SANGFOR
深信服科技

深信服科技

SSLVPN 产品白皮书

深信服科技股份有限公司

2020 年 6 月

版权声明

深信服科技股份有限公司版权所有，并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其它相关权利均属于深信服科技股份有限公司。未经深信服科技股份有限公司书面同意，任何人不得以任何方式或形式对本文档内的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

联系我们

售前咨询热线：400-860-6868 售后服务热线：400-630-6430 （中国大陆）

香港：(+852) 3427 9160

英国：(+44) 8455 332 371

新加坡：(+65) 9189 3267

马来西亚：(+60) 3 2201 0192

泰国：(+66) 2 254 5884

印尼：(+62) 21 5695 0789

您也可以访问深信服科技网站：www.sangfor.com.cn 获得最新技术和产品信息

目录

第 1 章 序言

随着互联网数据技术的进步和商务模式的发展，在互联网技术的帮助下提升业务效率已经是必然的选择：利用信息化，加速业务流程；利用互联网，实现随时随地的业务响应。互联网技术已经彻底改变了传统的业务办理模式，借助信息化，相关业务信息实现快速的处理和共享，人员无论在何时何地，只要能连上互联网，就能实现业务的及时处理。

与此同时，业务信息网络化另外一方面是带来了安全的威胁：越来越多的关键信息被保存在信息系统中，一旦被泄而一旦通讯或存储的信息被篡改，则更会带来难以估计的后果。为了保证这些系统的安全，这些系统被严格的限制在只允许园区网络内部访问。然而这与快速发展的技术与用户需求相背。于是提供一种既安全又方便的远程访问服务成了摆在网络维护与管理人员面前的重要问题。

在计算机网络中，除了建设物理隔离的业务网络之外，还拥有更具性价比的解决方案，使用 VPN（Virtual Private Network 虚拟专用网）技术来构建安全的业务网络。

VPN 利用的是包括认证、加密、安全检测、权限分配、访问记录等一系列手段来构建安全的业务网络。现存在的主流 VPN 远程访问方式有，传统 VPN（PPTP、IPSec）、SSL VPN、OpenVPN 等，在解决远程访问需求上，特点各异：

VPN 技术	PPTP	IPSec VPN	SSL VPN	OpenVPN	WEB VPN
数据加密	默认支持	默认支持	默认支持	默认支持	可选支持
客户端	操作系统自带	部分系统自带/独立客户端	浏览器插件/独立客户端	独立客户端	无
兼容性	较差、依赖系统支持	差、依赖系统支持	一般，浏览器插件方式依赖浏览器支持	差、依赖系统支持	好
身份认证	较差	较差	强	较差	一般
暴露端口	1723	500/7101/4500	443	自定义	443 或自定义
可维护性	差	较差	好	**较差**	好
安全性	弱	强	强	一般	弱

移动扩展性	一般	一般	好	差	较差

主流的 VPN 远程访问方式存在各自的弊端：

- 首先是客户端配置问题

除 WebVPN 外，其他方式在每个远程接入的终端都需要安装相应的客户端，并且需要做复杂的配置，随着这种远程接入客户端数量的增多将给网络管理员带来巨大的挑战。虽然一些领先的公司已经解决了部分客户端如 SSL VPN 客户端难以配置和维护的问题，但是还是无法避免在每个终端上安装客户端的麻烦，随着用户数量的增多，每天需要维护的客户端绝对数量也不少。

- 其次是兼容性问题

由于 VPN 涉及网络驱动的支持，因此 VPN 客户端对系统的兼容性需要投入大量研发精力解决，随着终端类型的频繁更新换代及操作系统的频繁升级，终端兼容性成为主流 VPN 在远程访问时的一大难点。

- 第三是身份认证问题

随着互联网威胁愈演愈烈，多因素认证已经成为系统远程访问最为有效的安全方案，但主流的 VPN 远程访问方案，除 SSL VPN 外，其他对多因素的支持普遍较差。

- 最后是移动设备支持问题

随着未来通讯技术的发展，移动终端的种类将会越来越多，VPN 客户端需要有更多的版本来适应这些终端，但随着终端种类的爆炸性增长，这几乎是不可能的。且移动应用程序的大量使用，VPN 除了要支持移动终端类型外，还需要兼容和适配大量的 APP，对于这种 C/S 架构的应用，WebVPN 就难以支持了。

基于上述背景，深信服 SSL VPN 以创新的 SSL VPN+WebVPN+EasyAPP 三合一 VPN 网关，完美的适用于各种远程访问场景。深信服三合一 VPN 网关的突出优势在于 Web 安全和移动接入，它可以提供远程的安全接入，而无需安装或设定客户端软件，同时针对安全要求高的系统，可以通过 SSL 构建高安全性的接入通道实现系统远程接入访问；针对移动 APP，提供深度融合的 SDK 方案，且可以自动封装应用实现 APP 的远程接入。

第 2 章 深信服 SSL VPN 三合一网关简介

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更快、更安全、更好用的远程接入产品，保护客户的业务安全可靠，提高客户的业务效率，从而实现共同成长。

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，深信服科技运用最为创新性的方案，为客户有效地解决业务在互联网转化的过程中所遇到的问题。除了像移动办公方案和多方接入的权限分配方案这些传统 SSL VPN 应用之外，深信服科技还不断提出创新性的运用，比如使用 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 加密和逻辑隔离的特性为客户的核心数据实现安全防泄密。另外，结合深信服科技在前沿网络领域中完善的技术，为客户提供了更具价值的整体解决方案，比如 SSL VPN 和 WebVPN 二合一的解决方案，EasyApp 方案等。通过大量的成功客户案例，证明了深信服科技在以客户为导向理念下，已经获得了市场的高度认可。

业界持续领先的技术理念

为了给客户提供最为完善的SSL VPN 产品，深信服科技持续引领着业界内的技术创新。从 2005 年在全球第一家推出 IPsec/SSL 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，2009 年在全球首家实现非对称集群、智能隧道选路等技术，2010 年更是推出了更快速的流缓存加速技术，2013 年推出了 APP 应用封装方案，2017 年对 Web 接入技术进行革新，将 WebVPN 的系统兼容性再次提高到业内领先水平。深信服科技，运用最为创新的 SSL VPN 技术理念，为客户提供最好的 VPN，并主导了中华人民共和国国家 VPN 标准制定。

最广泛的客户认可度

深信服科技 SSL VPN 到 2019 年底为止，已经服务于超过 21000 家的用户，值得一提的是：世界五百强中的中国企业 80%都选用深信服科技的 VPN 解决方案。深信服科技 SSL VPN 从 2008 年开始，便以超过三分之一的市场，一直占据中国市场第一的位置，而且份额还在不断扩大，2015 年，深信服 SSL VPN 在大中华区市场占有率为 47.8%

第 3 章　深信服 SSL VPN 三合一网关技术优势

作为中国市场占有率第一的 VPN 解决方案供应商，深信服科技推出的三合一 VPN 网关有以下多种功能和技术特色：

3.1 更轻量的 WebVPN 提升访问体验

3.1.1 免客户端或浏览器插件远程接入

针对高校等大并发接入的 Web 业务系统，如果采用传统的 VPN 系统需要安装客户端或者浏览器插件，影响用户的使用体验，且增加了终端客户端的维护工作，深信服三合一 VPN 网关支持免客户端、免浏览器插件安全接入内网访问业务系统。

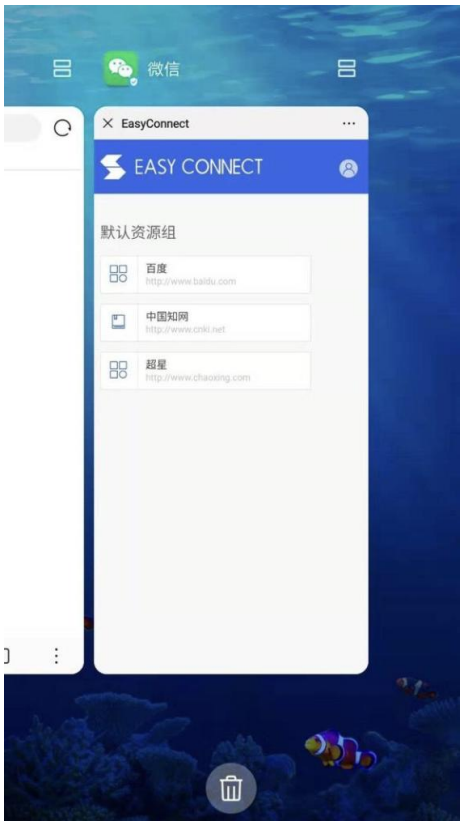
深信服采用的 WebVPN 技术，以 HTTP/HTTPS 透明代理技术，无需客户端即可实现像访问普通 Web 系统一样登录 VPN、访问内网资源。该技术以标准 HTTP 及 SSL 协议为基础，兼容所有标准浏览器及微信、企业微信、钉钉等超级 APP 内置浏览器。

3.1.2 用户端零配置使用

相比传统 IPSEC、PPTP 等 VPN 客户端的繁琐的配置过程，深信服三合一 VPN 的 WebVPN 方案无需 VPN 用户进行任何配置工作，只需浏览器打开指定 VPN 页面，即可实现即开即用、即关即走。

3.1.3支持第三方平台免插件接入

支持微信公众号、企业号、钉钉作为企业移动办公门户入口的接入场景，轻松结合 CAS 认证实现单点登录，让用户在微信上也可以享受免插件无感知的超便捷办公体验；



3.1.4 隐藏内部业务系统端口，减少暴露面

使用深信服 VPN 后，可以将所有的业务系统隐藏在内网，对外只开放 VPN 设备的 443 端口即可，用户如需访问内网业务系统，需要经过认证授权后才允许访问。

3.1.5 电子图书馆资源便捷访问

WebVPN 全网代理功能，支持在校外使用学校购买的图书馆资源，只需发布校内图书馆导航页，即可实现便捷访问所有图书馆资源，避免因资源漏配导致的无法访问。

3.1.6 对接统一认证，实现无感知访问

深信服 WebVPN 支持与各种统一认证系统对接，如 LDAP、radius、CAS 等，使用统一身份认证用户可以直接登录 WebVPN 使用。支持对接单点登录，访问校内业务系统无需二次认证。支持与校内统一门户的深度对接，实现无感知访问，用户在校外访问统一门户，登录后即可同步登录 VPN，无感知访问门户内校内业务系统。

3.2 更安全的 SSL VPN 为业务互联保驾护航

3.2.1丰富的认证方式

深信服 SSL VPN 三合一网关支持 LocalDB、LDAP/AD、Radius、第三方 CA、自建 CA、Dkey、短信认证（短信猫和短信网关）、企业微信、钉钉、硬件特征码、动态令牌多种安全认证方式，最大限度地保证了接入用户的合法性。

