1 深信服上网行为管理–上网行为管理第一品牌

A 深信服科技简介

深信服科技有限公司是中国规模最大、创新能力最强的前沿网络设备供应商，致力于通过提供品质卓越的Internet网络设备，帮助用户的业务向互联网成功转型。

作为一家专注于广域网市场的厂商，深信服提供了贯穿用户广域网建设生命周期的前沿产品及解决方案，包括IPSec VPN、SSL VPN、上网行为管理、上网优化、广域网加速、应用交付、流量控制等，并被公认为其中多个领域的技术及市场领导者。

截止2010年5月，已有超过16,000家用户选择了同深信服合作并取得了显著收益。这些用户包括中国移动、通用电气、壳牌石油、丰田汽车等世界500强企业，也包括中国人民银行、国资委、招商银行、南方航空、中国人民大学等中国知名用户。

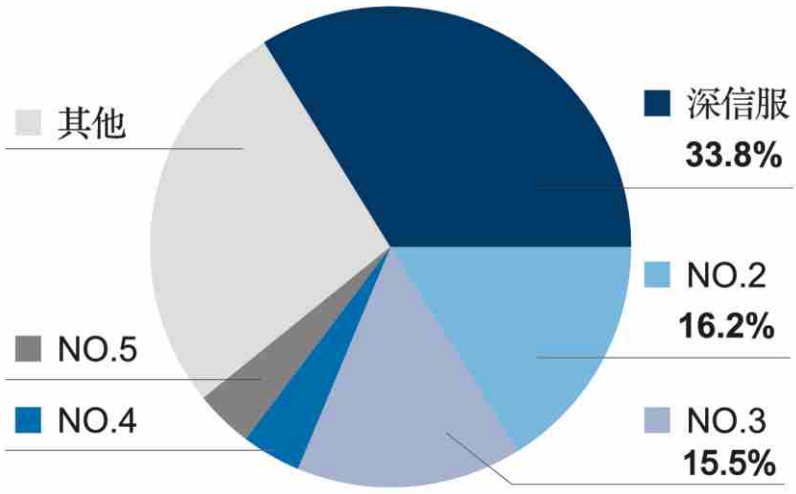
目前，深信服公司总人数已达900余人，在全球设有40个直属代表处，包括中国内地主要城市及英国、新加坡、马来西亚、泰国、香港等国家和地区。

2005－2009年,深信服连续五界蝉联德勤“中国高科技高成长50强”、“亚太地区高科技高成长500强”,并荣获渣打银行”最具成长性新锐企业“中型企业金奖、《computer world》”中国 ITC十强“、《财富》杂志”卓越雇主奖“等，众多大奖。

B 上网行为管理市场占有率第一

在安全内容管理硬件市场，有超过17家主流安全厂家可以提供该产品，排在第一位是深信服，市场占比为33.8%，为第二位厂商的两倍以上,超出达17.6%。“安全内容管理硬件市场精简格局，2009年下半年”如下图所示。

安全内容管理硬件市场精简格局,2009年下半年



C 不断创新的上网行为管理产品

在核心技术创新方面，深信服科技申请的上网行为管理领域相关发明专利数已超过6个，并不断增加中，在业内遥遥领先。

专利：

ZL 200510037455.1 **一种在网关、网桥上实现用户安全接入外网的方法**

ZL 200610061591.9 **一种基于网关/网桥的线路自动选路方法**

ZL 200710072997.1 **基于网关、网桥防范网络钓鱼网站的方法**

200810141807.1 **一种网路插件的安全检测方法、系统及安全检查设备**

200810241565.3 **一种在网关进行数据安全检测方法、系统及设备**

200910108672.3 **一种网络数据流识别方法**

2005年深信服创造了“上网行为管理”这一品类，经过持续创新和发展，共历经12个大版本、25个小版本，不断完善着“上网行为管理”的概念，引领着整个行业产品的理念、技术的发展方向。

