计算机网络信息安全中防火墙技术研究

罗荣艇　江志晃
广东培正学院　广东　广州　510830

摘　要：当前，计算机技术对人们生活、工作的影响已经显然可见，成为现代人们离不开的技术支撑。但是计算机的推广范围越来越大，其安全问题不得不引起高度重视。计算机网络促进了信息技术的创新和变革，逐步成熟的计算机网络技术，普及率越来越高，涉及的领域也愈发广泛，其不仅改变了人们的生活方式，也给生产带来了新的机遇和突破，有着较好的发展前景，但与此同时计算机网络安全问题越来越受关注，人们对网络信息安全的要求也逐渐提高，应当采取有效技术措施来加以防范，可充分发挥防火墙技术作用，保障计算机网络安全，避免信息泄漏，以防带来严重的经济损失和恶劣的社会影响，从而为计算机网络的长远发展创造良好的环境。本文就计算机网络信息安全中防火墙技术进行了详细的分析探讨。

关键词：防火墙技术；计算机网络；信息安全；应用分析

1 防火墙的概述

1.1 基本概念

防火墙是计算机信息安全技术的一种，是对个人网络以及企业信息安全的重要保护措施，防火墙的技术十分简单易操作，所以应用极为广泛，很多非技术人员的计算机上也会安装防火墙技术保护电脑信息安全。其特点就是不需要改变原有的互联网系统，同样可以进行系统检查，智能将系统流出的IP包过滤，并且将电脑外部引进的危险地址进行屏蔽。其实相较于其他计算机安全技术，防火墙无论从操作难度还是原理来看都十分简洁，相当于计算机中的闸门，用于对互联网来往地址的筛选和拦截工作，只有符合互联网安全才能通过防火墙技术，一旦发现危险讯号，防火墙会自动拦截，防火墙具有强大的过滤功能，具体表现为由外而内和由内而外两种形式。不仅如此，为了更好地进行网络保护，使计算机不被入侵，防火墙技术具备预防外来入侵的功能，不过防火墙的安装位置特殊，所以在一定程度上降低了信息传输速度，然而相较于计算机安全，对于信息技术的影响几乎可以忽略不计[1]。

1.2 功能用途

计算机网络构建的过程中，通过防火墙技术的应用，能够对系统内的数据包予以截取、分析与识别，以此有效对数据予以管理。当有存在安全隐患的数据流想要进入互联网时，防火墙会自动将其拦截，并判断该数据流是否安全，在确定信息安全后，随之进行启动或关闭等操作，从而对计算机网络数据的集中化管理，防止外界不良数据进入到系统内，提升了系统内部的安全性，有利于系统安全、稳定地运行。近年来，随着大数据时代的到来，使得计算机领域出现了更多有价值的数据，从而出现了越来越多计算机数据泄露的问题，大大增加了计算机网络信息安全问题的严峻性，如果安装防火墙，将会显著提升系统的安全性。另外，安装防火墙后，整个计算机网络具有更强的抵抗能力，不论是病毒的入侵，还是黑客的攻击，防火墙均会将其拦截下来，只有通过验证，才可将数据流放进来，以使计算机能够安全、稳定地运行。同时，当计算机被黑客、木马、病毒攻击后，防火墙还会第一时间向用户发送相应报告，以提升用户对安全问题的了解程度，使其能够快速做出应对。

2 计算机网络信息安全中防火墙技术的重要性

第一，对网络情况的实时监控。当下计算机网络技术得到了快速发展，同时与许多行业领域都建立极其紧密的联系，平时生活与工作中对计算机网络的依赖性越来越强，不管是办公、教学还是休闲娱乐等都需要应用到计算机网络，从而导致计算机网络发展面临较为复杂繁琐的环境，这时必须要构建切实可行的安全护盾，提高计算机网络的安全性，确保其能够稳定、高效运行。将防火墙技术应用到计算机网络当中，可以实现对网络情况的实时监控，加强对各个网络数据的判断，避免出现侵犯个人信息等不良现象发生，当识别到存在不安全因素时，可以在第一时间采用可行手段断开计算机与公共网络的交流渠道，确保用户计算机的安全性。当出现非法入侵以及外界干扰，防火墙技术也可以第一时间识别，及时使用有效的隔离措施防止非法入侵和外界干扰，为计算机网络安全提供良好保障[2]。

