NETCOMMANDER

NC-ASG

NETCOMMANDER

网帅（NC-ASG）

互联网应用安全管理系统

产品白皮书

北京奕恒佳源软件技术有限公司

2010 年 01 月

声 明

本手册为希望与北京奕恒佳源软件技术有限公司建立商业关系者而写。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。本文包含的任何文字均非基于（也不应基于）对未来的设想或表述。

NC-ASG 为北京奕恒佳源软件技术有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 背景

当今的互联网已经从简单的信息增长时代过渡到网络应用的爆炸性增长时代；各类包含特定目的与特定用户体验的网络应用层出不穷。上网条件得到了改善，工作效率也得到了提升，与此同时因为缺乏有效的管理机制，导致网络给企业带来更多的安全威胁。

企业中的互联网用户使用互联网在做什么？是否和工作相关？是否影响了自己或其他人的工作效率？还有其他诸多的问题：

- ✓ 为什么对外的带宽永远都不够？如何控管分配？
- ✓ 员工在上班时间，到底迷失在那些网站？
- ✓ 每年爆增的邮件量，是否真与公司的业绩成长等比例？如何来做分析审计？
- ✓ 即时通讯软件拉近了沟通的距离和速度，但也拉远了工作的效率，如何控管约束？
- ✓ 除了拥有由外到内的攻击防护安全设备外，对于内部隐藏的不当网络行为危机，能否预防掌握？
- ✓ 如何有效引导员工网络安全观念，分析网络行为，并制定安全政策？
- ✓ 出现不法言论或违规事件后，如何锁定责任人？

从管理的角度来看，已经很难通过简单的识别区分用户使用互联网行为。

为“公”还是为“私”。 从技术的角度来看，这些网络应用使用的网络协议，占用网络资源的方式，呈现更加多样化的趋势，为管理带来了更大的难度。由于以上原因，很多企业在互联网应用的管理策略和管理手段方面存在严重的缺失，也给企业的经营管理带来了许多负面的影响。

- ✓ 工作效率的降低。最新的调查报告显示超 60%的企业互联网访问包括了与业务无关的、不恰当的、甚至危险的站点。另外，超过 82%的员工承认在每个工作日都会使用互联网处理个人的事务，包括娱乐。由于在工作时间的网络行为难以受到控制，在上班时间看新闻、聊私事、打游戏、炒股票等已经成为了众人皆知的秘密，这些活动的背后则是效率的下降、生产力的流失，以及长期停滞不前的营业额。

- ✓ 敏感信息泄露。电子邮件（包括 webmail）,MSN/QQ 和 BBS 论坛等网络应用，已经成为提高工作效率的工具，但如果不加以监管，也可能成为泄密的工具。对于政府机关，上市公司和知识密集型企业，关键的设计文档，软件源代码，市场销售计划等核心机密文件，可以通过 webmail，在线聊天工具，BBS 等，轻易地传递到外部，从而给组织造成重大损失。

- ✓ 安全隐患。安全问题也在困扰着 IT 主管。木马、病毒和恶意代码的入侵，使局域网命牵一线，而钓鱼网站、间谍工具的泛滥更使信息安全关系到每一个人。同时，由于缺乏信息安全意识，很多员工将组织的机密文件和信息通过互联网传播，后果严重的甚至使组织被摧毁。

- ✓ 网络带宽浪费。大多数的用户都觉得带宽越来越不够用。其实，很多问题并非出在运营商，而在于局域网中发生的网络活动难以得到控制，例如 BT、电驴、迅雷等 P2P 下载工具的泛滥。使用公司的网络资源下载娱乐内容是非常浪费的，而且有可能影响公司的关键业务。

- ✓ 法律风险。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，工信部都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得技术手段对互联网的使用进行管理和控制。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，给组织带来法律风险。

缺乏管理的互联网已经给所有的用户敲响了警钟，应对互联网工作、生活时代的管理要求，您准备好了没有？

2. 制定互联网应用的管理策略

为消除或减小使用互联网为企业带来的负面印象，需要制定组织内互联网应用安全使用政策。保证企业的网络是健康的, 安全的, 有效率的。从管理策略上可以从以下几个方面入手。

- 哪些人可以访问互联网.

纵向管理体制：按照部门划分，企业可以规定某些部门的员工可以访问互联网，例如人事部门、市场部门、销售部门等；而另外一些与互联网无关的部门，例如财务部门，不允许在企业内部访问互联网。横向管理体制：按照级别划分，总裁和高级经理可能需要更高的访问权限和更少的控制，普通员工可能受到更多的监控。

- 哪些互联网内容是严格禁止访问的.

企业员工使用互联网处理个人事务也是正常的情况, 有些时候也很难严格区分个人事务与企业事务之间区别. 但有些互联网内容是应该严格禁止从企业内部访问的，包括成人/色情，反动/暴力，黑客/破解等内容。企业管理者需要知道什么人在什么时候访问了什么网站，或者在浏览的同时就进行警告和阻止。

- 哪些互联网内容是严格禁止访问由企业内部对外传播的.

这里涉及到企业信息安全甚至法律安全的问题, 比如员工通过邮件或即时通讯软件发送了涉及企业机密的文件, 或者通过网站发布了触犯法律的言论, 都应该受到严密的控制和严格禁止。

- 如果这些政策被触犯将有什么后果？

如果这些政策被触犯，管理者应该有一份详尽的报表，了解谁在什么时间触犯了什么规则。管理者有权在触发的同时就进行阻止，也可以在事后进行警告和处理。

从技术手段上来说，应该从事前，事中，事后三个不同的阶段来进行管理和控制，方法如下图所示：

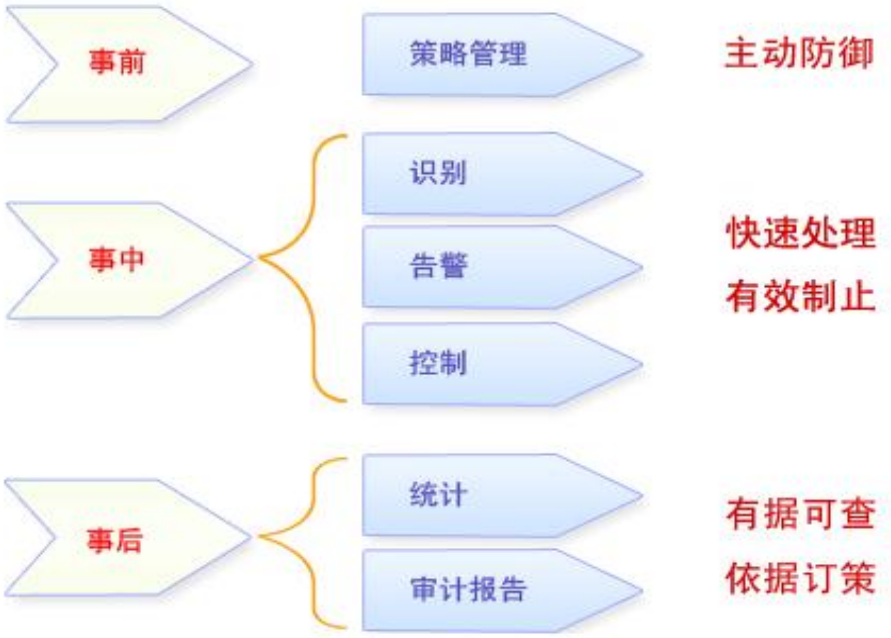


图 1 互联网应用安全的管理策略

3. 互联网应用安全管理系统

为了保证上述相关互联网上网安全管理的政策的实施，还需要技术手段和产品来保证这些政策的实施和执行。

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，能够有效防护来自互联网的攻击，然而对于组织内部员工上网的行为不当而引起的上述安全和管理隐患却无能为力。

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手段实现，必须使用能够识别并管理网络应用的特定管理设备来实现。简而言之，就是“互联网应用安全管理网关”来对基于员工和网络应用内容的访问行为进行管理，管理主要体现在：

- ✓ 组织内部谁在使用上网网络应用（哪个部门，哪个员工）。
- ✓ 使用网络应用的时间（工作日/周末，上班时间/休息时间等）。
- ✓ 访问了哪些外部网络资源（网站，下载文件，发送邮件，聊天，游戏等）。
- ✓ 占用的带宽和流量情况如何。
- ✓ 是否有敏感的信息内容和有威胁的内容。
- ✓ 管理互联网访问不仅仅是阻止对特定网站的访问，而是要针对企业和组织的实际情况制定灵活的访问策略。

互联网应用安全管理网关帮助一个组织基于用户，时间，应用，行为，带宽等要素对组织的互联网上网管理从“通信安全”提升到了“应用安全”，将“被动响应管理”提升到了“主动预警管理”，使企业内外兼修，将防犯管理提升为控制管理，弥补了防火墙等传统安全设备重外不重内、对上网行为缺乏有效管理的不足，带来了全面而细致的互联网行为管理解决方案。

4. NC-ASG 的管理能力

NC-ASG 作为一款专业的互联网上网应用安全管理工具，是面向企业用户的软硬一体化的互联网应用安全管理网关，强大的网页过滤功能，屏蔽员工对非法网站的访问；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，以及无节制的网络聊天，从而保障工作效率；提供对电子邮件（包括 webmail）,即时通讯，BBS 发贴等途径的外发信息的监控审计，避免企业机密信息泄露；此外，NC-ASG ™还具有对系统应用层的带宽管理，有效阻止，限制 P2P 等严重消耗带宽的应用，确保组织的核心业务的带宽得以保障。

NC-ASG 采用循环式的管理方法,使得企业的互联网环境得到全面的改善。

图 2 NC-ASG 的循环管理方式

环境的改善体现在以下几个方面

✓ **工作效率的全面提升**

NC-ASG 上网行为管理设备不仅可以对员工访问 Web、Ftp、Mail 等常用服务的内容进行控制，更可以对 QQ、BT、MSN、Skype 等各种 P2P 软件的行为进行限制和控制。同时，NC-ASG 提供了一套人性化的时间管理策略，管理员可根据业务情况为各部门和个人分配合理的上网时间，并可针对不同时间指定不同的互联网访问权限，有效地提高了组织的工作效率。

✓ **网络带宽的全面优化**

通过网络流量智能分析技术，管理员可以为不同部门和不同应用分配指定的带宽，不仅解决了各类 P2P 软件对带宽的占用，还进一步完善了网络资源的管理。

✓ **保护信息资产，规避法律风险**

作为专业的上网行为管理产品，NC-ASG 对内网发送至互联网的所有信息都可进行全面的记录与保存。除了常见的 URL 记录、FTP 上传下载、BBS 发帖等应用外，对于 IM 软件和 Webmail，通过先进的同步侦听技术，实现对聊天内容及 webmail 内容进行监控和记录。

✓ **技术优势**

更彻底的 P2P 封堵：基于对网络应用协议的特征和行为的分析和流量检测，NC-ASG 可以彻底封堵各类 P2P 软件，并可对 P2P 软件进行基于用户的流量控制，使得不同的用户获得不同的网络带宽。

