上网行为管理技术白皮书

满足 Internet 行为的管理需求

2006 年 12 月

深信服电子科技有限公司

文档编号：20061205 - 410

目录

全文介绍

在中国，Internet 的普及为组织带来了更多的商业机会，极大地降低了运营和沟通成本。同时，由于对互联网访问缺乏必要的管理措施，组织的网络资源往往得不到有效的利用，并由此引发了一系列安全、效率和法律问题。

本文针对互联网行为的管理和控制，介绍了一套行之有效的解决方案，旨在帮助用户实现对核心网络资源的保护，规避不良行为带来的法律风险，在有效提升组织工作效率的同时也使网络带宽资源得到合理的利用。

一．互联网对组织提出挑战

过去，中国员工通过与同事闲聊来打发上班时间。随着计算机和互联网的普及，员工有了更多的选择，网上购物、与好友聊天、下载手机铃声、在线欣赏音乐、下载电影、收发个人邮件、在论坛上舞文弄墨……。只要员工有兴趣，他们就能在上班时间尽情享受互联网带来的乐趣。

Dynamic Markets Limited 每年会对全球的企业员工和 IT 主管进行调查，重点探讨在办公环境中互联网及应用系统的使用情况，一方面从中了解员工的上网习惯，另一方面可从 IT 主管的立场来认识企业所面临的网络问题。其中，对中国的调查结果令人吃惊：在办公室中，和其他国家相比，中国员工每周多花 7.6 小时来使用 IM、玩游戏、P2P 或在线媒体；中国员工上网下载音乐的时间比拉美高 16%；上网进入聊天室和玩在线游戏两方面花费的时间分别比其他国家高约 8%和 12%；在同为发展中国家的印度，只有 26% 员工在工作场合浏览个人信件，而在中国，这个数字则是 60%！

员工沉迷在互联网带来的诱惑之中，组织的网络却被不断蚕食和破坏。中国的大多数企事业单位网络出口带宽不足 10M，更多的机构甚至与其他组织分享 1M 的 ADSL 线路。很多员工一打开电脑就会自觉地开始各种下载工作，包括 BT、电骡、迅雷这些网络资源的“吞噬者“，这些员工在大量下载电影和软件的同时却在不停地抱怨网速太慢！同时，不管员工有意还是无意，他们都能够而且有办法去访问一些对组织网络基础设施有害的内容，通过 Web 访问、及时通讯工具（Instant Messenger，IM）和文件共享（Peer to Peer，P2P）带来的病毒、蠕虫和木马，都可以随着简单鼠标点击轻而易举的侵入内网。

让人无奈的是，员工的不规范网络行往往需要组织的管理者为其买单。信息充斥着互联网的每一个角落，未授权的论文、音频和视频文件都可能被员工们无意下载并传播，

而这一行为将会招致比以往更多的惩罚，来自多方的压力迫使中国政府前所未有的重视知识产权的保护。而一些员工利用上班时间访问内容偏激的网站甚至组织、参与非法网络活动，例如网上诈骗、网络攻击，这些行为使组织名声扫地，蒙受牵连。

组织核心资源的未授权传播同样令管理者痛心疾首，也就是我们经常提到的员工泄密行为，这在国内已有众多先例。由于互联网行为复杂且难以预料，无论是存心还是意外，一个居心叵测的员工和一个忠实可靠的干将都有可能将局域网内的重要资料泄露给第三方组织甚至竞争对手。

以上所提到的问题不是耸人听闻，而是实实在在地存在于每一个互联网络，也许你还没有意识到问题的严重性，那只是因为事态的发展还没有到达让你震惊的地步。

值得庆幸的是，越来越多务实、具备安全意识的管理者发现了问题所在，并希望通过有效而可靠的途径来实现对员工的网络行为管理。在这里，深信服科技（SINFOR）的 AC 上网行为管理就是其中最具竞争力的解决方案。

二．AC 给用户带来的价值

深信服科技(SINFOR)的 AC 产品带来了全面而细致的互联网行为管理解决方案。在此，我们通过对 AC 在管理网络带宽、保障内容安全、提高生产效率和规避法律风险这四个方面来具体阐述其为用户带来的商用价值。

✓ 管理网络带宽

网络流量管理

AC 上网行为管理产品通过审计、控制、优化和带宽叠加等功能，协助管理者全面分析和优化广域网带宽资源。

AC 的数据中心（Network Data Center， NDC）对局域网发生的所有网络行为进行记录、分析和趋势报告。借助图形化的数据和报表，用户可以直观地了解到哪些服务占用了广域网宝贵的带宽资源，网页浏览，收发邮件，还是疯狂的 P2P 下载。同样，我们还可以了解到哪个员工在网上购物方面表现出了异于常人的活跃，哪些部门在上班时间观看了最多的在线影片。通过对网络使用情况的深入了解，管理者能够制定出最适合自身组织机构情况和的互联网访问策略。

由于 AC 提供对各种网络服务的拦截和管理，以往的拔网线、通报点名的强制性手段将成为过去，如何发挥 AC 的强大功能只取决于你的决心。如果你在“彻底封杀某个服务”，还是“完全放开这项服务”的决定中摇摆不定（例如 P2P 下载，其吞噬带宽的同时也带给了我们丰富的信息资源），你也可以选择对应用的流量进行调整。

P2P 软件的控制

P2P 技术使人们可以高速获取海量的网络资源，而 P2P 软件对带宽的占用也使其招致种种恶言。一个 2M 以太网出口的局域网，只要有 2 个以上的员工不限速地使用 BT，所有人的正常网络浏览都将成为不可完成的任务（Mission Impossible）。每天，

互联网上都会有人发布最新的 P2P 软件，这让大多数的 P2P 控制工具望尘莫及，它们往往只能封堵“昨天的 BT 软件”。

AC 改变了这一切。通过对 P2P 下载软件的智能检测（专利号：200610156977.8），管理员甚至可以彻底封锁所有的 P2P 流量。如果你不想做的太绝，你可以选择针对特定用户和相应的 P2P 工具进行流量控制，只要不超出网络使用者的容忍程度，大多数用户还是可以允许内网中存在 P2P 下载。

带宽优化和多线路策略

QOS（网络服务质量）技术包括专用带宽、抖动控制和延迟、丢包率的改进以及对指定高优先级网络服务的流量保证。AC 同样采用了 QOS 技术，对流经 WAN 和 LAN 的数据进行了优先级处理，保证了重要服务的带宽质量。

AC 产品也继承了深信服科技（SINFOR）其他产品线的领先技术。借助多线路负载均衡技术（专利号：ZL03113974.4），内网用户访问不同的运营商网络时可以自动匹配最优的网络出口；而通过配置带宽叠加策略（专利号：200310112006X），组织可以把多条 Internet 线路合为一条公网总出口，以获得更好的互联网访问感受。

✓ 保障内容安全

拦截不良网页

AC 设备内置了可自动更新的分类 URL 库，其中包含了海量的成人、暴力、反动和恶意网站信息，这有助于将不健康和包含潜在威胁的网站拦截在外。由于每天互联网都会涌现出大量的站点，AC 的 URL 库也提供了使用者分享功能，用户可以在 AC 的 URL 库自定义需要被拦截的 URL。通过对 URL 的阻拦，可大大地降低了内网用户对不良 Web 页面的访问。

对于很多 URL 过滤设备无法控制的 SSL 加密页面，AC 同样能够施展拳脚。很多钓鱼网页伪造成网上银行企图骗取出用户的银行卡密码和资金，通过在 AC 中导入和设定 SSL 证书和链接的黑白名单和证书时效性确认，将有力地避免网络行骗者使用的伎俩。这对使用 SSL 方式进行加密的反动、色情、邪教等网站同样有效。

文件传输控制

Http 下载和 FTP 下载经常会发生令你意想不到的“Surprise”。当你打开辛辛苦苦下载到本地的压缩包，却发现里面根本不是你需要的文件，然而你的电脑却在瞬间“毫无预兆”地瘫痪了。同样，将病毒和蠕虫潜入 IM（即时通讯）软件也是黑客们非常热衷采取的手段，你 QQ 或 MSN 上的“好友”可能在不经意间将木马、钓鱼网站地址、间谍工具发送给你，再利用你传播给更多的人。当局域网中有人接受到恶意的文件，受伤的将不止他（她）一个。

针对文件的传输，AC 提供了更细致的解决方案。通过对象设置，你可以将关键字、文件类型、网络服务与 IP 地址组进行关联，再进一步实现细颗粒的控制策略。如果你想拒绝从 IP 地址为 202.96.137.75 的站点通过 Web 方式下载一个包含“hijacking”关键字的 cpp 文件，那么你应该选择像 AC 这样的内容安全设备。

✓ 提高生产效率

URL 匹配策略

在工作时间里，员工往往在从事私人活动，这是办公室众人皆知的秘密。管理者和决策者许能够影响一个员工的生活质量和职业方向，但却难以阻止员工在上班时间通过网络投递简历或在虚拟社区中开 Party，这些都是随机而难以控制的。AC 提供基于角色的管理方法，你可以让你的员工和部门在工作时间访问特定的网站，例如提供行业信

息的网站、合作伙伴链接和公司的门户网站，而其他未经允许的网页浏览都将是被拒绝的。

IM（即时通讯）软件的管理

在工作时间，太多的人在使用聊天工具，也许在和同事讨论工作，也许更多时间在同家人、朋友甚至是陌生人聊天搭讪。你无法确定员工何时使用 IM 谈业务，何时用来聊私人话题。当管理者无所侍从时会想到如何来屏蔽聊天工具，网管员或一些工具通过将聊天软件使用的服务器加入黑名单来杜绝 IM 的使用。但聊天工具层出不穷，QQ、MSN、Skype、Yahoo！Messenger、ICQ……，封服务器地址最大的特色就是治标不治本，而且会浪费大量得到时间。AC 通过对聊天工具网络访问规律和特征代码的深入分析，实现了对聊天工具的全面控制。AC 不仅可以对特定的聊天软件进行封堵，还可以记录通话信息，管理聊天软件的文件传输。对于聊天软件扩展的相关应用程序，例如游戏、视频等同样可以做到封锁和控制。

对各种应用的管理

互联网的成员有着各种兴趣和爱好，仅实现对 IM 和 URL 的访问控制对一个亟待完善管理的网络来说还远远不够。视频、语音、图片、文档也同样被大量的上传和下载。你的员工可能刚进办公室就迫不及待地下载一部电视剧，因为他昨天下午只欣赏了前两集；还有的员工会利用上班时间更新自己博客中的文章和照片，虽然这段时间你更希望他（她）做一些和工作相关的事情。对于上述的问题，AC 同样能够实现上传和下载管理，避免员工在网上花费大量的时间来从事娱乐活动。

上网时间管理

每个组织都有朝九晚五的工作时间安排，弹性工作时间的制定让员工能够更合理地安排工作内容，让组织更有效率也更富人情味。同样，将员工每天接触的互联网访问时

间也进行合理有序的安排，也是专业的网络行为管理设备应该考虑的问题。通过 AC 对员工个人和部门的上网计时管理，你可以合理安排各个成员和部门的上网时间。而对于希望通过某种手段来实现上网计费的组织，这个功能也极具扩展价值。

✓ 规避法律风险

外发信息控制

办公室中有太多的信息，无论是涉及组织生死存亡的机密资料还是总裁办公室的八卦新闻，员工们总是希望一吐为快。除了打电话和写信，他们现在有更多的选择，即时通讯软件、邮件、BBS 论坛、个人博客等 ,都为倾诉和抱怨提供了 Anywhere、Anytime、To Anyone 的条件。同时，各种组织都存在人员的流动性问题，组织的商业合作伙伴、投资人、审计员乃至新员工随时都可能接入内网，他们可以通过网上邻居下载机密的财务报表或人事档案，再打包发到互联网的某一个角落。组织需要一个完整的认证体系来确保每个接入者的网络使用权限。

