



网络安全关口监测系统

用户使用说明书



©2015 长安通信

■版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**长安通信科技有限责任公司**（简称**长安通信**）所有，受到有关产权及版权法保护。任何个人、机构未经**长安通信**的书面授权许可，不得以任何方式复制或引用本文的任何片断。

长安通信科技有限责任公司

网站：<http://www.chanct.com/>

电子信箱：gms-support@chanct.com

服务热线：400-070-6665

目录

前言	1
概述	1
读者对象	1
内容简介	1
格式约定	2
1 章节 产品说明	3
1.1 术语表	3
1.1.1 名词解释	3
1.2 产品说明	4
1.2.1 型号及外观	4
1.2.2 硬件规格	5
2 章节 详细使用说明	6
2.1 首页展示	6
2.1.1 用户登录	6
2.1.2 logo 栏展示内容和功能	8
2.1.3 今日分类事件统计	9
2.1.4 最近流量曲线	11
2.1.5 系统状态	14
2.1.6 今日 TOP5 被攻击 IP	16
2.1.7 事件实时监控	18
2.2 查询	20
2.2.1 流量分析 (2.3 版本功能)	20
2.2.2 恶意代码感染事件查询	41
2.2.3 网站事件查询	45
2.2.4 通信行为异常事件查询	50
2.2.5 恶意代码传播事件查询	54
2.2.6 恶意 URL 访问事件查询	59
2.2.7 攻击尝试事件查询	64
2.2.8 其他事件查询	69
2.2.9 流量查询	74
2.3 报表	76

2.3.1 报表下载	76
2.4 系统管理.....	78
2.4.1 节点管理（2.3 版本功能）	78
2.4.2 设备管理	79
2.4.3 网络配置	83
2.4.4 用户管理	85
2.4.5 捕包设置（2.3 版本不具备此功能）	88
2.4.6 引擎设置	89
2.4.7 时间设置	93
2.4.8 预警管理	98
2.4.9 升级设置	100
2.4.10 维护设置.....	102
2.4.11 重要用户	103
2.4.12 自定义流量.....	107
2.4.13 白名单配置.....	110
2.4.14 系统操作日志.....	113
2.5 授权.....	116
2.5.1 WEB 界面登录.....	116
2.5.2 填写授权申请.....	116
2.5.3 导出授权申请文件.....	117
2.5.4 获取授权文件.....	118
2.5.5 授权文件导入.....	119
2.5.6 授权成功提醒.....	119

插图

图 1-1 GMS1140-E 外观示意图.....	4
图 1-2 GMS1280-E 外观示意图.....	4
图 1-3 硬件规格	5
图 2-1 logo 栏效果图	8
图 2-2 今日事件分类统计效果图.....	9
图 2-3 最近流量曲线	12
图 2-4 系统状态	14
图 2-5 拓扑图的图层	15
图 2-6 今日 TOP5 被攻击 IP.....	16
图 2-7 事件实时监控展示.....	18
图 2-8 用户数统计粒度分钟查询效果.....	21
图 2-9 用户数统计粒度小时查询效果.....	22
图 2-10 用户数统计粒度小时查询效果.....	22
图 2-11 用户数统计粒度月查询效果.....	23
图 2-12 用户归属地分布粒度分钟查询效果.....	24
图 2-13 用户归属地分布粒度小时查询效果.....	24
图 2-14 用户归属地分布粒度天查询效果.....	25
图 2-15 用户归属地分布粒度月查询效果.....	25
图 2-16 用户浏览器/版本分布粒度分钟查询效果.....	26
图 2-17 用户浏览器/版本分布粒度小时查询效果.....	26
图 2-18 用户浏览器/版本分布粒度天查询效果.....	27
图 2-19 用户浏览器/版本分布粒度月查询效果.....	27
图 2-20 访问时长统计粒度分钟查询效果.....	28
图 2-21 访问时长统计粒度小时查询效果.....	29
图 2-22 访问时长统计粒度天查询效果.....	29
图 2-23 访问时长统计粒度月查询效果.....	29
图 2-24 访问次数统计粒度分钟查询效果.....	31
图 2-25 访问次数统计粒度小时查询效果.....	31

图 2-26 访问次数统计粒度天查询效果	32
图 2-27 访问次数统计粒度月查询效果	32
图 2-28 用户流量统计粒度分钟查询效果	33
图 2-29 用户流量统计粒度小时查询效果	33
图 2-30 用户流量统计粒度天查询效果	34
图 2-31 用户流量统计粒度月查询效果	34
图 2-32 TCP 连接成功率统计粒度分钟查询效果	35
图 2-33 TCP 连接成功率统计粒度小时查询效果	35
图 2-34 TCP 连接成功率统计粒度天查询效果	36
图 2-35 TCP 连接成功率统计粒度月查询效果	36
图 2-36 网银访问成功率统计粒度分钟查询效果	37
图 2-37 网银访问成功率统计粒度小时查询效果	37
图 2-38 网银访问成功率统计粒度天查询效果	38
图 2-39 网银访问成功率统计粒度月查询效果	38
图 2-40 端到端时延统计粒度分钟查询效果	39
图 2-41 端到端时延统计粒度小时查询效果	39
图 2-42 端到端时延统计粒度天查询效果	40
图 2-43 端到端时延统计粒度月查询效果	40
图 2-44 恶意代码感染事件查询效果	41
图 2-45 网站事件查询效果展示图	46
图 2-46 通信行为异常事件查询效果展示图	50
图 2-47 恶意代码传播事件查询效果展示图	55
图 2-48 恶意 URL 访问事件查询	60
图 2-49 攻击尝试事件查询	65
图 2-50 其他事件查询	70
图 2-51 流量查询效果展示图	74
图 2-52 报表下载效果展示图	76
图 2-53 节点管理效果展示图	79
图 2-54 设备管理效果展示图	80
图 2-55 网络配置效果展示图	84
图 2-56 用户管理效果展示图	86
图 2-57 捕包设置效果展示图	88
图 2-58 引擎设置效果展示图	90
图 2-59 时间同步效果展示图	93
图 2-60 预警管理效果展示图	98

图 2-61 升级管理效果展示图.....	100
图 2-62 调试配置效果展示图.....	102
图 2-63 重要用户	104
图 2-64 自定义流量配置效果展示图.....	107
图 2-65 白名单配置效果展示图.....	111
图 2-66 操作日志查看效果展示图.....	114
图 2-67 关口 web 界面登录.....	116
图 2-68 关口 web 界面展示.....	116
图 2-69 授权申请填写界面.....	117
图 2-70 授权申请导出界面.....	118
图 2-71 授权申请导出路径界面.....	118
图 2-72 授权导入界面	119

前言

概述

对网络安全关口监测系统的常规功能使用进行详细说明。以便系统使用者随时查阅。

读者对象

网络安全关口监测系统使用者。

内容简介

章节	概述
章节一	产品说明，包括 1. 术语表：名词解释 2. 产品说明：型号及外观，硬件规格
章节二	详细使用说明，包括 1. 首页展示：用户登录，logo 栏展示内容和功能，今日事件分类统计，最近流量曲线，系统状态，今日 TOP5 被攻击 IP，事件实时监控 2. 查询：流量分析（2.3 版本功能），恶意代码感染事件，网站事件，通信行为异常事件，恶意代码传播事件，恶意 URL 访问事件查询，攻击尝试事件查询，其他事件查询，流量查询 3. 报表下载：日报表，周报表，月报表，年报表（均支持 word 格式） 4. 系统管理：节点管理（2.3 版本功能），设备管理，网络配置，用户管理，捕包设置（2.3 不具备此功能），时间设置，预警管理，升级管理，维护设置，重要用户配置，自定义流量配置，白名单配

章节	概述
	置, 操作日志查看 5. 系统授权。

格式约定

符号	说明
粗体字	菜单、命令和关键字
斜体字	文档名、变量
 说明	对描述内容的补充和引用信息
 提示	使用设备时的技巧和建议
 注意	需要特别注意的事项和重要信息

1 章节 产品说明

1.1 术语表

1.1.1 名词解释

缩写、术语	解释
GMS	网络安全关口监测系统 (Gateway Monitor System) 英文简称。
DNS	DNS (Domain Name System) 域名系统。
HTTP	超文本传输协议 (HTTP, HyperText Transfer Protocol)。
HTTPS	以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。
TCP	Transmission Control Protocol 传输控制协议。
SSH	SSH 为 Secure Shell 的缩写，安全外壳协议。
特征事件	指特征监测获取的木马、僵尸网络恶意活动事件、恶意代码感染与传播事件。
安全事件	包括特征事件、恶意代码传播事件、通信行为异常事件、恶意 URL 访问事件、流量事件。
异常记录	基于行为分析产生的异常行为记录
黑名单	主要包括：恶意 URL、域名、IP。
系统版本	指系统软件版本号。
特征库版本	病毒库版本号。
最大上传/下载速度	指跟阿里云外网交互时占用宽带的大小。

1.2 产品说明

1.2.1 型号及外观

一、 GMS1140-E 百兆关口设备

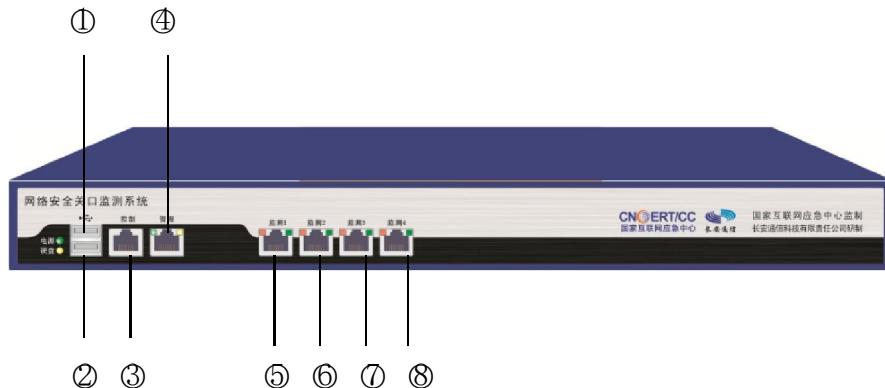


图1-1 GMS1140-E 外观示意图

说明：

- ①②为 USB 接口；
- ③为控制口，连接 Console 线，进入串口设置模块；
- ④为管理口，连接 RJ45 网线，需接入互联网；
- ⑤⑥⑦⑧为电口监测口，连接 RJ45，接入监测流量。

二、 GMS1280-E 千兆关口设备

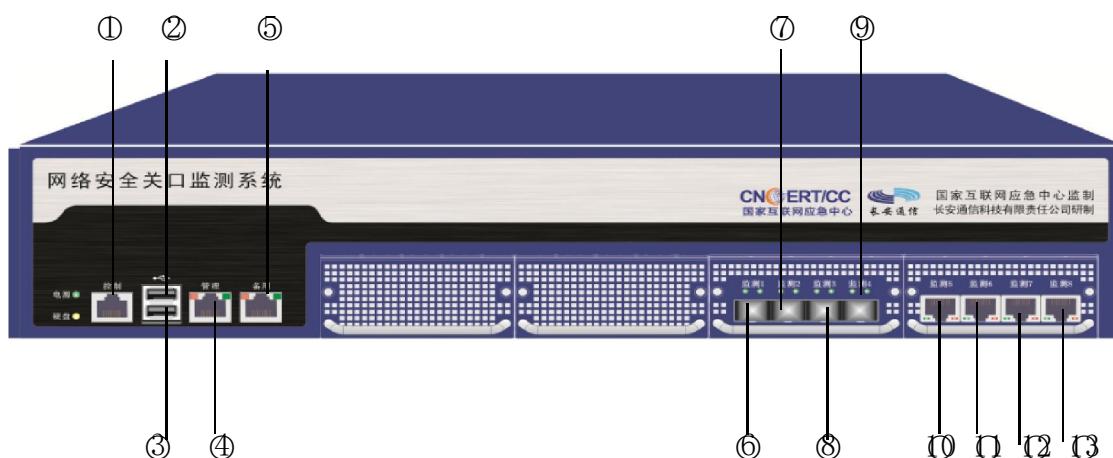


图1-2 GMS1280-E 外观示意图

说明：

- ①为控制口，连接 Console 线，进入串口设置模块；
 ②③为 USB 接口； ④为管理口，连接 RJ45 网线，需接入互联网；
 ⑤为备用口，连接 RJ45 网线，需接入互联网，④和⑤二选一接入互联网即可；
 ⑥⑦⑧⑨为光口监测口，连接光纤，接入监测流量；
 ⑩⑪⑫⑬为电口监测口，连接 RJ45 网线，接入监测流量。

1.2.2 硬件规格

硬件指标	百兆 GMS1140-E	千兆 GMS1280-E
平台	X86架构的专用网络安全平台	
高度	1U	2U
CPU	单路4核	双路6核
内存	16G	32G
硬盘	1T以上	2T以上
管理口	千兆	千兆
捕包口	四光/四电	四光四电
电源	350W	760W
USB	2	2
Console口	RJ45*1	RJ45*1

图1-3 硬件规格

2 章节 详细使用说明

2.1 首页展示

2.1.1 用户登录

通过 WEB 登录，登录地址 <https://192.168.0.171> (192.168.0.171 为设备的默认管理 IP 地址)。

操作说明：

- 1、设备默认用户名：admin，密码：123456。
- 2、进入登录界面。



- 3、用户名和密码、验证码有一项输入错误或者用户被锁定，都会有提示，用户输入错误的用户名系统会提示“用户不存在”，用户输入错误的验证码会在验证码右侧出现红叉提示，用户在 5 分钟内连续错误输入密码登录 10 次，用户将被锁定。非管理员用户，需要管理员解锁，如果管理员被锁，2 分钟后自动解锁。

网络安全关口监测系统

用户名	jskd	用户不存在
密码	*****	
验证码	j80l	NB8V
威胁等级	事件名	发生时间

登录

网络安全关口监测系统

用户名	admin	
密码	*****	
验证码	nv88	NB8V 
威胁等级	事件名	发生时间

登录

网络安全关口监测系统

admin的剩余登陆次数：9

用户名	admin	
密码	*****	密码错误
验证码	242b	ZFX2

登录

4、输入正确的用户名和密码后，进入界面，如果30分钟内没有任何操作，系统将自动退出系统返回登录界面。

5、用户想要退出可点击首页退出按钮，然后点击“是”，退出系统返回登录界面。



2.1.2 logo 栏展示内容和功能

此模块展示了系统相关的 logo、热线电话、用户登录信息和授权状态。



图2-1 logo 样例图

此模块可进行的操作：

1、点击向右箭头标退出系统。



2、点击用户名可以更改密码。



3、点击授权信息钮可查看当前授权状态。



授权

1. 请填写如下授权申请信息，并导出授权申请文件：

申请人：	xx
联系电话：	1234567890
单位地址：	xicheng
合同编号：	333
设备名称：	100监测
设备ID：	M788-HMAF-CCRV
设备IP：	172.31.100.100
设备类型：	监测点设备

2. 请将授权申请文件发送至邮箱: gms-support@chanct.com

3. 请将收到的授权文件导入：

网络安全关口监测系统授权状态：

- 授权状态：永久授权
- Cncert深度报文检测引擎：永久授权
- Cncert病毒检测引擎：永久授权
- Cncert异常通信行为监测引擎：永久授权
- 最大入口流量：1000
- 升级剩余时间：永久授权

导出申请

保存

2.1.3 今日分类事件统计

此模块主要提供了今日实时的事件总数和七种事件发生次数的分类统计以及它们最近 7 天的事件数据统计，分别为：恶意代码感染事件、网站事件、通讯行为异常事件、恶意代码传播事件、恶意 URL 访问事件、攻击尝试事件和其他事件。



说明 今日事件总条数：通过动态的翻盘展示实时的动态信息。



说明 七种事件发生次数：以不同颜色的柱状图形式展示，鼠标移动到对应的柱状图会出现相对应的事件发生次数。图表标题为事件类型，横坐标为日期（年月日格式），纵坐标为事件数量。



图2-2 今日事件分类统计效果图

一、 此模块可进行的操作：

点击翻牌数字或某类事件对应的柱状图，能够弹出图层，以柱状图显示所有事件或某类事件最近 7 天（不含今日）的事件数量。查看今日事件时可以执行自选和全部的放大查看功能。

二、 此模块的操作流程：

- 1、进入界面；

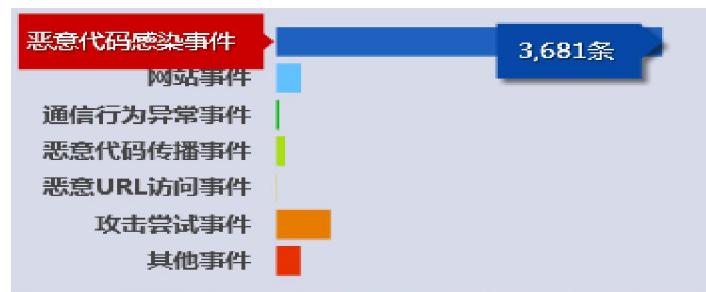
2、左上角可以看到今日事件的统计数以翻牌的形式在统计；



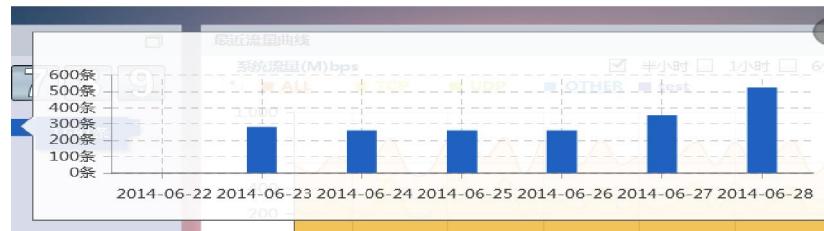
3、单击翻牌数字可看到所有事件最近 7 天的统计，将鼠标停滞在某一天的柱状图上可看到各类事件的统计数据；



4、将鼠标停滞在任何一类事件的柱状图上可看到事件的总数；



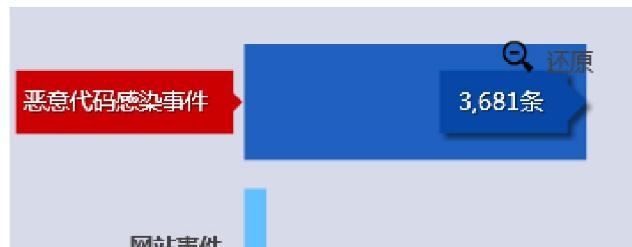
5、单击柱状图可看到此事件最近 7 天的统计；



6、如果感觉事件今日分类事件统计小的话，可以点击其右上角的放大图标“”，可放大。



- 7、如果想要某个或几个柱状图放大，可按住鼠标左键将柱状图选中，松开鼠标左键就可看到放大的效果。



2.1.4 最近流量曲线

默认展示最近半小时的系统流量(ALL/TCP/UDP/OTHER)及需要在首页展示的自定义流量，展示时间提供给用户三种选择：最近半小时、最近1小时、最近6小时；用户可单独查看或组合查看某一类流量。

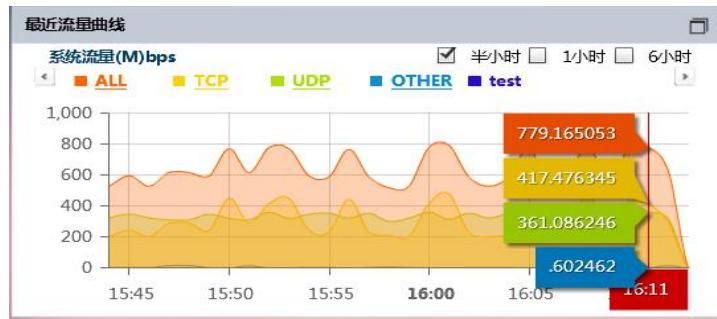


图2-3 最近流量曲线



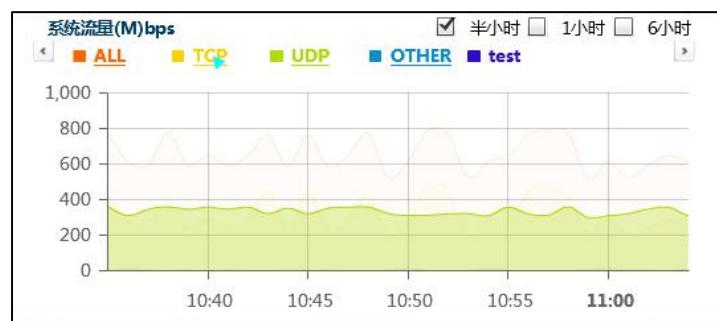
提示 点击流量曲线名称出现下划线，这时候鼠标浮动到流量曲线上会出现该名称的数量指示牌，数量指示牌显示的数据是光标所在位置的该曲线的数据。没有下划线不显示数量指示牌。点击名称前面的小方块，流量名称会变成灰色，不在图中显示该流量曲线。

一、此模块可进行的操作：

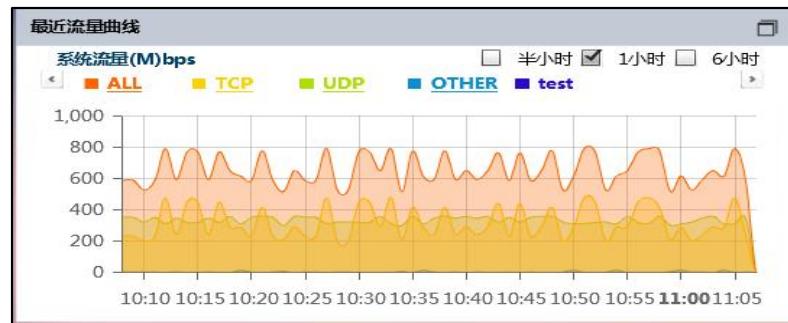
双击如图中的流量曲线的横轴时间跳转到自定义流量查询，自定义流量查询为查询功能中的模块。选择想要查看的流量时段和流量类型组合并可以执行自选和全部的放大查看功能。

二、此模块的操作流程：

- 1、可直接观看某一类型的流量曲线，例如只看“UDP”的，只要将鼠标停滞在 UDP 上即可。



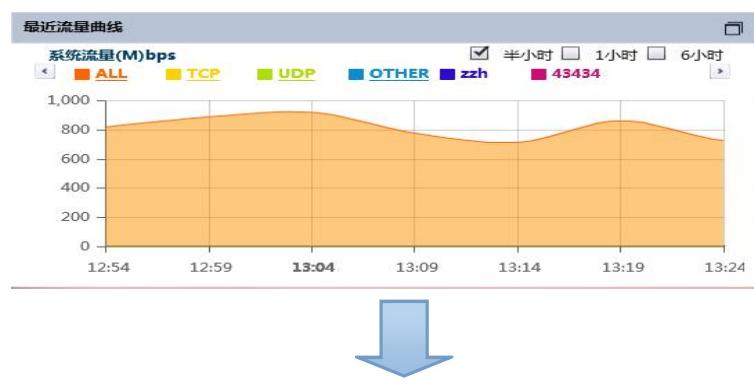
- 2、可选择查看半小时、1小时和6小时的流量。



3、用鼠标左键选中某段流量可放大。



4、点击右上角的放大图标“”，可放大。





5、双击某个时间点可以直接跳转到流量查询页面。

2.1.5 系统状态

默认展示了设备名称、设备的 CPU 占用率、内存占用率、磁盘占用率、系统版本号和特征库的版本信息，可查看设备网络拓扑图。

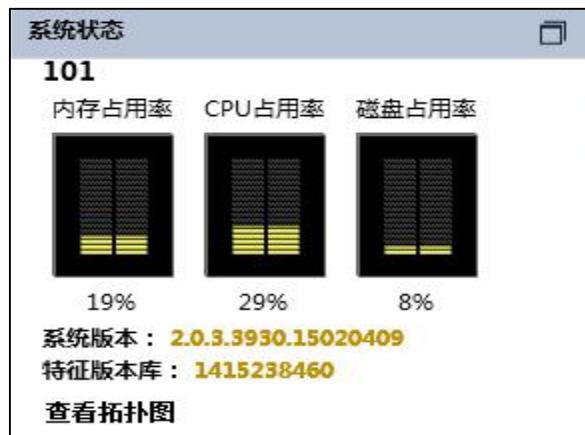


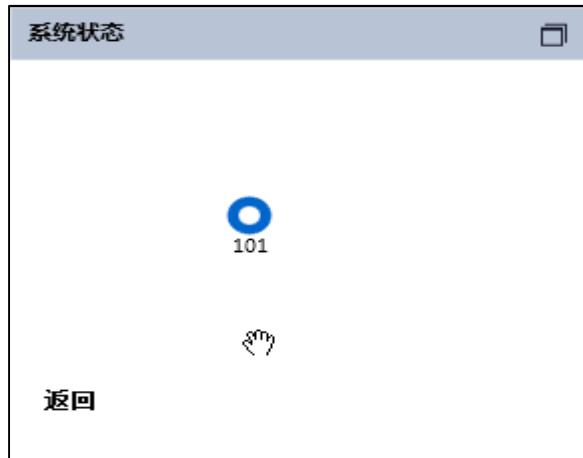
图2-4 系统状态

一、此模块可进行的操作:

点击查看拓扑图，可查看设备的网络拓扑图并可以放大查看。点击返回，可查看设备名称、设备的 CPU 占用率、内存占用率、磁盘占用率、系统版本号和特征库的版本信息。

二、此模块的操作流程:

1、点击查看拓扑图，可查看设备的网络拓扑图。



2、点击右上角的放大图标“”，可放大。

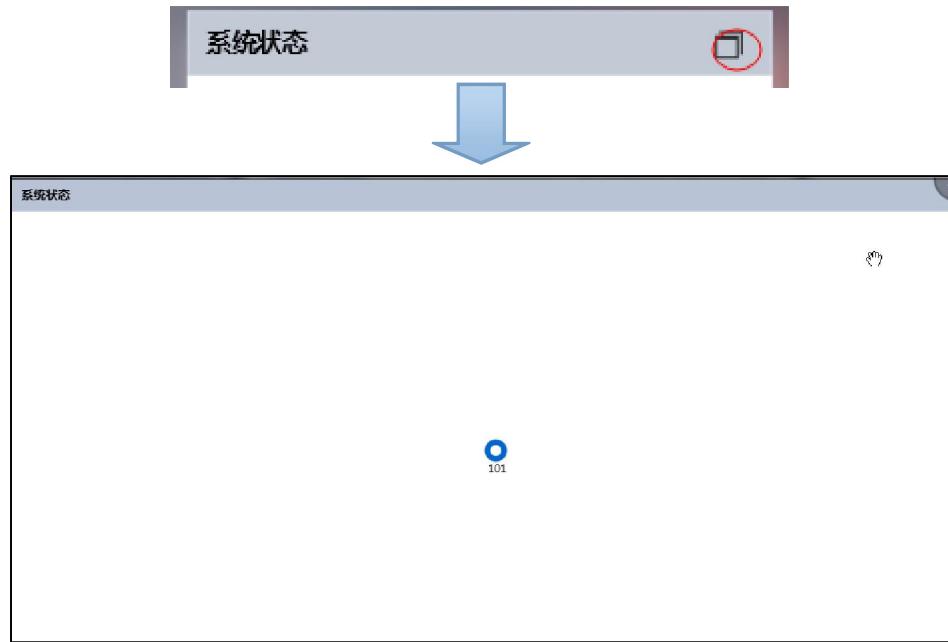
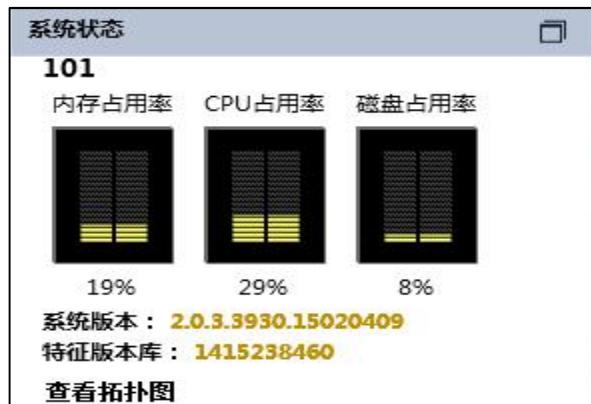


图2-5 拓扑图的图层

3、点击返回，可查看设备系统状态。





2.1.6 今日 TOP5 被攻击 IP

此模块综合统计恶意代码感染事件(感染 IP)/网站事件(网站 IP)/攻击尝试事件(被攻击 IP)/其他事件(被攻击 IP)中被攻击次数最多的 5 个 IP。

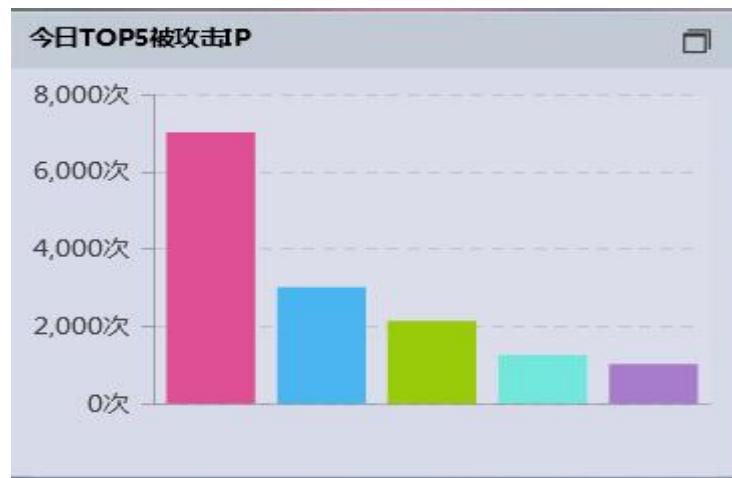


图2-6 今日 TOP5 被攻击 IP

一、 此模块可进行的操作：

当鼠标悬浮在某一柱图上时，能够显示该柱图对应的 IP 及被攻击次数，鼠标移走以上内容消失。查看今日 TOP5 被攻击 IP 时可以执行自选和全部的放大查看功能。

二、 此模块的操作流程：

1、当鼠标悬浮在某一柱图上时，能够显示该柱图对应的 IP 及被攻击次数，鼠标移走以上内容消失。



2、鼠标选中某一柱状图可放大。



3、点击右上角的放大图标 “□”，可放大。



2.1.7 事件实时监控

事件实时监控展示的事件类别为：恶意代码感染事件、网站事件、通信行为异常事件、恶意代码传播事件、恶意 URL 访问事件、攻击尝试事件、其他事件；分别为各类别最新的 20 条事件。

事件实时监控								
恶意代码感染事件		网站事件	通信行为异常事件	恶意代码传播事件	恶意URL访问事件	攻击尝试事件	其它事件	
威胁等级	事件名	发生时间	感染IP	控制端IP	感染端口	控制端端口	设备名称	
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:53	211.94.163.18	42.156.140.222	26570	80	190	
疑似	木马-其他-malicious.URI.C61...	2014-06-29 09:59:53	211.94.163.18	42.156.140.222	26570	80	190	
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:50	211.94.162.115	42.156.140.222	13807	80	190	
疑似	木马-其他-malicious.URI.C61...	2014-06-29 09:59:50	211.94.162.115	42.156.140.222	13807	80	190	
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:50	211.94.163.5	42.156.140.23	39385	80	190	
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:50	211.94.163.217	42.156.140.19	13178	80	190	
疑似	木马-其他-malicious.URI.C61...	2014-06-29 09:59:50	211.94.163.217	42.156.140.19	13178	80	190	

图2-7 事件实时监控展示

一、此模块可进行的操作：

- 1、单击如图上面蓝色的部分可以跳转到对应的事件列表并且每一类事件都可放大查看；
- 2、双击事件下面的某一条事件弹出对应的详细信息。

二、此模块的操作流程：

- 1、选中任何一类事件都可看到最近 20 条事件，用鼠标拉动右侧的下拉框可查看。

事件实时监控							
恶意代码感染事件		网站事件	通信行为异常事件	恶意代码传播事件	恶意URL访问事件	攻击尝试事件	其它事件
威胁等级	事件名	发生时间	感染IP	控制端IP	感染端口	控制端端口	设备名称
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:50	211.94.163.5	42.156.140.23	39385	80	190
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:50	211.94.163.217	42.156.140.19	13178	80	190
疑似	木马-其他-malicious.URI.C61...	2014-06-29 09:59:50	211.94.163.217	42.156.140.19	13178	80	190
疑似	木马-其他-malicious.URI.C61...	2014-06-29 09:59:50	211.94.163.217	42.156.140.19	13178	80	190
疑似	木马-其他-malicious.URI.C61...	2014-06-29 09:59:50	211.94.163.5	42.156.140.23	39385	80	190
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:50	211.94.163.5	42.156.140.23	39385	80	190

2、双击任何一类事件可查看详情。

恶意代码感染事件详细信息	
设备名称 :	190
事件名称 :	木马-其他-Trojan.Win32.Sasfis.ABDB
发生次数 :	1
开始时间 :	2014-06-29 09:59:53
结束时间 :	2014-06-29 09:59:53
感染IP :	211.94.163.18
控制端IP :	42.156.140.222
感染端口 :	26570
控制端端口 :	80
返回信息 :	url=/stat.htm?id=1000322102&r=&lg=zh-cn&ntime=14017562638&repeatip=0&rttime=0&cnzz_eid=835373754-1400994069-&howp=1440x900&t=87341&sin=&ei=quwen1%7Cs%7C%67C0%7C&t=undefined undefined undefined &nd=521449926;host=ei.cnzz.comhead=GET /stat.htm?id=1000322102&r=&lg=zh-

3、点击右上角的放大图标“□”，可放大。

事件实时监控							
恶意代码感染事件		网站事件	通信行为异常事件	恶意代码传播事件	恶意URL访问事件	攻击尝试事件	其它事件
威胁等级	事件名	发生时间	感染IP	控制端IP	感染端口	控制端端口	设备名称
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:53	211.94.163.18	42.156.140.222	26570	80	190
疑似	木马-其他-malicious.URI.C61C	2014-06-29 09:59:53	211.94.163.18	42.156.140.222	26570	80	190
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:47	211.94.163.217	42.156.140.19	12937	80	190
疑似	木马-其他-malicious.URI.C61C	2014-06-29 09:59:47	211.94.163.217	42.156.140.19	12937	80	190
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:47	211.94.163.18	42.156.140.222	34028	80	190
疑似	木马-其他-malicious.URI.C61C	2014-06-29 09:59:48	211.94.163.18	42.156.140.222	34028	80	190
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:48	211.94.163.18	42.156.140.222	34028	80	190
疑似	木马-其他-malicious.URI.C61C	2014-06-29 09:59:48	211.94.163.18	42.156.140.222	34028	80	190
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:50	211.94.162.115	42.156.140.222	13807	80	190
疑似	木马-其他-malicious.URI.C61C	2014-06-29 09:59:50	211.94.162.115	42.156.140.222	13807	80	190
疑似	木马-其他-Trojan.Win32...	2014-06-29 09:59:50	211.94.163.5	42.156.140.23	39385	80	190
疑似	木马-其他-malicious.URI.C61C	2014-06-29 09:59:50	211.94.163.5	42.156.140.23	39385	80	190

2.2 查询

2.2.1 流量分析（2.3 版本功能）

流量分析是用户针对不同的报表，选择不同的时间颗粒度进行分析查询，并生成相应的结果和图表。

一、有如下报表可供用户进行查询：

1. 用户数统计
2. 用户归属地分布
3. 用户浏览器/版本分布
4. 访问时长统计
5. 访问次数统计
6. 用户流量统计
7. TCP 连接成功率统计
8. 网银访问成功率统计
9. 端到端时延统计

二、用户可以选择如下粒度进行查询：

1. 分钟（查询离结束时间最近的一小时内的数据）
2. 小时（查询离结束时间最近的一天内的数据）
3. 天（查询离结束时间最近的一个月内的数据）
4. 月（查询离结束时间最近的一年内的数据）

三、流量分析查询结果主要以下几种图表进行展示：

1. 统计表格

统计表格主要统计该时段内 PC 端，移动端，以及全部的最大值，平均值，最小值情况。

PC 端及移动端（最大值/最小值）=该时段内系统获取的最大值/最小值记录。

全部（最大值/最小值）=该时段内某时间粒度的全部最大值/全部最小值记录。

PC 端、移动端、全部（平均值）=该时段内记录总和/该时段内记录数。

2. 趋势图

以折线图形式展示各时段内 PC 端，移动端，以及 PC 端加移动端的数据。

3. 分布图

以饼图形式展示各时段内各统计对象所在百分比情况。

4. TOP10 表

统计该时段内 TOP10 的记录。



注意 注意以下几点：

1. 开始时间不可选。
2. 默认结束时间应为当前系统时间，用户可以自行设置结束时间。
3. 通常情况下，系统里只存有系统开始运行以后的数据，系统开始运行之前是没有相应数据的，没有数据的时间段将不在趋势图中展示。

2.2.1.1 用户数统计-流量分析

用户进入流量分析界面，报表选择“用户数统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将以“该时段内用户变化趋势”图和“该时段内用户数量”表显示，以下是各个不同粒度时，用户数统计的查询效果：



图2-8 用户数统计粒度分钟查询效果

当前位置：查询 > 流量分析



图2-9 用户数统计粒度小时查询效果

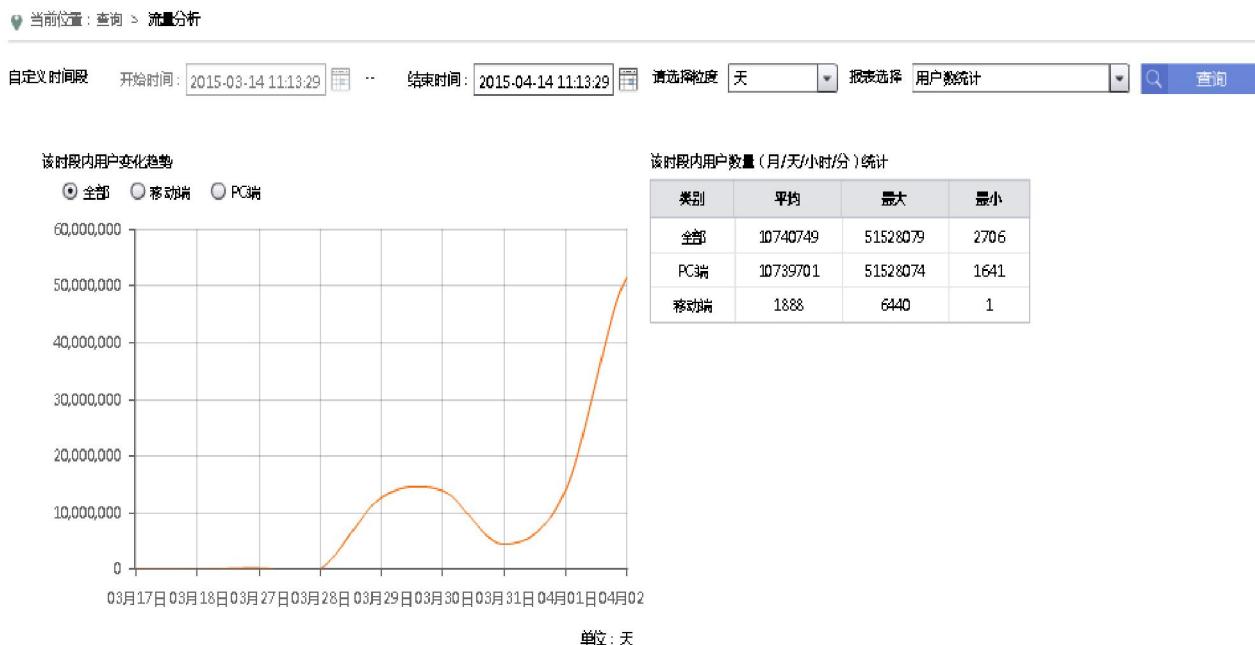


图2-10 用户数统计粒度小时查询效果



图2-11 用户数统计粒度月查询效果

一、 用户变化趋势图描述：

1. 用户可以选择“全部”选项，选择显示全部的该时段内用户变化的趋势情况。
2. 用户可以选择“移动端”选项，选择显示全部的该时段内移动端的用户变化趋势情况。
3. 用户可以选择“PC 端”选项，选择显示全部的该时段内 PC 端的用户变化趋势情况。
4. 横坐标为粒度，纵坐标为用户数量值。

二、 该时段内用户数量统计描述：

1. 统计该时段内全部的用户数平均值，最大值，最小值。
2. 统计该时段内 PC 端的用户数平均值，最大值，最小值。
3. 统计该时段内移动端的用户数平均值，最大值，最小值。

2.2.1.2 用户归属地分布-流量分析

用户进入流量分析界面，报表选择“用户归属地分布”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将以饼图方式显示“访问用户按国家分布”，“国内访问用户按省份分布”，“国内访问用户按地市分布”信息，以下是各个不同粒度时，用户数统计的查询效果：



图2-12 用户归属地分布粒度分钟查询效果



图2-13 用户归属地分布粒度小时查询效果



图2-14 用户归属地分布粒度天查询效果

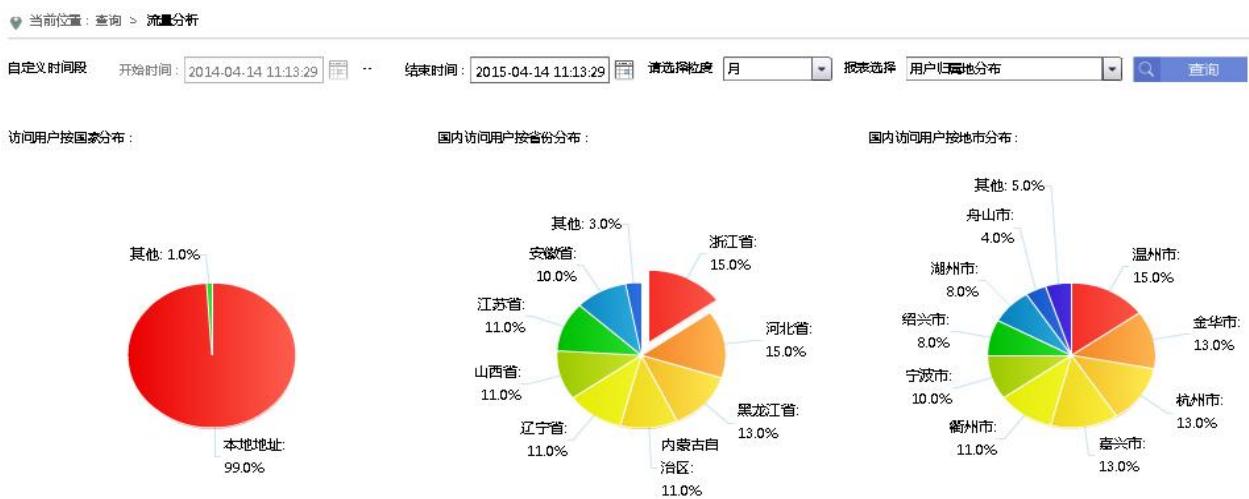


图2-15 用户归属地分布粒度月查询效果

一、访问用户按国家分布描述：

1. ”统计本地数据和非本地数据，数据以饼图形式呈现，用百分比作为统计单位，点击本地地址，或非本地地址颜色区，可以展开各自所在的扇形区域。

二、国内访问用户按省份分布描述：

- 按省市统计用户分布情况，点击各省市所在扇形区域使之展开，将会在“国内访问用户按地市分布”图中展示省市对应的地市用户分布情况。



注意 注意以下几点：

1. 国内访问用户按地市分布图只能展示最近展开的省市扇形图所对应的数据。
 2. 鼠标停留在任意饼图的扇形区域上面，将突出显示该扇形区的区域信息及百分比数据。

如下图所示：



2.2.1.3 用户浏览器/版本分布-流量分析

用户进入流量分析界面，报表选择“用户浏览器/版本分布”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将以饼图方式显示“用户浏览器/版本分布”，具体数据以表格形式展示，以下是各个不同粒度时，用户数统计的查询效果：

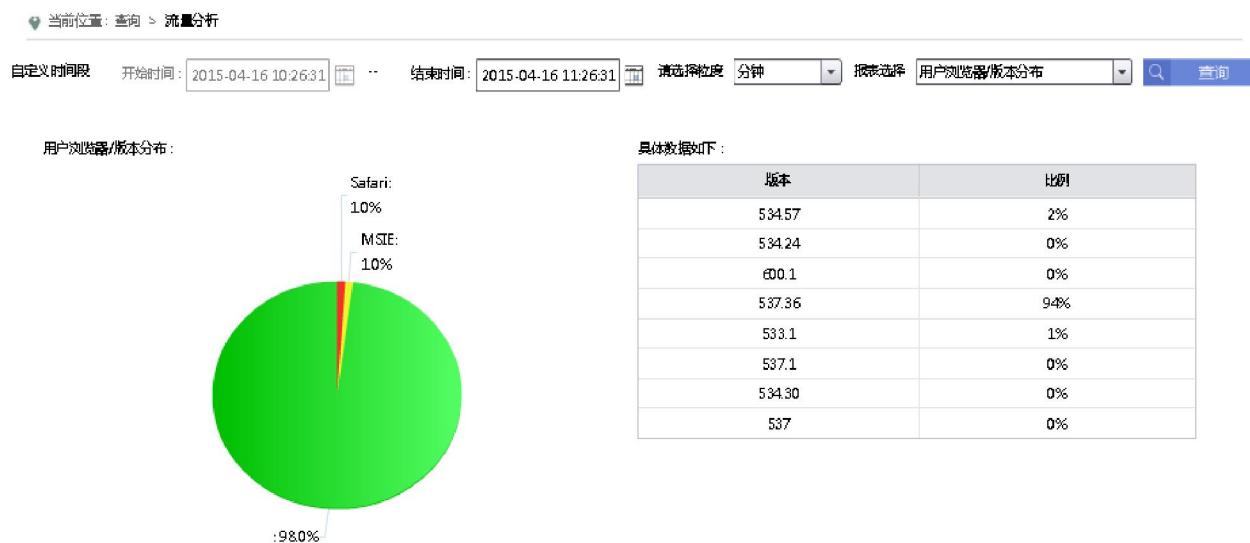


图2-16 用户浏览器/版本分布粒度分钟查询效果

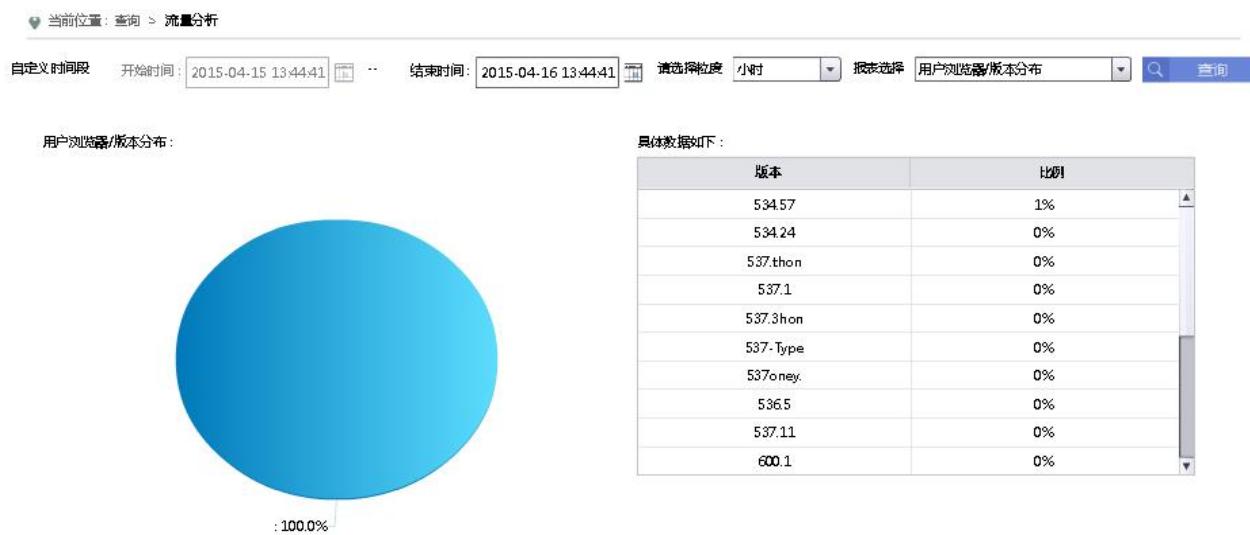


图2-17 用户浏览器/版本分布粒度小时查询效果



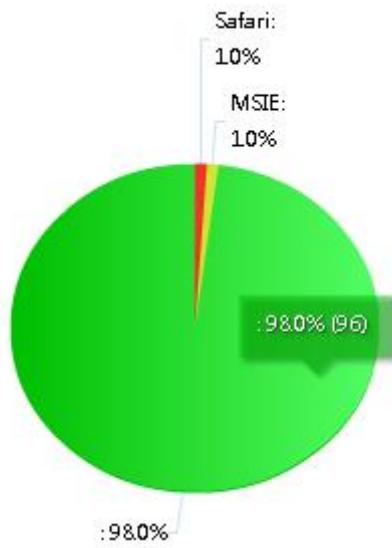
图2-18 用户浏览器/版本分布粒度天查询效果



图2-19 用户浏览器/版本分布粒度月查询效果

一、用户浏览器/版本分布图描述:

