计算机网络信息安全中的防火墙技术应用策略分析

徐春一

（佳木斯大学附属第一医院，黑龙江 佳木斯 154003）

摘要：随着大数据、互联网技术的飞速发展，对于数据的安全保护也成了一个首要的问题。基于此问题，本文深入研究了计算机网络信息安全的种类：黑客、病毒、恶意程序以及计算机网络信息安全中的防火墙技术应用策略：智能网络安全防护体系、智能防火墙、防火墙技术多样化处理、防火墙联动技术、防火墙联动技术等方式，更好地服务于计算机的网络信息安全。

关键词：计算机网络信息安全；防火墙技术；策略分析

引言：中华人民共和国国务院令网络平台服务提供者应当通过平台规则或者合同等明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促第三方产品和服务提供者加强网络数据安全管理。预装应用程序的智能终端等设备生产者，适用前款规定。第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展网络数据处理活动，对用户造成损害的，网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。国家鼓励保险公司开发网络数据损害赔偿责任险种，鼓励网络平台服务提供者、预装应用程序的智能终端提供者。应该根据国家的政策性文件，进行计算机网络信息安全中的防火墙技术应用的使用，使其更好地能够防御外来的黑客、病毒以及恶意程序，保证数据的安全。

一、威胁计算机网络信息安全的种类

（一）病毒

电脑病毒的学术名称为计算机病毒，就是一组精心设计的计算机指令或程序代码感染计算机里面的软件、扰乱计算机的功能、损坏计算机内的数据，使计算机不能够正常地运行。在这个数据资源共享的时代下，病毒一旦进入网络资源库或通信通道内，就会展现出极强破坏性，对计算机中的各种数据发起攻击。这些病毒的种类是多种多样的，如：信息窃取、程序篡改及数据库损坏等，它们会如同网络世界中的隐形刺客，让使用人员在短时间内造成重大损失。

（二）黑客

黑客一词出现在 1976 年是随着计算机的出现而产生的，并随着互联网等技术的发展迅速席卷全球。黑客活动与计算机病毒的破坏力虽在某些方面有相似之处，但两者还有一定的区别。黑客往往会有一定的目标性和针对性，利用自己高超的技术手段，将矛头对准特定的企业、组织或个人发起攻击，窃取公司内的宝贵资源，进行篡改数据，给受害方带来难以估量的损失，例如商业黑客窃取机密文档，或是间谍黑客盗取军事情报等。

（三）恶意程序

恶意程序是一种介于标准应用程序与病毒之间的特殊软件实体，它们表面上执行着正常的功能，然而却暗中执行一系列非预期的、异常的指令，比如擅自安装其他程序或执行特定操作。这类程序的破坏力呈现出高度的不确定性，多数情况下并不直接针对数据库进行信息复制或资源窃取，但部分恶意程序会持续地对计算机系统发起无差别的攻击，导致数据库崩溃、系统功能失效等严重后果。尤为值得关注的是，恶意程序往往具备高超的伪装技巧，这使得多数安全防护软件难以直接识别其真实面目。例如，近年来备受瞩目的小黑记事本案例，就是一个典型的恶意程序伪装成普通工作软件的实例。一旦用户下载并安装了这类伪装后的程序，它不仅会自行下载并安装各类附加的程序和软件，其中甚至可能包含具有破坏性的病毒程序，从而极大地增加了网络安全事件的风险。

