

计算机网络信息安全中防火墙技术研究

刘静宜

潍坊职业学院 山东 潍坊 262737

摘要：随着信息时代的迅猛发展，计算机网络已成为人们日常生活、学习工作中不可或缺的一部分。计算机网络的普及和使用，使人们享受了前所未有的信息化便利和高效性，同时也导致了计算机网络安全隐患与风险。恶意攻击、网络病毒、黑客入侵等都会对计算机网络的信息安全造成不同程度的威胁和损失。针对这些安全隐患，防火墙技术应运而生，成为计算机网络信息安全中必不可少的环节之一，也成为许多企事业单位信息安全保障的重要手段之一。

关键词：计算机网络；信息安全；防火墙技术

引言

本文将从防火墙技术的基本概念入手，探讨防火墙技术在计算机网络信息安全中的作用，针对当前防火墙技术面临的挑战，分别从技术、管理、监管等方面进行分析和探讨，提出相应的应对策略和建议，以全面提升计算机网络信息安全保障水平。

1 防火墙技术基础

防火墙，是指在计算机网络中设置的安全措施，旨在控制将（不）允许通过网络边界的网络流量，并在其中认证和授权用户。可确保网络系统的安全性、可靠性和完整性，有效地保障网络业务的信息安全。防火墙技术的主要功能有：包过滤、应用层网关、网络地址转换、流量管理等。其实质是通过限制计算机网络中各个网络节点之间的通讯，保证了特定节点或者网络之内的信息传输安全性。防火墙的设置，能够帮助企业或者单位建立起安全的网络边界，构建一个相对安全的互联网环境^[1]。

2 防火墙技术在计算机网络信息安全中的作用

防火墙技术在计算机网络信息安全中的作用主要有以下几个方面：

2.1 保护私有网络资源

企业或事业单位的网络系统是包括多个节点的网络结构体系，其中部分节点是用于提供服务的，另外一部分节点则是作用户终端进行使用的。如果在网络中没有设置防火墙，那么外来用户就可以直接通过互联网入侵到企业内部的网络系统，获取相关信息，造成巨大的财产和人员损失。而设置防火墙，就可以有效的保护企业内部网络，实现网络资源的有效保护。

2.2 防范黑客攻击

黑客作为计算机网络安全的一大威胁，其手段多样，能力过硬，一旦入侵企业或事业单位的网络系统，

就有可能造成极大的损失。而防火墙通过对网络流量的控制和检测，可以有效地识别网络中的恶意攻击和威胁，防止黑客攻击^[2]。

2.3 保障网络通信安全

企业或事业单位的网络平台之间经常需要进行数据传输、文件共享等操作，内容涉及机密信息泄露的风险。针对这种情况，防火墙的设置可以有效地保障网络通信的安全，防止机密信息泄露的风险。

2.4 控制网络资源开销

针对一些企业或者事业单位的网络，网络带宽很宝贵，对于一些滥用网络资源的用户或者计算机程序，会对网络系统的通讯质量和效率造成很大的影响。因此，针对这种情况，防火墙的设置可以有效地控制网络资源的开销，让网络资源得到更合理的利用。

3 防火墙技术面临的挑战

作为计算机网络信息安全保障中的一个主要环节，防火墙技术在其发展过程中面临着如下几个主要挑战：

3.1 新型网络威胁的不断增多

随着计算机网络技术的发展，新型威胁有进一步增多，如恶意软件、僵尸网络等^[3]。这些威胁都具有隐蔽性、渗透性、多样性等特点，会对网络的信息安全造成极大的威胁，给防火墙技术带来巨大的考验。

3.2 防火墙技术与业务质量之间的平衡

防火墙技术作为保障网络安全的一环，不可避免地会对业务质量造成一定的损失，如过滤数据包会导致一定的通讯延迟；加密会消耗大量的计算资源等。如何在保障网络安全的前提下兼顾业务网络的高效性和高质量，是防火墙技术的发展中需要解决的一个问题。

3.3 防火墙技术管理的复杂性

防火墙技术的管理需要网络管理人员具备一定的技术水平和管理经验，特别是在大型网络系统中，防火墙

技术管理需要关注的方面比较多,管理的复杂性也相对较高。

3.4 防火墙技术的监管不足

防火墙技术作为计算机网络安全的中流砥柱,其重要作用不可忽略。然而,防火墙技术的监管不足,导致很多企事业单位在网络安全保障方面投入不足,存在安全漏洞隐患。因此,加强对防火墙技术的监管是保障网络安全的必要条件^[4]。

4 针对防火墙技术面临的挑战的应对策略和建议

针对防火墙技术发展面临的挑战,应提出相应的应对策略和建议,以提升网络信息安全保障水平。具体如下:

