网康上网行为管理（NS-ICG）产品介绍

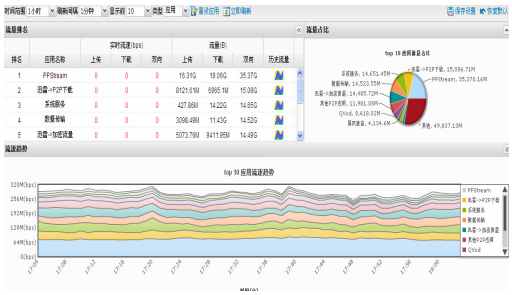
产品概述

NS-ICG（Netentsec Internet Control Gateway）网康上网行为管理是中国第一款专业的硬件上网行为管理产品。

为用户提供专业的用户管理、应用控制、网页过滤、内容审计、流量管理和行为分析等功能。可以帮助客户达成上网行为可视、减少安全风险，减少信息泄密、遵从法律法规、提升工作效率、优化带宽资源。ICG 广泛应用于政府、金融、能源、教育、运营商、大型企业等领域，帮助单位管理者全面有效的管理上网行为。

产品价值

- **上网行为可视：**



直观掌握各种上网行为，便于快速制定上网行为管理策略。

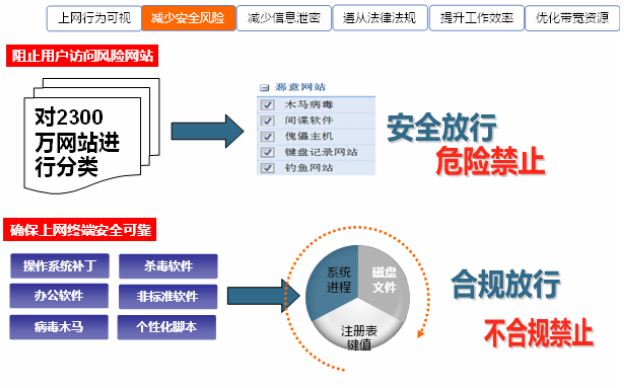
- ✓ P2P 流量占到了整体流量的 50%以上
- ✓ 迅雷下载和 P2P 电影是员工的主要行为
- ✓ **需要限制 P2P 的速率**

- ✓ 网站访问第一、第二名都是购物网站
- ✓ 存在较多以 IP 方式访问的财经及国外站点
- ✓ **需要在上班时间控制购物网站的访问**

- ✓ 邮件发送敏感关键字信息，存在泄密风险
- ✓ 搜索引擎在搜索大量的敏感关键字，存在法律风险
- ✓ **需要过滤外发邮件和搜索关键字**

● 减少安全风险

内置专业的海量网页分类库，帮助用户识别大量的风险网站，可以有效阻止员工访问这些带毒站点；配合终端准入机制，强制员工在计算机上安装必要的安全软件，降低桌面安全漏洞带来的安全风险

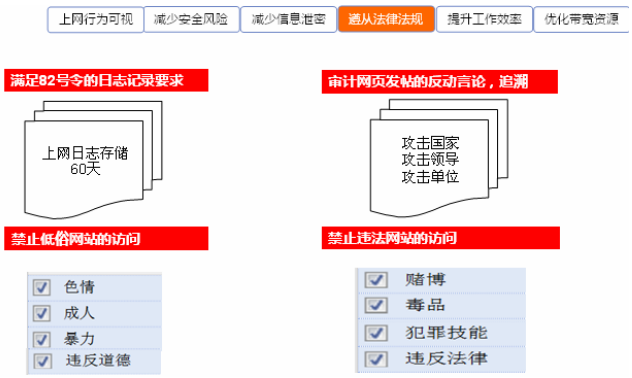


● 减少信息泄密

对网页发帖、邮件、IM、FTP 等上网应用所传输的文字、文件进行全面审计，便于产生泄密事件时快速追溯。如果传输的信息中包含了预设的敏感关键字，还可进行告警、阻断，快速发现泄密行为，防止信息外泄。

● 遵从法律法规

满足公安部门要求的上网日志记录 60 天的要求。避免员工访问低俗类网站和违法类网站，净化网页的访问。还可以过滤、审计论坛发帖，IM 聊天中存在的政治言论，提前规避法律风险。