AC 提供了完整的身份认证体系。你可以启用基于 Web 方式的用户名/密码认证，IP 和 MAC 地址的绑定，如果你的内网已经部署了 Radius 域认证或者微软的 LDAP，你同样可以在 AC 中找到它们的设置选项。通过和域认证的联动，你甚至可以通过 AC 来保护内部服务器的访问安全。如果你的组织已经部署了邮件服务器，你也可以把所有人的邮件帐号导入 AC，让员工在收取邮件的同时直接通过 AC 的 POP3 认证。有了这些认证机制，只有受组织信赖的部门和成员才能访问特定的网络资源，未经授权的局域网接入用户只能望着自己的显示器发呆。

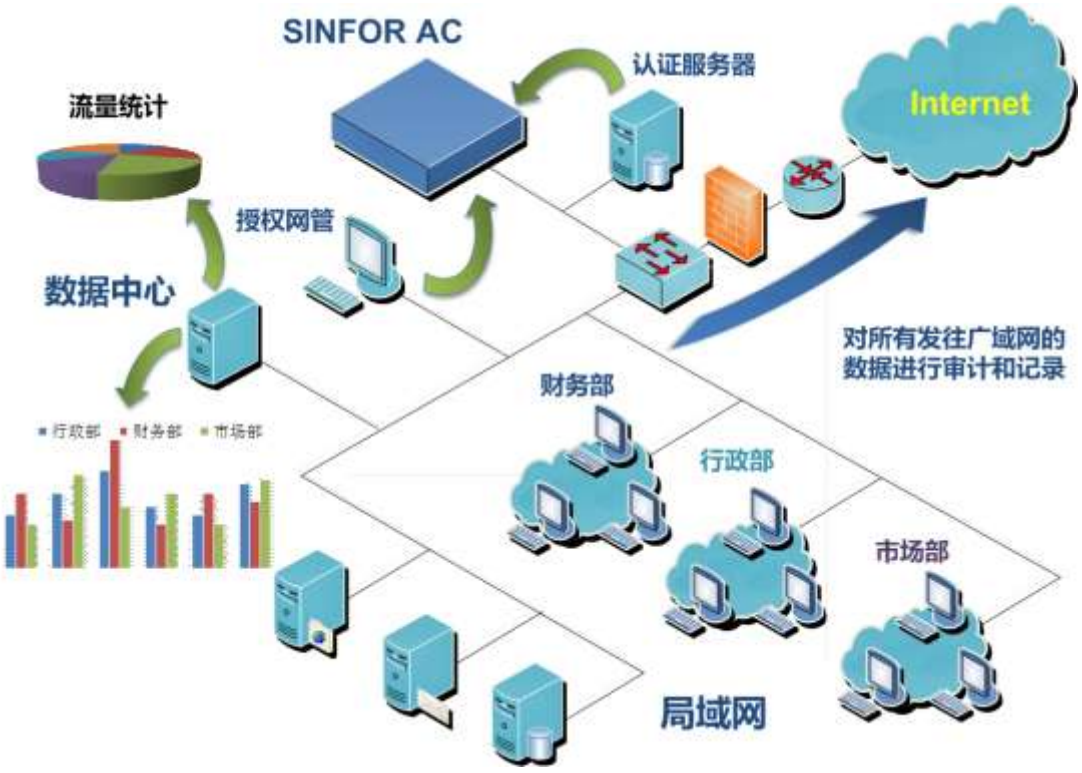
保护版权资料

互联网充斥了大量的免费资源 ,涉及版权纠葛的音乐、视频和论文可以随意的下载。个人用户对版权的忽视往往会若上相关部门的注意，当这些免费的下载和共享是发生在

局域网时，组织难免惹火上身。AC 的访问控制系统通过对 HTTP、FTP、IM 软件、邮件收发的内容检测和控制，可以尽量阻止员工搅入版权话题；同样，当员工已经出现问题时，你可以在 AC 的数据中心中找到其个人的违规记录，进而为组织摆脱不必要的纠纷。

法律遵从和举证

由于员工的个人偏好导致的非正当的行为，例如对色情、暴力、反动、邪教方面网站的访问，AC 将有效的避免和拦截；当内部员工发出的不负责任的言论已经难以挽回时，例如在 BBS 中发煽动性言论、网上聊天中采用侵犯性语言等，你都可以在 AC 中找到相关记录作为法律举证的重要依据。



三．功能实现

在这一部分，我们会向您展示借助于 AC 实现的一些令人兴奋的功能。基于在网络行为管理领域的丰富经验，我们强烈建议您按照顺序阅读，这样会使网络的管理具有方向性，更有助于后期的管理和维护。

3.1 规划你的部门

如果你所在组织已经建立了完善的职能部门和成熟的决策流程，作为网络的管理者，你也有权利规划局域网的组织结构。在 AC 中，我们建议你通过 IP 组设置来实现。

首先你需要收集局域网中所有 IP 地址，然后再根据职能部门来划分用户组。有些部门由于物理环境的限制无法获取连续的 C 类地址（如下图所示），但这不会影响 AC 的使用，你需要做的就是继续添加。对于某些不属于特定部门的人群，如每周来办公室工作两天的股东、新入职的员工，你可以另外给他们建组。记住，不要逃避这个步骤！在后面你会发现，细致的准备会让你在突发事件来临时镇定自若。

3.2 建立身份认证体系

在这里，我们讨论一下互联网访问的认证机制。

3A（认证，授权和审计）是组织安全基础设施的基础，将对用户和内容进行有效的保护和控制。认证对于一个局域网来说主要分为两个层面，首先是借助应用系统自身的认证，例如 OA 系统的用户名/密码，这可以从一定程度上避免非授权用户对内网核心资源的访问；另一层面是借助于网络部门建立的 Radius 域认证、微软 LDAP（Lightweight Directory Access Protocol，LDAP）等来对内部用户进行身份认证管理。然而，基于内网的安全的认证机制还需要进一步完善。试想，如果可信用户例如一个打算离职的员工把内网中的财务报表通过 E-mail 发送给好友，或将组织辛苦搜集到的客户信息打个包上传到公网的一台 FTP 服务器 ,这些行为对组织的经济效益将带来巨大的损失。

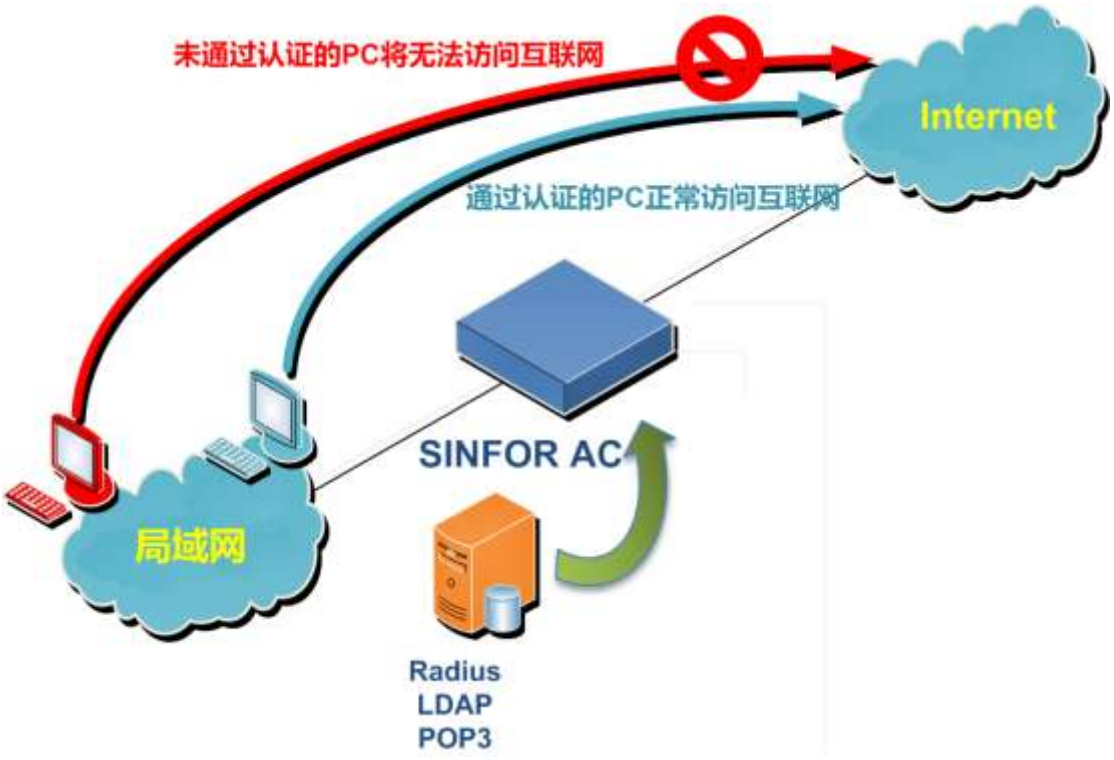
所以，我们还需要管理局域网中所有用户的 Internet 访问。上一步骤中，我们已经划分了用户组，现在我们需要对用户组进行认证方式的设置。

在 AC 中你将切实感受到多种认证方式带来的方便。身份认证主要有两种方式，免客户端认证和客户端认证，AC 中的 Web 认证属于前者。Web 认证通过浏览器即可完成全部认证，即使对计算机操作并不熟悉的用户也能够理解和操作，很好提高了操作的互动性和弹性。

Web 认证是这样运行的：内网的用户第一次开机时，只要在浏览器中输入网址，AC 将自动把用户的访问页面重定向到预设的 Web 认证界面。只有在页面中正确输入管理员分配的帐号信息才能正常访问 Internet 并获取相应权限，否则网关将拒绝用户的所有 Internet 连接请求。另外，为了避免用户离开后主机被他人利用，当用户再一

段时间内没有发生任何网络流量，AC 的 Web 认证将断开其网络连接，直到用户再次通过 Web 认证。

AC 支持多种认证方式，除了通过用户名/密码、IP/Mac 认证外， AC 的 Web 认证还可以透明结合 Radius、LDAP、POP3 等认证服务系统进行用户身份校验。IP/Mac 认证可以通过 AC 自带的局域网扫描功能实现。对于后几种认证手段，只要在 AC 中正确填入域、活动目录和邮件服务器的地址和端口，AC 将自动更新用户列表和策略，这对建立了完善的内网认证体系的用户非常方便。



在下一版本的 AC 中，你还将有机会体验更多的身份认证机制，这包括 PPPOE 认证、802.1X 认证和 USB Key 认证。通过给内网用户颁发随身携带的 USB 密钥，用户的身份认证信息将被存储到一枚小小的智能钥匙（Key）中，只要在电脑的 USB 口插上加密 Key 就可以正常上网 拔掉 Key 以后 即使他人能够有机会使用你的 PC 或笔记本，他仍然无法获得互联网的访问权限。

3.3 开始分析网络流量

恭喜你走到这一步。当用户通过认证系统的身份校验后，AC 将为不同的用户组进行授权 ,将系统管理员设定的策略同用户的标识相对应。简单的讲 ,授权就是一组规则，这些规则决定了哪些用户可以访问哪些资源 ,以及这些用户可对这些资源执行哪些操作。在 AC 中，这些规则的制定主要从保护、控制和监控出发，并将这些规则和用户有机地结合在一起，进而形成一套完整的访问控制策略。

当局域网中的用户通过了认证、授权后 ,你往往要面临严峻的广域网带宽使用问题。不要抱怨运营商给你的带宽永远不够，即使你拥有千兆的公网出口，广域网中传输的延时和低效率的 TCP 握手协议同样会让你的网络访问拥塞不堪。好的改变方法是部署基于广域网的加速设备，已经有一些领先的厂商在这个领域有所建树。如果你暂时还没有这个计划，我们可以考虑从自身的管理入手。

