深信服科技

SSL VPN 产品白皮书

深信服科技有限公司
2015 年 11 月

版权声明

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。

深圳市深信服电子科技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，但深圳市深信服电子科技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：800-830-9565 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

深信服科技网站：www.sangfor.com.cn

深信服社区：bbs.sangfor.com.cn

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：企业本身的商业数据、企业的客户数据信息等一旦被泄露，则会带来难以估计的损失，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。由此，业务信息化，首先需要解决的是安全问题。

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。过去，大多数公司都是使用传统的 IPSec VPN 来解决远程接入的问题。但是 IPSec VPN 最初是为了解决 Lan To Lan（网对网）的安全问题而制定的协议，因此在此基础上建立的远程接入方案在面临越来越多的 End To Lan（点对网）应用情况下已经力不从心。

IPSec VPN 应用于端点接入的不便：

- 首先是客户端配置问题

在每个远程接入的终端都需要安装相应的 IPSec 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 IPSec 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，即使这些客户端很少出问题，但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 IPSec VPN 自身安全问题

往往传统的 IPSec 解决方案都没有很好的解决移动用户接入到私有网络的安全控制问题，这样就为病毒传播和黑客入侵提供了很多可能的途径深信服科技的 IPSec VPN 已经比较好的解决了这个问题，深信服科技使用硬件鉴权认证来实现设备的认证接入，使用 VPN 专线功能来实现和互联网的逻辑隔离，来保证入侵安全性。如果仅仅在受控的电脑上，比如员工办公电脑上使用 IPSec 客户端则可以通过部署统一的安全策略来解决该问题，但如果要

让合作伙伴或者客户的电脑接入，就难以控制了。

- 然后是对网络的支持问题

传统的 IPSec VPN 在网络适应性上都存在一些问题，虽然一些领导厂商已经或正在解决网络兼容性问题，但由于 IPSec VPN 对防火墙的安全策略的配置较为复杂（往往要开放一些非常用端口），因此客户端的网络适应性还是不能做到百分之百完美。

- 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，IPSec 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。

因此 SSL VPN 技术就孕育而生了，SSL VPN 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。SSL 在 Web 的易用性和安全性方面架起了一座桥梁。目前，对 SSL VPN 公认的三大好处是：首先是它的简单性，它不需要复杂配置，可以立即安装、立即生效；第二个好处是不需要安装客户端，直接利用浏览器中内嵌的 SSL 协议就行；第三个好处是兼容性好，可以适用于任何的终端及操作系统。

但 SSL VPN 并不能完全取代 IPSec VPN，这两种技术目前应用在不同的领域，是可以进行互补的。SSL VPN 考虑的是单点接入网络，是应用在点对网结构的接入模式；而 IPSec VPN 是在两个局域网之间通过 Internet 建立的安全连接，保护的是网对网之间的通信。在现代的商业机构模式中，普遍都存在着这两种需求，所以我们在选择 VPN 技术的时候应该根据实际的业务需求出发，选择某一种或者二合一的 VPN 技术。

SSL VPN 给您带来的价值

安全护航，保证业务信息安全

SSLVPN 采用严谨的认证方式，高强度的加密模式，细致的权限分配和访问记录，实现对业务访问过程的全场护航，保证业务畅通无阻的同时规避网络安全风险。

提高办公效率，提升组织响应能力

为了实现随时随地地办公，进一步提高办公效率。但是网络中无处不在的网络延时、网络丢包导致业务访问速度急剧下降，原本需要几秒处理的事情，现在却拖延到了几分钟，严重影响了办公效率。深信服针对网络中存在的问题，通过深信服的 HTP 技术、动态压缩技术、多线路智能选路技术、不断加入的广域网优化技术将进一步解决恶劣环境下访问速度慢的问题，全面提高远程接入访问的办公效率。

降低管理成本，提升组织经营效益

由于 SSL VPN 无需安装客户端，对于使用端透明，无需安排专门的人员进行维护，针对于传统的 IPSEC 需要安装客户端，一旦出现意外需要远程进行维护，不管是派专人维护还是远程维护必将增加维护成本，对于一两个点接入的情况这样的维护成本还可以接受，但是面对成千上百个点来说，那将是一笔巨大的维护成本，而且极容易造成业务效率的下降。SSL VPN 无需安装客户端，仅仅依托于浏览器，不依赖网络环境（只要能上网均可访问），这三大特点将进一步降低组织的维护运维成本，从而进一步降低整体管理成本。

保障组织信息安全，防止核心信息外泄

随着组织规模的扩大，业务系统也在不断增多，也有越来越多外部人员需要访问内部的应用系统，但是通过广域网访问存在的安全隐患让组织非常害怕这些关键业务数据的泄密，因此需要建立一种安全可靠的远程接入访问机制，针对众多的应用系统提供细致的权限划分、高效的数据加密机制、丰富多样的身份认证手段、全面的单点接入安全检查、完整的日志审计，全面防止内部核心应用系统的数据泄密，保护组织信息安全

第 2 章 SANGFOR SSL VPN 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 SSL VPN 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 IPSec VPN 二合一的解决方案，加速 VPN 解决方案等。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 年更是推出了业内的更快速的 SSL——流缓存加速技术。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 2010 年初为止，已经服务于超过一万八千家的用户，值得一提的是：世界五百强中的中国企业 70%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。截止 2015 年，深信服 SSL VPN 在大中华区市场占有率为 47.8%

第 3 章 SANGFOR SSL VPN 网关技术

作为中国市场占有率第一的 SSLVPN 解决方案供应商，深信服科技推出的 IPSec/SSL 一体化网关有以下多种功能和技术特色：

3.1 更安全的 SSL VPN 为业务互联保驾护航

3.1.1 丰富的认证方式

在 SANGFOR SSL VPN 安全网关支持 LocalDB、LDAP/AD、Radius、第三方 CA、自建 CA、Dkey、短信认证（短信猫和短信网关）、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。

3.1.2 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。

3.1.3 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

SANGFOR SSL VPN 安全网关采用 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

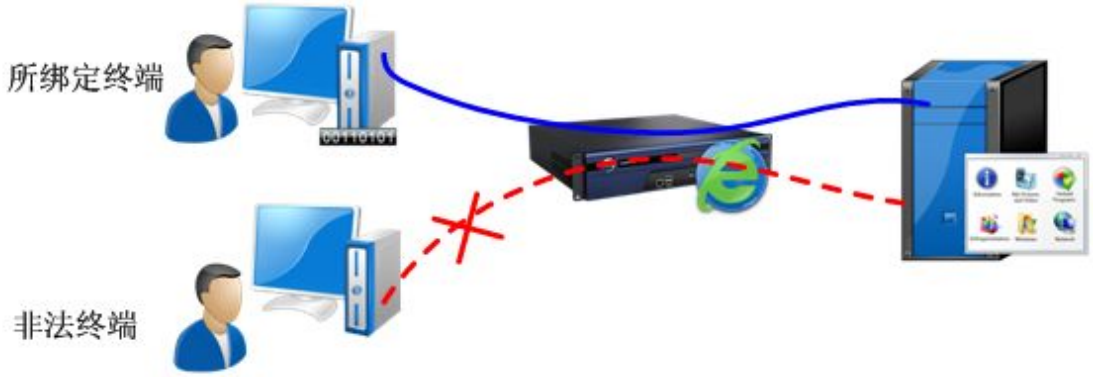
除了通过短信猫方式进行短信发送外，深信服还支持运营商的短信网关，如果您的网络中已经部署了短信网关（移动、联通或电信的短信网关），深信服可以和您的短信网关结合，实现短信认证。

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。

3.1.4 内置的 CA 中心提供完整认证体系

SANGFOR SSL VPN 安全网关内置了 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，SANGFOR SSL VPN 安全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。

3.1.5 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。

3.1.6 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。

3.1.7 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。

3.1.8 开放数据接口提供二次开发

通过 SSL VPN 已经建立了一整套完善的认证体系，对于这样的完整体系需要引入到第三方的系统之上继续做认证，针对于这样的情况深信服通过开放 SSL VPN 中的部分数据库信息，第三方可以调取其中的数据信息，通过这些信息可以根据实际的需要进行二次开发，从而跟更多的应用系统结合。

3.1.9 与其他第三方认证系统结合，保护前期投资

从整个业界范围来看，认证系统多种多样，采用的数据格式也不禁相同，为了保护前提的投资，需要跟原有的认证系统进行结合，但是作为 SSL VPN 来说不能完美对于所有的认证系统都能进行充分的结合，深信服提出了通过深信服自己的 Radius 服务器作为中转，从而实现与其他认证系统的完美结合，而且 SANGFOR Radius 强大的扩展性可以满足您与第三方进行对接的要求。

3.1.10 图形码验证功能

SANGFOR SSL VPN 安全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。

3.1.11 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，SANGFOR SSL VPN 安全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。

3.1.12 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，SANGFOR SSL VPN 安全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 网关将自动弹出对话框，提示用户“SSL 连接会在 X 秒内超时关闭，继续还是注销？”若用户在该时间内仍未选择相应动作，则 SANGFOR SSL VPN 安全网关将自动注销，中断会话并重新返回