1. 以饼图显示各个浏览器的百分比分布情况。
2. 鼠标停留在扇形区，将会显示所在扇形区浏览器的百分比状况。



3. 点击不同的浏览器扇形区，相应的数据表将会在“具体数据表”中显示。

二、具体数据报表描述：

1. 显示所选扇形区浏览器的版本和各个版本所占的比例。

2.2.1.4 访问时长统计-流量分析

用户进入流量分析界面，报表选择“访问时长统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将显示“该时段内按分钟统计”表，“该时段内用户平均访问时长变化趋势”图，“该时段内用户访问时长 top10”表，以下是各个不同粒度时，访问时长统计的查询效果：

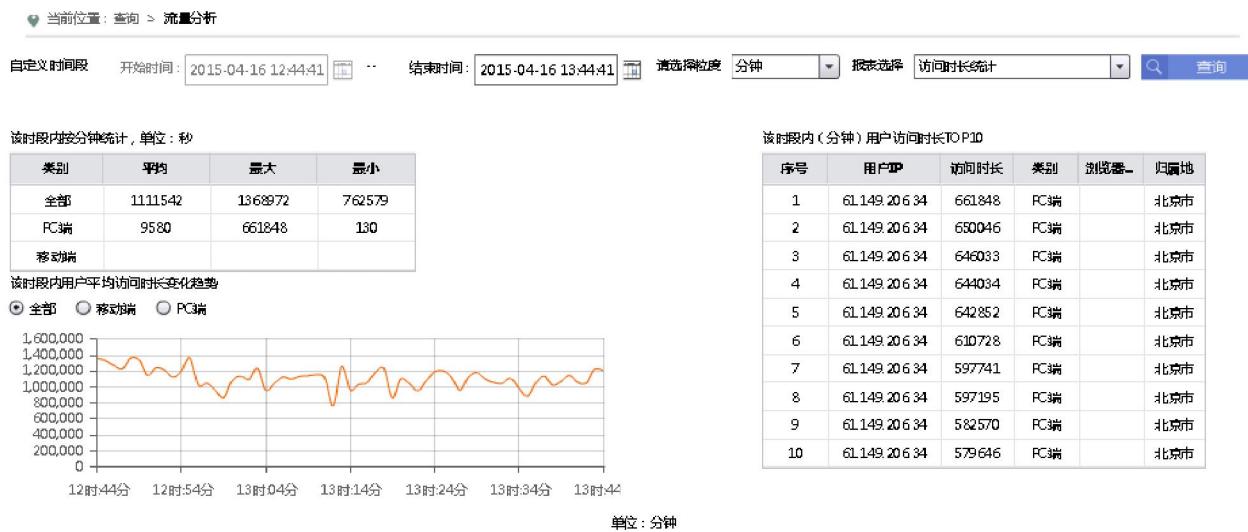


图2-20 访问时长统计粒度分钟查询效果



图2-21 访问时长统计粒度小时查询效果

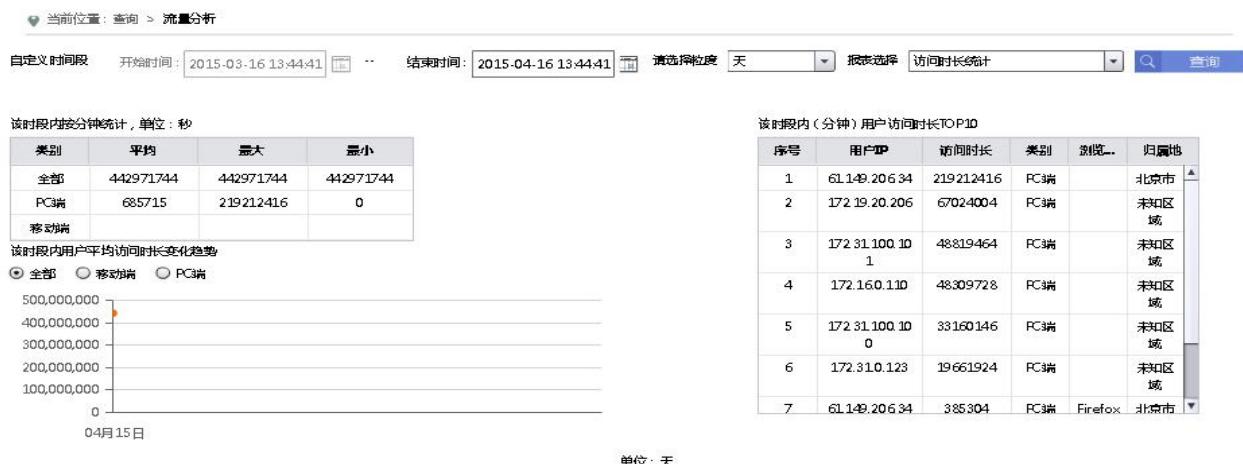


图2-22 访问时长统计粒度天查询效果

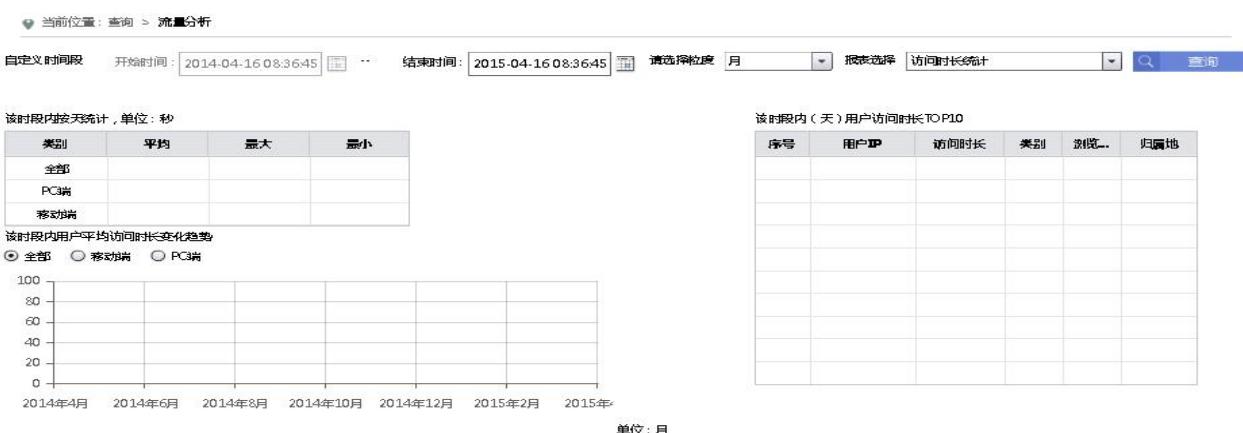


图2-23 访问时长统计粒度月查询效果

一、该时段内用户访问时长统计表描述:

1. 分类统计 PC 端, 移动端, 及全部的访问时长平均值, 最大值, 最小值, 单位为秒。

二、该时段内用户平均访问时长变化趋势图描述:

1. 以曲线图形式分类统计 PC 端, 移动端, 及全部的用户平均访问时长变化趋势, 横坐标为粒度, 纵坐标为访问时长单位秒。

三、该时段内用户访问时长 TOP10 描述:

1. 统计 TOP10 的用户 IP, 访问时长, 类别 (PC 或者手机端), 浏览器版本, 归属地信息。

2.2.1.5 访问次数统计-流量分析

用户进入流量分析界面, 报表选择“访问次数统计”, 颗粒度选择“分钟/小时/天/月”, 点击查询按钮, 查询结果将显示“该时段内用户访问次数统计”表, “该时段内平均访问次数变化趋势”图, “该时段内用户访问次数 top10”表, 以下是各个不同粒度时, 访问次数统计的查询效果:





图2-24 访问次数统计粒度分钟查询效果



图2-25 访问次数统计粒度小时查询效果



图2-26 访问次数统计粒度天查询效果



图2-27 访问次数统计粒度月查询效果

一、该时段内用户访问次数统计表描述:

1. 分类统计 PC 端, 移动端, 及全部的访问时长平均值, 最大值, 最小值。

二、该时段内用户平均访问次数变化趋势图描述:

1. 以曲线图形式分类统计 PC 端, 移动端, 及全部的用户平均访问次数变化趋势, 横坐标为粒度, 纵坐标为数值。

三、该时段内用户访问次数 TOP10 描述:

1. 统计 TOP10 的用户 IP, 访问次数, 类别 (PC 或者手机端), 浏览器版本, 归属地信息。

2.2.1.6 用户流量统计-流量分析

用户进入流量分析界面, 报表选择“用户流量统计”, 颗粒度选择“分钟/小时/天/月”, 点击查询按钮, 查询结果将显示“该时段内用户流量统计”表, “该时段内用户流量变化趋势”图, “该时段内用户流量 top10”表, 以下是各个不同粒度时, 用户流量统计的查询效果:

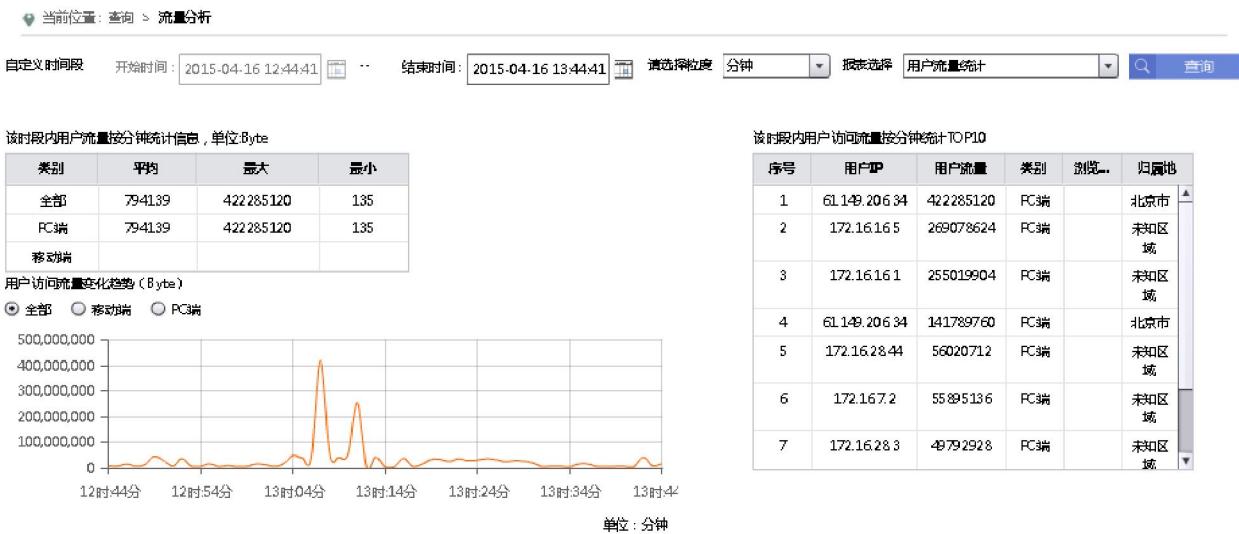


图2-28 用户流量统计粒度分钟查询效果

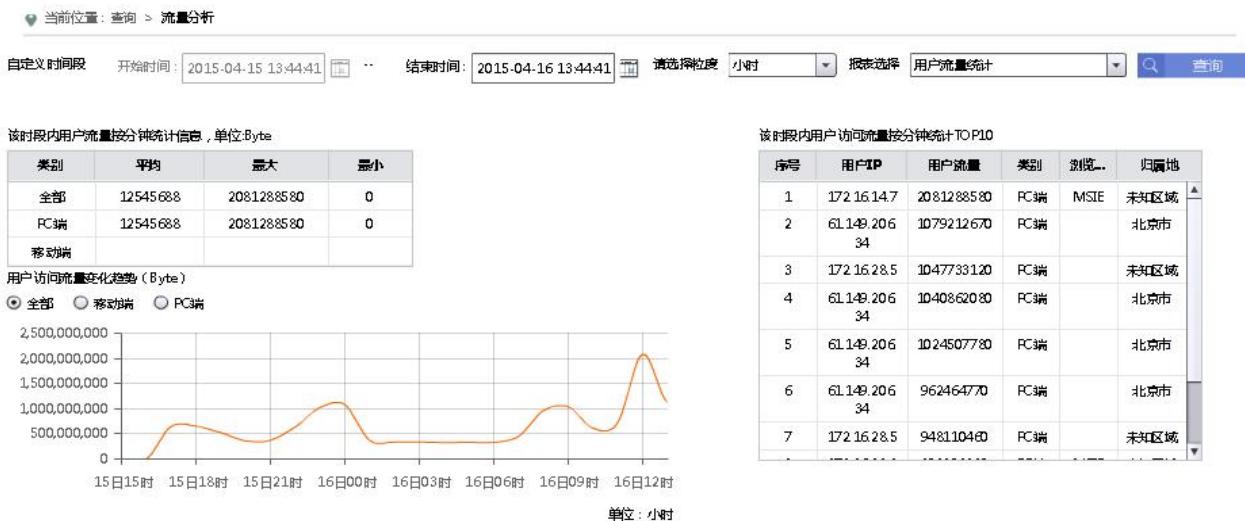


图2-29 用户流量统计粒度小时查询效果



图2-30 用户流量统计粒度天查询效果



图2-31 用户流量统计粒度月查询效果

一、该时段内用户流量统计表描述:

1. 分类统计 PC 端, 移动端, 及全部的访问时长平均值, 最大值, 最小值, 单位为 Bytes。

二、该时段内用户流量变化趋势图描述:

1. 以曲线图形式分类统计 PC 端, 移动端, 及全部的用户平均访问次数变化趋势, 横坐标为粒度, 纵坐标为 Bytes。

三、该时段内用户流量 TOP10 描述:

1. 统计 TOP10 的用户 IP, 用户流量, 类别 (PC 或者手机端), 浏览器版本, 归属地信息。

2.2.1.7 TCP 连接成功率统计-流量分析

用户进入流量分析界面，报表选择“TCP连接成功率统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将显示“该时段内 TCP 连接成功率变化趋势”图，“该时段内 TCP 连接成功率”表，以下是各个不同粒度时，TCP 连接成功率统计的查询效果：



图2-32 TCP 连接成功率统计粒度分钟查询效果



图2-33 TCP 连接成功率统计粒度小时查询效果



图2-34 TCP 连接成功率统计粒度天查询效果



图2-35 TCP 连接成功率统计粒度月查询效果

一、该时段内 TCP 连接成功率变化趋势描述:

1. 以曲线图形式分类统计 PC 端, 移动端, 及全部的 TCP 连接成功率变化趋势, 横坐标为粒度, 纵坐标为百分比。

二、该时段内 TCP 连接成功率统计表描述:

1. 统计 PC 端, 移动端, 及全部的 TCP 连接成功率平均值, 最大值, 最小值。

2.2.1.8 网银访问成功率统计-流量分析

用户进入流量分析界面，报表选择“网银访问成功率统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将显示“该时段内网银访问成功率变化趋势”图，“该时段内网银访问成功率”表，以下是各个不同粒度时，网银访问成功率统计的查询效果：



图2-36 网银访问成功率统计粒度分钟查询效果



图2-37 网银访问成功率统计粒度小时查询效果



图2-38 网银访问成功率统计粒度天查询效果



图2-39 网银访问成功率统计粒度月查询效果

一、该时段内网银访问成功率变化趋势描述：

- 以曲线图形式分类统计 PC 端，移动端，及全部的网银访问成功率变化趋势，横坐标为粒度，纵坐标为百分比。

二、该时段内网银访问成功率统计表描述：

- 统计 PC 端，移动端，及全部的网银访问成功率平均值，最大值，最小值。

2.2.1.9 端到端时延统计-流量分析

用户进入流量分析界面，报表选择“端到端时延统计”，颗粒度选择“分钟/小时/天/月”，点击查询按钮，查询结果将显示“该时段内端到端时延变化趋势”图，“该时段内网银访问成功率”表，以下是各个不同粒度时，端到端时延统计的查询效果：



图2-40 端到端时延统计粒度分钟查询效果



图2-41 端到端时延统计粒度小时查询效果



图2-42 端到端时延统计粒度天查询效果



图2-43 端到端时延统计粒度月查询效果

一、该时段内网银访问成功率变化趋势描述：

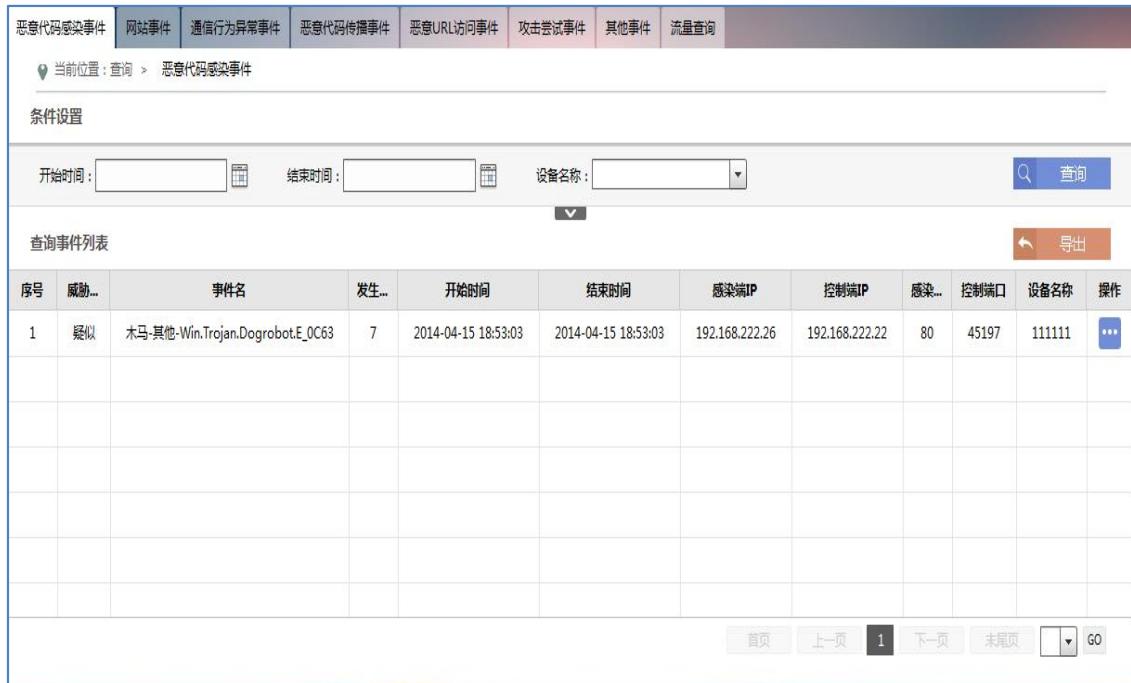
1. 以曲线图形式分类统计 PC 端，移动端，及全部的端到端时延变化趋势，横坐标为粒度，纵坐标为百分比。

二、该时段内网银访问成功率统计表描述：

1. 统计 PC 端，移动端，及全部的端到端时延平均值，最大值，最小值。

2.2.2 恶意代码感染事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有））；点击“下拉开启高级搜索”按钮进入高级查询条件（感染 IP、控制端 IP、感染端口、控制端端口、事件名、重要用户、威胁等级）；查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、感染 IP、控制端 IP、感染端口、控制端口、设备名称。



序号	威胁...	事件名	发生...	开始时间	结束时间	感染端IP	控制端IP	感染...	控制端口	设备名称	操作
1	疑似	木马-其他-Win.Trojan.Dogrobot.E_0C63	7	2014-04-15 18:53:03	2014-04-15 18:53:03	192.168.222.26	192.168.222.22	80	45197	111111	

图2-44 恶意代码感染事件查询效果

一、此模块可进行的操作：

- 1、查询：查询的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、感染 IP、控制端 IP、感染端口、控制端口、设备名称、详细信息。右击感染 IP 或控制端 IP 能够查询该 IP 同一时间段内相关的其他 6 类事件。
- 2、导出：支持用户对查询结果进行导出，导出文件格式支持 TXT/CSV。
- 3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。
- 4、翻页跳转：如果查询结果过多，可以通过翻页跳转功能便于查阅。

二、具体操作说明：

1、时间段的查询：

- 1) 点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。
- 2) 选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。
- 3) 点击右上角关闭，会将当前已选时间保存并关闭时间选择框。
- 4) 点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



2、高级查询：

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为感染端 IP、控制端 IP、重要用户、事件名、感染端口、控制端口、威胁等级。需要说明的有：

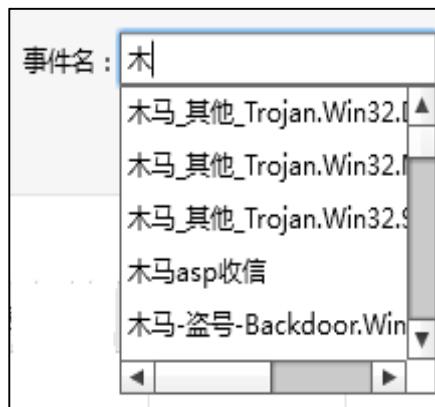
- 1) 感染端 IP 和控制端 IP 需要手动输入 1.0.0.0~255.255.255.255 范围内的 IP，否则校验无法通过。

感染端IP : 请输入正确IP地址

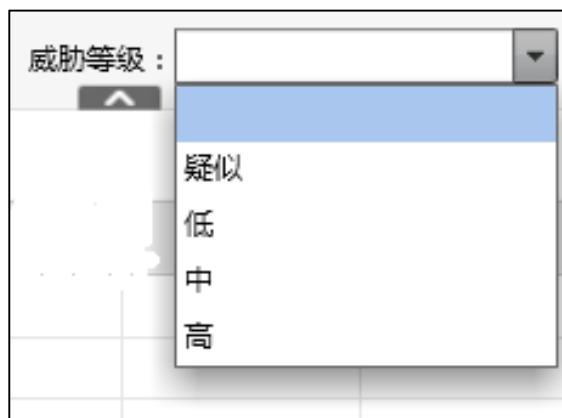
- 2) 感染端口和控制端口需要手动输入 2~65534 范围内的端口（包括 2 和 65534），否则校验无法通过。

感染端口 : 请输入正确端口 (1-65535)

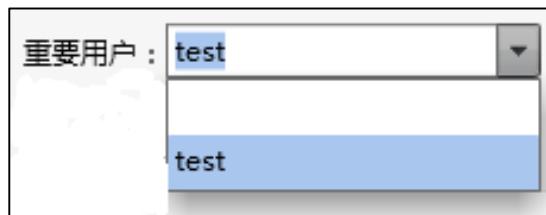
- 3) 关于事件名查询为模糊查询，如输入“木”后，会出现一个下拉列表，下拉列表里面会出现含有“木”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“木”会查询出所有包含其的事件名，也就是说模糊查询。



- 4) 威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项：空、疑似、低、中和高，这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



- 5) 重要用户查询，在系统设置里面我们可以设置一个 IP 或者一个 IP 端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户 test，IP 为 211.94.163.18。随后在重要用户下拉列表中会出现 test 这个重要用户，选择这个重要用户进行查询。



6) 查询出的结果为这个重要用户的 IP 地址 211.94.163.18，而且会标记为红色（不对重要用户查询包含有这个 IP 的事件也会标记为红色）。

查询事件列表												导出
序号	威胁等级	事件名	发生次数	开始时间	结束时间	感染端IP	控制端IP	感染端口	控制端口	设备名称	操作	
1	疑似	木马-其他-Trojan.Win32.Sasfis.ABDB	2	2014-06-29 09:59:53	2014-06-29 09:59:53	211.94.163.18	42.156.140.222	26570	80	190		
2	疑似	木马-其他-malicious.URLC61C	2	2014-06-29 09:59:53	2014-06-29 09:59:53	211.94.163.18	42.156.140.222	26570	80	190		
3	疑似	木马-其他-Trojan.Win32.Sasfis.ABDB	4	2014-06-29 09:59:48	2014-06-29 09:59:48	211.94.163.18	42.156.140.222	34028	80	190		
4	疑似	木马-其他-malicious.URLC61C	4	2014-06-29 09:59:48	2014-06-29 09:59:48	211.94.163.18	42.156.140.222	34028	80	190		
5	疑似	木马-其他-malicious.URLC61C	4	2014-06-29 09:59:43	2014-06-29 09:59:43	211.94.163.18	42.156.140.222	33754	80	190		

三、 导出功能:

1、导出功能可以导出 CSV 和 TXT 两种格式的文件，导出文件的默认名称为 report。



2、导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。

四、事件详细信息和翻页跳转页码：

1、点击查询事件列表每条事件最后一个操作的按钮会出现该条事件的详细信息，如图：



2、如果查询结果过多，可以通过翻页跳转功能便于查阅，根据查阅需求用户可以随意点击翻页的各个按钮来查阅某一页的数据，分页下面的下拉列表选择某页，点击 GO 按钮，可以直接跳转到该页。



2.2.3 网站事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有））；点击“下拉开启高级搜索”按钮进入高级查询条件（攻击 IP、网站 IP、

攻击端口、网站端口、事件名、重要用户、威胁等级); 查询结果包括: 威胁等级、事件名、发生次数、开始时间、结束时间、攻击 IP、网站 IP、攻击端口、网站端口、设备名称。



The screenshot shows a web-based event query interface. At the top, there is a navigation bar with tabs: 恶意代码感染事件, 网站事件, 邮件行为异常事件, 恶意代码传播事件, 恶意URL访问事件, 攻击尝试事件, 其他事件, and 流量查询. The "网站事件" tab is selected. Below the navigation bar, there is a breadcrumb trail: 当前位置: 查询 > 网站事件. A "条件设置" (Condition Settings) section contains fields for "开始时间" (Start Time), "结束时间" (End Time), and "设备名称" (Device Name). To the right of these fields are a search icon and a "查询" (Query) button. Below this is a "查询事件列表" (Query Event List) section. It includes a table with columns: 序号 (Index), 威胁等级 (Threat Level), 事件名 (Event Name), 发生次数 (Occurrence Count), 开始时间 (Start Time), 结束时间 (End Time), 攻击IP (Attack IP), 网站IP (Website IP), 攻击端口 (Attack Port), 网站端口 (Website Port), 设备名称 (Device Name), and 操作 (Operation). There are also "导出" (Export) and back/forward navigation buttons.