4.1 提高防火墙技术保护能力

随着数码技术的飞速发展,网络安全问题也愈发突出。不仅仅是黑客攻击和病毒感染等常见威胁,如今出现了许多新型的网络威胁,这些威胁的基本特征是攻击手段难以被传统的防火墙技术检测到和防御。因此,必须采取新型的技术手段来加强防火墙的保护能力。

提高防火墙技术保护能力,需要考虑的因素非常多,比如需要考虑的网络流量,攻击特征等等。为了保障网络的安全性,防火墙需要具备强大的加密和检测功能,这也是提升防火墙技术的核心方向之一。在加密方面,新型防火墙技术可以采用更为先进的算法来加密和保护数据,比如利用高级的加密算法、区块链技术等来保证数据的安全。在防御方面,可以利用大数据技术和人工智能算法来识别和过滤网络流量^[5]。这些技术可以预测特定的威胁模式,并提供建议和反馈,以便及时做出应对措施。此外,还可以借助虚拟隧道技术来实现网络跟踪和定位,加强网络管理与维护能力。同时,不断加强网络安全意识的普及和技术员的职业素养析,也是提升防火墙技术保护能力的重要因素之一。

总之,提高防火墙技术保护能力不是一朝一夕的事情,需要针对不同的网络威胁,采取不同的技术手段和策略,才能真正实现网络安全和信息保护的目标。

4.2 强化防火墙技术与业务质量之间的平衡

防火墙技术在保障网络安全方面起着至关重要的作用,但是如果不注意防火墙技术与业务质量之间的平衡,可能会导致业务网络的效率和质量受到影响,这对于企业或组织的日常运营和发展都将带来一定的风险和挑战。

为了强化防火墙技术与业务质量之间的平衡,需要在提高防火墙技术处理能力和性能优化方面下功夫。具体来说,可以采用以下措施:

第一,通过升级防火墙硬件和软件配置,提高其运

行性能。可以考虑采用高效的多核处理器、高速网络接口、快速缓存等硬件设备,或者采用先进的技术和算法来优化防火墙软件的功能和性能。第二,优化防火墙策略,减少对业务网络的影响。可以通过合理的策略配置和流量过滤来减少对业务流量的影响,确保业务网络的畅通和高效。此外,可以定期优化防火墙策略和规则,以应对新兴的威胁和攻击方式。第三,采用新型的质量保证技术,确保业务网络的稳定性和可靠性。可以借助网络监控和流量分析等技术,及时发现和排除业务网络中的问题,确保网络的稳定与高效。总之,强化防火墙技术与业务质量之间的平衡对于保障网络信息安全和企业的日常运营都至关重要。需要通过提高防火墙技术的处理能力和性能优化,以保证在保障网络安全的前提下,确保业务网络的高效性、高质量。

4.3 加强防火墙技术管理

随着防火墙技术的不断发展和应用,防火墙技术管理的复杂性也不断增加。为了更好地保护网络的安全性,网络管理人员需要具备一定的技术能力和管理经验,并且需要不断学习和培训,不断提高自身的技能水平和管理能力。

首先,网络管理人员需要具备良好的防火墙技术基础,能够熟练掌握防火墙的配置、管理、监控等方面的知识,能够对互联网和内部网络的流量进行有效的过滤和防御。网络管理人员还需要具备一定的网络安全知识,了解各种网络攻击和威胁的特征和防御措施,并能够制定相应的应对策略。其次,网络管理人员需要加强学习 and 培训,不断提高技能水平和管理能力。可以通过参加各种培训课程和活动来提高自身的技术水平和管理能力,还可以参加各种安全技术讲座、技术交流会等活动,了解最新的安全技术和解决方案,积累丰富的实践经验。最后,网络管理人员需要认真履行自己的职责,建立完善的防火墙技术管理制度和流程,确保防火墙的及时更新和漏洞修复,定期进行安全审查和检测,及时发现和排除各种安全隐患和漏洞,保证防火墙技术的有效应用,提高网络安全的整体水平。总之,加强防火墙技术管理是确保网络安全和信息保护不可或缺的一环。网络管理人员需要具备良好的技术能力和管理经验,加强学习和培训,不断提高自身的技能水平和管理能力,以建立完善的防火墙技术管理制度和流程,确保防火墙技术的有效应用,保障网络的稳定和安全。