AC 的网络数据中心（Network Data Center， NDC）是一种统计分析工具，它可以记录局域网用户访问 Internet 的所有流量，例如哪个时段有最多的人观看网络视频点播，哪个部门的人收到了最多的含有病毒附件的邮件。根据网络数据中心提供的数据统计以及各种图表，你可以立刻展开行动。

举一个例子，通过在数据中心对组流量进行统计，你发现工作内容和 Internet 并不怎么相关的财务部却占用了广域网 45%的总流量，而财务部门的 PC 只是局域网 PC 数量的 2%，那么你就有必要深入调查一下了。你可以查询一下财务组中哪些服务占用了最多的带宽，Web 浏览、FTP 上传还是 P2P 共享。如果资源大户是 PTP 共享，那么你可以进一步查询财务组中是哪个人使用了最多的 P2P 下载，是在哪一时间段使用的。如果他（她）的 P2P 下载都发生在上午 9 点到 12 点和下午 2 点到 5 点半的工作时段，那么你就可以采取进一步的措施了：1.限制这个员工的网络权限，不允许他（她）下载 P2P；2.为他设定网络使用时间，既然他（她）对互联网充满了兴趣和渴望，不妨把活动安排在下班时间；3.控制他（她）的 P2P 下载流量，让他（她）可以照常使用 P2P，但只能使用有限的速度来下载。

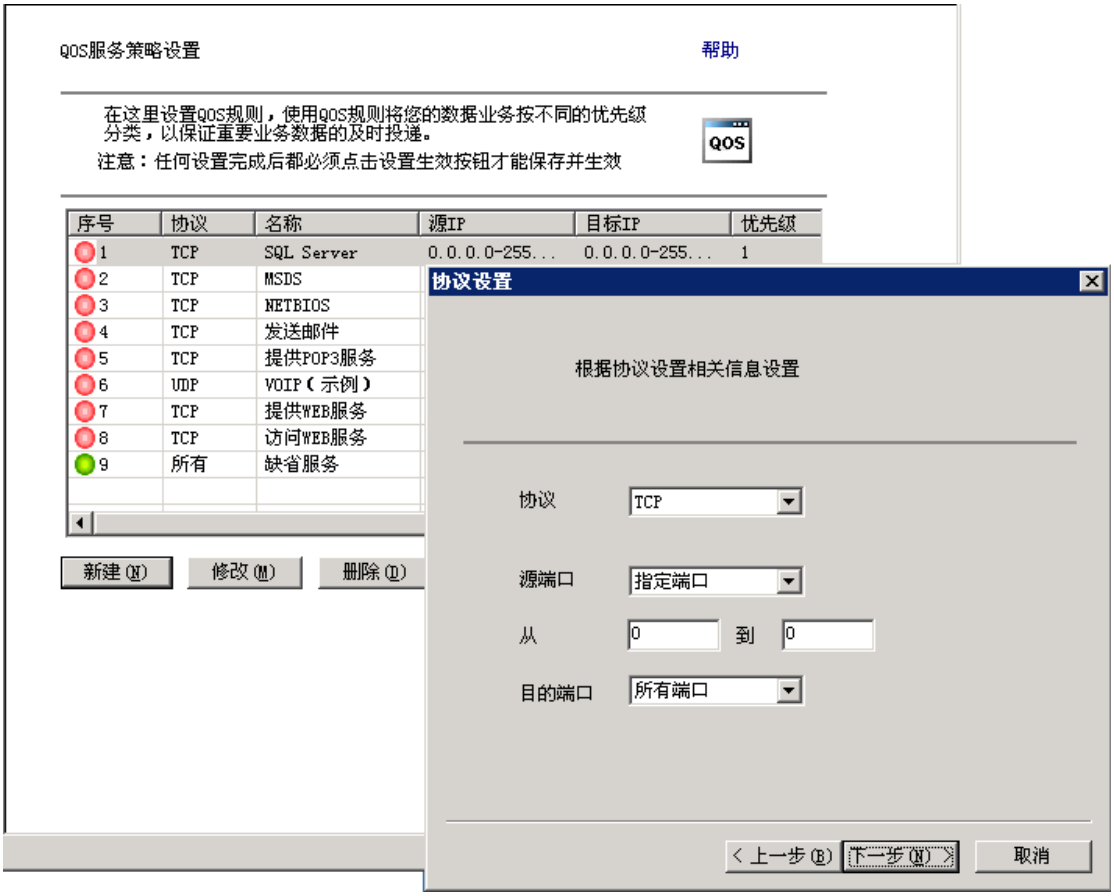
我们只举了这个简单的例子。如果你是一位身处大型的机构的 CIO 或 CEO，你需要面对的问题将远远不止这些，而 AC 的网络数据中心包含的内容需要你自己去亲身体验和掌握。当你面对数据中心的 Web 页面，通过几次鼠标点击就发现了网络中存在的问题时，你将感受到领先技术带来的极富乐趣的用户体验。

3.4 优化带宽资源

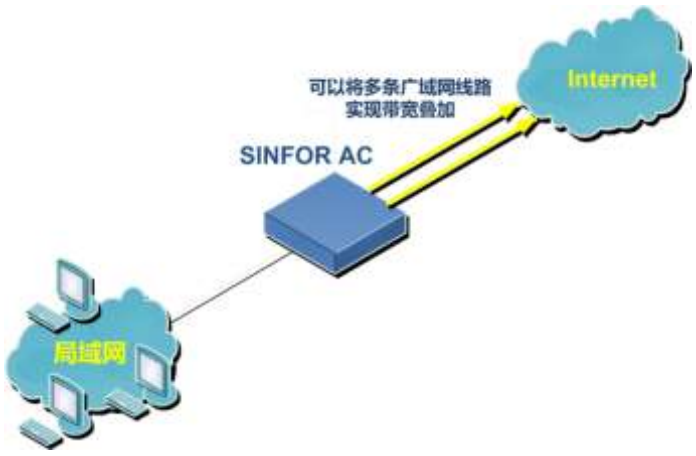
在不能改变你狭窄带宽的前提下，你需要学会去适应带宽，进而优化带宽。试想一个公司的大门并排走可同时经过 20 个人，100 个人如果按照顺序走出去不会花费超过 20 秒的时间。而如果 1000 个人同时冲出大门，门外还有 500 个人往里冲，那种情形将是难以控制的！而组织的互联网访问就经常如此。

优化组织的广域网带宽有多种方法。拿 AC 来说，如果你看了上一个小节，你可以学习对组织的部门和个人的上网情况进行分析，并调查清楚是哪些服务占用了最多的广域网带宽。根据这些资料，你心中应该有一个判断，对占用带宽最多的资源怎么处理，对互联网访问量最大的部门和个人该如何引导和规范，这从一定意义上已经属于管理的范畴。

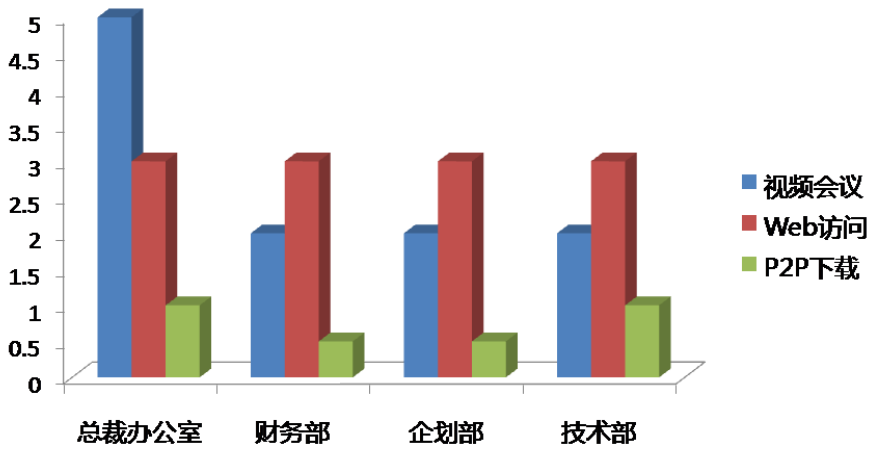
你首先可以考虑使用 AC 的 QOS 和带宽叠加功能，它们将对广域网的带宽优化起到有效作用。QOS 的设定有助于那些要求高传输质量、低时延的服务取得优先的带宽，例如视频和语音服务，人们难以忍受对端的一句话反复传送 3 遍到你耳边，或是你瞪着屏幕半天只看到了 10 分钟前对方的表情。



而带宽叠加技术作为深信服科技的一项专利（专利号：200310112006X），已被直接用在 AC 上网行为管理这条产品线了。通过绑定多条 ADSL 或专线，你可以获得更大的出口带宽，当你绑定多条 ADSL 时，你可以获得超过单条 FTTX 的带宽，而其费用却远远低于后者。这对于拨号和 xDSL 资费低廉而且专线线路难以申请的地区尤其有吸引力。



更具效力的网络流量优化方式是 AC 的基于用户的流量控制技术（User - Based Traffic Control, UBTC）。在广域网的访问中，有些部门的特殊应用是应该而且必须获得独占性资源的，例如总部的管理层同各分公司主管召开的视频会议，而有些部门的非工作相关服务本不应获得更高的带宽，例如采购部门的 P2P 下载。以往的带宽管理只能对特定服务分配相应的百分比带宽，属于“一刀切”行为。而通过 AC 的分组流量控制,你可以对不同用户组使用的服务进行精细到以 K/Bps 为单位的带宽分配，保障重要部门的重要服务得到足够带宽，使非重要的服务受到合理的流量限制。



当我们对互联网的使用情况有了大致的了解后，我们可以针对用户组的行为做出进一步的管理和控制。

3.5 网页浏览的控制

网页的浏览是互联网访问的主要内容。组织员工在这方面的共同点是，每个人来到

办公室后的第一个工作就是打开浏览器，而区别在于每个人浏览的内容差异和沉浸于其中的时间多寡。

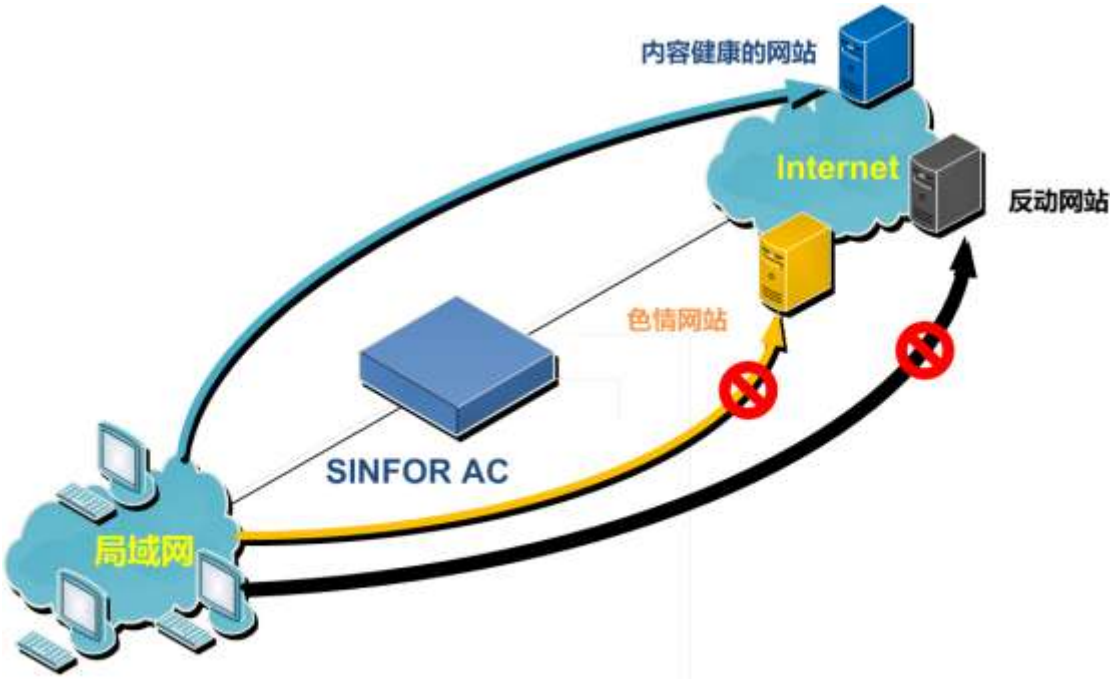
一方面，组织的管理者不希望给办公室营造监狱一样的环境，即使有些员工在八小时内做了很多与工作无关的事情，组织也不可能专设一个监视人员全天候的站在员工身后指手画脚。为了使员工得到更好的心情和满意度，组织需要一个人性化的环境。

