**上网行为管理系统产品白皮书**

# 目 录

[目 录 2](#_bookmark0)

[1 互联网给企业管理带来的挑战 4](#_bookmark1)

[1.1 互联网 一把双刃剑 4](#_bookmark2)

[1.2 对员工上网行为进行规范管理势在必行 5](#_bookmark3)

[1.3 360 上网行为管理系统 帮您用好双刃剑 6](#_bookmark4)

[2 产品形态 7](#_bookmark5)

[2.1 硬件平台 7](#_bookmark6)

[2.2 软件系统 7](#_bookmark7)

[3 功能介绍 9](#_bookmark8)

[3.1 网页访问审计与过滤 9](#_bookmark9)

[3.1.1 最领先的中文 URL 分类数据库 9](#_bookmark10)

[3.1.2 灵活的 Web 策略设置 10](#_bookmark11)

[3.1.3 Web 访问违禁提示 12](#_bookmark12)

[3.2 应用控制 13](#_bookmark13)

[3.2.1 基于特征识别的覆盖全面的应用协议数据库 13](#_bookmark14)

[3.2.2 支持用户各项应用限额管理 14](#_bookmark15)

[3.2.3 灵活精细的管控策略 14](#_bookmark16)

[3.3 带宽管理 15](#_bookmark17)

[3.3.1 识别控制 P2P 软件和加密 P2P 数据 16](#_bookmark18)

[3.3.2 针对用户/应用设置带宽 16](#_bookmark19)

[3.3.3 基于时间段流量控制 17](#_bookmark20)

[3.4 内容审计和过滤 17](#_bookmark21)

[3.4.1 邮件收发审计和过滤 17](#_bookmark22)

[3.4.2 IM 审计和过滤 19](#_bookmark23)

[3.4.3 论坛发帖审计和过滤 19](#_bookmark24)

[3.4.4 搜索引擎关键字审计和过滤 19](#_bookmark25)

[3.4.5 HTTP 文件传输审计和过滤 20](#_bookmark26)

[3.4.6 HTTPS 加密网页的审计和过滤 20](#_bookmark27)

[3.4.7 FTP 文件传输审计和过滤 20](#_bookmark28)

[3.4.8 TELNET 内容审计 20](#_bookmark29)

[3.4.9 SSL 内容审计 20](#_bookmark30)

[3.4.10 数据库审计 20](#_bookmark31)

[3.5 终端控制与准入 21](#_bookmark32)

[3.5.1 客户端准入 21](#_bookmark33)

[3.5.2 客户端应用封堵 21](#_bookmark34)

[3.5.3 移动终端管理与监控 22](#_bookmark35)

[3.6 实时监控 22](#_bookmark36)

[3.7 共享接入监控 24](#_bookmark37)

[3.8 报警管理中心 26](#_bookmark38)

[3.9 查询统计与报表分析 26](#_bookmark39)

[3.9.1 详细的日志查询 26](#_bookmark40)

[3.9.2 丰富的统计报告 28](#_bookmark41)

[3.10 日志管理 35](#_bookmark42)

[3.10.1 完整的日志记录与导出备份 35](#_bookmark43)

[3.10.2 日志中心 35](#_bookmark44)

[3.11 集中管理 SMC 36](#_bookmark45)

[3.12 用户管理 37](#_bookmark46)

[3.12.1 用户身份信息维护管理 37](#_bookmark47)

[3.12.2 用户身份识别与认证 40](#_bookmark48)

[3.13 分级分权管理 42](#_bookmark49)

[3.14 特权 USB-Key 43](#_bookmark50)

[3.15 设备自身安全 44](#_bookmark51)

[3.16 虚拟专用网络（IPSec VPN） 45](#_bookmark52)

[4 特点与优势 47](#_bookmark53)

[4.1 国际领先的中文 URL 过滤系统 47](#_bookmark54)

[4.2 国内最全面的网络应用协议数据库 48](#_bookmark55)

[4.3 精细化的策略管理 49](#_bookmark56)

[4.4 细化的应用带宽管理与流量控制 50](#_bookmark57)

[4.5 高效内容分析引擎 50](#_bookmark58)

[4.6 强大的查询统计与分析报告 51](#_bookmark59)

[4.7 完整的 BYOD 解决方案 51](#_bookmark60)

[4.8 人性化界面设计，易于操作管理 53](#_bookmark61)

[4.9 运行稳定可靠，确保网络畅通 53](#_bookmark62)

[4.10 灵活的部署方式 54](#_bookmark63)

[4.11 独立的日志中心 54](#_bookmark64)

[4.12 分布部署，集中管理 54](#_bookmark65)

[5 产品的部署 55](#_bookmark66)

[5.1 串行接入 55](#_bookmark67)

[5.2 镜像旁路 57](#_bookmark68)

[5.3 集中管理中心 57](#_bookmark69)

[6 产品荣誉 59](#_bookmark70)

# 1 互联网给企业管理带来的挑战

## 1.1 互联网 一把双刃剑

经过十几年的高速发展，互联网应用已经渗透到社会生活的每一个角落，成为人们学习、 工作、生活不可或缺的工具，成为企业高效运营、提高竞争力的基础平台。互联网的开放性、 交互性、延伸性为人们快速获取知识、即时沟通以及跨地域交流提供了极大的便利；与此同 时，互联网的便利性与虚拟性也成为各种不和谐行为滋生的温床，网络恶搞、诽谤中伤、侵 犯隐私、色情泛滥等问题，就像打开了潘多拉盒子，越来越对国家安定、社会和谐、企业效 率、青少年成长等提出了严峻的挑战。

在企业组织里，您是否对以下行为似曾相识，却苦无良策？

 *早晨上班，员工长时间沉溺于新闻浏览而不能尽快地投入工作；*

 *您疑惑地看到员工专注地敲击键盘，希望他在努力工作，而不是沉迷于聊天；*

 *您殚精竭虑制作的企业战略计划，竟然很快静静地摆在竞争对手的桌面；*

 *公司已经在所有电脑安装了防病毒软件，可内网病毒依然泛滥，愈杀愈多；*

 *您耗巨资购买的网络带宽，很快被非业务下载占满，核心业务却慢得无法忍受；*

 *有过激的言论从您的企业网络发出，可是无法知道是何人所为，何时所为；*

 *公司关于互联网访问的规章制度醒目地贴在墙上，却鲜有关注；*

 *内网用户在工作 PC 上安装非法软件，却不能及时安装系统补丁和有效的杀毒软件；*

 *…*

传统的网络安全设备，如防火墙、入侵检测系统、防病毒软件、反垃圾邮件系统等，构 成企业网络的边界防护屏障，能够有效地防护来自互联网的攻击，然而它们对于内部员工上 网行为不当引起的安全与管理隐患却无能为力，表现在：

 **安全事件频频发生** 四通八达的网络，方便的不仅仅是正常业务的传输，恶意代码、病毒、蠕虫、间谍软件

等等，也会搭乘“善良”的网页、Email、聊天工具、下载工具便车，悄悄侵入到网络的各 个角落。防火墙无法有效过滤应用层的内容，不能阻挡这些网页的下载，而防病毒工具由于 滞后效应，对于新的病毒以及恶意软件常常无能为力。由于员工不安全的互联网访问而造成 的病毒传播与黑客入侵，已成为网络安全的最大黑洞。

 **工作效率低下** 为了在日益激烈的竞争中获得优势，企业必须不断开发新产品，改善服务质量，提高工

作效率，降低运营成本，但未加管理的互联网应用可能会大大降低员工的工作效率。据一项 调查显示，普通企业员工每天的互联网访问活动中 40％与工作无关，在线聊天、浏览新闻 娱乐、网络视频、网络游戏、炒股、博客等无时无刻不在占用正常的工作时间。在高度网络 化的现代办公环境里，办公室可能成为“舒适的网吧”，人力资源在无形中浪费巨大。

 **敏感信息泄露**

电子邮件、QQ 以及 BBS 论坛等网络应用，已经成为提高工作效率的工具，但如果不 加监管，也可能成为泄密的工具。对于政府机关、上市公司以及知识敏感型企业，关键设计 文档、软件源代码、市场销售计划等核心机密文档，可以通过电子邮件与在线聊天工具“轻 易而快速”地传递到外部，给组织造成重大损失。

 **带宽资源浪费** 据一项统计，在互联网活动未加管理的企业中，宝贵的带宽资源超过 70％被文件、视

频下载等占用，尽管带宽一扩再扩，却总是很快又拥挤不堪。这不仅造成带宽资源大量浪费， 还使得企业正常业务得不到应有的带宽保证。由于缺乏有效的识别与控制手段，网络管理员 往往不能及时地定位并管理下载源。

 **导致法律风险** 互联网充斥着各种良莠不齐的信息，企业员工在获取有用信息的同时，也易被不良内容

侵蚀。为了加强对互联网的控制和管理，国务院、人大常委会、公安部、信息产业部皆相继 出台法律法规明文规定，接入互联网的单位和企业要采用相应的技术手段对互联网的使用进 行控制和管理。对于互联网资源的非法访问，比如访问色情、赌博、犯罪网站、发表反动言 论、泄露重大机密等，都会触犯相关法律，给企业带来法律风险。

## 1.2 对员工上网行为进行规范管理势在必行

员工的不当网络行为引发的问题无法通过传统的网络安全防护手段实现，必须通过专业 的上网行为管理产品解决。何为上网行为管理？简而言之，就是对员工主体的基于内容的网 络访问行为进行管理，包含如下几个要素：

第一、上网的人是谁（Who：哪个部门哪个员工）； 第二、上网的时间（When：工作日/周末，上班时间/午间休息/夜间，上午/下午）； 第三、访问了哪些网络资源（Where：浏览网页、下载文件、发送邮件、聊天、游戏等）；

第四、具体内容是什么（What：网页的内容、邮件的内容、聊天的内容）； 第五、占用的带宽和流量是多大（How much）。 上网行为管理产品基于用户、时间、应用、带宽等元素对员工的上网行为进行全面而灵

活的策略设置，把网络风险管理从“被动式响应管理”提升为“主动式预警管理”，从“防 范管理”提升为“控制管理”，把网络的“通信安全”提升为“应用安全”。为了实现真正安 全的网络环境，企业需要“内外兼修”，除了阻挡外部攻击外，还应该转换视角，大力加强 对内的管理，对员工的上网行为进行规范管理。

## 1.3 360 上网行为管理系统 帮您用好双刃剑

对于网络的滥用，封堵还是放任？这是摆在企业管理者面前的一道难题。武断封堵，无 疑是因噎废食。360 上网行为管理产品，提供灵活地策略管理，根据企业的个性需求量身定 制，帮助企业“上好网，用好网”，实现企业安全、文明、健康、高效的网络环境。

360 上网行为管理系统是 360 企业安全集团推出的一款专业的上网行为管理产品，是面 向企业用户的软硬件一体化的控制管理网关。它提供强大的网页过滤功能，屏蔽员工对非法 网站的访问；提供基于时间、用户、应用的精细管理控制策略，控制员工在上班时间玩网络 游戏、炒股、观看在线视频，以及无节制地网络聊天，从而保障工作效率；提供对通过电子 邮件、即时通讯、论坛发帖等途径的外发信息进行监控审计，避免企业机密信息泄露；此外， 360 上网行为管理系统还提供应用层的带宽管理功能，有效阻止、限制 P2P 等严重消耗带宽 的应用，确保企业的核心业务带宽得以保障。

# 2 产品形态

## 2.1 硬件平台

360 上网行为管理系统采用软硬一体的网络设备产品形态，与具有极高的稳定性与运行 效率，可方便部署于网络机房机架中，并且拥有 3 个系列，覆盖 SOHO 级、企业级、核心 级、电信级等多个级别，全面满足不同用户规模的客户需求。

 **低端系列：**建议用户数为 100-2000 人，适合中小型企业、分支机构、中小学校以及网 吧、咖啡厅等公共网络服务场所。

 **中端系列：**建议用户数为 3000-8000 人，适合中大型企业、政府机关等场所。

 **高端系列：**建议用户数为 8000-200000 人，适合电信运营商、办公园区、高校等场所。

360 上网行为管理系统硬件平台具有下列优势：

 **高运行效率**

360 上网行为管理系统产品全面采用先进的 X86 64bit 架构，配合 Intel 高性能处理器与 芯片组，可处理从 100Mbps 至 40Gbps 的数据吞吐，并且在全应用层功能开启时依然保持极 高的处理能力与运行效率。

##### 硬件 ByPass 功能

硬件设计方面，360 上网行为管理系统具有国际先进的硬件 ByPass 功能，能够在设备 宕机、关机时，使每对网络接口自动保持连同，从而使设备的网络连通性无需受到影响。此 外，360 上网行为管理系统 ByPass 功能支持主动开启，管理员可通过设备上的硬件 ByPass 按钮或系统控制台的操作按钮进行开启或关闭。

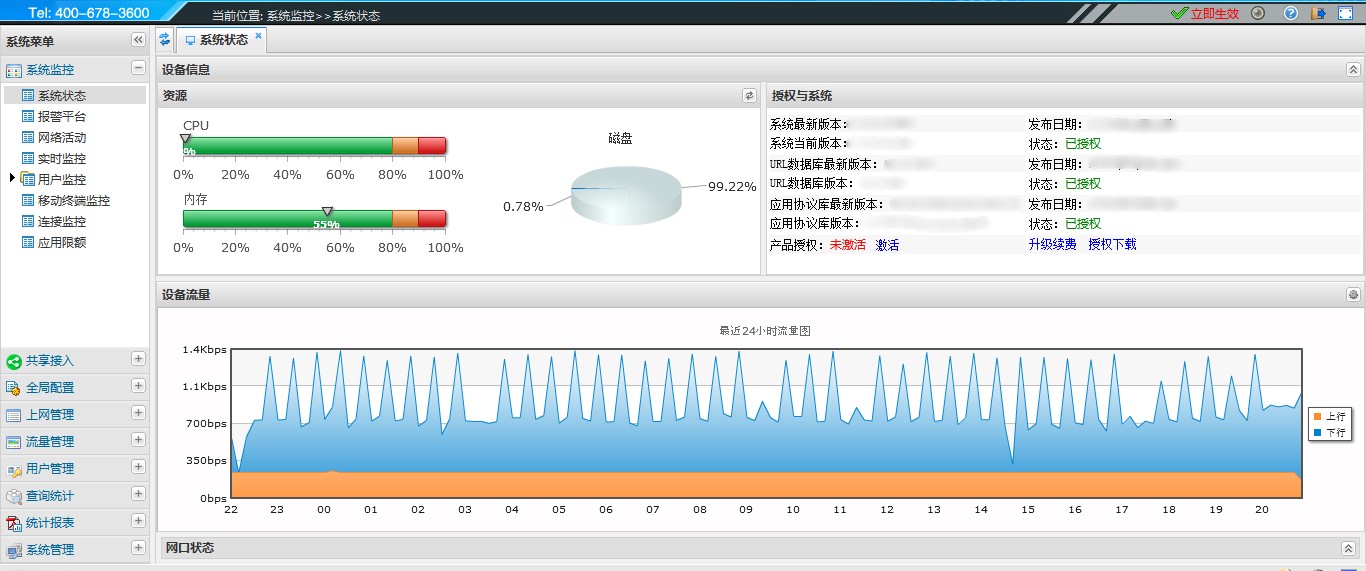
#####  支持扩展网卡插槽

360 上网行为管理系统的多个型号都同时支持电信号网络接口（电口）与光信号网络接 口（光口），以满足客户不同接口需求。同时，360 上网行为管理系统在某些型号中可支持 扩展网卡插槽，用户可根据自己实际需求更换网卡。

