工程管理
Journal of Project Management
第 6 卷◆第 4 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2737-4580(P) / 2737-4599(O)

网络信息安全中防火墙技术的应用研究

魏昌龙
中国电信武汉分公司

DOI:10.12238/jpm.v6i4.7927

[摘　要] 随着网络信息技术的飞速发展，互联网已经成为人们生活、工作不可或缺的一部分。然而，随着网络技术的不断进步，网络信息安全问题也日益凸显。网络信息安全是保障国家安全、社会稳定和经济发展的重要基石，也是确保公民个人权益不受侵犯的重要措施。合理有效地运用防火墙技术来保障网络信息安全至关重要，同时还需要加强网络信息安全中防火墙的防护措施，提高网络安全意识和技能。

[关键词] 网络信息安全；防火墙技术

Research on the application of firewall technology in network information security

Wei Changlong
China Telecom Wuhan Branch

[Abstract] With the rapid development of network information technology, the Internet has become an indispensable part of people's life and work.However, with the continuous progress of network technology, the problem of network information security has become increasingly prominent.Network information security is an important cornerstone for ensuring national security, social stability, and economic development, and is also an important measure to ensure that the rights and interests of individual citizens are not violated.It is very important to use firewall technology reasonably and effectively to ensure network information security, and it is also necessary to strengthen the protection measures of firewalls in network information security and improve network security awareness and skills.

[Key words] network information security; Firewall technology

引言

信息安全的保护方法多种多样，通过合理构造防火墙或者信息加密等有效措施，有利于保证系统的正常运行，确保系统的信息安全。

1、防火墙技术概述

防火墙技术是网络安全技术重要组成部分，它是一种隔离技术，有机结合各类用于安全管理与筛选的软件和硬件设备，同时帮助计算机网络在其内、外网之间构建一道相对隔绝的保护屏障，是保护用户资料与信息安全性的一种技术手段。防火墙技术的功能主要在于及时发现并处理计算机网络运行时面临的安全风险等问题，其中处理措施包括隔离与保护，同时可对计算机网络安全当中的各项操作实施记录与检测以确保计算机网络运行的安全性，保障用户资料与信息的完整性[1]。黑客能够通过非法控制和非法监视等手段获取用户相关信息，在获取用户信息的基础上，能够进入计算机系统，并对相关系统数据进行破坏，通常来说计算机病毒与计算机程序运行的相关基础资料息息相关。在计算机开启后，同样可能由于网络连锁传播的方式导致计算机死机等方面的问题，甚至出现网络瘫痪等极端情况。黑客病毒入侵的影响较大，危害范围较广，在实际安全防护中造成了巨大的影响和冲击，必须基于多种形式的统筹管控，避免由于网络下载不当等因素的干扰而导致黑客病毒入侵等方面的问题。实际上，在基于开放网络环境下，系统漏洞问题，不可避免在计算机网络信息技术发展速度不断加快的同时，尚未形成完全避免系统漏洞的相关机制。因此，必须

考虑到如何及时修复计算机系统漏洞，避免由于病毒入侵导致相关问题大范围传播。

2、大数据背景下网络安全面临的问题

2.1 用户网络安全意识缺乏

在大数据背景下，网络安全问题的解决不仅仅依赖于技术手段，而且更需要用户具备一定的网络安全意识。然而，当前许多用户对网络安全的重视程度不够，缺乏基本的网络安全意识和技能。这主要表现在以下几个方面：首先，许多用户对网络安全的重要性认识不足，缺乏主动防范网络攻击的意识。他们往往认为网络攻击离自己很远，不会对自己造成实质性的损失，因此忽视了网络安全的重要性。其次，许多用户在使用网络设备和软件时，缺乏基本的安全设置和使用习惯。例如，他们可能会使用简单的密码、不定期更新软件、随意点击不明链接等，这些都给网络攻击者提供了可乘之机。最后，许多用户在面对网络攻击时，缺乏正确的应对措施。他们往往无法判断网络攻击的性质和危害程度，也不知道如何采取有效的防范措施，这进一步加剧了网络安全问题。

2.2 计算机网络系统漏洞

计算机网络系统漏洞是导致大数据背景下网络安全问题的重要原因。随着计算机技术的不断发展，网络系统变得越来越复杂，系统中存在的漏洞也越来越多。这些漏洞可能来自于操作系统、数据库、网络设备等各个方面，成为黑客攻击的主要目标。在大数据背景下，网络系统的规模和复杂性进一步扩大，系统中的漏洞也随之增多。这些漏洞不仅增加了网络攻击的几率，也给网络安全防护带来了巨大的挑战。为了应对这一问题，我们需要加强对计算机网络系统漏洞的研究和分析，及时发现并修复系统中的漏洞，提高网络系统的安全性。

