L保护下的V 安全了吗？ PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/430/2021_2022_L_E4_BF_9D_E6_8A_A4_E4_B8_8B_c101_430317.htm 间谍软件、病毒、蠕虫、木马、广告软件及未授权的应用通过Web浏览渗透到企业网络中，从而造成了网络安全事件。在享受建立内部资源共享基础上高效率的协同工作的成果或Web上传下载的同时，也面临着保护内部网络及其数据安全性的挑战，包括网络反病毒、防入侵、防黑客、数据丢失等，基于SSL VPN的应用将会越来越多。面对当前的威胁，SSL保护下的 VPN 网络是否足够安全？ 当前信息安全分析 随着企业业务发展的需要，能够实现对网络具有高度安全性和稳定性的访问，一直是我们所追求的目标。远程安全访问是未来业务发展的趋势，在国内笔记本销售逐年增长情况下，通信工具迫切需要专门为其量身定做的远程安全访问方案。而伴随企业信息化程度的加深，企业和分支、企业和外地员工之间联系将不随地域分隔而分开，从信息流的传输、交换角度来看，它们之间更象一个整体，远程安全访问、协同工作的需求会日益明显。可见SSL VPN的安全对企业来说多么的重要。 我们知道传统上VPN系统的安全性主要包括三个层面：数据传输的安全、身份认证的安全、内网应用的安全。从协议上分析，SSL VPN采用标准的安全套接层协议对传输中的数据包进行加密。SSL协议则是浏览器自带的，加密强度一般为128位，从应用的实际情况看，完全能够满足数据传输层的安全需求。在身份认证的安全上，SSL VPN也日趋成熟。 可见更高的信息安全性和应用性能是 SSL VPN 来的最显而易见的好处。由

于SSL 协议本身就是一种安全技术，因此SSL VPN 就具有防止信息泄漏、拒绝非法访问、保护信息的完整性、防止用户假冒、保证系统可用性的特点，能够进一步保障访问安全，从而扩充了安全功能设施。而作为处 于应用层和TCP/UDP 层之间的一种安全协议，相比较处于网络层的IPSec，SSL可以提供基于应用层的访问控制，更适合远程安全访问的移动性和分散性的特点。 安全措施知多少 企业需要通过互联网（笔记本型计算机、移动个人计算机、远程用户接入）达到广泛而全面性的信息存取。SSL VPN 能满足目前所有的远程接入需要。SSL VPN技术为远程接入提供增强的灵活性，以便更好地配合公司网络的安全性和基础结构需要，同时给终端用户一个统一的、容易的界面和一个简化的用户体验。SSL VPN 具有高可用性，具备可靠的冗余能力，排除了单点故障发生的可能性，减少系统停机时间，另外它还具有负载均衡的能力，提高系统的整体性能。通过浏览器内置的SSL模块，与SSL VPN 在应用客户端与服务器之间建立一个受高等级保护的安全通信通道，确保网络传输的数据流量的机密性和完整性。应用要求企业实现高度的实时数据，以实现企业的日益高标准的协同工作的要求，特别是企业对零库存的要求压力越来越高，要求企业能对订单和生产的过程及库存和原材料同步协调，因此实时性的要求极高。同时，实现了数据的集中和供应链的管理，这就要求企业网络必须在高度的安全的保障下稳定地运行。而SSL VPN 提供的只是应用层的互连，每个使用者只能访问授权给他的应用，除此之外的其它任何资源都无法访问，确保了系统资源的安全性。 三点方案力保安全有了SSL VPN安全防护同时，我们还需要把基础设施与支撑

系统的防护做好。应该从以下三个方面来做： 第一、网络安全边界及SSL VPN设备的保护。比如：部署结合多种防护技术的多层式防御架构，应该分别在三个层级建置整合式的解决方案，包括了部署在互联网网关、网络传输过程中和桌面终端的各种创新技术，来达到网络安全保证。 第二、做好web威胁的防护。由于SSL网关隔离了内网服务器和客户端，只留下一个Web浏览接口。要避免被网页恶意代码感染关键是不要轻易去一些并不信任的站点，尤其是一些带有美女图片等的网址。但是这个并不能真正防止网页恶意代码的攻击，因为这些恶意代码有可能在任何地方出现。 第三、做好员工的培训工作，增强员工的安全意识，避免一些无操作造成的安全事件。 由此可见， SSL VPN 100%的应用加上100%的SSL VPN才是真正的企业核心应用，这就需要厂商对各种各样的企业应用进行更具深度的理解和响应，以及企业自身对各种层面业务的需求，只有做到深入有效的沟通后，才能使SSL VPN的功能发挥的更充分更高效。SSL保护下的 VPN 网络更安全。 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