5. NC-ASG 的产品特点

5.1 精细化的管理手段

- ✓ 渗透力：监控所有互联网络应用行为。
- ✓ 粒度化：可以监控层次极低的函数。
- ✓ 整合性：收集的所有指标将被发送到支持整合视图的同一逻辑中。
- ✓ 恒定：一周 7 天，一天 24 小实时显示：近乎实时显示选定指标的图表。
- ✓ 报告：生成的指标活动报告。这通常包括一系列固定报告和自定义报告，并能导出数据供用户在别处使用。
- ✓ 历史：监控的资源指标将持久化存储在一个专有数据库中，因此可以查看、比较和报告历史数据。包含原始或汇总指标的历史数据库，从而能够查看特定时间范围内的图表和报告。

- ✓ 报警：将收集指标确定的具体条件通知相关个体或组的功能。典型的报警方法是电子邮件和某种类型的自定义钩子接口，可以允许运营小组将事件传播给事件处理系统。
- ✓ 高效：性能数据收集不会对监控目标造成不利影响。
- ✓ 实时：可以实时显示、报告和警告监控的资源指标。
- ✓ Bypass: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。

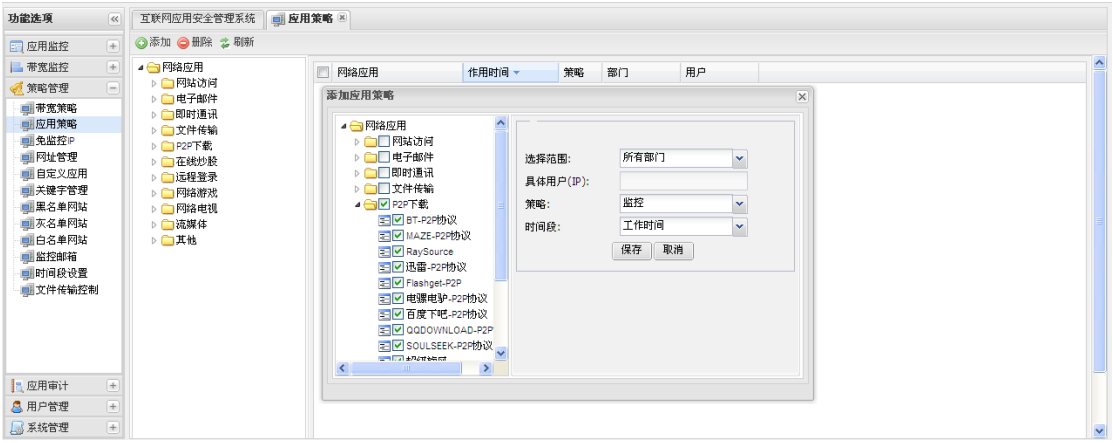


图 3 NC-ASG 的策略管理控制台

5.2 操作简单，界面美观清晰，运行稳定可靠，确保网络畅通

- ✓ 软硬件一体设备，易于安装部署和管理。
- ✓ 多种接入方式，网关（串联）/网桥（（串联）/旁路（并联）方式接入网，无缝接入用户现有的网络。
- ✓ 强化的系统架构，优化的控制引擎，专用的操作系统，更安全，更稳定。

- ✓ 新型基于 Web 的富客户端操作界面，结构清晰，美观大方，轻松使用，轻松管理。
- ✓ 全面支持软、硬件方式的 Bypass 支持，避免造成单点故障。

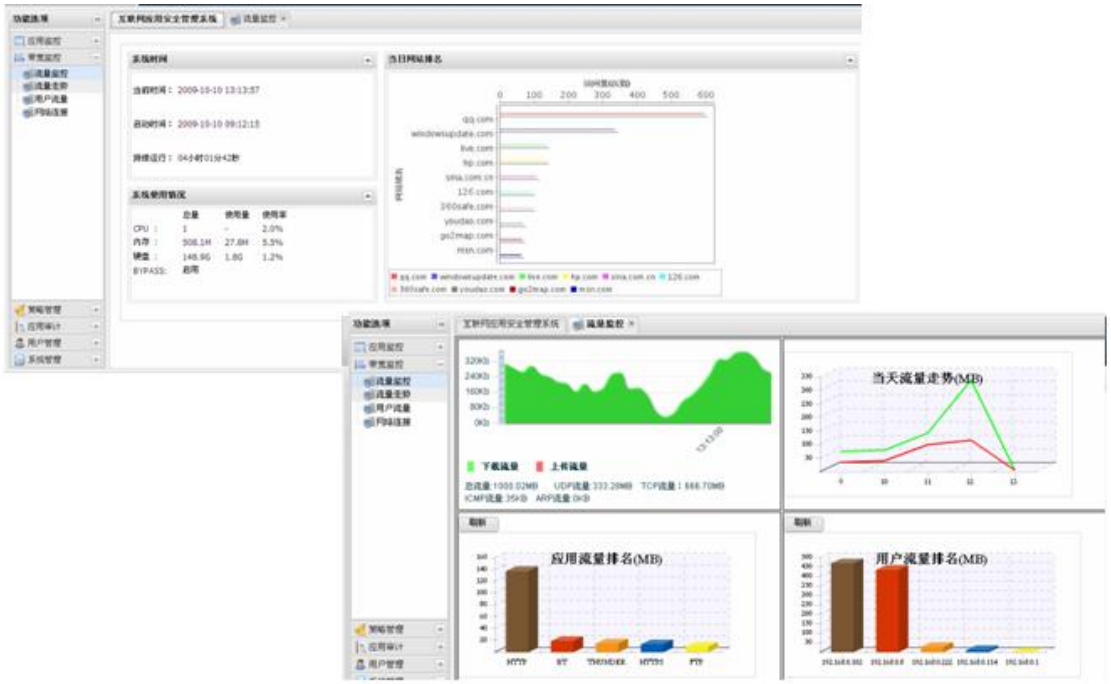


图 4 NC-ASG 的管理界面

5.3 管理全面、控制准确、更新及时

- ✓ DPI(深度报文检测)技术的高效内容分析引擎，择时组包。
- ✓ 基于智能流分析分层 QoS 机制，通过统一的策略控制，实现“基于用户和基于业务”的智能流量管理. 从而能够灵活的应用带宽分配管理，实时应用流量监控统计。
- ✓ 完善、准确，及时更新的 URL 网页过滤数据库：90 多种分类，即时更新。
- ✓ 全面基于应用特征和行为特征的网络应用识别和分析，多达 200 种流行网络应用。

- ✓ 完善、准确、及时更新的互联网应用协议控制数据库。
- ✓ 提供实时、快捷的数据更新，快速响应服务。
- ✓ 全面、直观的外发信息监控，有效防止保密数据的外泄。

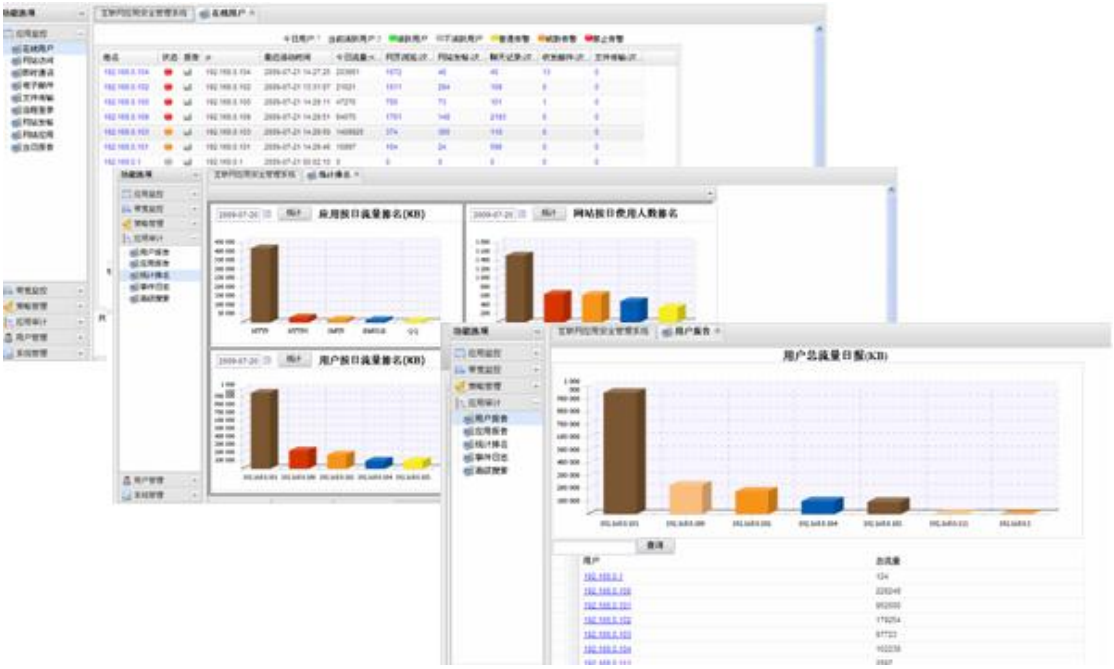


图 5 NC-ASG 的监控功能

5.4 强大的查询统计和报告分析

- ✓ 多达 100 余种的统计分析报告，及排名报告。
- ✓ 多维度，细粒度的高级查询搜索功能，提供更全面的审计。
- ✓ 分门别类的在线活动记录，清晰、直观的日志跟踪。
- ✓ Drill-down 方式的记录查询、统计、报表一体化功能。

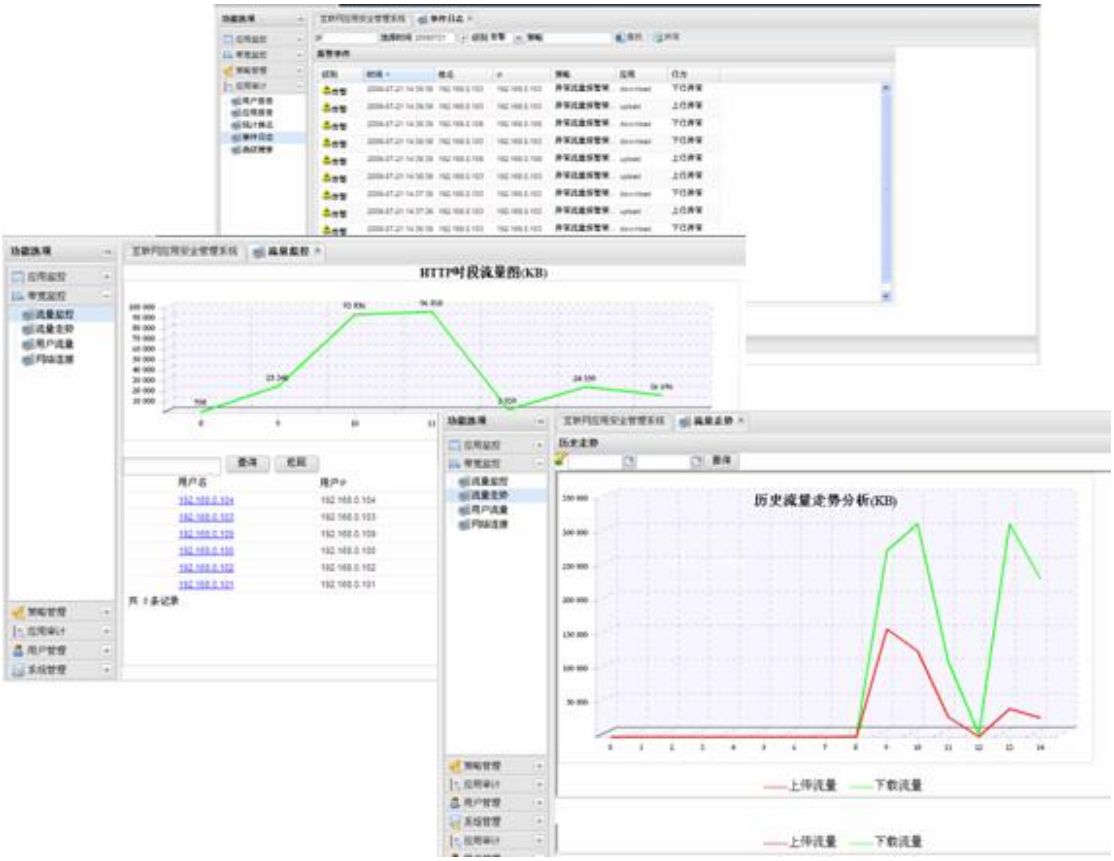


图 6 NC-ASG 的统计查询功能

5.5 精细的策略管理

- ✓ 支持基于用户、时间段的策略定制。
- ✓ 支持基于应用(协议)的带宽通道分配。
- ✓ 智能识别新协议，进行带宽管理与流量统计。
- ✓ 支持基于内容分类的 URL 访问控制。
- ✓ 支持基于 URL 关键字的正则表达式匹配过滤。
- ✓ 支持自定义 URL 分类，以及黑名单设置。
- ✓ 支持自定义策略提示页面。