3.2.2混合认证保护机制

单一的认证方式易被窃取，为了进一步提高身份认证的安全性，深信服创新性提出混合认证，针对上面提到的用户名和密码、CA 数字证书、LDAP/AD、Radius、Dkey、硬件特征码、短信认证、动态令牌认证方式可以进行五个因素以上的捆绑认证，这几种认证方式必须同时满足才能够接入 SSL VPN 系统。如果需要几种接入方式做备份接入选择，那么深信服创新性提出或组合，对于以上几种认证方式进行或组合，只要通过一种主认证方式即可接入到 SSL VPN 系统中。

多种认证方式、完善的认证体系，使得企业在选择的时候，可以根据相应的安全级别，对客户端的认证方式进行组合，最大限度地保证了接入用户的合法性和企业内网资源的高度

安全。

3.2.3动态身份认证提供多重保证

当前间谍软件、木马等安全威胁日益严重，传统的基于口令的认证方式容易被窃取，一旦泄漏将造成企业数据的安全隐患。深信服科技采用了多种动态身份认证系统来消除该隐患，保证了用户使用 SSL VPN 访问总部资源时的安全性。

- DKEY 认证

深信服 SSL VPN 三合一网关采用 SSL 协议加密建立安全的专用加密通道，除了使用标准 SSL 协议内置的 RC4 等加密算法和 RSA128bit 签名算法来保证数据的安全性之外，还使用 DKEY（一种 USB 的身份认证设备）进行双因素身份认证，并使用 PIN 码保护 DKEY 的安全。这种 USB DKEY 可以同时支持两套 VPN（IPSec 和 SSL）系统，安全方便。

- 免驱动 USBDKey

针对一般的 USBDKEY 在使用的过程中跟 U 盘一样需要安装该 USB Key 的驱动，但是往往驱动的兼容性问题导致无法正常登录 SSL VPN，导致业务无法开展。针对这样的情况，深信服提出免驱动 DKey 认证，当您首次使用 DKey 进行登录的时候，不需要安装 DKey 也能够正常登录 SSL VPN，无需担心驱动的兼容新问题，提高业务访问效率。

- 短信认证

无线技术的突飞猛进给网络世界又带来一次巨大的革命，其灵活可靠的特点吸引了所有人的视线，因此，依靠无线通讯技术的短信认证技术也应运而生。短信认证技术是一种革新型认证解决方案，此认证系统分为手机短信终端和短信认证服务器两部份。终端用户在既有移动电话和 PAD 的基础上，通过手机短信获得双因素用户认证访问代码，就能够安全地访问网络资源。深信服支持与短信猫进行互动来进行短信认证。

- 短信网关

除了通过短信猫方式进行短信发送外，深信服还支持运营商的短信网关，如果您的网络中已经部署了短信网关（移动、联通或电信的短信网关），深信服可以和您的短信网关结合，实现短信认证。

当可能由于网络的延时或者网络运营商的问题导致短信未及时发出，完全影响了使用者的使用，导致业务无法正常使用，针对这样的情况，深信服为您提供短信重发功能，让您能够方便快捷使用短信认证。

- 硬件绑定（HardCA）

传统的用户名和密码或者 CA 证书认证方式都存在证书或密码被盗用的问题。为避免传统方案的泄密缺陷，SANGFOR SSL VPN 使用了深信服公司的特色技术－基于 PC 硬件特征的证书认证系统（HARDCA）来实现基于硬件的认证。该认证原理是将用户账号与其所在计算机硬件信息（如 CPU、硬盘、网卡等）进行绑定，即便用户账号意外泄露，由于非法用户无法使用与此账号事先绑定的那台计算机，因而不会造成非法用户接入。

- 动态令牌认证

动态令牌是技术领先的一种双因素强身份认证体系，采用用户 PIN 码+动态令牌码构成完整用户口令，令牌码由令牌内置唯一种子和当前时间通过伪随机算法生成，每分钟改变一次，而且是一次性密码（密码使用后立即失效，不能重复使用）。由于实际上的安全问题都和密码有关，盗窃和破解密码是最常见的口令攻击手段，因此动态令牌很好的解决了以上问

题，为用户的使用提供了极高的安全性保证。

3.2.4内置的 CA 中心提供完整认证体系

深信服 SSL VPN 三合一网关内置了 CA 中心，企业或者事业单位可自建 CA 中心，用户可不必购买单独的 CA 认证体系，为企业减少了投入成本。同时，深信服 SSL VPN 三合一网关也可无缝支持已有的第三方 CA 认证。深信服内置的 CA 中心可以支持建立服务器证书和个人身份证书，在减少投资成本的同时可以满足组织对于 CA 的大规模使用，让您构建您自己的 CA 认证中心。

3.2.5与第三方 CA 结合

为了建立更加完善的认证体制，很多企业引进了 CA 中心，通过 CA 中心来建立更加完善的认证体制。深信服 SSLVPN 能够更好的实现与 CA 中心这样的认证体制的结合，支持包括 UCS-2， GBK， UTF-8， GB2312， BIG5 编码格式，支持 der、crt、cer、p12、pfx、p7b 格式证书，还可以读取 CA 证书中的指定字段，形成身份账号绑定和从而能够与第三方 CA 进行完美的结合，满足大规模用户对于认证的要求。

深信服 SSLVPN 与第三方 CA 结合，还可以支持设置证书中的内置授权值，并与之绑定账号完成组织结构的建立，达到更完美支持 CA 证书认证的效果。同时，深信服 SSL VPN 至少支持 5 张不同的 CA 根证书，，以及配置证书绑定字段以及批量导入/导出用户证书记录等，即使是复杂数字证书体系也能良好的支持。

3.2.6与 LDAP（AD）结合

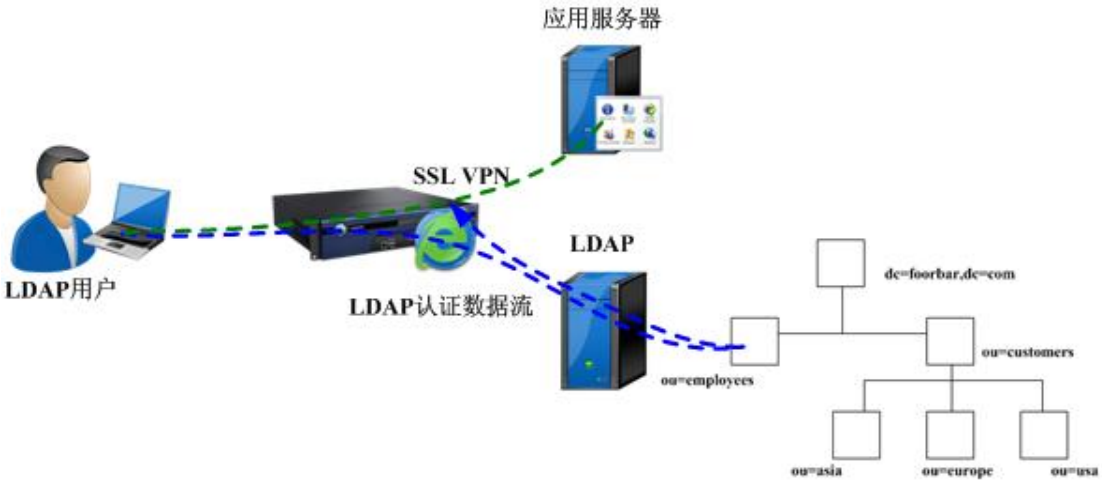
随着组织规模的扩大，为了更好的进行认证，大部分的组织都建立了 LDAP（AD）服务器，通过 LDAP 服务器来进行人员的统一管理。LDAP 可以根据组织内部的结构来进行人员的划分，完全根据企业内部的组织架构来建立 LDAP 的人员结构。

深信服能够与 LDAP 进行联动，无需在 SSL VPN 设备上建立 LDAP 上的用户，直接将认证的数据转向 LDAP 服务器，让 LDAP 进行判断。如果有一些特殊的需要，也可以将 LDAP 中的用户导入到设备中，可以根据您的需要定时进行同步，您可以选择一个固定的时间进行同步，也可以选择实时的进行同步，从而保证 LDAP 上的用户与 SSL VPN 上的用户信息保持同步。

为了更好的体现认证的多样性，深信服 SSL VPN 提供读取 LDAP 中的手机号码，可以跟短信认证结合起来，这样就可以实现与 LDAP 结合的双因素认证。

对于在 LDAP 中已经划分好了权限的情况，为了保持跟 LDAP 中权限的一致性，深信服 SSL VPN 支持导入 LDAP 中的 Group 属性，这样就可以完美继承 LDAP 中的权限属性，从而与 LDAP 中的权限保持一致。

当大量的用户通过 LDAP 进行认证，但是本地 SSL VPN 数据库中没有用户信息也无法分配虚拟 IP，那就没有办法使用 IP 资源。为了解决这样的问题，深信服可以读取 LDAP 中的 IP 字段属性，从而通过 LDAP 可以进行虚拟 IP 的分配，这样通过 LDAP 进行认证的用户可以得到虚拟 IP 实现双向访问。



3.2.7与 Radius 结合

Radius 作为 3A 体系中重要的一个元素，对于一些大型的集团型公司来说都部署了

Radius 服务器作为身份认证的一个因素，如果重新在 SSL VPN 上建立一套认证体制的化就会造成需要管理两套认证体制，因此为了减少增加认证体制所带来的麻烦。SSL VPN 需要与 Radius 进行完美的结合。

深信服 SSL VPN 能够读取 Radius 的分组权限信息，这样在 Radius 中已经建立好的分组就可以映射到 SSL VPN 中，从而实现角色的划分和资源的绑定。

同样为了实现多样的认证，深信服 SSL VPN 也支持读取 Radius 中的手机号码属性，从而跟短信认证可以完美结合，实现双因素的认证。

同样为了实现通过 Radius 进行认证的用户也能够分配到虚拟 IP，深信服 SSL VPN 可以读取 Radius 中的 IP 属性段，从而也可以绑定虚拟 IP，实现通过 Radius 访问也能够进行 IP 资源的正常访问。

3.2.8与口袋助理 APP 结合认证

SSL VPN 短信认证通常需要与企业短信平台进行集成，SSL VPN 短信认证模块支持与 GSM/CDMA 短信猫或短信网关联动，通过下发实时短信验证码的形式，验证用户信息，提高用户登录 SSL VPN 身份验证安全。

传统短信认证方式存在的问题：

费用高

使用短信猫方式，需要购买硬件短信猫，并支付短信费用

使用短信网关方式，同样需要支付短信费用，甚至需要购买短信代理平台

通过上面分析我们可以得出，无论是短信猫还是短信网关方式，都需要支付短信费，而且费用不低。以一个公司平均每天 1000 次登录为例计算，一条短信费大致为 8 分，那么一年的投入是：1000*0.08*365=29200 元

如果使用包月套餐，目前的市场价格大致为 2000 元/月包 30000 条短信，超出部分按一条 1 毛钱另外计费。那么一年的投入是：2000*12=24000 元。