另一方面，员工对互联网的滥用的确带来了严重的生产力流失。如果你的一个员工的月薪是 4500 元，其薪水平均到每小时大约是 20 元，而他（她）每天若只拿出 1 小时的时间进行网上购物、娱乐八卦浏览、网络炒股、成人网站欣赏，这个员工每年将给你带来近 6000 元的损失，你是否觉得他白白领了你一个半月的工资？而对于一个员工在 500 人左右的组织，在一年中因为互联网滥用带来的生产力流失将高达到 300 万人民币。

在“戴上手铐”和放任自由之间，你可以通过 AC 对 Web 页面的访问控制来进行更人性化的管理。

在 AC 的内置库中有着数百万的 URL 资料，分为新闻、音乐、视频、成人、财经、教育、科技等条目，如果你足够细心，你还可以发现“超级女声”、“台湾综艺”这样的 URL 组。在局域网中的用户浏览网页时，AC 的联动式分析系统（Link Analysis System, LAS）将发挥作用。由于每天互联网涌现出来的新网页数量超过 30 万，再强大的 URL 库也无法实现及时更新，这将导致大量的网站无法被网页过滤设备识别，进而无法实现对网页浏览的控制。通过 LAS 技术，AC 将根据网页的内容、用户可管理的关键字组、网页中包含的文件类型进行联动式分析，并根据 AC 默认的设置、管理员自定义的过滤规则对用户需要访问的网页进行过滤。

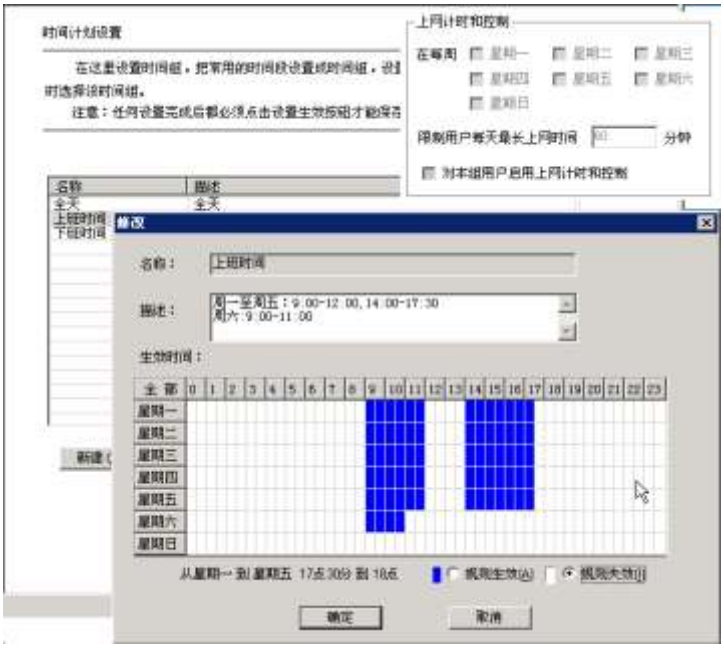
有了 LAS，你的员工依然可以上网，但其上网访问的内容却可以收到你的管理和控制。一般性的新闻、技术以及同工作相关的页面是可以被允许访问的，而涉及到色情、暴力、黑客、破解类的网站将无法打开。



同样，你也通过时间计划给予你的网络管理更多的人情味。大多数的网络行为管理方案只能采取时间段管理，例如把全天 24 小时划分为工作和非工作段，在非工作时间段内员工可以自由访问网络资源，而工作时间段中员工的互联网访问将受到控制，这种方式显然缺乏弹性。在不同的季度，不同的部门甚至每个员工都有着各异的工作习惯和工作时间安排，而时间管理应该是兼具计划性和灵活性的。

AC 的时间管理分为两种，一种是微观时间管理（Micro Time Control, MTC），MTC 将一周中每一天的时间进行划分 ,例如在周一的 8 点至 18 点禁止全公司内的一切娱乐网站的浏览，在周五的下午 16 点至 17 点放开信息中心和市场部门的 BT 下载等。另一种是总体时间管理（Overall Time Control ,OTC），OTC 可以为各个部门的员工设置一周内每天的总上网时间。有了这个选项，你可以进行广义的管理并取得很好的效

果：如果一个员工知道他周二的上网时间是 40 分钟，那么他会尽量在网上做一些工作相关的查询，否则他将无法完成上级分配的任务。同样，有着经济头脑的你会想到可以把 OTC 和上网计费结合在一起，超过时间限制的机构需要通过上缴费用才能继续上网，这种做法当然可以。



3.6 管理即时通讯工具

根据 IDC 的统计，每天全球有 120 亿条消息通过即时通讯工具（Instant Messaging，IM）被发送。中国腾讯公司的 QQ，其每天的独立上线人数高达 1200 万，活跃用户数更是达到了 5500 万，几乎覆盖了中国所有的网民。2006 年 12 月底，台湾地震引起的中美海底通讯光缆的断裂使中美之间的网络通讯受到了严重影响，一时间，中国上千万的 MSN 使用者不知所措。作为对人类社会生活产生最深刻影响的网络形态，IM 使商业人士之间的沟通超越了 Where、How 和 When 的限制，使客户服务人员的技术支持实现了快速到达用户桌面的能力。不断成长壮大的 IM 已经成为了事实上的企业通讯标准。

然而，IM 的大量使用也造成了生产力的流失和机要信息的泄露。你无法限制员工在上班时间在通过 QQ 群开 Party,或使用 MSN Messenger 和远在国外的女友视频聊天。同样，证券交易机构同外部投资银行客户之间的聊天有机会造成潜在的证券交易违规行为，产品研发人员与同行业合作伙伴或竞争对手的网络对话也存在泄露知识产权的可能。

“One Coin，Two Sides”，对于 IM 这种具有两面性的网络通讯工具，大多数同类产品采取的解决办法有两种：第一种是将 IM 的服务器地址列入黑名单，像封堵 URL 列表一样禁止内部用户访问 IM 的服务器；第二种方法是试图关闭路由器或防火墙的相应端口来禁止 IM 的流量。这两种都是工作量大、且注定无法取得预期效果的方法。

AC 可以提供对 IM 软件从禁止、监管、再到安全性审查的解决方法。

✓ **禁止**

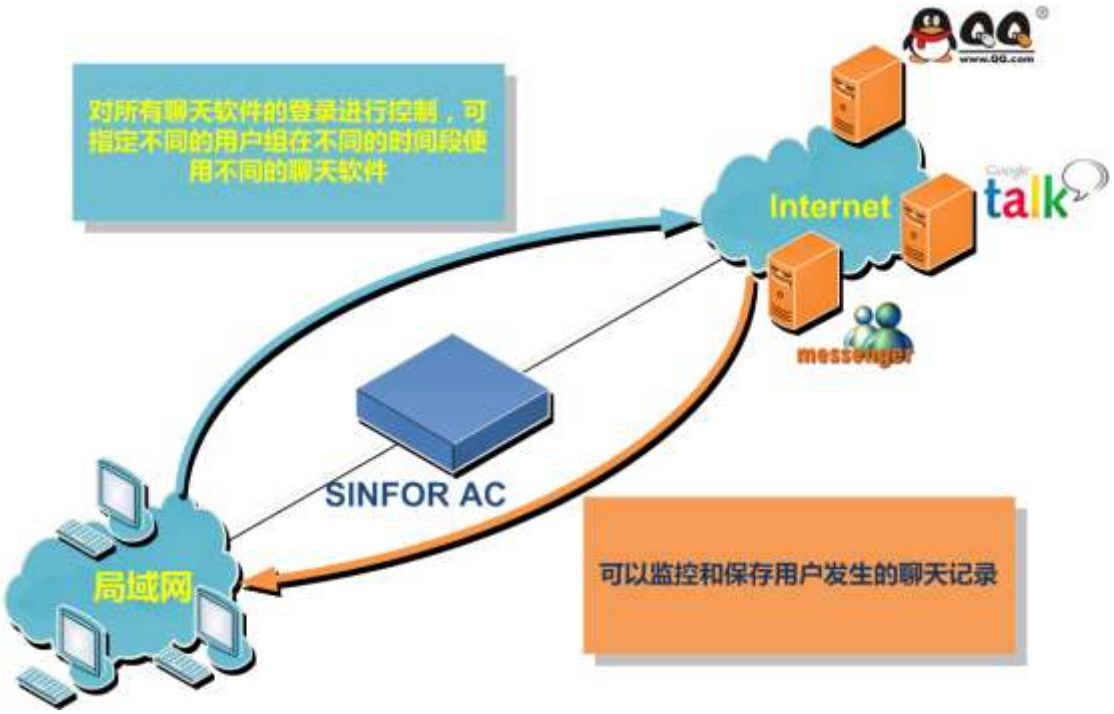
对于在工作时间不需要和外部频繁交流的某些部门，例如财务部、开发部，你可以控制他们对 IM 的使用。IM 协议的设计让使用者几乎能在任何网络情况下都能进行交流，利用现有的网络安全产品来控制非常困难。一些管理员试图通过关闭防火墙上 IM 流量的端口来禁止，但 IM 应用能够通过智能检测端口，自动转到其它防火墙上必须打开的供用户上网的端口上进行通讯，例如 80、443。AC 的行为诊断（Behaviors Diagnosis, BD）技术能够跟踪 IM 软件所使用的端口和相关协议，通过对行为的分析智能判断哪些端口使用的是标准 HTTP/HTTPS 协议，哪些端口在运行 IM 软件，进而非常有效的封掉 IM。而还有一些聊天工具使用的是标准的 HTTP 方式登录，这更让大多数的封堵方式望洋兴叹。这时，你需要做的就是借助 AC 的深度内容检测（Thorough Content Detection, TCD），这个功能将分析聊天工具发送和接受的数据包特征，只要你允许，AC 将通过过滤 IM 的关键字段来实现彻底封锁。

✓ **监管**

对于使用 IM 作为工作手段的部门，例如公关部门、市场部门等，我们希望他们可以利用 IM 进行更有效的商务活动，然而，对于一些通过 IM 泄露组织机密的行为也是管理者不愿看到的，我们需要用 AC 来进行进一步的管理。

我们可以通过设置用户组的时间计划来管理 IM，比如对企划部开放每天中午和下午 16 点至 18 点的 QQ 使用权限。对于全天都需要使用 IM 工具的部门和个人，我们一方面选择完全置之不理，这主要是对于总裁、CEO 级别的高管人员，他们不希望网络部门的人对他们的网上行为做出任何限制；

另一方面，我们可以使用 AC 的聊天内容同步侦听（Real-time Monitor for Messages， RMM)来实现对聊天内容的监督和记录。AC 的 RMM 技术是目前业界最有效的监控技术之一，通过与网络准入规则（Network Admission Rules, NAR）的配合，RMM 可以实现对腾讯 QQ、MSN Messenger、网易泡泡（POPO）、新浪 UC、ICQ、Skype、Google Talk、Yahoo！Messenger 等一系列主流 IM 的聊天内容监控。



强大的手段往往涉及到个人隐私，我们建议您在使用 AC 前向您的组织发出通知，让你的每一个员工了解到他们在工作时间发生的网络行为是可以受到监视的，这可以起到提醒的作用。