2 部署上网行为管理的必要性

A 防止带宽资源滥用

根据第三方数据显示，各国P2P流量均占互联网总流量的49%到83%，其中近20%是加密P2P在传输。在办公网络内，迅雷、在线影音等P2P行为时常将组织有限的带宽资源挤占殆尽，传统方式难以控制，不仅用户上网体验不佳，且基于网络的大量办公应用更是受到严重影响，阻碍了日常工作的正常开展。深信服AC通过基于应用类型、网站类别、文件类型、用户/用户组、时间段等的细致带宽分配策略限制P2P、在线视频、大文件下载等不良应用所占用的带宽，保障OA、ERP等办公应用获得足够的带宽支持，提升上网速度和网络办公应用的使用效率。

B 防止无关网络行为影响工作效率

上班时间玩游戏、网上购物、看网络视频，长时间进行IM聊天，严重影响工作效率；越来越多的网页游戏更进一步加大了网络行为管理的难度，办公室几乎成了免费的网吧。AC基于用户/用户组、应用、时间等条件的上网授权策略可以精细管控所有与工作无关的网络行为，并可根据各组织不同要求进行授权的灵活调整，包括基于不同用户身份差异化授权、智能提醒等。

C 记录上网轨迹满足法规要求

随着互联网的使用日渐融入我们的生活和生产，组织对内网用户通过互联网外发信息的监管需求也越来越大，对组织的网络行为记录能力提出了比以往更高的要求。深信服AC可以帮助组织详尽记录用户的上网轨迹，做到网络行为有据可查，满足组织对网络行为记录的相关要求、规避可能的法规风险。

D 管控外发信息，降低泄密风险

随着网络的普及，各种各样的“泄密门”已经屡见不鲜。据公安部数据，有63.6%的企业用户处于“高度风险”级别，我国每年因网络泄密导致的经济损失高达上百亿，而机密信息的泄漏往往给组织带来致命打击。AC充分考虑网络使用中的主动泄密、被动泄密行为，从事前防范、事中告警、事后追踪等多方面防范泄密，为组织保护信息资产安全，降低网络风险。

E 掌握组织动态、优化员工管理

Internet是反映员工思想动态的风向标，传统的审计方案无法帮助组织有效分析员工的行为动态，深信服通过风险智能报表来自动发现存在离职风险或有工作效率问题的员工，并通过关键字报表和热贴报表来反映员工思想动态。风险智能报表能够自动提示管理者关注离职倾向、泄密风险、工作效率降低等员工管理风险，而关键字报表和热贴排行等报表将有助于组织深入了解员工的思想动态，并以此为基础实施组织文化建设、制度改进等针对性措施，从而提高员工管理水平。

F 为网络管理与优化提供决策依据

出口带宽总是跑满，又要扩容了吗？重要的业务应用是否得到了足够的带宽保证？组织内谁使用网络最多、工作效率最低？不了解网络就无法及时发现并解决问题，更无法决策如何实现网络的有效管理与持续优化。深信服上网行为管理产品提供了丰富的网络可视化报表，能够提供详细报告让管理者清晰掌握互联网流量的使用情况，找到造成网络故障的原因和网络瓶颈所在，从而对精细化管理网络并持续加以优化提供了有效依据。

G 防止病毒木马等网络风险

互联网风险日渐突出，与此同时用户终端因为个人习惯或风险意识薄弱等多种因素导致终端安全强度不够造成安全短板，组织虽然部署了大量安全产品，但安全威胁总是被用户主动“请”进内网，网络中病毒/木马横行、ARP欺骗频发，传统管理手段和方法已经无法有效应对各种新式安全风险，Internet已经成为造成内网安全事件的主要来源。通过部署深信服AC，利用其内置的危险插件和恶意脚本过滤等创新技术过滤挂马网站的访问、封堵不良网站等，从源头上切断病毒、木马的潜入，再结合终端安全强度检查与网络准入、DOS防御、ARP欺骗防护等多种安全手段，实现立体式安全护航，确保组织安全上网。

