 0-120 秒，0 表示不合并，引擎默认的合并周期是 60 秒；

最多合并次数：配置事件合并的最多合并次数，范围是 0-1000 次，0 表示不限制最多合并次数，引擎默认的最多合并次数是 255。

合并周期和最多合并次数是可以配置的，输入正确的合并周期和最多合并次数后，点

击**[提交]**按钮，完成事件合并的配置。如下图：

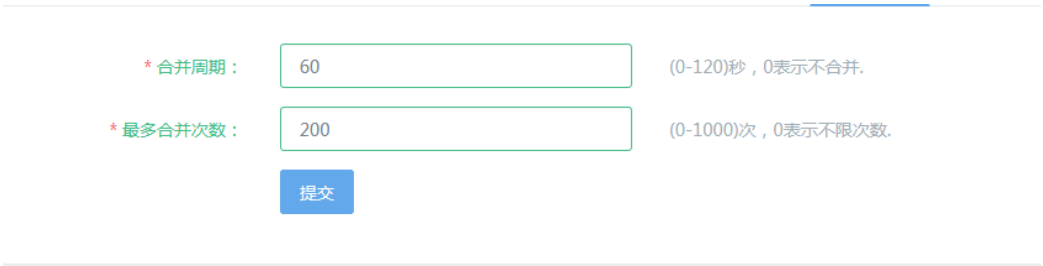

图 6-87 合并周期页面

点击**[提交]**按钮，弹窗“选择引擎”，在列表中勾选要下发配置的引擎，如下图：

图 6-88 选择引擎页面

点击**[确定]按钮**，会弹出成功的提示：

图 6-89 保存成功提示

注意

事件合并配置通过 web 页面下发到不同引擎，因此页面上不回显配置状态，页面默认展示为下图：

图 6-90 合并周期页面

6.2 资产配置

6.2.1 重点Web服务器

SQL 注入利用的是正常的 HTTP 服务端口，表面上看来和正常的 web 访问没有区别，隐蔽性极强，不易被发现；XSS 属于被动式的攻击。攻击者先构造一个跨站页面，利用 script 等各种方式使得用户浏览这个页面时，触发对被攻击站点的 http 请求。对用户具有很大的危害，该版本增加了重点 Web 服务器模块，该类事件可以进行准确及时的检测上报。

进入资产配置下的重点 Web 服务器三级菜单。如下图：

图 6-91 重点 Web 服务器页面

点击**[新建]**按钮，进入“新建重点 Web 服务器”界面，如下图所示。

图 6-92 新建重点 Web 服务器设置

参数说明：

服务器 IP：重点防护的服务器的 IP 地址；

服务器说明：对所要防护的服务器根据实际情况添加相应的说明信息；

服务器数据库类型：针对 HTTP_SQL 注入攻击具体防护的数据库类型进行选择，可以进行单选和多选；

XSS 防护：是否启用 XSS 防护功能。

根据实际情况填写完相应字段，如下图所示。

图 6-93 新建重点 Web 服务器演示

该配置指我们重点防护的是 IP 地址为 192.168.10.30 发生的 mssql 和 oracleHTTP_SQL 注入攻击，并启用了该 IP 地址的 XSS 防护。

点击**[确定]**按钮后，相应的配置就在“重点 Web 服务器”列表中显示，如下图所示。

图 6-94 新建重点 Web 服务器演示

配置完成后，勾选相应要防护的服务器，点击**[下发]**按钮，弹窗“选择引擎”，在列表中勾选要下发配置的引擎，如下图：

图 6-95 选择引擎页面

点击**[确定]**按钮，相应的配置就下发到了引擎，弹出成功提示对话框（回显信息速度较慢）。如下图：

图 6-96 引擎下发成功提示

点击**[编辑]**按钮，可以对已经配置的 Web 服务器进行修改，此处服务器 IP 地址是不允许修改的。如下图：

图 6-97 修改重点 Web 服务器配置页面

点击**[删除]**按钮，可以对配置条目进行删除操作，弹出询问框。如下图：

图 6-98 删除 Web 配置项页面提示

点击**[确定]**按钮，该服务器 IP 进行的 Web 服务器就被删除了。

该模块有几点需要注意的地方：

当未进行任何配置，直接点击**[下发]**按钮：

此种方法我们防护的是所有 IP 地址发生的 HTTP_SQL 注入攻击、HTTP_XSS 防护和 HTTP_XSS 脚本注入，任何 IP 发生的这三种事件都会被检测到并进行上报。

当进行了如下配置后，并且将这两个配置都进行勾选并下发到引擎后。如下图：

图 6-99 Web 服务器设置演示

此种方法，我们只重点防护 IP 为 192.168.10.30 发生的数据库类型为 mssql 的 oracle 注入攻击，重点防护 IP 为 192.168.10.50 发生的 HTTP_XSS 防护和 HTTP_XSS 脚本注入；所以相应我们只进行检测和上报的事件是 192.168.10.30 发生的数据库类型为 mssql 的 oracle 注入攻击、192.168.10.50 发生的 HTTP_XSS 防护和 HTTP_XSS 脚本注入；其他 IP 发生的这三种事件是不进行防护和上报的。

当进行了如下配置后，并且将这两个配置都进行勾选并下发到引擎后。如下图：

图 6-100 Web 服务器设置演示

此种方法，我们只重点防护 IP 为 192.168.10.50 发生的 HTTP_XSS 防护和 HTTP_XSS 脚本注入；所以相应我们只进行检测和上报的事件是 192.168.10.50 发生的 HTTP_XSS 防护和 HTTP_XSS 脚本注入；其他 IP 发生的 HTTP_XSS 防护和 HTTP_XSS 脚本注入事件是不进行防护和上报的。但是任何 IP 发生的 HTTP_SQL 注入攻击都是进行防护和上报的。

当进行了如下配置后，并且将这两个配置都进行勾选并下发到引擎后。如下图：

图 6-101 Web 服务器设置演示

此种方法，我们只重点防护 IP 为 192.168.10.30 发生的数据库类型为 mssql 或 mysql 的 HTTP_SQL 注入攻击，所以相应我们只进行检测和上报的事件是 192.168.10.30 发生的 HTTP_SQL 注入攻击；其他 IP 发生的 HTTP_SQL 注入攻击事件是不进行防护和上报的。但是任何 IP 发生的 HTTP_XSS 防护和 HTTP_XSS 脚本注入事件都是进行防护和上报的。

当进行了如下配置后，并且将这两个配置都进行勾选并下发到引擎后。如下图：

图 6-102 Web 服务器设置演示

此种配置和第一种未进行任何配置，直接点击**[下发]**按钮效果是一样的，防护的是所有 IP 地址发生的 HTTP_SQL 注入攻击、HTTP_XSS 防护和 HTTP_XSS 脚本注入，任何 IP 发生的这三种事件都会被检测到并进行上报。

6.2.2 IP-MAC绑定

IP-MAC 绑定是指将 IP 地址和 MAC 绑定在一起，可检测报文中的 ARP 地址欺骗与 ARP 地址冲突事件，可以区分 DHCP 动态 IP 地址分配与静态 IP 分配。

进入**资产配置>IP-MAC 绑定**三级菜单。如下图：

图 6-103 IP-MAC 绑定列表页面

在 IP 地址栏中输入 IP 地址，MAC 地址栏中输入需要绑定的 MAC 地址，点**[新建]**按钮即可新增一条 IP-MAC 绑定信息（最多可以下发 5 条 IP-MAC 绑定信息），如下图所示：

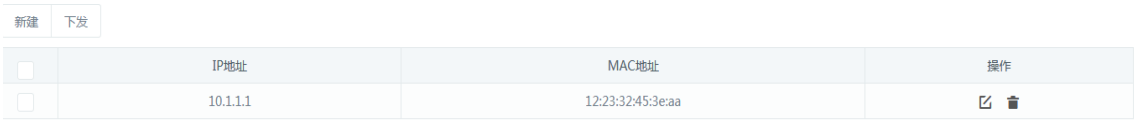

图 6-104 新建 IP-MAC 绑定页面

点击操作区的**[编辑]**按钮可以对绑定信息的 IP 或者 MAC 进行更改。如下图：

图 6-105 修改 IP-MAC 绑定配置页面

点击**[删除]**按钮可以删除 IP-MAC 绑定信息。如下图：

图 6-106 删除 IP-MAC 绑定页面提示

勾选配置点击**[下发]**按钮，弹窗“选择引擎”，在列表中勾选要下发配置的引擎，如下图：

图 6-107 选择引擎下发页面展示

点击**[确定]**按钮，就可以把 IP-MAC 绑定信息下发给引擎。

6.3 组件管理

对各组件进行管理，包括编辑、删除、连接/断开连接、授权配置、引擎详细信息、新建级联组件或多机引擎、配置动态检测引擎以及上级状态信息。组件管理列表如下。

图 6-108 组件管理页面展示

6.3.1 新建组件

新建功能用于对引擎进行多机、多级管理；引擎类型管理引擎和控制中心的级联管理。

图 6-109 新建组件页面展示

6.3.2 授权配置

授权配置用于进行授权码导入激活及授权状态展示。

点击**[授权信息]**按钮，进入授权配置页面；

图 6-110 授权信息按钮展示

（1）首次进入，激活试用授权

图 6-111 授权信息页面展示

点击**[试用激活]**按钮进行试用授权激活；成功授权后，各模块会自动更新授权信息。

图 6-112 成功激活授权页面展示

（2）导入授权文件

点击**[导入]**按钮，选择授权文件导入，成功授权后，各模块会根据授权码自动更新授

权信息。如下图：

图 6-113 导入授权文件页面展示

导入授权文件：点击**导入**按钮，定位到我司提供的授权文件后，点击**[确定]**按钮对该引擎进行导入授权操作。授权成功后，页面上该引擎的授权信息会更新。

引擎序列号：是产品的唯一标识，如需追加授权，需将引擎序列号提交给我司，我司将回复一个授权文件。用户可使用对应文件对引擎进行授权。

授权类型：显示该引擎的授权状态，包括正式、试用、未授权。

抓包口数量：显示授权抓包口数量。

事件库升级服务期：显示事件库升级服务期；

AV 病毒库升级服务期：AV 病毒库升级服务期；

静态检测服务期：显示静态检测服务期限；

动态检测服务期：显示动态检测服务期限；

Web 服务器攻击检测模块：显示是否对 Web 服务器攻击检测模块授权。

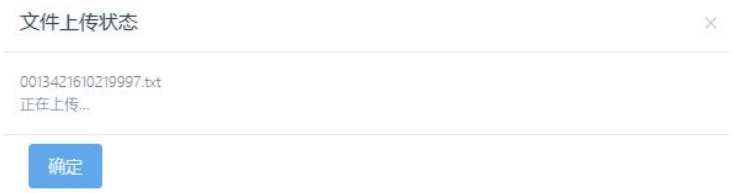

图 6-114 导入授权文件页面展示

点击**[抓包口数量]**链接进行抓包口授权界面，勾选需要使用的抓包口后确定，成功授权。如下图：

图6-115 抓包口信息页面展示

勾选抓包口的数量必须不大于实际授权的抓包口数量，否则会报错无法配置成功。如下图：

图 6-116 抓包口配置失败提示页面

6.3.3 设备状态

点击操作列的**[详细信息]**按钮，展示设备状态。设备状态展示内容包括三部分：设备

基本信息、引擎状态、配置明细。

基本信息：

基本信息记录设备的一般信息及会话统计信息。

引擎版本：特征检测模块版本；

引擎策略名称：当前引擎应用的策略集；

引擎并发 TCP 会话数：引擎累计统计的 TCP 会话个数；

引擎并发 HTTP 会话数：引擎累计统计的 HTTP 会话个数。

图 6-117 设备状态基本信息展示

引擎状态：

引擎状态记录特征检测模块的运行状态，包括：系统信息及网卡状态。

系统信息：记录特征检测模块的内核信息；

网卡状态：记录各网卡当前的双工模式、速率、用途、当前包数、当前比特数。

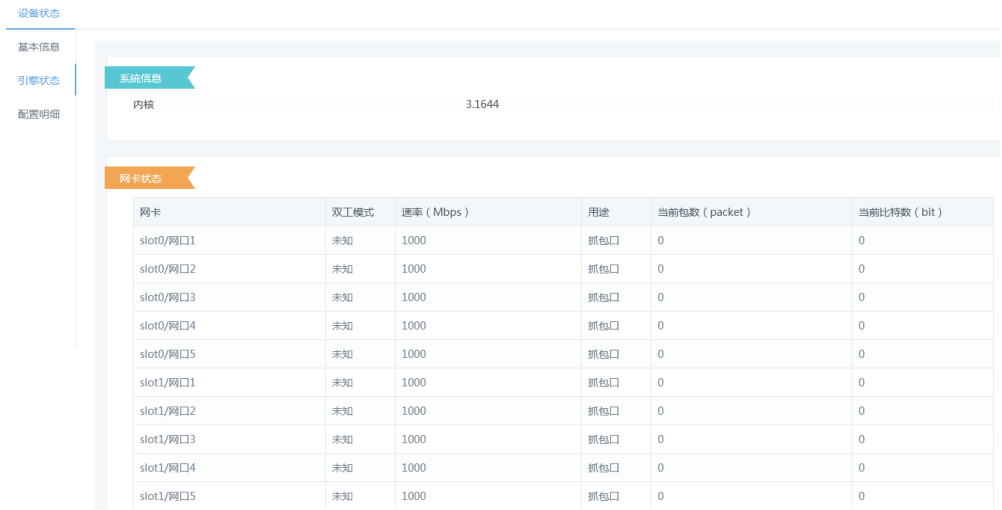

图 6-118 引擎状态信息页面展示

配置明细：

配置明细展示本机引擎的 Syslog 配置、事件合并、重点 web 服务器、URL 信誉库、威胁情报库、恶意样本库、病毒库、弱口令配置、IP-MAC 绑定、逃逸检测的配置信息。如下图：