● 提升工作效率

在上班时间限制游戏、聊天、炒股等上网行为，减少员工的工作时间浪费，提升员工的工作效率。

生成工作效率报告，提供给各个部门的管理者，便于清晰了解员工工作效率。

● 优化带宽资源

- ✓ 限制 P2P 下载，P2P 视频，网页视频，等浪费带宽资源应用的速率；
- ✓ 保障：OA、邮件、视频会议等关键应用的速率
- ✓ 在不增加带宽投资的情况下满足核心业务的带宽需求，保障业务质量。

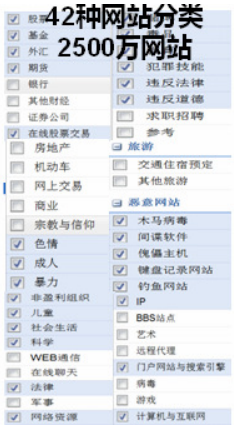
产品优势

● 识别精准：

上网行为管理产品的识别能力是产品是否有效的关键因素。只有识别范围广，识别准确率高，才能保证后期管理有效。

- ✧ **网页识别能力领先：**内置全球最大的中文网页分类库，可以识别 2500 万个站点的网页内容。
- ✧ **应用识别能力领先：**内置 600 多种主流网络应用协议库，完全不依赖于 IP，端口。无论应用 IP，端口如何变化，甚至加密也可以准确识别
- ✧ **更新频率领先：**网页分类库每天更新，应用库每 2 周更新一次。有效的避免网站和