- ✓ 支持基于用户组、用户的应用控制，如允许或禁止某人使用某种应用。
- ✓ 支持基于时间段的应用控制，如允许或禁止某时间段使用某种应用。
- ✓ 支持对 IM 即时通讯应用的控制，如：QQ、MSN、SKYPE、PHONE 等。
- ✓ 允许或禁止使用某种即时通讯工具。
- ✓ 记录某种即时通讯工具的聊天内容，如 MSN 等。
- ✓ 允许或禁止通过某种即时通讯工具传输文件。
- ✓ 允许或禁止通过某种即时通讯工具进行音视频。
- ✓ 支持对 P2P 应用的控制，如：迅雷、PP 点点通、BT、百度下吧、电驴、soulseek 等。
- ✓ 支持对网络电视的控制，如新浪 TV、搜狐 TV、PPLIVE、费点等。
- ✓ 支持对流媒体协议的控制，如 MMS、RTSP、QQ 直播、UUsee、暴风影音、PPstream 等。
- ✓ 支持对在线网络游戏的控制，如帝国时代、联众游戏、魔兽世界、征途、热血江湖、浩方游戏、传奇、泡泡堂等。
- ✓ 支持对在线炒股软件的控制，如和讯股道、平安证券、证券之星、大智慧、大福星、投资通、同花顺等。
- ✓ 支持对 FTP、Telnet 等协议的控制。
- ✓ 支持应用(协议)自定义，并对其进行控制。
- ✓ 支持对外发邮件的专项监控设置，如指定用户、收发件人、主题、附件大小等。

- ✓ 支持对外发 Webmail 的专项监控设置，如指定邮件服务提供商、收发件人、主题、附件等。

- ✓ 支持对外发帖子的专项监控设置，并支持基于关键字的过滤和 Email 报警。

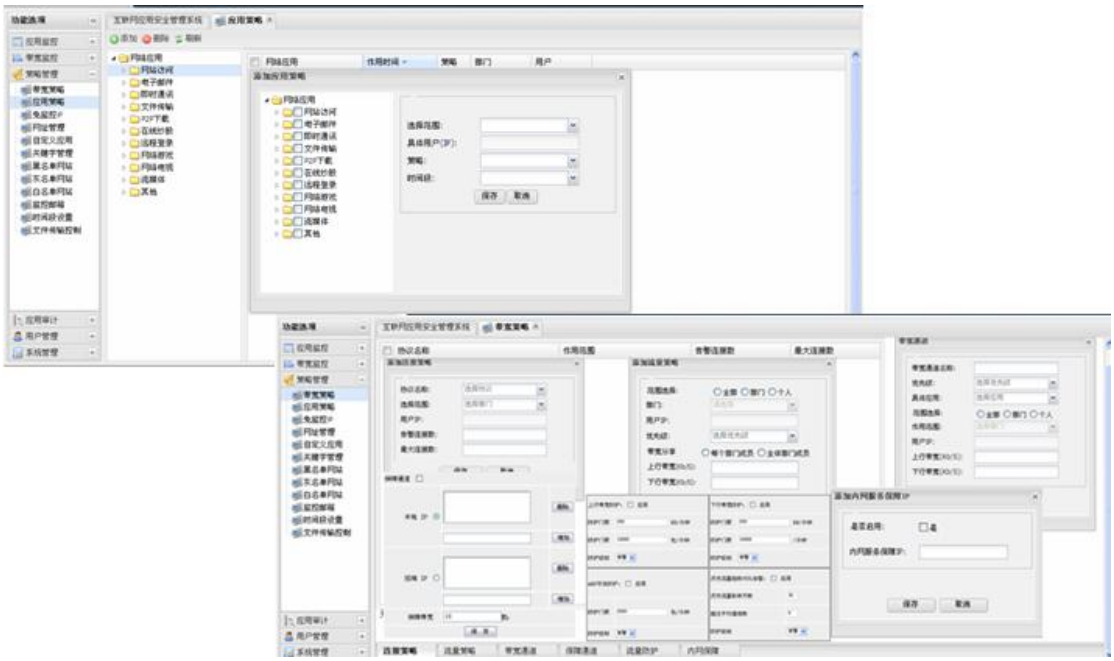


图 7 NC-ASG 的应用策略管理示意图

6. NC-ASG 产品功能介绍

NC-ASG 作为一种网络工具、上网行为管理工具、内容审计工具三种工具于一体的网络产品弥补了防火墙等传统安全设备重外不重内、对上网应用及行为缺乏有效管理的不足，其包含应用识别，应用报警，访问控制、内容监控、安全审计、带宽流量管理及应用行为分析，统计等多个功能。

6.1 网络工具

提供对 NC-ASG 所管理的网络环境中的网络应用、总流量、用户流量、网络连接状态进行监控分析及网络诊断，对应用的异常情况提供报警，并设置相应的带宽策略。

6.1.1 带宽监控

提供对 NC-ASG 所管理的网络环境中的网络带宽使用情况的实时监控和统计分析,包括

- ✓ 流量监控：监控网络的实时的流量情况，带宽监控图、当天流量走势图、当日应用流量排名图及当日用户流量排名图；同时，当日应用流量排名图和当日用户流量排名图提供继续向下钻取能力。

图 8 NC-ASG 系统控制台流量监控窗口

- ➢ 实时流量对比：分析任意 5 个用户针对 5 种应用的流量。

图 9 NC-ASG 系统控制台实时流量对比窗口

- 流量走势：分析当日及历史的流量趋势。
- 用户流量：实时监视每台上网机器的即时流量、上传/下载流量、当前 UDP/TCP 连接数，及时发现当前网络中的异常流量和连接数。
- 网络连接：监控网络全部的 TCP/UDP 连接的源端口和目的端口、时间戳，实时检查某个 IP 的全部连接的连接状态，及时发现异常连接。

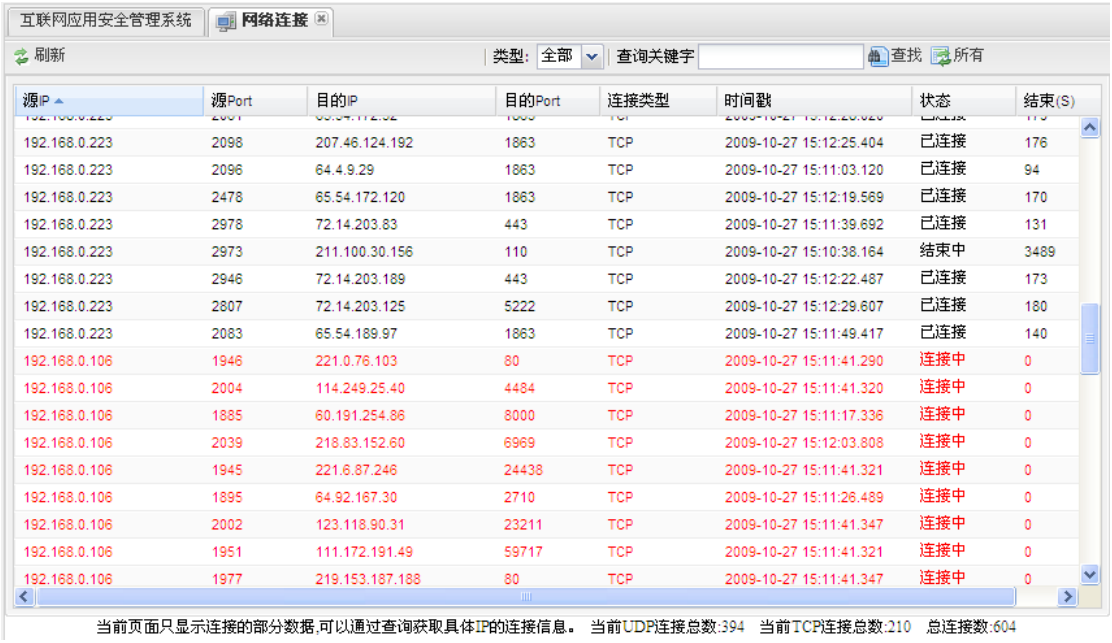


图 9 NC-ASG 系统控制台网络连接窗口

- 网络诊断：通过多角度统计为管理人员提供了一个实用的检查工具，通过它管理人员可以很直观的查看目前网络运行情况，并可以锁定流量异常的 IP。

图 10 NC-ASG 系统控制台网络诊断窗口

- 网络工具：提供 IP/MAC 转换查询、PING 命令、Tracepath 命令、CURL 命令和 NSLOOKUP 命令以及抓包工具和网络地址转换功能。

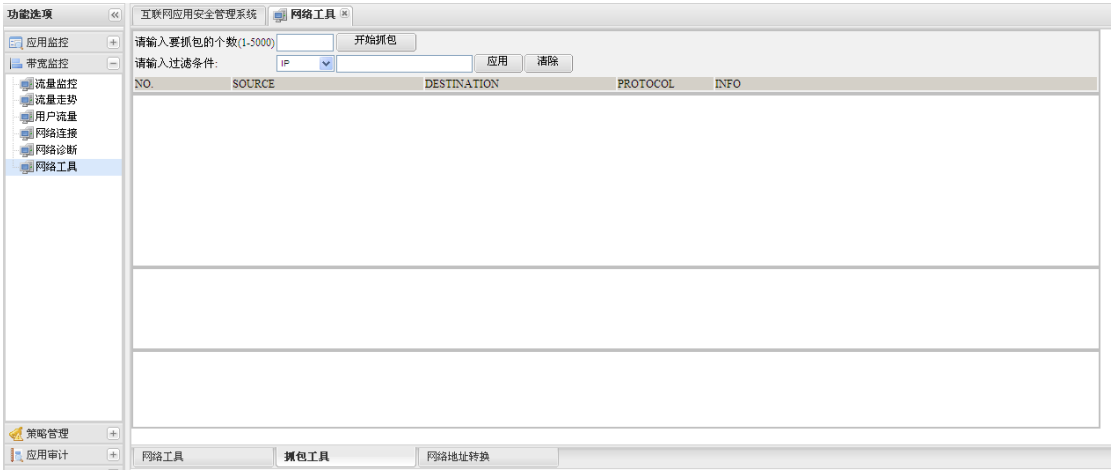


图 11 NC-ASG 系统控制台网络工具窗口

6.1.2 策略管理

提供对 NC-ASG 所管理的网络环境中的各种网络应用的安全策略配置和管理。

- ✓ 带宽策略:对各种协议（TCP、UDP）的控制策略，用户可以通过带宽策略限制某个用户或者多个用户、某个部门或者多个部门的带宽流量和连接数，并提供相应的报警机制。带宽策略又分连接策略、流量策略、带宽通道、保障带宽、流量防护和内网保障。