## 2.2 软件系统

360 上网行为管理系统软件系统采用自主研发的高性能操作系统，并针对上网行为管理 系统的各项功能进行了大量优化，从而在高负荷任务中依然保持着极强的可用性、稳定性与

运行效率。



360 上网行为管理系统软件系统具有下列优势：

#####  高可用性与稳定性

360 上网行为管理系统操作系统由 360 自主研发，采用极具稳定性的 Linux 内核，使操 作系统、底层功能核心、用户界面三者具有高度的耦合性，保证了系统的高可用性与稳定性。 此外，360 上网行为管理系统软件系统对硬件平台也进行了相应的优化，使产品的稳定性可 以与某些路由器、交换机等网络设备相媲美。

 **一键在线升级**

360 上网行为管理系统拥有完备的实时在线升级机制，用户可在授权许可期限内享受方 便的在线升级服务。只需要键入上网行为管理系统升级地址，系统会自动检测当前版本与最 新版本，并可进行一键升级。

 **人性化操作**

360 上网行为管理系统操作模式采用 B/S 架构，用户可在远端利用浏览器登陆 360 上网 行为管理系统管理平台。此外，上网行为管理系统在设计时就极为重视用户体验，在界面设 计上采用了互联网领域先进的用户体验设计思想，例如功能模块的多标签化、审计结果的图 表可视化等。

 **强大的互联网审计控制功能** 下一节重点描述

# 3 功能介绍

## 3.1 网页访问审计与过滤

Web 是互联网上内容最丰富、访问量最大的应用，然而网页内容良莠不齐，充斥许多反 动、暴力、色情以及其它不健康的信息；此外，大量网络应用，如 P2P，IM，网络电视、 游戏等等，也借助 HTTP 协议或者 80 端口，一方面躲避防火墙的封堵，一方面携带病毒、 恶意软件，为内网用户带来安全风险，挤占网络带宽。360 上网行为管理系统通过预分类过 滤技术、URL 自动分类引擎以及灵活的策略设置，对违反国家法律、危害企业安全的内容 进行过滤，避免用户有意无意访问包含非法内容的网页，净化网络，减少病毒进入局域网的 几率，降低企业法律风险，创造文明健康的上网环境。

### 3.1.1 最领先的中文 URL 分类数据库

网页内容浩如烟海，URL 数目数以千万计。传统的网页过滤通过预设的关键字，对网 页内容进行匹配，效率很低，而且误封率居高不下，已经退出应用的主流。另外一种方法是 预先设置需要封堵的 URL 列表，对 URL 进行实时的匹配过滤，这也存在很大的缺陷，由于 URL 数量巨大，依靠手工添加方式不可能实现完整的过滤，而且对 URL 列表的更新管理几 乎不可能。目前国际上最先进的方式是将 URL 按照一定的标准进行预分类，然后由网关设 备对类别进行过滤，既解决了过滤效率的问题，又保证了过滤的完整性与实效性。

360 上网行为管理系统采用 URL 预分类技术，根据中国的文化背景、伦理道德、法律 法规、应用领域、上网习惯等，进行全面采集、多级分类，并生成 URL 分类数据库。360 自主研发的 URL 搜索引擎，7x24 小时进行区域性（主要是中国大陆）URL 抓取，并对抓取 的网页进行相关性的链接分析。通过智能多级分类系统、人工校验审核等多级过滤技术对获 取到的 URL 进行有效性校验和内容分类匹配，导入数据库。目前 360 上网行为管理系统的 URL 数据库包括 150 个类别，超过 4000 万条的 URL，基本覆盖中国大陆区域的网站，是全 球最大的中文 URL 分类数据库。360URL 数据库保持定期更新，具体更新信息见官网产品 升级公告页面。

360URL 库的分类标准是基于行为后果而不是内容关键字，即把 URL 访问对企业生产 力的后果影响作为分类的原则。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **BBS 站点** | **Web 通信** | **在线聊天** | **游戏** | **计算机与互联网** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **违反法律** | **病毒** | **医疗健康** | **广告** | **财经** |
| **成人** | **赌博** | **博彩** | **毒品** | **暴力** |
| **新闻媒体** | **宗教与信仰** | **远程代理** | **房地产** | **求职招聘** |
| **搜索引擎** | **娱乐** | **机动车** | **信息参考** | **旅游** |
| **政治** | **军事** | **法律** | **艺术** | **教育** |
| **网上交易** | **违反道德** | **商业** | **文学** | **体育** |
| **科学** | **色情** | **犯罪技能** | **社会生活** | **门户网站** |
| **儿童** | **非盈利组织** |  |  |  |

图 2-1 360URL 预分类库

URL 自动分类引擎是 360 自主研发的 URL 智能分类技术，它根据增强的贝叶斯算法， 根据网页的文本、图片、框架、颜色、关键字的语义、关键字出现频率以及关键字之间的比 例关系、网页之间的相似度等多个维度，对网页进行智能分析，自动分类，这是 360Web 分 类的核心技术。为了保证 URL 分类的准确性，360 有一支专门的 URL 分类审核团队，负责 对 URL 自动分类结果进行人工校验审核，确保每一条 URL 都符合分类标准。

互联网上每天都有新的网站产生、老的网站消亡或者内容发生变更。为了保证 URL 分 类的实效性，360 的服务器群每时每刻都在对既有的 URL 库进行更新，每天更新的速度超 过 300 万条。这些变化内容可以自动更新到客户的在线设备上，使客户设备与 360URL 库保 持实时同步。

为了提高本地 URL 分类的覆盖度，在打开云模式开关后，对于本地未查询到的 URL 分 类，系统会自动去云端进行查询，并将结果更新到本地的 URL 分类库供下次查询使用。

有时上网行为管理系统的内置分类会出现不符合管理要求的情况。为便于管理员配置基 于 URL 分类的控制策略，该版本为系统管理员增加了查询 URL 分类的功能，并且对于 URL 分类错误的情况，为终端用户和系统管理员提供了主动反馈错误分类给 360 的功能。

### 3.1.2 灵活的 Web 策略设置

#####  360 上网行为管理系统支持灵活的策略设置，可以针对多种条件设置策略

 用户、部门及其组合

 时间段，如上班时间、下班时间、周末等

 网站类别

* URL 关键字

 网页标题关键字

 网页内容关键字

 下载文件类型 过滤方式包括：

 允许 / 阻塞

 记录行为 /记录快照

 报警 策略设置方法如下图所示：

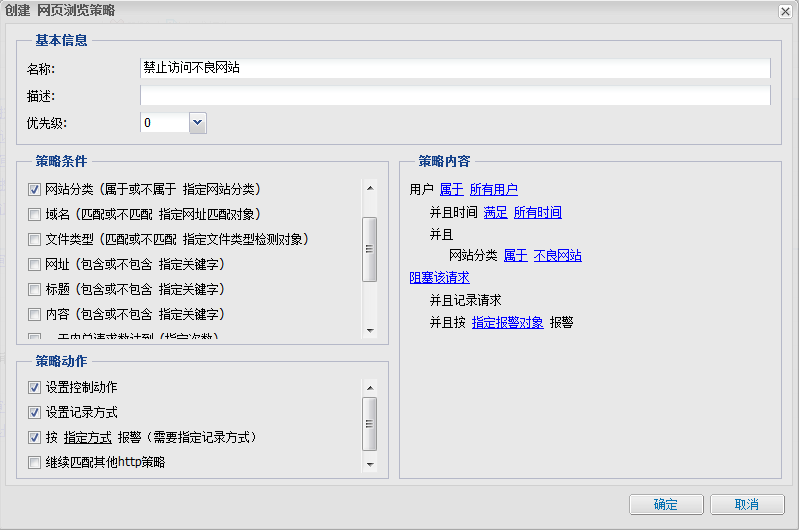


图 2-2 URL 过滤策略设置

#####  自定义 URL 类别

如果上网行为管理系统 内置 URL 类别不能完全满足用户的实际需求，用户可以根据企 业的需要自定义新的类别，以实现更精确的控制管理。



图 2-3 自定义 URL 分类

#####  URL 黑白名单

通过 URL 黑白名单，可以设置 Web 访问中的特例：对于一些网站可能需要跳过已定义 好的策略，而无条件地允许或阻塞，比如 Windows 自动更新服务，病毒库自动更新服务。 被直接允许访问的网站列表称为 URL 白名单；相反地，被直接阻塞访问的网站列表称为 URL 黑名单。黑名单、白名单和策略的优先级从高到低为黑名单 -> 白名单 -> 策略。

### 3.1.3 Web 访问违禁提示

用户访问 Web 失败后，通常在浏览器中显示“无法显示页面”的提示信息。如果是由 于被预设策略所阻塞，360 上网行为管理系统提供更友好的方式提示用户无法访问的原因， 如下图所示，提示内容可以自定义。

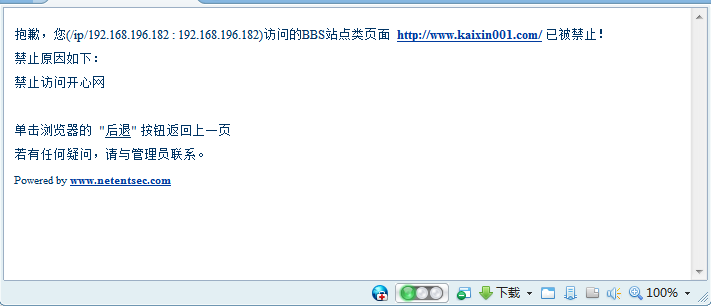


图 2-4 Web 访问违禁提示

## 3.2 应用控制

随着技术的迅猛发展，各种互联网应用层出不穷，如即时通讯（IM）、网络游戏、在线 炒股以及在线音乐视频等等。未加管理的使用，不可避免地影响员工的工作效率。在一项调 查中，超过 80%的员工在上班时间做过与工作无关的工作，其中，有 60%的被调查员工承 认其主要是在玩网络游戏、用 QQ 等即时通讯软件聊天，以及炒股等等。这些不当网络活动 大大降低了员工的工作效率，造成了企业人力资源的严重浪费。

### 3.2.1 基于特征识别的覆盖全面的应用协议数据库

欲控制各种网络应用，必先准确识别。传统安全产品通过 IP 或者端口封堵各种协议， 只能局限于标准的协议，如 HTTP，SMTP，且主要是在网络层以及传输层进行，对应用层 的内容无能为力，而且，如果 IP 与端口经过动态协商建立，比如 QQ，P2P 下载等，则完全 不能胜任。360 上网行为管理系统对应用的识别是通过应用特征与行为特征实现的。所谓应 用特征，是指在成序列的数据包的应用层信息中，存在有规律的字节特征，它可以唯一地标 识某种应用协议，就如同一个人无论穿什么颜色的衣服，其指纹特征不会改变，而且是唯一 的。类似地，上网行为管理系统可以通过特征值准确地识别网络应用；而行为特征，是指连 续多个包或者多个并发的网络连接表现出来的某种行为模式具有一定规律性，通过这些行为 模式可以识别特征值不明显的应用类型。

360 上网行为管理系统拥有国内最全面的网络应用协议数据库，分为 30 余个大类，共

4000 多种协议，主要包括如下大类：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **传统网络协议** | **VoIP** | **远程管理** | **网络游戏** | **通讯聊天** |
| P2P 下载 | 股票软件 | 在线视频 | 文件共享 | Http 应用 |
| 代理和隧道 | 木马软件 | 安全软件 | 网络管理 | 期货软件 |
| 移动应用 | 标准协议 | 软件更新 | 网上银行 | 网页应用 |
| 论坛发帖 | 其他 | 云笔记 | 网络会议 | 文库类 |
| 社交网络 | 办公 OA | P2P 影音 | 网盘 | 电子邮件 |
| 数据库 | 在线音乐 | 知名网站 | 在线购物 | 网络机顶盒 |
| 系统工具 | CRM | 地图导航 | 用户自定义 |  |

应用协议库定期更新，具体更新信息见官网产品升级公告页面

### 3.2.2 支持用户各项应用限额管理

 **应用时长限额**

360 上网行为管理系统可限定每个用户在一天之内累计上网时间额度，管理员可单独控 制用户的某项互联网应用每日上网时长限额，也可同时控制用户的多项互联网应用每日上网 时长限额。超出限制时间额度后，用户在当日内无法再使用该应用。

如：可限定用户每日仅允许 QQ 聊天累计时长 1 小时；也可限定用户每日仅允许炒股 30 分钟，即无论用户用哪种炒股软件，累计达到 30 分钟后，当天内无法再使用任何炒股软 件炒股。

 **应用流量限额**

360 上网行为管理系统可限定每个用户一天之内累计流量额度，管理员可以单独控制用 户的某项互联网应用每日流量限额，也可以控制用户的多项互联网一个月每日流量限额，流 量超出限制额度后，用户在当日内无法再使用该应用。

### 3.2.3 灵活精细的管控策略

 **灵活的策略设置**

360 上网行为管理系统能够根据多种条件及其组合对网络应用进行灵活的管理，包括：

 用户、部门及其组合

 时间段，如上班时间、下班时间、周末等

 提供自定义协议，对特定的应用进行控制

 对网络应用进行封堵、允许、以及流量控制管理

#####  精细化的控制管理

360 上网行为管理系统的一大优势是能够对各种网络应用进行精细粒度的管理控制，比 如可以通过阻塞每一种具体的网络电视、流媒体来减少带宽资源浪费，保障员工工作的效率 等。此外，对于一些多协议多用途的应用（如 IM），上网行为管理系统可以精确识别子协议， 将更多细节纳入策略框架中。例如：允许通过 QQ 聊天与文件传输进行产品技术支持，且保 障 QQ 远程协助的带宽，但禁止玩 QQ 游戏，禁止欣赏音乐视频等等，如下图所示：

