第 2 卷◆第 2 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

计算机网络发展中防火墙技术的研究与应用

刘岩岩　李祥宇
郑州科技学院
DOI:10.12238/acair.v2i2.7370

[摘　要] 本文探讨了计算机网络发展中防火墙技术的研究与应用,从相关概述、实际应用安全问题、防火墙技术的应用分析以及未来发展趋势等方面展开讨论。首先介绍了网络安全的重要性以及防火墙体系的结构,然后对常见的防火墙类型进行了详细分析。随后,讨论了计算机网络技术在实际应用中可能面临的安全问题,并探讨了防火墙技术在应对这些问题时的应用方法。最后,展望了防火墙技术未来的发展趋势,包括智能化、云原生化、多层次防御和零信任安全模型等方面的发展方向。
[关键词] 计算机网络；防火墙技术；网络安全；过滤型防火墙
中图分类号：TP393　**文献标识码**：A

Research and application of firewall technology in the development of computer network

Yanyan Liu　Xiangyu Li
Zhengzhou University of Science and Technology

[Abstract] This paper discusses the research and application of firewall technology in the development of computer network, and discusses the relevant overview, practical application security issues, application analysis of firewall technology and future development trends. First, the importance of network security and the structure of firewall architecture are introduced, and then the common types of firewalls are analyzed in detail. Subsequently, the security problems that may be faced by computer network technology in practical application are discussed, and the application methods of firewall technology in dealing with these problems are discussed. Finally, the future development trend of firewall technology is prospected, including the development direction of intelligence, cloud native, multi-level defense and zero trust security model.
[Key words] computer network; firewall technology; network security; filtering firewall

引言

随着数字化时代的到来,计算机网络已成为人们日常生活和工作中不可或缺的一部分。然而,网络安全问题也随之而来,如网络攻击、数据泄露等威胁日益严重。在这样的背景下,防火墙技术的研究与应用显得尤为重要。防火墙作为网络安全的第一道防线,可以有效监控和控制网络流量,保护网络系统免受未经授权的访问或攻击。深入了解防火墙技术的相关概念、结构和类型,以及其在实际应用中的安全问题和未来发展趋势,对于提高网络安全水平,保障个人和组织的信息资产安全具有重要意义。

1 相关概述

1.1网络安全

在当今数字化时代,网络安全是保护计算机系统及其数据不受未经授权的访问或损害的一系列措施的综合体。随着互联网的普及和信息技术的迅速发展,人们对网络安全的关注度越来越高。网络安全问题不仅涉及个人隐私和财产安全,还关系到国家的安全和经济发展。因此,加强网络安全意识,采取有效的安全措施,成为了当今社会的重要任务之一。

1.2防火墙体系的结构

防火墙体系是指由多种组件构成的网络安全系统,其目标是监控、过滤和控制网络流量,以保护网络不受未经授权的访问或攻击。防火墙体系的结构主要包括以下几个关键组件。网络边界设备通常是指位于内部网络和外部网络之间的设备,如防火墙、路由器等。它们负责过滤和控制进出网络的流量,是防火墙体系的第一道防线。安全策略是定义了网络安全规则和策略的集合,包括允许或拒绝特定类型的流量、设置访问控制规则等。制定合理的安全策略对于保护网络安全至关重要。访问控制列表(ACL)是用于根据预先定义的规则对数据包进行过滤和控制的工具。它们可以基于源地址、目标地址、端口号等信息来限制特定类型的流量。安全检测系统包括入侵检测系统(IDS)和入侵防御系统(IPS)等,用于检测和防止网络中的恶意活动和攻击。它们通过监控网络流量和系统日志来发现潜在的安全威胁,并采取相应的措施进行应对。

1.3常见的防火墙类型

1.3.1过滤型防火墙技术

过滤型防火墙技术是最早出现的防火墙类型之一,其原理是根据预先设定的规则对网络流量进行过滤和控制。它通过检查数据包的源地址、目标地址、端口号等信息,决定是否允许数据包通过防火墙。过滤型防火墙具有简单、高效的特点,适用于对网络流量进行基本过滤和控制的场景。

1.3.2代理型防火墙技术

代理型防火墙技术通过代理服务器代表客户端与服务器之间的通信,有效地隐藏了内部网络结构,并提供了对传输内容的深度检查和控制。它与传统的过滤型防火墙相比,具有更高的安全性和灵活性。代理型防火墙可以检查和过滤传输内容,防止恶意代码和攻击流量进入内部网络,是保护关键业务系统和数据的重要手段之一。

1.3.3复合型防火墙技术

复合型防火墙技术是将过滤型和代理型防火墙技术结合起来的一种防火墙形式。它既具有过滤型防火墙的高效性,又具有代理型防火墙的安全性。复合型防火墙可以根据具体的安全需求,灵活选择过滤和代理的方式来对网络流量进行处理,提供了更加全面和灵活的安全保护。

1.3.4配置技术

防火墙的配置技术是指对防火墙的配置和管理方法。合理的配置技术可以提高防火墙的安全性和性能,包括设置访问控制规则、更新安全策略、管理用户权限等。有效的配置技术可以帮助管理员及时发现和应对网络安全威胁,保护网络不受攻击和入侵。

1.3.5协议技术

防火墙的协议技术是指防火墙对网络协议的支持和处理能力。不同的防火墙可以支持不同的网络协议,如TCP/IP协议、UDP协议、HTTP协议等。协议技术决定了防火墙对网络流量的识别和处理能力,对于保护网络安全具有重要意义。有效的协议技术可以帮助防火墙准确识别和过滤不同类型的网络流量,提高网络的安全性和可靠性。