图2-45 网站事件查询效果展示图

一、此模块可进行的操作:

- 1、查询: 查询的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、攻击 IP、网站 IP、攻击端口、网站端口、设备名称。右击攻击 IP 或网站 IP 能够查询该 IP 同一时间段内相关的其他 6 类事件。
- 2、导出: 支持用户对查询结果进行导出, 导出文件格式支持 TXT/CSV。
- 3、详细: 点击“详情”按钮, 可查看事件详细信息, 除索引信息外, 还包括处置建议、事件描述。
- 4、翻页跳转: 如果查询结果过多, 可以通过翻页跳转功能便于查阅。

二、具体操作说明:

1、时间段的查询:

- 1) 点击开始时间或结束时间的查询框, 会弹出时间选择框(如图所示), 点击欲查询的日期, 选择后时间选择框会消失。
- 2) 选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

- 3) 点击右上角关闭，会将当前已选时间保存并关闭时间选择框。
- 4) 点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



2、高级查询：

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为攻击 IP、网站 IP、重要用户、事件名、攻击端口、网站端口和威胁等级。需要说明的有：

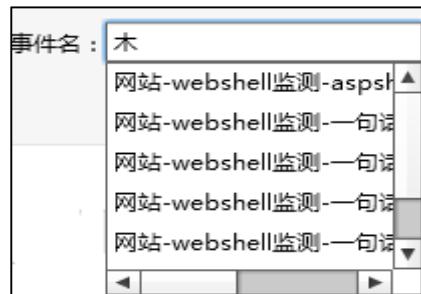
- 1) 攻击 IP 和网站 IP 需要手动输入 1.0.0.0~255.255.255.255 范围内的 IP，否则校验无法通过。

请输入正确IP地址

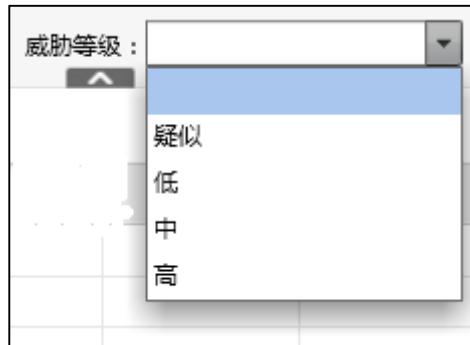
- 2) 攻击端口和网站端口需要手动输入 2~65534 范围内的端口（包括 2 和 65534），否则校验无法通过。

请输入正确端口(1-65535)

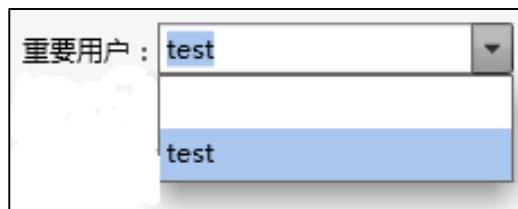
- 3) 关于事件名查询为模糊查询，如输入“木”后，会出现一个下拉列表，下拉列表里面会出现含有“木”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“木”会查询出所有包含其的事件名，也就是说模糊查询。



- 4) 威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项：空、疑似、低、中和高，这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



- 5) 重要用户查询，在系统设置里面我们可以设置一个 IP 或者一个 IP 端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户 test，IP 为 59.188.253.173。随后在重要用户的下拉列表中会出现 test 这个重要用户，选择这个重要用户进行查询。



- 6) 查询出的结果为这个重要用户的 IP 地址 59.188.253.173, 而且会标记为红色(不对重要用户查询包含有这个 IP 的事件也会标记为红色)。

三、 导出功能:

1、导出功能可以导出 CSV 和 TXT 两种格式的文件，导出文件的默认名称为 report。



2、导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。

四、事件详细信息和翻页跳转页码：

1、点击查询事件列表每条事件最后一个操作的按钮会出现该条事件的详细信息，如图：



2、如果查询结果过多，可以通过翻页跳转功能便于查阅，根据查阅需求用户可以随意点击翻页的各个按钮来查阅某一页的数据，分页下面的下拉列表选择某页，点击 GO 按钮，可以直接跳转到该页。



2.2.4 通信行为异常事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有）；点击“下拉开启高级搜索”按钮进入高级查询条件（源 IP、目的 IP、源端口、目的端口、事件名、重要用户、威胁等级）；查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、源 IP、目的 IP、源端口、目的端口、协议类型、设备名称。

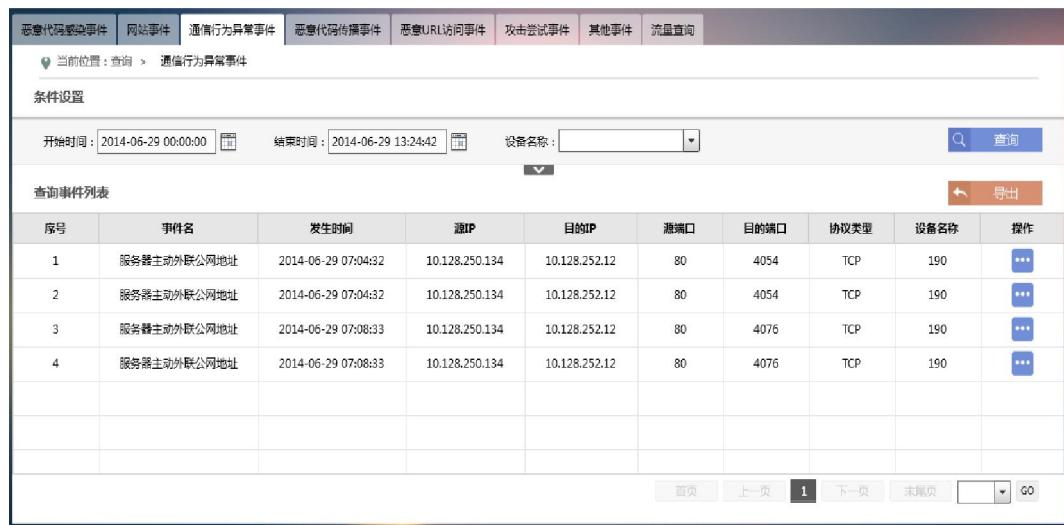


图2-46 通信行为异常事件查询效果展示图

一、此模块可进行的操作：

- 1、查询：查询的结果包括了事件名、发生次数、开始时间、结束时间、源 IP、目的 IP、源端口、目的端口、协议类型、设备名称。右击源 IP 或目的 IP 能够查询该 IP 同一时间段内相关的其他 6 类事件。
- 2、导出：支持用户对查询结果进行导出，导出文件格式支持 TXT/CSV。
- 3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。

4、翻页跳转：如果查询结果过多，可以通过翻页跳转功能便于查阅。

二、时间段的查询：

- 1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。
- 2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。
- 3、点击右上角关闭，会将当前已选时间保存并关闭时间选择框。
- 4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



三、高级查询：

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为源IP、目的IP、重要用户、事件名、源端口、目的端口、协议类型。需要说明的有：

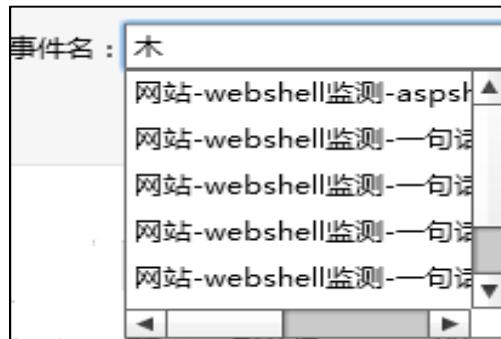
- 1、源IP和目的IP需要手动输入 $1.0.0.0 \sim 255.255.255.255$ 范围内的IP，否则校验无法通过。



- 2、源端口和目的端口需要手动输入 $2 \sim 65534$ 范围内的端口（包括2和65534），否则校验无法通过。

源端口 : 1 请输入正确端口 (1-65535)

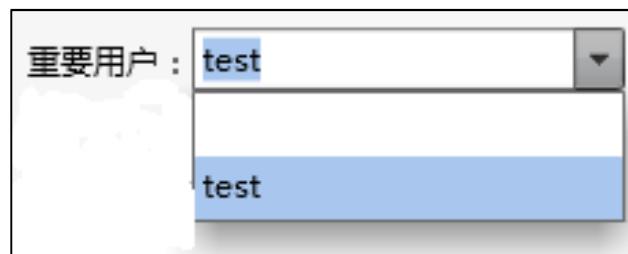
- 3、关于事件名查询为模糊查询，如输入“木”后，会出现一个下拉列表，下拉列表里面会出现含有“木”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“木”会查询出所有包含其的事件名，也就是说模糊查询。



- 4、威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项：空、疑似、低、中和高：这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



- 5、重要用户查询，在系统设置里面我们可以设置一个 IP 或者一个 IP 端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户 test，IP 为 10.128.252.12。随后在重要用户的下拉列表中会出现 test 这个重要用户，选择这个重要用户进行查询。



- 6、查询出的结果为这个重要用户的 IP 地址 10.128.252.12，而且会标记为红色（不对重要用户查询包含有这个 IP 的事件也会标记为红色）。

四、 导出功能:

1、导出功能可以导出 CSV 和 TXT 两种格式的文件，导出文件的默认名称为 report。



2、导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。

五、事件详细信息和翻页跳转页码：

1、点击查询事件列表每条事件最后一个操作的按钮会出现该条事件的详细信息，如图：



2、如果查询结果过多，可以通过翻页跳转功能便于查阅，根据查阅需求用户可以随意点击翻页的各个按钮来查阅某一页的数据，分页下面的下拉列表选择某页，点击 GO 按钮，可以直接跳转到该页。



2.2.5 恶意代码传播事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、病毒类型、设备名称（管理点独有））；点击“下拉开启高级搜索”按钮进入高级查询条件（传播源 IP、受害 IP、传播端口、受害端口、病毒名、重要用户、威胁等级、协议类型）；查询结果包括：威胁等级、病毒名称、发生时间、结束时间、传播 IP、受害 IP、传播端口、受害端口、协议类型、设备名称。



恶意代码感染事件 网站事件 通信行为异常事件 恶意代码传播事件 恶意URL访问事件 攻击尝试事件 其他事件 流量查询

当前位置：查询 > 恶意代码传播事件

条件设置

开始时间： 结束时间： 病毒类型： 设备名称：

查询

查询事件列表

序号	威胁等级	病毒名称	发生时间	传播源IP	受害IP	传播端口	受害端口	病毒类型	协议类型	设备名称	操作
1	低	1	2014-04-14 00:00:00	0.0.0.1	0.0.0.1	1	1				...
2	低	2	2014-04-12 01:00:00	0.0.0.2	0.0.0.2	2	2				...
3		1	2014-04-13 00:00:00	0.0.0.1	0.0.0.1	11					...
4	低	1	2014-04-15 01:00:00	0.0.0.1	0.0.0.1	1	1				...
5		qwe	2014-04-15 00:20:00	0.0.0.12	0.0.0.12	12	12				...
6		32	2014-04-15 10:00:00	0.0.0.32	0.0.0.32	32	32				...
7	低	2	2014-04-13 20:00:00	0.0.0.2	0.0.0.2	2	2				...

首页 上一页 1 下一页 末尾页 GO

图2-47 恶意代码传播事件查询效果展示图

一、此模块可进行的操作

- 1、查询：查询的结果包括了威胁等级、病毒名称、发生时间、传播源 IP、受害 IP、传播端口、受害端口、病毒类型、协议类型、设备名称。右击传播 IP 或受害 IP 能够查询该 IP 同一时间段内相关的其他 6 类事件。
- 2、导出：支持用户对查询结果进行导出，导出文件格式支持 TXT/CSV。
- 3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。
- 4、翻页跳转：如果查询结果过多，可以通过翻页跳转功能便于查阅。

二、时间段的查询

- 1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。
- 2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。
- 3、点击右上角关闭，会将当前已选时间保存并关闭时间选择框。
- 4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



三、 普通查询

- 1、 病毒类型查询框为一个下拉列表，可以在下拉列表中选取将要查询的病毒名称进行查询。
- 2、 设备名称查询框为一个下拉列表，管理点设备在下拉列表里面会出现下级的设备名称，选择设备名称进行查询。

四、 高级查询：

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现八个查询框，分别为传播源 IP、受害 IP、重要用户、协议类型、传播端口、受害端口、威胁等级和病毒名称。需要说明的有：

- 1、 传播源 IP 和目的 IP 需要手动输入 1.0.0.0~255.255.255.255 范围内的 IP，否则校验无法通过。

传播源IP : 请输入正确IP地址

- 2、 传播端口和受害端口需要手动输入 2~65534 范围内的端口（包括 2 和 65534），否则校验无法通过。

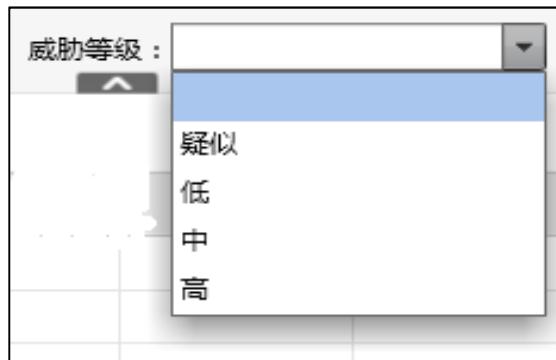
传播端口 : 请输入正确端口 (1-65535)

- 3、 关于病毒名称查询为模糊查询，如输入“V”后，查询出的结果病毒名称里面都含有字母“V”

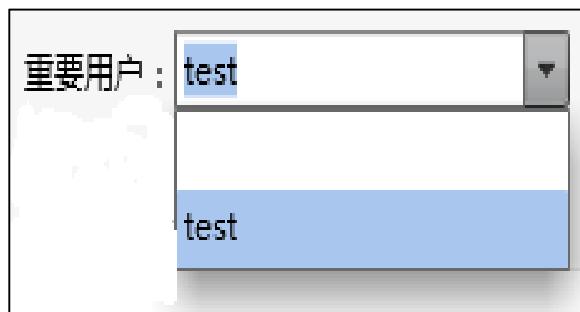
传播端口 :		受害端口 :		威胁等级 :		病毒名称 :		操作			
序号	威胁等级	病毒名称	发生时间	传播源IP	受害IP	传播端口	受害端口	病毒类型	协议类型	设备名称	操作
1	低	VCS/Environment.DigitalFN.a	2014-06-29 01:51:02	173.192.190.226	114.255.183.48	80	42966	风险软件	HTTP	190	
2	低	VCS/Environment.DigitalFN.a	2014-06-29 02:42:48	174.37.181.30	114.255.183.49	80	56524	风险软件	HTTP	190	
3	低	VCS/Environment.DigitalFN.a	2014-06-29 05:33:53	58.211.23.175	114.255.183.42	80	40111	风险软件	HTTP	190	
4	低	VCS/Environment.DigitalFN.a	2014-06-29 05:33:53	58.211.23.175	114.255.183.42	80	40111	风险软件	HTTP	190	
5	低	RiskWare[RiskTool:not-a-virus]/W	2014-06-29 03:10:44	1.93.38.11	114.255.183.46	80	45908	风险软件	HTTP	190	

首页 上一页 1 下一页 末尾页 Go

4、威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项：空、疑似、低、中和高，这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



5、重要用户查询，在系统设置里面我们可以设置一个 IP 或者一个 IP 端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户 test，IP 为 10.128.252.12。随后在重要用户的下拉列表中会出现 test 这个重要用户，选择这个重要用户进行查询。



6、查询出的结果为这个重要用户的 IP 地址 10.128.252.12，而且会标记为红色（不对重要用户查询包含有这个 IP 的事件也会标记为红色）。

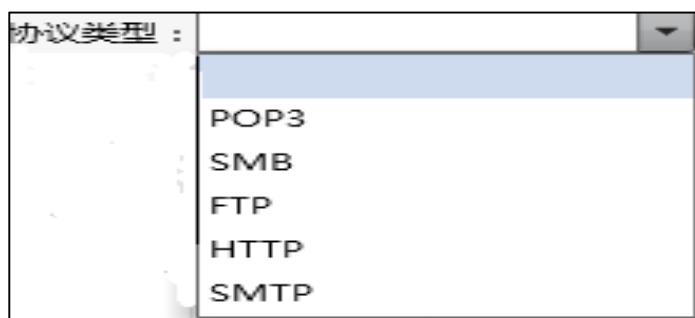
查询事件列表

导出

序号	威胁等级	病毒名称	发生时间	传播源IP	受害IP	传播端口	受害端口	病毒类型	协议类型	设备名称	操作
1	低	VCS/PEStruct.PatchedPE	2014-06-29 01:41:30	125.65.110.236	114.255.183.50	88	41211	风险软件	HTTP	190	
2	低	VCS/PEStruct.PatchedPE	2014-06-29 09:46:28	61.164.109.226	114.255.183.57	80	57189	风险软件	HTTP	190	
3	低	VCS/PEStruct.PatchedPE	2014-06-29 09:46:28	61.164.109.226	114.255.183.57	80	57189	风险软件	HTTP	190	
4	低	VCS/PEStruct.PatchedPE	2014-06-29 09:46:28	61.164.109.226	114.255.183.57	80	57189	风险软件	HTTP	190	
5	低	VCS/PEStruct.PatchedPE	2014-06-29 09:46:28	61.164.109.226	114.255.183.57	80	57189	风险软件	HTTP	190	

首页 上一页 1 2 3 4 5 下一页 末尾页 Go

7、 协议类型查询框为一个下拉列表，通过选择下拉列表里面的协议类型进行查询，下拉列表包括 POP3、SMB、FTP、HTTP 和 SMTP 五种协议类型。



五、 导出功能：

1、 导出功能可以导出 CSV 和 TXT 两种格式的文件，导出文件的默认名称为 report。



2、 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。

report - Excel

A	B	C	D	E	F	G	H	I	J	K	L	M
威胁等级	病毒名称	发生时间	传播源IP	传播端口	受害IP	受害端口	病毒类型	协议类型	设备名称	事件描述	处置建议	
1 低	VCS/PEStz	41:30:0 125.65.11	88	114.255.1	41211	57189	风险软件		190			
3 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
4 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
5 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
6 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
7 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
8 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
9 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
10 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
11 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
12 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
13 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
14 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
15 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
16 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
17 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
18 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
19 低	VCS/PEStz	46:28.0 61.164.1C	80	114.255.1	57189	风险软件			190			
20 低	VCS/Instz	43:06.0 125.39.1.	80	114.255.1	47517	风险软件			190			
21 低	VCS/Instz	43:24.0 221.5.47.	80	114.255.1	53845	风险软件			190			
22 中	Trojan/W1	43:32.0 50.117.11	80	114.255.1	45255	木马			190			
23 低	VCS/PEStz	47:12.0 70.39.87.	80	114.255.1	50147	风险软件			190			

六、事件详细信息和翻页跳转页码：

1、点击查询事件列表每条事件最后一个操作的按钮会出现该条事件的详细信息。如图。



2、如果查询结果过多，可以通过翻页跳转功能便于查阅，根据查阅需求用户可以随意点击翻页的各个按钮来查阅某一页的数据，分页下面的下拉列表选择某页，点击 GO 按钮，可以直接跳转到该页。



2.2.6 恶意 URL 访问事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、病毒类型、设备名称（管理点独有））；点击“下拉开启高级搜索”按钮进入高级查询条件（访问 IP、

服务器 IP、访问端口、服务器端口、URL); 查询结果包括: 设备名称、访问 IP、服务器 IP、访问端口、服务器端口、URL、访问方式、主机、浏览器类型、时间。

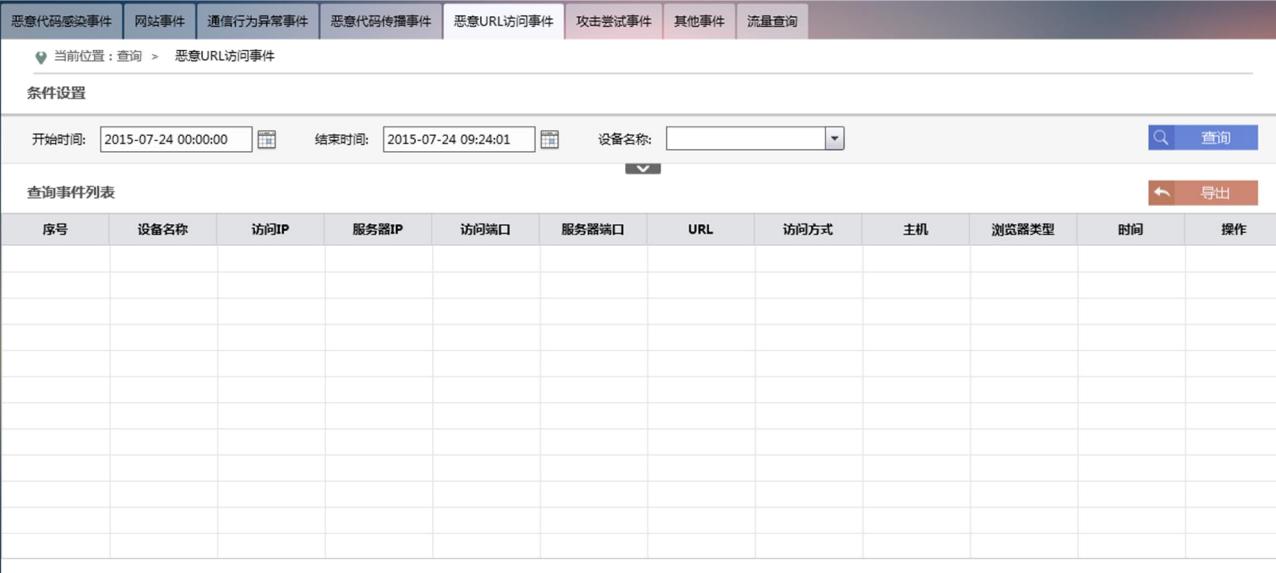


图2-48 恶意 URL 访问事件查询

一、此模块可进行的操作

- 1、查询: 查询的结果包括设备名称、访问 IP、服务器 IP、访问端口、服务器端口、URL、访问方式、主机、浏览器类型、时间。右击攻击 IP 或被攻击 IP 能够查询该 IP 同一时间段内相关的其他 6 类事件
- 2、导出: 支持用户对查询结果进行导出, 导出文件格式支持 TXT/CSV。
- 3、详细: 点击“详情”按钮, 可查看事件详细信息, 除索引信息外, 还包括处置建议、事件描述。
- 4、翻页跳转: 如果查询结果过多, 可以通过翻页跳转功能便于查阅。

二、时间段的查询

- 1、点击开始时间或结束时间的查询框, 会弹出时间选择框(如图所示), 点击欲查询的日期, 选择后时间选择框会消失。

- 2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。
- 3、点击右上角关闭，会将当前已选时间保存并关闭时间选择框。
- 4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



三、普通查询：

设备名称查询框为一个下拉列表，管理点设备在下拉列表里面会出现下级的设备名称，选择设备名称进行查询。

四、高级查询：

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为访问 IP、服务器 IP、URL、访问方式和主机。需要说明的有：

- 1、访问 IP 和服务器 IP 需要手动输入 1.0.0.0~255.255.255.255 范围内的 IP，否则校验无法通过。



A screenshot of an input field. The placeholder text '访问IP : 0.0.0.0' is visible, and a red arrow points from the text '请输入正确IP地址' (Please enter correct IP address) to the right side of the input field.

