基于新环境下探讨计算机网络信息安全及其防火墙技术的应用

张坤

周口职业技术学院　河南　周口　466000

[摘　要]计算机技术的应用范围随着我国经济的发展不断的扩大和发展，在这个信息化的时代，各行各业都运用着计算机网络技术为自身的经营生产带来便利。这种发展的态势虽然对计算机网络技术的发展十分有利，但是由于计算机网络技术当前发展的局限性，还无法保证计算机网络信息的百分之百安全，信息的泄漏成了桎梏计算机网络技术科学应用的问题。本文以计算机防火墙技术出发，对防火墙的分类及目前网络信息安全出现的原因进行分析，并最后针对防火墙防护体系的建设提供合理化建议，以期为探究防火墙技术在计算机网络信息安全中的应用提供参考。

[关键词]计算机；网络信息；信息安全；防火墙

【DOI】10.12252/j.issn.2096-6261.2021.09.825

Based on the new environment，this paper discusses the computer network information security and the application of firewall technology

Abstract: The application scope of computer technology continues to expand and develop with the development of China's economy.In this information age, all walks of life use computer network technology to bring convenience to their own operation and production.Although this development trend is very beneficial to the development of computer network technology, due to the limitations of the current development of computer network technology, it is still unable to ensure the 100% security of computer network information.The leakage of information has become a problem that shackles the scientific application of computer network technology. Based on the computer firewall technology, this paper analyzes the classification of firewall and the causes of the current network information security, and finally provides reasonable suggestions for the construction of firewall protection system, in order to provide reference for exploring the application of firewall technology in computer network information security.

Key words: computer; Network information; Information security; firewall

引言

计算机网络技术作为当前人们工作生活中必不可少的工具，在信息技术的不断发展下逐渐成了世界各国研究的重点主题。目前，常见的信息防护系统就是计算机的防火墙技术，加强多计算机防火墙的维护与发展，就是加强对计算机网络信息的安全技术研究，在信息泄漏问题发生时，发挥计算机防火墙的作用，避免出现严重的经济损失，可以让计算机互联网技术更好的服务于人民群正。

1 计算机网络防火墙技术的含义

1.1数据包过滤型防火墙技术

计算机系统中数据包过滤型防火墙技术通过防火墙系统经由计算机打包处理不同类型的网络端口类型、网络地址以及不同网络数据，随后计算机系统对整合好的计算机数据进行筛选处理。这种计算机系统技术的实践模式较为简单且成本很低，这种技术经常用于网络路由器的防火墙安全防护中。但是如果计算机系统运用数据包过滤型防火墙技术，就需要在技术的实践中注意两个方面的问题。第一个方面是由于此类防火墙的运转及工作模式较为简单，万一被黑客攻破系统，可能会被利用对相关计算机设备中的网络信息带来负面影响，这种防火墙类型并不适用于机密性文件与数据的存储，第二个方面是数据包过滤型防火墙技术整理好的数据包中是包含了源地址、端口号等关键信息的，容易在传递时导致这些信息被泄漏而影响计算机网络信息的安全[1]。

1.2检测型防火墙技术

计算机的防火墙类型中的检测型防火墙技术是对网络活动中的系统行为进行读取，在网络的上传下载过程中进行实时的监测，并对有安全风险的操作进行实时的提醒与警告。这种防火墙技术属于网络型防火墙技术的深层次应用。在计算机系统中加装检测型的防火墙，可以对计算机操作过程中各类的网络信息进行筛查，确保每一个计算机的关键数据包在运行的过程中不被网络病毒等破坏条件所影响，可以有效降低计算机系统被外部威胁攻击的概率，保证计算机系统的安全运行[2]。