由此可见，客户每年在短信费上投入的成本着实不少。而且用户越多，使用时间越长，成本越高。例如使用短信网关 5 年，投入成本将达 10 万以上。

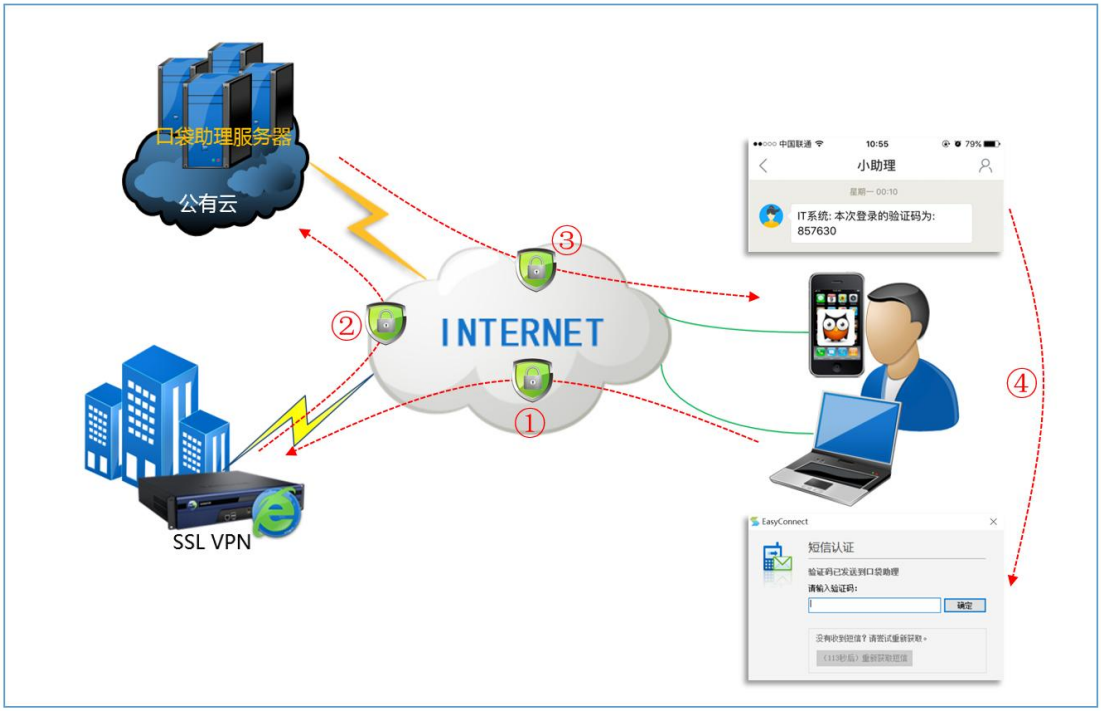
稳定差

使用短信猫方式，批量发送能力差、发送速度慢、有延时，在信号不好的机房使用可能发送质量不稳定。

使用短信网关方式，虽然批量发送能力较强，但是运营商对短信猫内容有严格的审计和过滤，可能导致 VPN 用户无法正常接收到验证码短信。

使用短信网关方式，每个手机号码在一定时间内发送的短信条数有限制，如果用户频繁获取短信验证码，可能导致短信通道被封，所有用户都无法正常接收短信验证码，严重影响办公。

将 SSL VPN 和深信服口袋助理 APP 相结合，用户登录 SSL VPN 时，SSL 设备将短信验证通过互联网发送至用户手机上安装的口袋助理 APP，替代使用短信猫或短信网关发送验证码的方式，实现短信认证



更低投入：口袋助理免费使用，只需开通短信认证模块，无需购买短信猫或短信网关，无需支付短信费用，每年可为客户节省 2 万元以上的短信费用（以每天 1000 次登录计算）

更稳定：通过口袋助理发送短信验证码，发送稳定，消息抵达率 99.99%；而一般的短信网关消息抵达率通常只有 95%左右。

更实时：通过口袋助理认证登录，能够即时抵达和校验。而短信消息通常会存在几秒甚至几分钟的延迟。

更佳体验：通过口袋助理扫描二维码认证登录，用户使用起来体验更佳，无需手工输入验证码。

更大并发：支持大并发，同一时间有大量用户登录都可以轻松应对，保障短信验证码如期到达。

免维护：用户无需自行维护短信猫或短信网关，降低运维难度和成本。

3.2.9丰富的第三方认证对接能力

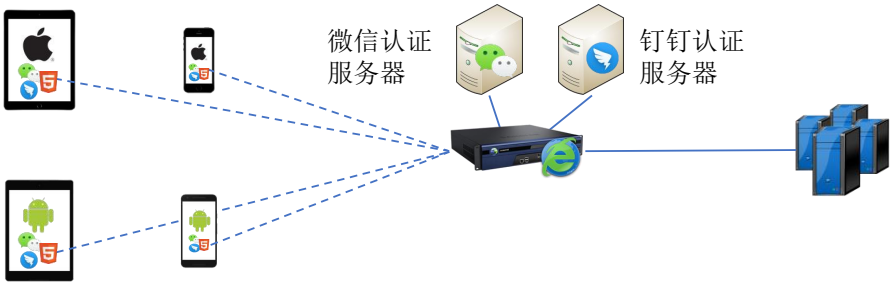
支持 http(s)认证插件，标准化对接第三方 Web 统一身份认证，可做到 95%以上第三方 HTTP(S)认证服务器免定制对接，再也不用担心提定制，同时大幅度降低用户的投入成本；

支持 http(s)令牌认证，免定制实现与各类第三方令牌认证对接，增强产品自身认证机制，为用户实现更灵活、成本更低的多因素认证方式；

支持与腾讯云网关、阿里云网关等第三方公有云短信平台平滑对接，并且可同时对接多个短信服务，配置更加灵活简单，全面满足用户短信验证需求；

3.2.10 支持与钉钉/企业微信等互联网 APP 结合认证

移动互联网的发展，使得微信、钉钉等互联网应用普及率非常高，很多组织都在利用这些社交应用来进行业务上的沟通。作为 VPN 市场的领导者，深信服在不断的创新，支持以微信企业号和钉钉企业应用作为入口，远程访问组织内部的 HTML5 移动 Web 应用。



利用深信服 SSL VPN，可将企业已有的 Web 应用与微信、钉钉的客户端、用户认证体系快速而安全集成在一起，保证用户身份安全的同时，业务的传输采用高强度企业级的 SSL 加密保护。

利用移动互联网应用作为移动办公的入口，有三大优势：

1、组织的员工不需要额外安装移动应用，移动办公可以快速推广普及；

2、基于 Web 技术的移动应用，几乎不需要培训，员工快速上手；

3、互联网应用的即时消息、语音视频通信功能，与组织的业务相关的应用互补，支撑组织业务移动化。

3.2.11 图形码验证功能

深信服 SSL VPN 三合一网关提供图形码校验功能，用户在输入用户名和密码以后还需要将系统随即生成图片中的信息输入才能实现正常登录，可以防止非法使用者用自动猜解程序来进行试探。深信服提供的图形验证码通过内部的计算程序可以实现数字和字母的组合，每次变换不同的图形验证码。

3.2.12 软键盘功能

为了提高用户密码的安全性，防止被木马程序截获用户输入的密码信息，深信服 SSL VPN 三合一网关提供了软键盘功能，用户在输入密码的时候可以使用界面上提供的软键盘，这样木马程序就无法采用截获用户键盘输入的方法来窃取密码了。为了进一步增加软键盘的安全性，深信服提供动态变换功能，即每次登陆的时候字母键和数字键跟上一次都是不同的，从而进一步保证密码的安全性。

3.2.13 会话超时控制功能

为防止用户在没有注销的情况下长时间离开，导致他人窥探到 SSL VPN 内的机密信息，深信服 SSL VPN 三合一网关特别加入了不活动检测引擎。

当检测到客户端在指定时间内没有任何访问内网资源的流量时，SSL VPN 网关将自动注销，中断会话并重新返回登录界面。

3.2.14 全面的密码安全保障

对于采用在 SSL VPN 上建立的用户名和密码，深信服采用了多种机制保证密码的安全性。

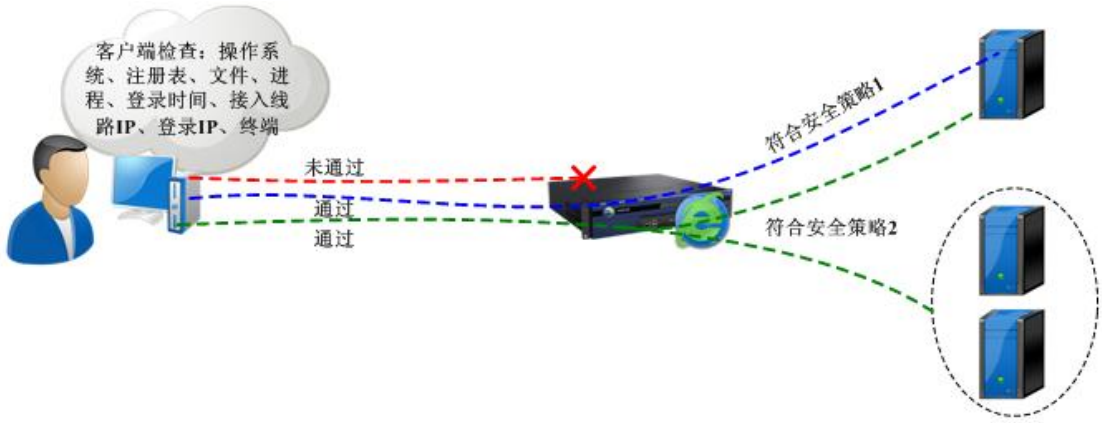
一旦系统启用防密码暴力功能以后，用户连续输入密码错误次数达到一定的数量以后，系统会将该帐号锁定一段时间，防止密码被暴力猜解。对于被锁定的用户可以通过查看锁定

用户在线列表来解除被锁定的用户，从而使其快速解冻。

面对大量的用户，管理员出于管理的方便可能针对每个用户设定了初始密码，但是出于密码的安全性考虑，必须提供一定的密码安全保障来保证密码的安全性。深信服提供强迫初次登陆修改密码，可以要求密码必须至少多少位，根据您的要求可以设定密码的最小长度，也可以设定密码必须包含数字、字母、特殊符号，从而保证密码的复杂度，但是不能要求密码与用户名相同、密码不能与旧密码相同。对于密码的管理，可以实现定时修改密码，密码过期前多少天提醒用户进行密码修改，通过上面一系列的措施保证用户的密码的安全性。