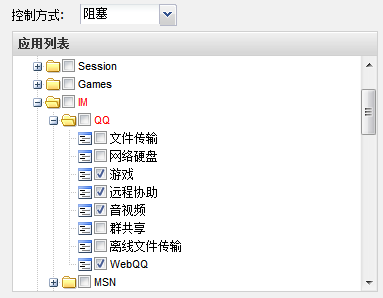
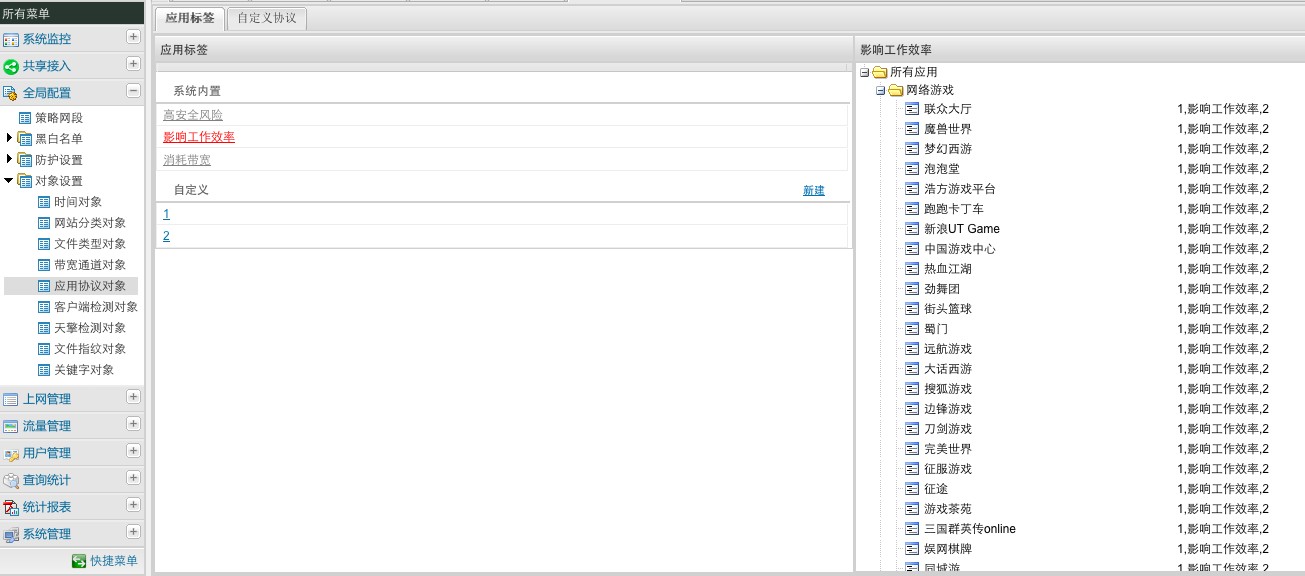


图 2-5 IM 子应用独立控制

 **精细化的控制管理** 支持配置应用标签并在应用控制、流量控制等策略中选择标签进行策略管理。默认提供

3 类应用标签，不可修改和删除。管理员可以自定义应用标签。



## 3.3 带宽管理

网络应用层出不穷，对带宽资源的占用也越来越高，特别是以 P2P 为代表的下载软件， 如果不加限制，会严重消耗企业的带宽资源，从而影响正常的业务数据的传输。360 上网行 为管理系统支持应用层的带宽分配与流量管理，可以针对用户或部门、按照时间段，对每一 种应用协议进行带宽限制。

360 上网行为管理系统像一台网络协议分析仪，能够识别并统计网络上有哪些类型的数 据在传输，哪些应用在运行，哪些协议在使用，哪些服务器的流量占用了主要的带宽资源， 哪个用户的上网行为显著消耗了带宽等。根据这些量化的统计数据，通过预先设定若干个虚 拟的带宽通道，将带宽通道与具体的用户或网络应用绑定，从而对其流量进行限制、整形， 达到带宽管理的目的。

### 3.3.1 识别控制 P2P 软件和加密 P2P 数据

BT、迅雷、电驴等 P2P 软件是造成带宽消耗最重要的因素，因此对 P2P 的封堵与限制 成为带宽管理最重要的手段。360 上网行为管理系统能够识别中国网民常用的 P2P 软件，进 行有效的封堵或者流量控制。除了控制传统的 P2P 软件，上网行为管理系统还能对多个变 种以及加密的 P2P 数据流进行完美的识别控制。

### 3.3.2 针对用户/应用设置带宽

上网行为管理系统可对用户、应用以及它们的组合设置带宽。首先根据需要定义多个带 宽通道，对于每个通道，可以指定其保障上下行速率、突发上下行速率、优先级等参数对数 据流近进行整形，可以选择将通道内流量对策略用户平均分配，见下图。



图 2-6 带宽对象设置

其中：

上传/下载速率：数据流的保障吞吐量。低于此临界值的数据流保障通过。 最大速率：数据流的峰值带宽。超过此临界值的数据流被抑制并丢弃。峰值带宽一

般设置为大于正常上传/下载的数值，意义在于：如果当前连接超过基本保障带宽，且 总体网络带宽有闲置未用部分，当前连接可以在峰值带宽之下暂时“借用”其它通道空 闲的资源，以提高总带宽利用率。 如果对一组用户设置了总带宽，为了防止组内个别成员独占带宽，可以通过勾选“平均

分配”将通道平均分配给每个策略用户，也可以针对组内每个成员设置平均带宽上限，实现 组内带宽资源的公平使用。

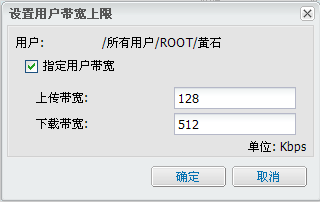


图 2-7 用户平均带宽设置

### 3.3.3 基于时间段流量控制

360 上网行为管理系统支持自定义时间对象，实现针对时间段进行带宽分配。时间对象 可以选择一周内的一天或多天，一天内可以灵活设置多个时间段。如下图所示：

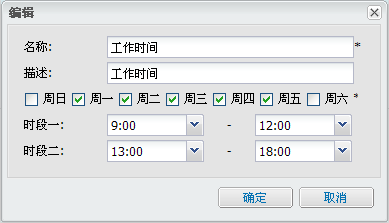


图 2-8 时间对象设置

## 3.4 内容审计和过滤

通过互联网传递信息已经成为企业的关键应用，然而信息的机密性、健康性、政治性等 问题也随之而来。通过 360 上网行为管理系统，您可以制定精细化的信息收发监控策略，有 效控制信息的传播范围，控制敏感信息的泄露，避免可能引起的法律风险。

### 3.4.1 邮件收发审计和过滤

360 上网行为管理系统不但可以审计通过任意端口的 IMAP、POP3 和 SMTP 协议收发

邮件内容，同时还可以审计通过 WEB-MAIL 发送邮件的内容，实现对用户邮件收发内容的 全面审计。

同时，360 上网行为管理系统可基于邮件特征对邮件外发内容进行审计和过滤，并能够 匹配收发邮件的标题及内容关键字等特征进行邮件报警，从根本上杜绝包含敏感信息邮件的 外发行为，保证企业信息的安全。

另外，360 上网行为管理系统支持对外发邮件的人工审核，将那些包含敏感信息的邮件 暂时拦截下来，缓存在上网行为管理系统本地，由审计员审核内容后在决定是否允许外发， 确保精准过滤。

 **邮件审计内容**

邮件收发时间

用户名称

发送邮箱地址

接收邮箱地址

收发类型

邮件主题

邮件正文

邮件附件名称及内容

 **过滤条件**

发信人地址

收信人地址

用户工具

用户位置

邮件主题关键字

邮件正文关键字

邮件附件名称、大小、类型及正文关键字

##### WEB-MAIL 站点

雅虎邮箱、搜狐邮箱、网易 163、网易 126、Msn Hotmail、Tom 邮箱、新浪邮箱、

G-Mail、QQ-Mail、Excite、Goo、Infoseek、Livedoor、21CN、139 邮箱等。 除上述免费邮箱外，360 上网行为管理系统还支持企业私有邮箱 webmail 外发邮件

的审计和过滤。

### 3.4.2 IM 审计和过滤

360 上网行为管理系统对 IM 行为及内容审计功能包括：

* **QQ 审计** 审计收发动作、发送账号（昵称）、接收账号（昵称）、聊天内容、语音聊天行为、 群组聊天内容、离线文件收发

 **飞信审计** 审计收发动作、发送账号、接收账号、聊天内容、音视频行为、文件传输行为 基于账号和聊天内容关键字、文件名称、文件类型过滤聊天行为和文件传输行为 对违反预定义规范的飞信聊天行为进行报警

* **Skype 审计** 审计收发动作、发送账号、接收账号、聊天内容、文件传输名称、文件内容、语音 聊天行为
* **Baidu HI 审计** 审计收发动作、收发账号、聊天内容

##### WebIM

支持 WebQQ，SmartQQ，Sina UC，网页版旺旺、微信网页版等常见 WebIM，支持 如登录、退出、收发消息等行为，并可根据登录账号、聊天内容等进行访问控制。

### 3.4.3 论坛发帖审计和过滤

360 上网行为管理系统能够针对各类 BBS 论坛、新闻评论、搜索引擎贴吧、博客、微 博的发帖内容进行监控审计，包括发帖账号、标题、正文、附件，对于违背预设关键字的发 帖进行实时阻断并报警。对于发帖日志，还可以通过时间、用户、关键字进行全面查询，准 确定位发帖行为与内容。此外，上网行为管理系统还支持对论坛投票行为及内容的审计，增 强了发帖审计的多样性。

### 3.4.4 搜索引擎关键字审计和过滤

360 上网行为管理系统支持“搜索引擎关键字审计与过滤”功能。可以记录用户通过搜 索引擎站点、门户网站、论坛贴吧、购物网站、视频网站等搜索的关键字内容，并可以基于 搜索类别、关键字内容过滤用户的非法搜索行为。

### 3.4.5 HTTP 文件传输审计和过滤

360 上网行为管理系统支持 HTTP 文件传输内容的审计和过滤功能。可以基于文件名称、 类型和大小审计 HTTP 文件上传下载内容，并可阻塞包含指定特征的文件传输行为。

### 3.4.6 HTTPS 加密网页的审计和过滤

360 上网行为管理系统可审计 HTTPS 加密网页的访问情况，并可基于网站分类、证书 合法性阻塞存在安全隐患 HTTPS 加密网页的访问，有效屏蔽用户对钓鱼网站的访问，保障 企业网络安全和用户信息安全。

### 3.4.7 FTP 文件传输审计和过滤

360 上网行为管理系统支持 FTP 审计和过滤功能，可以审计任意端口的 FTP 文件传输 行为；可基于所传输文件在 FTP 服务器中的路径、文件名称阻塞文件传输行为；并可还原 指定名称、大小或类型的文件内容。

### 3.4.8 TELNET 内容审计

360 上网行为管理系统支持 TELNET 审计功能，可审计内网用户的 TELENT 行为，记 录 TELNET 目标设备的 IP、端口信息；记录执行的指令内容和结果。

### 3.4.9 SSL 内容审计

360 上网行为管理系统支持 SSL 相关域名的内容审计功能，可审计以 SSL 加密方式接 入的网络活动，如网页浏览、论坛发帖、webmail 审计等。

### 3.4.10数据库审计

数据库是企业信息中心的核心，虽然主流数据库产品本身具有安全机制保证其安全性， 但对于通过盗取数据库管理员账户密码并窃取甚至破坏数据的非法行为，数据库产品本身的 安全机制存在天然瓶颈。

360 上网行为管理系统支持数据库访问操作的审计与控制，包括 Oracle、PostgreSQL、 MySQL、SQLServer 等，以保障客户数据库的安全。用户可通过配置控制方式、数据库类型、 关键字等，实现对用户数据库客户端使用的控制，如只允许特定用户远程登录或操作 Oracle

数据库并留下访问审计记录等，从而实现针对盗取账户密码等非法行为的安全性升级。

## 3.5 终端控制与准入

终端设备是网络安全的主体，不良软件的使用、防护系统缺失都可能带来终端安全隐患， 进而影响内网安全。360 上网行为管理系统设备能够通过统一下发的客户端软件，结合统一 的策略配置，检测终端系统的进程、文件、注册表、操作系统及补丁、杀毒软件及病毒库等 信息，制定准入规则。

### 3.5.1 客户端准入

 **系统进程检测**

系统内置了包括 CCProxy、Sygate 在内的五种常用的代理工具进程检测对象，同时可以 由管理者手动添加需要检测的进程对象。检测项目包括进程名、窗口名、特征文件名、服务 名等。通过策略配置控制开启了相关进程的终端能否访问网络。

 **硬盘文件检测**

360 上网行为管理系统能够通过客户端软件检测终端文件系统的内容，结合策略控制某 个包含了指定文件的终端设备能否访问网络。可以采用文件全路径结合 MD5 的方式核对文 件，确保检测结果的正确可靠。

 **注册表检测** 检测终端系统注册表项及键值，根据准入规则允许或阻止终端访问网络。

 **操作系统检测** 检测终端操作系统版本及 SP 补丁包版本。

 **杀毒软件检测** 检测终端设备安装的杀毒软件及病毒库版本，包括系统预置的杀毒软件检测对象以

及用户可自定义的检测对象。

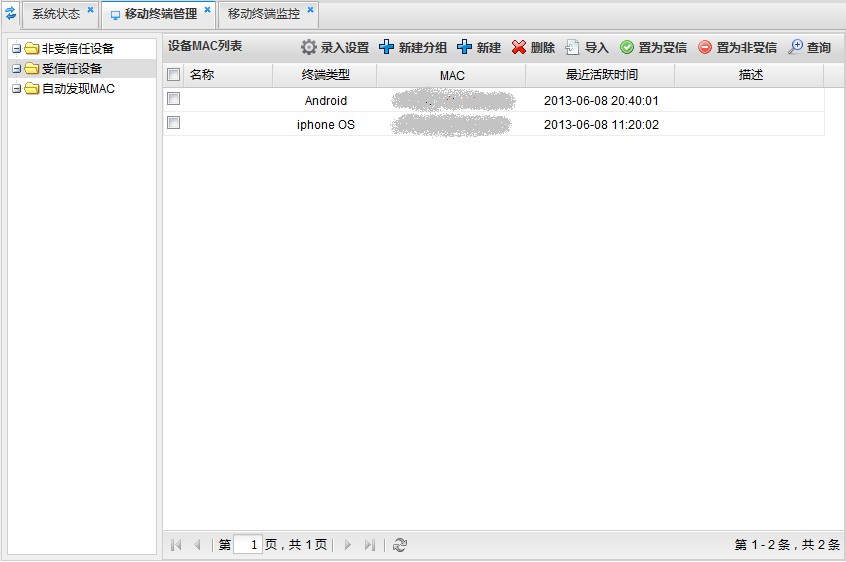
### 3.5.2 客户端应用封堵

360 上网行为管理系统能够通过客户端软件检测系统应用进程，并依据用户制定的策略 进行封堵。检测对象包括设备预置的对象和用户自定义的对象，可根据进程名、窗口名、特 征文件名、服务名等内容添加检测对象。

### 3.5.3 移动终端管理与监控

无论企业内部或是诸如咖啡厅、机场等公共区域，通过 WiFi 接入网络正在变得越来越 普遍。360 上网行为管理系统针对移动设备的管控进行大幅度的优化，可以实现对 iOS、 Android、Windows Phone 等移动设备的精确识别，并可对识别出的设备进行准入、封堵等 操作。

360 上网行为管理系统可将发现的设备自动列入“自动 MAC”组，并可将组内的设备通 过“设为受信”及“设为非授信”功能将设备列入允许准入类别及阻止准入类别。同时，上网行 为管理系统支持新建分组，其类别可以为“受信”或“非受信”。