H 低成本且有效推行IT制度

完善细致的IT制度，在组织内却得不到执行，网络问题仍然不断出现。如何防止精心制定的IT管理制度成为一纸空文，将组织的IT管理带上一个新的台阶，这一直是困扰IT管理部门的问题。深信服AC能够实现用户网络权限的细致分配以及带宽的优化管理，通过事前精细规范、事中智能提醒、事后报表呈现等手段实现有效管理；通过将是否具备上网权限与用户对IT制度的遵从情况进行绑定，强制要求用户遵从组织IT制度里的各项细则规定（如必须安装指定的杀毒软件或桌面管理软件等），并且可以根据组织要求进行各种智能提醒，通过创新技术的应用，让IT管理制度融入每位用户的日常工作中。

3 深信服上网行为管理产品优势

专业上网行为管理是涵盖网关与终端、行为与内容的整体方案，所以深信服AC产品提供包含“用户识别+终端识别+应用识别+内容识别”的完整技术方案，结合包含授权、流控和审计在内的全面灵活的管理手段，帮助客户轻松应对互联网挑战。

识别能力最强

深信服AC拥有国内最大的应用识别规则库，能够识别数百种主流网络应用，除能够识别各种常规应用外，还能有效识别各类加密应用，例如访问通过SSL加密的网站、BBS发帖、外发加密邮件，AC都能实现基于关键字的过滤；AC也可以有效识别并控制现在越来越流行的自由门、无界浏览器等加密代理软件；Google的数据表明互联网上有一万亿个独立网页，因此只有千万级的静态URL库是远远不够的，AC具有网页智能识别和分类技术，能够自动识别用户访问的网页内容并进行分类，从而有效解决海量URL的管理问题。

管理最智能

普通的上网行为管理产品需要管理员做大量的事后分析并协调其它部门或单位领导采取各种处理措施，管理成本很高，深信服AC提供很多智能化管理手段来降低管理成本，是最智能的上网行为管理产品。

AC提供风险智能报表功能，自动发现员工工作效率下降、离职、泄密等风险，大大减少管理员的数据分析工作量；对于员工长时间聊天娱乐或是持续产生较大的网络流量，人工管理不仅麻烦而且效果很差，AC可弹出提醒对话框自动提醒员工合理控制自己的上网行为；对于组织关心的泄密问题，不管是防止员工主动泄密还是试图减少过度审计可能产生的泄密，都需要投入很大的管理成本，AC采取很多措施来解决这些问题，比如说员工通过篡改或删除外发文件后缀名、压缩或加密再外发文件泄密，AC都能有效识别，发出告警并阻断，避免泄密；通过给高层领导配发免审计Key可以避免领导被审计，通过日志审查Key来避免AC记录下来的上网行为日志和信息被私自查看。

通过多年发展，深信服AC已经在业界成为市场占有率第一，树立了识别能力最强、上网最安全、管理最智能的功能优势与技术标杆，为客户提供了互联网管理的最佳解决方案。

上网最安全

深信服AC在如何提高用户的上网安全方面提供了大量的技术保证。统计发现，现在很多安全问题是由于用户访问含有木马病毒的网页所导致，AC能自动过滤含有病毒、木马的恶意脚本或插件的网页，该特性大幅减少类似的安全隐患；可能部署AC前内网已经有电脑感染木马、病毒，成为肉鸡甚至被动泄密，AC能通过危险流量识别技术自动封堵和报警，帮助管理员找出内网隐患并采取措施解决；当然组织希望终端电脑拥有足够的安全强度来应对各种风险，AC可以通过网络准入检测终端电脑，对于不符合指定安全策略的电脑禁止上网，最大程度的规避安全风险。

