CA电子商务安全解决方案eTrust PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/242/2021_2022_CA_E7_94_B5_E5_AD_90_E5_95_c40_242479.htm 一.防火墙的普遍局限 尽管很多企业已经实施了防火墙，但这不代表企业就此高枕无忧了。虽然大部分企业已意识到安全的重要性，并且众多的公司已开始采用防火墙技术进行网络安全防护，但是由于防火墙是基于授权机制来控制企业流入流出的信息流，所以网上的安全防护仅如果仅依赖于这种授权控制，那么疏漏就会很多。 随着人们网络安全意识的提高，采取防火墙保护系统的做法已被广泛采用，同时也出现了很多的防火墙产品。但据防火墙专家估计，由于缺乏专业技术，选用服务不当，配置不好和操作系统的脆弱性，50%左右的防火墙的实施是不正确的。另外，由于互联网的开放性，防火墙也有其局限性：1、防火墙不能防范不经由防火墙的攻击。例如，如果允许从受保护网内部不受限制的向外拨号，一些用户可以形成与Internet的直接的连接，从而绕过防火墙，造成一个潜在的后门攻击渠道。 2、防火墙不能防止感染了病毒的软件或文件的传输。只能在每台主机上装反病毒软件。 3、防火墙不能防止数据驱动式攻击。当有些表面看来无害的数据被邮寄或复制到Internet主机上并被执行而发起攻击时，就会发生数据驱动攻击。 关于防火墙的局限性，我们不妨举例来说明，比如A是B公司的职员，那么他经过MIS部门的授权就可以通过防火墙来访问企业内部资源了，现在他因一些原因离职，在人事部门未通知MIS部门收回对A的访问授权期间，A仍可畅通无阻的进入B公司的内部网。我们知道，企业内部存在信

息沟通延迟的情况是很常见的，所以仅有防火墙一层安全设置就将给A提供窃取公司内部信息的可乘之机。 二.Web服务器的安全受到威胁 在今年2月中旬，全球各大主要网站都不同程度地遭受到黑客的攻击。在这场“ 灾难 ”中，象雅虎、亚马逊等全球著名的网站都没有从这一事件幸免。有黑客在对这些开展电子商务网站大范围攻击中都使用了诸如TFN2K (Tribal Flood Network 2K)的拒绝服务攻击工具。在系统所有者不知情的情况下，黑客在Internet上的数千台系统中安装了TFN2K等程序。 专家调查发现，这一新的安全破坏行为所具有新的破坏特征是这样的：用户在点击网页、邮件、新闻组邮件中的链接时，也许就无心地执行了黑客的指令；用户在观看其他用户提供的动态网页时，也可能无心地执行恶意代码。这些危险事件的发生同时也表明：当今大多数Web服务器，包括那些提供创建电子商务模块的服务器在内，都面临着危险，都已成为黑客袭击的目标。 而现在对于电子商务企业来说，最危险的就是任何Web服务器都能通过远程控制轻易地转变为恶意代码的传播机器。通过Web内建的电子商务功能，黑客能够把Web服务器变成Web危险，也就是说现在每个Web服务器都可能被黑客用来分发恶意代码。 