SANGFOR
深信服科技

深信服上网行为管理系统

2005 年，深信服科技推出中国第一款专业上网行为管理产品，得益于深信服提供的专业上网行为管理技术和业界性能最强的处理平台，该产品的用户数量已达 30000 多家，其中超过 8000 家为中高端客户。正是由于客户的大力支持，深信服上网行为管理产品才能持续保持市场领先，成为业界第一品牌。



到目前为止，深信服上网行为产品已拥有十多项发明专利，并以大量创新技术和应用始终引领着中国上网行为管理的发展方向。深信服上网行为管理产品以用户识别、终端识别、应用识别为基础，结合封堵、流控、审计等管理手段，全面应对互联网给组织带来的工作效率下降、带宽效率下降、泄密风险、法律风险及上网安全风险等挑战，帮助组织有效管理组织的互联网应用，充分发挥互联网的价值。



性能参数

产品型号	AC-1000-B1500
网络层吞吐量	15Gb
应用层吞吐量	750Mb
带宽性能	500Mb
包转发率	90Kpps
每秒新建连接数	10000
最大并发连接数	2200000
内存	4G
硬盘	64G SSD+960G SSD
电源	单电源
接口	6 千兆电口+2 万兆光口
尺寸	1U

部分典型客户

政府	金融	教育科研	企业集团	运营商及能源
国家天文台信息中心	徽商银行	中国人民大学	南方航空公司	中国移动广东分公司
国务院参事室	中国进出口银行总行	中国政法大学	中兴通讯股份有限公司	中国联通陕西分公司
国务院新闻办公室	安邦财产保险股份有限公司	中央广播电视大学	南光集团	中国石油天然气股份有限公司
安徽省财政厅	中国人寿保险股份有限公司	华南师范大学	青岛啤酒	中国石化湖南分公司
湖南省农业厅	浦发银行	北京航空航天大学	华润万家	中国石化天津分公司
河北省审计厅	中信银行	杭州电子科技大学	吉利汽车	中国石油东北销售分公司
云南省交通厅	安信证券	厦门教育局	上海文广传媒集团	中国石油安徽销售分公司
江西省文化厅	华夏基金管理有限公司	北京朝阳区教育局	三生集团	中核集团泰山核电有限公司