应用变化带来的识别失效。



- **管理人性：**

上网行为管理产品需要能够有效避免员工的抵触。只有提供丰富、灵活、人性的管理方式，才能真正的使得上网管理制度能够落地

✧ 管理要素丰富：可以基于人员、时间、地点、应用类型、进行灵活的策略定义

✧ 员工自助管理：能够采用时间限额，流量限额的人性化方式让员工自己合理安排上网行为，避免简单粗暴阻断来带的抵触

- **安全可靠**

上网行为管理产品通常串联在网络中，并且能够审计到大量的敏感信息，需要提供高可靠性和数据安全保护

✧ **双系统引导：**一个系统不能工作时，另外一个系统可以接替工作

✧ **智能硬件 bypass：**支持死机保护、断电保护，在出现上述情况时会自动切换到直通状态，避免断网

✧ **数据传输防窃听：**所有设备管理及数据访问均在加密状态下完成，确保网络中传输的数据不会被窃听

✧ **三权分立：**网络管理员、日志审计员、权限审核员三权分立，确保网络管理员不会看到敏感信息。

- **简单易用**

上网行为管理产品需要能够快速跟进网络行为的发展变化，要可以简单的制定策略及更新升级设备

- ✧ 简单的界面：所具操作均为图形化操作
- ✧ 简单的更新：所有数据库更新均为一键式操作
- ✧ 简单的升级：出现新版本时管理员可一键升级

产品功能列表

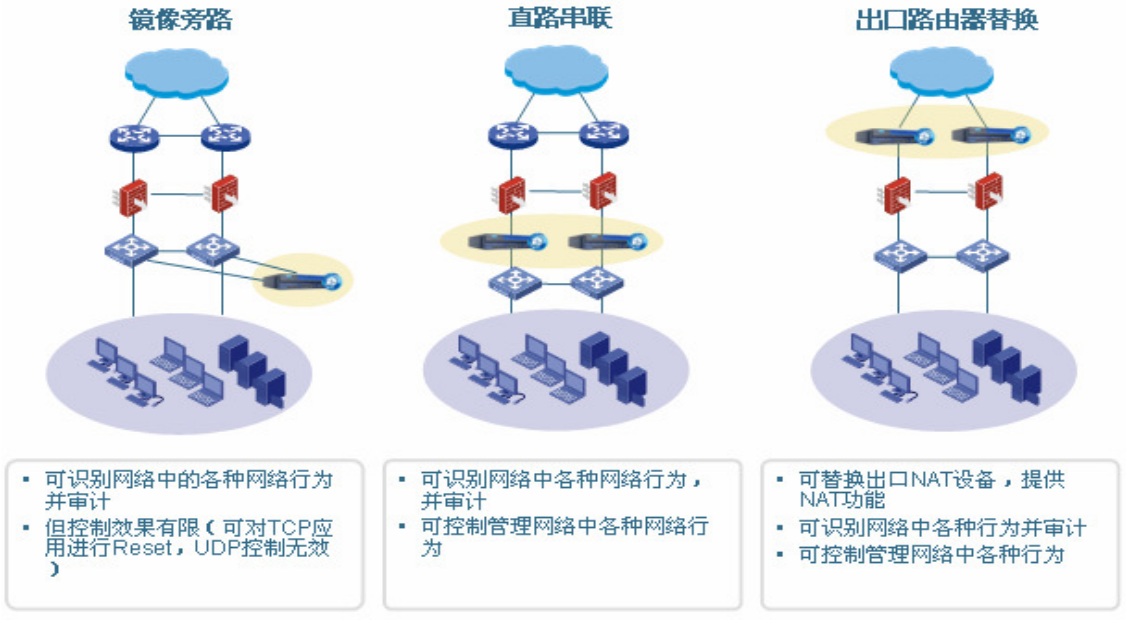
● 用户管理	
用户识别	IP、MAC、计算机名称识别 微软 AD、邮件、PPPOE、PORTAL 用户透明识别 华为 CAMS、城市热点、锐捷 SAM 用户透明识别
用户认证	网康本地认证 微软 AD、RADIUS、LDAP、邮件联动认证
终端准入	检查上网终端杀毒软件、操作系统补丁、标准办公软件的安装情况 确保注册表、运行进程、磁盘文件中没有威胁软件
● 应用控制	
应用识别	不依赖 IP、端口。可识别 P2P、在线视频、炒股、游戏、即时通讯等 600 多种主流应用协议。 用户可根据 IP、端口自定义应用协议
应用控制	根据人员、地点、时间、应用名称进行应用的放行、阻断
应用限额	设定应用可使用的时长，由用户自行安排使用，总计时长不能超过限额 设定应用可使用的流量，由用户自行安排使用，总计流量不能超过限额
● 网页过滤	
网页识别	通过网康的网页分类识别技术可识别病毒、木马、傀儡主机、色情、赌博、游戏等 2500 多万个网站的网页

	用户可以设定 URL 关键字自定义网页分类 用户可以设定网页智能学习分类，利用网页样本训练设备智能识别网页
网页 URL 过滤	根据人员、地点、时间、网站 URL 分类/URL 关键字 对 HTTP、HTTPS 网站进行访问的放行和阻断
网页内容过滤	根据网页标题、正文中的关键字进行网页过滤 根据网页下载文件类型、文件名称进行网页过滤
网页记录	记录员工访问 HTTP/HTTPS 网站的时间、地点、网站 URL、网站分类 记录员工访问 HTTP 网站的网页标题、网页正文、文件下载名称等信息
● 内容审计	
关键字库设定	用户可自行设定关键字库，每个库可设置 5000 个关键字，便于今后进行内容关键字过滤
网页外发审计	HTTP/ HTTPS 坛发帖审计，记录发帖的标题，正文，并可根据设定的关键字库进行发帖内容的阻断 记录论坛发帖上传的文件，并可根据文件名称关键字进行发帖的阻断 记录搜索引擎搜索的内容，并可根据设定的关键字库进行搜索内容的阻断
邮件审计	**POP3、SMTP 邮件审计：**可以记录发件人、收件人、标题、正文、附件；并可根据关键字库进行收件人、发件人、标题、正文、附件名称、附件内容的过滤 **SMTP 邮件外发预审：**可以临时缓存外发邮件，等到管理员审核完毕无泄密行为后再发送到外网 **WEBMAIL 审计:** 可对公共 WEBMAIL 或单位自身的 WEBMAIL 记录发件人、收件人、标题、正文、附件；并可根据关键字库进行收件人、发件人、标题、正文、附件名称、附件内容的过滤
IM 审计	可以对 QQ\飞信\MSN\YAHOO 通等 IM 进行账号审计、聊天内容、文件审计
telnet ，ftp 审计	可以对 FTP 上传、下载文件进行记录 可以对 telnet 上传、下载内容进行记录
● 流量管理	