- 2、关于主机查询为模糊查询，如输入“d”后，查询出的结果病毒名称里面都含有字母“d”。

查询事件列表											 导出
序号	设备...	访问IP	服务器IP	访问端口	服务器端口	URL	访问...	主机	浏览器类型	...	
1	190	114.255.183.59	216.137.52.178	45165	80	http://downloadcdn.betterinstaller.com/in...	HEAD	downloadcdn.betterinstaller.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...		
2	190	114.255.183.54	116.255.147....	45165	80	http://down.ku122.com/download...	HEAD	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...		
3	190	114.255.183.54	116.255.137....	45165	80	http://down.ku122.com/download...	GET	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...		
4	190	114.255.183.54	116.255.147....	45165	80	http://down.ku122.com/download...	HEAD	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...		
5	190	114.255.183.54	116.255.137....	45165	80	http://down.ku122.com/download...	GET	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...		
6	190	114.255.183.59	216.137.52.178	45165	80	http://downloadcdn.betterinstaller.com/in...	HEAD	downloadcdn.betterinstaller.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...		

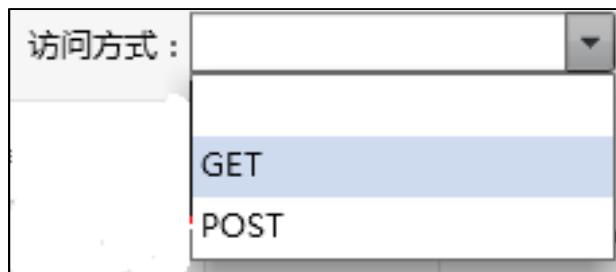
[Navigation buttons: 首页, 上一页, 1, 下一页, 未尾页, 搜索框, GO]

3、关于 URL 查询为模糊查询，如输入“2”后，查询出的结果病毒名称里面都含有数字“2”。

序号	设备...	访问IP	服务器IP	访问端口	服务器端口	URL	访问...	主机	浏览器类型	时间	...
1	190	114.255.183.54	116.255.147....	45165	80	http://down.ku122.com/download...	HEAD	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...	2014-06-18 18:05:31	
2	190	114.255.183.54	116.255.137....	45165	80	http://down.ku122.com/download...	GET	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...	2014-06-18 18:05:33	
3	190	114.255.183.54	116.255.147....	45165	80	http://down.ku122.com/download...	HEAD	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...	2014-06-22 18:05:31	
4	190	114.255.183.54	116.255.137....	45165	80	http://down.ku122.com/download...	GET	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...	2014-06-22 18:05:33	
5	190	114.255.183.54	116.255.147....	45165	80	http://down.ku122.com/download...	HEAD	down.ku122.com	Mozilla/5.0 (compatible; MSIE 9.0; Windo...	2014-06-22 18:05:33	

[Navigation buttons: 首页, 上一页, 1, 下一页, 未尾页, 搜索框, GO]

4、访问方式查询框为一个下拉列表，通过选择下拉列表里面的协议类型进行查询，下拉列表包括 GET 和 POST 两种协议类型。



五、导出功能：

1、导出功能可以导出 CSV 和 TXT 两种格式的文件，导出文件的默认名称为 report。



2、导出的文件为当前查询的结果，如查询访问方式为 GET，那么导出的文件内容就为访问方式为 GET 的事件。



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	设备名称	访问IP	服务器IP	URL	访问方式	主机	浏览器类型	时间					
2		190 114. 255. 1116. 255. 1	http://dc	GET		down.ku12Mozilla/5		2014-06-18/18:05:33					
3		190 114. 255. 1116. 255. 1	http://dc	GET		down.ku12Mozilla/5		2014-06-22/18:05:33					
4		190 114. 255. 1116. 255. 1	http://dc	GET		down.ku12Mozilla/5		2014-06-20/18:05:33					
5													
6													
7													
8													

六、事件详细信息和翻页跳转页码：

1、点击查询事件列表每条事件最后一个操作的按钮会出现该条事件的详细信息，如图：

恶意URL访问事件详细信息	
设备名称 :	190
访问IP :	114.255.183.54
服务器IP :	116.255.137.131
访问端口 :	45165
服务器端口 :	80
URL :	http://down.ku122.com/download/2345/2345.baiaasp.exe
访问方式 :	GET
主机 :	down.ku122.com
浏览器类型 :	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
时间 :	2014-06-18 18:05:33

2、如果查询结果过多，可以通过翻页跳转功能便于查阅，根据查阅需求用户可以随意点击翻页的各个按钮来查阅某一页的数据，分页下面的下拉列表选择某页，点击 GO 按钮，可以直接跳转到该页。



2.2.7 攻击尝试事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有）；点击“下拉开启高级搜索”按钮进入高级查询条件（攻击 IP、被攻击 IP、攻击端口、被攻击端口、事件名、重要用户、威胁等级）；查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、攻击 IP、被攻击 IP、攻击端口、被攻击端口、设备名称。

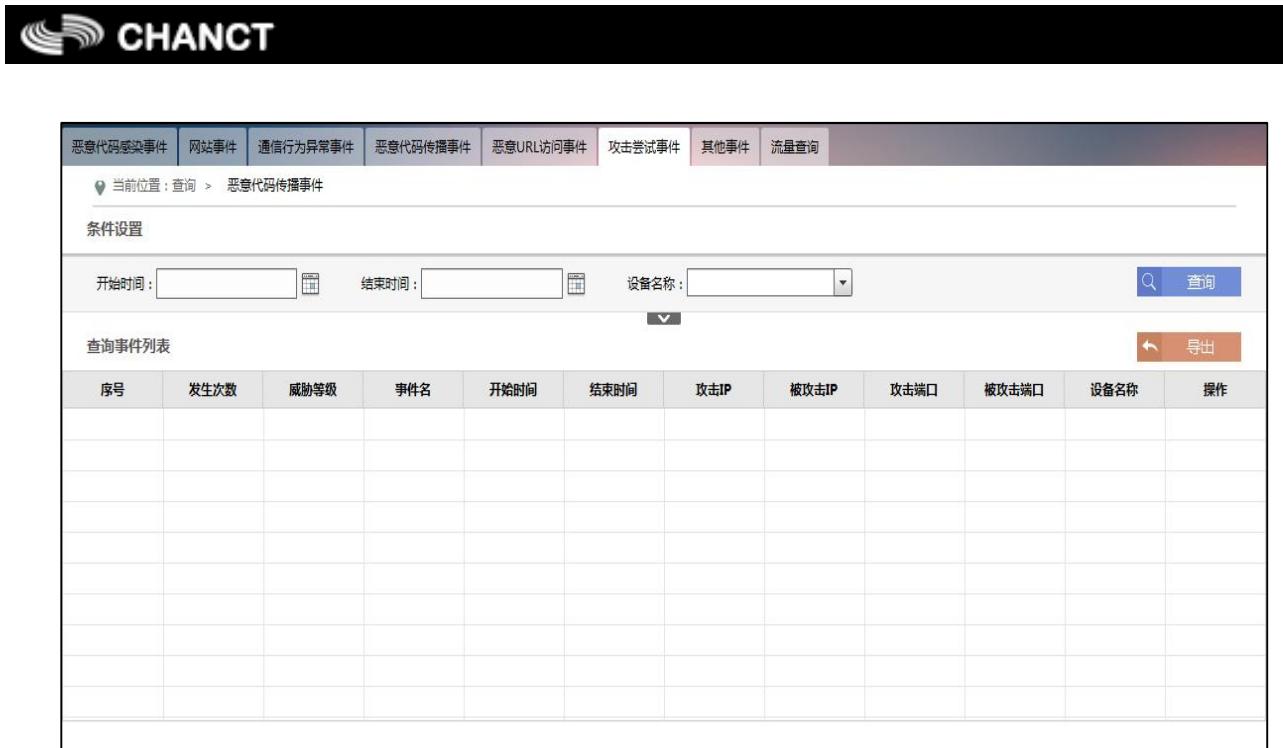


图2-49 攻击尝试事件查询

一、此模块可进行的操作

- 1、查询：查询后的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、攻击 IP、被攻击 IP、攻击端口、被攻击端口、设备名称。右击攻击 IP 或被攻击 IP 能够查询该 IP 同一时间段内相关的其他 6 类事件
 - 2、导出：支持用户对查询结果进行导出，导出文件格式支持 TXT/CSV。
 - 3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。
 - 4、翻页跳转：如果查询结果过多，可以通过翻页跳转功能便于查阅。

二、时间段的查询：

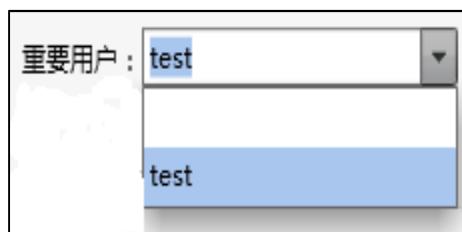
- 1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。
 - 2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。
 - 3、点击右上角关闭，会将当前已选时间保存并关闭时间选择框。

4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



三、 普通查询：

1、重要用户查询，在系统设置里面我们可以设置一个 IP 或者一个 IP 端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户 test，IP 为 211.94.163.5。随后在重要用户的下拉列表中会出现 test 这个重要用户，选择这个重要用户进行查询。



2、查询出的结果为这个重要用户的 IP 地址 211.94.163.5，而且会标记为红色（不对重要用户查询包含有这个 IP 的事件也会标记为红色）。

四、 高级查询：

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为被攻击 IP、攻击 IP、被攻击端口、攻击端口、威胁等级、事件名。需要说明的有：

- 1、 攻击 IP 和被攻击 IP 需要手动输入 1.0.0.0~255.255.255.255 范围内的 IP，否则校验无法通过。

攻击IP : 请输入正确IP地址

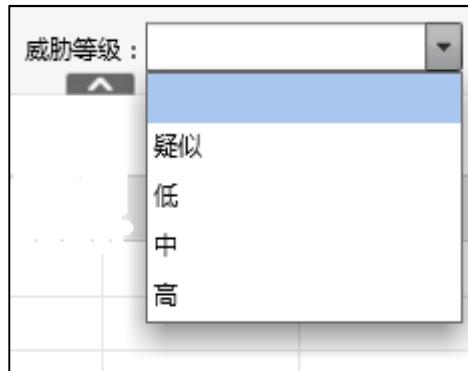
- 2、 攻击端口和被攻击端口需要手动输入 2~65534 范围内的端口（包括 2 和 65534），否则校验无法通过。

攻击端口 : 请输入正确端口 (1-65535)

- 3、关于事件名查询为模糊查询，如输入“2”后，会出现一个下拉列表，下拉列表里面会出现含有“2”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“2”会查询出所有包含其的事件名，也就是说模糊查询。

事件名 :	2
	攻击-ie 0day cve-2012-4696-01
	攻击-ie 0day cve-2012-4696-02
	攻击-ie 0day cve-2012-4696-03

- 4、威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项：空、疑似、低、中和高，这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



五、 导出功能：

1、 导出功能可以导出 CSV 和 TXT 两种格式的文件，导出文件的默认名称为 report。



2、 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	设备名	事件名称	开始时间	结束时间	攻击IP	攻击端口	被攻击IP	被攻击端口	威胁等级	被攻击次数	事件描述	处置建议						
2	190 攻击-Troj	2014-06-22 01:11:94.16			39385	42.156.14	80	疑似		6	url=/stat.htm?id=5257179&r=&lg=zh-cn&ntime=1401841512&repeatip=1&rtime=175							
3	190 攻击-mali	2014-06-22 01:11:94.16			39385	42.156.14	80	疑似		6	url=/stat.htm?id=5257179&r=&lg=zh-cn&ntime=1401841512&repeatip=1&rtime=175							
4																		
5																		
6																		
7																		
8																		
9																		

六、 事件详细信息和翻页跳转页码：

1、 点击查询事件列表每条事件最后一个操作的按钮会出现该条事件的详细信息，如图：

攻击尝试事件详细信息	
设备名称 :	190
事件名称 :	攻击-Trojan.Win32.Sasfis.ABDB
发生次数 :	2
开始时间 :	2014-06-29 09:59:50
结束时间 :	2014-06-29 09:59:50
攻击IP :	211.94.163.5
被攻击IP :	42.156.140.23
攻击端口 :	39385
被攻击端口 :	80
返回信息 :	

- 2、如果查询结果过多，可以通过翻页跳转功能便于查阅，根据查阅需求用户可以随意点击翻页的各个按钮来查阅某一页的数据，分页下面的下拉列表选择某页，点击 GO 按钮，可以直接跳转到该页。



2.2.8 其他事件查询

查询分默认查询及高级查询，进入查询页显示默认查询（开始时间、结束时间、设备名称（管理点独有）；点击“下拉开启高级搜索”按钮进入高级查询条件（感染端 IP、控制端 IP、感染端口、控制端口、事件名、重要用户、威胁等级）；查询结果包括：威胁等级、事件名、发生次数、开始时间、结束时间、感染 IP、控制端 IP、感染端口、控制端口、设备名称。

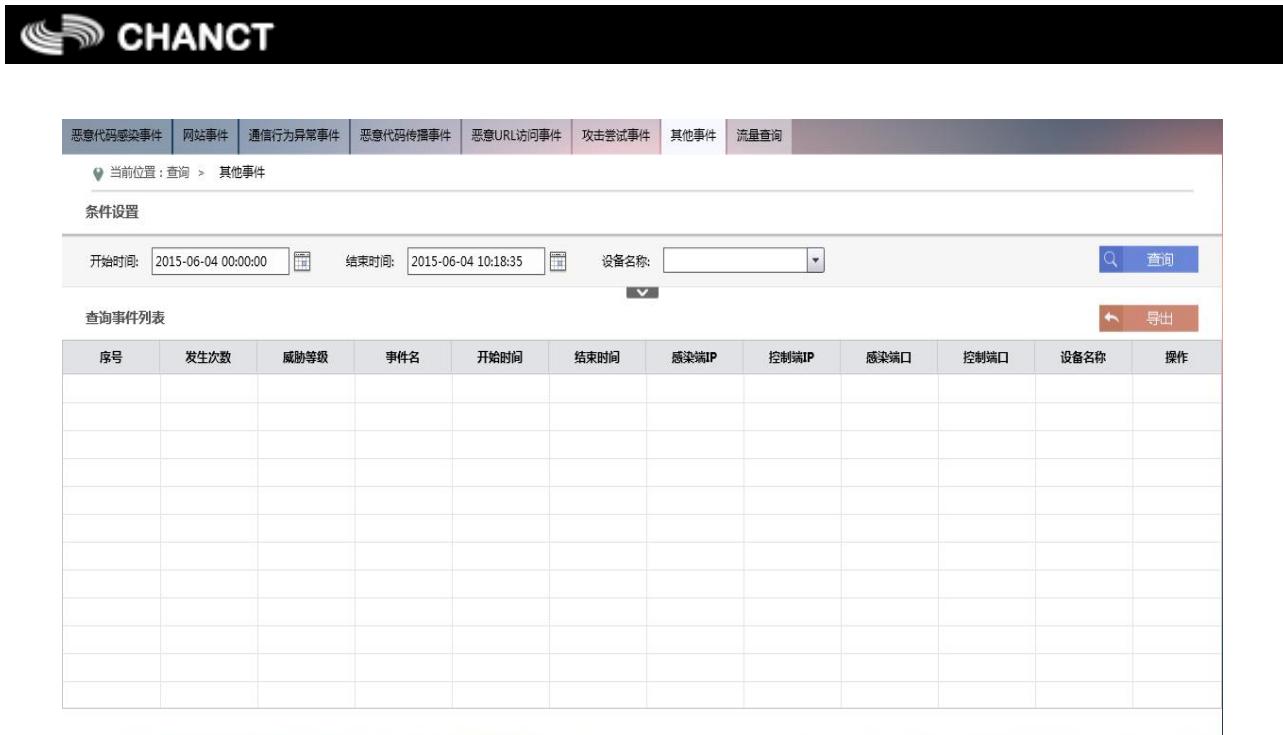


图2-50 其他事件查询

一、此模块可进行的操作

- 1、查询：查询的结果包括了威胁等级、事件名、发生次数、开始时间、结束时间、攻击 IP、被攻击 IP、攻击端口、被攻击端口、设备名称。右击攻击 IP 或被攻击 IP 能够查询该 IP 同一时间段内相关的其他 6 类事件。
 - 2、导出：支持用户对查询结果进行导出，导出文件格式支持 TXT/CSV。
 - 3、详细：点击“详情”按钮，可查看事件详细信息，除索引信息外，还包括处置建议、事件描述。
 - 4、翻页跳转：如果查询结果过多，可以通过翻页跳转功能便于查阅。

二、时间段的查询：

- 5、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。
 - 6、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。

- 7、点击右上角关闭，会将当前已选时间保存并关闭时间选择框。
- 8、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。



三、 高级查询：

点击查询框中的向下的箭头即可进入高级查询，高级查询会出现七个查询框，分别为感染端 IP、控制端 IP、重要用户、事件名、感染端口、控制端口、威胁等级。需要说明的有：

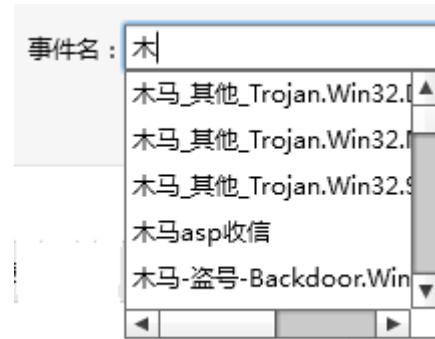
- 1、感染端 IP 和控制端 IP 需要手动输入 1.0.0.0~255.255.255.255 范围内的 IP，否则校验无法通过。

攻击IP : 请输入正确IP地址

- 2、感染端口和控制端口需要手动输入 2~65534 范围内的端口（包括 2 和 65534），否则校验无法通过。

攻击端口 : 请输入正确端口 (1-65535)

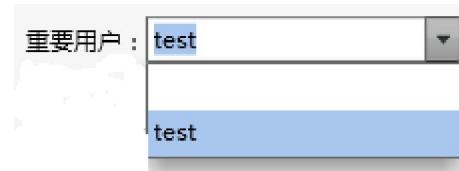
- 3、关于事件名查询为模糊查询，如输入“木”后，会出现一个下拉列表，下拉列表里面会出现含有“木”字的一些事件名，如果有想查询的可以直接点击进行查询。如果只输入“木”会查询出所有包含其的事件名，也就是说模糊查询。



4、威胁等级查询框，此查询框为一个下拉选择框，下拉列表里面包括五项：空、疑似、低、中和高，这几个选项可以进行选择查询，如果选择空那么代表此查询框为空。



5、重要用户查询，在系统设置里面我们可以设置一个 IP 或者一个 IP 端为重要用户，设置的这个重要用户会出现在高级查询的下拉列表中，如我们设置一个重要用户 test，IP 为 111.205.62.201。随后在重要用户的下拉列表中会出现 test 这个重要用户，选择这个重要用户进行查询。



6、查询出的结果为这个重要用户的 IP 地址 111.205.62.201，而且会标记为红色（不对重要用户查询包含有这个 IP 的事件也会标记为红色）。

四、 导出功能：

1、 导出功能可以导出 CSV 和 TXT 两种格式的文件，导出文件的默认名称为 report。



2、 导出的文件为当前查询的结果，如查询重要用户，那么导出的文件内容就为重要用户的事件。



A1	设备名	事件名称	开始时间	结束时间	攻击IP	攻击端口	被攻击IP	被攻击端口或威胁等级	发生次数	事件描述	处置建议
1	190 移动互联网	2014-06-21 11:205.62.201	2014-06-21 11:58.68.226		58215	58.68.226	80	疑似	10	r=GET /c.php?u=83CC8142455A95CC4CA409257CA5B4A2&v=2013.12.30.042&c=100&a=3&n=3&s=2cd2b4b41cf07efa6336ee4dcf15295b HTTP/1.1\0D\0AHost: ciba.count.www.iciba.com\0D\0AAccept: */*\0D\0AAccept-Encoding: gzip, deflate\0D\0A\0D\0A/b	
2											
3											
4											
5											
6											
7											

五、 事件详细信息和选择页码：

1、 点击查询事件列表每条事件最后一个操作的按钮会出现该条事件的详细信息，如图：



其它事件详细	
设备名称 :	190
事件名称 :	移动互联网恶意代码-其他-s.remote.DuMusicplay.c
发生次数 :	20
开始时间 :	2014-06-29 05:24:42
结束时间 :	2014-06-29 09:26:42
攻击IP :	111.205.62.201
被攻击IP :	58.68.226.21
攻击端口 :	58215
被攻击端口 :	80
返回信息 :	r=GET /c.php? u=83CC8142455A95CC4CA409257CA5B4A2&v =2013.12.30.042&c=100&a=3&n=3&s=2cd2b 4b41cf07efa6336ee4dcf15295b HTTP/1.1\0D \0AHost: ciba.count.www.iciba.com\0D \0AAccept: */*\0D\0AAccept-Encoding: gzip, deflate\0D\0A\0D\0A/b

2、如果查询结果过多，可以通过翻页跳转功能便于查阅，根据查阅需求用户可以随意点击翻页的各个按钮来查阅某一页的数据，分页下面的下拉列表选择某页，点击 GO 按钮，可以直接跳转到该页。



2.2.9 流量查询

流量查询模块默认展示的为最近一小时流量；此处不同于首页最近流量曲线的是可以对历史的流量进行查询；通过输入查询条件：开始时间、结束时间、流量类型、设备名称、自定义流量来进行查询。



图2-51 流量查询效果展示图

一、此模块可进行的操作

1、查询：输入开始时间、结束时间、流量类型、设备名称、自定义流量来进行查询，其中自定义流量为下拉框形式。

二、时间段的查询

- 1、点击开始时间或结束时间的查询框，会弹出时间选择框（如图所示），点击欲查询的日期，选择后时间选择框会消失。
- 2、选择某个时间点通过时间选择框左上角的两个时间点的下拉列表可以选择具体的时间点进行查询。
- 3、点击右上角关闭，会将当前已选时间保存并关闭时间选择框。
- 4、点击今天在选择框里会出现当前的时间点（开始时间默认框时间为今天零点，结束时间框默认时间为当前的时间）。