二、计算机网络信息安全中的防火墙技术应用策略

（一）医院神经网络防火墙：构建高效智能网络安全防护体系

随着数字化办公的深入发展，网络信息安全已经成为医院运营中不可忽视的关键环节，为了保证医院中的数据（患者的信息、患者的病历、医生的资料）等不被非法地访问以及获取，医院可通过一个基于神经网络工作模式来构建先进的防火墙系统，以提升医院的网络信息安全防护能力。医院可利用神经网络的多节点同步感知特性，将医院的每一台计算机（估计为 1000 台）都视为一个独立的“感知节点”，让其不仅负责日常的数据处理任务，还承担着监控网络环境的重任，将周围网络流量的细微变化（数据的来源、目的地、传输内容以及传输速度），也就是存在任何异常的、潜在的危险行为都能被迅速地捕捉到。当黑客通过恶意软件、钓鱼攻击或暴力破解等入侵企业网络的时候，这些节点都会感知到，并能够根据异常的数据流量激增、未经授权的访问尝试或是数据传输中的加密异常等影响来收集详细的信息（入侵者的 IP 地址、攻击类型、攻击时间），将收集到的详细信息通过网络发送给中央控制中心，让中央控制中心分析这个感知节点的数据报告，当分析结果显示某个尝试访问网络的实体（无论是程序、访问者还是文件包）是安全的，控制中心会立即授权其访问权限，确保正常的业务操作不受影响，但是，一旦检测是有非法入侵行为，控制中心会立即触发拦截机制，组织进一步的操作的同时记录下攻击的细节，以便日后的安全分析和追溯。医院通过将神经网络工作模式与防火墙技术相结合，成功构建了一个高效、智能且适应性强的网络安全防护体系，不仅极大地提升了医院对网络威胁的感知和响应速度，还有效降低了信息安全事故的风险，为医院的数字化转型和持续发展提供了坚实的安全保障。

（二）智能防火墙技术：保障医院网络安全的高效新策略

面对日益复杂多变的网络环境威胁，传统的防火墙技术已经很难满足当前的安全需求，因此需要引进先进的技术和算法，不断优化防火墙的识别能力，防火墙已经成为保障计算机网络信息

安全的重要手段。一方面：这要求防火墙系统能够通过深度包检测、行为分析、流量模式识别等多种技术手段，实时、全面地监控网络流量，对网络中的数据包进行细微的分析。其中深度包检测是用于检查数据包的内容，识别并阻止携带恶意代码或敏感信息的传输；行为分析则通过观察网络行为模式，来访问那些没有经过授权但尝试访问，数据泄露痕迹等可疑活动；流量识别则是从历史数据中学习正常网络流量的特征，准确来区分正常流量与异常流量。另一方面：还可通过训练模型，防火墙能够学习并理解网络流量的正常行为模式，自动调整安全策略，以应对新型威胁，提升防火墙的自适应性和智能化水平。例如：医院可利用深度学习算法来分析网络流量的时间序列数据，识别出潜在的攻击模式（包含一些之前出现过的与之前没有出现过的攻击模式），来优化威胁计算机的情报库，提升对已知威胁预测的同时，还能够提高威胁的识别精度。除了上面两个方面，医院的防火墙技术应该能够不断适应变化的网络环境，支持多种协议、应用和服务的同时还能够保持高性能和低延迟。引入先进技术、提升智能化水平、增强灵活性和可扩展性的方式，可以使计算机的防火墙技术更加高效、智能，从而为医院的网络安全保驾护航。

（三）防火墙技术多样化处理：精细控制医院网络安全

防火墙技术的多样化处理方法主要体现在其丰富的功能和应用策略上。首先，防火墙具备访问控制功能，能够依据设定的规则限制或允许特定类型的网络流量通过，实现对进出网络的数据包的精细控制，有效阻止未经授权的访问和攻击。这包括端口基规则，如只允许特定的通信端口（如 80 端口的 HTTP 和 443 端口的 HTTPS）进出，确保只有授权的数据能够通行；IP 地址过滤，通过设置规则限制或允许特定 IP 地址的数据通信，有效过滤掉潜在威胁；协议基规则，选择只让某些特定协议的数据通过，如 TCP 协议，而拦截其他潜在风险协议；时间基规则，根据时间来动态调整访问权限，确保网络安全与时间动态匹配。首先，医院可确定防火墙的部署位置、访问控制列表（ACL）的设置以及各种安全标准的设定（企业网络和外部网络的接口），运用 ACL 详细对特定 IP 地址、端口、协议和服务的限制。其次，在实施的时候，防火墙应该建立配套的管理制度，确保防火墙的配套符合安全策略，定期地进行升级和更新，保证最新的安全功能和补丁。随着技术的不断进步和攻击手段的日益复杂，防火墙技术也在不断发展和完善，以应对不断升级的安全挑战，更好地运用医院的防火墙技术。