SANGFOR
深信服科技

主要功能列表

分类	详细指标
部署模式	支持网关、网桥、旁路、多路桥接等部署模式，支持双机热备、多机部署、集中部署；
设备管理	支持 Web、CLI、SSH 等管理方式；管理员支持分级管理，能将所有功能模块按需分配给不同管理员；多台设备支持通过统一平台集中管理、集中配置；提供图形化排障工具，便于管理员排查策略错误等故障；
实时监控	首页可视化分析展示用户、流量、行为的情况；支持提供设备实时 CPU、内存、硬盘占有率、会话数、在线用户数、系统时间、网络接口等设备资源信息；支持实时提供在线用户信息、应用流量排名、连接排名、所有线路应用流速趋势、流量管理状态、连接监控信息等；支持实时查看各带宽通道的使用情况；支持实时显示当天的安全状况、最后发生安全事件的时间、类型、总次数、源对象，Web 访问质量检测；
用户识别	支持以 IP、MAC、IP/MAC 绑定、用户名密码等方式认证用户；支持 LDAP/RADIUS/POP3/数据库等第三方认证服务器；支持 USB-KEK 认证；支持 AD 域/POP3/Proxy/Web/第三方系统单点登录；支持指定网段/账号强制单点登录；支持账号公有/私有控制；支持账号有效期控制；用户账户支持文本导入、IP/MAC 扫描导入、或从 AD 服务器导入账户和组织结构信息；支持 AD 安全组嵌套同步；支持 LDAP 服务器的域对象的策略管理与同步，使策略管理与用户管理分离；支持短信认证；支持微信认证，无需修改微信第三方平台代码，支持二维码认证；
认证机制	新用户支持根据源 IP 段以 IP/MAC/计算机名等方式实现账户自动命名；支持认证冲突检测；支持认证失败后的权限管控；支持认证成功后的页面跳转控制；
网页监控	内置海量 URL 库且支持手工创建、支持基于 URL 地址/搜索词条/网页正文内容包含的关键字过滤网页访问行为；同时可基于关键字过滤网络发帖、Webmail 邮件外发行为，支持能看帖但不准发帖、能收邮件但不准发邮件的细致管控功能
高级管控	支持过滤 SSL 加密网址（专利），并能基于关键字过滤 SSL 加密的网络发帖和 Webmail；能够识别和过滤使用公网代理或自由门/无界浏览器等加密代理软件来试图规避管理的行为；能够管控通过安装代理软件将自己的上网权限共享给其他人的行为；
文件控制	支持 HTTP 上传/FTP/Email 附件等形式的外发文件行为，支持基于扩展名识别并拦截外发文件；支持控制通过 web IM 传文件的行为，支持审计 IM 传文件行为及内容；
应用控制	内置支持 2800 种以上网络主流应用，管理 IM、web IM、微博、网络游戏、网络炒股、P2P、流媒体、远程控制、木马、代理翻墙软件、移动 APP 等常用网络应用；支持应用更新版本后的主动识别和控制；支持给每种应用定义标签，通过选择标签指定多个应用；支持应用的细分控制；QQ 白名单
P2P 智能识别	通过 DPI 技术识别 BT、迅雷、电骡等 30 余种常见 P2P 应用协议，利用智能 P2P 识别技术实现变种 P2P、未知 P2P 应用的全面识别和管理；
邮件管控	支持完全封堵邮件收发行为；支持基于关键字、收发件人地址等多种条件过滤包括 SSL 加密邮件在内的外发邮件；
上网安全	支持识别和封堵无界浏览、自由门及在线代理，包括 HTTP 在线代理和 HTTPS 在线代理的翻墙行为；内置防火墙，能够防御 DOS 攻击、ARP 欺骗等影响网关稳定性的多种安全风险；内置专业杀毒引擎，支持网关杀毒功能（选配）；
上网授权	支持与组织结构一致的多级用户账号管理方式，可基于用户账号、IP、URL 类型、应用、行为、内容、域安全组，域 OU 组、域属性、用户属性、终端类型、位置、时间段等多种因素管控上网权限；结合对象化的上网策略模板，实现上网权限在不同用户用户组间的复用、集成、强制集成等效果；支持对指定用户的指定应用行为累计使用时长及最高流速进行监控，超出配额将自动弹出提醒对话框智能提醒用户自行采取措施解决，充分减少管理员人工干涉的工作量；
流量管理	支持多线路复用、智能选路（专利）、虚拟线路、虚拟子通道、动态流控等功能；可基于应用类型/网站类型/文件类型及用户、域安全组，域 OU 组、域属性、用户属性、终端类型、位置、时间、文件类型、URL 类型、源 IP、目标 IP 等条件分配带宽资源；支持由外网访问内网的流控和带宽平均分配效果；支持流控通道实时可视化；
运维审计	支持 telnet 协议，可对登陆的账号、执行的命令进行审计；支持 telnet 协议，可对登陆的账号、执行的命令进行审计
上网审计	记录访问的网页地址、标题、（含关键字网页）内容；记录 HTTP、FTP 等外发文件行为及内容，记录下载文件名及行为；记录明文及 SSL 加密论坛发帖，记录明文及 SSL 加密的 Email、Webmail；记录 IM 聊天及 Web IM 聊天内容；记录网游、炒股、影音娱乐、P2P 下载、Telnet 等应用行为；支持发送微博的行为和微博内容审计，支持审计微博上传附件；支持智能终端 web IM 聊天行为的审计，支持智能终端发送微博的行为审计；提示木马、病毒等危险行为；统计用户流量、上网时长等信息；支持行为和内容分开审计；支持对网页过滤和审计分开控制，支持审计指定类型的 URL；可审计外网用户在内网服务器上的网页/文件/邮件等访问行为；数据中心支持网页快照功能查看，审计网页的内容；移动 APP（微博，论坛，新闻）审计；
免审计 Key	避免对持有免审计 Key 人员的上网审计，且免审计状态不可由系统管理员私自变更（选配）；
日志审查 Key	管理过程记录的各类审计日志，数据中心管理员需持日志审查 Key 才能查看详细日志信息（选配）；
数据中心	支持内置和独立数据中心，海量存储日志，可实现不同管理员根据自己的管理对象分级审计；
报表	支持多种报表，包括流量报表、时长报表、行为统计报表、趋势报表、汇总报表、自定义报表等常规报表，以及关键字报表、网络整体状况报表等高级报表；支持数据下钻查询、支持递进查询等多维度查询方式；实现用户及用户组的上网流量、时间、行为的查询、统计、排行等各类统计报表功能、网站访问时长排行等数百种细节报表；
内容检索	提供类似 Google 的日志检索工具，管理者可输入多个关键字实现对日志的快速定位，包括对日志附件正文内容的检索和定位；支持主题订阅，自动将检索结果以 Email 形式发送到指定邮箱；