3.2.15 客户端安全检查从端点开始保障您的网络安全

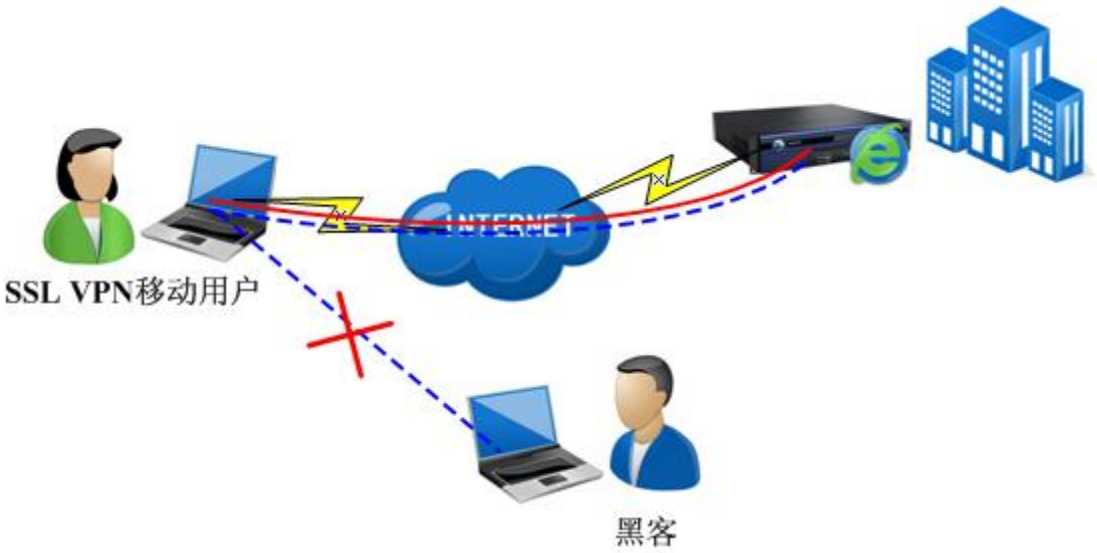
在用户通过计算机浏览器打开 SSL 登录界面时，深信服 SSL VPN 三合一网关通过客户端计算机安全扫描功能，检查计算机系统是否打了补丁、是否安装有相应杀毒程序等，保证 SANGFOR SSL VPN 接入安全，避免客户端计算机的不安全因素通过 SSL VPN 传输到企业内部网络产生的安全隐患。



SSL VPN 客户端安全检查保证接入安全

3.2.16 强化的网络防护－VPN 虚拟专线功能

虚拟专线指用户登录 SSL VPN 以后，和内部业务系统构成一条虚拟的专线，此时用户将不再能访问虚拟专线以外的网络资源。用户一旦启用虚拟专线功能后，一方面外部网络上面的不安全因素无法再对 VPN 系统构成威胁，同时也可以避免客户端上的不安全因素造成泄密的可能性，避免因客户端引发的安全隐患，确保内部业务系统的安全性。



3.2.17 零痕迹访问功能避免安全漏洞

SANGFOR SSL VPN 在用户结束访问以后会自动清除 Cookie、临时文件等遗留在客户端计算机上的信息，实现“零痕迹”访问，避免安全隐患。

3.2.18 支持国产商用密码标准

数据加密是信息安全体系中重要的安全保障环节，随着科技的不断发展，常用的商业密码算法（如 DES,RSA,MD5 等）已确认可被破解。密码技术存在短板，安全设备就形同虚设，只有采用相对安全的密码算法，才实现真正的网络安全。因此，国家密码管理局出台了新的密码算法（SM1，SM2，SM3，SM4）并要求相关单位选用国产商用密码标准。深信服 SSL VPN 支持常见的国际通用商用密码算法，同时也支持国密局规定的国产商用密码标准，全面保障用户的业务安全。

3.2.19 访问权限控制功能提供最细致的权限管理

SANGFOR SSL VPN 通过独特的角色管理功能，提供了细致到每个 URL 和不同应用的权限划分。通过给不同用户设置不同角色来分配访问授权，一个用户可以赋予多个角色以适合各种复杂的组织结构。基于角色的访问限制为企业网络提供了较强的安全性。通过行为跟踪引擎，管理员还可以查看远程接入用户的所有访问记录。

SANGFOR SSL VPN 内置有多种用户和资源管理方式，可以自建用户，也可以从第三方导入，支持 LDAP/AD、RADIUS 等第三方认证，可以根据用户、用户组、公用账号、私

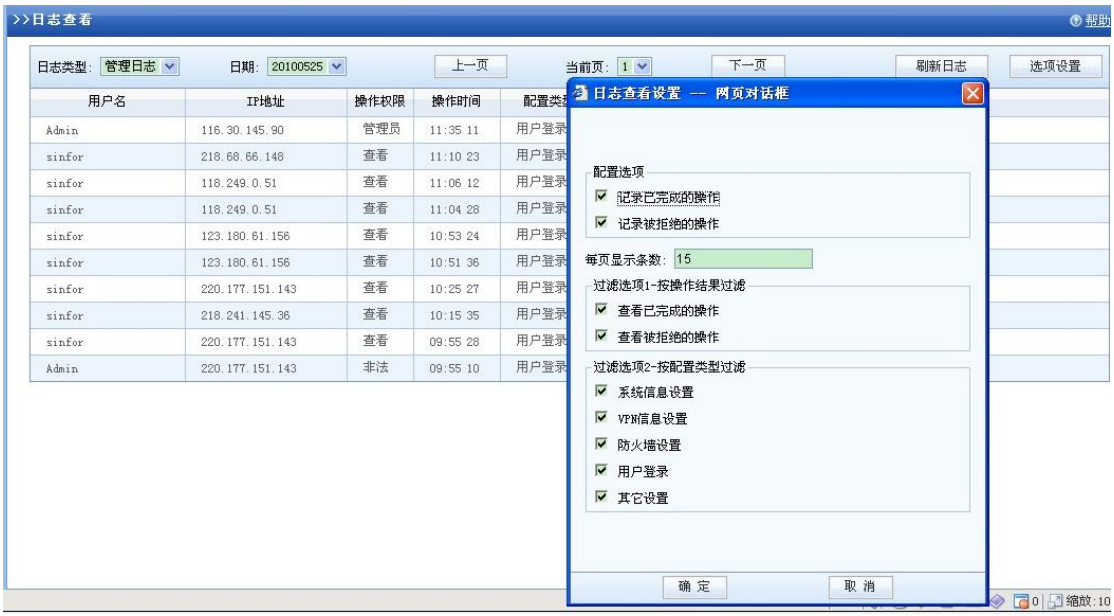
有账号等多种方式对用户进行管理。管理员可根据角色、Web 资源、C/S 资源、IP 资源等权限划分方式，为远程接入用户分配细致的访问权限控制。

同时，SANGFOR SSL VPN 集成了用户并发限制、公用账号并发限制和用户流量限制等多种方式，保证了用户合理地使用 VPN 资源。并且，在 SSL VPN 网关中的直观式管理图形用户界面（GUI）的实时监控状态栏中，可以实时地监控用户的接入情况，观察整个 VPN 系统的运行状况。

3.2.20 完善的日志系统

SANGFOR SSL VPN 网关提供了调试、信息、告警、错误四个级别的运行日志，帮助管理诊断系统。并提供了用户访问记录审计和报表来记录、跟踪用户行为。

由于 VPN 网关的存储空间有限，SANGFOR SSL VPN 还提供了独立的日志中心。通过第三方的日志中心，管理员可按照饼图、柱状图、曲线图等多种显示方式对服务的被访问次数、被拒绝次数，用户的登录次数、告警次数等进行直观显示，并可直接打印和导出。深信服 SSL VPN 三合一网关丰富的日志中心，为网络管理员和决策者了解 VPN 资源的详细使用情况提供了最有效的数据支持。

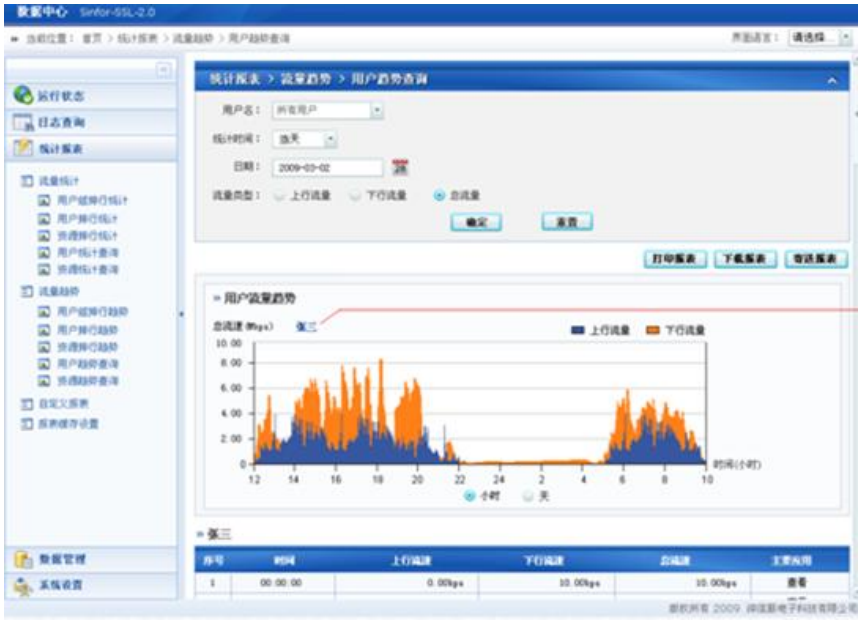


3.2.21 丰富的日志信息

SANGFOR SSL VPN 通过独立的第三方日志服务器，用户可以按照系统日志和用户日志两大类日志进行查询。管理员可对指定时间范围内的日志以及日志的级别如：错误、告警、

信息、调试和进程类型进行查询。

同时，管理员可按照饼图、柱状图、曲线图等多种显示方式对服务的被访问次数、被拒绝次数，用户的登录次数、告警次数等进行直观显示，并可直接打印和导出。深信服 SSL VPN 三合一网关丰富的日志中心，可详细分析出企业 VPN 资源的详细使用情况，为网络管理员和决策者提供了最有效的数据支持。



3.2.22 强大的实时监控能力

通过远程监控平台，管理员可以实时地监控用户的接入情况，实时观察 SSL VPN 安全网关的运行情况。通过 SSL VPN 丰富的系统日志，可以及时定位故障，并实施远程维护。

通过 Web 界面，管理员还可以随时查看每个在线用户的情况，可以随时中断可疑会话，方便快捷。还可以实现告警的短信通知，及时通知到终端用户。

3.2.23 集成企业级状态防火墙

和多数 SSL VPN 不同，SANGFOR SSL VPN 网关集成了高性能的企业级状态防火墙，对外只开放 443 端口，能有效保护内部服务器免受来自 Internet 的各种攻击。内置的防 DOS 攻击功能，不仅可以有效防范来自外部网络的 DOS 攻击，对于内网计算机发起的 DOS 攻击，SSL VPN 安全网关也可以进行防御。