图 12 NC-ASG 系统控制台带宽策略窗口

6.1.3 应用监控

提供对 NC-ASG 所管理的网络环境中的各种网络应用的实时监控和查询，例如：可以查看带宽监控中发现的占大量带宽或异常流量/连接数的用户的网络应用，进而判断某个用户是否中了蠕虫等病毒。还可以对违反策略的用户提供报警。

✓ 在线用户：可以递进式对用户的互联网应用和流量进行统计分析。

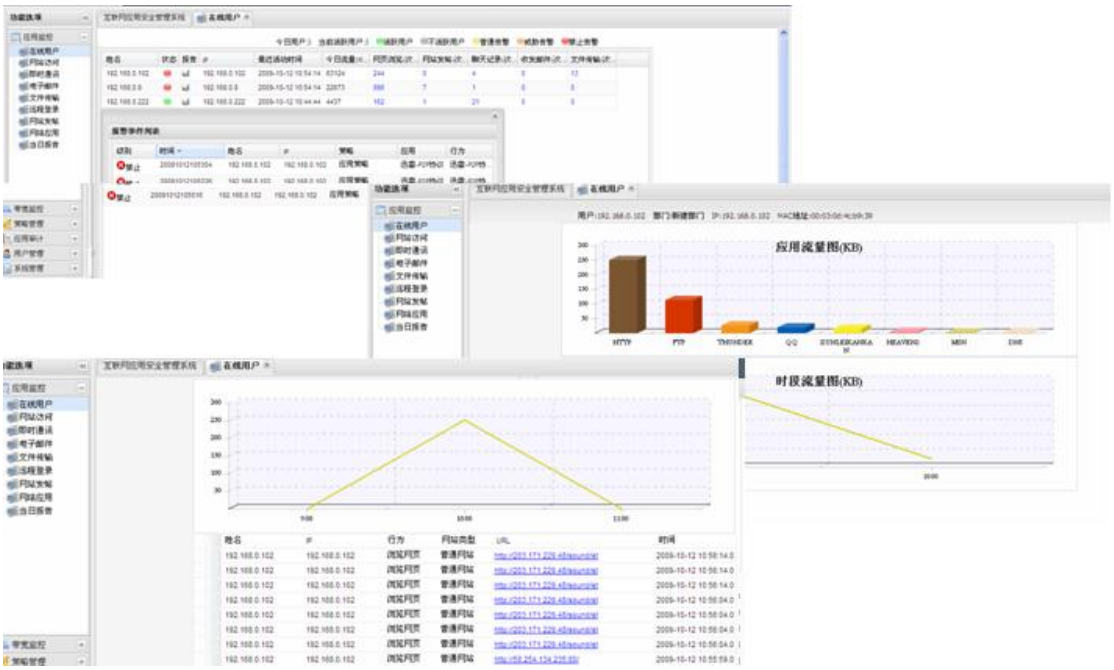


图 13 NC-ASG 的在线用户的实时监控页面

✓ 网络应用

显示用户在网络中的行为，包括 http 应用和 qq 应用等，以及应用的使用次数和流量大小。

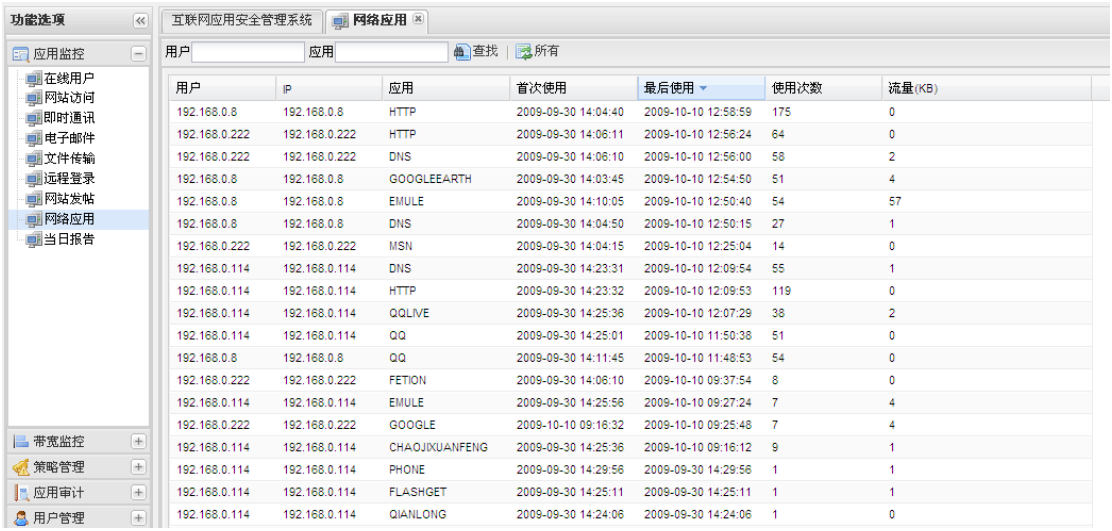


图 14 NC-ASG 系统控制台应用监控网络应用窗口

6.2 管理工具

利用准入管理、终端分组、网络诊断、应用监控及策略设置对 NC-ASG 所管理的网络环境中的用户或 IP 进行合理管控。

6.2.1 用户管理

NC-ASG 使用 IP 地址作为用户的唯一标记，同时可以自动记录 MAC 地址，管理员通过用户管理可以设置用户姓名、计算机名称，所属部门等信息，以方便管理工作。用户管理分为终端分组，终端管理，准入配置，本地账户分组，用户 IP 地址与 MAC 地址绑定、本地账户管理和锁定 IP 管理。

✓ 准入配置：对用户做认证配置，用户必须通过安全认证才可以在限定的时间内访问网络。从根本上提高了组织内网用户计算机的安全性，减少了内网用户感染蠕虫、病毒、木马以及间谍软件的风险。目前支

持的认证有 4 种，分别是 AD 认证，本地认证，LDAP 认证和 RADIUS 认证。

图 15　NC-ASG 系统控制台用户管理准入配置认证管理页面

✓ 终端分组：可以对企业内部各部门人员进行划分，更好的管理用户。

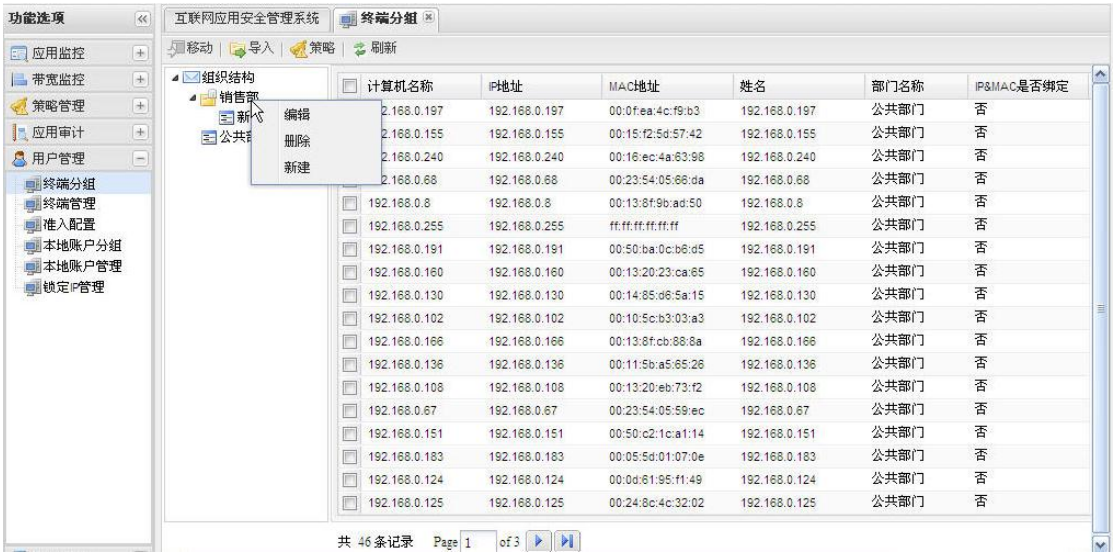


图 16　NC-ASG 系统控制台用户管理组织结构设置窗口

6.2.2 策略管理

通过设置网络应用策略、免监控 IP、网址管理、黑/灰/白名单、管理时间段对 NC-ASG 所管理的网络环境中的用户或 IP 进行合理管控。

✓ 应用策略:指定用户使用网络应用的策略，实现告警或禁止。

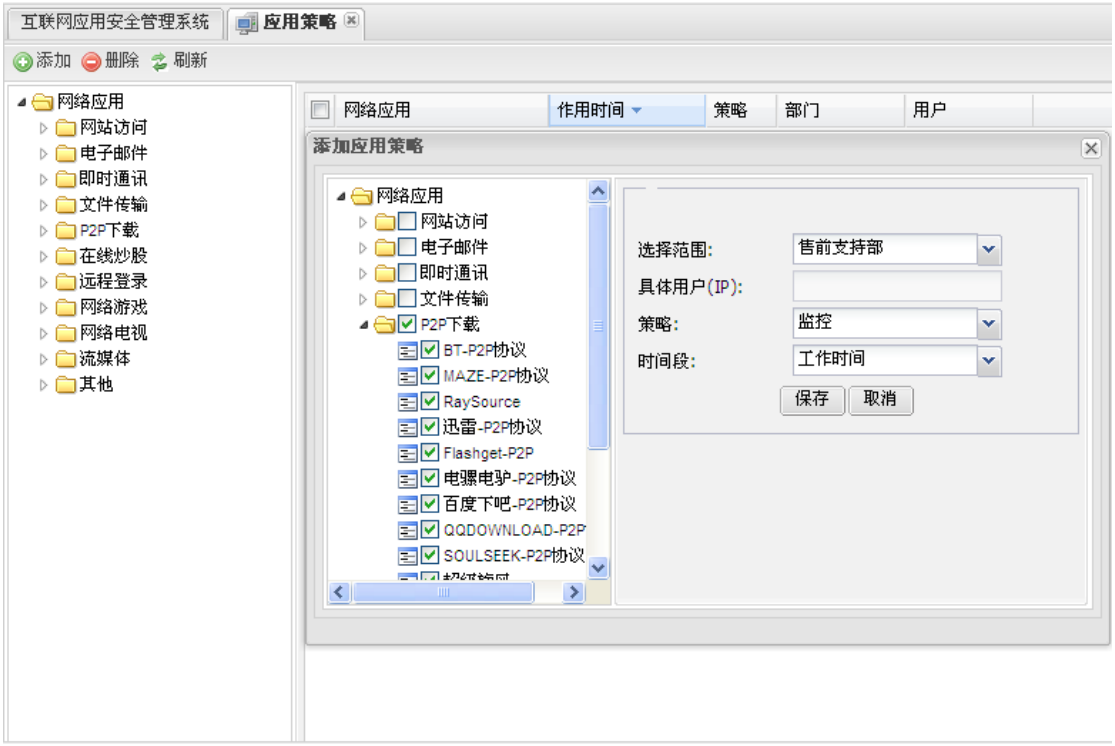


图 17 NC-ASG 系统控制台应用策略添加窗口

- ✓ 免监控 IP:可以设置某些不需要监控的 IP 地址,如网关设备,领导 IP 等。
- ✓ 网址管理:支持用户自己增加新的网址,提供网址库的查询功能。
- ✓ 时间段设置：为一种或多种策略设置作用时间段。
- ✓ 黑名单网站：管理非法的站点，对这些站点实行屏蔽。当网络使用者访问了非法的站点时，就会自动跳转到设置的网址，保护局域网的安全。为了有效的防止一些网站采取自动更换域名的方式来逃避系统识别，因此黑名单过滤采用域名模糊匹配，即：只要在域名中包含黑名单设置的关键字设置，此域名就会被系统屏蔽。
- ✓ 灰名单网站：允许用户在特定的时间内访问某些网站。

