防火墙技术在计算机网络安全中的应用

康　惠

（山东现代学院，山东 济南 250104）

摘　要　在信息时代，计算机网络技术为国民日常的生活、工作和学习提供了诸多便利，然而，也伴随着网络病毒、黑客攻击和信息泄露问题。对此，要注重改善网络安全功能，充分发挥防火墙技术在计算机网络安全中的应用方案，提高加密等级，设置安全访问，促进防火墙技术和人工智能技术的紧密融合，定期为计算机杀毒。本文将简单分析防火墙技术在计算机网络安全中的应用方案，希望能为提高计算机网络安全运行质量提供参考。

关键词　防火墙技术；计算机网络安全；应用方案

中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1007-0745(2023)06-0019-03

计算机网络技术不断发展，网络在运行过程中也面临着各方面的隐患，因此，必须全面优化网络安全管理策略，充分发挥防火墙技术的作用，不断加强计算机网络系统安全建设。本文将简单分析计算机网络安全隐患，并从设置网络安全防火墙，发挥智能化防火墙技术功能，提高防火墙安全加密等级，优化计算机网络安全功能，做好计算机网络日常维护工作等五个方面综合探讨解决对策。

1 计算机网络安全隐患

1.1 网络病毒

在互联网时代，网络病毒各种各样，常见病毒有勒索病毒、木马病毒、宏病毒、蠕虫病毒、垃圾邮件等，大多数病毒均具有隐蔽性，在安全等级较低的网站和下载软件中均有附带，一旦用户浏览过有病毒的网站，或者下载的软件有捆绑病毒，就会导致电脑被入侵[1]。网络病毒传播速度很快，会导致计算机网络运行速度骤降，电脑蓝屏，甚至会使整个网络系统瘫痪。因此，必须严加防御，定期为电脑杀毒。

1.2 系统漏洞

虽然计算机网络技术在不断发展，系统日益完善，安全等级在持续提高，然而，网络系统本身也存在漏洞，用户所使用的Windows系统难免会受到攻击，因此，要不断优化网络系统，定期升级，及时修复高危漏洞。

1.3 黑客入侵

从法律的角度来讲，黑客是熟练掌握计算机技术应用技能的犯罪分子，他们会通过非法链接、访问和病毒入侵其他计算机，窃取企业机密、政府文件信息和用户个人信息，黑客攻击的范围也很广泛，企业内部网、政府官网、医院内部网络和用户个人计算机系统都很有可能被黑客入侵，因而，必须严加防范。

1.4 网络诈骗

科技发展迅速，为广大民众的生活带来了许多便利，却也伴随着各种诈骗方式，严重威胁民众的生命财产安全，网络诈骗层出不穷，不少不法分子会利用网络技术平台进行诈骗，例如冒充淘宝客服、网络警察、快递、网络兼职管理人员进行诈骗。也有许多不法分子会利用聊天工具（像微信、YY、探探）进行诈骗，发布虚拟信息，以投资项目、参加文化栏目活动、医疗服务等为名实施诈骗[2]。因为计算机网络平台具有开放性和共享性，所以很难对网络虚假信息和诈骗进行全面禁止，一方面，国家一直在依法打击网络诈骗；另一方面，要及时清除虚假诈骗信息，做好宣传教育工作，提醒广大人民群众警惕网络诈骗，保护好个人信息和财产。

1.5 恶意攻击

据调查了解，网络恶意攻击大致可分为三种：

第一，非法攻击用户的IP地址。如今国家非常重视加强网络IP地址管理，所有电脑在接入网络后，会配置相应的互联协议地址（英文全称Internet Protocol，英文简称IP），以此满足网络系统不同的应用需求。然而，网络连接和访问也是非法攻击的常用手段。例如不法分子会运用IP跟踪技术执行Ping命令，通过空会话监控和连接目标IP，也会利用IP漏洞来非法获取对计算机管理的控制权，窃取机密信息，严重威胁网络安全。另外，不法分子会运用虚假IP和隐藏IP来“欺

骗”主机系统安全识别，然后，嵌入计算机网络系统内，运用不同方式对网络系统实施攻击，如果计算机网络防御系统存在漏洞，就会导致各分支系统被潜入非法程序和命令，严重损坏网络设备，导致信息被篡改和窃取。