2.3 软件更新不及时

软件资源对计算机网络信息安全的影响更为直接，在软件更新不及时的情况下，很容易导致系统漏洞的出现。通常来说软件开发商能够结合用户的使用环境以及用户的使用反馈，及时对软件进行更新，并且修复相应的系统漏洞，这对保障网络信息安全可以起到一定的促进作用。但是，目前部分用户在计算机网络信息安全方面表现出的意识素养较为薄弱，在运用防火墙技术进行防护时缺乏主动性，大多只是基于系统本身的防护功能，做好信息安全保障，而忽略了对相关软件资源更新的尝试，最终影响了计算机网络信息安全的整体效果。

3、网络信息安全中防火墙技术的应用研究

3.1 加强网络秩序建立

首先，相关部门根据网络发展和运行过程中的实际状况，制订有针对性的管理机制，并对现行制度的缺陷进行全方位改进，充分发挥制度体系的约束和规范功能，监督网络使用者正常、有序的上网行为。其次，安全健康网络环境，不仅需要管理者充分发挥职责，还需要所有的网络使用者参与进来，只有增强网络使用者的安全意识和自我约束能力，才能使信息安全得到有效保障，同时进一步提高管理工作的质量和效率。最后，建立健全审查与奖惩机制，在增加审核次数和强度的基础上，对违反法律法规的行为作出有效的惩戒措施，对遵守网络秩序的行为给予奖励，激发公众的积极性和主动性，共同维护网络安全。

3.2 提高计算机远程网络通信的速率

一方面，企业应购置先进的计算机通信技术设备，引入先进的计算机软件，定期对计算机硬软件系统进行优化升级，提升网络信息通信的效率与稳定性，有效处理信息在传输中产生的信息畸变、信息延时等问题。另一方面，全方位升级改造通信生产企业经营模式，为计算机远程网络通信服务业提供优质的软硬件设施，确保网络信息通信的速率与质量。企业应构建一套更科学、更完善的计算机远程网络通信服务链条，完善计算机通信技术中的缺点，有效提升信息传输的稳定性与可靠性[2]。

3.3 联动技术构建

构建联动安全系统如图 1 所示。防火墙可以接受来自入侵检测的消息，从而实现两者之间的交互，同时防火墙可以配置和监测入侵检测，实现构建网络安全的目的。防火墙可以处理入侵检测检测到的各种攻击并采取相应的措施，二者存在互补性，防火墙是一种被动防御手段，入侵检测是一种主动的防御手段，它可以识别防火墙不能识别的一些恶意攻击。入侵检测可以修改防火墙的控制规则，假如受到攻击，不用人们去改写规则，而由入侵检测自动去重新配置规则从而阻断来自攻击者的进一步的破坏，补充了防火墙自身的缺点。另一方面，防火墙又可以补充入侵检测自身防护机制的不足，入侵检测不能很有效的阻止网络中的恶意攻击，但和防火墙进行联动，可以要求防火墙来完成访问控制，提升入侵检测本身的安全性。

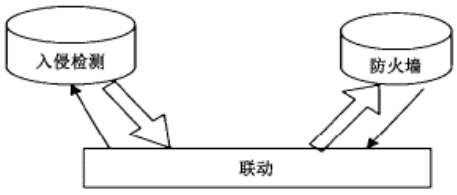

图 1　联动技术

3.4 配置访问措施

结合计算机的具体业务场景设置相对应的网络信息防火墙，能够有效地提升信息内容传送过程中的安全管理水平，为避免出现信息泄漏等安全风险提供相应支持。应用配置访问技术，需要考虑到防火墙技术参数规范，能够从监测系统的角度着手对操作系统层面的漏洞进行分析，同时基于系统软件和防火墙更新带来的影响，促进系统漏洞问题得到有效控制和解决。配备　地址环节，需要考虑到网络数据的具体种类在配置中能够考虑到网络信息传送的安全风险，同时基于防火墙技术做好配置访问，以提高计算机网络活动的安全性。

3.5 学会进行数据备份

数据备份是计算机网络用户在数据保存方面的优良习惯，能够让数据丢失的风险降到最低。但就目前而言，只有部分计算机网络用户有数据备份的习惯，有关数据备份方面的科普宣传工作，仍然需要得到进一步的推进。在日常的计算机网络使用过程中，要及时对重要核心数据进行备份。当计算机遭遇人为入侵，并且黑客已经对关键数据进行了大肆破坏，计算机网络用户可通过备份数据进行必要的数据恢复。即便计算机在使用过程中并未出现人为入侵方面的问题，计算机网络也很可能会在非正常情况下出现崩溃现象或者遭遇一些非正常断电事件，在这种情况下，容易出现数据遗失的问题。因此，计算机网络用户需要养成数据备份的习惯，及时完成数据备份[3]。