登录界面。

3.1.13 全面的密码安全保障

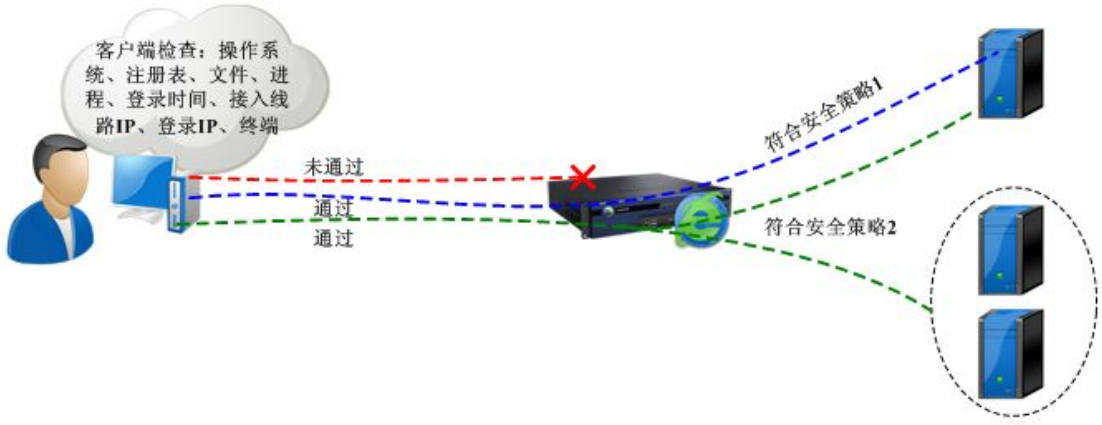
对于采用在 SSL VPN 上建立的用户名和密码，深信服采用了多种机制保证密码的安全性。

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。

3.1.14 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，SANGFOR SSL VPN 安全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。

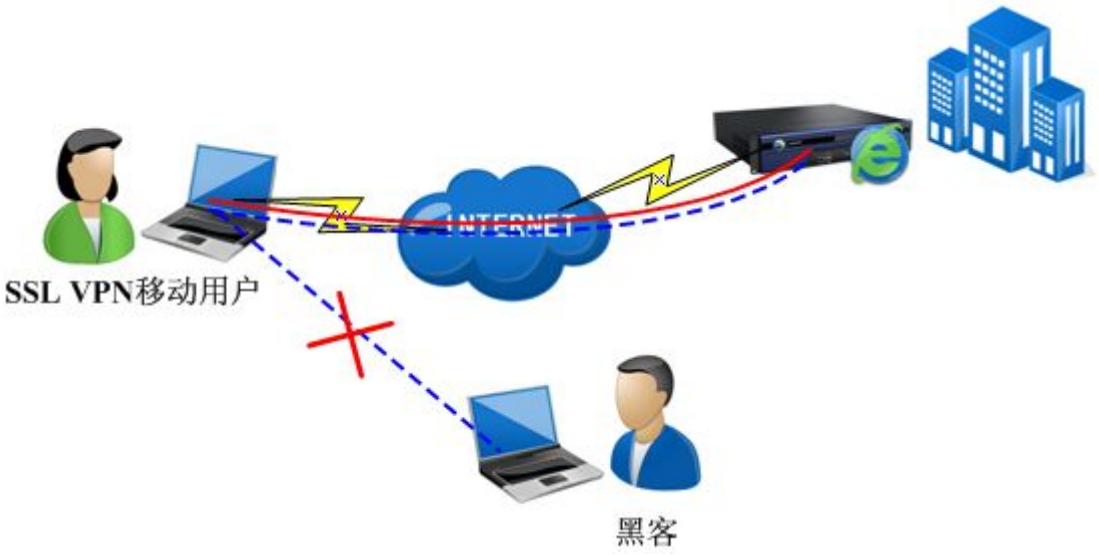


SSL VPN 客户端安全检查保证接入安全

3.1.15 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。



3.1.16 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。

3.1.17 真正的 SSL 协议加密传输

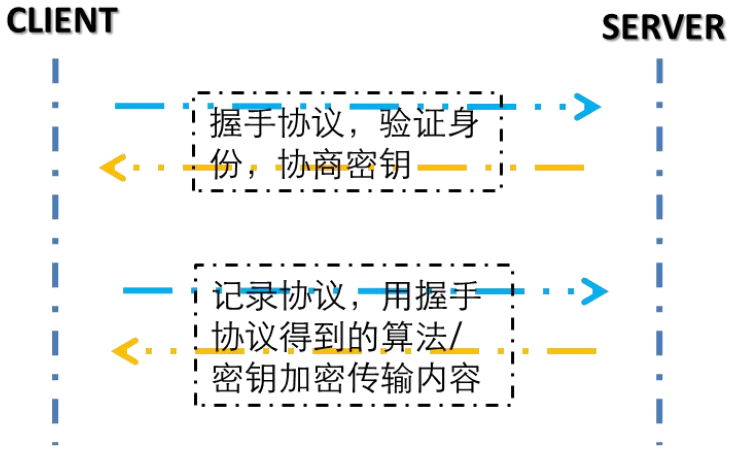
SSL VPN 依托于内嵌在各种浏览器当中 SSL 协议（RFC2246）。它是一种安全可靠的协议，包括以下三个协议：

握手协议：客户和服务器之间相互鉴别 -协商加密算法和密钥 -它提供连接安全性，有三个特点 身份鉴别，至少对一方实现鉴别，也可以是双向鉴别 协商得到的共享密钥是安全的，中间人不能够知道 协商过程是可靠的

记录协议：SSL 记录协议建立在可靠的传输协议（如 TCP）之上 它提供连接安全性，有两个特点 保密性，使用了对称加密算法 完整性，使用 HMAC 算法 用来封装高层的协议

警告协议：这个协议用于每时示在什么时候发生了错误或两个主机之间的会话在什么时候终止

SSL 协议数据交互的过程如下：



正是因为 SSL 协议本身的安全性也导致他被广泛的应用到网上银行。而真正的 SSL VPN 必须将 IP 层以上的数据都通过 SSL 协议进行封装。

如果仅仅将 TCP 数据做了简单的封装，或者把 IPSEC VPN 做些修改，将数据转发到 443 端口，不能算是真正的 SSL VPN。鉴别这种伪 SSL VPN，可以使用标准的 HTTP 流量测试工具如 Loadrunner，Web bench，Avalanche 等或者通过抓包工具 Wireshark、Sniffer。如果能进行 SSL 对接，并进行 SSL 负载测试的就是真正的 SSL VPN。但是普通客户往往没有这个测试条件，因此建议在 SSL VPN 选型时购买经过国家密码管理局批准的产品型号，以及经过公安部检测通过并获得 VPN 销售许可证的产品。

3.1.18 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。

3.1.19 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。

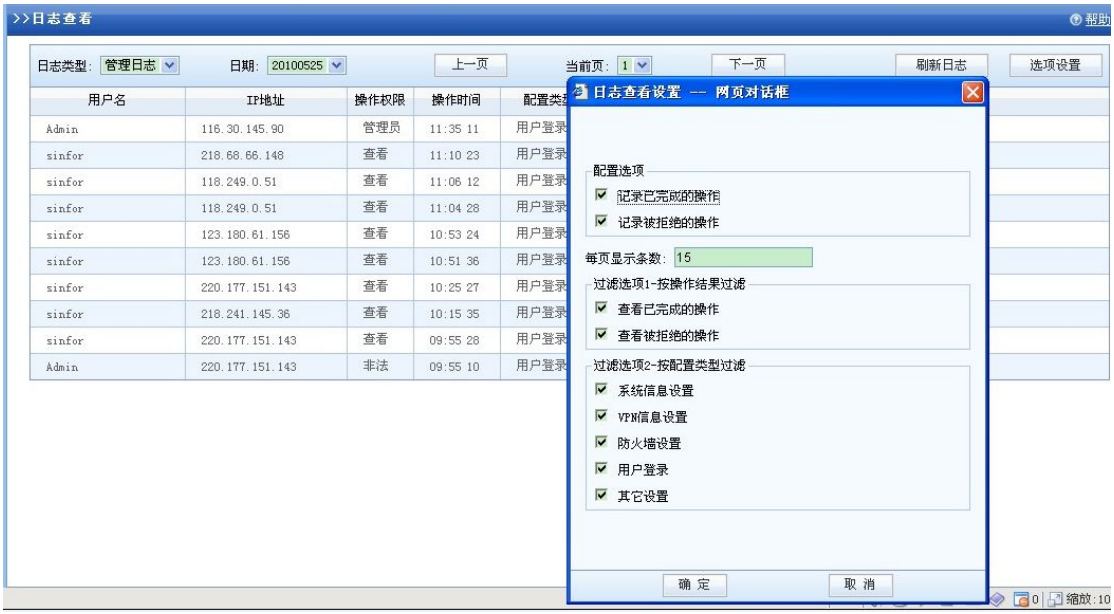
SANGFOR SSL VPN 内置有多种用户和资源管理方式，可以自建用户，也可以从第三方导入，支持 LDAP/AD、RADIUS 等第三方认证，可以根据用户、用户组、公用账号、私有账号等多种方式对用户进行管理。管理员可根据角色、Web 资源、C/S 资源、IP 资源等权限划分方式，为远程接入用户分配细致的访问权限控制。