- ✓ 分布部署集中管理：集中监控分布部署 NC 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；收集用户日志，统揽全局，综合分析。

6.2.3 应用监控

提供对 NC-ASG 所管理的网络环境中的各种网络应用的实时监控和查询，并对应用的异常情况提供报警。

- ✓ 在线用户：支持在线用户状态（在线用户、不活跃用户、普通告警、威胁告警、禁止告警）的实时监控，对违反策略的用户进行报警提示。

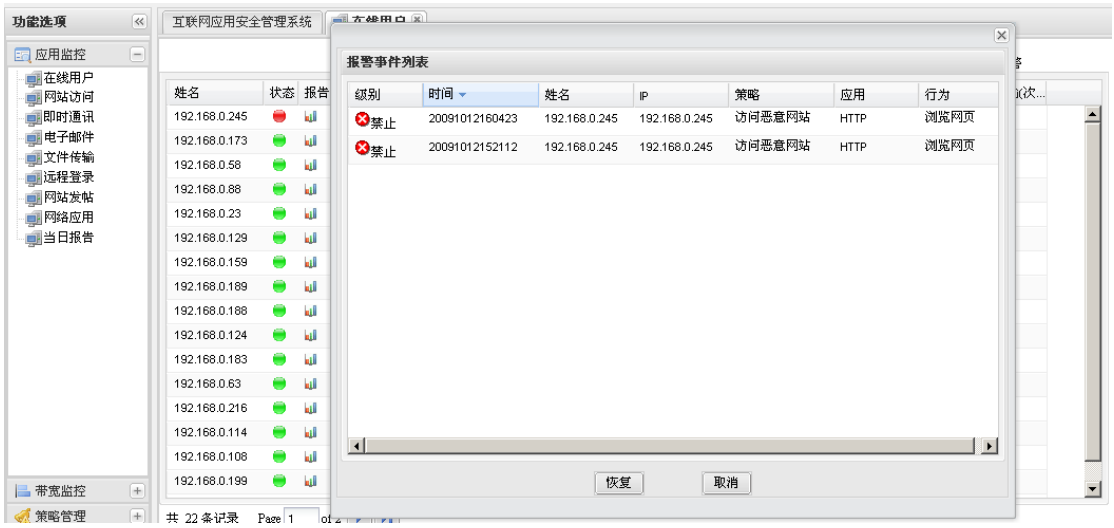


图 18 NC-ASG 系统控制台在线用户的报警窗口

6.3 内容审计工具

提供对 NC-ASG 所管理的网络环境中的各种网络应用的历史数据的查询，统计，审计，并将审计结果用各种报表的形式体现。

6.3.1 应用监控

对各种网络应用进行监控，对涉及用户隐私的内容进行选择性监控。

✓ 网站访问

- 监控上网网站的 URL
- 多种过滤库：过滤色情/暴力/游戏/股票/聊天/BBS，以及自定义过滤关键词等等
- 上网时间的控制：合理规定并控制不同机器的上网时间
- 过滤自定义端口、IP 等等
- 下载过滤：可对文件下载的类型进行控制。