（四）防火墙联动技术：构建多维度网络安全防御体系

第一：防火墙与入侵检测 / 防御系统的联动

防火墙可与入侵检测系统（IDS）和入侵防御系统（IPS）进行联动，IDS 能够实时监控网络流量，通过分析数据包的内容和行为模式，识别并报告潜在的安全威胁。而 IPS 则更进一步，能够主动阻断检测到的威胁。通过将防火墙与 IDS/IPS 联动，可以实现对网络流量的双重监测和防御。例如，当 IDS 检测到某个 IP 地址正在尝试进行 DDoS 攻击或 SQL 注入攻击时，可以立即通知防火墙将该 IP 地址加入黑名单，从而阻止其进一步的攻击行为，以提高安全响应的及时性和准确性，增强防火墙的防御能力，使其能够应对更复杂的网络攻击。

第二：防火墙与终端安全管理的联动

终端作为网络中的关键节点，其安全性直接关系到整个网络系统的稳定。当终端设备出现异常行为或者行为遭受攻击的时候，终端管理系统不仅可以及时地发现还能够进行报告，以实现对这些异常行为的快速响应。例如：医院的终端系统检测到某个终端设备正在尝试访问恶意网站或下载恶意软件时，可以立即通知防火墙对该终端设备的网络访问进行限制或阻断，防止这个不好的带来进行扩散和感染，保护内部网络不会受到外部的威胁与侵害。

第三：防火墙与大数据安全的联动

大数据安全技术则通过收集和分析海量的网络数据，发现潜在的安全威胁和异常行为可与防火墙的联动，实现对网络流量的智能分析和防御。发现 IP 地址的访问模式与已知模型中的行为模式是类似的，就可以通知防火墙对其进行监控与限制，多层次、立体化的安全防护体系，可以实现对网络流量的全面监控、智能分析和快速响应。

（五）强化医院网络安全意识：保障医疗服务稳定运行

在现如今数字化医疗飞速发展的情况下，医院内不仅承载着庞大的医疗数据存储与传输任务，还涉及对患者病历、诊疗记录、财务信息及个人身份资料这些信息的处理，可通过下列措施，增强医院用户的安全意识和防范能力，保证医院安全和患者信息隐私及保障医疗服务稳定运行。首先，医院可对医护人员、行政人员、IT 技术人员开展定期且系统的网络安全知识培训（网络安全基础知识、常见网络攻击手段及其防范措施、数据保护法律法规、密码安全策略、安全软件及硬件的使用规范），让每一位员工都能深刻理解网络安全的重要性，并掌握基本的安全操作技能。其次，医院可举行网络安全宣传栏、发布网络安全简报等活动的同时还利用医院内部通讯平台推送网络安全小贴士等，使医院内部的人员可以在关注网络安全的良好氛围中，进行不断地学习，形成“人人讲安全、事事为安全”的良好风尚。加强医院网络安全意识教育和培训，是一项系统工程，需要医院从上至下、全员参与，通过持续的教育引导、制度建设、技术投入和文化培育，形成强大的网络安全防护网，确保医院在数字化转型的道路上稳健前行，为患者提供更加安全、高效的医疗服务。

三、结束语

本文通过多种策略的应用，旨在促进医院系统的智能化，使医院的系统在受到攻击的时候可以进行防护，更好地提高医院的防护系统，使医院可以更好地发展，保护病人的隐私。防火墙技术的应用对计算机带来了革命性的变化，使计算机的安全上了一个新的台阶，能检测到一些恶意的攻击。

参考文献：

[1] 宋雅飞 . 计算机应用教学中的网络信息安全研究 [J]. 软件 ,2021,42(04):184-186.

[2] 何佳林 . 基于大数据分析的计算机网络时序信息安全监测 [J]. 信息与电脑 (理论版),2023,35(24):215-217.

[3] 孙美玲 . 基于大数据分析的计算机网络信息安全监测 [J]. 信息与电脑 (理论版),2023,35(22):239-241.

[4] 刘仲驰 . 基于信息融合的计算机网络信息传输安全监测方法 [J]. 长江信息通信 ,2023,36(04):137-139.