2 计算机网络技术在实际应用中的安全问题

2.1无法保证数据的绝对安全

在实际应用计算机互联网技术时,可能会因技术人员操作的方式以及主机的型号而产生不同的现象,这些差异上的表现能够导致后期网络防护能力出现较大的差异。所以,信息网络内的数据信息可能会因各种环境因素和人为操作因素的干扰出现泄露现象,严重威胁到个人的工作安全性。此外,还有部分熟知信息网络安全技术方式的人员,在追求利益的过程中可能出现方向偏差的状态,将自己的目标放于窃取个人信息方面,他们也会逐渐升级自己的操作技能来对抗当前不断丰富和完善的防火墙技术手段,都会对整个互联网信息造成极大的威胁。

2.2网络环境中的潜在威胁

人们在使用互联网信息技术过程中会存在信息交互的特点,能够在较短的时间内获得有用的信息,便于人们进行日常的生活和工作。但对于整个计算机互联网而言,其优势和劣势都会存在于整个互联网技术的应用过程中,而且当人们从不同的角度来进行信息搜索时,可能得到的结果并不完全一样,这些现象都会严重干扰人们的正确选择,甚至会威胁到人们使用计算机互联网的安全性。

2.3外力因素影响

在选择计算机设备时,用户根据需求和能力选购不同型号的设备,但制造商的设定差异会影响设备对信息侵扰的抗干扰能力。人为因素和自然因素是影响计算机系统安全的两大威胁。自然因素包括设备磨损和环境影响,如使用年限增加和环境腐蚀。然而,实际应用中人为因素更为重要。黑客攻击和病毒侵袭是主要威胁,黑客可能利用病毒窃取个人信息牟利,危及整个计算机系统。操作人员可能因误判而安装病毒,加剧安全风险。因此,加强对人为因素的防范和培训至关重要,以提高计算机网络系统的整体安全性。

3 计算机网络安全中防火墙技术的应用分析

3.1分析用户行为

在计算机互联网信息系统运行过程中,针对用户行为进行深入分析是必要的,基于收集到的各类信息,进行前瞻性预测与后期评估,为了更有效地识别项目进程中遇到的限制因素及优势条件,有必要进行全面分析,随后,通过整理这些信息数据,对互联网内部的系统进行相应参数的调整,选取最优秀的操作设备和系统,以减少安全风险。对用户的行为进行提前分析是必不可少的,特别地,需要预先精准预测那些可能诱发违法行为的活动,并充分利用各类丰富的数据库资源进行有效筛选,以确保网络整体安全。

3.2数据准确获取

在管理和应用整个互联网信息系统方面,系统管理人员扮演着关键角色,他们需要运用恰当的方法对各种信息进行全面深入的分析,并通过及时的监督来确保各类信息的完整性和准确性。其中,NAT(网络地址转换)技术在整个应用体系中发挥着至关重要的作用,它能够实现内部网络与外部网络的隔离,使两者在原地址上实现各自独立的发展目标,从而确保数据信息的安全传输。

3.3访问策略

在整个互联网操作应用技术的后期运行中,访问策略对于关键决策具有深远的影响。并且通过执行访问策略的操作方法,可以最大限度地保障信息安全,优化各种操作系统的合理性,减轻工作人员的工作负担。此外,访问策略还为工作人员在信息检索方面提供了有力支持,进一步提升网络安全防护能力。同时,访问策略的实施可以与相关安全技术协同进行,优化保护措施以满足用户合理需求,还可对访问者的每次操作进行实时信息收集与存储,为了便于后期分析,方便用户对个人数据进行全面比较,现将数据整合,搜集并分析员工个人信息以找到最适合他们的方案。最后,操作人员必须在检测过程中识别并解决潜在的

漏洞现象，只有不断对其进行适时调整，才能逐步提升安全防护能力。

3.4在日志监控中应用

在用户全面运用网络的过程中，鉴于信息复杂性，某些操作记录或许会存在，从而塑造出独特的互联网日志，防火墙可以借助对这些日志的分析来实现保护功能。此外，信息筛选功能得以实现，按照用户所处阶段进行分类储存，以有效提升防控成效。同时，日志监控对于确保整个系统的稳定运行具有显著作用，确保用户个人数据独立存在，依然能够保障整个网络信息系统的稳定运行。

4 计算机网络中防火墙技术的发展趋势

计算机网络中防火墙技术正迎来智能化发展，利用机器学习和人工智能实现实时监测和自动应对安全威胁。同时，防火墙与云计算融合，采用云原生技术在动态环境中保护网络流量。多层次防御成为主流，结合边界、内部和终端防火墙构建完整防御体系。零信任安全模型崭露头角，强调对每个访问请求进行严格验证和授权，实现精细化访问控制。

5 结语

随着计算机网络的不断发展，防火墙技术在确保网络安全方面扮演着至关重要的角色。通过不断创新和发展，防火墙技术已经逐步智能化、云原生化，并采用多层次防御和零信任安全模型等先进策略，以更好地适应日益复杂的网络安全威胁。未来，我们期待防火墙技术能够继续提升自身的智能化和自动化水平，与新兴技术紧密结合，为网络安全提供更加强大的保护。同时，我们也应不断加强对网络安全的重视，共同构建一个安全、稳定的网络环境，保护用户的数据和隐私不受侵害。

[参考文献]

[1]孙会儒.计算机网络安全技术及其完善对策探析[J].电子测试,2017(06):120+119.

[2]陈文涛.大数据时代计算机网络安全技术的优化策略[J].网络安全技术与应用,2023(11):157-158.

[3]包敏."互联网+"背景下中职计算机网络安全专业课程的教学创新探究[J].现代职业教育,2022(08):127-129.