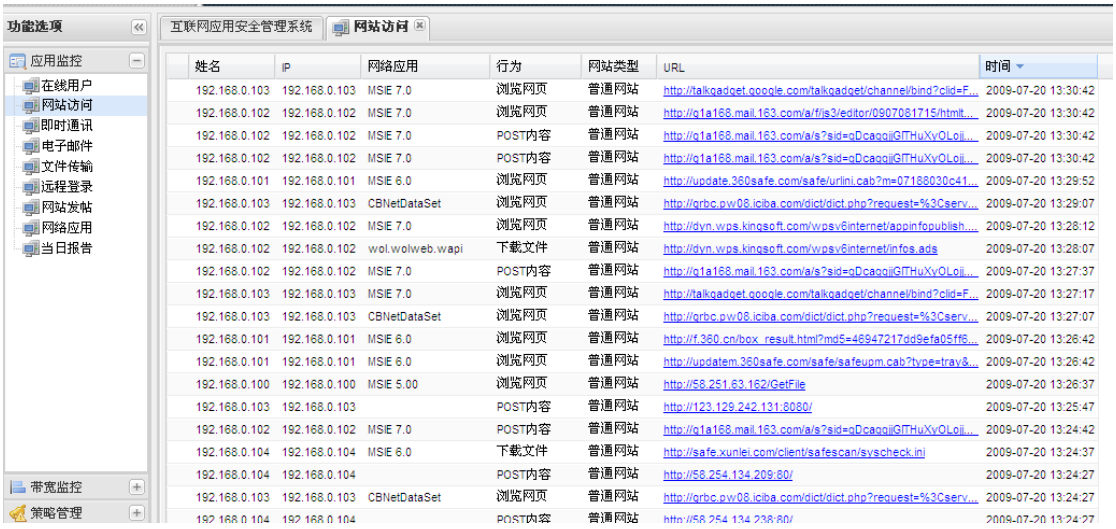


图 19 NC-ASG 系统控制台应用监控网站访问窗口

✓ 即时通讯

监控 QQ（MSN/ICQ）等聊天工具的类型，登录时间，选择性查看聊天内容，信息发送接收的时间，以及通过聊天工具传输的文件。

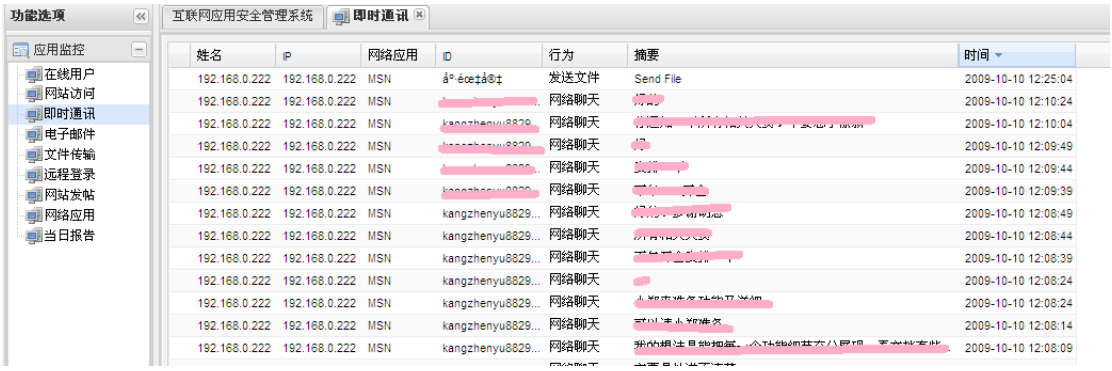


图 20 NC-ASG 系统控制台应用监控即时通讯窗口

✓ 电子邮件

显示用户收发邮件的行为和发件人收件人的 mail 地址和邮件的主题。

图 21 NC-ASG 系统控制台应用监控电子邮件窗口

✓ 文件传输

显示用户上传下载的行为，和所上传下载的文件的文件名。

图 22 NC-ASG 系统控制台应用监控文件传输窗口

✓ 远程登录

监控所有使用 telnet,SSH 等协议远程登录的网络应用。

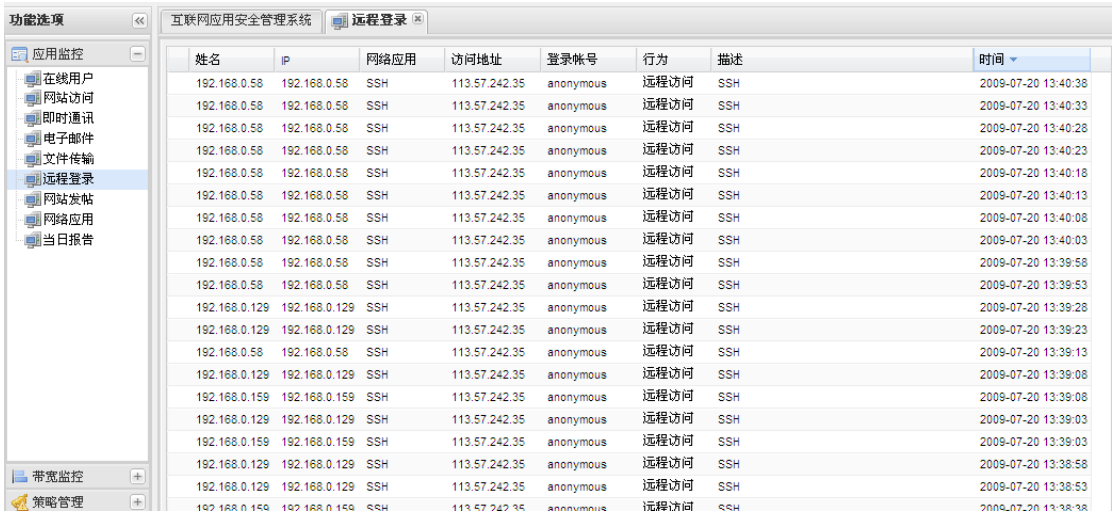


图 23 NC-ASG 系统控制台应用监控远程登录窗口

✓ 网站发帖

显示用户在网页中发表的信息，包括发表网站的 url，信息发表的时间和大小。

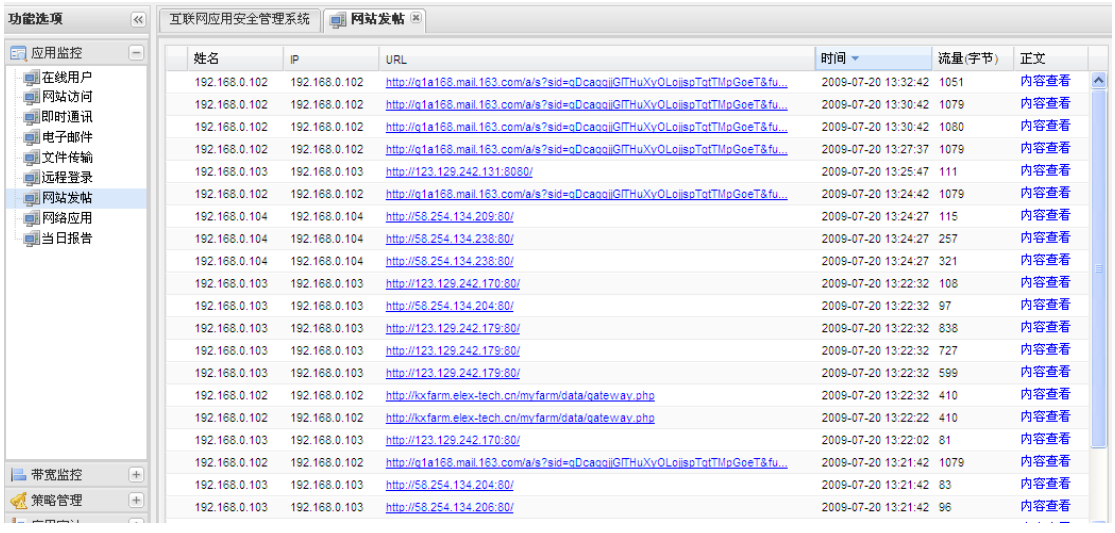


图 24 NC-ASG 系统控制台应用监控网站发帖窗口

- ✓ 当日报告：显示当日网络的初步统计情况，包括各应用使用人数的情况，和各种应用流量的报告，可以递进式对用户互联网应用和流量进行统计分析。

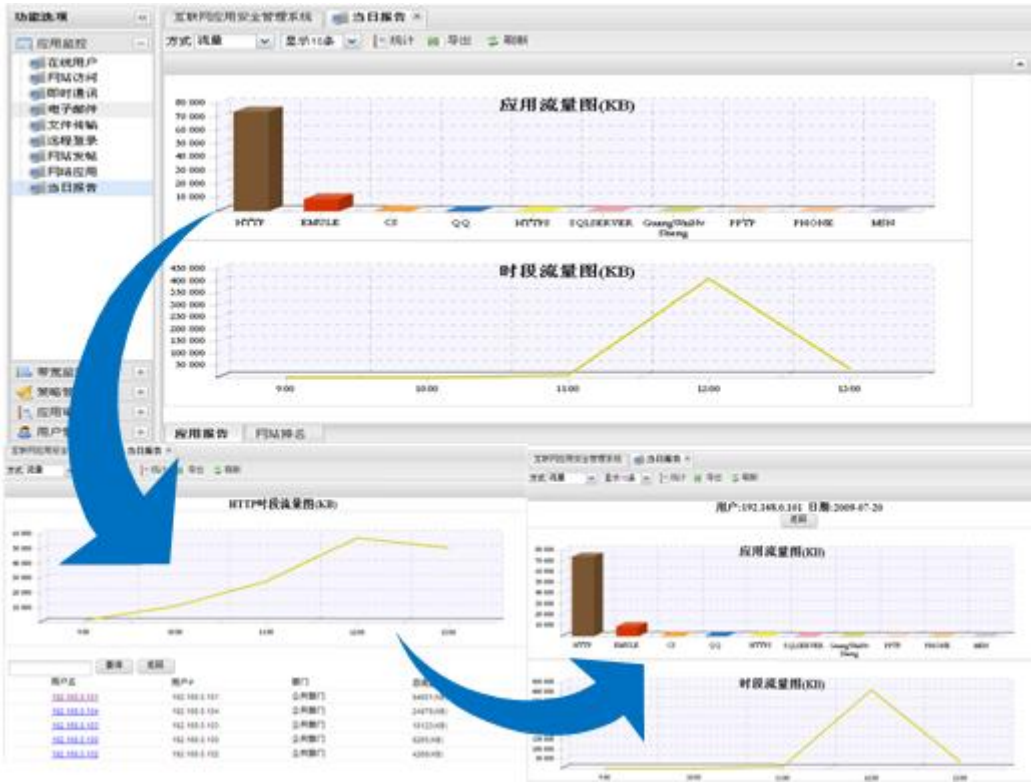


图 25 NC-ASG 系统控制台应用监控当日报告窗口

6.3.2 策略管理

设置相应的策略对网页、邮件、发帖等内容中涉及的涉密、非法、色情等关键字进行监控以及对特定的邮箱、传输的文件进行监控。

- ✓ 关键字管理:设置威胁或告警的关键字。
- ✓ 监控邮箱:提供邮箱的过滤功能，对指定的这些邮箱实行监控和屏蔽，阻止用户和这些邮箱的邮件收发操作。
- ✓ 文件传输控制:定义文件传输中的关键字,设置相关的策略。

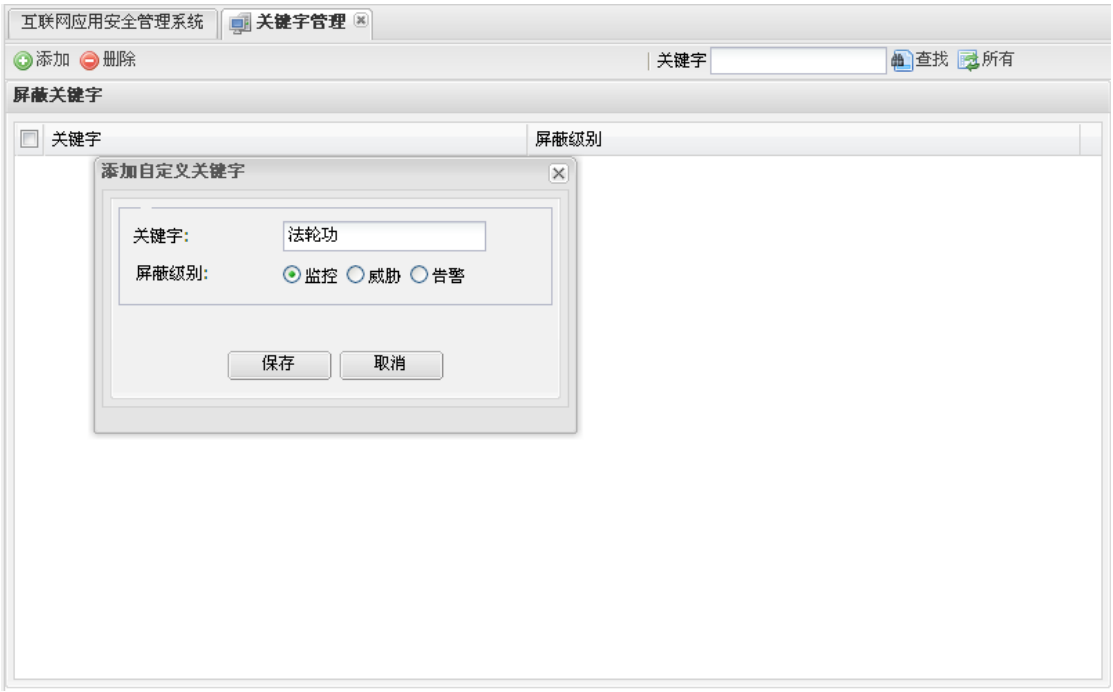


图 26 NC-ASG 系统控制台关键字添加窗口

6.3.2 应用审计

提供对 NC-ASG 所管理的网络环境中的各种网络应用的历史数据的查询，统计，审计，并将审计结果用各种报表的形式体现。

- ✓ 用户报告：显示用户的总流量，排名显示。并显示该用户每小时的流量情况，可以递进式对用户互联网应用和流量进行统计分析。

图 27　NC-ASG 系统控制台应用审计用户报告窗口

✓ 应用报告：针对用户所选择时间段内的所有协议，统计各个协议所占用的比例。可以对应用的使用人数和应用的流量分别统计。

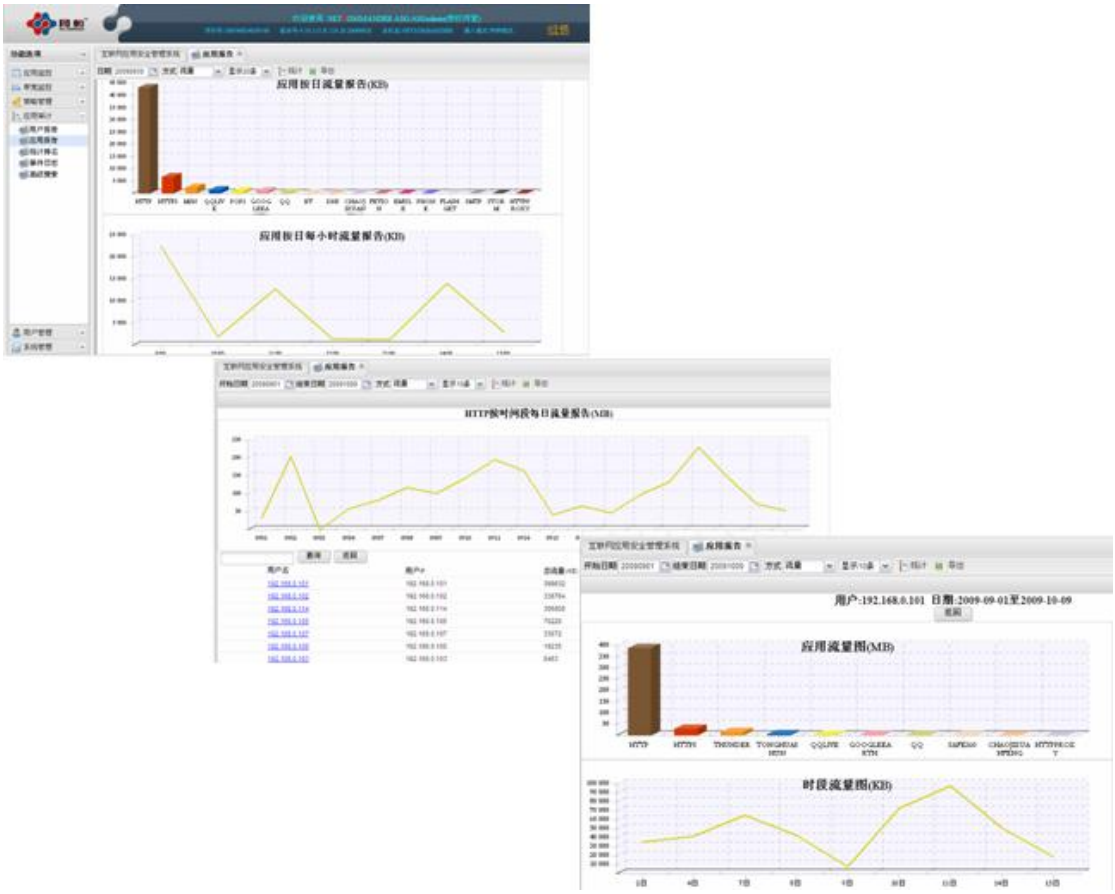


图 28 NC-ASG 系统控制台应用审计应用报告窗口

✓ 应用行为分析报告：对各种应用的流量和使用人数做整体的分析。

图 29 NC-ASG 系统控制台应用行为分析报告窗口

- ✓ HTTP 报告：展现 HTTP 详细分类流量图和时段流量图。
- ✓ 统计排名：统计排名分今日排名、本周排名和本月排名对流量、网站使用人数、用户流量、部门流量进行排名，可以递进式对用户的互联网应用和流量进行统计分析。