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。

3.1.20 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。SANGFOR SSL VPN 安全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。

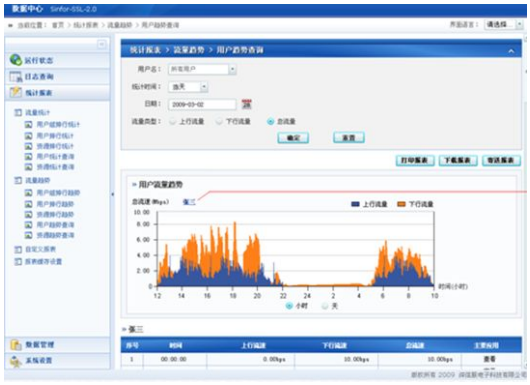


3.1.21 丰富的日志信息

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。SANGFOR SSL VPN 安全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。



3.1.22 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。

3.1.23 沙盒技术-安全桌面

很多商业系统都缺少信息防泄密手段，使用者可以任意在本地留存副本和相关信息，也可以把相关数据传到别的计算机或者网络上，造成信息系统的泄密。除了主动泄密，中了木马和病毒，或者被黑客攻击的被动泄密行为也可能为企业带来巨大的损失，尤其是一些对数

据安全性要求较高的机构及场合，如银行、基金、证券等金融单位，涉及重要研发机密的第三方接入等情况，尤其需要完善的信息保护方案，同时该方案不应该以牺牲工作效率为代价，最好不需要更改原来用户的办公习惯，从而在不影响业务的情况下，实现信息的防泄密保护工作。

深信服科技的 SSLVPN 使用沙盒技术，提供安全桌面功能，可以有效保护数据的安全性，解决用户的敏感数据被泄露的问题。安全桌面可以由管理员设定针对资源和用户进行强行启用，启用安全桌面以后，客户端将自动使用虚拟技术生成一个封闭式虚拟的工作环境——安全桌面。安全桌面将与默认桌面显示完全一致。在安全桌面中，所有操作全部虚拟化，安全桌面内的进程和安全桌面外的进程是隔离的，与其他在本地网络或者互联网网络中的终端都是隔离的，这样就能形成一个完全信息隔离的工作环境，达到防止信息泄密的效果。信息无法流传出安全桌面，而在安全桌面退出之后，安全桌面中的所有操作、临时使用或者接收到的数据都被删除，不会留下任何痕迹。

安全桌面可配合 SSLVPN 本身的用户身份认证、传输加密、授权访问等技术，可以提供给客户更为完整的安全网络解决方案。

3.1.24 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。

SANGFOR SSL VPN 安全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，SANGFOR SSL VPN 安全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。

SANGFOR SSL VPN 安全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 SANGFOR SSL VPN 安全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，SANGFOR SSL VPN 安全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，SANGFOR SSL VPN 安全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。

3.2 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。

3.2.1 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。

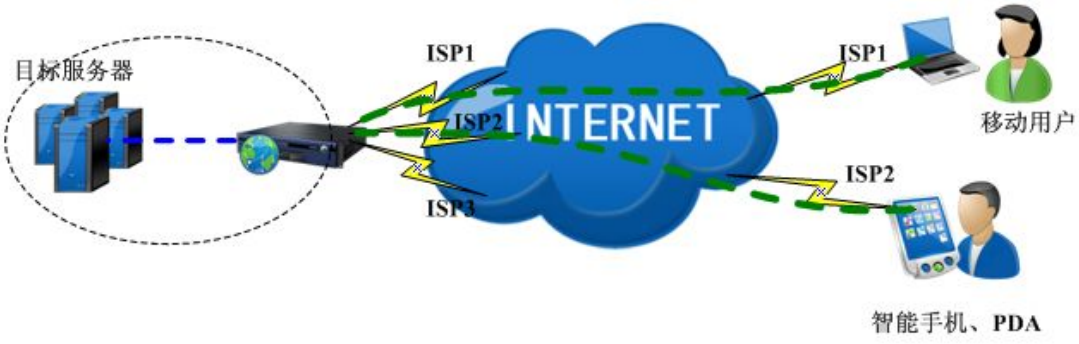
慢启动－避免发送 TCP 对等方拥塞整个网络的现有算法被称为“慢启动”和“拥塞避免”。在连接最初发送数据和还原丢失段时，这些算法可以增大发送窗口，即发送端可以发送的段数量。对于每个接收到的确认段或每个已经确认的段，“慢启动”算法会以一个完整的 TCP 段增大发送窗口。对于每个已经确认的完整窗口的数据，“拥塞避免”算法以一个完整的 TCP 段增大发送窗口。利用这些算法增大发送窗口的速度就足以充分利用连接带宽。

3.2.2 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 SANGFOR SSL VPN 安全网关中，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 SANGFOR SSL VPN 安全网关，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。



3.2.3 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）。SANGFOR SSL VPN 安全网关支

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。

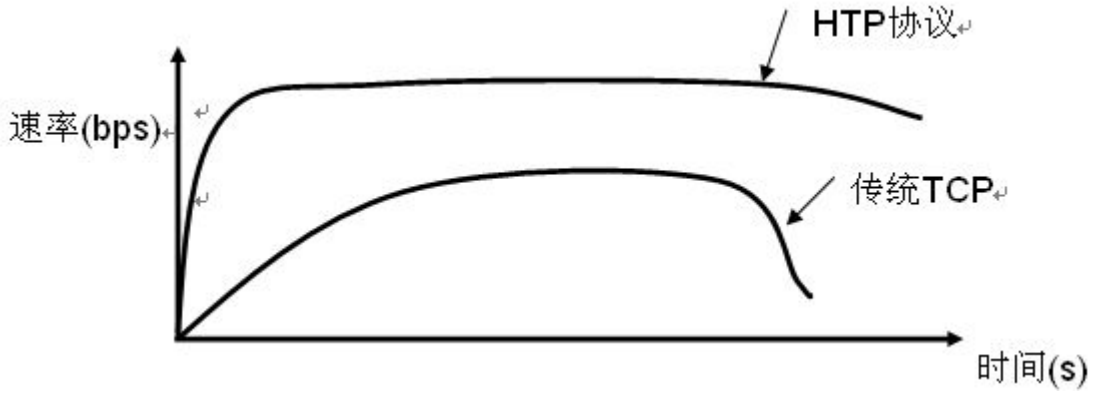
针对不同的上网线路，还可以启用多线路策略，用户可以根据线路情况选择带宽叠加模式、线路主备模式或者动态适应模式等多线路策略。同时，SANGFOR SSL VPN 安全网关内置了 5 个 Qos 级别和多条 Qos 规则，用户可根据自身实际情况设置相应的 QOS 级别。

3.2.4 HTP 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。



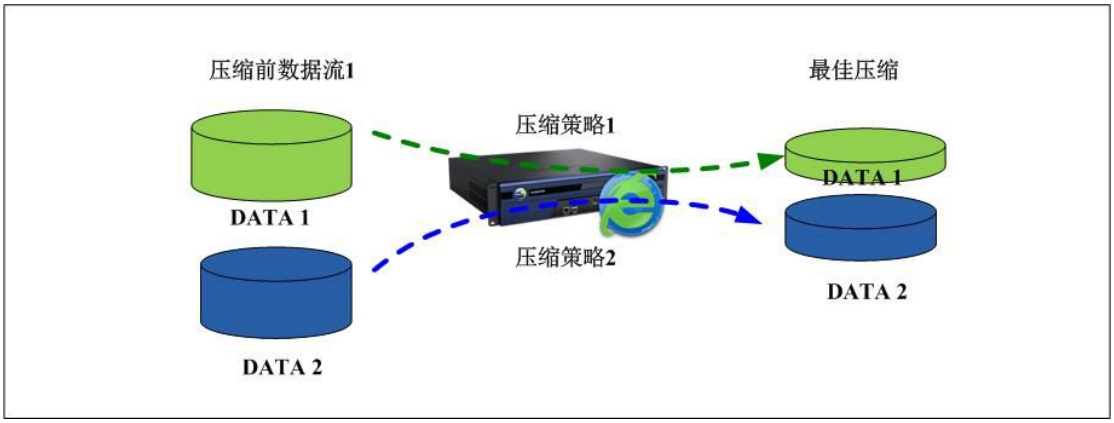
HTP 协议图示

3.2.5 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。



3.2.6 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。

3.2.7 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。

3.2.8 自主研发 SRAP 远程应用传输协议，提升远程应用访问速度

SRAP: 即 Sangfor Remote Access Protocol， 是深信服自主研发的终端虚拟化技术协议框架。是用于代替 RDP 协议，通过数据转发控制，数据压缩、缓存与过滤等方式，提升 EasyConnect 远程应用速度。SRAP 对于原来的 RDP 来说，无论是视频还是普通的 OA 等应用系统，数据压缩率都已经有较大的改进，速度方面也有很大提升。