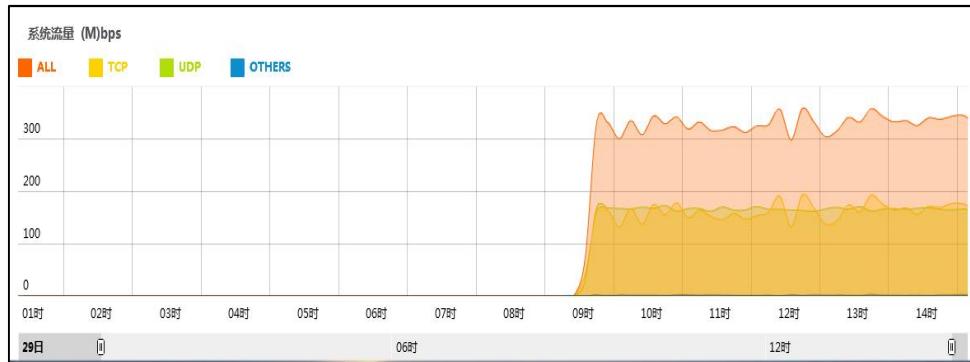


三、普通查询：

- 1、流量类型查询框为一个下拉列表，可以在下拉列表中选取将要查询的流量类型进行查询。（流量类型包括两种分别为 bps 和 pps）
- 2、设备名称查询框为一个下拉列表，管理点设备在下拉列表里面会出现下级的设备名称，选择设备名称进行查询。
- 3、在系统管理里面，添加一个自定义流量“test”，添加过后会在此查询框显示自定义流量名称“test”，点击这个名称进行查询。

四、系统流量查询结果：

- 1、流量查询结果是以坐标轴和曲线形式展现给用户的，用户可以通过点击坐标轴上方的流量名称来选择自己想要关注的流量曲线，每种流量曲线以颜色区分，横轴为时间轴，纵轴为流量轴。



- 2、用户可以在流量曲线上横向拖动光标，来放大要观察的流量曲线，点击还原流量曲线回到初始位置。
- 3、用户可以通过拖动时间轴下面的两个滑块来选择要观察的时间段的范围。

2.3 报表

2.3.1 报表下载

报表类型包括：日报/周报/月报/年报。每类报表均支持 word 格式。

报表命名规范：

日报： yyyy-mm-dd 日报表. doc;

周报： yyyy 年第 n 周 (mm 月 dd 日 -mm 月 dd 日) 周报表. doc; (以周一作为一周开始, 周跨年/月时, 以周一所在年月为准)

月报： yyyy-mm 月报表. doc;

年报： yyyy 年报表. doc。



图2-52 报表下载效果展示图

一、此模块可进行的操作：

1、 下载：进行日报/周报/月报/年报的下载。

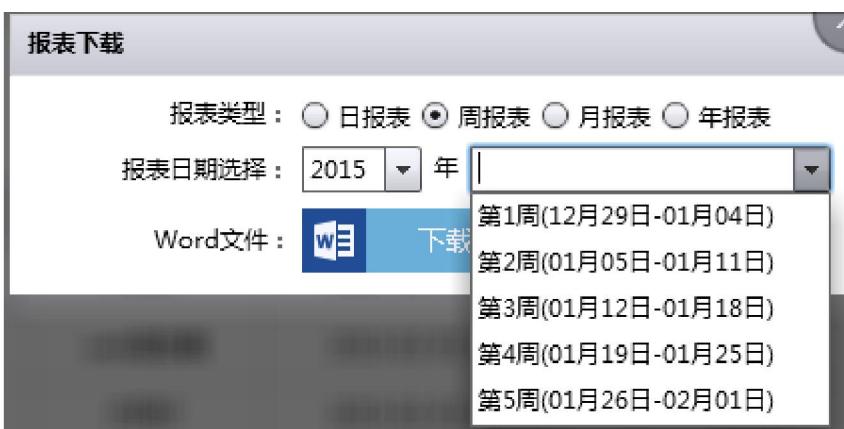
二、 此模块的操作流程：

1、 点击“报表下载”，会弹出图 4-1 报表下载页；

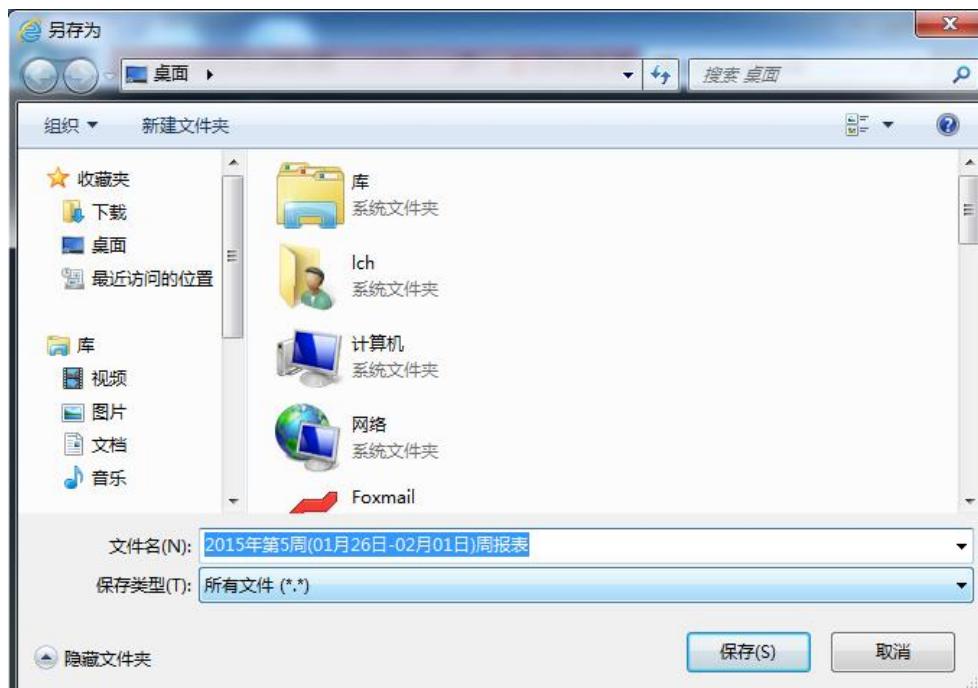
2、 选择报表类型；



3、 选择报表日期；



4、 点击  ，将报表下载到本地，可选任意路径存放。



注意 请使用 Microsoft Word 打开报表，WPS 打开报表为代码。

2.4 系统管理

2.4.1 节点管理（2.3 版本功能）

节点管理信息分左右两栏显示，左边显示当前设备的资源占用情况以及节点信息，资源占用情况包括：内存占用率，CPU 占用率，磁盘占用率，系统版本和特征库版本；节点信息包括：节点名称、网口类型、网口数量、是否启用。在设备状态树上展示设备正常/异常(异常叹号)、通讯正常/异常（异常虚线、叉号）、注册进行中/完成。右边显示设备拓扑图。

节点名称	网口类型	网口数量	是否启用
监测2	万兆	1	<input checked="" type="checkbox"/>
监测3	万兆	1	<input checked="" type="checkbox"/>
监测4	万兆	1	<input checked="" type="checkbox"/>

图2-53 节点管理效果展示图

一、此模块可进行的操作:

- 1、节点系统状态查看：用户可分别查看管理节点和各监测节点的系统状态信息，如内存占用率、CPU 占用率和磁盘占用率。
- 2、监测节点配置：用户可根据实际需要配置监测节点的启用和关闭。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“节点管理”选项卡，切换到“节点管理”页面。
- 2、查看检测节点配置信息：登陆页面后，页面左侧默认显示当前的检测节点配置信息，即哪些检测节点已启用。
- 3、查看节点拓扑状态：登陆页面后，页面右侧默认显示节点拓扑状态，当检测节点与管理节点连接正常时，通讯线路显示红色，检测节点显示彩色；当检测节点与管理节点连接断线时，通信线路显示灰色并带有图标，检测节点显示灰色并带有图标。
- 4、查看节点系统状态：单机拓扑图中的节点图标，页面左侧会显示该节点的内存占用率、CPU 占用率和磁盘占用率。
- 5、检测节点配置：在页面左侧检测节点配置表中，勾选需要启用的检测节点，然后点击“保存”按钮，保存节点配置。当节点配置成功后，页面右侧拓扑图会根据配置变化，显示管理节点和已启用的检测节点，未启用节点不显示。

2.4.2 设备管理

设备管理信息分左右两栏显示，左边显示设备拓扑图，右边默认显示当前设备的资源占用情况，包括内存占用率、CPU 占用率、磁盘占用率、系统版本和特征库版本。在设备状态树上展示设备正常/异常(异常叹号)、通讯正常/异常(异常虚线、叉号)、注册进行中/完成。



图2-54 设备管理效果展示图

一、此模块可进行的操作：

- 1、当设备类型为“监测点设备”时，此模块不能进行任何操作。
- 2、当设备类型为“管理点设备”时，此模块可进行如下操作：
 - 1) 新增：新增该节点管理的设备；
 - 2) 修改：修改该节点所管理设备的设备信息（注：不可修改根节点设备信息）；
 - 3) 删除：删除该节点所管理的设备（注：不可删除根节点；若删除普通管理点，其对应下级设备一并删除。）。

二、此模块的操作流程：

1、监测点设备此模块操作：

- 1) 登录界面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“设备管理”选项卡，切换到“设备管理”页面。
- 2) 查看设备状态：在界面右侧可以查看监测点设备的内存占用率、CPU 占用率、磁盘占用率、系统版本和特征库版本。
- 3) 查看设备拓扑状态：在页面左侧显示正确的设备拓扑状态，并且鼠标移到此设备上显示正确的此设备 IP。

4) 监测点设备此模块权限：新增、修改、删除按钮都为不可点击的状态。



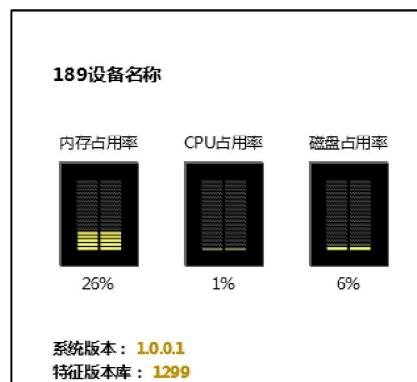
2、管理点设备此模块操作：

- 1) 登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“设备管理”选项卡，切换到“设备管理”页面。
- 2) 新增设备：点击“新增”按钮，弹出新增设备信息配置页面，在该页面中输入设备名称、IP 地址、命令端口、文件端口、联系人、联系电话及备注等设备信息，然后选择是否接入云，最后点击“保存”按钮，设备添加成功。

3) 查看设备拓扑状态：添加成功后，设备就会显示在首页系统状态和设备管理拓扑图中。根据设备的显示可以判断设备的连接情况，如果像上图中 185 的状态就说明，185 没有与上级连接，而 189 的状态是连接正常状态。



4) 查看设备系统状态：点击除本机及以外任何一个设备的拓扑图标，都可在右侧看到它的系统状态。



5) 对添加的设备，可做修改操作，点击  修改，会弹出修改界面，可在此界面上进行修改。



6) 点击  可将设备删除。

2.4.3 网络配置

此模块主要功能是显示和配置相关的网络配置信息，及代理的启动与关闭操作。

网络配置信息包括设备名称、最大上传速度、最大下载速度、设备IP地址、子网掩码、网关地址、DNS1、DNS2、命令端口、文件传输端口、启动代理、代理协议、代理服务器域名/IP、代理服务器PORT、代理服务器用户名、代理服务器密码。

图2-55 网络配置效果展示图

一、此模块可进行的操作：

- 1、基本信息配置：主要包括设备名称、IP地址、子网掩码、网关地址、DNS1、DNS2、通讯端口范围的配置。用户可根据实际需要对上述信息进行配置。
- 2、根节点选择：用户可根据实际情况，设置设备是否为根节点。
- 3、阿里云设置：主要包括接入阿里云选择、最大上传速度和最大下载速度。当设备为根节点时，可选择是否接入阿里云，并可以限制设备与阿里云之间的上传和下载速度。
- 4、代理设置：主要包括启用代理选择、代理协议选择、代理服务器域名/IP、代理服务器PORT、代理服务器用户名、代理服务器密码。设备支持通过代理服务器连接阿里云。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“网络配置”选项卡，切换到“网络配置”页面。
- 2、查看网络配置信息：登陆页面后，默认显示当前的网络配置相关信息。
- 3、配置基本信息：如果用户需要修改网络基本配置，可在预修改信息显示框里输入相关配置信息。基本配置信息包括：设备名称、IP 地址、子网掩码、网关地址、DNS1、DNS2、通讯端口范围。



说明

- a、设备名称长度不能超过 32 字节；
 - b、IP 地址、子网掩码、网关地址、DNS1、DNS2 输入规范正确的地址；
 - c、通讯端口的范围为 1024~65535。
- 4、根节点选择：用户可以根据需要设置设备是否为根节点，可通过是否勾选“根节点”选择框操作，设置设备是否为根节点。
 - 5、阿里云配置：当设备设置为根节点之后，用户可通过是否勾选“接入阿里云”操作选择是否接入阿里云，并可在“最大上传速度”和“最大下载速度”处限制上传下载速度。

6、代理设置：用户可以根据需要，通过是否勾选“开启代理”操作，选择是否开启代理。当启用代理后，需要对代理协议、代理服务器域名/IP、代理服务器PORT、用户名、密码进行配置。配置完上述信息后，点击“连接测试”按钮，当返回信息为“测试成功”表示代理配置成功，设备可以通过代理服务器接入阿里云，否则表示代理配置失败，设备无法通过代理服务器接入阿里云。

当前位置：系统管理 > 网络配置



设备名称：

根节点 接入阿里云

最大上传速度： Kbps, 0为不限速

最大下载速度： Kbps, 0为不限速

IP地址：

子网掩码：

网关地址：

DNS1：

DNS2：

通讯端口范围： ~

此端口范围是1024~65535,用于级联设备之间的通信。
指定的端口范围包含的端口不少于2个。

代理协议： HTTP SOCKS4 SOCKS5

服务器域名/IP：

服务器PORT：

用户名：

密码：

启动代理

7、保存配置：用户修改完相应配置信息后，点击“保存”按钮，保存配置修改。

2.4.4 用户管理

本系统共设置3种用户角色：系统管理员、系统配置员、系统审计员。

系统管理员：拥有系统最高权限，可查看、操作所有模块。

系统配置员：不可对用户管理模块进行修改、删除操作，但可进行查看操作；可操作除查询、报表下载、授权模块外的其他系统模块。

系统审计员：不可操作系统管理模块及授权申请模块。



设备管理	网络配置	用户管理	监听配置	组件设置	时间同步	预警管理	升级管理	调试配置	重要用户	自定义流量	白名单	系统操作日志	
当前位置：系统管理 > 用户管理													
条件设置													
用户名：	<input type="text"/>	用户角色：	<input type="text"/>	账户状态：	<input type="text"/>	创建者：	<input type="text"/>						
开始时间：	2015-02-04 00:00:00	<input type="button"/>	结束时间：	2015-02-04 11:32:00	<input type="button"/>								
+ 新增													
序号	用户名	用户角色	创建时间	创建者	账户状态	备注	操作						
1	test	系统审计员	2015-02-04 11:29:25	admin									
首页 上一页 1 下一页 末尾页 GO													

图2-56 用户管理效果展示图

一、此模块可进行的操作：

- 1、查询：可根据用户名、用户角色、账户状态、创建者、事件查询用户信息。
- 2、新增：新增系统用户信息，需要填写用户名（可输入中文）、密码、密码确认、用户角色、备注信息。
- 3、修改用户信息：通过点击预修改用户信息后面的修改按钮进行修改，创建时间则更新为修改时间。
- 4、删除用户信息：点击预删除用户后面的按钮，对用户进行单条删除。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“用户管理”选项卡，切换到“用户管理”页面。
- 2、查询用户信息：
 - 1) 默认查询：不输入任何过滤条件，点击“查询”按钮，页面会显示该时间段内创建或修改的所有用户信息。
 - 2) 条件查询：输入过滤条件，如用户名、用户角色、账户状态、创建者、开始时间、结束时间，然后点击“查询”按钮，页面显示符合过滤条件的用户信息。
- 3、新增用户信息：如果要新增用户信息，点击“新增”按钮，

设备管理	网络配置	用户管理	监听配置	组件设置	时间同步	预警管理	升级管理	调试配置	重要用户	自定义流量	白名单	系统操作日志
当前位置 : 系统管理 > 用户管理												
条件设置												
用户名 :	<input type="text"/>		用户角色 :	<input type="button" value="下拉"/>		账户状态 :	<input type="button" value="下拉"/>		创建者 :	<input type="text"/>		
开始时间 :	<input type="text" value="2015-02-04 00:00:00"/>		结束时间 :	<input type="text" value="2015-02-04 11:10:26"/>				<input type="button" value="查询"/>				
<input style="background-color: #c0392b; color: white; border-radius: 5px; padding: 2px 10px; margin-right: 10px;" type="button" value="+"/> 新增												
序号	用户名	用户角色	创建时间	创建者	账户状态	备注	操作					

弹出用户配置窗口,

添加用户

用户名 :	<input type="text"/>
密码 :	<input type="password"/>
密码确认 :	<input type="password"/>
用户角色 :	<input type="button" value="下拉"/>
备注 :	<input type="text"/>
<input style="background-color: #f0ad4e; color: white; border-radius: 5px; padding: 2px 10px; margin-right: 10px;" type="button" value="保存"/> <input type="button" value="取消"/>	

根据上图进行填写用户信息，然后点击“保存”按钮，新用户添加成功。



注意 系统配置员只能进入首页和系统管理（不包括用户管理）；

系统审计员只能进入首页、查询和报表下载；

系统管理员拥有的权限最高，可进入所有模块进行查看和配置。

4、修改用户信息：如果用户需要修改用户信息，在预修改用户信息上点击 修改按钮，

序号	用户名	用户角色	创建时间	创建者	账户状态	备注	操作
1	test_c	系统审计员	2015-06-30 16:54:35	admin		1234567890	
2	d	系统审计员	2015-06-30 13:50:27	admin			

弹出用户配置窗口,

修改用户

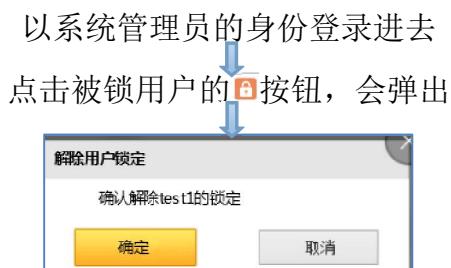
用户名 :	<input type="text" value="test_c"/>
密码 :	<input type="password"/>
密码确认 :	<input type="password"/>
用户角色 :	<input type="button" value="下拉"/>
备注 :	<input type="text" value="1234567890"/>
<small>注意：不输入密码，默认使用原密码。</small>	
<input style="background-color: #f0ad4e; color: white; border-radius: 5px; padding: 2px 10px; margin-right: 10px;" type="button" value="保存"/> <input type="button" value="取消"/>	

根据上图进行填写用户信息，然后点击“保存”按钮，修改用户信息成功。

5、解锁用户：如果任何一个用户被锁，那么它的账户状态就会变为锁定。

序号	用户名	用户角色	创建时间	创建者	账户状态
1	test2	系统审计员	2014-06-22 13:14:06	admin	
2	test1	系统配置员	2014-06-22 13:13:51	admin	
3	admin	系统管理员	2014-01-14 13:27:30	admin	

系统管理员可以为其他用户角色解锁，操作如下：



点击“确定”，解锁被锁的用户

6、删除用户信息：如果用户需要删除已存在的用户信息，点击对应用户信息信息上的的删除按钮，对应用户信息被删除。

2.4.5 捕包设置（2.3 版本不具备此功能）

此模块记录了设备监测口的连通状态及捕包情况。

网卡名	MAC地址	网卡流量	连通状态	捕包设置
eth2	00:90:0B:3D:0E:38	21833491880193		<input checked="" type="checkbox"/>
eth3	00:90:0B:3D:0E:39	3192903154279		<input checked="" type="checkbox"/>

保存

图2-57 捕包设置效果展示图

一、此模块可进行的操作：

- 1、连通设置：可将监测口进行物理连通，则连通状态显示为绿色。
- 2、捕包设置：可对已经连通的监测口（连通状态显示为绿色）进行捕包设置。



说明 如果连接状态始终显示红色，那说明该端口没有运行起来。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“捕包设置”选项卡，切换到“捕包设置”页面。
- 2、查看网口状态：登陆页面后，显示当前捕包设置状态，及各网卡信息。
- 3、捕包口设置：如果用户想将某一网口设为捕包口，先将预设捕包口进行物理连通，则连通状态显示为绿色，点击捕包设置的“□”按钮，捕包设置一栏变为“☑”，捕包口设置成功。



网卡名	MAC地址	网卡流量	连通状态	捕包设置
eth1	00:90:0B:35:3A:5A	0	●	<input type="checkbox"/>
eth2	00:90:0B:35:3A:5B	154010233	●	<input checked="" type="checkbox"/>
eth3	00:90:0B:35:3A:5C	0	●	<input type="checkbox"/>
eth4	00:90:0B:35:3A:5D	0	●	<input type="checkbox"/>

保存 **取消**



网卡名	MAC地址	网卡流量	连通状态	捕包设置
eth1	00:90:0B:35:3A:5A	0	●	<input type="checkbox"/>
eth2	00:90:0B:35:3A:5B	154010233	●	<input checked="" type="checkbox"/>
eth3	00:90:0B:35:3A:5C	0	●	<input type="checkbox"/>
eth4	00:90:0B:35:3A:5D	0	●	<input type="checkbox"/>

保存 **取消**

- 4、保存配置修改：点击“保存”按钮，捕包口设置保存成功。

2.4.6 引擎设置

此模块主要记录了 Cncert 深度报文检测引擎、Cncert 病毒检测引擎、Cncert 异常通信行为监测引擎的运行状态及内网信息配置表。



设备管理 网络配置 用户管理 捕包设置 引擎设置 时间设置 预警管理 升级设置 维护设置 重要用户 自定义流量 白名单 操作日志

当前位置：系统管理 > 引擎设置

根据需要，开启或关闭监测引擎：

Cncert深度报文检测引擎	<input checked="" type="checkbox"/> 开启
Cncert病毒检测引擎	<input checked="" type="checkbox"/> 开启
Cncert异常通信行为监测引擎	<input checked="" type="checkbox"/> 开启

内网信息配置表：

+ 新增

序号	名称	IP列表	IP类型	创建时间	创建者	创建者IP	备注	操作

保存 取消

图2-58 引擎设置效果展示图

一、此模块可进行的操作：

- 1、开启与关闭 Cncert 深度报文检测引擎。
- 2、开启与关闭 Cncert 病毒检测引擎。
- 3、开启与关闭 Cncert 异常通信行为监测引擎。
- 4、新增内网配置信息记录：需要填写名称、IP/IP 段、IP 类型、备注信息。
- 5、修改内网配置信息记录：通过点击预修改内网配置信息后面的修改按钮可以进行修改，创建时间更新为修改时间。
- 6、删除内网配置信息记录：点击预删除记录条后面的删除按钮，对内网信息配置表进行单条删除。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“引擎设置”选项卡，切换到“引擎设置”页面。
- 2、开启与关闭引擎：通过是否勾选各引擎“开启”选择框的操作，设置引擎状态。,

根据需要，开启或关闭监测引擎：

Cncert深度报文检测引擎 开启

Cncert病毒检测引擎 开启

Cncert异常通信行为监测引擎 开启

点击“保存”按钮，保存引擎状态更改。

设备管理	网络配置	用户管理	监听配置	组件设置	时间同步	预警管理	升级管理	调试配置	重要用户	自定义流量	白名单	系统操作日志																																																																																																		
当前位置：系统管理 > 组件设置																																																																																																														
根据需要，开启或关闭监测引擎：																																																																																																														
Cncert深度报文检测引擎		<input type="checkbox"/> 开启																																																																																																												
Cncert病毒检测引擎		<input checked="" type="checkbox"/> 开启																																																																																																												
Cncert异常通信行为监测引擎		<input checked="" type="checkbox"/> 开启																																																																																																												
内网信息配置表：																																																																																																														
<table border="1"> <thead> <tr> <th>+ 新增</th><th>序号</th><th>名称</th><th>IP列表</th><th>IP类型</th><th>创建时间</th><th>创建者</th><th>创建者IP</th><th>备注</th><th>操作</th><th colspan="4"></th></tr> </thead> <tbody> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4"></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4"></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4"></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4"></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4"></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td colspan="4"></td></tr> </tbody> </table>													+ 新增	序号	名称	IP列表	IP类型	创建时间	创建者	创建者IP	备注	操作																																																																																								
+ 新增	序号	名称	IP列表	IP类型	创建时间	创建者	创建者IP	备注	操作																																																																																																					
<table border="1"> <tr> <td><input type="button" value="保存"/></td><td><input type="button" value="取消"/></td><td colspan="11"></td></tr> </table>													<input type="button" value="保存"/>	<input type="button" value="取消"/>																																																																																																
<input type="button" value="保存"/>	<input type="button" value="取消"/>																																																																																																													