深信服 SSL VPN 三合一网关集成了企业级的状态检测防火墙。除了拥有企业级防火墙所具备的基本功能如：管理员权限分级、URL 过滤、NAT 功能、访问监控、上网控制、用户认证、流量控制、QOS、DHCP 服务、自动拨号等功能以外，内置了高、中、低和自定义 4 个安全级别，用户可以根据需要灵活配置。此外，深信服 SSL VPN 三合一网关独特的虚拟测试功能，为管理员创建了防火墙规则的虚拟测试环境。管理员通过可视化界面，对各种安全设置规则进行测试，从而杜绝人为配置错误导致的安全漏洞。

作为 HTTPS 服务器，所有 SSL VPN 都同样面临着 DOS 的威胁。所以大多数 SSL VPN 设备都需要前置防火墙保护其安全。而 SANGFOR SSL VPN 自身就是一个防火墙，集成了对 DOS 等攻击的防御手段。

对于来自外部的 DOS 攻击，其防御 DOS 的基本原理如下：在网络层模拟应用层对 DOS 攻击的主机发起应答，由于 DOS 攻击主机无法完成 3 次握手，因此可以识别出不完整的请求，避免了把攻击发送到 SSL VPN 应用上。而对于真实的 SYN，在网络层完成了 SYN 的 3 次握手后，再模拟请求的客户端把 SYN 请求发送到应用层。通过这种 SYN 代理的方法就使得正常的 SSL VPN 远程访问顺利的通过防火墙到达内部服务器，而 DOS 攻击则被拒之门外。

深信服 SSL VPN 三合一网关不仅可以防御来自外网的 DOS 攻击，对于内网计算机发起的 DOS 攻击，SSL VPN 安全网关也可以进行防御。管理员可以在深信服 SSL VPN 三合一网关内增添内网网段列表，若检测到来自该列表之内的计算机发起的连接请求，则认为是合法用户；而若是来自该列表之外的 IP 地址，则被认为是攻击。这对于通常伪造源 IP 地址的 DOS 攻击发起端来说，将是一个有效的防范措施。

同时，深信服 SSL VPN 三合一网关可以限制内部局域网每个 IP 地址在一分钟内可发起的最大 TCP 连接数和发送的最大 SYN 包次数（数值可依据内网计算机数量自定义），阻止

了局域网内某些计算机感染了病毒或者木马程序，对外发起大量的连接请求从而导致企业网络带宽耗尽、网关设备瘫痪宕机等情况的发生。一旦检测到攻击后，深信服 SSL VPN 三合一网关可以立即对攻击主机进行封锁，从而及时有效阻断了由企业局域网内部计算机发起的 DOS 攻击行为，避免了企业员工在上网时不小心感染了病毒而造成 DOS 攻击给企业带来的法律纠纷、名誉受损等风险。

3.3 更快的 SSL VPN 提升业务办公效率

SSLVPN 实现了便捷而又安全的办公同时，也受到了互联网的环境制约，办公效率会被互联网的链路质量所影响。如果是存在跨运营商的链路，向服务器传递一个附件需要等待几十秒毫不出奇，在业务操作的过程中反复的等待时间将会严重影响到办公效率。为了帮助客户更好利用互联网技术提升业务效率，深信服致力于开发更快速的的业务访问模式，利用多种广域网加速技术，提升系统的响应速度。

3.3.1自主研发单边加速技术，极大提升应用访问速度

深信服科技的单边加速技术，是一种兼具灵活性和普适性的传输优化手段，能够显著提高网络效率，提升空间一般在 2 倍至 10 倍之间，有的情况甚至高达 100 倍。以往通过广域网进行应用访问需几分钟甚至是几小时，现在只需几秒或数十秒就可完成，极大的提升用户的访问速度。

单边加速技术通过对拥塞算法做优化处理，解决一些 TCP 协议本身的缺陷，以实现加速的效果；其核心部分是对拥塞算法做优化，如慢启动，拥塞避免，快速重传，快速恢复等。

拥塞避免－能够快速的准确的预估出网络中可用带宽，并根据估计值确定拥塞避免窗口，从而最大限度的利用网络带宽。

快速重传－允许接收端通过使用 SACK TCP 选项指示最多四个接收数据的非邻接块。RFC 2883 定义用于确认重复的数据包的 SACK TCP 选项中的字段的额外使用。发送端可以通过此操作确定何时重传了不必要的段并调整其行为，以防今后不必要的重传。发送的重传越少，整体吞吐量越合理。

快速恢复－快速检测出丢包，并能快速准确重传该包，对时延较大，网络状况较差的情况能够有效的提升带宽利用率，通过更改快速恢复过程中发送端可以用来提高发送速率的方

法，提供更大的吞吐量。

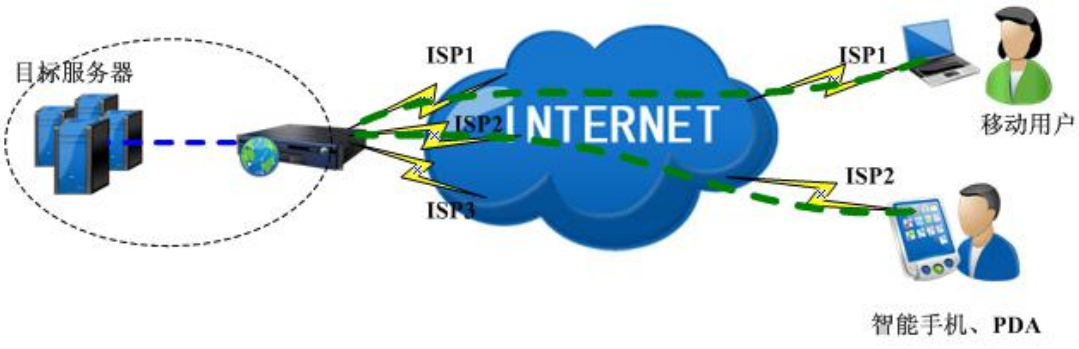
慢启动－避免发送 TCP 对等方拥塞整个网络的现有算法被称为“慢启动”和“拥塞避免”。在连接最初发送数据和还原丢失段时，这些算法可以增大发送窗口，即发送端可以发送的段数量。对于每个接收到的确认段或每个已经确认的段，“慢启动”算法会以一个完整的 TCP 段增大发送窗口。对于每个已经确认的完整窗口的数据，“拥塞避免”算法以一个完整的 TCP 段增大发送窗口。利用这些算法增大发送窗口的速度就足以充分利用连接带宽。

3.3.2多线路智能选路解决您的网络延迟问题

作为国内领先的 VPN 和网络安全研发产商，深信服科技在 IPSec VPN 中，创新性地采用了多线路智能选路功能，并成功应用到深信服 SSL VPN 三合一网关中，针对 SSL VPN 更多使用的是浏览器进行登录，深信服创造性的提出了一种基于 Web 的自动选路方法（ZL200510121083.0），该技术是深信服科技在 VPN 领域众多专利技术之一。

所谓多线路智能选路技术，即是指在企业数据中心网络的网关位置部署深信服 SSL VPN 三合一网关，并申请多条运营商的上网线路连接 Internet 实现线路捆绑和带宽迭加。当远程的众多商业用户通过 SSL VPN 在使用不同运营商的上网线路访问总部资源时，SANGFOR SSL VPN 网关会自动检测最优线路，使得商业用户访问组织内部数据时能得到最高的访问速度，解决了网络环境存在延迟大、带宽小的瓶颈问题。

对于部分大型组织机构来说，往往出口已经部署了高端的路由器或者防火墙作为网关，面对已经完善的网络建设，SSL VPN 应该如何部署能够利用前置的两条线路进行自动选路，让分布在全国各地的移动人员选择更快速的的线路接入，提高效率。深信服进一步扩展了智能自动选路技术，提供了基于单臂模式下的自动选路，让众多的组织结构也能够实现自动的选路，提高业务办公效率。



3.3.3多线路带宽叠加技术，扩大出口带宽

现在移动办公的规模已经快速发展，随用访问者增多，必然给企业的出口带宽带来压力，一般的企业都会准备有多条网络出口，以作备用，如何利用这多条带宽把业务访问效率提高？如何让多条业务线路形成智能的热备以增强系统平台的稳定性？

通常要实现链路的访问负载和智能热备，企业需要另外购买负载均衡设备，这样就增加了 IT 的投入成本。

为了解决上述问题，高性价比、低成本地满足企业对带宽的要求，深信服科技发明了多线路带宽迭加及复用技术（专利号：CN200310112006X）。深信服 SSL VPN 三合一网关支持各种不同接入方式的线路绑定，最多可支持 6 条不同线路的带宽叠加和负载均衡，大大提高了 SSL VPN 的数据传输速度，并且通过内置防火墙/NAT 模块，还可以实现多线路共同访问 Internet，成倍提高了企业局域网内用户的上网速度。

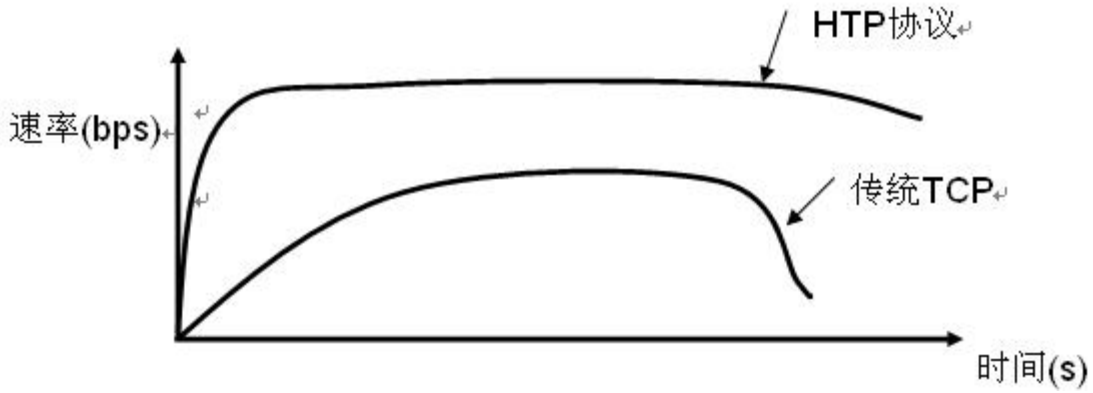
针对不同的上网线路，还可以启用多线路策略，用户可以根据线路情况选择带宽叠加模式、线路主备模式或者动态适应模式等多线路策略。同时，深信服 SSL VPN 三合一网关内置了 5 个 Qos 级别和多条 Qos 规则，用户可根据自身实际情况设置相应的 QOS 级别。

3.3.4HTP 技术，提高无线和恶劣环境下的访问速度

随着无线技术的发展，现在开始普遍使用 3G 网络来实现随时随地的商务接入，虽然 3G 网络速度对比以前的 GPRS 大有提升，但是仍然受环境影响。除了无线环境外，平时我们在公共网络中使用的网络由于 P2P 类下载软件的流行，导致带宽被占用，那么通过这样的线路访问 SSL VPN 的时候同样非常的慢。

