作为中国SSL VPN市场的第一品牌，深信服科技致力于为客户提供最快、最安全、最好用的SSL VPN产品，保护客户的业务安全可靠，提高客户的业务效率，与客户共同成长。

更懂客户业务的创新方案

从为客户创造价值的目标出发，在深入了解客户业务情况的基础上，深信服科技运用最具创新性的方案，为客户有效地解决在业务互联网化过程中所遇到的问题。除了移动办公方案、多方接入的权限分配等传统SSL VPN应用方案之外，深信服科技提出了更多创新性运用，如使用SSL安全特性为客户解决原有关键系统安全保障问题；运用SSL加密和逻辑隔离特性为客户的核心数据实现安全防泄密。另外，基于在前沿网络领域中完善的技术，深信服科技为客户提供了更具价值的整体解决方案，如SSL /IPSec VPN二合一解决方案，加速VPN解决方案等。大量的成功客户案例证明了深信服科技在以客户为导向的理念下，获得了市场的高度认可。

业界持续领先的技术理念

深信服科技不断引领业内技术创新，为客户提供最完善的SSL VPN 产品。 2005年推出全球第一款SSL/IPSec二合一的产品；2006年率先提供了包括短信、HardCA硬件鉴权、动态令牌、SSL VPN隧道逻辑隔离等安全技术；2007年根据中国实际网络环境率先实现跨运营商线路加速、SSL隧道自动愈合等技术；2008创新性地实现混合认证、动态压缩、无线线路优化等技术，并作为核心制定者参与国家SSL VPN标准的制定；2009年全球首家实现非对称集群、智能隧道选路等技术；2010年更是推出了业内的最快SSL VPN加速技术——流缓存技术。未来，深信服还将继续站着中国VPN技术最前沿的位置上，为客户提供最好的VPN。

最广泛的客户认可度

截止2010年初，深信服VPN已服务于超过一万家的用户，值得一提的是：在世界五百强的中国企业中，有70%都选择了深信服VPN解决方案。自2008年始，深信服SSL VPN便以超过三分之一的市场份额占据着中国SSL VPN市场第一的位置，并保持份额的不断扩大。

功能价值

1、深信服–国家SSL VPN标准主要制定者、市场占有率第一

国家SSL VPN标准的制定者

公安部颁发的《计算机信息系统安全专用产品销售许可证》

国家密码管理局颁发的《商用密码产品型号证书》

国家密码管理局颁发的《商用密码产品销售许可证》

国家密码管理局颁发的《商用密码产品生产定点单位证书》

深信服科技在2008年中国SSL VPN市场占有率第一，为31.1%

深信服科技在2009年中国SSL VPN市场占有率第一，为34.0%

——以上数据引自Frost & Sullivan针对中国2008年和2009年全年SSL VPN市场的调查报告

2、最快速的SSL VPN

七层技术保障SSL VPN接入的访问速度。

技术功能	功能价值
基于Web的智能选路	总部出口为多条运营商线路条件下，为远程用户提供最快的接入体验。
WebCache	提升基于Web的各类资源的访问速度。
多线路复用技术	充分利用多条线路，全面提高VPN接入速度，并支持单臂模式下的多线路技术。
HTP传输加速	提高无线GPRS/CDMA/EDGE下的SSL VPN访问接入速度。
IP资源全网优化	提高针对IP资源的访问速度。
资源负载均衡	融合服务器负载均衡技术，进行用户接入智能分配，提升访问速度。
高强度数据压缩	全面降低各应用传输所需要的带宽，提高传输效率。

可选配流缓存加速模块大幅加速SSL VPN访问体验:

技术功能	功能价值
流缓存加速	使用特有的加速技术大幅削减冗余传输数据，最高可削减多达80%的链路流量，大大提升用户访问速度。

另外可选配硬件加速卡，提升SSL VPN的加密性能。未来深信服SSL VPN将融入更多广域网加速产品的创新技术，全面提高SSL VPN接入访问速度。

3、最安全的SSL VPN

提供涵盖五个层次的安全保障：身份接入安全、单点安全、传输安全、权限安全、审计安全，为您打造最安全的SSL VPN。

3.1、身份认证安全

身份认证的安全作为整个SSL VPN安全接入中最重要的一环，直接关系到SSL VPN远程接入建立后内网的安全性，深信服科技提供业内最强大的认证手段，通过多种组合安全身份认证方式，保证接入人员身份的绝对安全。