3、添加内网信息：如果用户需新增内网配置信息，点击“新增”按钮，

根据需要，开启或关闭监测引擎：																																																																																					
Cncert深度报文检测引擎		<input type="checkbox"/> 开启																																																																																			
Cncert病毒检测引擎		<input checked="" type="checkbox"/> 开启																																																																																			
Cncert异常通信行为监测引擎		<input checked="" type="checkbox"/> 开启																																																																																			
内网信息配置表：																																																																																					
<table border="1"> <tr> <td>+ 新增</td><td>序号</td><td>名称</td><td>IP列表</td><td>IP类型</td><td>创建时间</td><td>创建者</td><td>创建者IP</td><td>备注</td><td>操作</td><td colspan="4"></td></tr> <tr><td></td><td>1</td><td>2</td><td>3.3.3.3-5.5.5.5</td><td>内网IP</td><td>2015-02-02 13:41:25</td><td>admin</td><td>172.16.19.5</td><td>111</td><td></td><td></td><td colspan="4"></td></tr> <tr><td></td><td>2</td><td>111</td><td>1.1.1.1-2.2.2.2</td><td>内网IP</td><td>2015-02-02 13:21:09</td><td>admin</td><td>172.16.19.5</td><td>q</td><td></td><td></td><td colspan="4"></td></tr> <tr><td></td><td>3</td><td>1</td><td>6.6.6.6-9.9.9.9</td><td>邮件服务器</td><td>2015-02-02 13:46:05</td><td>admin</td><td>172.16.19.5</td><td>111</td><td></td><td></td><td colspan="4"></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>													+ 新增	序号	名称	IP列表	IP类型	创建时间	创建者	创建者IP	备注	操作						1	2	3.3.3.3-5.5.5.5	内网IP	2015-02-02 13:41:25	admin	172.16.19.5	111								2	111	1.1.1.1-2.2.2.2	内网IP	2015-02-02 13:21:09	admin	172.16.19.5	q								3	1	6.6.6.6-9.9.9.9	邮件服务器	2015-02-02 13:46:05	admin	172.16.19.5	111																				
+ 新增	序号	名称	IP列表	IP类型	创建时间	创建者	创建者IP	备注	操作																																																																												
	1	2	3.3.3.3-5.5.5.5	内网IP	2015-02-02 13:41:25	admin	172.16.19.5	111																																																																													
	2	111	1.1.1.1-2.2.2.2	内网IP	2015-02-02 13:21:09	admin	172.16.19.5	q																																																																													
	3	1	6.6.6.6-9.9.9.9	邮件服务器	2015-02-02 13:46:05	admin	172.16.19.5	111																																																																													

弹出内网信息配置界面，

添加内网配置信息

名称：	<input type="text"/>
IP：	<input type="text"/> - <input type="text"/>
IP类型：	<input type="button" value="▼"/>
备注：	<input type="button" value="内网IP"/> <input type="button" value="web服务器"/> <input type="button" value="邮件服务器"/>

根据上图填写相关信息，然后点击“保存”按钮，内网配置信息添加成功。



注意

在开启 cncert 异常通信行为监测引擎时，必须添加相应的内网信息配置；内网信息配置表主要是配置用户需要监测的内网服务器，以及内网主机，以便 APT 引擎监测服务器的异常行为。APT 引擎会根据内网信息配置，监测如下几种异常通信行为情况，并且监测结果会实时地显示在首页：

- 1) 协议不匹配的异常通信行为。
- 2) 晚八点到早八点时间段之外的通信异常行为情况。
- 3) 内网服务器主动连接外网 IP 的异常通信行为。
- 4) 内网主机主动连接外网 IP 的异常行为。

4、内网信息修改：如果用户需要对已添加的内网信息修改，点击对应内网信的修改按钮 ，弹出内网信息修改页面，

修改APT引擎配置

名称 :	2
IP :	3.3.3.3 - 5.5.5.5
IP类型 :	内网IP
备注 :	111

根据上图输入修改信息，然后点击“保存”按钮，保存修改。

- 5、删除内网信息：如果用户需要删除已经配置的内网信息，点击对应内网信息上的删除按钮 ，对应内网信息被删除。

2.4.7 时间设置

此模块记录设备的时间，可以进行时间手动设置和自动同步。

设备管理 网络配置 用户管理 监听配置 组件设置 时间同步 预警管理 升级管理 调试配置 重要用户 自定义流量 白名单 系统操作日志

当前位置 : 系统管理 > 时间同步

同步方式: 自动 手动

当前时间: "2015-02-04 14:19:14 CST" *

同步NTP服务器: Time.windows.com *

端口号: 123 *

保存时立即同步时间

图2-59 时间同步效果展示图

一、此模块可进行的操作：

1、自动同步：可对同步 NTP 服务器 IP 地址、同步服务器端口号进行配置修改。

2、手动设置：可对当前时间、时区进行配置。

二、此模块的操作流程：

1、 登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“时间设置”选项卡，切换到“时间设置”页面。

2、 自动同步时间：如果用户想将设备时间设为自动同步，选择同步方式为“自动同步”，对同步 NTP 服务器 IP 地址、同步服务器端口号进行配置修改，点击保存时立即同步时间“”按钮，点击“保存”按钮，则时间同步设置成功。



同步方式: 自动 手动

当前时间: "2015-02-02 16:18:25 CST" *

同步NTP服务器: [] *

端口号 [] *

保存时立即同步时间

保存 取消

将同步方式选为“自动”

同步方式: 自动 手动

当前时间: "2015-02-02 16:20:00 CST" *

同步NTP服务器: *

端口号 *

保存时立即同步时间

保存 取消

对同步 NTP 服务器 IP 地址及端口号进行设置

同步方式: 自动 手动

当前时间: "2015-02-03 16:59:44 CST" *

同步NTP服务器: *

端口号 *

保存时立即同步时间

保存 取消

点击保存时立即同步时间 “” 按钮，点击“保存”，时间自动同步完成



注意 必须点击保存时立即同步时间 “” 按钮，否则时间将无法自动同步。

3、 手动修改时间：如果用户想手动设置时间，将同步方式选为“手动”，对当前时间及时区进行设置，点击保存，则手动设置时间成功。

同步方式: 自动 手动

当前时间: "2015-02-02 16:12:49 CST" *

设置当前时间:  *

时区选择:

将同步方式选为“手动”

同步方式: 自动 手动

当前时间: "2015-02-02 16:14:40 CST" *

设置当前时间:  2015年 二月

时区选择:

点击“

版权所有 © 长安通信

同步方式: 自动 手动

当前时间: "2015-02-02 16:14:57 CST" *

设置当前时间: 2015-02-02 15:54:49

时区选择:

- (UTC-12:00)国际日期变更线西
- (UTC-11:00)协调世界时-11
- (UTC-10:00)夏威夷
- (UTC-09:00)阿拉斯加
- (UTC-08:00)太平洋时间 (美国和加拿大)

在下拉菜单进行时区选择

同步方式: 自动 手动

当前时间: "2015-02-02 16:15:57 CST" *

设置当前时间: 2015-02-02 15:54:49

时区选择: (UTC+08:00)北京,重庆,香港特别行政区,乌鲁木齐 *

点击“保存按钮”，手动设置时间完成。

2.4.8 预警管理

此模块记录了预警设置的相关信息，包括：Syslog 接收服务器 IP 地址、Syslog 接收服务器端口、Syslog 程序模块（facility）、Syslog 严重级别（severity）的详细信息。



The screenshot shows the 'Syslog Alert Management' configuration page. At the top, there is a navigation bar with tabs: 设备管理, 网络配置, 用户管理, 捕包设置, 引擎设置, 时间设置, 预警管理 (highlighted in purple), 升级设置, 维护设置, 重要用户, 自定义流量, 白名单, and 操作日志. Below the navigation bar, a breadcrumb trail indicates the current location: 当前位置 : 系统管理 > 预警管理. The main content area is titled 'Syslog Alert Settings'. It contains the following configuration fields:

- 开启预警设置
- Syslog接收服务器IP地址: * 172.16.19.11
- Syslog接收服务器端口: * 254
- Syslog程序模块 (facility): all
- Syslog严重级别 (severity): 疑似

At the bottom of the form are two buttons: 保存 (Save) and 取消 (Cancel).

图2-60 预警管理效果展示图

一、此模块可进行的操作:

- 1、开启预警设置：可对 Syslog 接收服务器 IP 地址、Syslog 接受服务器端口、Syslog 程序模块（facility）、Syslog 严重级别（severity）进行修改。*为必填字段。
- 2、关闭预警设置。



说明

- a. 用户需要自行搭建 syslog 服务器，端口默认为 514。
- b. 程序模块分为 local 和 all。
 - 1) Local 代表模块日志
 - 2) All 代表系统日志
- c. 严重级别分为，高、中、低、疑似。

二、此模块的操作流程:

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“预警管理”选项卡，切换到“预警管理”页面。

2、开启预警设置：如果用户需开启预警设置，点击开启预警设置“”按钮，开启预警设置变为“”，对 Syslog 接收服务器 IP 地址、Syslog 接受服务器端口、Syslog 程序模块（facility）、Syslog（severity）进行配置，点击“保存”按钮，预警设置成功。



点击“”按钮，会弹出

Syslog接收服务器端口/IP地址：	172.16.19.11
Syslog接收服务器端口：	514
Syslog程序模块 (facility) :	local
Syslog程序模块 (severity) :	高

根据上图进行信息填写，点击“保存”按钮

3、关闭预警设置：如果用户需要关闭预警设置，点击开启预警设置“”按钮，开启预警设置变为“”，关闭预警管理。



Syslog接收服务器端口/IP地址 :

Syslog接收服务器端口:

Syslog程序模块 (facility):

Syslog程序模块 (severity):

保存 取消




开启预警设置

关闭预警功能

2.4.9 升级设置

用户从阿里云上下载最新的升级包，升级过程中用户界面应处于不可用状态。升级成功首页系统状态会显示升级后的版本。



序号	升级时间	升级内容	升级前版本	升级后版本	升级结果	操作用户	操作IP

图2-61 升级管理效果展示图

一、此模块可进行的操作：

- 1、升级日志查询：可根据升级时间、操作用户对升级日志进行查询。查询结果对用户的每次升级操作进行记录，记录信息包括升级时间、升级内容（事件库升级/

系统升级)、升级前版本、升级后版本、升级结果(成功/失败)、操作者、操作者IP。

2、离线升级：支持用户将通过其他方式（网站下载、厂商索取）获取的升级包进行导入，进行补救升级。

二、此模块的操作流程：

- 1、登陆页面：进入web界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“升级设置”选项卡，切换到“升级设置”页面。
- 2、离线升级：用户可进行离线升级，点击离线升级按钮，会弹出，将升级包导入，点击保存，开始升级，升级完成后，升级管理会记录此次升级的信息和结果。



当前位置：系统管理 > 系统升级

条件设置

开始时间： 结束时间： 操作用户：




当前位置：系统管理 > 系统升级

条件设置

开始时间： 结束时间： 操作用户：

序号	升级时间	升级内容	升级前版本	升级后版本	升级结果	操作用户	操作IP
1	2015-06-03 08:28:55	系统升级	2.2.0.5730.15060114	2.2.0.5759.15060216	升级成功		
2	2015-06-01 15:47:25	系统升级	2.2.0.5618.15052810	2.2.0.5730.15060114	升级成功		

3、查询升级记录：升级管理，用户可根据升级时间、操作用户对升级日志进行查询。



设备管理 网络配置 用户管理 插包设置 引擎设置 时间设置 预警管理 升级设置 维护设置 重要用户 自定义流量 白名单 操作日志

当前位置：系统管理 > 系统升级

条件设置

开始时间: 2015-06-01 00:00:00 结束时间: 2015-06-04 09:26:15 操作用户: []

查询

离线升级

序号	升级时间	升级内容	升级前版本	升级后版本	升级结果	操作用户	操作IP
1	2015-06-03 08:28:55	系统升级	2.2.0.5730.15060114	2.2.0.5759.15060216	升级成功		
2	2015-06-01 15:47:25	系统升级	2.2.0.5618.15052810	2.2.0.5730.15060114	升级成功		

2.4.10 维护设置

用户可以通过此模块开启或关闭 SSH 远程维护，并可以导出 des 加密的调试信息。



图2-62 调试配置效果展示图

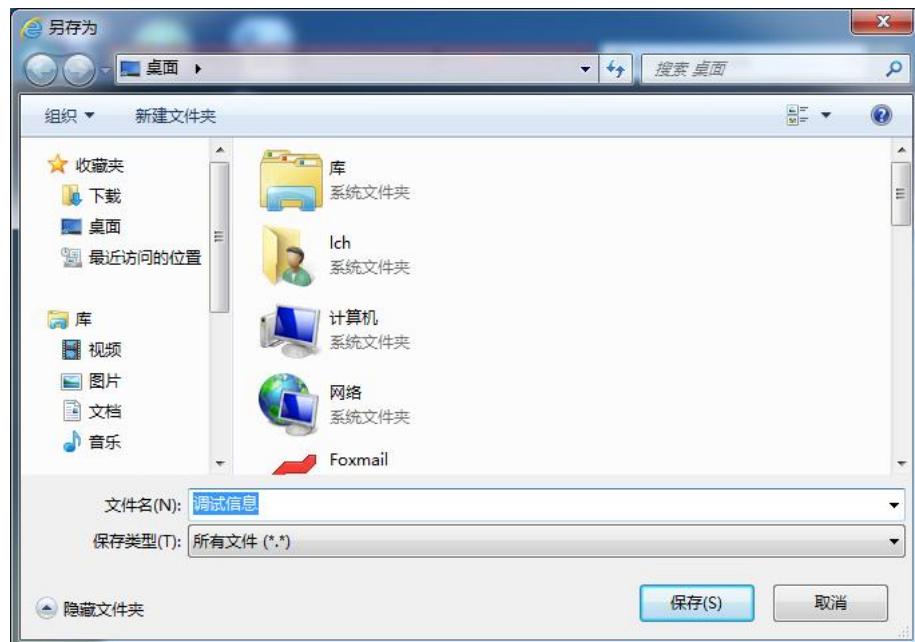
一、此模块可进行的操作：

- 1、开启与关闭远程维护 SSH 功能。
- 2、调试信息导出：可将调试信息（TXT 文件）导出到本地。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“维护设置”选项卡，切换到“维护设置”页面。

- 2、开启 SSH：点击开启“”按钮，启用远程维护（SSH）变为“”状态，开启成功，远程维护 SSH 开启后，用户可以用 putty 等支持 ssh 登录方式的工具进行系统后台登陆操作。
- 3、关闭 SSH：点击开启“”按钮，启用远程维护（SSH）变为“”状态，关闭成功。
- 4、导出：点击调试信息导出，会弹出存放路径界面，将调试信息保存到本地即可，可选任意路径存放。



说明 导出的调试信息是经过 des 加密的。

2.4.11 重要用户

此模块记录了一些重要用户的信息。

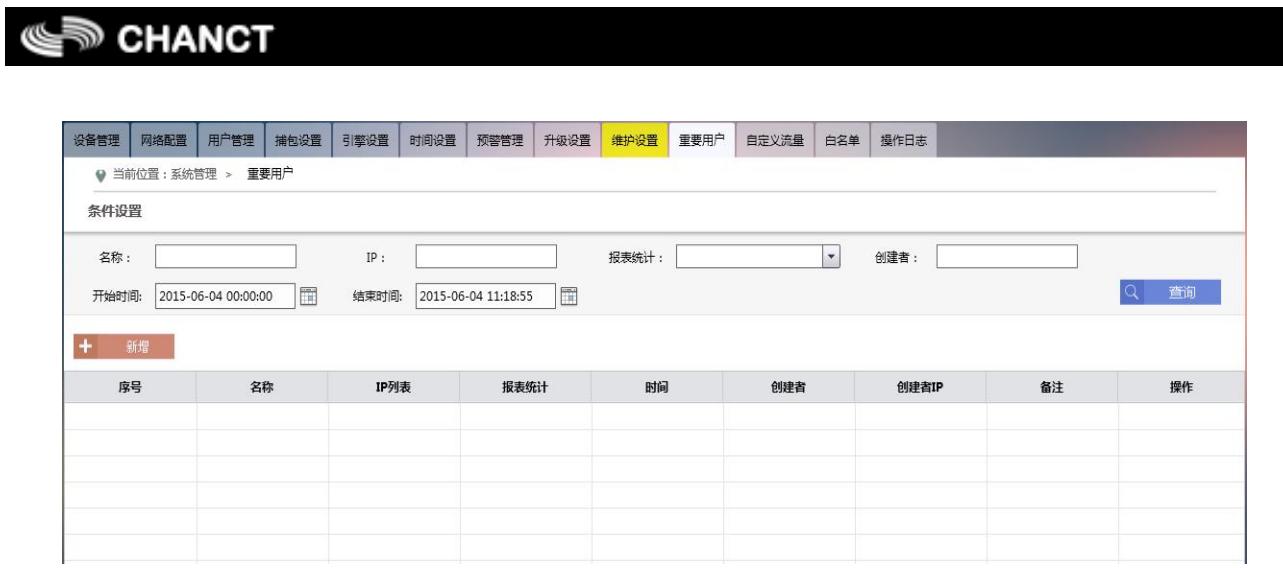


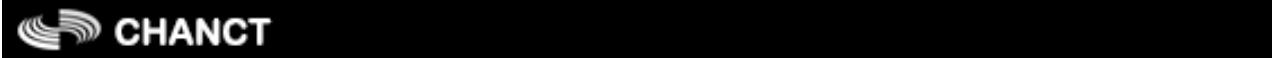
图2-63 重要用户

一、此模块可进行的操作：

- 1、查询：支持用户按名称、IP、是否报表统计、创建者、创建时间进行记录查询。
 - 2、新增：用户通过点击“新增”按钮添加记录，可配置信息包括：配置项名称、IP/IP段、是否进行报表统计、备注信息。
 - 3、修改：用户可以对已配置信息进行修改，可修改项包括：配置项名称、IP/IP段、是否进行报表统计、备注信息，若用户进行了修改，则时间对应更新为修改时间。
 - 4、删除：点击预删除用户后面的删除按钮，对用户进行单条删除。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“重要用户”选项卡，切换到“重要用户”页面。
 - 2、新增重要用户息：如果用户想要查看某一段的 IP，可点击“新增”，会弹出新增界面，根据界面需要填写的信息进行填写然后点击“保存”，重要用户就添加成功了。



设备管理	网络配置	用户管理	捕包设置	引擎设置	时间设置	预警管理	升级设置	维护设置	重要用户	自定义流量	白名单	操作日志
当前位置：系统管理 > 重要用户												
条件设置												
名称：	<input type="text"/>	IP：	<input type="text"/>	报表统计：	<input type="text"/>	创建者：	<input type="text"/>					
开始时间:	2015-06-01 00:00:00	<input type="button" value=""/>	结束时间:	2015-06-04 11:18:55	<input type="button" value=""/>							
+ 新增												
序号	名称	IP列表	报表统计	时间	创建者	创建者IP	备注	操作				
1	47dfjvfydfvdvn	2.2.2.3-3.3.3.242	是	2015-06-03 16:57:18	gly	172.16.11.12						
2	483875	1.1.1.1-2.2.2.2	是	2015-06-03 16:56:40	gly	172.16.11.12						
3	test	192.168.0.1-192.168.0.254	否	2015-06-03 15:32:09	admin	127.0.0.1						
4	zzh	192.0.0.1-192.255.255.254	是	2015-06-03 11:53:39	admin	172.16.10.17						

↓

添加重要用户

名称：

IP： -

备注：

报表中进行统计： 是 否

保存 **取消**

若添加的名称和 IP 段有重复，点击保存后，弹出提示信息。



3、查看重要用户事件：

- 1) 重要用户配置的 IP，在首页和查询中就会被标红。

序号	威胁等级	事件名	发生次数	开始时间	结束时间	感染端IP	控制端IP
1	疑似	木马-其他-malicious.URI.C61C	2	2014-06-29 09:59:53	2014-06-29 09:59:53	211.94.163.18	42.156.140.222
2	疑似	木马-其他-Trojan.Win32.Sasfis.AB	2	2014-06-29 09:59:53	2014-06-29 09:59:53	211.94.163.18	42.156.140.222
3	疑似	木马-其他-malicious.URI.C61C	4	2014-06-29 09:59:50	2014-06-29 09:59:50	211.94.163.5	42.156.140.23
4	疑似	木马-其他-Trojan.Win32.Sasfis.AB	4	2014-06-29 09:59:50	2014-06-29 09:59:50	211.94.163.217	42.156.140.19
5	疑似	木马-其他-malicious.URI.C61C	2	2014-06-29 09:59:50	2014-06-29 09:59:50	211.94.162.115	42.156.140.222
6	疑似	木马-其他-malicious.URI.C61C	4	2014-06-29 09:59:50	2014-06-29 09:59:50	211.94.163.217	42.156.140.19
7	疑似	木马-其他-Trojan.Win32.Sasfis.AB	4	2014-06-29 09:59:50	2014-06-29 09:59:50	211.94.163.5	42.156.140.23

2) 新增的重要用户名会在查询条件“重要用户”的下拉菜单中显示。

病毒类型 :

重要用户 :

威胁等级 :

4、重要用户信息查询：重要用户也可根据名称、IP、是否报表统计、创建者和时间查询。

设备管理 网络配置 用户管理 捕包设置 引擎设置 时间设置 预警管理 升级设置 维护设置 重要用户 自定义流量 白名单 操作日志

当前位置 : 系统管理 > 重要用户

条件设置

名称 :	<input type="text"/>	IP :	<input type="text"/>	报表统计 :	<input type="text"/>	创建者 :	<input type="text"/>
开始时间:	2015-06-01 00:00:00	结束时间:	2015-06-04 11:18:55	<input type="button" value="查询"/>			

+ 新增

序号	名称	IP列表	报表统计	时间	创建者	创建者IP	备注	操作
1	47dfjfyvdfvdvn	2.2.2.3-3.3.3.242	是	2015-06-03 16:57:18	gly	172.16.11.12		
2	483875	1.1.1.1-2.2.2.2	是	2015-06-03 16:56:40	gly	172.16.11.12		
3	test	192.168.0.1-192.168.0.254	否	2015-06-03 15:32:09	admin	127.0.0.1		
4	zzh	192.0.0.1-192.255.255.254	是	2015-06-03 11:53:39	admin	172.16.10.17		

5、重要用户信息修改：对已添加的重要用户做修改，点击笔状的图标，然后，会弹出修改界面，进行修改。





6、重要用户信息删除：可删除已经配置的重要用户，只需点击该条配置的  按钮。

2.4.12 自定义流量

此模块记录了一些自定义流量配置的信息。

图2-64 自定义流量配置效果展示图

一、此模块可进行的操作：

- 1、查询：支持用户按名称、IP、是否首页显示、创建者、创建时间查询。
- 2、新增：用户通过点击“新增”按钮添加记录，可配置信息包括：名称、IP/IP段、是否首页显示、备注。
- 3、修改：通过点击预修改用户信息后面的修改按钮可以进行修改，时间则对应更新为修改时间。

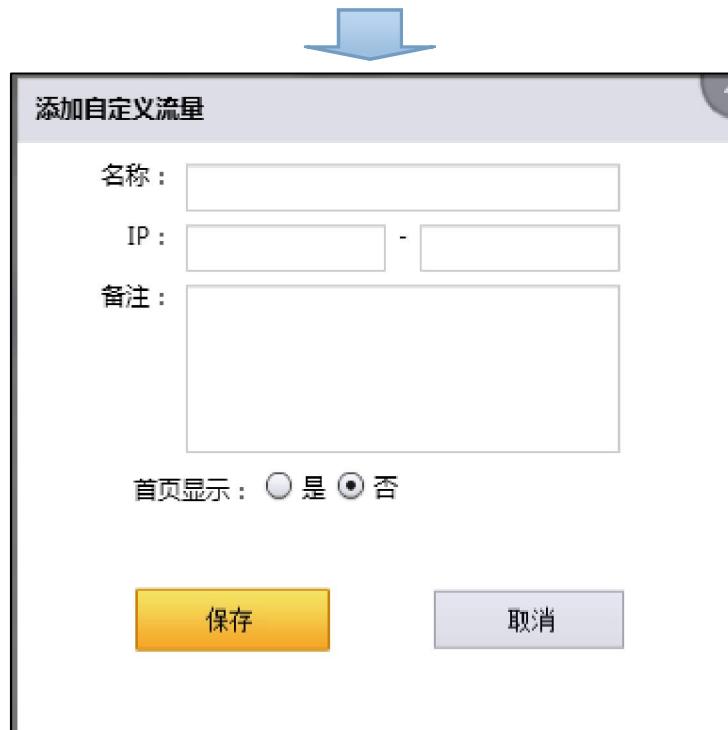
4、删除：点击预删除用户后面的按钮，对用户进行单条删除。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“自定义流量”选项卡，切换到“自定义流量”页面。
- 2、添加自定义流量：如果用户想要查看某段 IP 的流量可点击“新增”，会弹出新增界面，根据界面需要填写的信息进行填写然后点击“保存”，自定义流量就添加成功了。



The screenshot shows the 'Custom Traffic' management page. At the top, there is a navigation bar with various tabs: 设备管理, 网络配置, 用户管理, 捕包设置, 引擎设置, 时间设置, 预警管理, 升级设置, 维护设置, 重要用户, 自定义流量, 白名单, and 操作日志. The '自定义流量' tab is currently selected. Below the navigation bar, there is a breadcrumb trail: 当前位置: 系统管理 > 自定义流量. Underneath the breadcrumb, there is a 'Condition Settings' section with fields for Name, IP, Home Display, Creator, Start Time, and End Time. A search bar with a magnifying glass icon and a 'Query' button are also present. At the bottom of this section is a red-highlighted 'New' button (带有新增). Below this is a table with columns: 序号, 名称, 内容, 首页显示, 创建时间, 创建者, 创建者IP, 备注, and 操作. The table is currently empty.