第二，端口攻击。对于计算机网络设备来说，端口起到了连接计算机和外界的作用，能够实现网络资源共享，提供远程服务，具备邮件发送与接收功能，全面优化网络应用服务。然而，端口也是不法分子进行网络攻击的必经之路，不法分子会利用端口功能和不同端口号采取不尽相同的攻击手段。据统计，在传输控制协议端口（英文全称Transmission Control Protocol，简称TCP）被攻击的频率最高，许多网络用户对此感到恐惧。虽然国家网络安全管理部门建立了安全防火墙，对端口攻击有一定的作用，却无法消除这种威胁，防火墙自身覆盖范围有限，无法弥补所有系统漏洞，很难抵挡大量的非法数据包攻击端口。

第三，拒绝服务攻击。不法分子采用的这种网络攻击手段的危害性非常大，会导致主机瘫痪，许多服务请求被拒绝，资源被耗尽。不法分子经常会通过当前网络协议中的漏洞，设置虚假IP地址持续提出非法请求，也会发送大量的非法数据包，对主机实施持续性和集中性攻击，导致计算机和网络服务器之间的连接与交流被迫中止，电脑内存和中央处理器（英文全称Central Processing Unit，简称CPU）就要面临超大负荷的工作量，致使计算机系统功能最终出现紊乱和崩溃现象，电脑因此死机，无法正常开启和运行[3]。所有拒绝服务的攻击形式都存在这样的特征——其攻击对象非常广泛，非法请求和数据包繁多，其攻击制约也比较少，会导致网络服务功能和主机的运行受到严重影响。

2 防火墙技术在计算机网络安全中的应用方案

2.1 设置安全防火墙

抵御计算机网络系统风险，全面优化网络系统安全管理策略，建立安全、文明、绿色网络环境，首先要设置好安全防火墙[4]。一般来讲，在防火墙设置工作中，需要建立智能化防火墙，将网络分为内网和外网，防火墙所保护的网络就属于内网，防火墙会为内网设置安全账户，禁止非法登录。外网在访问内网之前，必须经过验证，验证合格方可允许访问，这样可以避免内网受到非法攻击，做好信息保护工作。

其次，要注意不断健全防火墙识别机制，以便于准确判断潜藏性病毒，及时防御来自外网的攻击，进一步加强计算机网络系统安全建设。

2.2 发挥智能化防火墙技术功能

提高防火墙技术应用效果，应注重促进人工智能和防火墙技术的紧密结合，以此形成智能化防火墙技术体系，进一步提高计算机网络安全防御质量。

首先，应发挥人工智能神经网络技术的作用，在计算机网络系统中配置该技术能够有效改善网络系统运行功能，提高计算机网络安全等级。

从技术组合来看，人工智能神经网络技术是根据人的脑神经结构所构建的一种技术。从本质上讲，该技术属于一种规模比较大的并行分布处理器，在神经网络中均有分布，同时，在具备不同的信息处理单元模块均有深度融合。发挥人工智能神经网络技术的功能，不仅可以维护单一化神经模块的安全独立运行，而且能够促进单个模块之间的互相配合，实现功能整合优化，提高计算机应用软件的安全性能，确保网络系统的安全、高效运行。

从应用效果来看，神经模块如果处于整体运行状态下，其网速更加流畅，能够为广大用户提供更为良好的应用体验，网络环境更安全，可以帮助用户运用计算机提高日常工作效率。

其次，运用人工智能神经网络技术可以对软件所涉及的各种入侵信息实施迅速检测，如果发现入侵软件存在危险因素，就会立刻迅速识别，及时拦截风险，发出预警信息，自动查杀已经通过防火墙的网络病毒。目前，不少企业组织和地方政府会运用神经网络技术为来改善本单位计算机软件系统结构，进一步优化安全防护功能，在处理海量信息的过程中，运用人工智能神经网络技术不仅可以有效提高信息的安全程度，而且能够使计算机网络安全知识的储备量得以增加，预测后期有可能面临的风险问题，运用数字模型分析各种网络风险，自动提出应对方案。

2.3 提高防火墙安全加密等级

加强计算机网络安全管理建设，避免网络系统受到非法攻击，必须重视提高防火墙安全加密技术。在当前网络平台中，所有信息的存在基础是二进制。就拿基础字符来讲，计算机系统会自动将用户所输入的字符运用ASCII编码转换成数字语言。如果是一串有特殊意义的数字，就需要采用特定的安全加密算法，