3.3 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。

3.3.1 支持所有网络应用

SANGFOR SSL VPN 安全网关通过 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，SANGFOR SSL VPN 安全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。

3.3.2 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。

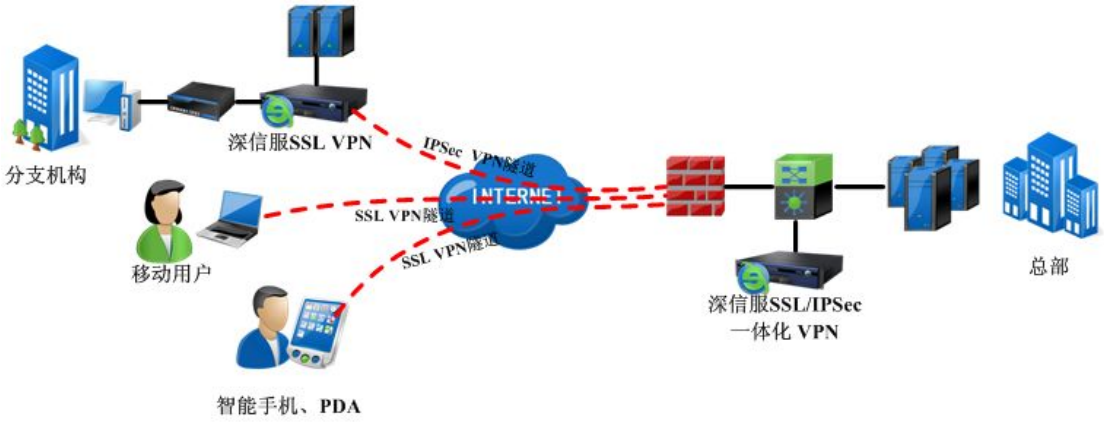
3.3.3 提供 IPSec/SSL 一体化选择

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。

SANGFOR SSL VPN 安全网关结合了 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 。



3.3.4 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。

3.3.5 配置向导简化管理员的操作过程

为了简化您的操作，SANGFOR SSL VPN 安全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。

3.3.6 隐藏服务模式

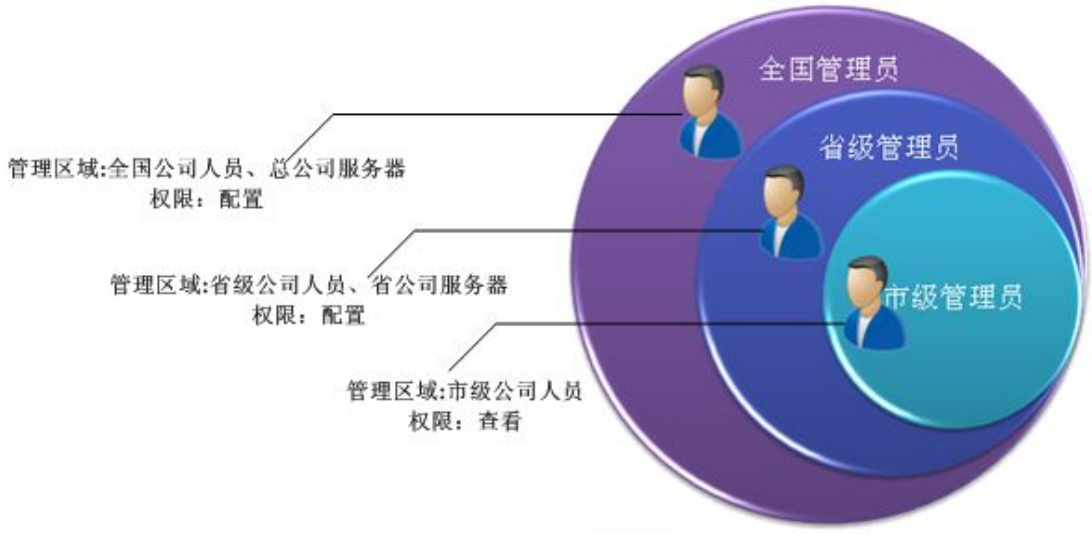
在用户的资源列表中，除了对 C/S 应用的透明支持之外，SANGFOR SSL VPN 还增加了一个隐藏服务。用户在访问总部的 SSL 资源时，SSL VPN 可以将某些特殊的资源隐藏起来，用户在其资源列表中无法看到该项资源，但用户仍然可以使用。这种支持隐藏服务的功能，更加保证了企业内网资源的安全性。

3.3.7 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。

3.3.8 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，SANGFOR SSL VPN 安全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。



3.3.9 定制登录界面功能

SANGFOR SSL VPN 安全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。

3.3.10 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。

3.3.11 移动终端设备的完美支持

对 Android、IOS、windows 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。

3.3.12 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。

3.3.13 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。

3.3.14 User 权限下正常访问

微软操作系统对于管理员也进行了分权限管理，在 Administrator 账号下可以安装任意的插件，从而可以进行任意资源的访问。但是在 User 权限下，由于微软操作系统的权限限制，因此在 User 权限下无法正常的安装各种插件。为了让用户更好的在 User 权限下正常使用，深信服提供了权限提升控件，只要在 Administrator 权限下安装了权限提升服务，那么在 User 权限下就可以正常使用所有的插件。

3.3.15 默认服务页面

对于应用资源的比较少的用户来说，往往可能只有一个资源，但是 SSL VPN 的登录流程是通过认证后必然要跳转到资源列表页面，然后点击应用资源才能登录到应用系统中。对于只要少量资源的用户来说通过认证后需要跳到资源列表页面再点击应用资源才能访问，为了进一步提高效率，可以根据用户经常使用的习惯来设置默认的应用服务页面，避免跳转到资源列表页面，而通过身份认证后直接跳转到应用资源列表，从而减少了登录等待时间，提高了登录效率。

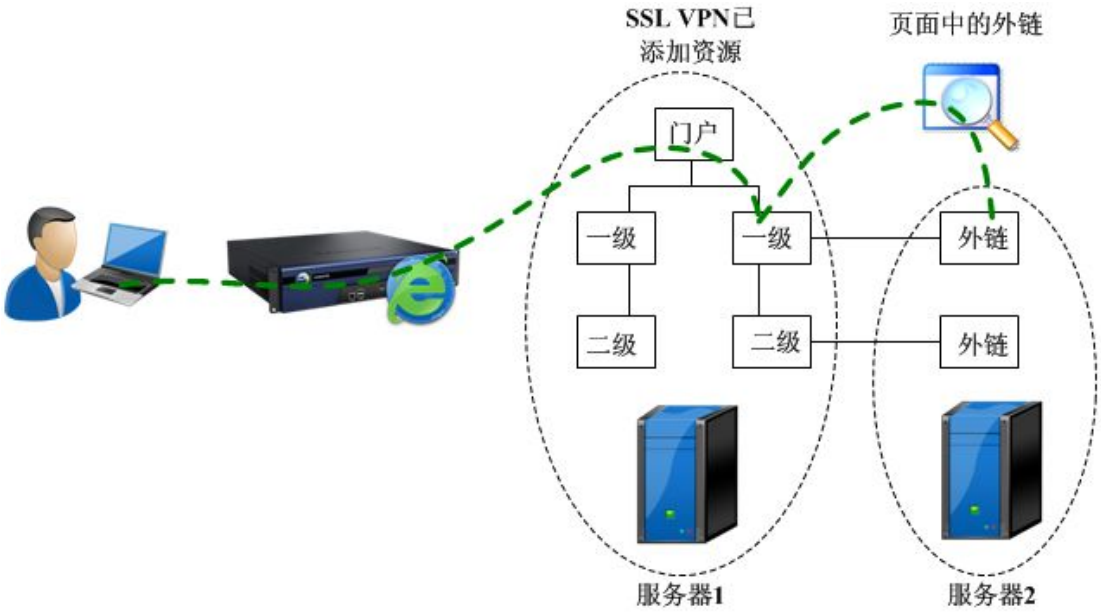
3.3.16 系统托盘

对于一些特殊的环境下，可能需要长时间的登录 SSL VPN，但是往往 SSL VPN 是依托于浏览器的，如果用户在操作的过程中不小心关闭了浏览器，那 SSL VPN 就有可能断开，导致业务中断，为了避免因为误操作而导致浏览器关闭，深信服提供了系统托盘，当您点击关闭的时候可以将浏览器最小化成任务栏的系统托盘，从而避免因为误操作导致 SSL VPN 关闭。

