计算机网络安全中防火墙技术的有效应用

郑　兵
海南科技职业大学，中国·海南 海口 571126

【摘　要】计算机网络的快速进步是现代化社会发展的表现，存储和信息传输主要依据互联网信息技术，促进了社会的进步，网络信息技术安全面对不断增加的网络病毒和恶意攻击，这就要增强安全技术手段。针对这一系列问题，相应的方法是有效应用防火墙技术来进行安全防护。本文对计算机网络安全中防火墙技术的应用进行了列举，具体分析计算机网络安全中防火墙应用，提出提高计算机网络安全发展的具体方案，促进计算机网络安全应用的可靠性。

【关键词】计算机网络安全；防火墙技术；应用措施

1　计算机网络安全问题发生的原因

1.1 个人因素

在计算机应用过程中，很多用户缺乏正确的操作规范，很多网络风险都是由于使用者自身的因素而产生的，对于网络风险的严重性没有明确的认识，这种不良行为习惯对网络风险的严重性是没有明确认识导致的，会造成严重损害，从而致使用户信息被盗。首先是无意识造成的，这是由多种因素引起的。例如，计算机网络用户自身的专业能力不足，不能形成良好的安全意识，或者在实际过程中，错误和操作不当而产生的安全问题，例如有些用户会查看不健康的网站，并在网站上跳出的小窗口，随意点击。有些电脑用户在实际操作过程中可能会威胁到电脑网络的安全，如不按正确的操作步骤或无意泄露相关信息等。在使用电脑方面，我们需要养成文明使用网络的习惯。不然会增加病毒入侵的危险，因此要真正实现安全的网络应用，必须规范自己的行为。

1.2 环境风险

电脑设备之间偶发性的自然灾害、计算机使用环境较差、元器件老化引发的问题较多，计算机网络共享环境对网络资源和信息的开放性有一定的影响，资源的开放性带来安全风险，威胁网络信息环境，破坏企业内部网络的安全保护结构，也有些外部攻击造成的安全情况，这些都使网络处于不安全状态，很多个人和企业不重视技术风险的防范，企业在使用网络系统时缺乏充分的风险意识，不使用防火墙技术与外网隔离，因此在计算机网络应用上增强对电脑设备的维护和管理，减少由此产生的网络安全问题，有效发挥其价值。

1.3 病毒原因

在计算机网络安全方面，计算机病毒也是原因之一，也是最重要的因素之一，计算机病毒本身可以直接插入计算机程序，也可能直接影响和破坏计算机的正常运行。电脑网络的安全功能当然会受到损害，而且大部分的电脑病毒都具有复制能力和隐藏能力，在使用电脑时很难及时发现它们的活动，不同病毒类型对电脑网络安全产生不同的影响，而且与其它黑客技术相结合，可能威胁到电脑网络安全。由此可见，计算机病毒是引发安全事件的重要的原因之一，所以要定期检查并杀死病毒，防止恶性攻击者熟悉用户的使用习惯。对病毒进行预先查杀，全面保护计算机网络安全，实施防火墙技术等技术手段，有效地避免潜在安全隐患，使计算机网络运行在全方位得到安全防护，优化和改善计算机网络环境，体现防火墙技术的实用价值，最终满足了计算机网络安全需求。

2　计算机网络安全中防火墙技术应用分析

2.1 访问控制措施

访问策略在计算机网络的应用过程中起着非常重要的效用，防火墙是计算机网络安全的重心，在访问控制措施中起着主要作用。技术而言，是通过对计算机网络运行的全过程进行统计分析，形成较为完整、科学的保护体系，有效地提高计算机网络的安全性，防火墙通过对计算机网络安全运行的网段来区分信息单位，根据不同类型的数据信息进行归档。在这一过程中，防火墙技术可以根据使用者的网络习惯来保护计算机网络，使用多种手段，控制网络风险对电脑的负面影响，基于防火墙技术的访问策略，用户能够全面掌握计算机网络的运行特征，从而为网络信息安全做出贡献，保障计算机网络的安全，在计算机网络应用过程中，随着时间的前进，越来越出现各种漏洞，网络危险机率增加。利用防火墙技术可以有效识别这些漏洞，处理漏洞。对防火墙规则进行调整，信息网络安全性得到增加，对其策略表执行，可以提高网络安全。带有安全配置的防火墙能够与计算机网络联接，使计算机网络就处于防火墙的保护之下。安全配置在防火墙技术中非常重要，其通过加强计算机网络运行的安全性，使计算机网络信息的交互通道得到改善。

2.2 用户身份信息识别

用户身份认证是防火墙技术的重要组成部分，是计算机和网络安全的基础部分，可以提高数据信息的机密性，对电脑用户身份认证也是防火墙的基础功能。计算机启动界面的用户设置权限，根据用户输入的账号密码，配对用户账户等级权限，确定用户账户信息，对计算机用户进行保障。认证主要是屏蔽用户身份，在网络应用前打开认证功能，对用户身份和使用权进行相应的认证工作，只有通过认证，用户才能有效地操作计算机网络，陌生用户将无法获得计算机网络操作权限，可以减少信息拦截或盗用的可能，可以设置高等级登录账号和密码长度，增强防火墙的防御能力，进一步增加计算机信息数据的可靠性。

2.3 及时更新病毒库

病毒的隐蔽性在提升，防火墙的技术也不断提升，计算机中存储着大量的数据，同时也会遇到各种类型病毒的感染，这给用户的数据安全带来严重的困扰。防火墙中的病毒库如果没有及时更新，一些新病毒是无法识别的，如果一台电脑被病毒入侵，整个企业的电脑和网络安全就会被破坏，甚至形成网络瘫痪会对企业发展造成严重的威胁，同时由于电脑网络结构具有开放性特征，容易遭遇病毒入侵，导致电脑内部数据外泄，影响用户个人权益。防火墙可以预防一些病毒但由于病毒形式的多样性，防火墙的保护和检测能力无法完全预防网络病毒，另外一些病毒有破坏性，会影响计算机网络，如果受到类似病毒的攻击，不仅电脑性能受到影响，整个内部网络都会受到攻击，导致网络堵塞不通。为了增强防火墙对病毒的防御能力，管理者要不断更新防火墙技术，提升防火墙的防护能力，最大程度地维持网络运行和安全，保护用户的信息和数据不被入侵，提高计算机网络的数据安全性。

参考文献:

[1]付俊芹.计算机网络安全中的防火墙技术应用研究 [J].电脑知识与技术,2018,14(24): 14-15.

[2]高鹤洋.关于计算机网络安全中防火墙技术的研究[J].中国新通信,2018,20(5): 202.

[3]何承.计算机网络安全中防火墙技术的有效运用分析[J].福建质量管理,2016(1): 171-172.