

解决方案：东阳市政务网VPN应用方案 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/213/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_213954.htm 东阳市电子政务网络平台覆盖了全市机关部门、18个镇乡街道和主要事业单位共150多家单位，在此平台上实行电子公文传输及多个应用系统。政务网的部分事业单位和企业，以及政府领导、工作人员下班或者出差时，通过最传统的远程拨号方式实现远程的网络接入和访问，但其速度和质量很差、安全性实际也缺乏保障，严重影响和制约了电子政务的发展。随着网络技术的发展，宽带的普及，基于宽带Internet的VPN互联方式以其低成本、高效率的解决方案正日益受到推崇。解决方案目前，VPN实现的技术有很多种，PPTP、L2TP、IPSec、Socket5和SSL，用的最常见的是IPSec VPN和SSL VPN，那么怎么选择适合自己需要的？首先要了解一下IPSec VPN和SSL VPN的概念及优缺点。IPSec VPN即指采用IPSec协议来实现远程接入的一种VPN技术，IPSec是IETF（Internet Engineer Task Force）正在完善的安全标准，IPSec协议是一个范围广泛、开放的虚拟专用网安全协议，它提供所有在网络层上的数据保护，提供透明的安全通信。IPSec是基于网络层的，不能穿越通常的NAT、防火墙。IPSec是到目前为止最为安全的协议。同时IPSec VPN能够真正解决局域网之间的互联，形成一个真正的私有网络。但是IPSec VPN使用十分复杂，必须安装和维护客户端软件。另外，从远程通过IPSec通道连接到企业内部网络可能会增加局域网受到攻击或被病毒感染的可能。SSL VPN即指采用SSL（Security Socket Layer）协议来实现远程接

入的一种新型VPN技术。SSL协议是网景公司提出的基于WEB应用的安全协议，它包括：服务器认证、客户认证（可选）、SSL链路上的数据完整性和SSL链路上的数据保密性。对于内、外部应用来说，使用SSL可保证信息的真实性、完整性和保密性。目前SSL协议被广泛应用于各种浏览器应用，也可以应用于Outlook等使用TCP协议传输数据的C/S应用。SSL VPN的突出优势在于Web安全和移动接入。目前，对SSL VPN公认的三大好处是：首先来自于它的简单性，它不需要配置，可以立即安装、立即生效；第二个好处是客户端不需要安装，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。缺点是对于非web页面的文件访问，往往要借助于应用转换。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，有的能很好地支持了FTP、网络文件系统和微软文件服务器的应用转换。但是并不能真正形成局域网对局域网的应用，形成一个大的私有网络。所以相对于传统的IPSec VPN而言，SSL VPN具有部署简单，无客户端，维护成本低，网络适应性强等特点，但SSL VPN并不能取代IPSec VPN.因为，这两种技术目前应用在不同的领域。SSL VPN考虑的是应用软件的安全性，更多应用在Web的远程安全接入方面；而IPSec VPN是在两个网站之间通过专线或互联网安全连接以及两台服务器之间的安全连接，保护的是点对点之间的通信，并且，它不局限于Web应用。考虑到不改变东阳政务外网现有网络结构，利用现有电子政务外网Internet接入；接入到政府外网的用户多，用户的电脑使用水平也是参差不齐；客户端的操作系统不一样，如Windows98、Windows2000、Windows XP等等

；接入网络运行商不一样，如电信的、网通的等等；接入方式也不一样，有局域网的、有拨号上网的等等。如果使用IPSec VPN，那么政府的信息中心的任务是巨大而繁重的，维护的成本也很大。综上所述，采用目前技术比较成熟的SSL VPN已经能够满足远程访问和移动办公的需求了。方案实施 信息中心经过对多家VPN产品进行功能测试、性能分析，深信服科技SSL VPN以其多项独创的技术，高性价比被选用。在东阳市信息中心部署一台Sinfor M5400S千兆级SSL VPN 设备，用户认证采用SSL VPN自带的认证机制有效集成。对远程数据报送的单位进行用户认证，认证通过后，通过客户端的IE浏览器进行SSL VPN访问，从而使远程用户进行统计数据加密报送，保证了数据的安全传输，很好地解决了远程访问和移动办公的需求。实现效果和技术特点：1、迅速拥有高效稳定的SSL VPN平台，用户只需使用浏览器即可接入方便是深信服SSL VPN的一大特点。广泛的兼容性使其可以很方便的部署于网络的任何位置。而简单明了又兼备完整逻辑思路的操作模式可以让管理员迅速掌握，从而方便地配置出满足自身需求的个性化配置方案。在客户端不需要安装任何应用软件，不需做任何配置，同时也减轻了信息管理中心的工作。2、接入后的用户受控于更细致的访问控制粒度。深信服SSL VPN对每个用户的访问控制粒度精确到了URL级别。根据组织的构架，用户可以分组管理，而授权粒度则可以按照角色进行管理，为每个用户或每个组分配一个或多个角色。比如可以为某用户分配办公收发文和财务查询的双重角色，这样他即可以访问办公OA的进行收发文又可以访问财务系统进行财务查询。3、数据传输的安全。深信服SSL VPN

采用SSL协议加密建立安全的专用通道，使用1024位的非对称密钥进行身份认证过程的加密，使用128位的RC4算法和3DES算法保护数据传输的安全。

4、对系统运行实时监控和报警，具备完善的日志功能。深信服SSL VPN提供了调试、信息、告警、错误的四个级别的运行日志，帮助管理诊断系统。并提供了用户活动日志来跟踪用户行为。

5、集成防火墙，有效保护内部服务。和多数SSL VPN不同，深信服SSL VPN集成了高性能的防火墙，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，包括对开放端口的DOS攻击。

6、客户端安全检查。SSL用户访问政务网内部资源时，有可能将间谍软件，病毒随着客户端对政务网的访问而进入内网，导致服务器遭受间谍软件、病毒的风险。深信服科技创新性地采用了网络访问准入规则，这一技术是管理员在SINFOR UTM 安全网关的准入规则中预先定制好SSL客户端计算机的安全策略。当SSL用户计算机通过SSL VPN连接政务网时，若启用客户端安全检查策略，此时用户的计算机会自动从SSL VPN下载相应的安全策略扫描程序，根据指定的安全策略启动扫描程序，并检查用户的计算机是否具备了相应的安全策略。只有符合相应的安全策略的用户才允许登陆，不具备相应安全条件的用户，不允许登陆到SSL设备，也连不同SSL通道。这样从根本上提高了SSL用户计算机的安全性，减少了SSL用户遭受蠕虫、病毒、木马以及间谍软件而导致服务器遭受破坏的风险。

7、硬件特征码与用户捆绑。深信服SSL VPN在用户第一次登陆时候，会自动发该用户第一次登陆的计算机的相关的硬件特征码信息发送到管理界面，管理员只需划钩即可把用户名和计算机绑定到一起，即此用户

只有用次计算机才能登陆SSL VPN，增加了客户认证的安全性。所有的办公用户通过已有的上网线路，通过浏览器建立SSL VPN连接，快速地接入市政府网络，进行统一的办公，同时也整合了各委办局的各种资源，通过安全的身份认证技术，建立了统一的政务办公平台，实现高度智能的办公平台和信息共享，降低办公成本，提高了政府办公效率，更好地为公众服务。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com