从哪着手提升企业网络安全 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/461/2021_2022__E4_BB_8E_E5_93_AA_E7_9D_80_E6_c101_461680.htm 病毒、间谍软件、垃圾邮件等网络威胁会破坏中小型企业的业务运营，不论是桌面端防护，还是边界设备防护，都不能保证网络100%的安全。如今的网络入侵和安全防范，实际上就是指网络攻防技术。攻击技术包括目标网络信息收集技术，目标网络权限提升技术，目标网络渗透技术，目标网络摧毁技术四大类。每一类技术，都是日新月异、不断更新的。所以在网络的安全防范上，企业需要面对越来越多来自四面八方的新技术的攻击。 漏洞来自何处 而目前的安全解决方案也只能提供风险管理，意味着尽量减少网络漏洞和风险。其实最好的办法就是改进预防方法，并且选择最适合自己网络的解决方案，才能有效的对抗攻击。网络主要面临有三种漏洞：策略、配置和技术漏洞。如果对网络所许可的或禁止的知之甚少，就会出现策略漏洞。配置漏洞很容易发生，此外，操作系统及缓冲器溢出等技术漏洞也是重大隐患。中小企业IT主管该如何着手如今网络安全呢？ 着手网络安全 我们知道网络安全70%来自于企业网内部，可见网络安全好比守护办公大楼，你会先给门上一道锁，将不速之客拒之门外，防火墙就是网络上的一把锁，它控制着访问网络的权限，只允许特许用户进出网络。当然，守护大楼不仅仅是给门上锁，网络安全也不仅仅是在网络周边设置防火墙，为了最有效地满足网络安全需求，还需要其它技术，如用户验证、虚拟专用网和入侵检测。从管理和技术两个角度来推进网络安全工作，不仅是现阶段

解决好网络安全问题的需要，也是今后网络安全发展的必然趋势。要想充分维护好企业的网络安全，必须遵以下三个方面：一、整体考虑，统一规划。网络安全取决于系统中最薄弱的环节。"一点突破，全网突破"，单个系统考虑安全问题并不能真正有效的保证安全，需要从整体IT体系层次建立网络安全架构，整体考虑，全面防护。二、对于用户数为50～500的中小型企业而言，使用普通的安全软件来抵挡日益猖獗的威胁已经显得力不从心，选择一款正确而有效的安全产品是中小型企业防范网络威胁的关键。在选择网络安全设备时应当具有长远的发展眼光，对未来的安全性和网络更有保障，谁也不希望部署一串安全孤岛？一般的安全产品要具有以下三方面的功能：1、全合一的网关安全：有助于防止多种威胁和不适当内容进入企业的网络。其安全防护包括防病毒、防垃圾邮件和内容过滤，无需额外付费的防间谍软件、防网络钓鱼、防僵尸保护以及URL过滤服务，SMTP、HTTP、FTP以及POP3协议发现恶意有效荷载。2、易于管理和部署：借助基于Web的控制台的单一集成解决方案简化管理。它可以自动清除桌面计算机中的间谍软件和病毒，显著减少宕机时间和管理工作量。简单而透明的嵌入式安装使企业无需重新配置防火墙、VPN以及桌面计算机的设置。3、有效的早期防护：较早地防止感染，无需任何人工干预，因此降低感染事件。能够通过封堵未知的恶件来确保早期保护；病毒爆发预防服务可以通过自动响应来防止病毒爆发。三、企业网络安全正在形成第三个阶段：网络行为管理安全。其根本立足点，不是对设备的保护，也不是对数据的看守，而是规范企业员工网络行为，这已经上升到了对人的管理的阶段

，通过技术设备和规章制度的结合来指导、规范员工正确使用单位的网络资源，从而对局域网的上网行为进行有效管理。为了避免增添人手，就要从基于设备的管理或基于多个设备的管理改为基于策略的管理。基于设备的管理需要为设备进行逐个管理及配置，这非常费时、费力，还容易出错。基于策略的管理方法要灵巧得多。它使你可以通过策略管理器集中管理策略（譬如允许指定的一组用户利用Http访问因特网），然后策略管理器会生产所有必要的配置文件，并对所有设备进行配置，而与数量或位置无关。这种管理可以合理配置有限资源、减少错误、确保网络一致性、减少时间和成本。