实际以上所有速度慢的问题都是由于网络中存在的延时和丢包导致的，时延大和高丢包导致网络传输环境非常的差，而往往时延越大传输速度越慢，如果丢包达到一定程度，速度就会更加的慢，双方根本就无线建立通信，更不要说进行数据的传输了。

针对这样的情况，深信服提出了 HTP 技术。HTP 协议（HighSpeed Transmission Protocol）是基于 UDP 的可靠传输协议，通过改善拥塞控制算法和提高窗口大小改善 TCP 传输效率，能够显著提升存在丢包和延时网络的传输速度。

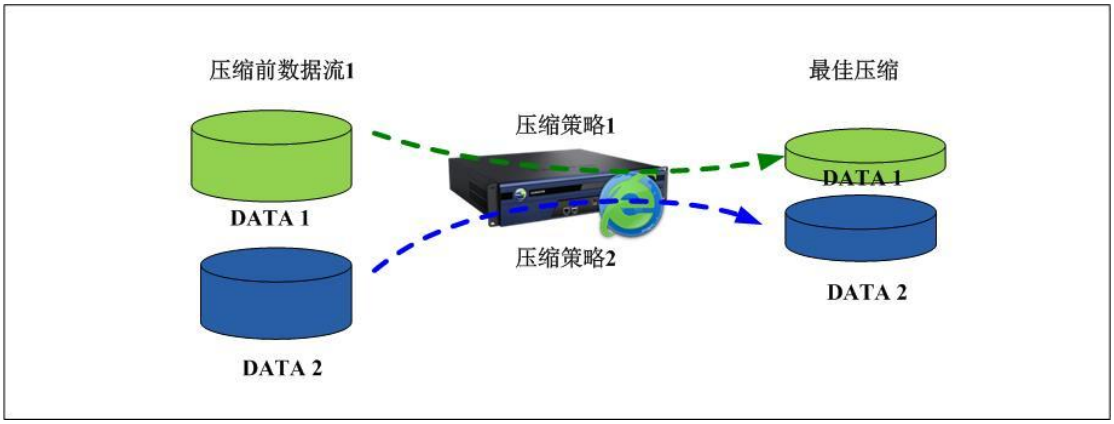


HTP 协议图示

3.3.5动态压缩技术，全面提高传输速度

随着业务的增长，交互的数据量也随之增加，本身传统的压缩对于所有类型的数据进行压缩，而压缩也必然会消耗系统资源，导致性能下降。本身有些数据由于结构的特殊性可能压缩比不高，一旦进行了压缩，消耗了系统资源却没有提升多少速度！严重影响了效率，降低了响应速度。

针对这样的应用背景，深信服提出了动态压缩（专利号：200810065397.7），针对不同的数据选用动态的压缩策略，根据上一次压缩状态来选择本次的压缩策略，通过动态选择策略来提高压缩效率的同时，降低系统负载，从而提高整体的数据处理速度，提高业务的访问速度。



3.3.6基于 Web 的压缩技术，进一步提高传输效率

随着软件技术的发展，越来越多的应用系统都采用了 B/S 的构架，当 B/S 应用数据量增大时，在一定的网络环境中必然会影响 B/S 应用的传输速度，因此有必要针对 B/S 类型的应用提供一定的压缩手段，深信服专门提供 Web 资源的压缩进一步提高传输效率。

3.3.7流缓存技术-大幅减少数据冗余碎片

SANGFOR SSL VPN 采用 SANGFORSpeed2 加速引擎中特有的“基于码流特征的数据优化”技术，能够大大降低广域网传输过程中的数据流量，根据实际的测试最多时甚至能够将流量减少 95%以上。

深信服流缓存技术原理是：在广域网中传输的是数据包，就是类似于“010100011”这样的 0 和 1 的数字组合排列，“基于码流特征的数据优化”技术能够把数据包拆分成很多“碎片”，并对“碎片”分配唯一指针，将指针分别存储在本地设备和目的地接收设备中，当具有相同指针内容再次需要传输时，只传输指针到目的地，接收设备根据指针便在本地的设备中提取出内容。

只要“碎片”足够小，传递内容相同的概率就会足够大。对于同一个用户而言，往往需要频繁传输相同或相似信息，效果非常明显。

举一个简单的例子，如对于 PPT 文件来讲，所有页码中 Logo、表头、表尾内容都是相同的，不需要重传，并且对再次更改的 PPT，往往只是更改了非常少的内容，再次传送则实际上仅需要传送更改的内容即可。

目前很多加速产品采用了文件缓存方式进行加速，即将文件缓存在网关上，用户访问文件的时候实际上是从本地网关取得文件，并没有直接访问远程服务器上的文件，这种方法存在两个比较明显的问题：

1、 无法保证文件的实时性，如果服务器上面的文件更新了，可能导致用户访问的还是更新以前的版本。

2、 如果服务器上面的文件变化较小，比如一个 100MB 的 ZIP 文件中增加了一个 1MB 打包文件，需要将整个文件重新传输一次。

SANGFORSpeed2 引擎中的“基于码流特征的数据优化”技术完全可以来替代文件缓存技术，通过优化的模式匹配算法，可以使网络中传输的数据足够小，能够达到和文件缓存相当的加速速度，还能在保证实时性同时对变化较小的文件同样能够起到加速作用。

使用流缓存的客户端，完全不需要做任何的配置，就可以自如启用，流缓存效果也会一一用直观的报表呈现出来。

3.4 更好用的 SSL VPN

SSLVPN 设备最终使用者是业务系统使用者，这样的终端用户通常不会具备过多的 IT 技能，所以 SSLVPN 作为业务登录平台，必须具备足够的易用性，才能更好帮助企业进行信息化建设。

3.4.1支持所有网络应用

深信服 SSL VPN 三合一网关通过 WEB 智能重构技术、应用转换技术和 IP Tunnel 技术，实现了对目前所有网络层以上各种静态或者动态端口应用的完全支持，WEB 智能重构技术，包括针对 HTML、XML、JS/VBS、Applet/ActiveX/Flash 等多种网页技术实现重构；应用包括：包括：网上邻居、文件共享、TELNET、FTP、OUTLOOK、SQL、Lotus NOTES、SYBASE、ORACLE、CITRIX 等所有 IPSEC 能够支持的应用。

由于采用了 IP Tunnel 技术，深信服 SSL VPN 三合一网关实现了对应用程序的完整支持，客户端在打开浏览器的 SSL VPN 登录界面时，只需安装一个 Active X 控件（可选），在客户端的机器上会生成一块专门用于 SSL VPN 通讯的虚拟网卡，因而 SSL 远程登录用户便可使用所有基于 IP 网络层以上的应用。若 SANGFOR SSL VPN 在总部网络采用路由模式的部署方式，总部网络还能够实现与远程接入用户的双向访问。这种领先技术的应用，使得 SANGFOR SSL VPN 能够支持任何复杂的各种 B/S 和 C/S 的应用。

3.4.2全面适应各种平台

借助于浏览器技术，SANGFOR SSL VPN 可以支持所有网络环境，只要浏览器能够上网就可以使用 SSL VPN。

目前，SANGFOR SSL VPN 所支持的浏览器类型包含 Html/Dhtml， Jsp， Asp，Java applet， Active， Cookies 等各种 Web 技术，支持包括 IE、FireFox ，Safari，Google chrome，Opera 等主流浏览器；同时支持微软 Windows 系列、Linux 系列、Mac OS 系列等操作系统。为业务访问提供最广泛的兼容性。

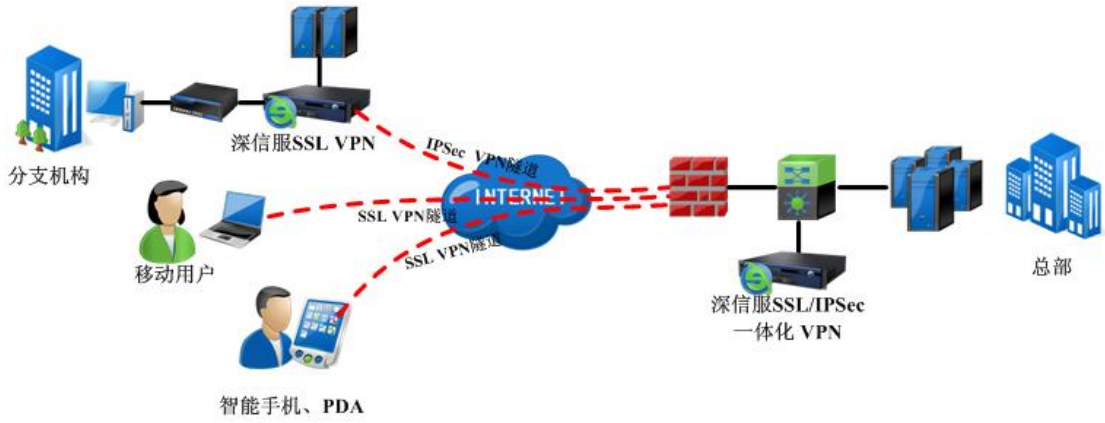
3.4.3提供 IPSec/SSL 一体化选择

传统的 IPSec VPN 在部署时，往往需要在每个远程接入的终端都安装相应的 IPSec 客户端，并需要做复杂的配置（SANGFOR IPSec VPN 采用 DKEY 方式实现 IPSec VPN 零配置）。

若企业的远程接入和移动办公数量增多，企业的维护成本将会成线性增加。而 SSL VPN 最大的好处之一就是不需要安装客户端程序，远程用户可以随时随地从任何浏览器上安全接入到内部网络，安全地访问应用程序，无需安装或设置客户端软件，降低了企业的维护成本。因而 SSL 在点对网互连方面，其易用性和安全性方面有着突出的优势。

由于 SSL VPN 只适合点对网的连接，无法实现多个网络之间的安全互连。因而，在企业组建网对网方面，IPSec VPN 就有着无可比拟的优势。而在点对网方面，由于 IPSec VPN 要求每个远程接入的终端都需要安装相应的 IPSec 客户端并需要配置，因而 IPSec VPN 在易用性和维护成本上远远不如 SSL VPN。

深信服 SSL VPN 三合一网关结合了 IPSec 和 SSL 两套主流的 VPN 技术，实现了在一台安全网关设备上稳定高效运行两套 VPN 系统。利用两者的优势进行互补，避免了单一 VPN 设备存在的不足。对于企业或者事业单位的分支网络，可以使用 IPSec VPN 实现安全互连，而对于内部员工、合作伙伴、移动人员可利用 SSL VPN 的易用性实现安全接入。最大限度地发挥了 IPSec /SSL VPN 给企业带来的效益，节约了企业大量的管理成本和投入成本，真正做到一台设备的投资，两种设备的功能 。



