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，致力于通过创新、高品质的产品及卓越的服务，帮助用户在将业务向互联网转型中获得成功。

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、流量管理、上网优化、广域网加速、应用交付等，并被公认为其中多个领域的技术及市场领导者。

截止2010年3月，已有超过16000家用户选择同深信服合作并取得显著收益。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、中国人民大学等国内知名客户。

目前深信服公司人员规模近1000人，直属分支机构36个（含香港、新加坡、阿联酋、泰国、英国等地的办事处）。2005年－2009年，深信服连续5次入选德勤“中国高科技高成长50强”、“亚太地区高科技高成长500强”，并于2009年荣获《财富》杂志“卓越雇主奖”。

一、“上网优化网关”的定义

海量的互联网资源与组织有限的网络带宽之间的矛盾由来已久，尤其近年互联网的高速发展使得内网用户渴望快速上网的诉求与日俱增，上网优化网关这一概念也应运而生。

专业上网优化网关是涵盖上网加速、带宽管理、上网安全三位一体的解决方案。其中融合缓存和代理的上网加速是核心，实现带宽资源合理分配的带宽管理是支撑，保障组织网络稳定可靠的上网安全是基础。

二、部署上网优化网关的必要性

自上世纪60年代“阿帕网”诞生，只短短半个世纪互联网就已经发展成含有一万亿个网页、1.8亿个独立域名的庞然大物，而当前中国网民的数量早已超过3亿、跃居全球之首。互联网的飞跃式发展，带动了信息的爆炸式传播，促使各色网络资源日趋庞杂，但缺乏上网加速、带宽管理、上网安全的互联网访问给组织带来的问题却是层出不穷：组织的互联网出口带宽数据占用率居高不下、上网速度慢、关键应用/用户带宽无法保障，又要扩容带宽来解决吗？内网病毒、木马等网络威胁频发，重新购买更贵的杀毒软件可以杜绝吗？组织的网络正在失控，上网优化时代已然来临！

1 带宽小、用户多、上网速度慢

虽然近年来组织的互联网带宽在不断增加，却仍然难以满足内网人员规模的日渐扩大；尤其与互联网资源海量而泛滥的现实相比，组织的互联网带宽更是捉襟见肘；众多内网用户和管理者纷纷抱怨上网速度慢，让IT部门倍感压力。

同时组织宝贵的互联网带宽也未获得高效利用，内网用户相似的网络访问习惯往往导致大量冗余数据在反复传输。例如，用户通常都去访问一些知名的门户网站；某网络事件爆发后大量用户浏览相同链接的视频；同一网页、图片、视频等数据反复传输并占用互联网带宽资源，导致了上网速度变慢！

鉴于此，深信服上网优化网关通过丰富的报表工具向IT人员直观展现互联网流量构成、带宽使用情况等信息；再借助上网优化网关的上网加速特性，减少冗余数据反复传输浪费带宽的频率；同时当内网用户访问相同互联网资源时，可直接从网关处提取传输，大幅提升上网速度。

2 P2P应用泛滥，带宽缺乏管理

第三方统计显示，全球P2P流量占互联网总流量49%到83%。当前办公室里普遍存在迅雷、在线影音等带宽杀手极度消耗组织有限带宽资源的情况，而防火墙等传统方案却难以管控，即使投入大量成本扩容带宽，新增带宽仍然很快被P2P蛀虫们吞噬。不仅上网速度慢如蜗牛，而且ERP等业务系统访问质量也强差人意，IT部门不得不为此承受巨大的绩效压力。

以丰富的报表工具向IT人员直观展示各应用、各用户的带宽使用情况后，深信服上网优化网关针对应用类型、网站类别、文件类型、用户/用户组、时间段等细致划分和分配带宽资源，既可有效限制P2P、在线影音、大文件下载等不良应用对带宽的大量占用，同时又保障领导等关键用户、ERP等关键应用的带宽需求，进而提升上网速度。

3 软件Proxy渐显瓶颈，传统方案难当大任

出于安全等因素考虑，银行、保险、集团企业等大中型组织通常都部署了传统的软件Proxy代理方案。但是由于其安装在服务器上，必须依赖通用操作系统提供代理功能，加上组织内网人数增加、互联网带宽增大等，软件Proxy代理方案无论性能、稳定性、安全性都已无法满足组织要求。

为此，在实现上网加速功效的同时，深信服上网优化网关提供硬件Proxy代理功能，为大型组织提供性能更强劲、更稳定可靠的硬件Proxy代理方案。借助Proxy代理将帮助组织实现内网与互联网的隔离保护，增强组织网络安全性，同时代理内网数万用户上网。