技术功能	功能价值
用户名/密码认证	提供基本的身份认证方式，以此方式为基石与其他认证方式进行结合。
数字证书认证	可与第三方CA体系进行结合，并支持OCSP服务器，融入PKI体系。
自建CA中心	提供自建CA，极大的降低企业IT建设成本。
终端硬件鉴权	支持基于终端硬件特征码的认证、审批、多对多绑定策略，有效防止非法终端的接入。
短信认证	支持短信猫、与运营商短信网关结合，轻松实现双因素认证，提高身份认证安全级别。
融合第三方认证体系	可与LDAP、Microsoft AD、RADIUS等第三方认证体系进行无缝集成，便于接入人员身份的统一管理。
动态令牌认证	基于事件的动态令牌认证技术，进一步提升身份认证安全性。
“与”、“或”组合认证	可实现多种认证方式“与”、“或”组合，满足不同使用者登录安全要求 。
主从账号绑定	实现了SSL VPN账号与访问资源的账号对应绑定，增强了认证强度，防止越权访问。
密码防暴力破解	基于用户名、IP进行防暴力破解，全面保障密码的安全性。
软键盘和图形码验证	可以有效的避免SSL VPN设备受到恶意软件的骚扰。
多重密码安全策略	支持强制设定多种终端登录密码安全策略，有效降低密码被破解的风险。

3.2、接入终端安全

深信服SSL VPN采用终端安全检查、沙盒技术等多项终端安全功能，有效保障在终端接入前、后的内网自身安全、机密信息安全。

技术功能	功能价值
客户端安全检查	提高整体防御水平，防止终端可能存在的木马病毒通过SSL VPN隧道传播到企业内网。
全面的安全策略授权	支持基于时间、接入IP、终端、接入线路、应用规则的客户端准入控制策略和资源访问授权策略，并支持规则策略库的升级和回滚，整体规划SSL VPN远程接入的安全。
安全策略组合	可实现安全检查规则的任意“与”、“或”组合，满足更多的个性化安全要求。
沙盒技术	启用沙盒技术，强制重要资源置于安全桌面中访问，安全桌面下禁止通过与默认桌面通信、外设拷贝、局域网通信、互联网通信等方式将受保护资源的数据的在本机保存或泄漏。用户退出SSL VPN后，安全桌面内所有资源交互数据将被销毁，防止数据在终端上的泄漏，保证重要应用在终端访问的安全性。
VPN专线功能	终端接入SSL VPN后自动断开其余所有Internet连接，规避黑客以终端作进攻内网跳板的风险。
终端“零”缓存	退出SSL VPN后自动清除本机缓存，避免机密信息泄露。

3.3、传输安全

深信服SSL VPN采用AES、DES、3DES、RC4、SHA、MD5等多种国际标准加密算法对传输数据进行加密处理，保障数据传输安全。

采用标准SSL 协议进行数据封装传输， 完全符合国家标准的SSL VPN技术规范。

3.4、权限管理的安全

人员接入网络后的权限划分向来是安全防护的重中之重，深信服SSL VPN为您提供全面、细致的安全管理和权限划分，免除后顾之忧。

技术功能	功能价值
基于角色的权限划分	可有效控制VPN接入用户访问权限，提高内网的安全级别。
高细粒度权限控制	可按URL、服务、IP等各项资源对SSL VPN接入用户进行高细粒度的接入控制和管理，实现更合理的权限分配。
关键文件保护	针对系统中关键文件进行保护，避免SSL VPN访问中重要文件被意外破坏的风险。
用户分级管理	支持多达16级的用户树形结构分级，模块化访问授权，最大程度贴合企业组织架构进行最精确细致业务资源访问管理。

3.5、日志审计的安全

深信服SSL VPN支持第三方日志中心，让您对远程接入平台的访问情况了如指掌，做到所有访问行为的有据可查。

技术功能	功能价值
丰富的日志数据	提供完整的系统日志、设备运行日志、管理员日志、用户日志，极大的方便了管理员进行查看和管理。
独立日志中心	可实现企业对海量日志数据存储的需求，避免内置数据中心对网关设备性能的影响。独立日志中心可提供详细的用户日志、资源访问日志、安全日志、管理员日志、系统日志、流量日志等多种日志类型，详尽的SSL VPN访问轨迹记录为日后的网络规划提供了可靠的依据。
多种数据表达方式	提供基于用户、用户组、流量、资源多因素的柱状图、曲线图、列表等多种显示方式，并可按年、月、日进行细致的日志查看。多样的数据表达访问为管理员提供更贴切的查看角度，便于管理员全面掌握SSL VPN运行、资源访问及用户SSL VPN的使用情况。
丰富的统计报表	提供多种统计报表功能，并支持自定义报表（用户、资源、流量），提供多种报表模板供用户选择，方便管理员进行数据的统计分析。
多设备日志汇集	支持多台设备日志统一同步到一个日志中心，便于网络管理员对企业远程接入的数据中心集中管理。
数据中心分级管理	数据中心支持分节点分级管理，防止轨迹记录被滥用。