3.6 网络安全防护策略

在信息化建设过程中，常见的网络安全风险包括黑客攻击、病毒感染、数据泄露和勒索软件等。黑客通过端口扫描、SQL 注入和 DDOS 攻击等方式进入系统，制造混乱或窃取机密信息。病毒和勒索软件在系统中传播加密文件，导致系统瘫痪或数据丢失。数据泄露则因为缺乏加密保护或权限控制而发生泄露用户个人隐私或公司重要信息的问题。针对上述网络安全风险，黑客和恶意用户采用多种攻击手段，包括网络钓鱼、社会工程、恶意代码和漏洞利用等。网络钓鱼通过仿冒网站或虚假邮件诱导用户提供个人信息；社会工程利用心理学手段获取重要信息；恶意代码植入正常系统中，从内部破坏系统；漏洞利用则是利用系统中的漏洞入侵系统。为了有效应对网络安全风险和攻击手段，信息化建设中应建立安全防护体系，包含安全防火墙、入侵检测系统和安全监控等设备，监控和防范网络入侵。对敏感数据进行加密处理，保护数据存储和传输过程中的安全。定期对系统和应用程序进行漏洞扫描和修复，及时堵塞系统漏洞。加强员工网络安全意识培训，防止点击恶意邮件或网页造成安全事件。制定综合的网络安全防护政策，采取多层次的安全防护措施，加强网络安全意识的培训，信息化建设能够更好地保障系统的安全性，提高网络安全防护的能力，确保信息系统的稳定运行和数据的安全保护。

3.7 在网络系统日志的应用

计算机网络在使用过程中会产生相关的系统日志，通过防火墙技术的应用，能够及时有效地发现计算机网络系统日志可能存在的病毒，然后根据病毒的种类和特征，采取及时有效防治措施。防火墙技术对网络系统日志中存在的异常处理不到位，也会对计算机网络系统中的相关数据信息进行全过程的跟踪监控，避免在后续使用过程中出现问题，保护计算机网络信息的安全。防火墙技术在计算机网络系统日志中的应用，能够有效节省人力物力，并且对计算机网络运行效率的提升也具有非常重要的作用。尤其是防火墙技术在网络信息数据的监管和储存方面具有明显的优势和特征，能够严格按照事前预防，事中监控和事后清理的原则，对计算机系统日志进行有效监控，使得计算机网络系统在使用过程中产生的大量数据信息都能够得到一定的保护，为计算机网络信息安全奠定良好的基础。

3.8 做好计算机硬件设备的维护

要进一步提高网络信息的安全水平，在开展安全防护工作时，也要做好硬件设备的维护工作。工作人员要定期对当前的计算机硬件设备进行检查和维护工作，只有确保硬件设备的正常运转，才能保证网络运行的有序性，才能保证网络信息的安全。计算机硬件的安全性，直接关系着网络信息储存的安全性，如果计算机硬件出现了故障或者问题，将会直接威胁到计算机储存信息的安全性。因此，作为技术人员，要定期对计算机硬件设备进行全面的检查，深入分析当前的网络运行情况，一旦发现异常情况，则要做好故障检修工作，保证各项设备的正常使用，确保网络的正常运行。

3.9 防火墙技术应用

在网络系统日志中的应用计算机网络在使用过程中会通过防火墙技术的应用产生相关的系统日志，能够及时有效地发现计算机网络系统日志可能存在的病毒，然后根据病毒的种类和特征，采取及时有效防治措施。防火墙技术对网络系统日志中存在的异常处理不到位，也会对计算机网络系统中的相关数据信息进行全过程的跟踪监控，避免在后续使用过程中出现问题，保护计算机网络信息的安全。防火墙技术在计算机网络系统日志中的应用，能够有效节省人力物力，并且对计算机网络运行效率的提升也具有非常重要的作用。尤其是防火墙技术在网络信息数据的监管和储存方面具有明显的优势和特征，能够严格按照事前预防，事中监控和事后清理的原则，对计算机系统日志进行有效监控，使得计算机网络系统在使用过程中产生的大量数据信息都能够得到一定的保护，为计算机网络信息安全奠定良好的基础。

结束语

总之，防火墙技术在网络信息安全措施中扮演着至关重要的角色。通过使用防火墙，组织或个人可以保护其网络免受未经授权的访问、数据泄露和恶意软件的攻击。在进行防火墙配置时，首先，要选择合适的防火墙设备，确保其性能满足网络安全的需求。其次，要根据实际需要配置安全规则，明确允许和拒绝的流量类型、来源和目标地址等。此外，还要对防火墙进行定期的日志记录和监控，及时发现和处理潜在的安全威胁和攻击行为。

[参考文献]

[1]贾燕.防火墙技术在计算机网络安全中的应用[J].电子技术与软件工程，2019，（23）：193-194.

[2]咎家玮.试论新时期计算机网络信息安全及防火墙技术应用研究[J].通信与信息技术，2019，（06）：41-43.

[3]陈勇.计算机网络安全中的防火墙技术应用研究[J].计算机产品与流通，2019，（10）：41.