4 病毒木马横行，网络可用性降低

一个病毒木马泛滥横行、时常故障甚至中断的网络，纵然优化和快速也无济于事，所以确保网络稳定、安全、可靠是上网加速的基础。

色情、反动等非法网站向来是病毒木马的重灾区，即使正规门户网站也可能被黑客挂载木马或植入病毒，同时含有恶意脚本/危险插件的网页层出不穷，普通用户的无意访问即会将威胁引入内网。Internet已经成为影响内网稳定、可靠的主要因素。另外一方面，存在漏洞、不满足IT规定的终端，其上网时极易感染网络威胁，进而在内网泛滥传播，使组织网络可用性岌岌堪忧。

深信服上网优化网关能主动清理流量中的恶意插件、危险脚本、病毒、木马等威胁，并封堵色情、反动等不良网站。即使内网用户不幸感染间谍软件、被黑客远程控制、甚至沦为僵尸网络等，深信服上网优化网关亦可识别、封堵、并向管理员报警。同时还可防御DoS攻击、ARP欺骗等恶意威胁。此外还将终端安全状况与其上网权限关联，终端不安全的就禁止上网。多手段、全方位确保组织上网环境的稳定、可靠与安全，为上网加速奠定坚实基础。

三、深信服上网优化网关优势

专业上网优化网关是涵盖上网加速、带宽管理、上网安全的整体解决方案，其中上网加速是核心。深信服SG上网优化网关具有上网加速效果最好、部署最智能、单台设备加速性能最强等明显优势，帮助组织显著提升上网速度。

1 上网加速效果最好

海量的互联网资源为上网加速提出了挑战。传统方案仅能加速部分网页访问行为；同时传统方案往往安装在服务器上、以windows等通用操作系统为基础平台，因此其加速效果、加速性能、稳定性、安全性等都存在先天不足。深信服上网优化网关利用“内存缓存、硬盘缓存和多值加权淘汰算法”，针对用户访问的网页、观看的在线视频、下载的文件等数据实现业界效果最好的上网加速，更可以借助深信服上网优化网关内置的柱状图、饼状图等直观展现加速效果。

2 部署最智能

如Proxy软件等传统上网加速方案使用时，内网用户必须进行配置并启用代理、修改浏览器设置等操作，这明显增加了部署难度和维护成本，对于成百上千内网用户的组织更如同噩梦。而深信服上网优化网关无需调整网络部署，支持以网桥模式透明串接在组织网络中；同时内网用户无视任何变动，保持原有上网习惯即可直接上网、立即加速；即使已部署Proxy代理的组织，用户也无需修改代理配置即可享受上网加速，从而真正实现智能部署和透明加速。不仅简化用户操作，更减轻IT部门部署和维护的工作量。此外，深信服上网优化网关也支持包括网关模式、网桥模式、多路桥接模式、双机模式、多机模式等丰富的部署方式，以满足不同客户网络环境的对设备部署的各种要求。

3 单台设备加速性能最强

一台传统Proxy软件服务器通常仅支持300-500并发用户的上网加速，而采用多服务器集群部署无疑增加了部署成本、维护成本。深信服上网优化网关采用专有硬件和自有操作系统，为高端客户提供了业界性能最强的上网加速解决方案：一台深信服上网优化网关即支持数万并发用户的上网加速，也可以将多台上网优化网关以多机模式部署，为超大规模组织提供性能更加强劲的上网加速解决方案。

四、主要功能及创新技术介绍

1 高效率Cache缓存与高性能Proxy代理

借助Cache缓存加速技术，相同网页、文件、视频等数据将被深信服上网优化网关缓存，内网用户再次访问时将直接从Cache缓存中提取传输，不仅提升上网速度，同时避免冗余数据反复传输所造成的带宽资源浪费，而且无需内网用户修改任何配置，完美实现智能部署、透明加速，实施与维护简单易行。

采用深信服上网优化网关的硬件Proxy代理功能，还可显著改善组织原有的软件Proxy代理方案普遍存在的性能低、不稳定等问题，进一步强化组织网络的安全与可用性。

功能	详细指标
缓存对象	网页/图片等静态文件，酷六/搜狐等在线视频数据均支持缓存和上网加速；
缓存机理	重复数据支持被内存缓存或硬盘缓存； 当用户访问重复数据时，将从Cache缓存中直接提取并返回给用户，提升网速并降低带宽占用率；
分权限缓存	指定用户/用户组可启用或禁用Cache缓存功能； 访问指定域名/IP支持优先缓存或禁止缓存效果；
缓存效果图	通过柱状图、饼状图等直观展示缓存效率和上网加速效果等；
透明缓存	内网用户无需更改任何配置即可实现透明缓存和上网加速；
Proxy代理	支持HTTP/Socks5代理，支持单臂部署，满足组织代理上网的需求；