4、最易用的SSL VPN

SSL VPN技术的诞生及发展就是因为其免客户端的简便性、易用性，深信服SSL VPN秉承该理念，其SSL VPN产品提供最易用的远程接入服务。

技术功能	功能价值
单点登录（SSO）	支持B/S、C/S系统的单点登录，免除用户重复输入账号或口令的繁琐操作，简化部署和维护工作，降低账户信息泄露的风险。
兼容多种终端环境	支持包括PDA、智能手机、3G手机等不同客户端环境，支持多种浏览器，做到接入平台的最大兼容。
页面完全定制	可提供登陆前、登录后界面的整体定制，满足客户个性化风格要求。
智能递推技术	有效防止资源漏访现象，极大的简化了管理员资源配置工作。
流量、会话控制	支持基于用户、用户组的流量控制以及会话控制，防止单个客户流量过大、挤占带宽的现象，整体提高用户访问体验。
默认服务页面	基于用户、用户组实现登录SSL VPN后直接跳转到指定应用系统资源页面，提供个性化门户服务。
系统托盘	关闭IE后资源页面最小化到系统托盘，防止误关操作导致的SSL VPN中断。支持开机SSL VPN自动登陆、断线自动重连。
终端个人设置	可允许用户登录SSL VPN后自定义设置密码、手机号等个人配置，单点登录SSO资源、密码配置等，简化管理员维护工作。
远程应用发布	采用虚拟终端技术，将一个或多个应用程序窗口发布到客户端，用户无需在本地安装客户端即可如运行本地应用程序一样访问内网应用。减少传输数据量、降低应用交互等待时间，大幅提高终端访问速度。
虚拟站点	将SSL VPN 设备虚拟成多个独立、互不干预的访问站点，实现高度的用户隔离和资源隔离，一台设备实现多台设备的服务效果。

5、高可靠、可扩展的SSL VPN

SSL VPN为企事业单位提供重要的远程接入平台，要求稳定使用、持续发展。深信服SSL VPN产品的高可靠性和可扩展性是客户稳定使用、持续发展的坚实保障。

技术功能	功能价值
Webagent技术	动态IP情况下为企业提供稳定VPN连接。
VPN线路备份	VPN链路备份技术，提高业务链路的可靠性。
双机热备、多机集群	在一台设备意外停止服务的情况下，另一台或几台设备自动接管所有SSL VPN发布服务，保证VPN服务的稳定可靠性。
非对称集群	可实现不同型号VPN设备的集群功能，完全保护网络前期投资，实现性能平滑升级。
全网分布式集群	对于分布式数据中心的SSL VPN组网，提供基于全网的分布式集群技术，实现统一域名接入、异地就近接入、异地热备接入、全网负载均衡、分布式设备统一配置管理的高速、高便利、高可靠价值。
SC集中管理	支持利用SC设备进行全网设备的集中管理、实时监控、远程维护、智能升级，降低管理员对大规模VPN网络的管理难度。
集成第三方管理系统	支持利用标准接口方式集成第三方管理系统，实现网络设备的统一管理。

SSL VPN系统安全优化方案

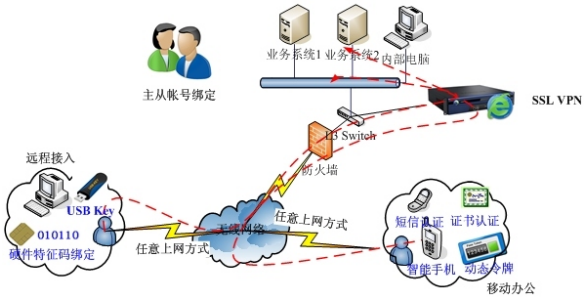
1.内网软件系统安全加固方案

重要的业务系统如OA、财务ERP等仍采用简单的用户名密码认证方式，在新的安全威胁下无法为系统提供可靠的安全保障，存在数据泄漏的风险。深信服SSL VPN提供内网软件系统安全加固方案，全面保障应用系统安全性。