SANGFOR
深信服科技

4 主要功能及创新技术介绍

A 精准的上网行为识别

精确识别是实现有效管理的基础，管理上网行为需要实现对“用户、终端、应用”这三个基础要素的识别。深信服AC可以实现丰富灵活的用户身份识别方式，能够适应各种网络环境、管理方式和使用习惯；独有的轻量级网络准入策略能够实现终端环境检查，提升内网可靠性；用户访问网页、发帖、传文件、P2P下载等数百种主流网络应用，无论明文还是加密传输深信服上网行为管理产品都能够有效识别。

功能	详细指标
用户认证	Web认证；绑定IP、MAC、IP/MAC认证；USB-Key双因素认证；LDAP、AD域、Radius等第三方认证；AD域、POP3、Proxy、Web单点登录；新用户自动认证等；
终端检查	专利技术：检查操作系统版本、补丁，杀毒软件安装、运行、更新情况，系统进程、注册表、硬盘文件等；并能自动调用管理员自编脚本程序实现终端个性化检查；
网站过滤	内置千万级预分类URL库，且能基于URL关键字、正文关键字过滤网页；过滤SSL加密的钓鱼网站、博彩网站等；
网页智能识别	专利技术：人工智能技术，根据网页特征自动学习未知网页类型并管理；
关键字过滤	基于多关键字过滤网络发帖、搜索引擎等行为；基于多关键字过滤用户在SSL加密论坛、BBS、博客上的发帖行为；
代理识别	过滤私装代理软件、私接NAT设备、私配公网代理等行为；封堵自由门、无界浏览器等加密代理软件；
应用识别	识别聊天、炒股、网游、P2P、流媒体等数百种主流网络应用；
P2P智能识别	专利技术：识别加密P2P、不常见P2P和未来出现的P2P，解决P2P种类多、版本杂、更新快的问题；
外发文件识别	识别篡改/删除扩展名、压缩/加密后再通过HTTP、FTP、Email附件外发指定类型文件的行为，告警并阻断。
Email识别	基于关键字、收发件人等多条件过滤外发邮件；专利技术：基于多条件拦截缓存邮件、人工审核后再外发； 过滤和审计SSL加密的Foxmail等客户端外发邮件行为、Webmail外发邮件行为；

网页智能识别

Google的数据表明互联网上有一万亿个独立网页，静态URL库显然是不够的。AC创新性的引入人工智能技术，能够根据语义、网址、正文、代码等特征实现未知网页的自动识别、归类和管理，并依据管理员配置的管理策略进行相应管控。

SSL加密流量识别（专利号 ZL 200710072997.1）

有别于封堵TCP 443端口的传统手段，AC不仅可以过滤SSL加密网址，而且可基于关键字过滤SSL加密论坛/BBS的发帖行为，过滤SSL加密Webmail邮件外发行为、及过滤通过SSL加密的Foxmail等客户端邮件外发行为，避免由于加密而给组织带来的管理漏洞。

基于特征的文件识别

具有一定技术水平的恶意用户可能会试图通过篡改/删除文件扩展名、压缩/加密文件后再外发的行为来绕过组织的监管，AC文件特征识别技术能精准识别文件类型，通知管理员采取必要管控措施，避免组织信息资产泄漏。

应用特征识别库+应用智能识别库

深信服AC拥有国内最大的互联网应用特征识别库，能精确识别数百种主流网络应用。同时AC内置应用智能识别库，智能判断不常见或未知的应用。深信服配备十余研发人员，成立“应用十倍专家组”，根据互联网应用的发展，确保应用特征识别库的及时更新和持续扩容。

B 灵活的授权策略

深信服AC能够根据组织的行政架构将用户按树型结构分组，并结合对象化的上网策略，实现上网权限的灵活划分与分配。同时通过上网策略重用、复用、继承、强制继承，满足灵活性、易用性和权限一致性等复杂授权要求。

功能	详细指标
时间控制	支持以时间段、上网总时间控制上网权限；
智能提醒	指定用户指定应用连网时长、流速超限后，自动弹出告警窗口；
树形组织结构	按照行政架构将用户以树型结构分组；
授权灵活性	支持基于用户、用户组、时间段、应用、行为、内容等控制上网权限；
上网策略	上网策略对象化、并与用户无关联，同一条上网策略支持复用、重用、继承等；
强制继承	父组要求子组强制继承的上网策略，子组无法删除、修改、绕过等；