## 3.6 实时监控

360 上网行为管理系统支持管理员实时地监控设备运行健康状况与当前网络活动，可在 第一时间内对网络异常进行定位分析。

#####  丰富全面的监控信息

 系统资源健康状况，如 CPU、内存、硬盘等使用信息；

 当前在线用户列表，包括全部合法用户以及活跃用户；

 当前网络实时流量以及最近 24 小时网络流量变化情况；

 本日应用流量排名、用户流量排名、网站点击量排名；

 预定义带宽通道资源使用情况； 下图显示了当前用户流量情况：

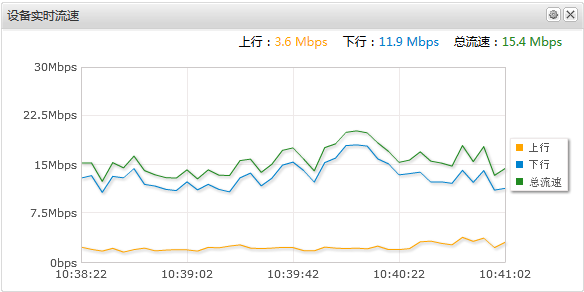


图 2-9 设备流速图

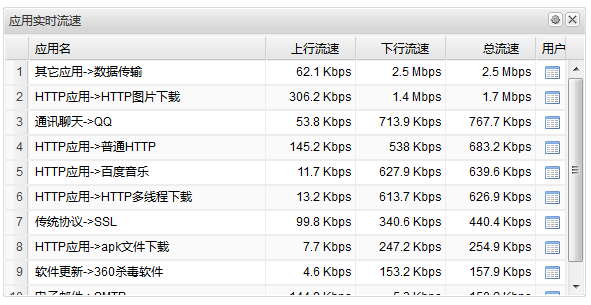


图 2-10 实时流量排名

 **灵活的监控设置**

 选择一个、多个用户或者用户组实时监控；

 选择一个、多个应用实时监控；

 监控特定端口的网络流量；

#####  贴近自然思维习惯的即席分析（Ad-hoc Analysis）

360 上网行为管理系统支持对实时监控信息的即席分析，通过对用户、应用、时间、流 量的关联分析，可以迅速了解网络流量的分布，定位问题发生的原因。比如，当发生网络拥 塞时，管理员可以查看当前应用流量的排名，对于流量最大的应用，如 BT，可以点击查看 有哪些人正在进行 BT 下载；也可以首先查看流量的用户排名，对于流量最大的用户，只需 轻点鼠标，即可清晰获知他正在访问哪些网络应用。

准确定位引起网络带宽拥塞的用户、应用以及异常流量后，管理员可以设置、调整应用 访问的策略以及带宽管理规则，抑制非关键流量，保障企业核心业务的畅通传输。此外，对 于有异常行为的用户/主机，还可以强制下线，或者放入黑名单中。

## 3.7 共享接入监控

共享接入是指使用 NAT 等 IP 映射技术将一个网络出口共享到多个主机。例如使用无线 路由器将一条宽带网络共享给多个 PC、智能手机或平板电脑连入 Internet。

360 上网行为管理系统共享接入模块能够对接入网络的设备做观察、控制，能够检测到 一个用户或 IP 所共享的终端数量，并可以对数量做策略控制，以达到掌控用户终端数量的 目的。

其主要实现下面具体的功能需求：

◇ 主机个数的识别；

◇ 对识别后的主机进行进一步的行为控制；

◇ 对私接情况进行进一步的统计和分析。 共享接入最核心的功能就是能够识别出一个用户所使用的终端个数，不论这个用户采用

的是分时分段上网，还是采用 NAT 路由或是代理同时上网的情形。

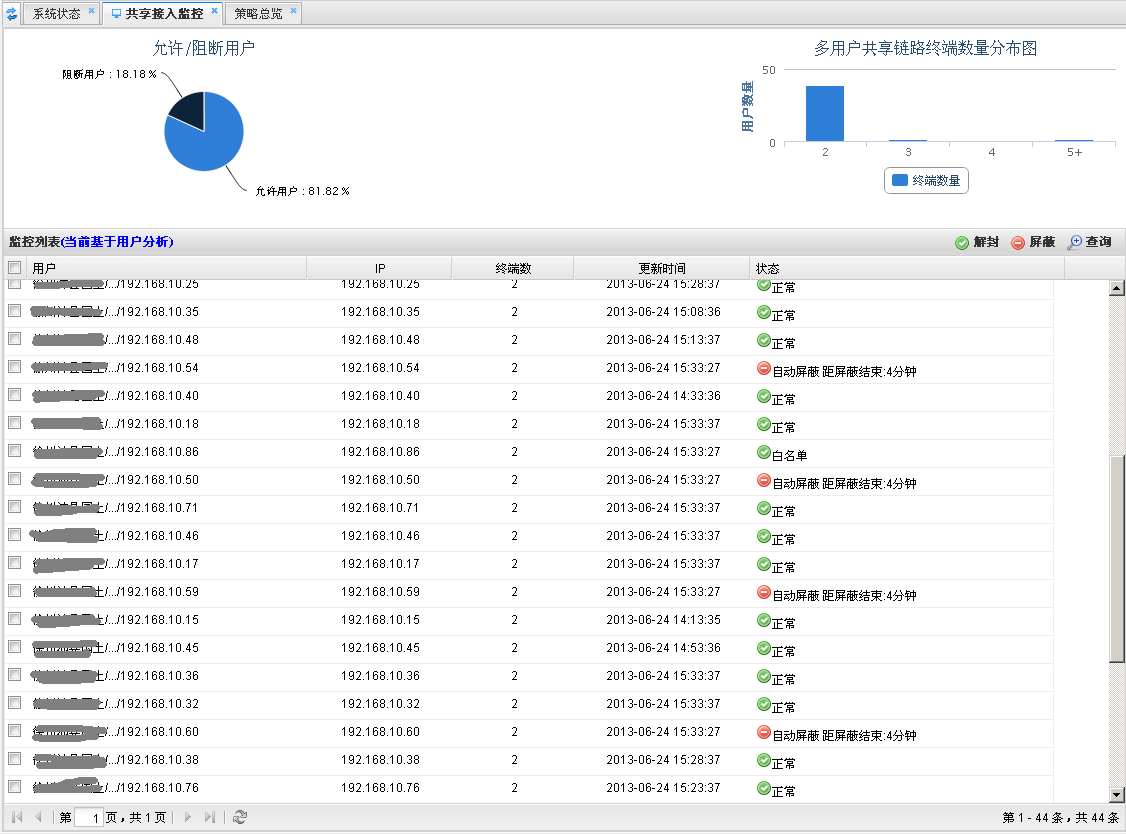


图 2-11 共享接入监控列表 在监控到用户使用的终端数后，可以对此进行控制，屏蔽该用户的上网流量，解除屏蔽，

永久屏蔽，管理员手工解除等用户控制的功能，并可对用户建立黑白名单，从而进行个性化 控制。

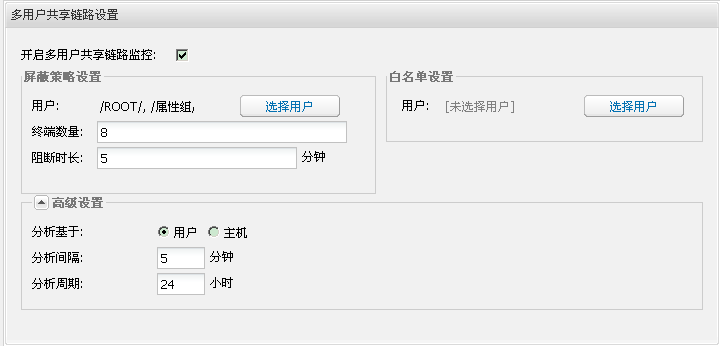


图 2-12 共享接入设置 私接状况查询也能够对历史情况做统计，能够查询到用户在过去一段时间的私接状态变

化，以便用户进行历史的回溯。



图 2-13 共享接入日志

## 3.8 报警管理中心

360 上网行为管理系统报警管理中心可对系统异常、网络异常、用户互联网违规行为， 以及外发内容不合规行为进行统一报警管理，并对不同级别的报警事件以声音、指示灯、邮 件等不同的方式进行报警，便于管理员第一时间知悉事件并采取措施，降低互联网管理的风 险和隐患。

## 3.9 查询统计与报表分析

对用户网络行为进行记录与分析，是上网行为管理产品必备的重要功能。对日志的存留 与分析，既是对国家法律法规的遵从，也是真正管理好企业员工上网、有效利用网络资源的 需要。针对用户上网行为以及相关内容查询统计，能够对用户的网络活动进行较长时间的回 溯与反查，帮助管理员全面了解网络的使用情况，为改进网络管理提供详实准确的依据。

### 3.9.1 详细的日志查询

#### 3.9.1.1 用户上网日志查询

信息查询的目的是对过去某时间段内选定用户的网络行为进行细节的查看，它反映了在 此时间段内用户的网络流水记录。

 **完整的查询内容**

 基于用户的综合上网行为查询

 网络流量查询，数据粒度可选，如：按汇总数据，小时流量，细节流量

 Web 访问记录查询，数据粒度可选，如：全链接，仅主链接；控制粒度可选，如允 许、阻塞

 应用行为阻塞日志信息查询，便于对违规互联网行为进行取证

 应用连接明细查询，便于追踪定位网络安全事件故障源

 用户上网时长查询，可基于时间段、用户、应用协议等多种条件进行查询分析

 电子邮件收发记录查询，可查看完整的邮件正文与附件内容

 IM 聊天内容查询，查看 QQ、Skype、飞信、WebIM 的聊天记录，同时，可方便追 踪某两个 IM 用户之间所有聊天过程信息

 论坛发帖内容查询，可查看完整的发帖正文与上传文件

 P2P、网游、炒股、视频等网络应用行为查询

 查询用户或用户组当前所适用的策略，便于排除或定位网络故障源

 用户认证上线历史查询，建立时间、用户、IP 间的对应关系

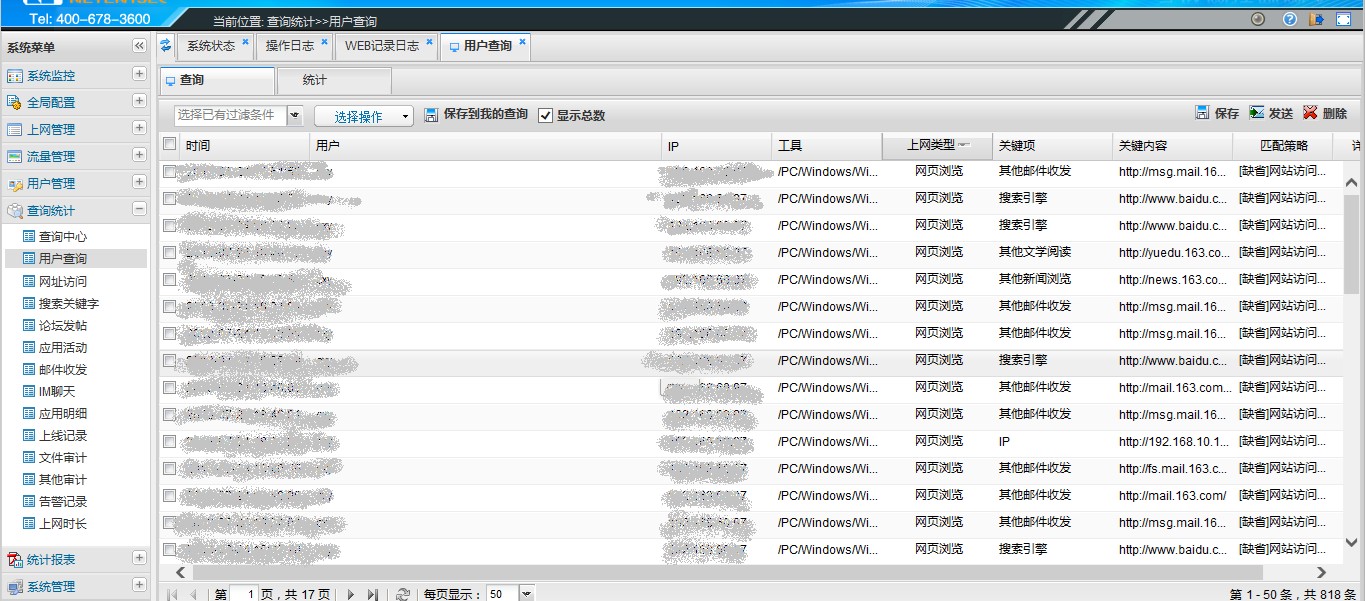


图 2-14 用户上网日志查询

#####  灵活的查询条件设置

根据日期范围，以及每天的特定时间段查询

根据用户或者用户组查询

根据网络应用查询流量

根据网站类别、URL 关键字、标题关键字、网页内容关键字、预设的过滤策略 查询 Web 访问记录

根据发件人、收件人、主题、附件名、邮件大小、email 类型、邮件主题及内容 的关键字查询发送与接收邮件

根据发送帐号、接收帐号、IM 类型、聊天内容关键字查询在线聊天记录

设置 URL 关键字与正文关键字查询论坛发帖记录

 **查询结果保存**

直接导出为 Excel 表格，方便二次处理

#### 3.9.1.2 系统报警日志查询

故障自检和报警机制是保障设备自身安全性和网络稳定性的必要条件。只有及时发现问 题、方便准确的定位问题根源，才能有效的解决问题并避免更大的网络安全故障发生。360 上网行为管理系统不但具备完善的设备自检机制，还对设备报警日志进行分级管理，便于网 络管理者快速准确获取重要报警信息。

#### 3.9.1.3 系统操作日志查询

操作日志是否完整、准确、易读是衡量网络安全产品专业化和成熟度的重要指标。360 上网行为管理系统可以完整记录用户及系统的所有操作管理日志，并以全中文的简明记录形 式展现在管理界面中，为网络管理者的 Troubleshooting 过程提供有效依据。

### 3.9.2 丰富的统计报告

360 上网行为管理系统支持根据时间、用户、应用对上网行为进行全方位的统计，内容 涵盖网络流量、Web 访问、邮件收发、IM 聊天、论坛发帖、P2P 下载等各种网络应用。并 提供多达 50 种预置报告模版，获得不同角度的统计报告。

#### 3.9.2.1 递进式统计分析

面对纷繁复杂的数据，人们习惯从宏观到微观、从全局到局部逐步地认知、理解，分析 的层次由浅入深，分析粒度由粗到细。事实上，多数抽象事务的分类与分层普遍遵循这一规 律，如日期以年、月、日表示，行政区按照国家、省、市、县进行组织，人们的思维习惯实 际上是这种客观存在的主观映射。

360 上网行为管理系统采用递进（drill-down）的方式，把统计数据层次分明地展现给用 户，帮助管理员快速在全局与细节上把握网络活动的状况。比如：为了了解一周内企业员工 访问 web 的情况，上网行为管理系统引导用户按照如下的操作：URL 总类别数 -> 哪些网 站类别 -> 某类网站所包含的具体网址 -> 某网址有哪些人在什么时间访问，层层递进，把 web 访问的信息清晰地展示出来，如下图所示。此外，除了按照网站类别查看，还可以按照