缓存透明部署

多数Cache缓存方案要求组织内网用户必须修改代理配置、修改浏览器配置等，导致部署繁琐、使用不便。而深信服上网优化网关无需内网用户修改任何配置，保持原有上网习惯即可透明缓存、透明加速，部署和使用更简单方便。

缓存效果最好、性能最强

传统Proxy软件等缓存方案需安装在服务器上，依赖通用操作系统实现缓存功能，不但缓存效果不理想，稳定性亦不足。深信服上网优化网关通过内存缓存、硬盘缓存、多值加权淘汰算法等手段提供业界最好的上网加速效果；专用硬件平台和精简优化的操作系统实现了业界性能最强的上网加速方案；同时用户可通过柱状图、饼状图等直观查看上网加速效果。

高性能硬件Proxy代理方案

众多中高端客户出于安全考虑等因素早已部署传统的软件Proxy代理方案，但随着组织规模扩大，软件方案无论性能、稳定性等均难以胜任更高的要求。深信服上网优化网关基于专有硬件平台、优化的操作系统为中高端客户提供性能强劲、稳定可靠的硬件Proxy代理方案。

2 最细致、最公平的带宽管理

深信服上网优化网关能够高效、智能的防范带宽滥用，提升带宽效率，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，帮助组织有效管理带宽和流量。

功能	详细指标
多线路	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，实现外网多链路差异化的精细流控；
父子通道	将物理线路、虚拟线路等带宽父通道划分成多条、多级子通道，实现流量精细划分与分配；
虚拟通道	根据应用类型、网站类型、文件类型、用户、IP等划分流量虚拟通道，流控最细致；
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；
流速提醒	指定用户的指定应用流速超限后能够对其自动提醒；

多线路流控技术，最智能（专利技术）

深信服上网优化设备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以提升稳定性；智能选路功能将为出站流量自动选择最合适的线路，从而有效解决跨运营商访问的问题。网桥模式部署下的深信服上网优化网关能将多条外网线路分别映射成为网桥模式下的“虚拟线路”，对虚拟线路流控即可实现对多条外网链路分别、精准的流控。

父子通道、应用／网站／文件虚拟通道，最细致

深信服上网优化网关可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带宽虚拟通道，进而基于用户、时间段、目标IP等分配带宽资源，实现业界最细致的流量管理。

带宽资源平均分配，最公平

当多用户使用同一带宽通道上网时，传统设备会导致多用户间互相争抢带宽，造成极大不公。而借助深信服上网优化网关所特有的“轮转调度+分层三色令牌桶”技术，带宽资源将在多用户间平均分配，且每位用户所获带宽资源能够在该用户多个并发会话连接间平均分配，实现带宽资源分配的最大公平性。

3 丰富的报表工具实现网络透明可视

路由器、交换机构建的基础网络和组织出口带宽究竟被哪些应用、哪些用户使用？深信服上网优化网关通过对网络流量和用户访问的详细识别与分析，借助丰富的图形化报表，以柱状图、饼状图等形式让网络更透明和可视，为组织的上网优化、IT规划提供详尽决策依据。

功能	详细指标
实时监控	实时监控CPU/硬盘/流量/连接/会话信息，实时监控在线用户信息、流量排名、连接排名等信息，实时监控各带宽通道的使用状况等；
流量可视	直观展示各条链路、各种应用、各用户/用户组的流量分布、流量统计和流量趋势状况；
时间可视	直观展示各时间段内的流量分布、应用访问行为、用户状态等信息；
访问可视	通过图表直观展示用户的互联网资源访问行为情况及信息；
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等进行统计排行，并输出报表；
趋势报表	将指定时间段/指定应用的流量或行为按照用户组/用户/IP等进行趋势分析，并输出报表；
对比报表	将指定用户/用户组/IP的指定网络访问行为的统计/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带宽滥用、病毒感染等网络风险；

最全最灵活的网络可视报表

深信服上网优化网关内置统计报表、趋势报表、对比报表等，用户轻松点击鼠标即可知悉带宽和互联网资源的使用情况。同时允许管理者输入众多自定义查询/统计条件，生成自己的个性化报表，并可将常用报表放置于首页方便访问。深信服上网优化网关内置报表模板和用户自定义报表总数量超过一千多种，足以满足各种网络可视要求。