上网策略对象化与强制继承

上网策略是上网权限的集合，其包含网页访问权限、应用权限、审计策略等。对象化的上网策略与用户无关联，同一条上网策略可多人多次重复使用、继承等。当父组使用某上网策略且要求子组强制继承时，子组将自动被该上网策略管制，且无法删除、绕过。管理思路更清晰、管理工作量更少。

人性化的授权管理

深信服AC可以实现多种人性化的授权管理方式，例如允许登录论坛、BBS等浏览帖子但禁止发帖，既降低管理阻力，又避免外发信息泄密或违法；允许登录Webmail收邮件但禁止外发邮件，允许下载某类型文件但禁止外发某类型文件；允许QQ、MSN等进行聊天，但禁止传文件；允许查看股市行情但禁止下单交易等。灵活的上网授权策略体现管理的人性化，在规避管理风险的同时还能够有效的减少管理工作量。

C 细致的带宽和流量管理

深信服AC能够高效、智能的提升带宽效率，防范带宽滥用，保障关键业务/用户带宽需求，再结合带宽分配公平性保障策略，以及QoS、流量整形、带宽借用等高级功能，帮助组织有效实现带宽和流量管理。

功能	详细指标
多线路复用	可最多连接四条外网线路，扩展带宽；且上网流量支持智能选路，解决跨运营商问题；
虚拟线路	将多条外网线路虚拟映射到设备上，实现外网多条线路差异化的精细流控；
父子通道	带宽父通道可虚拟成多条子通道，子通道可继续虚拟更多子通道；
虚拟通道	支持根据应用类型、网站类型、文件类型、用户、IP等划分虚拟通道；
带宽均分	同一通道内多用户平均分配带宽资源，避免流量争抢造成的不公；
时间段控制	流量管理策略基于时间段生效/失效；
带宽借用	多条带宽通道间允许盈余通道将带宽实时借用给拥塞通道；
流量整形	超限流量将被设备缓存并于空闲时转发，达到削峰填谷、流量整形的目的；

多线路流控技术

深信服AC以网关模式部署时可连接最多四条外网线路，不仅低成本扩容带宽，且多链路间互为备份提升稳定性；AC能够实现上网流量的智能选路，出站流量将自动选择最合适的线路，从而有效解决跨运营商问题。网桥模式部署下的AC能将多条外网线路映射成为桥模式下的“虚拟线路”，对虚拟线路流控即实现对多条外网链路分别流控、精准流控。

父子通道、应用/网站/文件虚拟通道

深信服AC将一条物理链路划为多条虚拟线路，将虚拟线路或物理链路再划为多条带宽父子通道，带宽父通道可继续划为默认三级、最多八级的带宽子通道。各级带宽通道又可根据应用类型、网站类型、文件类型继续细分为虚拟通道，进而基于用户、时间段、目标IP等分配带宽资源，满足用户精细化流量划分的需求。

带宽资源平均分配最公平

深信服AC的“轮转调度+分层三色令牌桶”技术，使得同一带宽通道内多用户平均分配带宽资源，且用户所获带宽资源能在该用户多个并发会话间平均分配，确保带宽资源分配的最大公平性。

D 详细的上网轨迹记录

互联网管理条例、组织单位内部控制基本规范、萨班斯法案等法规都对上网行为记录提出要求。AC精准的应用识别能力确保AC能记录最详细、最全面的上网日志，同时可提供数百种不同类型的报表工具为上网管理提供详尽的决策依据。