第二，避免网络信息被泄漏。在现代计算机网络快

速发展的背景下，网络中涵盖了形形色色的信息，假设一些重要信息被窃取或者泄漏，会对行业的稳定发展产生非常大的影响。所以，防火墙技术成为了确保计算机网络安全的关键举措，可以有效确保计算机网络数据的安全性。当下计算机网络已经与社会生产、人们生活等建立了十分紧密的联系，在为人们带来良好便利性的基础之上，也对计算机网络安全提出了更高的标准要求。将防火墙技术应用到计算机网络安全中，可以进一步强化网络信息的安全性，避免网络信息被泄漏，既可以实现对大众上网隐私空间的保护，也可以提高社会大众隐私安全性。科学使用防火墙技术可以有效防止网络信息被不良侵害与窃取，让使用者可以放心上网。总之，在计算机网络安全中引入防火墙技术，可以很好地防范盗取贩卖他人隐私信息现象的产生，可以为社会的和谐发展提供有效的保障。

3 计算机常见的安全问题

3.1 病毒、木马攻击

经济飞速发展推动了互联网技术的发展，使得计算机网络技术更加成熟与完善，对现代人类的生活与社会更好地发展提供了重要帮助。但与此同时，现代计算机领域还出现了越来越多的病毒与木马，在这些病毒与木马的作用下，对计算机网络造成巨大的冲击，轻者会出现数据泄露、丢失、降低系统运行速度等问题，严重情况下，还会导致系统完全瘫痪，对个人、企业或社会均造成严重影响。这是因为计算机病毒属于有害的数据代码，将其导入到计算机系统后，这些数据代码可对系统内原有数据或功能模块造成破坏，从而干扰系统的正常运行。以最为著名的“熊猫烧香”病毒为例，当计算机系统被感染后，不仅能够破坏exe、pif等文件，而且还能中止各种防病毒软件进程，并自动删除扩展名为gho的文件，使得所有.exe文件变成了熊猫举着三根香的模样。该病毒可通过多种途径传播，如邮件、网络地址等，正是由于其具备这一特点，加之病毒强度较高，使得病毒出现后的短短半个月就感染了数百万计算机用户，对计算机领域造成较大的破坏。对于网络风险管理而言，需要以网络安全危机为主要研究对象，并对造成主体危机问题的根本原因进行详细分析，并对问题产生的具体原因和发展过程做出详细的了解。在此之后，还需要针对研究主体进行专门的危机预防、风险处理和缓解风险等关键手段，运用更加有效的风险预防策略，保证网络数据信息的安全性。所以，现代计算机网络运行时，通常都会安装一些防病毒软件，以及时发现计算机内被侵入的病毒或木马，并立即将这些病毒清除，以提升计算机网络的安全性[3]。

3.2 数据传输问题

基于网络环境的复杂化发展，使得数据信息在传输、认证过程中面临着较多的隐患。首先，部分用户在使用计算机网络的过程中缺乏责任感与安全认知，不会有意识地借助防火墙对其网络环境进行防护，从而造成了数据的丢失抑或是篡改；其次，即使部分用户在使用计算机网络的过程中具备使用防火墙的观念，但却因为认知不足而使用了错误的杀毒软件抑或是防火墙设置，从而将计算机网络暴露在更为危险的环境中。除此之外，还存在部分用户未能定期清理计算机病毒、正确管理计算机网络的情况，对其自身上网体验、公共网络环境安全等间接造成了一定负面影响。

3.3 计算机信息安全性存疑

在信息化建设的过程中，大部分用户会使用内部局域网来促进信息数据间的相互交流、交换。而计算机网络作为办公与管理工作的重要平台，其往往储存着大量企业、机构的私密内部信息，一旦这部分材料在相互传递的过程中出现了丢失、泄露的问题便会给企业、机构、组织抑或是个人带来不可估量的经济损失。除此之外，部分不法分子也会凭借其愈发先进的网络技术主动攻击其他人的防火墙，去破坏软件与硬件系统来窃取相关企业、机构的机密信息以谋取钱财。由此需要相关工作人员加强对网络防火墙技术的关注，以预防重要信息的泄露。

4 防火墙技术在计算机网络信息安全中的应用

4.1 信息加密技术

用户在使用计算网络系统的过程中如若未能借助防火墙技术对其重要信息进行保护，便有可能出现信息数据丢失、隐私泄露等一系列问题。借助防火墙技术对信息数据加以保护，具体来讲就是利用信息加密技术对重要的文件数据、信息等进行加密防护，想要对相关文件进行下载、预览、转载、删除等操作，就一定要输入提前设置好的密钥。文件加密技术不仅是现阶段计算机网络用户最常用到的防火墙技术之一，同时也是保护信息文件不被恶意窃取、删改的最有效手段。基于防火墙技术中的信息加密技术主要包含了数据加密技术、认证技术、公钥技术等，可以依照用户的实际使用需求进行合理调配。以加密技术出发，其主要就是利用节点加密、端到端加密等方案，对数据信息进行逐层保护与筛选；以身份认证技术出发，其需要用户在进行数据传输、文件交换的情况下进行精准的身份认证，如若验证失败便无法继续操作，杜绝私密信息被盗取、被篡改的隐患；