当然，最好的管理是不需要管理，这也是深信服科技（SINFOR）的 AC 产品期望为用户带来的最终意义。当 AC 成为您网络中的一部分时，员工将意识到其在工作时间的网络行为有可能被审计和记录，便会主动减少上班时间的“无用功”，自觉地提高自身的工作效率。

✓ **安全性审查**

IM 带来的安全性问题同样不容忽视。根据 IMlogic 的统计，2005 年，针对 IM 和 P2P 软件的安全攻击达到 2403 起，其中 IM 的安全威胁比上一年增加了 1693%。当你兴奋地打开 IM 中好友向你发送的文件、图片、网址等诱惑性的信息后，蠕虫（Worms）、病毒（Virus）和木马（Trojans）像打开的“潘多拉盒子”一样涌入你的电脑，进而再次感染你好友列表上的所有人。

如果你不想让局域网变得混乱不堪，你可以通过 AC 来避免 IM 的安全性隐患。首先你可以将 AC 的 URL 控制同 IM 进行联动，当你通过在线升级 AC 的 URL 或者将一个危险网址添加到 AC 的 URL 库后，即使你的员工点击了好友消息中的可疑链接，AC 的网页浏览控制也不会允许用户访问到危险地址。其次，通过在 TCD（深度内容检测）中选取特定的规则，你可以对借助 QQ、MSN 等进行的文件传输进行有效管理。例如，你可以允许你的内网用户通过 IM 软件向外界发送文件，但其无法通过 IM 接受外网发送来的文件。另外，你也可以启用 AC 的网关杀毒功能进而更大程度上尽量避免蠕虫和病毒的入侵，这个内容将在后面的“更多的安全机制”章节提到。

3.7 应对 BT 类软件

P2P 是让人又爱又恨的网络技术。在内网 P2P 下载泛滥时你甚至想揪出 P2P 技术的发明者痛斥一顿，而当你想要下载一部 80 年代的经典老片时，你脑海里第一个浮现的工具也是 BT 或者电驴。

P2P 技术对带宽资源的争用使局域网有限的带宽被耗尽 ,无论你的带宽是 1M、10M 还是 100M，只要缺乏对 P2P 的有效管理，你内网的用户永远会抱怨带宽不够。P2P 的封堵应该是所有安全网关都需要关注的问题。

对 P2P 常用的封堵方法是端口封锁和种子服务器地址（IP）封锁。通过在访问控制列表（ACL）中对 6881 - 6890 端口、6969 端口的封堵，可以实现对一些使用静态端口的 P2P 软件的封锁。但更多的 BT 类软件在端口被封后会尝试使用 HTTP 的常用端口来进行连接 ,例如 8080 ,8000 ,甚至 80 端口 ,一味的端口封锁将会导致某些正常 HTTP 服务无法使用。而种子服务器的封锁是一种吃力不讨好的体力活，每天涌现出的大量种子服务器会让网管人员忙得焦头烂额。

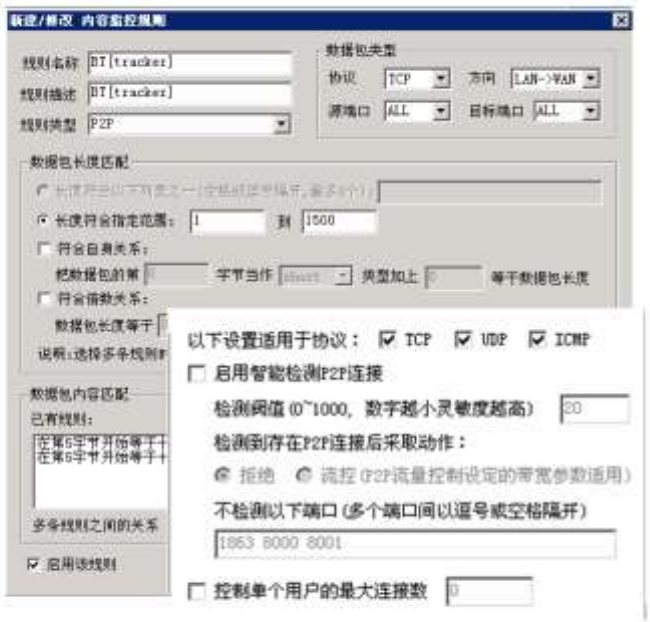
更有效的 P2P 封堵方法主要有两种，一种是基于应用协议和数据包的分析，另一种是针对流量进行检测。AC 可提供这两种封堵方法。

首先，AC 的深度内容检测服务（Thorough Content Detection, TCD）可以对 BT 类应用的数据包进行深入检测。TCD 通过分析 IP 数据包首部的服务类型、协议、源地址、目的地址以及数据包的数据部分，实现了从四层到七层的全面内容检测，能够更好的发现哪些服务是 P2P 类应用，而不再使封堵仅限于对端口的分析和封锁。

由于 TCD 技术将对数据包进行深入分析，当内网用户发出的会话较多时，网关设备也将花费较多的资源来处理更多的数据包。为了避免大量的数据包分析带来的资源消

耗，AC 采用了网络流量智能分析技术(Network Traffic Intelligence Analysis，NTIA）。区别于端口封堵和内容检测，NTIA 技术将对每一个用户和用户组的网络连接情况进行分析，当网络流量和网络连接超出 AC 规定的阀值时，用户的 P2P 行为将被限制流量。

一些 P2P 封堵技术实现了对某些 BT 类应用的“杜绝”，例如 Cisco 采用的 NBAR，NBAR 将对 BT 和电骡产生的数据包丢弃而不是管理，但更理想的方式应该是合理的利用 P2P 技术为我们的资源共享服务。我们上面提到的深度内容检测（TCD）和网络流量智能分析（NTIA）都能够提供给用户更多的选择。当 AC 确认某些用户在下载 P2P 文件时，网管员可以采取三种策略，首先是允许下载，这是对 VIP 和紧急用户的特权选项；其次是拒绝，你可以选择对某项 P2P 服务彻底封堵；最后是流量控制，即内网的用户可以使用 P2P 类软件，但他们产生的流量和连接能够被控制在一个可以接受的范围之内。



3.8 控制其他的网络应用

Internet 上的网络行为还远远不止以上提到的内容。需要管理者关注的还有网络游戏、在线视频（MMS、HTTP Streaming、RTSP 等）、在线炒股等应用。

AC 的深度内容检测（TCD）已经自带了众多应用程序的数据特征文件，通过对用户组的访问控制设定，你可以轻易地允许或者拒绝内网用户访问特定的网络服务。作为一种面向客户的开放式解决方案，AC 提供给用户更丰富的自定义功能。在 TCD 的高级设置中，AC 允许有编程基础的网络管理员添加、修改和导入自定义的网络应用规则。如果局域网内有人使用非公开工具进行不正当活动，通过分析其工具的数据内容，AC 同样可以实现封堵和控制。

3.9 防止机密泄露

通过深信服科技 2006 年 3 季度的调查，在工作时间的互联网机密泄露事件中，9%的事件通过 BBS、个人博客泄露，14%通过 ftp 等文件传输方式泄露，22%通过客户端邮件和 Web 邮件泄露，还有 31%是通过 IM 聊天工具发送给好友。

只要你允许员工上网，就有可能打开机密泄露的大门。对薪水的不满、同管理人员的摩擦或者是个人情绪的不稳定，都可能导致员工在互联网上泄露涉及知识产权、内部政策、产品报价的重要信息。

在“管理即时通讯工具”章节中，我们已经提到了如何管理聊天工具的消息内容。而在文件传输、邮件和 HTTP 页面的访问过程中，AC 也采取了丰富的内容检测措施以防内网机密泄露。

FTP 泄密事件经常发生，一个研发（Research & Development）部门的人员可能通过 FTP 将公司新产品的源代码发送给合作伙伴甚至是竞争对手。在 FTP 的防护措施上， AC 可以通过关键字和文件类型的设定来限制 FTP 的传输内容，对于内网通过 FTP

上传到公网的内容，AC 将进行记录和保存，以便更好的对违规、违法员工进行网络行为追踪，进而更好的保护组织资产。

在邮件的发送中，AC 可以启用邮件延迟审计（Postponed Sending after Audit，PSA），通过 PSA 技术，内网的邮件将收到更为细致和全面的审查，以避免机密信息的不慎或有意泄露。具体内容您可以参考下一章的“邮件延迟审计技术”介绍。

BBS 的访问主要分为 Web 登录和 Telnet 登录，对于 Web 方式的访问，AC 同样可以通过对关键字的审计来限制内网用户的发帖行为，例如包含反动、邪教、色情的关键字将无法通过内网发到 BBS 论坛中；而对于 Telnet 方式的登录，AC 亦可以记录命令的详细内容，以供后期的审查使用。

3.10 更多的安全机制

网络世界中每天都会出现不断变化的安全挑战，安全威胁的数量不断攀升，而对付他们的资源却十分有限。AC 提供了一种简单的、整合型的一体化扩展方案。作为内容安全的有效补充 融入了更多网络层安全策略的 AC 提供了从 TCP 3 - 7 层的全面防护。

VPN/防火墙

AC 集成的防火墙模块提供了虚拟测试功能，使误操作的几率降到最低，避免人为因素导致防火墙策略错误。而基于 **IPSec** 协议的 **VPN** 结合了深信服科技在 **VPN** 领域的多项领先技术，能够提供对网对网的连接和点对网的远程接入，通过高效率、低成本的方式实现组织和分支机构的网络互联以及内部员工的移动办公。

反垃圾邮件

AC 同样在反垃圾邮件方面作了积极的努力，通过关键字过滤技术、智能应答技术、黑白名单和指纹识别等技术，AC 可以有效地组织来自外网的垃圾邮件。

为了减少误判率，AC 通过对关键字设定阀值来完成判断过程。通过扫描结果和阀值比较，AC 将邮件分为三类：垃圾邮件（Spam）、正常邮件（Normal Mail）、可疑邮件（Doubtful Mail）。对于 Spam，AC 将直接删除。

对于可疑邮件，AC 将进一步采用智能应答技术来减少误判率，通过发送请求回答邮件来确认邮件发送者的身份。为了防止自动应答程序条件反射似的回复确认邮件，AC 还要求邮件发送者输入确认邮件中显示的随机特征码（数字和字母的祝贺），以避免自动回复程序企图伪装成正常用户来逃避 AC 的审判。

AC 的反垃圾邮件功能还借鉴了生物识别中的指纹概念。垃圾邮件多带有一些明显特征，例如含有很多广告的链接、大量极具诱惑又振奋人心的字眼，它们就是垃圾邮件的“指纹”。有些垃圾邮件程序还通过 html 等技术将一些含有垃圾邮件明显特征的内容、关键字做转换，以试图欺骗反垃圾邮件程序。AC 对邮件中的每一个字符赋予一个数值，这个数字的确定是按照特定垃圾邮件的用词规律特点进行分类的，再利用统计方法给这封邮件计算出一个综合数值，根据是否与其他多次受到的邮件相似性来判断是否是垃圾邮件，因为多次受到的邮件往往是垃圾邮件。

入侵防御系统

IPS，即入侵防御系统(Intrusion Prevention System, IPS)，是抵制外部网络威胁最有效的安全防范技术。AC 可为用户选配智能入侵防御系统，对所有流经网关的数据流进行实时检测，为企业提供了网络级的安全保护。由于采用了特征匹配、协议分析和异常行为检测等多项技术，智能入侵防御系统能够对所有可疑数据包实时阻拦，提高了对攻击行为判断的准确率，有效保证了企业的网络安全。

智能入侵防御系统对所有攻击特征库中的规则自动进行分类，分为高、中、低三个优先级别。管理员可以根据其自身网络的安全情况，对相应的优先级别规则启用 IPS 功能进行相应防御，同时还可规定发现入侵以后采取防御行为的时间间隔。一旦检测到可疑数据匹配到相应规则，则 AC 硬件网关的 IPS 系统就启动相应的防御措施。