3.3.17 全网资源-智能递推

对于一些高校或者大型的集团公司来说，面对众多的应用系统为了方便内部人员的访问，一般都做成了统一门户的访问方式。在门户页面中除了本身的各种应用系统外，内部还有大量的访问模块如果一一进行添加将非常麻烦。特别是针对一些资源中含有外联的地址，因此为了更好的实现与现有资源的匹配，深信服可以预先解析该页面中可能出现的链接，对于这些链接自动添加到资源中并放通（智能探测技术）。从而防止出现部分资源漏访的情况，保证业务正常访问，提高办公业务效率。

资源智能递推的实现价值：对于管理员来说，不需要针对门户中的多级域名和多级链接逐个添加资源，通过智能探测可以自动放通，大大降低管理员工作量，降低管理成本；而对安全性的考虑，对于管理员来说只需要将门户的域名添加到资源中，无需再去添加多级链接中的其他资源的 IP 和端口，大大降低了因开放多个 IP 和端口所带来的安全隐患，提高安全性。



3.4 更稳定的 SSL VPN

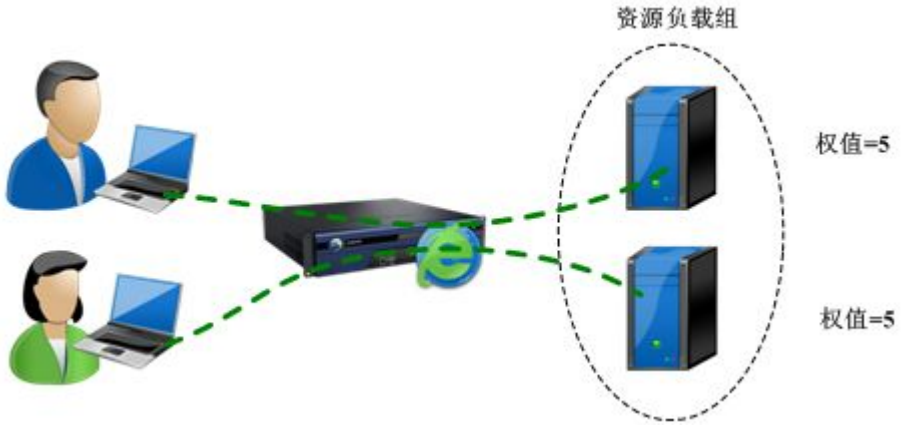
3.4.1 多线路技术实现线路备份，保证 VPN 线路稳定

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，SANGFOR SSL VPN 安全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。

3.4.2 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。



3.4.3 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。

3.4.4 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。

3.5 应用虚拟化

3.5.1 远程应用发布

移动互联网的发展带动了更多移动办公的需求。随着各种智能手机、平板电脑以及 3G 网络的普及，人们的操作习惯和使用偏好正从原来笨拙的台式机、笔记本慢慢迁移到更加便携更加灵活的智能终端。办公人员希望无论在何时何地，只要能连上互联网，就能实现业务的及时处理。

深信服科技推出的远程应用发布方案包含了多种技术及管理策略，全方位保证远程办公

中的数据安全；同智能终端完美结合，自主研发 SRAP 传输协议提供畅快的使用体验，方便客户快速开展业务；涵盖当今主流智能终端操作系统，满足不同人群的个性需求

远程应用发布功能通过以下组件来实现：

远程应用发布模块：内置在 SSLVPN 设备中，拥有获取应用发布服务器上的资源信息，为终端提供访问，并负责身份认证、传输数据处理等工作，是远程应用发布的核心组件。

RemoteApp Agent：深信服服务端控件，安装在应用发布服务器上，用来提供远程应用服务和监控应用发布服务器状态信息的程序。该程序默认为服务器开启自动启动。

RemoteApp Client：客户端控件，在移动终端上命名为 EasyConnect，提供接入终端服务器的功能，苹果终端可在 APPStore 免费下载安装，Android 终端可在 google play 及其他常见的安卓市场中下载使用，PC 终端将自动安装相应客户端控件。

应用程序客户端：需要发布给移动终端用户使用的应用程序，需要提前在应用发布服务器安装，如 Office、写字板等程序，基于 C/S 架构的应用系统需要在在应用发布服务器上安装客户端软件，B/S 架构业务系统，需要在应用发布服务器上安装相应版本的 IE 浏览器。

3.6 企业移动管理

支持扩展企业移动管理（EMM，Enterprise Mobility Management）解决方案。EMM 是指通过移动信息化管理手段，针对企业移动信息化建设过程中涉及到的企业移动设备、应用、信息等内容提供信息化管理及安全保障的解决方案。

深信服企业移动管理解决方案，是一种为企业用户打造的、解决客户移动信息化过程中的安全及管理问题的解决方案。用户通过简单的操作，对智能终端进行注册、同时配置深信服 EMM 管理网关即可实现移动设备管理（MDM）、移动用户管理（MUM）、移动应用管理（MAM）、移动内容管理（MCM）四项子管理方案功能，为用户提供从用户、设备到应用、内容的全面管理。

3.6.1 移动设备管理（MDM）

移动设备管理解决方案支持对移动设备进行管理，包括设备注册、设备擦除、用户关联、策略关联、状态监测等功能，帮助管理员管理轻松管理海量设备，降低运维成本。

3.6.2 便捷的批量移动终端管理

移动设备管理（MDM）方案可轻松使贵单位具备批量设备管理能力。当移动办公用户使用移动办公系统时，系统会按照用户权限策略要求，提示用户进行设备注册。用户注册后，贵单位管理员即可对该设备进行基础信息查看及相应的策略管控。可查看的信息包括用户设备名称、关联用户、注册时间、设备型号、操作系统、手机串号、是否 Root/越狱、设备状态是否正常等，一旦设备出现违规情况，系统界面会对管理员发出消息通知，管理员可根据以上信息对违规设备进行消息推送、设备锁定、数据擦除、弱口令拒绝等操作，强制用户终端达到公司规定的安全级别，以此保证数据不外泄。

3.6.3 严格的设备密码策略

移动设备管理（MDM）方案可以强制用户必须将密码设置为带有字母和数字的复杂密码；可强制手机超时自动锁屏；可设置修改密码规则（新密码与旧密码不能一样）；可设置密码有效周期，例如 1 个月要重新设置一次密码；可防止暴力破解，在多次输入错误密码时删除所有数据。

3.6.4 远程锁定移动设备

通过 MDM 方案的设备锁定功能，管理员可以远程锁定手机，让违规手机无法使用。Android 设备被锁定之后，设备将无法正常使用，目前只能从控制台进行解锁；iOS 设备被锁定之后，设备上输入解锁密码即可继续使用。

3.6.5 远程擦除办公终端数据

手机丢失、人员离职等情况下，把手机还原到出厂状态，擦除终端上的所有数据，避免企业信息泄露。

3.6.6 企业消息推送

MDM 方案集成消息推送功能，管理员可以定向给用户推送通知信息。有时候需要群发放假、会议等通知。为了企业数据安全，有些用户规定移动办公专用设备不允许安装 QQ、微信等应用，企业也没有内部专用的即时通讯系统，发邮件不一定经常接收，发短信成本较高。这种情况下，利用移动设备管理的消息推送功能可以将信息直接推送给所有移动办公用户，以上问题就解决了。

3.6.7 移动用户管理（MUM）

移动用户管理解决方案支持对移动用户的全面管理，包括 16 级用户认证鉴权、用户权限与移动设备关联等功能，轻松实现多部门用户管理以及细粒度权限管控，减轻管理员运维压力。

3.6.8 多种身份认证

通过 MAM 中 APP 安全加固解决方案，可以为移动阴公新增用户认证方法，包括用户名/密码、硬件特征（注：手动集成 SDK 方式支持）、短信、动态令牌、CA 证书、Ldap/Radius 单点登录等认证方式，可以对贵单位移动办公用户的用户身份进行高强度识别，避免用户名/密码被非法人员窃取后，冒用被盗用户身份信息登录办公系统，导致信息泄密的情况出现。同时支持与现有身份认证系统联动，避免一套系统登录需要重复认证的情况出现，增加易用性。

3.6.9 严格的权限管理

APP 安全加固后，新增资源权限划分功能，可以拒绝贵单位移动办公用户访问未经授权的业务系统，避免黑客通过对移动应用进行动态调试等方式，对贵单位内部其他系统肆意

发起跳板攻击。用户在进行身份鉴权后，贵单位管理员可为不同部门划分不同的系统访问权限，用户仅能访问权限允许范围内的系统。这样，业务系统进行移动化迁移的安全性就又多了一层保障。

3.6.10 移动应用管理（MAM）

支持手动/自动方式的 APP 安全加固、企业应用商店、移动应用单点登录等功能，简化应用加固、分发和用户登陆使用过程，为用户提供更加易用的企业应用使用环境。

3.6.11 影子 IT 避免，保护企业数据安全

BYOD 的移动办公开展方式能为贵单位节省终端批量采购的预算，但是这种情况会造成“影子 IT”（需求部分提到）的情况出现。MAM 方案的移动应用管理功能可以对受控终端的应用进行管理，控制用户在进行移动办公时，无法使用公有云应用，这样企业数据就不会被分发至个人云盘等第三方应用处，杜绝“影子 IT”的情况出现。