功能	详细指标
网页审计	记录访问的网址、网页标题、网页内容(或含指定关键字的网页内容);
发帖审计	记录外发帖子行为，即使通过SSL加密亦可审计和记录;
邮件审计	审计外发Email正文及附件，即使通过SSL加密亦可审计和记录;
应用审计	审计网游、炒股、P2P、IM聊天等各种应用行为;
逆向审计	外网用户访问内网服务器、下载文件、发帖等行为亦可审计;
更多审计	审计外发文件内容及下载文件行为、审计流量、审计时间等;
免审计	指定用户以免审计策略或免审计Key方式避免被审计;
数据中心	同时支持内置数据中心和独立数据中心以实现日志海量存储;
审计权限	支持划分管理员日志审计权限，支持以日志审查Key限制管理员内容审计权限;
统计报表	将指定时间段/指定应用的流量或行为按照用户组/用户/IP/应用类别等进行统计排行，并输出报表;
趋势报表	将指定用户/用户组/IP的指定上网行为的统计/流量/趋势等与前一天/前一周/前一月对比并输出报表;
对比报表	将指定用户/用户组/IP的指定上网行为的统计/流量/趋势等与前一天/前一周/前一月对比并输出报表;
风险智能报表	根据管理员设定特征自动挖掘日志并提前预知泄密、中毒、离职等组织运营风险;
更多报表	关键字报表、热帖报表、网站访问时长排行表、危险行为用户排行表等;
内容检索	采用类似Google的搜索引擎技术，从海量日志中快速、精准定位关键日志;

审计SSL加密行为

SSL加密应用日趋流行，通过传统技术方法无法实现用户在SSL加密网站上发帖、登录加密Webmail站点外发邮件、使用Foxmail等客户端发送SSL加密邮件的记录，深信服AC利用创新识别技术实现SSL加密应用的识有效识别并记录，避免给组织上网审计带来的严重漏洞问题。

内容检索

随着带宽越来越大、上网的人越来越多，大中型组织将产生数百G、甚至TB级的上网日志，如何从海量日志中找寻存在问题的日志？AC提供类似Google的搜索技术，允许以最多32个关键字精准、快速定位问题日志，支持对日志中OFFICE、TXT、PDF等文档正文内容的检索，并且能自动将指定检索结果周期性发动到指定邮箱。

E 安全防护能力

管理上网行为的一个重要原因即提升上网安全性，所以AC提供多种安全强化能力，包括过滤成人、色情网站等高风险网站，禁止从华军软件园等知名网站以外的文件下载行为，主动过滤恶意插件、危险脚本和挂马网站，即使内网感染木马、病毒、被黑客控制，AC同样可识别、封堵并报警。

功能	详细指标
过滤危险脚本	基于脚本行为特征，过滤含有危险脚本的网页访问行为；
过滤挂马网站	过滤隐蔽挂载木马、木马链接的网页访问行为；
过滤危险插件	基于插件名称、签名、有效期等过滤恶意插件、放通常用插件；
防范端口扫描	识别并封堵由于内网主机感染病毒、间谍软件等发生的端口扫描行为；
防范内网木马	识别并封堵内网主机感染木马后连接外网的行为；
防范黑客远控	能够识别并封堵内网主机被黑客远程控制、成为"肉鸡"的威胁；
防范ARP欺骗	不仅防御针对网关的ARP欺骗，同时防御三层网络环境中客户端间ARP欺骗问题；
防范DOS攻击	防御来自内网、外网的DOS攻击，提升网关自身安全稳定性；
网关杀毒	集成业内领先的杀毒引擎，查杀网页、FTP、Email等流量中潜藏的病毒；
防火墙	集成企业级防火墙模块，提升网关自身安全稳定性；

过滤恶意插件、危险脚本、病毒等

AC深层分析经过的网络流量，根据行为特征过滤危险脚本、网页木马，也可根据插件名称、签名、有效期等过滤危险插件，放行管理员指定的安全插件；同时对潜藏在网页、Email、文件中的病毒、蠕虫等， AC内置的业界知名杀毒引擎将进行彻底查杀，从源头上保护内网安全。