3.4.4虚拟门户功能

深信服 SSLVPN 借助于多页面隔离访问技术，实现独立的虚拟门户访问。

SSL VPN 虚拟门户功能的主要价值在于：

1、 安全性：实现登录用户的完全隔离访问。在终端登录用户使用中，他们将完全接触不到不同权限的其他用户，每一组单独使用不同的系统地址，不同的登录页面，不同的认证方式，访问不同的资源页面，从而实现完全的隔离访问。

2、 管理性：对于拥有不同的分支结构或者不同部门之间的登陆，虚拟门户能在一台设备上虚拟多个登录平台，提供给不用的用户组织使用，能实现多台设备分别登录的效果，实现更好的管理性。

虚拟门户功能，将让客户能把一台 SSLVPN 设备，虚拟成多台来提供不同的部门和分属子公司进行访问。

3.4.5配置向导简化管理员的操作过程

为了简化您的操作，深信服 SSL VPN 三合一网关提供了配置向导来对管理员的基本操作进行指引，管理员可以在配置向导的指引下完成对系统参数、资源、用户管理等的配置和修改，使得即使是对设备不太熟悉的用户也可以顺利的完成相关的配置工作。

3.4.6隐藏服务模式

在用户的资源列表中，除了对 C/S 应用的透明支持之外，SANGFOR SSL VPN 还增加了一个隐藏服务。用户在访问总部的 SSL 资源时，SSL VPN 可以将某些特殊的资源隐藏起来，用户在其资源列表中无法看到该项资源，但用户仍然可以使用。这种支持隐藏服务的功能，更加保证了企业内网资源的安全性。

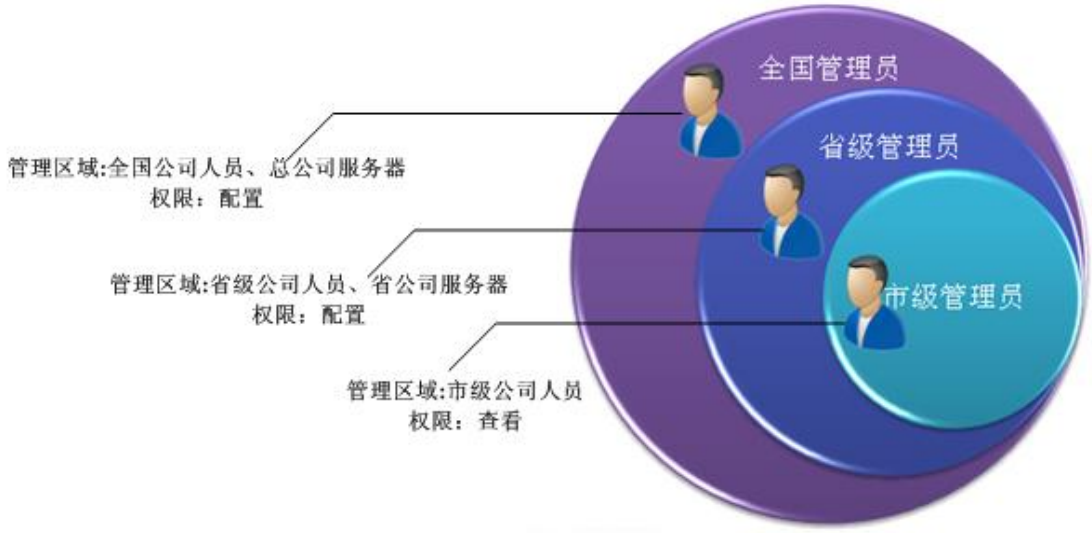
3.4.7支持动态 IP

由于宽带的普及以及 ADSL 资费的降低，国内中小型企业通常采用 ADSL 拨号等动态 IP 的方式接入互联网。SANGFOR SSL VPN 集成了深信服科技独创的基于 Web 的动态 IP 寻址技术（专利技术），使的 SANGFOR SSL VPN 网关在部署的时候无需固定 IP，完全支持动态 IP。并且，当企业在使用 SANGFOR SSL VPN 网关的 SSL VPN 功能时，可以使用和 IPSec VPN 相同的 Webagent 来解析网关的动态 IP，减少了管理员的维护量。移动办公人员使用浏览器连接入公司内网时，也更加便捷。由于支持动态 IP 接入，SANGFOR SSL VPN 同样也适合中小型企业。

3.4.8管理员分级分权限管理

通常我们在对普通用户管理的时候有多种的认证方法，但是却容易忽视另外一个和安全

密切相关的地方——没有为系统管理员提供足够的安全保障，普通的系统通常只需要使用用户名和密码就可以进行登录，深信服 SSL VPN 三合一网关能够为管理员访问也提供和普通用户相同的安全保障手段。根据企业内部的管理形式，深信服将设备管理员分为超级管理员和受限管理员，受限管理员只能管理所辖组的用户、用户组、所在组的硬件特征码、关联所在组的角色，不能对于不在所辖组的用户进行管理和维护。



3.4.9定制登录界面功能

深信服 SSL VPN 三合一网关的可定制登录界面功能，可以为远程用户创建全面可定制的登录界面，为不同角色的用户提供个性化的登录界面外观，从而改进用户体验。您可以将设计好的页面上传到设备中，从而完成登录页面的定制。可能在实际的操作中出现了一些意外，您也可以恢复到默认的页面，从而避免因为不合适的页面导致无法正常使用。

深信服在 SSL VPN 设备中已经建立了四套认证界面模板，您可以根据自身的需要选择合适的认证模板。

3.4.10 单点登录功能（SSO）

当通过 SSL VPN 发布了众多的应用系统之后，每登录一个应用系统都需要输入对应的用户名和密码才能够正常登录。但是众多的应用系统密码很容易是人搞混或者忘记，导致工作效率严重下降，为了避免记忆众多的应用系统密码而带来的麻烦，因此引入单点登录功能，您只需要登录 SSL VPN 系统后就可以直接登录到应用系统，避免再次手动输入用户名密码带来的麻烦，从而提高访问效率。深信服针对不同的应用系统提供不同的单点登录构建方式，针对 C/S 应用深信服采用提前录制的方式进行构建。针对 B/S 的应用解析其内部传递函数采

用自动构建访问参数的方式。为了提高单点登录数据传递的安全性，深信服提供根据javascript 函数来进行加密，保证单点登录信息传递的安全性。为了进一步提高单点登录的适用性，深信服提供针对不同的资源可以设定不同的单点登录账号，从而实现不同用户登录不同应用系统采用不同账号进行单点登录，提高了单点登录的方便性。

3.4.11 移动终端设备的完美支持

对 Android、IOS 等移动终端设备提供完美的支持，并且会根据终端设备的类型调整登录界面，为用户提供最好的显示效果。

3.4.12 移动 APP 安全接入

深信服 VPN 的 EasyApp 方案支持移动办公应用 VPN 安全接入。移动 App 通过轻量级 SDK 集成或自动封装，快速支持 VPN 接入，保护数据传输安全；移动应用服务器部署在内网，系统信息和漏洞被隐藏，有效降低恶意攻击和入侵的安全风险。加固后的安全应用可以安装在员工手机上(BYOD)和企业配发设备上(COPE)，快速满足移动邮件、移动 OA 等基本的移动办公需求。

3.4.13 内网 DNS 支持

内部拥有众多的应用系统，内部的 IP 都是随机进行分配，但是都通过一台 DNS 服务器进行解析。为了更好的实现解析，可以通过设置相关的解析规则，深信服 SSL VPN 支持“*”和“？”匹配符号的正则表达式（“*”表示任意字符串，“？”表示任意字符），可以设定内部的首选 DNS 和备选 DNS，从而实现对于域名的完整解析。

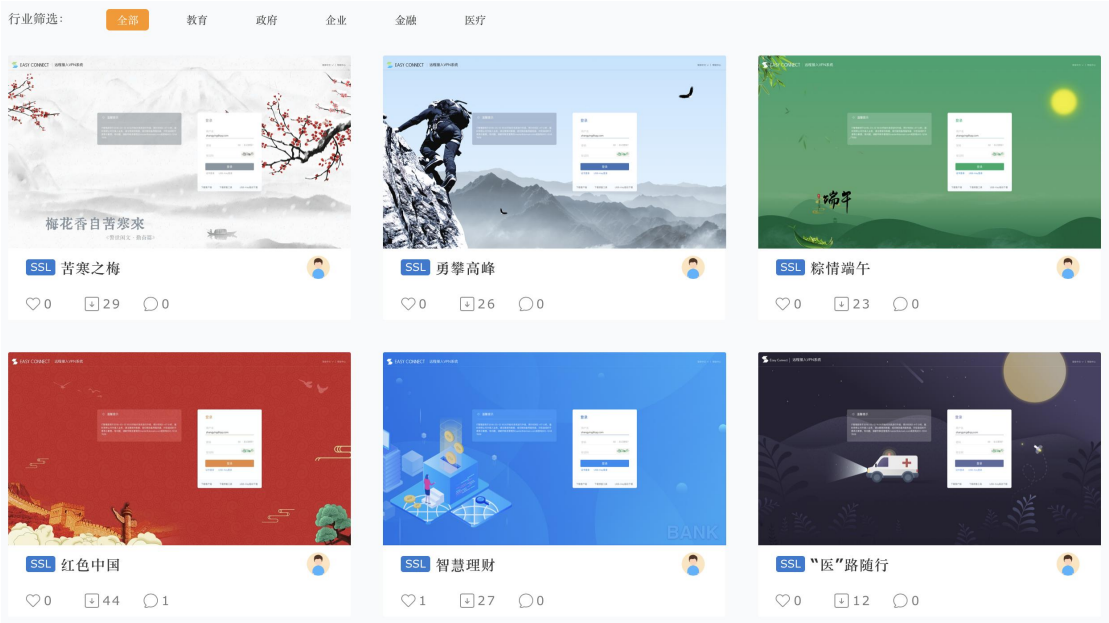
3.4.14 多虚拟 IP 池支持

通过深信服的 IP Tunnel 技术可以完美支持 IP 层以上的所有数据。为了让用户更好的使用 IP 资源，IPTunnel 必须获得相应的虚拟 IP 才可以正常的工作。但是对于一些大型的集团公司来说，已经规划好了 IP，需要实现根据远程接入的 IP 来实现身份的绑定，深信服可以针对每个人绑定固定的虚拟 IP，从而实现用户身份与虚拟 IP 的绑定。如果对于用户接入没有那么严格的要求，但是对于集团内部各个部门已经规划好了 IP 段，为了实现通过 IP 段来区分不同的部门，深信服可以实现用户组与 IP 池的绑定。对于通过第三方认证的用户，深