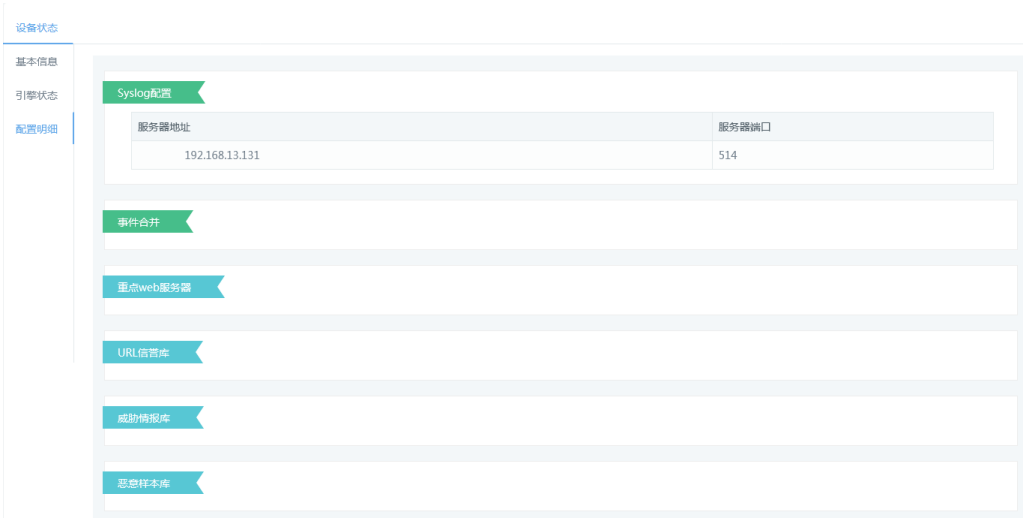

图 6-119 配置明细信息页面展示

6.3.4 动态引擎配置

点击[**新建**]按钮，弹出窗口，添加一条动态引擎。参数：引擎名称、引擎 IP、引擎说明、引擎端口、用户名、密码。如下图：

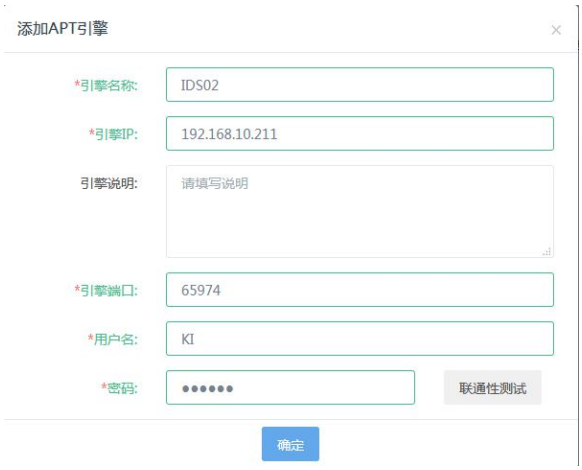

图 6-120 新建动态引擎页面

新建成功后弹出窗口如下图：

图 6-121 成功新建动态引擎页面

点击操作列**[编辑]**按钮可以对引擎进行修改，如下图：

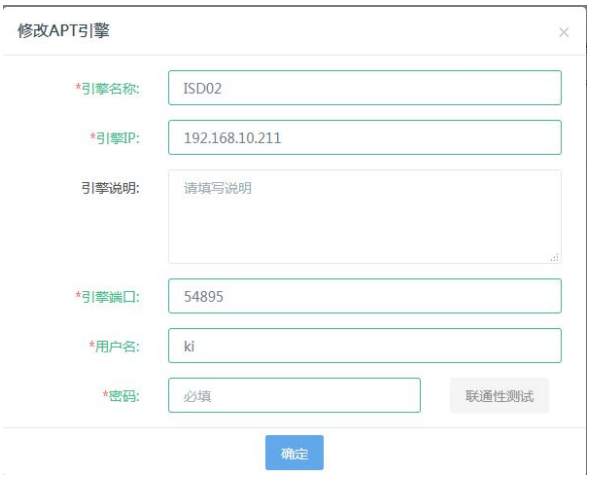

图 6-122 修改动态引擎页面

点击操作列**[删除]**按钮，删除引擎配置，如下图：

图 6-123 删除引擎提示页面

6.3.5 上级状态

上级控制中心 IP 地址展示管理本级引擎的上级引擎的 IP 地址；

连接状态展示本级引擎与上级引擎的连接状态（连接/断开）；

点击**[清除连接密钥]**按钮可以清除本级引擎控制中心与上级引擎控制中心的连接密钥，清除成功后才允许别的上级连接本级引擎控制中心。如下图：

图 6-124 清除连接密钥页面展示

6.4 文件检测配置

6.4.1 黑名单

该模块除自定义黑名单外，在样本日志中添加黑名单的样本文件，也会记录到该配置中。

操作按钮从左至右为：查询、新建、下发、上传（样本）文件、更多（批量导入配置、批量导出配置）。

查询：

通过配置查询条件对列表记录进行筛选，查询条件包括：名称、签名（MD5 值）、来源。如下图：

图 6-125 查询页面展示

新建：

通过添加签名（MD5 值）的方式，进行黑名单新建。如下图：

图 6-126 新建黑名单页面展示

点击**[提交]**按钮后，黑名单签名出现在配置列表中；展示列包括名称、签名、来源、时间及操作。如下图：

图 6-127 成功新建黑名单页面展示

来源记录黑名单的出处，用户添加记录用户名；

操作中可以执行黑名单配置删除。如下图：

图 6-128 删除名单提示页面

下发：

勾选黑名单项，点击[**下发**]按钮，弹窗“选择引擎”，在列表中勾选要下发配置的引擎，如下图：

图 6-129 选择引擎下发页面展示

点击**[确定]**按钮，会弹出成功的提示：

图 6-130 下发名单成功提示页面

上传文件：

通过手动上传样本文件的方式进行黑名单配置。文件上传大小上限阈值为 10MB，单次上传文件数上限为 300 个。如下图：

图 6-131 上传黑名单文件页面展示

更多：

导入：批量导入黑名单配置，文件类型要求 xls。如下图：

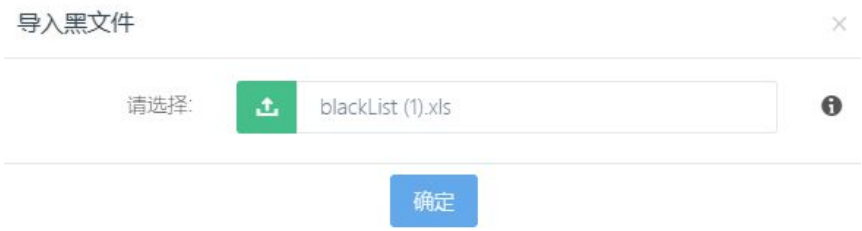

图 6-132 导入黑名单文件展示

导出：进行黑名单配置导出配置，选择存储路径进行配置留存。如下图：

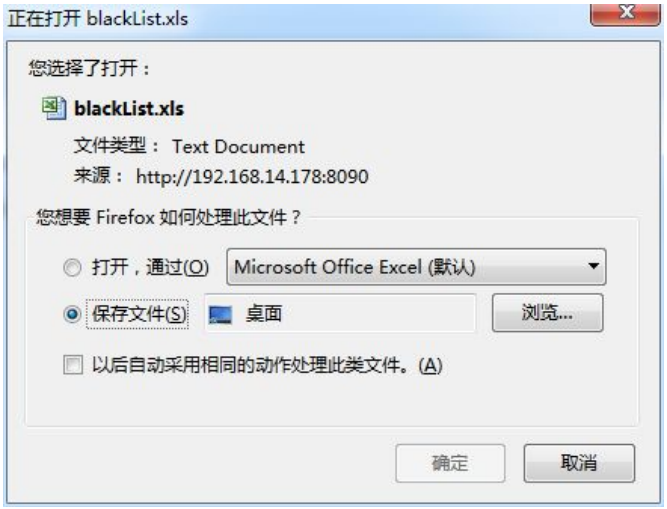

图 6-133 导出黑名单文件页面展示

6.4.2 白名单

该模块除自定义白名单外，在样本日志中添加白名单的样本文件，也会记录到该配置中。

操作按钮从左至右为：查询、新建、下发、上传（样本）文件、更多（批量导入配置、批量导出配置）。

查询：

通过配置查询条件对列表记录进行筛选，查询条件包括：名称、签名（MD5 值）、来源。如下图：

图 6-134 查询页面展示

新建：

通过添加签名（MD5 值）的方式，进行白名单新建。如下图：

图 6-135 新建白名单页面展示

下发：

勾选白名单项，点击**[下发]**按钮，弹窗“选择引擎”，在列表中勾选要下发配置的引擎，如下图：

图 6-136 选择引擎下发名单页面

点击**[确定]**按钮，会弹出成功的提示：

图 6-137 成功下发名单提示页面

上传文件：

通过手动上传样本文件的方式进行白名单配置。文件上传大小上限阈值为 10MB，单次上传文件数上限为 300 个。（可参考图 6-131）

更多：

导入：批量导入白名单配置，文件类型要求 xls。如下图：

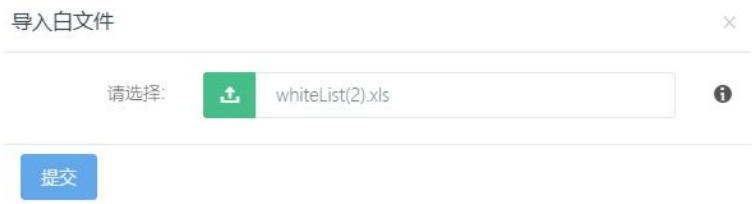

图 6-138 导入白名单文件页面展示

导出：进行白名单配置导出配置，选择存储路径进行配置留存。如下图：

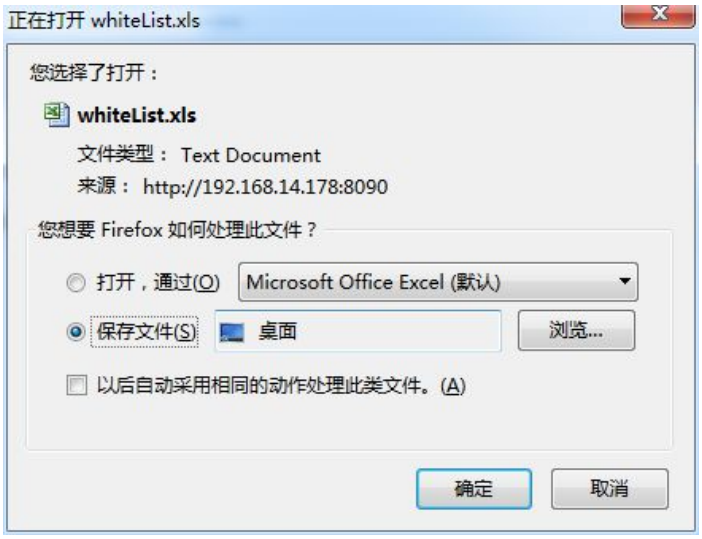

图 6-139 导出名单文件页面展示

6.5病毒检测配置

随着互联网的迅猛发展，计算机病毒对信息安全的威胁日益增加。特别是在网络环境下，传播路径和应用环境的多样化使得网络计算机病毒的发生频率较普通计算机病毒更高、潜伏性更强、影响面更广，破坏性更大。网络病毒的防治和信息安全问题已成为计算机领域的重点研究对象。

