 目前，许多中小用户因业务发展，不断更新或升级网络，从而造成自身用户环境差异较大，整个网络系统平台参差不齐，在服务器端大多使用 Linux和Unix的，PC端使用Windows 9X/2000/XP。所以在企业应用中往往是Linux/Unix和Windows操作系统共存形成异构网络。中小企业由于缺少经验丰富的Linux网 络管理员和安全产品采购资金，所以对于网络安全经常是头痛医头、脚痛医脚，缺乏缺乏全面的考虑。 这里笔者把中小企业的安全分为四种来提出解决方案。服务器安全、网络设备的安全、接入互联网的安全和内部网络的安全。 一、服务器安全： 1． 关闭无用的端口 任何网络连接都是通过开放的应用端口来实现的。如果我们尽可能少地开放端口，就使网络攻击变成无源之水，从而大大减少了攻击者成功的机会。 首先检查你的inetd．conf文件。inetd在某些端口上守侯，准备为你提供必要的服务。如果某人开发出一个特殊的inetd守护程序，这里 就存在一个安全隐患。你应当在inetd．conf文件中注释掉那些永不会用到的服务(如：echo、gopher、rsh、rlogin、rexec、ntalk、finger等)。注释除非绝对需要，你一定要注释掉rsh、rlogin和rexec，而telnet建议你使用更为安全的ssh来代替，然后杀掉lnetd进程。这样inetd不再监控你机器上的守护程序，从而杜绝有人利用它来窃取你的应用端口。你最好是下载一个端口扫描程序扫描你的系 统，如果发现有你不知道的开放端口，马上找到正使用它的进程，从而判断是否关闭它们

。 2． 删除不用的软件包 在进行系统规划时，总的原则是将不需要的服务一律去掉。默认的Linux就是一个强大的系统，运行了很多的服务。但有许多服务是不需要的，很容易引 起安全风险。这个文件就是/etc/inetd.conf，它制定了/usr/sbin/inetd将要监听的服务，你可能只需要其中的两个：telnet和ftp，其它的类如shell、login、exec、talk、ntalk、imap、pop-2、pop-3、finger、auth 等，除非你真的想用它，否则统统关闭。 3． 不设置缺省路由 在主机中，应该严格禁止设置缺省路由，即default route。建议为每一个子网或网段设置一个路由，否则其它机器就可能通过一定方式访问该主机 4． 口令管理 口令的长度一般不要少于8个字符，口令的组成应以无规则的大小写字母、数字和符号相结合，严格避免用英语单词或词组等设置口令，而且各用户的口令应 该养成定期更换的习惯。另外，口令的保护还涉及到对/etc/passwd和/etc/shadow文件的保护，必须做到只有系统管理员才能访问这2个文 件。安装一个口令过滤工具加npasswd，能帮你检查你的口令是否耐得住攻击。如果你以前没有安装此类的工具，建议你现在马上安装。如果你是系统管理 员，你的系统中又没有安装口令过滤工具，请你马上检查所有用户的口令是否能被穷尽搜索到，即对你的／ect／passwd文件实施穷尽搜索攻击。 5． 分区管理 一个潜在的攻击，它首先就会尝试缓冲区溢出。在过去的几年中，以缓冲区溢出为类型的安全漏洞是最为常见的一种形式了。更为严重的是，缓冲区溢出漏洞 占了远程网络攻击的绝大多数，这种攻击可以轻易使得一个匿名的Internet用户有机会获得一台主机的部分或全部的控制权！ 为了防止此类攻击，我们从安装系统时就应该注意

。如果用root分区记录数据，如log文件，就可能因为拒绝服务产生大量日志或垃圾邮件，从而导致 系统崩溃。所以建议为/var开辟单独的分区，用来存放日志和邮件，以避免root分区被溢出。最好为特殊的应用程序单独开一个分区，特别是可以产生大量 日志的程序，还建议为/home单独分一个区，这样他们就不能填满/分区了，从而就避免了部分针对Linux分区溢出的恶意攻击。 6． 防范网络嗅探： 嗅探器技术被广泛应用于网络维护和管理方面，它工作的时候就像一部被动声纳，默默的接收看来自网络的各种信息，通过对这些数据的分析，网络管理员可 以深入了解网络当前的运行状况，以便找出网络中的漏洞。在网络安全日益被注意的今天.我们不但要正确使用嗅探器.还要合理防范嗅探器的危害.嗅探器能够造成很大的安全危害，主要是因为它们不容易被发现。对于一个安全性能要求很严格的企业，同时使用安全的拓扑结构、会话加密、使用静态的ARP地址是有必要 的。 7． 完整的日志管理 日志文件时刻为你记录着你的系统的运行情况。当黑客光临时，也不能逃脱日志的法眼。所以黑客往往在攻击时修改日志文件，来隐藏踪迹。因此我们要限制对／var／log文件的访问，禁止一般权限的用户去查看日志文件。 另外，我们还可以安装一个icmp／tcp日志管理程序，如iplogger，来观察那些可疑的多次的连接尝试(加icmp flood3或一些类似的情况)。还要小心一些来自不明主机的登录。 完整的日志管理要包括网络数据的正确性、有效性、合法性。对日志文件的分析还可以预防入侵。例如、某一个用户几小时内的20次的注册失败记录，很可能是入侵者正在尝试该用户的口令。 8． 终止正进行的攻击 假如你在检查日志文件时，发现了一个用

户从你未知的主机登录，而且你确定此用户在这台主机上没有账号，此时你可能正被攻击。首先你要马上锁住此账号 (在口令文件或shadow文件中，此用户的口令前加一个Ib或其他的字符)。若攻击者已经连接到系统，你应马上断开主机与网络的物理连接。如有可能，你 还要进一步查看此用户的历史记录，查看其他用户是否也被假冒，攻击音是否拥有根权限。杀掉此用户的所有进程并把此主机的ip地址掩码加到文件hosts.deny中。 9. 使用安全工具软件： Linux已经有一些工具可以保障服 务器的安全。如bastille linux。对于不熟悉 linux 安全设定的使用者来说，是一套相当方便的软件，bastille linux 目的是希望在已经存在的 linux 系统上，建构出一个安全性的环境。另外随着Linux病毒的出现，现在已经有一些Linux服务器防病毒软件，安装Linux防病毒软件已经是非常迫切了。