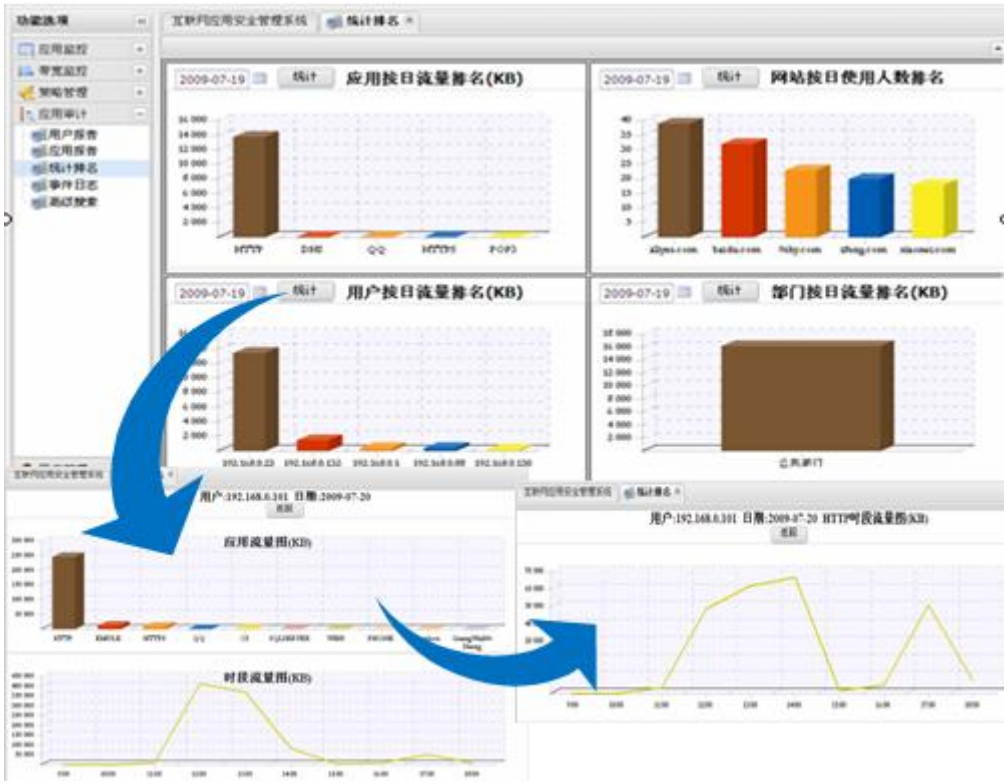


图 30 NC-ASG 系统控制台应用审计排名统计窗口

✓ 事件日志：提供各类告警,威胁和禁止日志的查询，记录用户违规次数并对违规用户的违规次数进行统计排名。

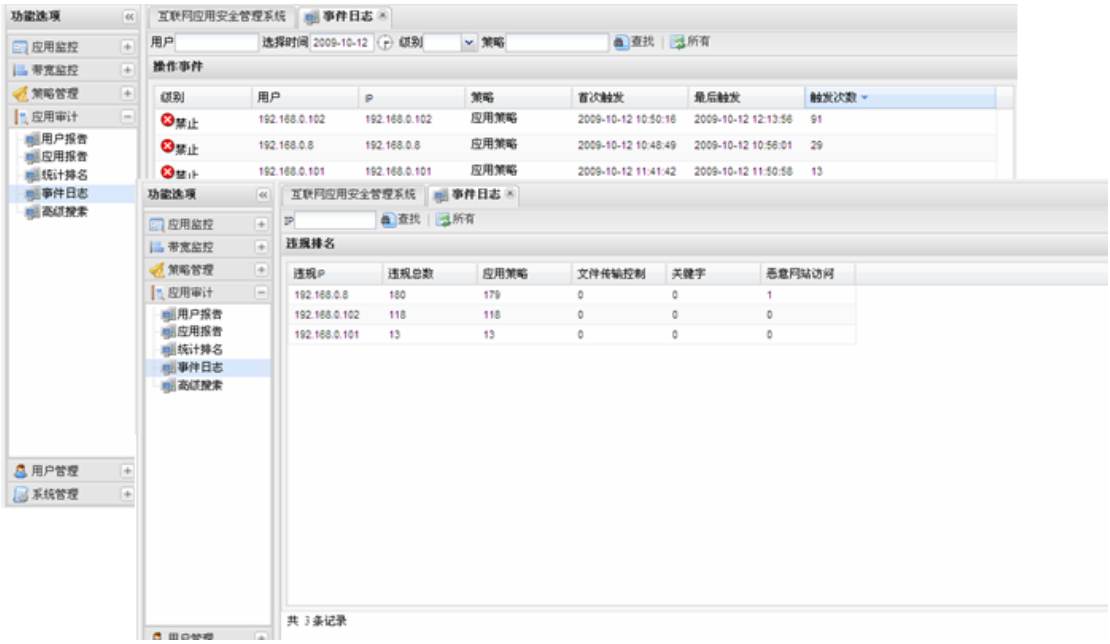


图 31 NC-ASG 系统控制台应用审计事件日志窗口

- ✓ 高级搜索：提供按照用户名，IP 地址,MAC 地址，时间段，网络应用类别，网络应用，网络行为的多维度高级查询功能。

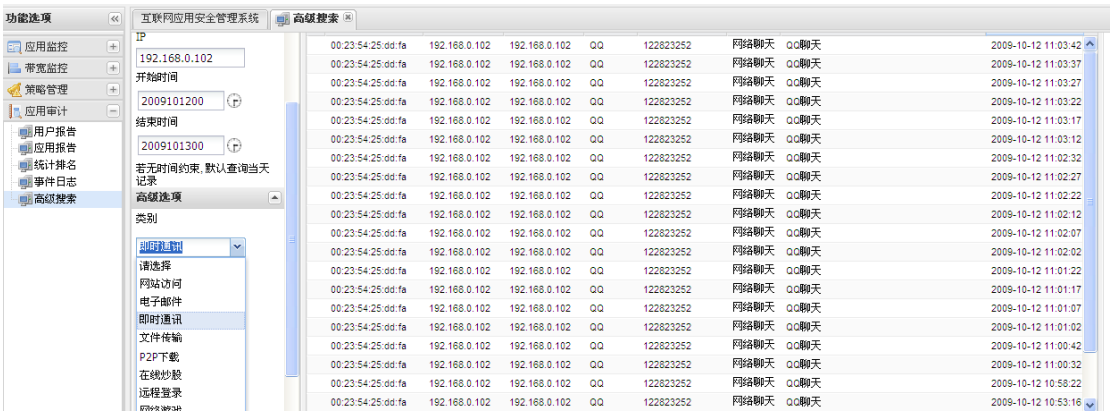


图 32 NC-ASG 系统控制台应用审计高级搜索窗口

7. NC-ASG 部署方式

NC-ASG系统支持多种接入方式，用户可以根据实际需要把设备接入到自己网络中。系统支持的接入方式如下：

- ✓ 旁路模式
- ✓ 网桥模式
- ✓ 网关模式

7.1 旁路模式

旁路模式接入方式对企业网结构影响最小，不需要改变任何路由配置，只需在出口交换机配置端口镜像，然后将NC-ASG的WAN口接入镜像端口即可。

旁路模式适用的网络环境：

- ✓ 企业网出口交换机支持端口镜像。
- ✓ 企业网出口使用集线器（HUB）。

对于大多数的企业网出口部署了交换机，并且可以支持端口镜像，但也有例外。在提出方案之前，需要详细了解客户出口交换机的品牌型号，查阅相关技术文档确认是否支持端口镜像。另外，企业网出口交换机在支持端口镜像的情况下，还必须有可以做端口镜像的空闲端口。对于企业网出口使用集线器的情况，利用数据广播技术，只需一个空闲端口即可。