Internet 环境下主要是源于四种安全威胁：其一，来自文件下载，这些被浏览的或是被下载的文件可能存在病毒；其二，来自电子邮件，大多数的互联网邮件系统提供了在网络间传输附带格式化文档邮件的功能；其三，聊天工具，一些聊天工具提供了在线的传输文件功能，如：MSN，QQ 等；其四，P2P 等下载工具，如：BT，电驴等。

IDS 防病毒检测功能，检测的协议主要有 HTTP、FTP、POP3、IMAP、SMTP 这五种协议，在文件扫描中，通过配置可以根据文件类型对网络传输的文件进行扫描检测，并上报扫描检测结果。

病毒检测配置前提，我们在进行病毒检测配置之前，必须确保两点：

首先，必须确保相应的引擎处于已连接状态；

其次，必须确保相应的引擎病毒库已经升级到所需版本，具体可以从设备管理的引擎详细信息配置明细中看到当前版本病毒库最后更新时间，如下图所示。

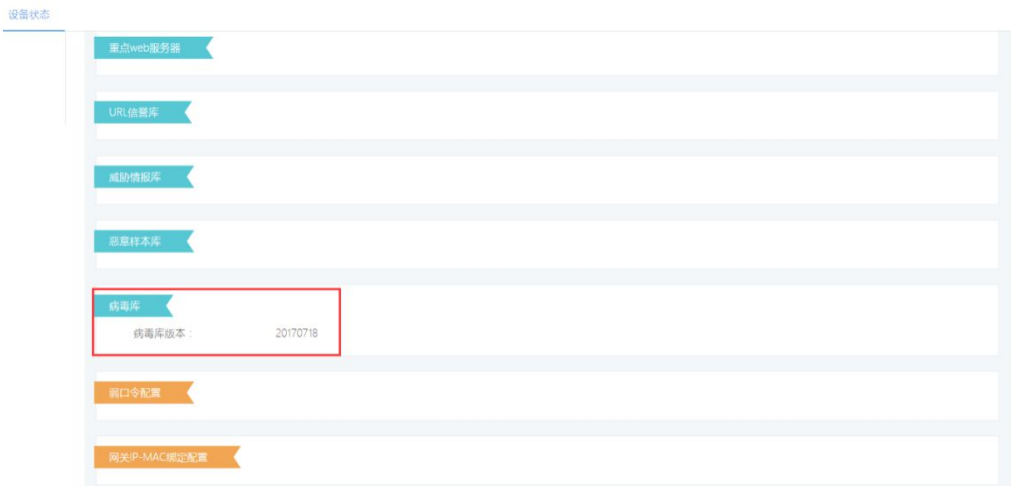

图 6-140 病毒库样本展示

病毒检测配置

进入“病毒检测配置”界面，点击相应引擎操作列**[病毒检测协议类型配置]**按钮弹出相应配置界面，如下图所示。

图形化用户界面

图 6-141 病毒检测协议类型配置页面

默认情况下，五种协议类型处于未被启用状态，如果想启用，需先勾选启用，然后选择所需要配置的协议类型，点击**[确定]**按钮即可，提交成功后，会弹出成功提示对话框，如下图所示。

图 6-142 配置病毒检测协议页面

点击**[确定]**按钮后，会提示配置协议成功。如下图：

图 6-143 配置协议类型成功提示页面

如果不想提交当前协议类型配置，可以点击 **X** 按钮，界面就会跳转回上级“**病毒检测配置**”界面。

病毒检测文件类型配置

进入“病毒检测配置”界面，点击相应引擎操作列**[病毒检测文件类型配置]**按钮弹出相应配置界面，如下图所示。

图 6-144 病毒检测文件类型配置页面

默认情况下，17 种文件类型处于全勾选启用状态，如果不想启用其中某些文件类型，可以将相应“启用”列的“√”去掉，点击**[确定]**按钮即可，如下图所示。此处需要注意的一点是默认的 17 种文件类型是不能进行删除操作的。

我们还可以自己定义病毒检测文件类型，具体操作步骤是：首先，在“文件类型”处添加所需文件类型，此时需要注意，新建的文件类型必须是以“*.”开始的长度不大于 10 的字母、数字的组合，例如“*.7z”；其次，点击**[新增]**按钮，新建的文件类型就添加到了文件类型列表中；最后点击**[确定]**按钮即可，如下图所示。

图 6-145 病毒检测文件类型配置成功页面

如果想将自建的检测文件类型删除，只需点击操作列的**[删除]**按钮，再点击**[确定]**按钮，即可将对应文件类型删除。

6.6 URL信誉库

该系统提供捕获恶意 URL 访问行为配置：

可以通过单独定义的形式，随时添加对指定 URL 的检测和报警；

内置一个 URL 信誉库；

引擎通过内置恶意 URL 库或者单独定义 URL，实现对访问恶意 URL 的检测。

首先，引擎内置 URL 信誉库，具体可以从设备管理的引擎详细信息配置明细中看到当前版本，也可以对 URL 信誉库进行升级，在**系统管理>系统维护>升级管理**中进行手动升级，如下图所示。

图 6-146 升级 URL 信誉库列表页面

6.6.1 黑名单

进入黑名单配置页面，如下图：

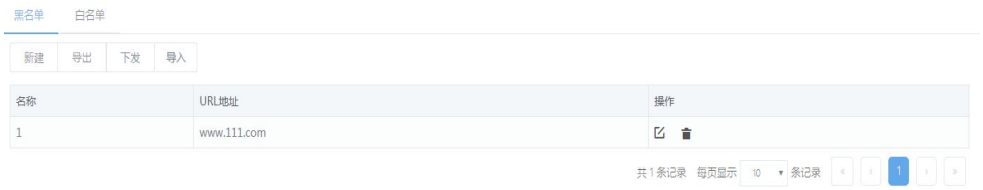

图 6-147 黑名单列表页面展示

操作按钮从左至右为：新建、导出、下发、导入。

新建：

新建黑名单，配置名称以及 URL 地址，二者均不能为空（在名称位置不允许输入特殊符号，在 URL 位置如果输入不合法的 URL 系统会有提示信息）点击确定**[提交]**按钮。如下图：

图 6-148 新建 URL 黑名单页面展示

提交后，URL 地址出现在配置列表中；展示列包括名称、URL 地址及操作。如下图：

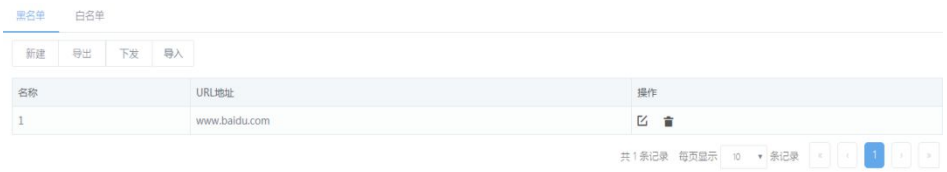

图 6-149 成功新建 URL 黑名单页面展示

注意

白名单与黑名单配置一致 ,当黑名单 URL 与白名单 URL 地址一致时，白名单优先。

导出：

进行黑名单配置导出，选择存储路径进行配置留存。如下图：

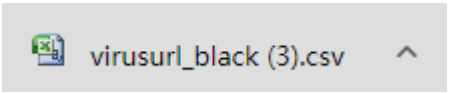

图 6-150 导出黑名单配置文件页面

下发：

点击**[下发]**按钮，弹窗“选择引擎”，在列表中勾选要下发配置的引擎，如下图：

图 6-151 选择引擎下发名单页面展示

点击**[确定]**按钮，会弹出成功的提示。如下图：

图 6-152 下发名单成功提示页面

导入：

批量导入 URL 黑名单配置，文件类型要求 xls。如下图：

图 6-153 导入黑名单文件页面展示

6.6.2 白名单

操作同 URL 黑名单配置，请参考 6.6.1 黑名单配置。

注意

白名单与黑名单配置一致，当黑名单 url 与白名单 url 地址一致时，白名单优先。

6.7隐蔽信道库

该模块除记录文件检测日志中添加过来的隐蔽信道特征外，还可以根据域名、主机与服务、URL 自定义隐蔽信道特征。

系统既内置一个隐蔽信道库，又可以通过自定义的形式，随时添加对指定隐蔽信道特征的检测和报警。

自定义隐蔽信道特征：

右上角操作按钮从左至右为：筛选、新建、下发、导出、导入。如下图：

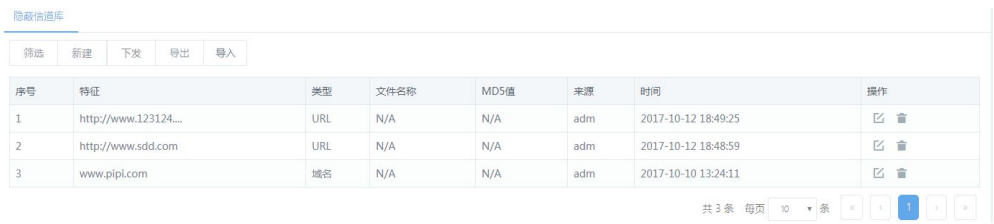

图 6-154 隐蔽信道库页面展示

筛选：

通过配置筛选条件对列表记录进行筛选，筛选条件包括：类型（域名、URL、主机与服务）、文件名称、MD5 值、特征。如下图：

图 6-155 隐蔽信道库筛选页面展示

新建：

用户可以根据实际需要，按照域名、URL、主机与服务进行隐蔽信道库特征的添加。如下图：

图 6-156 新建隐蔽信道库页面展示

添加成功后，相应的隐蔽信道库特征会出现在列表中。展示的列包括序号、特征、类型、文件名称、MD5 值、来源、时间及操作。如下图：

图 6-157 成功新建信道库页面展示

文件名称：如果从文件检测日志中添加过来的特征，文件名称显示实际恶意样本文件名称；如果是用户自定义的特征，文件名称显示 N/A；

MD5 值：如果从文件检测日志中添加过来的特征，MD5 值展示实际恶意样本文件的 MD5 值；如果是用户自定义的特征，MD5 值显示 N/A；

来源：用户自定义的特征，来源显示对应的用户名；从日志中添加过来的特征，来源显示样本检测。

操作列中的**[编辑]**按钮，实现对特征的编辑操作。

下发：

点击**[下发]**按钮，弹窗“选择引擎”，在列表中勾选要下发配置的引擎，如下图：

图 6-158 选择引擎下发页面展示

点击**[确定]**按钮，会弹出成功的提示。如下图：

图 6-159 下发引擎成功提示页面

导出：

进行隐蔽信道库导出配置，选择存储路径进行配置留存。如下图：

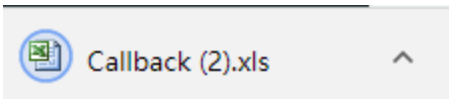

图 6-160 导出信道库文件页面展示

导入：

批量导入隐蔽信道库配置，文件类型要求 xls。如下图：

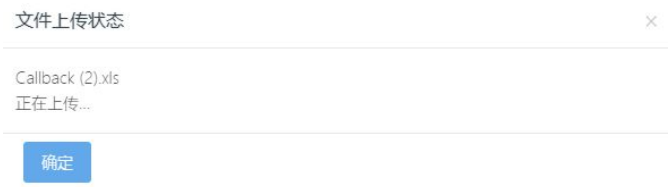

图 6-161 导入信道库文件页面展示

内置隐蔽信道库升级

从设备管理的引擎详细信息配置明细中看到当前版本，也可以对威胁情报库（隐蔽信道库）进行升级，在**系统管理>系统维护>升级管理**中进行手动升级，如下图所示。

图 6-162 内置隐蔽信道库升级页面展示

第7章 系统管理

系统管理模块由响应方式、系统维护、通用配置、运行日志组成。

响应方式包括：Syslog 配置、SNMP 配置、邮件配置、防火墙配置。

系统维护包括：升级管理、系统升级、存储维护。

通用配置包括：时间配置、代理配置、关注度配置。

运行日志包括：系统运行日志、诊断日志。

7.1 响应方式

7.1.1 Syslog配置

检测事件（包含：特征事件、隐蔽信道、URL 信誉检测、病毒检测、文件检测）、资源告警信息可以通过 Syslog 响应方式发送到指定 Syslog 服务器。

进入**系统管理>响应方式>Syslog 配置**中分别进行 Syslog 响应配置。如下图：

图 7-1 Syslog 配置页面展示

进入**检测配置>特征检测配置>策略集**中，针对指定事件勾选 Syslog 响应方式。若针对多条事件统一配置 Syslog 响应方式，可以先新增 Syslog 响应方式的策略模板，然后针对多条事件统一应用模板进行统一配置。如下图：

