电子商务安全技术：GAP创造安全的网络办公环境电子商务考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/582/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_582939.htm 目前，宽带网已经得到普及，业界电子商务的开展，海量的网络信息，日趋丰富的网络功能使“ 网上办公 ”条件已经成熟。随着我国电子政务的进一步发展，政府对企事业单位的管理将更多地在网络上进行，因此企业办公将不再局限于传统模式。根据现代办公的信息化程度，可以将其分成三个阶段。首先是机械电子设备代替大量手工操作的阶段，主要由电话、早期的计算机、打印机、模拟复印机实现。第二个阶段是办公自动化，办公室内甚至整个企业众多独立的计算机被局域网连接起来，数字复印机、网络打印机、扫描仪的普遍使用，使得原本分散、孤立的办公作业得到集成，初步具备了办公信息化的雏形。办公自动化的进一步发展就是办公信息化阶段，“ 网络办公 ”将实现“ 内部办公自动化，文件交换无纸化，管理决策网络化，服务用户电子化 ”的办公信息化目标。但随着办公信息化带来效率的提高，其安全性，特别是内部办公网络的安全问题，也引起人们更大的关注和思考。 办公网络面临的内部安全威胁 正如我们所知道的那样，70%的安全威胁来自网络内部，其形式主要表现在以下几个方面。 内部办公人员安全意识淡漠 内部办公人员每天都专注于本身的工作，认为网络安全与己无关，因此在意识上、行为上忽略了安全的规则。为了方便，他们常常会选择易于记忆但同时也易于被猜测或被黑客工具破解的密码，不经查杀病毒就使用来历不明的软件，随便将内部办公网络的软硬件配置、拓扑结构告

之外部无关人员，给黑客入侵留下隐患。 别有用心的内部人员故意破坏 办公室别有用心的内部人员会造成十分严重的破坏。防火墙、IDS检测系统等网络安全产品主要针对外部入侵进行防范，但面对内部人员的不安全行为却无法阻止。一些办公人员喜欢休息日在办公室内上网浏览网页，下载软件或玩网络游戏，但受到网络安全管理规定的限制，于是绕过防火墙的检测偷偷拨号上网，造成黑客可以通过这些拨号上网的计算机来攻入内部网络。而有些办公人员稍具网络知识，又对充当网络黑客感兴趣，于是私自修改系统或找到黑客工具在办公网络内运行，不知不觉中开启了后门或进行了网络破坏还浑然不觉。更为严重的是一些人员已经在准备跳槽或被施利收买，办公内部机密信息被其私自拷贝、复制后流失到外部。此外，还有那些被批评、解职、停职的内部人员，由于对内部办公网络比较熟悉，会借着各种机会（如找以前同事）进行报复，如使用病毒造成其传播感染，或删除一些重要的文件，甚至会与外部黑客相勾结，攻击、控制内部办公网络，使得系统无法正常工作，严重时造成系统瘫痪。 单位领导对办公网络安全没有足够重视 有些单位对办公网络存在着只用不管的现象，有的领导只关心网络有没有建起来，能否连得上，而对其安全没有概念，甚至对于网络基本情况，包括网络规模、网络结构、网络设备、网络出口等概不知情。对内部办公人员，公司平时很少进行安全技术培训和安全意识教育，没有建立相应的办公网络安全岗位和安全管理制度，对于黑客的攻击和内部违规操作则又存在侥幸心理，认为这些是非常遥远的事情。在硬件上，领导普遍认为只要安装了防火墙、IDS、IPS，设置了Honeypot就可以高枕无忧

。而没有对新的安全技术和安全产品做及时升级更新，对网络资源没有进行细粒度安全级别的划分，使内部不同密级的网络资源处于同样的安全级别，一旦低级别的数据信息出现安全问题，将直接影响核心保密信息的安全和完整。百考试题整理 缺乏足够的计算机网络安全专业人才 由于计算机网络安全在国内起步较晚，许多单位缺乏专门的信息安全人才，使办公信息化的网络安全防护只能由一些网络公司代为进行，但这些网络安全公司必定不能接触许多高级机密的办公信息区域，因此依然存在许多信息安全漏洞和隐患。没有内部信息安全专业人员对系统实施抗攻击能力测试，单位则无法掌握自身办公信息网络的安全强度和达到的安全等级。同时，网络系统的漏洞扫描，操作系统的补丁安装和网络设备的软、硬件升级，对办公网内外数据流的监控和入侵检测，系统日志的周期审计和分析等经常性的安全维护和管理也难以得到及时的实行。 网络隔离技术（GAP）初探 GAP技术 GAP是指通过专用硬件使两个或两个以上的网络在不连通的情况下进行网络之间的安全数据传输和资源共享的技术。简而言之，就是在不连通的网络之间提供数据传输，但不允许这些网络间运行交互式协议。GAP一般包括三个部分：内网处理单元、外网处理单元、专用隔离交换单元。其内、外网处理单元各拥有一个网络接口及相应的IP地址，分别对应连接内网（涉密网）和外网（互联网），专用隔离交换单元受硬件电路控制高速切换，在任一瞬间仅连接内网处理单元或外网处理单元之一。 GAP可以切断网络之间的TCP/IP连接，分解或重组TCP/IP数据包，进行安全审查，包括网络协议检查和内容确认等，在同一时间只和一边的网络连接，与之进行数

据交换。 GAP的数据传递过程 内网处理单元代理内网用户的网络服务请求，将数据通过专用隔离硬件交换单元转移至外网处理单元，外网处理单元负责向外网服务器发出连接请求并取得网络数据，然后通过专用隔离交换单元将数据转移回内网处理单元，再由其返回给内网用户。 GAP具有的高安全性 GAP设备具有安全隔离、内核防护、协议转换、病毒查杀、访问控制、安全审计和身份认证等安全功能。由于GAP断开链路层并切断所有的TCP连接，并对应用层的数据交换按安全策略进行安全检查，因此能够保证数据的安全性并防止未知病毒的感染破坏。 使用网络隔离技术（GAP）进行内部防护 我们知道，单台的计算机出现感染病毒或操作错误是难以避免的，而这种局部的问题较易解决并且带来的损失较小。但是，在办公信息化的条件下，如果这种错误在网络所允许的范围内无限制地扩大，则造成的损失和破坏就难以想象。因此，对办公内部网络的安全防范不是确保每一台网络内的计算机不发生安全问题，而是确保发生的安全问题只限于这一台计算机或这一小范围，控制其影响的区域。目前，对内网采取“ 多安全域划分 ”的技术较好地解决了这个问题，而GAP系统的一个典型的应用就是对内网的多个不同信任域的信息交换和访问进行控制。因此，使用GAP系统来实现办公内网的“ 多安全域划分 ”，是一个比较理想的方法。F8F8"