站点、请求数等进行递进查询分析。

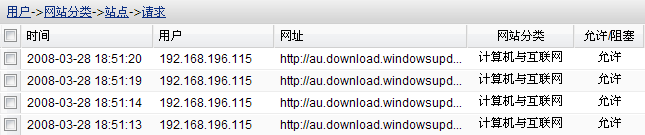
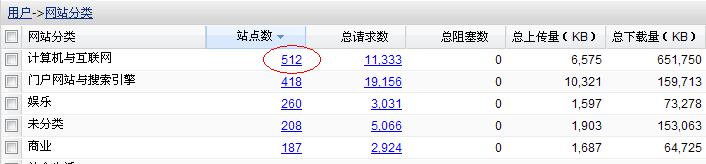


图 2-15 递进统计分析

#### 3.9.2.2 统计排名报告

统计报告是实施上网行为管理设备后进行效果评估的最直观工具，也是了解网络活动以 及调整管理策略的最重要的依据。360 上网行为管理系统提供用户/部门网络活动摘要、用户 行为统计、带宽资源统计、上网时长统计 4 大类 50 多种统计报告，以表格、饼图、柱图、 线图等多种形式展现，方便管理员进行全面的统计分析。

 **用户活动摘要统计报告** 在选定的时间范围内，对于选定的用户：

 用户行为摘要统计报告

− 网站访问量，以及网站请求数 TOP 用户

− 邮件收发量，以及收发量 TOP 用户

− 在线聊天量，以及在线聊天 TOP 用户

− 论坛发帖量，以及发帖量 TOP 用户

− 关键字搜索量，以及关键字搜索量 TOP 用户

− 文件收发量，以及文件收发量 TOP 用户

 网络流量摘要统计报告

− 网络总流量，以及流量 TOP 用户

− 网站访问总流量，以及流量 TOP 用户

− 邮件收发总流量，以及流量 TOP 用户

− 论坛发帖总流量，以及流量 TOP 用户

− 文件收发总流量，以及流量 TOP 用户

#####  用户行为统计报告

 网站访问行为统计报告

− 网站访问量（或阻塞量）随时间走势图

− 网站请求（或阻塞）数最多的用户排名，以及各用户访问量最大的网站

− 被访问次（或阻塞）数最多的网站类别及网站排名，以及各类别网站访问量最 大的用户



图 2-16 网站类别访问量排名饼状图

 邮件收发行为统计报告

− 邮件收发量（或阻塞量）随时间走势图

− 邮件收发量（或阻塞量）最多的用户排名，以及各用户使用的主要邮箱

− 收发量（或阻塞量）最大的邮件域名，以及使用各域名邮箱的主要用户

 在线聊天行为统计报告

− 在线聊天量（或阻塞量）随时间走势图

− 在线聊天量（或阻塞量）最多的用户排名，以及各用户使用的聊天工具

− 使用量最大的聊天工具排名，以及使用各聊天工具的主要用户

− 聊天最多的账号排名，或被阻塞量最大的账号排名

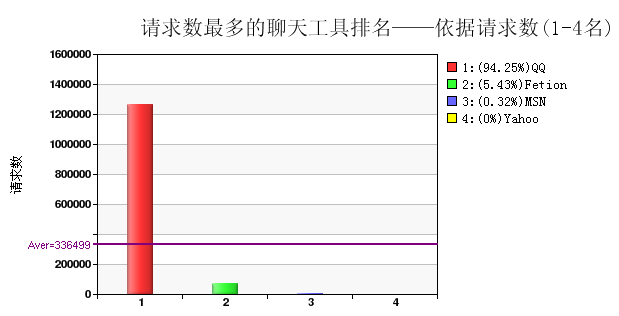


图 2-17 聊天工具使用排名柱状图

 论坛发帖行为统计报告

− 论坛发帖量（或阻塞量）随时间走势图

− 论坛发帖量（或阻塞量）最多的用户排名，以及各用户发帖最多的论坛

 关键字搜索行为统计报告

− 关键字搜索量（或阻塞量）随时间走势图

− 关键字搜索次数（或者阻塞次数）最多的用户排名，以及各用户搜索最多的关 键字

− 被搜索次数（或者阻塞次数）最多的关键字排名，以及各关键字搜索的主要用 户

− 搜索最多的关键字类别排名，以及各类别搜索的主要用户

− 访问量最大的搜索站点排名，以及访问各站点的主要用户

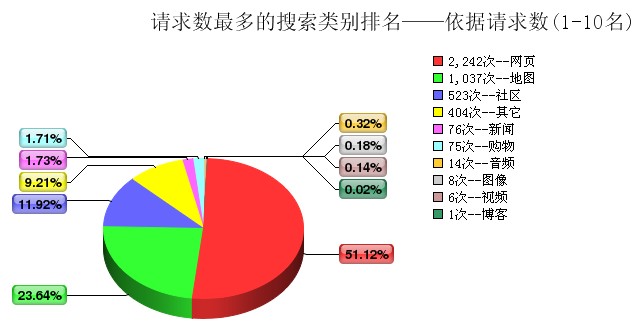


图 2-18 搜索类别排名饼状图

 文件传输行为统计报告

− 文件传输量（或阻塞量）随时间走势图

− 传输文件最多的用户排名

− 使用最大的文件传输工具排名

 **带宽资源统计报告** 在选定的时间范围内，对于选定的部门（用户组）：

− 上网时间最长的用户排名，及个用户的主要网络应用

− 使用时间最长的网络应用排名，及使用各应用的主要用户

− 流量最大的用户排名，及各用户的主要应用分布

− 流量最大的应用排名，及各应用的主要用户分布

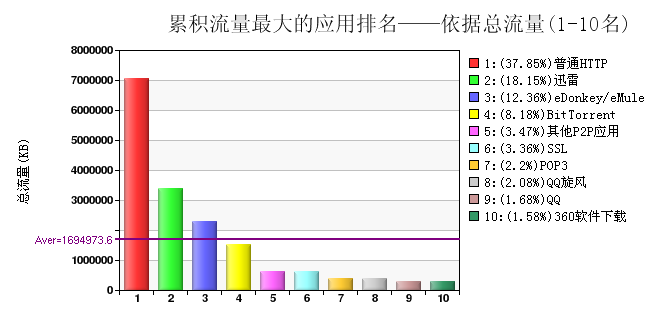


图 2-19 应用流量排名柱状图

 网站访问流量统计报告

− 网站访问流量走势图

− 网站访问流量最大的用户排名，以及各用户主要访问的网站

− 流量最大的网站类别排名，以及各类别网站访问的主要用户

− 流量最大的网站排名，以及各网站访问的主要用户

 邮件收发流量统计报告

− 邮件收发流量走势图

− 收发邮件流量最大的用户排名，以及各用户使用的主要邮箱

− 流量最大的邮件类型，以及各类型邮件的主要用户

 论坛发帖流量统计报告

− 论坛发帖流量走势图

− 论坛发帖流量最大的用户排名，以及各用户发帖的主要网站

− 流量最大的论坛排名，以及各论坛发帖的主要用户

 文件传输流量统计报告

− 文件传输流量走势图

− 文件传输流量最大的用户排名，以及各用户传输文件的主要类型

− 各类传输工具流量排名，以及使用各类传输工具的主要用户

− 各类型文件传输的流量排名，以及传输各类型文件的主要用户

 **上网时长统计报告** 在选定的时间范围内，对于选定的部门（用户组）：

− 上网时间最长的用户排名，及个用户的主要网络应用

− 使用时间最长的网络应用排名，及使用各应用的主要用户

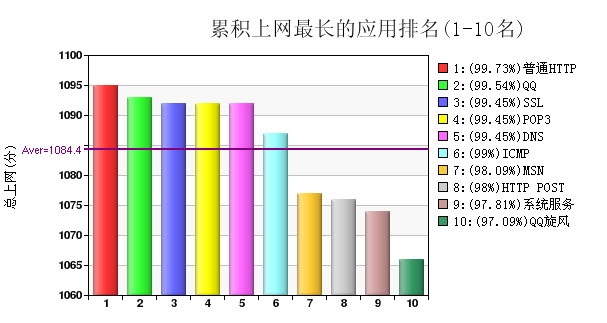


图 2-20 上网时长排名柱状图

#### 3.9.2.3 智能分析报告

360 上网行为管理系统提供面向管理者和决策者的智能分析报告。该报告基于对用户上 网日志的深度数据挖掘，以指数评估形式直观的向管理者提供员工工作效率分析报告、网络 带宽负载分析报告，以及员工互联网行为合规分析报告，并对如何提升网络健康指数（即， 网络综合指数）提出指导和建议。

 **带宽资源报告** 网络管理员希望网络能够流畅运行，组织管理者希望带宽资源的投入能够真正用于办

公，为了达到这样的目的，他们都需要知道网络带宽的使用情况、流量的分布情况，然后基 于这些实际情况采取针对性措施。“带宽资源报告”能够满足网络管理员和组织管理者了解 这些信息。

 **工作效率报告** 工作效率评估报告可以揭示员工互联网行为与工作的相关性，及非工作相关行为对工作

效率的影响程度，并指明影响工作效率问题的根结（哪些行为、主要是谁）；为 HR 部门和 部门经理对员工的绩效考核提供参考信息。

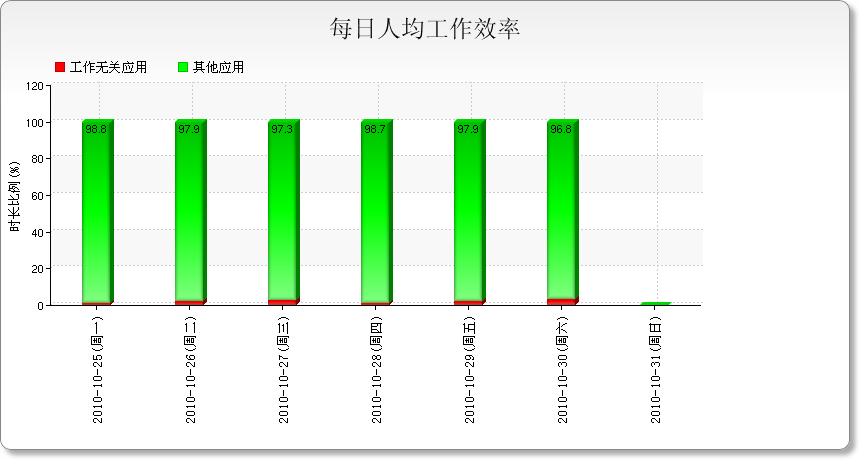


图 2-21 工作效率分析图

 **行为合规报告** 行为合规分析可对内网用户的互联网访问进行合规度分析，帮助管理者了解上网用户行

为是否符合国家政策法规、行业规范，以及企业规章制度。一方面告知整体上用户不合规行 为的严重程度，另一方面可以得到某用户或某部门不合规行为的分析结果。

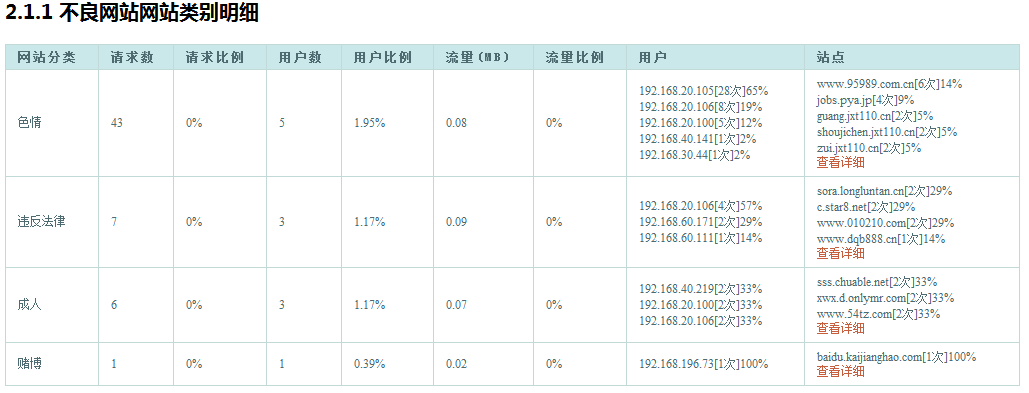


图 2-22 行为合规分析明细表

#####  带宽资源评估报告

IT 部门希望网络能够流畅运行，组织管理者希望带宽资源的投入能够真正用于办公， 为了达到这样的目的，需要全面了解网络带宽负载和流量的分布情况。系统通过柱状图，饼 状图及图表可以直观展示带宽负载分析结果。使管理者直观了解带宽资源的损失情况，以便 采取针对性措施降低企业运营成本。

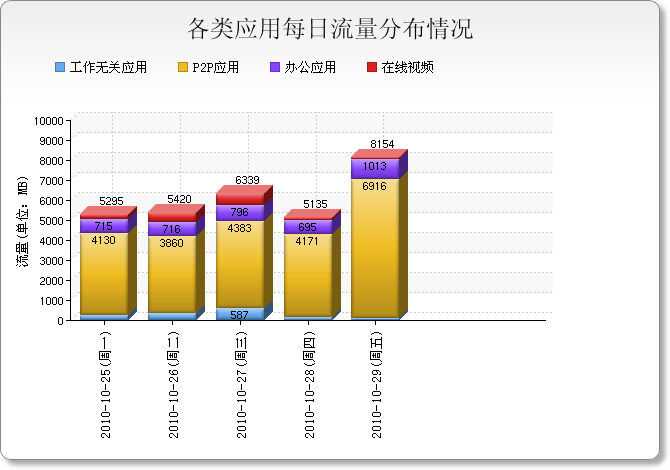


图 2-23 带宽占用分析图

## 3.10 日志管理

### 3.10.1完整的日志记录与导出备份

360 上网行为管理系统完整地记录内网用户网络访问的日志，包括上网时间、网络流量、 Web 访问记录、接收与发送的邮件、IM 聊天的内容、论坛发帖内容、网络游戏记录、P2P 下载记录，以及访问在线视频、在线炒股活动等等。为进一步的查询统计与报表分析提供了 完整的基础信息。

上网行为管理系统设备保存预设时间范围的所有数据（默认为 60 天），对于历史数据， 可以通过导出进行备份。备份方式包括 FTP 自动定期导出、USB 手工导出。

### 3.10.2日志中心

360 上网行为管理系统支持独立的日志中心，它可以将用户上网日志存储在外置存储设 备中。并拥有与上网行为管理系统一致的所有查询、统计、报告功能。其优点在于：

 **海量存储** 日志中心保证了日志存储的安全性与完整性。由于日志服务器的存储系统可以按需

扩展，容量仅受限于硬盘大小与数量，因此可以实现用户日志的长时间保存，为日 志分析与法律遵从提供完整的数据。

 **高性能日志离线查询** 日志中心提供强大的日志查询与分析能力，可以对用户上网的历史日志离线查询。 由于数据查询可以离线进行，不仅提高了日志查询统计的效率，还降低了上网行为 管理系统的计算压力，使得上网行为管理系统能够“专职”进行协议识别与过滤控 制。