虚拟通道	可将物理带宽分成多个虚拟通道，合理分配物理带宽资源
带宽控制	可以限制 P2P、视频等大流量应用的最大带宽上限，减少带宽的浪费
带宽保障	可以设定 OA、邮件、视频会议的基本带宽保障，保障关键应用必要的带宽资源
带宽借用	当部分虚拟通道空闲时，其带宽资源可以被繁忙的带宽通道借用，避免带宽浪费
带宽平均	可以根据用户平均分配虚拟通道内的带宽资源，使每个用户平均分配带宽，公平访问避免资源浪费。
● 行为分析	
实时监控	实时展示网络的带宽占用情况、应用使用情况、网页访问情况、人员访问分布、风险告警情况
日志查询	对整个网络的访问日志进行查询，包括：用户、应用流量、网站访问、搜索引擎、邮件收发等
统计报表	支持统计报告（用户活动、用户行为、带宽资源、上网时长）的订阅和管理 支持智能报告（工作效率、行为合规、带宽资源、综合评估）的生成和管理

应用场景

✧ 镜像模式、直路串联、出口路由器替换：

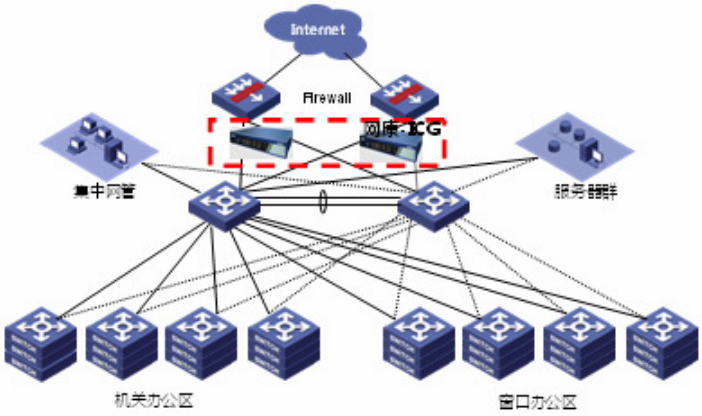


最佳实践

● 政府：

农业部
环保部
民政部
共青团中央
国家统计局
国家知识产权局
北京市发改委
吉林省委

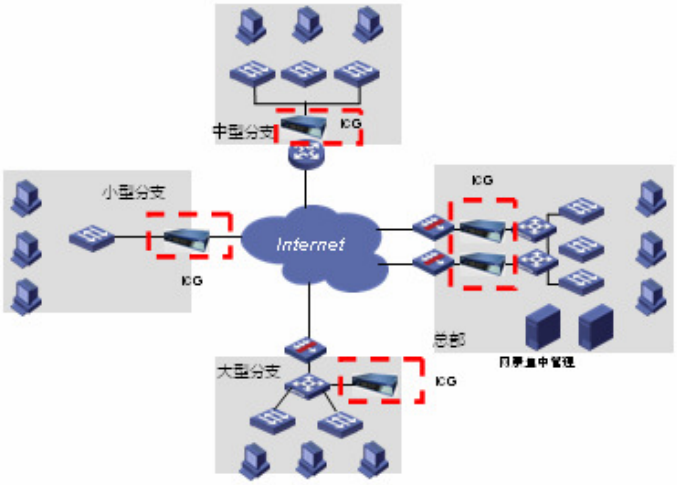
- 国家税务总局管理层对互联网上的潜在隐患具有高度的风险意识。通过管理规定严格要求单位各级员工遵守国家法律法规，禁止员工浏览不和谐的网站，更不能参与任何与国家法律法规违背的网上讨论。经过严格的筛选，国税总局最终认可网康科技提供的**法律法规遵从方案**，将单位的管理规定通过技术手段落到实处



