电子商务安全技术：浅析网络安全技术电子商务考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/513/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_513699.htm 1.概述 21世纪全世界的计算机都将通过Internet联到一起，信息安全的内涵也就发生了根本的变化。它不仅从一般性的防卫变成了一种非常普通的防范，而且还从一种专门的领域变成了无处不在。当人类步入21世纪这一信息社会、网络社会的时候，我国将建立起一套完整的网络安全体系，特别是从政策上和法律上建立起有中国自己特色的网络安全体系。 一个国家的信息安全体系实际上包括国家的法规和政策，以及技术与市场的发展平台。我国在构建信息防卫系统时，应着力发展自己独特的安全产品，我国要想真正解决网络安全问题，最终的办法就是通过发展民族的安全产业，带动我国网络安全技术的整体提高。 网络安全产品有以下几大特点：第一，网络安全来源于安全策略与技术的多样化，如果采用一种统一的技术和策略也就不安全了；第二，网络的安全机制与技术要不断地变化；第三，随着网络在社会个方面的延伸，进入网络的手段也越来越多，因此，网络安全技术是一个十分复杂的系统工程。为此建立有中国特色的网络安全体系，需要国家政策和法规的支持及集团联合研究开发。安全与反安全就像矛盾的两个方面，总是不断地向上攀升，所以安全产业将来也是一个随着新技术发展而不断发展的产业。 信息安全是国家发展所面临的一个重要问题。对于这个问题，我们还没有从系统的规划上去考虑它，从技术上、产业上、政策上来发展它。政府不仅应该看见信息安全的发展是我国高科技产业的一部分

，而且应该看到，发展安全产业的政策是信息安全保障系统的一个重要组成部分，甚至应该看到它对我国未来电子化、信息化的发展将起到非常重要的作用。 2.防火墙 网络防火墙技术是一种用来加强网络之间访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络，访问内部网络资源，保护内部网络操作环境的特殊网络互联设备。它对两个或多个网络之间传输的数据包如链接方式按照一定的安全策略来实施检查，以决定网络之间的通信是否被允许，并监视网络运行状态。 目前的防火墙产品主要有堡垒主机、包过滤路由器、应用层网关(代理服务器)以及电路层网关、屏蔽主机防火墙、双宿主机等类型。 虽然防火墙是目前保护网络免遭黑客袭击的有效手段，但也有明显不足：无法防范通过防火墙以外的其它途径的攻击，不能防止来自内部变节者和不经心的用户们带来的威胁，也不能完全防止传送已感染病毒的软件或文件，以及无法防范数据驱动型的攻击。 自从1986年美国Digital公司在Internet上安装了全球第一个商用防火墙系统，提出了防火墙概念后，防火墙技术得到了飞速的发展。国内外已有数十家公司推出了功能各不相同的防火墙产品系列。 防火墙处于5层网络安全体系中的最底层,属于网络层安全技术范畴。在这一层上,企业对安全系统提出的问题是:所有的IP是否都能访问到企业的内部网络系统?如果答案是“ 是 ”,则说明企业内部网还没有在网络层采取相应的防范措施。百考试题整理 作为内部网络与外部公共网络之间的第一道屏障,防火墙是最先受到人们重视的网络安全产品之一。虽然从理论上看,防火墙处于网络安全的最底层,负责网络间的安全认证与传输,但随着网络安全技术的整体发展和网络应用的不断变

化,现代防火墙技术已经逐步走向网络层之外的其他安全层次,不仅要完成传统防火墙的过滤任务,同时还能为各种网络应用提供相应的安全服务。另外还有多种防火墙产品正朝着数据安全与用户认证、防止病毒与黑客侵入等方向发展。 根据防火墙所采用的技术不同,我们可以将它分为四种基本类型:包过滤型、网络地址转换NAT、代理型和监测型。 2.1.包过滤型 包过滤型产品是防火墙的初级产品,其技术依据是网络中的分包传输技术。网络上的数据都是以“ 包 ”为单位进行传输的,数据被分割成为一定大小的数据包,每一个数据包中都会包含一些特定信息,如数据的源地址、目标地址、TCP/UDP源端口和目标端口等。防火墙通过读取数据包中的地址信息来判断这些“ 包 ”是否来自可信任的安全站点 ,一旦发现来自危险站点的数据包,防火墙便会将这些数据拒之门外。系统管理员也可以根据实际情况灵活制订判断规则。 包过滤技术的优点是简单实用,实现成本较低,在应用环境比较简单的情况下,能够以较小的代价在一定程度上保证系统的安全。 但包过滤技术的缺陷也是明显的。包过滤技术是一种完全基于网络层的安全技术,只能根据数据包的来源、目标和端口等网络信息进行判断,无法识别基于应用层的恶意侵入,如恶意的Java小程序以及电子邮件中附带的病毒。有经验的黑客很容易伪造IP地址,骗过包过滤型防火墙。 2.2.网络地址转化NAT 网络地址转换是一种用于把IP地址转换成临时的、外部的、注册的IP地址标准。它允许具有私有IP地址的内部网络访问因特网。它还意味着用户不许要为其网络中每一台机器取得注册的IP地址。 NAT的工作过程如图1所示： 在内部网络通过安全网卡访问外部网络时，将产生一个映射记录。系统将外出的源地址