防 DOS 攻击系统

DOS 攻击(拒绝服务攻击) ,通常是以消耗服务器端资源、迫使服务停止响应为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的。通常 DOS 攻击往往会导致服务器超负载运作，性能降低 影响正常用户的登陆 ,甚至造成服务器瘫痪。而 DDOS (Distributed Denial of Service，分布式拒绝服务) 是指攻击者从多个计算机系统上向一个目标系统同时发起攻击。因而比起 DOS 攻击，危险性更大。

通常 DDOS 攻击是由黑客手动寻找可入侵的计算机入侵并植入攻击程序 ,再下指令攻击目标。AC 不仅可以防御来自外网的 DOS 攻击，而且对于内网用户发起的 DOS 攻击，AC 也可以进行防御。通过 AC 的日志系统，管理员可以根据内网 DOS 攻击日志，查找出内网中了木马或者病毒的用户，从而及时有效地阻断由内网发起的 DOS 攻击。避免了 DOS 攻击造成的组织网络带宽耗尽，或者因发起 DOS 攻击可能产生的不必要法律纠纷。

网关杀毒

如果您的内网缺乏有效的网关级杀毒引擎，你可以考虑在 AC 中加装杀毒模块。

AC 可加载来自欧洲著名杀毒厂商的高效杀毒引擎，杀毒速度可达到 200Mb/s，大大超过大多数杀毒厂商的网络杀毒速度，也大大超过普通企业的 Internet 带宽。强大的杀毒功能支持 HTTP、SMTP、POP3、FTP、NETBIOS 等多种协议的数据流，不仅可以查杀普通病毒邮件，还可以检查出各种压缩包（zip,rar,gzip 等）隐藏的病毒，从而查找在合法内容中是否存在安全隐患。此外， AC 的杀毒功能还可以针对网站和文件类型进行灵活的设置。比如可以对于一些公认的安全网站，不启用杀毒功能。或者有选择地对某些以 exe、dll、dat 等为扩展名的容易感染病毒的文件启用杀毒。

AC 网关的杀毒引擎可指定时间每天自动升级，实现病毒库的实时更新，使 AC 更加灵活、安全地保护组织的信息资源。

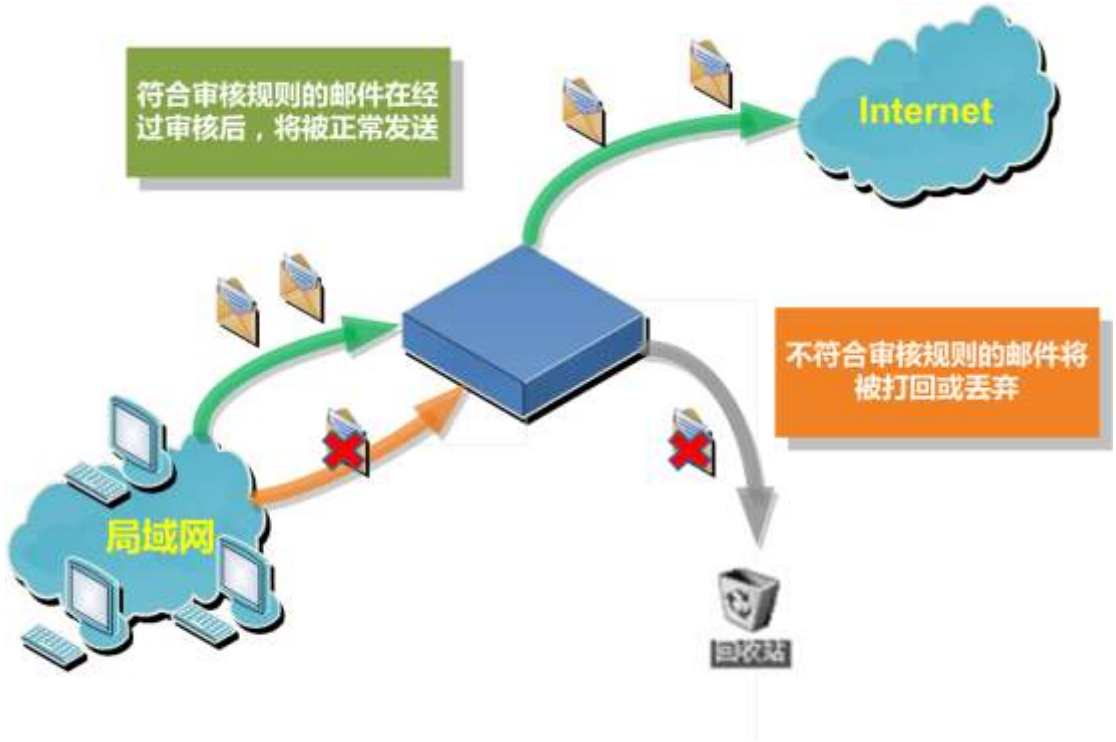
四．领先的技术优势

强大的功能源自技术的持续创新。在本章节，您将了解到 AC 的一系列深入用户需求的标杆性技术。

4.1 邮件延迟审计(PSA)

大多数的反垃圾邮件网关只能过滤“由外到内”的垃圾邮件，而对“从内到外”的邮件则完全放行，由于内网发送的邮件（Outbound Mail）存在着泄密风险，一名员工可能会把公司的商业机密发送给竞争对手，一位客户经理也可能将一份公司苦心搜集来的客户名单发送给其他组织。同普通的反垃圾邮件网关过滤单向的接受邮件相比，我们更希望能够实现“外反垃圾、内防泄密”的双向邮件过滤。

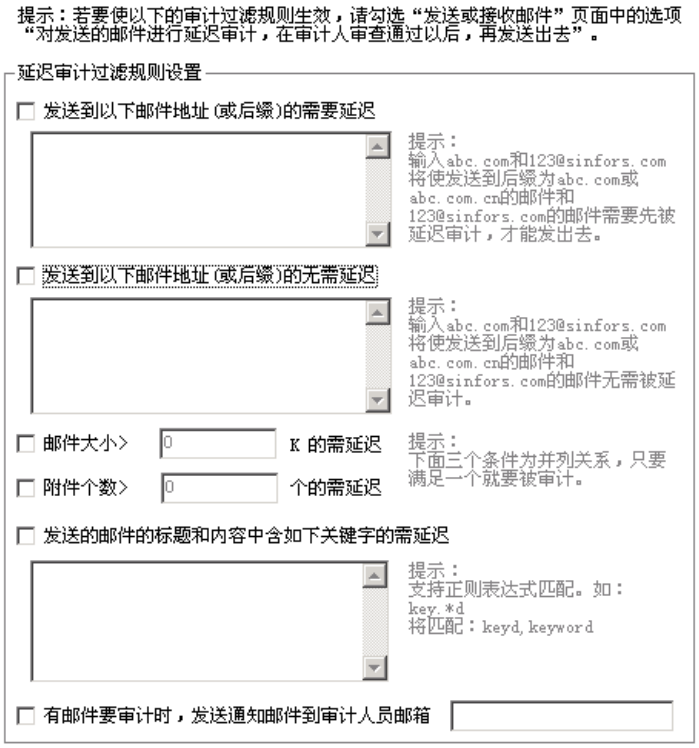
AC 集成的基于网关的邮件延迟审计技术(Postponed Sending after Audit, PSA ）为企业级用户提供了邮件内容防护的可靠途径。PSA 采用了邮件转移技术，内网用户发送的邮件会首先被 AC 网关转移至网关的邮件缓存区，邮件审核人员通过系统口令访问邮件缓存区并审核邮件正文及其附件，那些涉及到机密信息、侵犯性语言、非法 URL、个人隐私的邮件将被返回给发件人或者丢弃。而这一审核过程对局域网中的用户是完全透明的，邮件的发送过程和以往并没有任何不同。



你还可以对 PSA 做细粒度的审核机制，例如需要进行邮件审核的发件人、收件人以及邮件的特征。

PSA 提供对收件人和发件人名单的编辑。你可以对特定部门和特定员工启用审核功能，因为你的老板也许不希望自己的邮件行为受到他人监控。同样，你还能够对邮件的收件人进行黑白名单控制，如果你认为 somebody@trust.com 是一个可以值得信赖的收件人，那么所有发送到此地址的邮件将不会被 PSA 进行延迟处理；相反，如果 somebody@suspect.com 是一个可疑的收件人，任何人发往此地址的邮件都将被转移到邮件缓存区以待审核。

而邮件特征的定义细致了 PSA 的对象定义粒度。你可以调整需审核邮件的正文和附件大小以及邮件的关键字特征，例如你可以设定一条规则，只有正文中含有“Code”而且正文和附件大小不低于 10K 的邮件才需被 PSA 审计。



由于 PSA 涉及到人工的审核操作，所以邮件的延迟发送时间也是可控的，当有邮件进入缓存区等待审计时，AC 将通过邮件等方式通知邮件审核人员，如果邮件审核人员在长时间没有登录审计，待审计邮件将被 AC 自动发出，避免重要邮件被延误。

4.2 网络准入规则(NAR)

AC 的网络准入规则（Network Admission Rules, NAR）通过对客户端的评估来实现网络访问控制，并更好的维护网络安全防线。

NAR 的设计意义在于三个方面。

首先，仅靠网络边缘的外围设备已经无法保证安全性。提供边界防御的安全网关无法保护内部网络段，也无法替代内容安全防护措施。即便组织的网络出口处运行着防火墙等网络周边安全设备 ,病毒和蠕虫、特洛伊木马、等基于内容的恶意行为仍频繁渗入组织内网。

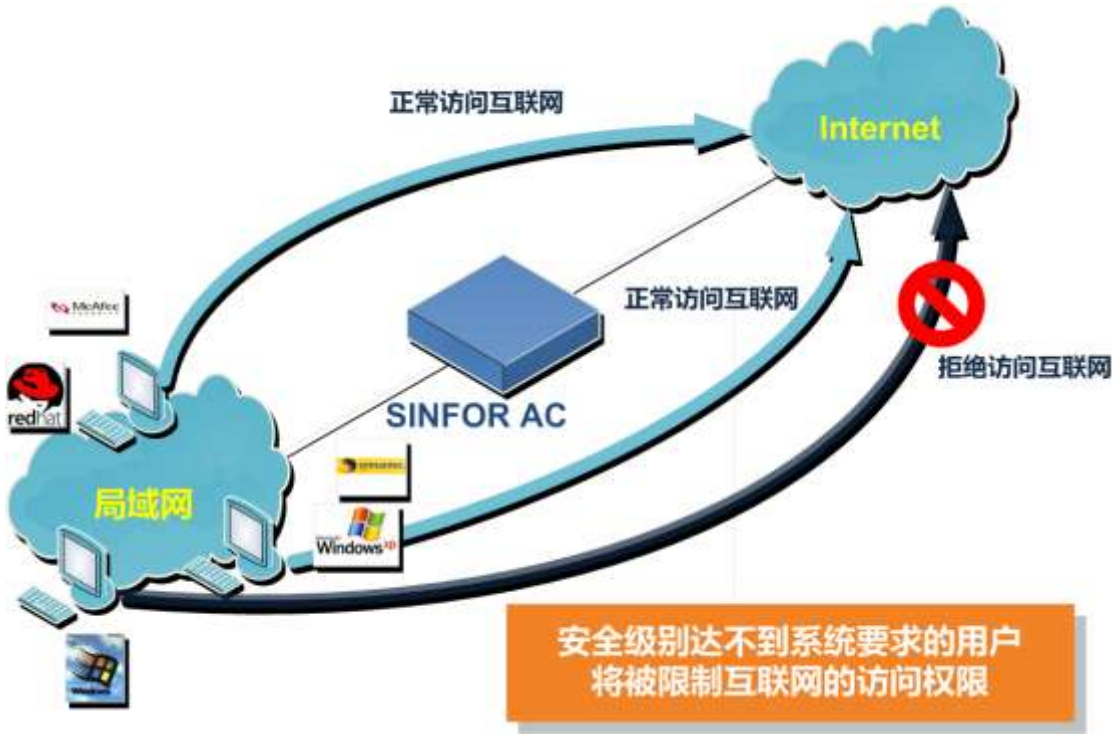
其次，边缘网关设备无法防止来自局域网内部的滥用、攻击和破坏。同时，日益提高的安全过滤和控制要求，以及不断增加的带宽需要，也给网关性能带来很大