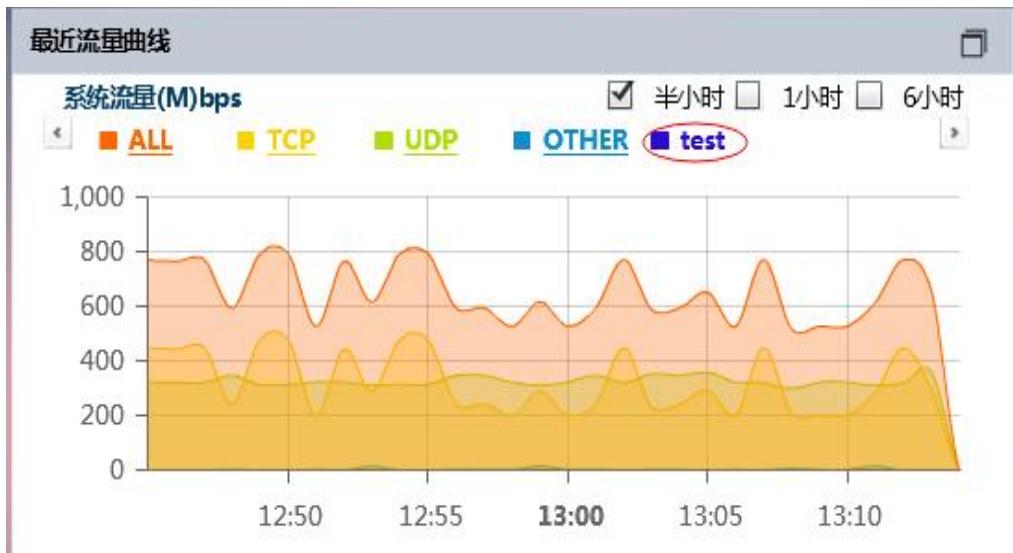


The screenshot shows the 'Add Custom Traffic' dialog box. It has fields for 'Name', 'IP' (with a range separator), and 'Remarks'. Below these fields is a 'Home Display' section with radio buttons for 'Yes' (selected) and 'No'. At the bottom of the dialog are two buttons: a yellow 'Save' button and a grey 'Cancel' button. A large blue arrow points from the 'New' button on the main page down to this dialog box.

若添加的名称和 IP 段有重复，点击保存后，弹出提示信息。



3、首页查看自定义流量：在首页中的最近流量曲线中就会显示添加的自定义流量。



4、查询页面查看自定义流量：新增的自定义流量，会在流量查询的条件设置中看到。

5、自定义流量信息查询：自定义流量也可根据名称、IP、首页显示、创建者和时间查询。

设备管理 网络配置 用户管理 捕包设置 引擎设置 时间设置 预警管理 升级设置 维护设置 重要用户 自定义流量 白名单 操作日志

当前位置：系统管理 > 自定义流量

条件设置

名称:	<input type="text"/>	IP:	<input type="text"/>	首页显示:	<input type="text"/>	创建者:	<input type="text"/>
开始时间:	<input type="text"/> 2015-06-04 00:00:00	结束时间:	<input type="text"/> 2015-06-04 11:26:34	<input type="button" value="查询"/>			

+ 新增

序号	名称	内容	首页显示	创建时间	创建者	创建者IP	备注	操作
----	----	----	------	------	-----	-------	----	----

6、自定义流量信息修改: 可对已添加的自定义流量做修改, 点击笔状的图标, 然后, 会弹出修改界面, 进行修改。



修改自定义流量

名称:	<input type="text"/> test
IP:	<input type="text"/> 172.31.0.11 - <input type="text"/> 172.31.0.100
备注:	<input type="text"/>
首页显示: <input checked="" type="radio"/> 是 <input type="radio"/> 否	
<input type="button" value="保存"/> <input type="button" value="取消"/>	

7、自定义流量信息删除: 可删除已经添加的自定义流量, 只需点击该条的  按钮。

2.4.13 白名单配置

此模块记录了一些白名单配置的信息。



设备管理 网络配置 用户管理 捕包设置 引擎设置 时间设置 预警管理 升级设置 维护设置 重要用户 自定义流量 白名单 操作日志

当前位置：系统管理 > 白名单

条件设置

名称： IP： 创建者：
开始时间： 结束时间：

+ 新增

序号	名称	IP列表	创建时间	创建者	创建者IP	备注	操作

图2-65 白名单配置效果展示图

一、此模块可进行的操作：

- 1、查询：用户可按名称、IP、创建者、时间进行配置查询。
- 2、新增：用户通过点击“新增”按钮添加记录，可配置信息包括：配置项名称、IP/IP段、备注信息。
- 3、修改：通过点击预修改用户信息后面的修改按钮可以进行修改，并将时间更新为修改时间。
- 4、删除：点击预删除用户后面的按钮，对用户进行单条删除。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“白名单”选项卡，切换到“白名单”页面。
- 2、新增白名单：如果用户不需要看到某段 IP 的事件可点击“新增”，会弹出新增界面，根据界面需要填写的信息进行填写然后点击“保存”，白名单就添加成功了。

设备管理 网络配置 用户管理 捕包设置 引擎设置 时间设置 预警管理 升级设置 维护设置 重要用户 自定义流量 白名单 操作日志

当前位置：系统管理 > 白名单

条件设置

名称： IP： 创建者：
开始时间： 结束时间：

+ 新增

序号	名称	IP列表	创建时间	创建者	创建者IP	备注	操作

添加白名单

名称 :	<input type="text"/>
IP :	<input type="text"/> - <input type="text"/>
备注 :	<input type="text"/>

保存 **取消**

若添加的名称和 IP 段有重复，点击保存后，弹出提示信息。



在“查询”模块中就不会看到这段 ip 的事件了。

3、白名单信息查询：白名单用户可按名称、IP、创建者、时间进行配置查询。

设备管理 网络配置 用户管理 捕包设置 引擎设置 时间设置 预警管理 升级设置 维护设置 重要用户 自定义流量 白名单 操作日志

当前位置：系统管理 > 白名单

条件设置

名称:	<input type="text"/>	IP:	<input type="text"/>	创建者:	<input type="text"/>
开始时间:	2015-06-04 20:00:00	结束时间:	2015-06-04 11:27:32	<input type="button" value="查询"/>	

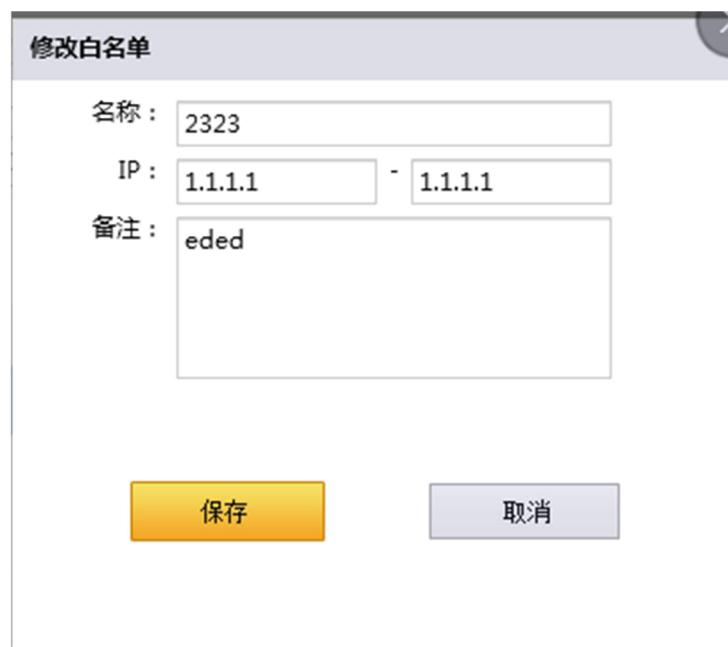
+ 新增

序号	名称	IP列表	创建时间	创建者	创建者IP	备注	操作

4、白名单信息修改：可对已添加的白名单做修改，点击笔状的图标。



然后，会弹出修改界面，进行修改。



5、白名单信息删除：可删除已经添加的白名单，只需点击该条的  按钮。

2.4.14 系统操作日志

此模块记录了登录与退出、数据查询、系统管理、报表管理、升级管理和用户帮助的各项操作。

主要展示了：用户名、用户IP、操作时间、操作模块（登录与退出，数据查询-恶意代码感染事件、网站事件、通信行为异常事件、恶意代码传播事件、恶意URL访问事件查询、攻击尝试事件查询、其他事件查询、流量查询，系统管理-重要用户配置、自定义流量配置、白名单配置、设备管理、用户管理、系统操作日志、数据备份、系统授权，报表管理，升级管理和用户帮助）、操作类型（登录与退出-（登录、退出）；恶意代码感染事件、网站事件、通信行为异常事件、恶意代码传播事件、恶意URL访问事件查询、攻击尝试事件查询、其他事件查询-（增删改查）、流量查询-（查询）；重要用户配置、自定义流量配置、白名单配置、设备管理-（增删改查）、用户管理-（增删改查、锁定、解锁）、系统操作日志-（查询、导出）、数据备份-（查询、备份、设定周期、下载）、系统授权-（授权申请、授权）；报表管理-更新、下载、生成；升级管理-查询、升级；用户帮助-查看）、操作描述。



设备管理	网络配置	用户管理	捕包设置	引擎设置	时间设置	预警管理	升级设置	维护设置	重要用户	自定义流量	白名单	操作日志																																																																																				
当前位置 : 系统管理 > 操作日志																																																																																																
条件设置																																																																																																
开始时间: 2015-06-04 00:00:00 <input type="button" value=""/>																																																																																																
结束时间: 2015-06-04 11:28:39 <input type="button" value=""/>																																																																																																
操作用户: <input type="text"/>																																																																																																
操作模块: <input type="text"/>																																																																																																
<input type="button"/> <input type="button" value="查询"/>																																																																																																
<table border="1"><thead><tr><th>序号</th><th>用户名</th><th>用户IP</th><th>操作时间</th><th>操作模块</th><th>操作类型</th><th>操作描述</th></tr></thead><tbody><tr><td>1</td><td>admin</td><td>172.16.10.7</td><td>2015-06-04 11:22:04</td><td>重要用户</td><td>查询</td><td>重要用户查询成功</td></tr><tr><td>2</td><td>admin</td><td>172.16.11.10</td><td>2015-06-04 11:14:08</td><td>登录与退出</td><td>退出</td><td>正常登出</td></tr><tr><td>3</td><td>admin</td><td>172.16.11.12</td><td>2015-06-04 11:13:43</td><td>登录与退出</td><td>登录</td><td>登录成功。</td></tr><tr><td>4</td><td>admin</td><td>172.16.11.12</td><td>2015-06-04 11:10:51</td><td>登录与退出</td><td>退出</td><td>登陆超时系统退出</td></tr><tr><td>5</td><td>admin</td><td>172.16.11.10</td><td>2015-06-04 11:09:11</td><td>登录与退出</td><td>登录</td><td>登录成功。</td></tr><tr><td>6</td><td>admin</td><td>172.16.10.19</td><td>2015-06-04 11:08:07</td><td>登录与退出</td><td>登录</td><td>登录成功。</td></tr><tr><td>7</td><td>admin</td><td>172.16.10.7</td><td>2015-06-04 11:03:25</td><td>升级管理</td><td>查询</td><td>查询升级列表成功</td></tr><tr><td>8</td><td>admin</td><td>172.16.10.7</td><td>2015-06-04 11:03:17</td><td>升级管理</td><td>查询</td><td>查询升级列表成功</td></tr><tr><td>9</td><td>admin</td><td>172.16.10.7</td><td>2015-06-04 10:58:23</td><td>升级管理</td><td>查询</td><td>查询升级列表成功</td></tr><tr><td>10</td><td>admin</td><td>172.16.10.7</td><td>2015-06-04 10:56:54</td><td>升级管理</td><td>查询</td><td>查询升级列表成功</td></tr><tr><td>11</td><td>admin</td><td>172.16.10.19</td><td>2015-06-04 10:30:02</td><td>登录与退出</td><td>退出</td><td>登陆超时系统退出</td></tr></tbody></table>													序号	用户名	用户IP	操作时间	操作模块	操作类型	操作描述	1	admin	172.16.10.7	2015-06-04 11:22:04	重要用户	查询	重要用户查询成功	2	admin	172.16.11.10	2015-06-04 11:14:08	登录与退出	退出	正常登出	3	admin	172.16.11.12	2015-06-04 11:13:43	登录与退出	登录	登录成功。	4	admin	172.16.11.12	2015-06-04 11:10:51	登录与退出	退出	登陆超时系统退出	5	admin	172.16.11.10	2015-06-04 11:09:11	登录与退出	登录	登录成功。	6	admin	172.16.10.19	2015-06-04 11:08:07	登录与退出	登录	登录成功。	7	admin	172.16.10.7	2015-06-04 11:03:25	升级管理	查询	查询升级列表成功	8	admin	172.16.10.7	2015-06-04 11:03:17	升级管理	查询	查询升级列表成功	9	admin	172.16.10.7	2015-06-04 10:58:23	升级管理	查询	查询升级列表成功	10	admin	172.16.10.7	2015-06-04 10:56:54	升级管理	查询	查询升级列表成功	11	admin	172.16.10.19	2015-06-04 10:30:02	登录与退出	退出	登陆超时系统退出
序号	用户名	用户IP	操作时间	操作模块	操作类型	操作描述																																																																																										
1	admin	172.16.10.7	2015-06-04 11:22:04	重要用户	查询	重要用户查询成功																																																																																										
2	admin	172.16.11.10	2015-06-04 11:14:08	登录与退出	退出	正常登出																																																																																										
3	admin	172.16.11.12	2015-06-04 11:13:43	登录与退出	登录	登录成功。																																																																																										
4	admin	172.16.11.12	2015-06-04 11:10:51	登录与退出	退出	登陆超时系统退出																																																																																										
5	admin	172.16.11.10	2015-06-04 11:09:11	登录与退出	登录	登录成功。																																																																																										
6	admin	172.16.10.19	2015-06-04 11:08:07	登录与退出	登录	登录成功。																																																																																										
7	admin	172.16.10.7	2015-06-04 11:03:25	升级管理	查询	查询升级列表成功																																																																																										
8	admin	172.16.10.7	2015-06-04 11:03:17	升级管理	查询	查询升级列表成功																																																																																										
9	admin	172.16.10.7	2015-06-04 10:58:23	升级管理	查询	查询升级列表成功																																																																																										
10	admin	172.16.10.7	2015-06-04 10:56:54	升级管理	查询	查询升级列表成功																																																																																										
11	admin	172.16.10.19	2015-06-04 10:30:02	登录与退出	退出	登陆超时系统退出																																																																																										
首页 <input type="button"/> 上一页 <input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/> 下一页 <input type="button" value="末尾页"/> <input type="text"/> GO																																																																																																

图2-66 操作日志查看效果展示图

一、此模块可进行的操作:

- 1、查询：对操作用户、操作模块、操作时间、操作类型几个条件进行查询。注意操作类型查询条件是在选择操作模块条件下进行查询的。

二、此模块的操作流程：

- 1、登陆页面：进入 web 界面，点击导航栏中“系统管理”按钮，进入“系统管理”页面，然后点击“操作日志”选项卡，切换到“操作日志”页面。
- 2、操作日志查询：系统操作日志，用户可根据对操作用户、操作模块、操作时间、操作类型几个作为条件进行查询。注意操作类型查询条件是在选择操作模块条件下进行查询的。

设备管理	网络配置	用户管理	捕包设置	引擎设置	时间设置	预警管理	升级设置	维护设置	重要用户	自定义流量	白名单	操作日志
当前位置 : 系统管理 > 操作日志												
条件设置												
开始时间: 2015-06-04 00:00:00 <input type="button" value=""/>												
结束时间: 2015-06-04 11:28:39 <input type="button" value=""/>												
操作用户: <input type="text"/>												
操作模块: <input type="text"/>												
<input type="button"/> <input type="button" value="查询"/>												

当前位置：系统管理 > 操作日志

条件设置

开始时间: 结束时间: 操作用户: 操作模块: 查询

序号	用户名	用户IP	操作时间	操作模块	操作类型	操作描述
1	admin	172.16.10.7	2015-06-04 11:22:04	重要用户	查询	重要用户查询成功
2	admin	172.16.11.10	2015-06-04 11:14:08	登录与退出	退出	正常登出
3	admin	172.16.11.12	2015-06-04 11:13:43	登录与退出	登录	登录成功。
4	admin	172.16.11.12	2015-06-04 11:10:51	登录与退出	退出	登陆超时系统退出
5	admin	172.16.11.10	2015-06-04 11:09:11	登录与退出	登录	登录成功。
6	admin	172.16.10.19	2015-06-04 11:08:07	登录与退出	登录	登录成功。
7	admin	172.16.10.7	2015-06-04 11:03:25	升级管理	查询	查询升级列表成功
8	admin	172.16.10.7	2015-06-04 11:03:17	升级管理	查询	查询升级列表成功
9	admin	172.16.10.7	2015-06-04 10:58:23	升级管理	查询	查询升级列表成功

2.5 授权

2.5.1 WEB 界面登录

在浏览器中输入 GMS 管理地址(默认 IP 为 https://192.168.0.171), 初始管理员帐号: admin, 密码: 123456。如下图所示:



图2-67 关口 web 界面登录

2.5.2 填写授权申请

一、系统首次登陆界面需要对系统进行授权。用户登录关口管理页面首页后，点击右面的导航按钮，进入授权页面，填写授权申请。如下图所示：

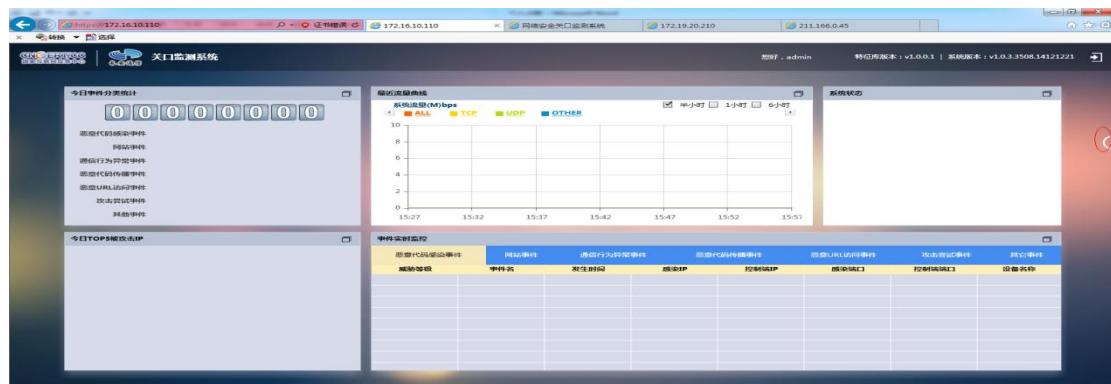


图2-68 关口 web 界面展示

授权

1.请填写如下授权申请信息，并导出授权申请文件：

申请人：

联系电话：

单位地址：

合同编号：

设备名称：

设备ID：

设备IP：

设备类型：

 导出申请

2.请将授权申请文件发送至邮箱:gms-support@chanct.com

3.请将收到的授权文件导入：

图2-69 授权申请填写界面

二、填写规范：

- 1、申请人：支持中文，长度不能超过 16byte；
- 2、联系电话：只能填写 11 个数字；
- 3、单位地址：支持中文，长度不能超过 32byte；
- 4、合同编号：长度不能超过 64byte；
- 5、设备名称：支持中文，长度不能超过 32byte（建议格式为“关口-单位名称”）；
- 6、设备 IP：请填写规范的 IP 地址；
- 7、设备类型：只有两种类型（监测点、管理点），请根据自身需要选择；
- 8、设备 ID 会默认显示在框中，如不显示说明设备有问题，请联系销售人员。

2.5.3 导出授权申请文件

一、授权信息填写无误后，点击“导出申请”。

授权

1. 请填写如下授权申请信息，并导出授权申请文件：

申请人：	xx
联系电话：	1234567890
单位地址：	xicheng
合同编号：	333
设备名称：	100监测
设备ID：	M788-HMAF-CCRV
设备IP：	172.31.100.100
设备类型：	监测点设备



图2-70 授权申请导出界面

二、点击“导出申请”后，选择授权申请文件存放路径。

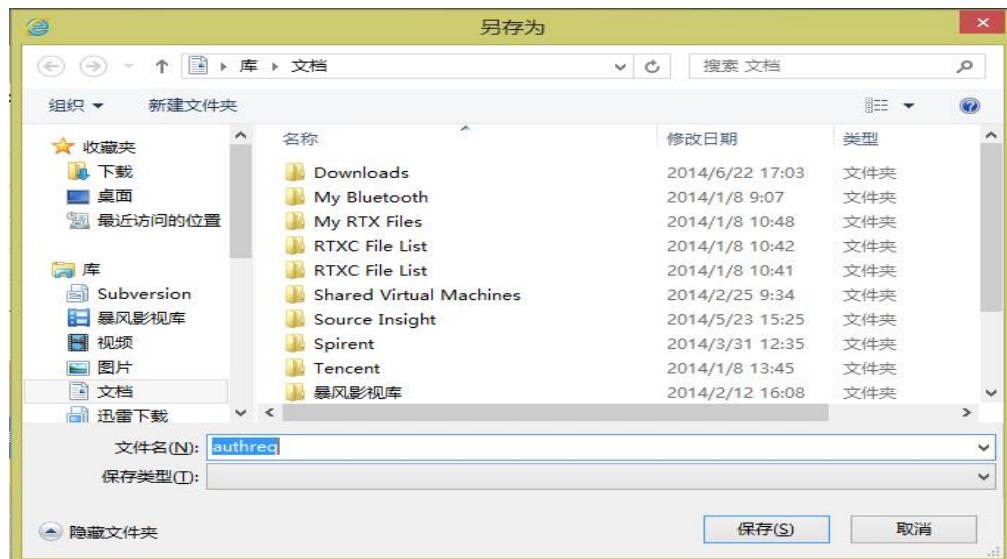


图2-71 授权申请导出路径界面

2.5.4 获取授权文件

将导出的授权申请文件发送至邮箱 gms-support@chanct.com，然后告知长安通信工作人员（热线电话 400-070-6665），稍后工作人员会将授权文件发送给您。

2.5.5 授权文件导入

收到授权文件后，登录 web 界面，切换到“授权”页面，在授权文件导入处，点击“浏览”按钮导入授权文件，然后点击“保存”按钮。



图2-72 授权导入界面

2.5.6 授权成功提醒

导入授权文件一分钟，会出现授权提醒：“授权成功！”。如下图所示：



说明 只有授权成功，查询模块、报表下载、系统管理才可使用。