 **日志信息全文检索** 日志中心支持用户日志的全文检索。可以通过关键字检索指定日期范围、指定应用 类型的用户日志。帮助管理员快捷获取与某用户、某敏感内容信息相关的所有日志 记录。

 **日志完整性保证** 当上网行为管理系统与日志中心的网络连接异常时，上网行为管理系统将在本地缓 存新生成的用户日志，待连接恢复后自动上传到日志中心，确保日志的完整性。

## 3.11 集中管理 SMC

对于分布式部署多台上网行为管理设备的集团用户，SMC 集中管理中心可以帮助管理 员随时了解各分支机构的设备运行状态，统一制定、下发上网行为管理的策略，并定期收集 各分支机构用户上网行为日志。从而节省企业网络运营和维护成本，便于网络管理者统揽全 局，提高对用户互联网行为管控的效率与力度。

 **设备管理** 实时监控：对所管控的上网行为管理系统设备进行分组管理，实时监控各上网行为

管理系统设备的状态信息，如在线用户数、上传流量、下载流量、并发 连接数等等。

运维管理：可远程完成上网行为管理系统设备的各项系统配置，远程控制上网行为 管理系统升级软件版本、应用协议库和 URL 库。

 **策略制定与下发** 集中管理中心能够设置统一管理策略，如网页过滤策略、应用控制策略、内容审计 策略等到那个，下发至所管理设备。

 **设备日志查询** 可以查询对设备的操作日志、系统报警日志和用户报警日志的查询功能。

## 3.12 用户管理

用户是上网行为管理产品最核心的要素，任何一条策略都是针对一个用户或者部门设置 的，因此对于用户的识别、认证与管理能力决定了上网行为管理的效果。360 上网行为管理 系统提供了丰富的用户认证方式以及符合企业实际的用户管理能力，很好地满足企业对于用 户的管理要求。

### 3.12.1用户身份信息维护管理

 **按照企业组织结构建立用户组** 当用户数目较多、组织结构比较复杂时，按照实际的组织结构管理用户是最有效的方式，

易于管理员查询、定位和设置策略。360 上网行为管理系统支持树型结构管理用户，能够完 全按照企业的实际情况建立用户组，如下图所示：

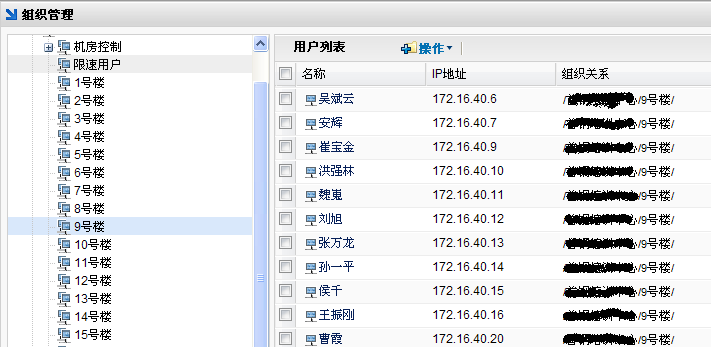


图 2-24 按照企业组织结构管理用户

 **IP 网段自动分组** 任何互联网行为管控和审计策略最终都将赋予到用户或用户组上，对于以 IP 网段划分

部门的机构，如果用户数目众多或者 IP 分配变化频繁（如大学的院系），针对每一个用户进 行单独的设置是不现实的，这些机构关心的更多的是对某一类用户进行管理，而不是特定的 用户。360 上网行为管理系统可以按照网段进行分组并设置策略，属于某网段的 IP 会自动 适用该网段的策略。上网行为管理系统支持将新入网的未注册 IP 自动加入到所属的 IP 分组

中，从而自动为该 IP 分配预定义的管控策略。对于那些临时来访的外来用户，管理员可以 将其计算机设备统一划分在某一 IP 范围内，并对该 IP 网段分组制定相关限制性策略，大大 增强了动态用户管理的灵活性。

此外，如果管理员没有预先设置 IP 网段，上网行为管理系统可以将未注册的用户实时 加入系统的未定义用户组中，管理员可以在合适的时机将其移动到已定义用户组中，从而逐 步完善用户的定义。

#####  支持用户的权限组管理

360 上网行为管理系统支持权限组的定义和管理。可在各级用户组织中建立“权限组”， 可将任意用户添加入“权限组”中，一个用户可以同时隶属于多个权限组。这一功能提高了 用户策略管理的灵活性，在不改变原用户的组织结构的情况下，可实现对一些分散在各组中 的用户进行统一策略管理。

#####  支持 AD 域权限组导入

360 上网行为管理系统可将 AD 域服务器中用户权限组信息导入到用户组织列表中，并 自动创建相对应的权限组，可定义各权限组的互联网行为管控策略。

针对企业网络最常用的认证体系联动（LDAP），重新调整功能实现，支持：

 可设置支持完整&部分 LDAP 导入，包括权限组导入；

 可灵活设置同步模式（导入、镜像），确保与 LDAP 服务器保持用户信息联动；

 支持多个 LDAP 服务器同时导入，无需担心组织冲突以及显示问题；

 **支持属性组**

360 上网行为管理系统率先支持属性组用户。属性组用户是指将某些具有一定共同特征

（如部门、职位、电话等）的用户以属性组进行保存，网络管理员可从属性这一维对用户进 行管理，例如，可通过策略方便实现财务部用户禁止使用 QQ 等功能。

#####  支持从多个 LDAP 服务器同时导入用户数据

对于那些拥有多 AD 子域服务器的网络环境，上网行为管理系统可同时同步所有 AD 子 域服务器中的用户信息数据，实现全网用户的统一管理。同时，可以自定义 LDAP 的导入 入口。

#####  支持用户对象的快速搜索选择

在用户数量庞大，用户组织结构复杂的网络环境中，管理员在制定策略或查询日志时， 按组织关系逐层筛选用户这一操作会耗费大量的时间和精力。

360 上网行为管理系统可以避免上述问题，在所有用户对象选择对话框中，支持用户搜 索定位功能。只要在搜索框中输入要选择的用户组或用户名称，即可直接将该用户或用户组 添加到用户对象中。

#####  支持 IP/MAC 绑定及自动绑定

360 上网行为管理系统支持二层网络环境和三层网络环境下的 IP/MAC 绑定。可自动阻 塞那些非法占用他人 IP 地址的用户。此外，系统支持在建立用户时自动进行 IP/MAC 的绑 定操作。

#####  支持免控制与免审计用户

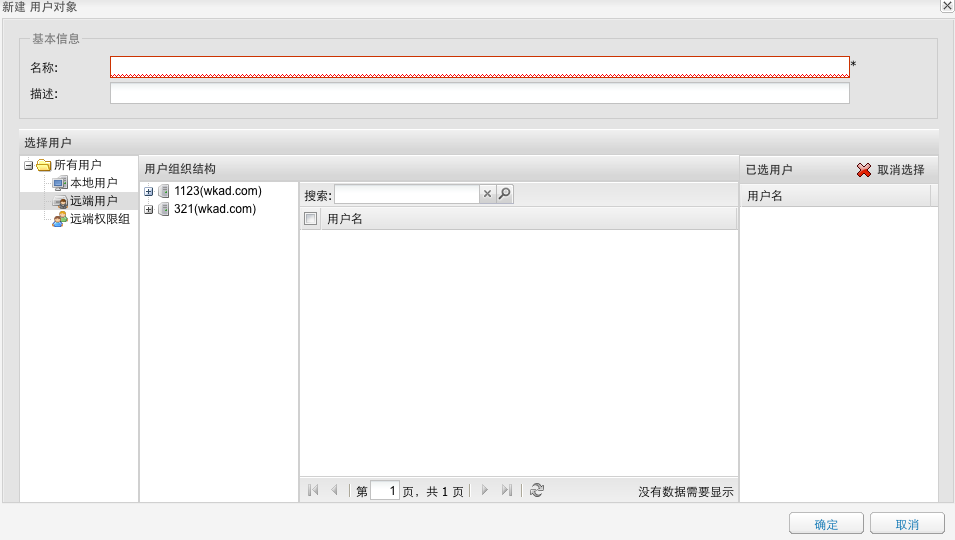
对于在特殊情况下不需要控制或审计监控的用户，360 上网行为管理系统提供免控制和 免审计功能。

#####  AD 用户远程管理

360 上网行为管理系统支持 AD 用户远程管理功能，无需将用户全部导入至上网行为管 理系统本地，即可满足用户管理需求。

在 AD 第三方服务器配置完成之后，配置策略时可选择本地用户和远端 AD 用户，如下

图：



其中远端用户是 AD 的用户和用户组，远端权限组是 AD 上的权限组息。

### 3.12.2用户身份识别与认证

#####  丰富的用户认证方式

360 上网行为管理系统提供多种用户认证和识别方式，为用户管理提供了灵活而完善的 方案，包括基本的 IP/MAC 绑定、三层网络环境下的 IP/MAC 绑定、网关 Web 认证、AD 域 透明认证、LDAP 认证、RADIUS 认证、POP3 认证、ESMTP 认证、SOCKS 认证、802.1x、 PPPoE 认证账号识别、第三方用户识别。此外，对于使用微软 ISA 系统的环境，上网行为 管理系统还支持 NTLM 认证和 BASIC 认证，实现与 ISA 的联动。对于每一种认证方式，上 网行为管理系统都支持分段/混合认证。通过规划并部署合适的认证方式，可以把互联网访 问管理应用到具体用户，实现基于用户身份的访问管理。

在有些企业，实行规划合理并且严格执行的 IP 地址分配制度，那么通过 IP 地址和网卡 MAC 地址来确定用户身份是可靠的；但是在有些网络环境下，用 IP 或网卡 MAC 地址并不 能确定一个人的身份，比如 DHCP 动态分配 IP、或多人共用一台设备的时候，就需要其它 方式确定用户身份，如网关本地 Web 认证或第三方认证。

在 WEB 认证方式下，管理员可以设定并分发统一的初始口令，并定义账号缓存的有效 时间，保障用户身份的安全，使用户身份的确定与具体上网设备完全无关。要实现 WEB 认 证，首先需要在 360 上网行为管理系统中建立用户信息。上网行为管理系统支持多种用户信 息获取方式，可以通过 IP 网段地址扫描，自动获取内网用户的 IP 地址、计算机名、MAC 地址信息，也可以通过 LDAP 同步的方式定期更新用户目录服务器的用户信息，支持 RADIUS 认证，此外，还可以使用 360 自定义用户导入功能，将微软 Excel 表格整理的用户 信息快速导入。

建立用户信息后，按照管理需求，基于网段、权限、行政职能自定义用户组和成员，并 且可以在不同用户组之间灵活调整成员用户，最终形成清晰直观的树型组织结构。这样就解 决了“确定用户身份”的问题，并为基于用户或用户组制定策略和统计报表奠定了基础。

上网行为管理系统支持专用Portal模式，由一台单独的上网行为管理系统设备提供高性 能的Portal服务。



#####  支持认证界面自定义发布信息

使用 360 上网行为管理系统的 web 认证界面登录时，管理者可以自定义登录界面的信 息。在登录界面有专用的窗口用于展示发布信息的标题和内容。同时，登录界面的图片也可 以有管理者自定义设置和变更。

 **支持混合认证**

360 上网行为管理系统支持多种认证方式的混合，可方便为不同的网段开启不同的认证 方式，实现不同用户群的差异化管理；同一网段用户也可同时开启多种认证方式，方便用户 在不同的应用环境下都可以认证入网。

#####  支持邮件用户识别

对于拥有独立企业邮箱的网络环境，上网行为管理系统支持 POP3 用户识别，用户入网 无需认证，只要通过 POP3 协议接收一封邮件，上网行为管理系统即可将邮件账号名记录下 来，该用户所有互联网行为都可实名制记录下来，便于日后日志的查询、定位。

#####  支持计算机名识别

360 上网行为管理系统支持根据内网计算机的计算机名识别，用户入网无需认证，360 上网行为管理系统能够自动扫描每一个入网计算机的计算机名并将其作为用户账号记录下， 在该计算机上发生的所有网络访问行为将记录在其计算机名下。

 **支持强制下线**

360 上网行为管理系统支持 WEB 认证、LDAP 认证、RADIUS 认证、邮件账号认证、IP

识别用户的强制下线。

使用者也可以随时将活跃用户列表中的 IP 加入“屏蔽 IP 列表”中。

 **支持认证账号有效期限制** 对于一些需求临时入网的用户，管理员可通过该功能限制这些用户可以入网的时间范

围，超出限定范围后，该用户无法再入网。一方面提高准入用户的安全性，另一方面可实现 入网限时的功能。

#####  支持认证账号唯一性控制

360 上网行为管理系统支持认证账号唯一性控制。这一功能可以方便控制同一认证账号 是否允许在多台计算机上同时登陆。从而适应不同用户的认证需求。

#####  支持认证账号黑名单

对于行为异常的认证账号，360 上网行为管理系统支持将其加入到认证账号黑名单。未 经管理员将其从黑名单中清除，该账号将无法通过认证。

#####  支持第三方认证信息联动接口

360 上网行为管理系统提供标准的第三方用户认证信息联动接口，可以接收来自第三方 网络准入系统或上网计费系统的用户认证信息。从而将上网行为日志准确关联到具体的用 户，并实现用户在多认证系统环境下的单点认证。

 **登录重定向**

360 上网行为管理系统提供登录重定向增值功能。用户认证通过后，第一次上网请求将 触发此功能，网页访问请求被重定向到预设的 URL。对于集团企业、政府机关和学校，便 于上网用户方便地获悉最新的公告或者相关信息。

## 3.13 分级分权管理

360 上网行为管理系统支持根据不同的管理权限和管理级别，创建不同级权的设备管理 员和日志审计员账号。能够多维度的划分管理权限，包括：

 策略配置权和日志审查权的划分，实现上网行为控制和上网行为审计的独立运作。

 所管辖的用户对象的划分，实现分部门、分人员的管理，不同部门和人员之间策略 配置互不干涉。

 功能模块的划分，实现策略管理、用户管理、系统管理的分权操作。

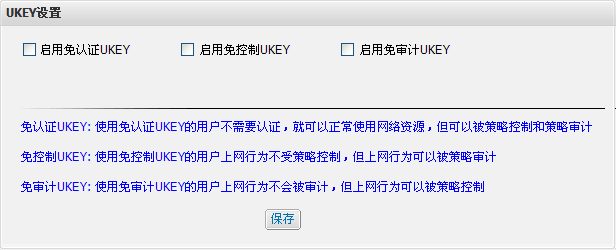
 日志查询模块划分，可限定日志审计员是否允许查看邮件、聊天、发帖等具体内容 丰富的，多维度的权限划分，充分满足企业或组织用户对账号权限管理的要求。

## 3.14 特权 USB-Key

在企业、政府机关、学校等组织中，某些网络用户因为工作或其他原因需要有具有 特殊上网权限，例如他们的上网行为不应当被审计，或者不应当被控制，甚至应当允许 无需认证就能上网，那么就需要用到 USB-Key。

360 上网行为管理系统 USB-Key 模块在实现特权用户管理的同时，以硬件方式避 免了因为病毒、木马导致的密码泄露、账号盗取等问题，并且具有极高的易用性，特权 用户只需在 PC 上插入上网行为管理系统 USB-Key 即可实现上述功能。