压力。

最后，客户端的安全级别往往难以保证，这对于内网用户数量众多的组织更为如此。使用版本陈旧的操作系统、长时间不更新个人防火墙和杀毒软件、应用具有潜在安全漏洞的软件，这些都将成为局域网安全中的“短板”。

基于此，AC的NAR通过对端点安全评估和访问策略列表来实现全方位的安全防护。

当启用了AC的NAR功能后，内网用户第一次发起互联网连接请求时，NAR将动态分发准入代理（Sinfor Ingress Agent， SIA）至客户端主机。SIA是轻量级软件代理，用于确定端点是否遵从管理员设定的安全策略，SIA中可配置用于检查预定义的和可定制的标准，包括操作系统、运行程序、系统进程、注册表的存在/版本/补丁等。当SIA将搜集到的客户端信息传回AC网关后，当内网用户的端点安全状态不符合SIA的规则设置时，AC将对相应用户执行预定义的策略，放行或强制关闭某项程序或进程。



如果你的一位内网用户矢志不渝地使用某些具有安全隐患的程序，而这一程序可能将病

毒、蠕虫和恶意程序从主机的桌面传播至整个网络。这时我们就可以通过NAR将此程序禁用，当用户一旦启用此程序后，用户的PC将同互联网“隔离”，只有关闭掉恶意程序才能正常访问互联网，这会使内网用户的网络行为更规范。

而NAR提供的可定制的网络行为标准可以给网关管理者更多的权限和扩展性，通过对程序、注册表、进程的自定义，NAR可以管理几乎所有的终端在线状态，使安全策略更有效地同整体安全防御体系结为一体。

4.3 数据中心(NDC)

AC 的数据中心（Network Data Center, NDC）提供了基于用户的最完整的互联网访问记录。

一个能够允许用户访问互联网的系统也必须及时关注用户对网络资源的使用情况。在出现滥用、误用、盗用的行为时，完整的统计信息是必不可少的。

通过使用 NDC，组织的管理者可以通过直观的、图象化的方式了解网络带宽的利用情况以及内网用户的网络访问状态，NDC 将网络使用情况自动生成报表并统计出网络访问的趋势，以帮助系统管理员更好的维护和管理网络。

不同于其他内容安全设备的日志系统，NDC 可提供更丰富和更具扩展性的互联网内容访问记录。

NDC 可以根据组、用户、规则和协议进行多向查询，并可生成饼状图、柱状图和曲线图等方式，使内网日志一目了然。对于日志的统计对象，NDC 提供了对流量、邮件、网络监控、准入规则（NAR）、IPS、防火墙、日志库、用户信息等 9 大对象的统计和查询。你可以了解局域网中发生的绝大多数网络行为，以便对内网进行更好的规划和管理。

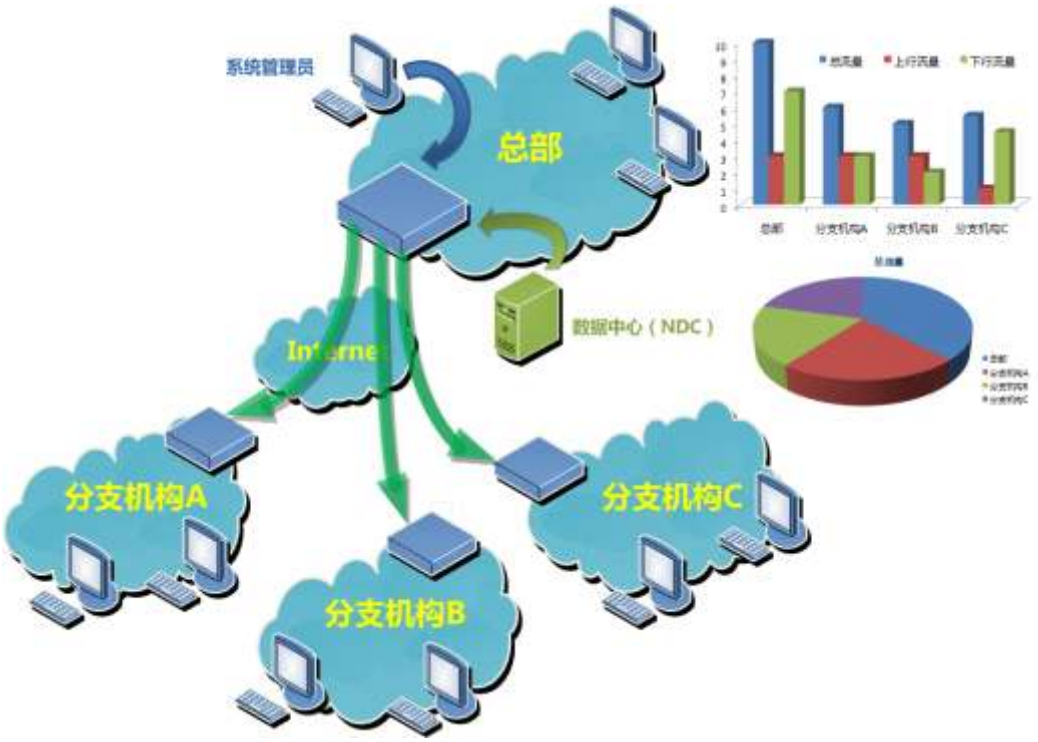
NDC 系统是一个可移植的日志平台。大规模的局域网访问将产生大量的网络日志，一个 PC 数目以 K(千)为单位的局域网 其一天内的互联网访问日志也将程指数倍增加。AC 内置的 NDC 系统可以移植到专门的日志记录服务器中 这将给组织带来多种好处。

首先，将日志记录完全整合到网关中会影响网关的性能，尤其是大规模查询和统计将占用极高的系统资源；其次，由于国内大多数机构都需要遵守公安部在 2006 年 3 月 1 日颁布的 82 号文件，即需要利用信息安全技术保留 3 个月的网站访问日志，以便

调查取证。而 90 天的日志对于网关内置的存储空间提出了挑战，对内网规模较大的用户， 9 天的存储都将成为问题。NDC 的可移植性使日志的存储不受网关硬件配置的限制，只要你有足够的硬盘，你可以使日志内容无限大。

NDC 提供对日志记录的导出和在线打印 ,你可以把统计和查询结果打印成文本，使对内网情况的报告更加方便，也更便于日志的储存。

AC 支持异地管理和维护，NDC 同样也能够查询远程的网络情况。这对于有多个分支机构的组织来说极为方便，管理员可以在通过 Web 方式实时地了解不同分支机构的网络运行状况和网络行为日志，并将日志记录统一导出，形成整个组织的网络行为分析记录，进而制定出细化的、多层次的安全策略。



4.4 单点登录技术(SSO)

值得肯定的是, AC 产品线的开发人员将单点登录技术同认证机制结合在了一起，让通过域认证的用户可以更加方便的实现 Web 认证。

我们每个人都有一套密码字典，银行卡取款密码、信用卡查询密码，PC 的登

陆密码，办公自动化系统的密码，机密 Word 文档的密码。。。过多的密码带来了对员工记忆力的挑战，一个解决办法就是找出一张白纸把所有密码都记下来，然而这张白纸却可以轻易泄露你的一切。单点登录技术(Single Sign On, SSO)可以更好的解决这个问题。通过在 AC 的活动目录中配置单点登陆选项，当你的主机登陆到域中便自动通过了 Web 认证，而不需要重复输入用户名和密码。

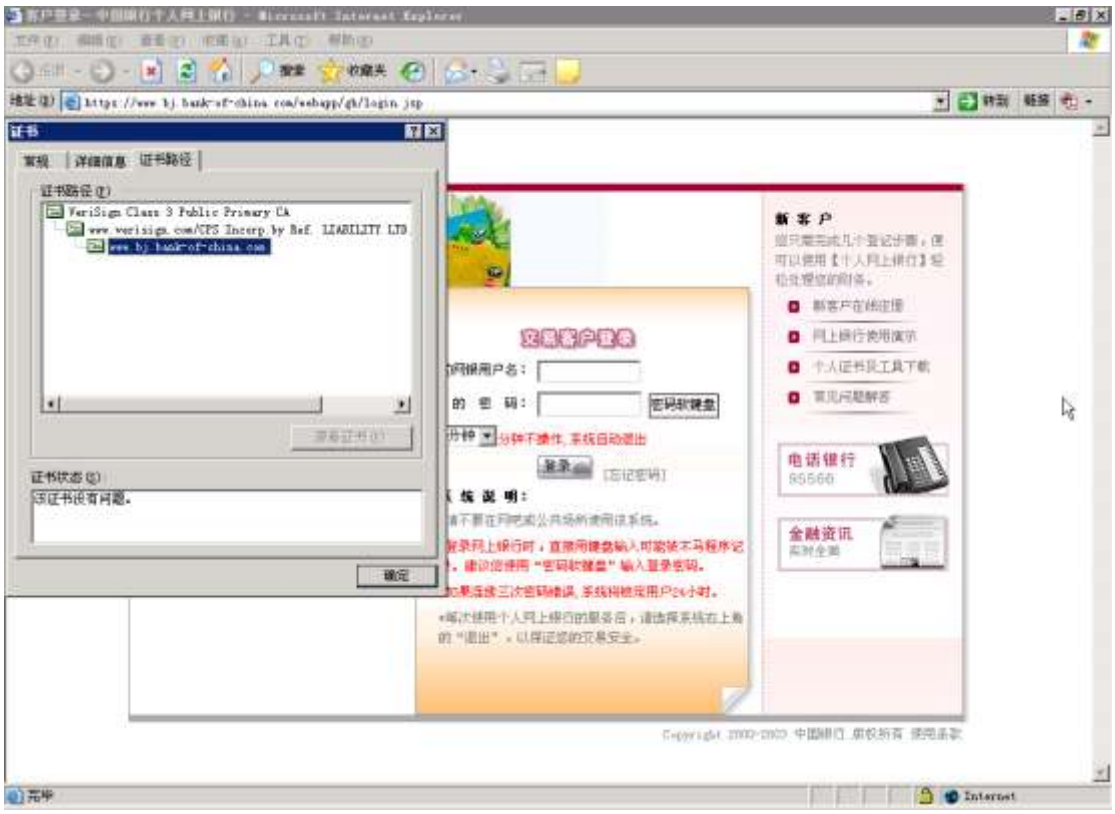
同样，POP3 的认证也实现了单点登录。构建了邮件服务器的用户都有一套邮件帐号，当 AC 把邮件服务器的帐号导入后，用户每次使用 Web 认证时只需要输入邮件的帐号即可访问互联网。另外，AC 考虑了更人性化的措施。当内网用户使用 Outlook、Foxmail 等邮件客户端成功登录到邮件服务器后，他（她）将自动通过 Web 认证。

4.5 反钓鱼网站功能

中国金融认证中心近日发布的《2006 中国网上银行调查报告》显示，虽然在过

去的一年中国内网上银行快速发展，但有 61%的受访者仍然不敢使用网上银行。安全问题仍然是非网银用户最担心的。据统计，网络钓鱼已经成为目前亚太地区（除日本外）银行业增长最快的非暴力犯罪行为之一。”钓鱼者”通过制造出与网上银行、网上购物等网上交易页面极其相似的界面，使用户在毫不知情的情况下泄露出自己的账户信息（账号、密码），导致银行资金被“网络姜太公”轻易盗取。