旁路监听仅仅是一种数据流镜像技术，在数据流控制方面受到制约，部分策略阻断和控制管理功能无法实现。

旁路监听典型网络部署拓扑图如下：

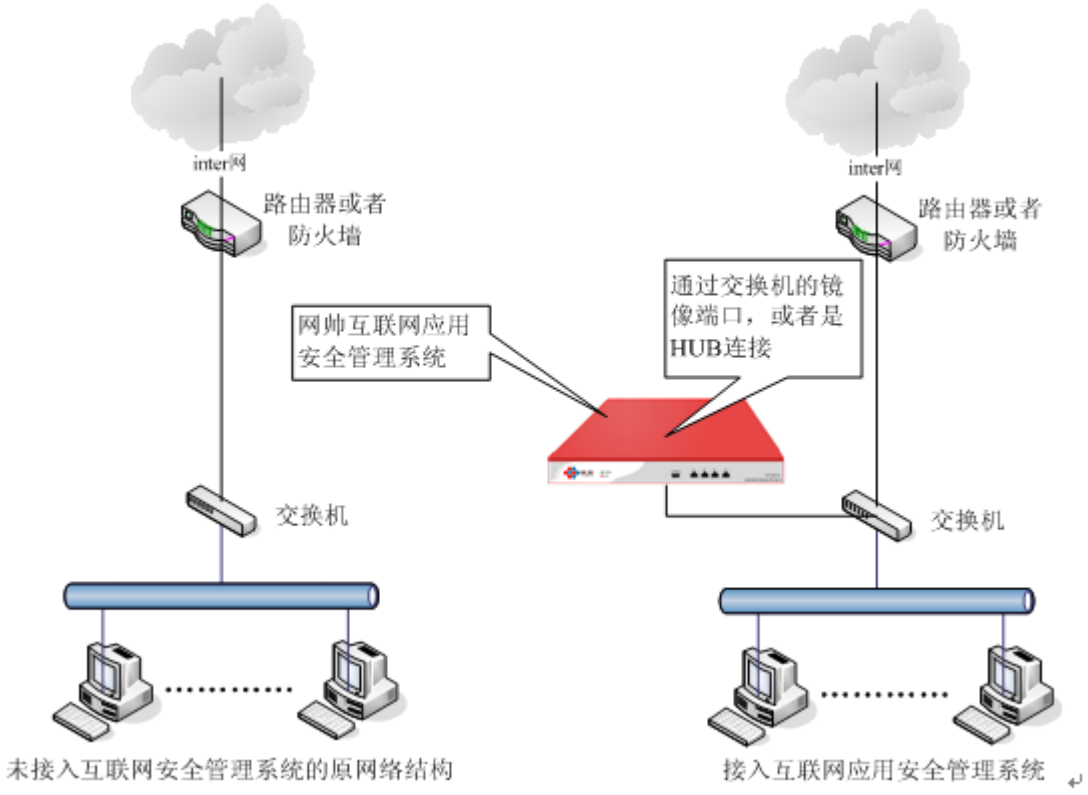


图 33 NC-ASG 旁路模式的网络部署拓扑图

7.2 网桥模式

网桥模式是把互联网安全管理系统视为一条带过滤功能的网线使用，在更改原有网络拓扑结构的情况下启用。将互联网安全管理系统的LAN口接入网络内网的出口，

将互联网安全管理系统的WAN口，接入作为出口的路由器或者防火墙。原网关及内网用户不需做任何配置改变。从NC-ASG 控制台对NC-ASG系统进行配置即可使用。

网桥模式适用的网络环境：

- ✓ 企业网出口交换机无法实现端口镜像。
- ✓ 客户需要严格的带宽管理。
- ✓ 企业网出口已经配置了路由器、防火墙或者 NAT 设备。

网桥模式对原网关及内网用户而言，感觉不到NC-ASG系统的存在，还可以实现对网络数据包的控制。

网桥模式典型网络部署拓扑图如下：

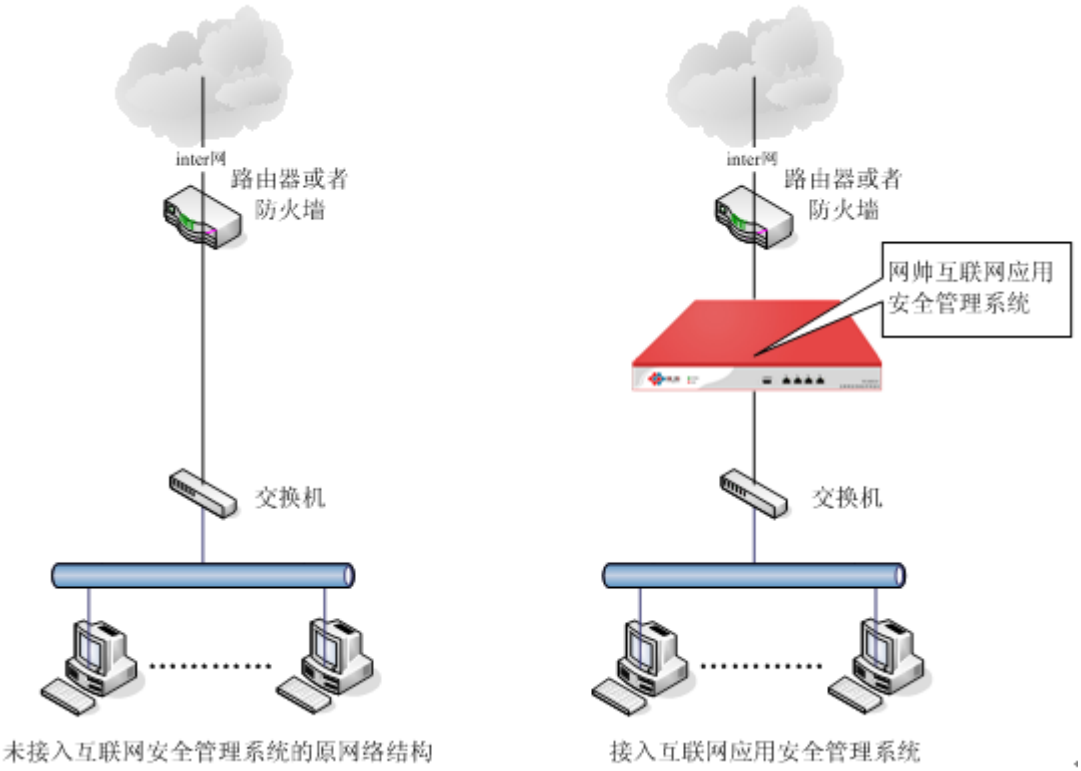


图 34 NC-ASG 网桥模式的网络部署拓扑图

7.3 网关模式

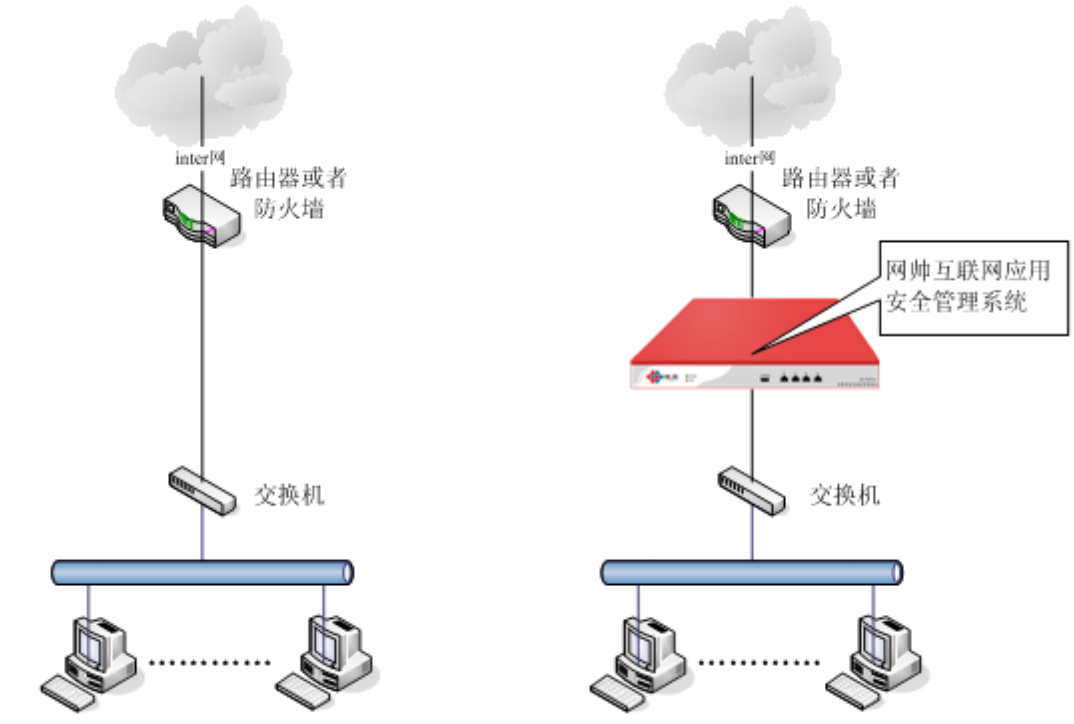
网关模式和网桥模区别是，网关模式的 WAN 口和 LAN 口都有独立的 IP 地址，WAN 口和 LAN 口之间，通过 NAT 转发数据。

网关模式适用的网络环境：

- ✓ 外网 IP 地址资源不足，目前又没有专用的 NAT 设备。
- ✓ 使用 ADSL 拨号技术的企业网出口。
- ✓ 需要隐藏企业网内部网络结构的环境。

网关模式需要将互联网安全管理系统当作一个网关来看带，所以使用网关模式，所有内网用户的网关都必须指定到互联网安全网关的 LAN 口 IP。WAN 口的 IP 设置要和路由器的 IP 在同一网段，要确保 WAN 口到外网的网络通畅。

网关模式典型网络部署拓扑图如下：



未接入互联网安全管理系统的原网络结构　　接入互联网应用安全管理系统

图 35　NC-ASG 网关模式的网络部署拓扑图

7.4 集中管理

网帅产品除了互联网应用安全管理（NC-ASG）产品外，同时还有集中管理平台产品。

对于分布式部署多台上网行为管理产品的集团用户，集中管理平台可以帮助管理员随时了解各分支结构的设备运行状态，统一制定、下发上网行为管理的策略，并定期收集各分支结构用户上网行为日志。集中管理使管理员能够统揽全局、统一设置策略，极大的提高了管理效率。

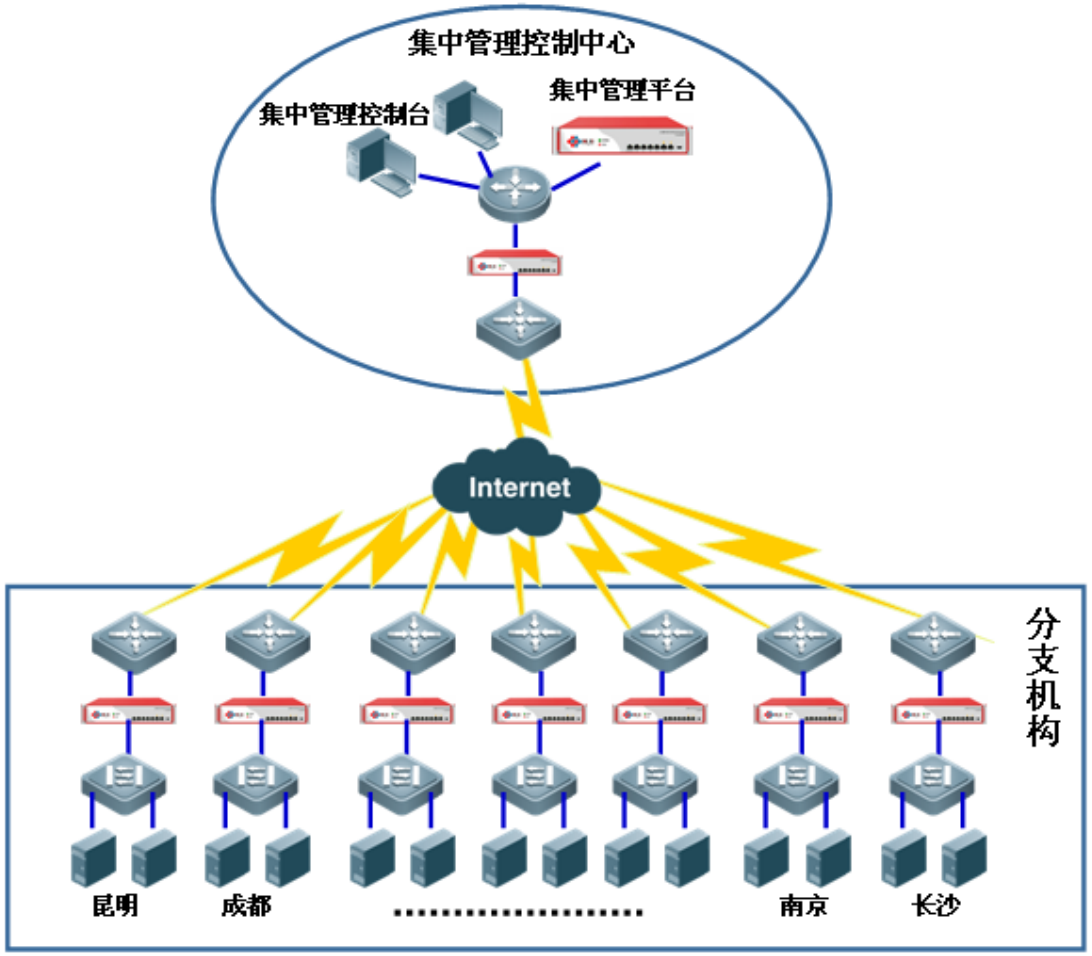


图 36　NC-ASG 集中管理的网络部署拓扑图

8. 资质认证

奕恒佳源软件技术有限公司自成立以来，先后获得了一系列的资质认证，包括软件企业认定证书、计算机软件著作权登记证书、北京软件行业协会团体会员证书、高新技术企业批准证书、公安部销售许可证和公安部检测报告等。

9. 关于我们

北京奕恒佳源软件技术有限公司成立于 2004 年，由来自美国硅谷的精英在北京创立，主要为爱立信，诺基亚，松下电器，中国移动，中国联通等提供电信软件开发，电信 IT 运营及安全服务。

厚积薄发，推出新品。公司针对市场的需要，经过长时间的研发，推出上网行为管理相关产品及服务。依托多年的软件开发经验，汲取国际先进技术，结合中国国情，研发，生产，销售了上网行为管理系列产品（NC-ASG110/30000）。并拥有全部的自主知识产权。

作为‘安全上网的引领者’，网帅的互联网安全管理系统产品先进，行业领先。采用先进的软件架构；拥有丰富、易用的控制策略；独具强大的识别、搜索功能，以及备有详尽、周密的统计报告等诸多功能。构成了网帅系列产品无愧于业界领先水平。

公司总部在北京，分别在上海、西安、黑龙江等地设有分支机构。

秉承“专心、专注、专业”的理念，网帅的研发团队依然没有停止脚步，努力为更广泛的客户提供实用、易用、功能强大的网络安全产品。

我们的价值：为客户提供优质产品，为客户创造价值。