1.3代理服务型防火墙技术

计算机系统的代理服务型防火墙技术主要是针对计算机系统的数据包过滤和应用网关技术的不安全缺陷而进一步优化设计的一项计算机系统的安全技术。计算机系统的代理服务的作用是给计算机的内外系统制作一层保护层，让计算机外部系统数据只能发送到代理服务器。同时，计算机系统的代理服务器会对外部系统传输的各种数据包进行筛选和安全检测，若发现服务器中的数据包存在安全隐患，则会及时向主系统发出安全预警信号，并阻断此数据包中的数据进入到计算机的系统中，实现了计算机数据内外系统的隔离。

1.4分布式防火墙技术

计算机系统的分布式防火墙技术指的是网络与主机系统都布设防火墙系统，其中主机的防火墙安全防护措施是针对局域网，而网络防护的防火墙则主要针对计算机内外系统的防火墙网络安全实施相应的应对措施。从其他计算机防火墙的应用上来看，分布式防火墙相对于其他技术来说是对其他技术的进一步完善，分布式防火墙技术可以弥补传统防火墙对于应用环境和条件的限制，从源头上来防护用户的网络信息安全。

2 造成计算机网络信息安全问题的因素

2.1黑客攻击

自从互联网技术产生发展至今，黑客的存在一直是网络安全专家需要考虑的一大难题。黑客对计算机系统的攻击不仅可以一次性造成计算机系统瘫痪，更可以潜伏在系统漏斗中偷取系统数据。计算机网络系统防火墙的建立要深刻考虑黑客群体的技术特点与攻击目的，避免黑客攻击对计算机用户造成严重影响。因从事于黑客的多为计算机专业人士，其人数众多，成分复杂。这些黑客分布的范围十分广泛，也许用户在本国进行网络操作，黑客可以从国外对其进行网络攻击。一般情况下，普通计算机用户很难通过自身的计算机技术对黑客攻击的行为进行及时阻挡与提前预知的。这种情况下需要依靠计算机的防火墙技术对黑客的入侵进行阻挡。黑客攻击计算机系统的行为习惯具体可以分为两种：第一种是黑客的主动型攻击，黑客主动性攻击计算机网络系统主要是根据计算机网络系统特点决定攻击目标的方式，并且有针对性地对计算机网络系统造成攻击破坏，从而使得攻击的目标信息缺乏完整性甚至损坏，带有被窃取复制等情况。第二种是被动型的攻击，黑客被动型的攻击计算机系统则是黑客根据个人对特殊的目标数据的需求，对计算机网络系统的某些类型的信息进行截获或破解，来达到自身窃取信息的目的。这种被动型的攻击虽然不会对计算机网络系统的正常运行造成较大影响，甚至有时候并不会被用户发现。但会很容易长期潜伏在用户的系统中，使用户的数据长期被窃取。这些黑客的攻击行为在很大程度上使得计算机网络系统信息的安全受到严重威胁，需要引起技术人员的高度重视[4]。

2.2用户操作不当

由于目前互联网用户群体大，但文化水平程度普遍减低，导致用户操作的错误成为防火墙失效的主要原因。造成这种操作不当的情况的原因有以下几个方面，首先，当前国民的网络安全意识普遍较差，由于网络技术的不断普及与发展，越来越多的国民涌入了网络，用户数量始终处于增长的状态。但是由于大多数的网民并没有接受过正规的网络操作培训，特别是文化程度较低的民众和计算机水平较低的用户，对网络上出现的危险信息很容易信以为真掉入陷阱。其次。国内层出不穷的诈骗网站与钓鱼链接，让民众防不胜防，有时虽然是正常的操作却还是掉进了网络诈骗的陷阱中，误点、错点的行为也给予了不法分子可乘之机，虽然公安部门再三强调网络犯罪的类型及手法，但是由于很多信息的泄漏存在网页的诱导性行为，让信息的泄漏悄无声息的进行，导致防范苦难。最后，很多用户在设置计算机网络系统软件的用户密码时，过于依赖计算机网络系统操作页面的自我保护，用户没有自我防范的意识。很多的互联网用户在网络认证或者密码设置的过程中都设置十分简单被破解的密码，很容易被不法分子盗窃与利用，对自身和他人的财产信息安全都造成了严重影响。