从而全面做好信息安全保护工作，避免信息被恶意篡改和窃取。目前，计算机网络系统加密技术大多运用了数学模型，不法分子一般很难破解，这样能够大幅度提高网络安全等级。当前计算机网络系统加密技术常用的模型有两种：一种是空间实体模型，另一种是拓扑关系模型。后者主要是 Polyvrt 结构，其记录内容为链信息，在多个不同对象中，可以共用运用同样的节点，这样能够节约存储空间。然而，拓扑关系模型有显著的不足之处——该模型结构组合复杂，难以做好数据编辑与维护工作。对此，可以运用空间实体模型来弥补这些缺陷，这种模型的公共节点时常会重复出现，即使修改模型内的某个对象，也不会影响其他对象，能够有效增强空间数据的可维护性。在计算机网络安全管理模型构建工作中，可以对这两种数据模型的优点进行结合，这样能够设计出节省存储空间且便于维护和编辑的数学模型。

总而言之，满足计算机网络系统安全运行需求，必须注重提升系统网络内部数据保密等级，在设置防火墙的同时引入先进的保密技术，以便于为网络系统设置完善的防护层。另外，要对访问密码进行定期更改，以此维护内部存储数据信息安全管理。在数据传输过程中，有时受网络病毒的影响，可能会出现拦截现象，为了避免这种问题，需要构建完善的信息传递线路保护机制，采用信息加密方式优化数据保护层，避免不法分子恶意攻击系统，不断加强计算机网络系统数据保密等级，为计算机网络安全管理工作创建良好的环境。

2.4 优化计算机网络安全功能

优化计算机网络安全功能，需要在设置防火墙的基础上充分发挥 TCP/UDP 端口的安全扫描防御作用。对于计算机网络系统来说，TCP/UDP 端口扫描工作是处理计算机网络安全问题的关键环节。通常，在通过执行 TCP/UDP 端口安全扫描工作期间，必须仔细检查该端口向计算机结构端口所发送的链接请求，与此同时，要严加审查来自外界的链接请求，对计算机系统常用端口的链接请求进行统一审计，一旦发现存在异常链接或者危险链接，就要立刻启用计算机安全防火墙，对这些链接迅速进行断开处理，并对存在攻击性的 IP 地址与 MAC 地址进行严格审查 [5]。

另外，如果计算机网络系统受到分布式攻击或者综合攻击，就必须通过模糊统计来防御和阻隔这些非法攻击进，同时借助网络拓扑结构维护网络安全运行，全面监测计算机网络系统运行状态，及时预防非法入侵问题。

2.5 做好计算机网络日常维护工作

优化计算机网络安全维护策略，加强网络系统安全建设：

首先，要做好计算机网络日常维护工作，对计算机硬件设备实施定期维护，按时检查计算机网卡与防火墙的功能，查看路由器、集线器和交换机等硬件设施是否能正常运转，与此同时，要对计算机硬盘、显示器和电脑内存的运行状态进行全面了解，查看是否存在异常问题，并及时进行修复和维护。

其次，需要对网络运行的畅通性实施定期检查，判断服务器的工作正常与否，全面掌握浏览访问状况，执行检查网络服务协议的运行情况，定期修复防火墙的漏洞。

最后，要重视增强计算机网络故障的处理能力。当前计算机网络故障类型具有多样化特征，其诱因往往是多方面的，故障的排查与维修工作需要相应的过程，为了降低故障带来的损失，维护网络用户的信息财产安全，必须重视增强计算机网络故障处理能力，设置代理防火墙（代理防火墙能够加强内部网络安全访问管理工作），构建故障预测模型，配置内部修复设备与程序，以此便于及时修复，保护好内部网络数据。

3 结语

综上所述，全面优化计算机网络安全防御系统，提高防火墙技术在计算机网络安全中的应用质量，需要设置好安全防火墙，构建智能化防火墙技术体系，不断优化计算机网络安全管理功能，提高网络安全加密等级，定期修复防火墙的漏洞。

参考文献：

[1] 高立静 . 防火墙技术在计算机网络安全中的应用 [J]. 网络安全技术与应用 ,2022(06):11-12.
[2] 王文霞 . 计算机网络安全中防火墙技术的应用探索 [J]. 网络安全技术与应用 ,2022(06):13-14.
[3] 王钦国 . 计算机网络安全与防火墙技术分析 [J]. 集成电路应用 ,2022,39(04):162-163.
[4] 蒙飞 , 孙华林 . 基于计算机网络技术的计算机网络信息安全及其防护策略 [J]. 计算机产品与流通 ,2019(09): 57-58.
[5] 向立莉 . 计算机网络信息安全及防护策略探讨 [J]. 数字通信世界 ,2021(02):34-36.