（1）USBKey、动态令牌、短信认证、硬件特征码等多种组合认证方式增强原有系统身份认证强度。

（2）专利技术主从帐号绑定实现VPN帐号与软件系统帐号强绑定，实现系统账号的安全加强；单点登录技术实现通过安全认证后直接访问系统，减少繁杂的系统登录操作。

（3）加密传输内容保证数据安全性，支持独立数据中心提供详细的接入访问轨迹记录。



2.业务系统安全逻辑隔离

置于内网中的核心业务系统已经与外网进行了隔离，但仍面对内网中存在的安全隐患：核心业务系统仅采用简单的用户名密码认证方式，极易遭到破解、冒名登录；关键业务数据在内网中仍采用明文传输，关键数据直接暴露给内网用户；核心业务系统面对内网访问用户所携带的病毒、木马束手无策，若遭到感染存在系统数据泄漏甚至业务瘫痪的风险。

深信服SSL VPN提供业务系统安全逻辑隔离方案，保障内网核心业务安全性。

（1）提供身份认证、传输加密、权限控制、客户端安全的多方面安全控制手段。

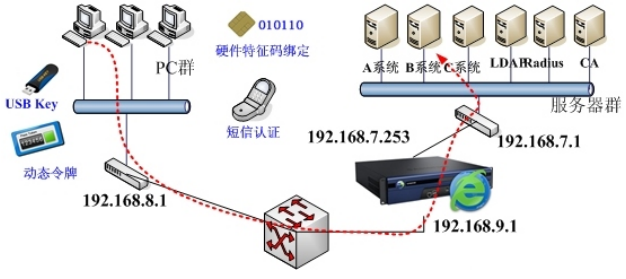
（2）接入SSL VPN后自动断开与外网的所有通讯，实现业务使用的逻辑隔离。

（3）使用安全桌面功能，保证重要数据留存在服务器，不被私自拷贝或其他方式泄露。

（4）可根据用户身份、用户终端访问设备安全检查及评估状况赋予不同的应用访问权限，进行智能的资源访问控制。

（5）使用SSL VPN的数据中心，对访问核心业务系统访问行为进行全面细致的审计和监控。

（6）通过SSL VPN实现应用系统访问的集中管控，降低管理和维护成本；结合SSL VPN自动登录及应用系统单点登录技术，大大提高业务系统登录易用性。



3.WLAN接入安全建设方案

WLAN技术已经成为扩大业务网络覆盖面不可或缺的助力，但是WLAN所采用的WEP和WPA加密方式早已遭遇了众多破解工具，安全隐患不容忽视；而面对众多的AP接入点，接入无线网络后需要统一的权限划分防止资源的滥防所导致的数据安全威胁。深信服SSL VPN提供WLAN安全加固方案，严防WLAN接入安全漏洞。

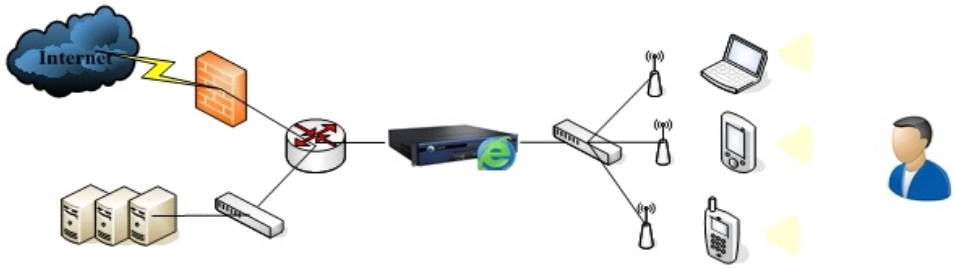
（1）提供多种组合认证方式加强WLAN身份认证安全性，杜绝非法用户。

（2）传输数据强加密保证数据安全性，让信息在空气中传播也能得到最完善的安全保护。

（3）细粒度权限划分机制，提供内网资源的授权访问。

（4）基于浏览器的接入访问及配置操作大大降低网络管理及维护成本。

（5）实现集中的网络接入权限控制和访问行为记录。



4.分布式统一接入方案

大型的网络往往采用分布式业务数据中心的方式构建，可采用SSL VPN实现全网移动办公、资源共享、安全接入。深信服SSL VPN提供分布式统一接入方案保证分布式业务数据中心最快速、最便捷的使用效果。

（1）多点SSL VPN采用统一域名接入即可实现全网资源的集中访问，大大提高易用性。

（2）无缝漫游特性，采用“就近接入”机制，自动选择速度最佳的访问点实现全网接入，提供最快速的资源访问效果。

（3）全网SSL VPN用户、资源、授权、安全集中管理配置，大大提高整网统一管理强度。

（4）异地热备接入，当其中一点设备无法正常工作，用户通过“就近”机制自动选择临近点接入，平滑过渡保障全网应用访问的稳定性。