信服可以读取 LDAP 和 Radius 服务器上的虚拟 IP 信息，从而实现与第三方的完美结合。

3.4.15 主题商城

VPN 支持主题商城，尽显行业风采，同时支持企业自定义个性 UI，彰显企业风格。



3.5 更稳定的 SSL VPN

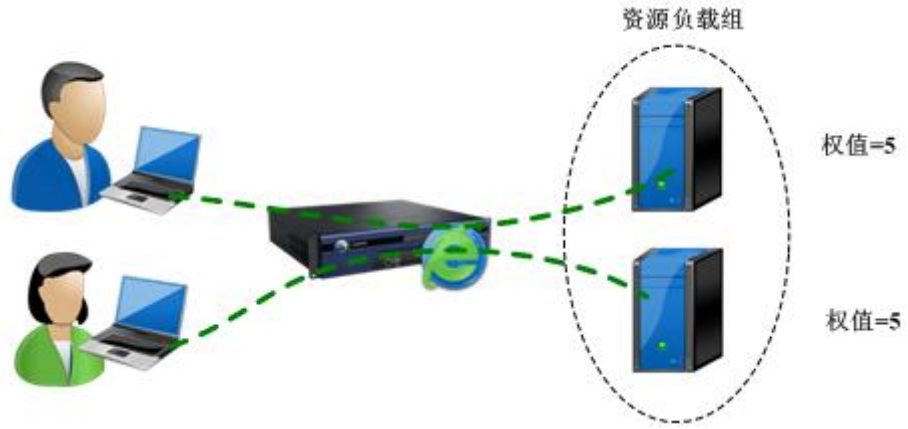
3.5.1多线路技术实现线路备份，保证 VPN 线路稳定

SANGFOR SSL VPN 支持多达 6 条线路的线路备份和负载均衡，大大提高了 VPN 网络的稳定性。由于 VPN 的稳定性是依赖于线路本身的稳定性，若采用单条线路，一旦中断，将造成整个 VPN 系统陷入瘫痪。通过多线路带宽迭加及复用技术（专利号：CN200310112006X），将多条线路、不同方式接入方式的上网线路实现带宽迭加和互为备份，保证了整个系统的持续可靠运行。若任何一条线路出现故障，SANGFOR SSL VPN 可以将数据无缝切换到其他正常线路，不会影响 SSL VPN 用户的接入和访问。并且若故障线路恢复正常，VPN 的连接隧道将自动愈合。这一切都是系统自动进行，无需人工干预，保证了用户的重要应用持续、不间断地稳定运行。

同时，深信服 SSL VPN 三合一网关还进一步实现了多条 Internet 线路的 QOS 功能，根据不同线路的带宽情况智能分配负载，最大限度的提高带宽利用率。

3.5.2资源服务器的智能负载功能

当业务系统访问量上去之后，单台服务器已经不足以支撑性能要求，这个时候就必须把多台服务器组建集群。为了能让多台服务器能更好工作，深信服 SSLVPN 设备可启用资源负载均衡访问机制。根据服务器自身的处理情况，可以对连入的多台资源服务器预设好的访问的权值，SSLVPN 设备智能分配终端用户的访问请求到对应的服务器。这样的好处一是能让终端用户得到效率最高的访问服务；二是在多台服务器之间实现了最佳的稳定性备份。



3.5.3会话自动恢复，提高网络适应能力

SANGFOR SSL VPN 提供了看门狗提供自动恢复功能和配置备份功能，支持 ADSL 断线重拨功能。若由于线路中断而造成的 VPN 隧道中断，一旦线路恢复，SANGFOR SSL VPN 随即将自动恢复，无需人工干预。

3.5.4非对称集群功能，满足大并发接入

面对大并发的用户量，单个设备所能承受的并发数毕竟有限。为了更好的支持大并发的用户，深信服可以通过多设备的集群功能实现接入的负载均衡，根据单台设备的性能将所有的 SSL VPN 连接动态的负载到所有设备上面，从而实现更大并发的用户接入。

深信服科技的多台集群之间实现了完美的 Session 同步，多台设备即时同时更新用户信息，在其中一台设备出现故障之后，该设备服务中的用户会被无缝迁移到其它设备，设备的意外事故将不会给用户的业务访问带来任何负面影响。

深信服 SSL VPN 创新地推出了非对称的跨型号集群功能，能支持不同型号的多台设备组建集群，这样企业就可以根据实际的需要情况，选择当前所需要购买的对应型号，给予企

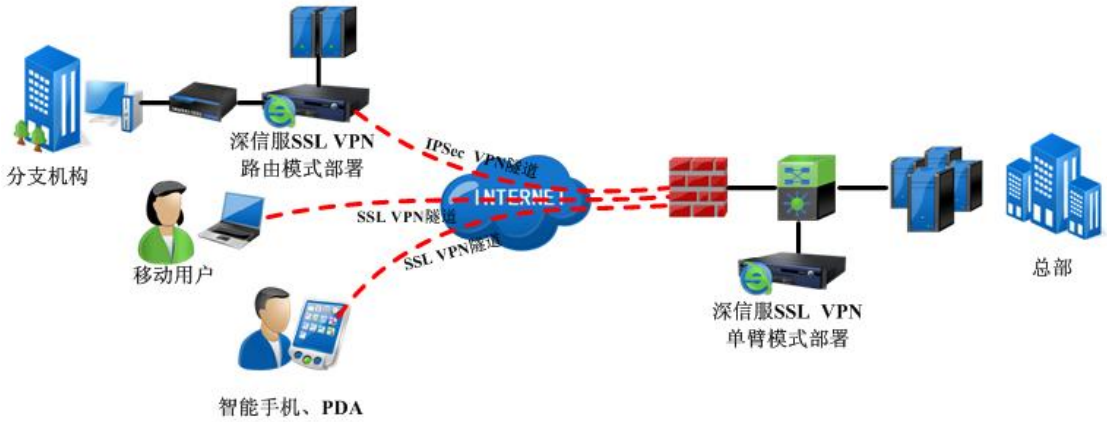
业信息化更为自主的规划空间。

第 4 章　SSL VPN 部署模式及用户使用

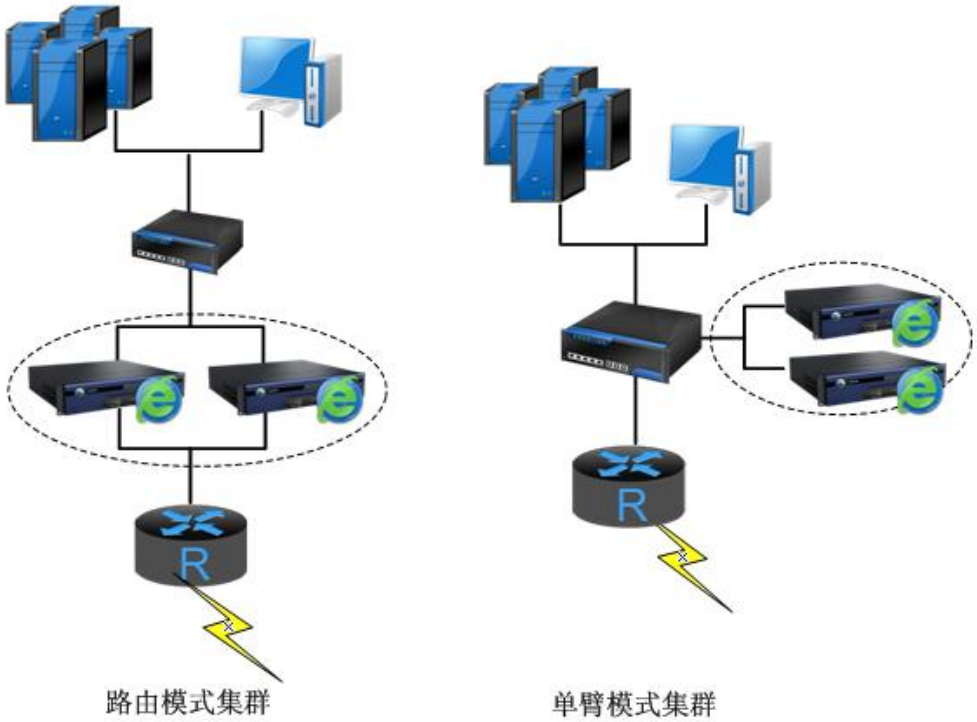
4.1 深信服 SSL VPN 三合一网关部署模式

深信服 SSL VPN 支持路由部署及单臂部署两种模式。

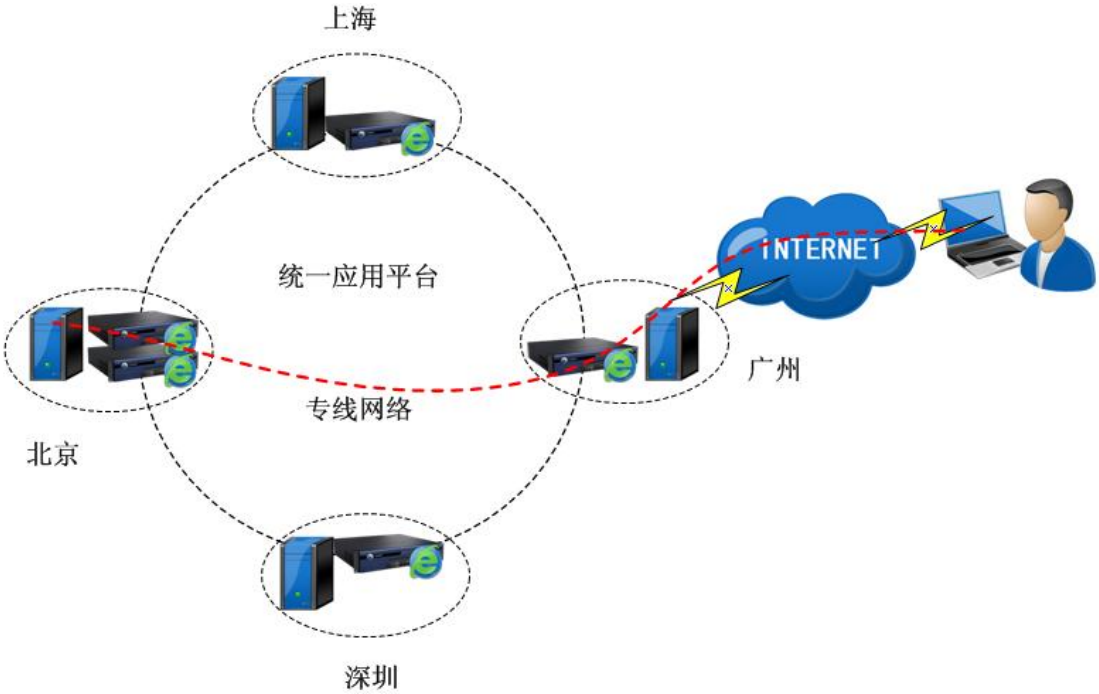
除了最基本的路由模式外，深信服 SSL VPN 支持单臂模式部署，不需要对用户现网结构做任何改变，不影响用户业务的正常使用。



支持路由模式、单臂模式部署



集群模式部署



全网分布式集群部署