● 能源：

中国石油
中国石化
中国海洋石油
长城润滑油
华能集团
山东电力
河南电力

- 中国石油昆仑润滑油公司是中国石油天然气股份有限公司旗下的润滑油公司。避免员工上班时间因为互联网无关访问降低工作效率，提升服务质量是昆仑的重点工作。
- 通过全国采用网康科技**互联网工作效率保障方案**，在上班时间限制了视频，炒股，购物，交友，非工作聊天的手段，降低了员工在互联网上的无关消耗，工作效率提升显著

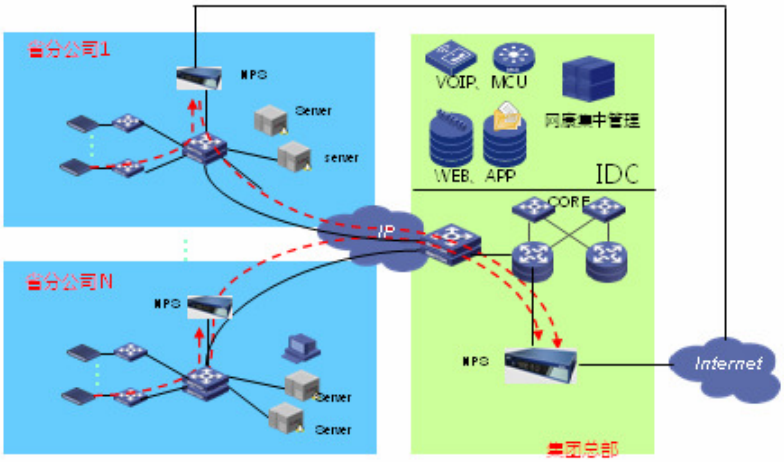


- **金融：**

泰康人寿
中国人寿
阳光保险
...
民生银行
国家开发银行
...
银河证券
招商证券

● 人保财险是中国最大的财产保险公司。在全国各地均有分支机构。通过互联网投保是该公司一个重点业务，提升互联网的安全等级是PICC的一个迫切需求。

●通过网康科技的恶意网站分类，阻止员工访问恶意风险网站，避免安全威胁进入内网，提升了互联网线路的安全等级。

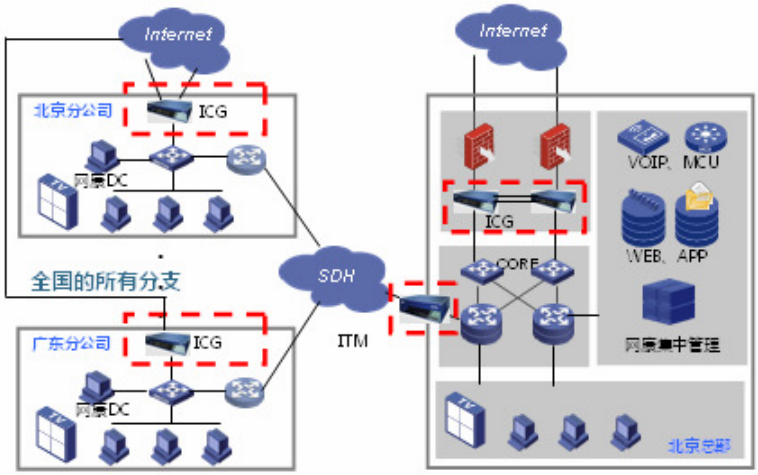


- **大型企业：**

搜狐
新浪
京东商城
赶集网
搜房
中华英才网
。。。

● 百度网络技术有限公司是中国最大的互联网公司，其业务覆盖中国的各个省市自治区。防止信息泄密是百度科技的一个迫切需求。

●通过采用网康科技泄密审计，审计过滤网页发帖文字及附件、邮件外发文字及附件、IM通信文字及附件、提升了百度科技的互联网防泄密等级



● 运营商

广东移动
贵州移动
新疆移动
南京移动
山西移动
深圳移动
东莞移动
辽宁联通
湛江电信

· 中国移动通信重庆分公司是中国4个直辖市移动公司之一。具有先进的IT运营理念。通过采用网康泄密审计方案、提升工作效率，强化了单位的信息安全等级，使得员工工作效率明显提升，得到了公司领导的高度认可