上网行为管理系统的 UKEY 主要支持 7 种特权：免认证、免审计、免控制、免认 证+免审计、免认证+免控制、免审计+免控制、免认证+免审计+免控制。



 免认证：使用免认证 UKEY 的用户不需要认证就可以使用网络资源，但可以被策 略控制和策略审计；

免审计：使用免审计 UKEY 的用户上网行为不受除邮件外发预审策略外的其他所 有审计策略的审计，也不受审计策略的控制（即审计策略对免审计用户不生效）。 但受控制策略的控制；

 免控制：使用免控制 UKEY 的用户上网行为不受流量控制策略、每用户控制策略、 应用控制策略的控制，也不受审计策略中控制动作的控制，但是仍然受审计策略的 审计。

## 3.15 设备自身安全

为了最充分地管理控制用户上网行为，360 上网行为管理系统部署在企业的网关位置， 因此，设备自身的安全稳定将直接影响网络运行。360 上网行为管理系统从软、硬件两方面 针对性地增强了系统的稳定可靠，确保网络运行畅通。

#####  专用的安全的软、硬件系统

360 上网行为管理系统采用专用的操作系统 NSOS，它在成熟的操作系统基础上，针对 上网行为管理的特点，进行了大幅度的裁减，关闭非相关端口与服务，确保不受网络病毒的 危害；重新编写 TCP/IP 协议栈，优化网络驱动，减少系统内核与用户空间的数据交换，大 大提高了网络数据的处理能力。

硬件方面，360 上网行为管理系统充分考虑用户机房网络环境，在设备的通风、电磁、 降噪、信息显示以及手工管控等方面进行了大量的革新，确保设备的高效运行与安全操作。

#####  软硬件旁路功能避免出现单点故障

360 上网行为管理系统提供硬件 bypass 与软件 bypass 双重保护，确保发生异常时网络 依然畅通。

**硬件 bypass：**由于意外原因发生设备掉电时，360 上网行为管理系统将自动启动硬件 bypass 功能，设备在物理上成为一条连通的网线，不会对已有的网络连接产生任何影响。此 外，360 独有的一键 bypass 功能，在设备有电的情况下，可以“主动”将设备切换为 bypass 状态，卸载网络流量。

**软件 bypass：**当网络负载超过设定的安全阀值时，系统自动启动软件 bypass 功能，选 择性停止对各种网络数据的分析处理，以设备最大带宽“放行”数据包。当网络负载恢复到 安全阀值以下时，系统自动恢复各种处理功能。

#####  支持双机冗余热备

360 上网行为管理系统支持单链路及多链路环境下的双机冗余热备。主机或主链路故障 后，备机或备链路上网行为管理系统可自动接管网络，执行与主机一致的管控策略，并且对 上网用户完全透明。

#####  控制内网病毒攻击导致的异常流量

360 上网行为管理系统通常部署在防火墙的内部，与防火墙互为补充，可以针对来自内 部的攻击进行识别与防范。如果内网发生 ARP 攻击事件，引起网络流量异常增加，上网行 为管理系统可以在第一时间识别感染 ARP 病毒的主机，并发送告警邮件给管理员，提示及

时防范。此外，当发生异常流量时，通过设置来源 IP 访问的上传包速率、上传速率、新建 连接速率、小包发送速率等多个阀值，对突发流量进行带宽整形，对危险主机进行带宽“抑 制”，同时保障上网行为管理系统自身的请求响应能力。对于超出阀值的流量，除了带宽限 制，还可以完全阻塞、或者只阻塞超出阀值部分的流量，对于异常流量的 IP，可以设置加 入黑名单进行屏蔽。

 **支持 DDoS 防护设置** 在内网有异常流量时，保护上网行为管理系统自身安全。



 **限制可访问上网行为管理系统的 IP 地址范围和登录时间** 为确保上网行为管理系统自身的安全，360 上网行为管理系统提供管理界面访问限制功

能，可定义允许登录上网行为管理系统管理界面的 IP 地址范围，非法用户即使获取了用户 名和口令，也无法登陆上网行为管理系统的管理界面。

同时，360 上网行为管理系统的 web 管理界面能够设置登录后未活动的会话超时时间， 当登录的管理账号未活动时间超过指定时间时将自动断开连接，以提高账号的安全性。

## 3.16 虚拟专用网络（IPSec VPN）

虚拟专用网络（Virtual Private Network ，简称 VPN）指的是在公用网络上建立专用网 络的技术。360 上网行为管理系统支持与其他厂商的 VPN 以标准 IPSec 进行互通。

360 上网行为管理系统支持完整的标准 IPSec 协议定义的 VPN 功能，并可对 VPN 隧道

的连接方式进行详细灵活的配置，如用户可配置 IKE 认证方式，是否需要 NAT 穿透等。

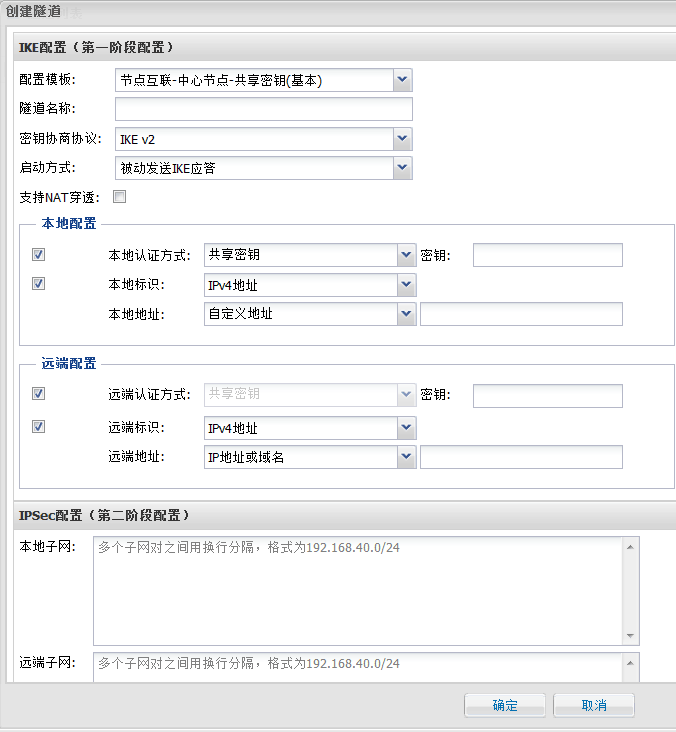


图 2-25 VPN 配置界面

360 上网行为管理系统的 VPN 模块同样支持隧道状态的实时监控。使用“红”、“黄”、“绿” 三种颜色的信号灯表示当前 VPN 隧道状态，并可以查看对端 IP、两端子网及流量统计信息。



图 2-26 VPN 隧道信息

360 上网行为管理系统支持 VPN 证书管理功能，包括导入 CA 签发的证书，或者生成 证书请求然后提交至 CA，使其依据请求生成证书，然后进行导入。导入证书后，可将证书 与 CA 证书进行比对，匹配后可通过认证，隧道建立成功。



图 2-27 证书管理

# 4 特点与优势

作为一款优秀的上网行为管理产品，360 上网行为管理系统全面引领国内行业潮流，并 在多个方面达到国际水平。

## 4.1 国际领先的中文 URL 过滤系统

URL 过滤是上网行为管理产品核心功能之一，360 上网行为管理系统在 URL 覆盖的全 面性、识别准确率、更新实效性、客户同步及时性等方面，具有国际领先的明显优势。

#####  最先进的基于行为结果的 URL 预分类模式

360 上网行为管理系统采用国际上最先进的 URL 预分类模式，基于行为结果（即： 访问后产生的后果、影响）而不是基于内容分类，通过机器学习、中文分词技术等对网 页内容进行全息分析和语义识别，从而对网站进行准确地分类。与字符串匹配方式不同 的是，网页全息分析技术从网页结构、语义、上下文、网页相似度等多角度分析网页， 能够“理解”网页的内容，确保网站不因关键词匹配的多寡误分类。

#####  全球最大的中文 URL 数据库

360 上网行为管理系统自主研发的 URL 自动抓取系统全天候获取 URL 信息，已基 本覆盖中国大陆地区的网站。此外，360URL 自动分类引擎根据中国的文化背景、伦理 道德、法律法规、上网习惯等，将 URL 分为 150 余类，目前已经超过 4000 万条，是全 球规模最大、内容最全的中文 URL 数据库。

#####  独有的二级 URL 分类数据库

360 上网行为管理系统独有的 URL 二级分类功能，在实现全面精细的 URL 分类的 同时，极大的提高了用户的网络管理维护效率。比如，将“财经”URL 分类细分为股 票、基金、外汇、期货、银行等子类。

#####  实时更新，每天更新超过 300 万条记录

360URL 库更新快速，对于新生、变更、消亡的 URL，360URL 服务器 7x24 小时 抓取更新，每天更新超过 300 万条，并自动分类，保证 URL 库的实效性。

#####  人工辅助校验审核

为了纠正自动分类的误差，360 配备了一支几十人的专业 URL 分类审核团队，负 责对 URL 自动分类结果做校验审核，做到对每一条 URL 确认，保证分类的准确性超过

99%。

#####  客户定期自动获得最新 URL 库

客户设备可设定时间，定期从 360 服务器获得最新 URL 库，保证设备 URL 的实效 性。

#####  未分类 URL 回传再分类，快速收敛用户管控 URL 范围

360 产品支持客户未分类 URL 回传、自动分类下发功能，使得通过一段时间的积 累，客户管控的 URL 范围快速收敛。

## 4.2 国内最全面的网络应用协议数据库

对网络应用的管理也是上网行为管理产品必不可少的核心功能。360 上网行为管理系统 能够识别国内主流的网络应用，是国内第一款支持在线炒股交易与查看行情区别控制、支持 迅雷 P2P 下载控制的上网行为管理产品。

#####  识别超过 4000 多种网络应用

360 上网行为管理系统能够对传统标准应用协议、电子邮件、P2P、IM 即时通信、

网络游戏、网络电视、在线炒股、在线购物、在线社交、远程登录、代理软件等 600

多类网络应用进行准确识别与控制，是国内最全面的网络应用数据库。

#####  全部基于应用特征与行为特征识别

传统安全产品通过 IP 或者端口封堵各种网络链接，只能局限于标准的协议，如 HTTP，SMTP，且主要是在网络层以及传输层进行，对应用层的内容无能为力，而且， 如果 IP 与端口经过动态协商建立，比如 QQ，P2P 下载等，则完全不能胜任。360 上网 行为管理系统对应用的识别是通过应用特征与行为特征实现的。所谓应用特征，是指在 成序列的数据包的应用层信息中，存在有规律的字节特征，它可以唯一地标识某种应用 协议，就如同一个人无论穿什么颜色的衣服，其指纹特征不会改变，而且是唯一的，类 似地，上网行为管理系统可以通过特征值准确地识别网络应用；而行为特征，是指连续 多个包或者多个并发的网络连接表现出来的某种行为模式具有一定规律性，通过这些行 为模式可以识别特征值不明显的应用类型。

 **实时维护，定期更新** 随着互联网的迅速普及，各种网络应用层出不穷，而且版本更新速度越来越快。360

的专业的应用协议分析团队实时跟踪网络应用的变化情况，在第一时间内提供升级包， 用户可以设置定期下载更新。

## 4.3 精细化的策略管理

精细管理是 360 上网行为管理系统的一大特点，无论是功能设计还是细节操作，上网行 为管理系统都充分考虑了操作人员的管理需求与工作习惯。

#####  精确控制 IM 软件的子应用

360 上网行为管理系统支持对 IM 软件的各种子应用进行独立控制，例如：允许通 过 QQ 聊天与文件传输进行客户支持，且保障 QQ 远程协助的带宽，但禁止玩 QQ 游戏， 禁止欣赏视频等。既充分利用 IM 即时沟通的便利性，又能防止沉迷游戏导致的工作效 率下降。

 **灵活的策略设置**

360 上网行为管理系统支持根据用户、时间、应用等条件设置灵活的策略，对于每 一种行为可以设置允许、阻塞、审计、以及流量控制。

对于特殊情况下不需要监控的用户，上网行为管理系统提供免监控功能。同时，对 于有攻击行为的 IP，管理员可以将其放入黑名单中，在一定时间内禁止上网。

#####  策略设置可细化至每个用户的每一个网络应用

360 独有的对用户以及应用的树型管理方式，可以针对用户的任何具体的网络应用 设置策略，如仅允许员工使用 263 邮箱发送邮件，其它 web email 全部禁止，再如禁止 用户使用 BitTorrent 软件下载视频文件。这为管理员设置精细的控制/审计策略提供了极 大的便利。

 **数据统计支持子查询** 面对海量的上网日志进行统计分析，上网行为管理系统支持在统计结果中设置关键

字进行子查询，以更准确地获取信息。此外，在统计日期范围内，还可以进一步限定每 一天的时间段，如：可以统计一周内上班时间各种网络应用的流量，从而把非工作时间 排除在外，更合理地反映网络带宽的使用情况。

 **按照不同粒度进行数据分析** 用户可以选择全链接或者仅主链接，查看实时的或者历史 Web 访问情况。而对于

流量的监控与统计，则可以选择按照天、小时以及更细的时间粒度进行查看，这对于管 理员准确定位与分析异常网络行为，无疑提供了非常实用的手段。

## 4.4 细化的应用带宽管理与流量控制

由于以 P2P 为代表的网络下载软件严重影响了企业网络的带宽使用，使得基于应 用层的带宽管理成为多数企业的迫切需求，从而带宽管理与流量控制也是上网行为管理 产品的重要功能。360 上网行为管理系统提供细化的管理策略，帮助企业实现带宽的合 理利用。

 **针对每一个用户/部门设置带宽** 上网行为管理系统可以为每一个用户或者部门设置带宽，该用户或者部门的所有应

用都被限制在设定的带宽内，对其他用户或部门不产生任何影响。

#####  针对每一种网络应用设置带宽

为某一种应用，如 BT 设置上限带宽，所有用户通过 BT 下载文件时，将共享设定 的带宽，从而避免对其它应用带宽的挤占。

 **防止个别成员独占部门带宽** 在某些情况下需要对部门设置总带宽，为了防止部门的个别成员因为 P2P 下载挤

占其它成员的带宽，上网行为管理系统可以设置部门成员的平均上限带宽，也可以将带 宽通道按用户动态平均分配，从而每个成员的网络访问都限制在自己的带宽范围内，实 现带宽资源的公平共享和最大化利用。

 **优先级设置** 上网行为管理系统的带宽通道可以设置优先级，高优先级的带宽通道数据优先通

过，保障企业的核心业务传输畅通无阻。此外，在总带宽资源相对富余时，高优先级的 应用可以借用空闲的通道，实现带宽资源的统计复用。

 **对突发流量进行整形** 上网行为管理系统可以设置内网主机的上传速率、新建连接速率、小包发送速率等

多个阀值，对于超出阀值的流量，可以进行带宽限制、阻塞超出阀值部分，或者全部阻 塞，甚至将异常 IP 加入黑名单，实现对突发流量的带宽整形。

## 4.5 高效内容分析引擎

#####  零拷贝技术，极大提高网络包处理速度

零拷贝（zero-copy）基本思想是：数据包从网络设备到用户程序空间传递的过程中， 减少数据拷贝次数，减少系统调用，提高 CPU 与内存的使用效率。实现零拷贝的最主