2.3垃圾信息与信息截取

民众在日常的网络使用过程中难免会被来自网页、邮件、捆绑软件的垃圾信息所困扰。许多的不良互联网公司在各种网站与软件中添加插件或攻击性的病毒，来破解用户电脑的系统防御。这些垃圾的信息和广告会充斥在计算机运行的每个环节中，这种低成本的病毒式信息传播方式屡禁不止。用户一旦误点进这些网页与软件中，计算机系统内的个人数据很容易被这些软件中的病毒获取，严重影响了用户的上网体验与计算机安全的运行环境[5]。

3 计算机网络信息系统中防火墙技术防护作用的提升措施分析

3.1防火墙的防护体系的建立

用户在计算机使用的过程中由于计算机系统的安全漏洞导致使用的体验感下降。近年来，许多的互联网服务公司在计算机软件的生产设计中有意识的加入防火墙的技术，以此来配合用户主机的防火墙防护。这种网络型的计算机防火墙设计可以帮助整个计算机建立完善的整体防护体系，当代防火墙技术的建立一定要重视互联网的防护。防火墙系统应该根据不同病毒类型进行针对性设置和调整，使得计算机网络系统防火墙可以在整个系统运行的过程中进行全程的、全方位的实时监控，以此来保障系统运行的流畅性。

3.2网络信息安全防护系统的建立

从目前计算机网络安全技术的发展态势角度来看，防火墙技术如果单纯的按照传统的防火墙设计思路来构造是不够的。计算机防火墙技术是一个复杂的而且专业性很强的工作。如果在当下的互联网信息时代要保证计算机长期的平稳运行，需要在防火墙技术设计的基础之上创造和设计出更加完善的网络系统信息防护体系。计算机网络系统技术人员充分利用不同类型的网络安全防护技术的差异性优势，建立完整的有针对性的网络安全防护系统。通过建立健全信息防护系统的方式，既可以避免各项计算机网络系统网络安全防护技术的漏洞所造成的危害，又可以有针对性的对计算机安全进行把控。

3.3网络数据包过滤技术水平的提高

防火墙防护的过程中关键性的一步就是对网络数据包的筛查和过滤，这种技术可以在计算机网络系统应用层面自动识别虚假的钓鱼网址，并可以对计算机网络系统用户的部分操作进行全程的实时监控，从而避免计算机网络系统的用户误操作引起的计算机网络安全及信息泄漏的事件。在服务器、PC 端以及 Rule1、Rule2 C 语言技术的共同筛查与防护作用下，使计算机网络系统数据包得到高效的过滤处理，从而保证用户数据的安全。

结束语

在目前看来，互联网技术的存在与发展对人民的生活利大于弊，在全新的信息化时代当中，面对纷繁复杂的数据，计算机网络信息的安全性是关乎于民生的非常重要的内容。有效利用防火墙技术，维护与提高计算机整体的安全系统，可对网络的危险以及可疑的数据进行分析与过滤，保证计算机用户的操作体验。

参考文献

[1]刘艳.计算机网络信息安全及其防火墙技术应用[J].互联网周刊，2021（19）：43-45.

[2]夏文英.基于计算机网络信息安全中防火墙技术的应用研究[J].长江信息通信，2021，34（07）：116-118.

[3]耿宇.计算机网络信息安全中防火墙技术的应用研究[J].石河子科技，2021（02）：47-48.

[4]赵茂伸，姜维.计算机网络信息安全及其防火墙技术应用[J].通信电源技术，2021，38（03）：177-178.

[5]陈军.计算机网络信息安全及其防火墙技术应用研究[J].中国新通信，2020，22（19）：129-130.

作者简介:

张坤（女），周口职业技术学院。