网上银行采用数字证书的加密方式来保障用户的交付安全，由于采用了可信的第三方机构颁布的数字证书，浏览器的右下角会出现一个黄色的小锁头。而一些钓鱼网站的地址也是采用 HTTPS 方式访问，甚至也可以在浏览器下方显示锁头标志。



很多的内容过滤设备可以对 HTTP 页面进行过滤和阻拦，而对基于 SSL 加密的页面无法审计，使钓鱼网站仍然可以穿透过滤系统进而欺骗网银用户。AC 通过对钓鱼网站的数字证书和数字签名进行审核和对照（专利号：200610062252.2），能够有效地防止钓鱼网站对用户的欺骗。

AC 内置的 SSL 库内置了可信任证书颁布机构列表，并可对 SSL 连接的证书内容进行可信度评估，如身份验证机构的标识信息、证书有效期、证书持有人的公钥、证书的签名和算法。当钓鱼网站采用了伪造的数字证书来骗取内网用户信任时，AC 可以判断出其本来面目并进行阻断，避免组织成员蒙受经济损失。

4.6 代理服务器识别

很多组织的内网用户通过 Microsoft ISA、Sygate、CCproxy 等代理服务器(Proxy Server)上网 ,这些软件在完成其代理任务的同时也给其他安全设备的管理带来了困难。由于防火墙、内容控制等设备对内网用户的管理是基于目的地址和端口的，当内网用户通过代理上网时所有数据是发向代理服务器的，这将使防火墙、内容控制设备的某些模块无法正确识别内网数据的真正流向，进而失去应有的防护作用。

对于通过 Proxy Server 代理上网的情况，AC 可以很好地适应并发挥其作用。AC 提供给网络管理员一个可编辑的界面，以将网络出口情况定义给 AC 的控制系统，AC 的控制系统通过正确识别用户的网络拓扑而做出正确的判断和管理。

4.7 智能排障技术(IBF)

错误配置引发的故障难以诊断和排除，这一点网络管理员一定深有体会。

内容安全产品的管理对象是天天翻新的应用软件、以及比软件更新速度快得更多的员工行为，虽然成熟的内容安全产品提供出厂默认设置和在线更新功能，但设备的主要操作人仍然是网络管理人员。网管员希望通过内容安全设备完成尽可能多的功能，虽然他们对产品的本身知之甚少，过多的尝试会使错误配置的发生几率大幅度上升。

AC 提供给网管人员“预知和补救”的机会。AC 的状态监测防火墙支持虚拟测试（Virtual Test）功能，网管员可以在 AC 提供的虚拟网络环境下测试各项配置，以得到配置在实际网络中的运行效果，例如一条规则是否会导致一个 Vlan 下的用户无法使

用 HTTP 服务，或是向公网某个 IP 段的用户敞开了进攻内网的大门，所有这些都可以在 AC 的虚拟环境下得到预先测试。

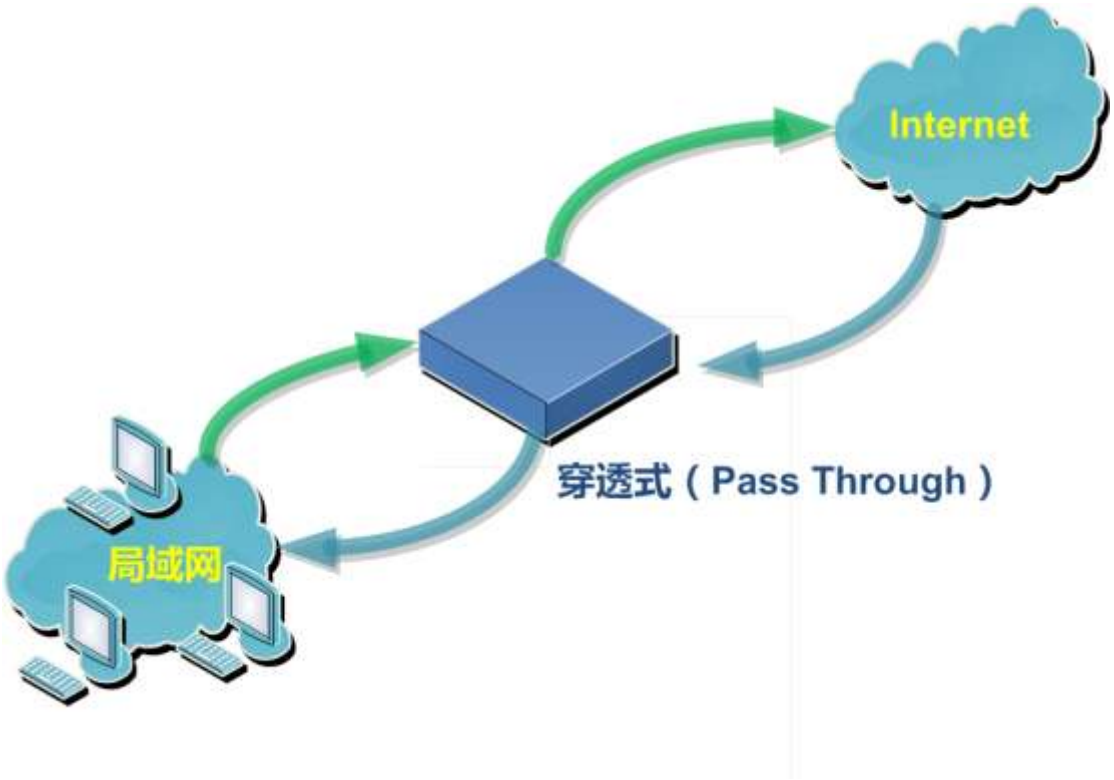
而 AC 的智能排障（Intelligent Barrier - Free, IBF）技术帮助管理员查找错误配置的源头。当内网的某个用户或用户组出现无法正常上网、个别网络应用不能正常运行时，网管员都可以借助 IBF 来反向查询障碍的原因 ,查询数据包是否被网关的某个模块拦截，为何被网关拦截，或者其他产生故障的原因等等，进而可以帮助网管员尽快的检查出问题的症结所在，迅速的排除和解决障碍。

五．部署您的 AC 产品

在深信服科技（SINFOR）的数千个用户中，从没有发现过两个完全相同的网络环境。作为保护组织网络资源的核心设备，AC 考虑到了各种可能的网络拓扑，并力求部署的最简化。

穿透式（Pass-Through）部署

穿透式部署将设备部署在局域网的主干部分以处理流经设备的数据流



✓ **网关（Gateway）模式**

网关模式适用于希望通过 AC 产品来实现所有的审计、控制和拦截功能，且对网络拓扑的更改不敏感的用户。

网关模式将 SINFOR AC 作为局域网的出口网代理内网 PC 上网，除完成 AC 的管理控制功能外还可以实现 NAT、路由和防火墙等网络与安全功能。

部署方式：AC 的 WAN 口与广域网的接入线路相连，一般是光纤、ADSL 线路或者是路由器，AC 的 LAN 口（DMZ 口）同局域网的交换机相连，内网的 PC 将网关指向 AC 的局域网口，进而通过 AC 代理上网。

✓ **网桥（Bridge）模式**

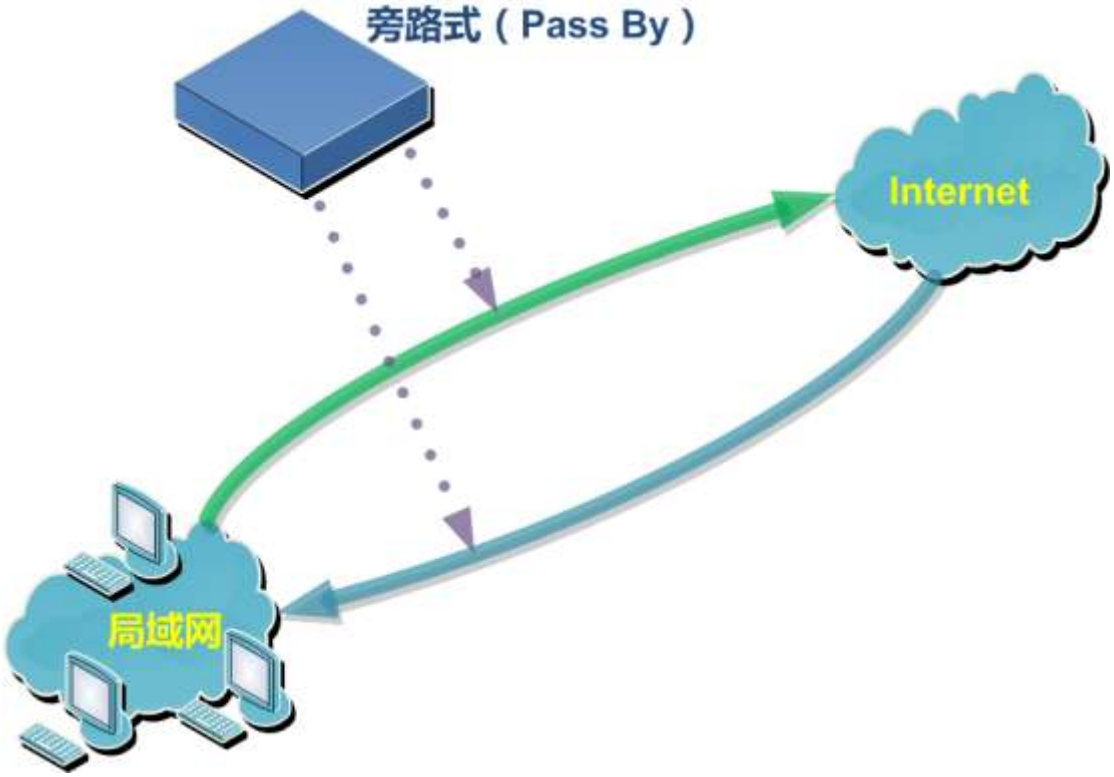
网桥模式适用于希望对内网完全监控、控制和管理，且不希望更改局域网的任何网络地址的用户。

网桥模式将 SINFOR AC 等同于一根连接在网关和交换机之间的“智能网线”，可以对所有流经 AC 的数据流进行审计、管理和控制。

部署方式：AC 的 WAN 口同局域网的网关相连，LAN 口（DMZ 口）同局域网交换机连接。局域网内的任何网络设备和 PC 都不需要更改 IP 地址。

旁路式（Pass-by）部署

旁路式部署将设备与交换机的镜像口相连，用于监听局域网中的数据流



✓ 旁路（Pass - by）模式

旁路模式适用于希望通过 AC 来实现内网监控和审计的用户。

旁路模式的部署不需要对内网拓扑作任何改动，使实施难度最低。而由于内网数据流不需要流经 AC 设备，避免了网络主干中设备过多引发的网络处理性能下降，也降低了网络单点故障的发生几率。

部署方式：在出口交换机中配置镜像端口，将 AC 的广域网口同镜像端口相连，实现对内网数据包的监听。

六．为何选择深信服科技

深信服科技有限公司（SINFOR）旨在提升商业用户的互联网带宽价值。凭借前瞻性的设计、创新的技术和高性价比的解决方案，深信服科技（SINFOR）已经成为国内上网行为管理、SSL/IPSec VPN、网间加速方面的领导者。通过在互联网边界领域的不断探索和创新，深信服科技（SINFOR）在协助用户提高生产力的同时，进一步增加了用户的商业投资回报。截至 2006 年 4 季度，已有超过 7000 家的用户采用了深信服科技（SINFOR）的解决方案并从中获益。

深信服科技（SINFOR）于 2004 年底推出了 AC 上网行为管理产品，定位于帮助用户实现对核心网络资源的保护，规避不良行为带来的法律风险，在使组织工作效率获得有效提升的同时更好地保障了网络带宽的安全和稳定。目前，深信服科技的 AC 产品已经成功运行在政府、教育科研、电信、金融证券、电网电力、石油石化、制造等行业，是安全防范意识强、需要管理和控制互联网访问的用户的第一选择。