危险流量识别与防御

已经有终端被感染病毒、木马等威胁的组织网络，AC可基于数据包深度分析，识别并封堵来自内网的病毒、木马、间谍软件、黑客远程控制、端口扫描等危险行为。同时AC可防御来自外网和内网的DOS攻击，防范导致众多用户无法上网的ARP欺骗问题等，为用户提供全方位、多层次的上网安全保护。

F 上网管理智能化，网络管理更轻松

上网行为管理设备是IT人员的重要管理工具，同时能够有效提升IT管理效率，降低管理工作量及成本.但逐渐增多的功能、海量日志、大量报表却增加了管理的难度和工作量，所以IT人员亟需智能化的上网行为管理以解决此类问题。

功能	详细指标
风险智能报表	根据管理者自定义的上网行为风险特征及风险系数，AC深入挖掘日志以形成风险智能报表，并自动发送到指定邮箱，预知组织运营风险；
智能提醒	指定用户使用指定应用的连网时长超限后，自动弹出告警窗口；指定用户使用指定应用的上网速度超限后，自动弹出告警窗口；
免审计KEY	AC将不审计使用免审计KEY用户的任何上网行为，避免过度审计造成的风险；
日志审查KEY	持有日志审查Key的管理员接入数据中心后，才能查询、审计他人的上网行为内容记录；否则只能查看行为统计、趋势报表等，避免上网行为日志被滥用而泄密的风险；
网络准入	不符合组织IT制度要求的终端将禁止其上网、或允许上网但对其警告；

风险智能报表

使用普通设备或方案，管理员事后必须做大量日志分析工作，才有可能发现部分组织运营风险。而AC风险智能报表功能，将按照管理员预设上网行为风险特征和风险系数自动分析和挖掘日志，自动发现“离职风险、泄密风险、工作效率低下”等存在风险的用户，将海量上网日志智能转化为组织运营风险分析结果，简化日志分析工作量。

上网智能提醒

能上网的员工很可能滥用其权限，如长时间网络聊天、持续产生大流量。传统的管理员人工管理不仅需要协调领导，还容易导致同事关系紧张。AC智能提醒则在用户指定应用时长超限、流速超限后自动弹出告警窗口，便于该用户自觉规范其上网行为。

免审计Key、日志审查KEY

为防止由于过度审计而引发泄密的问题，AC专门为高层管理者配备免审计Key，从设备底层免除对持免审计Key用户上网行为的记录。AC还为IT管理员配备日志审查Key，无Key管理员将只能查看行为统计、趋势等，无法查看详细的行为具体内容。通过两种Key保障个人、企业机密信息的安全性，最终在上网审计、信息安全和隐私保护之间达到平衡。

5 部署方式简介

深信服AC在8000多家成功客户实施中遇到了各种网络环境与要求，凭借丰富的部署方式满足了众多客户的各种部署要求：

网关模式：串接在链路中并启用路由功能，实现所有功能并能够通过NAT功能代理内网用户上网，特别适合于对网络结构调整不敏感的客户。

网桥模式：以透明方式串接在链路中，组织无需更改任何路由配置，实现所有功能，特别适合于对网络结构调整敏感的客户。

旁路模式：以旁路监听方式与组织的交换机镜像端口相连，通过对镜像数据包的处理实现所有上网行为审计和TCP应用的管控功能。特别适合于只需审计和不便调整网络结构的客户。

多路桥接模式：最多支持将四对网口形成四网桥，以“四进四出”方式管控客户四条链路中的上网行为。适合部署于冗余多链路、VRRP等网络环境中。

双机热备：无论网关、网桥、旁路还是多路桥接模式，都支持两台AC互为主备的部署方式，提升网络的可靠性和稳定性。

多机模式：两台或更多台AC设备形成多机组，多机组内每台AC设备均可处理上网流量，从而满足超大规模网络对性能的要求，满足VRRP等复杂网络环境要求，同时提升网络稳定性和可靠性。

集中管理模式：上万台AC设备支持被一套SC集中管理平台集中配置、集中监控、集中升级、集中管理，满足大型组织众多分支机构上网行为管理的方便性、一致性。