3.6.12 全面的移动应用管理

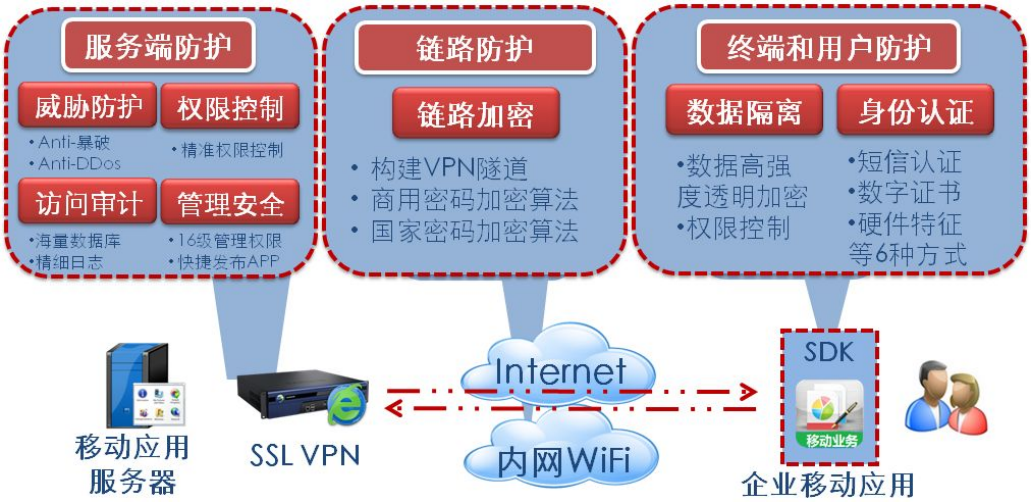
移动应用管理（MAM）方案可为贵单位提供企业应用发布、企业应用分发管控、用户应用使用控制等功能，保证应用层面的数据安全。

对于贵单位正在进行开发的新建移动办公业务系统，深信服企业移动管理解决方案能够从数据访问权限、数据存储、数据传输等环节为企业数据进行安全保障。

3.6.13 方便快速的应用安全封装

深信服 MAM 方案可为 APP 开发商提供用于与企业移动管理平台对接的安全加固 SDK，该安全加固 SDK 集成代码量约为 20 行左右，进行安全加固也仅需 1 名研发约 2 天时间即可完成；对于贵单位已经开发完成的业务系统，深信服提供安全加固 SDK 自动封装增值方案，无需开发商开发人员配合，通过上传、封装、下载 3 个动作，5 分钟内完成安全加固 SDK 封装。完成 SDK 封装后，贵单位即可为原有移动办公应用新增移动用户管理、SSL VPN 安全接入等功能，并可完整使用企业移动管理平台的其他功能。

深信服 SDK 包透明集成到用户的应用 APPS 中，用户无感知，提升用户使用体验。此外，深信服 EasyAPP 方案支持 VPN 隧道分流技术，用户可以在使用互联网体验的同时，使用企业移动应用。



3.6.14 多应用统一登录

考虑到贵单位后续会持续开展移动办公系统建设，深信服 MAM 方案预留可扩展的移动应用单点登录模块，在移动办公系统逐渐增多、各个系统间用户名/密码不同的情况下，为用户提供企业应用一键单点登录的功能，免除用户反复多次输入繁琐的用户名密码的麻烦，提高用户对贵单位 IT 部门的满意度。

3.6.15 C/S、B/S 架构企业应用商店，保证企业应用分发权威

企业应用一旦没有权威分发出口或者应用下载方式不够便捷，贵单位的用户在更换手机等情况下，大多会选择在互联网进行搜索、下载、安装移动办公应用。由于第三方分发平台的应用被篡改的可能性较大，用户自行搜索安装的企业应用很可能被植入过广告、病毒 SDK，肆虐用户的移动终端，对贵单位业务安全造成影响。MAM 方案可为贵单位提供自建企业应用商店的能力，为贵单位的移动办公应用提供权威分发出口。该功能可以在客户端使用，也可以用浏览器直接访问自建 WEB 应用商店，支持控制应用分发进行策略授权，例如仅限制在手机或者平板安装、限制该应用的使用用户等，既可满足应用分发需求，又能控制企业应用不被非单位用户下载使用，一举两得。

3.6.16 图形解锁，轻松的二次认证

新增应用图形锁功能，原本的企业应用从后台切换至前台时，都被要求重新认证，以保证数据的安全性。具备该功能后，重新认证方式被替换为输入图形解锁码，这样及防止企业应用未退出、其他人使用该用户手机偷窥机密信息的情况出现，又能简化用户重复认证登录过程，极大的平衡了企业应用的安全性和易用性。同时，该功能可以与 MDM 进行策略联动，

锁定多次解锁失败的设备，防止图形码被暴力破解。

3.6.17 应用黑白名单，用技术手段保证“专设专用”

支持应用黑白名单公呢个，使管理员可控制用户能否使用某些应用。例如被管理的手机在工作时间只能使用移动办公系统，不能进行 QQ 聊天、淘宝购物、刷微博等娱乐活动，提升员工办公效率。

3.6.18 移动内容管理（MCM）

支持对下载至移动终端的企业数据进行管理，包括落地数据加密、控制企业数据分享、远程数据擦除等，为企业提供安全的业务环境，避免企业数据泄露。

3.6.19 安全的企业移动内容管理

移动内容管理（MCM）能够为贵单位提供在 BYOD 办公环境下重新定义企业/个人应用边界的能力。MCM 方案支持对下载至移动终端的企业数据进行管理，包括企业/个人数据隔离、数据存储加密、控制文档分发、控制邮件分发以及限制终端自带截图工具和剪切板工具等功能，为用户提供企业文档安全阅读环境，避免企业数据被动泄密。

3.6.20 一机两用，BYOD 的公私隔离

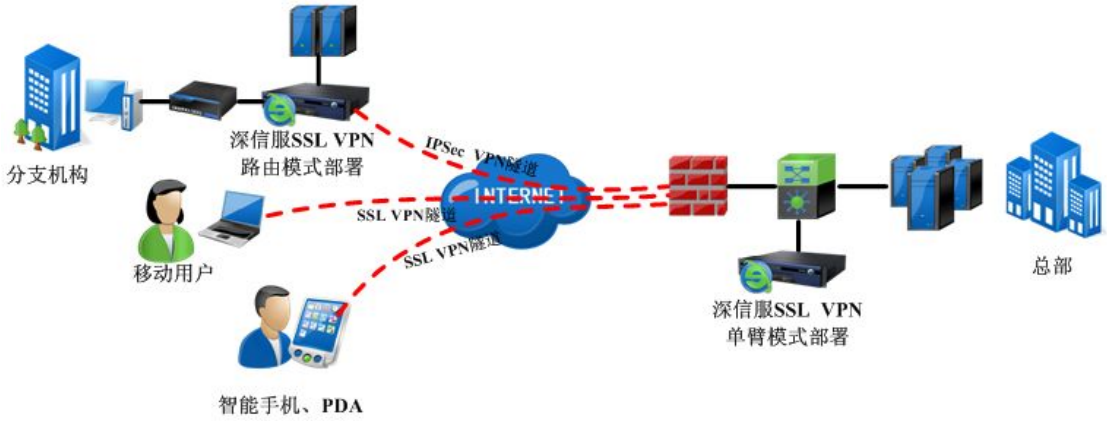
该方案将所有企业数据在进行传输时均通过 SSL VPN 加密隧道进行传输，并且下载的企业数据被单独保存在终端上的加密隔离区，以文件碎片形式保存。同时，下载的应用仅限于指定的企业应用可以打开，杜绝 QQ、微信等应用对其访问，避免数据被分享泄露。该方案还会对系统剪切板进行管理，防止拷贝、截屏泄密。