和源端口映射为一个伪装的地址和端口，让这个伪装的地址和端口通过非安全网卡与外部网络连接，这样对外就隐藏了真实的内部网络地址。在外部网络通过非安全网卡访问内部网络时，它并不知道内部网络的连接情况，而只是通过一个开放的IP地址和端口来请求访问。OLM防火墙根据预先定义好的映射规则来判断这个访问是否安全。当符合规则时，防火墙认为访问是安全的，可以接受访问请求，也可以将连接请求映射到不同的内部计算机中。当不符合规则时，防火墙认为该访问是不安全的，不能被接受，防火墙将屏蔽外部的连接请求。网络地址转换的过程对于用户来说是透明的，不需要用户进行设置，用户只要进行常规操作即可。百考试题收集 2.3.代理型 代理型防火墙也可以被称为代理服务器,它的安全性要高于包过滤型产品,并已经开始向应用层发展。代理服务器位于客户机与服务器之间,完全阻挡了二者间的数据交流。从客户机来看,代理服务器相当于一台真正的服务器.而从服务器来看,代理服务器又是一台真正的客户机。当客户机需要使用服务器上的数据时,首先将数据请求发给代理服务器,代理服务器再根据这一请求向服务器索取数据,然后再由代理服务器将数据传输给客户机。由于外部系统与内部服务器之间没有直接的数据通道,外部的恶意侵害也就很难伤害到企业内部网络系统。 代理型防火墙的优点是安全性较高,可以针对应用层进行侦测和扫描,对付基于应用层的侵入和病毒都十分有效。其缺点是对系统的整体性能有较大的影响,而且代理服务器必须针对客户机可能产生的所有应用类型逐一进行设置,大大增加了系统管理的复杂性。 2.4.监测型 监测型防火墙是新一代的产品,这一技术实际已经超越了最初的防火墙定义。监

测型防火墙能够对各层的数据进行主动的、实时的监测,在对这些数据加以分析的基础上,监测型防火墙能够有效地判断出各层中的非法侵入。同时,这种检测型防火墙产品一般还带有分布式探测器,这些探测器安置在各种应用服务器和其他网络的节点之中,不仅能够检测来自网络外部的攻击,同时对来自内部的恶意破坏也有极强的防范作用。据权威机构统计,在针对网络系统的攻击中,有相当比例的攻击来自网络内部。因此,监测型防火墙不仅超越了传统防火墙的定义,而且在安全性上也超越了前两代产品 虽然监测型防火墙安全性上已超越了包过滤型和代理服务器型防火墙,但由于监测型防火墙技术的实现成本较高,也不易管理,所以目前在实用中的防火墙产品仍然以第二代代理型产品为主,但在某些方面也已经开始使用监测型防火墙。基于对系统成本与安全技术成本的综合考虑,用户可以选择性地使用某些监测型技术。这样既能够保证网络系统的安全性需求,同时也能有效地控制安全系统的总拥有成本。实际上,作为当前防火墙产品的主流趋势,大多数代理服务器(也称应用网关)也集成了包过滤技术,这两种技术的混合应用显然比单独使用具有更大的优势。由于这种产品是基于应用的,应用网关能提供对协议的过滤。例如,它可以过滤掉FTP连接中的PUT命令,而且通过代理应用,应用网关能够有效地避免内部网络的信息外泄。正是由于应用网关的这些特点,使得应用过程中的矛盾主要集中在对多种网络应用协议的有效支持和对网络整体性能的影响上。F8F8" 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