4.4 加强防火墙技术监管

随着网络技术的普及和应用,网络安全问题也愈发突出。防火墙技术的应用对于保障网络安全起着至关键

要的作用。然而，由于防火墙技术监管不足，网络安全隐患问题持续存在。因此，加强防火墙技术的监管显得十分必要。

为了加强防火墙技术的监管，首先需要建立网络安全保障的法律体系和管理规范。在政策法规层面，需要针对网络攻击和违法行为制定相应的法律规定，完善网络安全的保护体系。政府和相关组织需要加大对防火墙技术监管的力度，制定相应的管理规范 and 标准，确保防火墙技术符合安全标准和监管要求。同时，必须要求企业和机构对于防火墙技术的应用进行有效控制和开展相关培训，确保技术的有效性 with 安全性。其次，对于违规操作和行为需要进行深入调查和严格处罚。网络攻击和安全事件发生之后，需要开展严格的调查工作，深入分析案件的原因和影响，并对违规操作者进行处罚。大力打击网络犯罪活动，加强网络安全维护，为防火墙技术的应用提供更加有力的保障。总之，加强防火墙技术的监管是保障网络安全和信息保护的关键环节之一。需要建立网络安全保障的法律体系和管理规范，加大对防火墙技术监管的力度，对于违规操作和行为进行深入调查和严格处罚。这将有效提高防火墙技术的管理水平，强化对网络安全的保障，给企业和群众带来更加安全的网络环境。

5 计算机网络信息安全中防火墙技术发展趋势

防火墙技术作为网络信息安全领域的重要组成部分，不断发展和演进，以适应网络安全威胁的不断变化。下面将从以下几个方面探讨防火墙技术的发展趋势。

云安全与SDN技术的融合随着云计算技术的逐渐普及和应用，云安全成为关注的热点之一。防火墙技术也要与云计算相结合，支持虚拟化环境，重新定义边界安全、虚拟化安全等新需求。云安全需要更高效、灵活和安全的网络安全技术，如网络功能虚拟化（NFV）和软件定义网络（SDN）等技术，SDN将网络控制平面从硬件设备中剥离，将其转化为可编程软件的控制平面，允许数据中心管理员编写控制规则，使其更具可扩展性、灵活性和协同性，提供更加高效、全面的安全保障措施。

网络安全与人工智能的结合现代网络安全攻击形势十分复杂，传统的安全机制难以胜任。为此，网络安全需要从被动防御转向主动防御。人工智能（AI）或机器学习技术可以提高网络安全的主动防御能力。利用大数据技术和机器学习算法对网络流量进行分析，识别异常流量和恶意攻击行为，并在发现异常时自动屏蔽和清

除，从而提高网络安全的能力。

IoT安全需求的增加物联网（IoT）终端设备越来越多，设备间连接越来越密切，但这同时也带来了更多的安全威胁。IoT安全问题是目前关注的重点之一。IoT环境中的防火墙技术更需要具备更高的可靠性、稳定性和安全性，能够实现对IoT设备的安全管理和控制。防火墙需要依据IoT网络设备的特点定制化安全策略和规则，可根据设备间的互联和数据交互模式，自适应地进行安全检测和访问控制。

多维度安全策略的应用在网络安全防护上，防火墙将不再只是单点防御，而是将多层面的防御方案进行结合，实现一体化防御，包括物理、虚拟、云环境、区域、全局的网络安全，同时也包括安全预警、反控制、溯源、自省、动态学习和应急响应等方面。这将更好地预防安全威胁，及时发现和排除安全问题。

总之，防火墙技术将在技术和应用方面不断演进和创新，以适应不断变化的网络安全威胁。云安全、SDN技术、人工智能和IoT安全，多维度安全策略等将成为防火墙技术发展的重要趋势。网络安全从被动防御到主动防御的转变是未来网络安全的核心趋势之一，防火墙技术也需要实现从单点防御向多层防御的转变。

结束语

防火墙技术在计算机网络信息安全保障中扮演着不可或缺的角色，通过对网络流入流出的数据包进行过滤、检测和加密，有效的实现了网络信息的安全保障。然而，防火墙技术在其发展过程中，不可避免的面临着新型网络威胁、业务质量平衡、管理复杂性和监管不足等挑战，因此，应提出相应的应对策略和建议，推动防火墙技术应用的进一步发展。

参考文献

- [1] 翟建华.基于深度学习的防火墙技术研究[J].网络安全技术与应用,2021,12(1):52-57.
- [2] 姚昊.基于区块链技术的防火墙技术研究[D].贵阳: 贵州民族大学,2021.10(7): 90-92.
- [3] 吕敏.基于协同过滤的防火墙技术研究[D].沈阳: 沈阳工业大学,2020.16(10): 60-61.
- [4] 徐玉枝.基于人工智能的防火墙技术研究[D].杭州: 浙江大学,2020.
- [5] 郭岳.基于SDN的防火墙技术研究[J].电脑知识与技术,2019,15(10):190-192.