第 4 章 SSL VPN 部署模式及用户使用

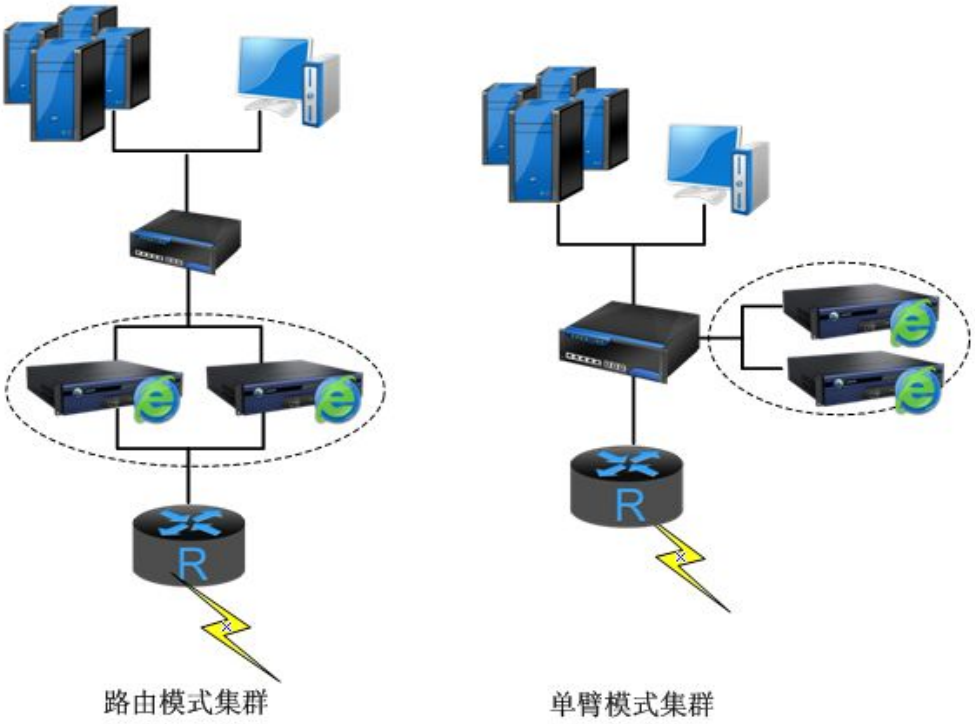
4.1 SANGFOR SSL VPN 部署模式

深信服 SSL VPN 支持路由部署及单臂部署两种模式。

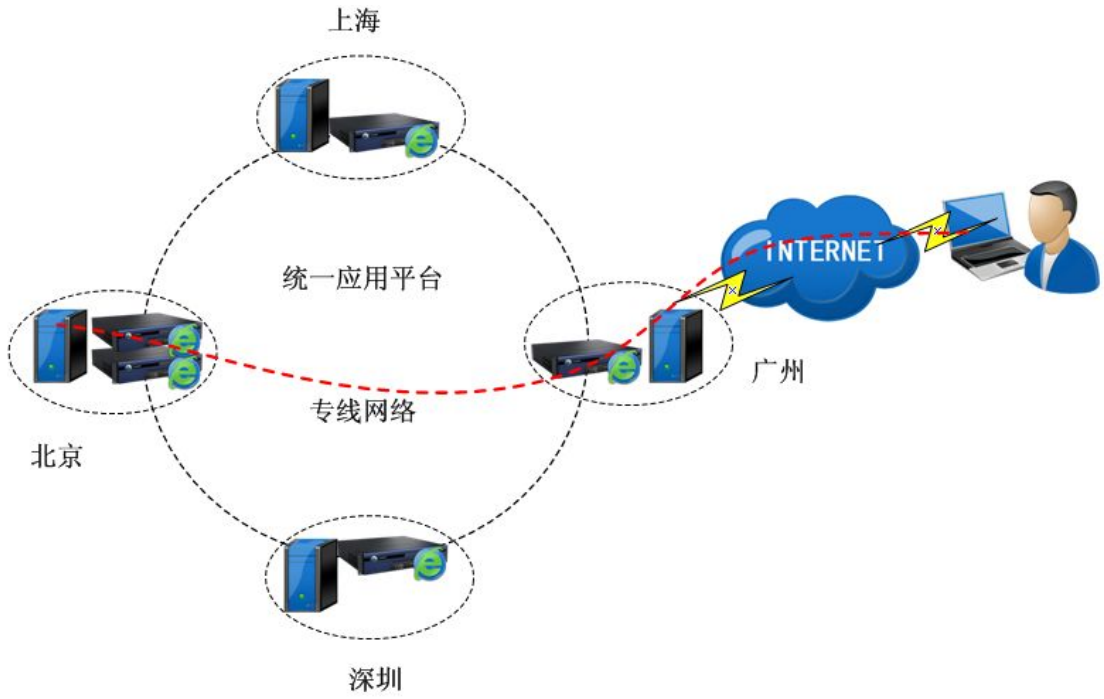
除了最基本的路由模式外，深信服 SSL VPN 支持单臂模式部署，不需要对用户现网结构做任何改变，不影响用户业务的正常使用。



支持路由模式、单臂模式部署



集群模式部署

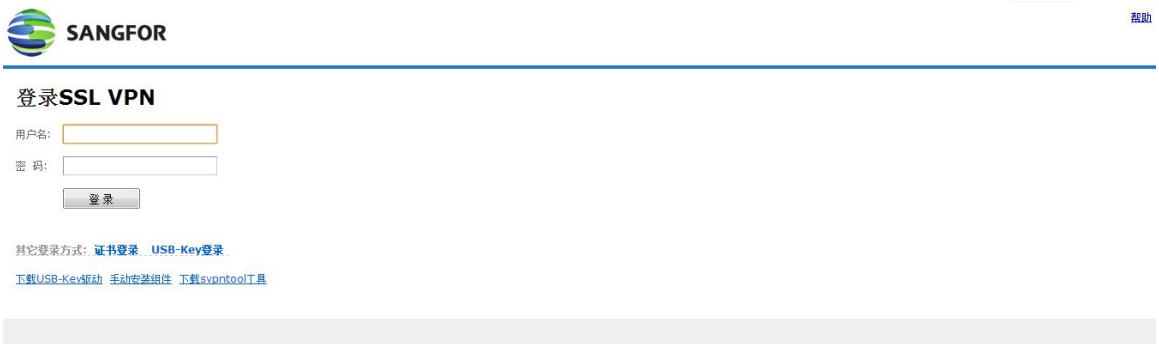


全网分布式集群部署

4.2 客户端登录和使用界面

4.2.1 缺省登录界面

说明：该页面使用 Portal 定制功能后，可以根据用户的要求进行定制。



定制页面：


SANGFOR
深信服科技
帮助
EasyConnect
登录SSL VPN
用户名
密 码
登 录
使用其它登录方式
证书登录
USB-Key登录
下载USB-Key驱动
手动安装组件
下载svpntool工具

4.2.2 可用资源界面


SANGFOR
深信服科技
cpxx [设置 加速效果 注销]
资源组列表
默认资源组
默认资源组
excel(REMOTEAPP)
word(REMOTEAPP)
powerpoint(REMOTEAPP)
财务系统(HTTP)
财务系统-权限限制(HTTP)
200.200.2.8(FileShare)
200.200.2.8(web)(FileShare)
200.200.2.8(web、URL授权控制)(FileShare)

第 5 章 深信服公司简介

关于深信服

深信服公司成立于 2000 年，是中国最大的应用层网络设备供应商，致力于提供基于网络应用层的产品及解决方案。目前，全球有超过 21,000 家用户正在使用深信服的产品。在中国入选世界 500 强的企业中，有 85%以上的企业都是深信服的用户。截止 2013 年 3 月，深信服在全球共设有 49 个直属分支机构，分布在全球 8 个国家和地区，并拥有超过 1400 名员工。

作为中国应用层网络市场的领导者，深信服每年保持着 50%以上的增长率，持续每年将总营收的 15%投入到研发，并在深圳和北京设有研发中心。截至 2013 年 3 月，深信服共申请超过 100 项发明专利。同时，深信服还是 IPSec VPN 和 SSL VPN 两项国家标准的主要承建单位。

深信服公司被评定为“国家规划布局内重点软件企业”，连续八年入选德勤“亚太地区高科技高成长 500 强”，连续两届荣获《财富》“卓越雇主——中国最适宜工作的公司”。

第 6 章 附录——VPN 技术背景知识

由于 SANGFOR VPN 的技术涉及到了 VPN，防火墙等多个领域，因此在这里对 VPN 和防火墙的背景知识做简单介绍。

6.1 VPN 简介

VPN 是虚拟专用网的简称，虚拟专用网不是真的专用网络，但却能够实现专用网络的功能。虚拟专用网指的是依靠 ISP（Internet Service Provider 因特网服务提供商）和其它 NSP（Network Service Provider 网络服务提供商），在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的固定物理链路，而是利用某种公众网的物理链路资源动态组成的。

IETF 组织对基于 IP 的 VPN 解释为：通过专门的隧道加密技术在公共数据网络上仿真一条点到点的专线技术。所谓虚拟，是指用户不再需要拥有实际的长途数据线路，而是使用 Internet 公众数据网络的长途数据线路。所谓专用网络，是指用户可以为自己制定一个最符

合自己需求的网络。早期的虚拟专用网一般指的是电信运营商提供的 Frame Relay 或 ATM 等虚拟固定线路（PVC）服务的网络，或通过运营商的 DDN 专线网络构建用户自己虚拟专用网。

现在的 VPN 是在 Internet 上临时建立的安全专用虚拟网络，用户节省了租用专线的费用，同时除了购买 VPN 设备或 VPN 软件产品外，企业所付出的仅仅是向企业所在地的 ISP 支付一定的上网费用，对于不同地区的客户联系也节省了长途电话费。这就是 VPN 价格低廉的原因。

按照 VPN 的网络连接类型主要分为 Site to Site 和 End to Site 两种类型。Site to Site 主要指的是网络和网络之间的 VPN 连接。而 End to Site 指的是移动终端到企业私有网络之间的 VPN 连接，而 SSL VPN 就是 End to Site 类型的 VPN。