图 7-2 配置 Syslog 页面展示

7.1.2 SNMP配置

特征检测日志可以通过 SNMP 响应方式发送到指定 SNMP 服务器。

进入**系统管理>响应方式>SNMP 配置**中进行特征检测日志 SNMP 响应配置。

配置 SNMP TRAP 版本、服务器端口和接收者 IP。如下图：

图 7-3 SNMP 配置页面展示

进入**检测配置>特征检测配置>策略集**中，针对指定事件勾选 SNMP 响应方式。若针对多条事件统一配置 SNMP 响应方式，可以先新增 SNMP 响应方式的策略模板，然后针对多条事件统一应用模板进行统一配置。如下图：

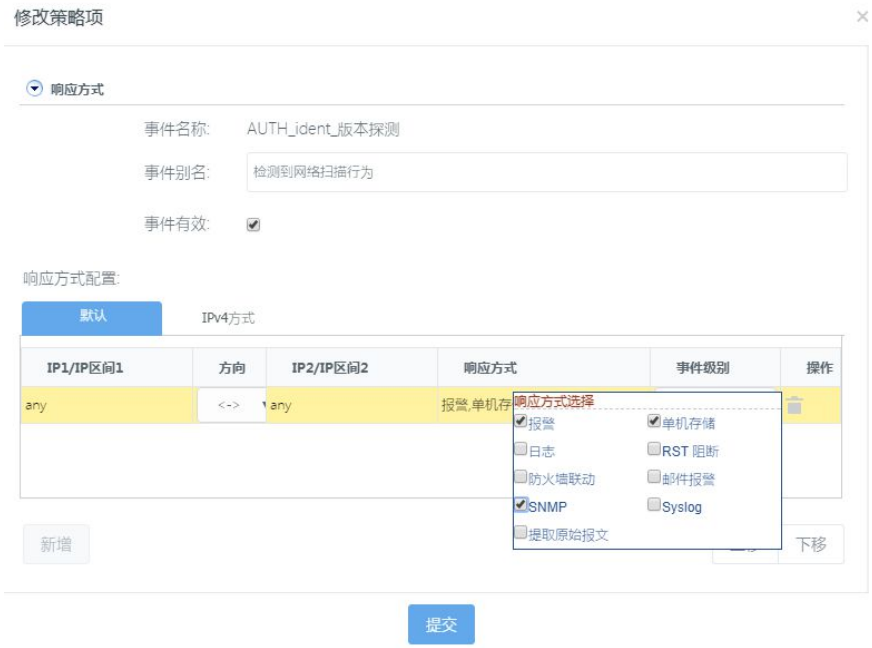

图 7-4 配置 SNMP 页面展示

7.1.3 邮件配置

特征检测日志可以通过邮件响应方式发送给指定邮件收件人。

发件人配置：

进入**系统管理>响应方式>邮件配置**中进行发件人配置。

配置邮件发件人服务器的地址、端口、SMTP 服务器身份认证、发送时间间隔等参数。如下图：

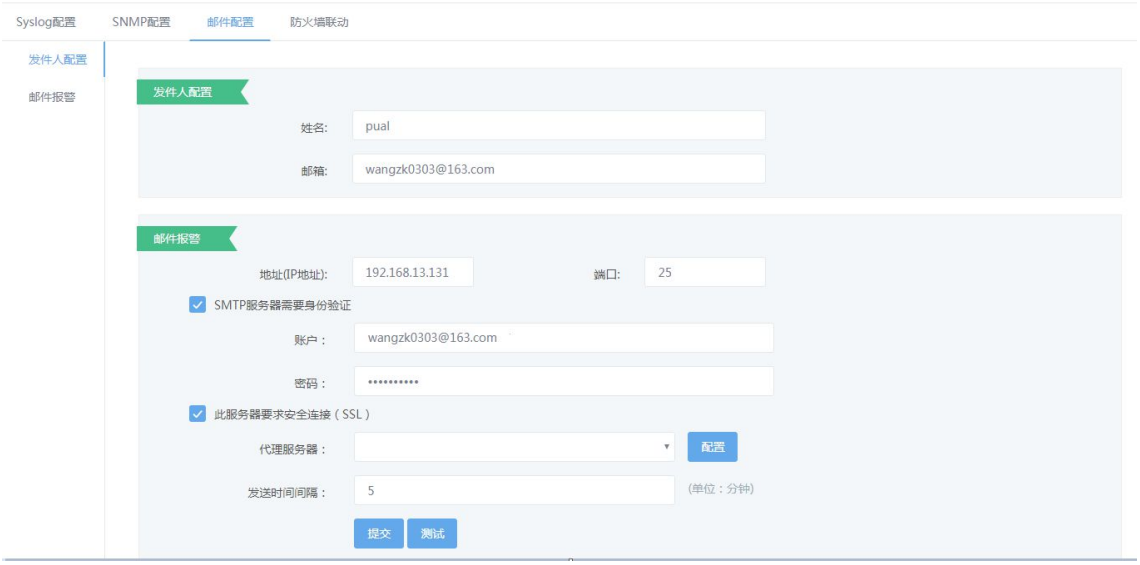

图 7-5 邮件配置页面展示

参数说明：

姓名：添加发件人姓名；

邮箱：添加发件人邮箱；

地址（IP 或域名）：添加邮件服务器的 IP 地址或者域名；

端口：默认配置为 25 端口，可以自行更改；

账户：发件人邮箱地址；

密码：发件人邮箱密码；

代理服务器：可以配置代理服务器；

邮件发送时间间隔：只针对于邮件报警功能，设置报警邮件发送的时间间隔，对于发送日志报表功能来说，不起作用。

注意

“此服务器要求安全连接 SSL”项，默认配置是被勾选上的，若使用 163、263 的邮箱作为发件人邮箱，请不要勾选此项，因为 163、263 邮箱不支持 SSL 加密协议。

正确配置发件人信息后，点击**[测试]**按钮，在已有收件人的情况下，测试邮件发送成功。

此时，进入相应的收件人邮箱中查看，可以看到一份测试邮件。

若发件人信息配置错误，或者没有配置收件人信息，此时点击**[测试]**按钮，测试邮件将发送失败。

配置好发件人信息后，点击**[提交]**按钮，发件人配置信息被保存。

特征检测邮件响应：

进入**系统管理>响应方式>邮件配置>邮件报警**中进行邮件响应配置。

新建收件人，添加收件人及邮箱。如下图：

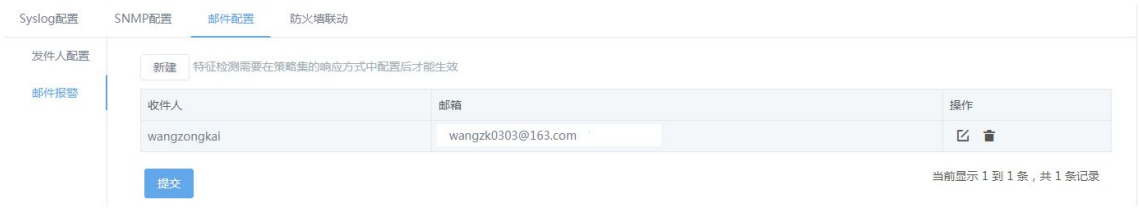

图 7-6 邮件配置收件人页面展示

可以通过**[新建]**按钮，进行收件人编辑。如下图：

图 7-7 新建收件人页面展示

可以通过操作列**[删除]**按钮，进行收件人删除。如下图：

图 7-8 删除收件人提示页面

进入**检测配置>特征检测配置>策略集**中，针对指定事件勾选邮件报警响应方式。若针对多条事件统一配置邮件报警响应方式，可以先新增邮件报警响应方式的策略模板，然后针对多条事件统一应用模板进行统一配置。如下图：

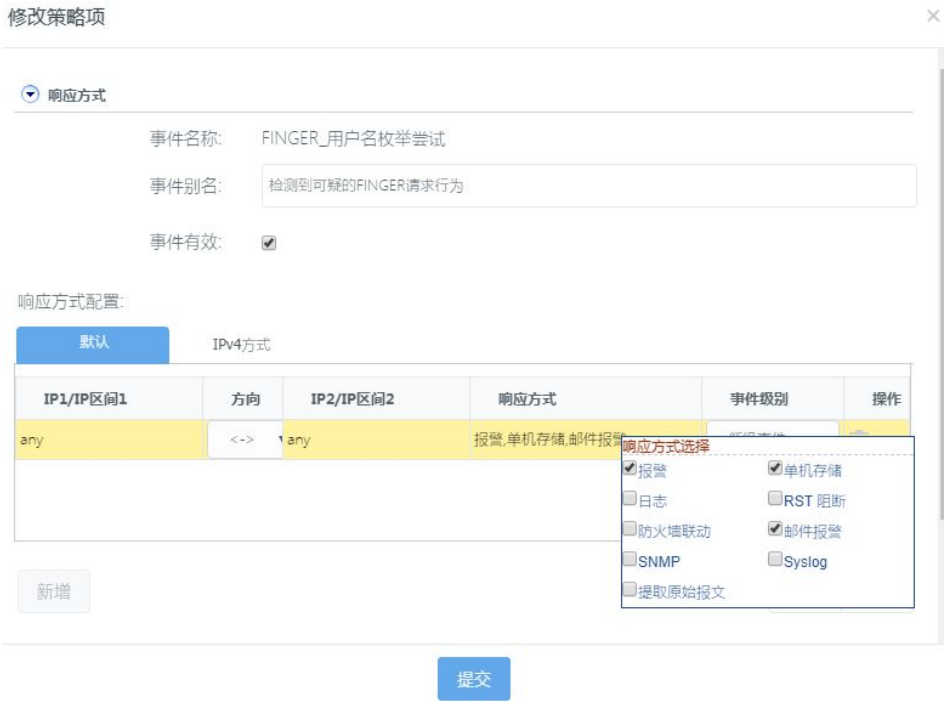

图 7-9 邮件报警设置页面展示

7.1.4 防火墙联动

RAVEN 入侵检测与管理系统可以和一些类型的防火墙联合防御网络攻击行为。防火墙联动动作的触发，需要为引擎配置联动防火墙，并且为关注的事件配置防火墙联动响应

方式，把该事件随策略下发给引擎。如下图：

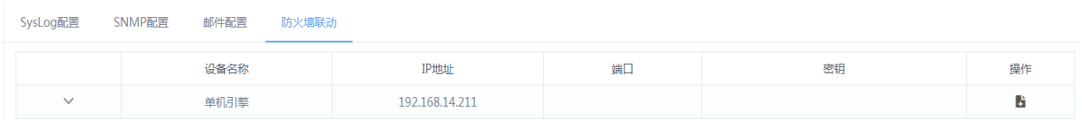

图 7-10 防火墙联动列表页面

添加防火墙：

点击引擎操作列**[增加]**按钮，添加防火墙。目前 RAVEN 入侵检测与管理系统支持 vip_fw、opsec、netscreen、topsec 四类防火墙。如下图：

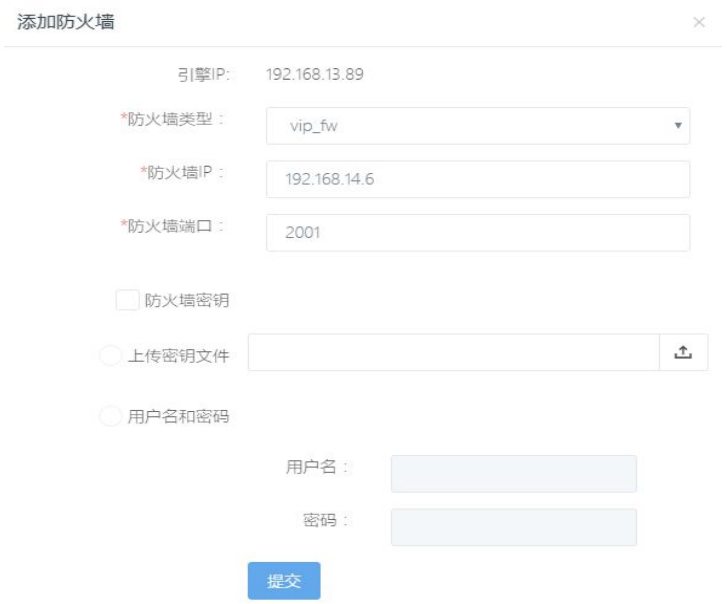

图 7-11 防火墙联动设置展示

参数说明：

防火墙类型：选择将要添加的防火墙类型；

防火墙 IP：必需填写。防火墙设备 IP 地址；

防火墙端口：防火墙联动功能的端口；

防火墙密钥：如果防火墙联动功能需要密钥，请启用添加密钥；。

上传密钥文件：如果是文件类型的密钥，在这里上传；

用户名、密码：如果密钥是用户名、密码，请在这里输入。

备注：最多只能添加 20 个防火墙。

删除防火墙：

点击防火墙列表后面**[删除]**按钮，弹出相应的询问对话框。如下图：

图 7-12 删除联动防火墙页面展示

点击**[确定]**按钮，即可以删除对应的防火墙。

7.2 系统维护

7.2.1 升级管理

升级管理主要包括六个模块：事件库升级、恶意样本库升级、URL 信誉库升级、威胁情报库升级、特征检测模块升级、病毒库升级。

事件库升级：手动对事件库进行升级。

恶意样本库升级：手动对恶意样本库进行升级。

URL 信誉库升级：手动对 URL 信誉库升级进行升级。

威胁情报库升级：手动对威胁情报库升级进行升级。

特征检测模块升级：手动对特征检测模块进行升级。

病毒库升级：手动对病毒库升级进行升级。

列表展示列包括升级模块、当前版本、最新版本、升级状态和操作。

升级模块：功能模块列表；

当前版本：当前模块版本；

最新版本：导入升级包的版本，可供升级；

升级状态：升级成功、升级失败、未升级；

操作：升级、删除。

注意：本版本不支持升级。

图 7-13 升级管理页面展示

注意

不同引擎各模块版本可能不同，因此升级管理页面列表恶意样本库、URL 信誉库、威胁情报库、特征检测模块、病毒库不展示当前版本（N/A），仅展示本机引擎的事件库、控制中心版本。