对比报表

上网优化等IT方案实施前后的效果如何展现？组织领导如何了解设备或方案的价值？通过深信服上网优化网关的对比报表将直观展现前后两段时间内网络流量、网络访问状况的对比信息，尤其可以将不同部门、不同用户的流量和访问对比输出报表，为网络管理、员工管理、绩效考核提供数据依据。

风险智能报表

使用普通设备或方案，管理者事后必须做大量分析工作，才有可能发现组织网络和运营的部分风险。而深信服上网优化网关的风险智能报表功能，将按照管理员预先设定的上网流量特征、时间特征、网络访问特征和风险系数等因素，自动分析和挖掘潜在的风险，将网络可视化进一步智能的转化为组织网络和运营风险的分析结果。

4 全面的危险过滤与流量清洗

“稳定、可靠、安全”是上网优化的基础，反之一个病毒泛滥、木马横行的网络，其上网优化必然首先从上网安全强化开始。所以深信服上网优化网关提供多种安全强化能力以清洗流量，包括过滤反动、色情等高风险网站，禁止从组织规定的网站以外的文件下载行为，主动过滤恶意插件、风险脚本和挂马网站等危险流量，即使内网感染木马、病毒、被黑客控制，深信服上网优化网关同样可以识别、封堵并报警。

功能	详细指标
过滤非法网站	识别并封堵极易潜藏病毒、木马的色情、成人等风险网站；
过滤脚本/插件	基于脚本特征、插件名称／签名/有效期等，过滤含危险脚本/恶意脚本的网页；
过滤挂马网站	过滤挂载木马、木马链接的网页；
危险行为防范	封堵源自内网主机的端口扫描、非法外联、黑客远控、僵尸肉鸡等危险行为；
防范ARP欺骗	防御针对网关的ARP欺骗，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，提升网关自身安全性和稳定性；
防火墙	集成企业级防火墙模块，提升网关自身安全性和稳定性；
终端检查	检查操作系统版本/补丁、进程、注册表、硬盘文件、杀毒软件安装/运行/更新情况等；
脚本调用	支持自动调用管理员自写脚本，以实现用户终端个性化检查；
网络准入	检查不通过的用户终端既可禁止其上网，也可允许上网但给予提醒；

清洗恶意插件、危险脚本等流量

深信服上网优化网关深层次分析组织单位的网络流量，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；根据行为特征过滤危险脚本；即便是互联网上越来越流行的挂马网站，包括门户网站被挂载木马等情况，深信服上网优化网关也可以精准识别和过滤，从源头上清洗流量以强化上网安全性。

危险流量识别与防御

即使组织内网已经有终端感染病毒、木马等威胁，深信服上网优化网关仍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。同时深信服上网优化网关还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欺骗等各种恶意行为，全方位、多层次的保障网络稳定、可靠和安全。

终端安全检查方案

终端检查与网络准入技术是修补网络漏洞和安全短板的常用技术之一。但部署传统NAC方案要求替换接入层交换机，昂贵的实施成本导致多数客户难下决心。然而，只需在组织互联网出口处部署一台深信服上网优化网关，将终端检查与上网权限关联，检查不通过就禁止其上网，从而以低成本实现NAC方案，帮助用户修补终端漏洞、提升终端安全性、强化组织网络安全性和可靠性。

五、典型客户

侨鑫集团

集团总部的互联网出口由互联网访问流量及集团与子公司的业务数据构成，二者相互影响。原本需要申请IT预算以扩容互联网带宽，但通过深信服SG上网优化网关的部署，一方面通过缓存重复数据并提升互联网访问速度，另一方面显著减少重复数据对带宽的浪费，为集团业务数据的传输节省出更多的带宽资源，一举两得。

江苏省建工集团

一期工程在集团总部和下属分公司共部署十几台深信服SG上网优化网关，在无需投入大量成本扩容各分支机构互联网带宽的前提下，SG显著提升用户上网速度，改善互联网访问体验，同时保障VPN隧道带宽，提升视频会议、邮件等办公应用的传输质量。

广西东方外语学院

深信服SG上网加速网关设备以网关模式部署，不仅显著削减并降低互联网出口中的重复流量，同时大幅提升师生们的上网速度。此外以网关模式部署的SG设备，还实现了学院两条互联网链路的负载均衡、互为备份的效果，大幅提升原有带宽的使用效率。