以公钥技术出发，其能够利用数字签名的方式对文件进行正数管理，以待用户在进行信息验证的情况下，将用户的密钥、身份信息、文件信息等多项数据文件进行整合，利用数字签名完成对身份密钥的管理[4]。

4.2 对恶性入侵代码进行抵挡

用户在使用计算机网络系统的过程中，经常会遭遇到病毒的侵扰，在计算机网络中应用防火墙技术能够精准识别网络恶性入侵代码，对有风险的信息进行拦截，从根源上杜绝病毒的入侵。同时防火墙还能够在检测到病毒的情况下及时做出反应，第一时间向用户发布警报，帮助用户养成正确的计算机使用意识与概念，进而确保计算机网络安全能够得到保障。但需要注意的是，计算机网络使用者需要根据各类型病毒的发展情况、种类的不断更迭等做出反应，需依照实际需求有意识的升级入侵防护系统，关注数据的集中处理。针对计算机网络安全防护系统中出现的病毒、非法入侵代码等需要利用病毒引擎技术将其整合，并以此为基础建立起与之相对应的特征文件，以保障在后续的工作中能够通过对文件的扫描来分析代码的特征，及时检测并精准拦截不良隐患。

4.3 网络安全防护中的防火墙技术

第一，安全配置的防护方法。网络中的安全配置起着重要的作用，计算机用户一定要格外重视这点，根据自身的实际需求以及应用情况采取合适的安全配置。防火墙技术能够对各类信息进行分类，并逐类进行安全保护。对于网络中的重点区域，防火墙技术能够采取专业的防护，以保证计算机网络安全运行。为了能够有效的对重要的信息资源进行防护，就需要对这类信息采取高级别的防护，除了应用防火墙技术外，还应该对一些不良信息的IP地址进行跟踪，及时有效的将各类不良信息阻拦在计算机网络之外。第二，访问界面的防护方法。访问界面是计算机网络与用户的“第一接触面”，需要重点加强对这一方面的网络安全防护工作。现阶段，计算机网络系统中的子网络系统、软件程序等层出不穷，需要结合具体的防火墙技术对其进行监管，以调整软件程序与子系统的方法获取访问控制权限，将与子系统相对应的访问权限划分为内部局域网与外部网络，进而开启双重筛查的防护模式。以信息检索为例，防火墙会在用户进行操作过程中对相关信息进行归档与划分，并依据不同信息的性质与用处，判断是否需要进行重点防护[5]。第三，日志监控的防护方法。用户正常使用计算机网络的过程中，必然会产生一定的常规性数据，也就是系统日志，可以借助防火墙技术对网络计算机中的系统日志开展甄别与筛查，将带有危险性的信息进行过滤，从而确保计算机网络能够得到安全保障。但由于计算机运行过程中所产生的日志规模十分庞大，无法依靠纯人工的方式进行甄别与监控。因此需要借助防火墙及时对计算机网络日志进行事前防控、及时甄别、及时报警与及时处理，对计算机中的数据信息进行全面管理。在计算机网络遭受攻击后，利用防火墙对相关信息进行记录，并借助日志数据对防火墙进行完善，使得计算机网络的安全性得以保障。

结束语

总之，现代计算机使用过程中，很容易受到黑客、木马、病毒等方面的侵害，导致计算机数据出现泄露的问题，不仅会造成经济财产的损失，而且还危害社会的发展。所以，为了提升计算机网络信息的安全性，需要利用现代先进的科学手段，设计出良好的防火墙，以加强对外界不法信息流的检查与阻挡，以保证整个计算机网络安全、稳定地运行。

参考文献

[1]李洪亮.基于大数据的计算机网络安全防范对策[J].网络安全技术与应用,2022(6):161-163.

[2]于晓飞.新环境下的计算机网络信息安全及防火墙技术应用研究[J].职业，2019,03(28):122-123.

[3]吴红.新环境下的计算机网络信息安全及其防火墙技术应用分析[J].网络安全技术与应用,2022,02(07):14-16.

[4]邓杰.新环境下计算机网络信息安全及防火墙技术应用分析[J].科学与信息化，2021（17）:29.

[5]杜博杰，钟慧茹，葛运伟.计算机网络信息安全中防火墙技术的有效运用分析[J]中国新通信，2020（1）:154-155.