通过**[导入]**按钮导入相应升级文件。如下图：

图 7-14 导入升级文件页面展示

升级包导入成功后，操作列**[升级]**按钮亮显，可以进行升级操作。如下图：

图 7-15 升级提示页面展示

通过操作列**[删除]**按钮，实现导入升级包的删除。如下图：

图 7-16 删除最新版本提示页面

注意

其他模块升级导入后升级需勾选引擎进行相应引擎的模块升级。

图 7-17 选择升级引擎页面提示

注意

恶意样本库、URL 信誉库、威胁情报库模块升级导入后升级需勾选引擎进行相应引擎的模块升级，并且这三个模块不能给 IDS7040 引擎进行升级，在勾选引擎页面有相应提示信息。

图 7-18 引擎信息提示页面

7.2.2 系统升级

系统升级实现对整个系统的升级，进入**系统管理>系统维护>系统升级**，版本号中展示系统当前版本信息。如下图：

图 7-19 系统升级页面展示

参数说明：

FTP 服务器 IP：填写升级包所在 FTP 服务器的 IP 地址；

FTP 服务器端口：填写 FTP 服务器端口；

用户名：填写具有下载升级包权限的 FTP 服务器用户名；

密码：填写用户名对应的密码；

升级包路径：填写升级包存储在 FTP 服务器路径。

完成 FTP 服务器搭建，并将系统升级文件放到相应路径，准确填写以上信息后，点击**提交**按钮进行升级，升级过程会持续一段时间，成功后 Web 端可正常登录。

7.2.3 存储维护

存储维护图形化展示了当前设备硬盘的使用情况，预警配置可设置告警阈值，超出阈值。可进行告警，便于用户及时获取磁盘使用信息，及时进行清理工作，确保系统正常使用。

数据清理预览：

饼图直观的展示了磁盘的使用情况，清理模块可选择清理原始报文和分析数据两个类型的数据。

依次进入**系统管理>系统维护>存储维护**，默认展示当天可清理的原始报文和分析数

据占用的磁盘空间，点击时间控件，选择起始时间，点击**[预览]**按钮可查看此范围的可清理数据。如下图：

图 7-20 数据清理页面展示

点击**[清理]**按钮，界面弹出提示信息，点击**[确定]**按钮，即可进行磁盘清理操作，同时清理选中时间段的原始报文和分析数据。如下图：

图 7-21 清理磁盘数据提示页面

注意

系统默认选中的日期是当天，清理操作的时候注意分析数据的时间范围，尽量不要删除近期的数据。

清除日志时，请优先做好数据备份，如导出期间的日志，对期间的数据执行报表等。

清除按钮 ,同时清除选中时间段的原始报文和分析数据，

请确认输入时间段无误再执行清除。

磁盘使用情况：

磁盘使用情况的饼图展示系统当前磁盘存储信息，包括三个模块：已用空间、可用空间和可释放空间。如下图：

图 7-22 磁盘使用情况展示

预警配置：预警模块可配置三种告警模式，磁盘可用空间、内存使用率和 CPU 使用率低于设定值时，可进行告警，便于用户及时获取磁盘以及系统使用信息，及时进行清理工作。如下图：

图 7-23 预警配置设置

本地预警：Web 界面推送告警信息，在重要消息里查看，告警周期为 5 分钟。

邮件预警：以邮件的形式进行告警，需确保邮件配置无误。磁盘可用空间告警周期为 12 小时，内存和 CPU 的告警周期为 5 分钟。

Syslog 预警：以 Syslog 日志的形式进行告警，需确保 syslog 配置无误。磁盘可用空间告警周期为 12 小时，内存和 CPU 的告警周期为 5 分钟。

7.3 通用配置

7.3.1 时间配置

时间同步：

时间配置的主要作用是用于配置系统时间。如下图：

图 7-24 时间同步设置页面展示

可以通过时间配置进行系统时间手动设置，点击时间配置右侧的显示框，弹出手动设置时间的窗口。也可以通过 NTP 服务器进行系统时间同步，选择与 NTP 服务器同步，进行网络校时，在服务器下拉菜单中，可以看到很多的备选服务器，任意选择一个服务器后，点击**[同步]**按钮，时间配置成功。如下图：

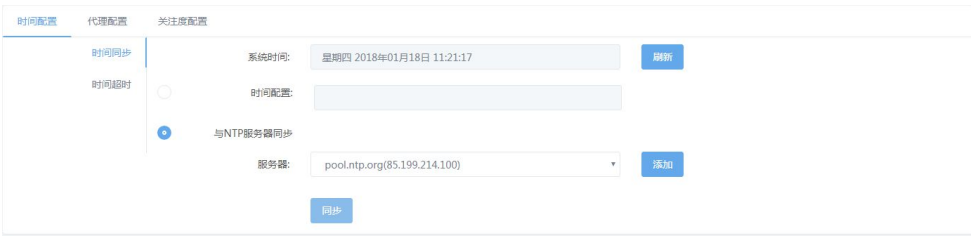

图 7-25 NTP 服务器同步设置展示

点击**[提交]**按钮，则添加的服务器地址以及名称出现在列表中。

点击界面右上角的**[返回]**按钮，回到时间同步界面，当勾选与 NTP 服务器同步后，在服务器下拉框中会看到自定义的 NTP 服务器，可以选择与其进行时间同步。如下图：

图 7-26 与其他时间同步设置展示

时间超时：

用于页面超时时间设置，系统默认超时时间是 30 分钟；未做操作时，系统达到设置的阈值会自动退出系统。如下图：

图 7-27 时间时设置页面展示

超时时间小于 999999，0 表示永不超时。

7.3.2 代理配置

代理服务器主要用于发送邮件功能。进入代理配置页面，可以看到已建立的代理服务器列表，列表中包含各个代理服务器的相关信息，如：代理名称、代理类型、服务器地址、端口、操作等内容。