以 OSI 模型参照标准，不同的 VPN 技术可以在不同的 OSI 协议层实现。

如下表：

VPN 在 OSI 中的层次	**VPN 实现技术**
数据链路层	PPTP 及 L2TP
网络层	IPSEC
应用层	SSL

链路层 VPN 技术

PPTP 协议：

PPTP（点到点隧道协议）是由 PPTP 论坛开发的点到点的安全隧道协议，为使用电话上网的用户提供安全 VPN 业务，1996 年成为 IETF 草案。PPTP 是 PPP 协议的一种扩展，提供了在 IP 网上建立多协议的安全 VPN 的通信方式，远端用户能够通过任何支持 PPTP 的 ISP 访问企业的专用网络。

PPTP 提供 PPTP 客户机和 PPTP 服务器之间的保密通信。PPTP 客户机是指运行该协议的 PC 机，PPTP 服务器是指运行该协议的服务器。通过 PPTP，客户可以采用拨号方式接入公共的 IP 网。拨号客户首先按常规方式拨号到 ISP 的接入服务器，建立 PPP 连接；在此基础上，客户进行二次拨号建立到 PPTP 服务器的连接，该连接称为 PPTP 隧道。PPTP 隧道实质上是基于 IP 协议的另一个 PPP 连接，其中 IP 包可以封装多种协议数据，包括 TCP/IP、IPX 和 NetBEUI。对于直接连接到 IP 网的客户则不需要第一次的 PPP 拨号连接，可以直接与 PPTP 服务器建立虚拟通路。

PPTP 的最大优势是 Microsoft 公司的支持，另外一个优势是它支持流量控制，可保证客

户机与服务器之间不拥塞，改善通信性能，最大限度地减少包丢失和重发现象。PPTP 把建立隧道的主动权交给了客户，但客户需要在其 PC 机上配置 PPTP，这样做既会增加用户的工作量，又会造成网络的安全隐患。另外，PPTP 仅工作于 IP，不具有隧道终点的验证功能，需要依赖用户的验证。

网络层 VPN 技术

IPSec 协议：

IPSec 也是 IETF 支持的标准之一，它和 PPTP、L2TP 不同之处在于它是第三层即 IP 层的加密。IPSec 不是某种特殊的加密算法或认证算法，也没有在它的数据结构中指定某种特殊的加密算法或认证算法，它只是一个开放的结构，定义在 IP 数据包格式中，不同的加密算法都可以利用 IPSec 定义的体系结构在网络数据传输过程中实施。

IPSec 协议可以设置成在两种模式下运行：一种是隧道（tunnel）模式，一种是传输（transport）模式。在隧道模式下，IPSec 把传输层的数据封装在安全的 IP 包中。传输模式是为了保护端到端的安全性，即在这种模式下不会隐藏路由信息。隧道模式是更安全的，但会带来较大的系统开销。由于 IPSec 是基于网络层的，不能穿越通常的 NAT、防火墙。

SANGFORSL 协议：

SANGFORSL 是 SANGFOR SSL VPN 中 IPSec VPN 采用的安全链路协议。

SANGFORSL 是基于 IPSec 协议的安全隧道，但改进了如下过程：提供压缩的 IP 头算法，由此提高网络利用率。普通的 IPSec 网络利用率在 70%左右，而 SANGFORSL 达到 90%改进的 IP 封装技术，使得 SANGFORSL 可通过任何路由器，提高对网络的适应能力。

SANGFORSL 提供基于挑战—响应模式的身份认证。同时也提供基于硬件证书（HARDCA）的鉴权体系。数据传输采用隧道模式，支持各种加密算法，对会话的管理更具有灵活性，同时能适应各种网络层。

会话层 VPN 技术

SOCKS 协议：

SOCKS 处于 OSI 模型的会话层，在 SOCKS 协议中，客户程序通常是先连接到防火墙 1080 端口，然后由防火墙建立到目的主机的单独会话，这种情况下客户程序对目的主机是不可见的。SOCKS 的问题在于必须对客户端应用程序做修改，加入对 SOCKS 协议的支持。

6.2 SSL 协议介绍

SSL 协议：

安全套接层（Secure Socket Layer，SSL）属于高层安全机制，广泛应用于 Web 浏览程序和 Web 服务器程序。在 SSL 中，身份认证是基于证书的。服务器方向客户方的认证是必须的，而 SSL 版本 3 中客户方向服务方的认证只是可选项，现在逐渐得到广泛的应用。

SSL 协议过程通过 3 个元素来完成：

（1）握手协议：这个协议负责配置用于客户机和服务器之间会话的加密参数。当一个 SSL 客户机和服务器第一次开始通信时，它们在一个协议版本上达成一致，选择加密算法和认证方式，并使用公钥来生成共享密钥。

（2）记录协议：这个协议用于交换应用数据。应用程序消息被分割成可管理的数据块，还可以压缩，并产生一个 MAC（消息认证代码），然后结果被加密并传输。接收方接收数据并对它解密，校验 MAC，解压并重新组合，把结果提供给应用程序协议。

（3）警告协议：这个协议用于表示在什么时候发生了错误或两个主机之间的会话在 SH 什么时候终止。

SSL 协议通信的握手步骤如下：

第 1 步，SSL 客户端连接至 SSL 服务器，并要求服务器验证它自身的身份；

第 2 步，服务器通过发送它的数字证书证明其身份。这个交换还可以包括整个证书链，直到某个根证书颁发机构（CA）通过检查有效日期并确认证书包含可信任 CA 的数字签名来验证证书的有效性。

第 3 步，服务器发出一个请求，对客户端的证书进行验证，但是由于缺乏公钥体系结构，当今的大多数服务器不进行客户端认证。但是完善的 SSL VPN 安全体系是需要对客户端的身份进行证书级验证的。

第 4 步，协商用于加密的消息加密算法和用于完整性检查的哈希函数，通常由客户端提供它支持的所有算法列表，然后由服务器选择最强大的加密算法。

第 5 步，客户机和服务器通过以下步骤生成会话密钥：

客户机生成一个随机数，并使用服务器的公钥（从服务器证书中获取）对它加密，以送到服务器上。 服务器用更加随机的数据（客户机的密钥可用时则使用客户机密钥，否则以明文方式发送数据）响应。使用哈希函数从随机数据中生成密钥。使用会话密钥和对称算法（通常是 RC4，DES，3DES）对以后通讯的数据进行加密。

在 SSL 通信中，服务器方使用 443 端口，而客户方的端口是任选的。

6.3 SSL VPN 技术

SSL VPN 技术帮助用户通过标准的 Web 浏览器就可以访问重要的企业应用。这使得企业员工出差时不必再携带自己的笔记本电脑，仅仅通过一台接入了 Internet 的计算机就能访问企业资源，这为企业提高了效率也带来了方便。SSL VPN 网关位于企业网的边缘，介于企业服务器与远程用户之间，控制二者的通信。

掌握三个关键术语的含义有助于理解 SSL VPN 是如何实现的。即：代理（Proxying）、应用转换（Application Translation）、端口转发（Port Forwarding）。

SSL VPN 网关至少要实现一种功能：代理 Web 页面。它将来自远端浏览器的页面请求（采用 HTTPS 协议）转发给 Web 服务器，然后将服务器的响应回传给终端用户。

对于非 Web 页面的文件访问，往往要借助于应用转换。SSL VPN 网关与企业网内部的微软 CIFS 或 FTP 服务器通信，将这些服务器对客户端的响应转化为 HTTPS 协议和 HTML 格式发往客户端，终端用户感觉这些服务器就是一些基于 Web 的应用。

有的 SSL VPN 产品所能支持的应用转换器和代理的数量非常少，有的则很好地支持了 FTP、网络文件系统和微软文件服务器的应用转换。用户在选择网关时，必须对自己所需要转换的应用有一个很明确的了解，并能够根据它们的重要性给它们排个先后顺序。

而有一些应用，如微软 Outlook 或 MSN，它们的外观会在转化为基于 Web 界面的过程中丢失。此时要用到端口转发技术。端口转发用于端口定义明确的应用。它需要在终端系统上运行一个非常小的 Java 或 ActiveX 程序作为端口转发器，监听某个端口上的连接。当数据包进入这个端口时，它们通过 SSL 连接中的隧道被传送到 SSL VPN 网关，SSL VPN 网关解开封装的数据包，将它们转发给目的应用服务器。使用端口转发器，需要终端用户指向他希望运行的本地应用程序，而不必指向真正的应用服务器。

良好的 SSL VPN 产品应该具有较好的互操作性，较为细致的访问控制能力，完善的日志和认证体系以及对应用的广泛支持。

SANGFOR
深信服科技

深圳市南山区麒麟路 1 号科技创业中心 4 楼

Add: 4th Floor， Incubation Center，

No.1 Qilin Road， Nanshan District，

Shenzhen P.C.:518052

产品咨询热线：800-830-9565

Email:master@sangfor.com.cn