要技术是 DMA 数据传输和内存区域映射技术。360 上网行为管理系统采用零拷贝抓包 技术，极大减少了 CPU 的中断调用，显著提高了包处理效率。

 **择时组包，智能流分析** 相比传统的防火墙设备，上网行为管理产品更多地关注内容层的处理。在 IP 网络

中，内容数据被分拆封装在多个数据包中传输，为了获得完整的内容，必须把连续的多 个包“拆封”重新组合起来。360 上网行为管理系统专有的择时组包技术，能够智能判 断哪些包可以放过，哪些包需要暂留重组，减少了包处理的数量，从而提高数据流的分 析效率。

## 4.6 强大的查询统计与分析报告

 **对任意用在任意时段的上网行为进行详细的查询** 内容含盖网页访问、邮件收发、IM 聊天、P2P 下载、论坛发帖、各类应用信息、 流量信息、在线娱乐等。

 **超过 80 种报告模版** 为管理员和企业决策人员提供完整的用户上网分析素材。

 **面向不同管理角色的分析报告** 对于设备管理员和企业决策人员，分别提供相应的分析报告。

#####  递进式分析，深入了解网络活动

360 上网行为管理系统独有的递进式（drill-down）统计分析，帮助管理员从宏观到 微观，从全局到局部，层层递进，深入分析，全面了解用户上网行为与网络资源的使用 效率。

 **即席（ad-hoc）关联分析，迅速定位问题** 上网行为管理系统独有的即席关联分析技术，可以帮助管理员在发生网络拥塞时，

迅速查看导致拥塞的用户和应用，以便立即采取措施调整网络负载。

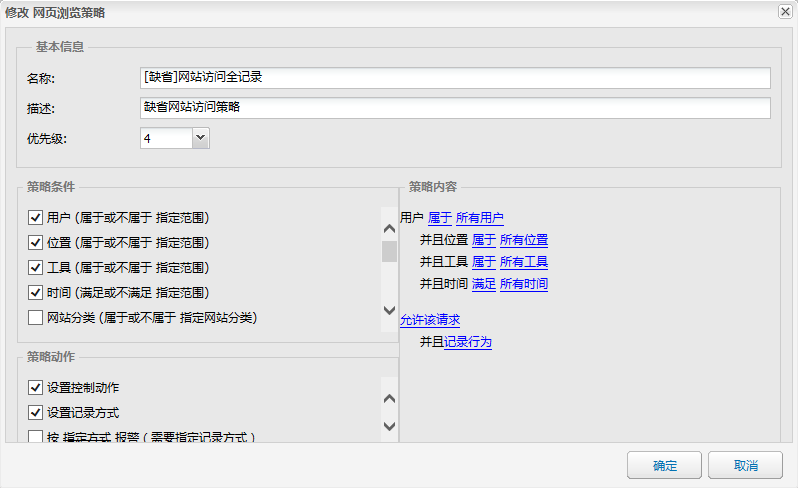
#####  所有分析报告都可以以表格、饼图、柱图或线图等方式清晰直观地展示

## 4.7 完整的 BYOD 解决方案

BYOD（Bring Your Own Device）是指携带自己的设备办公，这些设备包括个人电 脑、手机、平板电脑等（而更多的情况指手机或平板这样的移动智能终端设备）。360

上网行为管理系统具有业界最完整的 BYOD 审计控制解决方案，可对移动终端的类型 及移动应用网络协议进行精确的识别，并可制定策略实现审计、控制、日志记录等功能。

360 上网行为管理系统在用户属性中加入了“工具”属性，因此可精确识别用户上网 工具，如 Windows、Linux、iOS、Windows Phone、Android 等设备；此外网络管理员 可将 IP 范围定义为用户“地点”属性，因此可区分不同网段对应的不同地点。



网络管理员利用用户的“工具”及“地点”属性可灵活地制定针对 BYOD 移动设备的 审计控制策略，例如在一幢办公大厦的某一层，允许西区办公室的 iOS 及 Android 设备 接入互联网；而在东区办公室，则允许除了 Linux 外的所有设备接入互联网，但无法使 用 QQ 及移动 QQ。

360 上网行为管理系统 BYOD 审计解决方案具有如下特点：

#####  极高的识别准确率

360 上网行为管理系统可高效识别接入网络的主流移动设备并保持极高的识别准 确率，网络管理员完全无需对策略的漏网之鱼担心。

#####  业界最丰富的移动应用协议库

360 上网行为管理系统拥有业界最为丰富的移动应用协议库，目前已超过 500+，涵 盖浏览器、IM 聊天、新闻阅读、音乐播放、社交网络、支付购物、网络游戏等 10 个类 别，基本覆盖目前大多数主流移动应用。

 **灵活的策略配置**

360 上网行为管理系统支持多种用户属性作为策略条件，可实现移动终端准入、移 动用户管理、移动内容审计控制等多项功能。

## 4.8 人性化界面设计，易于操作管理

#####  管理界面简洁清晰，美观大方

360 上网行为管理系统管理界面采用最新的 web 技术，结合传统 C/S 的操作风格， 大大加强了 Web 操作的交互能力。界面结构清晰，美观大方，从整体布局到细小按钮 都经过精心设计，充分贴合用户的思维、操作习惯。

#####  树型控制元素，实现便捷操作

上网行为管理系统的 URL 分类、用户组织结构、应用协议结构等多种控制元素都 以树型结构展示，一目了然，便于操作和管理。

#####  标签子界面显示，方便模块切换

上网行为管理系统采用了先进的标签式模块 UI 设计，用户在开启一个模块后，会 以标签形式显示于主区域。用户可利用标签方便在多个模块进行切换，而无需再次在树 状结构中选择进入之前进入过的模块。

#####  在线帮助系统提供智能定位，精确解答操作疑问

#####  向导式配置，轻松完成网络配置

#####  Dashboard 方式集中显示系统宏观信息

上网行为管理系统采用 Dashboard（仪表盘）方式集中显示设备的运行状况与关键 网络活动，使管理员可以迅速了解最重要的信息。

 **界面元素灵活设置，预留充分的数据显示空间** 上网行为管理系统的界面元素如菜单、按钮、区域窗口都可以按需伸缩，列表窗口

的字段宽度也可以自由拖动交换，为数据的显示留出足够的空间，便于用户管理策略和 查看审计结果。

## 4.9 运行稳定可靠，确保网络畅通

#####  全系列设备支持硬件 bypass，避免电源失效导致的网络中断；

#####  独有的一键式 bypass 设计，支持管理员主动调整网络负载；

#####  独有的软件死锁与高负载跳转功能，根据预设阀值自动分流高负载流量；

#####  支持基于 SNMP 的网络管理，可以通过第三方网管软件查看设备的网络信息。

## 4.10 灵活的部署方式

#####  支持网桥模式、网关模式、旁路模式；

#####  网桥透明接入既有网络环境，不影响原有网络配置；

#####  网关模式支持多个网络出口，动态分配带宽资源；

#####  串接方式接入，过滤所有报文，实现完整过滤、审计；

#####  旁路方式确保网络无单点故障，不对网络性能产生任何影响。

## 4.11 独立的日志中心

#####  海量存储，保持日志数据的完整性；

#####  离线查询，降低 360 上网行为管理系统运算负载，提升查询统计效率；

## 4.12 分布部署，集中管理

#####  集中监控分布部署上网行为管理系统设备的运行状态；

#####  制定全局统一策略，集中管控用户的互联网行为；

#####  远程点对点完成分布部署上网行为管理系统设备的日常维护；

# 5 产品的部署

360 上网行为管理系统支持多种接入方式，以适应不同用户的网络环境和管理需求。

## 5.1 串行接入

串接方式能实现对每一种网络应用的精确控制，完整审计所有上网数据。串接分为网桥 模式和网关模式 2 种。

 **网桥模式** 以透明网桥方式接入网络，部署到企业或部门的网络出口位置，无需改动用户

网络结构和配置。

 **单网桥部署** 上网行为管理系统提供一个内网口和一个外网口，作为网桥接入到要管控网络

的出口处，是最普遍的部署模式。 如下图所示：

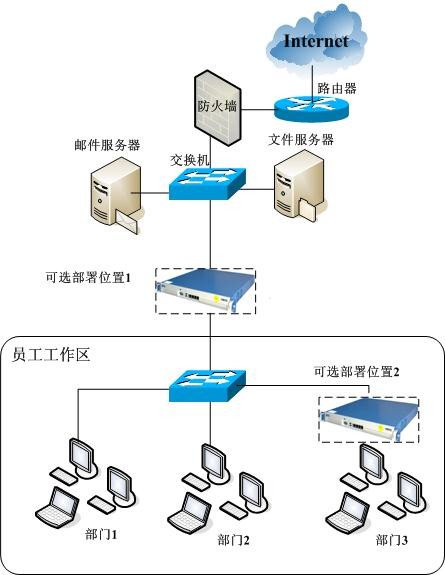


图 4-1 360 上网行为管理系统一入一出，单网桥串接部署示意

 **多网桥部署** 当企业拥有两个互联网出口，且企业内部不同子网需要通过不同的互联网出口

连接互联网时，上网行为管理系统可提供双入双出，双网桥的部署模式。通过一台 设备即可同时管控两条链路内的用户互联网行为。

 **网关模式**

也称为路由模式，将设备串接到网关处，起到隔离内外网和 NAT / 路由的作 用，需要为设备配置内网和外网 IP 地址。

上网行为管理系统在网关模式下，支持 DNAT 功能，可将内网某设备的 IP 或 特定端口映射到互联网中，使公网主机能够访问特定的内网服务器。

网关模式下，支持多出口网络，可以同时配置联通、电信等多线路。多出口环

境下同时支持静态 IP 接入和 ADSL 拨号接入。多线路间采用带宽权限分配机制， 根据链路状态及预设的链路权限动态选择出口，实现多线路的动态负载分配和链路 备份。

## 5.2 镜像旁路

对于那些对网络连续性需求极高，需要全面的行为审计功能，但是对流控和行为控 管功能需求相对较弱的环境，可以采用镜像旁路的部署模式。旁路模式使得上网行为管 理系统通过监听的方式抓取网络数据包，不影响数据包的正常传输，其优点是它对客户 网络环境和网络性能无任何影响，不会引入新的故障点。

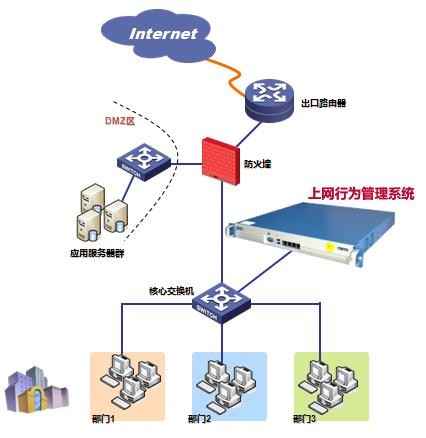


图 4-2 360 上网行为管理系统镜像旁路部署示意

## 5.3 集中管理中心

对于各分支机构都拥有独立互联网出口的集团性企业，通常需要在各地的分支机构分别 部署上网行为管理设备。这给全网的统一管控与用户行为统计分析带来了一定的困难。而 360 上网行为管理系统集中管理中心可以全面的为用户解决上述问题。

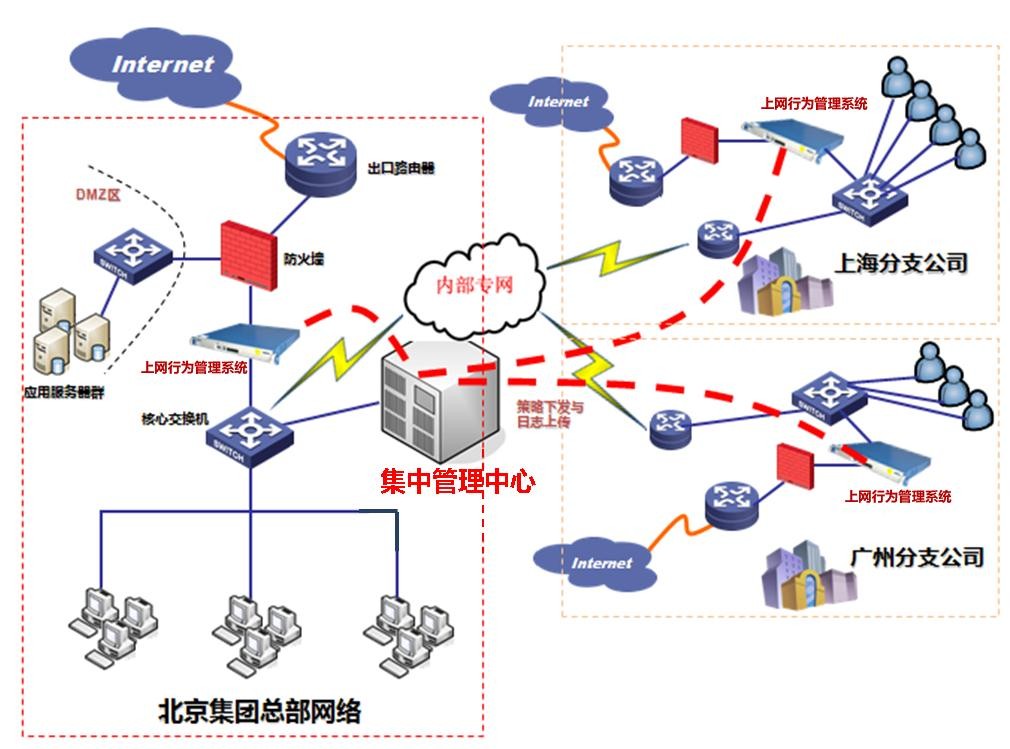


图 4-3 360 上网行为管理系统集中管理中心部署示意

360 上网行为管理系统集中管理中心 SMC 主要功能：

 上网行为管理系统设备状态监控与异常报警

 全局互联网行为管控与审计策略的定制和分发

 远程批量对上网行为管理系统设备进行特征库和软件版本的升级

 点对点远程对上网行为管理系统设备的日常维护

 远程设备用户日志实时查看 通过上网行为分布式集中管理，可以节省企业大量的网络运营和维护成本，便于网络管

理者统揽全局，提高对用户行为的管控效率。

# 6 产品荣誉

2012 年，中国信息安全突出贡献奖

2010 年，中国网络管理技术大会网管员最喜爱上网行为管理产品奖

2009 年，中国信息产业商会 IT 渠道委员会和《计算机产品与流通》中国 IT 金榜最佳 增值产品奖

2008 年，中国企业信息化 500 强大会“最佳上网行为管理产品”奖

2007 年，《网管员世界》编辑选择奖

2007 年，《计算机世界》中国信息安全保障突出贡献奖

2007 年，《51CTO》中小企业 IT 优选产品

2007 年，《中国电脑教育报》教育行业首选产品奖

2006 年，《中国计算机报》用户推荐产品奖

2005 年，《天极网》优秀解决方案奖