在代理配置页面中，点击**[新建]**按钮，进入新建代理服务器配置页面。如下图：

图 7-28 新建代理设置页面展示

参数说明：

代理名称：添加代理服务器的名称；

代理类型：Socks 类型；

服务器地址：添加代理服务器的 IP 地址；

端口：添加对应的端口号；

用户名：代理服务器用户名；

密码：服务器密码。

配置好代理服务器相关信息后，点击**[提交]**按钮，代理服务器新建成功；点击 **X** 按钮，则不创建该代理服务器。

在邮件配置中，点击**[配置]**按钮，同样可以进入到代理配置页面，进行代理服务器的配置。

注意

邮件配置中只支持 Socks 类型的代理服务器。

7.3.3 关注度配置

配置用户需要关注事件，主要用于主页 Top5 安全事件统计。

显示配置智能分析、无需关注和需要关注的事件统计信息，以及应用于 Top5 安全事件统计。关注度配置界面如下图：

图 7-29 关注度配置页面展示

编辑完成后，点击**[提交]**按钮，则应用生效，如下图：

图 7-30 关注度配置成功提示页面

编辑智能分析：

点击关注度类型中智能分析对应的**[编辑]**按钮，进行编辑关注事件页面，如果事件比较多时候，会出现等待页面。

打开编辑智能分析页面如下图：

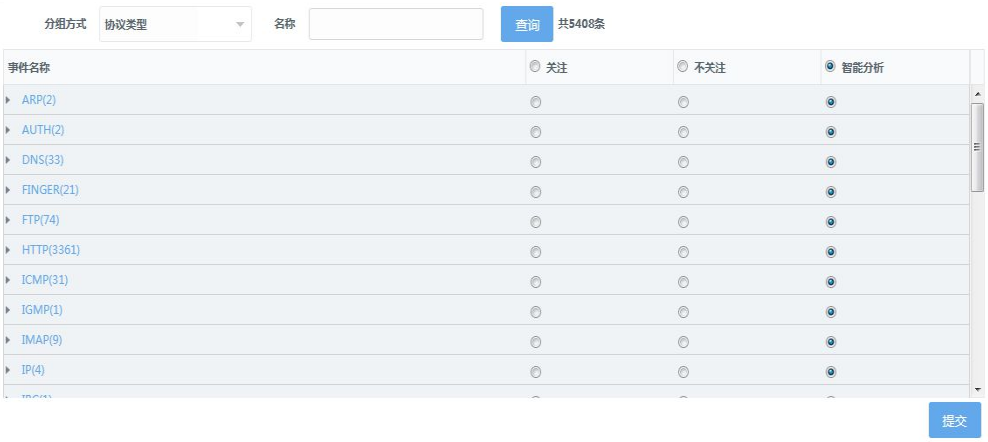

图 7-31 编辑智能分析页面展示

编辑每个事件的关注类型，点击**[提交]**按钮，保存成功返回关注度配置页面。

编辑无需关注：

点击关注类型中无需关注对应的**[编辑]**按钮，进行编辑不需要关注事件，如果事件比较多时候，会出现等待页面，不需要关注事件页面如下图：

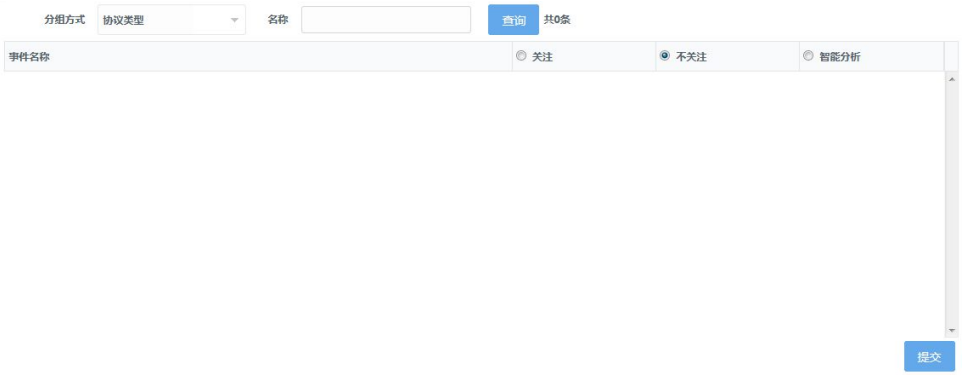

图 7-32 编辑无需关注页面展示

编辑每个事件的关注类型，点击**[提交]**按钮，保存成功返回关注度配置页面。

编辑需要关注：

点击关注类型中需要关注对应的**[编辑]**按钮，进行编辑需要关注事件页面，如果事件比较多时候，会出现等待页面，需要关注事件页面如下图：

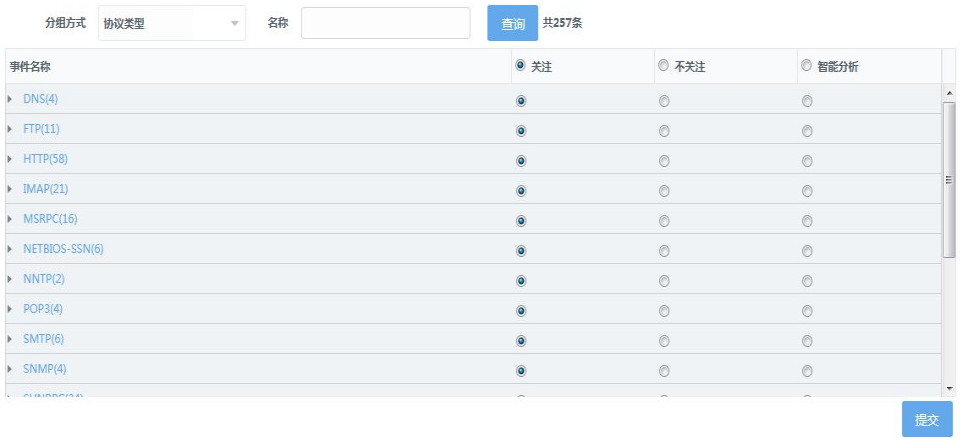

图 7-33 编辑需要关注页面展示

编辑每个事件的关注类型，点击**[提交]**按钮，保存成功返回关注度配置页面。

7.4 运行日志

7.4.1 运行日志

该模块记录系统的运行日志，展示列包括序号、时间、内容。如下图：

图 7-34 运行日志信息页面展示

可以根据内容、开始时间、结束时间进行运行日志筛选查询。如下图：

图 7-35 查询页面展示

可以导出运行日志为 Excel 格式进行保存查看。如下图：

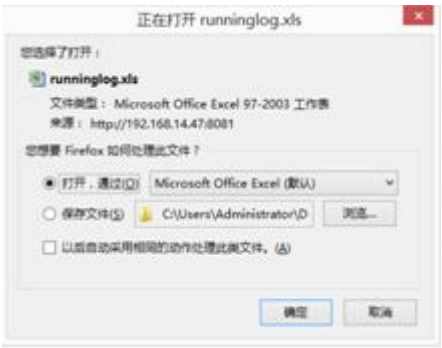

图 7-36 导出日志页面展示

注意

导出 xls 文件时，由于个人机器环境不同，有可能无法弹出确认对话框，而是 IE 直接调用已安装的 EXCEL 软件把需要下载的文件打开 ,这时只能通过 IE 的后退功能返回到报表文件列表页面。

7.4.2 诊断日志

诊断日志可导出系统日志，用于定位系统运行可能出现的异常。如下图：

图 7-37 诊断日志页面展示

可以导出诊断日志为.zip 压缩格式。如下图：

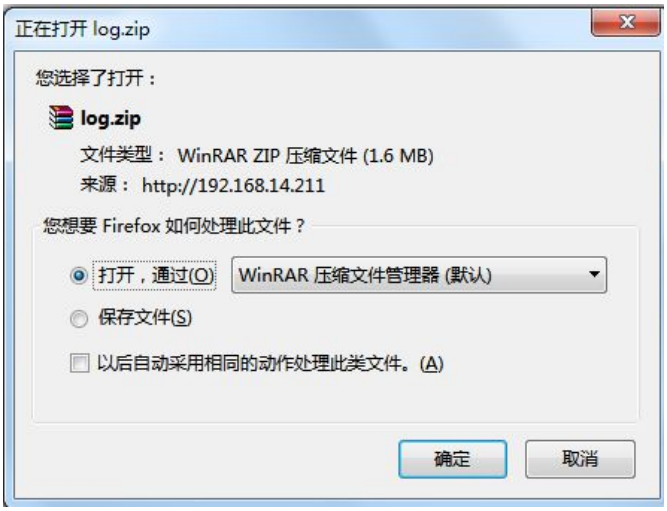

图 7-38 导出诊断日志页面展示

第8章 用户管理

系统对通过浏览器访问系统的用户，进行了角色的区分，把用户分为：“用户管理员”、“配置管理员”和“审计员”三种角色。

其中“用户管理员”和“审计员”是系统固有的角色，每个角色有一个预置的用户，除了密码之外，不可删除或更改。“配置管理员”角色可以有多个用户，“用户管理员”可以添加、删除、修改“配置管理员”信息，以及进行对其他用户锁定、解锁的操作。

用户管理员是系统固有的一个用户，默认用户名为“admin”，不可更改，初始密码“Raven.private”，用户管理员可以通过工具栏上的“修改密码”功能，修改自身密码。

用户管理员登录后，可见用户管理界面，可以添加、删除、修改、锁定配置管理员信息、设置连续登录时间及次数锁定和解锁被锁定的 IP。

审计员是系统固有的一个用户，默认用户名为“audit”，不可更改，初始密码“Raven.audit”，审计员可以通过工具栏上的“修改密码”功能，修改自身密码。

审计员登录后，可见审计日志界面，审计日志中记录了所有用户进入系统后的各种操作日志，审计员可以查询、删除、导入、导出这些操作日志。

配置管理员是执行系统主要业务的角色，系统中的业务除用户管理和审计日志其它的所有业务均由配置管理员完成。“配置管理员”由“用户管理员”添加，初始密码由“用户管理员”设定，配置管理员登录后，可以通过工具栏上的“修改密码”功能自行修改密码。

8.1用户列表

用户管理员以“admin”用户登录系统，登录后可见配置管理员用户列表，系统预置一个“adm”配置管理员用户，密码“Raven.public”。用户管理员可以新建、编辑、删除、锁定配置管理员。如下图：

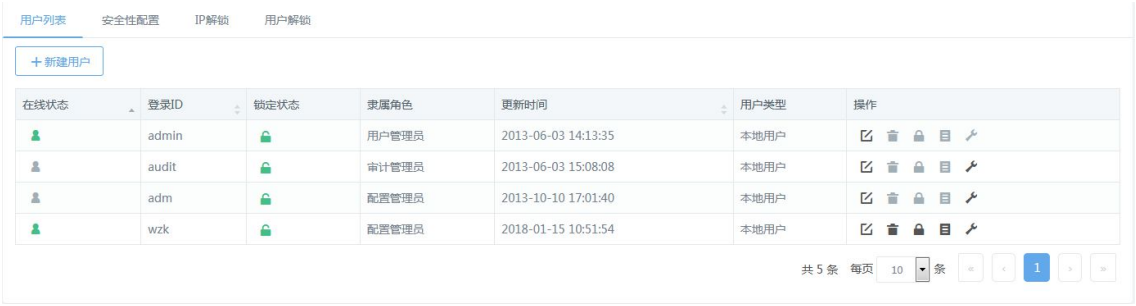

图 8-1 用户管理页面展示

8.1.1 新建用户

点击**[新建]**按钮添加用户，可以新建本地用户。新建用户时，必须填写登录 ID，密码，重输密码等信息。用户名称可以使用英文或数字，不超过 20 个字符；密码按照强度提示设置。

新建本地用户页面如下，登录 ID、密码、重输密码、允许访问的 IP 是必填项，其它项可以选填，用户类型为本地用户。如下图：

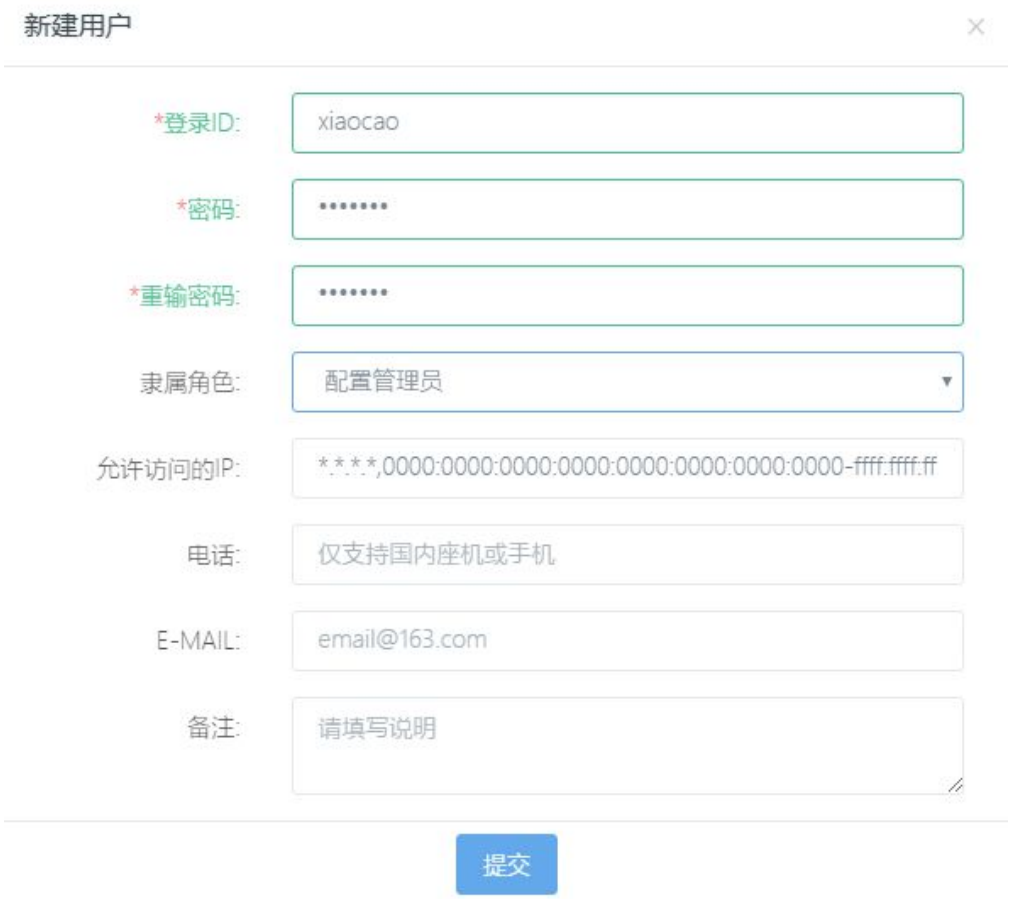

图 8-2 新建用户页面展示

其中，允许访问的 IP 默认是全开放的，任意相连通的 IP 地址都可以进行 Web 的登录，“*.*.*.*,0000:0000:0000:0000:0000:0000:0000:0000-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff”。如果配置访问的 IP 是“192.168.13.27”，则只有该 IP 地址可以登录控制中心，其他 IP 地址登录后，会提示“登录 IP 不在用户允许的登录 IP 范围内，请联系管理员!”。如下图：

图 8-3 登录 IP 范围提示错误页面

8.1.2 编辑用户

点击用户所在行的**[编辑]**按钮，进行用户修改。修改用户界面和新建用户类似，但登录 ID 不能修改，用户密码通过单独的重置密码功能完成，只允许修改联系电话、email 地址、描述等基本信息。如下图：

图 8-4 修改用户设置页面展示

8.1.3 删除用户

点击用户所在行的**[删除]**按钮，确认删除后，用户即被删除。如下图：

图 8-5 删除用户提示页面

注意 **用户管理员、审计管理员不能删除。**

8.1.4 锁定与解锁用户

点击用户所在行的**[锁定]**按钮，确认锁定后，用户即被锁定，用户锁定后，利用该登录 ID 进行登录，会弹出如下错误提示。如下图：

图 8-6 锁定用户提示页面展示

点击用户所在行的**[解锁]**按钮，确认解锁后，用户即被解锁。如下图：

图 8-7 解锁用户提示页面

8.1.5 授权

点击用户所在行的**[授权]**按钮，弹出用户授权页面，可以对用户进行授权角色。如下图：

图 8-8 用户授权页面展示

8.1.6 安全性配置

安全性配置主要包括最大在线用户数、密码强度、密码安全性、登录尝试。

最大在线用户数，默认值是 20 个，可以配置范围在 20-100 个。假设配置了 20 个，那么当在线用户个数超过 20 时，是禁止登录的。

密码强度，默认是包含字母、包含数字、长度 6-20 位；假设配置又变更为：

图 8-9 密码强度设置页面展示

那么密码强度不符合该配置的用户登录控制中心，会弹出修改密码界面，在界面标题处也给出了当前密码强度的要求，要求用户安装当前强度要求进行新密码的设定，设定成功后，会自动进入系统界面。如下图：

图 8-10 修改密码页面展示

如果启用了首次登录修改密码，那么用户首次登录会弹出首次登录修改密码对话框，强制用户修改密码后进行登录，以保证用户密码的安全性。如下图：

图 8-11 密码安全性设置页面展示

图 8-12 修改密码页面展示

针对密码过期后的处理有两种方式，警告和强制修改。

8.1.7 锁定解锁配置

用户管理员“admin”用户可以对 IP 锁定时间、同一 IP 连续登录失败次数、用户锁定时间、同一用户连续登录失败次数进行设置，并且能够给被锁定的用户或 IP 解锁。

用户管理员在同一用户登录失败锁定次数的文本框输入 2~5 范围的整数，同一用户登录失败锁定时间的文本框里输入 1~30 范围的整数，点击**[提交]**按钮，即设置了锁定时间及次数。如下图：

图 8-13 登录尝试设置页面展示

用户在同一 IP 登录失败锁定次数的文本框输入 2~5 范围的整数，同一 IP 登录失败锁定时间的文本框里输入 1~30 范围的整数，点击**[提交]**按钮，即设置了锁定时间及次数。如下图：

图 8-14 登录尝试页面展示

同一用户连续登录失败次数达到设定参数时，会提示如下错误。

图 8-15 多次登录失败锁定用户提示页面

同一 IP 连续登录失败次数达到设定参数时，会提示如下错误。

图 8-16 相同 IP 多次登录失败锁定提示页面

IP 解锁菜单下点击锁定 IP 所在的行“ ”图标，确认解锁后，IP 地址即被解锁。如下图：

图 8-17 IP 解锁页面展示

用户解锁菜单下点击锁定用户所在的行“ ”图标，确认解锁后，用户即被解锁。如下图：

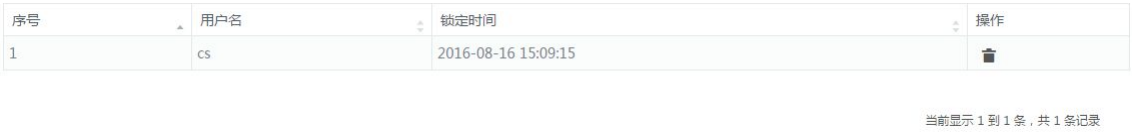

图 8-18 用户解锁页面展示

注意

当同一用户锁定次数和同一 IP 锁定次数配置相同时 ,优先锁定用户。

8.2 角色列表

用户管理员“admin”用户。用户管理员可以对角色进行新建、编辑、删除、授权操作。如下图：

图 8-19 角色列表页面展示

8.2.1 新建角色

点击**[新建]**按钮添加角色。如下图：

图 8-20 新建角色页面展示

8.2.2 编辑角色

点击**[编辑]**按钮，修改角色信息，如下图：

图 8-21 修改角色页面展示

8.2.3 删除角色

点击**[删除]**按钮，可以删除角色，但系统默认的用户管理员和审计管理员角色不让删除。如下图：

图 8-22 删除角色提示页面

8.2.4 授权

点击**[授权]**按钮，可以给角色授权，如下，针对该角色授权了哪些功能模块，则该角色下的用户登录控制中心，只能显示相应的授权模块，其他模块处于屏蔽状态。如下图：

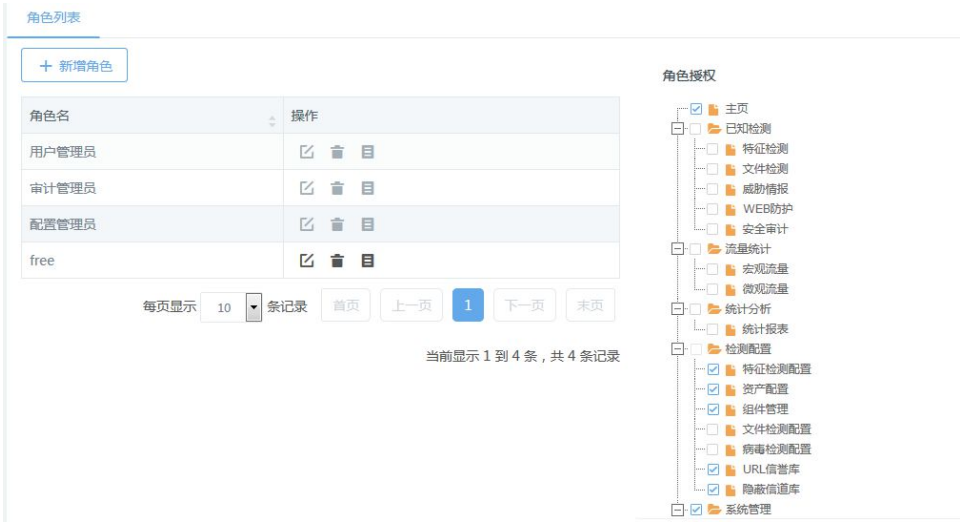

图 8-23 角色授权页面展示

8.3 审计日志

审计日志记录用户的关键操作，只有审计员角色能查看审计日志。如下图：

图 8-24 审计日志信息页面展示

8.3.1 查询审计日志

可以根据操作员、内容、用户 IP、日志记录时间（全部、1 天、1 周、1 个月、自定

义）筛选查询审计日志。如下图：

图 8-25 审计日志查询页面

8.3.2 导出审计日志

导出审计日志便于查看，导出格式为 xls；可以用 Excel 打开。

点击**[导出]**按钮弹出保存对话框如下图所示：

图 8-26 导出日志页面展示

注意

导出 xls 文件时，由于个人机器环境不同，有可能无法弹出确认对话框，而是 IE 直接调用已安装的 EXCEL 软件把

需要下载的文件打开 ,这时只能通过 IE 的后退功能返回到报表文件列表页面。

8.3.3 清除审计日志

点击**[清除]**按钮，可以进行审计日志全部删除。如下图：

图 8-27 删除审计日志提示页面

点击**[确定]**按钮，所查询的审计日志都会被删除。

8.3.4 更改IE直接在页面打开下载文件

如果需要修改 IE 直接在页面打开下载文件的方式，可以通过以下步骤实现：

打开我的电脑，选择菜单—>工具—>文件夹选项，选择文件类型选项，在已注册的文件类型中选择需要更改的文件类型如：xls，选择高级按钮，勾选下载后确认打开，不勾选在同一窗口中浏览，点击**[确定]**按钮，设置完毕。重新启动 IE，看是否会弹出确认对话框。

8.3.5 翻页功能

日志每页默认显示 20 条，后面有总的页码数，点击分页按钮可以分页查看每页日志。可以通过按钮实现向前、先后翻页，以及首页、末页跳转。如下图：

图 8-28 翻页功能展示

可以动态设置每页显示记录条数。如下图所示：

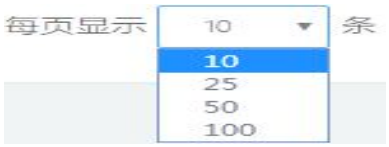

图 8-29 设置每页记录条数展示

附录 1 系统日志备份

系统日志数据备份

系统日志包括：检测事件（包含：特征事件、隐蔽信道、URL 信誉检测、病毒检测、文件检测）日志和运行日志。各日志的备份分别通过日志导出和生成报表的方式进行，在确定相应日志成功备份后，方可进行磁盘清理和数据清理工作。

特征事件日志

通过日志导出进行备份、报表任务进行记录。

日志导出备份：

进入系统**已知检测>特征检测**，根据时间筛选需备份的日志，点击**[导出]**按钮，会后台执行导出操作，成功导出后，重要消息会有提示，通过计划任务进入导出结果日志查询模块，点击操作列中的**[下载]**按钮，实现日志导出备份功能。如下图：

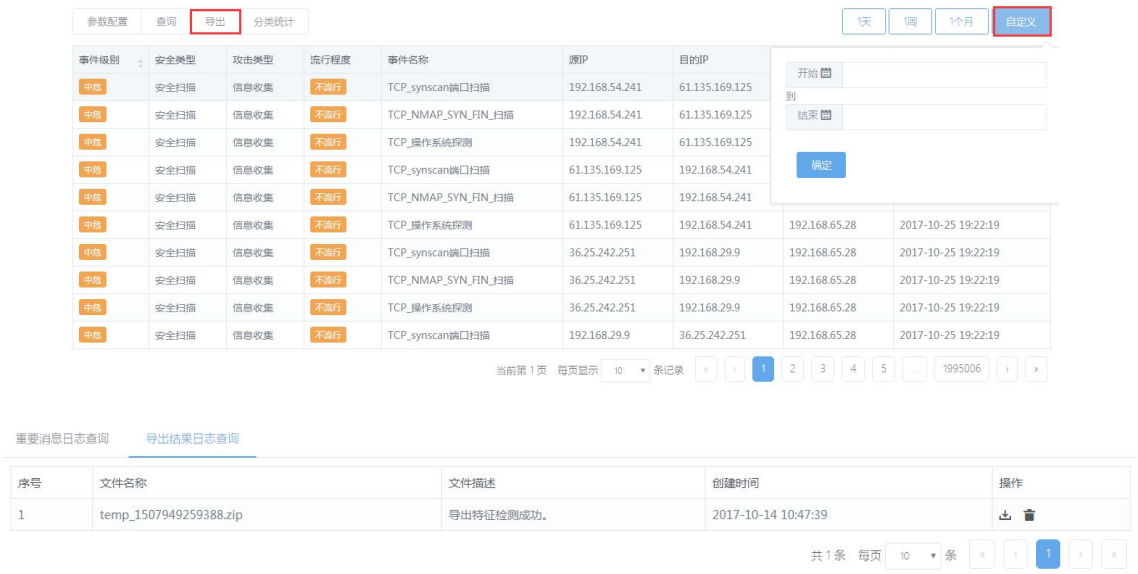

图 附录 1-1 导出备份日志页面展示

日志报表记录：

系统提供四种形式的报表统计特征检测日志，具体操作请参考 5.1 报表任务配置、5.2 报表执行结果，将报表结果下载备份。

隐蔽信道日志：

通过隐蔽信道日志导出进行备份。具体操作参考 3.4.1 隐蔽信道中的导出，将导出的文件下载备份。

恶意 URL 日志：

通过恶意 URL 日志导出进行备份。具体操作参考 3.4.2 恶意 URL 中的导出，将导出的文件下载备份。

病毒检测：

通过病毒检测日志导出进行备份。具体操作参考 3.2.4 病毒检测中的导出，将导出的文件下载备份。

文件检测：

通过文件检测日志导出进行备份。具体操作参考 3.3 文件检测中的导出，将导出的文件下载备份。

基础统计报表记录：

系统提供基础统计报表记录基本分析日志，具体操作请参考 5.1 报表任务配置、5.2 报表执行结果，将报表结果下载备份。

运行日志

系统运行日志支持导出备份，具体操作请参考 7.4.1 运行日志中的导出，将结果下载备份。

附录 2 引擎配置说明

引擎利用超级终端进行基本设置，配置好超级终端以后，回车进入引擎启动画面。如图所示：

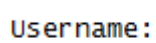

图 附录 2-1 进入引擎界面展示

输入用户名：adm，回车后再输入正确的密码（出厂密码设置为 Raven.public）后进入如图所示：

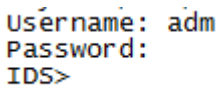

图 附录 2-2 输入账号、密码页面展示

基本功能介绍及对应命令

配置选项：

【功能 1】：显示当前设置

显示当前配置信息。包括产品 ID 号、设备序列号、通讯网口的 IP 地址、子网掩码、路由配置等信息，在“IDS>”模式下可以通过 enable 命令进入“IDS#”模式；在“IDS#”模式下可以通过 configure terminal 命令进入“IDS(config)#”模式；

“IDS#”模式下命令：show config ；

```
IDS# show config
************************************************************
Current product_info.id is NULL
Current Serial:

  eth0 :    Communicate 192.168.11.  ./255.255.255.0


SLOT 1
  ge1/0:    Capture
  ge1/1:    Capture
  ge1/2:    Capture
  ge1/3:    Capture
  ge1/4:    Capture
  ge1/5:    Capture
  ge1/6:    Capture
  ge1/7:    Capture


SLOT 0
 xge0/0:    Capture
 xge0/1:    Capture


Current VCECOMM PORT: 20001
Current Route:
Gateway[1]: <0.0.0.0/0.0.0.0> <192.168.11.1>
allow access:   ping   telnet   ssh
************************************************************
```

图 附录 2-3 show config 信息

【功能 2】：更改 IP 地址/子网掩码

更改通讯网口的 IP 地址及子网掩码。引擎的 IP 地址及子网掩码请向网络管理员申请。

修改方式：“IDS (config)#”模式下命令：ip address；

如将 ip 地址改为 192.168.11.182，24 位掩码时，命令如下图：

```
IDS(config)# ip address 192.168.11.182/24
```

图 附录 2-4 更改 IP 地址页面展示

【功能 3】：重置引擎认证密钥

可以重置控制中心与引擎认证密钥，当引擎与不同于原控制中心的另外控制中心相连时必须重置密钥。

“IDS(config)#”模式下命令：reset vcecomm key；

命令如下图：

```
IDS(config)# reset vcecomm key
Key will be reset
Agree?
    (1)==yes
    (2)==no
->1
Key has been reset
```

图 附录 2-5 重置引擎认证密钥页面展示

【功能 4】：更改路由配置

可以添加和更改原有路由配置。

“IDS(config)#”模式下命令： route add | del；

举例：

添加路由

输入网关 IP 地址：与要设定路由的网口地址在同一个网段内。

IDS(config)#route add 0.0.0.0/0 192.168.11.1

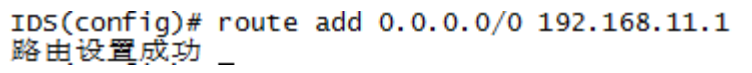

图 附录 2-6 更改路由页面展示

删除路由：IDS(config)# route del；

举例：删除上一步添加的路由：

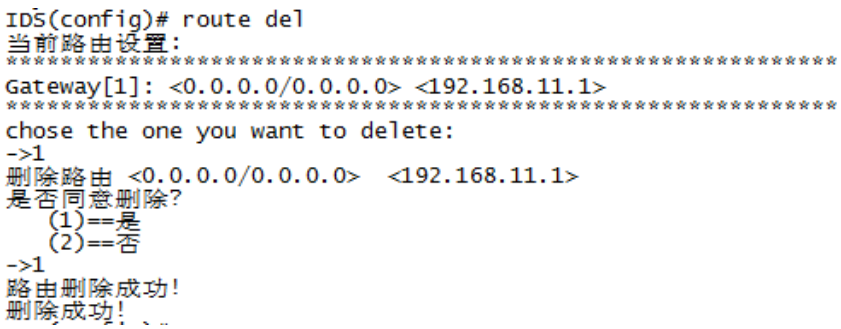

图 附录 2-7 删除路由页面展示

【功能 5】：更改串口登录口令

可更改网络引擎密码。网络引擎密码为不少于 6 位的任意数字或字符。新密码输入少于 6 位时，会提示错误信息“Password of user is too short, should longer than or equal to 6!”。

注：

（1）新引擎出厂时密码统一为“Raven.public”，请注意更改。

（2）密码设置不要过于简单，以免被盗用。

“IDS(config)#”模式下命令：adm-set-new-password 新密码；

如设置新密码为“Raven4000”时，命令如下：

“IDS(config)# adm-set-new-password Raven4000”

【功能 6】：打开和关闭 SSH 登录

用于打开是否支持通过 SSH 登录本配置界面，缺省为打开。

“IDS(config)#”模式下命令：allow access ssh enable / disable；（其中，enable 代表打开，disable 代表禁用）

【功能 7】：允许和禁止 Ping 入

打开后可以使设备管理口被 ping 通。

“IDS(config)#”模式下命令：allow access ping enable / disable；（其中，enable 代表打开，disable 代表禁用）

【功能 8】：允许和禁止 telnet 登录

用于打开是否支持通过 telnet 登录本配置界面，缺省为打开。

“IDS(config)#”模式下命令：allow access telnet enable / disable；（其中，enable 代表打开，disable 代表禁用）

【功能 9】：用户自定义通讯端口

用户自定义通讯端口可以修改引擎的通讯端口，缺省为 20001，当 20001 端口被占用时可以修改成其他的数值。

“IDS(config)#”模式下命令：set vcecomm xxx（xxx 表示端口号）；

如要设置新的通讯端口为 2001，命令如下：

“IDS(config)# set vcecomm 2001”

【功能 10】：设置网口协商模式

“IDS(config)#”模式下命令：set if-parameters xxx（xxx 表示网卡名）；

举例：设置网卡 ge1/2 的协商模式为自协商：

```
IDS(config)# set if-parameters ge1/2
autoneg :[  on       |      off       ]
speed   :[ 10 | 100 | 1000 | 10000 ]
duplex  :[  half     |     full       ]
please input format like autoneg/speed/duplex
->on
设定成功!
```

图 附录 2-8 设置网口自协商模式展示

设置网卡 ge1/2 的协商模式为非自协商，1000，全双工：

```
IDS(config)# set if-parameters ge1/2
autoneg :[  on       |      off       ]
speed   :[ 10 | 100 | 1000 | 10000 ]
duplex  :[  half     |     full       ]
please input format like autoneg/speed/duplex
->off/1000/full
设定成功!
IDS(config)#
```

图 附录 2-9 设置网口非自协商展示

【功能 11】：授权管理

显示引擎序列号，授权类型，抓包口数量，威胁检测服务期，流量检测与分析服务期，APT 静态检测与动态联动服务期。

“IDS#”模式下命令：show license ；

如下图：

```
IDS# show license
激活时间:                          Wed Jun 27 14:33:02 2018
入侵特征库授权到期时间: Wed Jun 24 11:11:28 2020
病毒特征库授权到期时间: Thu Jun 27 14:33:02 2019
静态检测授权到期时间:   Thu Jun 27 14:33:02 2019
动态检测授权到期时间:   Thu Jun 27 14:33:02 2019
专业WEB服务器攻击检测:  未授权
抓包口总数:                        5
```

图 附录 2-10 授权管理页面展示

【功能 12】：用户自定义抓包口：根据用户需要调整网口的抓包口，管理口和备用管理口不能调整为抓包口。

“IDS(config)#”模式下命令：set capcomm ；

如设置第一个板卡的第二个口为抓包口，命令如下图：

```
IDS(config)# set capcomm
Input format as:
0:0-0:1-1:0-1:1-2:0
interface 0:0,0:1,1:0,1:1,2:0 will be setted to capture:
->1:1
抓包口设置完毕
IDS(config)#
```

图 附录 2-11 用户自定义抓包口设置展示

【功能 13】：重启引擎操作系统

“IDS#”模式下命令：reboot；

命令如下图：

```
IDS# reboot
The system will be rebooted! Please enter "y/n"  to confirm:  y
```

图 附录 2-12 重启引擎页面展示

【功能 14】：PING 测试

PING 测试，用于测试指定 IP 地址是否存在活动主机，提示信息为“连接正常”或者“连接异常”。

“IDS#”模式下命令：ping A.B.C.D(A.B.C.D 表示 IP 地址)；

如 ping 192.168.11.197，连接正常时，显示如下图：

```
IDS# ping 192.168.11.197
PING 192.168.11.197 (192.168.11.197): 56 data bytes
64 bytes from 192.168.11.197: seq=0 ttl=128 time=0.296 ms
64 bytes from 192.168.11.197: seq=1 ttl=128 time=0.481 ms
64 bytes from 192.168.11.197: seq=2 ttl=128 time=0.460 ms
64 bytes from 192.168.11.197: seq=3 ttl=128 time=0.436 ms

--- 192.168.11.197 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.296/0.418/0.481 ms
```

图 附录 2-13 PING 测试页面展示

【功能 15】：TRACEROUTE 测试

TRACEROUTE 测试，用于测试引擎能否成功路由到指定 IP。

“IDS#”模式下命令：traceroute A.B.C.D(A.B.C.D 表示 IP 地址)；

如下图：

```
IDS# traceroute 192.168.13.1
traceroute to 192.168.13.1 (192.168.13.1), 30 hops max, 46 byte packets
 1  192.168.13.1 (192.168.13.1)  0.654 ms  0.368 ms  0.788 ms
```

图 附录 2-14 TRACEROUTE 测试页面展示

【功能 16】：显示引擎版本

显示当前引擎的版本信息。

“IDS#”模式下命令：show version packet；

命令如下图，其中 PSKey 显示的就是引擎版本：

```
IDS# show version packet
PSKey: 0700R0402B20180108103526
```

图 附录 2-15 显示引擎版本页面展示

【功能 17】：显示控制中心 IP 地址

“IDS#”模式下命令：show connect；

命令如下图所示：

```
IDS# show connect
************************************************************
控制端IP地址:192.168.11.182
************************************************************
```

图 附录 2-16 控制中心 IP 地址显示页面

【功能 18】：退出串口配置程序

退出串口配置程序；如果不退出，用户可以通过串口无需登录而直接操作串口配置

“IDS#”模式下命令：exit；

注：超级终端不能用窗口右上脚的关闭按钮直接关闭，因为这样只关闭了“超级终端”的界面，而超级终端与探测引擎的通讯并未关闭。因此，每次更改探测引擎的基本参数后，必须用 exit 命令退出。

【功能 19】：用户忘记 adm 用户密码，恢复方式：

当 adm 用户忘记登录密码后，可以通过 admin 用户登录进行密码的重置，admin 用户登录用户名默认为：admin，密码为：Raven.private；

在“IDS(config)#”下通过 user administrator USER local PASSWORD priv all 命令进行用户密码重置。

举例：将 adm 用户密码重置为 Raven.public：

```
IDS(config)# user administrator adm local venus70 priv all
```

图 附录 2-17 忘记密码恢复方式页面

【功能 20】：查看网口运行态势：

adm 用户登录，在“IDS#”下 show interface 即可，如果想查看具体某个网口的收发包情况，show interface [INTERFACE_NAME]。

举例：查看 ge1/1 网口的运行情况；

```
IDS# show interface ge1/1
ge1/1     Link encap:Ethernet  HWaddr 00:10:F3:63:CE:92
          UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

图 附录 2-18 查看网口运行态势页面展示

【功能 21】：配置 SNMP 团体字：

adm 用户登录，进入 IDS(config)#模式下，利用命令 snmp community 配置 SNMP 团体字：

```
IDS(config)# snmp community public
```

图 附录 2-19 配置 SNMP 团体字展示

进入 IDS#模式，利用命令 show snmp community 进行引擎 SNMP 团体字查询。

```
IDS# show snmp community
#          sec.name  source          community
com2sec venus      default         SNMPPublic
com2sec6 venus     default         SNMPPublic
```

图 附录 2-20 引擎 SNMP 团体字查询展示

【功能 22】：管理口切换：

支持切换抓包口作管理口，完成后，只能使用切换后的管理口。

默认使用管理口 eth0：

```
IDS# show config

************************************************************
Current product_info.id is NULL
Current Serial: [redacted]

  eth0 :    Communicate 192.168.11.182/255.255.255.0


SLOT 1
  ge1/0:    Unused
  ge1/1:    Capture
  ge1/2:    Unused
  ge1/3:    Unused
  ge1/4:    Unused
  ge1/5:    Unused
  ge1/6:    Unused
  ge1/7:    Unused


SLOT 0
 xge0/0:    Unused
 xge0/1:    Unused


Current VCECOMM PORT: 20001
Current Route:
Gateway[1]: <0.0.0.0/0.0.0.0> <192.168.11.1>
allow access:   ping   telnet
************************************************************
```

图 附录 2-21 管理口切换展示

切换抓包口为管理口，若抓包口此时处于启用状态（capture），则需要确认操作：

```
IDS(config)# set  communication interface ge1/1
[ge1/1] now is capture nic, set to communicate nic?
    (1)==yes
    (2)==no
->1
```

图 附录 2-22 查修改管理口为 ge1/1

切换后，使用 ge1/1 口作为管理口。

管理口切换后需要配置一次 IP 地址及路由信息，配置后，IP 地址、路由信息被永久保存，以后切换无需再次进行该次配置即可正常使用，配置方法参考功能 2、功能 4。

【功能 23】：查看硬件信息：show hardware info。

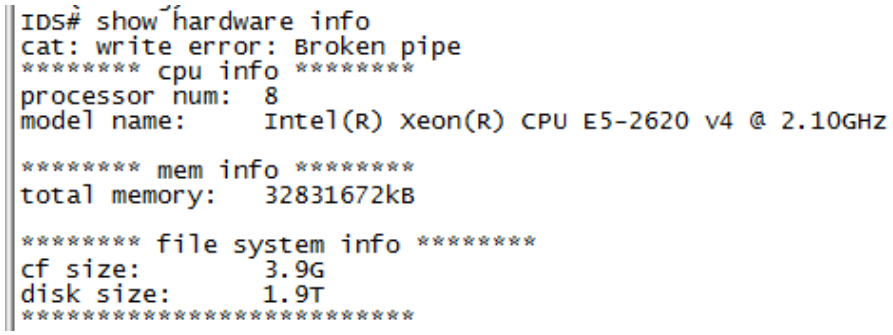

图 附录 2-23 查看硬件信息展示

初始应用

第一次安装应该配置引擎通讯 IP 地址，出厂缺省地址为：192.168.0.200；（如果数据中心和 IDS 引擎是跨网段控制，需要使用“更改路由配置”来设置相关路由信息。）

配置完毕以后可以使用辅助选项中的“PING 测试”和“TRACEROUTE 测试”来检查是否可以和网络连通。

当重新安装了数据中心或更改了数据中心的主机地址，需要使用“重置引擎认证密钥”来清除原来的认证信息保证和新的数据中心建立认证关系。

更改引擎 IP、路由的方法和过程见附录 2 功能 2、功能 4 描述。

HIRSCHMANN IT

A BELDEN BRAND